About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



E20
DOOR PHONE
Administrator Guide

Thank you for choosing Akuvox E20S door phone. This manual is for administrators who need to configure the door phone.

This manual applies to 120.1.1.25 and it provides an overview of all functions and features of E20S.

Product Overview

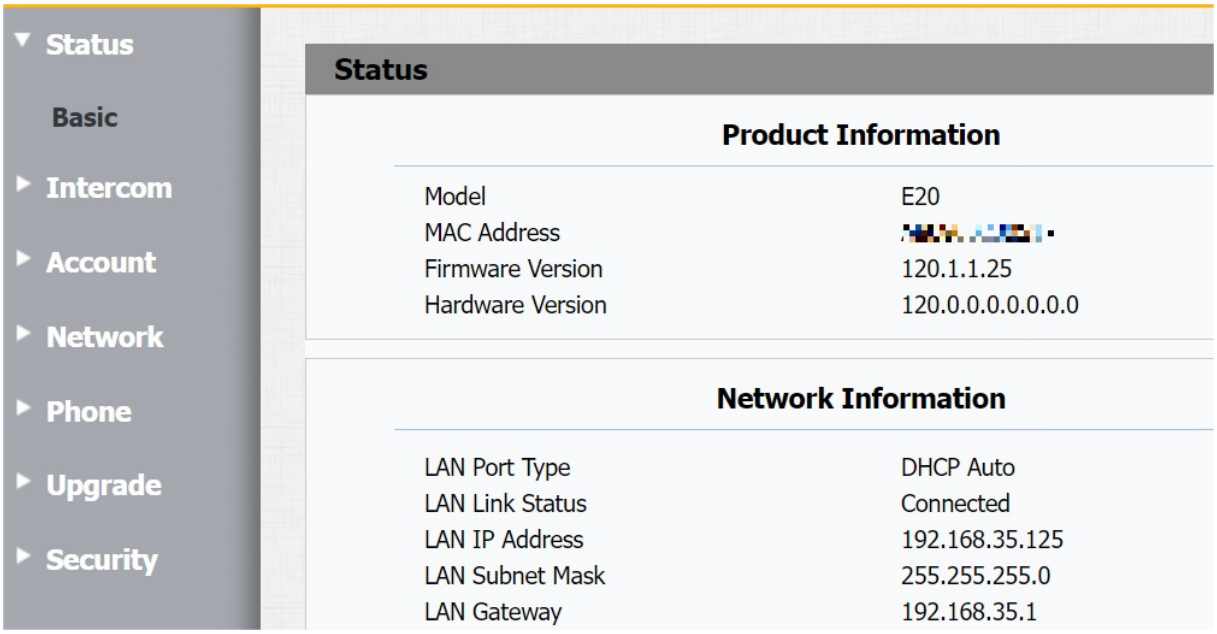
Akuvox E20S door phones are SIP-compliant door phones. They can be used with Akuvox indoor monitors and SamrtPlus app, making door access convenient and the remote control possible.

Model Specification

Model	E20S
Camera	×
Speaker	1
Microphone	1
Relay In	x
Relay Out	x
RS485	x
Card Reader	x
System	Linux

Configuration Menu Overview

- **Status**: This section gives basic information about product, network, and account.
- **Account**: This section concerns SIP configuration, proxy server, transport protocol type, audio&video codec, DTMF, session timer, NAT,etc.
- **Network**: This section is mainly about DHCP&Static IP setting, PC port setting, RTP, VLAN, VPN, TR069, etc.
- **Phone**: This section covers device display settings, sounds and ringtones, various call features, multicast and more.
- **Phonebook**: All the call histories are displayed in this section.
- **Upgrade**: This section covers firmware upgrade, device reset&reboot, configuration file auto-provisioning, PCAP, and more.
- **Security**: This section includes web password reset, session time out, web server certificate and client certificate.



Color Codes of Indicator Light

E20S door phone has an indicator light installed visible on the left side of the push button. The light colors vary by the state the device is currently in.

Color	LED Light Status	Color Code
Blue	A solid blue light	Normal status
		A call ends
		Broadcasting IP address
	A blinking blue light	Calling out
Green	A solid green light	During a call
Red	A slowly blinking red light	Failed to obtain IP address
	A rapidly blinking red light	Failed to update the device
Red&Yellow	An alternately flashing red and yellow light	During an updating process
Green to Red	From a solid green light to a blinking red light	Booting up the device
White, Green, then White	First, a white light flashes. Next, a green light is on for 3 seconds. Then switch to a solid white light.	Factor Resetting the device
White,Green, White, Red, finally Green	First, a white light flashes, Next changes to a green light that will be on for 3 seconds. Then, a solid white light displays. Followed by a red light that will stay on for 2 seconds, Lastly, a green light turns on	Failed to factor reset the device

Access Device Settings

E20S door phone can be configured on the device web interface whose address is https://device_IP_address.

Obtain Device IP Address

IP Broadcast Automatically

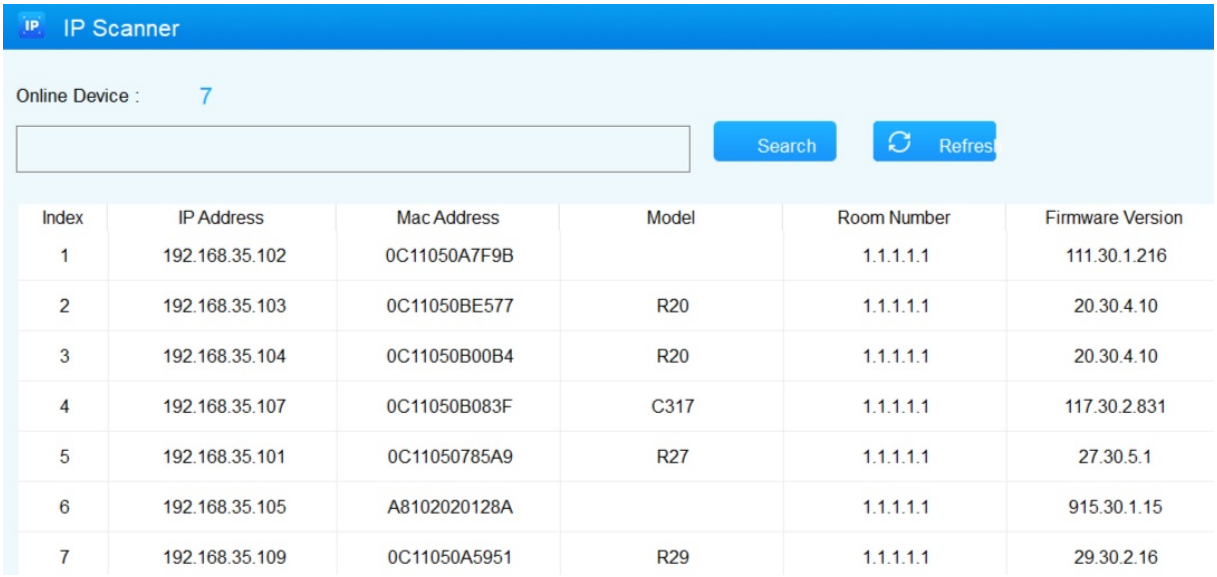
The device will automatically broadcast its IP address three times once it is powered on and connected to the network.

To disable the auto-IP-broadcast, log into the web interface and go to **Phone > Preference > IP Broadcast**.



Use IP Scanner

You can use the IP Scanner software to check the device IP on the same local network.



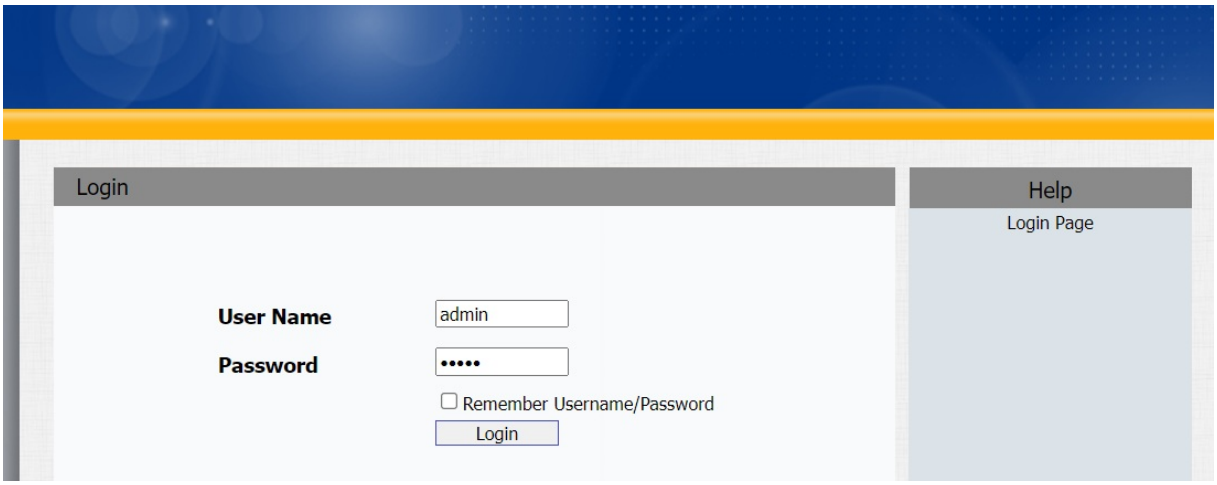
Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C11050A7F9B		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C11050BE577	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C11050B00B4	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C11050B083F	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101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

Note

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

Log in to the Device Setting Web Interface

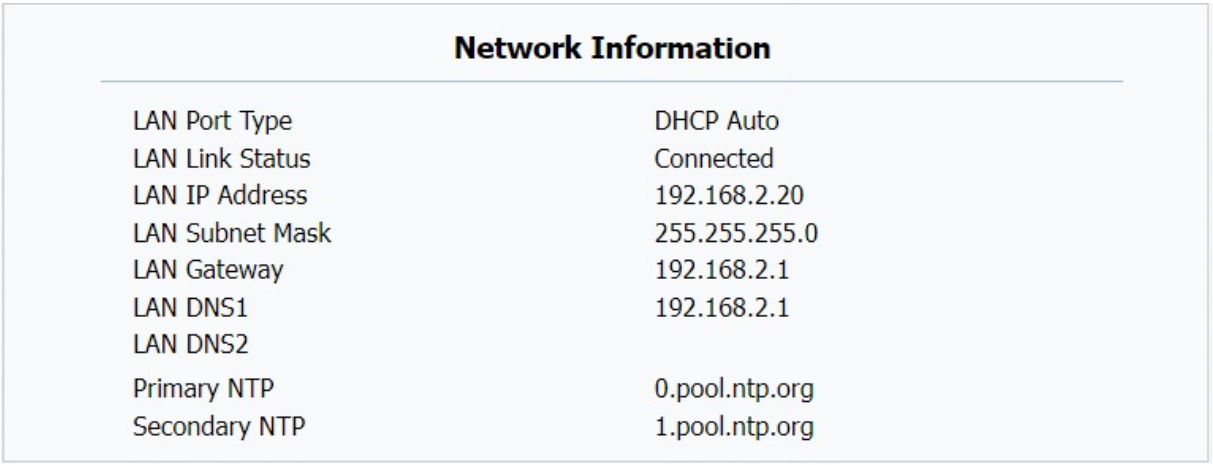
To log in to device web interface where you can configure and change parameters, enter the device IP address on the browser. The default user name and password are both **admin**.



Network Settings

Network Information

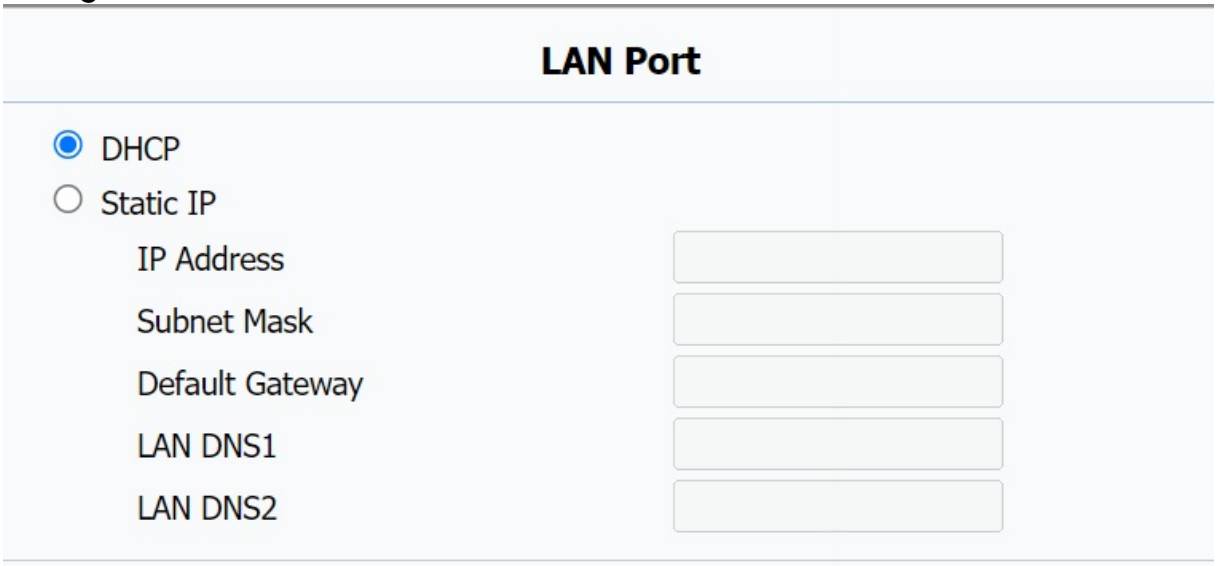
To check the current network information, go to **Status > Basic > Network** Information.



Device Network Configuration

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

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



Parameters Set-up:

- **DHCP**: Click on DHCP to enable this mode. DHCP mode is the default network connection. If the mode is turned on, then the device will be assigned by the DHCP server with IP address, subnet mask, default gateway and DNS server address automatically.
- **Static IP**: Click on Static IP to enable this mode. If selected, you have to configure the IP address, subnet mask, default gateway, and DNS servers address manually based on the actual network environment.
    - **IP Address**: Enter the IP Address.
    - **Subnet Mask**: Enter the subnet mask according to your actual network environment.
    - **Default Gateway**: Enter the correct gateway default gateway according to the IP address of the default gateway.
    - **LAN DNS1/DNS 2**: Enter preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. DNS1 server is the primary DNS server address while DNS2 is the alternative.

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.

To do so, go to **Network > Advanced > Local RTP**.



Parameters Set-up:

- **Max RTP Port**: Set the maximum end port that RTP stream can use. The default port is 12000.
- **Starting RTP Port**: Set the minimum start port that RTP stream

can use. The default port is 11800.

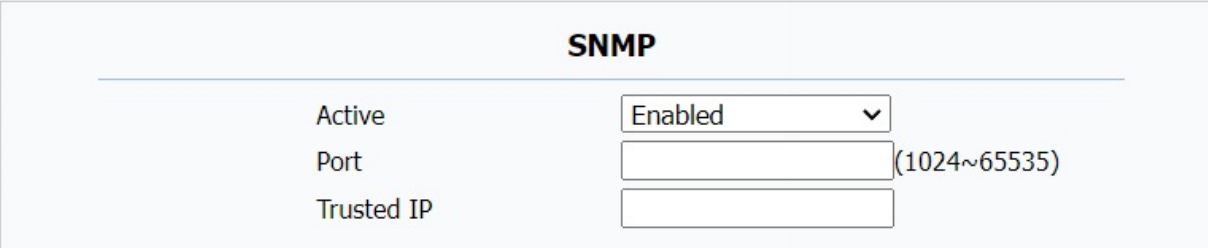
Note

- The max port value must always be 2 greater than the min one.

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 up SNMP, go to **Network > Advanced > SNMP**.



Parameters Set-up:

- **Port**: To configure SNMP server's port.
- **Trusted IP**: The IP address of the computer on which the MIB Browser tool is enabled.

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 up VLAN, go to **Network > Advanced > VLAN > LAN Port**.



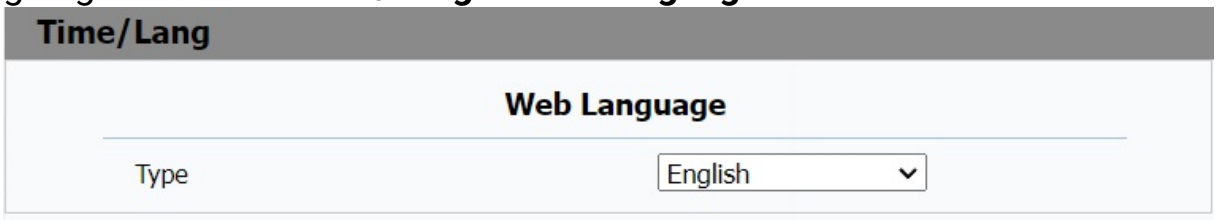
Parameters Set-up:

- **Active**: To enable or disable VLAN feature for designated port. The default option is Disable.
- **VID**: To configure VLAN ID for designated port.
- **Priority**: To select VLAN priority for designated port.

Language and Time Settings

Language Setting

You con set up the display language for the device web interface by going to **Phone > Time/Lang > Web Language**.



Parameters Set-up:

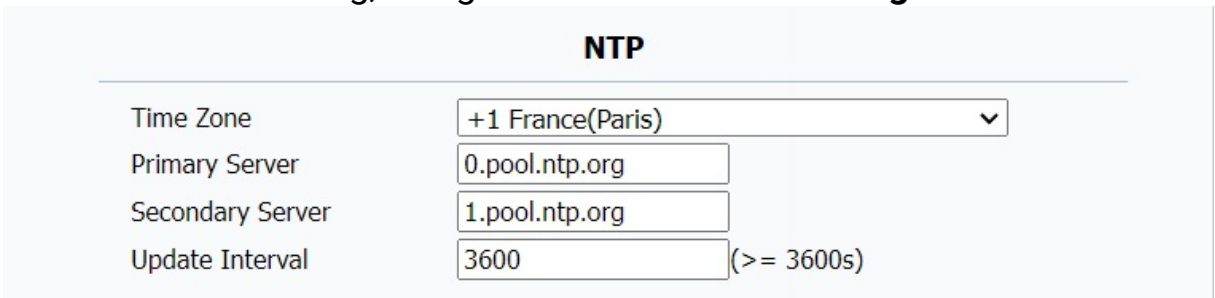
- **Type**: Choose a preferred web language. English is the default one.

Time Setting

Set up Standard 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.

To access this setting, navigate to **Phone > Time/Lang > NTP**.



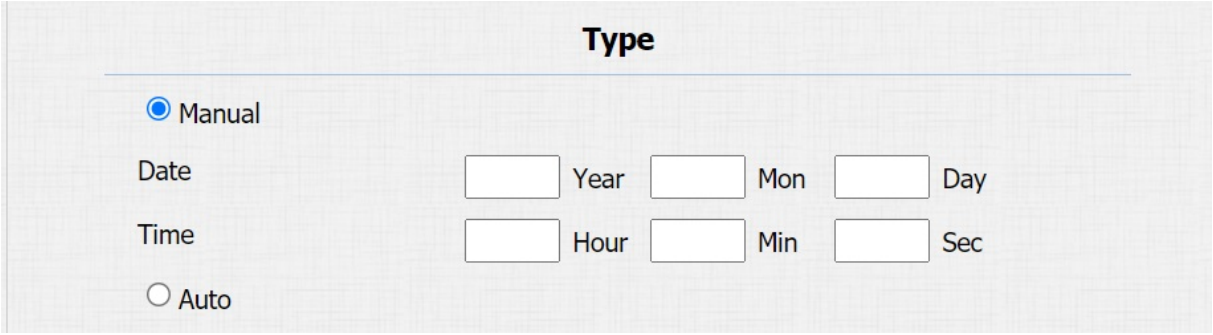
Parameters Set-up:

- **Time Zone**: Select the specific time zone depending on where the device is used and then press **Confirm** tab for the confirmation.

The default time zone is **GMT GMT+0.00**.

- **Primary/Secondary Server**: Enter the NTP server address. The secondary server will take effect when the primary server is invalid.
- **Update Interval**: To configure the interval between two consecutive NTP requests. The device will then automatically synchronize its time with the NTP server at this set intervals.

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



Sound Settings

Audio

Ringtone

To adjust the ringtone volume, go to **Phone > Preference > Ringtone Volume**. The volume level by default is 8.



System Volume

To set up the mic, speaker or ringback tone volumes, go to **Phone > Voice**.

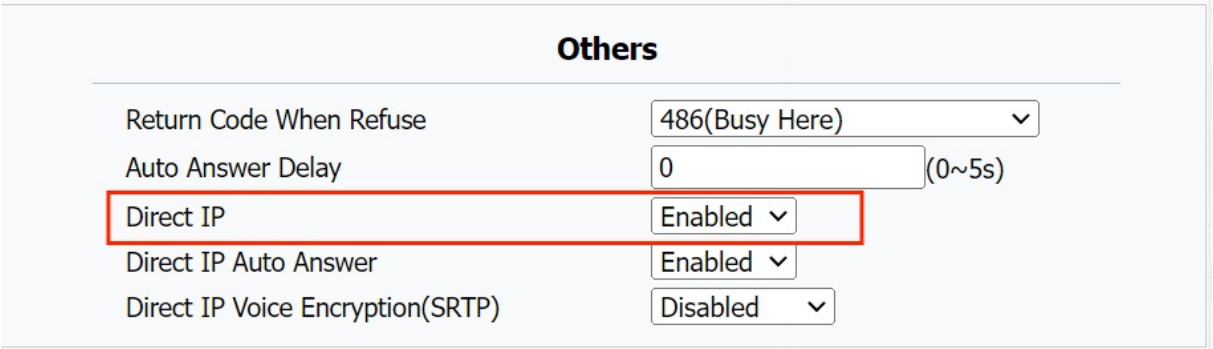


IP Call and SIP Call Configurations

IP Call

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.

To do so, go to **Phone > Call Feature > Others**.



SIP Call

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.

Go to **Account > Basic > SIP Account**. **Register Name, User Name**, and **Password** are obtained from SIP account administrator.



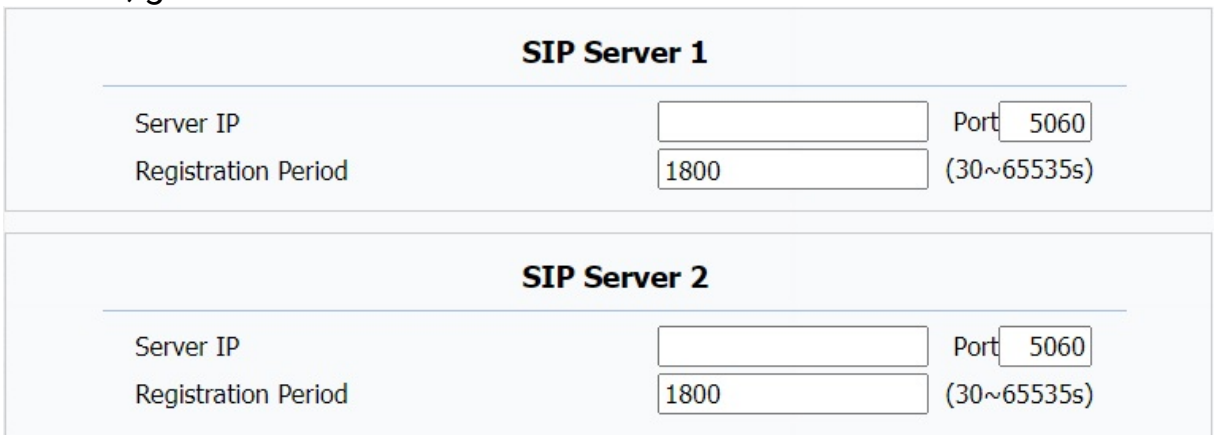
Parameters Set-up:

- **Status**: To see if the SIP account is registered or not.
- **Account**: Select the account (Account 1 only) to be configured.
- **Account Active**: To activate or deactivate the registered SIP account.
- **Display Label**: Optional. To configure the account label displayed on the screen.
- **Display Name**: Optional. To configure the account's name displayed on the called device.

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 primary(SIP Server 1) and secondary(SIP Server 2) SIP servers, go to **Account > Basic > SIP Server**.



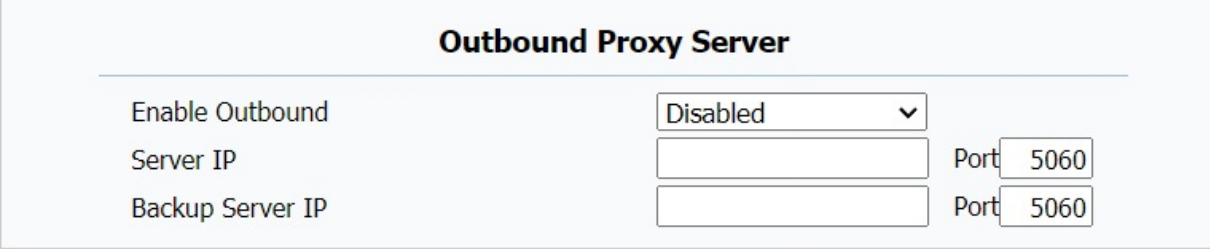
Parameter Set-up:

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

Configure Outbound Proxy Server

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

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



Parameters Set-up:

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

Configure Data Transmission Type

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 this up, go to **Account > Basic > Transport Type**.



Parameters Set-up:

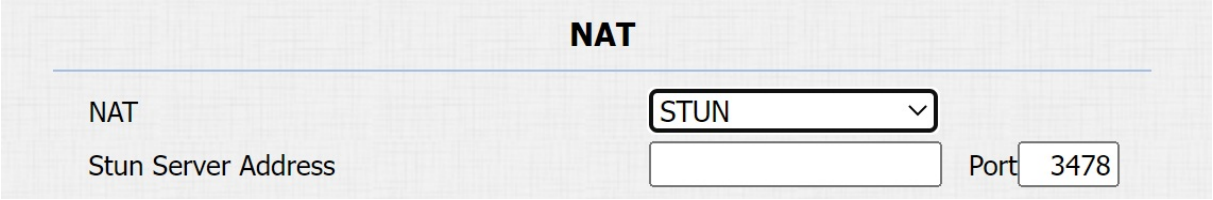
- **Transport Type**: To select from 4 SIP message transmission types.
- **UDP**: Select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: Select **TCP** for Reliable but less-efficient transport layer protocol.
- **TLS**: Select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: Select **DNS-SRV** to obtain DNS record for specifying the location of servers. And SRV not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

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 NAT, go to **Account > Basic > NAT**.

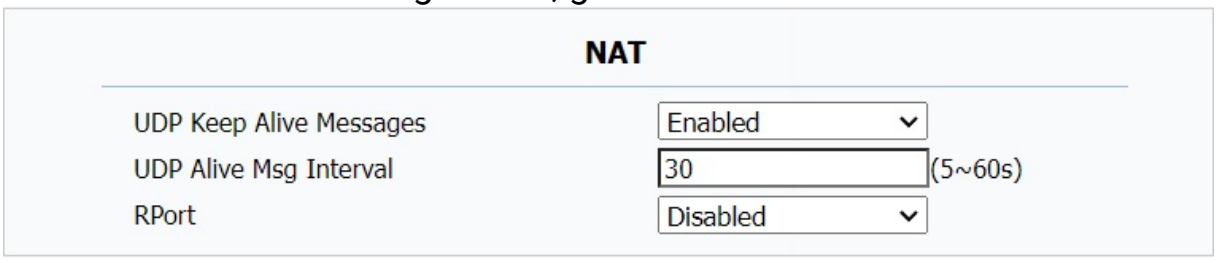


Parameters Set-up:

- **NAT**: To select STUN (short for Simple Traversal of UDP over NATS) to enable the function, then you need to install a NAT sever. The default is **Disable**.

- **Stun Server Address**: To enter the STUN server IP.
- Port: To enter the STUN server port. The default port is 3478.

To make advanced configuration, go to **Account > Advanced > NAT**.



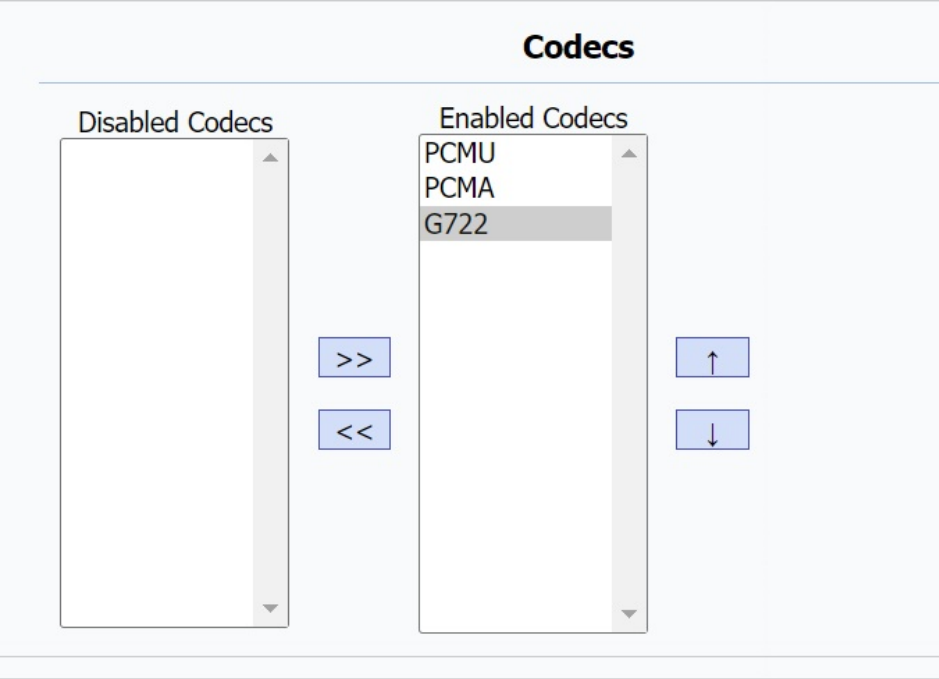
Parameters Set-up:

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

Audio Codec for SIP Call

The door phone supports three types of Codec (PCMU, PCMA, nd 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 make the configuration, go to **Account > Advanced > Codecs**.

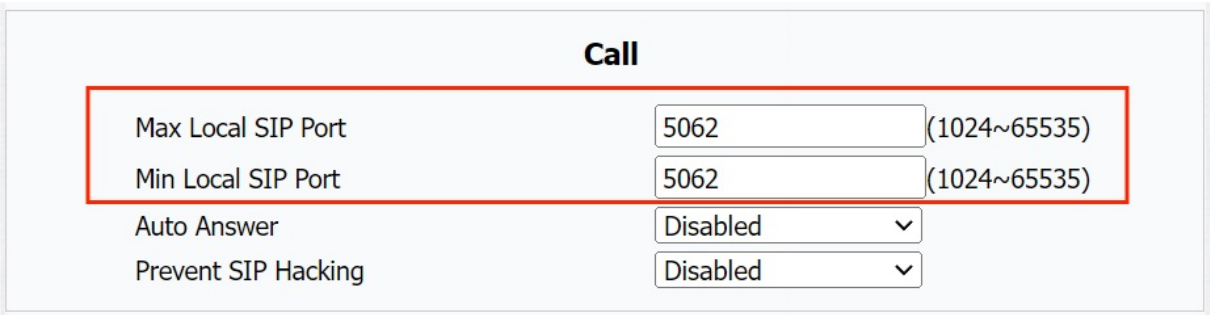


The following are the bandwidth consumption and sample rate of the 3 codec types.

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

Other SIP Call Settings

For other SIP call related settings, go to **Account > Advanced > Call**.



Parameters Set-up:

- **Max Local SIP Port**: To set the highest port number that can be used for SIP traffic on a device. The default port is 5062.

- **Min Local SIP Port**: To set the lowest port number that can be used for SIP traffic on a device. The default port is 5062.

Intercom Calling Features

Press Button to Make a Call

You can quickly make a call with the preset numbers by pressing the physical push button on E20S. When press the button, all the numbers added from the web interface are called simultaneously. Once any of the numbers receives the call and answers it, the system will automatically terminate the call to the other numbers.

To set up the feature, go to **Intercom > Basic > Push Button**.



Parameters Set-up:

- **Number 1-3**: The SIP number or IP address of devices. One box for one number.
- **Number 4/5**: You can type in 2 numbers in this box and you have to separate them with a semicolon ";".

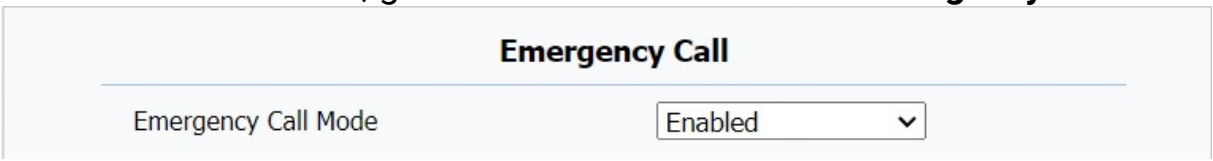
Note

- You are allowed to add up to 5 SIP/IP numbers.
- The numbers are regarded as the whitelist numbers.

Emergency Call Mode

You can let the door phone to be used for emergency calls. In this case, when the door phone initials a call, it ONLY ends when the other party picks up or hangs up the call.

To enable the feature, go to **Phone > Call Feature > Emergency Call**.



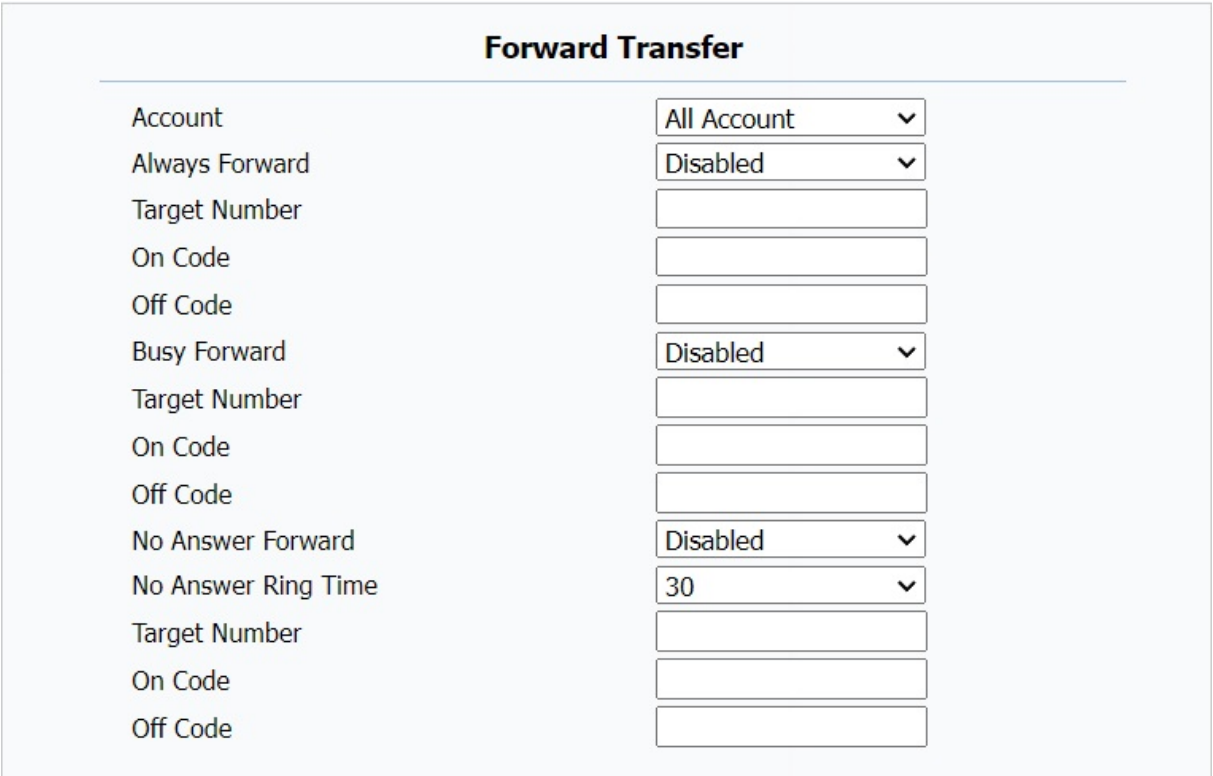
Parameters Set-up:

- **Emergency Call Mode**: If enabled, any calls made by the door phone will only stop when the other party responds by picking up or hanging up the call.

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.

To set up call forwarding, go to **Phone > Call Feature > Forward Transfer**.



Parameters Set-up:

- **Account**: To select the account you want to apply this feature to. The options include All Account, Account 1(SIP account), and Direct IP.

- **Always Forward**: Always to redirect all incoming calls to the designated number.
- **Target Number:** Set up the forwarded-to number when the call forwarding is enabled.
- **On Code**: A feature code used to activate the call forwarding function on the server. This feature code can remotely enable call forwarding without changing the phone's settings.
- **Off Code**: A feature code used to turn off the call forwarding function on the server. It can remotely disable call forwarding without changing the phone's settings.
- **Busy Forward**: To redirect incoming calls to the designated number when the door phone is busy.
- **No Answer Forward**: To redirect incoming calls to the preset number when the phone is not answered within a set ringing time. The default time is 30 seconds.
- **No Answer Ring Time**: To set how long the door phone rings before the incoming call is forwarded to the preset number.

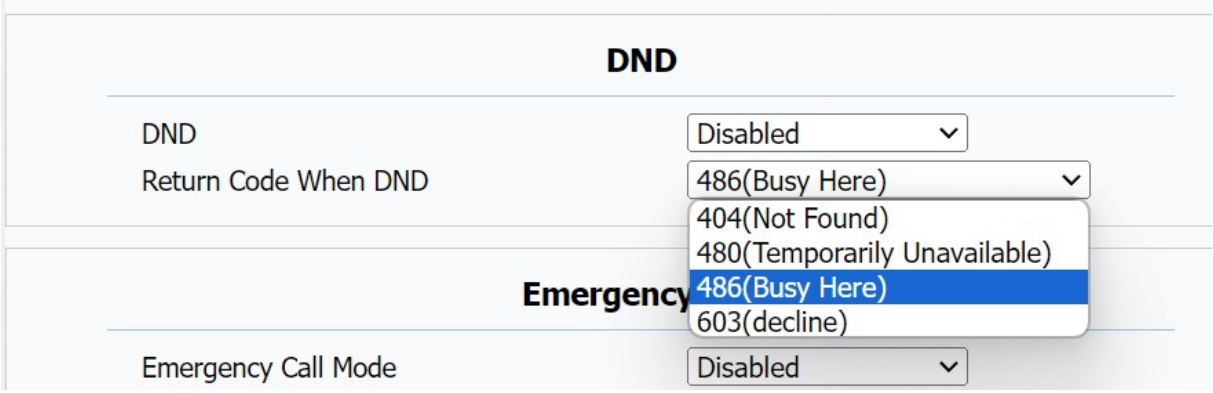
Note

- In terms of priority, **Always Forward** takes precedence over **Busy Forward**, and **Busy Forward** over **No Answer Forward**.

DND

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

To set up DND, go to **Phone > Call Feature > DND.**



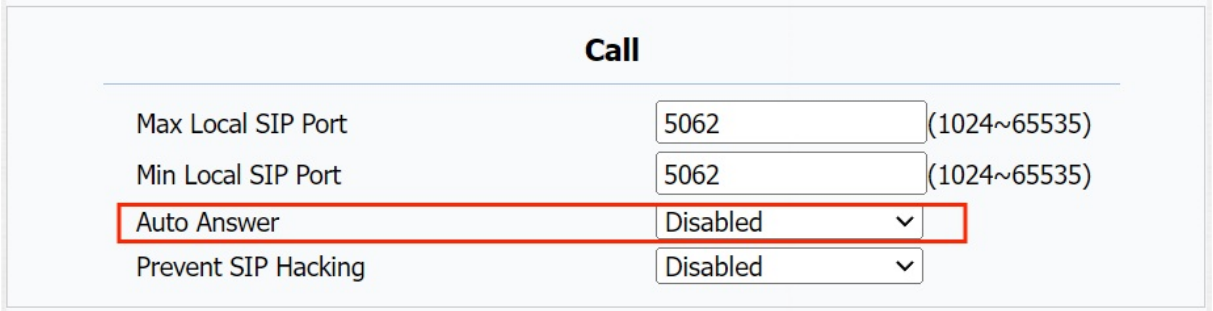
Parameters Set-up:

- **Return Code When DND**: To select the code to be sent to the caller side via SIP server when the incoming call is rejected. **404 for Not Found; 480 for Temporary Unavailable; 486 for Busy Here; 603 for Decline**.

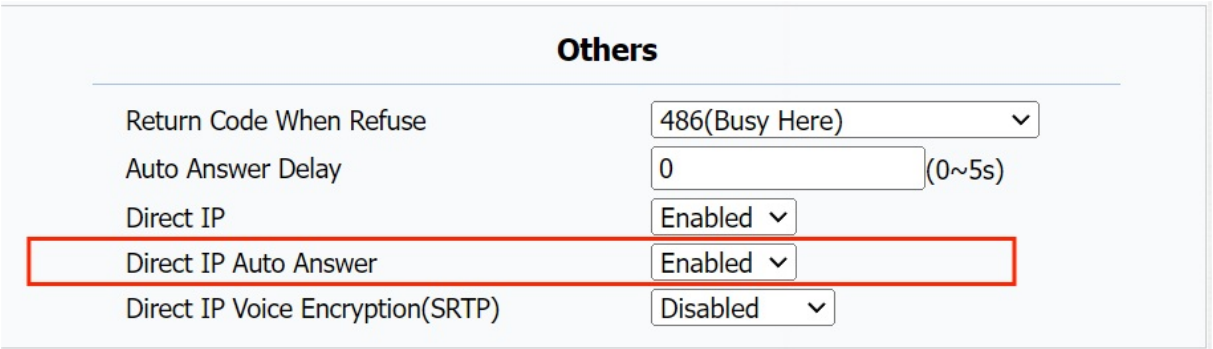
Auto Answer

You can define how quickly the door phone should respond by answering the incoming SIP/IP call automatically by setting up the time-related parameters.

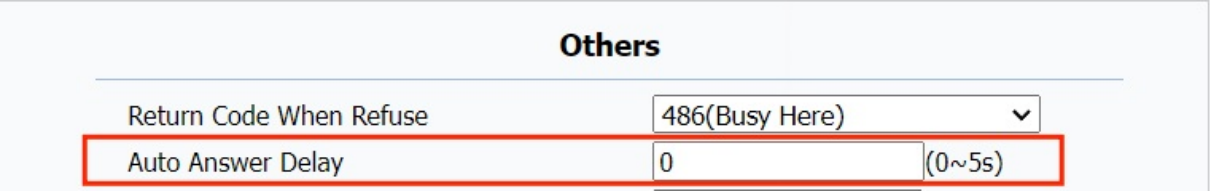
To enable auto answer feature for **SIP** calls, go to **Account > Advanced > Call > Auto Answer**.



To enable auto answer feature for **IP** calls, go to **Phone > Call Feature > Others > Direct IP Auto Answer**.



If you want to set how long the door phone will wait before it automatically answer a call, go to **Phone > Call Feature > Others > Auto Answer Delay**.

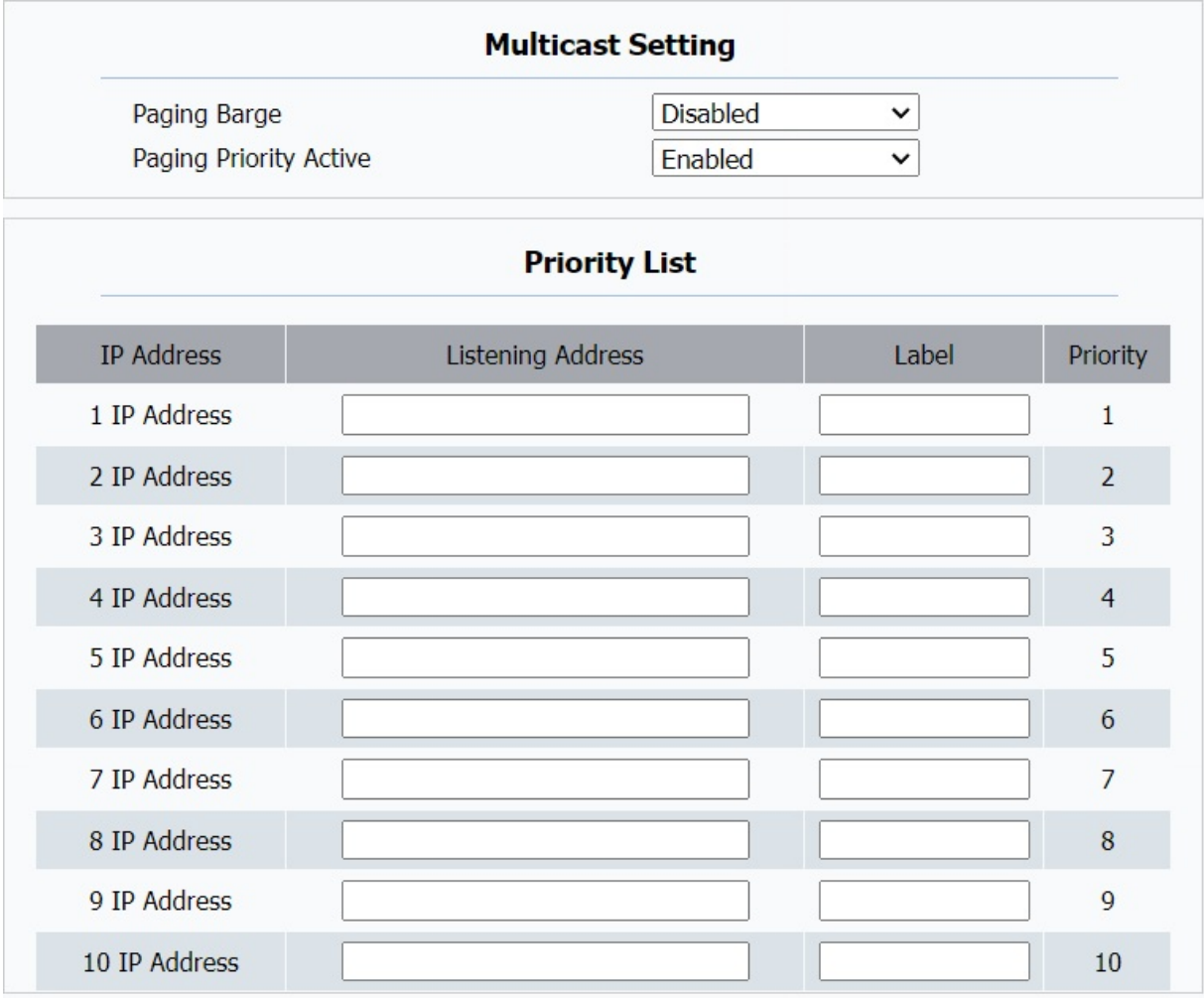


Multicast

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

Click here to watch the demonstration video.

Navigate to **Phone > Multicast** interface.



Parameters Set-up:

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

Return Code

The door phone allows you to select the return code when you reject a call. The default code is **486(Busy Here)**.

To change the code, go to **Phone > Call Feature > Others**.



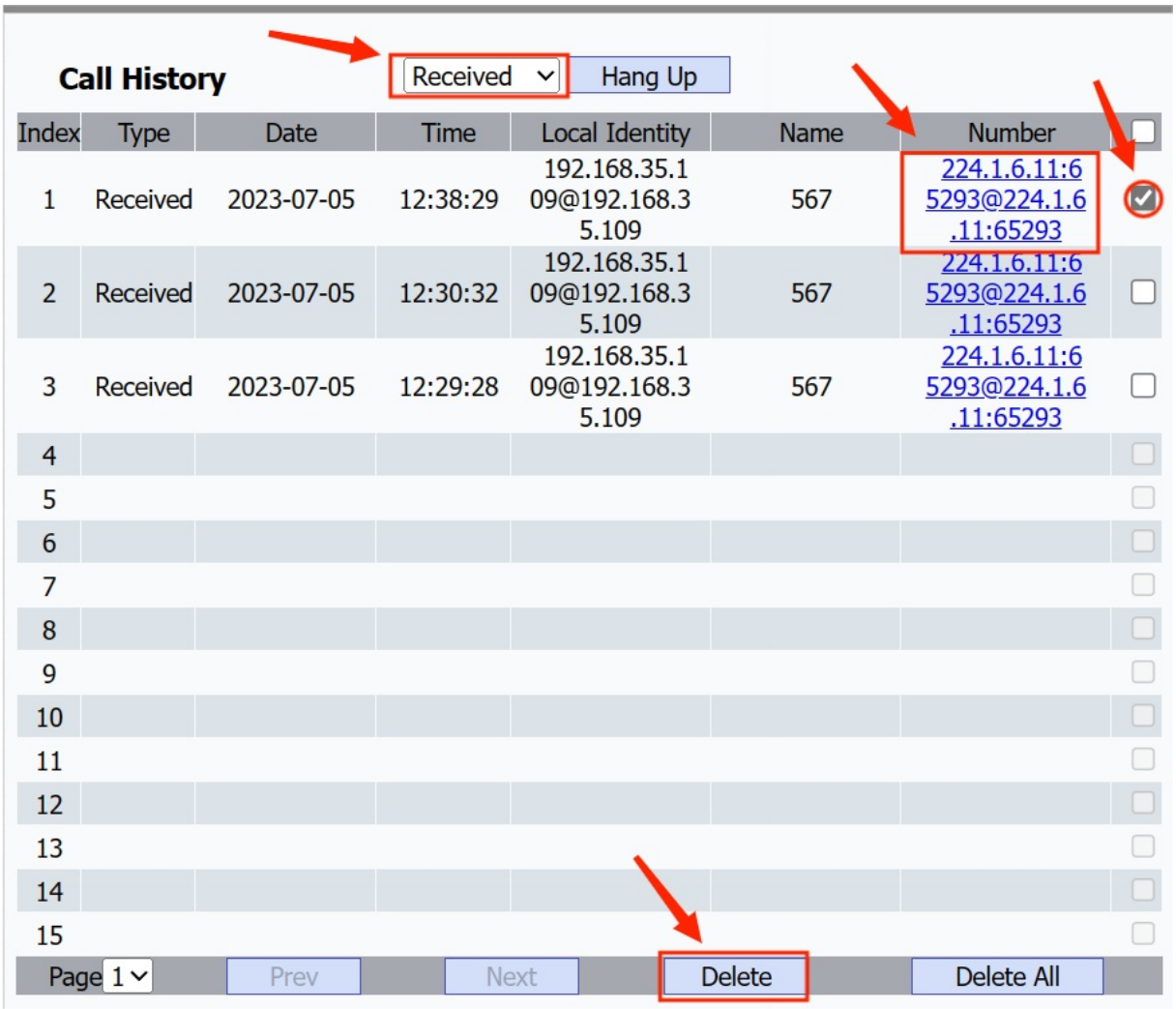
Parameters Set-up:

- **Return Code When Refuse**: To select the return code when you reject a call. The 4 options are **404(Not Found), 480(Temporarily Unavailable), 486(Busy Here)**, and **603(Decline)**.

Call Log

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

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



On this page, do any of the following:

- To filter the call logs based on **All, Dialed, Received, Missed**, and **Forwarded** types.
- To delete any or all logs, check off the box(es) in the last column, and click **Delete** at the bottom. Before deleting, tick the box of the desired log.
- To call any of the number from the web interface, click the number in the **Number** column.

Security

Client Certificate Setting

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

Web Server Certificate

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

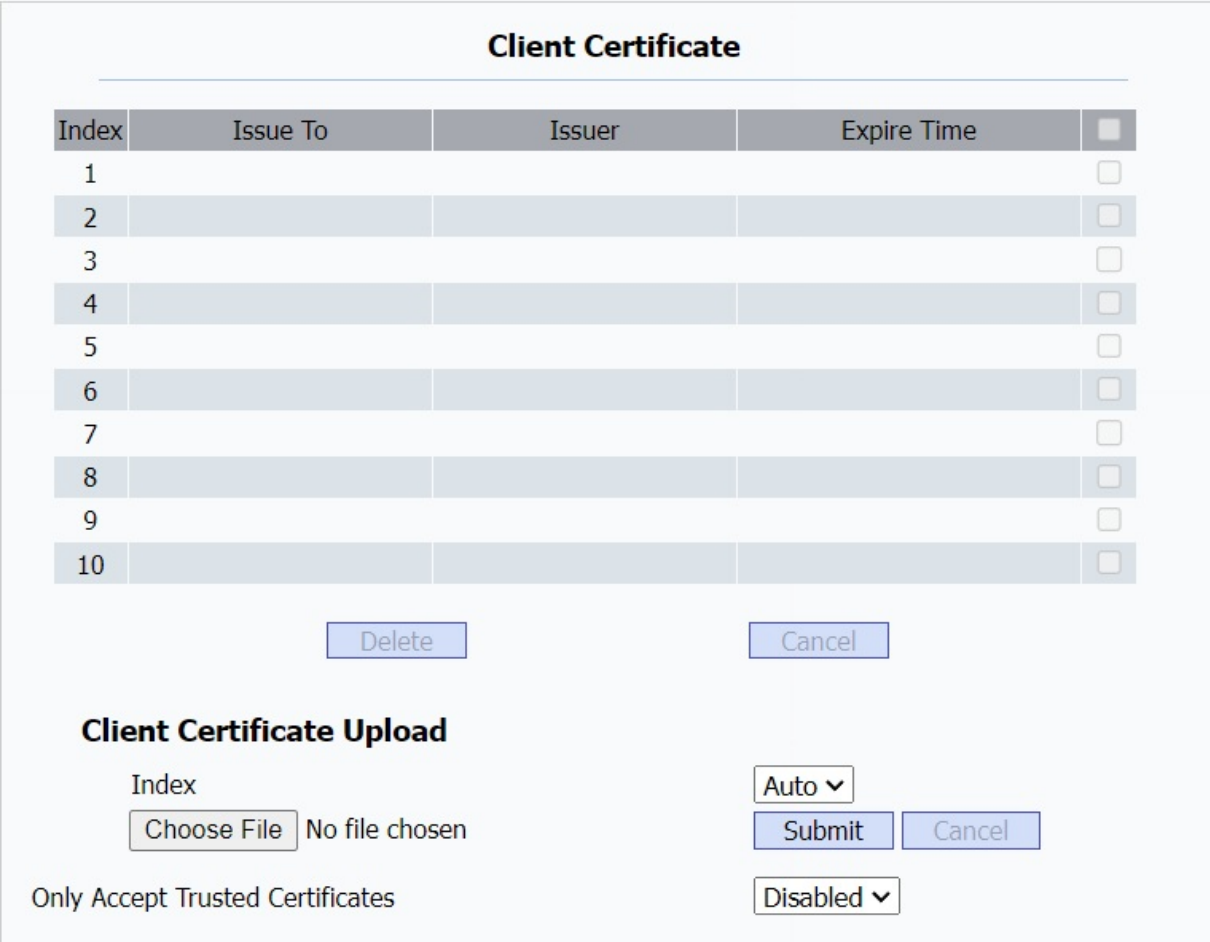
To upload **Web Server Certificate**, go to **Security > Advanced > Web Server Certificate**.



Client Certificate

This certificate verifies the server to the Akuvox door phone when they want to connect using SSL. The door phone verifies the server's certificate against its client certificate list.

To upload and configure client certificate, go to **Security > Advanced > Client Certificate**.



Parameters Set-up:

- **Index**: To select the desired value from drop-down list of Index. If you select Auto, the uploaded certificate will be displayed in numeric order. If you select the value from 1 to 10, the uploaded certificate will be displayed according to the value that the user selected.
- **Select File**: Click Choose File to upload the desired certificate (*.pem only).
- **Only Accept Trusted Certificates**: If select **Enabled**, as long as the authentication success, the phone will verify the server certificate based on the client certificate list. If select **Disabled**, the phone will not verify the server certificate no matter whether the certificate is valid or not.

Voice Encryption

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

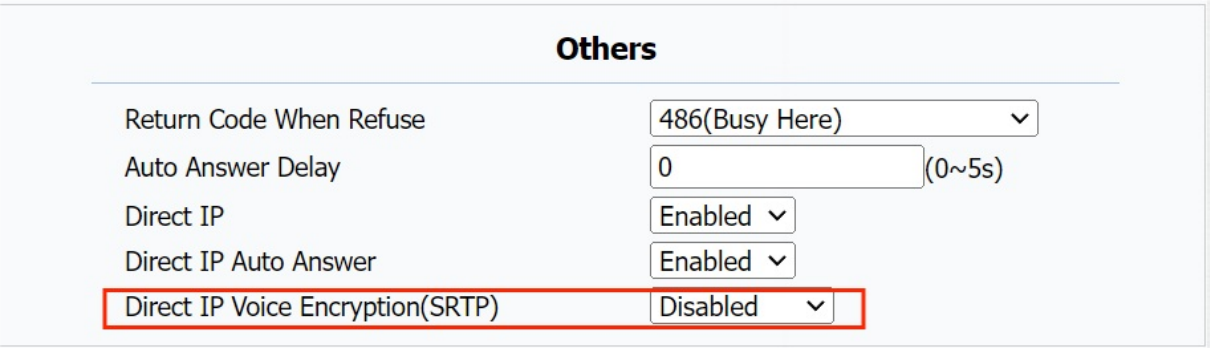
To enable this feature for **SIP** calls, go to **Account > Advanced > Encryption**.



Parameters Set-up:

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

To enable this feature for **IP** calls, go to **Phone > Call Feature > Others**.



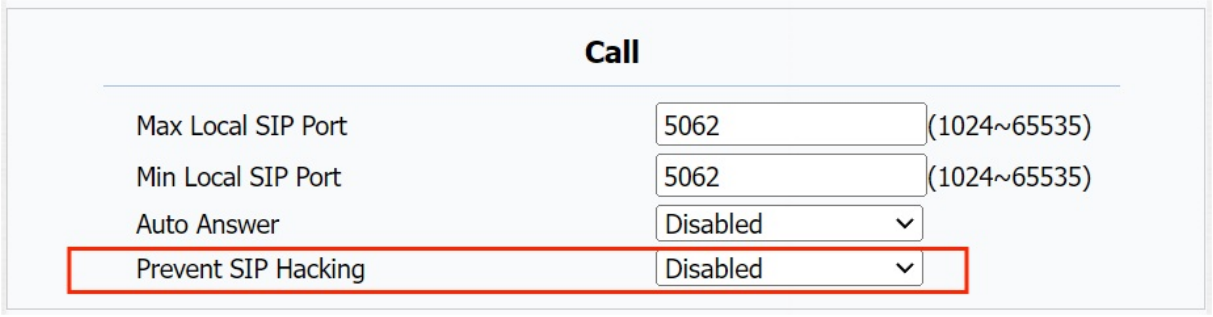
Parameters Set-up:

- **Direct IP Voice Encryption(SRTP)**: To select among **Disabled, Optional** or **Compulsory** for SRTP.

Prevent SIP Hacking

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

To enable this feature, go to **Account > Advanced > Prevent SIP Hacking**.

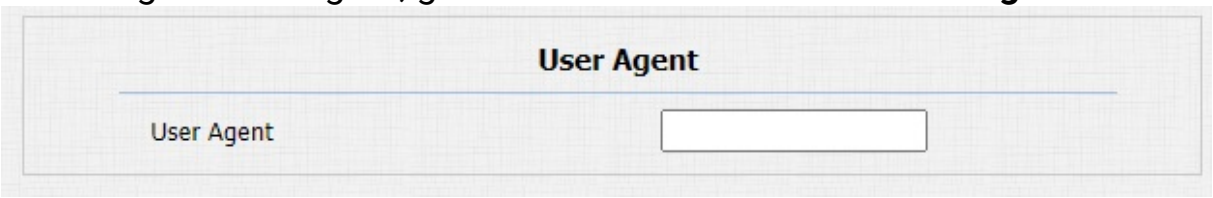


User Agent

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

If user agent is blank by default, users can see the company name Akuvox, model number and firmware version from PCAP.

To configure user agent, go to **Account > Advanced > User Agent**.



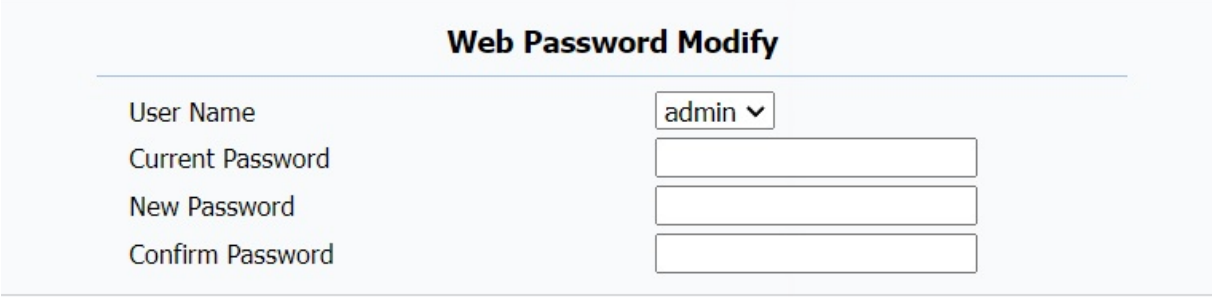
Parameters Set-up:

- **User Agent**: To customize SIP account information to identify the device, which can be viewed by capturing SIP packets.

Device Web Interface Security

Modify Web Interface Password

To change the default web password, go to **Security > Basic > Web Password Modify**.



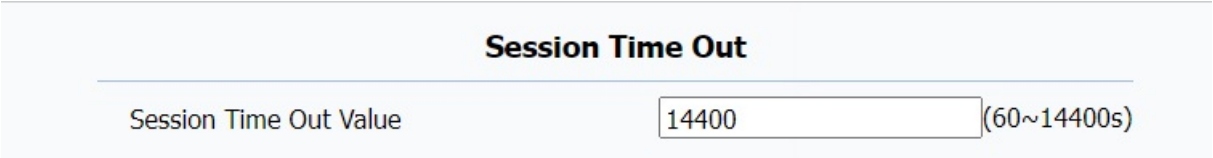
Parameters Set-up:

- **User Name**: To modify either the **admin** or **user** password.
- **Current Password**: Enter the old password for web interface login. It is **admin** by default.
- **New Password**: Enter the new password.
- **Confirm Password**: Enter the new password again and make sure it is the same with the one you entered in the **New Password** box.

Configure Web Interface Automatic Logout

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.

To change the time value, go to **Security > Basic > Session Time Out**.



Parameters Set-up:

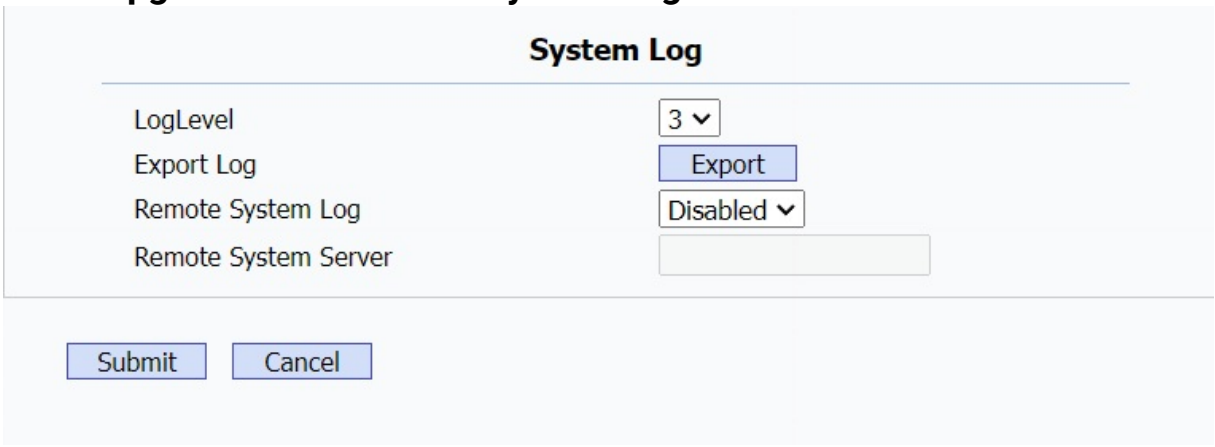
- **Session Time Out Value**: The range is from 60 to 14400 seconds.

Debug

System Log

System logs can be used for debugging purposes.

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



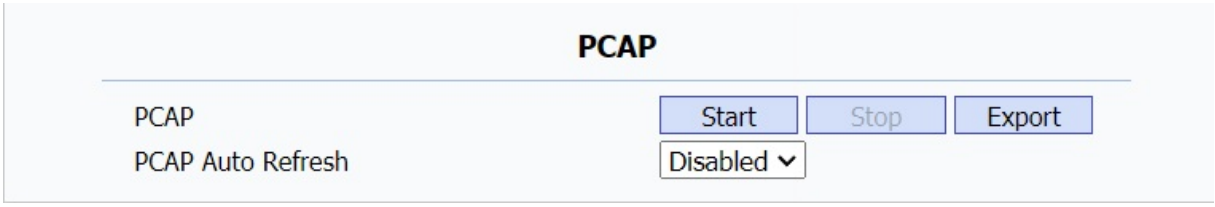
Parameters Set-up:

- **Log Level**: To select the log level from 0 to 7 levels. The default log level is 3. The higher the level, the more detailed the log.
- **Remote System Server**: Enter 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.

Go to **Upgrade > Advanced > PCAP** page to set up properly before using it.



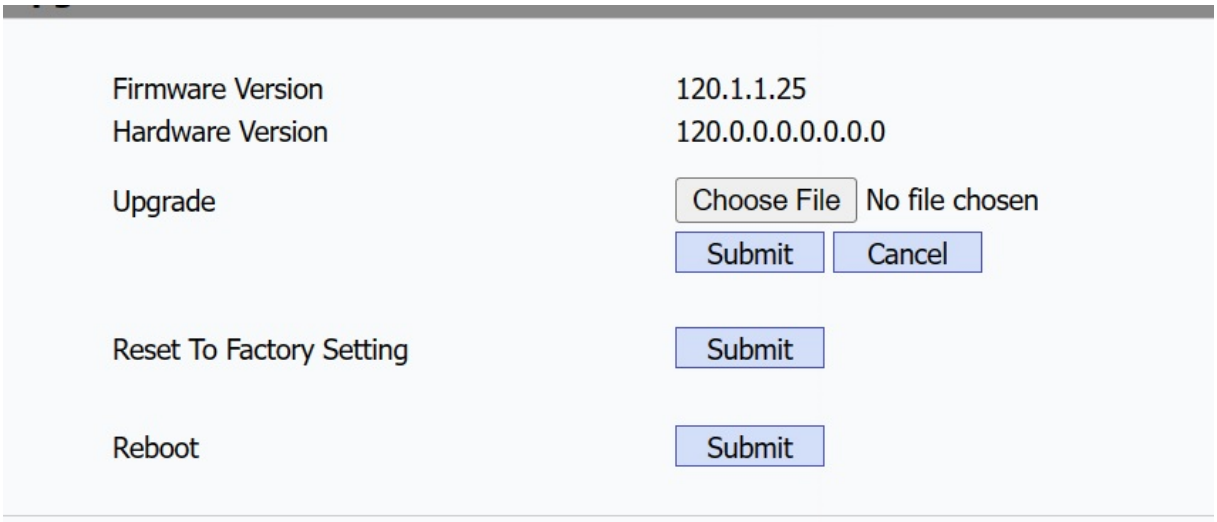
Parameters Set-up:

- **PCAP**: Click **Start** and **Stop** to capture a certain range of data packets before clicking **Export** tab to export the data packets to your computer.
- **PCAP Auto Refresh**: To turn on or off the PCAP auto fresh function. If enabled, the PCAP will continue to capture data packets even after the data packets reached their 1M maximum in capacity. If it is disabled, the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1MB.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **Upgrade > Basic**.



Parameter Set-up:

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

Note

- Firmware files to be uploaded must be .rom format.
- The device must keep being connected to internet and power supply when the firmware upgrade is in progress, otherwise, the upgrade may fail.

Backup

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

To do so, go to **Upgrade > Advanced > Others**.



Parameter Set-up:

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

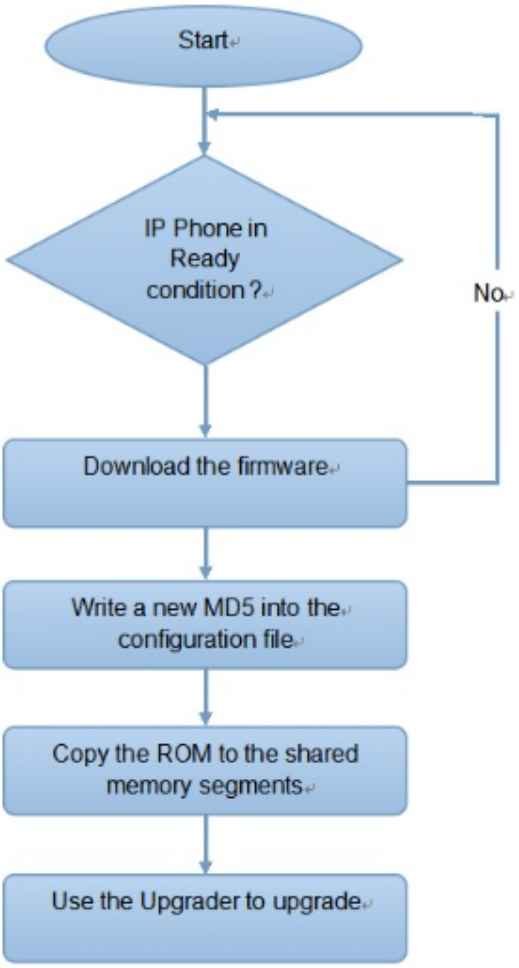
Auto-Provisioning

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**:

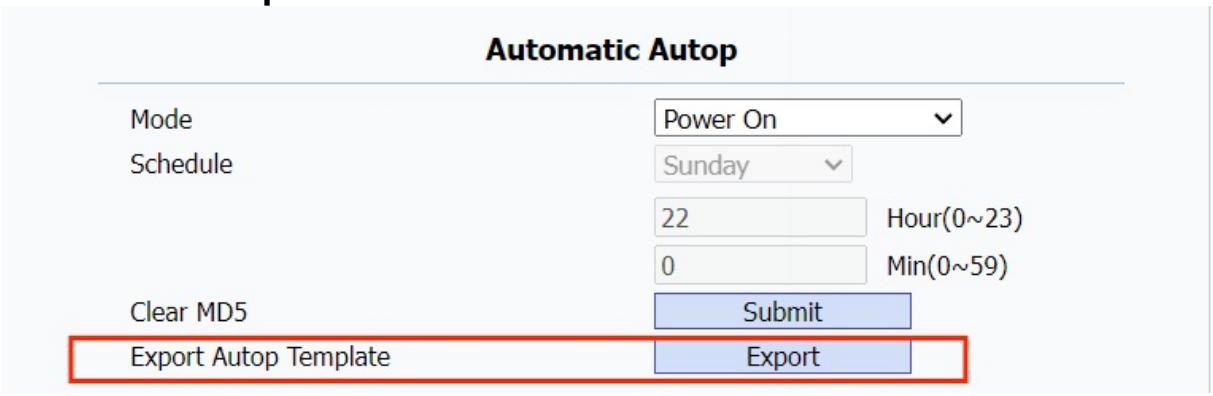
MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

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.

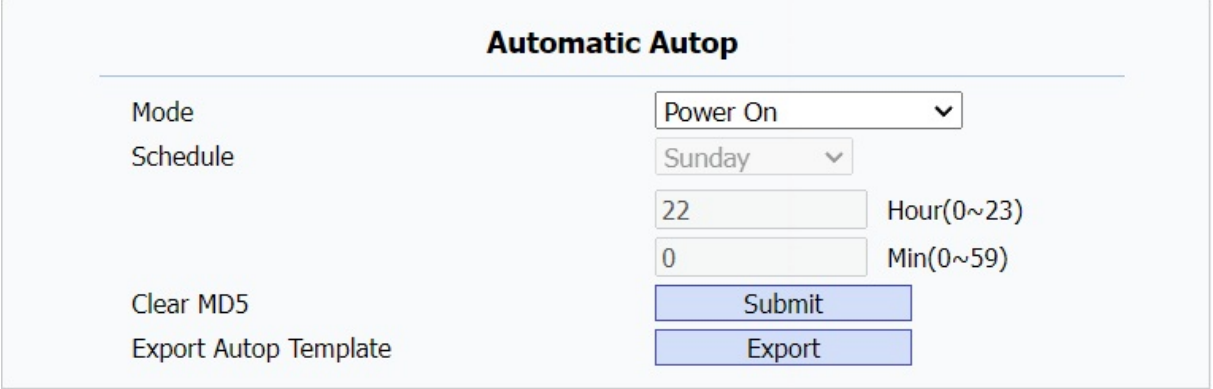
To get the Autop configuration file template on **Upgrade > Advanced > Automatic Autop** interface.



Automatic Provisioning Configuration

Akuvox door phones can perform provisioning for itself at a specific time according to the preset schedule.

To set a schedule, go to **Upgrade > Advanced > Automatic Autop** interface.



Parameters Set-up:

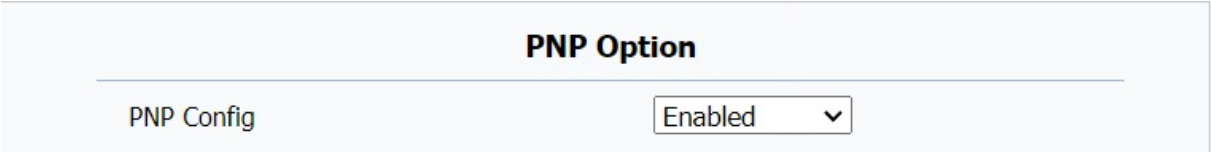
- **Mode**:
  - **Power on**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode. The mode enables the device to perform Autop every time it boots up or according to the schedule you set up.
  - **Hourly Repeat**: The device will perform Autop every hour.
  - **Disable**: To turn off the AutoP feature.
- **Schedule**: When you select **Repeatedly** mode, you need to set up the time schedule for the AutoP.

PNP Configuration

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

Click here to watch the configuration video.

To enable PNP settings, go to **Upgrade > Advanced > PNP Option**.



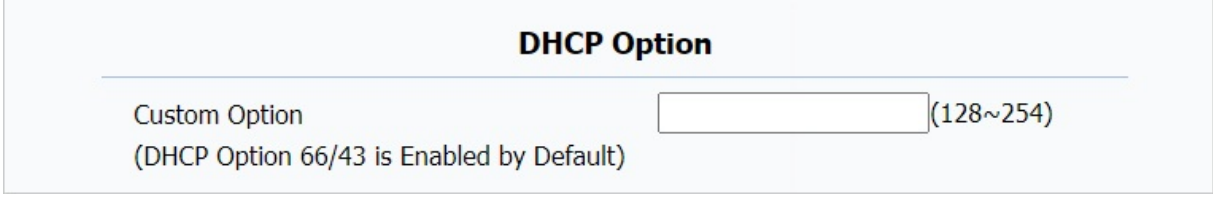
DHCP Option

DHCP is another method for auto-provisioning on Akuvox devices. When using DHCP to obtain an IP address, the devices will automatically check the DHCP server for upgrades to both the general and MAC configuration files, provided that the auto-provisioning mode is set to **Power On**.

- The device is set up to use DHCP option 43 and option 66 by default.
- You can also customize the options.

- The priority in the order is custom option > DHCP option43 > option 66.

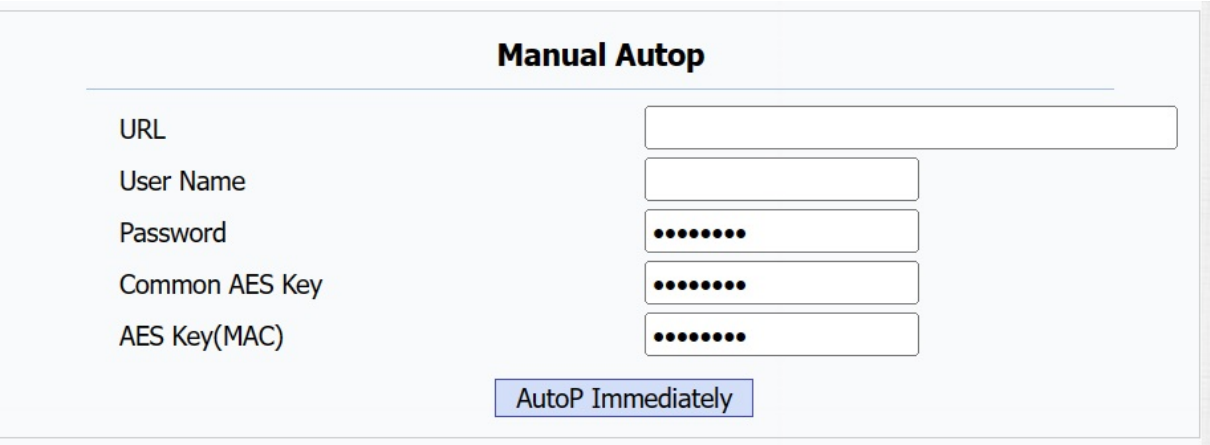
To customize the DHCP option, go to **Upgrade > Advanced > DHCP Option**.



Manual Provisioning Configuration

- You can manually set up a server URL for downloading firmware or configuration files.
- If an Autop schedule is established, the door phone will perform auto-provisioning at a specific time as defined by the schedule.
- Upgrading the device firmware and configuration can be done using TFTP, FTP, HTTP, and HTTPS protocols.

To configure the manual Autop, go to **Upgrade > Advanced > Manual Autop**. Enter the **User Name**/**Password** if the server needs a username/password to be accessed, otherwise leave it blank.



Parameters Set-up:

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

MAC-based auto provisioning configuration file.

Note

- To use the manual Autop, you need to disable both the PNP and DHCP options. Otherwise, the device will prioritize upgrading PNP or DHCP option and will not upgrade the manual URL.
- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

Note

Server Address format:

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

Note

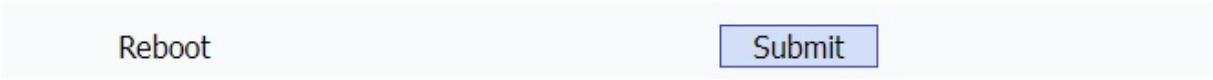
Akuvox do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

System Reboot&Reset

Reboot

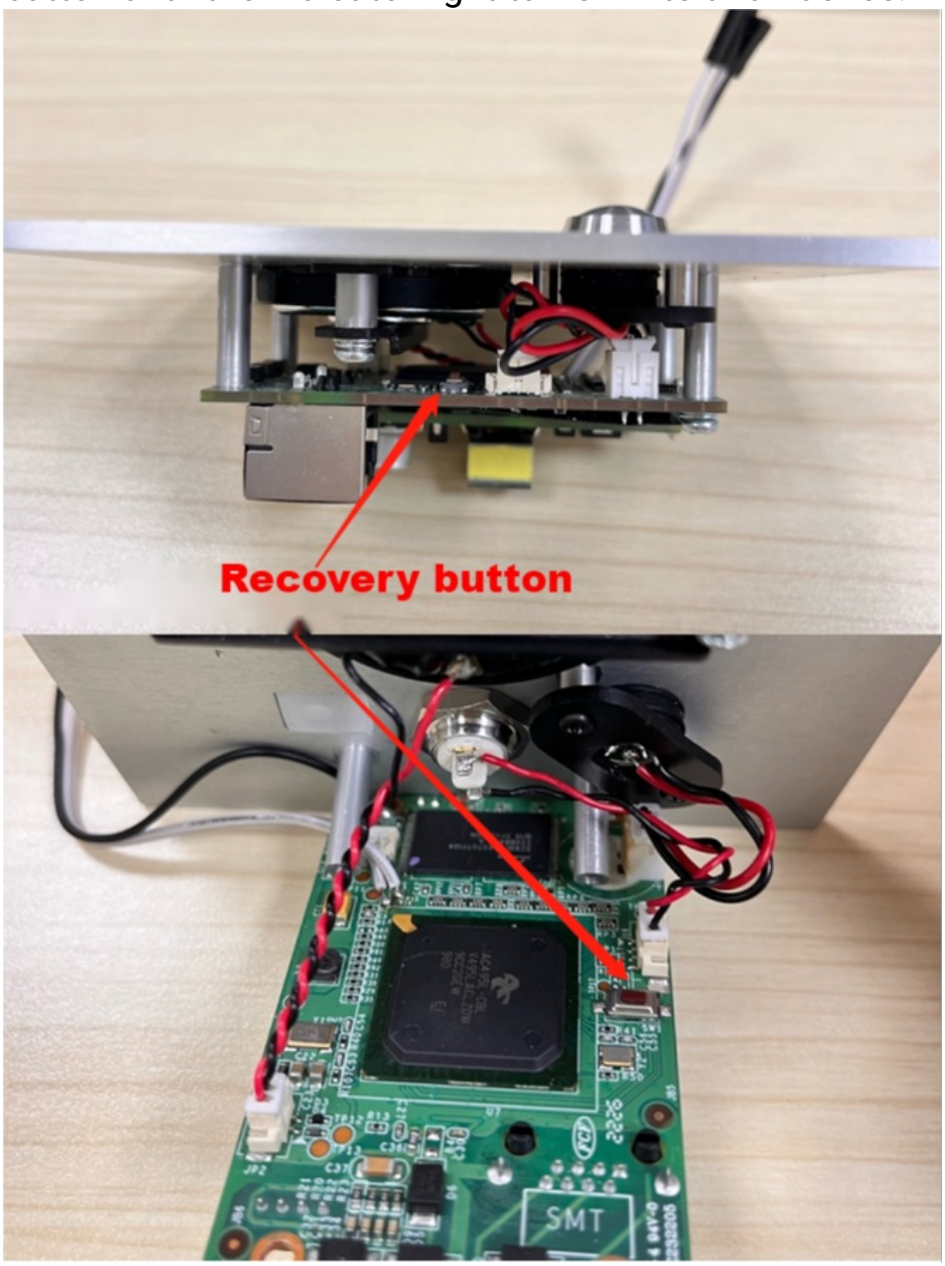
Reboot Device from Web Interface

You can restart the device by going to **Upgrade > Basic** web interface.



Reboot Device by the Recovery Button

The device reset can also be done by long pressing the physical recovery button until the indicator light turns white and flashes.



Factory Reset

To reset the device system to the factory setting, go to the web **Upgrade > Basic**.



Powered by Document360