Table of contents

Akuvox C310 Indoor Monitor Administrator Guide

About This Manual

Akuvox

Open A Smart World

WWW.AKUVOX.COM

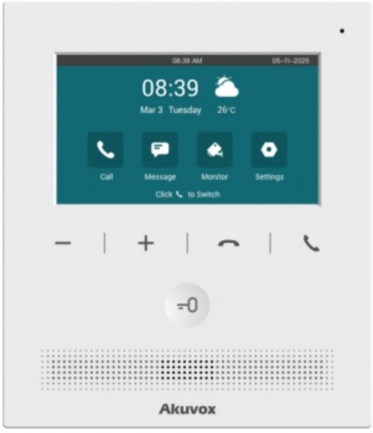
C310

INDOOR MONITOR

Admin Guide

Thank you for choosing the Akuvox C310 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. This manual is written based on firmware 310.30.15.25, and it provides all the configurations for the functions and features of the C310 series indoor monitor. Please visit the Akuvox website or consult technical support for any new information or the latest firmware.

Product Overview



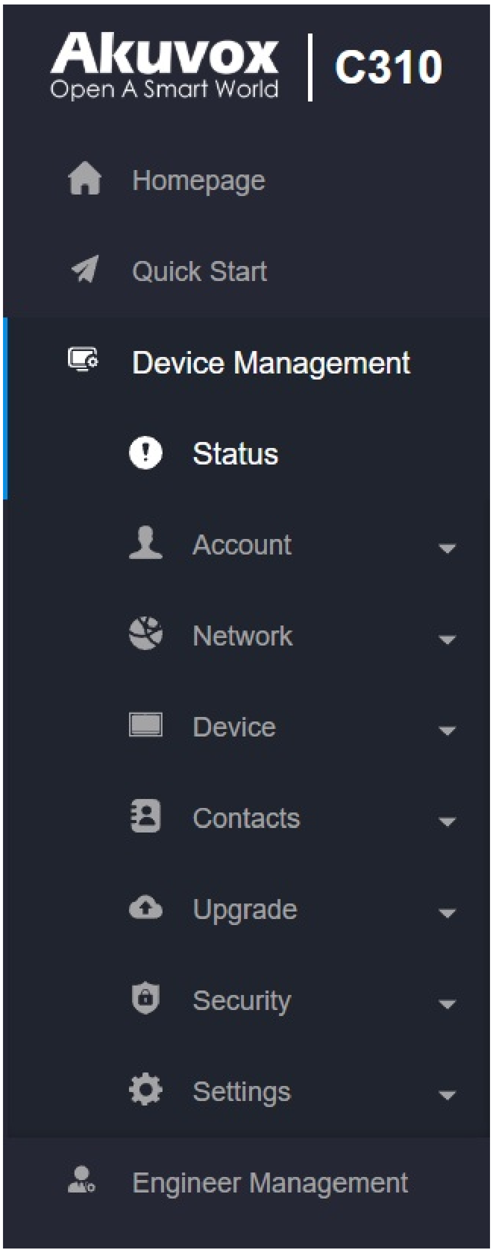
The device can be connected to the Akuvox door phone for audio/video communication, unlocking, and monitoring. Residents can communicate with visitors via audio/video calls, and the system supports remote door opening. It is more convenient and safer for residents to check the visitor's identity through its video preview function. C310 can be applied to scenarios such as villas, apartments, and buildings.

Model Specification

Model	**C310**
Touch Screen	X
Front Panel	Plastic
Microphone	x1, -34dB
Ethernet Port	1xRJ45, 10/100Mbps adaptive
Power Supply	802.3af Power-over-Ethernet or 12V DC Connector

Introduction to Configuration Menu

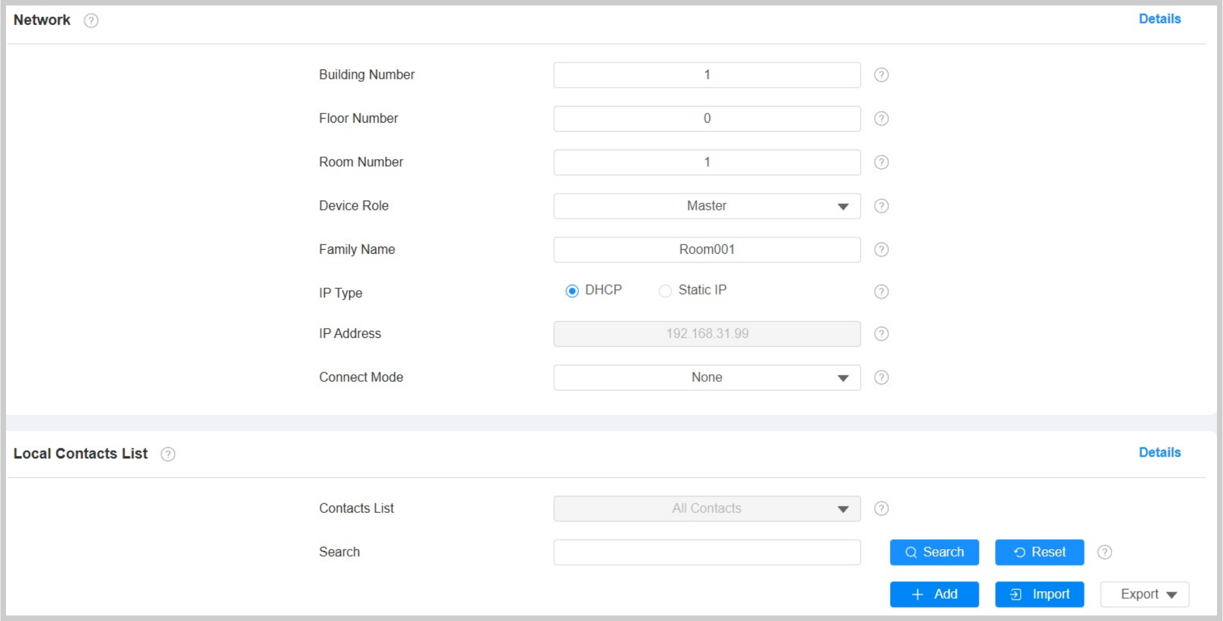
- **Quick Start**: This section provides quick access to the device's key settings, such as network, user, relay, etc.
- **Device Management**:
    - **Status**: This section gives you basic information, such as product information, network information, account information, etc.
    - **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio and video codec, DTMF, etc.
    - **Network**: This section mainly deals with network connections, RTP port settings, device deployment, etc.
    - **Device**: This section includes time & language, call feature, screen display, multicast, audio intercom feature, monitor, relay, lift control, etc.
    - **Contacts**: This section allows the user to configure the local contact list stored in the device.
    - **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 certificates upload.
    - **Settings**: This section includes the RTSP settings.
- **Engineer Management**: This section provides quick access to upgrading, maintaining, and debugging the device.



Introduction to Quick Start Module

The Quick Start module allows you to configure the device's core features on a single interface, instead of switching between different interfaces.

You can redirect to the feature detail interface by clicking **Details** in the upper right corner.



Network

Building Number: 1

Floor Number: 0

Room Number: 1

Device Role: Master

Family Name: Room001

IP Type: ● DHCP ○ Static IP

IP Address: 192.168.31.99

Connect Mode: None

Local Contacts List

Contacts List: All Contacts

Search:

- **Network**: Display the location information of the device.
    - **Connect Mode**: It is automatically set up according to the actual device connection with a specific server in the network, such as SDMC, Cloud, or None.
- **Local Contacts List**: Display local contacts.
- **Auto-Discovery Contact List**: Display the contacts, such as door phones, in the Self-organizing Network Solution.
    - **Show LCD Auto-Discovery Contact List**: Set whether to display these contacts on the device screen.
- **Remote Relay by HTTP**: Display the HTTP commands to remotely control relays connected to door phones.
- **Door Phone**: You can add video streams of door phones via RTSP.
    - **Show Building Door Phone**: Set whether to display door phones at the building gate in the monitoring list.
    - **Show Public Door Phone**: Set whether to display door phones in the public area in the monitoring list.
    - **Device Number**: The device's SIP/IP number for identification.
    - **Device Name**: The device name for identification.
    - **RTSP Address**: The RTSP address of the monitoring device. RTSP format: *rtsp://Device IP address/live/ch00_0.*
    - **Username**: The username of the monitoring device for authentication.
    - **Password**: The password of the monitoring device for authentication.

- **Display In Call**: Enable it to display the monitoring video during a call.

Access the Device

Akuvox indoor monitor system settings can be either accessed on the device or its web interface.

Device Initial Setup

After the device boots, select the language, time zone, set up location, and network.

Press **+** and **—** to select up and down.

Press 🔓 to enter the configuration.

Press 📞 to proceed, and press ☎ to return to the previous step.

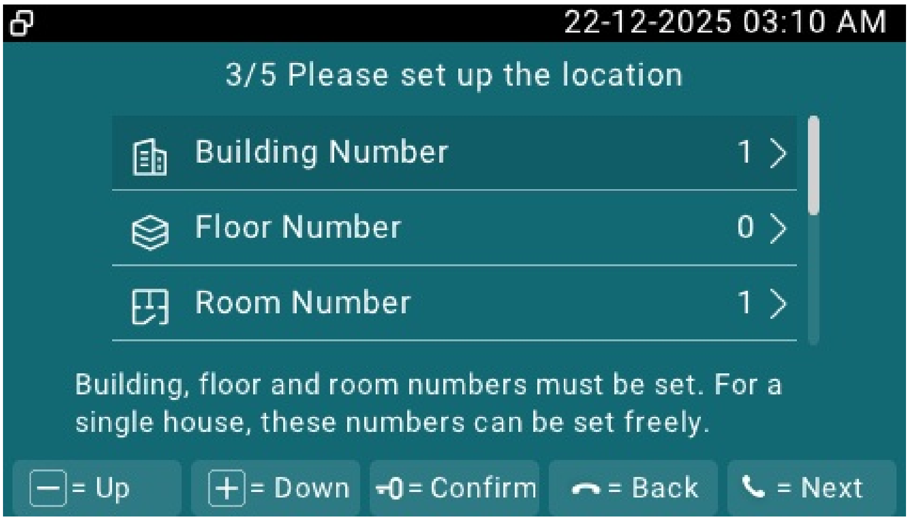
Location

To change the building, floor, and room numbers, press 🔓 to select the option.

Then, press **+** and **—** to increase and decrease the number by 1.

Press 📞 to switch between the units and tens digit.

Press 🔓 to confirm the setting and press ☎ to cancel the setting.



22-12-2025 03:10 AM

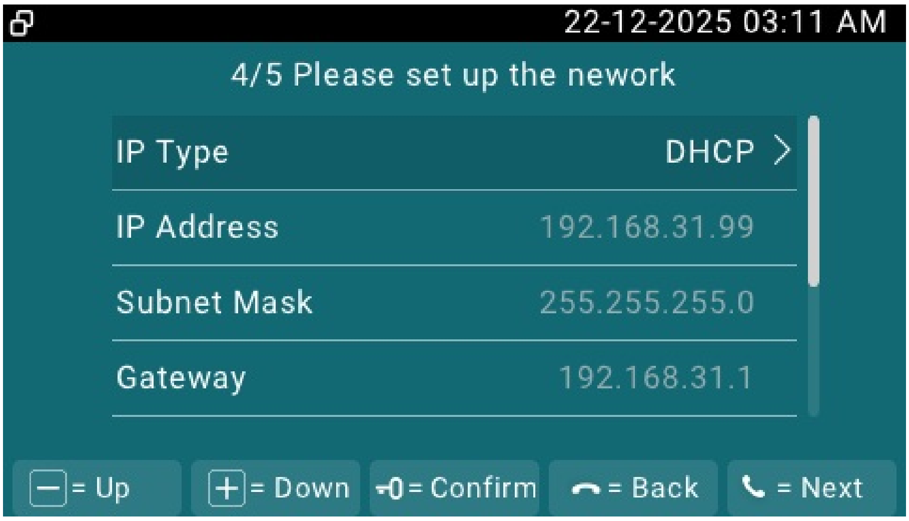
3/5 Please set up the location

Building Number	1 >
Floor Number	0 >
Room Number	1 >

Building, floor and room numbers must be set. For a single house, these numbers can be set freely.

Network

To select the network configuration, press -0.



22-12-2025 03:11 AM

4/5 Please set up the nework

IP Type	DHCP >
IP Address	192.168.31.99
Subnet Mask	255.255.255.0
Gateway	192.168.31.1

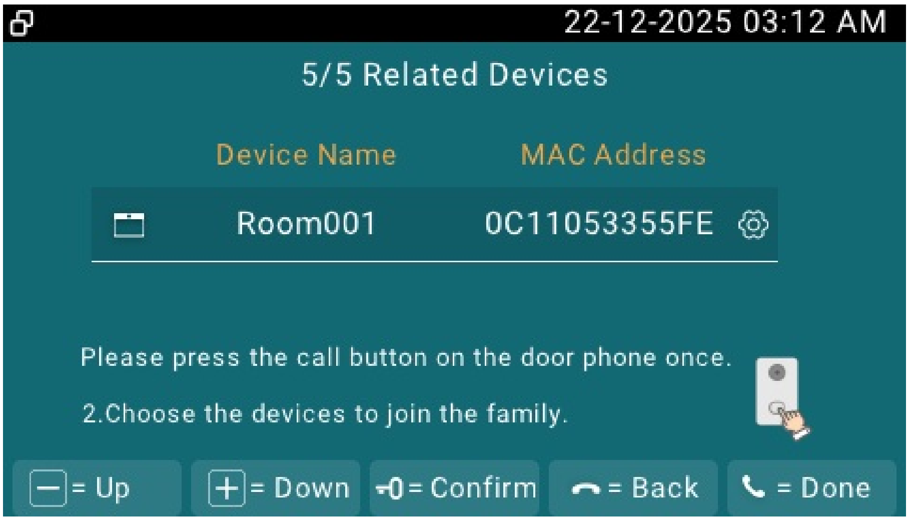
Related Devices

This step is designed for the Self-Organizing Network Solution.

The indoor monitor scans devices on the same local area network(LAN). When the apartment door phone is detected, it plays a ding sound. Press the push button on the door phone within 5 minutes to pair the door phone and the indoor monitor.

Press -0 to configure the selected device.

After editing the device, directly press ☎ to save and exit the settings.


22-12-2025 03:12 AM

5/5 Related Devices

Device Name	MAC Address
Room001	0C11053355FE

Please press the call button on the door phone once.

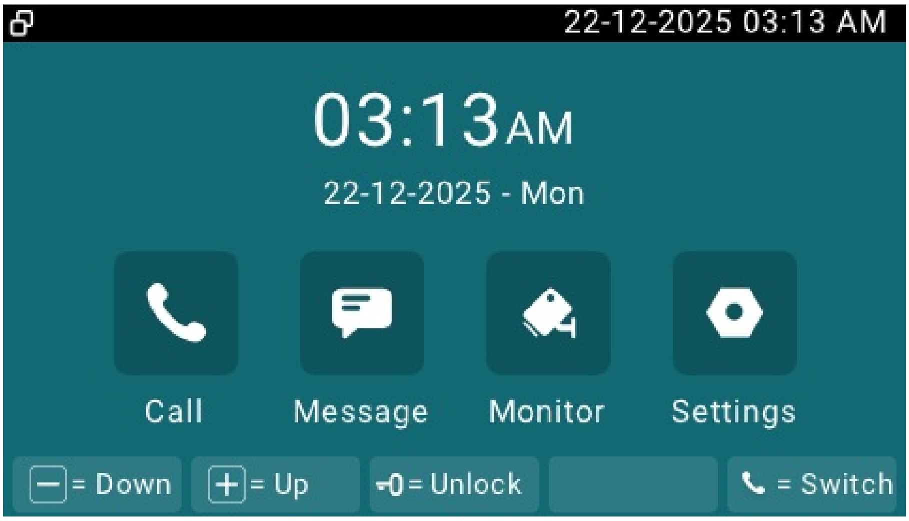
2.Choose the devices to join the family.

Home Screen Overview

Press ☎ to switch between areas and press ⊸0 to confirm the selection.

Without selecting an area, pressing ⊸0 to open the door via the HTTP command.

Press **+** and **—** to adjust volumes of incoming call ringtone and message notifications.

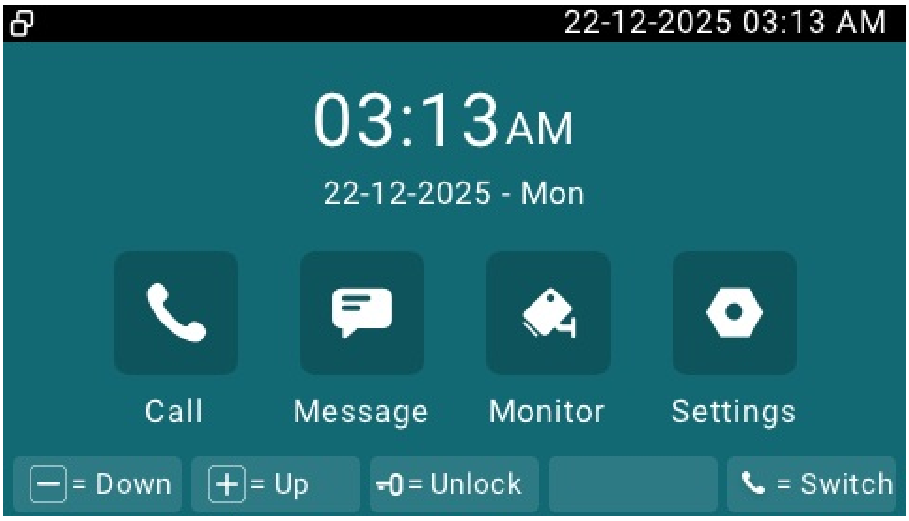

22-12-2025 03:13 AM

03:13 AM

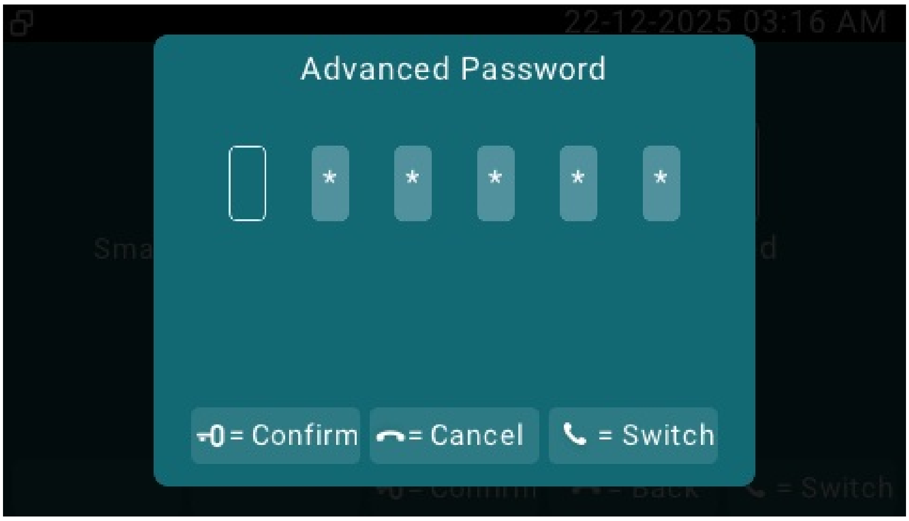
22-12-2025 - Mon

Access the Device Settings

Select the **Settings** area and press ⊸0.



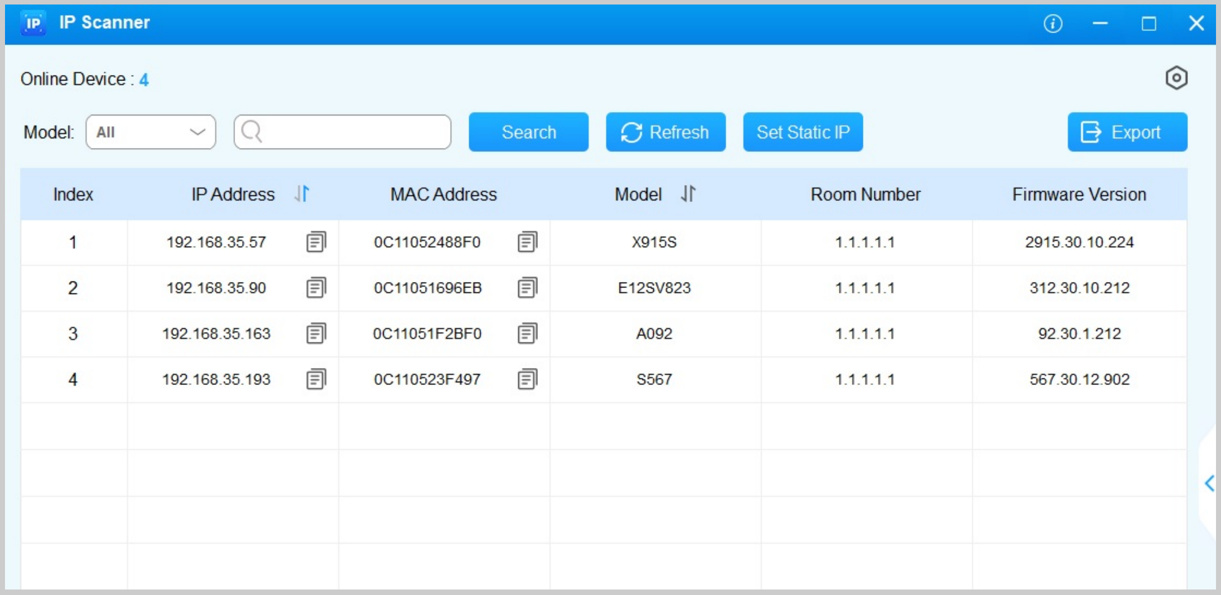
Select **Advanced** and press -0. Enter the password by pressing **+** and **—**(Increase and decrease numbers) and pressing ☎ to switch between digits. The default is 123456.



Access the Device Web Settings

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

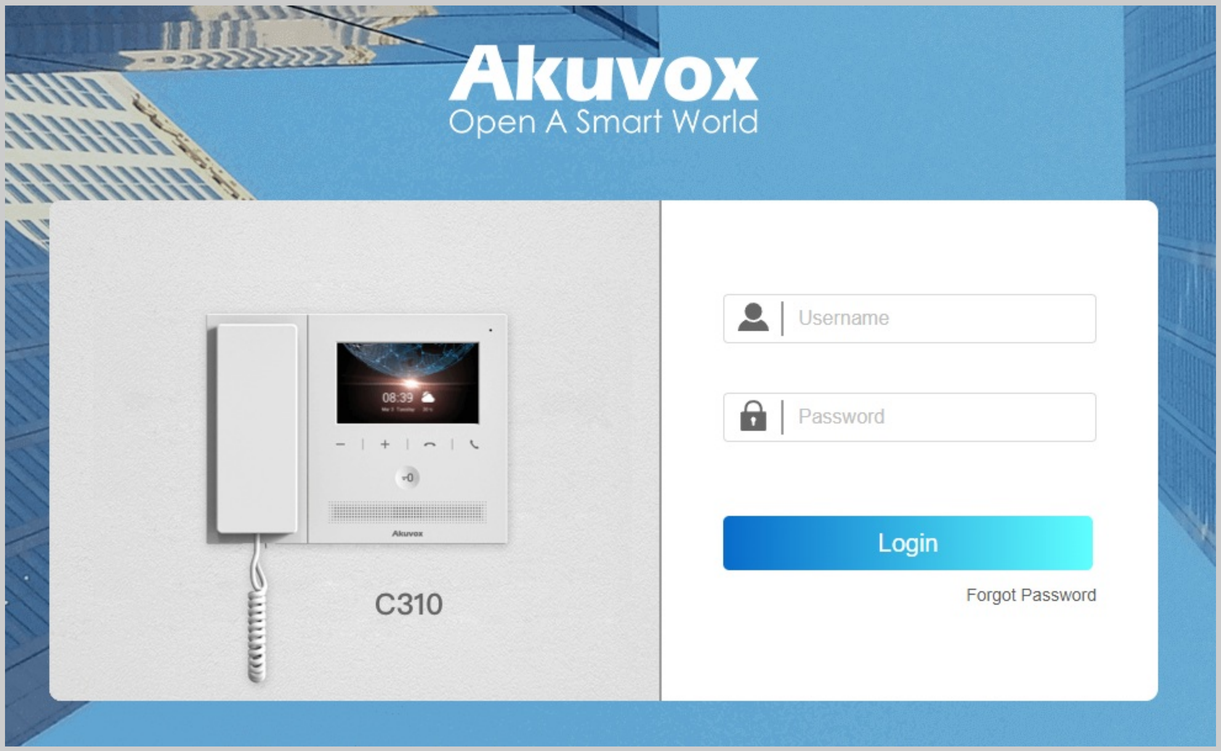
To check the IP address, go to the device **Settings > Status > Network** screen. You can also search for the device by IP scanner, which can search all the devices on the same LAN.



Online Device : 4

Model: All

Index	IP Address	MAC Address	Model	Room Number	Firmware Version
1	192.168.35.57	0C11052488F0	X915S	1.1.1.1.1	2915.30.10.224
2	192.168.35.90	0C11051696EB	E12SV823	1.1.1.1.1	312.30.10.212
3	192.168.35.163	0C11051F2BF0	A092	1.1.1.1.1	92.30.1.212
4	192.168.35.193	0C110523F497	S567	1.1.1.1.1	567.30.12.902



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
- Google Chrome browser is strongly recommended.
- The initial username and password are **admin** and please be case-sensitive to the user names and passwords entered.
- Your computer should be on the same LAN as the device.

Language and Time

Language

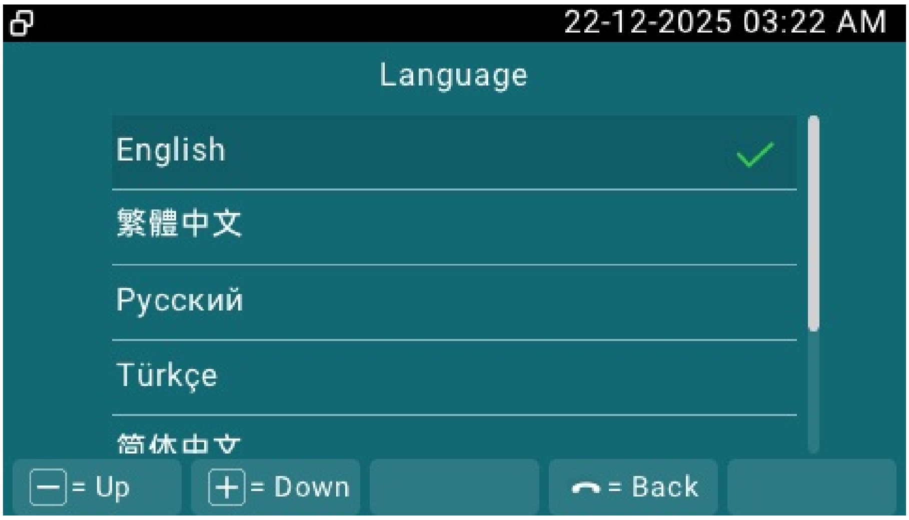
Set up the language during initial device setup or later through the device or web interface according to your preference.

On the Device

To select the desired language, go to **Settings > Language** screen.

The device supports the following languages:

- English, Traditional Chinese, Russian, Turkish, Simplified Chinese, Arabic, and Persian.

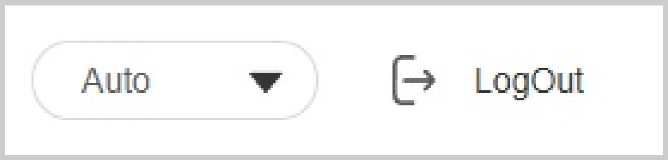


On the Web Interface

You can switch the device's web language in the upper-right corner.

The device web interface supports the following languages:

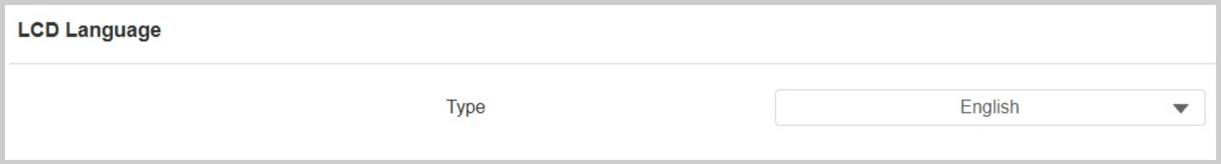
- English, Traditional Chinese, Russian, Turkish, Simplified Chinese, Arabic, and Persian.



Change the LCD language on the **Device > Time/Lang** interface.

The device supports the following languages:

- English, Traditional Chinese, Russian, Turkish, Simplified Chinese, Arabic, and Persian.



LCD Language

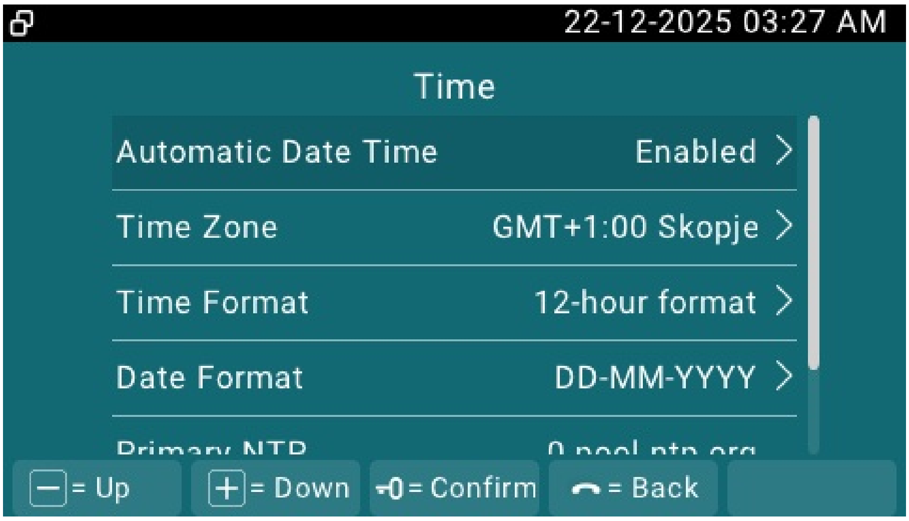
Type: English

Time

Time settings, including time zone, date and time format, and more, can be configured either on the device or the web interface.

On the Device

Set up time on the device **Settings > Time** screen.



22-12-2025 03:27 AM

Time

Automatic Date Time: Enabled

Time Zone: GMT+1:00 Skopje

Time Format: 12-hour format

Date Format: DD-MM-YYYY

Primary NTP: 0.pool.ntp.org

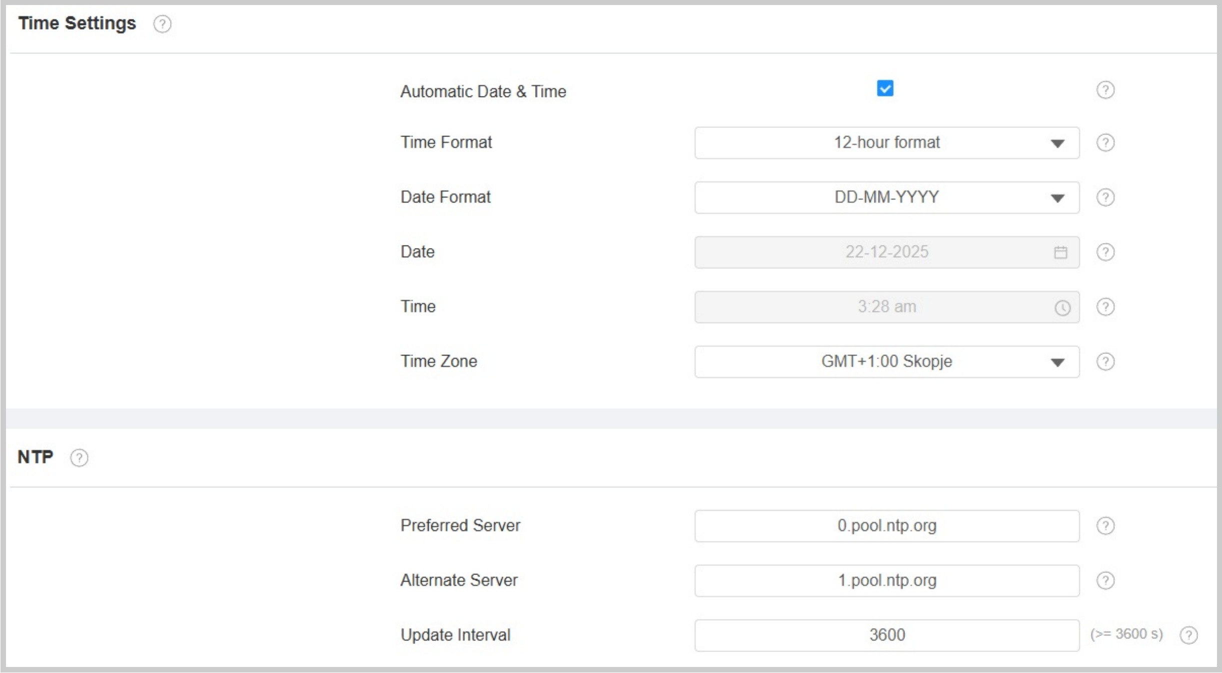
- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.

- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Date Format**: Select the date format from the available options.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **Primary/Secondary NTP**: Enter the NTP server address. The secondary NTP is the backup.

On the Web Interface

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.

Navigate to **Device > Time/Lang** interface.



Time Settings

Automatic Date & Time	☑
Time Format	12-hour format
Date Format	DD-MM-YYYY
Date	22-12-2025
Time	3:28 am
Time Zone	GMT+1:00 Skopje

NTP

Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>= 3600 s)

- **Automatic Date & Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **Date Format**: Select the date format from the available options.

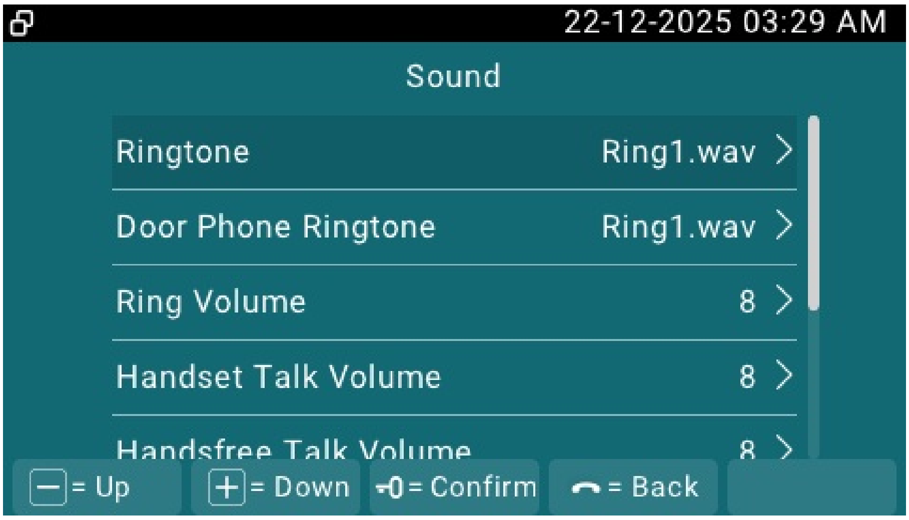
- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Preferred Server**: Enter the NTP server address.
- **Alternate Server**: Enter the backup server address. When the main NTP server fails, it will change to the backup server automatically.
- **Update Interval**: The time between sending the update request to the NTP server.

Sound and Volume

Akuvox indoor monitor provides you with various types of ringtones and volume configurations. You can configure them on the device directly or on the web interface.

On the Device

Set up the volumes on the device **Settings > Sound** screen.



22-12-2025 03:29 AM

Sound

Ringtone Ring1.wav

Door Phone Ringtone Ring1.wav

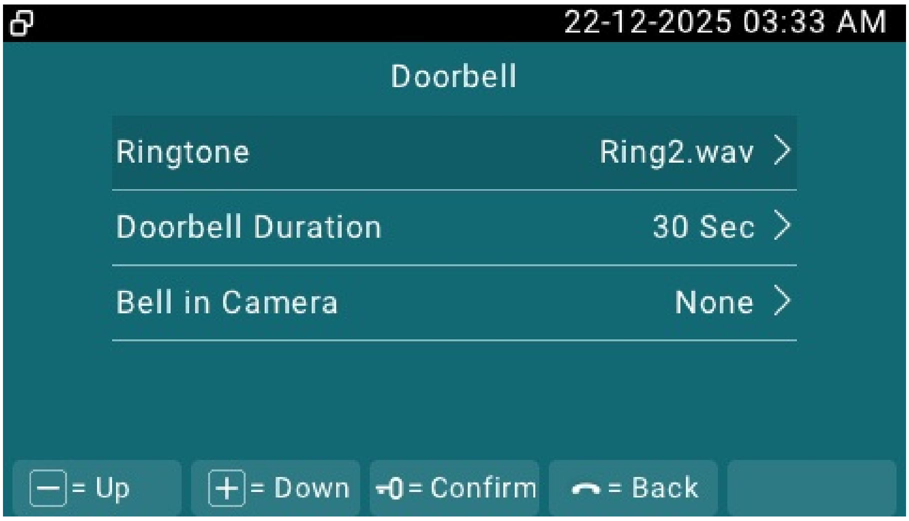
Ring Volume 8

Handset Talk Volume 8

Handsfree Talk Volume 8

- **Ringtone**: The incoming call ringtone.
- **Door Phone Ring Tones**: The tone sounds when the indoor monitor receives calls from a door phone.
- **Ring Volume**: The incoming call ringtone volume.
- **Talk Volume**: The speaker volume during a call.
- **MIC Volume**: The microphone volume during a call.
- **Touch Sound**: The icon tapping sound.

You can configure the doorbell sound and select the local relay to be triggered along with the doorbell on the **Settings > Doorbell** screen.



22-12-2025 03:33 AM

Doorbell

Ringtone Ring2.wav

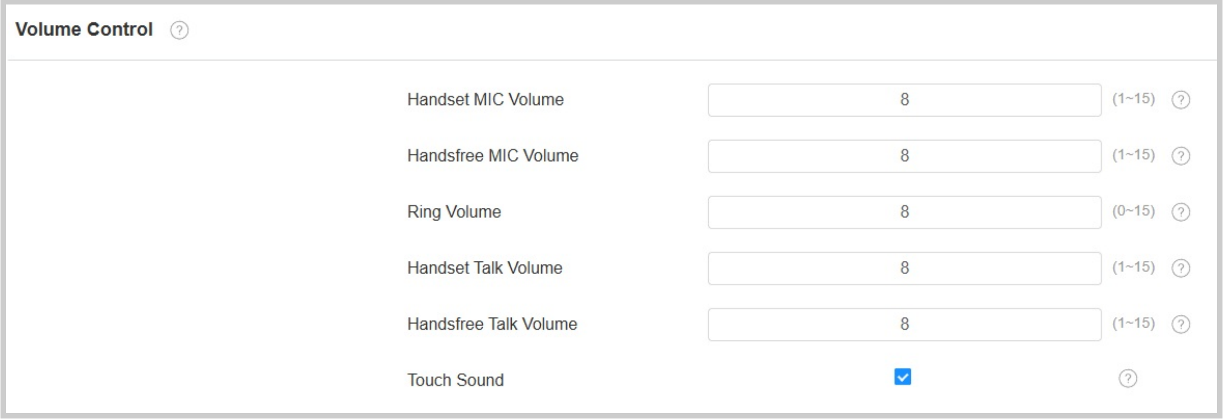
Doorbell Duration 30 Sec

Bell in Camera None

- **Ringtone**: Select the doorbell sound.
- **Doorbell Duration:** Set the doorbell duration(from 10 seconds to 5 minutes).
- **Bell In Camera**: Select the camera to be triggered along with the doorbell.

On the Web Interface

You can configure volumes on the **Device > Audio** interface.



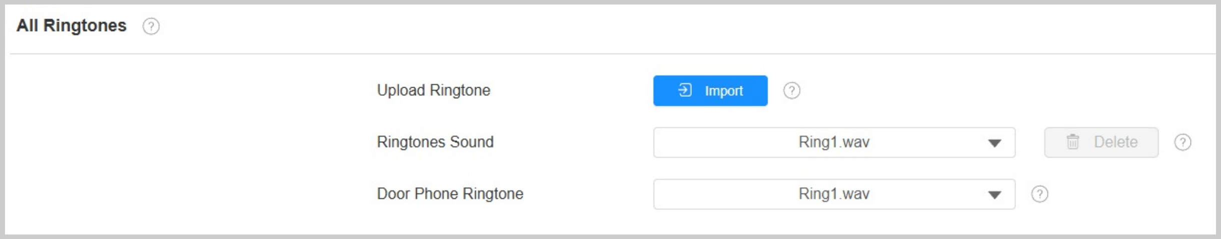
Volume Control

Handset MIC Volume	8	(1~15)
Handsfree MIC Volume	8	(1~15)
Ring Volume	8	(0~15)
Handset Talk Volume	8	(1~15)
Handsfree Talk Volume	8	(1~15)
Touch Sound	☑	

- **MIC Volume**: The microphone volume.
- **Ring Volume**: The incoming call ringtone volume.
- **Talk Volume**: The speaker volume during the call.
- **Touch Sound**: The icon tapping sound.

Upload Tones

You can customize ringtones on the **Device > Audio** interface. Click **Import** to upload the ringtone and **Delete** to delete the existing one.



All Ringtones

Upload Ringtone: Import

Ringtones Sound: Ring1.wav

Door Phone Ringtone: Ring1.wav

Note

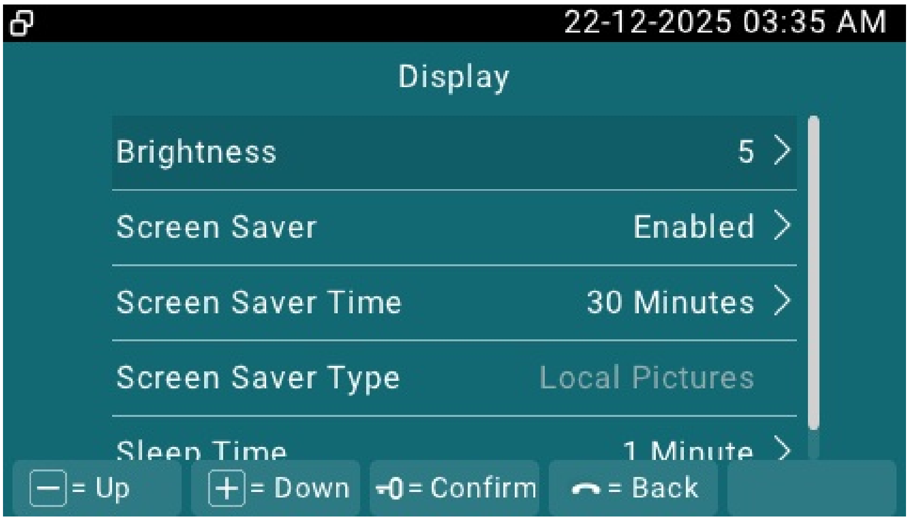
File Format: WAV; Max Size: 250 KB; File Name: Less than 8 Chinese characters or 23 characters, &'` characters are not supported; Sample Rate: 8,000 Hz; Bit Rate: 64 kbps; Channels: Mono; Audio Codec: PCMU or PCM.

Screen Display

On the Device

You can configure a variety of features of the screen display in terms of brightness, screen saver and font size, etc.

Set up the screen display on the **Settings > Display** screen.



22-12-2025 03:35 AM

Display

Brightness 5

Screen Saver Enabled

Screen Saver Time 30 Minutes

Screen Saver Type Local Pictures

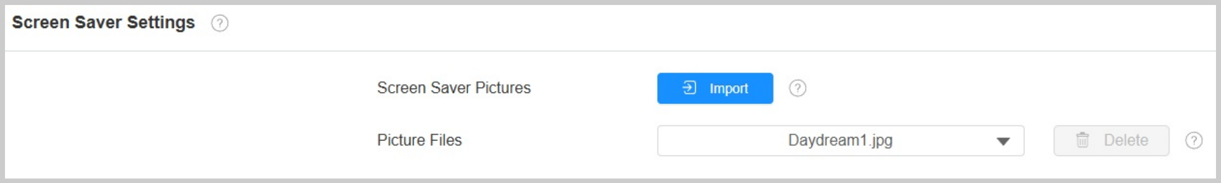
Sleep Time 1 Minute

- **Brightness**: Select the brightness value. The default is 5. The higher the value, the brighter the screen.
- **Screen Saver**: Determine whether to display the screensaver when the device goes into sleep mode.
- **Screen Saver Time**: The time for displaying the screensaver.
- **Screen Saver Type**:
  - **SDMC Pictures:** Display pictures uploaded to the SDMC.
  - **Local Pictures:** Display pictures uploaded to the indoor monitor as the screen saver.
- **Sleep Time**: Set the sleep timing based on the screen saver (15 seconds to 30 minutes).
  - If the screen saver is enabled, the sleep time here is the screen saver start time. For example, if you set it to 1 minute, the screen saver will start automatically when the device has no operation for 1 minute.

- If the screen saver is disabled, the sleep time here is the screen turn-off time. For example, if you set it to 1 minute, the screen will be turned off automatically when the device has no operation for 1 minute.

On the Web Interface

You can upload screen saver pictures on the **Device > Display Settings > Screen Saver Settings** interface.


Screen Saver Settings

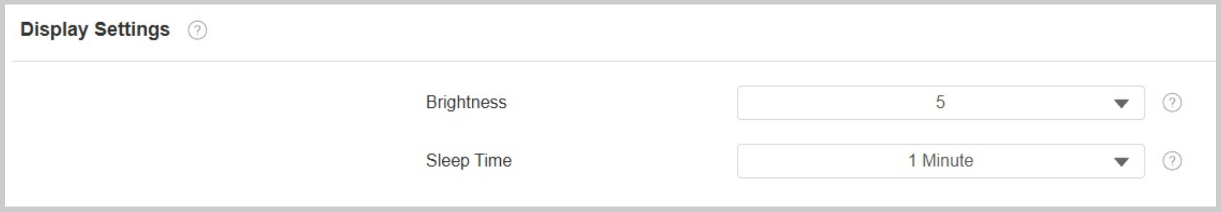
Screen Saver Pictures

Picture Files: Daydream1.jpg

- **Screen Saver Pictures**: Max Size:256K; Format: 480x272 jpg; File name can only contain digits, letters, and "_".

> **Note**
>
> Previous pictures with the same ID will be overwritten if they are designated again.

You can set the screen brightness and sleep time on the **Device > Display Settings> Display Settings** interface.


Display Settings

Brightness: 5

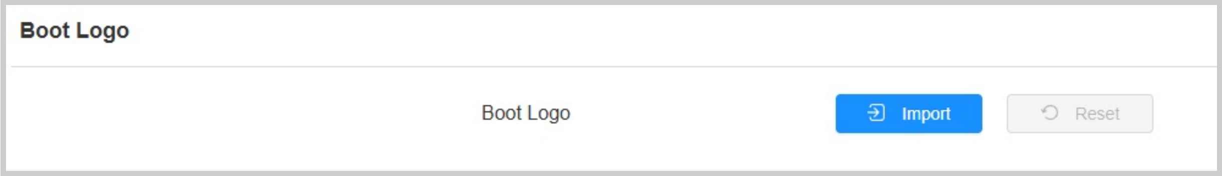
Sleep Time: 1 Minute

- **Brightness**: Select the brightness value. The default is 5. The higher the value, the brighter the screen.
- **Sleep Time**: If the screen saver is enabled, the sleep time is the screen saver's start time. For example, if you set it to 1 minute, the screen saver will start automatically when the device has no operation for 1 minute. If the screen saver is disabled, the screen will be turned off automatically when the device has not been used for 1 minute.

Upload Device Booting Image

You can upload the booting image to be displayed during the device’s booting process.

Navigate to **Device > Display Settings> Boot Logo** interface.



Boot Logo

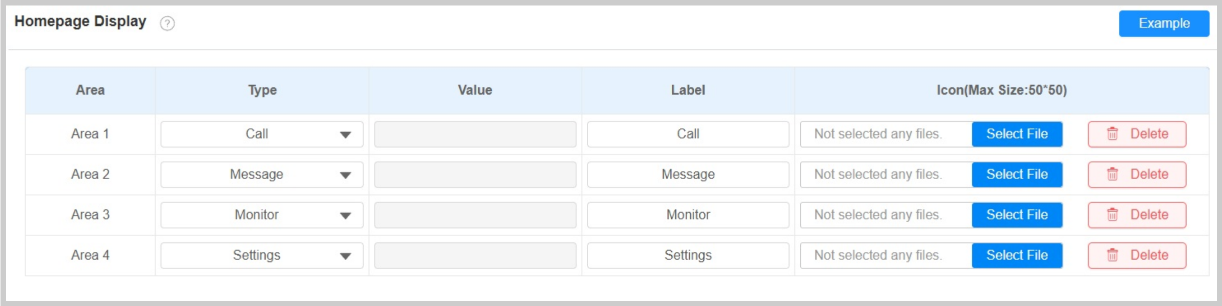
Boot Logo

- **Boot Logo**: Max size:100K; Format:480×272 jpg; File name can only contain digits, letters, and “_”.

Home Screen Tab Display

Akuvox indoor monitor allows you to customize icon display on the home screen for the convenience of users' operation.

To set it up, navigate to **Device > Display Settings** interface.



Homepage Display

Area	Type	Value	Label	Icon(Max Size:50*50)
Area 1	Call		Call	Not selected any files. Select File Delete
Area 2	Message		Message	Not selected any files. Select File Delete
Area 3	Monitor		Monitor	Not selected any files. Select File Delete
Area 4	Settings		Settings	Not selected any files. Select File Delete

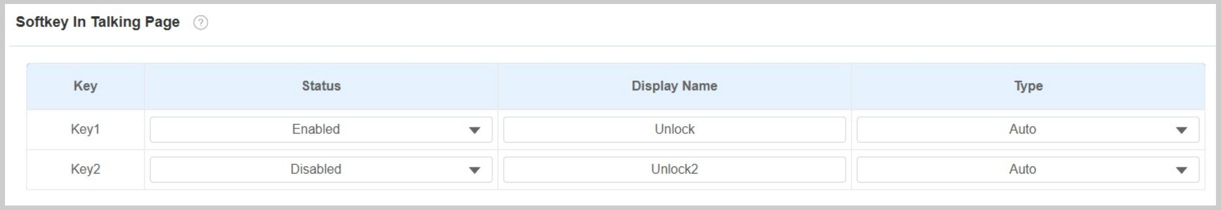
- **Type**: Select the functional icon to be displayed on the home screen.
  - **All Call/All Call 1-3**: Tap to initiate multicast calls. When **All Call** is selected, and more than one multicast group is configured, users can choose the desired group after tapping All Call. All Call 1-3 correspond to the multicast groups 1 to 3.
- **Label**: Name the icon. The DND icon cannot be renamed.
- **Type**: Click to upload the icon picture. The maximum icon size is 50×50. The picture format can be JPG, JPEG, or PNG.

You can click **Example** to see the icon layout.

Unlock Tab Configuration

You can customize the unlock tab and select the relay type on the talking, monitor, and call preview screen for the door opening.

To set up the unlock tab on the talking screen, go to **Device > Relay > SoftKey In Talking Page** interface.

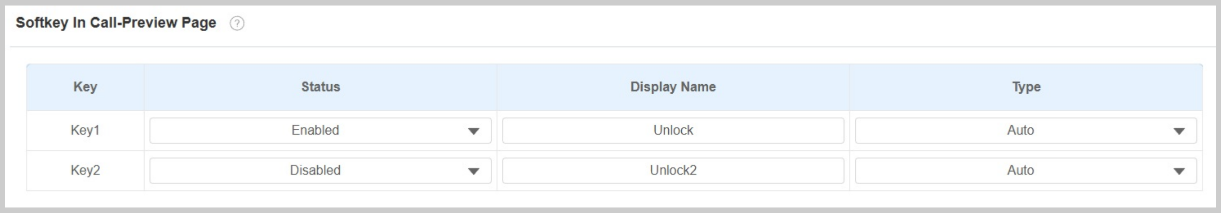


Softkey In Talking Page

Key	Status	Display Name	Type
Key1	Enabled	Unlock	Auto
Key2	Disabled	Unlock2	Auto

- **Status**: With it enabled, the unlock tab will be displayed on the talking screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up the unlock tab on the **Call Preview** screen.

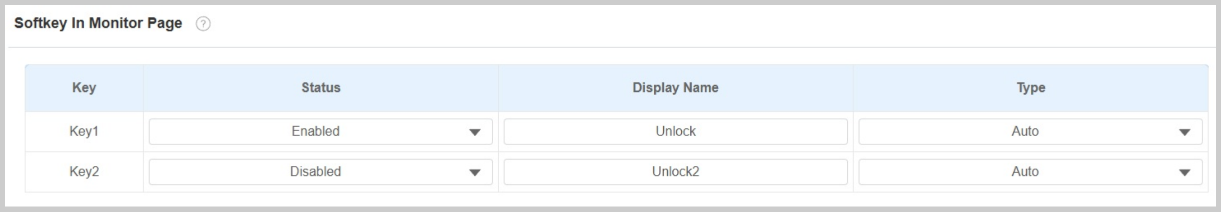


Softkey In Call-Preview Page

Key	Status	Display Name	Type
Key1	Enabled	Unlock	Auto
Key2	Disabled	Unlock2	Auto

- **Status**: With it enabled, the unlock tab will be displayed on the call-preview screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up unlock tabs on the **Monitor** screen.

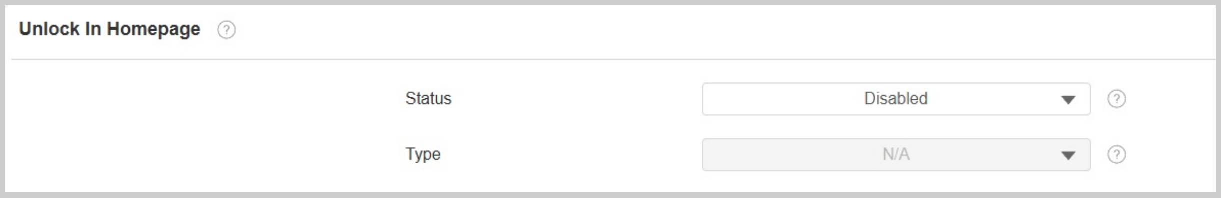


Softkey In Monitor Page

Key	Status	Display Name	Type
Key1	Enabled	Unlock	Auto
Key2	Disabled	Unlock2	Auto

- **Status**: With it enabled, the unlock tab will be displayed on the monitoring screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up the unlock button ⊸0 .



Unlock In Homepage

Status	Disabled
Type	N/A

- **Status**: It is enabled by default.
- **Type**: Select the relay trigger type according to the actual setup.

> **Note**
>
> Please refer to the **Access Control Configuration** chapter for different unlock types setup.

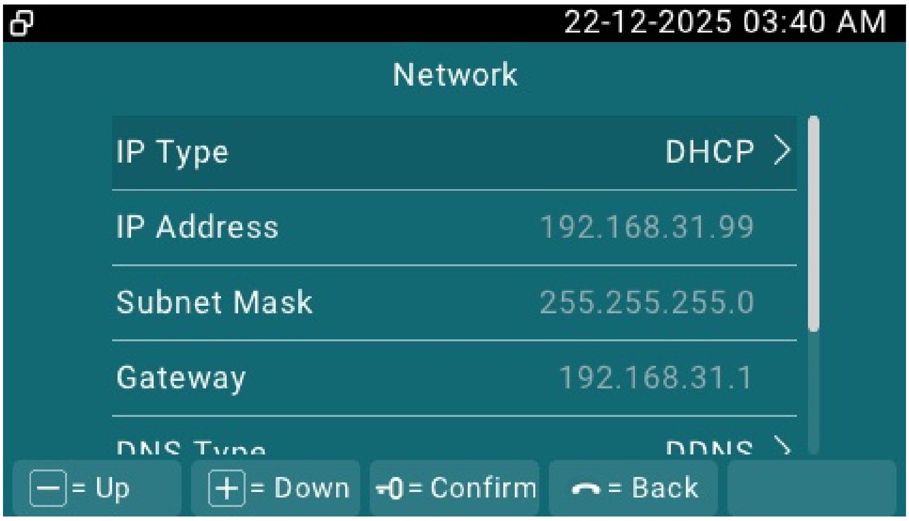
Network Setting

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.

On the Device

Check and configure the network connection on the device **Settings > Advanced > Network** screen.



22-12-2025 03:40 AM

Network

IP Type DHCP

IP Address 192.168.31.99

Subnet Mask 255.255.255.0

Gateway 192.168.31.1

DNS Type DDNS

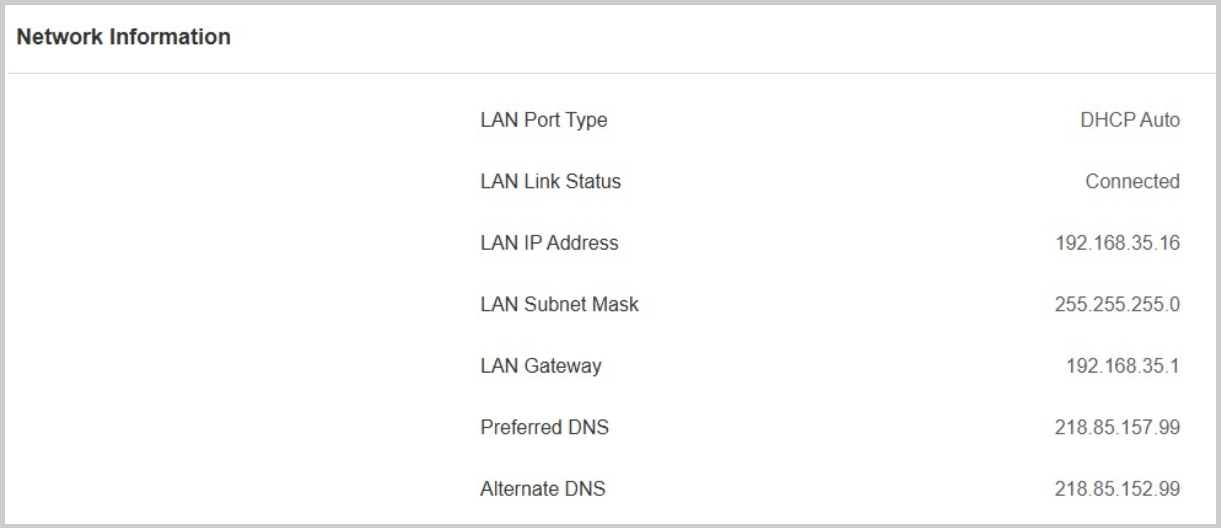
- **IP Type:** DHCP mode is the default network connection. The device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. In static IP mode, the IP address, subnet mask, default gateway, and DNS server address have to be manually 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.

- **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.
- **DNS Type**: 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.
    - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
    - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred & Alternate DNS Server**: The preferred and alternative Domain Name Server(DNS). The device will connect to the alternative server when the primary server is unavailable.

> **Note**
>
> - You can go to **Settings > Status > Network** screen to check device network status.
> - To access advanced settings, the default password is 123456.

On the Web Interface

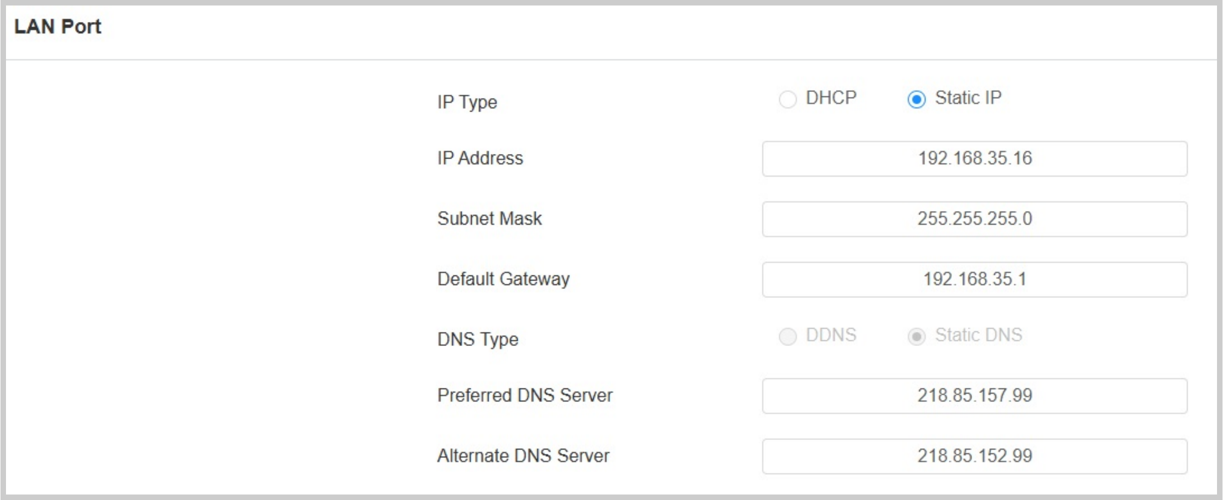
Check the network on the web **Status > Network Information** interface.



Network Information

LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.35.16
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.35.1
Preferred DNS	218.85.157.99
Alternate DNS	218.85.152.99

Check and configure the network connection on the web **Network > Basic > LAN Port** interface.



LAN Port

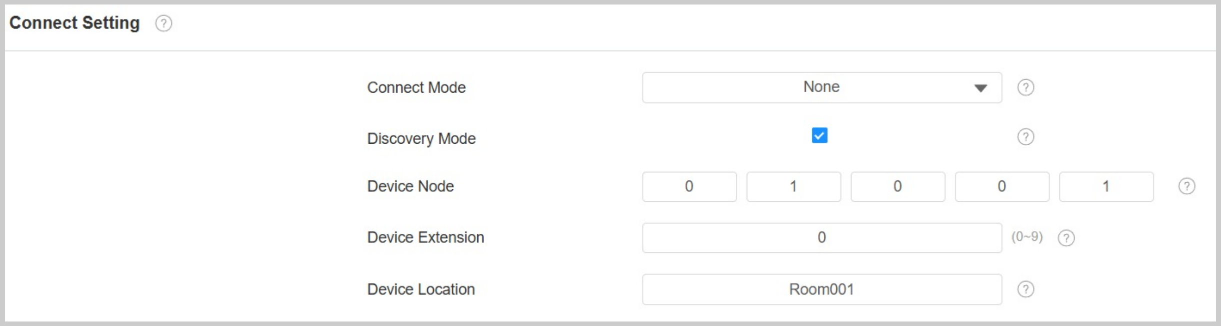
IP Type	○ DHCP ● Static IP
IP Address	192.168.35.16
Subnet Mask	255.255.255.0
Default Gateway	192.168.35.1
DNS Type	○ DDNS ● Static DNS
Preferred DNS Server	218.85.157.99
Alternate DNS Server	218.85.152.99

- **IP Type**:
  - **DHCP** mode will enable the indoor monitor to be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
  - **Static IP** allows you to enter the IP address, subnet mask, default gateway, and DNS address manually 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.
- **DNS Type**: 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.
  - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
  - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred/Alternate DNS Server**: The device will connect to the alternative server when the primary server 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 > Connect Setting** interface.



Connect Setting

Connect Mode: None

Discovery Mode: ☑

Device Node: 0 1 0 0 1

Device Extension: 0 (0~9)

Device Location: Room001

- **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**.
  - **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**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.

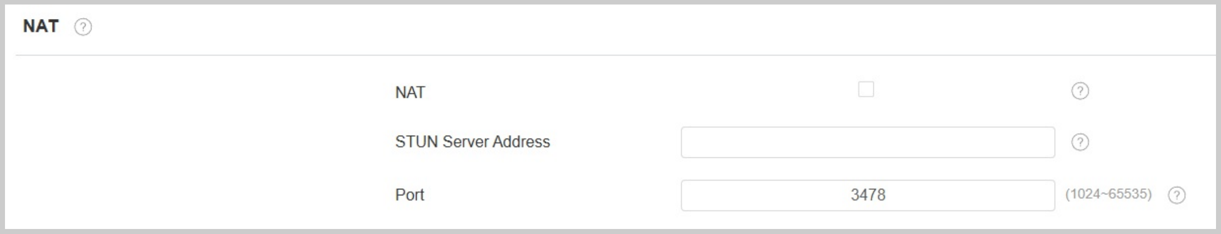
- **Device Node**: Available for **None** server mode. It can be used to call the device. Specify the device address by entering device location information from left to right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for **None** server mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for **None** server mode.

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 set up NAT, go to **Account> Basic > NAT** interface.



NAT

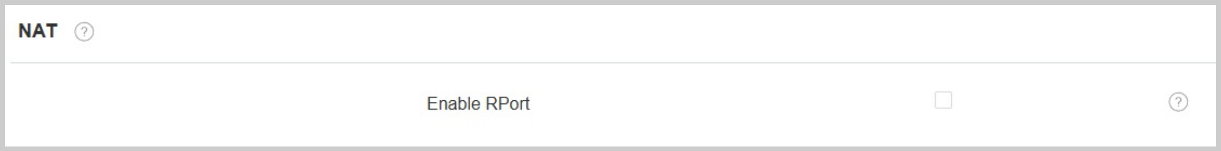
NAT □

STUN Server Address

Port 3478 (1024~65535)

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

Then go to **Account > Advanced > NAT** interface.



NAT

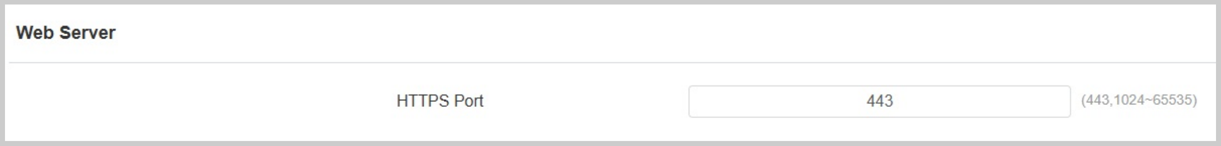
Enable RPort □

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

Device Web HTTP Setting

This function manages device website access. The device supports the HTTPS remote access method.

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



Web Server

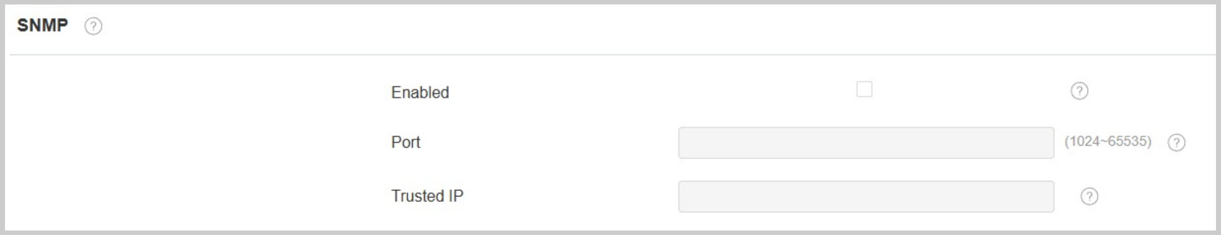
HTTPS Port 443 (443,1024~65535)

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

SNMP Setting

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

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



SNMP

Enabled □

Port (1024~65535)

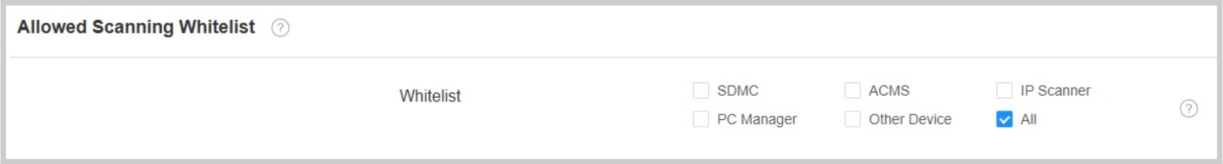
Trusted IP

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

Allowed Scanning Whitelist

You can limit devices from scanning the indoor monitor on the same LAN to enhance security.

Set it up on the **Network > Advanced > Allowed Scanning Whitelist** interface.



Allowed Scanning Whitelist

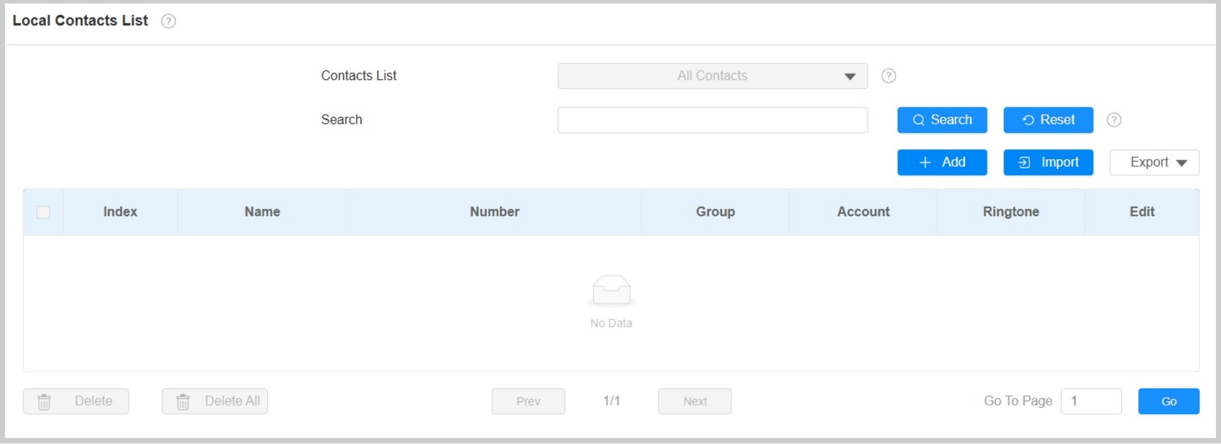
Whitelist ☐ SDMC ☐ ACMS ☐ IP Scanner ☐ PC Manager ☐ Other Device ☑ All

Contacts Configuration

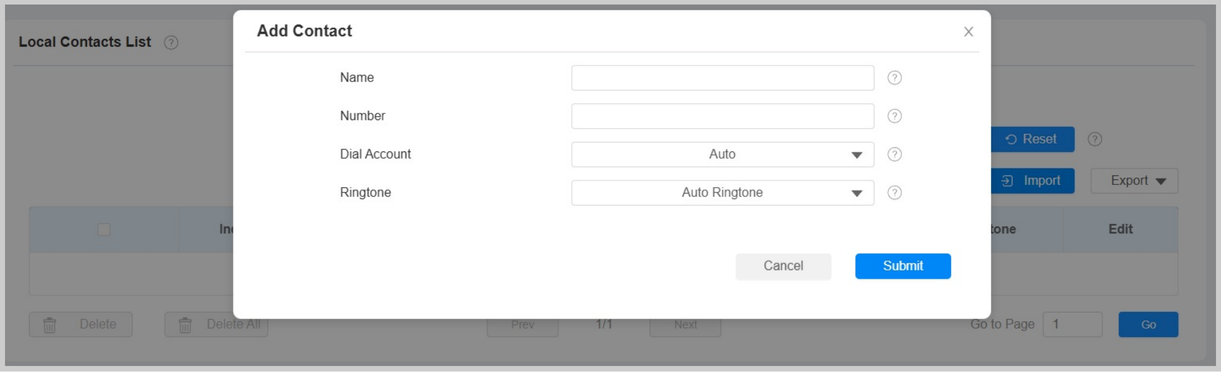
The local contact information is used to initiate SIP or IP calls to other intercom devices.

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, then click **+Add**. You can add up to 500 contacts.


Local Contacts List

Contacts List: All Contacts


Add Contact

Dial Account: Auto

Ringtone: Auto Ringtone

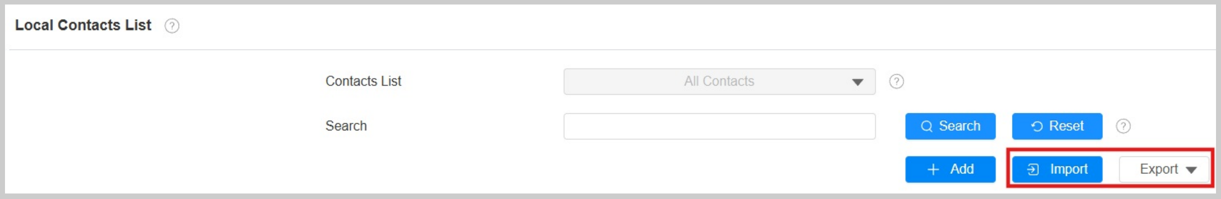
- **Contacts List**: **All Contacts** displays all the contacts in the contact list.
- **Search**: Search for a contact by its name or number.
- **Name**: The contact's name to distinguish it from others.
- **Number**: The SIP or IP number of the contact.
- **Dial Account**: The account to make the call, Account 1 or Account 2.

- **Ringtone**: The ringtone for the incoming call from the contact.

Import and Export Contacts

You can import and export contacts in batches. The file should be in .xml or .csv format.

To import or export contacts, go to **Contacts > Local Contacts > Local Contacts List** interface.



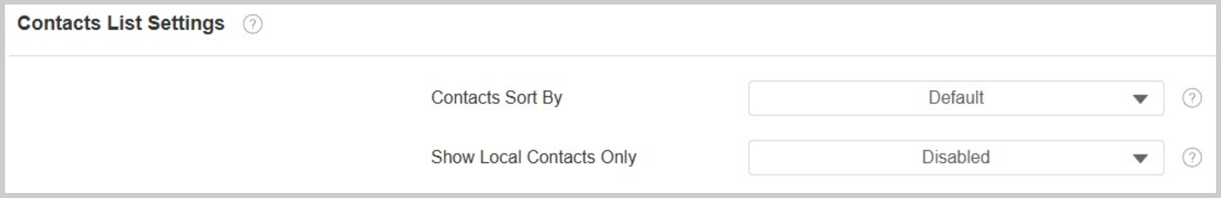
Local Contacts List

Contacts List: All Contacts

Search:

Contact List Display

To set up contact display, go to the **Contacts > Local Contacts > Contacts List Settings** interface.



Contacts List Settings

Contacts Sort By: Default

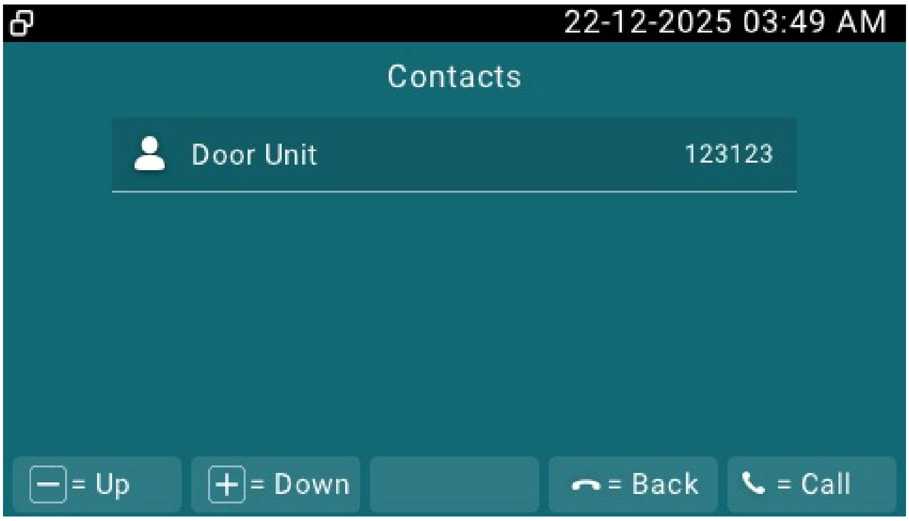
Show Local Contacts Only: Disabled

- **Contacts Sort By**:
    - **Default**: The local contacts will be displayed before those from SmartPlus, SDMC, etc.
    - **ASCII Code**: The contacts will be displayed in order based on the first letter of the contact names.
    - **Created Time**: The contacts will be displayed by their created time.
- **Show Local Contacts Only**: If enabled, only the local contacts will be displayed. If disabled, all the contacts from SmartPlus Cloud, SDMC, and so on will be displayed.

Intercom Call Configuration

Call Contacts

Go to the **Call > Contacts** screen. Select the desired contact and press the dial key to call.



22-12-2025 03:49 AM

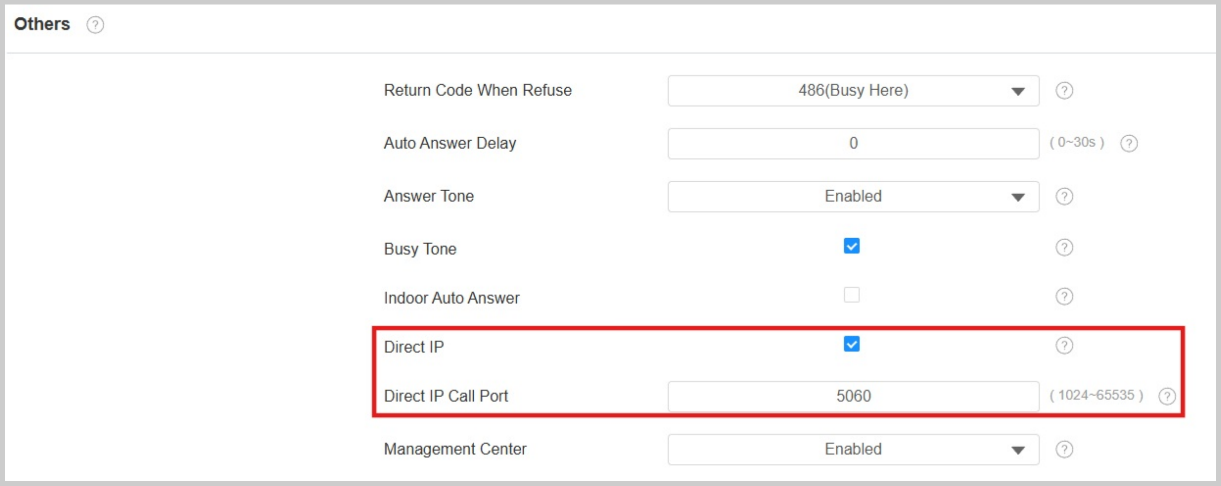
Contacts

Door Unit 123123

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.

To configure the IP call feature and port, go to the web **Device > Call Feature > Others** interface.



Others

Return Code When Refuse	486(Busy Here)	
Auto Answer Delay	0	(0~30s)
Answer Tone	Enabled	
Busy Tone	☑	
Indoor Auto Answer	□	
Direct IP	☑	
Direct IP Call Port	5060	(1024~65535)
Management Center	Enabled	

- **Direct IP Call**: If you do not allow direct IP calls to be made on the device, you can untick the check box to terminate the function.
- **Direct IP Call Port**: Set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

SIP Call 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.

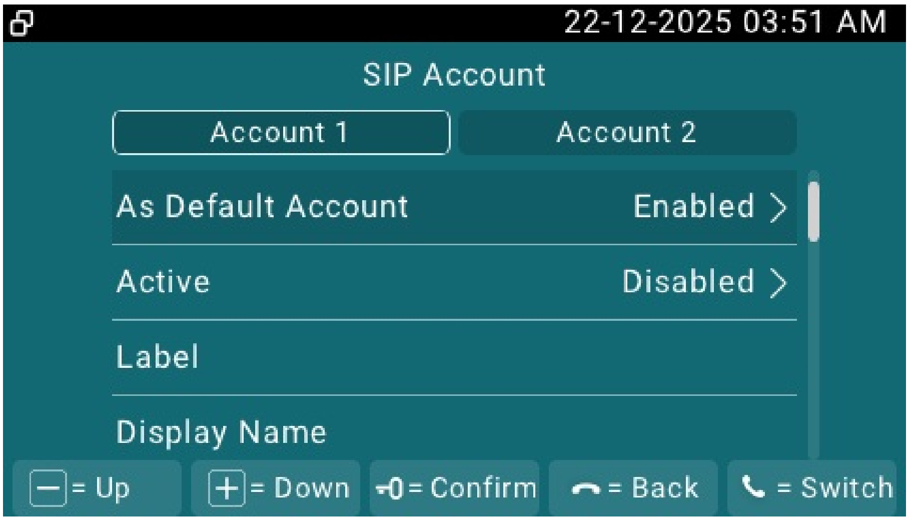
SIP Account Registration

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.

On the device screen, navigate to **Settings > Advanced > SIP Account** screen.



22-12-2025 03:51 AM

SIP Account

Account 1 | Account 2

As Default Account: Enabled

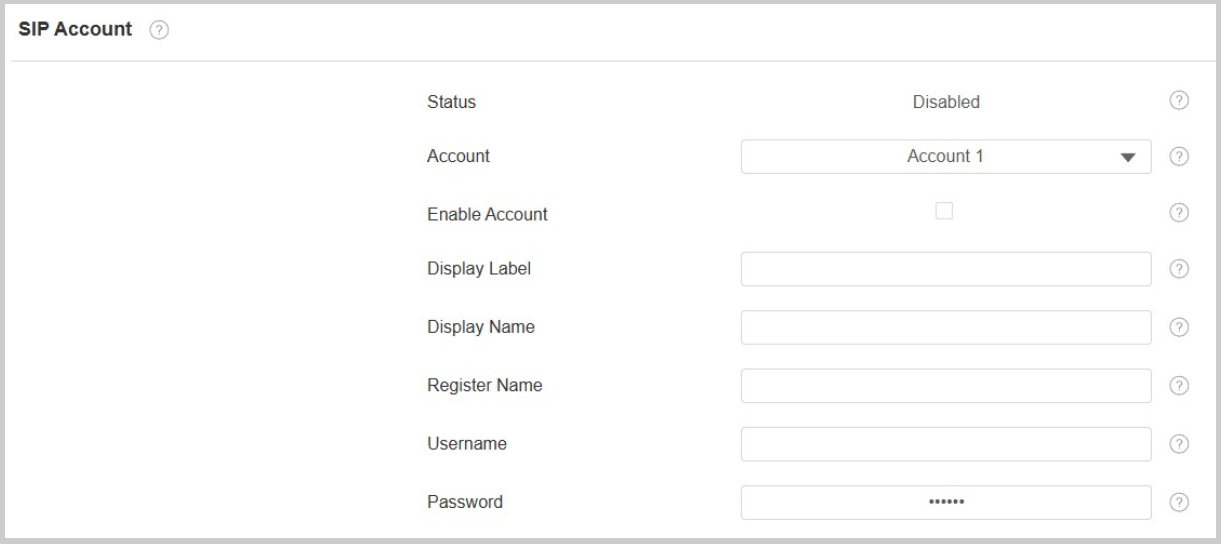
Active: Disabled

Label

Display Name

- **Account 1/Account 2:** The device supports 2 SIP accounts.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus Cloud service is activated.
  - The system switches to Account 2 if Account 1 is not registered.
- **Active**: Check to activate the registered SIP account.
- **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.

The SIP account registration can also be configured on the device web **Account > Basic > SIP Account** interface.



SIP Account

Status	Disabled
Account	Account 1 ▾
Enable Account	□
Display Label	
Display Name	
Register Name	
Username	
Password	••••••

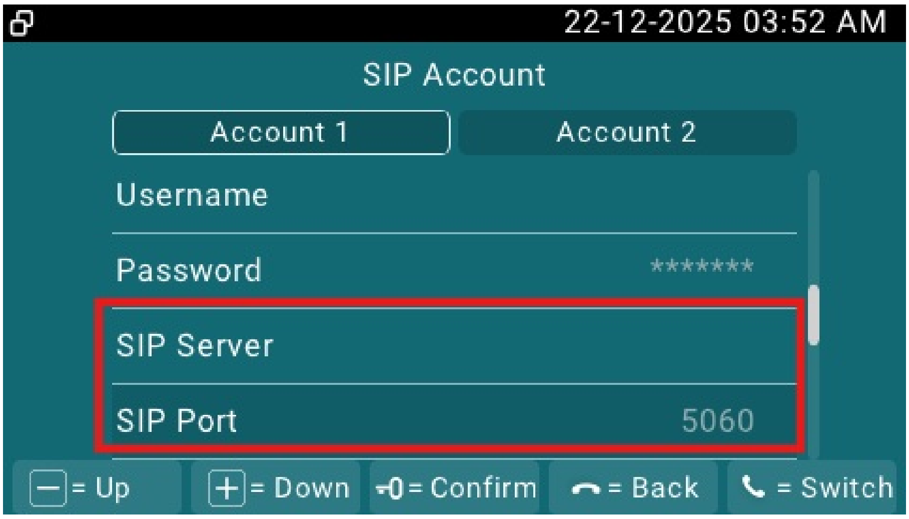
- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same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

> **Tip**
>
> When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

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.

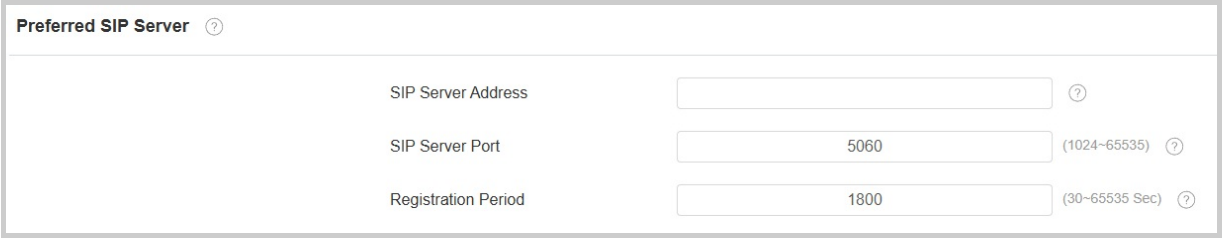
To set it up, go to **Settings > Advanced > SIP Account** screen or navigate to the web **Account > Basic** interface.



22-12-2025 03:52 AM

SIP Account

Username	
Password	*******
SIP Server	
SIP Port	5060



Preferred SIP Server

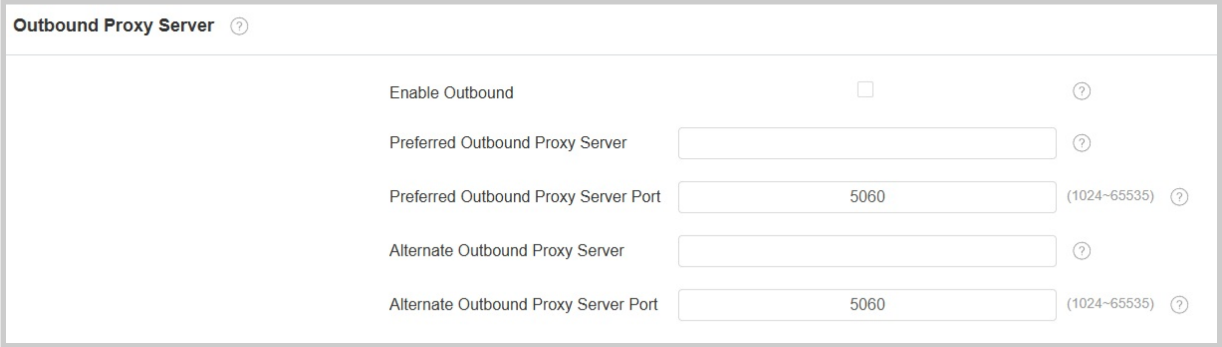
SIP Server Address			
SIP Server Port	5060	(1024~65535)	
Registration Period	1800	(30~65535 Sec)	

- **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.



Outbound Proxy Server

Enable Outbound	□	
Preferred Outbound Proxy Server		
Preferred Outbound Proxy Server Port	5060	(1024~65535)
Alternate Outbound Proxy Server		
Alternate Outbound Proxy Server Port	5060	(1024~65535)

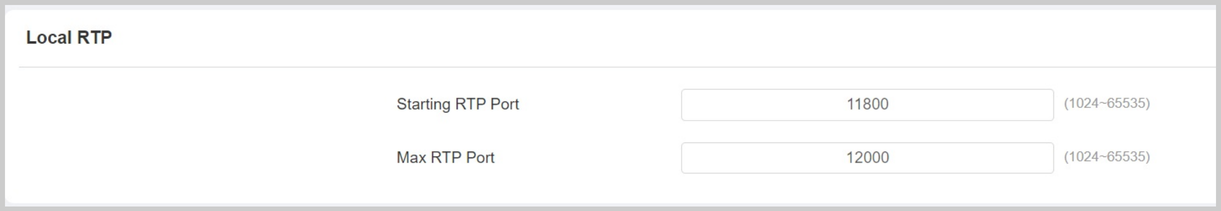
- **Preferred Outbound Proxy Server**: Enter the SIP proxy IP address.
- **Preferred Outbound Proxy Server Port**: Set the port for establishing a call session via the outbound proxy server.
- **Alternate Outbound Proxy Server**: Enter the SIP proxy IP address to be used when the main proxy malfunctions.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

Device Local RTP

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

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

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



Local RTP

Starting RTP Port: 11800 (1024~65535)

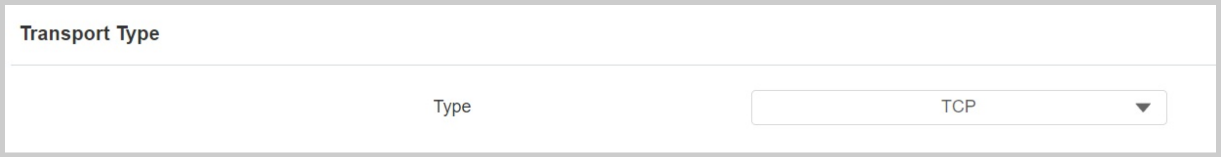
Max RTP Port: 12000 (1024~65535)

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

Data Transmission Type

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

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



Transport Type

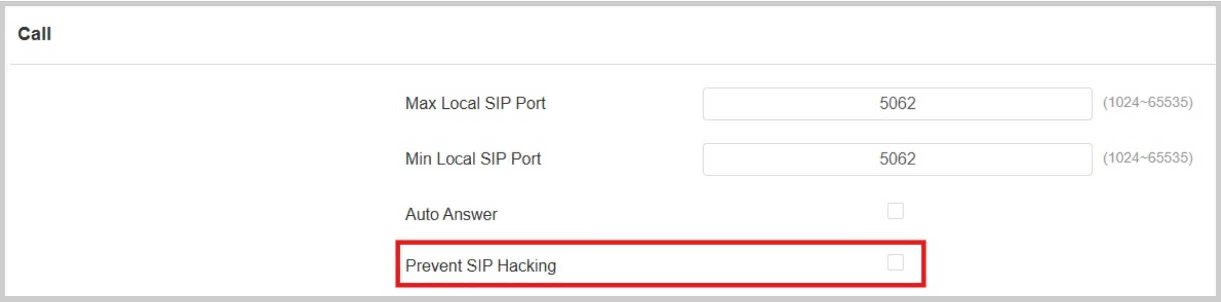
Type: TCP

- **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 secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.

SIP Hacking Protection

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

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



Call

Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Auto Answer	☐	
Prevent SIP Hacking	☐	

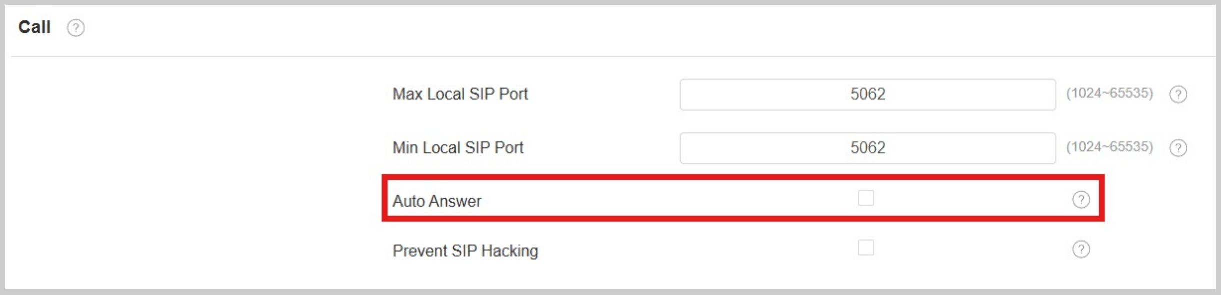
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Setting

Auto-answer Configuration

Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention.

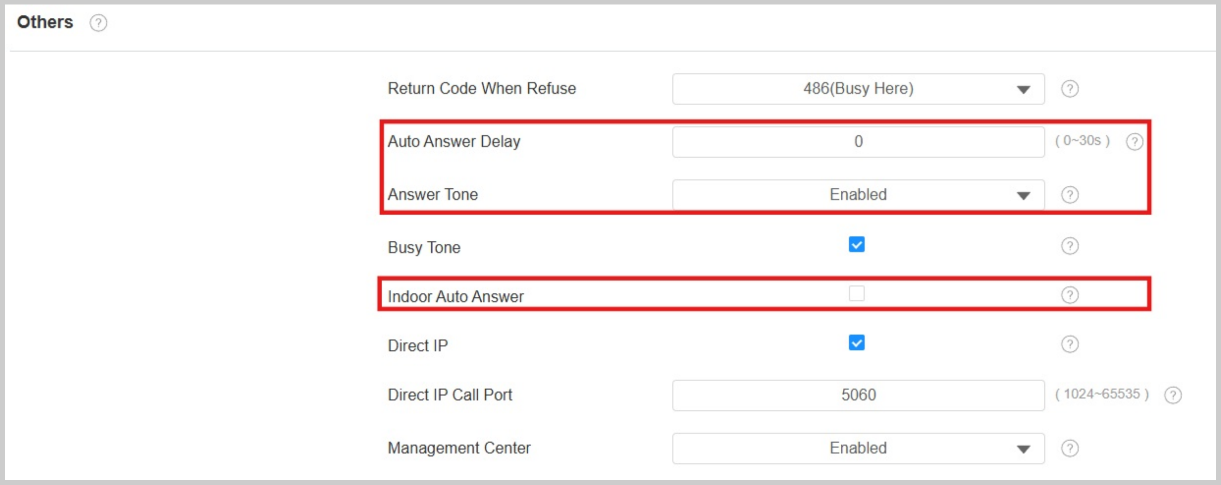
To enable the auto-answer feature, go to the web **Account > Advanced > Call** interface.



Call ?

Max Local SIP Port	5062	(1024~65535)	?
Min Local SIP Port	5062	(1024~65535)	?
Auto Answer	□		?
Prevent SIP Hacking	□		?

To set it up, go to the web **Device > Call Feature > Others** interface.



Others ?

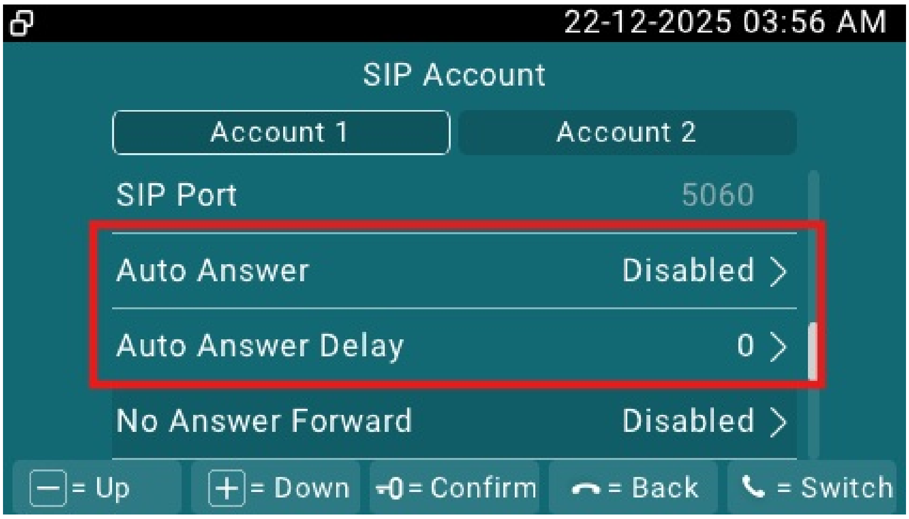
Return Code When Refuse	486(Busy Here)		?
Auto Answer Delay	0	(0~30s)	?
Answer Tone	Enabled		?
Busy Tone	☑		?
Indoor Auto Answer	□		?
Direct IP	☑		?
Direct IP Call Port	5060	(1024~65535)	?
Management Center	Enabled		?

- **Auto Answer Delay:** Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the device will answer the call automatically after 5 seconds.
- **Answer Tone**: Select the tone for answering calls automatically.
- **Indoor Auto Answer**: Allow calls from other indoor monitors to be answered by the device automatically.

Other Options:

- **Return Code When Refuse**: Decide the code sent to the caller side via the SIP server when rejecting the incoming call.
- **Busy Tone**: Decide whether to sound a busy tone when a call is hung up by the callee.
- **Management Center**: Decide whether to generate the contact labeled Management Center.
    - When the device is deployed on the SmartPlus Cloud, the cloud system will issue the SmartPlus Property Manager App and the guard phone R49 as a contact labeled Management Center. When this function is disabled, the PM App and guard phone will be displayed as contacts separately.
    - When the device is deployed on the SDMC, SDMC is shown as Management Center on the device screen. When the function is disabled, no contacts will be displayed as Management Center.

You can also set up the auto-answer feature on the **Settings > Advanced > SIP Account** screen.



22-12-2025 03:56 AM

SIP Account

Account 1 | Account 2

SIP Port 5060

Auto Answer Disabled

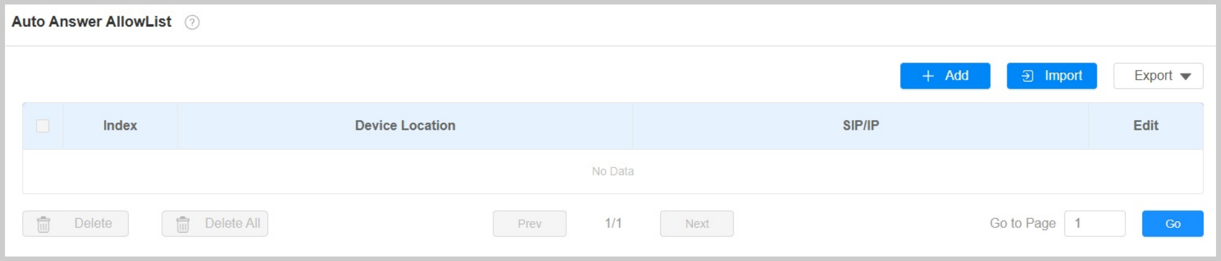
Auto Answer Delay 0

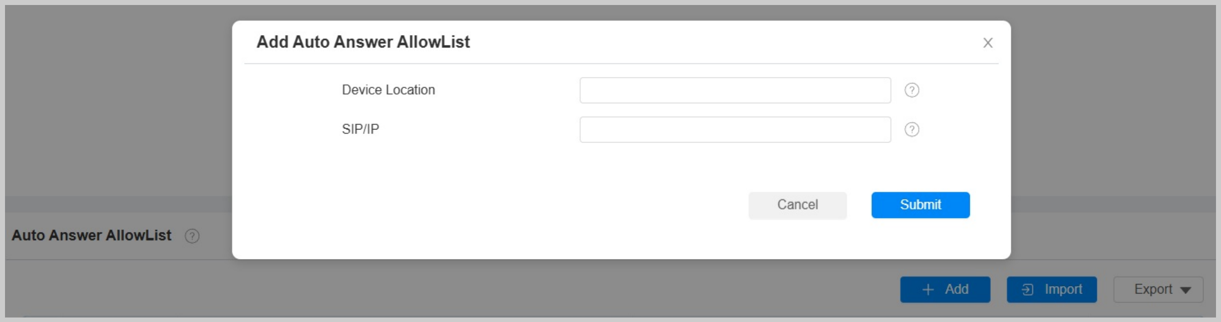
No Answer Forward Disabled

Auto-answer Allowlist Setting

Auto-answer can only be applicable to the SIP or IP numbers that are already added in the auto-answer allow list of your indoor monitor. Therefore, you are required to configure or edit the numbers in the allow list on the web interface.

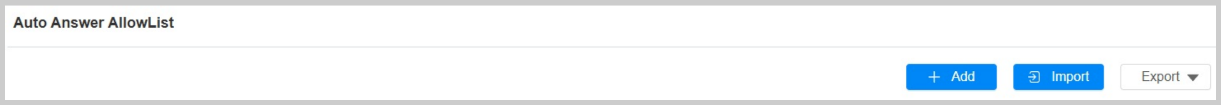
To set it up, go to the **Device > Call Feature > Auto Answer AllowList** interface. Click **+Add** to add the allowed device.





- **Device Location**: Specify the allowed device's name or location.
- **SIP/IP**: Enter the allowed device's SIP or IP number.

You can import and export the auto-answer allowlist for quick setup.

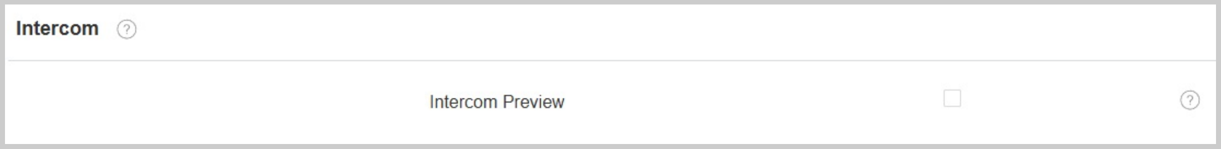


Note

- SIP/IP number files to be imported or exported must be in either .xml or .csv format.
- SIP/IP numbers must be set up in the contacts of the indoor monitor before they can be valid for the auto-answer function.

Intercom Preview

To see the image at the door station before answering the incoming call, you can enable the intercom preview function on the web **Device > Intercom > Intercom** interface.



Intercom

Intercom Preview □

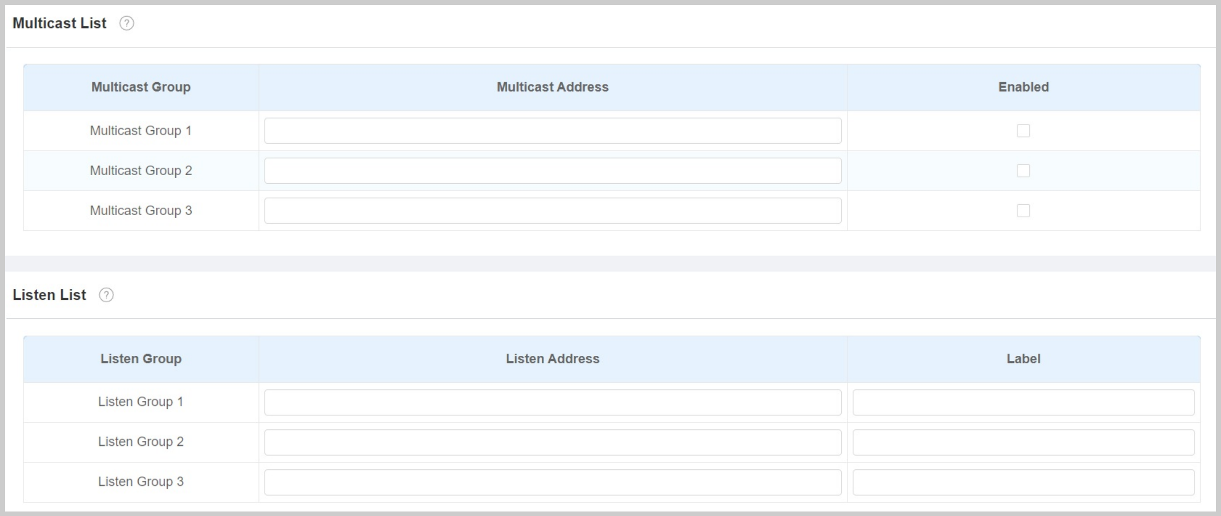
- **Intercom Preview**: It is disabled by default. When it is enabled, the group call is not available. Enabling the **Intercom Preview** option or not depends on whether the other party features RTSP.
    - For devices without RTSP: Enable this option. The indoor monitor will automatically answer incoming calls and display the live stream on the preview screen.
    - For devices with RTSP: Disable this option, as RTSP already provides real-time audio and video for intercom preview.

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.

To set it up, go to the web **Device > Multicast** interface.



Multicast List

Multicast Group	Multicast Address	Enabled
Multicast Group 1		□
Multicast Group 2		□
Multicast Group 3		□

Listen List

Listen Group	Listen Address	Label
Listen Group 1		
Listen Group 2		
Listen Group 3		

- **Multicast Address**: The multicast IP address is the same as the listen address.

- **Listen Address**: The listen address is the same as the multicast address.
- **Label**: The label name will be shown on the calling screen.

> **Note**
>
> The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult Akuvox tech team for more information.

Call Forwarding

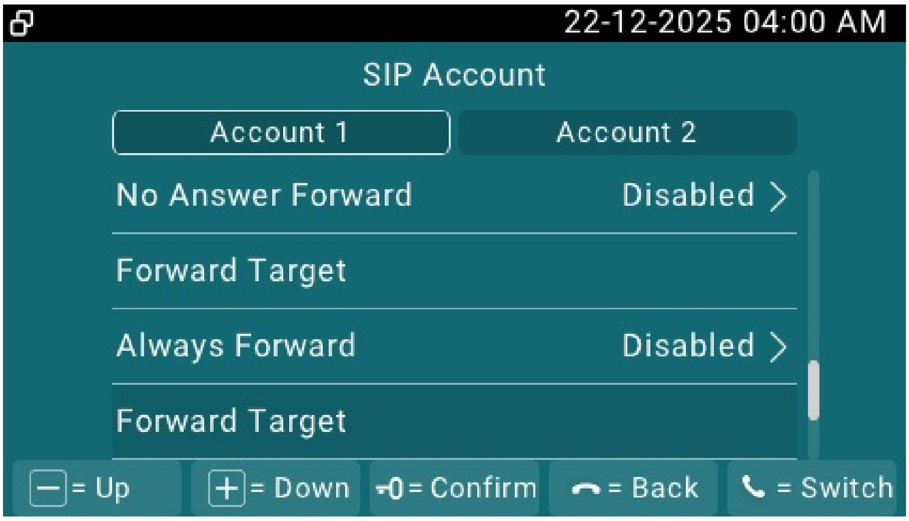
Call Forward is a feature that allows for transferring incoming calls to another number. Users can set up call forwarding according to different situations, such as always forwarding calls, forwarding calls when the indoor monitor is busy, or when it doesn't pick up the call.

On the Device

To set it up for SIP calls, go to the **Settings > Advanced > SIP Account** screen.

To set it up for IP calls, go to the **Settings > Advanced > Direct IP** screen.

You can enable/disable the call forward feature, but not set the target numbers on the device screen.



SIP Account

No Answer Forward: Disabled

Forward Target

Always Forward: Disabled

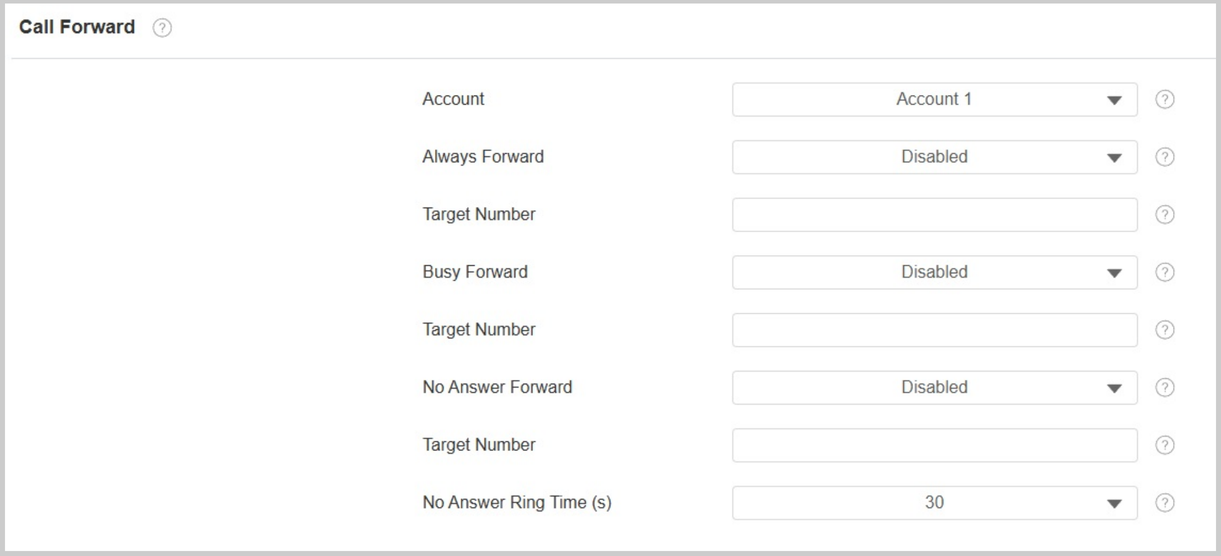
Forward Target

- **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.
- **Forward Target**: Display the forward number that is configured on the web interface.
- **No Answer Ring Time(Sec)**: The time ranges from 0-120 seconds. This option is available when **No Answer Forward** is enabled on the web interface.

On the Web Interface

Set up the forward function on the web **Device > Call Feature > Call Forward** interface.



Call Forward

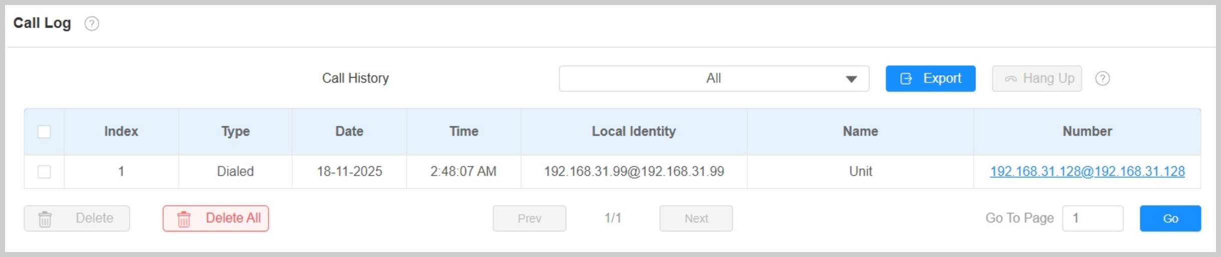
Account	Account 1
Always Forward	Disabled
Target Number	
Busy Forward	Disabled
Target Number	
No Answer Forward	Disabled
Target Number	
No Answer Ring Time (s)	30

- **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**: The specific forward number when Always Forward, Busy Forward, or No Answer Forward is enabled.
- **No Answer Ring Time(s)**: The time ranges from 0-120 seconds.

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.

To set it up, go to the **Contacts > Call Log** interface. The device supports up to 100 local call logs.



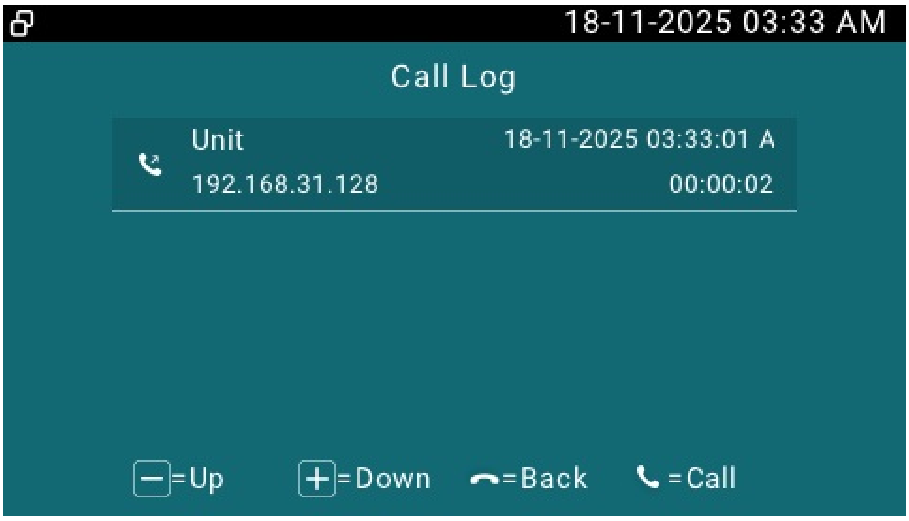
Call History: All

	Index	Type	Date	Time	Local Identity	Name	Number
□	1	Dialed	18-11-2025	2:48:07 AM	192.168.31.99@192.168.31.99	Unit	192.168.31.128@192.168.31.128

Go To Page: 1

- **Call History**: There are five types of call history: All, Dialed, Received, Missed, and Forwarded.

To check call logs on the device, tap **Call > Call Log**.



18-11-2025 03:33 AM

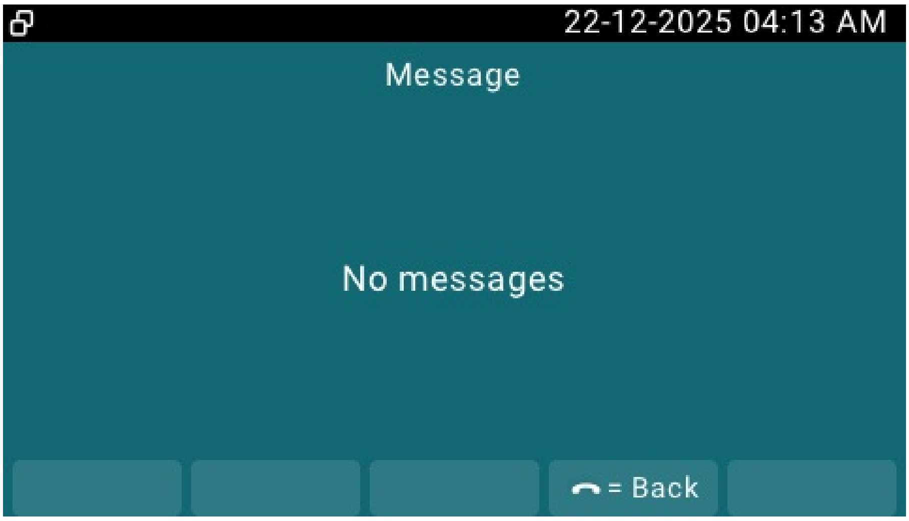
Call Log

Unit 18-11-2025 03:33:01 A
192.168.31.128 00:00:02

Intercom Message Setting

The device can receive messages when it is connected to the SmartPlus Cloud or SDMC. You can check messages on the **Messages** screen.

The device can store up to 100 messages.



22-12-2025 04:13 AM

Message

No messages

= Back

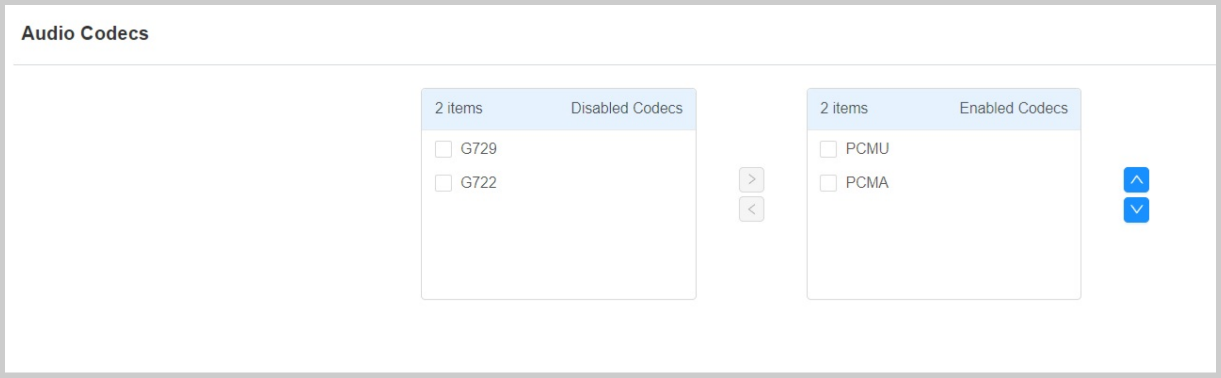
Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The device supports four types of codecs (PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each codec varies in terms of sound quality. Higher bandwidth means the device can capture more detail, leading to clearer sound and higher sample rates capture more data, reducing distortion and preserving sound quality.

You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

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


Audio Codecs

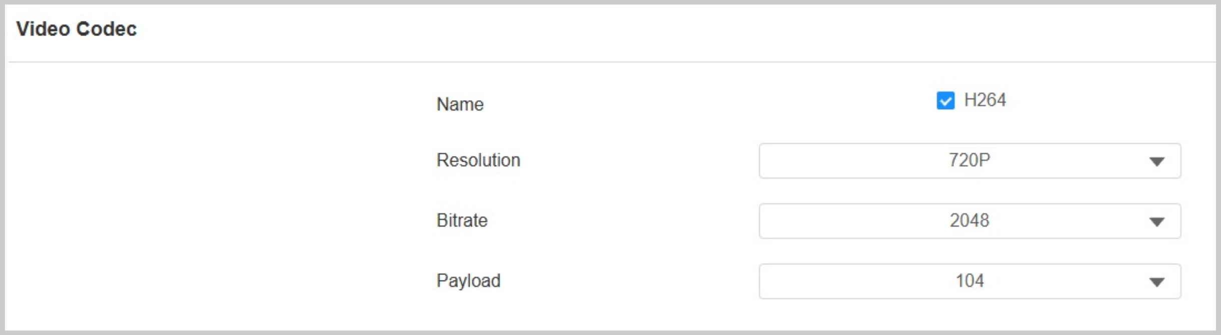
Please refer to the bandwidth consumption and sample rate for the codec types below:

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

Video Codec Configuration

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

To set it up, go to the web **Account > Advanced > Video Codec** interface.



Video Codec

Name	☑ H264
Resolution	720P
Bitrate	2048
Payload	104

- **Resolution**: Specify the code resolution for the video quality. The default is 720P(1280X720 pixels).
- **Bitrate**: Select the video stream bitrate. It varies by the resolution. The default is 2048.
- **Payload**: The payload ranges from 90-119 for the audio/video configuration file.

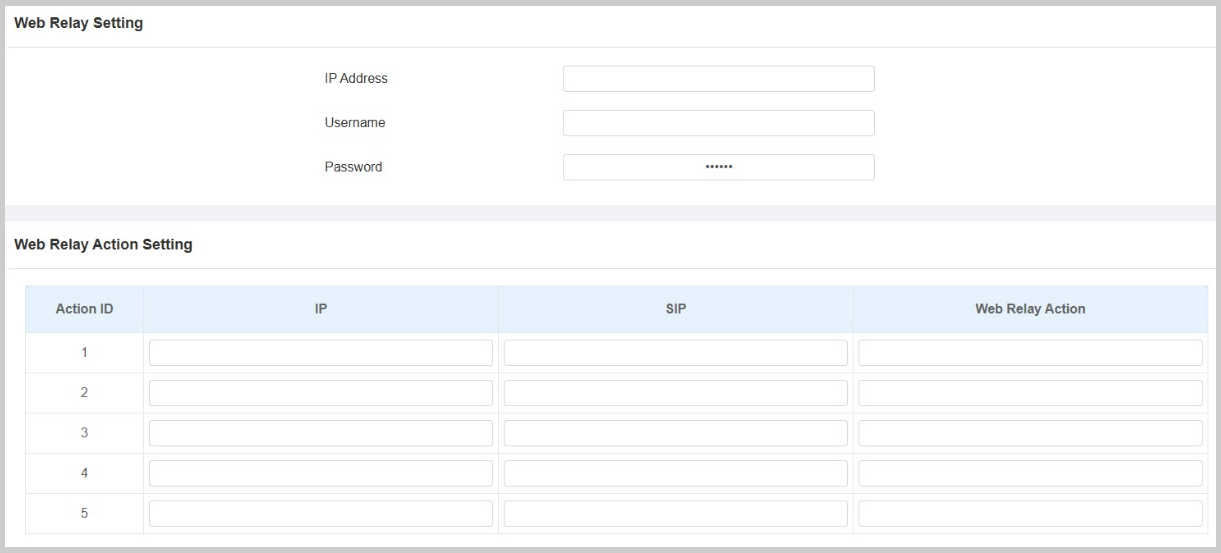
Access Control Configuration

Web Relay

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

Click here to view how to set up web relay.

To set it up, go to the web **Device > Relay > Web Relay** interface.



Web Relay Setting

IP Address	
Username	
Password	••••••

Web Relay Action Setting

Action ID	IP	SIP	Web Relay Action
1			
2			
3			
4			
5			

- **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.

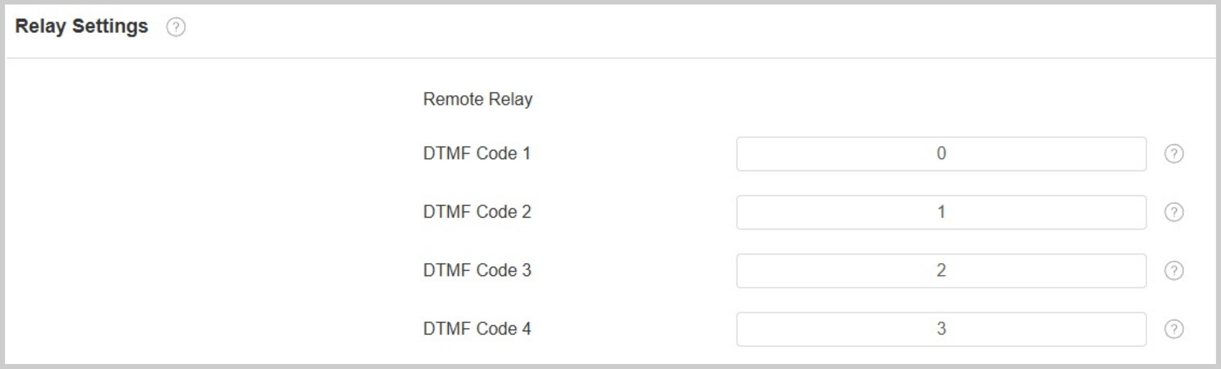
> **Note**
>
> If the URL includes full HTTP content(e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., "state.xml?relayState=2"), the relay uses the entered IP address.

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.

To set it up, go to **Device > Relay > Relay Setting** interface.



Relay Settings

Remote Relay

DTMF Code 1	0
DTMF Code 2	1
DTMF Code 3	2
DTMF Code 4	3

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

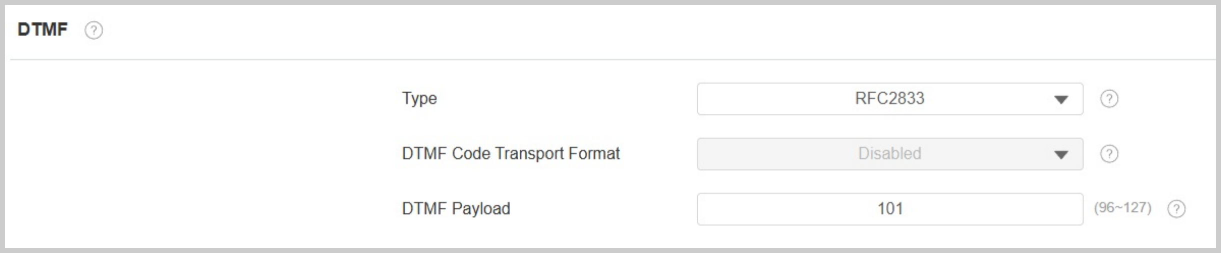
DTMF Transport Type

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

DTMF Type Differences:

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

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



DTMF

Type: RFC2833

DTMF Code Transport Format: Disabled

DTMF Payload: 101 (96~127)

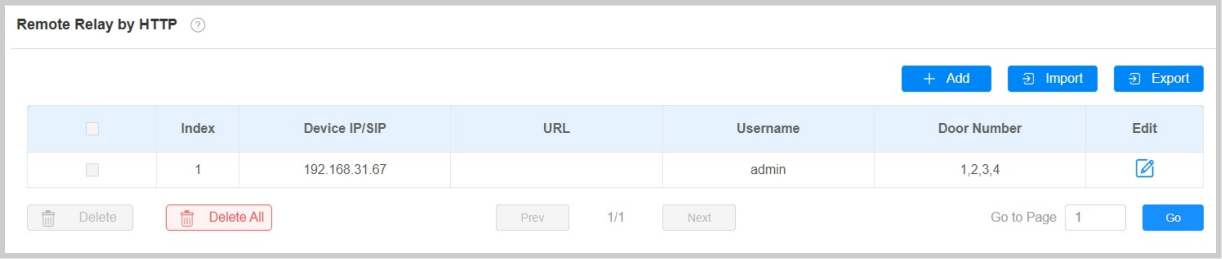
- **Type**: Select from the provided options.
- **DTMF Code Transport Format**: There are four options: Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via 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.

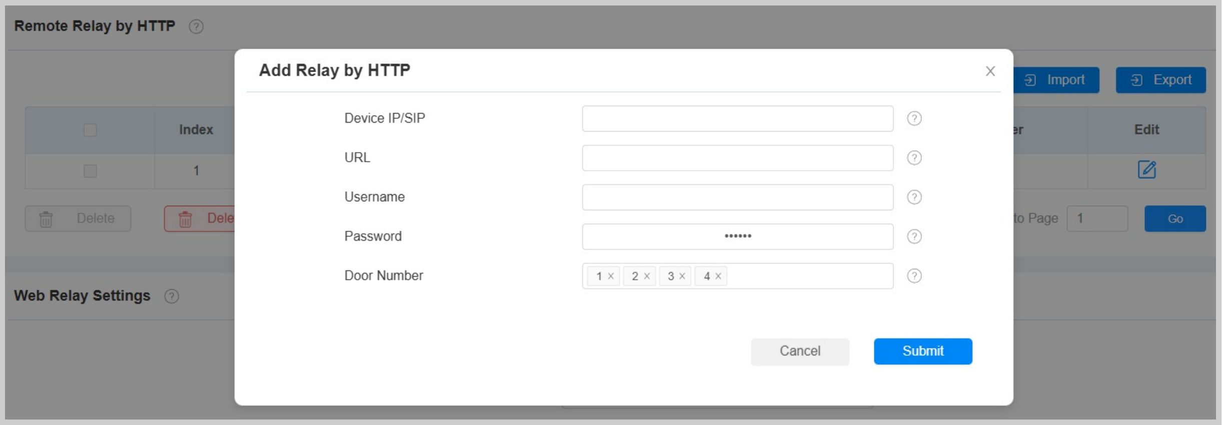
Go to the web **Device > Relay > Remote Relay By HTTP** interface.



Remote Relay by HTTP

□	Index	Device IP/SIP	URL	Username	Door Number	Edit
□	1	192.168.31.67		admin	1,2,3,4	✎

Click **Add** to add an HTTP command.



Add Relay by HTTP

Device IP/SIP:

URL:

Username:

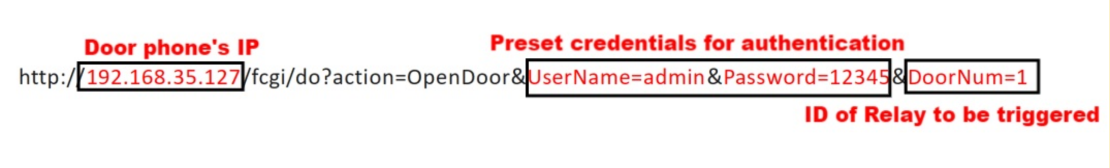
Password: ••••••

Door Number: 1 × 2 × 3 × 4 ×

- **Device IP/SIP**: Specify the IP or SIP number of the door phone.
- **URL**: Enter the HTTP URL.
- **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 Number**: Specify the door to be opened.

Tip

Here is an HTTP command URL example for relay triggering.



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

Door phone's IP
Preset credentials for authentication
ID of Relay to be triggered

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.

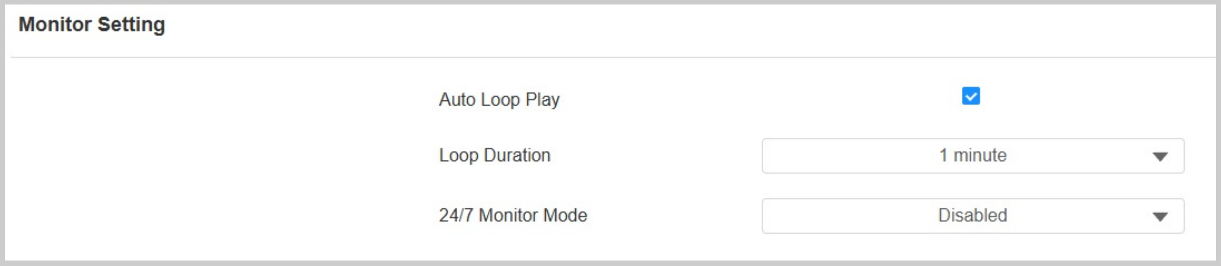
Security

Monitor and Image

Monitor Setting

You can add video streams using RTSP. If the Display in Call function is enabled, the video of the added monitor device will show up when it calls the indoor monitor.

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

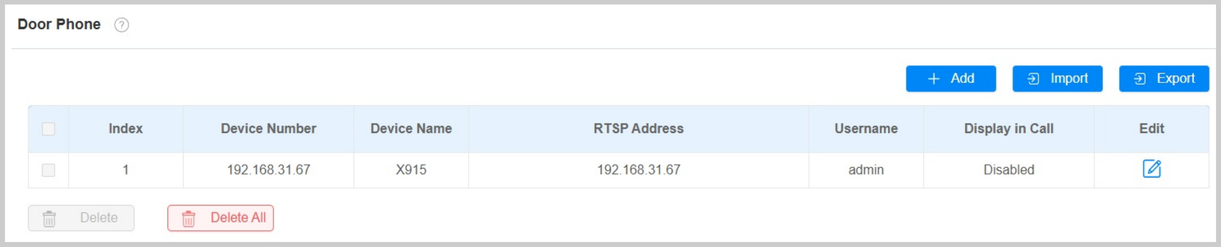


Monitor Setting

Auto Loop Play	☑
Loop Duration	1 minute
24/7 Monitor Mode	Disabled

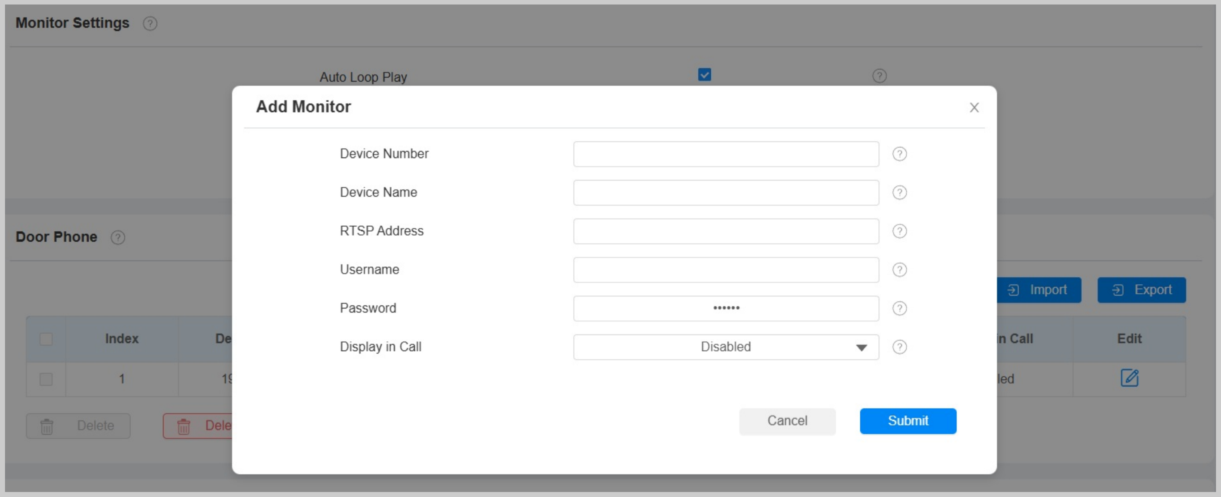
- **Auto Loop Play**: Set whether to play all monitoring streams in rotation.
- **Loop Duration**: The duration of playing each monitoring stream. The default is 1 minute.
- **24/7 Monitor Mode**: When enabled, the indoor monitor displays the monitoring screen for 6 hours, then plays a 10-second screensaver before resuming the monitoring stream.

On the **Device > Monitor > Door Phone** section, click **+Add** to add a monitor.



Door Phone

□	Index	Device Number	Device Name	RTSP Address	Username	Display in Call	Edit
□	1	192.168.31.67	X915	192.168.31.67	admin	Disabled	✎



Monitor Settings

Auto Loop Play ☑

Add Monitor

Device Number

Device Name

RTSP Address

Username

Password ••••••

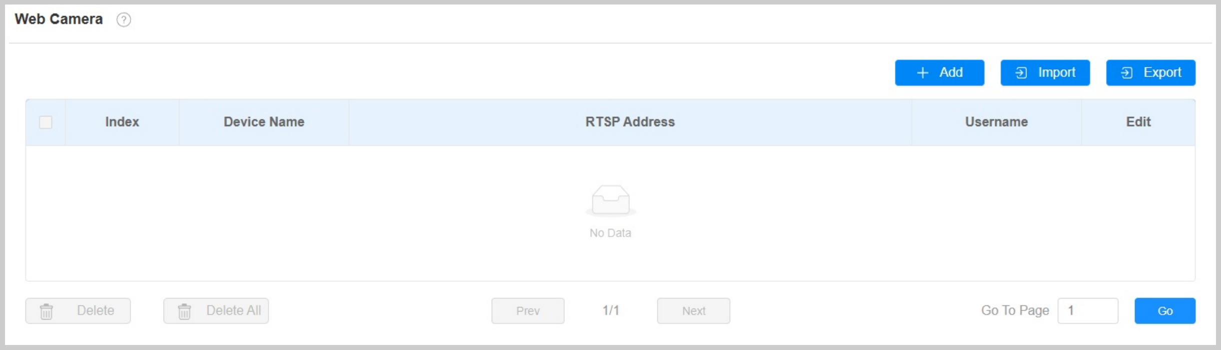
Display in Call: Disabled

- **Device Number**: The device's SIP/IP number for identification.
- **Device Name**: The device name for identification.
- **RTSP Address**: The RTSP address of the monitoring device. RTSP format: *rtsp://Device IP address/live/ch00_0.*
- **Username**: The username of the monitoring device for authentication.
- **Password**: The password of the monitoring device for authentication.
- **Display In Call**: Enable it to display the monitoring video during a call.

> **Note**
>
> You can import and export the monitoring device settings via a template in .xml format.

Web Camera Setting

You can configure the monitor feature for third-party cameras on the web **Device > Monitor > Web Camera** interface.

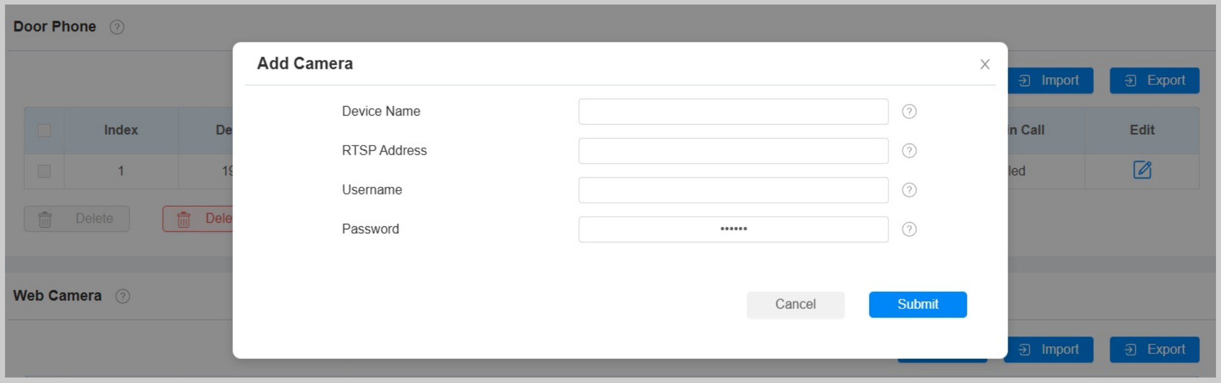


Web Camera

□	Index	Device Name	RTSP Address	Username	Edit

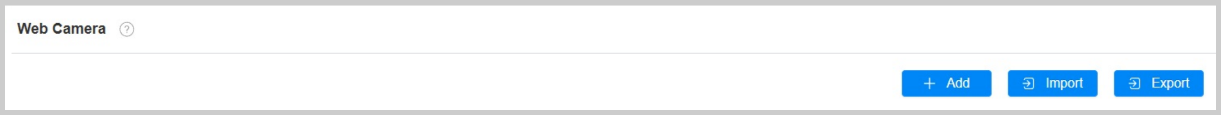
No Data

Click **Add** to add a camera.



- **Device Name**: The name of the third-party camera.
- **RTSP Address**: The RTSP URL for the third-party camera. Confirm it with the third-party service provider.
- **Username**: The username of the monitoring device for authentication.
- **Password**: The password of the monitoring device for authentication.

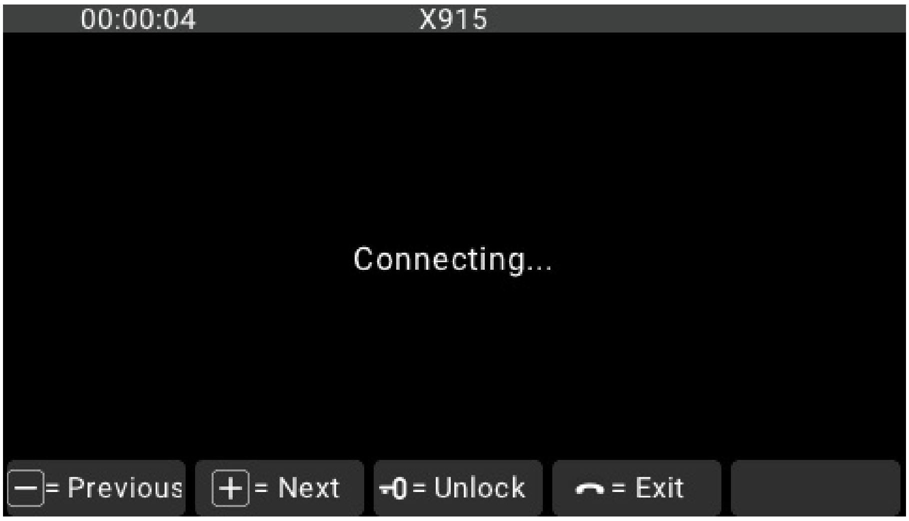
You can also import or export the monitor list in batch on the same interface. The import file only supports the **.xml** format.



View Monitoring Streams

After adding the monitored device's RTSP URL, select **Monitor** on the home screen.

Tap **+** and **—** to switch between channels.

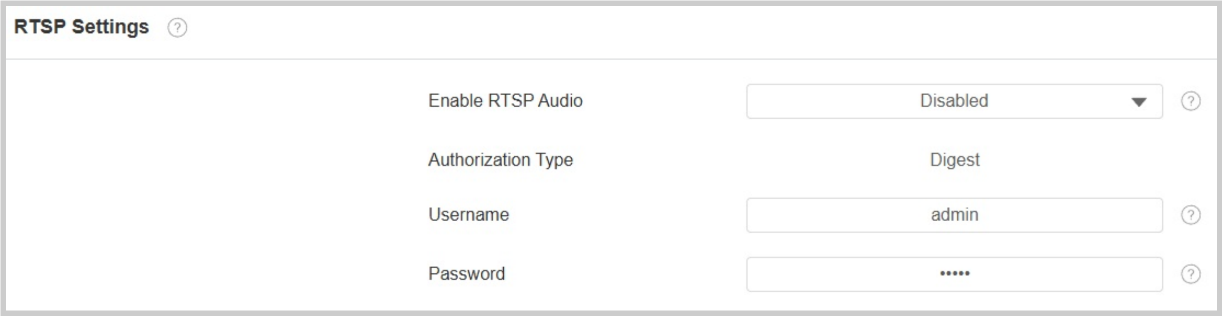


Connecting...

RTSP Authentication

With RTSP authentication, users can monitor the indoor monitor via RTSP audio stream. This feature can be applied to, for example, listen to the baby in the baby’s room for safety.

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



RTSP Settings

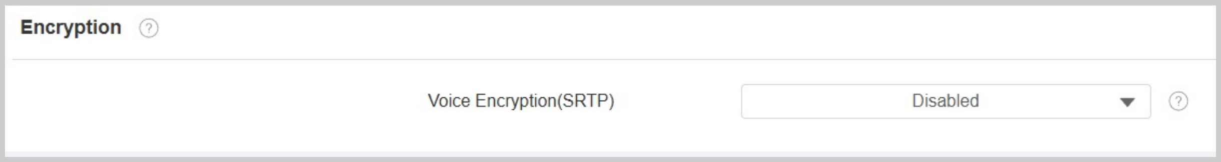
Enable RTSP Audio	Disabled
Authorization Type	Digest
Username	admin
Password	•••••

- **Enable RTSP Audio**: Enable it if you want to monitor the device via RTSP audio stream.
- **Authorization Type**: It is Digest by default.
- **Username**: Set the username for the authentication.
- **Password**: Set the password for the authentication.

Voice Encryption

The encryption function provides three encryption methods to protect voice signals from eavesdropping during a call.

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



Encryption

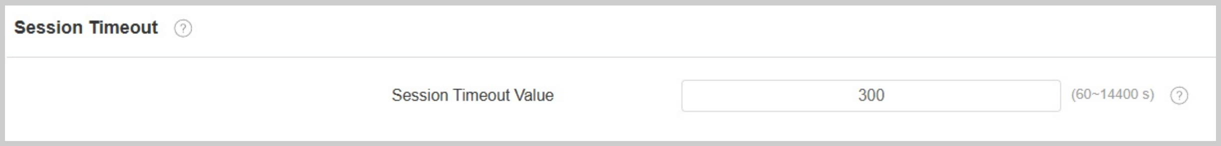
Voice Encryption(SRTP) Disabled

- **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.

To set it up, go to the web **Security > Basic > Session Timeout** interface.



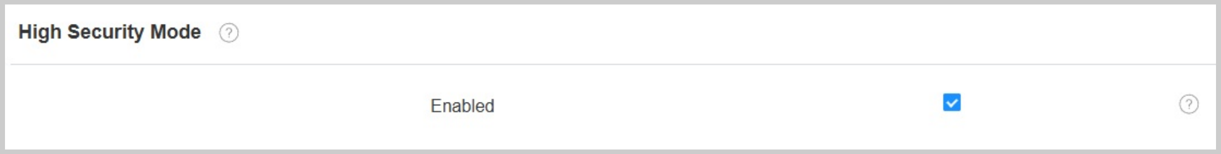
Session Timeout

Session Timeout Value 300 (60~14400 s)

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.

To set it up, go to the web **Security > Basic > High Security Mode** interface.



High Security Mode

Enabled ☑

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

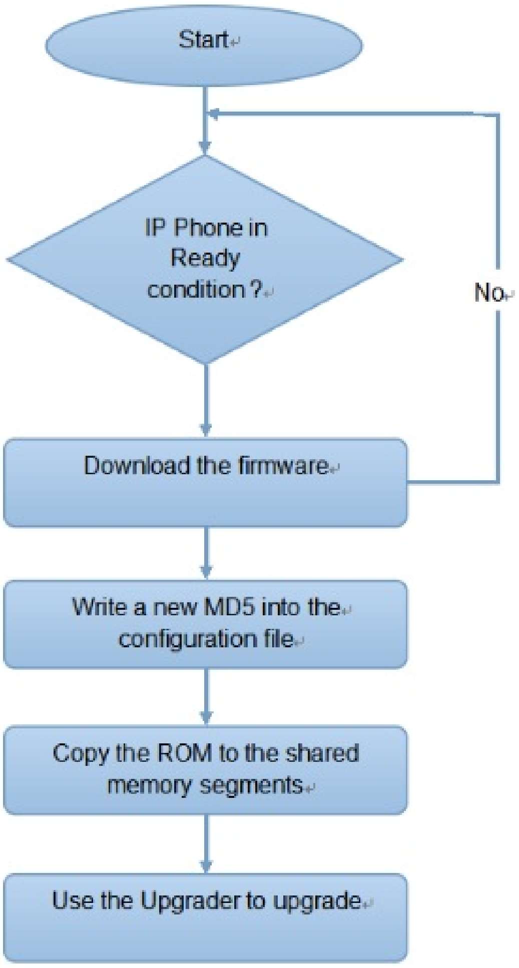
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Auto-provisioning

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:


Start
IP Phone in Ready condition ?
No
Download the firmware
Write a new MD5 into the configuration file
Copy the ROM to the shared memory segments
Use the Upgrader to upgrade

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**:

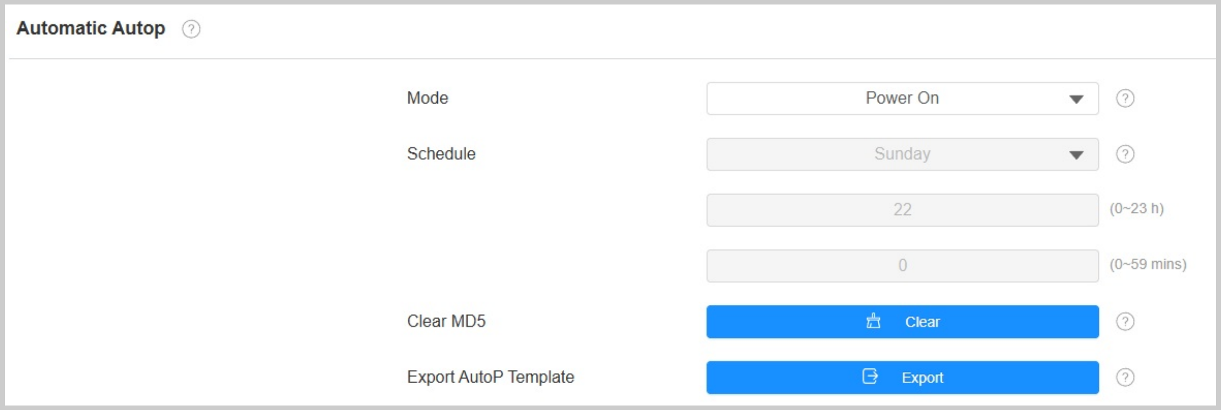
MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

> 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.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 (0~23 h)

0 (0~59 mins)

Clear MD5: Clear

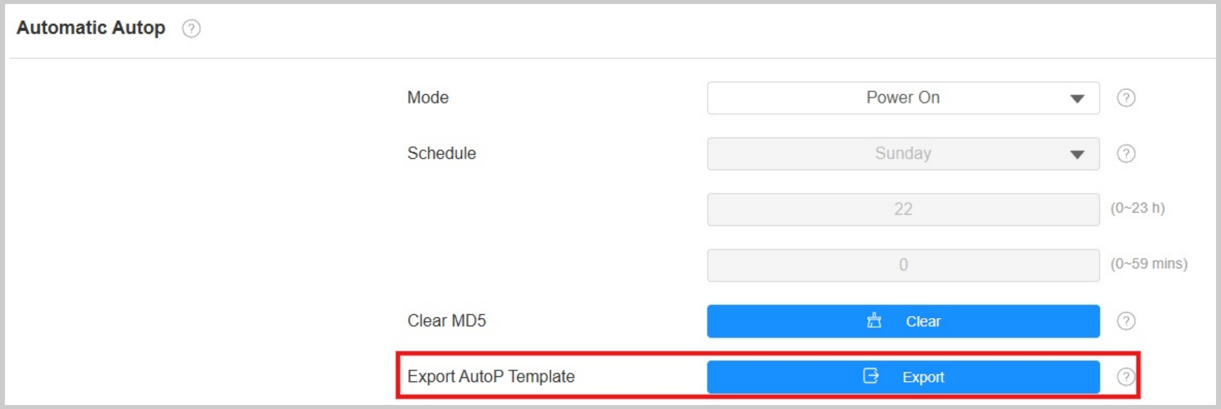
Export AutoP Template: Export

- **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, which 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.



Automatic Autop

Mode: Power On

Schedule: Sunday

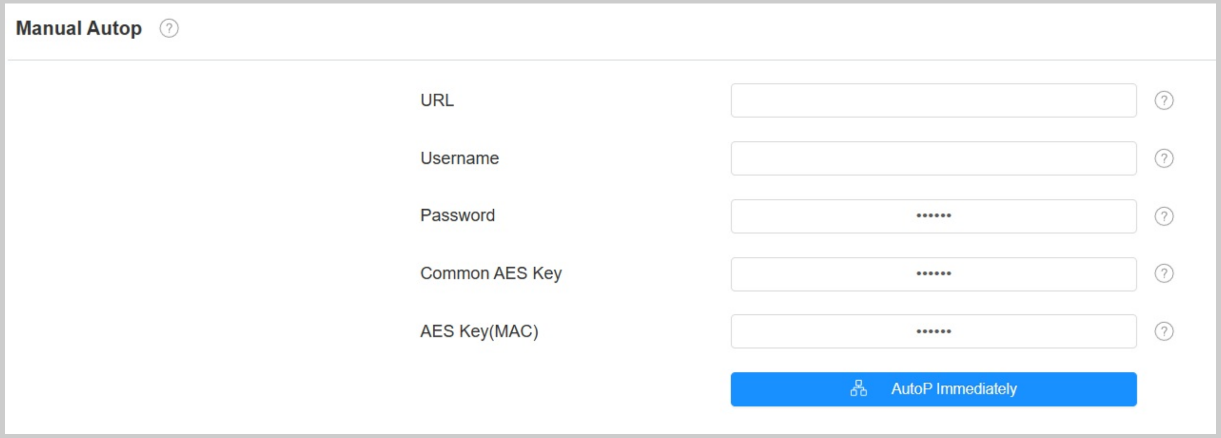
22 (0~23 h)

0 (0~59 mins)

Clear MD5: Clear

Export AutoP Template: Export

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



Manual Autop

URL

Username

Password ••••••

Common AES Key ••••••

AES Key(MAC) ••••••

- **URL**: Specify the TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: Enter the username if the server requires a username to be accessed.
- **Password**: Enter the password if the server requires 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

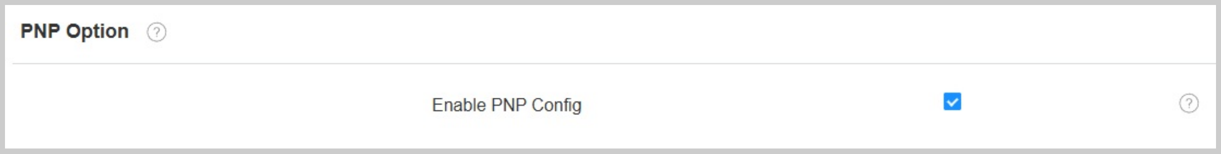
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

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.

To enable the function, go to the **Upgrade > Advanced > PNP Option** interface.

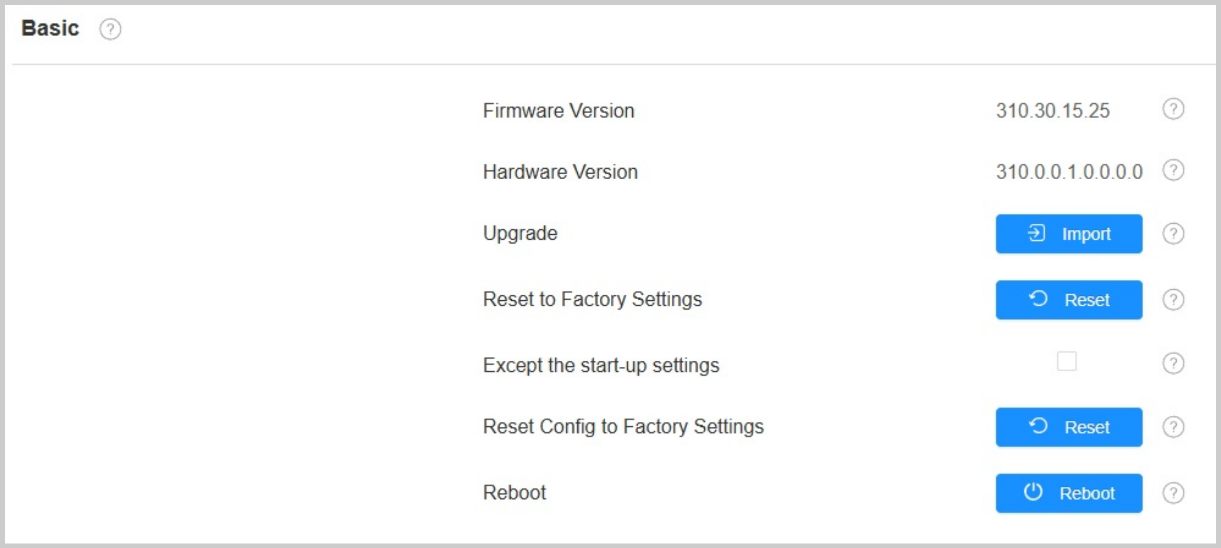


PNP Option

Enable PNP Config ☑

Firmware Upgrade

To upgrade the device, navigate to the **Upgrade > Basic** interface.



Basic

Firmware Version	310.30.15.25
Hardware Version	310.0.0.1.0.0.0.0
Upgrade	Import
Reset to Factory Settings	Reset
Except the start-up settings	□
Reset Config to Factory Settings	Reset
Reboot	Reboot

Note

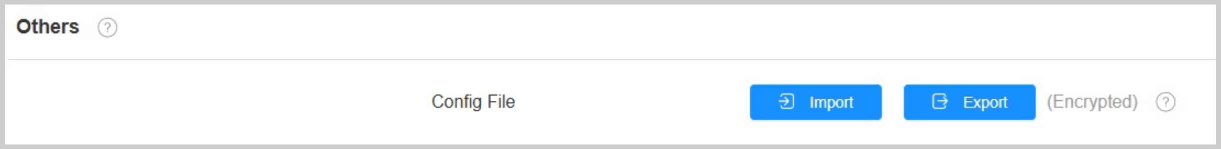
Firmware files should be .rom format for an upgrade.

Backup

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

To export the file, navigate to the **Upgrade > Advanced > Others** interface. The export file is in the TGZ file.

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



Others

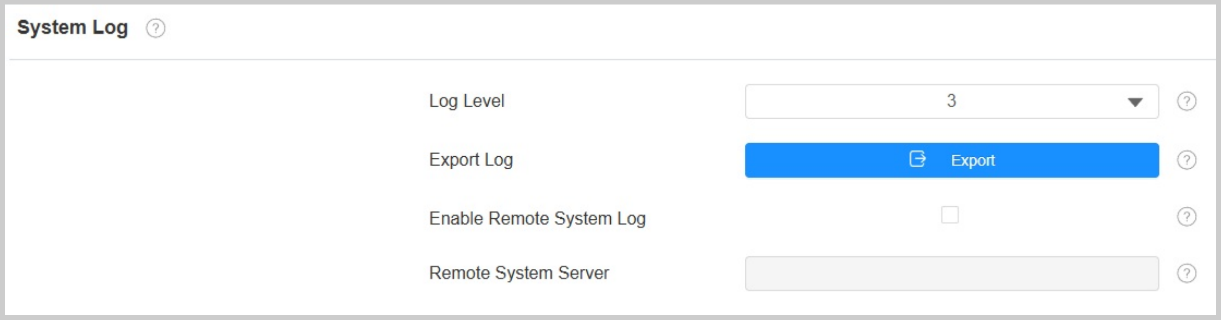
Config File Import Export (Encrypted)

Debug

System Log for Debugging

System logs can be used for debugging purposes.

If you want to export the system log to a local PC or a remote server for debugging, you can set up the function on the web **Upgrade > Diagnosis > System Log** interface.



System Log

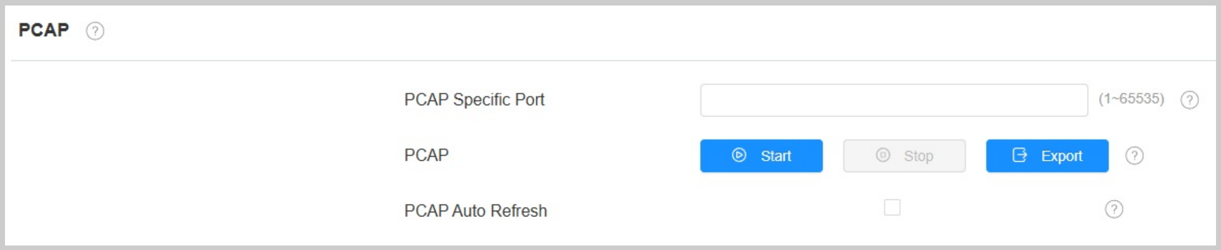
Log Level	3
Export Log	Export
Enable Remote System Log	□
Remote System Server	

- **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.

To set up PCAP, go to the web **Upgrade > Diagnosis > PCAP** interface.


PCAP

PCAP Specific Port (1~65535)

PCAP

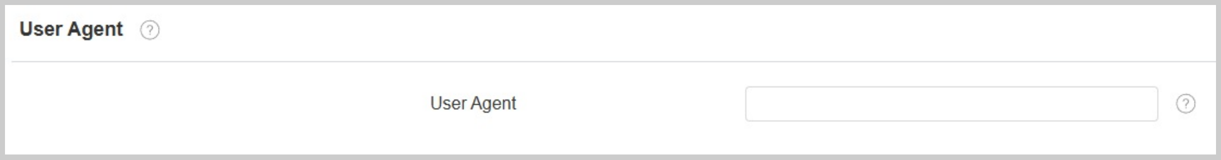
PCAP Auto Refresh □

- **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 50 MB 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.

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

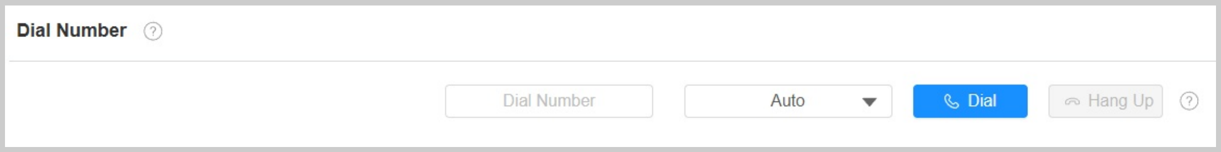

User Agent

User Agent

Web Call

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

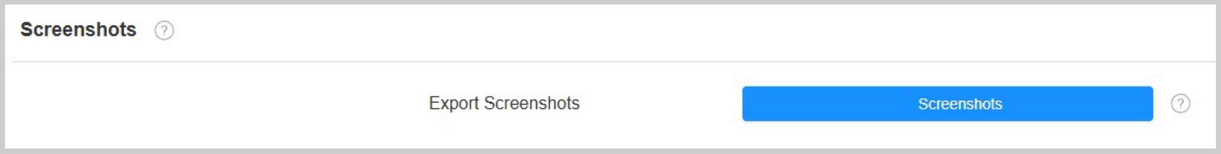
To set it up, navigate to the **Contacts > Local Contacts > Dial Number** interface. Enter the target number and select the account to dial out.


Dial Number

Screenshots

You can take a screenshot of the specific device screen to help with the troubleshooting and so on.

To take screenshots, go to **Upgrade > Diagnosis > Screenshots** interface, then click **Screenshots**.

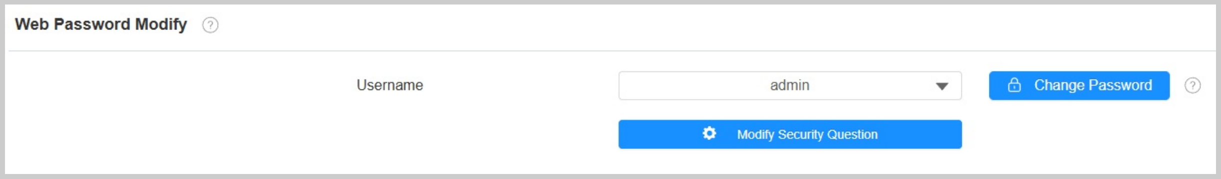


Password Modification

Modify Device Web Interface Password

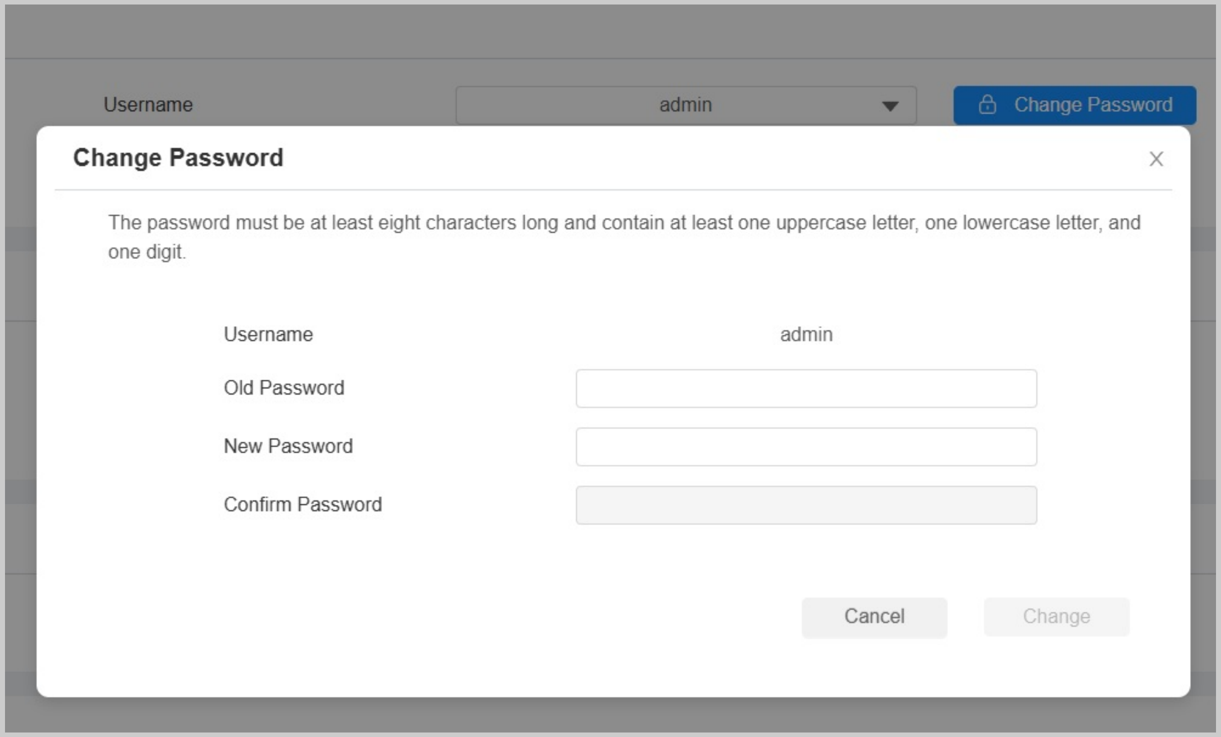
Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.

To set it up, navigate to the **Security > Basic > Web Password Modify** interface.



Web Password Modify

Username: admin



Change Password

The password must be at least eight characters long and contain at least one uppercase letter, one lowercase letter, and one digit.

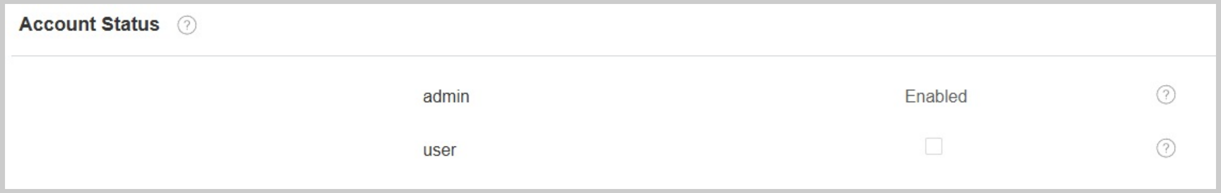
Username: admin

Old Password:

New Password:

Confirm Password:

You can enable or disable the user account on the **Security > Basic** interface.



Account Status

admin	Enabled
user	□

Note

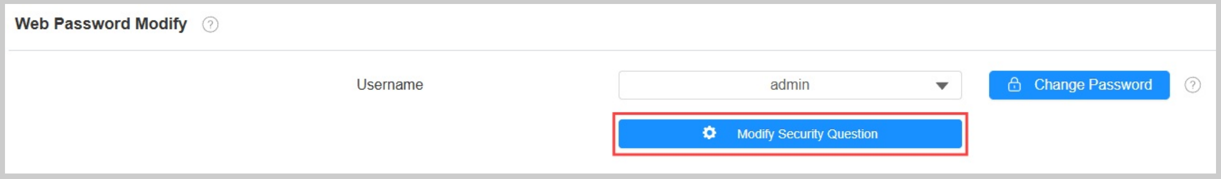
There are two accounts, one is admin, its password is admin, the other is user, and its password is user.

Modify Security Questions

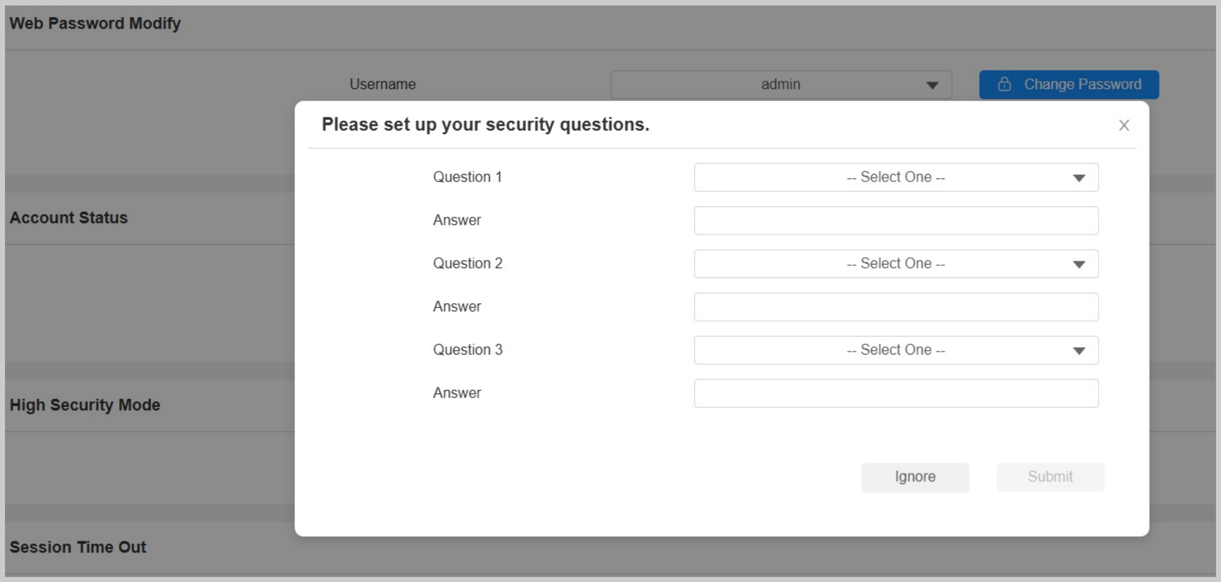
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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 > Web Password Modify** interface.



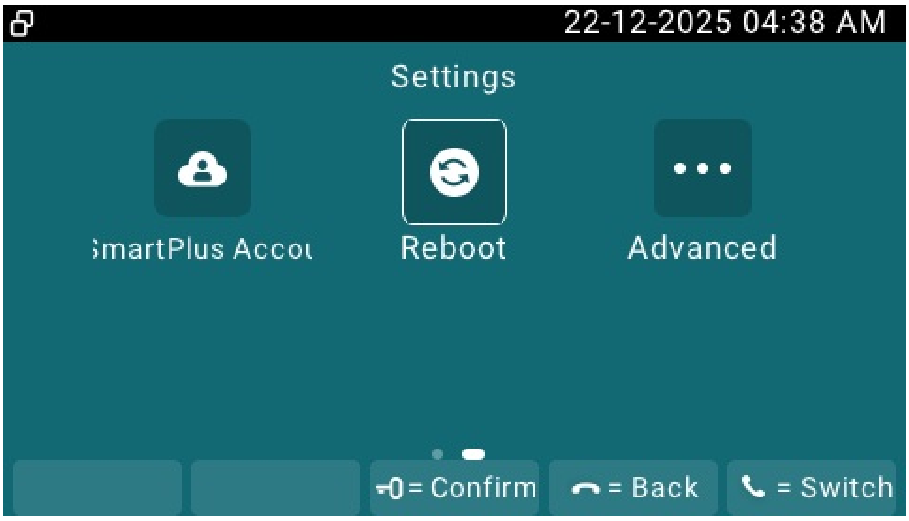
You are required to fill in the correct password before modifying the security questions.



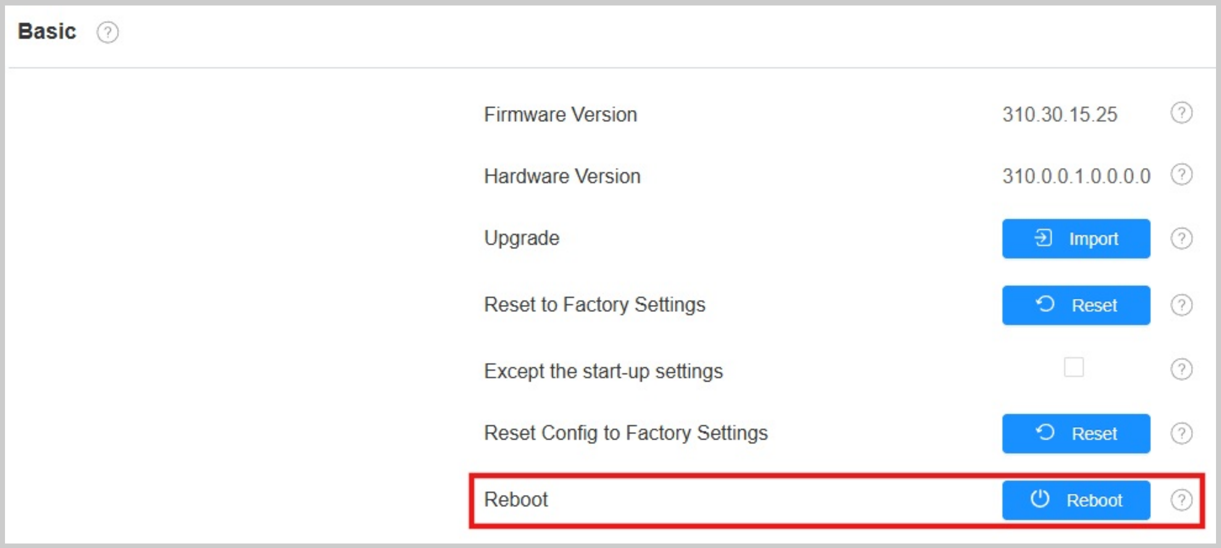
System Reboot & Reset

Reboot

You can reboot the device on its **Settings** screen.



Or, go to the **Upgrade > Basic** interface.

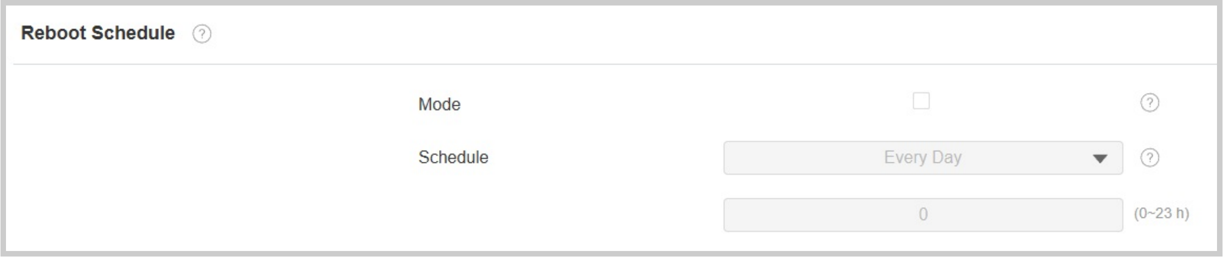


Basic

Firmware Version	310.30.15.25
Hardware Version	310.0.0.1.0.0.0.0
Upgrade	Import
Reset to Factory Settings	Reset
Except the start-up settings	□
Reset Config to Factory Settings	Reset
Reboot	Reboot

Besides, you can set up a reboot schedule to make the device restart at designated times.

Set it up on the **Upgrade > Advanced > Reboot Schedule** interface.

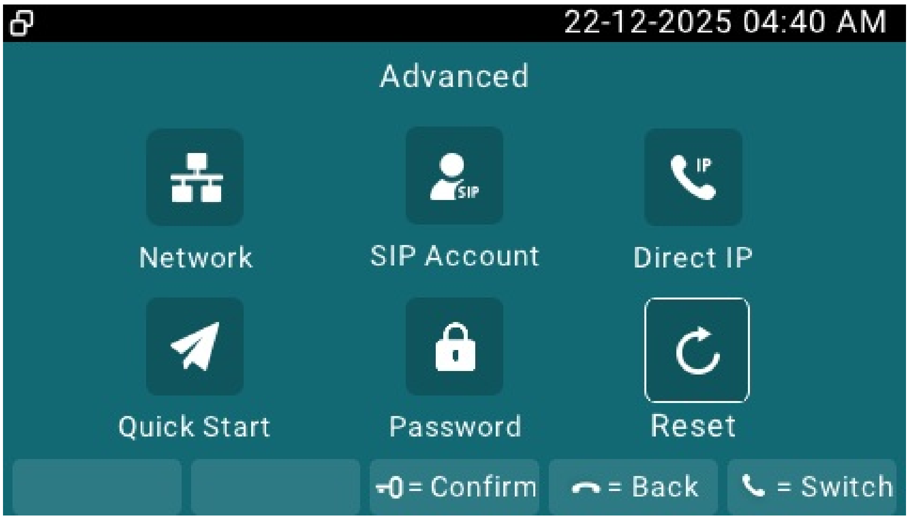


Reboot Schedule

Mode	□	
Schedule	Every Day	
	0	(0~23 h)

Reset

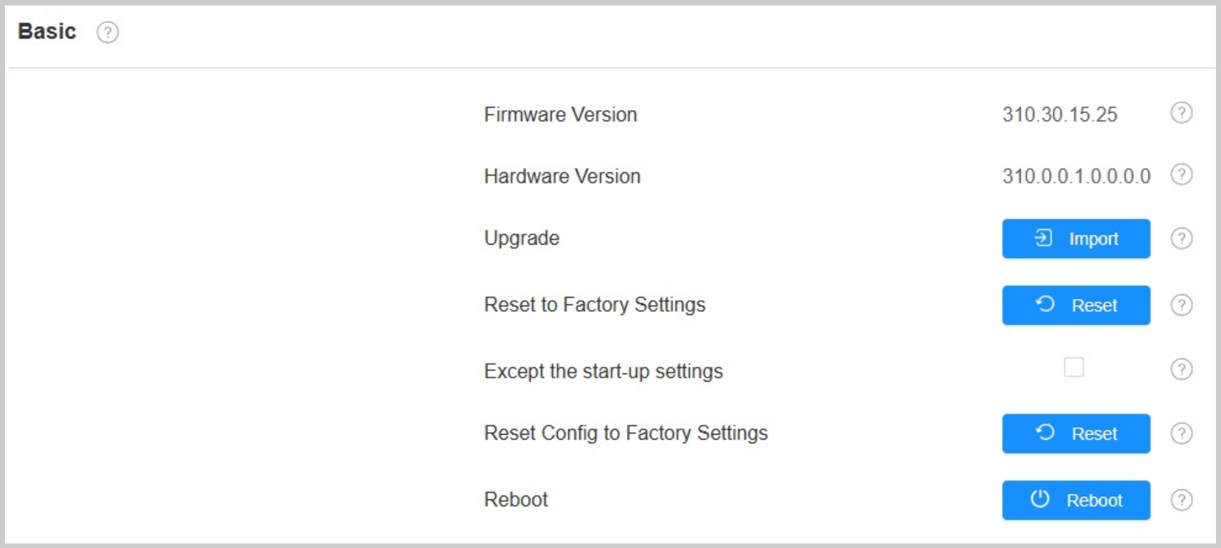
You can reset the device on its **Settings > Advanced** screen.



Or, go to the **Upgrade > Basic** interface.

The device provides two reset options:

- **Reset to Factory Settings**: Reset all data to the factory default.
- **Reset Config to Factory Settings**: Retain the user data, such as the RF cards, face data, schedules, and call logs.



Basic

Firmware Version	310.30.15.25
Hardware Version	310.0.0.1.0.0.0.0
Upgrade	Import
Reset to Factory Settings	Reset
Except the start-up settings	□
Reset Config to Factory Settings	Reset
Reboot	Reboot

- **Except the start-up settings**: Check to retain the initial settings, such as network and time zone.