Akuvox

Table of contents

Akuvox S560 Series Indoor Monitor Administrator Guide

About This Manual 5

Product Overview 7

Changelog 8

Model Specifications 9

Introduction to Configuration Menu 10

Access the Device 12

- Obtain Device IP Address 12
  - IP Broadcast 12
  - Use IP Scanner 12
- Access Web Settings 13

Language and Time 15

- Language 15
  - Custom Language 15
- Time 16
- Daylight Saving Time 17

Indicator Light Setting 19

Sound and Volume 21
Volume Configuration 21
Upload Tone Files 22
Network Setting 23
Device Network Configuration 23
Device Deployment in Network 24
Device Local RTP Configuration 25
Device Web HTTP Setting 26
Device NAT Setting 26
SNMP Setting 27
Intercom Call Configuration 28
IP Call Configuration 28
Make IP Calls 28
SIP Call Configuration 28
SIP Account Registration 28
SIP Server Configuration 29
Outbound Proxy Server 30
SIP Call DND & Return Code Configuration 30
SIP Hacking Protection 31
Data Transmission Type 32

Call Setting 33
Press Button to Make a Call 33
Speed Dial 34
Call Forwarding 35
Pick up the Handle to Call 36
Contacts Management 38
Add Local Contacts 38
Import/Export Contacts 39
Audio Codec Configuration 40
Access Control Configuration 41
Remote Relay 41
Web Relay 41
Door-opening Configuration 44
Unlock by DTMF Code 44
Unlock via HTTP Command 45
HTTP or HTTPS Command Import/Export 46
Unlock Key Setup 47
Security 48
Voice Encryption 48
Web Interface Automatic Log-out 48

High Security Mode 49
Auto-provisioning via Configuration File 51
Provisioning Principle 51
Introduction to the Configuration Files for Auto-Provisioning 52
Autop Schedule 53
Static Provisioning 54
PNP Configuration 56
Call Logs 57
Firmware Upgrade 58
Backup 59
Debug 60
System Log for Debugging 60
PCAP for Debugging 60
User Agent 61
Password Modification 62
Modify Device Web Interface Password 62
Modify Security Questions 63
System Reboot & Reset 65
Reboot 65
Reset 65

Akuvox

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



S560
INDOOR MONITOR
Administrator Guide

Akuvox

Thank you for choosing the Akuvox S560 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. This manual applies to the 560.30.11.905 version, and it provides all the configurations for the functions and features of the S560 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



S560 series is a Linux SIP-based indoor device. It can be connected to the Akuvox door phone for audio communication and unlocking and can be deployed and maintained on the SmartPlus platform along with Akuvox door phones and SmartPlus app. It is economical, easy, and simple to use in such scenarios as small and medium-sized apartments.

Changelog

What's new in version 560.30.11.905:

- Added new web languages: Korean, Italian, Dutch, French, Vietnamese, and Arabic .
- Support selecting a ringtone for a specific contact.

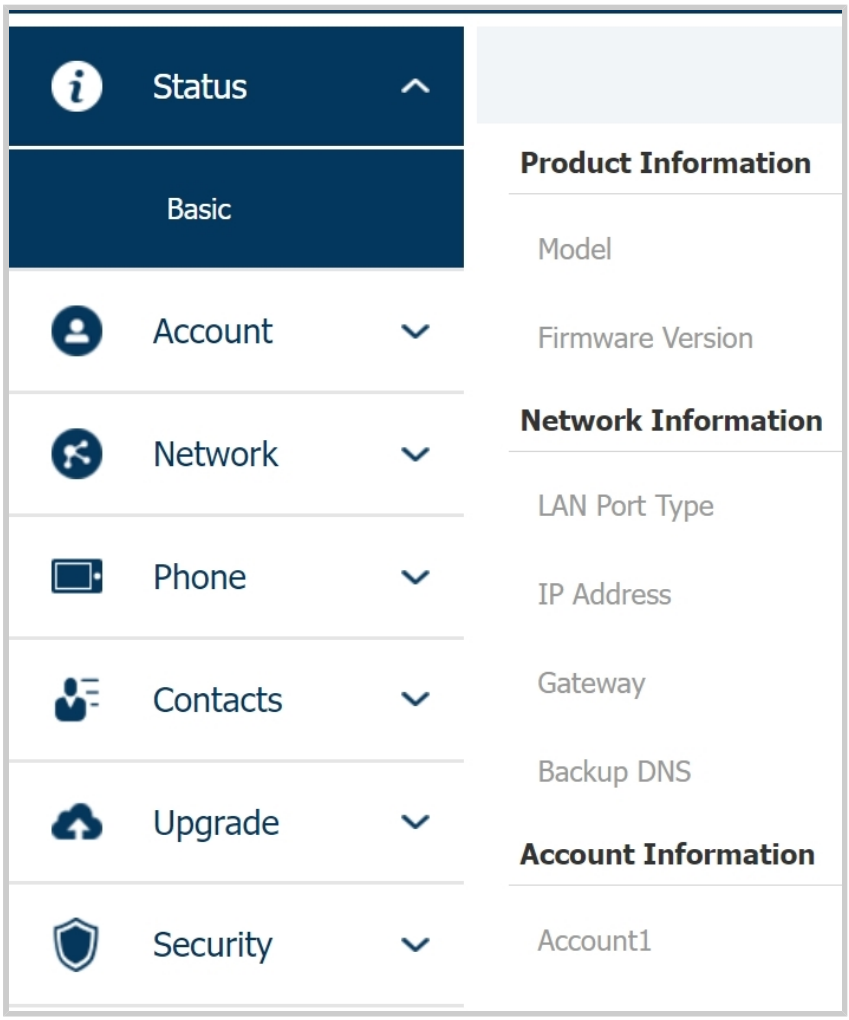
Click here to view the changelog of the device's previous versions.

Model Specifications

Model	S560
Speaker	Main unit: 8Ω1W
	Earpiece: 32Ω0.25W
MIC	-36dB
Card Reader	NA
Wi-Fi	NA
Bluetooth	NA
RJ45	x1, 10/100Mbps
Indicator light	x1
Power Supply	12VDC/1A or IEEE 802.3af PoE

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, account information, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio codecs, DTMF, etc.
- **Network**: This section mainly deals with DHCP & Static IP setting, RTP port setting, device deployment, etc.
- **Phone**: This section includes time and language management, call feature, audio control, light setting, key management, relay control, etc.
- **Contacts**: This section is for local contacts management.
- **Upgrade**: This section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.
- **Security**: This section is for password modification, account status & session time-out configuration, as well as high security mode switching.


Status
Basic
Account
Network
Phone
Contacts
Upgrade
Security
Product Information
Model
Firmware Version
Network Information
LAN Port Type
IP Address
Gateway
Backup DNS
Account Information
Account1

Access the Device

Within the same local network, you can enter the device IP address on the web browser to log in to the device web interface where you can configure parameters.

Obtain Device IP Address

> **Note**
>
> Ensure the device is connected to Ethernet and the handset is linked to the main unit; otherwise, it will be unable to obtain the IP address.

IP Broadcast

Press the **#** key for about 5 seconds, and the device will broadcast its IP address.

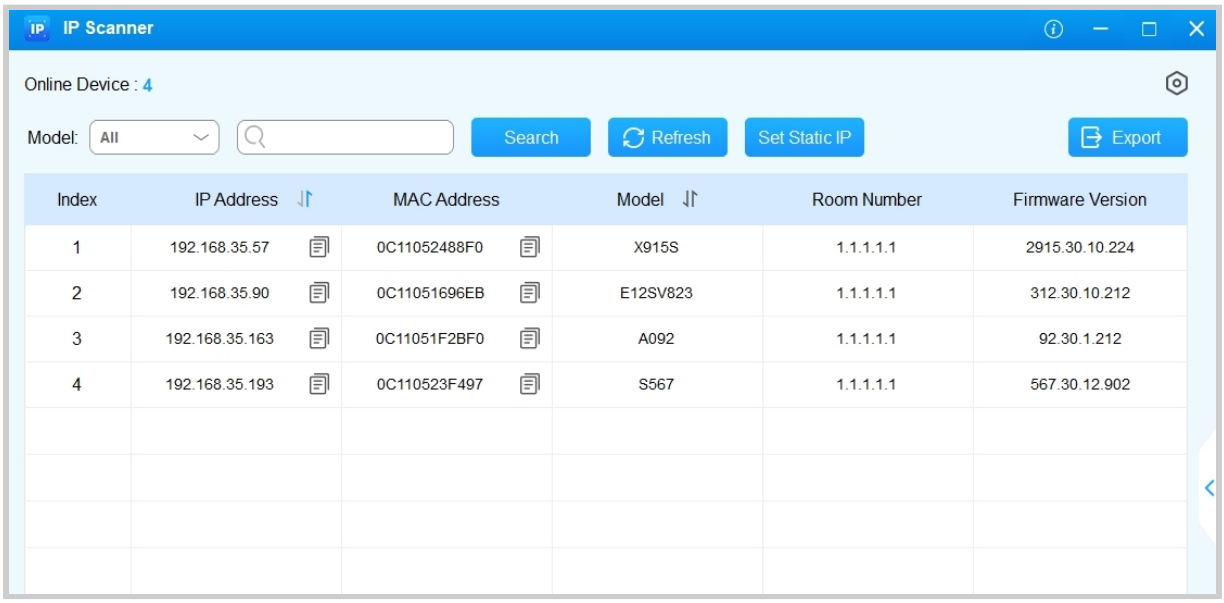
After logging in to the device web, you can set the IP announcement loop times on the **Phone > Audio** interface.



- **Loop Times**: The options range from 1 to 10.

Use IP Scanner

You can use the IP scanner tool to check the device's IP on the same local network.



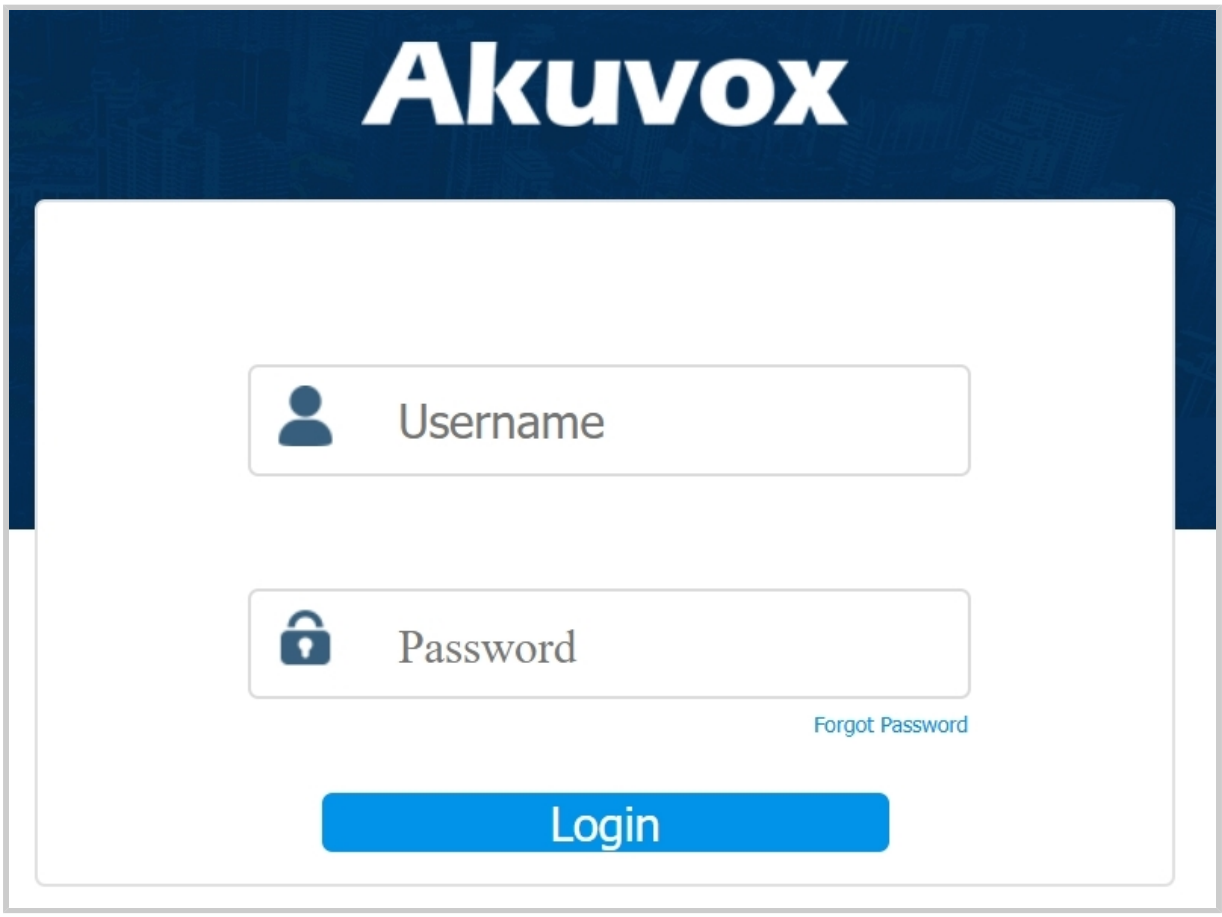
Note

- 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
- Your computer should be on the same network as the device.

Access Web Settings

Enter the device IP in a browser(Google Chrome is recommended).

Enter the username and password(The initials are both **admin**). Please be case-sensitive to the username and password entered.


Akuvox
Username
Password
Forgot Password
Login

Language and Time

Language

Select the web language on the **Phone > Time/Lang** interface.



- **Type**: Support **Auto** option and the following languages: English, Traditional Chinese, Russian, Korean, Portuguese, Spanish, Italian, Dutch, French, German, Polish, Turkish, Japanese, Simplified Chinese, Vietnamese, and Arabic. English is the default web language.

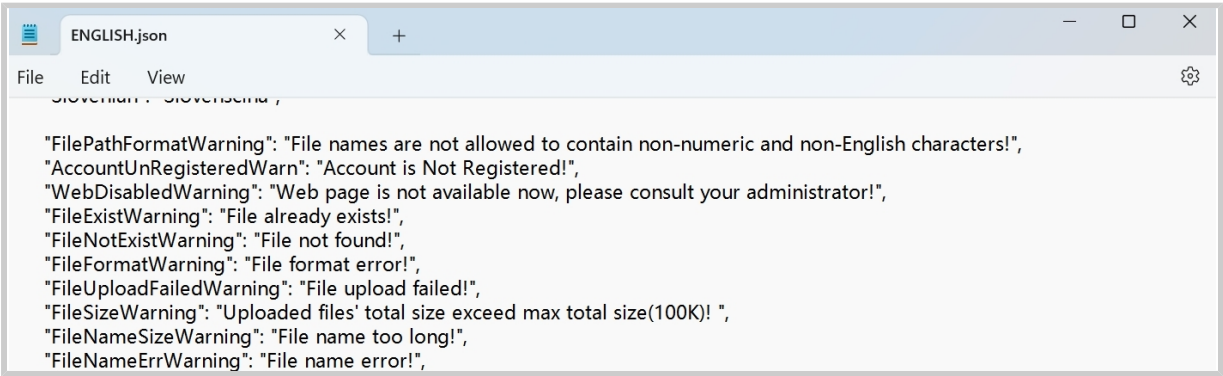
Custom Language

You can customize the configuration names and prompt texts on the device's web portal, such as the file name error warning.

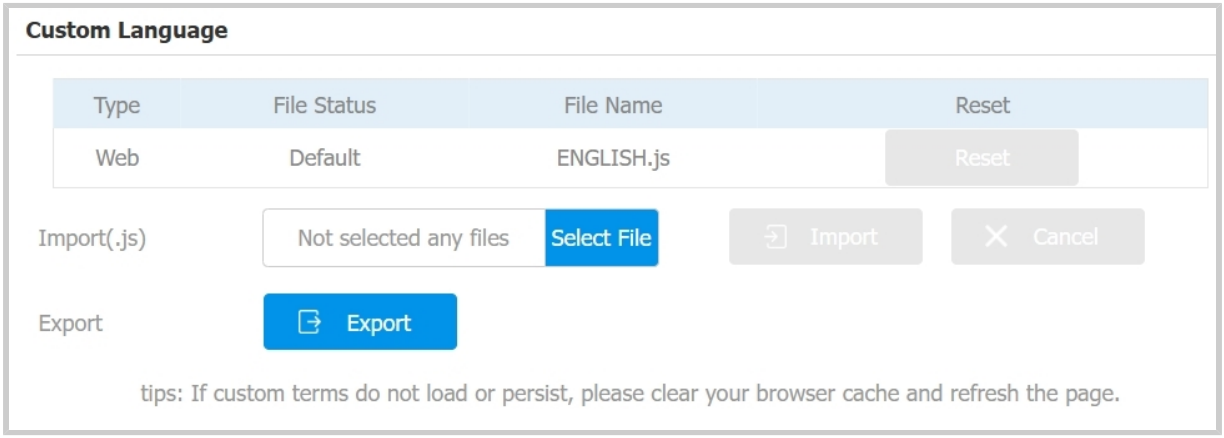
Export the .json file for editing. You may edit it with Notepad on your computer.

Import the .json file, and its size should be smaller than 1 MB.

File Example:



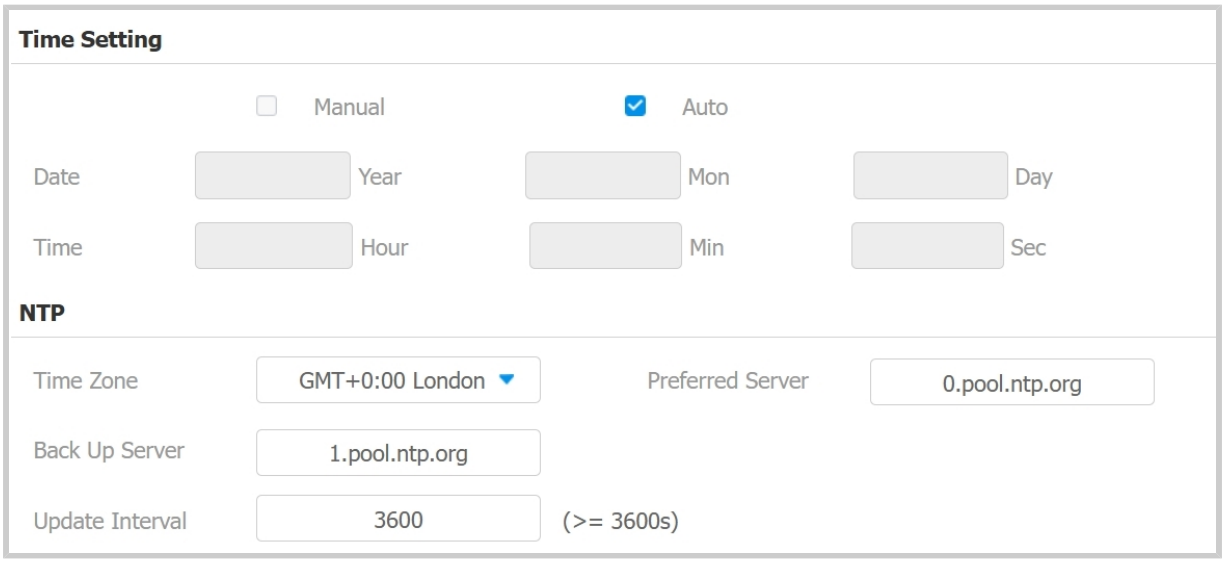
Set it up on the **Phone > Time/Lang** interface.



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 **Phone > Time/Lang** interface.

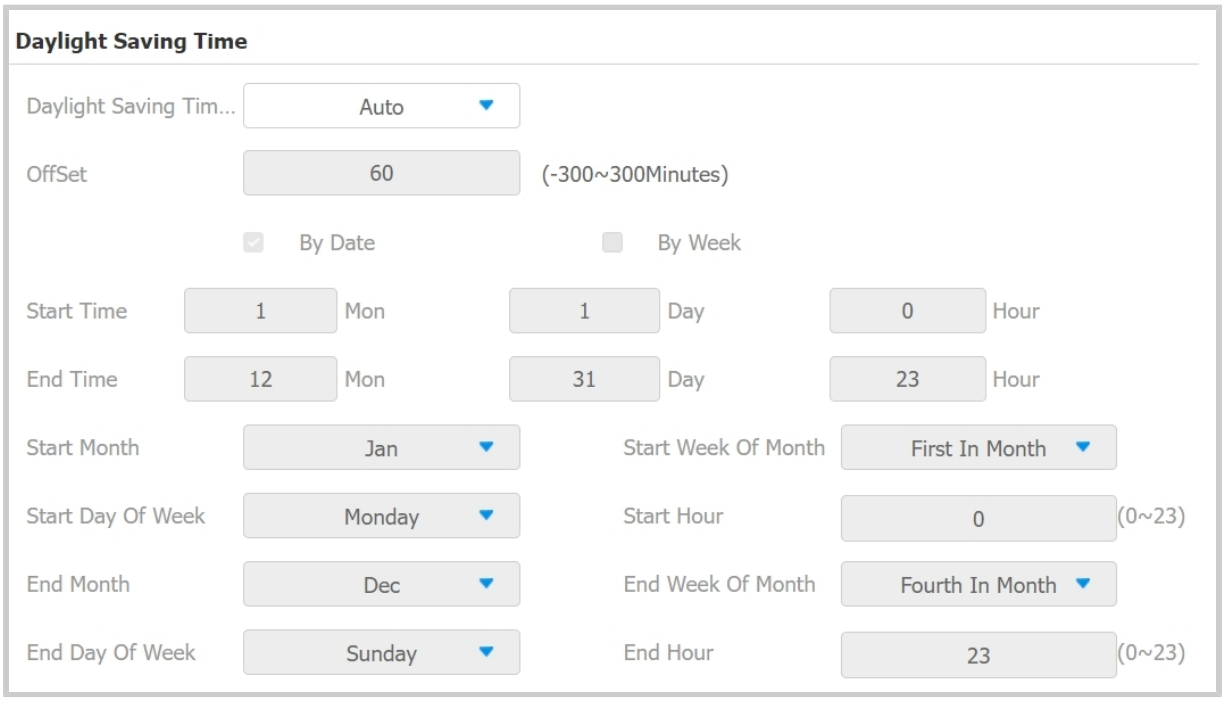


- **Time Setting**: Choose to set up time manually or automatically. Auto is the default option.
  - **Manual**: When checked, choose the date and time.
  - **Auto:** The device will update time based on the NTP settings below.
- **Preferred/Backup Server**: Enter the NTP server address. The backup server will take effect when the preferred server is invalid.
- **Update Interval**: The interval between two consecutive NTP requests.

Daylight Saving Time

Daylight Saving Time is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. You can modify the time parameters to achieve longer evenings or daytime, especially in summer.

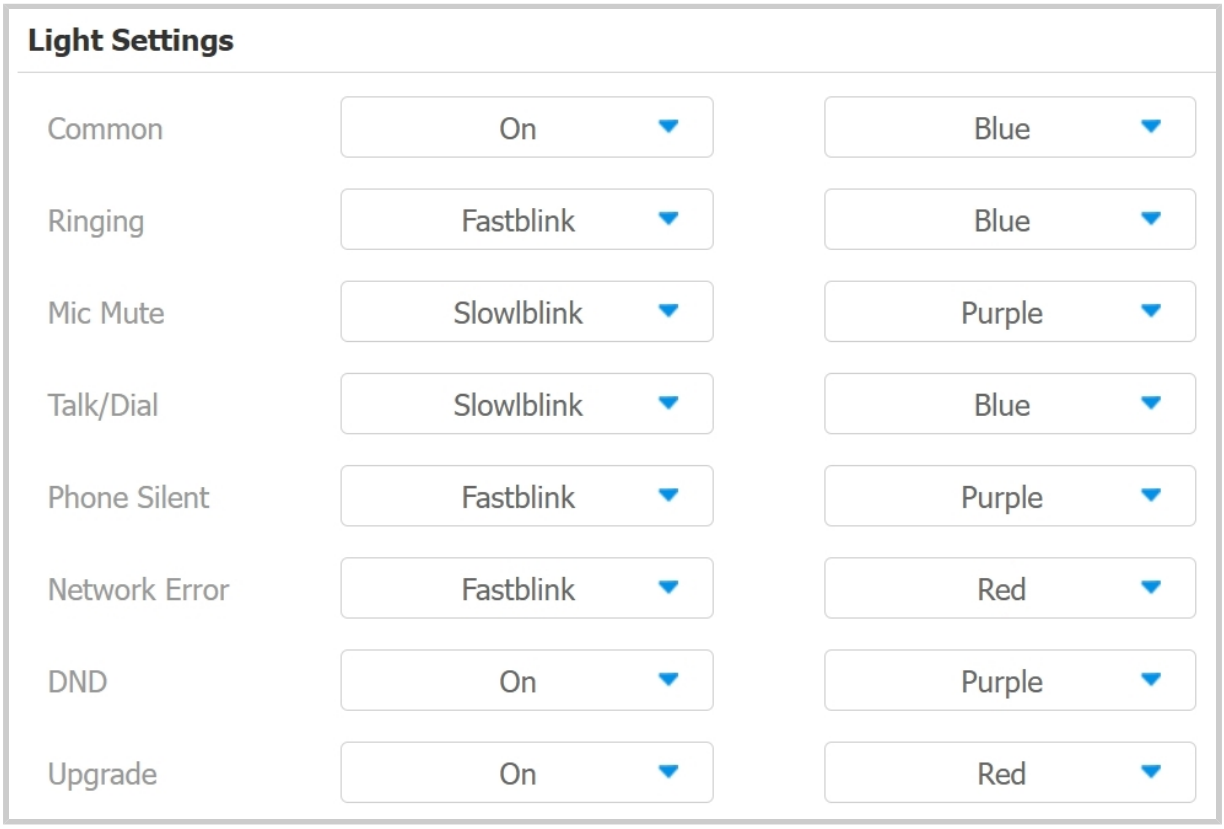
Set it up on the **Phone > Time/Lang** interface.



- **Daylight Saving Time Enabled**: Enable or disable the feature. **Auto** means that the device adjusts the daylight saving time automatically.
- **Offset**: 60 minutes as default, setting the clocks an hour ahead of the standard time.
- **By Date/By Week**: By Date sets the date schedule for daylight saving time. By Week sets the schedule for daylight saving time according to the week and month.

Indicator Light Setting

The device has an indicator light installed on the top surface. The light colors vary by the state the device is currently in. You can change light colors and states that represent the device status on the **Phone > Display** interface.



- **Status**: Select from On, Off, Fastblink, and Slowblink.
- **Color**: Select from Red, Blue, and Purple.

The default indicator light status:

Color	Indicator Light Status	Color Code
Blue	A solid blue light	Normal status
	A fast blinking blue light	Ringing
	A slowly blinking blue light	During a call or calling

Color	Indicator Light Status	Color Code
Purple	A solid purple light	Do Not Disturb is on
	A solid purple light	The handle is picked up
	A fast blinking purple light	Mute ringing
	A slowly blinking purple light	Mute MIC
Red	A solid red light	Rebooting or upgrading
	A fast blinking red light	Network error

Note

- The default indicator light priority:

DND > Network error > Mute ringing = Mute MIC > Ringing = During a call = Calling > The handle is picked up = Normal status

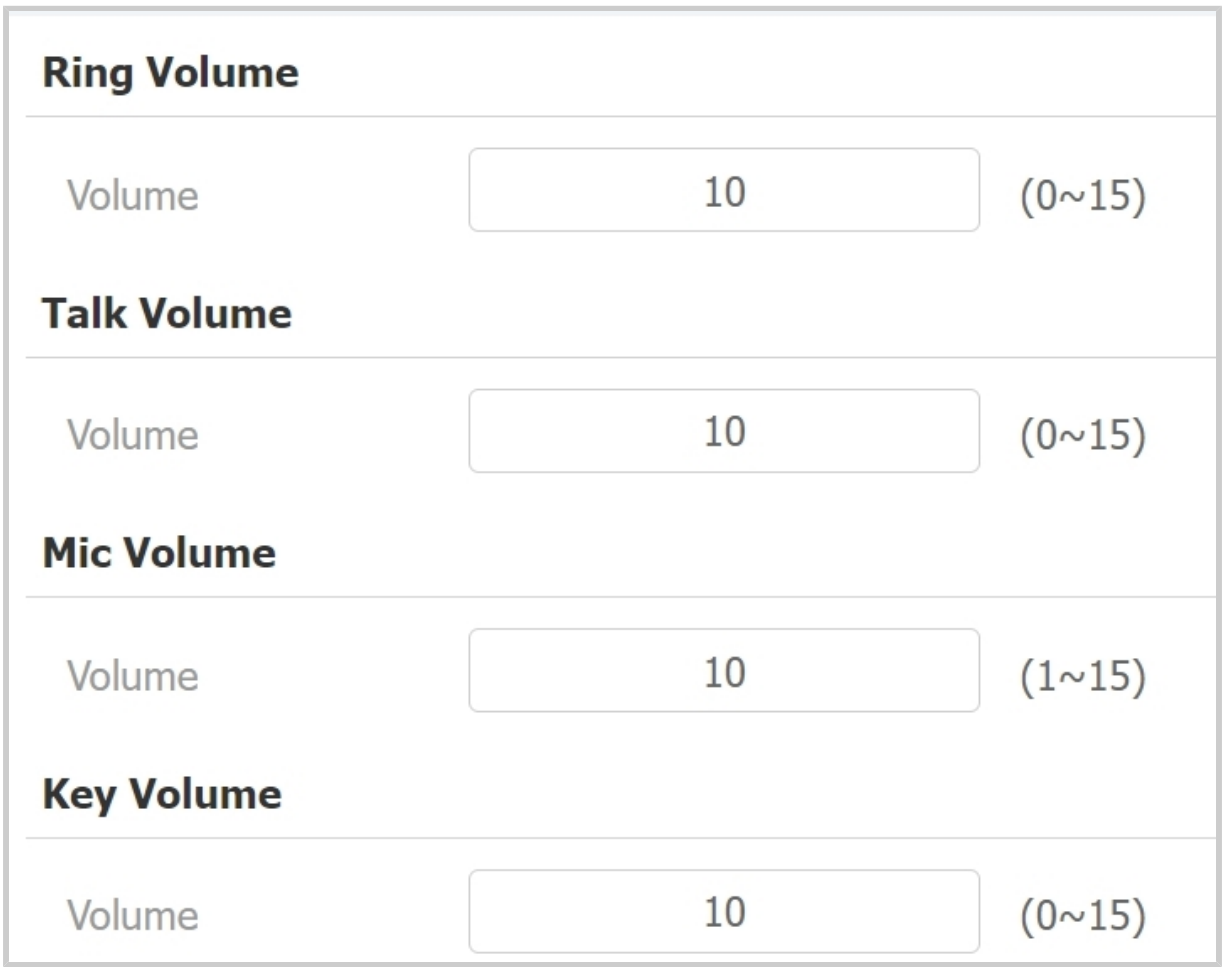
- Among the states with the same priority, the indicator light of the latest state will be on.

Sound and Volume

S560 provides you with various types of ringtones and volume configurations.

Volume Configuration

Set up volumes on the device **Phone > Audio** interface.

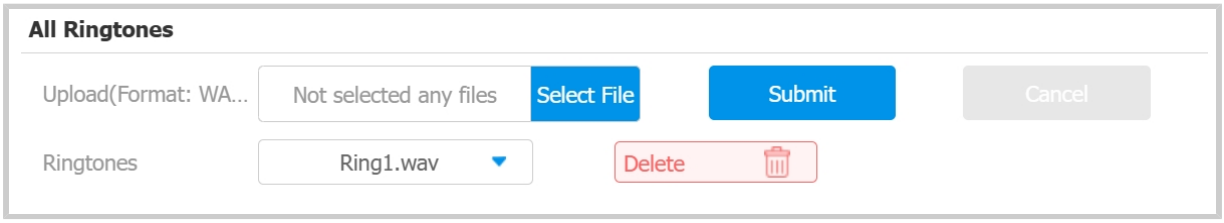


Note

Ring volume and talk volume can also be adjusted on the device by pressing the + and - buttons.

Upload Tone Files

Select and upload ringtones on the **Phone > Audio** interface.



File Requirements

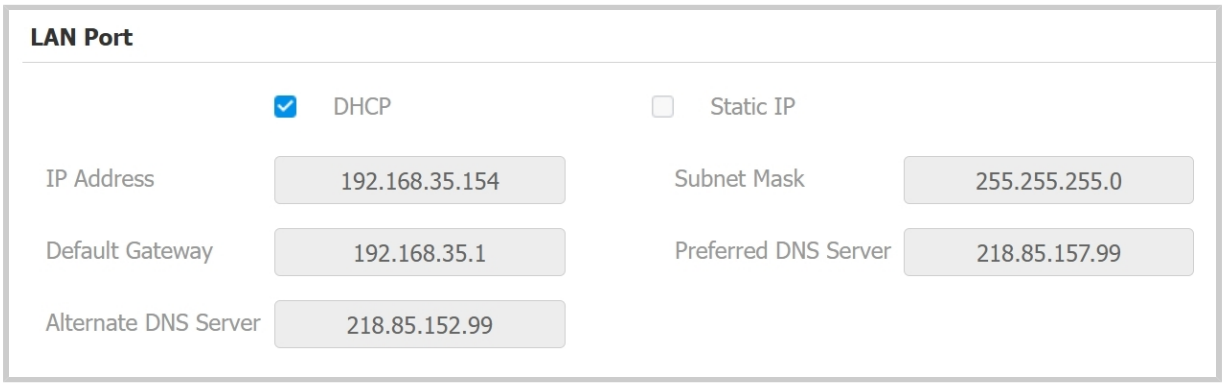
Format: WAV; Max Size: 250 KB; File Name: Less than 8 Chinese characters or 23 characters, &'` characters are not supported; Sample Rate: 8,000Hz; Bit Rate: 64 kbps; Channels: Mono; Audio Codec: PCMU or PCM.

Network Setting

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.

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



- **DHCP**: The default network connection. If the DHCP mode is selected, the device will be assigned by the DHCP server with an 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(es) have to be manually configured according to the actual network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.

- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **Preferred/Alternate DNS Server**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The device connects to the alternative DNS server when the primary one is unavailable.

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.

Deploy the device in the network on the web **Network > Advanced** interface.



- **Connect Mode**: You can set up the connect mode according to the device connection with a specific server in the network, such as **SDMC**, **Cloud,** or **None**. You can also select it manually.

  - **None**: None is the default factory setting, indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.

  - **Cloud**: The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.
  - **SDMC**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

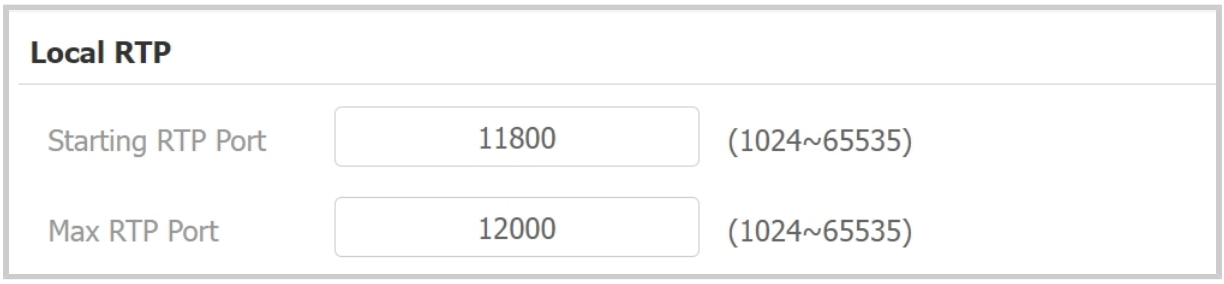
- **Discovery Mode**: With discovery mode enabled, the device can be discovered by other devices in the network. Uncheck the box if you want to conceal the device.
- **Device Node**: Specify the device address by entering device location info from left to right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: The device extension number for the device you installed.
- **Device Location**: The location in which the device is installed and used.

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.

Set it up on the **Network > Advanced** interface.



- **Starting RTP Port**: Set the port value to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: Set the port value to establish the endpoint for the exclusive data transmission range.

Device Web HTTP Setting

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

Set it up on the **Network > Advanced** interface.



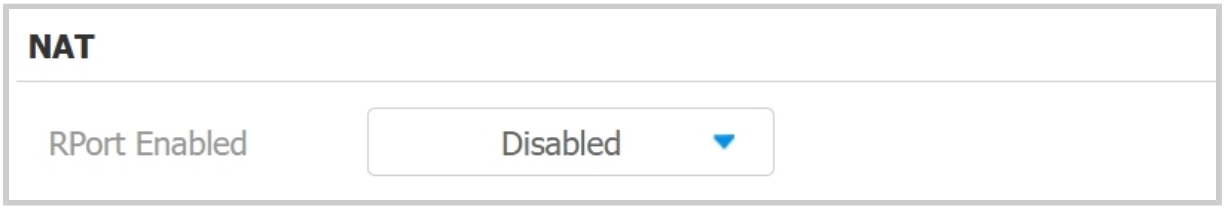
- **HTTPS Port**: Set the HTTPS port within the valid range.

Device 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 enable it, go to **Account > Advanced** interface.

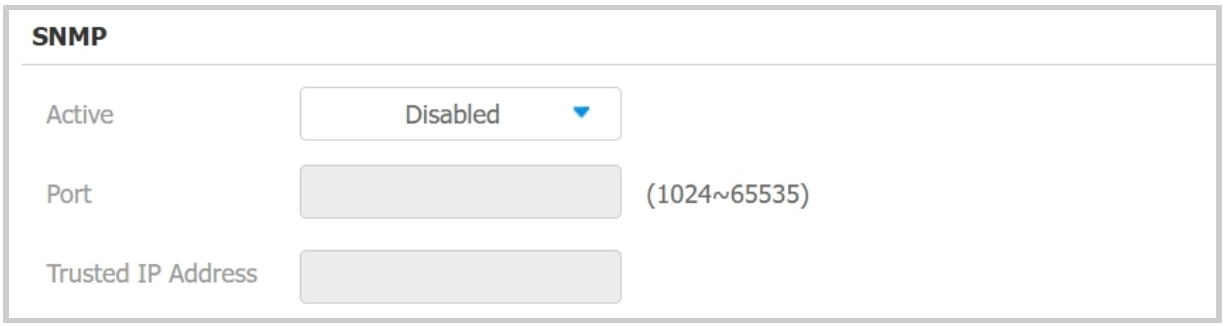


- **RPort**: Enable the RPort when the SIP server is in the WAN for the SIP account registration.

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).

Set it up on the **Network > Advanced** interface.



- **Port**: Set a specific port for the data transmission from 1024-65535.
- **Trusted IP Address**: Enter the third-party IP address.

Intercom Call Configuration

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.

Make IP Calls

Press the target IP number, e.g. 192*168*35×134 on the handset and press # to 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.

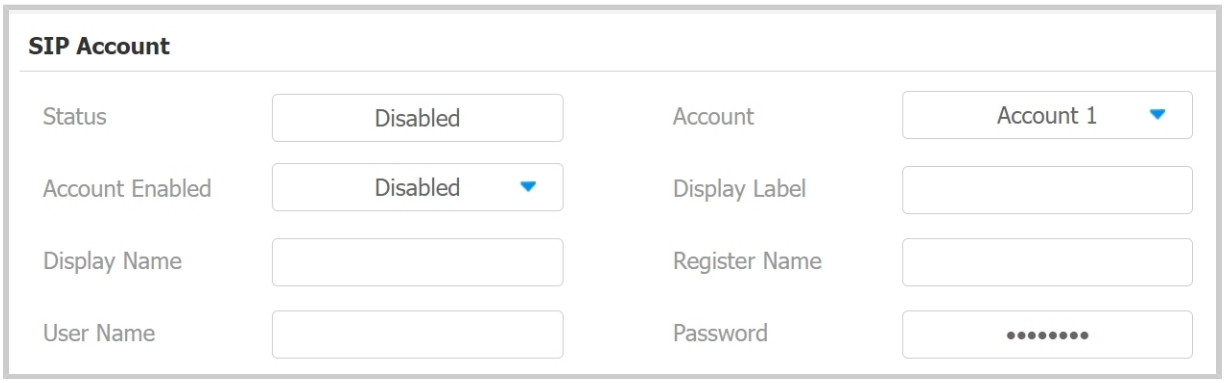
SIP Account Registration

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 accounts on the **Account > Basic** interface.

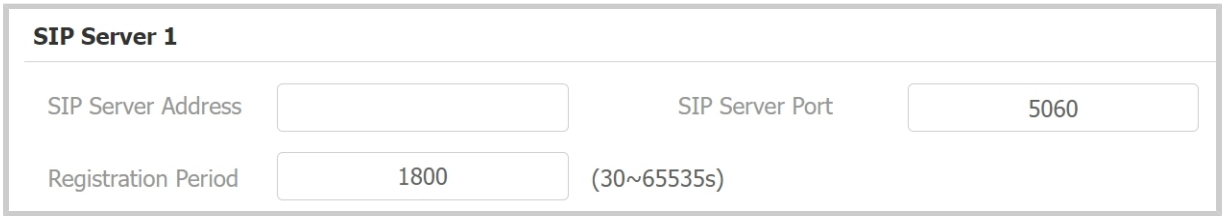


- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same 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.

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



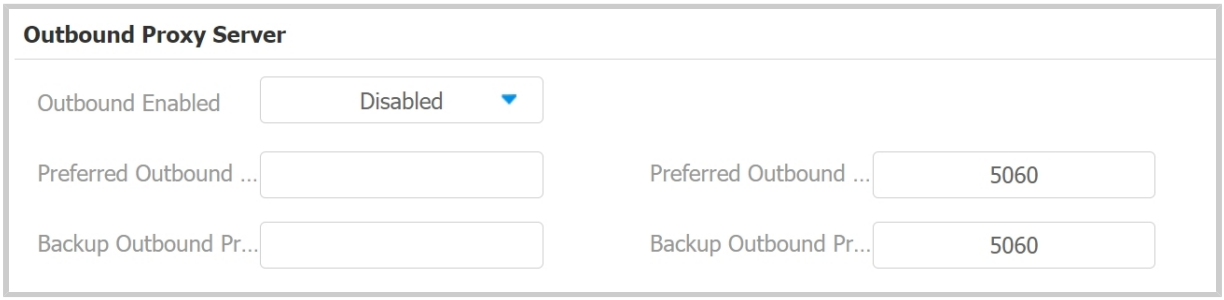
- **SIP Server Address**: Enter the server's IP address or its domain name.
- **SIP Server Port**: Specify the SIP server port for data transmission.

- **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, navigate to **Account > Basic** interface.

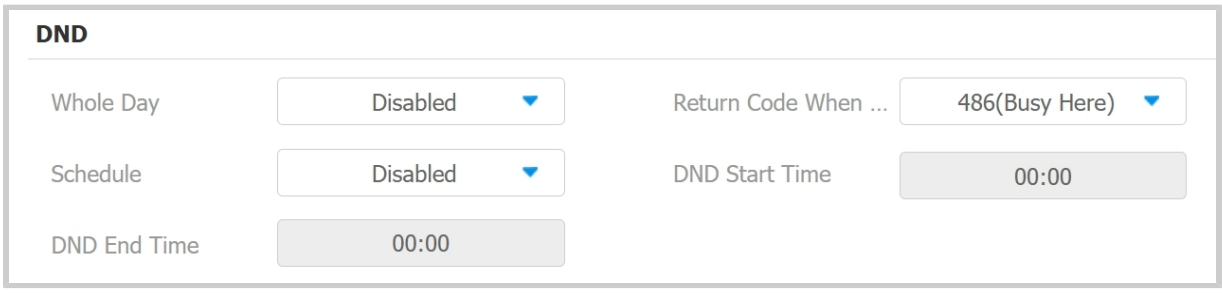


- **Preferred Outbound Proxy Server**: Enter the SIP proxy IP address.
- **Preferred Outbound Proxy Server Port**: Set the port for establishing a call session via the outbound proxy server.
- **Backup Outbound Proxy Server**: Enter the SIP proxy IP address to be used when the main proxy malfunctions.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

SIP Call DND & Return Code Configuration

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.

Set it up on the **Phone > Call Feature** interface.



- **DND**: Check **Whole Day** or **Schedule** to enable the DND function. The DND function is disabled by default.
- **Schedule**: Determine the DND period by selecting DND Start Time and DND End Time.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

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.

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

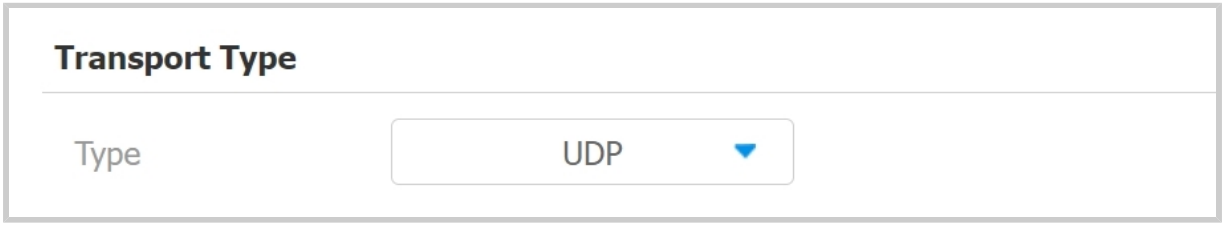


- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

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.



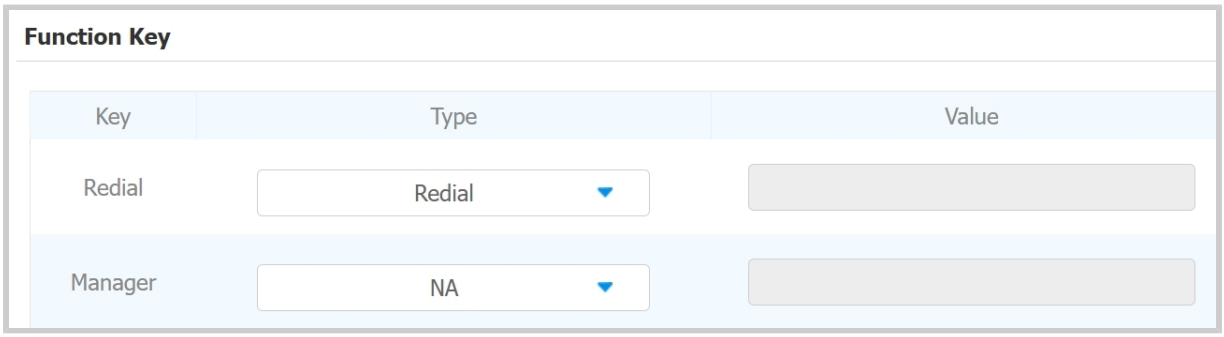
- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.
- **DNS-SRV**: A DNS service record defines the location of servers. This record includes the hostname and port number of the server, as well as the priority and weight values that determine the order and frequency of using the server.

Call Setting

Press Button to Make a Call

You can set up the call features by pressing and on the device.

Set up this feature on the **Phone > Function Key** interface.



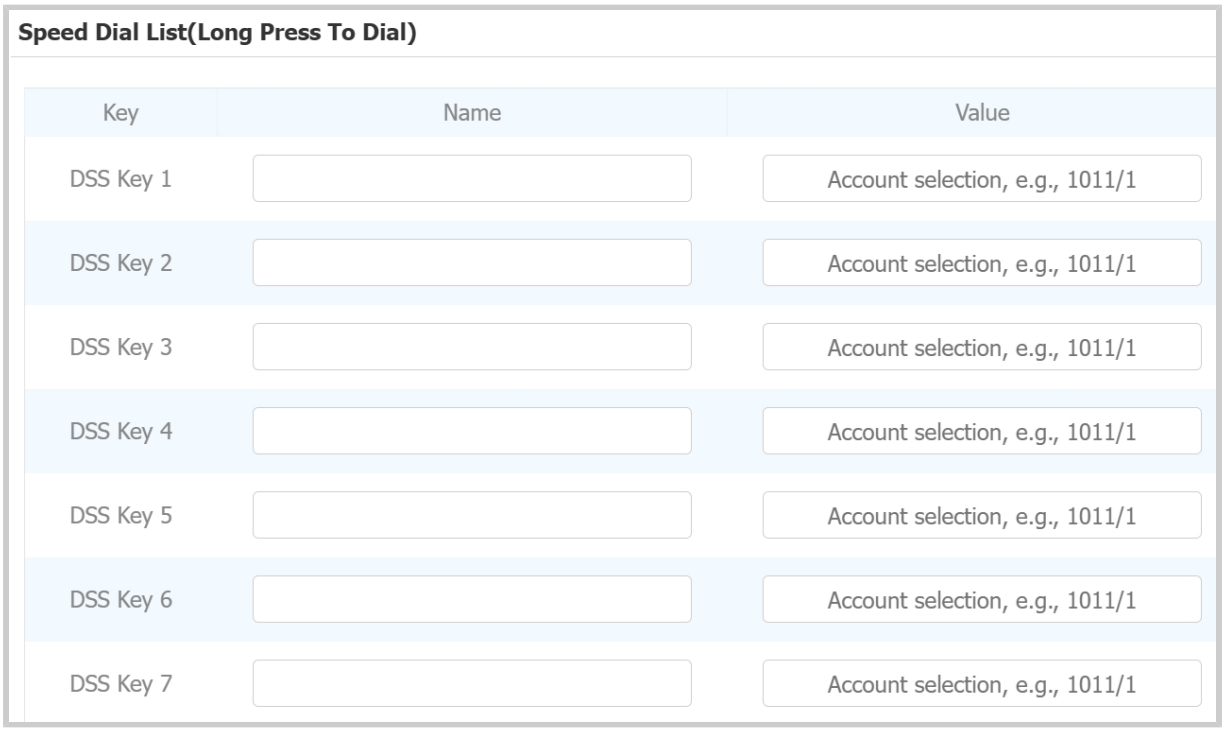
- **Key**:
  - By pressing the **Redial** key, the device will call the last called number even in standby mode.
  - By pressing the **Manager** key, the device will perform the action you select in the Type field.
- **Type**:
  - **NA**: Disable the key.
  - **Unlock**: When selected, specify the unlock method available in the Value field, including remote relay by HTTP and remote relay by HTTP command. To learn how to set up the unlock methods, please refer to the Door-opening Configuration chapter.

- **Action URL**: When selected, enter the HTTP URL command sent to other intercom devices. For example, you can enter a door-opening command to a door phone in the format: http://{*username*}:{*password*}@{*deviceIP*}/fcgi/OpenDoor?action=OpenDoor&DoorNum=1, like http://admin:Admin123@192.168.35.123/fcgi/OpenDoor?action=OpenDoor&DoorNum=1. Click here to learn how to choose the format.
- **Transfer**: When selected, enter a SIP number in the value field. When users press the Manager key during a call, the call will be transferred to the number.
- **Call Manager**: When selected, enter an IP or a SIP number. When users press the Manager key, a call will be made to the number.

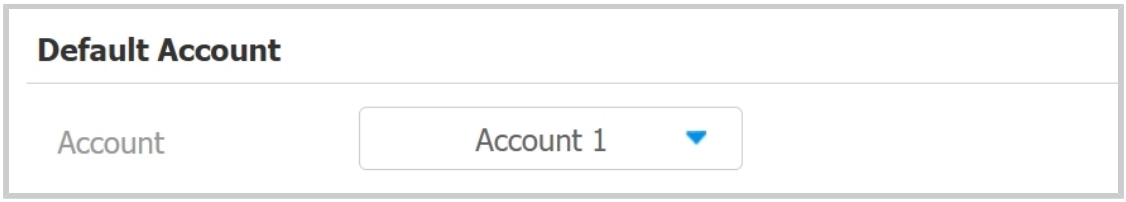
Speed Dial

Speed dial is a function that allows you to make speedy calls by long pressing the specific tabs without entering any dial numbers.

Set it up on the **Phone > Function Key** interface. The device supports up to 10 speed dial keys.



- **Key**: Each DDS Key corresponds to the numeric key on the device from 0-9.
- **Name**: Name the key. It supports up to 63 bytes.
- **Value**:
  - If you simply enter a SIP number such as 1013, the device will use the default SIP account to make the call. The default account can be chosen on the **Phone > Call Feature** interface.

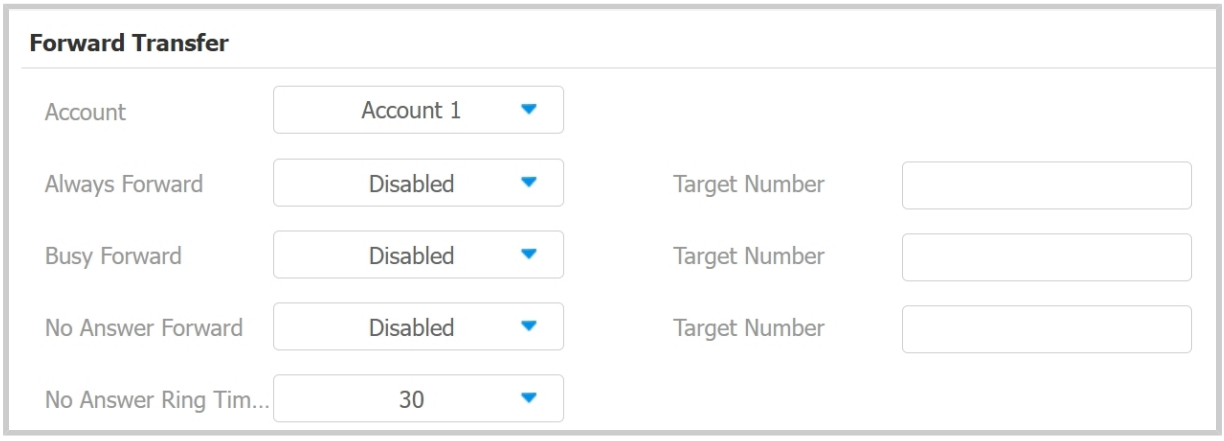


  - To make the call with Account 1, enter the value in **SIP Number/1** format such as 1011/1.
  - To make the call with Account 2, enter the value in **SIP Number/2** format such as 1012/2.

Call Forwarding

Call Forward is a feature that allows for transferring incoming calls to another number. Users can set up call forwarding according to different situations, such as always forwarding calls, forwarding calls when the indoor monitor is busy, or when it doesn't pick up the call.

Set it up on the **Phone > Call Feature** interface.

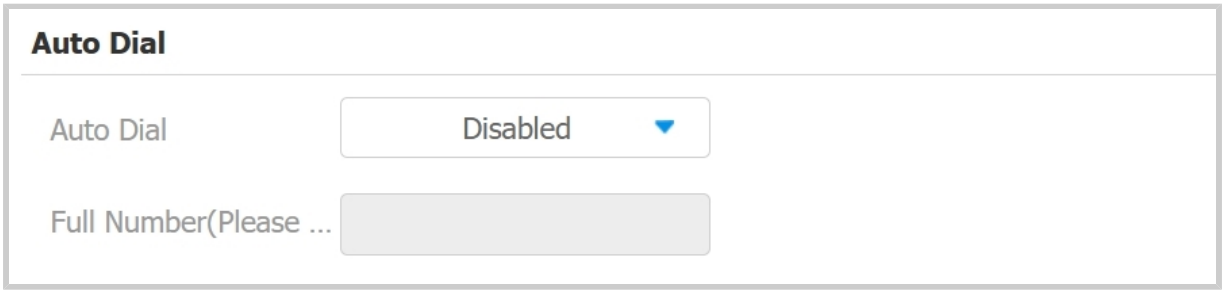


- **Account**: The account or direct IP call to implement the call forwarding feature.
- **Always Forward**: All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: Incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward**: Incoming calls will be forwarded to a specific number if the call is not picked up within the no-answer ring time.
- **Target Number**: Specify the forward number when Always Forward, Busy Forward, or No Answer Forward is enabled.
- **No Answer Ring Time(Sec)**: The time ranges from 0-120 seconds. This option is available for No Answer Forward.

Pick up the Handle to Call

You can set a designated number to be called when picking up the handle. This saves the effort of entering numbers on the main unit.

To set it up, go to the **Contacts > Local Contacts** interface.



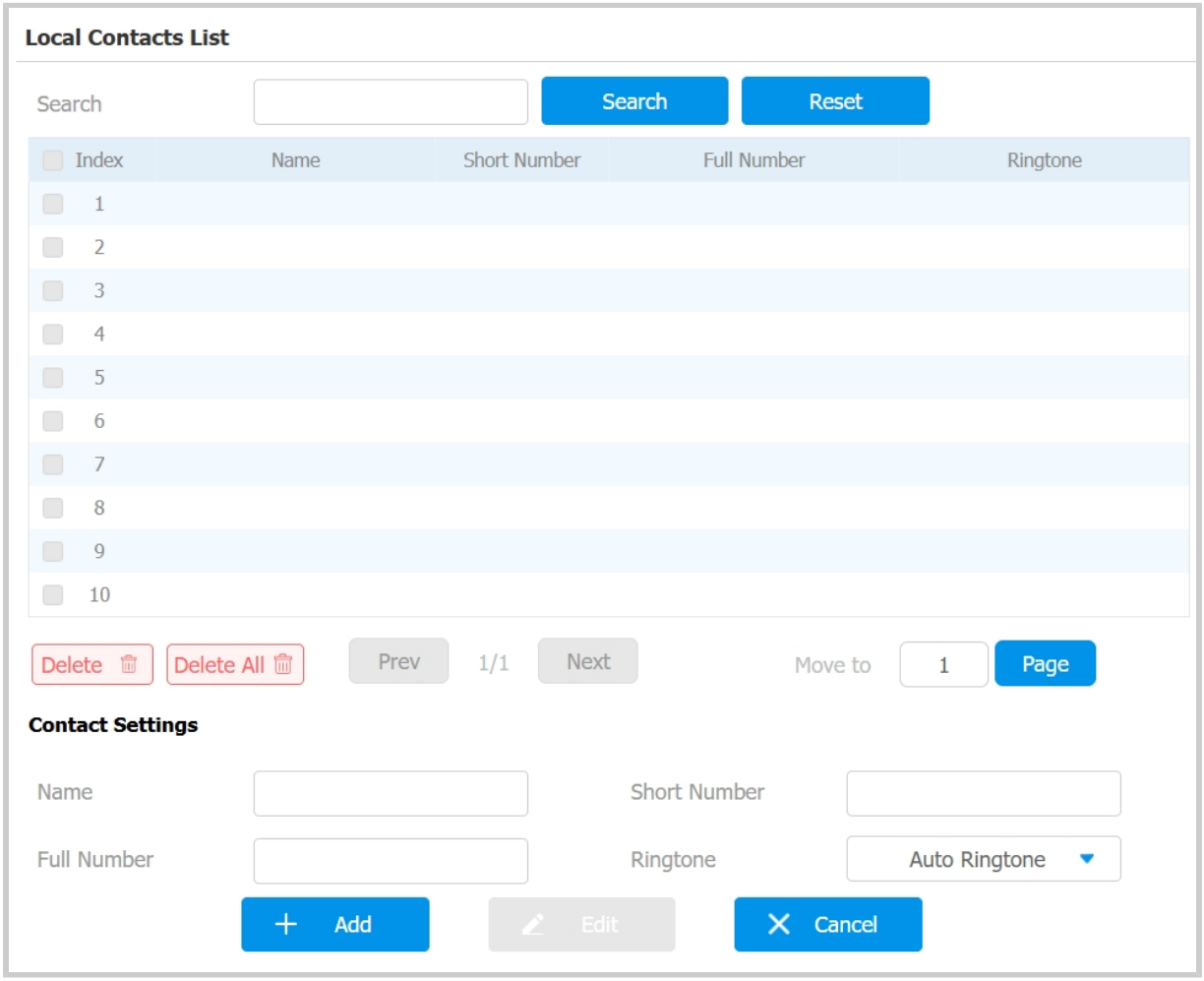
- **Auto Dial**: It is disabled by default.
- **Full Number**: Enter the target IP or SIP number.

Contacts Management

Add Local Contacts

You can add, edit, and search local contacts on the device's web interface. To add contacts, go to **Contacts > Local Contacts > Local Contacts List** interface. Enter the contact information and click +Add.

The maximum number of contacts is 500.



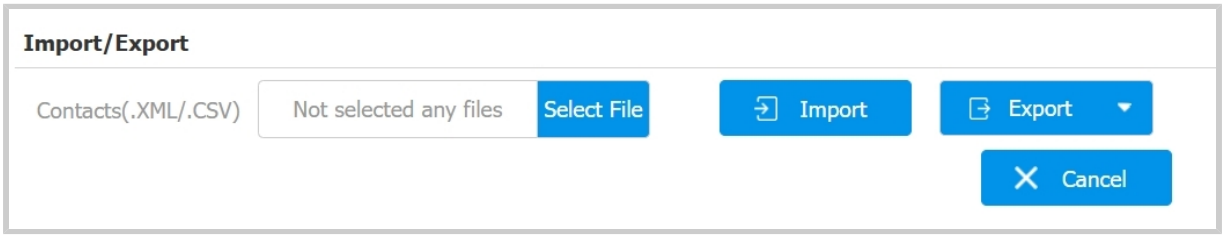
- **Name**: The contact's name to distinguish it from others.
- **Short Number**: The short number replaces the SIP or IP number. It should be within 5 digits.

- **Full Number**: The SIP or IP number of the contact.
- **Ringtone**: The phone ringtone for incoming calls.

Import/Export Contacts

You can easily import and export contacts for quick management.

Set it up on the **Contacts > Local Contacts** interface. The export/import file is in XML or CSV format.



Audio Codec Configuration

The device supports four types of codec (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each 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.

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



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

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

Access Control Configuration

Remote Relay

The remote relay refers to the relay of another intercom, such as a door phone. During calls, users can enter a DTMF code or press the Unlock tab to unlock the door lock connected to the door phone.

Set it up on the **Phone > Relay** interface.



- **DTMF Code**: Define the DTMF code within the range(0-9 and *,#) for the remote relay.

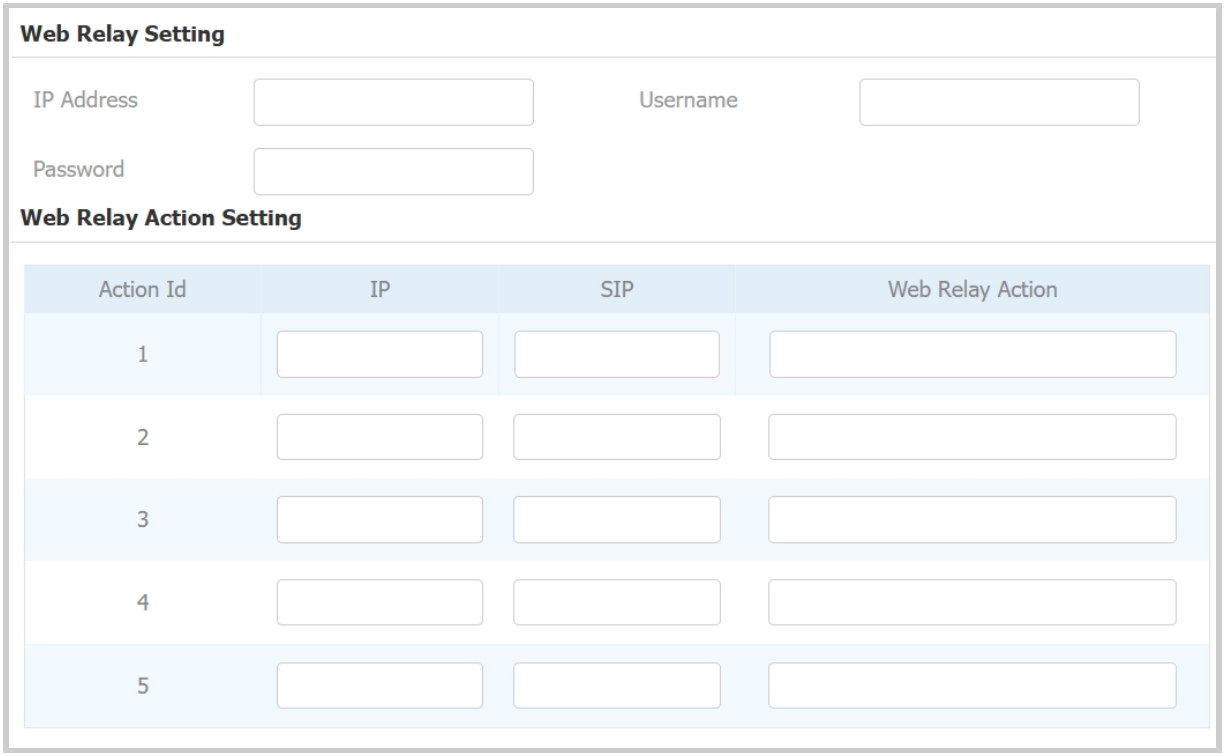
Web Relay

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.

Set up web relay on the **Phone > Relay** interface.



- **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.
- **IP/SIP**: The relay extension information, which can be an IP address or SIP account 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. This setting is optional.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions.

> **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.

Door-opening Configuration

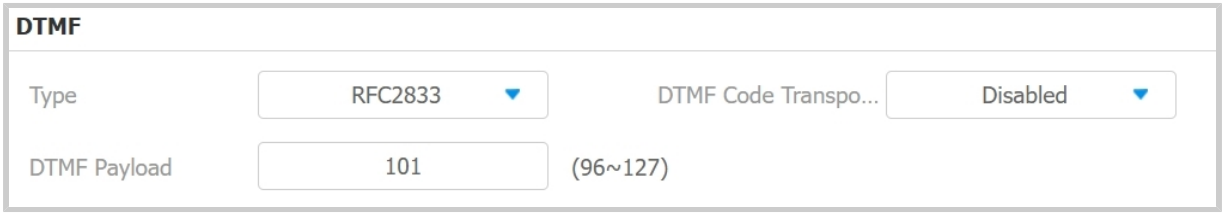
Unlock by DTMF Code

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.

Set up DTMF codes for remote relays on the **Phone > Relay** interface.



To configure the DTMF code transport format, navigate to the web **Account > Advanced** interface.



- **Type**: Select from the provided options.

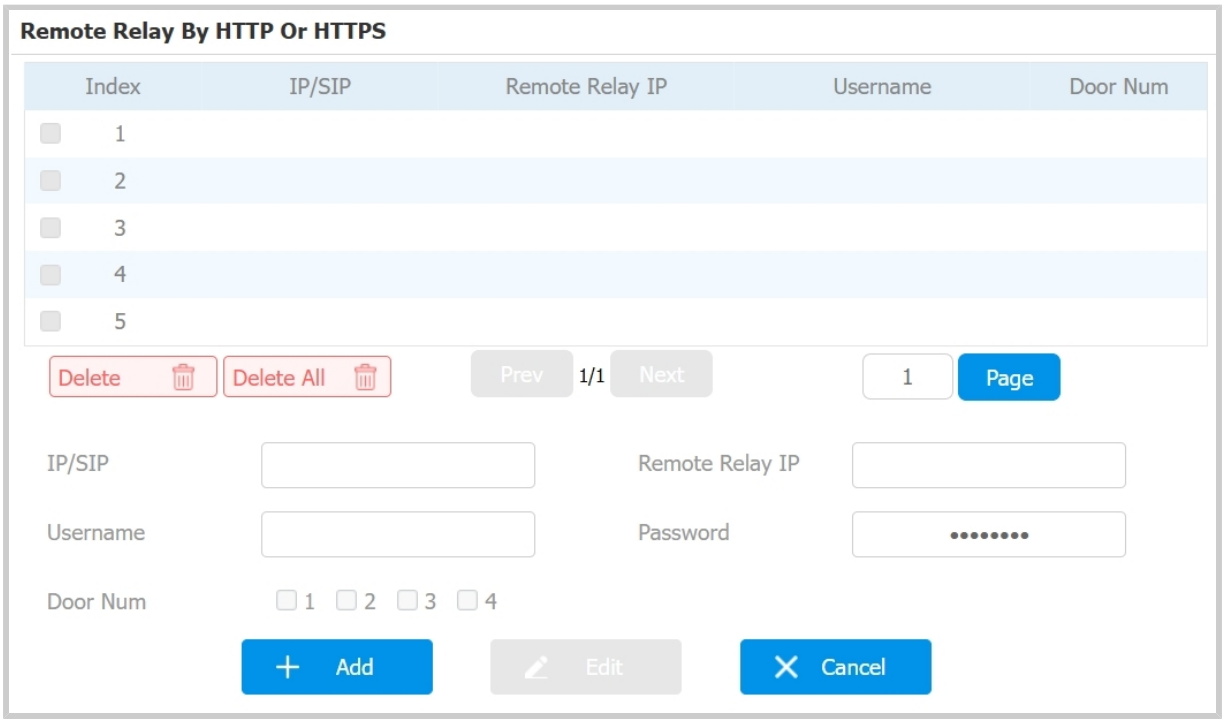
- **DTMF Code Transport Format**: There are four options: Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via signaling, while other transport format does it via RTP audio packet transmission. Select the DTMF transferring format according to the third-party device.
- **DTMF Payload**: It is for data transmission identification ranging from 96-127.

> **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.

Unlock via 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 **Phone > Relay** interface.

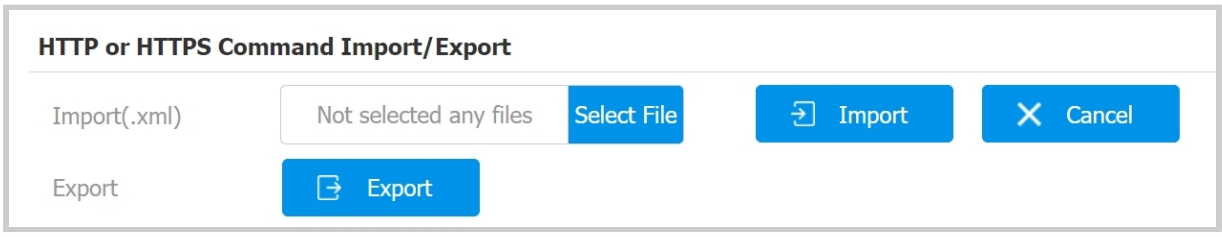


- **IP/SIP**: Specify the IP or SIP number of the door phone.
- **Remote Relay IP**: Enter the door phone's IP.
- **Username**: Enter the username the same as that configured on the door phone's web interface.
- **Password**: Enter the password the same as that configured on the door phone's web interface.
- **Door Num**: Specify the door to be opened.

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

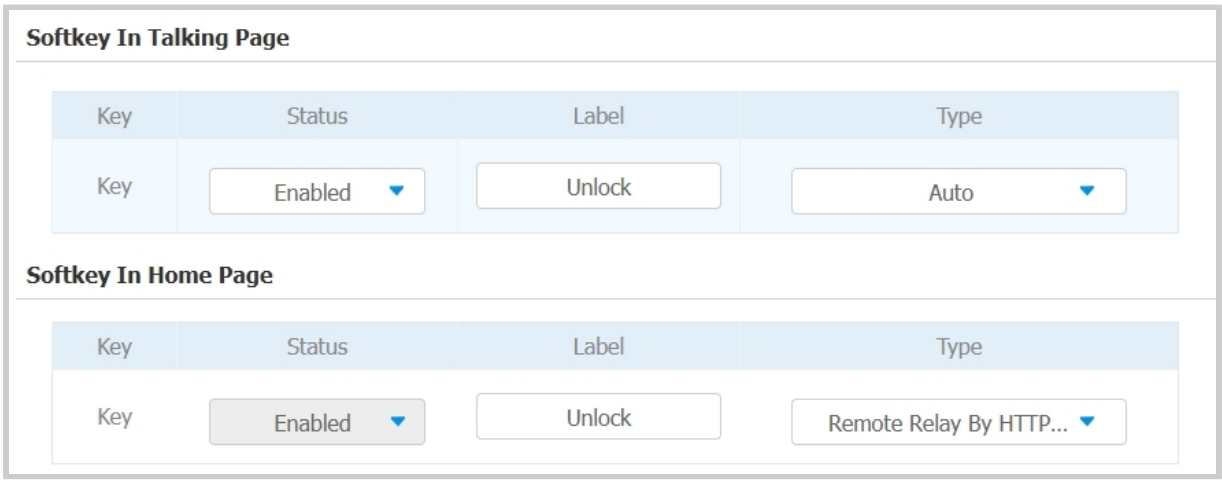
HTTP or HTTPS Command Import/Export

You can import and export HTTP or HTTPS commands on the device **Phone > Relay** interface.



Unlock Key Setup

You can set up the unlock key on the device's main unit on the **Phone > Relay** interface.



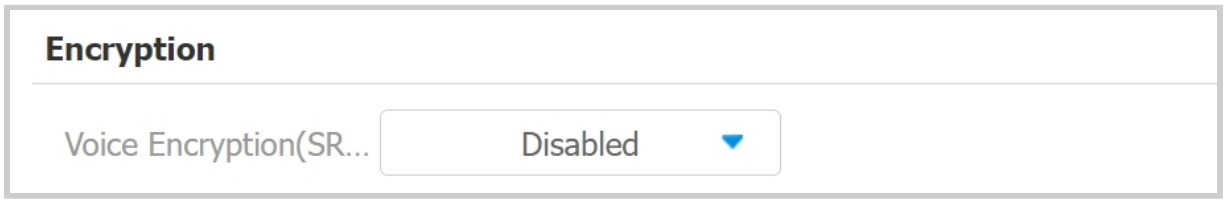
- **Softkey in Talking Page**: Press the key to open the door during a call.
- **Softkey in Home Page**: Press the key to open the door when the device is in standby mode.
- **Status**: The key is enabled by default.
- **Type**: Select the unlock type based on the actual setup.

Security

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 **Account > Advanced** interface.



- **Voice Encryption**:
  - **Disabled**: The call will not be encrypted.
  - **SRTP(Compulsory)**: All audio signals(technically speaking it is RTP streams) will be encrypted to improve security.
  - **SRTP(Optional)**: Encrypt the voice from the caller. If the caller also enables SRTP, the voice signals will also be encrypted.
  - **ZRTP(Optional)**: The protocol that the two parties use to negotiate the SRTP session key.

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

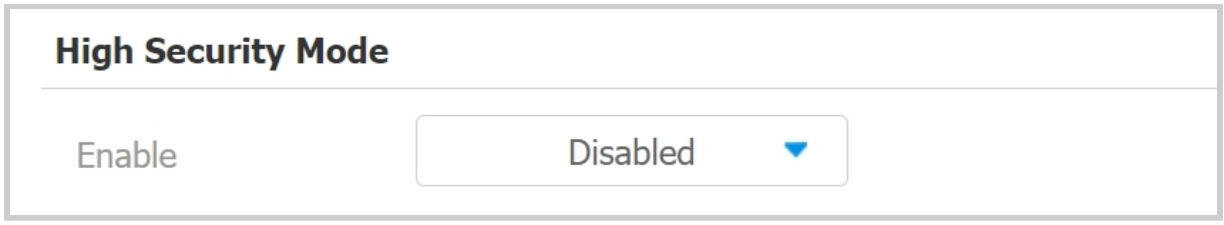
Set it up on the web **Security > Basic** interface.



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/disable the mode on the **Security > Basic** 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.

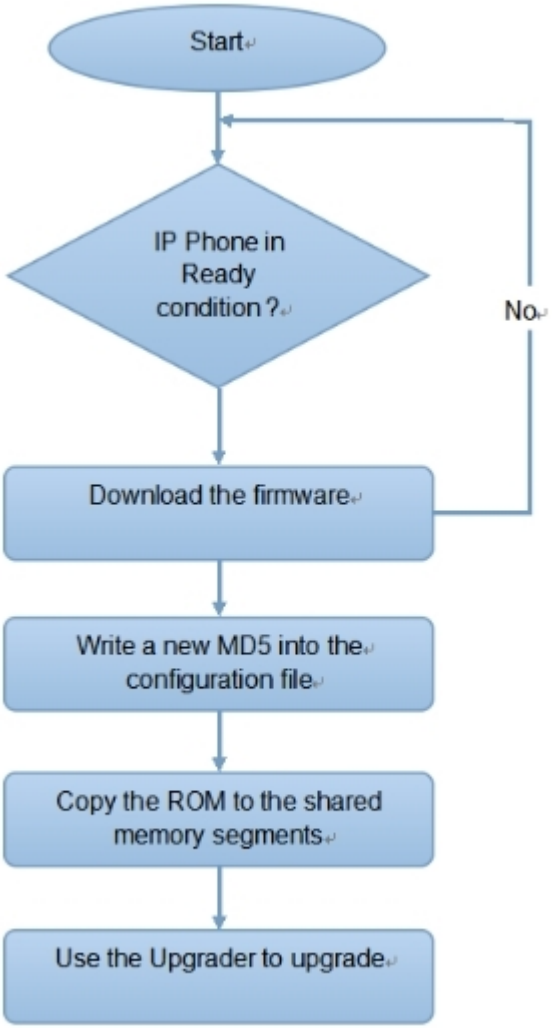
Auto-provisioning via Configuration File

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:



Introduction to the 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

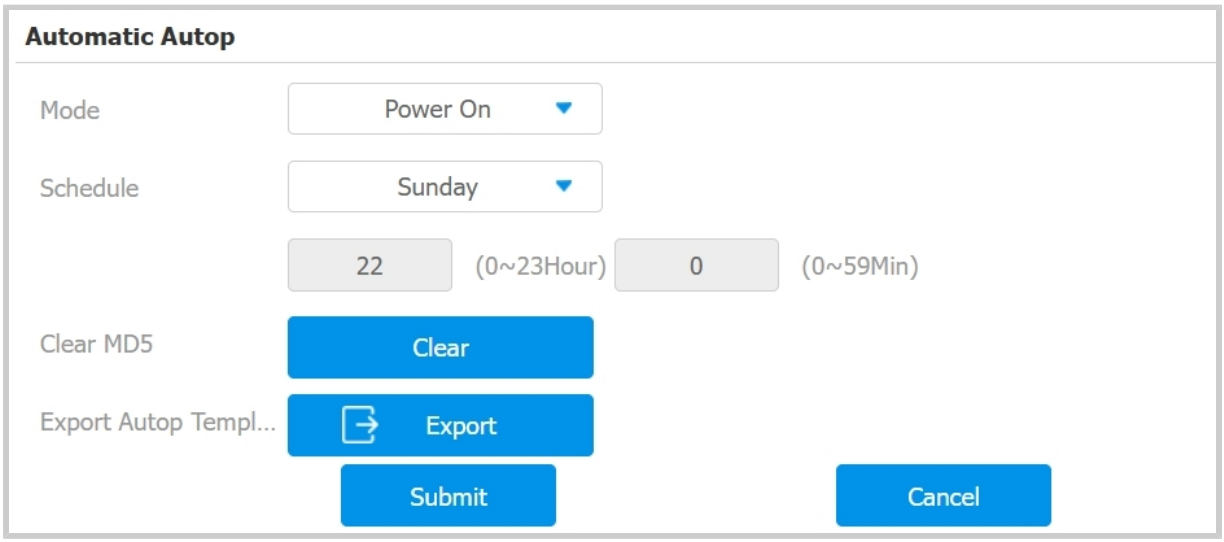
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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 up the schedule, go to the web **Upgrade > Advanced > Automatic Autop** interface.

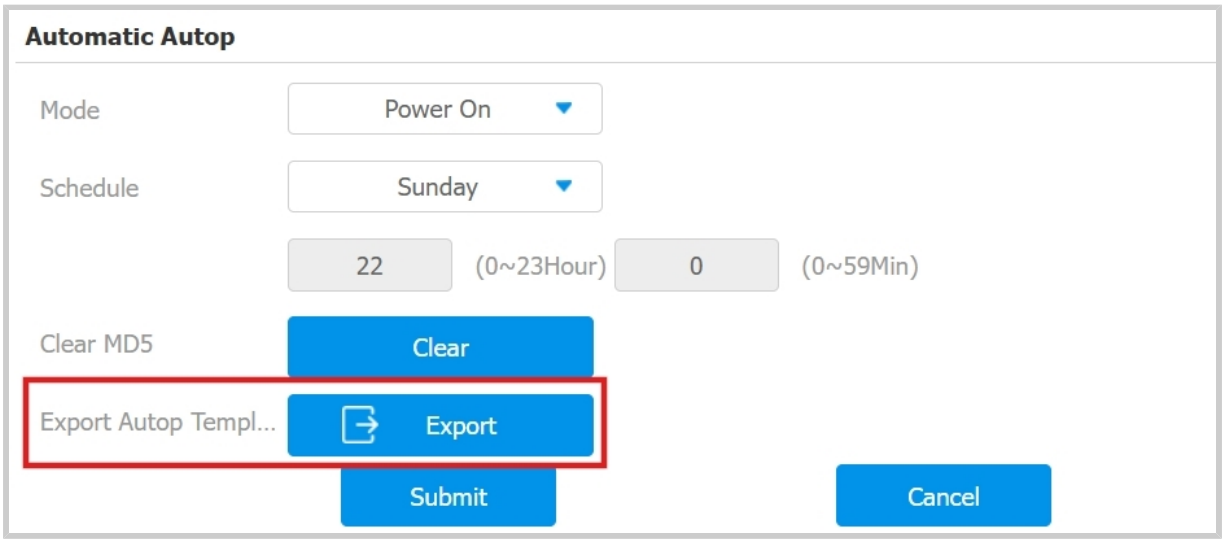


- Mode:
  - Power On: The device will perform Autop every time it boots up.
  - Repeatedly: The device will perform Autop according to the schedule you set up.
  - Power On + Repeatedly: Combine Power On mode and Repeatedly mode that will enable the device to perform Autop every time it boots up or according to the schedule.
  - Hourly Repeat: The device will perform Autop every hour.

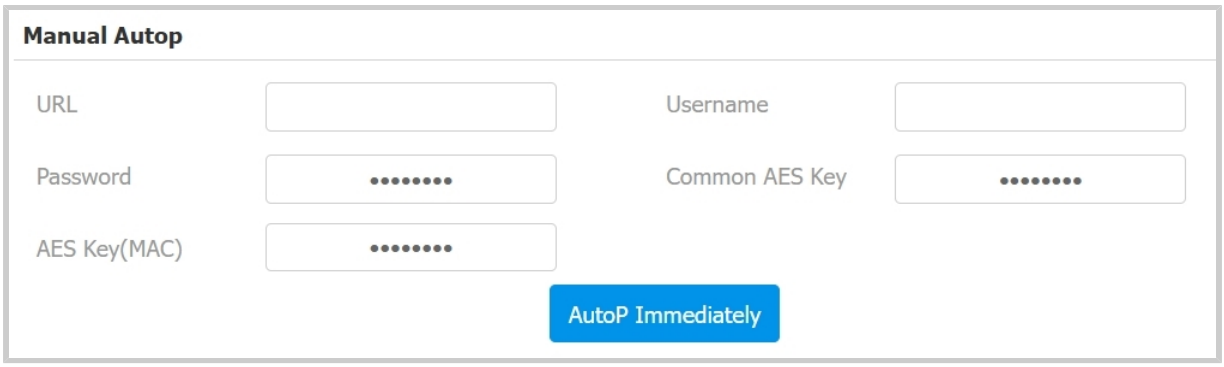
Static Provisioning

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 download the template, go to the **Upgrade > Advanced > Automatic Autop** interface.



To set up the server, go to the **Upgrade > Advanced > Manual Autop** interface.



- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server needs a username to be accessed.
- **Password**: Enter the password if the server needs a password to be accessed.
- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop 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

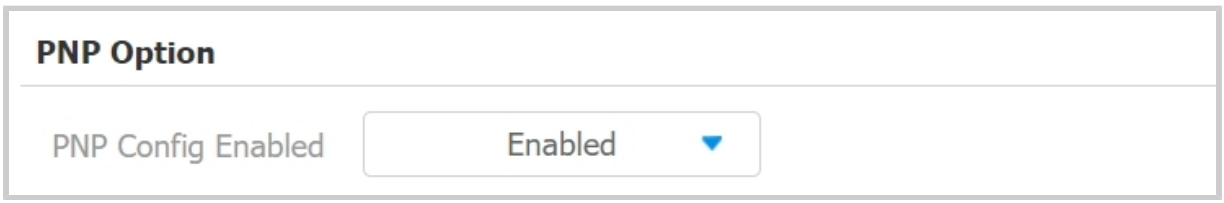
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

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.

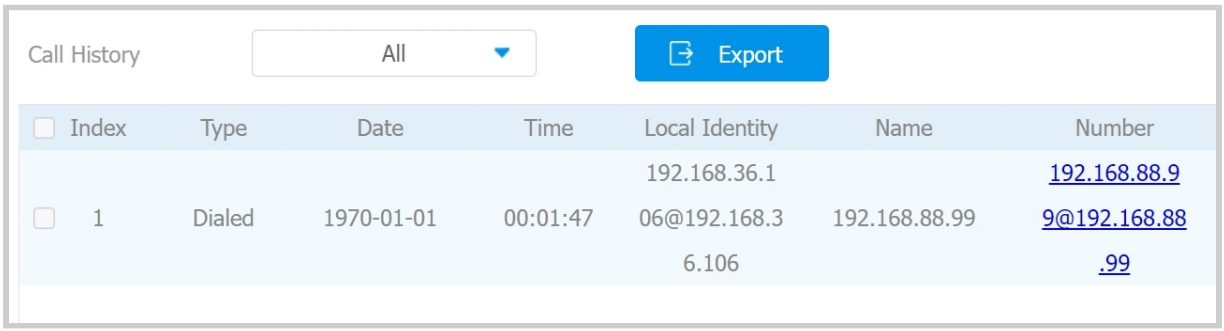
Enable it on the web **Upgrade > Advanced** interface.



Call 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.

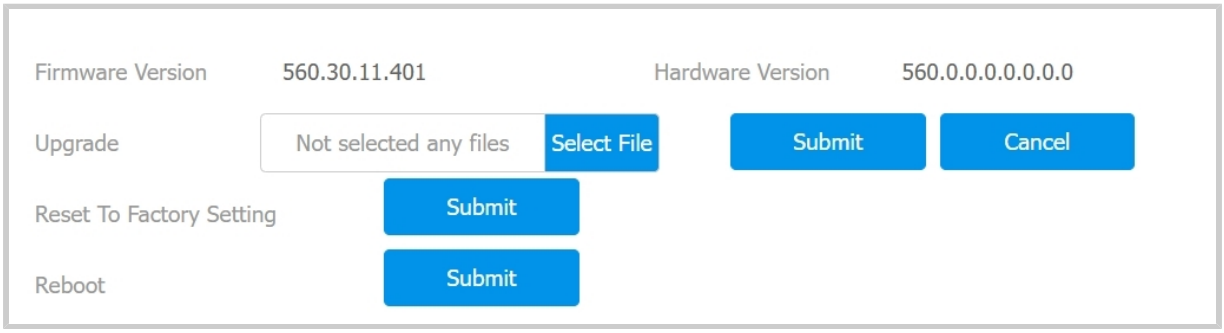
Check call logs on the **Contacts > Call Log** interface. It can display up to 100 logs.



- **Call History**: There are five types of call history, All, Dialed, Received, Missed, and Forwarded.
- **Local Identity**: Display the device's SIP account or IP number that receives incoming calls.
- **Export**: Click to export the call logs.

Firmware Upgrade

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



Note

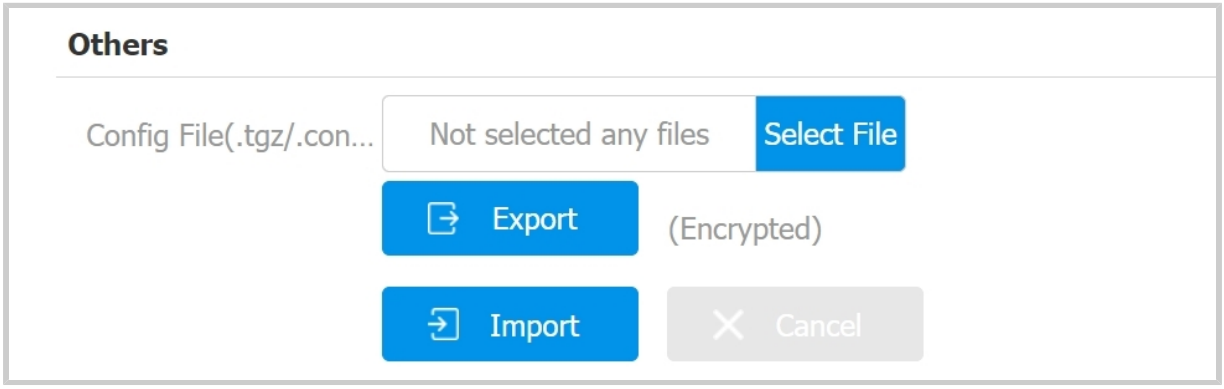
The file uploaded should be in **.rom** format.

Backup

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

Go to **Upgrade > Advanced** interface.

The import file should be in TGZ, CONF, or CFG format.

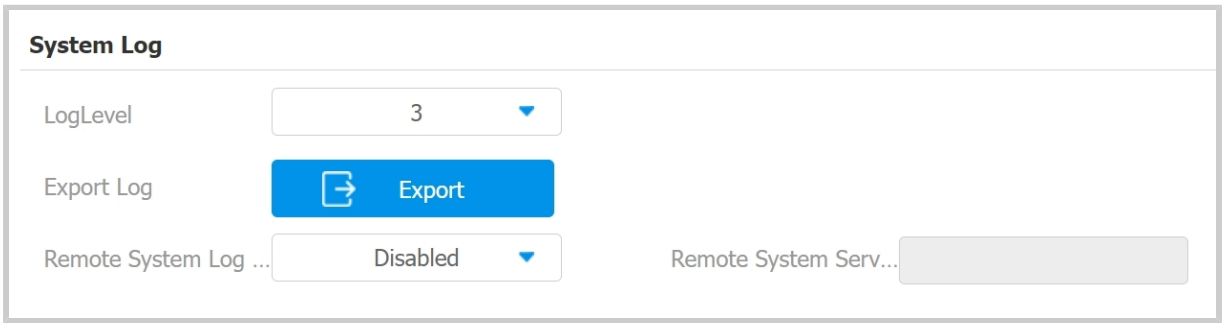


Debug

System Log for Debugging

System logs can be used for debugging purposes.

Set it up on the **Upgrade > Diagnosis** interface.

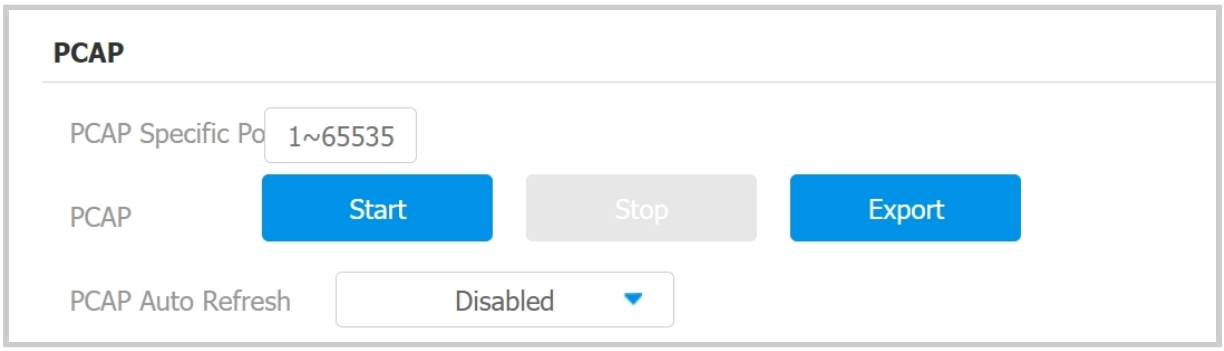


- **Log Level**: Log level ranges from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Server**: Enter the remote server address to receive the system log and it will be provided by Akuvox technical support.

PCAP for Debugging

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 > Diagnosis** interface.



- **PCAP Specific Port**: Select the specific port 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.
- **PCAP Auto Refresh**: When enabled, the PCAP will continue to capture data packets even after the data packets reach 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets reach the maximum capturing capacity of 1MB.

User Agent

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

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

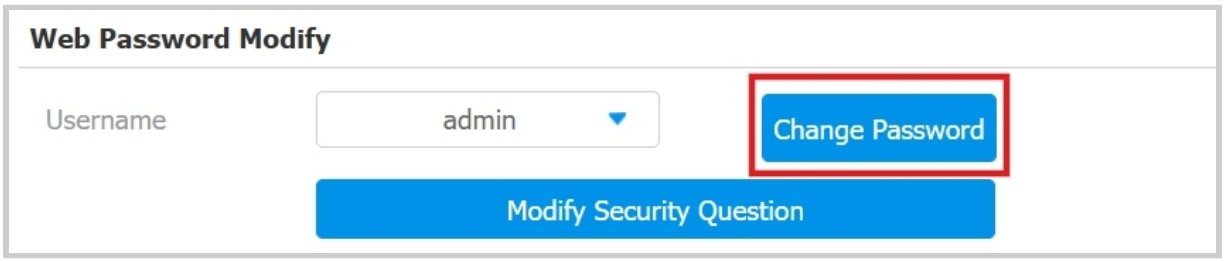


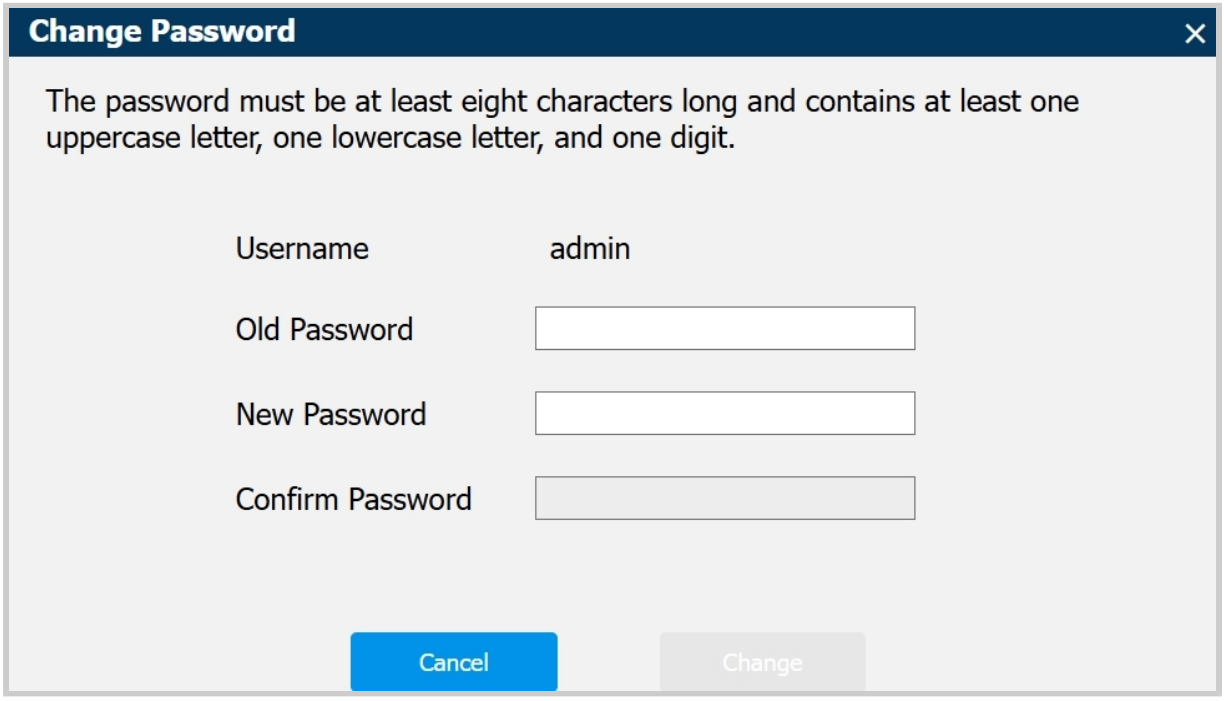
Password Modification

Modify Device Web Interface Password

The device web password is used to access the web settings. You can modify it on the **Security > Basic** interface.

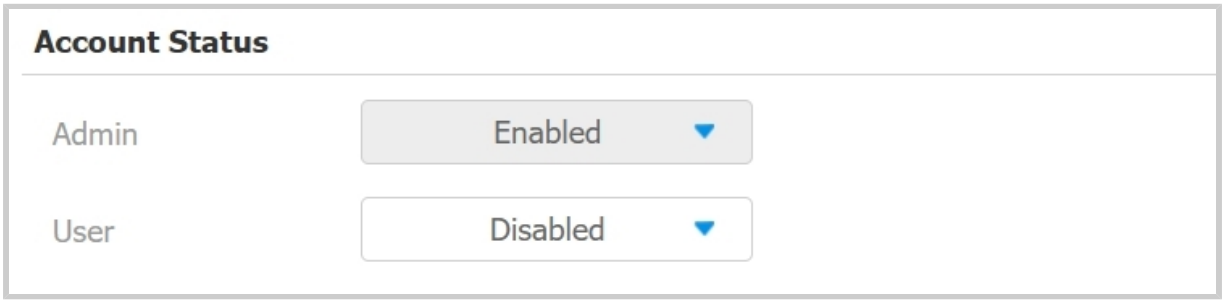
Select **admin** for the administrator account and **user** for the user account. Click the **Change Password**.





> **Note**
>
> When the device's version is 560.30.11.509 or higher, it supports web password containing special characters . , ; : " ? ! - _ ( ) [ ] { } + * / < > ^ ~ | $ @ # ` " ñ Ñ á é í ó ú ü ¡ ¿ º ª ç € « » .

You can enable or disable the user account on the **Security > Basic** interface. The default password for the user account is **user**.

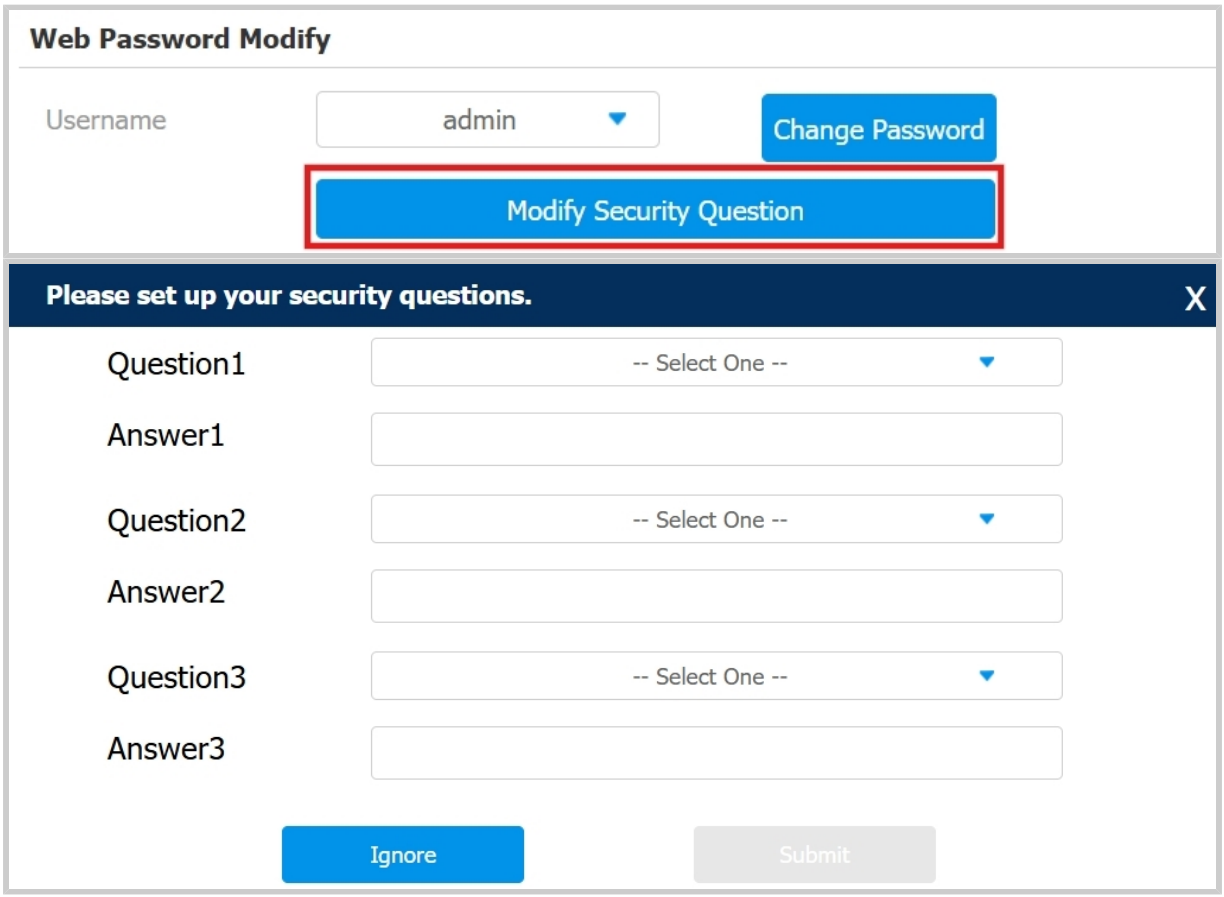


Modify Security Questions

Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

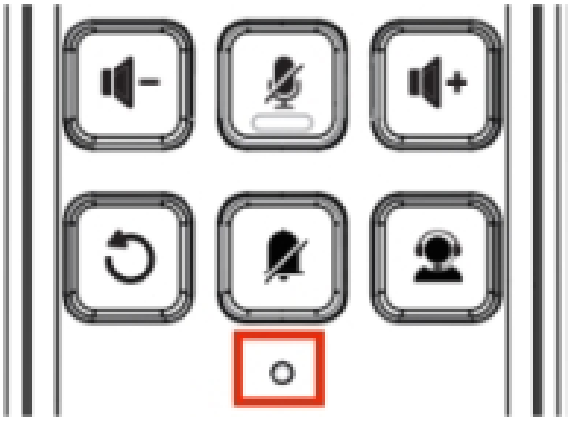
Set it up on the **Security > Basic** interface.


Web Password Modify
Username
admin
Change Password
Modify Security Question
Please set up your security questions.
X
Question1
-- Select One --
Answer1
Question2
-- Select One --
Answer2
Question3
-- Select One --
Answer3
Ignore
Submit

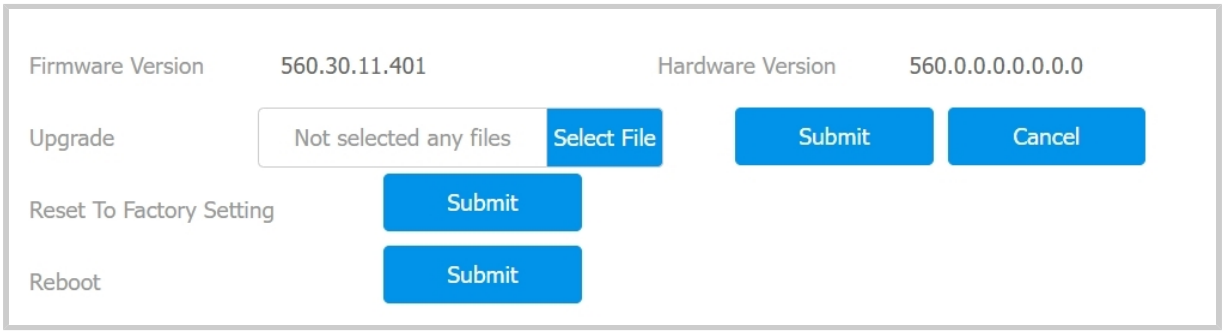
System Reboot & Reset

Reboot

You can reboot the device by inserting a pin into the reset hole and holding it for three seconds.

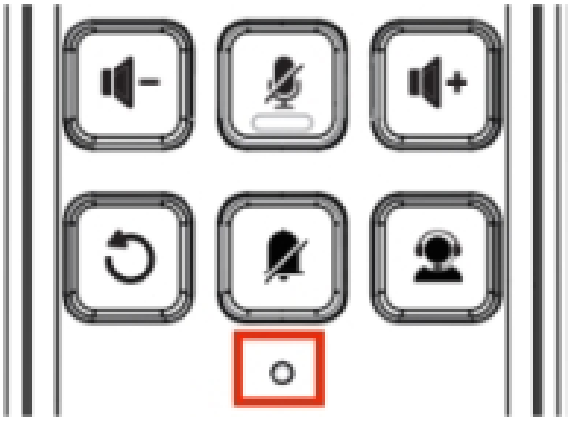


You can also reboot it on the **Upgrade > Basic** interface.



Reset

You can reset the device by inserting a pin into the reset hole and holding it for about 5 seconds.



You can also reset it on the **Upgrade > Basic** interface.

