About This Manual

Thank you for choosing Akuvox R20A V5.0 door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to320.30.3.18 and it provides all the configurations for the functions and features of Akuvox door phone. Please visit Akuvox forum or consult technical support for any new information or latest firmware.

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

FCC Caution:

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

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

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

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

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

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

Table of Contents

1. Product Overview 1

2. Change Log 2

3. Model Specification 3

4. Introduction to Configuration Menu 4

5. Access the Device 8

5.1. Obtain Device IP Address 8

5.2. Access the Device Setting on the Web Interface 9

6. Language and Time Setting 10

6.1. Language Setting 10

6.2. Time Setting 11

7. LED Setting 13

7.1. Infrared LED Setting 13

7.2. LED Display Status 14

7.3. Setup LED Display from HTTP URL 16

7.4. LED Setting on Card Reader Area 17

8. Volume and Tone Configuration 19

8.1. Volume Configuration 19

8.2. IP Announcement 21

8.3. Open Door Tone Configuration 21

8.4. Upload Tone Files 23
8.4.1. Upload Ringback Tone 23
8.4.2. Upload Open Door Tone 23
9. Network Setting 26
9.1. Network Status 26
9.2. Device Network Configuration 26
9.3. Device Deployment in Network 28
9.4. Device Local RTP configuration 30
9.5. NAT Setting 31
9.6. SNMP Setting 33
9.7. VLAN Setting 34
9.8. TR069 Setting 35
9.9. Device Web HTTPSetting 37
10. Intercom Call Configuration 39
10.1. IP call & IP Call Configuration 39
10.2. SIP Call &SIP Call Configuration 40
10.3. SIP Account Registration 40
10.4. SIP Server Configuration 42
10.5. Configure Outbound Proxy Server 43
10.6. Configure Data Transmission Type 45
10.7. Configure Calling Feature 46

10.7.1. DND 46
10.7.2. Manager Dial Call 47
10.7.3. Call Hang-up 49
10.7.4. Web Call 49
10.7.5. Auto Answer 50
10.7.6. Multicast 51
10.7.7. Configure Maximum Call Duration 53
10.7.8. Maximum Dial Duration 54
10.7.9. Hang Up After Open Door 56
11. Audio& Video Codec Configuration for SIP Calls 57
11.1. Audio Codec Configuration 57
11.2. Video Codec Configuration 58
11.3. Video Codec Configuration for IP Direct Calls 59
11.4. Configure DTMF Data Transmission 61
12. Access White List Configuration 63
12.1. Managing Contacts 63
13. Relay Setting 65
13.1. Relay Switch Setting 65
13.2. Web Relay Setting 68
14. Door Access Schedule Management 72
14.1. Relay schedule 72

14.2. Configure Door Access Schedule 73
14.2.1. Create Door Access Schedule 73
14.2.2. Import and Export Door Access Schedule 75
14.2.3. Import and Export User 76
15. Door Unlock Configuration 77
15.1. IC/ID Card Control 77
15.2. Configure Access Card Format 78
15.3. Configuring RF Card for Door Unlock 79
15.3.1. Configure RF Card on the Web Interface 79
15.4. Import and Export Card Data of Access Control 81
15.5. Mifare/Defire CarD Encryption 82
15.5.1. NFC Card Setting 83
15.6. Configure Open Relay via HTTP for Door Unlock 84
15.7. Configure Exit Button for Door Unlock 85
16. Security 88
16.1. Tamper Alarm Setting 88
16.2. Client Certificate Setting 89
16.2.1. Web Server Certificate 89
16.2.2. Client Certificate 90
16.3. Motion Detection 91
16.3.1. Configure Motion Detection 92

16.4. Security Notification Setting 94
16.4.1. Email Notification Setting 94
16.4.2. FTP Notification Setting 96
16.4.3. SIP Call Notification Setting 97
16.4.4. HTTP URL Notification Configuration 97
16.5. Security Action Configuration 98
16.5.1. Configure Push Button Action 98
16.5.2. Configure Motion Action 99
16.5.3. Configure Input Action 99
16.5.4. Call Event Notification 100
16.6. Voice Encryption 101
16.7. User Agent 102
17. Monitor and Image 103
17.1. RTSP Stream Monitoring 103
17.1.1. RTSP Basic Setting 103
17.1.2. RTSP Stream Setting 104
17.1.3. NACK 107
17.2. MJPEG Image Capturing 108
17.3. ONVIF 110
17.4. Live Stream 111
18. Logs 113

18.1. Call Logs 113
18.2. Door Logs 114
19. Debug 117
19.1. System Log 117
19.2. PCAP 118
20. Firmware Upgrade 120
21. Backup 121
22. Auto-provisioning via Configuration File 122
22.1. Provisioning Principle 122
22.2. Configuration Files for Auto-provisioning 123
22.3. AutoP Schedule 125
22.4. PNP Configuration 126
22.5. Static Provisioning Configuration 127
23. Integration with Third Party Device 130
23.1. Integration via Wiegand 130
23.2. Integration via HTTP API 132
23.3. Lift Control Configuration 135
23.4. KeyKing Setting 137
23.5. Akuvox EC32 Lift Controller 138
23.6. ZKTLift Controller 140
23.7. Chiyu Lift Controller 141

24. Password Modification 142

24.1. Modifying Device Web Interface Password..... 142

24.2. Configure Web Interface Automatic Logout 143

25. System Reboot&Reset 144

25.1. Reboot 144

25.2. Reset 144

26. Abbreviations 145

27. FAQ 147

28. Contact us 151

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 isimmeasurable. Akuvox R20A V5.0are SIP-compliantdoor phones. They can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. The door phone enables you to easily monitor an entrance door or gate and gives you the peace of mind knowing that your facility is more secure.

Tx/Rx:NFC:13.56MHz;125kHz

H-Field: NFC:13.56MHz:2.22dBμA/m@3m

125kHz:18.66dBμA/m@3m

2. Change Log

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

3. Model Specification

Model & Feature	R20A
Button	1 Physical button
Housing Material	Aluminum
Camera	2 Mega pixels, automatic lighting
Relay In	2
Relay Out	2
RS485	√
PoE	√
WiFi	X
RAM	64MB
ROM	128MB
Card Reader	√
IP Rating	IP65
IK Rating	X
Wall Mounting	√
Flush Mounting	√

4. Introduction to Configuration Menu

- **Status:** this section gives you basic information such as product information, Network Information, and account information, etc.

- **Account**:this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.

- **Network**: this section mainly deals with DHCP&Static IP setting, RTP port setting, and device deployment, etc.

- **Intercom**:this section covers Intercom settings, Call Log,etc.

- **Surveillance**: this section covers Motion Detection, RTSP, MJPEG, ONVIF,Live stream.

- **Access Control**: this section covers Input control, Relay, Card settings, Face Recognition setting, Private PIN Code, Wiegand connection,etc.

- **Tenants**:this section involves Tenants management and Dial Plan.

- **Device**: this section includes Light settings, tab&button display, LCD settings and Voice settings.

- **Settings**: this section includes Time&language, Action settings, Door settings, Schedule for access control.

- **Upgrade**:this section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault Diagnosis.

- **Security**: this section is for Password modification.

- Mode selection :

1. **Discovery mode**: it is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to network. It is a super time-saving mode and it will greatly bring users convenience by reducing manual operations. This mode requires no prior configurations previously by the administrator.

2. **Cloud mode:** Akuvox Cloud is an all-in-one management system. Akuvox

Cloud is a mobile service that allows audio, video, remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from the cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using them.

3. **SDMC mode**: SDMC (**SIP Device Management Controller**) is a simple and comprehensive software for building management. It provides a topography for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm, etc. It is a convenient tool for property managers to manage, operate and maintain the community.

Tool selection

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

1. **SDMC**: SDMC is suitable for the management of Akuvox devices in large communities, including access control, resident information, remote device control, etc.

2. **Akuvox Upgrade tool**: upgrade Akuvox devices in batch on a LAN(**Local Area Network**)

3. **Akuvox PC Manager**: distribute all configuration items in batch on a LAN.

4. **IP scanner**: it is used to search Akuvox device IP addresses on a LAN.

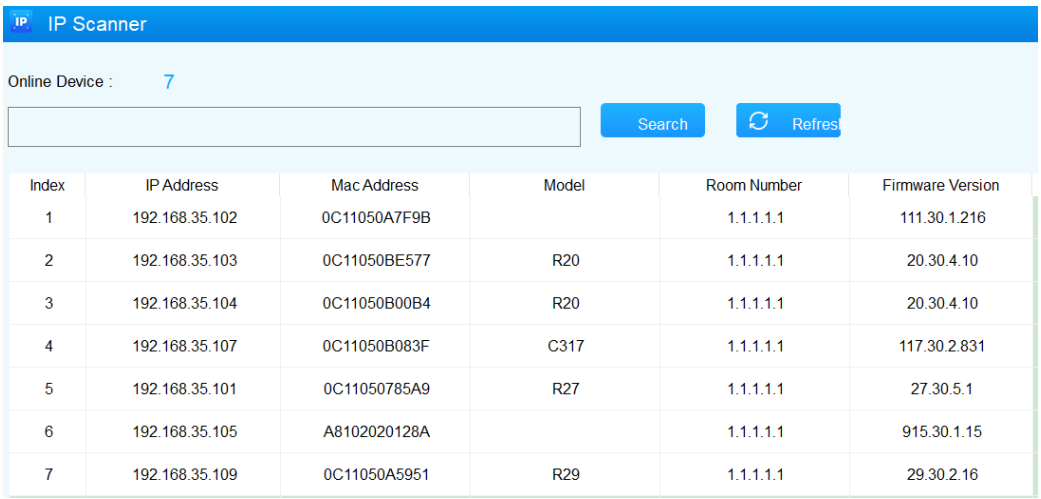
5. **FacePro**: manage face data in batch for the door phone on a LAN.

5. Access the Device

R20Aseriessystem setting can be accessed on the device web interface.

5.1. Obtain Device IP Address

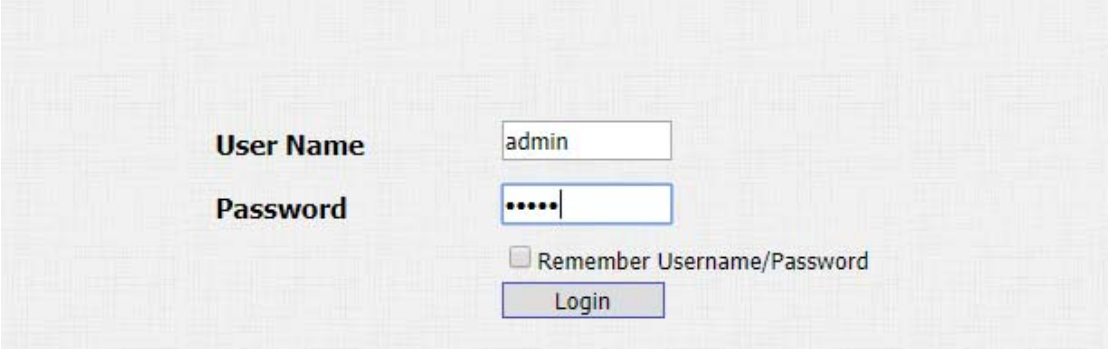
Check the Device IP address by holding the push button for 5s. Or searching the device IP by the IP scanner in the same LAN network. Just click **Scan** tab in the IP scanner to check the device IP.



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

5.2. Access the Device Setting on the Web Interface

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



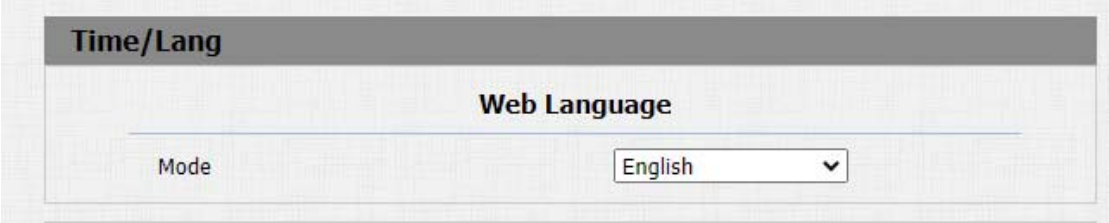
Note:

- You can also obtain the device IP address using the Akuvox IP scanner to log into the device web interface. Please refer to the URL below for the IP scanner application: https://knowledge.akuvox.com/docs/how-to-obtain-ip-address-via-ip-scanner-1?highlight=IP%20SCANNER
- Google Chrome browser is strongly recommended.

6. Language and Time Setting

6.1. Language Setting

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

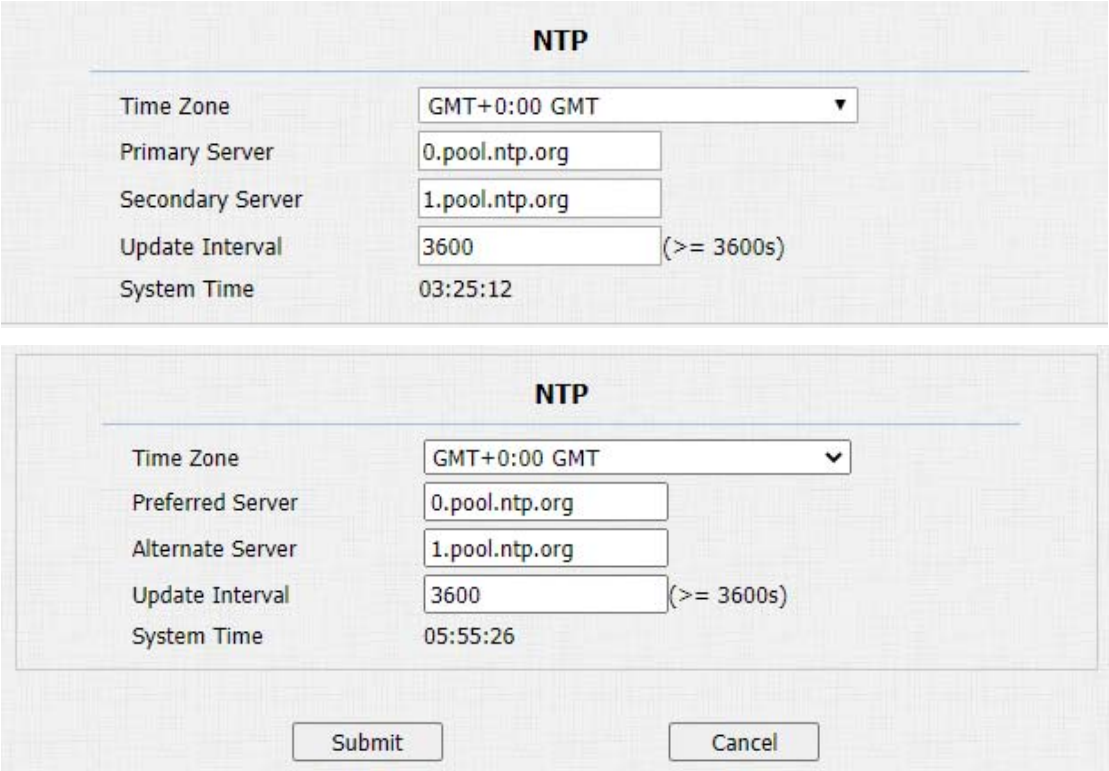


Parameter Set-up:

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

6.2. Time Setting

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



Parameter Set-up:

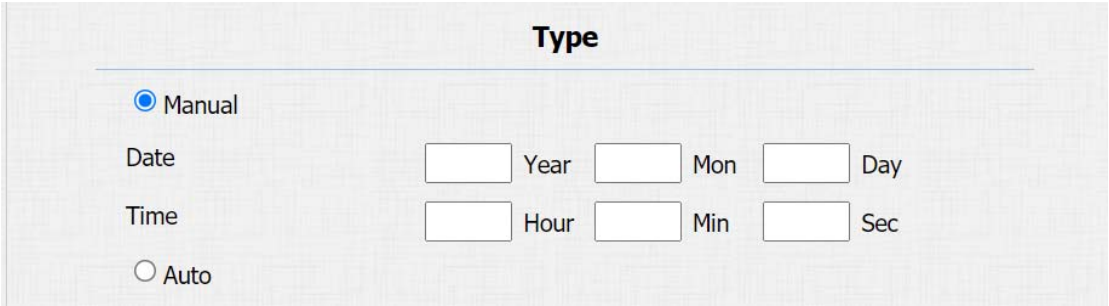
- **Time Zone**: select the specific time zone depending on where the device is used and then press **Confirm**tab for the confirmation. The default time zone is **GMT GMT+0.00**.

- **Preferred/Alternate Server:**enter the NTP server address. The alternate server will take effect when the primary server is invalid.

- **Update Interval:** to configure the interval between two consecutive NTP requests.

- **System Time**: indicate the current device time.

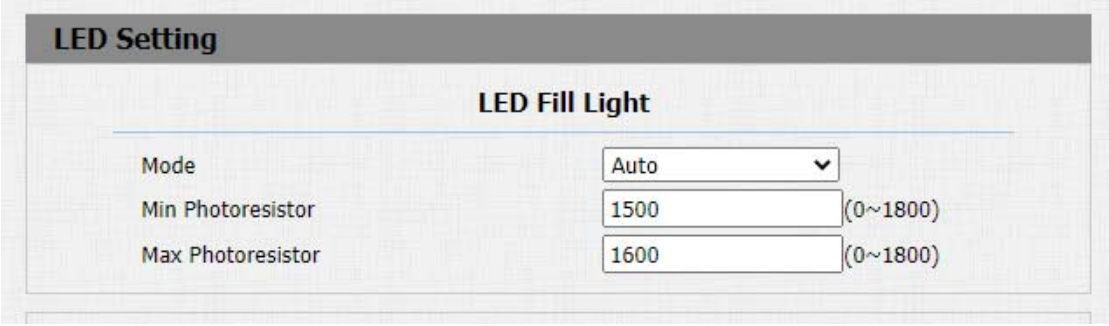
You can also set up time manually, select the **Manual** checkbox, and input time data.



7. LED Setting

7.1. Infrared LED Setting

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



Parameter Set-up:

- **Mode:** select"**Auto**" if you want the Infrared LED light to be turned on automatically according to the setting. select "**Aways ON**" to enable the Infrared LED light to stay on permanently. select "**Aways OFF**" to turn off the Infrared LED light. LED mode is set "**Always OFF**" by default. select "**Schedule**" to turn on the infrared LED according to the time schedule.

- **Min/Max Photoresistor:** set the minimum and maximum photoresistor value based on the current actual photo-resistor value detected to control the **ON-OFF** of the LED light. You can set the maximum photoresistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Minimum and maximum photoresistor value arefrom "**0**" minimum to "**1000**" maximum respectively.

- **Start Time**: set the start time for the infrared LED to be turned on.

- **End Time**: set the end time for the infrared LED to be turned off.

Note:

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

7.2. LED Display Status

LED display adjustment is used to display the light changes of thecall button in the six statuses - normal(idle), offline, calling, talking and receiving a call. and

the user can also verify the current mode of the device through the LED status.

To setup on device web**Intercom>LED Setting> LED Status** interface.

The default LED Display Status:

LED Status		Description
Blue	Always on	Normal status
	Flashing	Calling
Red	Flashing	Network is unavailable
Green	Alwayson	Talking on a call
	Flashing	Receiving a call
Pink	Flashing	Upgrading

Parameters Set-up:

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

- **LED Color:** it can support three colors: **Red, Green, Blue.**

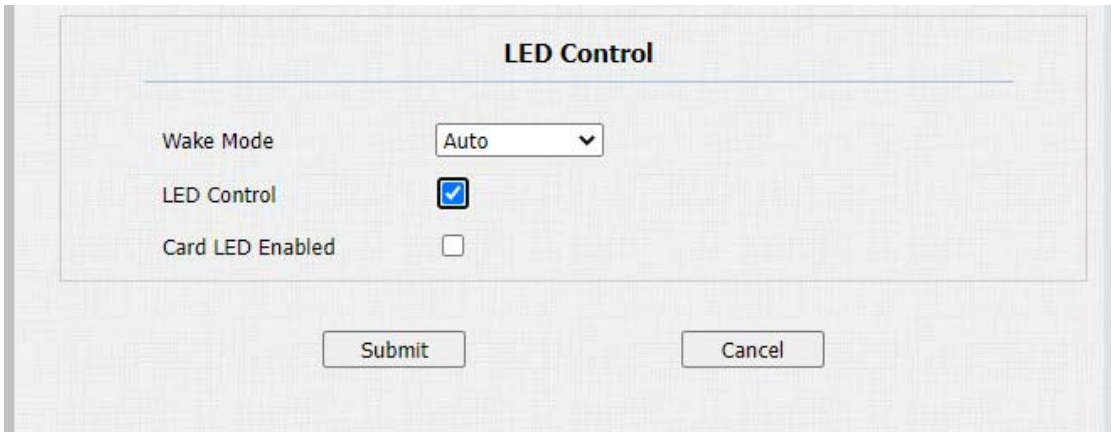
- **LED Display Mode:** to setup the different blink frequencies.

Note:

- The Status and Color of item can not be changed.
- The LED of upgrading mode can not be adjusted.

7.3. Setup LED Display from HTTP URL

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



Parameters Set-up:

- HTTP URL format:

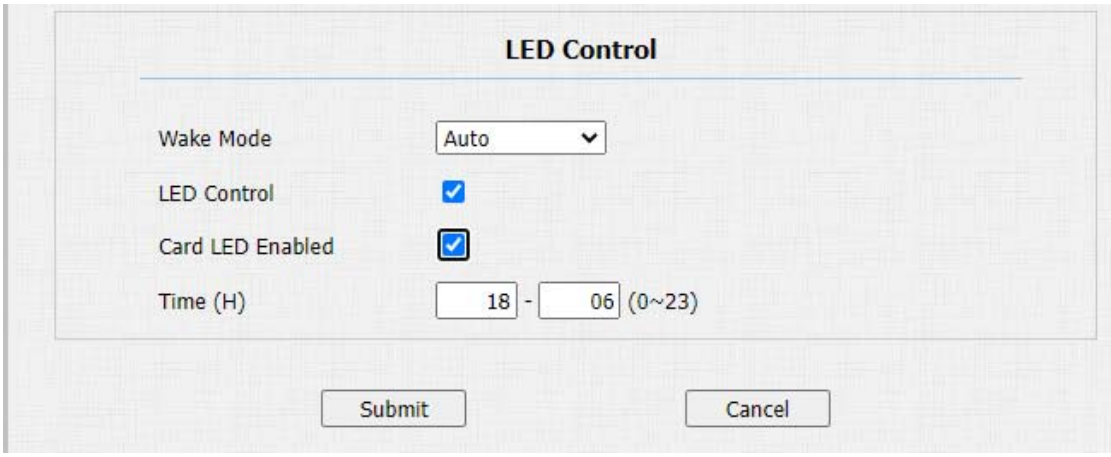
  http://PhoneIP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500

- Status: 1=Idle; 2=OffLine; 3=Calling; 4=Talking; 5=Receiving; Color: 1=Green; 2=Blue; 3=Red; Mode: 0=Always On; 1=Always Off; 500/1000/1500/2000/25000/3000

7.4. LED Setting on Card Reader Area

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, If you do not want to have the LED light on the card reader area to stay on, you can also set the timing for the exact time span during which theLED light can be disabled in order to reduce the

electrical power consumption. Path: **Intercom>LED Setting> LED Control**.



ParametersSet-up:

- **Card LED Enabled:**tick the check box if want to enable the card reader LED lighting and vice versa.

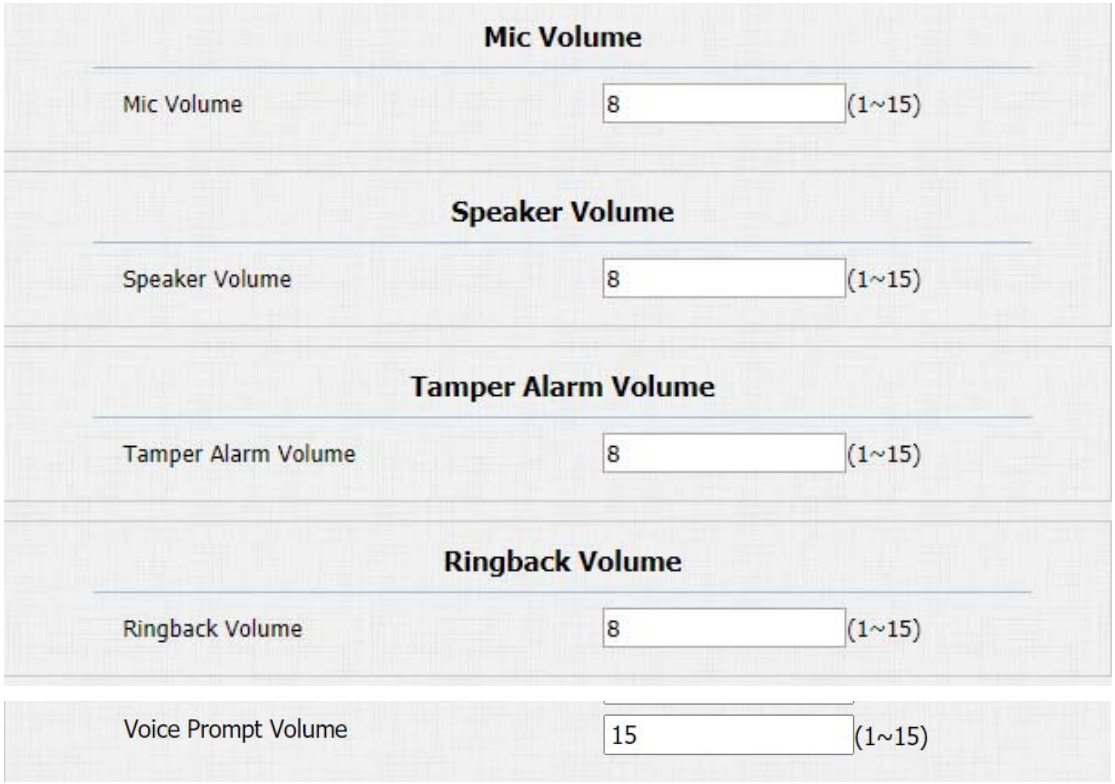
- **Time(H)**: enter the time span for the LED lighting to be valid,e.g. if the time span is set from **8-0 (Sart time- End time)** it means LED light will stay on during the time span from **8:00** am to**12:00** pm during one day (24 hours).

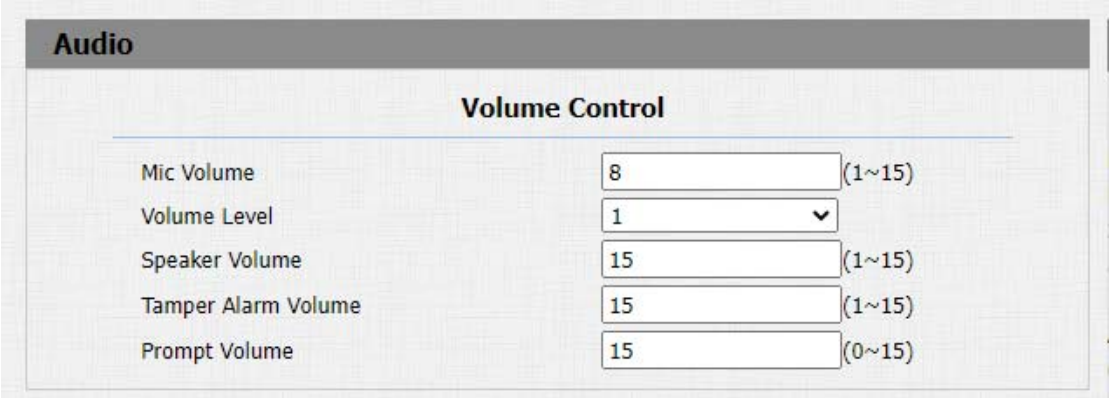
8. Volume and Tone Configuration

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

8.1. Volume Configuration

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



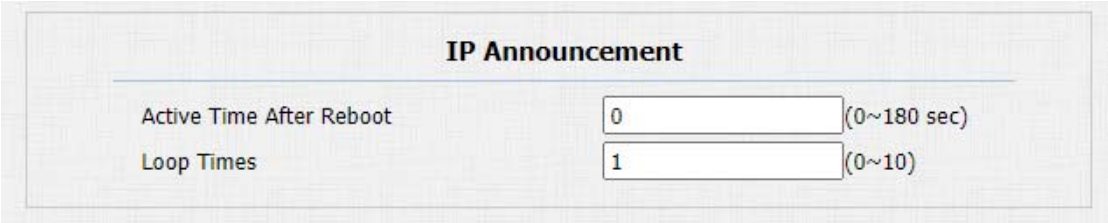


Parameters Set-up:

- **Mic Volume:** adjust the mic volume as needed.
- **Volume level:** adjust the volume level as needed.
- **Speaker Volume**: Adjust the speaker volume as needed.
- **Tamp Alarm Volume:** Adjust the volume for the tamper alarm.
- **Prompt Volume:** Adjust the volume for voice prompt.

8.2. IP Announcement

To set up device IP number announcement, navigate to **Phone > Audio > IP announcement**.

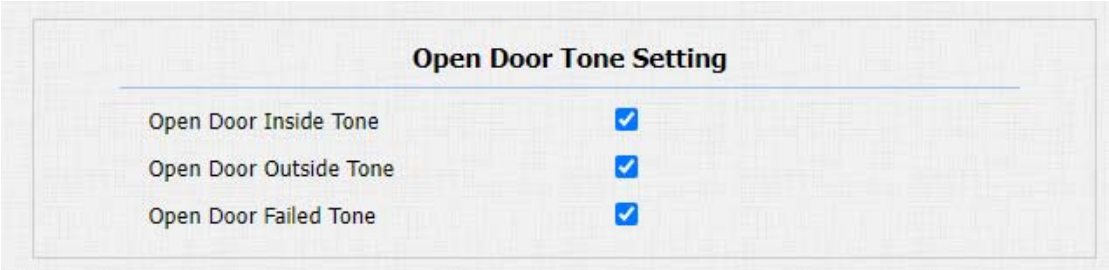


Parameter Set-up:

- **Active Time After Reboot**: select IP announcement time after the device reboot. For example, if you set it as 30 seconds, then you must press the call button within 30 seconds for the IP announcement after the device is rebooted, otherwise, the IP announcement will expire. If you set it as “0” seconds, then you can press the call button any time after the reboot for the IP announcement.
- **Loop Times**: set the IP announcement loop times.

8.3. Open Door Tone Configuration

You can not only enable or disable the Open Door Tone but also control the prompt words that accompanies the tone on the web **Phone>Audio > Open Door Tone Setting** interface.



Parameters Set-up:

- **Open Door Inside Tone:** select the checkbox to enable the open door inside tone. Open door inside tone is what you can hear when you open the door by pressing the Exit button in side.

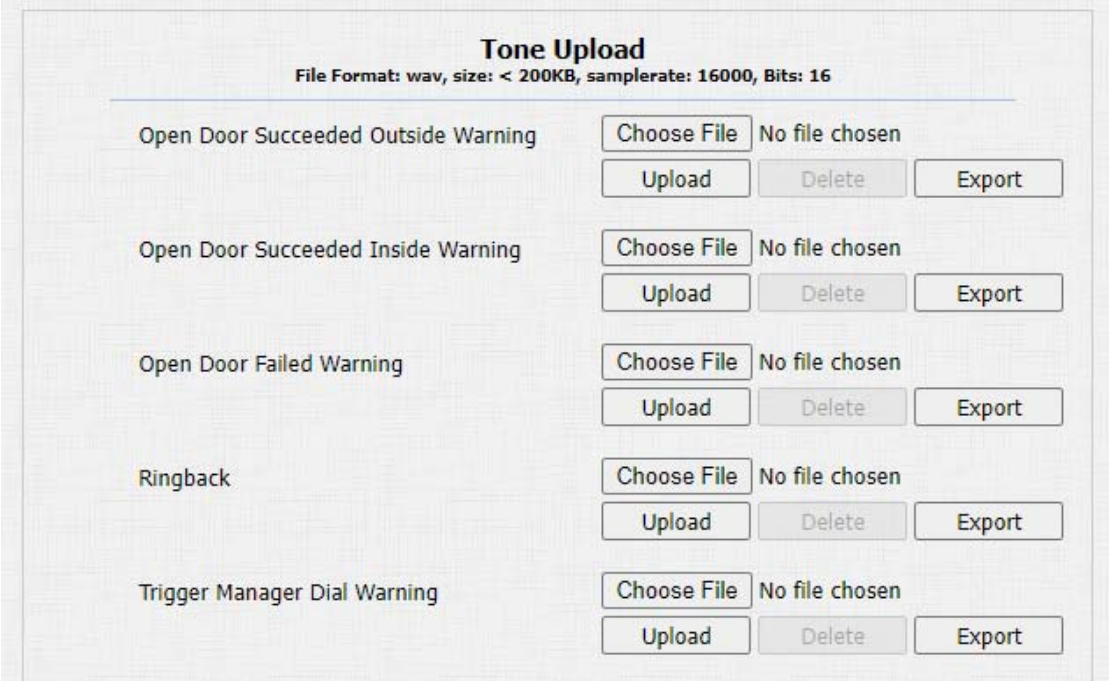
- **Open Door Outside Tone:** select the checkbox to enable the open door outside tone. Open door outside tone is what you can hear when you are granted door access via various access methods on the door phone.

- **Open Door Failed Tone**: enable the open door failure tone.

8.4. Upload Tone Files

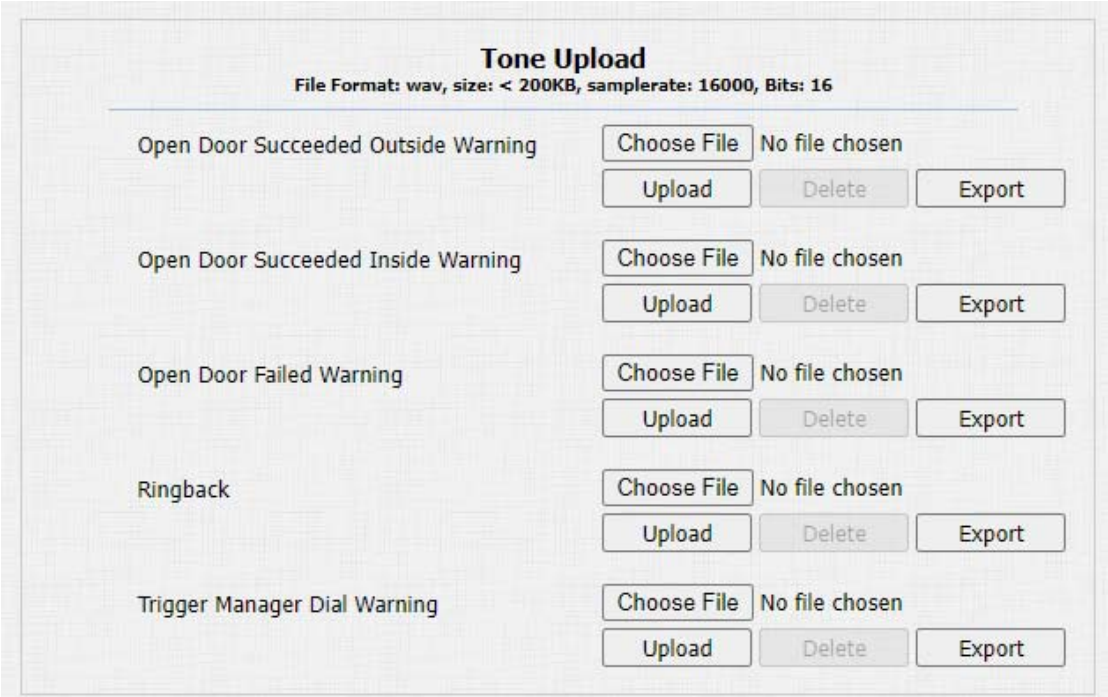
8.4.1. Upload Ringback Tone

You can customize the ringback tone if you need. Please follow the prompt about the file size and format. Navigate to **Phone>Audio >Tone Upload** interface.



8.4.2. Upload Open Door Tone

You can customize the door open tone if you need. The outside tone is used to open door via card or DTMF. The inside tone is used to open door via triggered input interface. Please follow the prompt about the file size and format. Path: **Phone>Audio >Tone Upload.**



Parameter Set-up:

- **Open Door Succeeded outside Warning**: 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.

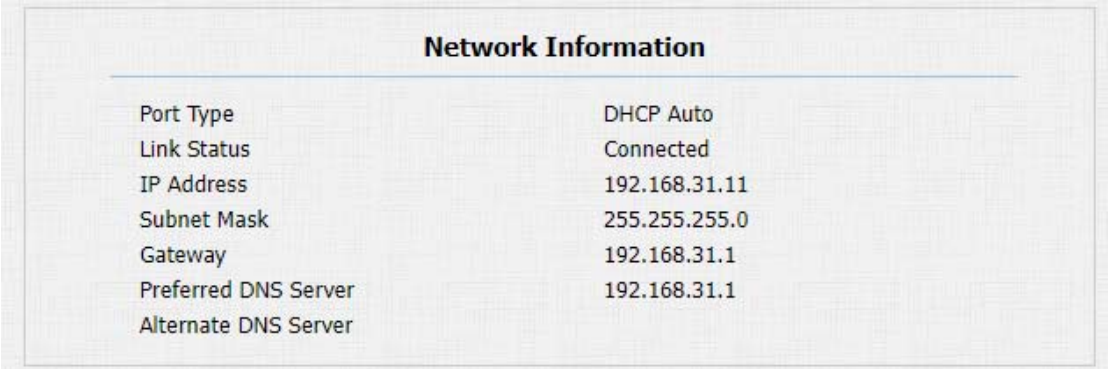
- **Open Door Succeeded Inside Warning**:warning tone that will go off when you opened the door from inside.Open door succeeded inside warning is what you can hear when you open the door by pressing the Exit button in side.

- **Trigger Manager Dial Warning**: warning tone that will go off when pressing the push-button to make manager dial call.

9. Network Setting

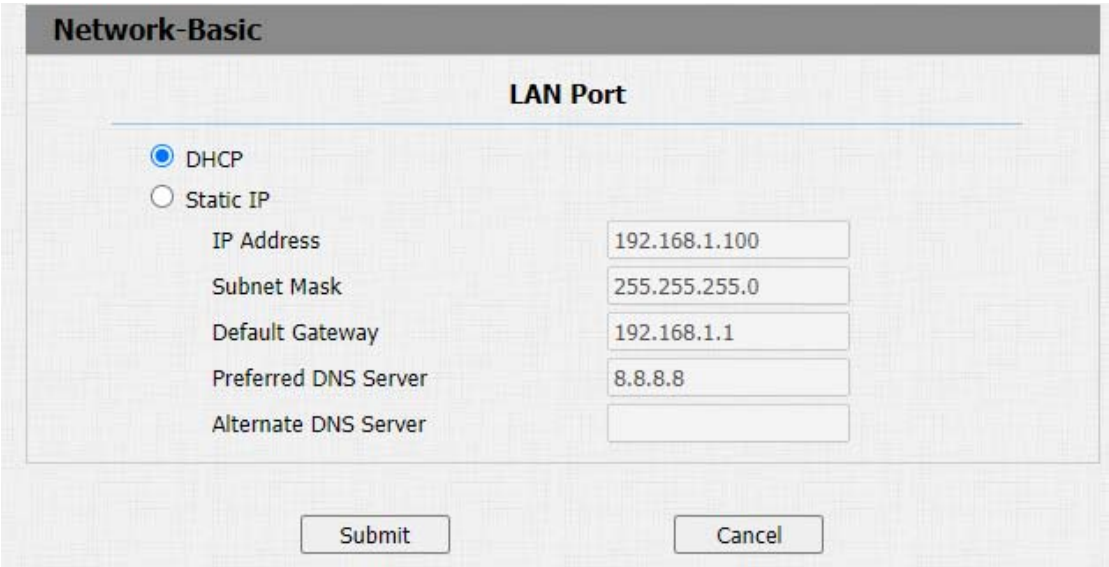
9.1. Network Status

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



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.



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 gatewayand 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.

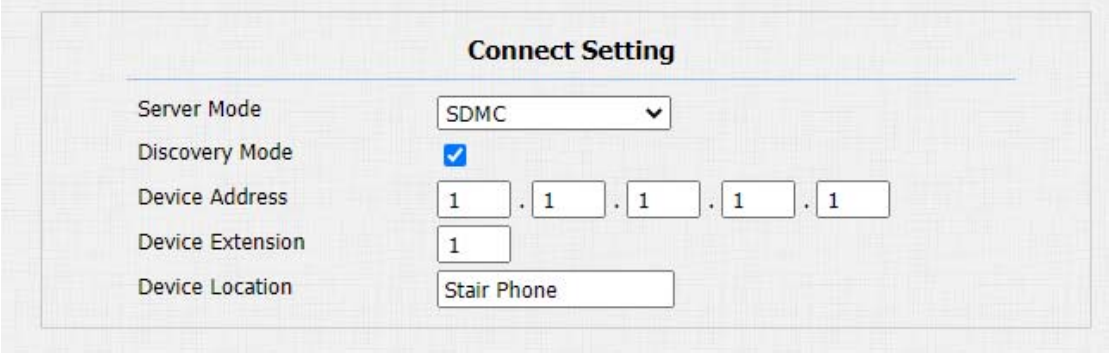
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.

- **Preferred/Alternate DNS:** 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 the device control and the

convenience of the management. So you can do it on web **Network > Advanced > Connect Setting**interface.



Parameter Set-up:

- **Server Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud and None. None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Cloud, SMDC in discovery mode.

- **Discovery Mode:** click "**Enable**" to turn on the discovery mode of the device so that it can be discovered by other devices in the network,and click "**Disable**" if you want to conceal the device so as not to be discovered by other devices.

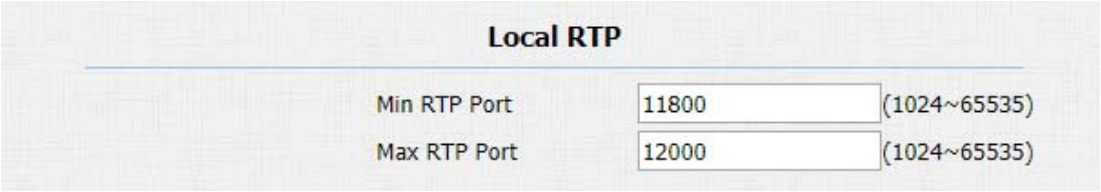
- **Device Address:** specify the device address by entering device location information from the left to the right:**Community, Unit, Stair, Floor, Room** in sequence.

- **Device extension**: enter the device extension number for the device you installed.

- **Device Location**: enter the location in which the device is installed and used.

9.4. 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 > Advanced >Local RTP**interface.



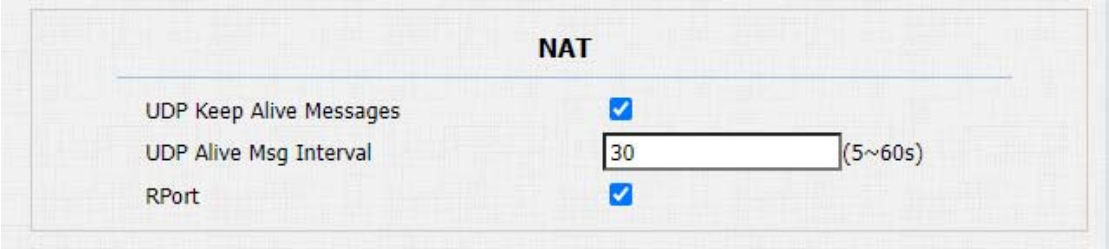
Parameter Set-up:

- **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. To do this configuration on web **Account > Advance > NAT** interface.



Parameter Set-up:

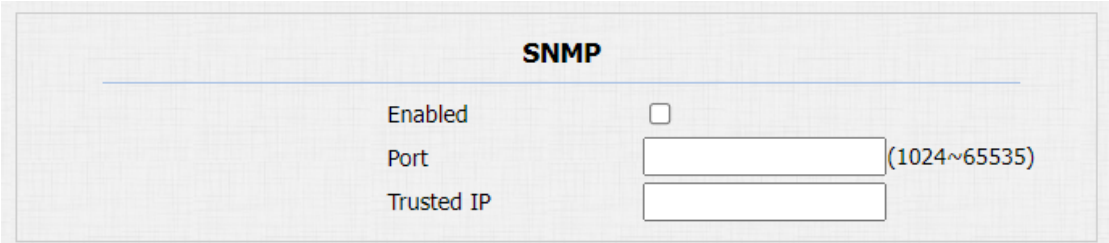
- **UDP Keep Alive Messages**: if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.

- **UDP Alive Msg Interval**: set the message sending time interval from 5-60 seconds, the default is 30 seconds.

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

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



Parameter Set-up:

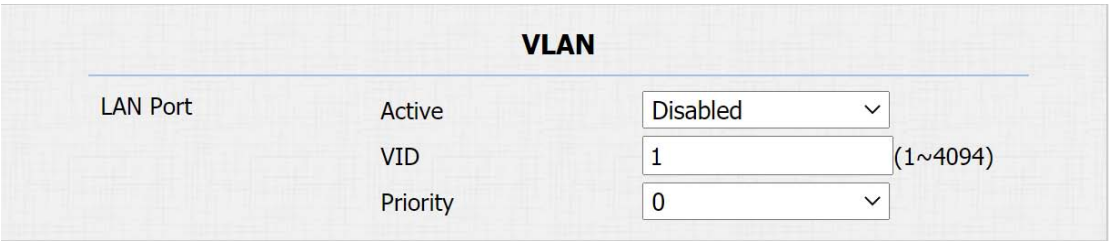
- **Active:** to enable or disable SNMP feature.

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



Parameter Set-up:

- **Active:**to enable or disable VLAN feature for designated port.

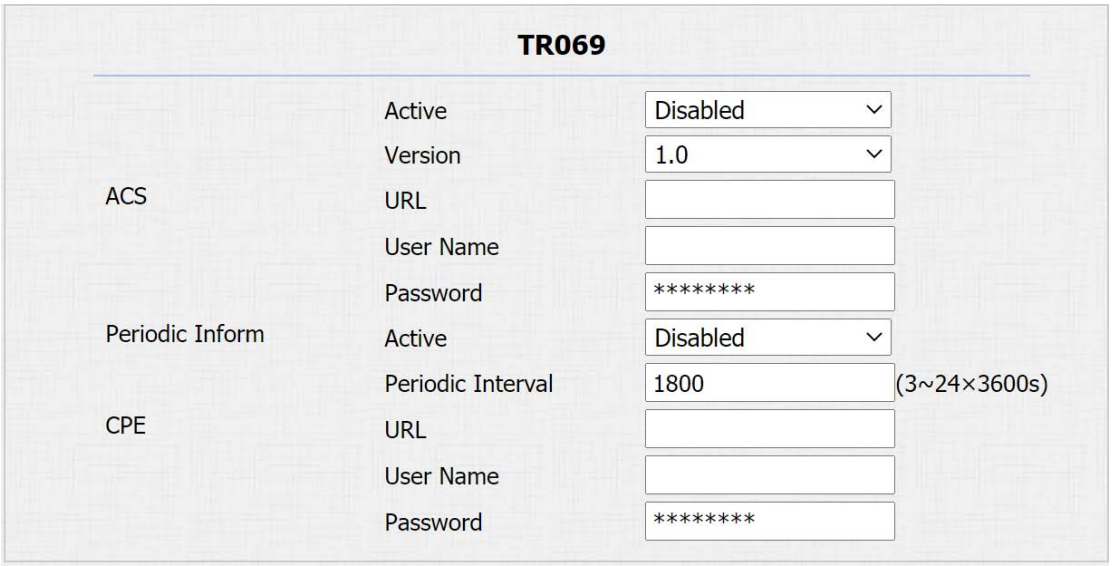
- **VID:**to configure VLAN ID for designated port.

- **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.



Parameter Set-up:

- **Active:** to enable or disable TR069 feature.

- **Version:** to select supported TR069 version (version 1.0 or 1.1).

- **ACS/CPE:** ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client side devices.

- **URL:** to configure URL address for ACS or CPE.

- **User Name:** to configure username for ACS or CPE.

- **Password:** to configure password for ACS or CPE.

- **Periodic Inform:** to enable periodically inform.

- **Periodic Interval:** to configure interval for periodic inform.

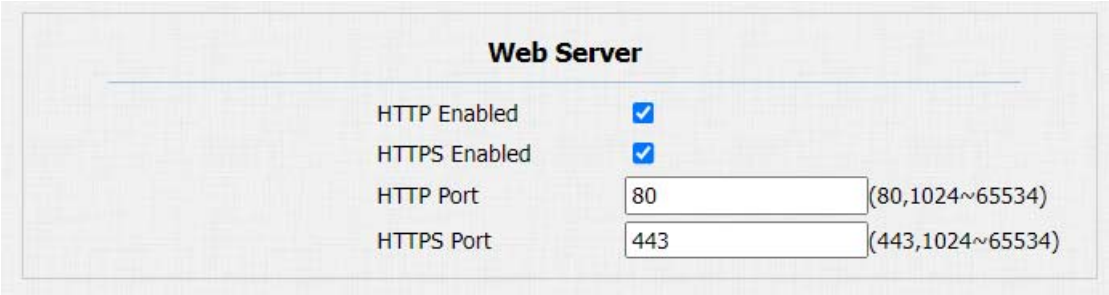
Note:

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

9.9. Device Web HTTPSetting

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.



Parameters Set-up:

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

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

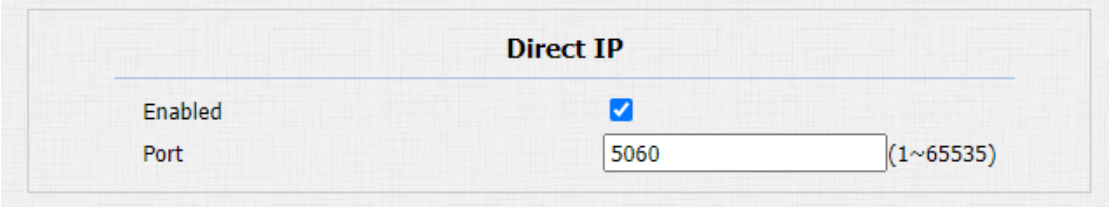
- **HTTP Port:**set up the port for HTTP access method. 80 is the default port.
- **HTTPS Port**: set up the port for HTTPS access method. 443 is the default port.

10. Intercom Call Configuration

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

10.1. IP call & IP Call Configuration

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



Parameters Set-up:

- **Enabled**: 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.

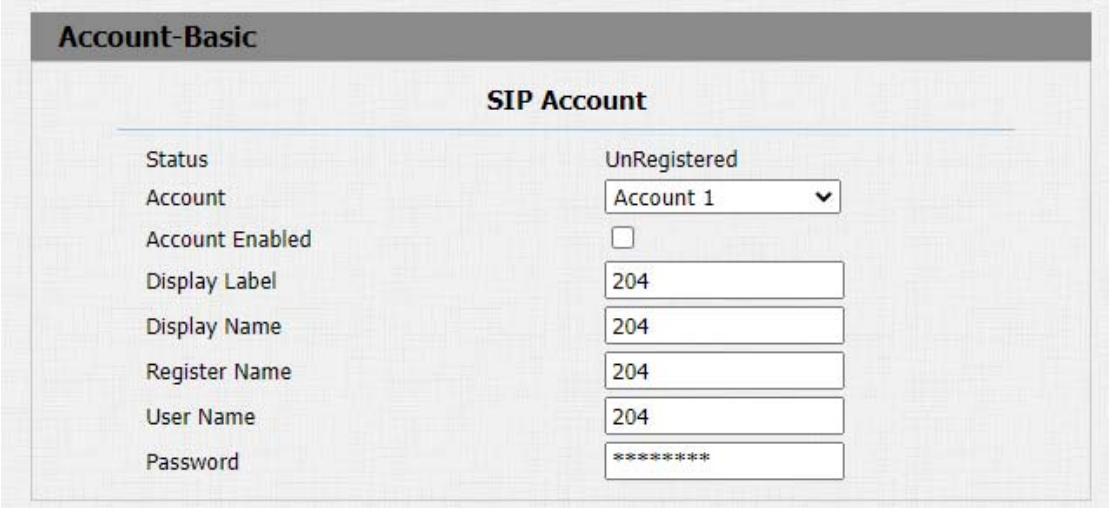
- **Port:** setup the IP direct call port, 5060 is the default port.

10.2. SIP Call &SIP Call Configuration

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

10.3. SIP Account Registration

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



Parameter Set-up:

- **Status:** check to see if the SIP account is registered or not.

- **Account**: select the exact account (Account 1&2) to be configured.

- **Account Enabled:** click **Enable** or **Disable** to activate or deactivate the registered SIP account.

- **Display Label:** configure the device label to be shown on the device screen.

- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.

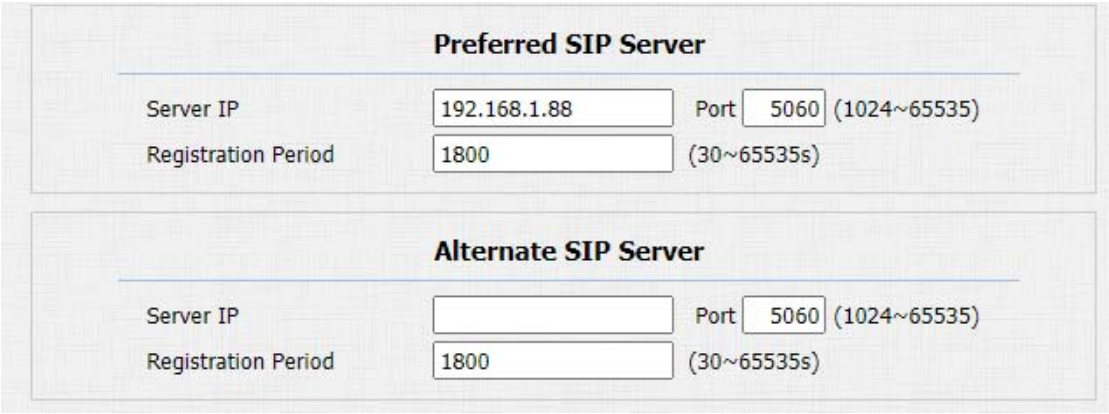
- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.

- **User Name:**enter the user name obtained from SIP account administrator.

- **Password:** enter the password obtained from the SIP account administrator.

10.4. SIP Server Configuration

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



Parameter Set-up:

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

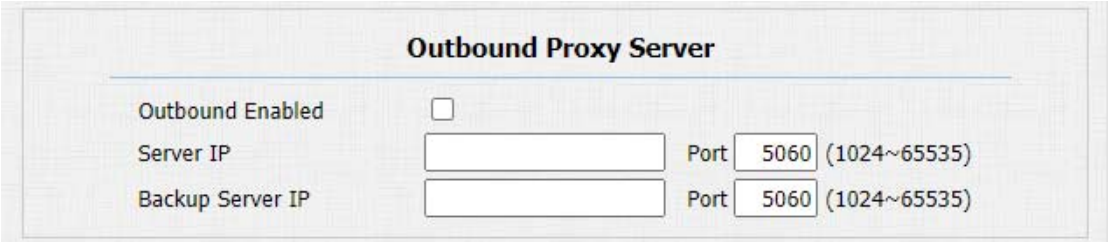
- **Alternate SIP Server:** enter the backup SIP server IP address or its URL.

- **Port:** set up SIP server port for data transmission.

- **Registration Period:** set up SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **"1800"**, ranging from **30-65535s**.

10.5. Configure Outbound Proxy Server

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



Parameter Set-up:

- **Outbound Enabled:** click "**Enable**" and "**Disable**" to turn on or turn off the outbound proxy server.

- **Server IP:** enter the SIP address of the primary outbound proxy server.

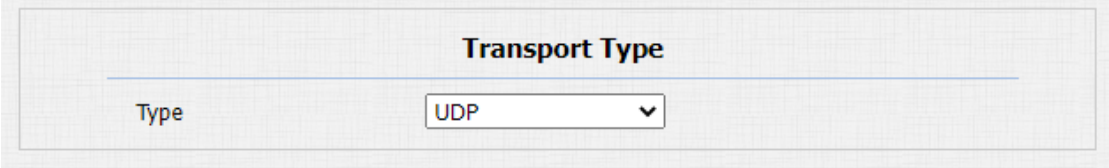
- **Port:** enter the Port number for establishing call session via the primary outbound proxy server

- **BackupServer IP:** set up Backup Server IP for the backup outbound proxy server.

- **Port:** enter the port number for establishing call session via the backup outbound proxy server.

10.6. Configure Data Transmission Type

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



Parameter Set-up:

- **UDP**:select **"UDP"** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.

- **TCP:** select **"TCP**" for Reliable but less-efficient transport layer protocol.

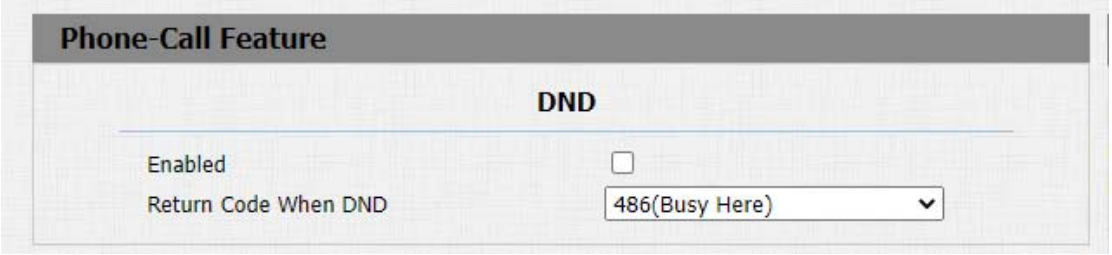
- **TLS**: select "**TLS**" for Secured and Reliable transport layer protocol.

- **DNS-SRV:** select "**DNS-SRV**" to obtain DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

10.7. Configure Calling Feature

10.7.1. DND

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



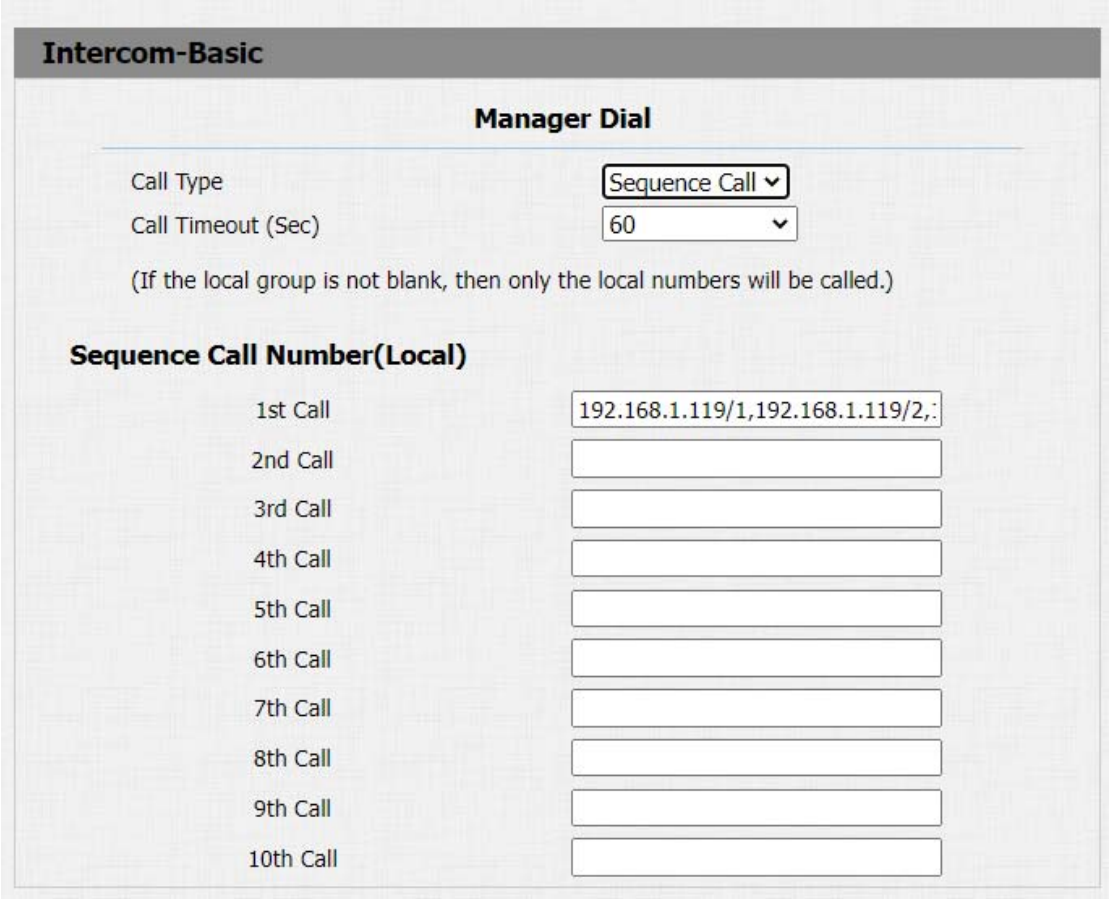
Parameter Set-up:

- **Enabled**: enable or disable the DND function. DND function is disabled by default.

- **Return Code When Refuse**: select code to be sent to the caller side via SIP server when you rejected the incoming call.

10.7.2. Manager Dial Call

Manger dial call consist of Robin call and group call. Manager Dialis used to quickly initiate the pre-configured numbers by pressing the Management key on door phone. You can create up 10 numbers. To do the configuration on the web **Intercom > Basic > Manager Dial** interface.



Parameter Set-up:

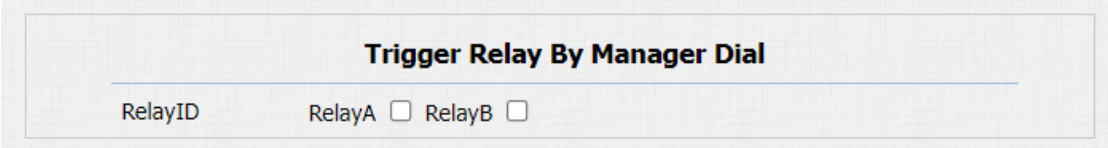
- **Call Type**: select the group call or sequence call (Robin call) for the manager dial call.

- **Sequence Call**: sequence call is used to initiate multiple numbers when your press the manager dial button. 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 callee, the call will not be transferred anymore.

- **Group Call**: group call is used to initiate calls to multiple numbers at the same when you press the manager dial button.

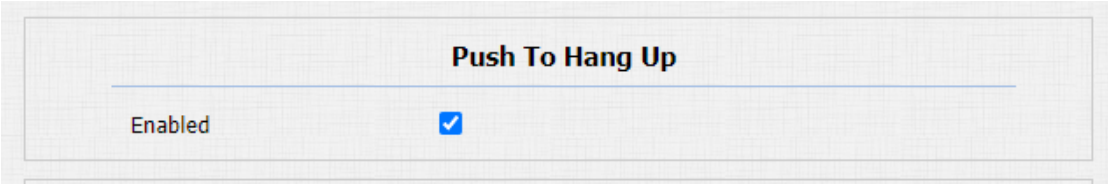
- **Sequence Call Number(Local):**enter the sequence call number. You can enter five sequence call number maximum in each line.

After the manager dial is set up, you can set up relays to be triggered by the manager dial if needed.



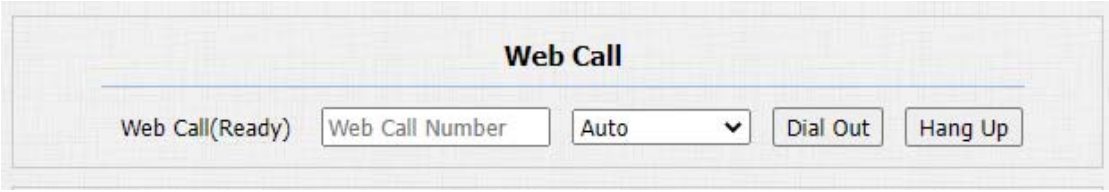
10.7.3. Call Hang-up

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



10.7.4. Web Call

In addition to making IP/SIP call directly on the device, you can also make the call on the device web interface without approaching to device physically for testing purpose, etc. You can navigate to **Intercom > Basic > Web Call**.

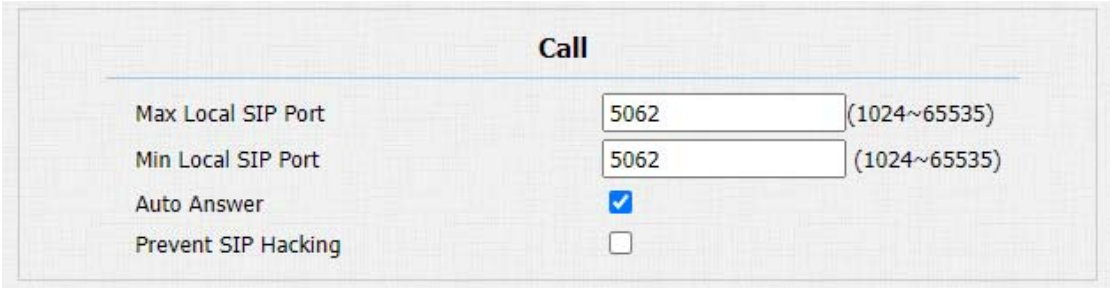


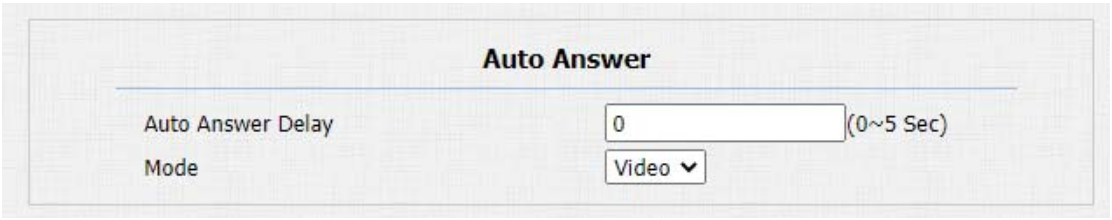
ParametersSet-up:

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

10.7.5. Auto Answer

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





Parameters Set-up:

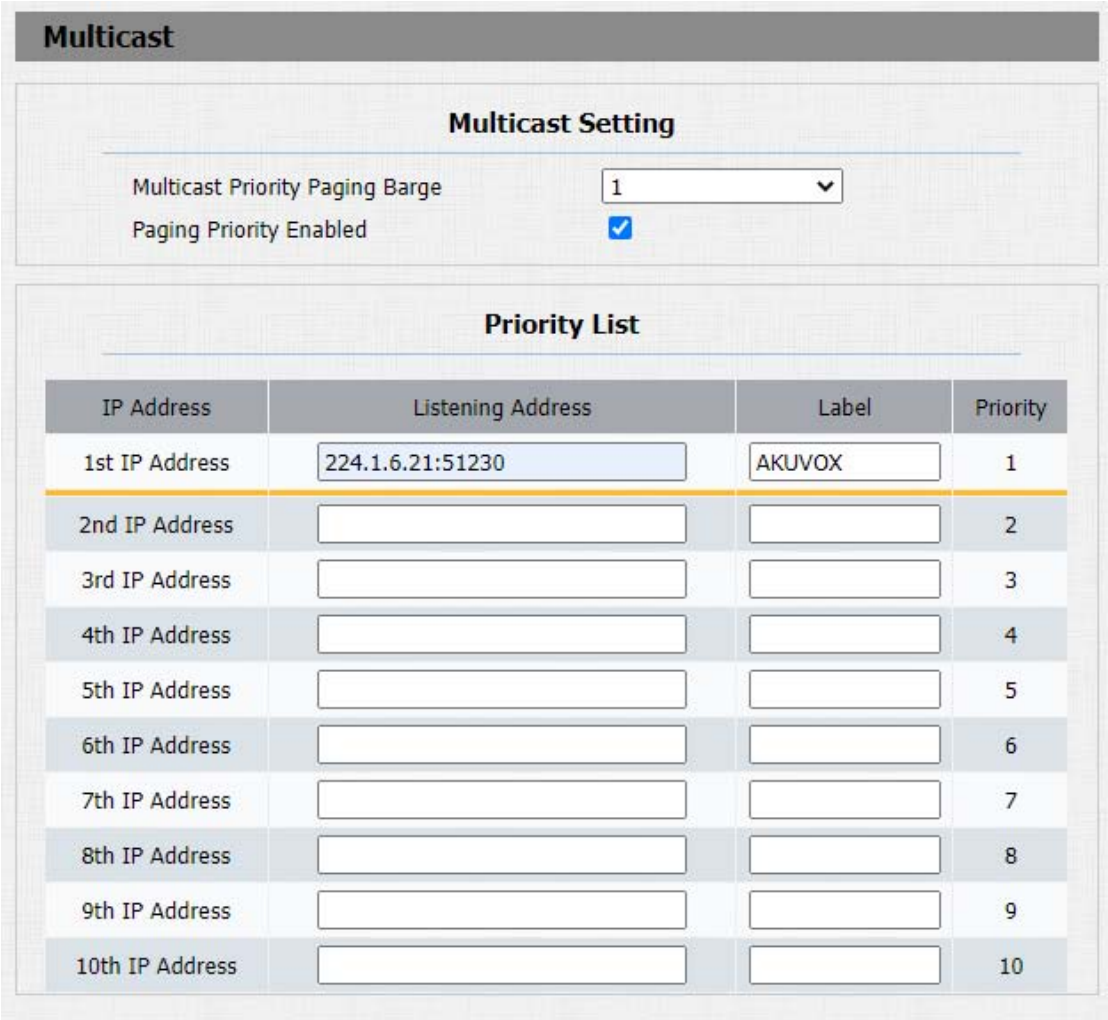
- **Auto Answer:**turn on the Auto Answer function by clicking "**Enable**".

- **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.

- **Mode:**set up the video or audio mode you preferred for answering the call automatically.

10.7.6. Multicast

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



Parameters Set-up:

- **Multicast Priority Paging Barge:** multicast or how many multicast calls are higher priority than SIP call, if you disable Paging Priority Active, SIP call will have high priority.

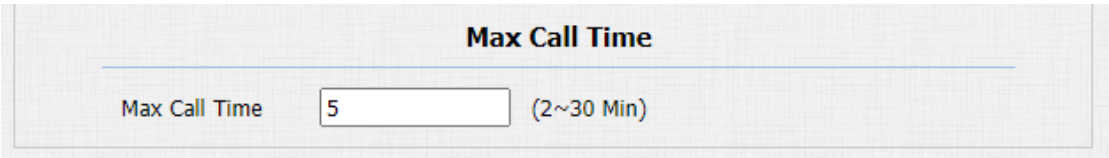
- **Paging Priority enabled:** multicast calls are called in order of priority or not.

- **Listening Address:** enter the multicast IP address you want to listen. The multicast IP address needs to be the same as the listened part and the multicast port can not be the same for each IP address. Multicast IP address is from 224.0.0.0 to 239.255.255.255.

- **Label:** enter the label for each listening address.

10.7.7. Configure Maximum Call Duration

Door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will terminate the calling automatically. You can navigate **Intercom > Basic > Max Call Time**.



Parameters Set-up:

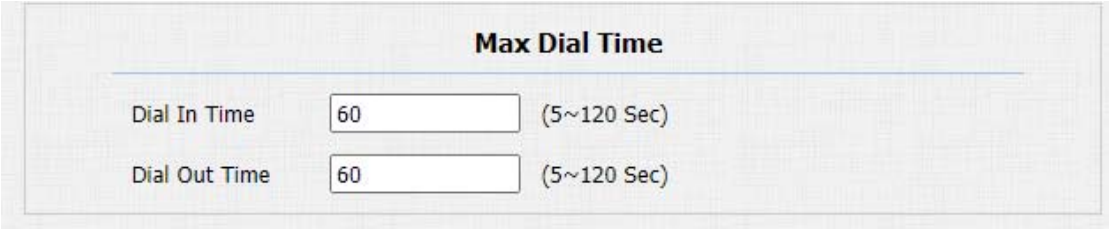
- **Max Call Time:**enter the call time duration according to your need (Ranging from 0-120 min). The default call time duration is 5 min.

Note:

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

10.7.8. Maximum Dial Duration

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



Parameters Set-up:

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

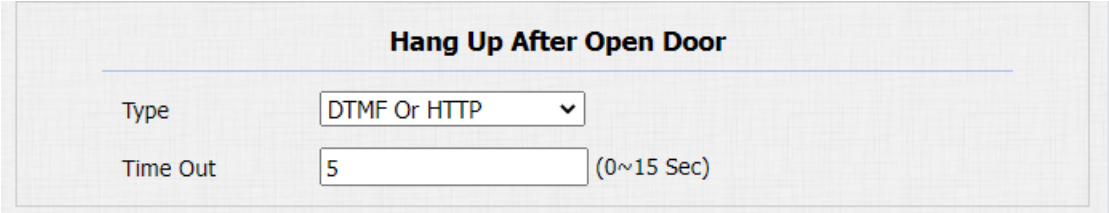
- **Dial out Time:** enter the dial in time duration for your door phone (ranging from 5-120 sec.) for example, if you set the dial out time duration is 60 seconds in your door phone, then the door phone will hang up the call it dialed out automatically if the call is not answered by the device being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

Note:

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

10.7.9. Hang Up After Open Door

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



Parameter Set-up:

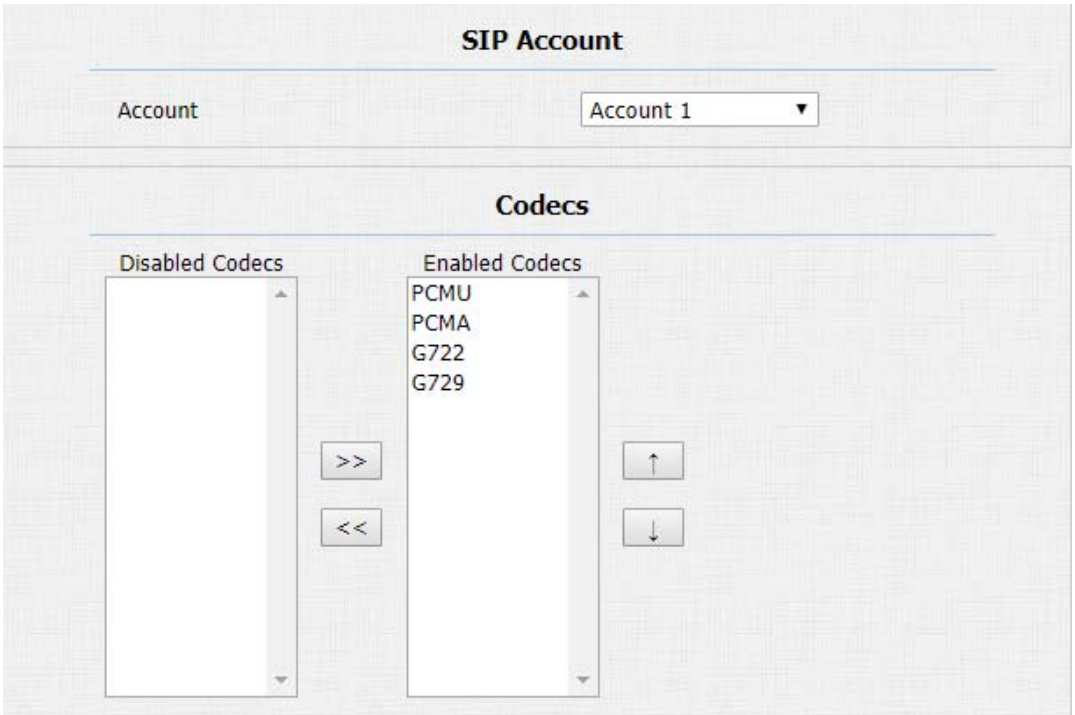
- **Type**: select the open door type. Door can be unlocked via "**DTMF**", "**HTTP**" command, "**DTMF Or HTTP**", and "**DTMF, HTTP or Input**".

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

11. Audio& Video Codec Configuration for SIP Calls

11.1. Audio Codec Configuration

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

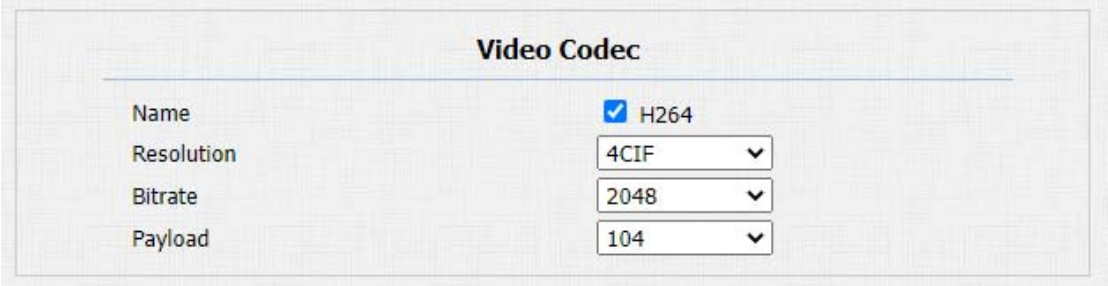


Please refers to the bandwidth consumption and sample rate for the four codecs types below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ

11.2. Video Codec Configuration

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



Parameter Set-up:

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

- **Resolution:** select the code resolution for the video quality among four options:**"QCIF", "CIF", "VGA", "4CIF" and "720P"** according to your actual network environment. The default code resolution is 4CIF.

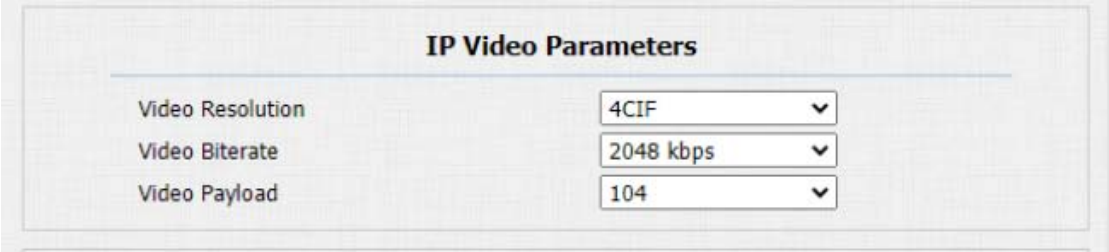
- **Bitrate:** select the video stream bit rate (Ranging from 320-2048). The greater the bitrate, the data transmitted in every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048.

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

11.3. Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to your actual network condition. To do so , you can go to

Phone>Call Feature > IP Video Parameters.



Parameter Set-up：

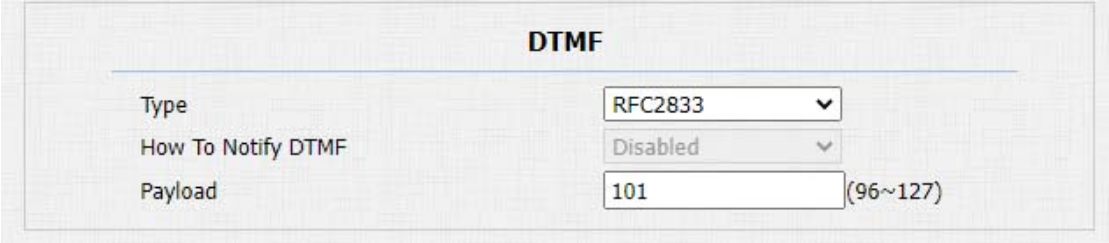
- Video Resolution:select the code resolution for the video quality among four options: “CIF”, “VGA”, “4CIF” and “720P”. The default code resolution is 4CIF.

- Video Bitrate: 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 kpbs”.

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

11.4. Configure DTMF Data Transmission

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



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

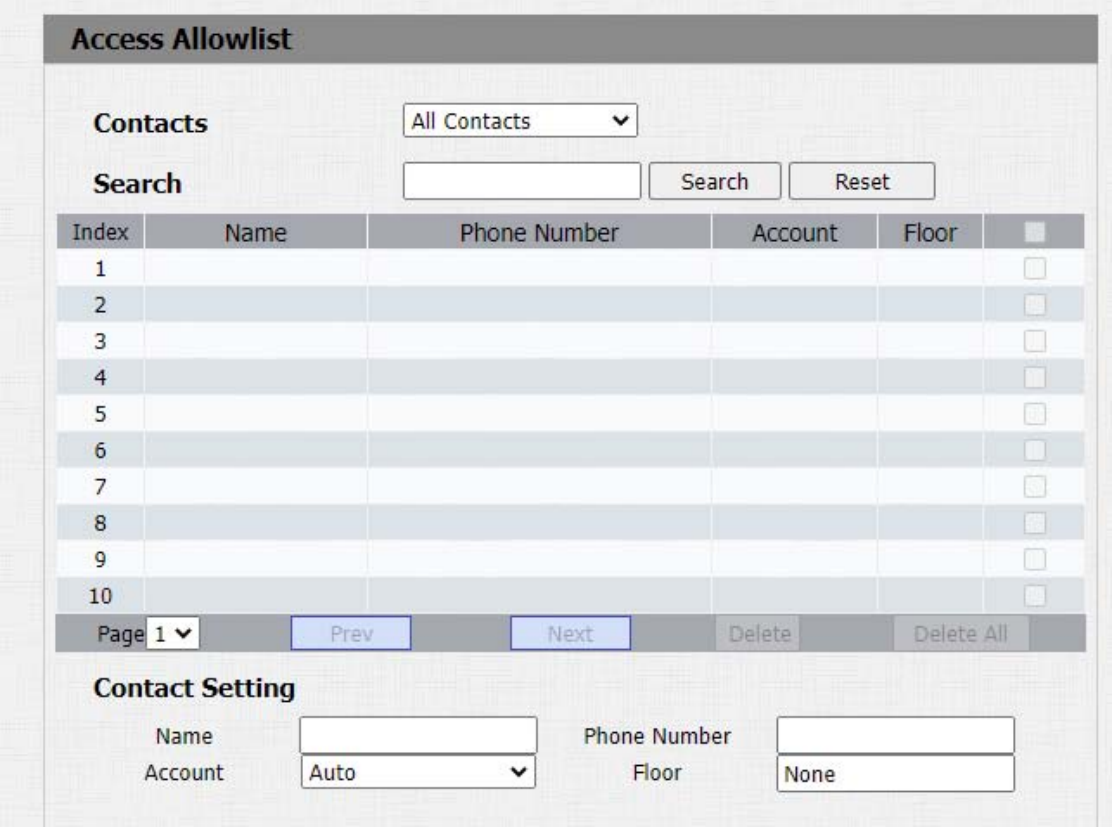
- Payload: set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

12. Access White List Configuration

Akuvox door phone supports to store up to 500 contacts that can give access permission to the indoor monitor or other devices. Access White list includes group setting and contact setting and management. To setit up on web **Contacts> Access Allowlist**.

12.1. Managing Contacts

You can search, create, display,edit and delete the contacts in your phone book. Path: **Contacts> Access Allowlist**.



Parameters Set-up：

- **Name:**enter the contact name, which is required.

- **Phone Number:**enter the phone number of the contact, which is required.

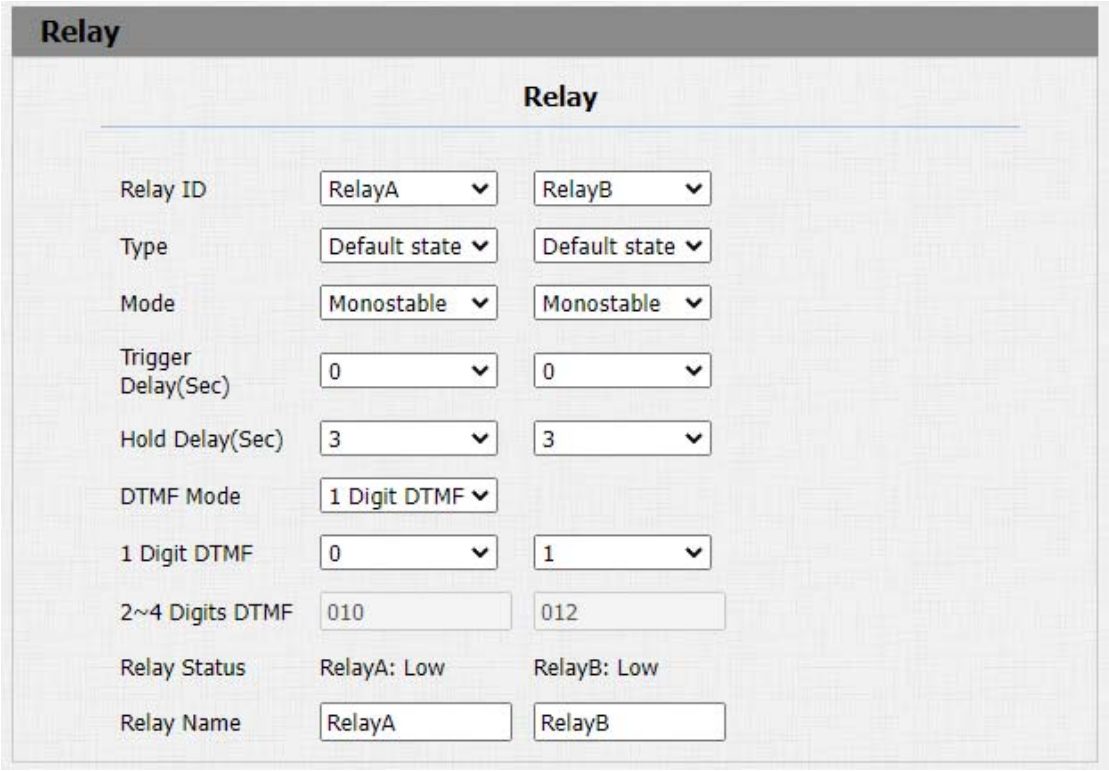
- **Account:** select which SIP account will be used to call out. If using IP direct call, it is not available.

- **Floor:**enter the floor number if needed.

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.



Parameter Set-up:

- **Relay ID:** you are allowed to set up three relay switches in total for the door access control (R29Z/R29ZL has only 1 relay).

- **Type:** if Default state is selected, the Relay Status shows Low which means the door is closed, the Relay Status shows which means the door is opened. If Invert State is selected, the Relay Status hows High which means the door is closed, and Low means the door is opened.

- **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.

- **Trigger 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.

- **Hold Delay (Sec):** set the relay hold delay timing (Ranging from 1-10 Sec.) For example, if you set the hold delay time as "**5**" Sec.Then the relay will resume the initial state after maintaining the triggered state for 5s.

- **DTMF Mode:** 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.

- **1 Digit DTMF:** set the 1-digt DTMF code within range from (**0-9 and *,#**) if the DTMF Option is set as "**1-digit**".

- **2~4 Digits DTMF:** set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if **DTMP Option** is set as 3-digits.

- **Relay Status:** relay status is low by default which means normally closed(NC) If the relay status is high, then it is in Normally Open status(NO).

- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note:

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

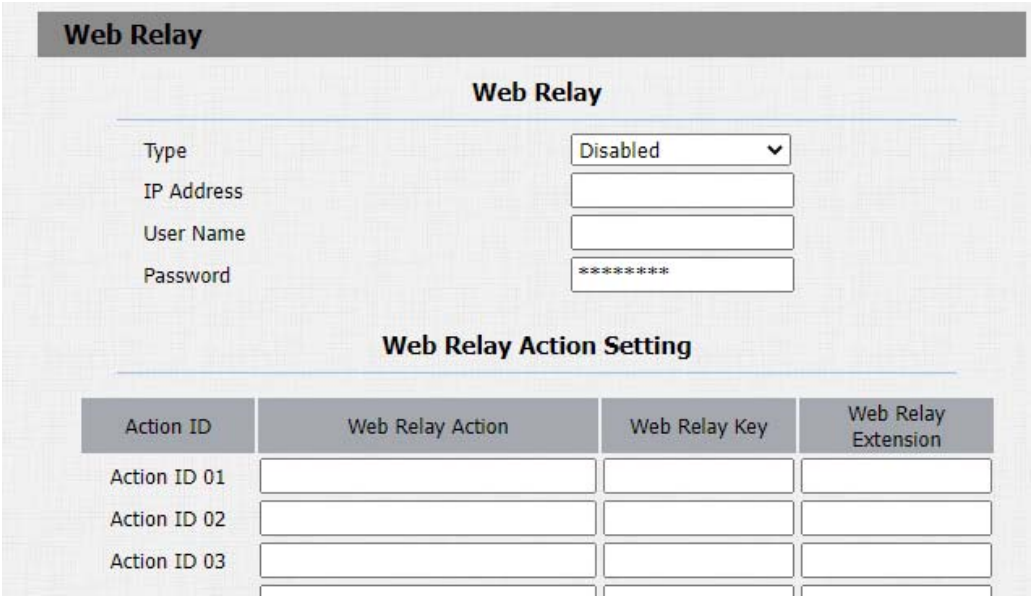
Note:

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

13.2. Web Relay Setting

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

Web relay needs to be set up on the web **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.



Parameter Set-up:

- **Type:** select among three options "**Disabled**" "**WebRelay**" and "**Both**". Select "**Web relay**" to enable the web relay. Select "**Disable**" to disable the web relay. Select "**Both**" to enable both local relay and web relay.

- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.

- **User Name**: enter the User name provided by the web relay manufacturer.

- **Password:**enter the password provided by the web relay manufacturer.The password is authenticated via HTTP and you can define the passwords using "**http get**" in Action.

- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding IP, username, pwd, you can fill in the HTTP command in the web relay action, so you can configure multiple web relays. See the HTTP command example below:

  a. If you do not fill in IP address in the IP Address Field above, fill in a complete HTTP command.

  For example, Http://admin:admin@192.168.1.2/state.xml?relayState=2.

(HTTP://:@IP address>/state.xml?relayState=2)

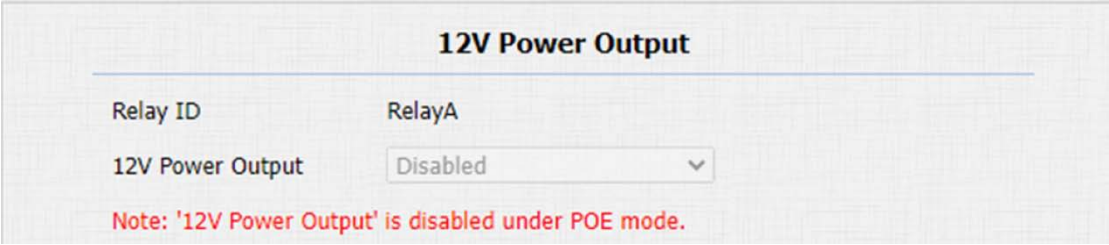
b. If you have already filled in the IP address above, fill in the omitted HTTP command, eg. state.xml?relayState=2.

- **Web Relay Key:**it can be null orenter the configured DTMF code, when the door is unlock via DTMF code, the action command will be sent to the web relay automatically.

- **Web Relay Extension:** it can be null or enter the relay extension information, which can be a SIP Account user name of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device, while this setting is optional.

13.3. Power Output Control

R20A can serve as a power supplyfor the external relays.You can set it up on the web **Intercom > Relay > 12V Power Output**.



Parameter Set-up:

- **Relay ID**: the relay you use to supply power.

- **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 **Trigger By Open Relay** if you want the R20Ato 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.

Note:

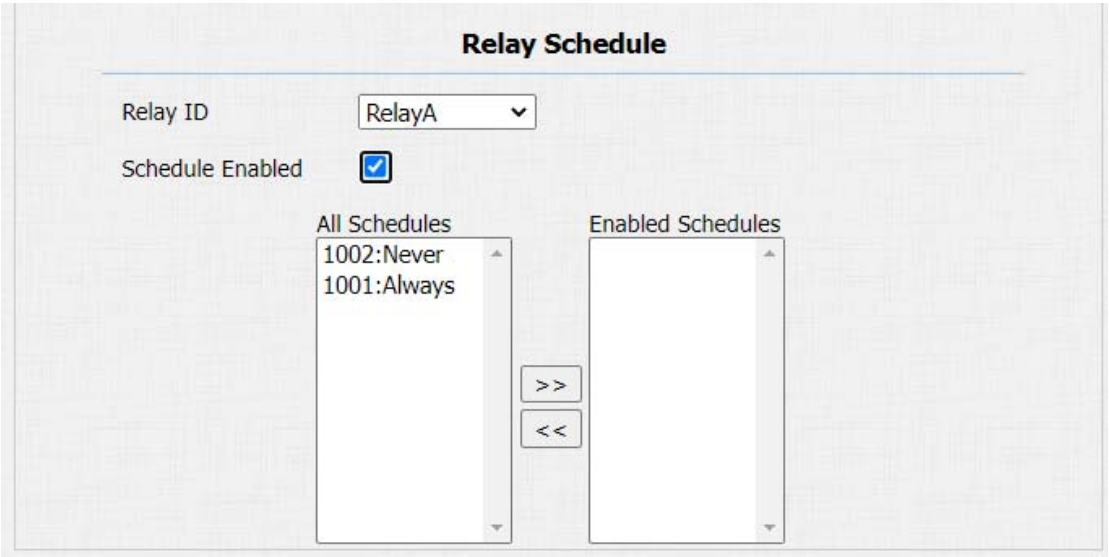
- '12V Power Output' is disabled under POE mode.

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. Relay schedule

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



Parameter Set-up:

- **Relay ID:** choose on the relay you need to set up.

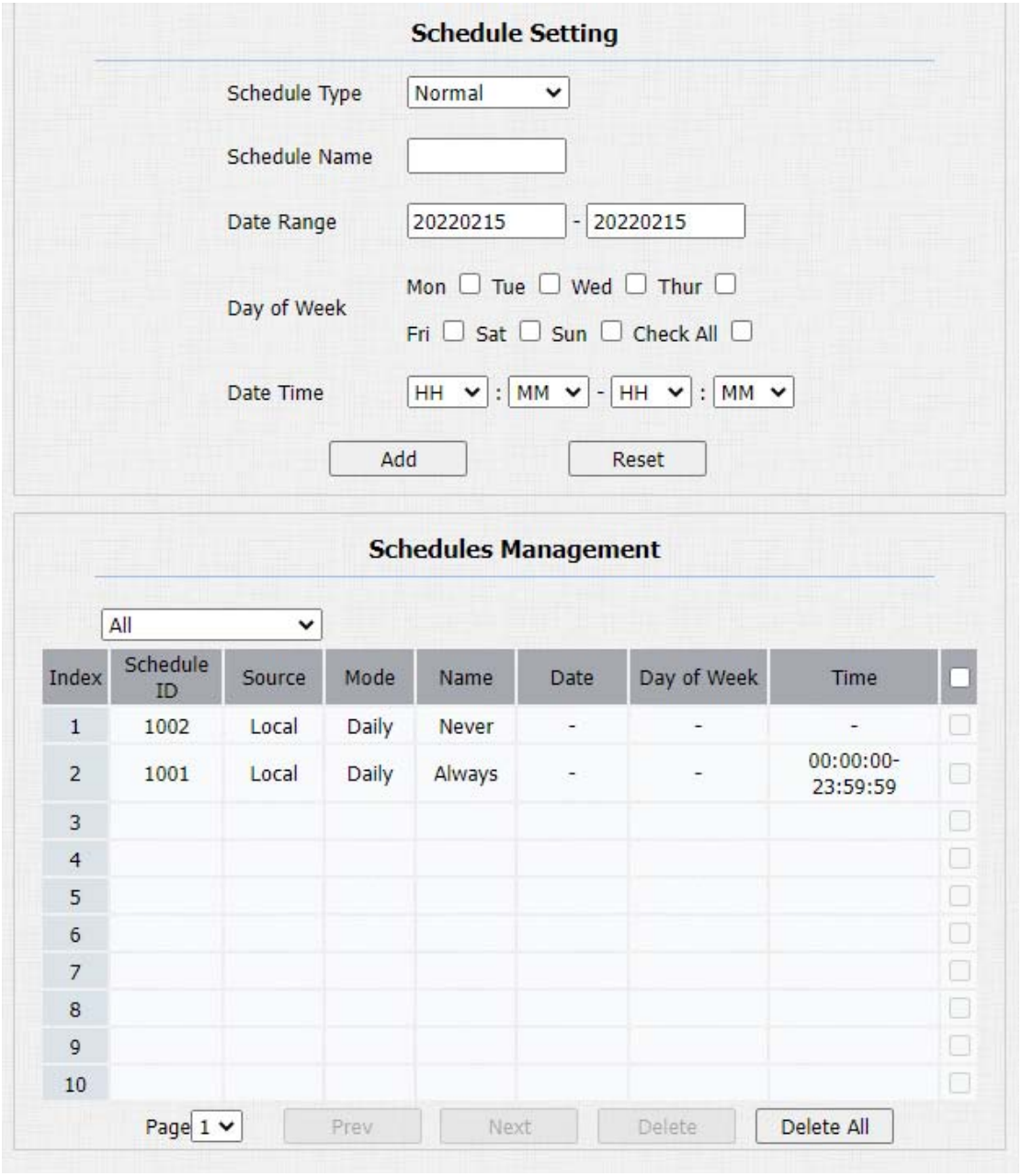
- **Schedule Enabled**: it is disabled by default. Only choose to enable it, that you can select the schedule. For creating the schedule, please refer to door access schedule configuration.

14.2. Configure Door Access Schedule

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

14.2.1. Create Door Access Schedule

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



Parameters Set-up:

- **Schedule Type:**set the type of time period. There are three types to choose from: Daily, Weekly, and Normal. The default is Daily.

- **Schedule Name:**set the name of the time period.

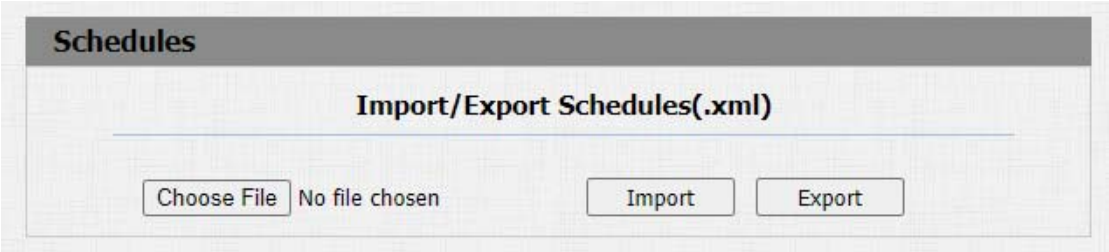
- **Date Time:** set the corresponding time period.

- **Day of Week:**select the corresponding day of the week. This field will only be displayed when the Week and Normal types are selected.

- **Date Range:** set the corresponding date. This field will only be displayed when the Normal type is selected.

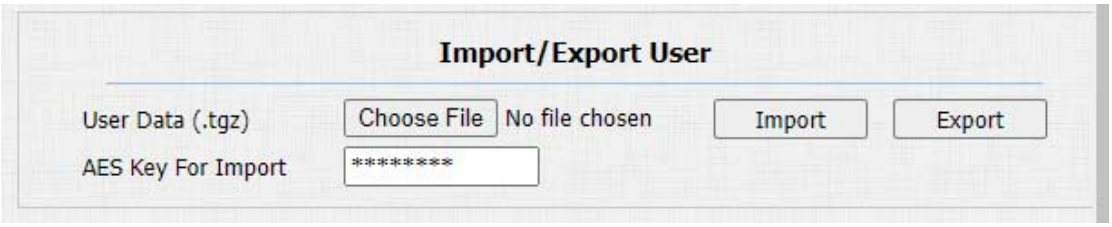
14.2.2. Import and Export Door Access Schedule

In addition to creating 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).**



14.2.3. Import and Export User

You can import and export the user in batch. You can navigate to **Intercom > User**.



Parameter Set-up:

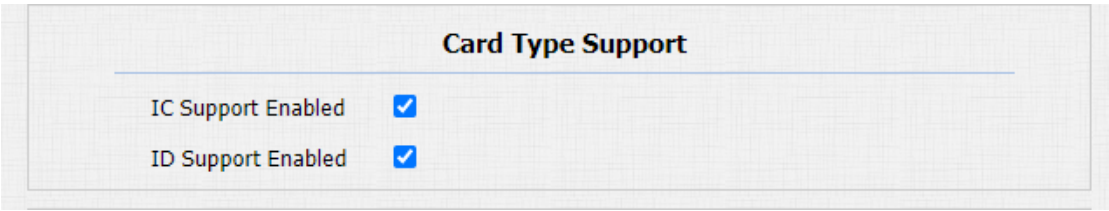
- **AES Key For Import**:enter the AES code before importing the AES-encrypted.tgz file to the door phone.

15. Door Unlock Configuration

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

15.1. IC/ID Card Control

You can enable or disable the IC and ID card function if needed. You can navigate to **Intercom > Card Setting > Card Type Support**.



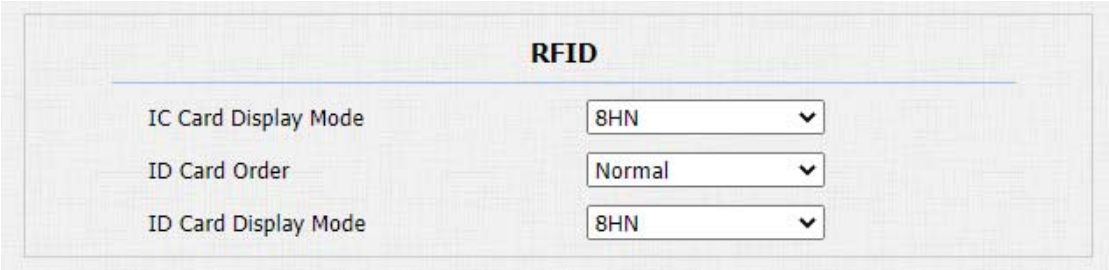
Parameter Set-up:

- **IC Support Enabled:** tick this feature to allow to use IC card for access door access.

- **ID Support Enabled:** tick this feature to allow to use ID card for door access.

15.2. 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.



Parameters Set-up:

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

- **ID Card Order**: select normal or reversed display of ID card.

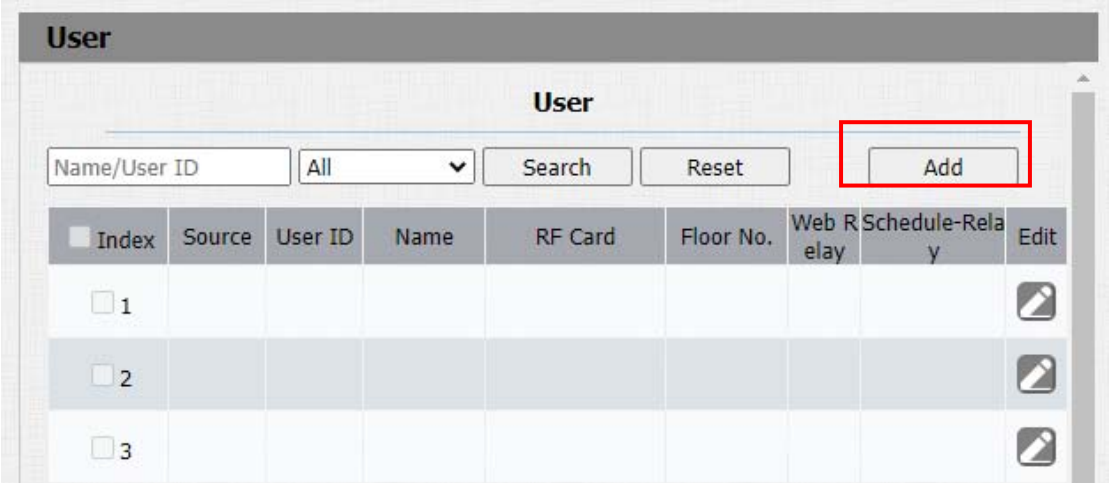
- **IDCard Display Mode:** select the card format for the **ID Card** for the door access among five format options: **8H10D; 6H3D5D(W26); 6H8D; 8HN; 8HR.** The card code format is 8HN by default in the door phone.

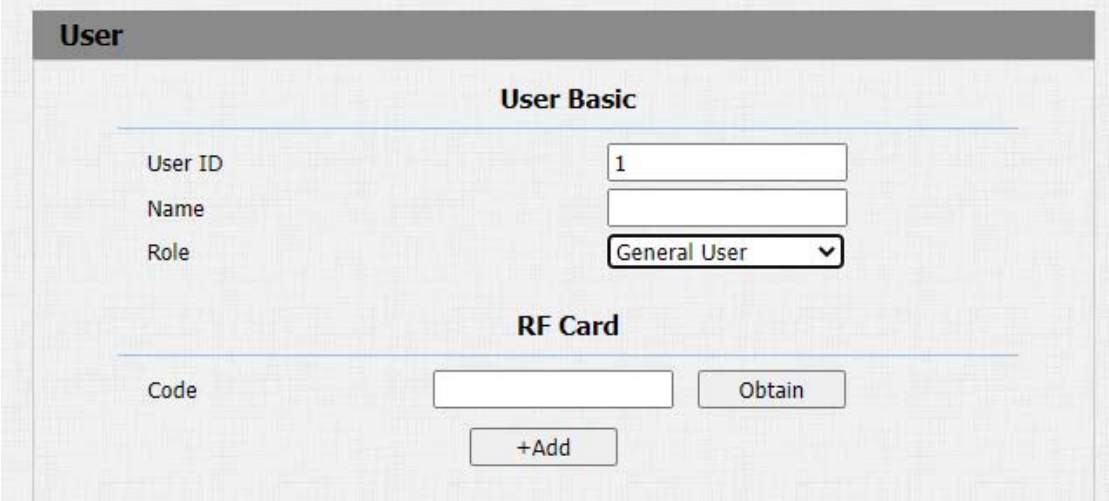
15.3. Configuring RF Card for Door Unlock

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

15.3.1. Configure RF Card on the Web Interface

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 maximumin length and can not be reused for other users. The User ID can be generated automatically or manually.

- Name: enter the user name.

- Role: select general users for residents and select administrator for the administrator.

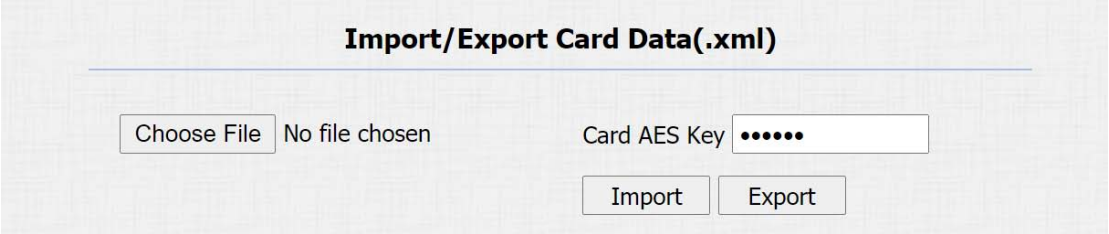
- **Code**: place the card on the device card reader area and click obtain.

Note:

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

15.4. Import and Export Card Data of Access Control

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



Parameter Set-up:

- **Card AES Key**: enter the AES code before importing the AES-encrypted.xml file to the door phone.

15.5. Mifare/Defire CarD Encryption

Mifare card and Defire card can be encrypted for greater security. To encrypt the card, you can navigate to **Intercom > Card setting > Mifare/Defire Card Encryption.**

Parameter Set-up:

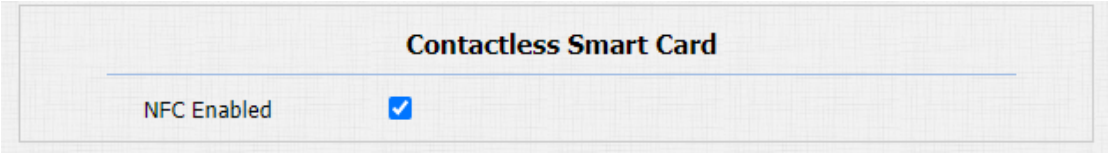
- **Enabled**: enable the Mifare/Defire Card Encryption.

- **Sector/Block**: enter the sector and block that you want the card number to be written into the Mifare/Defire Card. For example, you can write the card number into sector 3 and block 3 in the card.

- **Block Key**: enter the block password for access.

15.5.1. NFC Card Setting

NFC function needs to be enabled before you can use the NFC for contactless door access. Path:**Intercom > Card Setting**interface.

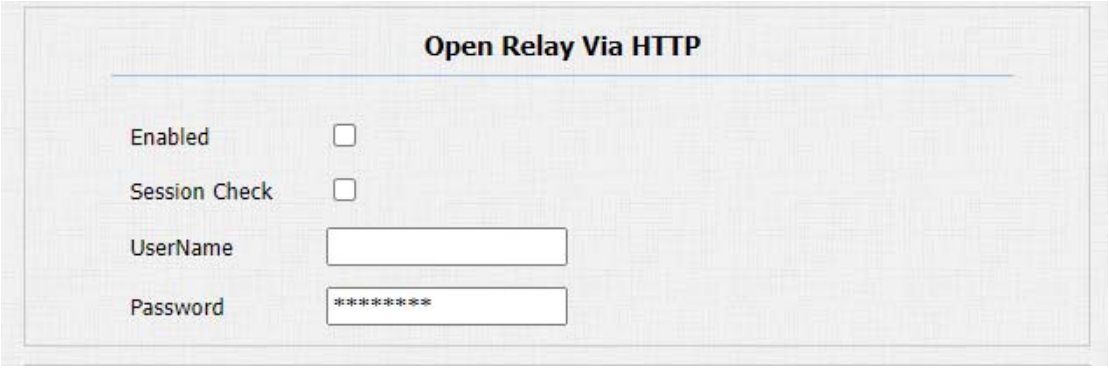


Parameter Set-up:

- **NFC Enabled:** NFC feature is enabled by default. The device must be connected to SmartPlus for the NFC application.

15.6. 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:

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

- **Session Check**: enable it to protect data transmission security.

- **UserName:** enter the user name of the device web interface, for example, "**Admin**".

- **Password**: enter the password for the HTTP command. For example: "**12345**".

Please refer to the following example:

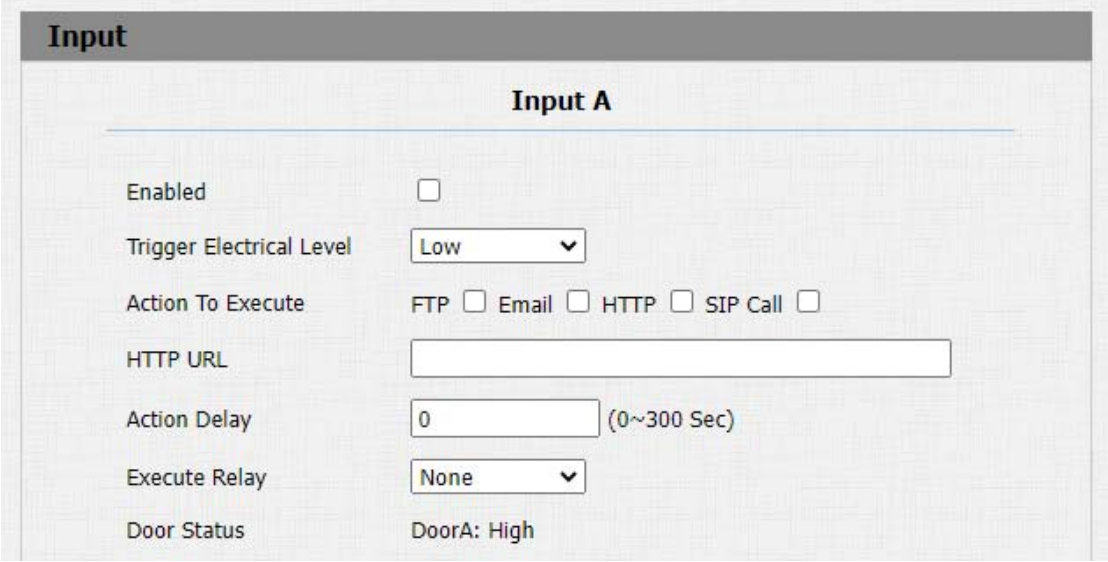
http://192.168.35.127/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note:

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

15.7. 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.



Parameter set-up:

- **Enabled:**enable the function if needed.

- **Trigger Electrical Level:** select the trigger electrical level options between "**High**" and **"Low**" according to the actual operation on the exit button.

- **Action To Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.

- **Http URL:** enter the URL if you select the HTTP to carry out the action.

- **Action Delay:** set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after your press the button.

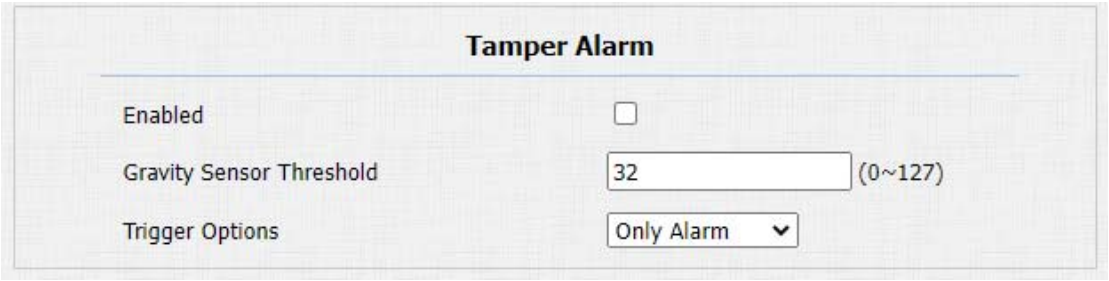
- **Execute Relay:** set up relays to be triggered by the actions.

- **Door Status:**display the status of the input signal.

16. Security

16.1. Tamper Alarm Setting

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



Parameter Set-up:

- **Tamper Alarm**: enable the anti-theft alarm function.

- **Gravity sensor Threshold**: set the threshold for the gravity sensory sensitivity. The lower the value is, the higher the value will be. The gravity sensor value is 32 by default.

- **Trigger Options**: select what can be triggered when the gravity sensor is triggered.

16.2. Client Certificate Setting

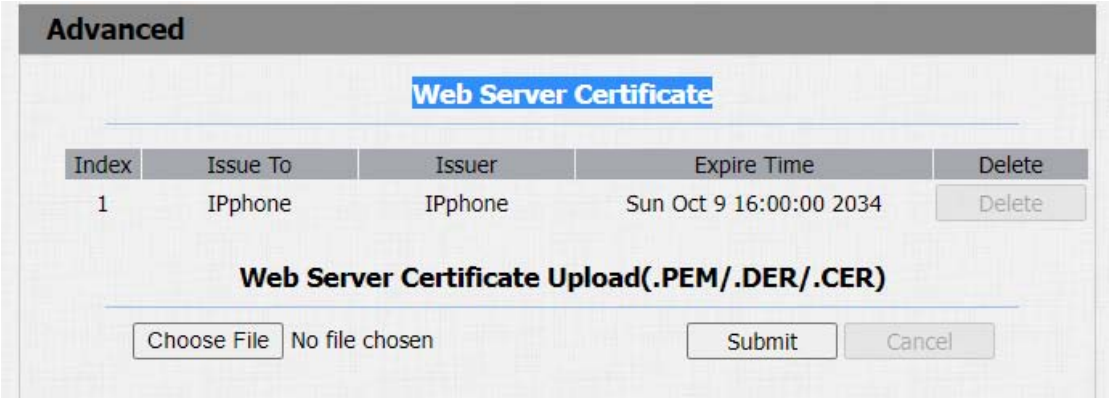
Certificates can ensure communication integrity and privacy when deploying Akuvox door phone. So, when the user needs to establish SSL protocol, it is necessary to upload corresponding certificates for verification.

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

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

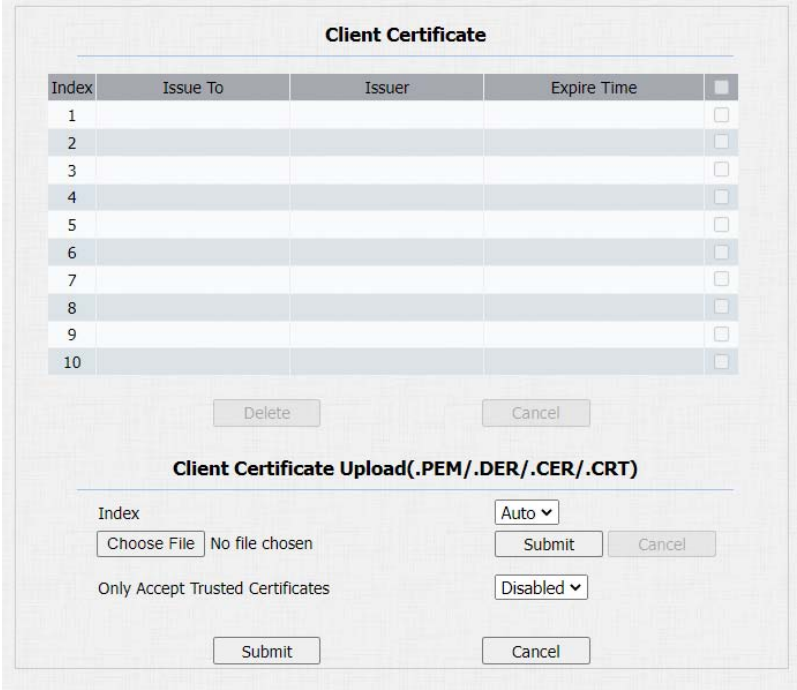
16.2.1. Web Server Certificate

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



16.2.2. Client Certificate

To upload and configure client certificate on the same page.



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 in numeric order. If you select the 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 select Enabled, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If select Disabled, the phone will not verify the server certificate no matter whether the certificate is valid or not.

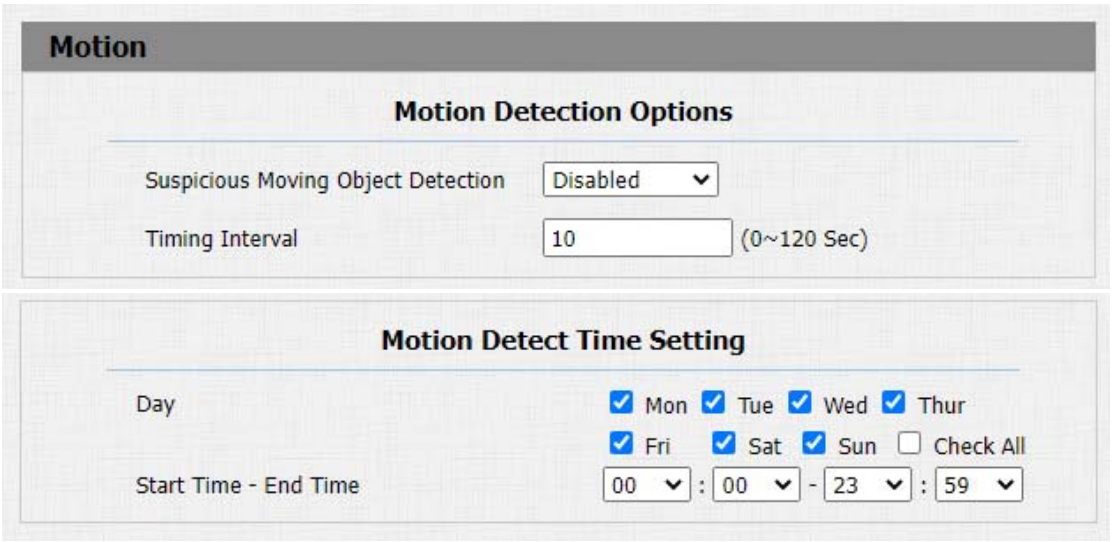
16.3. Motion Detection

Motion Detection is often used for unattended surveillance video and automatic alarms. The images collected by the camera at different frame rates will be calculated and compared by the CPU according to a certain algorithm.

When the picture changes, if someone walks by, the lens is moved, the number obtained by the calculation and comparison result will exceed the threshold and indicate that the system can the corresponding processing is made automatically.

16.3.1. Configure Motion Detection

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



Parameter Set-up:

- **Suspicious Moving Object Detection**:select “disable” to disable the motion detection. Select “IR detection” to enable the IR sensor based motion

detection for the suspicious moving objects. And select " Video detection" to enable the video-based motion detection during the monitoring for the suspicious moving object.

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

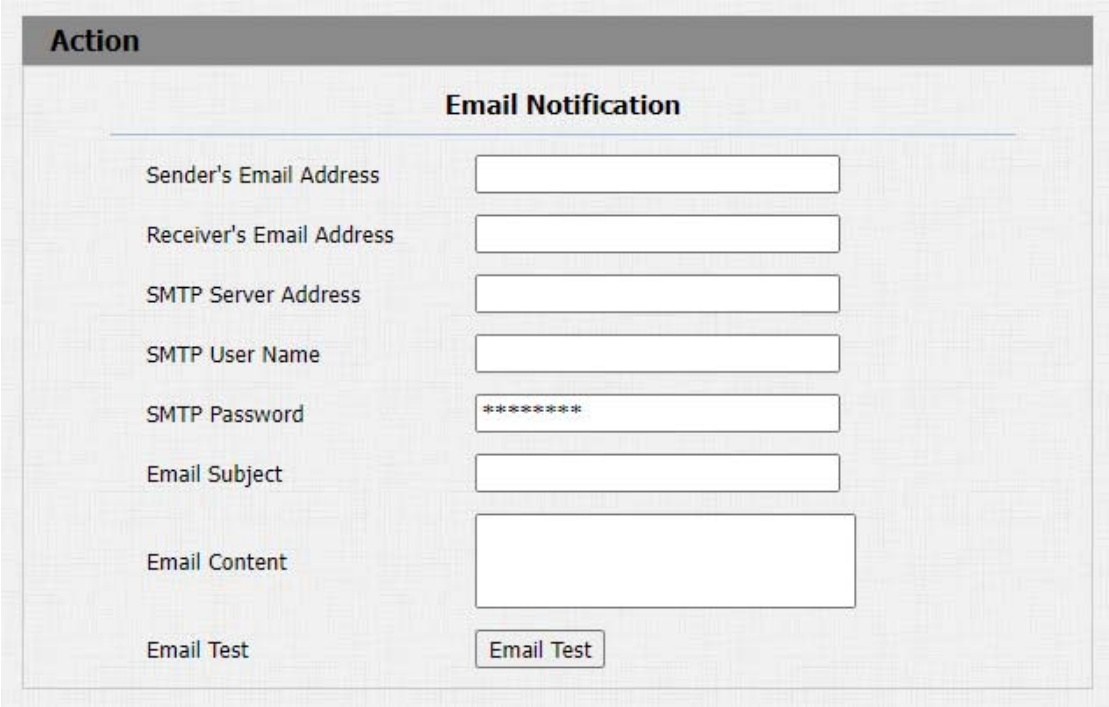
- **Day**: set up the motion detection schedule.

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

16.4. Security Notification Setting

16.4.1. 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.



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 asthe sender's email address.

- **SMTP Password:**configure the password of SMTP service, which is the same as the sender's email address.

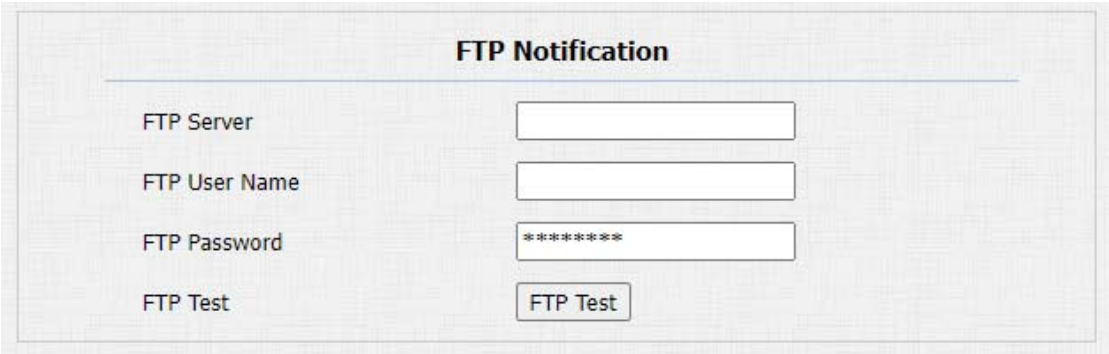
- **Email Subject:** enter the subject of the email.

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

- **Email Test**: click **Email Test** to test if you can receive the Email.

16.4.2. FTP Notification Setting

If you want to receive the security notification via FTP, you can configure the FTP notification on the webIntercom > Action >FTP Notificationproperly.

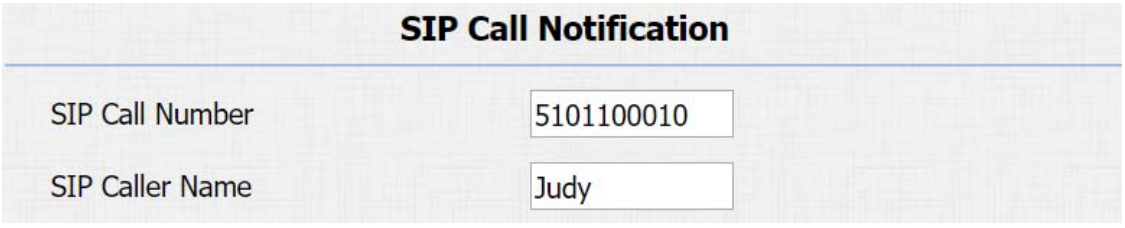


Parameter Set-up:

- FTP Server: enter the address (URL) of the FTP server for the FTP notification.
- FTP User Name: enter the FTP server user name.
- FTP Password: enter the FTP server password.
- FTP Test: run the test to see if FTP notification can be sent and received by the FTP server.

16.4.3. 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.



Parameter Set-up:

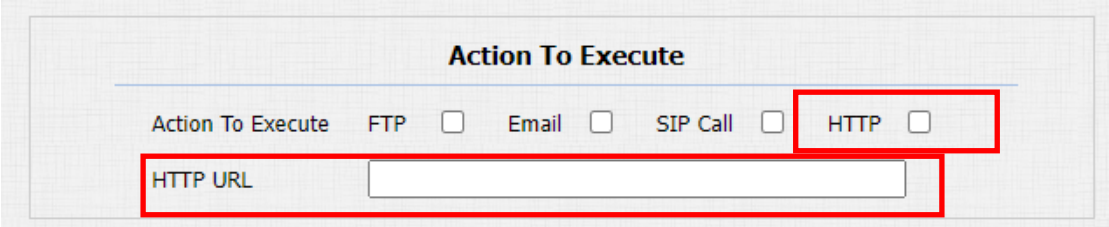
- **SIP Call Number:**to configure SIP call number.

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

16.4.4. HTTP URL Notification Configuration

Akuvox door phone support sending the HTTP notification to the third party when some featuresare triggered. HTTP notification can be setup in specific chapters, please check chapter 15.4. The URL format: **http://http server IP**

address/any information.Refer to: **Intercom > Motion > Action to Execute**.



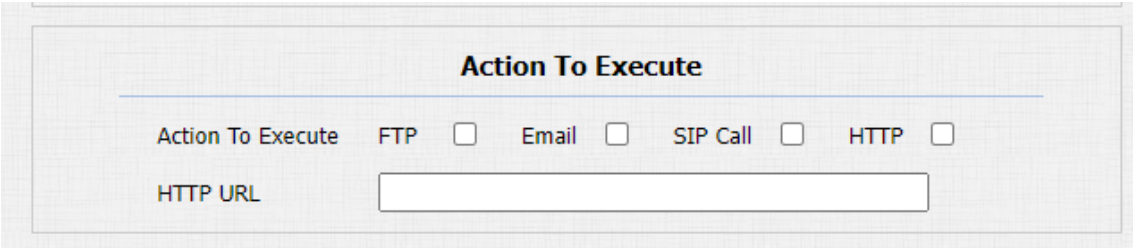
Parameter Set-up:

- **HTTP URL:** tick the check box to enable HTTP URL notification.
- **HTTP URL:**if you choose HTTP mode, enter the URL format:**http://http server IP address/any information**.

16.5. Security Action Configuration

16.5.1. Configure Push Button Action

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

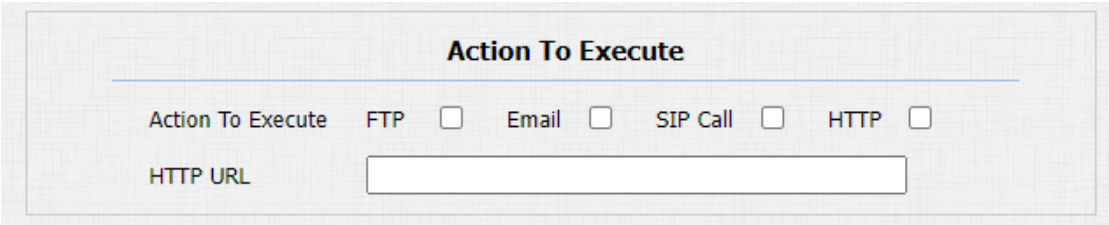


Parameter Set-up:

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

16.5.2. Configure Motion Action

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

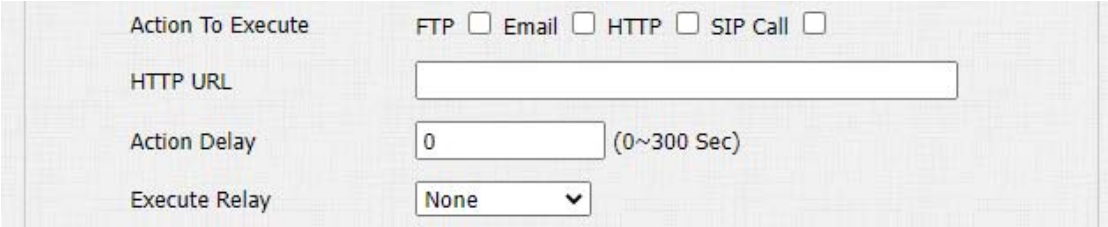


Parameter Set-up:

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

16.5.3. Configure Input Action

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

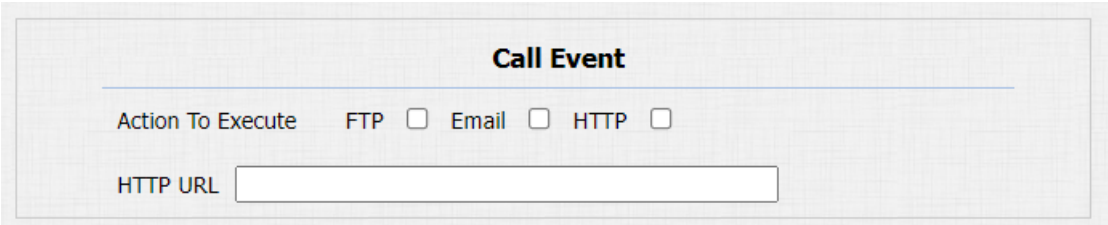


Parameter Set-up:

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

16.5.4. Call Event Notification

If you want to be notified of the call event (call receiving, answering, etc.) navigate to **Intercom > Basic > Call Event**.



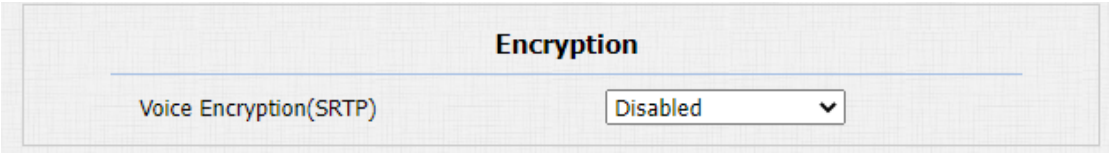
Parameter Set-up:

- **Action To Execute:** select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.

- **HTTP URL:** enter the URL if you select the HTTP to carry out the action.

16.6. Voice Encryption

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

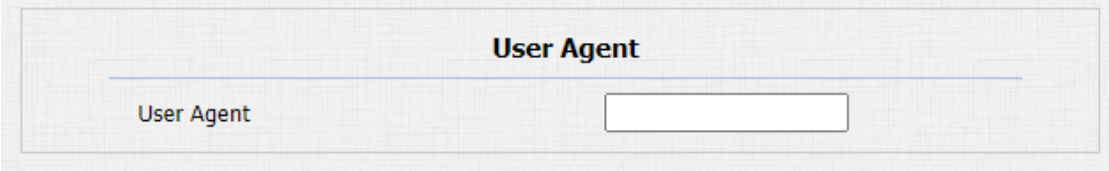


Parameter Set-up:

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

16.7. User Agent

You can customizeuser agent field in the SIP message. If user agent is set to a specific value, users can see the information from PCAP. If user agent is blank, by default, users can see the company name “Akuvox”, model number and firmware version from PCAP. Path: **Account > Advanced > User Agent**.



Parameter Set-up:

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

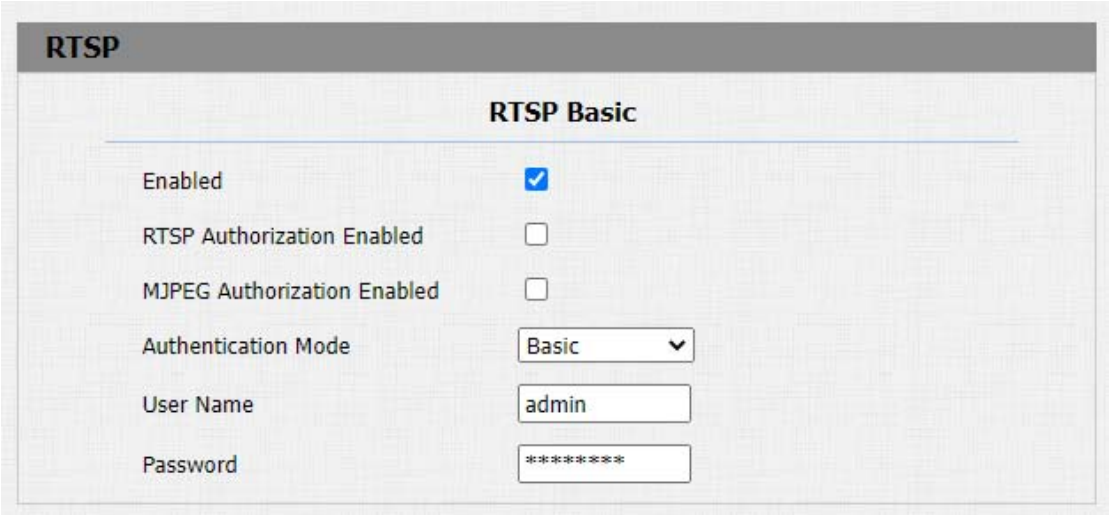
17. Monitor and Image

17.1. RTSP Stream Monitoring

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

17.1.1. RTSP Basic Setting

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



Parameter Set-up:

- **RTSP Server Enable:** click on Enable and Disable in **RTSP Enable** field to turn on or turn off the RTSP function.

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

- **RTSP User Name**: enter the name used for RTSP authorization.

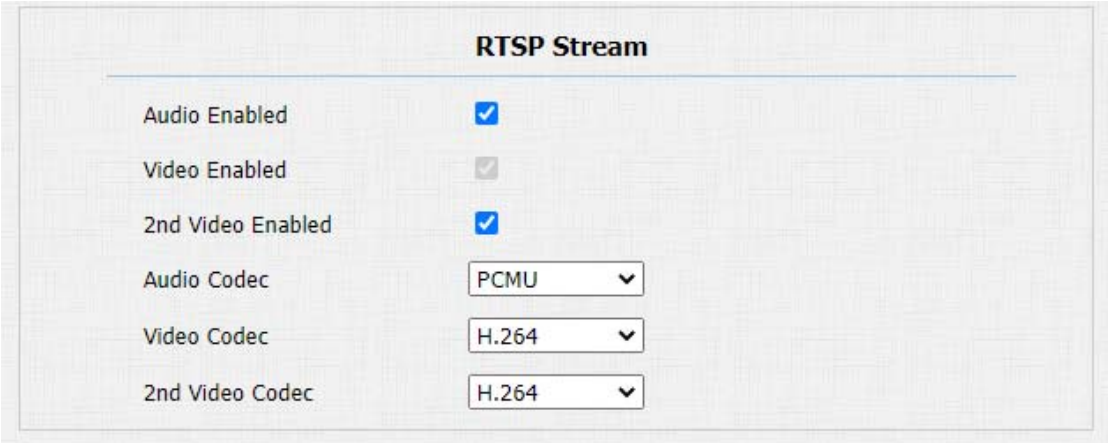
- **RTSP User Password**: enter the password for RTSP authorization.

- **RTSP Authentication Type**: select RTSP authentication type between "**Basic**" and "**Digest**". "**Basic**" is the default authentication type.

17.1.2. RTSP Stream Setting

You can select the video codec format for the RTSP stream for the monitoring and configure video resolution and bit-rate etcbased on your actual network

environment on the webIntercom > RTSP > RTSP stream interface.



Parameter Set-up：

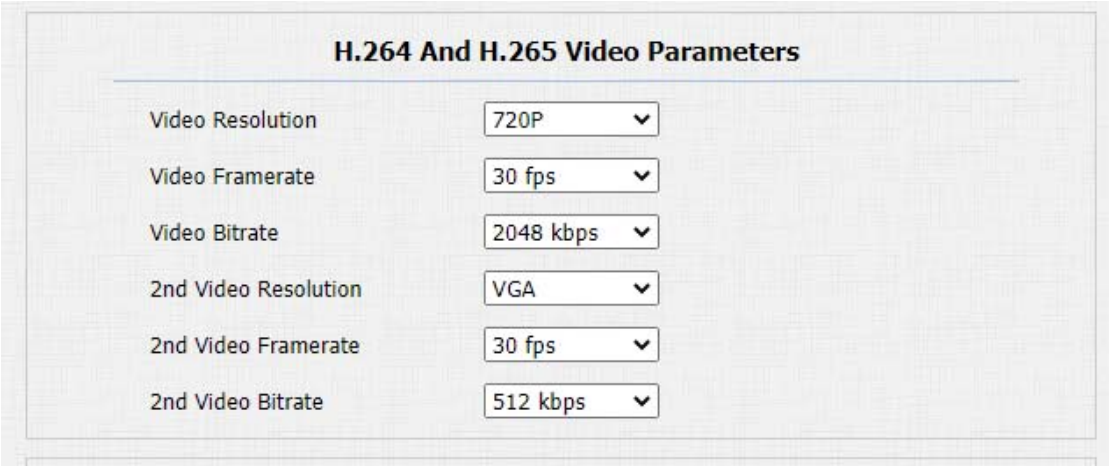
- Audio Enabled: tick to enable RTSP audio which means, the door phone can also send audio information to the monitor by RTSP.

- Video Enabled: the door phone can send the video information to the monitor. After enabling RTSP feature, the video RTSP is enabled by default and can not be modified.

- 2nd VideoEnabled: Akuvox door phones support 2 RTSP streams, you can enable the second one.

- Audio Codec: choose a suitable audio codec for RTSP audio.

- **Video Codec:** choose a suitable video codec for RTSP video.



Parameter Set-up:

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

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

- **Video Bitrate**: select video bit-rate among six options:"**64 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps"** according to your network environment. The default video bit-rate is " **2048 kpbs**".

- **2nd Video Resolution**: select video resolution for the second video stream channel. While the default video solution is "**VGA**".

- **2nd Video 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.

- **2nd Video Bitrate**: select video bitrate among the six options for the second video stream channel. While the second video stream channel is "**512 kpbs**" by default.

17.1.3. NACK

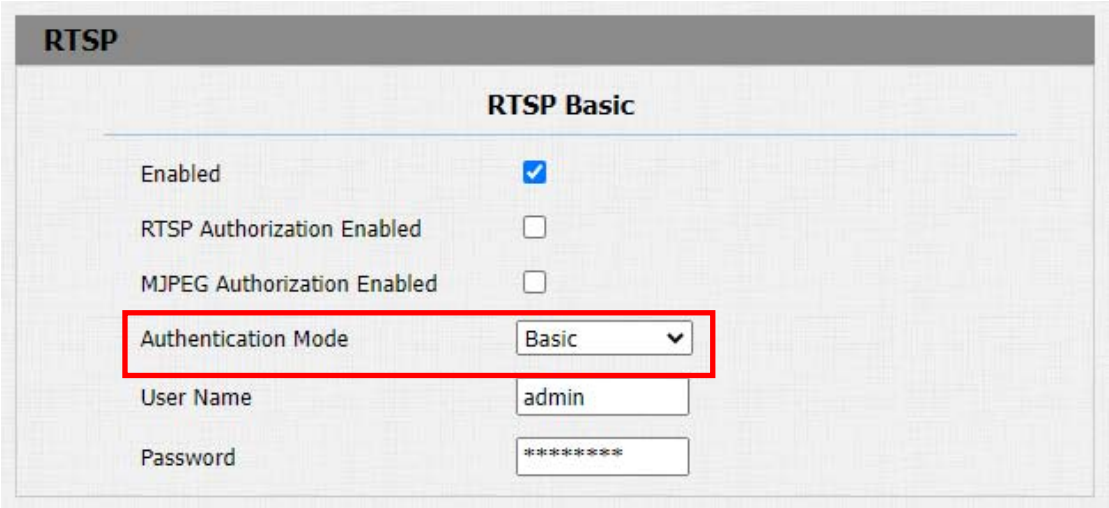
NACK(**Negative Acknowledgement**) is used to ensure the smooth and continued data transmission for the video call. To enable NACK, navigate to **Phone > Call Feature > Others**.

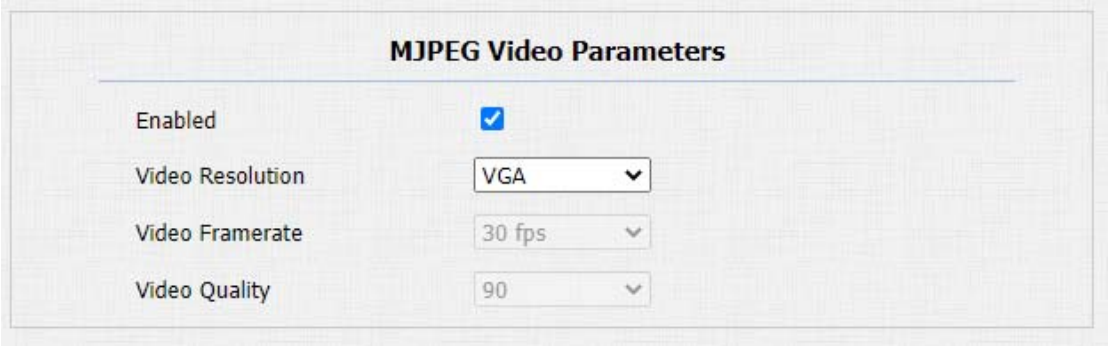
Parameter Set-up:

- **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.

17.2. MJPEG Image Capturing

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





Parameter Set-up:

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

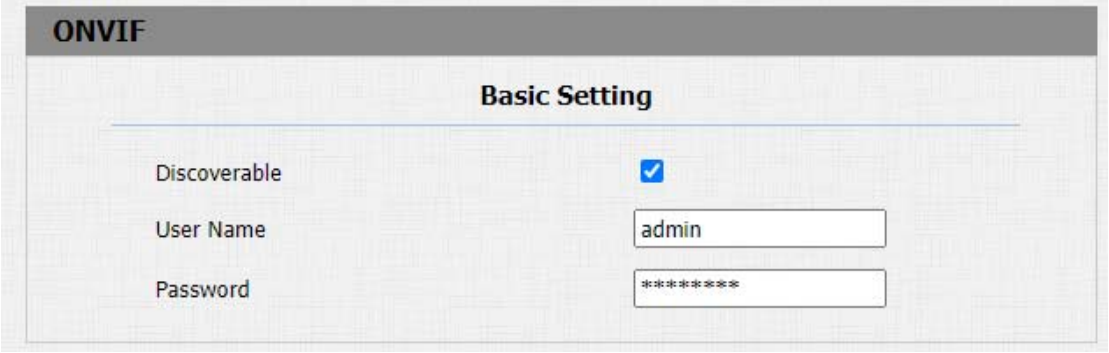
- **Video Resolution:** select video resolutions among seven options: "**QCIF**", "**QVGA**","**CIF**","**VGA**","**4CIF**","**720P**". The default video resolution is "**4CIF**". and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than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

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

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

17.3. 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.



Parameter Set-up:

- **Discoverable:** tick the check box to enable the DiscoverableONVIF mode. If you select "**Discoverable**" then the video from the door phone camera can be searched by other devices.

- **UserName:** enter the user name. The user name is " **admin**" by default.

- **Password**: enter the password. The password is " **admin**" by default.

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

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

Note:

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

17.4. Live Stream

If you want to check the real-time video from the door phone, you can go to the 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.

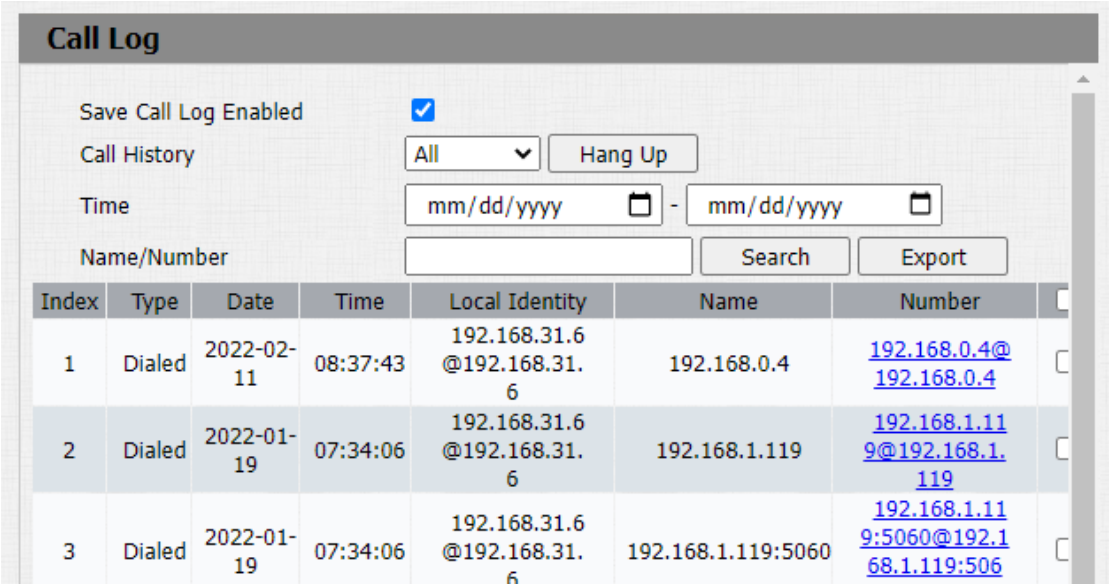
To check the real time video using URL, you canEnter the correct URL (**http://IP_address:8080/video.cgi**) on the web browser if you want to obtain the real-time video directly instead of going to the web interface.

Live Stream

18. Logs

18.1. Call Logs

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



Parameter Set-up:

- **Save Call Log Enabled**:select "**Enable**" or "**Disable**" to turn on or turn off the call log function.

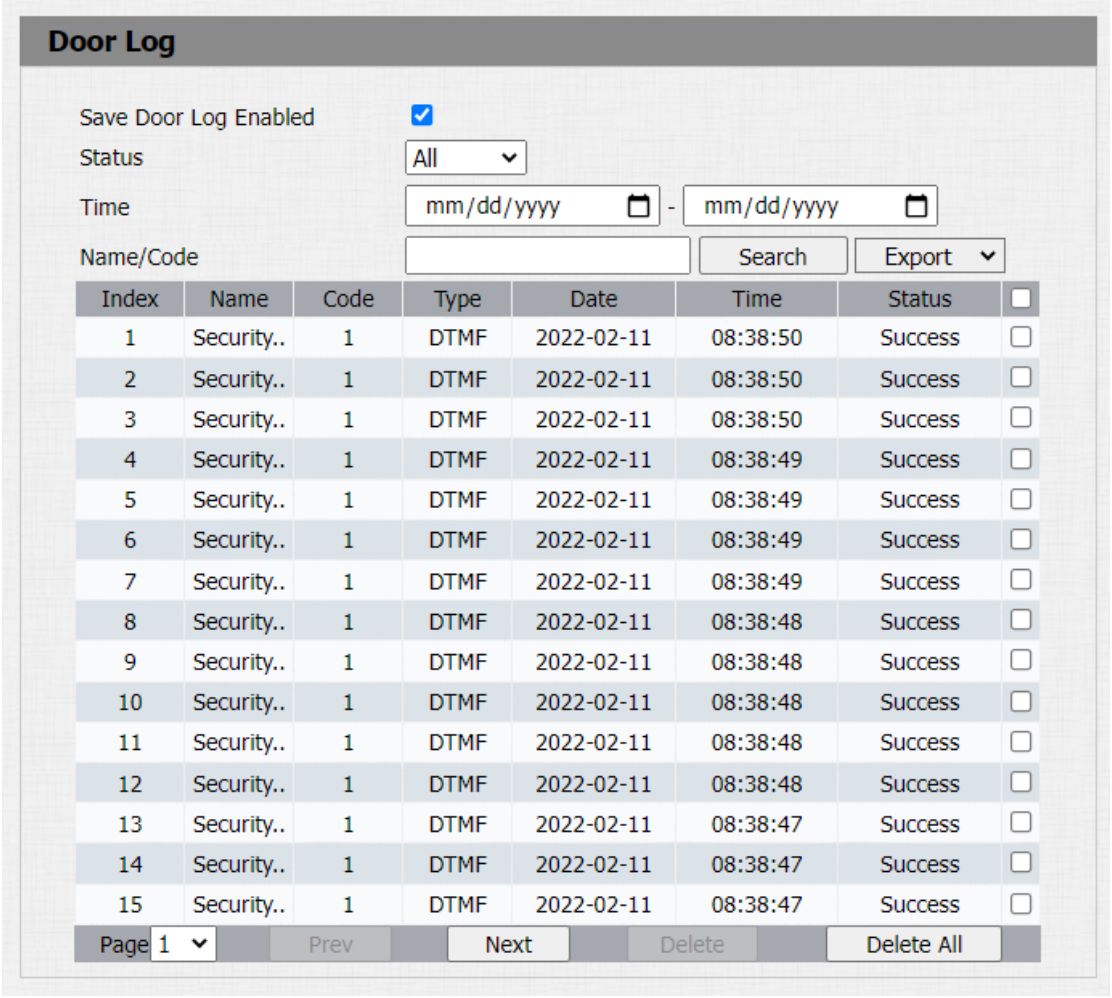
- **Call History**: select call history among four options: "**All**", "**Dialed**" "**Received**" "**Missed**" for the specific type of call log to be displayed.

- **Time**:select the specific time span of the call logs you want to search, check or export.

- **Name/Number**: select the "**Name**" and "**Number**" options to search call log by the name or by the SIP or IP number.

18.2. Door Logs

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



Parameter Set-up:

- **Save Door Log Enabled**:select "**Enable"** or "**Disable"** to turn on or turn off the call log function.

- **Status:** select **"All"** to check all door logs; select "**Success**" to check successfully opened door logs; Select **"Failed"** to check door logs for opening failure.

- **Time**: set the time range for the door logs you want to check.

- **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.

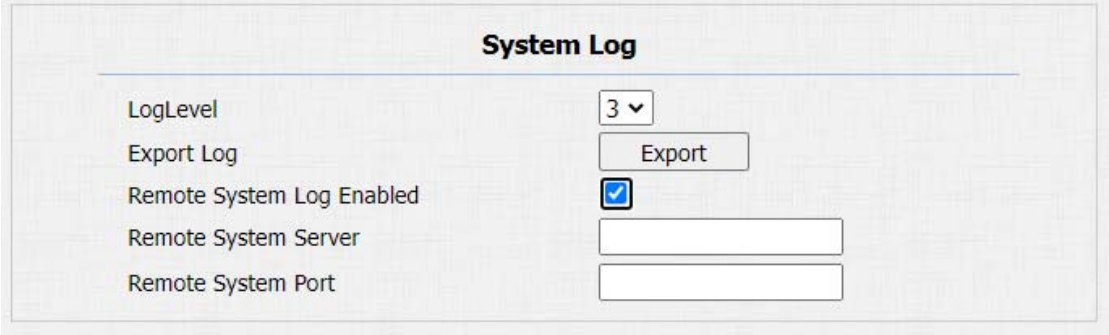
- **Time:** the time for opening the door.

- **Status:** the door opening result **Success** or **Failed.**

19. Debug

19.1. 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.



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.

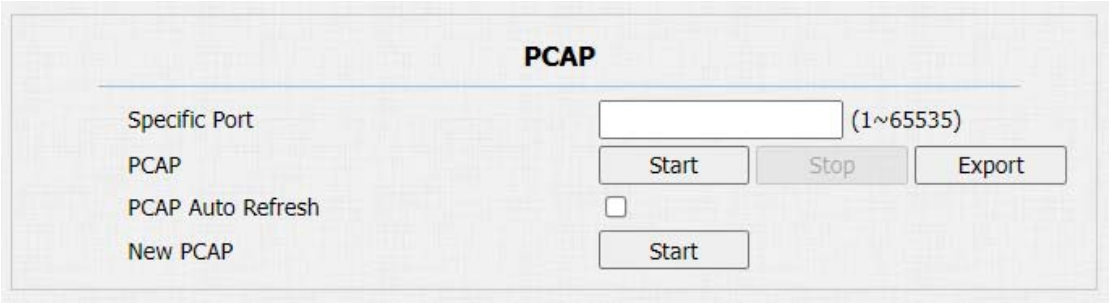
- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.

- **Remote System LogEnabled**: 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.
- **Remote System Port**: enter the port of the remote server.

19.2. PCAP

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



Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.

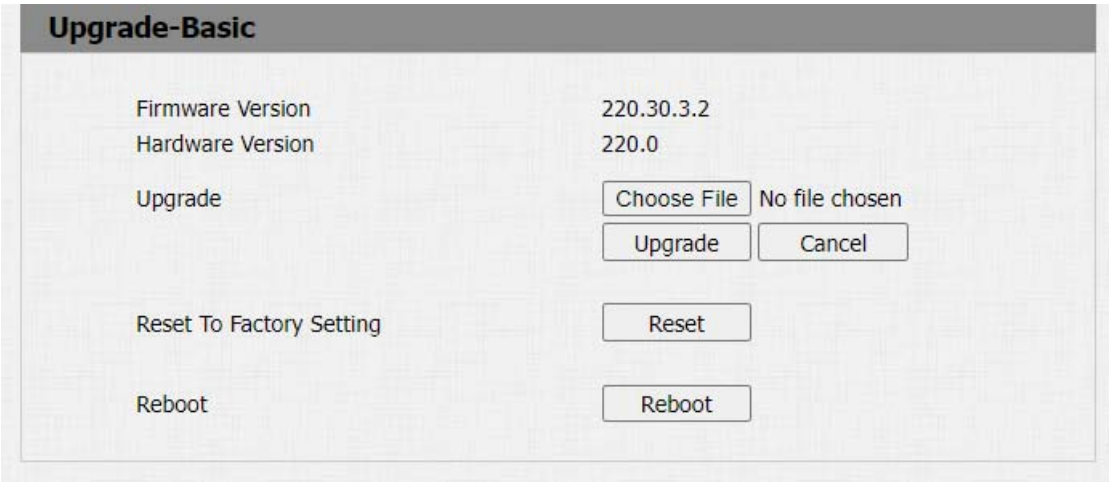
- **PCAP**: click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.

- **PCAP Auto Refresh**: select "**Enable**" or "**Disable**" to turn on or turn off the PCAP auto fresh function. If you set it as **"Enable"** then the PCAP will continue to capture data packets even after the data packets reached their1M 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.

- **New PCAP**:click start to capture bigger data package.

20. Firmware Upgrade

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



Parameter Set-up:

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

Note:

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

21. Backup

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

Parameter Set-up:

- **Export Config File:**to export current config file.

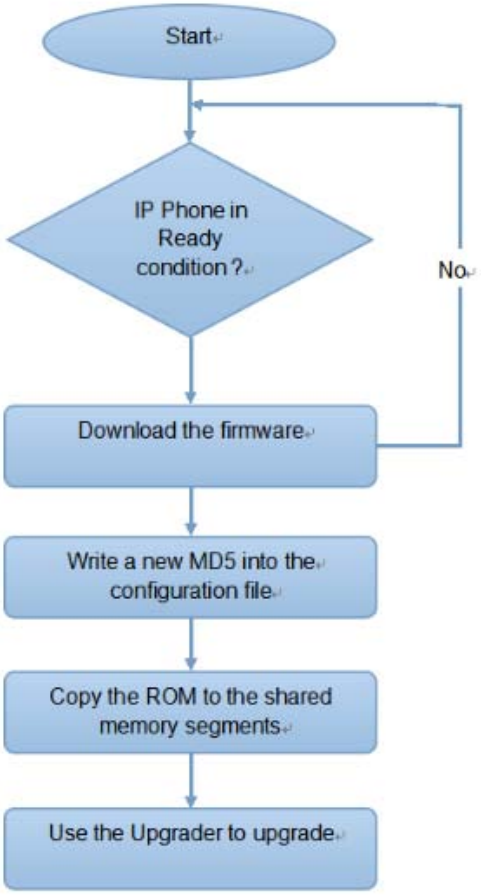
- **Export/Import:**to export current config file (Encrypted) or import new config file.

22. Auto-provisioning via Configuration File

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

22.1. Provisioning Principle

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



22.2. Configuration Files for Auto-provisioning

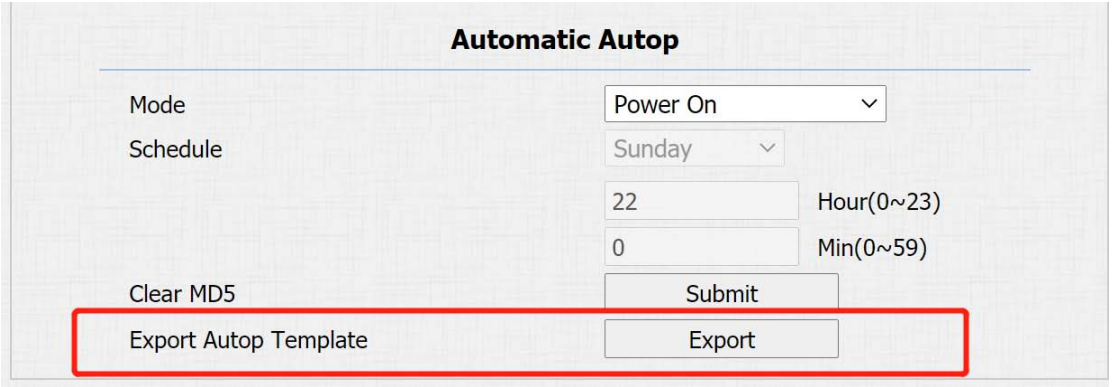
Configuration files have two formats for the auto-provisioning. One is general configuration files used for general provisioning and other one is MAC-based configuration provisioning.

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

- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example：r000000000020.cfg.

- **MAC-based configuration provisioning**: MAC-based configuration files are used for the auto-provisioning on a specific device as distinguished by its unique MAC number. And the configuration files named with device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

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



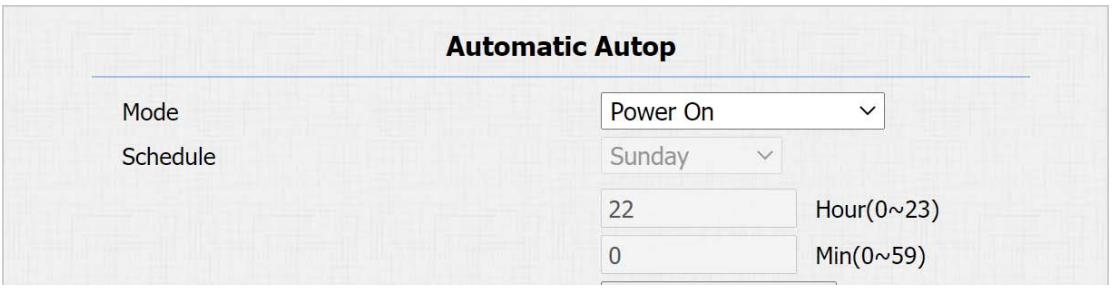
Note:

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

22.3. AutoP Schedule

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

Path:**Upgrade > Advanced > Automatic Autop** interface.



Parameter Set-up:

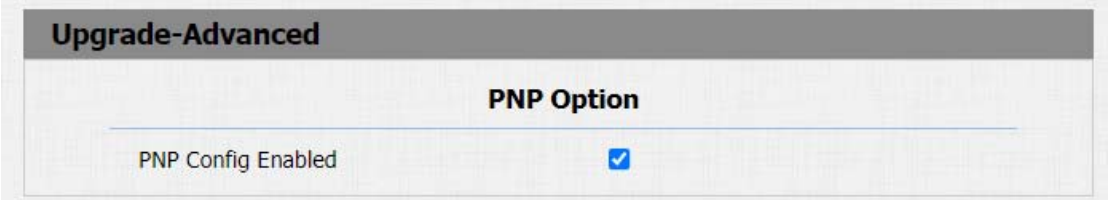
- **Mode:**select "**Power on**", if you want the device to perform Autop every

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

- **Schedule**: if “**Repeatedly**” is selected, you can set up the time schedulefor the AutoP.

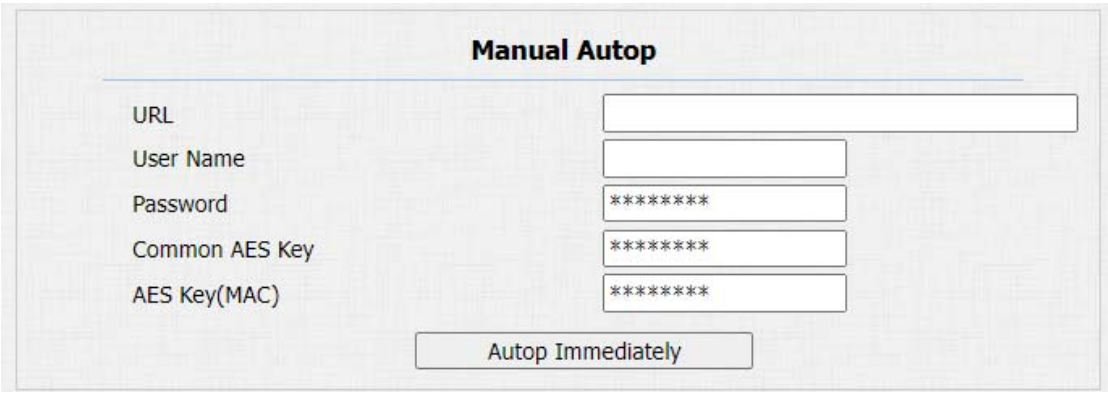
22.4. PNP Configuration

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



22.5. Static Provisioning Configuration

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



Parameter Set-up:

- **URL**: setup TFTP, HTTP, HTTPS, FTP server address for the provisioning

- **User Name**: set up a user name if the server needs a username to be accessed otherwise leave it blank.

- **Password**: set up a password if the server needs a password to be accessed otherwise leave it blank.

- **Common AES Key**: set upAES code for the intercom to decipher the general Auto Provisioning configuration file.

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

Note:

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

Note:

Server Address format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
  ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)

Note:

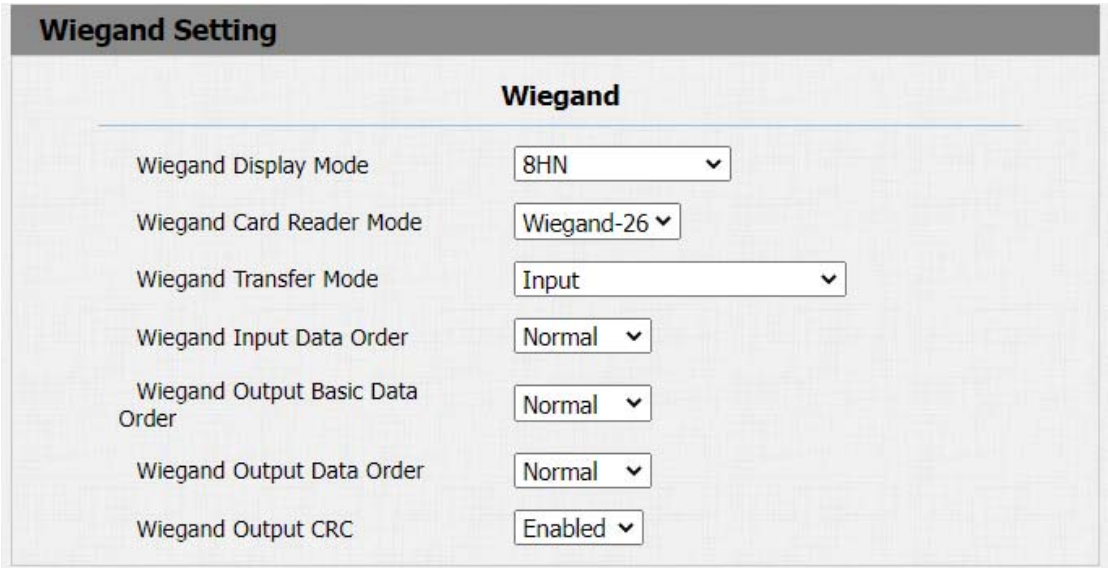
- Akuvox do not provide user specified server.

  Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.**Note:**

23. Integration with Third Party Device

23.1. Integration via Wiegand

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



Parameter Set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among8H10D; 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 binary system.

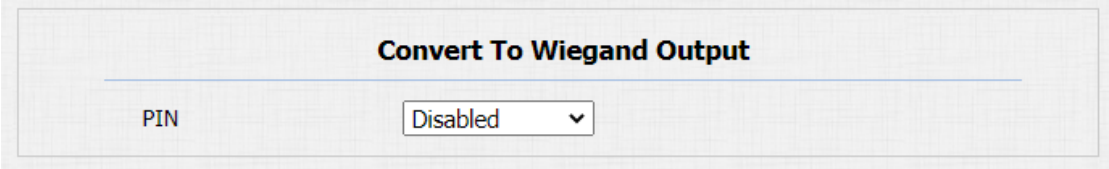
- **Wiegand Input Data Order:** set the Wiegand input data sequence between "Normal" and "Reversed" if you select "Reversed" then the input card number will be reversed and vice versa.

- **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.

You can configure the wiegand output mode if needed. The output occurs

when you press the PIN code on the device.

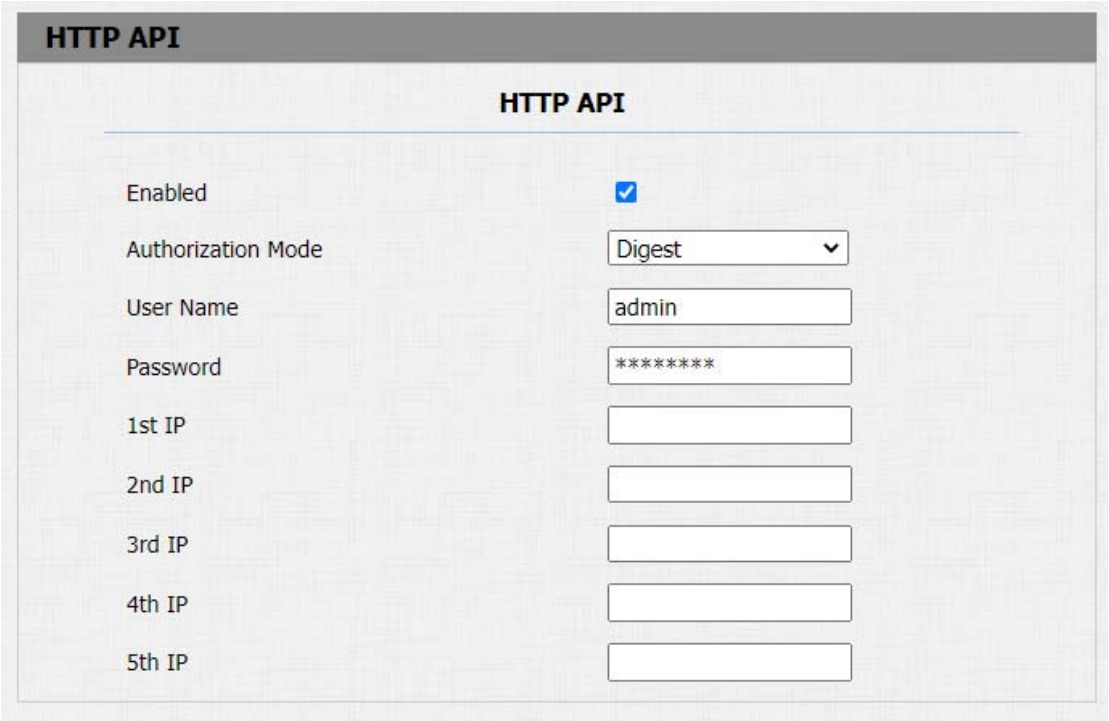


Parameter Set-up:

- **PIN**: select “Disabled” if you want to disable the function. Select “4 bits per digit” of you want to output the PIN code by four continuous bits as a set. Select “8 bits per digit”if you want to output the PIN code by eight continuous bits as a set.

23.2. Integration via HTTP API

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



Parameter Set-up:

- **Enabled:** enable or disable the HPTT API function for the third party integration. For example, if the function is disabled any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.

- **Authorization Mode:** select among four options: **"None" "WhiteList" "Basic", "Digest"** 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".

- **1st IP-5th IP:** enter the IP address of the third party devices when the "WhiteList" authorization is selected for the integration.

Please refer to the following description for the Authentication mode:

NO.	Authorization Mode	Description
1	None	No authentication is required for HTTP API as it is only used for demo testing.
2	Normal	This mode is used by Akuvox developers only.
3	WhiteList	If this mode is selected, you are only required to fill in the IP address of the third party device for the authentication. The whitelist is suitable for operation in the LAN.

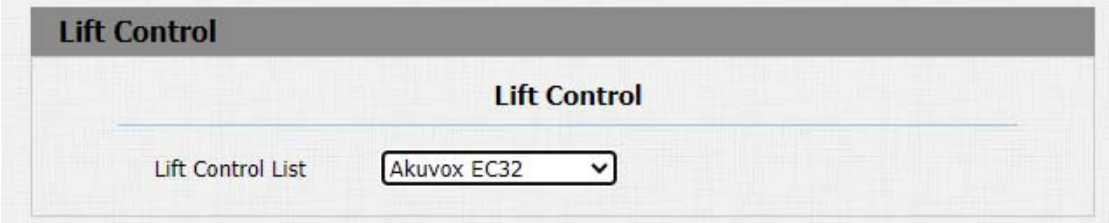
4	Basic	If this mode is selected, you are required to fill in the User name and the password for the authentication.In Authorization field of HTTP request header, use Base64 encode method to encode of username and password.
5	Digest	Password encryption method only supports MD5. MD5(Message-Digest Algorithm) In Authorization field of Http request header: WWW-Authenticate:Digest realm="HTTPAPI",qop="auth,auth-int",nonce="xx", opaque="xx".
6	Token	This mode is used by Akuvox developers only.

23.3. Lift Control Configuration

Integration between the door phone and third party devices such as intercom devices for door access and lift control should be configured in the device web interface before the integration can be made.

Life control should be configured properly on the door phone's web **Intercom >Lift Control>Lift Control List**interface before you can implement the

integration between the door phone and the third party devices.



Parameter Set-up:

- **Life Control List**: select the lift controller brand you need.

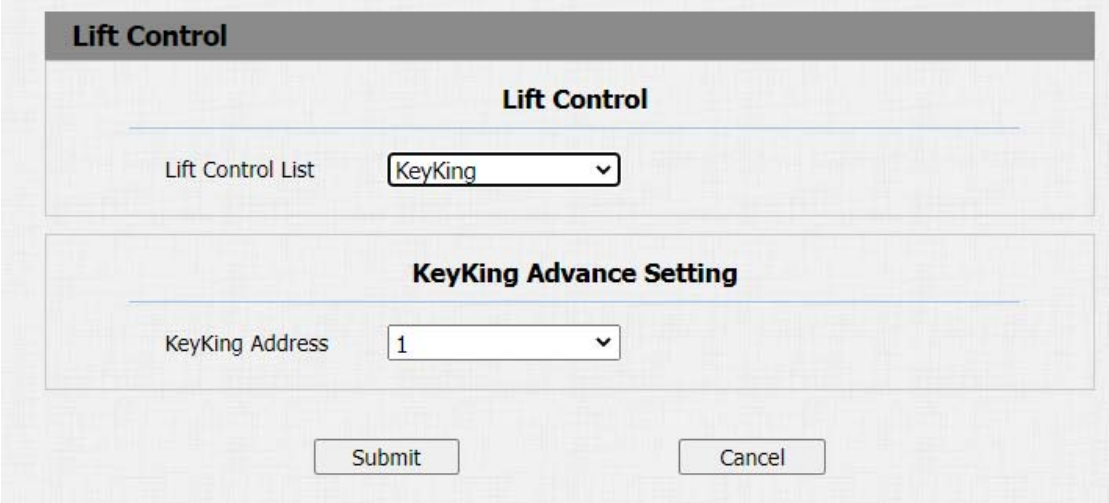
NO.	Integration Mode	Description
1	**None**	If you select "**None**" then the RS485 integration will be disabled.
2	**Akuvox EC32**	Select" Akuvox EC32" if you want to connect the device with Akuvox EC32 lift controller.
3	**KEKING**	Select "KEYKING" if you want to integrate with KEYKING lift controller.
4	**ZKT**	Select "ZKT" if you want to integrate with ZKTeco lift controller
5	**Chiyu**	Select "**Chiyu**" if you want to integrate with **Chiyu** lift controller

Note:

- Please consult with Akuvox technical support if you have any inquiries on the integration mode of any OEM lift controller integration project.

23.4. KeyKing Setting

To integrate KeyKing lift controller, you are required to set up the KeyKing address obtained from your solution provider. You can navigate to Intercom **>Lift Control> KeyKing Advance Setting**.

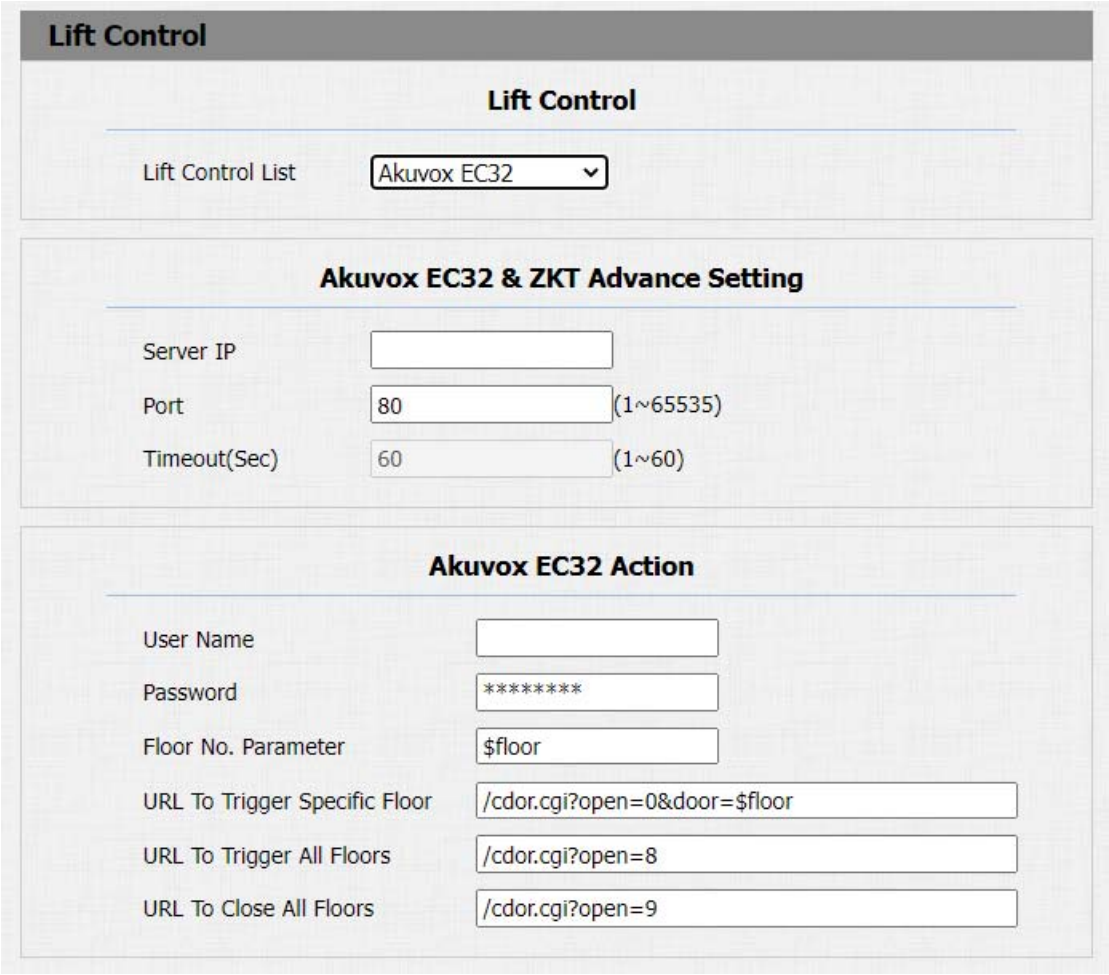


Parameter Set-up:

KeyKing Address: enter the KeyKing address provided by your solution provider. The address number must be identical with the address number on the lift controller board.

23.5. Akuvox EC32 Lift Controller

You are required to configure Akuvox EC32 before you can connect the door phone to the lift controller. You can navigate to **Intercom > Lift Control > Akuvox EC32 & ZKT Advance Setting**.



Parameter Set-up:

- **Server IP**:enter the IP address of the Akuvox EC32 controller server.

- **Port:** enter the port of Akuvox EC32 controller server.

- **Timeout (Sec):** enter the lift controller timeout. For example, if you set the timeout as “30 seconds” have to press the lift button corresponding to the floor you are going to within 30 seconds, otherwise, the button will be locked again, and you have to go out of the lift and do it all over again.

- **User Name:** enter the user name of the lift controller for the authentication.

- **Password:** enter the password of the lift controller for the authentication.

- **Floor NO. Parameter:** enter the Floor number parameter provided by Akuvox. The default parameter string is “**$floor**”. You can define your own parameter string if needed.

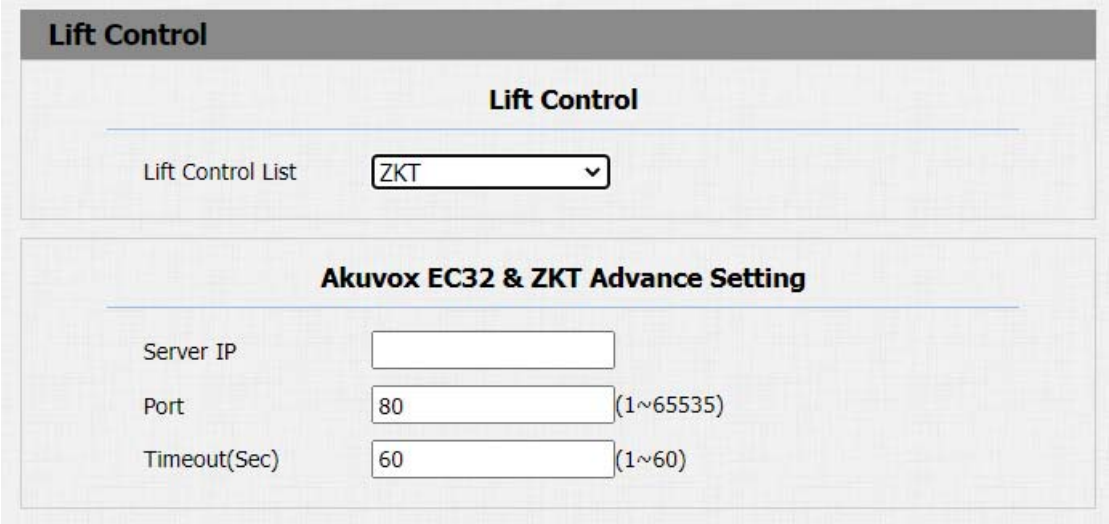
- **URL To Trigger Specific Floor:** enter the Akuvox life control URL for triggering a specific floor. The URL is “**/cdor.cgi?open=0&door=$floor**”, but the string “$floor” at the end must be identical with the parameter string you defined.

- **URL To Trigger All Floors:** enter the Akuvox URL for triggering all floors.

- **URL To Close All Floors:** enter the Akuvox URL used for closing all floors.

23.6. ZKTLift Controller

You are required to configure ZKteco lift controller before you can connect the door phone to the lift controller. You can navigate to **Lift Control > Akuvox EC32 & ZKT Advance Setting**.



Parameter Set-up:

- **Server IP**:enter the IP address of the Akuvox EC32 controller server.

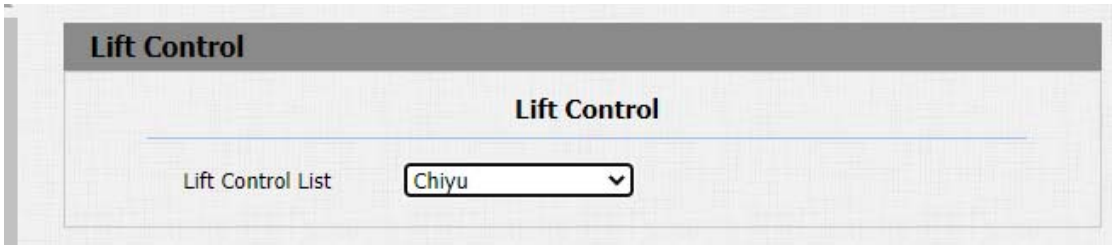
- **Port:** enter the port of Akuvox EC32 controller server.

- **Timeout (Sec):** enter the lift controller timeout. For example, if you set the

timeout as “30 seconds” have to press the lift button corresponding to the floor you are going to within 30 seconds, otherwise, the button will be locked again, and you have to go out of the lift and do it all over again.

23.7. Chiyu Lift Controller

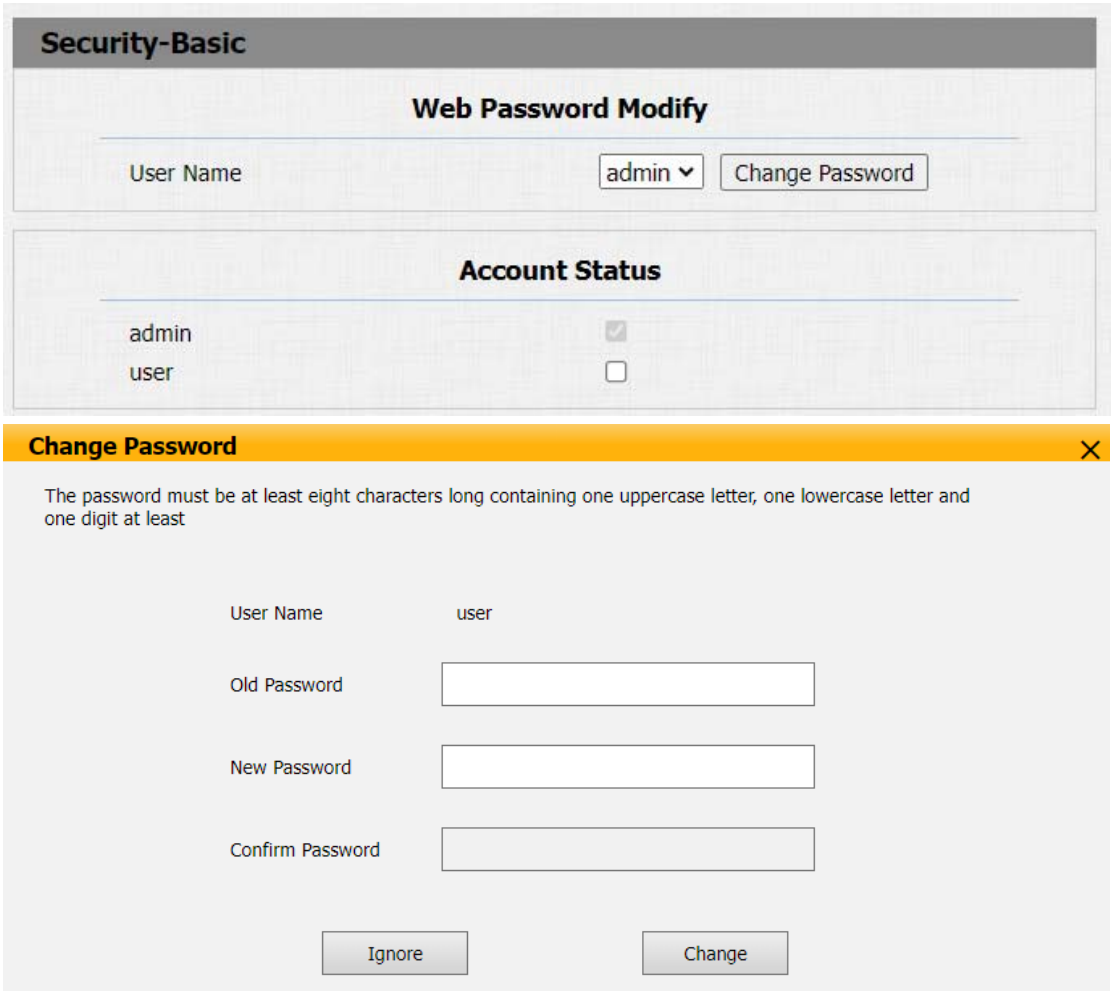
You need to select Chiyu lift controller to integrate with Chiyu lift controller. You can navigate to **Intercom > Lift Control**.



24. Password Modification

24.1. Modifying Device Web Interface Password

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



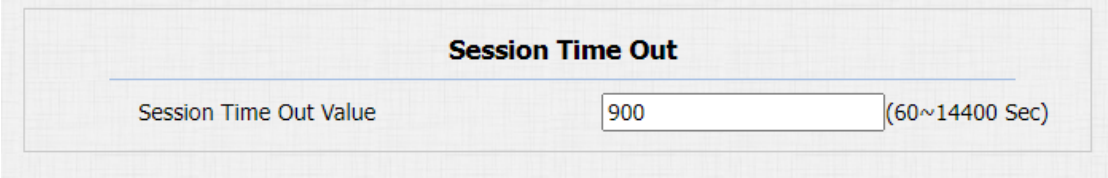
Parameter Set-up:

- **User Name:**modify the Admin or user password if needed.

- **User:** enable the user account if needed.

24.2. Configure Web Interface Automatic Logout

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



Parameters Set-up:

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

25. System Reboot&Reset

25.1. Reboot

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

25.2. Reset

If you want to reset the device system to the factory setting, navigate to the webUpgrade > Basicinterface.

26. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

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

SNMP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

27. FAQ

Q1: How to obtain IP address of R2X

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

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

✓ For devices with multiple numeric keyboard - R27:

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

✓ For devices with touch screen - X915/R29:

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

✓Common method:

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

Q2: Do Akuvox devices support opus codec?

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

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

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

R27/X915 with heating supporting --- 40 degrees

R28 -- (-40°C~55°C)

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

IPPhone -- 32º~104ºF(0~40ºC)

Q4: Do Akuvox devices support Modbus protocol?

A4: No.

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

A5: Please confirm the following steps：

The import format is zip;

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

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

A6: Onvif 18.04 profiles

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

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

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

A8: 1.Label

- **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.

28. Contact us

For more information about the product, please visit us atwww.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.