About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

E21
DOOR PHONE
Administrator Guide

Thank you for choosing Akuvox E21 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to versions 321.30.1.110 or above.

Please visit Akuvox forum or consult technical support for any new information or latest firmware.

Product Overview

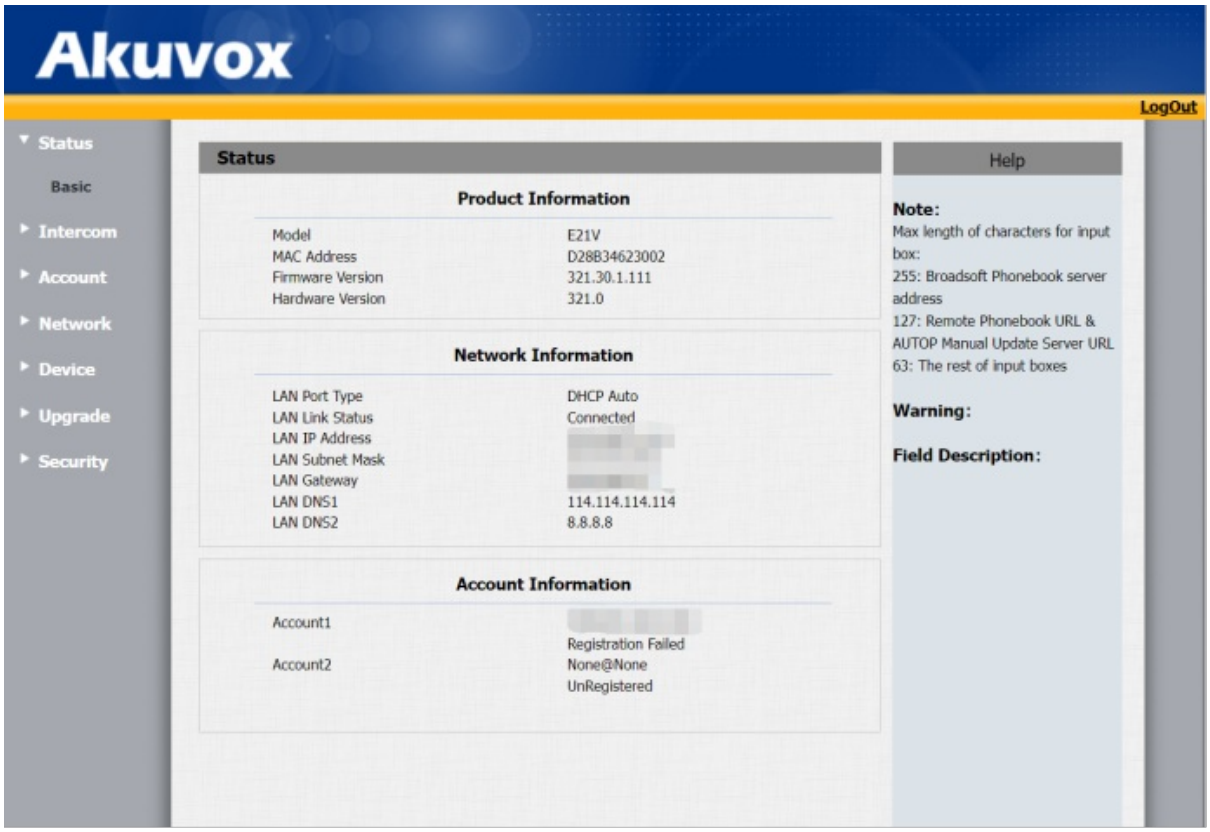
The security that comes with being able to control who comes into your building along with the ability to verbally and visually confirm their identity is immeasurable. Akuvox E21 series is SIP-compliant door phones. They can be connected with Akuvox indoor monitors for remote access controlling and monitoring. Users can communicate with visitors via audio and video calls, and unlock the door if they need. The door phone enables you to easily monitor an entrance door or gate and gives you the peace of mind knowing that your facility is more secure.

Model Specification

Model	E21V	E21A
Camera	2 Mega pixels, automatic lighting	X
Relay In	2	2
Relay Out	2	2
RS485	X	X
WiFi	X	X
Card Reader	X	X

Introduction to Configuration Menu

- **Status**: this section gives you basic information such as product information, Network information, and account information, etc.
- **Intercom**: this section covers intercom settings, motion detection, RTSP, MJPEG, ONVIF, live stream etc.
- **Account**: this section concerns SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.
- **Network**: this section mainly deals with DHCP&Static IP setting, RTP port setting, and device deployment, etc.
- **Device**: this section includes time&language, action settings, door settings, schedule for access control.
- **Upgrade**: this section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, fault diagnosis.
- **Security**: this section is for password modification.

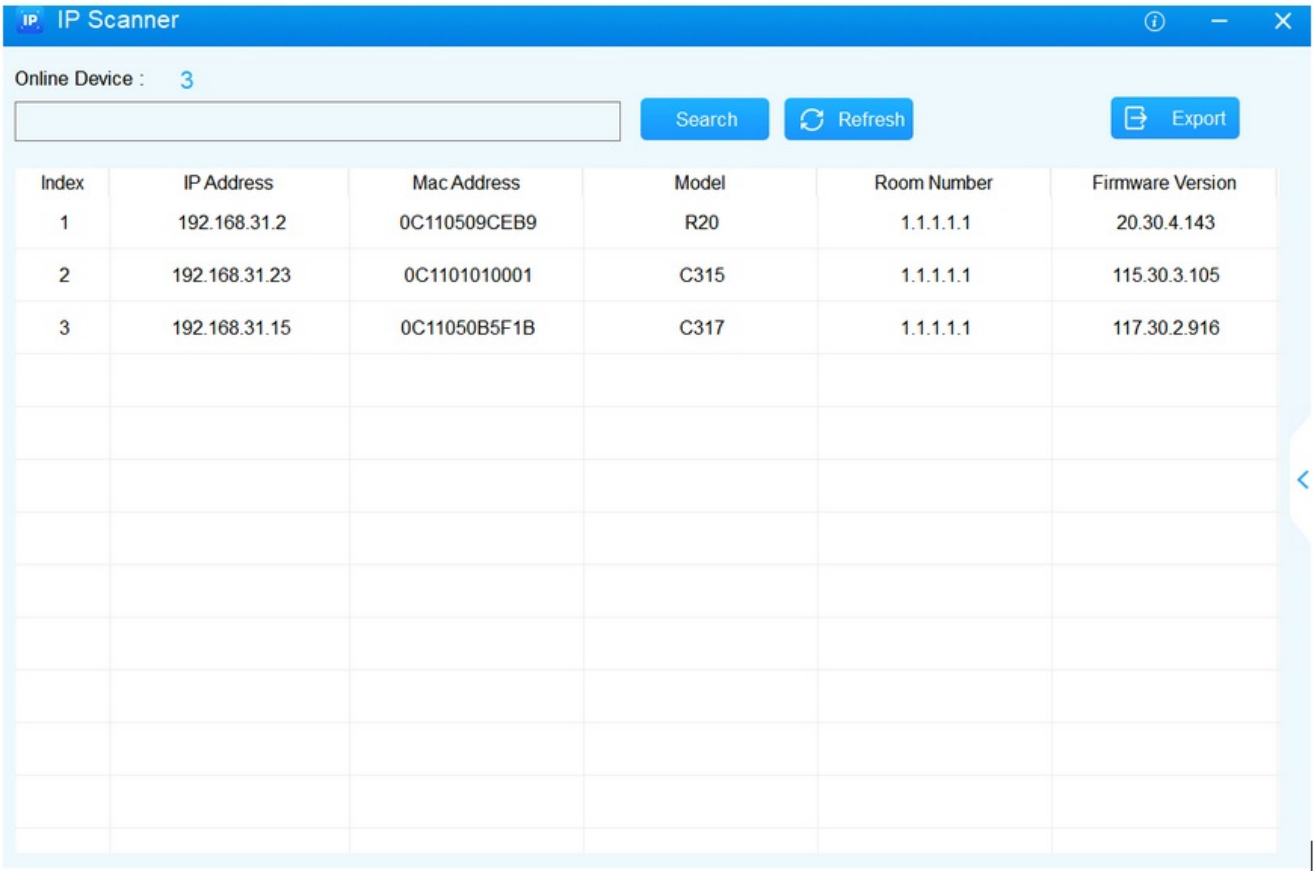


Access the Device

Door phones' system settings can be either accessed on the device directly or on the device web interface.

Obtain Device IP Address

Check the device IP address by holding the push button for 5s. Or searching the device IP by the IP scanner in the same LAN network.

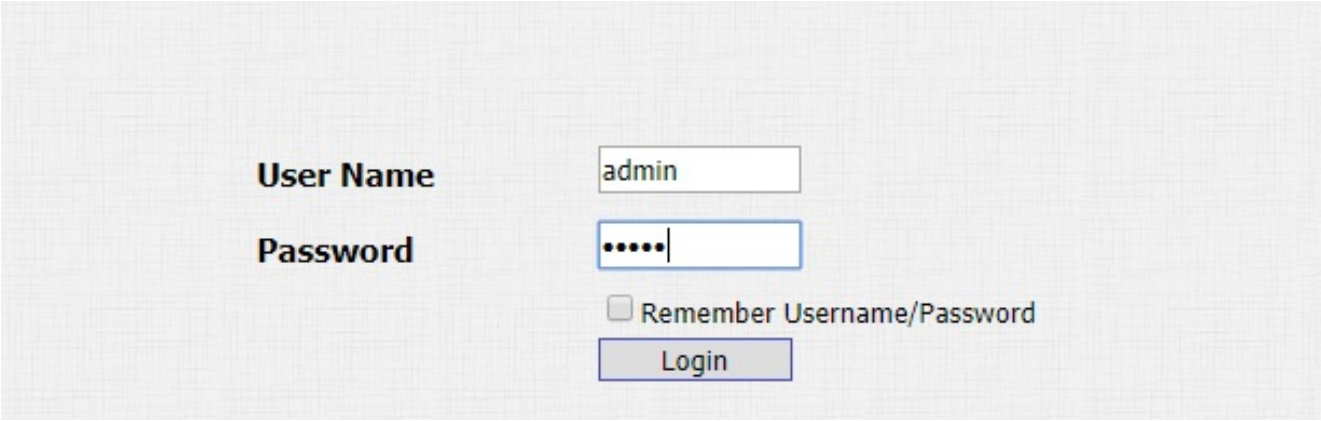


Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.31.2	0C110509CEB9	R20	1.1.1.1.1	20.30.4.143
2	192.168.31.23	0C1101010001	C315	1.1.1.1.1	115.30.3.105
3	192.168.31.15	0C11050B5F1B	C317	1.1.1.1.1	117.30.2.916

Access the Device Setting on the Web Interface

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

The initial user name and password are both **admin** and please be case-sensitive to the user names and passwords entered.



Note

You can also obtain the device IP address using the Akuvox IP scanner to log into the device web interface.

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.

Language and Time Setting

Language Settin

Language can be set up on the device web **Device > Time/Lang > Web Language** interface according to your preference.

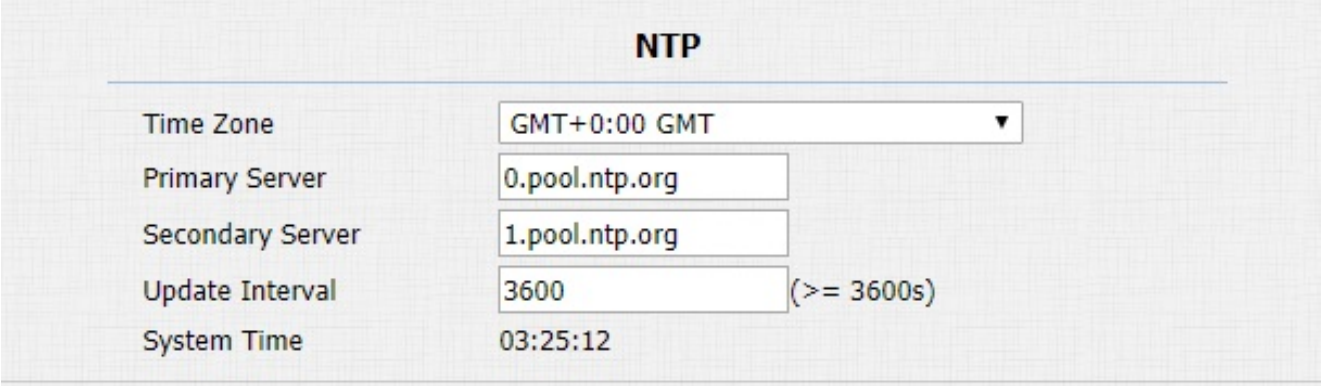
Parameter Set-up:

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

Time Setting

Time settings on the web interface allows you to set up the NTP server address that you obtained to automatically synchronize your time and date. When a time zone is selected, the device will automatically notify the NTP server of the time zone so that the NTP server can synchronize the time zone setting in your device.

You can navigate to **Device > Time/Lang > NTP**.



Parameter Set-up:

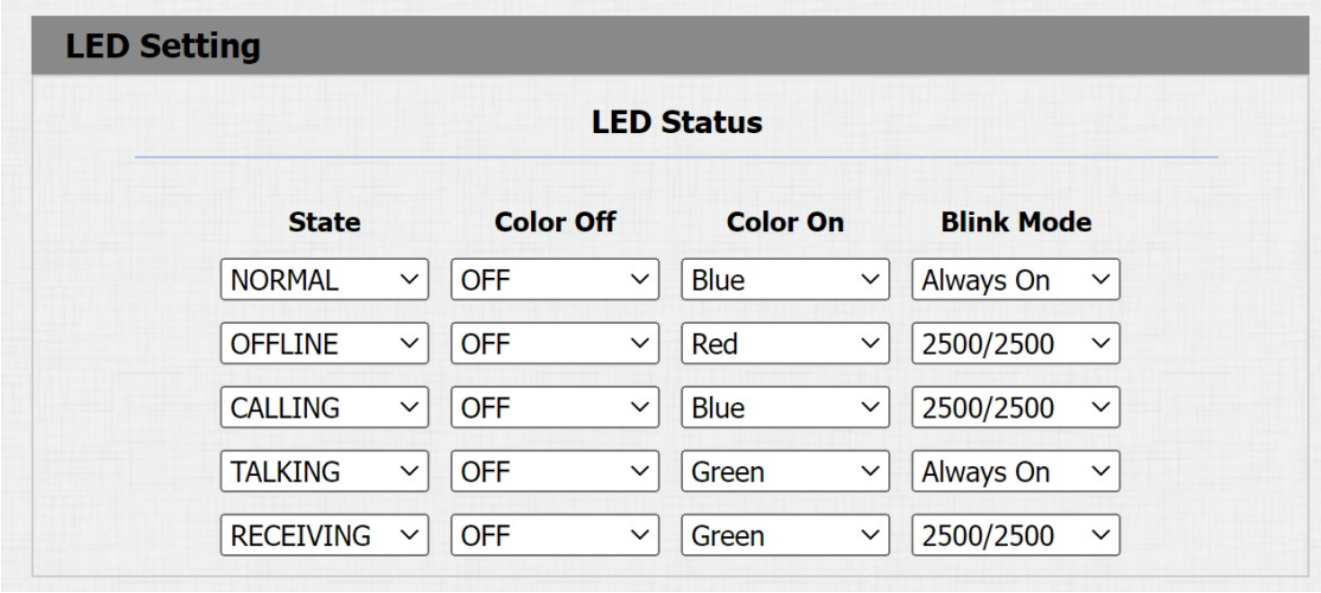
- **Preferred/Alternate Server**: enter the NTP server address. The alternate server will take effect when the primary server is invalid.
- **Update Interval**: to configure the interval between two consecutive NTP requests.

LED Setting

Infrared LED Setting

Infrared LED is mainly designed to reinforce the light for facial recognition at night or in a dark environment, you can configure the infrared LED on the web interface.

You can navigate to **Intercom > LED Setting > LED Setting**.



The default LED Display Status:

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

Parameter Set-up:

- **State**: there are five states: **Normal, Offline, Calling, Talking**, and **Receiving**.
- **Color Off**: you can turn off LED light.
- **Color On**: set color of LED light, it can support four colors: **Red, Green, Blue, Yellow**.
- **Blink Mode**: select **Always ON** to enable the Infrared LED light to stay on permanently. Select **Always OFF** to turn off the Infrared LED light. Or, you can set up the different blink frequencies.

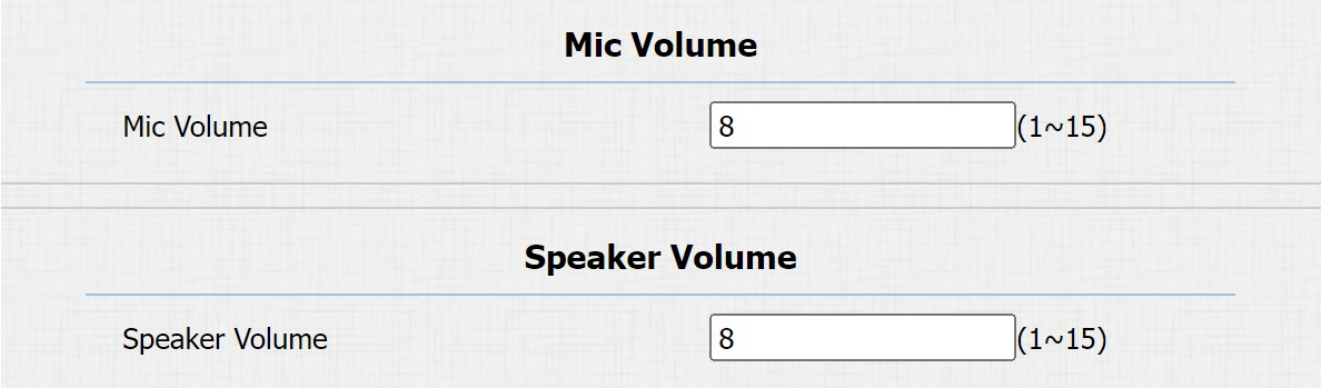
Volume and Tone Configuration

Volume and tone configuration include microphone volume, the AD volume, keypad volume, speaker volume, tamper alarm volume, and open-door tone configuration. Moreover, you can upload the tone you like to enrich your personalized user experience.

Volume Configuration

You can configure the Mic volume according to your need for open-door notification. Moreover, you can also set up the tamper alarm volume when unwanted removal of the access control terminal occurs.

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

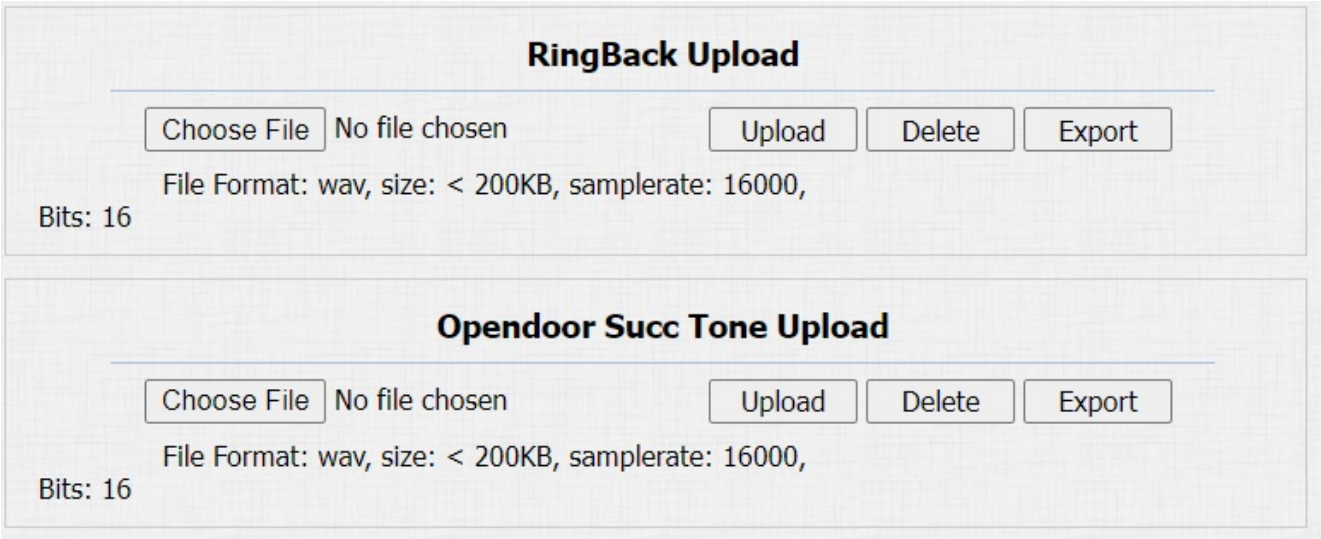


Open Door Warning

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

Upload Tone Files

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



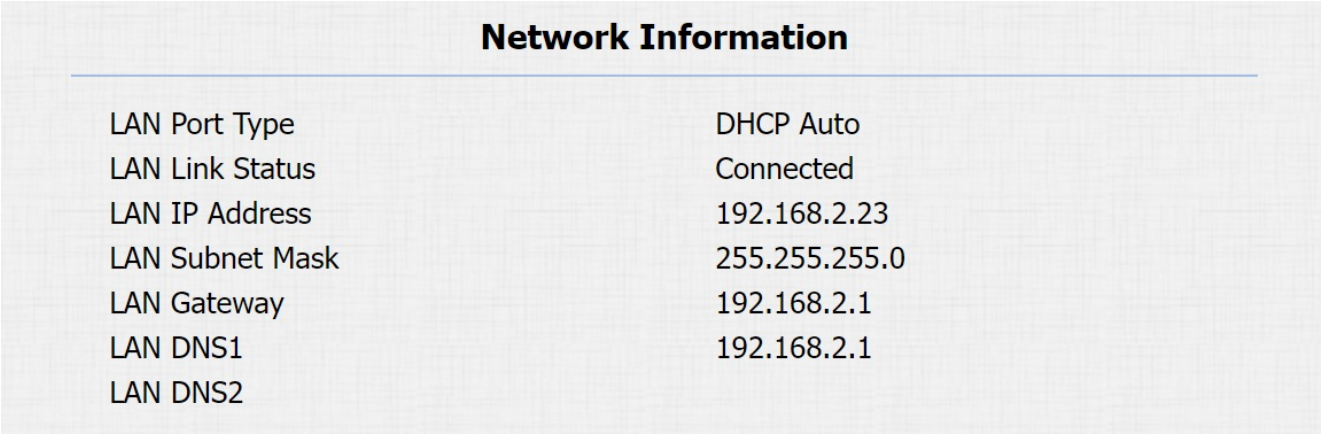
Parameter Set-up:

- **RingBack**: the tone that will go off when you call others.
- **Open Door Success Tone Upload**: upload the tone that will go off when you open door successfully.

Network Setting

Network Status

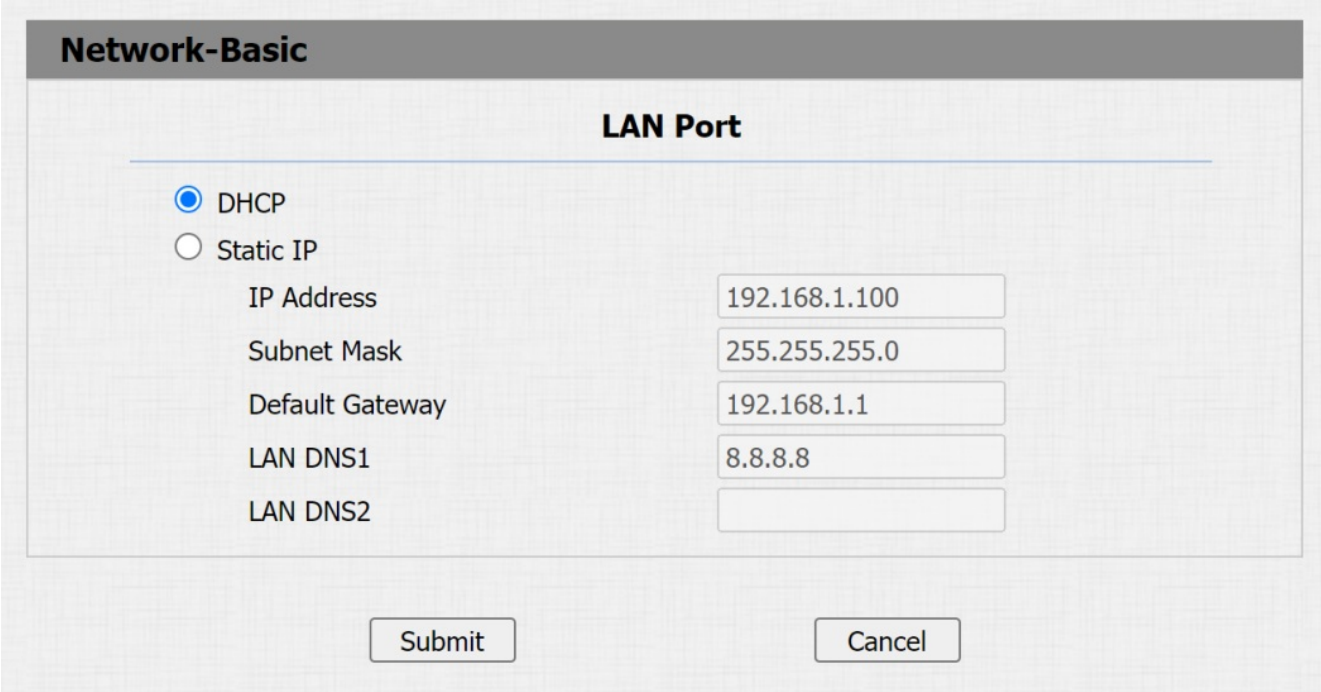
To check the network status on the web **Status > Network Information** interface.



Device Network Configuration

To ensure normal functioning, make sure that the device has its IP address set correctly or obtained automatically from the DHCP server.

Navigate to **Network > Basic** interface..



Parameter Set-up:

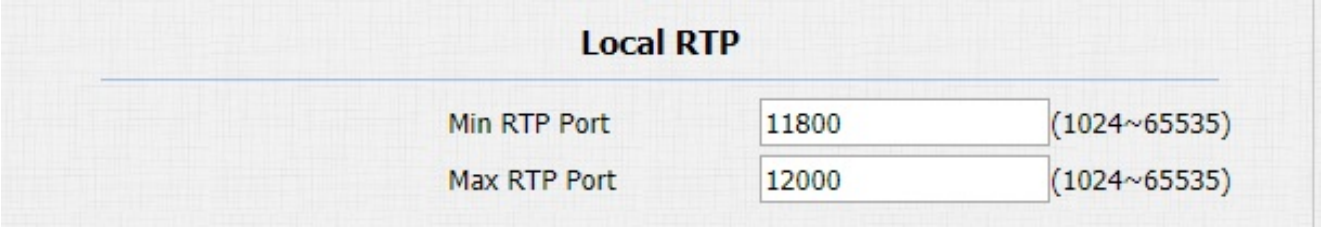
- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP**: When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway default gateway according to the IP address of the default gateway.
- **LAN DNS1/ LAN DNS2**: set up preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address and the door phone will connect to the alternate server when the primary DNS server is unavailable.

Device Local RTP configuration

Real-time Transport Protocol(**RTP**) lets devices stream audio and video data over a network in real time.

To use RTP, devices need a range of ports. A port is like a channel for data on a network. By setting up RTP ports on your device and router, you can avoid network interference and improve audio and video quality.

Path: **Network > Advanced > Local RTP** interface



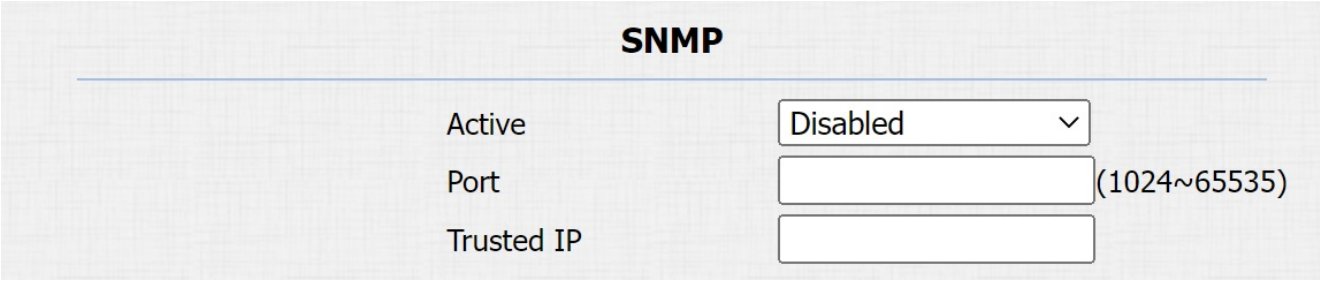
Parameter Set-up:

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

SNMP Setting

Simple Network Management Protocol(**SNMP**) is a protocol for managing IP network devices. It allows network administrators to monitor devices and receive alerts for attention-worthy conditions. SNMP provides variables describing system configuration, organized in hierarchies and described by Management Information Bases (MIBs).

To do the configuration on the web **Network > Advanced > SNMP** interface.



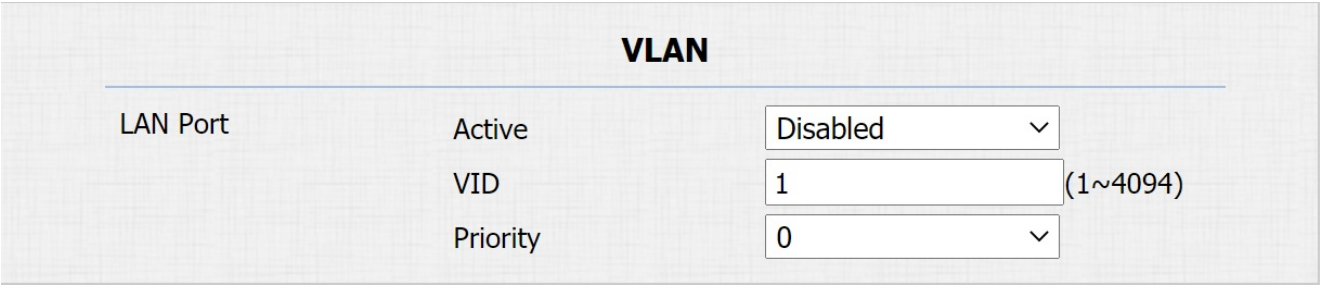
Parameter Set-up:

- **Trusted IP**: to configure allowed SNMP server address. It could be an IP address or any valid URL domain name.

VLAN Setting

A Virtual Local Area Network (VLAN) is a logical group of nodes from the same IP domain, regardless of their physical network segment. It separates the layer 2 broadcast domain via switches or routers, sending tagged packets only to ports with matching VLAN IDs. Utilizing VLANs enhances security by limiting ARP attacks to specific hosts and improves network performance by minimizing unnecessary broadcast frames, thereby conserving bandwidth for increased efficiency.

To do the configuration on the web **Network > Advanced > VLAN** interface.



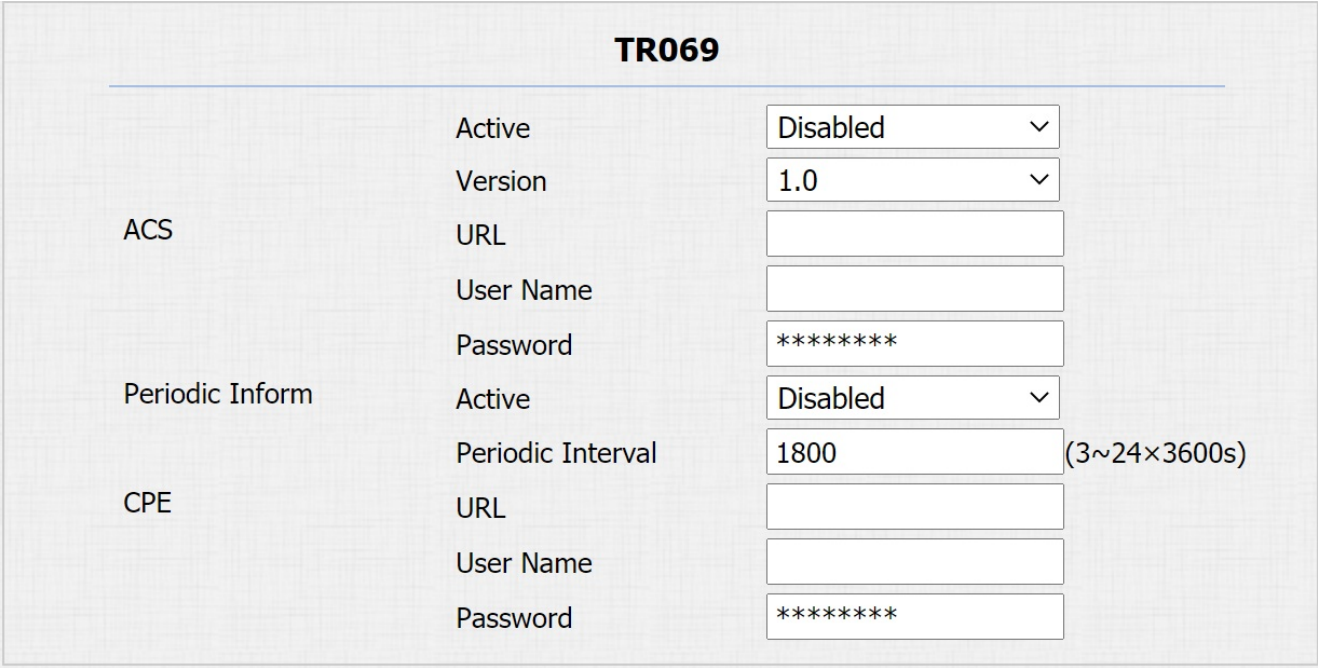
Parameter Set-up:

- **Priority**: to select VLAN priority for designated port.

TR069 Setting

TR-069 (Technical Report 069) provides the communication between Customer-Premises Equipment (CPE) and Auto-Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. For door phones, the administrators can manage all the devices on a common TR-069 Platform. IP phones can be easily and securely configured on the TR-069 platform to make mass deployment more efficient.

To do the configuration on the web **Network > Advanced > TR069** interface.



Parameter Set-up:

- **Version**: to select supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE**: ACS is short for auto configuration servers as server side, and CPE is short for customer-premise equipment as client side devices.

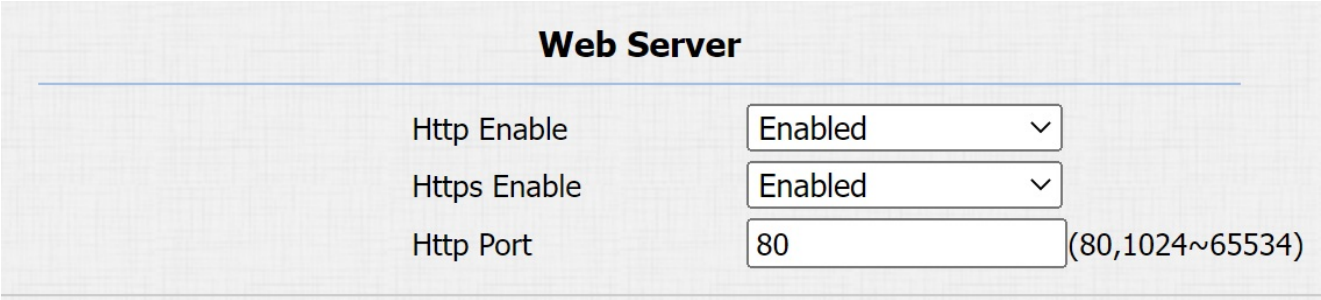
Note

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

Device Web HTTP Setting

This function manages device website access. The door phone supports two remote access methods: HTTP and HTTPS (encryption).

To do this configuration on the web **Network > Advanced > Web Server** interface.



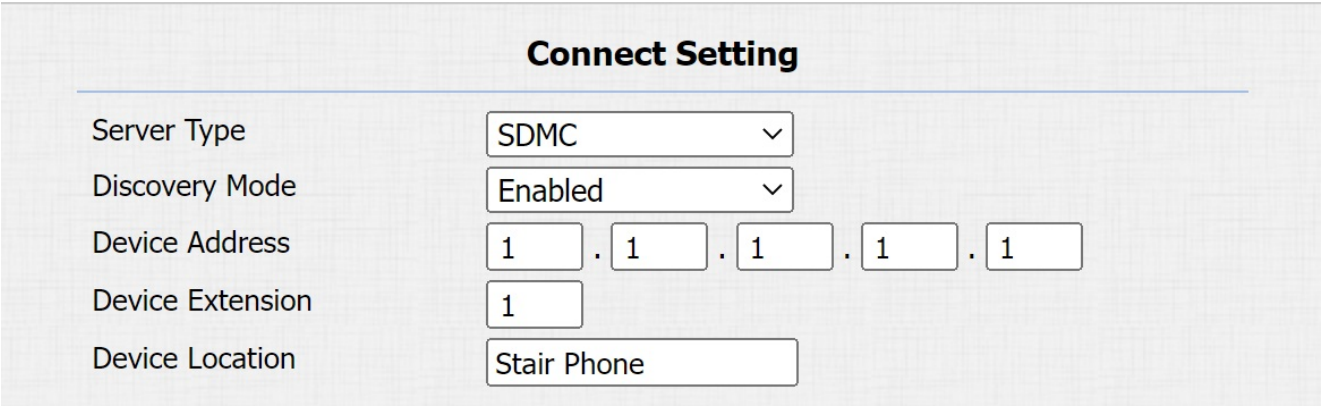
Parameters Set-up:

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

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

So you can do it on web **Network > Advanced > Connect Setting** interface.



Parameter Set-up:

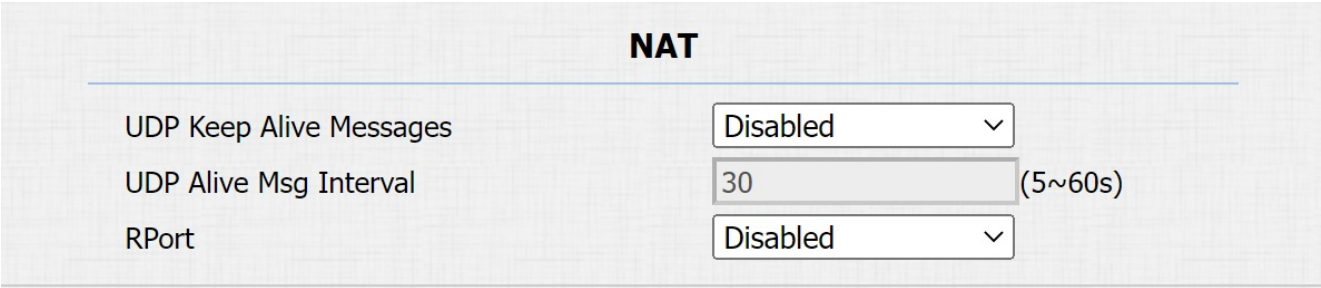
- **Server Mode**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC** or **Cloud** and **None**. **SDMC** is the default factory setting.

- **Discovery Mode**: click **Enable** to turn on the discovery mode of the device so that it can be discovered by other devices in the network, and click **Disable** if you want to conceal the device so as not to be discovered by other devices.
- **Device Address**: specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension**: enter the device extension number for the device you installed.
- **Device Location**: enter the location in which the device is installed and used.

NAT Setting

Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

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



Parameter Set-up:

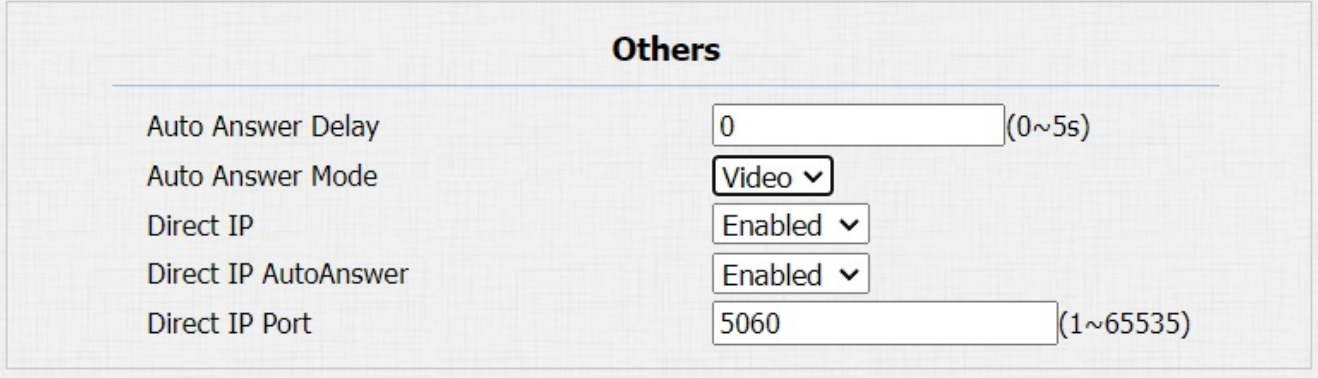
- **UDP Keep Alive Messages**: if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval**: set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort**: enable the RPort when the SIP server is in WAN (**Wide Area Network**).

Intercom Call Configuration

IP Call & IP Call Configuration

An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Path: **Device > Call Feature > Others**



Parameters Set-up:

- **Direct IP**: choose **Enabled** or **Disabled** to turn the direct IP call on or off. For example, if you do not allow direct IP call to be made on the device, you can click **Disable** to terminate the function.
- **Port**: set up the IP direct call port, 5060 is the default port.

SIP Call & SIP Call Configuration

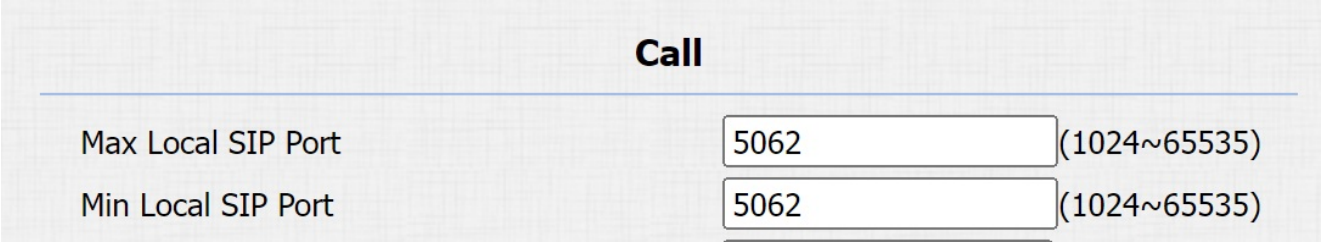
Session Initiation Protocol(**SIP**) is a signaling transmission protocol used for initiating, maintaining, and terminating calls.

A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Port

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

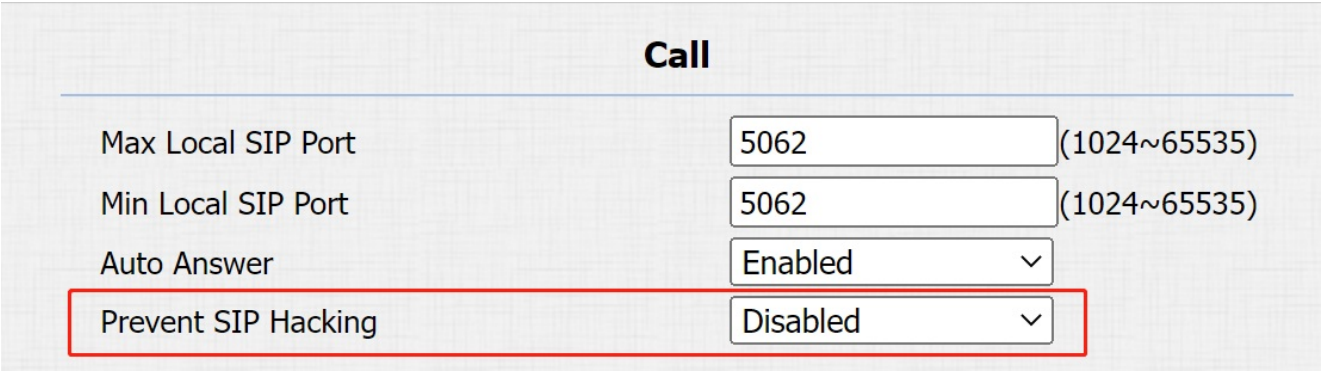
Path: **Account > Advanced > Call**.



Prevent SIP Hacking

Internet phone eavesdropping is a network attack that allows unauthorized parties to intercept and access the content of the communication sessions between intercom users. This can expose sensitive and confidential information to the attackers. SIP hacking protection is a technique that secures SIP calls from being compromised on the Internet.

To enable this function on **Account > Advanced > Call** interface.

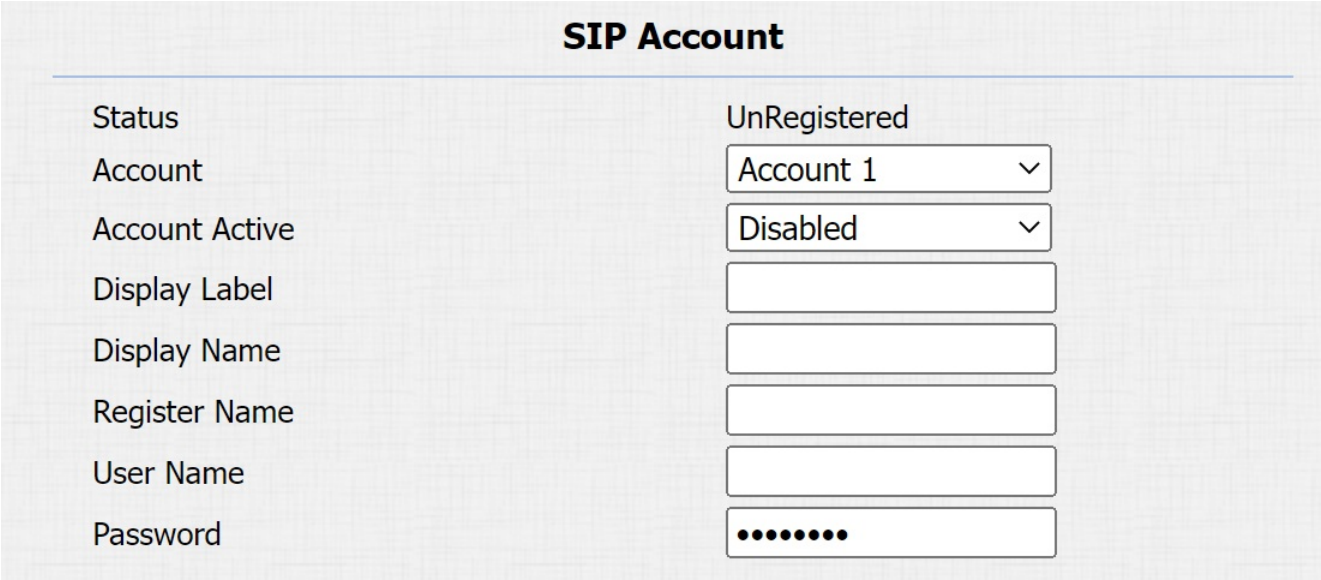


SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

To perform the SIP account setting on the web **Account > Basic > SIP Account** Interface. **Register Name, User Name**, and** Password** are provided by the SIP account administrator.



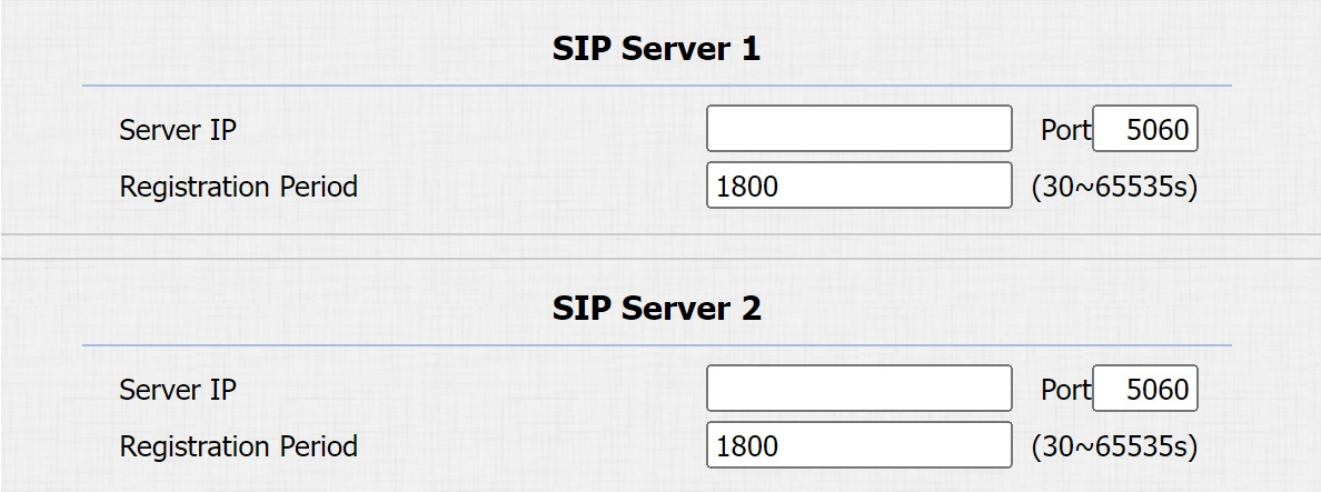
Parameter Set-up:

- **Status**: check to see if the SIP account is registered or not.
- **Account**: select the exact account (Account 1&2) to be configured.
- **Display Label**: configure the device label to be shown on the device screen.
- **Display Name**: configure the name, for example, the device's name to be shown on the device being called to.

SIP Server Configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

To do this configuration also on web **Account > Basic > SIP Server** interface.



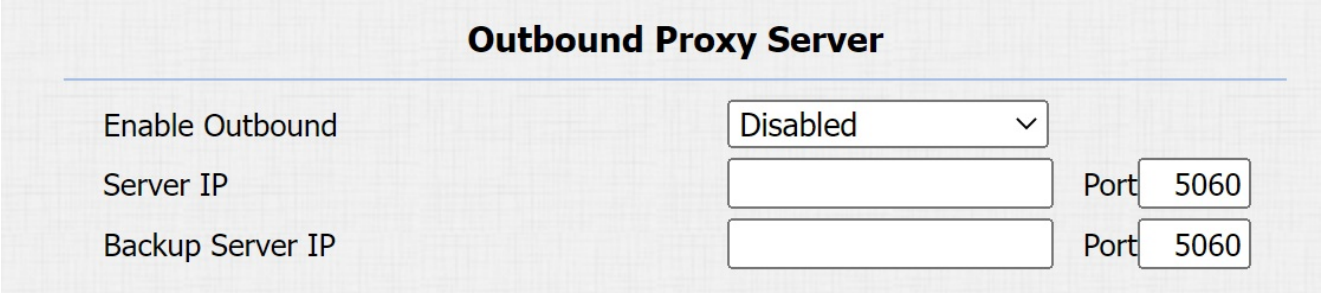
Parameter Set-up:

- **SIP Server 1**: enter the primary server IP address number or its URL.
- **SIP Server 2**: enter the backup SIP server IP address or its URL.
- **Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is "**1800**", ranging from **30-65535**s.

Configure Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission.

To do this configuration also on web **Account > Basic > Outbound Proxy Server** interface.



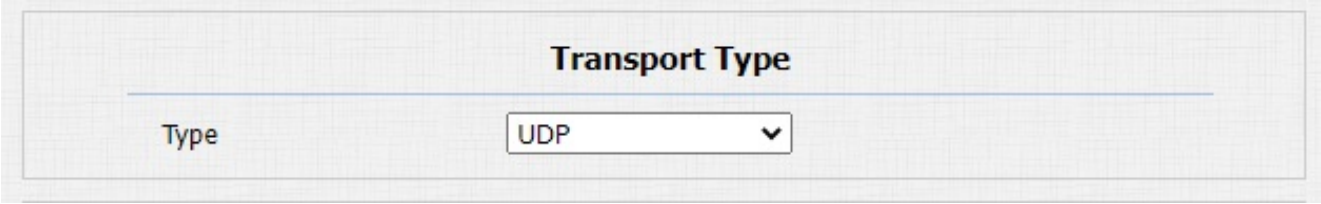
Parameter Set-up:

- **Server IP**: enter the SIP address of the primary outbound proxy server.
- **Backup Server IP**: set up Backup Server IP for the backup outbound proxy server.
- **Port**: enter the port number for establishing call session via the backup outbound proxy server.

Configure Data Transmission Type

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

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



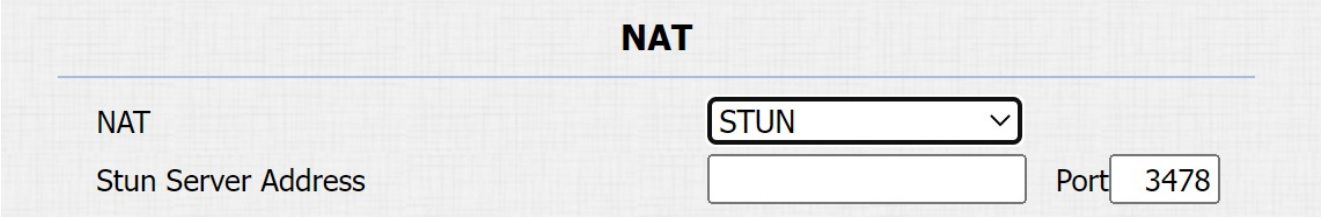
Parameter Set-up:

- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for teliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for secured and reliable transport layer protocol.

Configure NAT

Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

Path: **Account > Basic > NAT**



Parameter Set-up:

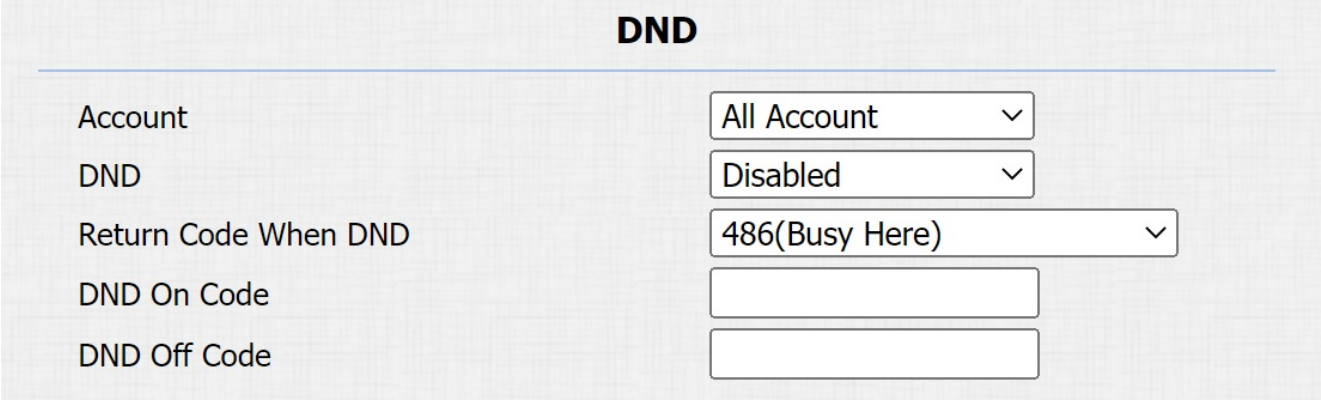
- **NAT**: choose STUN (Short for Simple Traversal of UDP over NATS) to enable the function, you need to install NAT sever. The default is **Disabled**.
- **Stun Server Address**: enter the STUN server IP, and the default port is 3478.

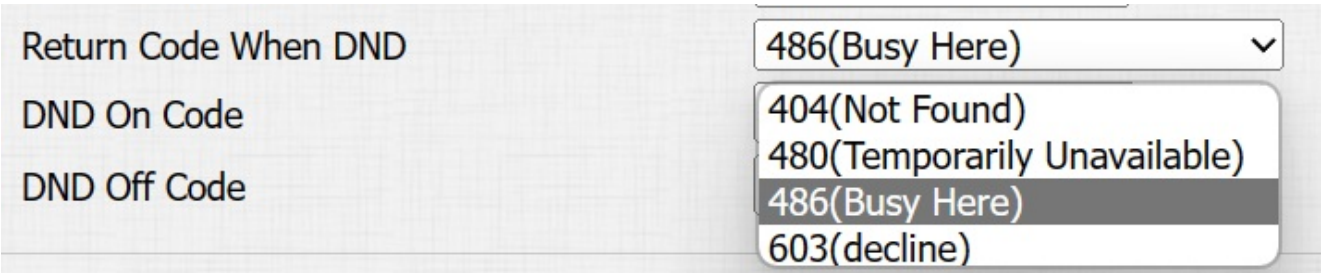
Configure Calling Feature

DND

The Do Not Disturb(**DND**) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

Navigate to **Device > Call Feature** interface.





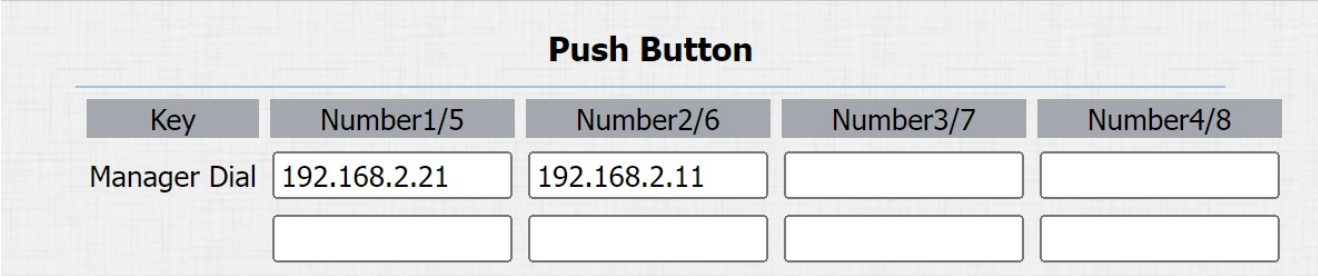
Parameter Set-up:

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

Manager Dial Call

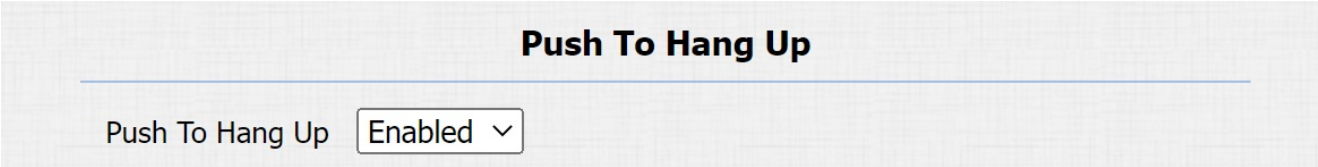
Manager Dial Call includes two types of calls: Sequence call and group call. It allows quick initiation of pre-configured numbers by pressing the Management key on the door phone.

To do the configuration on the web **Intercom > Basic > Push Button** interface.



Call Hang-up

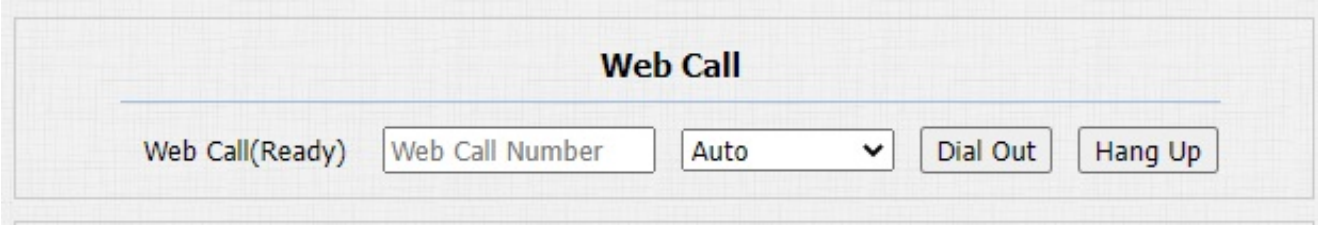
You can hang up the call on the door phone by pressing the push button if needed. To enable the push-button cal hang-up, navigate to **Intercom > Basic**.



Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

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



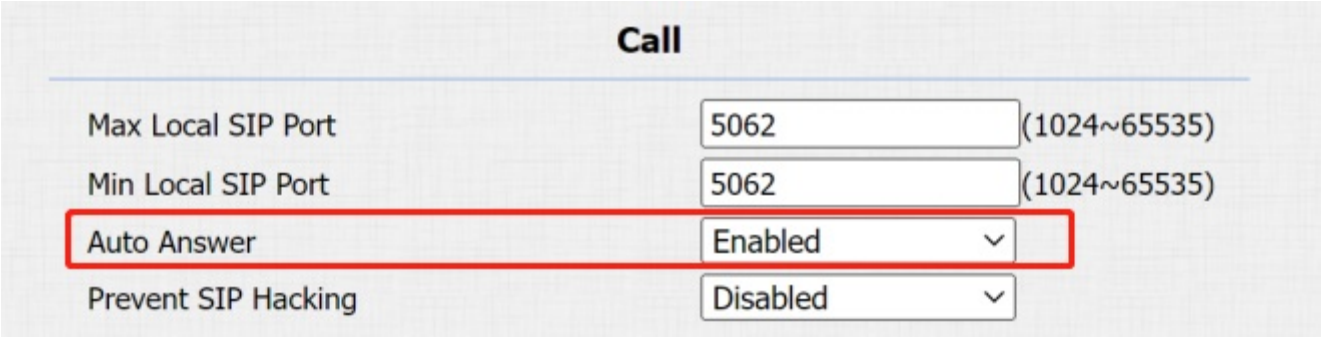
Parameters Set-up:

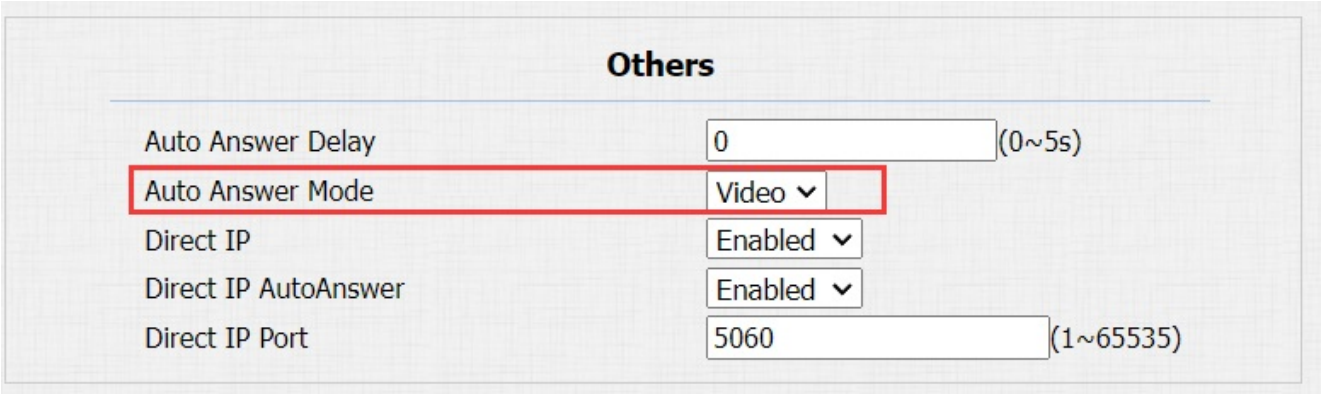
- **Web Call (Ready)**: enter the IP/SIP number to dial out.

Auto Answer

Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable this feature on web **Account > Advanced > Call** interface, you can set up the related parameters on web **Device > Call Feature > Others**.





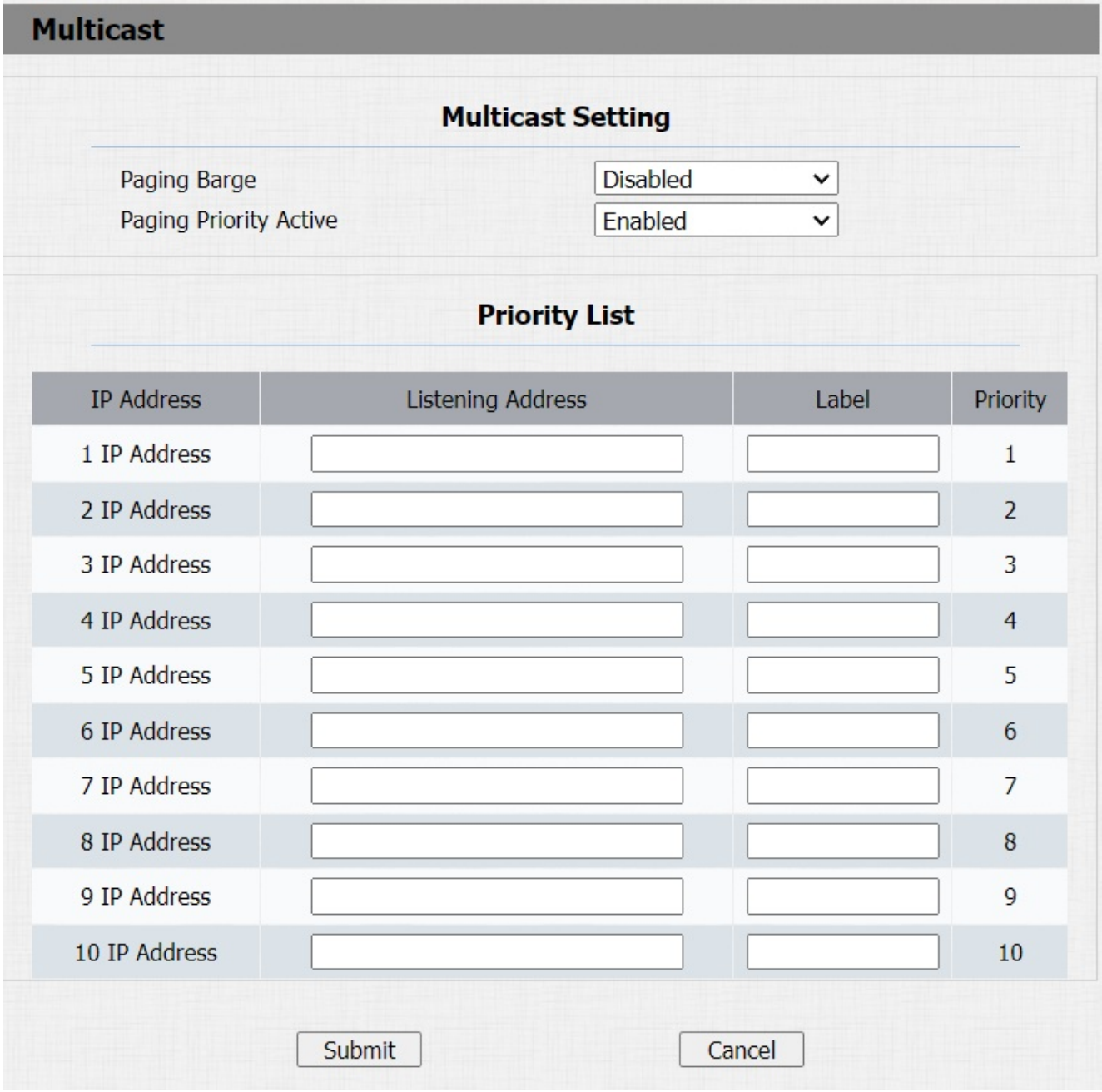
Parameters Set-up:

- **Auto Answer Mode/Direct IP Auto Answer**: turn on the **Auto Answer** function by choosing **Enable**.
- **Auto Answer Delay**: set up the delay time (from 0-5 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Auto Answer Mode**: the default is auto answer with voice call.

Multicast

The Multicast function allows one-to-many broadcasting for different purposes. For example, it enables the indoor monitor to announce messages from the kitchen to other rooms, or to broadcast notifications from the management office to multiple locations. In these scenarios, indoor monitors can either listen to or send audio broadcasts.

Path: **Device > Multicast**.



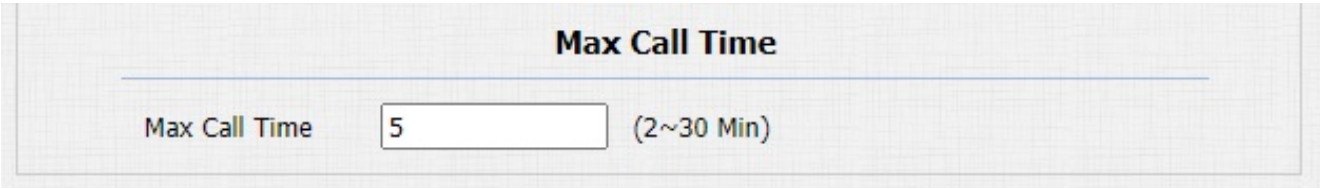
Parameters Set-up:

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

Maximum Call Duration

The 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 call automatically.

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



Parameters Set-up:

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

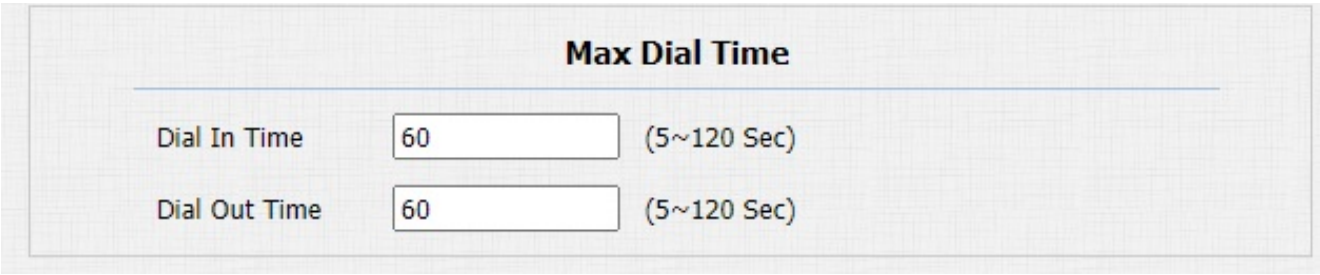
Note

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

Maximum Dial Duration

Maximum Dial Duration is the time limit for incoming- and/or outgoing calls on the door phone. If configured, the door phone will automatically terminate the call if no one answers the call within the preset time, whether it is incoming or outgoing.

You can navigate to **Intercom > Basic > Max Dial Time**.



Parameters Set-up:

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

Note

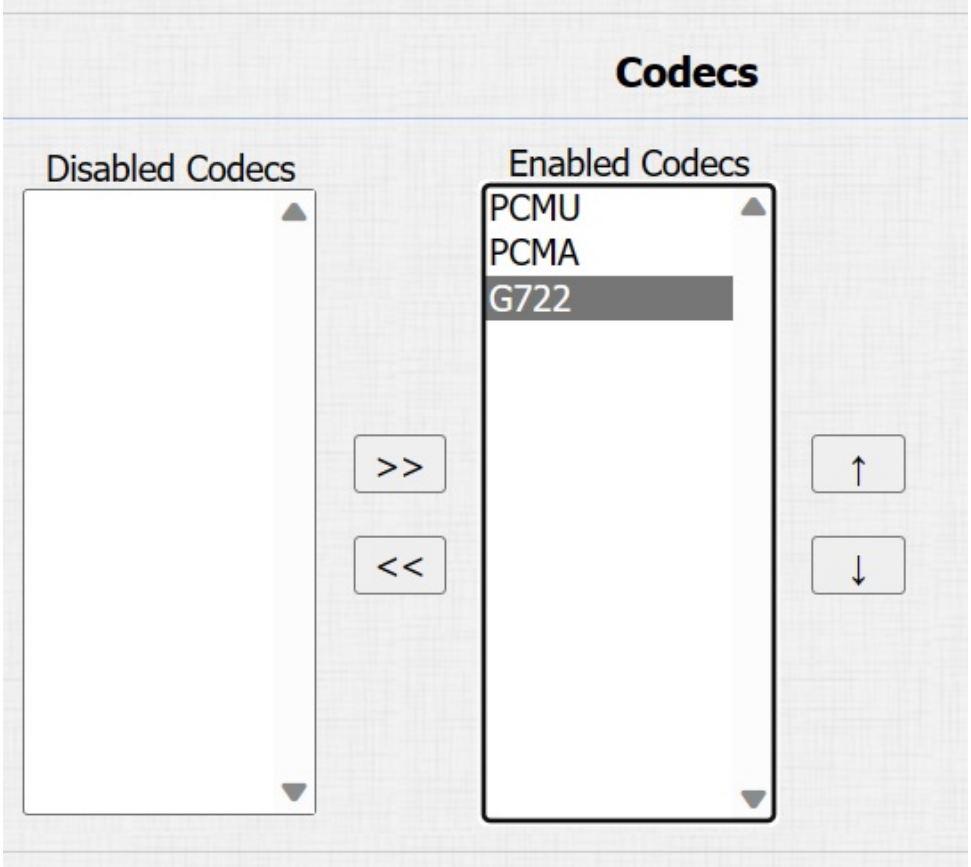
- Max dial time of device is also related with max dial time of SIP server. If using SIP account to make a call, please pay attention to the max dial time of SIP server. If the max dial time of SIP server is shorter than the max dial time of device, the shorter one is available.

Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The door phone supports three types of Codec (PCMU, PCMA, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To do the configuration on device web **Account > Advanced** interface.



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

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

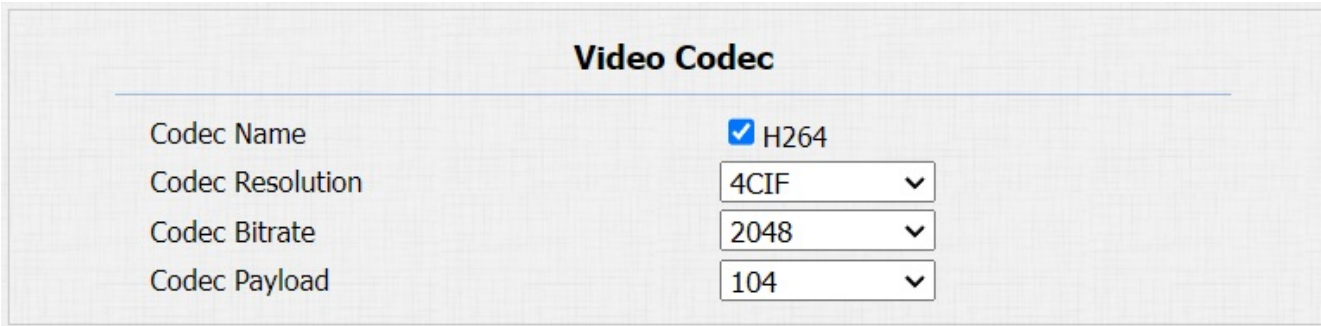
Video Codec Configuration

Note

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

The door phone supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

To set up video codec on web **Account > Advanced** interface.



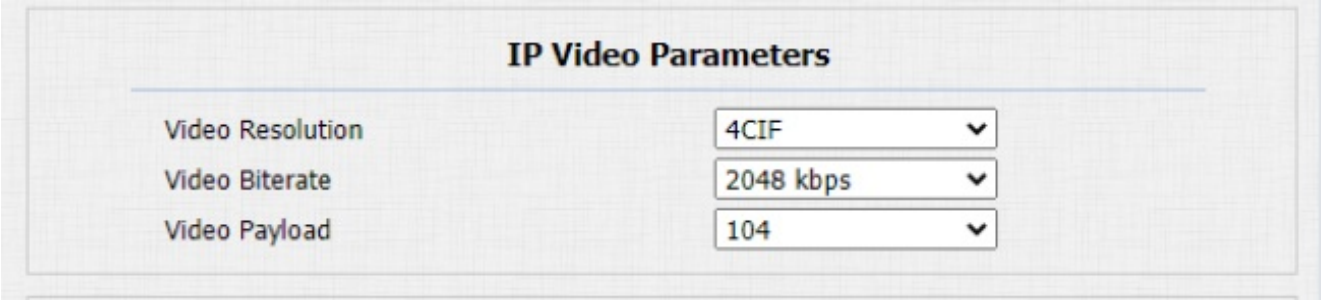
Parameter Set-up:

- **Codec Name**: check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Codec Resolution**: select the code resolution for the video quality among four options: **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 128-2048). 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 90-119) to configure audio/video configuration file. The default payload is 104.

Video Codec Configuration for IP Direct Calls

You can select the IP call video quality by selecting the proper codec resolution according to the network condition.

To do so , you can go to **Device > Call Feature > IP Video Parameters**.



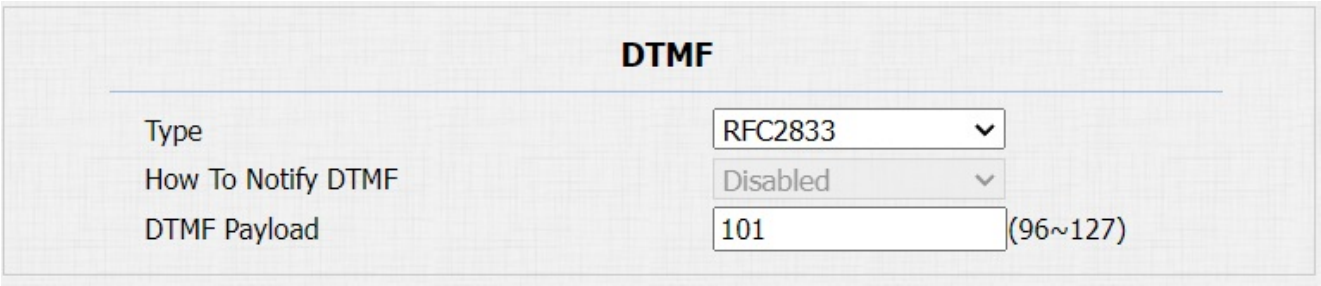
Parameter Set-up:

- **Video Resolution**: select the code resolution for the video quality among four options: **CIF, VGA, 4CIF**, and **720P**. The default code resolution is **4CIF**.
- **Video Bitrate**: Video Bitrate: select video bit-rate among seven options: **128 kbps, 256kbps, 320kbps, 512 kbps, 1024 kbps, 1536kbps, 2048 kbps** according to your network environment. The default video bit-rate is **2048 kpbs**.
- **Video Payload**: select the payload type (ranging from 90-119) to configure audio/video configuration file. The default payload is **104**.

Configure DTMF Data Transmission

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

Navigate to **Account > Advanced > DTMF** interface.



Parameter Set-up:

- **Type**: select DTMF mode among five options: **Inband, RFC2833, Info,Info+Inband**, and **Info+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: select among four types: **Disable, DTMF, DTMF-Relay**, and **Telephone-Event** according to the specific type adopted by the third party device. You

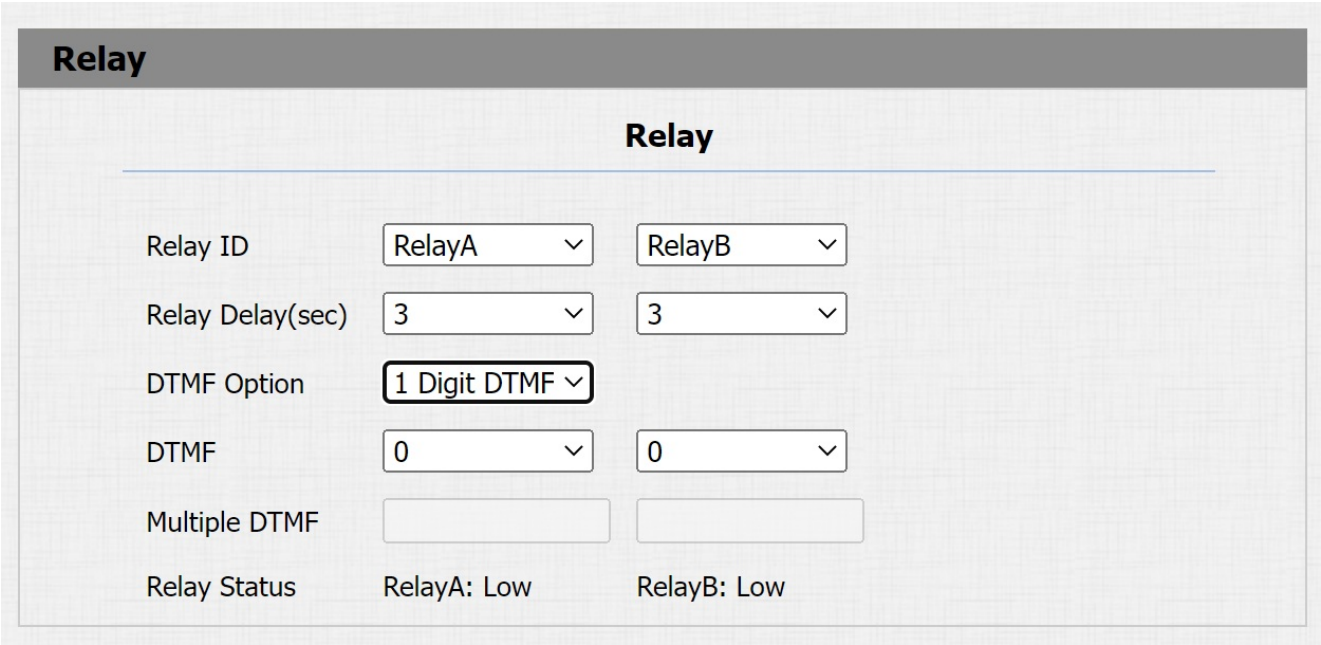
are required to set it up only when the third party device to be matched with adopts Info mode.

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

Relay Setting

Relay Switch Setting

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



Parameter Set-up:

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

Note

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

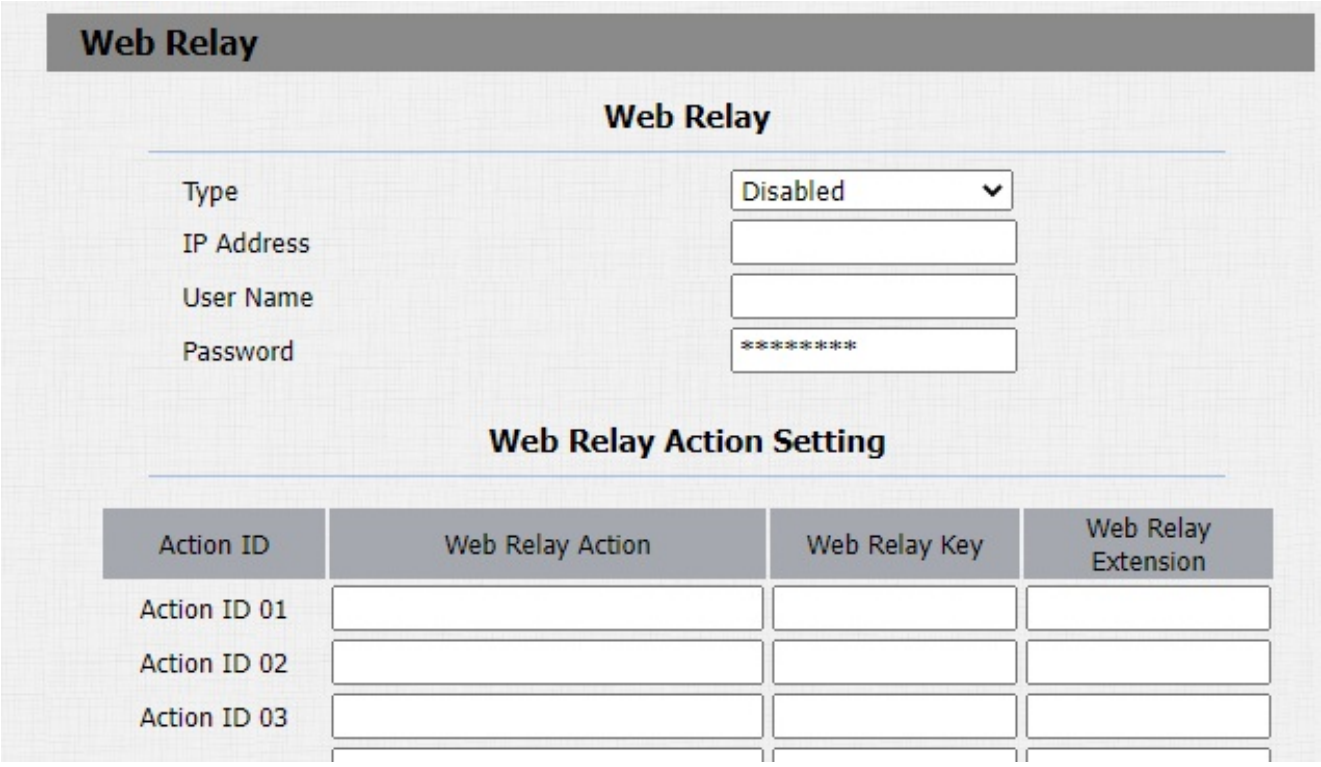
Note

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

Web Relay Setting

A web relay has a built-in web server and can be controlled via the Internet or a local network. The device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.

Navigate to **Device > Web Relay** interface. The IP Address, User Name, and Password are provided by the web relay manufacturer.



Parameter Set-up:

- **Type**: select among three options **Disabled, Web Relay**, and **Both**. Select **Web Relay** to enable the web relay. Select **Disable** to disable the web relay. Select **Both** to enable both local relay and web relay.
- **Password**: The password is authenticated via HTTP and you can define the passwords using **http get** in Action.
- **Web Relay Action**: enter the specific web relay action command provided by the web manufacturer for different actions by the web relay. Without adding IP, username, password, you can fill in the HTTP command in the web relay action, so you can configure multiple web relays. See the HTTP command example below:

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

For example, http://admin:admin@192.168.1.2/state.xml?relayState=2. (HTTP://:@IP address>/state.xml?relayState=2)

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

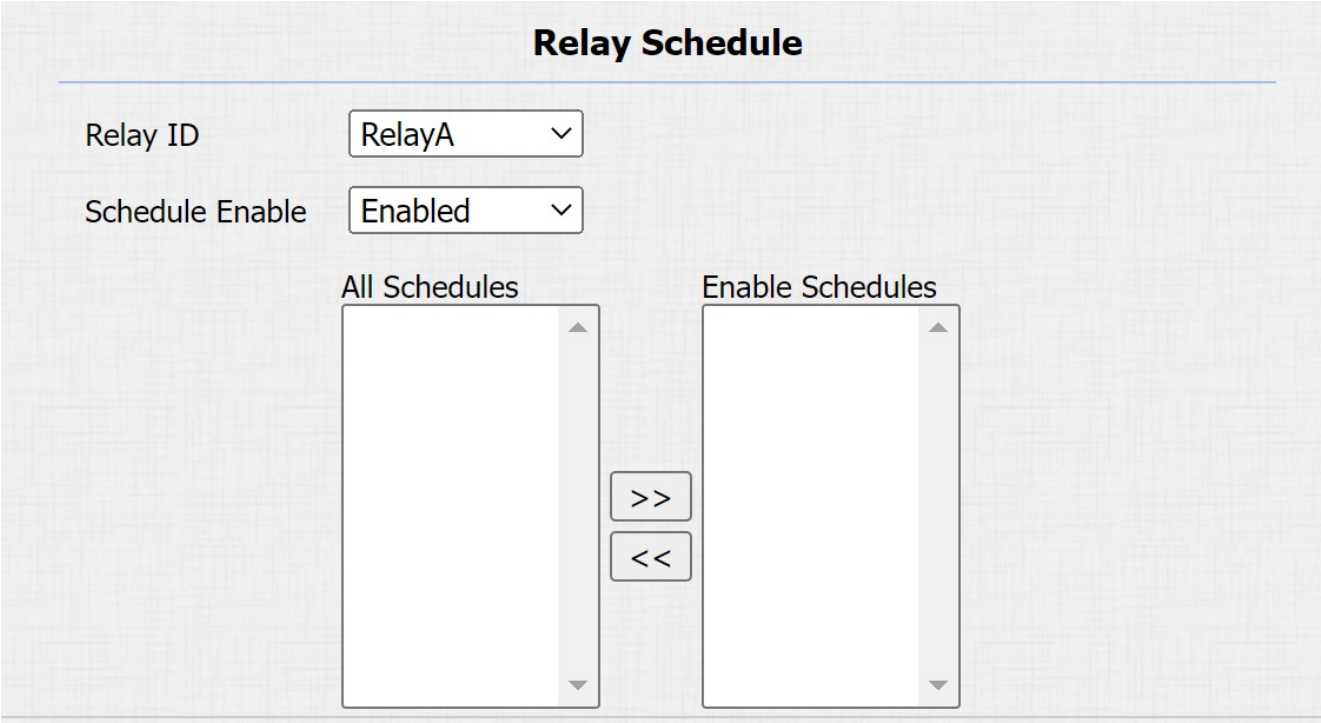
- **Web Relay Key**: it can be null or enter the configured DTMF code, when the door is unlock via DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension**: it can be null or enter the relay extension information, which can be a SIP Account user name of an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

Door Access Schedule Management

Relay Schedule

The relay schedule allows you to set a specific relay to always open at a certain time. This is helpful for situations like keeping the gate open after school or keeping the door open during work hours.

To do the configuration, navigate to **Intercom > Relay > Relay Schedule** interface.



Parameter Set-up:

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

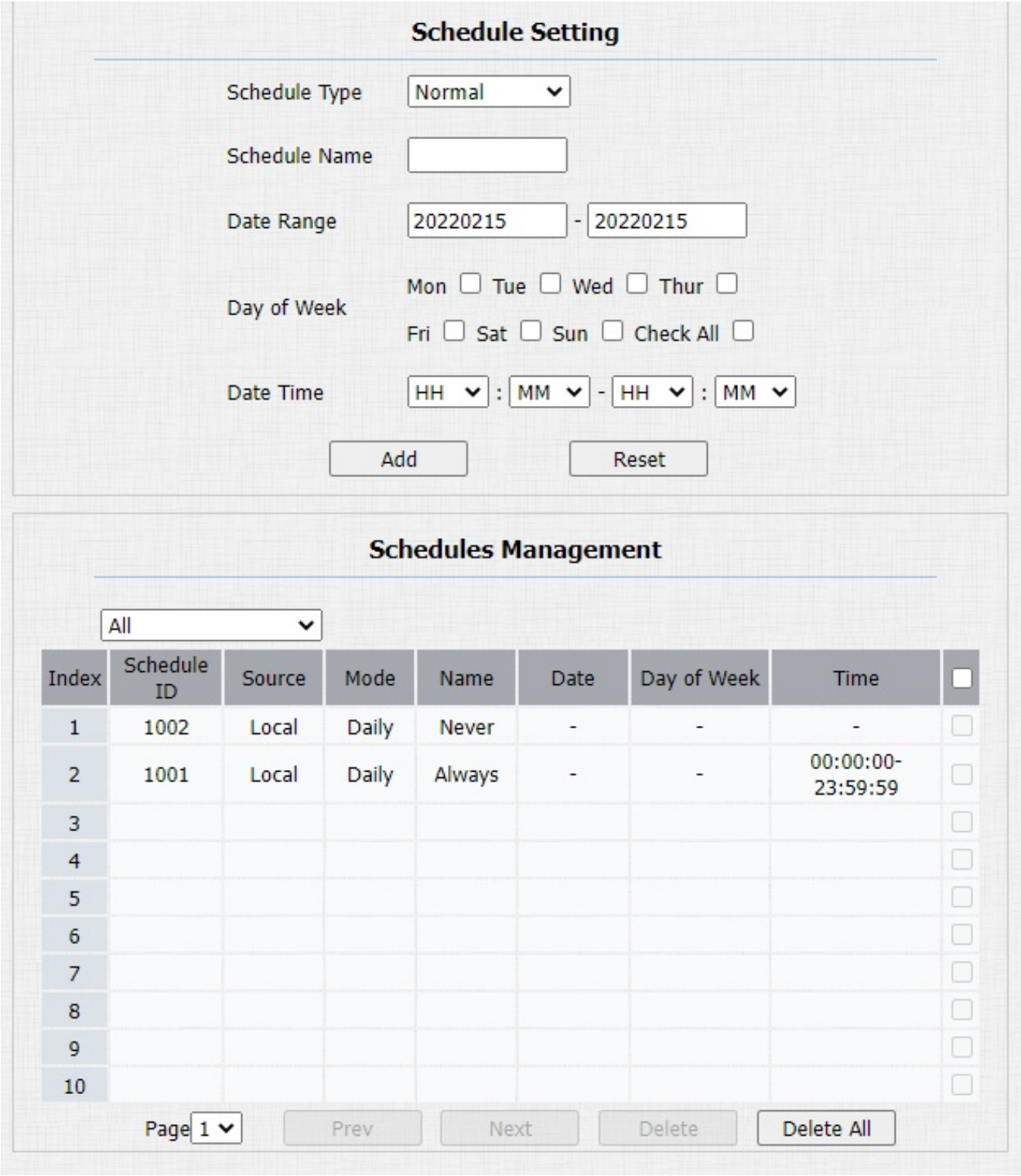
Configure Door Access Schedule

A door access schedule lets you decide who can open the door and when. It applies to both individuals and groups, ensuring that users within the schedule can only open the door using the authorized method during designated time periods.

Create Door Access Schedule

You can create door access schedules for daily, weekly, or custom time periods.

To do this configuration on web **Intercom > Schedules** interface.



Parameters Set-up:

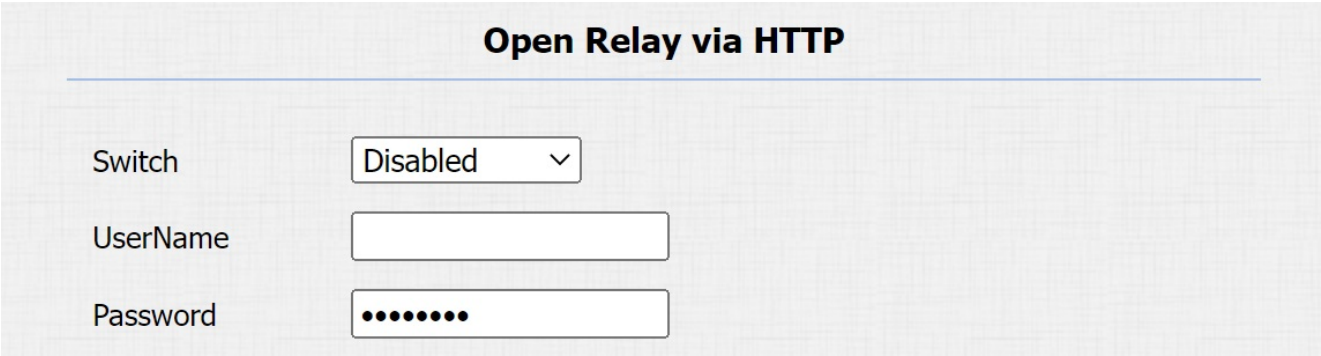
- **Schedule Type**: set the type of time period. There are three types to choose from: **Daily, Weekly**, and **Normal**. The default is **Daily**.
- **Day of Week**: select the corresponding day of the week. This field will only be displayed when the **Week** and **Normal** types are selected.
- **Date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

Door Unlock Configuration

Configure Open Relay via HTTP for Door Unlock

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

To do this configuration on web **Intercom > Relay > Open Relay Via HTTP** interface.



Parameter Set-up:

- **Switch**: enable or disable the HTTP command unlock function.
- **User Name**: enter the user name of the device web interface, for example, **admin**.
- **Password**: enter the password for the HTTP command. For example: **12345**.

Please refer to the following example:

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

Note

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

Configure Open Relay via DTMF

Dual-tone multi-frequency signaling(**DTMF**) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

Path: **Intercom > Relay > Open Relay Via DTMF**

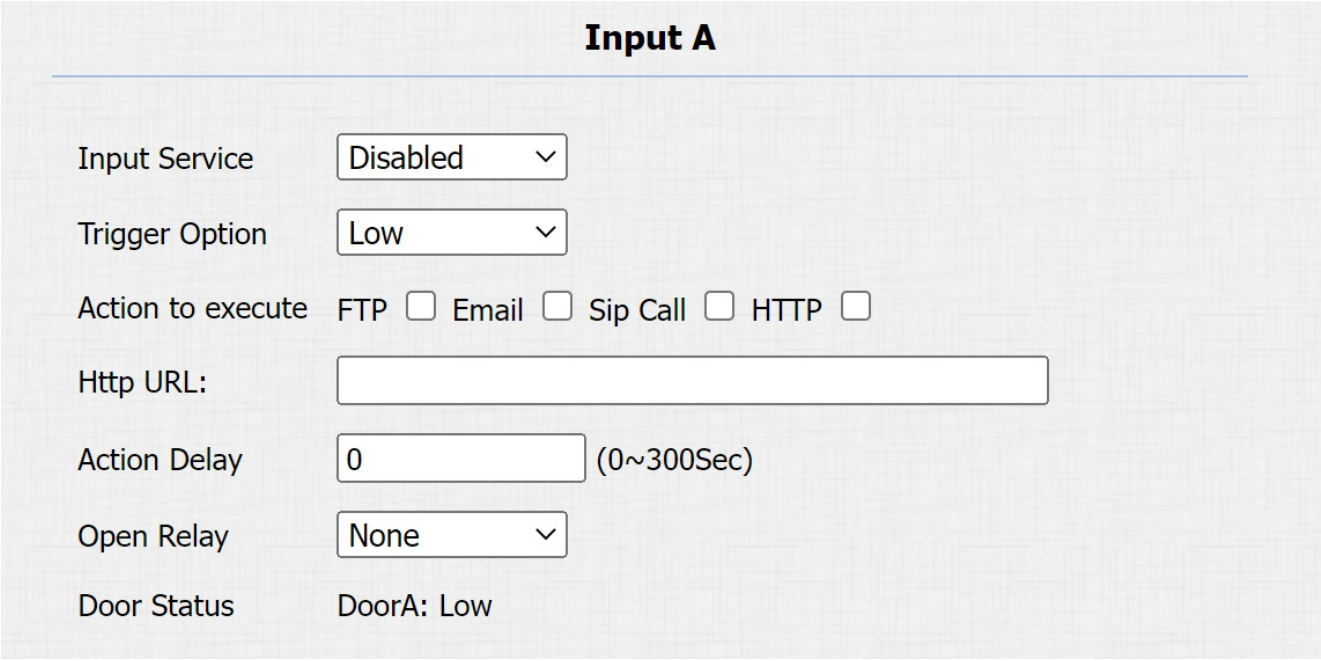
Parameter Set-up:

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

Configure Exit Button for Door Unlock

When users need to open the door from inside by pressing the Exit button, you need to set up the Input terminal that matches the Exit button to activate the relay for the door access.

Go to **Intercom > Input** interface.



Parameter Set-up:

- **Trigger Option**: select the trigger electrical level options between **High** and **Low** according to the actual operation on the exit button.
- **Action To Execute**: select the method to carry out the action among four options: **FTP, Email, SIP Call**, and **HTTP**.
- **Http URL**: enter the URL if you select the HTTP to carry out the action.
- **Action Delay**: set up the delay time when the action is carried out. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 minutes after your press the button.
- **Open Relay**: set up relays to be triggered by the actions.

Security

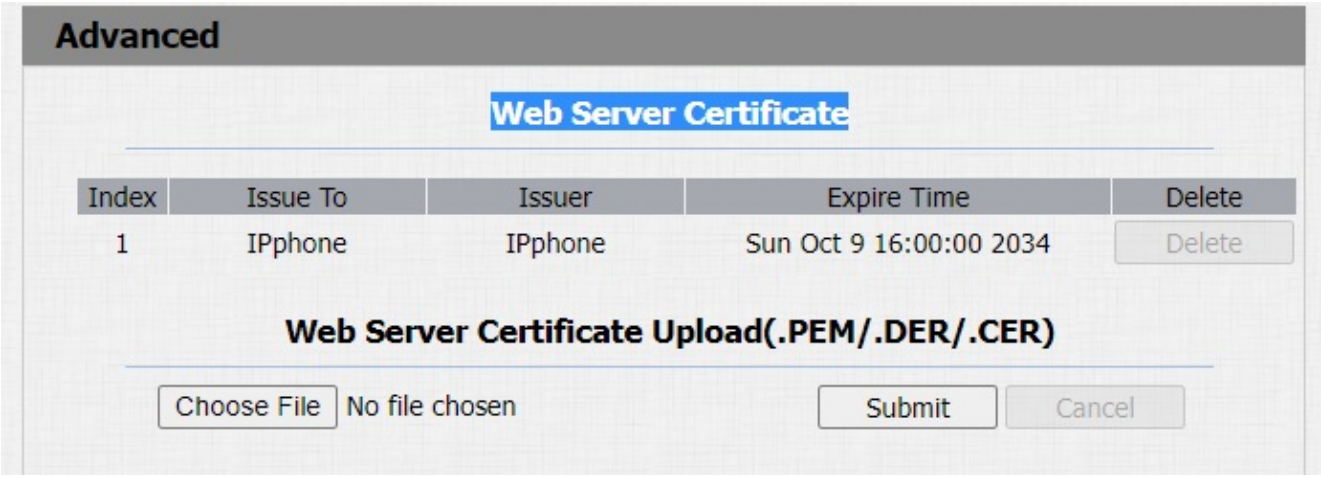
Client Certificate Setting

Certificates ensure communication integrity and privacy. To use the SSL protocol, you need to upload the right certificates for verification.

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox door phone. Please upload the certificates in accepted formats.

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



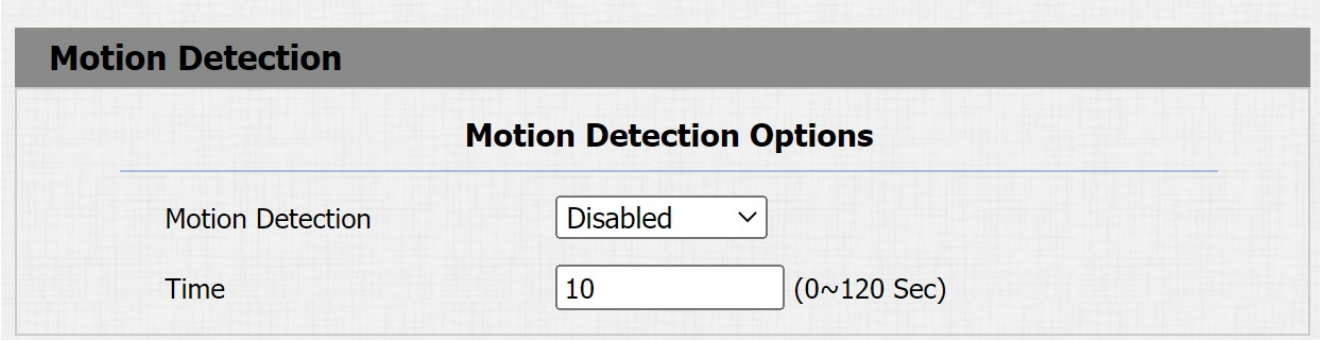
Motion Detection

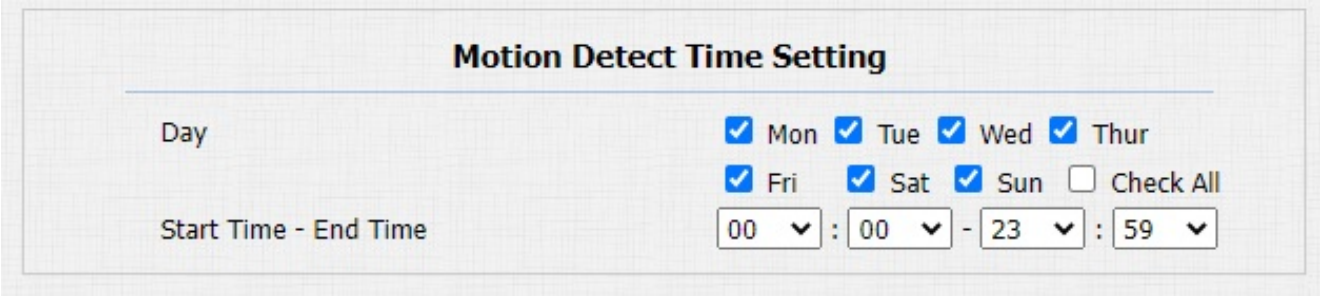
Motion Detection is a feature that allows unattended video surveillance and automatic alarms. It detects any changes in the image captured by the camera, such as someone walking by or the lens being moved, and activates the system to perform the appropriate action.

Configure Motion Detection

On the device web interface, you can not only set the motion detection interval but detection schedule.

Path: **Intercom > Motion > Motion Detection Options**.





Parameter Set-up:

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

Action URL

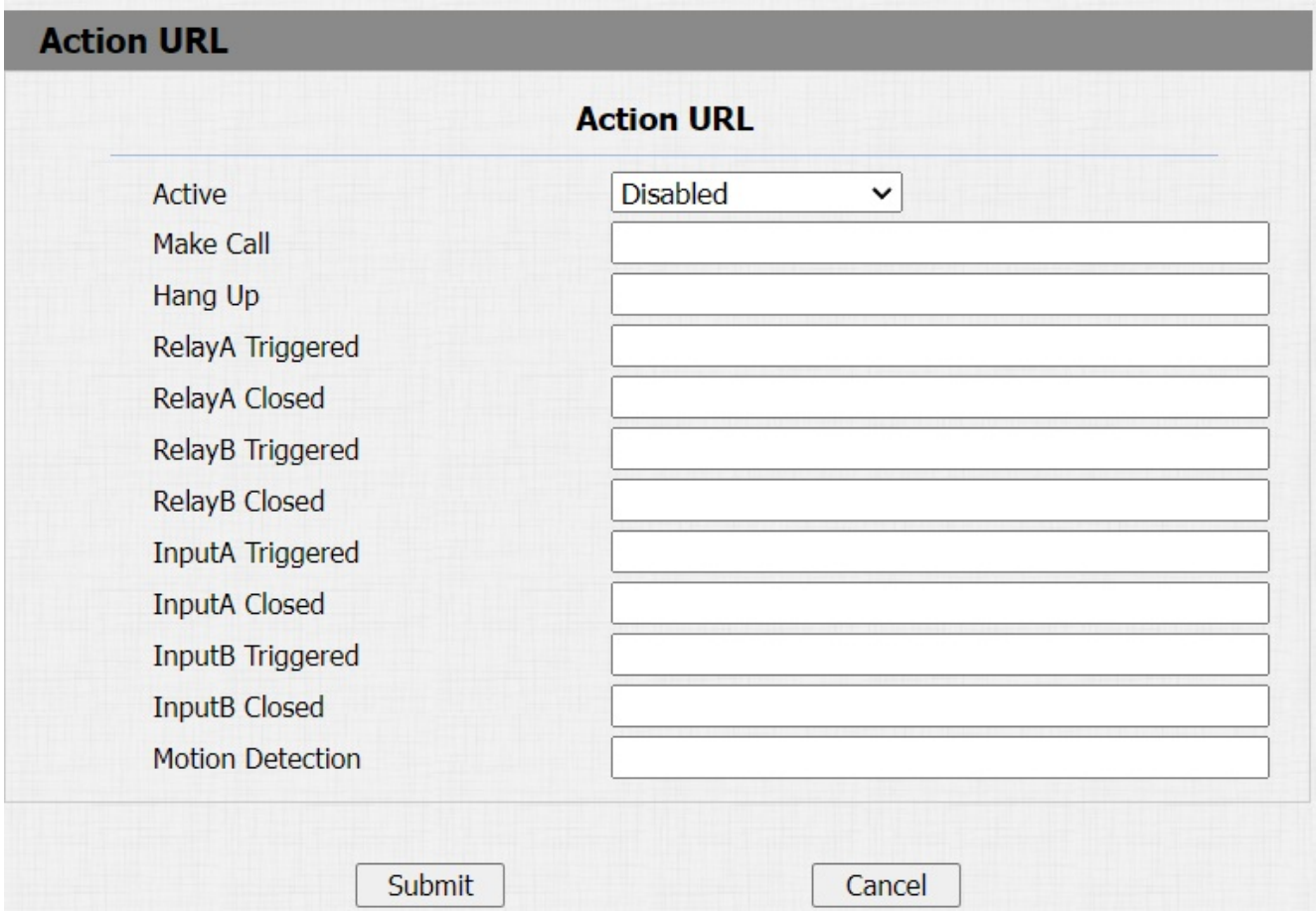
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status, input status, PIN code, or RF card access changes.

Akuvox Action URL:

No	Event	Parameter format	Example
1	Make Call	$remote	Http://server ip/ Callnumber=$remote
2	Hang Up	$remote	Http://server ip/ Callnumber=$remote
3	Relay Triggered	$relay1status	Http://server ip/ relaytrigger=$relay1status
4	Relay Closed	$relay1status	Http://server ip/ relayclose=$relay1status
5	Input Triggered	$input1status	Http://server ip/ inputtrigger=$input1status
6	Input Closed	$input1status	Http://server ip/ inputclose=$input1status
7	Valid Code Entered	$code	Http://server ip/ validcode=$code
8	Invalid Code Entered	$code	Http://server ip/ invalidcode=$code
9	Valid Card Entered	$card_sn	Http://server ip/ validcard=$card_sn
10	Invalid Card Entered	$card_sn	Http://server ip/ invalidcard=$card_sn
11	Tamper Alarm Triggered	$alarm status	Http://server ip/tampertrigger=$alarm status

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

Path: **Device > Action URL**.

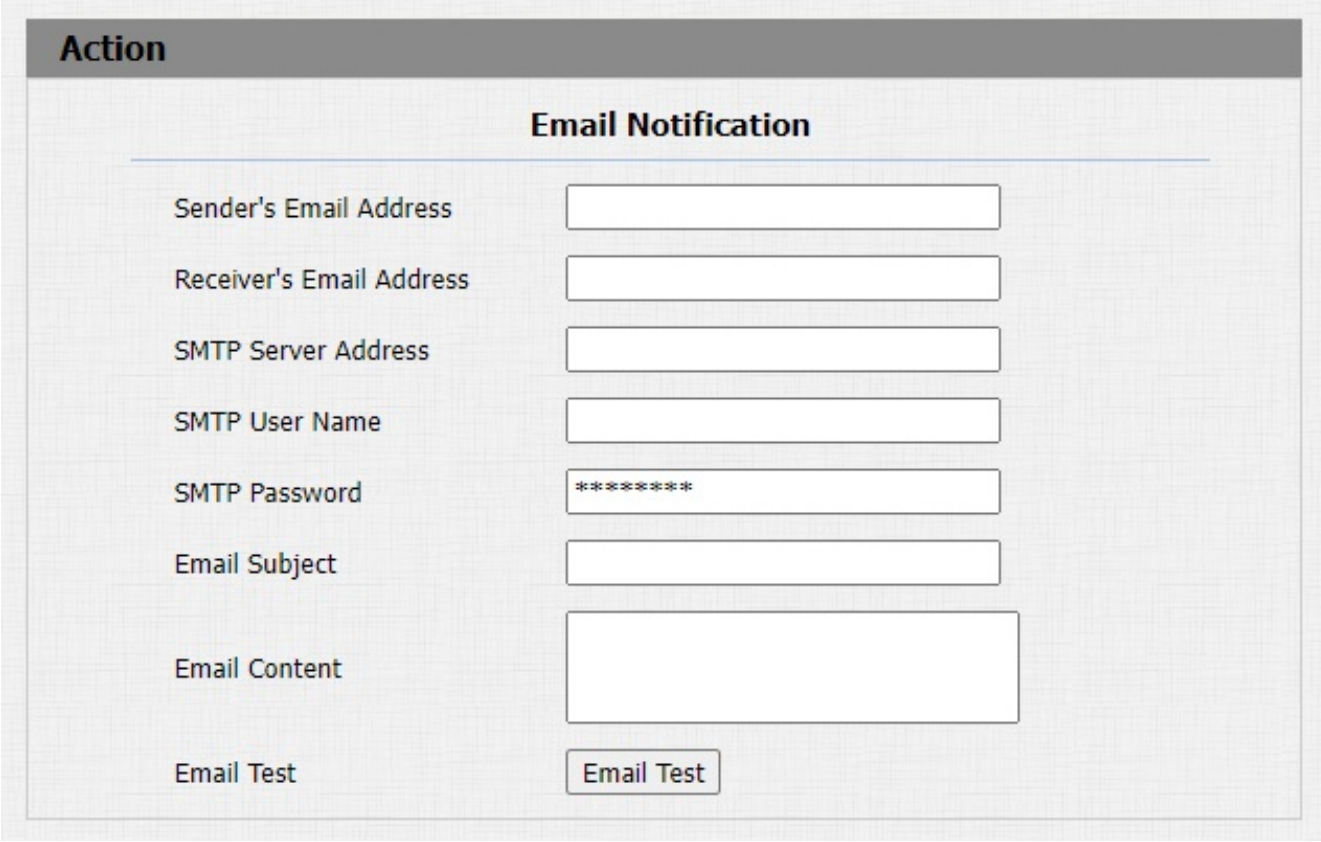


Security Notification Setting

Email Notification Setting

Set up email notification to receive screenshots of unusual motion from the door phone.

Go to **Intercom > Action > Email Notification** interface.



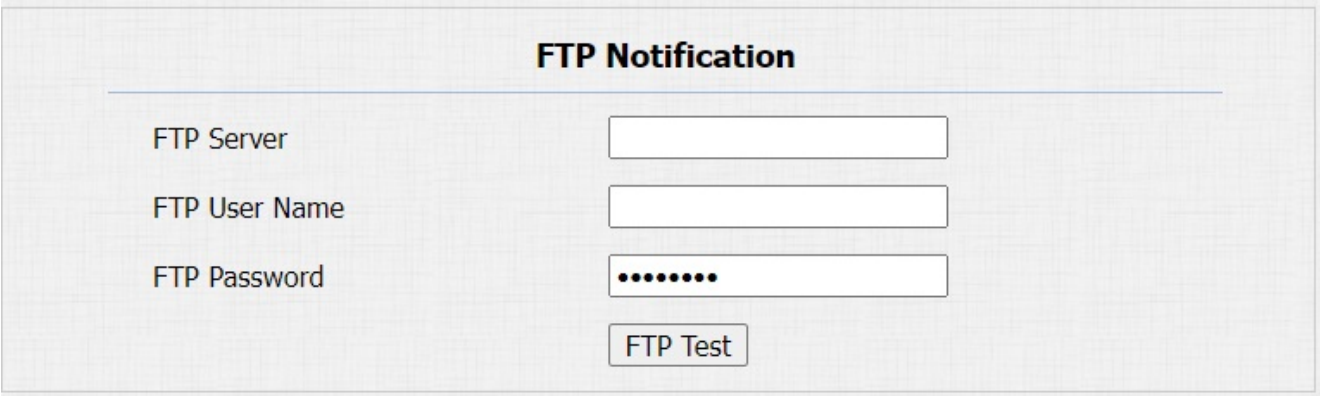
Parameter Set-up:

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

FTP Notification Setting

To get notifications through FTP server, you need to set up the FTP settings. The door phone will upload a screenshot to the specified FTP folder if it senses any unusual motion.

Go to **Intercom > Action > FTP Notification** interface.

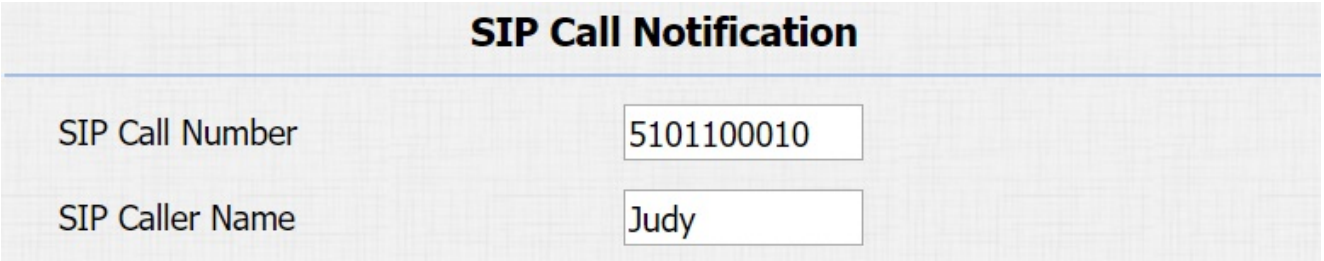


Parameter Set-up:

- **FTP Server**: enter the address (URL) of the FTP server for the FTP notification.

SIP Call Notification Setting

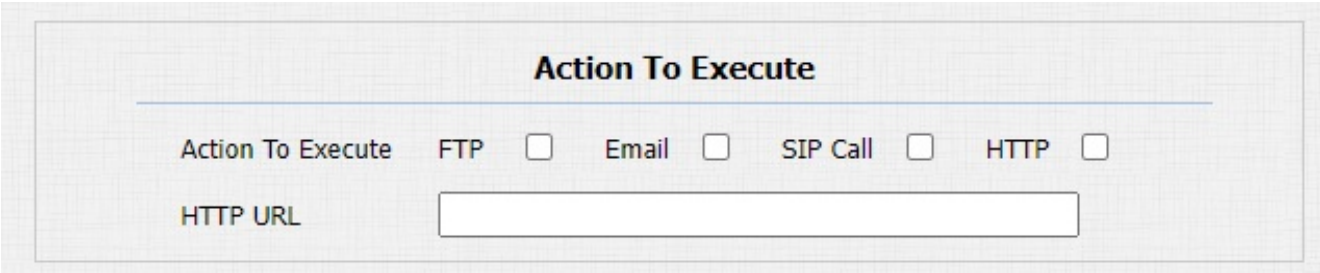
In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered. To configure a SIP call notification on web **Intercom > Action > SIP Call Notification** interface.



HTTP URL Notification Configuration

Akuvox door phone support sending the HTTP notification to the third party when some features are triggered.

The URL format: **http://http server IP address/any information**. Refer to: **Intercom > Motion > Action to Execute**.



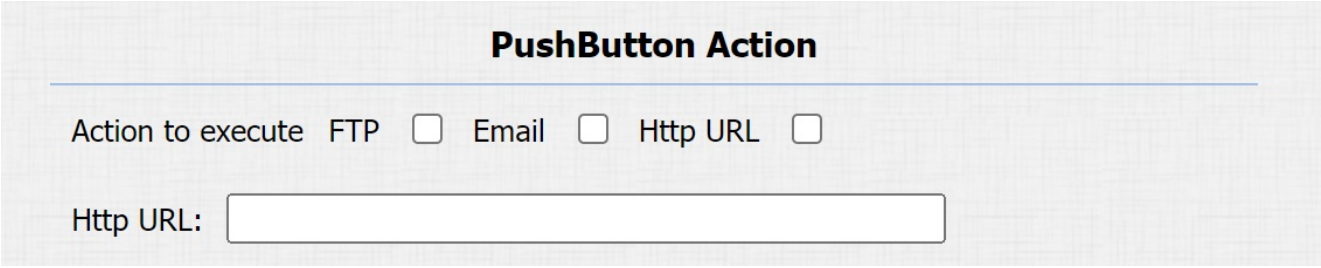
Parameter Set-up:

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

Security Action Configuration

Configure Push Button Action

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

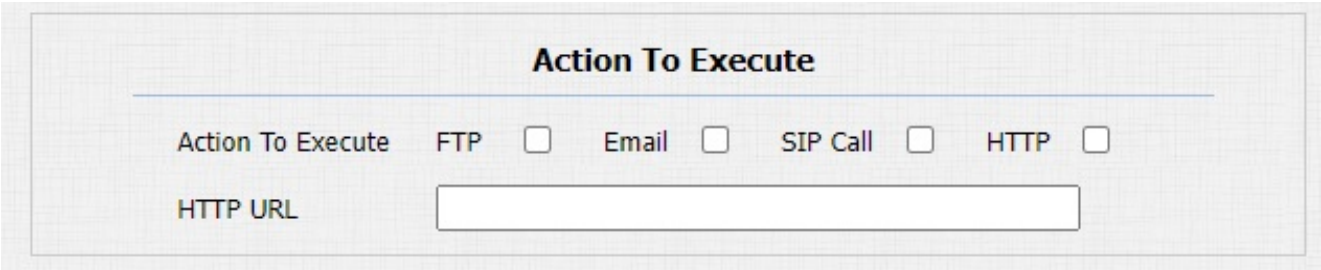


Parameter Set-up:

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

Configure Motion Action

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

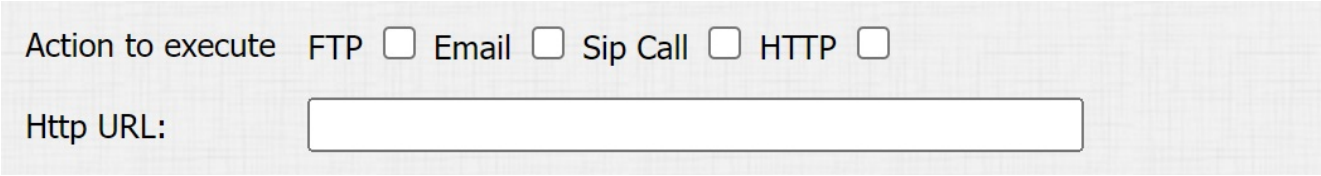


Parameter Set-up:

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

Configure Input Action

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



Parameter Set-up:

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

Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

To configure this feature on web **Account > Advanced > Encryption** interface.

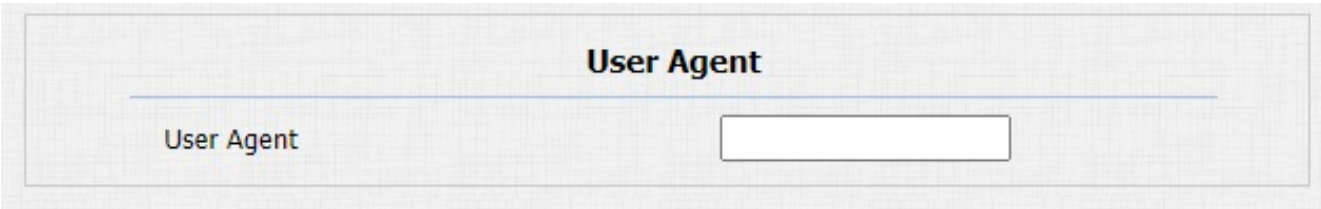
Parameter Set-up:

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

User Agent

User agent is used for identification purpose when you are analyzing the SIP data packet.

Path: **Account > Advanced > User Agent.**



Parameter Set-up:

- **User Agent**: support for entering another specific value, it is Akuvox by default.

Monitor and Image

MJPEG and RTSP are the primary monitoring stream types discussed in this chapter.

MJPEG, or Motion JPEG, is a video compression format that uses JPEG images for each video frame. Akuvox devices display live streams on the web interface and capture monitoring screenshots in MJPEG format. Settings related to MJPEG determine video quality and the on/off status of the live stream function.

RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

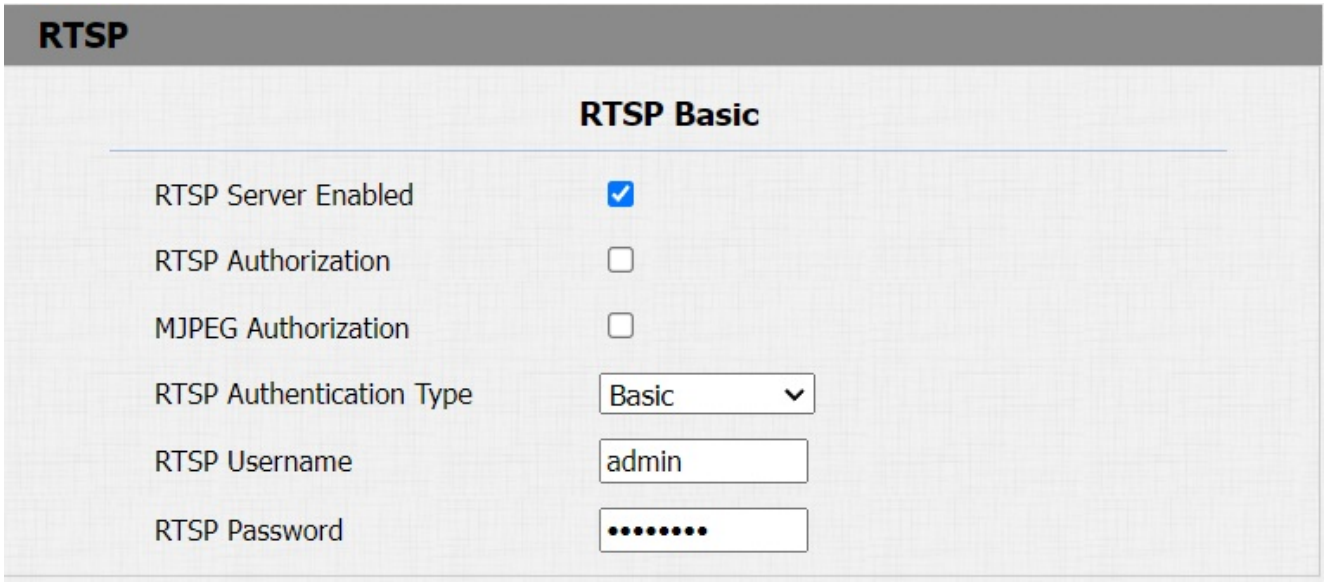
ONVIF is an Open Network Video Interface Forum. It enables the device to scan and discover cameras or intercom devices with activated ONVIF functions. Live streams obtained through ONVIF are essentially in RTSP format.

RTSP Stream Monitoring

You can use RTSP to watch a live video stream from other intercom devices on the device.

RTSP Basic Setting

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



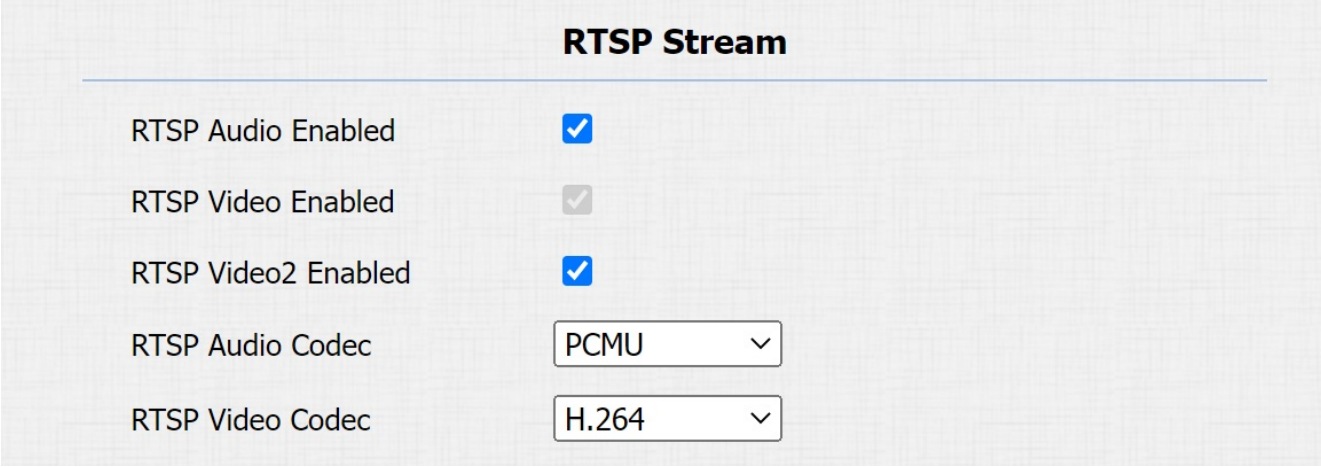
Parameter Set-up:

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

RTSP Stream Setting

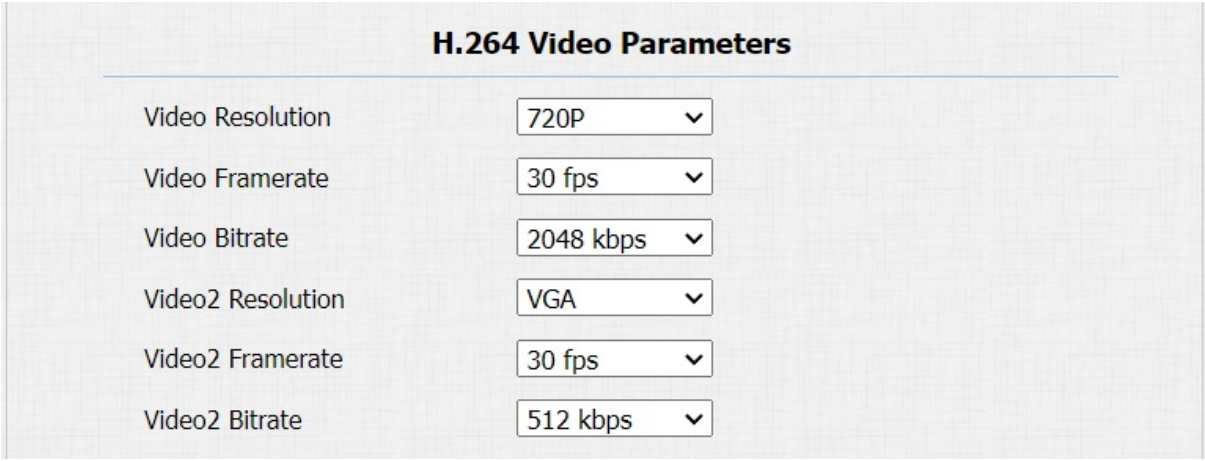
The RTSP stream can use either H.264 or Mjpeg as the video codec. If you choose H.264, you can also adjust the video resolution, bitrate, and other settings.

Go to **Intercom > RTSP > RTSP Stream** interface.



Parameter Set-up:

- **RTSP Audio Enabled**: select Enable so that the door phone can also send audio information to the monitor by RTSP.
- **RTSP Video Enabled**: the door phone can send the video information to the monitor. After enabling RTSP feature, the video RTSP is enabled by default and can not be modified.
- **RTSP Video2 Enabled**: Akuvox door phones support 2 RTSP streams, you can enable the second one.



Parameter Set-up:

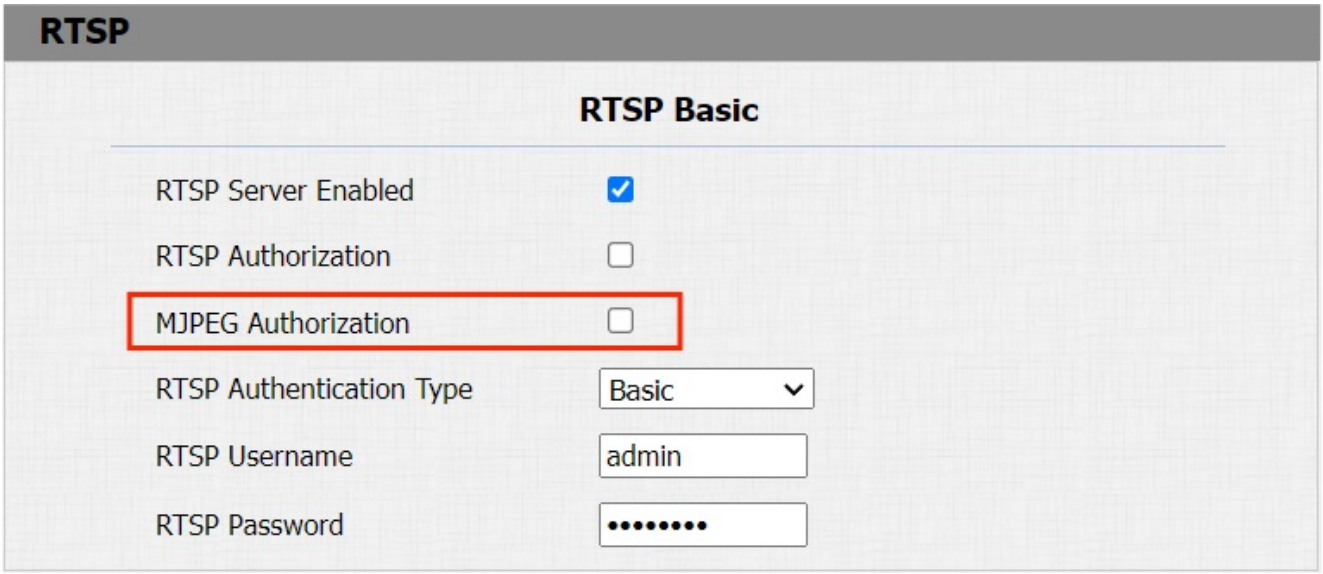
- **Video Resolution**: select video resolutions among five options: **CIF, VGA, 4CIF, 720P, 1080P**. The default video resolution is **720P**. and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate**: **30fps** is the video frame rate by default.
- **Video Bitrate**: select video bit-rate among six options: **64kbps, 128kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps** according to your network environment. The default video bit-rate is **2048 kpbs**.

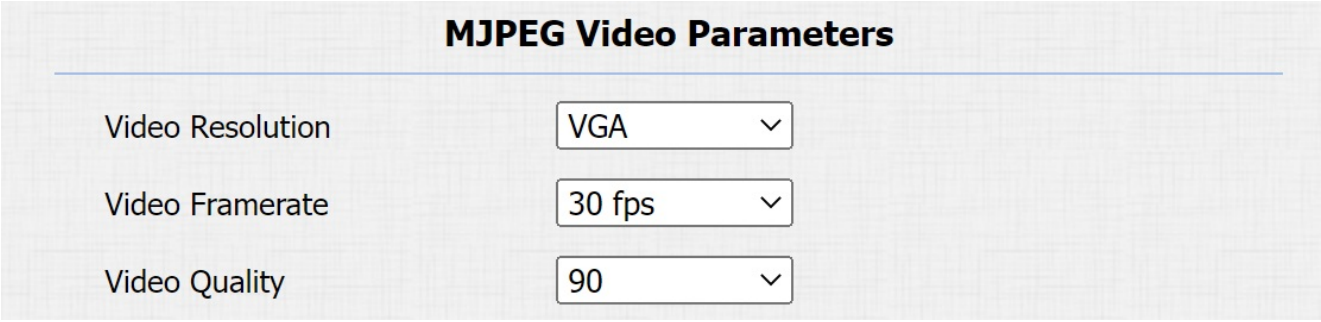
- **Video2 Resolution**: select video resolution for the second video stream channel. The default video solution is **VGA**.
- **Video2 Framerate**: select the video framerate for the second video stream channel. **30fps** is the video frame rate by default for the second video stream channel.
- **Video2 Bitrate**: select video bitrate among the six options for the second video stream channel. While the second video stream channel is **512 kpbs** by default.

MJPEG Image Capturing

You can take a monitoring image in Mjpeg format with the device. To do this, you need to turn on the Mjpeg function and choose the image quality.

Go to **Intercom > RTSP > RTSP Basic** and **Intercom > RTSP > MJPEG Video Parameters** interface.





Parameter Set-up:

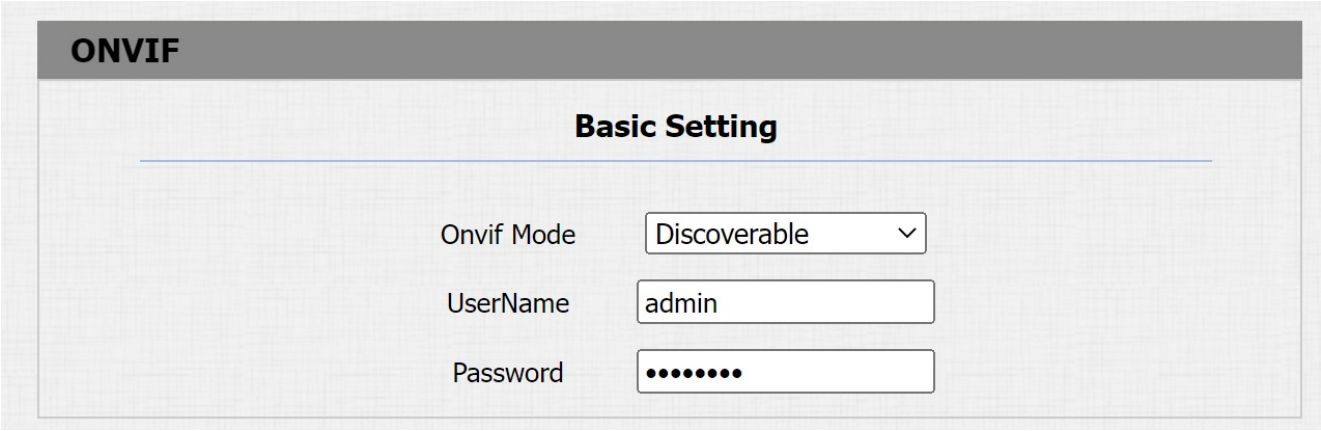
- **Video Resolution**: select video resolutions among five options: **CIF, VGA, 4CIF, 720P**, and **1080P**. The default video resolution is **VGA**, and the video from the door phone might not be able to be shown in the indoor monitor if the resolution is set higher than **VGA**.

- **Video Framerate**: **30fps** is the video frame rate by default.
- **Video Quality**: the video bitrate, from 50 to 90.

ONVIF

You can access the real-time video from the device's camera using the Akuvox indoor monitor or other third-party devices like Network Video Recorder(**NVR**). Enabling and setting up the ONVIF function on the device will allow its video to be visible on other devices.

Go to **Intercom** > **ONVIF** interface.



Parameter Set-up:

- **Onvif Mode**: select **Discoverable**, then the video from the door phone camera can be searched by other devices.
- **User Name**: enter the user name. The default is **admin**.
- **Password**: enter the password. The default is **admin**.

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

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

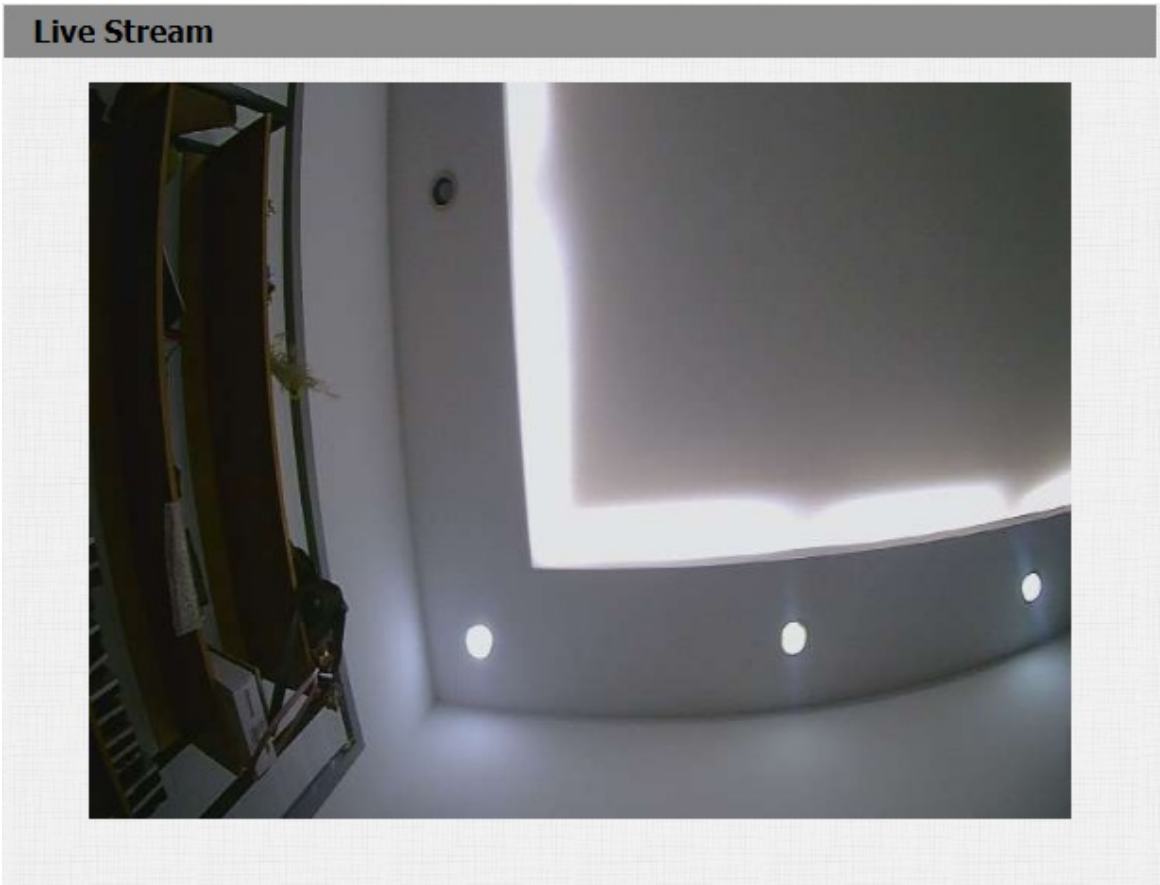
Note

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

Live Stream

There are two ways to check the real-time video from the device. One is to go to the device web interface and view the video there. The other is to enter the correct URL on the web browser and access the video directly.

Go to **Intercom > Live Stream** to view the real-time video.

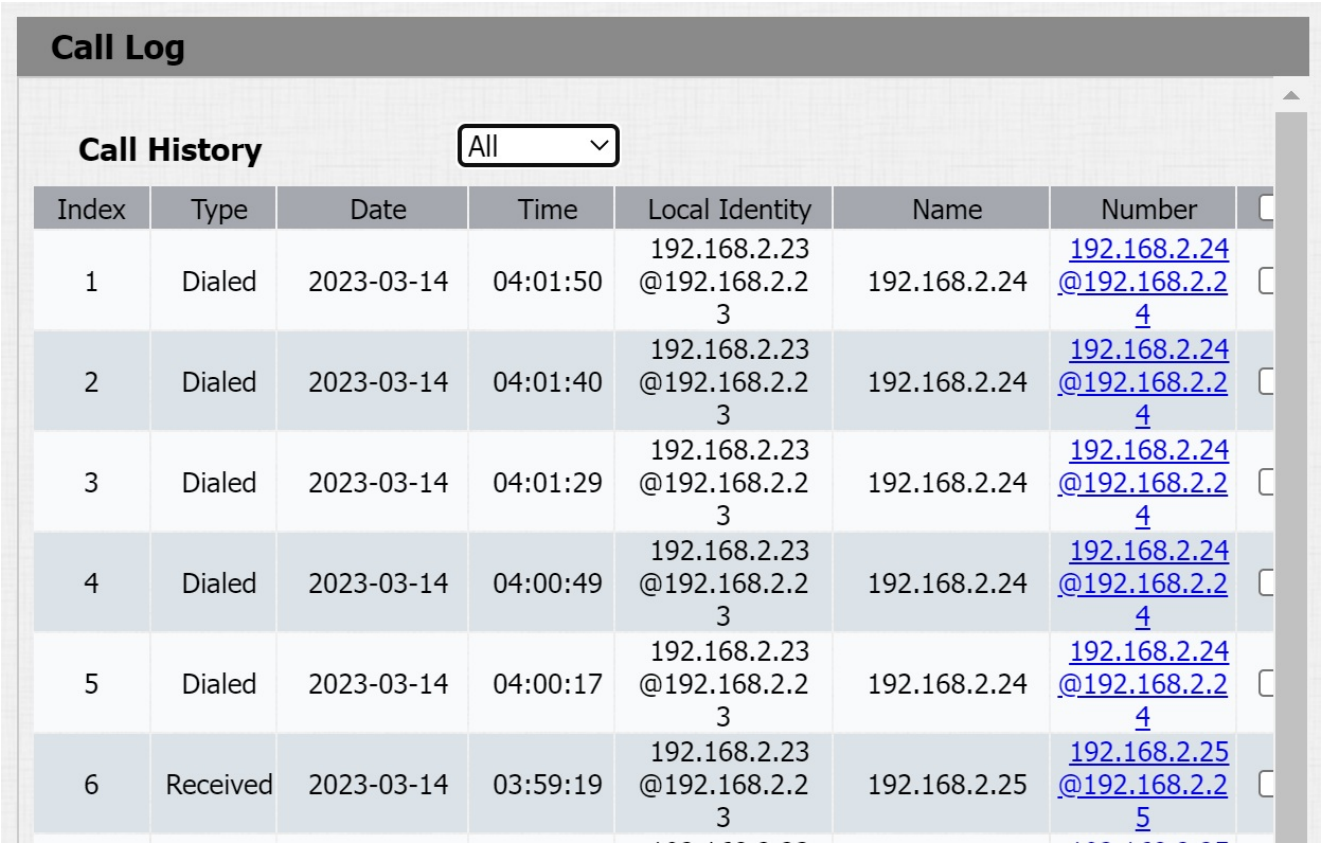


Logs

Call Logs

If you want to check on the calls inclusive of the dial-out calls, received calls, and missed calls in a certain period of time, you can check and search the call log on the device web interface and export the call log from the device if needed.

Navigate to **Device > Call Log** interface.



Call Log

Call History All

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

Parameter Set-up:

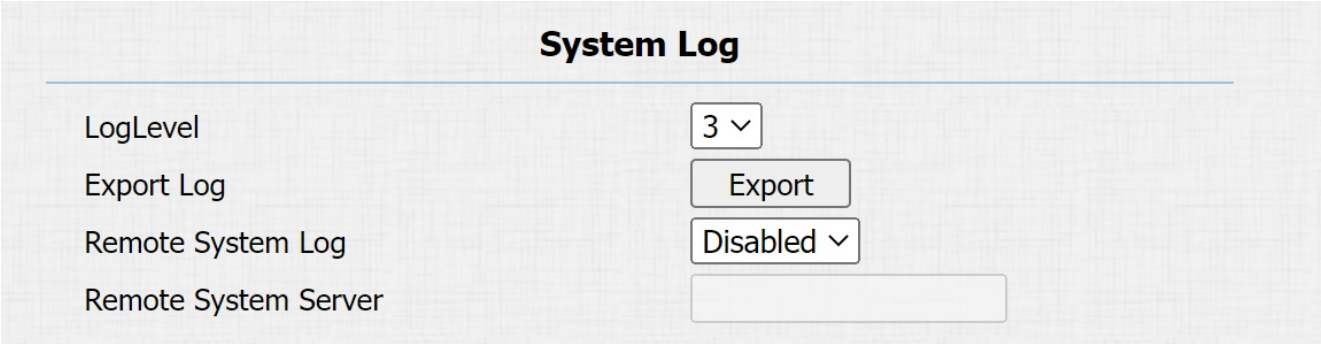
- **Call History**: select call history among four options: **All, Dialed, Received, Missed** for the specific type of call log to be displayed.

Debug

System Log

System logs can be used for debugging purposes.

Go to **Upgrade > Advanced > System Log** interface.



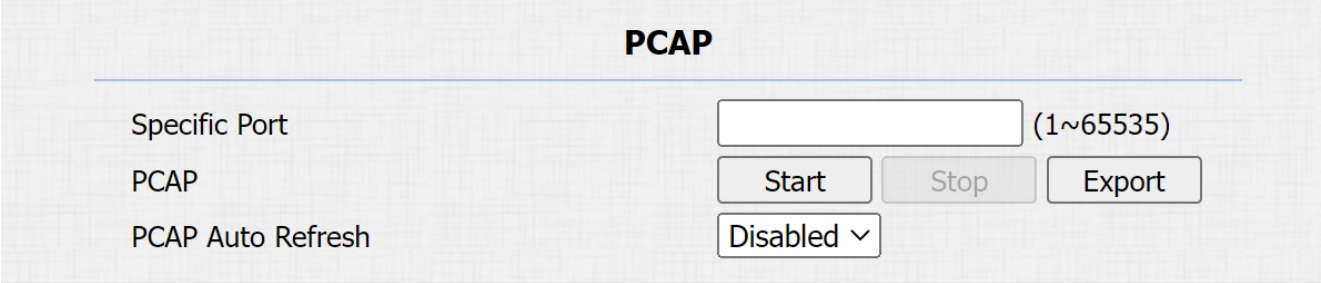
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.
- **Remote System Server**: enter the remote server address to receive the device log. And the remote server address will be provided by Akuvox technical support.

PCAP

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

You can set up the PCAP on the device web **Upgrade > Advanced > PCAP** interface properly before using it.



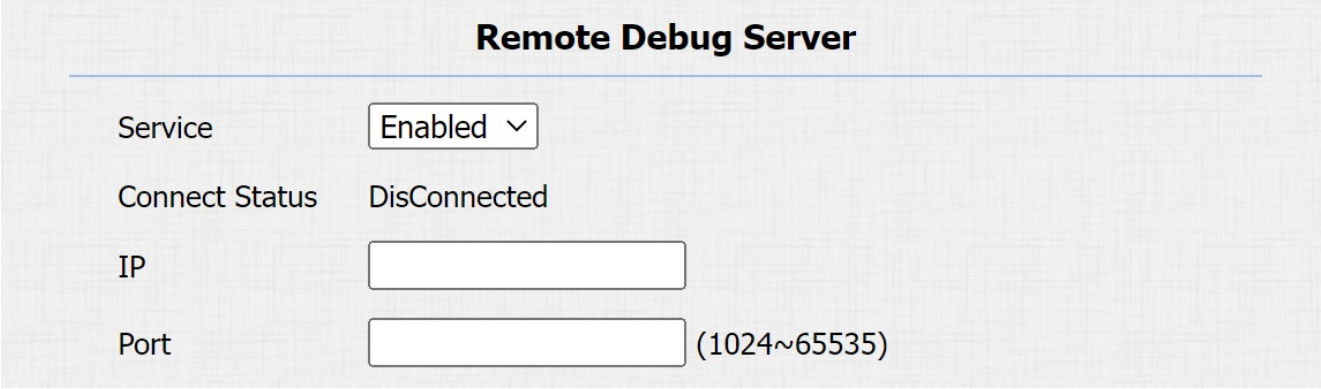
Parameter Set-up:

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

Remote Debug

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

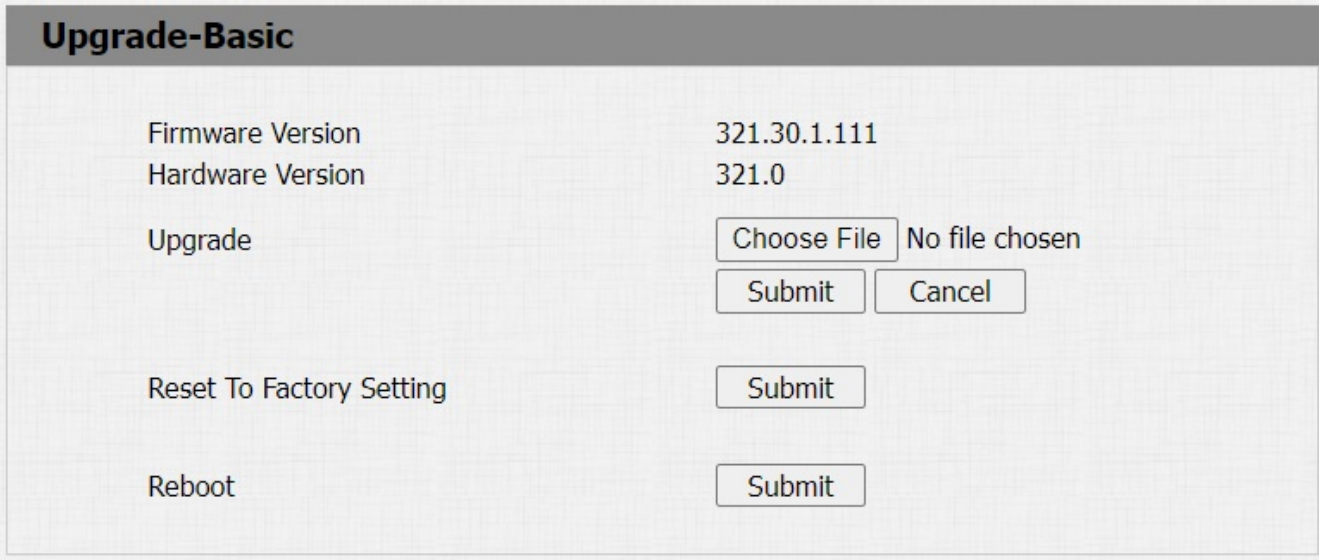
Path: **Intercom > Advanced**.
Fill in the IP and Port number provided by Akuvox tech team.



Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **Upgrade** > **Basic** interface.



Note

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

Backup

You can import or export encrypted configuration files to your Local PC.

Go to **Upgrade** > **Advanced** > **Others** interface if needed.

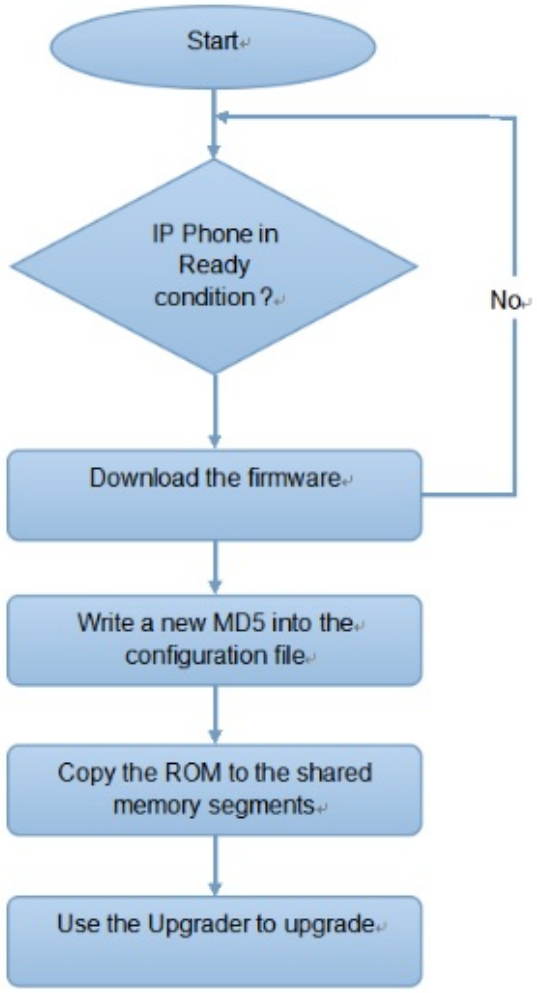
Auto-provisioning via Configuration File

You can configure and upgrade the door phone on the web interface via one-time auto- provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-provisioning

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

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

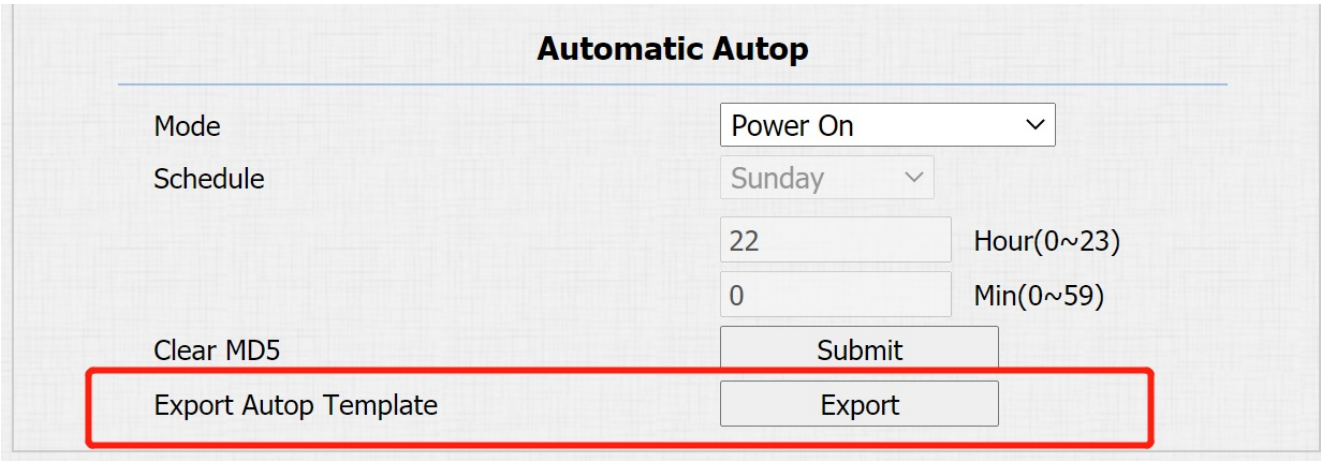
- **General configuration provisioning**: a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices, such as cfg.
- **MAC-based configuration provisioning**: MAC-based configuration files are used for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

Note

- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will first access the general configuration files before accessing the MAC-based configuration files.

You may click **here** to see the detailed format and steps.

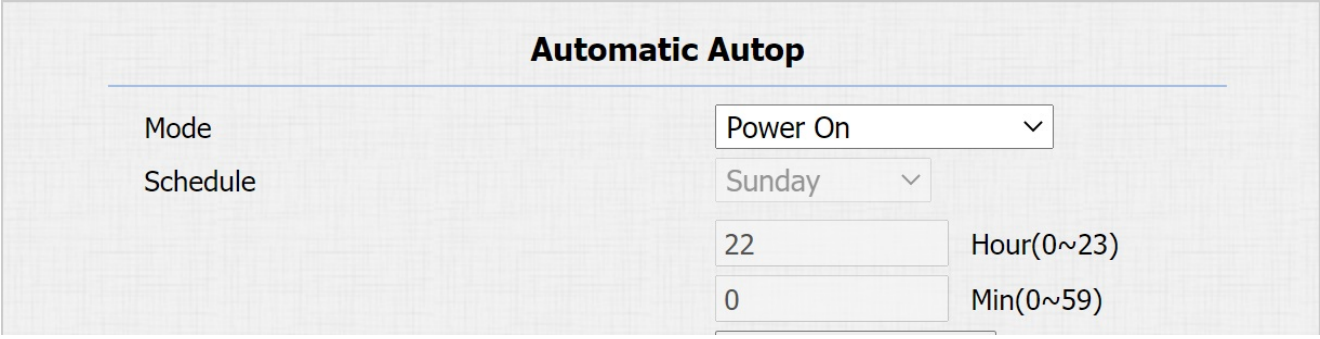
To get the Autop configuration file template on **Upgrade > Advanced > Automatic Autop** interface.



AutoP Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself according to the schedule.

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



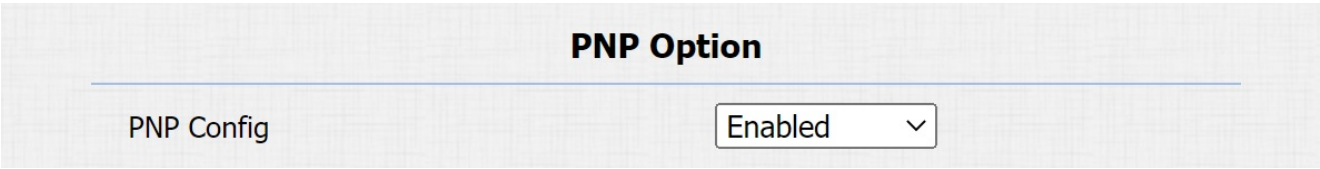
Parameter Set-up:

- **Mode**:
  - Select **Power On**, if you want the device to perform Autop every time it boots up.
  - Select **Repeatedly**, if you want the device to perform autop according to the schedule you set up.
  - Select **Power On + Repeatedly** if you want to combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
  - Select **Hourly Repeat** if you want the device to perform Autop every hour.
- **Schedule**: if **Repeatedly** is selected, you can set up the time schedule for the AutoP.

PNP Configuration

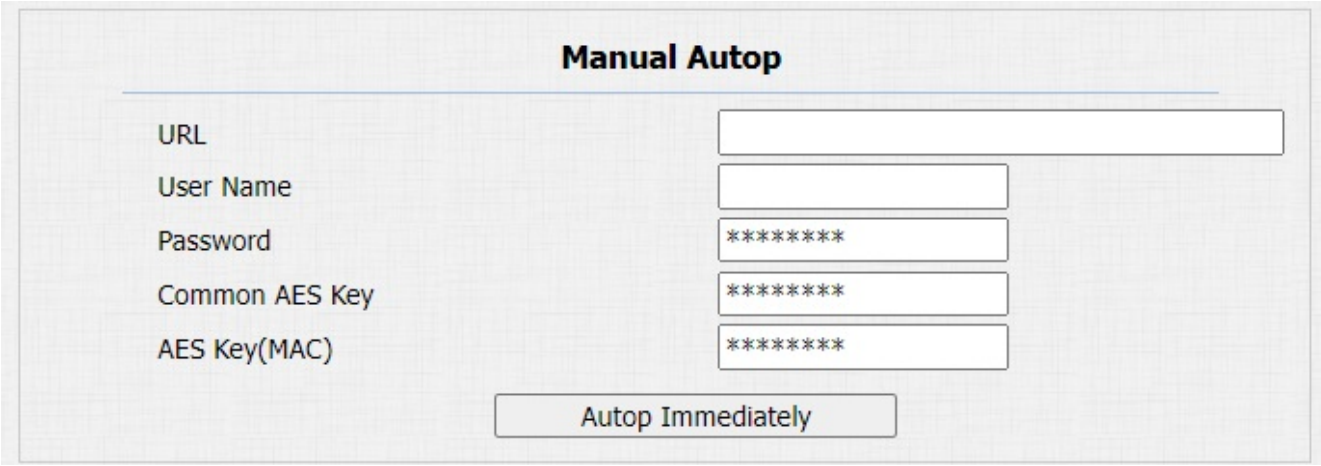
Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

To do this configuration on web **Upgrade > Advanced > PNP Option** interface.



Static Provisioning Configuration

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



Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, FTP server address for the provisioning
- **Common AES Key**: set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Tip

- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.

Note

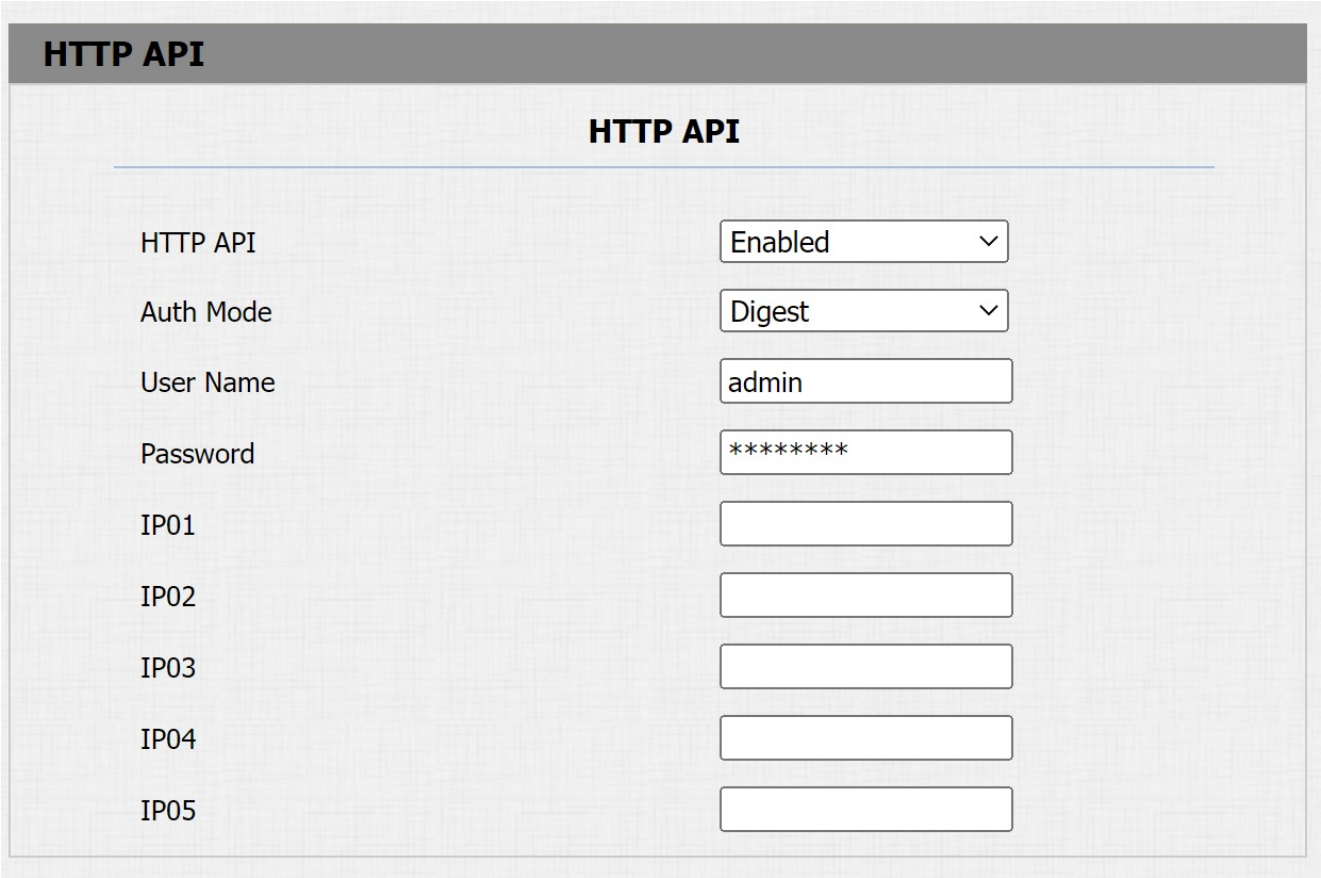
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (allows anonymous login) ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/ (use the default port 80) http://192.168.0.19:8080/ (use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/ (use the default port 443)
- Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Integration with Third Party Device

Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device and the Akuvox device.

Go to **Intercom > HTTP API** interface for the integration.



Parameter Set-up:

- **HTTP API**: enable or disable the HTTP API function for the third party integration. For example, if the function is disabled, any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Authorization Mode**: select among six options: **None**, **Normal**, **White List**, **Basic**, **Digest**, and **Token** for authorization type, which will be explained in detail in the following chart.
- **User Name**: enter the user name when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.

- **Password**: enter the password when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **IP 01-05**: enter the IP address of the third party devices when the **WhiteList** authorization is selected for the integration.

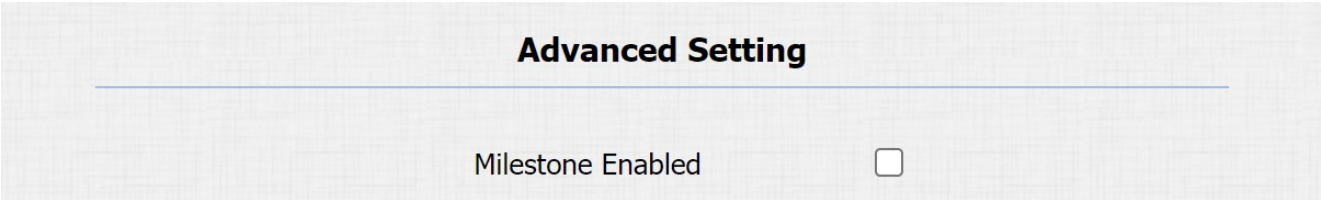
Please refer to the following description for the Authentication mode:

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

Integration with Milestone

If you want the door phone to be monitored by Milestone or any third-party devices that have been integrated with Milestone, you need to enable the feature.

Path: **Intercom > ONVIF > Advanced Setting**



Note

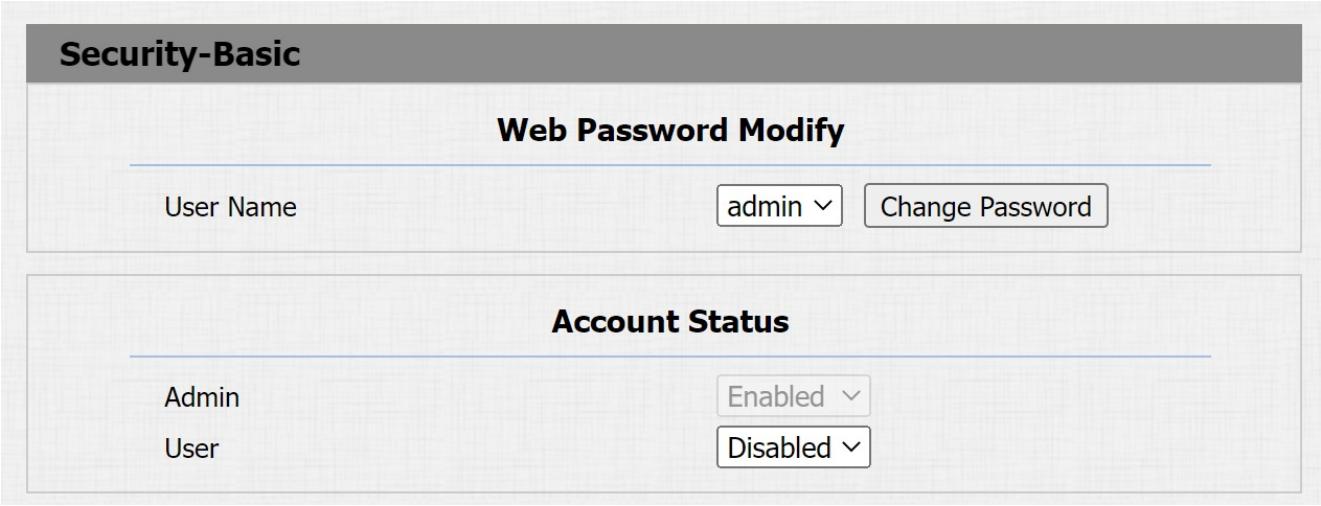
- Please read the details and configuration of the integration in https://knowledge.akuvox.com/docs/integration-with-milestone-v1-202008019

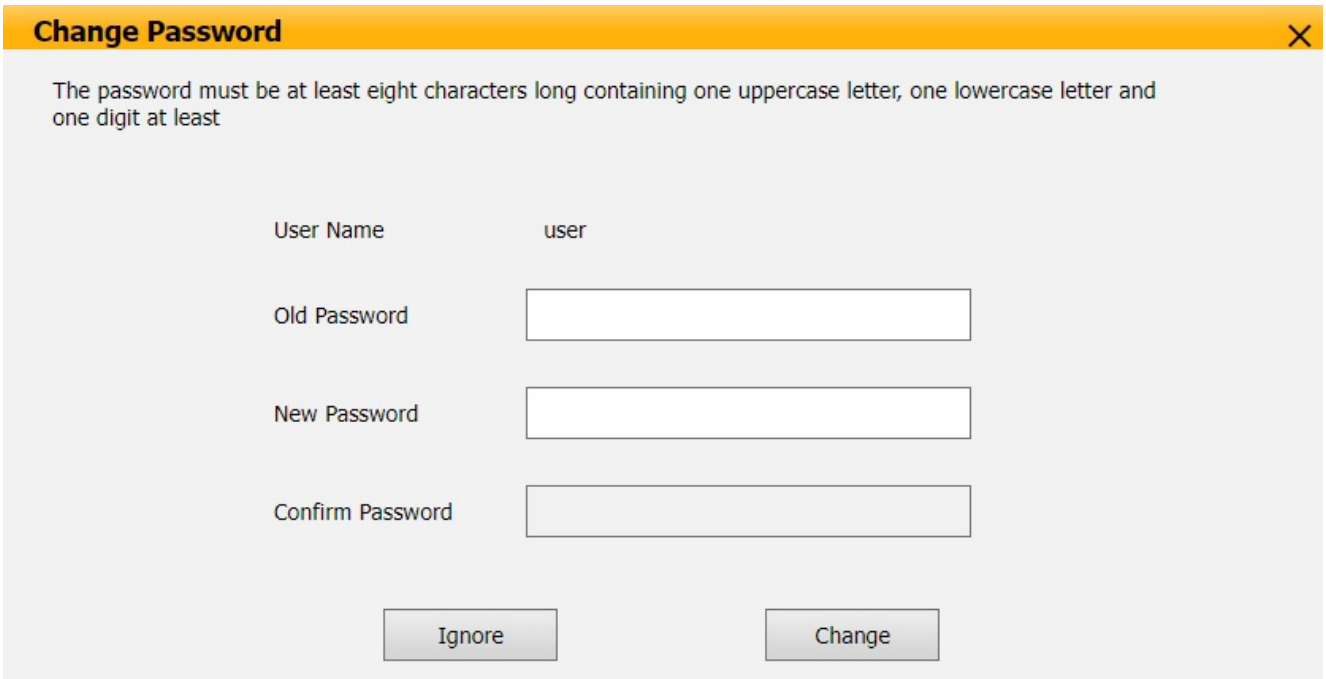
Password Modification

Modifying Device Web Interface Password

To change the default web password on web **Security > Basic** interface.

Select **admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.

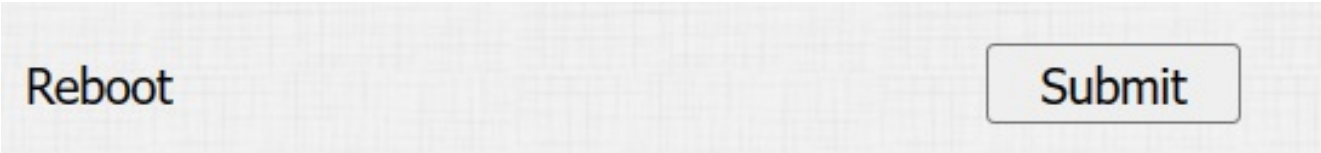




System Reboot&Reset

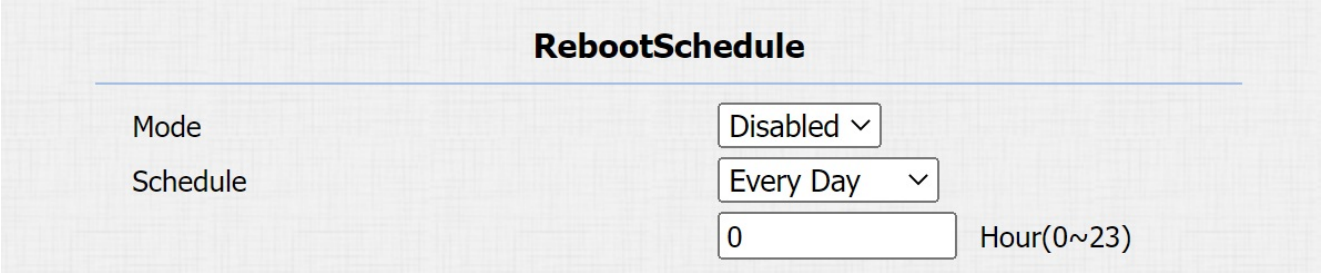
Reboot

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



Reboot Schedule

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



Reset

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