About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

AKUVOX S563
INDOOR MONITOR

Administrator Guide

Thank you for choosing the Akuvox S563 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. It is written based on firmware version 563.30.13.901 and provides all the configurations for the functions and features of the S563 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

S563 series is an Android SIP-based with a smooth touch-screen indoor monitor. It can be connected to the Akuvox door phone for audio/video communication, unlocking, and monitoring. Residents can communicate with visitors via audio/video calls, and it supports unlocking the door remotely. It is more convenient and safer for residents to check the visitor's identity through its smart voice changer. S563 series is often applied to scenarios such as villas, apartment complexes, home automation systems, and modern interiors.

Changelog

What's new in version 563.30.13.901:

- Support keeping the monitoring screen on.
- Support switching the live streams between the main and auxiliary cameras during a call with the door phone X910.

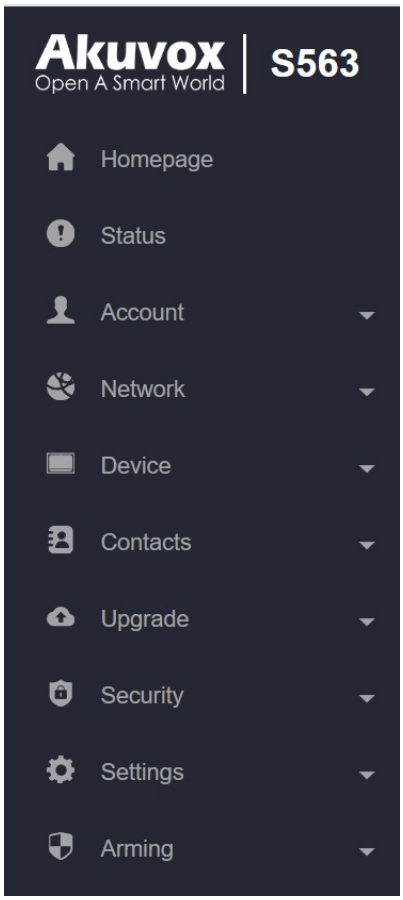
Click here to view the changelog of the device's previous versions.

Model Specification

Model	S563
OS	Android 12
Color	Black
Display	8 Inch IPS LCD
Resolution	1280 x 800
MIC	One microphone,-26dB
Speaker	One speaker, 4Ω / 2W
Wi-Fi	IEEE802.11 b/g/n
Bluetooth	4.2
Ethernet	2xRJ45, 10/100Mbps adaptive
Power Supply	12V DC 1A
Alarm Input	8 x Alarm Inputs
Door Bell Input	1 x Bell In
Relay Output	1 x Relay Out

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.

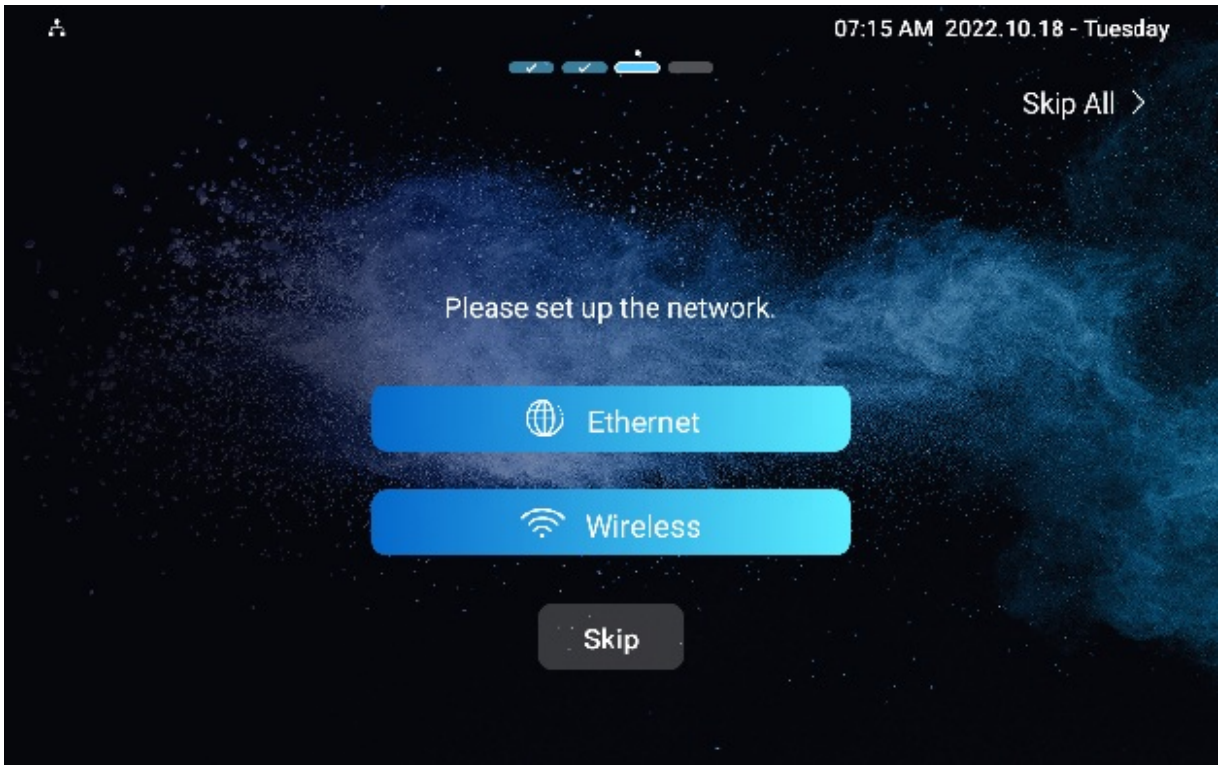

Akuvox
Open A Smart World
S563
Homepage
Status
Account
Network
Device
Contacts
Upgrade
Security
Settings
Arming

Access the Device

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

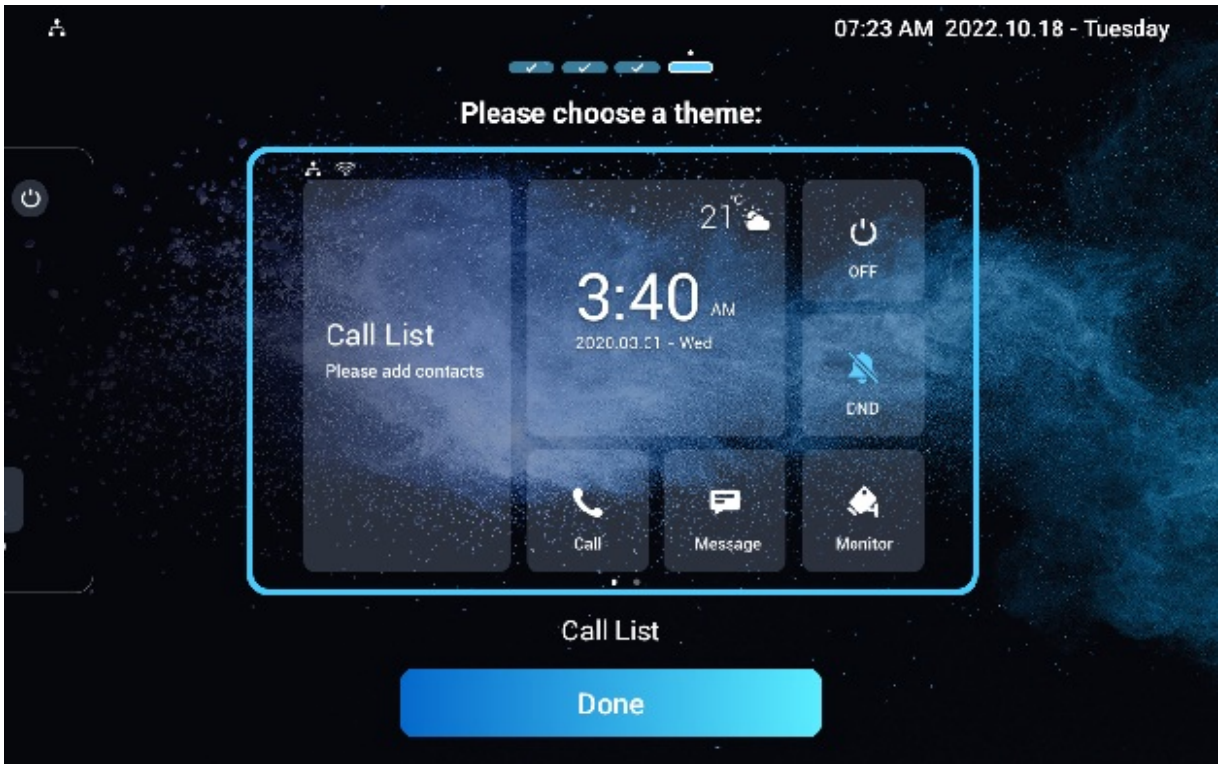


Note

Please refer to **Network Setting & Other Connection** for network configuration.

Device Home Screen Type Selection

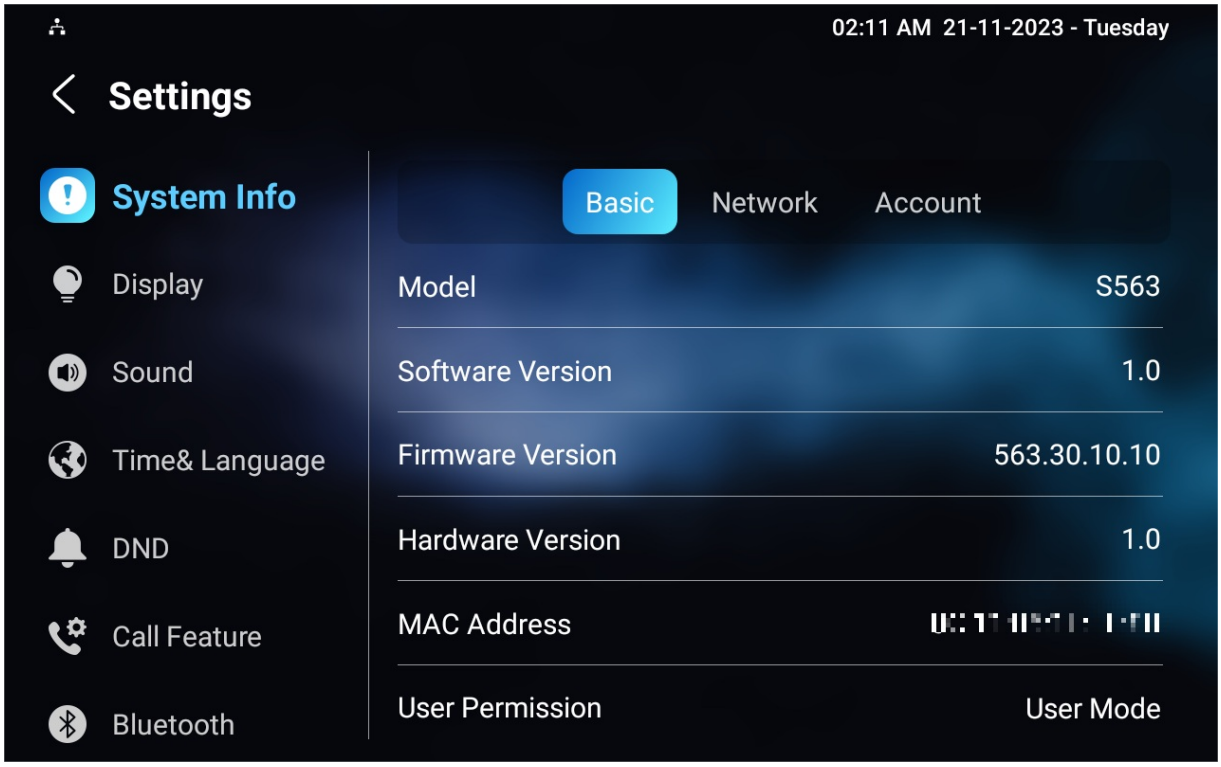
Akuvox indoor monitor supports two different home screen display modes: **Default** and **Call List**. Choose the desired mode.



Access the Device Settings on the Device

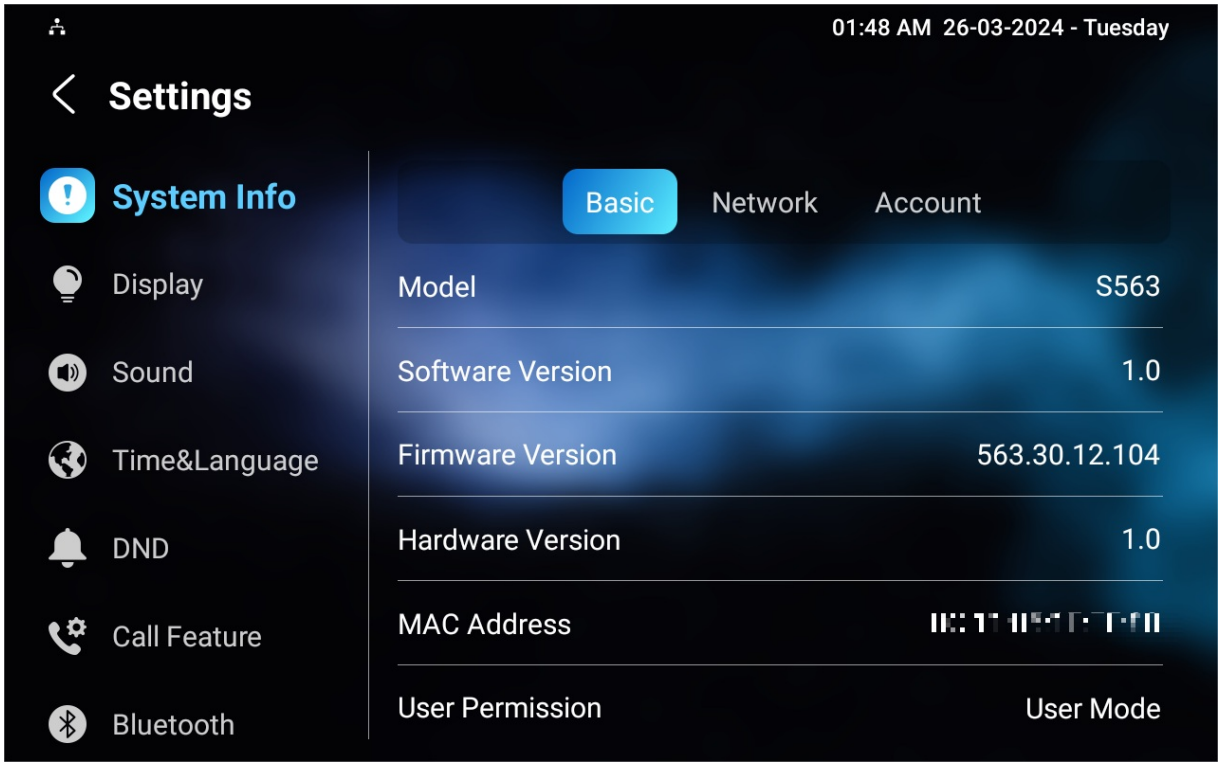
Access Device Basic Settings

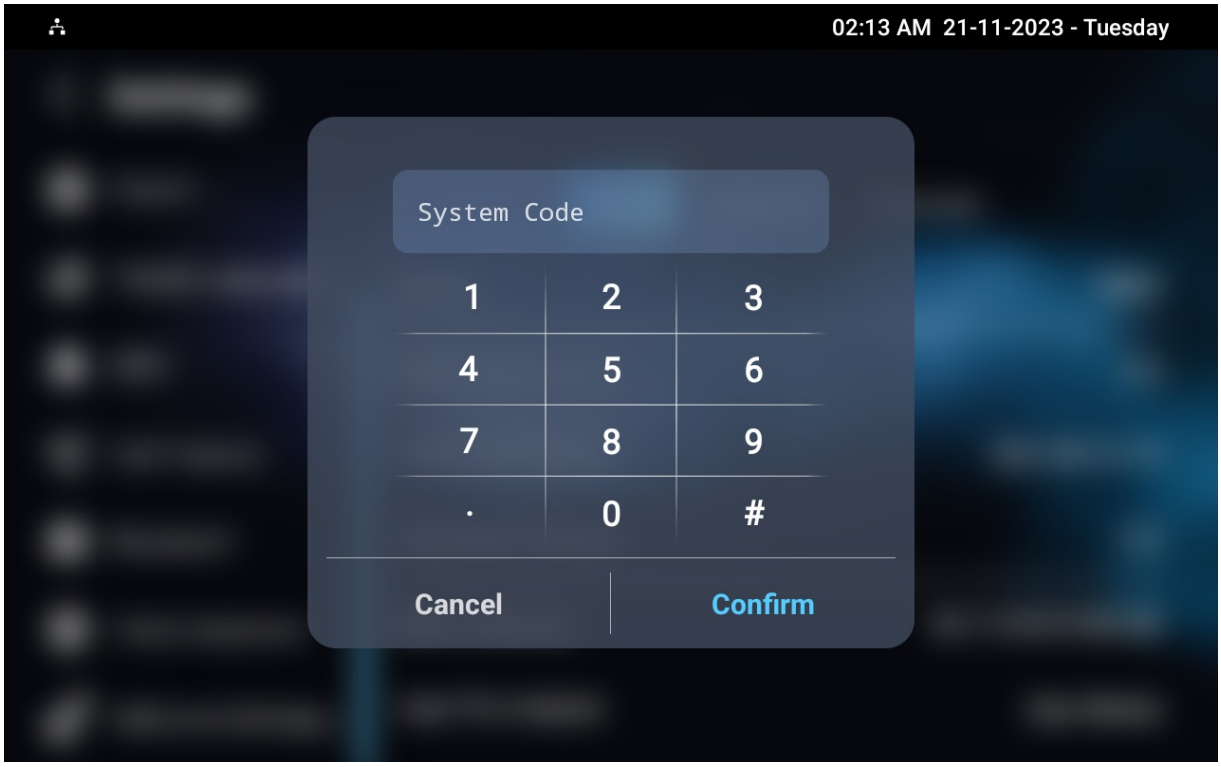
You can access the device's basic and advanced settings to configure different functions. To access the device's basic settings, swipe your finger left on the home screen, then tap . You can check the basic information like MAC, firmware, etc.



Access Device Advance Settings

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

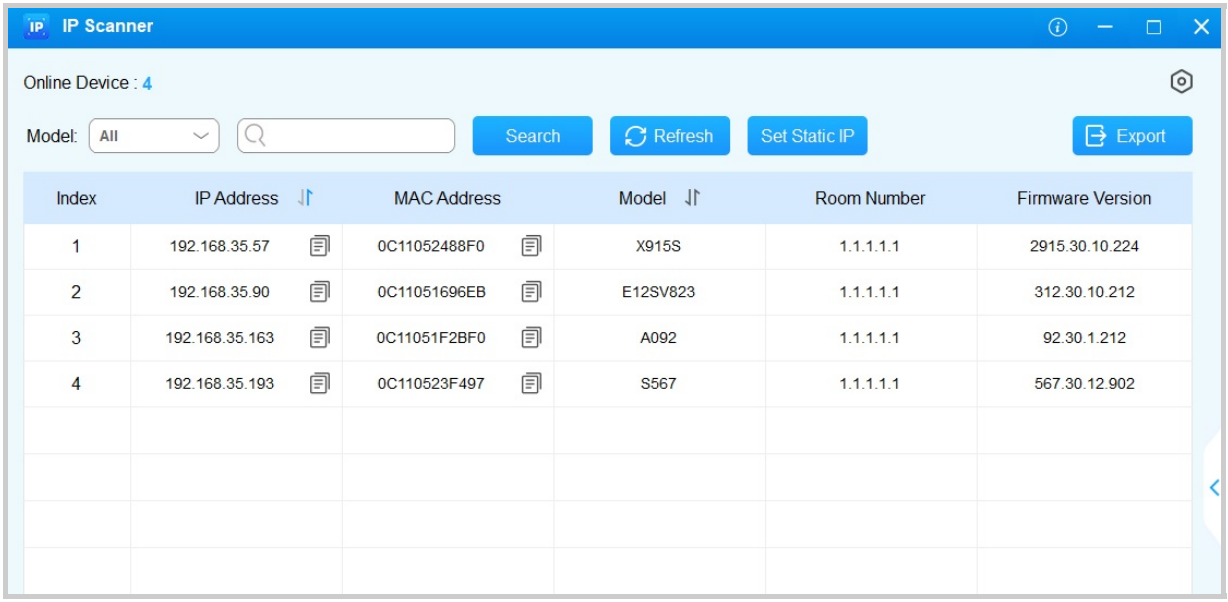


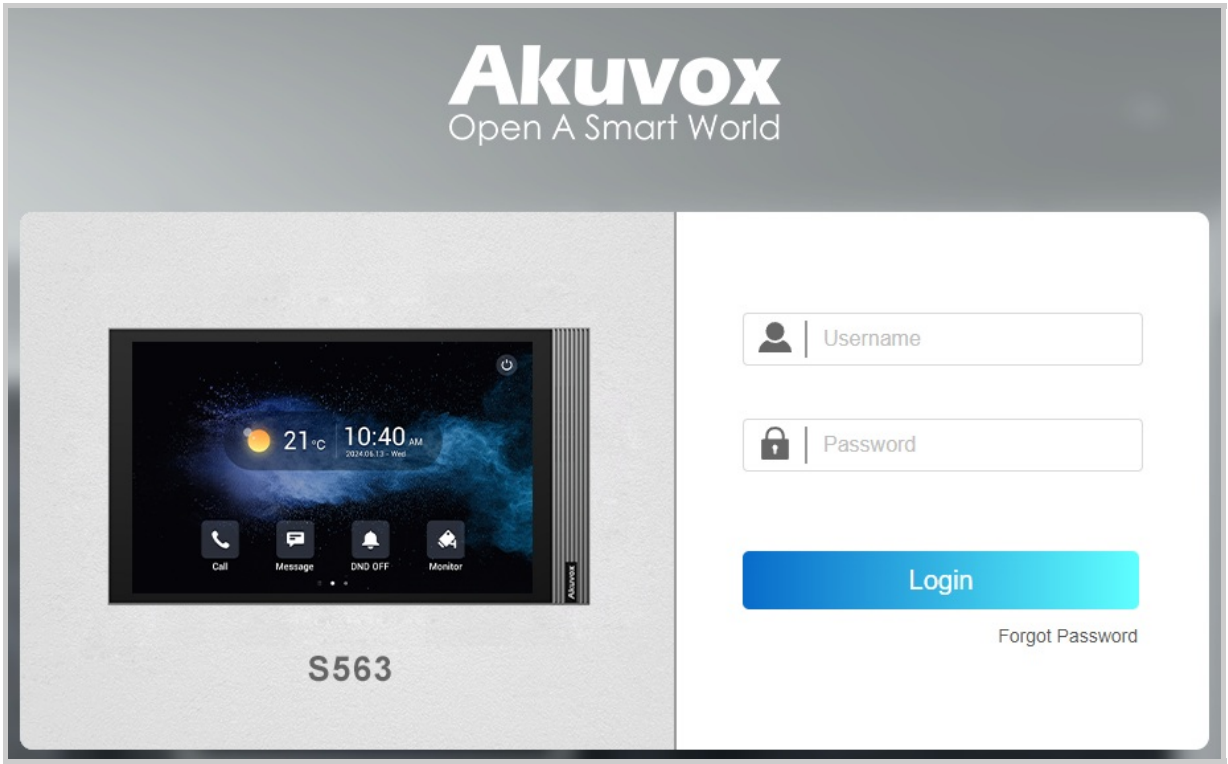


Access the Device Web Settings

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

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





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

Language

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

On the Device

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

The device supports the following languages:

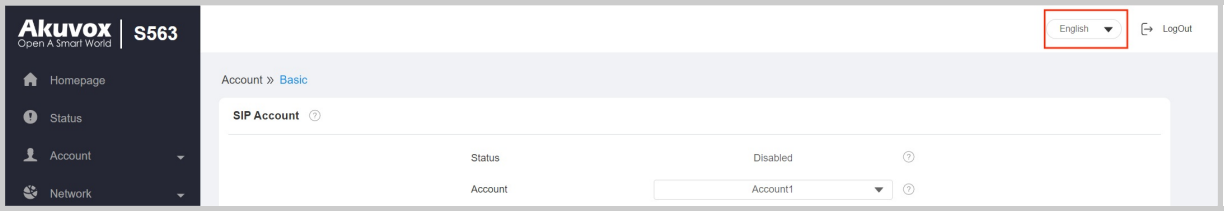
- Bosnian, Czech, Danish, German, English, Spanish, French, Italian, Lithuanian, Mongolian, Norwegian, Polish, Portuguese, Russian, Slovene, Swedish, Turkish, Vietnamese, Korean, Simplified Chinese, Traditional Chinese, Japanese, Ukrainian, Dutch, Arabic, and Hebrew.

On the Web Interface

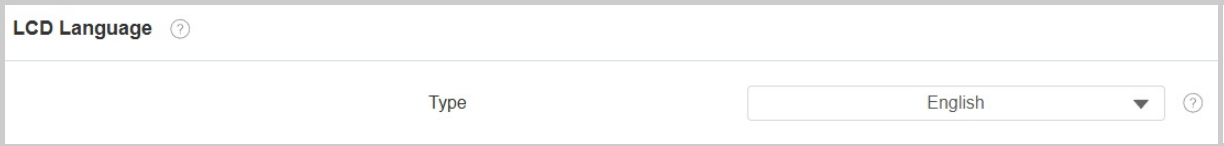
You can select the device web language in the upper right corner.

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

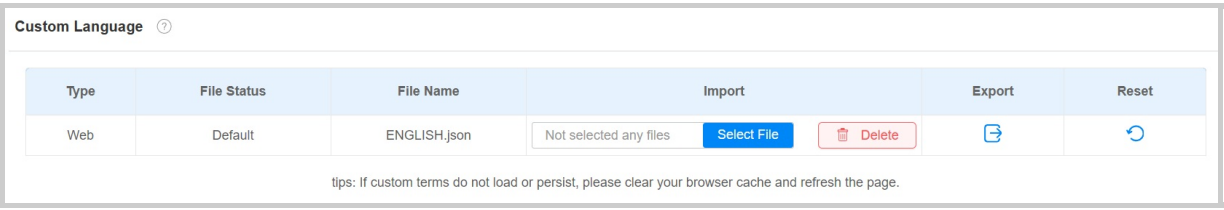


The device supports the following languages:

- 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, Arabic, and Hebrew.

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.

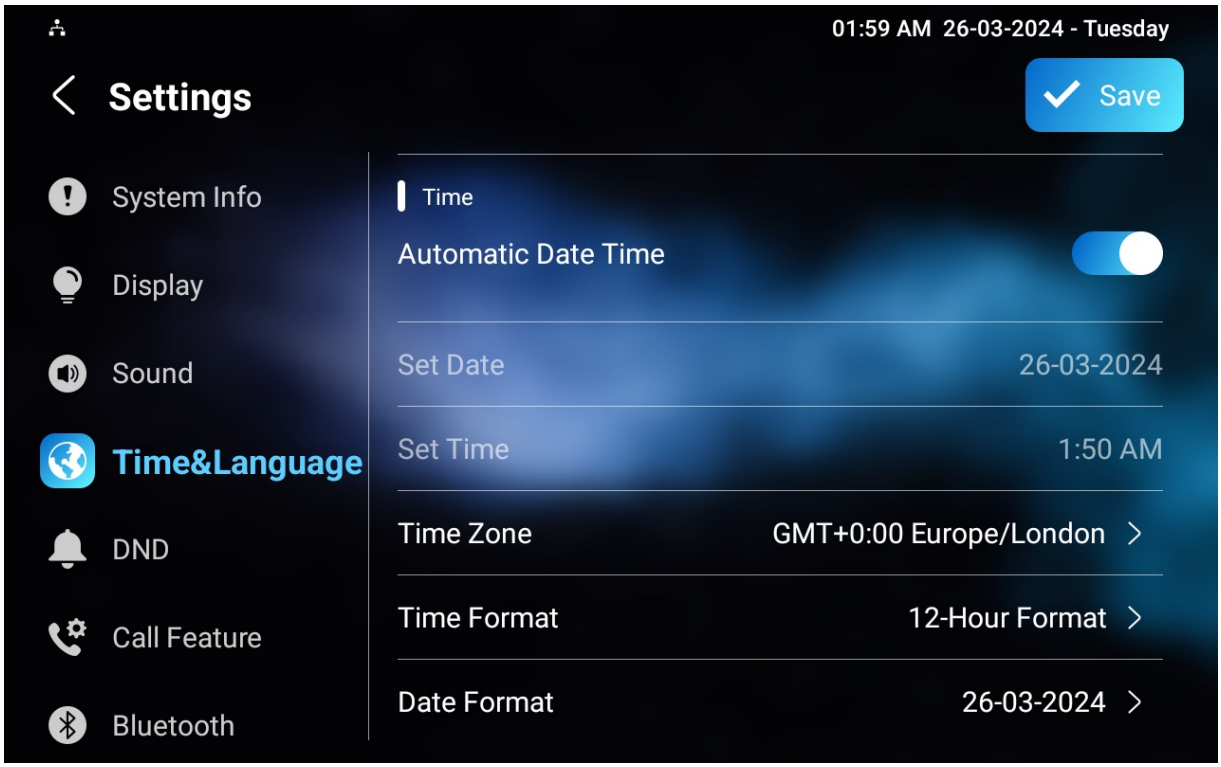


Time

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

On the Device

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

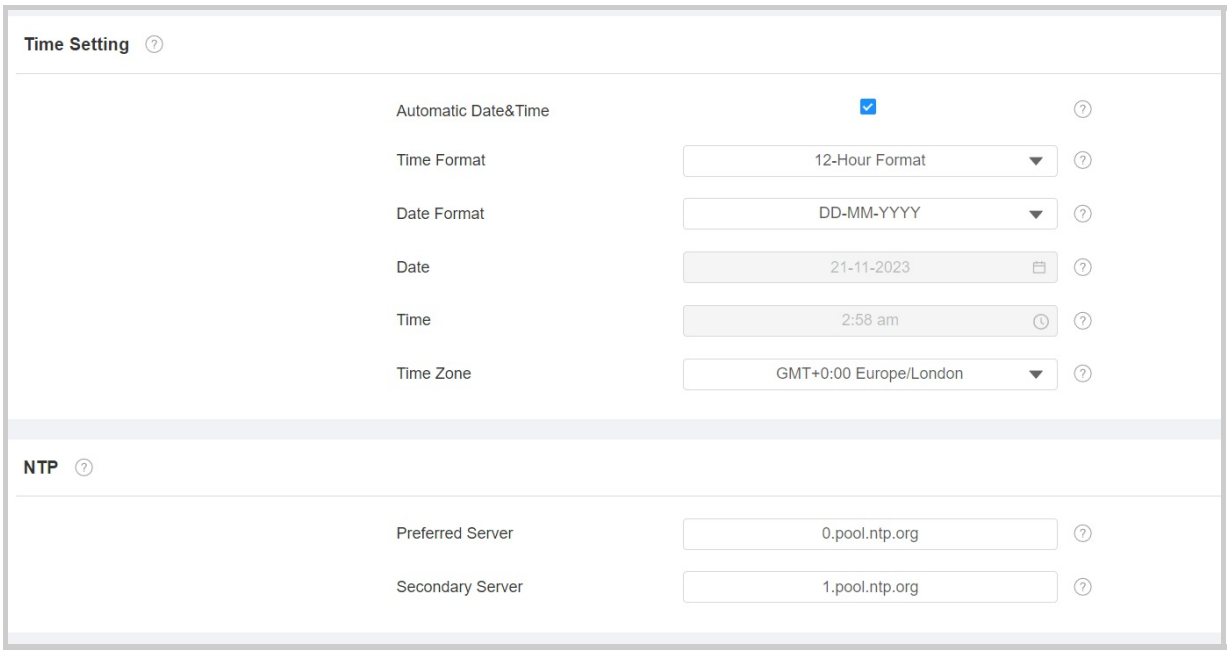


- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the 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 Server/NTP Server2**: Enter the NTP server address. NTP server 2 is the backup.

On the Web Interface

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

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



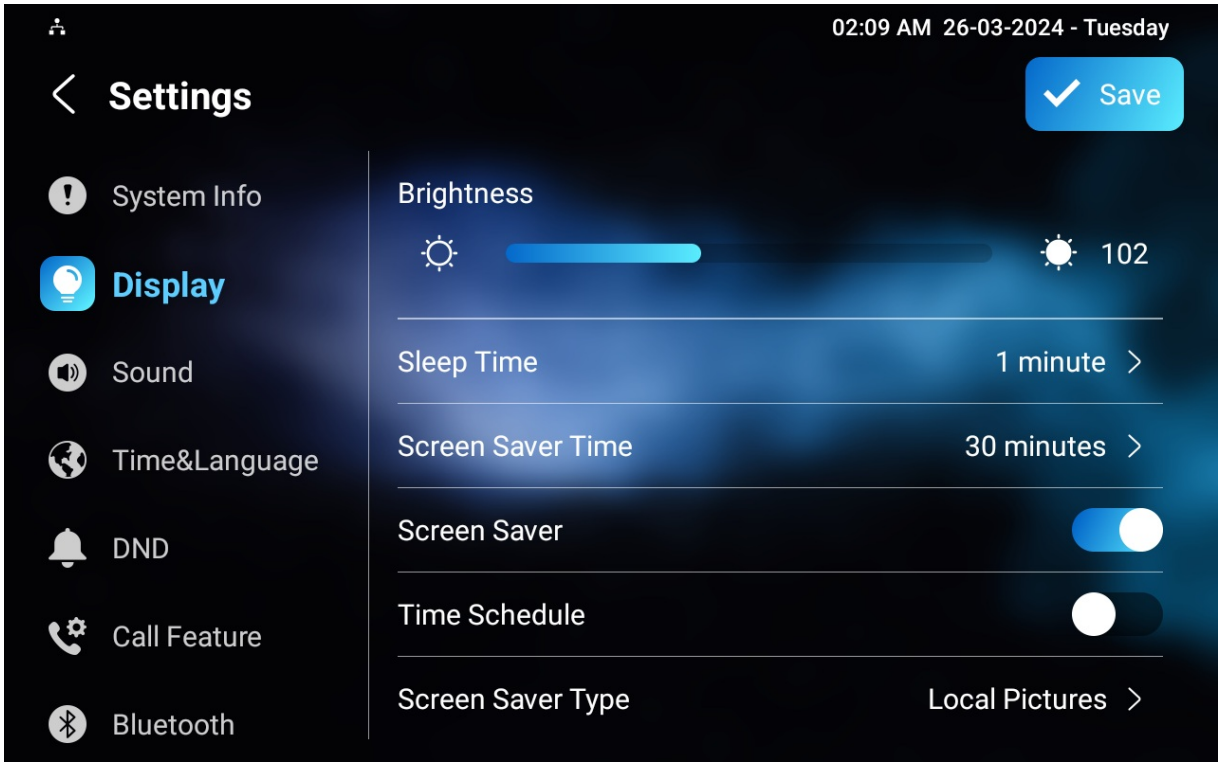
- **Automatic Date & Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the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

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.

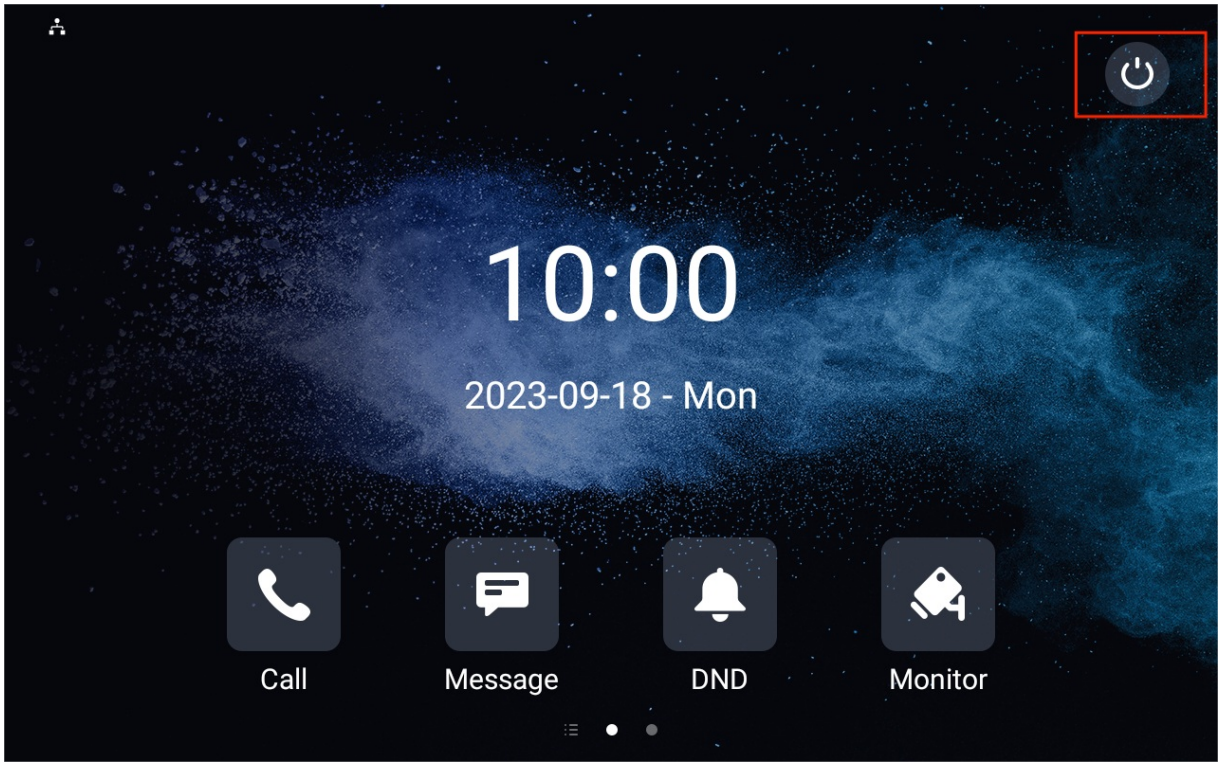


- **Brightness**: Move the blue bar to adjust the screen brightness. The default brightness is 145.
- **Sleep Time**: Set the sleep timing based on the screen saver (15 seconds to 30 minutes).
    - If the screen saver is enabled, the sleep time here is the screen saver start time. For example, if you 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 here 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**:
    - **Local Pictures:** Display pictures uploaded to the indoor monitor as the screen saver.
    - **Local Videos:** Display videos from the indoor monitor as the screen saver
    - **Clock:** Display the clock as the screen saver.

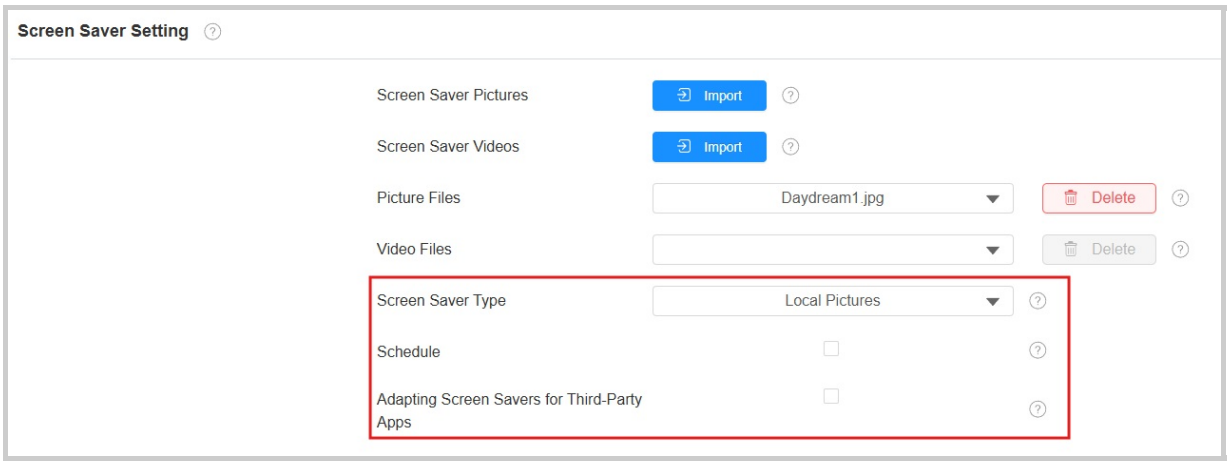
- **Screen Lock**: Lock the screen after the screen is turned off(turn dark). You are required to enter the code to unlock the screen. The default code is 123456.
- **Screen Clean**: Allow users to wipe the screen clean without triggering unwanted changes in the settings.
- **Font Size**: Select the 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.



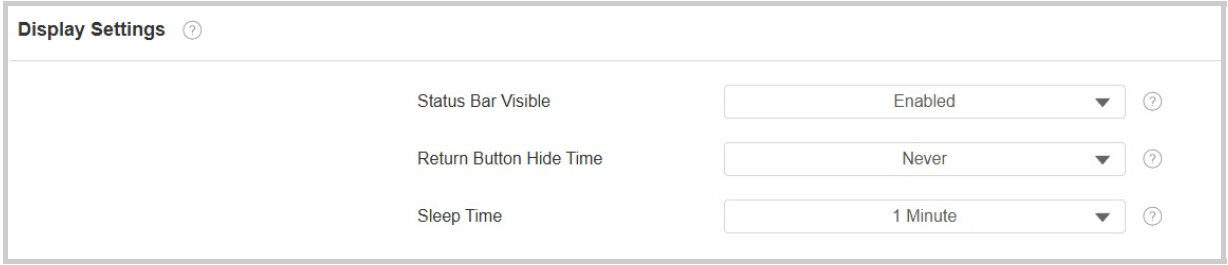
Screen Display Setting on the Web Interface

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



- **Screen Saver Type**:
  - **Local Pictures:** Display pictures uploaded to the indoor monitor as the screen saver.
  - **Local Videos:** Display videos from the indoor monitor as the screen saver
  - **Clock:** Display the clock as the screen saver.
- **Schedule**: Decide the specific time range to display the screen saver.
- **Adapting Screen Savers for Third-Party Apps**: This feature keeps third-party apps running in the background. 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.

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



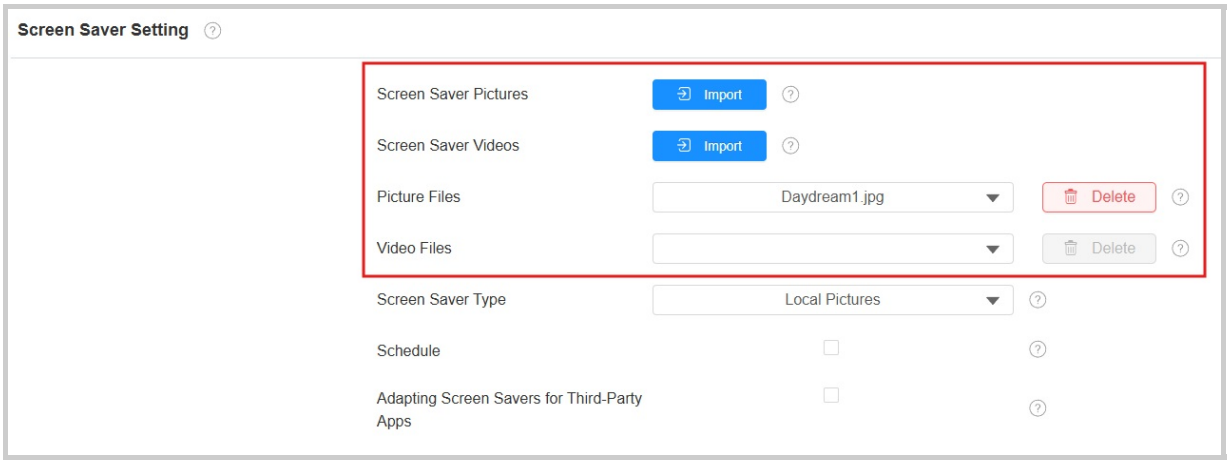
- **Sleep Time**: If the screen saver is enabled, the sleep time is the screen saver's start time. For example, if you set it as 1 minute, the screen saver will start automatically when the device has no operation for 1 minute. If the screen saver is disabled, the screen will be turned off automatically when the device has no operation for 1 minute.

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.



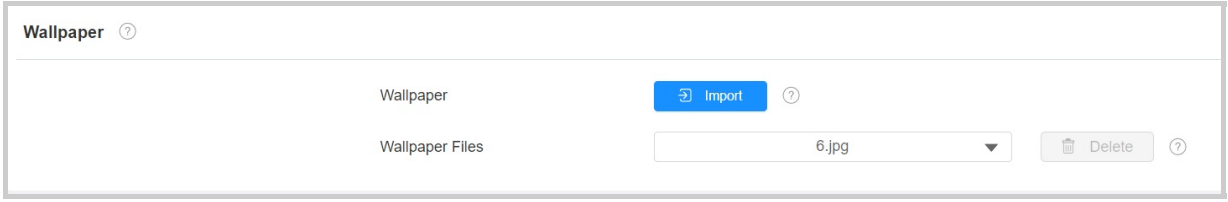
Note

- 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 720*1080.

Upload Wall Paper

You can customize your screen background picture on the device web to achieve the visual effect and experience for users.

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



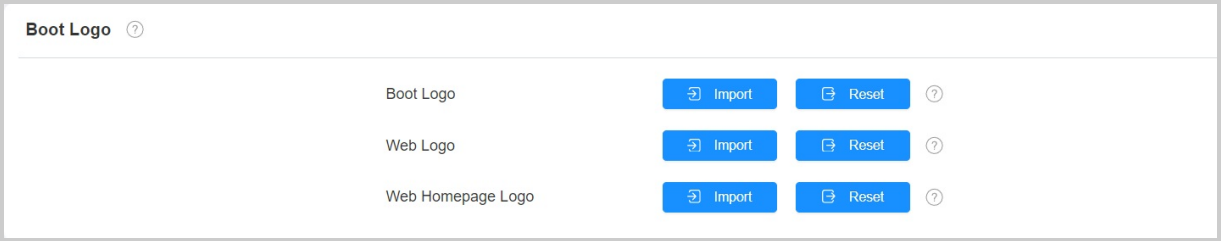
Note

- The pictures uploaded should be in JPG, JPEG, 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.

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

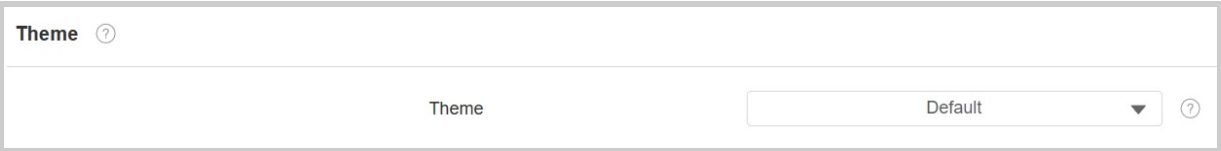


- **Boot Logo**: The logo will appear on the screen when you reboot the device. Supported format: ZIP and PNG; Max size: 1280*800 png.
- **Web Logo**: The logo will appear in the upper left corner of the web interface. Supported format: JPG and PNG; Max size: 252*76 png.
- **Web Homepage Logo**: The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

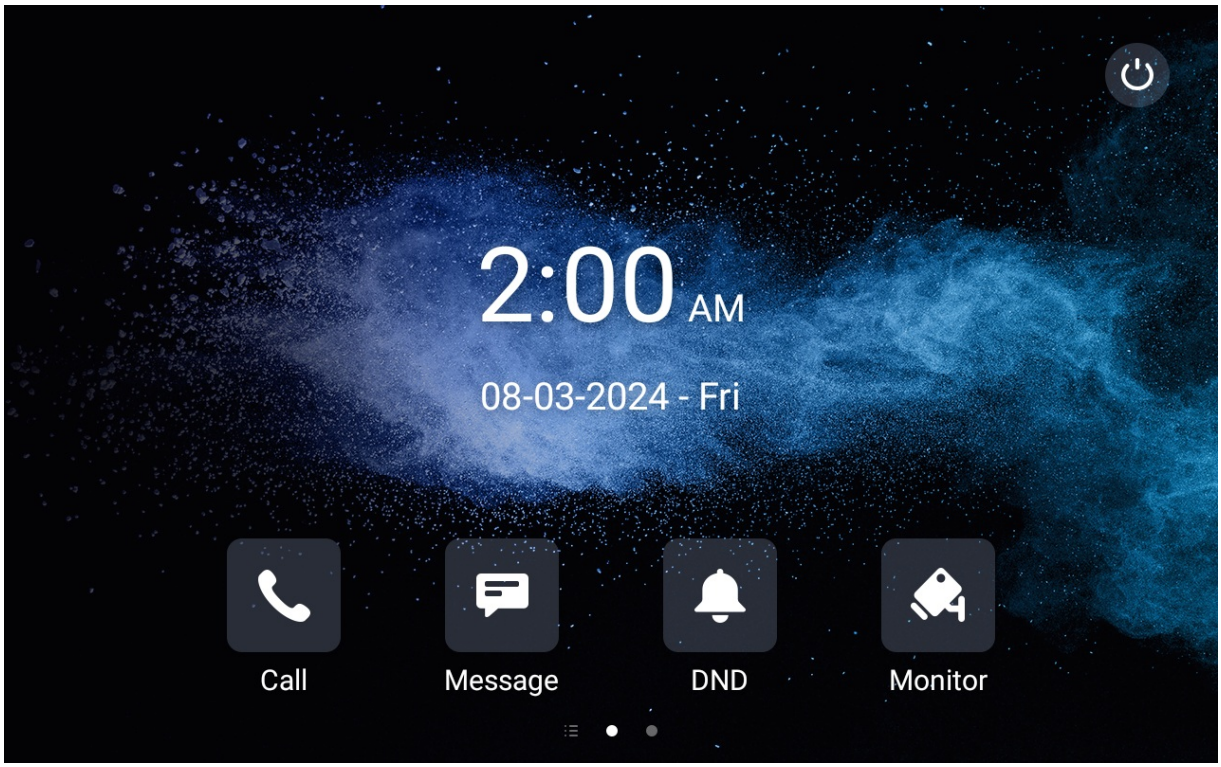
Home Screen Display

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

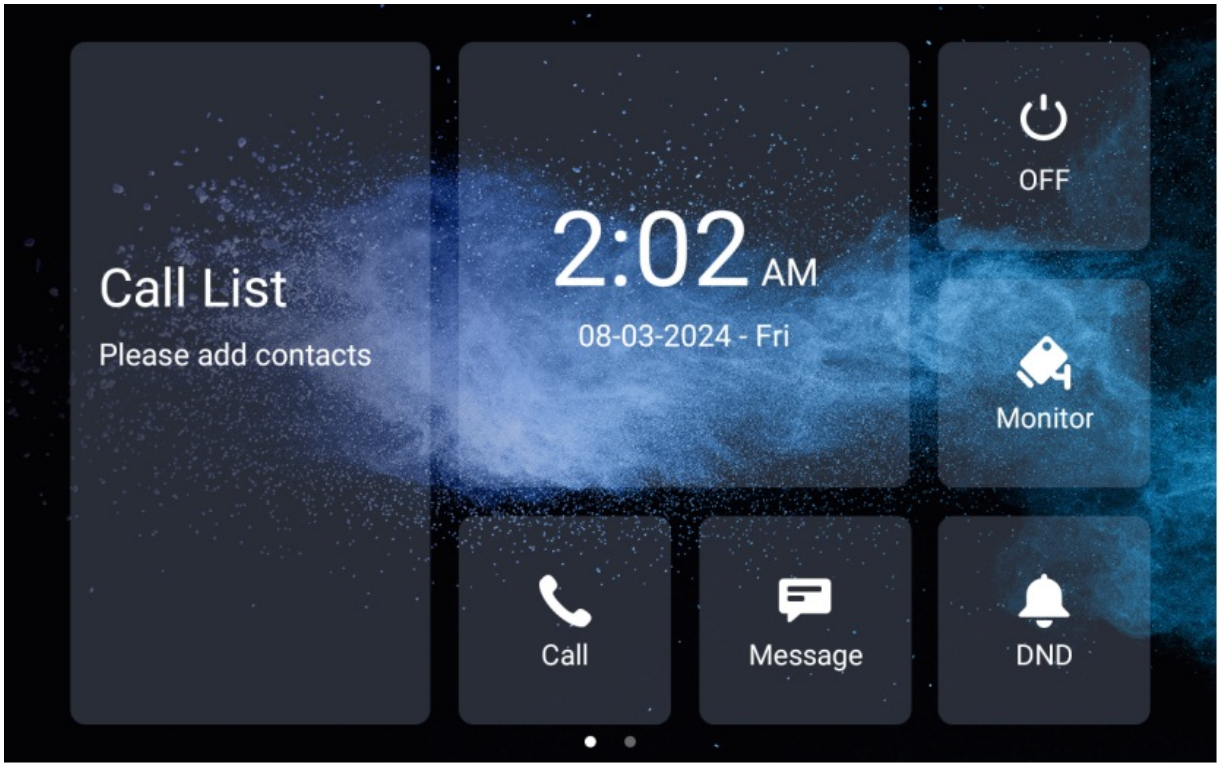
Go to **Device > Display Setting > Theme** interface.



Default Home Screen:



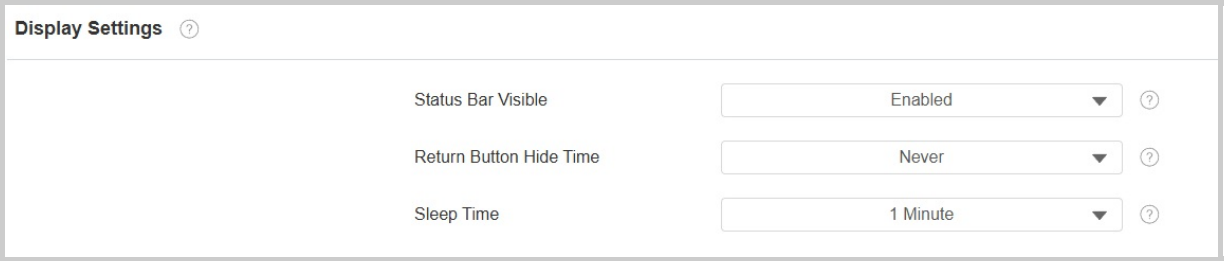
Call List Screen:



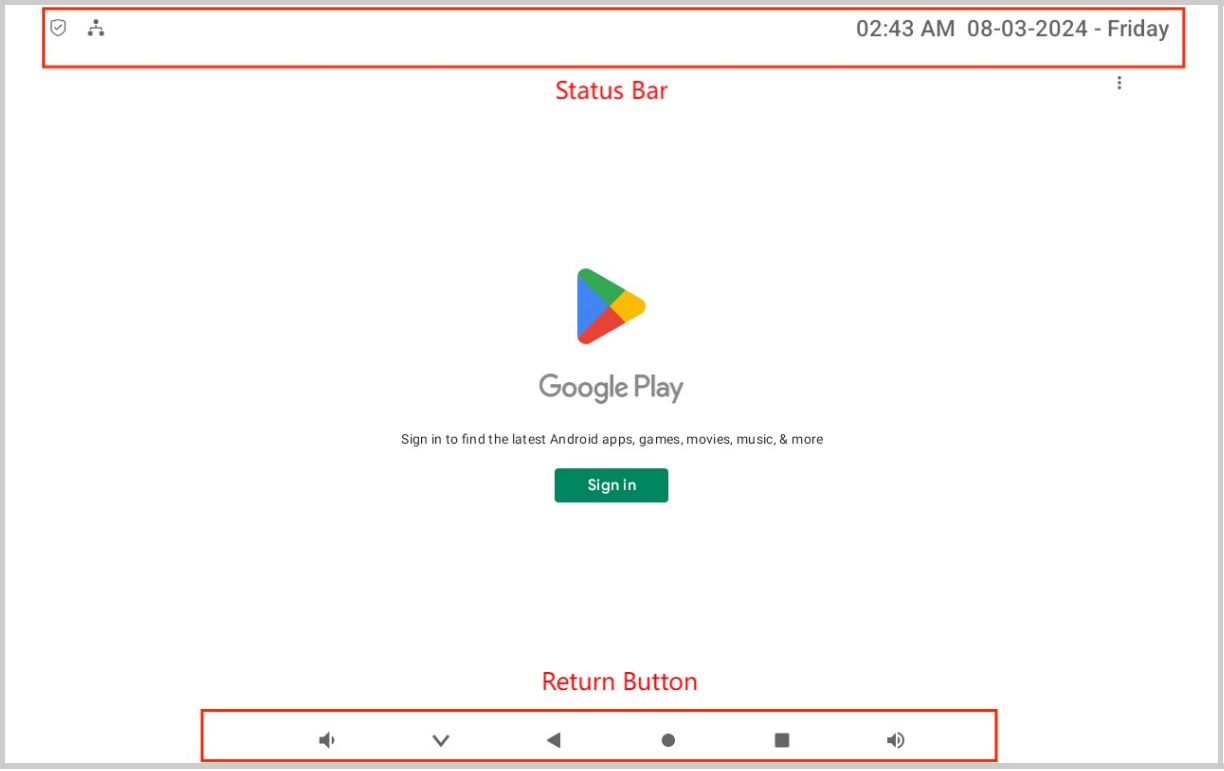
Status Bar Display Configuration

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.



- **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.



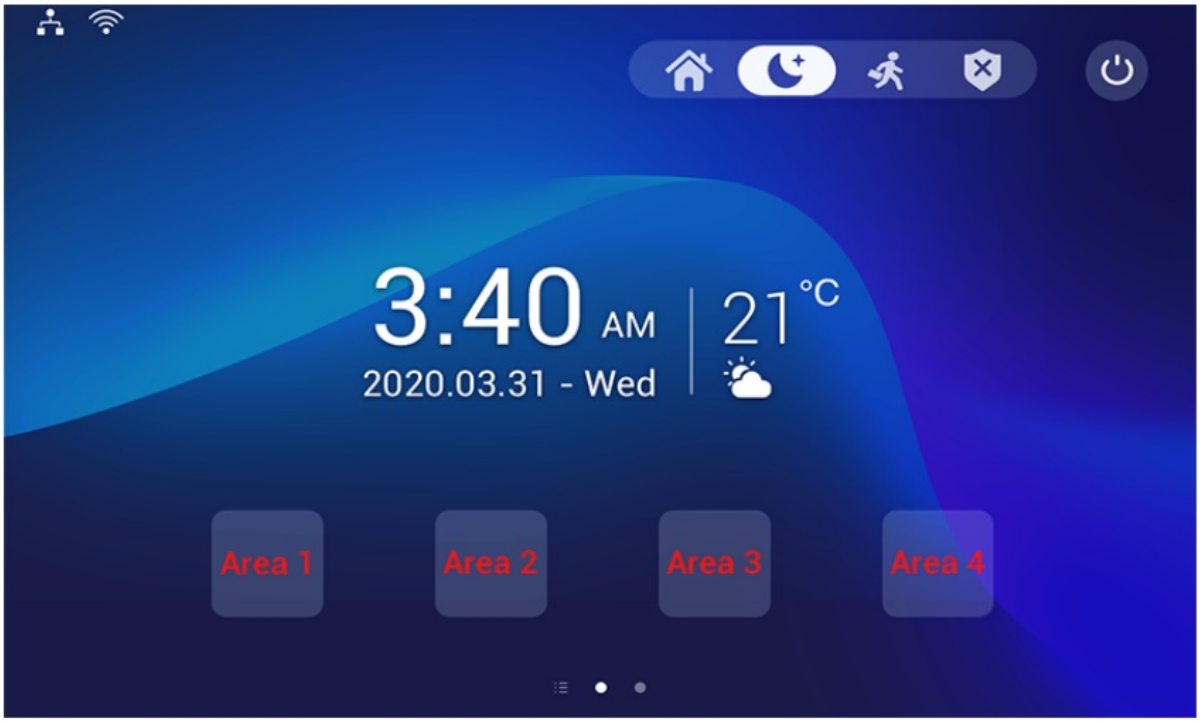
Home Screen Tab Display

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

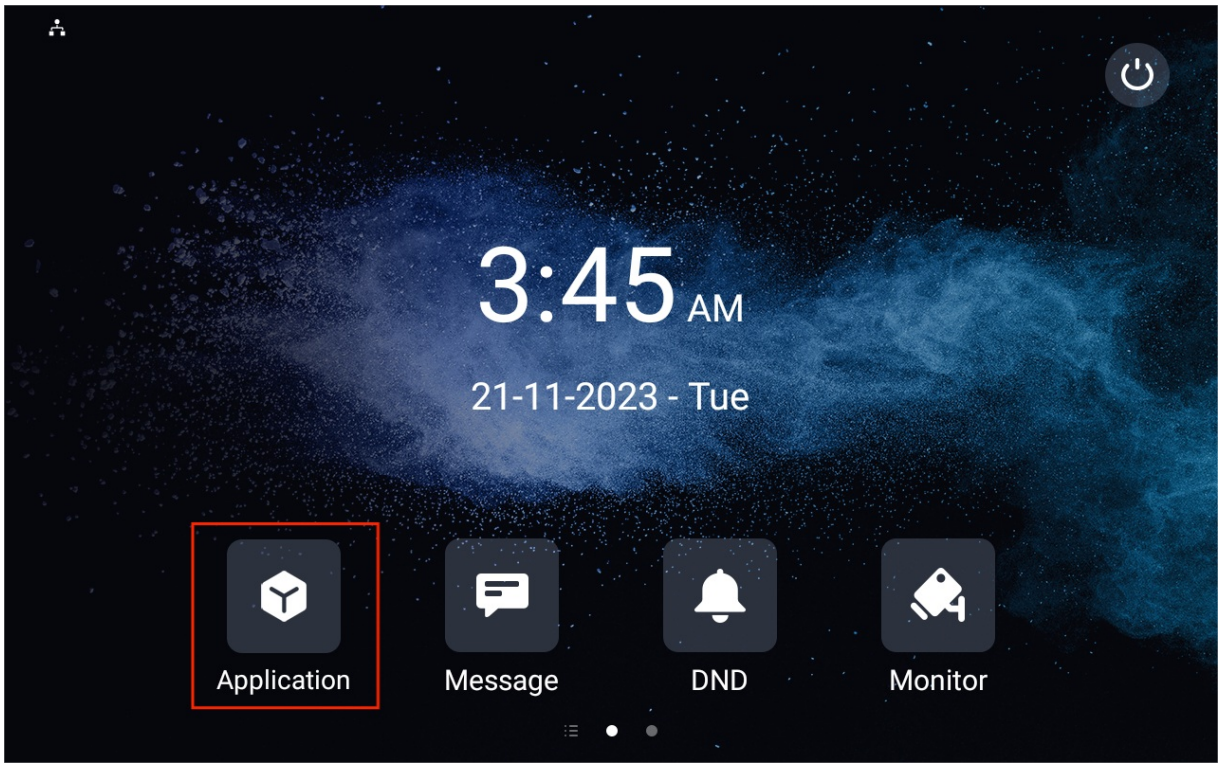
To set it up, navigate to **Device > Display Setting** interface.

- **Type**: Select the functional icon to be displayed on the home screen.
- **Value**:
  - The value field for **Custom APK** will be automatically filled in if you have already installed a third-party app.
  - When you select **Browser**, you are required to enter the URL of the browser before the browser icon can be displayed.
  - When you select **Unlock**, you can select the unlock command from Remote Relay HTTP1-10(Configure Remote Relay HTTP on the **Device > Relay** interface). If the value is left blank, the tab will adopt the setting of Long Press RF Key to Unlock on Idle on the **Device > Relay** interface.
  - When you select **Concierge**, you can enter a speed dial number in the Value field.
- **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.

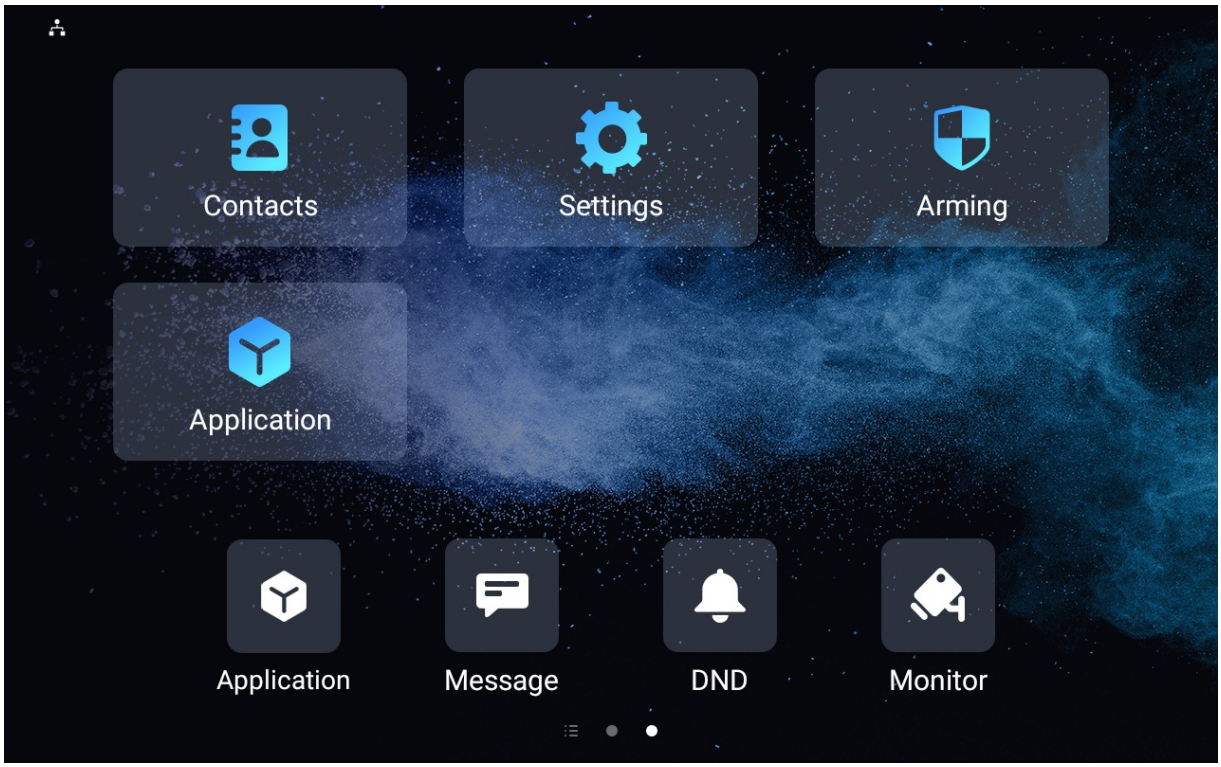
You can click **Example** to see the icon layout.



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.

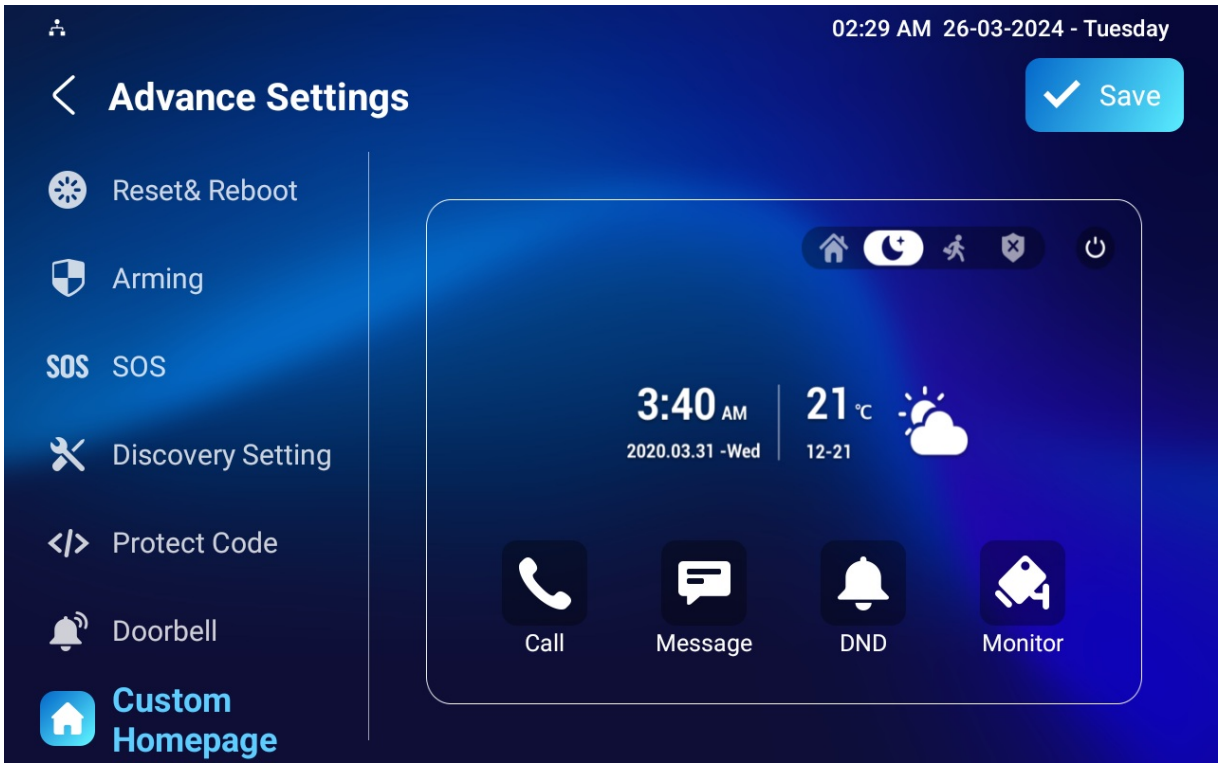


Configure the icons displayed on **More Page Display** on the same interface.



You can also customize the homepage display by selecting your favorite functions on the device screen.

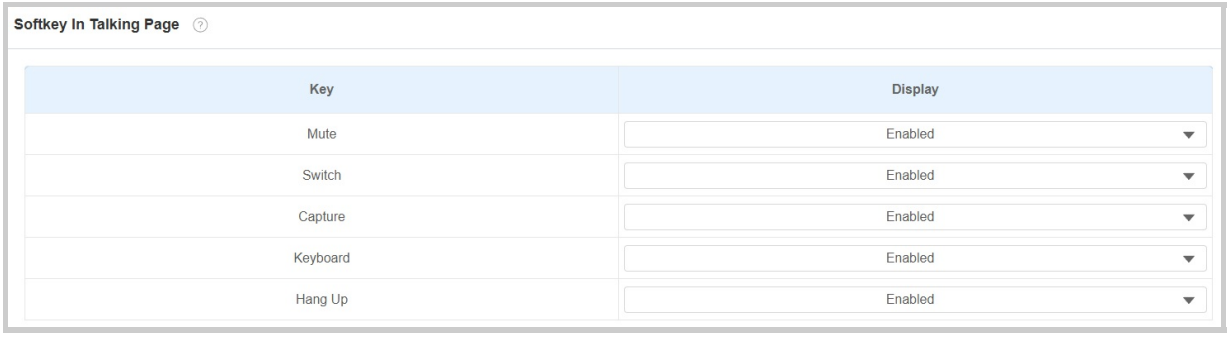
To configure it, tap **Settings > Advance Settings**, and enter the default system code 123456. Tap **Custom Homepage**, then tap any of the icons to select the desired function.



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.



- **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.

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

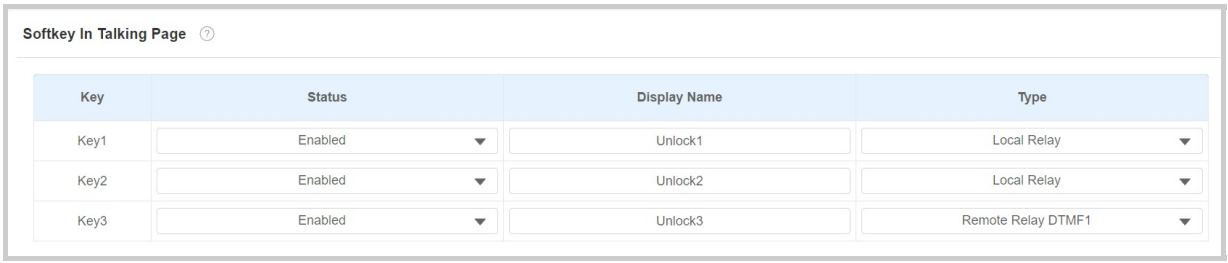
To set up tabs on the **Monitor** screen, go to **Device > Display Setting > Softkey in Monitor Page** interface.

- **Video**: Tap to make a video call to the door phone.
- **Audio**: Tap to make an audio call to the door phone.
- **Capture**: Tap to take a screenshot of the monitor screen.
- **Cancel**: Tap to exit the monitor screen.

Unlock Tab Configuration

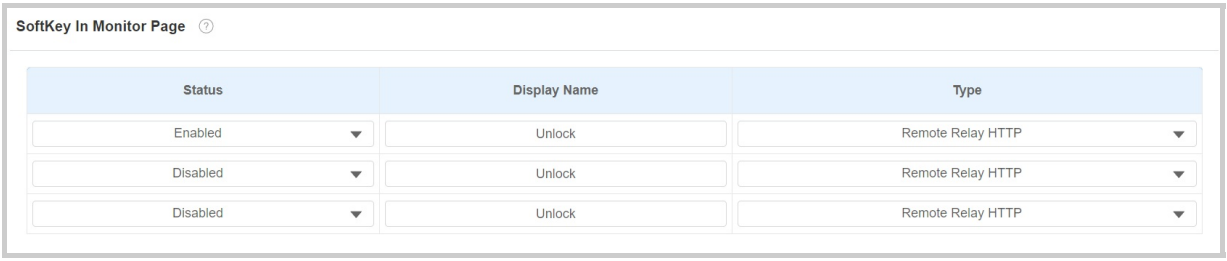
You can customize the unlock tab and select the relay type on the talking, monitor, and call preview screen for the door opening.

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



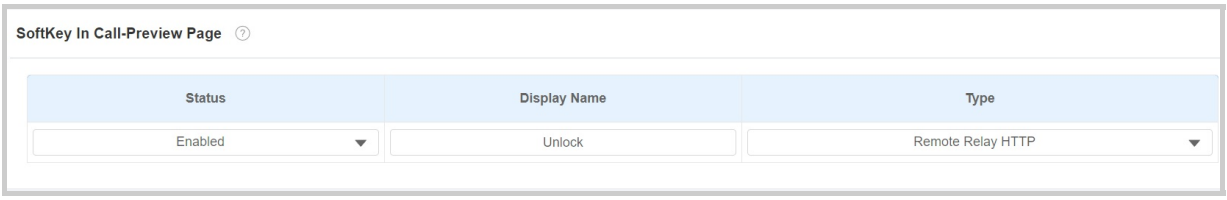
- **Status**: With it enabled, the unlock tab will be displayed on the talking screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up the unlock tab on the **Monitor** screen on the **SoftKey In Monitor Page** section.



- **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.

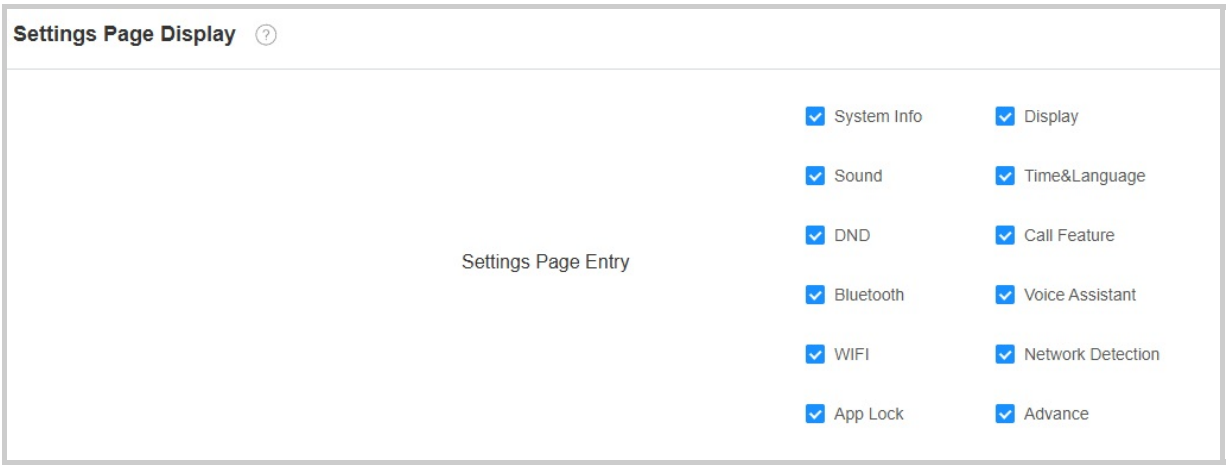


- **Status**: With it enabled, it will be displayed on the call preview screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Function Display on the Settings Screen

You can set the functions to be displayed on the **Settings** screen.

Set it up on the **Device > Display Settings > Settings Page Display** interface.

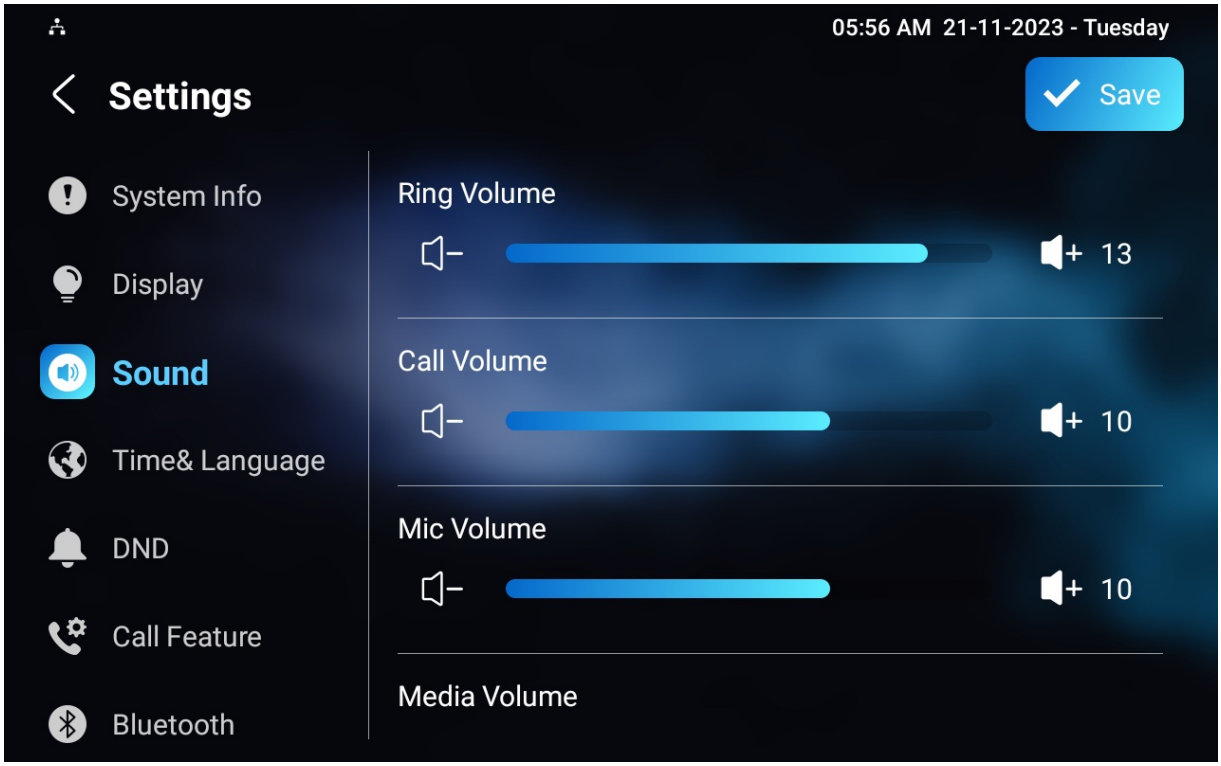


Sound and Volume

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

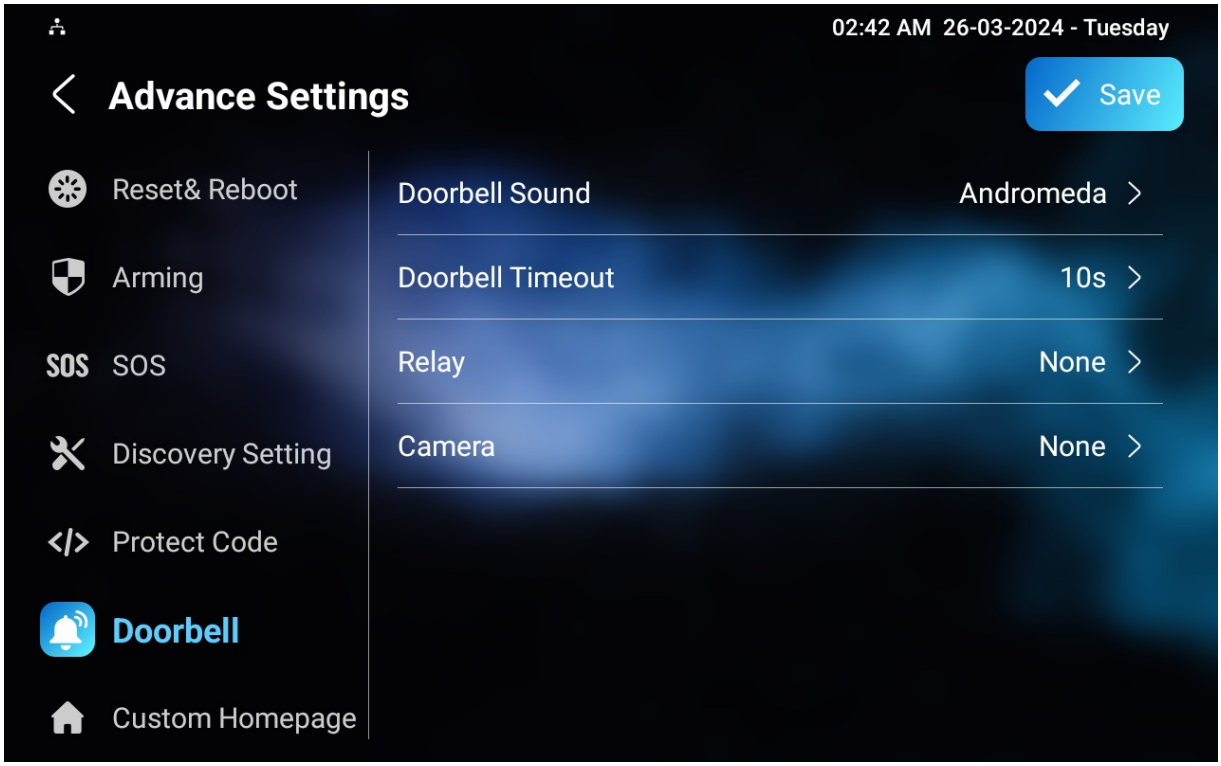
Configure Volume on the Device

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.

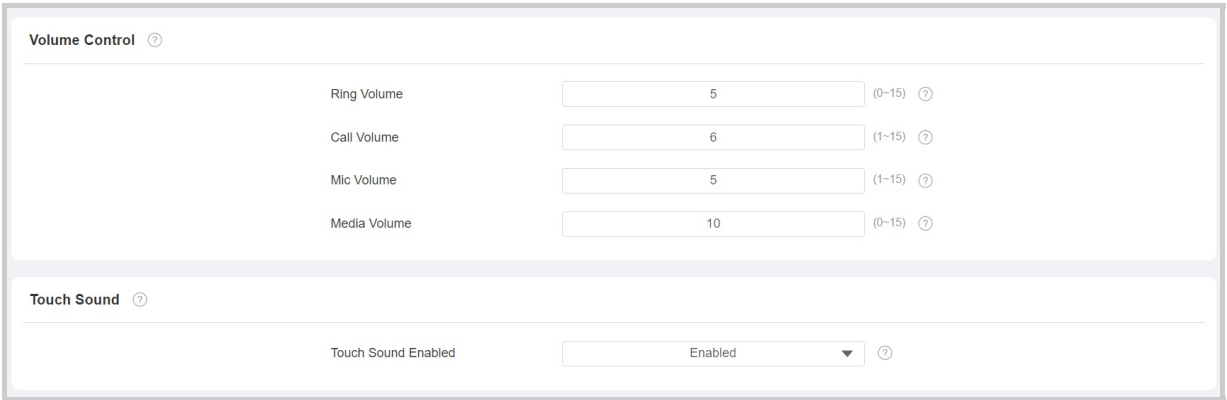
You can configure the doorbell sound and select the local relay to be triggered along with the doorbell on the **Settings > Advance Settings > Doorbell** screen.



- **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.

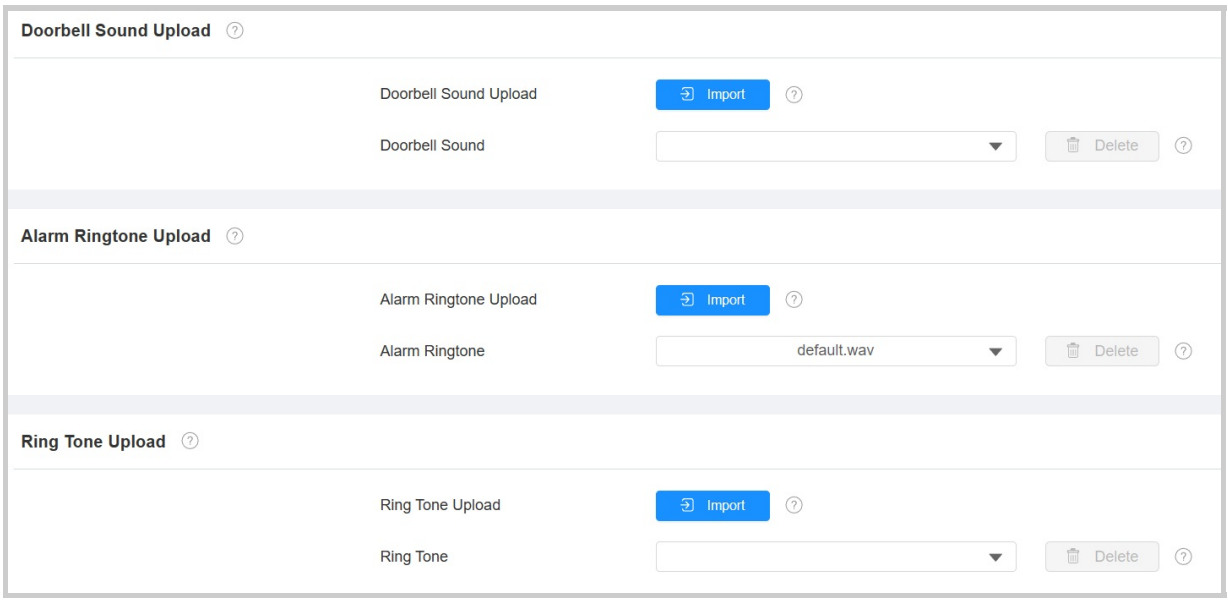
Configure Volume on the Web Interface

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



Upload Tones

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



Note

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

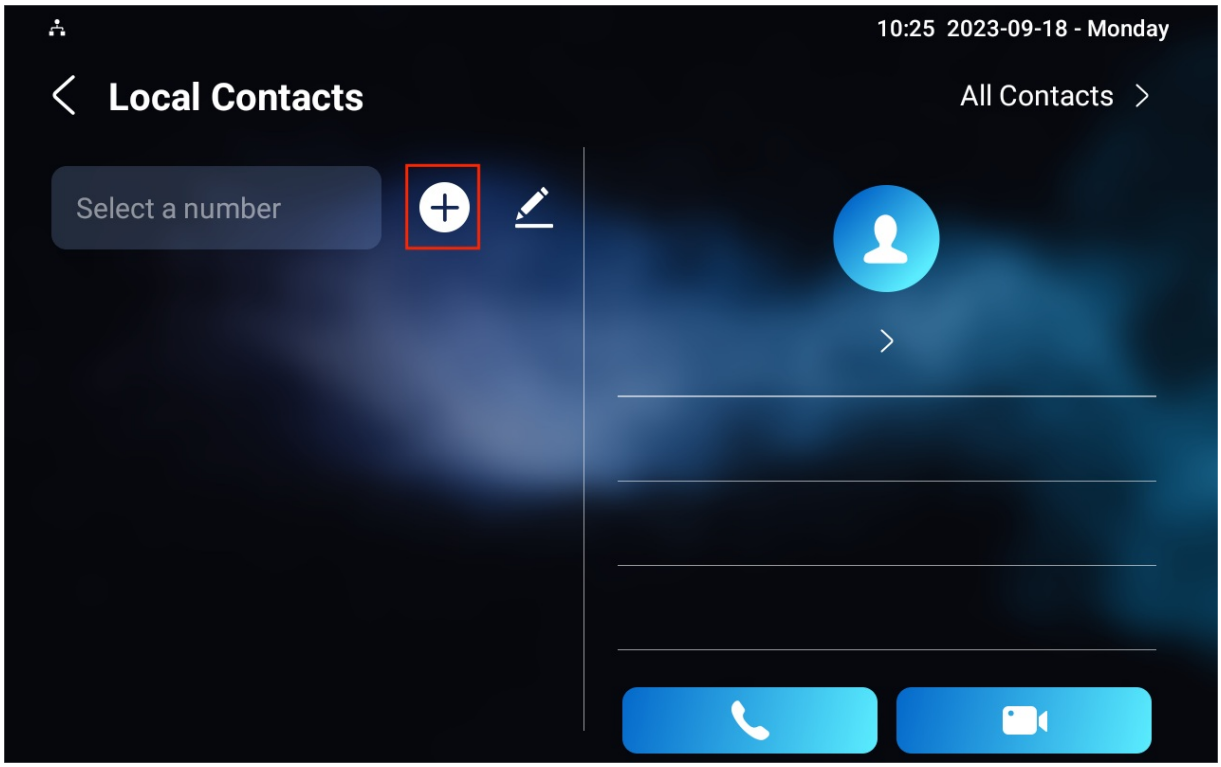
Contacts Configuration

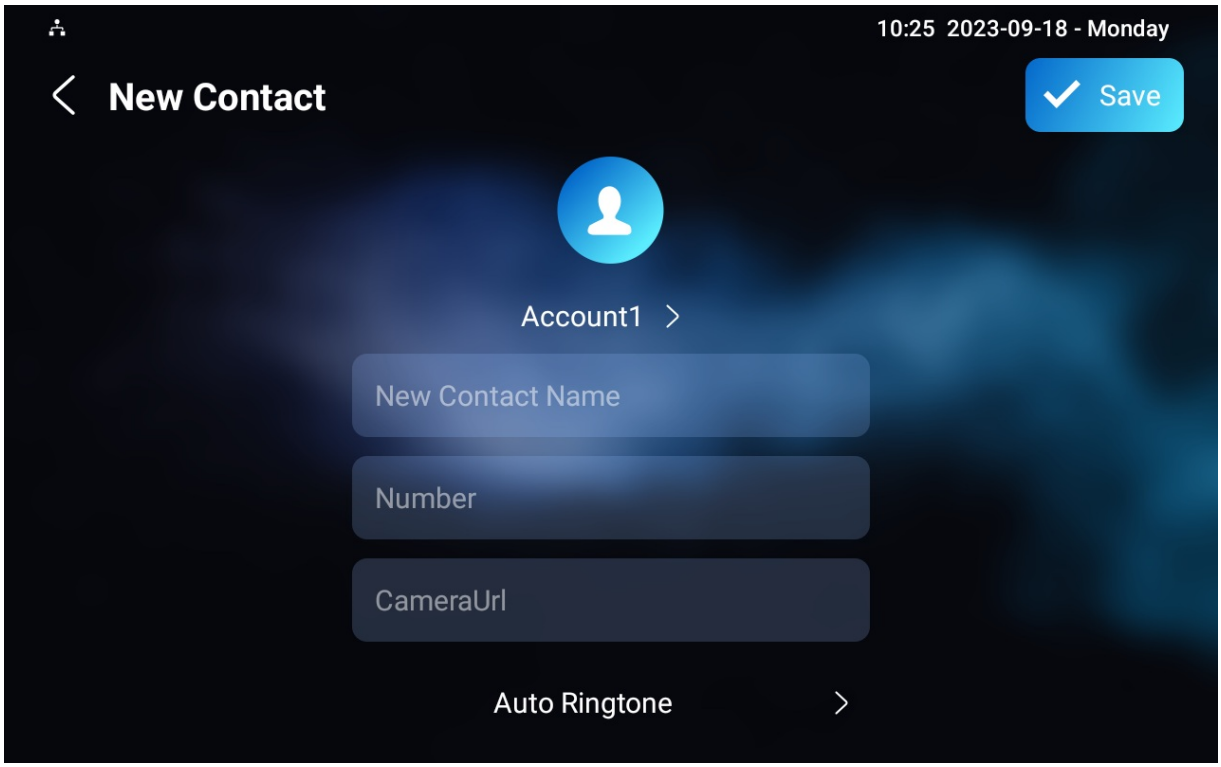
Contacts Configuration on the Device

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.



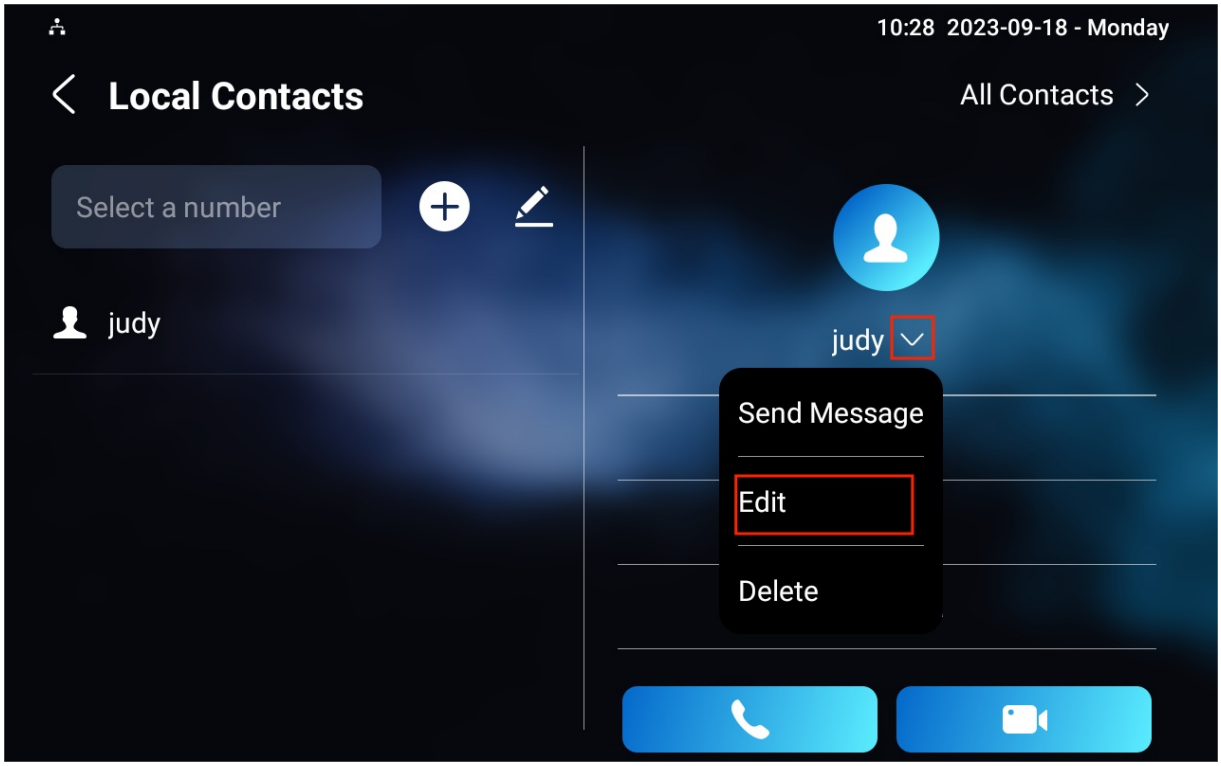


- **Account 1**: The account to make the call, Account 1 or Account 2.
- **New Contact Name**: Name the contact to distinguish it from others.
- **Number**: The IP or SIP number.
- **CameraUrl**: The RTSP URL for video preview.
- **Auto Ringtone**: The phone ringtone for incoming calls.

> **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

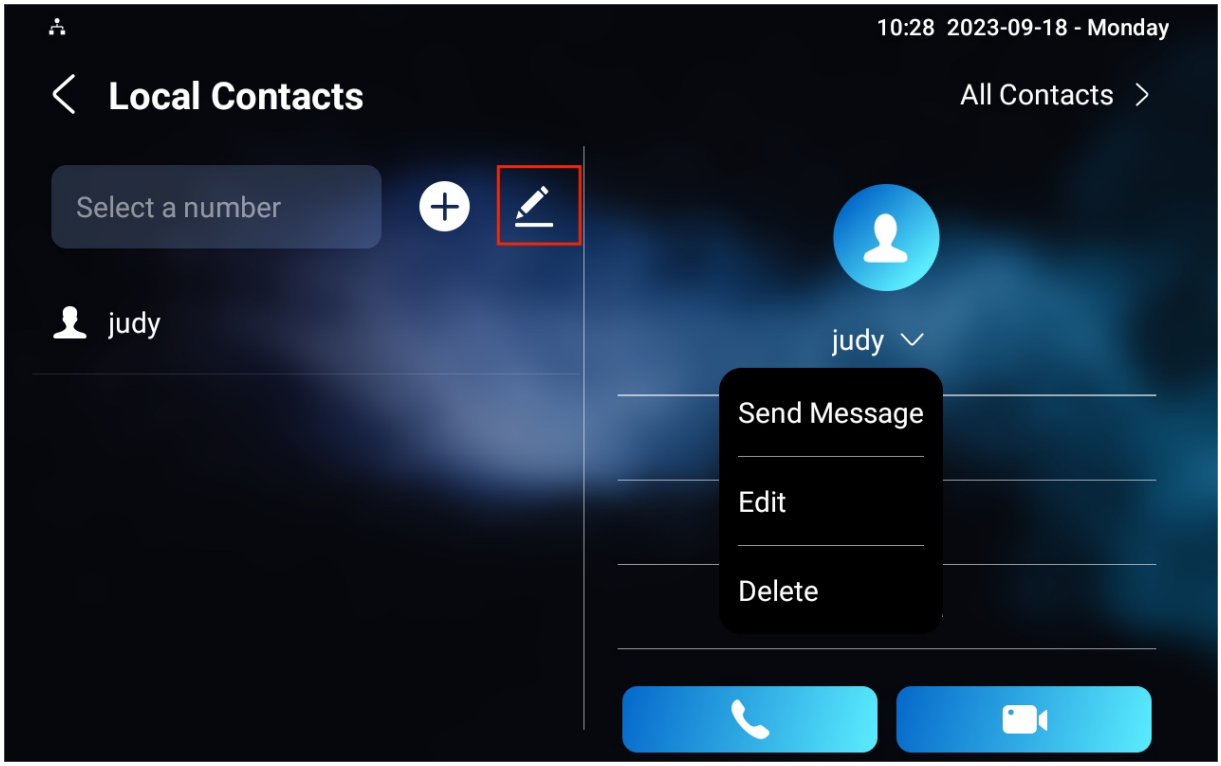
You can check and edit the existing contacts in the contact list. Choose one and click **Edit** to modify.

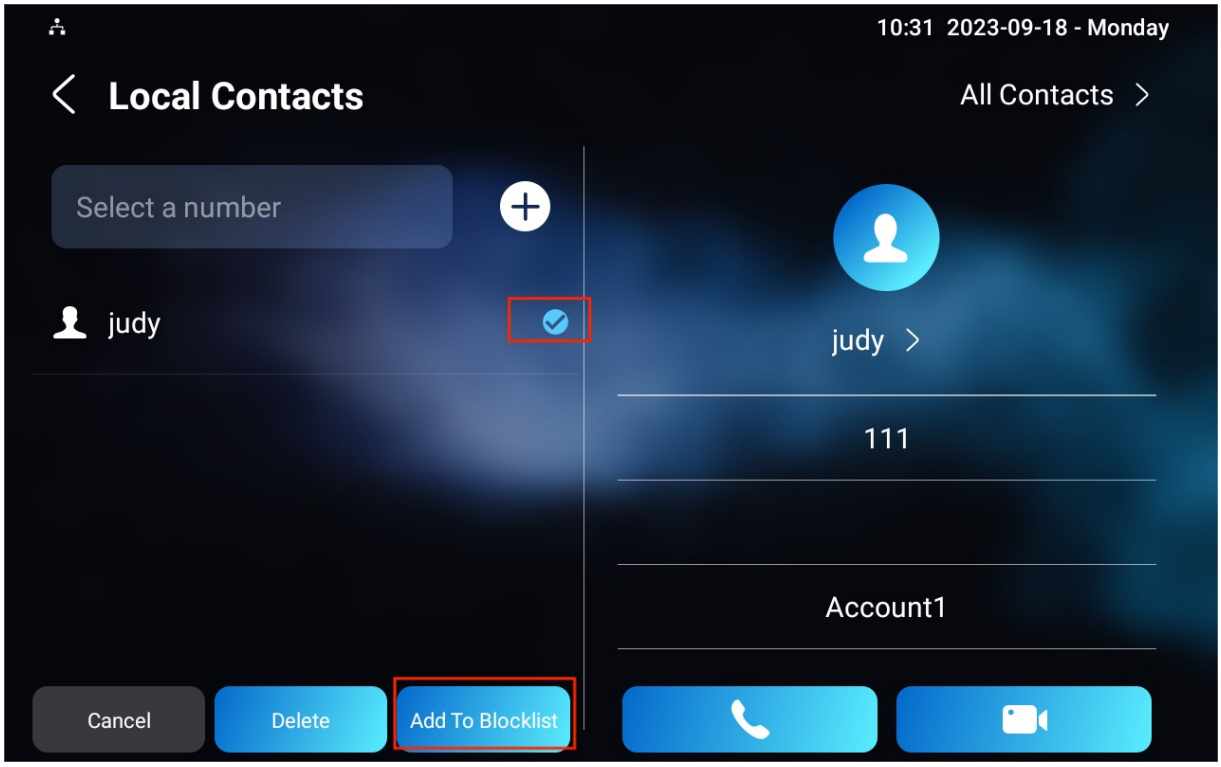


Block List Setting on the Device

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**.





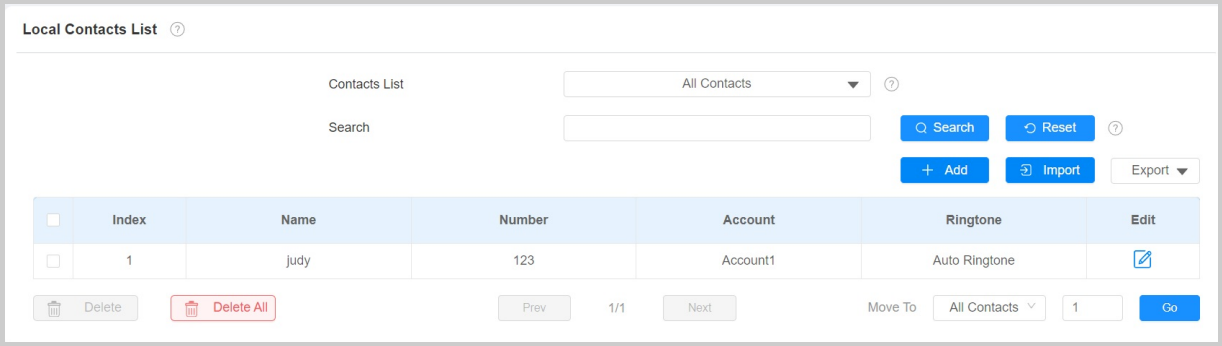
Note

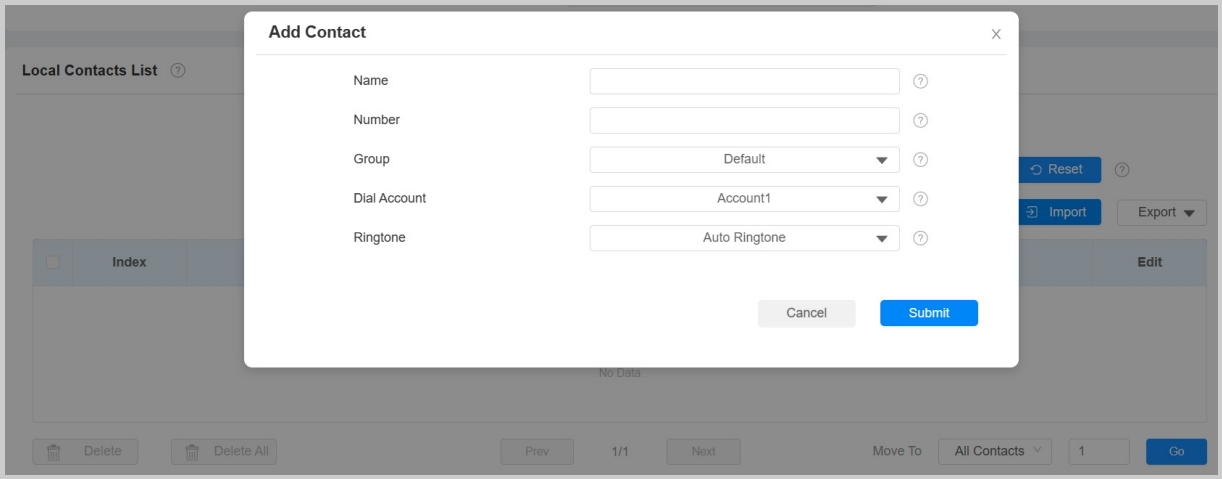
You can delete contacts regardless of whether it is in Blocklist.

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**.





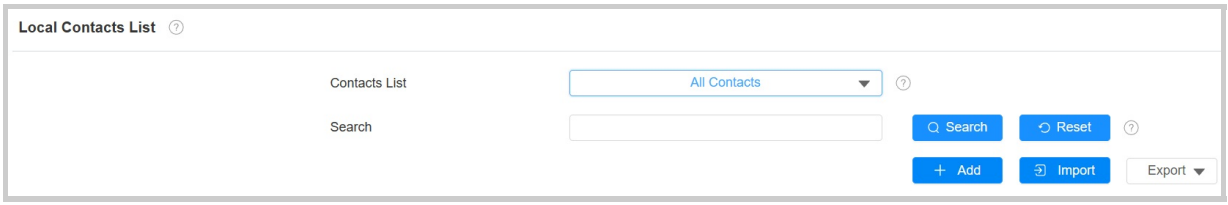
- **Contacts List**: **All Contacts** displays all the contacts in the contact list. **Blocklist** displays the contacts in the blocklist.
- **Search**: Search a contact by its name or number.
- **Name**: The contact's name to distinguish it from others.
- **Number**: The SIP or IP number of the contact.
- **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

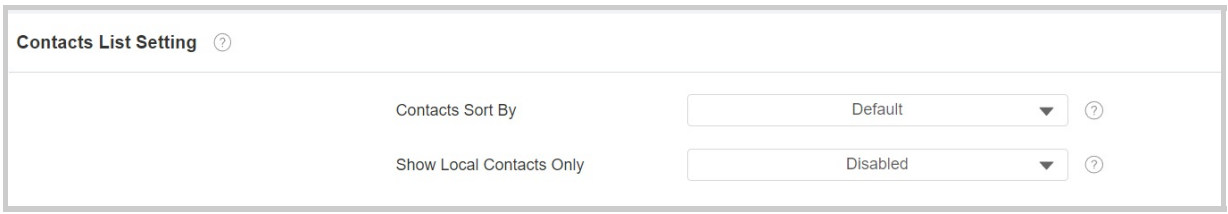
You can import and export contacts in batch. The file should be in .xml or .csv format.

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.

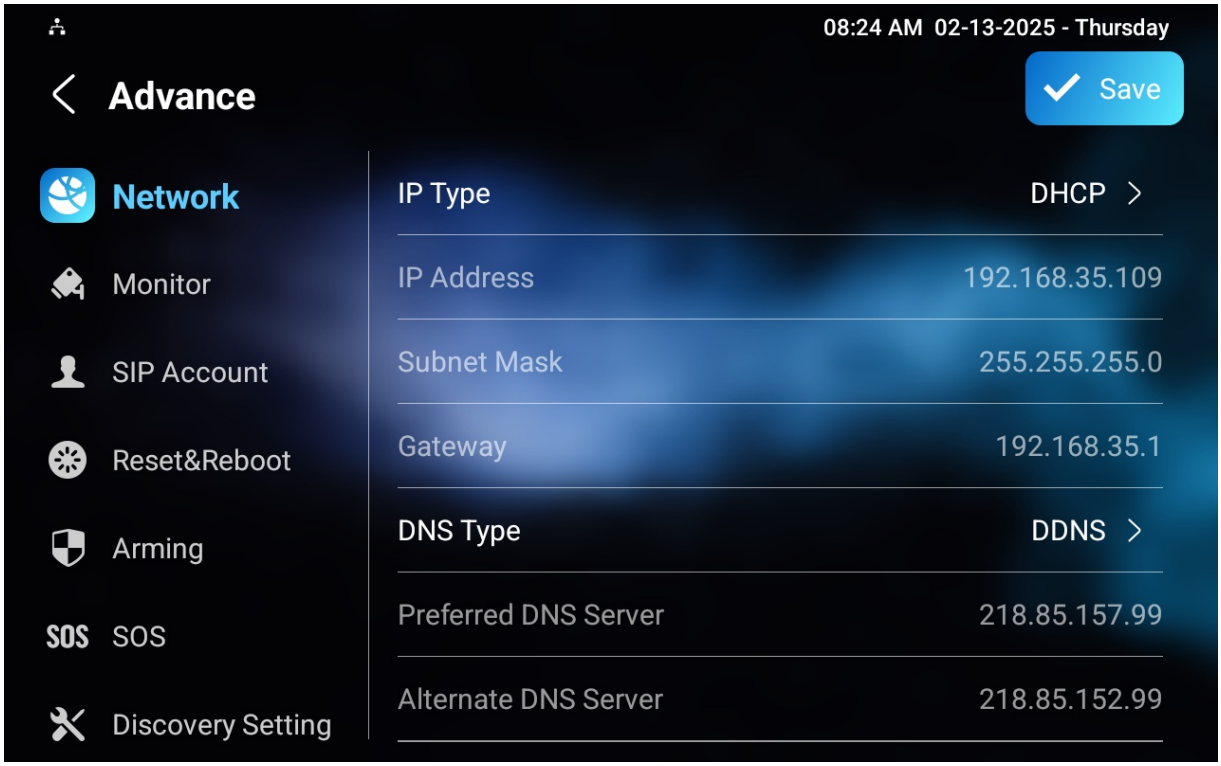
Network Setting & Other Connection

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.

On the Device

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

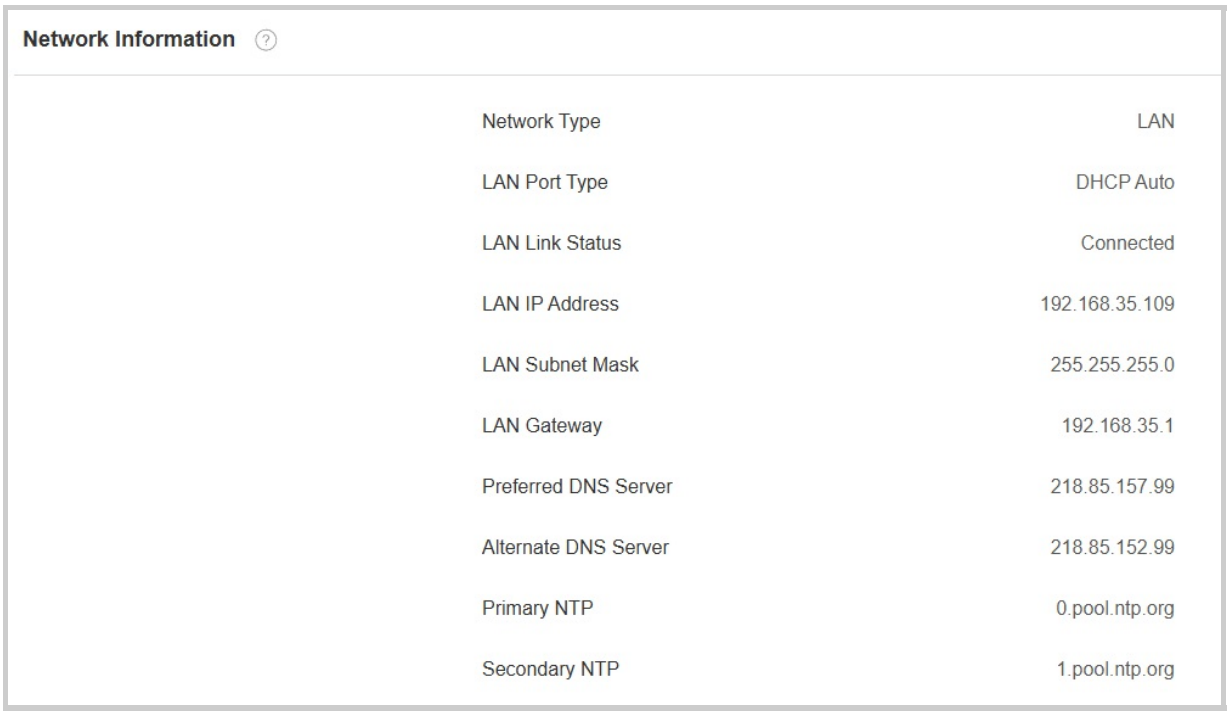
- **Gateway**: The gateway should be set up according to the IP address.
- **DNS Type**: Domain Name Server(DNS) type.
    - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
    - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred & Alternate DNS Server**: The preferred and 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.
- **Preferred Network**: Specify the preferred network connection, WLAN or Ethernet. It is Ethernet by default. When Ethernet is unavailable, the device will automatically switch to a WLAN connection and vice versa.

Note

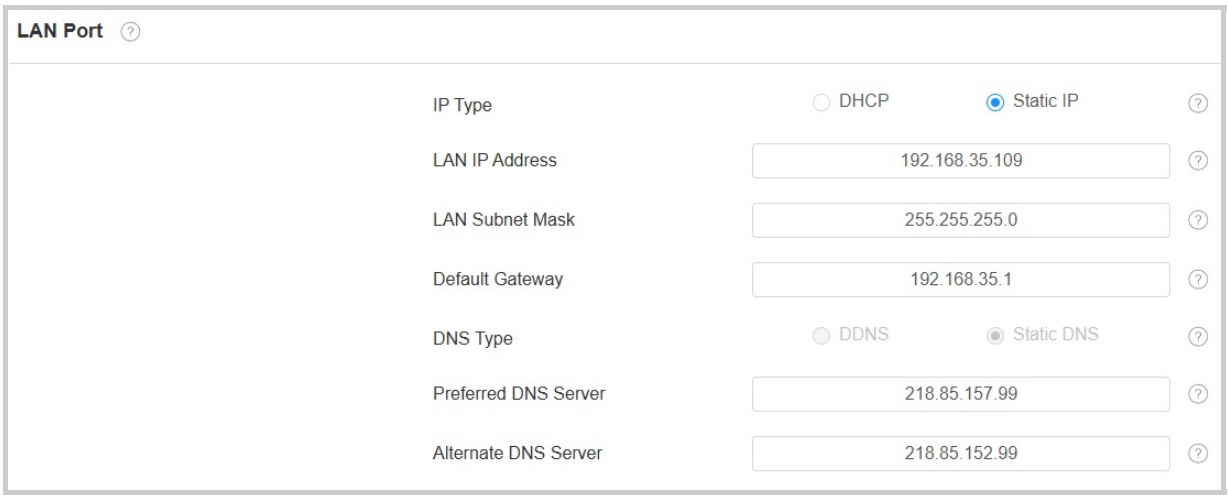
- You can press System Info, and then press Network on the Settings screen to check device network status.
- The default code to enter advanced settings is 123456.

On the Web Interface

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



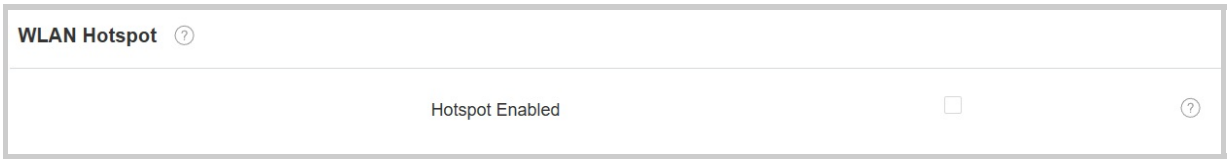
Check and configure the network connection on the device web **Network > Basic > LAN Port** interface.



- **IP Type**:
  - **DHCP** mode will enable the indoor monitor to be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
  - **Static IP** allows you to enter the IP address, subnet mask, default gateway, and DNS address manually according to the actual network environment.
- **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.

- **DNS Type**: Domain Name Server(DNS) type.
  - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
  - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred/Alternate DNS Server**: The preferred and 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.

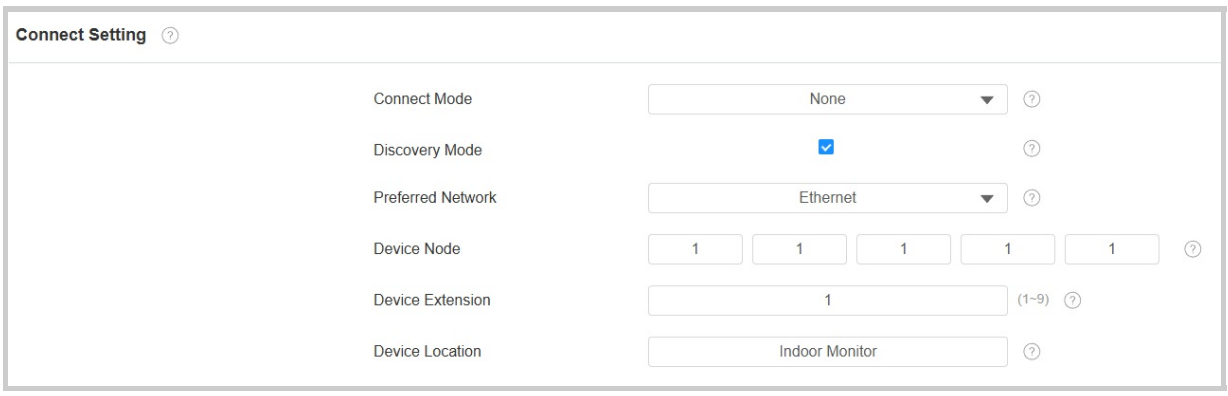
To enable the WLAN hotspot, go to the **Network > Advanced > WLAN Hotspot** interface.



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.

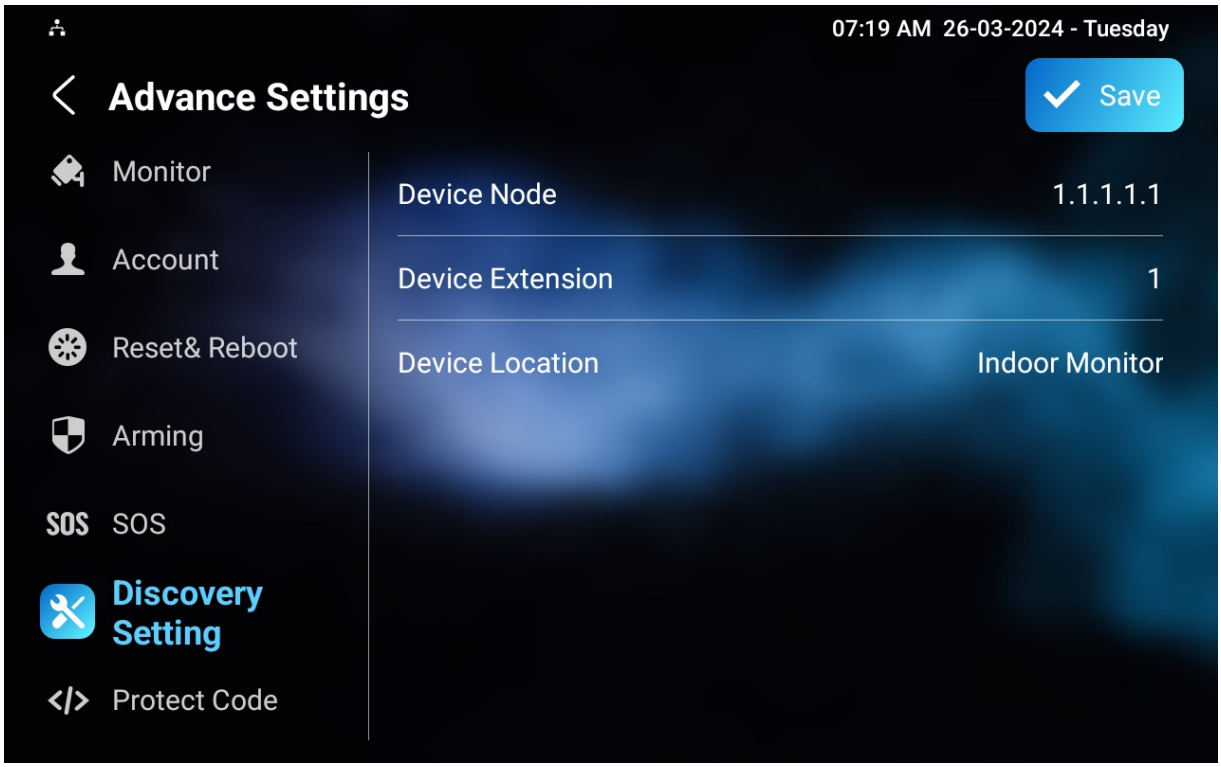
Deploy the device in the network on the web **Network > Advanced > Connect Setting** interface.



- **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**. You can also select it manually. **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.
- **Preferred Network**: Specify the preferred network connection, WLAN or Ethernet. It is Ethernet by default. When Ethernet is unavailable, the device will automatically switch to a WLAN connection and vice versa.
- **Device Node**: Specify the device address by entering device location info from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: The device extension number for the device you installed.
- **Device Location**: The location in which the device is installed and used.

You can also set up the device node, extension number, and location on the **Settings > Advance Settings > Discovery Setting** screen.

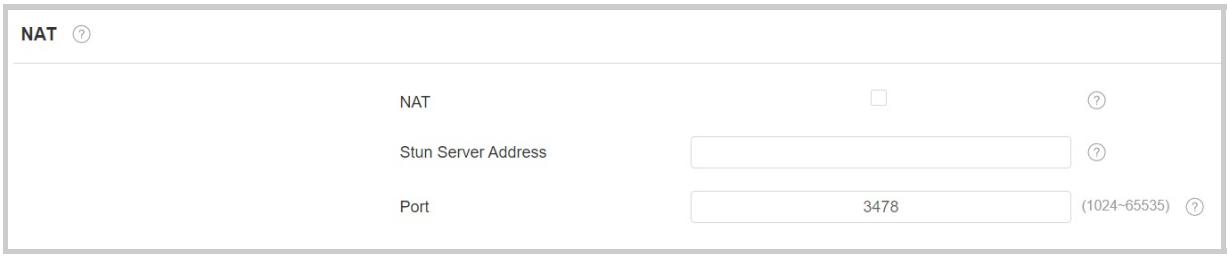


Device NAT Setting

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

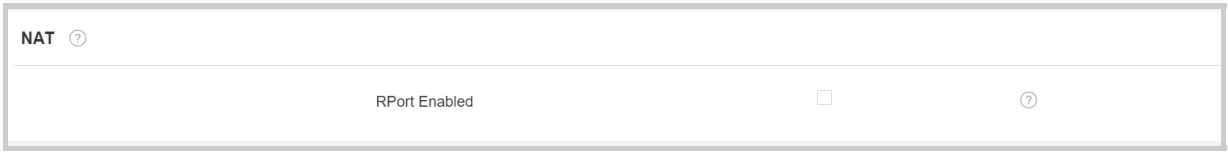
To register SIP accounts on third-party servers in a Wide Area Network(WAN), you need to enable the RPort feature on the intercom devices to establish a stable connection.

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



- **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 WAN for the SIP account registration.

Device Web HTTP Setting

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

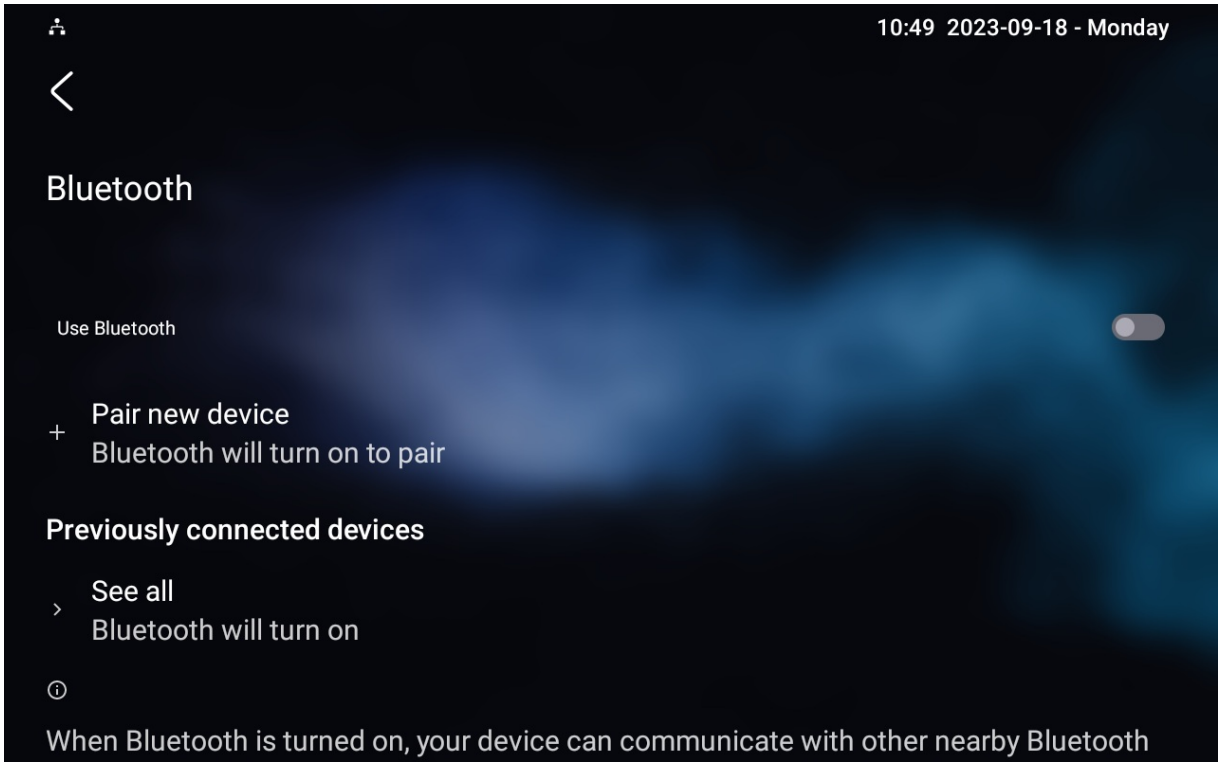
To set it up, go to the **Network > Advanced > Web Server** interface.

Device Bluetooth Setting

Device Bluetooth Pairing

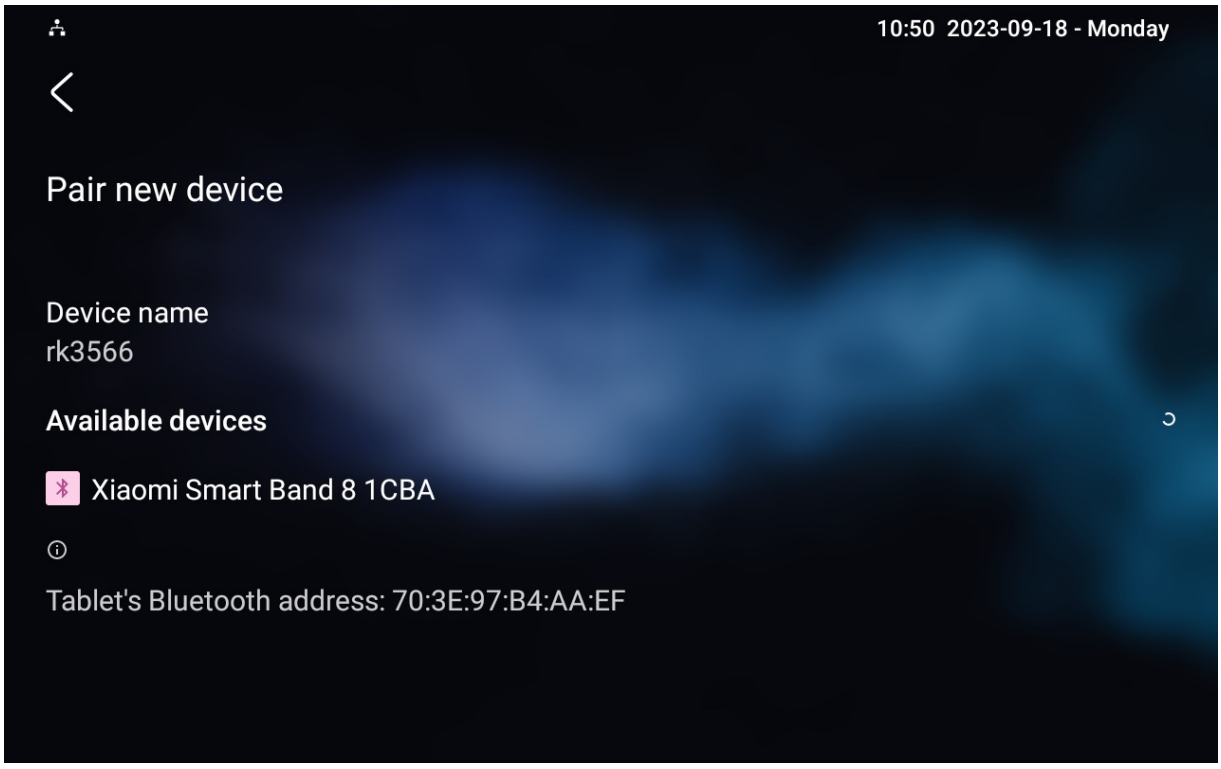
You need to enable the Bluetooth feature on the device before you can pair the indoor monitor with other Bluetooth-featured devices.

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



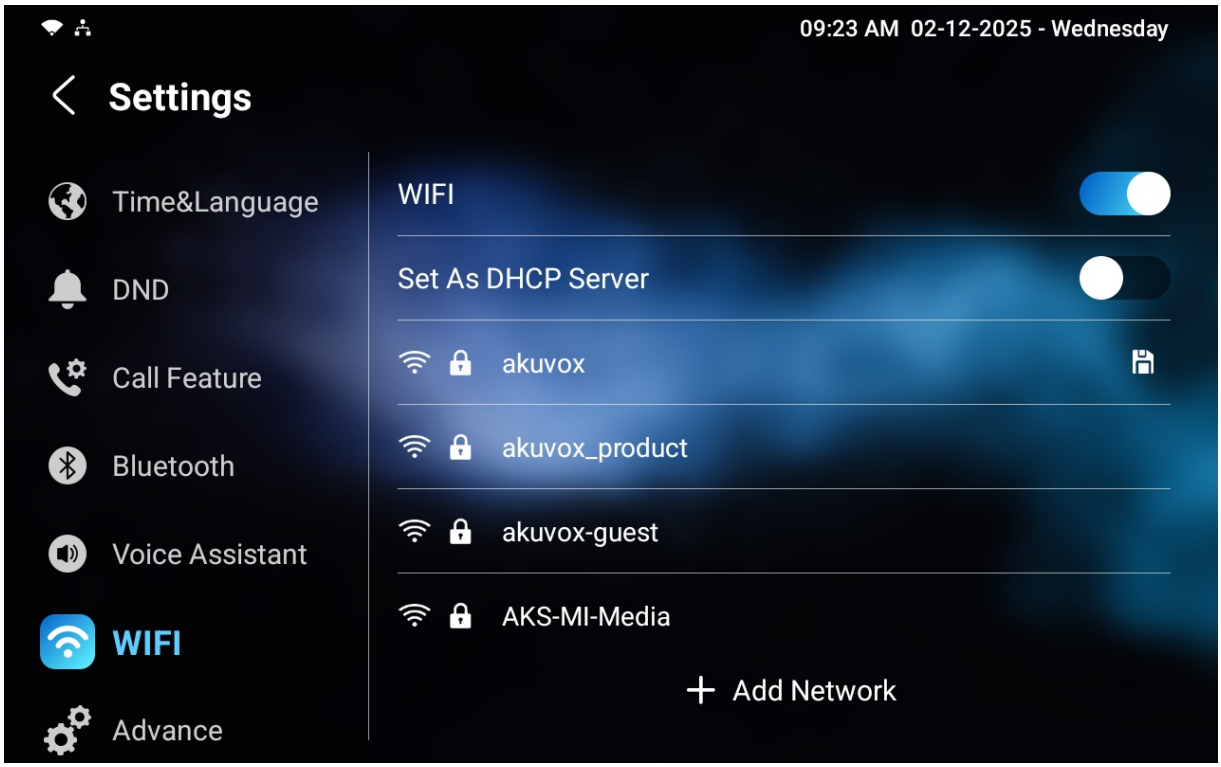
Device Bluetooth Data Transmission

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

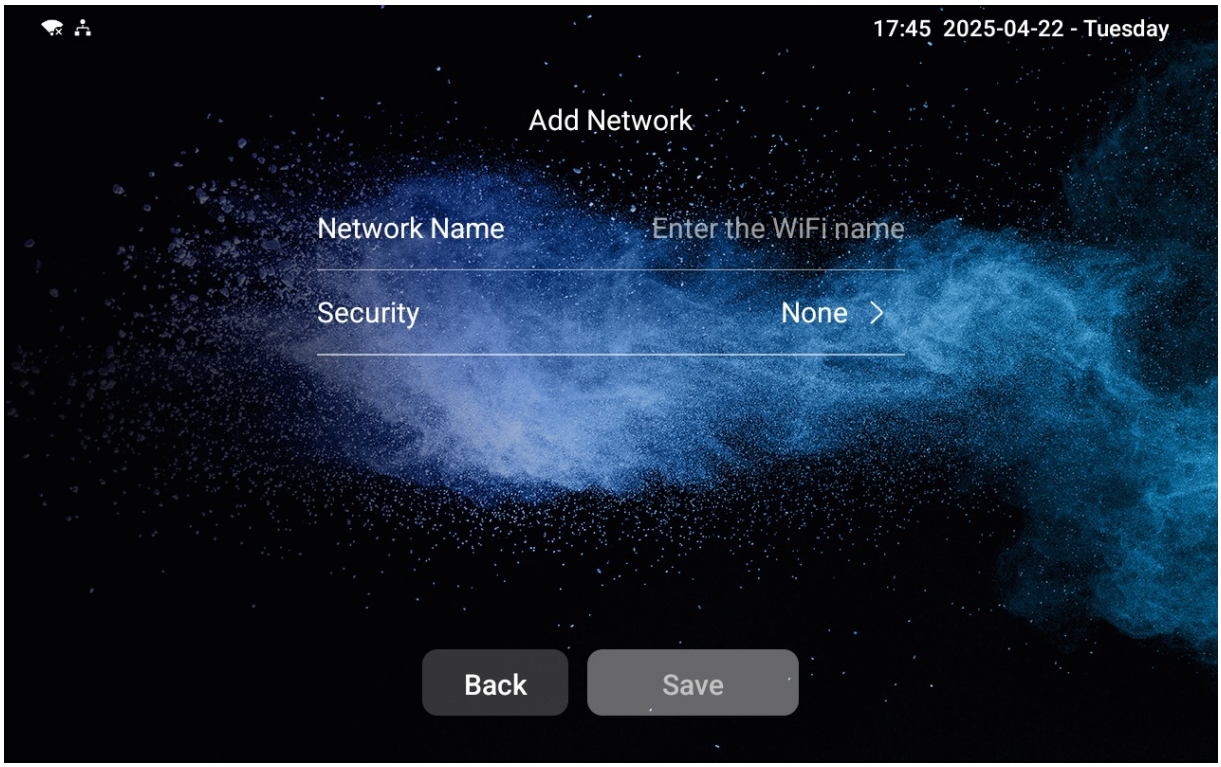


Device Wi-Fi Setting

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



- **Set As DHCP Server**: Use Wi-Fi as the DHCP server.
- **Add Network**: Tap to add a Wi-Fi manually.
    - **Security**: Select the network encryption type and enter the password for connection. The default is **None**.


17:45 2025-04-22 - Tuesday
Add Network
Network Name
Enter the WiFi name
Security
None
Back
Save

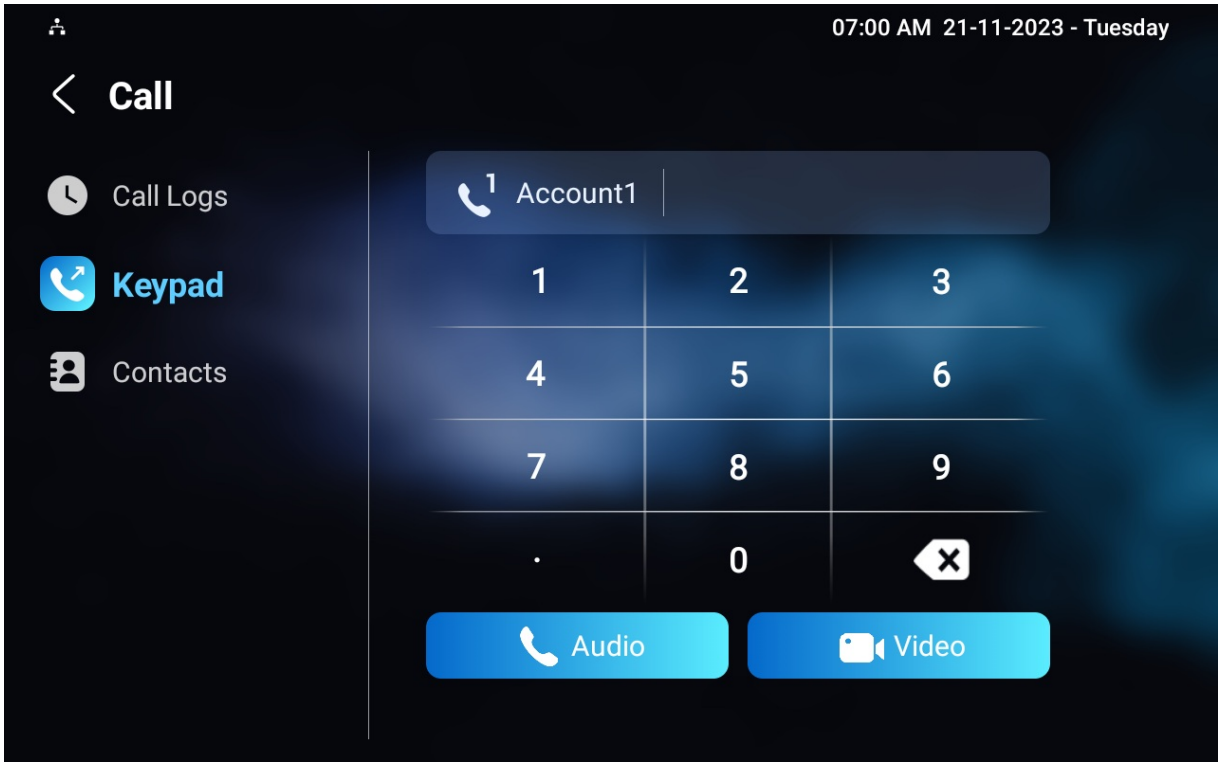
Intercom Call Configuration

IP Call & IP Call Configuration

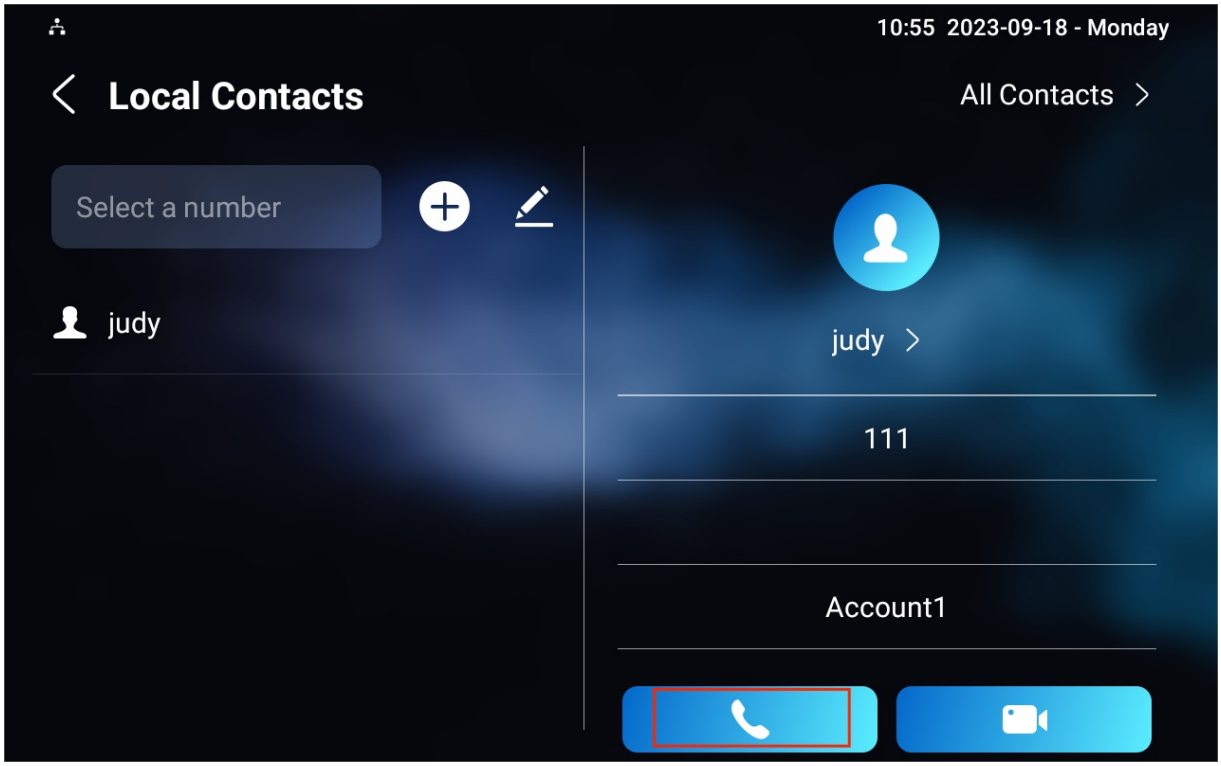
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

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.

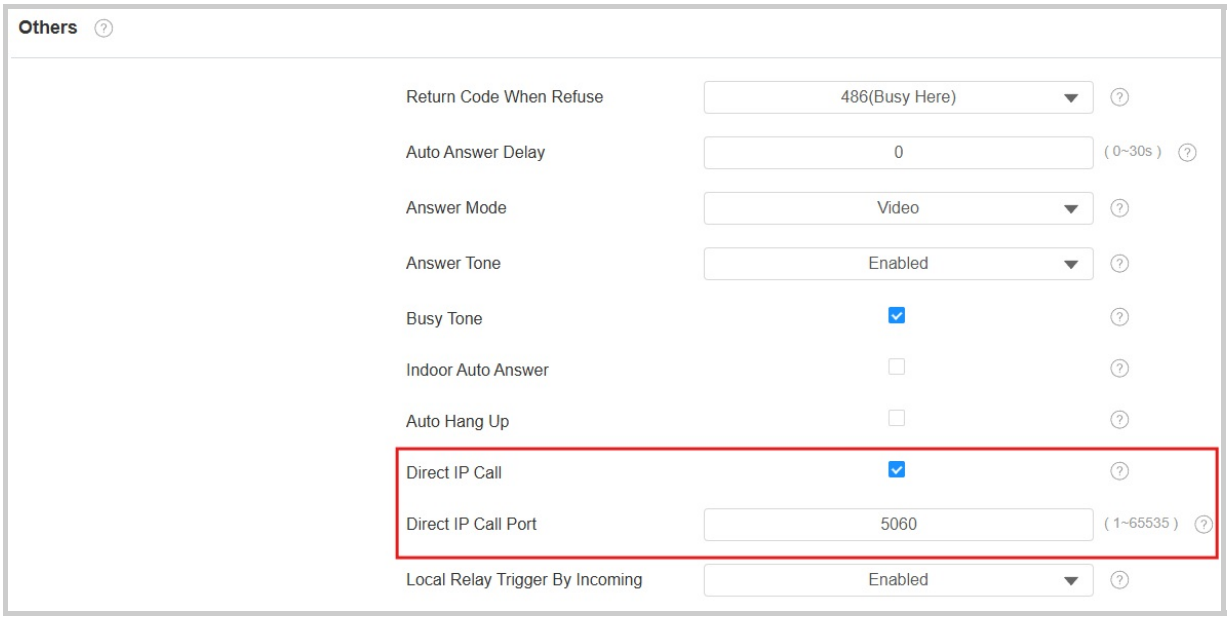


In addition, you can also make IP calls on the **Contacts > Local Contacts** screen.



IP Call Configuration

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



- **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.

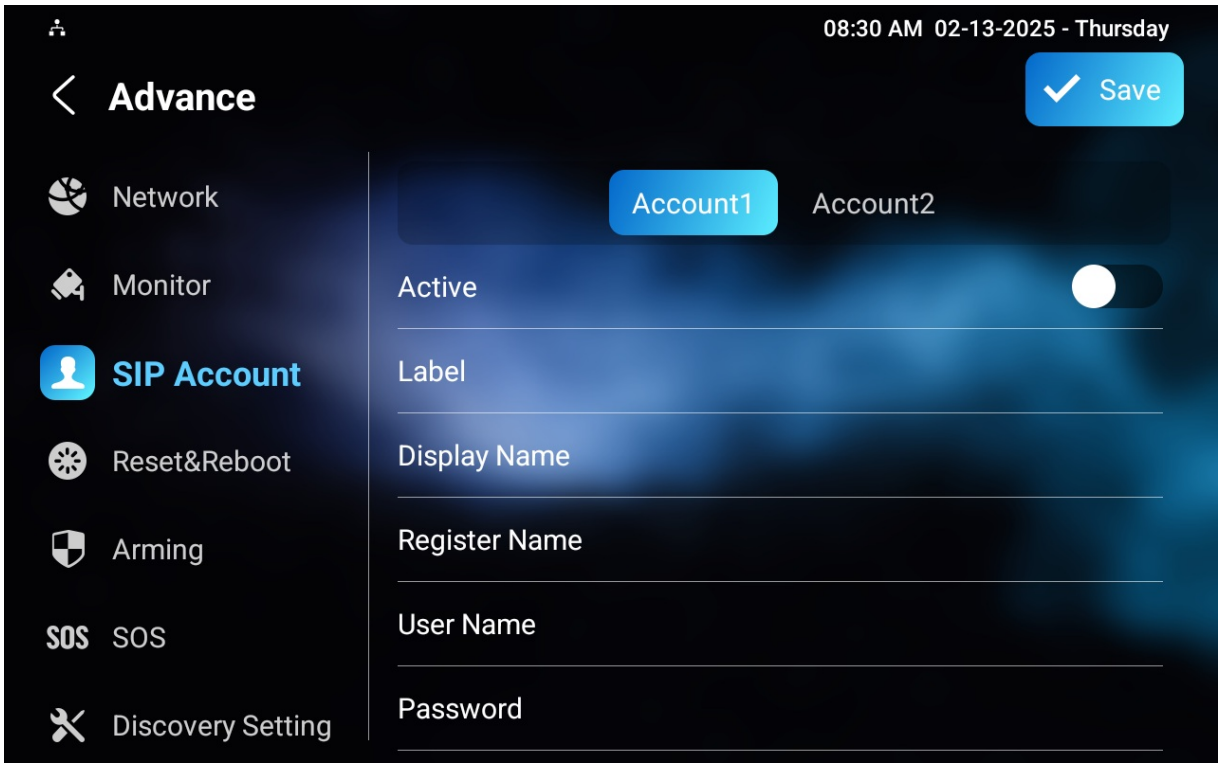
SIP Account Registration

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.

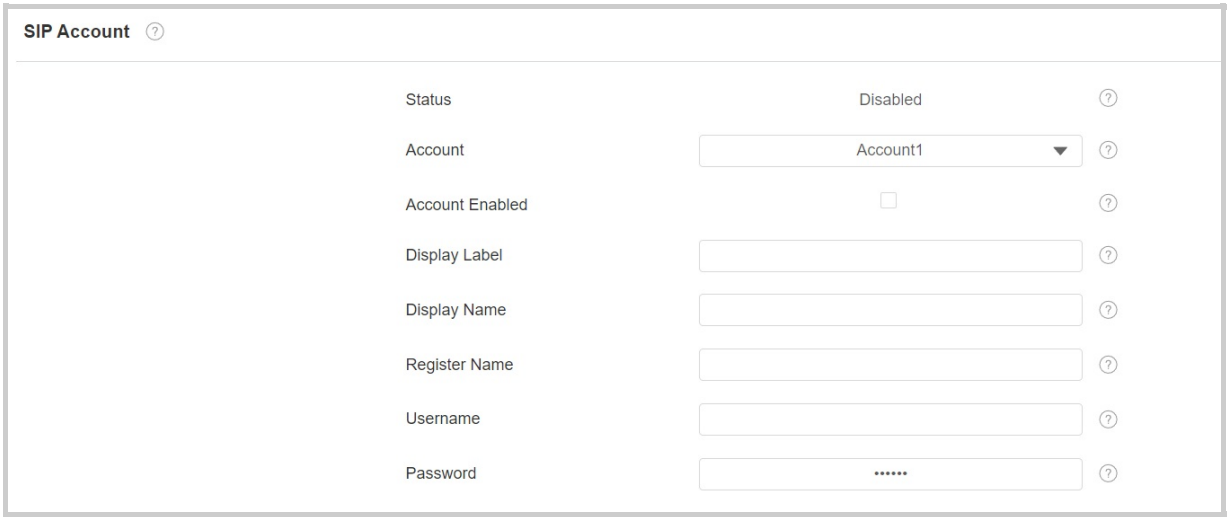
Click here to view the SIP account registration example.

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

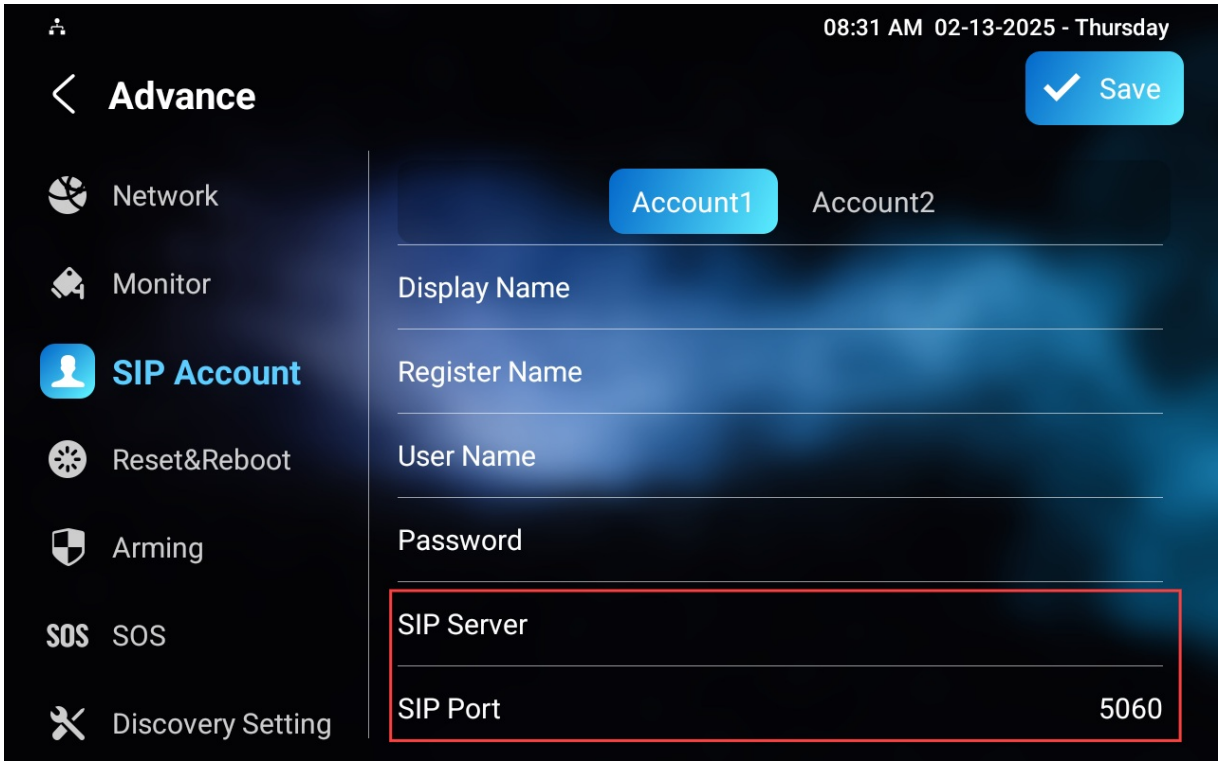


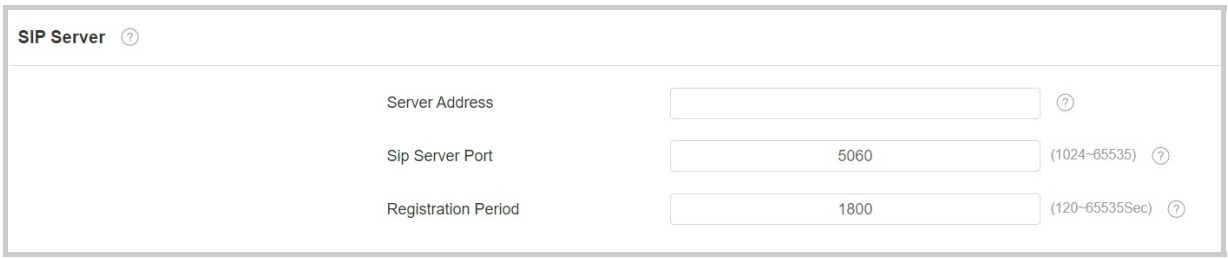
- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same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



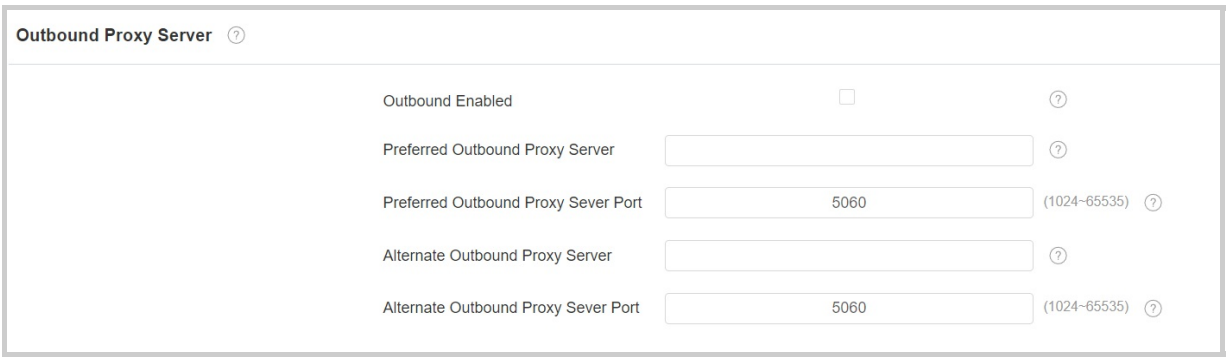


- **Server Address**: Enter the server's IP address or its domain name.
- **Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails within this specified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

Outbound Proxy Server

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

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

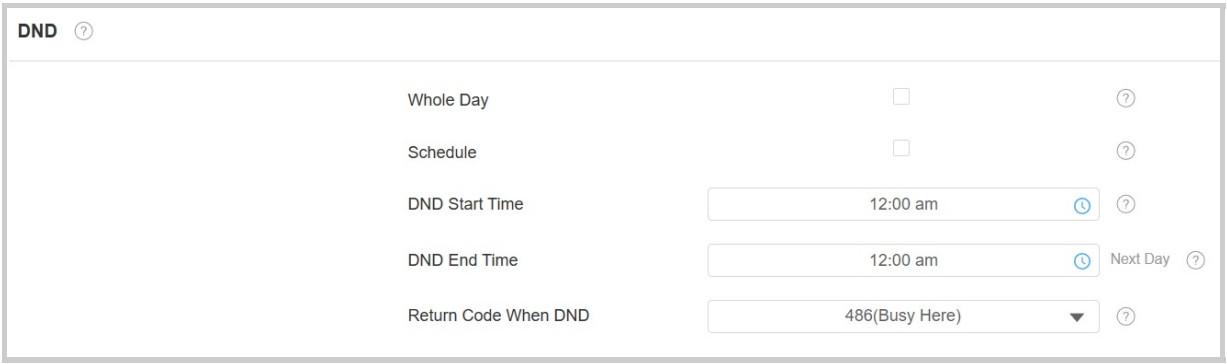


- **Preferred Outbound Proxy Server**: Enter the SIP proxy IP address.
- **Preferred Outbound Proxy Server Port**: Set the port for establishing a call session via the outbound proxy server.
- **Alternate Outbound Proxy Server**: Enter the SIP proxy IP address to be used when the main proxy malfunctions.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

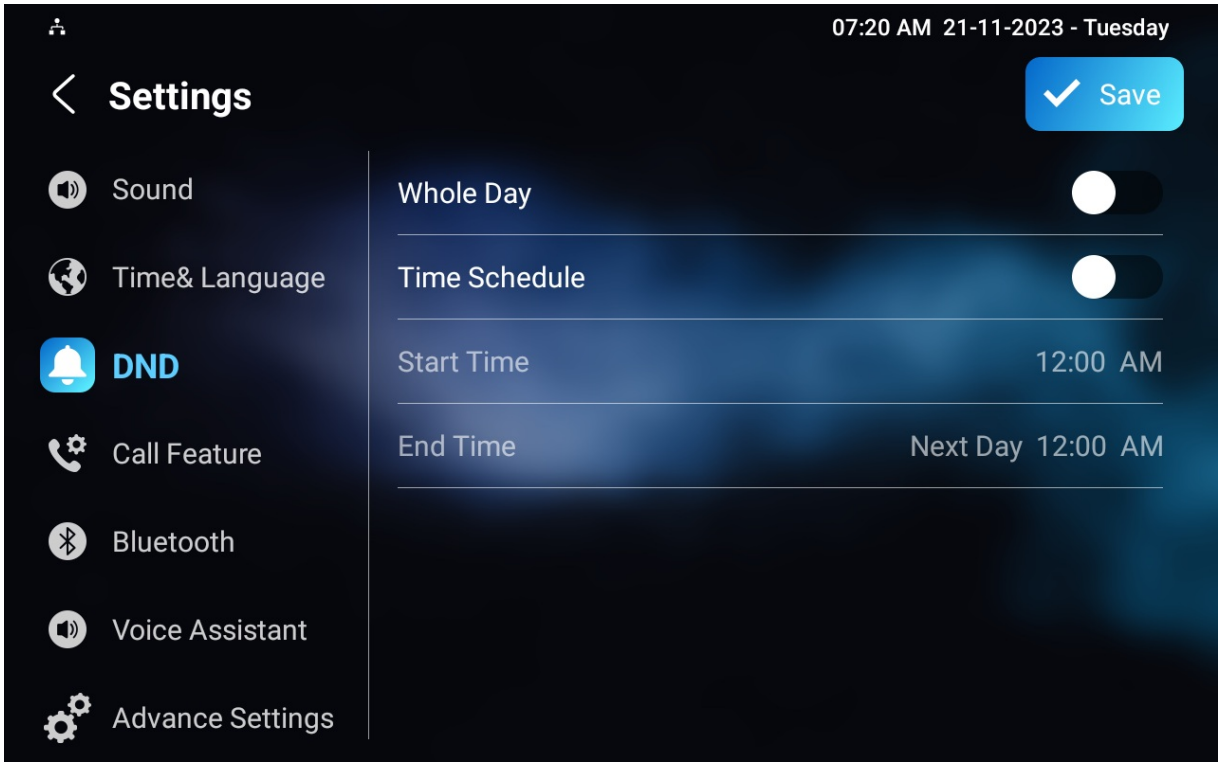
The Do Not Disturb(**DND**) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

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**.

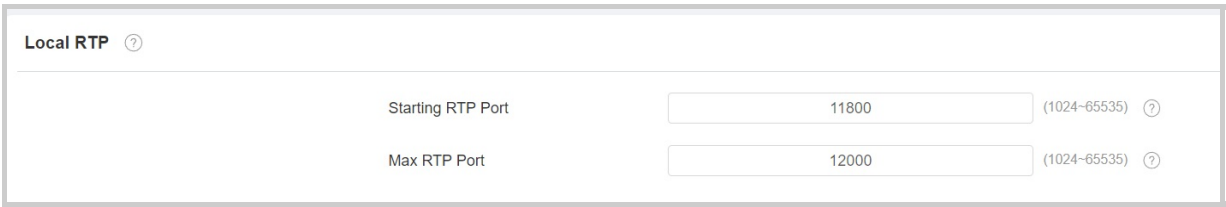


Device Local RTP Configuration

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.

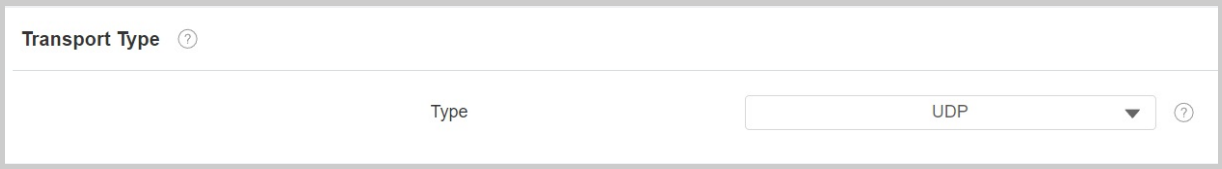


- **Starting RTP Port**: The port value to establish the start point for the exclusive data transmission range.
- **Max RTP port**: The port value to establish the endpoint for the exclusive data transmission range.

Data Transmission Type

Akuvox intercom devices support 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.

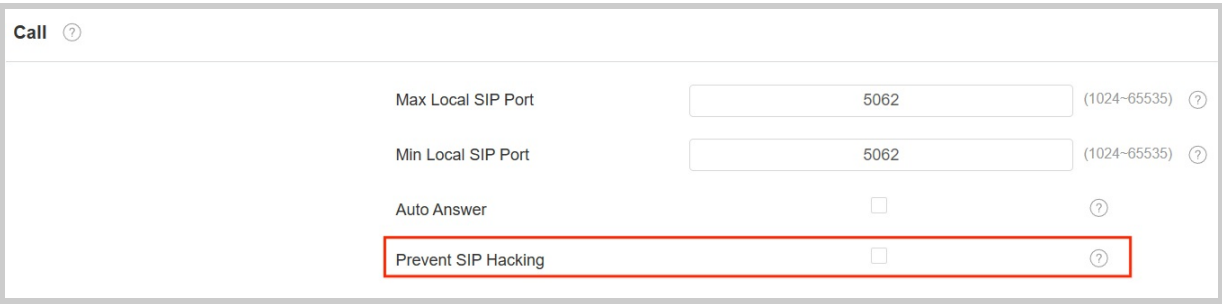


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced 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.



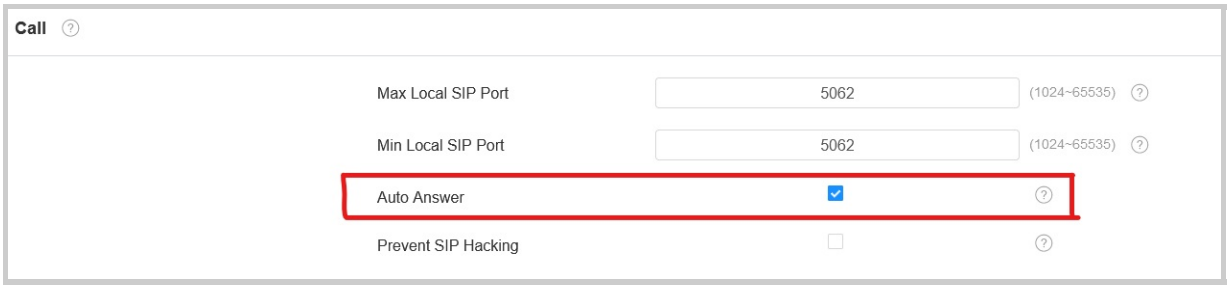
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Setting

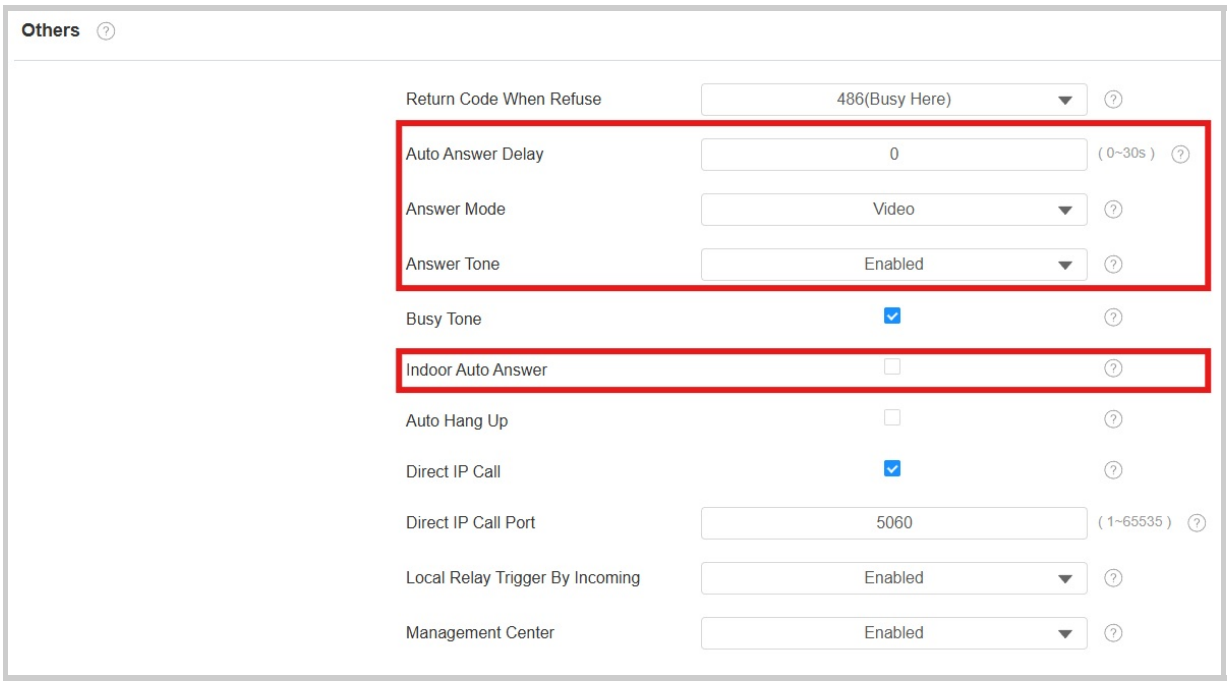
Auto-answer Configuration

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.



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



- **Auto Answer Delay:** Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the 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.

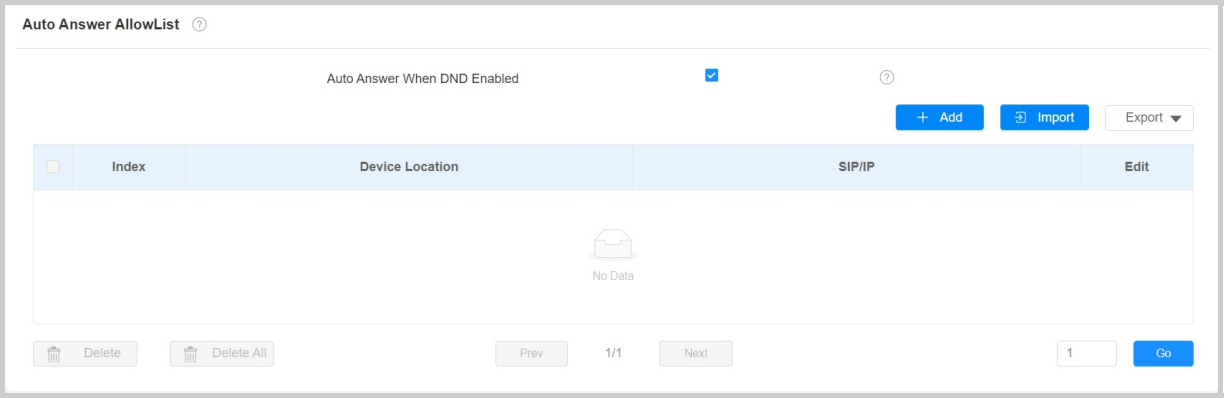
Other Options:

- **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 Relay Trigger By Incoming**: Set whether to trigger the local relay by incoming calls.
- **Management Center**: Decide whether to generate the contact labeled Management Center.
    - When the device is deployed on the SmartPlus Cloud, the cloud system will issue the SmartPlus Property Manager App and the guard phone R49 as a contact labeled Management Center. When this function is disabled, the PM App and guard phone will be displayed as contacts separately.
    - When the device is deployed on the SDMC, SDMC is shown as Management Center on the device screen. When the function is disabled, no contacts will be displayed as Management Center.

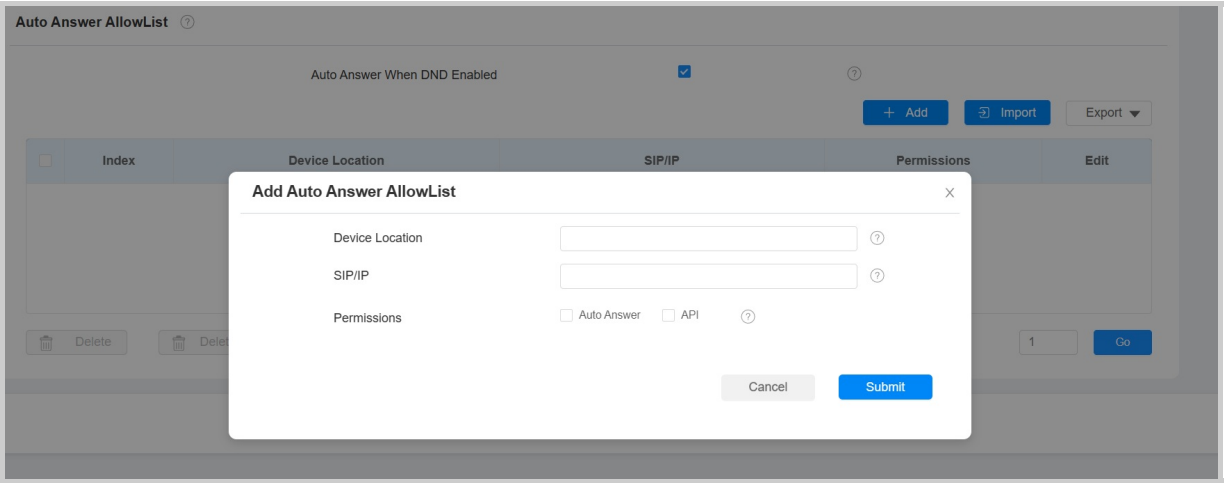
Auto-answer Allow List Setting

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.

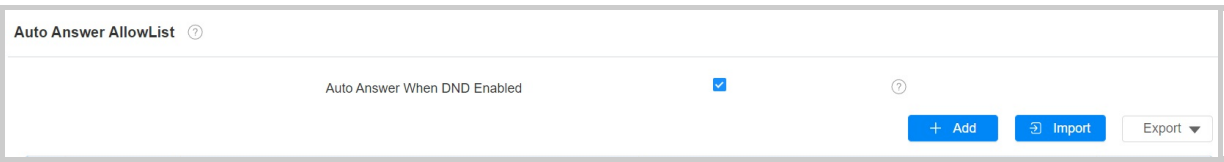


- **Auto Answer When DND Enabled**: Indicate that the auto-answer feature is effective when DND is turned on.



- **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.



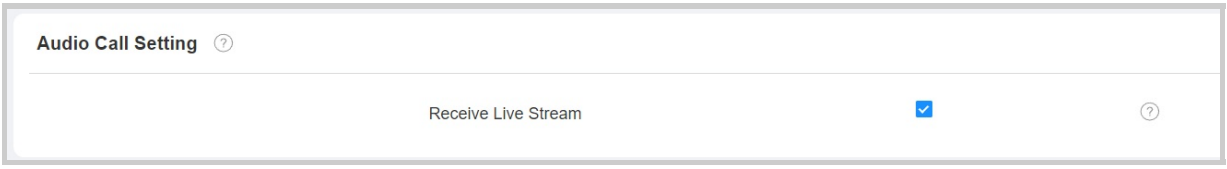
Note

- 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:

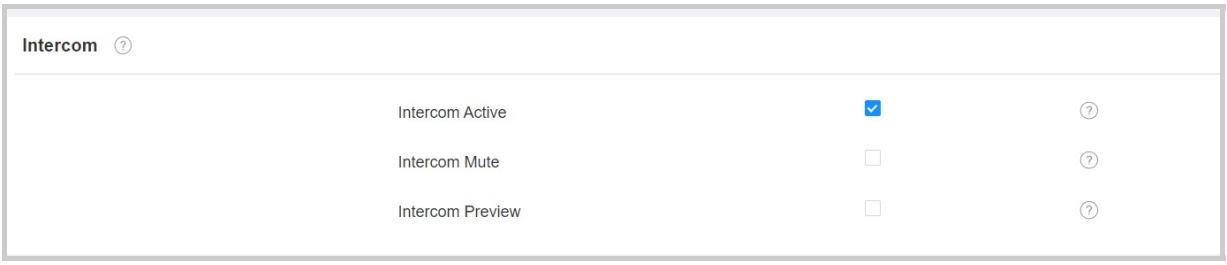
- If an incoming call is received on an audio basis on the device, the user can still see the video image of the calling party, while the calling party cannot see the user's. Thus, it protects the user's privacy.
- If an incoming call is received on a video basis on the device, the user and the calling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

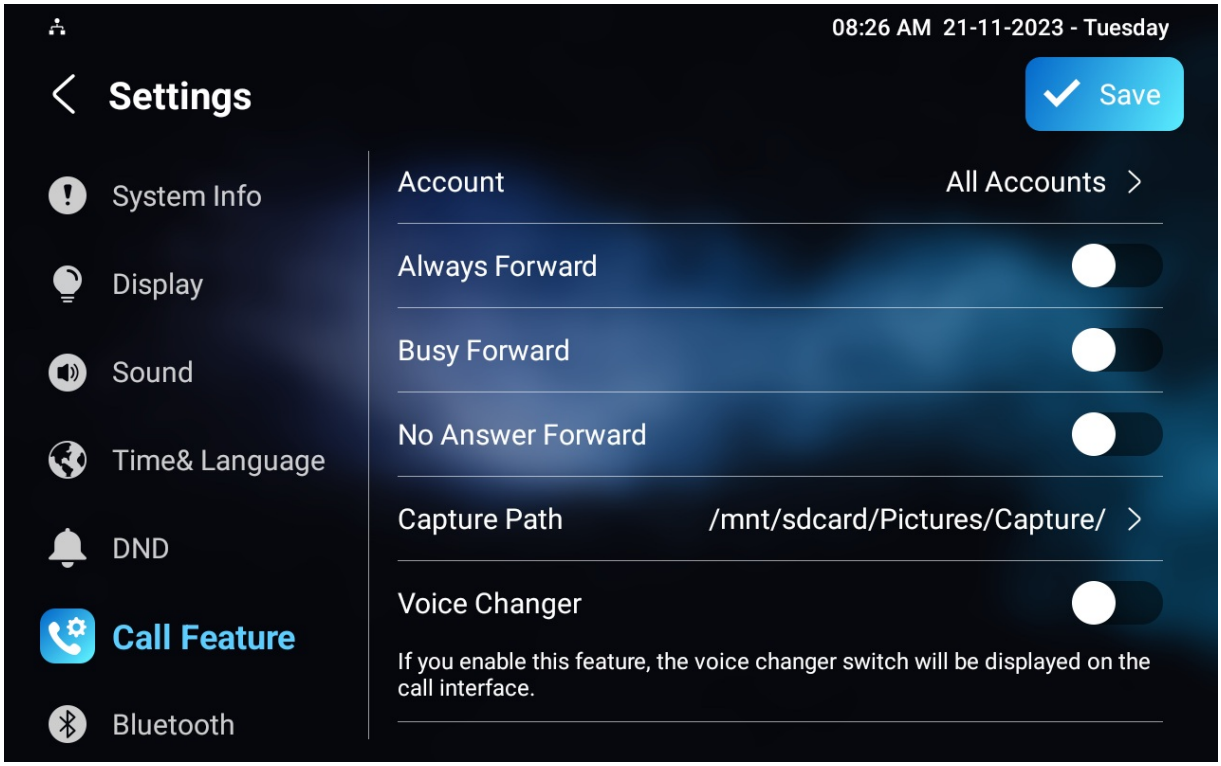


- **Intercom Active**: It is enabled by default.
- **Intercom Mute**: Mute the voice from the callee side.
- **Intercom Preview**: Enable the incoming call preview. If it is enabled, the group call is not available.

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.

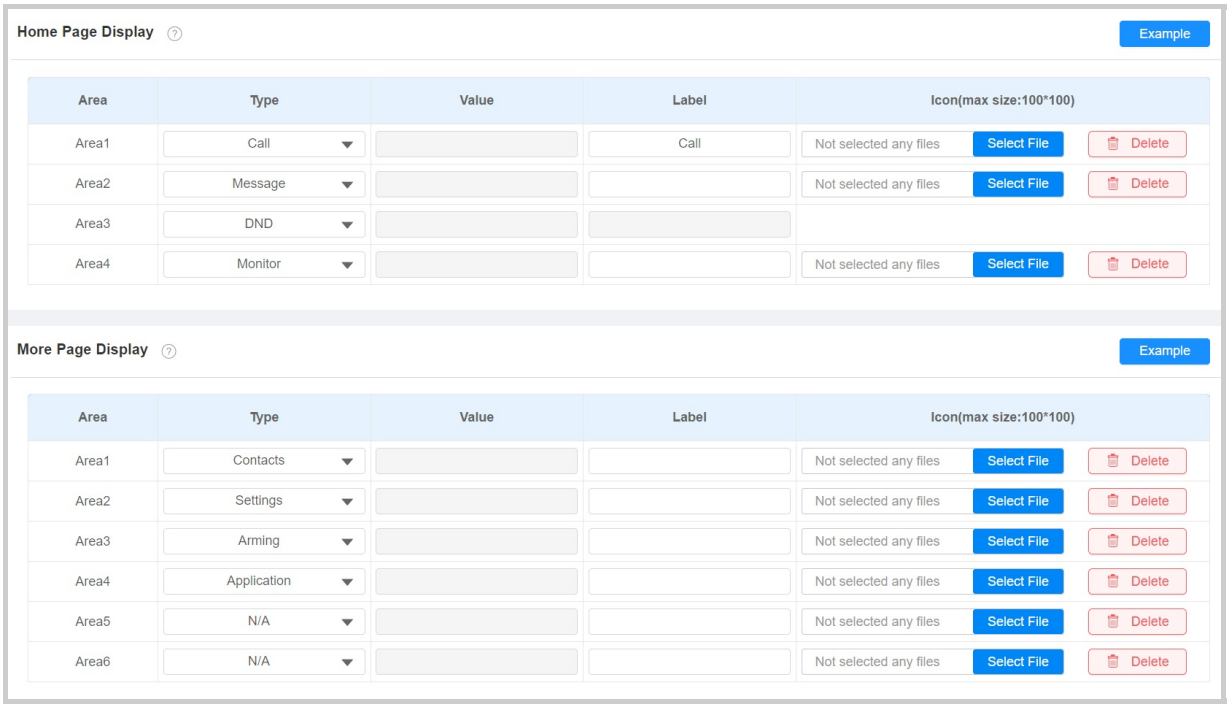
Set it up on the device **Settings > Call Feature** screen.



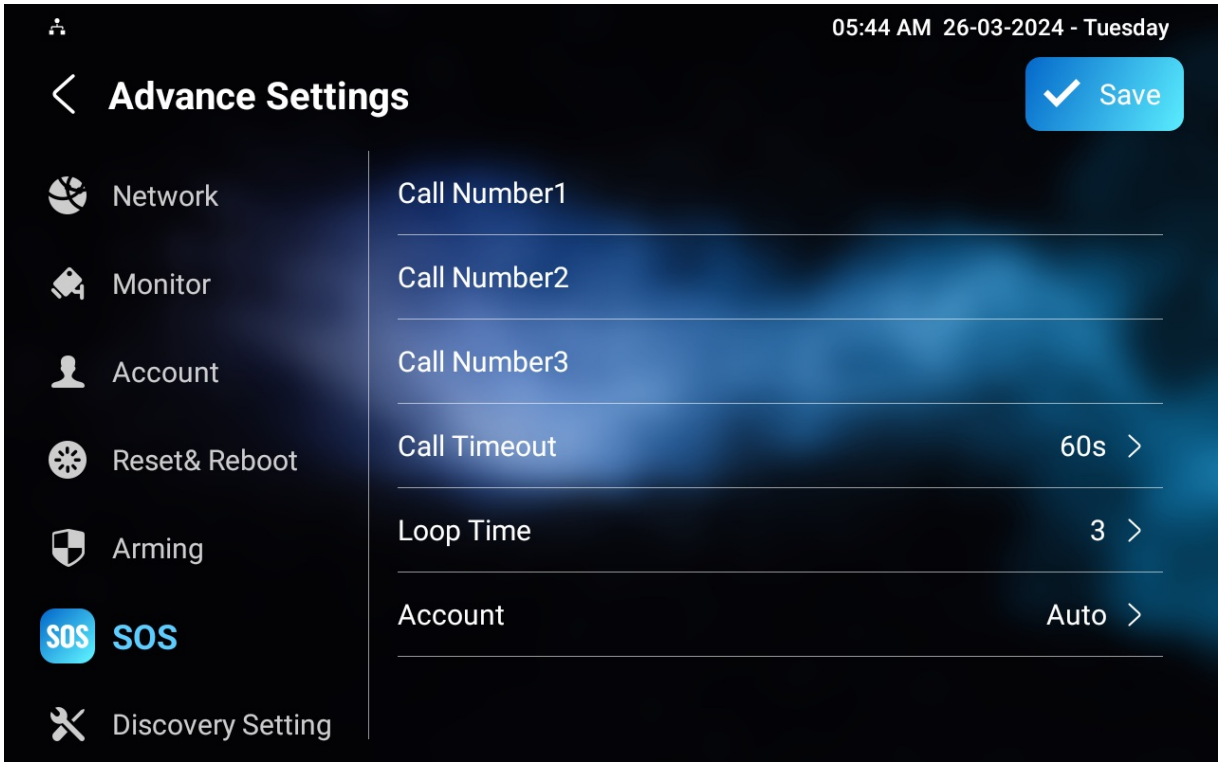
Emergency Call Setting

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.

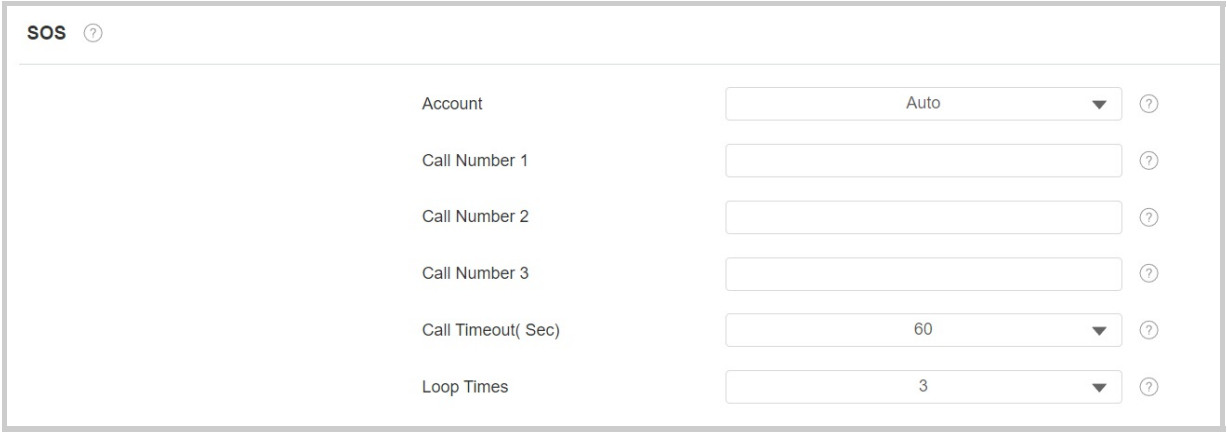


You also need to set up specific parameters on the device or the device web interface. To set it up on the device, go to **Settings > Advance Settings > SOS** screen.



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

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

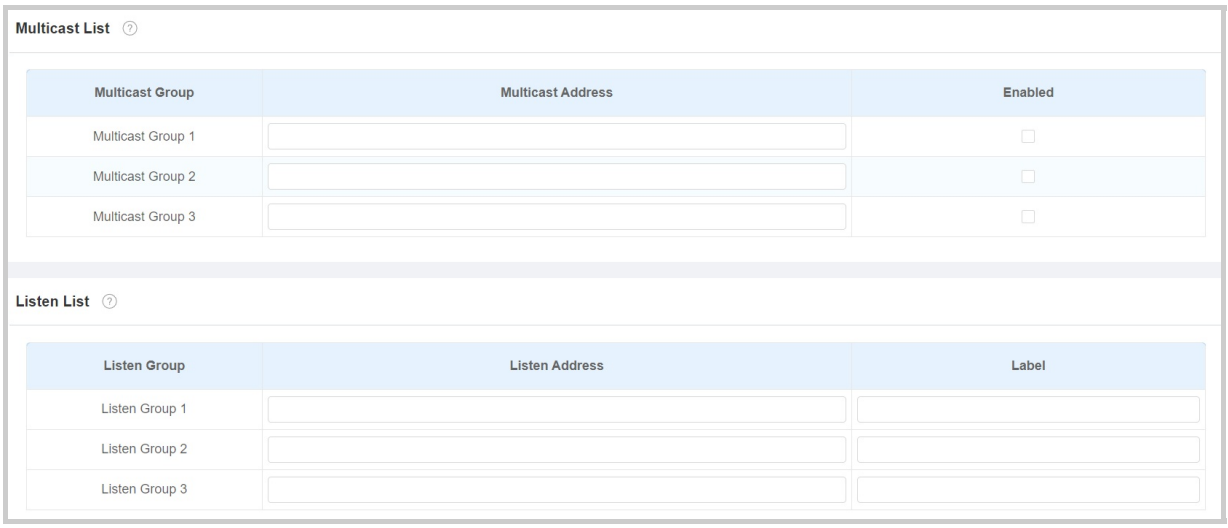


Multicast Configuration

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 listen to or send audio broadcasts.

Click here to watch the demonstration video.

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



- **Multicast 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.

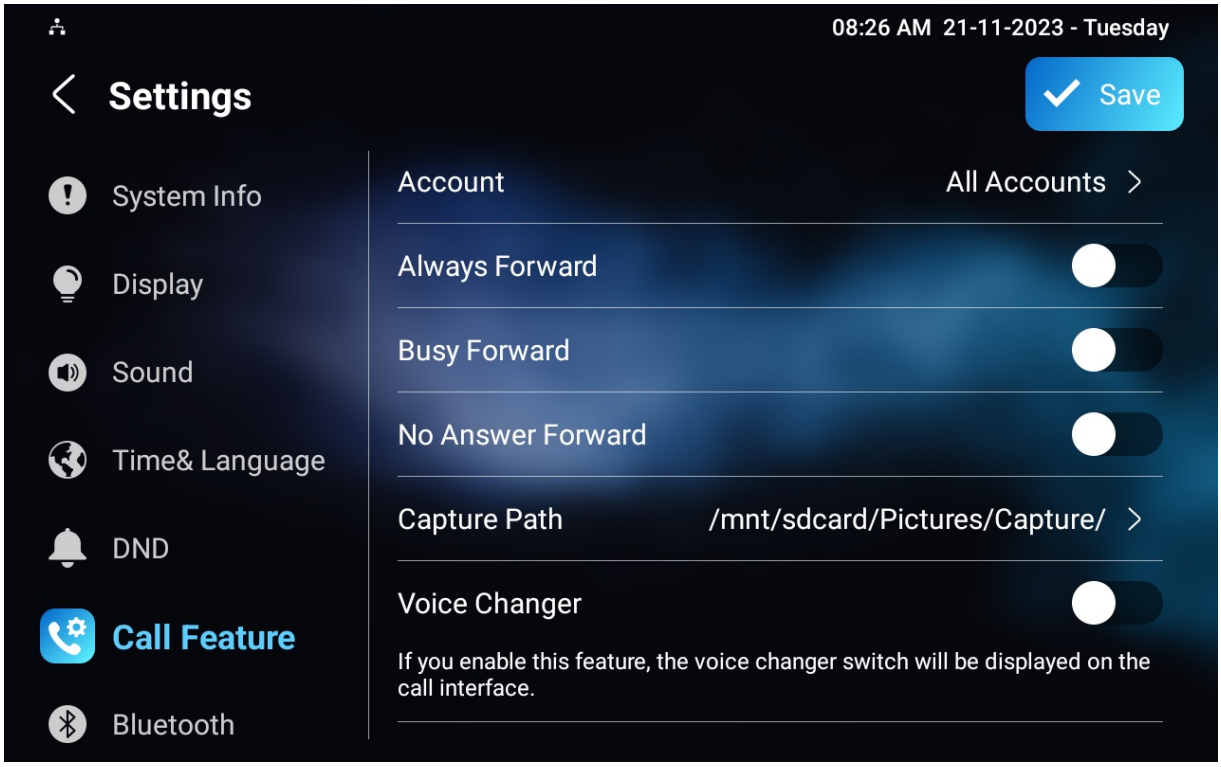
> **Note**
>
> The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult Akuvox tech team for more information.

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.

On the Device

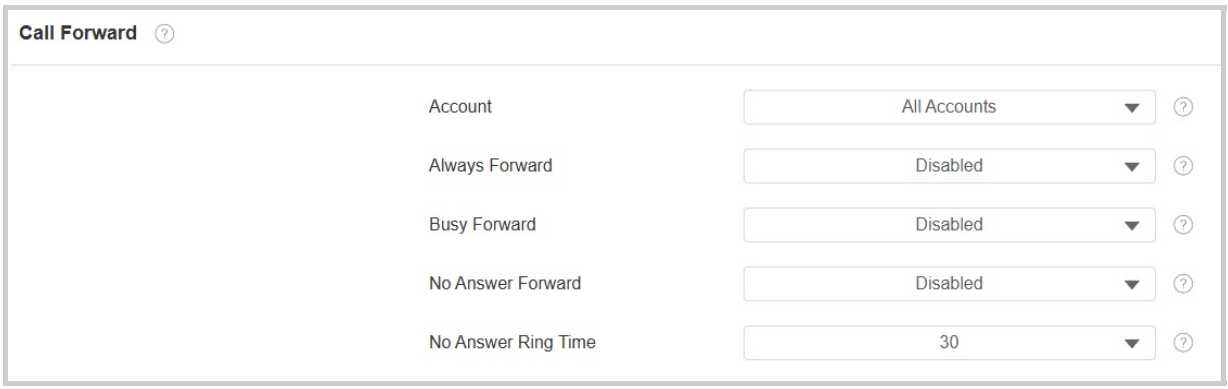
To set it up, go to the device **Settings > Call Feature** screen.



- **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.

On the Web Interface

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

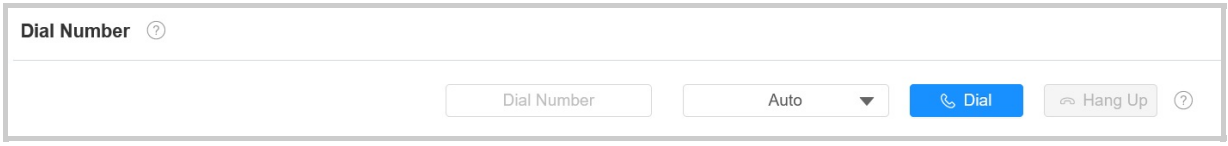


- **Account**: The account to implement the call forwarding feature.
- **Always Forward**: All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: Incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward**: Incoming calls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

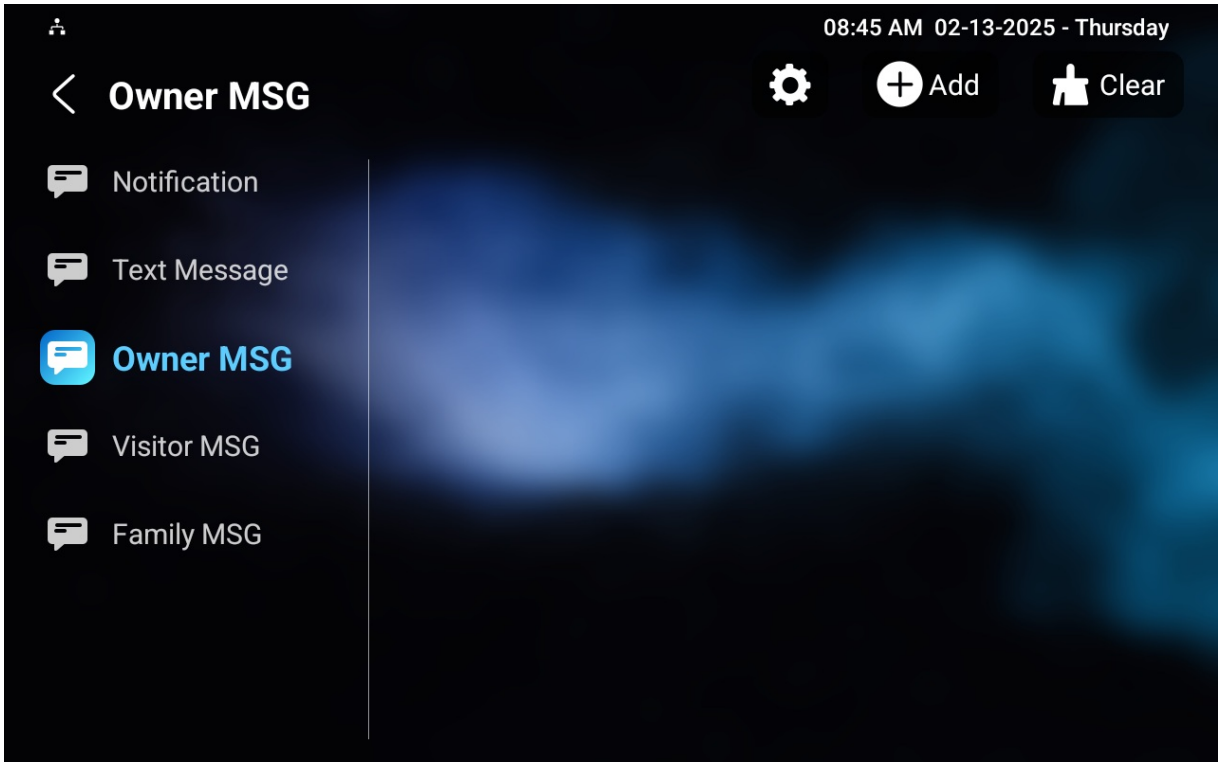


Intercom Message Setting

Manage Messages

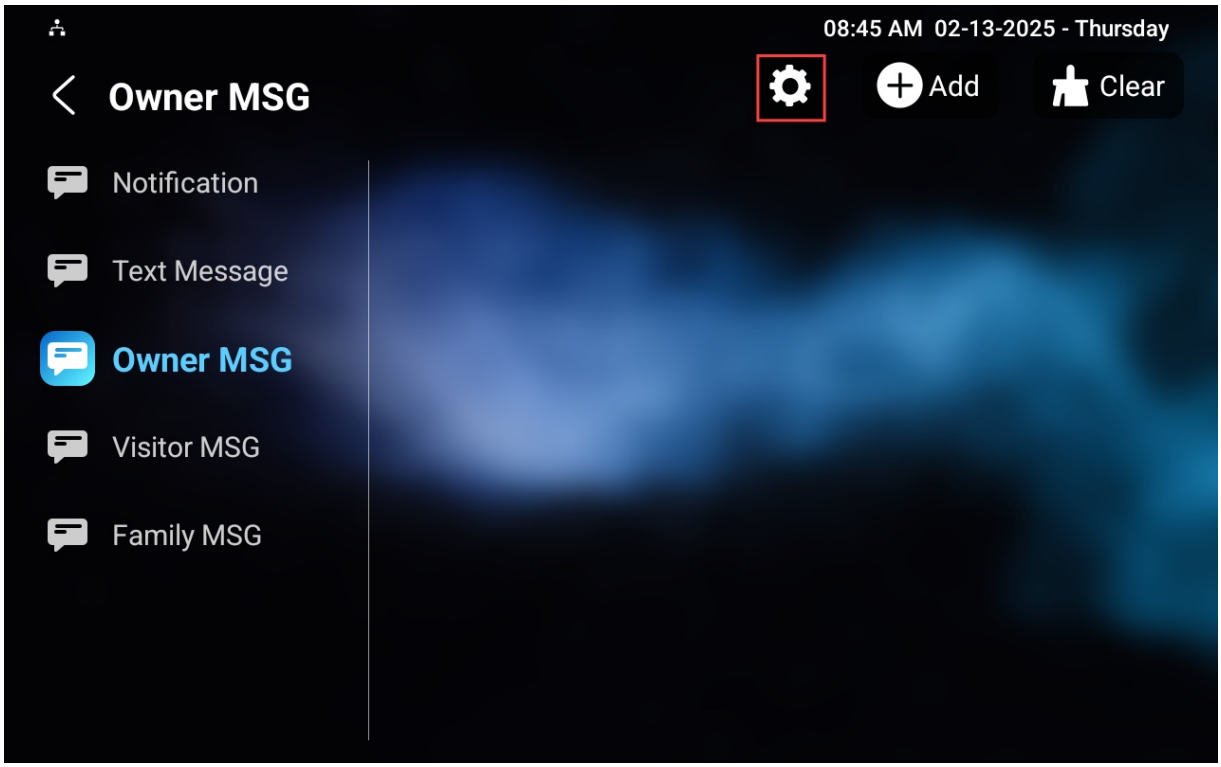
You can check, create and clear messages as needed on the device **Messages** screen.

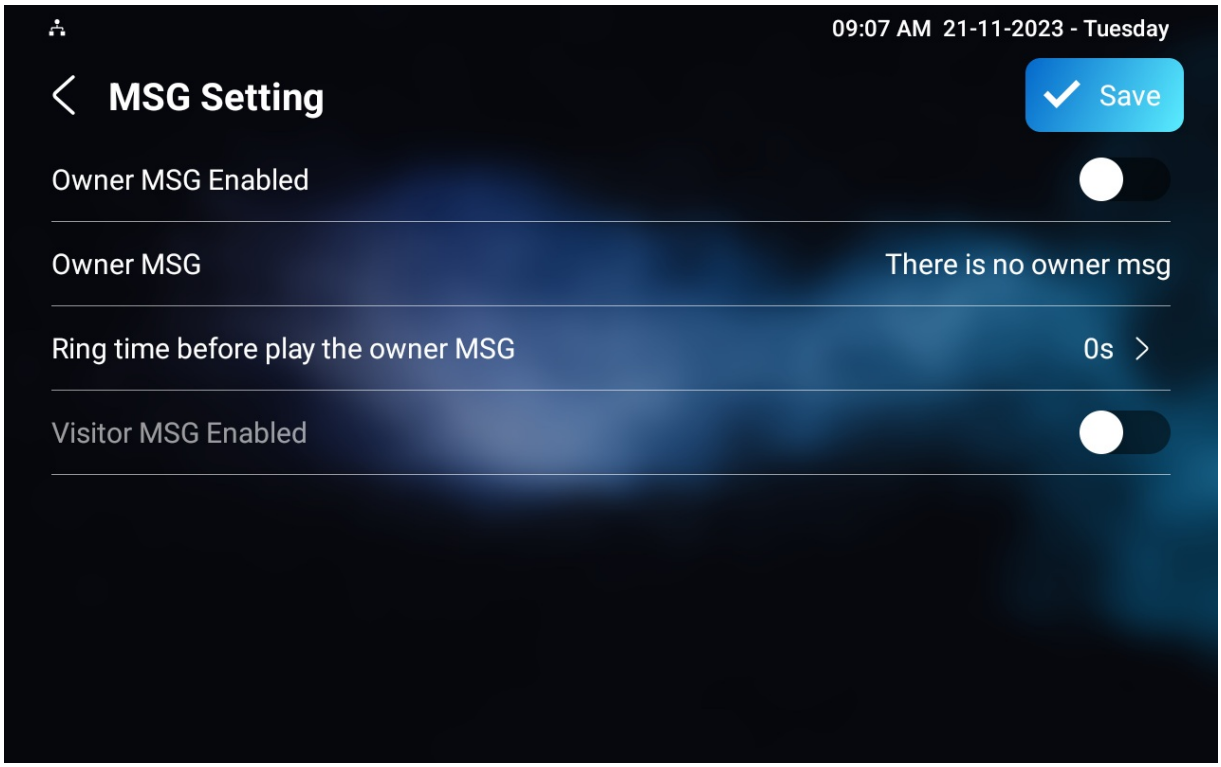
Tap **+Add** to create a message and tap **Clear** to delete messages.



- **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.


08:45 AM 02-13-2025 - Thursday
Owner MSG
Add
Clear
Notification
Text Message
Owner MSG
Visitor MSG
Family MSG


09:07 AM 21-11-2023 - Tuesday
MSG Setting
Save
Owner MSG Enabled
Owner MSG
There is no owner msg
Ring time before play the owner MSG
0s
Visitor MSG Enabled

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.

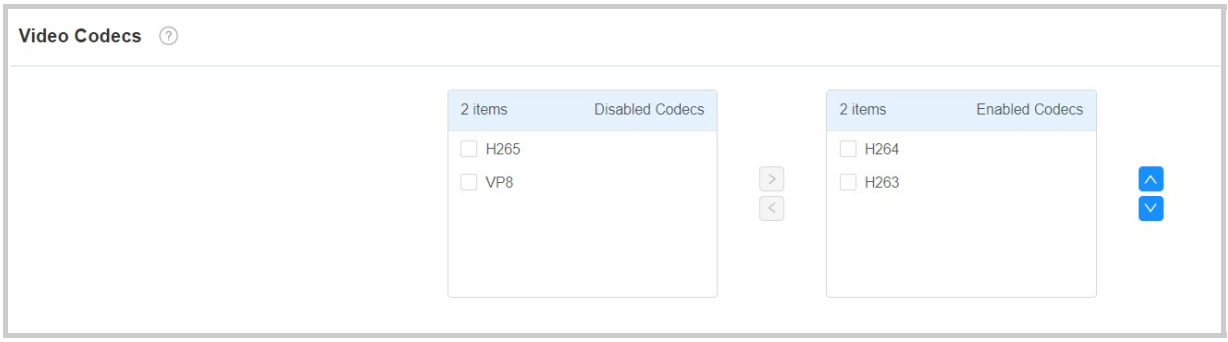
Please refer to the bandwidth consumption and sample rate for the codec types below:

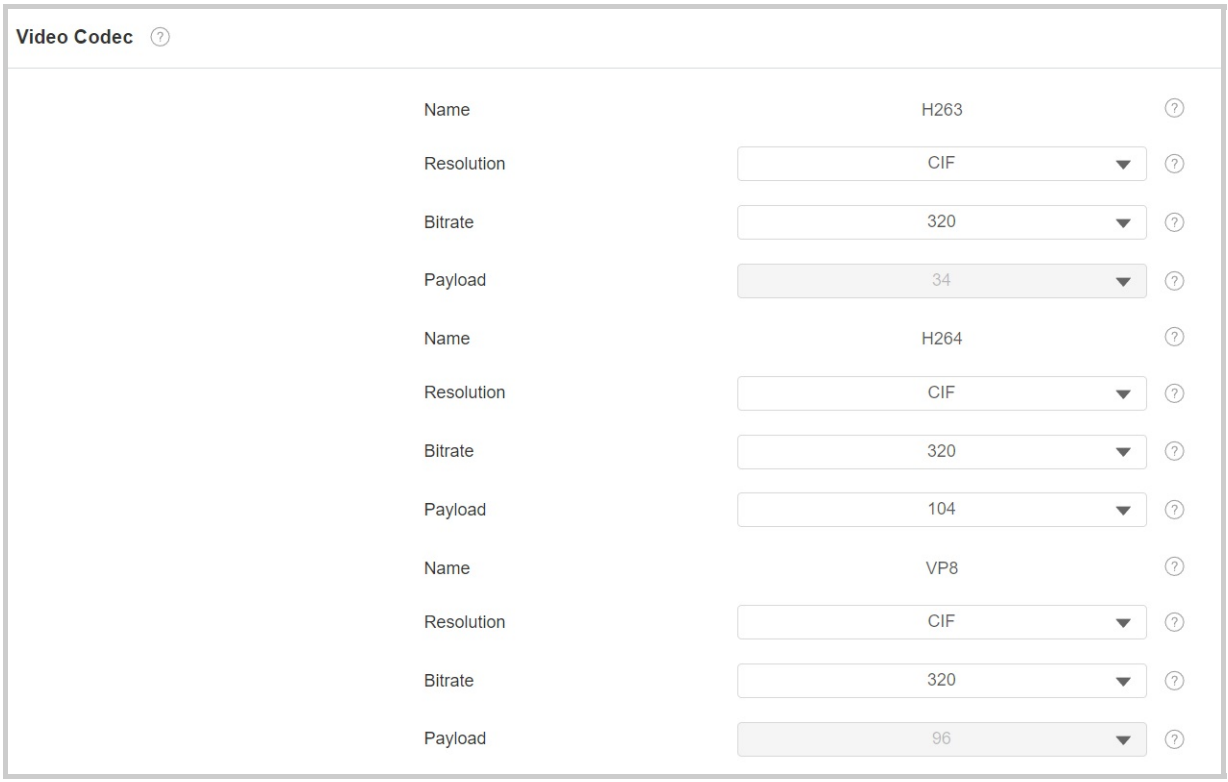
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ
iLBC_13_3	8,16 kbit/s	13.3kHZ
iLBC_15_2	8,16 kbit/s	15.2kHZ
OPUS	154.4 kbit/s	48kHZ
L16	128 kbit/s	variable

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.





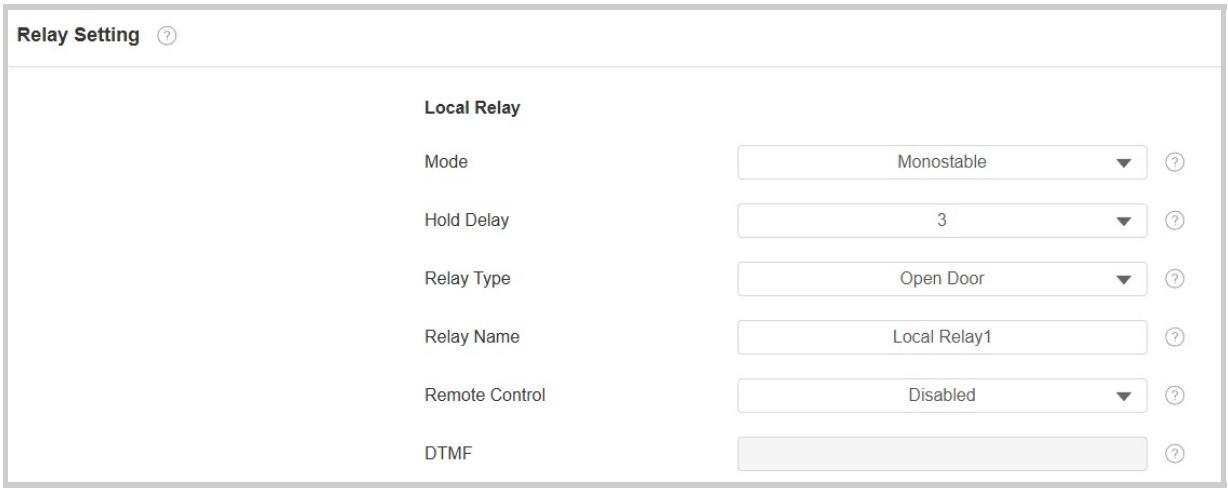
- **Resolution**: The code resolution for the video quality has five options: QCIF, CIF, VGA, 4CIF, and 720P. H263 only has **QCIF, CIF, 4CIF**. Select the resolution according to the network environment.
- **Bitrate**: Select the video stream bitrate. It varies by the resolution.
- **Payload**: The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

Access Control Configuration

Local Relay

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

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

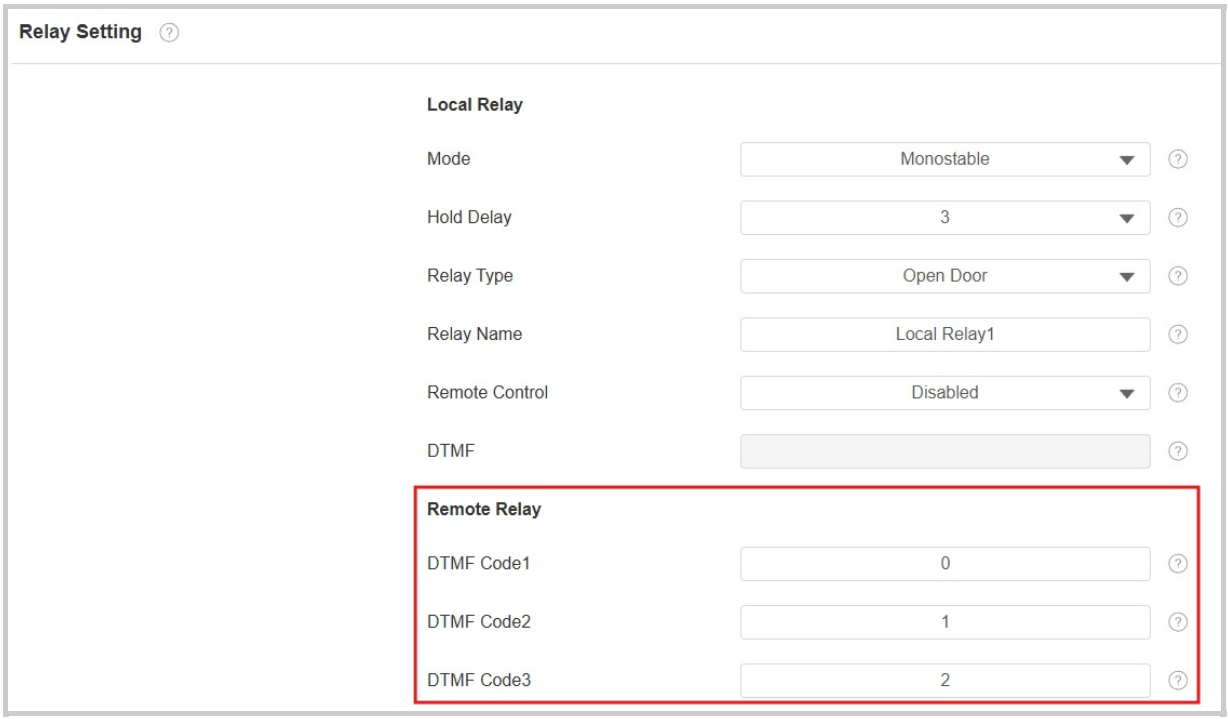


- **Mode**: Specify the conditions for automatically resetting the relay status.
    - **Monostable**: The relay status resets automatically within the relay delay time after activation.
    - **Bistable**: The relay status resets upon triggering the relay again.
- **Hold Delay(Sec)**: Determine how 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

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.



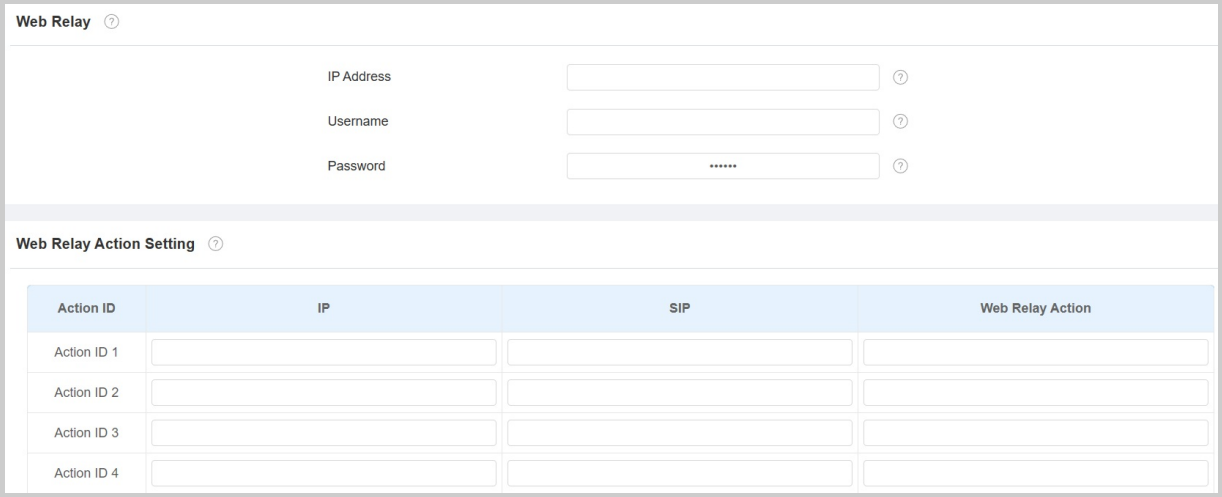
- **DTMF Code**: Define the DTMF code within the range(0-9 and *,#) for the remote relay.

Web Relay

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

Click here to view how to set up web relay.

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



- **IP Address**: The web relay IP address provided by the web relay manufacturer.
- **Username**: The user name provided by the web relay manufacturer.
- **Password**: The manufacturer-provided authentication key for the web relay. Authentication occurs via HTTP. Leaving the Password field blank indicates non-use of HTTP authentication. You can define the password using HTTP GET in the Web Relay Action field.
- **IP/SIP**: The relay extension information, which can be an IP address or SIP account of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device. This setting is optional.
- **Web Relay Action**: Configure the actions to be performed by the web relay upon triggering. Enter the manufacturer-provided URLs for various actions.

Note

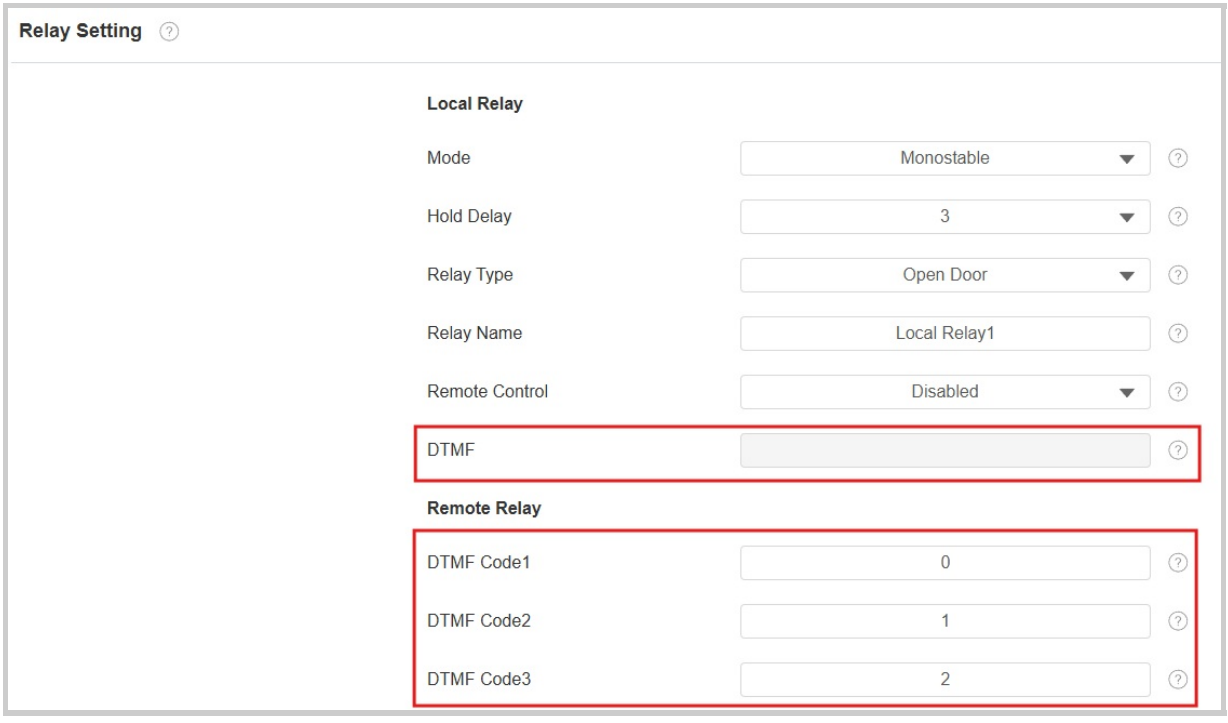
If the URL includes full HTTP content(e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., "state.xml?relayState=2"), the relay uses the entered IP address.

Door-opening Configuration

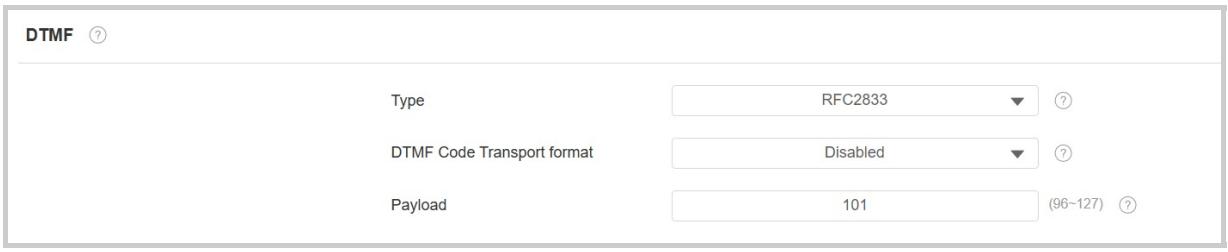
Unlock by DTMF Code

Dual-tone multi-frequency signaling(**DTMF**) is a way of sending signals over phone lines by using different voice-frequency bands. Users can use the DTMF function to unlock the door for visitors during a call by either typing the DTMF code on the soft keypad, or tapping the unlock tab with the DTMF code on the screen.

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



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



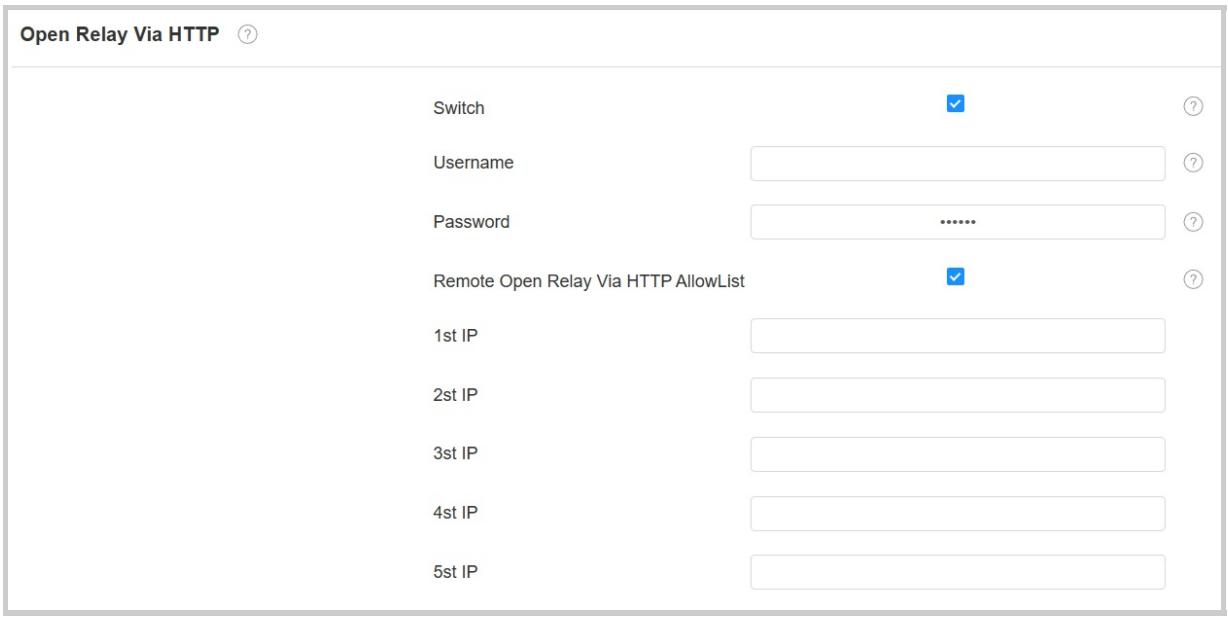
- **Type**: Select from the provided options.
- **DTMF Code Transport Format**: There are four options, Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via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

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

Unlock via HTTP Command

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

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

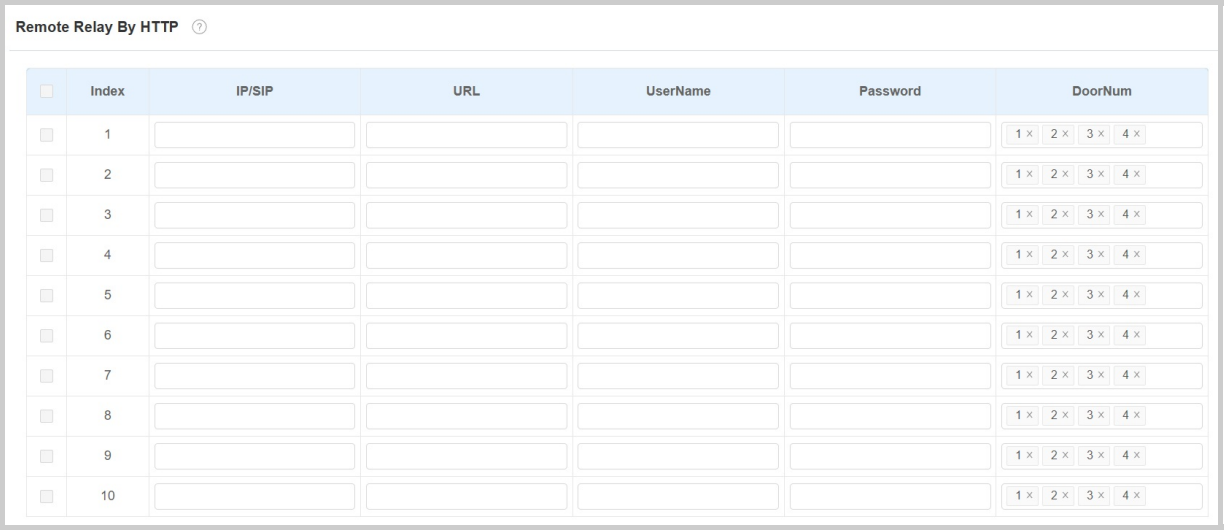


- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a username for authentication in HTTP command URLs.
- **Remote Open Relay Via HTTP AllowList**: Enable it and type in the IP address of the server that you allow to send the HTTP command to the indoor monitor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

Note

- If you do not set up the username and password, the remote door phone can trigger the indoor monitor's relay without authentication.
- The URL format is http://{deviceIP}/fcgi/OpenDoor?action=OpenDoor&DoorNum=1.

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.



- **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.

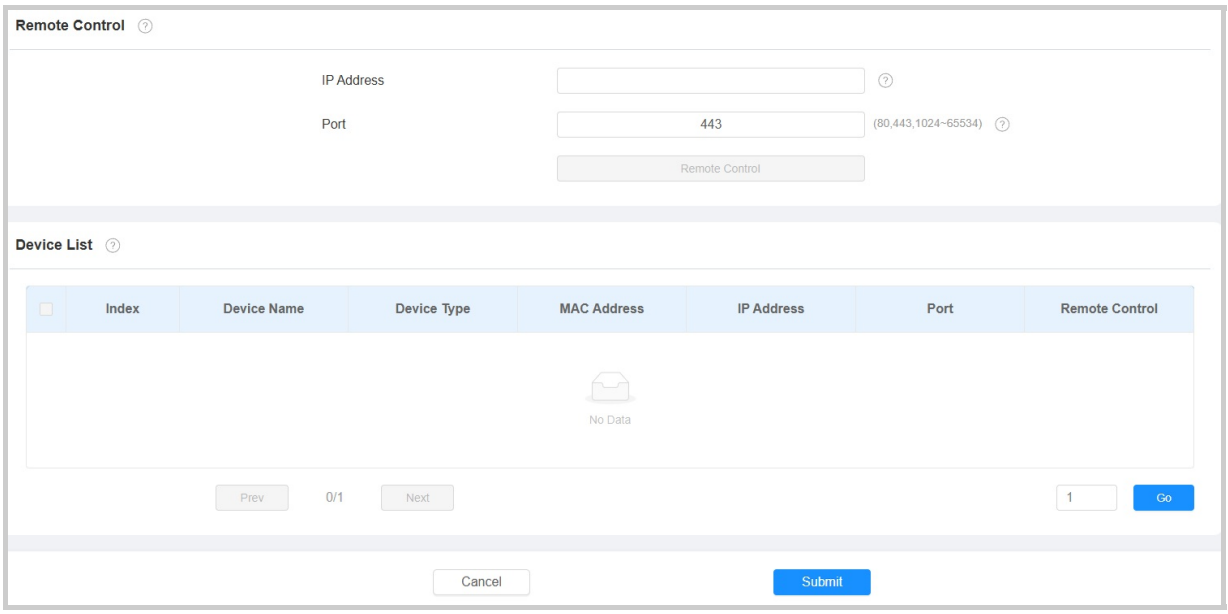
Note

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.

Remote Control

The device can scan other intercom devices on the same LAN. You can redirect to their web interfaces for configuration.

Set it up on the **Device > Remote Control** interface.



- **IP Address**: The IP address of the device to be accessed remotely.
- **Port**: The port of the device to be accessed remotely. If the port is not filled in, the device will use 80 or 443 by default for access.
- **Remote Control**: Click to redirect to the device's web interface.

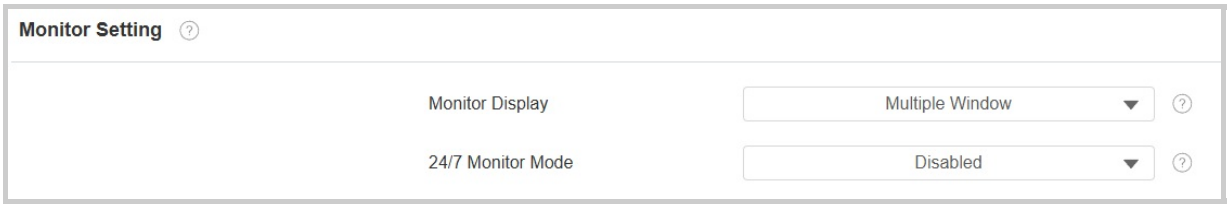
Security

Monitor and Image

Monitor Setting

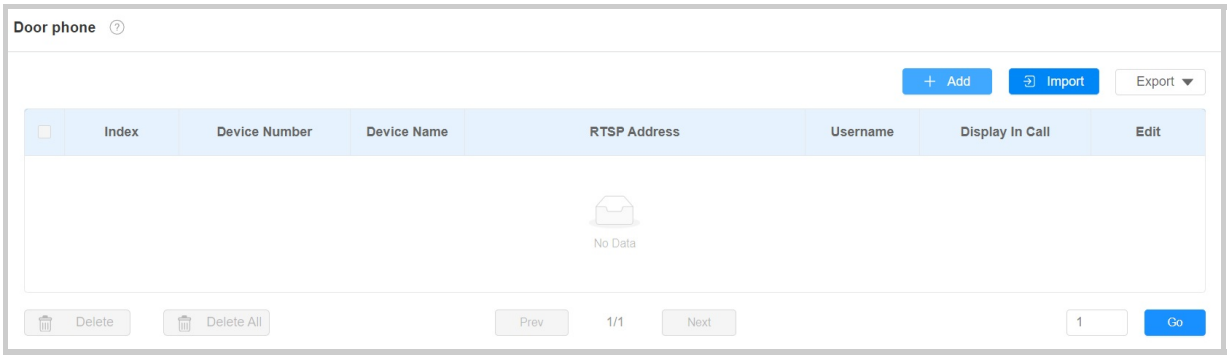
You can add video streams using RTSP. If the Display in Call function is enabled, the video of the added monitor device will show up when it calls the indoor monitor.

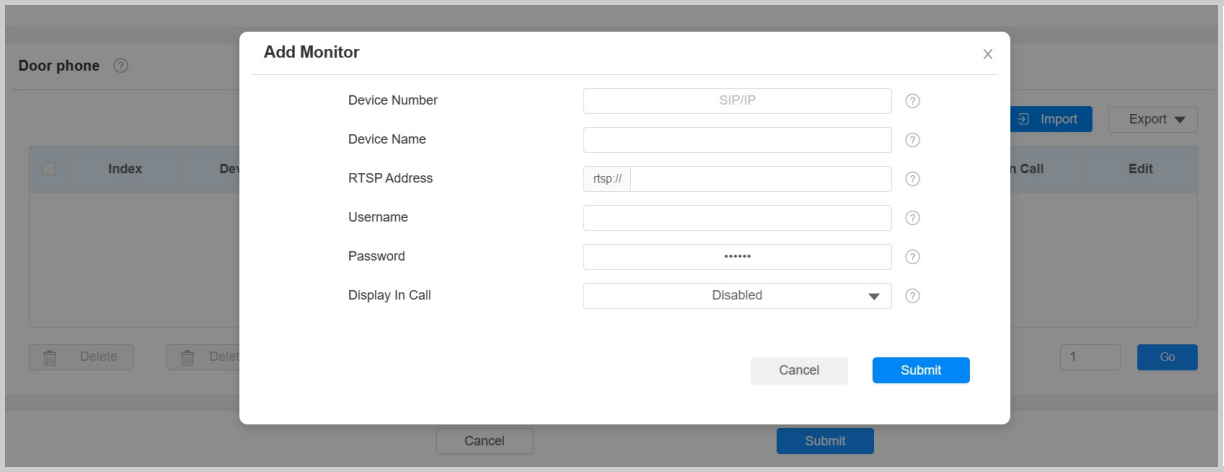
To set it up, go to the **Device > Monitor** interface.



- **Monitor Display**:
  - **Multiple Windows**: Display four video monitoring channels on the screen.
  - **Single Window:** Display only one video monitoring channel.
- **24/7 Monitor Mode**: When enabled, the indoor monitor displays the monitoring screen for 6 hours, then plays a 10-second screensaver before resuming the monitoring stream.

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



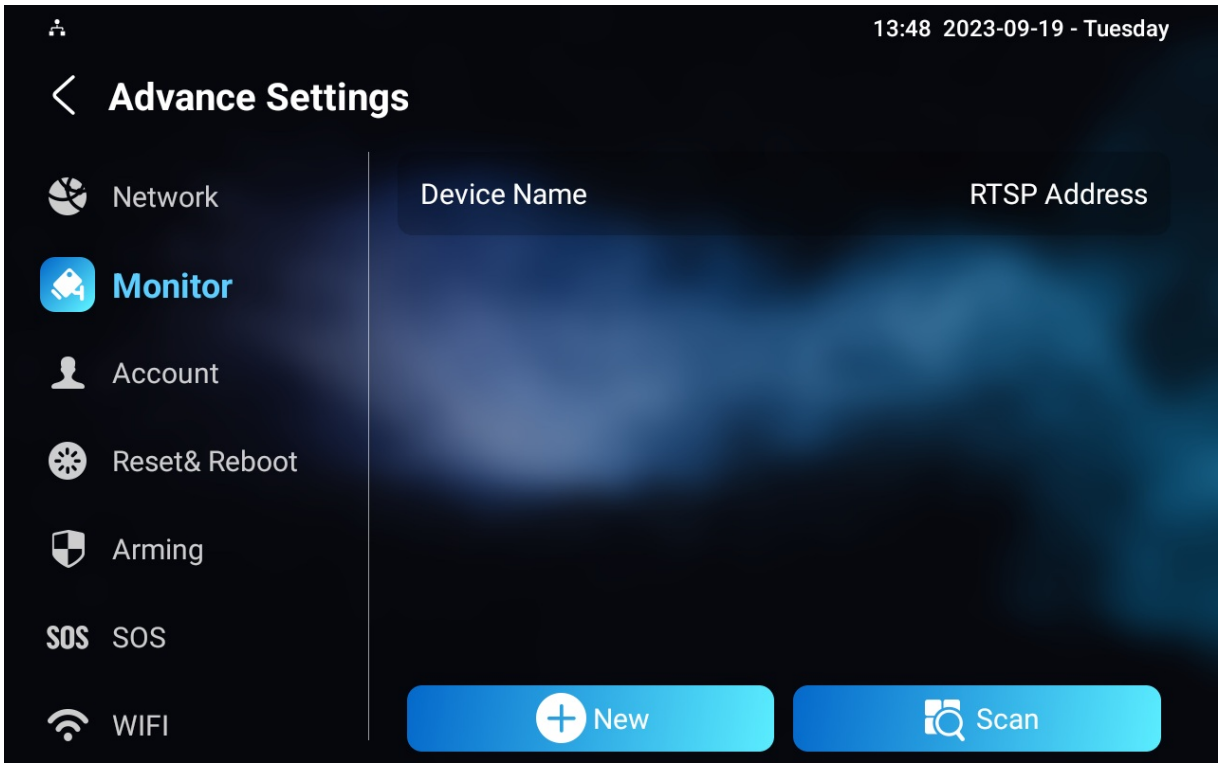


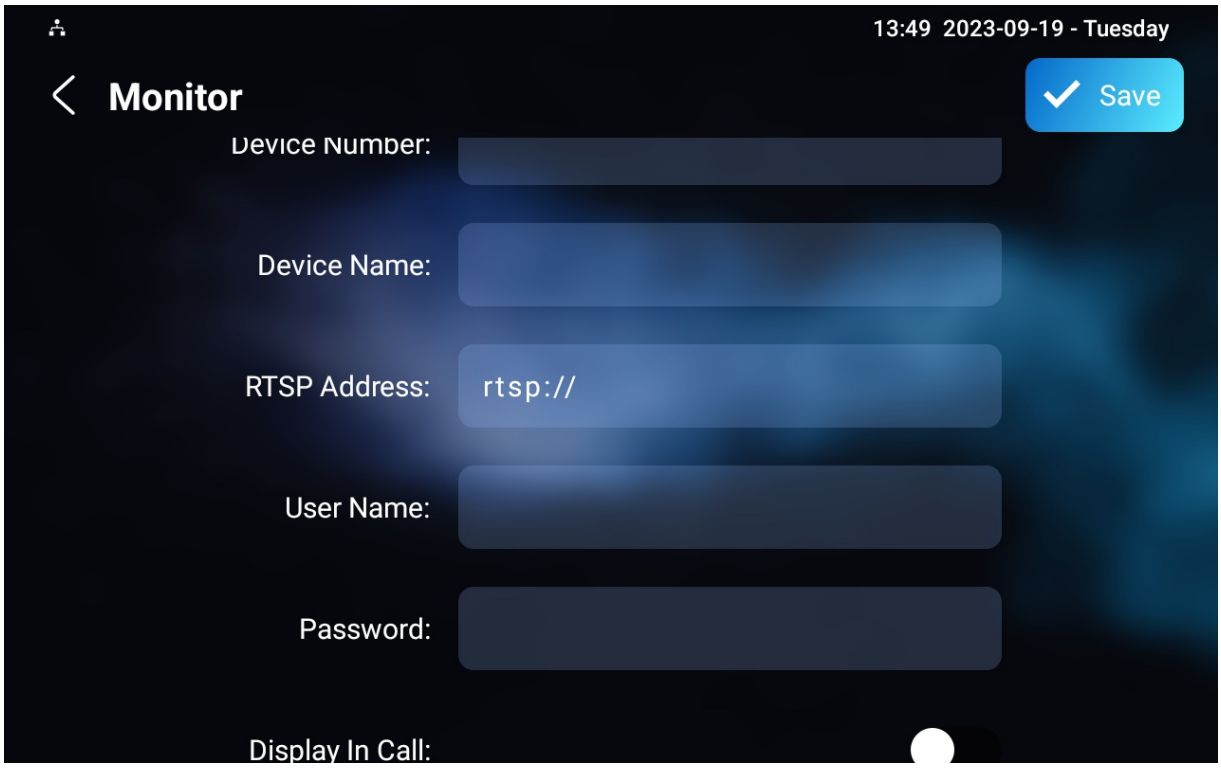
- **Device Number**: The device's SIP/IP number for identification.
- **Device Name**: The device name for identification.
- **RTSP Address**: The RTSP address of the monitoring device. RTSP format: rtsp://Device IP address/live/ch00_0.
- **Username**: The username of the monitoring device for authentication.
- **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 Settings > Monitor** screen. Tap **+New** to add the monitor device.

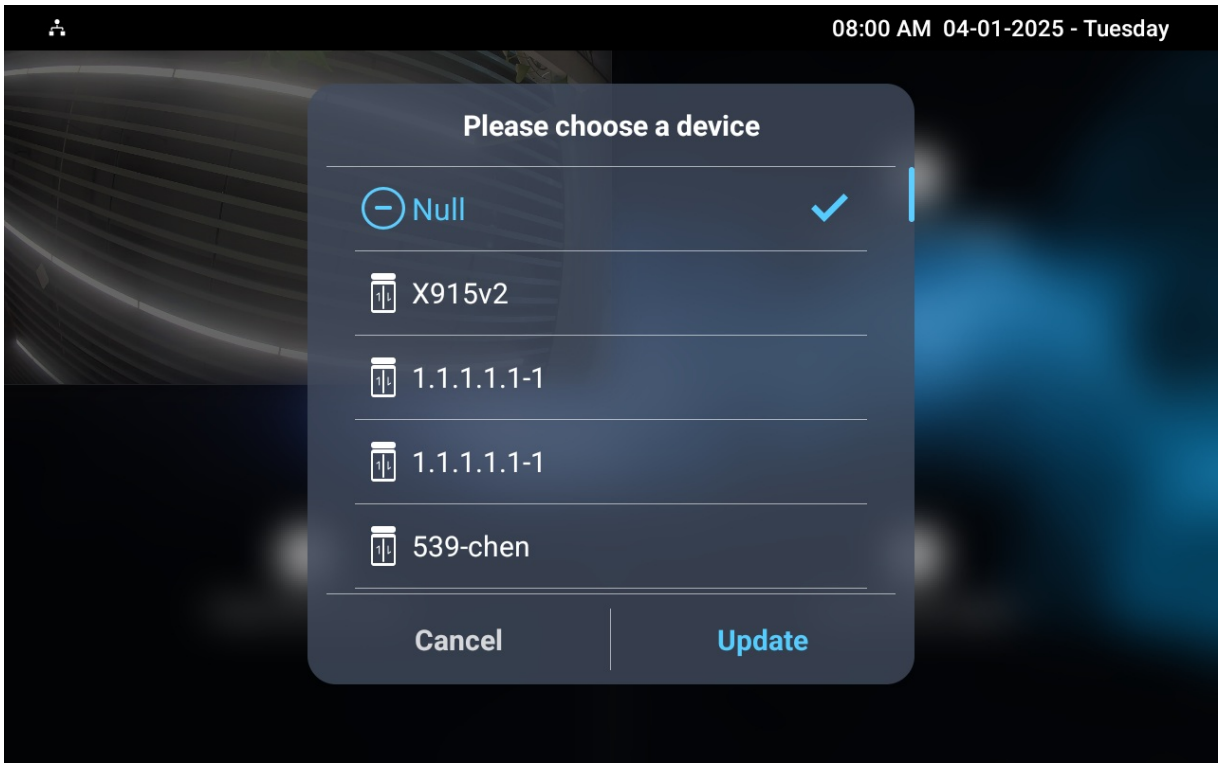
When the monitoring device is an Akuvox door phone and its RTSP username and password are not changed(admin by default), you can directly scan and add the door phone on the indoor monitor's **Monitor** screen. If the username and password are changed, make sure they are consistent between the devices.

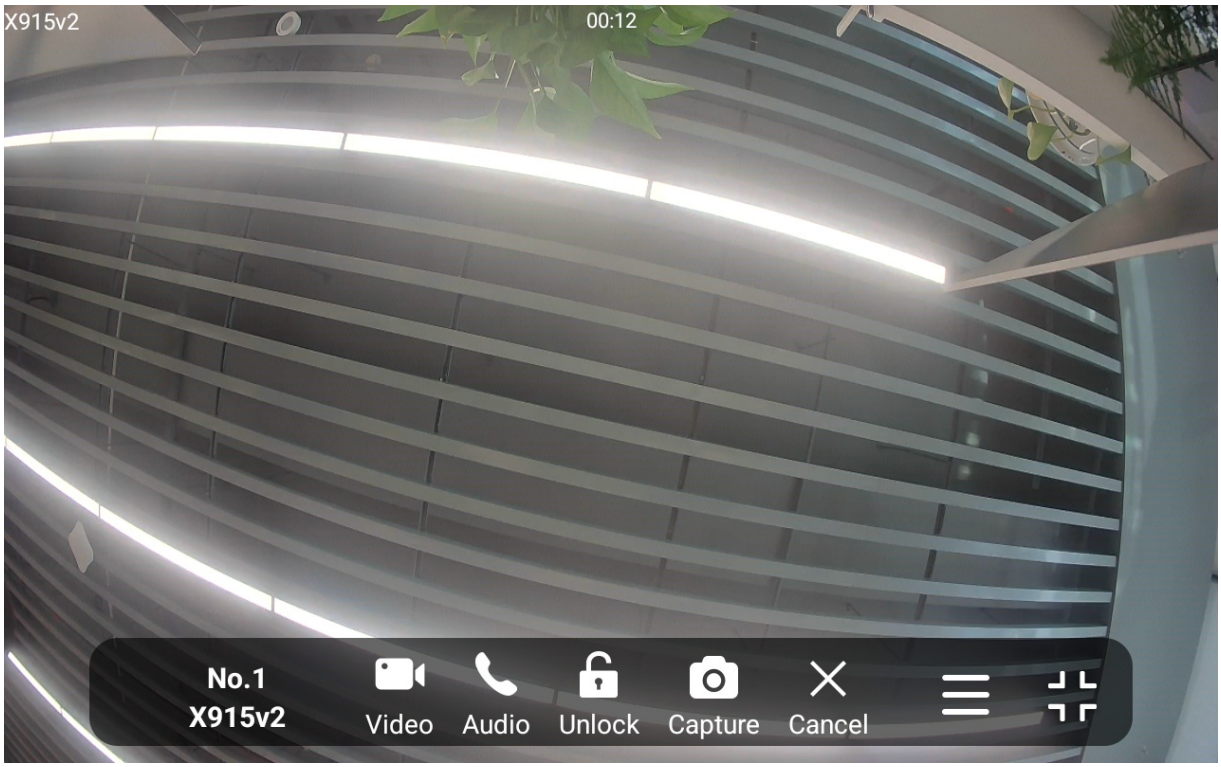




View Monitoring Streams

After adding the monitored device's RTSP URL, tap **Monitor** on the home screen and select the desired channel to view the stream.





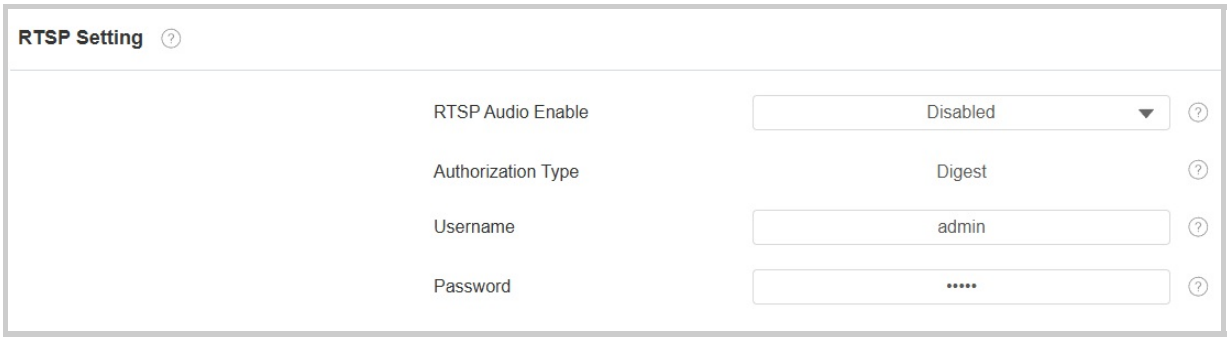
- **Video**: Tap to make a video call to the monitored door phone.
- **Audio**: Tap to make an audio call to the monitored door phone.
- **Unlock**: Tap to open the door.
- **Capture**: Tap to take a screenshot.
- **Cancel**: Tap to exit the monitoring.
- : Tap to display the monitor list.

> **Note**
>
> During monitoring, calls can only be made to Akuvox door phones, neither access control terminals nor third-party devices.

RTSP Authentication

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

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



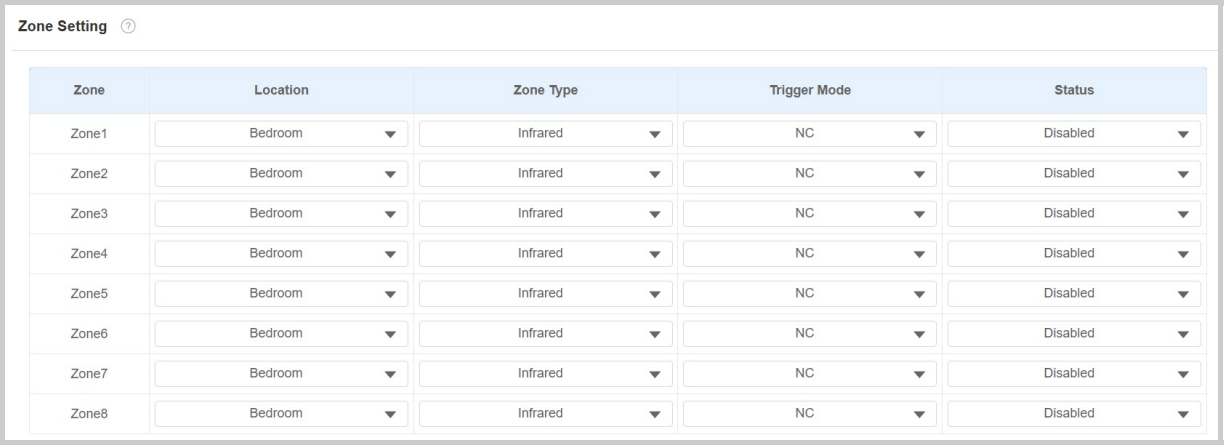
- **Authorization Type**: It is Digest by default.
- **Username**: Set the username for the authentication.
- **Password**: Set the password for the authentication.

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.

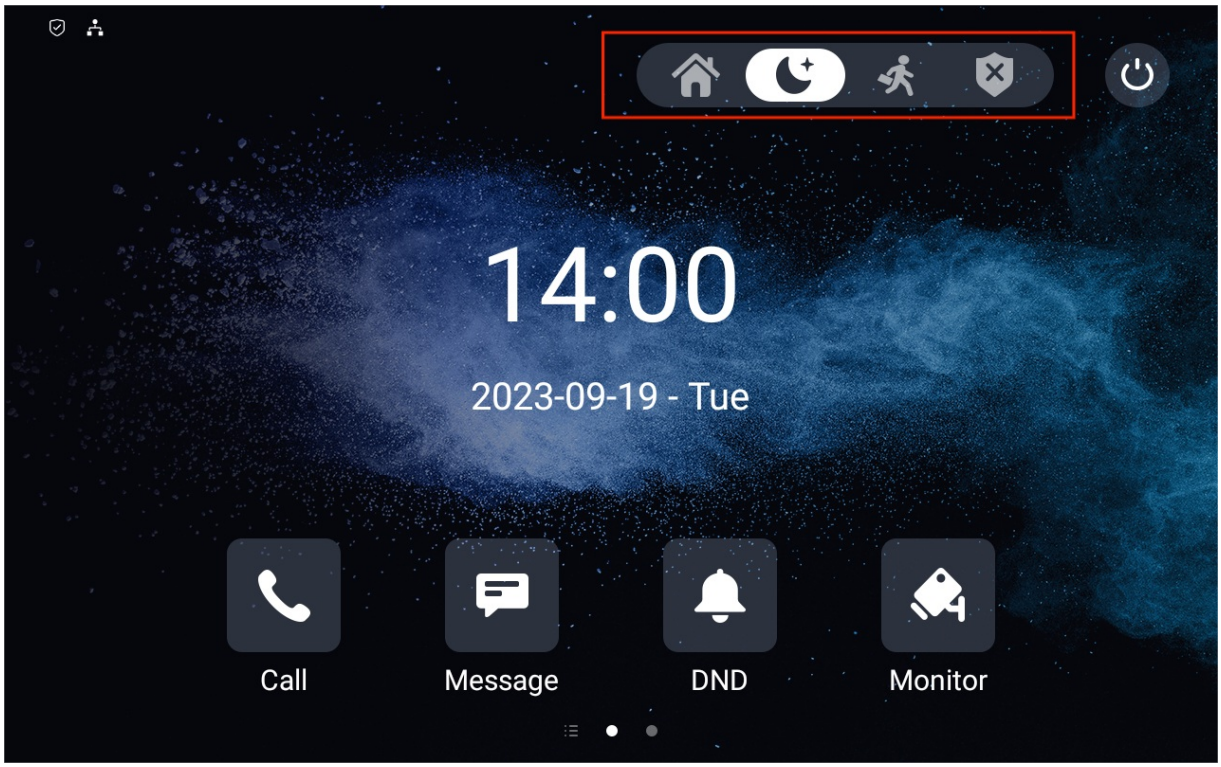
Set up Location-based Alarm Sensors

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

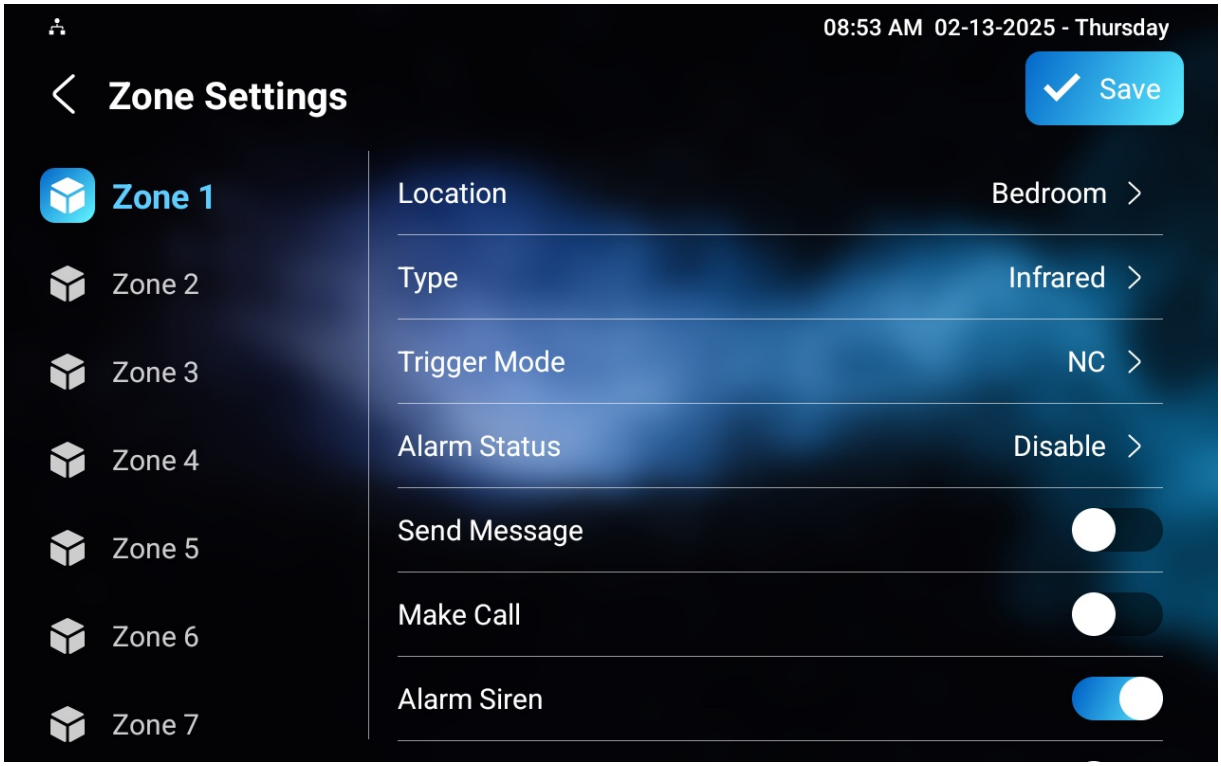


- **Location**: Indicate where the alarm sensor is installed. There are ten location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type**: The alarm sensor types.
- **Trigger Mode**: Set sensor trigger mode between NC and NO.
- **Status**: Set the 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.



You can also set up alarm sensors on the **Settings > Advance > Arming** screen.

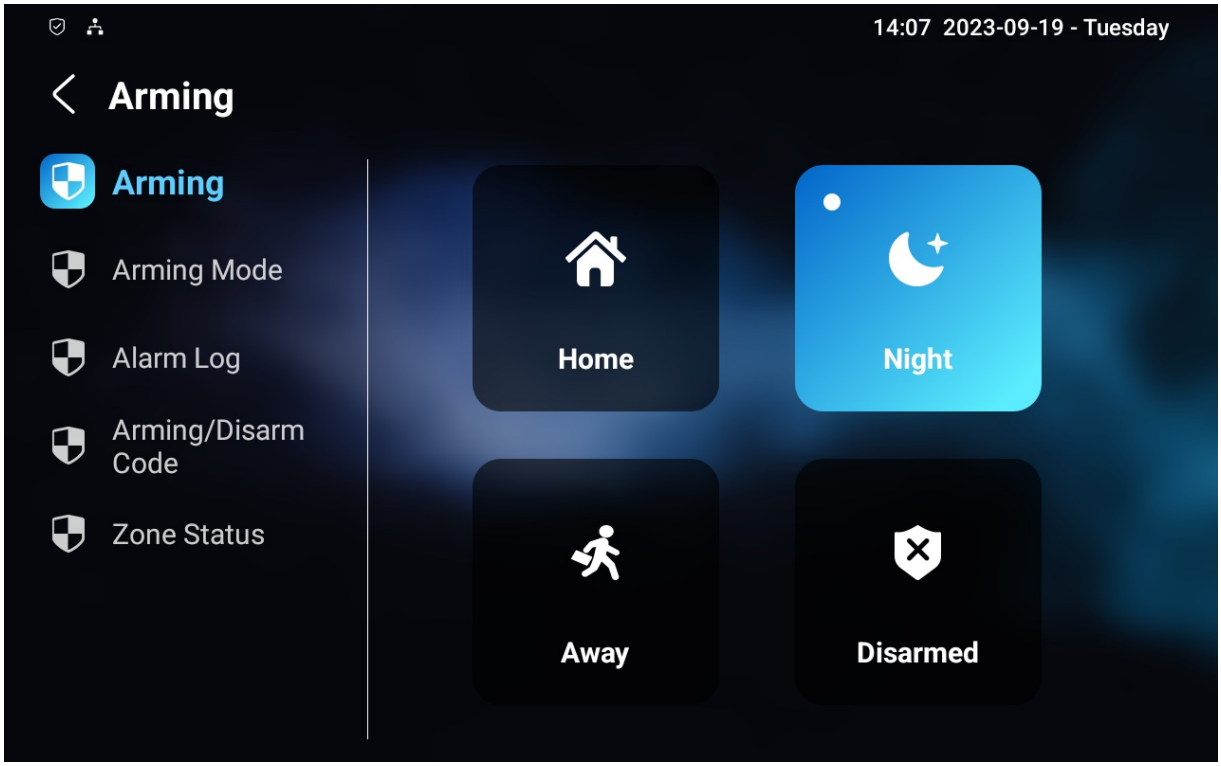


Select an Arming Mode

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

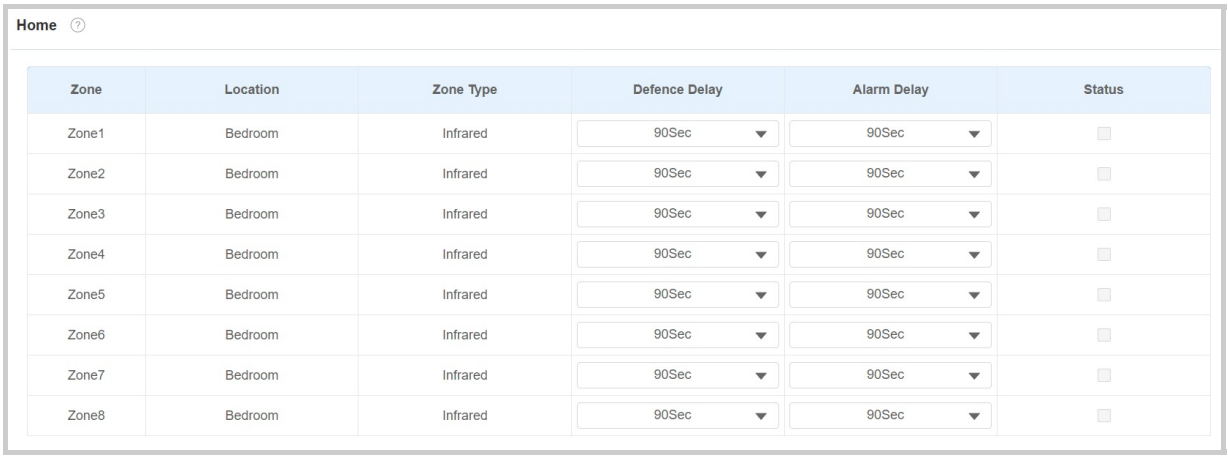
After displaying the Arming tab on the device screen, users can switch arming mode on the Arming screen.

Set the arming tab display on the **Device > Display Setting** interface.



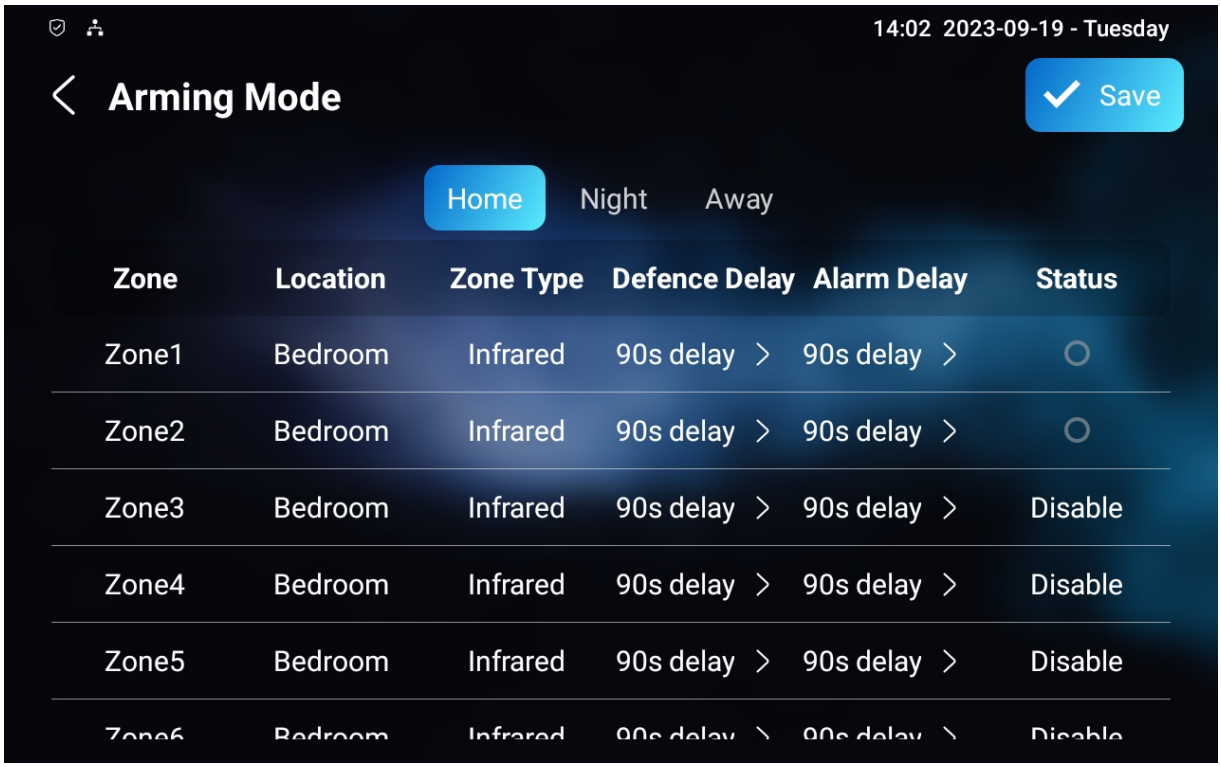
Set up Alarm Sensors in Different Arming Modes

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



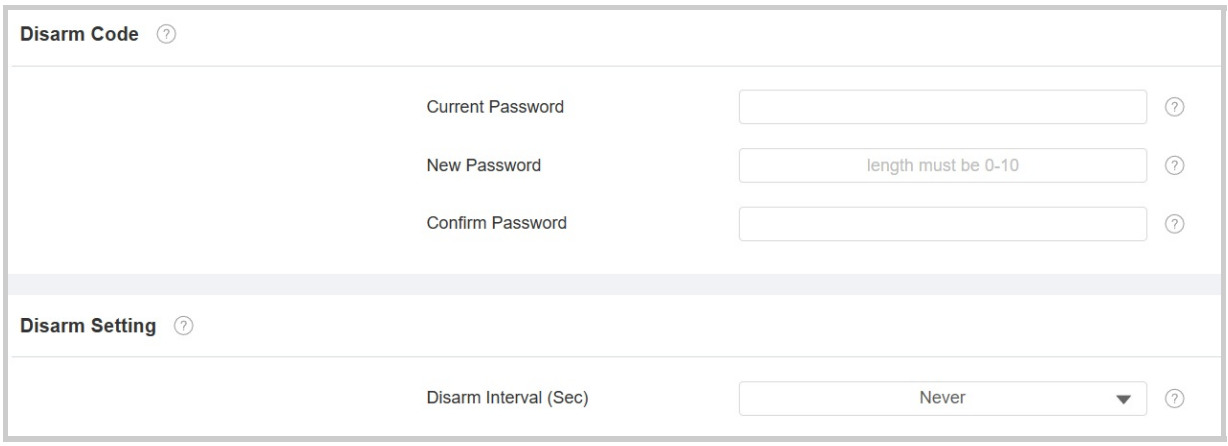
- **Location**: Display which location the detection device is in, including Bedroom, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type**: Display the alarm sensor type.
- **Defence Delay**: It means when users change the arming mode from other modes, there will be 90 seconds 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.

You can also set it up on the **Arming > Arming Mode** screen.



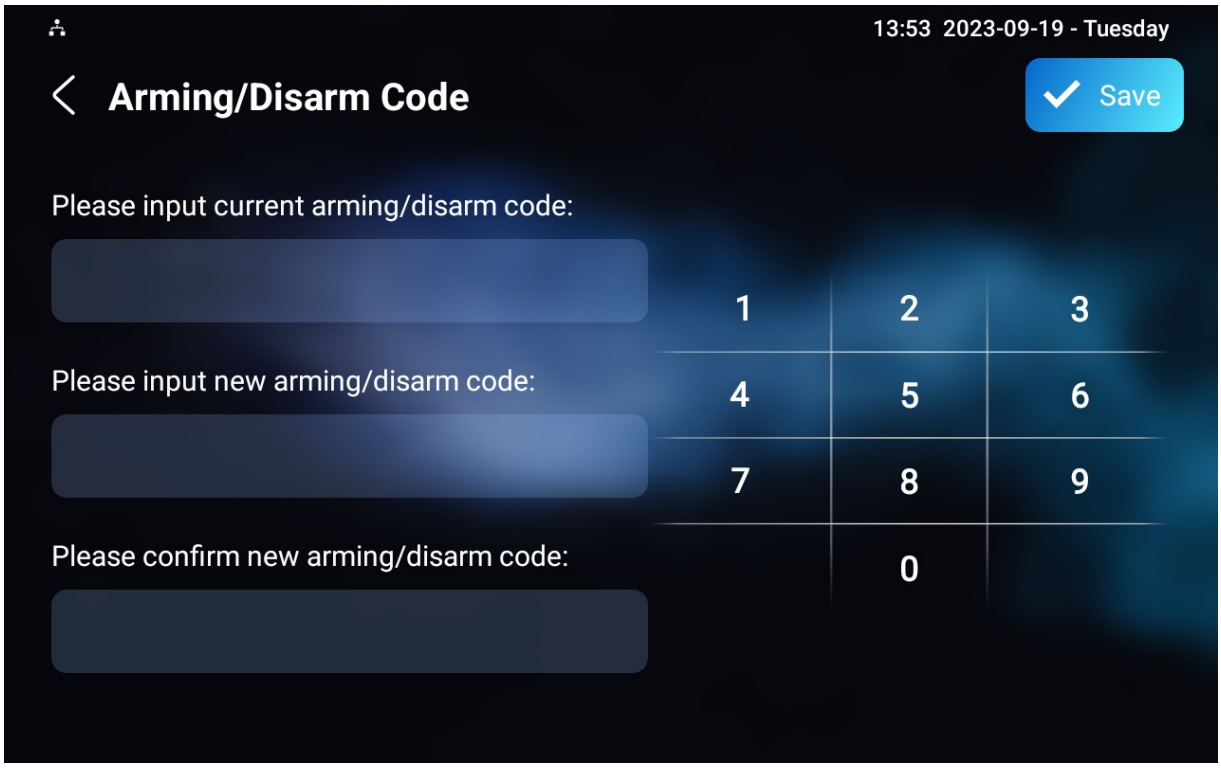
Set up the Disarm Codes

To configure the arming and disarm codes, go to the **Arming > Disarm Code** interface.



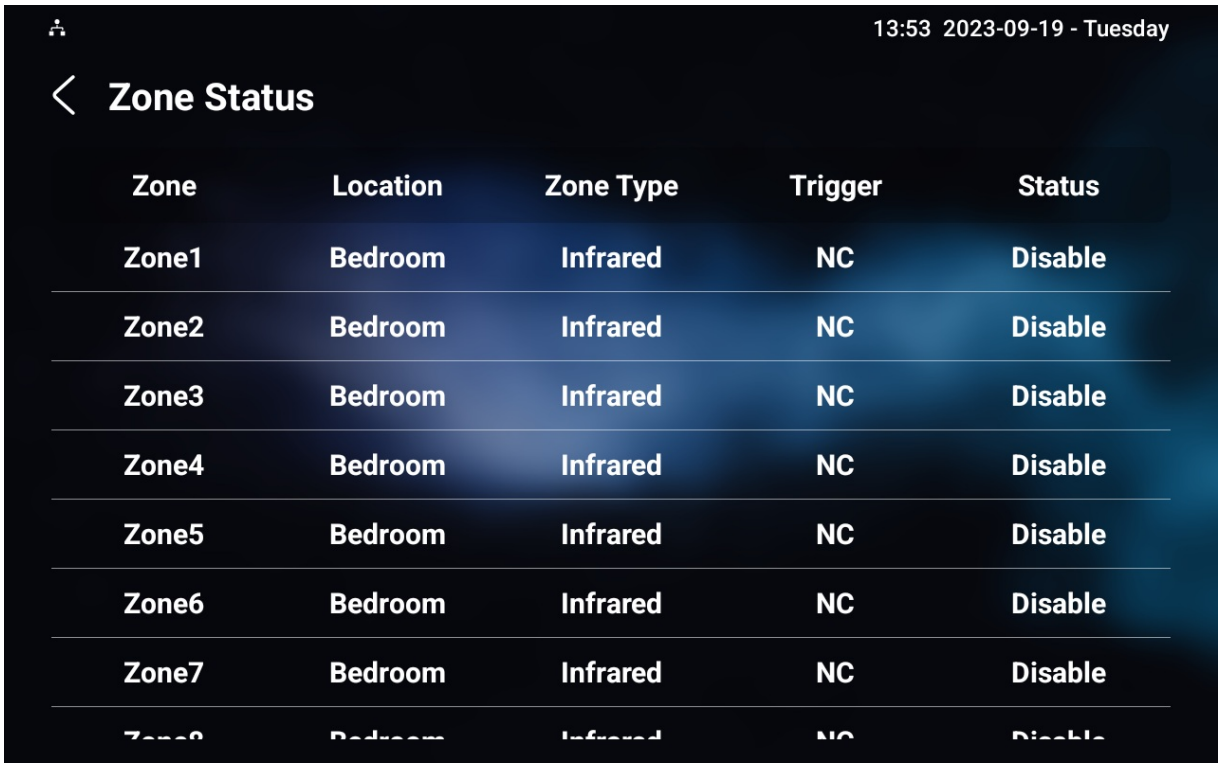
- **Disarm Interval(Sec)**: Set the alarm sound duration after the alarm is triggered.

You can also set it up on the **Arming > Arming/Disarm Code** screen.



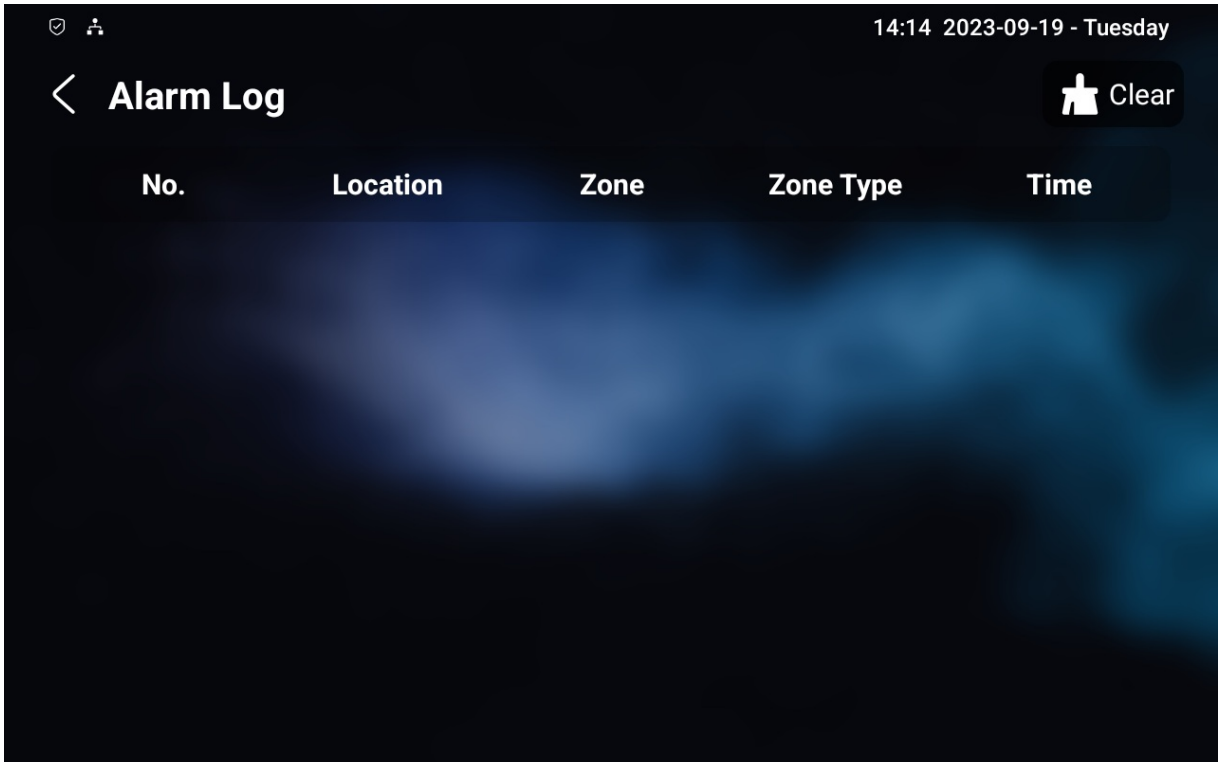
Check Zone Status

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



Check Alarm Logs

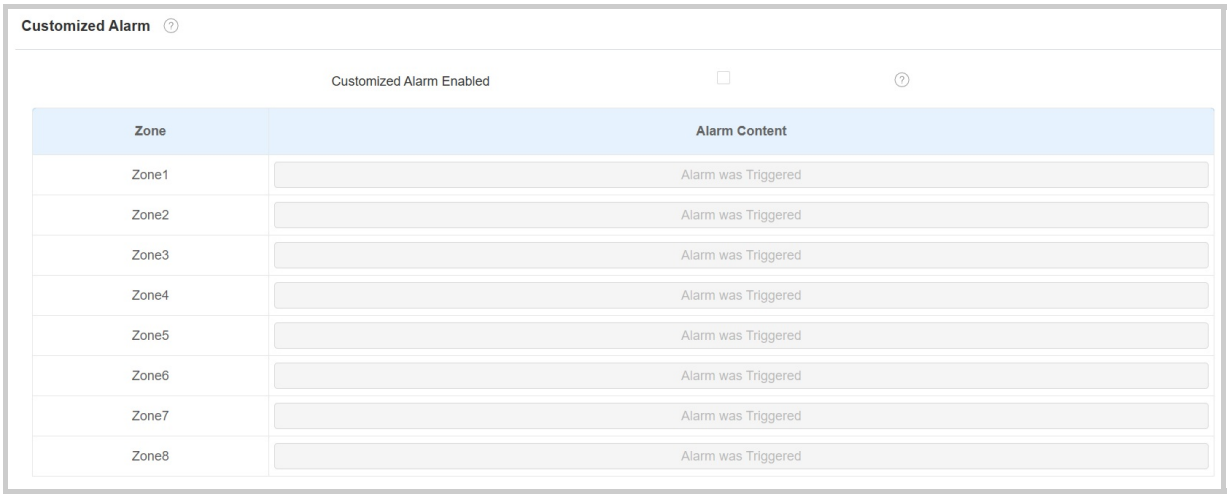
To check the alarm log, go to the **Arming > Alarm Log** screen.



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.

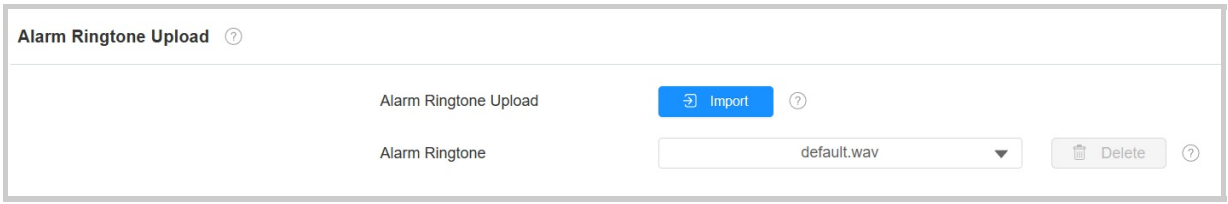
To set it up, navigate to the web **Arming > Zone Setting > Customized Alarm** interface.



- **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.



Note

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

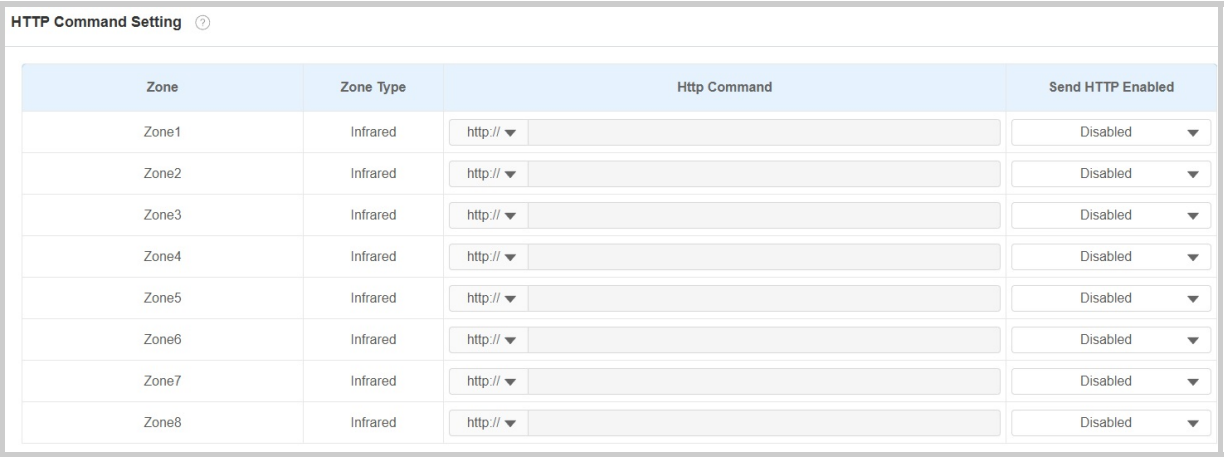
Alarm Action Configuration

When the alarm sensor is triggered, it can start different actions, such as HTTP commands, SIP messages, calls, and local relay activation after setup.

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

Alarm Action via HTTP Command

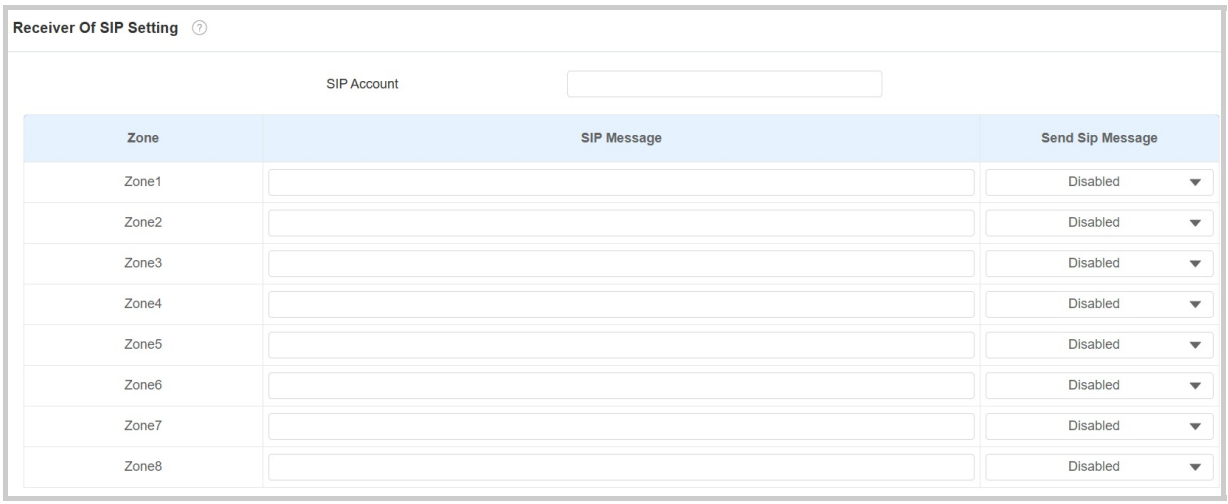
To set up the HTTP command action, you can select **Enabled** in the **Send HTTP** field to enable the actions for the alarm sensor installed in different locations. Then enter the HTTP command provided by the device manufacturer on which the action is to be carried.



- **Zone Type**: Display the zone type set on the **Arming > Zone Setting** interface.
- **HTTP Command**: Enter the HTTP command provided by the third-party device manufacturer.
- **Send HTTP Enabled**: Enable it if you want the action to be implemented on a designated third-party device.
- **Send Delay**: This option is only available when the Zone Type is **Motion** and Send HTTP is enabled. When enabled, the HTTP command will be sent in a delay time that is the same as the **Alarm Delay** set on the **Arming > Arming Mode** interface.

Alarm Action via SIP Message

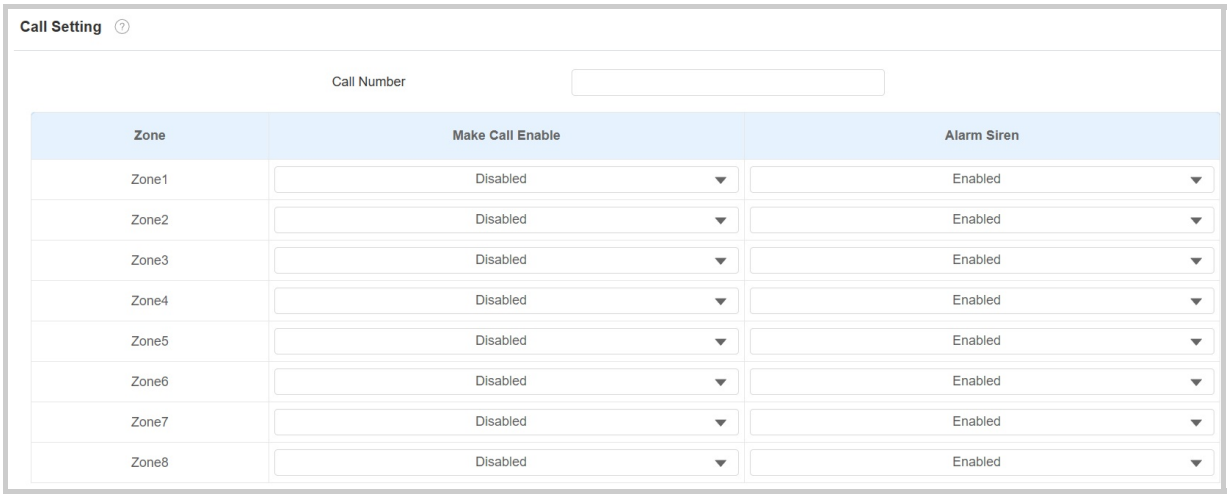
The device can send messages to a designated device when the alarm is triggered. To set this up, enter a SIP number or IP address along with the message content.



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

Alarm Action via SIP Call

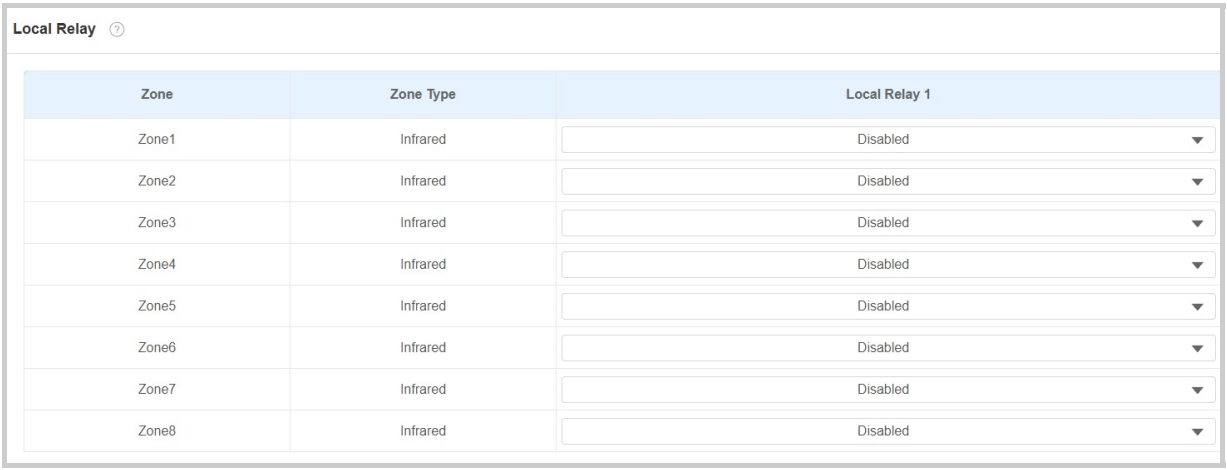
To enable the device to make a call when the alarm is triggered, enter the SIP or IP number of the called party. Additionally, you can allow the indoor monitor to sound a siren simultaneously.



- **Call 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.

Alarm-Triggered Local Relay

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

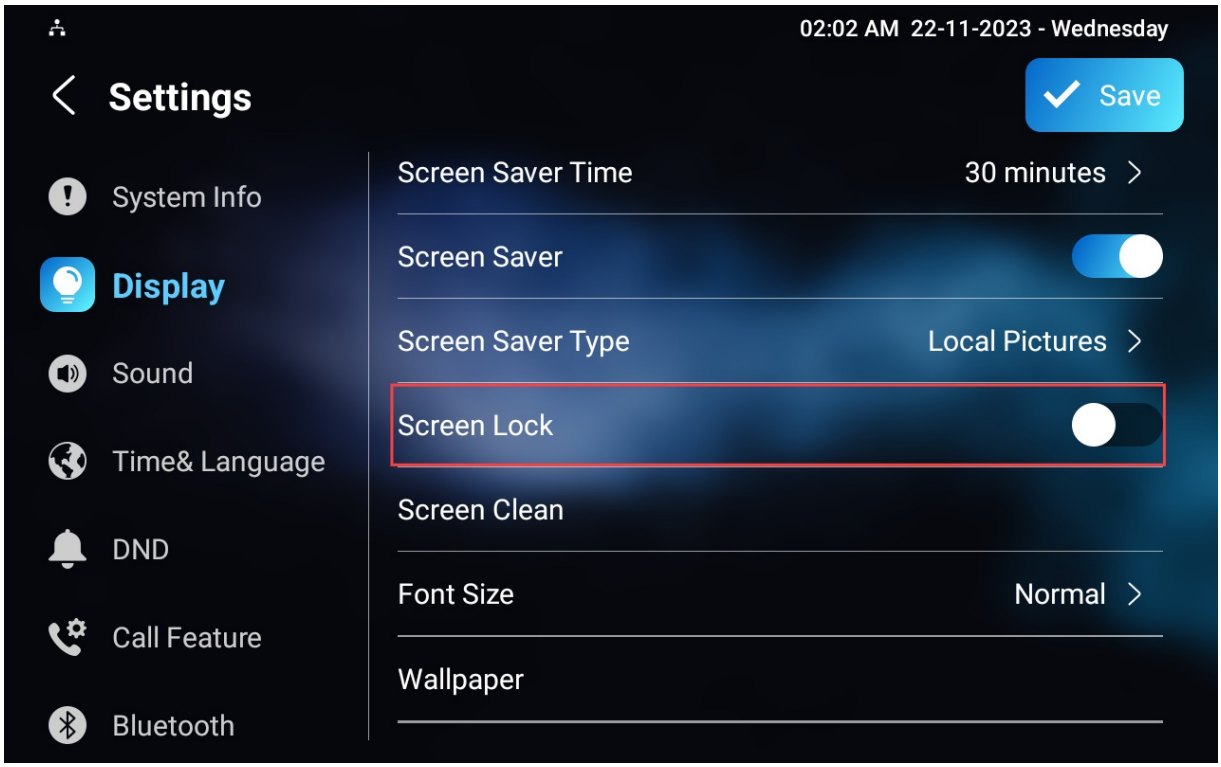


- **Zone Type**: Display the zone type set on the **Arming > Zone Setting** interface.
- **Local Relay1**: Enable it if you want the local relay to be triggered with the sensor.
- **Open Delay**: This option is only available when the Zone Type is **Motion** and Local Relay 1 is enabled. When enabled, the relay will be triggered in a delay time that is the same as the **Alarm Delay** set on the **Arming > Arming Mode** interface.

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.

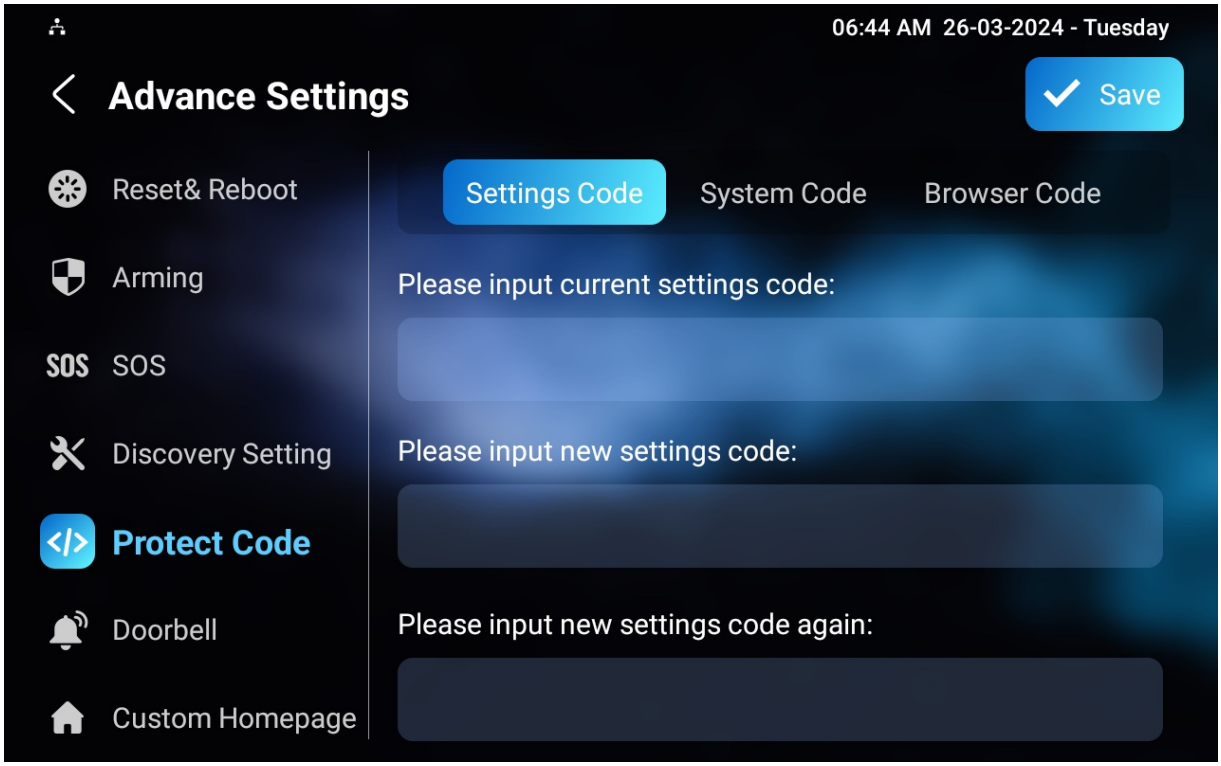
You can enable the screen lock function directly on the device **Settings > Display** screen.



Screen Unlock by PIN Code

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

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

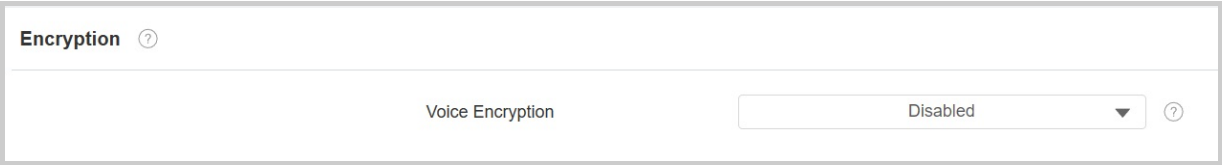


> **Note**
>
> The default password is 123456.

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.

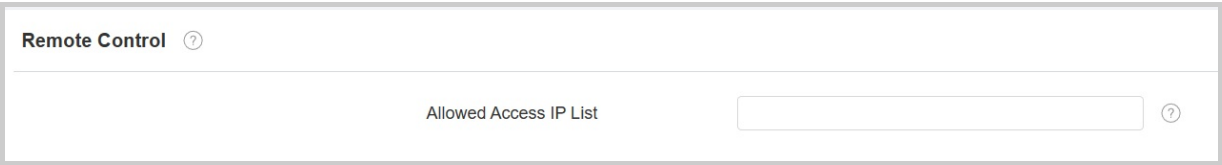


- **Voice Encryption**:
  - **Disabled**: The call will not be encrypted.
  - **SRTP(Compulsory)**: All audio signals(technically speaking it is RTP streams) will be encrypted to improve security.
  - **SRTP(Optional)**: Encrypt the voice from the caller. If the caller also enables SRTP, the voice signals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

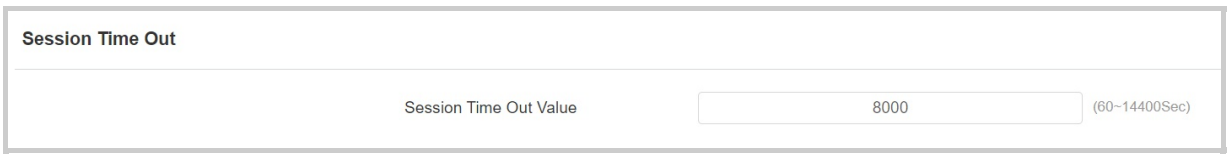


- **Allowed Access IP List**: Set up the server IP address that can be allowed to send the HTTP commands to the indoor monitor.

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.

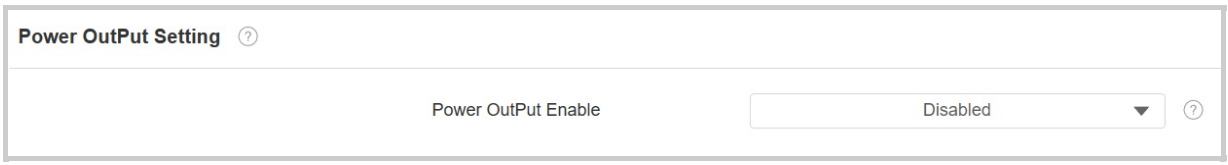
To set it up, go to the web **Security > Basic > Session Time Out** interface.



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.

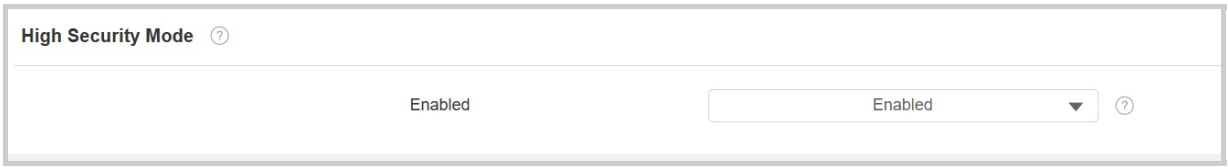
To enable it, go to **Settings > Basic > Power Output Setting** interface.



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.auto



Important Notes

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

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

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

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

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

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

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

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

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

Lift Control

You can summon a lift via the lift control feature.

Configure Lift Control

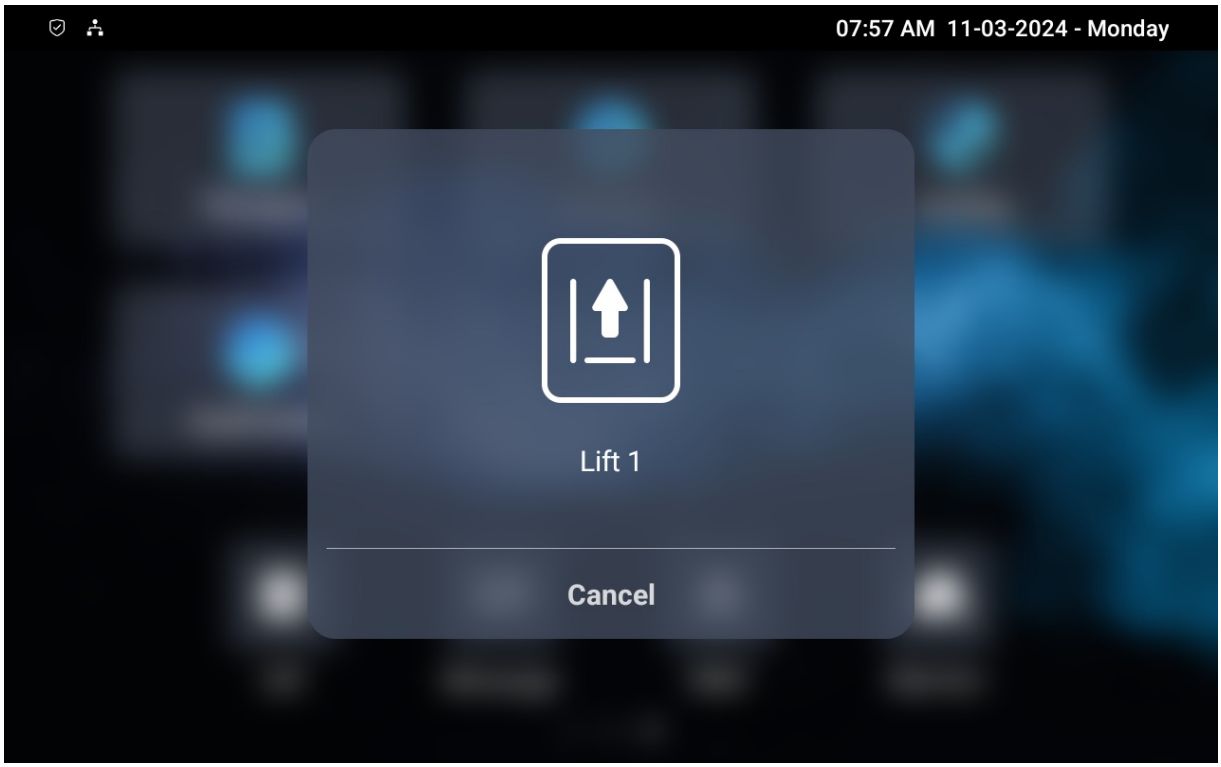
Before setting the Lift icon, display it on the Home or More screen.

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

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

- **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.



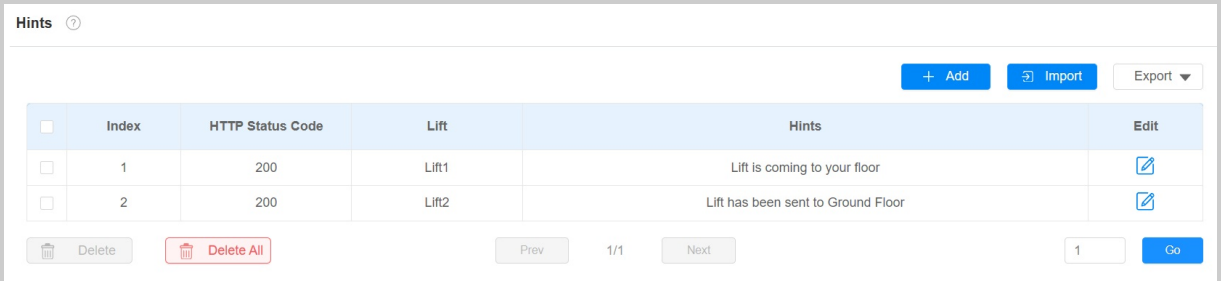
Note

Click here to view the detailed configuration of lift control on indoor monitors.

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.



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

Voice Assistant

Albert is a voice assistant from Akuvox. It can help you with intercom calls, door opening, arming modes, and other functions. As for the door access control, you can choose which relay to activate by this voice assistant.

To set it up, go to the device **Settings > Voice Assistant** screen.

- **Language Type**: Select the language. Currently, only English and Chinese are supported.
- **Recognition Sensitivity**: Adjust the voice assistance recognition sensitivity among Low, Normal, and High.
- **Talk Mode**: When Talk Mode is enabled, the voice assistant will stay on to receive the voice commands for 30 seconds without calling **Albert** again to wake up the voice assistant. When disabled, the voice assistant will wake up for each voice command.
- **Not Disturb At Night**: This function is applied when users want the voice assistant to stay silent while carrying out what it is made to do according to the voice commands.
- **Supported Commands**: Tap to check the supported commands. Enable or disable the command(s).

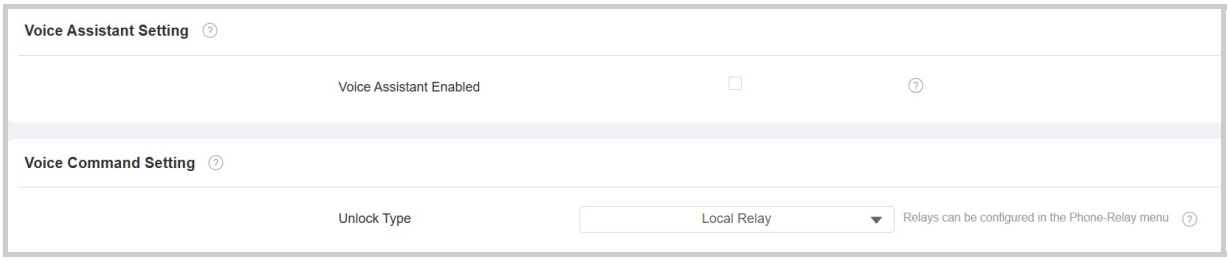
- **Answer Call Permission**: Enable it to answer or reject the incoming call via voice assistant by replying "Yes" or "No".
- **Call Fuzzy Match**: Enable it to allow fuzzy matching of the contact name, for example, if users have Tom and Tomy in their contacts, then Tomy will also appear when they call Tom, and they are required to select the right contact manually.

Please see the voice command details below:

NO	Voice Command	Description	Voice Prompt
1	Intruder mode off	Use it when you want to clear the arming mode when the arming alarm is triggered. (you are required to enter the disarm password in the pop-out window initiated by the voice assistant)	Please Input Password
2	Clear arming	ibid	ibid
3	night mode	Use it when you want to change the arming mode to night mode	• Started it, sweet dreams! • Made it, good night • Sure, sleep mode is on • OK, start sleep mode, have a good night Alright, sleep mode is opened, have a nice dream
4	sleep mode	Use it when you want to change the arming mode to sleep mode	• Sure, sleep mode is on • OK, start sleep mode, have a good night • Alright, sleep mode is opened, have a nice dream • Made it, good night • Started it, sweet dreams!
5	away mode	Use it when you want to change the arming mode to away mode	• Sure, away mode is on • OK, start away mode • Alright, away mode is opened • Made it • Made it, have a good day • Done, away mode is started
6	home mode	Use it when you want to change the arming mode to home mode	• Sure, home mode is on • OK, start home mode • Alright, home mode is opened • Made it • Done, home mode is started
7	open door	Use it when you want to open the door	• Sure, the door is open • The door is open for you • No problem, open the door • Opened, always here for you Yep, door is opened now
8	open the door	Use it when you want to open the door	• Sure, the door is open • The door is open for you • No problem, open the door • Opened, always here for you Yep, door is opened now

9	disable DND	Use it when you want to disable the DND mode	• Yes, closed it for you • Welcome back, DND is off • DND is closed, to mingle with the world • Sure, DND is off
10	enable DND	Use it when you want to enable the DND mode	• OK, DND is on • Done, enjoy yourself • DND is on, feel your inner peace • Turn on it now
11	emergency	Use it when you want to dial SOS number	• Got it, calling SOS as soon as possible • OKay, be relaxed, making a emergency call now • Calling ambulance now • Calling SOS now, please hold on • God bless you, calling emergency now • Hold on please, calling emergency right now • Take it easy, calling emergency right now
12	help me	ibid	ibid
13	call manager	use it when you want to call "manager" you name set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
14	call staff	use it when you want to call "stuff" you named and set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
15	call carer	use it when you want to call "carer" you named and set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
16	open message	use it when you want to check text message.	• Got it, please check • OK, message is opened, you can write some contents to send • Message is ready for you • already opened it for you
17	open monitor	use it when you want to check monitor	Got it , please check
18	homepage	use it when you want to go to home screen	• Home page is already for you. Already got it for you
19	enable mute	use it when you want to mute your voice on the indoor monitor so that the caller or callee will be not be able to hear you.	• OK, mute is on • Done, enjoy yourself • Mute is on, feel your inner peace • Set it now
20	disable mute	use it when you want to unmute your voice on the indoor monitor so that the caller or callee will be able to hear you.	• Sure, mute is off • Mute is closed, to mingle with the world • Welcome back, mute is off • Yes, closed it for you
21	shut down/cancel	Use it when you want to turn off the voice assistant function.	• See you • See you later • Bye • Good bye • See you next time • Bye, best regards • See you, have a great time

To enable the voice assistant and set the voice assistant-controlled relay, go to the web **Settings > Voice Assistant** interface.

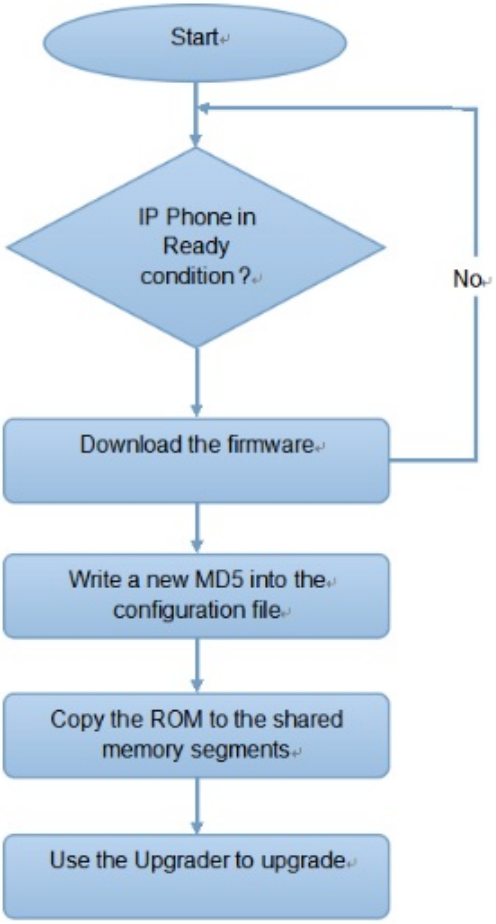

Voice Assistant Setting
Voice Assistant Enabled
Voice Command Setting
Unlock Type
Local Relay
Relays can be configured in the Phone-Relay menu

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

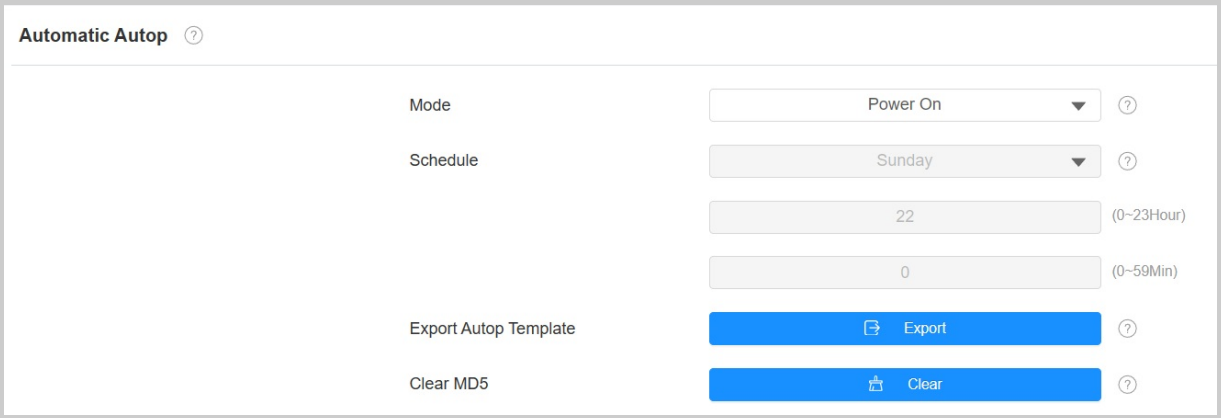
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

Autop Schedule

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

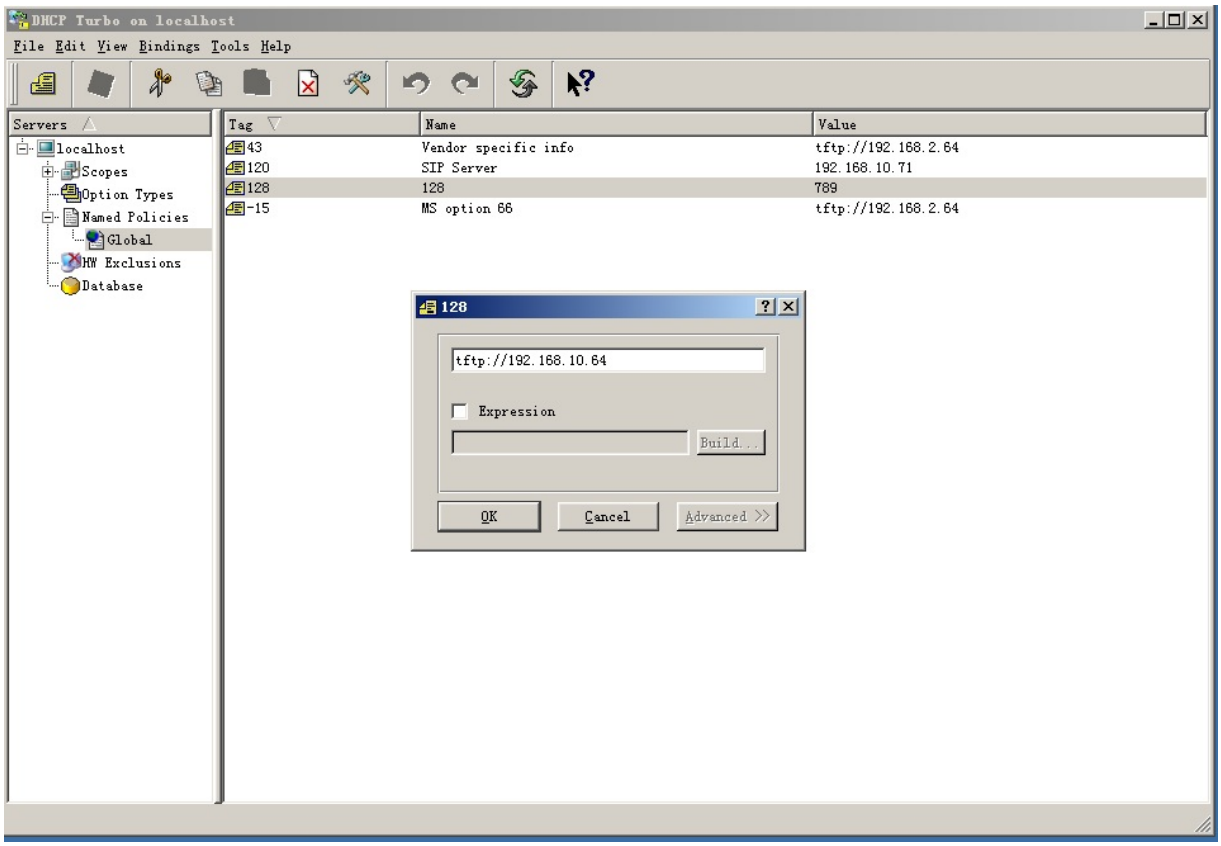
To set up the schedule, go to the web **Upgrade > Advanced > Automatic Autop** interface.



- **Mode**:
  - **Power On**: the device will perform Autop every time it boots up.
  - **Repeatedly**: the device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: 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

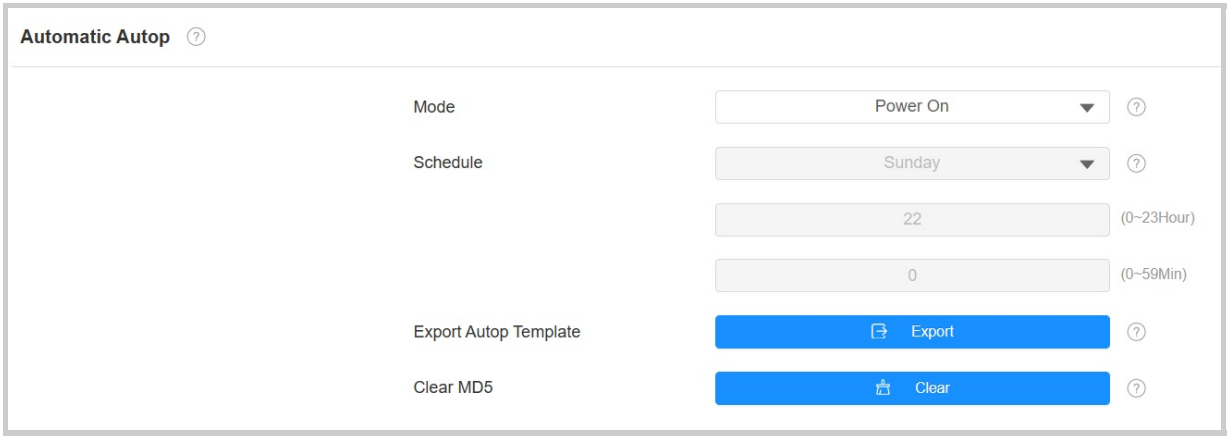
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option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



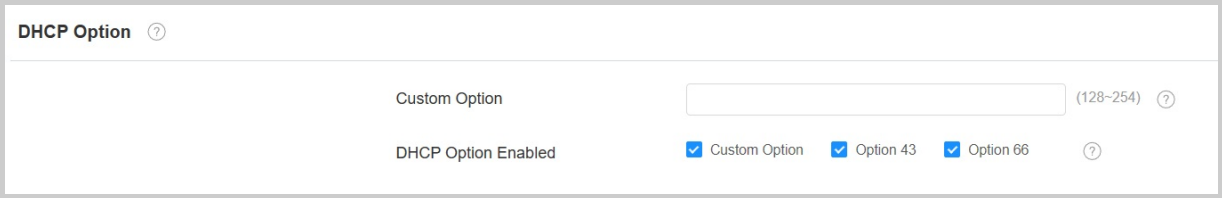
Note

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

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



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

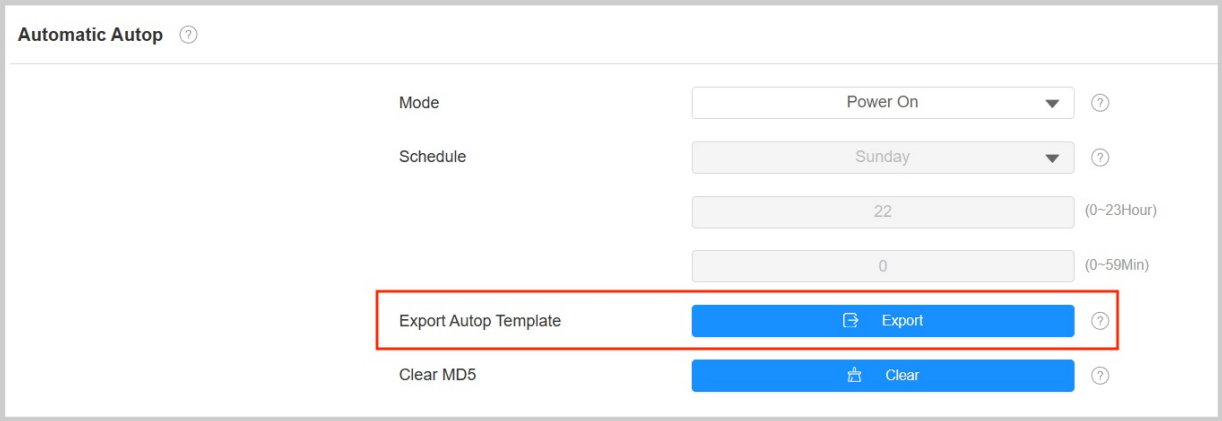


- **Custom Option**: Enter the DHCP code that matches with corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 43**: If the device does not get a URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done 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.

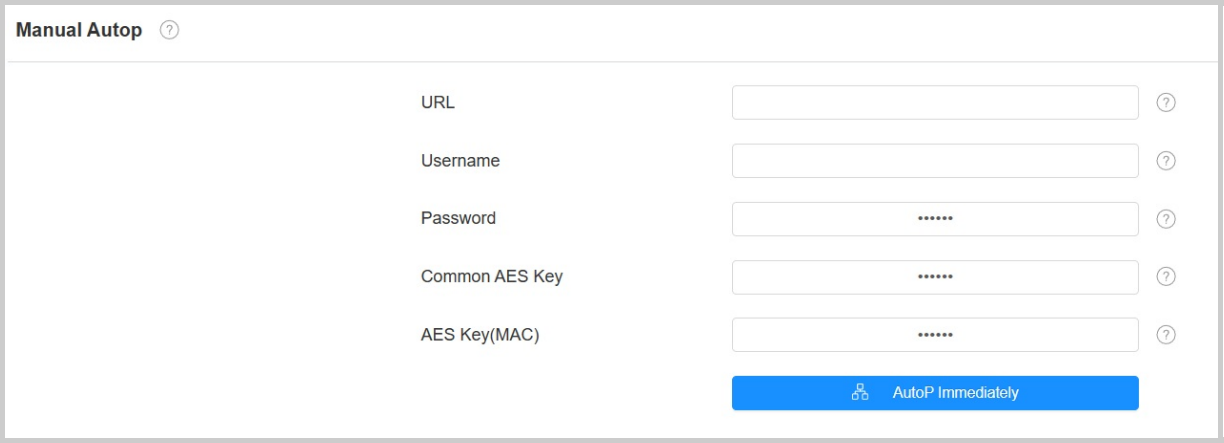
Static Provisioning Configuration

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.



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



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

Note

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

Tip

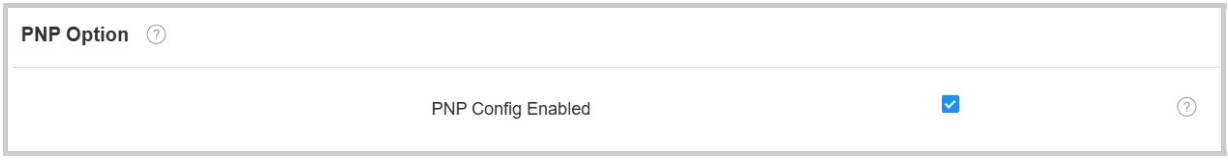
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

Click here to watch the configuration video.

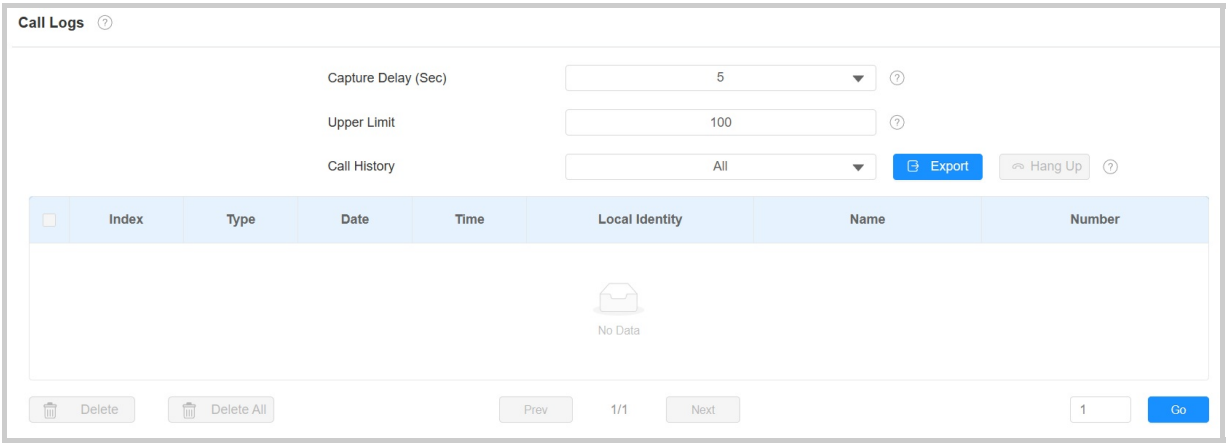
To enable the function, go to the **Upgrade > Advanced > PNP Option** interface.



Call Logs

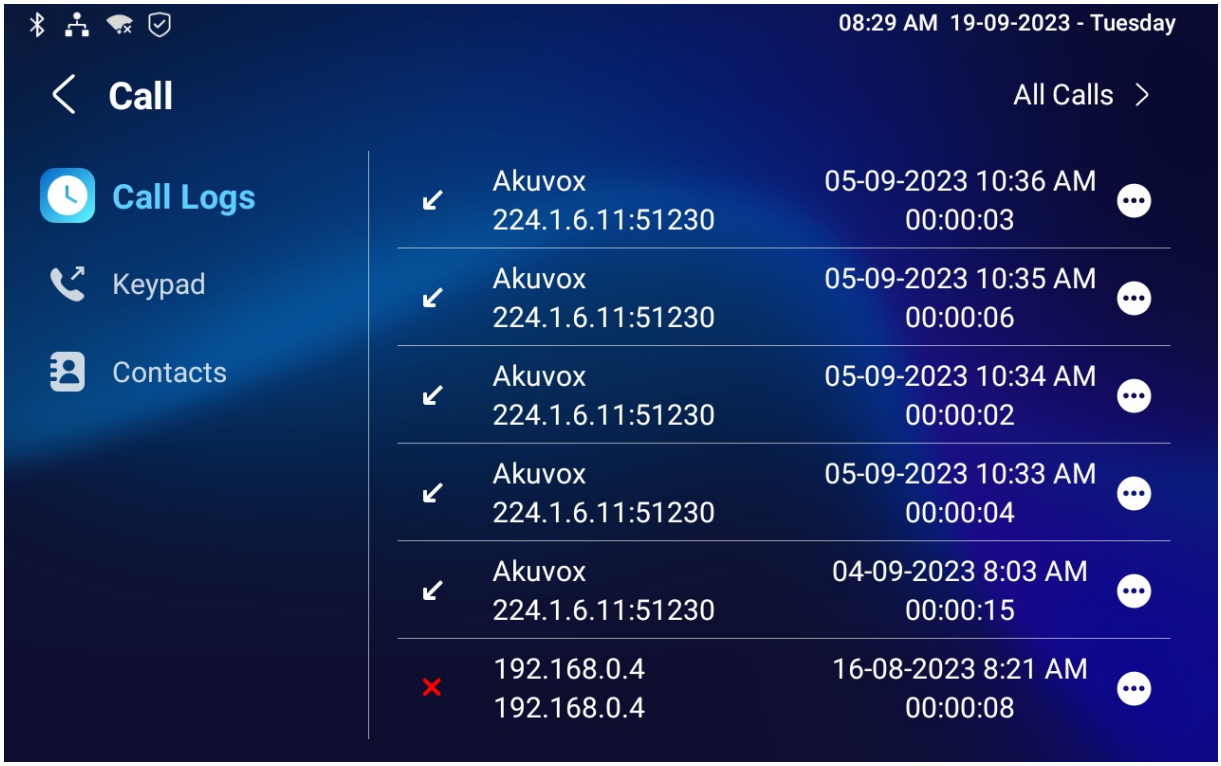
To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

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



- **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.

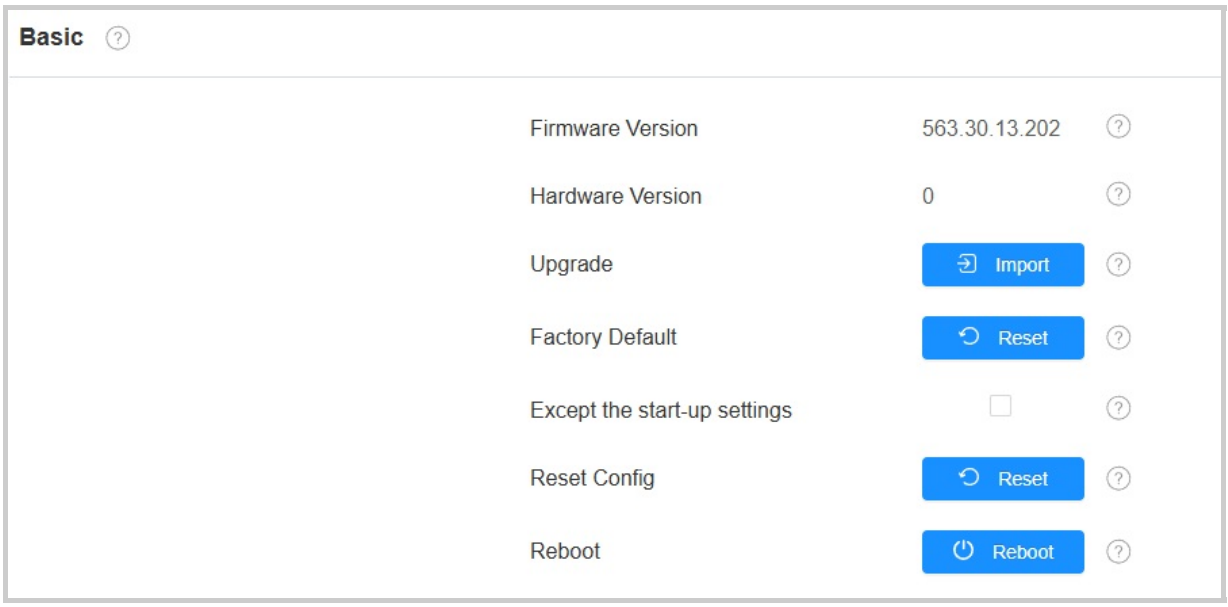
To check call logs on the device, tap **Call > Call Logs**.


08:29 AM 19-09-2023 - Tuesday
Call
All Calls
Call Logs
Keypad
Contacts
Akuvox
224.1.6.11:51230
05-09-2023 10:36 AM
00:00:03
Akuvox
224.1.6.11:51230
05-09-2023 10:35 AM
00:00:06
Akuvox
224.1.6.11:51230
05-09-2023 10:34 AM
00:00:02
Akuvox
224.1.6.11:51230
05-09-2023 10:33 AM
00:00:04
Akuvox
224.1.6.11:51230
04-09-2023 8:03 AM
00:00:15
192.168.0.4
192.168.0.4
16-08-2023 8:21 AM
00:00:08

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



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.

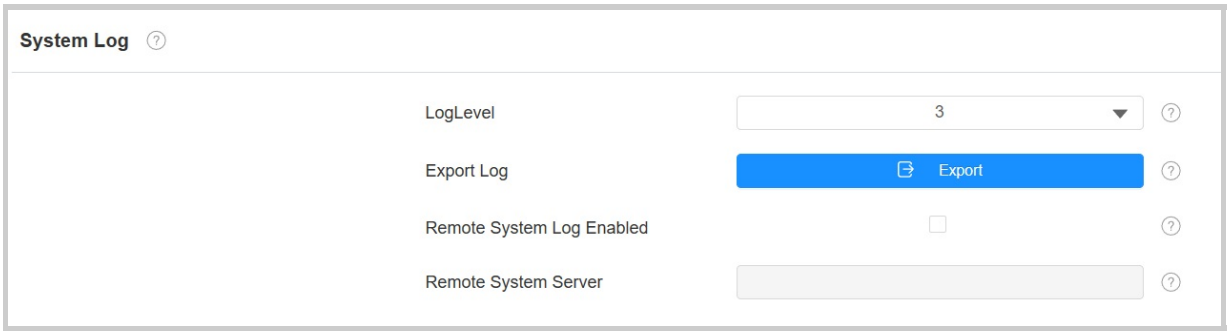
The import file should be in TGZ, CONF, or CFG format.

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.

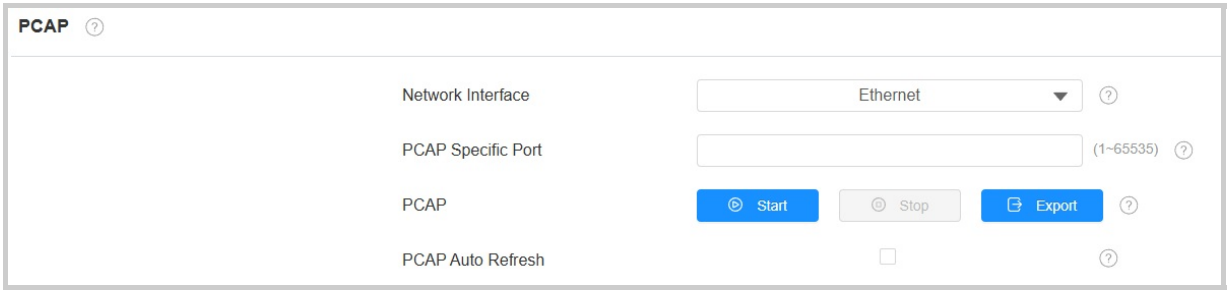


- **Log Level**: Log level ranges from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export 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.

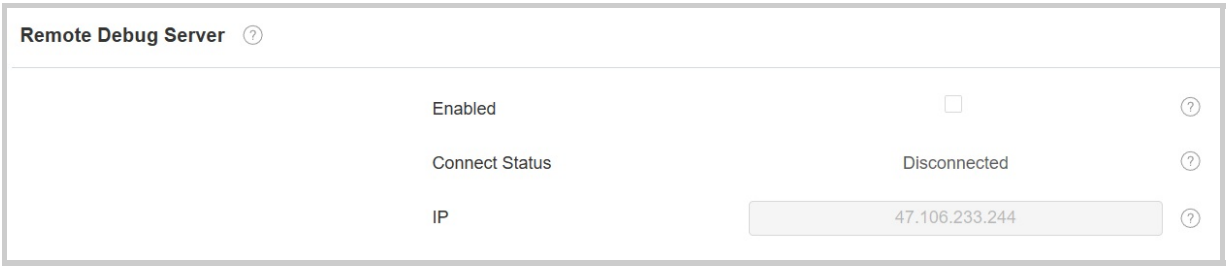


- **Network Interface**: Specify the network interface based on the device's network connection.
    - **Ethernet**: The captured data is from the wired network packets.
    - **WLAN**: The captured data is from the wireless network packets.
- **PCAP Specific Port**: Select the specific port from 1-65535 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.



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

User Agent

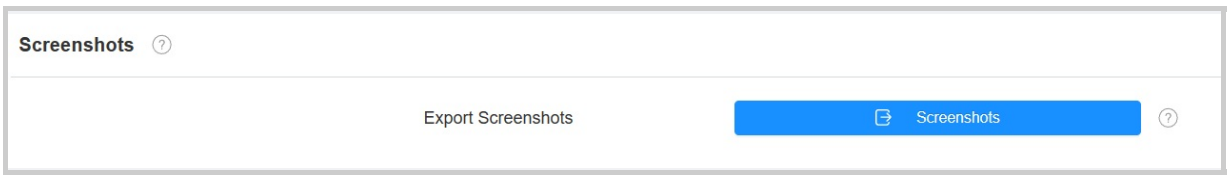
User agent is used for identification purpose when you are analyzing the SIP data packet.

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

Screenshots

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

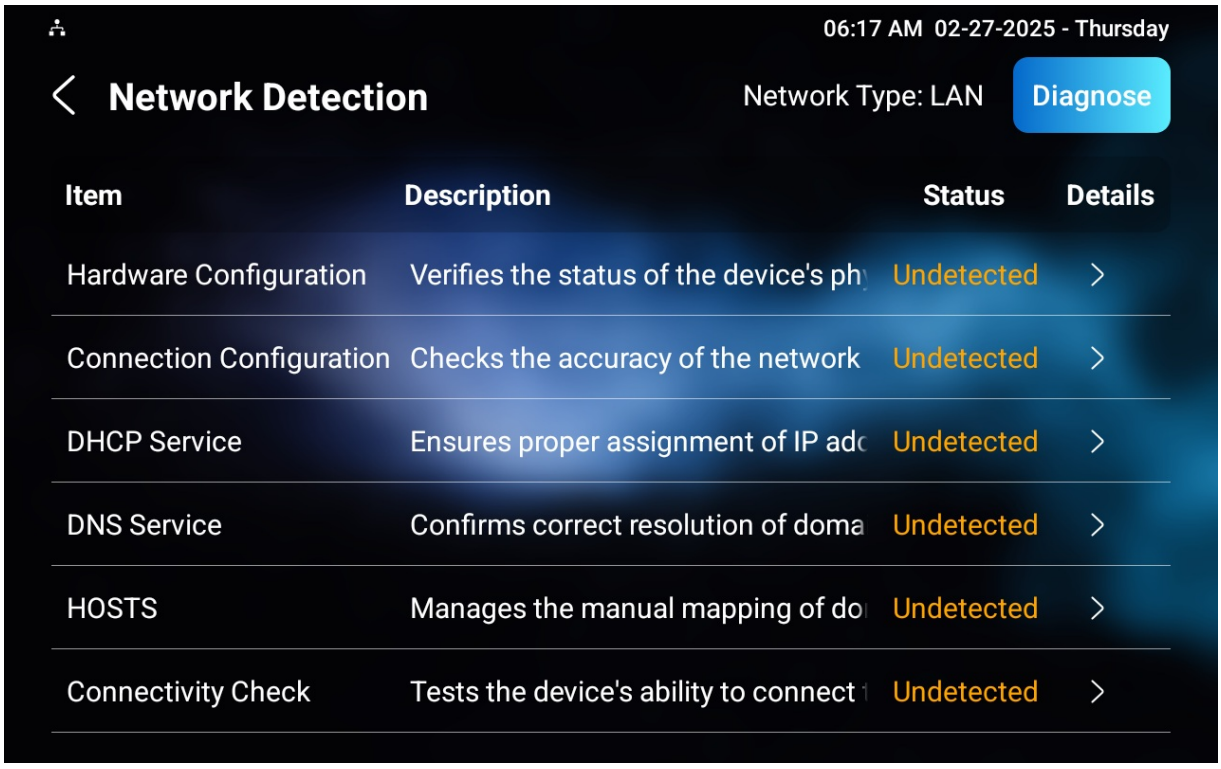
To take screenshots, go to **Upgrade > Diagnosis > Screenshots** interface. Click **Screenshots** to capture the current screen.



Network Detection

The network detection feature allows for troubleshooting network problems quickly.

Set it up on the **Settings > Network Detection** screen.



- **Diagnose:** Tap to start detection.

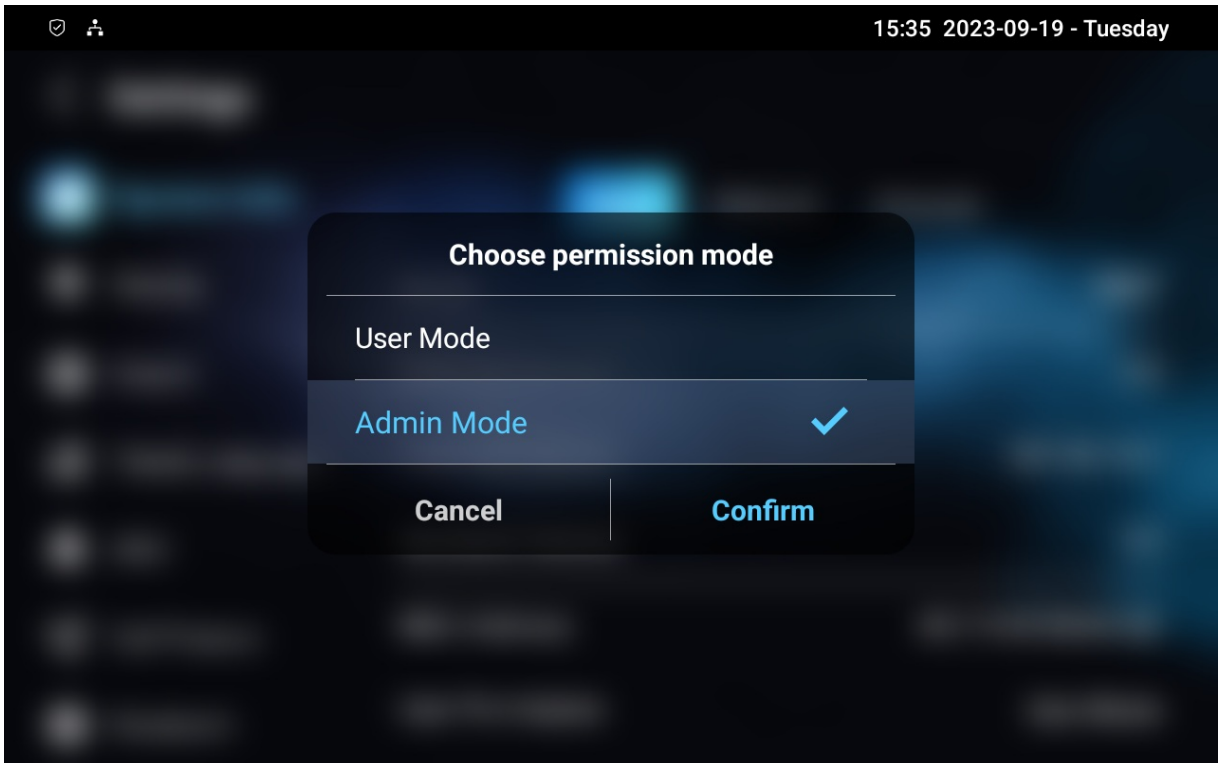
- **Status**: Display a loading icon when the detection starts; display ✔ for normal results and X for abnormal results.
- **Details**: Tap to view the detection details.

Integration with Third-party Devices

Enter Applications Screen

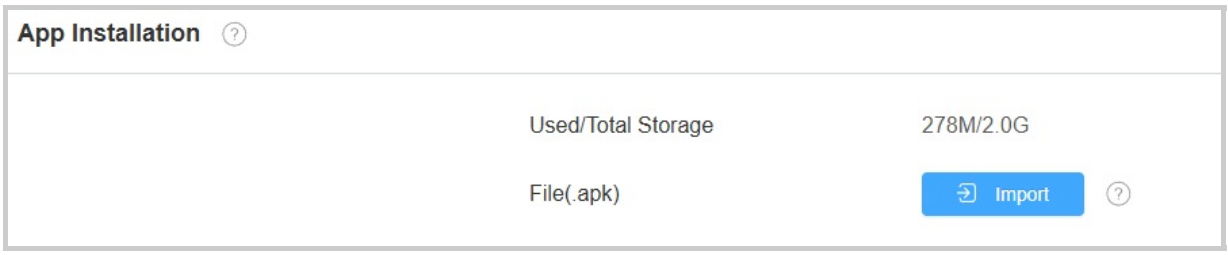
The indoor monitor supports **User** and **Admin** modes. In Admin mode, you can access both the third-party and default applications.

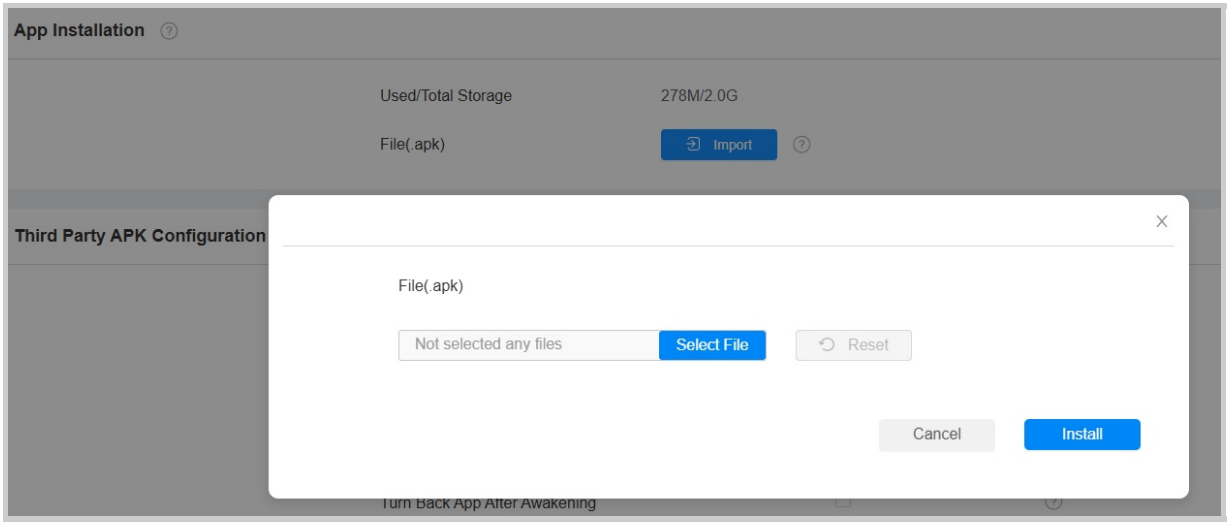
Go to the **Settings > System Info** interface. Tap on **User Mode** 10 times. Then select **Admin Mode** and tap Confirm.



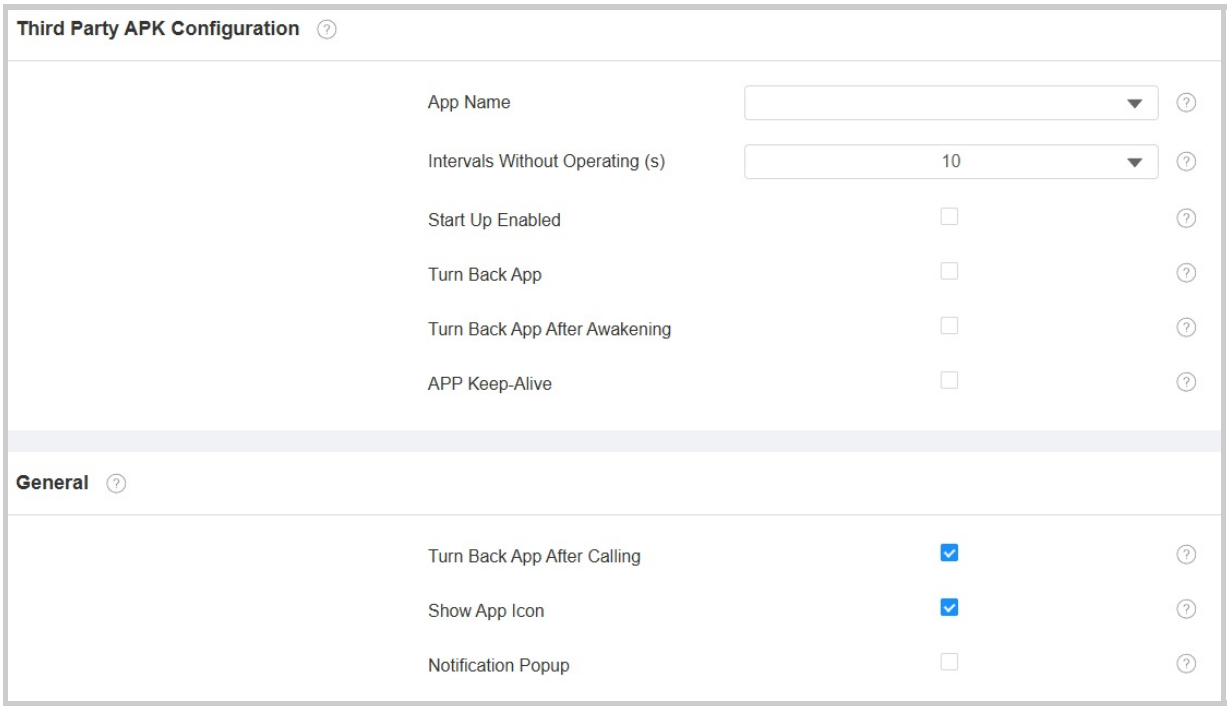
Install and Configure Third-party App

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.



- **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.

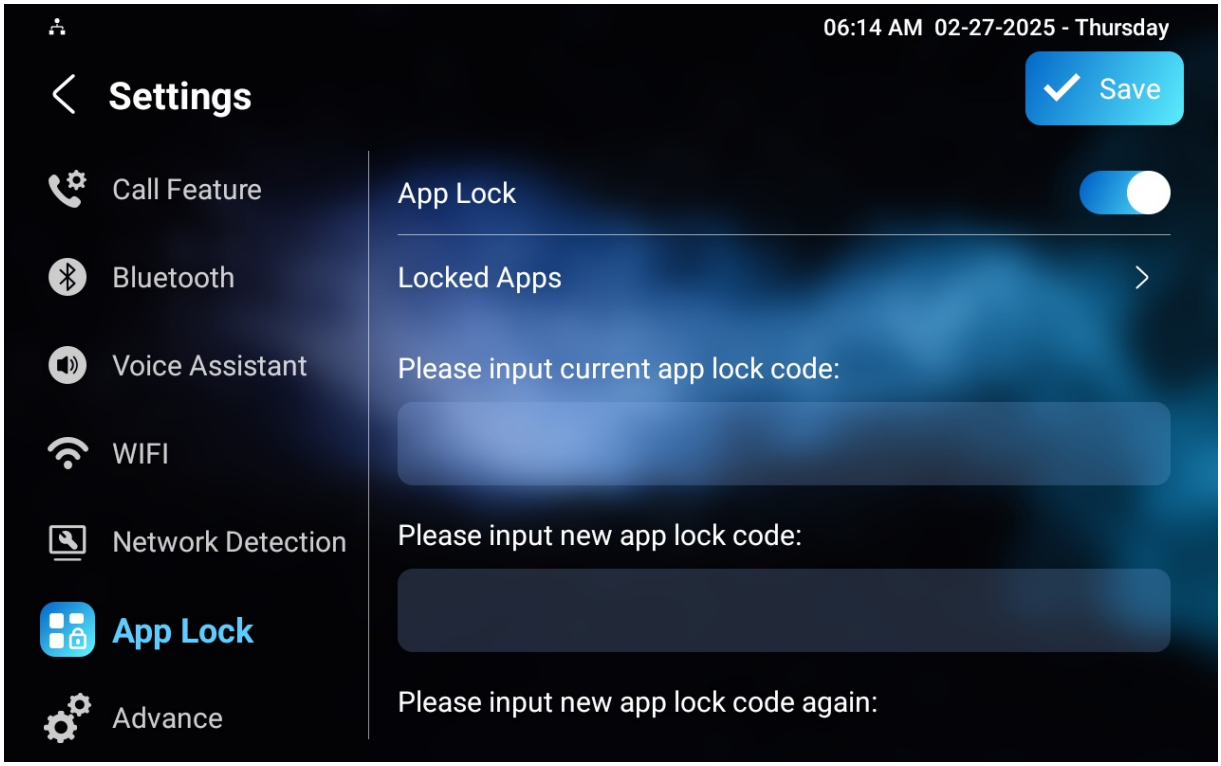
- **Start Up Enabled**: Allow the app to run automatically when the device is turned on.
- **Turn Back App**: Allow automatic returning to the app.
- **Turn Back App After Awakening**: Allow the device to return to the app when the screen is awakened.
- **APP Keep-Alive**: Allow the app to stay running 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.
- **Notification Pop-up**: If enabled, the device will have a sound alert and pop-up notification when receiving notifications from third-party apps.

App Lock

The App Lock feature prevents abused access to third-party apps by requiring users to enter a password before accessing them.

It is available when third-party apps are installed on the device.

Set it up on the **Settings > App Lock** screen. It is disabled by default.

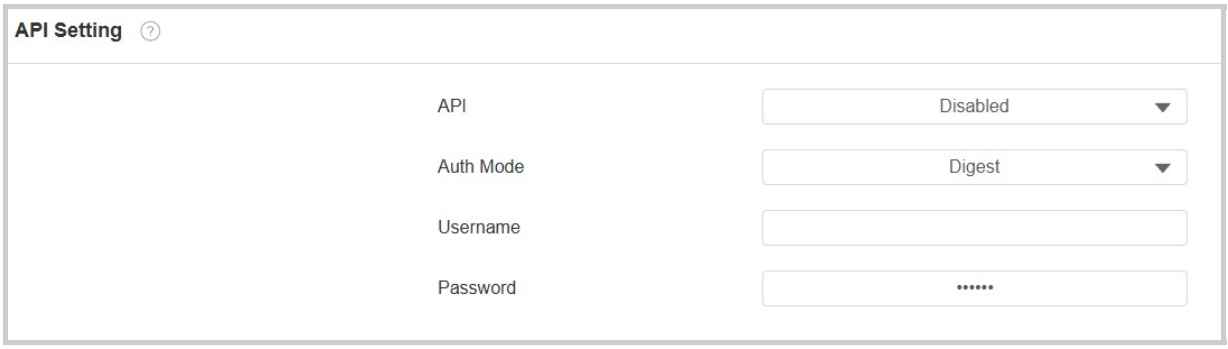


- **Locked App**: Select the app to apply this feature.
- **Lock Code**: The default code is 123456.

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.

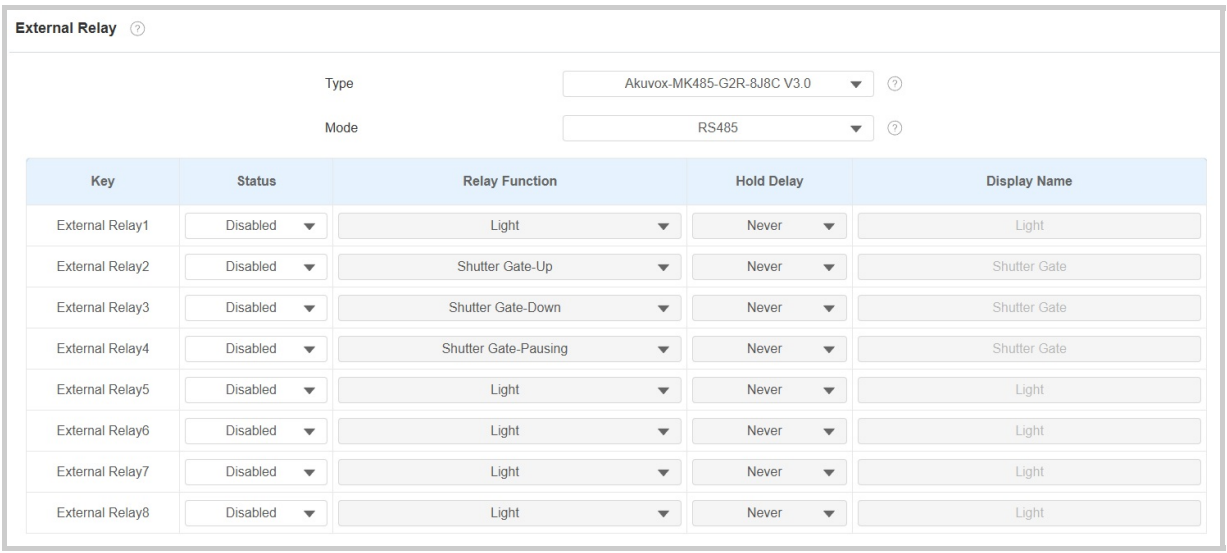


- **HTTP API:** When the function is disabled, any request to initiate the integration will be denied and be returned HTTP 403 forbidden status.
- **Auth Mode**:
  - **Allowlist**: You are required to fill in the IP address of the third-party device for authentication. It is suitable for operation in LAN.
  - **Digest**: 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.

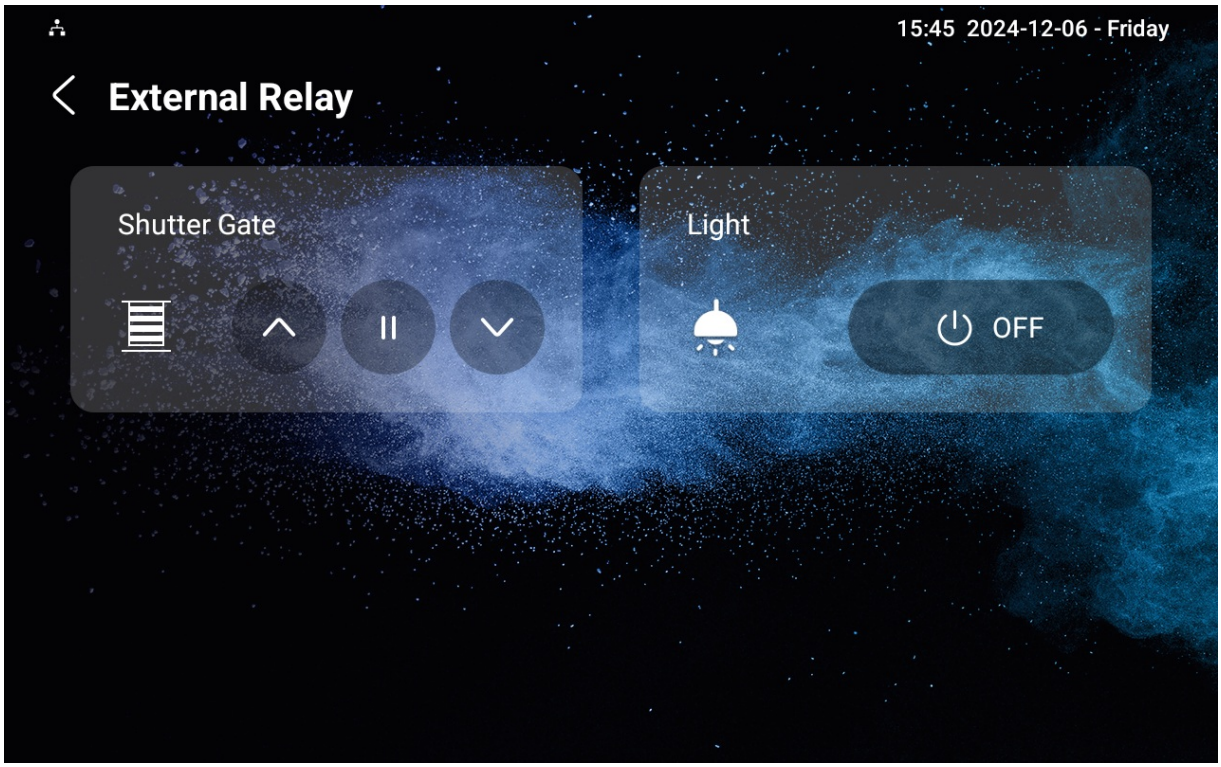
Integration via External Relay

Users can control akubela or third-party smart home devices on the indoor monitor through an external relay controller.

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



- **Type**: Select the external relay type.
- **Mode**: Set the external relay mode based on its connection with the indoor monitor. If it is the akubela RSAC-C1-R8, this option is RS485 by default.
- **Status**: Enable/disable the relay.
- **Relay Function**: Set the relay function based on the smart home devices connected.
- **Hold Delay**: Specify the relay reset time from 1 to 60 seconds. **Never** means it keeps activated once it is triggered. By default, it is 3 seconds for Door and Others relay functions and Never for other functions.
- **Display Name**: Set the tab's name displayed on the indoor monitor's External Relay screen.



Note

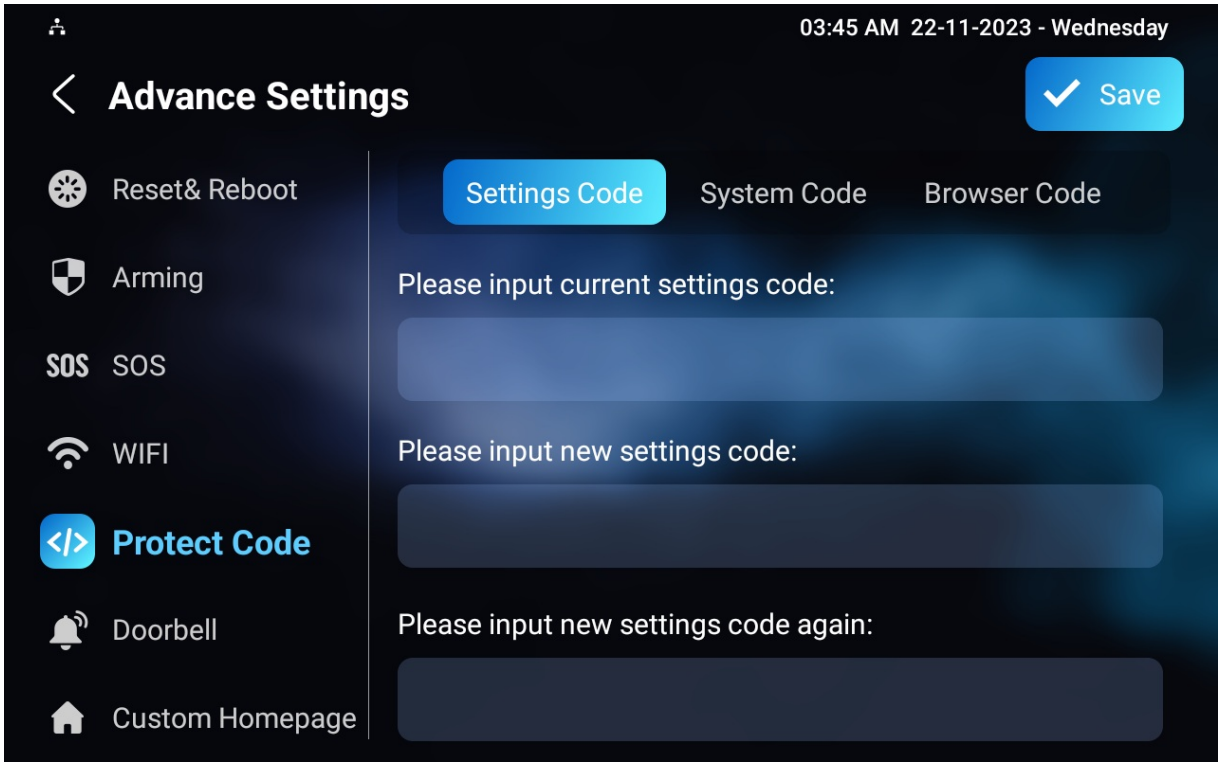
- To display the External Relay button on the home screen, set it up on the **Device > Display Setting** interface.
- Click **here** to view the detailed configuration of the external relay feature.

Password Modification

Modify Device Basic Setting Password

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

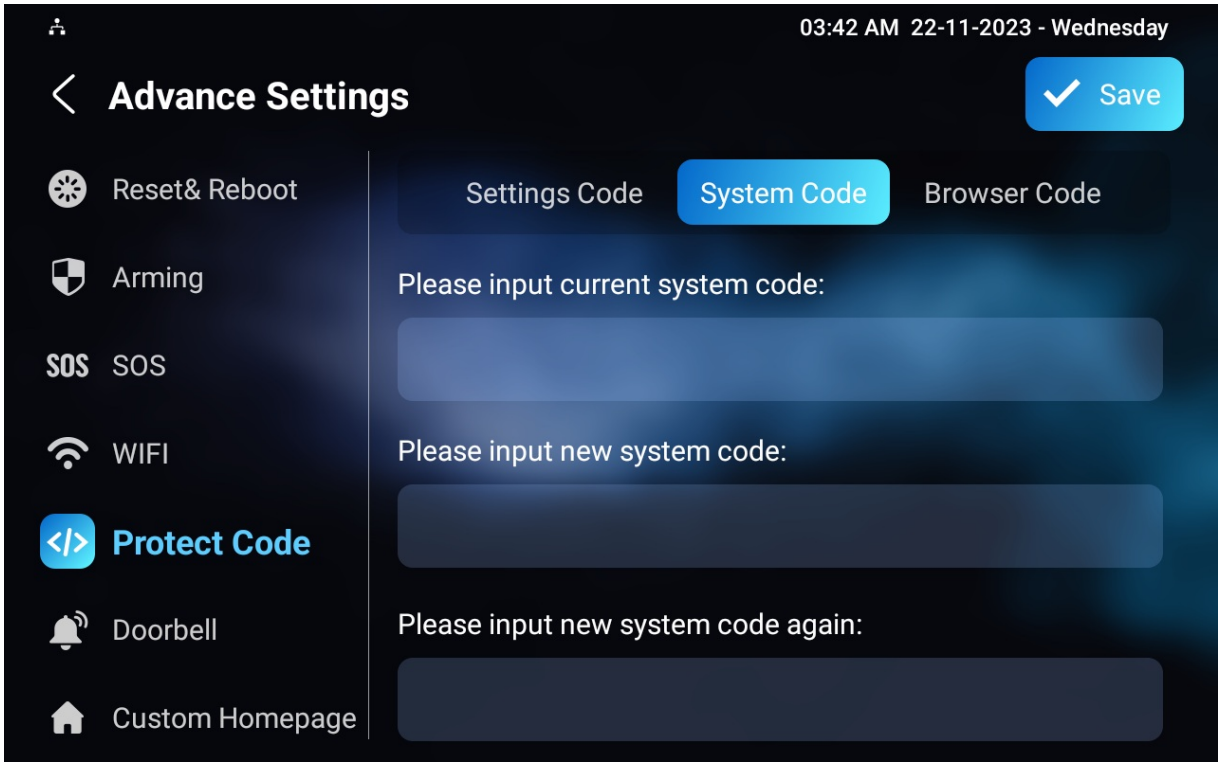
To modify it, go to the **Settings > Advance Settings > Protect Code** screen and select **Settings Code**.



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.

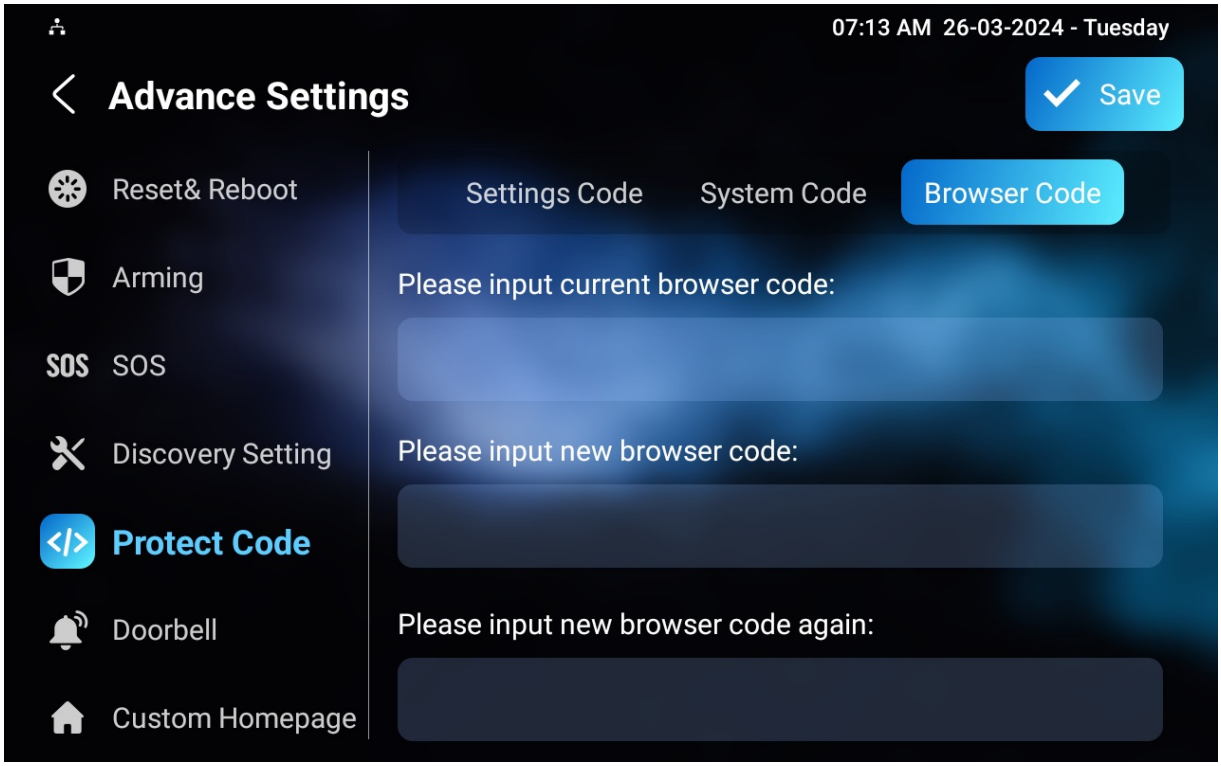
To modify it, navigate to the **Settings > Advance Settings > Protected Code** screen and select **System Code**.



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.

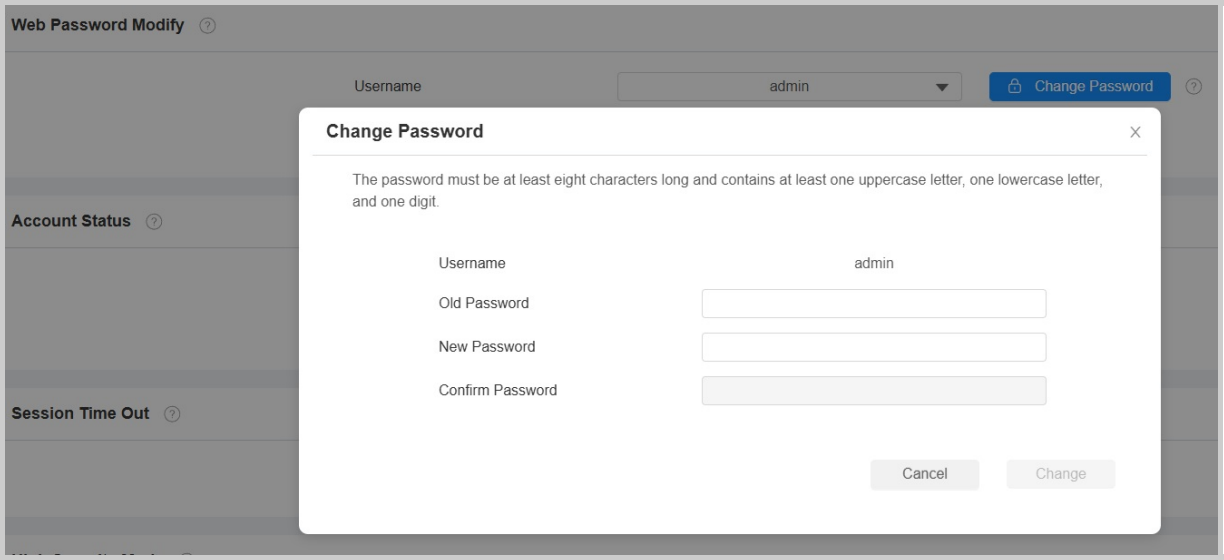
To modify it, go to the **Settings > Advance Settings > Protected Code** screen and select **Browser Code.**



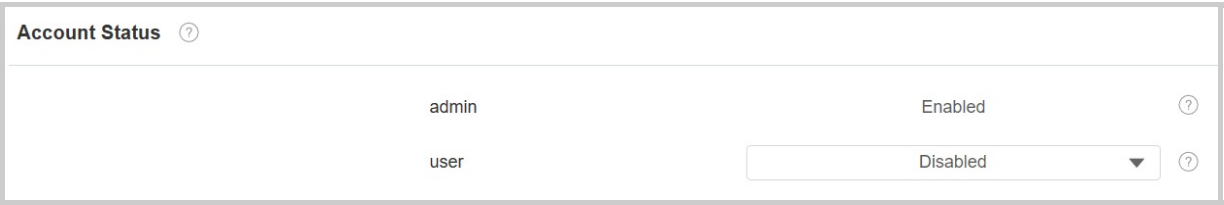
Modify Device Web Interface Password

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.



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



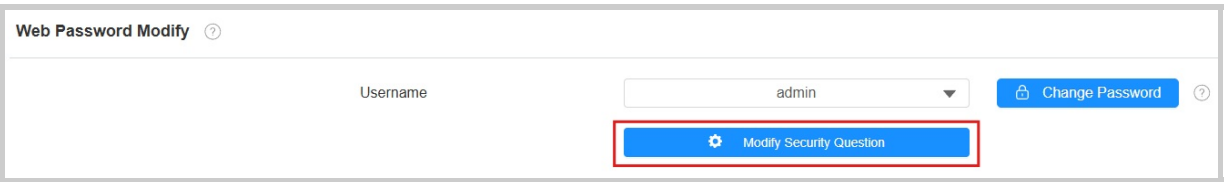
> **Note**
>
> There are two accounts, one is admin, its password is admin, the other is user, and its password is user.

Modify Security Questions

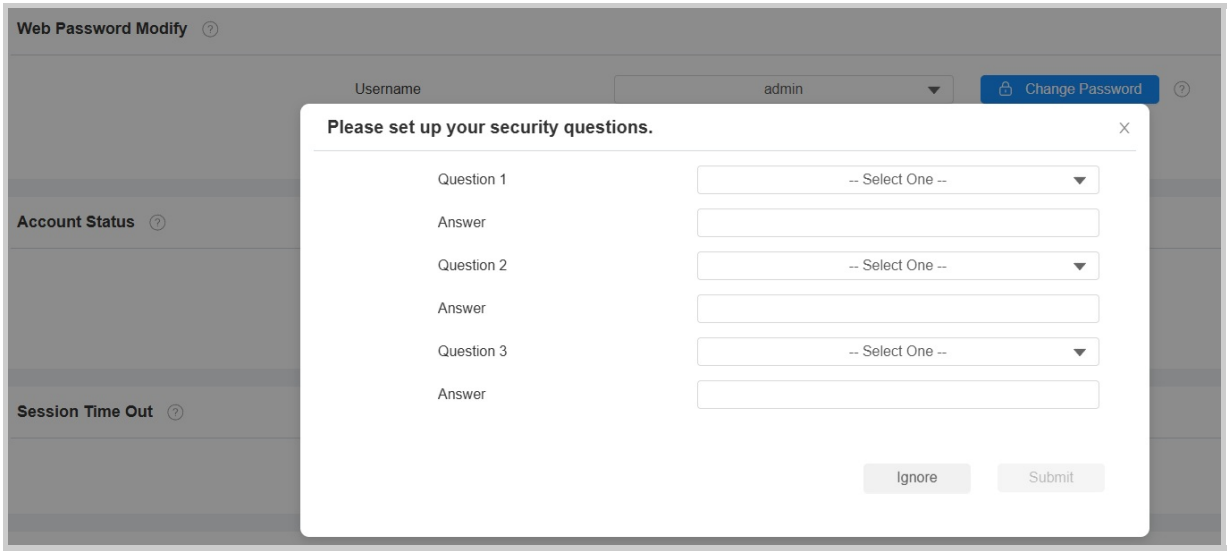
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

To set it up, go to the **Security > Basic** interface. Click Modify Security Questions.



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



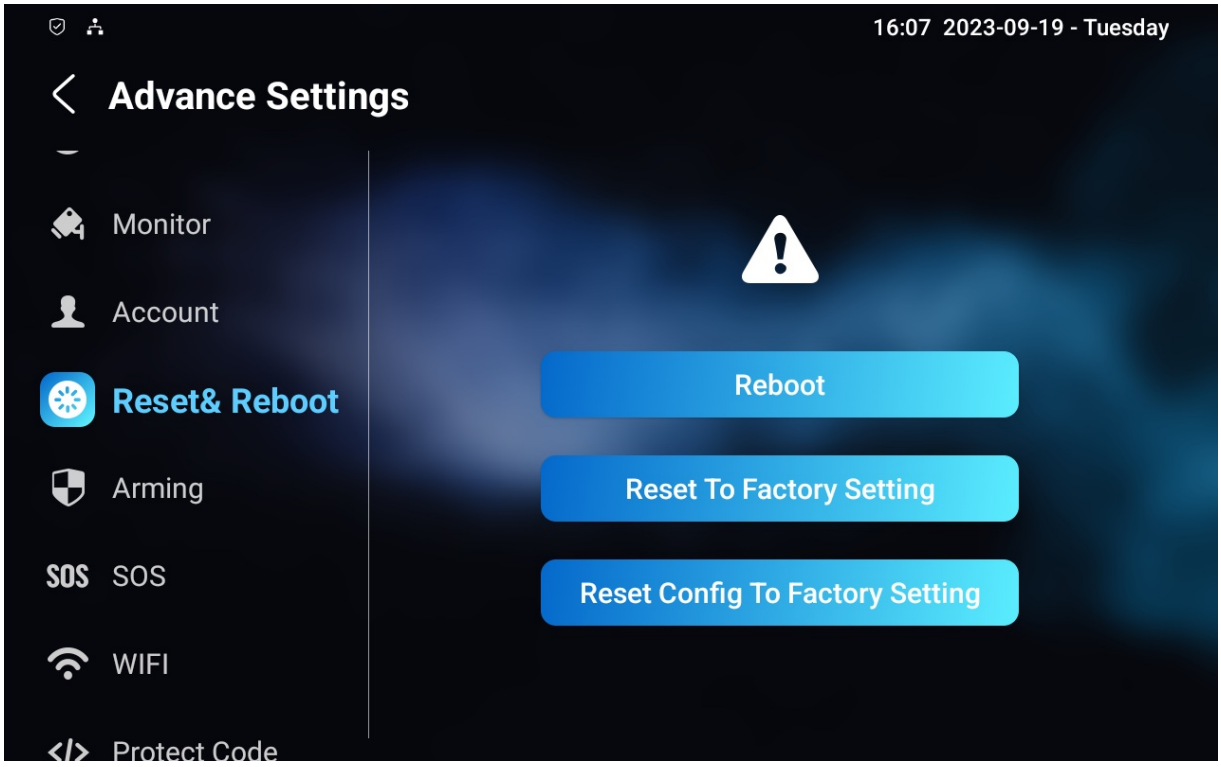
System Reboot & Reset

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.

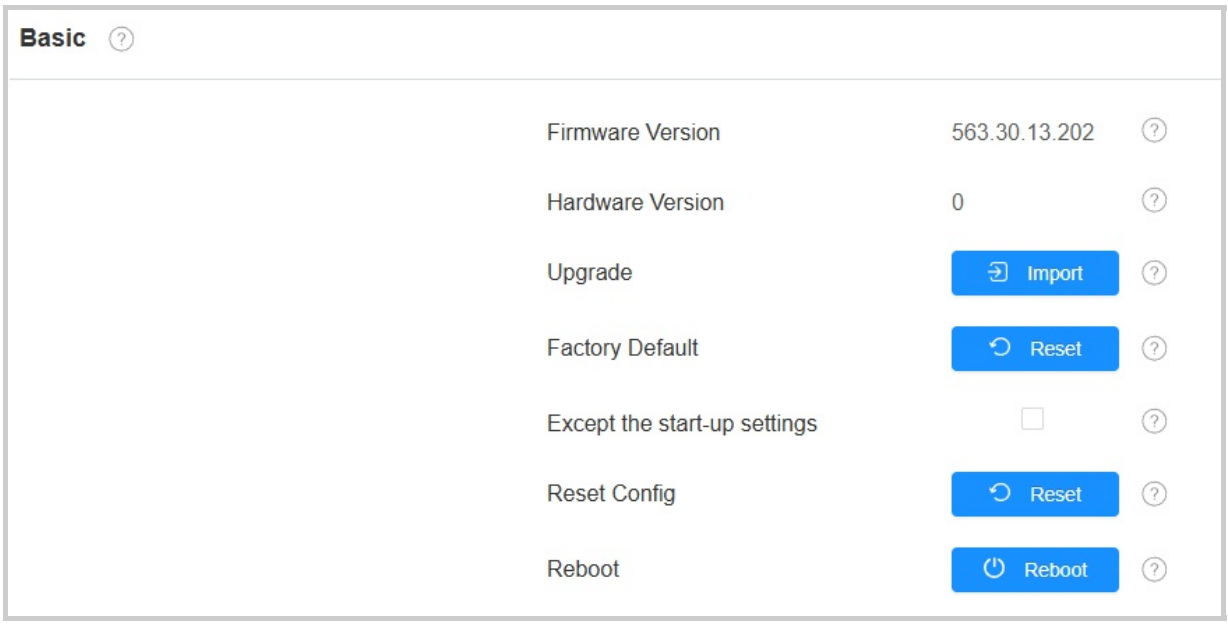
To restart the system on the device, go to **Settings > Advance Settings > Reset&Reboot** screen.



Reboot on the Web Interface

You can reboot the device on its web interface and set a reboot schedule.

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



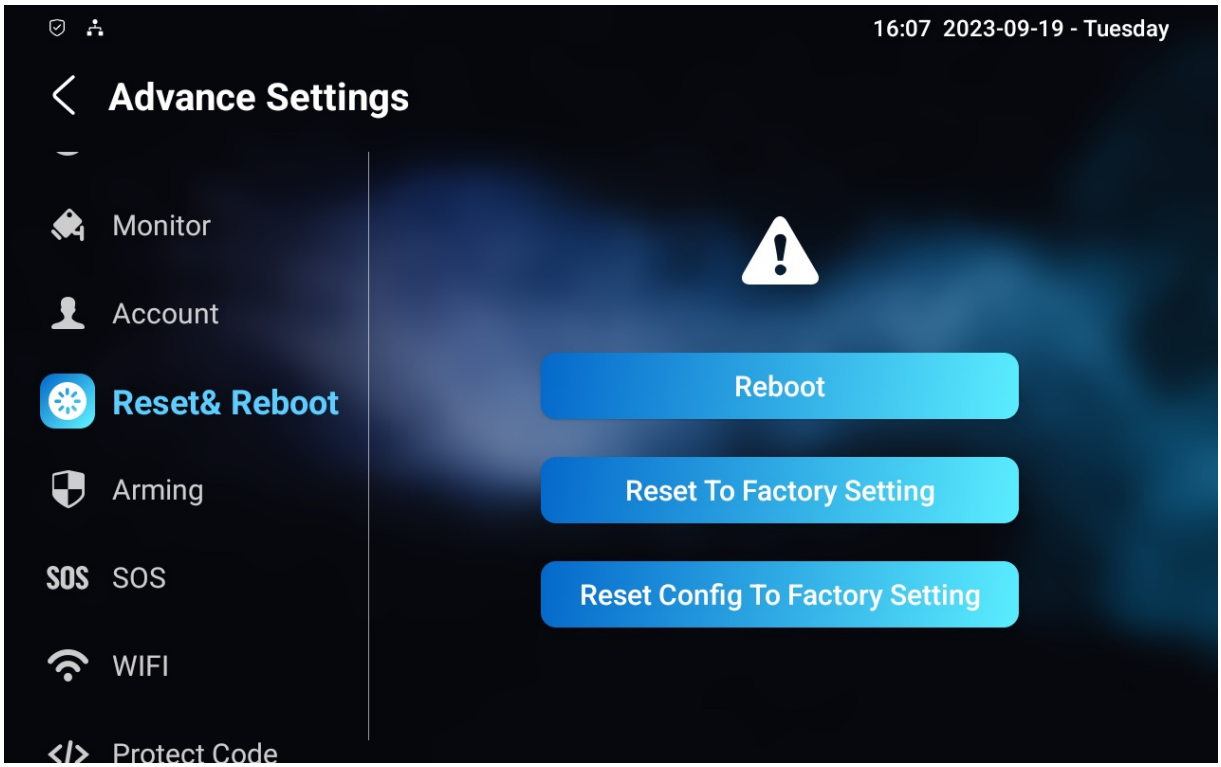
To set up the device restart schedule on web **Upgrade > Advanced > Reboot Schedule** interface.

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 Settings > 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.