

About This Manual

Thank you for choosing Akuvox R20K-2 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to 28.30.3.111 version, and it provides all the configurations for the functions and features of Akuvox door phone. Please visit [Akuvox web](#) or consult technical support for any new information or latest firmwares.

Introduction of Icons and Symbols



Warning:

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



Caution:

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



Note:

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

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	8
2. Change Log	9
3. Model Specification	10
4. Introduction to Configuration Menu	11
5. Access the Device	13
5.1. Obtain Device IP Address	13
5.2. Access the Device Setting on the Device	14
5.2.1. Access Advance Setting Screen	14
5.3. Access the Device Setting on the Web Interface	14
6. Language and Time Setting	16
6.1. Language Setting	16
6.2. Time Setting	16
7. LED Setting	18
7.1. Infrared LED Setting	18
7.2. LED Setting on Card Reader Area	19
7.3. LED Settings on Keypad	20
7.4. LED Settings on Screen	20
7.5. LCD Text Display	21
7.6. Backlight Setting	22
7.7. Standby Mode Setting	22
8. Volume and Tone Configuration	24
8.1. Volume Configuration	24
8.1.1. Open Door Tone Configuration	25
8.1.2. Upload Tone Files	25
9. Network Setting	28
9.1. Network Status	28
9.2. Device Network Configuration	28
9.3. Device Deployment in Network	29
9.4. Device Local RTP configuration	30
9.5. NAT Setting	31
9.6. SNMP Setting	32
9.7. VLAN Setting	32
9.8. TR069 Setting	33
9.9. Device Web HTTP Setting	35
10. Intercom Call	36
10.1. IP call & IP Call Configuration	36
10.2. SIP Call &SIP Call Configuration	36
10.2.1. SIP Account Registration	37
10.2.2. SIP Server Configuration	38

10.2.3. Configure Outbound Proxy Server	39
10.2.4. Configure Data Transmission Type	39
10.3. Configure Calling Feature	40
10.3.1. DND	40
10.3.2. Speed Dial Call	41
10.3.3. Robin Call	42
10.3.4. Web Call	42
10.3.5. Dial Option	43
10.3.6. Auto Answer	44
10.3.7. Multicast	45
10.3.8. Configure Maximum Call Duration	46
10.3.9. Maximum Dial Duration	47
10.3.10. Hang Up After Open Door	48
10.3.11. Switch Cancel&Dial Key	49
11. Audio& Video Codec Configuration	50
11.1. Audio Codec Configuration	50
11.2. Video Codec Configuration	51
11.3. Video Codec Configuration for IP Direct Calls	52
11.4. Configure DTMF Data Transmission	52
12. Phone Book Configuration	54
12.1. Managing Contact Group	54
12.2. Managing Contacts	55
12.3. Export/Import Contacts	56
13. Relay Setting	58
13.1. Relay Switch Setting	58
13.2. Select Speed Dial triggered Relay	60
13.3. Web Relay Setting	60
13.4. Configure White List for Door Relay	62
14. Door Access Schedule Management	63
14.1. Configure Door Access Schedule	63
14.1.1. Manage Relay Schedule	63
14.1.2. Create Door Access Schedule	64
14.1.3. Import and Export Door Access Schedule	65
14.2. Door Unlock Configuration	65
14.3. Configure Access Card Format	66
14.4. Configure RF Card for Door Unlock	67
14.5. Edit the User-specific door access data	68
14.6. Import and Export User Data of Access Control	68
14.7. Configure Open Relay via HTTP for Door Unlock	69
14.8. Configure Exit Button for Door Unlock	70
14.9. Configure PIN Code for Door Unlock	71
14.10. Configure Public Code for Door Unlock	72
14.10.1. Configure Private PIN Code on the Web Interface	72
15. Security	75

15.1. Tamper Alarm Setting	75
15.2. Client Certificate Setting	75
15.2.1. Configure Action of Input	76
15.2.2. Web Server Certificate	76
15.2.3. Client Certificate	76
15.3. Motion Detection	78
15.3.1. Configure Motion Detection	78
15.4. Security Notification Setting	79
15.4.1. Email Notification Setting	79
15.4.2. FTP Notification Setting	80
15.4.3. SIP Call Notification Setting	80
15.4.4. Call Event Notification	81
15.4.5. HTTP URL Notification Configuration	82
15.5. Action URL	82
15.6. Security Action Configuration	83
15.6.1. Configure Action of Call	83
15.6.2. Configure Action of Motion	84
15.6.3. Configure Action of Body Temperature	84
15.7. Voice Encryption	85
15.8. User Agent	86
15.9. Body Temperature	86
16. Monitor and Image	88
16.1. RTSP Stream Monitoring	88
16.1.1. RTSP Basic Setting	88
16.1.2. RTSP OSD Setting	89
16.1.3. RTSP Stream Setting	89
16.2. MJPEG Image Capturing	91
16.2.1. NACK	92
16.3. ONVIF	93
16.4. Live Stream	94
17. Logs	95
17.1. Call Logs	95
17.2. Door Logs	96
18. Debug	98
18.1. System Log	98
18.2. Remote Debug Server	99
18.3. PCAP	99
19. Firmware Upgrade	101
20. Backup	102
21. Auto-provisioning	103
21.1. Provisioning Principle	103
21.2. Configuration Files for Auto-provisioning	104
21.3. AutoP Schedule	105
21.4. PNP Configuration	105

21.5. Static Provisioning Configuration	106
22. Integration with Third Party Device	108
22.1. Integration via Wiegand	108
22.2. Integration via HTTP API	109
22.3. Integration with Milestone	112
22.4. Power Output Control	112
22.5. Integration with Lift Control	113
23. Password Modification	114
23.1. Modifying Device Web Interface Password	114
23.2. Modifying Device System Password	114
23.3. Configure Web Interface Automatic Logout	115
24. System Reboot&Reset	116
24.1. Reboot	116
24.2. Reset	116
25. Abbreviations	117
26. FAQ	119
27. Contact us	122


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 R28A is a SIP-compliant, hands-free and video(optional) door phone. It can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. The door phone enables you to easily monitor an entrance door or gate and gives you 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

	R20K-2
Model & Feature	
Button	Numeric keypad + 3 physical buttons
Housing Material	Aluminum alloy
Camera	2M pixels, automatic lighting
Relay In	1
Relay Out	1
RS485	Optional
PoE	X
RAM	64MB
ROM	128MB
Card Reader	13.56MHz (with NFC) & 125kHz
IP Rating	IP65
IK Rating	X
Wall Mounting	√
Flush Mounting	√
Wall Mounting Dimension	185x85x29mm
Flush Mounting Dimension	226x108x52mm

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 the 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 cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using it.
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.

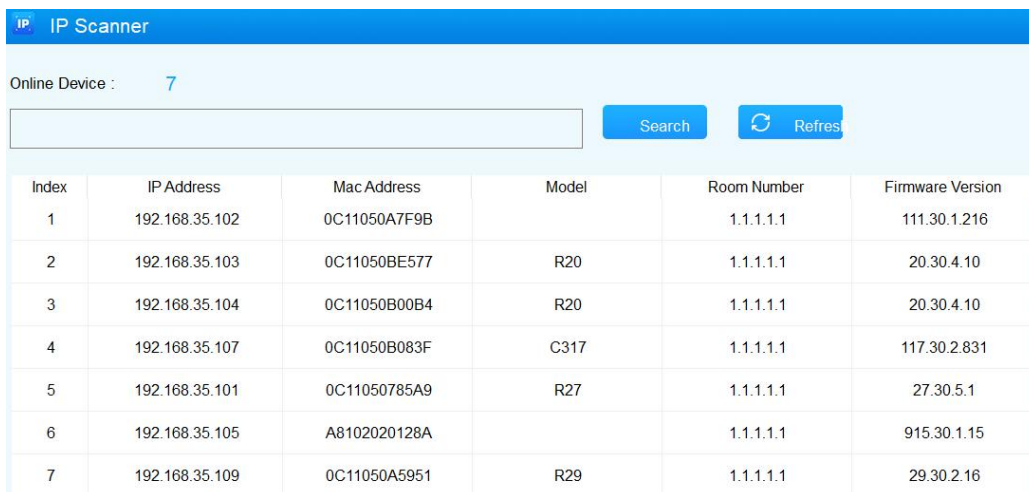
1. **SDMC:** SDMC is suitable for the management of Akuvox devices in large communities, including access control, resident information, remote device control, etc.
2. **Akuvox Upgrade tool:** Upgrade Akuvox devices in batch on a LAN (Local Area Network)
3. **Akuvox PC Manager:** Distribute all configuration 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

R28A series system setting can be accessed on the device web interface. And it can also be accessed on the device screen for some basic settings.

5.1. Obtain Device IP Address

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. Or checking the device IP address from the device setting screen. Please refer to [chapter 5.2](#) for device settings.



The screenshot shows the 'IP Scanner' interface. At the top, it says 'Online Device : 7'. Below this is a search bar and two buttons: 'Search' and 'Refresh'. The main part of the interface is a table with the following columns: Index, IP Address, Mac Address, Model, Room Number, and Firmware Version. The table contains 7 rows of data.

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



Note:

- Only R27A/R28A supports checking IP address from device setting screen.

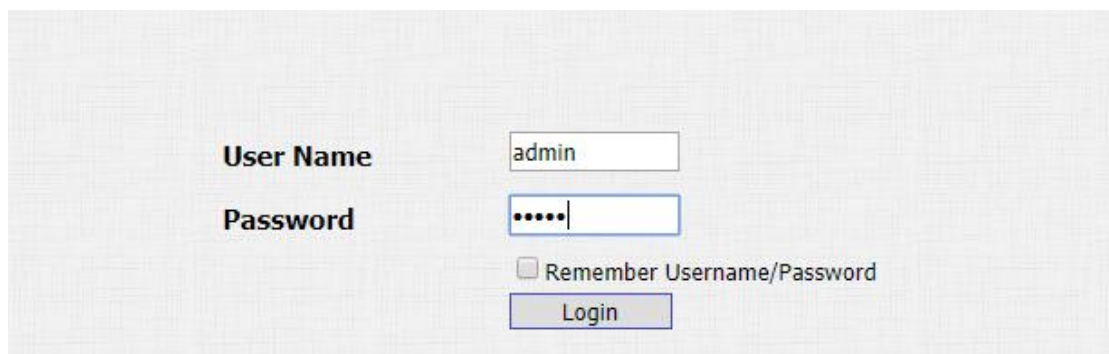
5.2. Access the Device Setting on the Device

5.2.1. Access Advance Setting Screen

Press “*2396#” to enter the advanced setting screen. It provides some advanced permissions like editing network, reset, admin password modification to administrators, including “System Information,” “Admin Settings” and “System Settings”.

5.3. Access the Device Setting on the Web Interface

Enter the device IP address on the web browser in order to log in to the 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.



The screenshot shows a login form with the following elements:

- User Name:** A text input field containing the text "admin".
- Password:** A text input field containing five dots, indicating a masked password.
- Remember Username/Password
- Login:** A button with the text "Login".

**Note:**

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

**Note:**

- Google Chrome browser is strongly recommended.

6. Language and Time Setting

6.1. Language Setting

When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can be set up on the device web Phone > Time/Lang > Web Language/LCD Language interface according to your preference.

The screenshot shows two sections for language settings. The first section is titled "Web Language" and has a "Type" label followed by a dropdown menu currently set to "English". The second section is titled "LCD Language" and also has a "Type" label followed by a dropdown menu currently set to "English".

Parameter Set-up:

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

6.2. Time Setting

The set-up on the device web Phone > Time/Lang > Type/NTP 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 with your device.

Type

Manual
 Auto

Date: Year Mon Day
 Time: Hour Min Sec

NTP

Time Zone:

Primary Server:

Secondary Server:

Update Interval: ($\geq 3600s$)

System Time: 10:20:19

Parameter Set-up:

- **Manual/Auto:** you can choose automatically to gain the time or manually configure the date and time.
- **Date:** it is available when you choose Manual. Set up the year, month and day according to your need.
- **Time:** it is available when you choose Manual. Set up the hour, minute and second according to your need.
- **Time Zone:** it is available when you choose Auto. Select the specific time zone depending on where the device is used and then press Confirm tab for the confirmation. The default time zone is GMT GMT+0.00.
- **Primary/Secondary Server:** it is available when you choose Auto. The time zone server, normally will automatically obtain the time when connecting to the network. The secondary server will take effect when the primary server is invalid.
- **Update Interval:** it is available when you choose Auto. To configure interval between two consecutive NTP requests.

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. If the infrared LED is turned off, the door phone will turn to night mode so that you can have a clear view of the visitor. You can set up it on the device web Intercom > Advanced interface.

Photoresistor	
Photoresistor Setting	<input type="text" value="1500"/> - <input type="text" value="1600"/> (0~1800)
Now	<input type="text" value="1174"/> <input type="button" value="Read"/>

Parameter Set-up:

- **Photoresistor Setting:** set the triggering points for disabling the infrared LED and enabling the infrared LED. For example, if you set the triggering points at 1500-1600, the infrared LED will be enabled when the photoresistor value gets higher than 1600 (the video image you see from the door phone will become black and white) and if the value gets lower than 1500, then the infrared light will be disabled (the video image you see will have color).
- **Now:** click Read to obtain the current environment brightness and use it as a reference to set up the photoresistor setting.

7.2. LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be disabled in order to reduce the electrical power consumption. To do this configuration on the web Intercom > LED Setting interface.

Card LED Enable	Disabled	▼		
Start Time (H)	18	-	06	(0~24)

Parameter Set-up:

- **Card LED Enable:** if enabled, the LED light will stay on during the time interval (Start Time (H)). If disabled, the LED light will stay off and will turn on only when you swipe cards or press the keypad, and the time interval will become non-editable.
- **Start Time (H):** set the time interval for the light to stay on. enter the time interval for the LED light to be turned on, e.g. if the time interval is set from 8-0 (Sart time- End time) it means LED light will stay on during the time span from 8:00 am to 12:00 pm during one day (24 hours). This setting can not be set up when you disable the LED light.

7.3. LED Settings on Keypad

You can enable or disable the LED lighting of keypad as needed on the web interface. Meanwhile, If you prefer not to have the LED light of keypad stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption, etc. To do this configuration on the web Intercom > LED Setting interface.

Start Time (H)	<input type="text" value="18"/> - <input type="text" value="06"/> (0~24)
KeyPad LED Enable	<input type="text" value="Disabled"/> ▾

Parameter Set-up:

- **Keypad LED Enable:** Click to enable or disable the keypad LED lighting.
- **Start Time (H):** Enter the time span for the LED lighting to be valid. Eg. If the time span is from 18-22 it means LED light will stay on during the time span from 6:00 pm to 22:00 pm during a day.

7.4. LED Settings on Screen

You can enable or disable the LED lighting of the screen as needed on the web interface. Meanwhile, If you prefer not to have the LED light of screen stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption, etc.

Wake Mode	<input type="text" value="Auto"/> ▾
Screen LED Enable	<input type="text" value="Disabled"/> ▾
Start Time (H)	<input type="text" value="18"/> - <input type="text" value="06"/> (0~24)

Parameter Set-up:

- **Wake Mode:** There are two modes - Auto and Manual for waking up the device when idle. If you select "Auto" mode then the screen will be

awakened when someone approaches, the IR sensor will be triggered. And if "Manual" mode is selected, then you have to touch the keypad.

- **Screen LED Enable:** click to enable or disable the screen LED lighting.
- **Start Time(H):** enter the time span for the LED lighting to be valid. Eg. If the time span is from 18-22 it means LED light will stay on during the time span from 6:00 pm to 22:00 pm during a day.

7.5. LCD Text Display

You can customize the LCD text during the idle by themselves, such as "Welcome" or something else. Only R27X and R28A support this function, you can do this configuration on the web Intercom > Advanced interface.

LCD Display	
LCD Display	Default ▾
LCD Text	Press call button

Parameter Set-up:

- **LED Display:** there are four modes - Default, Hide Contacts, Text Only and Contacts Only. If Default is selected, the main screen shows Call, Contacts, PIN Entry and Security Center. If Hide Contacts is selected, the main screen shows Call, PIN Entry and Security Center. If Text Only is selected, it will only show the customized text you entered. If Contacts Only is selected, it will only show Contacts.
- **LCD Text:** it is available when you choose Text Only. Enter the display content you need.

7.6. Backlight Setting

If you want to brighten up the screen in order to see the screen at greater ease in an environment with higher light intensity, you need to set up the related parameters in web Intercom > LED Setting > LED Control interface.

Backlight Value	<input type="text" value="180"/>	(0~255)
Backlight Stand by Value	<input type="text" value="0"/>	(0~255)

Parameter Set-up:

- **Backlight Stand by Value:** adjust the backlight for the screen in the standby mode with the value ranging from 0-255.
- **Backlight value:** set the backlight value when the device is working with the value ranging from 0-255.



Note:

- Only R27A and R28A support Backlight Settings.

7.7. Standby Mode Setting

Standby mode is mainly a function for screen protection. You can make the device go into idle status for a predefined time span when there is no operation on the device or no one is detected approaching the device screen. To do this configuration on the web Intercom > LED Setting > LED Control interface.

Standby Mode	<input type="text" value="Disabled"/>	▼
Time Out	<input type="text" value="15"/>	(5~300)

Parameter Set-up:

- **Standby Mode:** enable the standby feature, it screen will enter sleep mode within the time out value if there is no operation.
- **Time Out:** select the time duration from 15 seconds to 180 seconds before the device goes into idle status if the screen is not awakened. For example, if you set the “Standby Time” as 30 seconds, then the screen will go idle (Await screen) when the screen is not awakened for 30 seconds.

8. Volume and Tone Configuration

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

8.1. Volume Configuration

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

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

Volume Level	
Volume Level	<input type="text" value="1"/> ▾

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

Tamper Alarm Volume	
Tamper Alarm Volume	<input type="text" value="15"/> (1~15)

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

Parameters Set-up:

- **Mic Volume:** adjust the mic volume as needed.
- **Volume Level:** control the volume of all speakers. The default is 1, the first level of volume, the volume range is roughly 80-95, and 2 is the

second level of volume, the volume range is roughly 95-109.

- **Speaker Volume:** adjust the speaker volume as needed.
- **Tamp Alarm Volume:** adjust the volume for the tamper alarm.
- **Keypad volume:** adjust the volume of the keypad.

8.1.1. Open Door Tone Configuration

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



Open Door Warning	
Open Door Succ Warning	Enabled ▾
Open Door Failed Warning	Enabled ▾

Parameters Set-up:

- **Open Door Success Warning:** click the field Enabled or Disabled depending on if you want to hear the prompt words that accompany that Open Door Success tone.
- **Open Door Failed Warning:** click the field Enabled or Disabled depending on if you want to hear the prompt words that accompany that Open Door Failed tone.

8.1.2. Upload Tone Files

You can configure door phone ringback tone and other tones related to the door opening.

8.1.2.1. Upload Ringback Tone

You can customize the ringback tone if you need. Please follow the prompt about the file size and format. On the web, navigate to Phone > Voice > Ringback Tone.

RingBack Upload

No file chosen

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

8.1.2.2. Upload Open Door Tone

You can customize the tone of door open successful/failed if you need. Outside tone is used to open door via card or DTMF or PIN code. Inside tone is used to open door via triggered input interface. Please follow the prompt about the file size and format. On the web, navigate to Phone > Voice.

Opendoor Outside Tone Setting

Opendoor Outside Tone Setting

No file chosen

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

Opendoor Inside Tone Setting

Opendoor Inside Tone Setting

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:

- **Open Door Inside Tone:** warning tone that will go off when you opened the door from inside. Open door succeeded inside warning is what you can hear when you open the door by pressing the Exit button in side.
- **Broadcast Delay:** set open door success announcement delay from 0-60 seconds. For example, if you set it as "2" seconds, then you will hear the announcement 2 seconds after the successful door unlock.
- **Broadcast Frequency:** set the number of open door success announcements.
- **Broadcast Interval:** set the interval between the two open door success announcements.
- **Open Door outside Tone:** warning tone that will go off when you opened the door from outside. Open door succeeded outside warning is what you can hear when you are granted door access via access methods on the door phone.

9. Network Setting

9.1. Network Status

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

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

9.2. Device Network Configuration

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

LAN Port

DHCP
 Static IP

IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
LAN DNS1	8.8.8.8
LAN DNS2	

Parameter Set-up:

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

9.3. Device Deployment in Network

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

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

ConnectSetting	
Connect Type	Cloud <input type="button" value="v"/>
Discovery Mode	Enabled <input type="button" value="v"/>
Device Address	<input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="R28"/>

Parameter Set-up:

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

9.4. Device Local RTP configuration

For the device network data transmission purpose, 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 >

Local RTP	
Min RTP Port	11800 (1024~65535)
Max RTP Port	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.

9.5. NAT Setting

NAT (Network Address Translation) allows hosts in an organization's private intranet to transparently connect to hosts in the public domain. There is no need for internal hosts to have registered Internet addresses. It is a way to translate the internal private network IP address into a legal network IP address technology. The NAT in the device web is limited to maintaining a connection with the remote SIP server. The principle is to send a heartbeat message to the remote SIP server at a set interval after the function is turned on. Otherwise, the server may judge that the device is offline and allocate the SIP assigned to other devices, resulting in failure to connect to it in the future. To do this configuration on web Account > Advance > NAT interface.

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

Parameter Set-up:

- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that SIP server will recognize if the device is in online status.

- **UDP Alive Msg Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort:** enable the RPort when the SIP server is in WAN (Wide Area Network).

9.6. SNMP Setting

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. SNMP is widely used in 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	<input type="text" value="Disabled"/>
Port	<input type="text" value=""/> (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.

9.7. VLAN Setting

Virtual Local Area Network is a logical grouping of two or more nodes that 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 the 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 hosts 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 the broadcast frame. To save bandwidth for high efficiency, it will be better to separate broadcast domain by deploying VLAN. To do the configuration on the web Network > Advanced > VLAN interface.

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

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.

9.8. 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 <input type="button" value="v"/>
	Version	1.0 <input type="button" value="v"/>
	URL	<input type="text"/>
	User Name	<input type="text"/>
Periodic Inform	Password	*****
	Active	Disabled <input type="button" value="v"/>
	Periodic Interval	1800 (3~24×3600s)
CPE	URL	<input type="text"/>
	User Name	<input type="text"/>
	Password	*****

Parameter Set-up:

- **Active:** to enable or disable the 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.

9.9. 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	<input type="text" value="Enabled"/>
Https Enable	<input type="text" value="Enabled"/>
Http Port	<input type="text" value="80"/> (80,1024~65534)

Parameters Set-up:

- **Http Enable:** set whether HTTP access to the device webpage is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **Https Enable:** set whether HTTPS access to the device webpage 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.

10. Intercom Call

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. To do this configuration on web Phone > Call Feature > Others interface.

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

Parameters Set-up:

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

10.2. SIP Call &SIP Call Configuration

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

10.2.1. SIP Account Registration

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

10.2.1.1. Configure SIP Account Configuration

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 Active:** click Enable or Disable to activate or deactivate the registered SIP account.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.
- **User Name:** enter the user name obtained from SIP account administrator.
- **Account:** select the exact account (Account 1&2) to be configured.

- **Display Label:** configure the device label to be shown on the device screen.
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

10.2.2. SIP Server Configuration

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

SIP Server 1		
Server IP	<input type="text" value="192.168.35.11"/>	Port <input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

SIP Server 2		
Server IP	<input type="text"/>	Port <input type="text" value="5060"/>
Registration Period	<input type="text" value="1800"/>	(30~65535s)

Parameter Set-up:

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

10.2.3. Configure Outbound Proxy Server

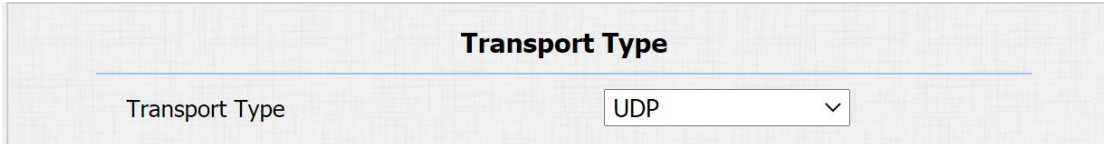
An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish call session via port-based data transmission. To set it up on the device web Account > Basic > Outbound Proxy Server Interface.

Parameter Set-up:

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

10.2.4. Configure Data Transmission Type

SIP messages 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. To do this configuration on web Account > Basic > Transport Type interface.



Transport 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.

10.3. Configure Calling Feature

You can select the SIP account for making SIP calls. On the web, navigate to Intercom > Basic.



Intercom-Basic

Basic

Select Account

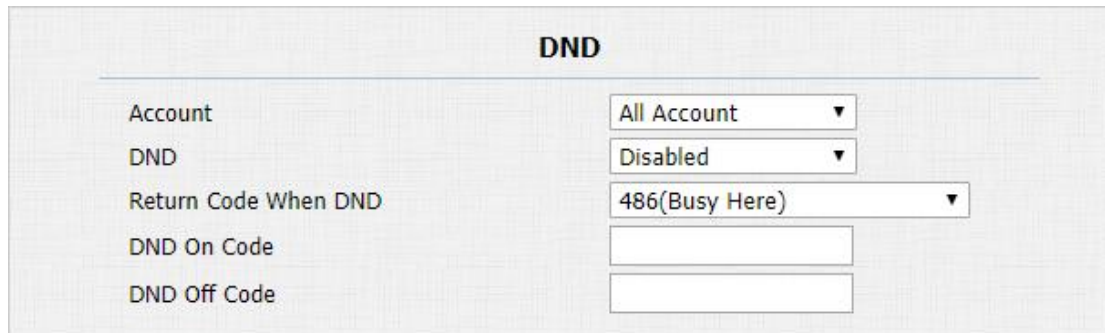
Auto

Parameter Set-up:

- **Select Account:** if you select “Auto” when both account 1 and account 2 are registered, then the call will be made from account 1, however, if either account 1 or account 2 is registered, then the call will only be made from the registered account. You cannot make any calls from the account1/2 that are not registered.

10.3.1. DND

DND (Do not disturb) setting allows you not to be disturbed by any unwanted incoming SIP calls. You can set up DND related parameters properly on the device web Phone > Call Feature > DND 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	<input type="text"/>
DND Off Code	<input type="text"/>

Parameter Set-up:

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

10.3.2. Speed Dial Call

Speed Dial is used to quickly initiate the pre-configured numbers by pressing Dial key. You can create up to 40 numbers on R28A and up to 80 numbers on R27A. To do the configuration on the web Intercom > Basic > Speed Dial

interface.

Key	Number	Number	Number	Number
Speed Dial 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Speed Dial 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameters Set-up :

- **Add :** click to show more numbers.

10.3.3. Robin Call

Robin call is used to initiate multiple numbers from one family in Akuvox SmartPlus one by one. If the previous callee does not answer within the robin call timeout, the call will be transferred to the next one. If the call is answered by one of the callees, the call will not be transferred anymore. This feature is only available when connecting Akuvox SmartPlus. To do the configuration on the web Intercom > Basic > Robin Call interface.

Robin Call

Robin Call Enable

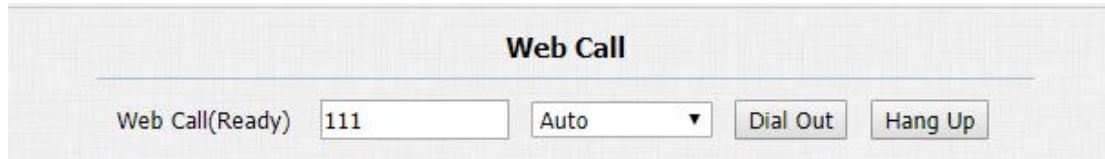
Robin Call Timeout

Parameters Set-up:

- **Robin Call Enable:** it is disabled by default. It needs to be controlled by Akuvox SmartPlus.
- **Robin Call Timeout:** call out time value for each number, ranging from 5 - 60s.

10.3.4. 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. To do the configuration on the web Intercom > Basic > Web Call interface.



The screenshot shows a web interface titled "Web Call". Below the title is a horizontal line. Underneath the line, there is a status indicator "Web Call(Ready)", a text input field containing "111", a dropdown menu currently showing "Auto", and two buttons labeled "Dial Out" and "Hang Up".

Parameters Set-up:

- **Auto/Account1/Account2:** to choose a suitable SIP account to make a web call. If you call out using IP address, Account selection is not need to be chosen.

10.3.5. Dial Option

If you want to replace the long and complex dial number with a shorter number that can be memorized at greater ease and convenience for making calls. You can replace multiple device dial numbers such as IP addresses with only one short number. To configure the number replacement on the device, navigate to Phone > Dial Plan, then click Add. To replace the number in batch, you can import the .xml file to the door phone. And the file from the door phone can be exported out before importing them to other door phones.

Dial Plan

Rules Management

No file chosen (.XML)

Index	Account	Name	Prefix	Replace 1	Replace 2	Replace 3	Replace 4	Replace 5	<input type="checkbox"/>
1	Auto	123	1	akuvox002					<input type="checkbox"/>
2									<input type="checkbox"/>
3									<input type="checkbox"/>
4									<input type="checkbox"/>
5									<input type="checkbox"/>
6									<input type="checkbox"/>
7									<input type="checkbox"/>
8									<input type="checkbox"/>
9									<input type="checkbox"/>
10									<input type="checkbox"/>

Page:

Rules Modify >>

Account	Auto <input type="button" value="v"/>
Name	
Prefix	
Replace 1	
Replace 2	
Replace 3	
Replace 4	
Replace 5	

10.3.6. 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 Phone > Call Feature>Others.

Auto Answer	Enabled ▾
Auto Answer Delay	0 (0~5s)
Auto Answer Mode	Video ▾

Parameters Set-up:

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

10.3.7. 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. To do the configuration on the web Phone > Multicast interface.

Multicast Setting

Paging Barge

Paging Priority Active

Priority List

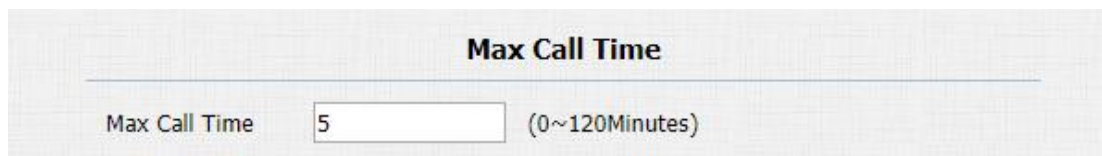
IP Address	Listening Address	Label	Priority
1 IP Address	<input type="text" value="224.1.6.11:1200"/>	<input type="text" value="Akuvox"/>	1
2 IP Address	<input type="text"/>	<input type="text"/>	2
3 IP Address	<input type="text"/>	<input type="text"/>	3
4 IP Address	<input type="text"/>	<input type="text"/>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

Parameters Set-up:

- **Paging Barge:** multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority Active, SIP call will have high priority.
- **Paging Priority Active:** multicast calls are called in order of priority or not.
- **Listening Address:** enter the multicast IP address you want to listen. The multicast IP address 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.

10.3.8. 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. To do this configuration on the web Intercom > Basic > Max Call Time interface.



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


10.3.9. Maximum Dial Duration

Maximum Dial duration consists 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 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. To do this configuration on the web Intercom > Basic > Max Dial Time interface.

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

Parameters Set-up:

- **Dial in Time:** enter the dial in time duration for 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 out the call it dialed out automatically if the call is not answered by the device being called.

 **Note:**

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

10.3.10. Hang Up After Open Door

This feature is used to hang up the call automatically after the door is released during a call. So the caller or callee does not need to click hang up key again. To do this configuration on the web Intercom > Basic> Hang Up After Open Door interface.

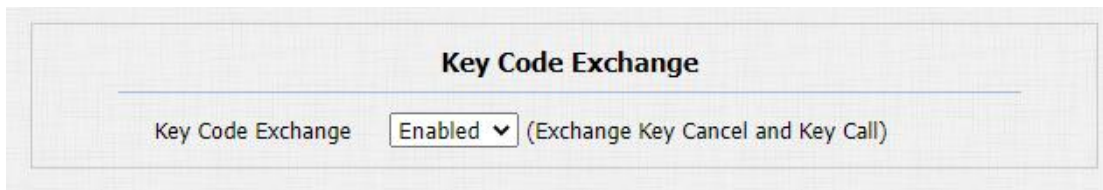
Hang Up After Open Door	
Timeout	<input type="text" value="5"/> (0~15)

Parameter Set-up :

- **Timeout:** the time out value can be set up from 1 second to 15seconds. 5 seconds is the default. The call will be automatically hang up within this value after the door is opened.

10.3.11. Switch Cancel&Dial Key

On R28 door phones, the Cancel Keys and Dial keys can be different in their positions functionally and physically. Either the Cancel key is right on the top of the Dial key or the other way round. You can reverse their functional positions on the web to match their physical position on the keypad. On the web, navigate to Intercom > Advanced > Key Code Exchange.



Key Code Exchange

Key Code Exchange (Exchange Key Cancel and Key Call)

Parameter set-up:

- **Key Code Exchange:** if enabled, the Cancel function will be placed right on the top of Dial function in their functional location. If disabled, their functional location will be functionally reversed.

11. Audio & Video Codec Configuration

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 bandwidths and sample rates flexibly according to the actual network environment. It is only available for SIP call. To do the configuration on device web Account > Advanced interface.

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

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

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

11.2. Video Codec Configuration

Akuvox door phone support H264 codec that provides a better video quality at a much lower bit rate with different video quality and payload. It is only available for SIP call. To set up video codec on web Account > Advanced interface.

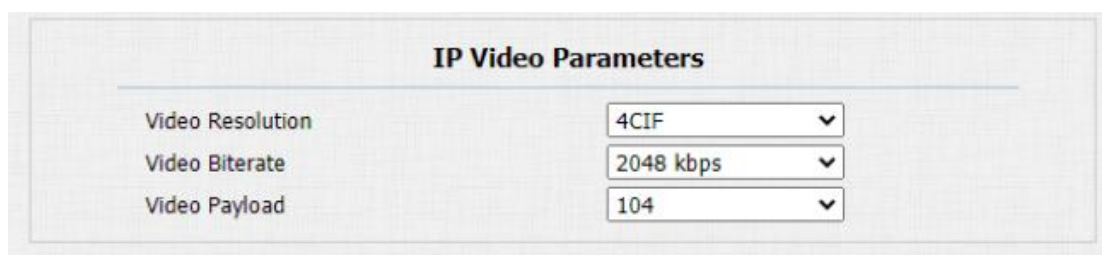
Parameter Set-up:

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

configure the 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 **Phone>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 the 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
DTMF Payload	101 (96~127)

Parameter Set-up:

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

12. Phone Book Configuration

Akuvox door phone supports storing up to 500 contacts that can give access permission to the indoor monitor or another device. Access White list includes group setting and contact setting and management. To set it up on web PhoneBook > Local Book interface.

12.1. Managing Contact Group

You can set up contact group first before you move the contacts into the group, to do so navigate to on web PhoneBook > Local Book >Group.

Group					
Index	Name	Firstly Called	Secondary Called	Lastly Called	<input type="checkbox"/>
1	akuvox	inn,Ann	Lin	Julia	<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>

Page: 1 ▾ Prev Next

Group Setting

Name

Parameter Set-up:

- **Name:** enter the group name.

12.2. Managing Contacts

You can search, create, display, edit and delete the contacts in your phone book. Path: PhoneBook > Local Book.

Local Book

Contact ▼

Contacts Sort By ▼

Show Cloud Contacts ▼

Caller Display ▼

Search

Dial ▼

Index	Name	Phone Number	Group	Account	Priority Of Call	Floor	<input type="checkbox"/>
1							<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>

Page: ▼

Contact Setting

Name

Group ▼

Priority Of Call ▼

Phone Number

Account ▼

Floor ▼

Parameters Set-up:

- **Contact:** you can choose to show all contacts information or one group's contact information.
- **Contacts short by:** there are three options ASCII Code, Room Number and Import. If ASCII Code is selected, sort in ascending ASCII order, for example: 0-9, a-z, numbers take precedence over letters. Not case

sensitive, but the same letter, lowercase is sorted before uppercase. If Room Number is selected, sort by room name. if there is no room name, the room number is taken as the room name by default. Room number is available after enabling Cloud contact. If Import is selected, sort by contacts in the imported file

- **Show Cloud Contacts:** enable it to show the contacts issued from Akuvox SmartPlus.
- **Caller display:** display the caller by name or group name.
- **Search:** enter the key number or key letter of the name to quickly search the contact.
- **Dial:** enter a phone number then click Dial to initiate the call from the web.
- **Name:** enter the contact name, which is required.
- **Phone:** enter the phone number of the contact, which is required.
- **Group:** click the green tab to select the group name you have created. You cannot select the group name if no group name has been created.
- **Account:** select which SIP account will be used to call out. If using IP direct call, it is not available.
- **Priority of Call:** up to 3 numbers in one group and set up the call sequence for these numbers.
- **Floor:** enter the floor number of the contact if needed.

12.3. Export/Import Contacts

When the contact becomes so many that you can not afford to manage each contact one by one manually, you can import and export the contacts in batch on the device web interface.

Import/Export

Contact No file chosen (.XML)

13. Relay Setting

13.1. Relay Switch Setting

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

The screenshot shows a web interface titled "Relay" with a sub-header "Relay". It contains a table of configuration options for three relays: RelayA, RelayB, and RelayC. The options include Relay ID, Relay Type, Relay Mode, Relay Delay (Sec), DTMF Option, DTMF, Multiple DTMF, Relay Status, Opendoor Outside Tone, and Opendoor Inside Tone. Each option is represented by a dropdown menu or a text input field.

Parameter	RelayA	RelayB	RelayC
Relay ID	RelayA	RelayB	RelayC
Relay Type	Default state	Default state	Default state
Relay Mode	Monostable	Monostable	Monostable
Relay Delay(Sec)	3	3	3
DTMF Option	1 Digit DTMF		
DTMF	0	0	0
Multiple DTMF			
Relay Status	RelayA: Low	RelayB: Low	RelayC: Low
Opendoor Outside Tone	Default	Default	Default
Opendoor Inside Tone	Default	Default	Default

Parameter Set-up:

- **Relay ID:** you are allowed to set up three relay switches in total for the door access control.
- **Relay Type:** if the Default state is selected, the Relay Status shows Low which means the door is closed, the Relay Status shows High which means the door is opened. If Invert State is selected, the Relay Status shows High which means the door is closed, and Low means the door is opened.
- **Relay Mode:** there are two modes Monostable and Bistable. If Monostable is selected, the relay status will be automatically reset within the relay delay time after the relay is triggered. If Bistable is selected, relay status will be reset after the relay is triggered again.

- **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 *,#).
- **Multiple DTMF:** set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digits DTMF code if DTMF Mode is set as 3-digits.
- **Relay Status:** relay status is low by default which means normally closed(NC) If the relay status is high, then it is in Normally Open status(NO).
- **Opendoor Outside/Inside Tone:** you can choose the customized open door tone. To configure the tone please refer to [chapter 8.1.3.2](#).

**Note:**


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

**Note:**

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

13.2. Select Speed Dial triggered Relay

This function is used to trigger a relay when you initiate the speed dial numbers. To do this configuration on the web Intercom > Basic>Trigger Relay Of Speed Dial interface.



Trigger Relay Of Speed Dial

RelayID RelayA RelayB RelayC

Parameters Set-up:

- **RelayID:** tick the checkbox of the relay. You can choose one or all relays.

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

Web Relay

Type	Disabled ▾
IP Address	<input type="text"/>
UserName	<input type="text"/>
Password	••••••

Web Relay Action Setting

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

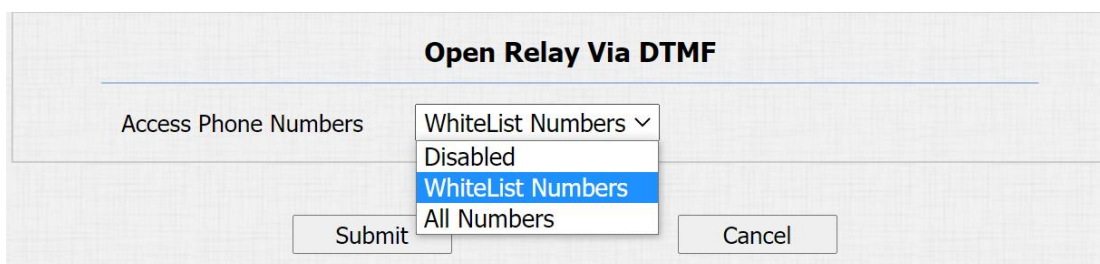
Parameter Set-up:

- **Type:** select among three options “Disabled” “WebRelay” and “Both”. Select “Webrelay” to enable the web relay. Select “Disable” to disable the web relay. Select “Both” to enable both local relay and web relay.
- **IP Address:** enter the 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 passwords are authenticated via HTTP and you can define the passwords using “http get” in Action.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding ip, username, pwd, you can fill in the HTTP command in the web relay action, so you can configure multiple webrelays.
- **Web Relay Key:** it can be null or enter the configured DTMF code, when the door is unlocked via DTMF code, the action command will be sent to the web relay automatically.

- **Web Relay Extension:** it can be null or enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional. And please refer to the example below:
<http://admin:admin@192.168.1.2/state.xml?relayState=2>.

13.4. Configure White List for Door Relay

For security, Akuvox door phone give permission for who can unlock the door by DTMF code. To do this configuration on the web Intercom > Relay > Open Relay Via DTMF interface.



The screenshot displays the 'Open Relay Via DTMF' configuration page. It features a form with a label 'Access Phone Numbers' and a dropdown menu for 'WhiteList Numbers'. The dropdown menu is open, showing three options: 'Disabled', 'WhiteList Numbers' (which is highlighted in blue), and 'All Numbers'. Below the form, there are two buttons: 'Submit' and 'Cancel'.

Parameter Set-up:

- **Access Phone Numbers:** there are three options - Disabled, WhiteList Number and All Number. If Disabled is selected, the DTMF code for unlock can not be available during the call. If WhiteList is selected, Akuvox door phone can only be unlocked by the contacts existing in the phone book. If All Number is selected, all callees can open the door phone during the call by using DTMF code.

14. Door Access Schedule Management

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

14.1. Configure Door Access Schedule

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

14.1.1. Manage 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 on the web Intercom > Relay > Relay Schedule interface.

Relay Schedule

Relay ID

Schedule Enable

All Schedules

Enable Schedules

>>

<<

Parameter Set-up:

- **Relay ID:** choose the relay you need to set up.
- **Schedule Enable:** it is disabled by default. Only choose to enable it, that

you can select the schedule. For creating the schedule please refer to [chapter 14.1.2.](#)

14.1.2. Create Door Access Schedule

You can create the door access schedule on a daily, weekly, and 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.

To create a daily schedule, you can do as follows:

Schedule Setting

Schedule Type:

Schedule Name:

Date Range: -

Day of Week: Mon Tue Wed Thur
 Fri Sat Sun Check All

Date Time: : - :

Schedules Management

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"/>

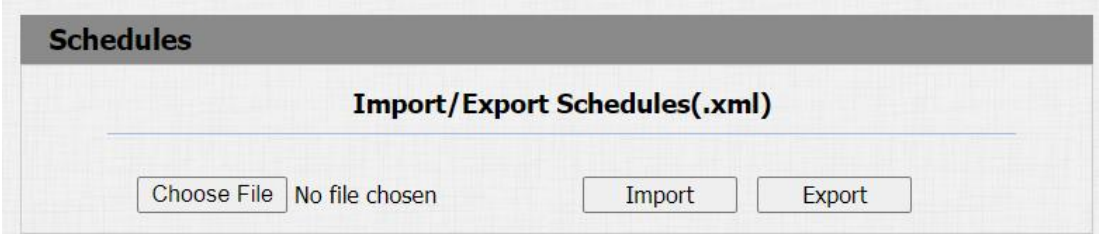
Page:

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 Range:** set the corresponding time period.
- **Day of Week:** select the corresponding day of the week. This field will only be displayed when the Week and Normal types are selected.
- **Date Range:** set the corresponding date. This field will only be displayed when the Normal type is selected.

14.1.3. Import and Export Door Access Schedule

In addition to creating a door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedule management efficiency. Path: Intercom > Schedule > Import/Export Schedule(.xml).



The screenshot shows a web interface titled "Schedules" with a sub-section "Import/Export Schedules(.xml)". Below the title is a file selection area with a "Choose File" button, the text "No file chosen", and two buttons labeled "Import" and "Export".

**Note:**

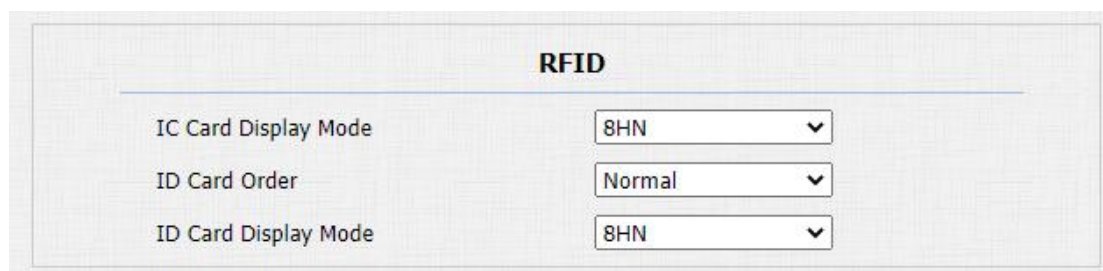
- It only supports .xml format file for importing and exporting the schedule.

14.2. Door Unlock Configuration

R28 door phone offers you two types of access methods: PIN code and RF card.

14.3. Configure Access Card Format

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



The screenshot shows a configuration window titled "RFID". It contains three rows of settings, each with a label and a dropdown menu:

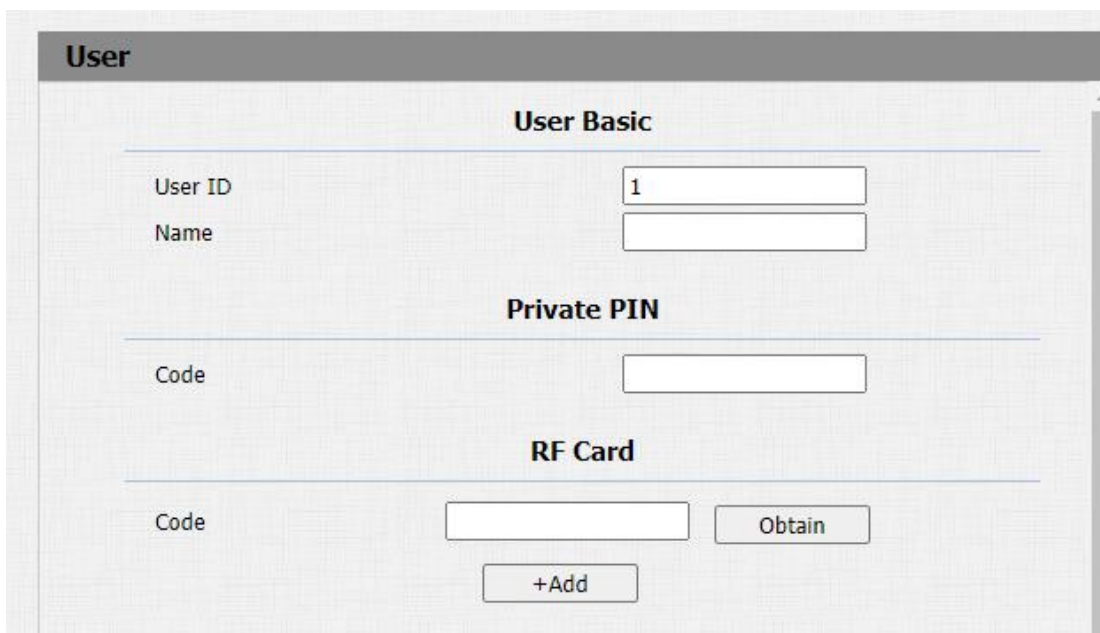
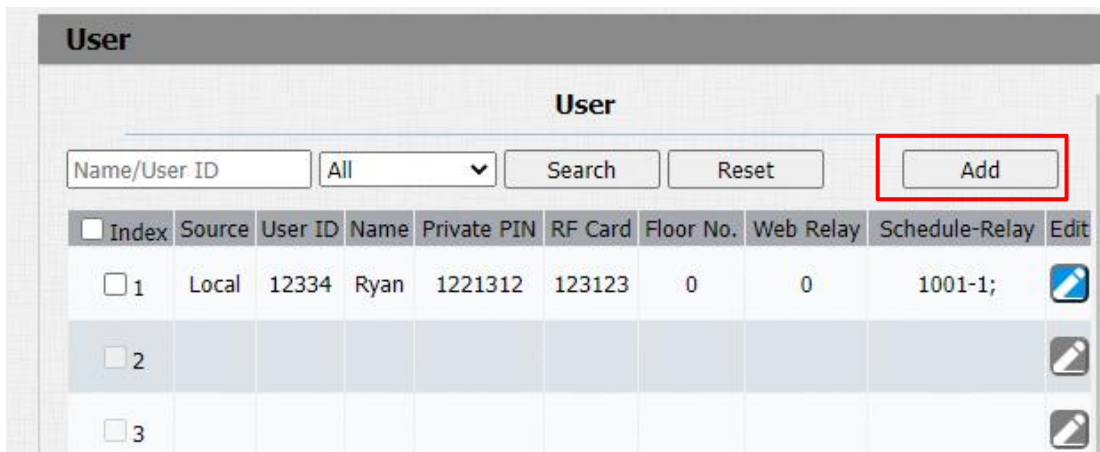
RFID	
IC Card Display Mode	8HN
ID Card Order	Normal
ID Card Display Mode	8HN

Parameters Set-up:

- **IC CARD Display Mode:** Select the card code format for the **IC card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR**. The card code format is 8HN by default in the door phone.
- **ID Card Order:** select normal or reversed display of ID card.
- **ID Card Display Mode:** Select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR**. The card code format is 8HN by default in the door phone.

14.4. Configure RF Card for Door Unlock

You can tap the RF card on the reader and click obtain to add RF card for the user. Path: Intercom > User.



Parameter Set-up:

- **User ID:** enter the user ID. The user ID is 11 digits maximum in length and can not be reused for other users. The User ID can be generated automatically or manually.
- **Name:** enter the user name.
- **Code:** place the card on the device card reader area and click obtain.

Note:

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

14.5. Edit the User-specific door access data

You can search user(s)-specific door access and edit the door access data on the web Intercom > User interface.

Index	Source	User ID	Name	Private PIN	RF Card	Floor No.	Web Relay	Schedule-Relay	Edit
<input checked="" type="checkbox"/> 1	Local	12334	Ryan	1221312	123123	0	0	1001-1;	
<input type="checkbox"/> 2									
<input type="checkbox"/> 3									

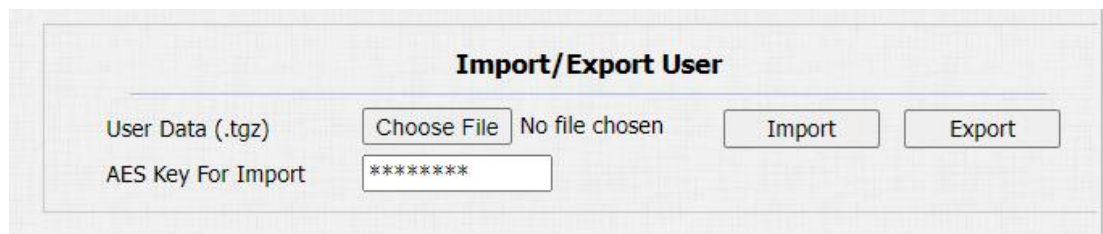
Note:

- Users synchronized from the SmartPlus can not be edited or deleted.

14.6. Import and Export User Data of Access Control

R28 series support User Data of access control to be shared among Akuvox

R28 series door phones through import and export while you can also export the facial data out of the door phone and then import it to a third-party device. To configure the configuration on the web Intercom > User > Import/Export User interface.



Parameter Set-up:

- **AES Key For Import:** enter the AES code before importing the AES-encrypted .tgz file to the door phone.

14.7. 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.



Parameter Set-up:

- **Switch:** enable the HTTP command to unlock the function by clicking on Enable field.

- **Session Check:** this feature is for some network security limitations, if you enable it, the door may not be unlocked in this way.
- **User Name:** enter the user name of the device web interface, for example, "Admin".
- **Password:** enter the password for the HTTP command. For example: "12345".

Please refer to the following example:

<http://192.168.35.127/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.

14.8. 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

Input A

Input Service	<input type="text" value="Disabled"/>
Trigger Option	<input type="text" value="Low"/>
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> Email <input type="checkbox"/> Sip Call <input type="checkbox"/> HTTP <input type="checkbox"/> Speed Dial
Http URL:	<input type="text"/>
Action Delay	<input type="text" value="0"/> (0~300Sec)
Open Relay	<input type="text" value="None"/>
Door Status	DoorA: High

Parameter Set-up:

- **Input service:** select "Enable " to be able to use the Input function.
- **Trigger Option:** select the trigger options according to the actual operation on the exit button.
- **Action To Execute:** select the method to carry out the action among six options: FTP, Email, HTTP, TFTP, Manager Dial and Speed Dial. Only R27X support Manager Dial and R28X supports Speed Dial.
- **Http URL:** enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds., then the corresponding actions will be carried out 5 seconds after your press the button.
- **Open Relay:** set up relays to be triggered by the input.
- **Door Status:** display the status of the input signal.

14.9. Configure PIN Code for Door Unlock

You can create and modify both public PIN code and private PIN code for the door access on R28 door phone.

14.10. Configure Public Code for Door Unlock

Public PIN code is configured and used by the property in the same building or in the same community. To do this configuration on the web Intercom > PIN Setting > Public PIN interface.



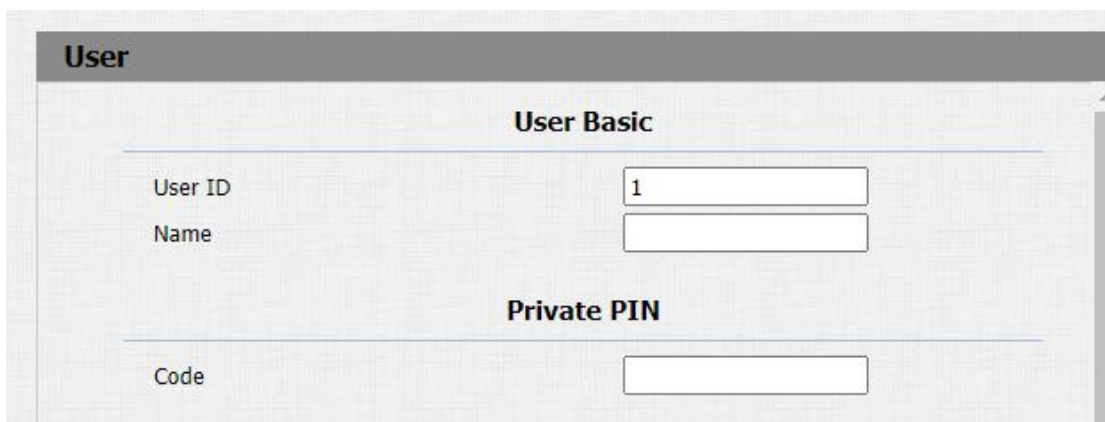
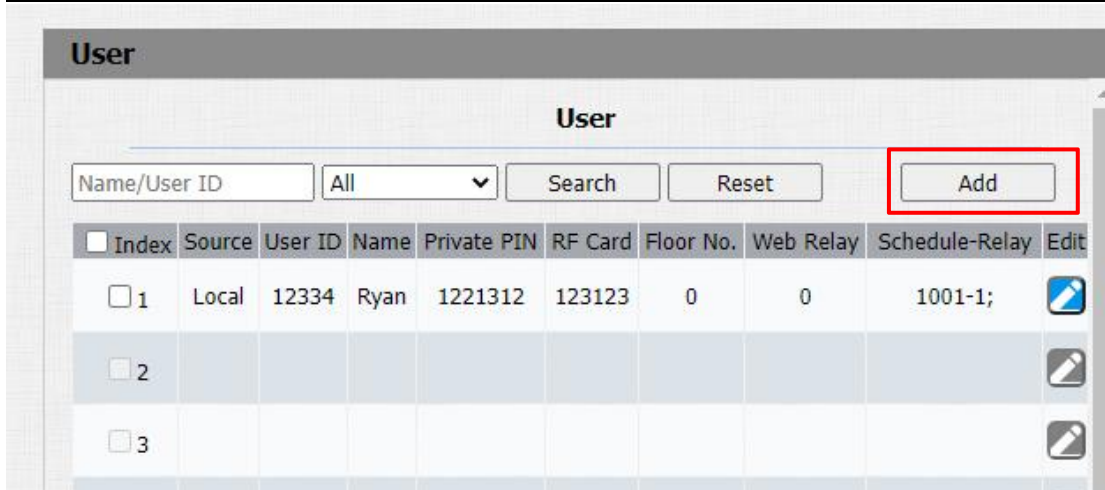
Public PIN	
Enabled	Disabled ▾
PIN Code	33333333 (3-8 digit number)

Parameter Set-up:

- **Enabled:** Disable public key feature, the door can not be opened by public key. Enable it, you can use public key to open the door.
- **PIN Code:** customize 3-8 digit numbers for public key value.

14.10.1. Configure Private PIN Code on the Web Interface

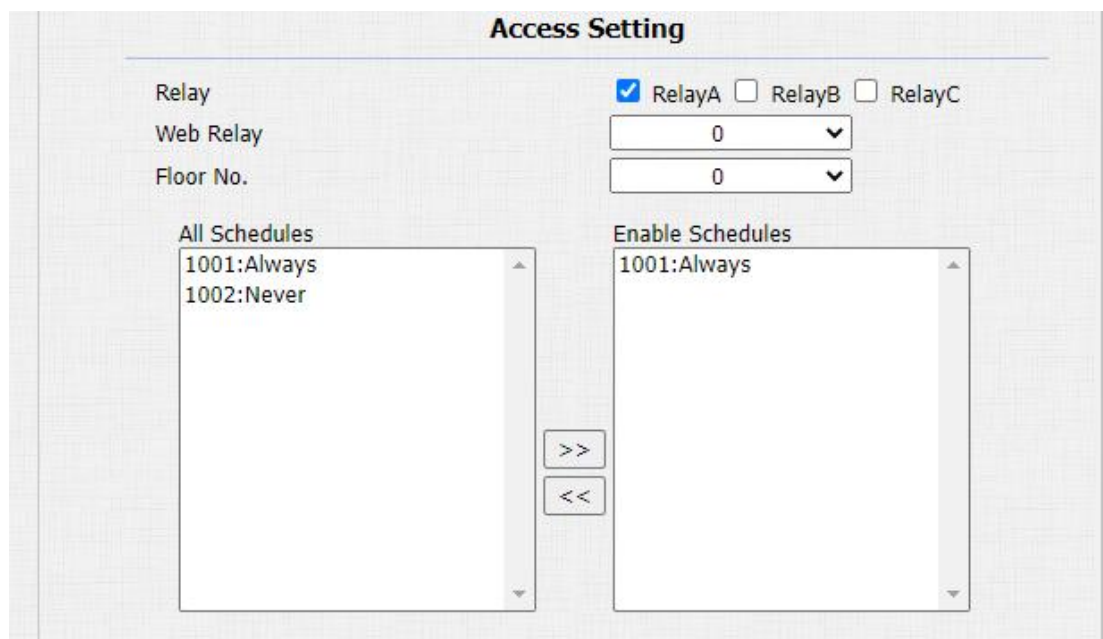
On the web interface, you can not only set up PIN code, but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. Path: Intercom > User.



Parameter Set-up:

- **User ID:** enter user's ID.
- **Name:** enter the user name (resident's name).
- **Code:** enter the user's private PIN.

After user information and PIN code are entered, you can scroll down to Access Setting and configure private PIN code access control.



Parameter Set-up:

- **Relay:** select the relay(s) that you want to apply the private PIN code for the door unlock.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Floor NO:** enter the resident's floor number.
- **Schedule:** select from the created door access schedule on the right box and move the one to be applied to the user(s)-specific PIN code door access to the box on the right side.

You are required to enable the PIN code before you can get door access via private PIN code, you can navigate to Intercom > PIN setting > Private PIN.



15. Security

15.1. Tamper Alarm Setting

Tamper alarm function serves as a protection against any unauthorized removal of the devices by triggering off the temper alarm while sending out calls to the designated location. Tamper alarm will be triggered off when the door phone changes its gravity value as opposed to its original gravity value set up when the device is installed. To do this configuration on the web Intercom > Advanced > Tamper Alarm interface.

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

Parameter Set-up:

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

15.2. Client Certificate Setting

Certificates can ensure communication integrity and privacy when deploying Akuvox door phone. So, when 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 client for authentication when client require an SSL connection with Akuvox door phone. Currently, the format of certificate can be accepted by Akuvox door phone is *.PEM file.

Client Certificate: When Akuvox door phone Phone required an SSL connection with server, 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.

15.2.1. Configure Action of Input

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

Action To Execute: FTP Email Sip Call HTTP Speed Dial

Http URL:

Parameter Set-up:

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

15.2.2. Web Server Certificate

To upload Web Server certificate on the device web interface Security > 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

15.2.3. Client Certificate

To upload and configure client certificate on the same page.

Client Certificate

Index	Issue To	Issuer	Expire Time	<input type="checkbox"/>
1				<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

Client Certificate Upload(.PEM/.DER/.CER/.CRT)

Index

 No file chosen

Auto ▾

Only Accept Trusted Certificates

Disabled ▾

Parameter Set-up:

- **Index:** select the desired value from drop-down list of Index. If you select Auto value, the uploaded certificate will be displayed by numeric order. If you select value from 1 to 10, the uploaded certificate will be displayed according to the value that the user selected.
- **Select File:** click Choose file browse local drive, and locate the desired certificate. (*.pem only)
- **Only Accept Trusted certificates:** if you select Enabled, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If you select Disabled, the phone will not verify the server certificate no matter whether the certificate is valid or not.

15.3. Motion Detection

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

15.3.1. Configure Motion Detection

You can turn on the motion detection and set up the motion detection interval on the web Intercom > Motion interface.

Motion Detection Options

Motion Detection Disabled ▾

Time 10 (0~120 Sec)

Motion Detect Time Setting

Mon Tue Wed Thur

Fri Sat Sun Check All

00 ▾ : 00 ▾ - 23 ▾ : 59 ▾

Parameter Set-up:

- **Motion Detection:** To enable or disable Motion Detection.
- **Time:** set the time interval for the motion detection. If you set the default time interval as "10" Sec, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as "10" then, and the first movement captured can be seen as the start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 seconds (the first

trigger point) and motion detection action can be triggered (sending out notification) any where between 7-10 seconds once the movement is detected. "10" Sec interval is a complete cycle of the motion detection before it starts another cycle of the same time interval. To be more specific, the first trigger point can be calculated as the "Time interval minus three".

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.

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

Parameter Set-up:

- **Sender's email address:** enter the sender's email address from which the email notification will be sent out.
- **Receiver's Email Address:** enter the receiver's email address.

- **SMTP Server Address:** enter the SMTP server address of the sender.
- **SMTP User Name:** enter the SMTP user name, which is usually the same with sender's email address.
- **SMTP Password:** configure the password of SMTP service, which is same with sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the contents of emails according to your need.

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

Parameter set-up:

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

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 the SIP call number.
- **SIP Call Name:** to configure the display name of door phone.

15.4.4. Call Event Notification

Enable this feature if you want to be notified when any outgoing calls from the door phone are not answered. The notification is made via FTP, Email, and HTTP. On the web, navigate to Intercom > Basic > Call Event.

Call Event	
No Answer Action	<input type="text" value="Disabled"/>
Action To Execute	FTP <input type="checkbox"/> Email <input type="checkbox"/> Http <input type="checkbox"/>
Http URL:	<input type="text"/>

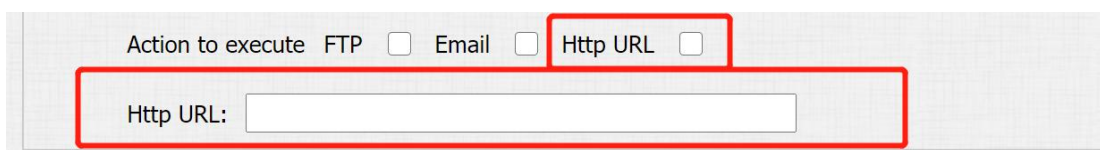
Parameter Set-up:

- **No Answer Action:** enable the feature if needed.
- **Action To Execute:** select FTP, Email or HTTP method for the notification. If FTP is selected, a screenshot of the caller will be sent via as notification. If Email is selected, the Emails containing a screenshot of the caller will be sent. If HTTP is selected, you can add the event message to the HTTP URL before sending.

- **Http URL:** enter the HTTP URL that will be sent to the Http server. For example:http//192.168.31.6/door phone#1.

15.4.5. HTTP URL Notification Configuration

Akuvox door phones 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 16.4](#). The URL format: http://http server IP address/any information.



Action to execute FTP Email Http URL

Http URL:

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. Action URL

R28 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 occurs any changes in the relay status, input status, PIN code, and RF card access for security purpose. Path: Phone > Actions URL.

Action URL	
	Action URL
Active	Disabled <input type="button" value="v"/>
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
RelayA Triggered	<input type="text"/>
RelayB Triggered	<input type="text"/>
RelayC Triggered	<input type="text"/>
RelayA Closed	<input type="text"/>
RelayB Closed	<input type="text"/>
RelayC Closed	<input type="text"/>
InputA Triggered	<input type="text"/>
InputB Triggered	<input type="text"/>
InputC Triggered	<input type="text"/>
InputA Closed	<input type="text"/>
InputB Closed	<input type="text"/>
InputC Closed	<input type="text"/>
Valid Code Entered	<input type="text"/>
Invalid Code Entered	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>

15.6. Security Action Configuration

15.6.1. Configure Action of Call

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

Call Event

No Answer Action Disabled ▾

Action To Execute FTP Email Http

Http URL:

Parameter Set-up:

- **No Answer Action:** if the call will not be answered, it still trigger the action event after enabling this feature.
- **Action to execute:** to choose which action to be executed after triggering.

15.6.2. Configure Action of Motion

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

Action to execute

Action to execute FTP Email Sip Call HTTP

Http URL:

Parameter Set-up:

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

15.6.3. Configure Action of Body Temperature

When the detected wrist temperature is higher than the normal body temperature, it will trigger the SIP/IP call if you tick the checkbox of Action To Execute. To do this configuration on the web Intercom > Body

Temperature interface.

Measuring Body Temperature

Mode Disabled ▾

Temperature Unit Fahrenheit ▾

Normal Body Temperature 99.14 (Below99.14°F)

(If the detected temperature is lower than 95.00°F , the device will prompt low temperature, please try again later)

Action To Execute SIP/IP Call

SIP/IP Call Number 111

Parameter Set-up:

- **Action to execute:** to choose which action to execute after triggering.
- **SIP/IP Number:** enter the SIP/IP Number you need. The SIP number here is different from the SIP number in Action interface. This SIP number is only available when body temperature is triggered.

15.7. 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

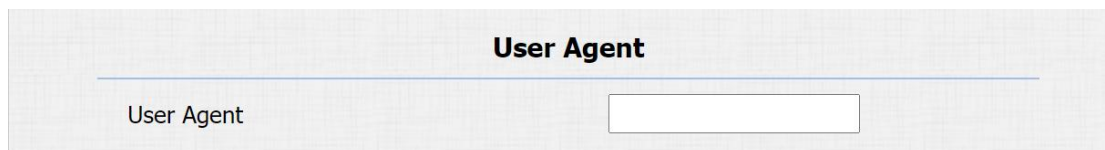
Voice Encryption(SRTP) Disabled ▾

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.

15.8. User Agent

You can customize user agent field in the SIP message. If user agent is set to specific value, users can see the information from PCAP. If user agent is blank, by default, users can see the company name "Akuvox", model number and firmware version from PCAP. To do this configuration on the web Account > Advanced > User Agent interface.



Parameter Set-up:

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

15.9. Body Temperature

R28A provides you with an optional wrist temperature measurement function designed to be applied in the situation where the measurement becomes necessary for the safety of the residents and visitors etc. Residents and visitors are required to go through temperature measurement before they are allowed the door access. Before entering the configuration, you need to correctly connect the MD01 external temperature measurement module to cooperate with the software's wrist temperature function. The MD01 module can be connected normally through the RS485A, RS485B, 12V Power Output, and GND interfaces of the docking device.

Note: This feature need to be worked with extra wrist temperature detection sensor Akuvox MD01, please consult Akuvox technical team for this model in detail.



Akuvox MD01

Measuring Body Temperature

Mode	<input type="text" value="Disabled"/>	▼
Temperature Unit	<input type="text" value="Fahrenheit"/>	▼
Normal Body Temperature	<input type="text" value="99.14"/>	(Below 99.14°F)

(If the detected temperature is lower than 95.00°F , the device will prompt low temperature, please try again later)

Parameter Set-up:

- **Mode:** there are two drop-down options, "Disabled" and "Wrist", select "Disabled", the device displays the home page normally (display call, contact, pin, security); select "Wrist", the device will open the wrist temperature test function.

- **Temperature Unit:** there are two drop-down options, "Fahrenheit" and "Centigrade". The value displayed by the device will change with the selection, and the value in the corresponding prompt will also change. The conversion formula between Fahrenheit and Celsius: $^{\circ}\text{C} = 5/9 \times (^{\circ}\text{F} - 32)$.

- **Normal Body Temperature:** the default setting is 99.14 degrees Fahrenheit (37.3 degrees Celsius). If the detected temperature is lower than 95.00 degrees Fahrenheit (35 degrees Celsius), the device will prompt low temperature, please try again later.

16. Monitor and Image

16.1. RTSP Stream Monitoring

Akuvox door phones support RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or 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

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

Parameter Set-up:

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

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

16.1.2. RTSP OSD Setting

This feature is used to add watermark to the RTSP video or picture. To protect the owner of the video or image. To do this configuration on the web Intercom > RTSP > RTSP OSD Setting interface.

RTSP OSD Setting	
RTSP OSD Color	White ▾
RTSP OSD Text	<input type="text"/>

Parameter Set-up:

- **RTSP OSD Color:** there are five color options - White, Black, Red, Green, Blue for RTSP watermark text.
- **RTSP OSD Text:** enter the customized text you want to show for the watermark.

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

Parameter Set-up:

- **RTSP Audio Enabled:** tick to enable RTSP audio which means, the door phone can also send audio information to the monitor by RTSP.
- **RTSP Video Enabled:** the door phone can send the video information to the monitor. After enabling RTSP feature, the video RTSP is enabled by default and can not be modified.
- **RTSP Video2 Enabled:** Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **RTSP Audio Codec:** choose a suitable audio codec for RTSP audio.
- **RTSP Video/Video2 Codec:** choose a suitable video codec for RTSP video.

H.264 And H.265 Video Parameters	
Video Resolution	720P ▾
Video Framerate	30 fps ▾
Video Bitrate	2048 kbps ▾
Video2 Resolution	VGA ▾
Video2 Framerate	30 fps ▾
Video2 Bitrate	512 kbps ▾

Parameter Set-up:

- **Video Resolution:** select video resolutions among seven options: "QCIF",

"QVGA", "CIF", "VGA", "4CIF", "720P". The default video resolution is "4CIF". and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than "4CIF".

- **Video Framerate:** "30fps" is the video frame rate by default.
- **Video Bitrate:** select video bit-rate among six options: "128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs" according to your network environment. The default video bit-rate is "2048 kpbs".
- **Video2 Resolution:** select video resolution for the second video stream channel. While the default video solution is "VGA".
- **Video2 Framerate:** select the video framerate for the second video stream channel. "25fps" is the video frame rate by default for the second video stream channel.
- **Video2 Bitrate:** select video bit-rate among the six options for the second video stream channel. While the second video stream channel is "512 kpbs" by default.

16.2. MJPEG Image Capturing

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

The screenshot shows the 'RTSP Basic' configuration page. It contains several settings:

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

The 'MJPEG Authorization' row is highlighted with a red rectangular border.

MJPEG Video Parameters	
Video Resolution	CIF
Video Framerate	25 fps
Video Quality	90

Parameter Set-up:

- **MJPEG Authorization:** tick it to access device video or real-time screenshots through a browser (http address such as: http://device IP:8080/video.cgi (dynamic video), http://device IP:8080/jpeg.cgi (static screenshot))
- **Video Resolution:** select video resolutions among seven options: "QCIF", "QVGA", "CIF", "VGA", "4CIF", "720P". The default video resolution is "4CIF". And the video from the door phone might not be able to be shown on 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.

16.2.1. NACK

NACK (Negative Acknowledgement) used to ensure the smooth and continued data transmission for the video call. To enable NACK, navigate to Phone > Call Feature > Others.

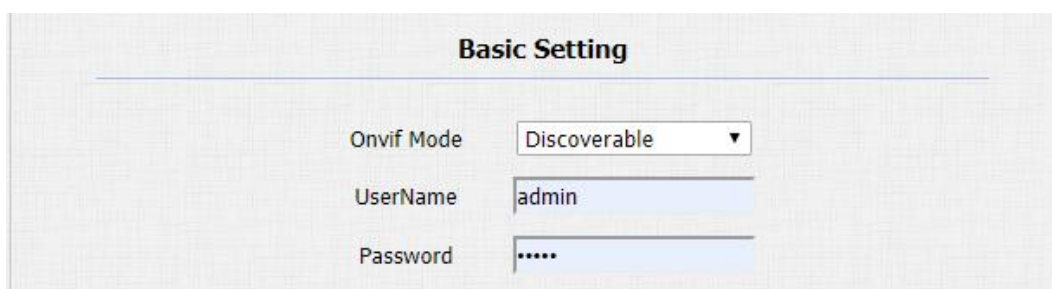
Others	
Return Code When Refuse	486(Busy Here)
Auto Answer Delay	0 (0~5Sec)
Auto Answer Mode	Video
Direct IP	Enabled
Direct IP AutoAnswer	Enabled
Direct IP Port	5060 (1~65535)
NACK	Disabled

Parameter Set-up:

- **NACK Enabled:** enable the NACK. It can be used to prevent losing data packet in the weak network environment when discontinued and mosaic video image occurred.

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.



Basic Setting	
Onvif Mode	Discoverable ▼
UserName	admin
Password

Parameter Set-up:

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

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

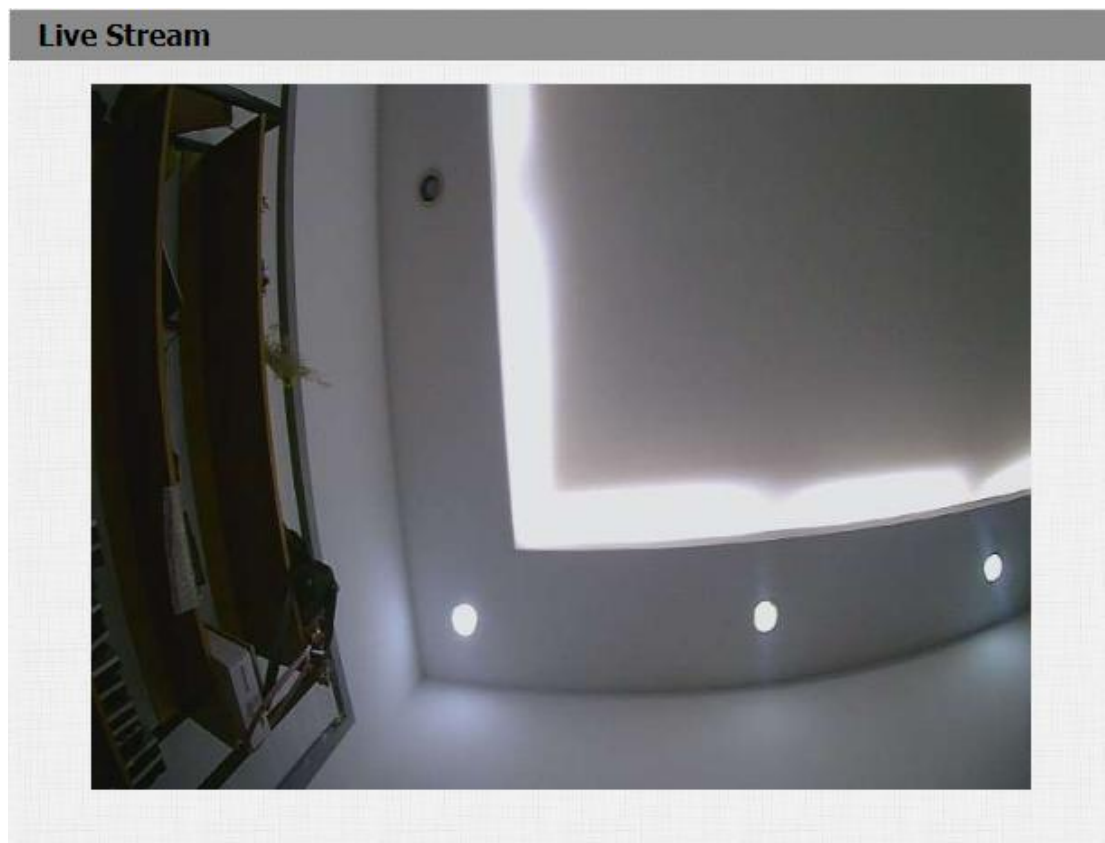
For example: http://IP address:80/onvif/device_service

**Note:**

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

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 Phone > Call Log interface.

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

Parameter Set-up:

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

17.2. Door Logs

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

Door Log

Index	Name	Code	Type	Date	Time	Status	
1	Unknown	01320C39	Card	2021-05-13	03:50:55	Failed	<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>
9							<input type="checkbox"/>
10							<input type="checkbox"/>
11							<input type="checkbox"/>
12							<input type="checkbox"/>
13							<input type="checkbox"/>
14							<input type="checkbox"/>
15							<input type="checkbox"/>

Page: 1

Import/Export Door Log(.xml)

No file chosen

Parameter Set-up:

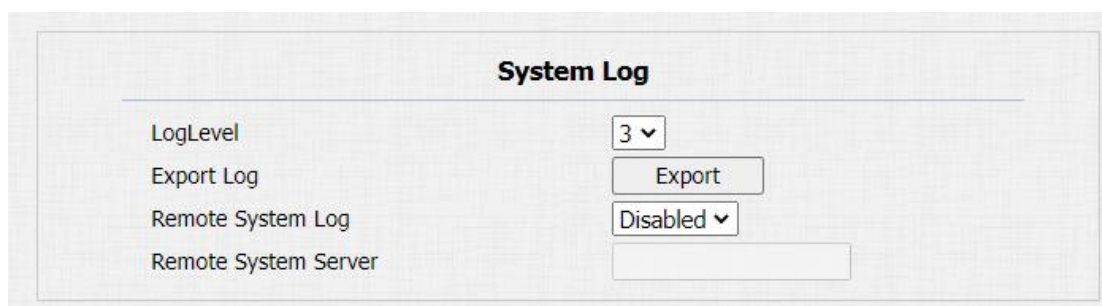
- **Index:** the order of the call logs.
- **Name:** if it is a locally added key or card, the corresponding added name will be displayed. If it is an unknown key or card, it will display Unknown.
- **Code:** if opening the door via PIN code, the corresponding PIN code will be displayed. If opening the door via RF cards, the corresponding card number will be displayed, and if the door is opened by HTTP command, it will be empty.

- **Type:** if opening the door via PIN code, Password will be displayed. If opening the door via RF cards, Card will be displayed, and if the door is opened by HTTP command, Http will be displayed.
- **Date:** the date for opening the door.
- **Time:** the time for opening the door.
- **Status:** the door opening result Success or Failed.

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.



System Log	
LogLevel	3 ▾
Export Log	Export
Remote System Log	Disabled ▾
Remote System Server	

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. Remote Debug Server

Remote debug server is used to access the log remotely for debugging purpose. On the web,\. Navigate to Intercom > Advanced > Remote Debug Server.

Parameter Set-up:

- **Service:** disable or enable the remote debug server.
- **Connect Status:** displays the remote debug server connection status.
- **IP:** enter the remote debug server IP address.
- **Port:** enter the remote debug server port.

18.3. PCAP

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

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 packet 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.

19. Firmware Upgrade

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

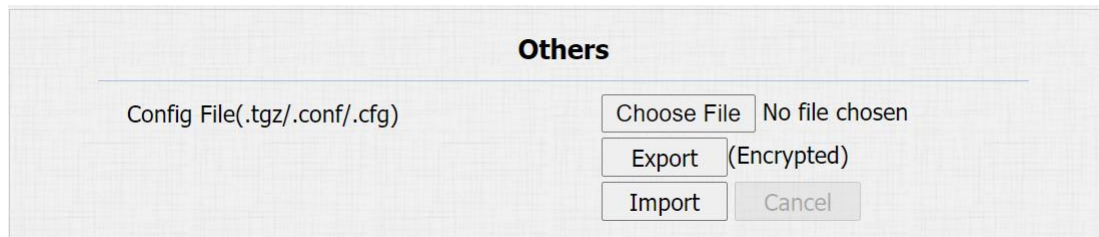
Firmware Version	28.30.2.215
Hardware Version	28.0
Upgrade	<input type="button" value="Choose File"/> No file chosen
	Reset: <input type="checkbox"/>
	<input type="button" value="Submit"/> <input type="button" value="Cancel"/>

Parameter Set-up:

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

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.



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

Parameter Set-up:

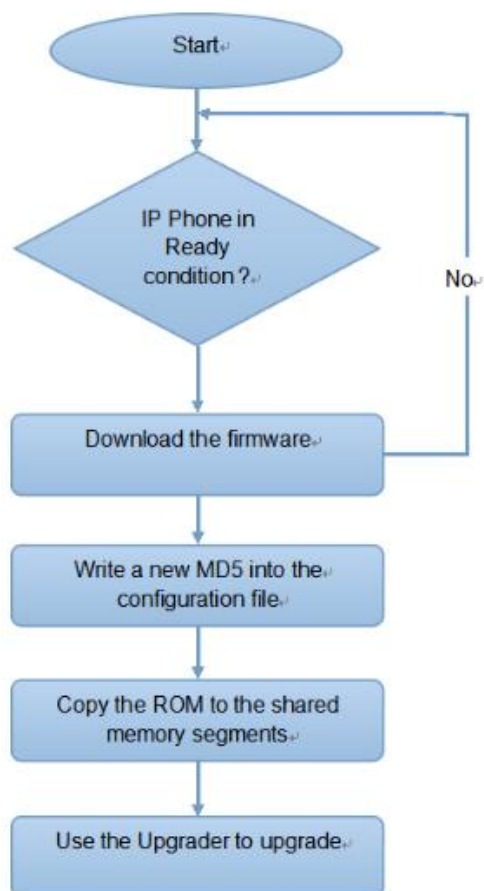
- **Export Config File:** to export the **current config file**.
- **Export/Import:** to export the **current config file (Encrypted)** or import new config file.

21. Auto-provisioning

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 configurations 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 firmware, 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 auto-provisioning. One is general configuration files used for the general provisioning and another one is the MAC-based configuration provisioning.

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

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

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

Automatic Autop

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



Note:

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

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.

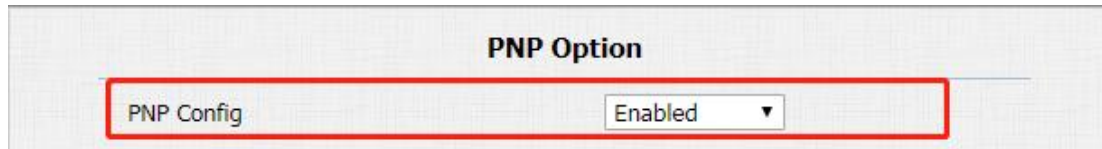
Automatic Autop	
Mode	Power On <input type="button" value="v"/>
Schedule	Sunday <input type="button" value="v"/>
	22 <input type="button" value="v"/> Hour(0~23)
	0 <input type="button" value="v"/> Min(0~59)

Parameter Set-up:

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

21.4. PNP Configuration

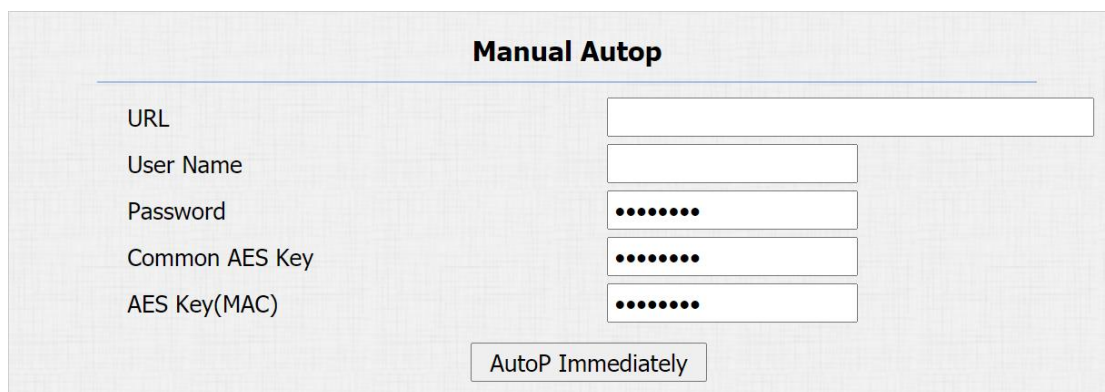
Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user. To do this configuration on web Upgrade > Advanced > PNP Option interface.



The screenshot shows a web interface titled "PNP Option". Below the title, there is a dropdown menu labeled "PNP Config" which is currently set to "Enabled". The dropdown menu is highlighted with a red rectangular border.

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 on a specific timing according to Autop schedule you set up. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.



The screenshot shows a web interface titled "Manual Autop". It contains five input fields for configuration: "URL", "User Name", "Password", "Common AES Key", and "AES Key(MAC)". Each field is followed by a text input box. The "Password", "Common AES Key", and "AES Key(MAC)" fields are masked with dots. Below the input fields, there 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 be accessed to otherwise leave it blank.
- **Password:** set up a password if the server needs a password be accessed to otherwise leave it blank.
- **Common AES Key:** set up AES code for the intercom to decipher the

general Auto Provisioning configuration files.

- **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)

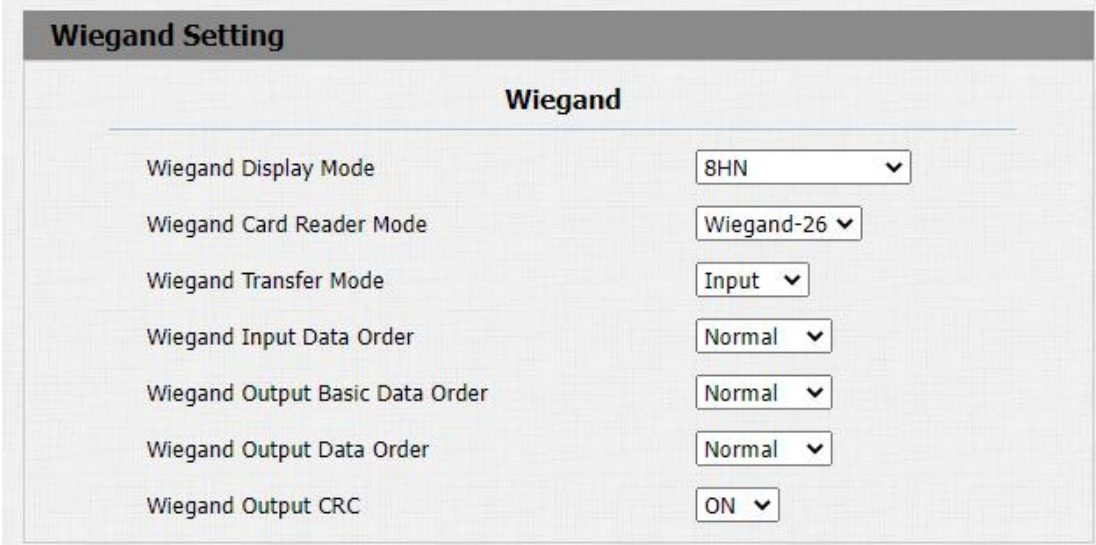
 **Note:**

- **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 Wiegand

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



Wiegand	
Wiegand Display Mode	8HN
Wiegand Card Reader Mode	Wiegand-26
Wiegand Transfer Mode	Input
Wiegand Input Data Order	Normal
Wiegand Output Basic Data Order	Normal
Wiegand Output Data Order	Normal
Wiegand Output CRC	ON

Parameter Set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among 8H10D; 6H3D5D; 6H8D; 8HN; 8HR; RAW.
- **Wiegand Card Reader Mode:** set the wiegand data transmission format among three options: "Wiegand 26", "Wiegand 34", "Wiegand 58". The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode:** select Input, Output, Convert to Card No.OutputWiegand. if the door phone is used as a receiver, then set it as "Input" for the door phone. Select "Output" If you want wiegand output to be converted to card number before sending it from the door phone to a receiver. For facial recognition access, the user card number corresponding to the facial recognition access will be sent out in a binary system.

- **Wiegand Input Data Order:** set the Wiegand input data sequence between "Normal" and "Reversed" if you select "Reversed" then the input card number will be reversed and vice versa.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between "Normal" and "Reversed" if you select "Reversed" then the input card number will be reversed and vice versa.
- **Wiegand Output CRC:** tick to enable the parity check function to ensure that signal-based data can be transmitted correctly according to the established data transmission format.
- **RF Card Verification:** enable the RF card verification if needed.

You can configure the wiegand output mode if needed. The output occurs when you press the PIN code on the device.

The screenshot shows a web interface titled "Forward To Wiegand Output". Below the title is a horizontal line. Underneath the line, there is a text input field labeled "PIN" and a dropdown menu currently showing "Disabled". At the bottom of the interface, there are two buttons: "Submit" and "Cancel".

22.2. Integration via HTTP API

HTTP API is designed to achieve a 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

HTTP API	<input type="text" value="Enabled"/>
Auth Mode	<input type="text" value="Digest"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>
IP01	<input type="text"/>
IP02	<input type="text"/>
IP03	<input type="text"/>
IP04	<input type="text"/>
IP05	<input type="text"/>

Parameter Set-up:

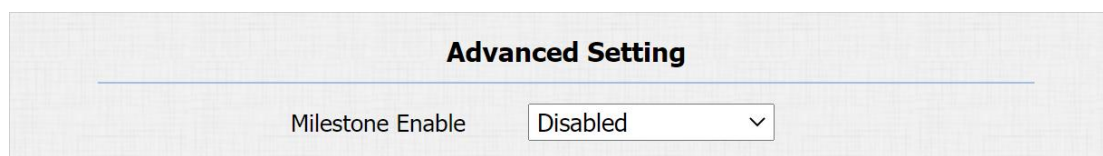
- **HTTP API:** select “Enable” or “Disable ” to enable or disable the HTTP API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** select among four options: “None” “WhiteList” “Basic”, “Digest” for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when “Basic” and “Digest” authorization mode is selected. The default user name is “Admin”.
- **Password:** enter the password when “Basic” and “Digest” authorization mode is selected. The default user name is “Admin”.
- **IP01-IP05:** enter the IP address of the third party devices when the “WhiteList” authorization is 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 developer only.
3	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication. In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method, only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of Http request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developer only.

22.3. Integration with Milestone

Akuvox multi-tenant door phone integrate with Milestone surveillance system, to do this configuration on the web Intercom > Onvif interface.



Advanced Setting

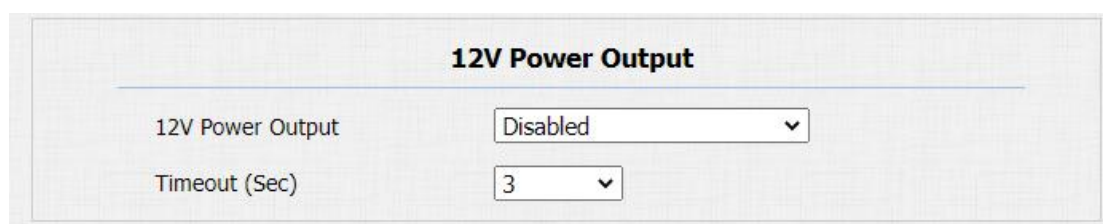
Milestone Enable

Parameter Set-up:

- **Milestone Enable:** enable to integrate with Milestone system. It is disabled by default.

22.4. Power Output Control

R28 can serve as a power supply for the external relays. Path: Intercom > Advanced > 12V Power Output.



12V Power Output

12V Power Output

Timeout (Sec)

Parameter Set-up:

- **12V Power Output:** select Disabled to disable the power output function; select Always to enable the access controller to provide continuous power to the third party device. Select Triggered By Open Relay if you want the E18 to provide power to the third party device via 12 output and GND interface during the timeout when the status of relays is shifted from low to high.

- **Time Out (Sec):** select the power supply time duration after the relay is triggered. Three options: 3, 5, 10. It is 3 seconds by default. The power output is 12V , and the maximum output amperage is 0.8A.

22.5. Integration with Lift Control

Akuvox multi-tenant door phone integrated with ZKTECO lift control. The local contact, card, and privatekey of the device can be edited by editing the corresponding floor field to recruit elevators at the same time as the door is opened. If the device connects Akuvox SmartPlus, and the cloud sends the corresponding floor information to open the door. Bluetooth, PIN code, App both can open the door at the same time. The device connects to the cloud mode and can only be placed in the public equipment under the building. At this time, Unit-APT can be used to match the corresponding floor. For example: 2-803, where 803 is the room number, the last two 03 represents the room number, and 8 represents the floor number. To do this configuration on the web Intercom > Lift Control interface.

Lift Control	
Lift Control	Disabled ▾
Server IP	<input type="text"/>
Server Port	<input type="text"/>
Timeout	60 (1~60s)

Parameter Set-up:

- **Lift Control:** enable to use lift control feature.
- **Server IP:** enter the ZKT lift control panel IP address.
- **Server Port:** enter the lift control port of the IP address.
- **Timeout:** The default value is 60, the value range is 1~60s, which means that within the Timeout value after the door is opened successfully, the corresponding floor button can be pressed. After timeout, it will not take effect.

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. You can also disable User account permission to login in the web.

Web Password Modify

User Name admin ▾ Change Password

Account Status

Admin	Enabled ▾
User	Disabled ▾

23.2. Modifying Device System Password

You can modify both device system password and service (setting) password on the web or on the device. On the web, navigate to Security > Basic > LCD Password Modify, and change the passwords if needed. The default system password is *2396#, the default service (setting) password is 3888.

LCD Password Modify

System Password	<input type="text" value="****"/>	(4 Digits)	Apply
Service Password	<input type="text" value="****"/>	(4 Digits)	Apply

To set or modify the system and service passwords on the device, press the system password (which is *2396# by default), select "Admin Access", and select "Set Admin Password", then set the system password. Select "Set Service Password", then set the service password. You can delete the passwords if needed.

23.3. Configure Web Interface Automatic Logout

It is a protection design. When there is no operation on the website and when the Session Time Out Value time is reached, the website will automatically log out. To do the configuration on the web Security > Basic > Session Time Out interface.

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

Parameters Set-up:

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

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.

24.2. Reset

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

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 the 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 the 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 does R20 and X915 support?

A6: Onvif 18.04 profiles

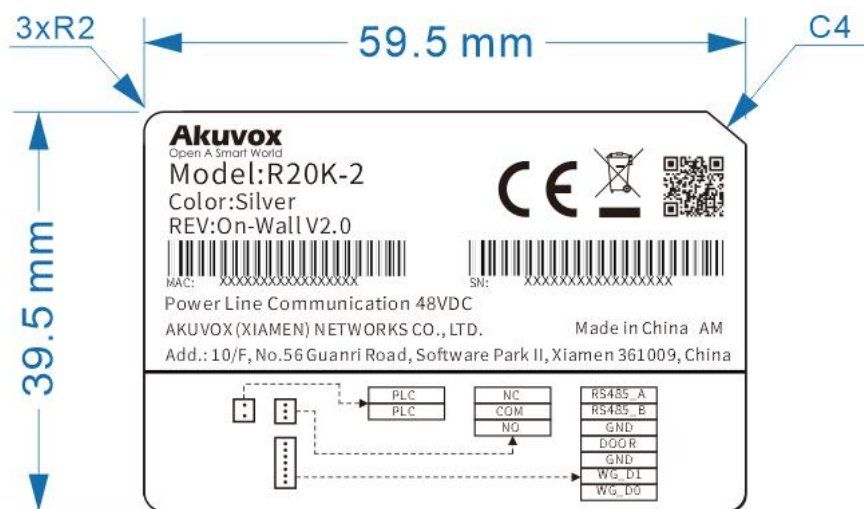
Q7: Do door phones support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS

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

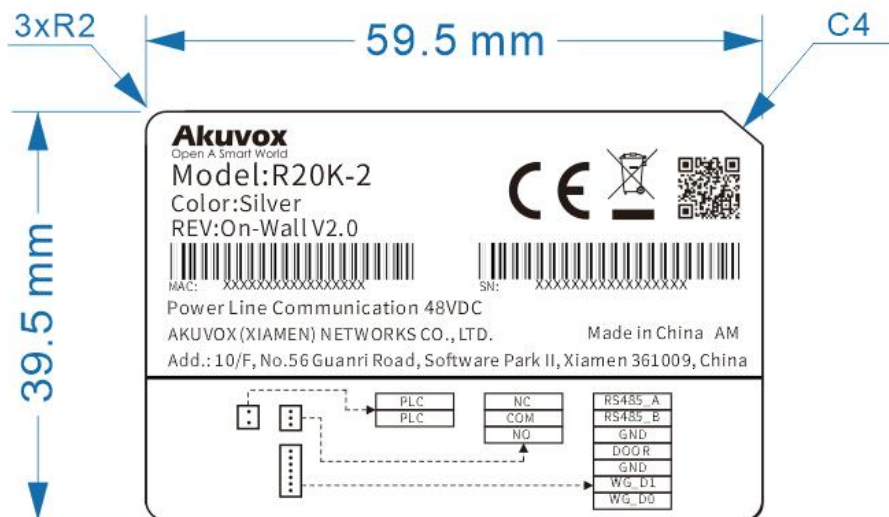
Q8: How to confirm whether my device is hardware version 1 or hardware version 2?

A8: 1.Label

- **Hardware version 1**



- **Hardware version 2**

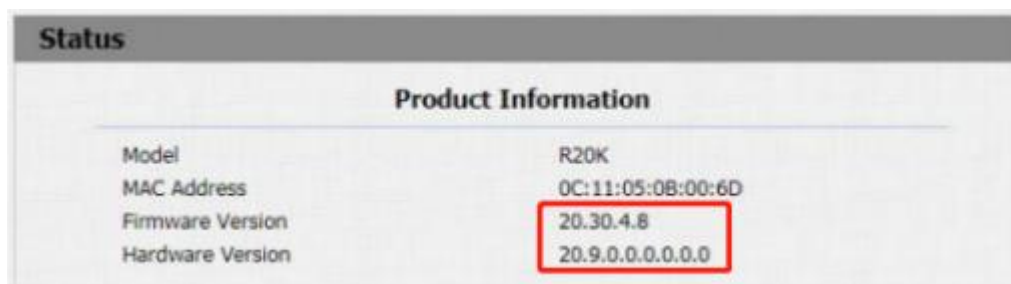


● **Firmware Version**

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.



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.



**FCC Caution:**

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

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

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

FCC Radiation Exposure Statement:

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

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

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