Akuvox Smart Intercom

Akuvox R20B Series Door Phone Admin Guide

Version：V 1.0

Date： 202009

About This Manual

Thank you for choosing Akuvox's R20B series (this series includes R20BX5, R20BX4, R20BX3 and R20BX2) door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to hardware 220.0 and firmware 220.30.1.105 version, and it provides all the configurations for the functions and features of R20B series door phone. Please note that for a better understanding, our software does not distinguish between models, and they are displayed as R20B. Please visit Akuvox official website or consult Akuvox technical team for any new information or latest firmware.

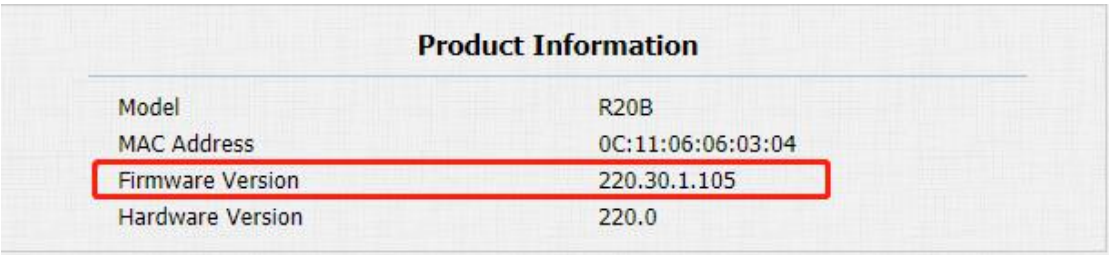
Content

1. Product Overview

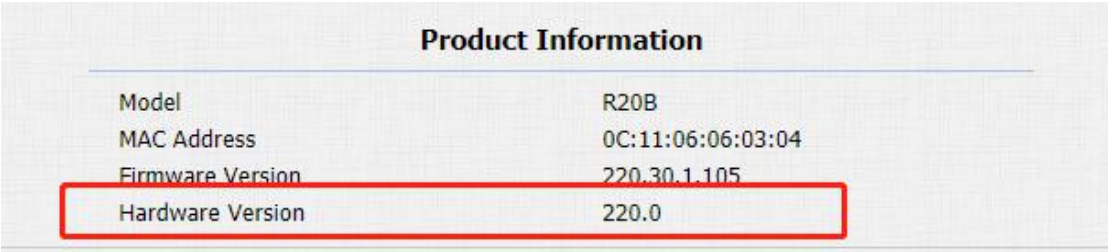
The security that comes with being able to control who comes into your building along with the ability to verbally and visually confirm their identity is immeasurable. Akuvox R20B is a SIP-compliant, hands-free and video door phone. It can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. Akuvox's Video Doorphone R20B enables you to easily monitor an entrance door or gate and gives you the peace of mind knowing that your facility is more secure.

2. Version

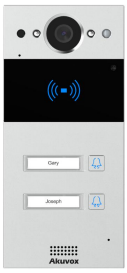
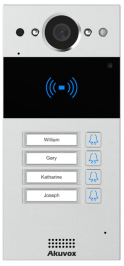
This manual applies to hardware 2.0 and firmware 220.30.1.105 version. Please check the firmware version in website Status - Basic.



Please check the hardware version in website Status - Basic or the label in the back cover.



3. Model Difference

Feature /Model	R20BX2	R20BX3	R20BX4	R20BX5
Picture				
Display	X	X	X	X
Touch Screen	X	X	X	X
Button	2 Physical button	3 Physical buttons	4 Physical buttons	5 Physical button

Housing Material	Aluminum alloy	Aluminum alloy	Aluminum alloy	Aluminum alloy
Relay In	2	2	2	2
Relay Out	2	2	2	2
Alarm In	X	X	X	X
RS485	√	√	√	√
POE	√	√	√	√
Wiegand	optional	optional	optional	optional
Reset button	X	X	X	X
SIP	√	√	√	√
Operating System	Linux	Linux	Linux	Linux
RAM	128MB	128MB	128MB	128MB
ROM	16MB	16MB	16MB	16MB
Card Reader	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ	13.56MHZ & 125KHZ
Camera	3 Mega pixels, automatic lighting	3 Mega pixels, automatic lighting	3 Mega pixels, automatic lighting	3 Mega pixels, automatic lighting
ONVIF	√	√	√	√
Wi-Fi	X	X	X	X
Blueto oth	X	X	X	X
PIN / Card Entry	Card Entry	Card Entry	Card Entry	Card Entry
QR code Entry	X	X	X	X
NFC	√	√	√	√
IP Rating	IP65	IP65	IP65	IP65
Temper	X	X	X	X

ature detecti on				
Face recogni tion	X	X	X	X
LTE	X	X	X	X
HDMI	X	X	X	X
USB	X	X	X	X
Extren al SD card	X	X	X	X
Wall Mounti ng	√	√	√	√
Flush Mounti ng	√	√	√	√
Desk Mounti ng	X	X	x	X
Wall Mounti ng DIM	185x85x24m m	185x85x24mm	185x85x24mm	185x85x24mm
Flush Mounti ng DIM	226x108x52 mm	226x108x52mm	226x108x52m m	226x108x52mm
POE standy power	2.3W	2.3W	2.3W	2.3W
POE full load consu mption	6.425W	6.425W	6.425W	6.425W
Power adapter standb y powe	1.9W	1.9W	1.9W	1.9W
Power adapter full load	5.58W	5.58W	5.58W	5.58W

consumption				

4. Introduction to Configuration Menu

4.1. Feature Overview

- **Status:** This section gives you basic information such as product information, Network Information, and account information etc.
- **Intercom**: Intercom call, LED setting, Relay, input control, Live stream, RTSP, ONVIF, motion detection, card setting, etc.
- **Account**: SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer etc.,
- **Network**: DHCP&Static IP setting, RTP port setting, and device deployment etc.,
- **Phone**: Time&language, call feature, dial management, log etc.
- **Access Whitelist:** Phone book management

- **Upgrade:** Firmware upgrade, device reset&reboot, configuration file auto-provisioning, PCAP.
- **Security**: Password modification and certifications

4.2. Mode Selection

- **Discovery mode:** It is a plug and play configuration mode. Akuvox devices will configure themselves automatically when users power on the devices and connect them to network. It is super time-saving mode and it will greatly bring users convenience by reducing manual operations. This mode requires no configurations previously by the administrator.
- **Cloud mode:** Akuvox Cloud is an all-in-one management system. Akuvox Cloud is the mobile service that allows audio, video, remote access control between smart phones and Akuvox intercoms. All configurations in the device will be issued automatically from cloud. If users decide to use Akuvox cloud, please contact Akuvox technical support, and they will help you configure the related settings before using.
- **SDMC mode:** SDMC (SIP Device Management Controller) is a simple and comprehensive software for building management. It provides a visuable topograph for a community while offering you a graphical configuration interface for the door access, intercom, monitoring, alarm etc.,. It is a convenient tool for property manager to manage , operate and maintain the community.

4.3. Tool Selection

Akuvox has many configuration tools for you to set up devices more conveniently. Here we list the common tools, please contact Akuvox technical

team to get the tool if you need it.

- **SDMC:** SDMC is short for SIP Device Management center, which is suitable to manage Akuvox devices in a large community, including access control,resident information, remote device control and information expression.
- **Akuvox Upgrade Tool:** Upgrade Akuvox devices in batch in the LAN.
- **Akuvox PC Manager:** Distribute all configuration items in batch in the LAN.
- **IP scanner:** it is used to searching Akuvox device IP addresses in the LAN

5. Phone Configurations

5.1. Device Login

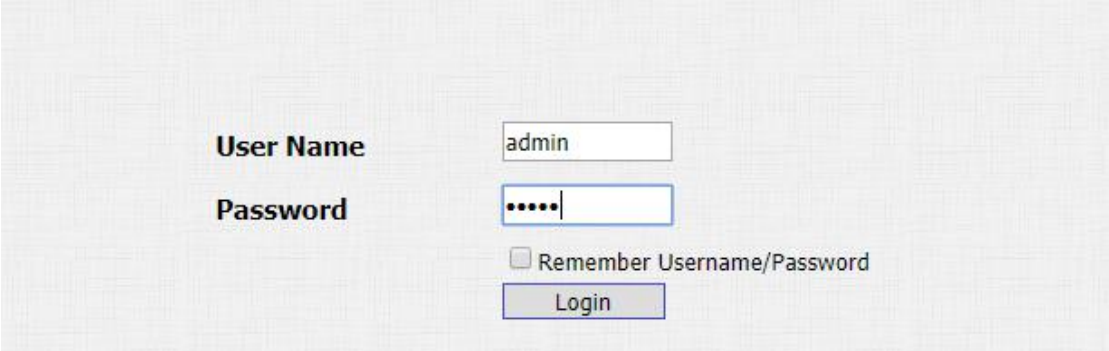
5.1.1. Access the Device Web Interface Setting

You can enter the device IP address on the web browser in order to log in the device web interface where you can configure and adjust parameter etc., if needed.

To do so, you can do as follows:

1. Check the Device IP address by holding the push button 5s or searching by IP scanner.
2. Enter the IP address on the web browser.
3. Enter the **User Name** and **Password**,the default user name and password is **admin**/**admin**.

4. Press **Login** tab to log in the web interface.



Note:

- **Google Chrome browser is strongly recommended.**
- **User name and password are case sensitive.**

Tip:

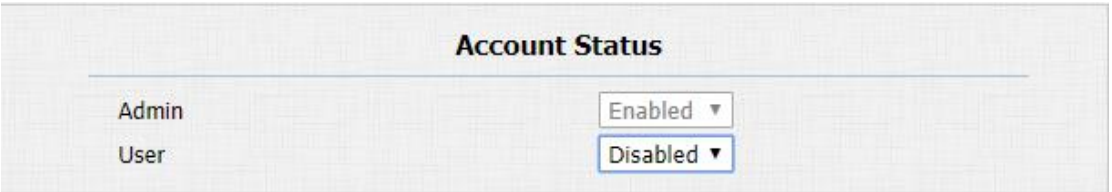
- **You can obtain the device IP address using the Akuvox IP scanner to access the device web interface. Please refer to URL below for the IP scanner application.**

5.1.2. Login Permission

This feature is used to give a login permission for admin or user. Admin authentication is enabled by default and it can not be changed. If you enable user authentication, you can login with username and password as user/user.

To do so, you can do as follows:

1. Click **Security** - **Basic** to find **Account Status**.
2. **Enable** or **Disable** the login permission.
3. Click **Submit** tab to save.



Parameters Set-up:

- **Admin:**This item can only be enabled by default that means you can login with username and password as admin/admin.
- **User:** This item is disabled by default that means you can login with username and password as user/user.

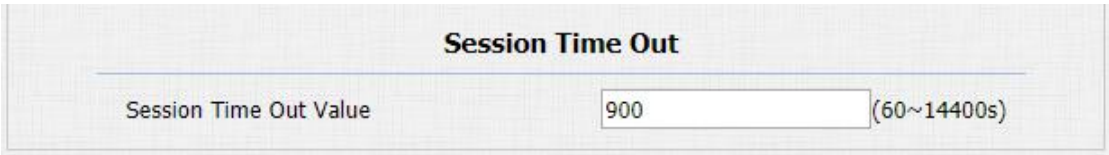
Note:

- **The username and password mentioned below is default value**

5.1.3. Login Time Out

It is a protection design. When there is no operation on the website and the Session Time Out Value time is reached, the website will automatically log out. To do so , you can do as follows:

1. Click **Security - Basic** to find **Session Time Out.**
2. Setup the time value.
3. Click **Submit** tab to save.



Parameters Set-up:

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

5.2. Phone Customization

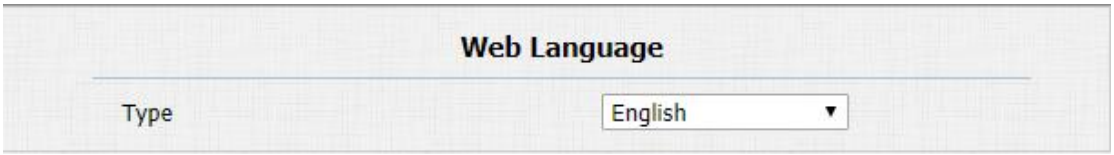
5.2.1. Time&Language Settings

When you first set up the device, you might need to set both the time and language to your need or you can do it later as needed. And the time and language can be either be set up directly on the device web interface.

5.2.1.1. Language Setting

To do so, you can follow the following process

1. Click **Phone - Time/Lang** to find **Web Language**.
2. Select the language you preferred and press **Submit** button to validate the setting.



Parameters Set-up:

- **Type:** R20B only supports English web display.

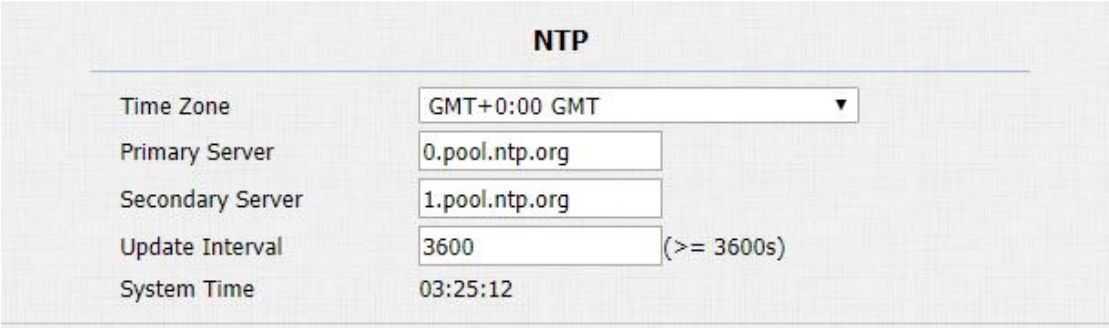
5.2.1.2. Time Settings

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

To do so, you can do as follows:

1. Click **Phone - Time/Lang** to find **NTP**.

2. Enter the NPT server you obtained in the field of the NPT sever.
3. Press the **Submit** button to save the setting and press the **Cancel** button to cancel the setting.



Parameters Set-up:

- **NTP Server:** Enter the NPT server you obtained in the NPT server field.

5.2.2. Infrared LED Setting

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

To do the set-up on the device web interface, you can start with the following process:

1. Click **Intercom** - **Advanced** to find **Photoresistor**.
2. Adjust the parameters and press the **Submit** tab to validate the setting.
3. Click **Read** to confirm the photoresistor value under the current ambient brightness.

Parameters Set-up:

- **Photoresistor Settings:** Set the minimum and maximum photo-resistor value based on the current actual photo-resistor value detected to control the on-off of the LED light. You set the maximum photo-resistor value for the IR LED to be turned on and the minimum value for it to be turned off. While the default Min/Max photo-resistor value is 1500 and 1600 respectively.
- **Threshold:** Refers to the current light intensity indicated by the photo-resistor value. The higher photo-resistor values correspond conversely to the lower light intensity and vice versa (darker). The default photo-resistor value (Threshhold) is 1132, however you can click **Read** several times in order to obtain the actual photo-resistor value in a specific environment (the value fluctuation is about 5), and the value is what you based on to configure the minimum and maximum photo-resistor values.

5.2.3. LED Display Status

LED display adjustment is used to display the light changes of the device in six states - normal(idle), offline, calling, talking and receiving a call. and the user can also judge the current mode of the device through the state of the led.

5.2.3.1. Setup LED Display from Website

To do so, you can follow the following process.

1. Click **Intercom - LED Setting**.
2. Adjust the Color on and blink mode as you need.
3. Click **Submit** tab to save.

The default LED Display Status

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

Parameters set-up:

- **State:** There is five states: **Normal, Offline, Calling, Talking and Receiving**.
- **Color Off:** The default status is **OFF**.
- **Color On:** It can support three color: **Red, Green, Blue.**
- **Blink Mode:** To setup the different blink frequency.

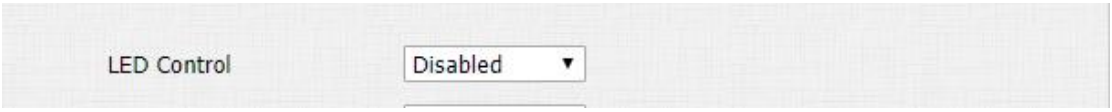
5.2.3.2. Setup LED display from HTTP URL

Use HTTP URL to remote control the LED display status.

To do so, you can follow the following process:

1. Click **Intercom - LED Setting** to find **LED Control**.
2. Enable/disable **LED Control**.

3. Click **Submit** tab to save.



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

Note:

1.The Status and Color off item can not be changed.

2.The LED of upgrading mode can not be adjusted.

5.2.4. 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 prefer not to have the LED light on the card reader area stay on, you can also set the timing for the exact time span during which the LED light can be enabled in order to reduce the electrical power consumption etc.,

To do so , you can follow the following process.

1. Click **Intercom** - **LED Setting** to find **LED Control**.
2. Set the parameter and press **Submit** button to validate the setting.

Parameters Set-up:

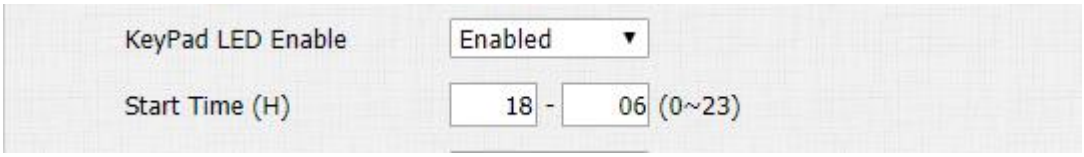
- **Card LED enable:** Click to enable or disable the card reader LED lighting.
- **Start Time (H):** Enter the time span for the LED lighting to be valid. Eg. If the time span is from 18-06 it means LED light will stay on during the time span from 6:00 pm to 6:00 am during a day.

5.2.5. LED Setting on Keypad Area

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

To do so , you can follow the following process:

1. Click **Intercom** - **LED Setting** to find **LED Control**.
2. Set the parameter and press **Submit** button to validate the setting.



Parameters Set-up:

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

5.2.6. Voice Configuration

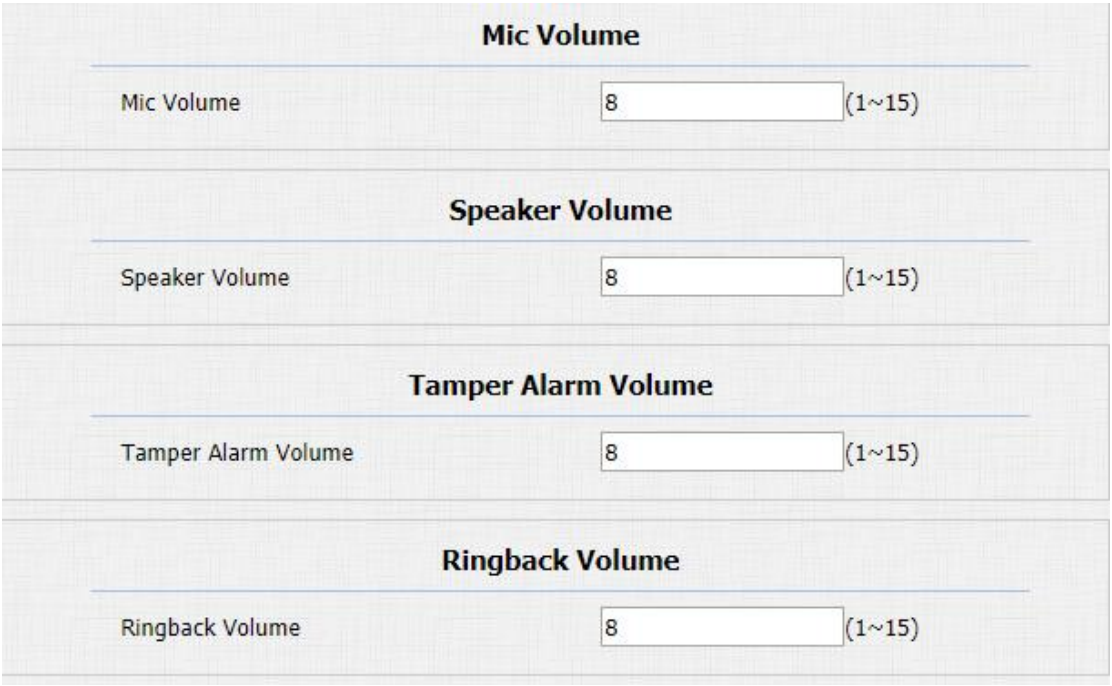
Volume and Tone configuration in R20B refers to the Mic volume, the speaker volume, tamp alarm volume, ring back volume and IP announcement volume and open door tone configuration. More over, you can upload the tone you like

to enrich your personalized user experience.

5.2.6.1. Volume Configuration

To set up the volumes, you can start with the following process:

1. Click **Phone - Voice**.
2. Enter the volume value in **Volume** field ,1 is minimum, 15 is maximum.
3. Click **submit** Tab for confirmation.



Parameters Set-up:

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

5.2.6.2. Open Door Tone Configuration

You can not only enable or disable the Open Door Tone but also controls the prompt words that accompanies the tone.

To enable or disable the open door tone, you can do as follows:

1. Click **Intercom** - **Voice**.
2. Select **Enable/Disable** in the Open Door field.
3. Press **Submit** Tab to validate the setting.

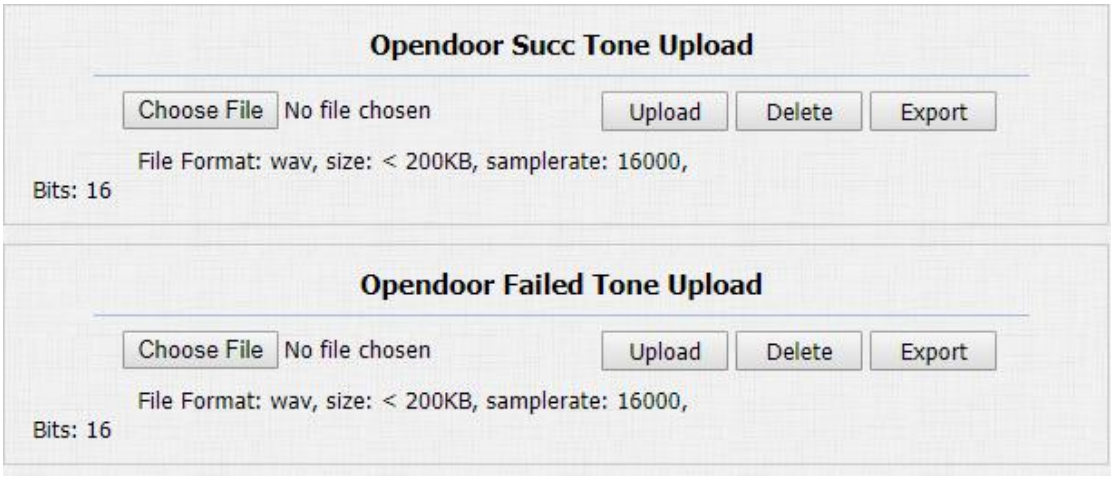
Parameters Set-up:

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

5.2.6.3. Upload Open Door Tone

To upload open door success or failed tone, you can start with following process:

1. Click **Phone** - **Voice**.
2. Click **Choose File** tab to upload the .wav files you selected to the device.
3. Click **Upload** Tab to import the .wav file.
4. Click **Export** Tab to export the existed voice file.
5. Click **Delete** Tab to remove the existed voice file.
6. Press **Submit** tab to validate the setting.



5.2.6.4. Upload Ring Back Tone

To upload ringback tone, you can start with following process:

1. Click **Phone - Voice**.
2. Click **Choose File** tab to upload the .wav files you selected to the device.
3. Click **Upload** Tab to import the .wav files.
4. Click **Export** Tab to export the existed voice file.
5. Click **Delete** Tab to remove the existed voice file.
6. Press **Submit** tab to validate the setting.

5.3. Network

5.3.1. Device Network Connection Setting

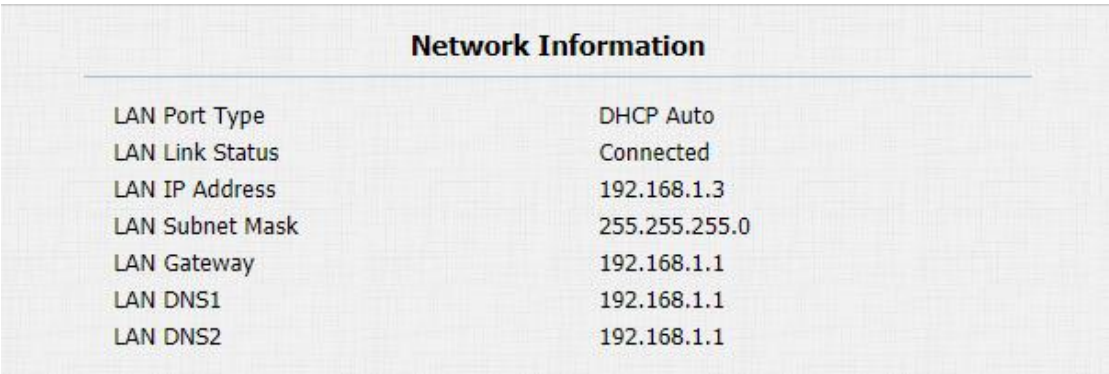
You can check for the door phone's network connection info and configure the

default DHCP mode and static IP connection for the device on the device web interface.

5.3.1.1. Network Status

To check the network status on the web interface, you can do as follows:

1. Click **Status** to find **Network Information**.
2. Check for the network information for the device.



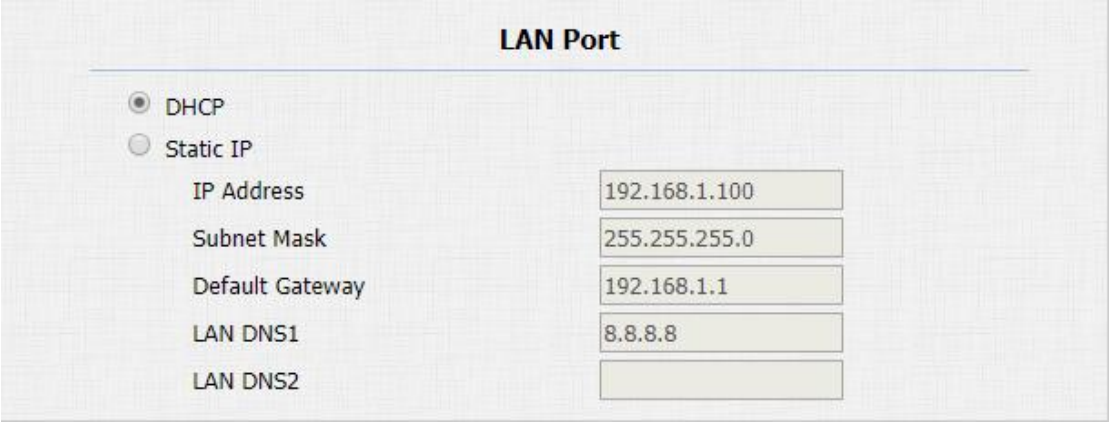
Parameters Set-up:

- **DHCP**: Select the **DHCP** mode (**Dynamic Host Configuration Protocol)** by checking the DHCP box. DHCP mode is the default network connection. If the DHCP mode is selected, then the door phone will be assigned by the DHCP server with IP address, subnet mask,default gateway,and DNS servers address automatically.
- **Static IP**: Select the Static IP mode (**Internet Protocol**) by checking off the DHCP square 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
- **Default Gateway**: set up the correct gateway default gateway according to your actual network environment.
- **LAN DNS1/DNS2**: Set up DNS1/ DNS2 (**Domain Name Serve**r)according to your actual network environment.

5.3.1.2. Network Mode Configuration

To check and configure network connection on the device web interface, you can start with following process:

1. Click **Network - Basic**.
2. Select **DHCP** mode or **Static IP** mode by clicking their respective square box.
3. Set up the parameters in the exact the same way as you do for the set-up on the device.
4. Click **Submit** tab to validate the setting or **Cancel** tab to cancel the setting.



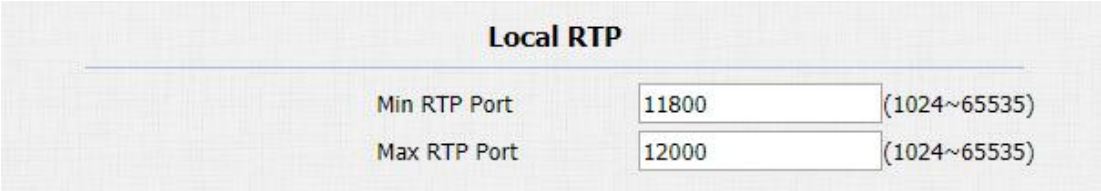
5.3.2. Device Local RTP configuration

For the device network data transmission purpose, device needs to be set up with a range of RTP port for establishing an exclusive range of data transmission in the network.

To set up device local RTP, you can start with following process:

1. Click **Network** - **Advanced** - **Local RTP**
2. Set the **Starting RTP port** to establish the (start point) for the data transmission within the range from 1024 -65535.
3. Set the **Max RTP Port** to establish the (End point) for the data transmission

within the range from 1024 -65535.



Parameters Set-up:

Starting RTP Port: Enter the Port value in order to establish the start point for the exclusive data transmission range.

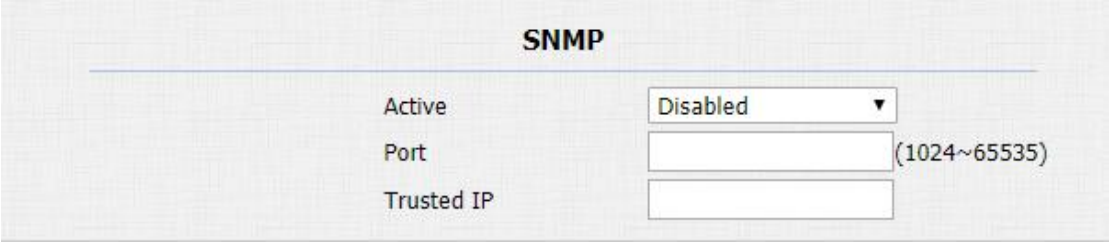
Max RPT Port: Enter the Port value in order to establish the end port for the exclusive data transmission range.

5.3.3. Device SNMP Configuration

SNMP (Simple Network Management Protocols) is Internet-standard protocol for managing devices on IP networks. It is an application layer protocol. With this feature, our intercom can be easily integrated with other 3rd party management system.

To do so, you can do as follows:

1. Click **Network - Advanced** to find **SNMP**.
2. Enter the parameters and click **Submit** tab to save.



Parameters 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.

Note:

The port and IP address value is provided by SNMP server.

5.3.4. Device VLAN Configuration

VLAN（Virtual Local Area Network）makes the device under different router work as in the same local area network. In this way, VLAN can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

To do so, you can do as follows:

1. Click **Network - Advanced** to find **VLAN**.
2. Enter the parameters and click **Submit** to save.

Parameters Set-up:

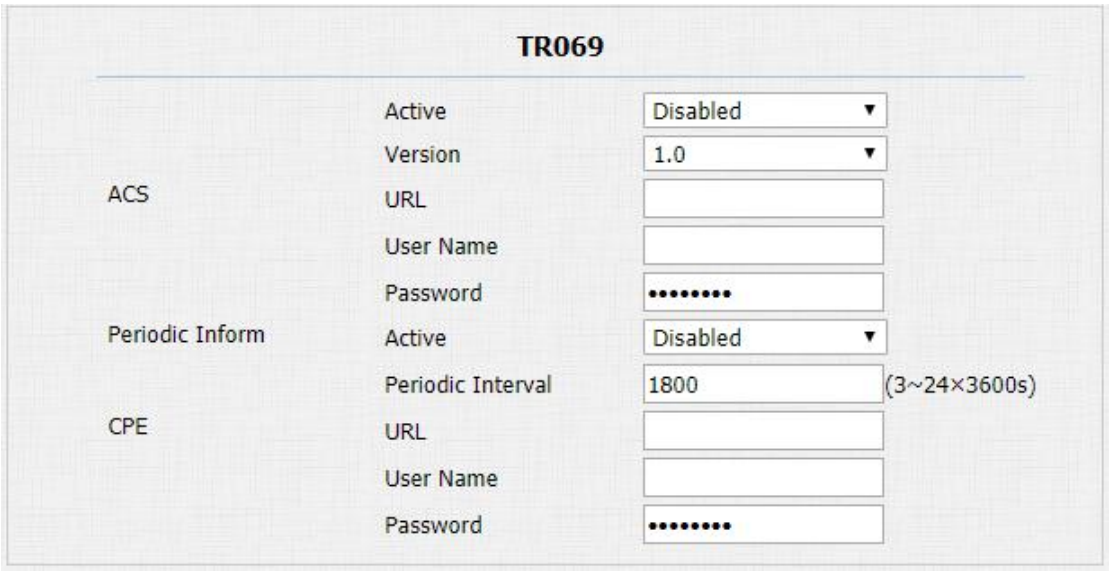
- **Active:** To enable or disable VLAN feature for designated port,disable by default.
- **VID:** To configure VLAN id for designated port，range from 1- 4094.
- **Priority:** To select VLAN priority for designated port，range from 0-7.

5.3.5. Device TR069 Configuration

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

To do so, you can do as follows:

1. Click **Network - Advanced** to find **TR069**.
2. Enter the parameters and click **Submit** tab to save.



Parameters 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, 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.

5.3.6. Device Web HTTP Configuration

This function is used to manage whether the device website is allowed to be accessed. R20B supports two types remote access method HTTP and HTTPS(encryption).

To do so, you can do as follows:

3. Click **Network - Advanced** to find **Web Server**.
4. Enter the parameters and click **Submit** tab to save.

Parameters Set-up:

- **Http Enable:** Set whether HTTP access to the device webpage is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **Https Enable:** Set whether HTTPS access to the device webpage is allowed, Enabled is allowed, Disabled is not allowed, the default is Enabled.
- **Http Port:** Setup the port for HTTP access method. 80 is default port.

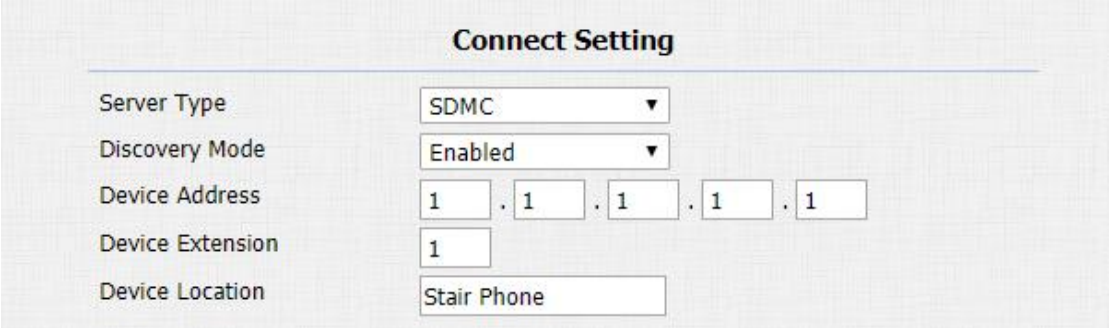
5.3.7. Device Deployment in Network

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.

To deploy the device in the network, you can start with the following process:

1. Click **Network - Advanced** to find **Connect Setting**.

2. Set up correct parameters according to your actual application and deployment.
3. Click **Submit** tab to validate the setting and **Cancel** tab to cancel the setting.



Parameters Set-up:

- **Server Type:** It is automatically set up according to the actual device connection in the network such as **SDMC** or **Cloud** or **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. Each part of the node can be set to 0-10, and the node can be directly used for calling.
- **Device Extension: I**t is used to distinguish different devices in the same device address ,range from 0-10.
- **Device Location**:Enter the location in which the device is installed and used.

Note:

- **Discovery Mode, Device Extension and Device Location item can only be edited in Discovery mode.**

5.4. Intercom Call Configuration

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

5.4.1. IP call & IP Call Configuration

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

To configure the IP call on the device web interface, you can do as follows.

1. Click **Phone - Call Feature** to find **Others**.
2. Set up related parameters as needed.
3. Press **Submit** button tab to validate the setting and **Cancel** Button to cancel the setting.

Parameters Set-up:

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

Tip:

- **Auto answer feature please refer to the chapter**

5.4.2. SIP Call

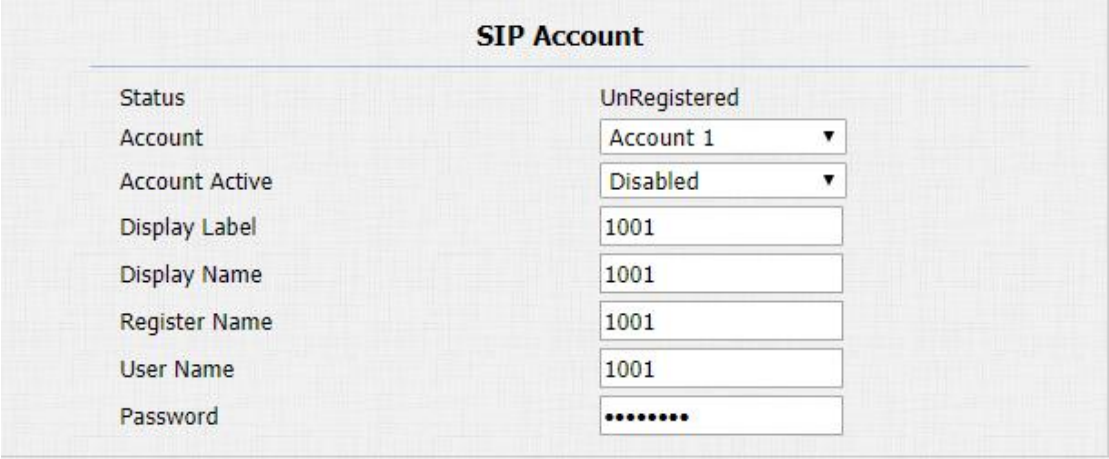
You can make SIP call (Session Initiation Protocol) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to configured first before you can make calls on the device.

5.4.2.1. SIP Account Registration

R20B door door phone supports two SIP accounts that can all be registered according to your applications. You can for example, switch between them if any one of the account failed and become valid. The SIP account can be configured on the device web interface.

To perform the SIP account setting, you can do as follows:

1. Click **Account - Basic** to find **SIP Account.**
2. Set up parameters for the SIP Account.
3. Click **Submit** tab to validate the setting and **Cancel** tab to cancel the setting.



Parameters Set-up:

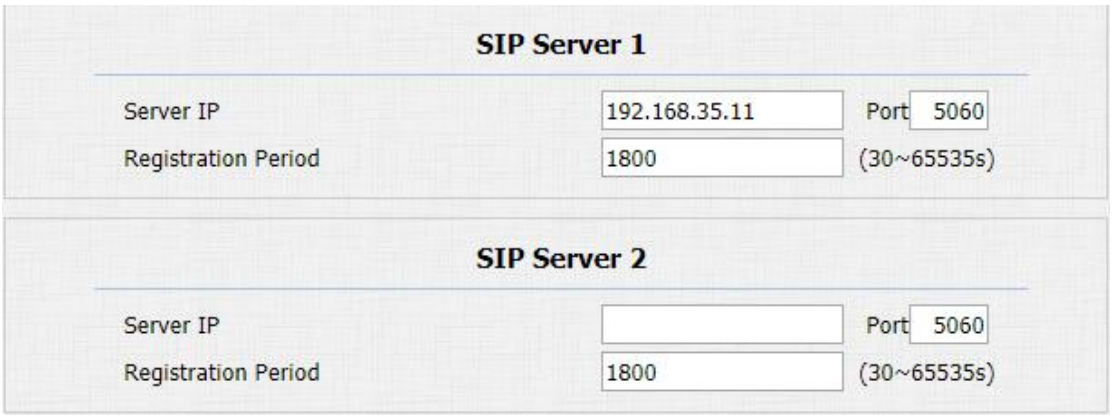
- **Account status:** Check to see if the SIP account is registered or not.
- **Account Active:** Click “enable” or “Disable” to activate or deactivate the registered SIP account.
- **Display Name:** Configure the name, for example the device’s name to be be shown on the device being called to.
- **User Name:** Enter the user name obtained from SIP account administrator
- **Account:** Select the exact account (Account 1/2) to be configured.
- **Display Label:** Configure the device label to be shown on the device screen.
- **Register Name:** Enter the SIP account register Name obtained from the SIP server.
- **Password:** Enter the password obtained from the SIP server.

5.4.2.2. SIP Server Configuration

Two SIP severs can be set up for device in order to achieve call session through SIP sever between intercom devices. SIP sever 2 serves as a backup to the SIP sever 1.

To do the setup, please do as follows :

1. Click **Account - Basic** to find **SIP server1 /SIP serer 2**.
2. Enter parameters required.
3. Press **Submit** tab to validate the setting and **Cancel** to cancel the setting.



Parameters Set-up:

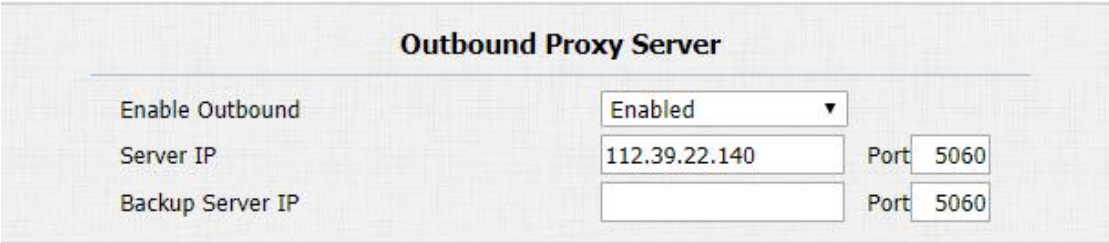
- **Server IP**: Enter the Server's IP address number or its URL.
- **Port:** Set up SIP server port for data transmission.
- **Registration Period:** Set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time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

5.4.2.3. Outbound Proxy Server Configuration

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 configure outbound Proxy server, you can do as follows:

1. Click **Account - Basic - Outbound Proxy Server**
2. Set up parameters properly.
3. Press **Submit** to validate the setting.



Parameters Set-up:

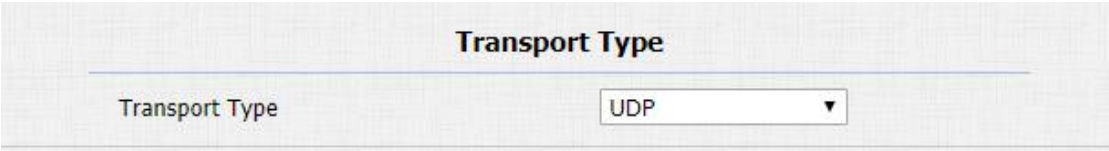
- **Enable Outbound:** Click "**Enable**" and "**Disable**" to turn on or turn off the outbound proxy sever.
- **Server IP:** Enter the SIP address of the outbound proxy server.
- **Port:** Enter the Port number for establish call session via the outbound proxy server.
- **Backup Sever IP:** Set up Backup Server IP for the back up outbound proxy sever.
- **Port:** Enter the Port number for establish call session via the backup outbound proxy server.

5.4.2.4. Data Transmission Type Configuration

SIP message can be transmitted in three data transmission protocols: UDP (User Datagram Protocol), TCP(Transmission Control Protocol) and TLS (Transport Layer Security). In the meantime, you can also identify the sever from which the data come from

To do the configuration , you can do as follows:

1. Click **Account - Basic** to find T**ransport Type**.
2. Select the Transport type according to your need.
3. Click **Submit** tab to validate the setting and **Cancel** tab to cancel the setting.



Parameters 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 services. 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.

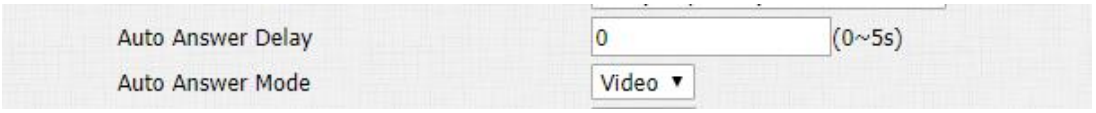
5.4.3. Auto Answer

You can define how quick the door phone should response in answering the incoming SIP/IP call automatically by setting up the time related parameters. In addition you can also define the in what mode the calls are answered (video mode or audio mode).

To do so, you can do as follows:

1. Click **Account** - **Advanced** to find **Call**.
2. **Enable/Disable** Auto Answer feature, click **Submit** tab to save.

3. Click **Phone** - **Call Feature** to find **Others**.
4. Setup the Auto answer related parameters, click **Submit** tab to save.



Parameters Set-up:

- **Auto Answer:** Turn on the the Auto Answer function by clicking "**Enable**".
- **Auto Answer Delay:** Set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1

second, then the call will be answer in 1 second automatically.

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

Note:

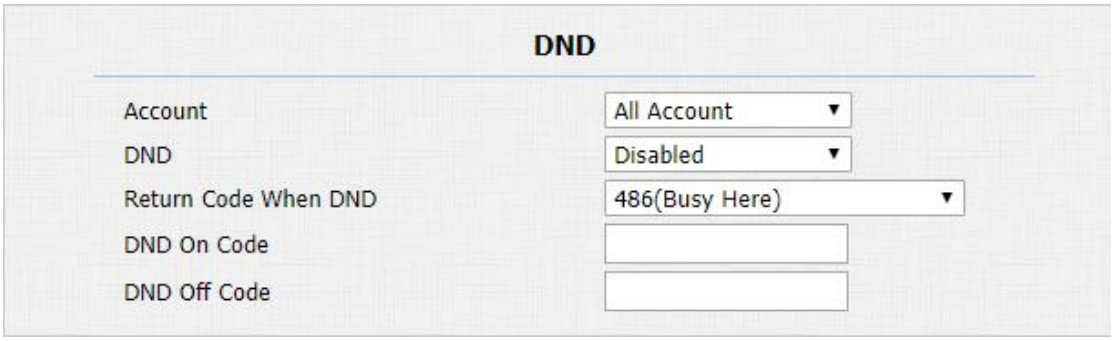
- **Auto Answer Delay and Auto Answer Mode are available after Auto Answer feature.**

5.4.4. 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 interface to block SIP calls you do not intend to answer. In the mean time, you can also defined the code to be sent to the SIP sever when you want to reject the call.

To configure the DND setting on the interface, you can do as follows:

1. Click **Phone - Call Feature** to find **DND**.
2. Set up parameters properly according to your need.
3. Press **Submit** tab to validate your setting..



Parameters Set-up:

- **Account:** Select account Account1, Account2 or All account for the DND

application.

- **DND:** Enable or disable the DND function. DND function is disabled by default.
- **Return Code When DND:** Select what code should be sent to the calling device via SIP sever. **404 for "Not found"**; **480 for " Temporary unavailable**" **486 for "busy here**".
- **DND On Code:** Turn on the DND on server using the Code obtained. The DND on Code is 78 by default.
- **DND Off Code:** Turn off the DND on server using the code obtained. The DND off Code is 79 by default.

5.4.5. SIP Call Related

There are some SIP call related settings including SIP port range, caller ID display, anonymous call settings and etc.

To configure the SIP call related settings, you can do as follows:

1. Click **Account - Advanced** to find Call.
2. Enter or enable/disable the parameters, click **Submit** tab to save.

Parameters Set-up:

- **Max Local SIP Port:** To configure maximum local SIP port for designated

SIP account.

- **Min Local SIP Port:** To configure maximum local SIP port for designated SIP account.
- **Caller ID Header:** To choose caller ID header format. There are 6 options - FROM, PAI, PAI-FROM, RPID-FROM, PAI-RPID-FROM, RPID-PAI-FROM.
- **Provisional Response ACK:** 100% reliability for all provisional messages, this means it will send ACK every time the phone receives a provisional SIP message from SIP server.
- **Register with user=phone:** If enabled, the phone will send user=phone within SIP message.
- **Anonymous Call:** If enabled, R20K will block its information when calling out.
- **Anonymous Call Rejection:** If enabled, calls who block their information will be screened out.
- **Missed Call Log:** If enabled, any missed call will be recorded into call log.
- **Prevent Hacking:** If enabled, it will prevent SIP call from attacking in the Internet

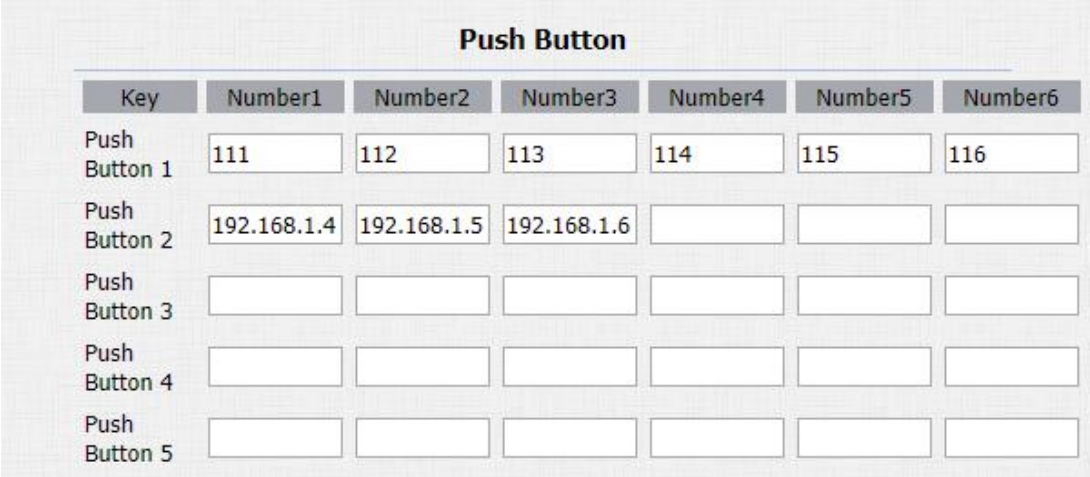
5.4.6. Push Button Call

R20B has 5 push buttons which are used to call out. Each push button can be setup up to 6 sip numbers or IP addresses, that means users can call out 6 numbers at one time by pressing push button.

To do so, you can do as follows:

1. Click **Intercom** - **Basic** to find **Push Button**.
2. Enter sip accounts or IP addresses for the push button, click **Submit** tab to

save.

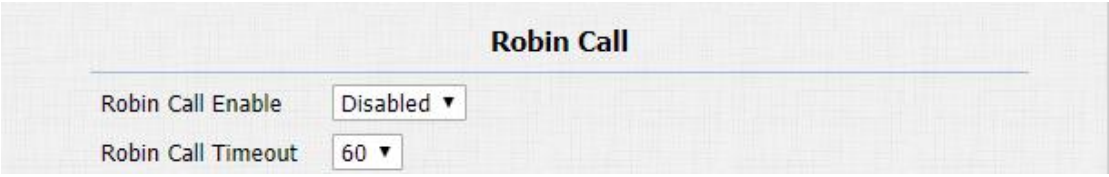


5.4.7. Robin Call

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

To do so, you can do as follows:

1. Click **Intercom** - **Basic** to find **Robin call.**
2. Setup the parameters and click **Submit** tab to save.



Parameters Set-up:

- **Robin Call Enable:** Enable or disable the robin call function. It is disabled by default.
- **Robin Call Timeout:** Call out time value for each number, range from 5 - 60s.

5.4.8. Web Call

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

To do so , you can do as follows

1. Click **Intercom** - **Basic** to find **Web Call**.
2. Enter the number you want to dial out in the **Dial** field using a specific SIP account.
3. Click **Dial** tab to initiate the calling.
4. Click **Hang Up** tab to hang up.

Parameters Set-up:

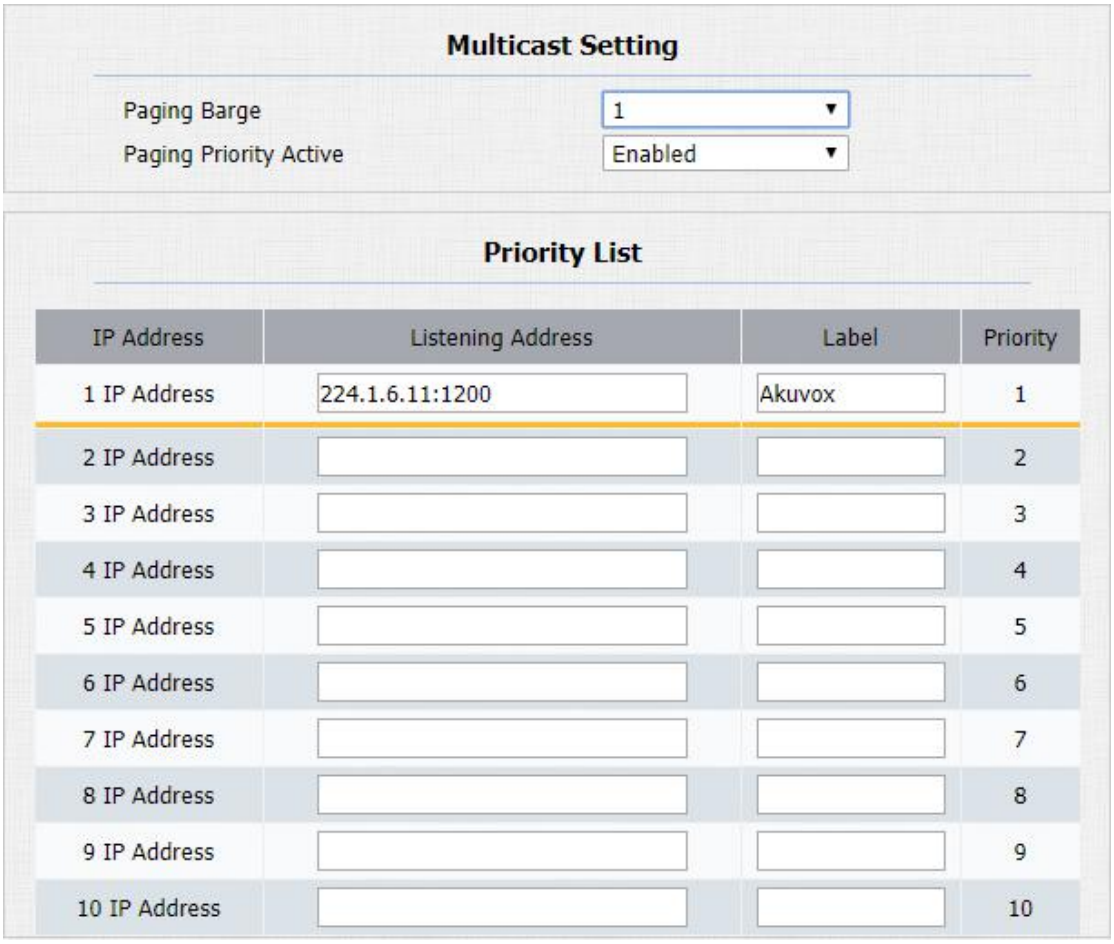
- **Auto/Account1/Account2:** To choose a suitable sip account to make a web call. If you call out using IP address, Account selection is no need to chosen.

5.4.9. Multicast

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

To do so, you can do as follows:

1. Click **Phone** - **Multicast**.
2. Setup the parameters and click **Submit** tab to save.



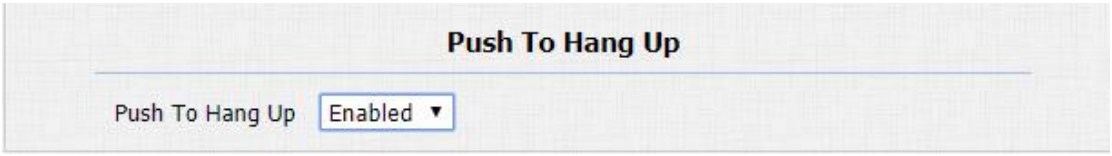
Parameters Set-up:

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

5.4.10. Push to Hang Up

Setup the Push button for hang up the call when press again the button during

the call.



Parameters Set-up:

- **Push To Hang Up :** Enable or Disable this function.

5.4.11. Hang Up After Open Door

This function is used to automatically hang up the call after triggering the relay. To do so, you can do as follows:

1. Click **Intercom** - **Basic** to find **Hang Up After Open Door**.
2. Setup the time out value and click **Submit** tab to save.

Parameters set-up

- **Time out :** Set the call hold delay timing (Ranging from 0-15 Sec.). For example, if you set the hold delay time as “ 5” Sec, then the call will be delayed for 5 min after the door is unlocked.

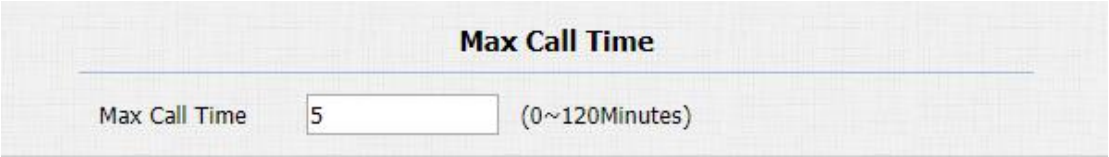
5.4.12. Maximum Call Duration

R20B door phone allows you to set up the call time duration in receiving the call from the calling device as the caller side might forget to hang up the intercom device. When the call time duration is reached, the door phone will

terminate the calling automatically.

To do the configuration, you can do as follow:

1. Click **Intercom - Basic - Max Call Time**.
2. Enter the time duration in in the **Max Call Time** field.



Parameters Set-up:

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

Note:

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

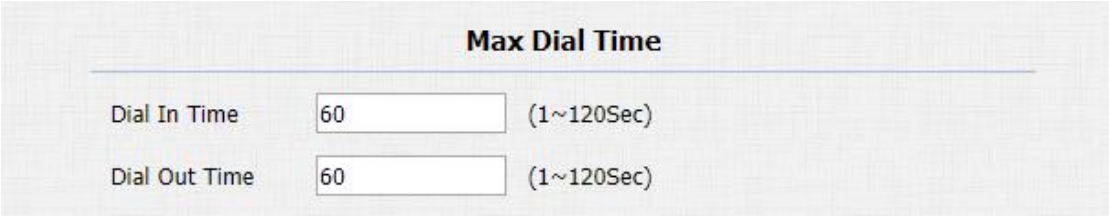
5.4.13. Maximum Dial Duration Setting

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

To do the configuration, you can do as follows:

1. Click **Intercom - Basic** to find **Max Dial Time**.
2. Click and enter the timing parameters you need.

3. Click **Submit** tab to validate setting and Cancel tab to cancel the setting.



Parameters Set-up:

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

Note:

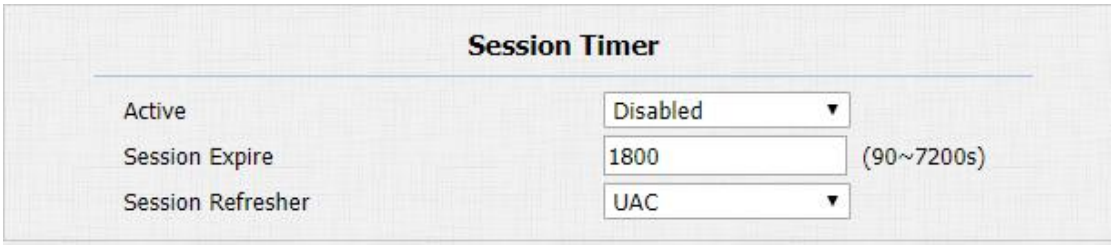
- **Max dial time of device is also related with max dial time of sip server. If using sip account to make a call, please pay attention to the max dial time of sip server. If the max dial time of sip server is less than the max dial time of device , the shorter one is available.**

5.4.14. Call Session Timer

RFC4028 defines a survival mechanism for SIP sessions. The user agent or proxy server periodically sends re-INVITE or UPDATE requests to keep the session active. The interval of session update requests is determined by its defined negotiation mechanism. Assuming that no session update request is received within the interval, the session is considered terminated.

To do the configuration, you can do as follows:

1. Click **Account - Advanced** to find **Session Timer**.
2. Set up the parameters properly.
3. Press **Submit** tab to valid the setting and Cancel tab to cancel the setting.



Parameters Set-up:

- **Active:** Click to enable or disable the Call session timer function. Call session timer is "**Disabled**" be default.
- **Session Expire:** Enter the Session call duration before the call expires or ends automatically for refreshment. For example if you set the session expiration as 1800 second (Ranging from 90- 7200 sec) you can have the door phone to terminate the ongoing call with other intercom device in 1800 second.
- **Session Refresher:** Select UAC (User Agent Client) or UAS (User Agent Server)for the call session refreshment.

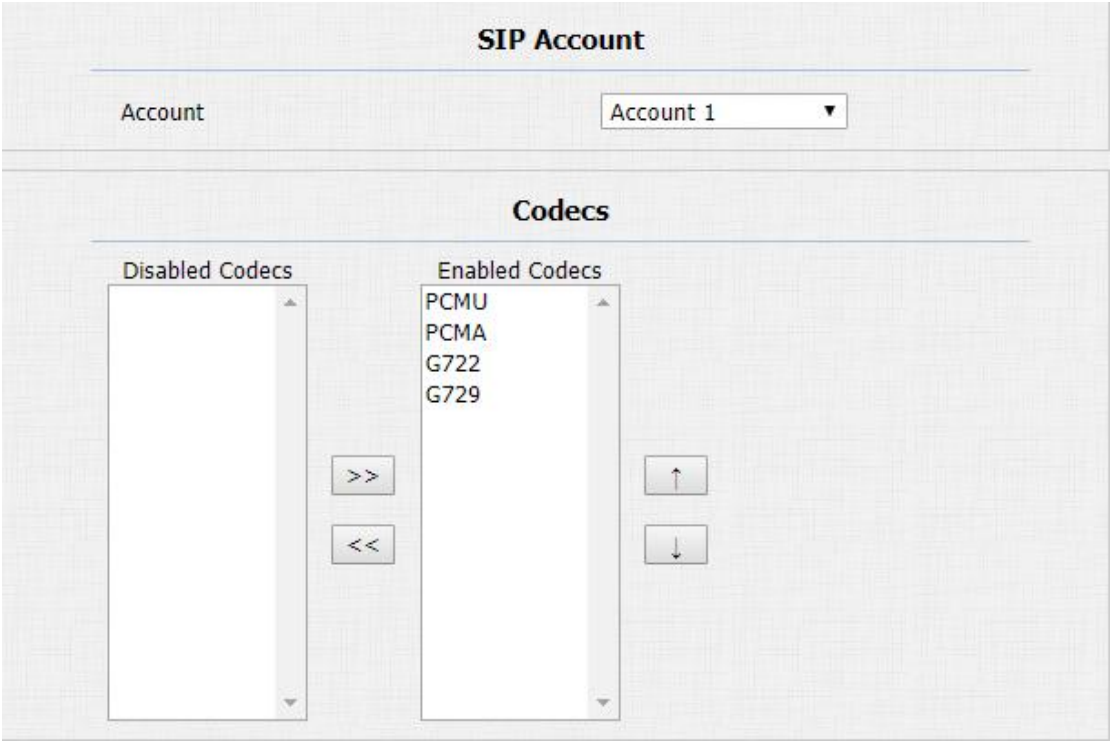
5.5. Codecs

5.5.1. Audio Codec Configuration

R20B supports four types codecs (PCMU, PCMA, G729, G722) for encoding and decoding the the audio data during the call session. Each type of codec vary in terms of the sound quality. You can select the specific codec with different bandwidth and sample rate flexibly according to the actual network environment.

To do the configuration, you can do as follows:

1. Click **Account** - **Advanced.**
2. Select the Account for which you want to apply the codec .
3. Click on arrows and move the codec type left and right in order to enable an disable the codec function.
4. Click **Submit** tab to validate the setting and **Cancel** to cancel the setting.



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

Codec Type	Bandwidth Consumption	Sample Rates
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Note:

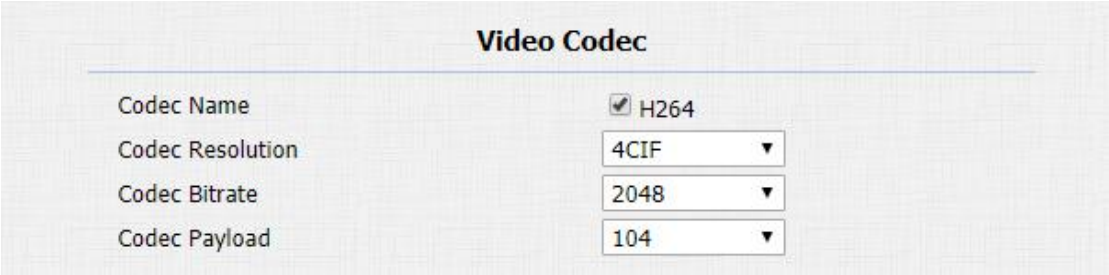
- Audio codecs adjustment is only available for SIP call.

5.5.2. Video Codec Configuration

R20B supports H264 codec that provides a better video quality at much lower bit rate with different video quality and payload.

To do the configuration, you can do as follows:

1. Click **Account** - **Advanced** to find **Video Codec**.
2. Check the H264 Code name square box.
3. Set up parameters according to your need.
4. Click **Submit** tab to validate the setting.



Parameters Set-up:

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

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

Note:

- Audio codecs adjustment is only available for SIP call.

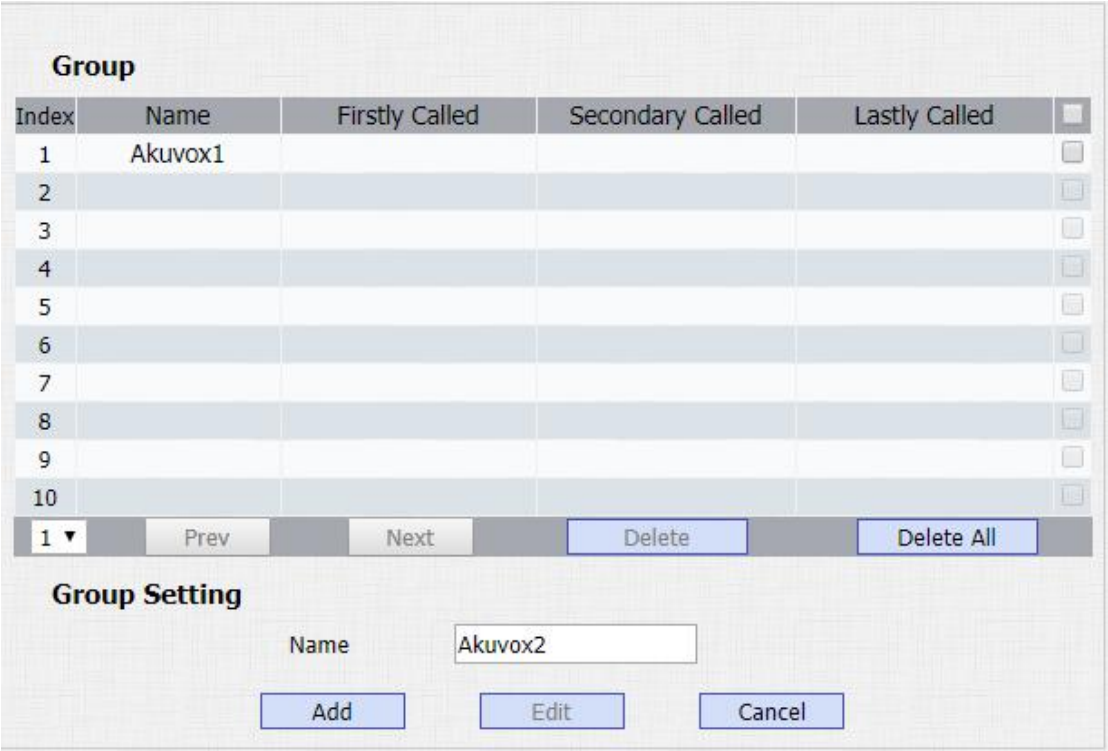
5.6. Access Whitelist Configuration

R20B supports to store up to 500 contacts who can give a access permission to R20B. Access Whitelist includes group setting and contact setting and management.

5.6.1. Group Settings

To configure contact group, you can do as follows:

1. Click **Access Whitelist - Access Whitelist** to find **Group Setting**.
2. Enter the group name in the **Name** field.
3. Click Add tab for confirmation and click Cancel tab to cancel the setting.
4. Check box for the group name to be deleted or edited.
5. Edit the name in the Name field and click **Edit** tab to finish the editing.



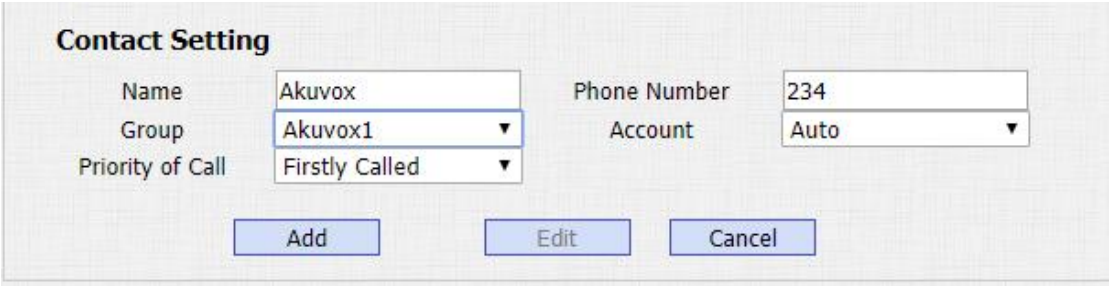
Parameters Set-up:

- **Group:** Click the green tab to select the group name you have created. You cannot select the group name If no group name has been created.
- **Name:** Enter the contact name, which is required.
- **Phone:** Enter the phone number of the contact, which is required.
- **Email**: Enter the contact's Email, which is optional.
- **Dial Type**: Select and assign the group name to an account. If you select default option, then the number will be assigned to the account 1 if the account is registered.

5.6.2. Contact Settings

To do configure contacts, you can do as follows:

1. Click **Access Whitelist** - **Access Whitelist**.
2. Enter the contact information before pressing **Add** tab for confirmation and **Cancel** to cancel the setting.



Parameters Set-up：

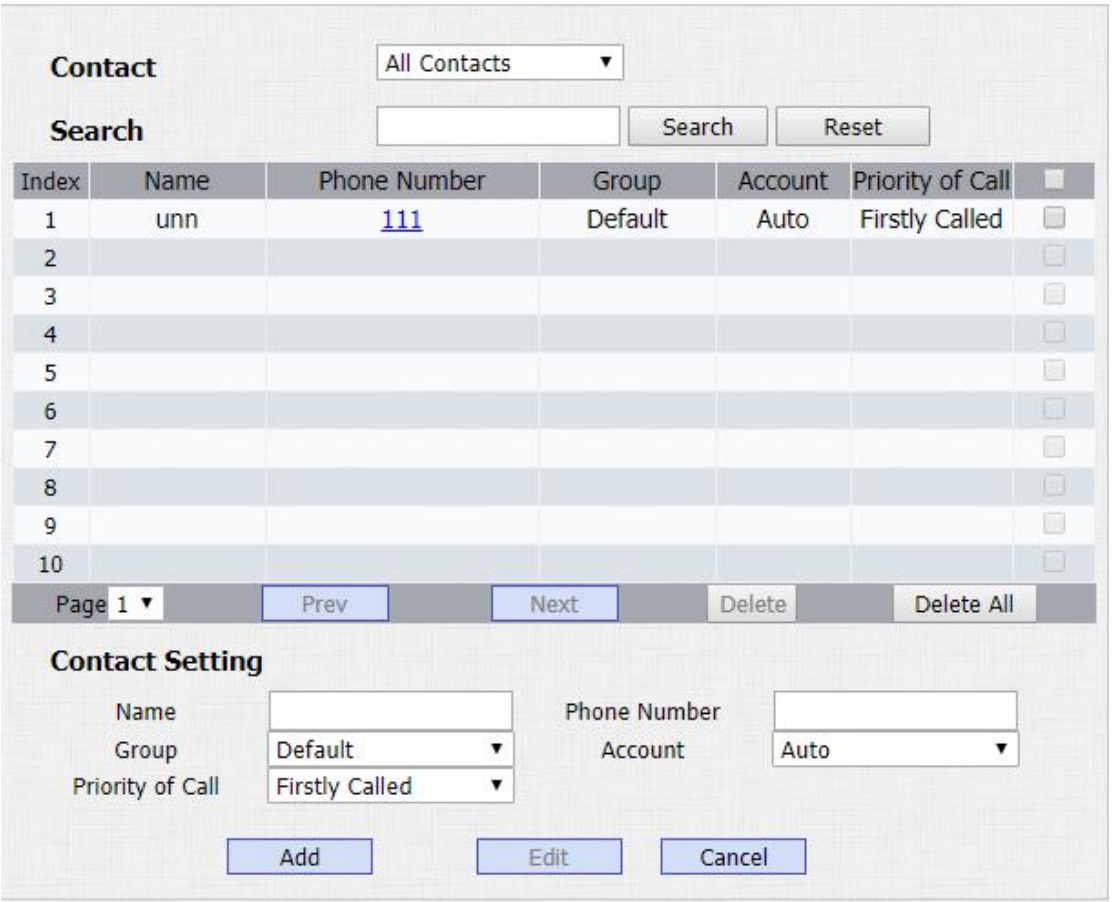
- **Name:** Enter the contact name, which is required.
- **Phone:** Enter the phone number of the contact, which is required.
- **Group:** Click the green tab to select the group name you have created. You cannot select the group name If no group name has been created.
- **Account:** Select which sip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

5.6.3. Contact Management

You can search, display ,edit and delete the contacts in your phone book. More over, you can also dial out using the contact phone number directly.

To do so , you can do as follows:

1. Click **Access Whitelist** - **Access Whitelist**.
2. Select the searching range in the **Contact** field.
3. Enter the contact information and press **Search** tab.
4. Check ☐ to edit the contact information in “**Contact setting**”in the same interface.
5. Move down to **Contact Setting** and press **Edit** tab to complete the edit.
6. Press delete tab if you want to delete any contact.



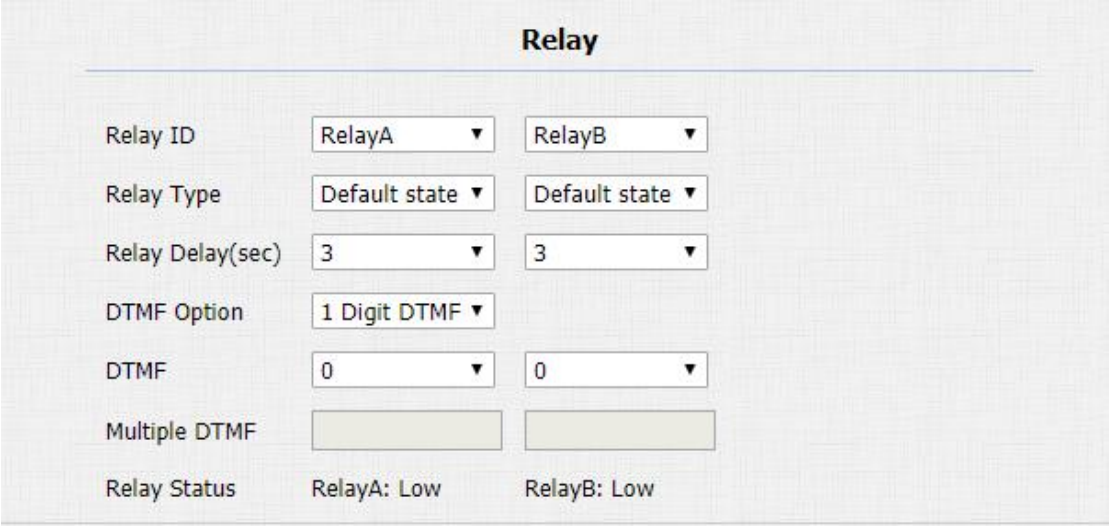
5.7. Door Access

5.7.1. Unlock by DTMF

DTMF codes can be configured on the door phone web interface and set up identical DTMF code on the corresponding intercom devices such as indoor monitor, which allows residents to press unlock button on the screen to unlock the door for visitors etc during a call.

To do the configuration, please do as follows:

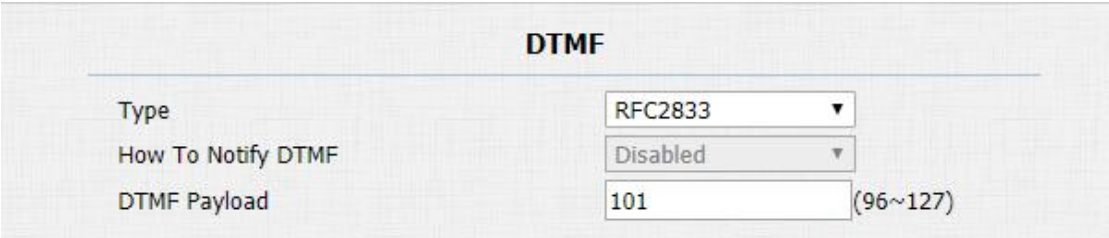
1. Click **Intercom - Relay** to find **Relay**.
2. Set up relay related parameters properly according to your need.
3. Click **Submit** tab to validate the setting and Cancel tab to cancel the setting.



- **Relay ID:** You are allowed to set up three relay switches in total for the door access control (Relay A, Relay B).
- **Relay 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 be delayed for 5 min after the door is unlocked.
- **DTMF Option:** Select the number of DTMF digit for the door access control (Ranging from 1- 4 digits) For example, you can select 1 digit DTMF code or 2-digit DTMF code etc, according to your need.
- **DTMF:** Set the 1-digt DTMF code within range from (0-9 and *,#) if the DTMF Option is set as "1-digit".
- **Multiple DTMF:** Set the DTMF code according to the **DMTP Option** setting. For example, you are required to set the 3-digits DTMF code if DTMF option is set as 3-digits.
- **Relay Status:** Relay status is low by default which means normal close.

To do the extra DTMF configuration on the web interface, you can do as follows:

1. Click **Account** - **Advanced** to find **DTMF**.
2. Choose suitable DTMF parameters and click **Submit** to save.



Parameters Set-up:

- **Type:** Select DTMF type among five options: **“ Inband”,“ RFC2833”, “ Info+Inband” and “Info+RFC2833”** according to you need.
- **RFC2833:** By filtering rtpevent and checking if there is RTP EVENT packet.
  SIP INFO: By filtering sip, and checking if there is sip info message.
  Inband: Not able to see it in the packets. It is in the voice band, and we can try to play RTP to check.
- **How to Notify DTMF:** Select among four options: “**Disable**” “ **DTMF**” “**DTMF-Relay**” “**Telephone-Event**” according to your need.
- **DTMF Payload:** Select the payload 96-127 for data transmission identification

5.7.2. Unlock by RF Card

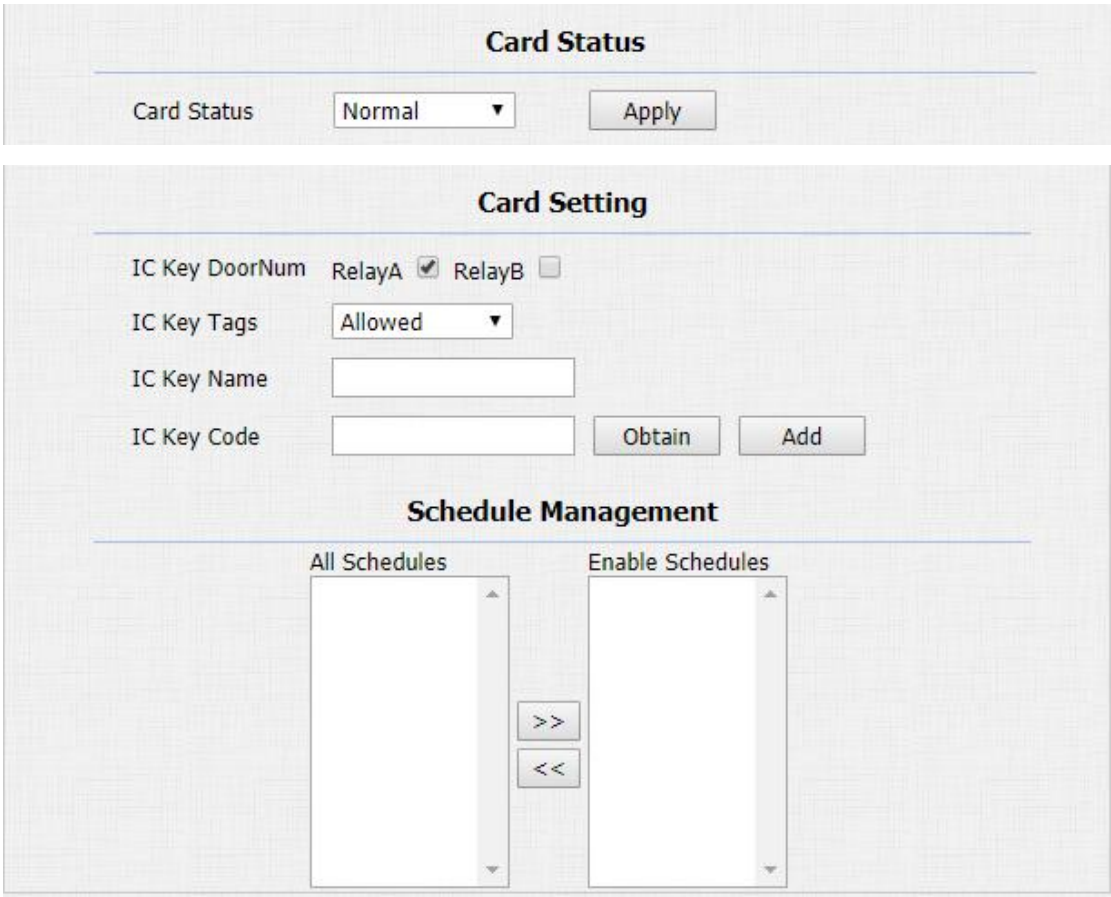
On the device web interface, you can not only configure the RIFID card one by one manually but also import or export the RFID card files to the device in batch in order to maximize card configuration efficiency.

5.7.2.1. Add RF Cards

To configure the RFID Card individually, you can do as follows:

1. Click **Intercom** - **Card setting**.
2. Select **“Card Issuing”** in the **Card Status** Field and click **Apply** tab.
3. Click **Obtain** tab and place your RFID card on the card reader area.
4. Click Add tab to add the RFID card.

5. Set the time schedule and limit for the RIFD card access.
6. Change the "**Card Issuing**" in the Card Status to "**Normal**".
7. Click **Submit** tab for validation and Cancel tab for cancellation.



Parameters Set-up:

- **Card Status:** Select **"Car Issuing**" in the field before adding the RFID card and change the status back to "**Normal**" after the card is added.
- **IC key DoorNum:** Select the relay switch available for the RIFD card door access.
- **IC Key Tags:** Select the frequency of the validity the RFID card for the door access among three options**: "Allow" "Schedule" and " Forbidden"** For example, if you select **"Allowed"** then the card is always valid for unlimited door access according to your setting. If you select "Schedule" you are required to set up the specific time of the RFID card access validity. If you select "Forbidden" then the RFID card will never

be valid for the door access.

- **Frequency:** If setup the Tags as “schedule”, you also need to setup the using frequency which means the number of times the card can be used in a special time period
- **IC key Code:** Find the RFID card code in the field.
- **Schedule Management:** Select a available time for the card from All Schedule to Enable Schedule.

Note:

- **RFID card with 13.56 MHZ and 125 KHZ can be applicable to the door phone for the door access.**
- **Please check chapter 5.7.3 for setting schedule.**

Tip:

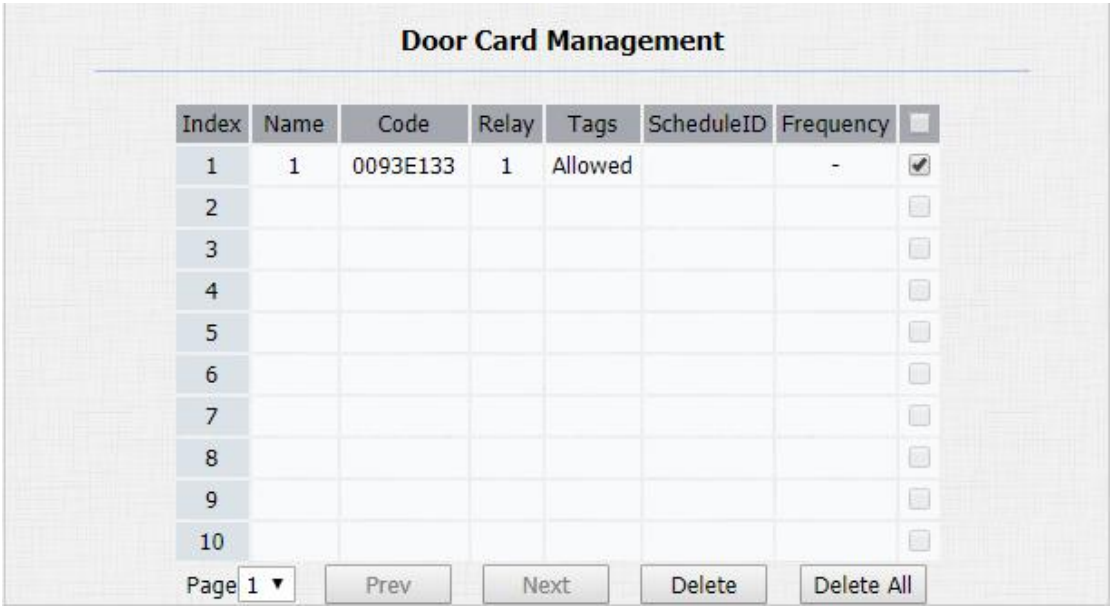
- **The maximum card storage of R20B is 5000.**

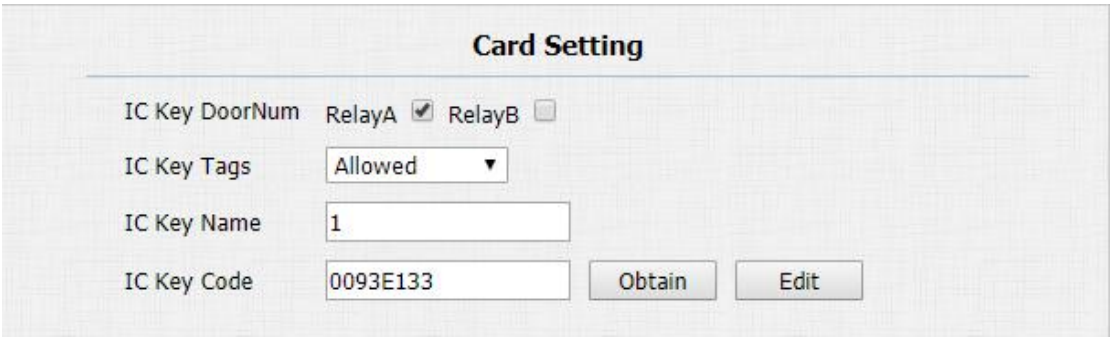
5.7.2.2. Edit RFID Cards

If you want to change or adjust your RFID card configurations, you can edit or delete the configured RIFID cards one by one or in batch on the web interface.

To edit or delete the RFID cards , you can do as follows:

1. Click **Intercom - Card Setting** to find **Door Card Management**.
2. Check the RFID card you wish to edit or delete.
3. Go to **Card Setting** section in the same interface.
4. Edit the RFID card setting according to your need.
5. Click **Edit** tab in the **Card Setting** section for validation.





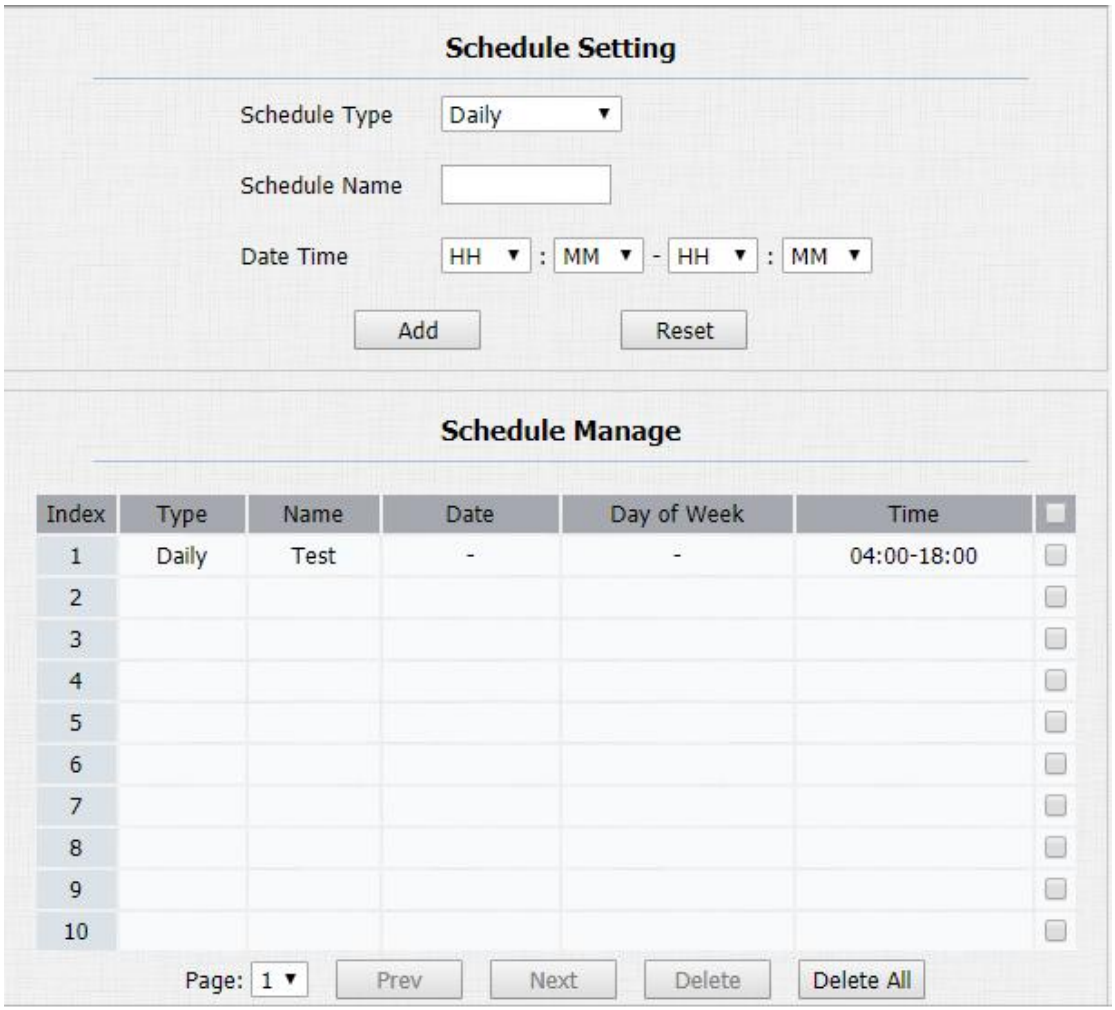
5.7.3. Schedule Setting

This function is used to set a special time period for RFID card, which means that residents can only use this card to enter and exit during a certain period of time.

5.7.3.1. Create a schedule

To create a schedule, you can do as follows:

1. Click **Intercom** - **Schedule**.
2. Setup the schedule type, name and date time for creating a schedule.
3. Click **Add** to save.



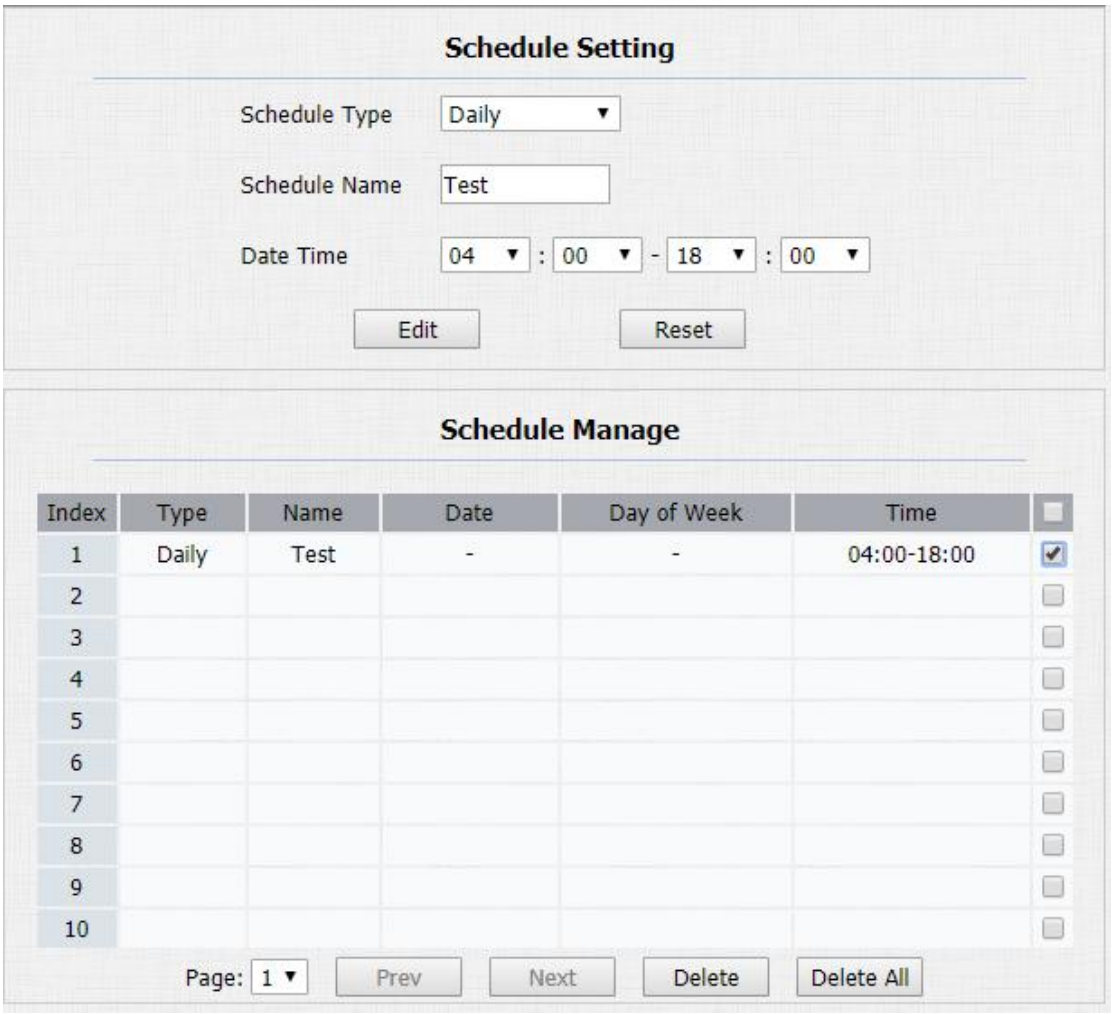
Parameters Set-up:

- **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.

5.7.3.2. Edit a schedule

To edit a schedule, you can do as follows:

1. Choose a existed schedule.
2. Edit the type ,name or date ,click **Edit** to save.
3. Click **Reset** to restore the contents of all fields to the initial state.
4. click **Delete** to remove the selected schedule.
5. Click **Delete All** to remove all existed schedule.

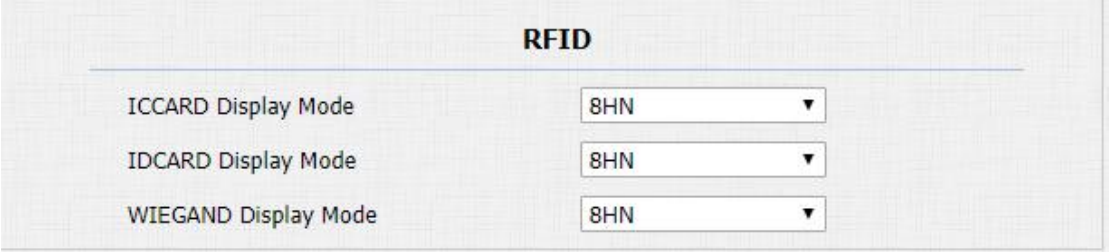


5.7.4. RF Card Code Format Selection

If you want to integrate with the third party intercom system in terms of RF card door access, you can change the RF car code format to be identical with that applied in the third party system.

To select the RF card format, you can do as follows:

1. Click **Intercom** - **Card Setting** to find **RFID**.
2. Select Card display format.
3. Click **Submit** tab to validate the selection and **Cancel** tab for the cancellation.



Parameters Set-up:

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

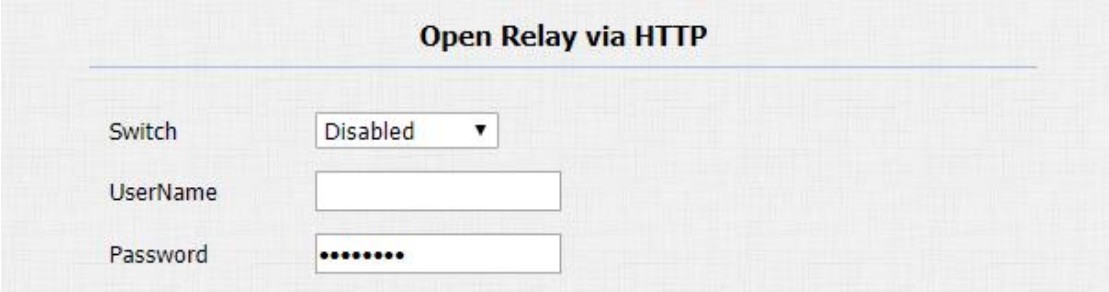
5.7.5. Unlock by HTTP Command

You can unlock the door remotely without approaching the device physically for the door access by typing the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access.

To do the configuration, you can do as follows:

1. Click **Intercom** - **Relay** to find **Open Relay via HTTP**.

2. Enable/Disabled this feature.
3. Enter the authentication user name and password.



Parameters Set-up:

- **Switch:** Enable/disable the HTTP command unlock function by clicking on **Enable** field
- **UserName:** Enter the User name of the device web interface, for example "**Admin**"
- **Password:** Enter the password for the HTTP command. For example : "**12345**"
- **HTTP URL:** The url must contain the IP address of the door phone, the authentication information and which door you want to open.
- Please refer to the following URL example:

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

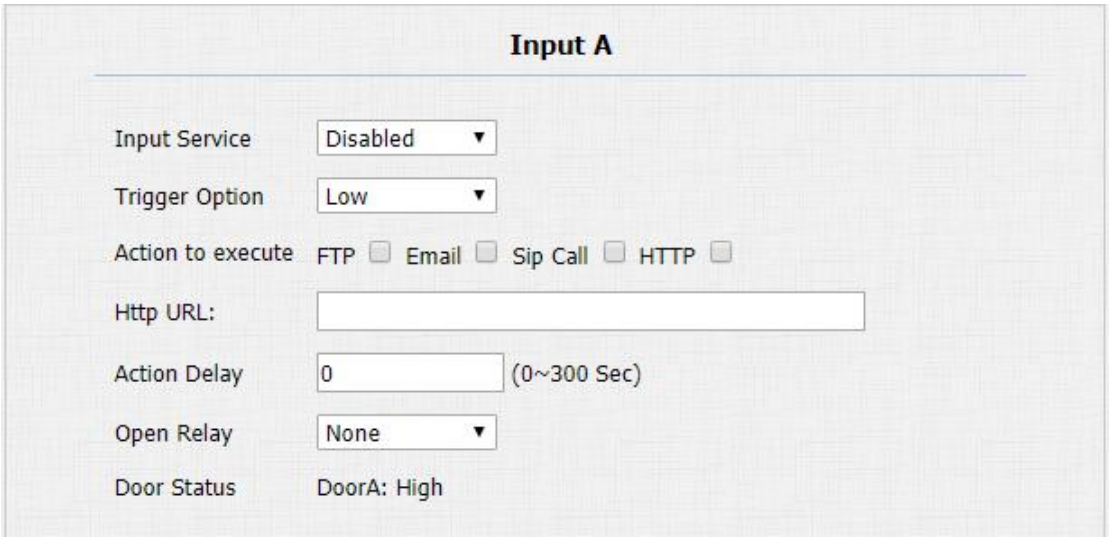
5.7.6. Unlock via Exit Button

When you need to open the door from inside using the Exit button installed by the door, you can configure the door phone Input A/B to trigger the two relay switches maximum for the door access.

To do the configuration, you can do as follows:

1. **Click Intercom- Input** to find **Input A/B**.
2. Click to enable the Input function in the **Input Service** field.

3. Set up the parameters according to your need.
4. Press **Submit** tab for validation and **Cancel** tab for cancellation



Parameters Set-up:

- **Input service:** Select " **Enable** " to be able to use the Input function.
- **Trigger Option:** Select the trigger options according the actual operation on the exit button.
- **Action To Execute:** Select the method to carry out the action among four options: FTP, Email, HTTP, TFTP.
- **Http URL:** Enter the URL if you select the HTTP to carry out the action.
- **Action Delay:** Set up the delay time when the action is carried out. For example, if you set the action delay time at 5 sec, then the corresponding actions will be carried out 5 minutes after your press the button.
- **Open Relay:** To set up relays to be triggered the input terminal.
- **Door A:** To show the status of input signal.

Tip:

- **Please refer to chapter 5.8.1 about Action setting.**

5.7.7. ChimeBell Setting

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

Parameters Set-up:

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

5.8. Security

5.8.1. Action

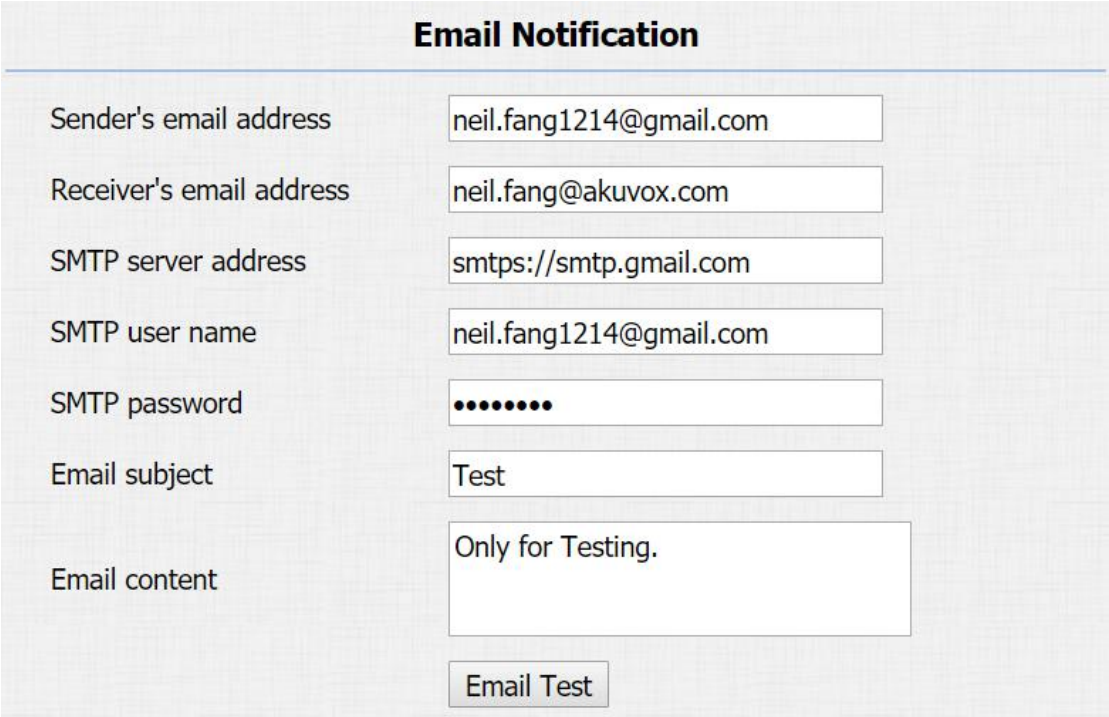
R20B supports to send notifications via HTTP, snapshots via email and FTP transfer method, or calls via SIP call method, when trigger specific actions.There are 3 specific actions - push button call, Input and Motion detection which will be triggered in R20B.

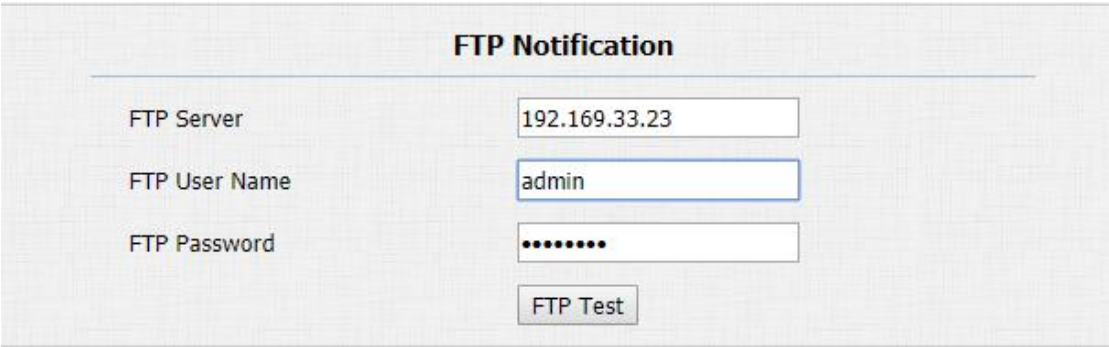
5.8.1.1. Action Parameters

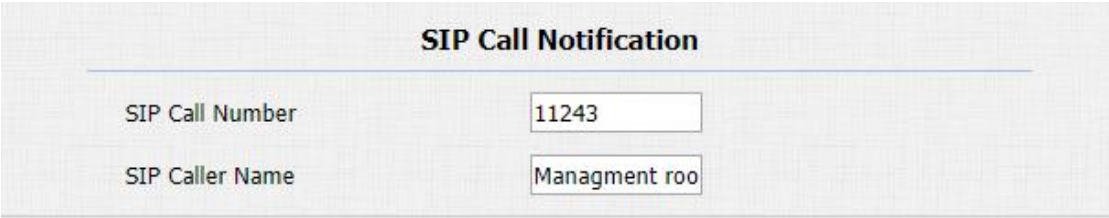
When you enable any action operations, you need to setup the corresponding action parameters first.

To setup action parameters, you can do as follows:

1. Click **Intercom** - **Action** to set action receiver.
2. Enter the parameters and click **Submit** tab to save.







Parameters Set-up:

Email Notification

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

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

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

SMTP user name: To configure user name of SMTP service (usually it is same with sender's email address).

SMTP password: To configure password of SMTP service (usually it is the same with the password of sender's email).

Email subject: To configure subject of email.

Email content: To configure content of email.

Email Test: To test whether email notification is available.

FTP Notification

FTP Server: To configure URL of FTP server.

FTP User Name: To configure user name of FTP server.

FTP Password: To configure password of FTP server.

FTP Test: To test whether FTP notification is available.

SIP Notification

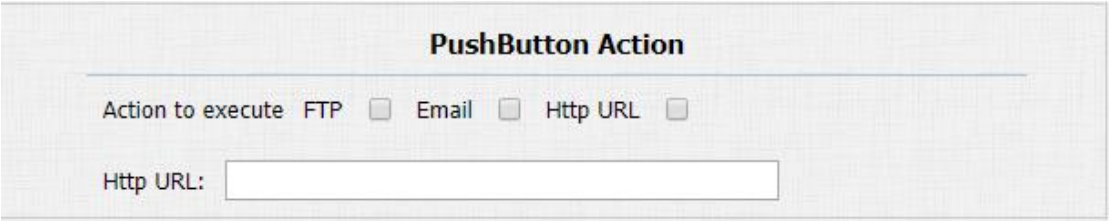
SIP Call Number: To configure sip call number.

SIP Call Name: To configure display name of R20B.

5.8.1.2. Trigger Action by Push Button Call

To do so, you can do as follows:

1. Go to **Intercom** - **Basic** to find **PushButton Action**.
2. Choose a suitable action method and click **Submit** tab to save.



Parameters-Setup:

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

Http URL: To configure URL, if HTTP action is chosen. The URL includes HTTP server IP address and any formation you want to send as suffix, like device Mac and etc.

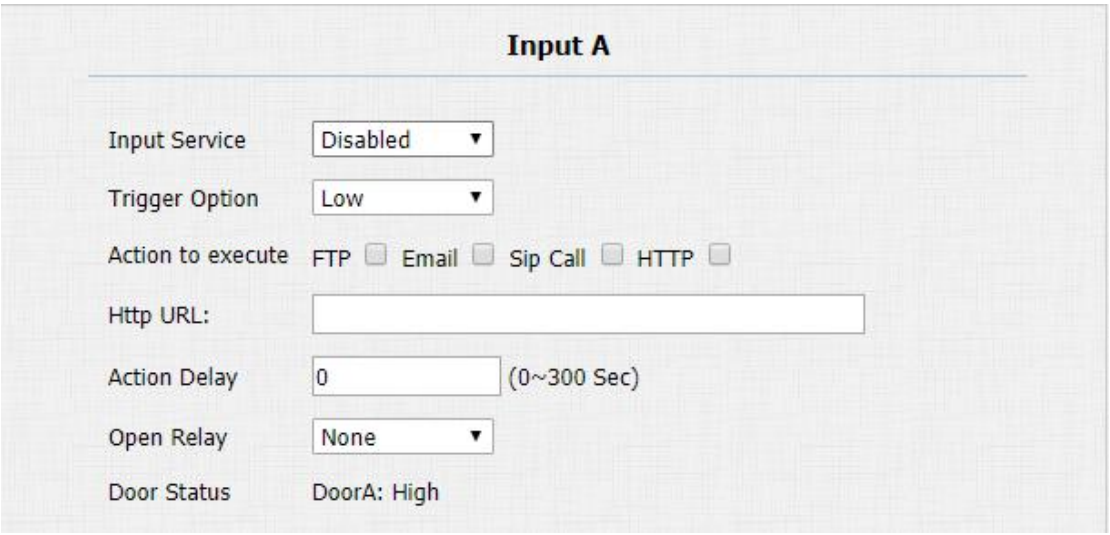
Note:

- **Akuvox do not provide HTTP server.**

5.8.1.3. Trigger Action by Input

To do so, you can do as follows:

1. Go to **Intercom** - **Input** to configure.
2. Enable/disable the input service and setup the action related parameters.
3. Click **Submit** to save.



Parameters-Setup:

- **Action to execute:** To choose which action to execute after triggering.
- **Http URL:** To configure URL, if HTTP action is chosen.The URL includes HTTP server IP address and any formation you want to send as suffix, like device Mac and etc.
- **Action Delay:** To configure after how long to execute to send out notifications and trigger relay.

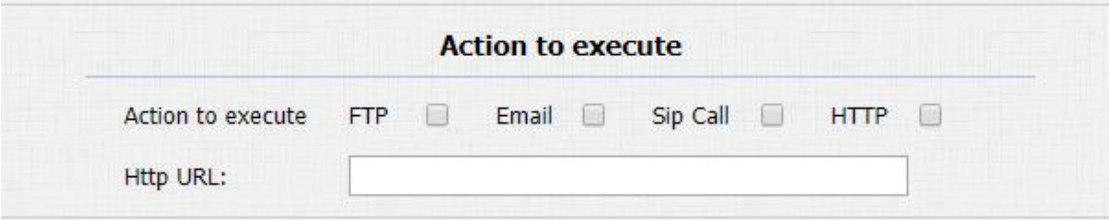
Note:

- **Akuvox do not provide HTTP server.**

5.8.1.4. Trigger Action by Motion

To do so, you can do as follows:

4. Go to **Intercom - Motion**.
5. Enable/disable the Motion feature and setup the action related parameters.
6. Click **Submit** to save.



Parameters-Setup:

- **Action to execute:** To choose which action to execute after triggering.
- **Http URL:** To configure URL, if HTTP action is chosen.The URL includes HTTP server IP address and any formation you want to send as suffix, like device Mac and etc.

Note:

- **Akuvox do not provide HTTP server.**

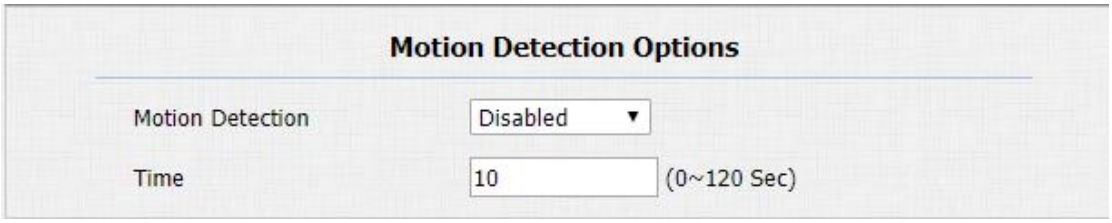
5.8.2. Motion

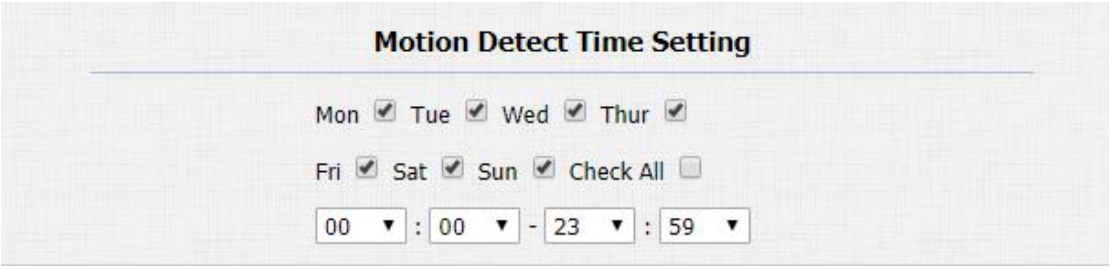
Motion detection is used to detect and record any change from the surrounding in a fix period, such as suspicious people loitering around, and send

notification message to a monitor unit. The door phone will send the notification to the destination.

To setup Motion configuration, you can do as follows:

1. Click **Intercom** - **Motion**.
2. Enable/disable the Motion detection feature, and setup the time settings.
3. Click **Submit** tab to save.





Parameters Set-up:

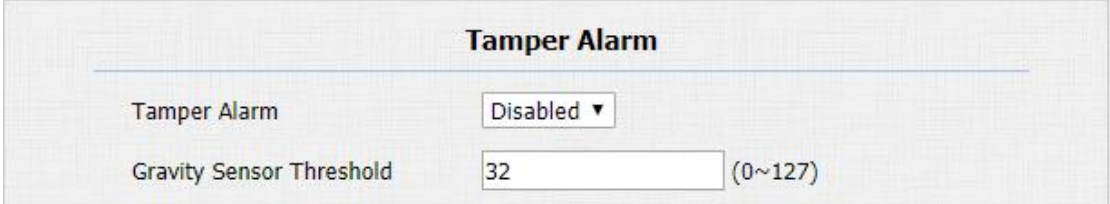
- **Motion Detection:** To enable or disable motion detection.
- **Time:** set the time interval for the motion detection. If you set the default time interval as “10 “second, then the motion detection time span will be 10 seconds. Assuming that we set the time interval as “10” then, and the first movement captured can be seen as start point of the motion detection, and if the movement continues through 7 seconds of the 10 second interval, then the alarm will be triggered at 7 second (the first trigger point) and motion detection action can be triggered (sending out notification) any where between 7-10 seconds once movement is detected.“10”second 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”.
- **Motion Detect Time Setting:** To configure motion detect time schedule.

5.8.3. Tamper alarm

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

To do the configuration on the web interface, please do as follows:

1. Click **Intercom - Advanced** to find **Tamper Alarm**.
2. Set up parameters properly.
3. Click **Submit** tab for validation and **Cancel** tab for the cancellation.



Parameters set-up:

- **Tamper Alarm**: Click to select “on “ in the Tamper Alarm field in order to enable the anti-theft alarm function.
- **Gravity sensor Threshold**: Set the threshhold for the gravity sensory sensitivity. The lower the the value is, the higher the value will be. The gravity sensor value is 32 by default.

5.8.4. Certification

Web server certificate, used for SIP communication when HTTPS login and TLS are used as the transmission method.

As a web server certificate, upload a self-signed ssl server certificate, and log in to the device via HTTPS (the device has a self-signed certificate by default). Upload the CA signed SSL server certificate to log in to the device securely via

HTTPS.

As the sip communication SSL certificate, upload the self-signed CA certificate to the device, and configure the decryption key to the server at the same time, register the sip account and set the transmission mode to tls, the device can normally perform sip registration and SIP communication such as calls.

To setup certification, you can do as follows:

1. Click **Security** - **Advanced**.
2. Choose the certification from your PC, click **Submit** tab to save.
3. Or choose the existed certification, click **Delete** tab to remove.

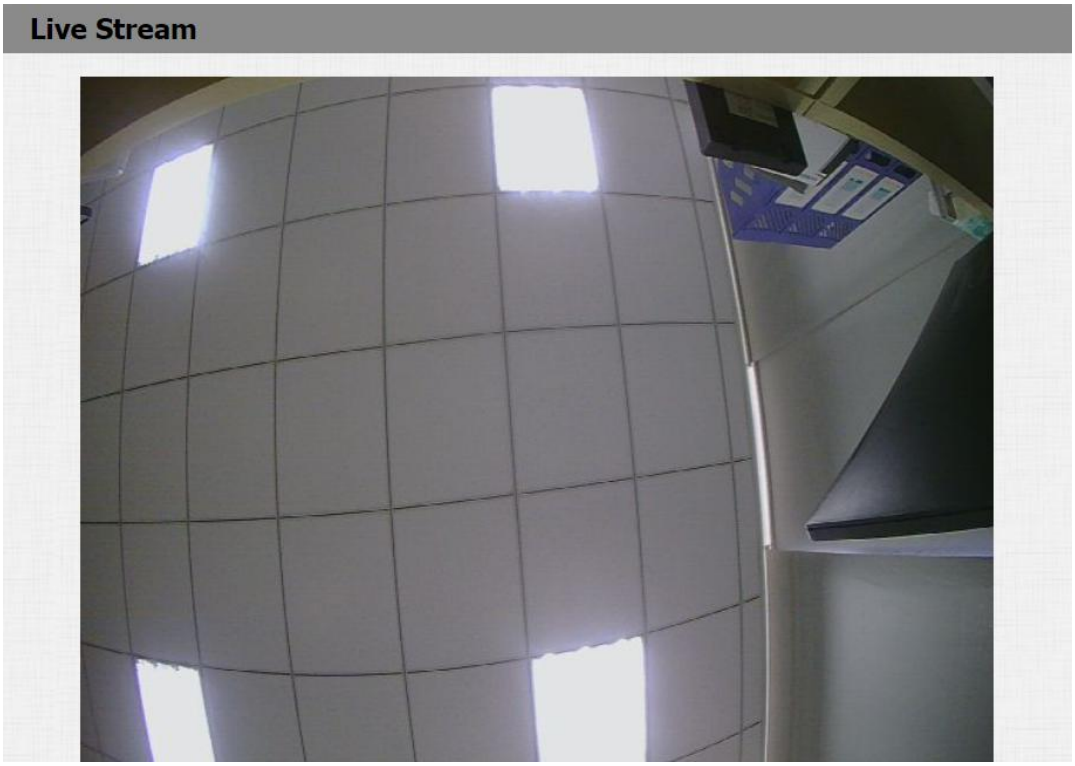
5.9. Monitor and Image

5.9.1. Live Stream

This feature is used to check the real-time video from door phone website, you can go the the device web interface to obtain the real-time video or you can also enter the correct URL on the we browser to obtain it directly.

To Check the real time video, you can do as follows:

1. Click **Intercom** - **Live Stream.**
2. Check the real time video on the web interface.
3. Enter the correct URL on the web browser if you want to obtain the real-time video directly with going to the web interface.



Parameters Set-up:

- **The video URL is:**

http://IP_address:8080/video.cgi

- **The picture URL is:**

http:// device ip:8080/picture.cgi

http://device ip:8080/picture.jpg

http://device ip:8080/jpeg.cgi

5.9.2. RTSP

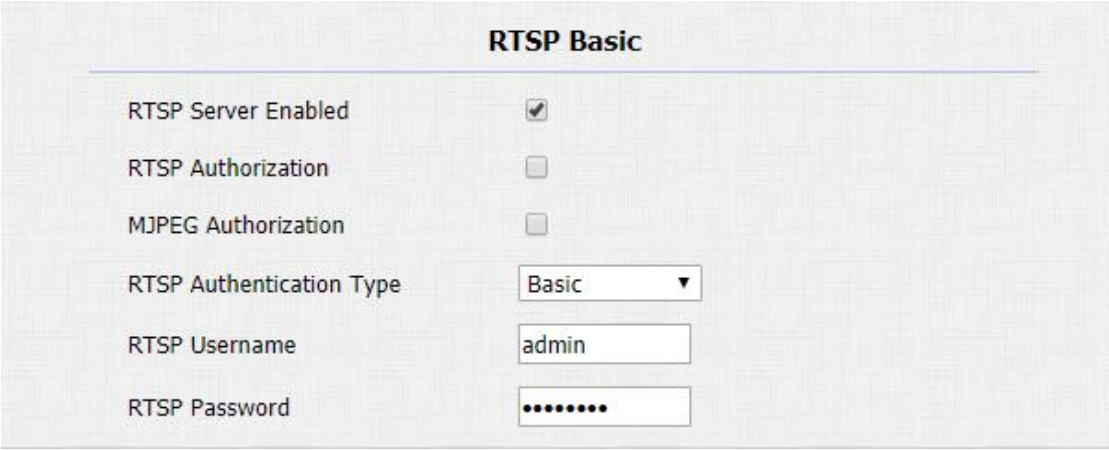
The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to controlstreaming media servers. The protocol is used for establishing and controlling media sessions between end points. RTSP, RFC2326, is an application layer protocol in the TCP/IP protocol system. This protocol defines how one-to-many applications can effectively transmit multimedia data through

an IP network.

R20B supports RTSP stream that allows intercom devices such as indoor monitor or the monitoring unit from the third party to monitor or obtain the the real time audio/ video (RTSP stream) from the door phone using the correct URL.

To do the configuration, you can do as follows:

1. Click **Intercom - RTSP** to find **RTPS Basic**.
2. Set up parameter properly.
3. Click **Submit** tab for validation and **Cancel** tab for Cancellation.



Parameters Set-up:

- **RTSP Enable:** Click on Enable and Disable in **RTSP Enable** field to turn on or turn off the RTSP function.
- **RTSP Authorization**: Click on Enable and Disable in RTSP Authorization field to enable or disable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, RTSP Password on the intercom device such as indoor monitor for authorization.
- **MJPEG Authorization:** If you use MJPEG video format for rtsp, you are required to enter the authentication information
- **RTSP User Name:** Enter the name used for RTSP/MJPEG authorization.
- **RTSP User Password:** Enter the password for RTSP/MJPEG

authorization.

- **RTSP Authentication Type:** Select RTSP authentication type between “ Basic” and “ Digest”. “Basic “ is the default authentication type.

Tip:

- **Basic authentication is an authentication scheme proposed by http 1.0, and its message transmission is not encrypted and converted, so there are serious security risks.**
- **Digest authentication is an alternative to the basic authentication proposed by http 1.1. The message is converted by MD5 hash, so it has higher security**

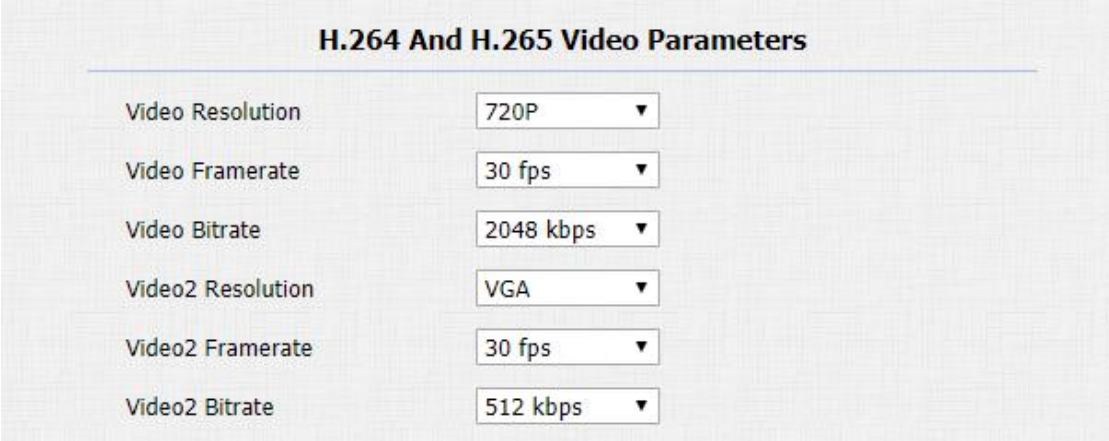
5.9.3. RTSP Stream Setting

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

5.9.3.1. H.264 And H.265 Video Codecs

To configure the parameters, please do as follows:

1. Click k **Intercom - RTSP** to find **H.264 And H.265 Video Parameters**.
2. Set up video parameters according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



Parameters Set-up:

- **Video Resolution:** Select video resolutions among seven option: "**QCIF**", "**QVGA**","**CIF**","**VGA**","**4CIF**","**720P**,""**1080P**". The default video resolution is "**720P.**
- **Video Framerate: "30fps"** is the video frame rate by default.
- **Video Bitrate**: Select video bit-rate among six options: "**128 kbps", "256kbps", "512 kbps", "1024 kbps", "2048 kbps", "4096 kpbs"** according to your network environment. The default video bit-rate is " **2048 kpbs**"
- **Video Resolution2:** Select video resolution for the second video stream channel. While the default video solution is "**VGA**"
- **Video Framerate2: "25fps"** is the video frame rate by default for the second video stream channel
- **Video Bitrate2:** Select video bit-rate among the six options for the second video stream channel. While the second video stream channel is "**512 kpbs**" by default

Note:

- **R20B supports two video stream channels for H.264 codec video stream, only one video stream channel for H.265 and MJPEG**
  rtsp://device IP address/live/ch00_0（The first RTSP stream）
  rtsp://device IP address/live/ch00_1（The second RTSP stream）

5.9.3.2. MJPEG Codecs

To configure the parameters, please do as follows:

1. Click **Intercom** - **RTSP** to find **MJPEG Video Parameters**.
2. Set up video parameters according to your need.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.

Parameters Set-up:

- **Video Resolution:** Select video resolutions among seven option: "**QCIF**", "**QVGA**","**CIF**","**VGA**","**4CIF**","**720P**,""**1080P**". The default video resolution is "**720P.**
- **Video Framerate: "30fps"** is the video frame rate by default.
- **Video Quality:** Video bitrate, the default is 90.

Note:

- **Video framerate and quality of MJPEG is fixed.**

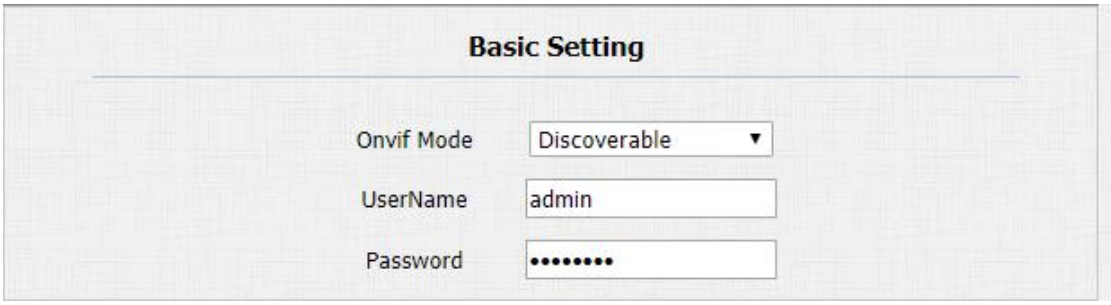
5.9.4. ONVIF

The ONVIF specification describes the network video model, interface, data type, and data interaction mode. And reuse some existing standards, such as WS series standards. The goal of the ONVIF specification is to implement a network video framework protocol, so that network video products (including

camera heads, video equipment, etc.) produced by different manufacturers are completely interoperable. After the setting is complete, you can enter the ONVIF URL on the third party device to view the video stream.

To do the configuration, you can do as follows:

1. Click **Intercom** - **ONVIF**.
2. Set up parameter properly.
3. Click **Submit** tab for validation and **Cancel** tab for cancellation.



Parameters Set-up:

- **Onvif Mode:** Select " **Discoverable**" or " **Non- Discoverable**" to turn on or turn off the the Onvfi mode. If you select " **Discoverable**" then the video from the door phone camera can be searched by other devices and vice versa. Onvif mode is " **Discoverable**" by default
- **UserName:** Enter the user name. The user name is " admin" by default
- **Password:** Enter the password. The password is " admin" by default.
- **The URL of Onvif:** http://IP address:80/onvif/device_service

5.10. Log

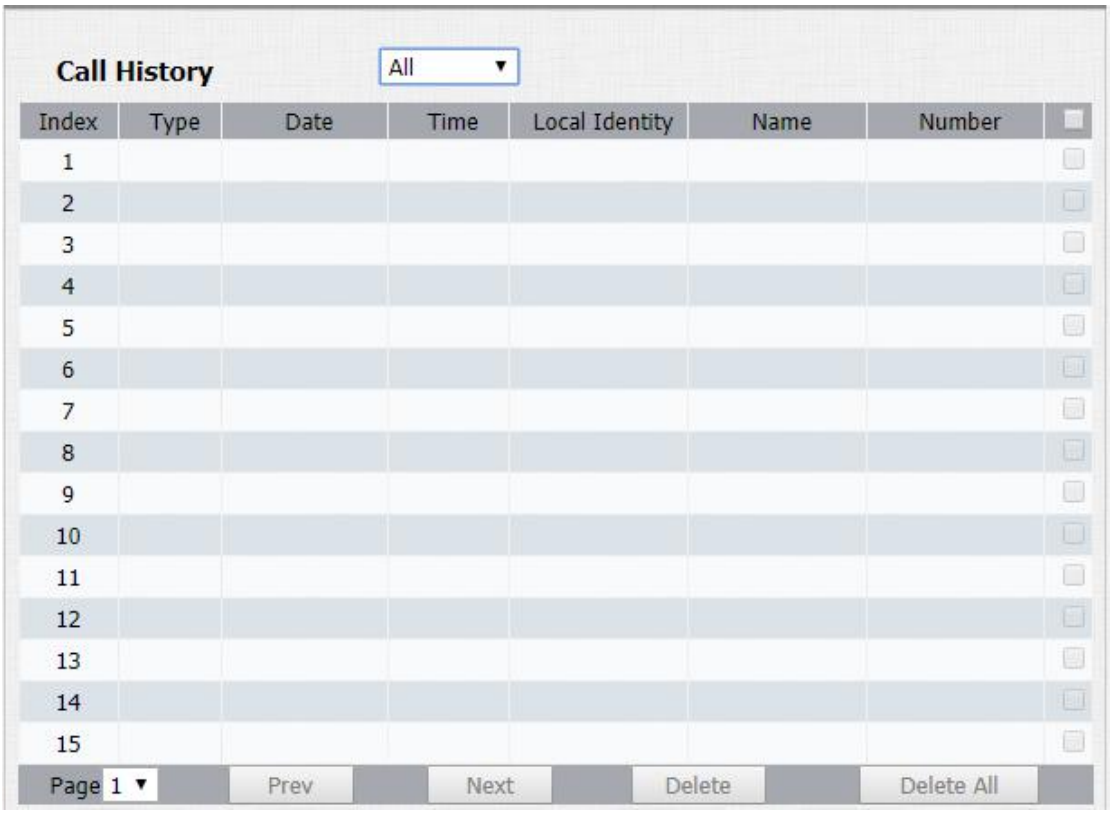
5.10.1. Call Log

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 interface and export the call log from the device if

needed.

To check the call log, you can do as follows:

1. Click **Phone** - **Call Log**.
2. Drop down **Call History** to filter call log type.
3. Click on the specific call log and click **Delete** tab to delete.
4. Click **Delete all** tab if you want to delete all of the call logs.



Parameters Set-up:

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

5.10.2. Door Log

If want to search and check on the various types of door access history, you can search and check the door logs on the device web interface.

To access the door logs , you can do as follows.

1. Click **Phone - Door log**.
2. Click on the specific door log and click **Delete** tab to delete.
3. Click **Delete all** tab if you want to delete all of the door logs.
4. Click **Export** Tab if you want to export the door log
5. Click **Import** Tab if you wan to import the existed door log

Note:

- **The import and export door log format is .xml**

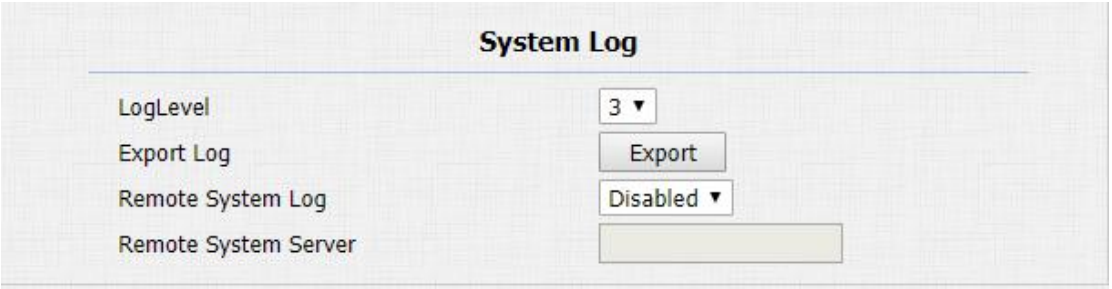
5.11. Debug

5.11.1. System Log for Debugging

System log in the door phone can be used for debugging purpose. System log records all operation log of device itself. If you want to export the system out to a local PC or to a remote server for debugging.

To set up the function, you can do as follows:

1. Click **Upgrade - Advanced** to find **System Log**.
2. Enter the parameters properly.
3. Click **Export** tab to export logs.
4. Click **Submit** tab for validation and **Cancel** for cancellation.



Parameters 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 level means the more specific syslog is saved to a temporary file.
- **Export Log:** Click the **Export** tab to export temporary debug log file to a local PC
- **Export Debug Log:** Click the **Export** tab to export debug log file to a local PC
- **Remote System Log:** Select “Enable” or “ Disable” if you wan to enable or disable the remote system log.
- **Remote System Server:** Enter the remote server address (URL) to

receive the the device log.

Note:

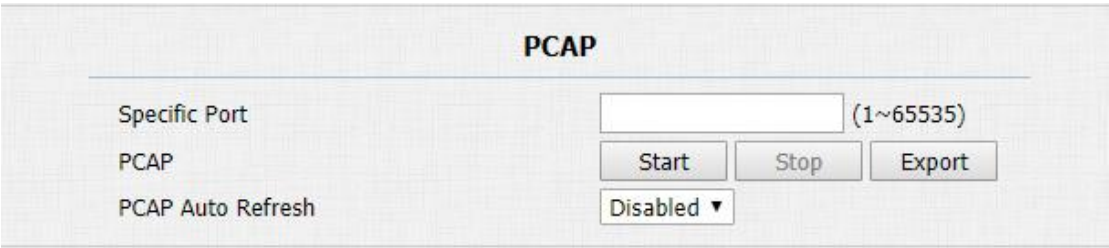
- **The remote system server is provided by Akuvox.**

5.11.2. PCAP for Debugging

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

To do the configuration, you can do as follows:

1. Click **Upgrade - Advanced** to find **PCAP**.
2. Set up parameters properly.
3. Start PCAP data packets capturing by clicking on **Start** tab.
4. Stop PCAP data packets capturing by clicking on the **Stop** tab.
5. Export the data packets captured by PCAP by clicking on **Export** tab.



Parameters Set-up:

- **Specific Port**: select the specific ports range from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click **Start** tab and **Stop** tab to capture the a certain range of data packets before clicking **Export** tab to export the data packets to you Local PC.

- **PCAP Auto Refresh**: select “Enable” or “ Disable” to turn on or turn off the PCAP auto fresh function. If you set it as “ Enable” then the PACP will continue to capture data packet even after the data packets reached its 1M maximum in capacity. If you set it as “ Disable” the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1M.

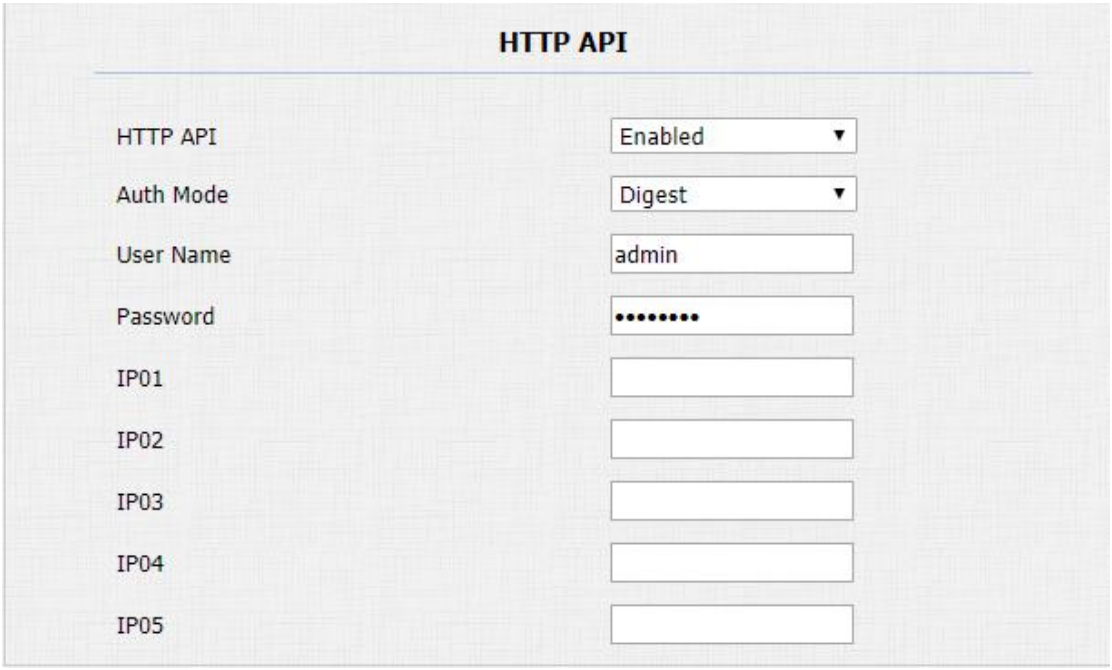
5.12. Integration

5.12.1. Integration via HTTP API

HTTP API is designed to achieve an network-based integration between the third party device with the Akuvox intercom device such R29 series door phone. You can configure the HTTP API function on the web interface for the integration.

To do the configuration, please do as follows:

1. Click **Intercom - HTTP API**.
2. Set up parameters properly.
3. Click **Submit** tab for validation and **Cancel** tab for Cancellation.



Parameters set-up:

- **HTTP API:** select "**Enable**" or " **Disable** " to enable or disable the HPTT API function for the third party integration. For example, if the function is disable any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** select among four options**: "None" " WhiteList" " Basic", " Digest"** for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "Admin"
- **Password:** enter the password when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "hattpapi"
- **IP01-IP05:** enter the IP address of the third party devices when the "WhiteList" authorization is select for the integration.

5.13. Password Modification

5.13.1. Modify Device's Web Interface Password

On the device web interface, you can access and change both the project passwords and setting password if needed.

1. Click **Security** - **Basic** to find **Web Password Modify**.
2. Chose the user name as admin or user
3. Click **Change Password** then enter the old password and new password
4. Click on **Change** tab for validation and **Ignore** tab for cancellation

Parameters Set-up:

- **User name:** There are two option admin or user.
- **Change Password:** Click to pop up the password modification windows.
- **Old Password:** If user name is admin, the default password is admin. If user name is user, the default password is user.
- **New Password:** The new password you need.
- **Confirm Password:** Enter the new password for double confirm.

Note:

- **The password is case sensitive.**

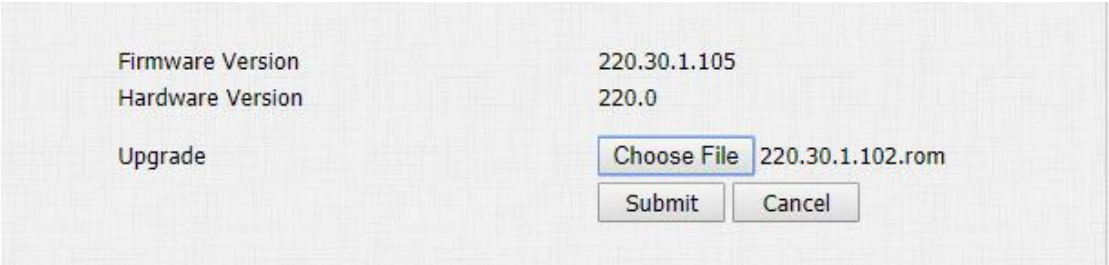
5.14. Firmware Upgrade

5.14.1. Web Upgrade

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

To upgrade the firmware, you can do as follows:

1. Click **Upgrade** - **Basic**.
2. Click **Choose File** to Select firmware files from your local PC.
3. Press **Submit** tab for the validation and **Cancel** tab for the cancellation.



Note:

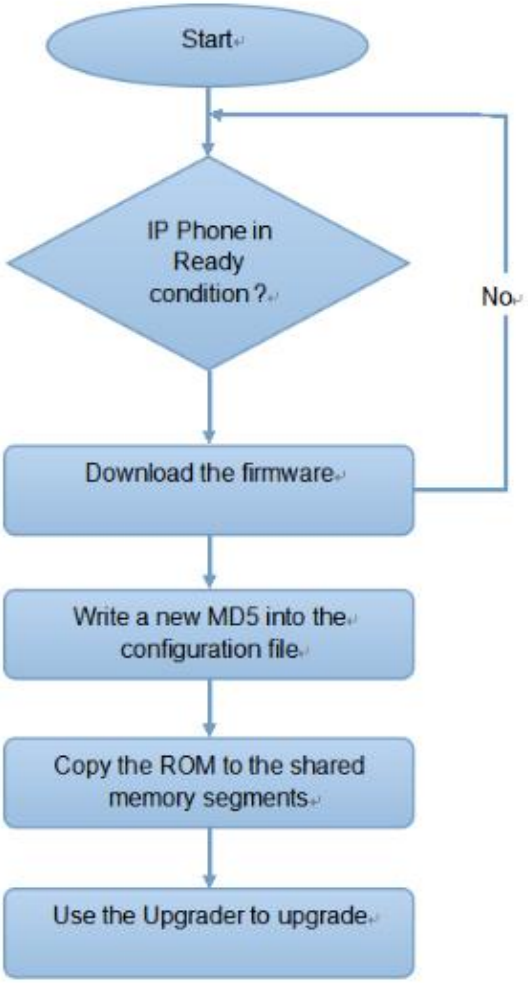
- **Firmware files should be .rom format for upgrade.**

5.15. Phone Provisioning

5.15.1. Provision Principle

Autop (Auto-Provisioning), this feature is used to configure or upgrade devices in batch via third party servers.

Akuvox products use DHCP/PNP/TFTP/FTP/HTTP/HTTPS network protocols to get URL, and then download firmware and/or its corresponding configuration files from that server. These configuration files and firmware will be used to update firmware and the corresponding parameters on the phone.



5.15.1.1. Config File

Automatic deployment has the following applications:

General configuration provisioning: In this scenario, a general configuration file is stored in the server and all devices download the same configuration file to update their parameters.

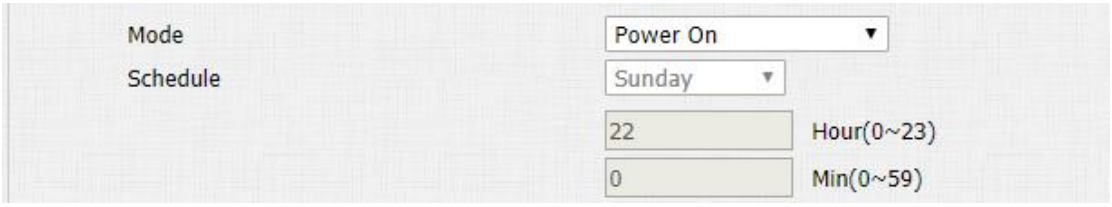
MAC based configuration provisioning: In this scenario, each configuration file is for a specific device with the MAC address that matches the file name. The parameters in this configuration file are for that specific device only. This is normally for the account related parameters.

If you have both of these files on the server, IP device will first get the General configuration file first and then get the MAC based configuration file using its MAC address as the ID.

5.15.1.2. AutoP Schedule

Akuvox provide different AutoP methods to let the device can do phone provisioning in a fixed time.

To setup schedule, you can do as follows:



Parameters Set-up:

- **Power On:** Device will start to do AutoP every time it boots up.
- **Repeatedly:** Device will start to do AutoP by following the predefined

schedule.

- **Power On + Repeatedly:** Combined with Power On mode and Repeatedly mode. Device will start to do AutoP when every time it boots up or by following the schedule.
- **Hourly Repeat:** Device will start to do AutoP every hour.

5.15.1.3. Procedure to setup AutoP

A complete automatic upgrade process consists of the following:

1. Administrator sets up the NPS and ACS servers with the required information;
2. Device gets the URL of the TFTP/FTP /HTTP/HTTPS server;
3. Device download the configuration file from the configuration server with URL.
4. If configuration file contains the content for updating any configurations or upgrading the firmware, device will get the firmware and do a firmware update.

By default, a profile resync is only attempted when Akuvox products are idle, because the upgrade might trigger a software reboot interrupting a call.

5.15.2. PNP for Autop

PNP stands for Plug and Play (Plug and Play). PNP provides a proprietary automatic upgrade, when PNP upgrade mode is enabled, the phone will broadcast a “SIP SUBSCRIBE” in the network. A SIP server will reply with a “SIP NOTIFY” with the URL of the firmware and/or configuration file server.

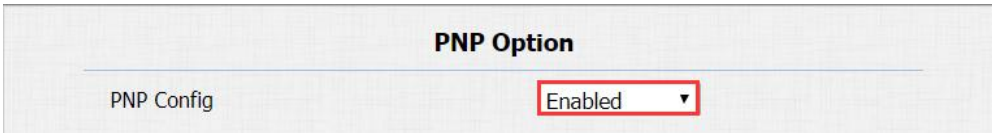
Tip:

- **Akuvox do not provide PNP server.**

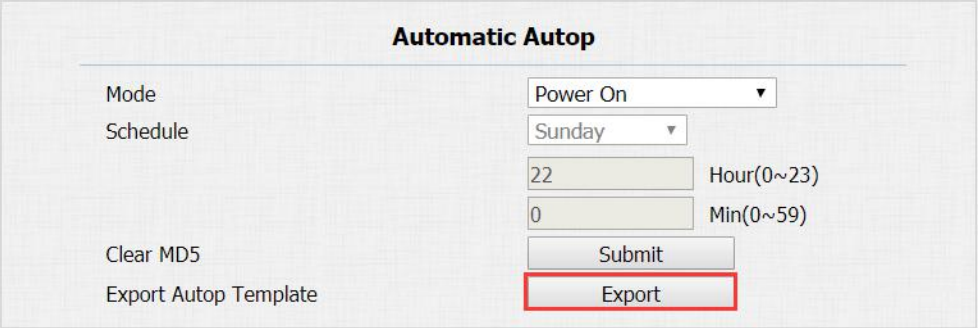
5.15.2.1. Procedures to setup PNP AutoP

To setup PNP AutoP, you can do as follows:

1. Click **Upgrade** - **Basic**.
2. Make sure PNP(Under the path “Upgrade-Advanced” on the web GUI of device) is enabled.



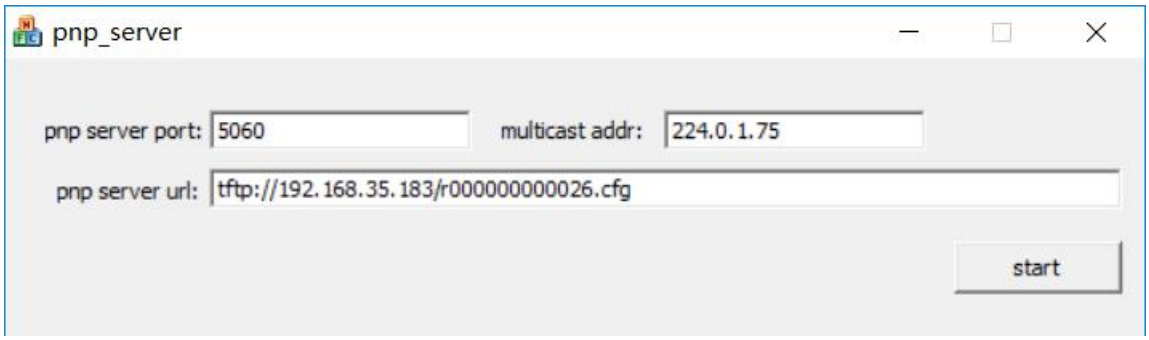
3. Export Autop template from **Export Autop Template**.



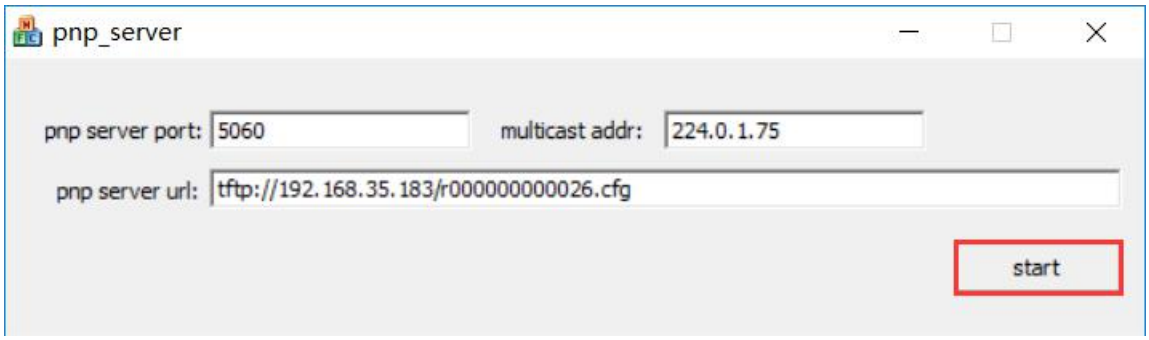
Following the steps to get PNP AutoP done(Under “Power On” mode):

1. Rename the AutoP config template(here we upgrade for mass devices, so make it general configuration provisioning).
2. For general configuration provisioning: r0000000000xx.cfg (There are 12 digits in total, for example: C315 -- r000000000115, R29 -- r000000000029)
3. For MAC based configuration provisioning:<MAC_Address of the device>.cfg, eg. 0C110504AE5B.cfg.

4. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server.
5. Edit AutoP config template.
6. Upload the AutoP config template to DHCP/TFTP/FTP/HTTP/HTTPS server.
7. Run PNP server and fill in the URL of AutoP config template.



8. Click start to start PNP AutoP.



9. Power on devices, they will start to upgrade after booting up.

Note:

- **Remember to turn off PNP server after AutoP done.**

5.15.3. Autop via User-Specified Server

Users can manually set a specific server URL for downloading the firmware or configuration file. If autop schedule is set, the phone will do the auto provisioning on the specified time frame as set in the autop schedule.

We can also use FTP, HTTP, or HTTPS as the protocol for upgrading the

device firmware or configuration.

Note:

- **The format of them are as follows:**

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

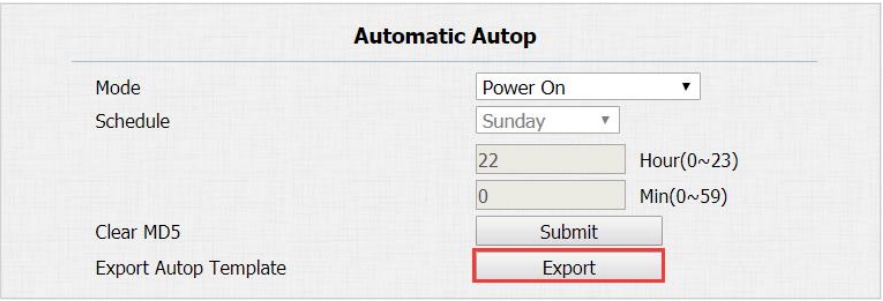
Tip:

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

5.15.3.1. Procedure to setup User-Specified AutoP

To setup user specified autop, you can do as follows:

1. Click **Upgrade** - **Basic**.
2. Export Autop template from **Export Autop Template**.

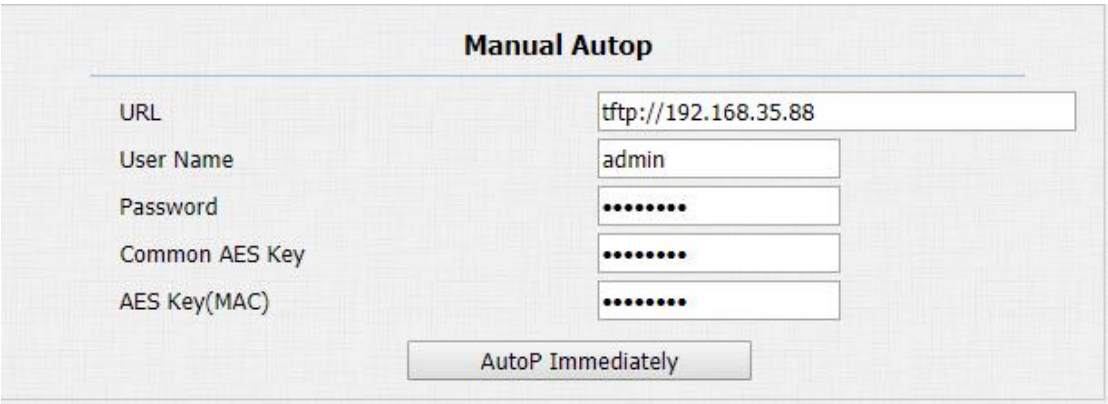


Following the steps to get User-Specified AutoP done:

1. Rename the AutoP config template (here we upgrade for mass devices, so

make it general configuration provisioning.);

2. For general configuration provisioning: r0000000000xx.cfg (There are 12 digits in total, for example: C315 --> r000000000115, R29 --> r000000000029)
3. For MAC based configuration provisioning: <MAC_Address of the device>.cfg, eg. 0C110504AE5B.cfg.
4. Upload firmware to DHCP/TFTP/FTP/HTTP/HTTPS server;
5. Edit AutoP config template;
6. Upload the AutoP config template to DHCP/TFTP/FTP/HTTP/HTTPS server;
7. Enter TFTP URL into the box(under the path “Upgrade-Advanced”) and click AutoP Immediately
8. You can also power device up to make it work when PNP server is disabled



5.16. Backup

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

To do so , you can do as follows:

1. Click **Upgrade** - **Advanced** to to find **Others**.
2. Select config file to be imported.

3. Click **Import** tab if you want to import the selected config file
4. Click **Export** tab if you want to export the existing config files to you local PC.

Note:

- **The import file can be .tgz/.conf/.cfg format.**
- **The exported config file is encrypted.**
- **The default exported fiels is config.tgz.**
- **The exported config file includes.**

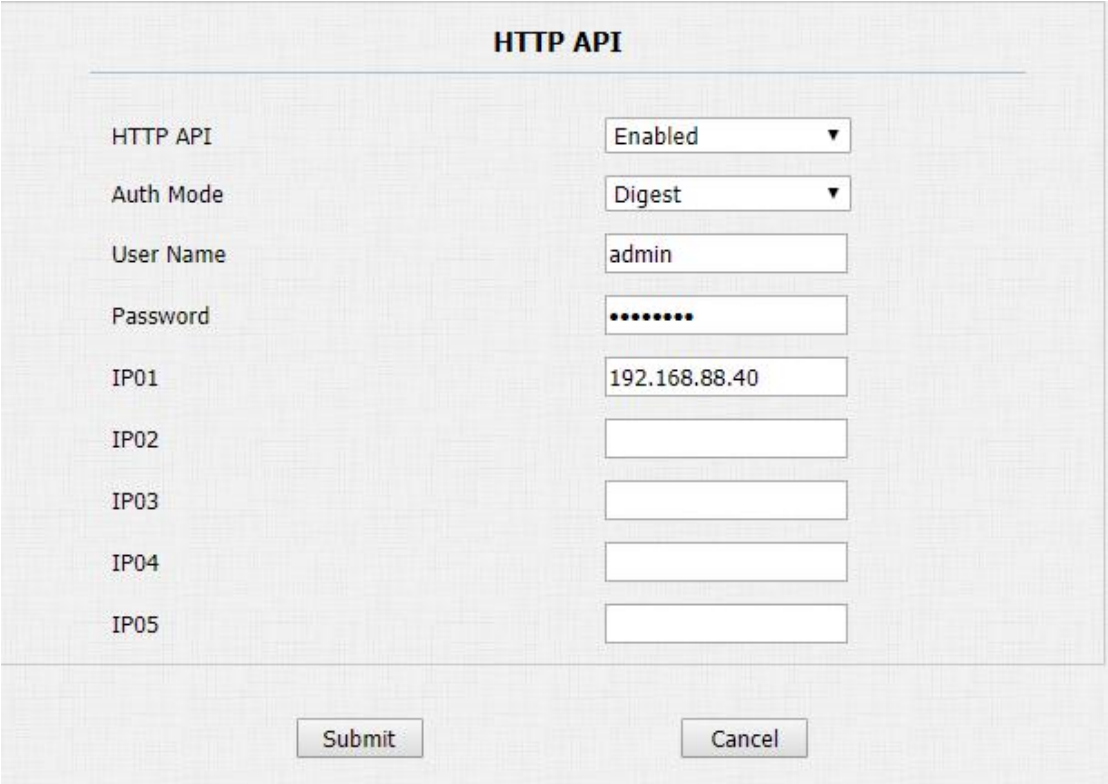
5.17. Integration

5.17.1. Integration via HTTP API

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

To do the configuration, please do as follows:

1. Click **Intercom - HTTP API**.
2. Set up parameters properly.
3. Click **Submit** tab for validation and **Cancel** tab for Cancellation.



Parameters set-up:

- **HTTP API:** select "**Enable**" or " **Disable** " to enable or disable the HPTT API function for the third party integration. For example, if the function is disable any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** select among four options**: "None" " WhiteList" " Basic", " Digest"** for authorization type, which will be explained in detail in the following chart.
- **User Name:** enter the user name when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "Admin"
- **Password:** enter the password when "**Basic**" and **"Digest**" authorization mode is selected. The default user name is "hattpapi"
- **IP01-IP05:** enter the IP address of the third party devices when the "WhiteList" authorization is select for the integration.

5.18. System reboot/reset

5.18.1. Reboot

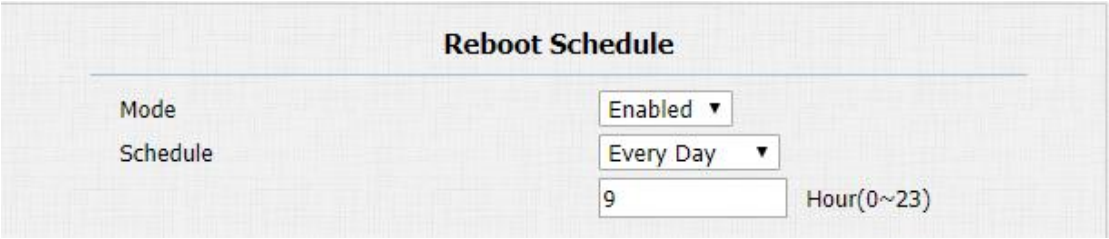
If you want to restart the device system, you can operate it on the device web interface . More over, you can set up schedule for the device to be restarted.

To restart the system setting on the web interface, you can do as follows:

1. Click **Upgrade** - **Basic**.
2. Click on **Submit** tab for **Reboot**.

To set up the device restart schedule, you can do as follows:

1. Click **Upgrade** - **Advanced** to find **Reboot Schedule**.
2. Enable the scheduled Reboot mode.
3. Set up the device restart day and timing (0-23).
4. Press **Submit tab** for the validation and **Cancel** tab for the Cancellation.



Parameters Set-up:

Schedule: Setup it as " Every Day" "Sunday" "Monday" "Tuesday" "Wednesday" "Thursday" "Friday" "Saturday" " Every Month"

5.18.2. Reset

Device system can be reset on device web interface without approaching the

device.

To reset the device on the web interface, you can do as follows:

1. Click **Upgrade** - **Basic**.
2. Click on Reboot **Submit** tab to reset the device system setting.

6. 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

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

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ-Law

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

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

7. FAQ

Q1: How to obtain IP address of R2X

✔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: Do Akuvox devices support Modbus protocol?

A4: No.

Q4: Which version of ONVIF do R20B support?

A55: Onvif 18.04 profiles

Q6: Do door phone support these card types? Prox, Legacy iClass,iClassSE,HID Mifare, HID DESFire,HID SEOS

A6: Sorry, they are not supported. They need to be implemented via hardware modifications.

- **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.

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

We highly appreciate your feedback about our products.

FCC Statement:
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,
(2) This device must accept any interference received, including interference t 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.