About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM

S567
INDOOR MONITOR
Admin Guide

Thank you for choosing the Akuvox S567 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. This manual is written based on firmware version 567.30.13.804, and it provides all the configurations for the functions and features of the S567 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

The S567 series is an Android SIP-based indoor monitor with a smooth touch-screen. 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 video preview function. S567 series is often applied to scenarios such as villas, apartment complexes, home automation systems, and modern interiors.

Changelog

What’s new in version 567.30.13.804:

- Support keeping the monitoring screen on.
- Support the integration with Hikvision NVR.

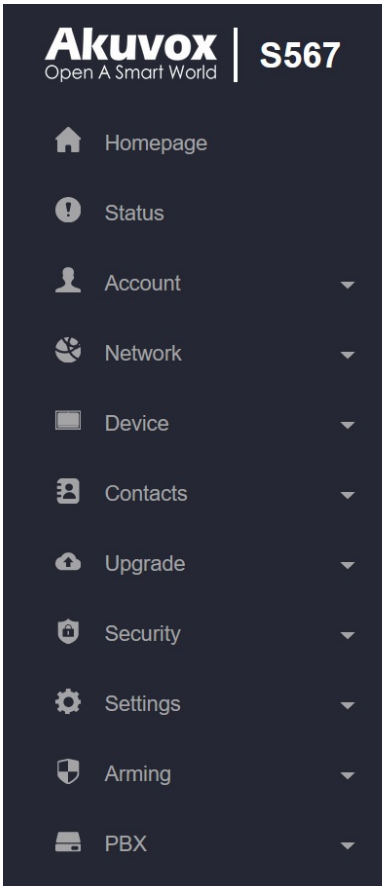
Click here to view the changelog of the device’s previous versions.

Model Specification

Model	S567
CPU	CPU Quad Cortex-A55/1.8GHz
OS	Android 12
Color	Black
Display	10 Inch IPS LCD
Resolution	1280 x 800
MIC	Dual microphone, -26dB
Speaker	Quad speakers, 8Ω / 2W
Wi-Fi	IEEE802.11 b/g/n/ax
Bluetooth	5.0
Ethernet	1xRJ45, 10/100Mbps adaptive
Power Supply	12VDC/1.5A
Alarm Input	8 x Alarm Inputs
Door Bell Input	1 x Bell In
Relay Output	2 x Relay Out (NO/COM/NC)

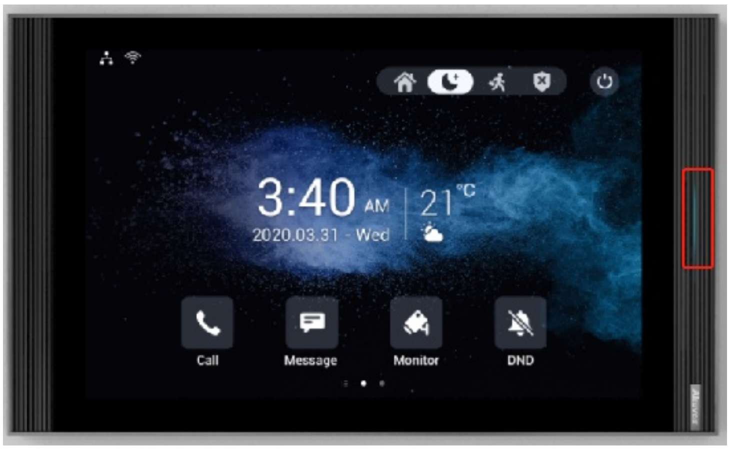
Introduction to Configuration Menu

- **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, as well as 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.
- **PBX**: This section allows you to create SIP numbers and manage SIP account settings.



Breathing Light Status

The indicator light is on the right side of the device, showing the different status of the device.



See the indicator light status below:

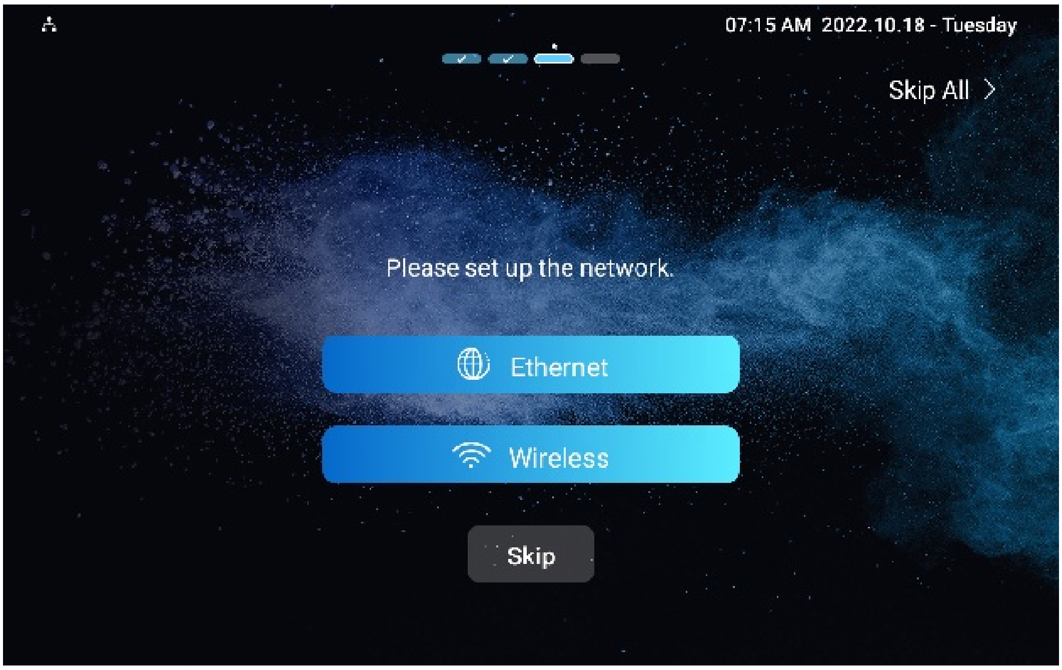
Indicator Name	Color	Status	Description
Power	Blue	ON	System is working
Power	Blue	OFF	System is not working
System status	Blue	ON	System is working
Device booting	Purple	ON	The device is powered on and booting
Network	Red	Flashing	Failed to obtain the IP address
Incoming call	Blue	Flashing	Receiving an incoming call
Outgoing call	Blue	Flashing	Making an outgoing call
In a call	Blue	ON	During a call
End a call	Blue	ON	End a call
Miss a call	Purple	ON	Missed a call
Message	Purple	ON	Contains an unread message
Screen/System	N/A	OFF	The screen is turned off The device is turned off
Alarm	Red	Flashing	An alarm is triggered
Voice assistant	Blue	ON	Waking up voice assistant
Doorbell	Blue	Flashing	Doorbell rings
Device upgrade	Red	ON	Upgrading the device
Reset	Red	ON	Reset the device to the factory setting

Access the Device

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

Device Start-up Network Selection

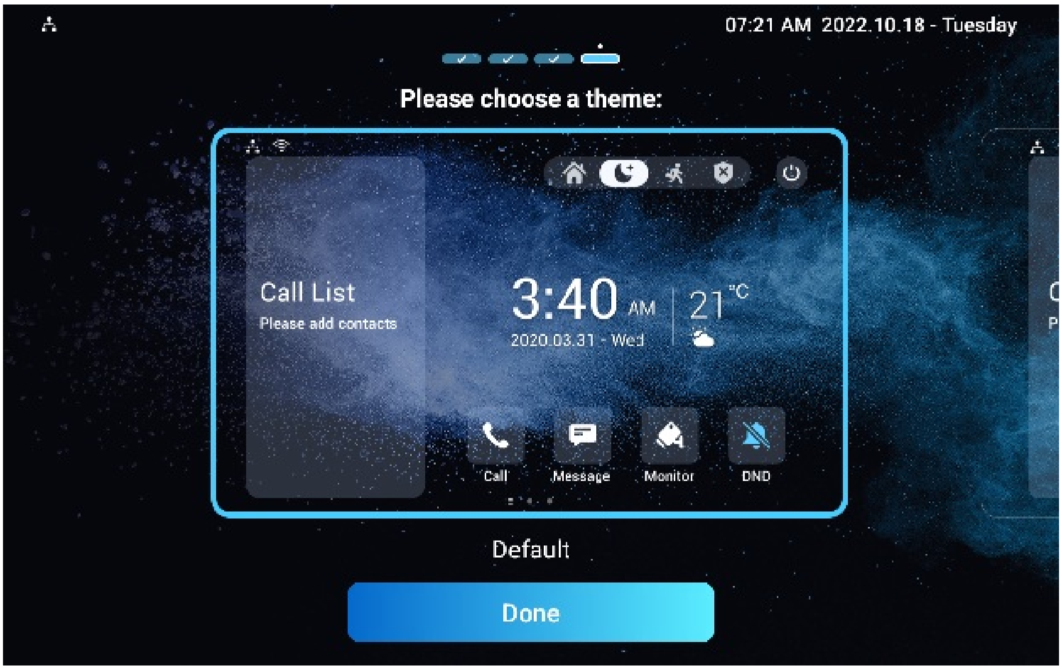
After the device boots up initially, you are required to select the network connection for the device. You can either select Ethernet or a Wireless network connection.

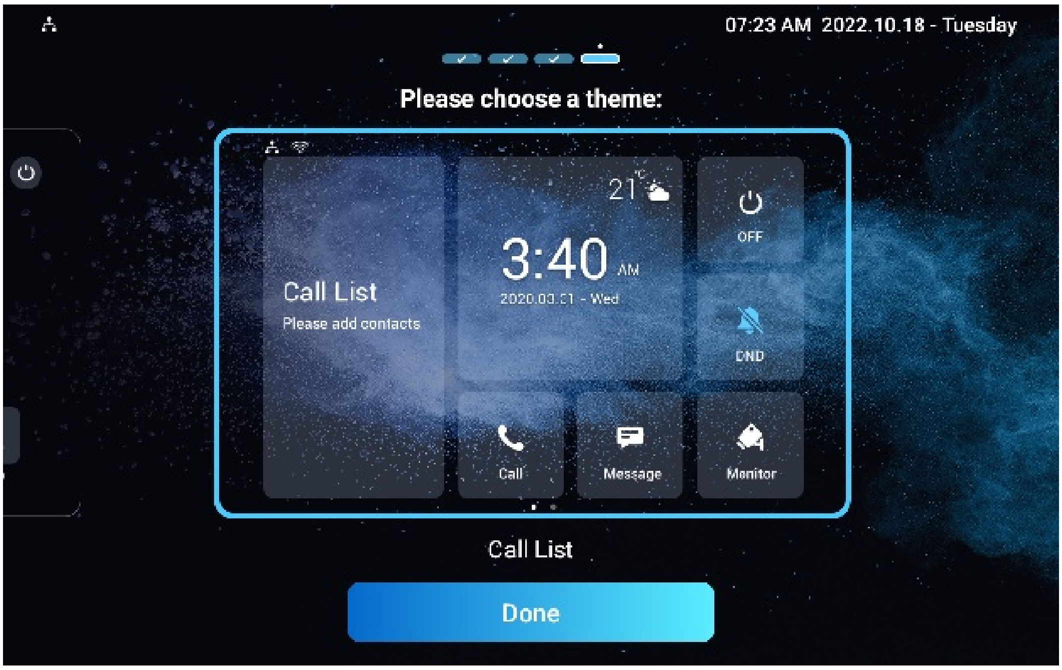


> **Note**
>
> Please refer to Network Setting & Other Connection for the configuration of the Ethernet and wireless network connection.

Device Home Screen Type Selection

Akuvox indoor monitor supports two different home screen display modes: **Default** and **Call List**. Choose one suitable mode for your scenarios.

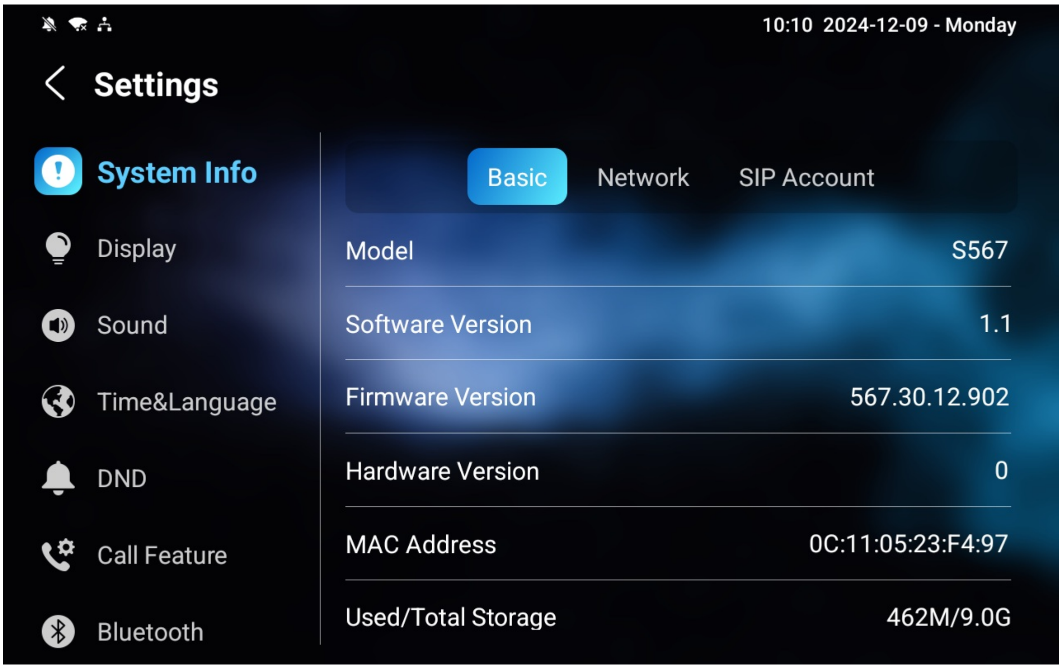




Access the Device Settings

Access Device Basic Settings

You can access the device's basic settings and advanced settings where you can configure different types of functions as needed. To access the device's basic setting, swipe your finger left on the home screen, then tap ⚙. You can check the basic information like MAC, firmware, etc.



10:10 2024-12-09 - Monday

Settings

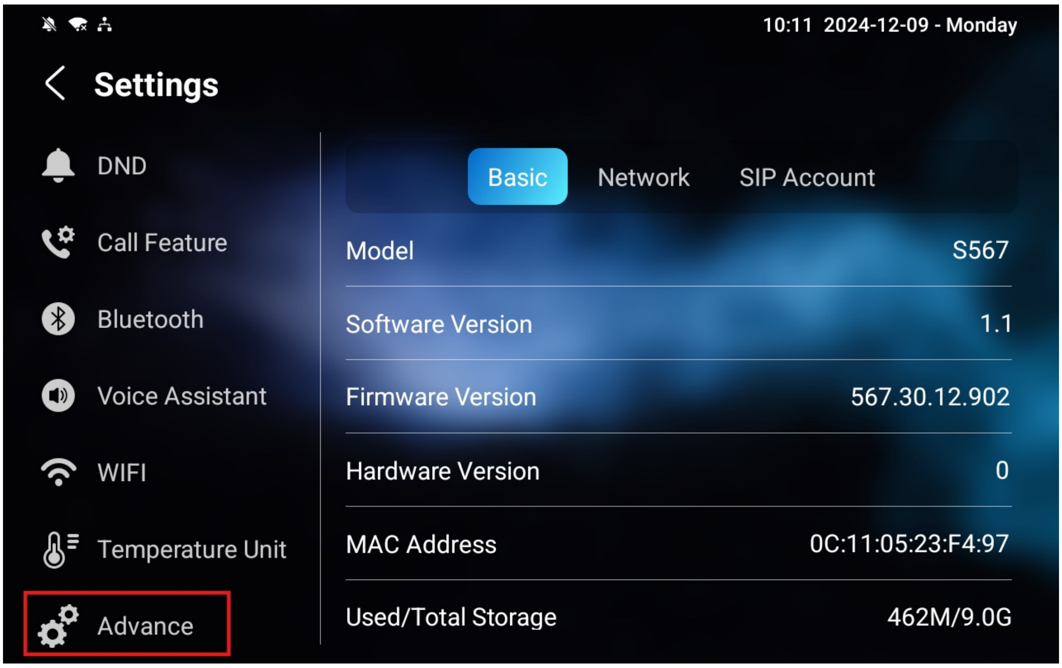
- System Info
- Display
- Sound
- Time&Language
- DND
- Call Feature
- Bluetooth

Basic | Network | SIP Account

Model	S567
Software Version	1.1
Firmware Version	567.30.12.902
Hardware Version	0
MAC Address	0C:11:05:23:F4:97
Used/Total Storage	462M/9.0G

Access Device Advance Settings

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



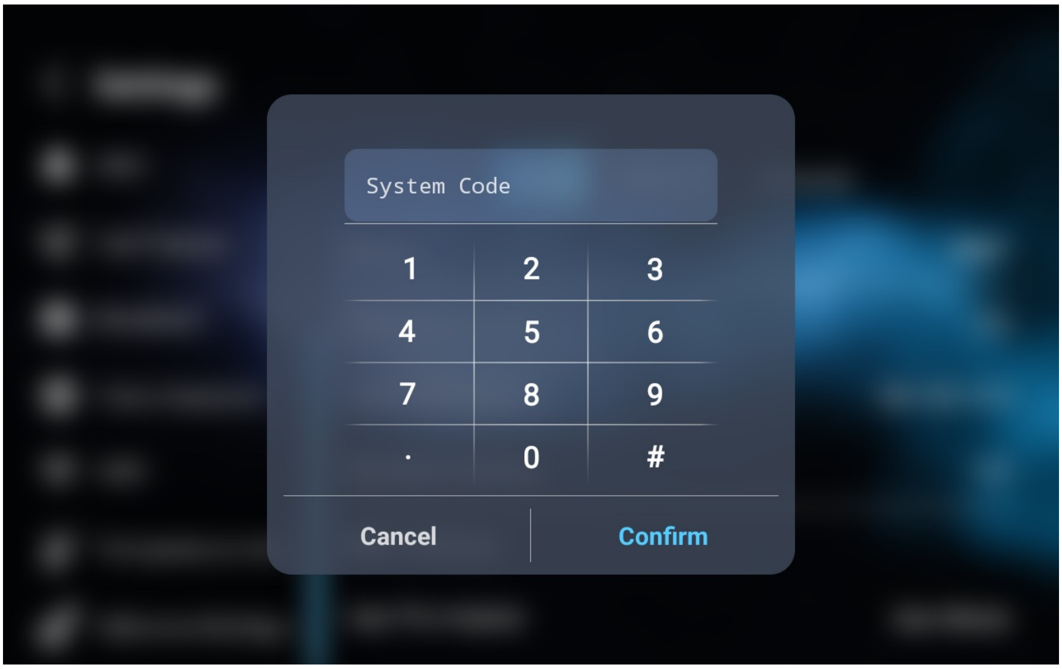
10:11 2024-12-09 - Monday

Settings

- DND
- Call Feature
- Bluetooth
- Voice Assistant
- WIFI
- Temperature Unit
- Advance

Basic | Network | SIP Account

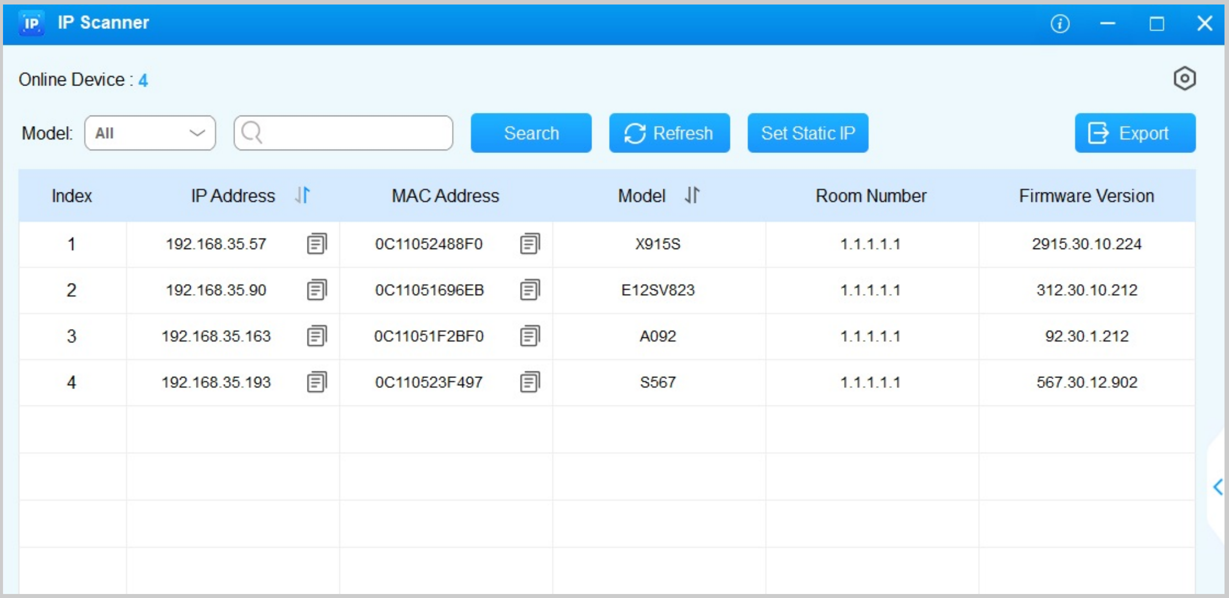
Model	S567
Software Version	1.1
Firmware Version	567.30.12.902
Hardware Version	0
MAC Address	0C:11:05:23:F4:97
Used/Total Storage	462M/9.0G



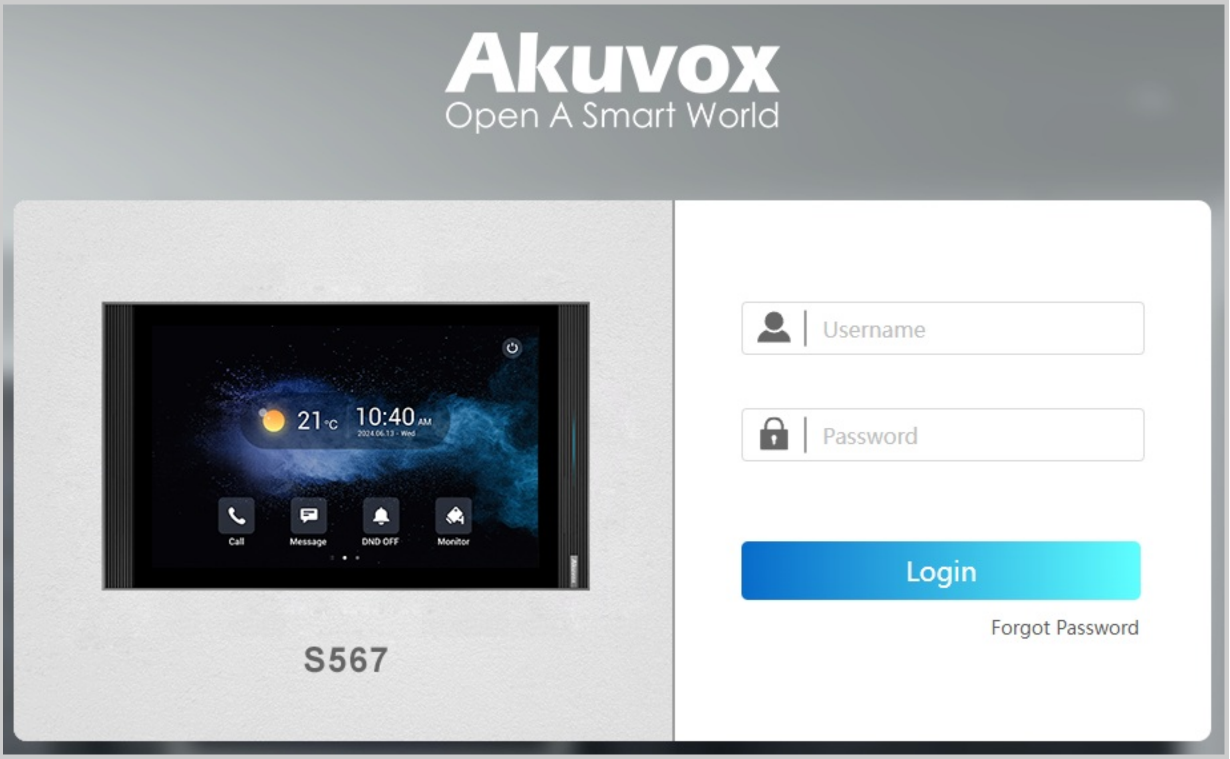
Access the Device Web Settings

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

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



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



Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See detailed guide:
- https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- The initial username and password are **admin** and please be case-sensitive to the user names and passwords entered.
- Your computer should be on the same LAN as the device.

Language and Time

Language

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

On the Device

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

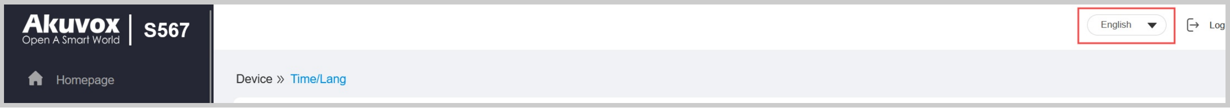
- The device supports the following languages: Bosnian, Czech, Danish, German, English, Spanish, French, Italian, Lithuanian, Mongolian, Norsk, Polish, Portuguese, Russian, Slovene, Swedish, Turkish, Vietnamese, Korean, Simplified Chinese, Traditional Chinese, Japanese, Ukrainian, Dutch, Arabic, and Hebrew.

On the Web Interface

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

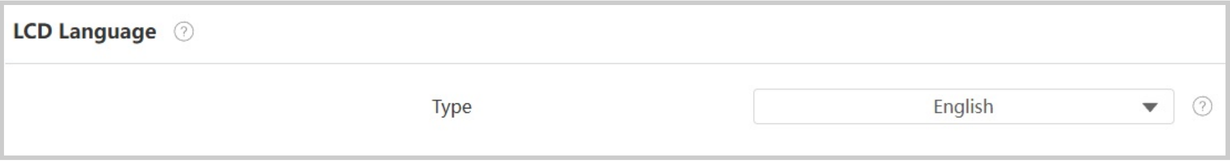
The device web interface supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Czech, Portuguese, Spanish, Dutch, French, 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, Norsk, Polish, Portuguese, Russian, Slovene, Swedish, Turkish, Vietnamese, Korean, Simplified Chinese, Traditional Chinese, Japanese, Ukrainian, Dutch, Arabic, and Hebrew.



LCD Language

Type: English

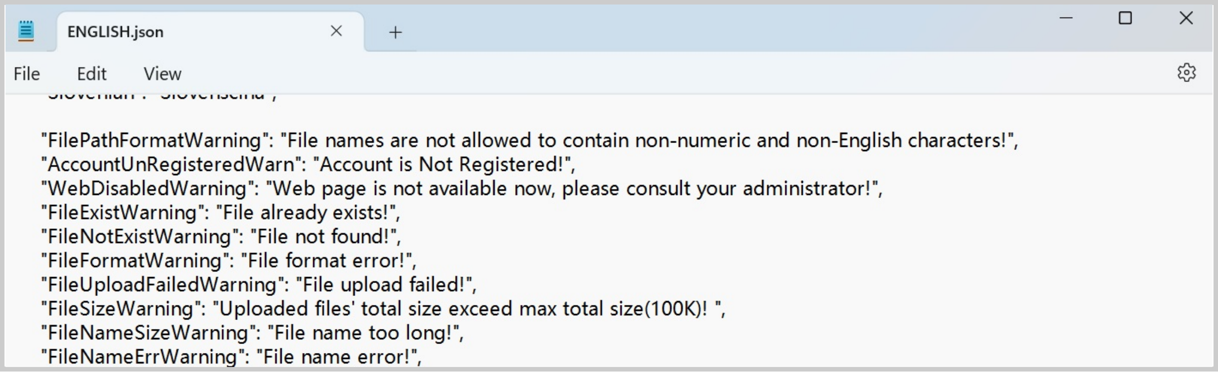
Custom Language

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

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

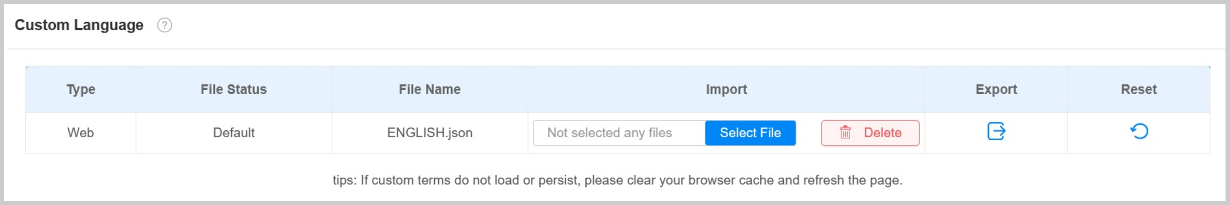
Import the .json file and its size should be smaller than 1 MB.

File Example:



```
"FilePathFormatWarning": "File names are not allowed to contain non-numeric and non-English characters!",
"AccountUnRegisteredWarn": "Account is Not Registered!",
"WebDisabledWarning": "Web page is not available now, please consult your administrator!",
"FileExistWarning": "File already exists!",
"FileNotExistWarning": "File not found!",
"FileFormatWarning": "File format error!",
"FileUploadFailedWarning": "File upload failed!",
"FileSizeWarning": "Uploaded files' total size exceed max total size(100K)! ",
"FileNameSizeWarning": "File name too long!",
"FileNameErrWarning": "File name error!",
```

To set it up, navigate to **Device > Time/Lang > Custom Language** interface.


Custom Language

Type	File Status	File Name	Import	Export	Reset
Web	Default	ENGLISH.json	Not selected any files Select File Delete		

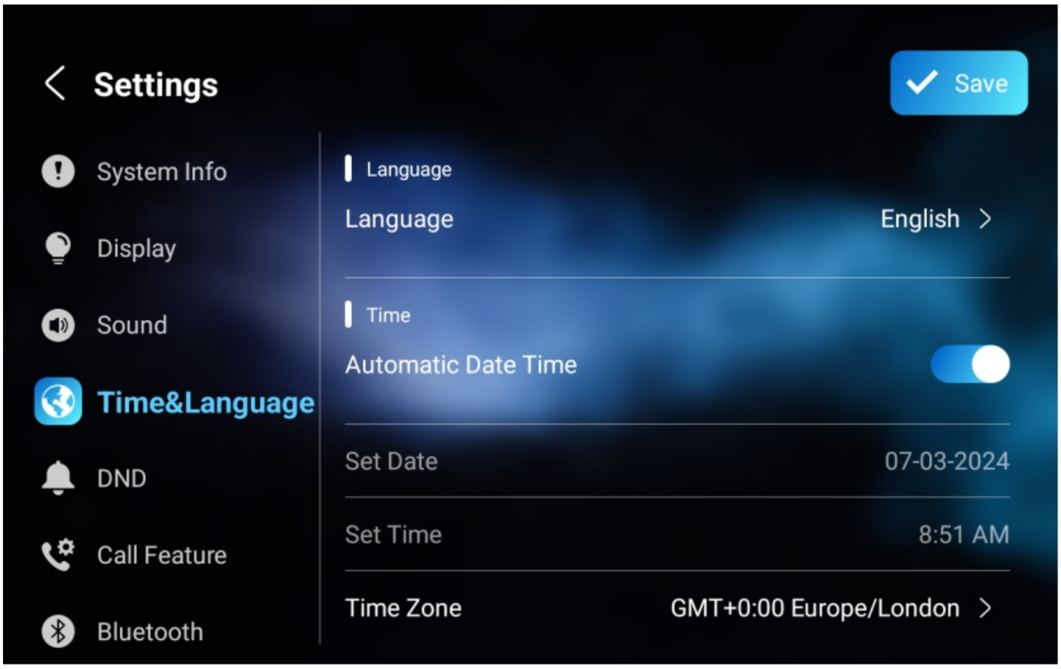
tips: If custom terms do not load or persist, please clear your browser cache and refresh the page.

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.



Language

Language English

Time

Automatic Date Time

Set Date 07-03-2024

Set Time 8:51 AM

Time Zone GMT+0:00 Europe/London

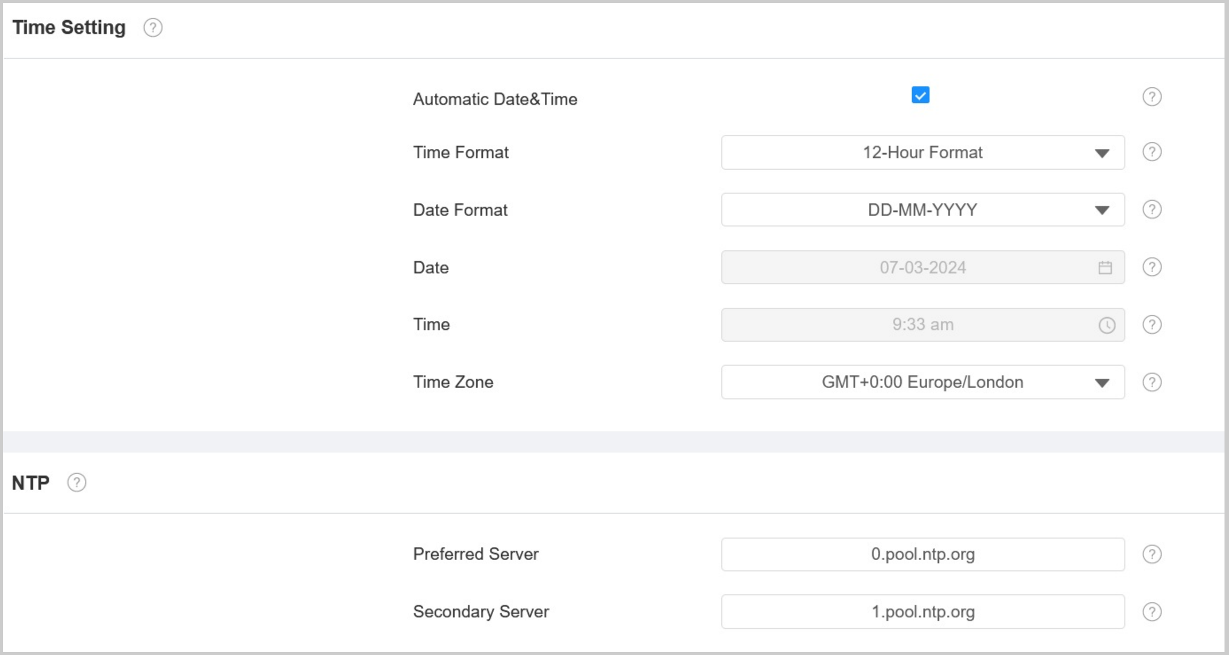
- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the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

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



Time Setting

Automatic Date&Time	☑
Time Format	12-Hour Format
Date Format	DD-MM-YYYY
Date	07-03-2024
Time	9:33 am
Time Zone	GMT+0:00 Europe/London

NTP

Preferred Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org

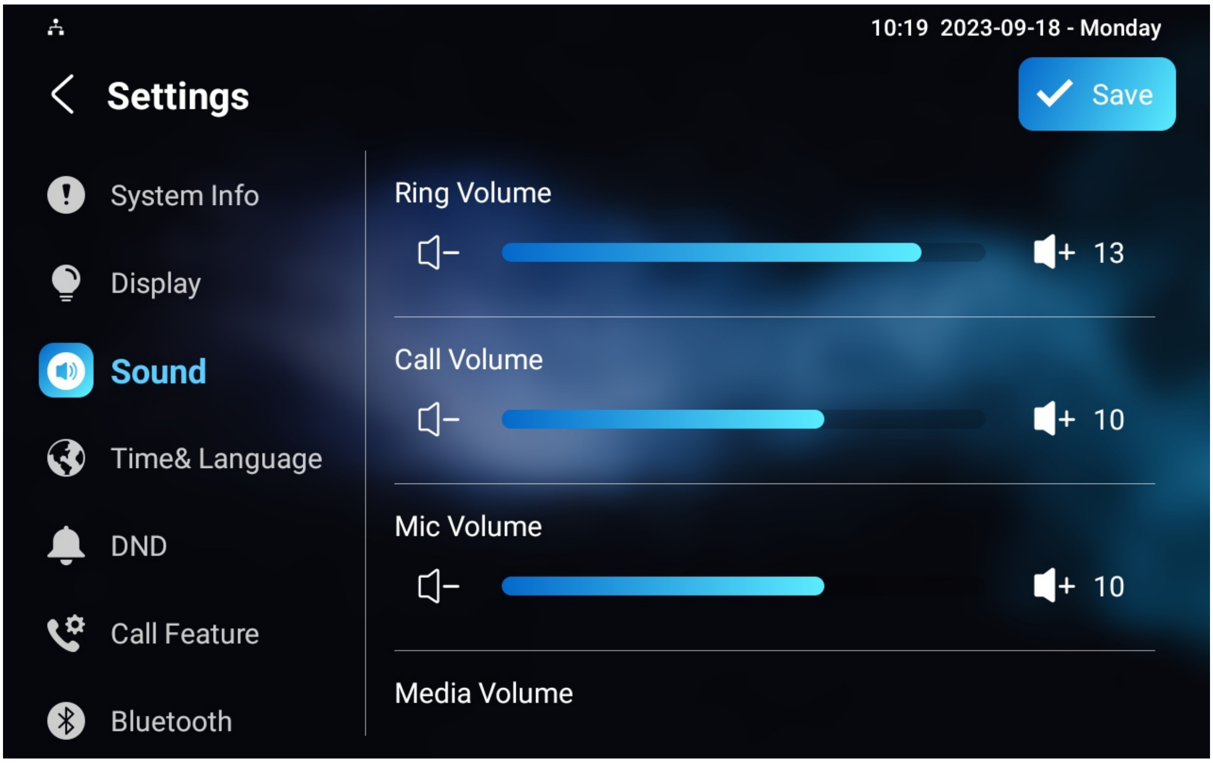
- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **Date Format**: Select the date format from the available options.
- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Preferred Server**: Enter the NTP server address.
- **Secondary Server**: Enter the backup server address. When the main NTP server fails, it will change to the backup server automatically.

Sound and Volume

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

On the Device

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



Ring Volume 13

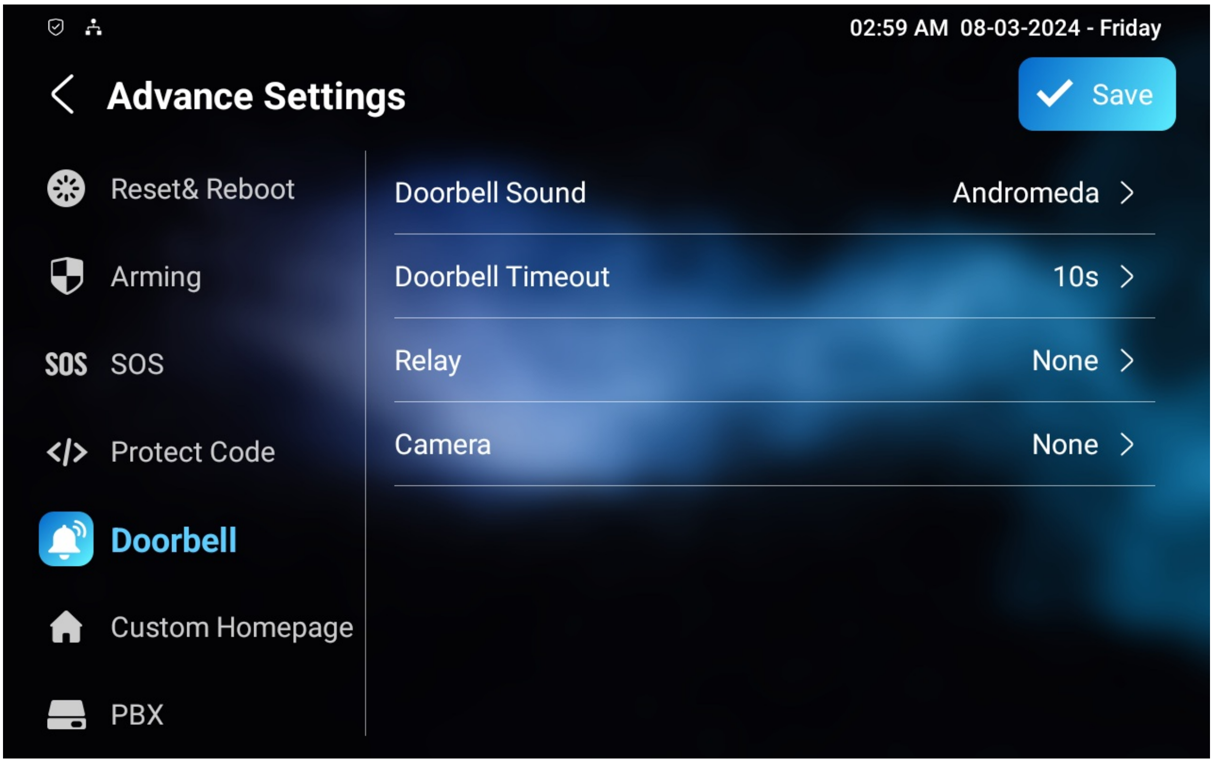
Call Volume 10

Mic Volume 10

Media Volume

- **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 screensaver.
- **Touch Sound**: The icon tapping sound.
- **Phone Ringtone**: The ringtone for incoming calls.
- **Notification Sound**: The ringtone for the incoming messages.
- **Call Audio Routing**: Available when the device is connected to Bluetooth devices. This setting determines through which the incoming call ringtone and audio of the call session will be played.

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.

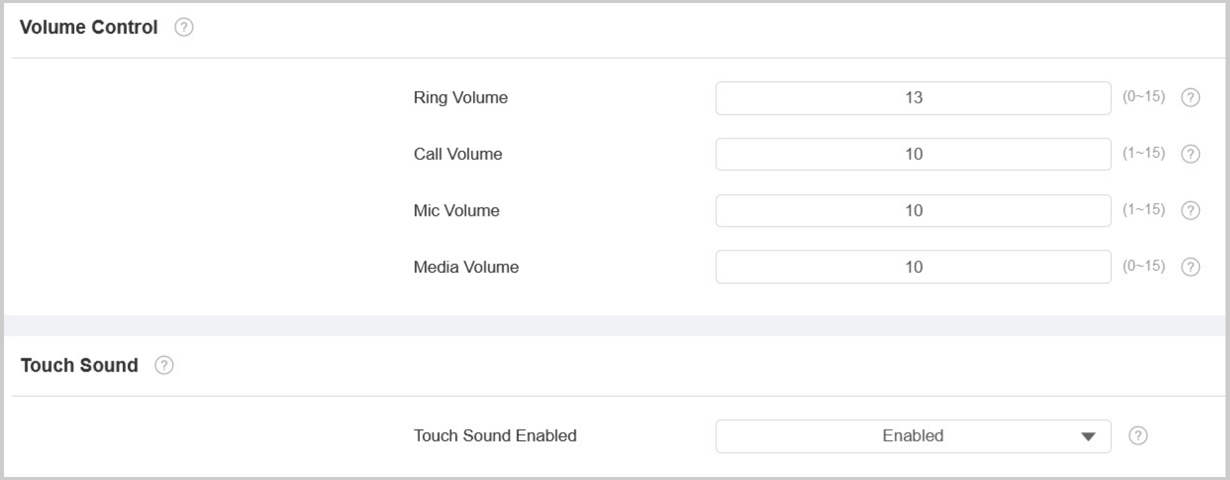


Doorbell Sound	Andromeda
Doorbell Timeout	10s
Relay	None
Camera	None

- **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.

On the Web Interface

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



Volume Control

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

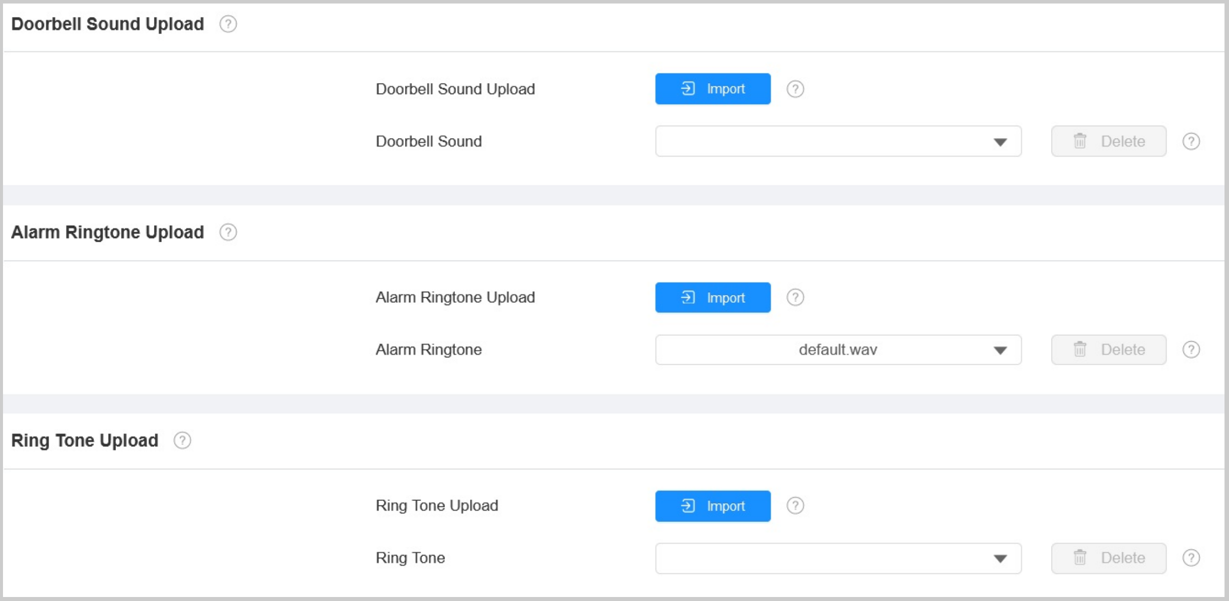
Touch Sound

Touch Sound Enabled	Enabled

- **Ring Volume**: The incoming call ringtone volume. The default is 13.
- **Call Volume**: The speaker volume during the call. The default is 10.
- **Mic Volume**: The mic volume. The default is 10.
- **Media Volume**: The volume for the video screen saver. The default is 10.
- **Touch Sound Enabled**: The icon tapping sound.

Upload Tones

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



Doorbell Sound Upload

Doorbell Sound Upload: Import

Doorbell Sound: Delete

Alarm Ringtone Upload

Alarm Ringtone Upload: Import

Alarm Ringtone: default.wav Delete

Ring Tone Upload

Ring Tone Upload: Import

Ring Tone: Delete

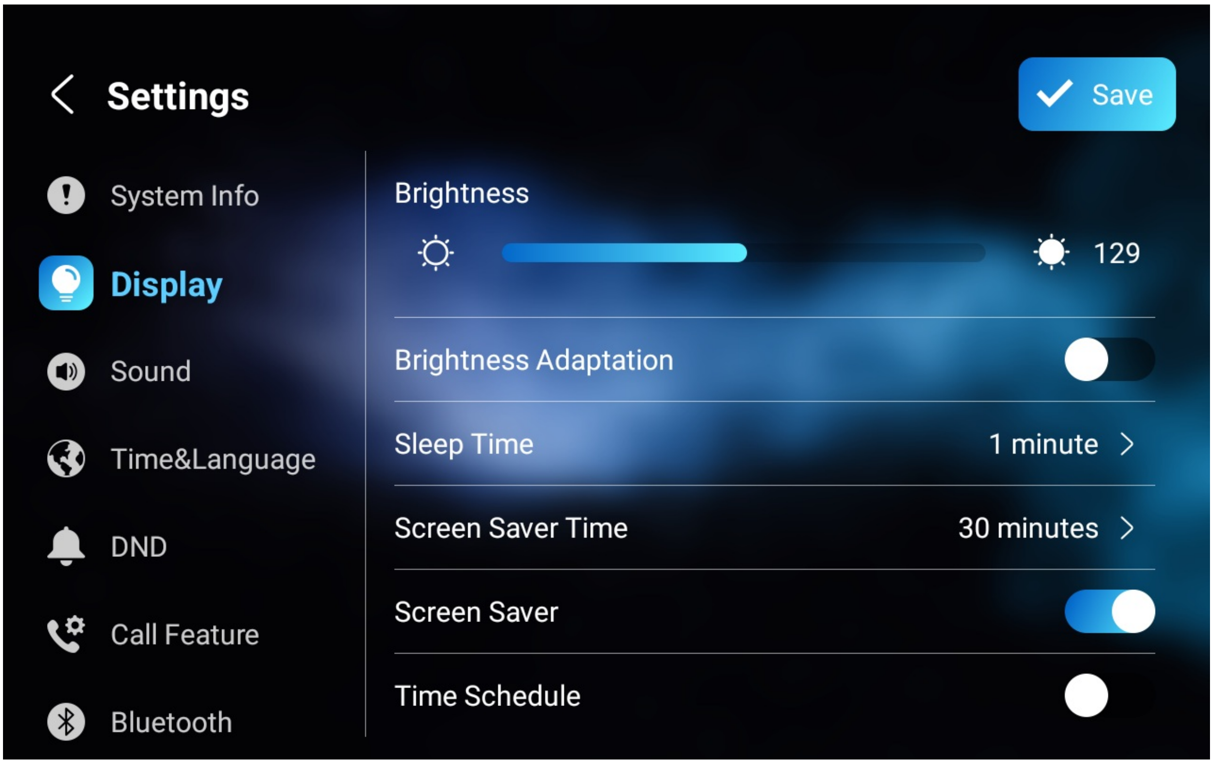
> **Note**
>
> The files to be uploaded should be in WAV or MP3 format. No limitation on the file size.

Screen Display

On the Device

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

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



Brightness 129

Brightness Adaptation

Sleep Time 1 minute

Screen Saver Time 30 minutes

Screen Saver

Time Schedule

- **Brightness**: Move the blue bar to adjust the screen brightness. The default brightness is **145**.

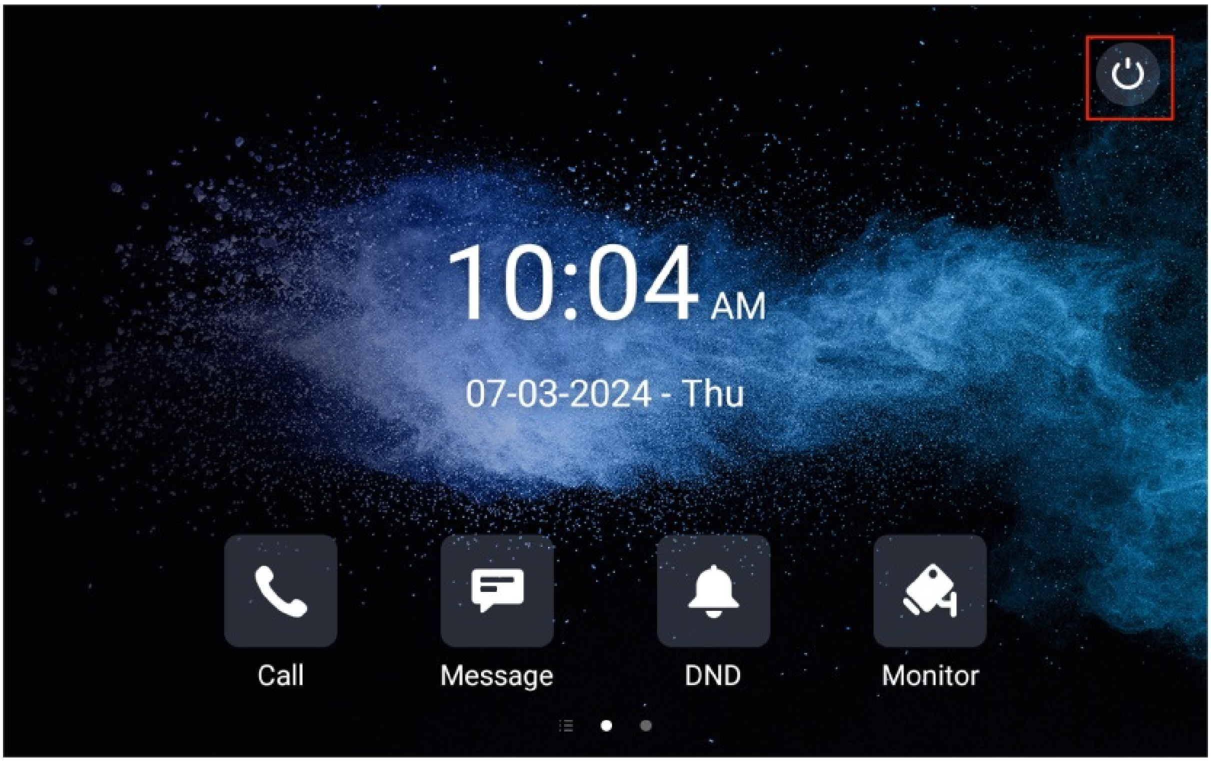
> **Note**
>
> You cannot adjust the screen brightness manually when the **Brightness Adaptation** is enabled.

- **Brightness Adaptation**: Enable the device to adjust automatically to natural light.
- **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.

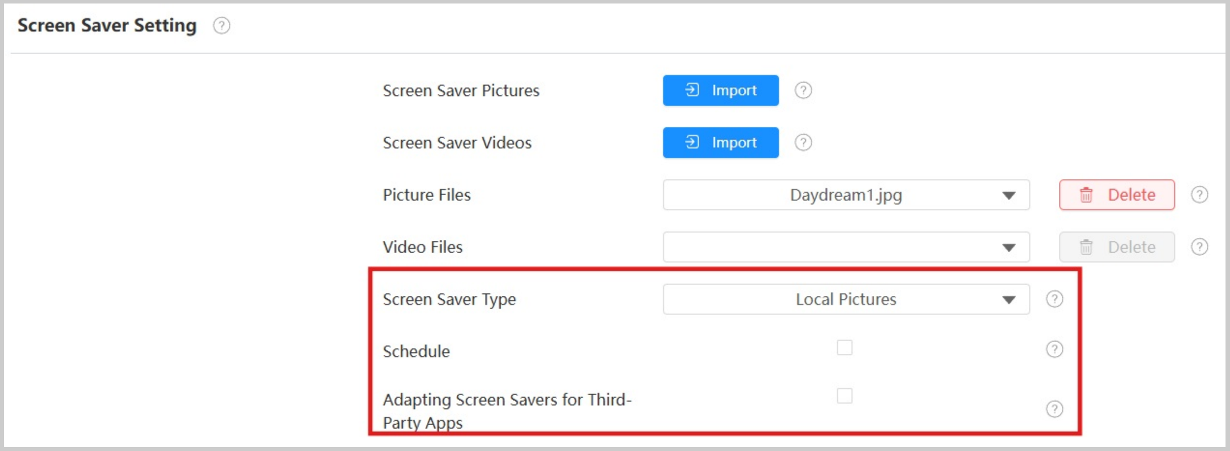
- **Screen Lock**: Lock the screen after the screen is turned off(turn dark). You are required to enter the code to unlock the screen. The default code is 123456.
- **Screen Clean**: Allow users to wipe the screen clean without triggering unwanted changes in the settings.
- **Font Size**: Select the font size among four options: Small, Normal, Large, and Huge.
- **Breathing Light**: Enable or disable the breathing light.
- **Wallpaper**: It is for local wallpaper selection.
- **Theme Style**: Choose the preferred theme style from the available options. The style applies to all screens.
- **Festival Theme Auto-Switch**: When enabled, the screensaver and wallpaper will automatically change when the following festivals arrive.
    - New Year - 1.1
    - Valentine's Day - 2.14
    - Earth Day - 4.22
    - International Worker’s Day - 5.1
    - Halloween - 10.31
    - Christmas - 12.25
- **Wake Up Mode**:
    - **Manual**: Touch the screen to wake up the device.
    - **Auto**: Approach the device to wake it up. It is the default option.
- **Wake Up Distance**: Select the distance to wake up the device. The short distance is 30 cm and the long distance is 80 cm.

Users can also turn off the screen manually by tapping the icon⏻.



On the Web Interface

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

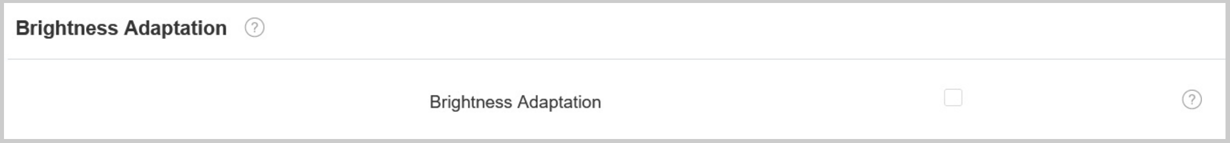


Screen Saver Setting

Screen Saver Pictures	Import	
Screen Saver Videos	Import	
Picture Files	Daydream1.jpg	Delete
Video Files		Delete
Screen Saver Type	Local Pictures	
Schedule	□	
Adapting Screen Savers for Third-Party Apps	□	

- **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 screensaver. The screen-saver parameters will be hidden on the web interface and the device.

To enable the brightness adaptation, go to **Settings > Basic > Brightness Adaptation** interface.

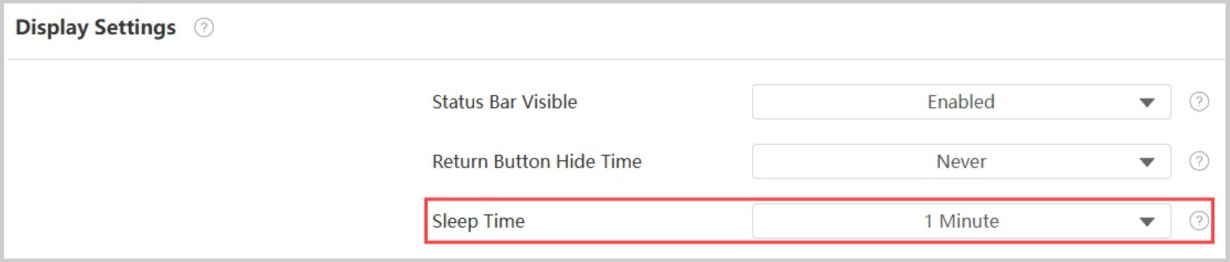


Brightness Adaptation

Brightness Adaptation	□

- **Brightness Adaptation**: Enable the device to adjust automatically to natural light. When enabled, you cannot adjust brightness manually.

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



Display Settings

Status Bar Visible	Enabled
Return Button Hide Time	Never
Sleep Time	1 Minute

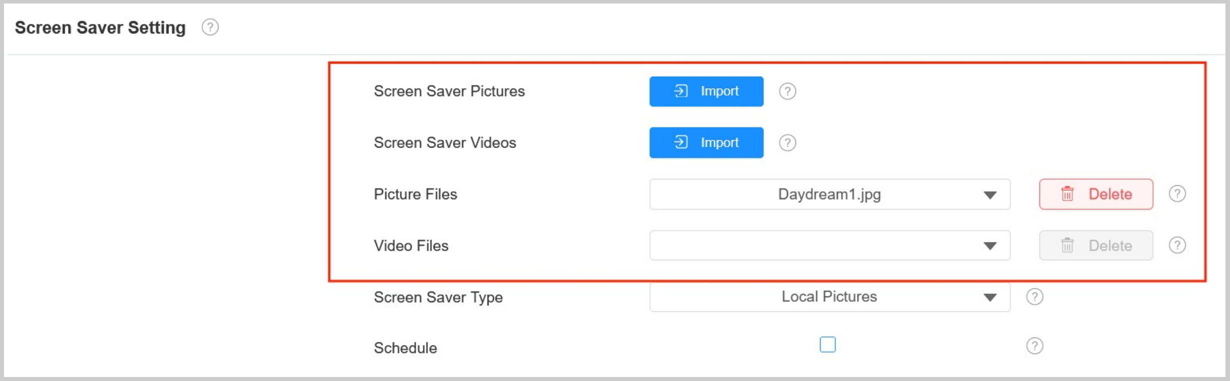
- **Sleep Time**: If the screen saver is enabled, the sleep time is the screen saver's start time. For example, if you set it as 1 minute, the screen saver will start automatically when the device has no operation for 1 minute. If the screen saver is disabled, the screen will be turned off automatically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

Upload Screen Saver

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

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

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



Screen Saver Setting

Screen Saver Pictures	Import	
Screen Saver Videos	Import	
Picture Files	Daydream1.jpg	Delete
Video Files		Delete
Screen Saver Type	Local Pictures	
Schedule	□	

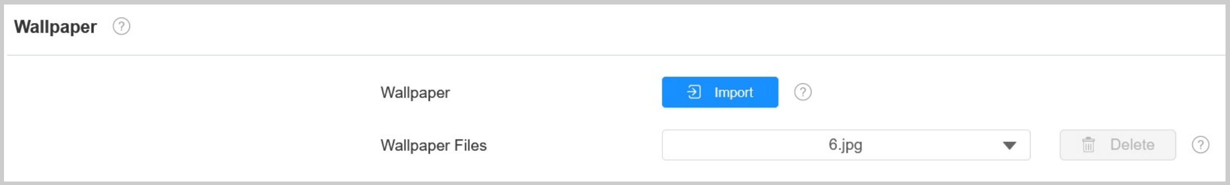
Note

- 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 720P/1080P.

Upload Wallpaper

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.



Wallpaper

Wallpaper: Import

Wallpaper Files: 6.jpg — Delete

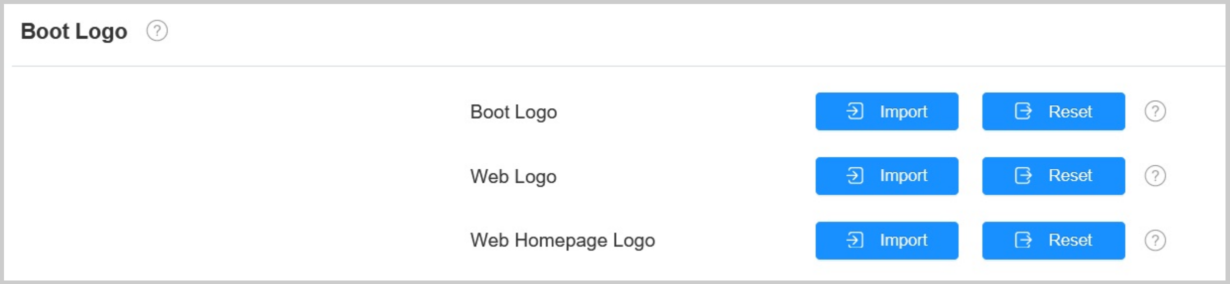
Note

- 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

Boot Logo: Import — Reset

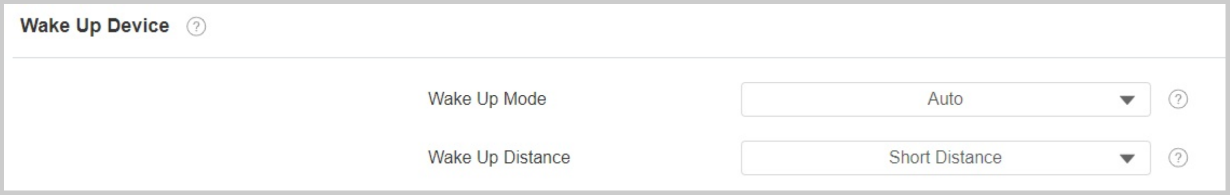
Web Logo: Import — Reset

Web Homepage Logo: Import — Reset

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

Approach to Wake up

You can manually wake up the device by tapping the device screen, or wake up the device automatically as you walk up to the device within the preset distance. To set it up, go to **Settings > Basic > Wake Up Device** interface.



Wake Up Device ?

Wake Up Mode: Auto ?

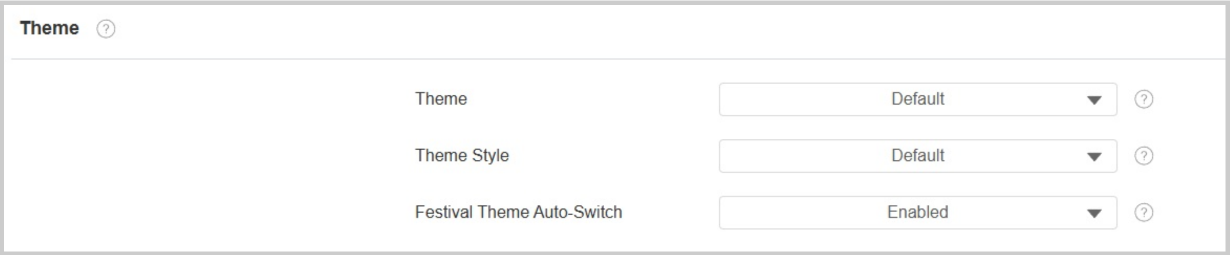
Wake Up Distance: Short Distance ?

- **Wake Up Mode:**
  - **Manual**: Touch the screen to wake up the device.
  - **Auto**: Approach the device to wake it up. It is the default option.
- **Wake Up Distance**: Select the distance to wake up the device. The short distance is 30 cm. The long distance is 80 cm.

Home Screen Display

You can select the **Default** or **Call List** home screen display and choose the preferred theme style.

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



Theme ?

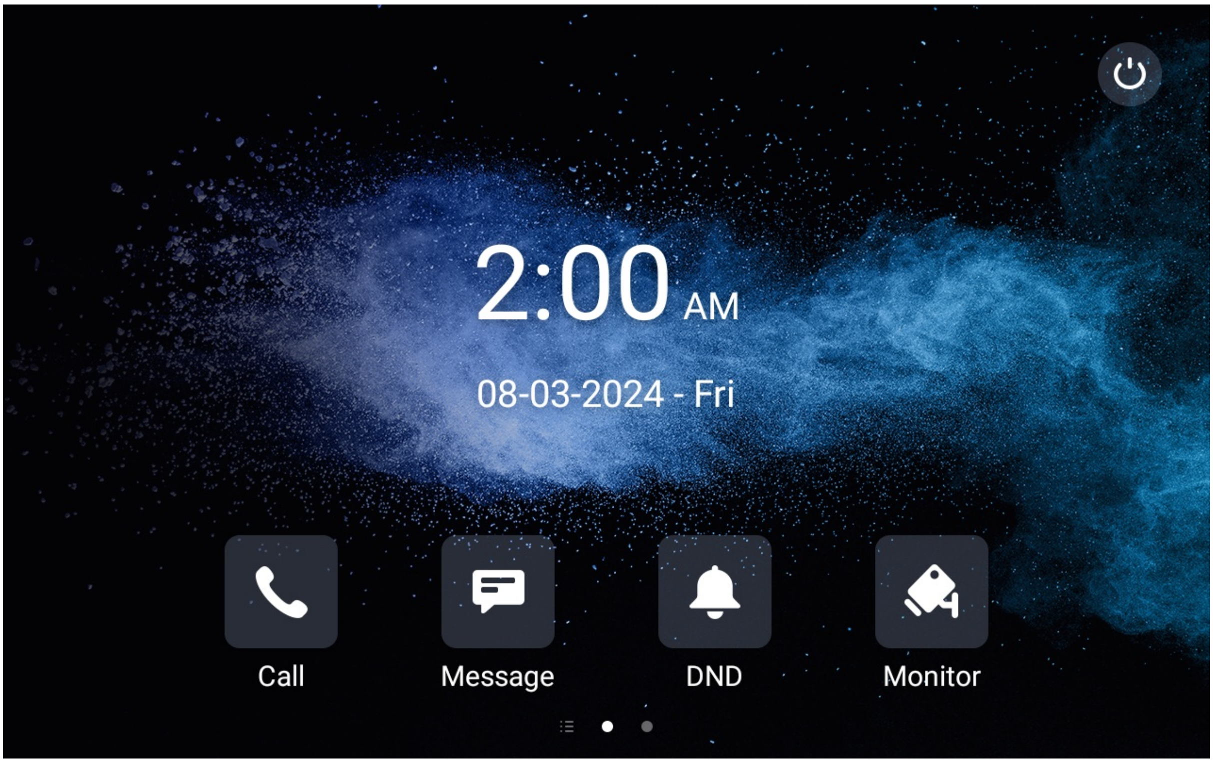
Theme: Default ?

Theme Style: Default ?

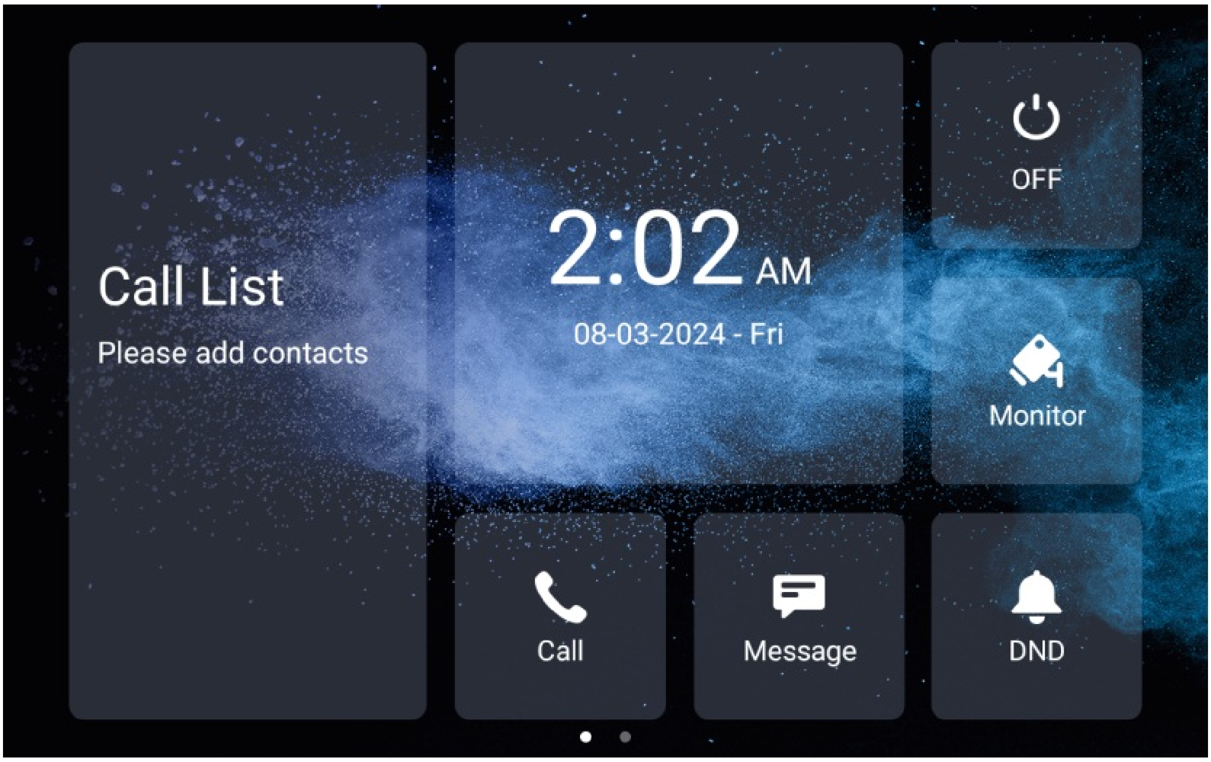
Festival Theme Auto-Switch: Enabled ?

- **Festival Theme Auto-Switch**: When enabled, the screensaver and wallpaper will automatically change when the following festivals arrive.
  - New Year - 1.1
  - Valentine's Day - 2.14
  - Earth Day - 4.22
  - International Worker’s Day - 5.1
  - Halloween - 10.31
  - Christmas - 12.25

Default Home Screen:



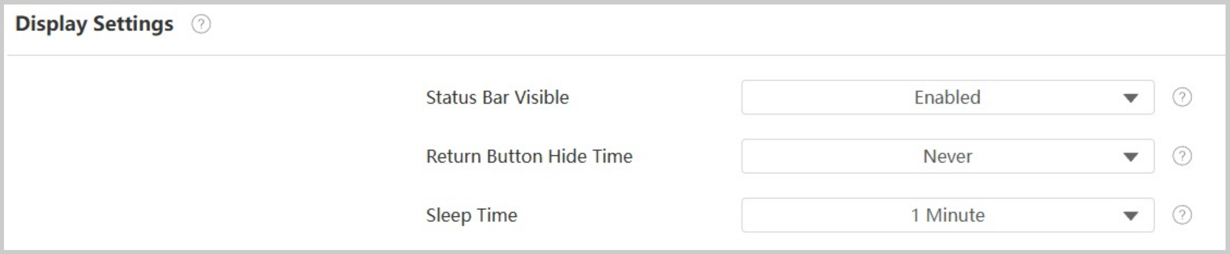
Call List Home Screen:



Status Bar Display Configuration

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

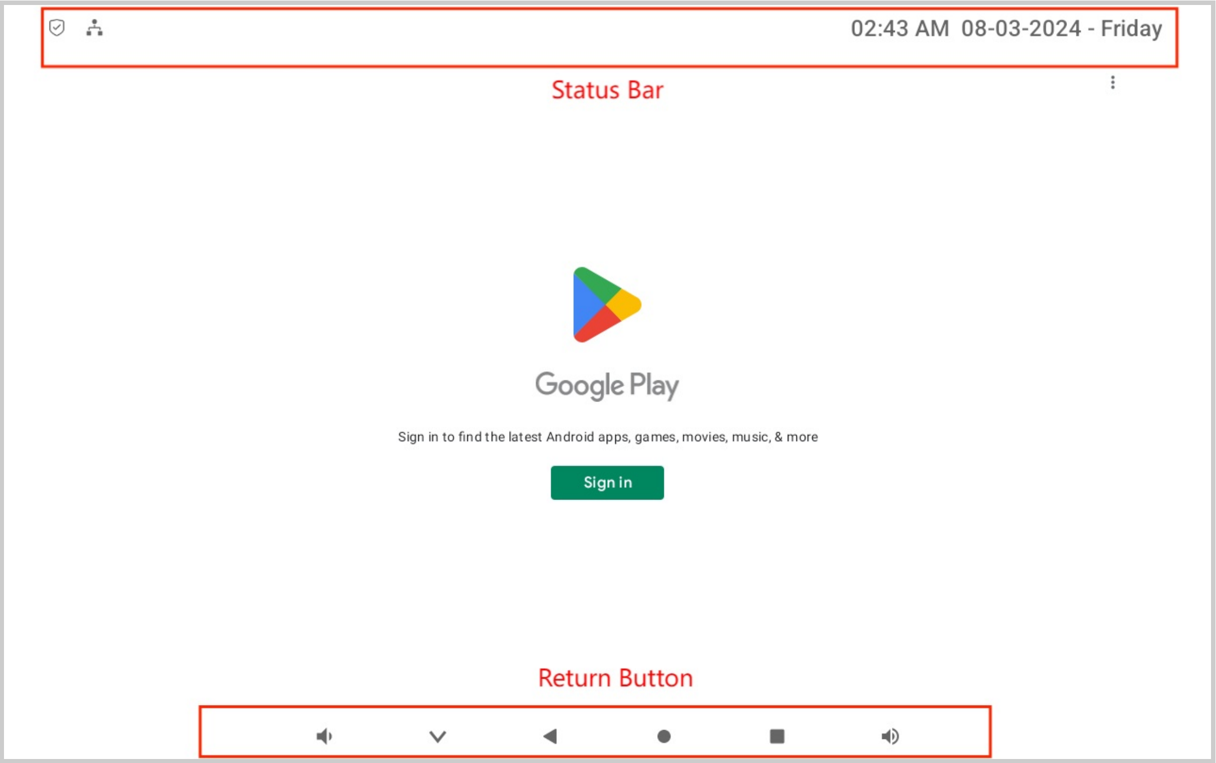
To set it up, go to the **Device > Display Setting > Display Settings** interface.



Display Settings

Status Bar Visible	Enabled
Return Button Hide Time	Never
Sleep Time	1 Minute

- **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.

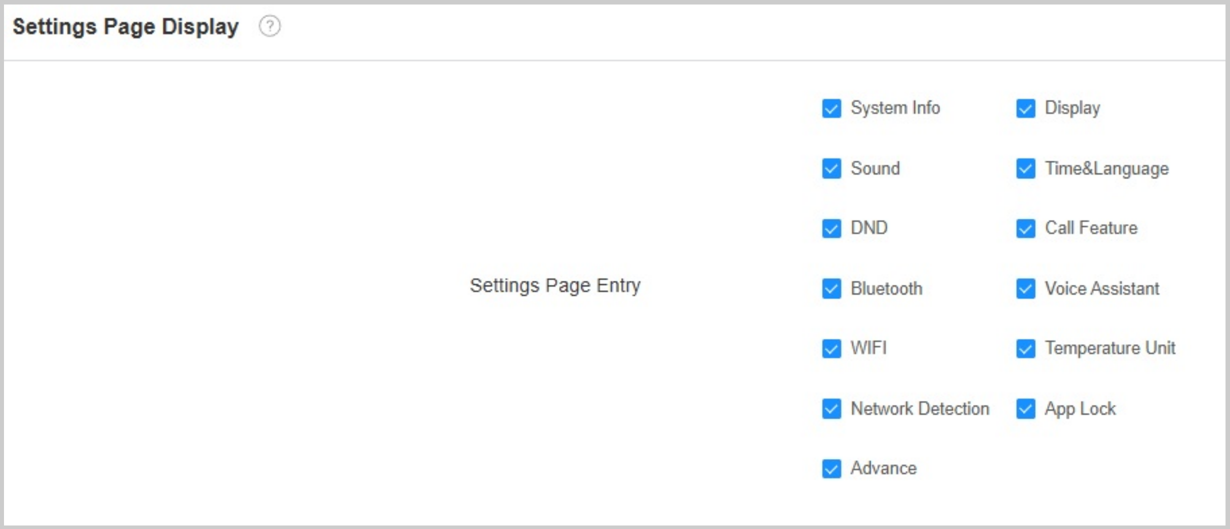


02:43 AM 08-03-2024 - Friday
Status Bar
Google Play
Sign in to find the latest Android apps, games, movies, music, & more
Sign in
Return Button

Function Display on the Settings Screen

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

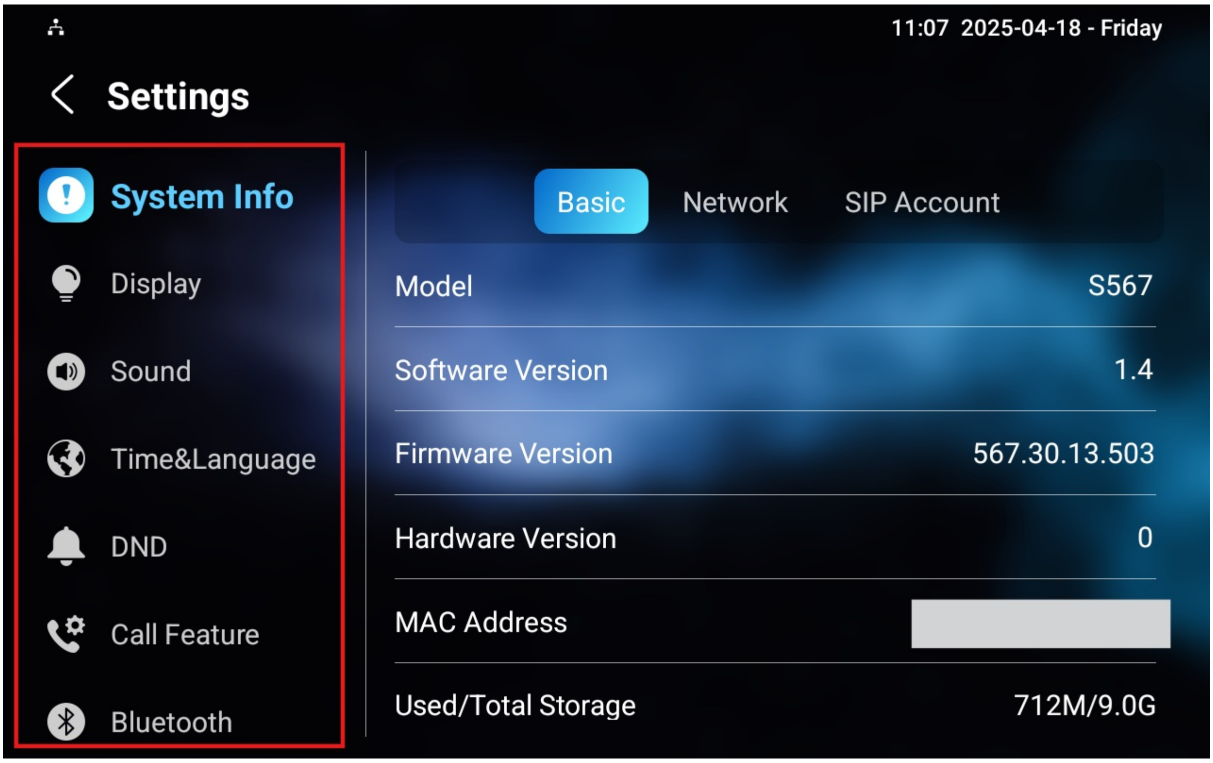
Set it up on the **Device > Display Setting > Settings Page Display** interface.



Settings Page Display

Settings Page Entry

☑ System Info ☑ Display
☑ Sound ☑ Time&Language
☑ DND ☑ Call Feature
☑ Bluetooth ☑ Voice Assistant
☑ WIFI ☑ Temperature Unit
☑ Network Detection ☑ App Lock
☑ Advance



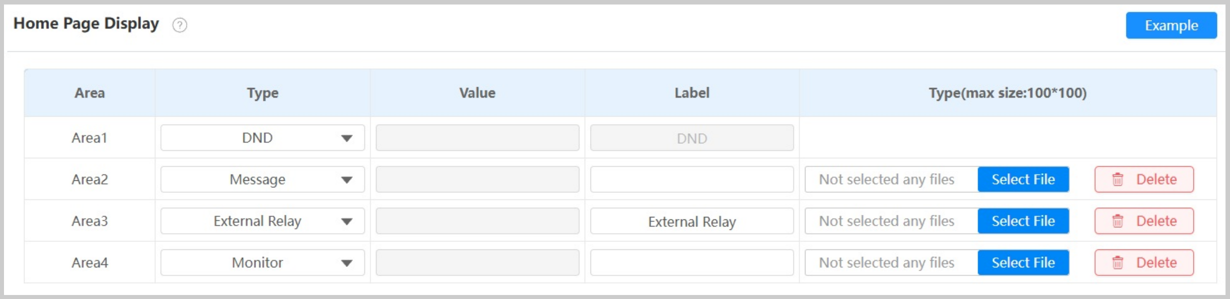
Model S567
Software Version 1.4
Firmware Version 567.30.13.503
Hardware Version 0
MAC Address [redacted]
Used/Total Storage 712M/9.0G

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.

On the Web Interface

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

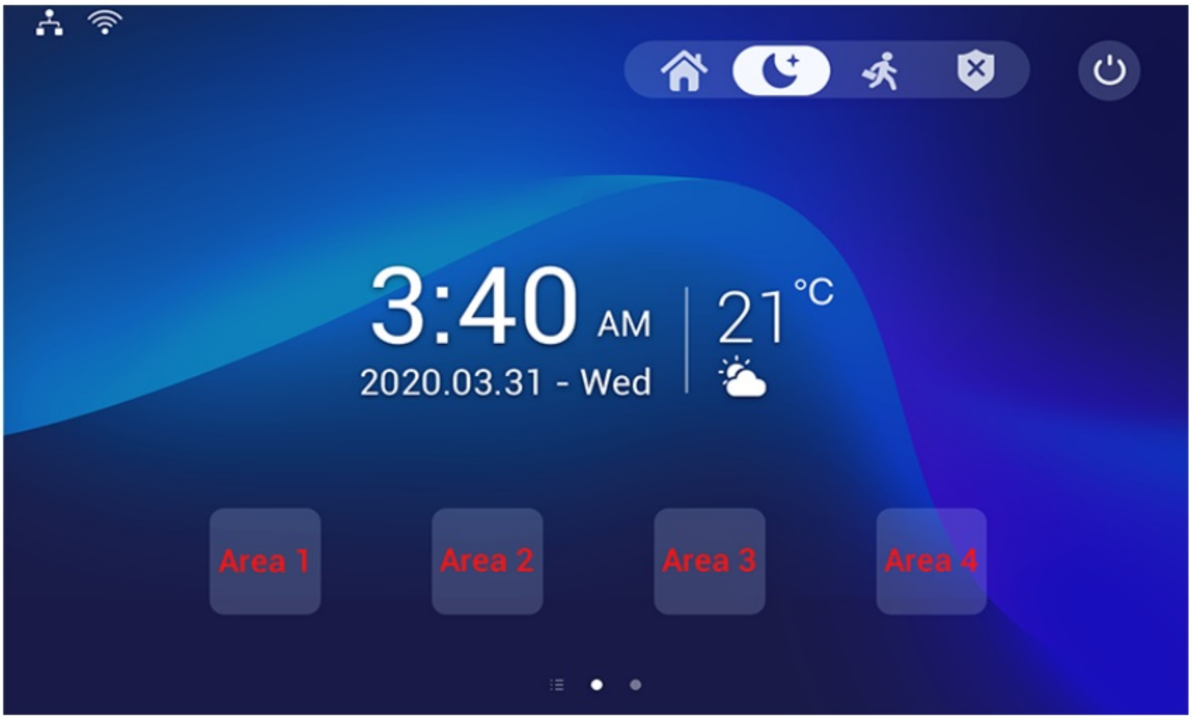


Home Page Display

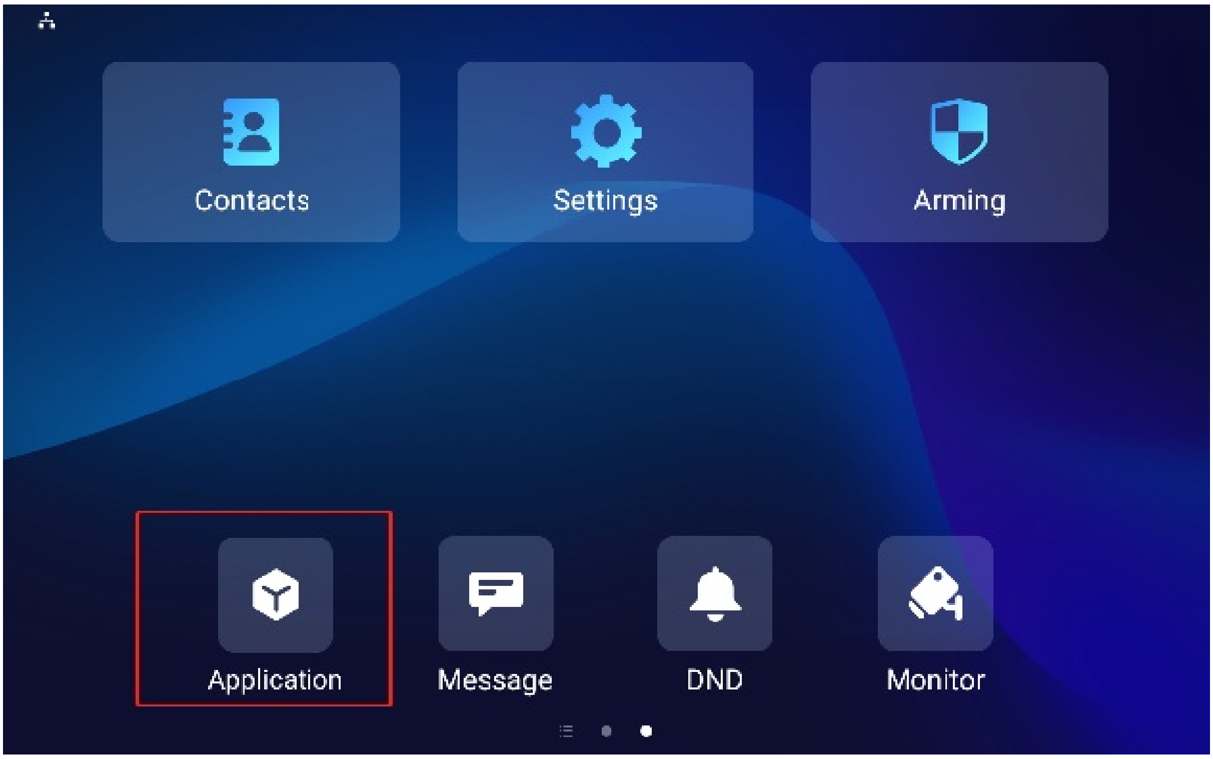
Area	Type	Value	Label	Type(max size:100*100)
Area1	DND		DND	
Area2	Message			Not selected any files
Area3	External Relay		External Relay	Not selected any files
Area4	Monitor			Not selected any files

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

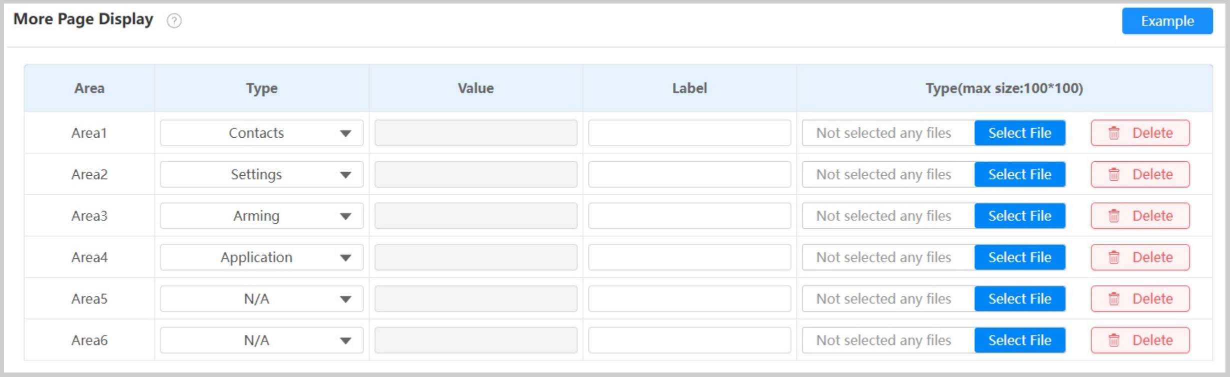
You can click **Example** to see the icon layout.



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



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



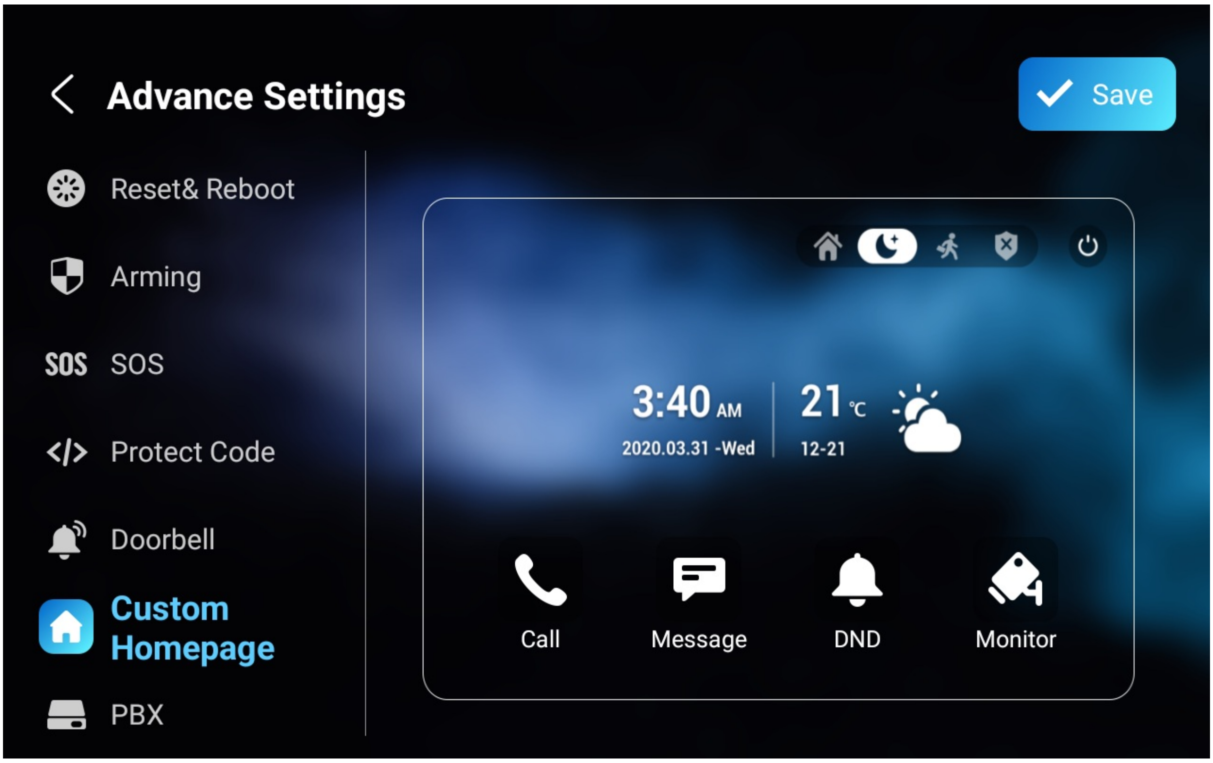
More Page Display

Example

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

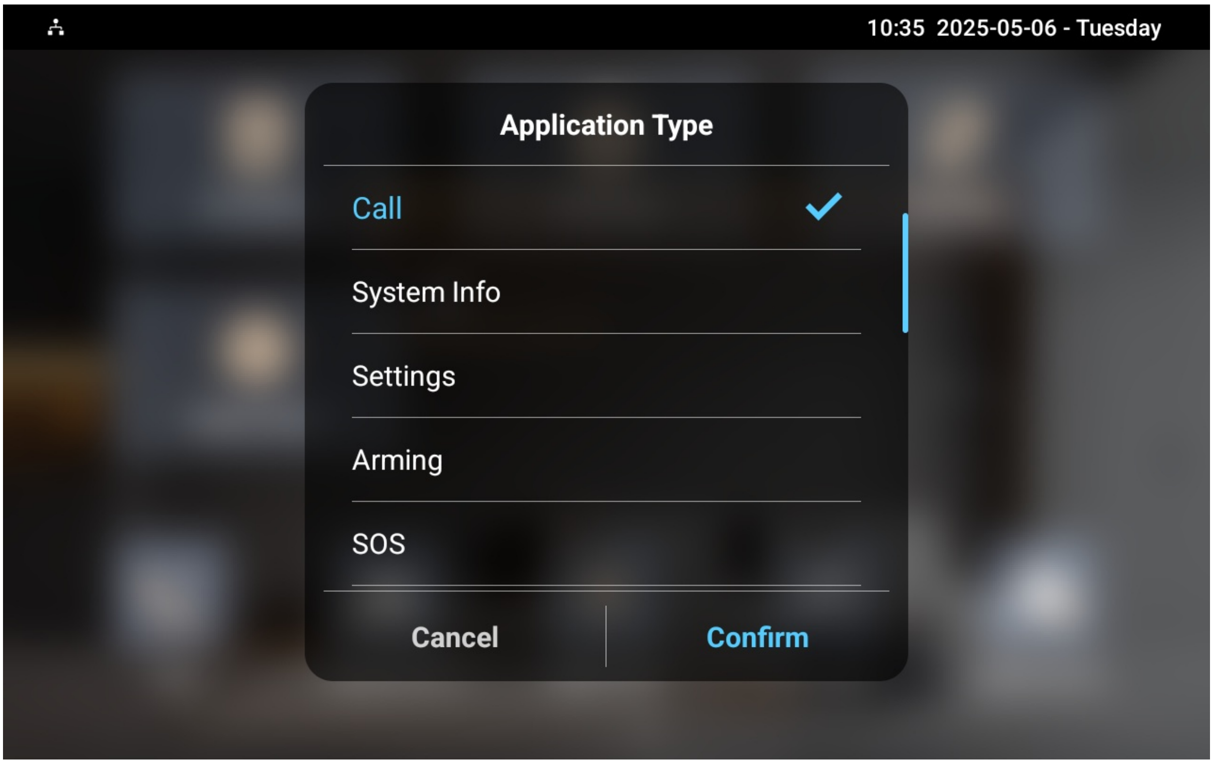
You can also customize the homepage display by selecting your favorite functions on the device screen.

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.



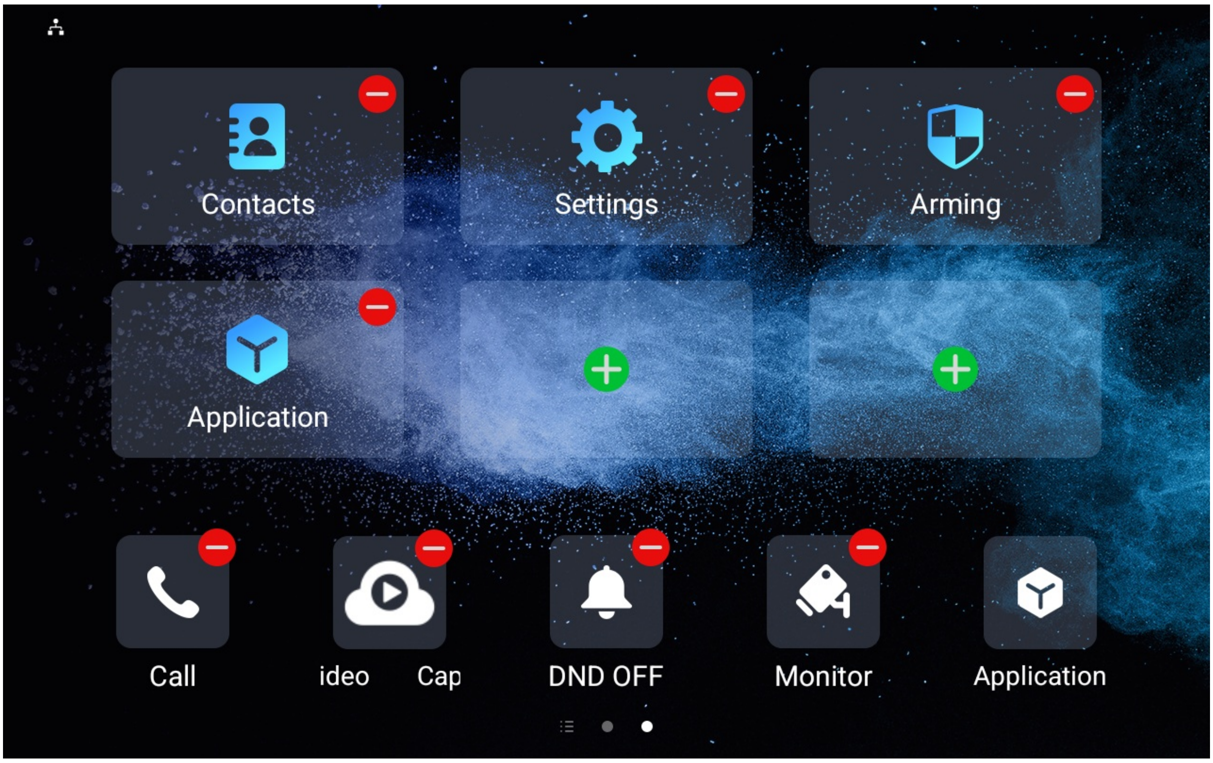
On the Device

Users can press a tab for about 3 seconds on the home or more screen to change its application type.



Users can remove and add desired tabs by long-pressing a specific tab until ⊖ and ⊕ icons appear.

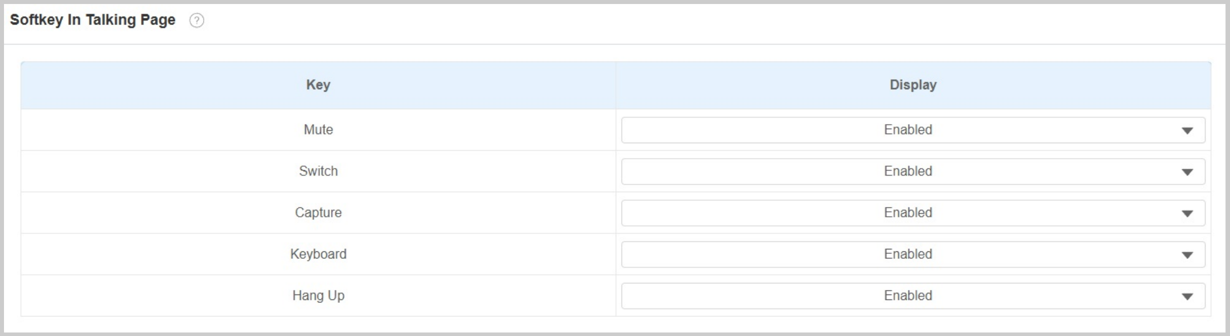
Tap ⊖ to remove a tab and tap ⊕ to add one.



Function Tabs Configuration

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

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

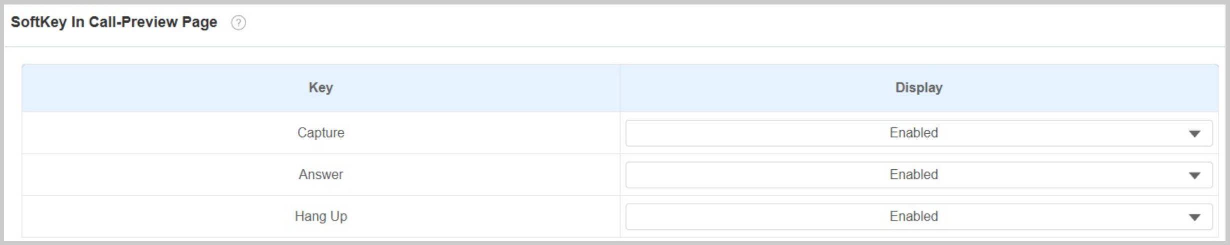


Softkey In Talking Page

Key	Display
Mute	Enabled
Switch	Enabled
Capture	Enabled
Keyboard	Enabled
Hang Up	Enabled

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

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

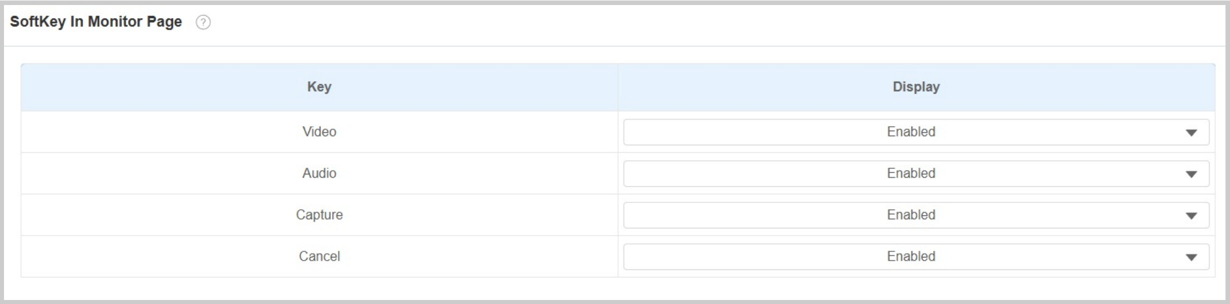


SoftKey In Call-Preview Page

Key	Display
Capture	Enabled
Answer	Enabled
Hang Up	Enabled

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

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



SoftKey In Monitor Page

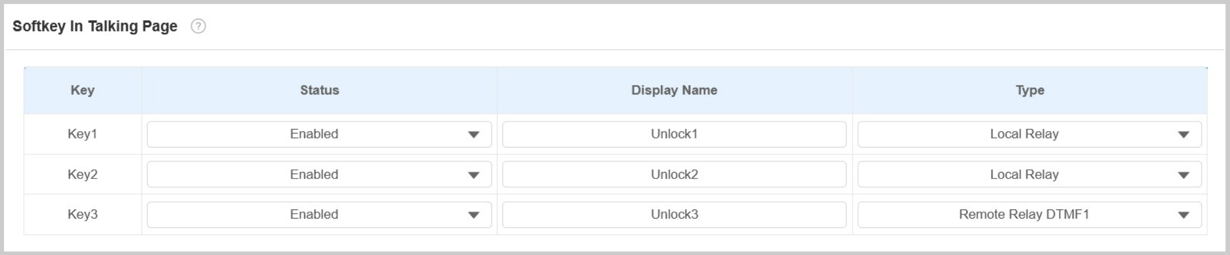
Key	Display
Video	Enabled
Audio	Enabled
Capture	Enabled
Cancel	Enabled

- **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 Tabs Configuration

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

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

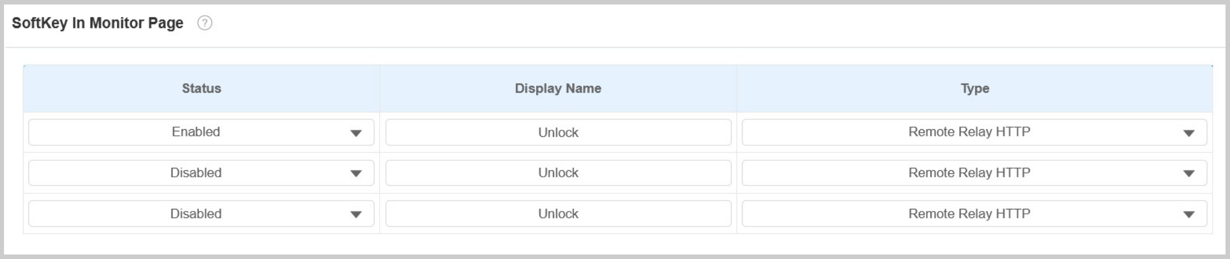


Softkey In Talking Page

Key	Status	Display Name	Type
Key1	Enabled	Unlock1	Local Relay
Key2	Enabled	Unlock2	Local Relay
Key3	Enabled	Unlock3	Remote Relay DTMF1

- **Status**: With it enabled, the unlock tab will be displayed on the talking screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup. When you set Type to **Remote Relay HTTP1-10** and the door phone is connected to multiple locks, the unlock options will display when users tap the Unlock tab. In this case, users can open a specific door while keeping other doors closed.

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

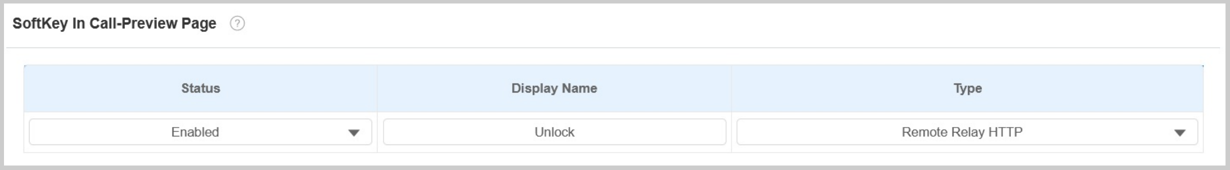


SoftKey In Monitor Page

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

- **Status**: With it enabled, the unlock tab will be displayed on the monitor screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup. When you set Type to **Remote Relay HTTP1-10** and the door phone is connected to multiple locks, the unlock options will display when users tap the Unlock tab. In this case, users can open a specific door while keeping other doors closed.

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



SoftKey In Call-Preview Page

Status	Display Name	Type
Enabled	Unlock	Remote Relay HTTP

- **Status**: With it enabled, it will be displayed on the call preview screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup. When you set Type to **Remote Relay HTTP1-10** and the door phone is connected to multiple locks, the unlock options will display when users tap the Unlock tab. In this case, users can open a specific door while keeping other doors closed.

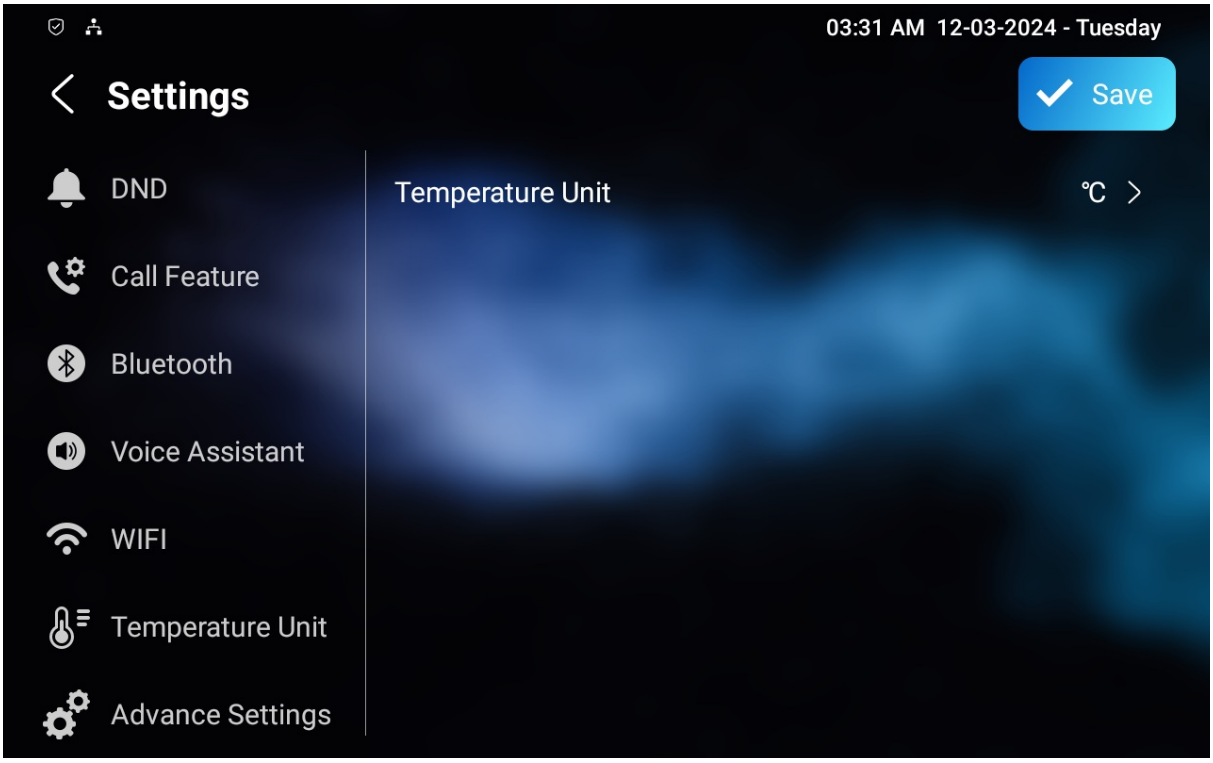
> **Note**
>
> Please refer to the Access Control Configuration chapter for different unlock types setup.

Temperature Display Setting

When the device is connected to the SmartPlus Cloud, temperature information will be displayed on the device's Home screen.

You can switch the temperature unit between Fahrenheit and Centigrade on the device.

To set it up, go to the **Settings > Temperature Unit** screen.



03:31 AM 12-03-2024 - Tuesday

Settings

Save

Temperature Unit ℃

Note

Please refer to **Configure Weather Display on Indoor Monitors** for configuration details.

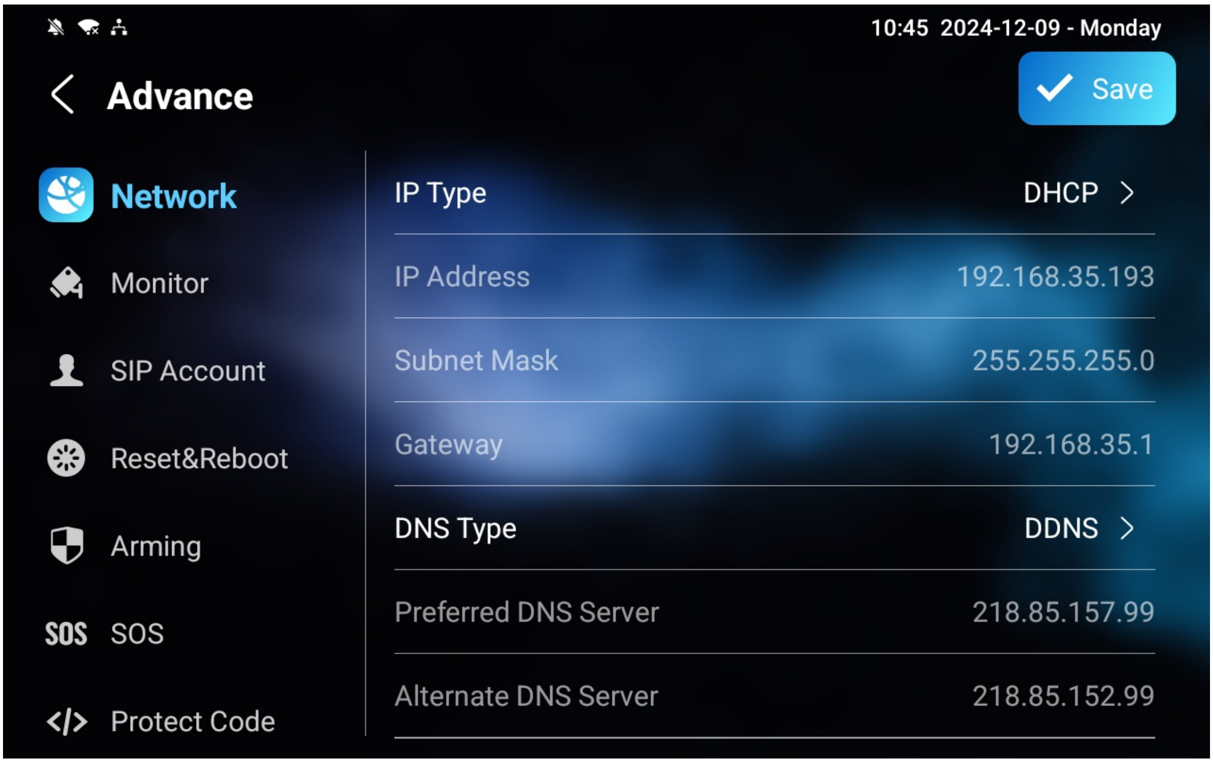
Network Setting & Other Connection

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.



IP Type: DHCP

IP Address: 192.168.35.193

Subnet Mask: 255.255.255.0

Gateway: 192.168.35.1

DNS Type: DDNS

Preferred DNS Server: 218.85.157.99

Alternate DNS Server: 218.85.152.99

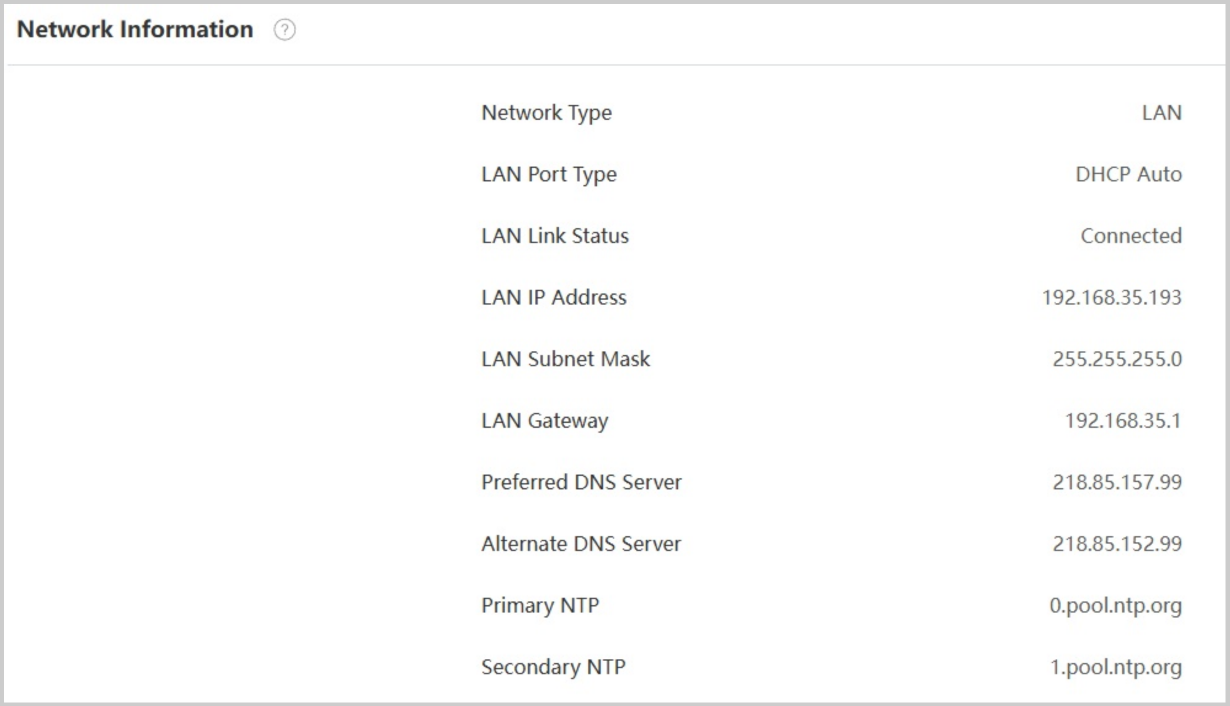
- **IP Type:** DHCP mode is the default network connection. The device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. In static IP mode, the IP address, subnet mask, default gateway, and DNS server address have to be manually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

- **DNS Type**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network.
    - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
    - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred & Alternate DNS Server**: The preferred and alternate Domain Name Server(DNS). The device will connect to the alternate server when the primary server is unavailable.
- **Hotspot Enabled**: With it enabled, S567 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

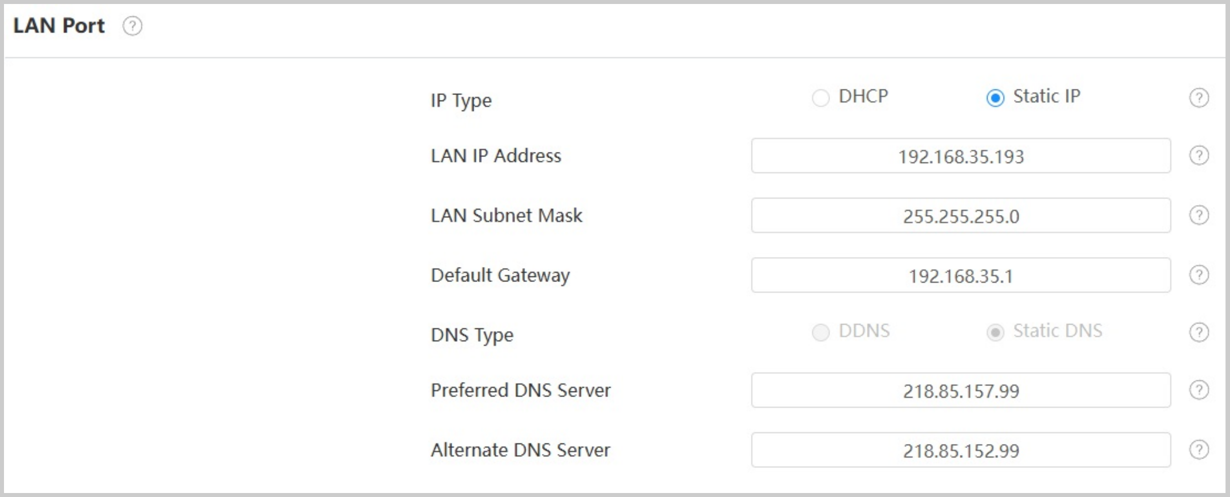
Check the network on the web **Status > Network Information** interface.



Network Information

Network Type	LAN
LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.35.193
LAN Subnet Mask	255.255.255.0
LAN Gateway	192.168.35.1
Preferred DNS Server	218.85.157.99
Alternate DNS Server	218.85.152.99
Primary NTP	0.pool.ntp.org
Secondary NTP	1.pool.ntp.org

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

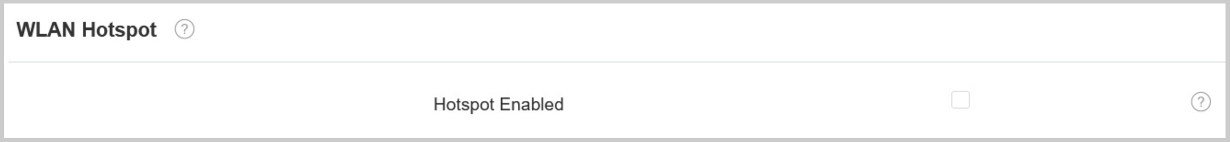


LAN Port

IP Type	○ DHCP	● Static IP
LAN IP Address	192.168.35.193	
LAN Subnet Mask	255.255.255.0	
Default Gateway	192.168.35.1	
DNS Type	○ DDNS	● Static DNS
Preferred DNS Server	218.85.157.99	
Alternate DNS Server	218.85.152.99	

- **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**: Set up the IP address when the static IP mode is selected. To access the device's web settings, you computer should be on the same local network as the device.
- **LAN Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not. For example, if the subnet mask is 255.255.255.0, it means that devices with similar starting IPs (like 192.168.1.x) are in the same network.
- **Default Gateway**: The gateway is like a bridge between your device and other networks, such as the internet. Usually, it's the IP address of your router.
- **DNS Type**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network.
  - **DDNS**: Dynamic DNS. It is obtained automatically through the DHCP server.
  - **Static DNS**: When selected, you need to enter the DNS manually.
- **Preferred/Alternate DNS Server**: The device will connect to the alternate server when the primary server is unavailable.

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



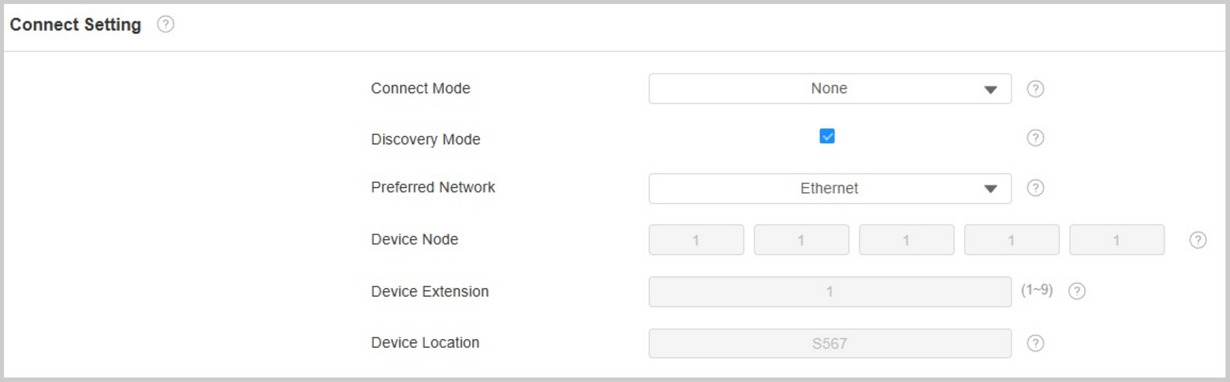
WLAN Hotspot

Hotspot Enabled □

Device Deployment in Network

To facilitate device control and management, configure Akuvox intercom devices with details such as location, operation mode, address, and extension numbers.

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



Connect Setting

Connect Mode	None
Discovery Mode	☑
Preferred Network	Ethernet
Device Node	1 1 1 1 1
Device Extension	1 (1~9)
Device Location	S567

- **Connect Mode**: It is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud,** or **None**. **None** is the default factory setting indicating the device is not in any server type.

    - **None**: None is the default factory setting indicating the device is not in any server type. Devices connect directly to each other or within a local area network (LAN) without relying on external servers.
    - **Cloud**: The device is connected to the SmartPlus Cloud, a cloud-based system simplifying property access management. The Cloud mode allows devices to interact intelligently with one another and the mobile SmartPlus App, backing up data daily and on different hosts. It suits projects requiring smart, flexible, and secure deployment and management.
    - **SDMC**: The device is connected to the SDMC, a management platform designed for on-premise projects. The SDMC mode manages and backs up data remotely on a local network. It also boasts many features suitable for projects requiring high privacy, lower cost, and centralized management.

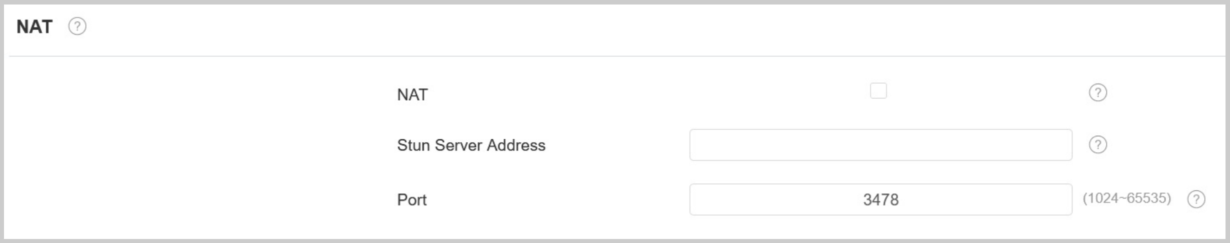
- **Discovery Mode**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Preferred Network**: Specify the preferred network connection, WLAN or Ethernet. It is Ethernet by default. When Ethernet is unavailable, the device will automatically switch to a WLAN connection and vice versa.
- **Device Node**: Available for **None** server mode. Uneditable in Cloud and SDMC mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for **None** server mode. Uneditable in Cloud and SDMC mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for **None** server mode. Uneditable in Cloud and SDMC mode.

Device NAT Setting

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

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

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

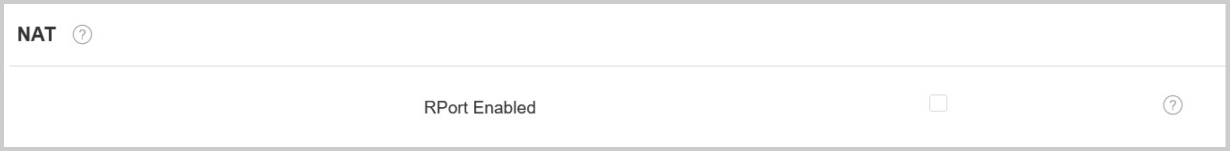


NAT

NAT	□	
Stun Server Address		
Port	3478	(1024~65535)

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

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



NAT

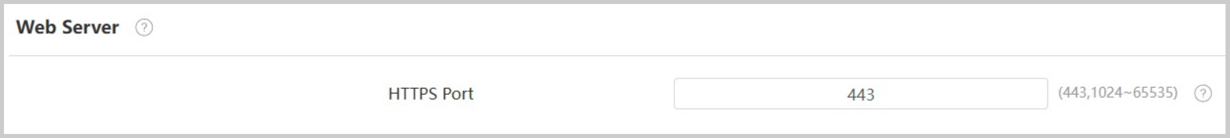
RPort Enabled □

- **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.

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



Web Server

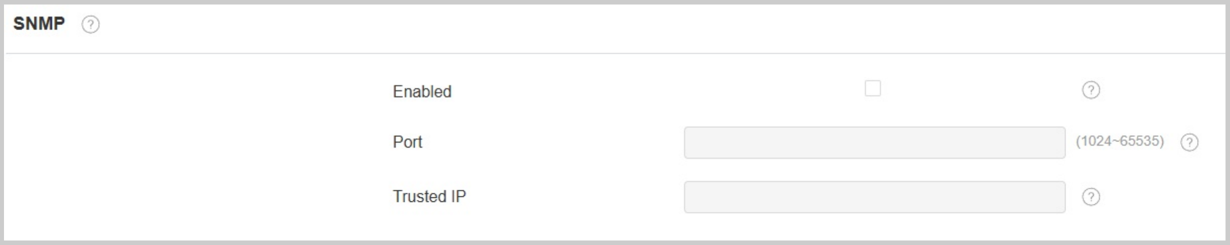
HTTPS Port 443 (443,1024~65535)

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

SNMP Setting

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

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



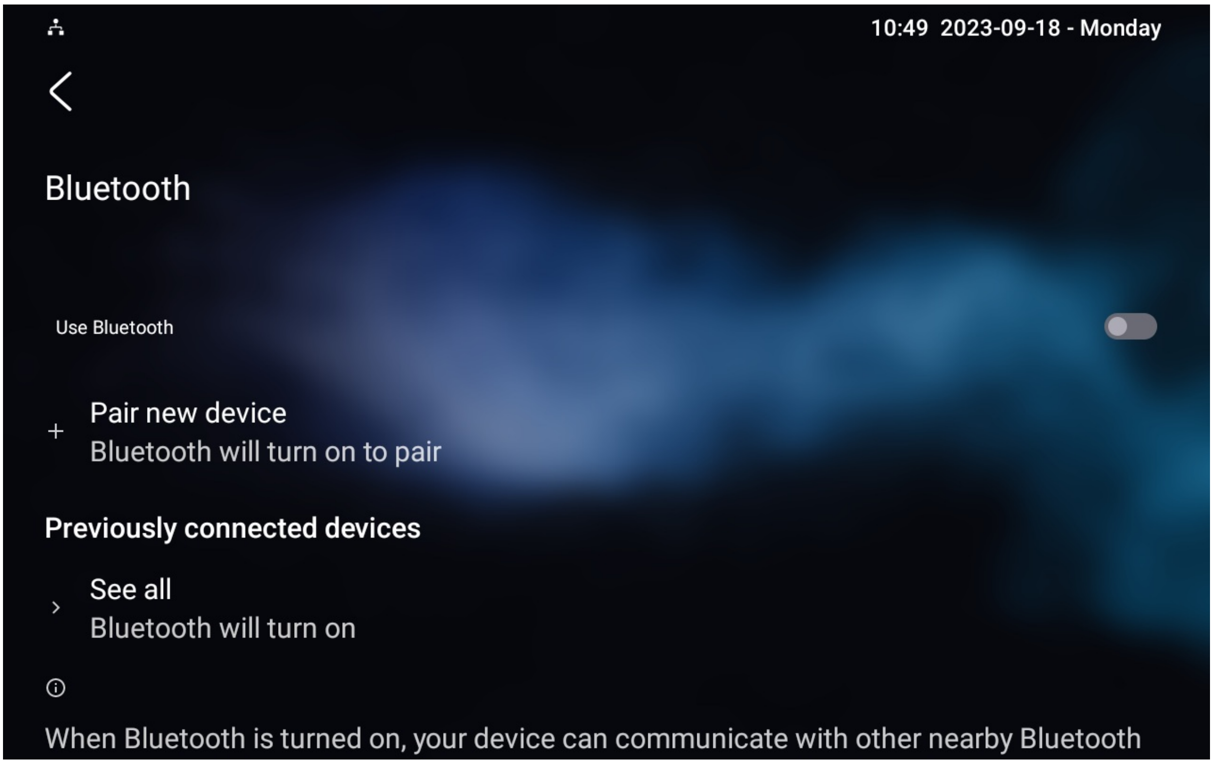
SNMP

Enabled	□	?
Port		(1024~65535) ?
Trusted IP		?

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

Device Bluetooth Setting

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.



10:49 2023-09-18 - Monday

Bluetooth

Use Bluetooth

Pair new device
Bluetooth will turn on to pair

Previously connected devices

See all
Bluetooth will turn on

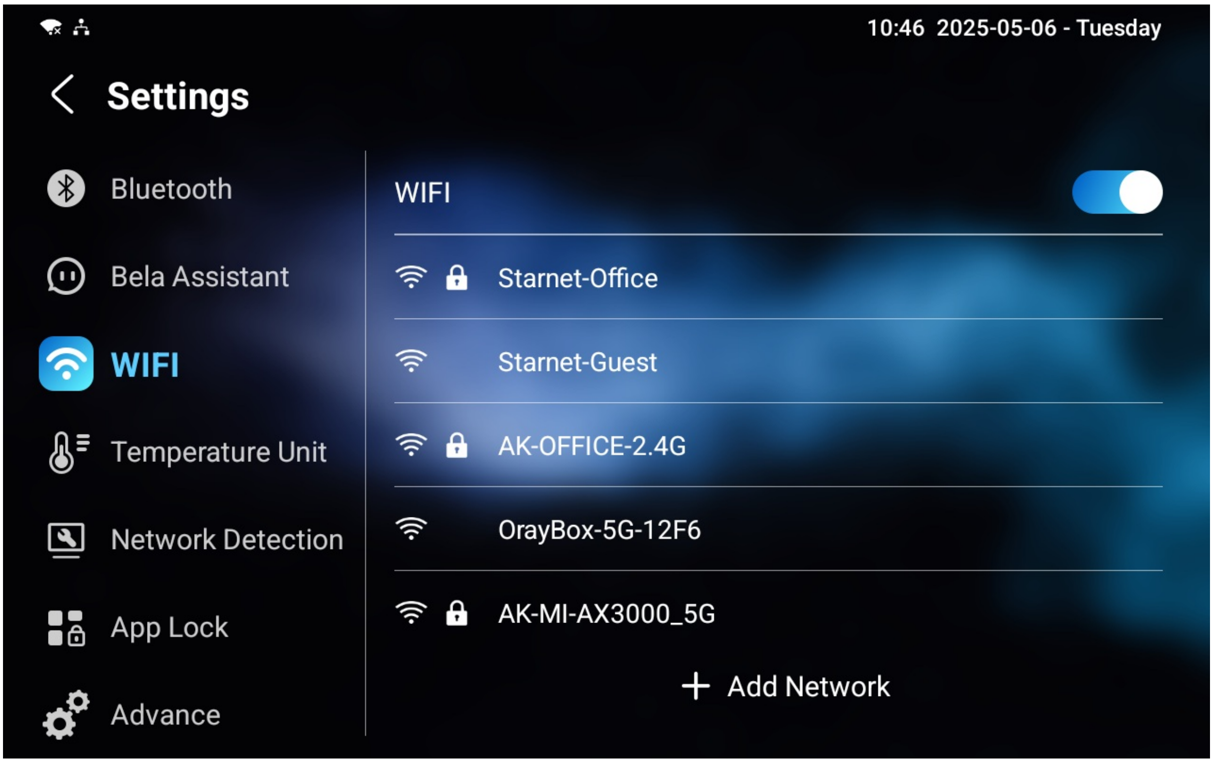
When Bluetooth is turned on, your device can communicate with other nearby Bluetooth

- **Use Bluetooth**: When enabled, other Bluetooth devices will display.
- **Pair new device**: Tap to pair with available Bluetooth devices.
- **Previously connected devices**: Tap **See all** to view the previously connected devices.

Device Wi-Fi Setting

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

Tap the desired Wi-Fi and enter the password to connect.



10:46 2025-05-06 - Tuesday

Settings

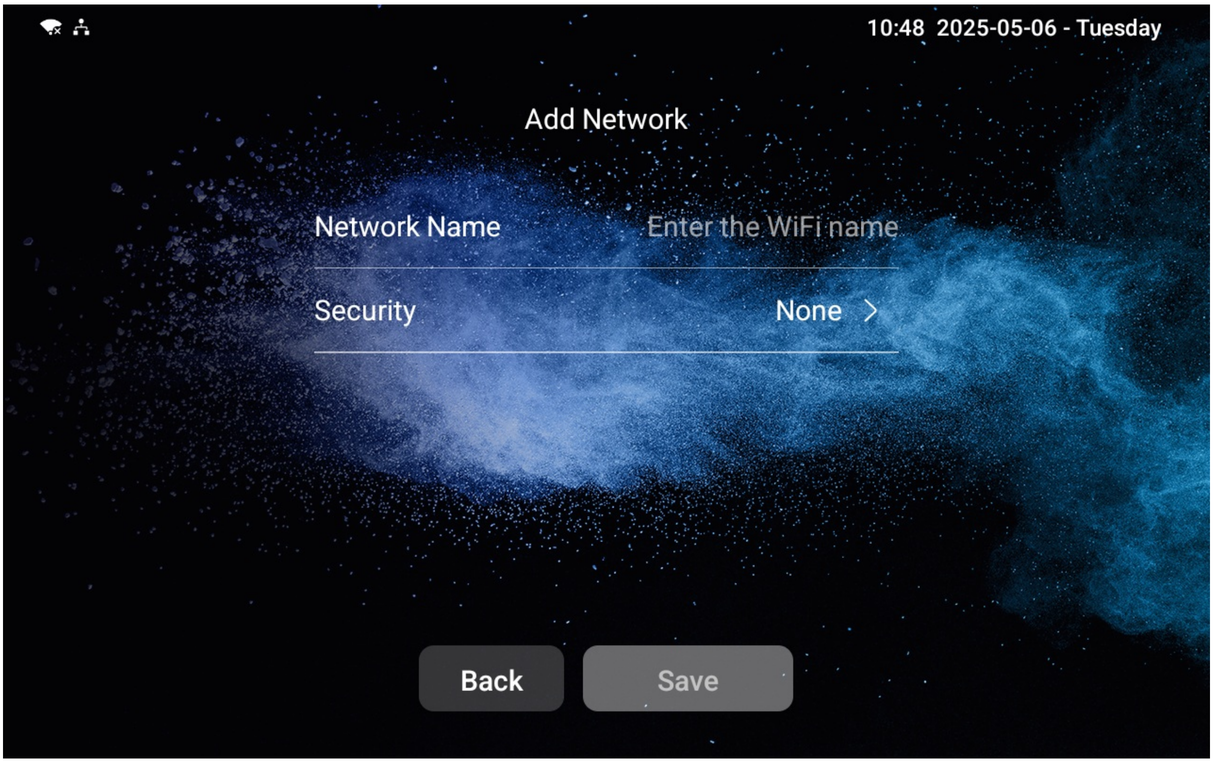
- Bluetooth
- Bela Assistant
- WIFI
- Temperature Unit
- Network Detection
- App Lock
- Advance

WIFI: on

- Starnet-Office
- Starnet-Guest
- AK-OFFICE-2.4G
- OrayBox-5G-12F6
- AK-MI-AX3000_5G

+ Add Network

- **Add Network**: Tap to add a Wi-Fi manually.
  - **Security**: Select the network encryption type and enter the password to connect. The default is **None**.



10:48 2025-05-06 - Tuesday

Add Network

Network Name: Enter the WiFi name

Security: None >

Contacts Configuration

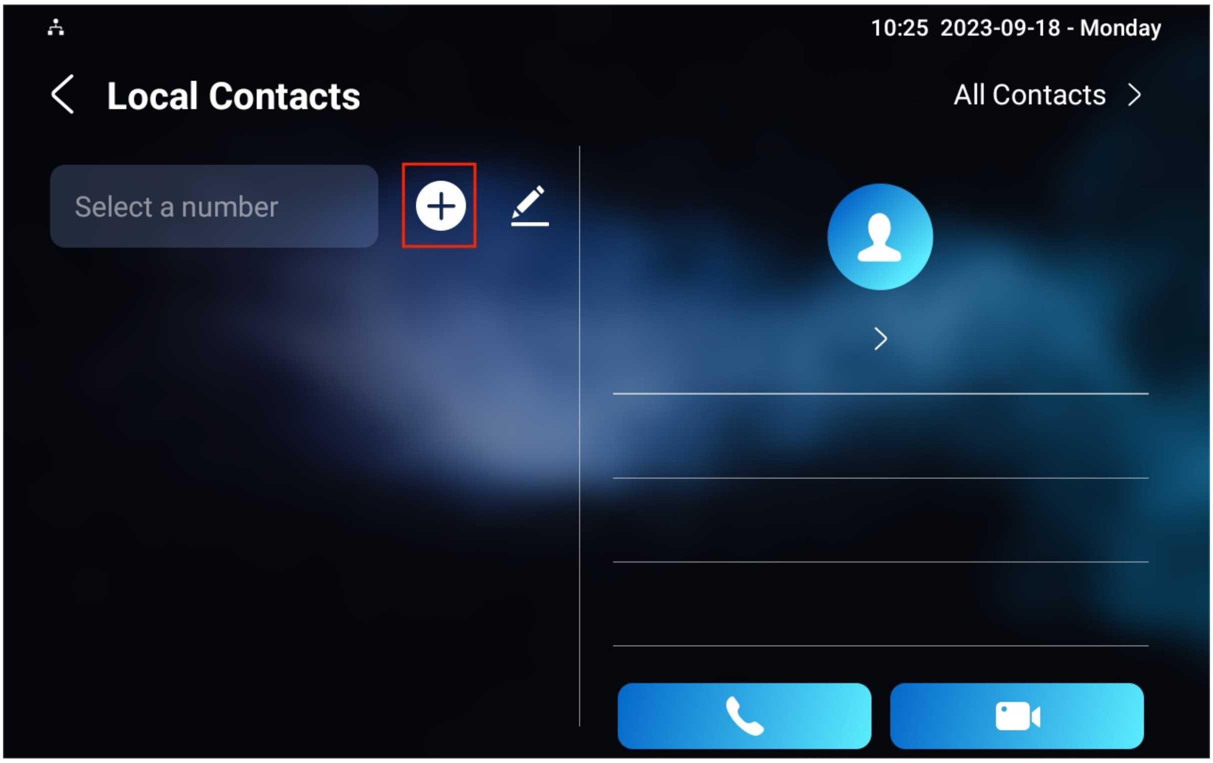
The local contact information is used to initiate SIP or IP calls to other intercom devices. You can group the contact information to facilitate group calls. Moreover, you can add the camera URL of the target device, allowing users to view its live stream during a call or a call preview.

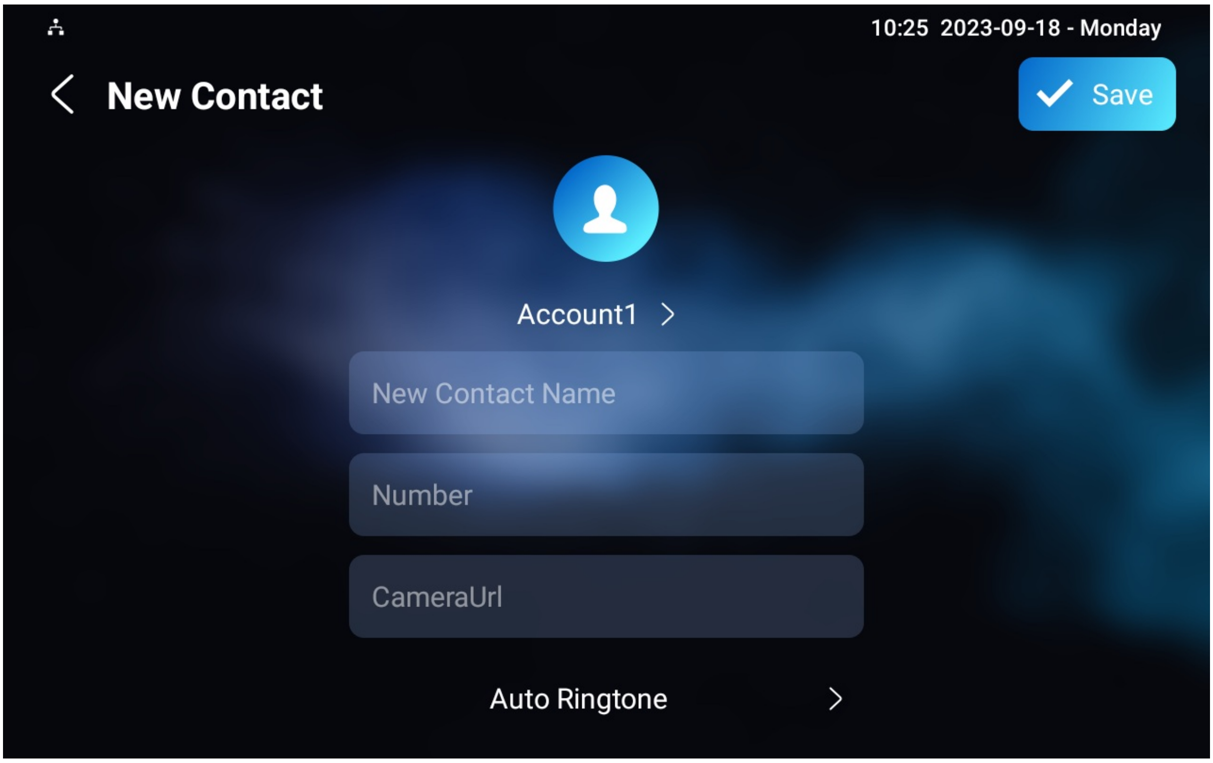
On the Device

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

Add Local Contacts

Tap the **Add** icon to add a contact. You can add up to 3,000 contacts.





10:25 2023-09-18 - Monday

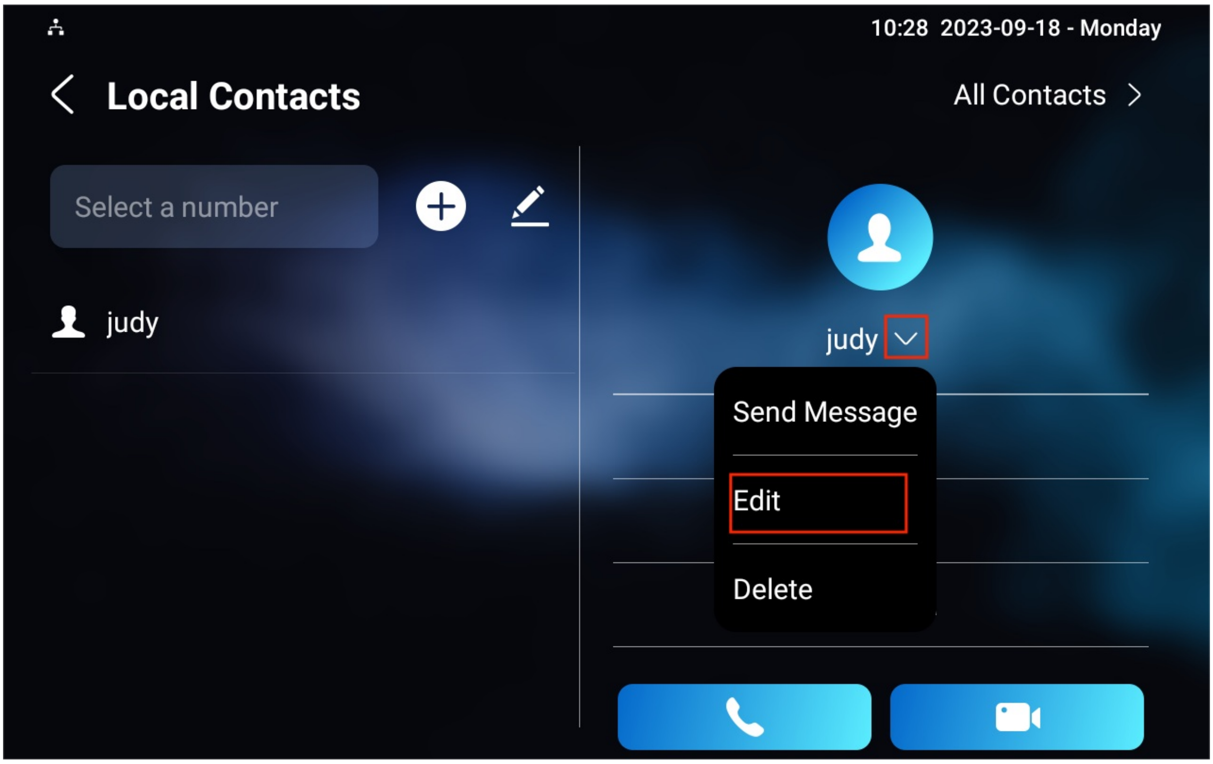
New Contact

- **Account**: 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

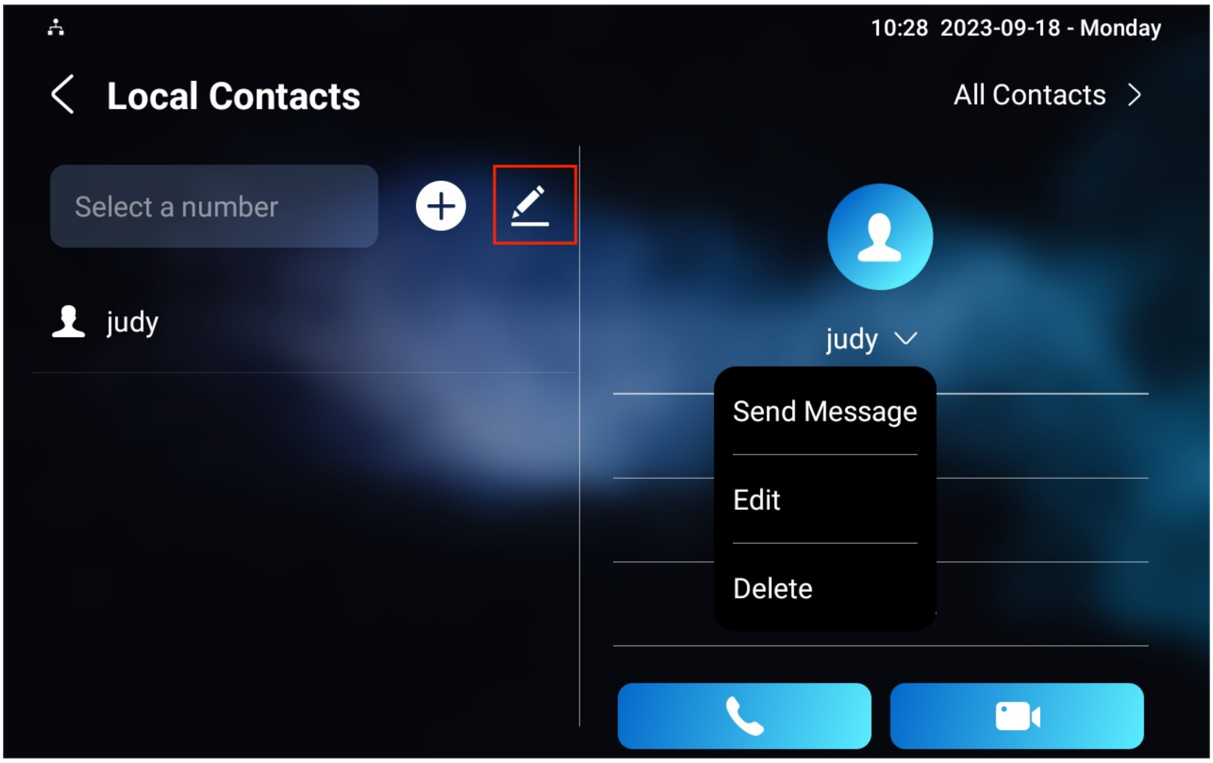
You can check and edit the existing contacts in the contacts list. Choose one and click **Edit** to modify.

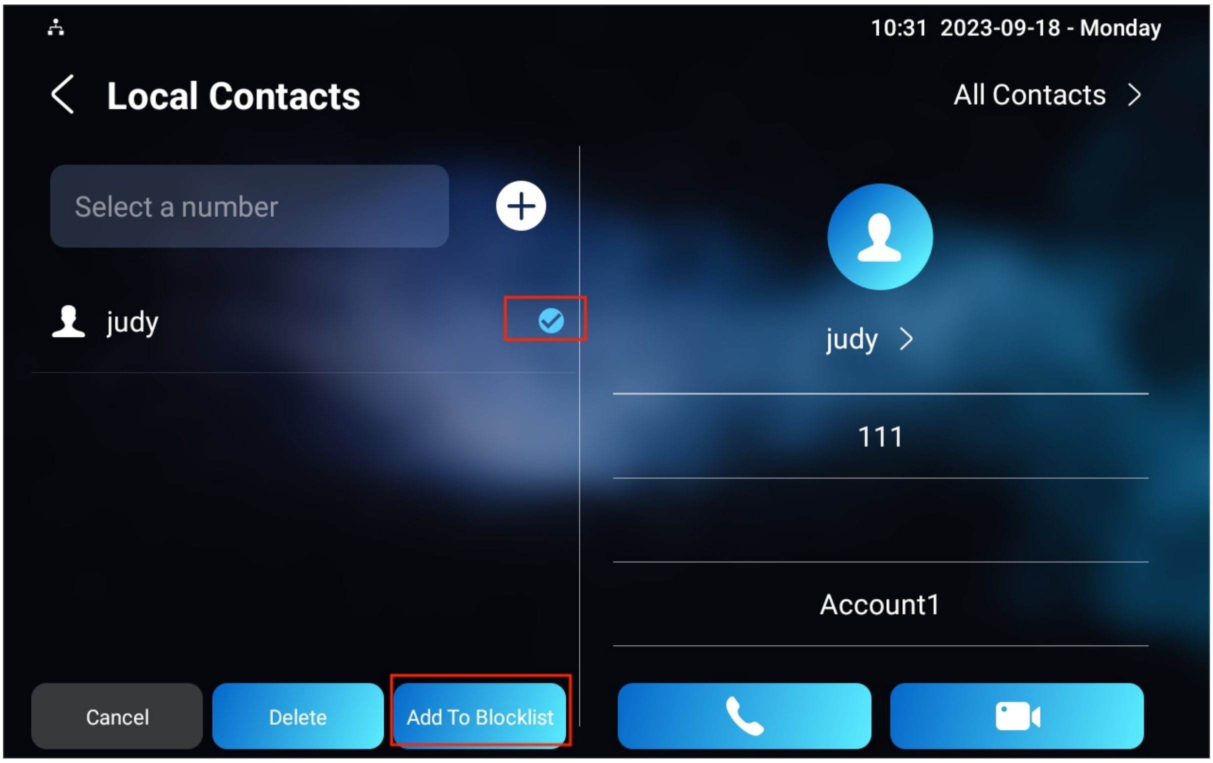


Blocklist Contacts

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**.





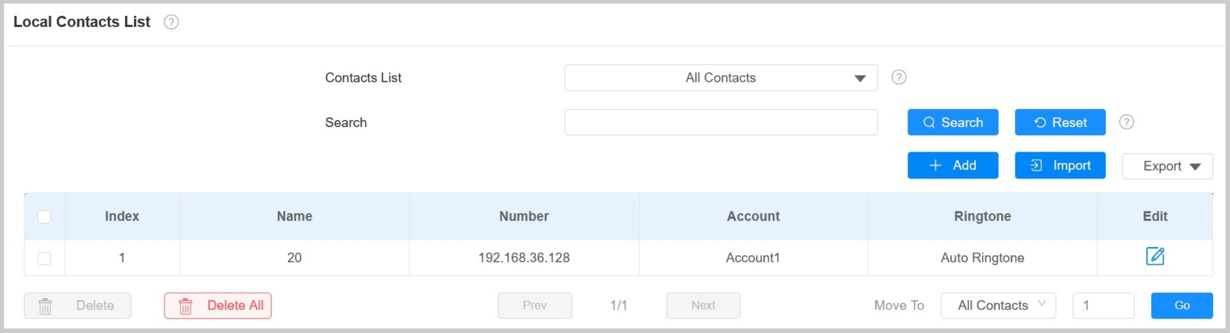
Note

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

On the Web Interface

Add Local Contacts

To add contacts, go to **Contacts > Local Contacts > Local Contacts List** interface, then click **+Add**. You can add up to 3,000 contacts.

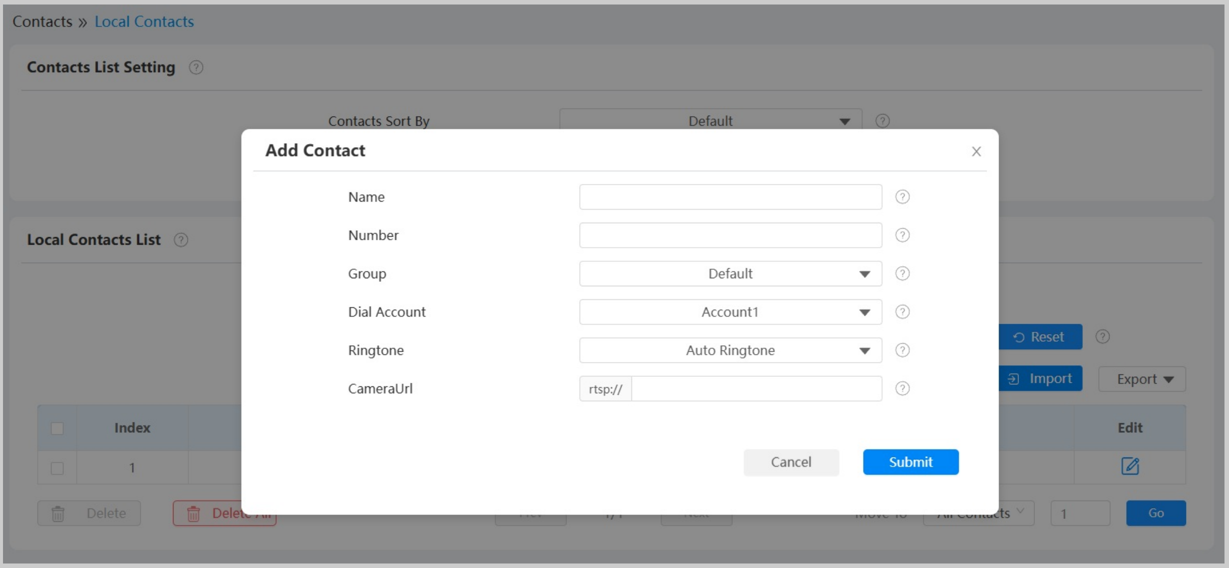


Local Contacts List

Contacts List: All Contacts

Search:

□	Index	Name	Number	Account	Ringtone	Edit
□	1	20	192.168.36.128	Account1	Auto Ringtone	✎


Contacts » Local Contacts

Contacts List Setting

Contacts Sort By: Default

Add Contact

Name:

Number:

Group: Default

Dial Account: Account1

Ringtone: Auto Ringtone

CameraUrl: rtsp://

Local Contacts List

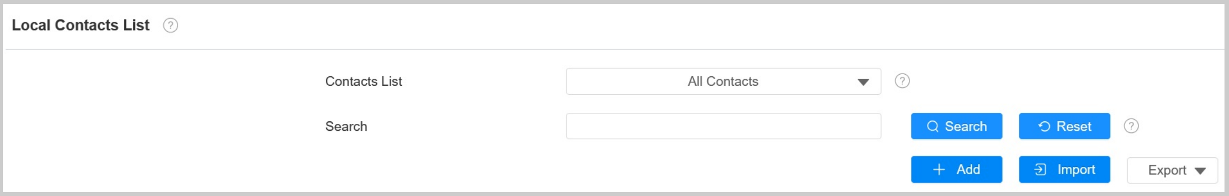
- **Contacts List**: **All Contacts** displays all the contacts in the contact list. **Blocklist** displays the contacts in the blocklist.
- **Search**: Search a contact by its name or number.
- **Name**: The contact's name to distinguish it from others.
- **Number**: The SIP or IP number of the contact.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

> **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.

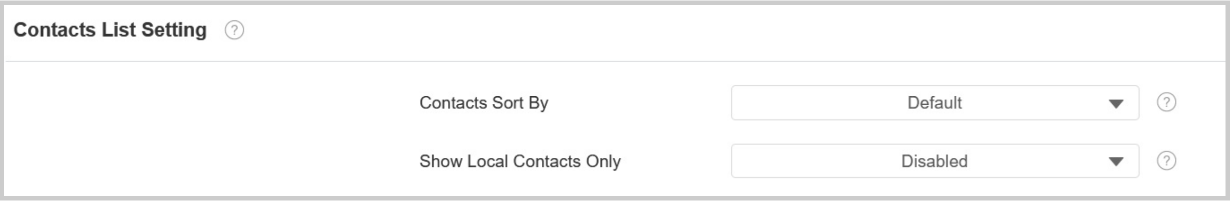

Local Contacts List

Contacts List: All Contacts

Search:

Contact List Display

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



Contacts List Setting

Contacts Sort By: Default

Show Local Contacts Only: Disabled

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

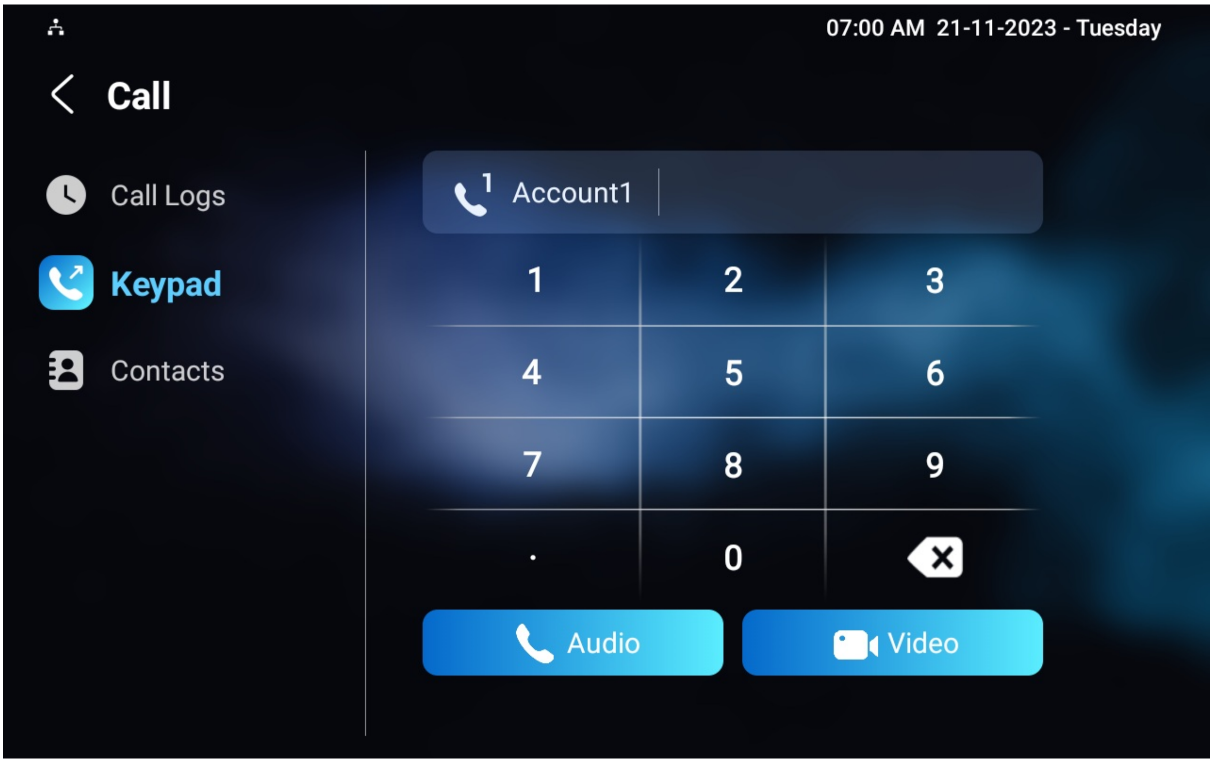
Intercom Call Configuration

IP Call Configuration

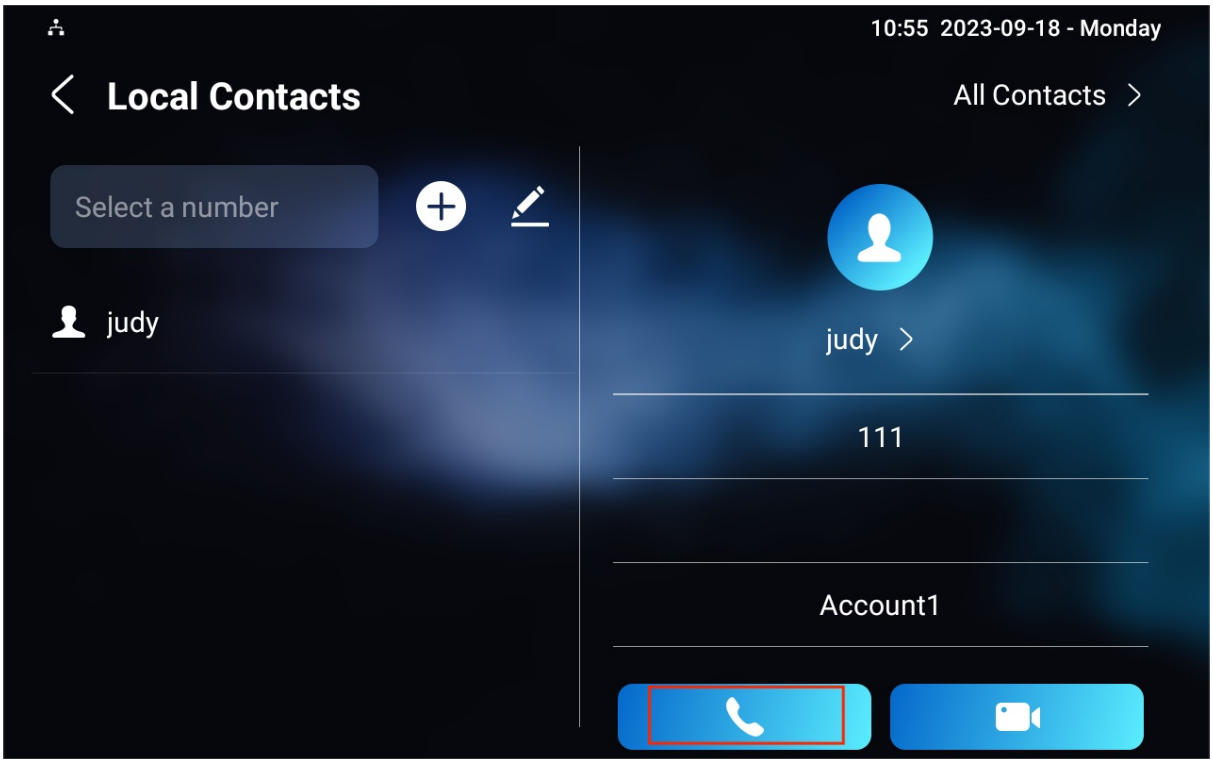
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Make IP Calls

Make a direct IP call on the device **Call > Keypad** screen.
Enter the IP address, e.g., 192.168.35.123, on the soft keyboard, select the account to make the call, and press the **Audio** or **Video** tab to call out.

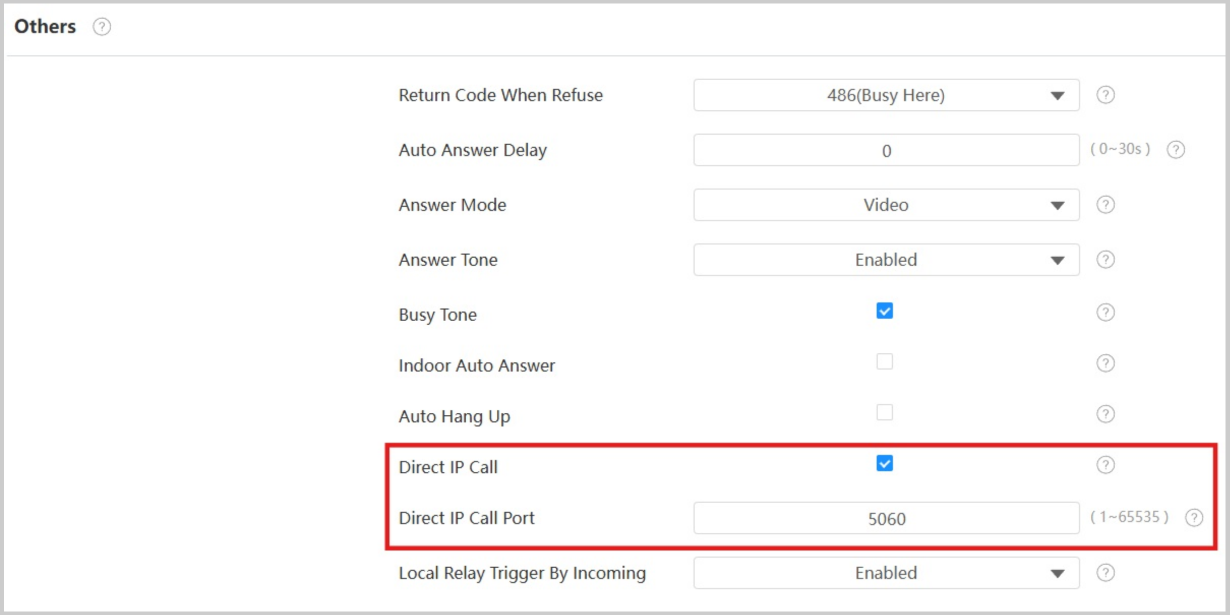


In addition, you can also make IP calls on the **Contacts > Local Contacts** screen.



IP Call Setup

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



Others

Return Code When Refuse	486(Busy Here)	
Auto Answer Delay	0	(0~30s)
Answer Mode	Video	
Answer Tone	Enabled	
Busy Tone	☑	
Indoor Auto Answer	□	
Auto Hang Up	□	
Direct IP Call	☑	
Direct IP Call Port	5060	(1~65535)
Local Relay Trigger By Incoming	Enabled	

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

SIP Call 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.

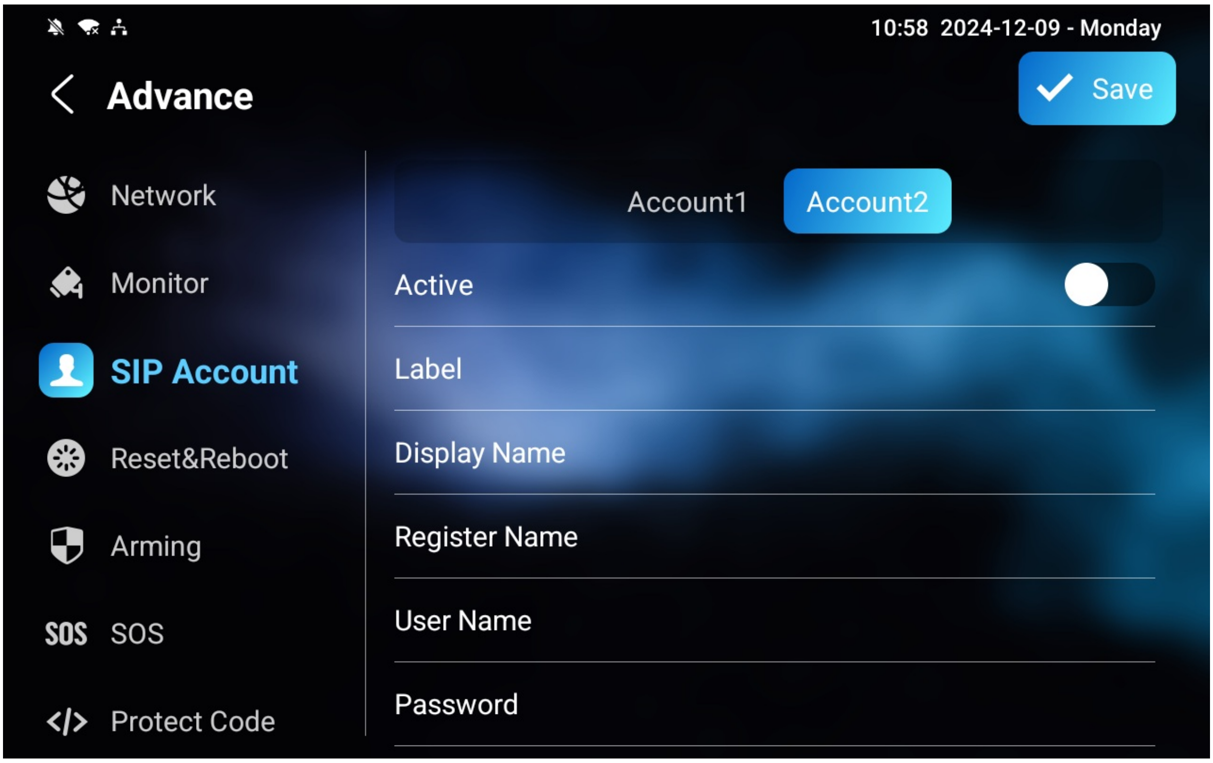
SIP Account Registration

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.

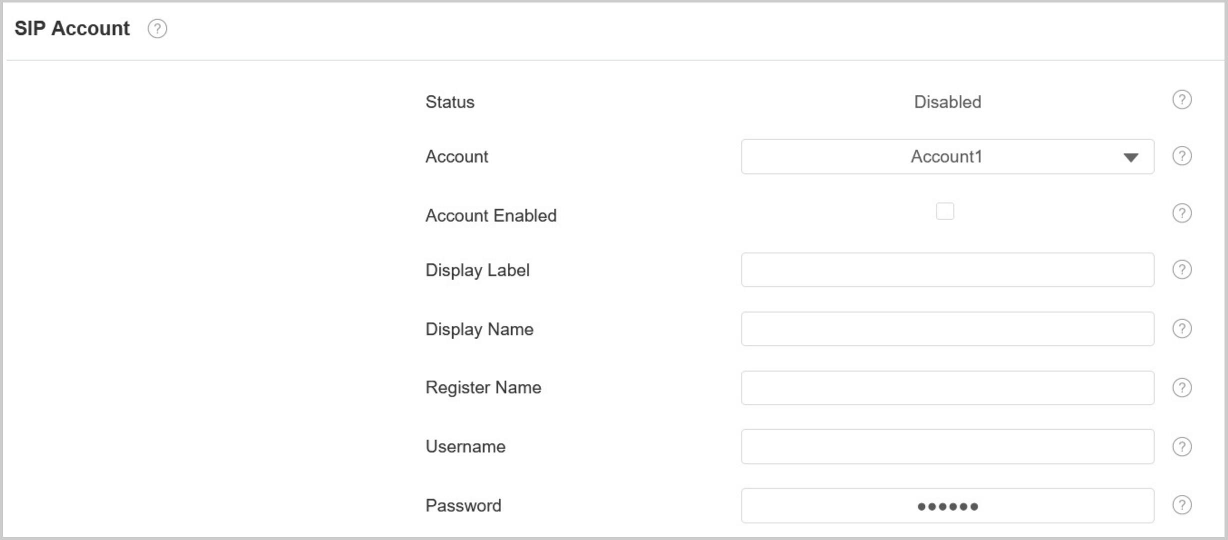
Click here to view the SIP account registration example.

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



- **Account 1/Account 2:** The device supports 2 SIP accounts.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus Cloud service is activated.
  - The system switches to Account 2 if Account 1 is not registered.
- **Active**: Check to activate the registered SIP account.
- **Label**: The label of the device.
- **Display Name**: The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same as the username from the PBX server.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

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



SIP Account

Status	Disabled
Account	Account1
Account Enabled	□
Display Label	
Display Name	
Register Name	
Username	
Password	••••••

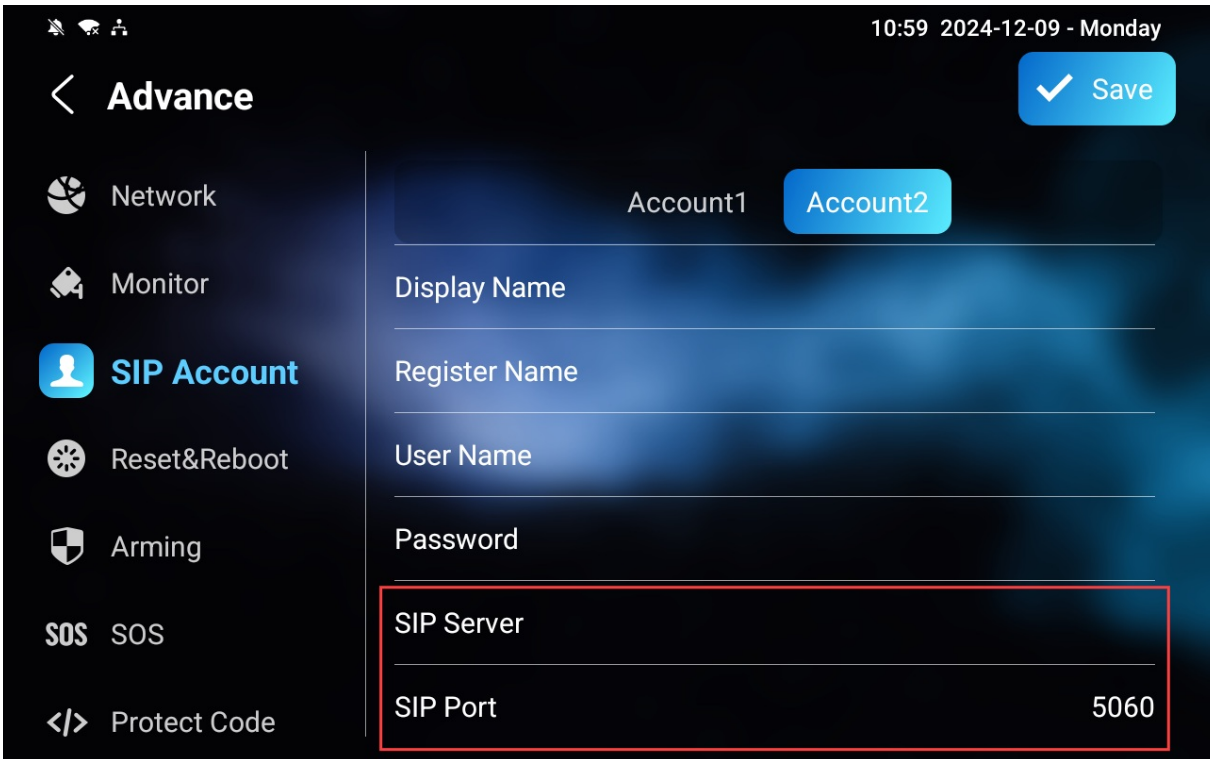
- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same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

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

SIP Server Configuration

SIP servers enable devices to establish and manage call sessions with other intercom devices using the SIP protocol. They can be third-party servers or built-in PBX in Akuvox indoor monitor.

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



Display Name

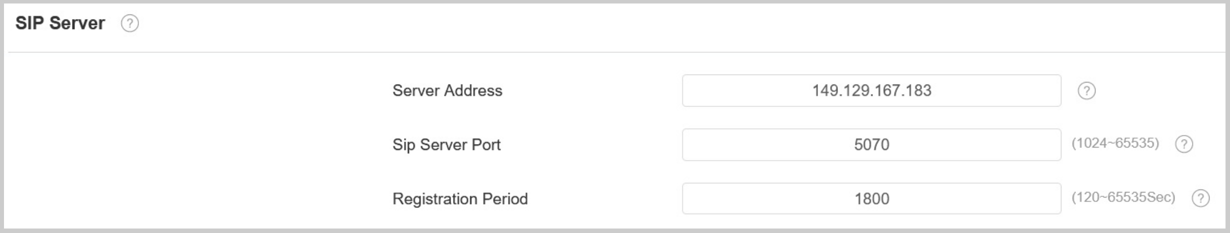
Register Name

User Name

Password

SIP Server

SIP Port 5060



SIP Server

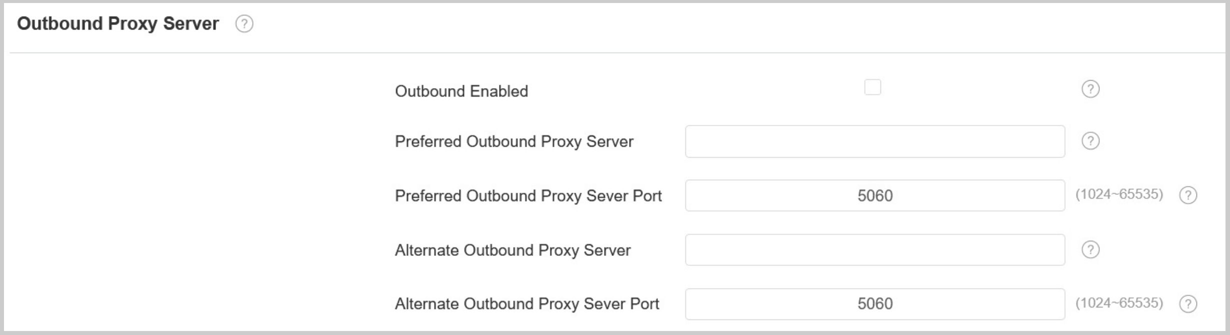
Server Address	149.129.167.183	
Sip Server Port	5070	(1024~65535)
Registration Period	1800	(120~65535Sec)

- **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.



Outbound Proxy Server

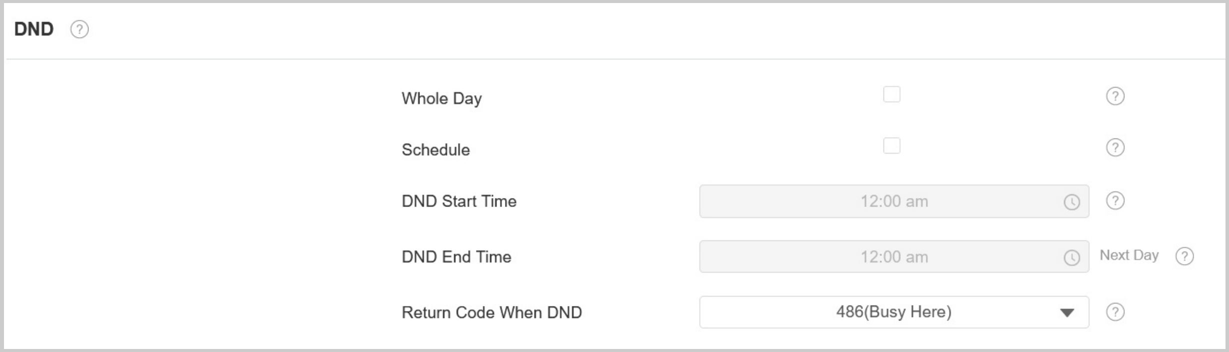
Outbound Enabled	□	
Preferred Outbound Proxy Server		
Preferred Outbound Proxy Sever Port	5060	(1024~65535)
Alternate Outbound Proxy Server		
Alternate Outbound Proxy Sever Port	5060	(1024~65535)

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

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.

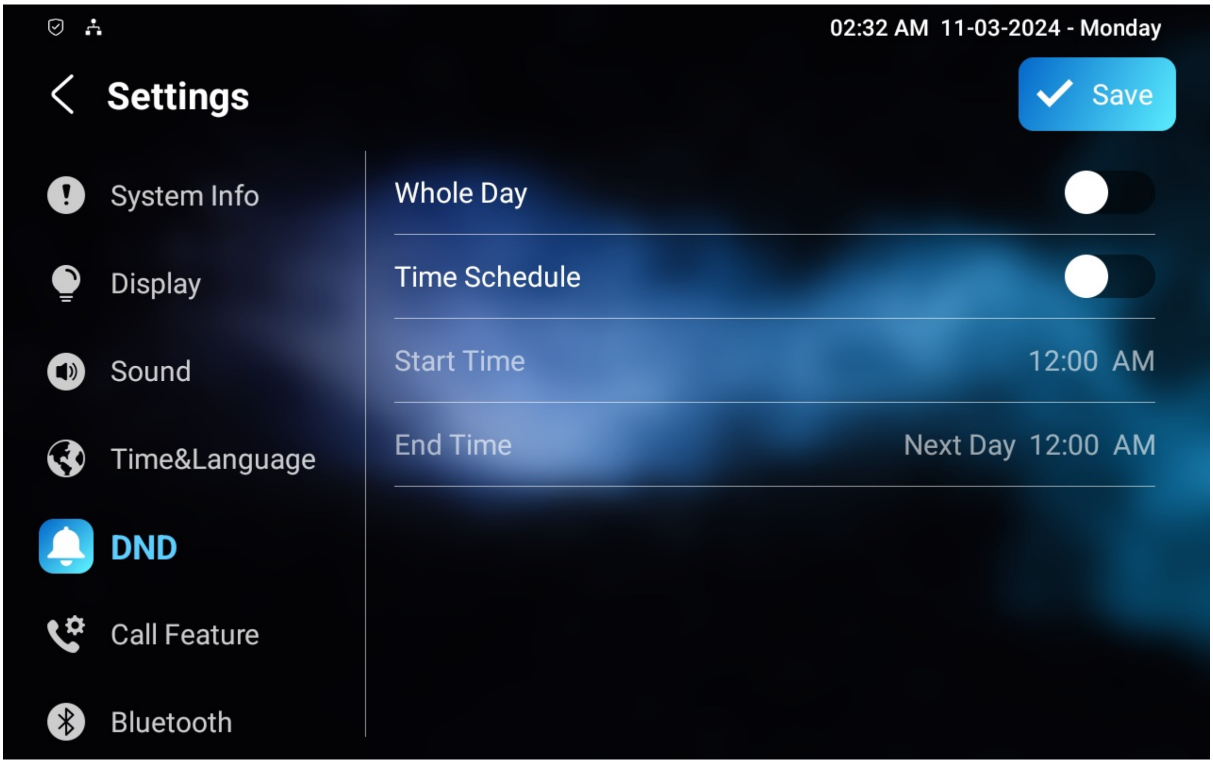


DND

Whole Day	□	
Schedule	□	
DND Start Time	12:00 am	
DND End Time	12:00 am	Next Day
Return Code When DND	486(Busy Here)	

- **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**.



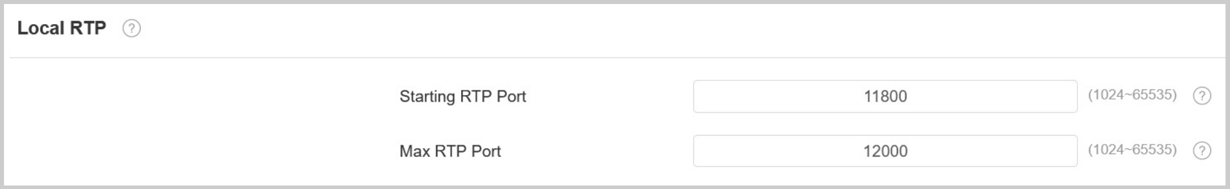
Whole Day ○
Time Schedule ○
Start Time 12:00 AM
End Time Next Day 12:00 AM

Device Local RTP Configuration

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

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

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



Local RTP

Starting RTP Port 11800 (1024~65535)

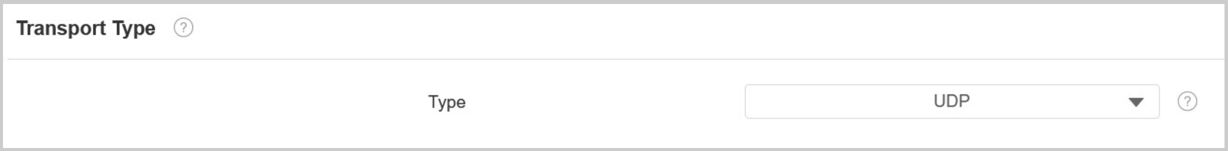
Max RTP Port 12000 (1024~65535)

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

Data Transmission Type Configuration

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

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



Transport Type

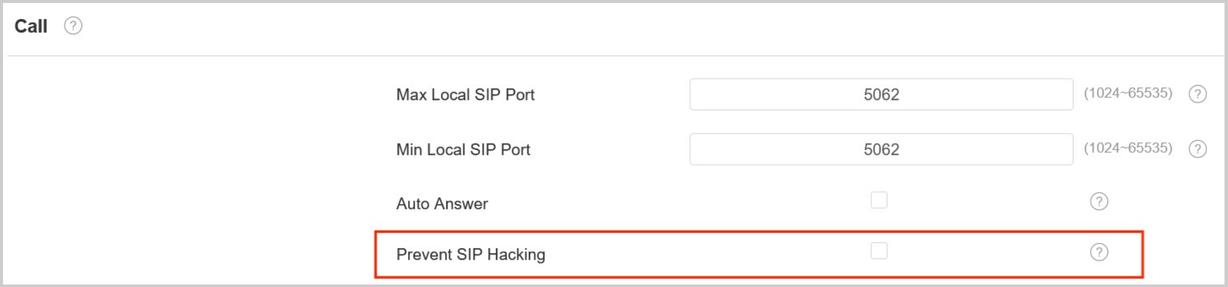
Type	UDP

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

SIP Hacking Protection

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

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



Call

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

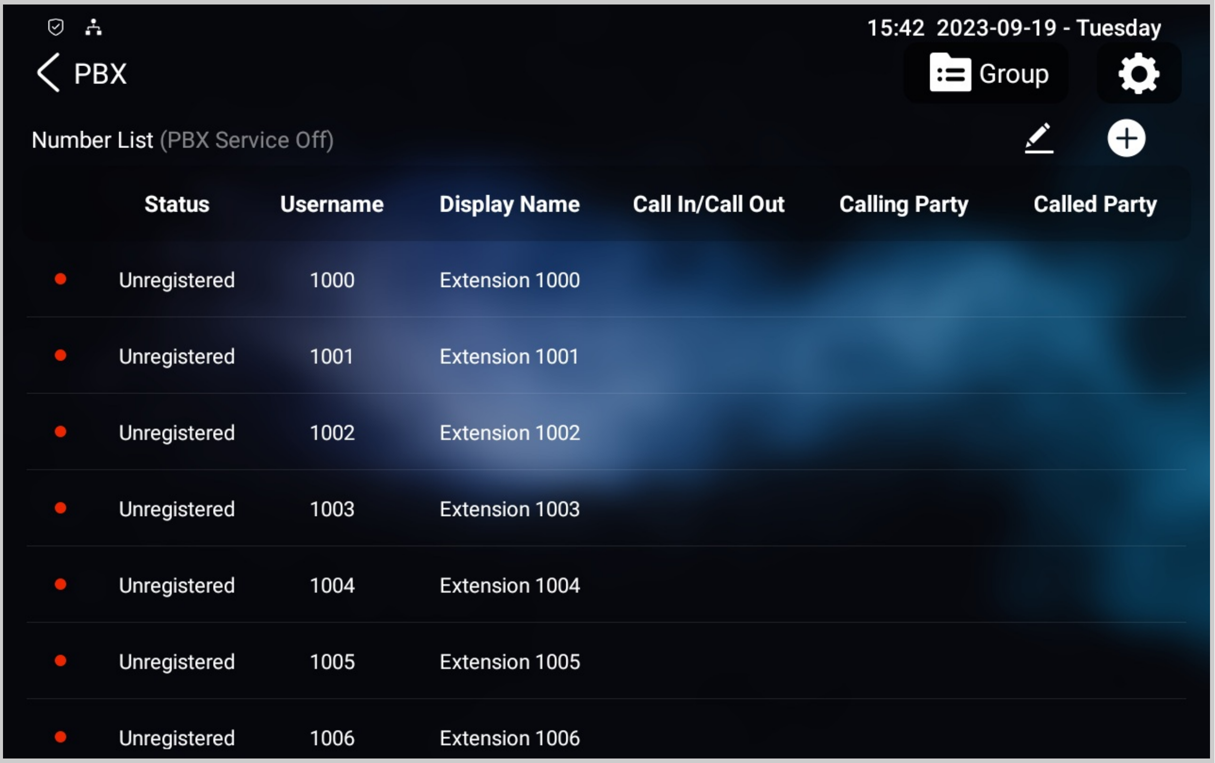
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

PBX Feature

The indoor monitor has a built-in PBX server which allows the device to serve as an intercom monitor and a SIP PBX, so users do not bother to prepare an extra SIP PBX again. The PBX supports call forward, transfer, conference, ring group features, and so on. You can set it up on the device screen or web interface.

On The Device

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

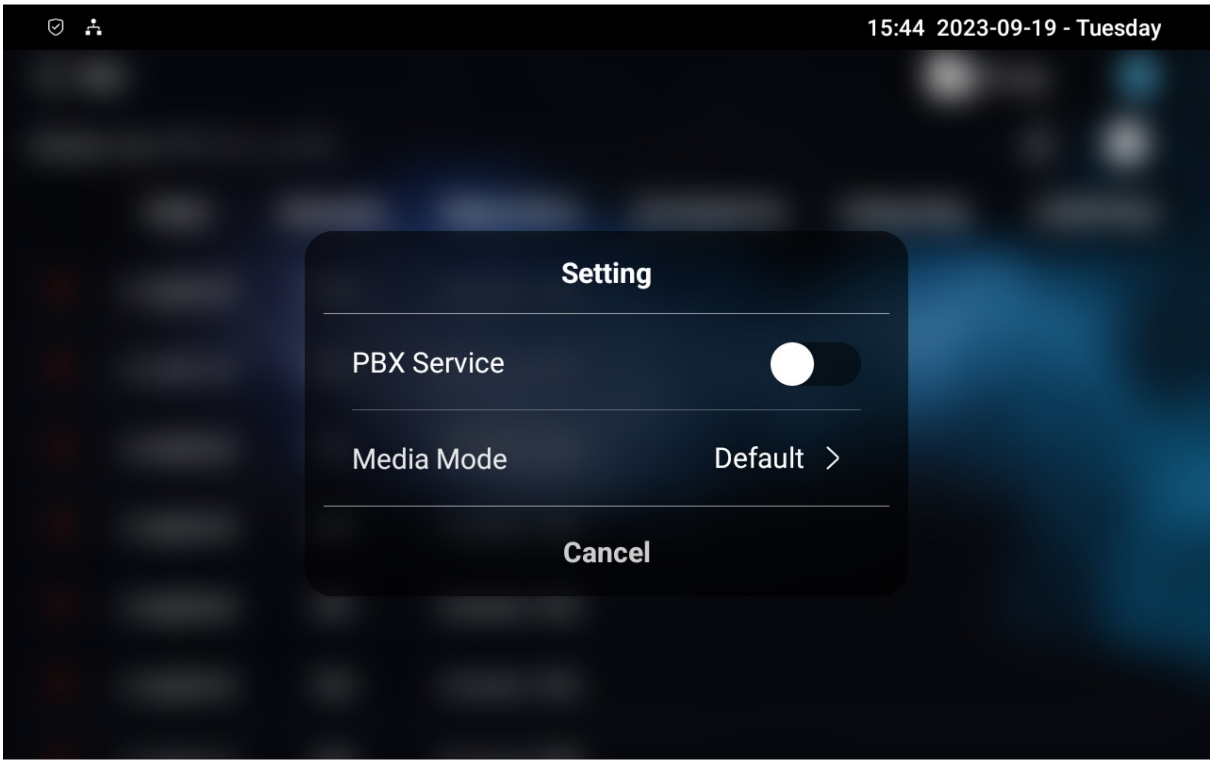


Number List (PBX Service Off)

	Status	Username	Display Name	Call In/Call Out	Calling Party	Called Party
●	Unregistered	1000	Extension 1000			
●	Unregistered	1001	Extension 1001			
●	Unregistered	1002	Extension 1002			
●	Unregistered	1003	Extension 1003			
●	Unregistered	1004	Extension 1004			
●	Unregistered	1005	Extension 1005			
●	Unregistered	1006	Extension 1006			

Enable PBX Service

On the PBX screen, tap the **Setting** icon ⚙ in the upper right corner to enable the PBX. After turning on the PBX server, you can check the server address and port in the upper left corner.



15:44 2023-09-19 - Tuesday

Setting

PBX Service

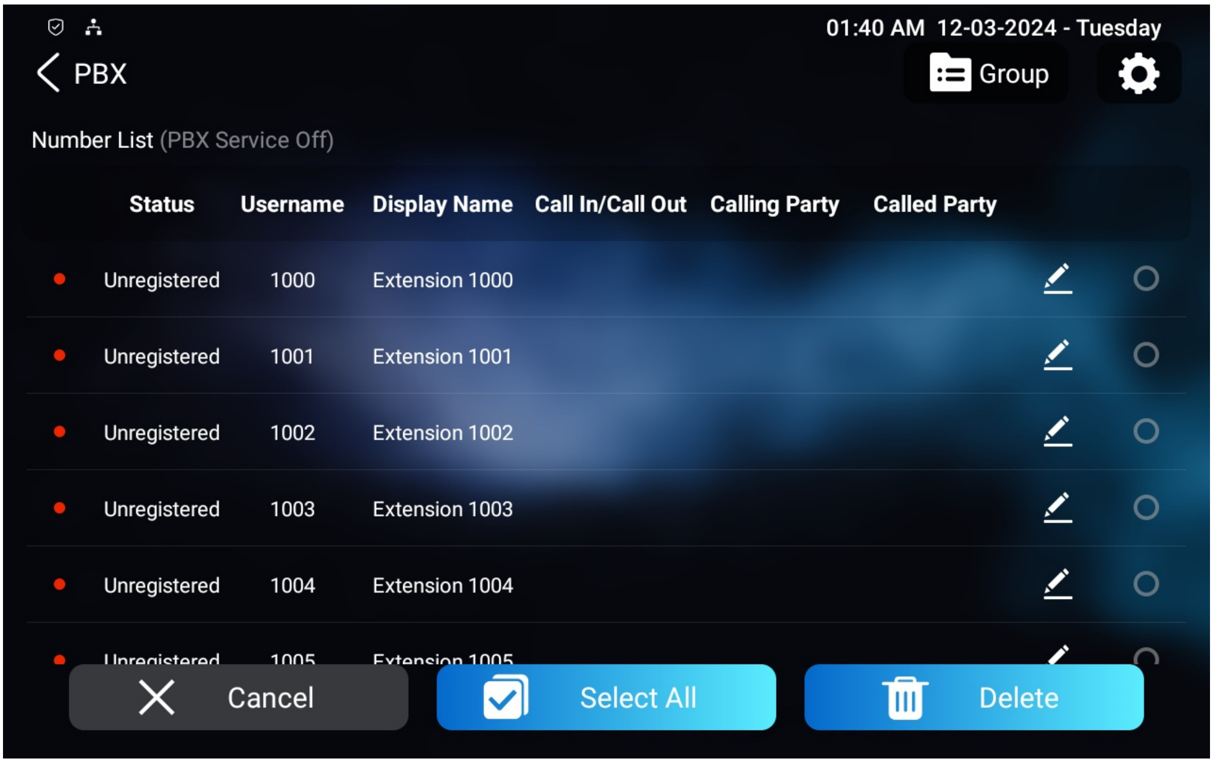
Media Mode Default >

Cancel

- **Media Mode**:
  - **Default**: Select it when the intercom devices are deployed in the same LAN network.
  - **Bypass**: Select it when the devices are deployed in different LAN networks where PBX serves as a bridge or a media for the network data transmission.

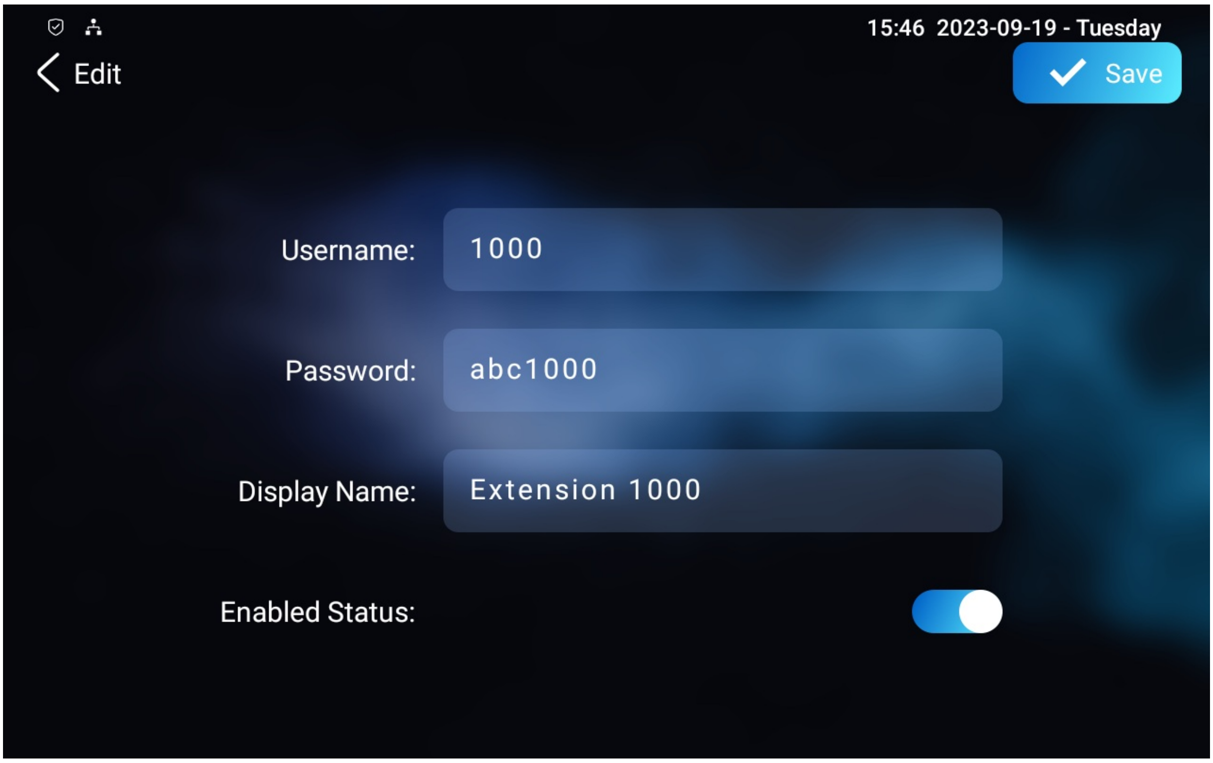
Manage PBX Accounts

You can check the basic PBX information like PBX account status by tapping ✎ in the upper right corner. Then, select the desired row by tapping ✎.



Number List (PBX Service Off)

Status	Username	Display Name	Call In/Call Out	Calling Party	Called Party
● Unregistered	1000	Extension 1000			
● Unregistered	1001	Extension 1001			
● Unregistered	1002	Extension 1002			
● Unregistered	1003	Extension 1003			
● Unregistered	1004	Extension 1004			
● Unregistered	1005	Extension 1005			



Username: 1000

Password: abc1000

Display Name: Extension 1000

Enabled Status: on

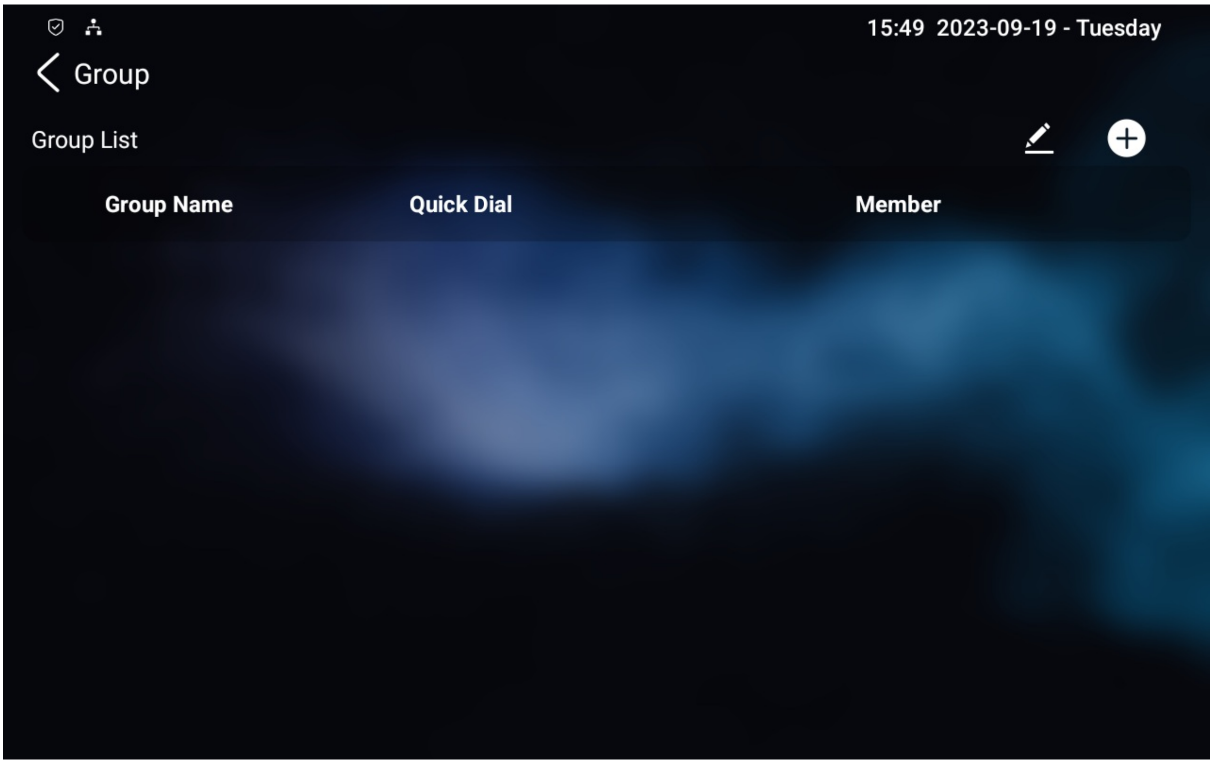
- **Status**: Indicate whether the account is registered or not.
- **Username**: Enter the extension number registered onto the SIP server.
- **Display Name**: Enter the display name of this account, which will be shown on other devices when making calls.
- **Password**: Enter the password of the corresponding users.
- **Enabled Status**: Activate or deactivate the SIP account.
- **Call In/Call Out**: The calling status of this account.
- **Calling Party**: The callee number.

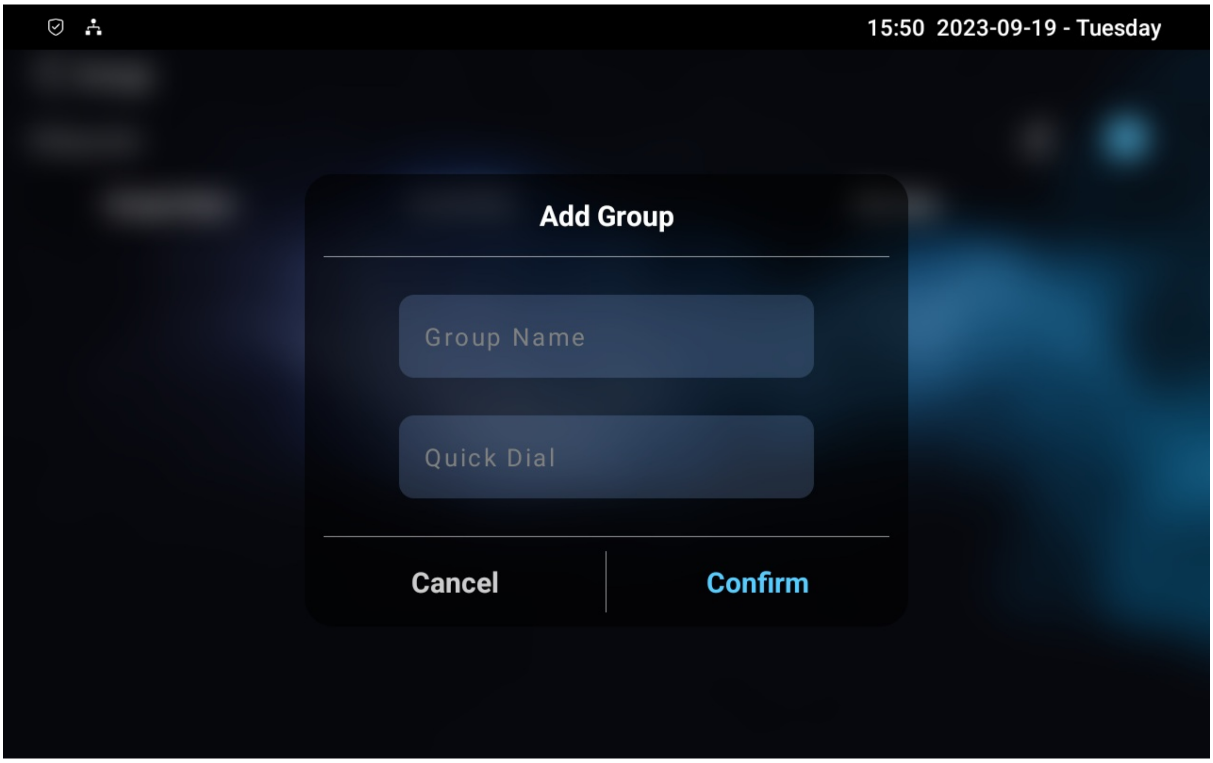
- **Caller Party**: The caller number.

Manage PBX Groups

One number can be added to different ring groups. Once receiving an incoming call, the numbers in one group will ring up at the same time.

Tap **Group** in the upper right corner to add a new ring group or edit the existing group.



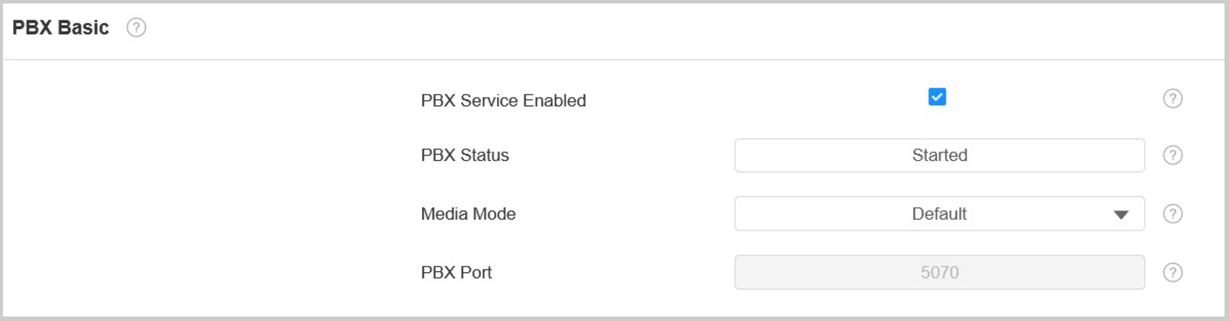


- **Group Name**: Name the group.
- **Quick Dial**: Enter the number used to call members of the group.
- **Member**: Select the registered number from the number list by pressing the area below **Member**.

On the Web Interface

Enable PBX Service

To set up the PBX feature on the web, go to the **PBX > Basic** interface.



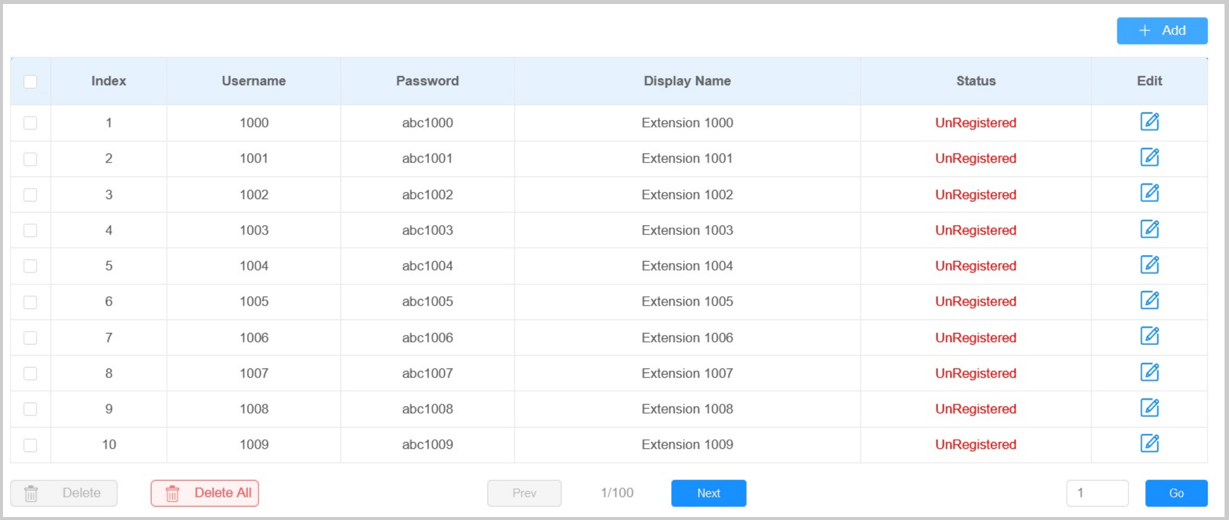
PBX Basic

PBX Service Enabled	☑
PBX Status	Started
Media Mode	Default
PBX Port	5070

- **PBX Status**: Indicate whether the PBX is on or off.
- **Media Mode**:
  - **Default**: Select it when the intercom devices are deployed in the same LAN network.
  - **Bypass**: Select it when the devices are deployed in different LAN networks where PBX serves as a bridge or a media for the network data transmission.
- **PBX Port**: Display the port of the server.

Manage PBX Accounts

You can add or edit accounts on the **PBX > Basic** interface.



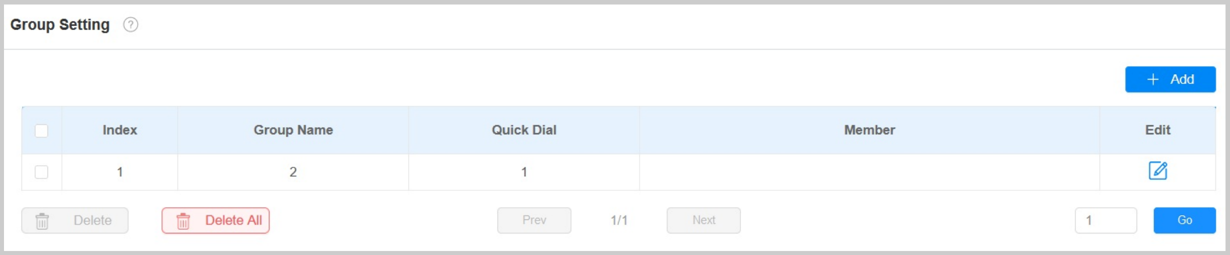
□	Index	Username	Password	Display Name	Status	Edit
□	1	1000	abc1000	Extension 1000	UnRegistered	✎
□	2	1001	abc1001	Extension 1001	UnRegistered	✎
□	3	1002	abc1002	Extension 1002	UnRegistered	✎
□	4	1003	abc1003	Extension 1003	UnRegistered	✎
□	5	1004	abc1004	Extension 1004	UnRegistered	✎
□	6	1005	abc1005	Extension 1005	UnRegistered	✎
□	7	1006	abc1006	Extension 1006	UnRegistered	✎
□	8	1007	abc1007	Extension 1007	UnRegistered	✎
□	9	1008	abc1008	Extension 1008	UnRegistered	✎
□	10	1009	abc1009	Extension 1009	UnRegistered	✎

- **Username**: Enter the extension number registered onto the SIP server.
- **Password**: Enter the password of the corresponding users.

- **Display Name**: Enter the display name of this account, which will be shown on other devices when making calls.
- **Status**: Indicate whether the account is registered or not.

Manage PBX Groups

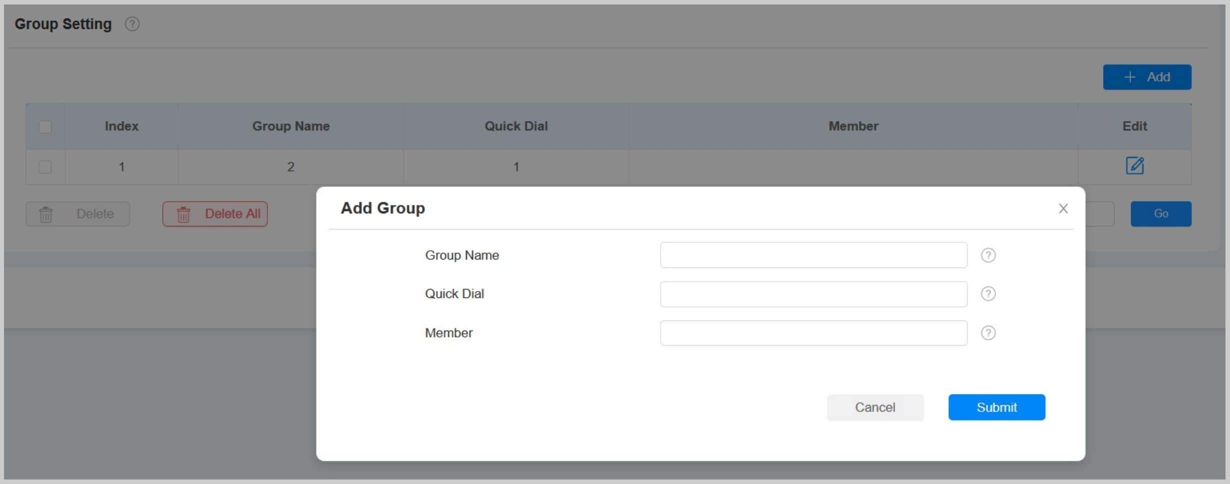
To set up PBX groups, go to the **PBX > Ring Group** interface. Click **+Add** or ✎ to create or modify a group.



Group Setting ?

＋ Add

□	Index	Group Name	Quick Dial	Member	Edit
□	1	2	1		✎



Add Group

Group Name:
Quick Dial:
Member:

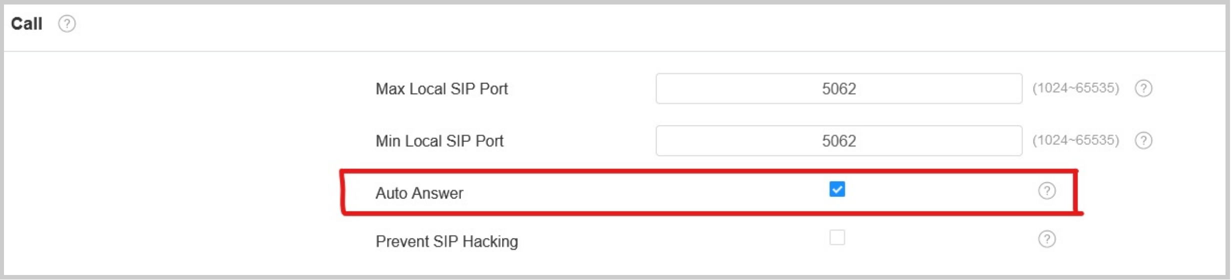
- **Group Name**: Name the group.
- **Quick Dial**: Enter the number used to call members of the group.
- **Member**: Select the registered number from the number list.

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.

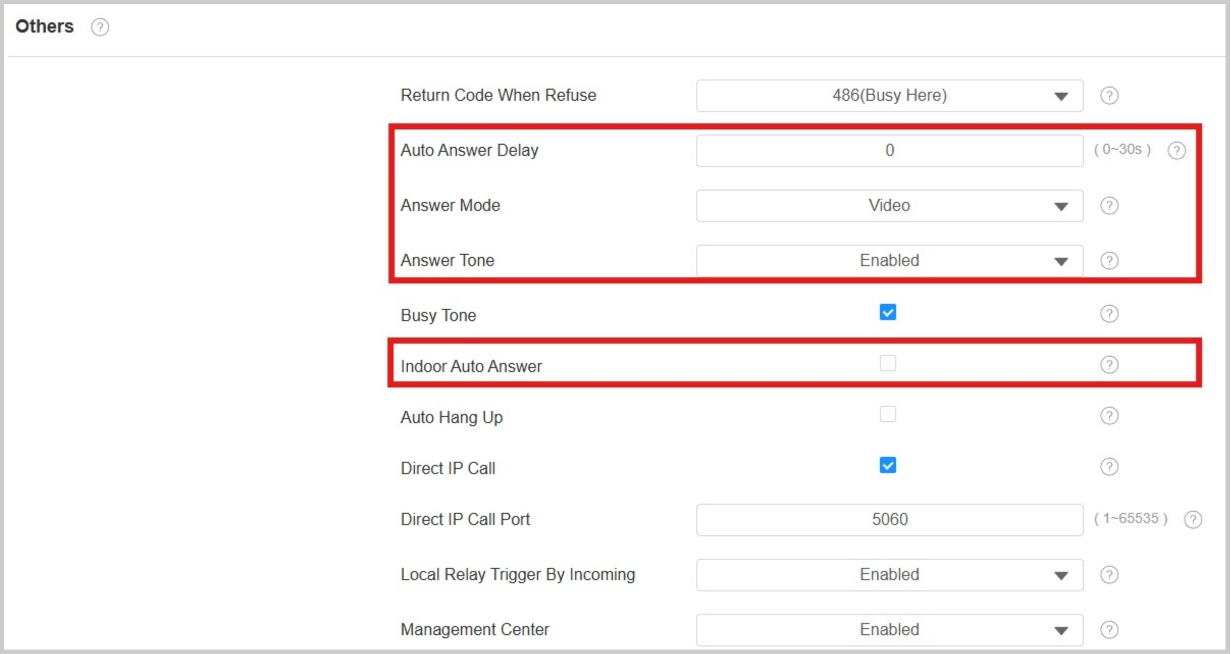
To enable the auto-answer feature for SIP calls, go to the web **Account > Advanced > Call** interface.



Call

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

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



Others

Return Code When Refuse	486(Busy Here)	
Auto Answer Delay	0	(0~30s)
Answer Mode	Video	
Answer Tone	Enabled	
Busy Tone	☑	
Indoor Auto Answer	□	
Auto Hang Up	□	
Direct IP Call	☑	
Direct IP Call Port	5060	(1~65535)
Local Relay Trigger By Incoming	Enabled	
Management Center	Enabled	

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

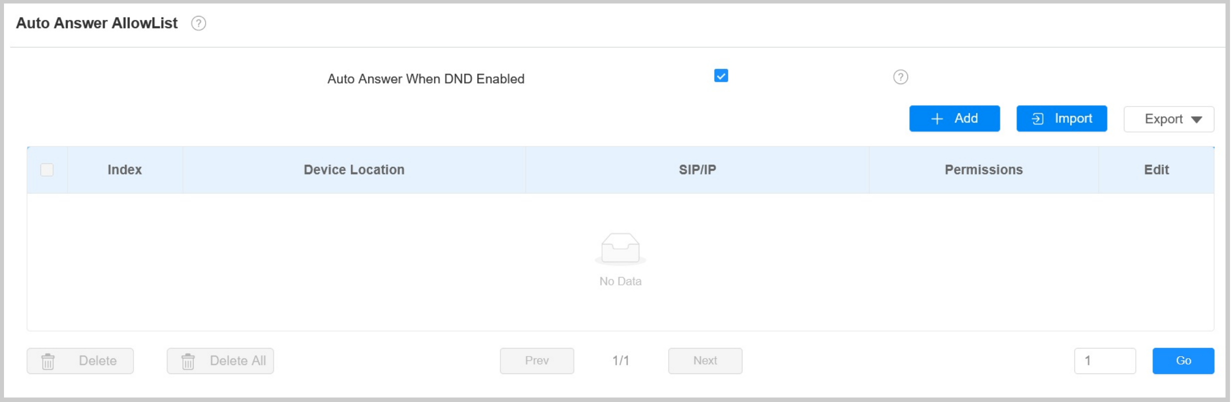
Other Options:

- **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 Allowlist Setting

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

To set it up, go to the **Security > Allowlist** interface. Click **+Add** to add the allowed device.



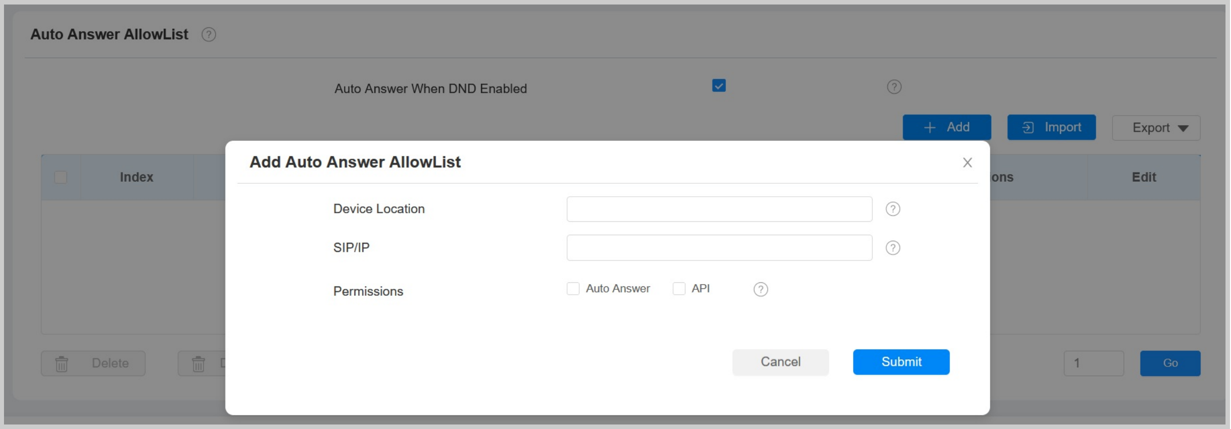
Auto Answer AllowList

Auto Answer When DND Enabled ☑

□	Index	Device Location	SIP/IP	Permissions	Edit

No Data

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



Add Auto Answer AllowList

Device Location

SIP/IP

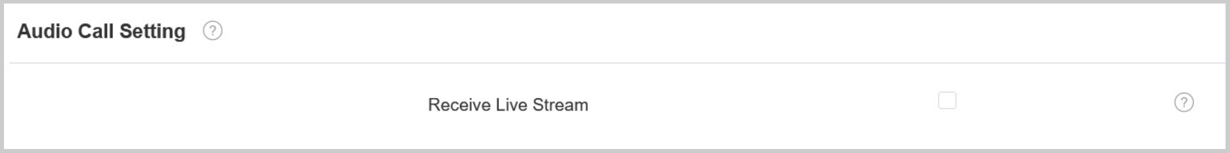
Permissions □ Auto Answer □ API

- **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.

Live Stream

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.



Audio Call Setting

Receive Live Stream □

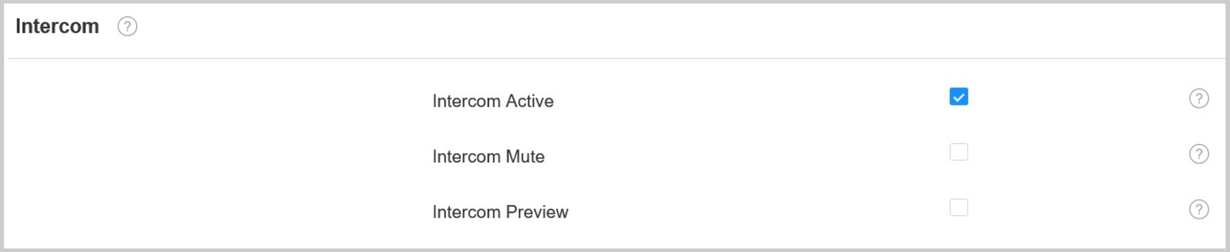
When it is enabled, calling parties cannot see users when they want to have a two-way video call with users. See the details below:

- If an incoming call is received on an audio basis on the S567, 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 S567, 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

Intercom Active ☑

Intercom Mute □

Intercom Preview □

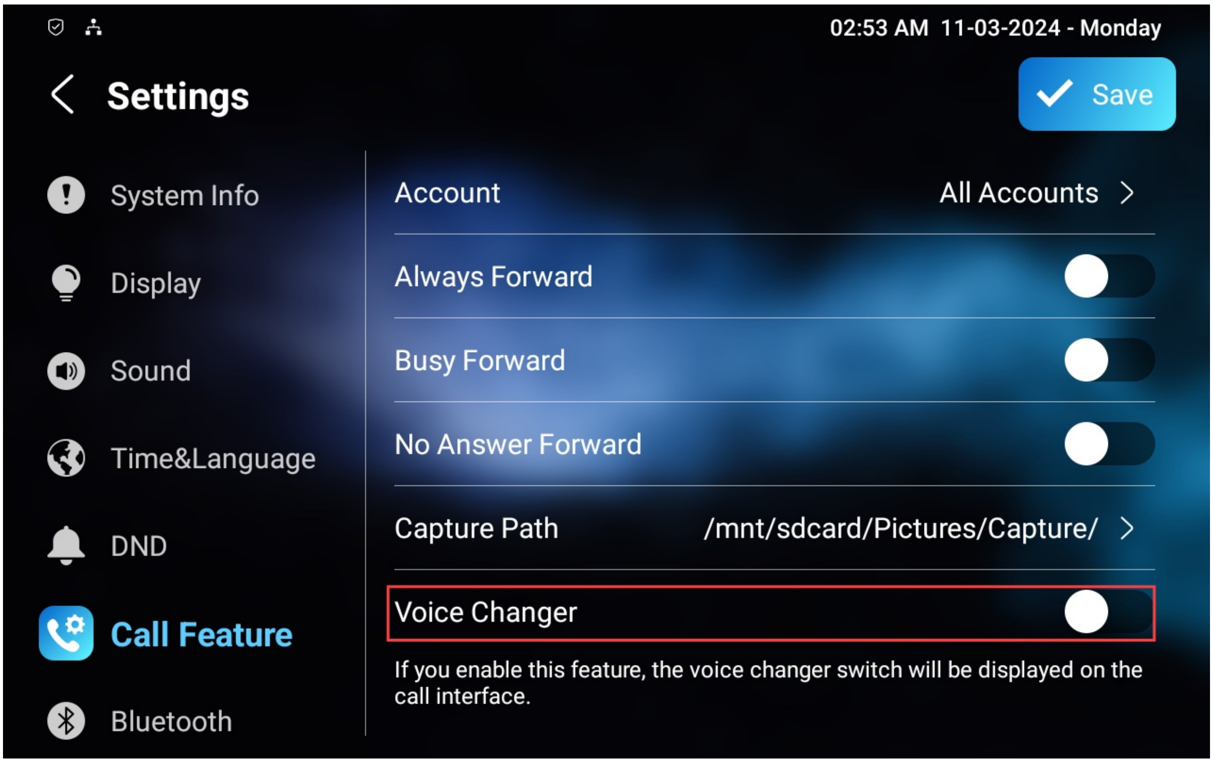
- **Intercom Active**: It is enabled by default.
- **Intercom Mute**: Available when Intercom Active is enabled. Mute the voice from the callee side.
- **Intercom Preview**: Available when Intercom Active is enabled. If it is enabled, the group call is not available.

> **Note**
>
> Enabling **Intercom Preview** option or not depends on whether the other party features RTSP.
>
> - For devices without RTSP: Enable this option. The indoor monitor will automatically answer incoming calls and display the live stream on the preview screen.
> - For devices with RTSP: Disable this option, as RTSP already provides real-time audio and video for intercom preview.

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.



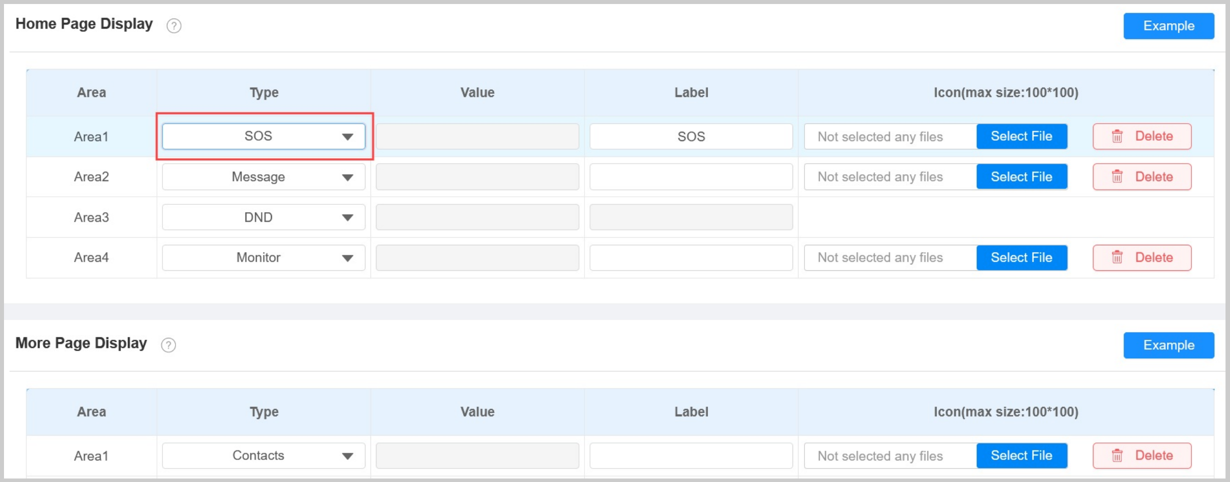
Account: All Accounts
Always Forward
Busy Forward
No Answer Forward
Capture Path: /mnt/sdcard/Pictures/Capture/
Voice Changer

If you enable this feature, the voice changer switch will be displayed on the call interface.

Emergency Call

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

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



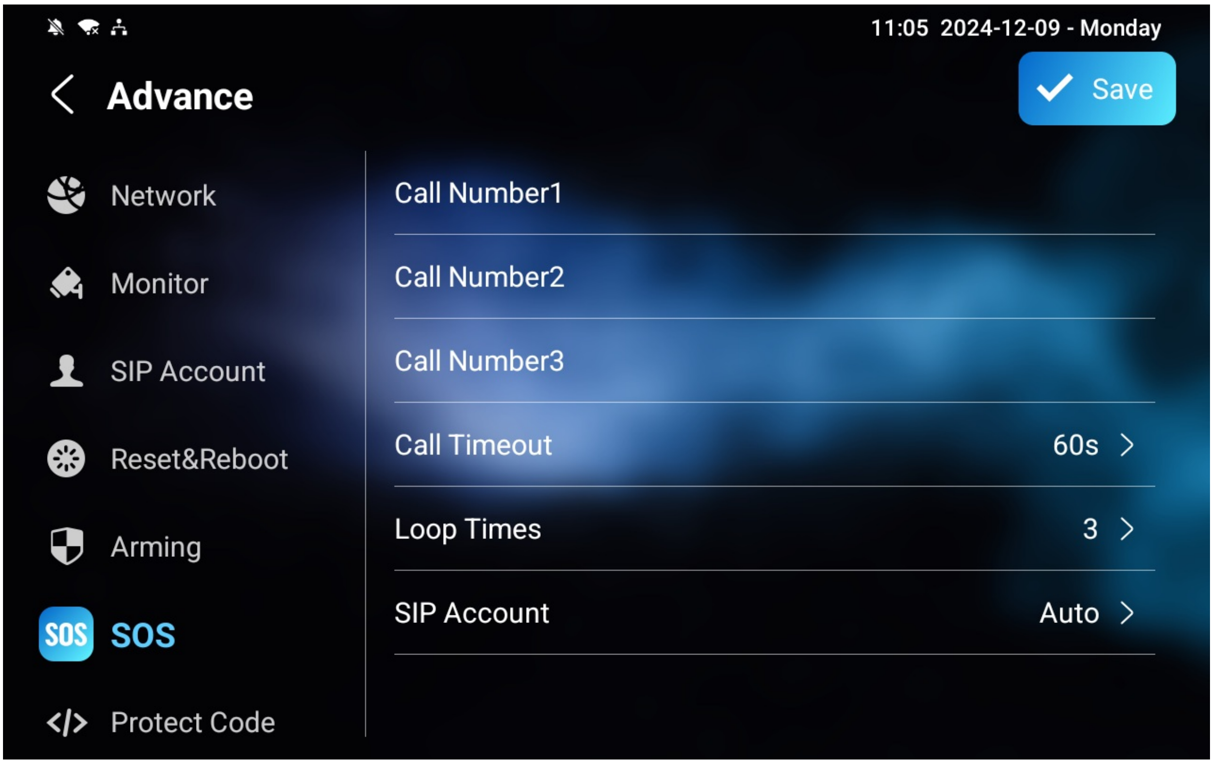
Home Page Display

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

More Page Display

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

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



Call Number1

Call Number2

Call Number3

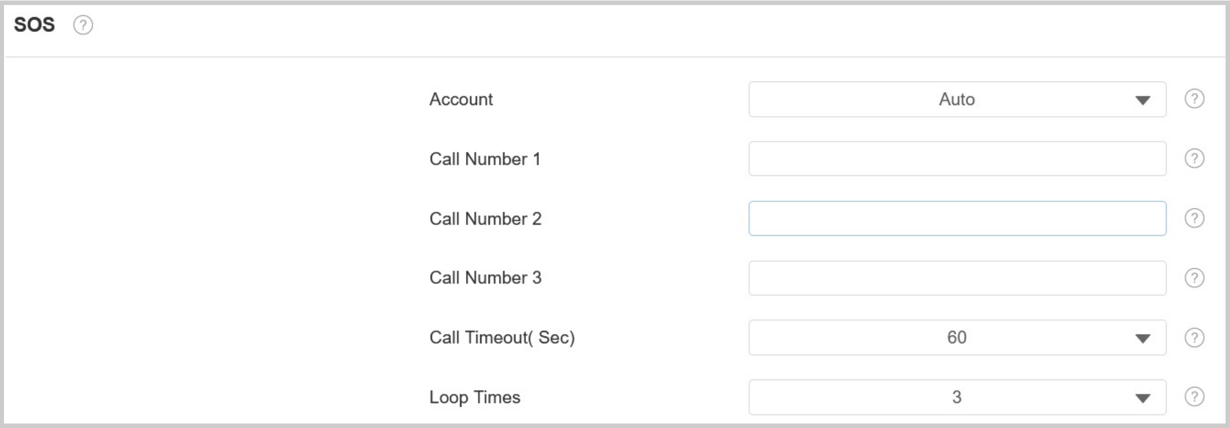
Call Timeout 60s

Loop Times 3

SIP Account Auto

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

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



SOS

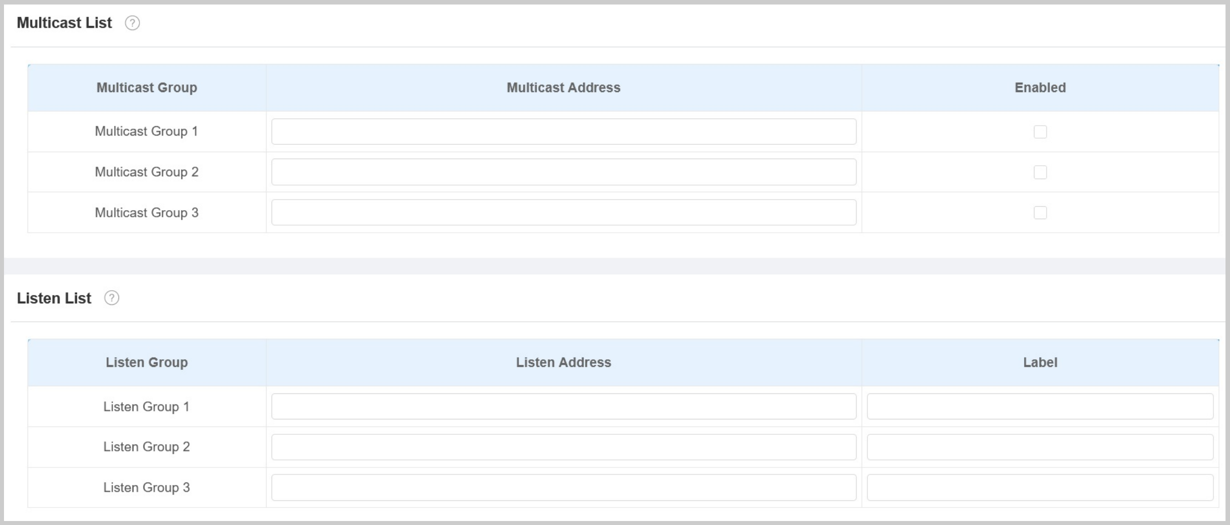
Account	Auto
Call Number 1	
Call Number 2	
Call Number 3	
Call Timeout(Sec)	60
Loop Times	3

Multicast

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

Click here to watch the demonstration video.

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



Multicast List

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

Listen List

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

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

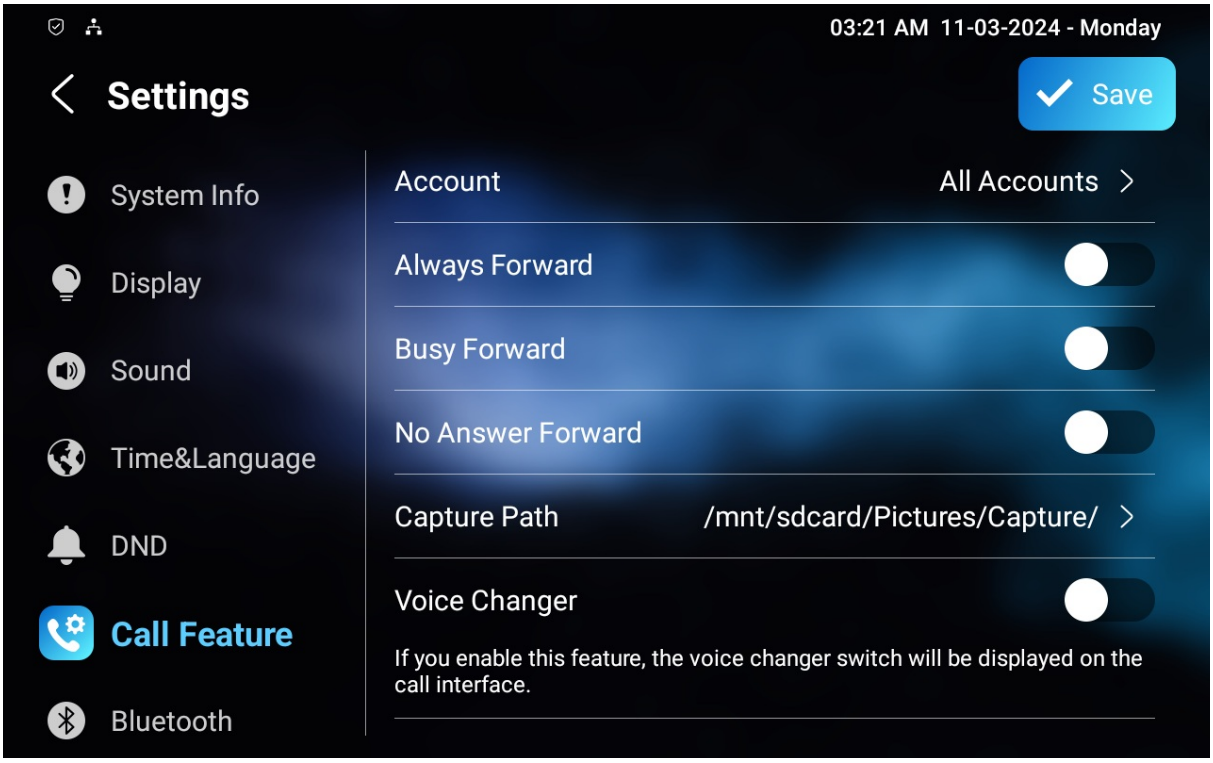
> **Note**
>
> The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult Akuvox tech team for more information.

Call Forwarding

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

On the Device

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



Account: All Accounts

Always Forward ○

Busy Forward ○

No Answer Forward ○

Capture Path: /mnt/sdcard/Pictures/Capture/

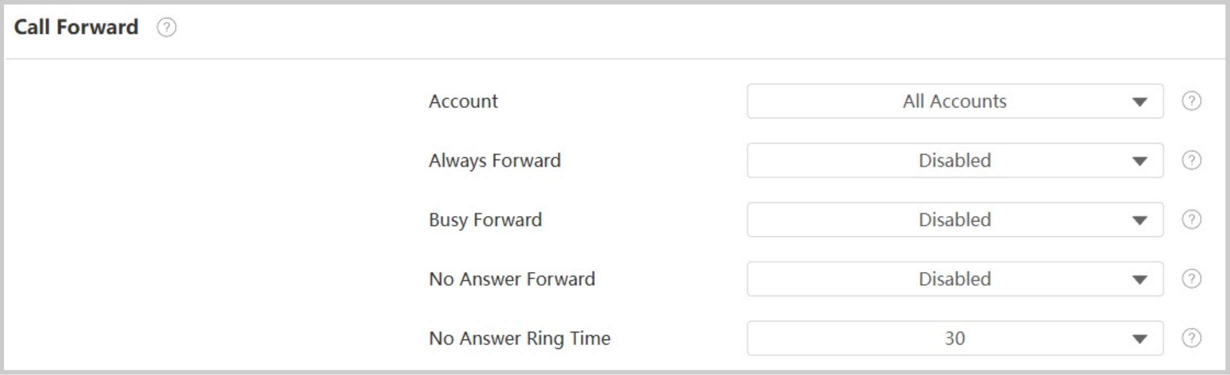
Voice Changer ○

If you enable this feature, the voice changer switch will be displayed on the call 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**: 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.
- **Capture Path**: The storage location for all the captured pictures.

On the Web Interface

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



Call Forward

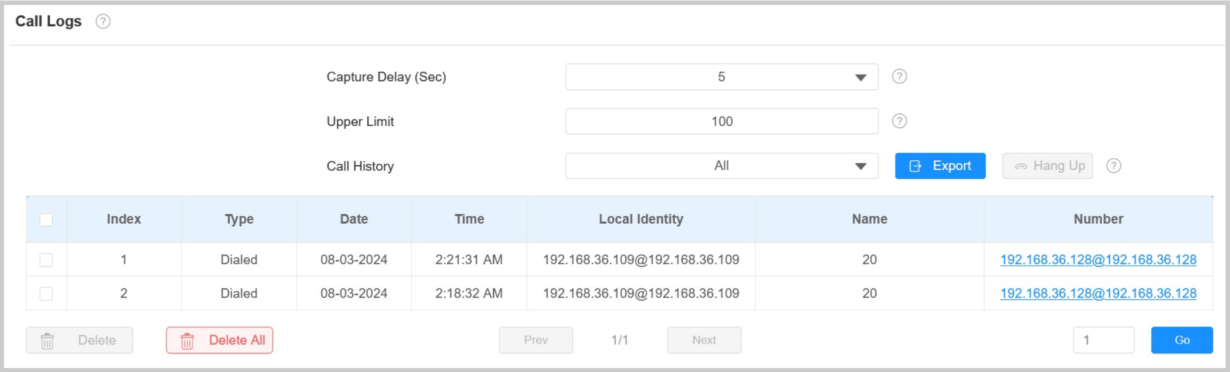
Account	All Accounts
Always Forward	Disabled
Busy Forward	Disabled
No Answer Forward	Disabled
No Answer Ring Time	30

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

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. The device supports up to 1,000 call logs.



Call Logs

Capture Delay (Sec): 5

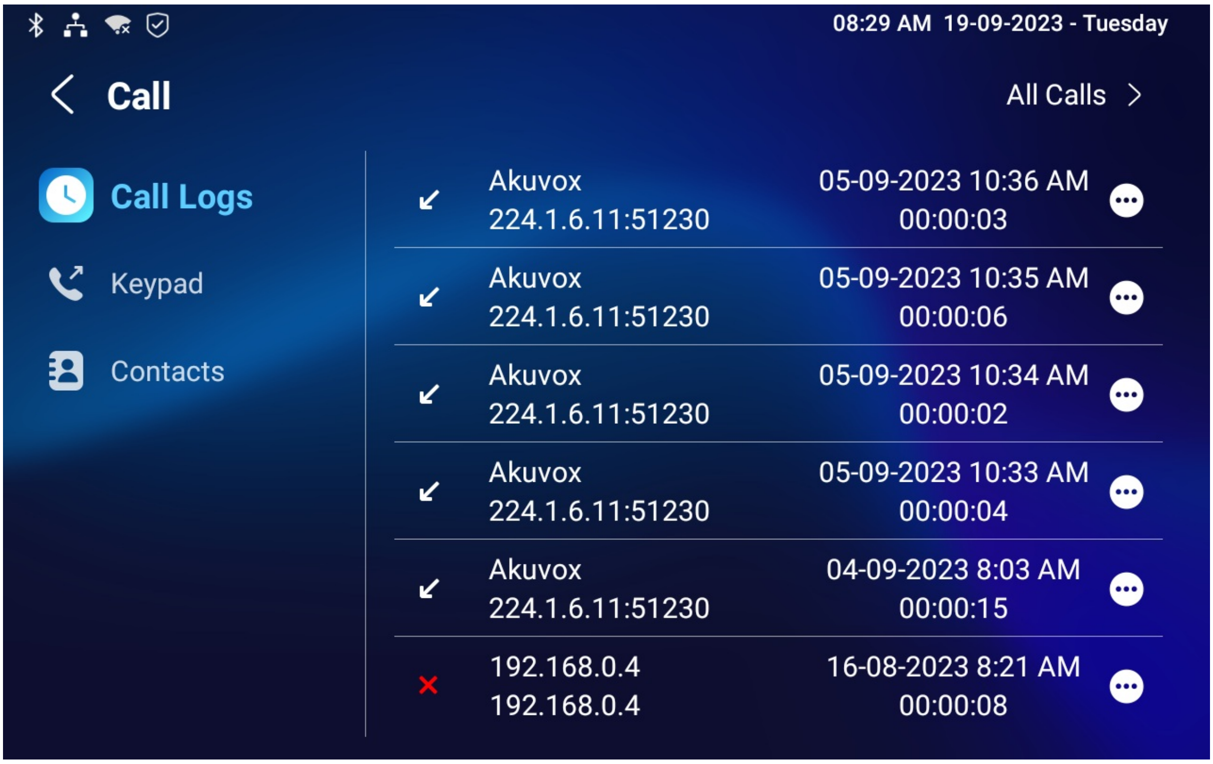
Upper Limit: 100

Call History: All

□	Index	Type	Date	Time	Local Identity	Name	Number
□	1	Dialed	08-03-2024	2:21:31 AM	192.168.36.109@192.168.36.109	20	192.168.36.128@192.168.36.128
□	2	Dialed	08-03-2024	2:18:32 AM	192.168.36.109@192.168.36.109	20	192.168.36.128@192.168.36.128

- **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**.



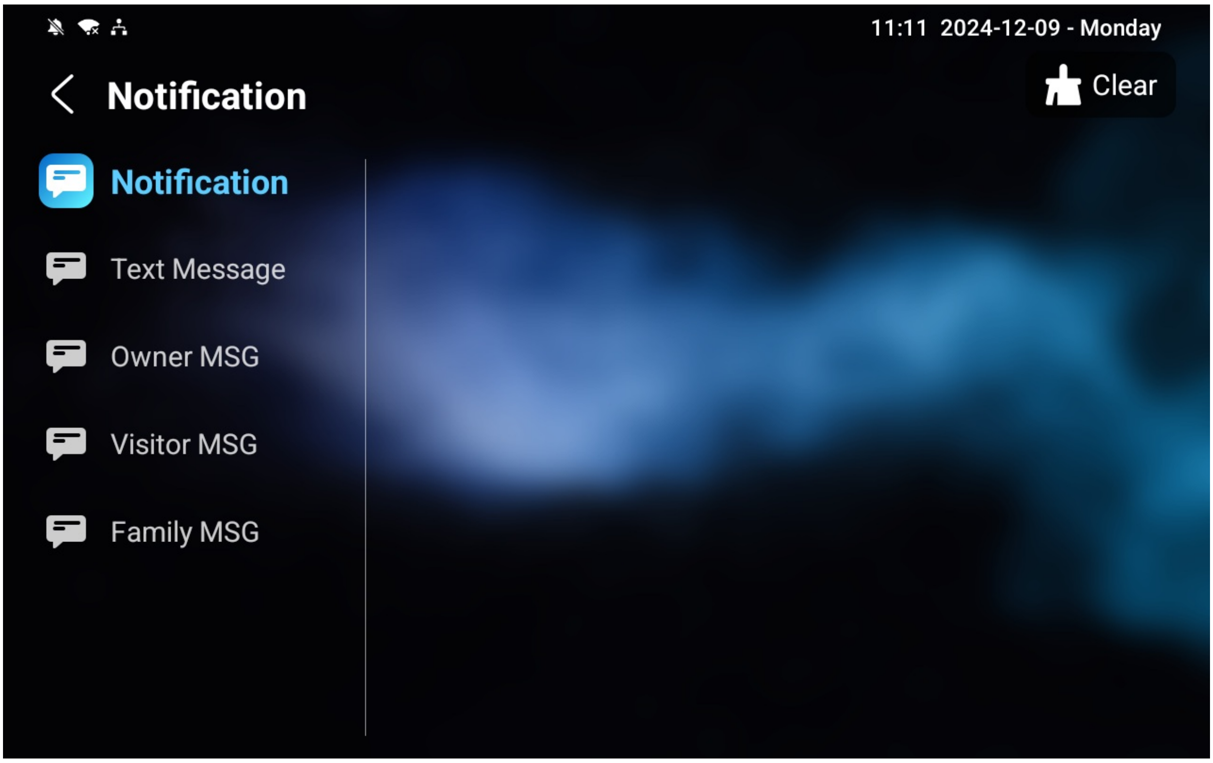
↙	Akuvox 224.1.6.11:51230	05-09-2023 10:36 AM 00:00:03
↙	Akuvox 224.1.6.11:51230	05-09-2023 10:35 AM 00:00:06
↙	Akuvox 224.1.6.11:51230	05-09-2023 10:34 AM 00:00:02
↙	Akuvox 224.1.6.11:51230	05-09-2023 10:33 AM 00:00:04
↙	Akuvox 224.1.6.11:51230	04-09-2023 8:03 AM 00:00:15
✕	192.168.0.4 192.168.0.4	16-08-2023 8:21 AM 00:00:08

Intercom Message Setting

Manage Messages

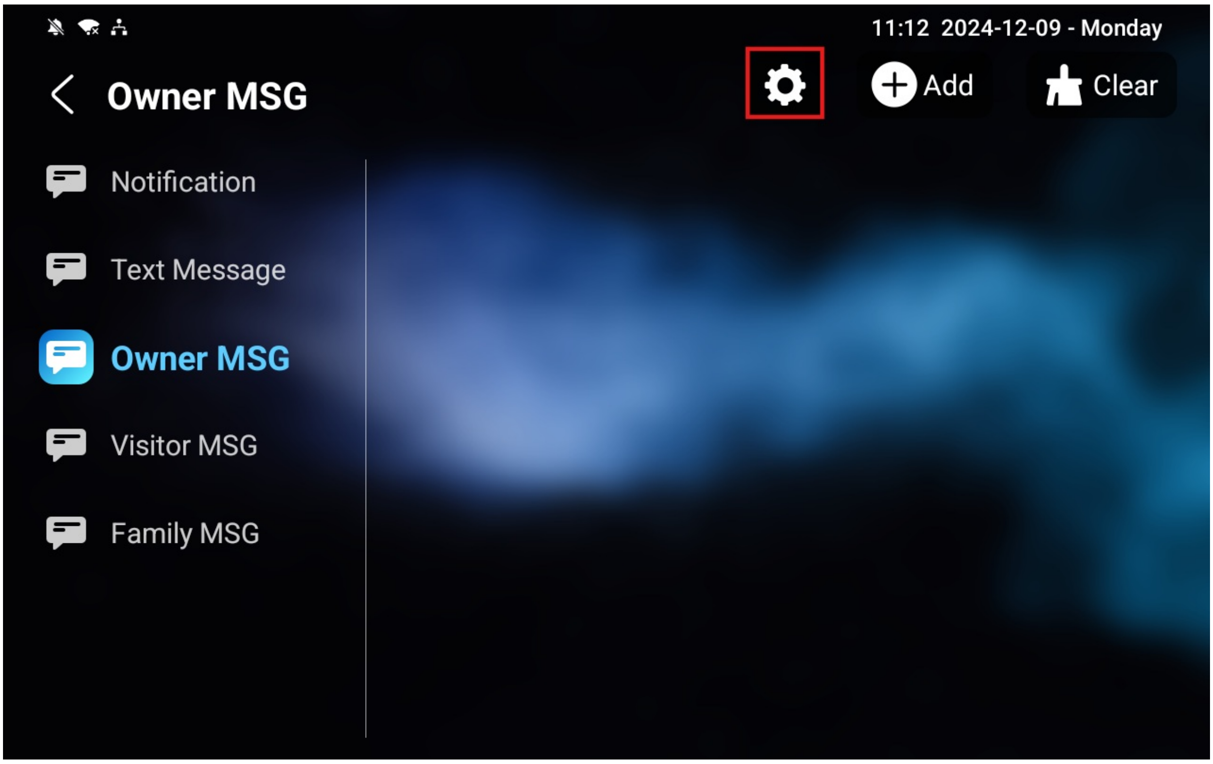
You can check, create and clear messages as needed on the device **Messages** screen.

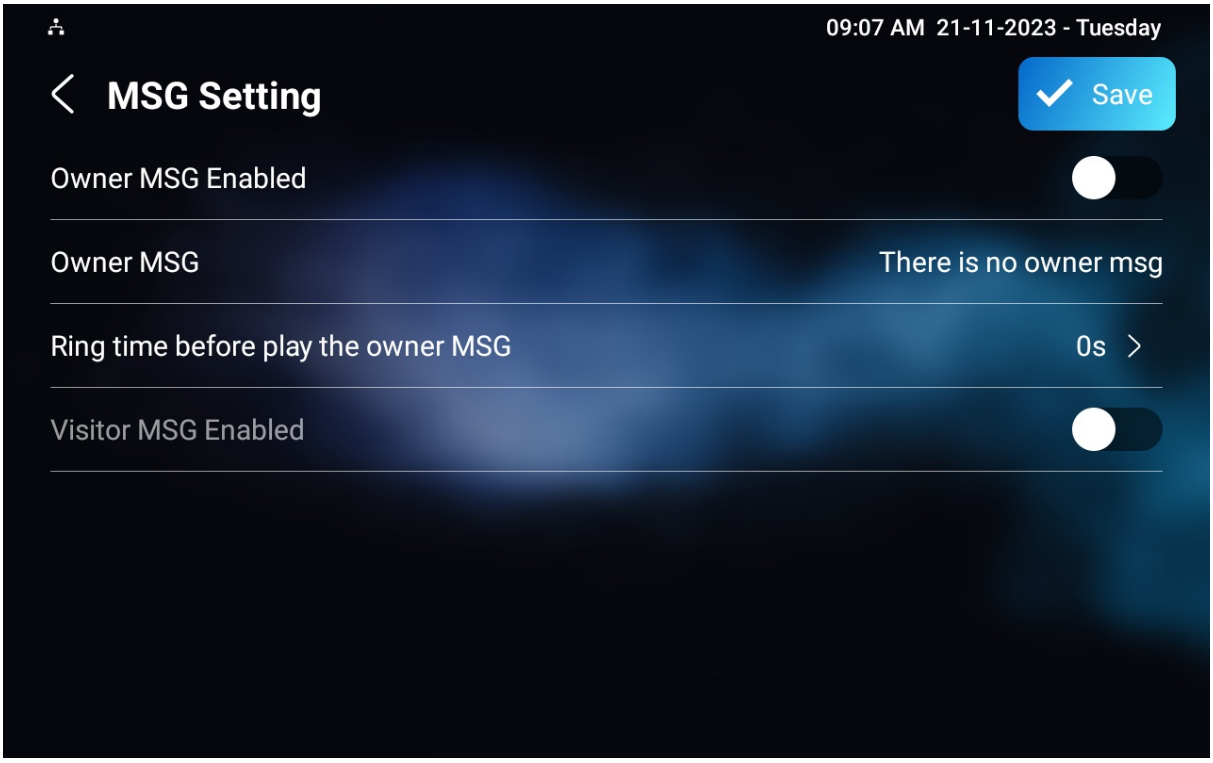
Tap **+Add** to create a message and tap **Clear** to delete messages. The device can store up to 1,000 messages.



- **Notification**: The message from the property manager. This feature is only available when using SDMC or Akuvox SmartPlus.
- **Text Message**: 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.





Owner MSG Enabled

Owner MSG: There is no owner msg

Ring time before play the owner MSG: 0s

Visitor MSG Enabled

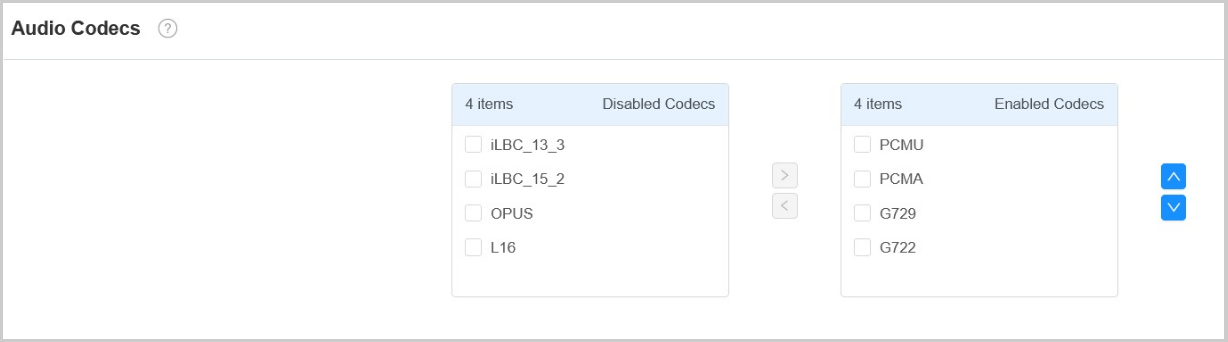
Audio & Video Codec Configuration for SIP Calls

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. Higher bandwidth means the device can capture more detail, leading to clearer sound and higher sample rates capture more data, reducing distortion and preserving sound quality.

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

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



Audio Codecs

4 items	Disabled Codecs
□ iLBC_13_3	
□ iLBC_15_2	
□ OPUS	
□ L16	

4 items	Enabled Codecs
□ PCMU	
□ PCMA	
□ G729	
□ G722	

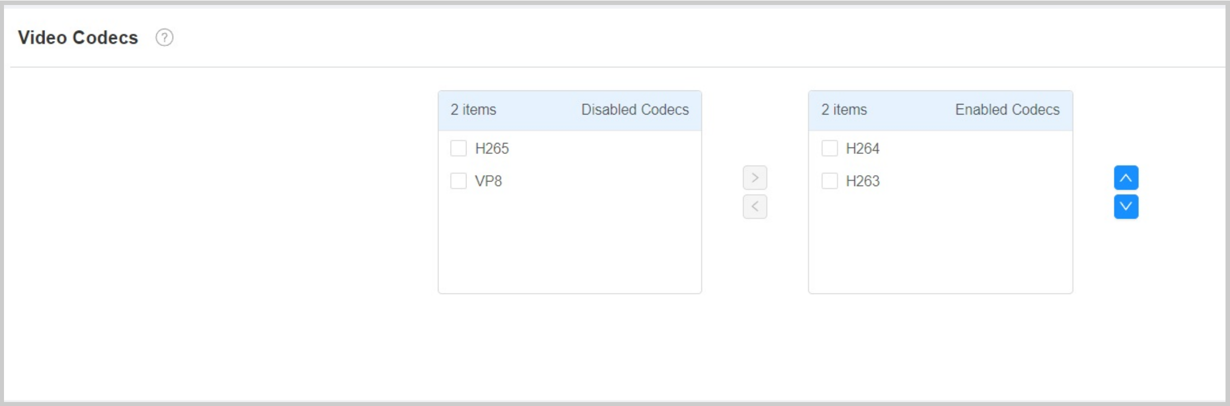
Please refer to the bandwidth consumption and sample rate for the codec types below:

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

S567 series supports VP8, H263, H264, and H265 codecs.

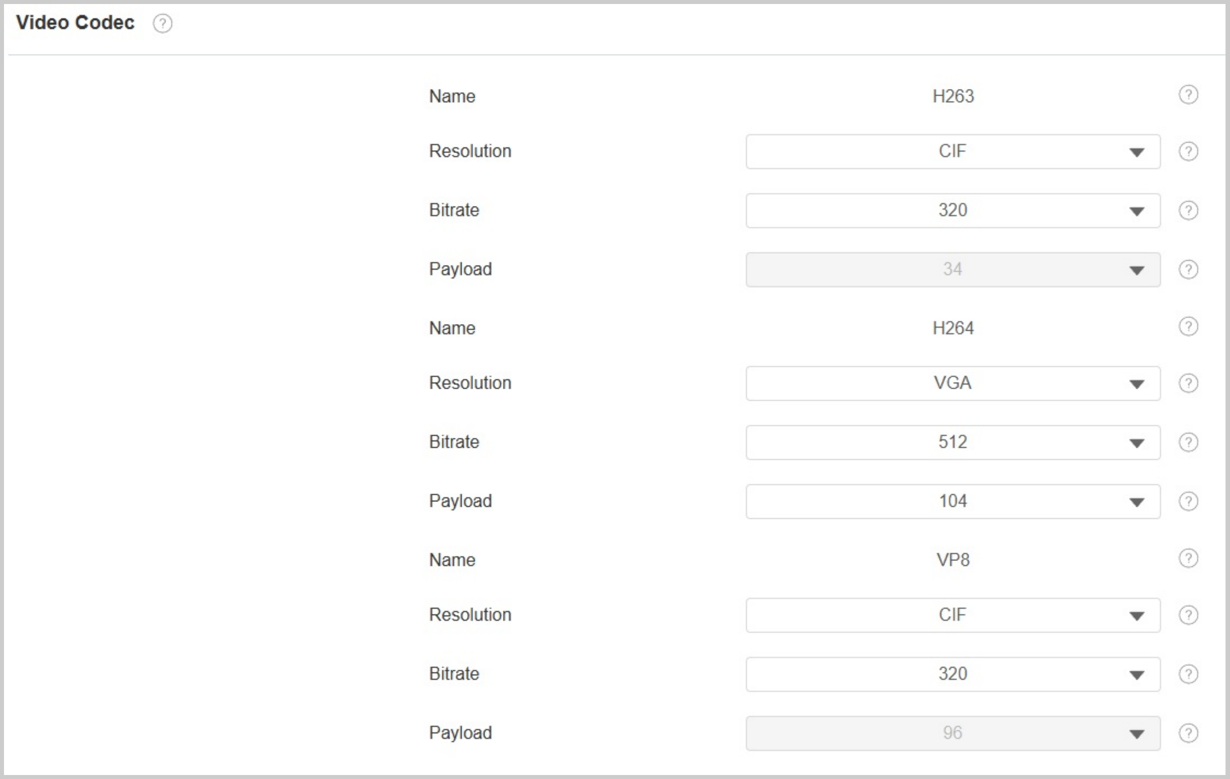
To set it up, go to the web **Account > Advanced > Video Codecs** interface. Choose an available video codec and set up the codec parameters.



Video Codecs

2 items	Disabled Codecs
□ H265	
□ VP8	

2 items	Enabled Codecs
□ H264	
□ H263	



Video Codec

Name	H263
Resolution	CIF
Bitrate	320
Payload	34
Name	H264
Resolution	VGA
Bitrate	512
Payload	104
Name	VP8
Resolution	CIF
Bitrate	320
Payload	96

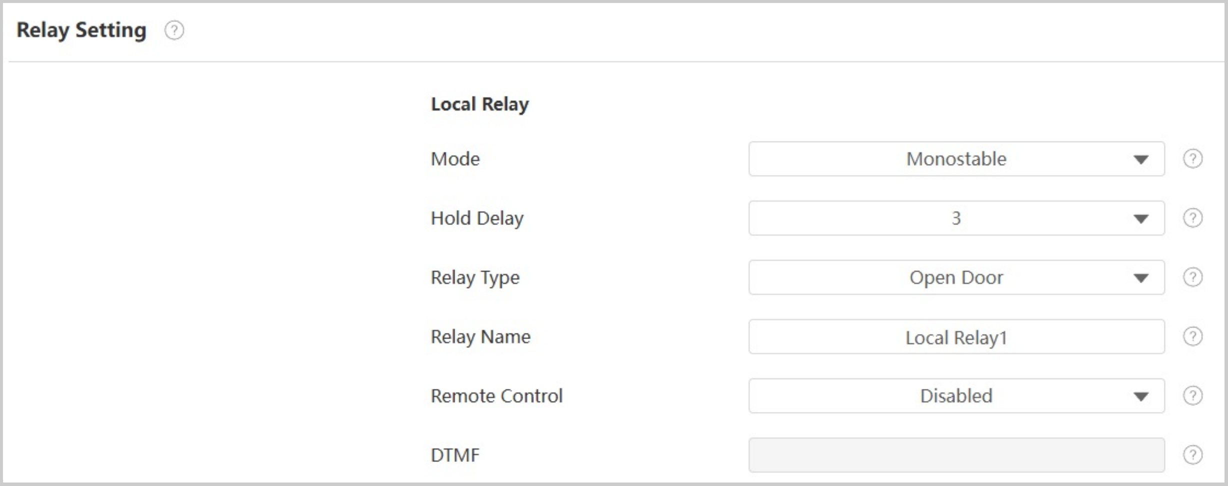
- **Resolution**: Select the resolution from the provided options. The default for H263 and VP8 is CIF(176×144 pixels) and for H264 is VGA(352×288 pixels). Select the resolution according to the network environment.
- **Bitrate**: Select the video stream bitrate. It varies by the resolution.
- **Payload**: 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.



Relay Setting

Local Relay

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

- **Mode**: Specify the conditions for automatically resetting the relay status.
    - **Monostable**: After activation, the relay status resets automatically after the Hold Delay time.
    - **Bistable**: The relay status resets upon triggering it again. This keeps the relay activated until it receives a new command, including receiving an HTTP command, DTMF code, and any event selected in the **Relay Type** drop-down menu.
- **Hold Delay(Sec)**: Available for **Monostable**. Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing. **Never** means the relay keeps activated.
- **Relay Type**:
    - **Open Door**: The relay is triggered when users open the door such as by pressing the Unlock key and remotely opening via an HTTP command. In this case, the relay trigger time is not limited to the **Hold Delay**.

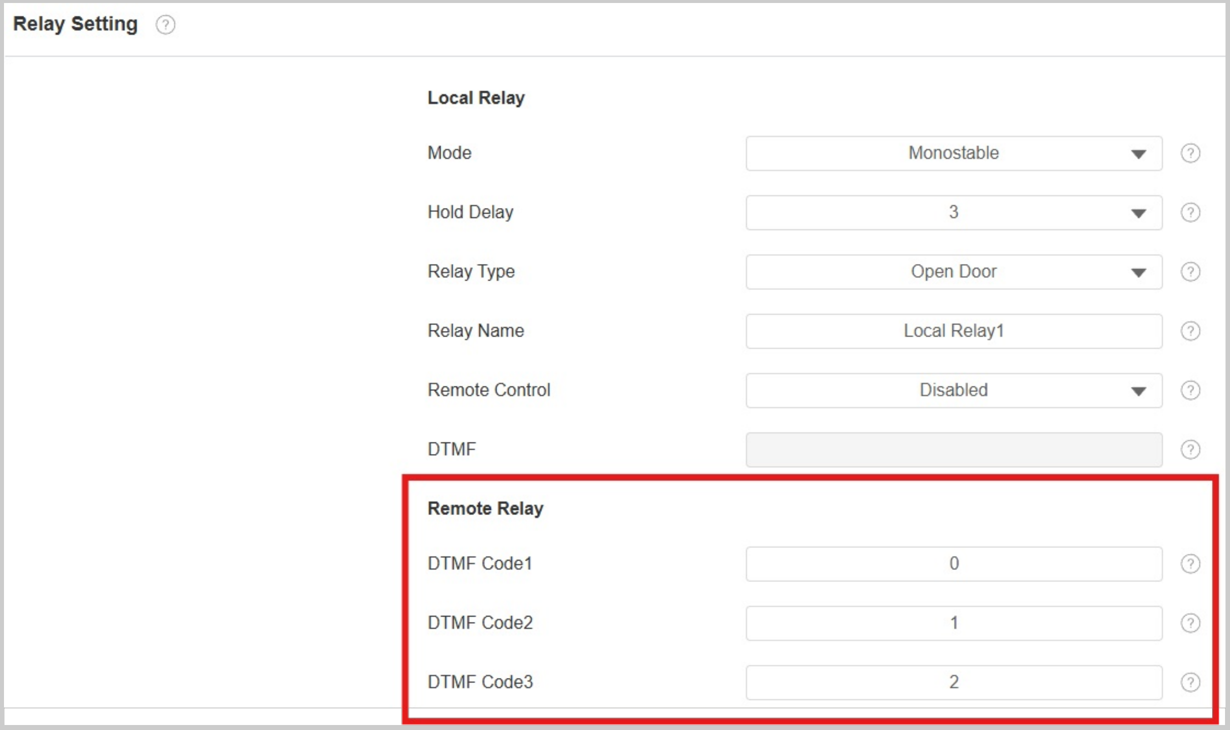
> **Tip**
>
> The relay can be connected to an alarm sensor and triggered alongside it. In this case, **Hold Delay** takes effect.
>
> - If the alarm is cleared before the Hold Delay, the relay resets immediately.
> - If the alarm is cleared after the Hold Delay, the relay resets based on the Hold Delay time.
> - If Hold Delay is set to "Never", the relay resets instantly the alarm is cleared.

   - **Chime Bell**: The relay is triggered when the indoor monitor receives calls and the doorbell rings.
     - When the call is picked up, rejected, or hung up, the relay resets.
     - The relay trigger time is not limited to Hold Delay when the doorbell rings. It follows the settings on the Doorbell screen.
   - **Other Switches(Reset By Event)**: The relay resets 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

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

Set up 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.



Relay Setting

Local Relay

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

Remote Relay

DTMF Code1	0
DTMF Code2	1
DTMF Code3	2

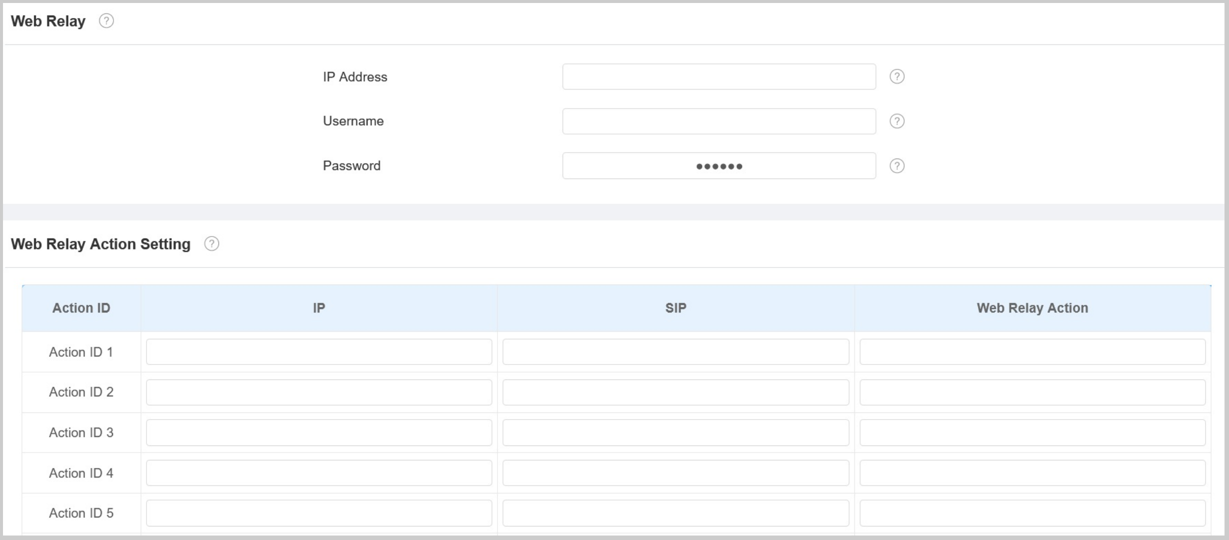
- **DTMF Code**: Define the DTMF code within the range(0-9 and *,#) for the remote relay.

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.



Web Relay

IP Address	
Username	
Password	••••••

Web Relay Action Setting

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

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

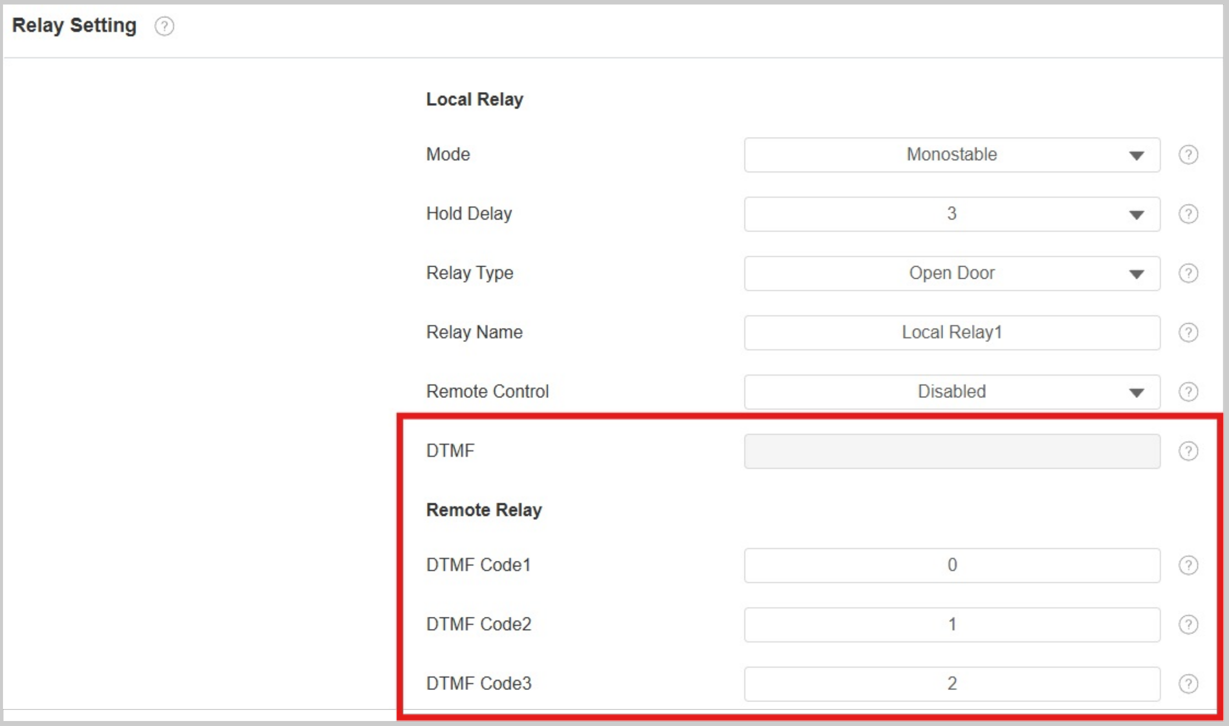
> **Note**
>
> If the URL includes full HTTP content(e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., "state.xml?relayState=2"), the relay uses the entered IP address.

Door-opening Configuration

Unlock by DTMF Code

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

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



Relay Setting

Local Relay

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

Remote Relay

DTMF Code1	0
DTMF Code2	1
DTMF Code3	2

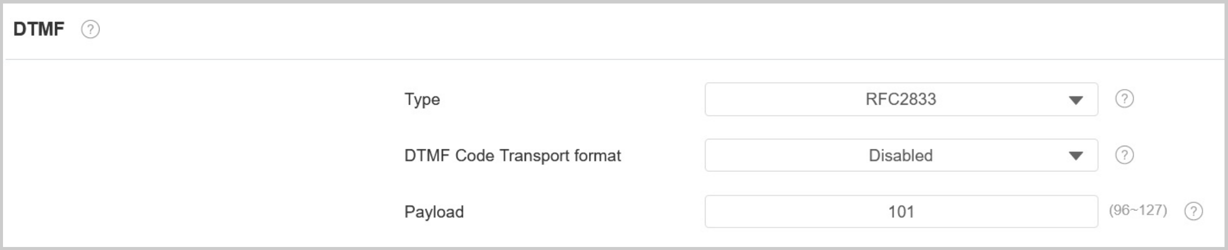
DTMF Transport Type

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

DTMF Type Differences:

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

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


DTMF

Type: RFC2833

DTMF Code Transport format: Disabled

Payload: 101 (96~127)

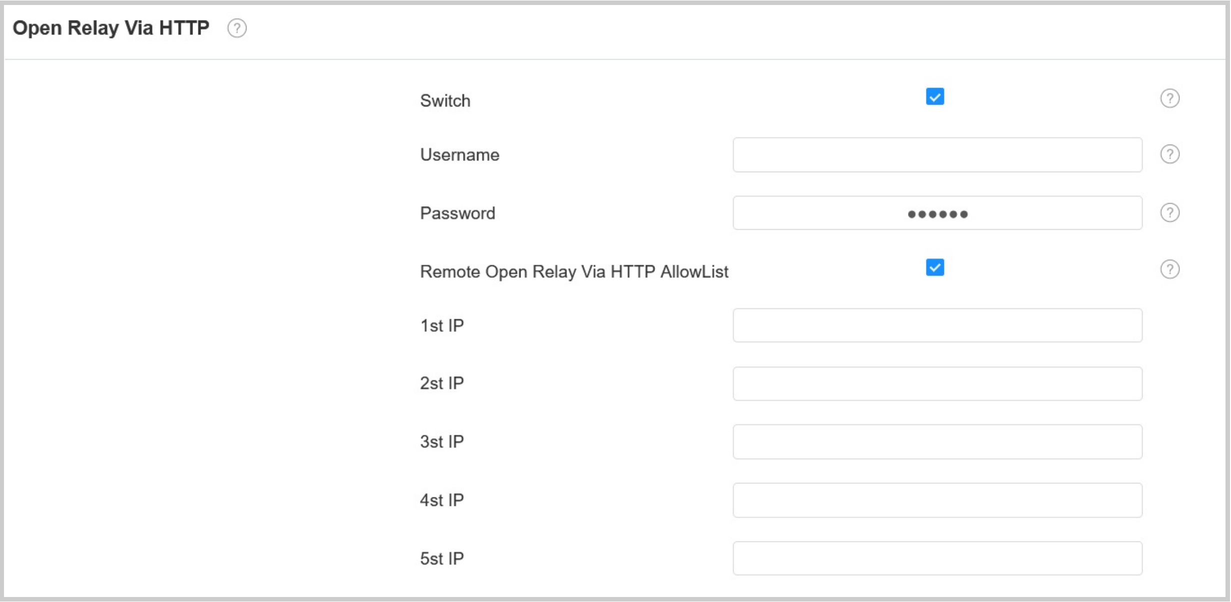
- **Type**: Select from the provided options.
- **DTMF Code Transport Format**: There are four options, Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via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

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

Unlock via HTTP Command

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

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



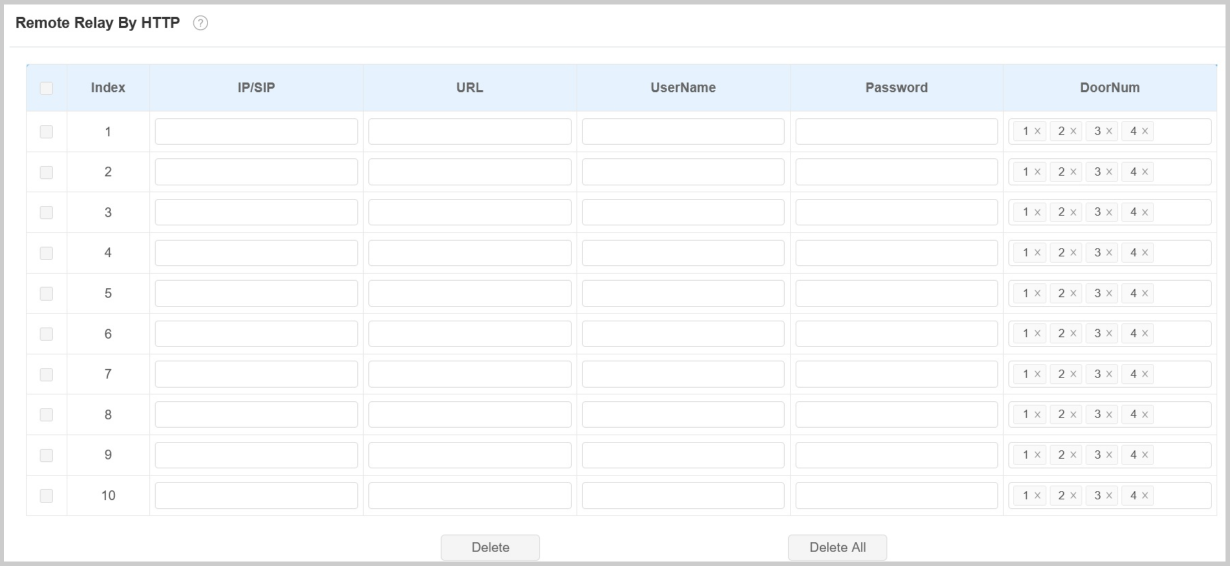
Open Relay Via HTTP

Switch	☑
Username	
Password	••••••
Remote Open Relay Via HTTP AllowList	☑
1st IP	
2st IP	
3st IP	
4st IP	
5st IP	

- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a 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.



Remote Relay By HTTP

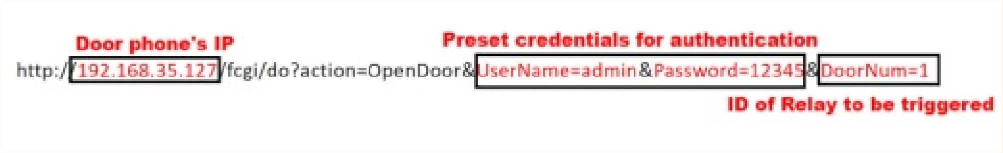
□	Index	IP/SIP	URL	UserName	Password	DoorNum
□	1					1 × 2 × 3 × 4 ×
□	2					1 × 2 × 3 × 4 ×
□	3					1 × 2 × 3 × 4 ×
□	4					1 × 2 × 3 × 4 ×
□	5					1 × 2 × 3 × 4 ×
□	6					1 × 2 × 3 × 4 ×
□	7					1 × 2 × 3 × 4 ×
□	8					1 × 2 × 3 × 4 ×
□	9					1 × 2 × 3 × 4 ×
□	10					1 × 2 × 3 × 4 ×

- **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.



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

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

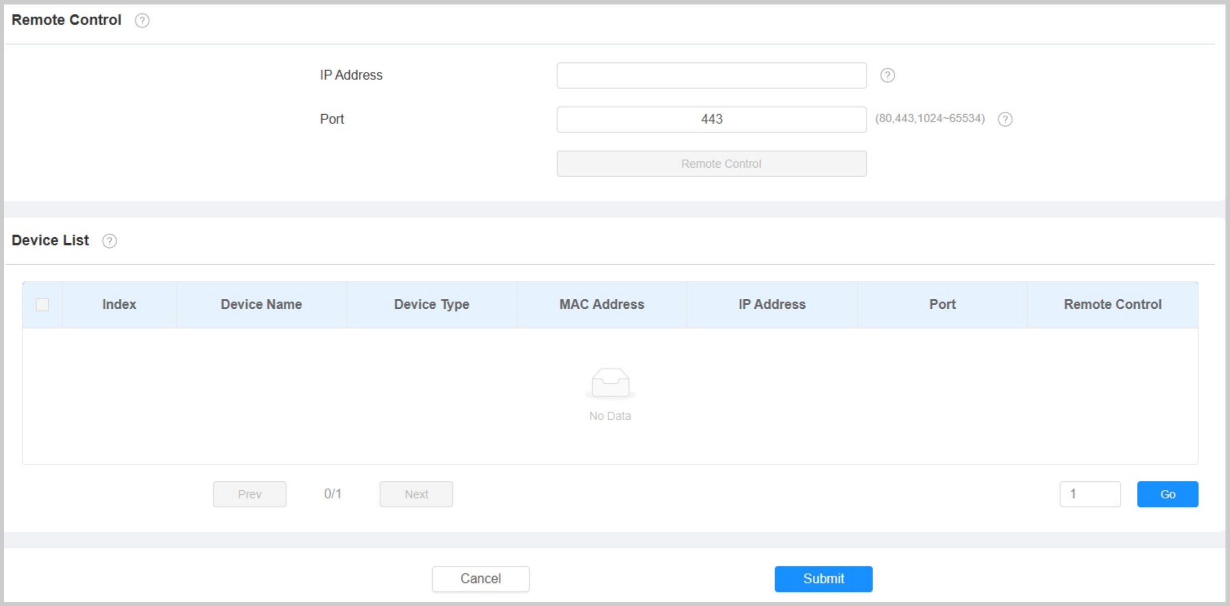
Note

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

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.



Remote Control

IP Address:

Port: 443 (80,443,1024~65534)

Device List

□	Index	Device Name	Device Type	MAC Address	IP Address	Port	Remote Control

No Data

- **IP Address**: The IP address of the device to be accessed remotely.
- **Port**: The port of the device to be accessed remotely.
- **Remote Control**: Click to redirect to the device’s web interface.

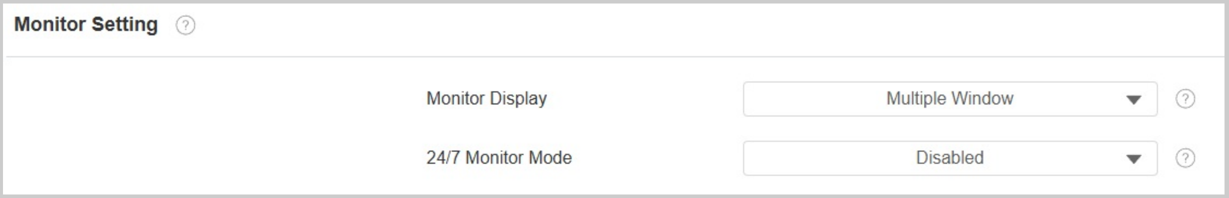
Security

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.

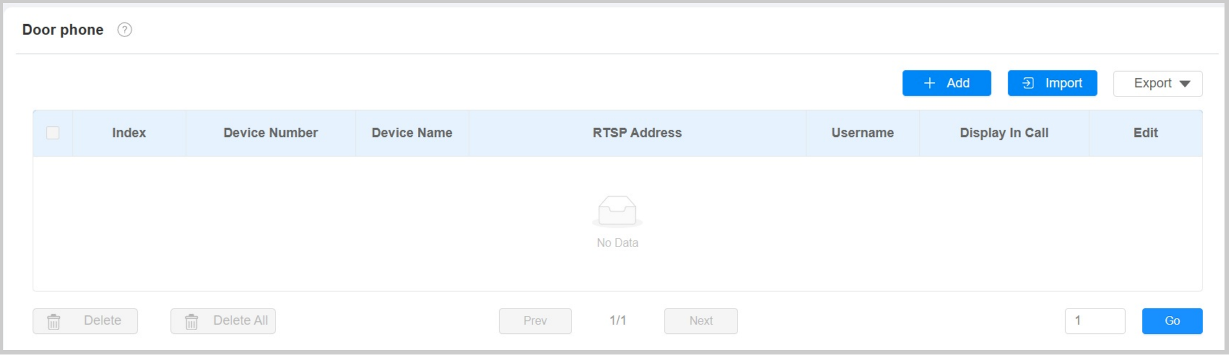


Monitor Setting

Monitor Display	Multiple Window
24/7 Monitor Mode	Disabled

- **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.

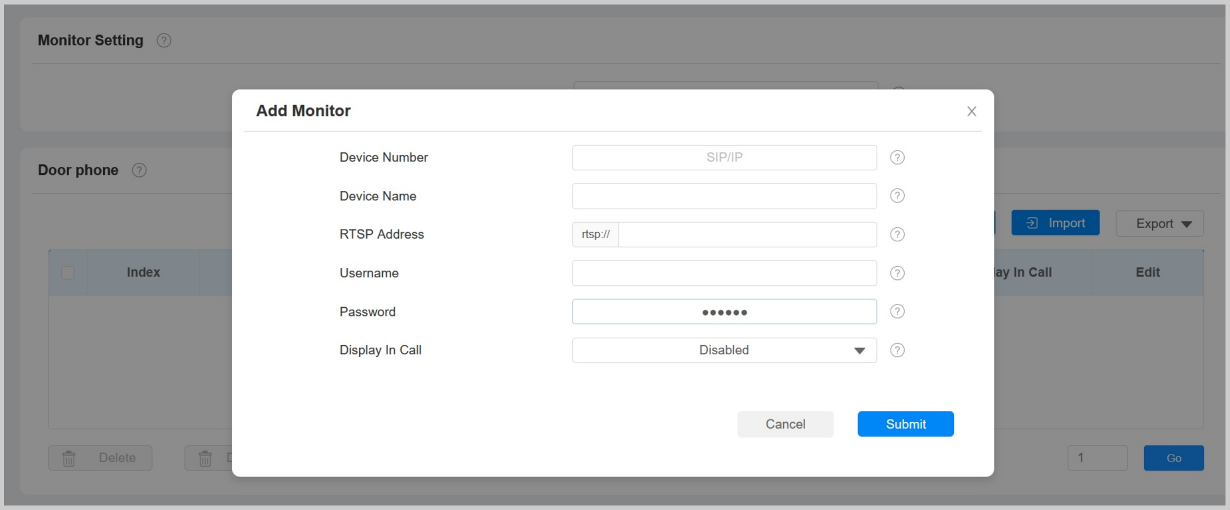
On the **Device > Monitor > Door phone** section, click **+Add** to add a monitor.



Door phone

□	Index	Device Number	Device Name	RTSP Address	Username	Display In Call	Edit

No Data



Monitor Setting

Door phone

Add Monitor

Device Number: SIP/IP

Device Name:

RTSP Address: rtsp://

Username:

Password: ••••••

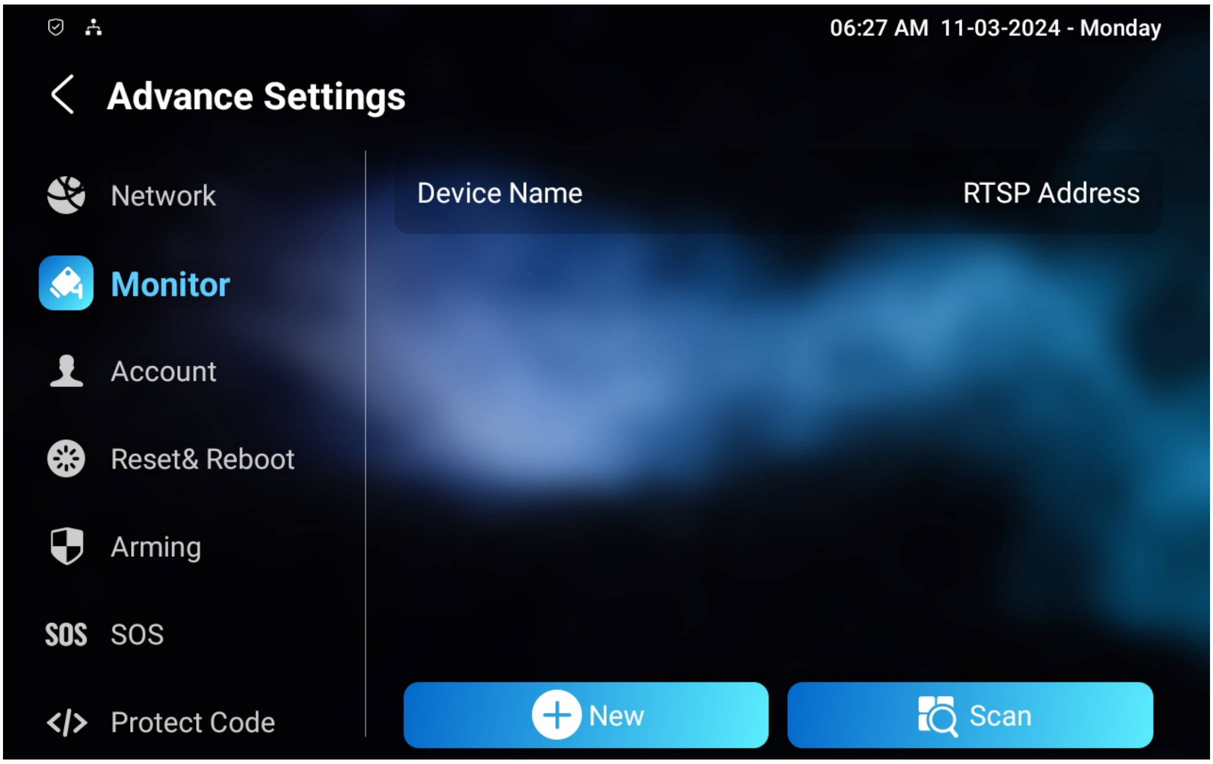
Display In Call: Disabled

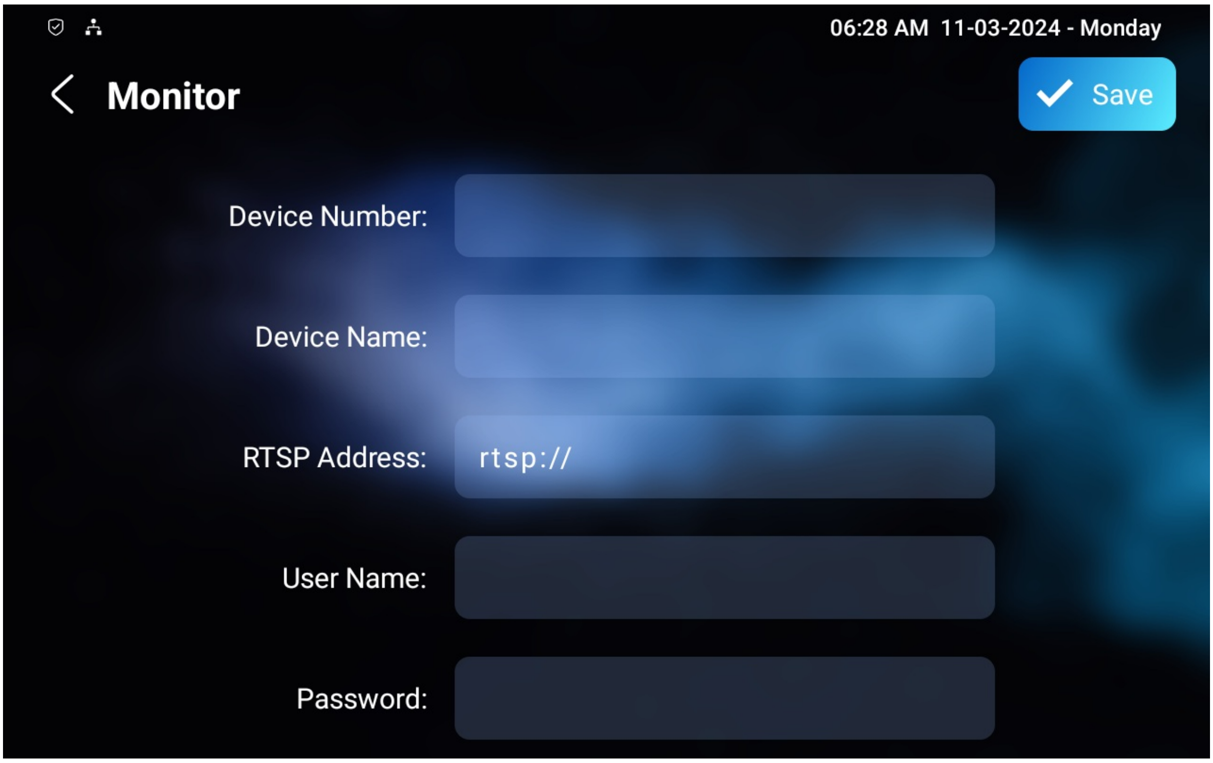
- **Device Number**: The device's SIP/IP number for identification.
- **Device Name**: The device name for identification.
- **RTSP Address**: The RTSP address of the monitoring device. RTSP format: *rtsp://Device IP address/live/ch00_0.*
- **Username**: The username of the monitoring device for authentication.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

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

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

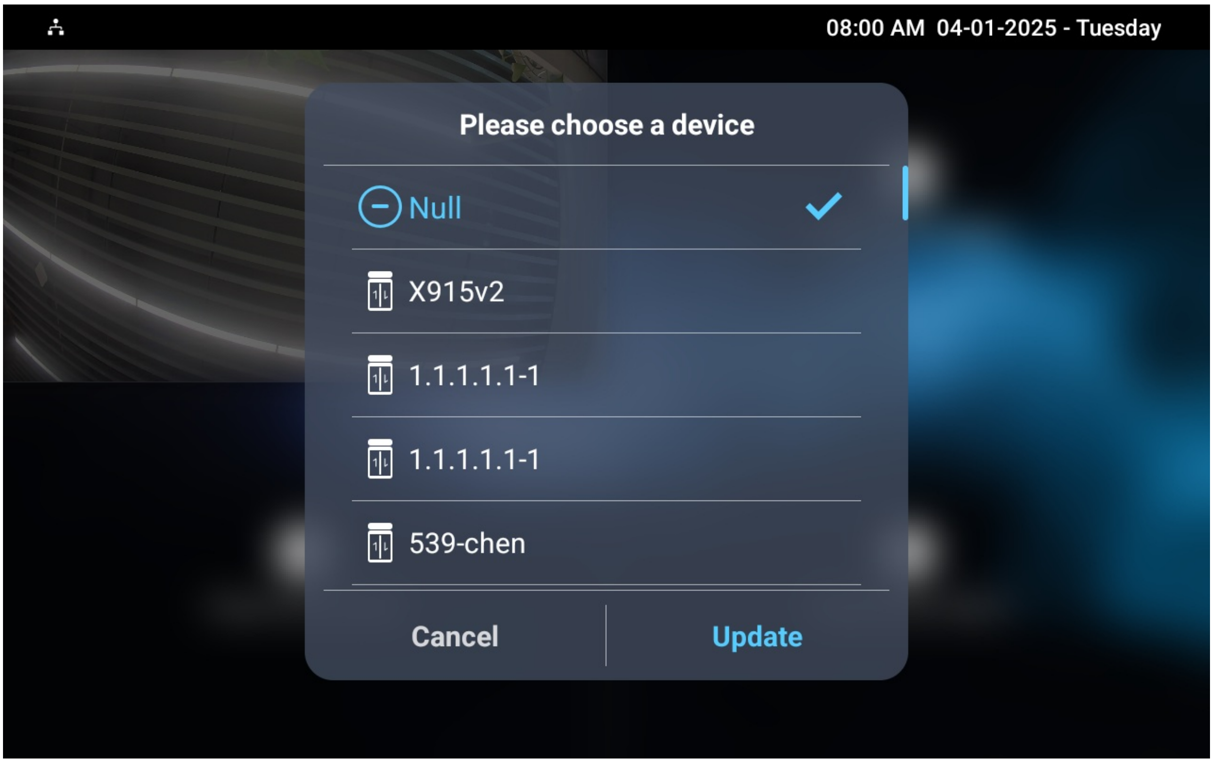
When the monitoring device is an Akuvox door phone and its RTSP username and password are not changed(admin by default), you can directly scan and add the door phone on the indoor monitor’s **Monitor** screen. If the username and password are changed, make sure they are consistent between the devices.

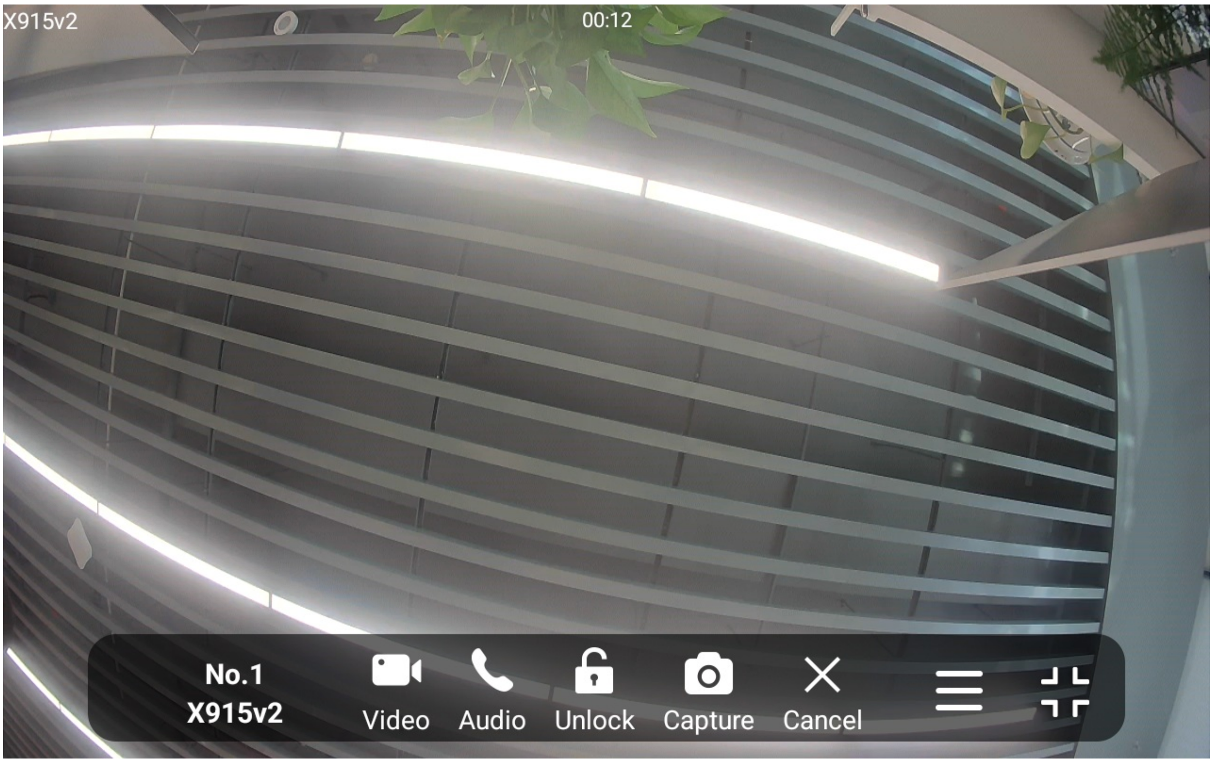




View Monitoring Streams

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





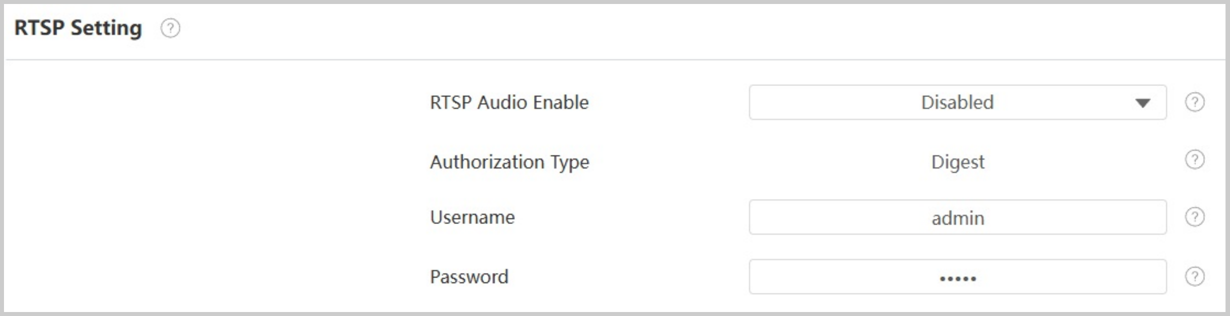
- **Video**: Tap to make a video call to the monitored door phone.
- **Audio**: Tap to make an audio call to the monitored door phone.
- **Unlock**: Tap to open the door.
- **Capture**: Tap to take a screenshot.
- **Cancel**: Tap to exit the monitoring.
- ☰: Tap to display the monitor list.

> **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.



RTSP Setting

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

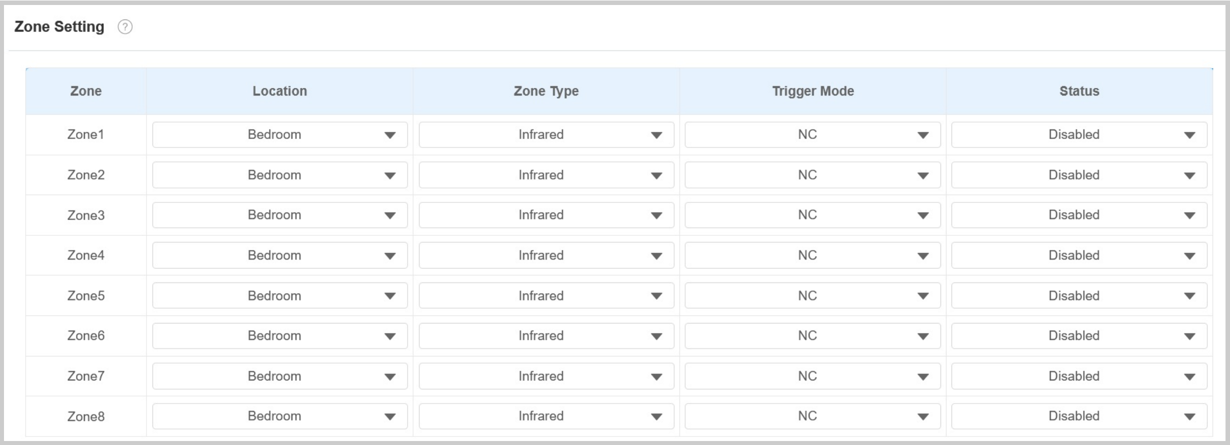
- **Authorization Type**: It is Digest by default.
- **User Name**: Set the username for the authentication.
- **Password**: Set the password for the authentication.

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.

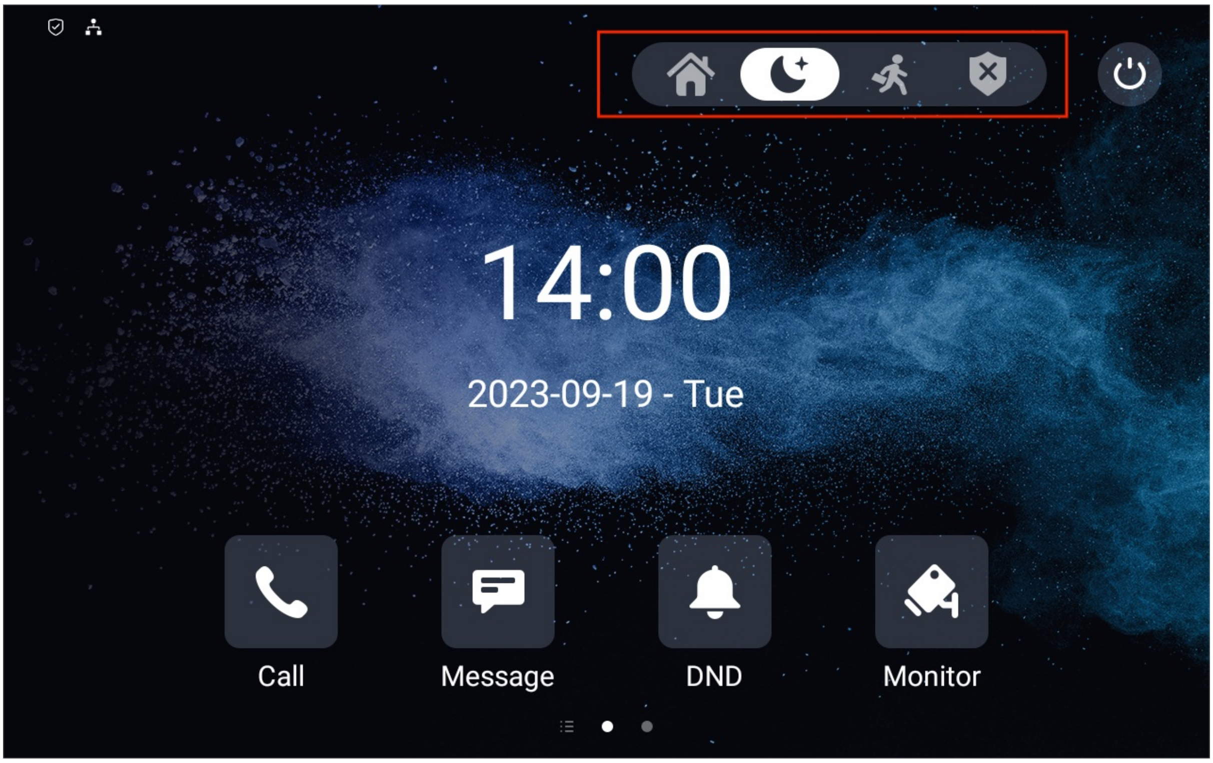


Zone Setting

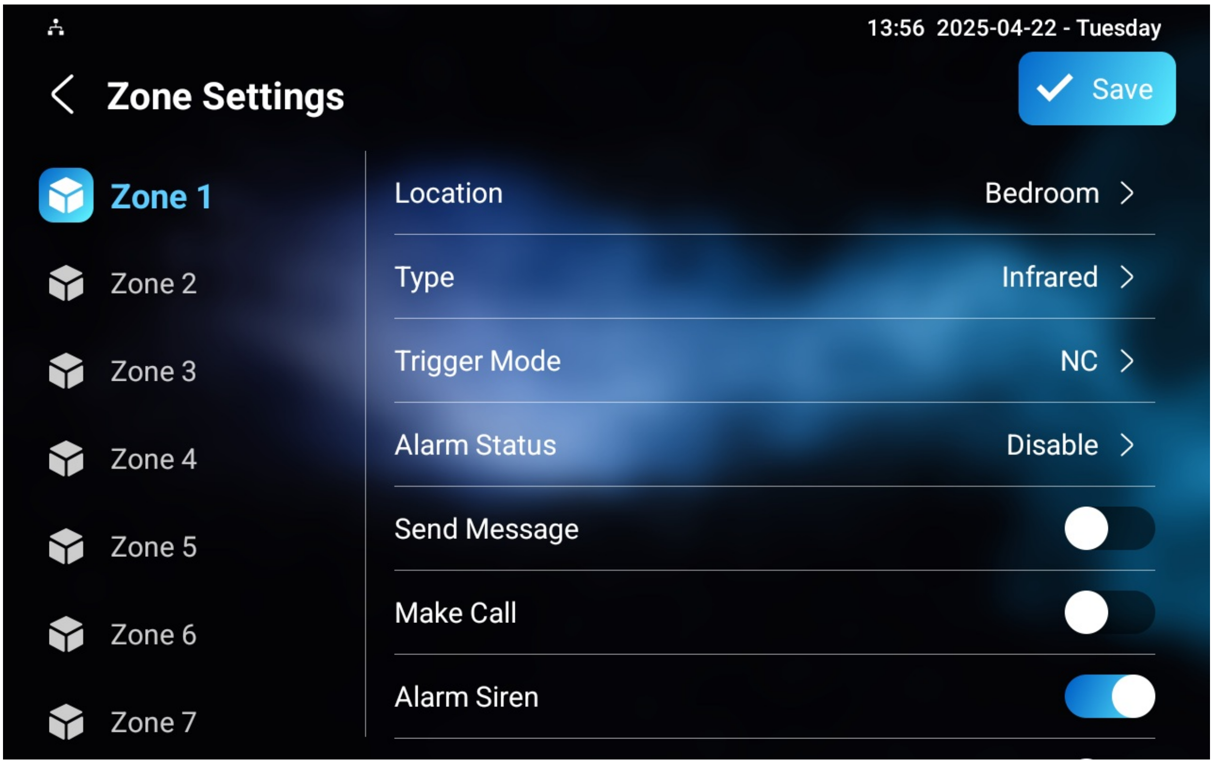
Zone	Location	Zone Type	Trigger Mode	Status
Zone1	Bedroom	Infrared	NC	Disabled
Zone2	Bedroom	Infrared	NC	Disabled
Zone3	Bedroom	Infrared	NC	Disabled
Zone4	Bedroom	Infrared	NC	Disabled
Zone5	Bedroom	Infrared	NC	Disabled
Zone6	Bedroom	Infrared	NC	Disabled
Zone7	Bedroom	Infrared	NC	Disabled
Zone8	Bedroom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

- **Location**: Indicate where the alarm sensor is installed. There are ten location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type**: The alarm sensor types.
- **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.



13:56 2025-04-22 - Tuesday

Zone Settings

Location: Bedroom

Type: Infrared

Trigger Mode: NC

Alarm Status: Disable

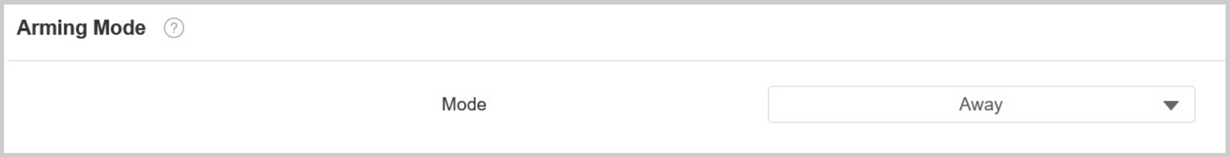
Send Message: Off

Make Call: Off

Alarm Siren: On

Select an Arming Mode

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

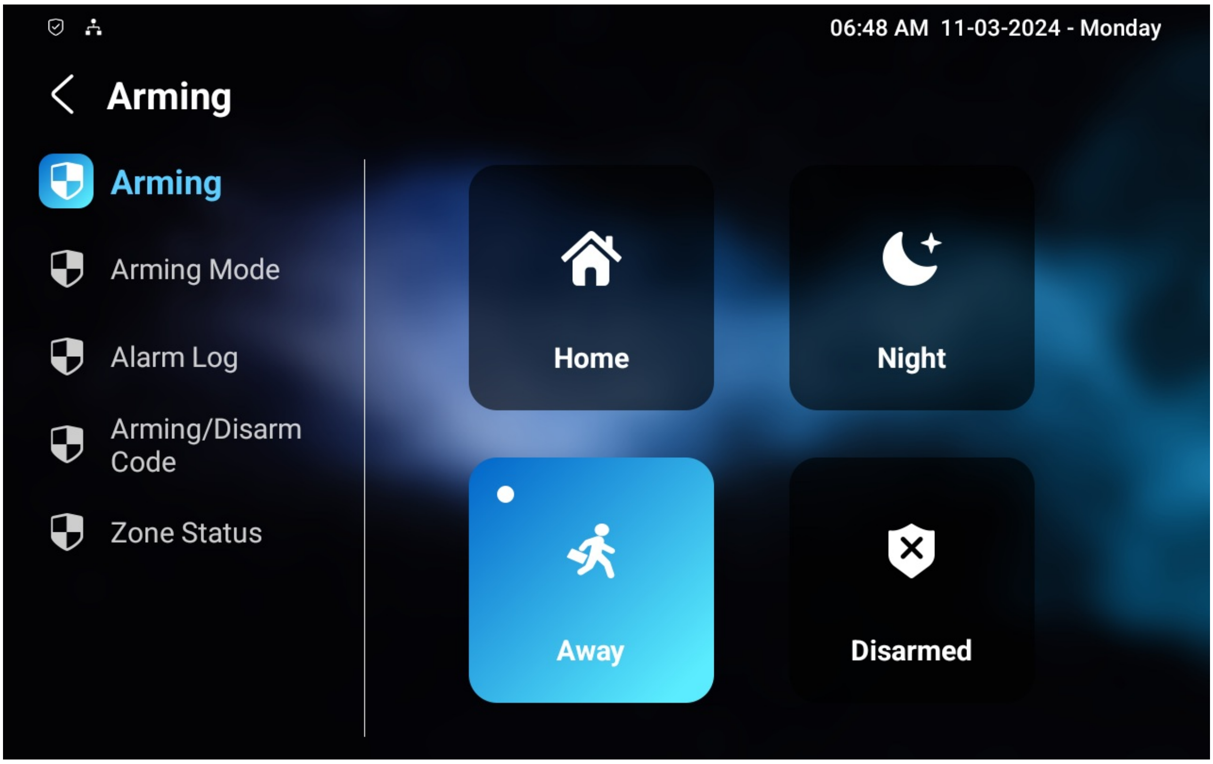


Arming Mode

Mode: Away

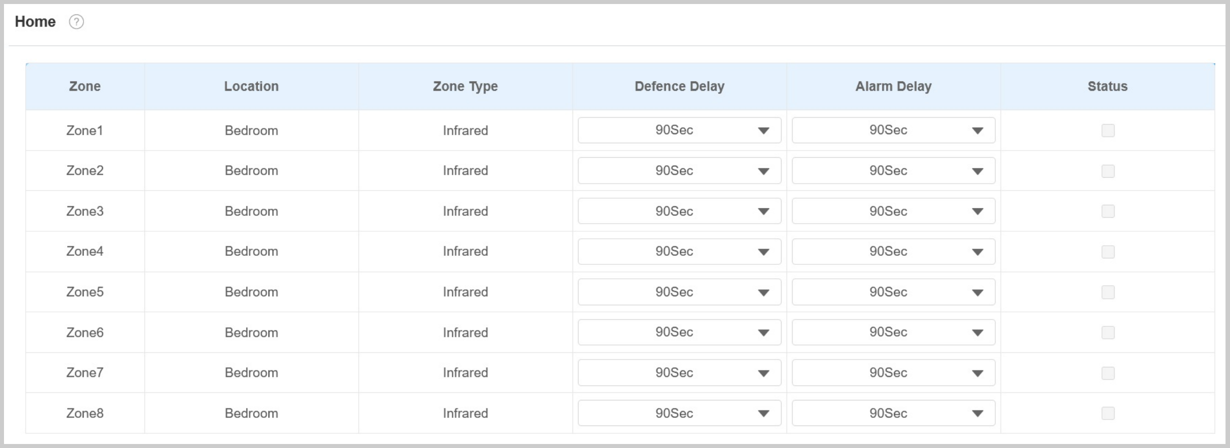
After displaying the Arming tab on the device screen, users can switch arming mode on the Arming screen.

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.

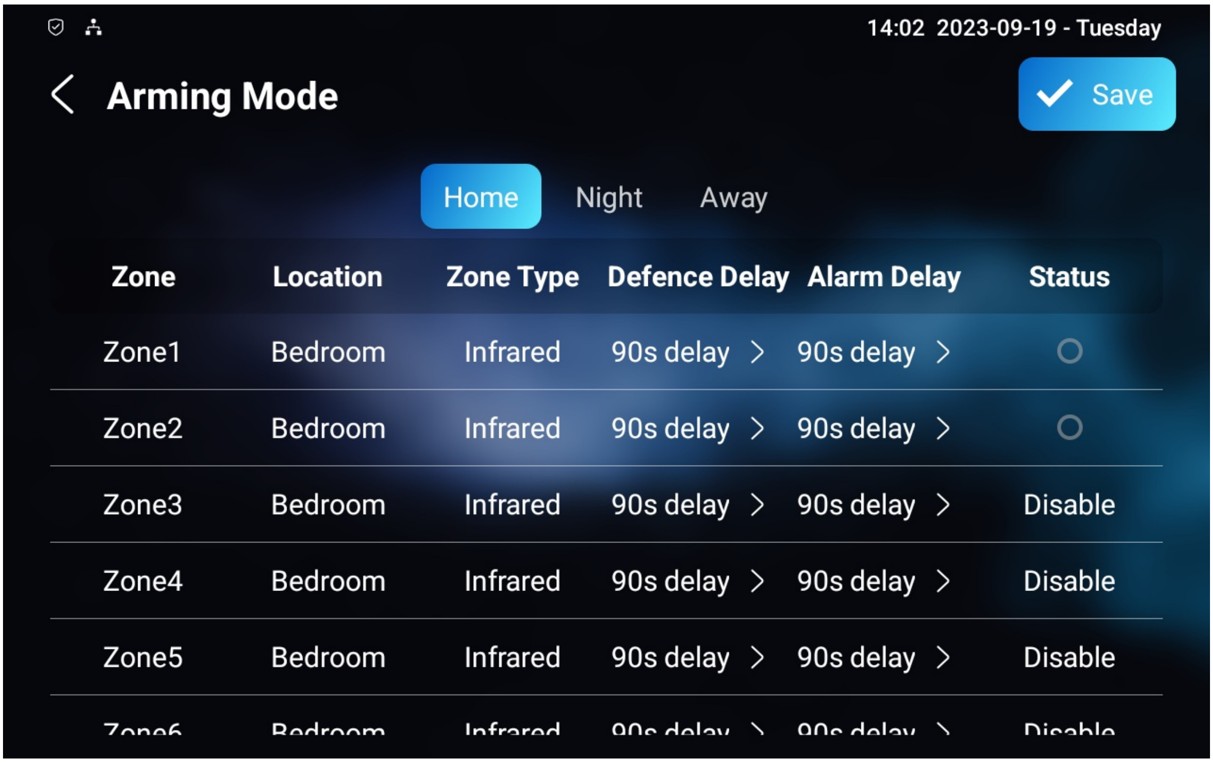


Home

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

- **Location**: Display which location the detection device is in, including Bedroom, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type**: Display the alarm sensor type.
- **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.

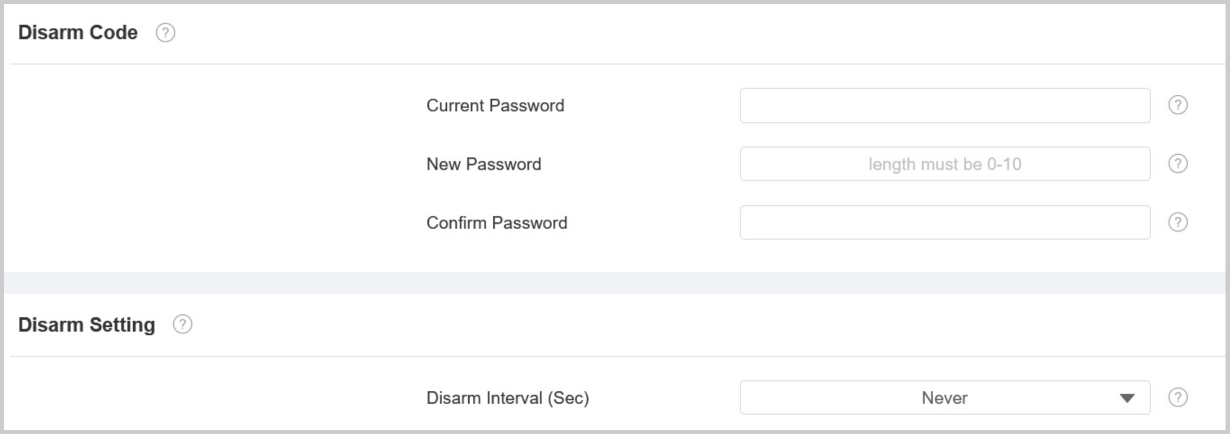
You can also set it up on the **Arming > Arming Mode** screen.



Zone	Location	Zone Type	Defence Delay	Alarm Delay	Status
Zone1	Bedroom	Infrared	90s delay >	90s delay >	○
Zone2	Bedroom	Infrared	90s delay >	90s delay >	○
Zone3	Bedroom	Infrared	90s delay >	90s delay >	Disable
Zone4	Bedroom	Infrared	90s delay >	90s delay >	Disable
Zone5	Bedroom	Infrared	90s delay >	90s delay >	Disable
Zone6	Bedroom	Infrared	90s delay >	90s delay >	Disable

Set up the Disarm Codes

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



Disarm Code

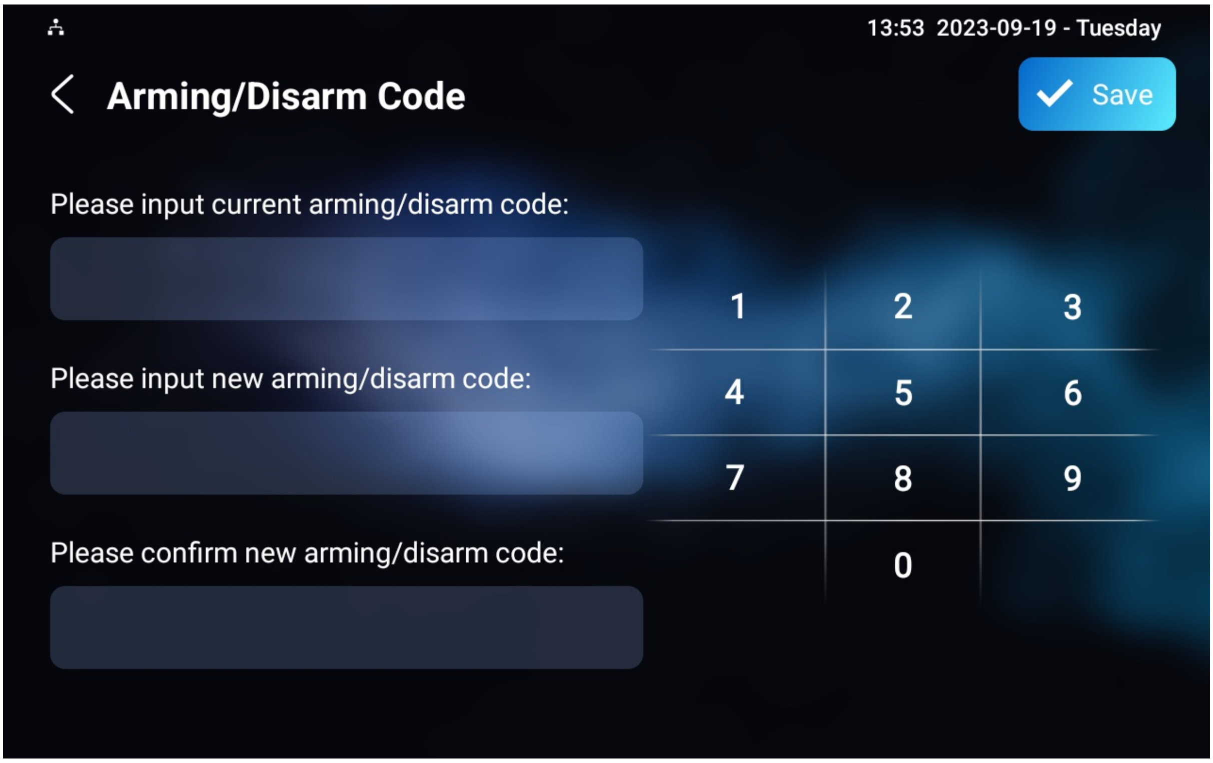
Current Password	
New Password	length must be 0-10
Confirm Password	

Disarm Setting

Disarm Interval (Sec)	Never

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

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



13:53 2023-09-19 - Tuesday

Arming/Disarm Code

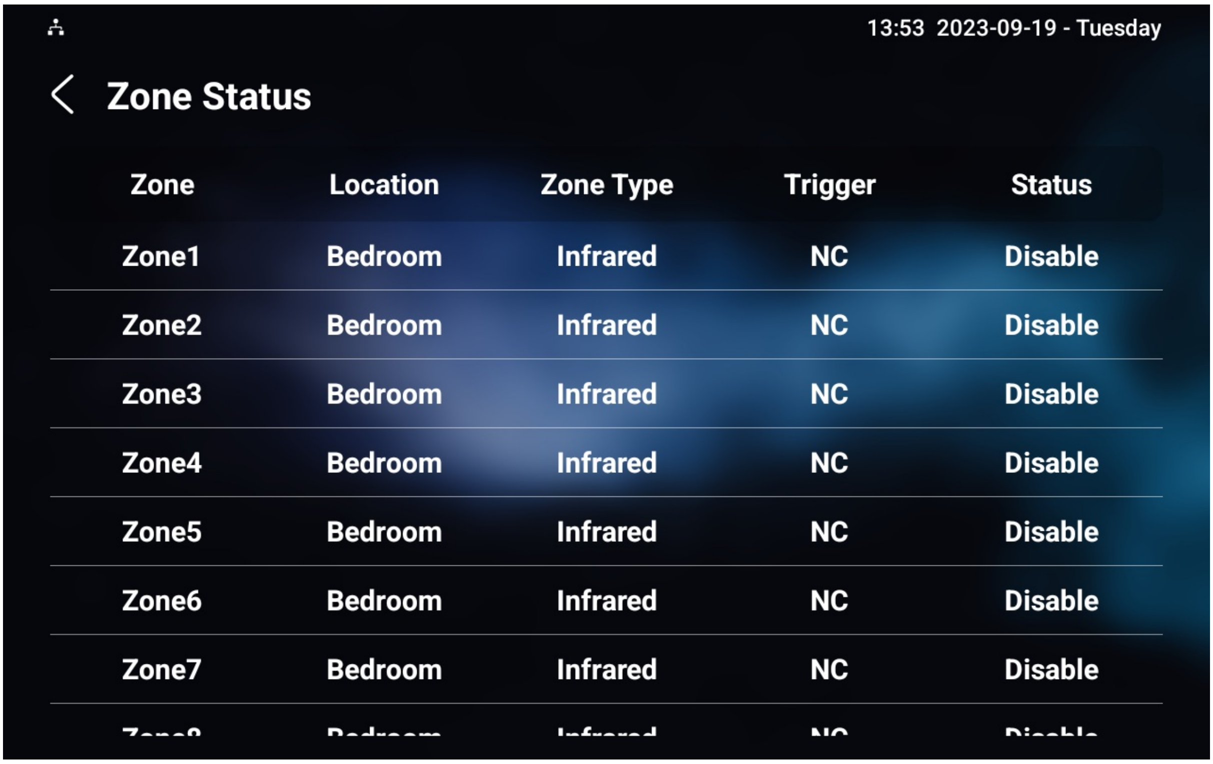
Please input current arming/disarm code:

Please input new arming/disarm code:

Please confirm new arming/disarm code:

Check Zone Status

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



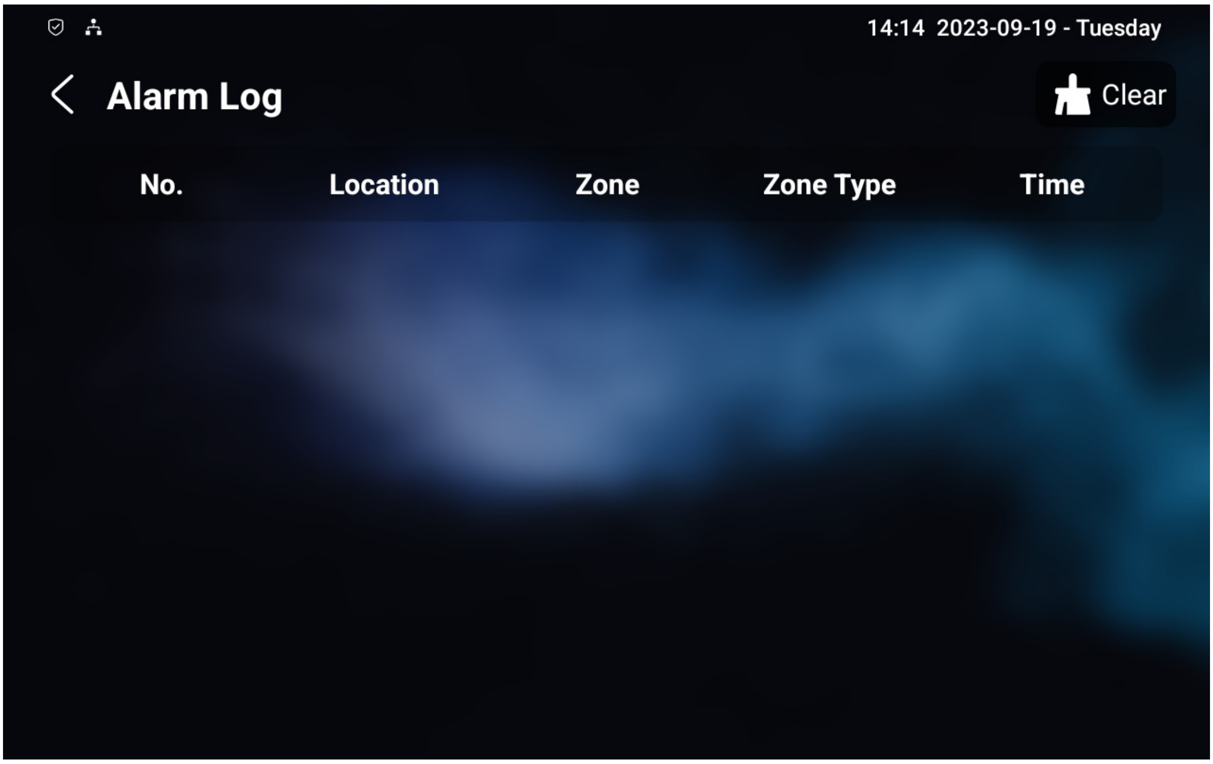
13:53 2023-09-19 - Tuesday

Zone Status

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

Check Alarm Logs

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


14:14 2023-09-19 - Tuesday

Alarm Log

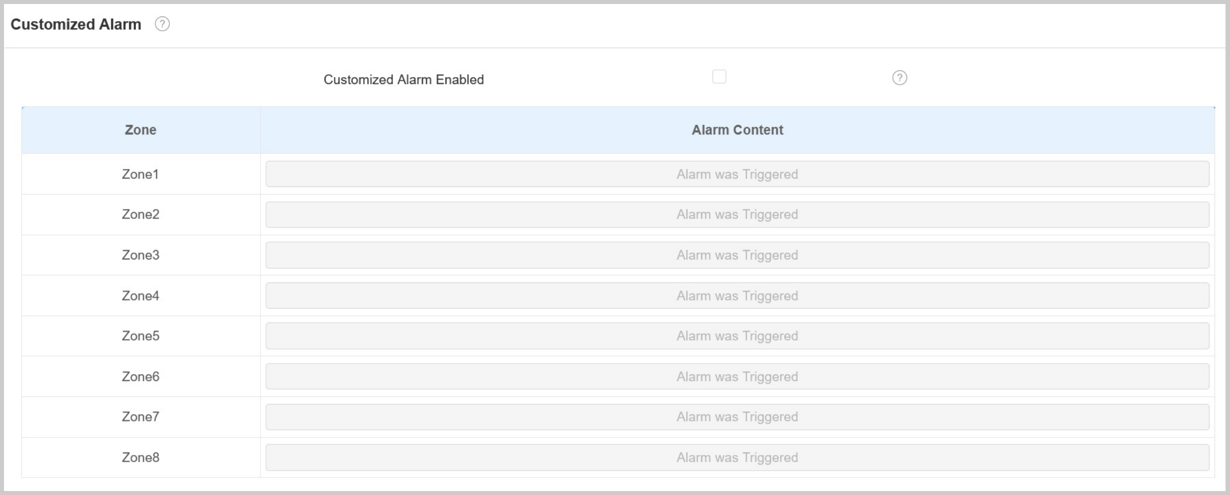
Clear

No.	Location	Zone	Zone Type	Time

Configure Alarm Text

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

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


Customized Alarm

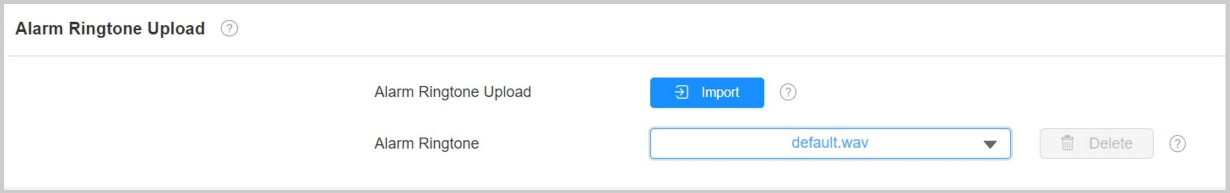
Customized Alarm Enabled □

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

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

Configure Alarm Ringtone

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



Alarm Ringtone Upload

Alarm Ringtone Upload: Import

Alarm Ringtone: default.wav — Delete

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

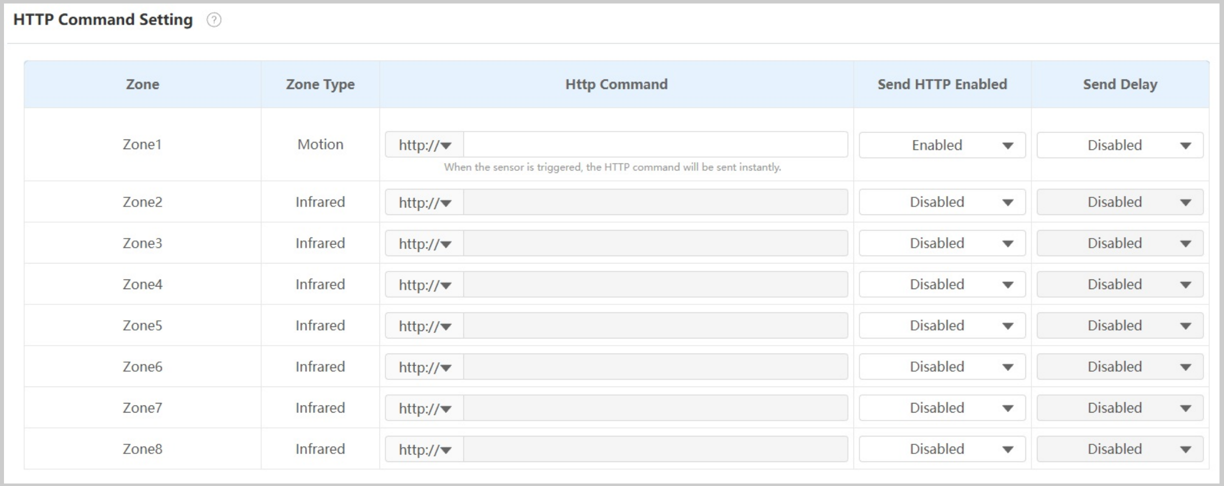
Alarm Action Configuration

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

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

HTTP Command

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



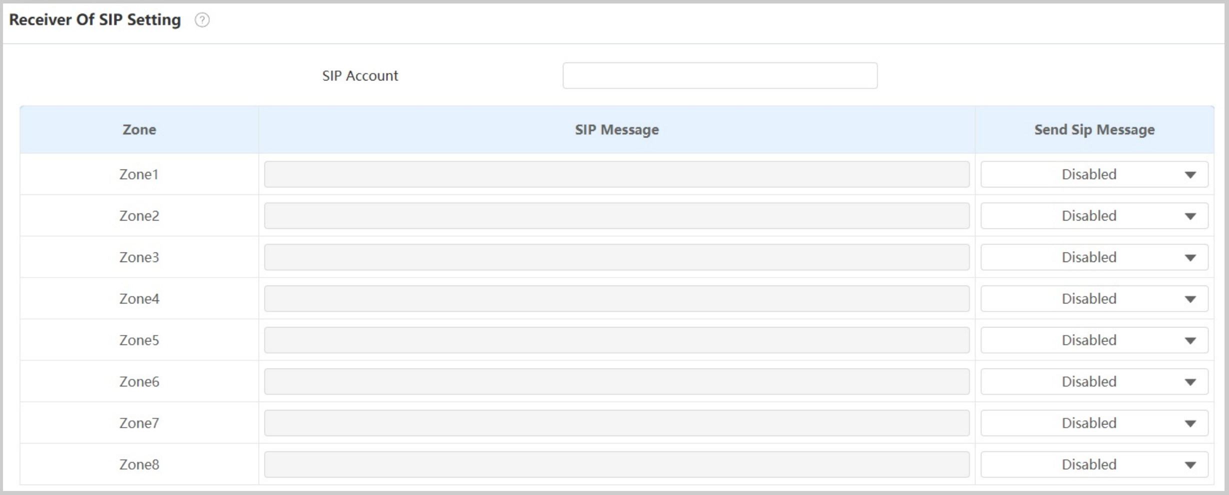
HTTP Command Setting

Zone	Zone Type	Http Command	Send HTTP Enabled	Send Delay
Zone1	Motion	http:// When the sensor is triggered, the HTTP command will be sent instantly.	Enabled	Disabled
Zone2	Infrared	http://	Disabled	Disabled
Zone3	Infrared	http://	Disabled	Disabled
Zone4	Infrared	http://	Disabled	Disabled
Zone5	Infrared	http://	Disabled	Disabled
Zone6	Infrared	http://	Disabled	Disabled
Zone7	Infrared	http://	Disabled	Disabled
Zone8	Infrared	http://	Disabled	Disabled

- **Zone Type**: Display the zone type set on the **Arming > Zone Setting** interface.
- **Send HTTP**: Enable it if you want the action to be implemented on a designated third-party device.
- **HTTP Command**: Enter the HTTP command provided by the third-party device manufacturer.
- **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.

SIP Message

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



Receiver Of SIP Setting

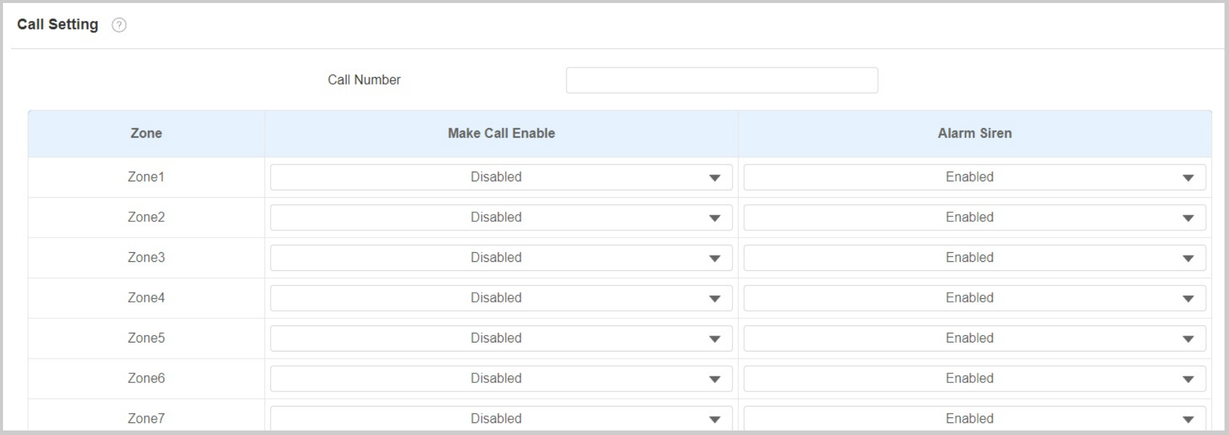
SIP Account

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

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

SIP Call

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



Call Setting

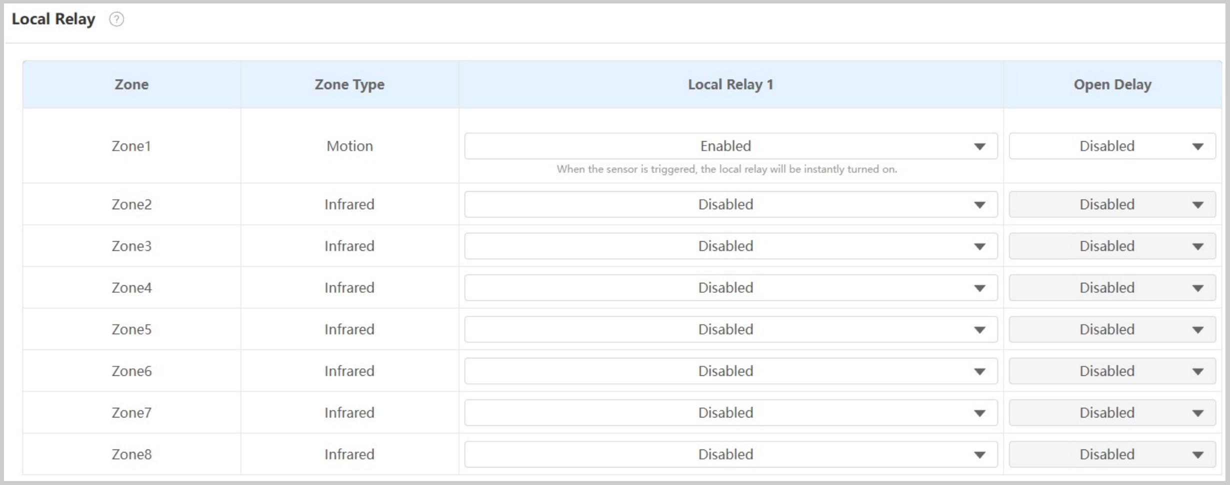
Call Number

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

- **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.

Local Relay

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



Local Relay

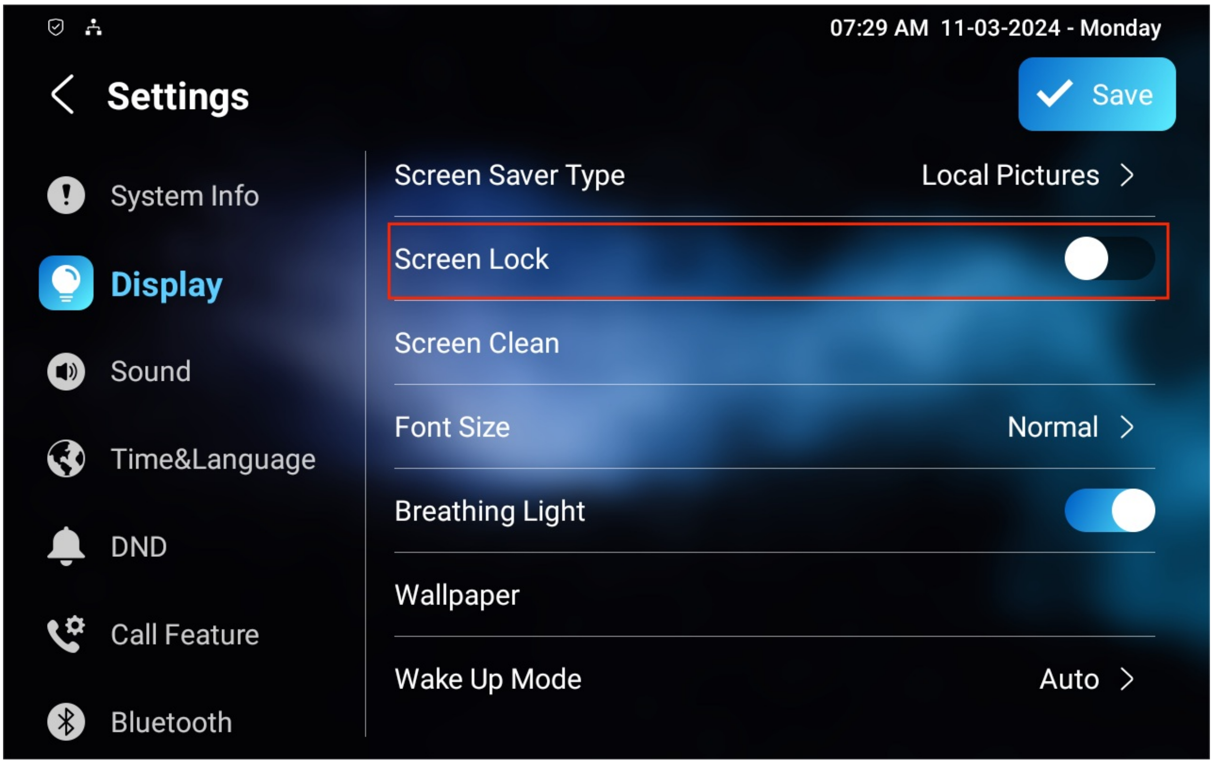
Zone	Zone Type	Local Relay 1	Open Delay
Zone1	Motion	Enabled When the sensor is triggered, the local relay will be instantly turned on.	Disabled
Zone2	Infrared	Disabled	Disabled
Zone3	Infrared	Disabled	Disabled
Zone4	Infrared	Disabled	Disabled
Zone5	Infrared	Disabled	Disabled
Zone6	Infrared	Disabled	Disabled
Zone7	Infrared	Disabled	Disabled
Zone8	Infrared	Disabled	Disabled

- **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.



07:29 AM 11-03-2024 - Monday

Settings

Screen Saver Type: Local Pictures

Screen Lock: off

Screen Clean

Font Size: Normal

Breathing Light: on

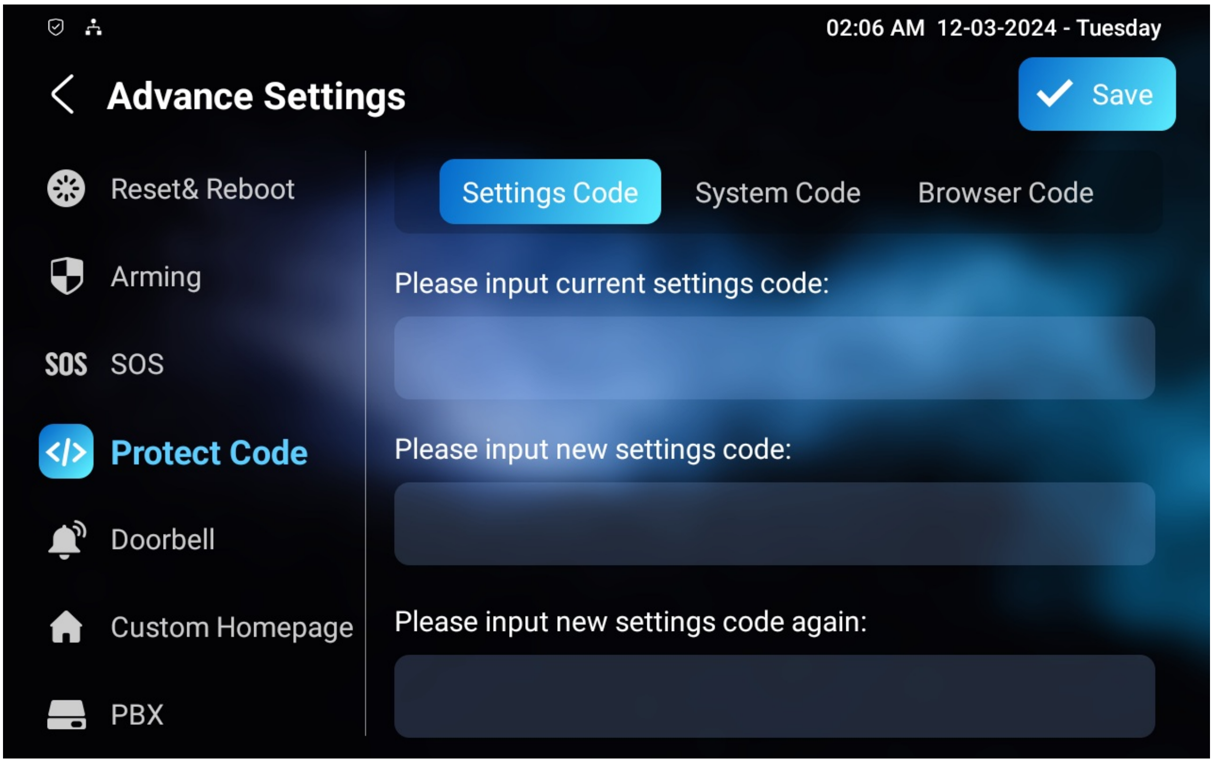
Wallpaper

Wake Up Mode: Auto

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 the password.



Please input current settings code:

Please input new settings code:

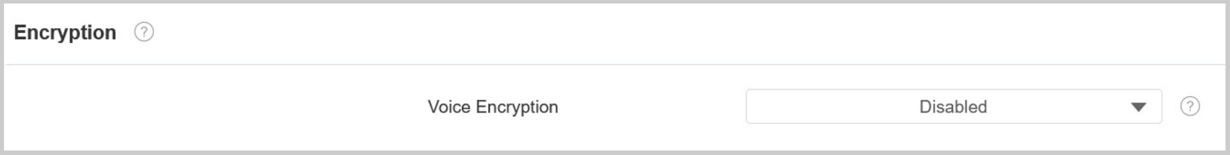
Please input new settings code again:

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

Voice Encryption

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

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



Encryption

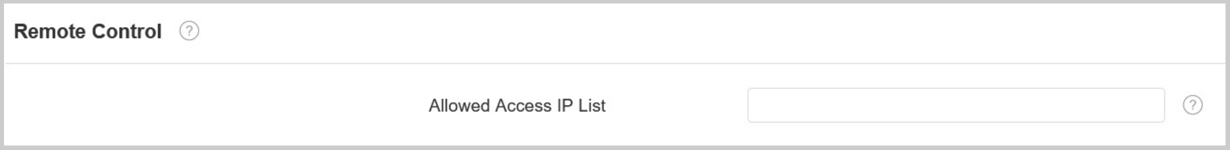
Voice Encryption: Disabled

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

Remote Control

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

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



Remote Control

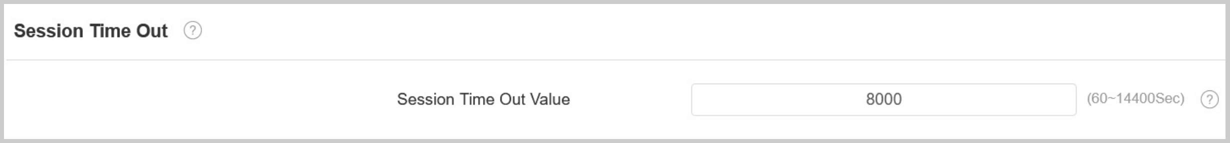
Allowed Access IP List:

- **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.



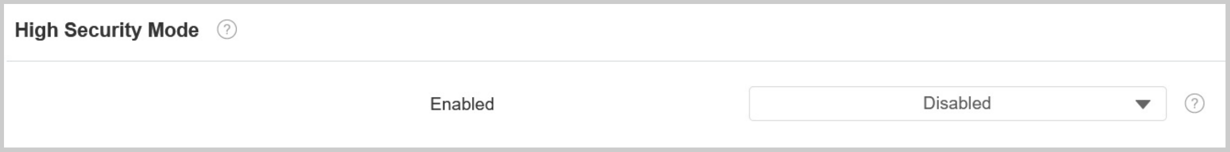
Session Time Out

Session Time Out Value: 8000 (60~14400Sec)

High Security Mode

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

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



High Security Mode

Enabled: Disabled

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

Residents can summon and send the lift by simply tapping on the Akuvox indoor monitor.

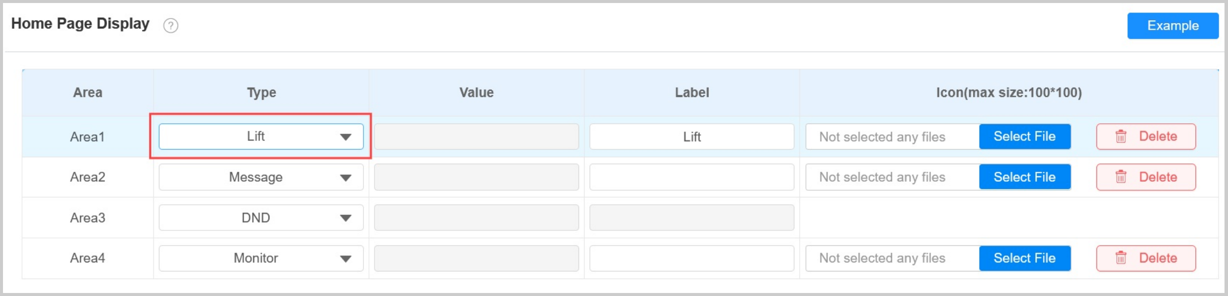
To achieve this function, you need to set up the lift control feature on both the indoor monitor and the lift controller EC33.

Click here to view the configuration steps.

Set Lift Control Icon

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

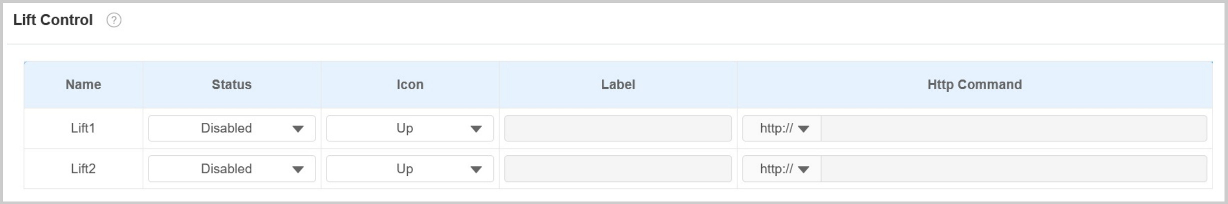
To display the icon, go to the **Device > Display Setting** interface.



Home Page Display

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

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

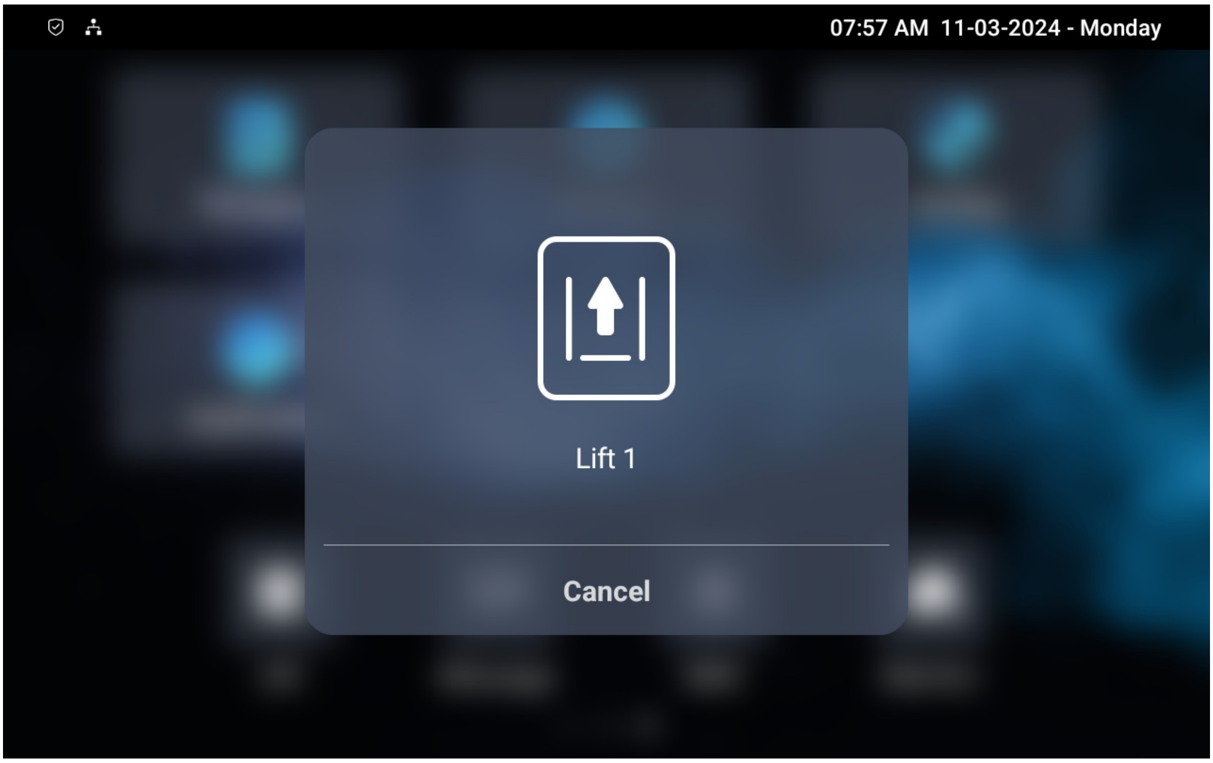


Lift Control

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

- **Status**: Enable or disable the lift button.
- **Icon**: 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.

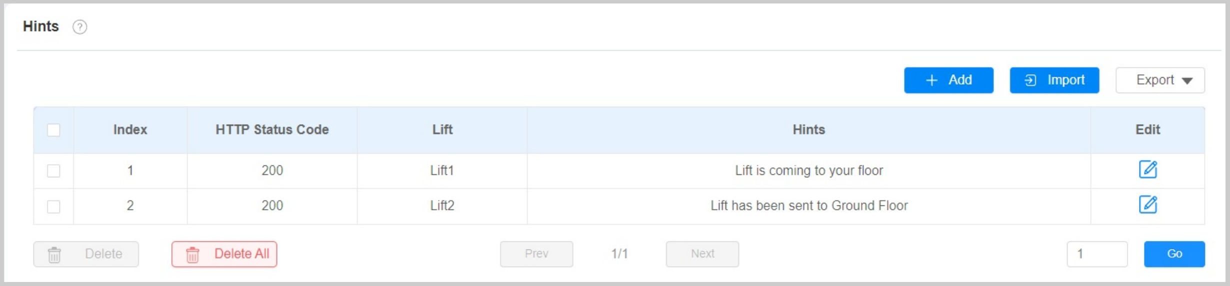
Users can tap the icon to summon or send a lift.



Set Lift Control Prompt

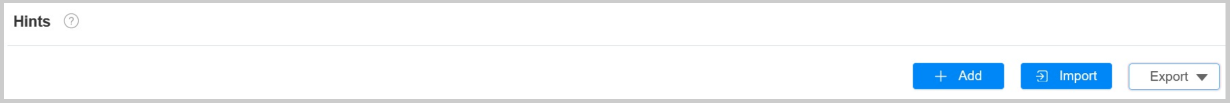
When the lift controller receives the HTTP command, it will give feedback on the current lift status with a prompt.

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



□	Index	HTTP Status Code	Lift	Hints	Edit
□	1	200	Lift1	Lift is coming to your floor	✎
□	2	200	Lift2	Lift has been sent to Ground Floor	✎

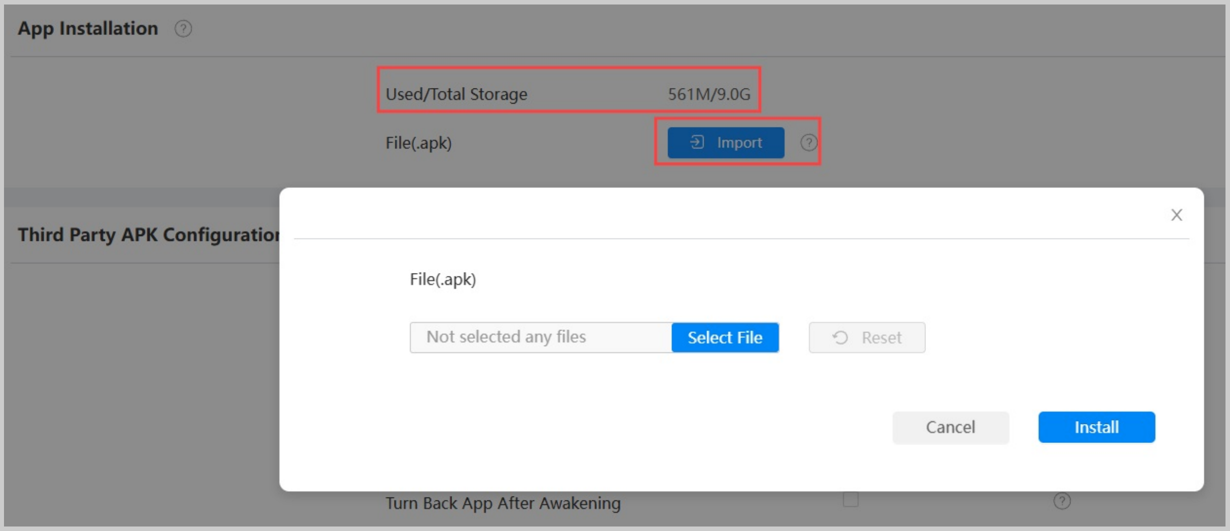
If there are huge amounts of prompts that need to be added, you can click the **Export** tab to export a template and import the file after editing. The import and export files should be in XML format.



Integration with Third-party Devices

Install Third-party App

To check the used/total storage of the device and 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**.



App Installation

Used/Total Storage 561M/9.0G

File(.apk) Import

Third Party APK Configuration

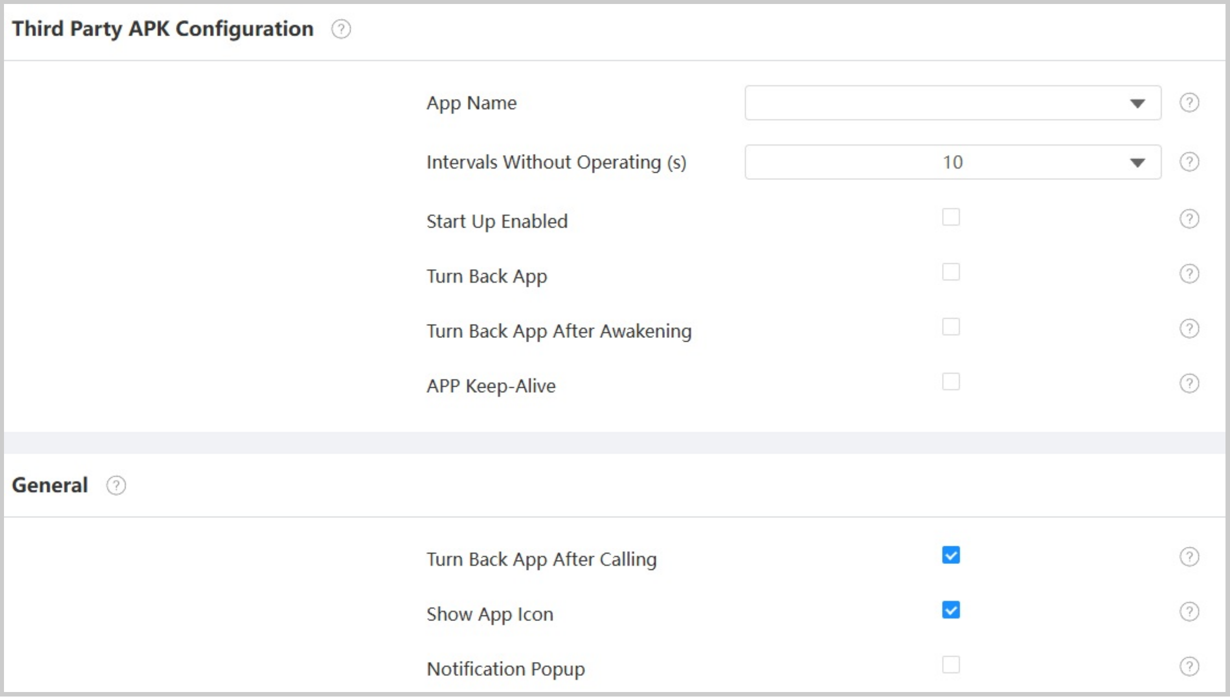
File(.apk)

Not selected any files | Select File | Reset

Cancel | Install

Turn Back App After Awakening □

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



Third Party APK Configuration

App Name

Intervals Without Operating (s) 10

Start Up Enabled □

Turn Back App □

Turn Back App After Awakening □

APP Keep-Alive □

General

Turn Back App After Calling ☑

Show App Icon ☑

Notification Popup □

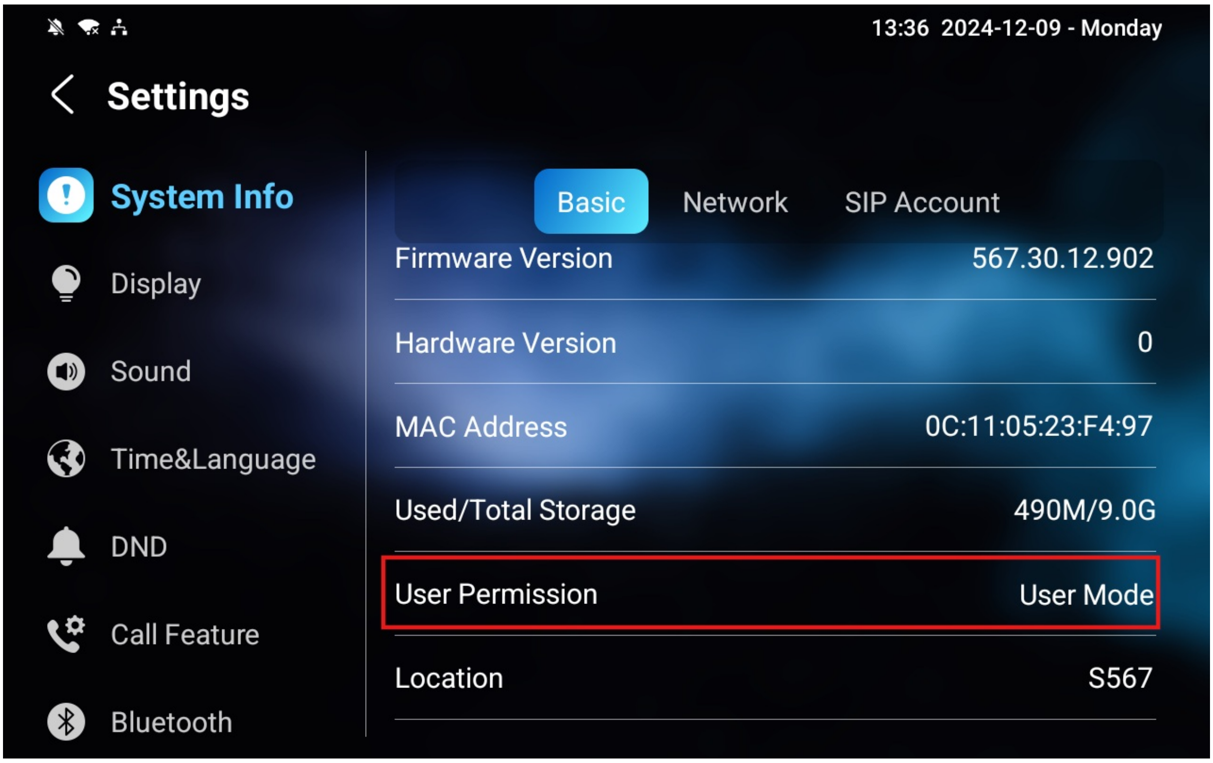
- **App Name**: Select the app to be configured.
- **Intervals Without Operating(Sec)**: Set the time to return to the app when there is no operation on the device.

- **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.

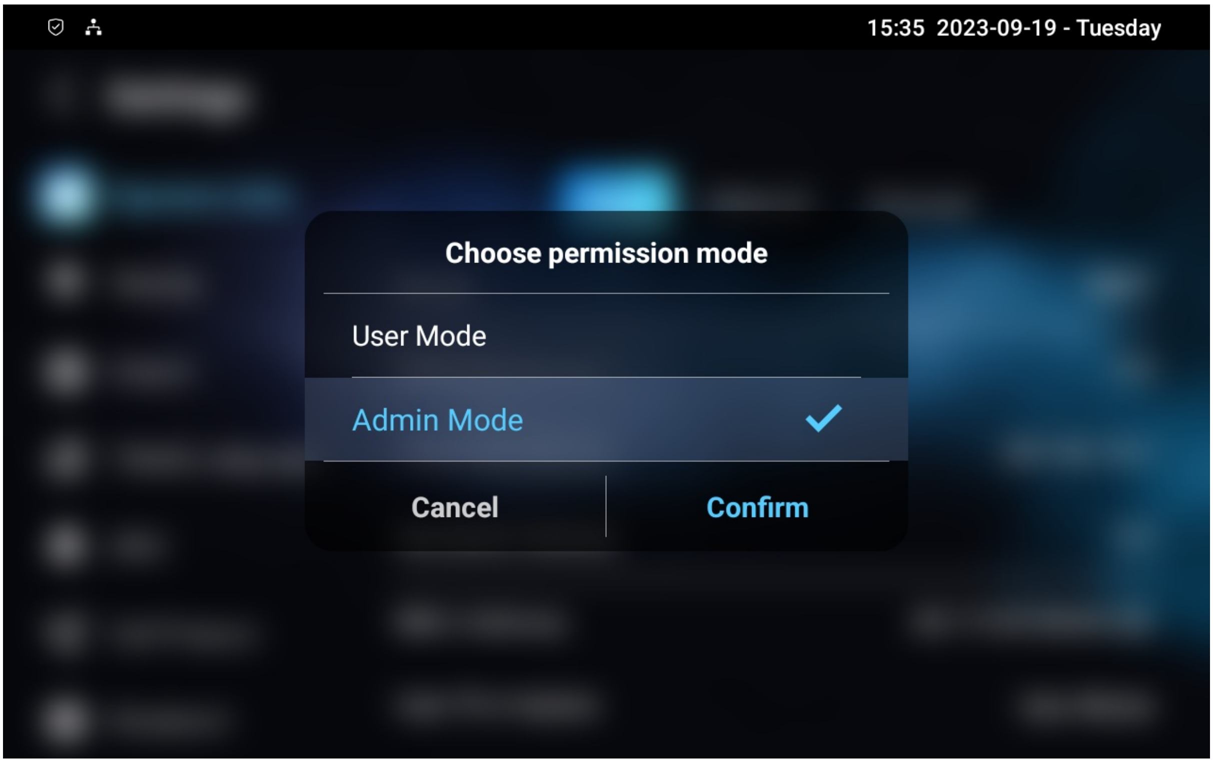
Enter Applications Screen

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

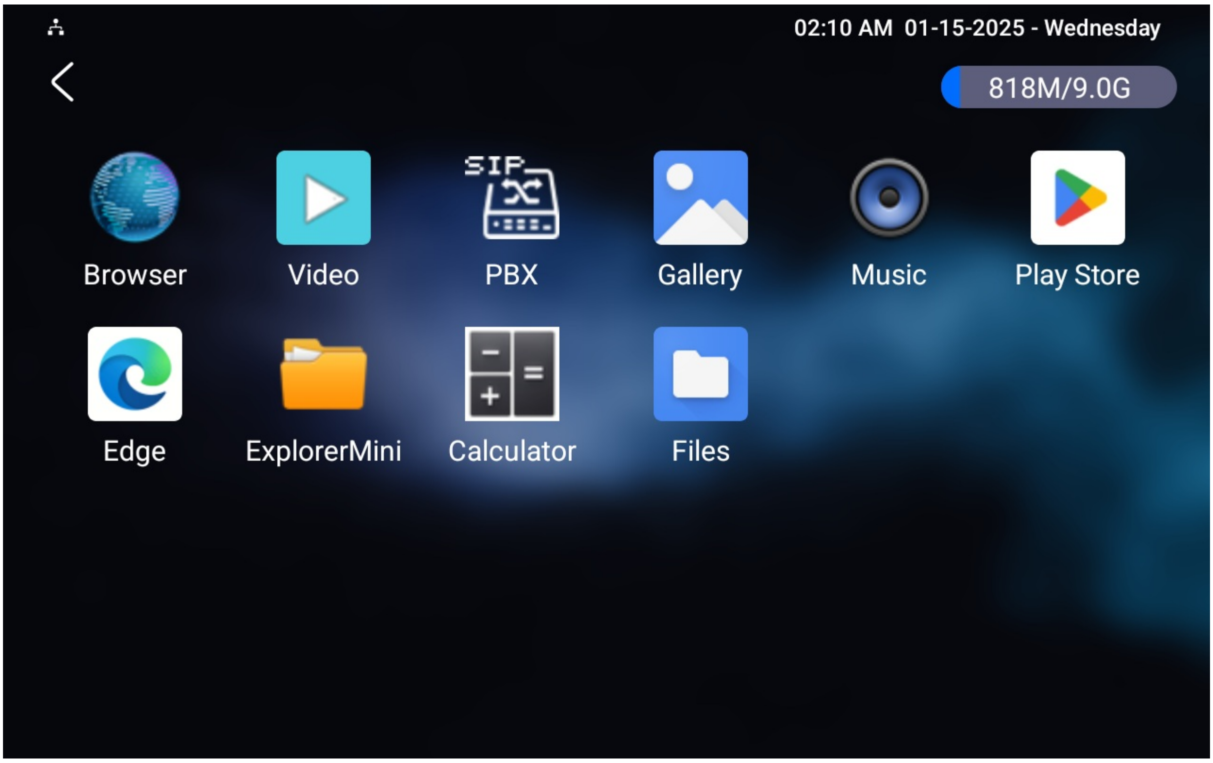
Go to the **Settings > System Info** interface. Tap on **User Mode** 10 times. Then select **Admin Mode** and tap Confirm.



Firmware Version	567.30.12.902
Hardware Version	0
MAC Address	0C:11:05:23:F4:97
Used/Total Storage	490M/9.0G
User Permission	User Mode
Location	S567



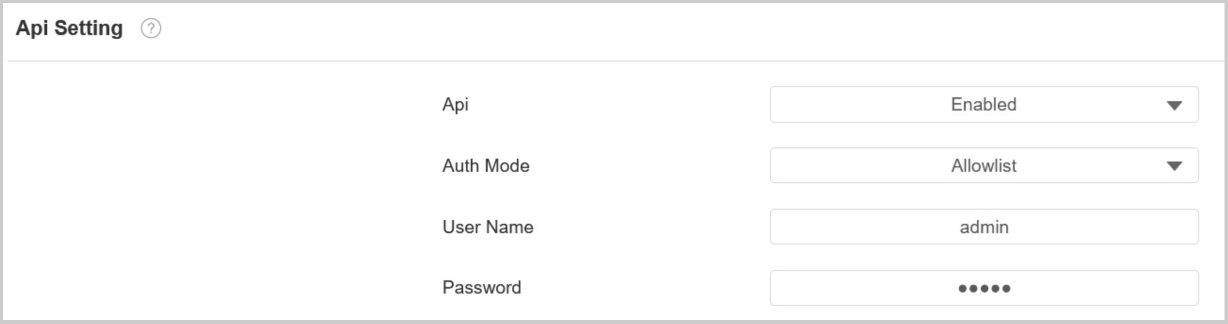
The Application tab will display on the home screen. Tap it to access applications.



Integration via HTTP API

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

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



Api Setting

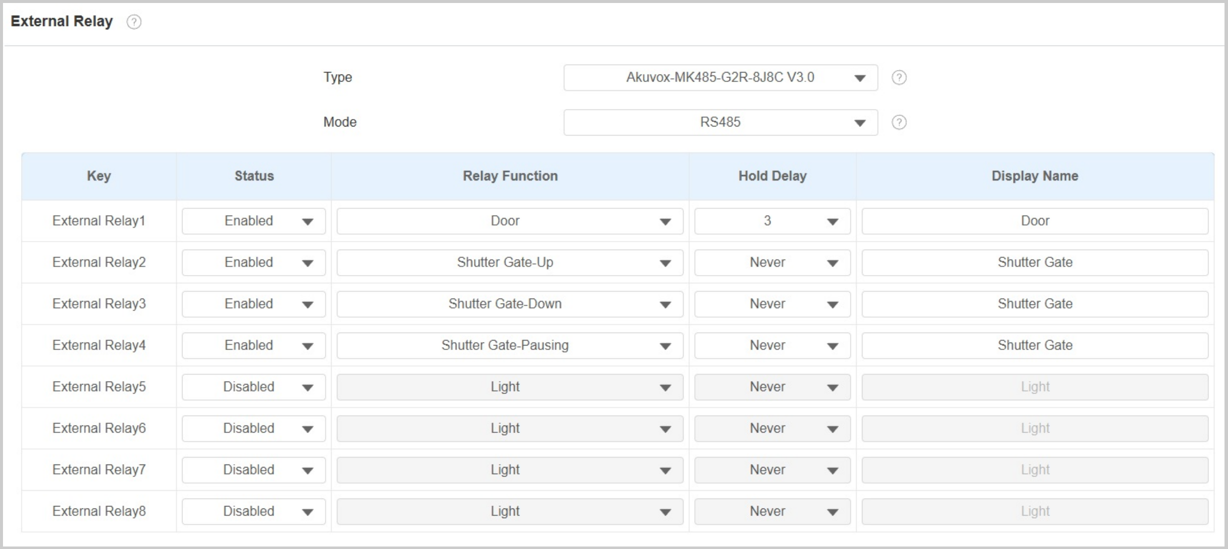
Api	Enabled
Auth Mode	Allowlist
User Name	admin
Password	●●●●●

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



External Relay

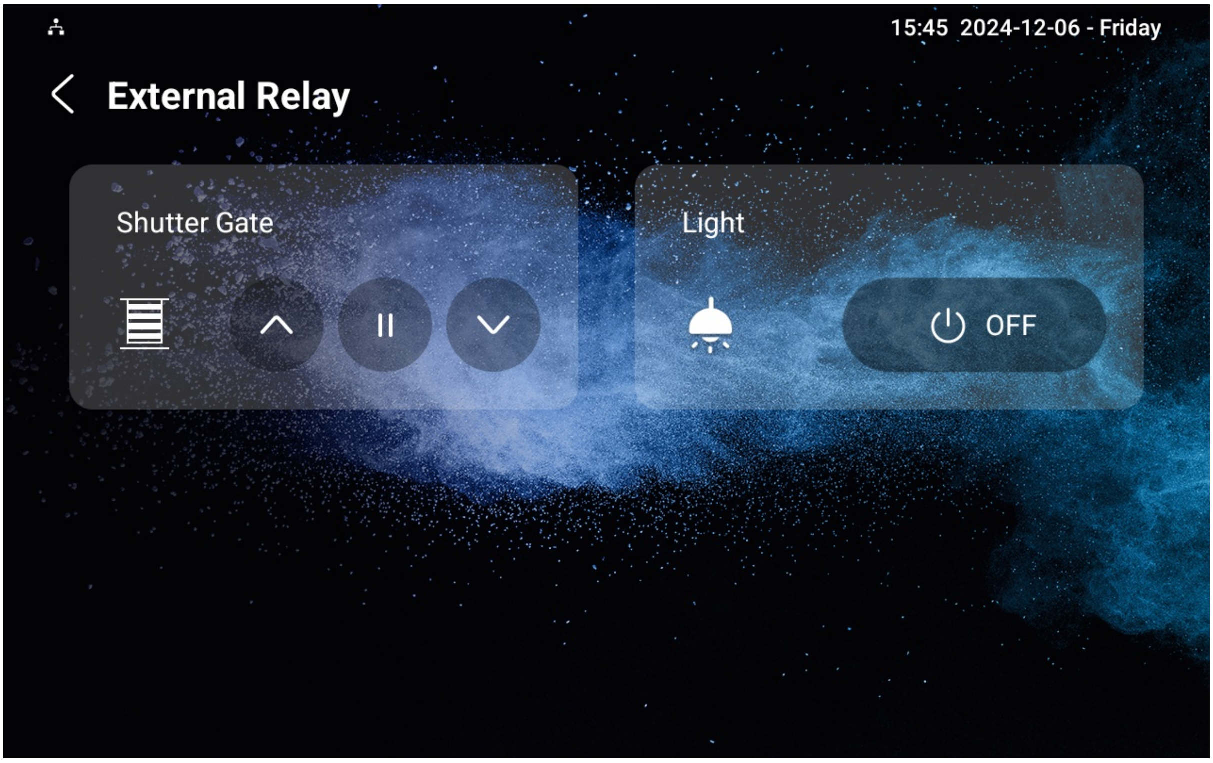
Type: Akuvox-MK485-G2R-8J8C V3.0

Mode: RS485

Key	Status	Relay Function	Hold Delay	Display Name
External Relay1	Enabled	Door	3	Door
External Relay2	Enabled	Shutter Gate-Up	Never	Shutter Gate
External Relay3	Enabled	Shutter Gate-Down	Never	Shutter Gate
External Relay4	Enabled	Shutter Gate-Pausing	Never	Shutter Gate
External Relay5	Disabled	Light	Never	Light
External Relay6	Disabled	Light	Never	Light
External Relay7	Disabled	Light	Never	Light
External Relay8	Disabled	Light	Never	Light

- **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

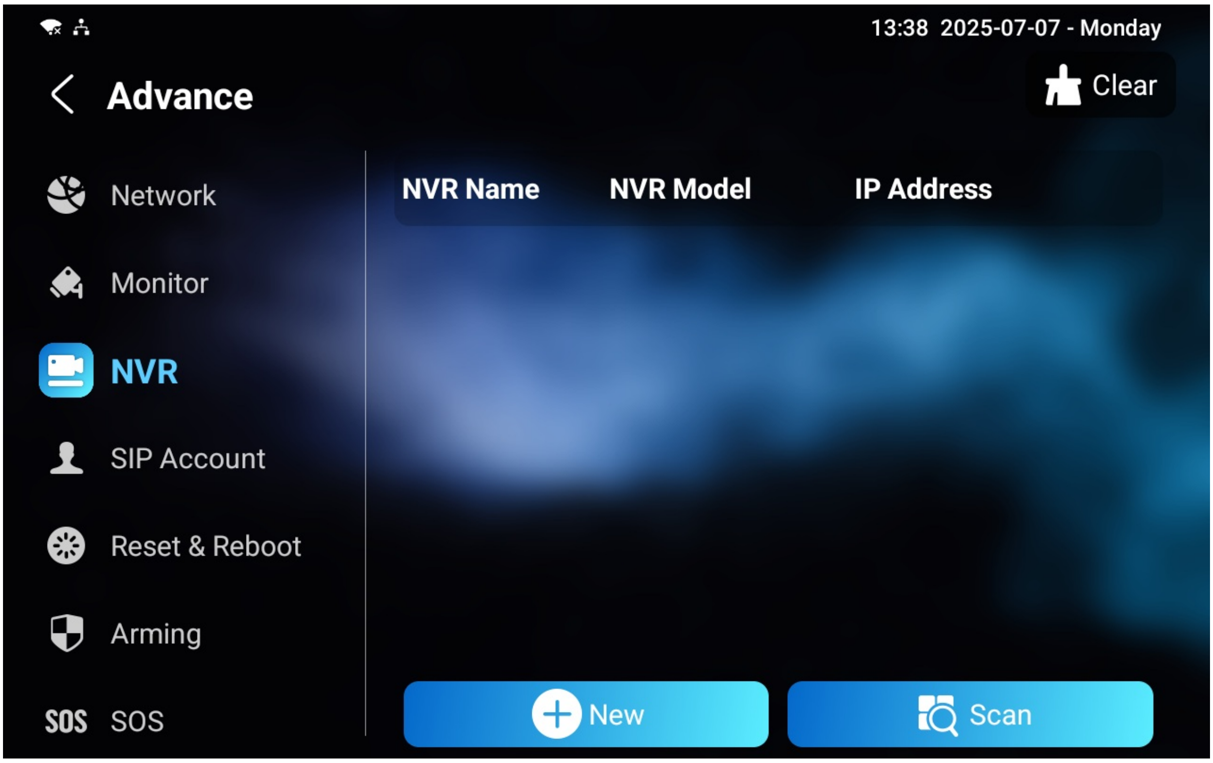
- To display the External Relay button on the home screen, set it up on the **Device > Display Setting** interface.
- Click here to view the detailed configuration of the external relay feature.

Integration with Hikvision NVR

The device can be integrated with the Hikvision NVR, which allows users to view the live stream from IP cameras.

Click here to view the detailed configuration.

To set it up, go to **Settings > Advance > NVR** screen. Click **New** to add the IP camera manually; click **Scan** to detect it.



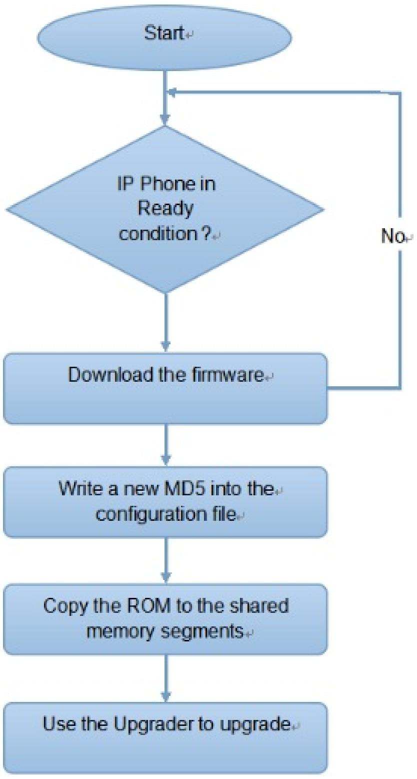
13:38 2025-07-07 - Monday
Advance
Clear
Network
Monitor
NVR
SIP Account
Reset & Reboot
Arming
SOS
NVR Name
NVR Model
IP Address
New
Scan

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:


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

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**:

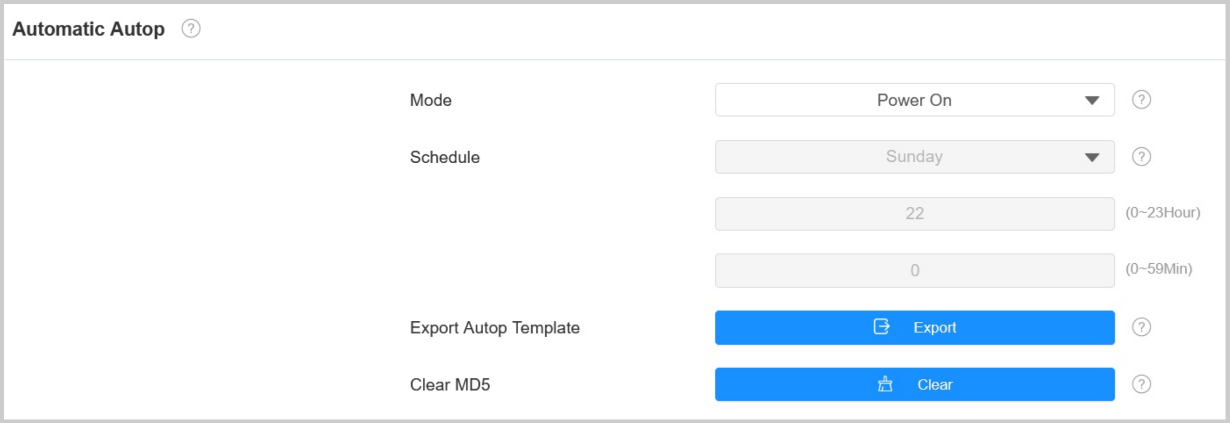
MAC-based configuration files are specific to individual devices, identified by their unique MAC addresses. Files named with the device's MAC address will be matched automatically before downloading for provisioning.

> **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.



Automatic Autop

Mode: Power On

Schedule: Sunday

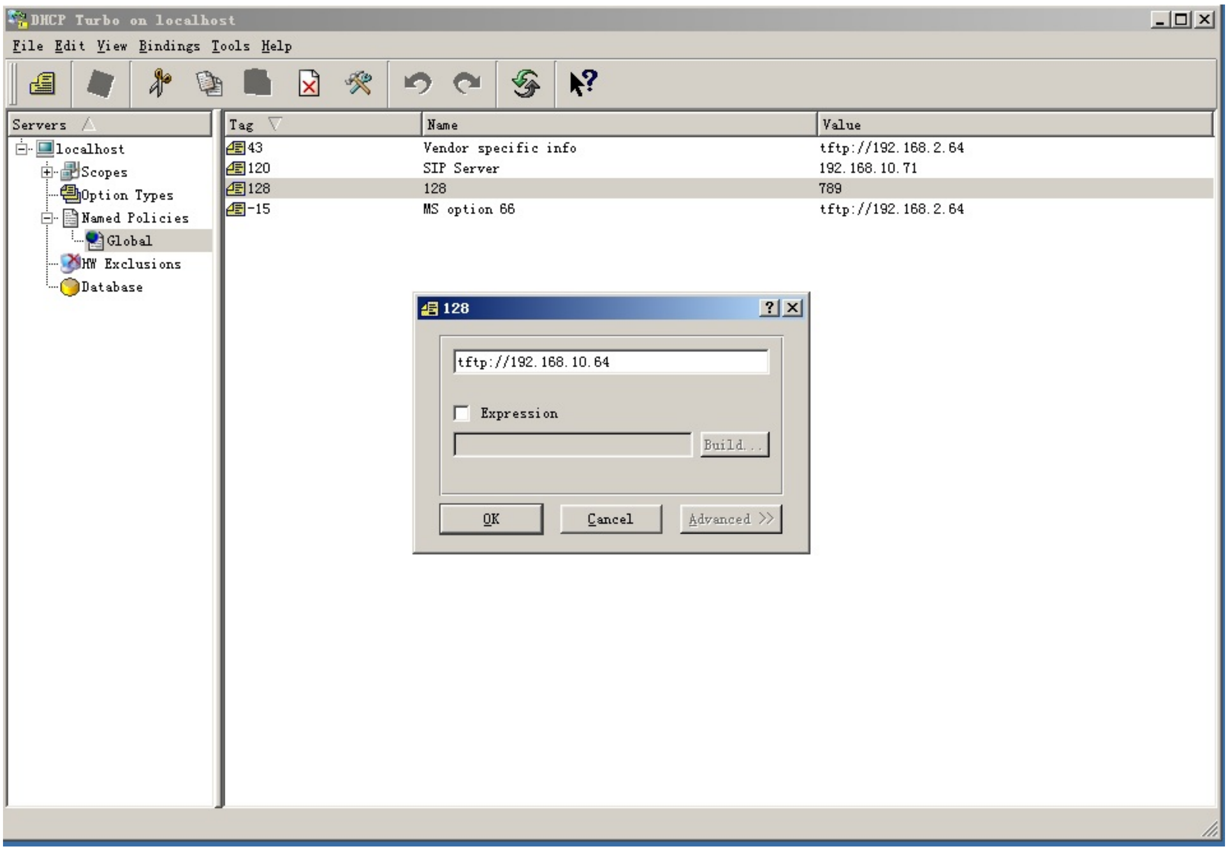
22 (0~23Hour)

0 (0~59Min)

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

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.



Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

128

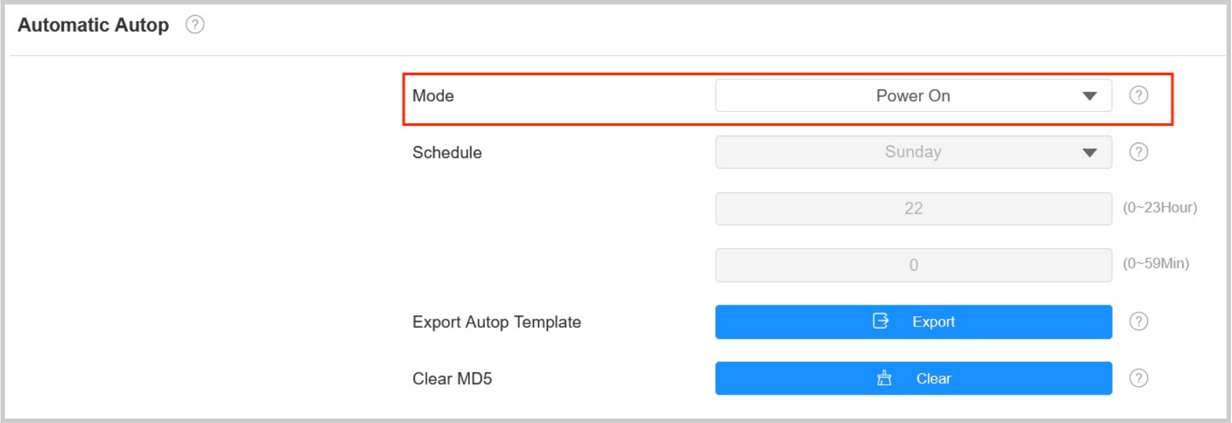
tftp://192.168.10.64

□ Expression

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.


Automatic Autop

Mode: Power On

Schedule: Sunday

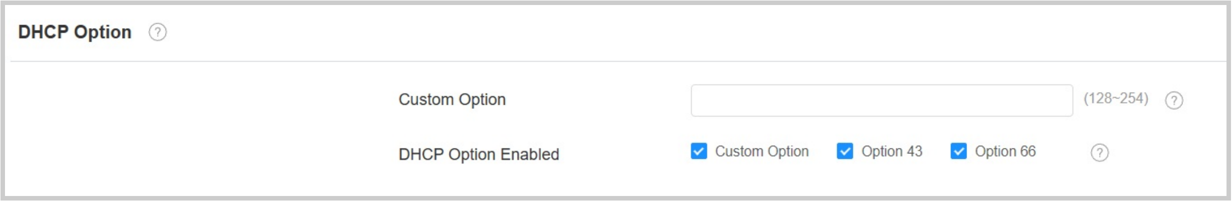
22 (0~23Hour)

0 (0~59Min)

Export Autop Template: Export

Clear MD5: Clear

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


DHCP Option

Custom Option: (128~254)

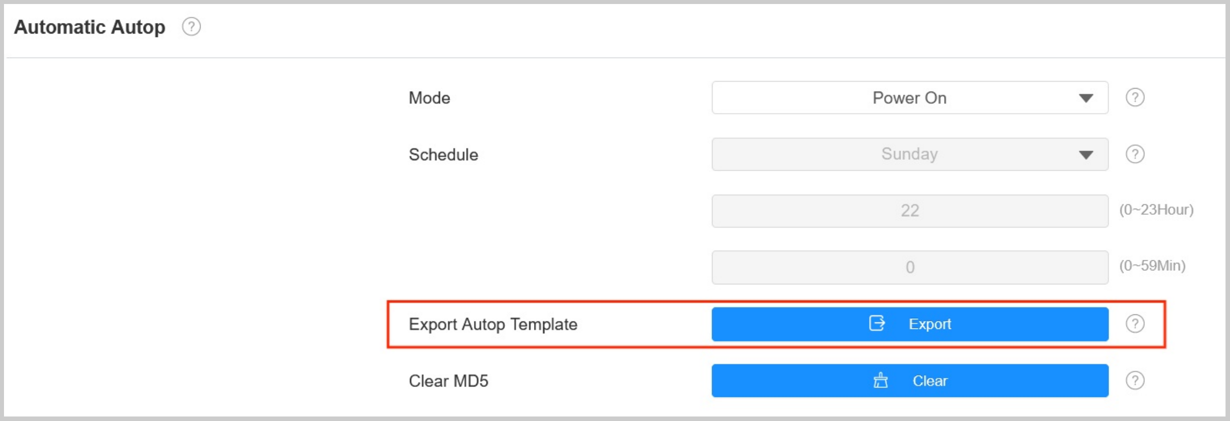
DHCP Option Enabled: ☑ Custom Option ☑ Option 43 ☑ Option 66

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

Static Provisioning Configuration

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

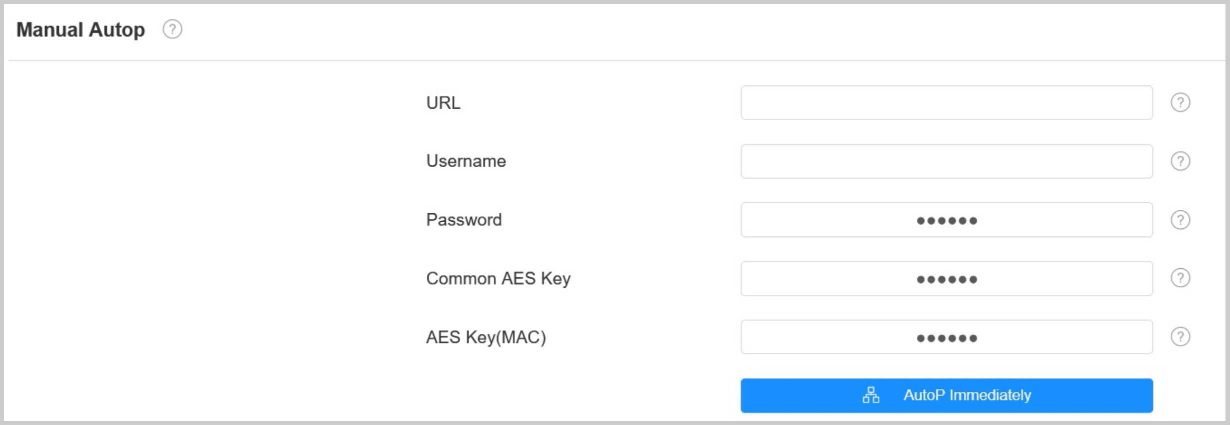
To download the template, go to the **Upgrade > Advanced > Automatic Autop** interface.



Automatic Autop

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

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



Manual Autop

URL	
Username	
Password	••••••
Common AES Key	••••••
AES Key(MAC)	••••••
	AutoP Immediately

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

- **Common AES Key**: It is used for the intercom to decipher general Autop configuration files.
- **AES Key (MAC)**: It is used for the intercom to decipher the MAC-based Autop configuration file.

Note

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

Tip

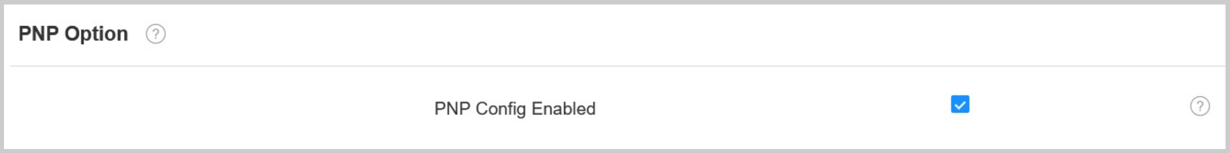
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

Click here to watch the configuration video.

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



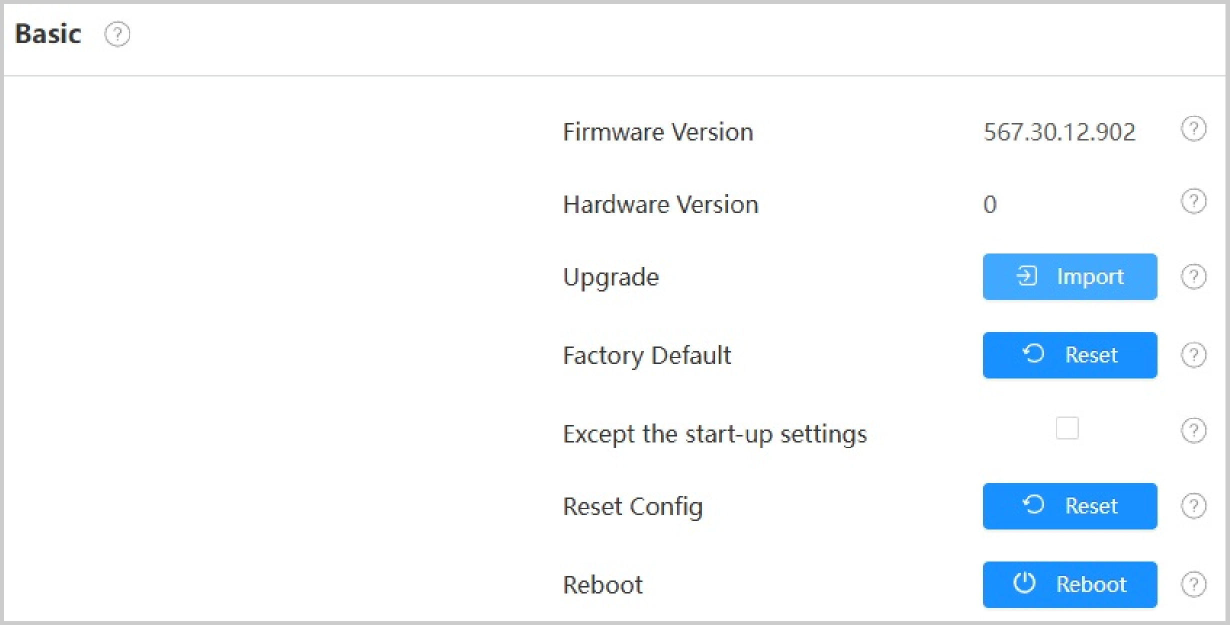
PNP Option

PNP Config Enabled ☑

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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



Basic

Firmware Version 567.30.12.902

Hardware Version 0

Upgrade

Factory Default

Except the start-up settings □

Reset Config

Reboot

Note

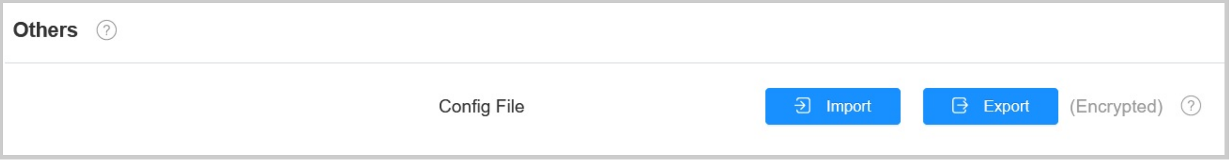
- Firmware files should be **.zip** format for the upgrade.
- Click here to download the latest released firmware and view the new features.

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.

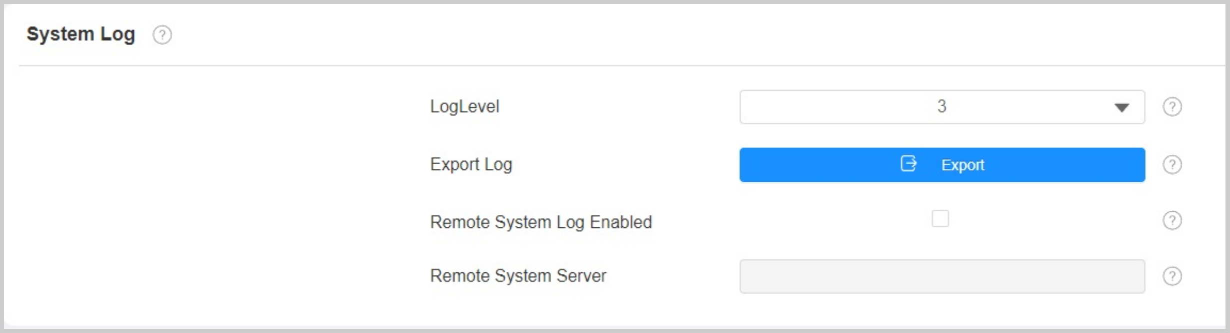


Debug

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.



System Log

LogLevel: 3

Export Log: Export

Remote System Log Enabled: □

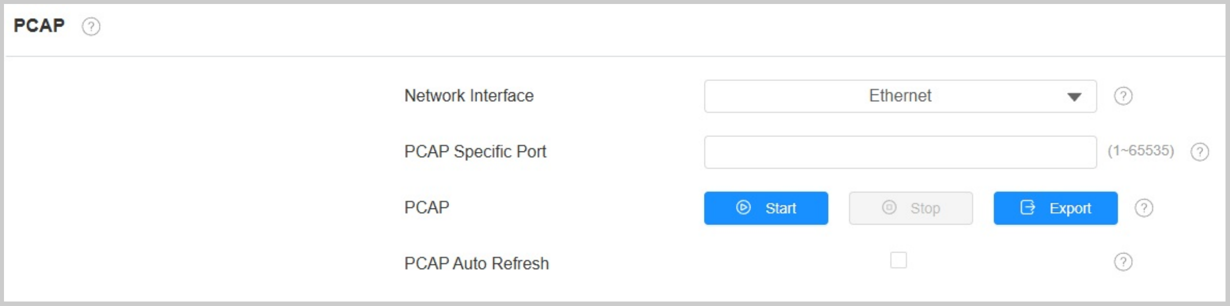
Remote System Server:

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

PCAP for Debugging

PCAP is used to capture the data package going in and out of the devices for debugging and troubleshooting purposes.

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



PCAP

Network Interface: Ethernet

PCAP Specific Port: (1~65535)

PCAP: Start Stop Export

PCAP Auto Refresh: □

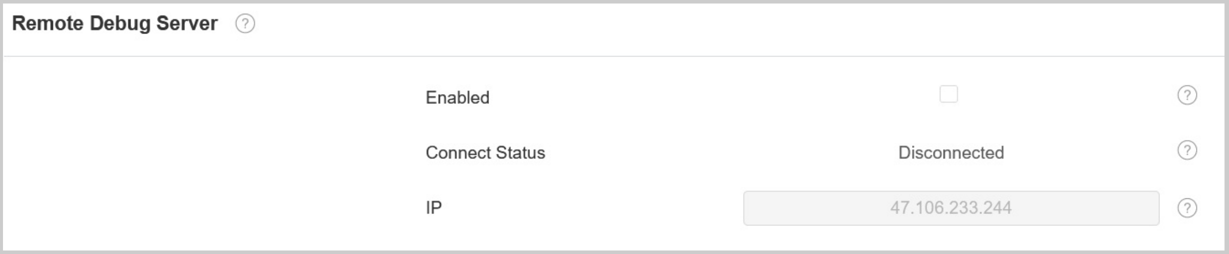
- **Network Interface**: Specify network interface based on the device's network connection.
    - **Ethernet**: The captured data is from the wired network packets.
    - **WLAN**: The captured data is from the wireless network packets.
- **PCAP Specific Port**: Select the specific port from 1-65535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



Remote Debug Server ⓘ

Enabled □

Connect Status: Disconnected

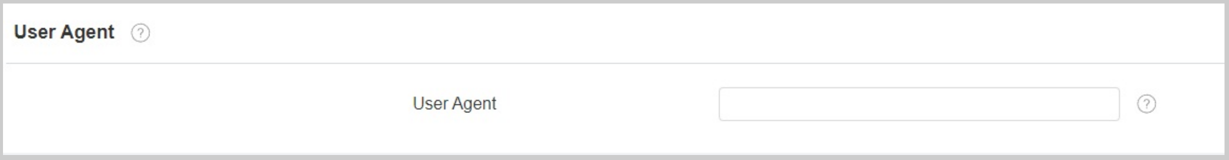
IP: 47.106.233.244

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

User Agent

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

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



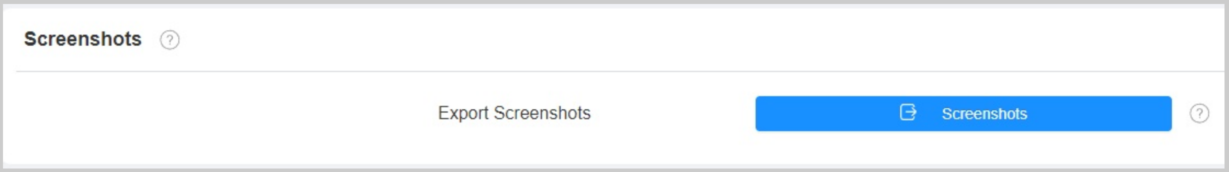
User Agent ⓘ

User Agent:

Screenshots

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

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



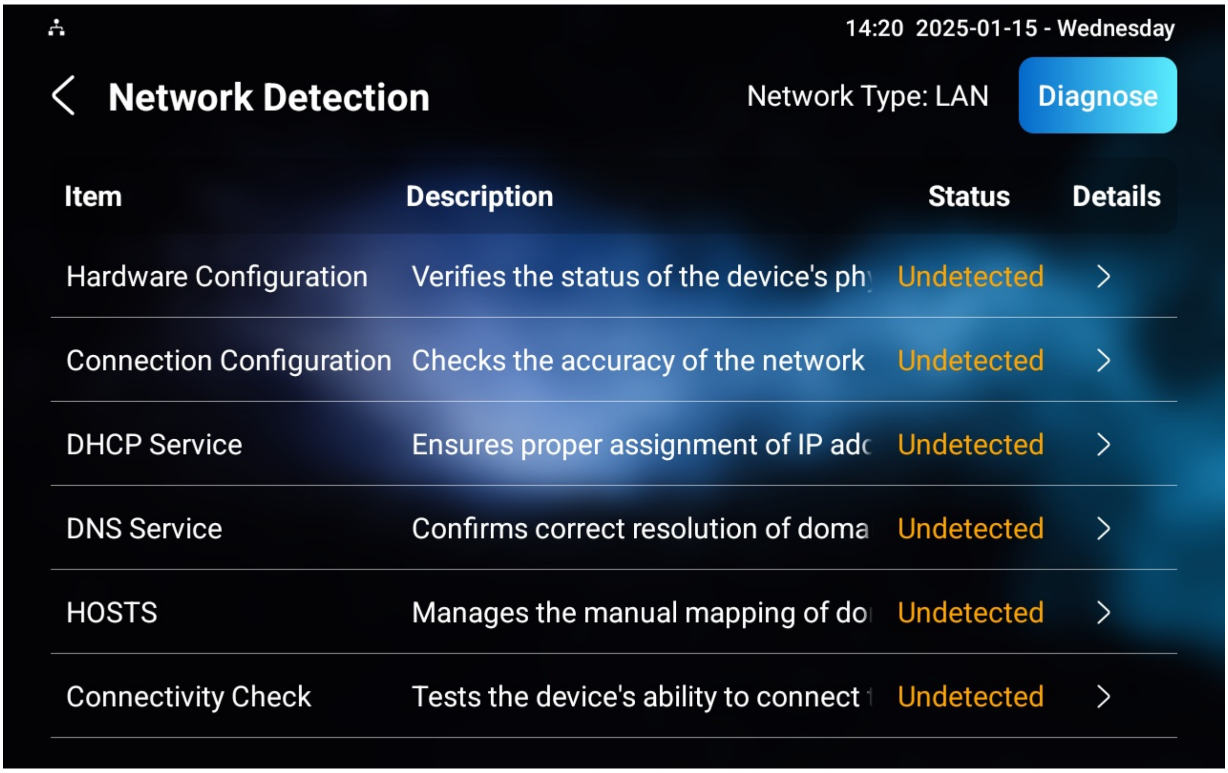
Screenshots ⓘ

Export Screenshots

Network Detection

The network detection feature allows for troubleshooting network problems quickly.

Go to the **Settings > Network Detection** screen.



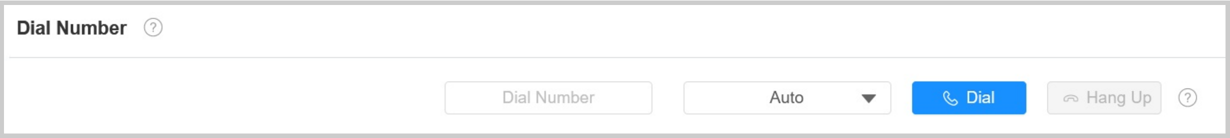
Item	Description	Status	Details
Hardware Configuration	Verifies the status of the device's phy	Undetected	>
Connection Configuration	Checks the accuracy of the network	Undetected	>
DHCP Service	Ensures proper assignment of IP adc	Undetected	>
DNS Service	Confirms correct resolution of doma	Undetected	>
HOSTS	Manages the manual mapping of do	Undetected	>
Connectivity Check	Tests the device's ability to connect t	Undetected	>

- **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.

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.

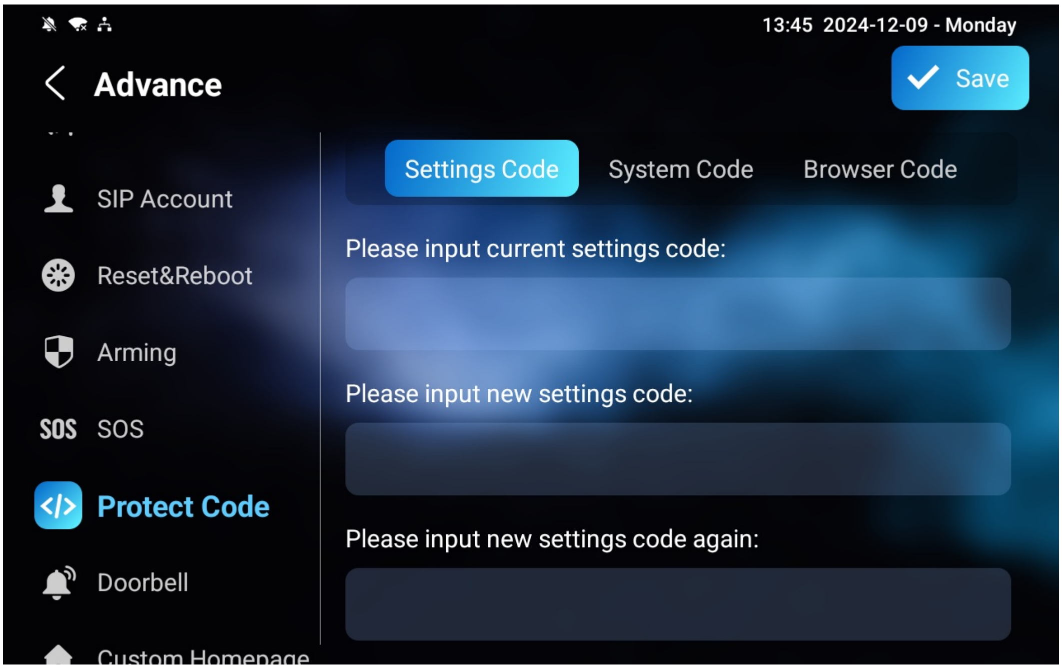


Password Modification

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**.



Please input current settings code:

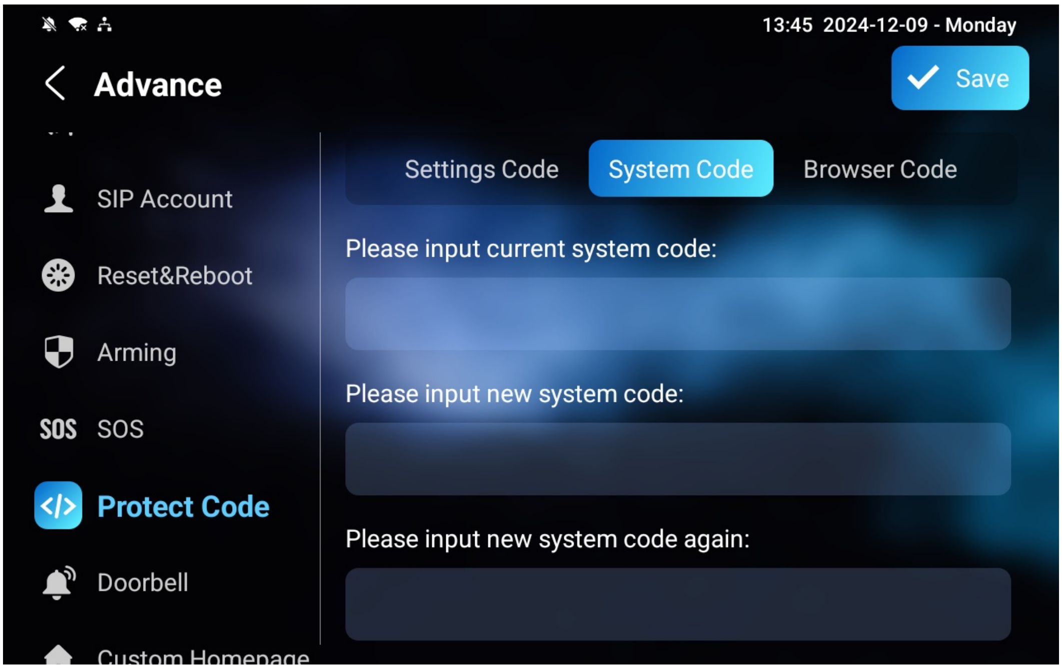
Please input new settings code:

Please input new settings code again:

Modify Device Advance Setting Password

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

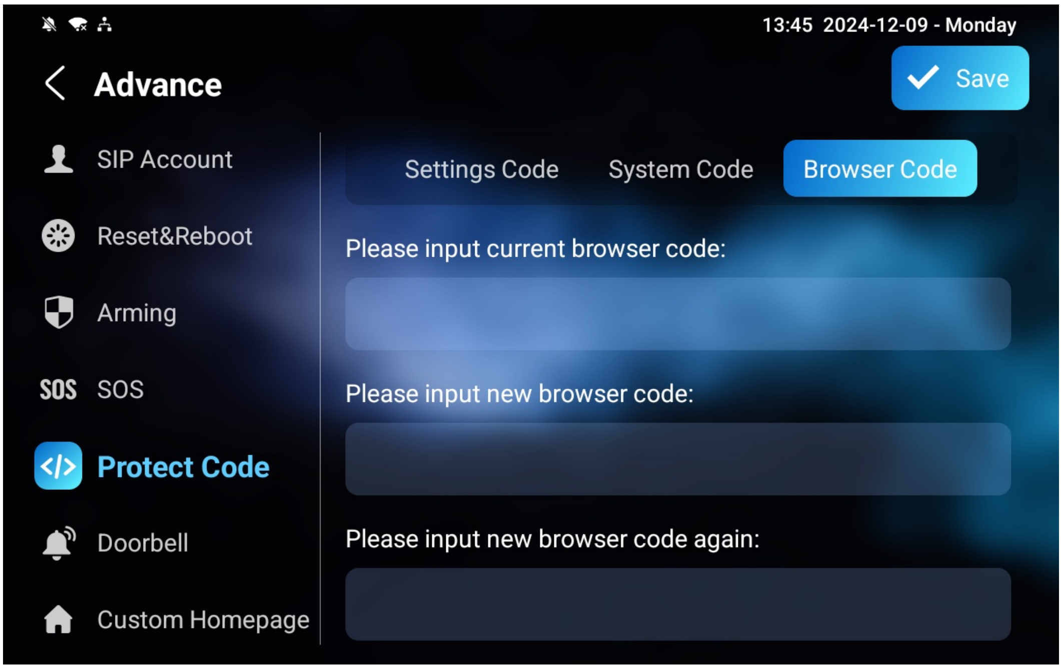
To modify it, navigate to the **Settings > Advance Settings > Protected Code** screen and select **System Code**.


13:45 2024-12-09 - Monday
Advance
Save
SIP Account
Reset&Reboot
Arming
SOS
Protect Code
Doorbell
Custom Homepage
Settings Code
System Code
Browser Code
Please input current system code:
Please input new system code:
Please input new system code again:

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.

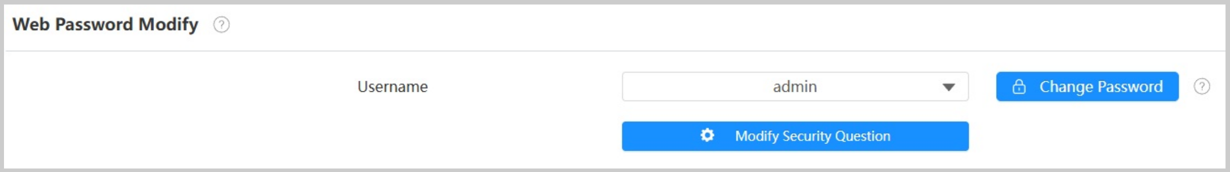
To modify it, go to the **Settings > Advance Settings > Protected Code** screen and select **Browser Code.**


13:45 2024-12-09 - Monday
Advance
Save
SIP Account
Reset&Reboot
Arming
SOS
Protect Code
Doorbell
Custom Homepage
Settings Code
System Code
Browser Code
Please input current browser code:
Please input new browser code:
Please input new browser code again:

Modify Device Web Interface Password

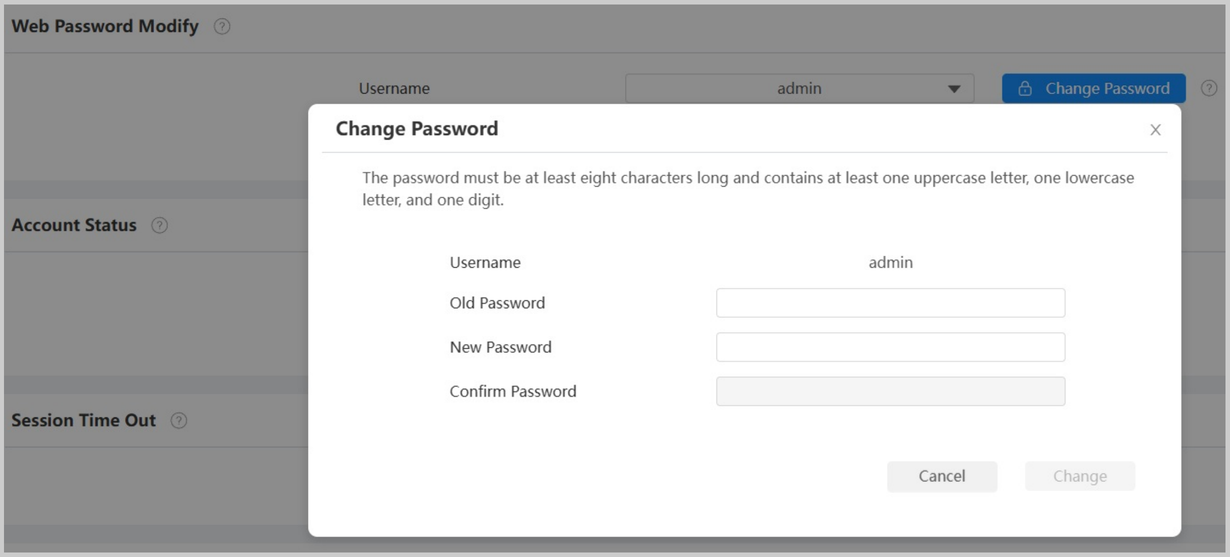
Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.

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



Web Password Modify

Username: admin



Change Password

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

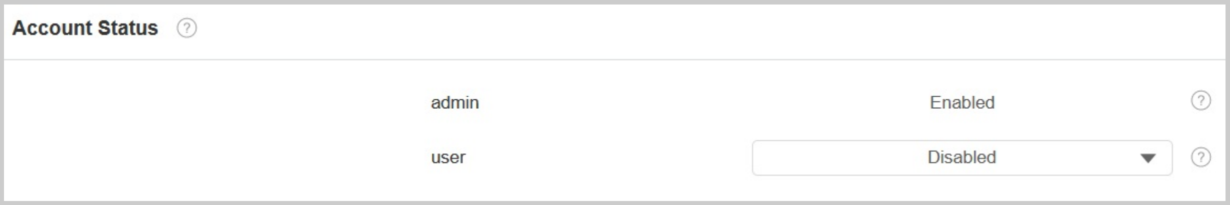
Username: admin

Old Password:

New Password:

Confirm Password:

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



Account Status

admin	Enabled
user	Disabled

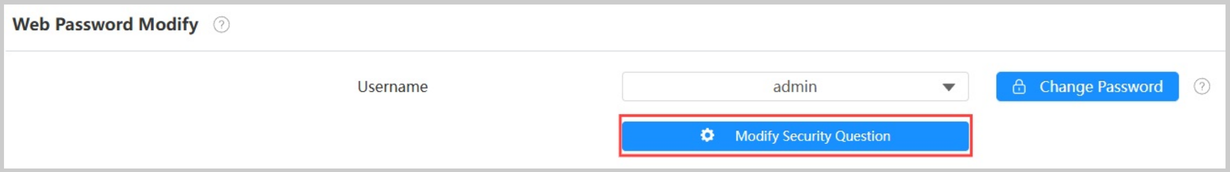
> **Note**
>
> There are two accounts, one is admin, its password is admin, the other is user, and its password is user.

Modify Security Questions

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

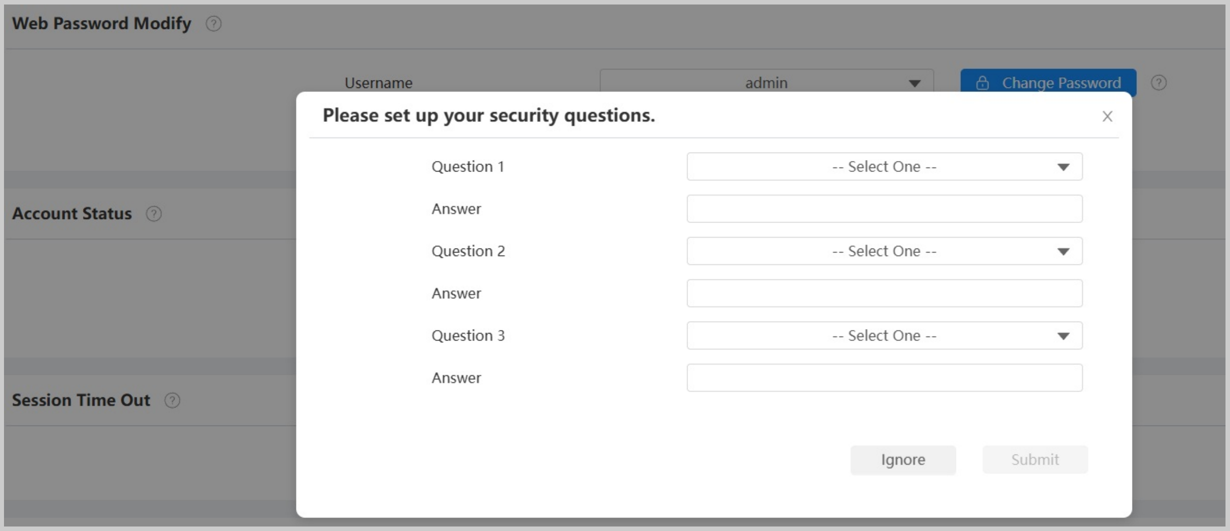
If you do not set up the security questions, clicking "Answer security questions" will prompt you to "Please contact your service provider".

Set it up on the **Security > Basic > Web Password Modify** interface.



Web Password Modify

Username: admin



Please set up your security questions.

Question 1: -- Select One --

Answer:

Question 2: -- Select One --

Answer:

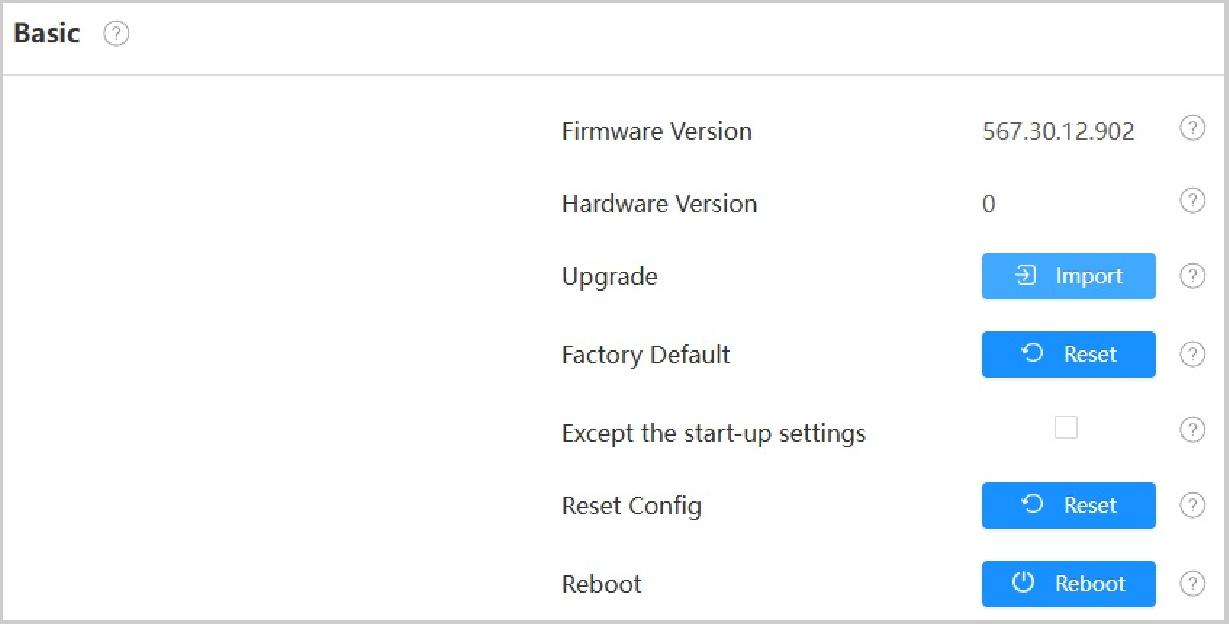
Question 3: -- Select One --

Answer:

System Reboot & Reset

Reboot

You can reboot the device on its **Settings > Advance > Reset&Reboot** screen. Or, go to the **Upgrade > Basic** interface.



Basic

Firmware Version: 567.30.12.902

Hardware Version: 0

Upgrade

Factory Default

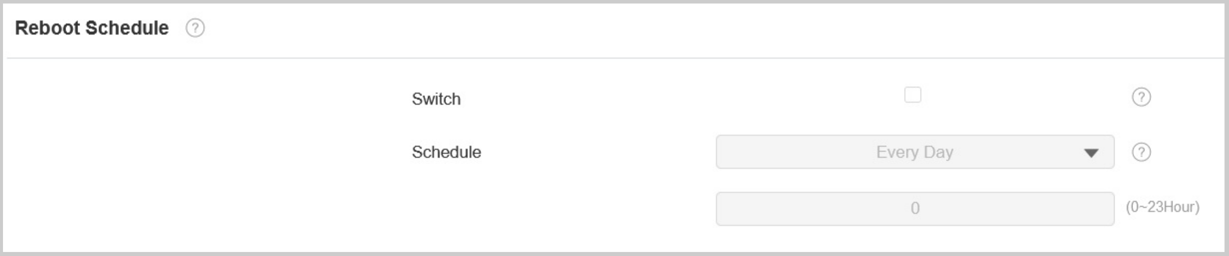
Except the start-up settings: □

Reset Config

Reboot

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

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



Reboot Schedule

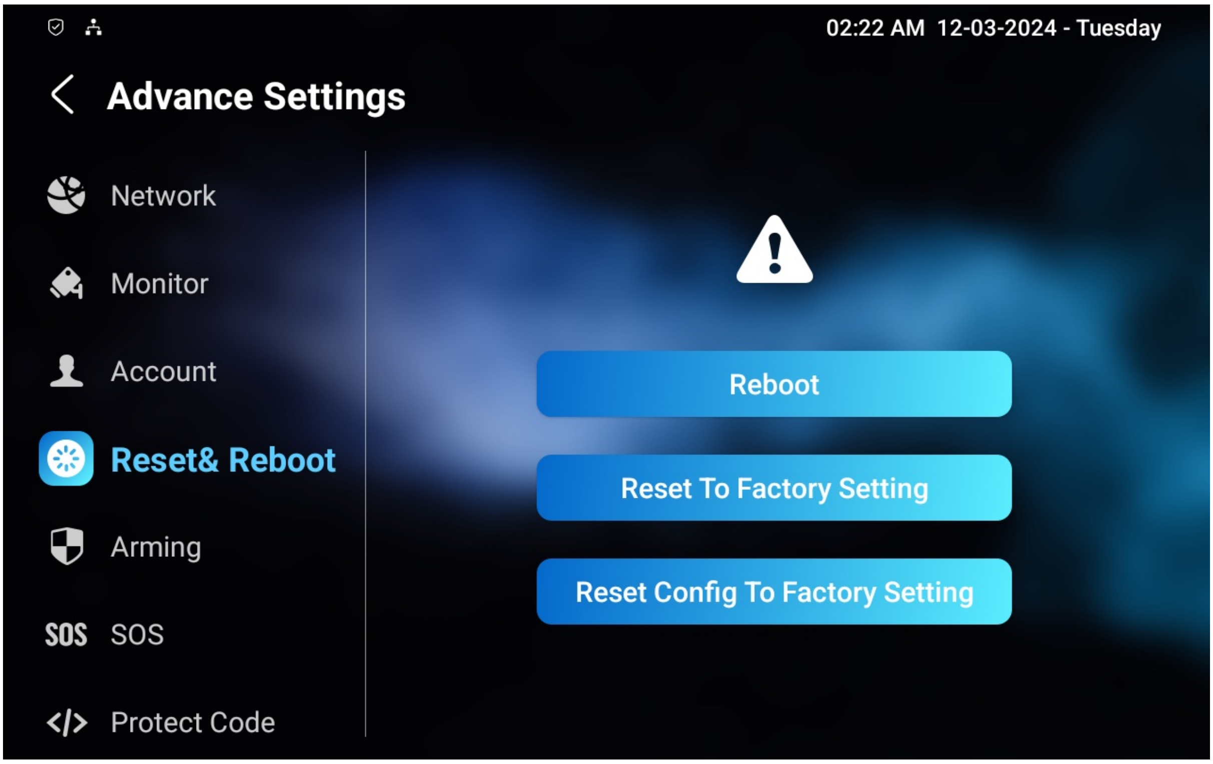
Switch: □

Schedule: Every Day

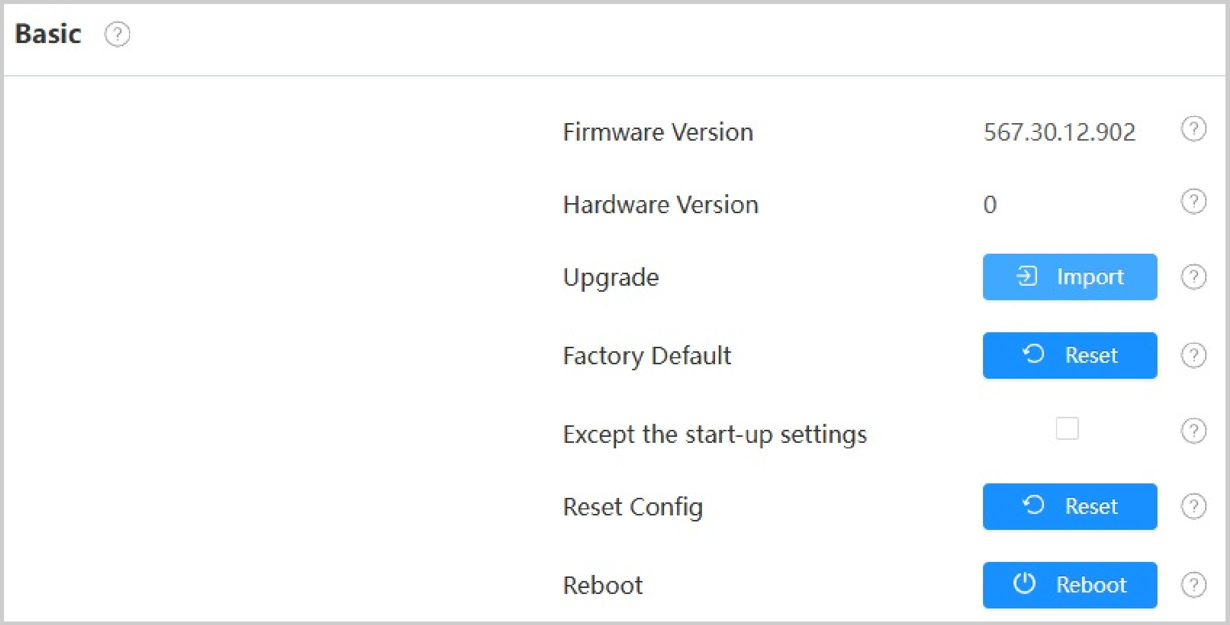
0 (0~23Hour)

Reset

You can reset the device on its **Settings > Advance > Reset&Reboot** screen. Or, go to the **Upgrade > Basic** interface.



- **Reset to Factory Setting**: Reset all data to the factory default.
- **Reset Config to Factory Setting**: Retain the user data such as contacts.



Basic

Firmware Version	567.30.12.902
Hardware Version	0
Upgrade	Import
Factory Default	Reset
Except the start-up settings	□
Reset Config	Reset
Reboot	Reboot

- **Factory Default**: Reset all data to the factory default.
- **Except the start-up settings**: Check to retain the initial settings such as network and time zone.
- **Reset Config**: Retain the user data such as contacts.