Table of contents

Akuvox E21 Series Door Phone Administrator Guide

About This Manual 4
Product Overview 6
Changelog 7
Model Specification 8
Introduction to Configuration Menu 9
Access the Device 10
  Obtain Device IP Address 10
  Access the Device Web Settings 11
Language and Time 12
  Language 12
  Time 12
LED Setting 14
  Infrared LED Setting 14
  LED Control 14
  Photoresistor Setting 14
Volume and Tone 16
  Volumes 16
  Open Door Tones 17
  Upload Tone Files 17
Network Setting 18
  Network Status 18
  Device Network Configuration 18
  Device Deployment in Network 19
  Device Local RTP 20
  SNMP Setting 20
  VLAN Setting 21
  TR069 Setting 21
  Device Web HTTP Setting 22
  NAT Setting 23
Intercom Call Configuration 25
  IP Call & IP Call Configuration 25
  SIP Call & SIP Call Configuration 25
    SIP Account Registration 25
    SIP Server Configuration 26
  Outbound Proxy Server 27

Data Transmission Type 28
SIP Hacking Protection 28
Call Settings 30
Do Not Disturb 30
Maximum Call Duration 30
Maximum Dial Duration 31
Auto-answer Configuration 31
Hang Up After Opening the Door 32
Group Call 33
Sequence Call 34
Push Button Action 35
Push to Hang Up 35
Multicast 36
Web Call 37
Call Schedule 38
Audio & Video Codec Configuration 40
Audio Codec Configuration 40
Video Codec Configuration 41
Video Codec for IP Direct Calls 41
Relay Setting 43
Local Relay 43
Web Relay 44
Access Control Schedule Management 47
Configure Door Access Schedule 47
Create Door Access Schedule 47
Relay Schedule 48
Door-opening Configuration 50
Unlock by HTTP Command 50
Unlock by DTMF Code 51
DTMF White List 51
DTMF Data Transmission 52
Unlock by Exit Button 53
Monitor and Image 56
MJPEG Image Capturing 56
RTSP Stream Monitoring 58
RTSP Basic Setting 58
RTSP Stream Setting 59
H.264 Video Parameters Setup 59
ONVIF 60
Live Stream 61

Security 63
Client Certificate Setting 63
Web Server Certificate 63
Motion Detection 63
Security Notification 65
Email Notification 65
FTP Notification 66
SIP Call Notification 66
Action URL 67
Voice Encryption 68
User Agent 68
High Security Mode 69
Real-time Monitoring 70
Emergency Audio-Visual Alert Setup 70
Logs 73
Firmware Upgrade 74
Auto-provisioning via Configuration File 75
Provisioning Principle 75
Configuration Files for Auto-provisioning 76
AutoP Schedule 77
Static Provisioning Configuration 78
PNP Configuration 80
Backup 81
Debug 82
System Log 82
PCAP 82
Remote Debug Server 83
Integration with Third Party Device 84
Integration via HTTP API 84
Integration with Milestone 85
Password Modification 87
System Reboot&Reset 88
Reboot 88
Reset 88

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



E21
DOOR PHONE
Administrator Guide

Thank you for choosing the Akuvox E21 series door phone. This manual is intended for the administrators who need to properly configure the door phone. This manual applies to version 321.30.10.34.

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

Changelog

What's new in version 321.30.10.34:

- Expanded the maximum dial duration range from 5–120 seconds to 5–300 seconds.

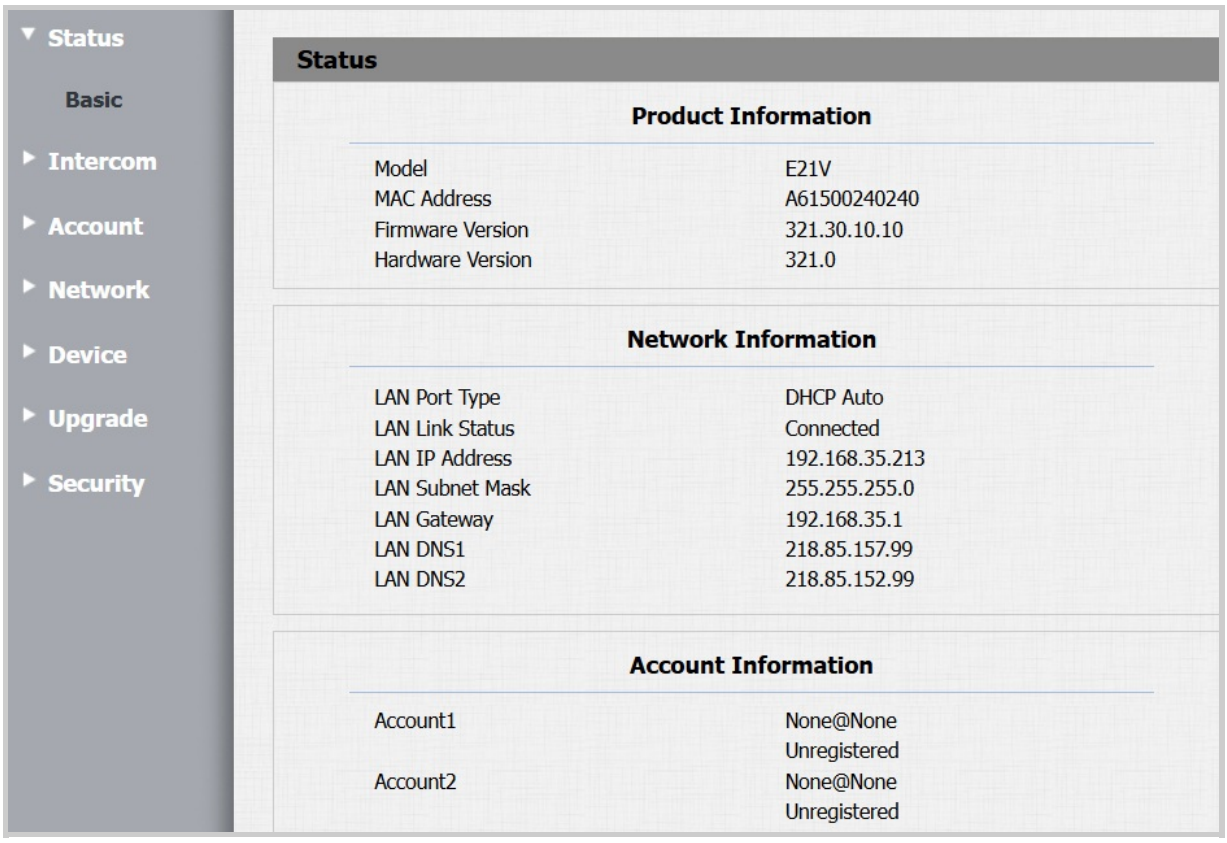
Click here to view the changelog of the device's previous versions.

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

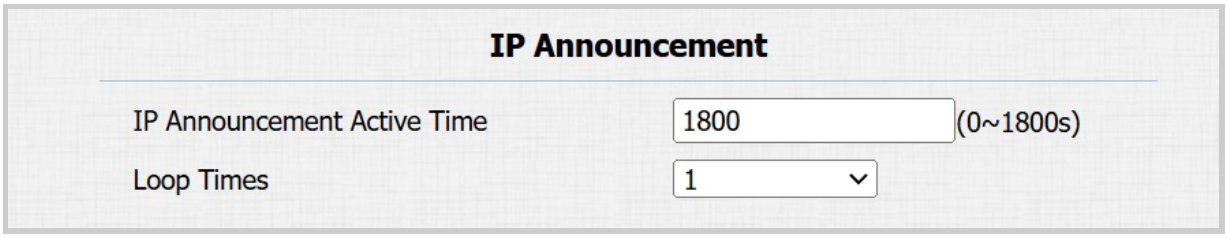


Access the Device

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

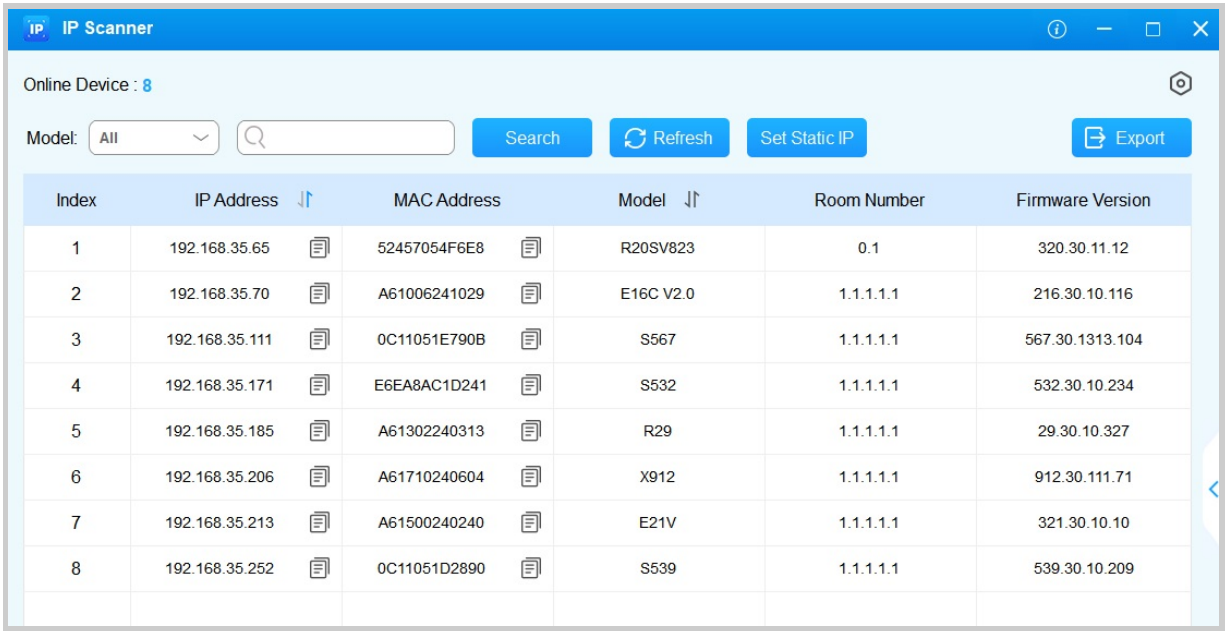
Obtain Device IP Address

Hold the device push button for 5 seconds and it will announce the IP address. You can set up the IP announcement loop times on the **Device > Voice** interface.



- **IP Announcement Active Time:** Set the time within which users should hold the call button to make the device pronounce the IP address after the device reboots.
- **Loop Times:** Set the IP announcement loop times.

Or, search the device IP by the IP scanner in the same LAN network.

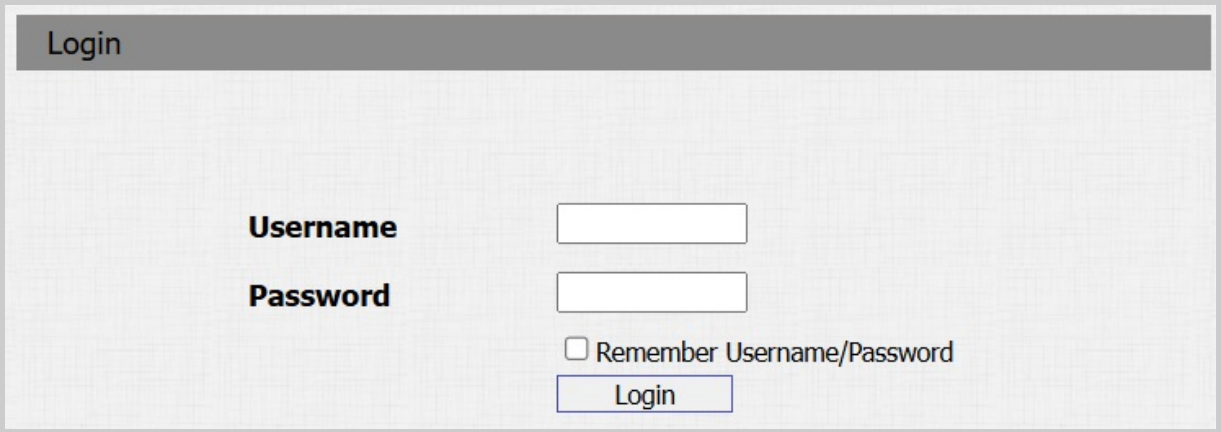


Index	IP Address	MAC Address	Model	Room Number	Firmware Version
1	192.168.35.65	52457054F6E8	R20SV823	0.1	320.30.11.12
2	192.168.35.70	A61006241029	E16C V2.0	1.1.1.1.1	216.30.10.116
3	192.168.35.111	0C11051E790B	S567	1.1.1.1.1	567.30.1313.104
4	192.168.35.171	E6EA8AC1D241	S532	1.1.1.1.1	532.30.10.234
5	192.168.35.185	A61302240313	R29	1.1.1.1.1	29.30.10.327
6	192.168.35.206	A61710240604	X912	1.1.1.1.1	912.30.111.71
7	192.168.35.213	A61500240240	E21V	1.1.1.1.1	321.30.10.10
8	192.168.35.252	0C11051D2890	S539	1.1.1.1.1	539.30.10.209

Access the Device Web Settings

You can enter the device IP address in a browser and log into the device web interface where you can configure and adjust parameters.

The initial username and password are both **admin** and please be case-sensitive to the username and password entered.



Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the 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

Language

Select the device web language on the **Device > Time/Lang > Web Language** interface.

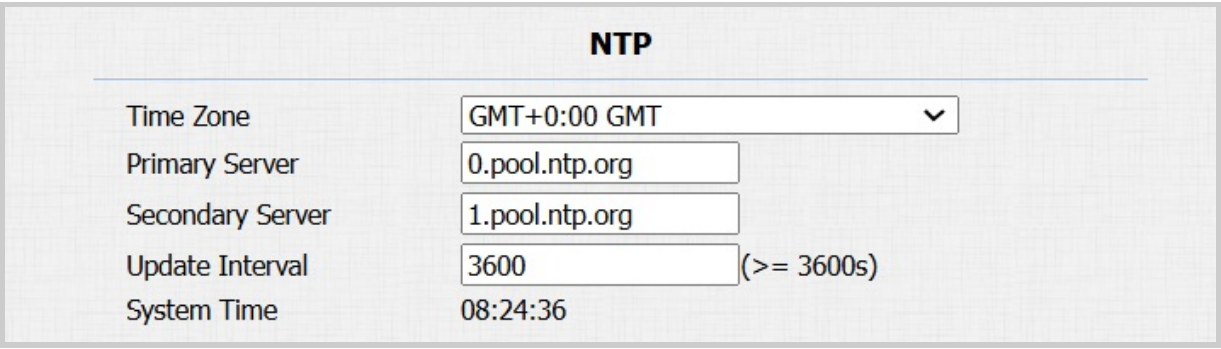


- **Type**: The device supports English, Simplified Chinese, Traditional Chinese, Spanish, French, German, Italian, and Dutch.

Time

The time settings on the web interface allow you to configure the NTP server address for automatic time and date synchronization. Once a time zone is selected, the device will notify the NTP server of the chosen time zone, enabling it to synchronize the time zone settings on your device.

Set up time on the **Device > Time/Lang > NTP** interface.



- **Time Zone**: Select the specific time zone based on where the device is used. The default time zone is GMT+0:00.

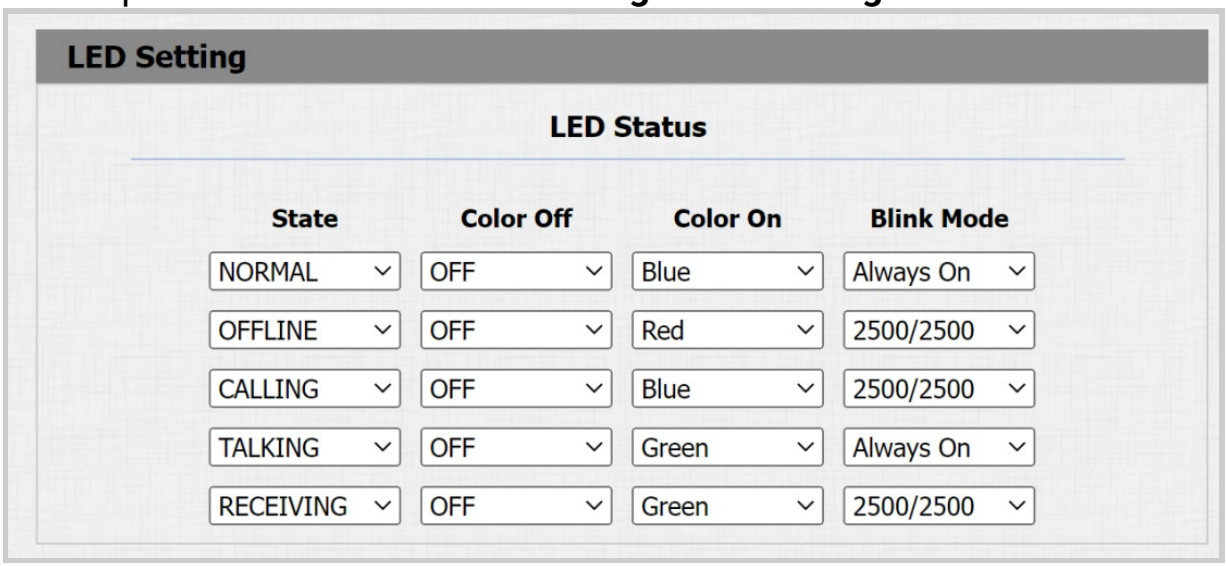
- **Primary Server**: Enter the primary NTP server address for updating the time. The default NTP server address is 0.pool.ntp.org.
- **Secondary Server**: Enter the backup NTP server address when the primary one fails.
- **Update Interval**: Set the time update interval. For example, if you set it as 3600s, the device will send a request to the NTP server for the time update every 3600 seconds.
- **System Time**: Display the current device time.

LED Setting

Infrared LED Setting

Infrared LED is mainly designed to reinforce the light for facial recognition at night or in a dark environment.

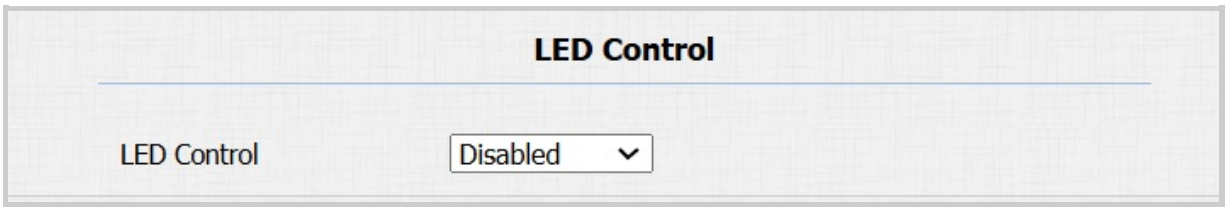
Set it up on the **Intercom > LED Setting > LED Setting** interface.



- **Device Status:** There are five statuses, Normal, Offline, Calling, Talking, and Receiving. The status cannot be changed.
- **Color:** Select from Red, Green, Blue, and Yellow.
- **Display Mode:** Set the different flashing frequencies.

LED Control

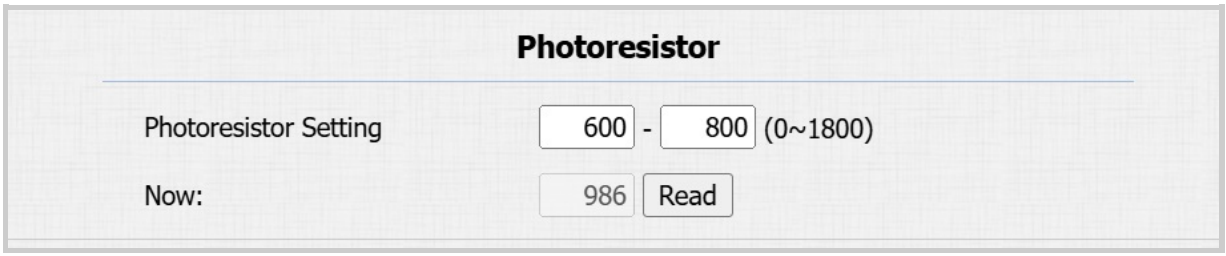
You can enable or disable the LED on the **Intercom > LED Setting** interface.



Photoresistor Setting

You can set the minimum and maximum photoresistor value to automatically control the ON-OFF of the infrared fill light.

To set it up, go to the **Intercom > Advanced** interface.



- **Photoresistor Setting**: If the photoresistor value is less than the minimum threshold, turn off the infrared fill light. If the photoresistor value is greater than the maximum threshold, turn it on.
- **Now**: Click **Read** to obtain the current photoresistor value.

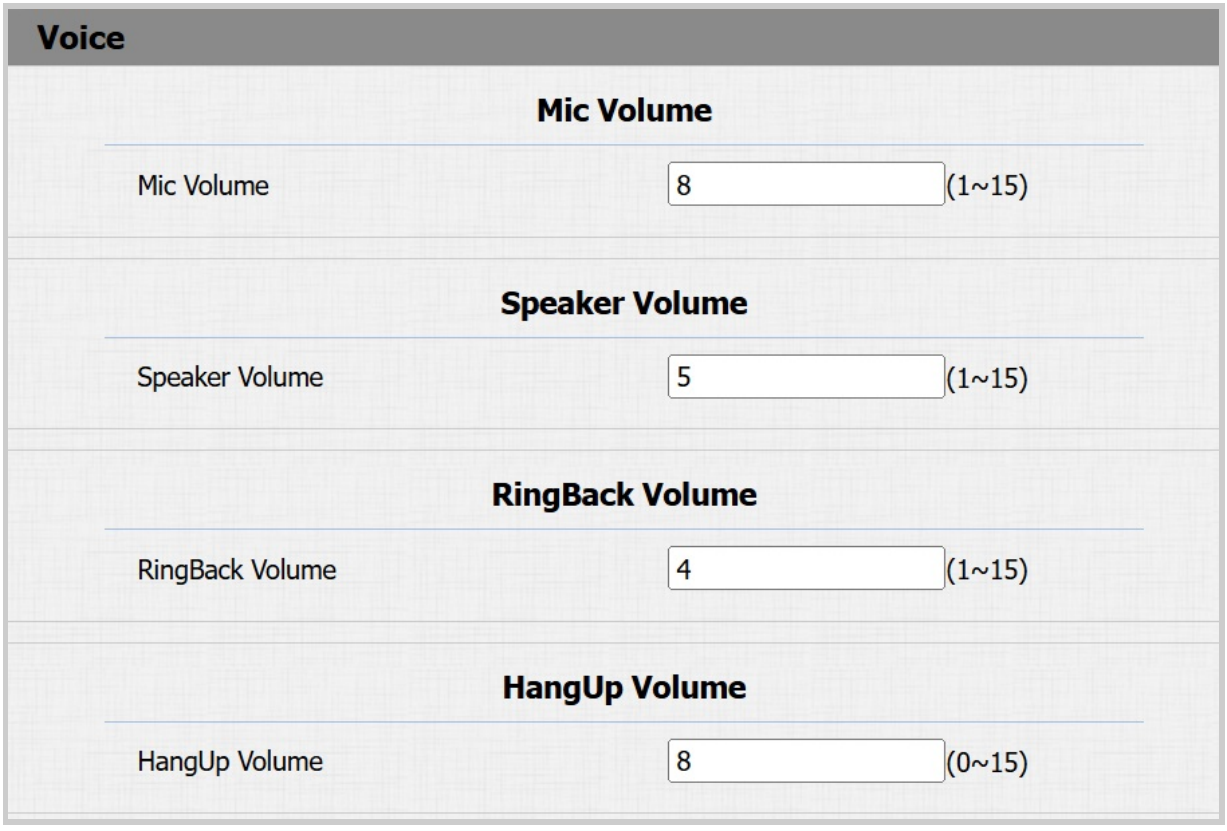
Volume and Tone

Volume and ringtone configurations include microphone volume, speaker volume, alarm volume, and more. In addition, you can upload door-opening tones to enrich the user's personalized experience.

Volumes

You can configure the volume of the microphone, speaker, etc. Moreover, you can also set up the tamper alarm volume when unwanted removal of the device occurs.

To set up volumes, go to the web **Device > Voice** interface.



- **Mic Volume**: The default is 8.
- **Speaker Volume**: The default is 8.
- **Ringback Volume**: The default is 5.
- **Hangup Volume**: The default is 8. The sound plays when users hang up a call.

Open Door Tones

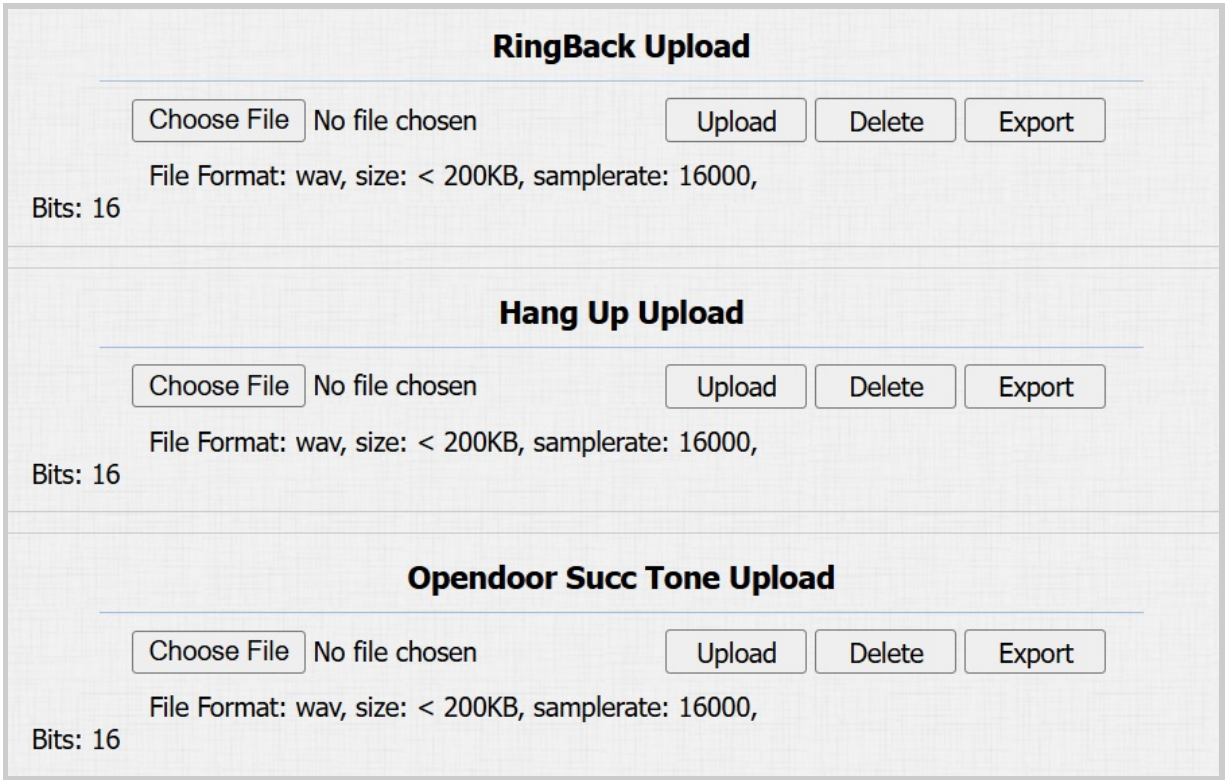
You can enable or disable the door-opening succeeded tone on the web **Device > Voice** interface.



Upload Tone Files

You can customize ringback and door-opening tones.

Upload files on the **Device > Voice** interface.

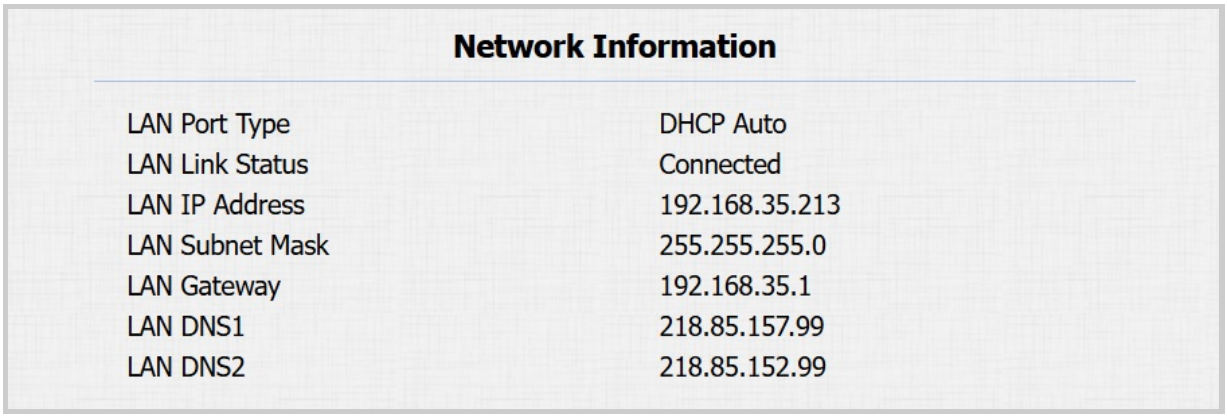


- **RingBack Upload**: The tone is heard by users who call the device.
- **Hang Up Upload**: The tone plays when users hang up a call.
- **Open Door Success Tone Upload**: The tone plays when the door opens successfully.

Network Setting

Network Status

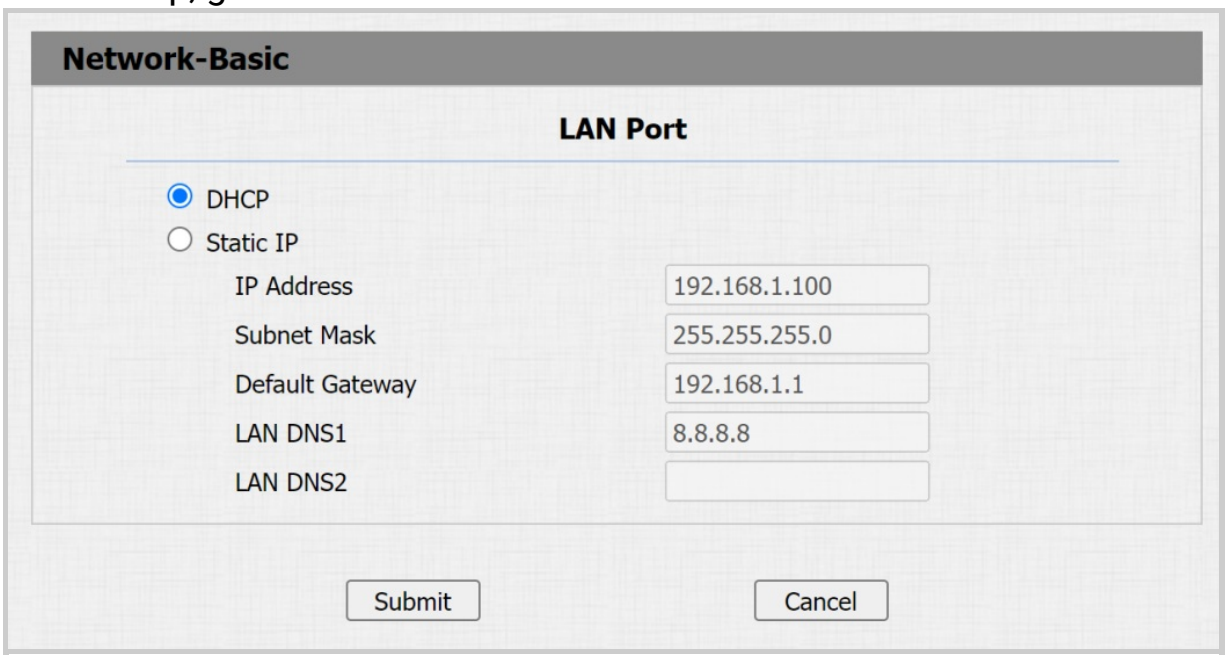
Check the network status on the **Status > Network Information** interface.



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.

To set it up, go to **Network > Basic** interface.

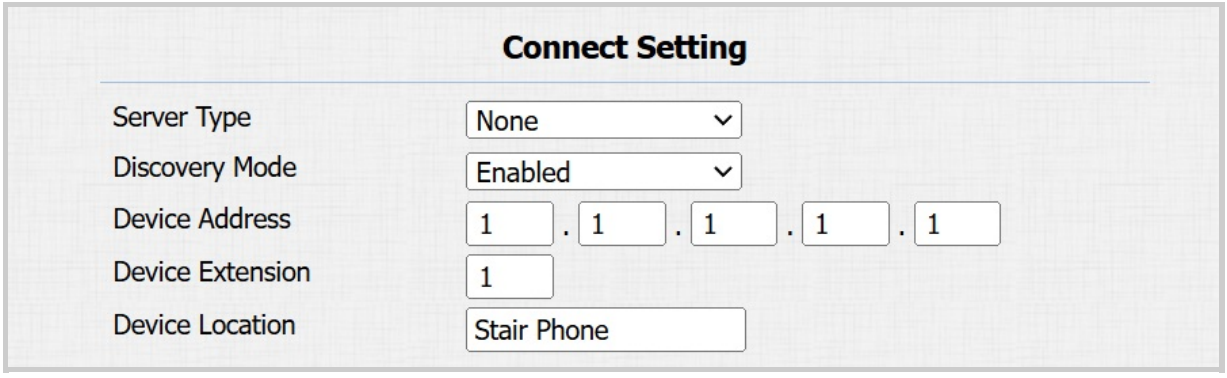


- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, the IP address, subnet mask, default gateway, and DNS server address should be configured according to the network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected.
- **Subnet Mask**: Set up the subnet mask according to the actual network environment.
- **Default Gateway**: Set up the correct gateway according to the IP address.
- **LAN DNS1/2**: Set up the preferred or alternate Domain Name Server(DNS) server according to the actual network environment. The preferred DNS server is the primary server while the alternate DNS server is the secondary one. The secondary server is for backup.

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.

To set it up, navigate to the web **Network > Advanced > Connect Setting** interface.



- **Server Type**: It is automatically set up according to the device connection with a specific server in the network such as SDMC, Cloud, or None. **None** is the default factory setting indicating the device is not in any server type.

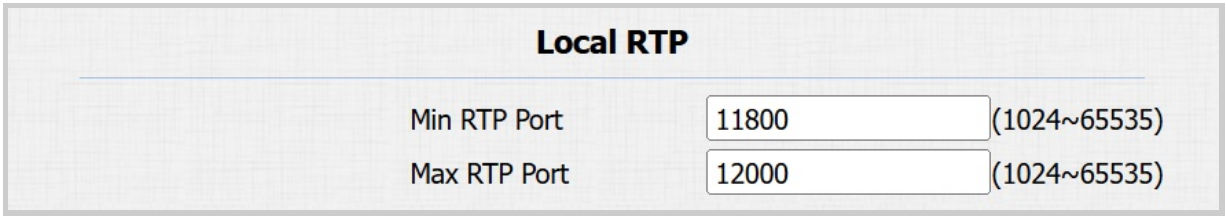
- **Discovery Mode**: When enabled, the device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: The device extension number.
- **Device Location**: The location in which the device is installed and used.

Device Local RTP

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.

To set it up, go to the **Network > Advanced** interface.

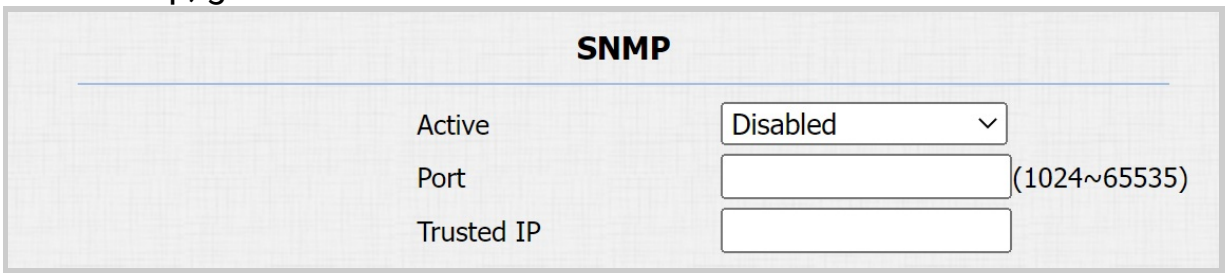


- **Min RTP Port**: The port value for establishing the start point for the exclusive data transmission range.
- **Max RTP Port**: The port value for establishing the endpoint for the exclusive data transmission range.

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 set it up, go to the **Network > Advanced > SNMP** interface.

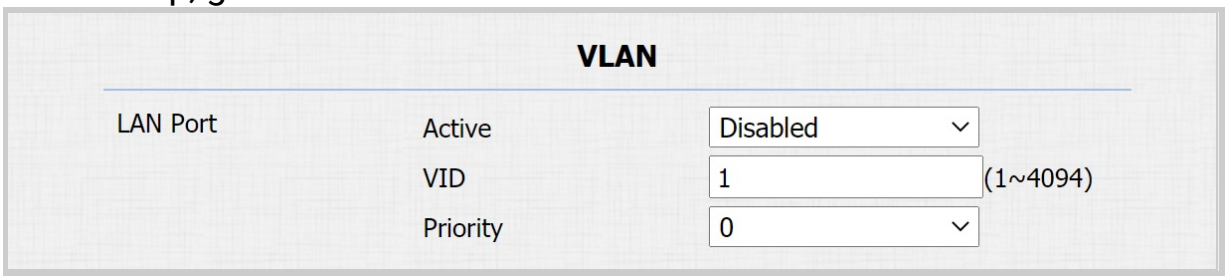


- **Port**: The SNMP server's port.
- **Trusted IP**: The allowed SNMP server address. It can be an IP address or any valid URL domain name.

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 set it up, go to the **Network > Advanced > VLAN** interface.

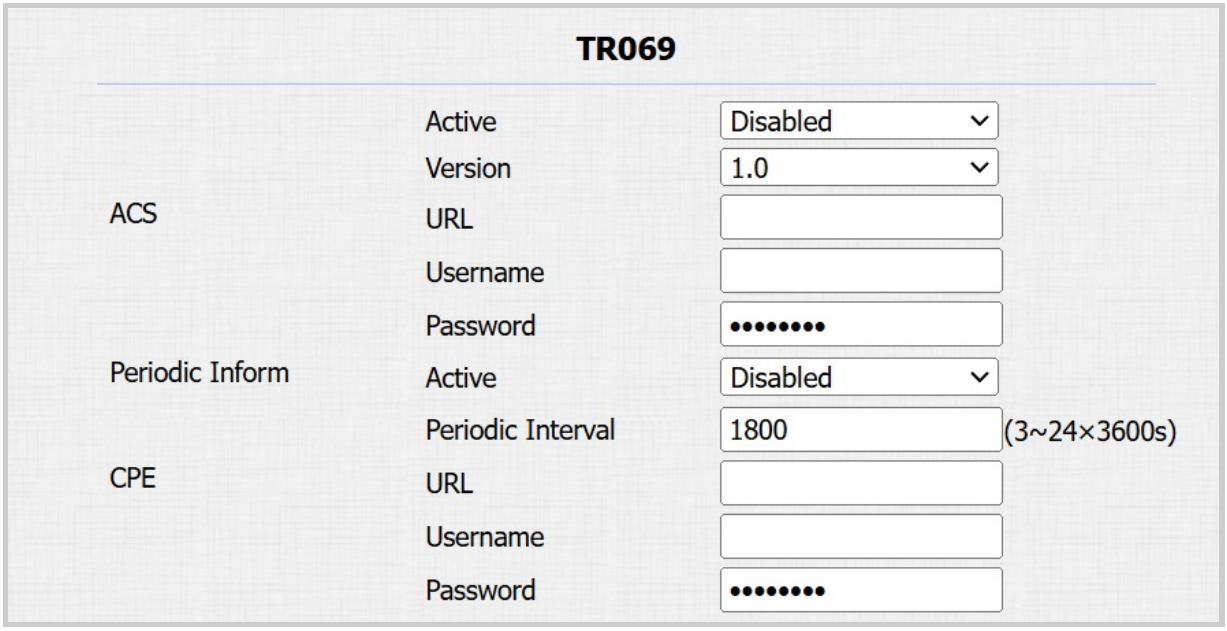


- **VID**: The VLAN ID for the designated port.
- **Priority**: The VLAN priority for the designated port.

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 set it up, go to the **Network > Advanced > TR069** interface.

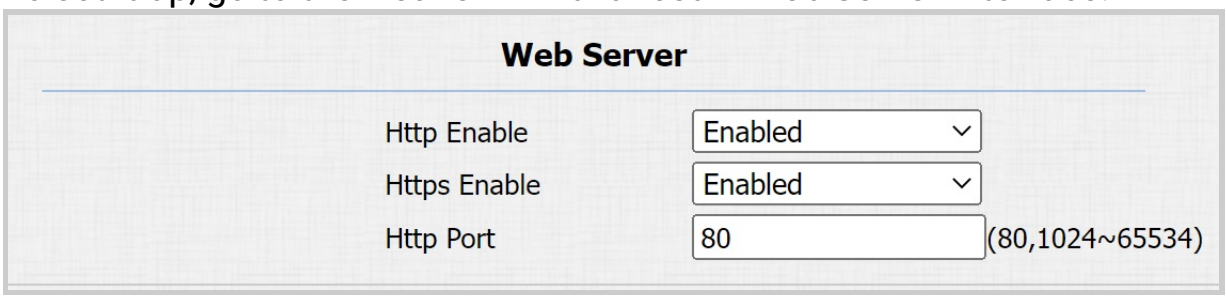


- **Version**: Select the supported TR069 version (version 1.0 or 1.1).
- **ACS/CPE URL**: The URL address for ACS or CPE. ACS is short for auto-configuration servers on the server side, and CPE is short for customer-premise equipment as client-side devices.
- **Periodic Interval**: The interval for periodic notifications.

Device Web HTTP Setting

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

To set it up, go to the **Network > Advanced > Web Server** interface.



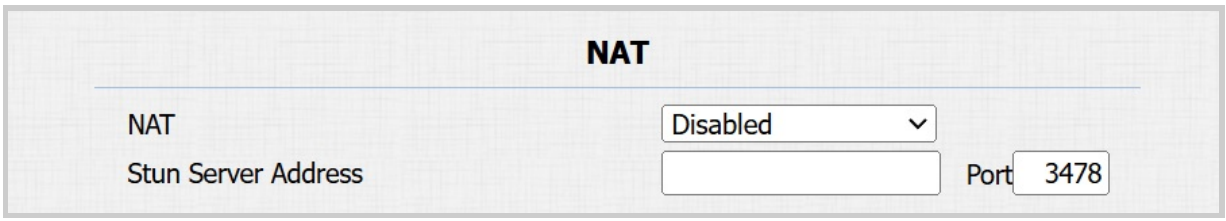
- **HTTP Port**: The port for the HTTP access method. 80 is the default port.

NAT Setting

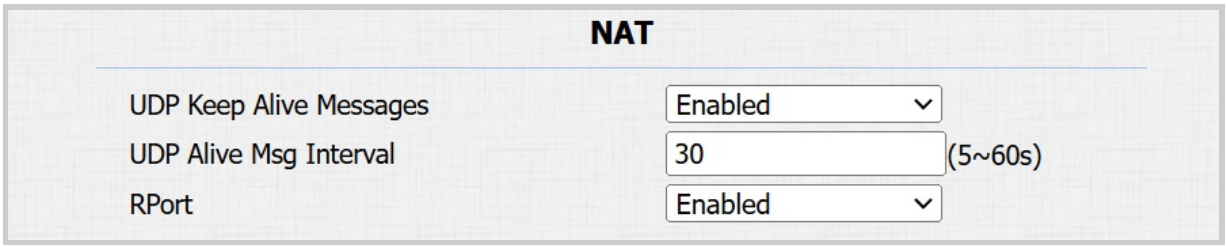
Network Address Translation(NAT) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses and hides the internal IP addresses and ports from the outside world.

To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

To set up NAT, navigate to the **Account > Basic > NAT** interface.



- **Stun Server IP**: Set the SIP server address in the Wide Area Network(WAN).
- **Port**: Set the SIP server port.



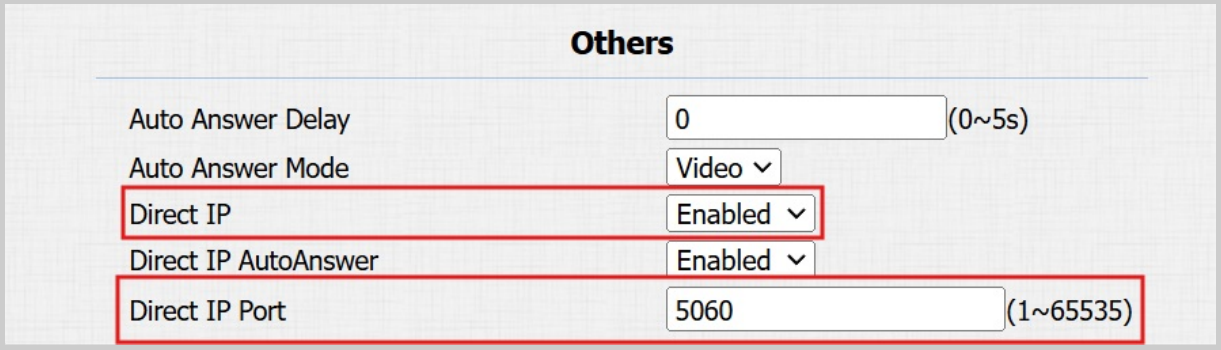
- **UDP Keep Alive Messages**: If enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval**: The message-sending time interval ranges from 5 to 60 seconds. The default is 30 seconds.
- **RPort**: Enable the RPort when the SIP server is in WAN.

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.

Enable or disable the direct IP call function on the web **Device > Call Feature** interface.



- **Port**: Set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

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.

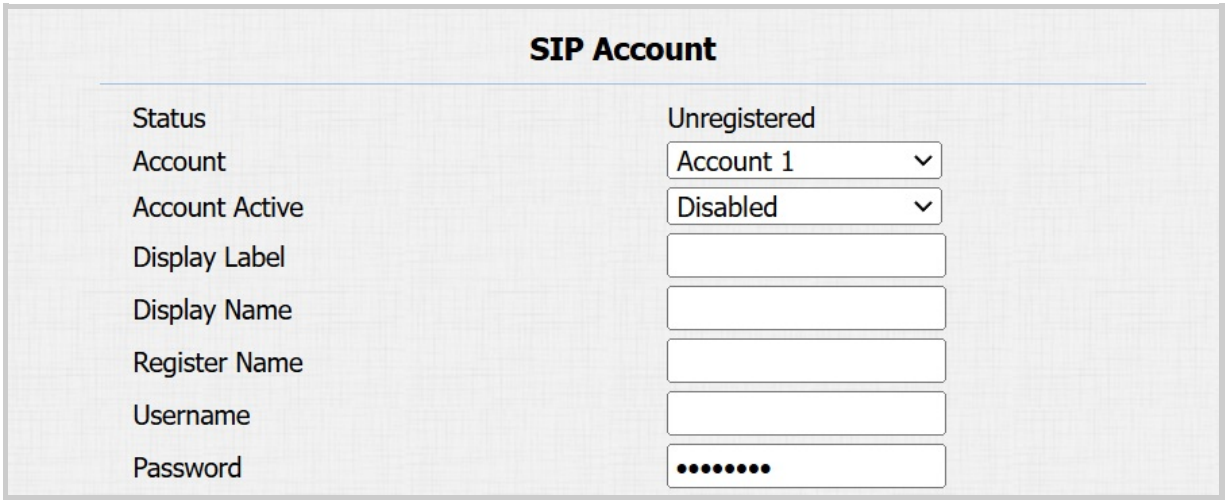
SIP Account Registration

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.

Click here to view the SIP account registration example.

Register SIP account on the web **Account > Basic** interface.

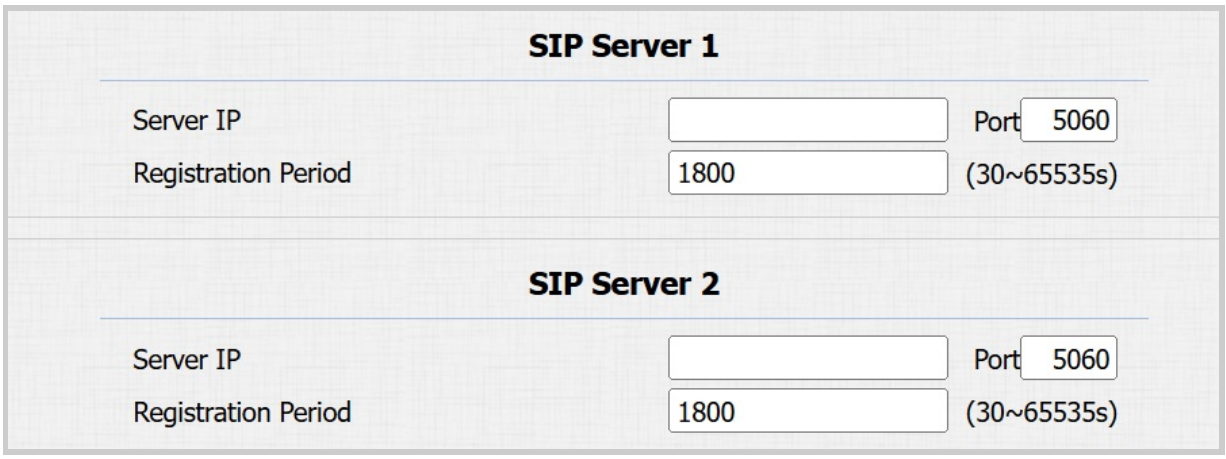


- **Status**: Displays whether the SIP account is registered or not.
- **Account 1/Account 2:** The door phone supports 2 SIP accounts.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
  - The system switches to Account 2 if Account 1 is not registered.
- **Account Active**: Check to activate the registered SIP account.
- **Display Label**: The device label to be shown on the device screen.
- **Display Name**: The device's name to be shown on the device being called to.
- **Register Name:** Same as the username from the PBX server.
- **Username:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

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 configure the SIP server, go to the web **Account > Basic** interface.

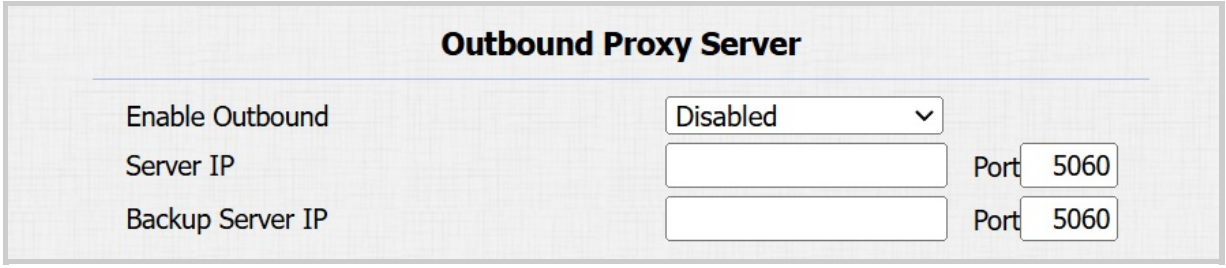


- **Server IP**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified period.

Outbound Proxy Server

An outbound proxy server receives and forwards all requests the designated server. It is an optional configuration, but if set it up, all future SIP requests get sent there in the first instance.

To set it up, go to the web **Account > Basic > Outbound Proxy Server** interface.

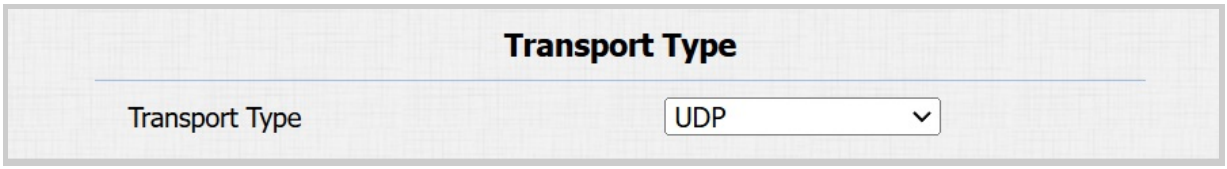


- **Server IP**: Enter the SIP proxy IP address.
- **Port**: Set the port for establishing a call session via the outbound proxy server.
- **Backup Server IP**: Enter the SIP proxy IP address to be used when the main proxy malfunctions.
- **Port**: Set the proxy port for establishing a call session via the backup outbound proxy server.

Data Transmission Type

Akuvox intercom devices support four data transmission protocols: **User Datagram Protocol(UDP)**, **Transmission Control Protocol(TCP)**, **Transport Layer Security**(**TLS**), and **DNS-SRV**.

To set it up, go to the web **Account > Basic** interface.

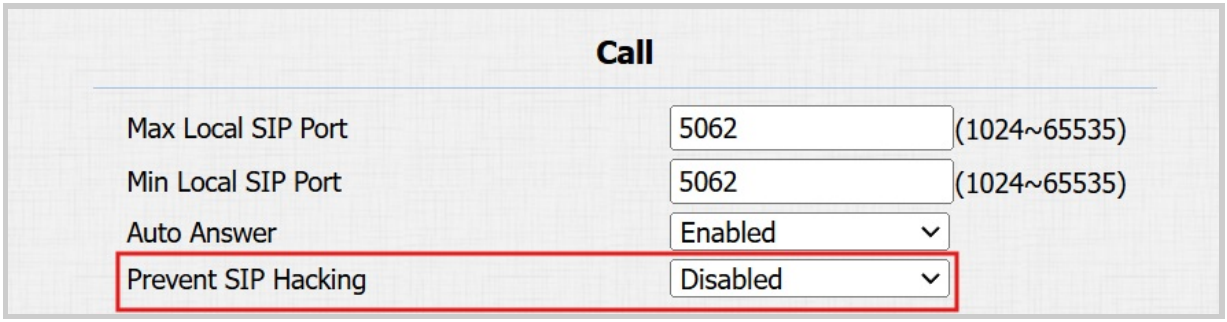


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.

SIP Hacking Protection

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.

Enable or disable this function on **Account > Advanced > Call** interface.



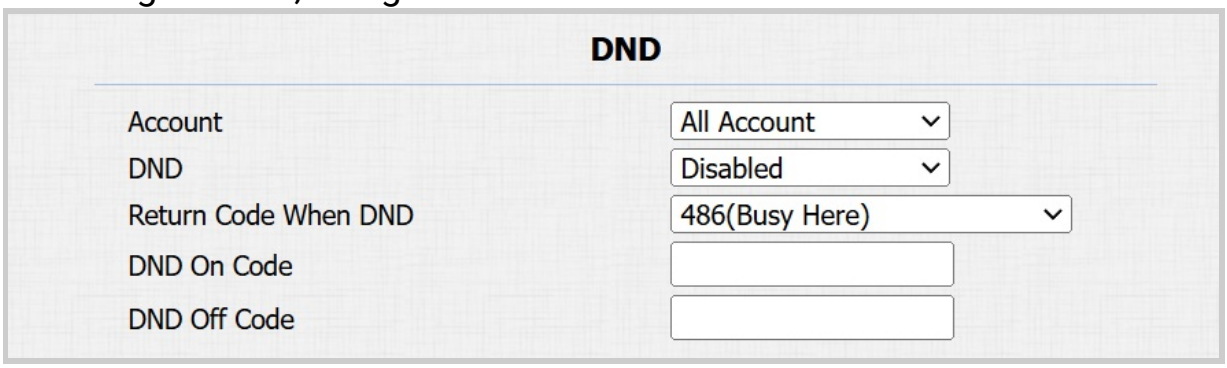
- **Prevent SIP Hacking**: Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Settings

Do Not Disturb

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.

To configure DND, navigate to the web **Device > Call Feature** interface.

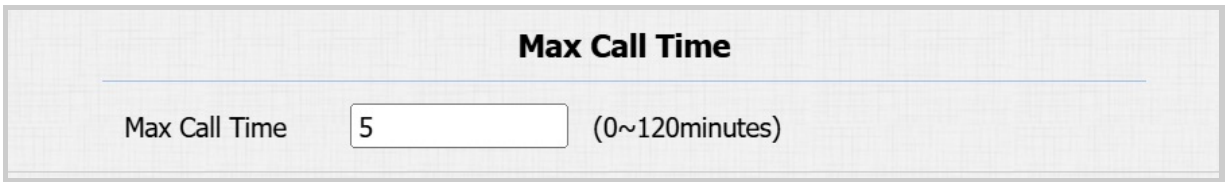


- **Account**: The account to apply the DND feature.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.
- **DND On Code**: The code used to turn on DND in the SIP server.
- **DND Off Code**: The code used to turn off DND in the SIP server.

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.

To configure call time duration, navigate to the web **Intercom > Basic** interface.

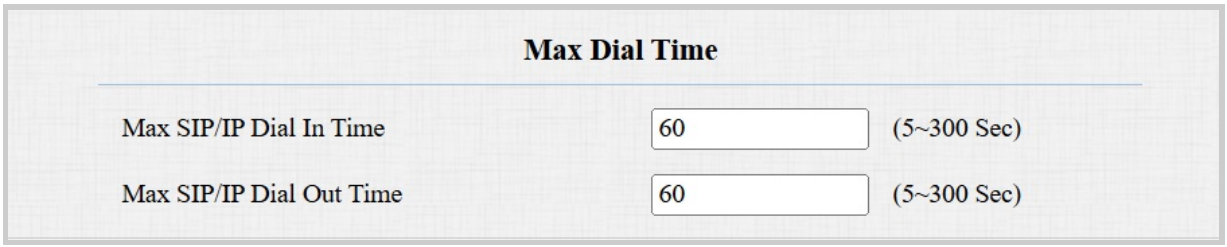


- **Max Call Time**: Specify the maximum duration of all calls. The door phone will end the call automatically when the time limit is reached.

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.

To configure maximum dial duration, navigate to the web **Intercom > Basic** interface.

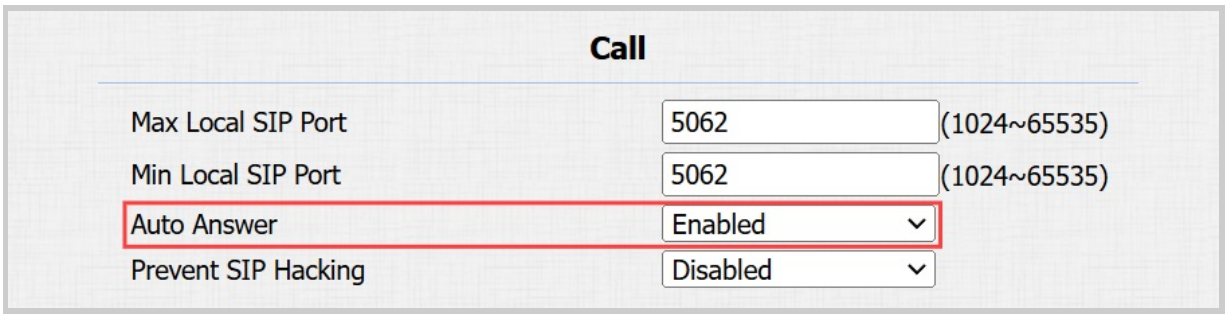


- **Max SIP/IP Dial In Time**: Specify the maximum duration of an incoming call. The door phone will automatically end the incoming call if it is not answered within the preset time.
- **Max SIP/IP Dial In Time**: Specify the maximum duration of an outgoing call. The door phone will automatically end the call it dialed out if there is no answer from the recipient within the preset time.

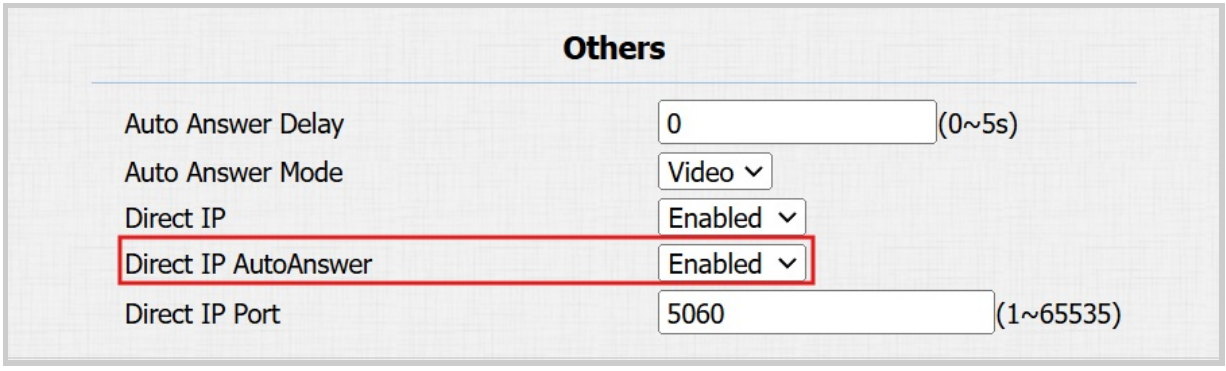
Auto-answer Configuration

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 auto-answer for SIP calls, navigate to the web **Intercom > Call Feature** interface.



To enable auto-answer for IP calls, navigate to the web **Device > Call Feature > Others** interface.

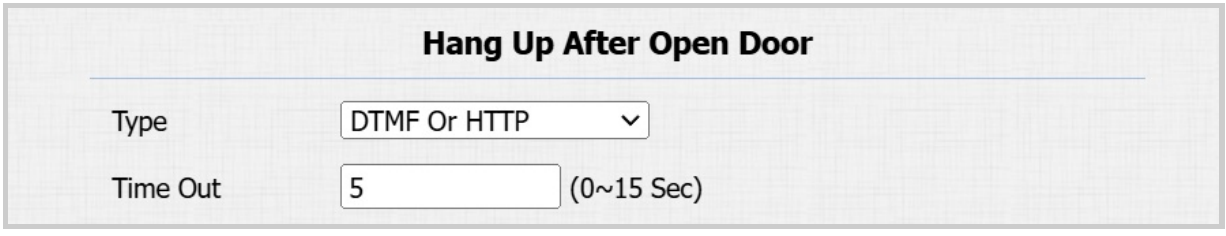


- **Auto Answer Delay**: Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the door phone will answer the call automatically after 5 seconds.
- **Auto Answer Mode**: Determine whether to auto-answer the call as a video or audio call.

Hang Up After Opening the Door

This feature automatically ends the call once the door is released, allowing for the seamless reception of subsequent calls.

To configure it, navigate to the web **Intercom > Basic** interface.



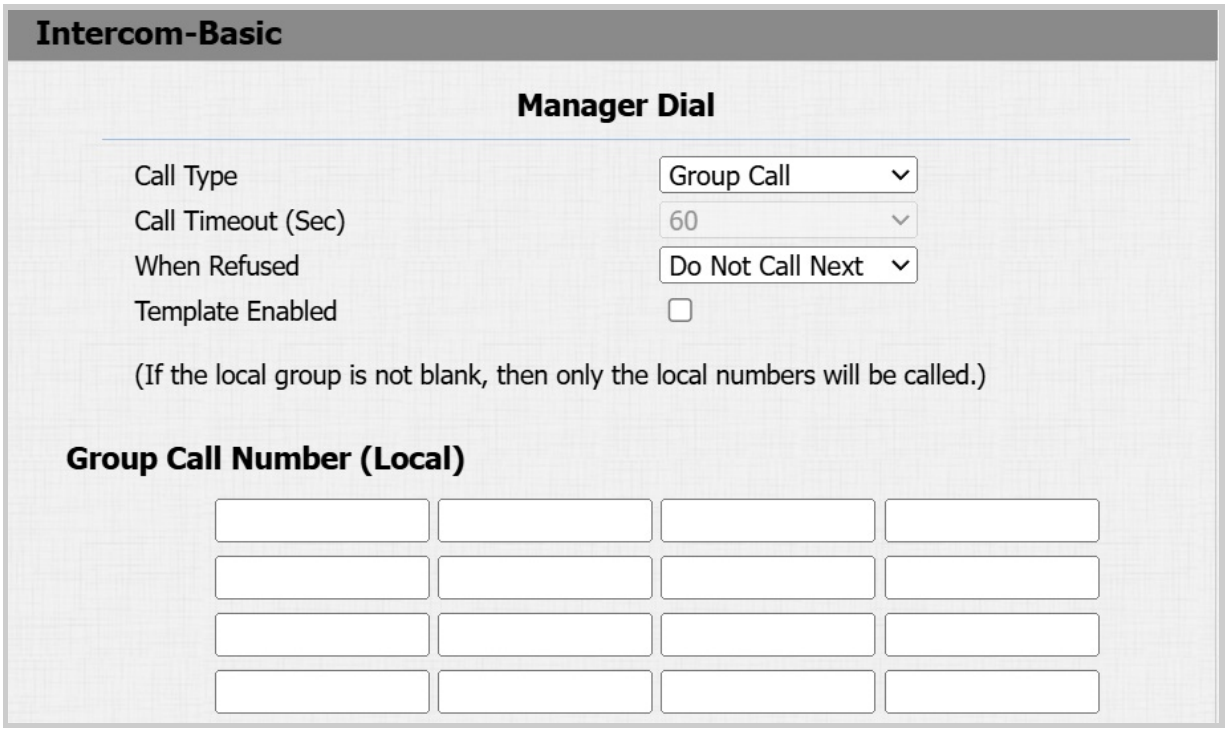
- **Type**: Specify the door unlock method. If this specific method is used to release the door during a call, the door phone will end the call when the preset hang-up time is reached.

- **Time Out**: Specify the hang-up time limit. The door phone will automatically terminate the call when the specific time is reached after the door is opened.

Group Call

This feature allows users to call a group of contacts by a single press. The device supports local and SmartPlus-featured group calls. To learn about the detailed configuration, please click here.

To configure the group call, navigate to the web **Intercom > Basic** interface.

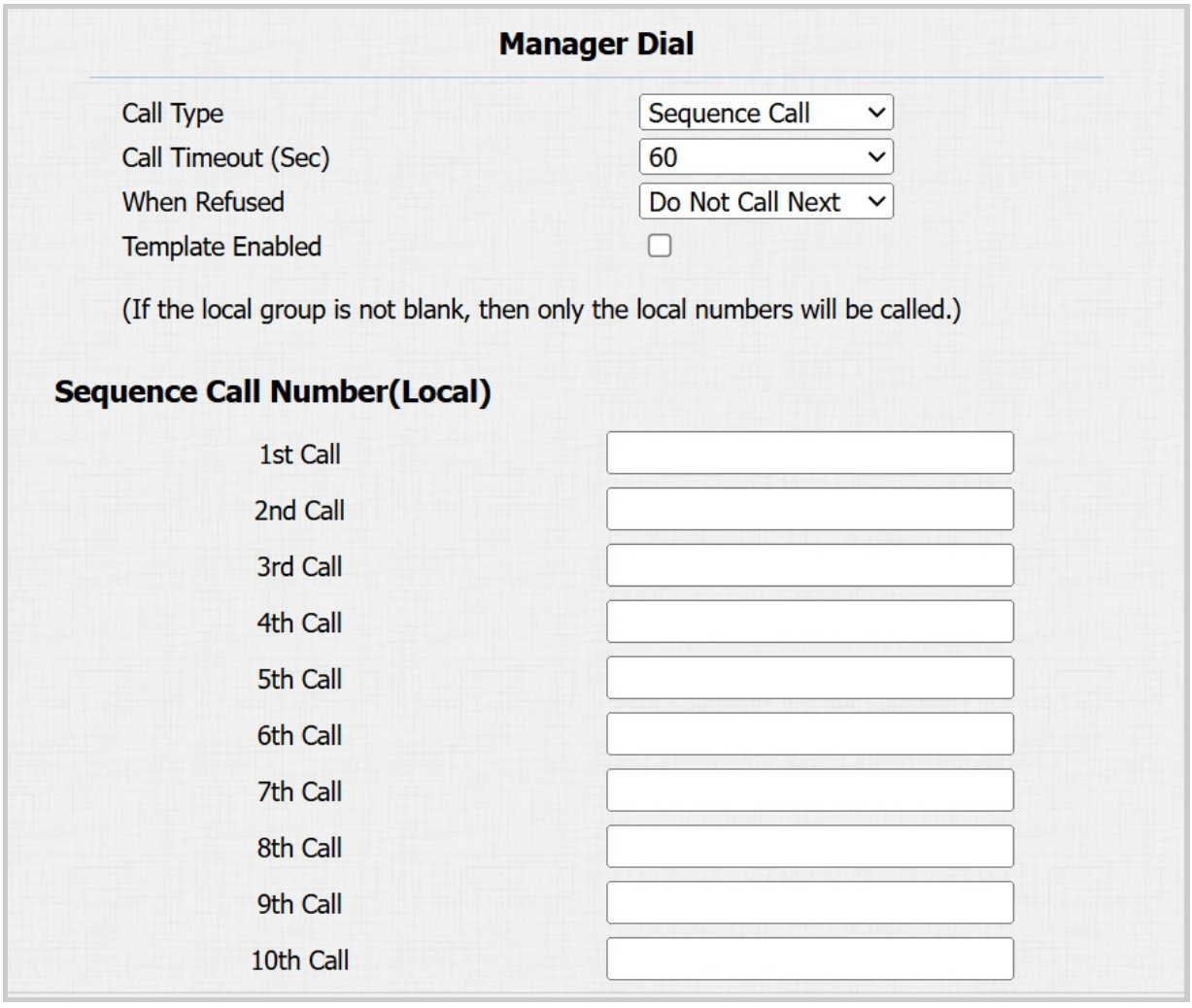


- **Call Type**: Group Call or Sequence Call.
- **When Refused**:
  - **Call Next**: The device will continue to call other numbers.
  - **Do Not Call Next:** The device will stop calling.
- **Template Enabled**: When the call schedule feature is enabled, group call is unavailable.
- **Group Call Number**: If you fill in the local group call number, the local group number will be called instead of the SmartPlus group call number.

Sequence Call

Sequence Call is a feature that allows you to dial a group of numbers in a predefined order until one of them answers. This feature is supported by Akuvox SmartPlus, which provides a set of sequence call numbers for the application. Please click here for the detailed configuration.

To configure the sequence call, navigate to the web **Intercom > Basic** interface.

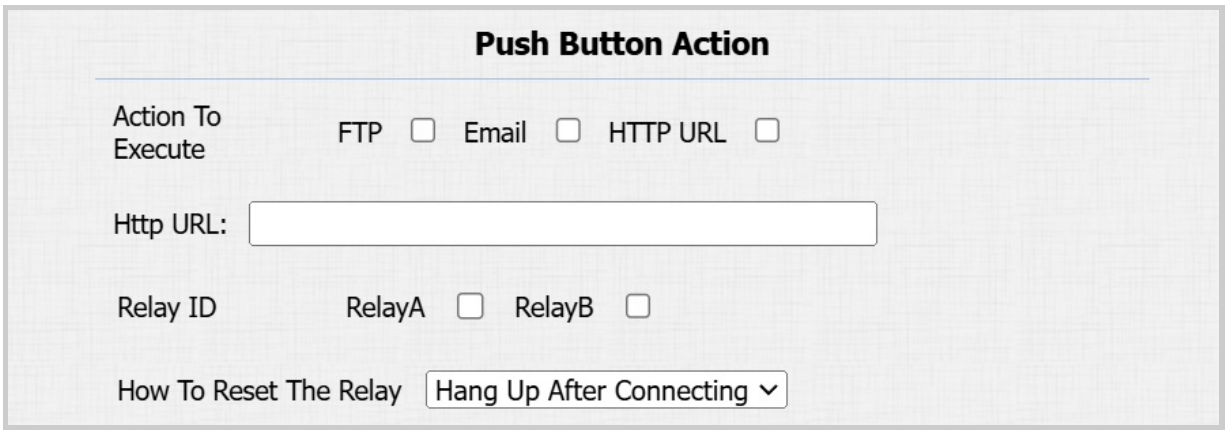


- **Call Type**: Group Call or Sequence Call.
- **Time Out(Sec)**: Set the call timeout before calling the next called party when the first called party does not receive the call within the timeout.
- **When Refused**:
  - **Do Not Call Next**: The device will stop calling.
  - **Call Next**: The device will continue to call other numbers.

- **Template Enabled**: When the call schedule feature is enabled, sequence call is unavailable.

Push Button Action

You can set actions triggered by pressing the push button on the **Intercom > Basic** interface.



- **Action to Execute**: Set the desired actions that occur when pressing the push button.
  - **FTP**: Send a message to the preconfigured FTP address.
  - **Email**: Send a message to the preconfigured Email address.
  - **HTTP URL**: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.
- **Relay ID**: Specify the relay to be unlocked.
- **How To Reset The Relay**: Specify when the relay is reset.
  - **Hang Up After Connecting**: The relay will be reset when the call is ended.
  - **Line Connected**: The relay will be reset when the call is picked up.

Push to Hang Up

Users can hang up the call on the door phone by pressing the push button. To enable the feature, navigate to **Intercom > Basic > Push To Hang Up** interface.

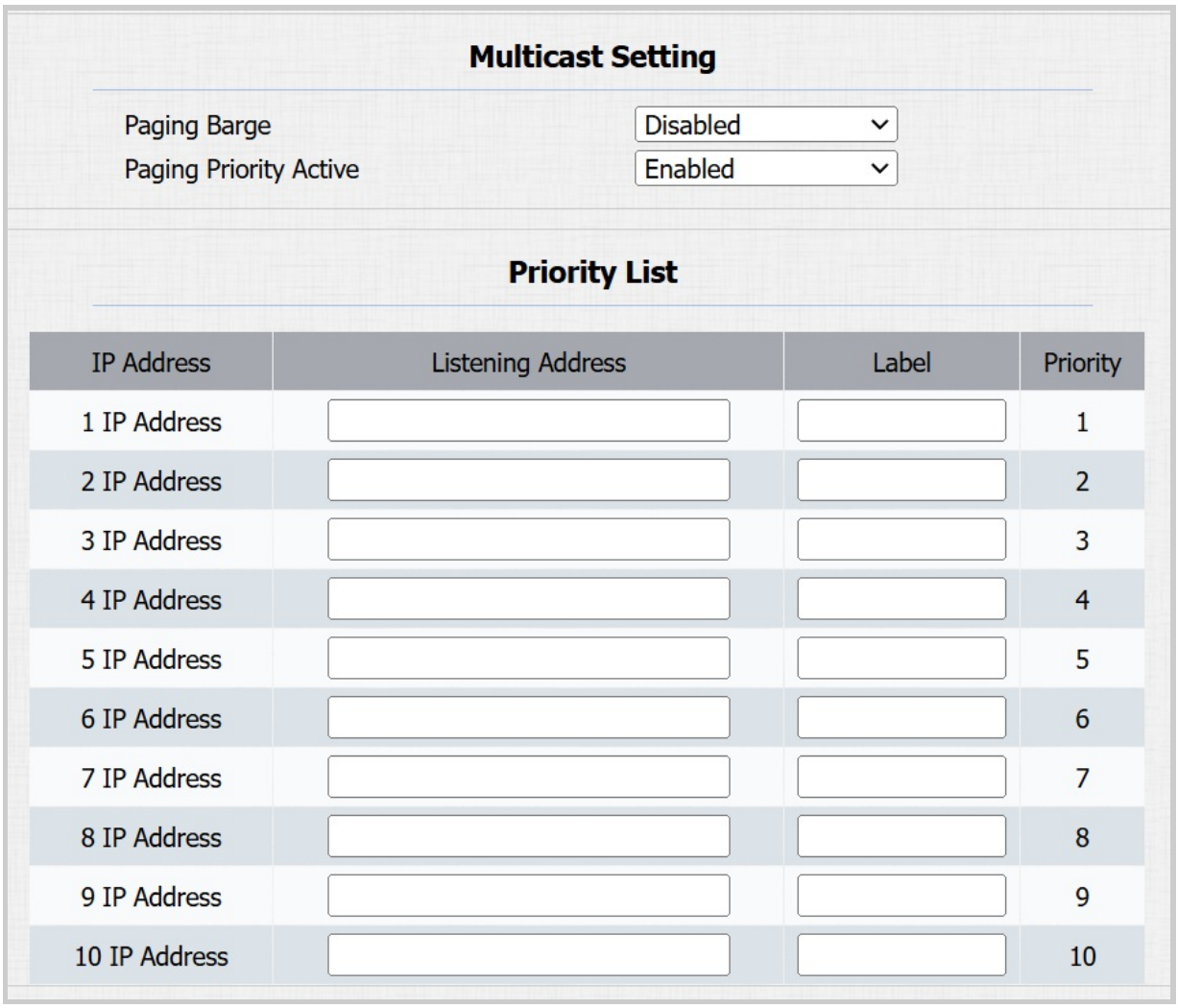


- **Hold Time**: Within the hold time, the call will not be hung up when users press the push button.

Multicast

Multicast is a one-to-many communication within a range. The door phone can act as a listener and receive audio from the broadcasting source.

To configure multicast, navigate to **Device > Multicast** interface.

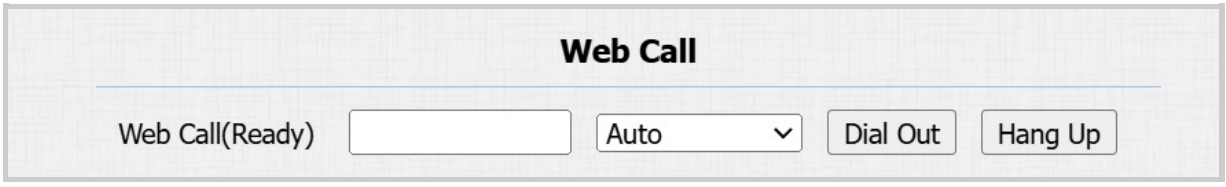


- **Paging Barge**: Multicast or how many multicast calls have higher priority than SIP call, if you disable Paging Priority, SIP call will have higher priority.
- **Paging Priority Active**: Multicast calls are called in order of priority or not.
- **Listening Address**: The multicast IP address to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

Web Call

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

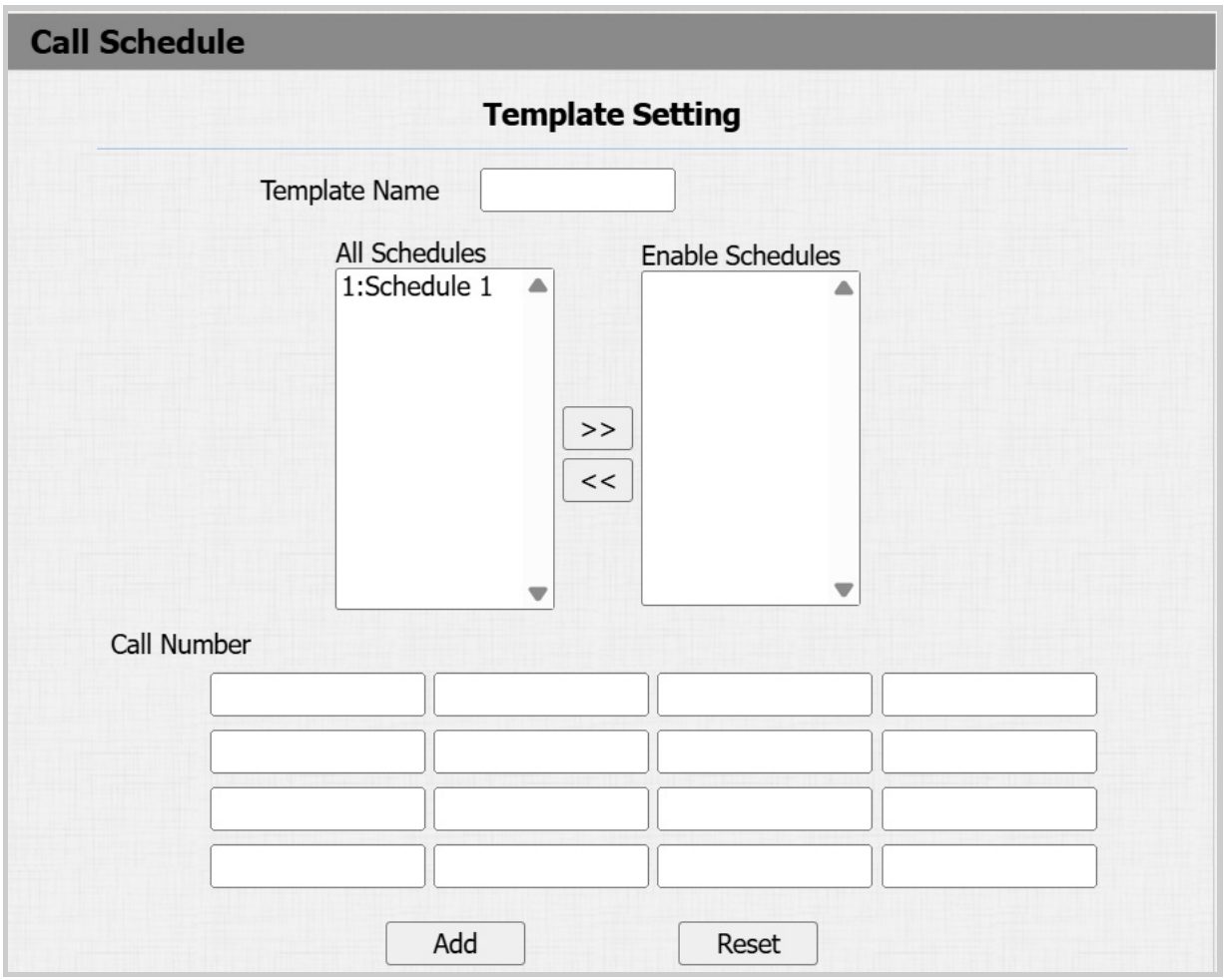
To set it up, go to the **Intercom > Basic > Web Call**. Select the registered SIP account, enter the IP/SIP number, and click Dial Out to make the call.



Call Schedule

This feature allows you to create templates that define call numbers and schedules, then assign them to specific input ports. By pressing external buttons at designated times, users can initiate calls to different numbers.

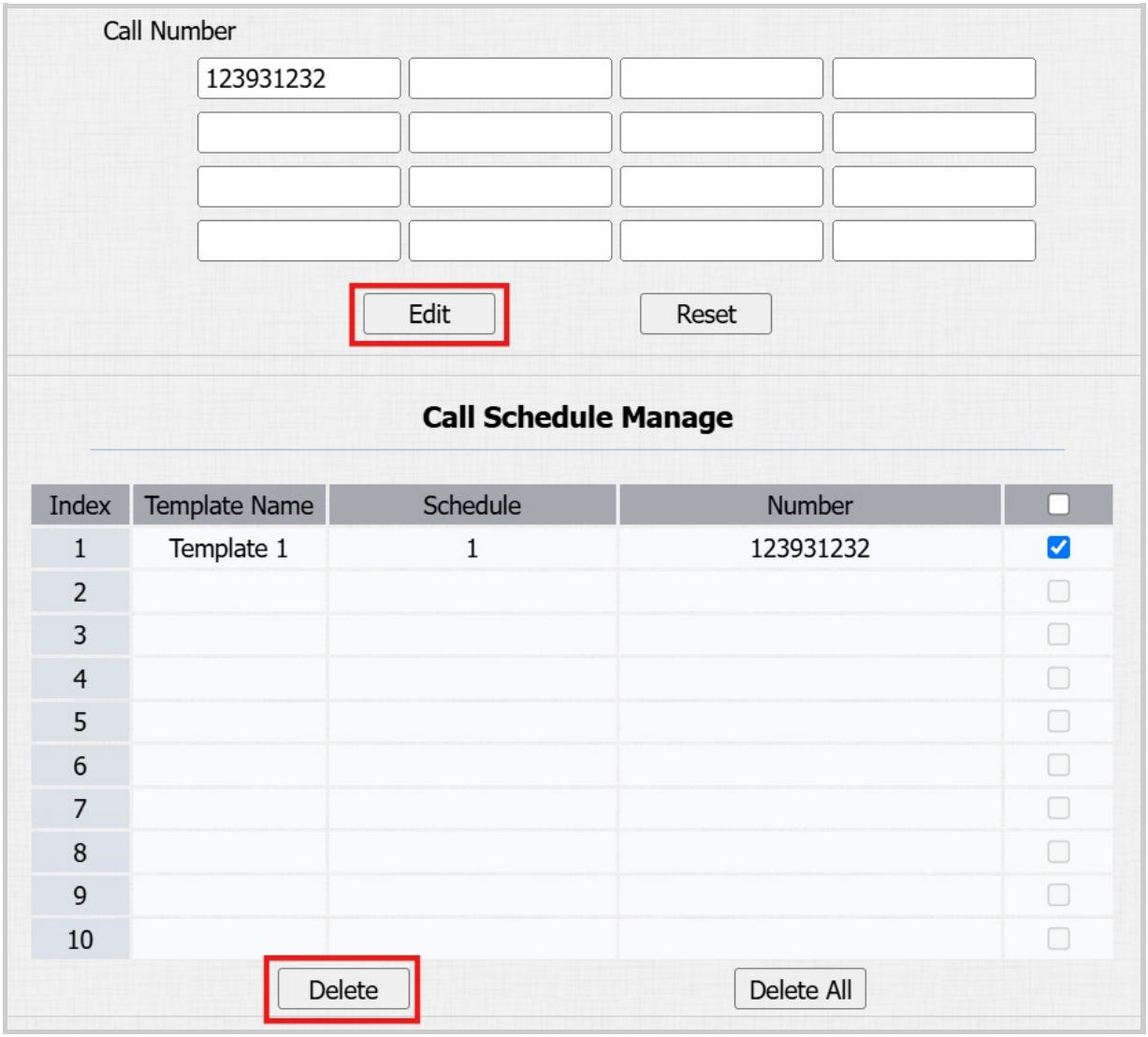
Set it up on the **Intercom > Call Schedule** interface.



- **Template Name**: Name the template. You can add up to 10 templates.

- **Call Number**: Enter the target called IP or SIP numbers. Each template can contain 16 numbers at a maximum.
- **Enabled Schedules**: Select the desired schedule on the left box and move it to the right. For instructions on creating schedules, please refer to Access Control Schedule Management chapter.
- **Reset**: Click to clear entered data.
- **Add**: Click to save the template.

After adding a template, you can check it for modification or deletion.



Note

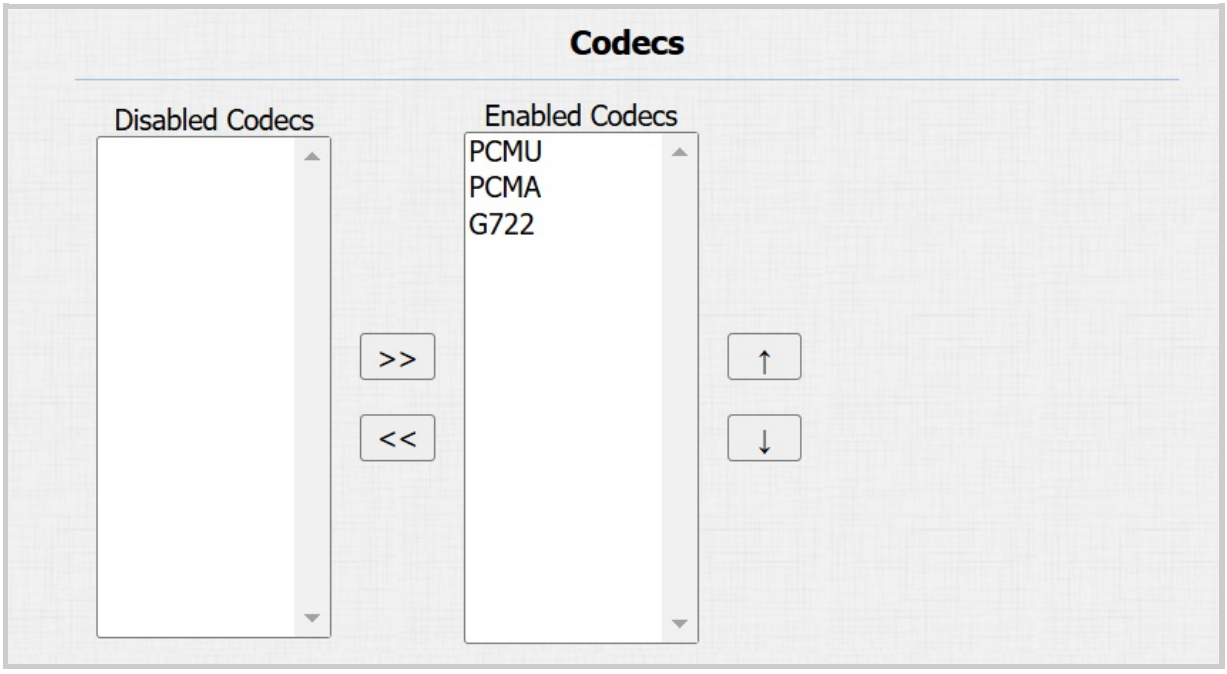
Click **here** to view instructions on assigning templates to inputs.

Audio & Video Codec Configuration

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 configure the audio codec, navigate to the web **Account > Advanced** interface.



Please refer to the bandwidth consumption and sample rate for the three codec types below:

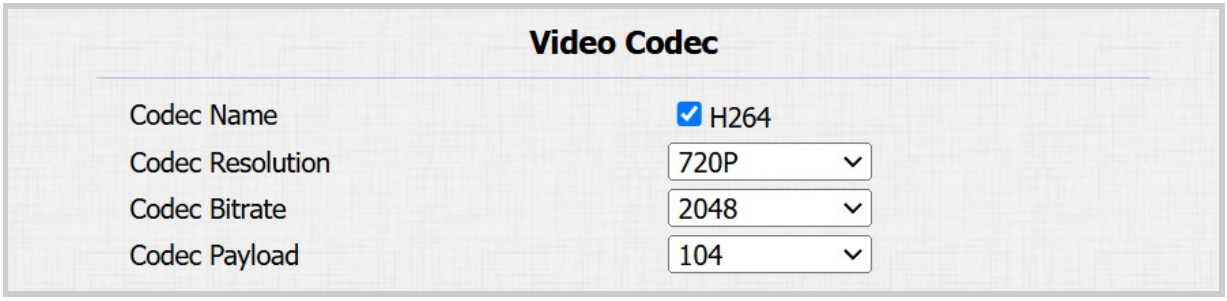
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec Configuration

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

> **Note**
>
> Since E21A does not have the camera, it does not support camera-related functions.

To configure the video codec, navigate to the web **Account > Advanced** interface.

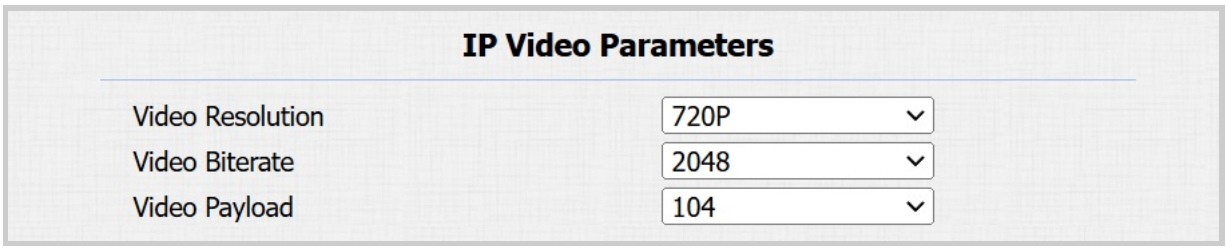


- **Codec Name**: Check to enable the H264 video codec format for the door phone video stream.
- **Codec Resolution**: Select the resolution from the provided options. The default code resolution is 720P.
- **CodecBitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The greater the bitrate, the more data transmitted every second and the clearer the video will be. The default code bitrate is 2048.
- **Codec Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Video Codec for IP Direct Calls

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

To set it up, navigate to the **Device > Call Feature > Direct IP** interface.



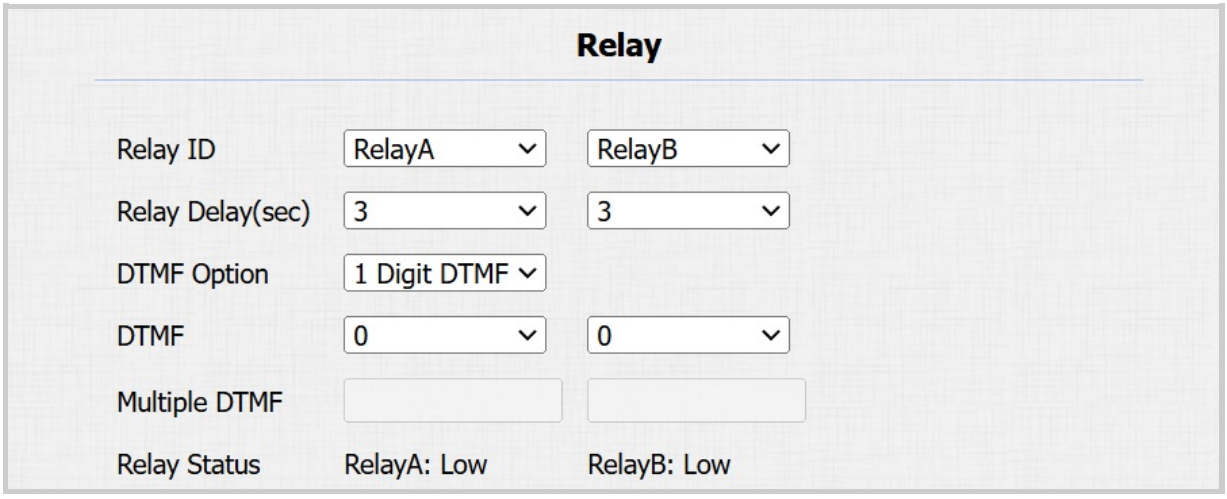
- **Video Resolution**: Select the resolution from the provided options. The default is 720P.
- **Video Bitrate**: The video stream bitrate ranges from 128 to 2048 kbps. The default bitrate is 2048.
- **Video Payload**: The payload ranges from 90 to 119 for configuring audio/video configuration files. The default is 104.

Relay Setting

Local Relay

A local relay is an external unit that is physically nearby and directly connected to the intercom device. It allows the intercom system to trigger actions, such as unlocking a door, based on user input or authorization.

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



- **Relay Delay(Sec)**: Set the delay time before the relay triggers. For example, if set to 5 seconds, the relay activates 5 seconds after pressing the Unlock button.
- **DTMF Option**: Set the digits of the DTMF code.
- **DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **Multiple DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.
- **Relay Status**: Indicate the states of the relay, which are normally opened and closed. By default, it shows low for normally closed(NC) and high for Normally Open(NO).

> **Note**
>
> External devices connected to the relay require separate power adapter.

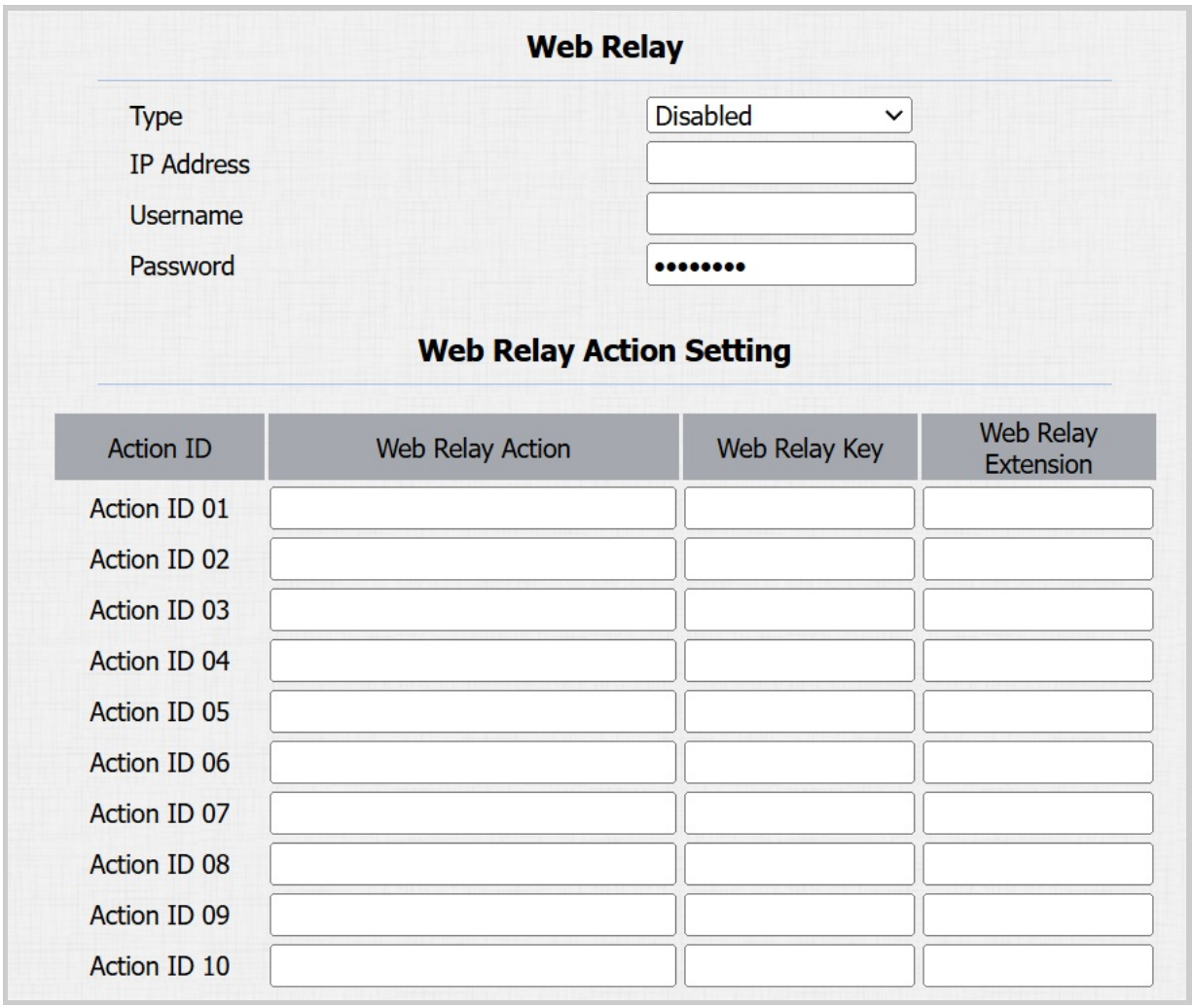
Web Relay

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.



Click here to view how to set up web relay.

To set it up, navigate to **Device > Web Relay** interface.



- **Type**: Determine the type of relay activated when employing door access methods for entry.
    - **Disabled**: Only activate the local relay.
    - **Web Relay**: Only activate the web relay.
    - **Both**: Activate both the local relay and web relay. Typically, the local relay is triggered first, followed by the web relay to execute their pre-configured actions.
- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **Username**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.

- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions, with up to 50 commands.

> **NOTE**
>
> If the URL includes full HTTP content (e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., state.xml?relayState=2), the relay uses the entered IP address.

- **Web Relay Key**: Determine the methods to activate the web relay based on whether the DTMF code is filled.

- Filling with the configured DTMF code restricts activation to card swiping and DTMF.

- Leaving it blank enables all door-opening methods.

- **Web Relay Extension**: Specify the intercom device and the methods it can use to activate the web relay during calls.

- When an intercom device’s IP/SIP is specified, only that device can trigger the web relay (except for via card swiping or DTMF) during calls.

- If left blank, all devices can trigger the relay during calls.

Access Control Schedule Management

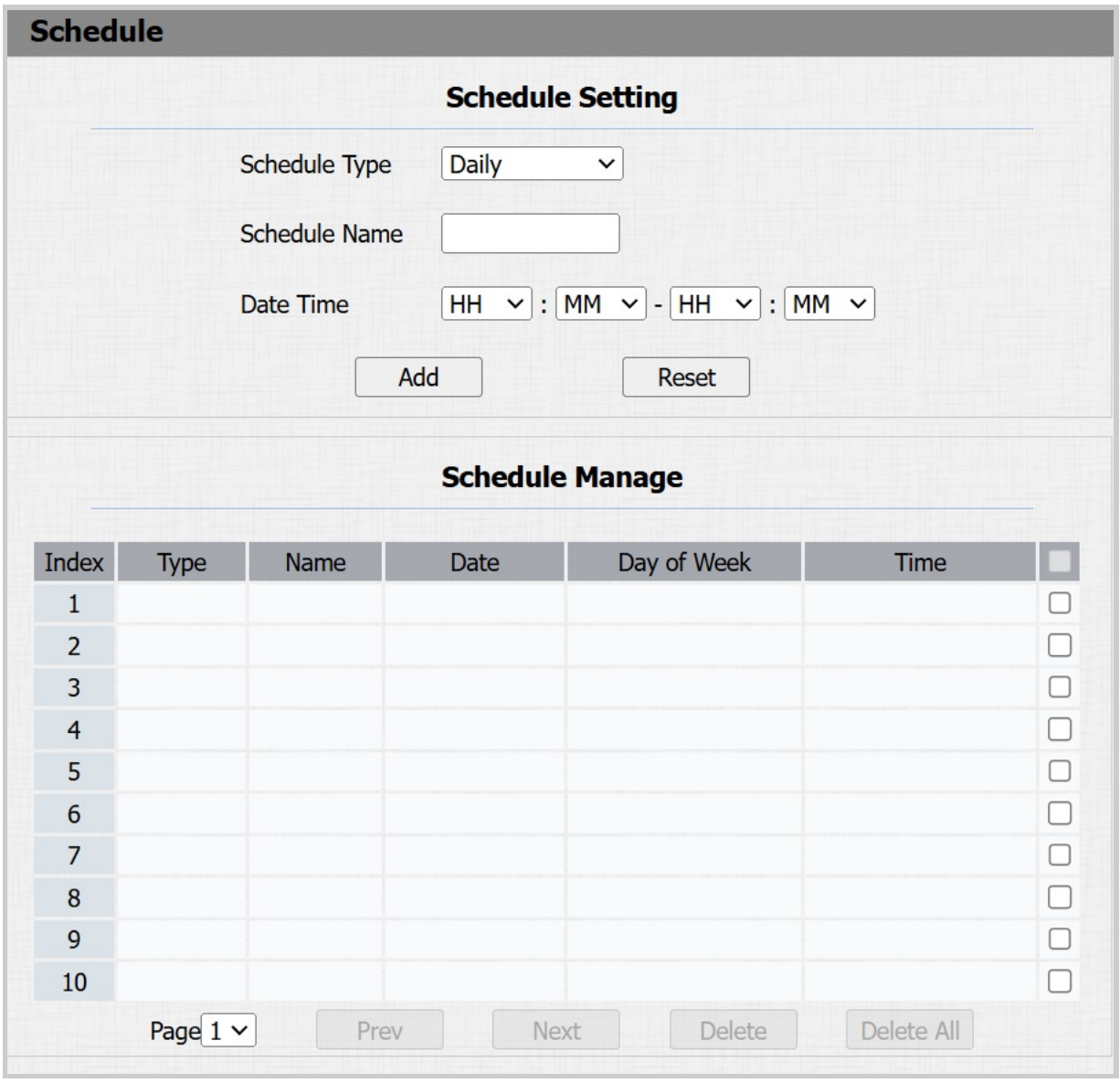
Configure Door Access Schedule

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 set it up, navigate to the web **Intercom > Schedule** interface.

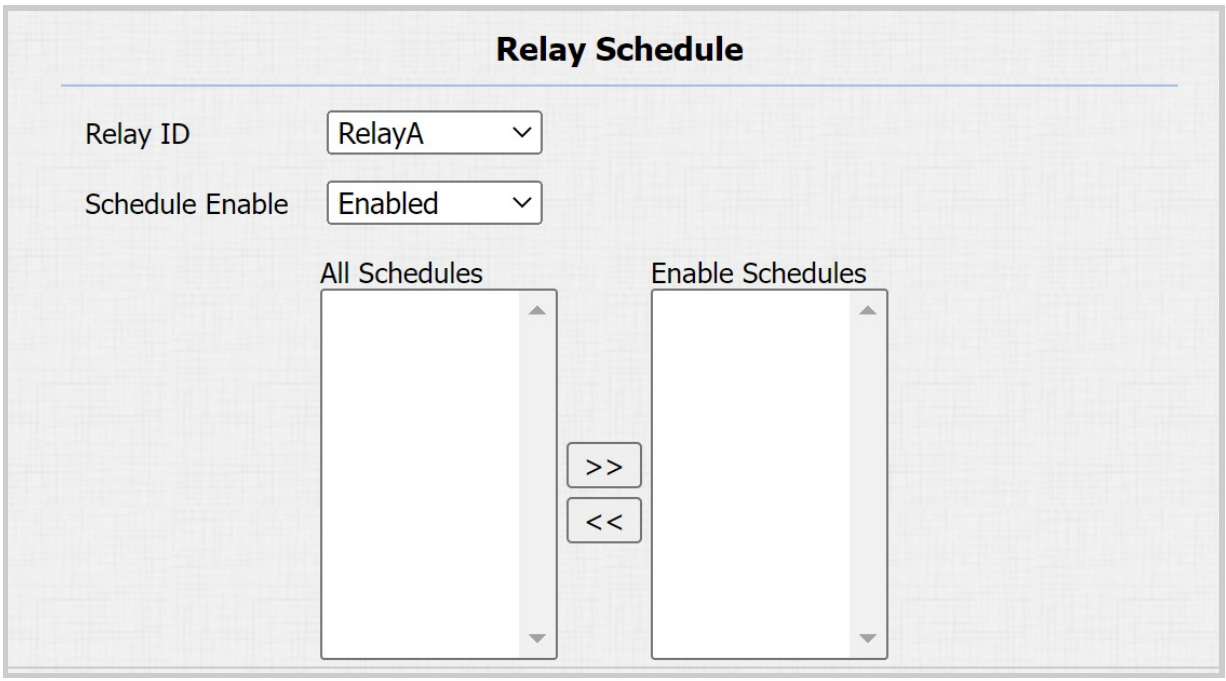


- **Schedule Type**:
  - **Normal**: Set the schedule based on the month, week, and day. It is used for a long period schedule.
  - **Weekly**: Set the schedule based on the week.
  - **Daily**: Set the schedule based on 24 hours a day.
- **Schedule Name**: Name the schedule.

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 set up a relay schedule, navigate to the **Intercom > Relay > Relay Schedule** interface.



- **Relay ID**: Specify the relay that adopts the schedule.
- **Schedule Enable**: Assign particular door access schedules to the chosen relay. Simply move them to the Selected Schedules box.

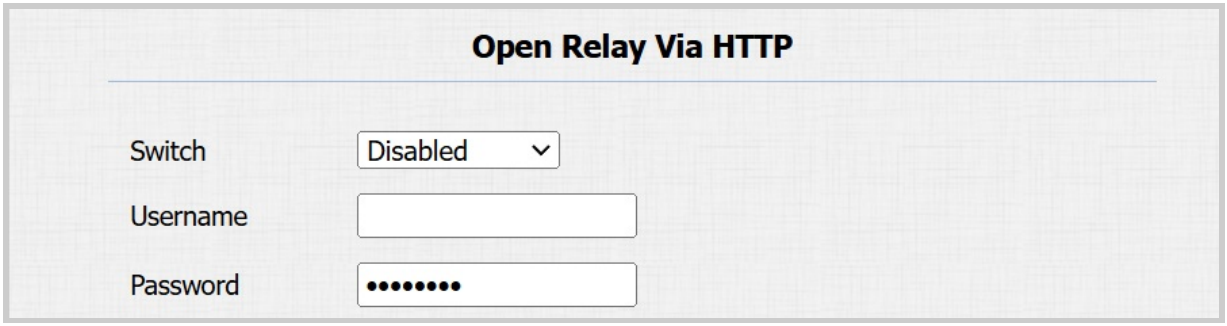
For instructions on creating schedules, kindly consult the Create Door Access Schedule section.

Door-opening Configuration

Unlock by HTTP Command

The device supports remote door unlocking via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the device. This will trigger the relay and open the door, even if the users are away from the device.

Set it up on the web **Device > Relay > Open Relay Via HTTP** interface.



- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a password for authentication in HTTP command URLs.

Tip

Here is an HTTP command URL example for relay triggering.



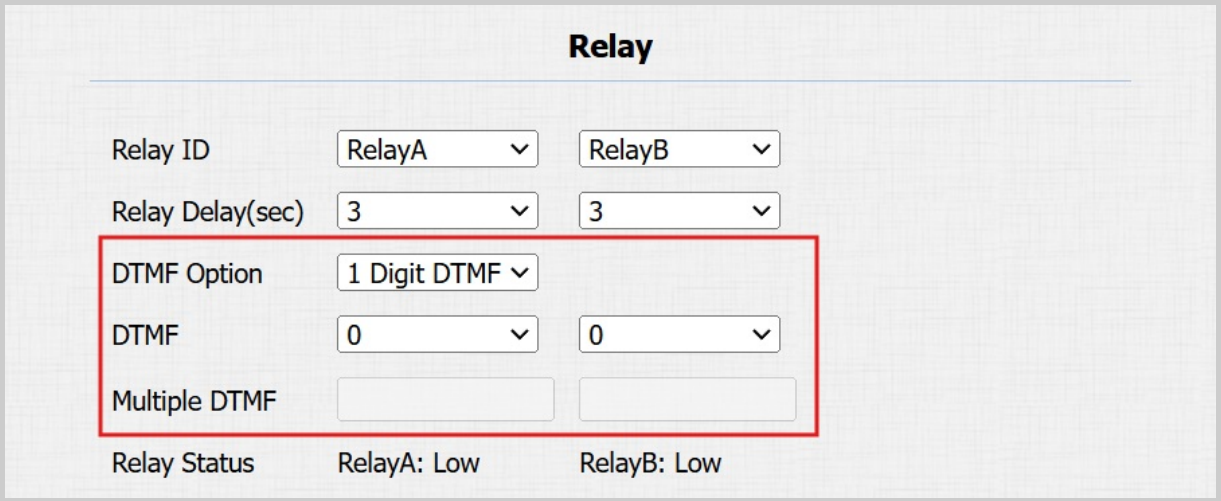
Note

The HTTP format for relay triggering varies depending on whether the door phone's high secure mode is enabled. Please refer to this how-to guide **Opening the Door via HTTP Command** for more information.

Unlock by DTMF Code

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.

To configure DTMF codes, go to **Intercom > Relay** interface.



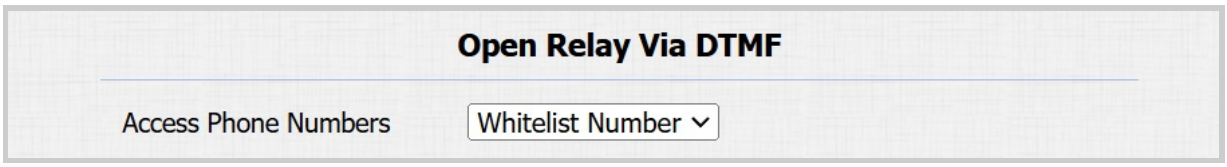
- **DTMF Option**: Set the number of digits for the DTMF code.
- **DTMF**: Define the 1-digit DTMF code within the range(0-9 and *,#) when the DTMF Mode is set to 1-digit.
- **Multiple DTMF**: Set the DTMF code based on the number of digits selected in the DTMF Mode.

Note

To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail. See **here** for the detailed DTMF configuration steps.

DTMF White List

To secure door access via DTMF codes, you can set up the DTMF whitelist on the device web **Intercom > Relay > Open Relay via DTMF** interface so that only the caller numbers you designated in the door phone can use the DTMF code to gain door access.



- **Access Phone Numbers**: Specify the contacts authorized to open doors via DTMF:
  - Disabled: No numbers can unlock doors using DTMF.
  - Whitelist Number: Doors can be opened by pressing the push button and SmartPlus Cloud numbers.
  - All Numbers: Any numbers can unlock using DTMF.

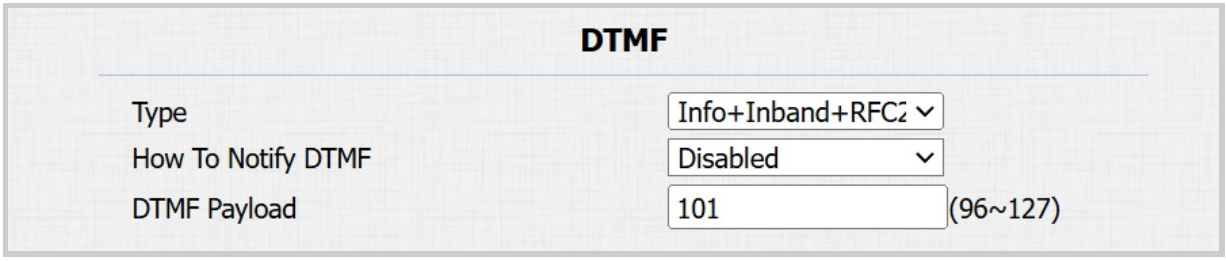
DTMF Data Transmission

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 device and other intercom devices.

DTMF Type Differences:

Inband	DTMF signals are transmitted within the same audio channel as voice data. Simple implementation but signal distortion may occur with highly compressed codecs (e.g., G.729).
RFC2833	Transmits DTMF as special event packets over RTP (Real-Time Transport Protocol), known as out-of-band transmission. Reliable and unaffected by codecs.
Info	Sends DTMF signals via SIP (Session Initiation Protocol) signaling channel. Separate from voice transmission, ensuring audio quality.
Info+Inband	Combines Info and Inband methods.
Info+RFC2833	Combines both Info and RFC2833 methods.
Info+Inband+RFC2833	All three methods are used simultaneously.

To set it up, navigate to the **Account > Advanced > DTMF** interface.



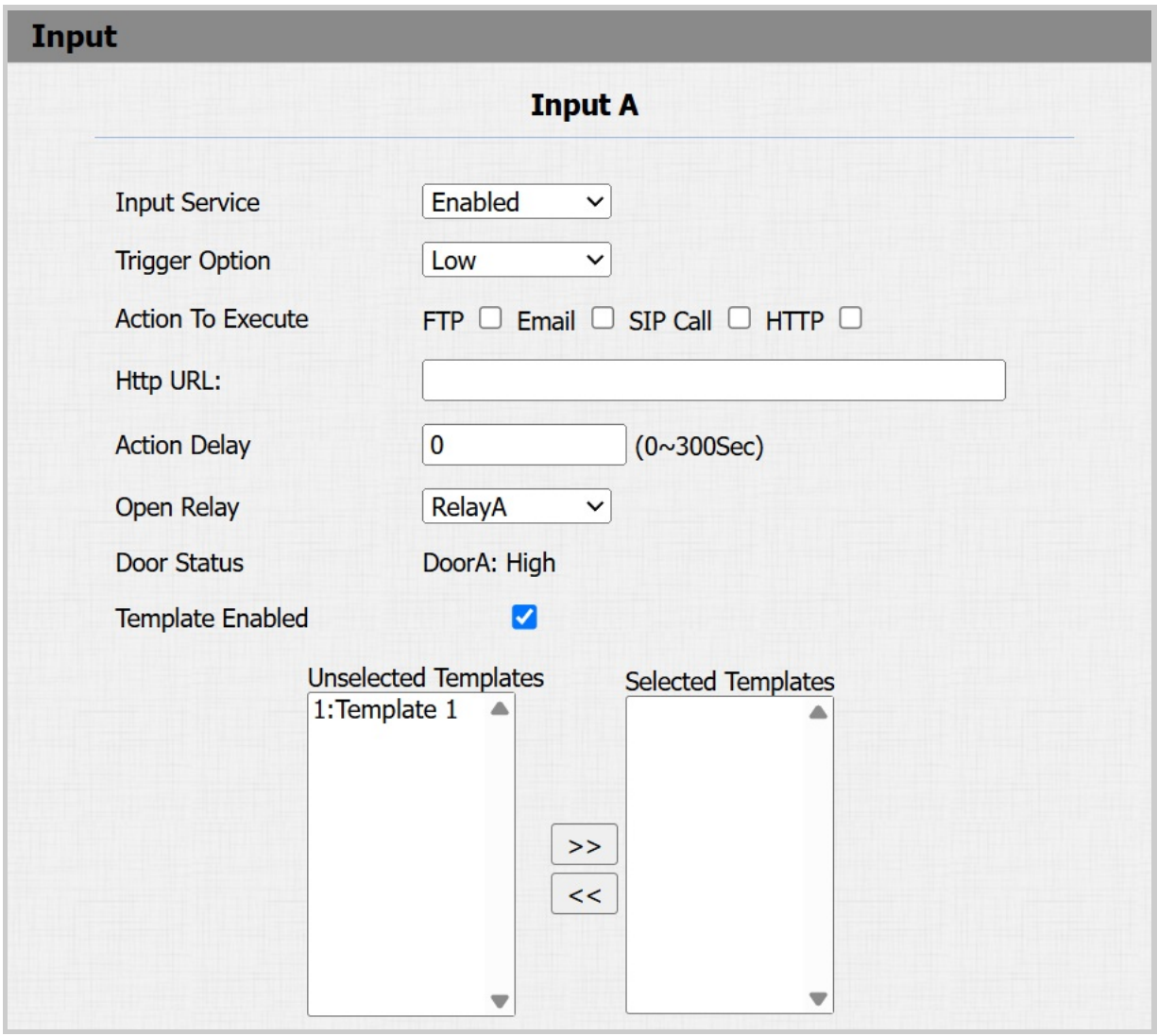
- **Type:** Select from the available options based on the specific DTMF transmission type of the third-party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF**: Select **Disabled, DTMF, DTMF-Relay**, or **Telephone-Event** according to the specific type adopted 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.

Unlock by Exit Button

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.

Click here to watch the instruction video.

To set it up, go to the **Intercom > Input** interface.



- **Enabled**: To use a specific input interface.
- **Trigger Electrical Level**: Set the input interface to trigger at a low or high electrical level.
- **Action To Execute**: Set the desired actions that occur when the specific Input interface is triggered.
    - FTP: Send a screenshot to the preconfigured FTP server.
    - Email: Send a screenshot to the preconfigured Email address.
    - SIP Call: Call the preset number upon the trigger.
    - HTTP: When triggered, the HTTP message can be captured and displayed in the corresponding packets. To utilize this feature, enable the HTTP server and enter the message content in the designated box below.
- **HTTP URL**: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

- **Action Delay**: Specify how many seconds to delay executing the preconfigured actions, or to delay making calls by pressing the external button.
- **Open Relay**: Specify the relay to be triggered along with the input triggering.
- **Door Status**: Display the status of the input signal.
- **Template Enabled**: This option is used to make calls to target numbers set in the template. Make a template effective by moving it from the left to the right box.
    - This function is incompatible with the SIP Call action when the input is triggered.
    - This function is incompatible with group call and sequence call.
    - You cannot choose templates that have overlapping times.

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.

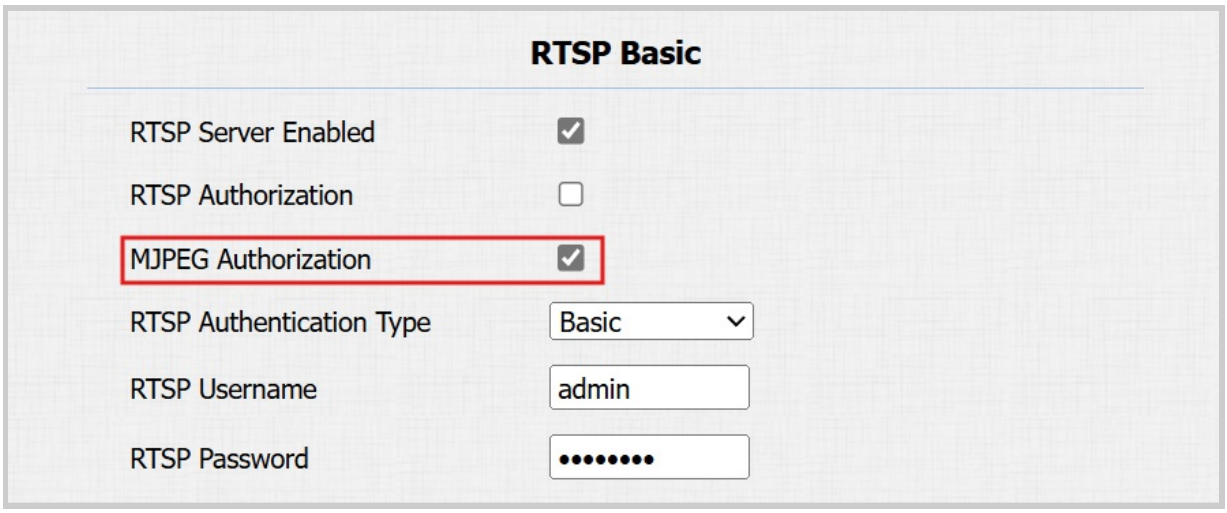
RTSP stands for Real Time Streaming Protocol. It can be used to stream video and audio from the third-party cameras to the device. You can add a camera's stream by adding its URL. The URL format of Akuvox devices is rtsp://Device's IP/live/ch00_0

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.

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.

To set it up, navigate to **Intercom > RTSP** interface.



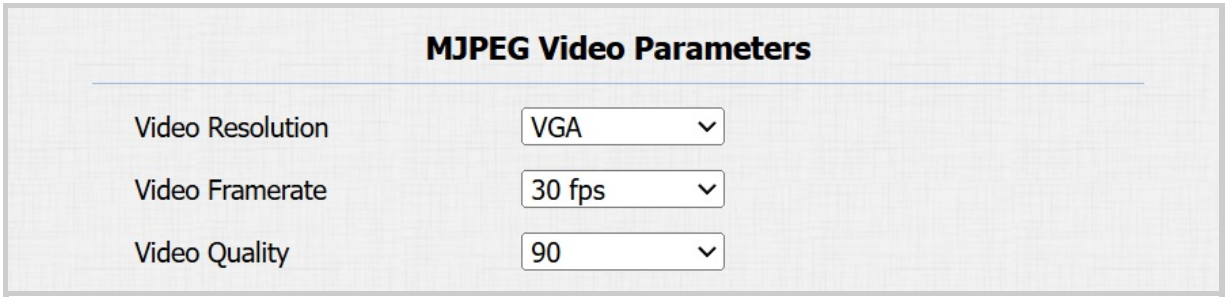
- **MJPEG Authorization**: Once enabled, accessing the door phone's real-time image or video by entering the URL into the browser requires verification of the Authentication Mode, RTSP Username, and RTSP Password.

Tip

- To view a dynamic stream, use the URL http://device_IP:8080/video.cgi.
- For capturing a screenshot, use the following URLs, with the image formats varying accordingly:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi

For example, if you want to capture the jpg format image of the door phone with the IP address 192.168.1.104, you can enter http://192.168.1.104:8080/picture.jpg on the web browser.

You can set up the MJPEG video parameters in the **MJPEG Video Parameters** section.



- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Frame rate(fps)**: Frames per second, refers to how many frames are displayed in one second of video. The default frame rate is 30fps.
- **Video Quality**: The video bitrate ranges from 50 to 90.

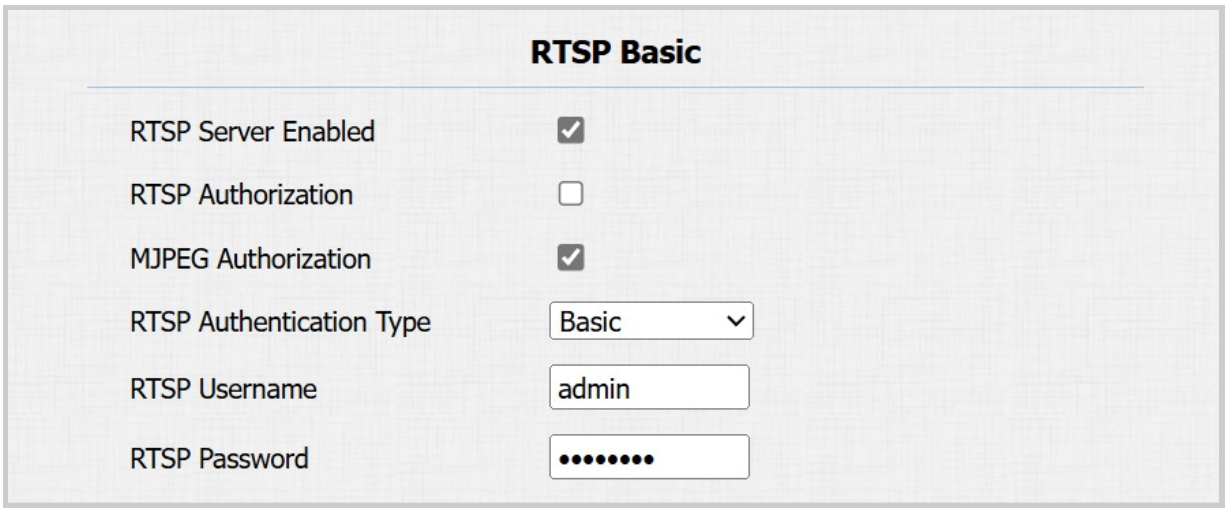
RTSP Stream Monitoring

The RTSP feature allows Akuvox indoor monitors, or third-party devices, to obtain the live stream from the door phone.

You can set up the RTSP authentication credentials and video parameters.

RTSP Basic Setting

Before you can use the RTSP function, you are required to set up the RTSP function on the device web **Intercom > RTSP > RTSP Basic** interface in terms of RTSP authorization, authentication, password, etc.



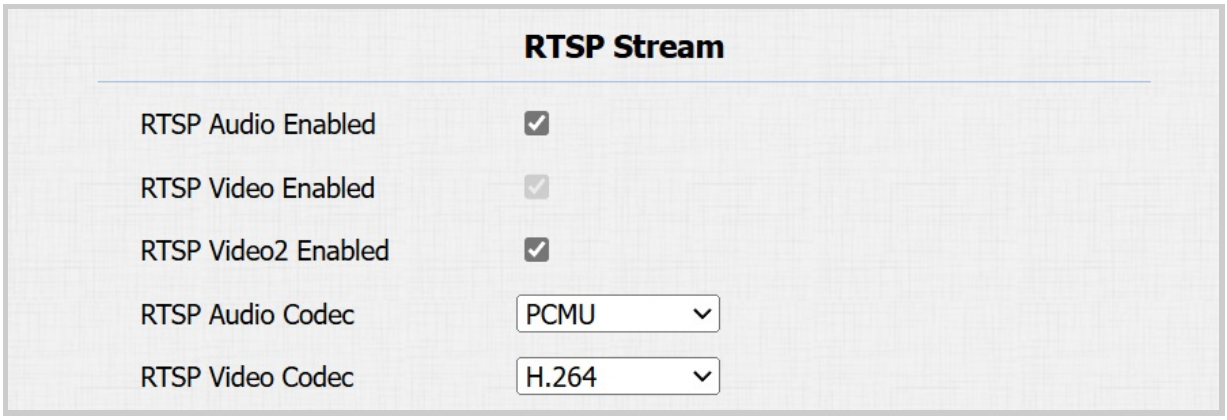
- **RTSP Authorization:** Once enabled, configure RTSP Authentication Mode, RTSP Username, and RTSP Password. These credentials are required for accessing the door phone's RTSP stream from other intercom devices like indoor monitors.
- **RTSP Authentication Type**: Select between Basic and Digest. It is Digest by default that uses hashing instead of the easily reversible Base64 encoding. A token is used for verification.

- **RTSP Username**: Set the username for authorization.
- **RTSP Password**: Set the password for authorization.

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.

To set it up, go to **Intercom > RTSP > RTSP Stream** interface.



- **RTSP Audio Enabled**: Allow the door phone to send audio information to the monitor by RTSP.
- **RTSP Video Enabled**: The door phone can send the video information to the monitor. After enabling the RTSP feature, the video RTSP is enabled by default and cannot be modified.
- **RTSP Video 2 Enabled**: Akuvox door phones support 2 RTSP streams, you can enable the second one.
- **RTSP Audio Codec**: Choose a suitable audio codec for RTSP audio.
- **RTSP Video Codec**: Choose a suitable video codec for RTSP video.

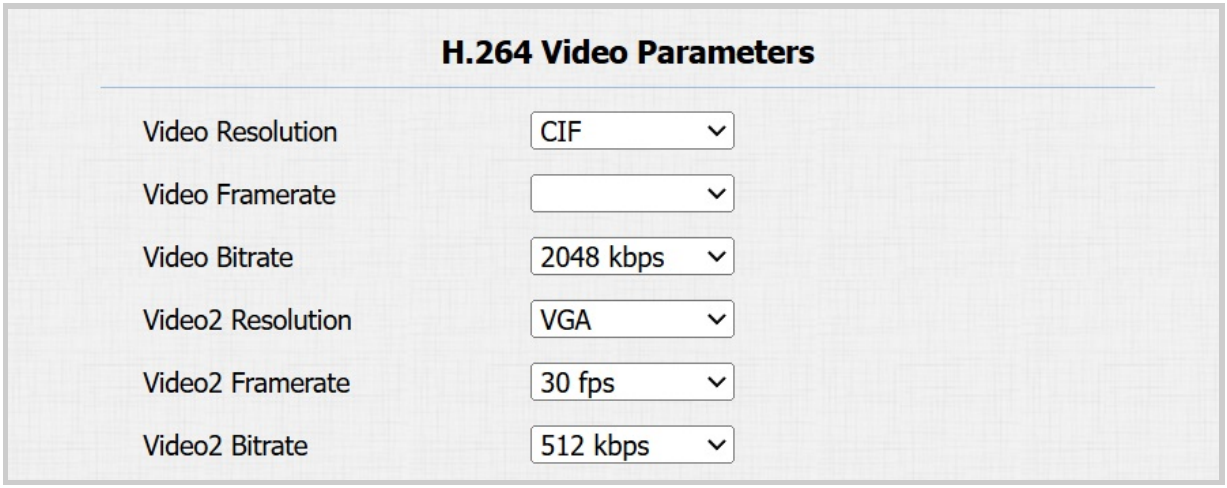
Tip

To view the audio and video stream using RTSP:

- First channel: rtsp://Device's IP/live/ch00_0
- Second channel: rtsp://Device's IP/live/ch00_1

H.264 Video Parameters Setup

Set up the H.264 video parameters for the RTSP video stream on the **Intercom > RTSP > H.264 Video Parameters** interface.



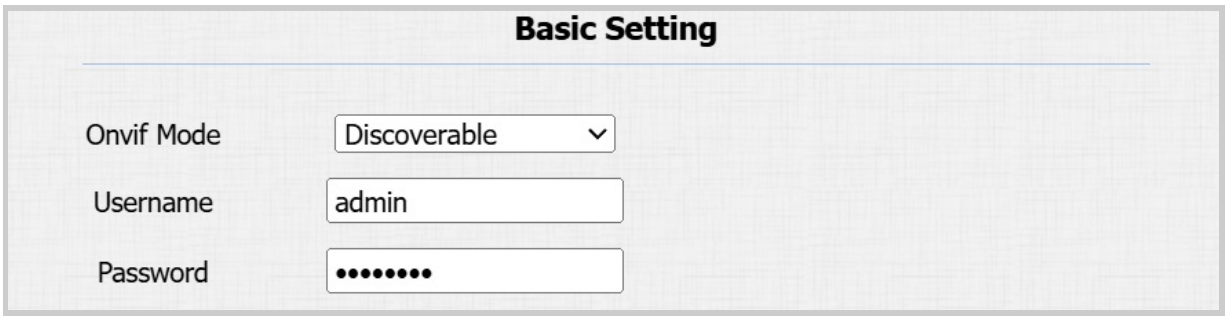
- **Video Resolution**: Specify the image resolution, varying from the lowest CIF(352×288 pixels) to the highest 1080P(1920x1080 pixels).
- **Video Framerate**: Frames per second, refers to how many frames are displayed in one second of video.
- **Video Bitrate**: The amount of video data transferred in a specific duration of time. A higher video bitrate means a higher possible quality, but also higher file sizes and more bandwidth.
- **Video2 Resolution**: Specify the image resolution for the second video stream channel.
- **Video2 Framerate**: Set the frame rate for the second video stream channel.
- **Video2 Bitrate**: Set the bit rate for the second video stream channel. The default is 512 kbps.

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.

Click here to view an example of using the ONVIF feature: the integration with Uniview NVR System.

To set it up, go to the **Intercom > ONVIF** interface.



- **Onvif Mode**: Select Discoverable to enable this feature. The video from the door phone camera will be searched by other devices.
- **Username**: Set the username required for accessing the door phone's video stream on other devices. It is admin by default.
- **Password**: Set the password required for accessing the door phone's video stream on other devices. It is admin by default.

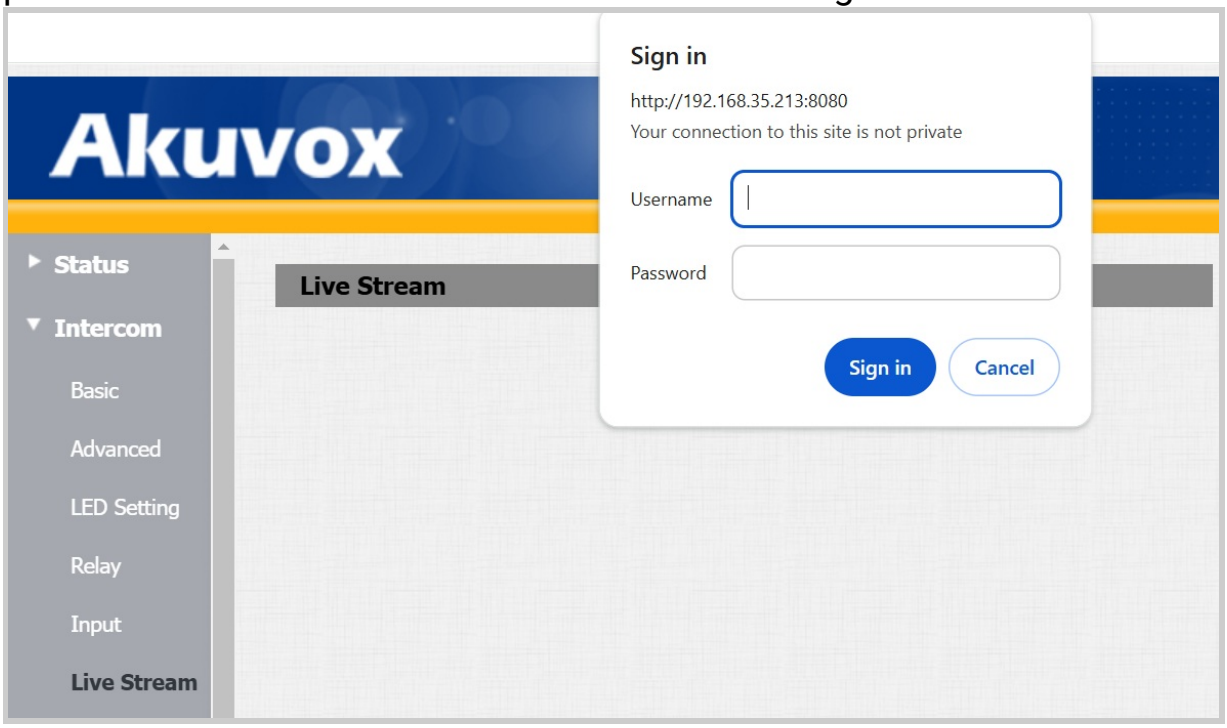
Tip

Once the settings are configured, to access the video stream on the third-party device, simply enter the ONVIF URL: http://Device's IP:80/onvif/device_service.

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.

View the video stream on the **Intercom > Live Stream** interface. If you have enabled RTSP authorization, you need to enter the user name and password set in the RTSP Basic section for viewing the stream.



Security

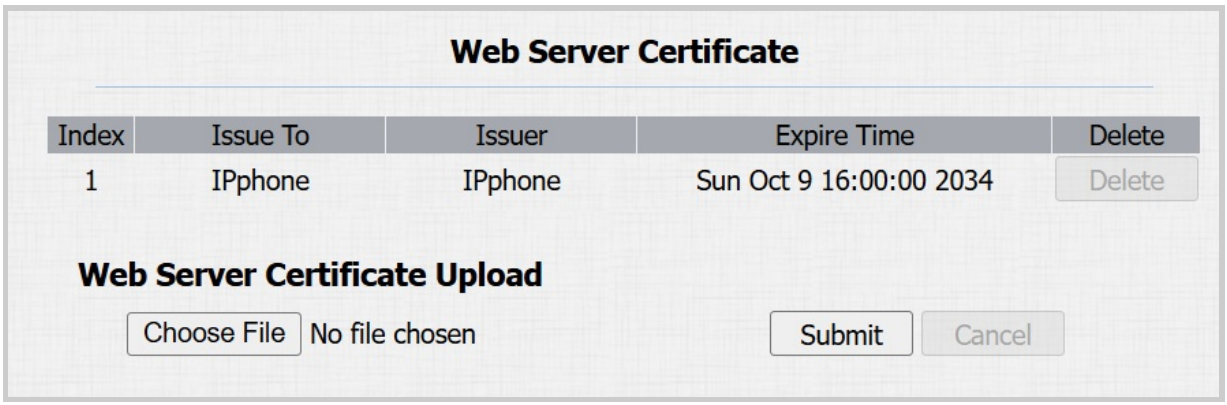
Client Certificate Setting

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.

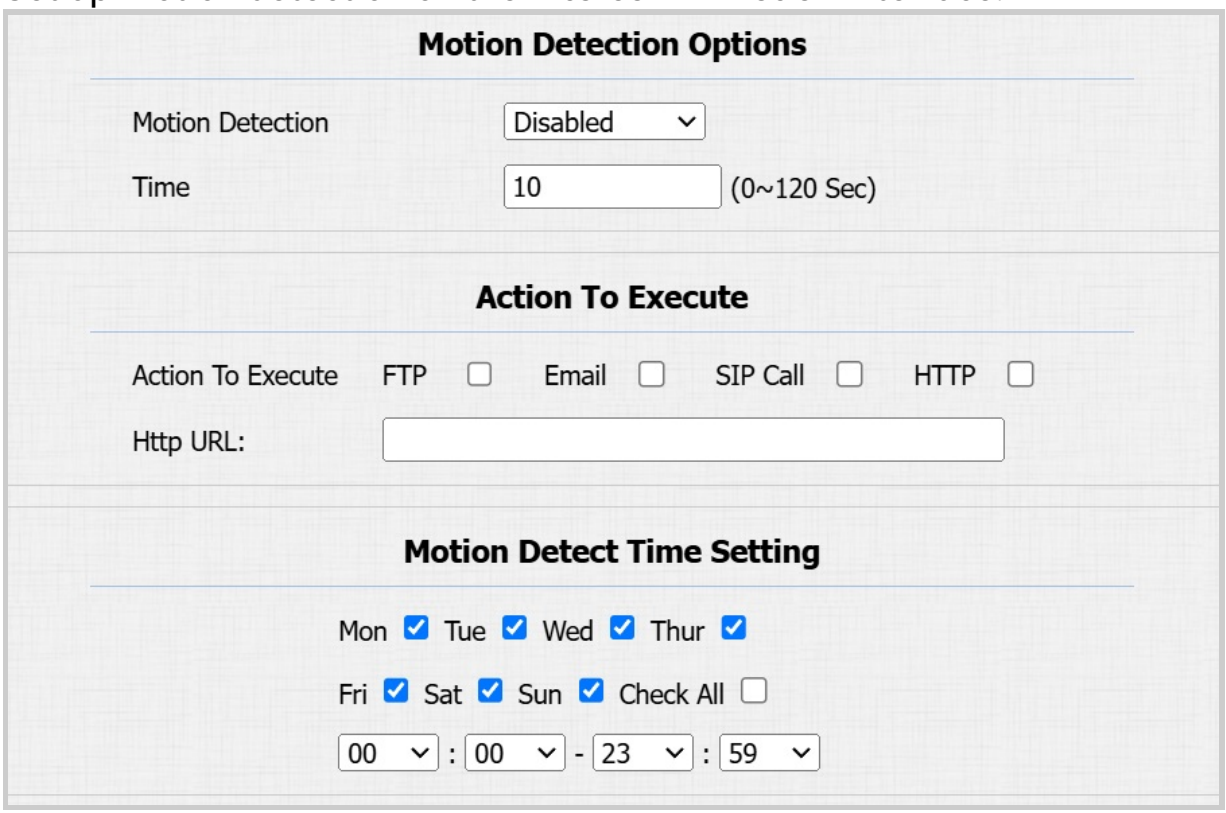
Upload the web server certificate on the **Security > Advanced > Web Server Certificate** interface.



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.

Set up motion detection on the **Intercom > Motion** interface.



- **Motion Detection**: Enable or disable the IR sensor-based motion detection for suspicious moving objects.
- **Time**: The absolute triggering interval is 3 seconds. If you select a number greater than 3 seconds, then it requires a second triggering interval to trigger the alarm. For example, if you select 3 seconds, then the alarm will be triggered when a moving object is detected one time from 0 to 3 seconds (triggered any time from 0 to 3 seconds). However, for example, if you select 5 seconds (greater than 3), then the alarm will not be triggered until a moving object is detected for the second time from 3 to 5 seconds (triggered any time from 3 to 5 seconds). The default interval is 10 seconds.
- **Action to Execute**: The notification type includes FTP, Email, SIP Call, and HTTP.
    - FTP: The notification will be sent to the designated FTP server.
    - Email: The email will be sent to the pre-configured email address.
    - SIP Call: A call will be made to the pre-configured number.
    - HTTP: The notification will be sent to the designated server.

- HTTP URL: Enter the HTTP message if selecting HTTP as the action to execute. The format is http://HTTP server's IP/Message content.

- **Motion Detect Time Setting**: When motion detection is enabled, you can set a specific time for the feature to be effective.

Security Notification

A security notification informs users or security personnel of any breach or threat that the device detects. For example, if the device detects something unusual, the system sends a notification to users or security through email, phone calls, or other methods.

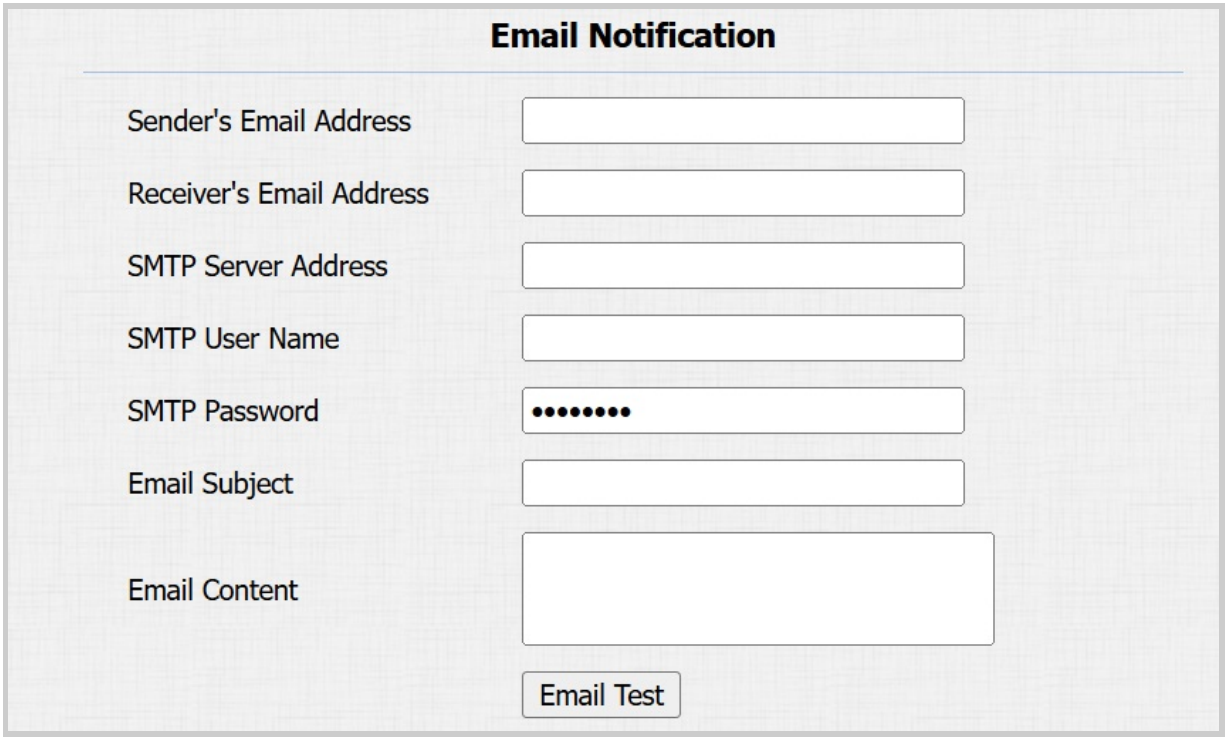
To set up security notifications, go to the **Intercom > Action** interface.

Email Notification

Set up email notifications to receive screenshots of unusual motion from the device.

Click here to view how to set this feature up.

Set it up in the **Email Notification** section.



- **SMTP Server Address**: The SMTP server address of the sender.

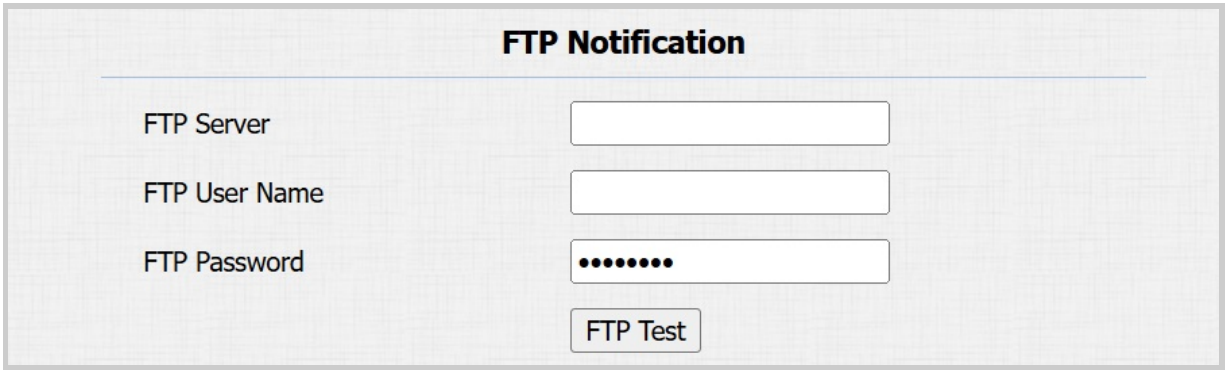
- **SMTP User Name**: The SMTP username is usually the same as the sender's email address.
- **SMTP Password**: The password of the SMTP service is the same as the sender's email address.

FTP Notification

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.

Click here to view the configuration steps.

Set it up in the **FTP Notification** section.

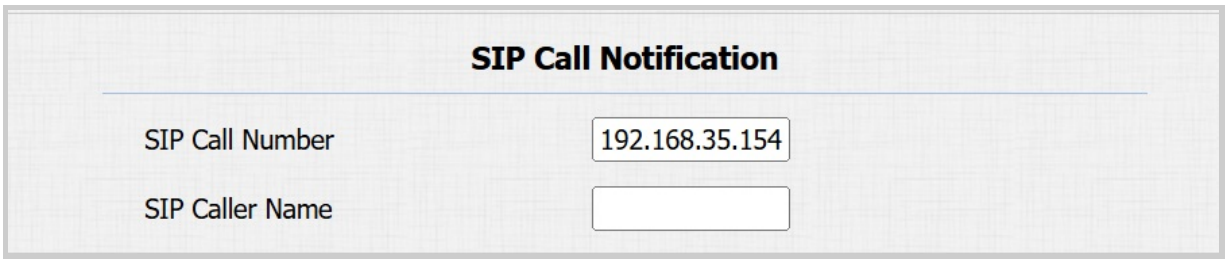


- **FTP Server:** Set the address (URL) of the FTP server.
- **FTP User Name**: Enter the user name to access the FTP server.
- **FTP Password**: Enter the password to access the FTP server.

SIP Call Notification

In addition to FTP and Email notification, the door phone can also make a SIP call when some feature action is triggered.

Set it up in the **SIP Call Notification** section.



Action URL

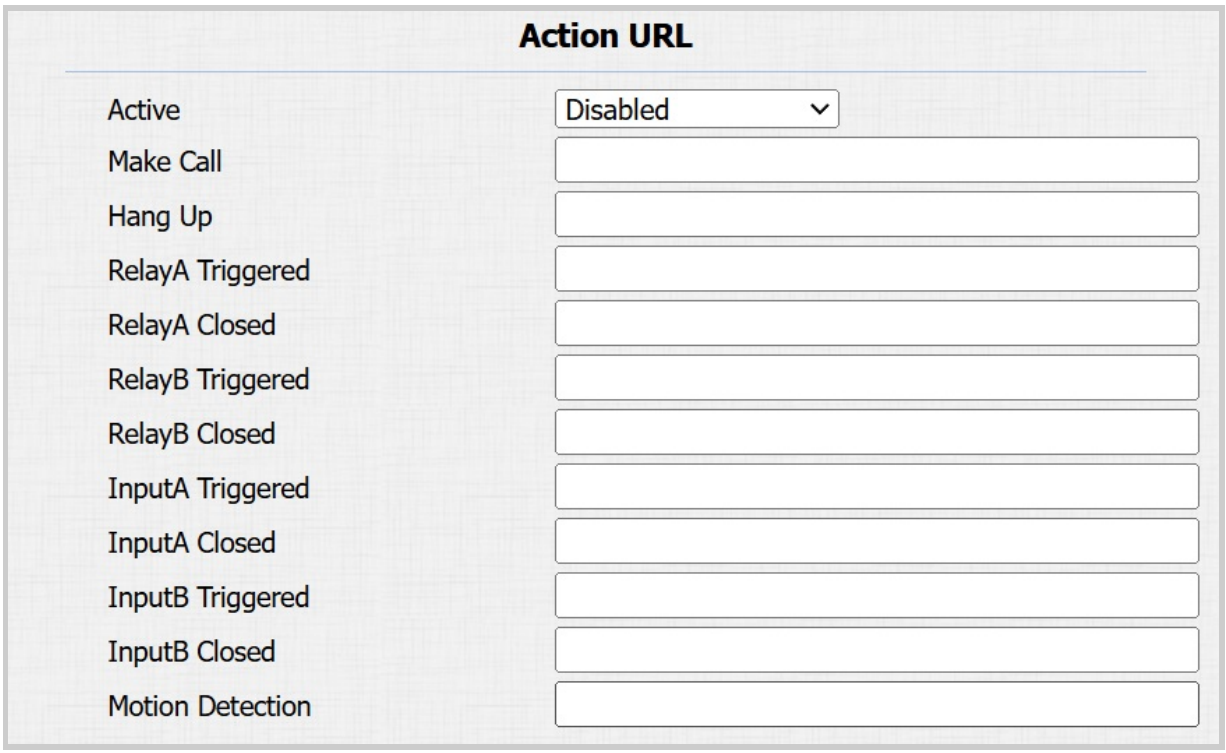
You can use the device to send specific HTTP URL commands to the HTTP server for certain actions. These actions will be triggered when the relay status and input status change.

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	Motion Detection	$active_user	Http://server ip/active_user=$active_user

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

To set it up, go to the **Device > Action URL** interface.



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.

Set it up on the web **Account > Advanced > Encryption** interface.

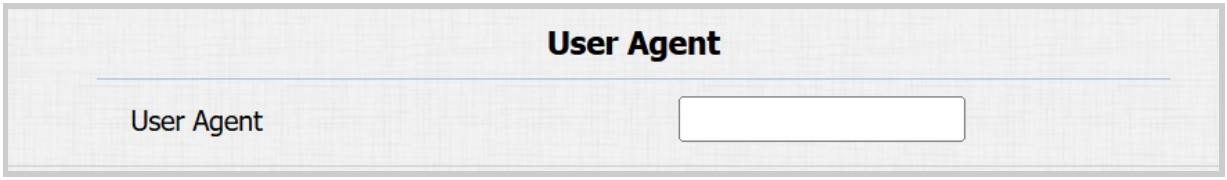


- **Voice Encryption(SRTP):** Choose Disabled, Optional, or Compulsory for SRTP. If **Optional** or **Compulsory** is selected, the voice during the call is encrypted, and you can grab the RTP packet to view it.

User Agent

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

To set it up, navigate to the **Account > Advanced > User Agent** interface.



- **User Agent:** Akuvox is by default.

High Security Mode

High security mode is designed to enhance the security. It employs encryption across various facets, including the communication process, door opening commands, password storage methods, and more.

Enable it on the **Security > Basic > High Security Mode** interface.



Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.

2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

- PC Manager: 1.2.0.0
- IP Scanner: 2.2.0.0
- Upgrade Tool: 4.1.0.0
- SDMC: 6.0.0.34

3. The supported HTTP format for relay triggering varies depending on whether high secure mode is enabled or disabled.

If the mode is on, the device only accepts the new HTTP formats below for door opening.

- http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

If the mode is off, the device can use both the new formats above and the old format below:

- http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

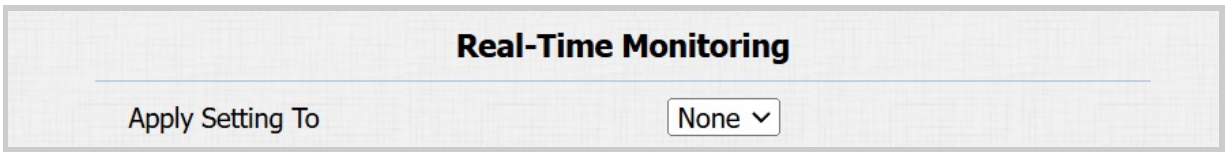
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Real-time Monitoring

This feature displays the door status when the device is connected to the SmartPlus Cloud. Property managers and end users can check the door status, respectively, on the SmartPlus Property Manager platform and SmartPlus App. You need to specify the relay(s) or input(s) that apply this feature.

Click here to see the detailed configuration.

To set it up, go to the **Security > Basic > Real-time Monitoring** interface.



- **Apply Setting To**:
  - **None**: Not display door status.
  - **Input**: The door is opened by triggering the input.
  - **Relay**: The door is opened by triggering the relay.

Emergency Audio-Visual Alert Setup

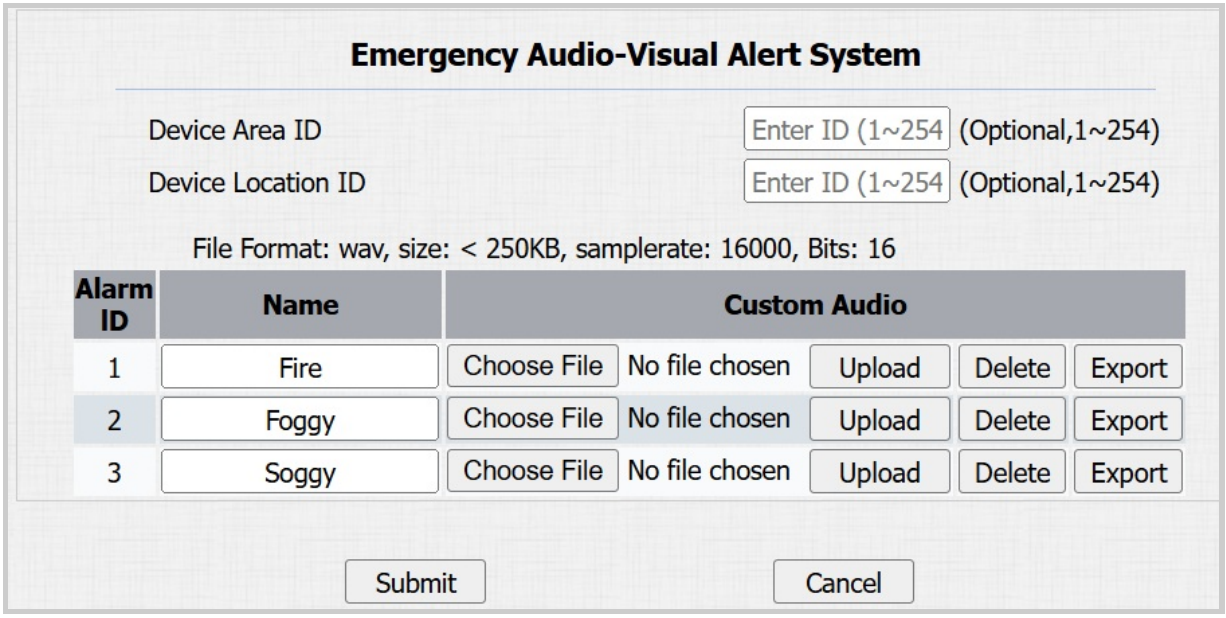
This feature allows E21 to manage and broadcast customized alarm audio files based on predefined alarm IDs.

When an alarm is triggered by the R49 broadcast, E21 can:

- Play a predefined audio file.
- Activate relay outputs for external alarm devices (such as LED indicators or speakers).
- Identify devices by area and location for zone-based alarm management.

This feature supports zone-oriented emergency notification and coordinated alarm control.

Set it up on the **Security > Basic** interface.



- **Device Area ID**: The range is 1–254 (optional).
  Defines the area number to which the E21 device belongs.
  This parameter is used for zone-based alarm control and broadcast management.
  - If configured, the device responds to alarm broadcasts targeting the same Area ID.
  - If left empty, the device is not restricted by area-based filtering.
- **Device Location ID**: The range is 1–254 (optional).
  Defines the specific location number of the device within an area.
  It is also used to determine how the E21 activates its relay outputs when receiving an alarm broadcast containing a location ID.
  If the received Location ID is less than the device's Location ID:
  → Relay 1 is activated.

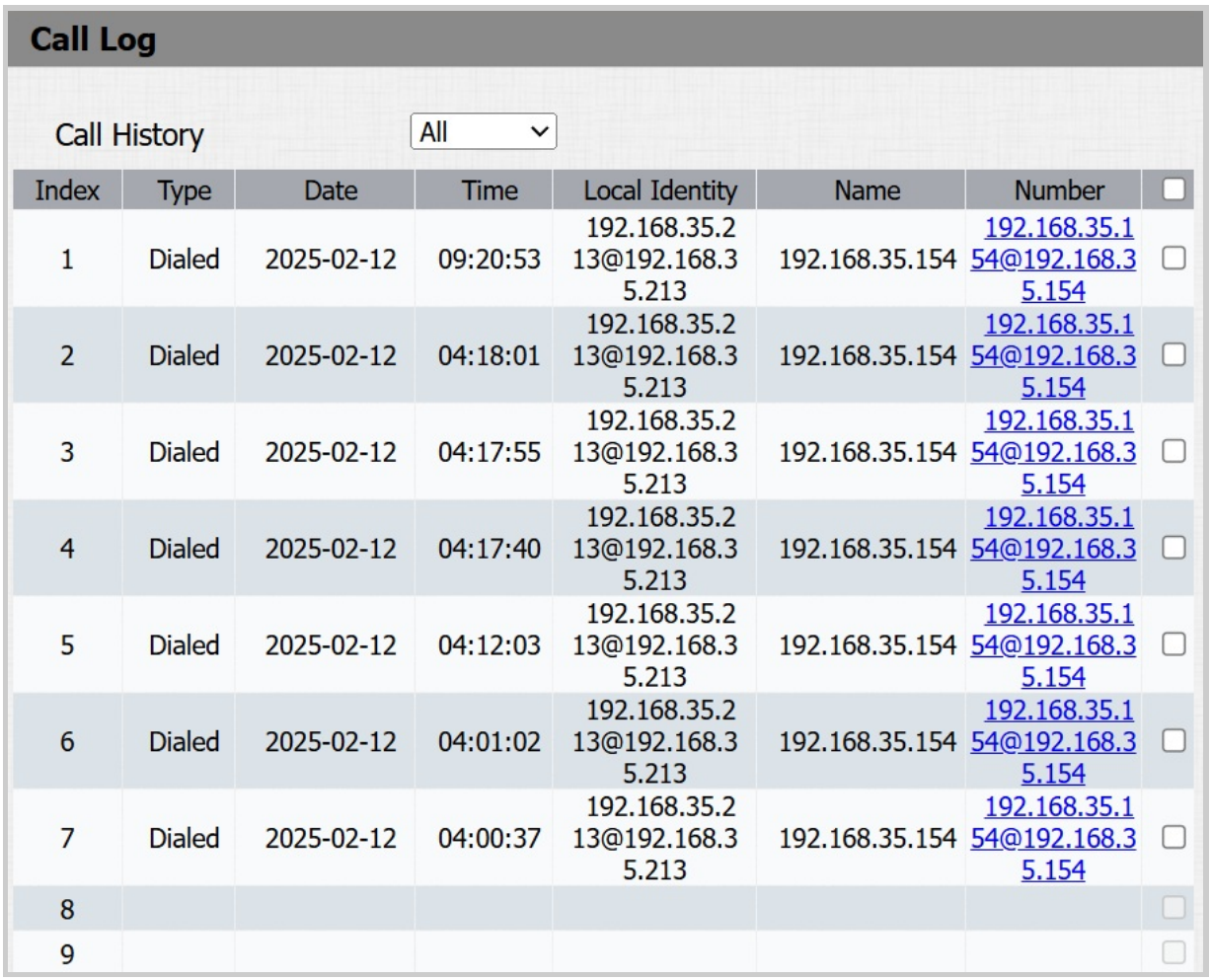
If the received Location ID is greater than the device's Location ID:
→ Relay 2 is activated.
If the received Location ID is equal to the device's Location ID:
→ Both Relay 1 and Relay 2 are activated.

- **Alarm Name**: A user-defined label for each alarm ID. Used for identification in the configuration interface. Does not affect triggering logic.
- **Custom Audio**: Each Alarm ID supports uploading a dedicated audio file.
    - File Requirements: Format: WAV; Maximum file size: < 250 KB; Sample rate: 16,000 Hz; Bit depth: 16-bit.
- **Available Actions**:
    - Choose File – Select a local audio file.
    - Upload – Upload the selected file to the device.
    - Delete – Remove the currently uploaded audio file.
    - Export – Download the configured audio file.

Logs

To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

Check call logs on the **Device > Call Log** interface.



Call Log

Call History: All

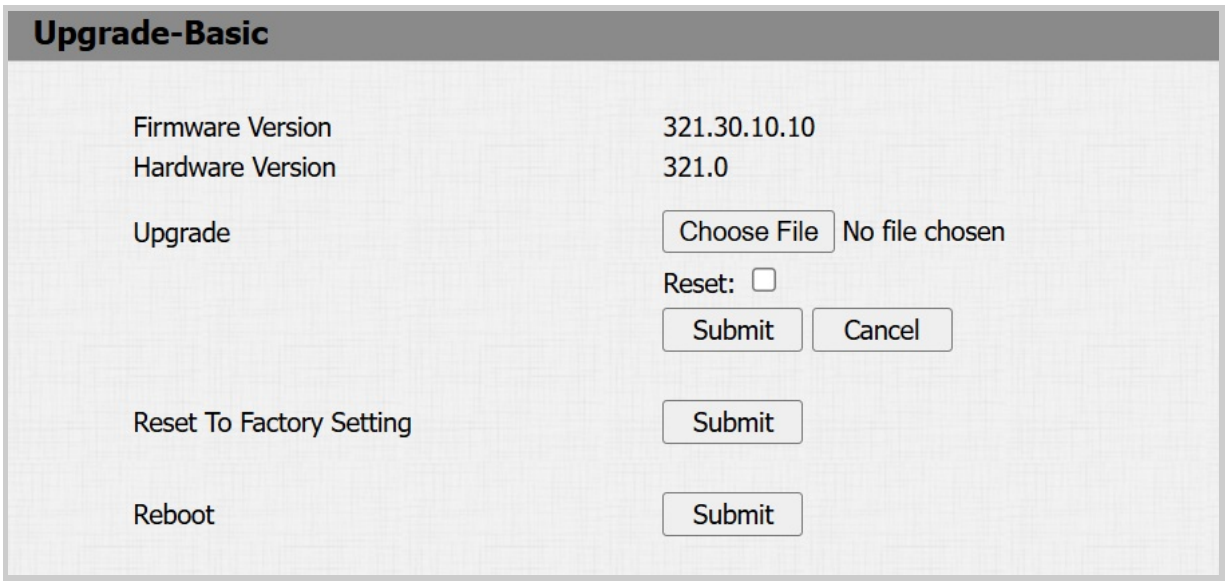
Index	Type	Date	Time	Local Identity	Name	Number
1	Dialed	2025-02-12	09:20:53	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
2	Dialed	2025-02-12	04:18:01	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
3	Dialed	2025-02-12	04:17:55	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
4	Dialed	2025-02-12	04:17:40	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
5	Dialed	2025-02-12	04:12:03	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
6	Dialed	2025-02-12	04:01:02	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
7	Dialed	2025-02-12	04:00:37	192.168.35.213@192.168.35.213	192.168.35.154	192.168.35.154@192.168.35.154
8						
9						

- **Call History**: Four types of call history are available: All, Dialed, Received, and Missed。
- **Local Identity**: Display the device's SIP account or IP number that receives incoming calls.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Upgrade the firmware on the **Upgrade > Basic** interface.



Note

Firmware files should be in .rom format for upgrade.

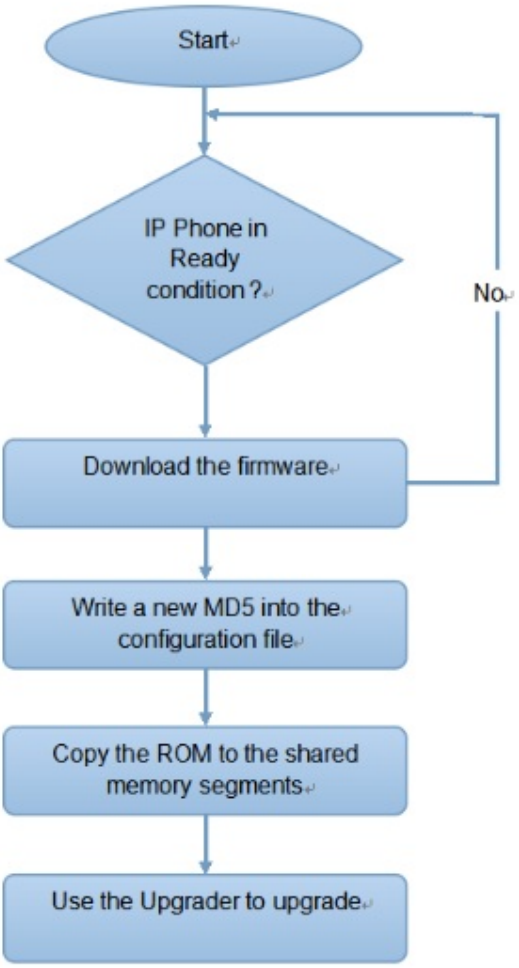
Auto-provisioning via Configuration File

You can configure and upgrade the device through the web interface using one-time or scheduled auto-provisioning with configuration files. This eliminates the need to set up configurations manually, saving you time and effort.

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 for auto-provisioning come in two formats: general configuration files and MAC-based configuration files.

Differences:

- **General Configuration Provisioning**:

A general configuration file is stored on a server, allowing all related devices to download the same file to update parameters.

- **MAC-Based Configuration Provisioning**:

MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

Note

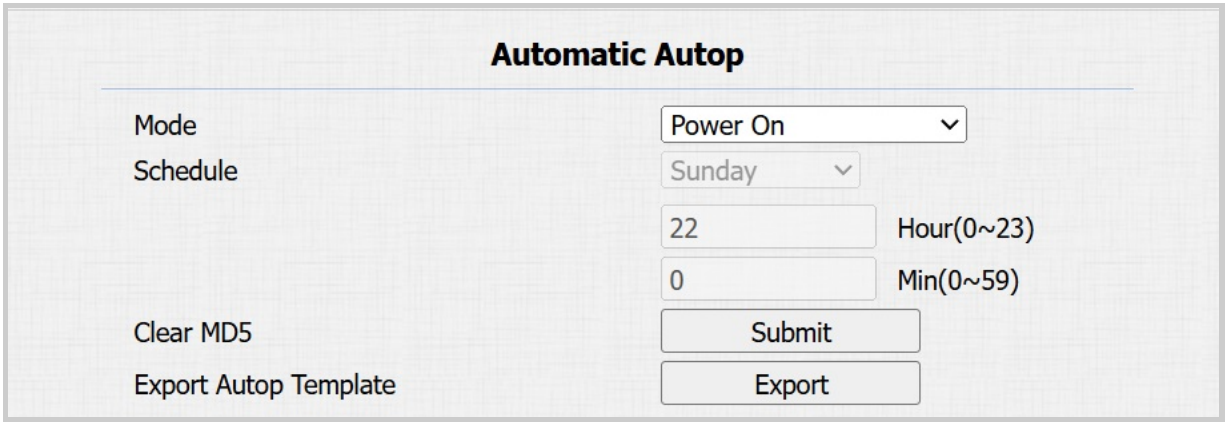
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

AutoP Schedule

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

To set it up, go to the web **Upgrade > Advanced > Automatic Autop** interface.



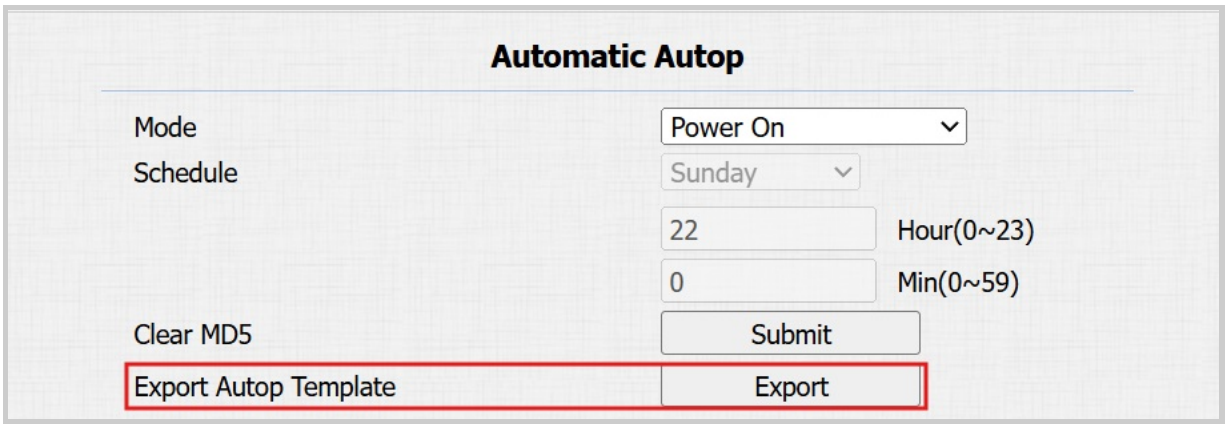
- **Mode**:
  - **Power On**: Allow the device to perform Autop every time it boots up.

  - **Repeatedly**: Allow the device to perform Autop according to the schedule.
  - **Power On + Repeatedly**: Combine **Power On** and **Repeatedly** modes, allowing the device to perform Autop every time it boots up or according to the schedule.
  - **Hourly Repeat**: Allow the device to perform Autop every hour.
- **Schedule**: When **Power On + Repeatedly** mode is selected, you can select the specific day and time for the Autop.
- **Clear MD5**: Used to compare the existing autop file with the autop file in the server, if the files are the same, then the provisioning will be stopped, thus avoiding unnecessary auto-provisioning.

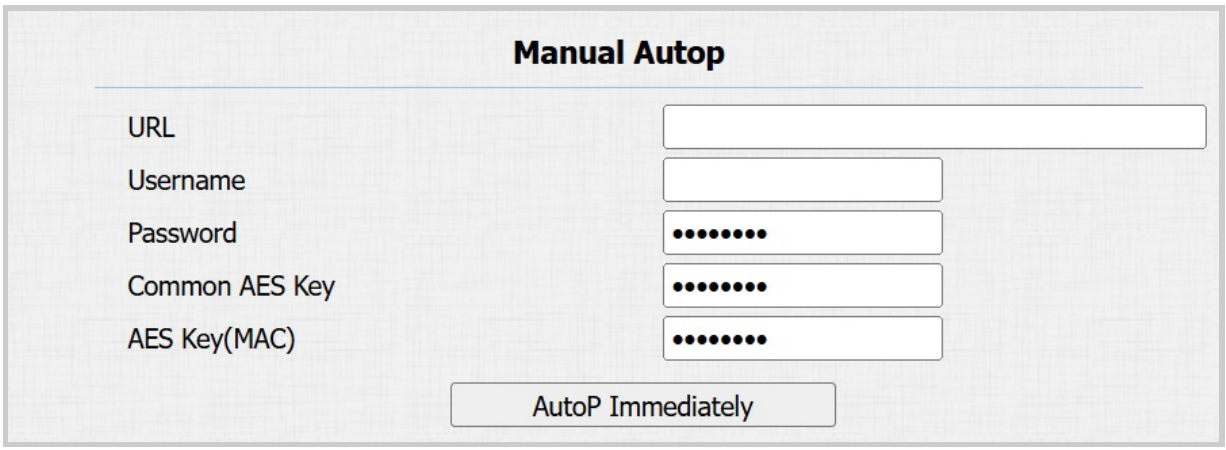
Static Provisioning Configuration

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.

To set it up, download the template on **Upgrade > Advanced > Automatic Autop** interface first.



Set up the Autop server in the **Manual Autop** section.



- **URL**: The TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Set up a username if the server needs a username to be accessed.
- **Password**: Set up a password if the server needs a password to be accessed.
- **Common AES Key**: Set up AES code for the intercom to decipher the general Auto Provisioning configuration file.
- **AES Key(MAC)**: Set up the AES code for the intercom to decipher the MAC-based auto-provisioning configuration file.

Note

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

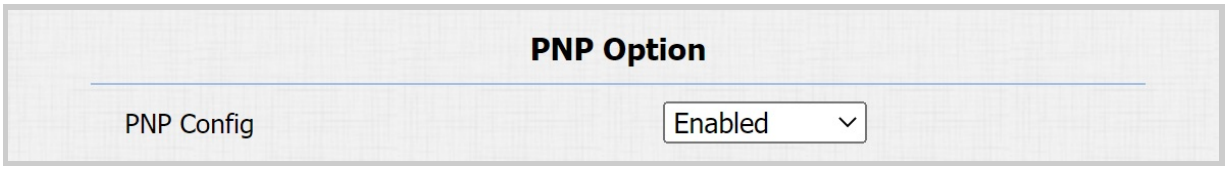
> **Tip**
>
> Akuvox does not provide a user-specified server. Please prepare the TFTP/FTP/HTTP/HTTPS server by yourself.

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.

Click here to watch the configuration video.

Set it up on the **Upgrade > Advanced > PNP Option** interface.



Backup

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

Export the file on the **Upgrade > Advanced** interface. The import file should be in .tgz/.conf/.cfg format.

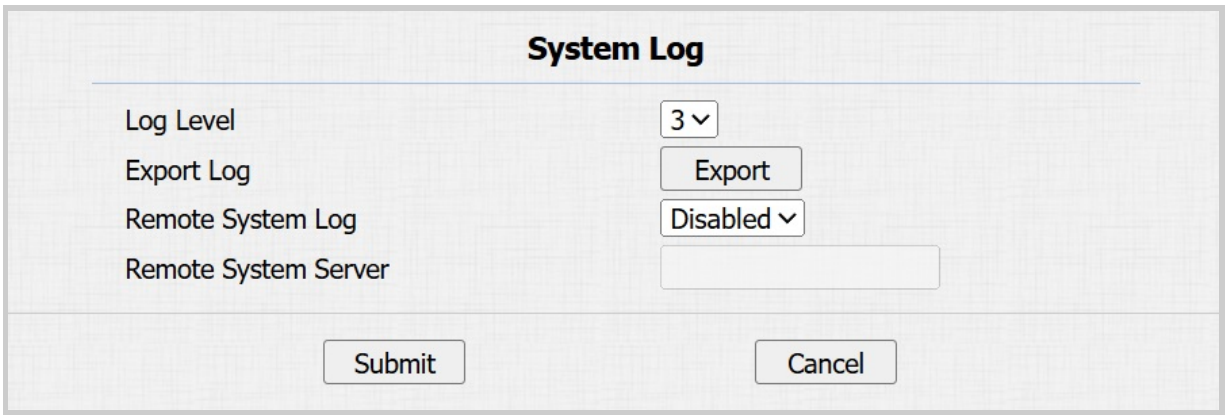


Debug

System Log

System logs can be used for debugging purposes.

To set it up, go to **Upgrade > Advanced > System Log** interface.

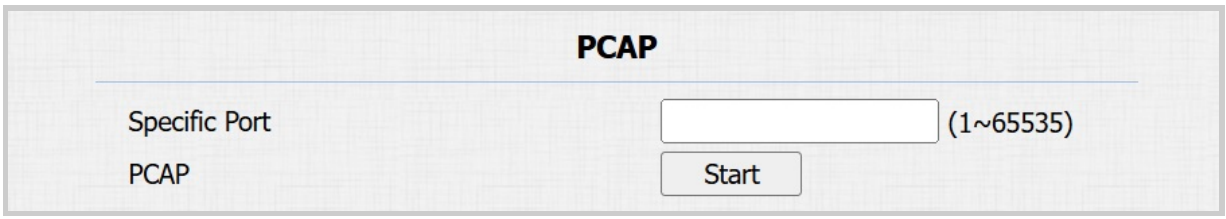


- **Log Level:** Select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log:** Click the Export tab to export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

Set it up on the **Upgrade > Advanced > PCAP** interface.

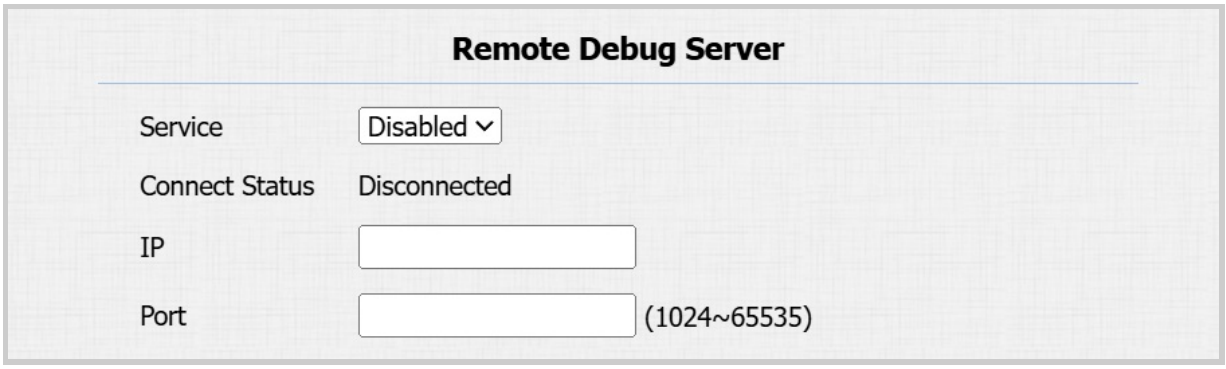


- **Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the Start tab and Stop tab to capture a certain range of data packets before clicking the Export tab to export the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

Remote Debug Server

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

To set it up, go to the **Intercom > Advanced** interface.



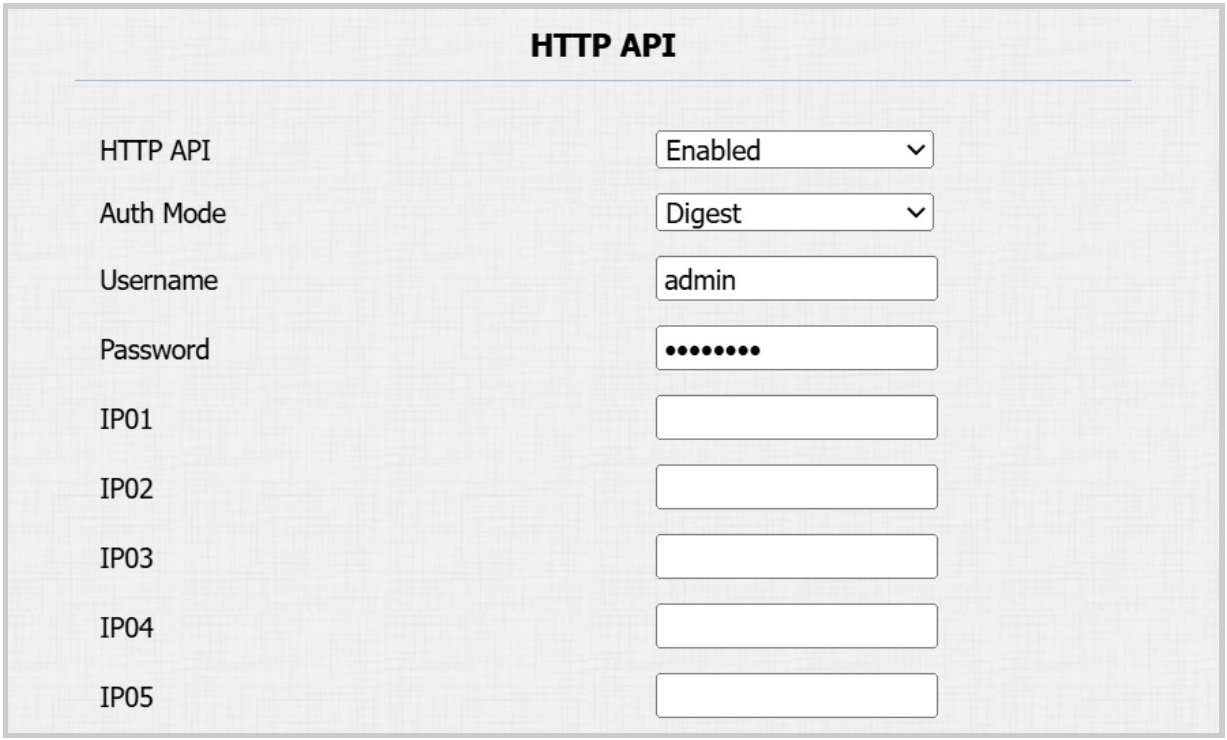
- **Connect Status**: Display the connection status between the device and the server.
- **IP**: Enter the IP address of the server.
- **Port**: Enter the port of the server.

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.

To set it up, go to the **Intercom > HTTP API** interface.



- **HTTP API** Enable or disable the HTTP API function for third-party integration. If the function is disabled, any request to initiate the integration will be denied and return HTTP 403 forbidden status.
- **Authorization Mode**: Select among the following options: None, Normal, Whitelist, Basic, Digest, and Token for authorization type, which will be explained in detail in the following chart.
- **Username**: Enter the user name when **Basic** or **Digest** authorization mode is selected. The default username is admin.
- **Password**: Enter the password when **Basic** or **Digest** authorization mode is selected. The default password is admin.
- **1st IP-5th IP**: Enter the IP address of the third-party devices when the **Allowlist** authorization is selected for the integration.

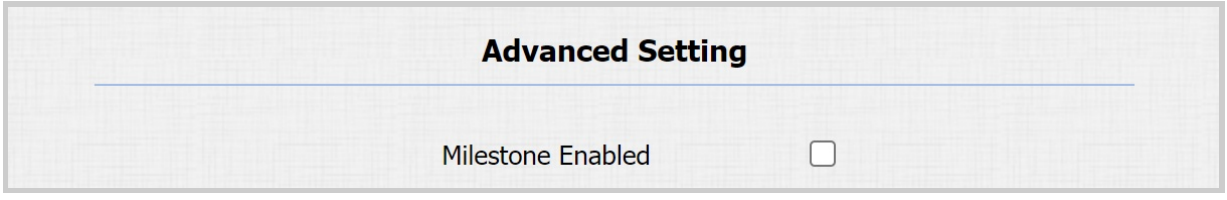
Please refer to the following description for the authentication mode:

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 allowlist is suitable for operation in the LAN.
4	Basic	If this mode is selected, you are required to fill in the username and password for the authentication. In the Authorization field of the HTTP request header, use the Base64 encode method to encode of username and password.
5	Digest	The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the 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.

To set it up, go to the **Intercom > ONVIF** interface.



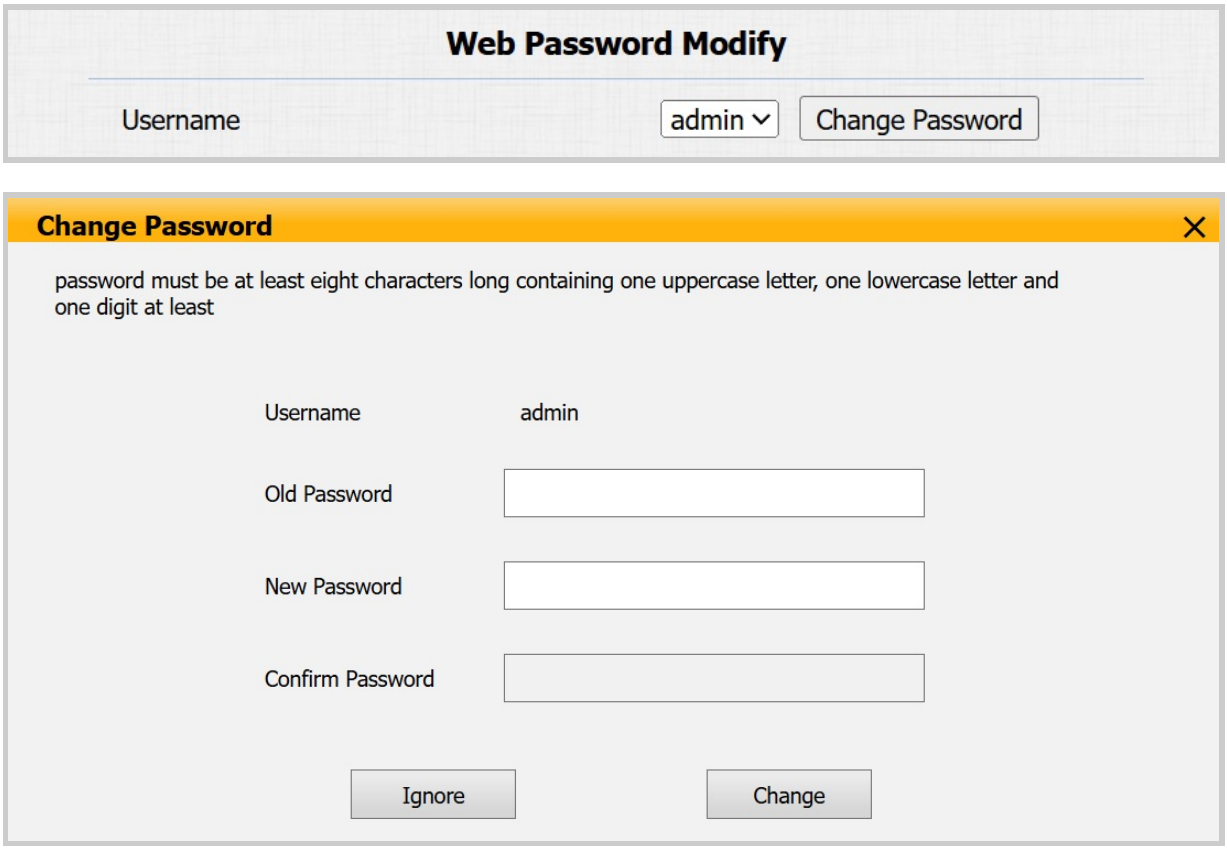
Note

Click **here** to view the details of integration with Milestone.

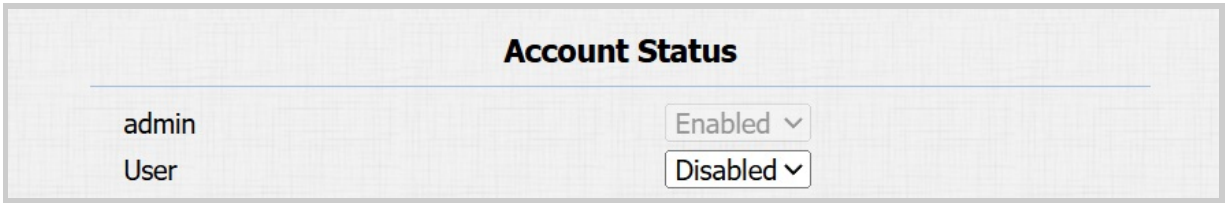
Password Modification

You can modify the device web interface login password for both administrator and user accounts.

Go to the **Security > Basic** interface and click **Change Password**.



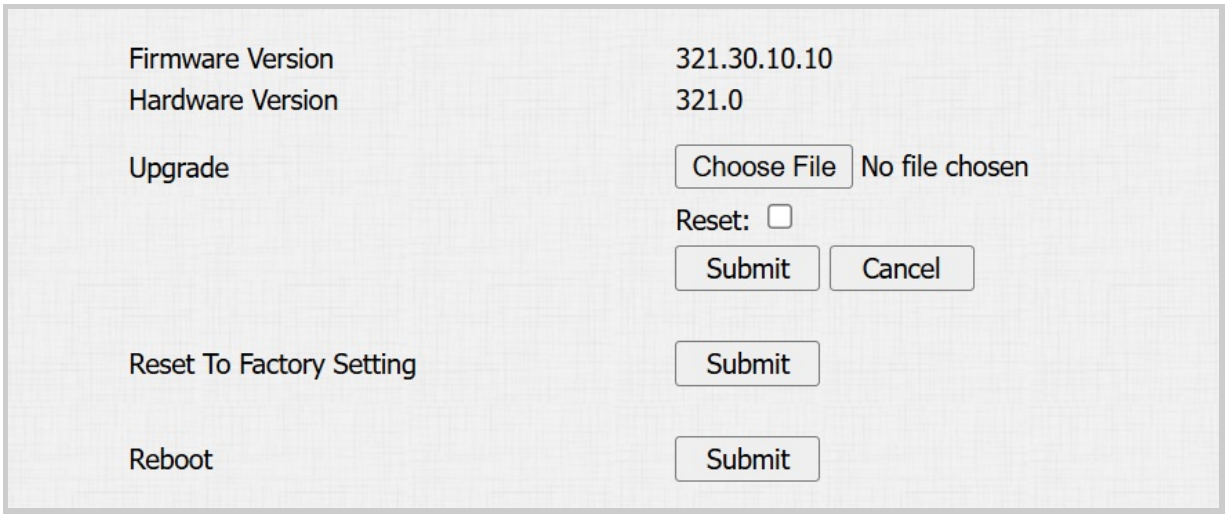
You can enable or disable the use of the user account on the **Account Status** part.



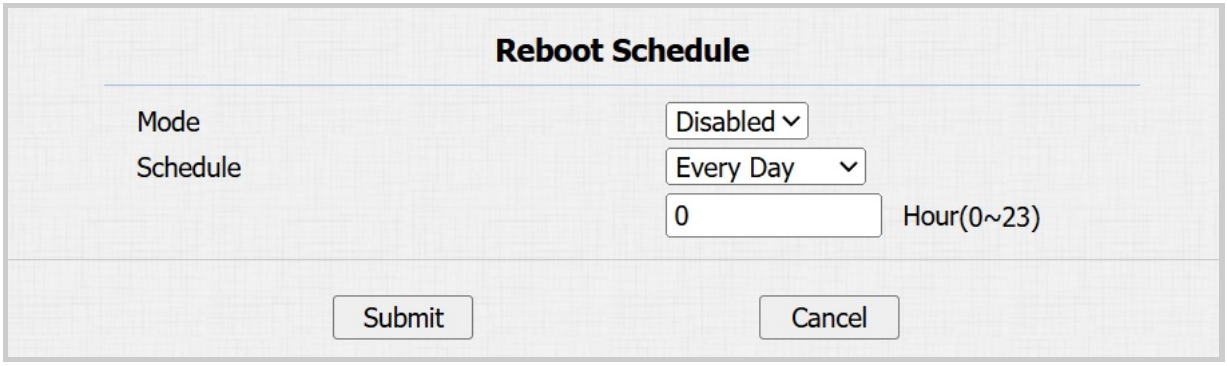
System Reboot&Reset

Reboot

Reboot the device on the web **Upgrade > Basic** interface.

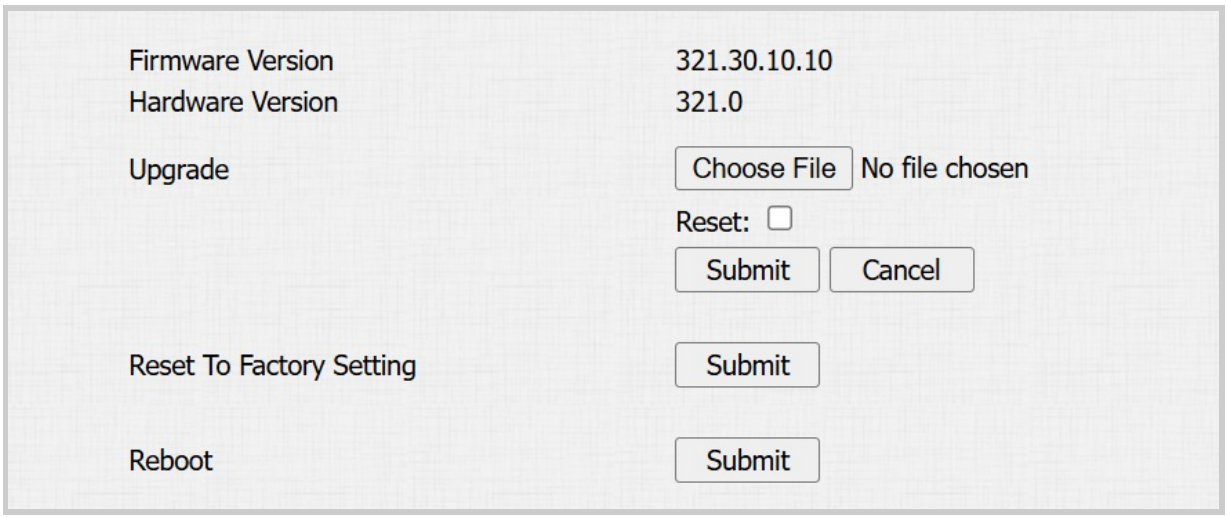


You can set up the reboot schedule on the web **Upgrade > Advanced > Reboot Schedule** interface.



Reset

Reset the device on the web **Upgrade > Basic** interface.



Powered by Document360