

About This Manual



WWW.AKUVOX.COM



C316 SERIES INDOOR MONITOR

Admin Guide

Thank you for choosing the Akuvox C316 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. This manual is written based on firmware version: 316.30.12.113, and it provides all the configurations for the functions and features of the C316 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

The Akuvox C316 multifunctional communicator, with an Android 12 operating system, provides audio and video communication with door phones via SIP 2.0

protocol. It delivers the ultimate touchscreen experience in an unobtrusive, space-saving design featuring a brilliant 7-inch capacitive touchscreen display.

Model Differences

Model	C316W	C316S
OS	Android 12	Android 12
RAM / ROM	2GB / 8GB	2GB / 8GB
Display	7 Inch TFT LCD	7 Inch TFT LCD
Wi-Fi	IEEE802.11 b/g/n @2.4GHz	X
Bluetooth	Bluetooth 4.2	X
RS485 port	✓	✓
Relay out	1	1
Bell in	1	1
I/O	8	8
Power Supply	802.3af Power-over-Ethernet or 12V DC connector if not using PoE	802.3af Power-over-Ethernet or 12V DC connector if not using PoE

Introduction to Configuration Menu

- **Status:** This section gives you basic information such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, NAT, user agent, etc.
- **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
- **Device:** This section includes time, language, call feature, NTP, display setting, audio, multicast, relay, third-party APP, intercom, relay monitor, lift control, etc.
- **Contacts:** This section allows the user to configure the local contact list stored on the device and check call logs.
- **Upgrade:** This section covers firmware upgrade, device reset & reboot, screenshots, configuration file auto-provisioning, and PCAP.
- **Security:** This section is for password modification, account status & session time-out configuration, client certificate, and service location.
- **Settings:** This section includes the RTSP setting, voice assistant, and brightness adaptation.
- **Arming:** This section covers the configuration including arming zone setting, arming mode, disarm code, and alarm action.

Akuvox
Open A Smart World

C316



Homepage



Status



Account



Network



Device



Contacts



Upgrade



Security



Settings



Arming

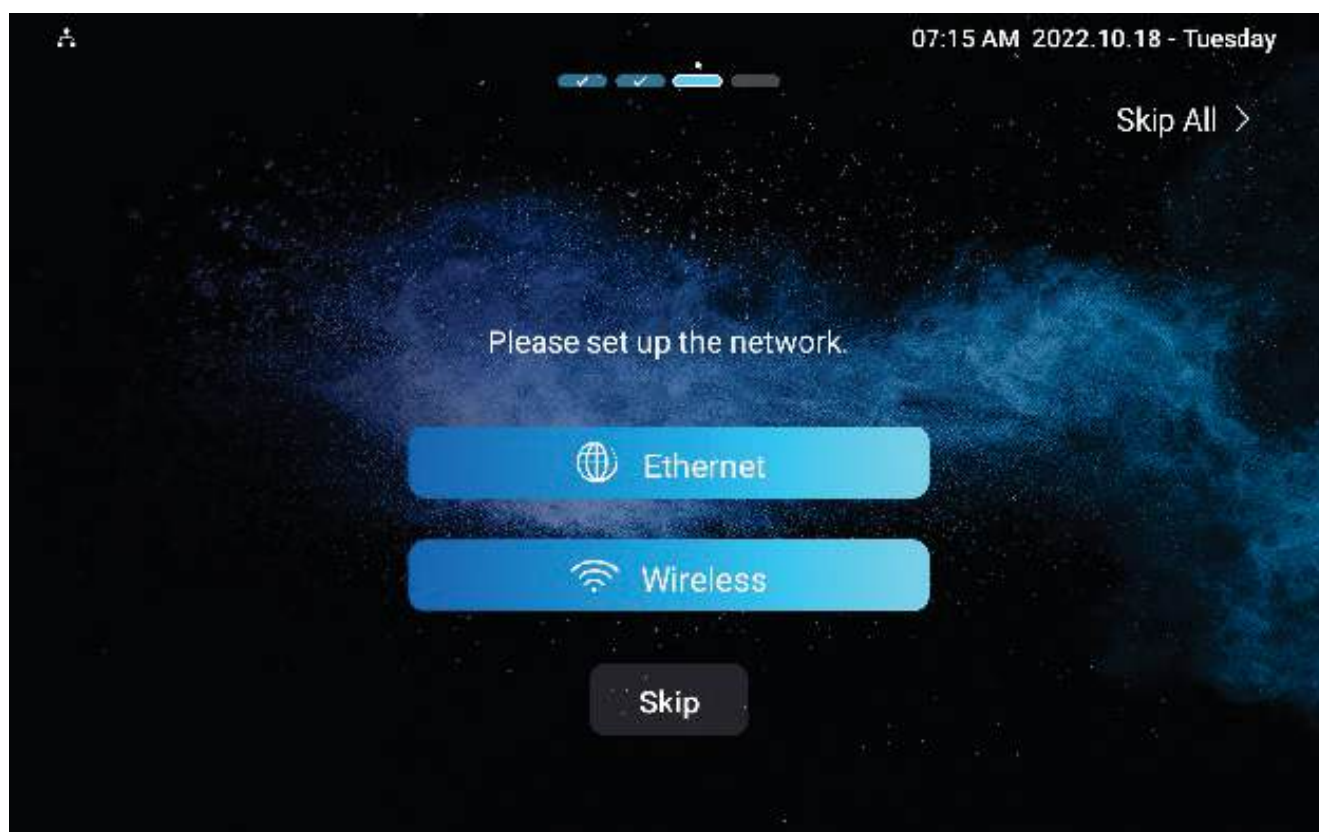


Access the Device

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

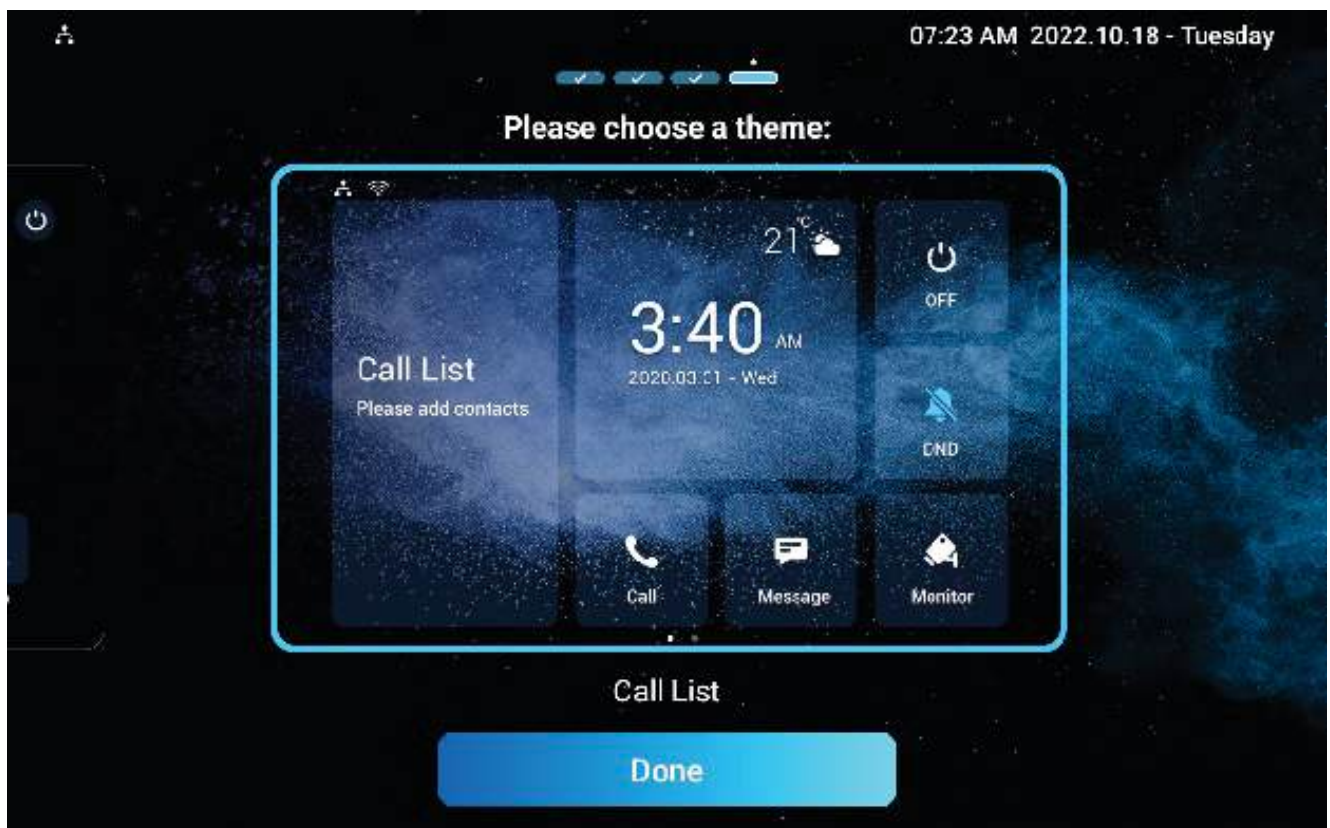
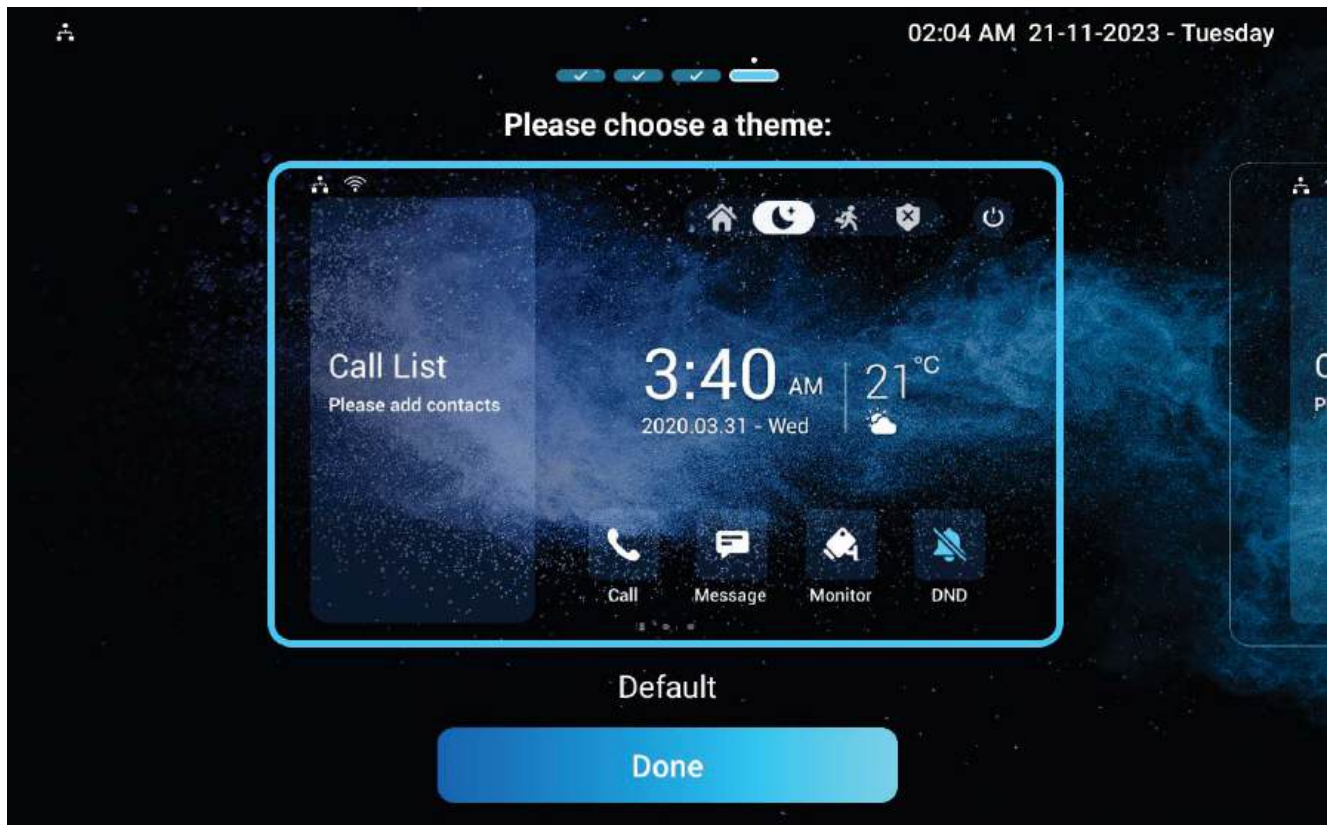
Device Start-up Network Selection

After the device boots up initially, you are required to select the network connection for the device. You can either select Ethernet or wireless network connection according to your need.



Device Home Screen Type Selection

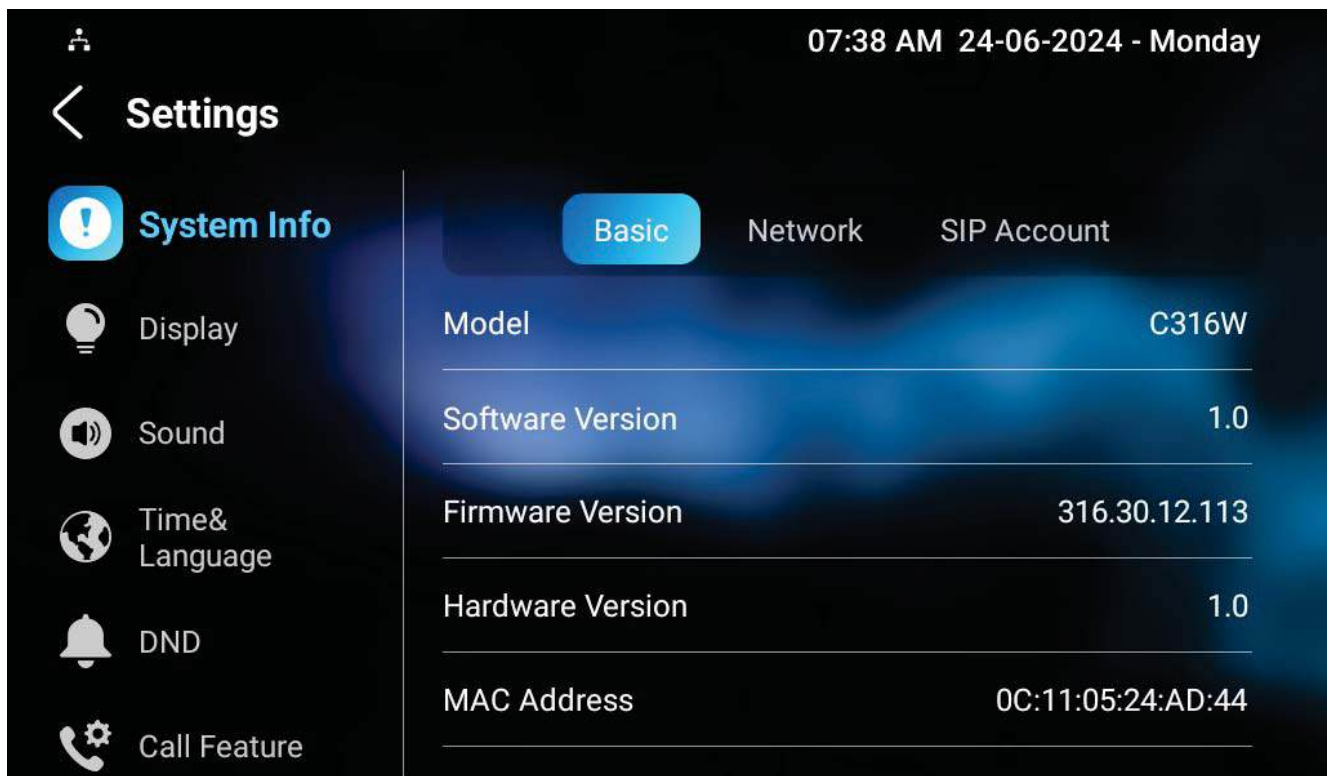
Akuvox indoor monitor supports two different home screen display modes: **Default** and **Call List**. Choose the desired mode.



Access the Device Settings on the Device

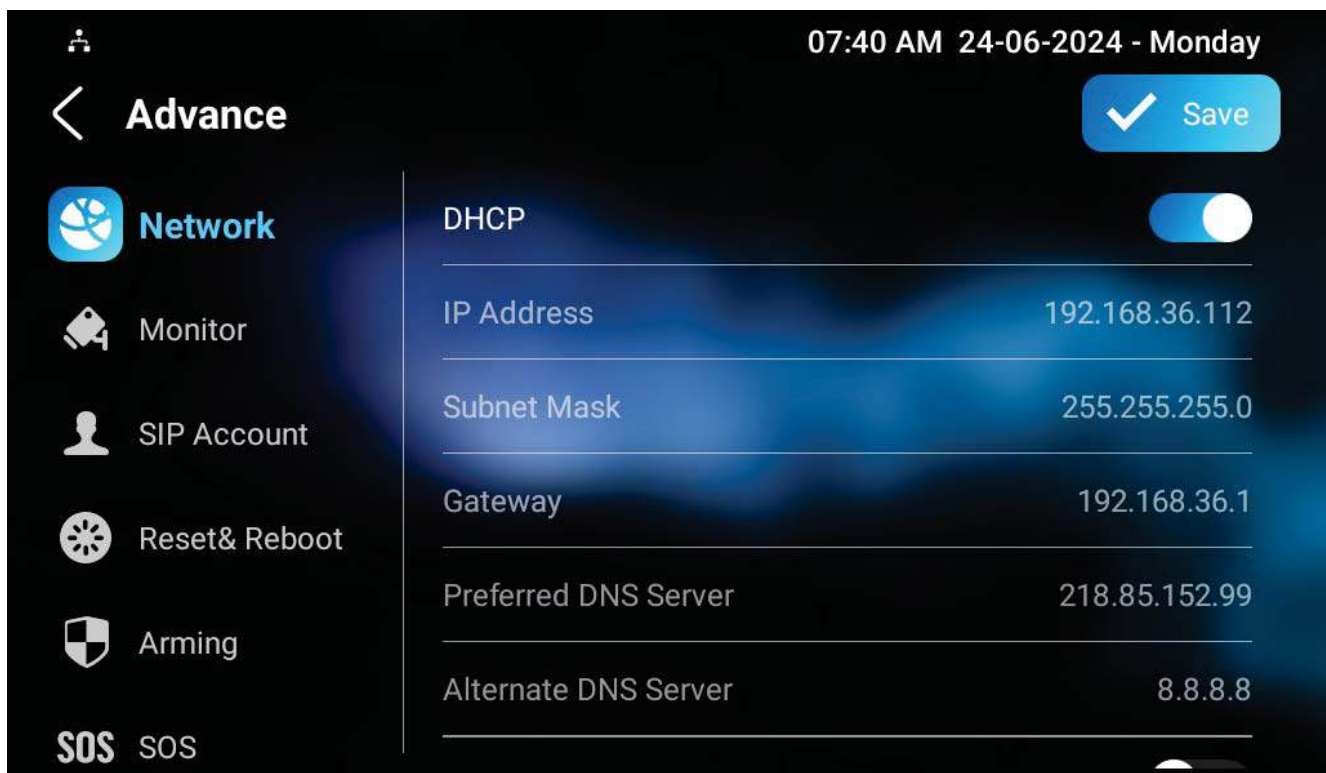
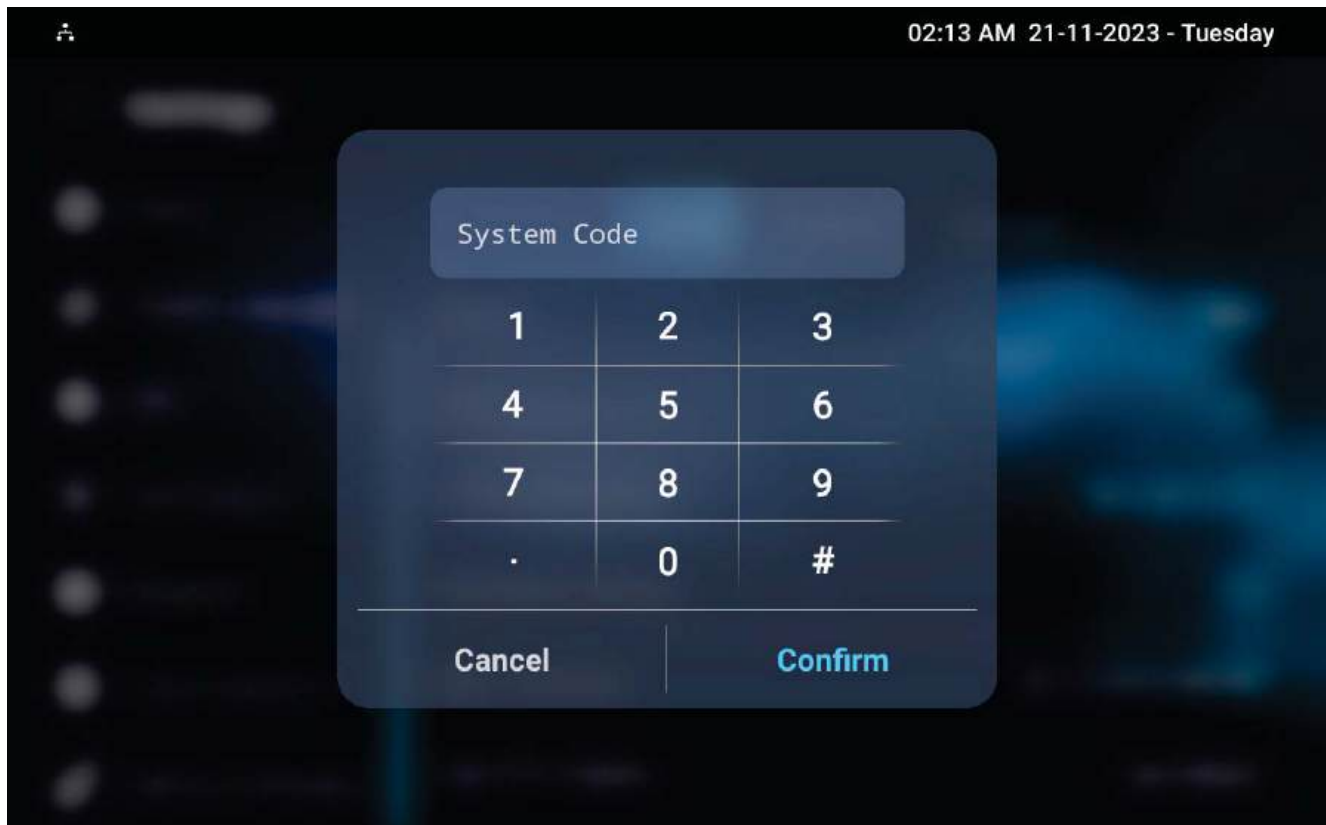
Access Device Basic Settings

You can access the device's basic and advanced settings to configure different functions. To access the device's basic settings, swipe your finger left on the home screen, then tap . You can check the basic information like MAC, firmware, etc.



Access Device Advance Settings

To access the advanced settings, press  and tap **Advance**. Press the default password 123456 to enter the advanced settings.



Access the Device Settings on the Web Interface

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

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

IP Scanner					
Online Device : 7					
			Search	Refresh	
Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C...		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0C...	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C...	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C...	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C...	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A...		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C...	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 the detailed guide:
<https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner>
- Google Chrome browser is strongly recommended.
- The initial username and password are admin and please be case-sensitive to the user names and passwords entered.

Language and Time Setting

Language Setting

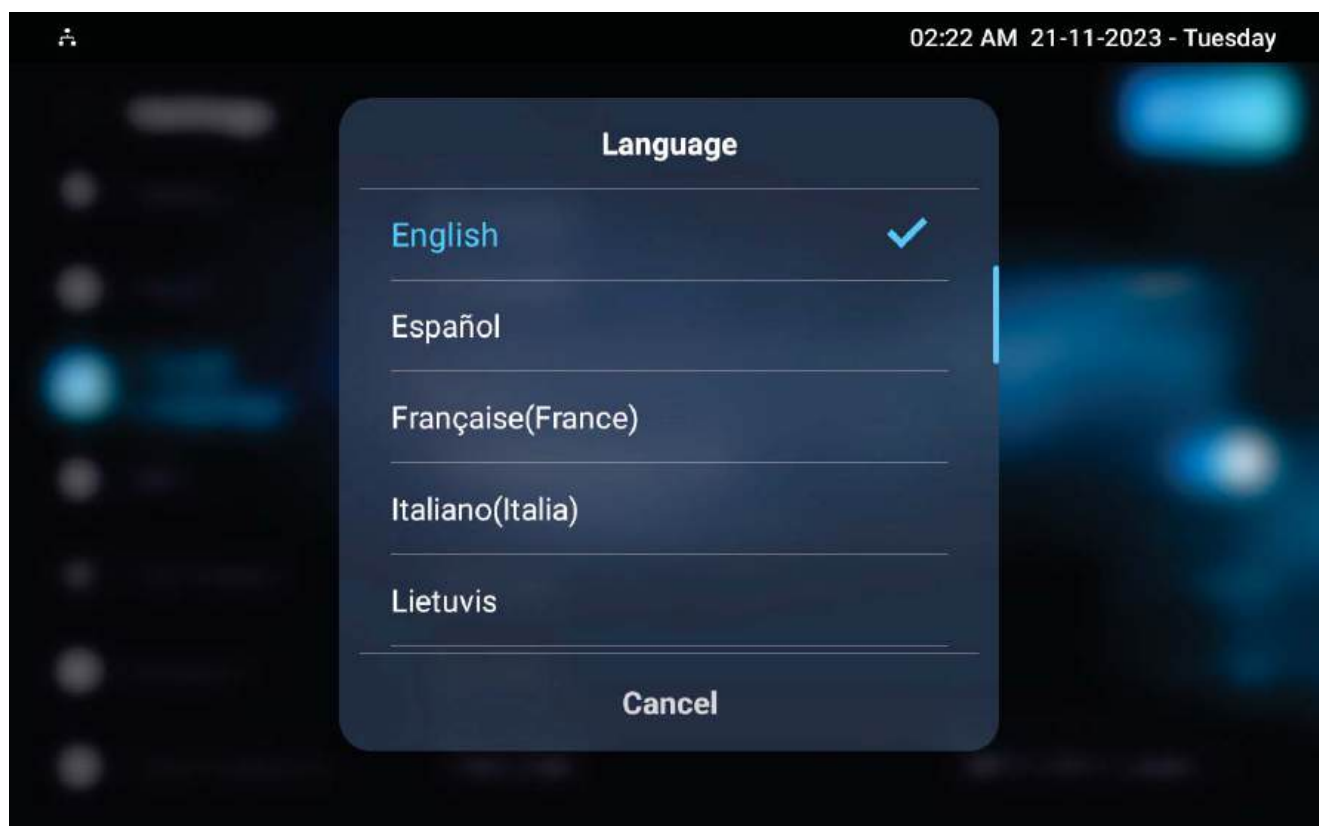
Set up the language during initial device setup or later through the device or web interface according to your preference.

Language Setting on the Device

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

The device supports the following languages:

- Bosnian, Czech, Danish, German, English, Spanish, French, Italian, Lithuanian, Mongolian, Norwegian, Polish, Portuguese, Russian, Slovene, Swedish, Turkish, Vietnamese, Korean, Simplified Chinese, Traditional Chinese, Japanese, Ukrainian, Dutch, and Arabic.



Language Setting on the Web Interface

You can select the device web language in the upper right corner.

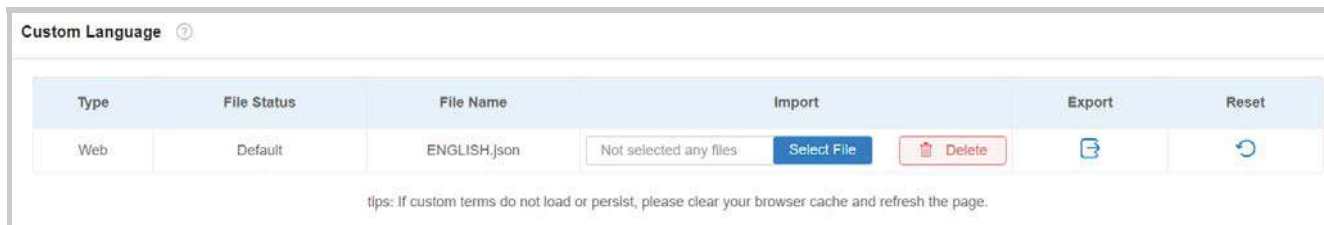
The device web interface supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Czech, Portuguese, Spanish, Dutch, French, German, Polish, Turkish, Japanese, Mongolian, Vietnamese, and Italian.



You can customize interface text including configuration names and prompt text.

To set it up, go to **Device > Time/Lang** interface. Export and edit the .json file. Then import the file to the device.

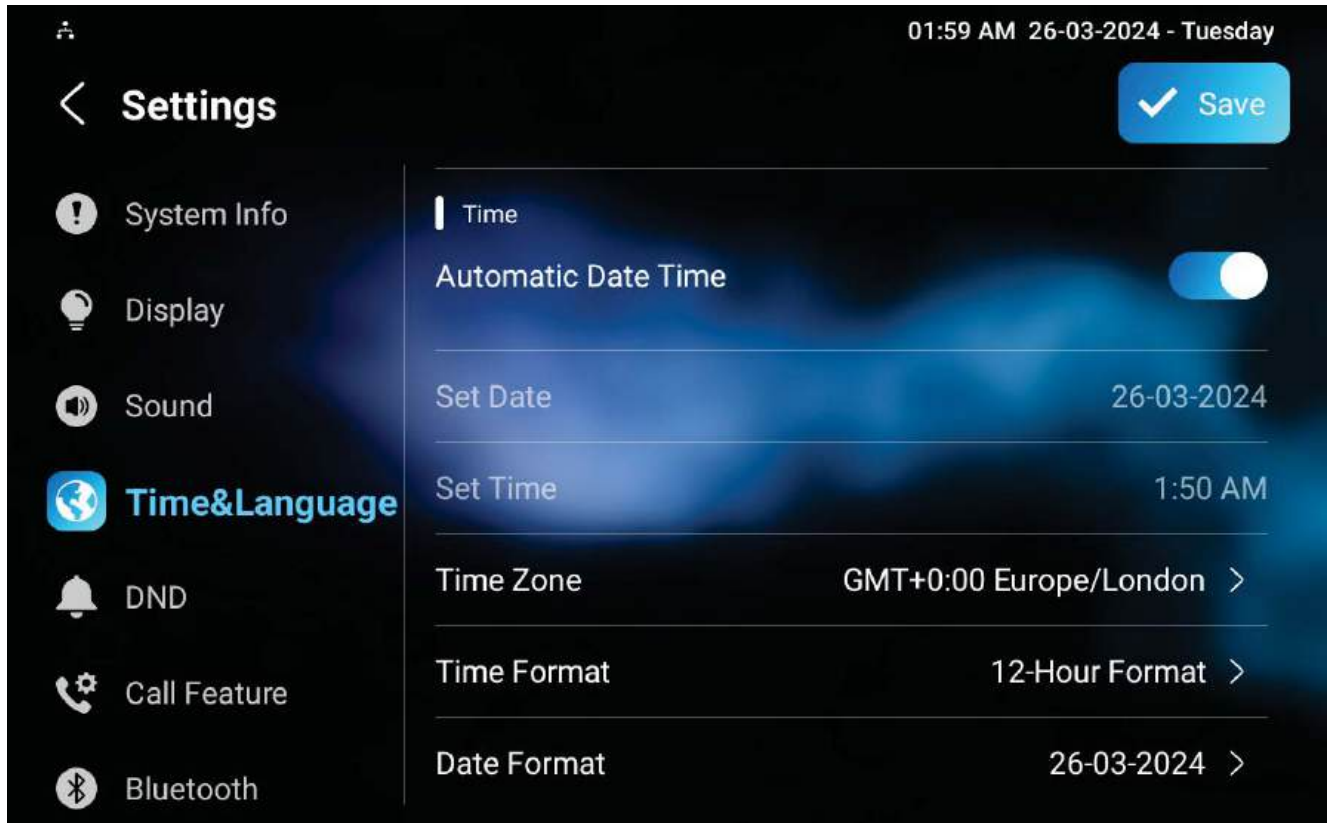


Time Setting

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

Time Setting on the Device

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



- **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.
- **Time Format:** Select a 12-hour or 24-hour time format.
- **Date Format:** Select the date format from the provided options: Y-M-D, Y/M/D, D-M-Y, D/M/Y, M-D-Y, and M/D/Y.
- **NTP Server1/NTP Server2:** Enter the NTP server address. NTP server 2 is the backup.

Time Setting on the Web Interface

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

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

Time Setting

Automatic Date&Time

☒

Time Format

12-Hour Format

Date Format

DD-MM-YYYY

Date

24-06-2024

Time

7:47 am

Time Zone

GMT+1:00 Europe/London

NTP

Preferred Server

0.pool.ntp.org

Secondary Server

1.pool.ntp.org

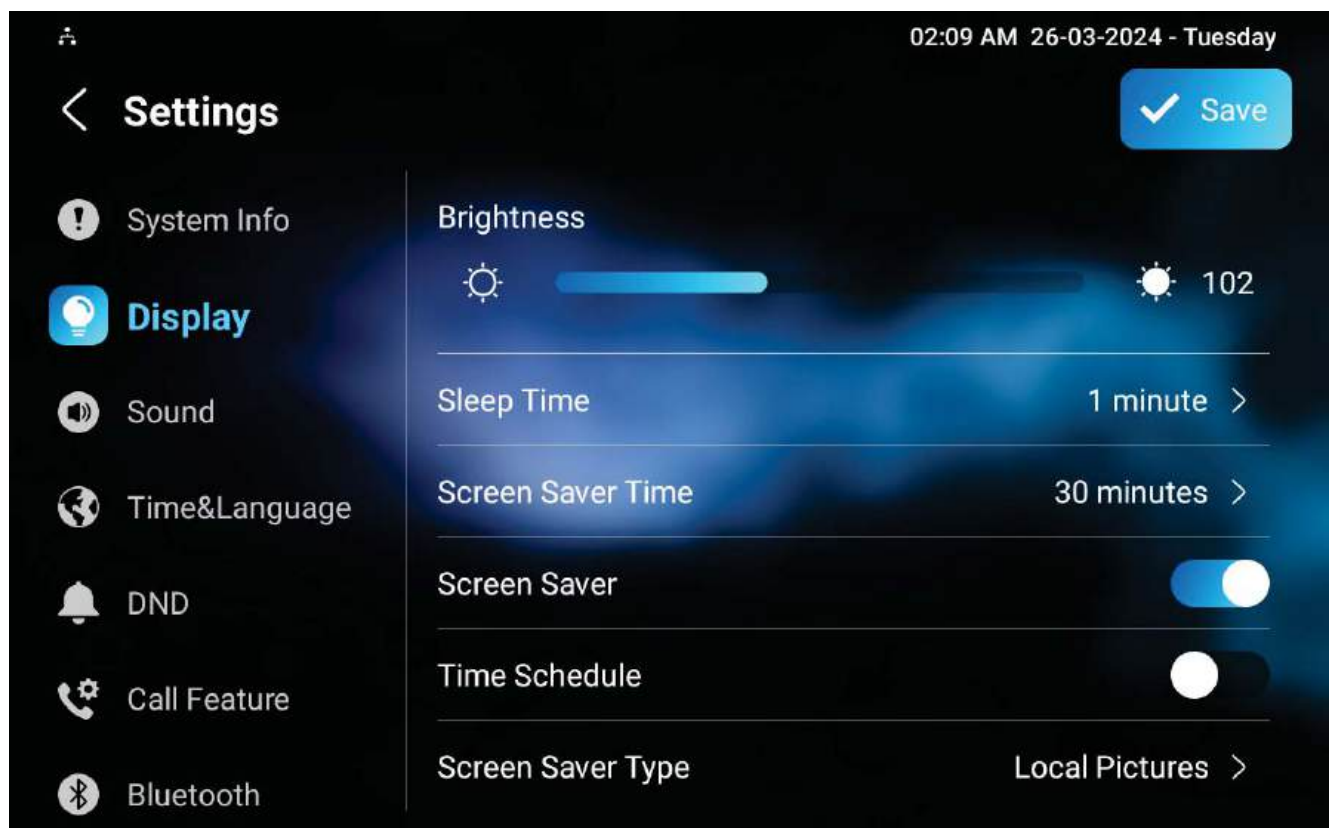
- **Automatic Date & Time:** The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Format:** Select a 12-hour or 24-hour time format.
- **Date Format:** Select the date format from the provided options: Y-M-D, Y/M/D, D-M-Y, D/M/Y, M-D-Y, and M/D/Y.
- **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.
- **Secondary Server:** Enter the backup server address. When the main NTP server fails, it will change to the backup server automatically.

Screen Display Configuration

Screen Display Setting on the Device

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

Navigate to the device **Settings > Display** screen.



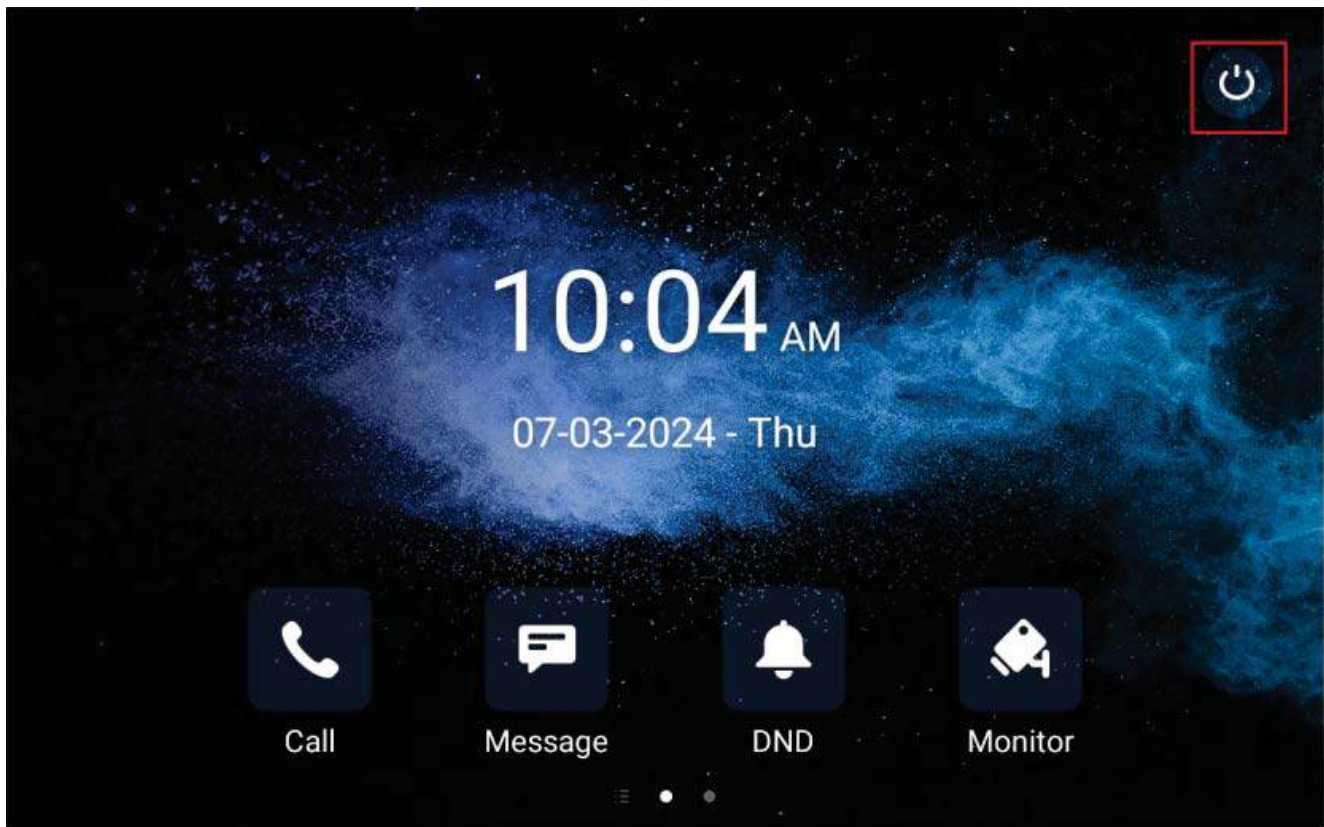
- **Brightness:** Move the blue bar to adjust the screen brightness. The default brightness is 145.
- **Sleep Time:** Set the sleep timing based on the screen saver (15 seconds to 30 minutes).
 - If the screen saver is enabled, the sleep time is the screen saver start time. For example, if you set it as 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 is the screen turn-off time. For example, if you set it as 1 minute, the screen will be turned off automatically when the device has no operation for 1 minute.

- **Screen Saver Time:** The time for displaying the screensaver.
- **Screen Saver:** Determine whether to display the screensaver when the device goes into sleep mode.
- **Time Schedule:** Decide the specific time range to display the screen saver.
- **Screen Saver Type:** Please refer to the chart below.

NO.	Screen Saver Type	Type Description
1	SDMC Pictures	Display pictures from SDMC as the screen saver.
2	Local Pictures	Display picture uploaded to the indoor monitor as the screen saver.
3	SDMC+Local Pictures	Display pictures from SDMC and the indoor monitor in rotation as the screen saver.
4	SDMC Videos	Display videos from SDMC as the screen saver.
5	Local Videos	Display videos from the indoor monitor as the screen saver
6	SDMC+Local Videos	Display videos from SDMC and the door phone in rotation as the screen saver.
7	Clock	Display the clock as the screen saver.

- **Screen Lock:** Lock the screen after the screen is turned off(turn dark). You are required to enter the code to unlock the screen. The default code is 123456.
- **Screen Clean:** Allow users to wipe the screen clean without triggering unwanted changes in the settings.
- **Font Size:** Select the font size among four options: Small, Normal, Large, and Huge.
- **Wallpaper:** It is for local wallpaper selection.

You can also turn off the screen manually.



Screen Display Setting on the Web Interface

You can configure the screen display on the **Device > Display Setting > Screen Saver Setting** interface.

Screen Saver Setting

Screen Saver Pictures

Import

Screen Saver Videos

Import

Picture Files

Daydream1.jpg

Delete

Video Files

Delete

Screen Saver Type

Local Pictures

Schedule

☐

Adapting Screen Savers for Third-Part...

☐

- **Screen Saver Type:**

NO.	Screen Saver Type	Type Description
1	SDMC Pictures	Display pictures from SDMC as the screen saver.
2	Local Pictures	Display picture uploaded to the indoor monitor as the screen saver.
3	SDMC+Local Pictures	Display pictures from SDMC and the indoor monitor in rotation as the screen saver.
4	SDMC Videos	Display videos from SDMC as the screen saver.
5	Local Videos	Display videos from the indoor monitor as the screen saver
6	SDMC+Local Videos	Display videos from SDMC and the door phone in rotation as the screen saver.
7	Clock	Display the clock as the screen saver.

- **Schedule:** When enabled, you can decide the specific time range to display the screen saver.
- **Adapting Screen Savers for Third-Party Apps:** When enabled, the screen will turn off without a screen saver. The screen-saver parameters will be hidden on the web interface and the device. This feature keeps third-party apps running in the background.

Upload Screensaver

You can upload screen-saver pictures or videos to the device for a public purpose or greater visual experience.

Navigate to the web **Device > Display Setting > Screen Saver Setting** interface.

You can click **Delete** to delete the existing files.

Screen Saver Setting

Screen Saver Pictures
Import

Screen Saver Videos
Import

Picture Files
Daydream1.jpg
Delete

Video Files
Delete

Screen Saver Type
Local Pictures

Schedule
☐

Adapting Screen Savers for Third-Part...
☐

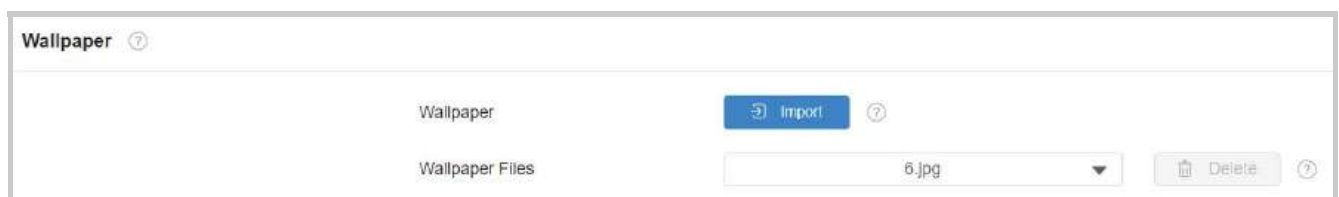
Note

- The pictures uploaded should be in JPG, JPEG, or PNG format with a 2M maximum. The recommended resolution is 1280*800.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurs.
- The videos uploaded should be in MP4, WMV, or AVI format with a 500M maximum. The recommended resolution is 1080*720.

Upload Wall Paper

You can customize your screen background picture on the device web to achieve the visual effect and experience you need for your personalized screen background display.

Navigate to **Device > Display Setting > Wallpaper** interface.



Wallpaper	Wallpaper Files
	Import 6.jpg Delete

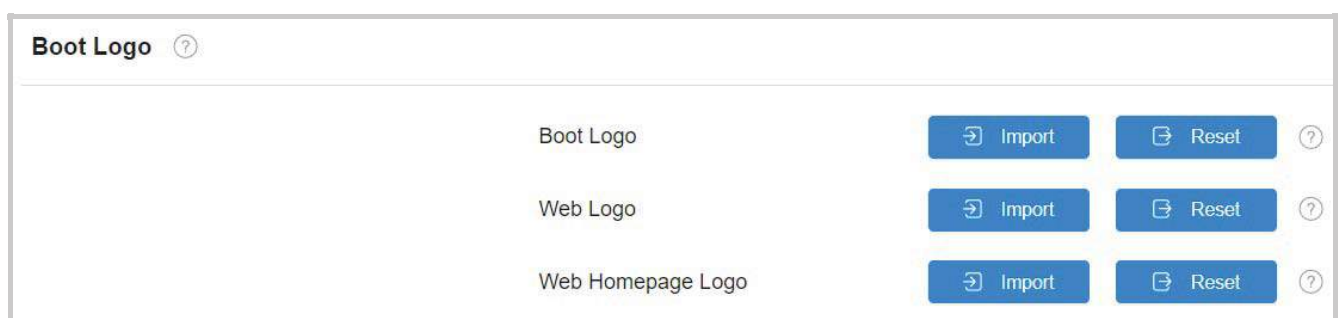
Note

- The pictures uploaded should be in JPG, JPEG, or PNG format with a 2M maximum.
- The recommended resolution is 1280*800.

Upload Device Booting Image

You can upload the booting image to be displayed during the device's booting process if needed.

Go to **Device > Display Setting > Boot Logo** interface.



Boot Logo	Web Logo	Web Homepage Logo
Import Reset	Import Reset	Import Reset

- **Boot Logo:** The logo will appear on the screen when you reboot the device. Supported format: ZIP and PNG; Max size: 1280*800 png.
- **Web Logo:** The logo will appear in the upper left corner of the web interface. Supported format: JPG and PNG; Max size: 252*76 png.
- **Web Homepage Logo:** The logo will appear on the login page of the web interface. Supported format: JPG and PNG; Max size: 182*55 png.

Home Screen Display

You can select the **Default** or **Call List** home screen display.

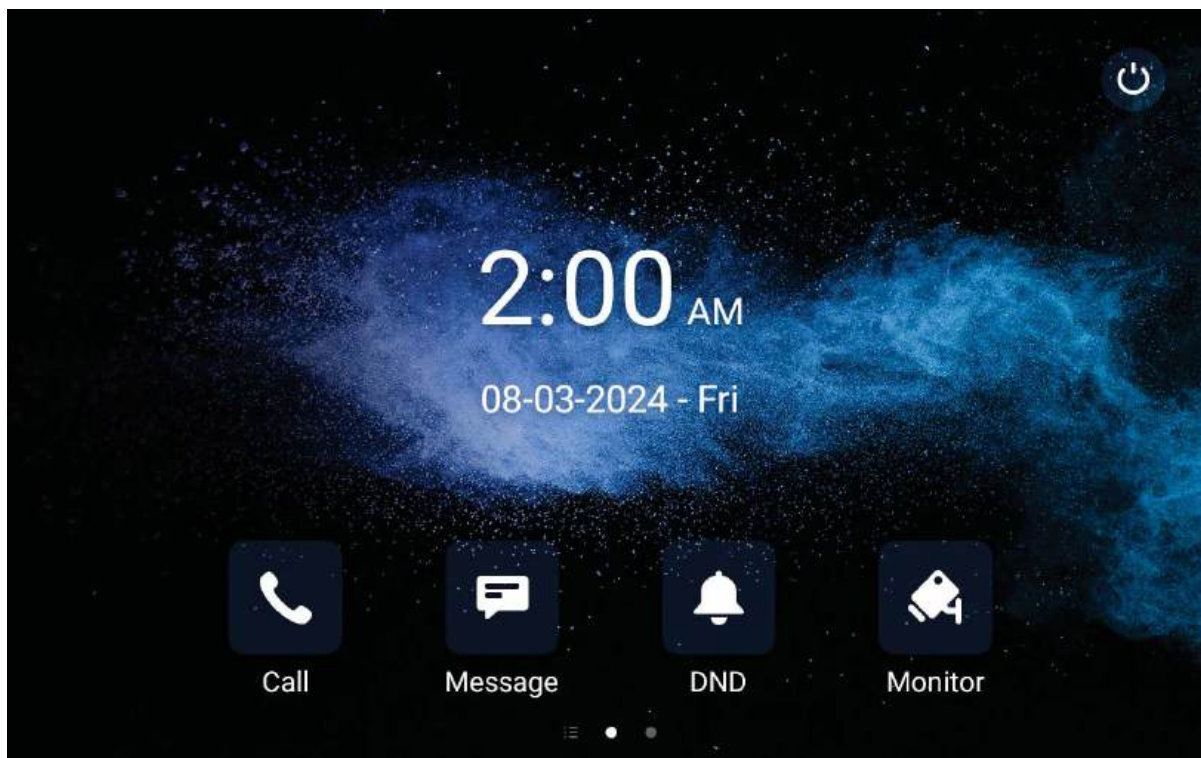
Go to **Device > Display Setting > Theme** interface.

Theme ?

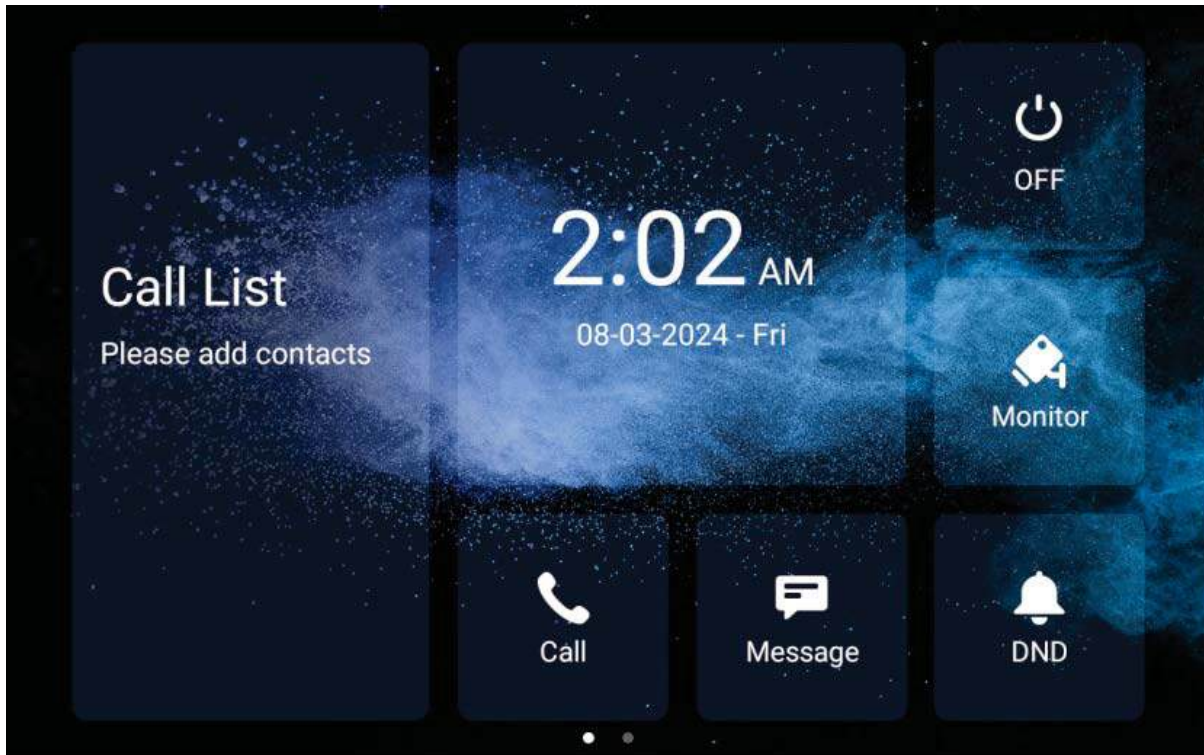
Theme

Default ?

Default Home Screen:



Call List Screen:



Status Bar Display Configuration

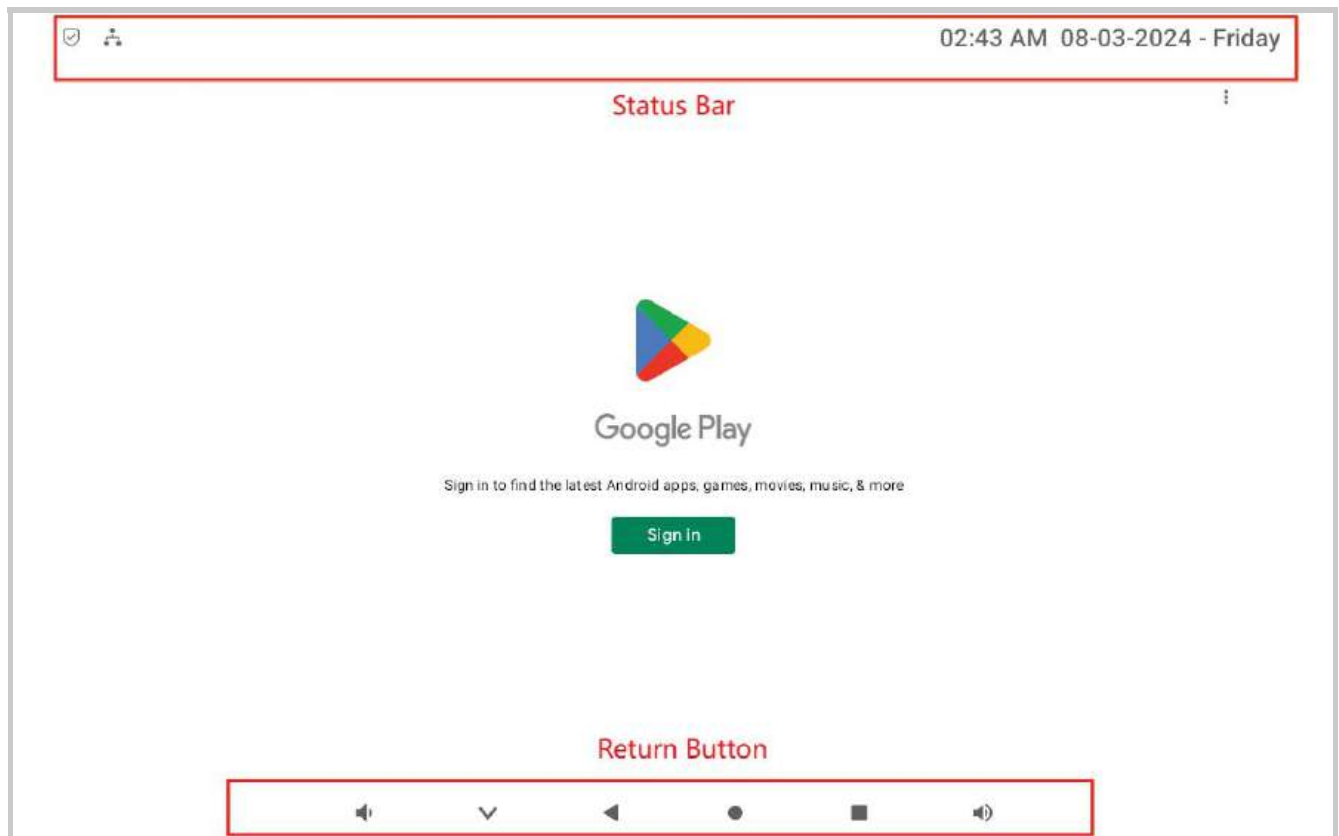
You can configure whether to display the status bar and return button when running a third-party app.

To set it up, go to the **Device > Display Setting > Display Settings** interface.

Display Settings

Status Bar Visible	Enabled	?
Return Button Hide Time	Never	?

- **Status Bar Visible:** Determine whether to display the status bar when running a third-party app.
- **Return Button Hide Time:** Determine that the return button will be concealed for certain seconds. If you select **Never**, the button will keep displaying. Users can swipe up on the screen to make the button appear.



Icon Display Configuration

Akuvox indoor monitor allows you to customize icon display on the **Home** screen and **More** screen for the convenience of your operation on the device web.

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

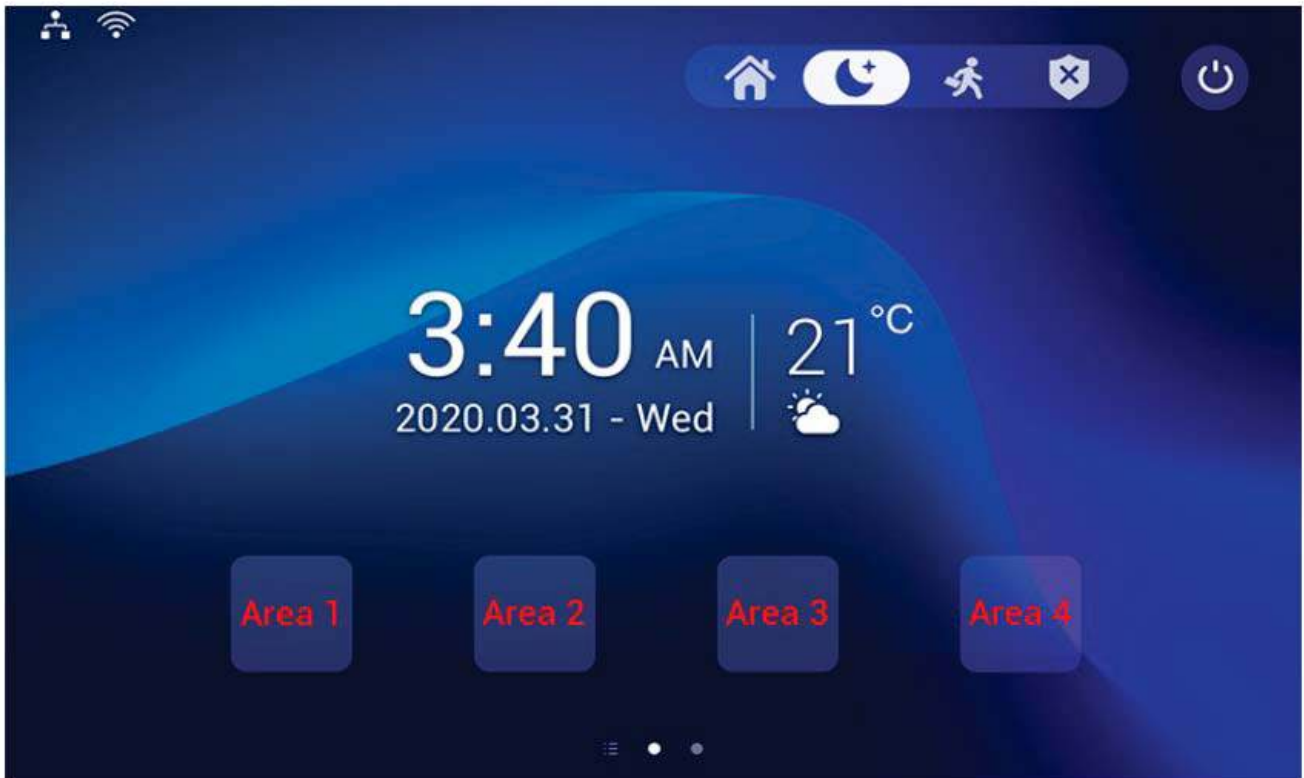
Home Page Display ? Example

Area	Type	Value	Label	Type(max size:100*100)
Area1	Call			Not selected any files Select File Delete
Area2	Message			Not selected any files Select File Delete
Area3	DND			
Area4	Monitor			Not selected any files Select File Delete

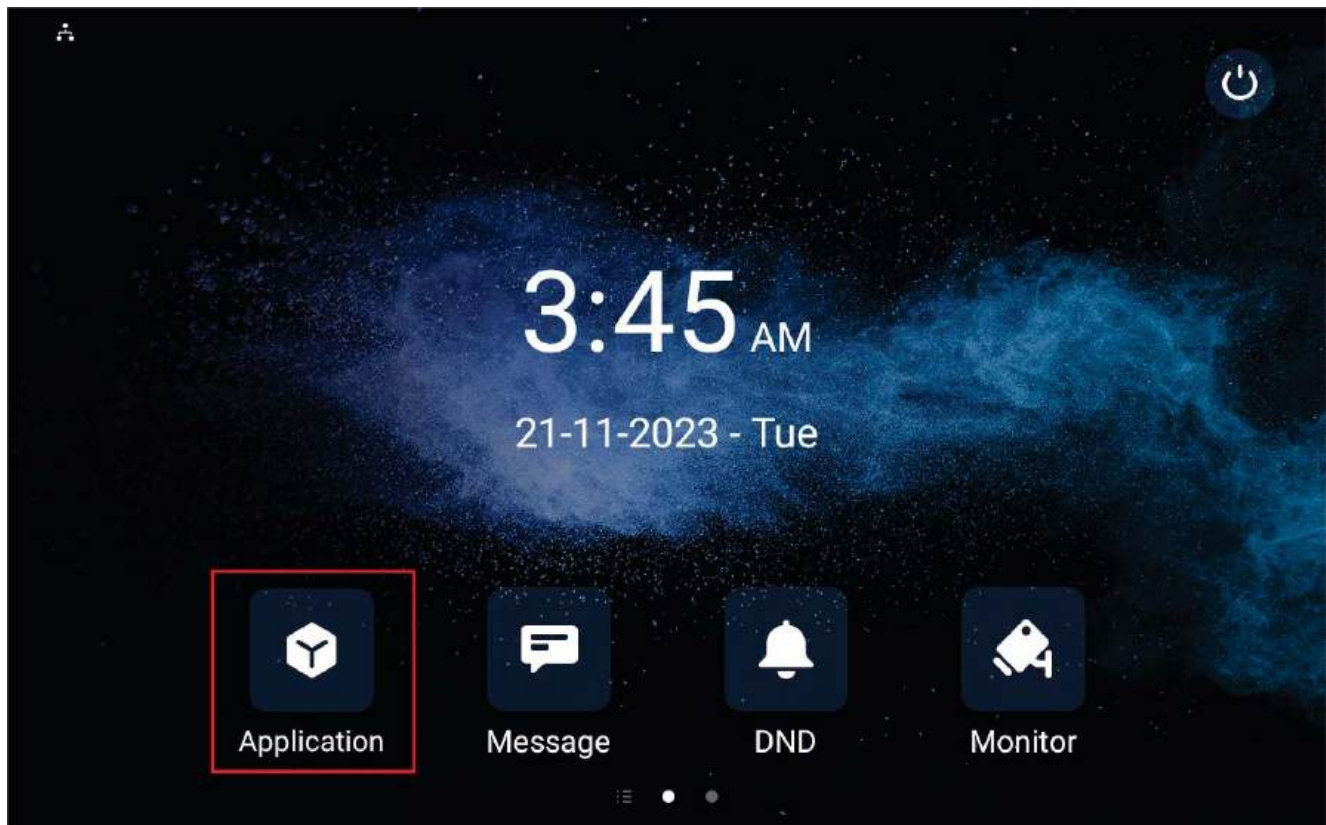
- **Type:** Select the functional icon to be displayed on the home screen(DND, Message, Contacts, Call, System Info, Settings, Arming, Lift, SOS, Unlock, Browser, Custom APK, Monitor, Relays, All Calls, Control4 Unlock, Application).
- **Value:** The value field for **Custom APK** will be automatically filled in if you have already installed a third-party app. If you select **Browser**, you are required to enter the URL of the browser before the browser icon can be displayed.
- **Label:** Name the icon. The DND icon cannot be renamed.

- **Icon:** Click to upload the icon picture. The maximum icon size is 100*100. The picture format can be JPG, JPEG, and PNG.

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



To easily access the third-party app, you can create an Application icon on the home screen. Tap the icon and run the desired app.



Configure the icons displayed on **More Page Display** on the same interface.

More Page Display ? Example

Area	Type	Value	Label	Type(max size:100*100)		
Area1	Contacts ▼			Not selected any files	Select File	Delete
Area2	Settings ▼			Not selected any files	Select File	Delete
Area3	Arming ▼			Not selected any files	Select File	Delete
Area4	Application ▼			Not selected any files	Select File	Delete
Area5	N/A ▼			Not selected any files	Select File	Delete
Area6	N/A ▼			Not selected any files	Select File	Delete

Function Tabs Configuration

You can set up the display of functional tabs on the talking, monitor, and call preview screens.

To set up tabs on the **Talking** screen, go to **Device > Display Setting > Softkey in Talking Page** interface.

Softkey In Talking Page ?

Key	Display	Label
Mute	Enabled ▼	
Switch	Enabled ▼	
Capture	Enabled ▼	
Keyboard	Enabled ▼	
Hang up	Enabled ▼	

- **Mute:** Tap to mute the talking.
- **Switch:** Tap to switch between Video and Audio talking mode.
- **Capture:** Tap to take a screenshot of the talking screen.
- **Keyboard:** Tap to display the keyboard.
- **Hang up:** Tap to end the call.

To set up tabs on the **Call Preview** screen, go to **Device > Display Setting > Softkey in Call-Preview Page** interface.

SoftKey In Call-Preview Page ?

Key	Display	Label
Capture	Enabled ▼	
Answer	Enabled ▼	
Hang up	Enabled ▼	

- **Capture:** Tap to take a screenshot of the preview screen.
- **Answer:** Tap to answer the incoming call.
- **Hang up:** Tap to end the call.

To set up tabs on the **Monitor** screen, go to **Device > Display Setting > Softkey in Monitor Page** interface.

SoftKey In Monitor Page ?

Key	Display	Label
Capture	Enabled ▼	
Cancel	Enabled ▼	

- **Capture:** Tap to take a screenshot of the monitor screen.
- **Cancel:** Tap to exit the monitor screen.

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 ▼	Unlock1	Local Relay ▼
Key2	Enabled ▼	Unlock2	Local Relay ▼
Key3	Enabled ▼	Unlock3	Remote Relay DTMF1 ▼

- **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 unlock tabs on the **Home** screen and **More** screen on the **SoftKey In Home Or More Page** section.

Softkey In Homepage or More Page ?

Status	Display Name	Type
Enabled ▼	Unlock	Remote Relay HTTP1 ▼

- **Status:** It is enabled by default.
- **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 **Monitor** screen on the **SoftKey In Monitor Page** section.

SoftKey In Monitor Page ?

Status	Display Name	Type
Enabled ▼	Unlock	Remote Relay HTTP ▼
Disabled ▼	Unlock	Remote Relay HTTP ▼
Disabled ▼	Unlock	Remote Relay HTTP ▼

- **Status:** With it enabled, the unlock tab will be displayed on the monitor 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 on the **SoftKey In Call-Preview Page** section.

Status	Display Name	Type
Enabled ▼	Unlock	Remote Relay HTTP ▼

- **Status:** With it enabled, it 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.

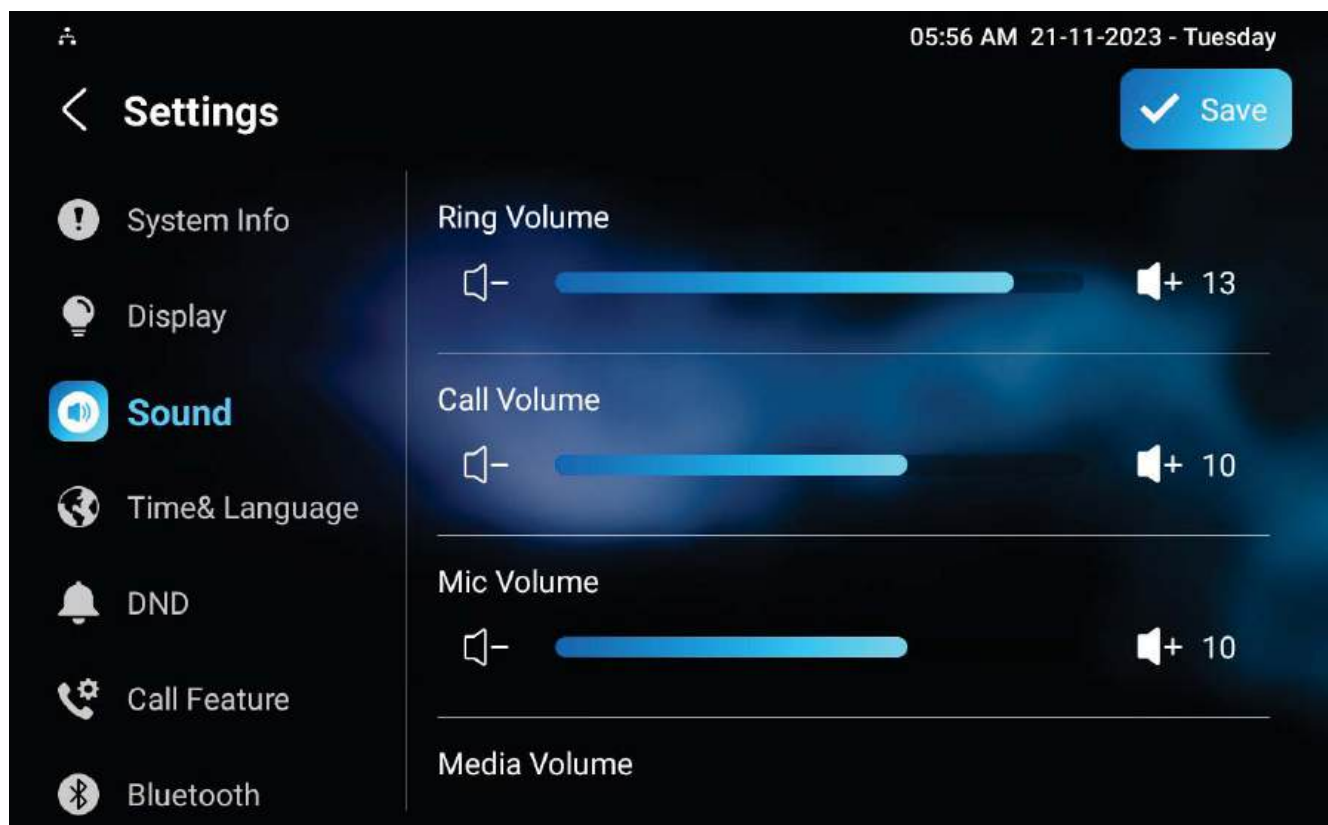
Sound and Volume Configuration

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.

Volume Configuration

Configure Volume on the Device

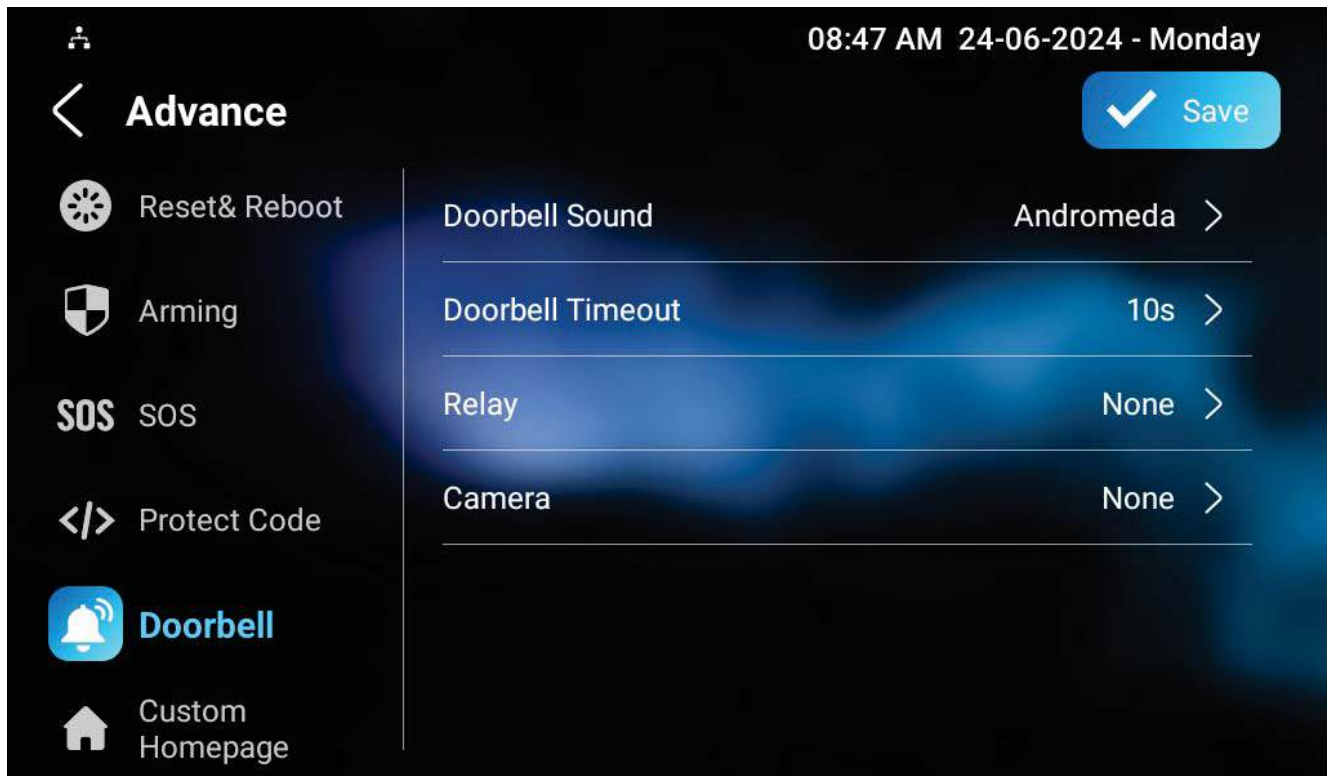
Set up the volumes on the device **Settings > Sound** screen.



- **Ring Volume:** The incoming call ringtone volume.
- **Call Volume:** The speaker volume during the call.
- **Mic Volume:** The mic volume.
- **Media Volume:** The volume for the video screen saver.
- **Touch Sound:** The icon tapping sound.
- **Phone Ringtone:** The ringtone for incoming calls.

- **Notification Sound:** The ringtone for the incoming messages.

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



- **Doorbell Sound:** Select the doorbell sound.
- **Doorbell Timeout:** Set the doorbell duration(from 10 seconds to 5 minutes).
- **Relay:** Select the local relay to be triggered along with the doorbell.
- **Camera:** Select the camera to be triggered along with the doorbell.

Configure Volume on the Web Interface

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

Volume Control

Ring Volume	13	(0~15)
Call Volume	10	(1~15)
Mic Volume	10	(1~15)
Media Volume	10	(0~15)

Touch Sound

Touch Sound Enabled	Enabled
---------------------	--------------------------------------

Upload Tones

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

Doorbell Sound Upload

Doorbell Sound Upload	Import
Doorbell Sound	Delete

Alarm Ringtone Upload

Alarm Ringtone Upload	Import
Alarm Ringtone	default.wav Delete

Ring Tone Upload

Ring Tone Upload	Import
Ring Tone	Delete

Note

The files to be uploaded should be in WAV or MP3 format. No limitation on the file size.

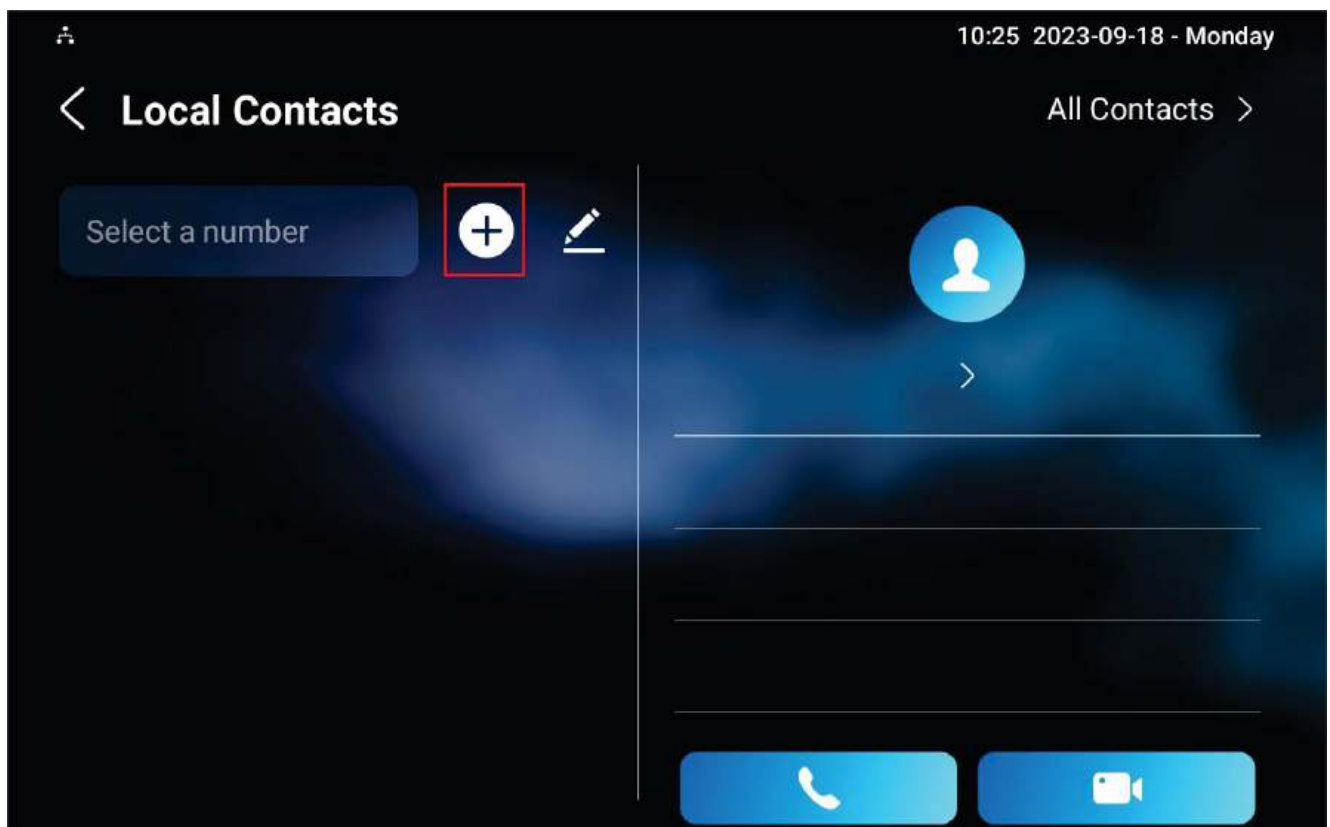
Contacts Configuration

Contacts Configuration on the Device

You can add, edit, and delete contacts on the device **Contacts> Local Contacts** screen directly.

Add Local Contact

Tap the **Add** icon to add a contact.



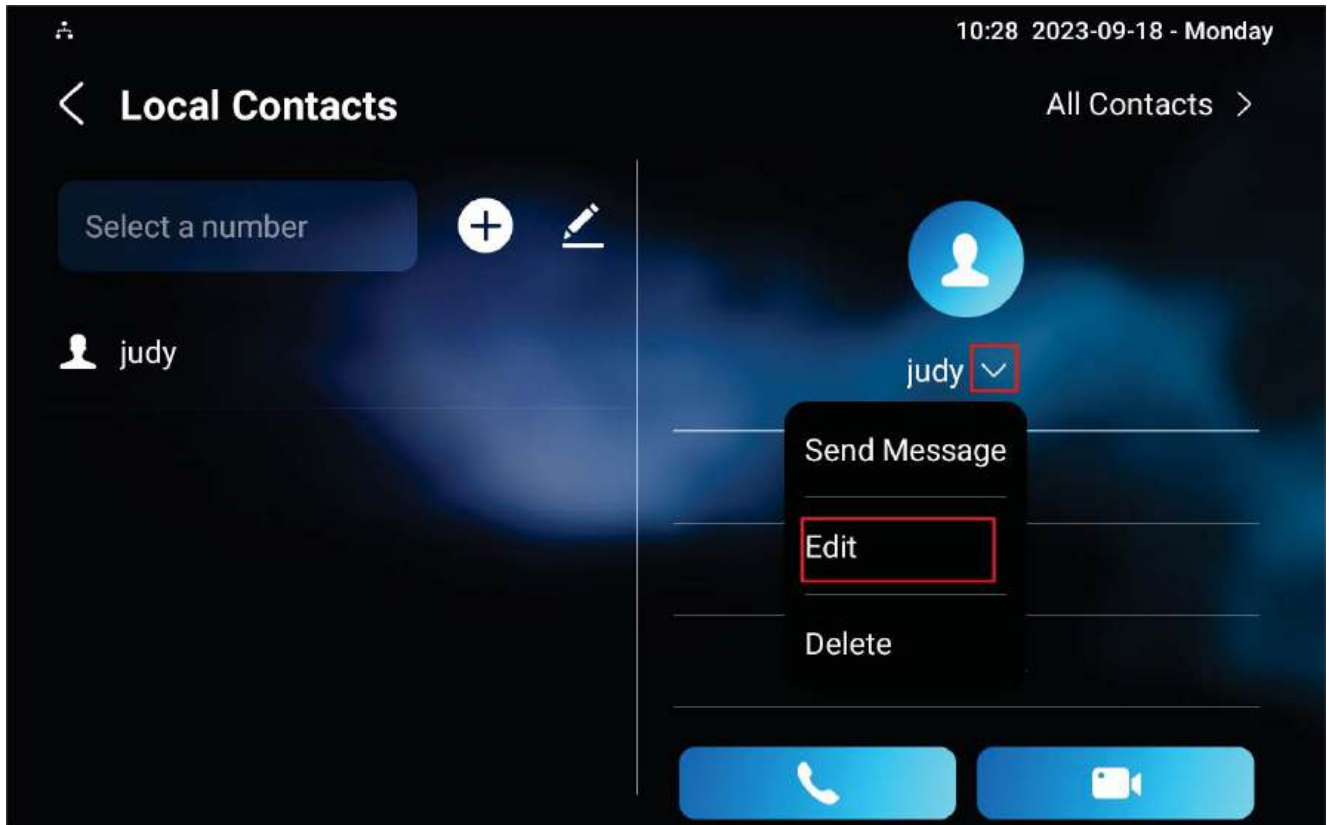
- **Account 1**: The account to make the call, Account 1 or Account 2.
- **New Contact Name**: Name the contact to distinguish it from others.
- **Number**: The IP or SIP number.
- **CameraUrl**: The RTSP URL for video preview.
- **Auto Ringtone**: The phone ringtone for incoming calls.

Note

Akuvox devices' RTSP URL format is [rtsp://device IP/live/ch00_0](#). If you use a third-party device, please confirm the URL format with the service provider.

Edit Contact

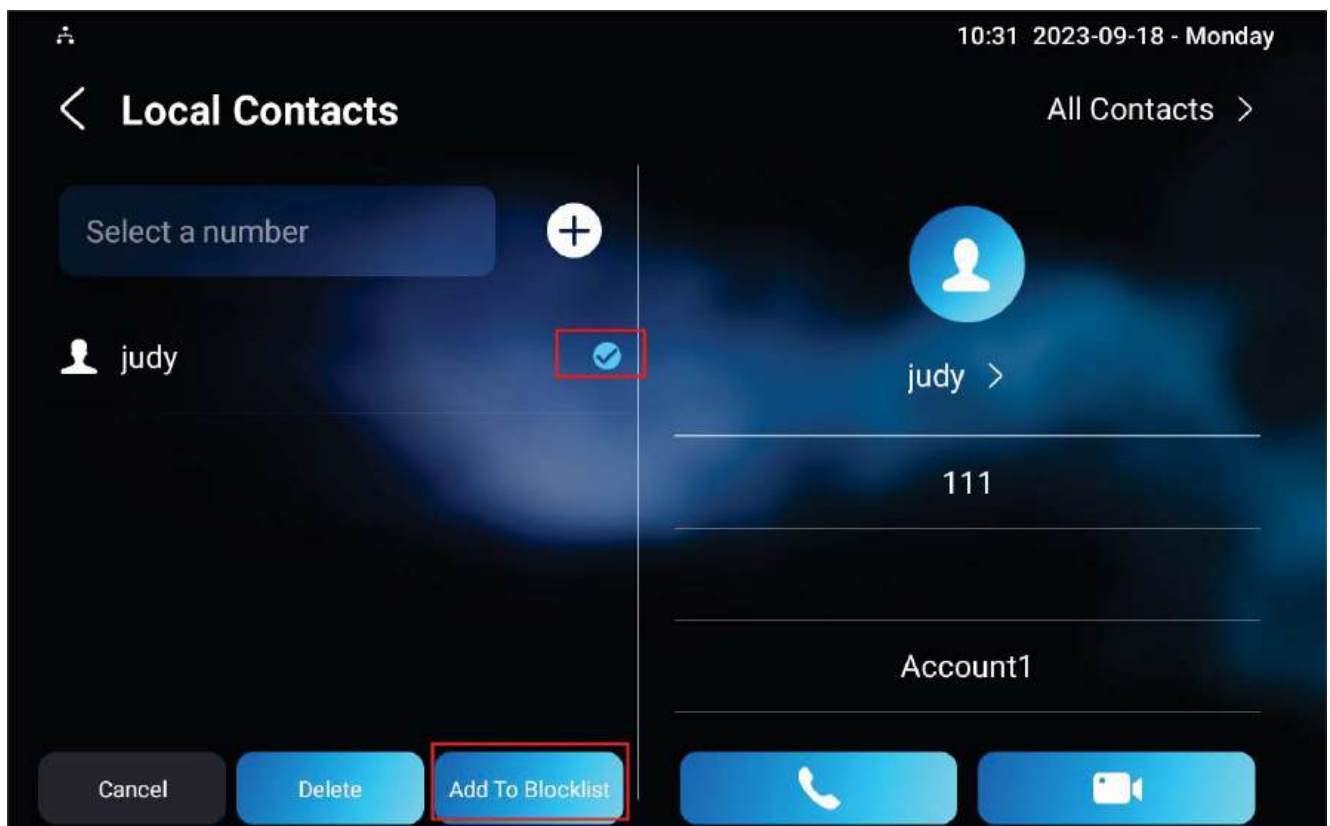
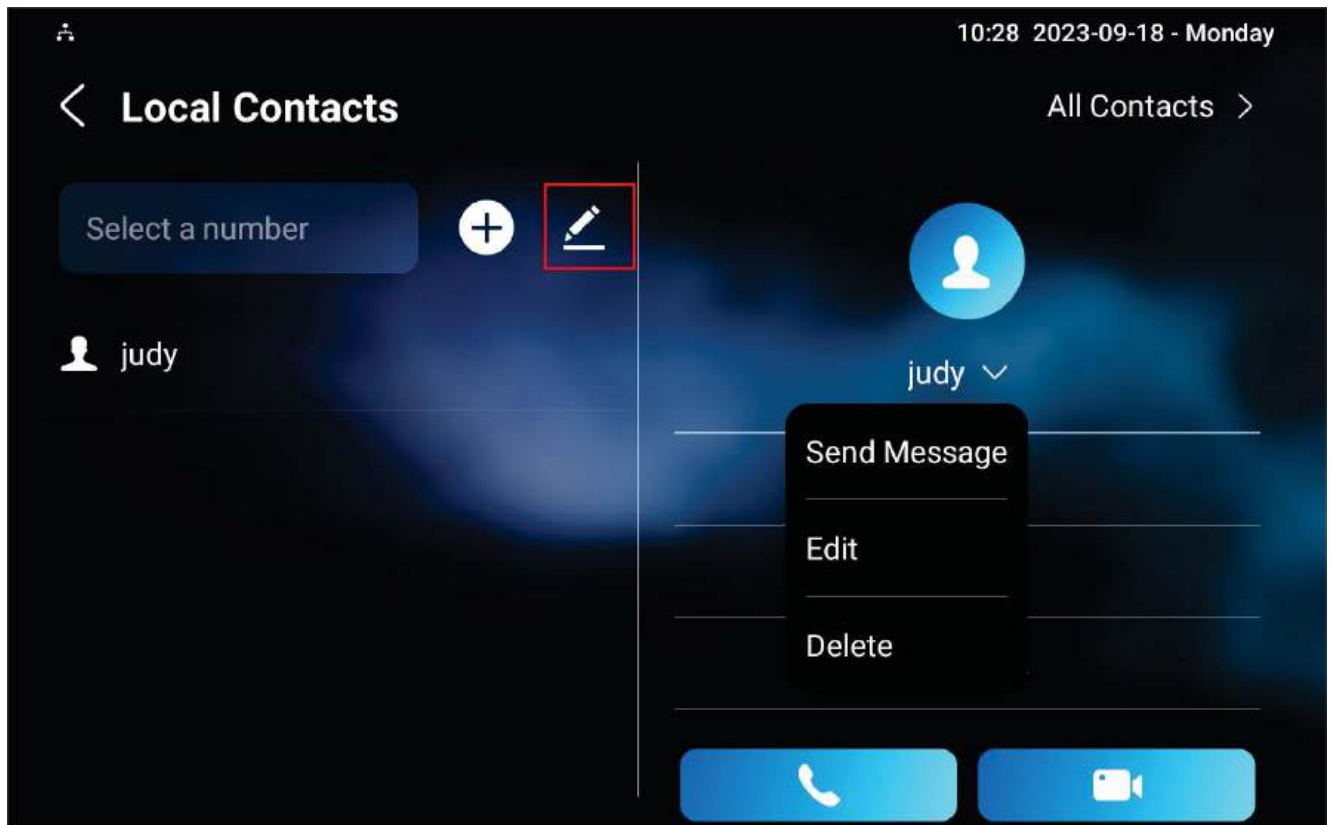
You can check and edit the existing contacts in the contact list. Choose one and click **Edit** to modify.



Block List Setting on the Device

You can choose from the contact list the contact you want to add to the block list.

Incoming calls from the contacts in the blocklist will be rejected. Press the **Edit** icon, select the contact, and press **Add To Blocklist**.



Note

You can delete contacts regardless of whether it is in Blocklist.

Contacts Configuration on the Web Interface

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**.

The screenshot displays the 'Local Contacts List' web interface. At the top, there's a 'Contacts List' dropdown menu set to 'All Contacts'. Below it is a search bar and buttons for 'Search', 'Reset', '+ Add', 'Import', and 'Export'. The main area is a table with columns: Index, Name, Number, Account, Ringtone, and Edit. The table is currently empty, showing 'No Data'. Below the table are pagination controls (Prev, 1/1, Next) and a 'Move To' dropdown set to 'All Contacts' with a 'Go' button. An 'Add Contact' modal is open, showing fields for Name, Number, Group (Default), Dial Account (Account1), and Ringtone (Auto Ringtone), with Cancel and Submit buttons.

- **Contacts List:** **All Contacts** displays all the contacts in the contact list. **Blocklist** displays the contacts in the blocklist.
- **Search:** Search 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.
- **Group:** Calls from contacts in **Blocklist** will be rejected.
- **Dial Account:** The account to make the call, Account 1 or Account 2.
- **Ringtone:** The ringtone for the incoming call from the contact.

Note

If you want to remove the contact from the blocklist on the web interface, you can change the group to Default when editing the contact.

Import and Export Contacts

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

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

Contact List Display Configuration

To conduct the contact display, go to the web **Contacts > Local Contacts > Contacts List Setting** interface.

- **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.

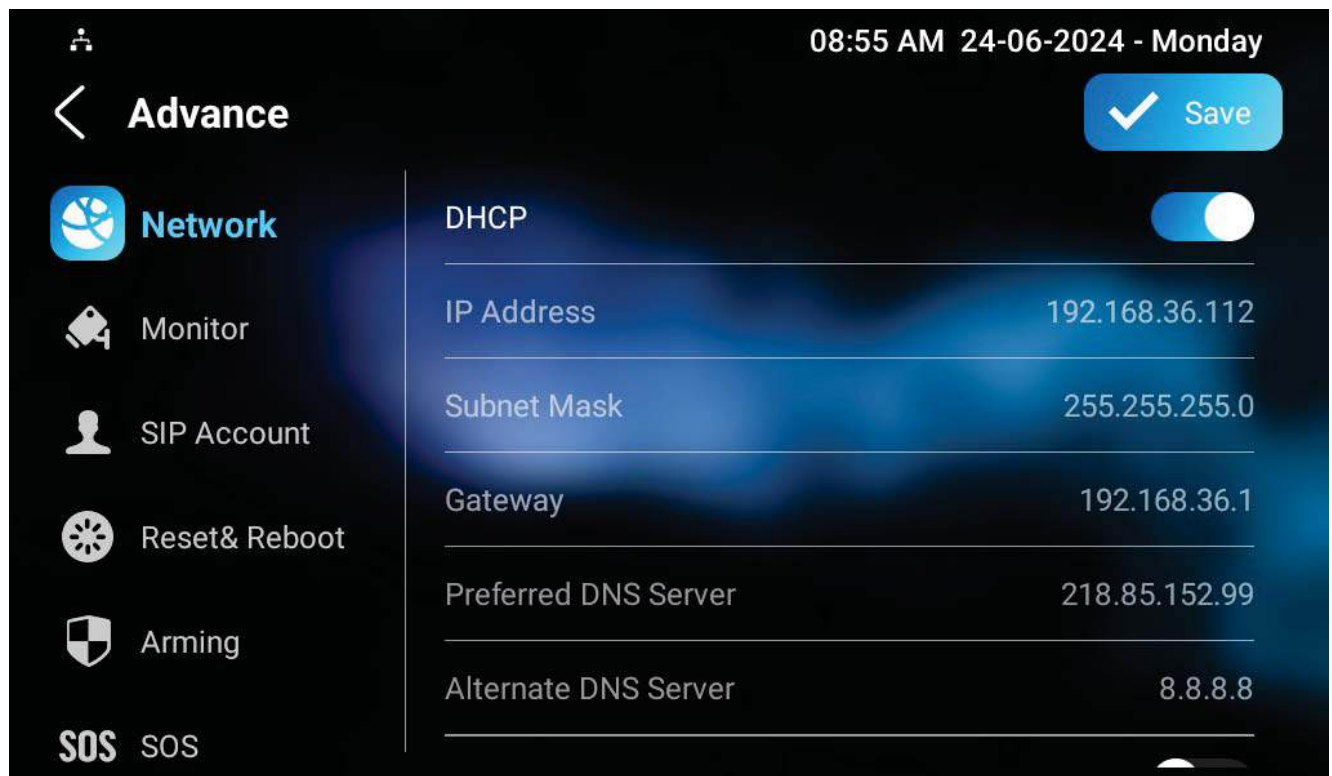
Network Setting & Other Connection

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.

Configure Device Network Connection on the Device

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



- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is turned on, the device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. If you turn off the DHCP mode, the device will be changed to static IP mode, and the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **IP Address:** The IP address when the static IP mode is selected.

- **Subnet Mask:** The subnet mask should be set up according to the actual network environment.
- **Gateway:** The gateway should be set up according to the IP address.
- **Preferred & Alternate DNS Server:** The preferred and alternate Domain Name Server(DNS). The preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.
- **Hotspot Enabled:** With it enabled, the device can provide the network for other devices.

Note

- You can press System Info, and then press Network on the Settings screen to check device network status.
- The default code to enter advanced settings is 123456.

Configure Device Network Connection on the Web Interface

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

Network Information ?	
Network Type	LAN
LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.36.112
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.36.1
Preferred DNS Server	218.85.152.99
Alternate DNS Server	8.8.8.8
Primary NTP	0.pool.ntp.org
Secondary NTP	1.pool.ntp.org

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

LAN Port ?

Type	☐ DHCP ☒ Static IP ?
LAN IP Address	192.168.36.112 ?
LAN Subnet Mask	255.255.255.0 ?
Default Gateway	192.168.36.1 ?
Preferred DNS Server	218.85.152.99 ?
Alternate DNS Server	8.8.8.8 ?

- **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.
- **LAN IP Address:** The IP address when the static IP mode is selected.
- **LAN Subnet Mask:** The subnet mask should be set up according to the actual network environment.
- **Default Gateway:** The gateway should be set up according to the IP address.
- **Preferred/Alternate DNS Server:** The preferred and alternate Domain Name Server(DNS). The preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

To enable the WLAN hotspot, go to the **Network > Advanced > WLAN Hotspot** interface.

WLAN Hotspot ?

Hotspot Enabled
☐
?

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 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**. **None** is the default factory setting indicating the device is not in any server type.
- **Discovery Mode:** With discovery mode enabled, the device can be discovered by other devices in the network. Uncheck the box if you want to conceal the device.
- **Device Node:** Specify the device address by entering device location info from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.
- **Device Extension:** The device extension number for the device you installed.
- **Device Location:** The location in which the device is installed and used.

Device NAT Setting

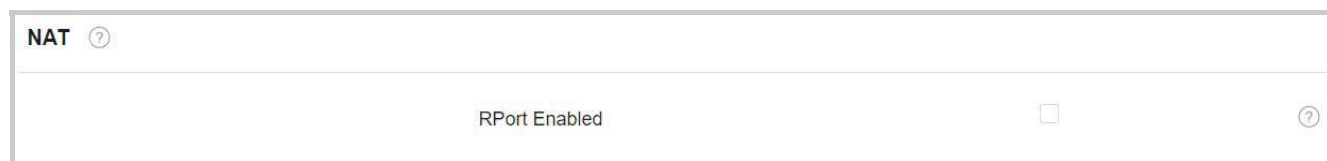
Network Address Translation(**NAT**) lets devices on a private network use a single public IP address to access the internet or other public networks. NAT saves the limited public IP addresses, and hides the internal IP addresses and ports from the outside world.

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

- **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.



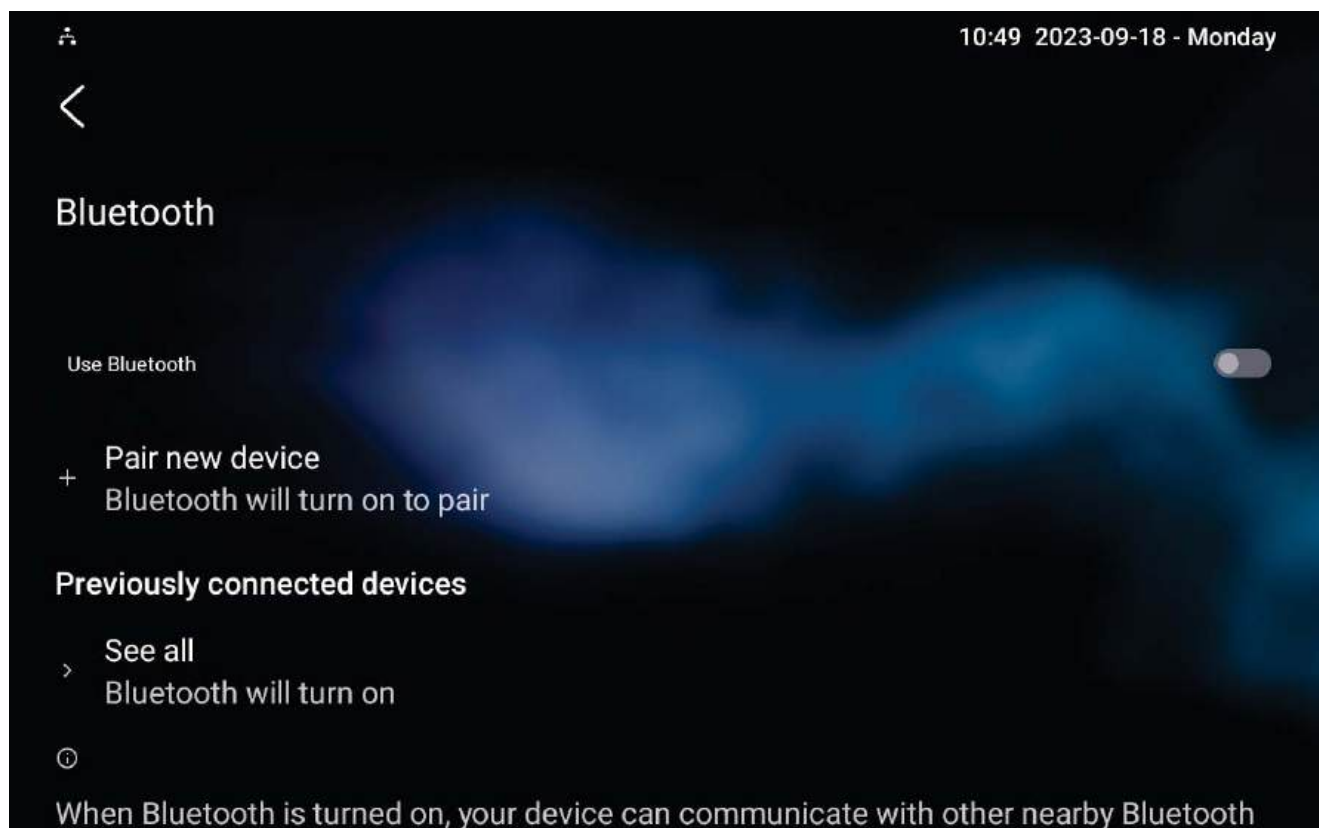
- **RPort:** Enable the RPort when the SIP server is in a WAN.

Device Bluetooth Setting

Device Bluetooth Pairing

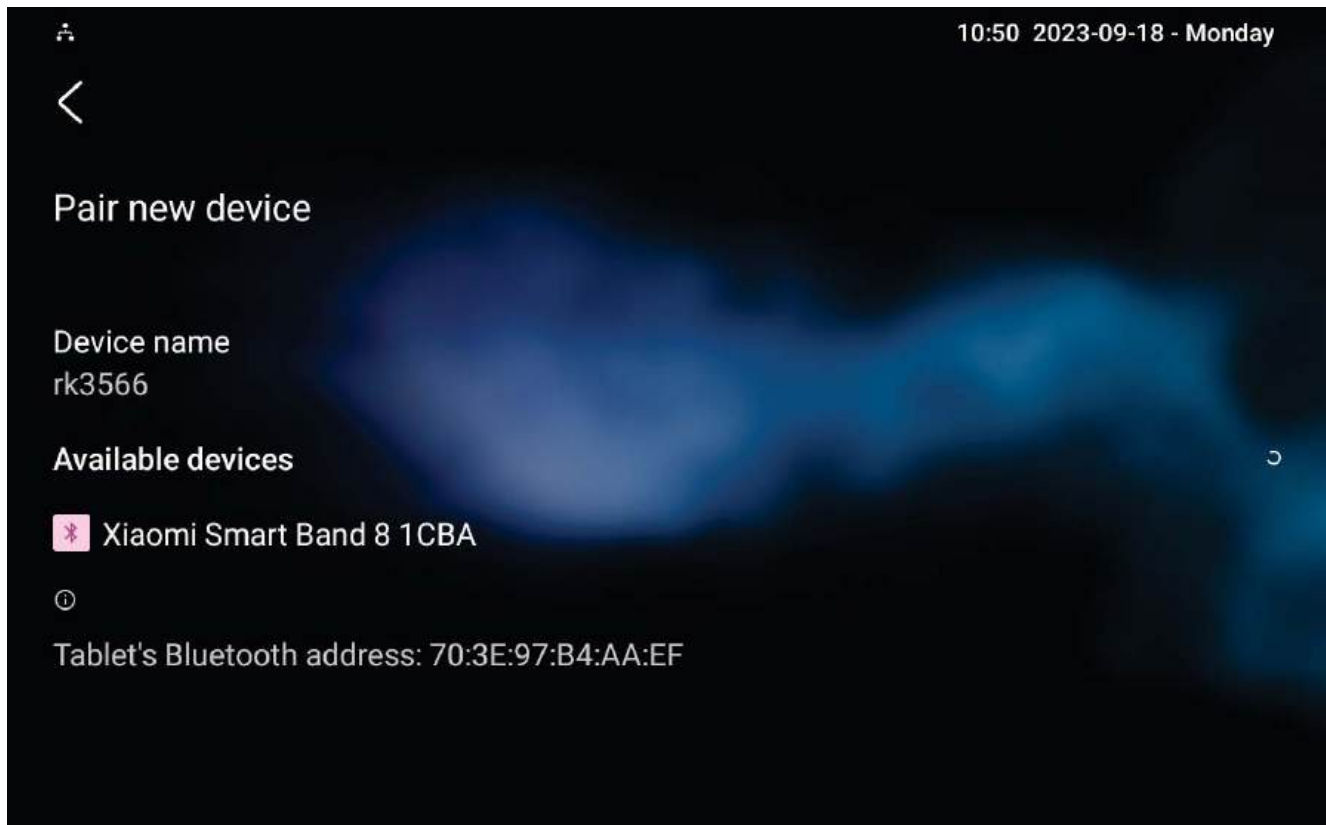
You need to enable the Bluetooth feature on the device before you can pair the indoor monitor with other Bluetooth-featured devices.

To set it up, go to **Settings > Bluetooth** screen.



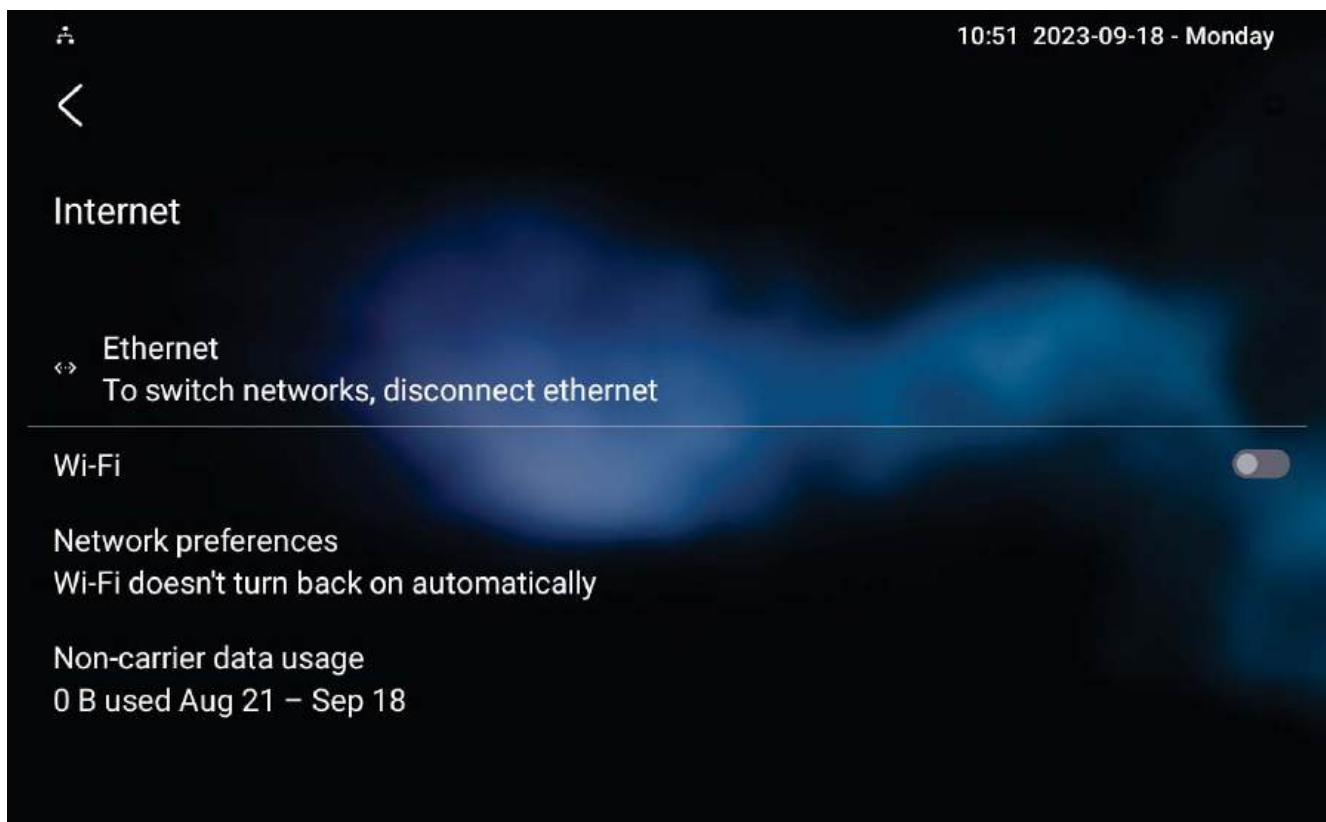
Device Bluetooth Data Transmission

Transfer data via Bluetooth by pressing **Pair new device**.



Device Wi-Fi Setting

Set the Wi-Fi on the device **Settings > WIFI** screen.



Intercom Call Configuration

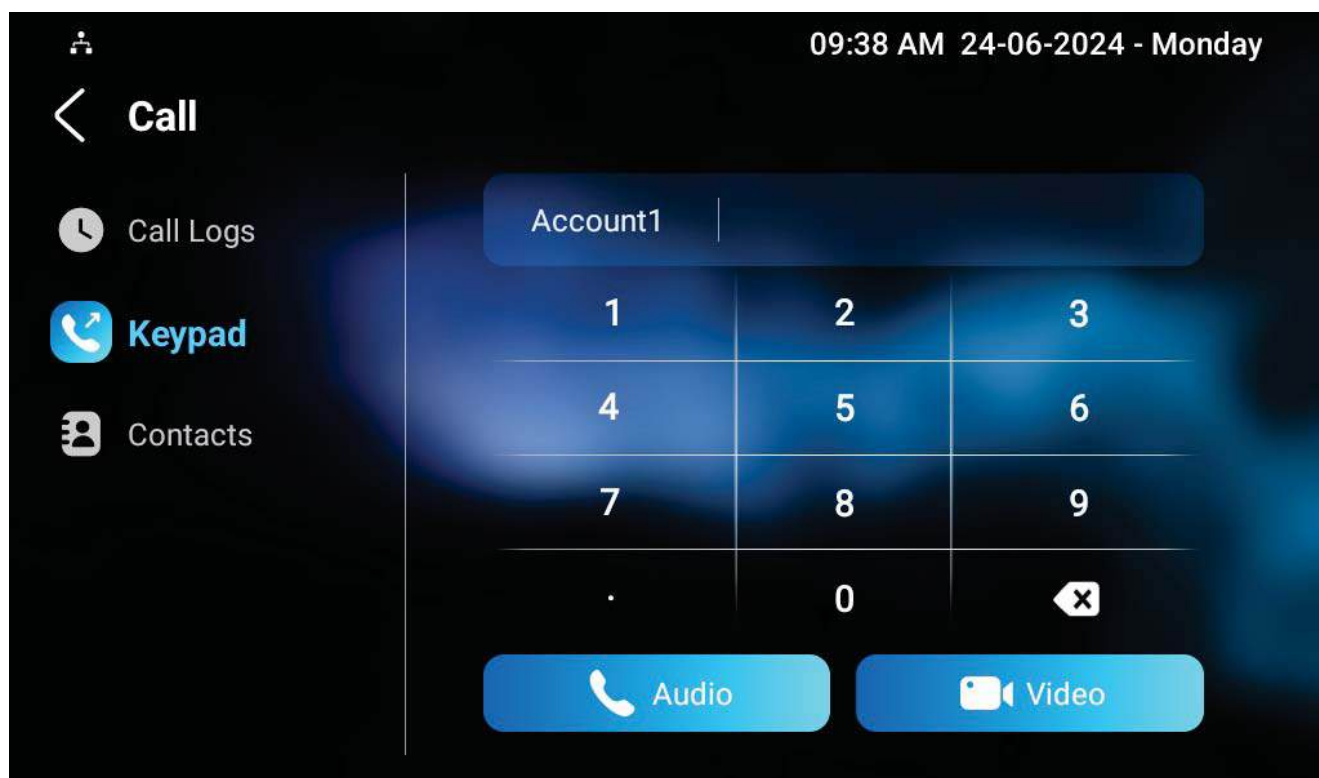
IP Call & IP Call Configuration

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

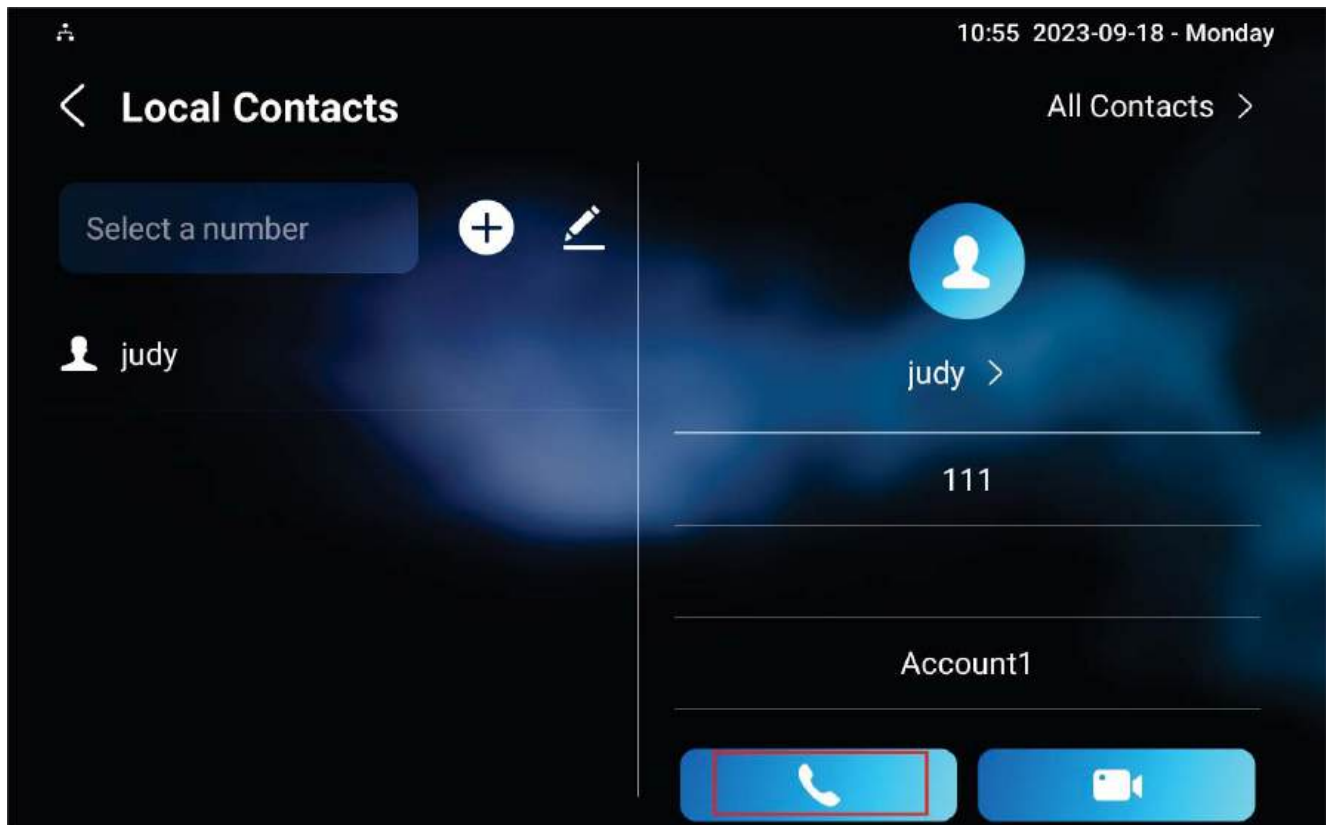
Make IP Calls

Make a direct IP call on the device **Call > Keypad** screen.

Enter the IP address on the soft keyboard, select the account to make the call, and press the **Audio** or **Video** tab to call out.



In addition, you can also make IP calls on the **Contacts > Local Contacts** screen.



IP Call Configuration

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 (0~30Sec) ?	
Answer Mode	Video ▼	?
Answer Tone	Enabled ▼	?
Busy Tone	☒	?
Indoor Auto Answer	☐	?
Auto Hang Up	☐	?
Direct IP Call	☒	?
Direct IP Call Port	5060 (1~65535) ?	
Local Relay1 Trigger By Incoming	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 & SIP Call Configuration

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

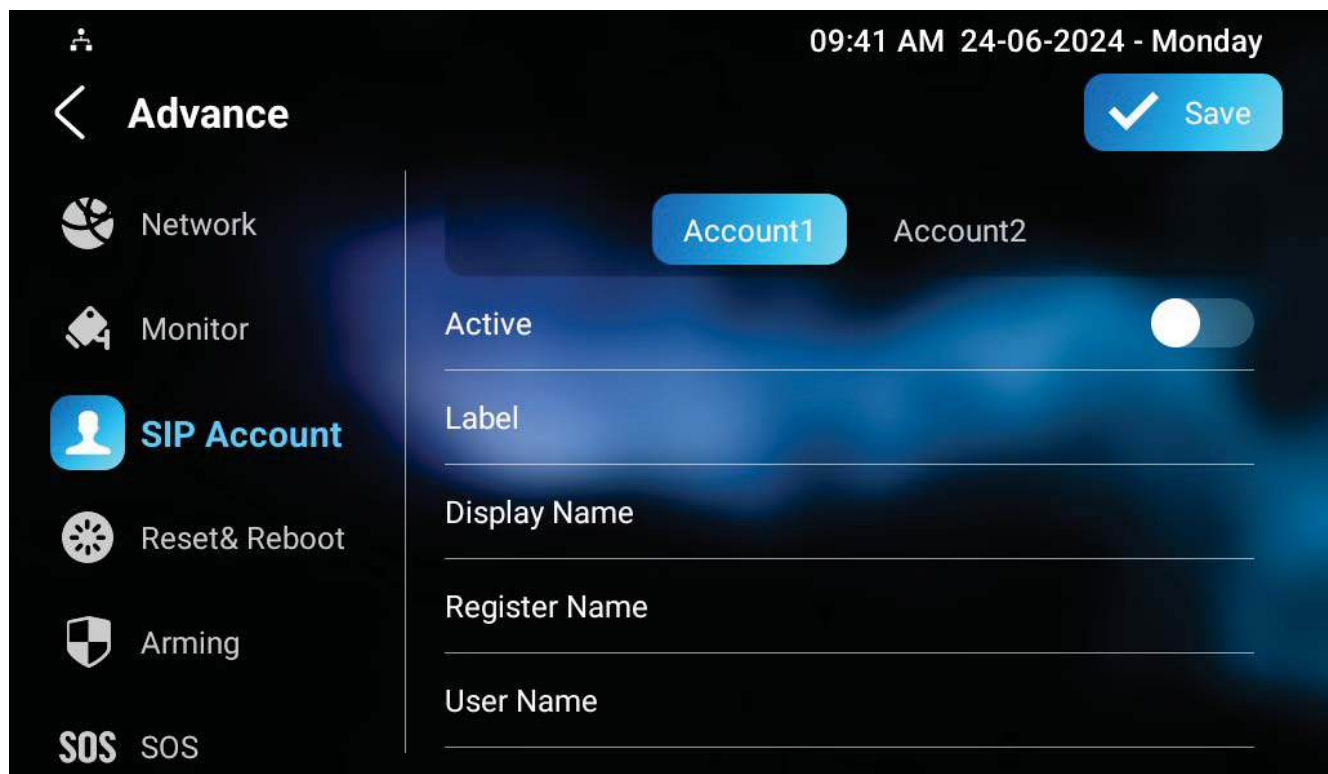
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

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.

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



- **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.
- **User Name:** 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.

The screenshot shows the 'SIP Account' configuration page. At the top left is the title 'SIP Account' with a help icon. Below it is a table with two columns: labels on the left and input fields on the right. Each input field has a help icon to its right. The fields are: 'Status' (a dropdown menu showing 'Disabled'), 'Account' (a dropdown menu showing 'Account1'), 'Account Enabled' (a checkbox), 'Display Label' (a text input field), 'Display Name' (a text input field), 'Register Name' (a text input field), 'Username' (a text input field), and 'Password' (a text input field with masked characters '*****').

Field	Value
Status	Disabled
Account	Account1
Account Enabled	☐
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.

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 > Advance > SIP Account** screen or navigate to the web **Account > Basic > SIP Account** interface.

The screenshot shows the 'Advance' settings menu with 'SIP Account' selected. The configuration for 'Account1' is displayed with the following fields:

- Register Name
- User Name
- Password
- SIP Server
- SIP Port: 5060

A red box highlights the 'SIP Server' and 'SIP Port' fields. A 'Save' button is located in the top right corner.

The web interface for 'SIP Server' configuration contains the following fields:

Field	Value	Help Icon
Server Address		?
Sip Server Port	5060	(1024~65535) ?
Registration Period	1800	(120~65535S) ?

- **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 Configuration

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

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

- **Preferred Outbound Proxy Server:** Enter the SIP proxy IP address.
- **Preferred Outbound Proxy Server Port:** Set the port for establishing a call session via the outbound proxy server.
- **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.

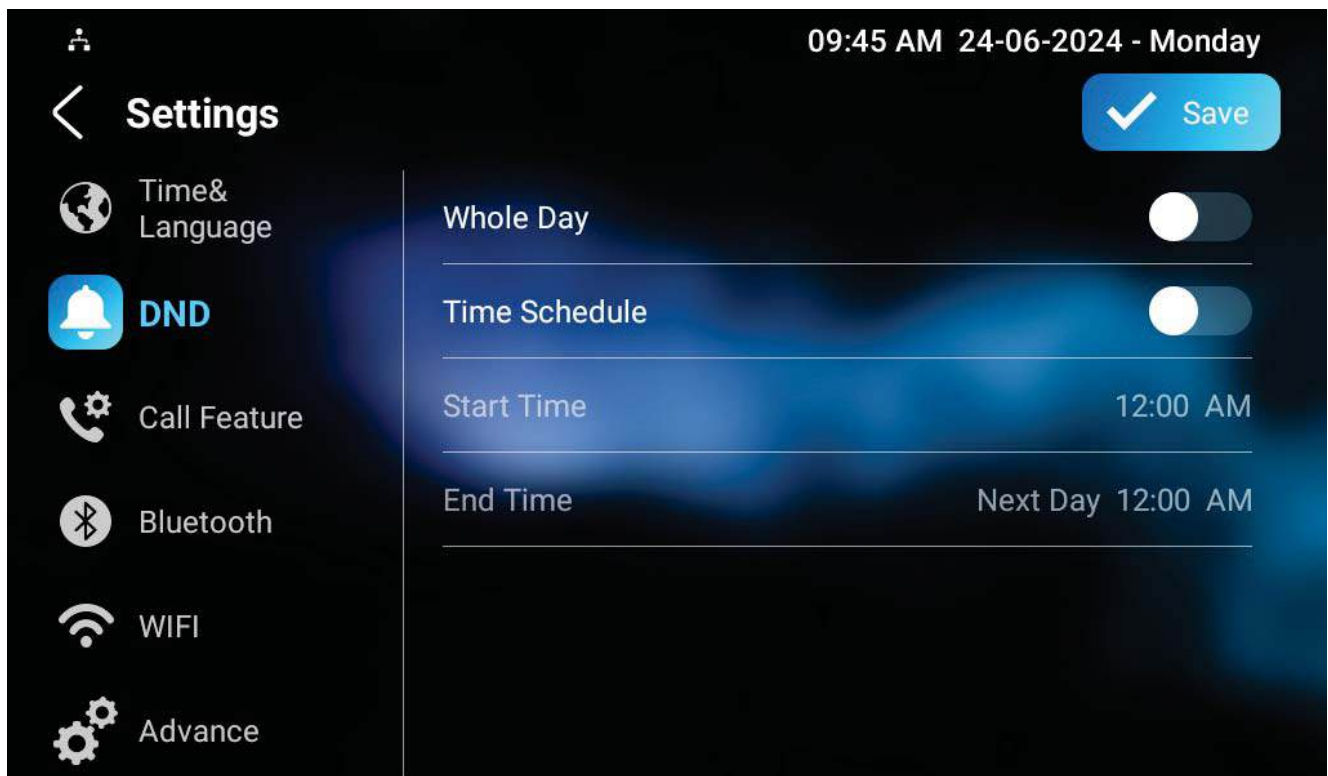
SIP Call DND & Return Code Configuration

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

To set it up, go to **Device > Call Feature > DND** interface.

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

You can also set up DND on the device. Tap **Settings > DND**.



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

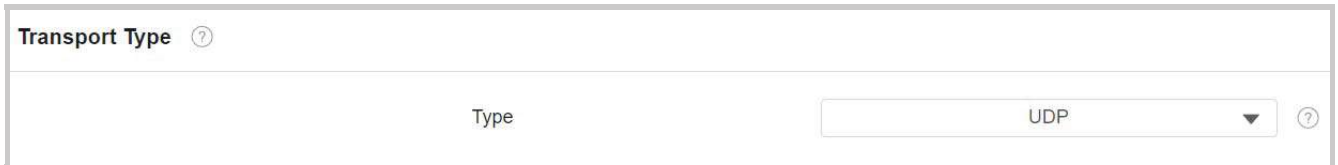
Local RTP ?		
Starting RTP Port	11800	(1024-65535) ?
Max RTP Port	12000	(1024-65535) ?

- **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 Configuration

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

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



Type
UDP

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

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. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

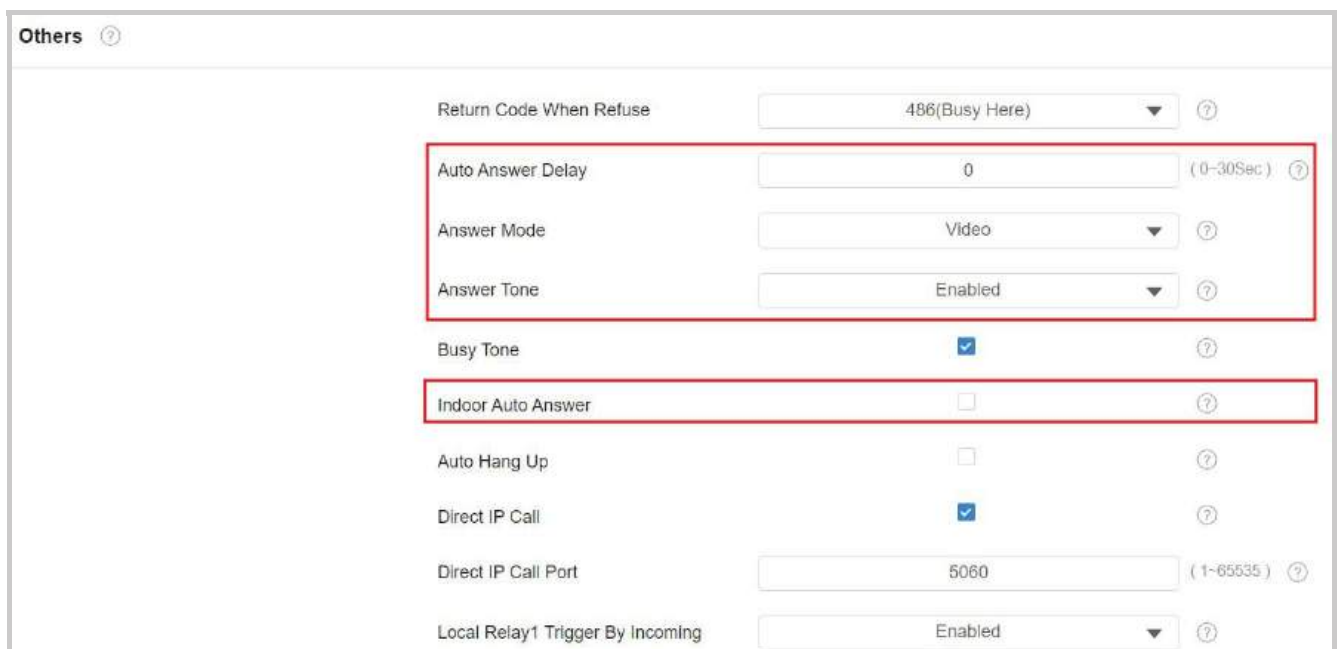
To enable the auto-answer feature, go to the web **Account > Advanced > Call** interface.



The screenshot shows the 'Call' configuration page with the following settings:

Setting	Value	Range/Options
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.



The screenshot shows the 'Others' configuration page with the following settings:

Setting	Value	Range/Options
Return Code When Refuse	486(Busy Here)	
Auto Answer Delay	0	(0-30Sec)
Answer Mode	Video	
Answer Tone	Enabled	
Busy Tone	☒	
Indoor Auto Answer	☐	
Auto Hang Up	☐	
Direct IP Call	☒	
Direct IP Call Port	5060	(1-65535)
Local Relay1 Trigger By Incoming	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 Mode:** Determine whether to auto-answer the call as a video or audio call.
- **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.
- **Auto Hang Up:** Set whether to hang up the incoming calls automatically.
- **Local Relay1 Trigger By Incoming:** Set whether to trigger the local relay by incoming calls.

Auto-answer Allow List 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 **Security > Allowlist** interface. Click **+Add** to add the allowed device.

Auto Answer AllowList ⓘ

Auto Answer When DND Enabled ☒ ⓘ

[+ Add](#) [Import](#) [Export](#)

Index	Device Location	SIP/IP	Permissions	Edit
No Data				

[Delete](#) [Delete All](#) [Prev](#) [Next](#) 1/1 [Go](#)

- **Auto Answer When DND Enabled:** Indicate that the auto-answer feature is effective when DND is turned on.

The screenshot shows the 'Auto Answer AllowList' management interface. At the top, there's a toggle for 'Auto Answer When DND Enabled' which is checked. Below this are buttons for '+ Add', 'Import', and 'Export'. A table with columns 'Index', 'Device Location', 'SIP/IP', 'Permissions', and 'Edit' is visible in the background. In the foreground, a modal window titled 'Add Auto Answer AllowList' is open. It contains three input fields: 'Device Location', 'SIP/IP', and 'Permissions'. The 'Permissions' field has two checkboxes: 'Auto Answer' and 'API'. At the bottom of the modal are 'Cancel' and 'Submit' buttons.

- **Device Location:** Specify the allowed device's name or location.
- **SIP/IP:** Enter the allowed device's SIP or IP number.
- **Permissions:**
 - **Auto Answer:** The call from the device will be answered automatically.
 - **API:** The device is allowed to access API.

You can import or export the allowlist on the same interface.

Auto Answer AllowList

Auto Answer When DND Enabled ☒

+ Add

Import

Export

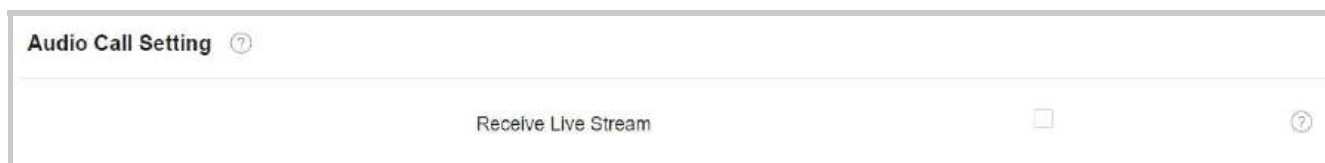
Note

- 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.

Live Stream Setting

The Receive Live Stream function enables the indoor monitor to view the one-way video stream from the calling party, regardless of whether the call is audio or video. Meanwhile, the video feed from the indoor monitor is not transmitted to the calling device, protecting the privacy.

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



When it is enabled, calling parties cannot see users when they want to have a two-way video call with users. See the details below:

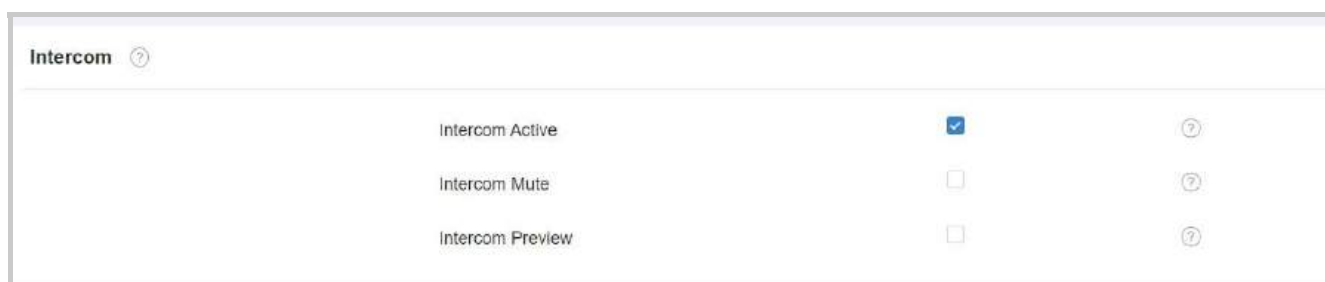
- If an incoming call is received on an audio basis on the device, the user can still see the video image of the calling party, while the calling party cannot see the user's. Thus, it protects the user's privacy.
- If an incoming call is received on a video basis on the device, the user and the calling party can see each other in the two-way video call.

Note

Only the indoor monitor with a camera module has this feature.

Intercom Active, Mute, and Preview

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

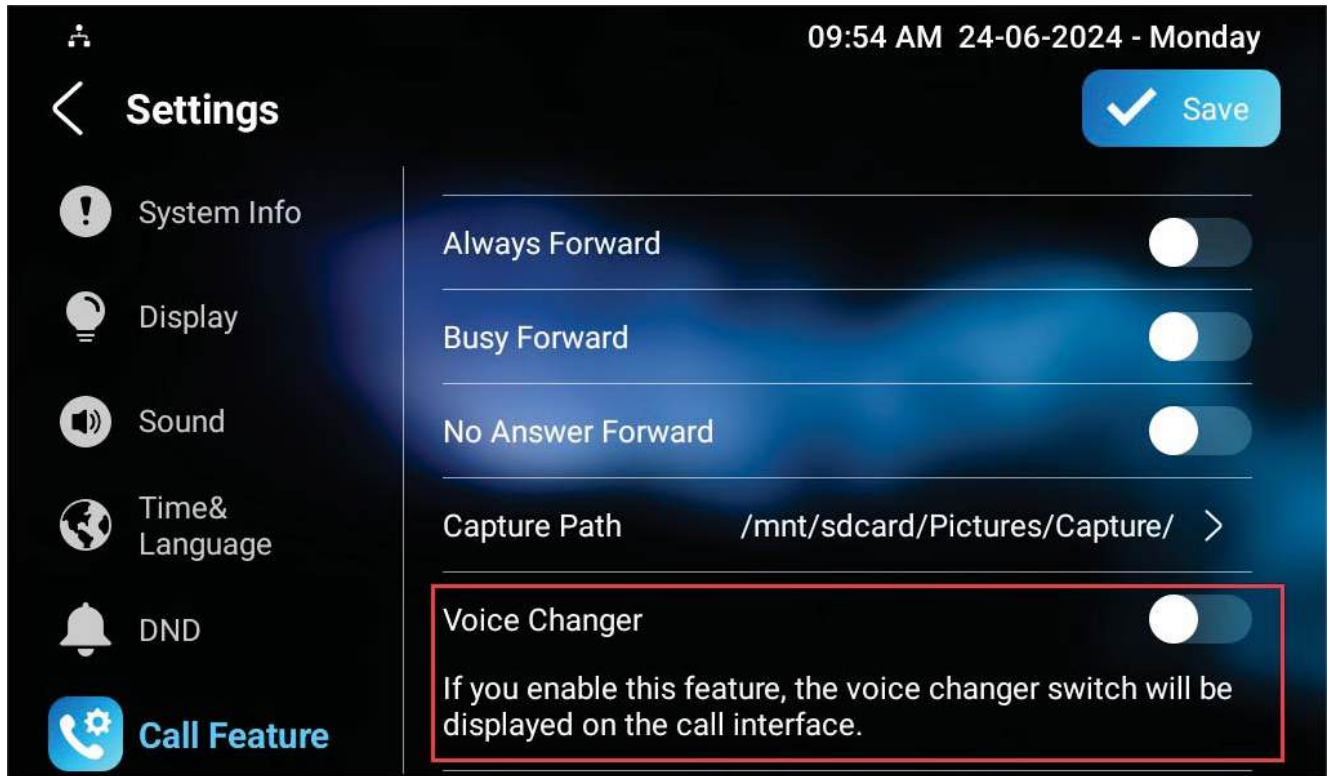


- **Intercom Active** : It is enabled by default.
- **Intercom Mute** : Mute the voice from the callee side.
- **Intercom Preview** : Enable the incoming call preview. If it is enabled, the group call is not available.

Voice Changer

Voice changer ensures users' privacy and home security. For example, users (especially women and children) can protect themselves by changing their voices when talking to a stranger.

Set it up on the device **Settings > Call Feature** screen.



Emergency Call Setting

The Emergency Call function is designed for urgent situations, particularly beneficial for the elderly and children. Users can display the SOS button on the indoor monitor's screen. When the button is pressed, the device automatically calls the designated emergency contacts, ensuring quick help when needed.

To display the emergency call softkey, navigate to the web **Device > Display Setting > Home Page Display/More Page Display** interface.

Home Page Display
Example

Area	Type	Value	Label	Type(max size:100*100)
Area1	Call			Not selected any files Select File Delete
Area2	SOS		SOS	Not selected any files Select File Delete
Area3	DND			
Area4	Monitor			Not selected any files Select File Delete

More Page Display
Example

Area	Type	Value	Label	Type(max size:100*100)
Area1	Contacts			Not selected any files Select File Delete
Area2	Settings			Not selected any files Select File Delete
Area3	Arming			Not selected any files Select File Delete
Area4	Application			Not selected any files Select File Delete
Area5	N/A			Not selected any files Select File Delete
Area6	N/A			Not selected any files Select File Delete

You also need to set up specific parameters on the device or the device web interface. To set it up on the device, go to **Settings > Advance > SOS** screen.

09:56 AM 24-06-2024 - Monday

< Advance
Save

Monitor
SIP Account
Reset& Reboot
Arming
SOS SOS
</> Protect Code

Call Number1
Call Number2
Call Number3
Call Timeout 60s >
Loop Times 3 >
SIP Account Auto >

- **Call Number:** 3 SOS numbers can be set up. Once users press the SOS key on the home page, indoor monitors will call out the numbers in order.
- **Call Timeout:** The call duration for each number. When users call out and the other side does not answer within the timeout, indoor monitors will continue to call the next number.

- **Loop Times:** Set up the call loop times.
- **SIP Account:** The account to make SOS calls.

To set it up on the web interface, go to **Device > Intercom > SOS** interface.

SOS ?

Account	Auto ▼	?
Call Number 1		?
Call Number 2		?
Call Number 3		?
Call Timeout	60 ▼	?
Loop Times	3 ▼	?

Multicast Configuration

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

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

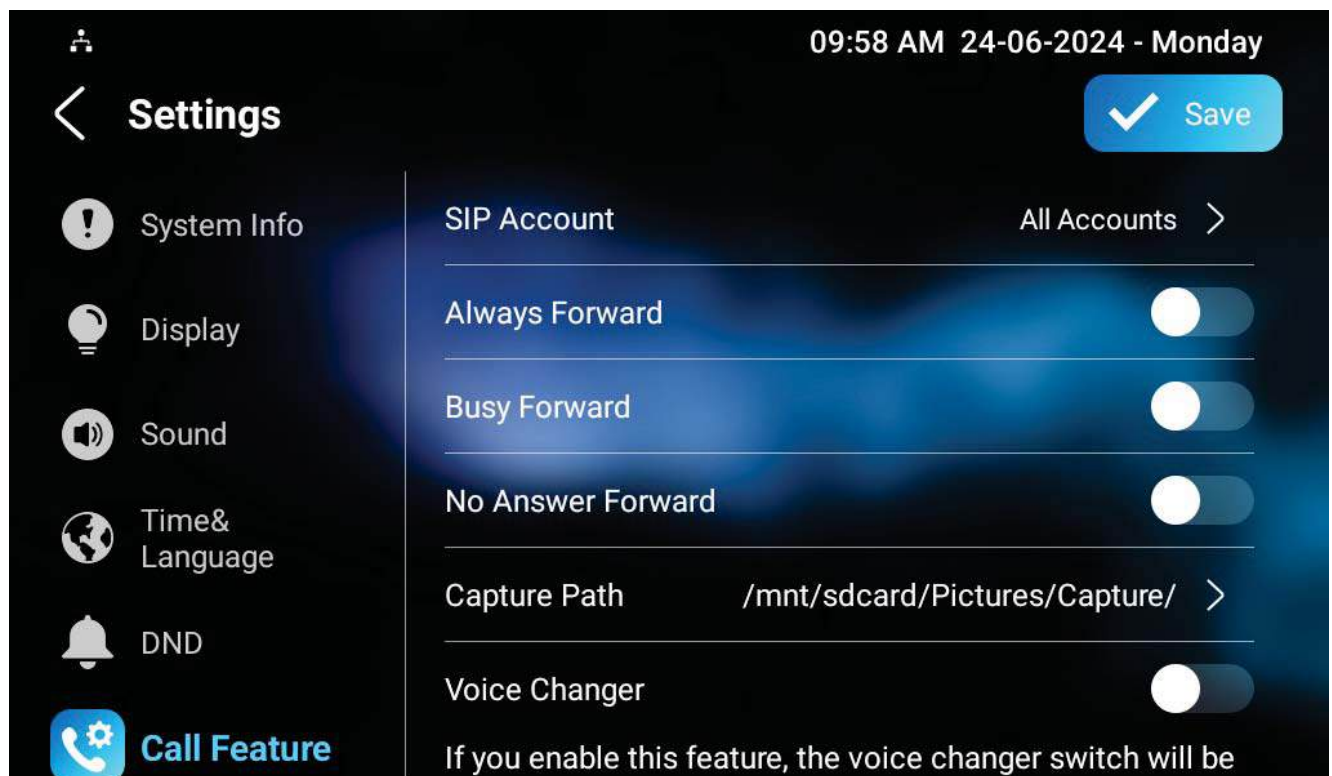
The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult Akuvox tech team for more information.

Call Forwarding Setting

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.

Call Forwarding Setting on the Device

To set it up, go to the device **Settings > Call Feature** screen.

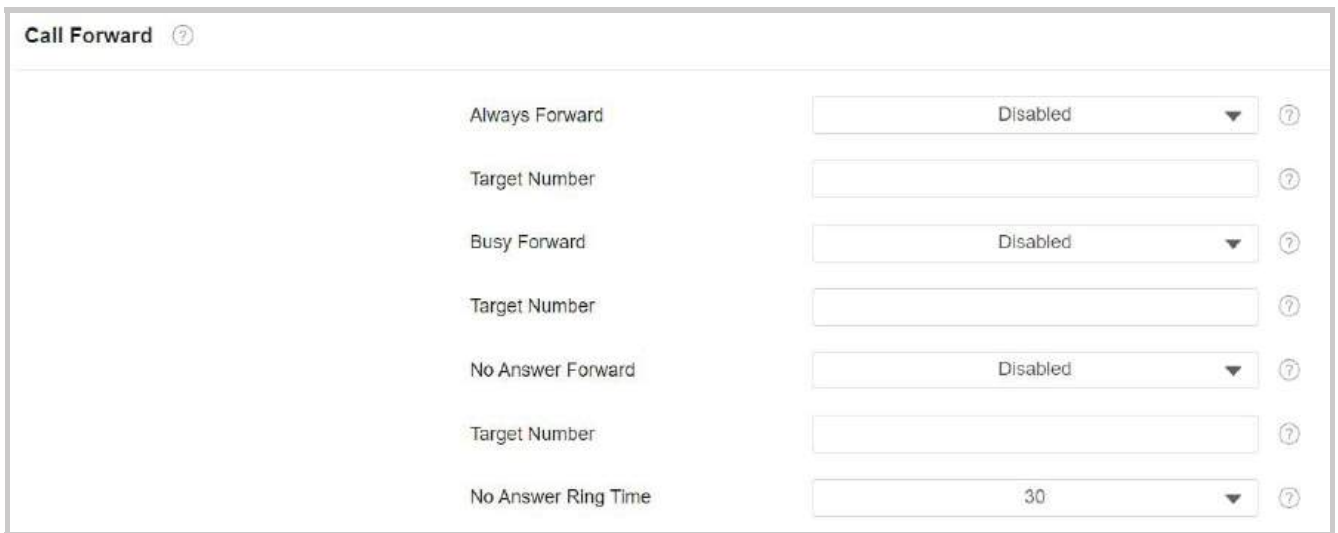


- **SIP Account:** The account to implement the call forwarding feature.
- **Always Forward:** All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward:** Incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward:** Incoming calls will be forwarded to a specific number if the call is not picked up within no answer ring time.

- **Capture Path:** The storage location for all the captured pictures.
- **Target Number:** Specify the forward number when Always Forward, Busy Forward, or No Answer Forward is enabled.
- **No Answer Ring Time(Sec):** The time ranges from 0-120 seconds. This option appears when No Answer Forward is enabled.

Call Forwarding Setting on the Web Interface

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



The screenshot shows the 'Call Forward' web interface. It has a title bar 'Call Forward' with a help icon. Below it, there are three sections for 'Always Forward', 'Busy Forward', and 'No Answer Forward'. Each section has a dropdown menu for the status (currently 'Disabled'), a text input field for the 'Target Number', and a dropdown menu for 'No Answer Ring Time' (currently '30'). Each dropdown and text field has a help icon to its right.

- **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 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:** The time ranges from 0-120 seconds. This option appears when No Answer Forward is enabled.

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 ?

Dial Number

Auto ▼

Dial

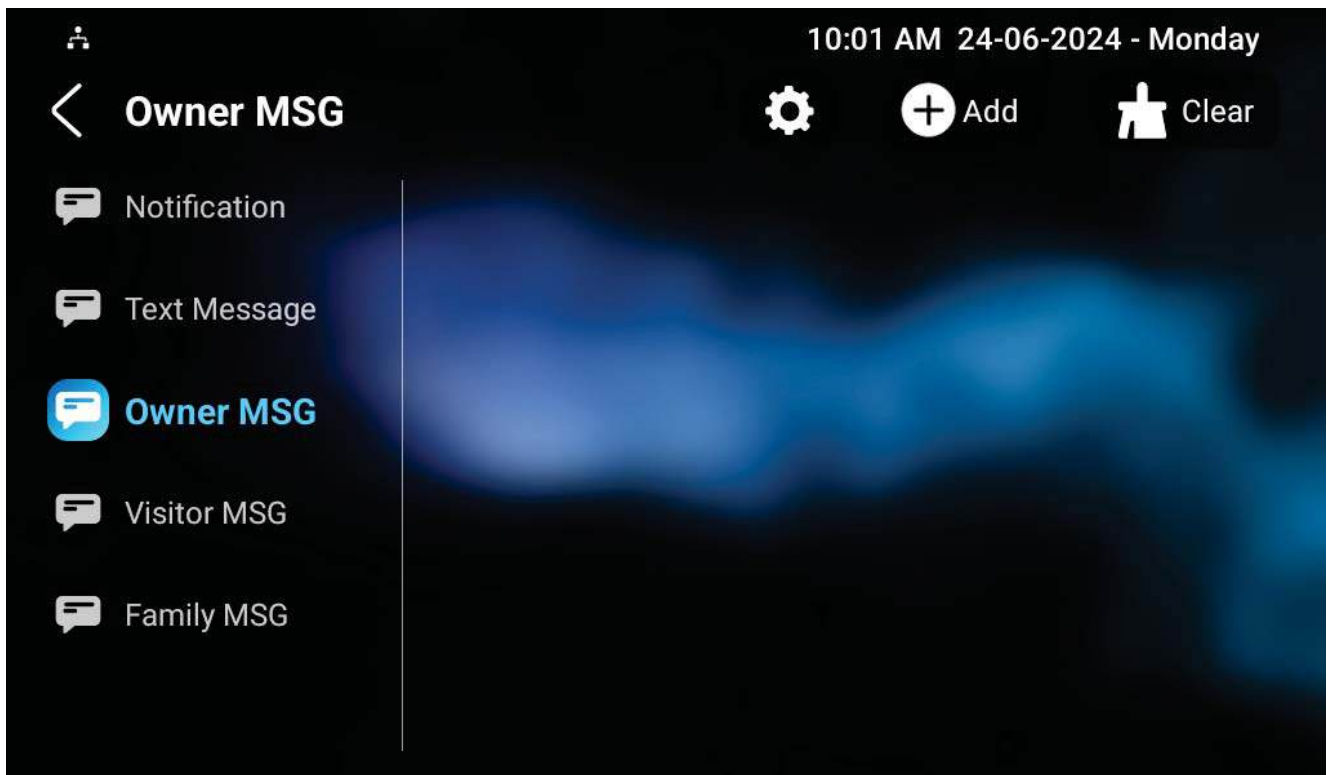
Hang Up ?

Intercom Message Setting

Manage Messages

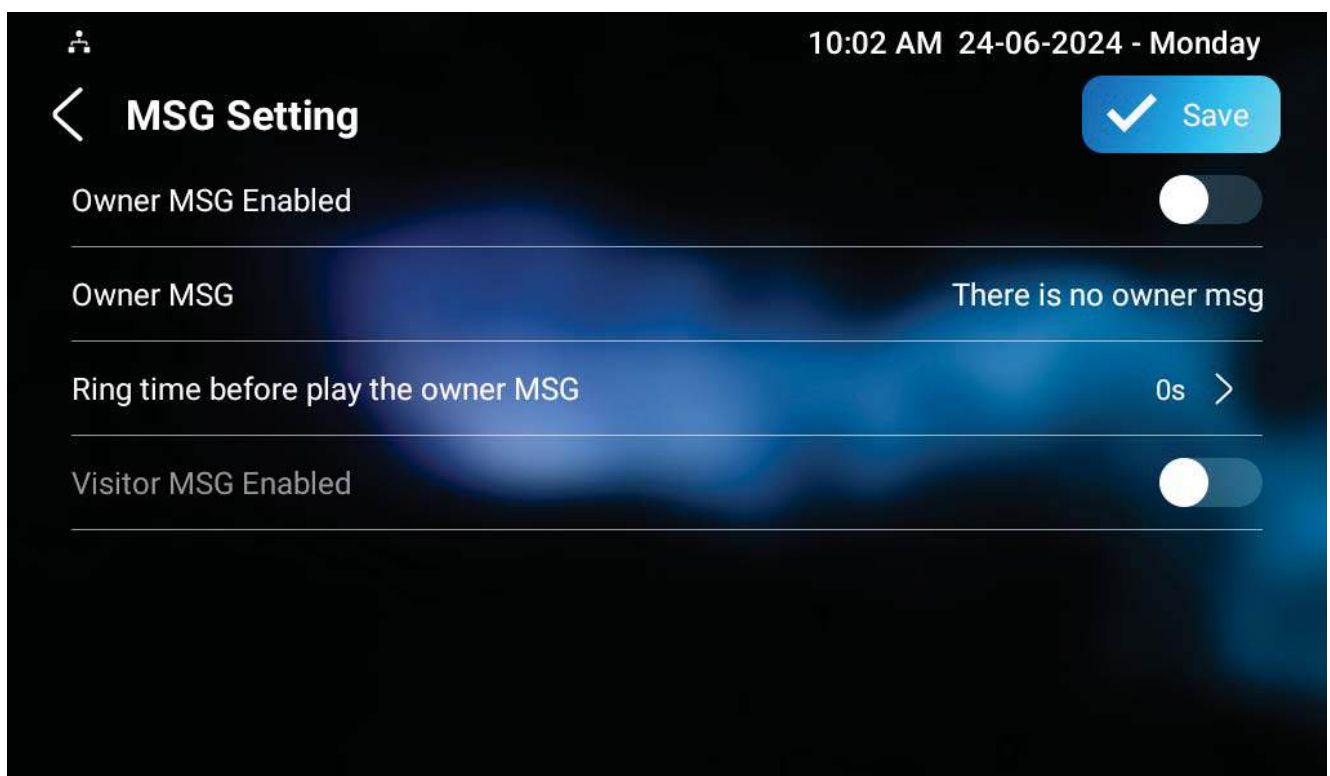
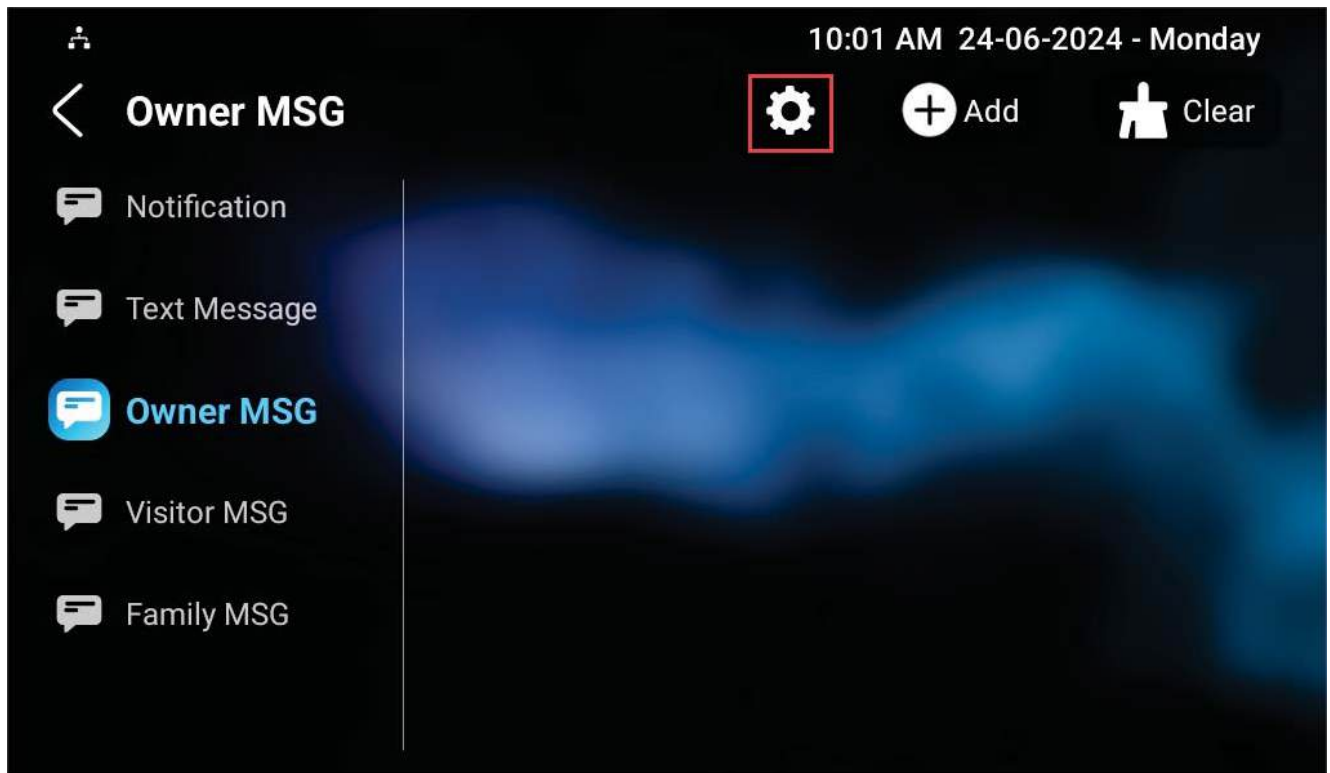
You can check, create and clear messages as needed on the device **Messages** screen.

Tap **+Add** to create a message and tap **Clear** to delete messages.



- **Notification:** The message from the property manager. This feature is only available when using SDMC or Akuvox SmartPlus.
- **Text Message:** To send, receive, or manage the text message here.
- **Owner MSG:** When nobody answers the incoming call within the pre-configured ring time, the visitor will hear the owner's audio message.
- **Visitor MSG:** When nobody answers the incoming call within the pre-set ring time, it will save the visitor record.
- **Family MSG:** Audio messages recorded for family members.

To configure ring time, press the **Settings** icon on the screen.



Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The indoor monitor supports eight types of codecs 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 set it up, go to the web **Account > Advanced** interface.

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

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz
iLBC_13_3	8,16 kbit/s	13.3kHz
iLBC_15_2	8,16 kbit/s	15.2kHz
OPUS	154.4 kbit/s	48kHz
L16	128 kbit/s	variable

Video Codec Configuration

The device supports VP8, H263, H264, and H265 codecs.

To set it up, go to the web **Account > Advanced > Video Codecs** interface. Choose an available video codec and set up the codec parameters.

Video Codecs

2 items Disabled Codecs

☐ H265
☐ VP8

2 items Enabled Codecs

☐ H264
☐ H263

Video Codec

Name	H263
Resolution	CIF
Bitrate	320
Payload	34
Name	H264
Resolution	CIF
Bitrate	320
Payload	104
Name	VP8
Resolution	CIF
Bitrate	320
Payload	96

- **Resolution:** The code resolution for the video quality has five options: QCIF, CIF, VGA, 4CIF, and 720P. H263 only has QCIF, CIF, and 4CIF. Select the resolution according to the network environment.
- **Bitrate:** Select the video stream bitrate. It varies by the resolution.
- **Payload:** The payload ranges from 90-119 for the audio/video configuration file.

Access Control Configuration

Relay Switch Setting

Local Relay Setting

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

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

Relay Setting

Local Relay	
Hold Delay	3
Relay Type	Open Door
Relay Name	Local Relay1
Remote Control	Disabled
DTMF	

- **Hold Delay:** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **Relay Type:**
 - **Chime Bell:** When there is a call and the relay is triggered, the chime bell will ring.
 - **Open Door:** When the unlock icon is pressed and the relay is triggered, the door will be opened.
 - **Other Switches(Reset By Event):** The relay will reset after the triggered event is dealt with.
- **Relay Name:** Assign a distinct name for identification purposes.
- **Remote Control:** Enable it to trigger local relay by DTMF.

- **DTMF**: The DTMF code to trigger the local relay.

Remote Relay Switch Setting

You can use the unlock tab during the call to open the door, and configure this feature on web **Device > Relay > Relay Setting > Remote Relay** interface. You are required to set up the same DTMF code in the door phone and indoor monitor.

Local Relay	
Hold Delay	3
Relay Type	Open Door
Relay Name	Local Relay1
Remote Control	Disabled
DTMF	

Remote Relay	
DTMF1 Code	0
DTMF2 Code	1
DTMF3 Code	2

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

Web Relay Setting

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



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

Web Relay ⓘ

IP Address

 ⓘ

Username

 ⓘ

Password

 ⓘ

Web Relay Action Setting ⓘ

- **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 Unlock Configuration

Door 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 Setting

Local Relay1

Hold Delay (Sec)

3

Relay Type

Open Door

Relay Name

Local Relay1

Remote Control

Disabled

DTMF

Remote Relay

DTMF1 Code

0

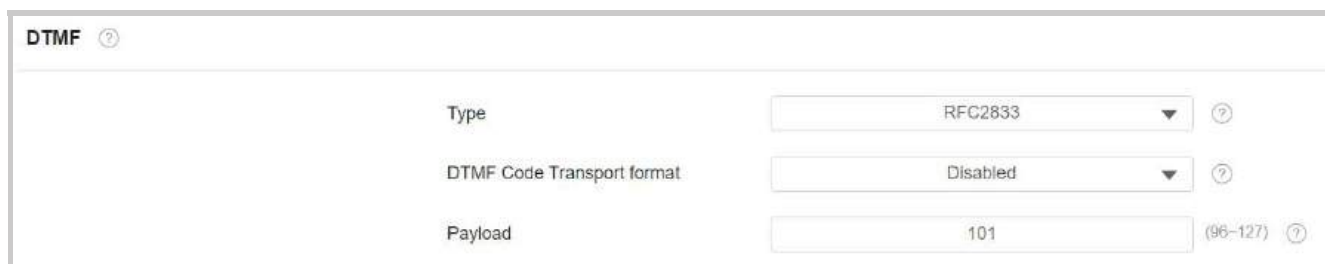
DTMF2 Code

1

DTMF3 Code

2

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



DTMF	
Type	RFC2833
DTMF Code Transport format	Disabled
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.
- **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.

Door 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.

To set it up, go to the web **Device > Relay > Open Relay via HTTP** interface.

Open Relay Via HTTP

Switch

☒

?

Username

?

Password

?

Remote Open Relay Via HTTP AllowList

☒

?

1st IP

2st IP

3st IP

4st IP

5st IP

- **Username:** Set a username for authentication in HTTP command URLs.
- **Password:** Set a password for authentication in HTTP command URLs.
- **Remote Open Relay Via HTTP AllowList:** Enable it and type in the IP address of the server that you allow to send the HTTP command to the indoor monitor and trigger the local relay.

You can also set up HTTP commands to remotely control relays connected to door phones, go to the web **Device > Relay > Remote Relay By HTTP** interface.

Remote Relay By HTTP

	Index	IP/SIP	URL	UserName	Password	DoorNum
☐	1					1 x 2 x 3 x 4 x
☐	2					1 x 2 x 3 x 4 x
☐	3					1 x 2 x 3 x 4 x
☐	4					1 x 2 x 3 x 4 x
☐	5					1 x 2 x 3 x 4 x
☐	6					1 x 2 x 3 x 4 x
☐	7					1 x 2 x 3 x 4 x
☐	8					1 x 2 x 3 x 4 x
☐	9					1 x 2 x 3 x 4 x
☐	10					1 x 2 x 3 x 4 x

Delete
Delete All

- **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 is configured on the door phone's web interface.
- **Password:** Enter the password the same as that is configured on the door phone's web interface.

Tip

Here is an HTTP command URL example for relay triggering.

Door phone's IP
http://192.168.35.127/fcgi/do?action=OpenDoor&
Preset credentials for authentication
UserName=admin&Password=1234568
ID of Relay to be triggered
DoorNum=1

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 up to four 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 ?

Monitor Display

Multiple Window ?

- **Monitor Display:**
 - **Multiple Window:** Display four video monitoring channels on the screen.
 - **Single Window:** Display only one video monitoring channel.

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

Door phone ?

+ Add
Import
Export ▼

	Index	Device Number	Device Name	RTSP Address	Username	Display In Call	Edit
No Data							

Delete
Delete All

Prev
1/1
Next

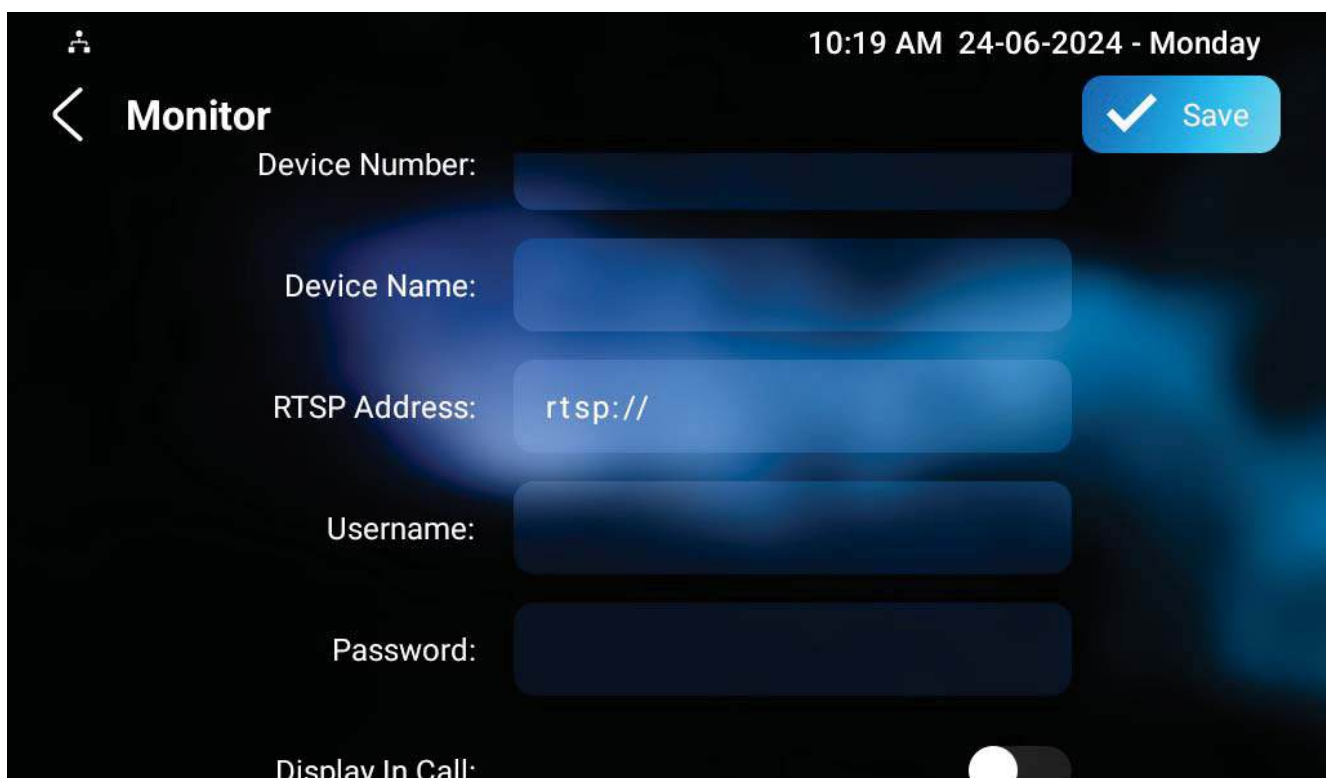
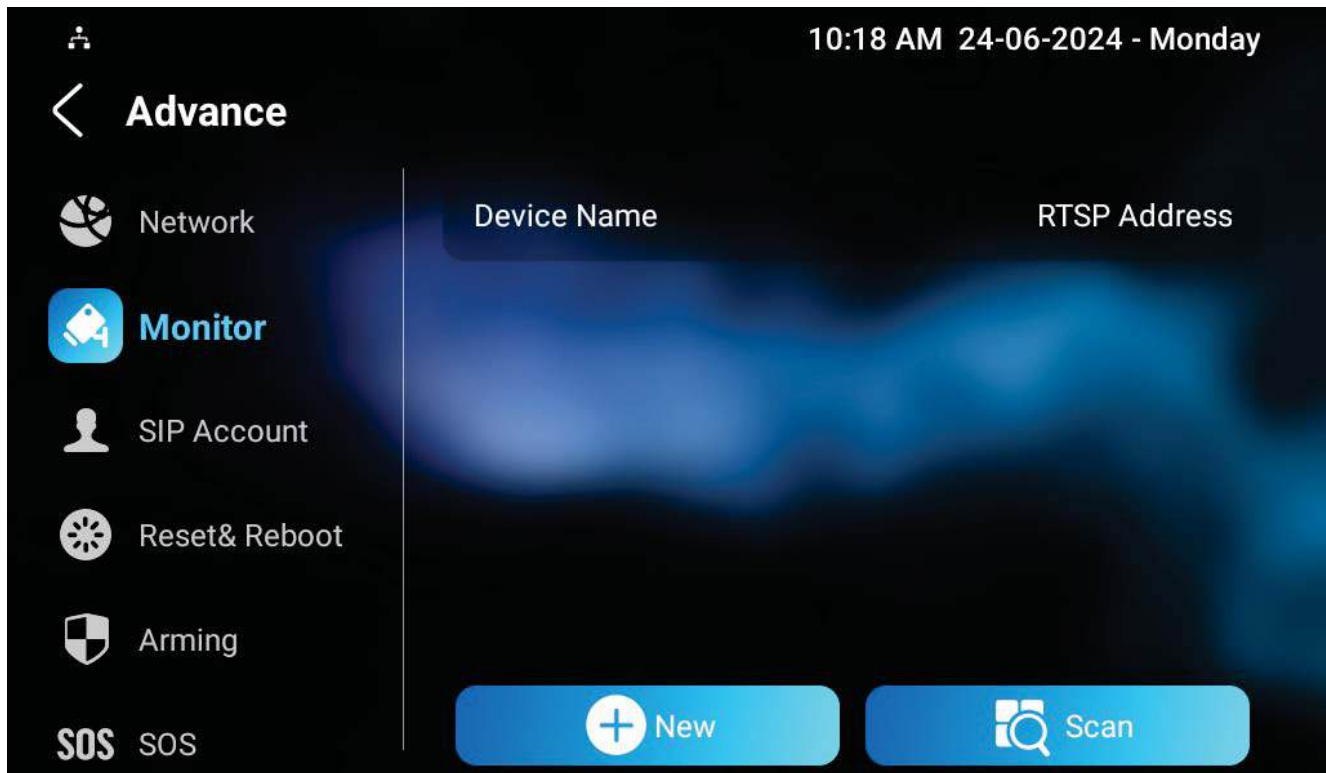
1
Go

- **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

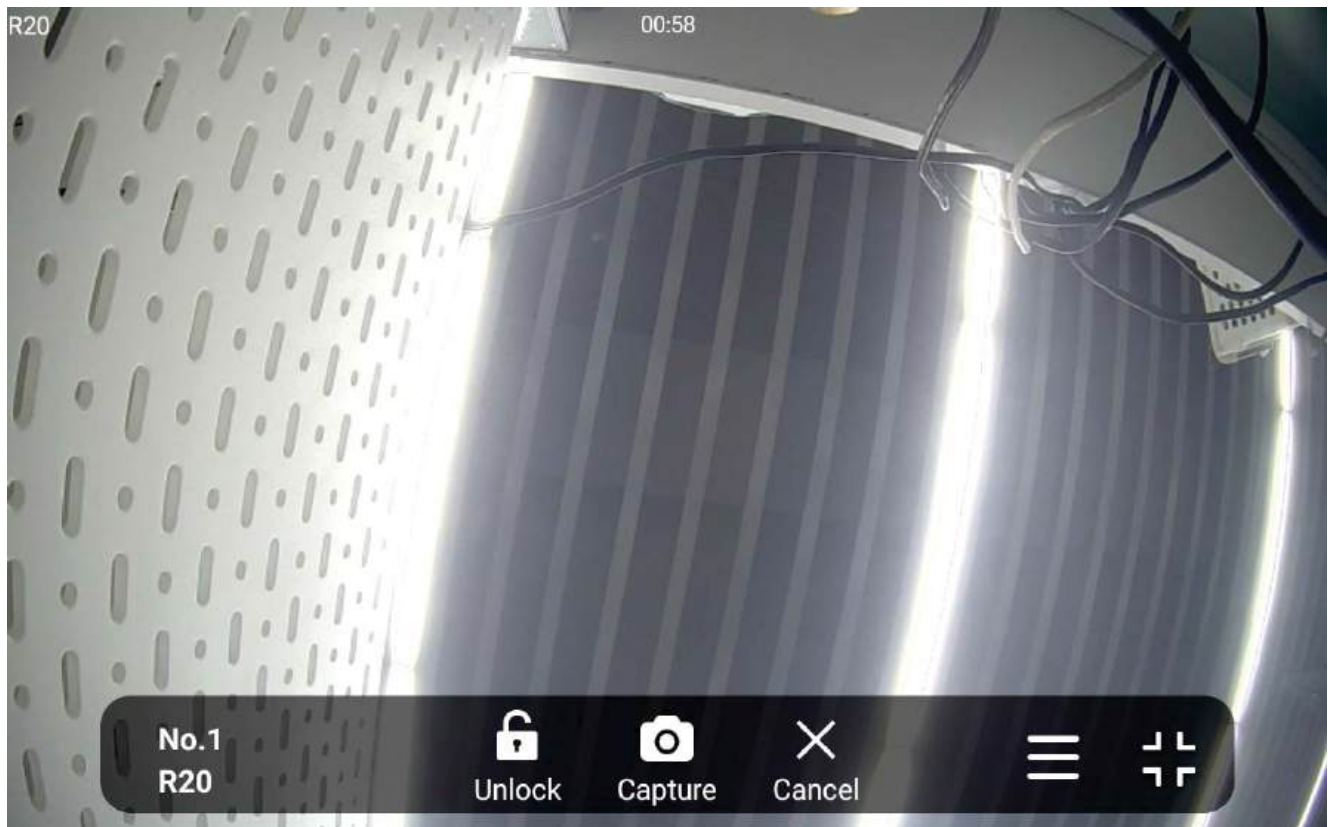
You can import and export the monitoring device settings via a template in .xml format.

You can also set it up on the device **Settings > Advance > Monitor** screen. Tap **+New** to add the monitor device.



Video Image Capturing

The device lets users take a screenshot during a video call or while using the monitor if they notice anything unusual. To take a screenshot, simply tap the Capture button.



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's room for safety.

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

RTSP Setting ?

RTSP Audio Enable	Disabled ?
Authorization Type	Digest ?
Username	admin ?
Password	***** ?

- **RTSP Audio Enable:** Decide whether the device can be audio monitored by other devices.
- **Authorization Type:** It is Digest by default.
- **Username:** Set the username for the authentication.
- **Password:** Set the password for the authentication.

Alarm and Arming Configuration

The Arming function is designed to enhance home security by offering three modes with custom zone settings for connected sensors. When armed, the device will sound a siren and notify specific people if a sensor detects something unusual.

Configure Alarm and Arming on the Device

Set up Arming and Disarm Codes

To configure the arming and disarm codes, go to the **Arming > Arming/Disarm Code** screen. Change the current password and save it. The default code is 0000.

13:53 2023-09-19 - Tuesday

< Arming/Disarm Code

✓ Save

Please input current arming/disarm code:

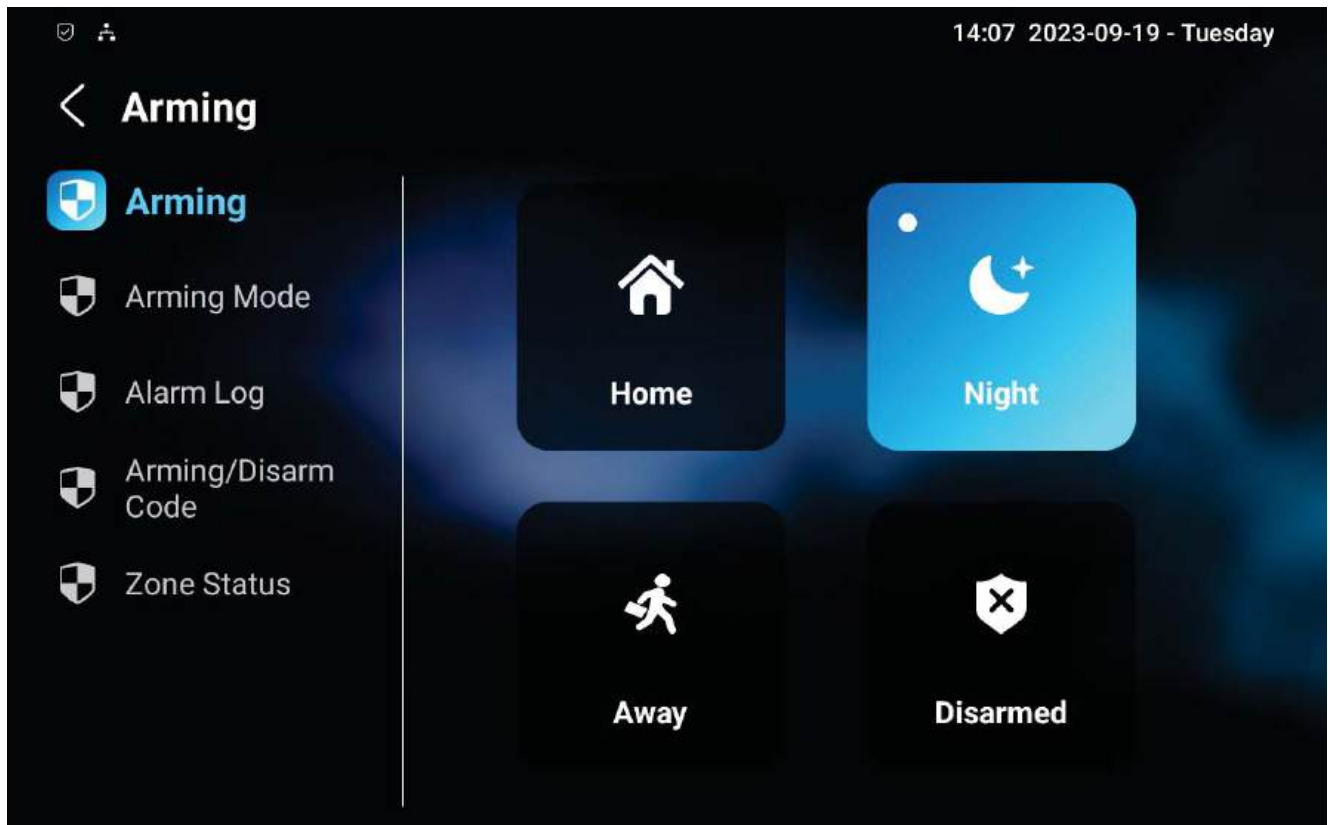
Please input new arming/disarm code:

Please confirm new arming/disarm code:

1	2	3
4	5	6
7	8	9
	0	

Select an Arming Mode

To select an arming mode, go to the **Arming** screen. Tap the desired mode to enable it.



Check Zone Status

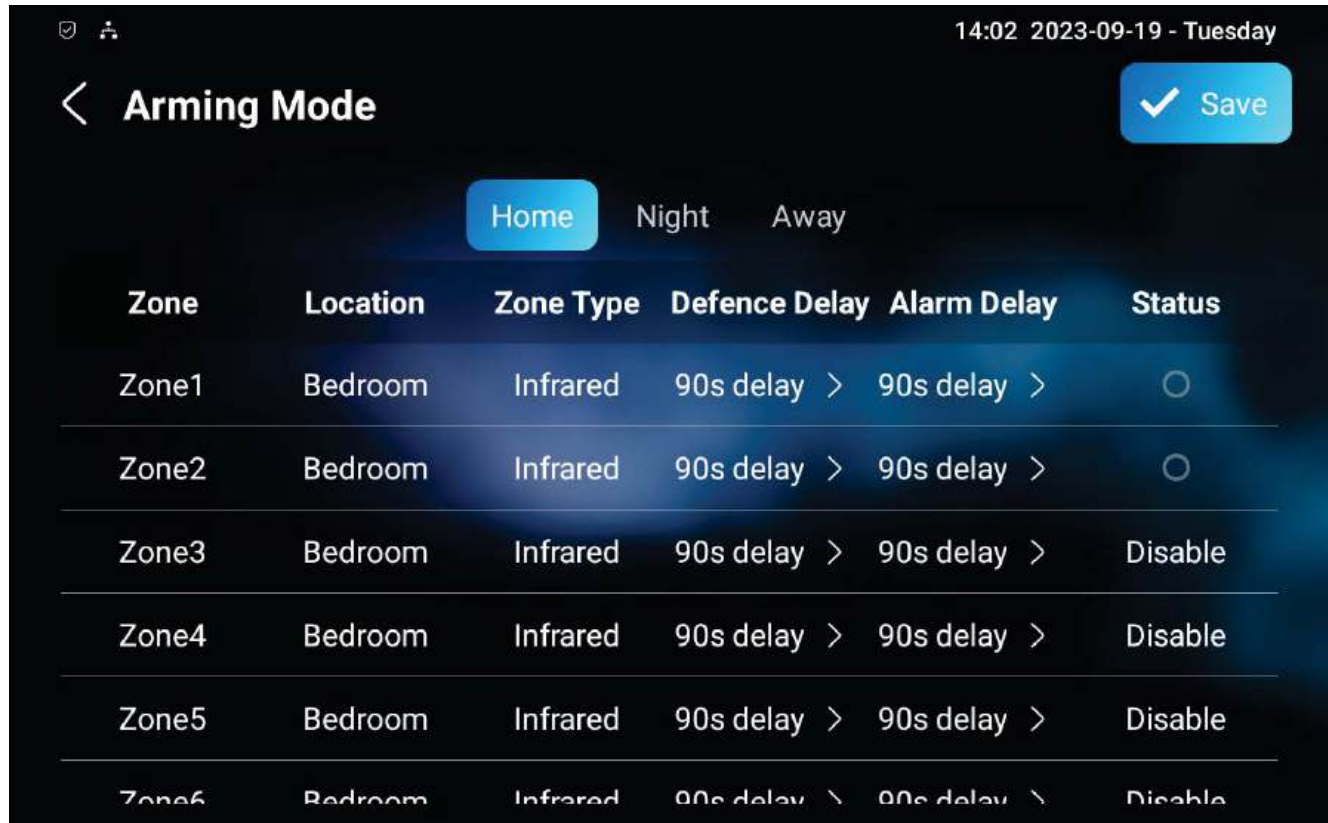
Check the zone status on the Arming > Zone Status screen.

The screenshot shows the 'Zone Status' screen of the Akuvox app. At the top right, the time is 13:53 on 2023-09-19, Tuesday. The sidebar menu on the left includes 'Zone Status' (highlighted with a blue icon). The main content area displays a table with the following data:

Zone	Location	Zone Type	Trigger	Status
Zone1	Bedroom	Infrared	NC	Disable
Zone2	Bedroom	Infrared	NC	Disable
Zone3	Bedroom	Infrared	NC	Disable
Zone4	Bedroom	Infrared	NC	Disable
Zone5	Bedroom	Infrared	NC	Disable
Zone6	Bedroom	Infrared	NC	Disable
Zone7	Bedroom	Infrared	NC	Disable
Zone8	Bedroom	Infrared	NC	Disable

Set up Alarm Sensors

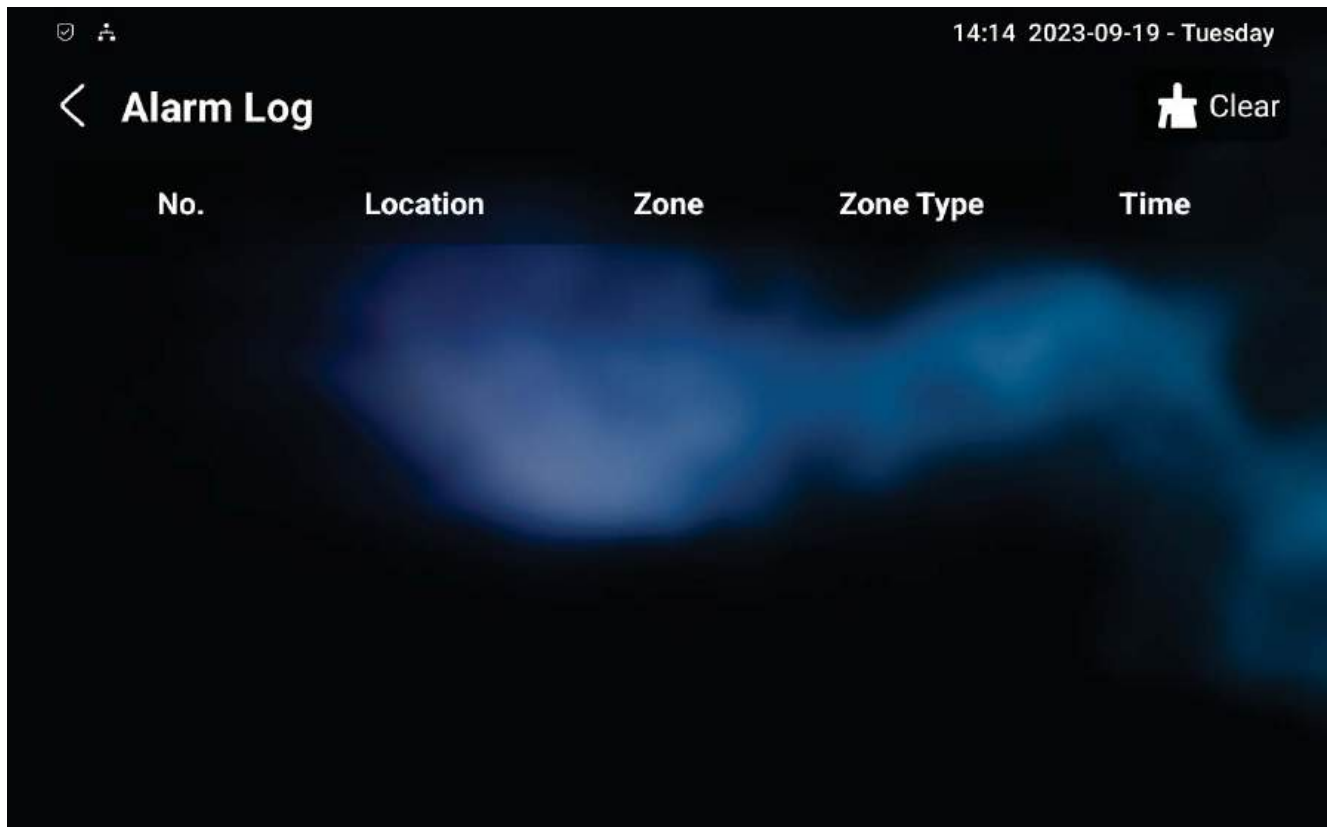
To configure the alarm sensor in different modes, go to the **Arming > Arming Mode** screen.



- **Location:** Display which location the detection device is in, including Bedroom, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type:** Display the alarm sensor type, including Infrared, Drmagnet, Smoke, Gas, and Urgency.
- **Defence Delay:** It means when users change the arming mode from other modes, there will be 90 seconds delay time to get activated.
- **Alarm Delay:** It means when the sensor is triggered, there will be 90 seconds delay time to announce the notification.
- **Status:** Enable or disable Arming Mode on the corresponding zone.

Check Alarm Logs

To check the alarm log, go to the **Arming > Alarm Log** screen.



Configure Alarm and Arming on the Web Interface

Set up Arming and Disarm Codes

To configure the arming and disarm codes, go to the **Arming > Disarm Code** interface. The default code is 0000.

Disarm Code

Current Password

New Password

length must be 0-10

Confirm Password

Disarm Setting

Disarm Interval (Sec)

Never

- **Disarm Interval(Sec):** Set the alarm sound duration after the alarm is triggered.

Select an Arming Mode

To select an arming mode, go to the **Arming > Arming Mode** interface.

Arming Mode ?

Mode
Disarmed ▼

Set up Location-based Alarm Sensors

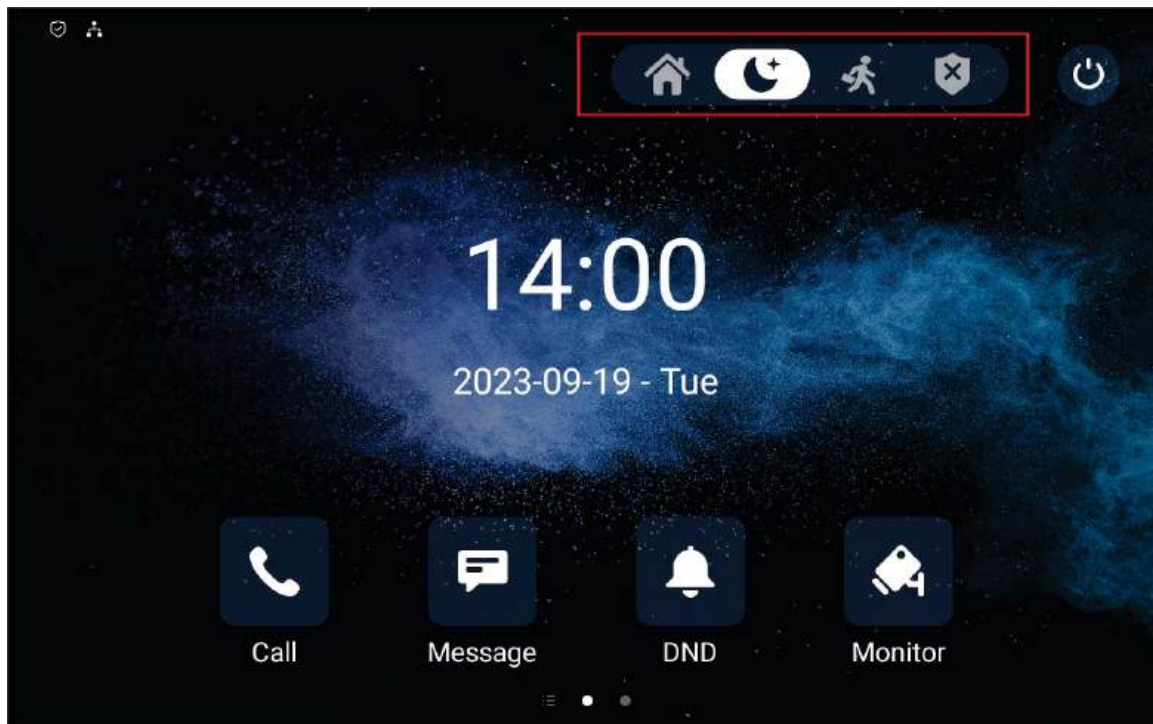
To set up a location-based alarm sensor, go to the web **Arming > Zone Setting > Zone Setting** interface.

Zone Setting ?

Zone	Location	Zone Type	Trigger Mode	Status
Zone1	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone2	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone3	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone4	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone5	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone6	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone7	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼
Zone8	Bedroom ▼	Infrared ▼	NC ▼	Disabled ▼

- **Location:** Indicate where the alarm sensor is installed. There are ten location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type:** The alarm sensor types. There are five sensor types: Infrared, Drmagnet, Smoke, Gas, and Urgency.
- **Trigger Mode:** Set sensor trigger mode between NC and NO.
- **Status:** Set the alarm sensor status among three options: Enabled, Disabled, and 24H.
 - **Enabled:** The alarm needs to be set again after disarming.
 - **Disabled:** Disarm the alarm.
 - **24H:** The alarm sensor will stay enabled for 24 hours without setting up the alarm manually again after the alarm is disarmed.

If any of the zones is enabled or set to **24H**, the alarm-related icons will be displayed on the home screen for quick access.



Set up Alarm Sensors in Different Arming Modes

To configure the alarm in different modes, go to the **Arming > Arming Mode** interface.

Home ?					
Zone	Location	Zone Type	Defence Delay	Alarm Delay	Status
Zone1	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone2	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone3	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone4	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone5	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone6	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone7	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐
Zone8	Bedroom	Infrared	90Sec ▼	90Sec ▼	☐

- **Location:** Display which location the detection device is in, including Bedroom, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type:** Display the alarm sensor type, including Infrared, Dmagnet, Smoke, Gas, and Urgency.
- **Defence Delay:** It means when users change the arming mode from other modes, there will be 90 seconds delay time to get activated.
- **Alarm Delay:** It means when the sensor is triggered, there will be 90 seconds delay time to announce the notification.

- **Status:** Enable or disable Arming Mode on the corresponding zone.

Configure Alarm Text

Once the alarm sensor is configured, you can access the device's web interface to personalize the alert content displayed on the screen when an alarm is triggered.

To set it up, navigate to the web **Arming > Zone Setting > Customized Alarm** interface.

Customized Alarm ⓘ

Customized Alarm Enabled
☐ ⓘ

Zone	Alarm Content
Zone1	Alarm was Triggered
Zone2	Alarm was Triggered
Zone3	Alarm was Triggered
Zone4	Alarm was Triggered
Zone5	Alarm was Triggered
Zone6	Alarm was Triggered
Zone7	Alarm was Triggered
Zone8	Alarm was Triggered

- **Alarm Content:** The alarm text will display on the device screen when an arming is triggered.

Configure Alarm Ringtone

You can upload a customized alarm ringtone by choosing the local audio file on the web **Device > Audio > Alarm Ringtone Upload** interface.

Alarm Ringtone Upload ⓘ

Alarm Ringtone Upload
 ⓘ

Alarm Ringtone
 ⓘ

Note

The file format of customized ringtone should be in WAV or MP3 format. No limitation to the file size.

Alarm Action Configuration

When the alarm sensor is triggered, it can start different actions, such as HTTP commands, SIP messages, calls, and local relay activation, if they are set up.

To select and set up actions, go to the web **Arming > Alarm Action** interface.

Configure Alarm Action via HTTP Command

To set up the HTTP command action, you can select **Enabled** in the **Send HTTP** field to enable the actions for the alarm sensor installed in different locations. Then enter the HTTP command provided by the device manufacturer on which the action is to be carried.

HTTP Command Setting ⓘ		
Zone	Http Command	Send HTTP Enabled
Zone1	http://	Disabled ▼
Zone2	http://	Disabled ▼
Zone3	http://	Disabled ▼
Zone4	http://	Disabled ▼
Zone5	http://	Disabled ▼
Zone6	http://	Disabled ▼
Zone7	http://	Disabled ▼
Zone8	http://	Disabled ▼

- **Send HTTP Enabled:** Enable it if you want the action to be implemented on a designated third-party device.
- **HTTP Command:** Enter the HTTP command provided by the third-party device manufacturer.

Configure Alarm Action via SIP Message

The device can send messages to a designated device when the alarm is triggered. To set this up, enter a SIP number or IP address along with the message content.

Receiver Of SIP Setting ?

SIP Account

Zone	SIP Message	Send Sip Message
Zone1		Disabled ▼
Zone2		Disabled ▼
Zone3		Disabled ▼
Zone4		Disabled ▼
Zone5		Disabled ▼
Zone6		Disabled ▼
Zone7		Disabled ▼
Zone8		Disabled ▼

- **SIP Account:** The SIP number to receive the message.
- **SIP Message:** The message sent to the designated SIP number when the alarm is triggered.

Configure Alarm Action via SIP Call

To enable the device to make a call when the alarm is triggered, enter the SIP or IP number of the called party. Additionally, you can allow the indoor monitor to sound a siren simultaneously.

Call Setting ?

Call Number

Zone	Make Call Enable	Alarm Siren
Zone1	Disabled ▼	Enabled ▼
Zone2	Disabled ▼	Enabled ▼
Zone3	Disabled ▼	Enabled ▼
Zone4	Disabled ▼	Enabled ▼
Zone5	Disabled ▼	Enabled ▼
Zone6	Disabled ▼	Enabled ▼
Zone7	Disabled ▼	Enabled ▼
Zone8	Disabled ▼	Enabled ▼

- **Call Number:** The SIP number or IP number to receive the calls when the alarm is triggered.
- **Make Call Enable:** Enable it so that a call will be made to the designated SIP or IP number when the alarm is triggered.
- **Alarm Siren:** Enable it to trigger an alarm siren on the indoor monitor when the alarm is triggered.

Configure Alarm-Triggered Local Relay

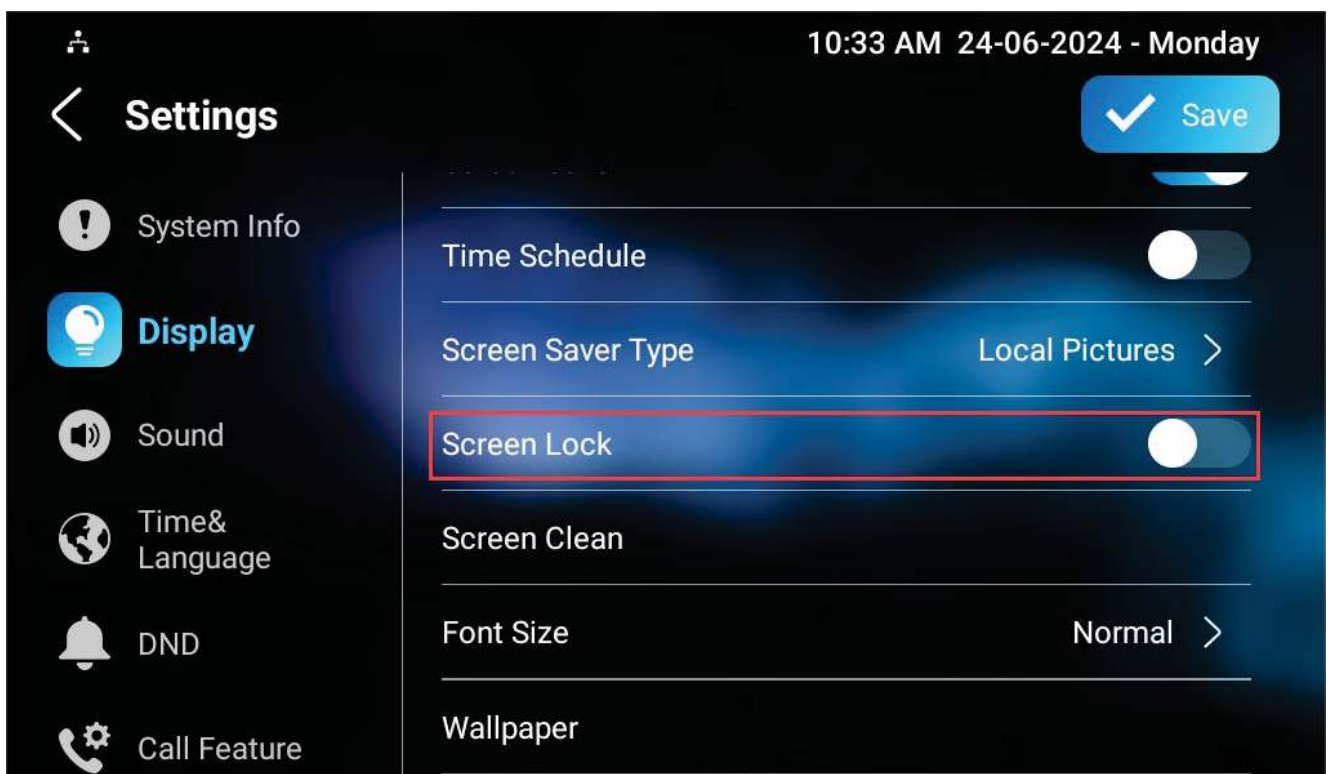
You can select the local relay to be triggered by the alarm.

Local Relay ?	
Zone	Local Relay 1
Zone1	Disabled
Zone2	Disabled
Zone3	Disabled
Zone4	Disabled
Zone5	Disabled
Zone6	Disabled
Zone7	Disabled
Zone8	Disabled

Screen Unlock Setting

To prevent unauthorized access to the device when it is not being used, enable the Screen Lock function. This feature automatically locks the device after a period of inactivity, requiring a password to unlock.

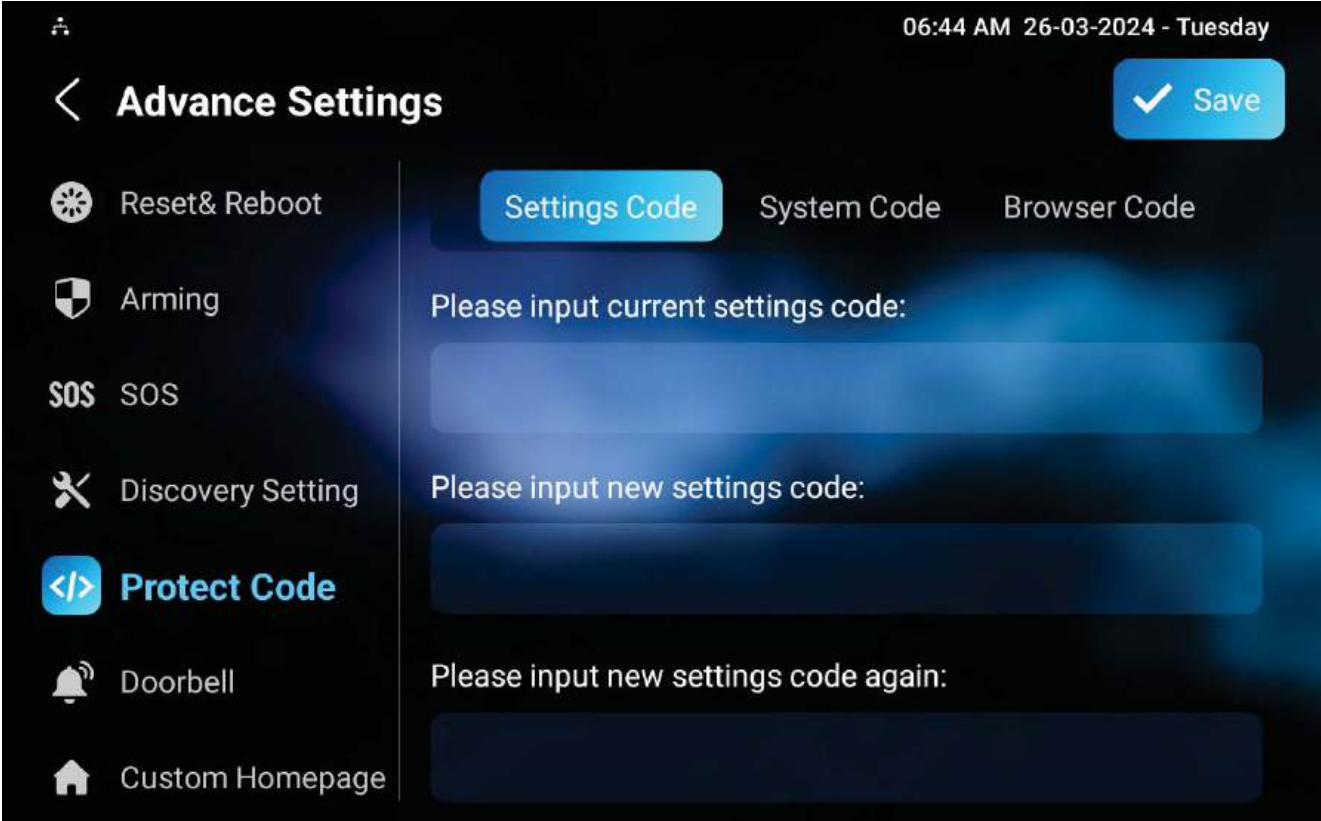
You can enable the screen lock function directly on the device **Settings > Display** screen.



Screen Unlock by PIN Code

To unlock the screen, users need to enter the preset PIN code.

Navigate to **Settings > Advance > Protect Code** screen and select **Settings Code** to change a new password.



06:44 AM 26-03-2024 - Tuesday

Advance Settings ✓ Save

Reset & Reboot

Arming

SOS SOS

Discovery Setting

Protect Code

Doorbell

Custom Homepage

Settings Code System Code Browser Code

Please input current settings code:

Please input new settings code:

Please input new settings code again:

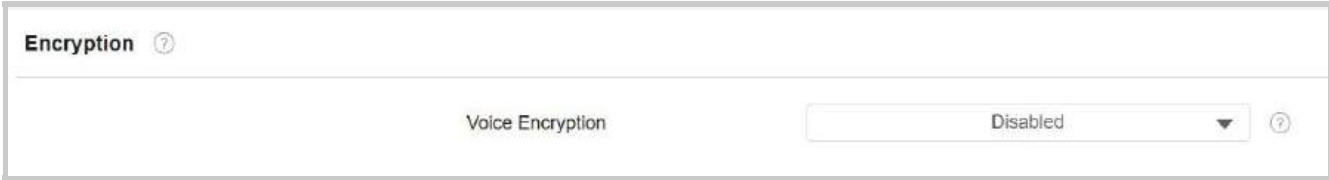
Note

The default password is 123456.

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

Disabled ?

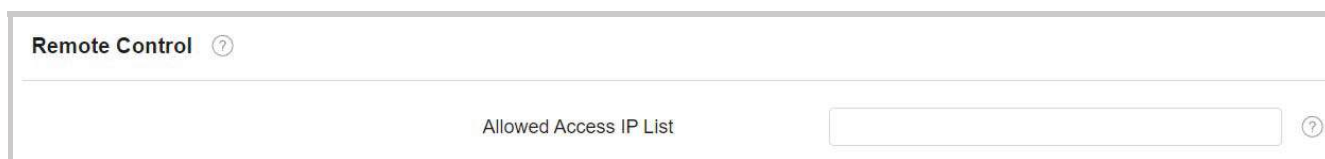
- **Voice Encryption:**

- **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.

Remote Control

The remote control function allows a specific server to send HTTP commands or requests to the indoor monitor for actions like unlocking a local relay.

To set it up, navigate to the web **Device > Relay > Remote Control** interface.

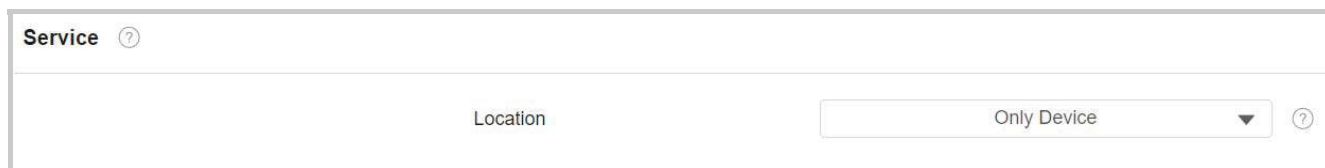


- **Allowed Access IP List:** Set up the server IP address that can be allowed to send the HTTP commands to the indoor monitor.

Location

With users' permission, Location service uses information from cellular, Wi-Fi, Global Positioning System (GPS), and Bluetooth to determine the device's location. Users can turn off this service or change its settings anytime.

To set it up, navigate to the web **Security > Advanced** interface.



- **Disabled:** Not allow any app to find the device location.
- **Only Device:** The device location can be determined using GPS.
- **High Accuracy:** The device location can be determined via WAN, Bluetooth, or cellular networks.

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 Time Out** interface.

Power Output Setting

The indoor monitor can serve as a power supply to the Akuvox door phone with 12V power supply for example E10. You can enable the power output, then connect the door phone to the RJ45 port on the indoor monitor. Also, you can connect E10 to the 12_out port for the power supply.

To enable it, go to **Settings > Basic > Power Output Setting** interface.

High Security Mode

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

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

Important Notes

1. The High Security mode is off by default when you upgrade the device from a version without the mode to one with it. But if you reset the device to its factory settings, the mode is on by default.
2. This mode makes the old version tools incompatible. You need to upgrade them to the following versions or higher to use them.

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

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

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

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

- I 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.

Lift Control

You can summon a lift via the lift control feature.

Configure Lift Control

Before setting the Lift icon, display it on the Home or More screen.

To display the icon, go to the **Device > Display Setting** interface.

Home Page Display ?

Example

Area	Type	Value	Label	Type(max size:100*100)
Area1	Lift		Lift	Not selected any files Select File Delete
Area2	Message			Not selected any files Select File Delete
Area3	DND			
Area4	Monitor			Not selected any files Select File Delete

More Page Display ?

Example

Area	Type	Value	Label	Type(max size:100*100)
Area1	Contacts			Not selected any files Select File Delete
Area2	Settings			Not selected any files Select File Delete
Area3	Arming			Not selected any files Select File Delete

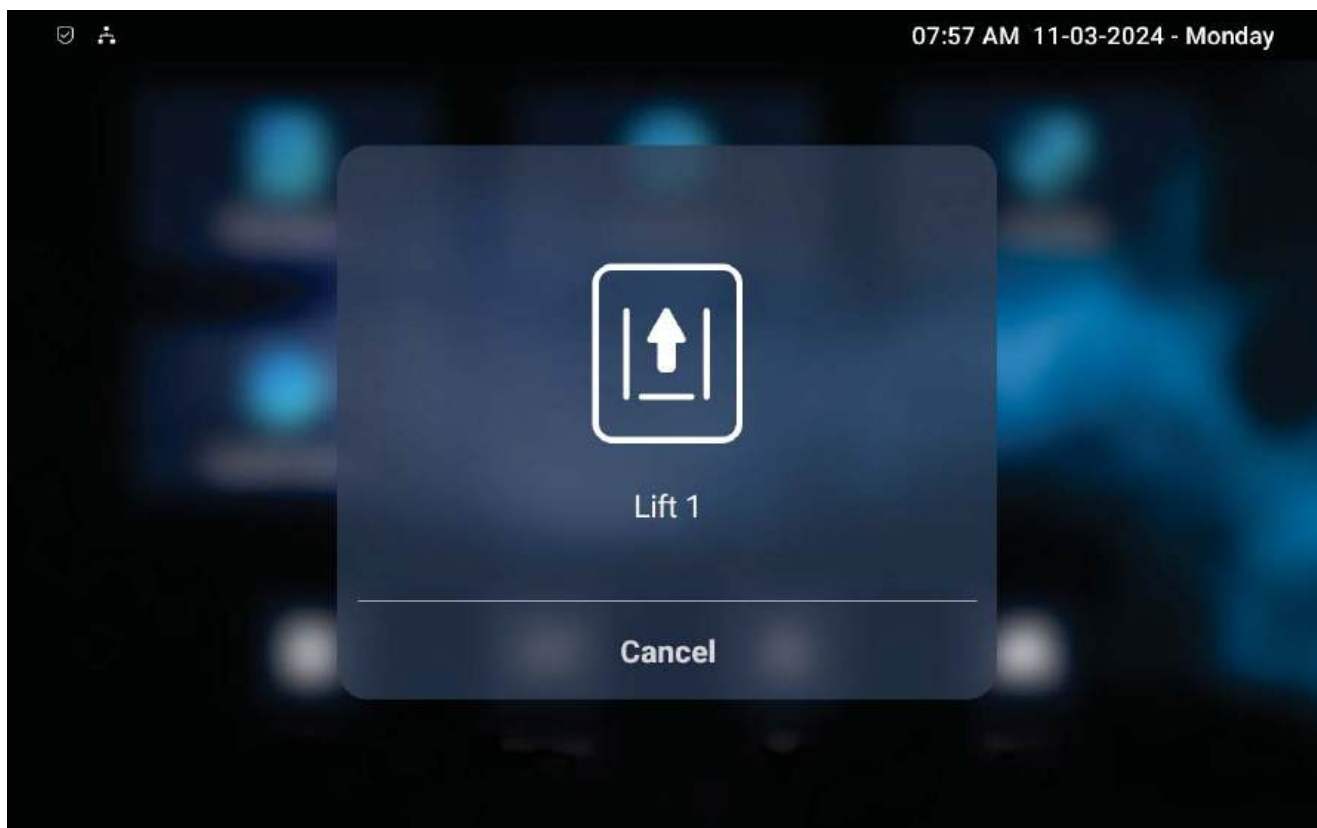
To set the Lift icon, go to the web **Device > Lift > Lift Control** interface.

Lift Control ?

Name	Status	Type	Label	Http Command
Lift1	Disabled	Up		http://
Lift2	Disabled	Up		http://

- **Status:** Enable or disable the lift button.
- **Type:** Decide the button icon.
- **Label:** Name the button.
- **HTTP Command:** Select http:// or https:// for the head of the HTTP command and enter the HTTP command.

Users can tap the icon to summon or send a lift.



Configure Lift Control Prompt

When the lift controller receives the HTTP command, it will give feedback on the current lift status with a prompt.

To set it up, go to the web **Device > Lift > Hints** interface. Click the Edit icon  to modify the desired prompt.

Hints ?					
+ Add Import Export ▼					
☐	Index	HTTP Status Code	Lift	Hints	Edit
☐	1	200	Lift1	Lift is coming to your floor	
☐	2	200	Lift2	Lift has been sent to Ground Floor	
Delete Delete All		Prev 1/1 Next		1 Go	

If many prompts need to be added, you can click the **Export** tab to export a template and import the file after editing. The import and export files should be in XML format.

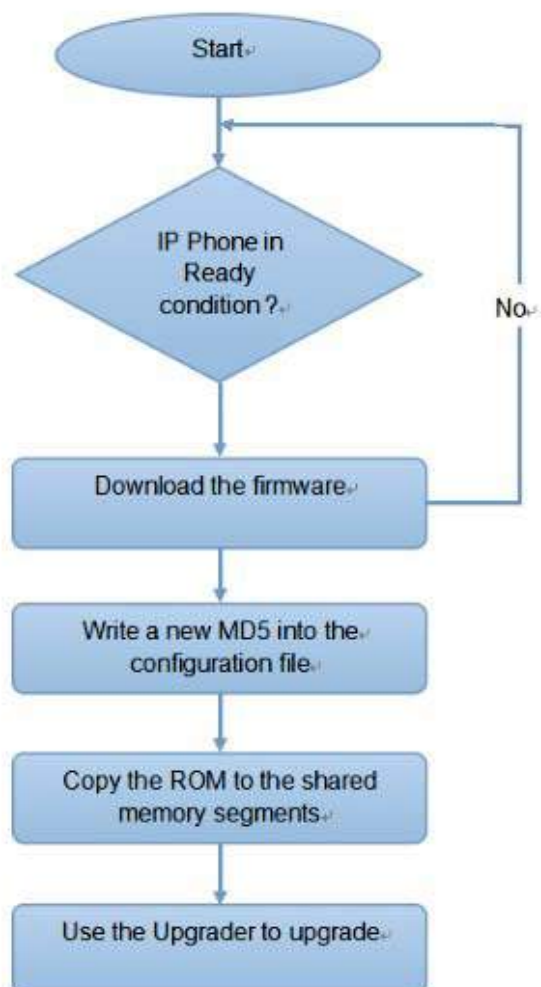
Hints ?					
+ Add Import Export ▼					

Auto-provisioning via Configuration File

Provisioning Principle

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

Please see the flow chart below:



Introduction to the Configuration Files for Auto-Provisioning

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

The difference between the two types of configuration files:

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

Note

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

You may click [here](#) to see the detailed format and steps.

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

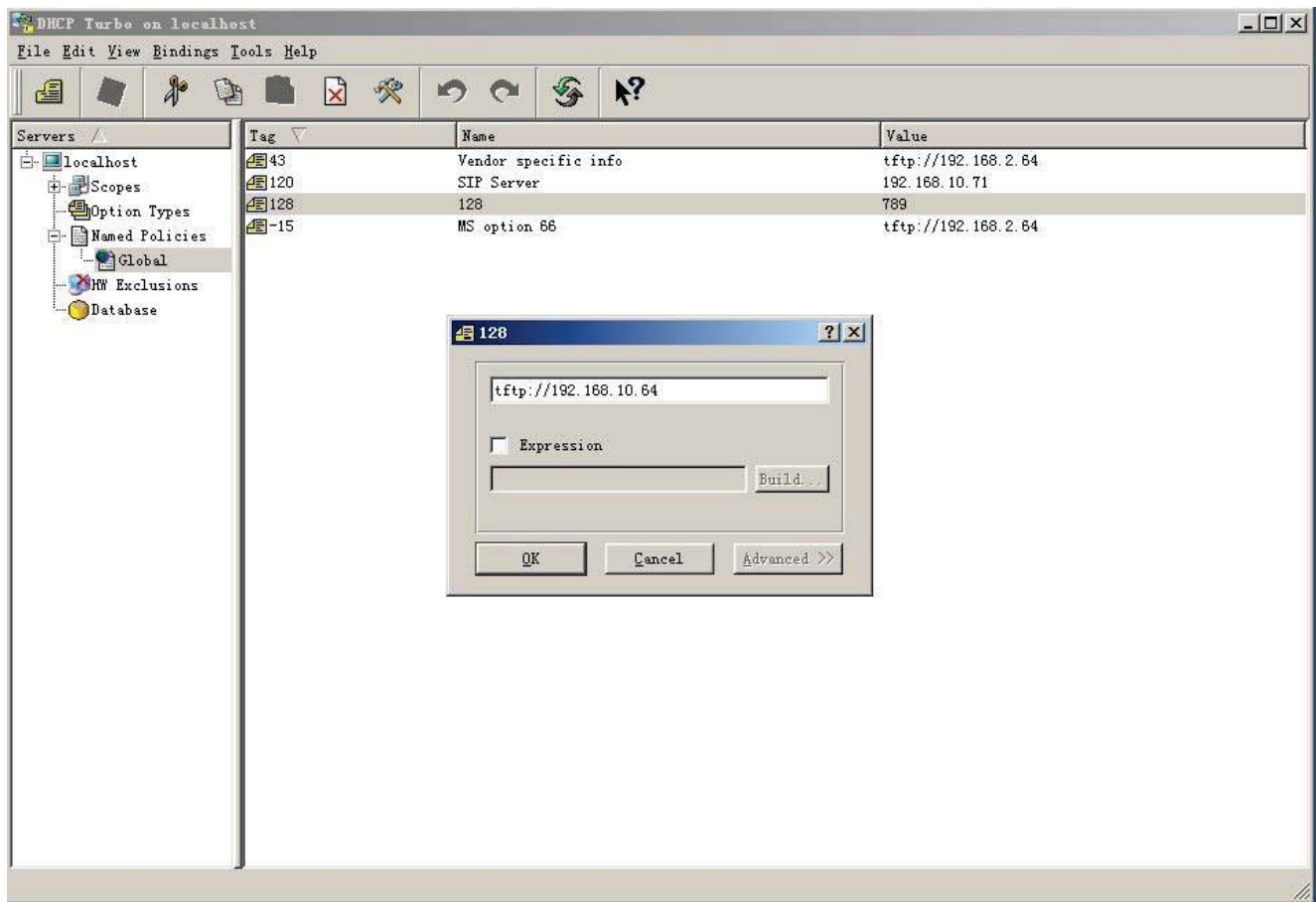
Mode	Power On ?
Schedule	Sunday ?
	22 (0~23Hour)
	0 (0~59Min)
Export Autop Template	Export ?
Clear MD5	Clear ?

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

DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.



Note

- The Custom Option type must be a string. The value is the URL of TFTP server.

To set up DHCP Autop with **Power On** mode, go to the web **Upgrade > Advanced > Automatic Autop** interface.

Automatic Autop

Mode	Power On	?
Schedule	Sunday	?
	22	(0~23Hour)
	0	(0~59Min)
Export Autop Template	Export	?
Clear MD5	Clear	?

To set up the DHCP Option, scroll to the **DHCP Option** section.

DHCP Option ?

Custom Option

(128-254) ?

DHCP Option Enabled

☒ Custom Option
 ☒ Option 43
 ☒ Option 66
 ?

- **Custom Option:** Enter the DHCP code that matches with corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43:** If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the upgrade server URL in it.
- **DHCP Option 66:** If none of the above is set, the device will automatically use DHCP Option 66 to get the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 66 with the upgrade server URL in it.

Static Provisioning Configuration

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

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

Automatic Autop ?

Mode

Power On

?

Schedule

Sunday

?

22

(0-23Hour)

0

(0-59Min)

Export Autop Template

Export

?

Clear MD5

Clear

?

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

Manual Autop

URL		?
Username		?
Password		?
Common AES Key		?
AES Key(MAC)		?

 AutoP Immediately

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

Note

- AES as one type of encryption should be configured only when the config file is encrypted with AES.
- Server Address Format:
 - TFTP: tftp://192.168.0.19/
 - FTP: ftp://192.168.0.19/(allows anonymous login)
ftp://username:password@192.168.0.19/(requires a user name and password)
 - HTTP: http://192.168.0.19/(use the default port 80)
http://192.168.0.19:8080/(use other ports, such as 8080)
 - HTTPS: https://192.168.0.19/(use the default port 443)

Tip

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

PNP Configuration

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

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

PNP Option ?	
PNP Config Enabled	☒ ?

Call Logs

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

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

Call Logs ⓘ

Capture Delay (Sec) ⓘ

Upper Limit ⓘ

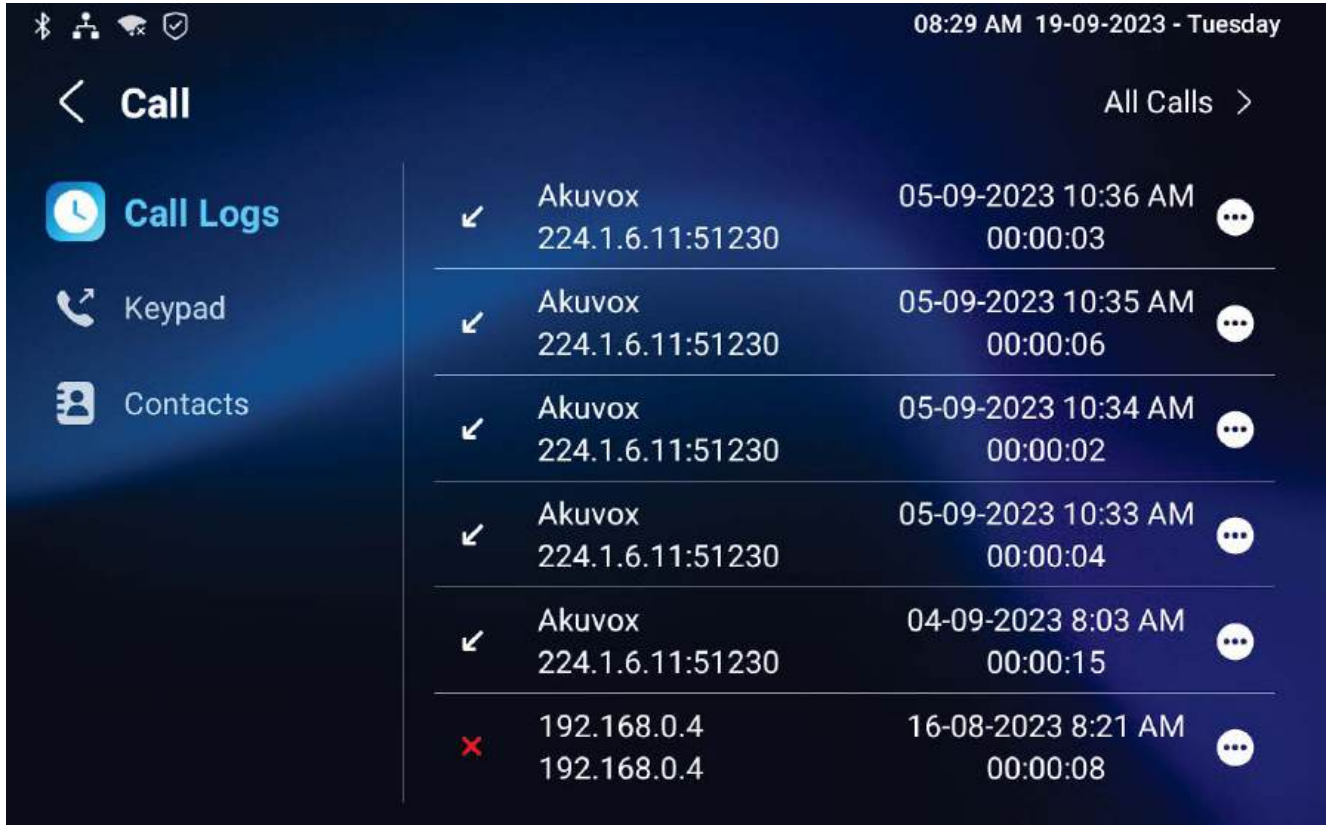
Call History ⓘ

Index	Type	Date	Time	Local Identity	Name	Number
 No Data						

1/1

- **Capture Delay(Sec):** Set the image capturing starting time when the device goes into a video preview.
- **Upper Limit:** The maximum screenshot storage capacity. When the capacity reaches its limit, the previous screenshots will be overwritten.
- **Call History:** There are five types of call history, All, Dialed, Received, Missed, and Forwarded.
- **Local Identity:** Display the device's SIP account or IP number that receives incoming calls.

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



Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

Basic ?			
Firmware Version	316.30.12.113		?
Hardware Version	1.0		?
Upgrade	 Import		?
Factory Default	 Reset		?
Reset Config	 Reset		?
Reboot	 Reboot		?

Note

Firmware files should be .zip format for the 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.

- **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 Specific Port:** Select the specific port from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** When enabled, the PCAP will continue to capture data packets even after the data packets reach 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets reach the maximum capturing capacity of 1MB.

Remote Debug Server

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

To set it up, go to the **Upgrade > Diagnosis > Remote Debug Server** interface.

Remote Debug Server ?	
Enabled	☒ ?
Connect Status	Disconnected ?
IP	47.106.233.244 ?

- **Connect Status:** Indicate the remote debug server's connection status.
- **IP:** Specify the server's IP address.

User Agent

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

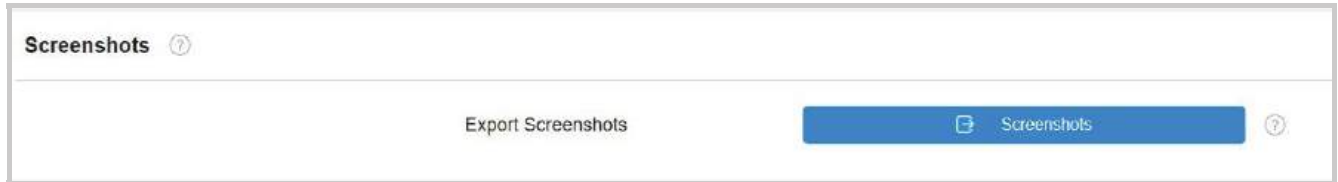
To set it up, go to the web **Account > Advanced > User Agent** interface.

User Agent ?	
User Agent	?

Screenshots

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

To take screenshots, go to **Upgrade > Diagnosis > Screenshots** interface. Click **Screenshots** to capture the current screen.

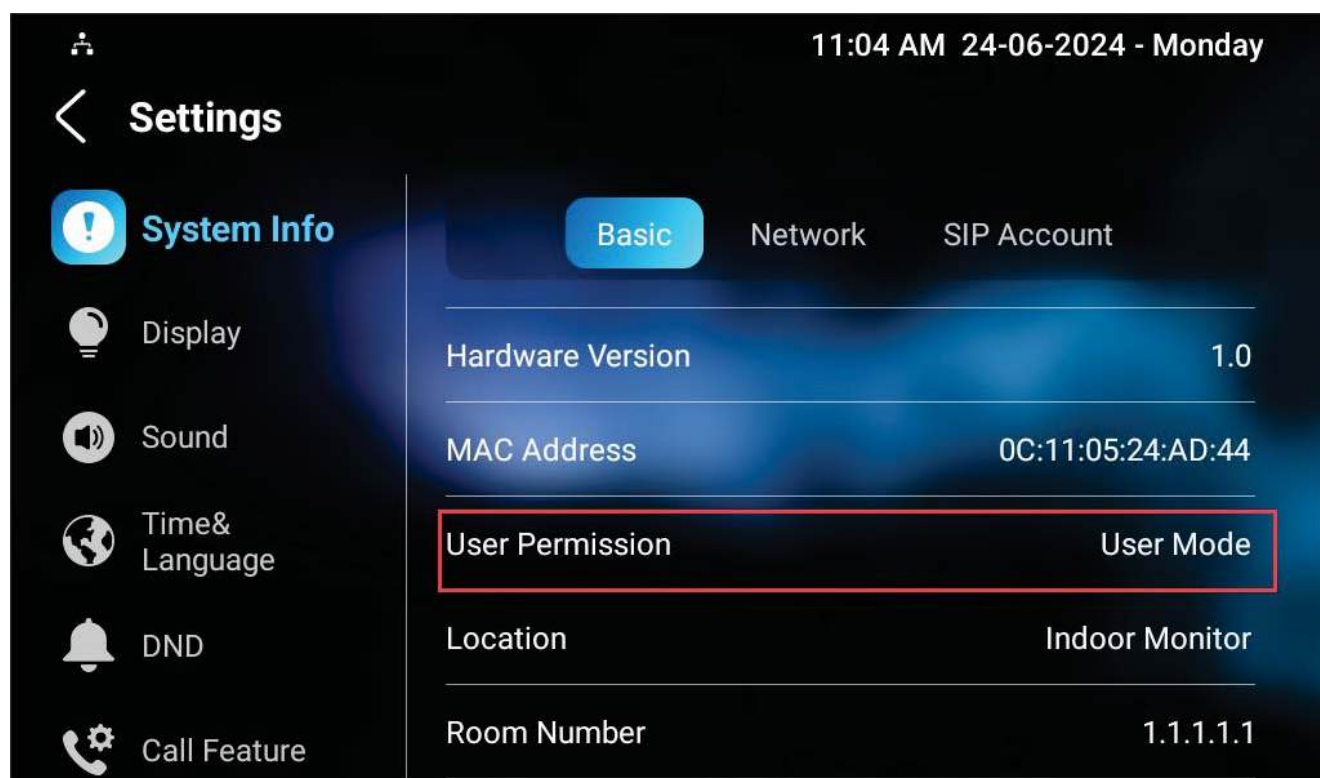


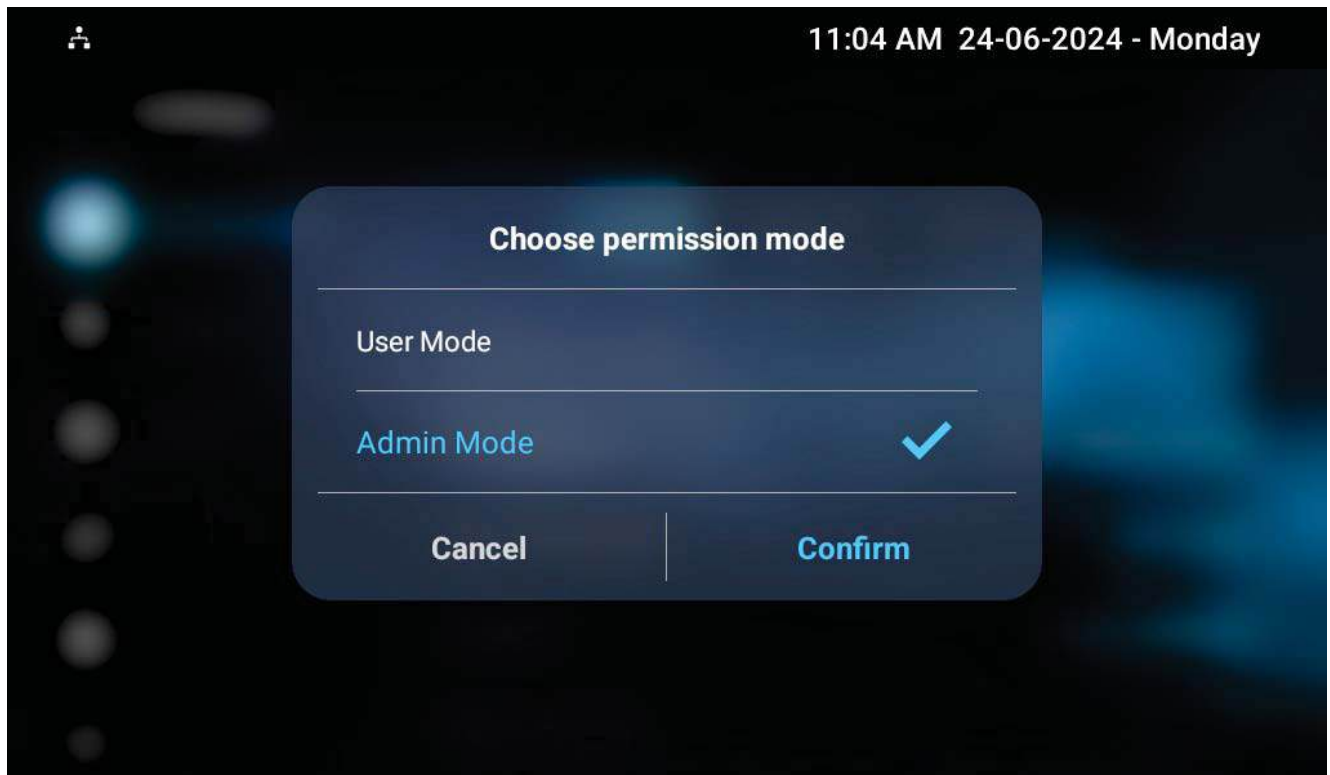
Device Integration with Third Party

Enter Applications Screen

The content of this part mainly teaches you how to enter the APK interface through hidden operations.

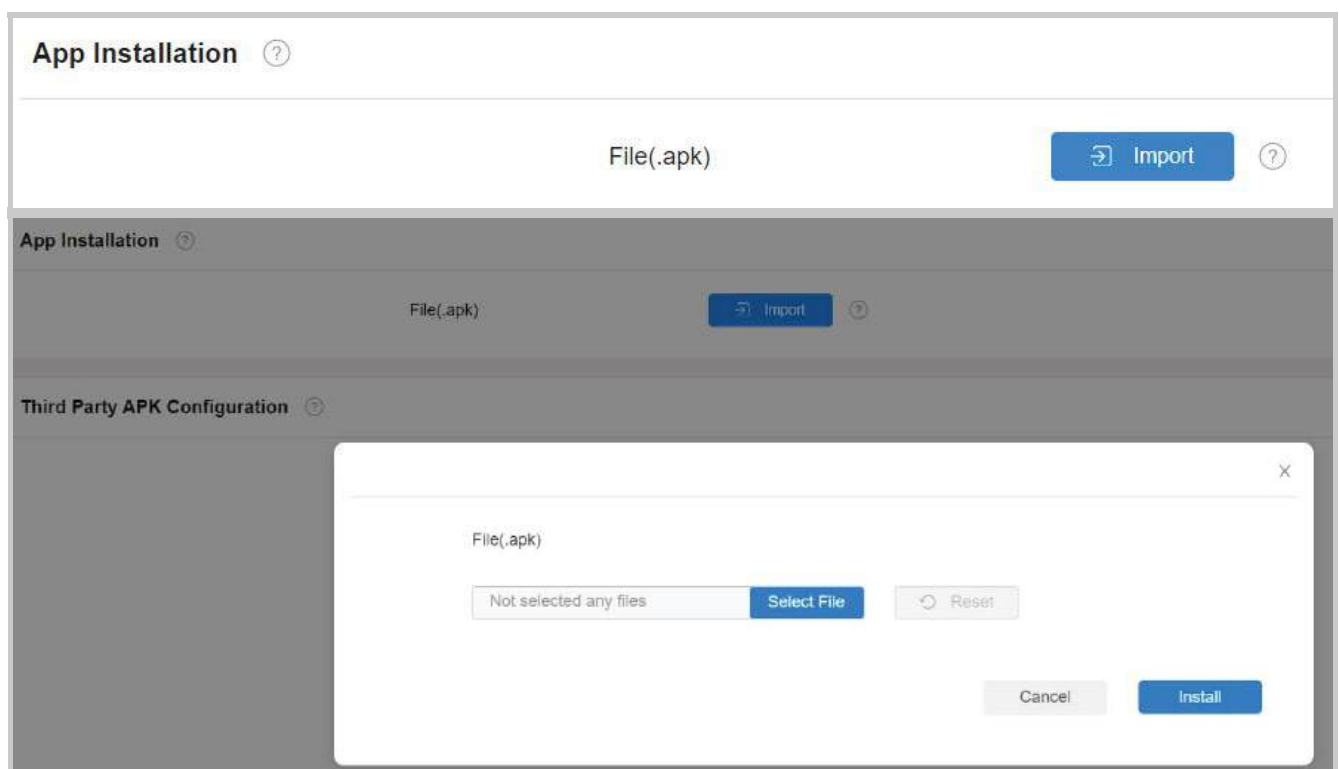
Go to the **Settings > System Info** interface. Tap on **User Mode** 10 times. Then select **Admin Mode** and tap Confirm.





Install and Configure Third-party App

To install the third-party app, go to the web **Device > Third Party APK** interface. Upload the APK file from the PC. If you want to clear the APK file uploaded, click **Reset**.



To configure the installed third-party app, you can click the **App Name** to select the specific app for configuration. Then tick the check boxes of each field for the specific configuration.

Third Party APK Configuration

App Name		?
Intervals Without Operating (Sec)	10	?
Start Up Enabled	☐	?
Turn Back App	☐	?
Turn Back App After Awakening	☐	?
APP Keep-Alive	☐	?

General

Turn Back App After Calling	☒	?
Show App Icon	☒	?

- **App Name:** Select the app to be configured.
- **Intervals Without Operating(Sec):** Set the time to return to the app when there is no operation on the device.
- **Start Up Enabled:** Allow the app to run automatically when the device is turned on.
- **Turn Back App :** Allow automatic returning to the app.
- **Turn Back App After Awakening :** Allow the device to return to the app when the screen is awakened.
- **APP Keep-Alive:** Allow the app to stay running without being turned off.
- **Turn Back App After Calling:** Allow the device to return to the app automatically after finishing a call.
- **Show App Icon:** Allow the app icon to be displayed on the screen.

Integration via HTTP API

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

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

API Setting

API	Disabled
Auth Mode	Digest
Username	
Password	*****

- **API:** When the function is disabled, any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode:** It is Digest by default. The password encryption method only supports MD5. MD5(Message-Digest Algorithm) In the Authorization field of the HTTP request header: WWW-Authenticate: Digest realm="HTTP API",qop="auth,auth-int",nonce="xx",opaque="xx".
- **Username:** Set the user name when Digest authorization mode is selected. The default user name is admin.
- **Password:** Set the password when Digest authorization mode is selected. The default password is admin.

RS485 Setting

The indoor monitor can be connected to relays via RS485 for third-party relay control.

To set it up, go to **Device > RS485** interface.

RS485

RS485 Type	RT-100	?
Destination ID		?

- **RS485 Type:** Select the type of RS485.
- **Destination ID:** Enter the target device ID.

Password Modification

Modify Device Basic Setting Password

Settings Code is used to unlock the screen. The default is 123456.

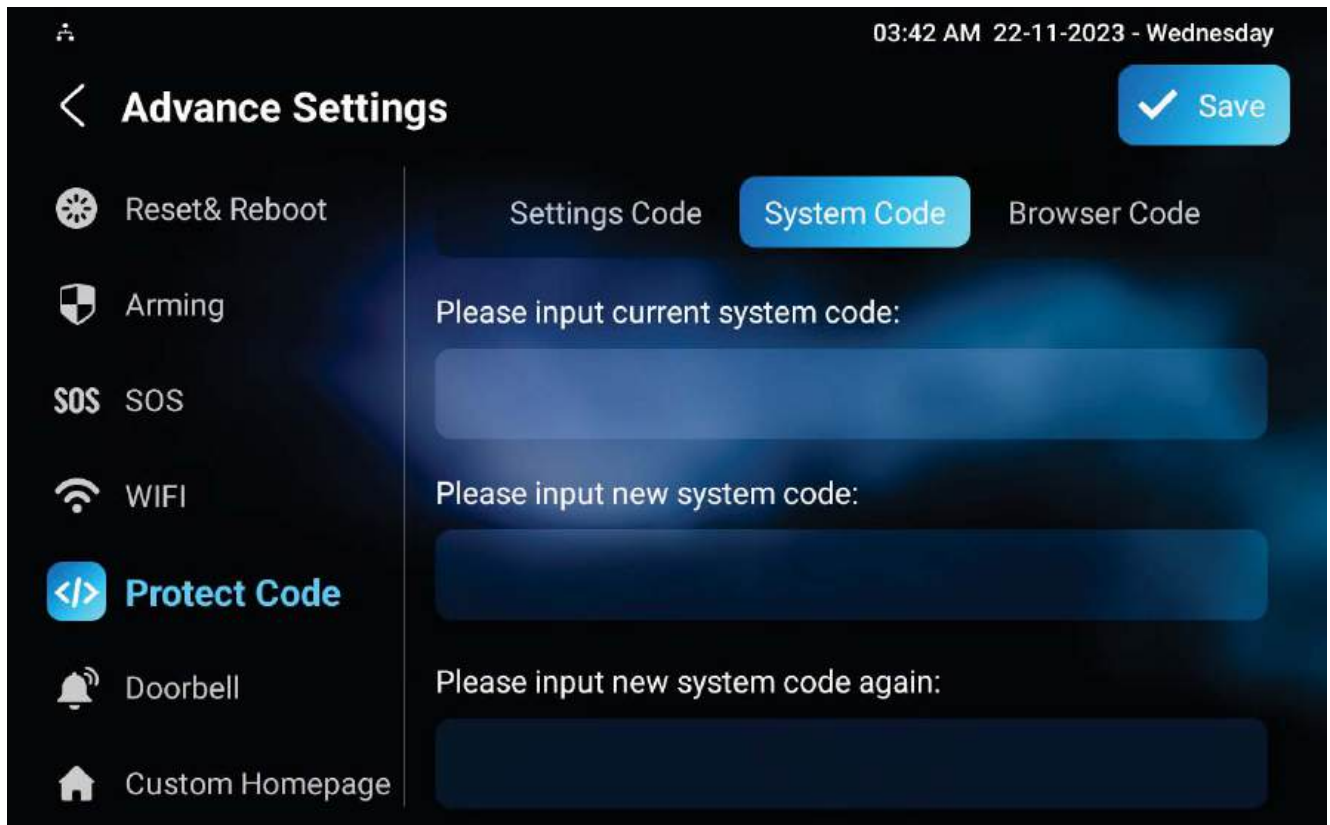
To modify it, go to the **Settings > Advance Settings > Protect Code** screen and select **Settings Code**.

The screenshot shows the 'Advance Settings' interface. On the left is a sidebar menu with options: 'Reset& Reboot', 'Arming', 'SOS', 'WIFI', 'Protect Code' (highlighted with a blue icon), 'Doorbell', and 'Custom Homepage'. The main area has a top bar with a back arrow, the title 'Advance Settings', and a 'Save' button. Below the title are three tabs: 'Settings Code' (selected), 'System Code', and 'Browser Code'. The 'Settings Code' section contains three input fields: 'Please input current settings code:', 'Please input new settings code:', and 'Please input new settings code again:'.

Modify Device Advance Setting Password

This password is used to enter the advance settings of the device, including password settings, account numbers, SOS numbers, network settings, etc. The default password is 123456.

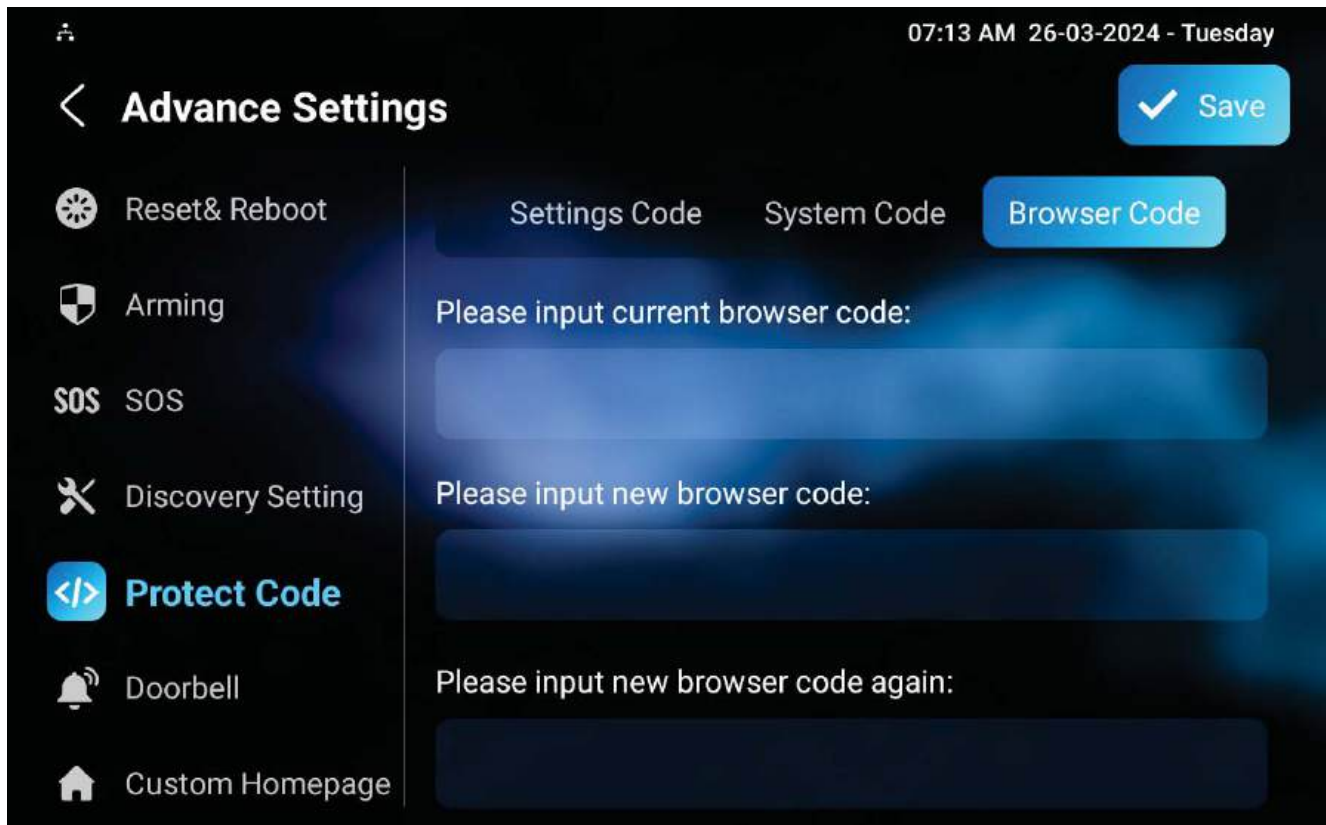
To modify it, navigate to the **Settings > Advance Settings > Protected Code** screen and select **System Code**.



Modify Browser Password

This password is used to lock the browser on the device in case someone abuses the browser for any unwanted application. You can do this configuration on the device screen. The default password is 123456.

To modify it, go to the **Settings > Advance Settings > Protected Code** screen and select **Browser Code**.



Modify Device Web Interface Password

To modify web interface password, you can do it on device web interface. 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

Web Password Modify ?

Username [Change Password](#) ?

Account Status ?

Session Time Out ?

High Security Mode ?

Enabled ?

Change Password

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

Username

Old Password

New Password

Confirm Password

Cancel Change

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

Account Status ?

admin	Enabled	?
user	Disabled	?

Note

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

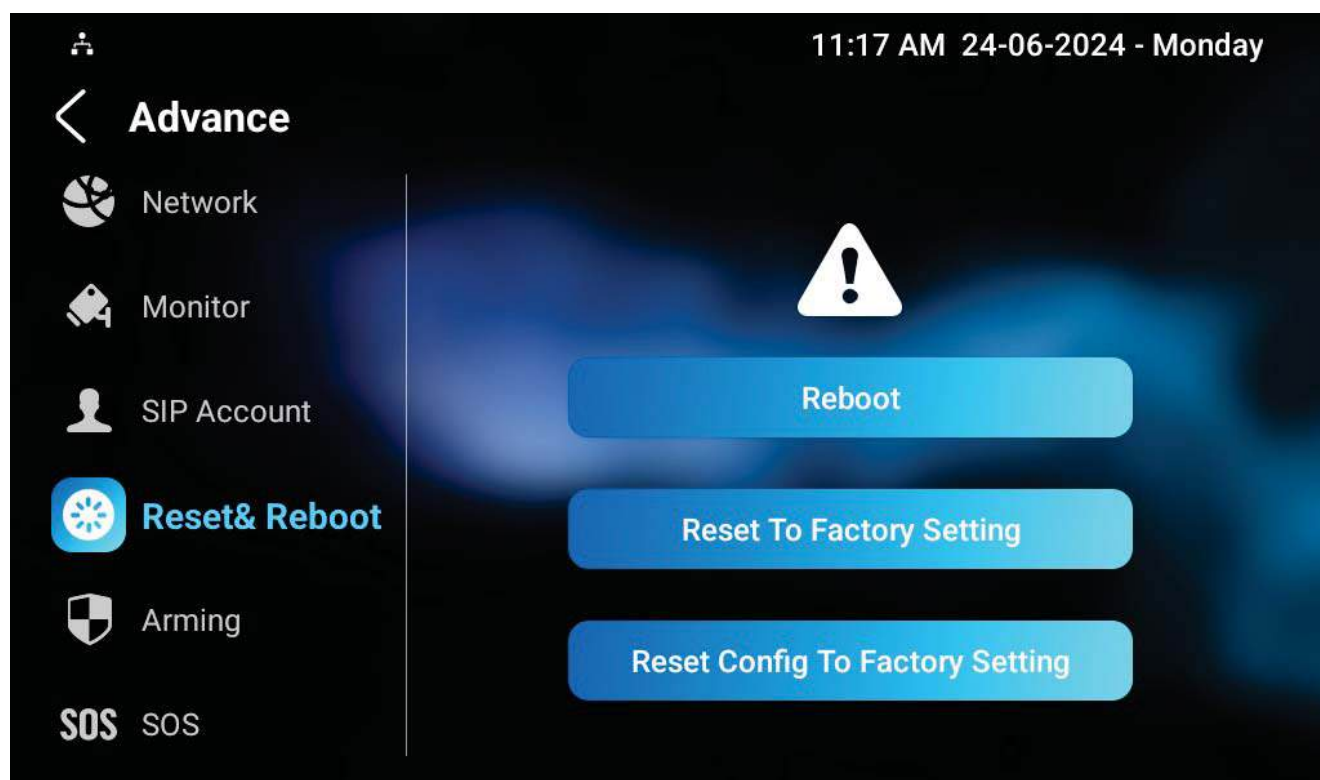
System Reboot & Reset

Reboot

Reboot on the Device

If you want to reboot the system setting of the device, you can operate it directly on the device setting screen or on the device web interface.

To restart the system on the device, go to **Settings > Advance > Reset&Reboot** screen.



Reboot on the Web Interface

If you want to reboot the device system, you can operate it on the device web interface as well. Moreover, you can set up a schedule for the device to be restarted.

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

Basic

Firmware Version	316.30.12.113	
Hardware Version	1.0	
Upgrade	Import	
Factory Default	Reset	
Reset Config	Reset	
Reboot	Reboot	

To set up the device restart schedule on web **Upgrade > Advanced > Reboot Schedule** interface.

Reboot Schedule

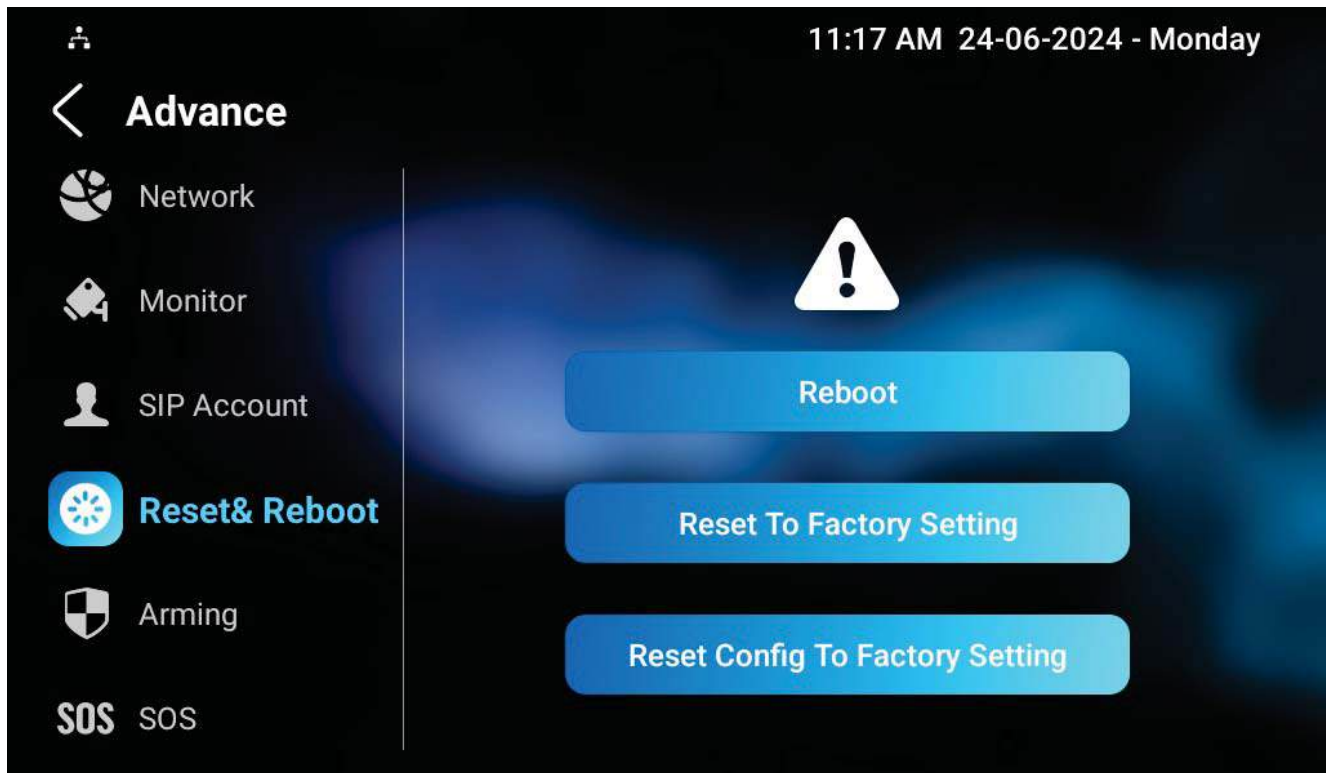
Switch	☐	
Schedule	Every Day	
	0	Hour(0~23)

Reset

Reset on the Device

If you want to reset the whole device system to the factory setting, you can operate it directly on the device screen. If you only want to reset the configuration file to the factory setting instead of the whole device system, you can press **Reset Config To Factory Setting** tab.

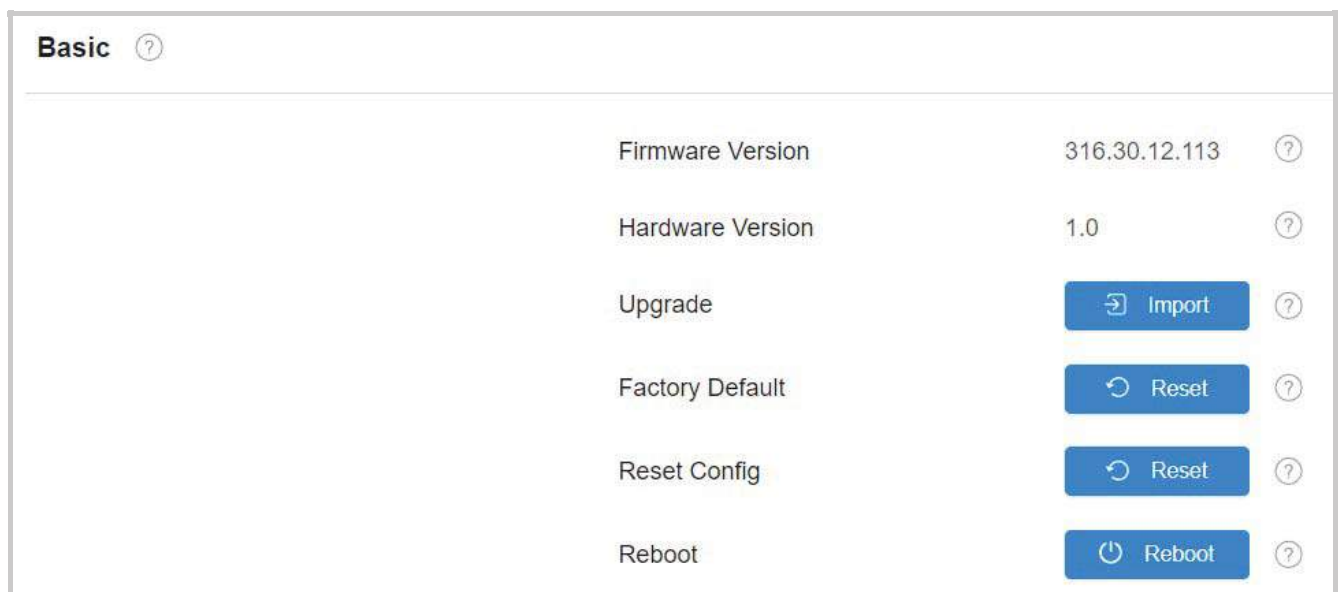
Navigate to **Settings > Advance > Reset&Reboot** screen.



Reset on the Web Interface

The device system can also be reset on device web interface without approaching the device. If you only want to reset the configuration file to the factory setting, you can click **Reset Config**.

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





FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be co - located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator&you body.