About This Manual

Akuvox
Open A Smart World

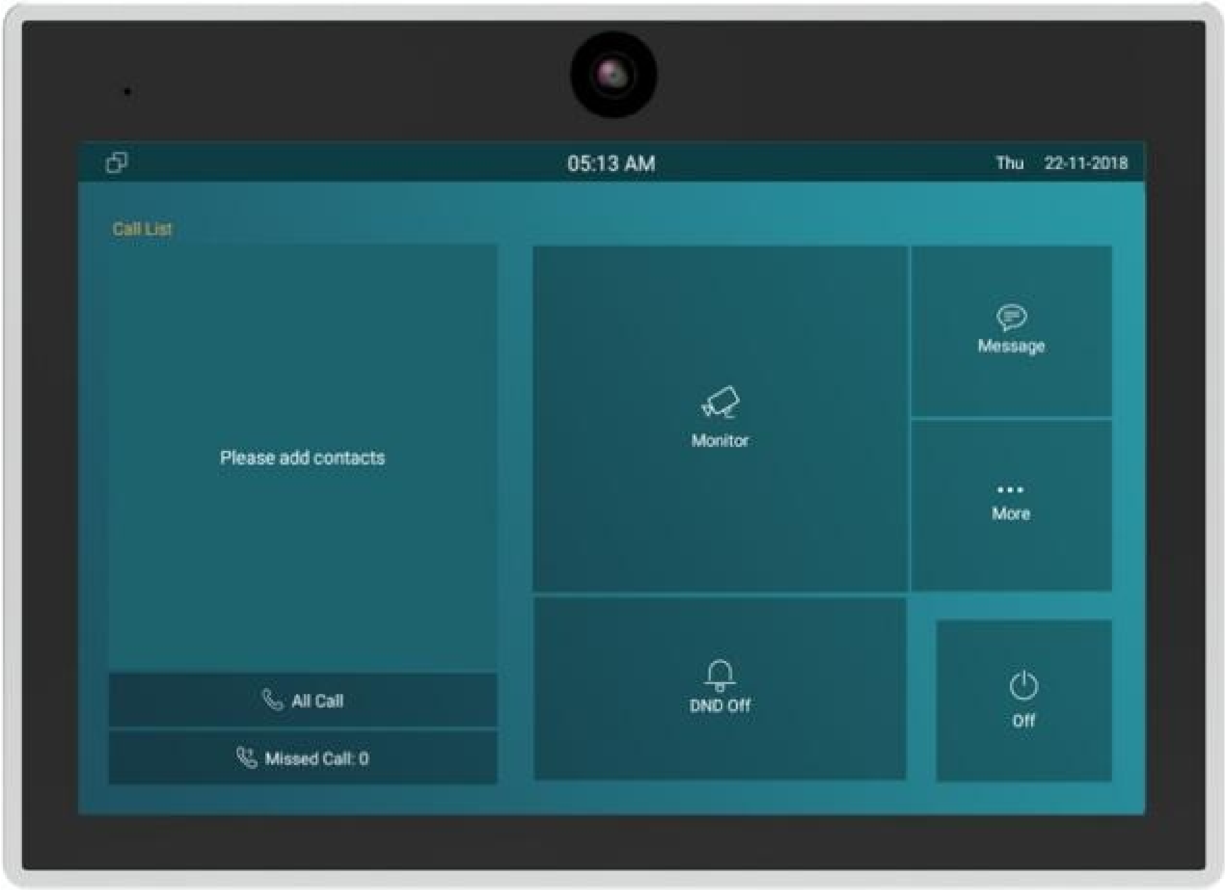
WWW.AKUVOX.COM

C315 SERIES INDOOR MONITOR

Admin Guide

Thank you for choosing the Akuvox C315 series indoor monitor. This manual is intended for the administrators who need to properly configure the indoor monitor. This manual applies to the 115.30.10.4 version, and it provides all the configurations for the functions and features of the C315 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview



C315 series is an Android SIP-based indoor monitor with a smooth touch-screen. It can be connected with the Akuvox door phone for audio/video communication, unlocking, and monitoring. Residents can communicate with visitors via audio/video call, 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. C315 series is often applied to scenarios such as villas, apartments, and buildings.

Change Log

Add High Security Mode.

Model Specification

Model	C315X
Feature	
Housing Material	Plastics
OS	Android 6
Display	7 inch (176 mm) diagonal
Resolution	1024*600
Wi-Fi	IEEE802.11b/g/n, @2.4GHz Optional
Bluetooth	X
Ethernet	2xRJ45, 10/100Mbps adaptive
Power Supply	12V DC connector
POE	802.3af Power-over-Ethernet
Alarm Input	8
Relay Output	1

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, etc.

Network: this section mainly deals with DHCP & Static IP setting, RTP port setting, device deployment, etc.

Phone: this section includes time, language, call feature, display setting, audio, multicast, relay, third-party app, intercom, monitor, Smart Living, web view, etc.

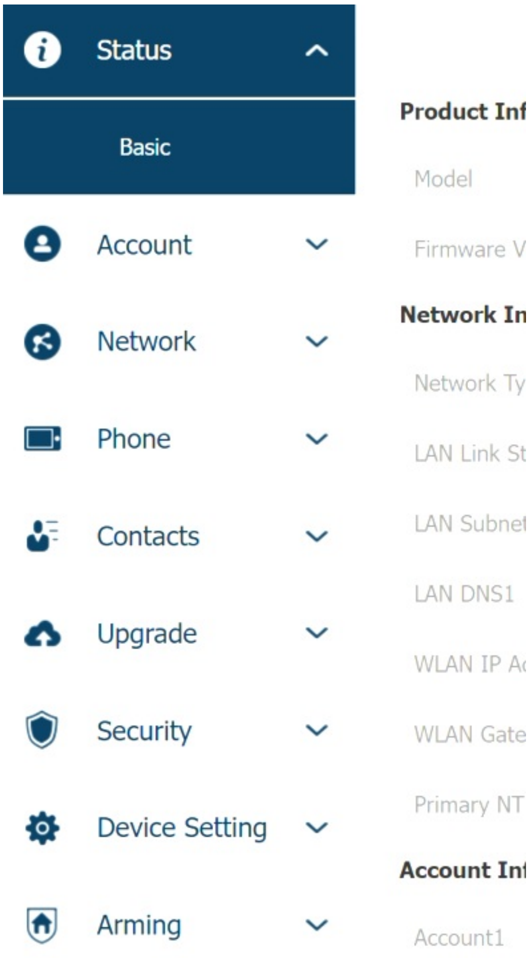
Contacts: this section allows the user to configure the local contact list stored on the device.

Upgrade: this section covers firmware upgrade, device reset & reboot, configuration file auto-provisioning, and PCAP.

Security: this section is for password modification, account status & session time-out configuration, client certificate, as well as service location, etc.

Device Setting: this section includes the RTSP setting, and power output setting.

Arming: this section covers the configuration including arming zone setting, arming mode, disarm code, and alarm action.

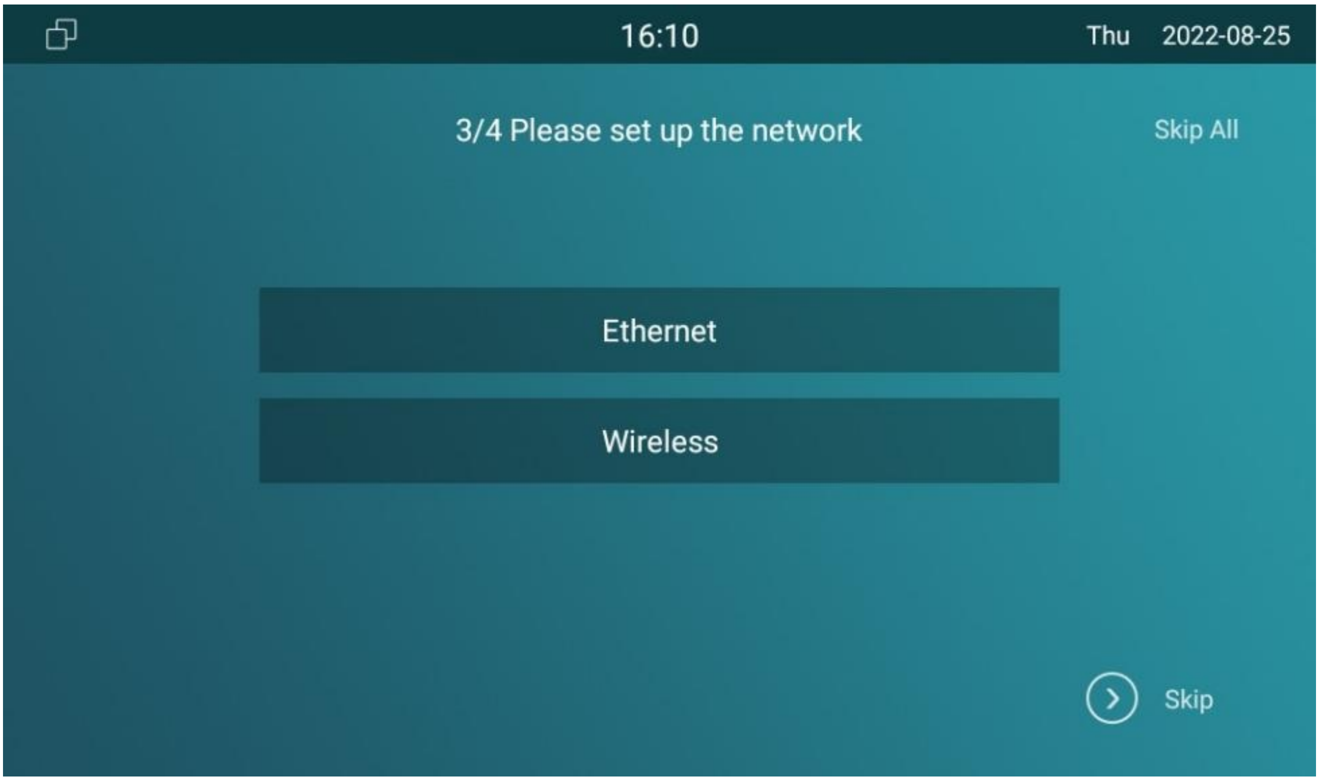

Status
Basic
Account
Network
Phone
Contacts
Upgrade
Security
Device Setting
Arming
Product Inf
Model
Firmware V
Network In
Network Ty
LAN Link St
LAN Subnet
LAN DNS1
WLAN IP Ad
WLAN Gate
Primary NT
Account Inf
Account1

Access the Device

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

Device Start-up Network Selection

Akuvox indoor monitor system settings can be either accessed on the device directly or on the device's web interface. After the device boots up initially, you are required to select the network connection for the device. You can either select Ethernet or wireless network connection according to your need.

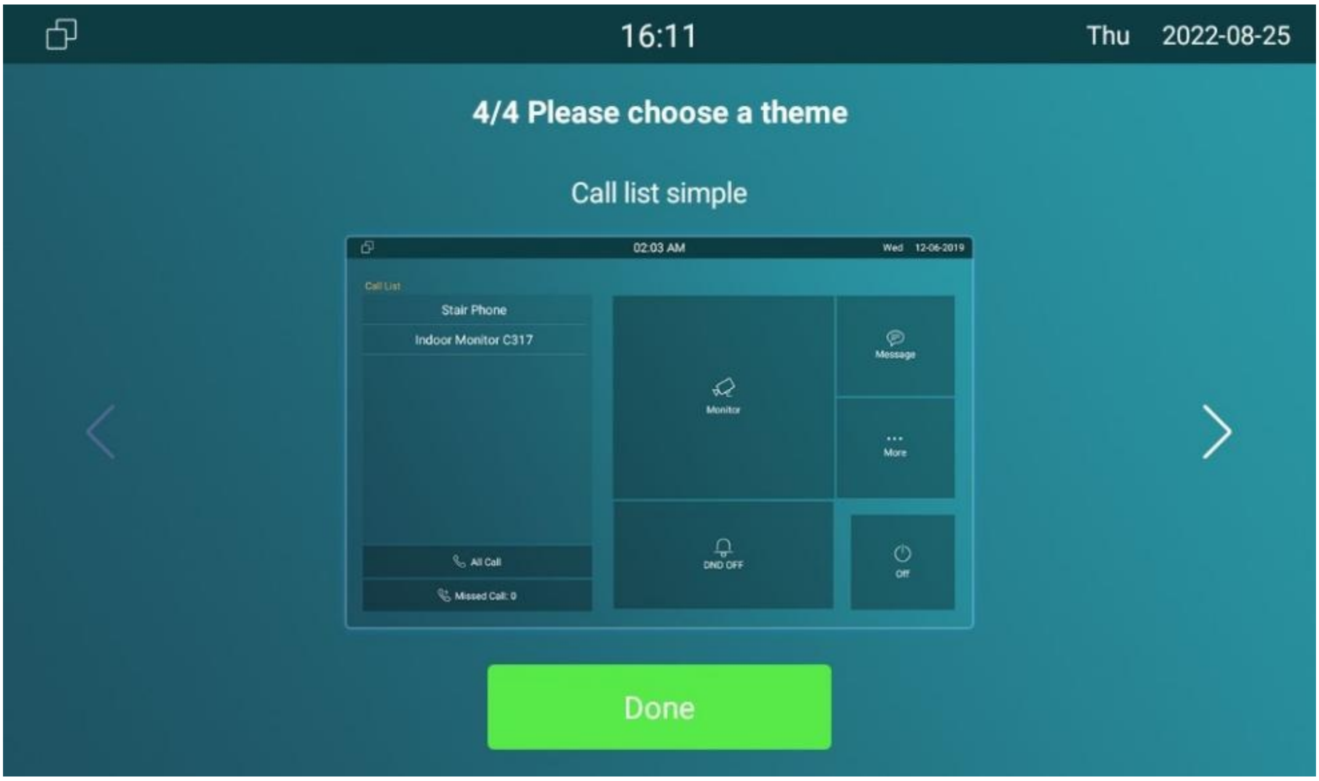


Note

- Please refer to the chapter on **Network Setting & Other Connection** for the configuration of the Ethernet and wireless network connection.

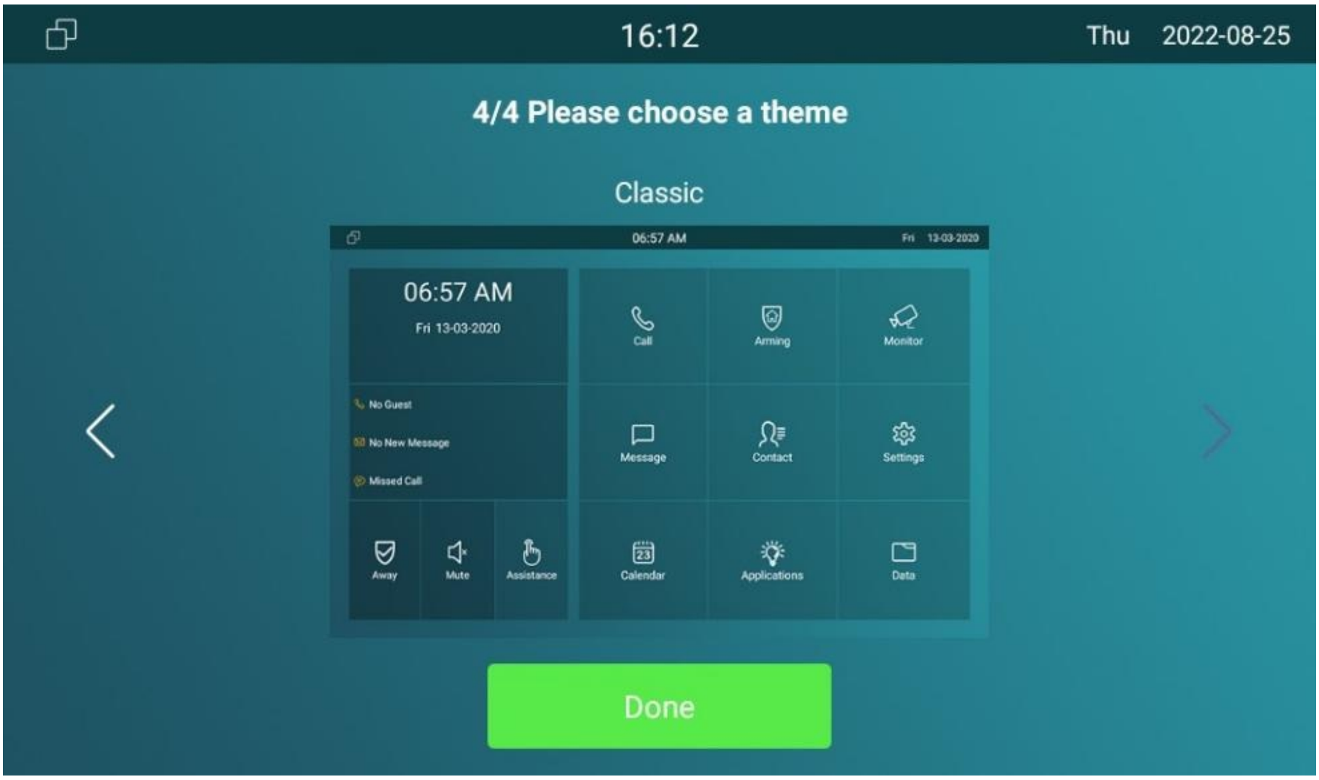
Device Home Screen Type Selection

Akuvox indoor monitor supports two different home screen display modes: **Call list simple, Classic.** Choose one suitable mode for your scenarios.



4/4 Please choose a theme

Call list simple



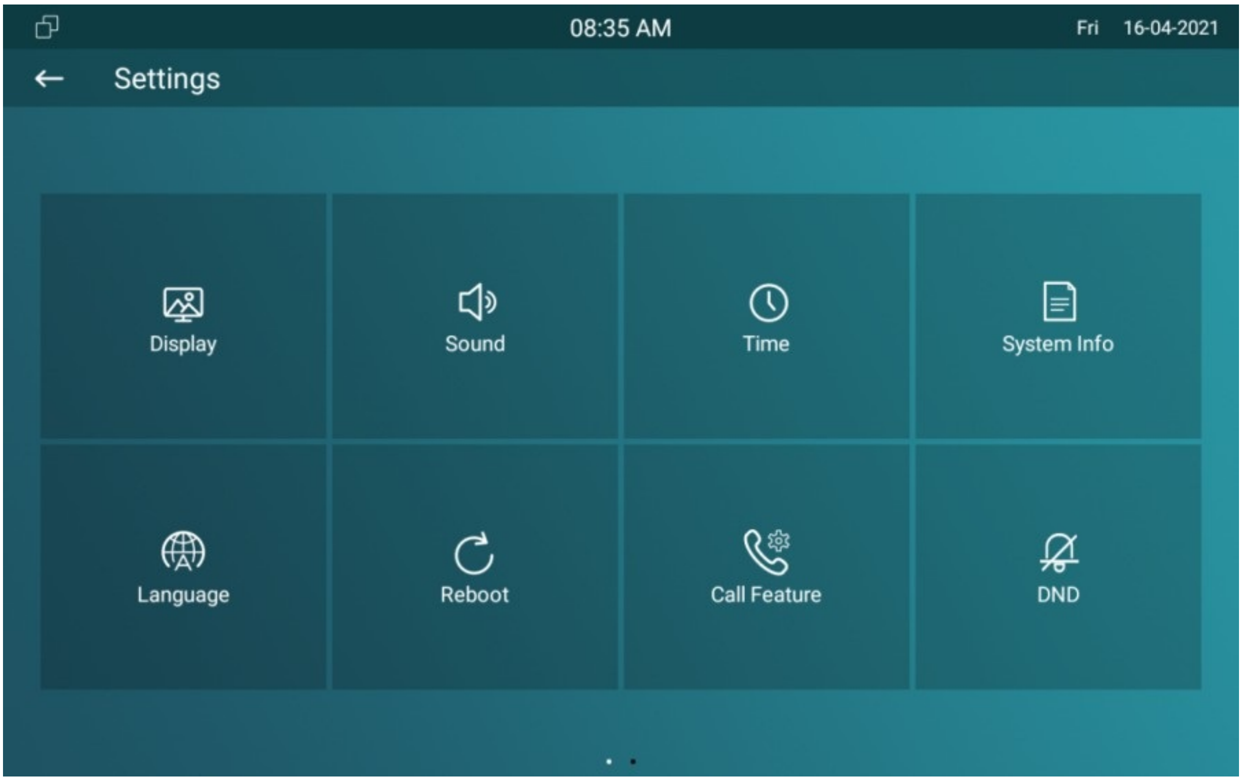
4/4 Please choose a theme

Classic

Access the Device Setting on the Device

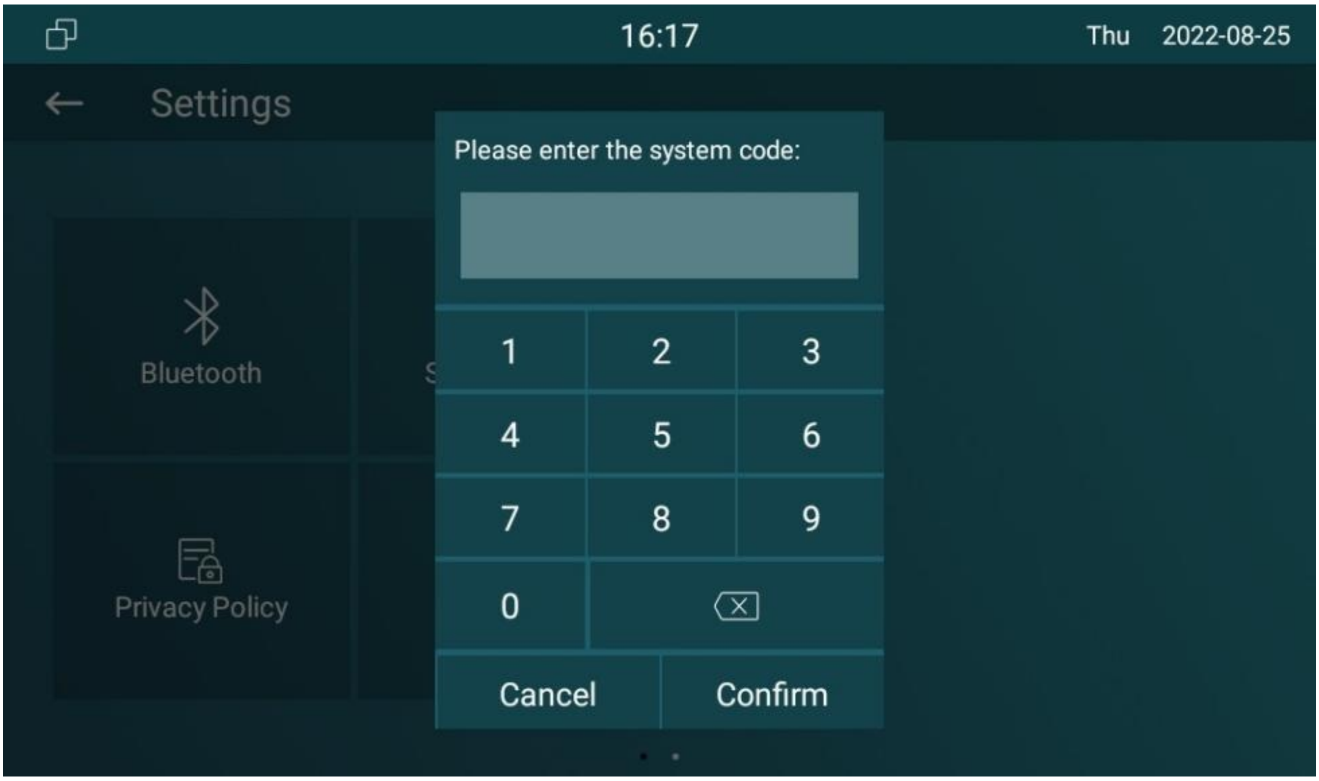
Access Device Basic Setting

You can access the device's basic setting and advance setting where you can configure different types of functions as needed. To access the device's basic setting by pressing **More > Settings.**



Access Device Advance Settings

To access the advance settings, press **Settings** and then **More.** Press password **123456** (by default) to enter the advance settings.

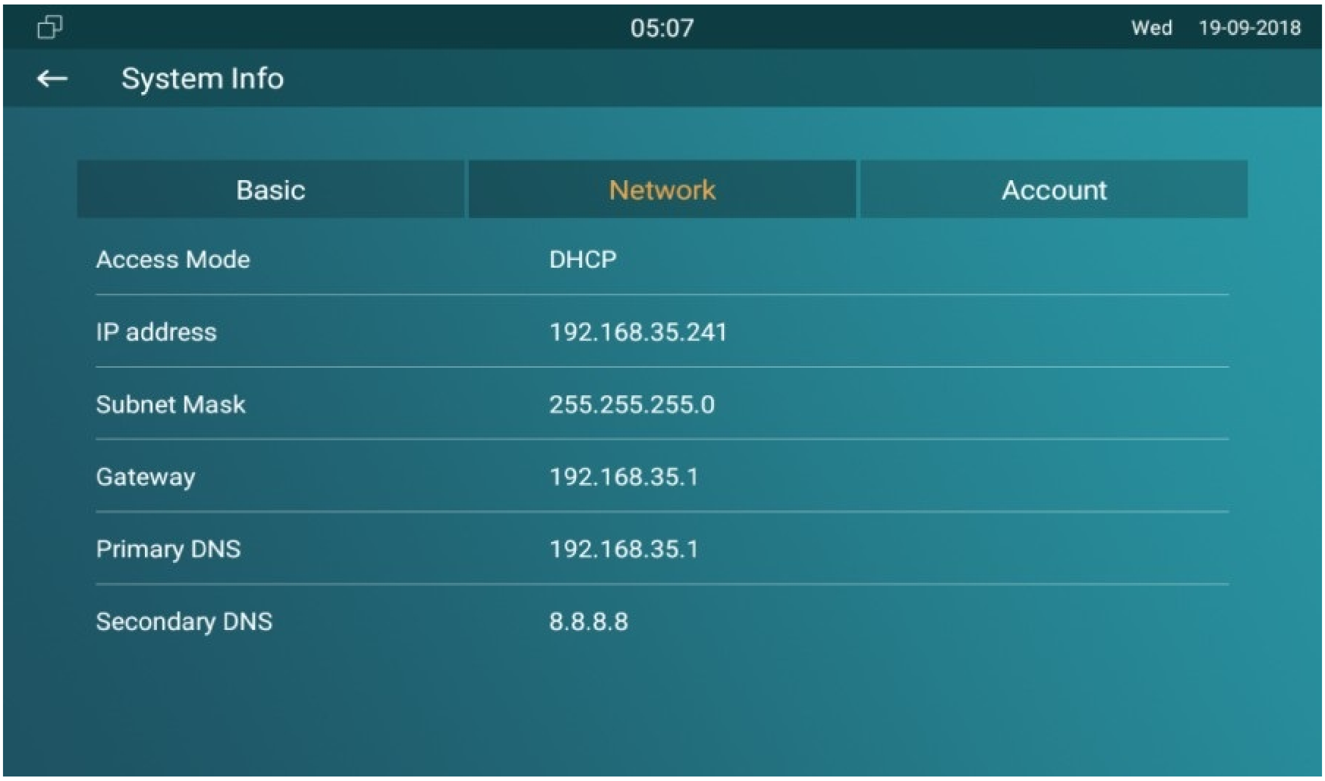


Please enter the system code:

Access the Device Setting on the Web Interface

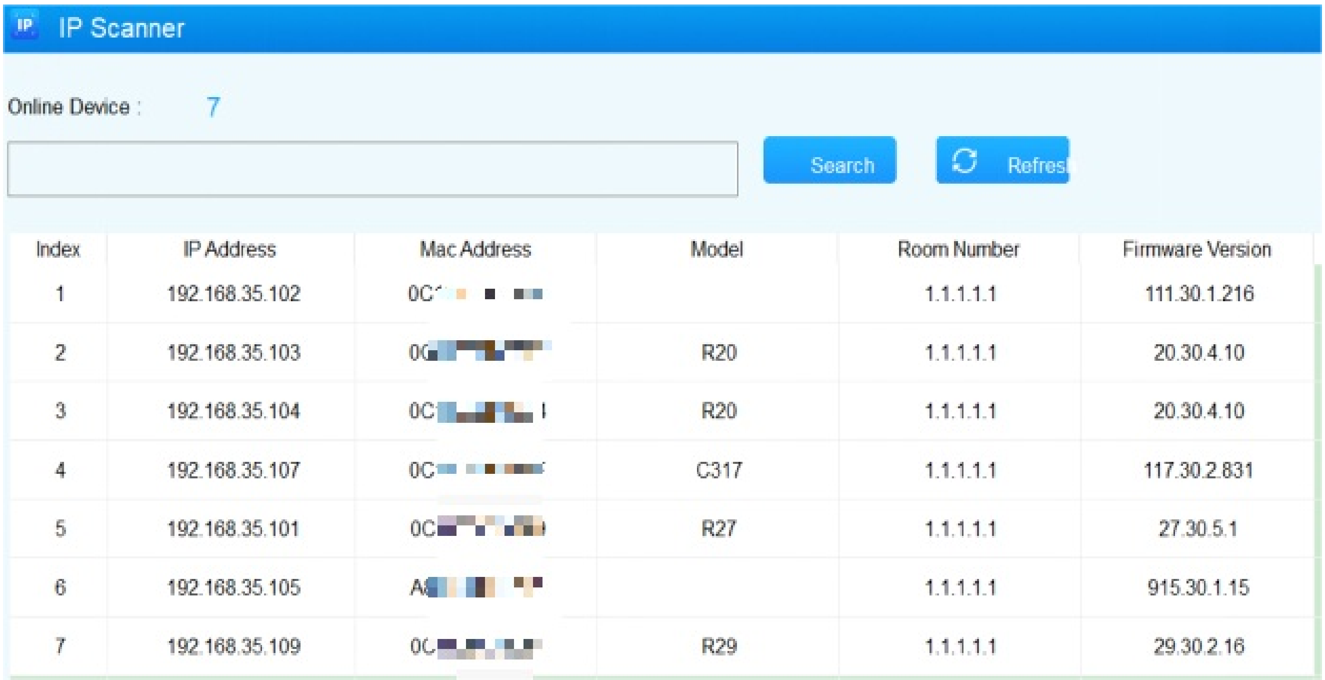
You can also enter the device IP address on the web browser in order to log in to the device web interface where you can configure and adjust parameters, etc.

You can check device IP on device **Settings** > **System Info** > **Network** screen. Or searching by IP scanner tool in the same LAN with the device.



System Info

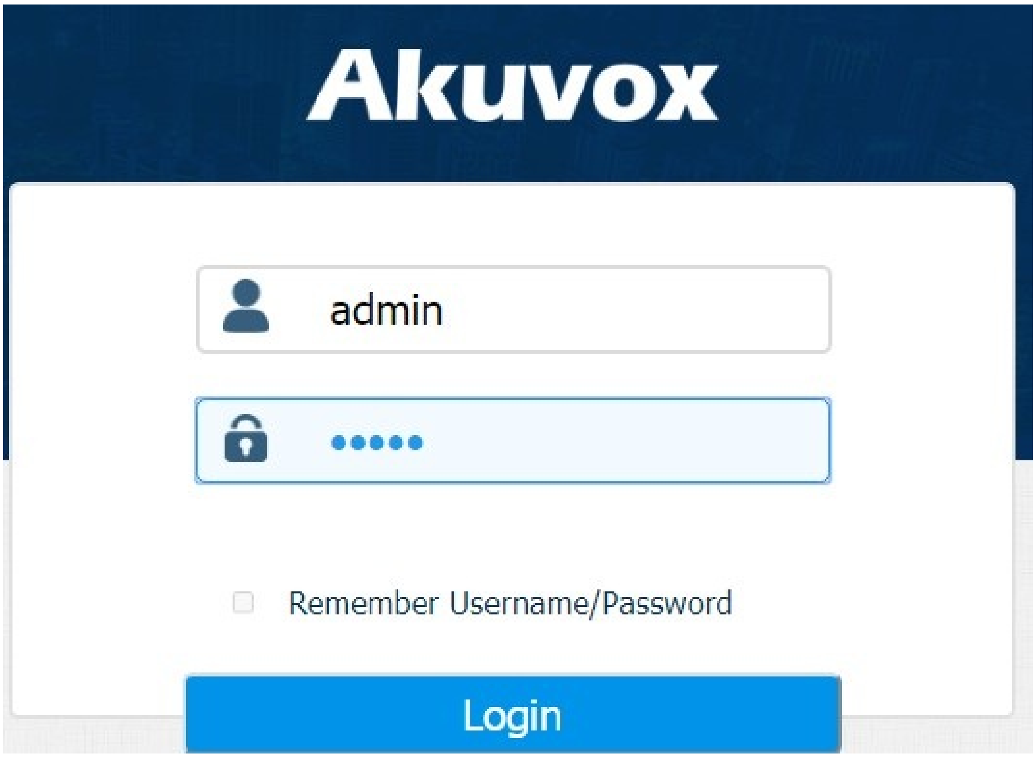
Access Mode	DHCP
IP address	192.168.35.241
Subnet Mask	255.255.255.0
Gateway	192.168.35.1
Primary DNS	192.168.35.1
Secondary DNS	8.8.8.8



IP Scanner

Online Device : 7

Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C[redacted]		1.1.1.1.1	111.30.1.216
2	192.168.35.103	0[redacted]	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C[redacted]	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C[redacted]	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C[redacted]	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A[redacted]		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C[redacted]	R29	1.1.1.1.1	29.30.2.16



Note

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

Language and Time Setting

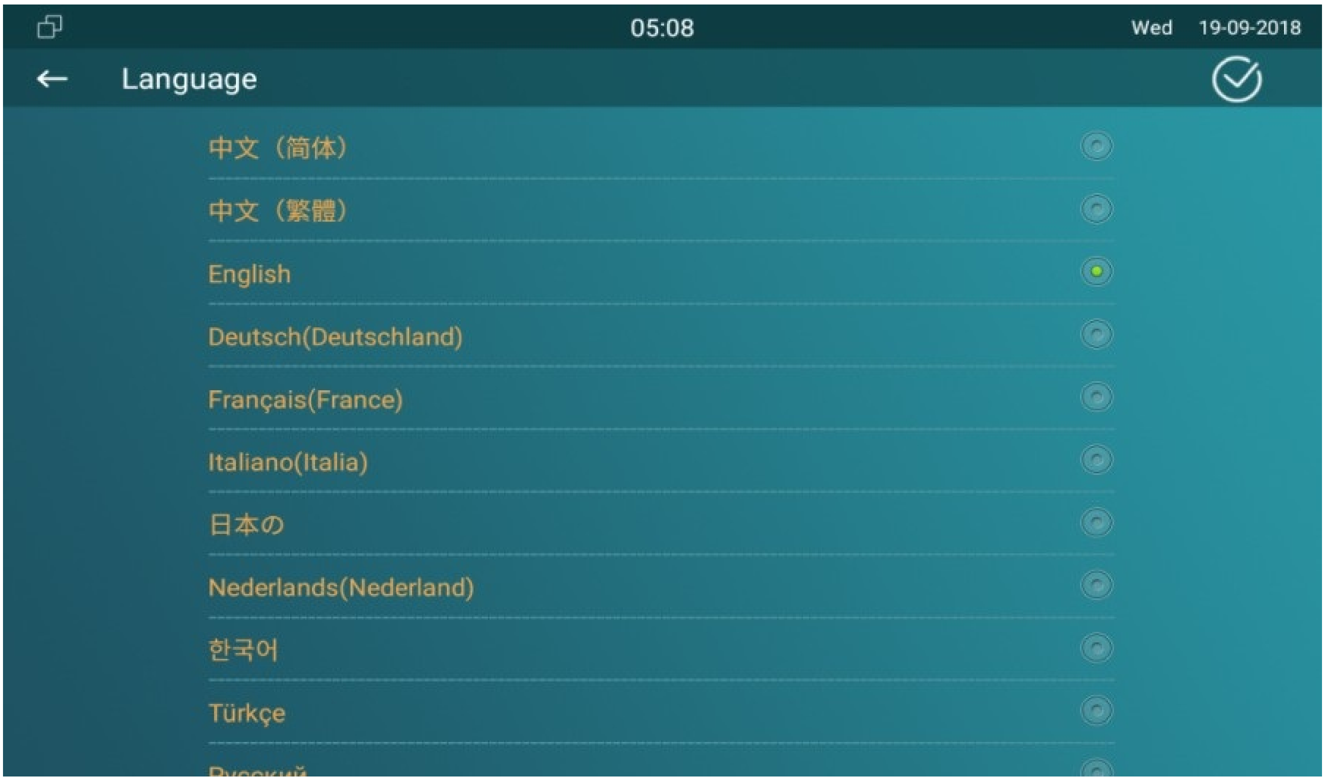
When you first set up the device, you might need to set the language to your need or you can do it later if needed. And the language can either be set up directly on the device or on the device web interface according to your preference.

Language Setting

Language Setting on the Device

To configure the language display on the device **Settings** > **Language** screen. The device supports the following languages:

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



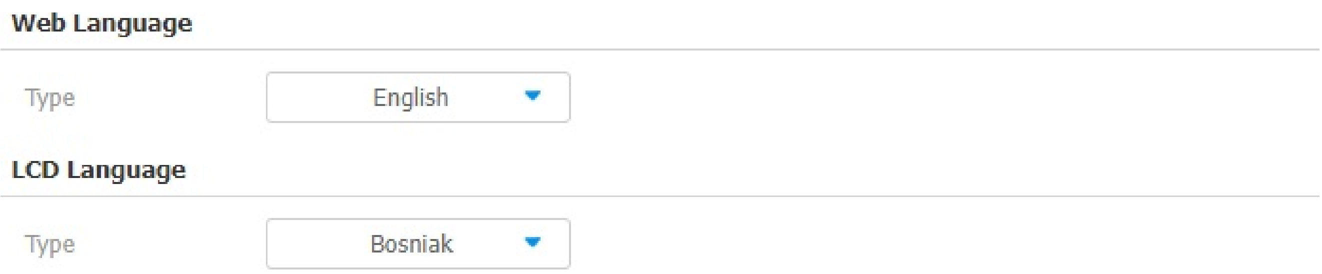
05:08 Wed 19-09-2018

← Language ✓

中文（简体） ○
中文（繁體） ○
English ●
Deutsch(Deutschland) ○
Français(France) ○
Italiano(Italia) ○
日本の ○
Nederlands(Nederland) ○
한국어 ○
Türkçe ○
Русский ○

Language Setting on the Web Interface

To configure the language display on the device web **Phone** > **Time/Lang** interface.



Web Language

Type: English

LCD Language

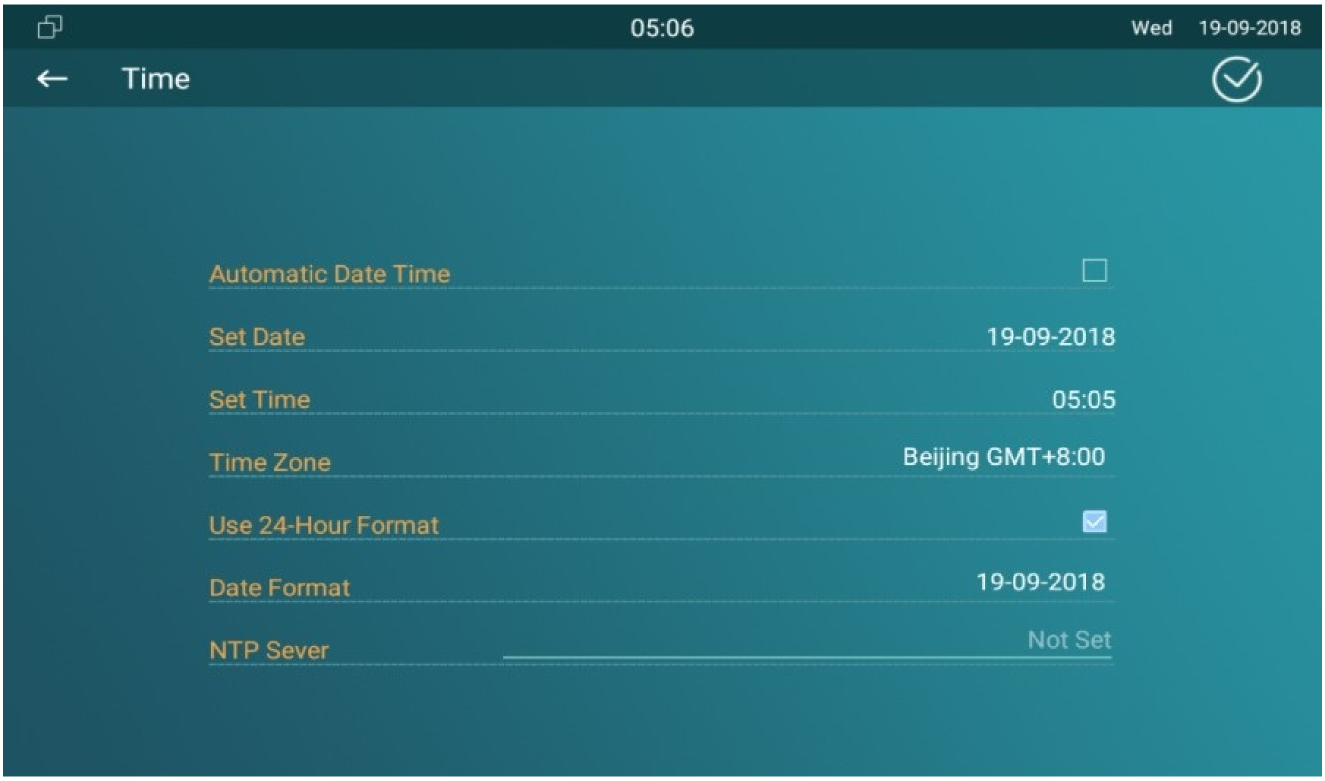
Type: Bosniak

Time Setting

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

Time Setting on the Device

To set up time setting on the device **Settings > Time** screen.



05:06 Wed 19-09-2018

Time

Automatic Date Time □

Set Date 19-09-2018

Set Time 05:05

Time Zone Beijing GMT+8:00

Use 24-Hour Format ☑

Date Format 19-09-2018

NTP Sever Not Set

Parameter Set-up:

- **Automatic Date Time**: NTP-based automatic date time is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**). You can also set it up manually by unchecking the box and then entering the time and date you want and pressing the **Save** tab to save the setting.

- **Set Date**: enter the date when it is in manual mode.
- **Set Time**: enter the time when it is in manual mode.
- **Use 24-Hour Format**: tick the checkbox to select 24-hour time format.
- **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 as you like among options: **Y-M-D, Y/M/D, D-M-Y, D/M/Y, M-D-Y, M/D/Y.**
- **Time Format**: select 12-hour or 24-hour time format as you like.
- **NTP Server**: enter the NTP server you obtained in the NTP server field.

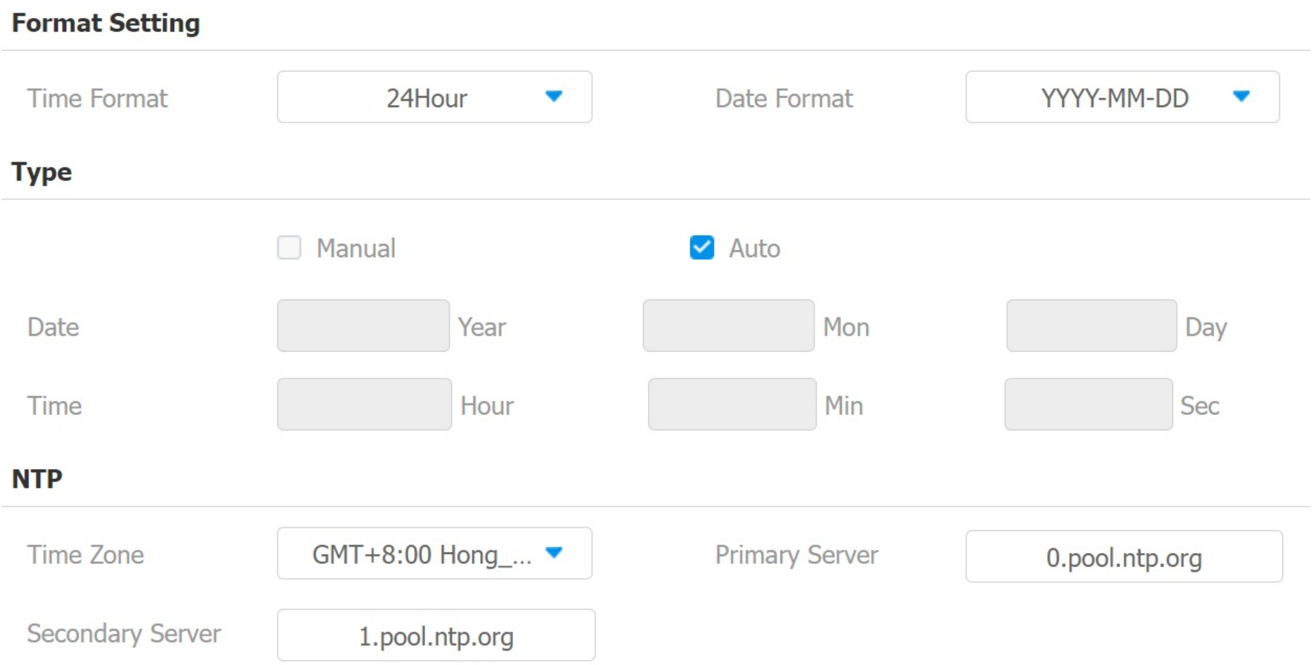
Note

- When the **NTP-based automatic date and time** is switched off, then parameters related to NTP server will become non-editable. And when it is switched on, then time and date will be denied editing.

Time Setting on the Device Web Interface

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

To set it up on the device **Phone > Time/Lang** interface.



Format Setting

Time Format	24Hour ▼	Date Format	YYYY-MM-DD ▼

Type

□ Manual ☑ Auto

Date		Year		Mon		Day
Time		Hour		Min		Sec

NTP

Time Zone	GMT+8:00 Hong_... ▼	Primary Server	0.pool.ntp.org
Secondary Server	1.pool.ntp.org		

Parameter Set-up:

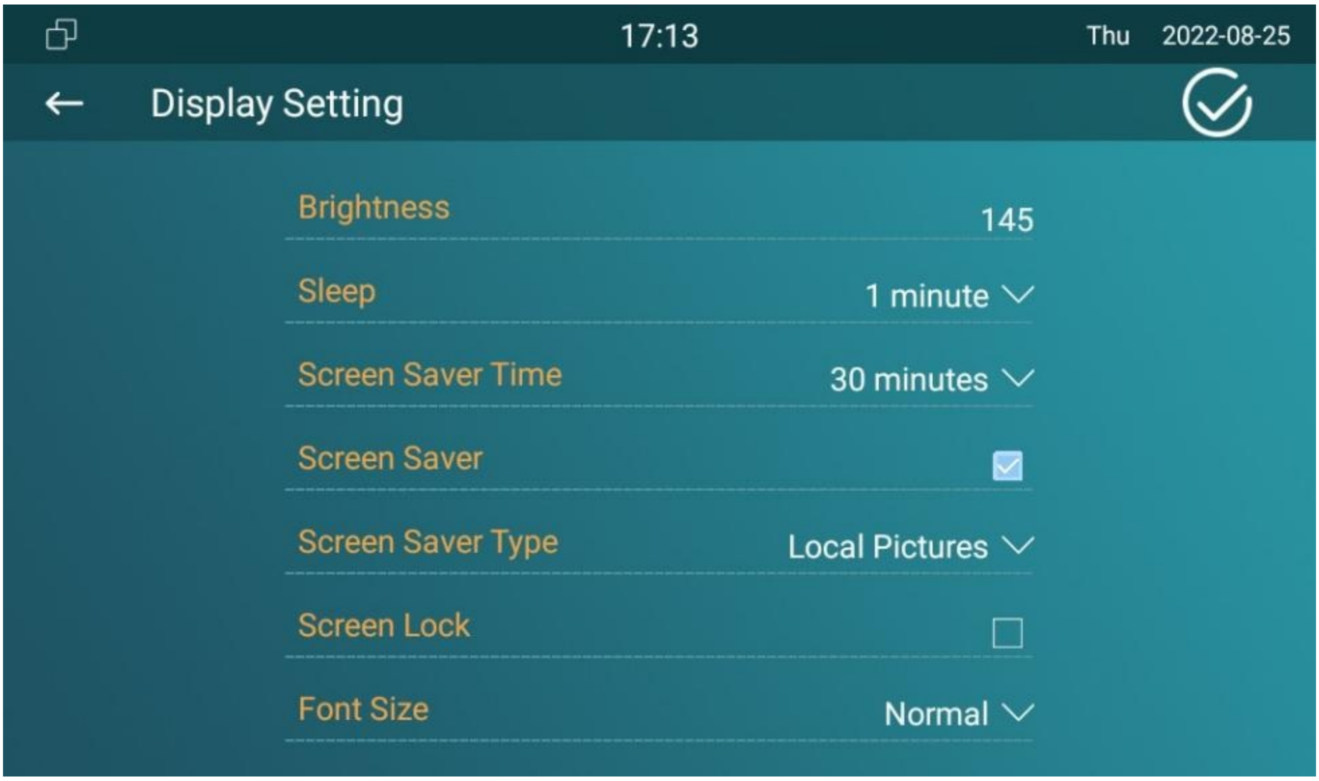
- **Preferred Server**: enter the NTP server address you obtained.
- **Secondary Server**: enter the back up server address. When the main NTP server failed, it will change to the back up server automatically.

Screen Display Setting

Screen Display Setting on the Device

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

You can do this configuration on the device **More > Settings > Display** screen.



17:13 Thu 2022-08-25

Display Setting

Brightness 145

Sleep 1 minute

Screen Saver Time 30 minutes

Screen Saver ☑

Screen Saver Type Local Pictures

Screen Lock □

Font Size Normal

Parameter Set-up:

- **Brightness**: press on the brightness setting and move the yellow dots to adjust the screen brightness. The default brightness is 145.
- **Sleep**: set the screensaver time duration before the screen turns off. You can select from 15 seconds to 30 minutes.
  - If the screen saver is enabled, then the sleep time here is the screen saver start time. For example, if you set it as 1 min, then the screen saver will start automatically when the device has no operation for 1 min.
  - If the screen saver is disabled, then the sleep time here is the screen turn-off time.

for example, if you set it as 1 min, then the screen will be turned off automatically when the device has no operation for 1 min.

- **Screen Saver Time**: set the screen saver start time from 1 minute up to 2 hours. Screen saver starts when the device detects no operation, or no one is approaching
- **Screen Saver**: tick the square box to enable the screen saver function.
- **Screen Lock**: tick the screen lock if you want to lock the screen after the screen is turned off (turn dark). You are required to enter the system code to unlock the screen or you can unlock the screen by facial recognition.
- **Screen Saver Type**: select screen saver type among **Local Pictures, Local Videos**, and **Clock.**

NO.	Screen Saver Type	Type Description
1	Local Pictures	Display picture uploaded to the indoor monitor as the screen saver.
2	Local Videos	Display videos from the indoor monitor as the screen saver
3	Clock	Display the clock as the screen saver.

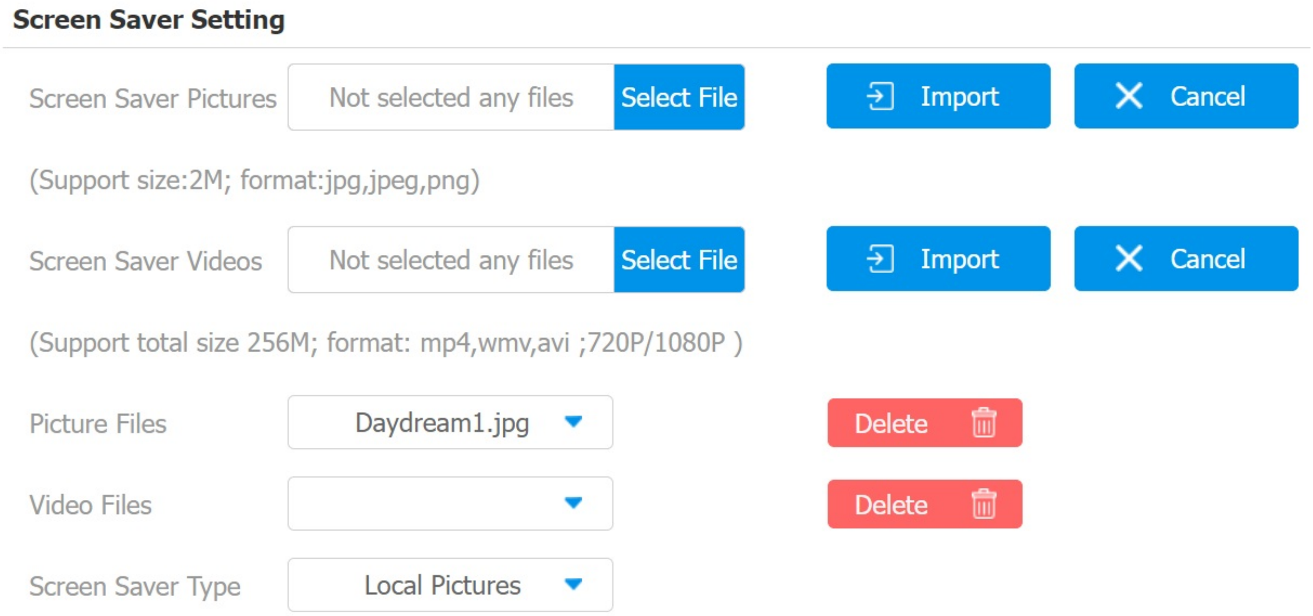
Screen Display Setting on the Web Interface

Akuvox series indoor monitor allows you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

Upload ScreenSaver

You can upload screen-saver pictures separately or in batches to the device and to the device web interface for publicity purposes or for a greater visual experience.

To upload screen saver on device web interface **Phone > Display Setting > Screen Saver** Setting.



Screen Saver Setting

Screen Saver Pictures: Not selected any files

(Support size:2M; format:jpg,jpeg,png)

Screen Saver Videos: Not selected any files

(Support total size 256M; format: mp4,wmv,avi ;720P/1080P)

Picture Files: Daydream1.jpg

Video Files:

Screen Saver Type: Local Pictures

Parameter Set-up:

- **Screen Saver Pictures**: select the existing screen saver pictures.
- **Screen Saver Videos**: select the existing screen saver video.
- **Picture Files**: choose a picture file you want to use for the screen saver.
- **Video Files**: choose a video file you want to use for the screen saver.
- **Screen Saver Type**: select screen saver type among **Local Pictures, Local Videos**, and **Clock**.

NO.	Screen Saver Type	Type Description
1	Local Pictures	Display picture uploaded to the indoor monitor as the screen saver.
2	Local Videos	Display videos from the indoor monitor as the screen saver
3	Clock	Display the clock as the screen saver.

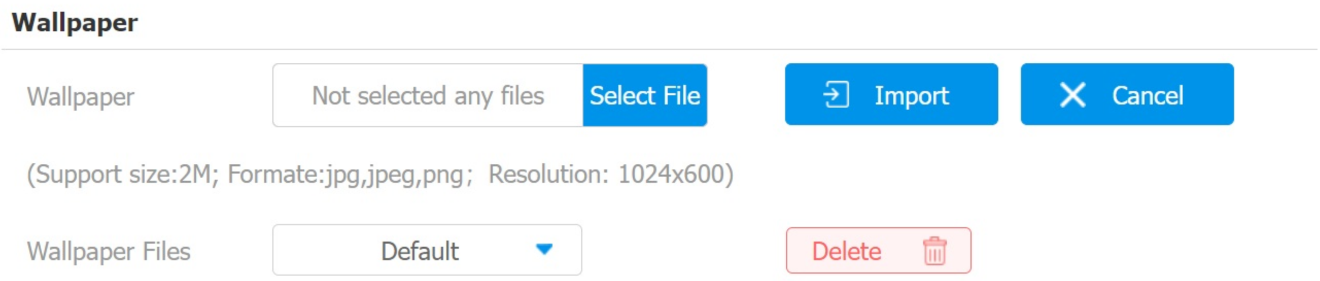
Note

- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurs.
- The pictures uploaded should be in **JPG format** with 2M maximum.

Upload Wall Paper

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

To configure it on the web **Phone** > **Display Setting** > **Wallpaper** interface.



Wallpaper

Wallpaper: Not selected any files

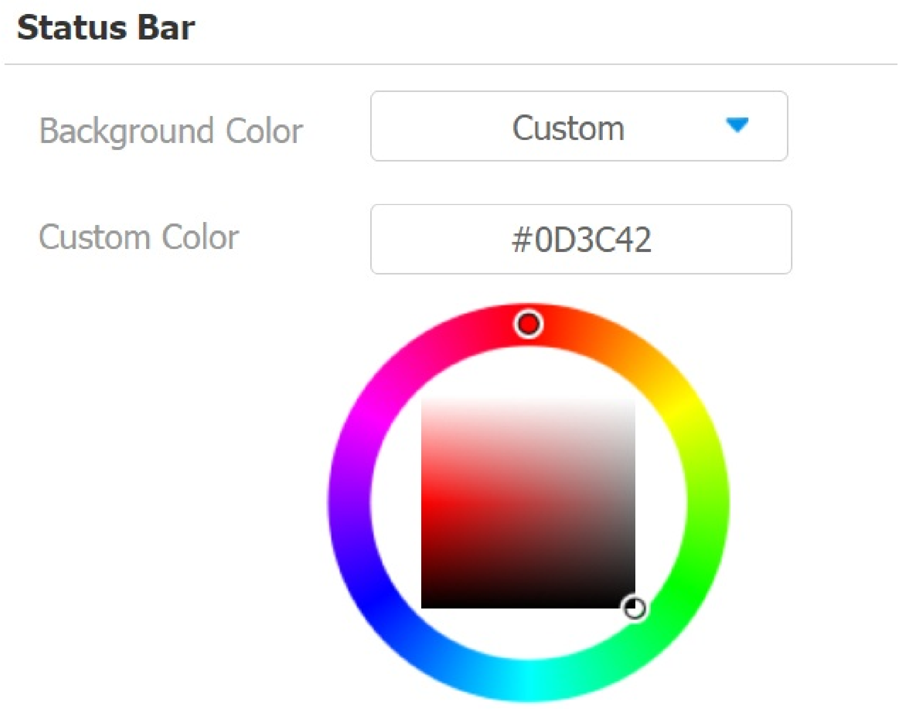
(Support size:2M; Formate:jpg,jpeg,png; Resolution: 1024x600)

Wallpaper Files: Default

Status Bar

Status bar setting is for you to customize the device status bar color according to your scenarios. You can do this configuration on web. Choose Custom mode then adjust the RGB value for the status bar.

To configure it on the web **Phone** > **Display Setting** > **Wallpaper** interface.



Status Bar

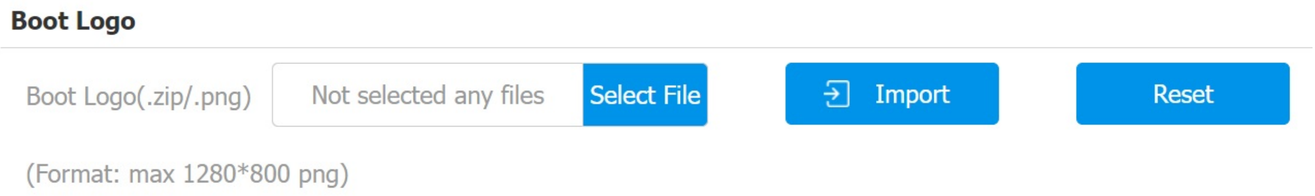
Background Color: Custom

Custom Color: #0D3C42

Upload Device Booting Image

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

To set it up on the web **Phone > Logo** interface.



Boot Logo

Boot Logo(.zip/.png) Not selected any files

(Format: max 1280*800 png)

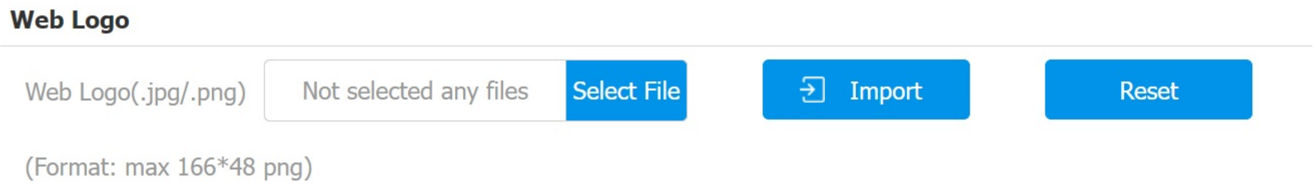
Note

- The pictures uploaded should be in **.png** or **.zip** format.

Upload Device Web Logo

You can customize the web Logo on the upper left corner of the web interface if needed.

To upload the web logo, go to **Phone > Logo > Web Logo** interface.



Web Logo

Web Logo(.jpg/.png) Not selected any files

(Format: max 166*48 png)

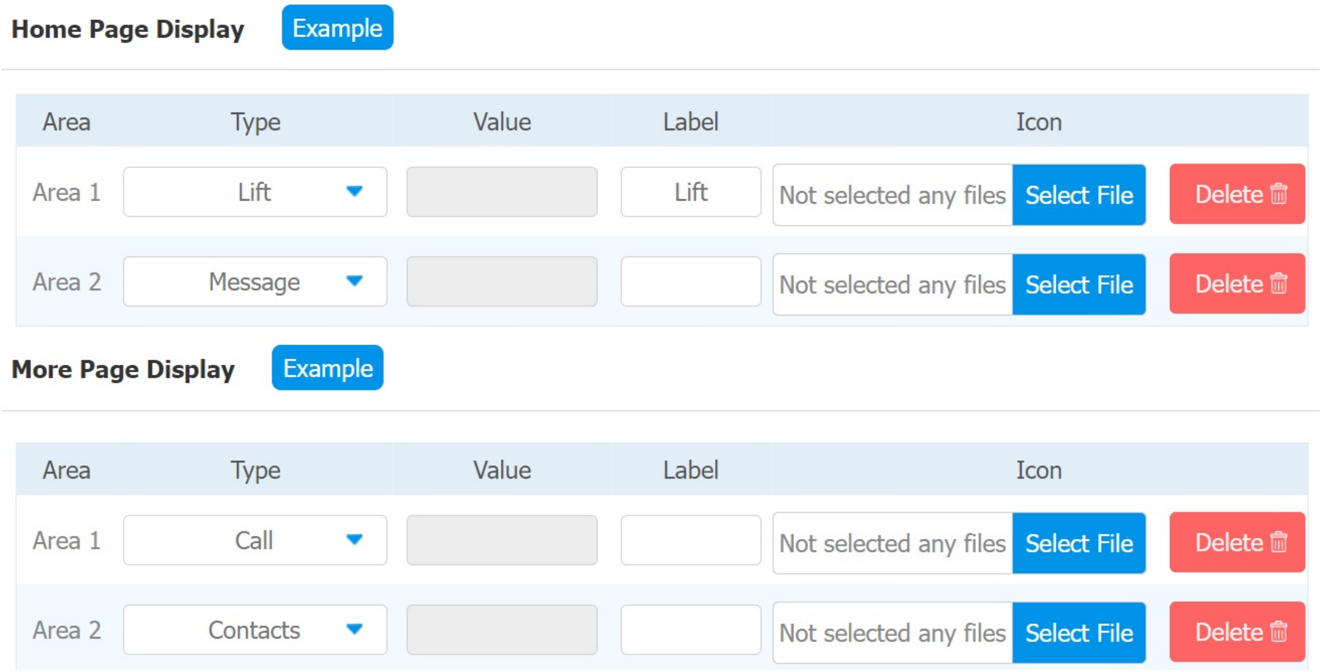
Note

- The pictures uploaded should be in **.jpg** or **.png** format with 50K maximum.

Icon Screen Display Configuration

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

Navigate to **Phone > Key/Display** interface.



Home Page Display

Area	Type	Value	Label	Icon	
Area 1	Lift		Lift	Not selected any files Select File	Delete
Area 2	Message			Not selected any files Select File	Delete

More Page Display

Area	Type	Value	Label	Icon	
Area 1	Call			Not selected any files Select File	Delete
Area 2	Contacts			Not selected any files Select File	Delete

Parameter Set-up:

- **Type**: click to select among options: **DND, Message, Contact, Call, Display, System Info, Setting, Sound, Arming, SOS, Browser, Motion Detection, Custom APK, Lift, Relays, Unlock, Smart Living, Doorbell, N/A**. When **N/A** is selected, the icon display in the corresponding area will disappear.

- **Value**: enter the value if you select the icon type **Custom APK** and **Browser**. For example, when you select **Custom APK**, you are required to enter its package name and class name in the corresponding **Value** field before the APK icon can be displayed on the home screen. If **Browser** is selected, you are required to enter the URL of the browser before the browser icon can be displayed, while the value does not apply to other icon types.

- **Label**: click to rename the icon if needed, while the **DND** icon cannot be renamed.

- **Icons**: click to select the picture to be uploaded as the icon to be displayed.

Note

- You can configure 2 icons in areas 1 and 2 on the home screen.
- You can configure 8 icons on the **More** screen.

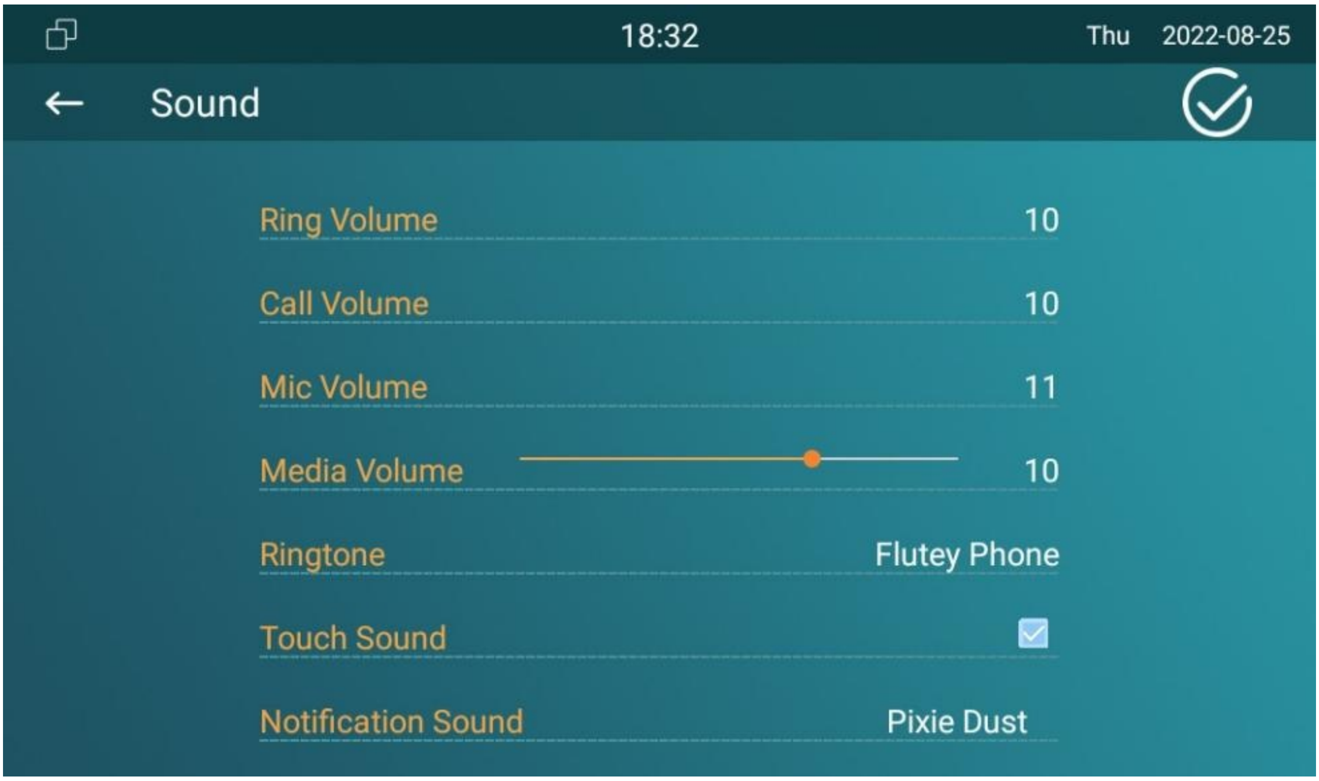
Sound and Volume Configuration

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

Configure Volume on the Device

You can adjust the microphone volume, speaker volume, keypad volume, and AD volume on the device.

To set up the volumes on the device **Setting** > **Sound** screen.



18:32 Thu 2022-08-25

Sound

Ring Volume 10

Call Volume 10

Mic Volume 11

Media Volume 10

Ringtone Flutey Phone

Touch Sound ☑

Notification Sound Pixie Dust

Parameter Set-up:

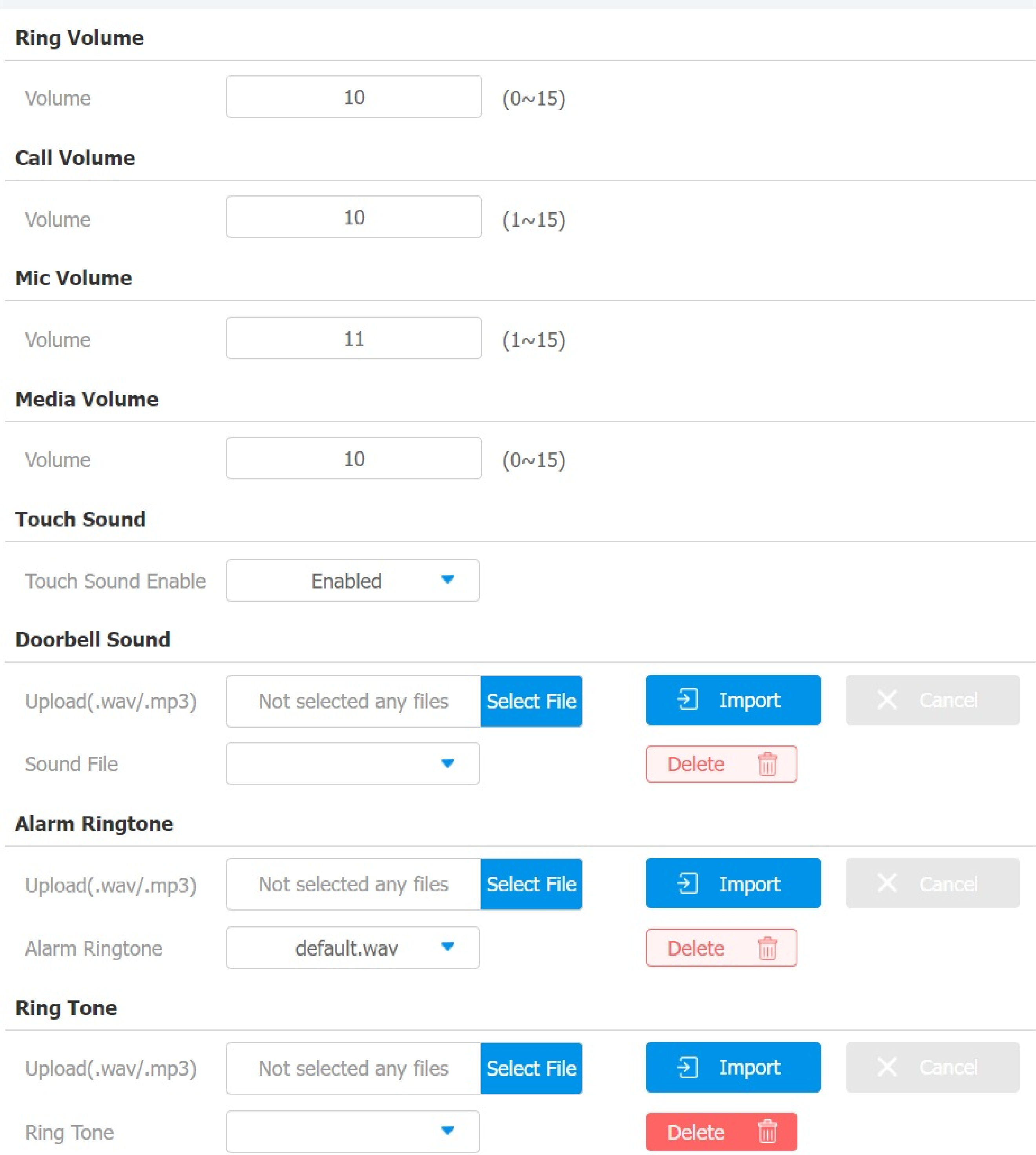
- **Ring Volume**: adjust the incoming call ringtone volume.
- **Call Volume**: adjust the speaker volume during the call.
- **Mic Volume**: adjust the volume of your voice to be heard.
- **Media Volume**: adjust the volume for the video screen saver.
- **Ringtone**: select ringtone for incoming calls.
- **Touch Sound**: adjust the icon tapping sound.

- **Notification Sound**: select the ringtone for the incoming message.
- **Doorbell Ringtone**: select the ringtone for doorbell.

Configure Volume on the Web Interface

On the web interface, you can set the tamper alarm volume, mic volume, etc.

Go to **Phone** > **Audio** interface.



Ring Volume

Volume: 10 (0~15)

Call Volume

Volume: 10 (1~15)

Mic Volume

Volume: 11 (1~15)

Media Volume

Volume: 10 (0~15)

Touch Sound

Touch Sound Enable: Enabled

Doorbell Sound

Upload(.wav/.mp3): Not selected any files

Sound File:

Alarm Ringtone

Upload(.wav/.mp3): Not selected any files

Alarm Ringtone: default.wav

Ring Tone

Upload(.wav/.mp3): Not selected any files

Ring Tone:

Note

- Doorbell sound files and Alarm ringtone files to be uploaded must be **.WAV** or **MP3** format.

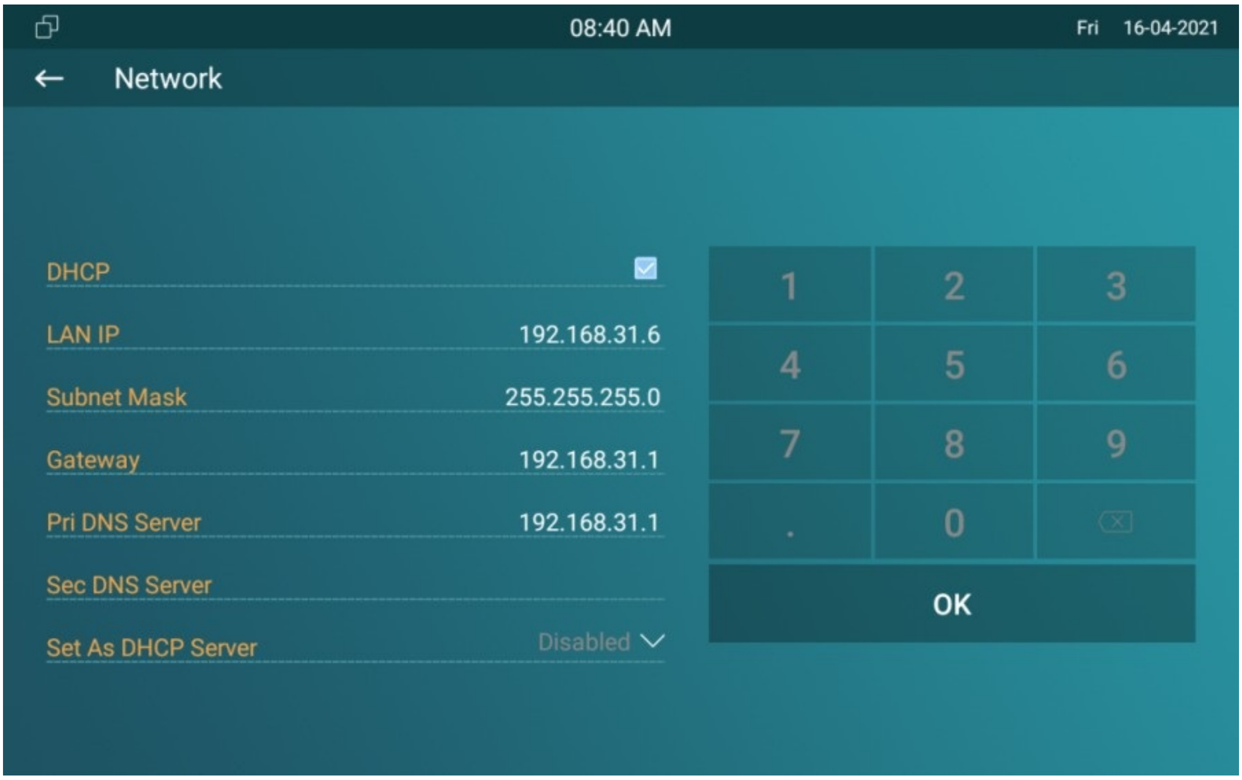
Network Setting & Other Connection

Device Network Configuration

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

Configure Network Connection on the Device

To check and configure the network connection on the device **More > Settings > Advance Settings > Network.**



08:40 AM Fri 16-04-2021

← Network

DHCP	☑
LAN IP	192.168.31.6
Subnet Mask	255.255.255.0
Gateway	192.168.31.1
Pri DNS Server	192.168.31.1
Sec DNS Server	
Set As DHCP Server	Disabled

Parameter Set-up:

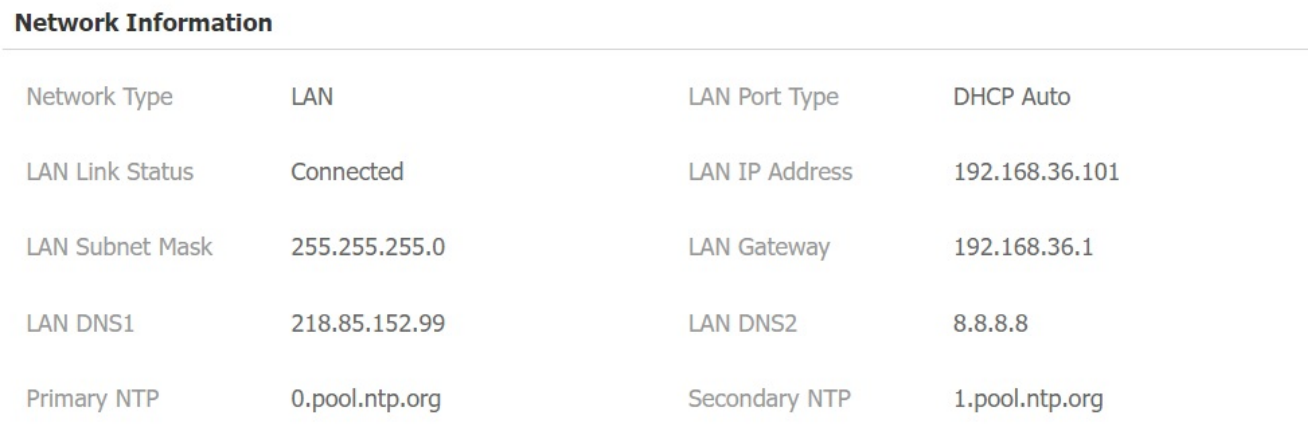
- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, then the device will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: when static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.

- **IP Address**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Pri/Sec DNS Server**: set up preferred or alternate DNS Server (Domain Name Server) according to your actual network environment. Pri DNS server is the primary DNS server address while the sec DNS server is the secondary server address and the device will connect to the alternate server when the primary DNS server is unavailable.

> **Note**
>
> - You can press the **System Info** and then **Network** on the **Settings** screen to check the device network status.
> - The default system code is **123456**.

Configure Device Network Connection on the Web Interface

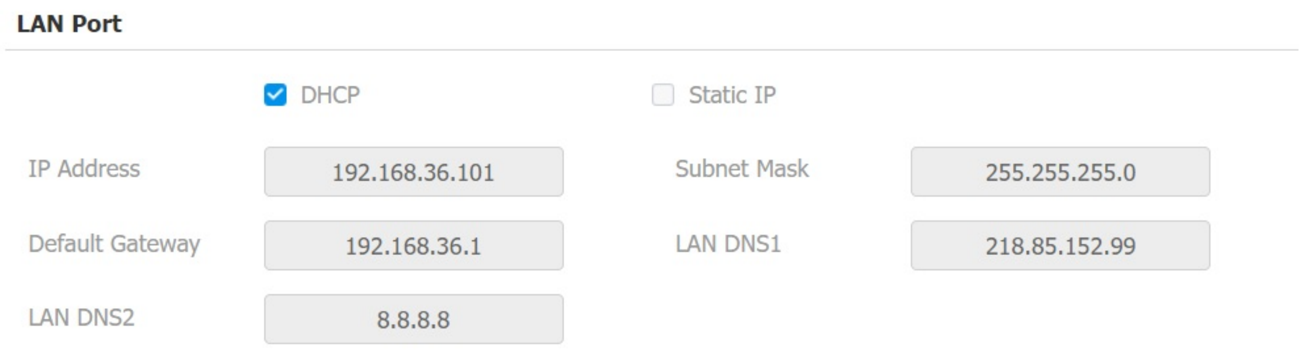
To check the network on the web **Status > Basic > Network information** interface.



Network Information

Network Type	LAN	LAN Port Type	DHCP Auto
LAN Link Status	Connected	LAN IP Address	192.168.36.101
LAN Subnet Mask	255.255.255.0	LAN Gateway	192.168.36.1
LAN DNS1	218.85.152.99	LAN DNS2	8.8.8.8
Primary NTP	0.pool.ntp.org	Secondary NTP	1.pool.ntp.org

To check and configure the network connection on the device web **Network > Basic** interface.



LAN Port

☑ DHCP ☐ Static IP

IP Address	192.168.36.101	Subnet Mask	255.255.255.0
Default Gateway	192.168.36.1	LAN DNS1	218.85.152.99
LAN DNS2	8.8.8.8		

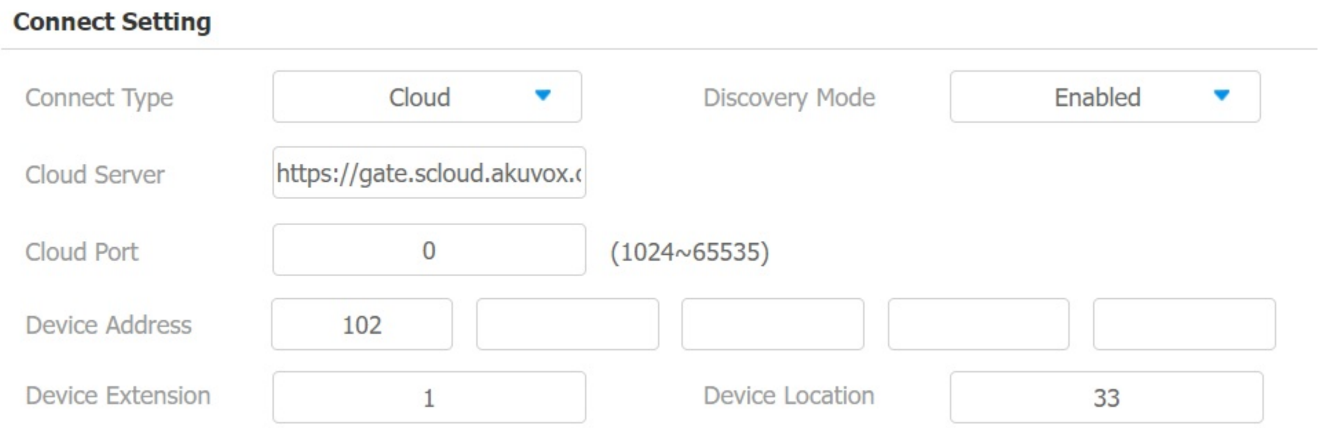
Parameter Set-up:

- **DHCP**: select the DHCP mode by checking the DHCP box. DHCP mode is the default network connection. If the DHCP mode is selected, then the indoor monitor will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: select the static IP mode by checking off the DHCP square box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS servers address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **LAN DNS1/2 Server**: set up DNS (Domain Name Server) according to your actual network environment. LAN DNS1 is the primary DNS server address while the LAN DNS2 is the secondary server address and the device connects to the alternate DNS server when the primary DNS server is unavailable.

Device Deployment in Network

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

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



Connect Setting

Connect Type: Cloud
Discovery Mode: Enabled
Cloud Server: https://gate.scloud.akuvox.c
Cloud Port: 0 (1024~65535)
Device Address: 102
Device Extension: 1
Device Location: 33

Parameter Set-up:

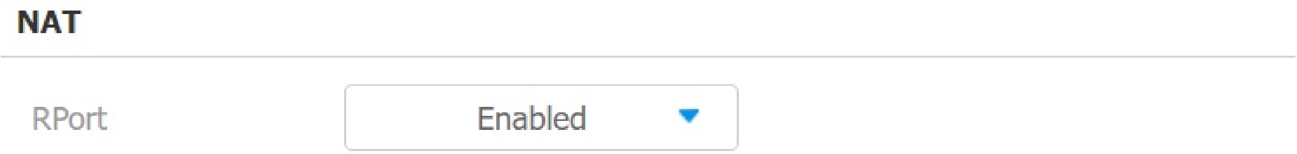
- **Connect Type**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore, you are allowed to choose **Cloud** or **SDMC** in discovery mode.

- **Discovery Mode**: turn on the discovery mode of the device so that it can be discovered by other devices in the network, and disable it if you want to conceal the device so as not to be discovered by other devices.
- **Device Address**: specify the device address by entering device location info from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension**: enter the device extension number for the device you installed.
- **Device Location**: enter the location in which the device is installed and used to distinguish the device from others.

Device NAT Setting

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

To set up NAT, you can do it on web **Account** > **Advanced** > **NAT** interface.



NAT

RPort: Enabled

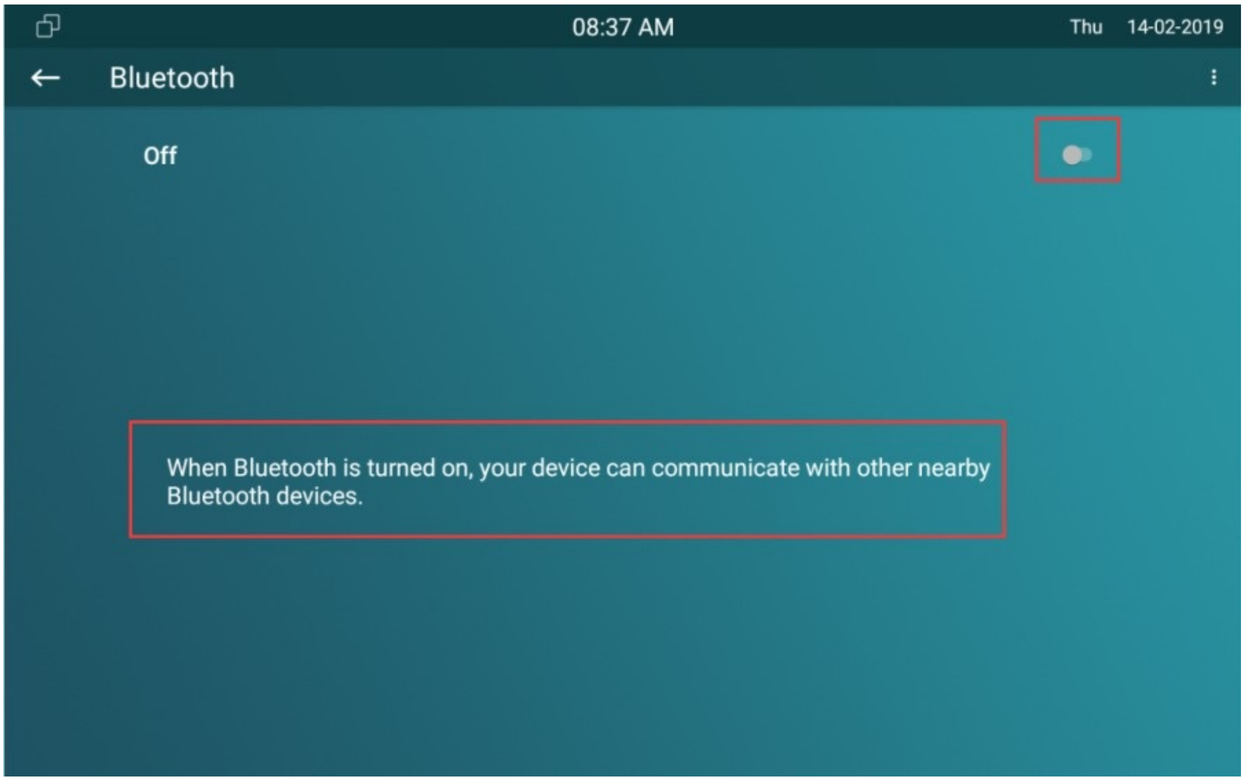
Parameter Set-up:

- **RPort**: check the RPort when the SIP server is in WAN (**Wide Area Network**).

Device Bluetooth Setting

Device Bluetooth Pairing

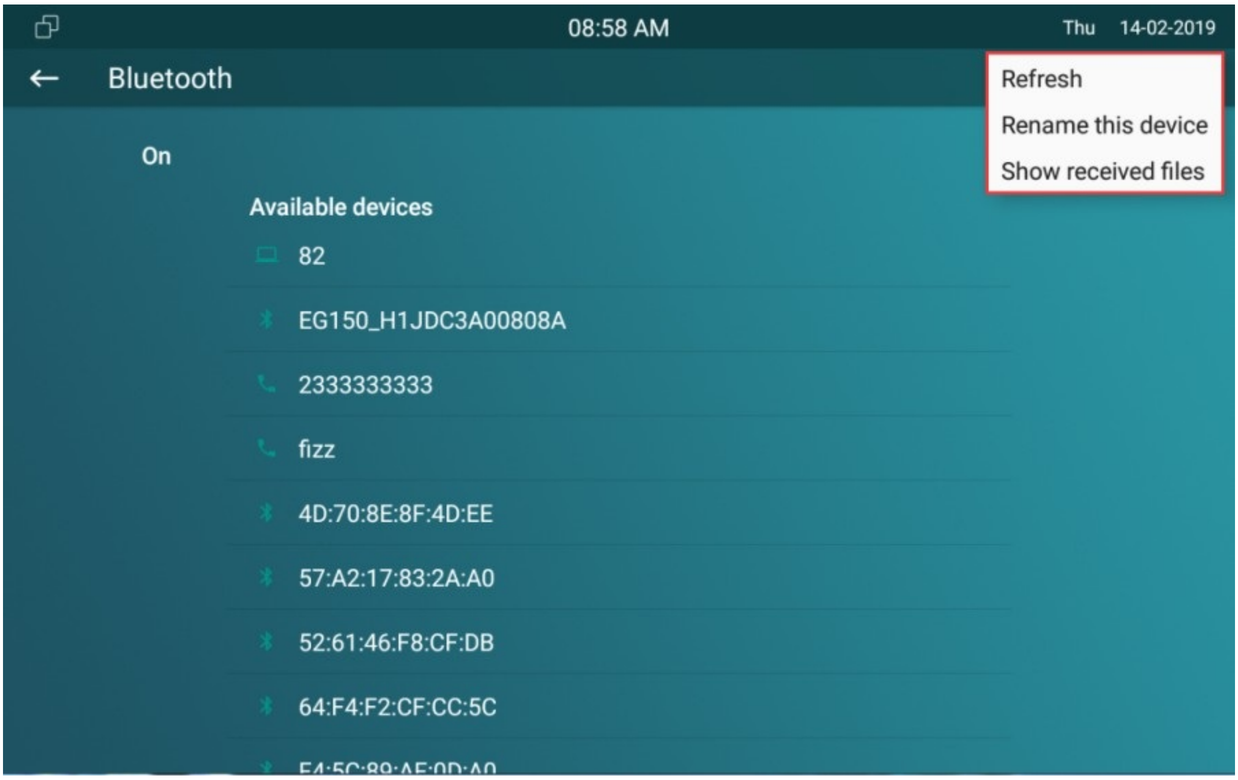
After indoor monitors turn on the Bluetooth on the device **More** > **Settings** > **Bluetooth** screen, it can be paired with other devices via Bluetooth.

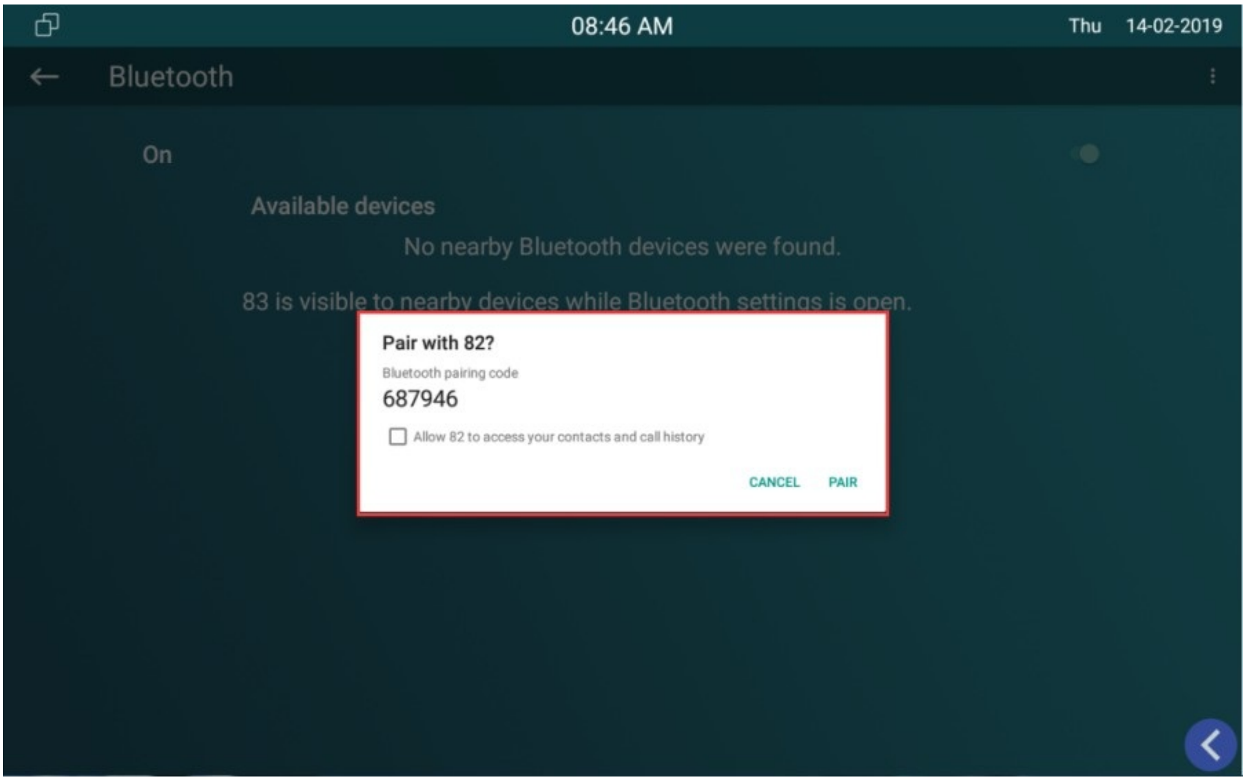


When Bluetooth is turned on, your device can communicate with other nearby Bluetooth devices.

Device Bluetooth Data Transmission

To transfer data via Bluetooth by pressing **Pair new device.**





08:46 AM Thu 14-02-2019

Bluetooth

On

Available devices

No nearby Bluetooth devices were found.

83 is visible to nearby devices while Bluetooth settings is open.

Pair with 82?

Bluetooth pairing code

687946

□ Allow 82 to access your contacts and call history

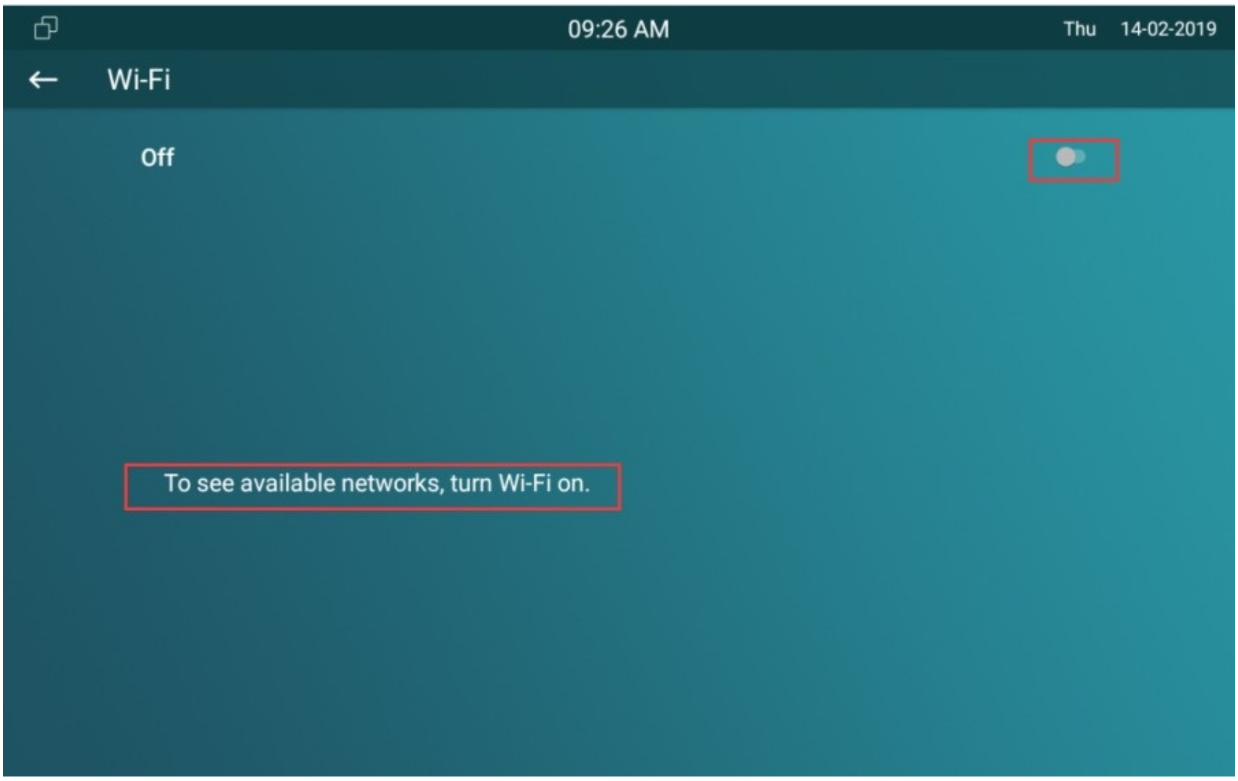
CANCEL PAIR

Note

- After successful Bluetooth pairing, data transmission can be carried out.

Device Wi-Fi Setting

You can set the Wi-Fi on the device at **More** > **Settings** > **Advance Settings** > **WLAN** screen.



To see available networks, turn Wi-Fi on.

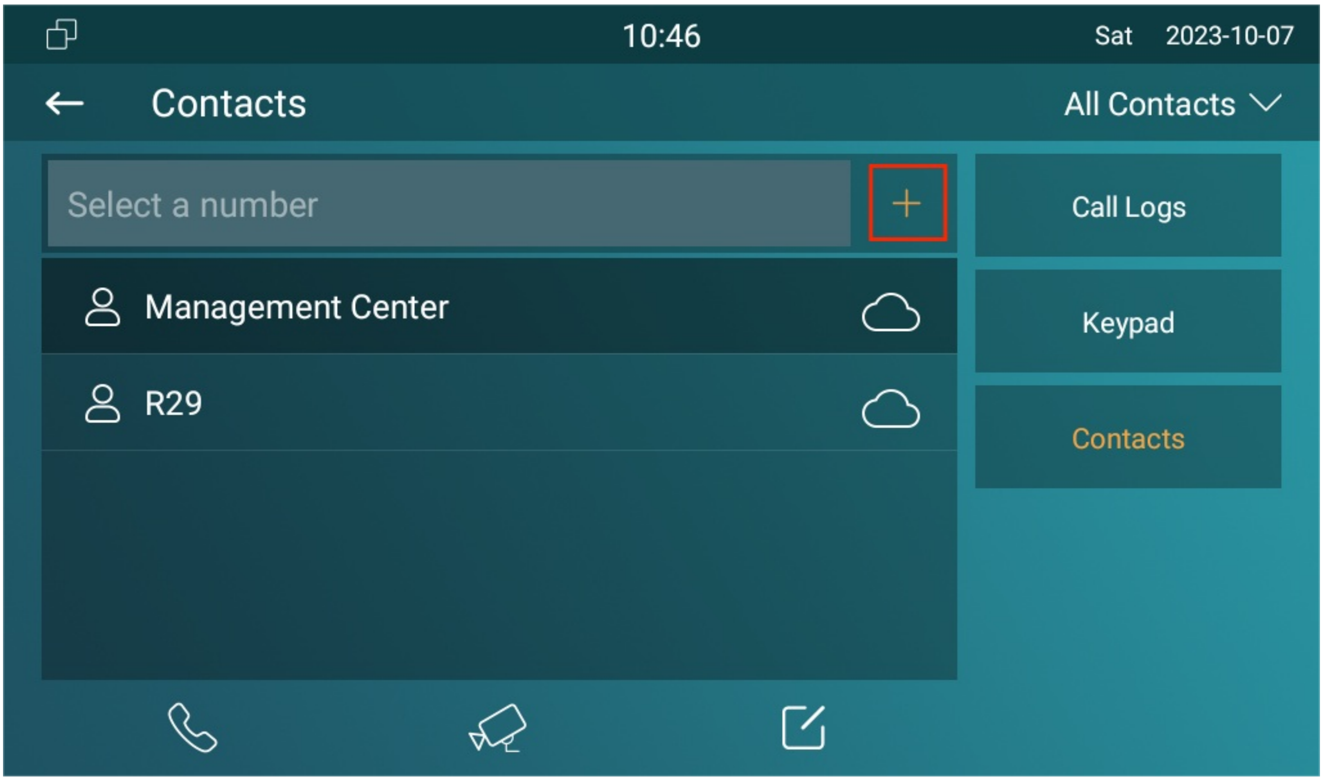
Phone Book Configuration

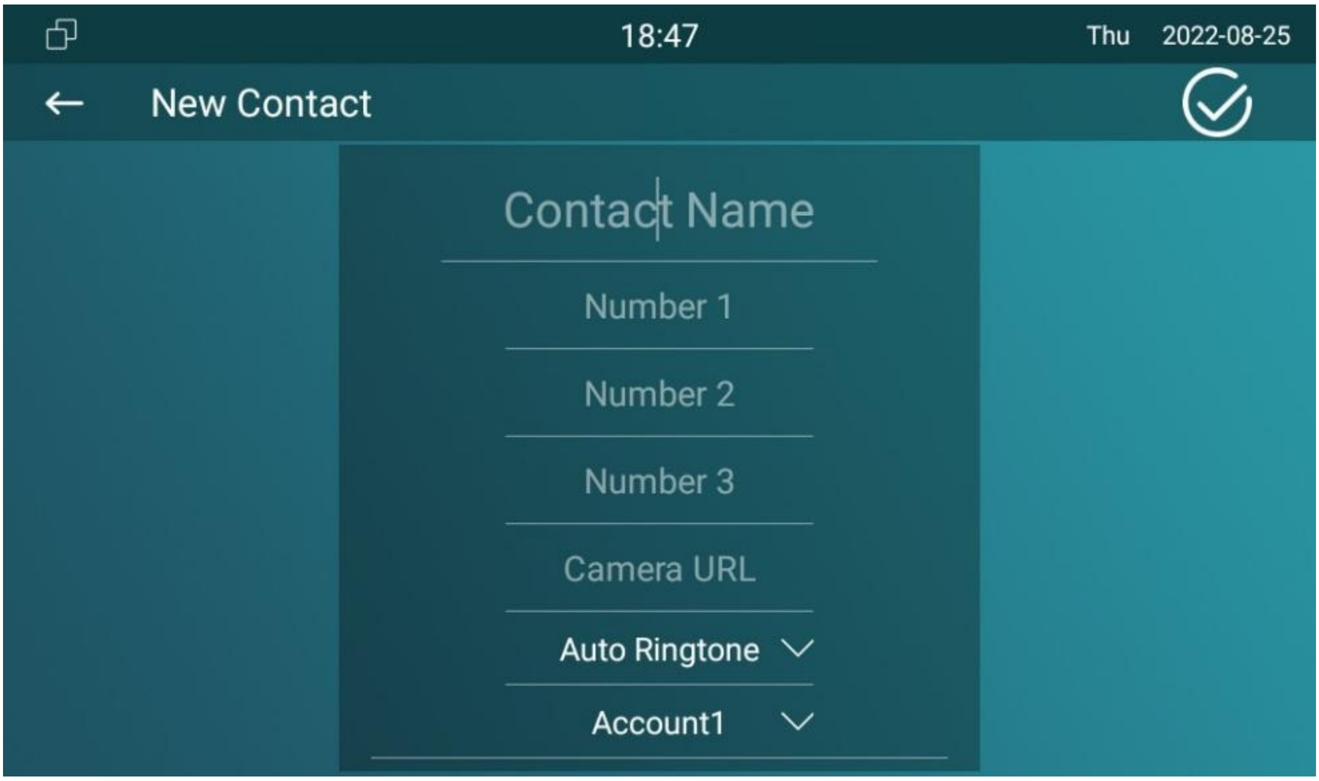
Phone Book Configuration on the Device

You can configure the contacts list in terms of adding and modifying contact groups or contacts on the device **More** > **Contacts** directly.

Add Contacts

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





18:47 Thu 2022-08-25

New Contact

Parameter Set-up:

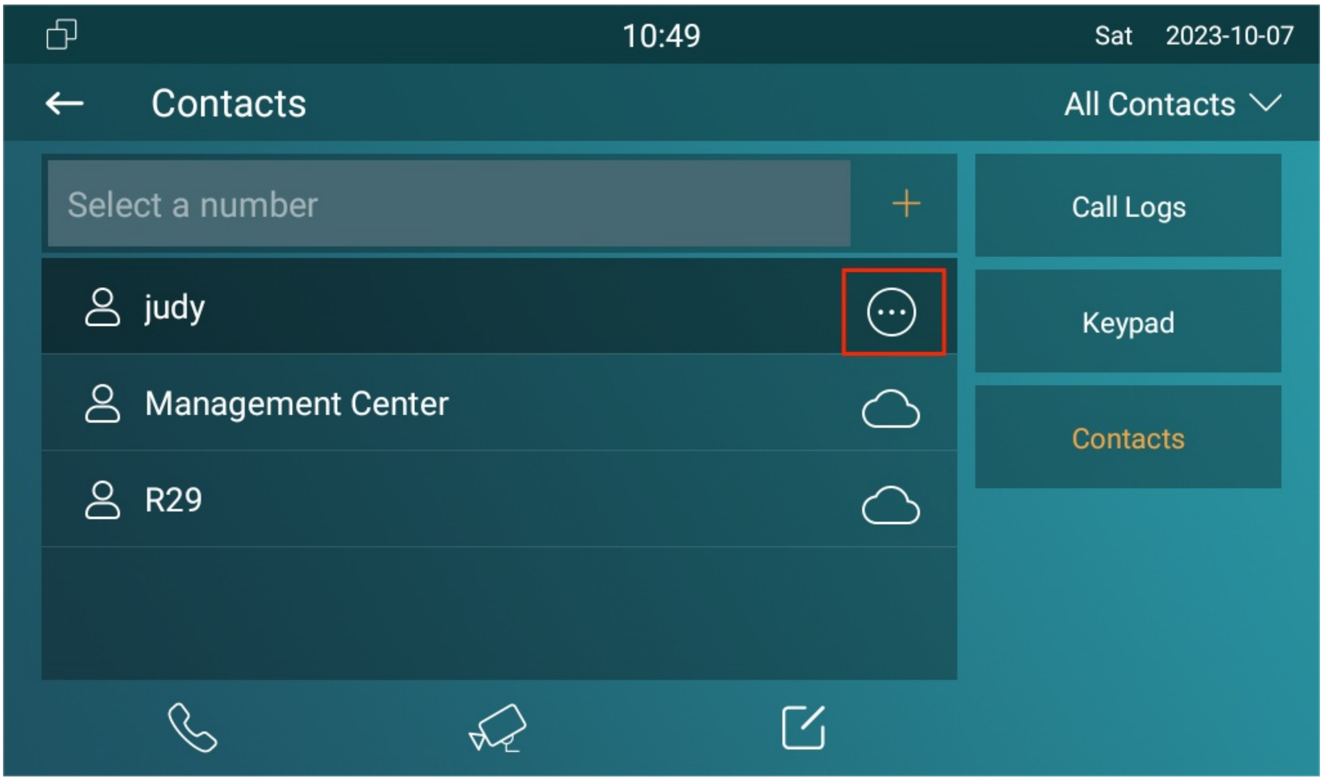
- **Contact Name**: name the contact.
- **Number**: enter the IP or SIP number.
- **Camera URL** enter the RTSP URL for video preview.
- **Auto Ringtone**: select the phone ringtone for incoming calls.
- **Account1**: select which account to use to dial out, Account 1 or Account 2.

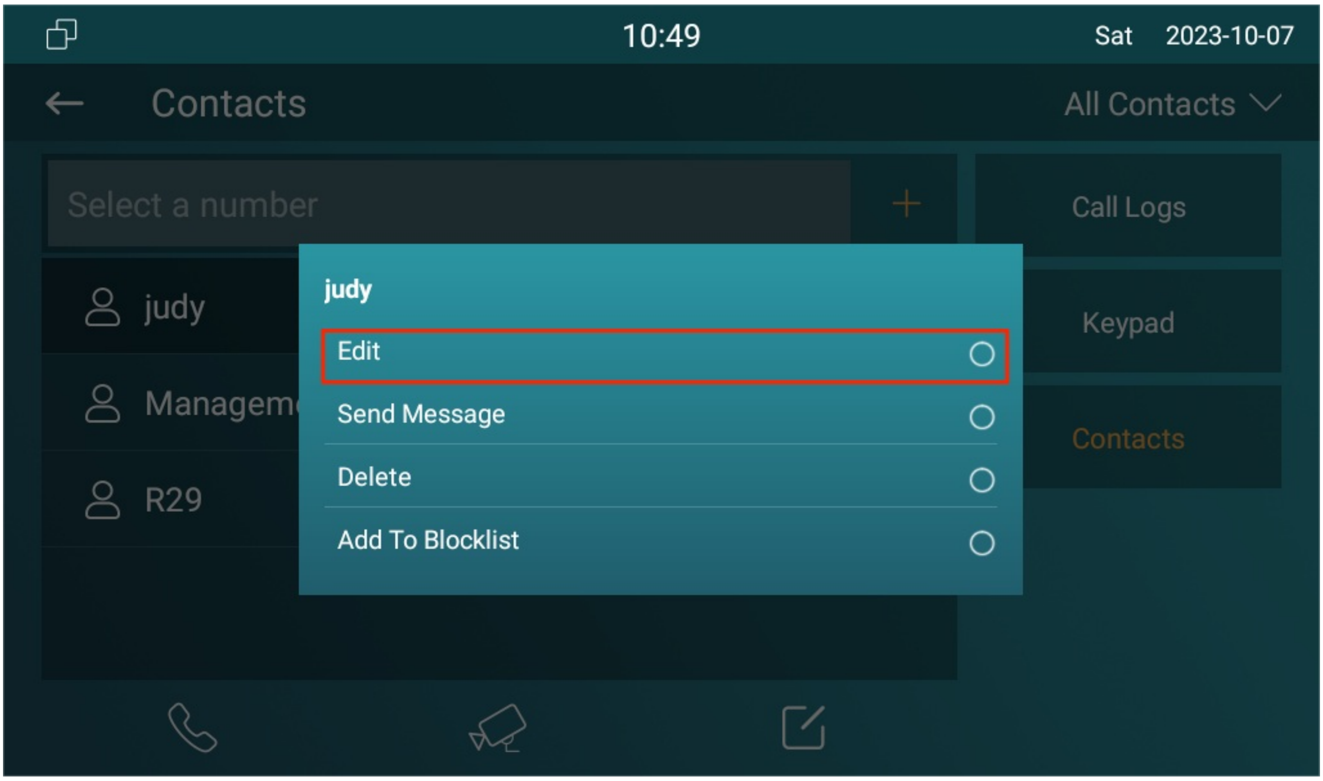
Note

- The RTSP URL format is rtsp://device IP/live/ch00_0.

Edit Contacts

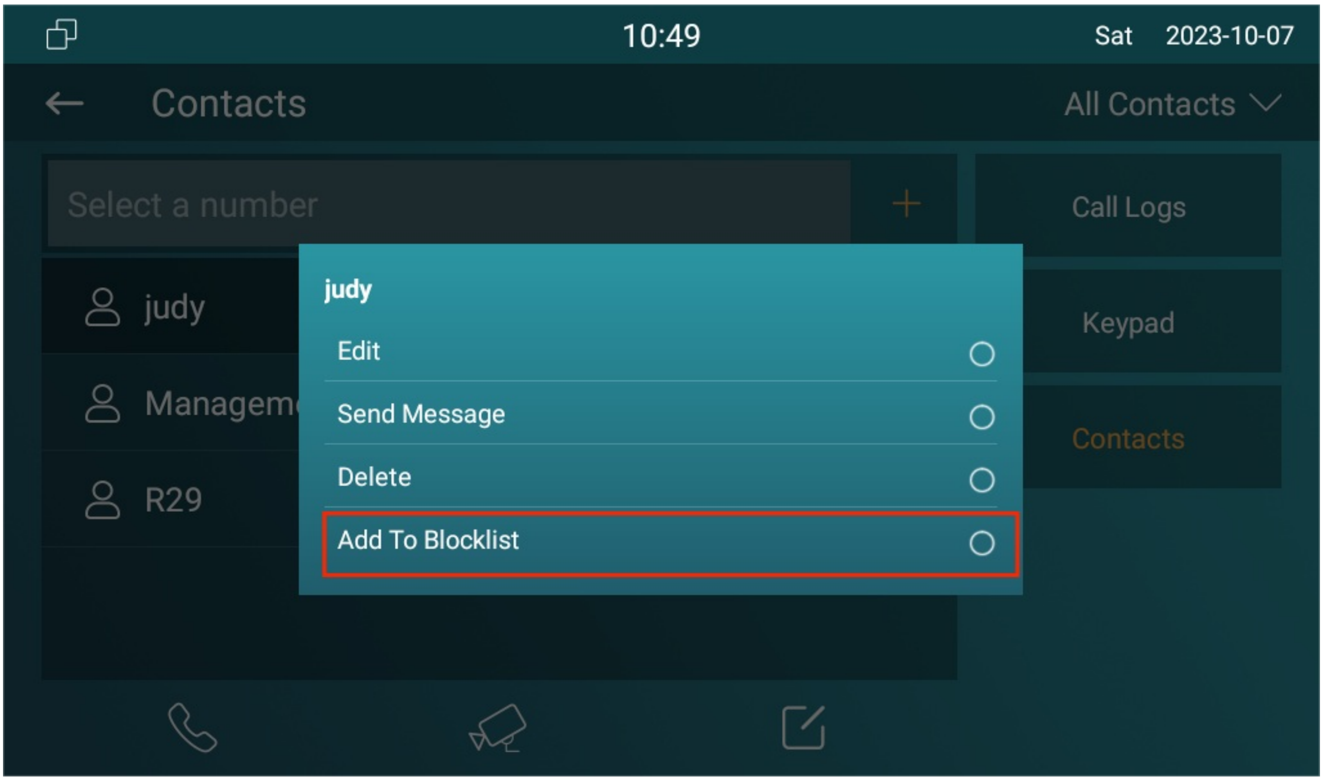
Select the existing contact and click **Edit** to modify.





Blocklist Settings on the Device

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



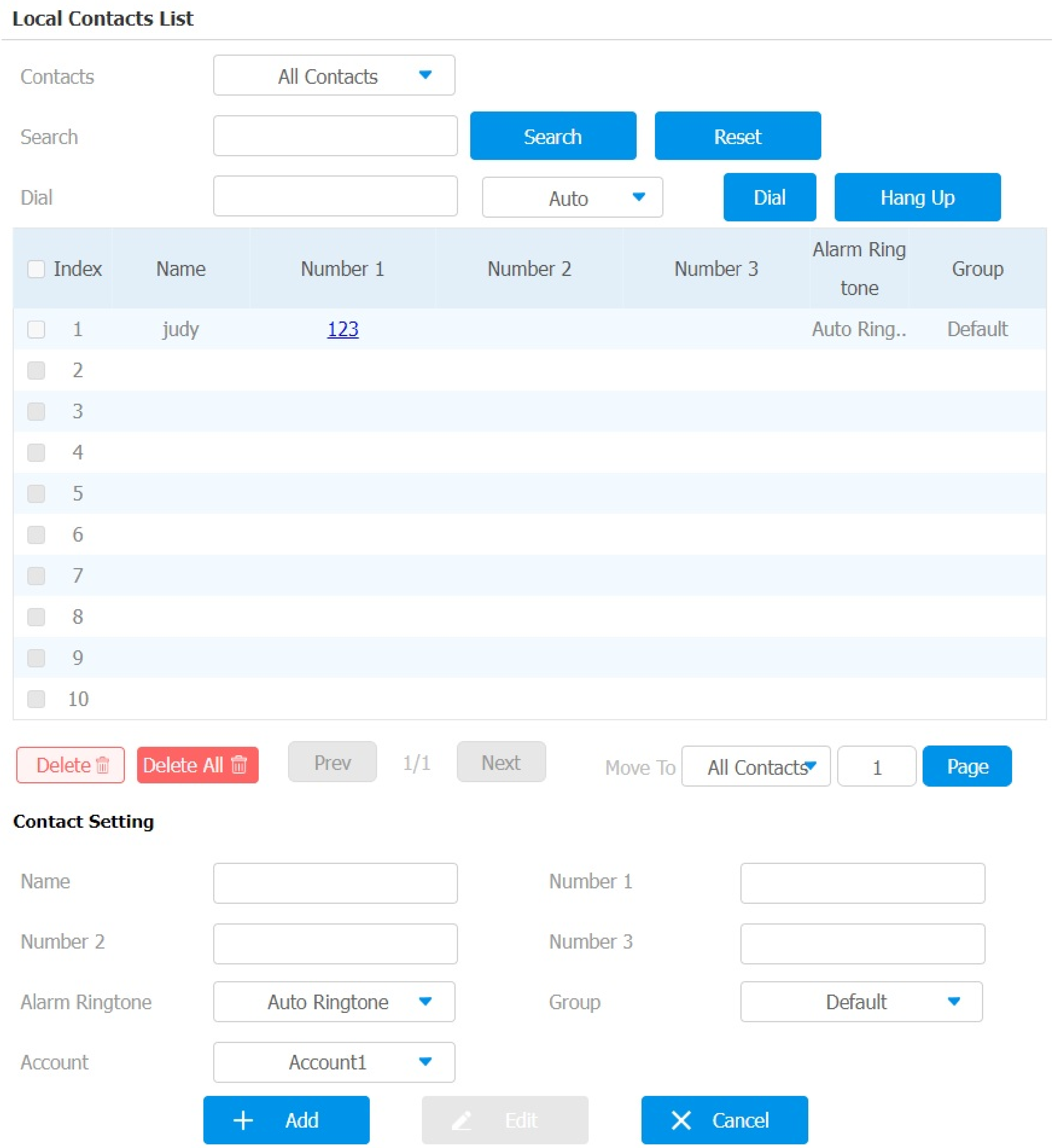
Note

- You can delete contacts regardless of whether it is on the **All Contacts** screen or the **Blocklist** screen.

Phone Book Configuration on the Web Interface

Contact Configuration

To conduct contact configuration on the web **Contacts > Local Contacts** interface. The existing contacts will show in the below list after they are added.



Local Contacts List

Contacts: All Contacts

Search:

Dial: Auto

□ Index	Name	Number 1	Number 2	Number 3	Alarm Ring tone	Group
□ 1	judy	123			Auto Ring..	Default
□ 2						
□ 3						
□ 4						
□ 5						
□ 6						
□ 7						
□ 8						
□ 9						
□ 10						

Move To: All Contacts 1

Contact Setting

Name		Number 1	
Number 2		Number 3	
Alarm Ringtone	Auto Ringtone	Group	Default
Account	Account1		

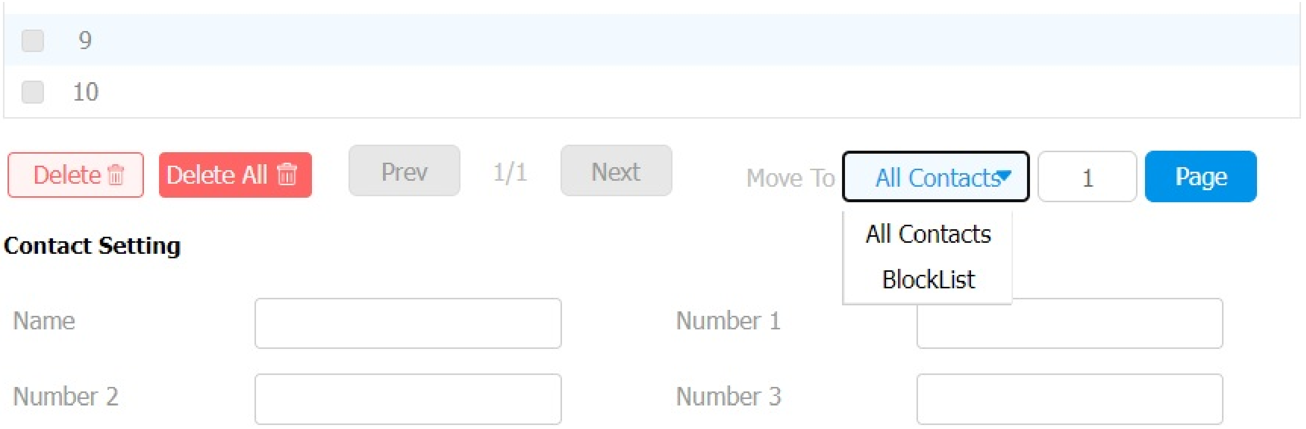
Parameter Set-up:

- **Name**: name the contact.
- **Number**: enter the contact number (SIP or IP number).
- **Group**: select Default or Blocklist group.
- **Account**: select Account1 or Account2 to dial out.

You can dial out a number using the contact phone number.

Block List Setting on the Web Interface

You can set the blocklist directly in the contact list on the web **Contacts > Local Contacts > Local Contacts List** interface or set it when editing a contact.

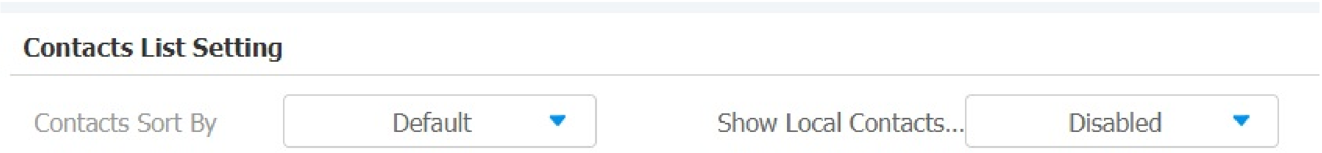


> **Note**
>
> - If you want to remove the contact from the blocklist on the web interface, you can change the group to **Default** when editing the contact.

Contact Display

You can configure the contact display order and control whether to display the discovery device on the device.

To configure it on the **Contacts > Local Contacts > Contacts List Setting** interface.



Contacts Sort By: Default

Show Local Contacts...: Disabled

Parameters Set-up:

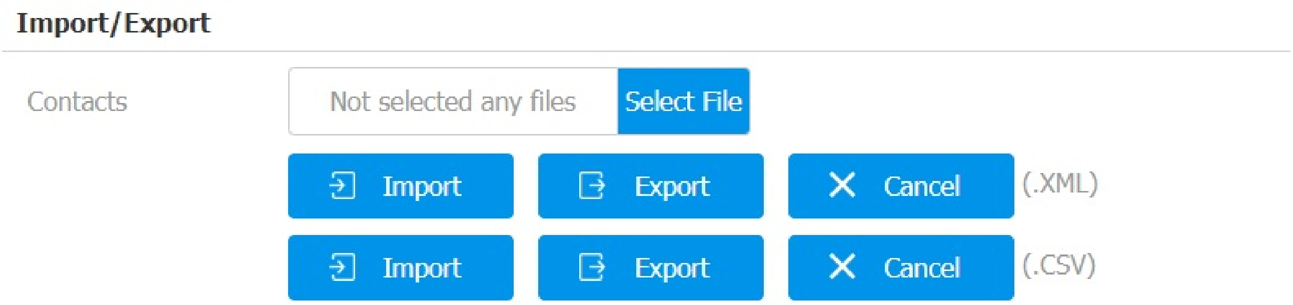
- **Contacts Sort By**: there are three modes **Default, ASCII code**, and **Created Time** for showing the contact list.

- **Show Local Contacts Only**: if you enable the function, the contact on the device will only show the local phonebook, and the contact for discovery mode will be hidden.

Contacts Import and Export on the Web Interface

When the contact becomes so many that you cannot afford to manage each contact one by one manually, you can import and export the contacts in batch on the device web.

Go to **Contacts** > **Local Contacts** > **Import/Export** interface.



Note

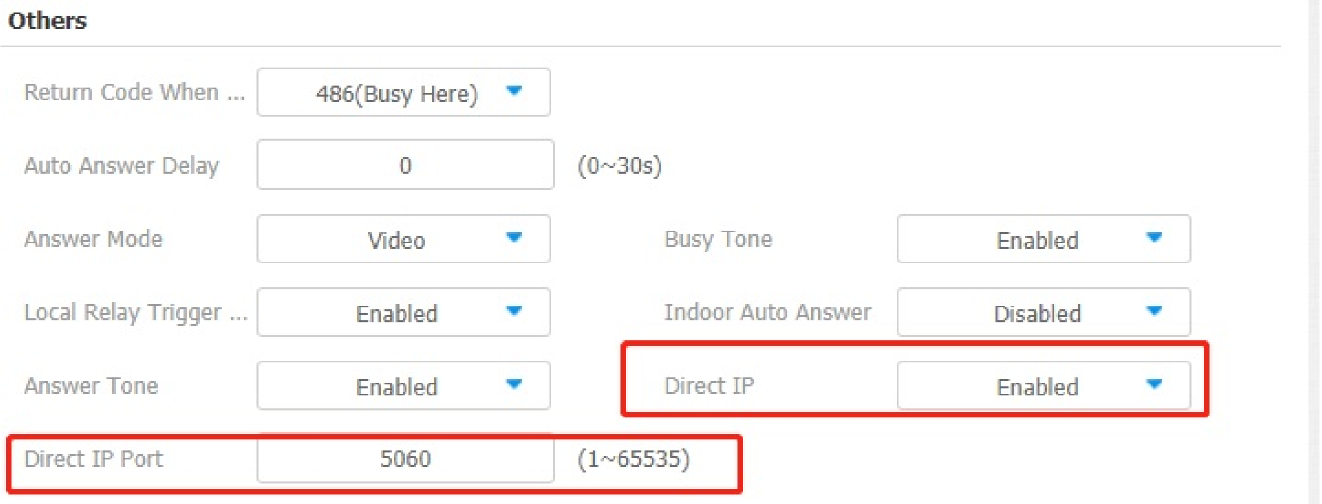
- The contact file can only be imported or exported in **.xml** or **.csv** format.

Intercom Call Configuration

IP Call & IP Call Configuration

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

To configure the IP call feature and port on the device web **Phone > Call Feature > Others** interface.



Others

Return Code When ...	486(Busy Here)			
Auto Answer Delay	0	(0~30s)		
Answer Mode	Video		Busy Tone	Enabled
Local Relay Trigger ...	Enabled		Indoor Auto Answer	Disabled
Answer Tone	Enabled		Direct IP	Enabled
Direct IP Port	5060	(1~65535)		

Parameter Set-up:

- **Direct IP**: enable the 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 Port**: the direct IP port is **5060** by default with the port range from **1-65535.** If you enter any values within the range other than **5060**, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

SIP Call & SIP Call Configuration

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

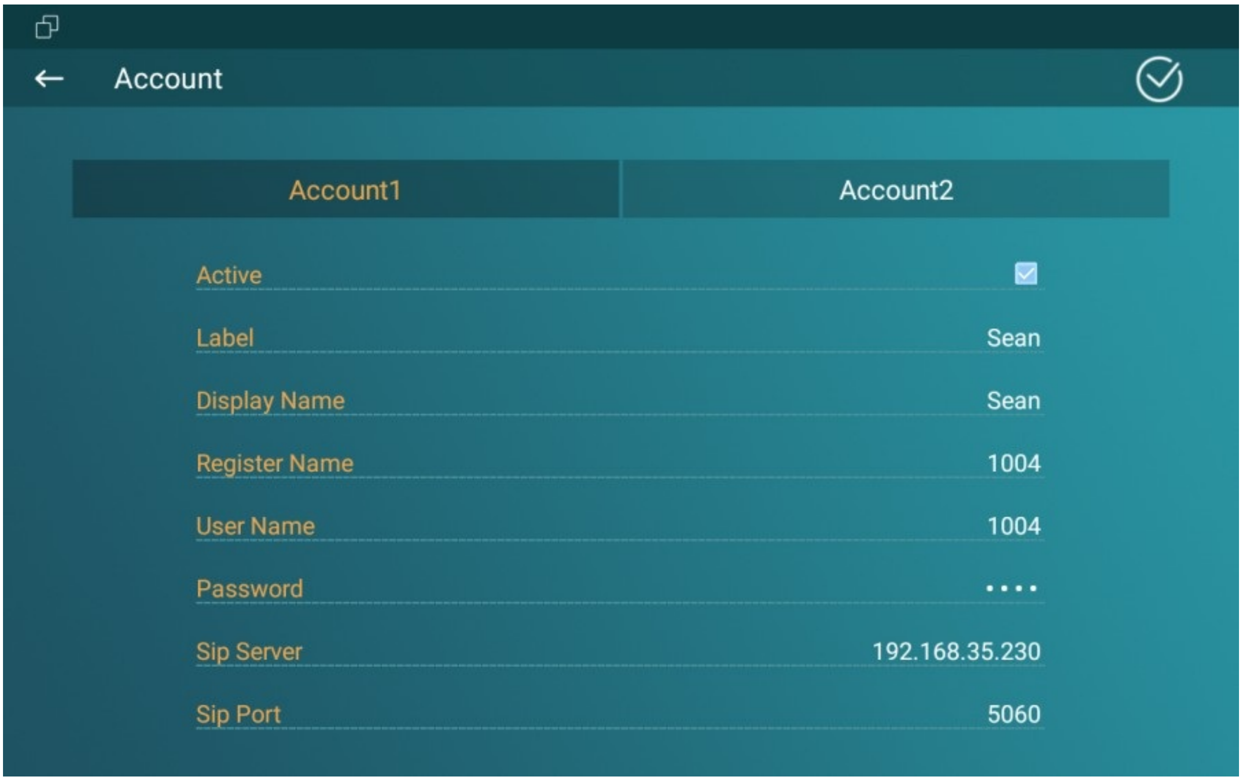
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

Each device needs a SIP account to make and receive SIP calls.

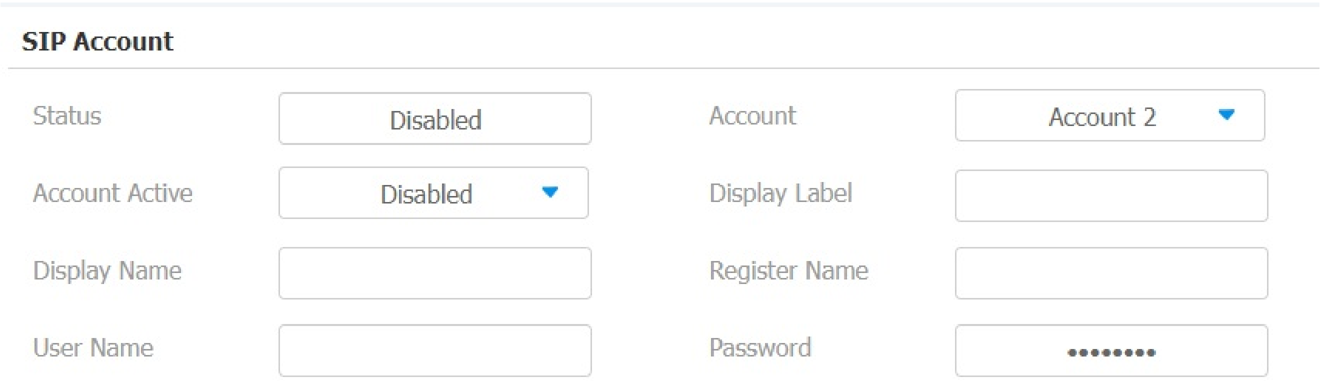
Akuvox intercom devices support the configuration of two SIP accounts, which can be registered under two independent servers.

To configure the SIP account on the device **More** > **Settings** > **Advance Settings** > **Account** screen.



Active	☑
Label	Sean
Display Name	Sean
Register Name	1004
User Name	1004
Password	••••
Sip Server	192.168.35.230
Sip Port	5060

The parameter settings for SIP account registration can be configured on the **Account Setting** screen and they can also be configured on the device web interface. To perform the SIP account setting on the web **Account** > **Basic** > **SIP Account** Interface.



SIP Account

Status	Disabled	Account	Account 2
Account Active	Disabled	Display Label	
Display Name		Register Name	
User Name		Password	•••••••••

Parameter Set-up:

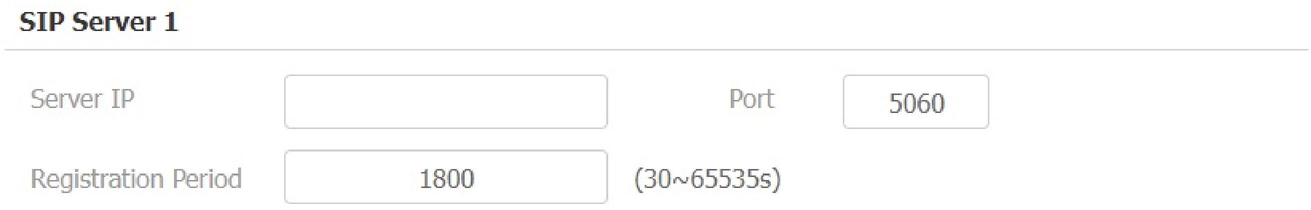
- **Status**: Check to see if the SIP account is registered or not.
- **Account**: Select Account1 or Account2.
- **Active**: Check to activate the registered SIP account.
- **Display Label**: Configure the device label to be shown on the device screen.
- **Display Name**: Configure the device's name to be shown on the device being called to.

a. To register SIP account for Akuvox indoor monitors, obtain **Register Name, Username**, and **Password** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Register Name, Username**, and **Password** from third-party service provider.

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 perform the SIP account setting on the web **Account > Basic > SIP Account** Interface.



SIP Server 1

Server IP		Port	5060
Registration Period	1800	(30~65535s)	

Parameter Set-up:

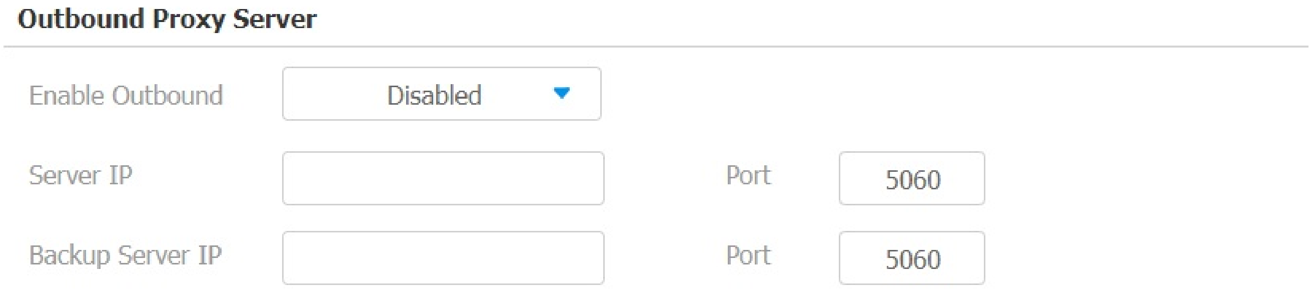
- **Server IP**: Enter the server's IP address or its URL.
- **Port**: Set up SIP server port for data transmission.
- **Registration Period**: Set up SIP account registration time span. SIP re-registration will

start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535s**.

Outbound Proxy Server configuration

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

To configure the outbound proxy server on **Account > Basic > Outbound Proxy Server** interface.



Outbound Proxy Server

Enable Outbound	Disabled		
Server IP		Port	5060
Backup Server IP		Port	5060

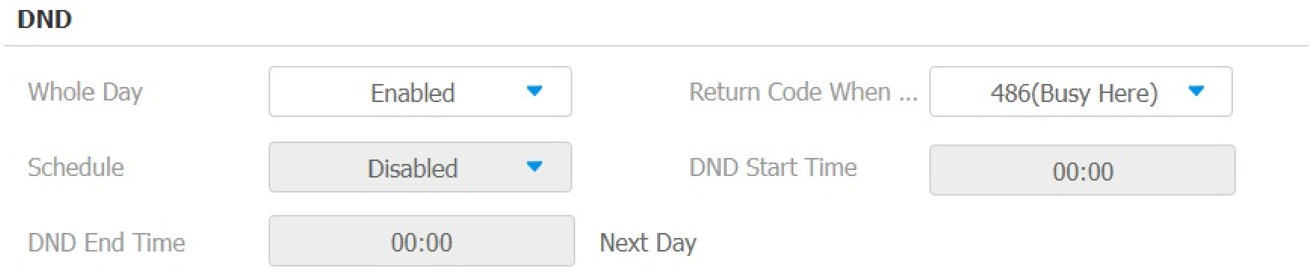
Parameter Set-up:

- **Server IP**: Enter the IP address of the outbound proxy server.
- **Backup Server IP**: Set up backup server IP for the backup outbound proxy server.
- **Port**: Enter the port number to establish a call session via the outbound proxy server or the backup one.

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.

Path: **Phone > Call Feature > DND**



DND

Whole Day	Enabled	Return Code When ...	486(Busy Here)
Schedule	Disabled	DND Start Time	00:00
DND End Time	00:00	Next Day	

Parameter Set-up:

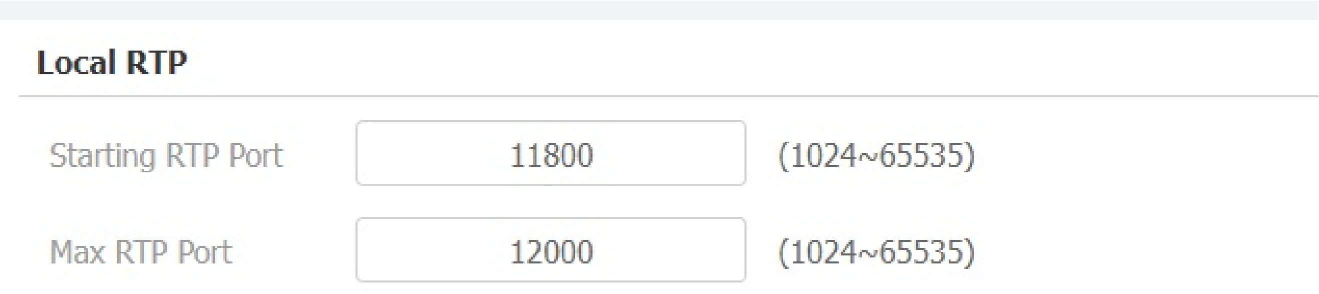
- **DND**: Check the **Whole Day** or **Schedule** to enable the DND function. DND function is disabled by default.
- **Schedule**: Enable the DND schedule for your indoor monitor. To configure a specific time to enable the DND feature. If you choose **Schedule** for DND, the **Whole Day** will be checked on the device.
- **Return Code When DND**: Select what code should be sent to the calling device via the SIP server. 404 for Not Found; 480 for Temporarily Unavailable; 486 for Busy Here; 603 for Decline.

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 up device local RTP on web **Network** > **Advanced** > **Local RTP** interface.



Local RTP

Starting RTP Port: 11800 (1024~65535)

Max RTP Port: 12000 (1024~65535)

Parameter Set-up:

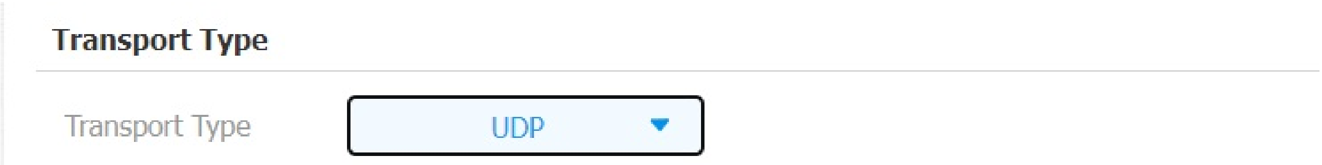
- **Starting RTP Port**: enter the port value in order to establish the start point for the exclusive data transmission range.

- **Max RTP port**: enter the port value in order to establish the end point 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 do this configuration on web **Account > Basic > Transport Type** interface.



Transport Type

Transport Type: UDP

Parameter Set-up:

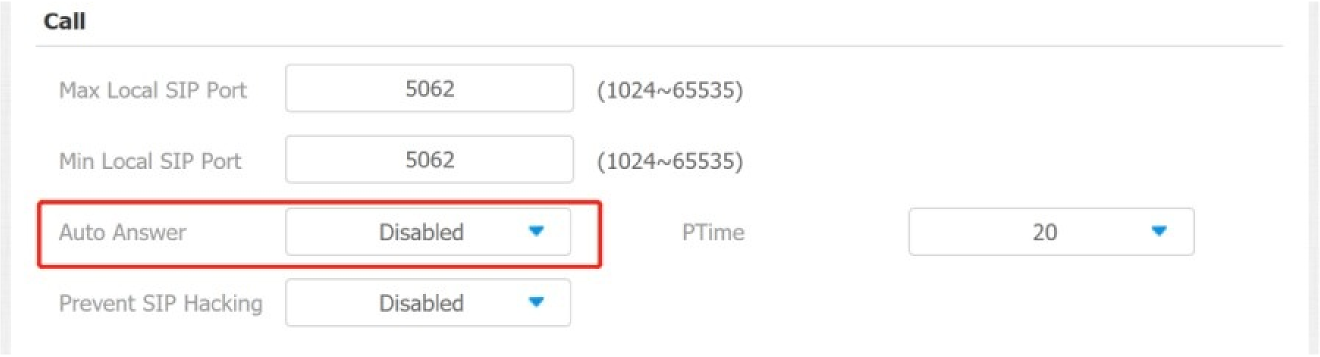
- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for secured and reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain DNS record for specifying the location of services. And SRV not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

Call Setting

Call Auto-answer Configuration

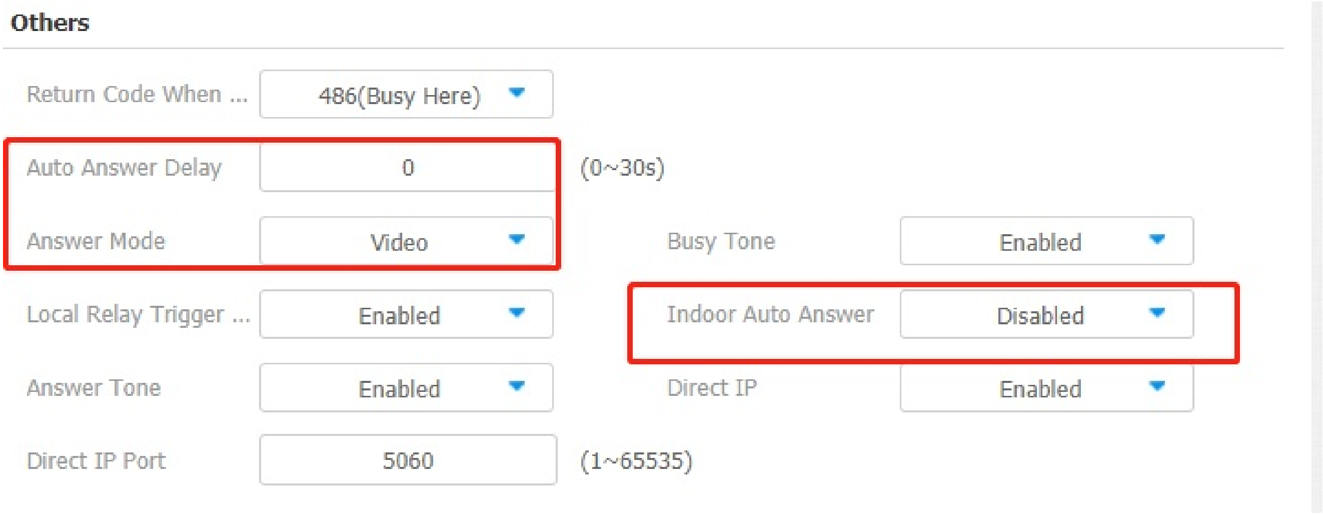
Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

To enable or disable on web **Account > Advanced > Call > Auto Answer** interface. And set up the corresponding auto-answer parameters on the web **Phone > Call Feature > Others** interface.



Call

Max Local SIP Port	5062	(1024~65535)		
Min Local SIP Port	5062	(1024~65535)		
Auto Answer	Disabled		PTime	20
Prevent SIP Hacking	Disabled			



Others

Return Code When ...	486(Busy Here)			
Auto Answer Delay	0	(0~30s)		
Answer Mode	Video		Busy Tone	Enabled
Local Relay Trigger ...	Enabled		Indoor Auto Answer	Disabled
Answer Tone	Enabled		Direct IP	Enabled
Direct IP Port	5060	(1~65535)		

Parameter Set-up:

- **Auto Answer Delay**: set up the delay time (from 0-30 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.

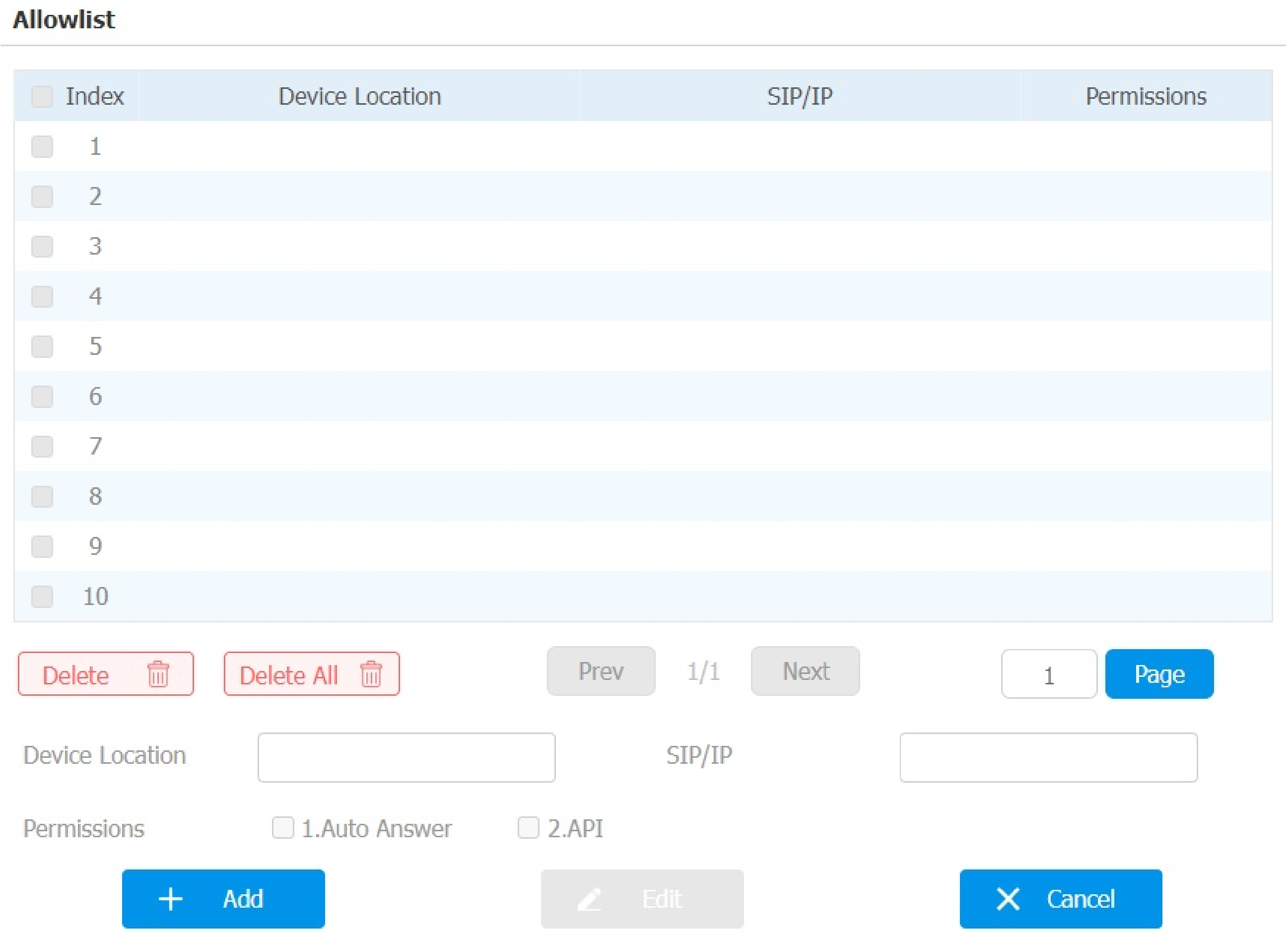
- **Answer Mode**: set up the video or audio mode you preferred for answering the call automatically.

- **Indoor Auto Answer Mode**: turn on the **Auto Answer** function for calls from other indoor monitors by ticking the check box.

Auto-answer Allow List Setting

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

Navigate to **Security > Allowlist** interface.



Allowlist

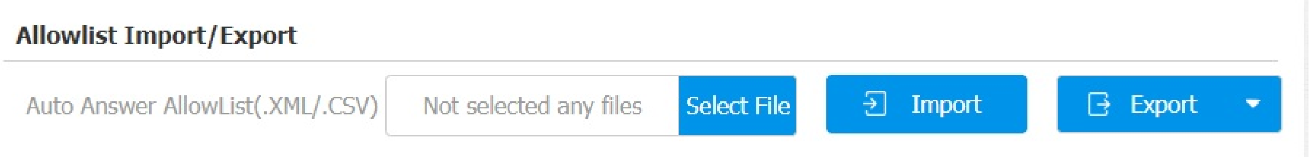
□ Index	Device Location	SIP/IP	Permissions
□ 1			
□ 2			
□ 3			
□ 4			
□ 5			
□ 6			
□ 7			
□ 8			
□ 9			
□ 10			

Device Location

SIP/IP

Permissions □ 1.Auto Answer □ 2.API

SIP/IP numbers can be imported to or exported out of the indoor monitor in batch on web **Security > Allowlist** interface.



Allowlist Import/Export

Auto Answer AllowList(.XML/.CSV) Not selected any files

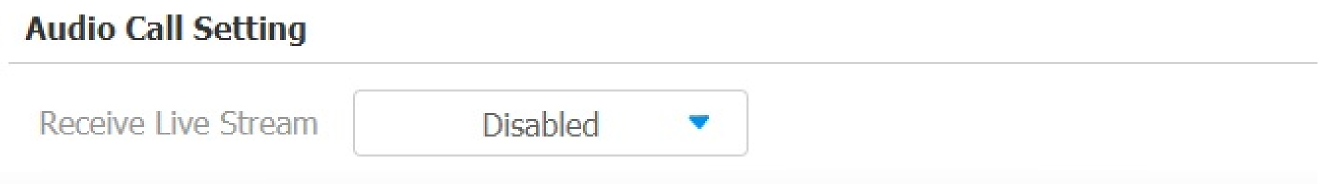
Note

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

Live Stream Setting

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

To do the configuration on web **Phone > Call Feature > Audio Call Settings** interface.



Audio Call Setting

Receive Live Stream: Disabled

When the feature is enabled, once a caller requires a video call:

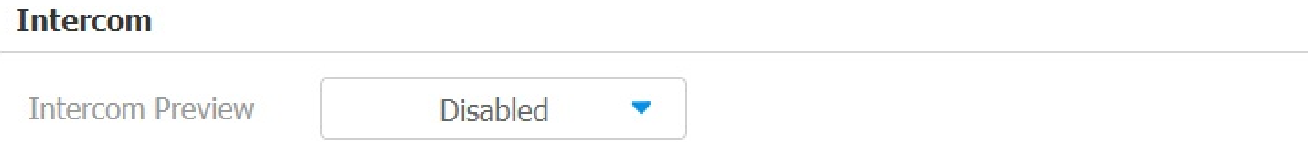
- Receive the incoming calls in video call mode so that both sides can see each while talking in the two-way video conversation.
- Receive the incoming calls in audio call so that you can see the caller in the one-way video conversation while the call can not see you.

Note

- Only devices with camera module will have this feature.

Intercom Call Configuration

If you want to see the image at the door station before answering the incoming call, you can enable the intercom preview function on web **Phone > Call Feature > Intercom** interface.



Intercom

Intercom Preview: Disabled

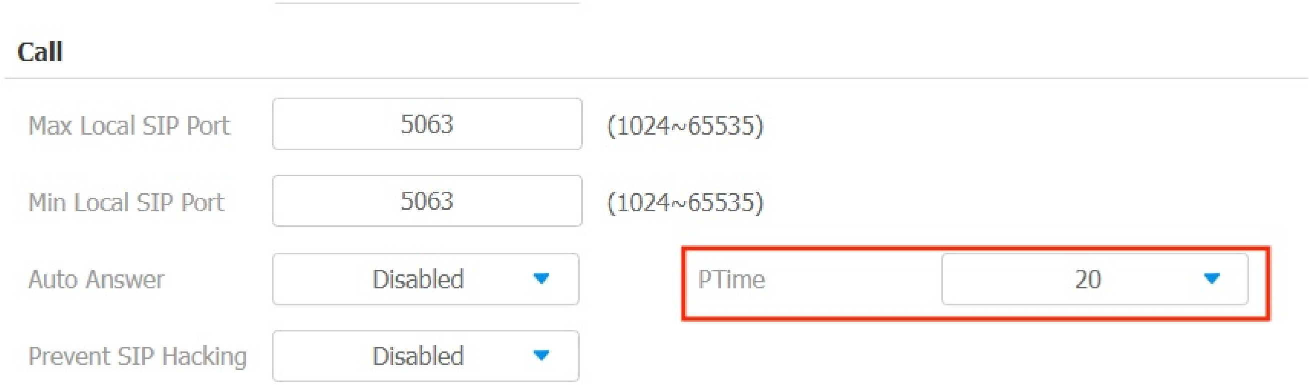
Parameter Set-up:

- **Intercom Preview**: enable the incoming call preview function.

PTime Configuration

Ptime gives the length of time in milliseconds represented by the media in a packet. The SDP in the INVITE request sent by the calling party carries the Ptime attribute, which indicates that the packing duration of the calling party's media is the value carried by Ptime. After receiving the request message, the server replies with the Ptime attribute in the SDP in 200 OK, indicating that the server-side support for the packaging time of the media is the value carried by Ptime. The caller negotiates according to the Ptime attribute carried in the SDP in the 200 OK, and finally sends the media package time, that is, the Ptime value.

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



Call

Max Local SIP Port: 5063 (1024~65535)

Min Local SIP Port: 5063 (1024~65535)

Auto Answer: Disabled

PTime: 20

Prevent SIP Hacking: Disabled

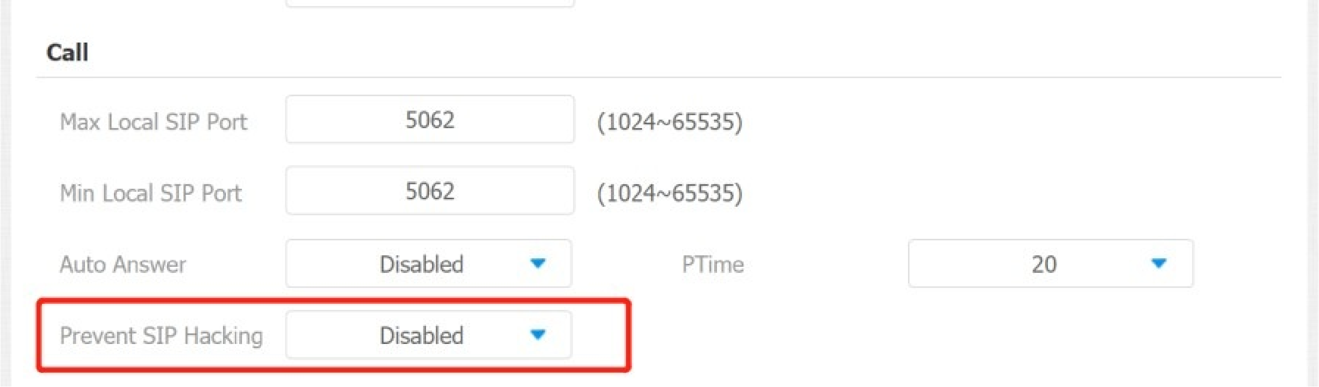
Parameter Set-up:

- **PTime**: you can disable the PTime feature. Or set up it from 10 to 60 seconds.

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 **Account > Advanced > Call** interface.



Call

Max Local SIP Port	5062	(1024~65535)		
Min Local SIP Port	5062	(1024~65535)		
Auto Answer	Disabled		PTime	20
Prevent SIP Hacking	Disabled			

Parameters Set-up:

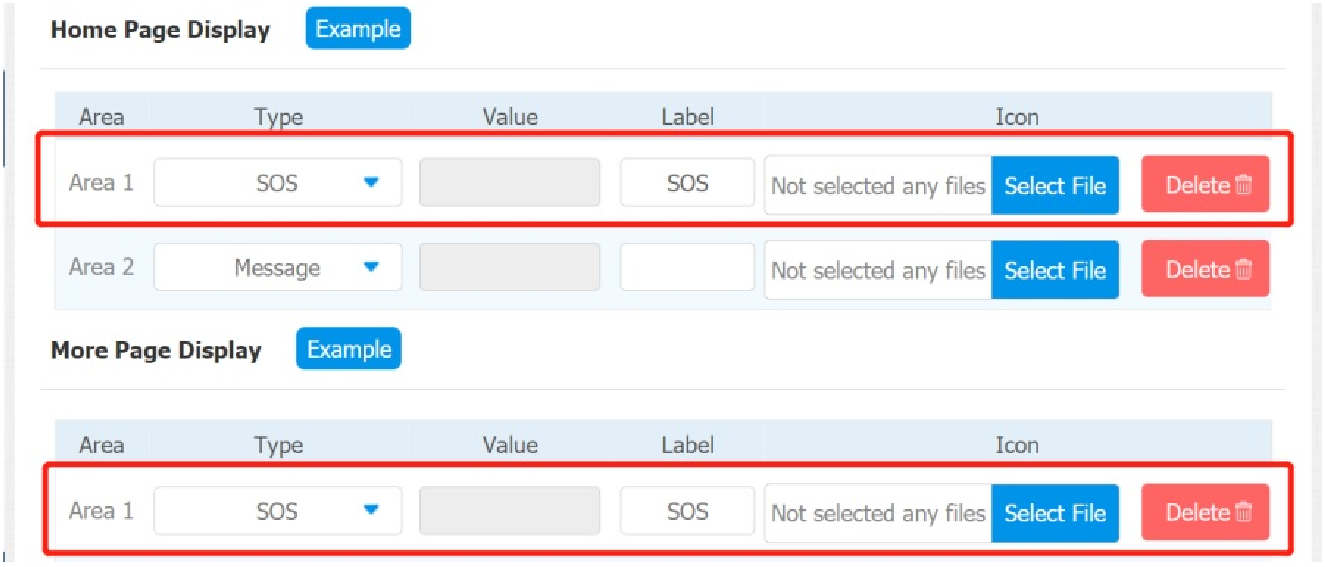
- **Prevent SIP Hacking**: enable to activate this feature during using sip call. This feature is only available for SIP calls.

Emergency Call Setting

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

SOS Number Display

To display SOS softkey on web **Phone > Key/Display > Home Page Display** interface. The icon will be shown in the main interface or more interface after configuring.



Home Page Display **Example**

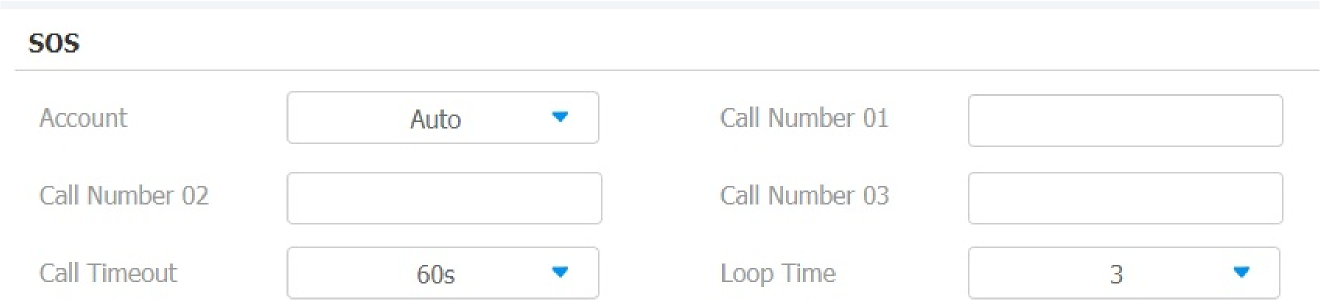
Area	Type	Value	Label	Icon	
Area 1	SOS		SOS	Not selected any files **Select File**	Delete
Area 2	Message			Not selected any files **Select File**	Delete

More Page Display **Example**

Area	Type	Value	Label	Icon	
Area 1	SOS		SOS	Not selected any files **Select File**	Delete

SOS Number Settings

To set up SOS numbers on device web **Phone** > **Intercom** interface.



SOS

Account	Auto	Call Number 01	
Call Number 02		Call Number 03	
Call Timeout	60s	Loop Time	3

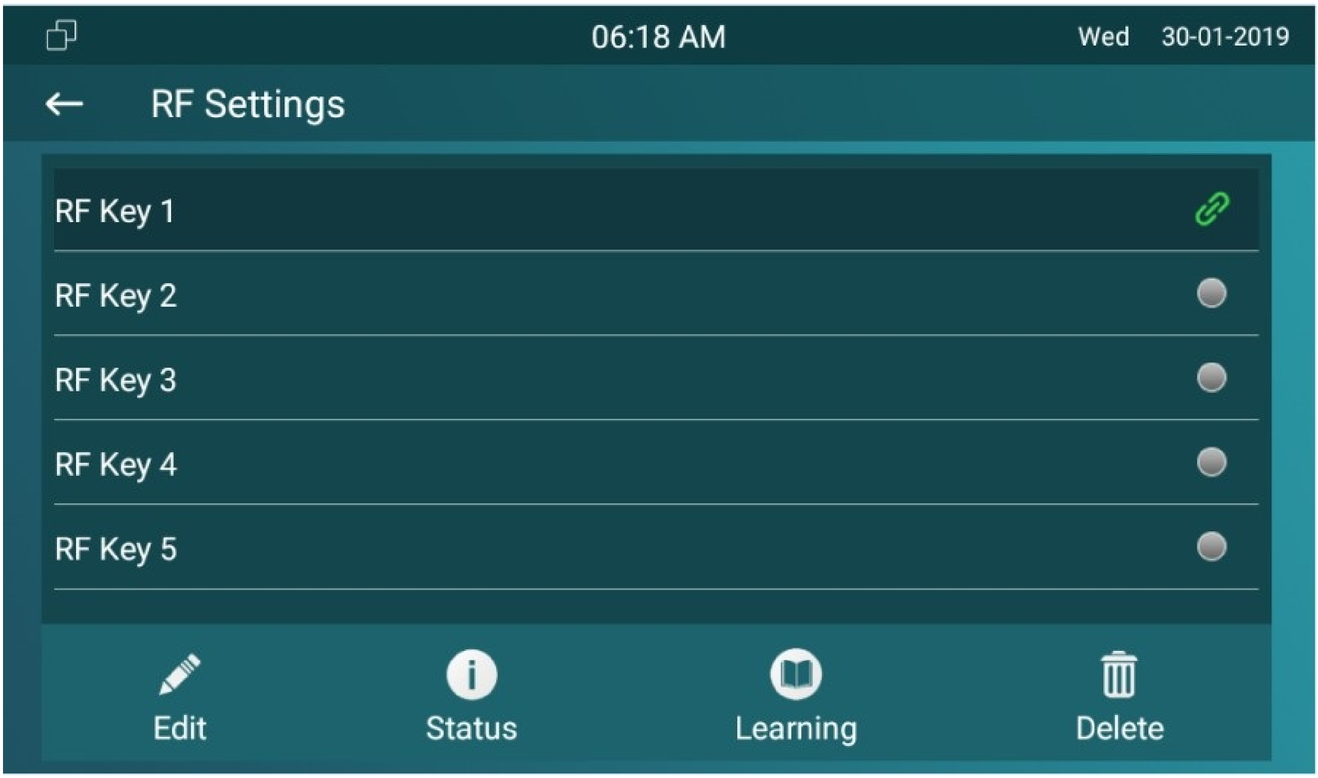
Parameter Set-up:

- **Account**: Select the account you want to make SOS from account 1 or account 2.
- **Call Number**: To set up 3 SOS numbers. Once users press SOS key on the home screen (SOS display key shall be set on the web manually), indoor monitors will call out the number in order.
- **Call Timeout**: Set up the timeout for each number. Once users call out, if the other side does not answer within the timeout, indoor monitors will continue to call the next number.
- **Loop Times**: To set up times of re-dialing.

RF Setting (Optional)

The indoor monior supports RF (Radio Frequency) module to connect a pendant to trigger some actions, like unlocking or making an emergency call. After pairing pendants and indoor monitors, then setup different RF actions on device. After powering on the pendant, click **Learning** and press pendant one time, they will be paired. The green indicator means pairing successfully.

To set it up on the device **Advance Settings** > **RF Settings** screen.



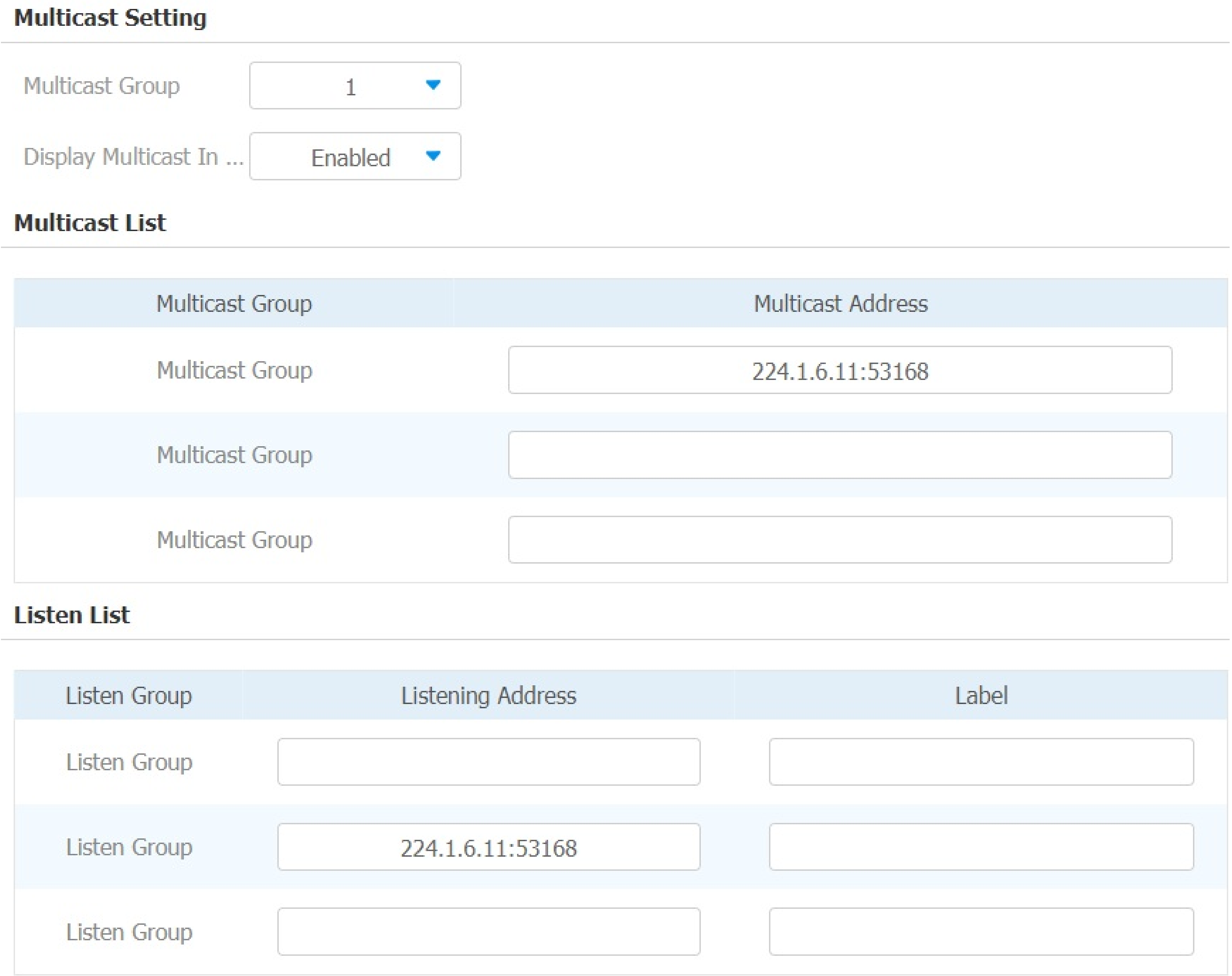
Parameters Set-up:

- **Short Press When Idle**: if you choose **Assistance Call** for short pressing, which means when you press the pendant for about 1s, the indoor monitor will make the pre-configured emergency call. **No Action** is default.
- **Long Press**: if you choose Unlock1/2/3 for long pressing, which means when you press the pendant for about 3s, it will send out an unlocking signal to the door phone during a call.

Multicast Configuration

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

To configure it on web **Phone** > **Multicast** interface.



Multicast Setting

Multicast Group: 1

Display Multicast In ...: Enabled

Multicast List

Multicast Group	Multicast Address
Multicast Group	224.1.6.11:53168
Multicast Group	
Multicast Group	

Listen List

Listen Group	Listening Address	Label
Listen Group		
Listen Group	224.1.6.11:53168	
Listen Group		

Parameter Set-up:

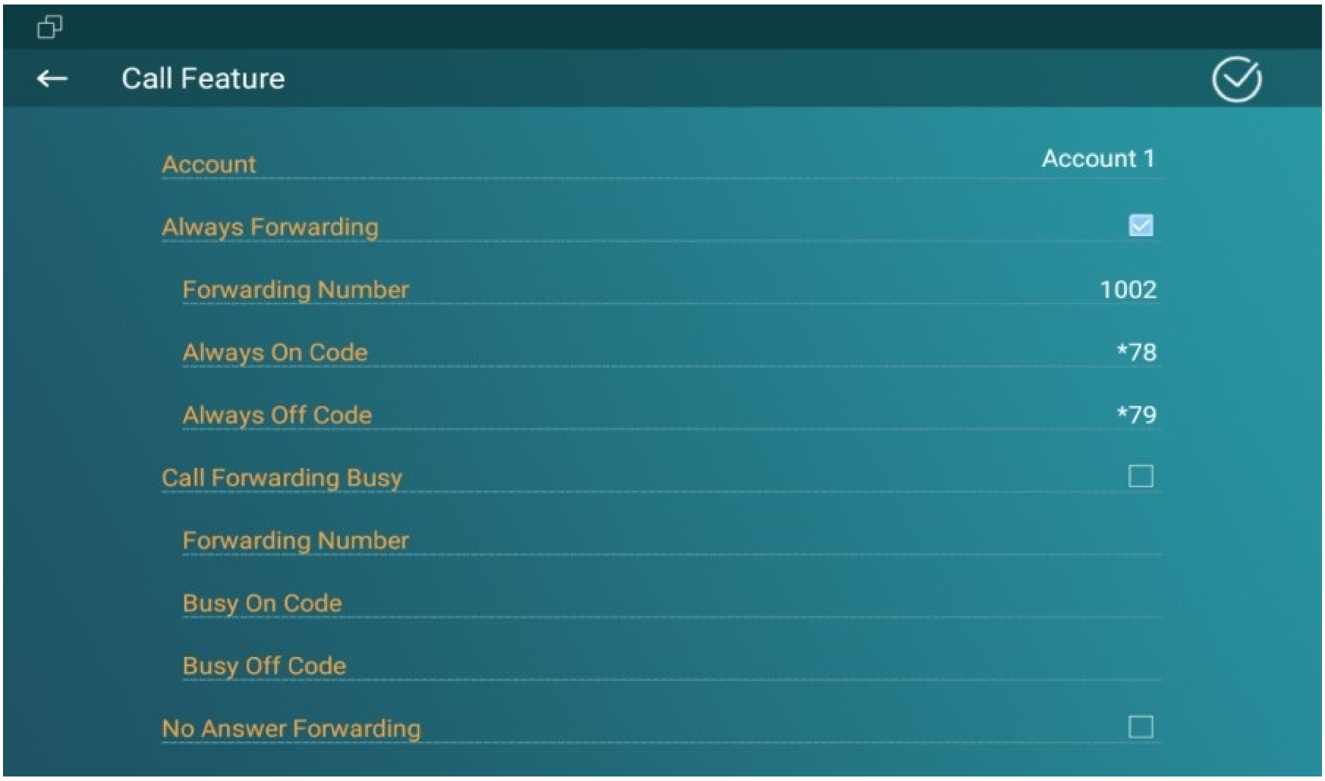
- **Multicast Group**: set the indoor monitor in one of the groups or disable this function.
- **Display Multicast In Homepage**: if you disable it, the **All Call** on the left side of the device screen will be hidden.
- **Multicast List**: to fill in the parameters of the multicast group. Indoor monitor will establish multicast calls to other indoor monitors which are set in the multicast group.
- **Listen List**: to fill in the parameters of listen group. Indoor monitor will receive multicast calls if some indoor monitors call the listening group.
- **Label**: to show the label name on the calling interface if users establish all calls.

Call Forwarding Setting

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

Call Forwarding Configuration on the Device

To do the configuration on the device **Settings** > **Call Feature** interface.



Account: Account 1

Always Forwarding ☑

Forwarding Number: 1002

Always On Code: *78

Always Off Code: *79

Call Forwarding Busy □

Forwarding Number

Busy On Code

Busy Off Code

No Answer Forwarding □

Parameter Set-up:

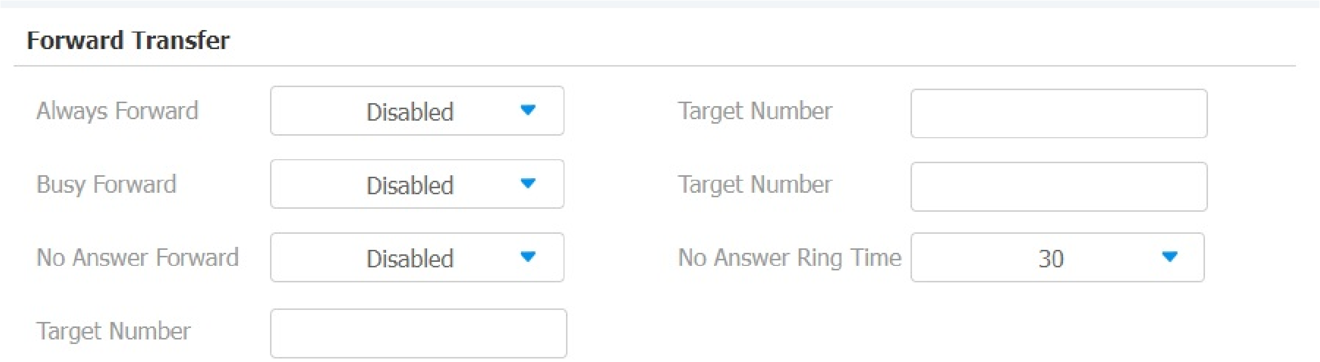
- **Account**: to choose which account to implement the call forwarding feature.
- **Always Forwarding**: all incoming calls will be automatically forwarded to a specific number.
- **Call Forwarding Busy**: incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forwarding**: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

- **Forwarding Number**: To enter the specific forward number if the device enables always forward/busy forward/no answer forward.

- **Capture Path**: select the storage location for all the captured pictures.

Call Forwarding Configuration on the Web Interface

To set up forward function on web **Phone > Call Feature > Forward Transfer** interface.



Forward Transfer

Always Forward	Disabled	Target Number	
Busy Forward	Disabled	Target Number	
No Answer Forward	Disabled	No Answer Ring Time	30
Target Number			

Parameter Set-up:

- **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 device is not picked up within no answer ring time.
- **Target Number**: to enter the specific forward number if the device enables always forward/busy forward/no answer forward.
- **No Answer Ring Time**: set the number of seconds to wait for call pick-up before transferring to a designated number (0-120 seconds).

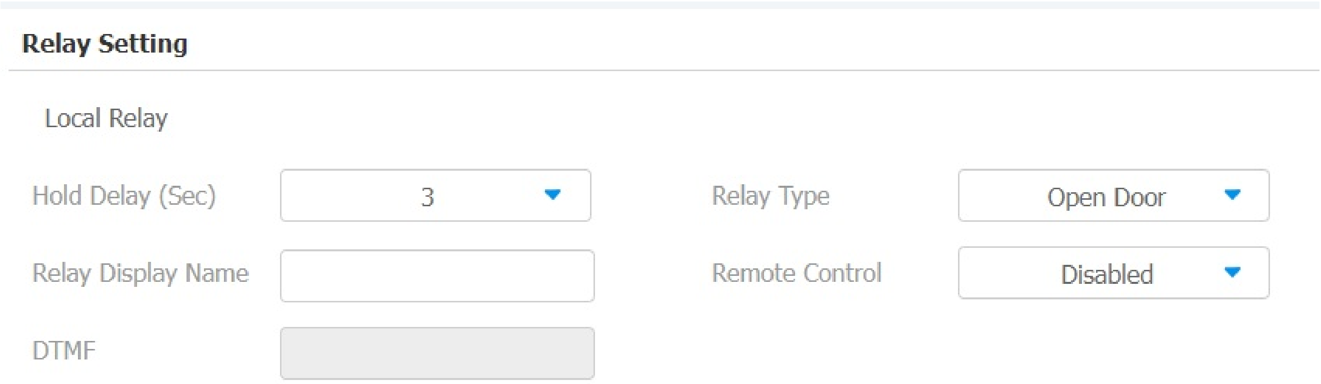
Door Access Control Configuration

Relay Switch Setting

Local Relay Setting

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

You can do this configuration on web **Phone > Relay > Relay Setting > Local Relay** interface.



Relay Setting

Local Relay

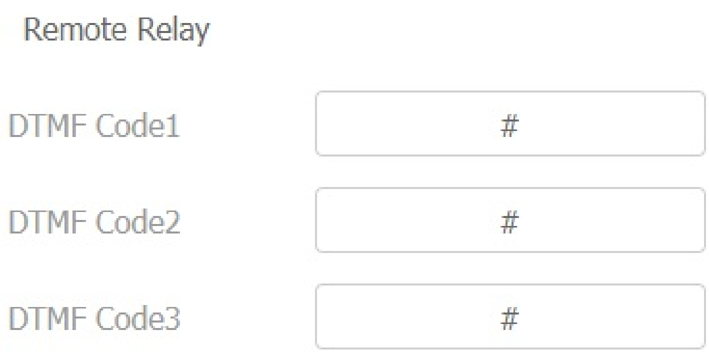
Hold Delay (Sec)	3	Relay Type	Open Door
Relay Display Name		Remote Control	Disabled
DTMF			

Parameter Set-up:

- **Hold Delay (Sec)**: set the relay hold delay timing (Ranging from 0-60 Sec). For example, if you set the hold delay time as 5 Sec. Then the relay will be delayed for 5 seconds after the door is unlocked.
- **Relay Display Name**: name the relay switch according to your need. For example, you can name the relay switch according to where it is located for convenience.
- **DTMF**: Set the DTMF code for the local relay.
- **Relay Type**: Set relay action type. There are three options, chime bell, open door, and other switches(reset by event).
  - **Chime Bell**: when there is a call, the chime bell will ring.
  - **Open Door**: when pressing the unlock icon, the local relay will be opened.
  - **Other Switches(Reset By Event)**: when the call is answered, the relay will be reset.

Remote Relay Switch Setting

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



Remote Relay

DTMF Code1	#
DTMF Code2	#
DTMF Code3	#

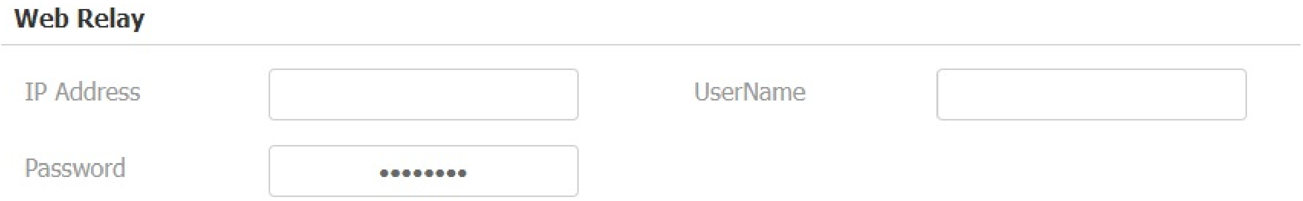
Parameter Set-up:

- **DTMF Code**: to set DTMF code for the remote relay, which is **#** by default.

Web Relay Setting

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

To do this configuration on web **Phone > Relay > Web Relay** interface. **IP Address, User Name**, and **Password** are provided by the web relay service provider.



Web Relay

IP Address		UserName	
Password	••••••••		

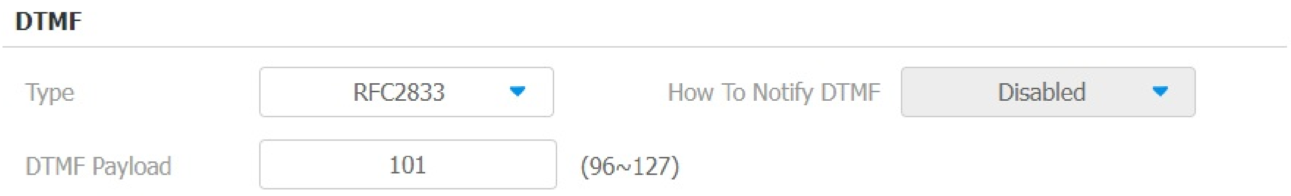
Parameter Set-up:

- **Password**: the passwords are authenticated via HTTP and you can define the passwords using HTTP Get in Action.
- **Web Relay Action**: enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.

Door Unlock Configuration

Door Unlock by DTMF Code

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



DTMF

Type: RFC2833
How To Notify DTMF: Disabled
DTMF Payload: 101 (96~127)

Parameter Set-up:

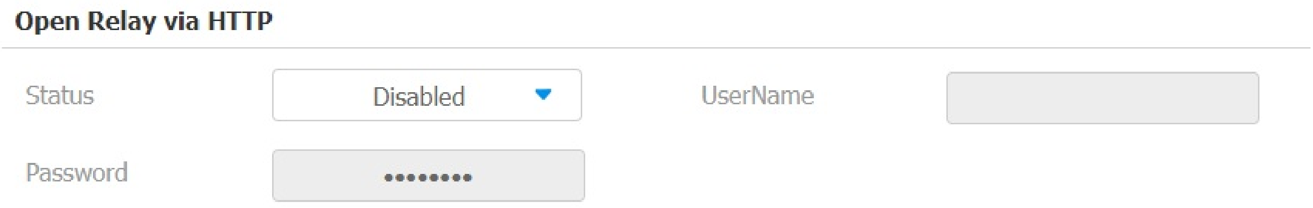
- **Type**: select DTMF type among **Inband**, **RFC2833**, **Info**, **Info+Inband** and **Info+RFC2833** according to your need.
- **How to Notify DTMF**: select among four options: **Disable**, **DTMF**, **DTMF-Relay**, and **Telephone-Event** according to your need.
- **DTMF Payload**: select the payload (96-127) for data transmission identification.

> **Note**
>
> - Please refer to Relay Switch Setting for the specific DTMF code setting. Intercom devices involved must be consistent in the DTMF type, otherwise, DTMF code cannot be applied.

Door Unlock via HTTP Command

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

To do this configuration on web interface **Phone > Relay > Open Relay via HTTP**.


Open Relay via HTTP

Status: Disabled

UserName:

Password: ••••••••

Parameter Set-up:

- **Status**: enable it to allow the relay to be triggered remotely using the HTTP command.
- **Username**: enter the device username to be used as a part of the HTTP command to trigger the local relay.
- **Password**: enter the device password to be used as part of the HTTP command to trigger the local relay.

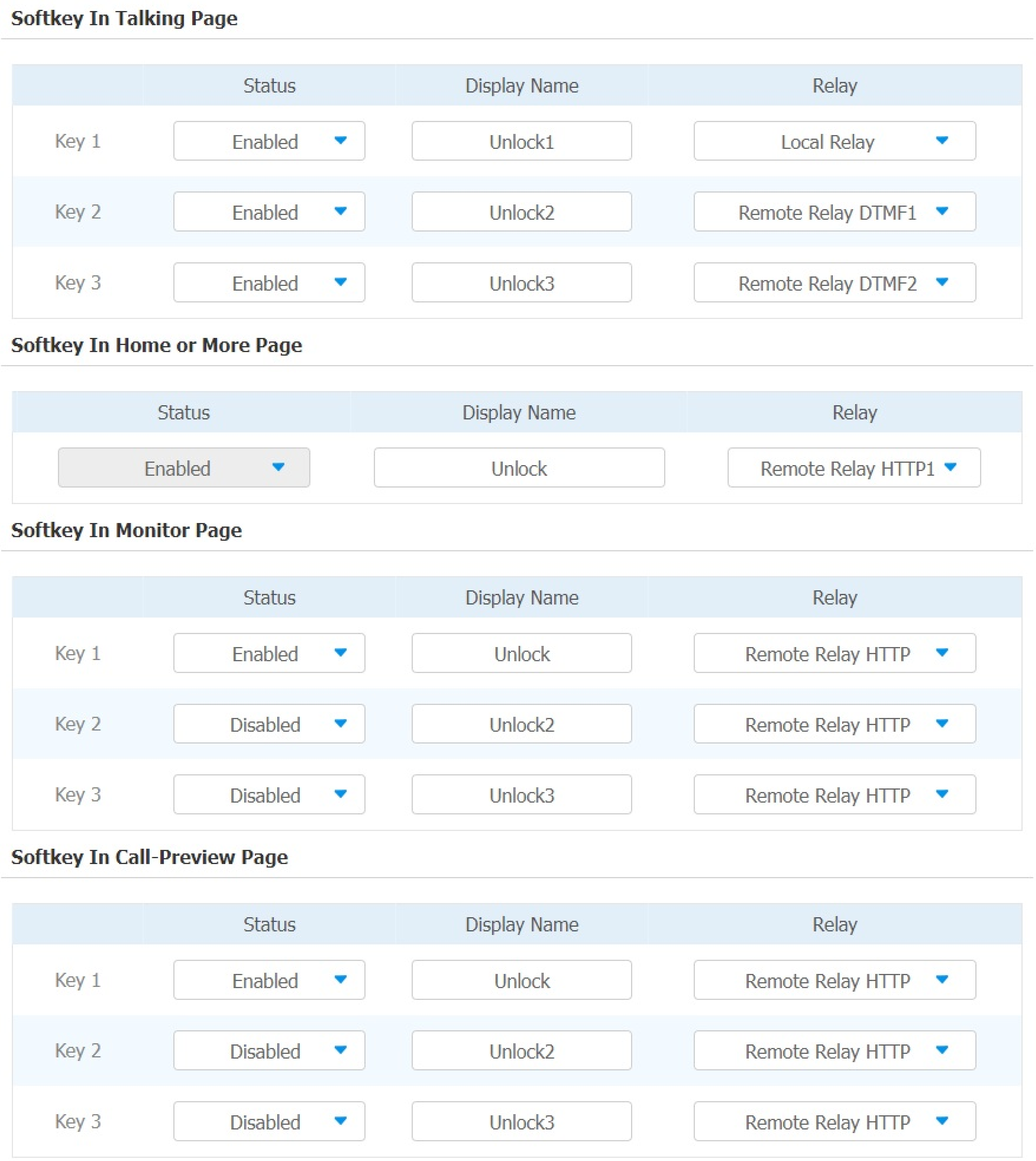
  Please refer to the following example: http://192.168.35.127/ fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note

- DoorNum in the HTTP command above refers to the relay number #1 to be triggered.

Unlock by Icon Button

To set up the unlock key for unlocking on web interface **Phone > Relay.**



Softkey In Talking Page

	Status	Display Name	Relay
Key 1	Enabled	Unlock1	Local Relay
Key 2	Enabled	Unlock2	Remote Relay DTMF1
Key 3	Enabled	Unlock3	Remote Relay DTMF2

Softkey In Home or More Page

Status	Display Name	Relay
Enabled	Unlock	Remote Relay HTTP1

Softkey In Monitor Page

	Status	Display Name	Relay
Key 1	Enabled	Unlock	Remote Relay HTTP
Key 2	Disabled	Unlock2	Remote Relay HTTP
Key 3	Disabled	Unlock3	Remote Relay HTTP

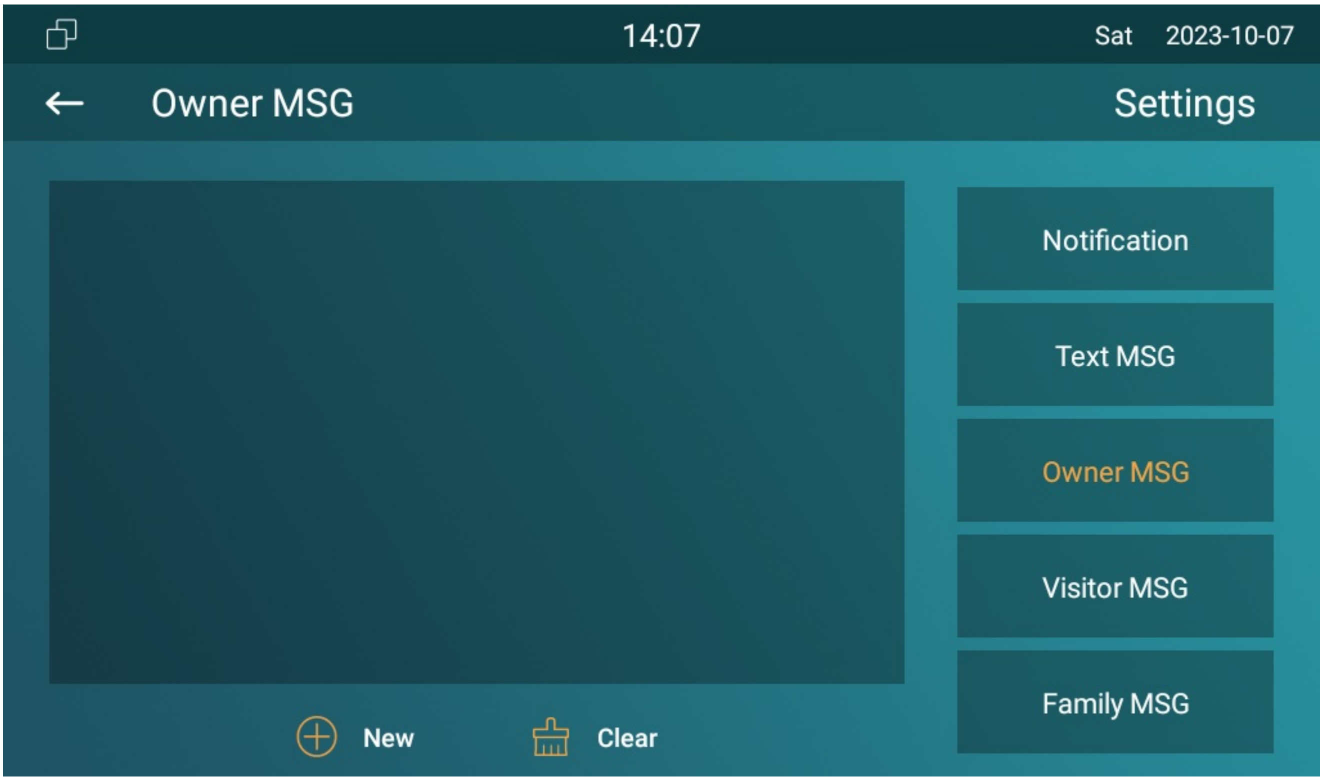
Softkey In Call-Preview Page

	Status	Display Name	Relay
Key 1	Enabled	Unlock	Remote Relay HTTP
Key 2	Disabled	Unlock2	Remote Relay HTTP
Key 3	Disabled	Unlock3	Remote Relay HTTP

Intercom Message Setting

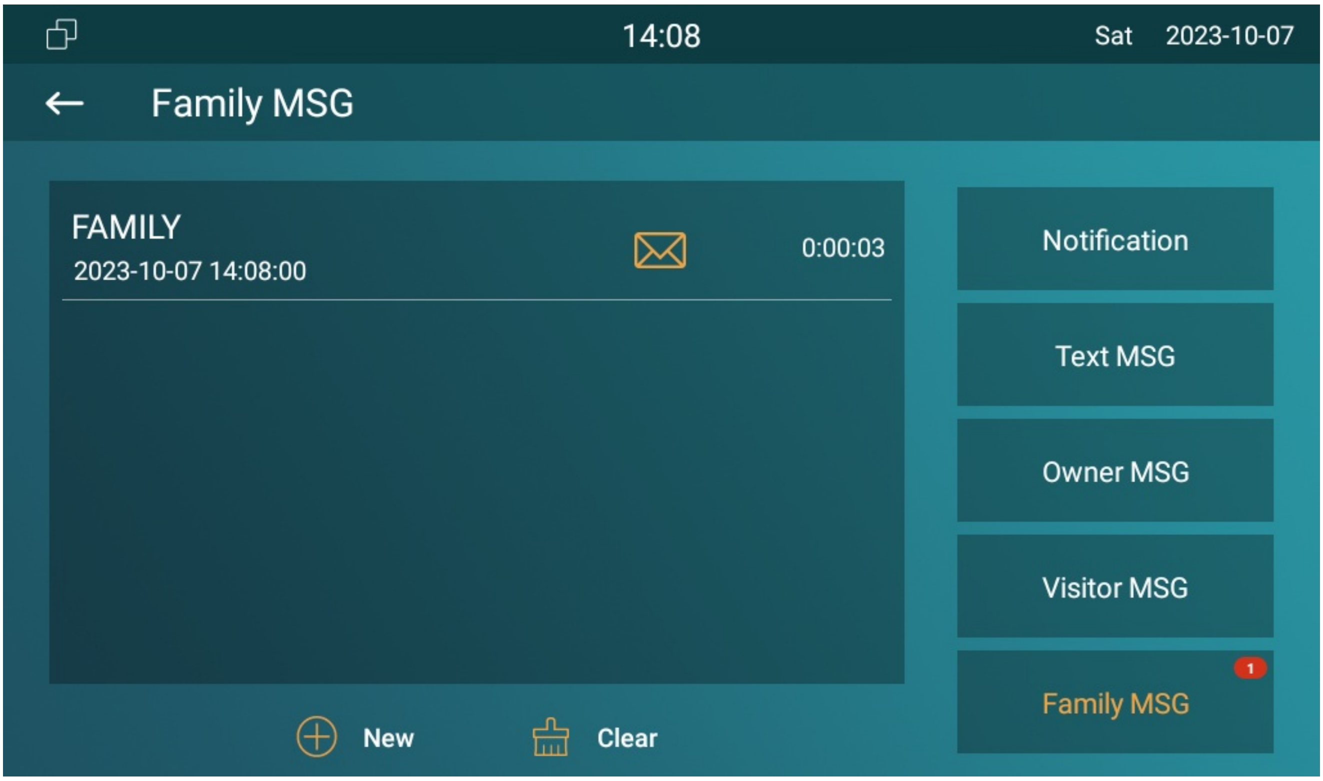
Manage Text Messages

You can check, create and clear messages as needed on the indoor monitor **Messages** screen. Click **New** to create a new text message and **Clear** icon to delete the existing messages.



Manage Voice Messages

You can create, delete and view the audio messages recorded by family members on the device screen **Messages > Family MSG**.



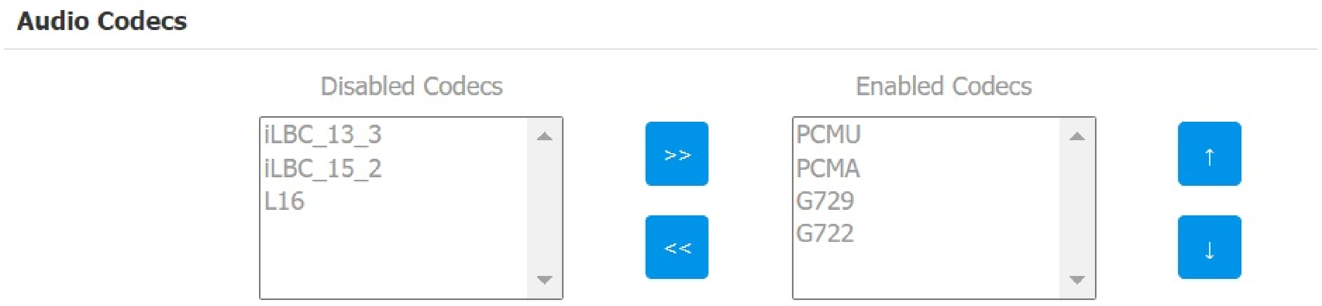
FAMILY
2023-10-07 14:08:00
0:00:03

Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

The device supports seven types of Codec (iLBC_13_3, iLBC_15_2, L16, PCMU, PCMA, G729, and G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To do the configuration on web **Account > Advanced > Audio Codecs** interface.

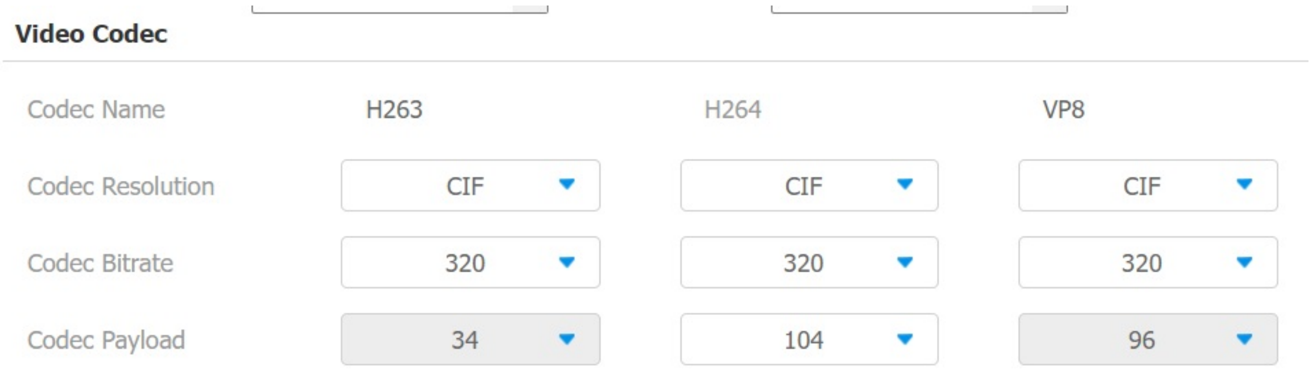


Please refer to the bandwidth consumption and sample rate for the codecs types below:

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
L16	128 kbit/s	variable

Video Codec Configuration

C315 series supports VP8, H263, H264, H265 codec that provides a better video quality at a much lower bit rate with different video quality and payload. To do the configuration on web **Account > Advanced > Video Codecs** interface. Choose an available video codec and set up the codec parameters.



Video Codec

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

Parameter Set-up:

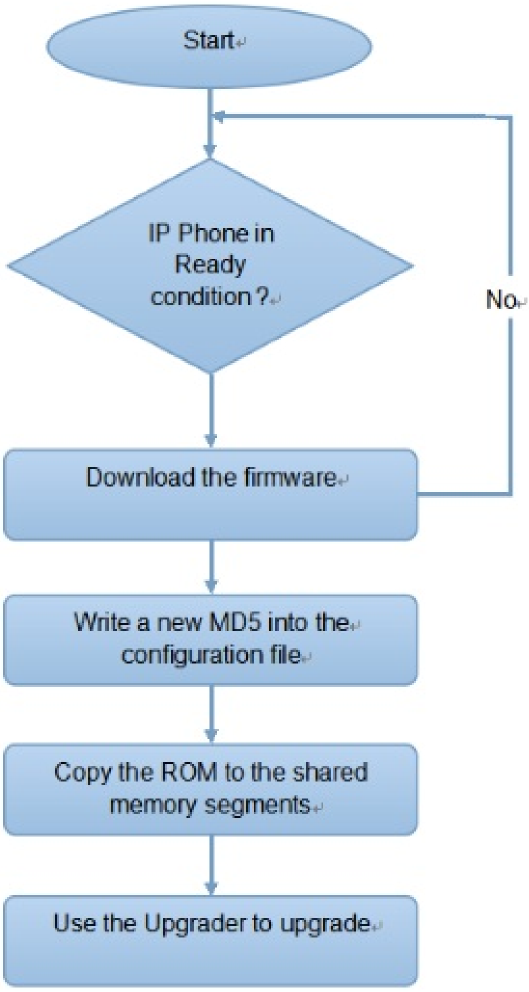
- **Codec Resolution**: select the codec resolution for the video quality among five options: **QCIF, CIF, VGA, 4CIF** and **720P** according to your actual network environment. H263 only has **QCIF, CIF, 4CIF**.
- **Codec Bitrate**: select the video stream bit rate (ranging from 128-512). The greater the bitrate, the data transmitted every second is greater in amount. Therefore, the video will be clearer.
- **Payload**: select the payload type (ranging from 90-119) to configure the audio/video configuration file. The default payload is **104**.

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

The difference between the two types of configuration files:

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

Note

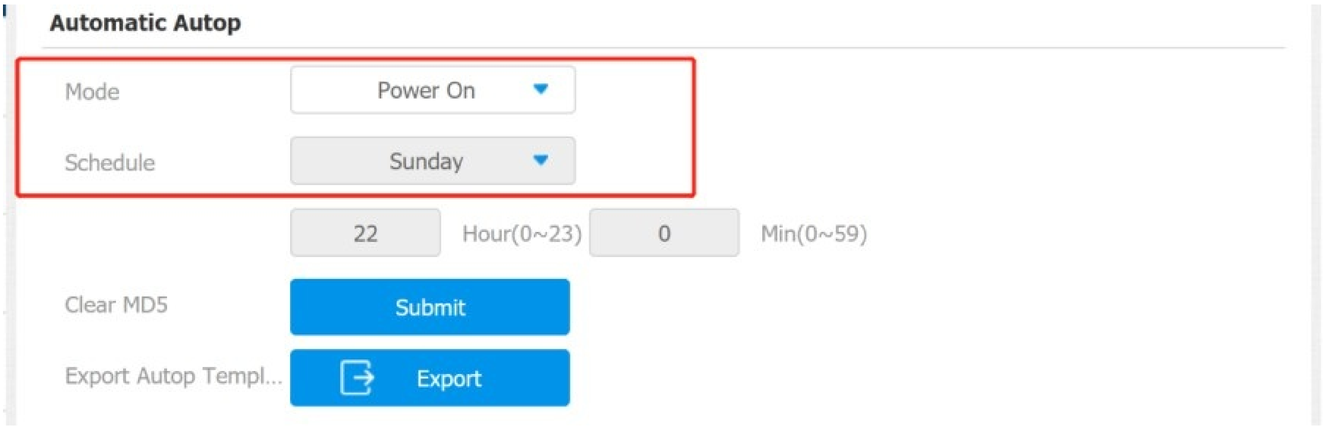
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will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

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

Autop Schedule

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

To set up the schedule on the device web **Upgrade > Advanced > Automatic Autop** interface.



Automatic Autop

Mode: Power On

Schedule: Sunday

22 Hour(0~23) 0 Min(0~59)

Clear MD5: Submit

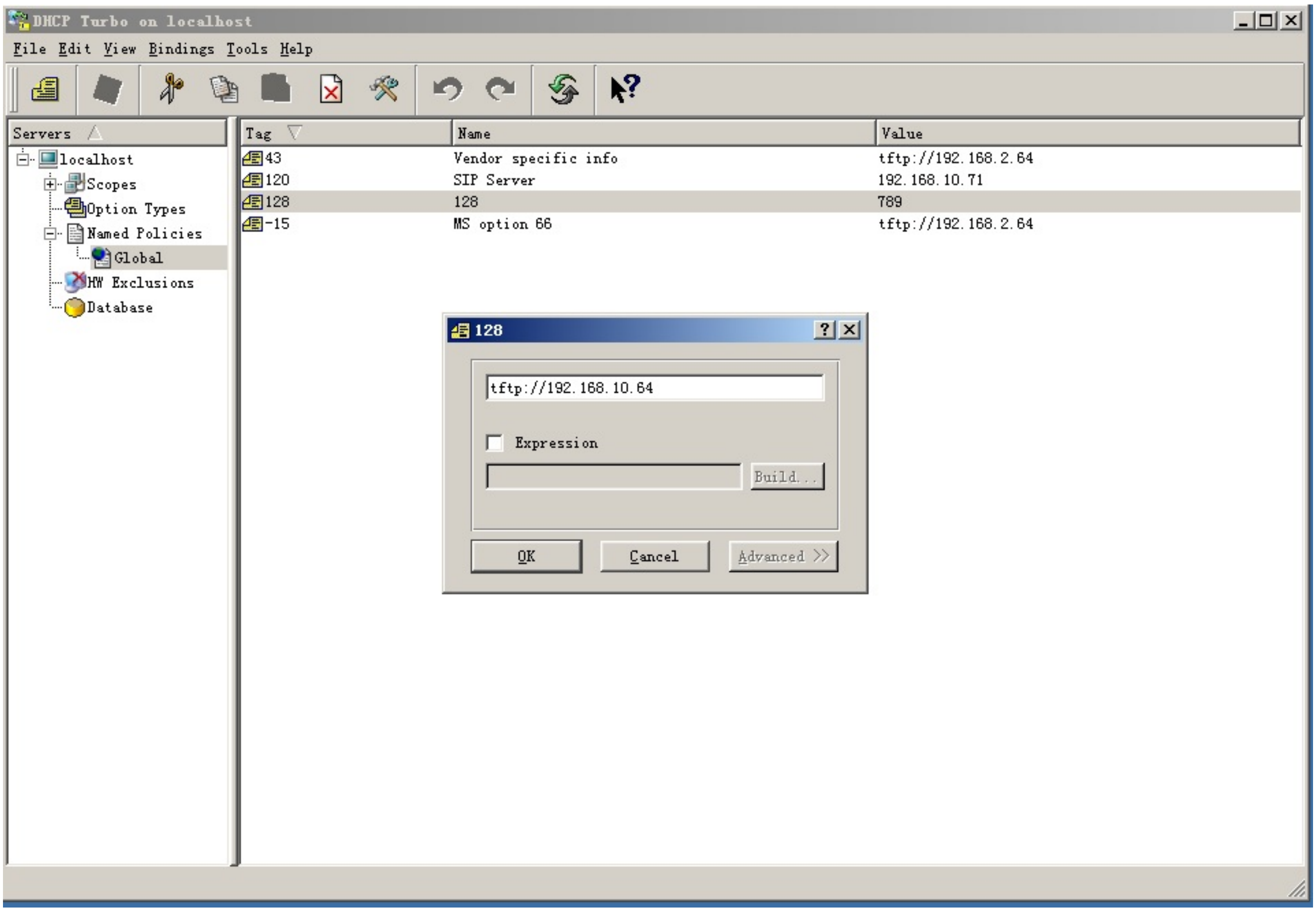
Export Autop Templ...: Export

Parameter Set-up:

- **Power On**: select **Power on** if you want the device to perform Autop every time it boots up.
- **Repeatedly**: select **Repeatedly** if you want the device to perform Autop according to the schedule you set up.
- **Power On + Repeatedly**: select **Power On + Repeatedly** if you want to combine these two modes that will enable the device to perform Autop every time it boots up or according to the schedule you set up.
- **Hourly Repeat**: select **Hourly Repeat** if you want the device to 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

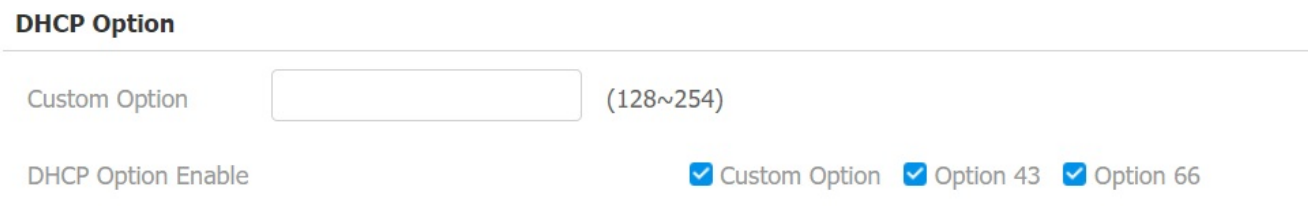
tftp://192.168.10.64

□ Expression

Note

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

Navigate to **Upgrade > Advanced > DHCP Option** interface.



DHCP Option

Custom Option (128~254)

DHCP Option Enable ☑ Custom Option ☑ Option 43 ☑ Option 66

Parameter Set-up:

- **Custom Option**: enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.

- **DHCP Option 66**: if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgraded 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 updated server URL in it.

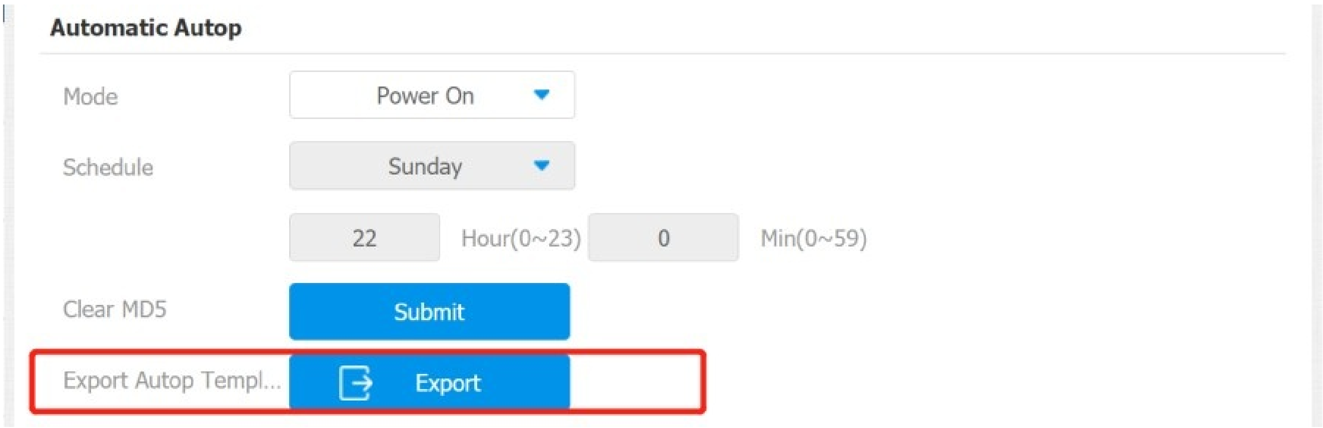
- **DHCP Option 43**: if the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

> **Note**
>
> - The general configuration file for the in-batch provisioning is with the format cfg taking R29 as an example r000000000029.cfg (10 zeros in total), while the MAC- based configuration file for the specific device provisioning is with the format MAC_Address of the device.cfg, for example, **0C110504AE5B.cfg**.

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 on **Upgrade > Advanced > Automatic Autop** , and set up the Auto-provisioning server on **Upgrade > Advanced > Manual Autop** interface.



Automatic Autop

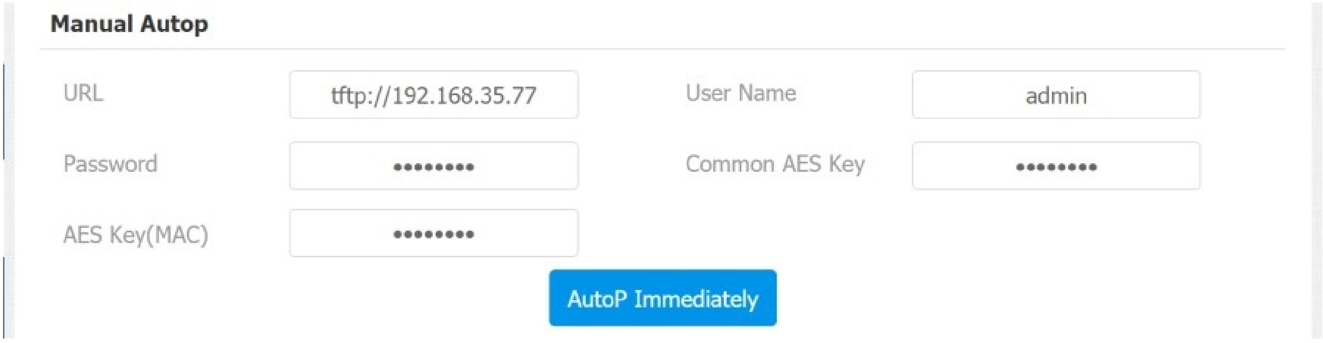
Mode: Power On

Schedule: Sunday

22 Hour(0~23) 0 Min(0~59)

Clear MD5: Submit

Export Autop Templ...: Export



Manual Autop

URL: tftp://192.168.35.77

User Name: admin

Password: ••••••••

Common AES Key: ••••••••

AES Key(MAC): ••••••••

Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, and FTP server address for the provisioning.
- **User Name**: set up a username if the server needs a username to be accessed to.
- **Password**: set up a password if the server needs a password to be accessed to.
- **Common AES Key**: set up AES code for the intercom to decipher general Auto-provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based Auto-provisioning 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 do not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

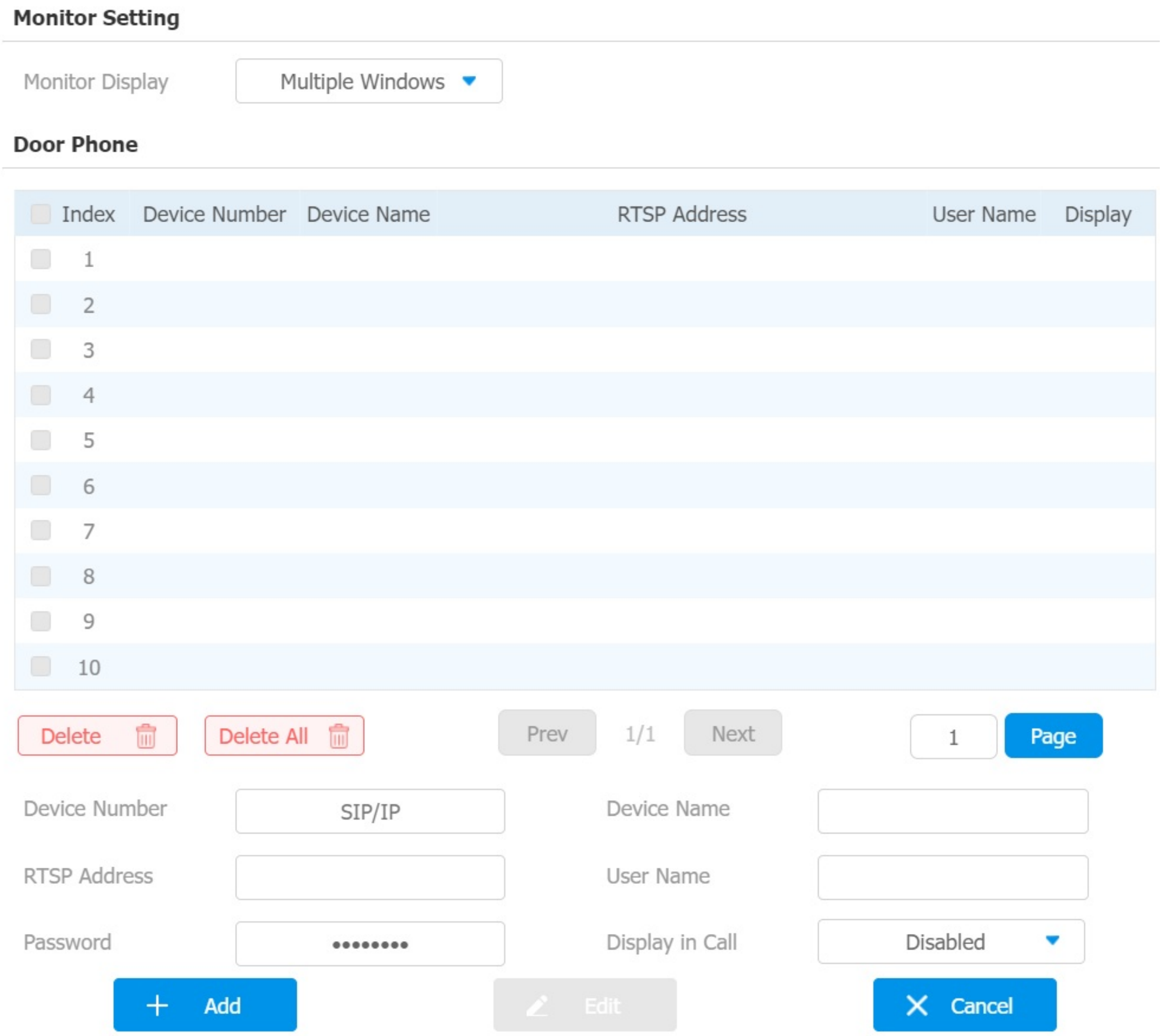
Security

Monitor and Image

Monitor Setting

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

Navigate to the web **Phone** > **Monitor** interface.



Monitor Setting

Monitor Display: Multiple Windows

Door Phone

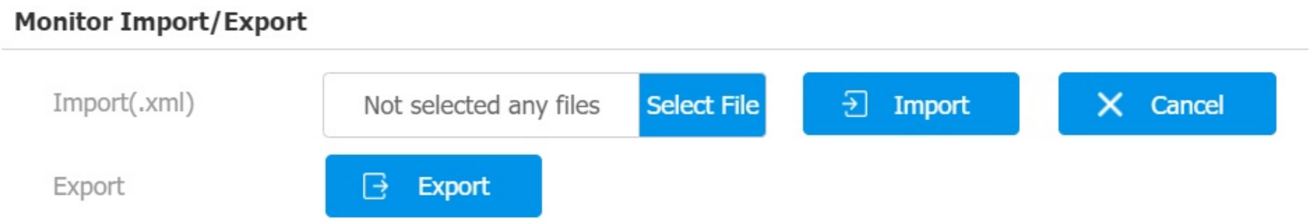
□	Index	Device Number	Device Name	RTSP Address	User Name	Display
□	1					
□	2					
□	3					
□	4					
□	5					
□	6					
□	7					
□	8					
□	9					
□	10					

Device Number	SIP/IP	Device Name	
RTSP Address		User Name	
Password	••••••••	Display in Call	Disabled

Parameter Set-up:

- **Monitor Display**: select **Multiple Window** if you want to display four video monitoring channels on the screen. Select **Single Window** if you want to display only one video monitoring channel.
- **Device Number**: type in the monitored device number for identification.
- **Device Name**: type in the device name for identification.
- **RTSP Address**: type in the RTSP address of the monitored device. RTSP format: rtsp://Device IP address/live/ch00_0.
- **Username**: type in the username of the monitored device for monitoring authentication.
- **Password**: type in the password of the monitored device for monitoring authentication.
- **Display In Call**: enable it if you want to display the monitoring video when you are in the call.

You can import and export the monitored device setting via a template in .xml format.

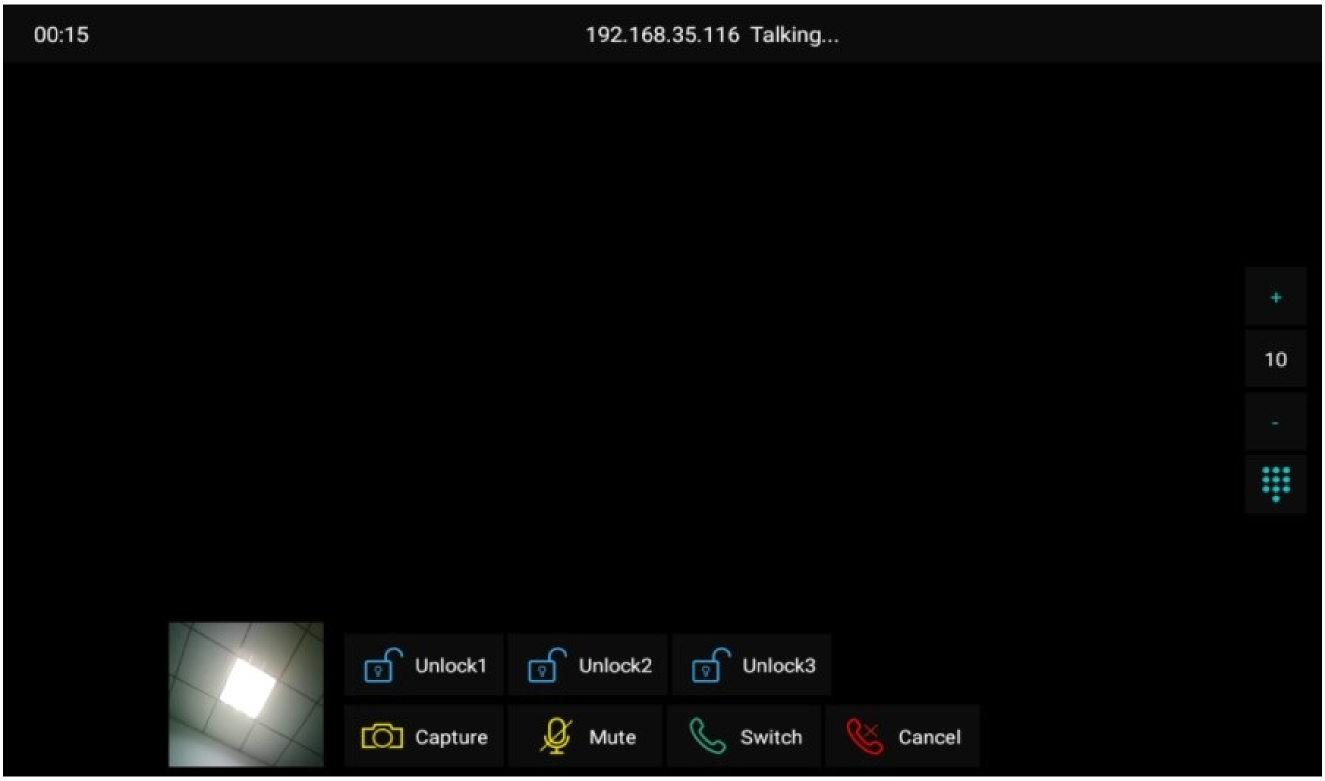

Monitor Import/Export

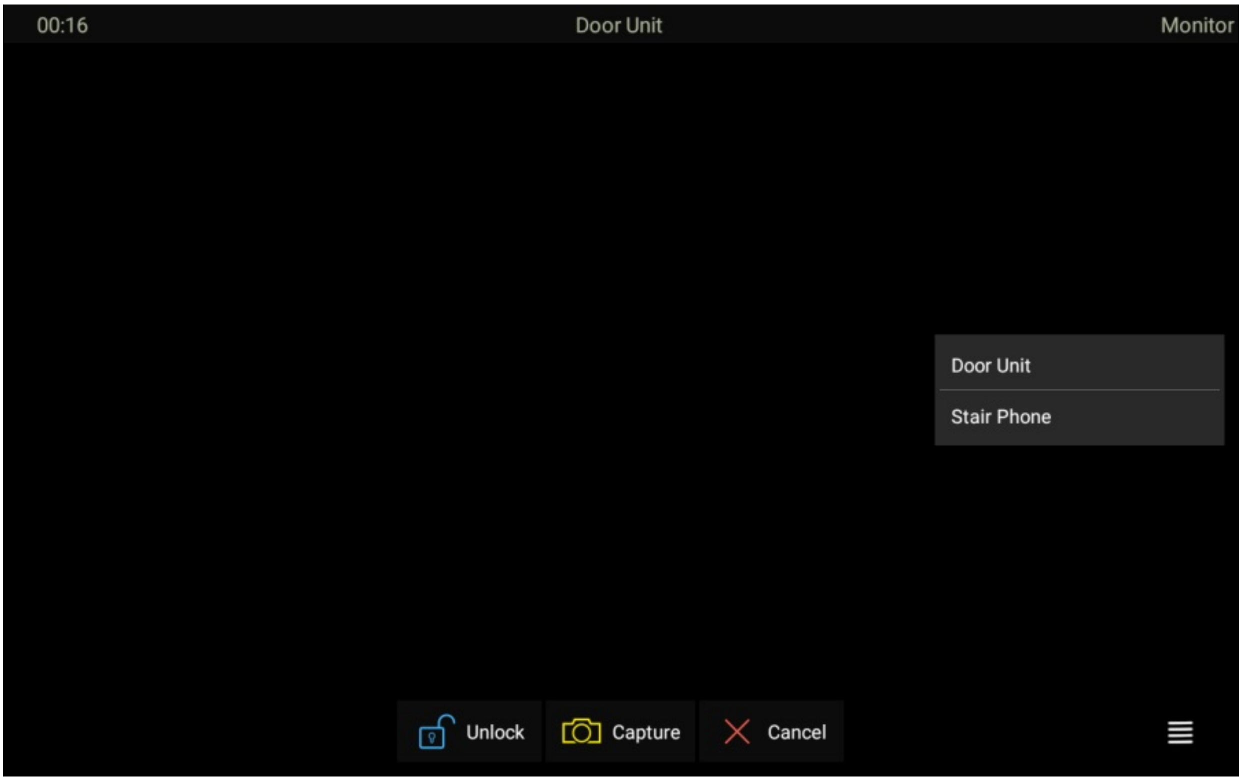
Import(.xml) Not selected any files

Export

Video Image Capturing

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

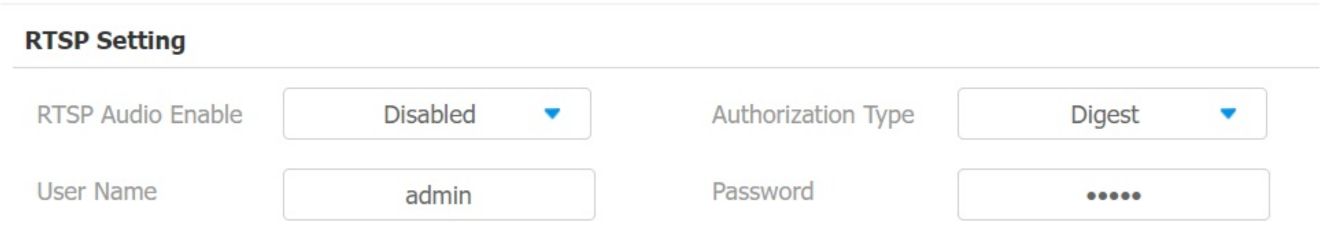




RTSP Authentication

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

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



RTSP Setting

RTSP Audio Enable	Disabled	Authorization Type	Digest
User Name	admin	Password	•••••

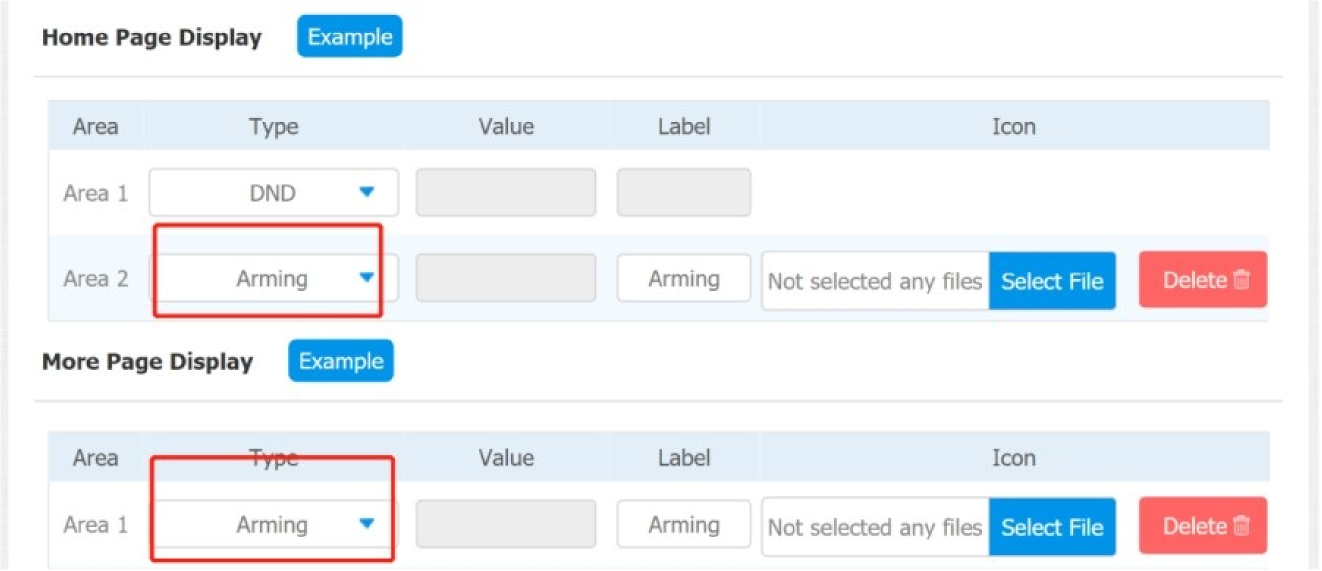
Parameter Set-up:

- **Authorization Type**: select the authorization type (**Basic, Digest**). Select **None** if you allow all types of authorization types for the RTSP audio stream.
- **User Name**: type in the username used for the authentication.
- **Password**: type in the password used 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.

To configure the **Arming** icon on the web **Phone > Key/Display** interface.



Home Page Display Example

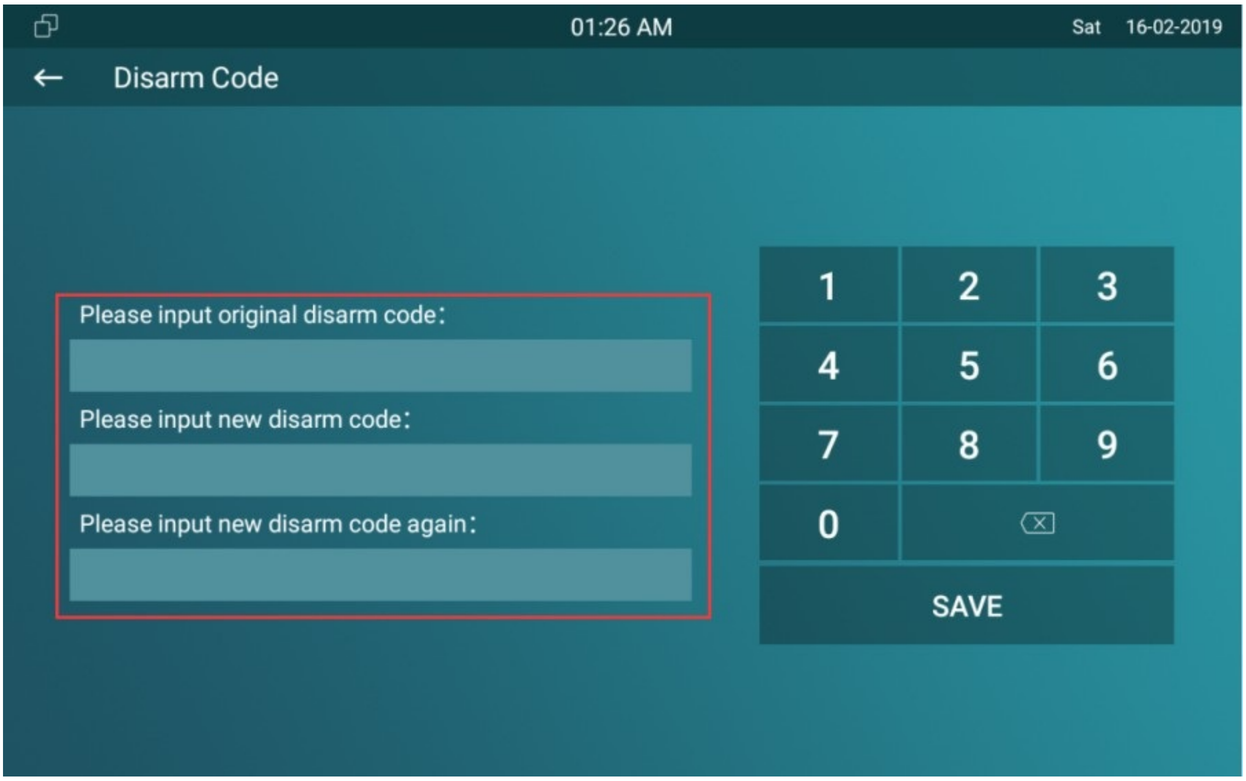
Area	Type	Value	Label	Icon
Area 1	DND			
Area 2	Arming		Arming	Not selected any files Select File Delete

More Page Display Example

Area	Type	Value	Label	Icon
Area 1	Arming		Arming	Not selected any files Select File Delete

Configure Alarm and Arming on the Device

To configure the arming and disarm code on device **Arming** screen. Change the current password and save it.



01:26 AM Sat 16-02-2019

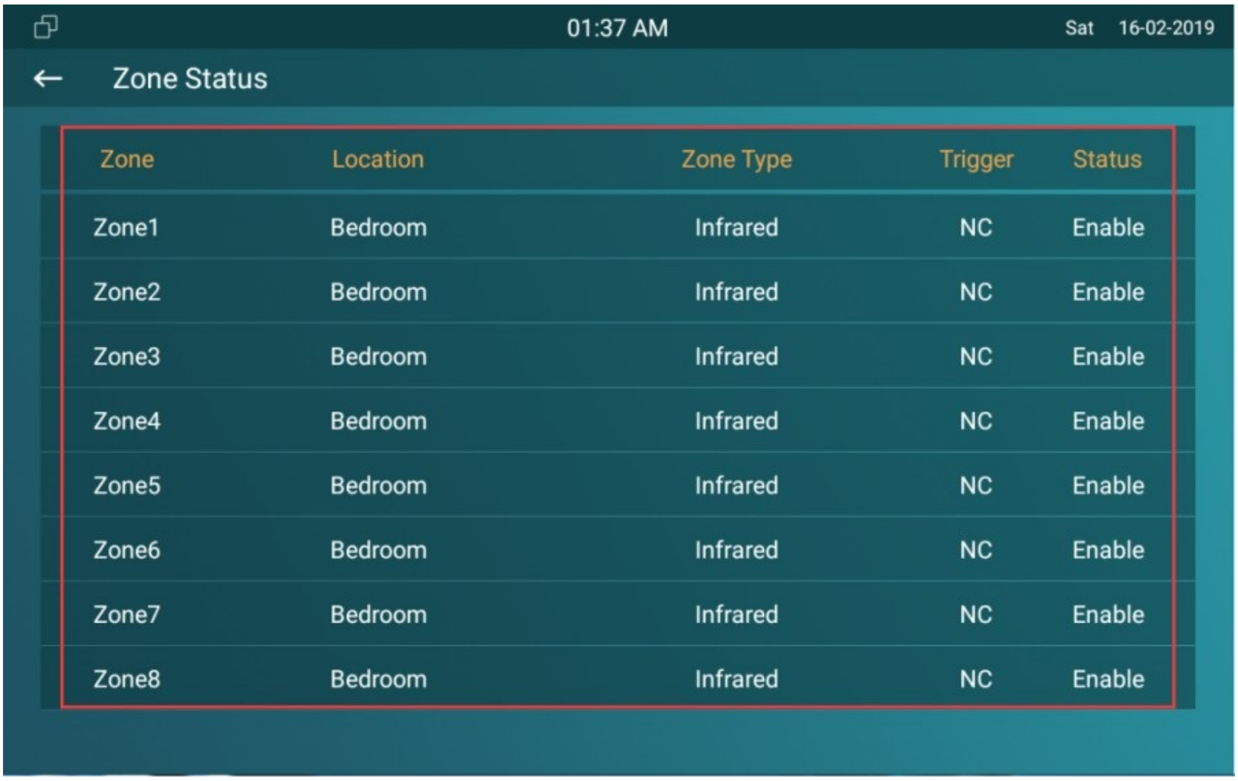
Disarm Code

Please input original disarm code：

Please input new disarm code：

Please input new disarm code again：

To check the zone status on **Arming > Zone Status** screen.



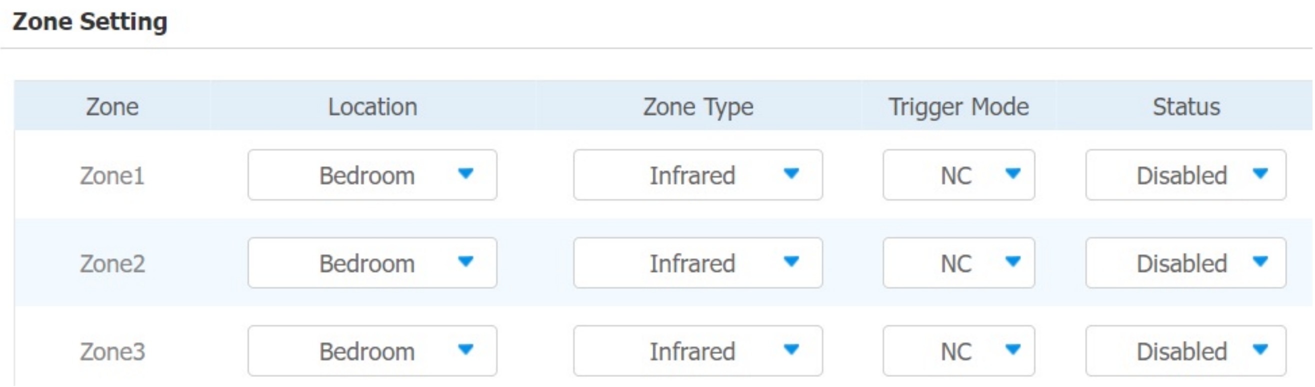
01:37 AM Sat 16-02-2019

Zone Status

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

Configure Alarm and Arming on the Web Interface

To set up a location-based alarm sensor on the device 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

Parameter Set-up:

- **Location**: set up the location according to where the alarm sensor is stalled. You can select among ten location types: **Bedroom, Gate, Door, Guest Room, Hall, Window, Balcony, Kitchen, Study**, and **Bathroom**.

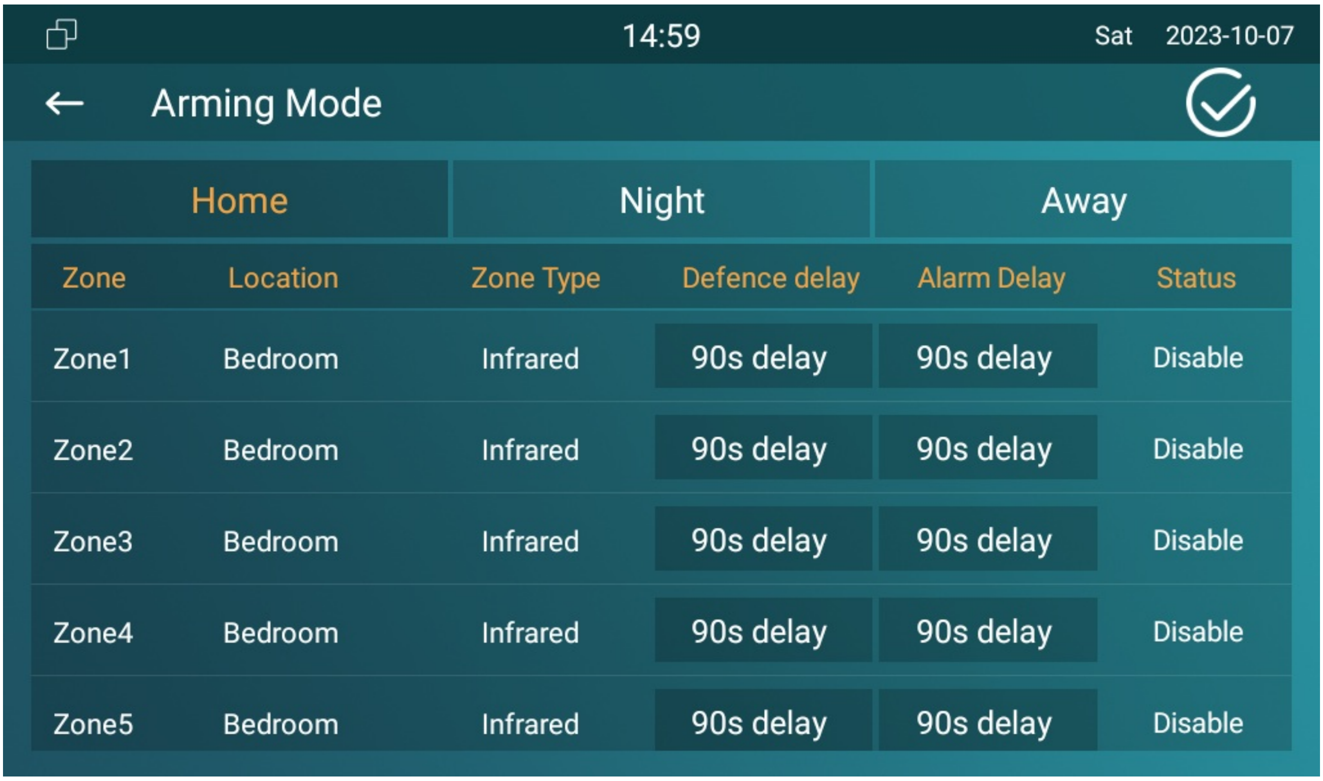
- **Zone Type**: set up the alarm sensor types (**Infrared, Drmagnet, Smoke, Gas**, and **Urgency**).

- **Trigger Mode**: set sensor trigger mode between **NC** and **NO** according to your need.

- **Status**: set the alarm sensor status among three options: **Enabled, Disabled**, and **24H**. Select **Enabled** if you want to enable the alarm, however, you are required to set the alarm again after an alarm is disarmed. Select **Disabled** if you want to disable the alarm, and select **24H** if you want the alarm sensor to stay enabled for 24 hours without needing to set up the alarm manually again after the alarm is disarmed.

Configure Location-based Alarm

Configure the alarm sensor in the same way as you do on the web interface on the **Arming > Arming Mode** screen.



14:59 Sat 2023-10-07

Arming Mode

Home | Night | Away

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

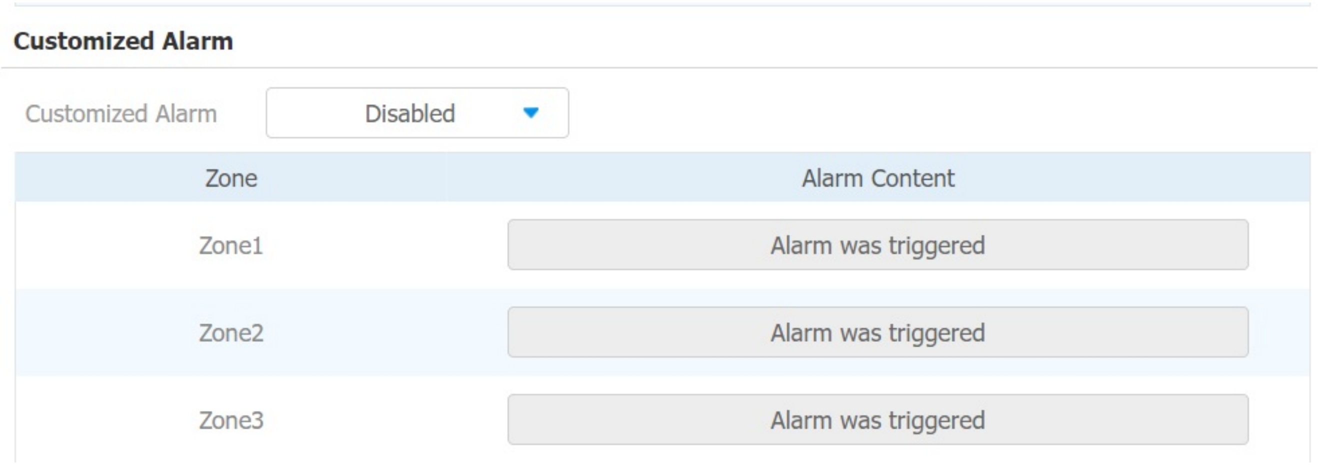
Parameters Set-up:

- **Location**: to select which location the detection device is located, including **Bedroom, Guest Room, Hall, Window, Balcony, Kitchen, Study**, and **Bathroom**.
- **Zone Type**: to select the type of detection device, including **Infrared, Drmagnet, Smoke, Gas**, and **Urgency**.
- **Defence Delay**: it means when users enable the arming mode, there will be 90 seconds delay time for the alarm mode to be activated.
- **Alarm Delay**: it means when the sensor is triggered, there will be 90 seconds delay time to announce the notification.
- **Status**: to enable or disable arming mode on the corresponding zone.

Configure Alarm Text

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

Go to **Arming > Zone Setting > Customized Alarm** interface.



Customized Alarm

Customized Alarm: Disabled

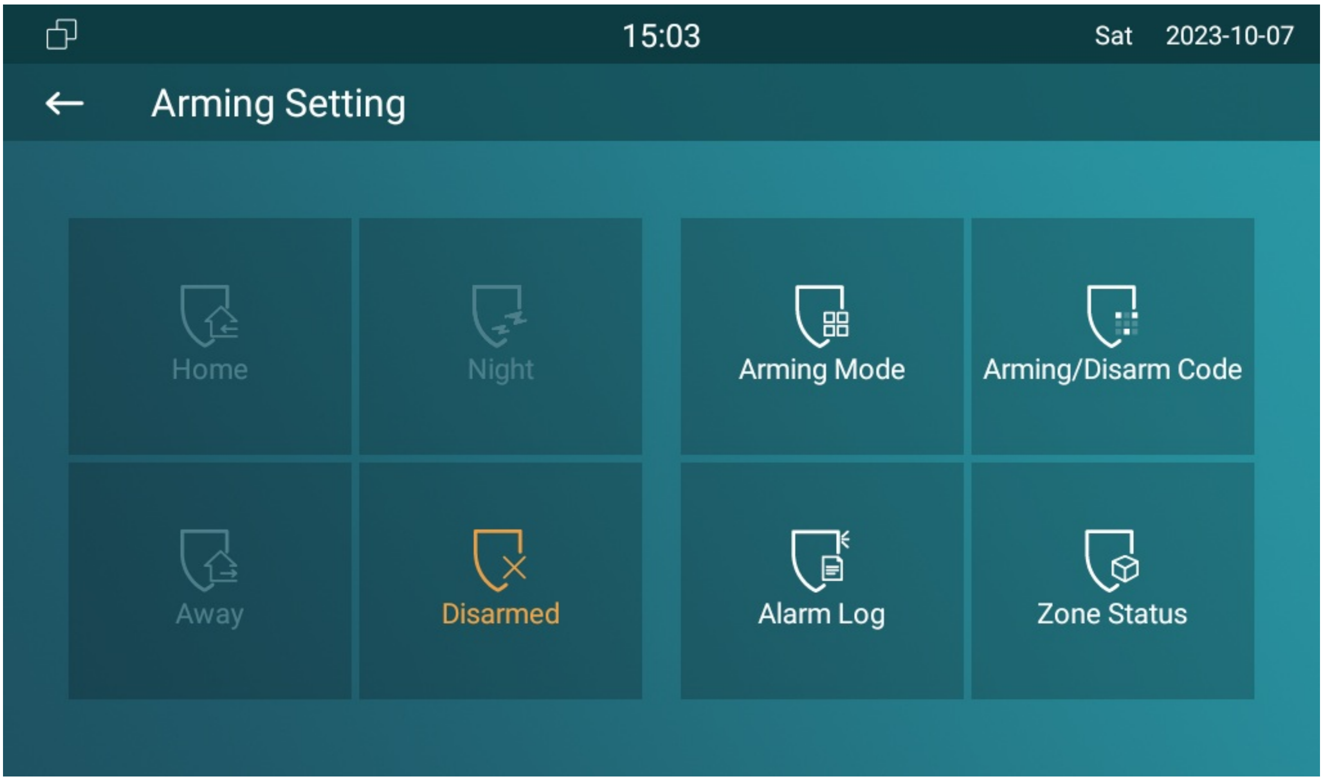
Zone	Alarm Content
Zone1	Alarm was triggered
Zone2	Alarm was triggered
Zone3	Alarm was triggered

Parameter Set-up:

- **Customized Alarm**: enable the feature before you can type in the customized alarm text.
- **Alarm Context**: type in the alarm text in the specific arming zone. The alarm text will be displayed when an arming is triggered.

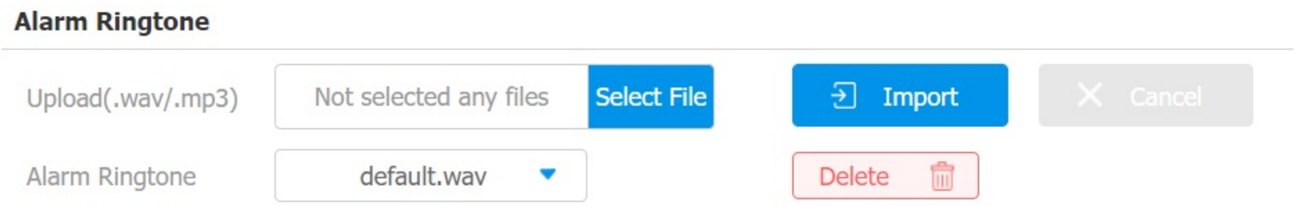
Configure Arming Mode

Users can set the system to a certain mode, such as Away mode when they leave home. To do this, tap the icon of the desired mode. To disarming the system, tap Disarmed.



Configure Alarm Ringtone

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



Alarm Ringtone

Upload(.wav/.mp3): Not selected any files

Alarm Ringtone: default.wav

Note

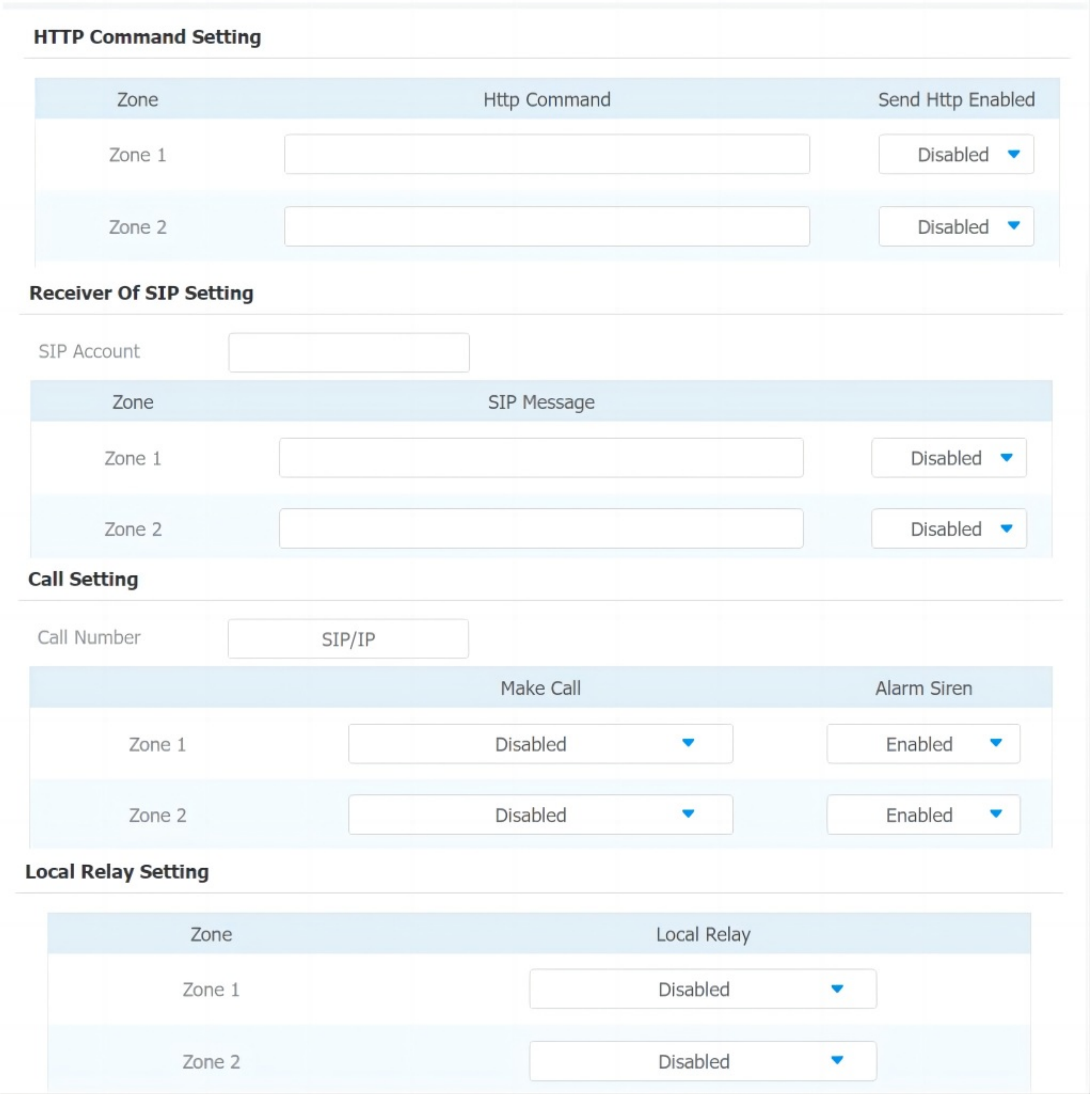
- The file format of the customized ringtone should be .wav.

Alarm Action Configuration

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

Select Alarm Action Types

Select and set up actions on web **Arming > Alarm Action** interface.



HTTP Command Setting

Zone	Http Command	Send Http Enabled
Zone 1		Disabled
Zone 2		Disabled

Receiver Of SIP Setting

SIP Account

Zone	SIP Message	
Zone 1		Disabled
Zone 2		Disabled

Call Setting

Call Number: SIP/IP

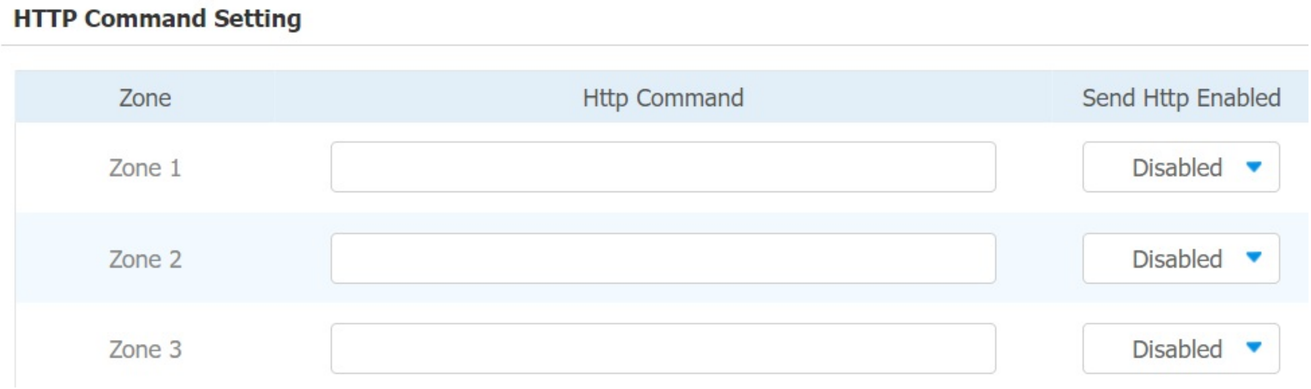
	Make Call	Alarm Siren
Zone 1	Disabled	Enabled
Zone 2	Disabled	Enabled

Local Relay Setting

Zone	Local Relay
Zone 1	Disabled
Zone 2	Disabled

Configure Alarm Action via HTTP Command

To set up the HTTP Command action, you can click **Enable** 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 manufacturer of the device on which the action is to be carried out.

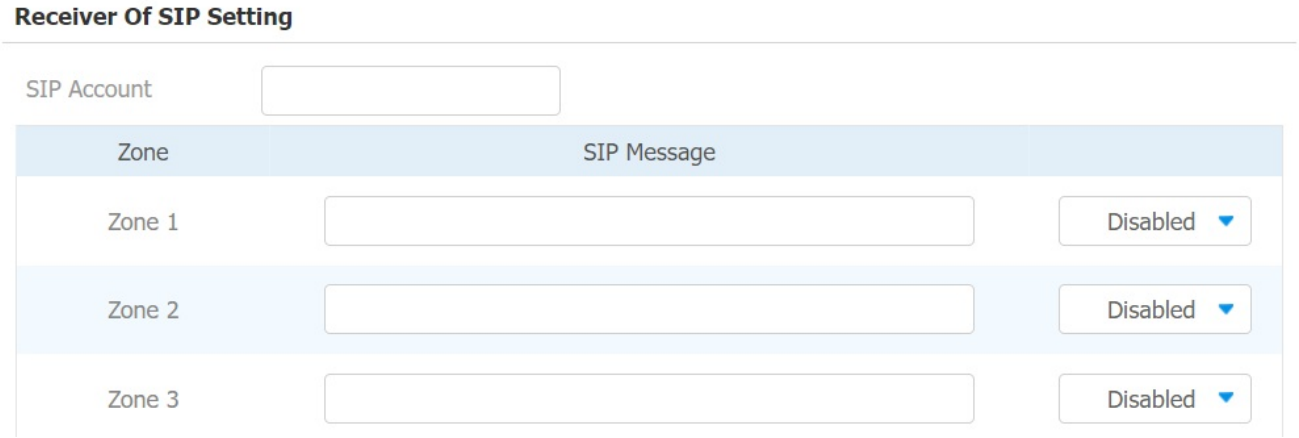


HTTP Command Setting

Zone	Http Command	Send Http Enabled
Zone 1		Disabled ▼
Zone 2		Disabled ▼
Zone 3		Disabled ▼

Configure Alarm Action via SIP Message

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



Receiver Of SIP Setting

SIP Account

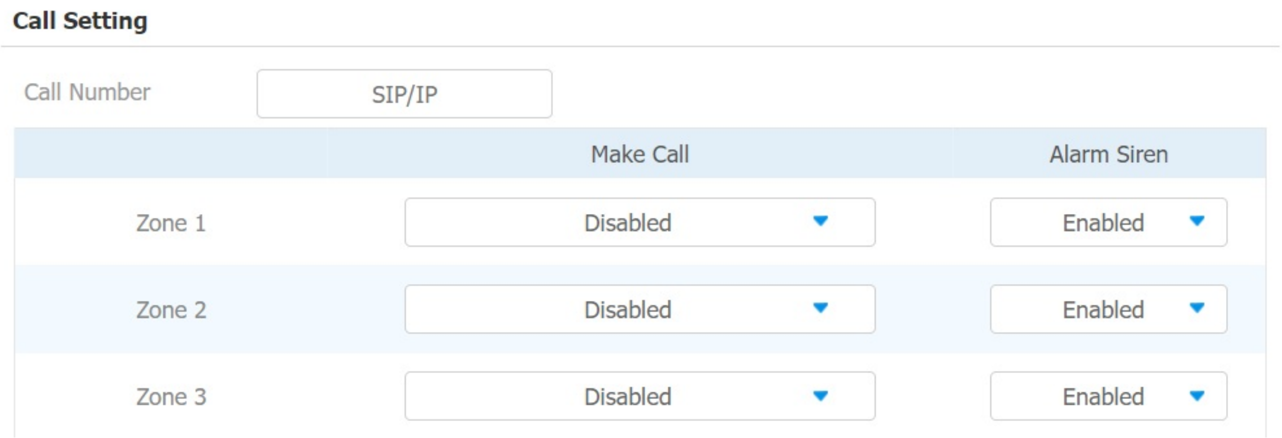
Zone	SIP Message	
Zone 1		Disabled ▼
Zone 2		Disabled ▼
Zone 3		Disabled ▼

Parameter Set-up:

- **Enabled/Disabled**: enable it before you can send the customized messages to a designated SIP number or an IP number when the alarm is triggered.
- **SIP Message**: type in the message you want to send to the designated SIP number or IP number when the alarm is triggered.

Configure Alarm Action via SIP Call

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



Call Setting

Call Number: SIP/IP

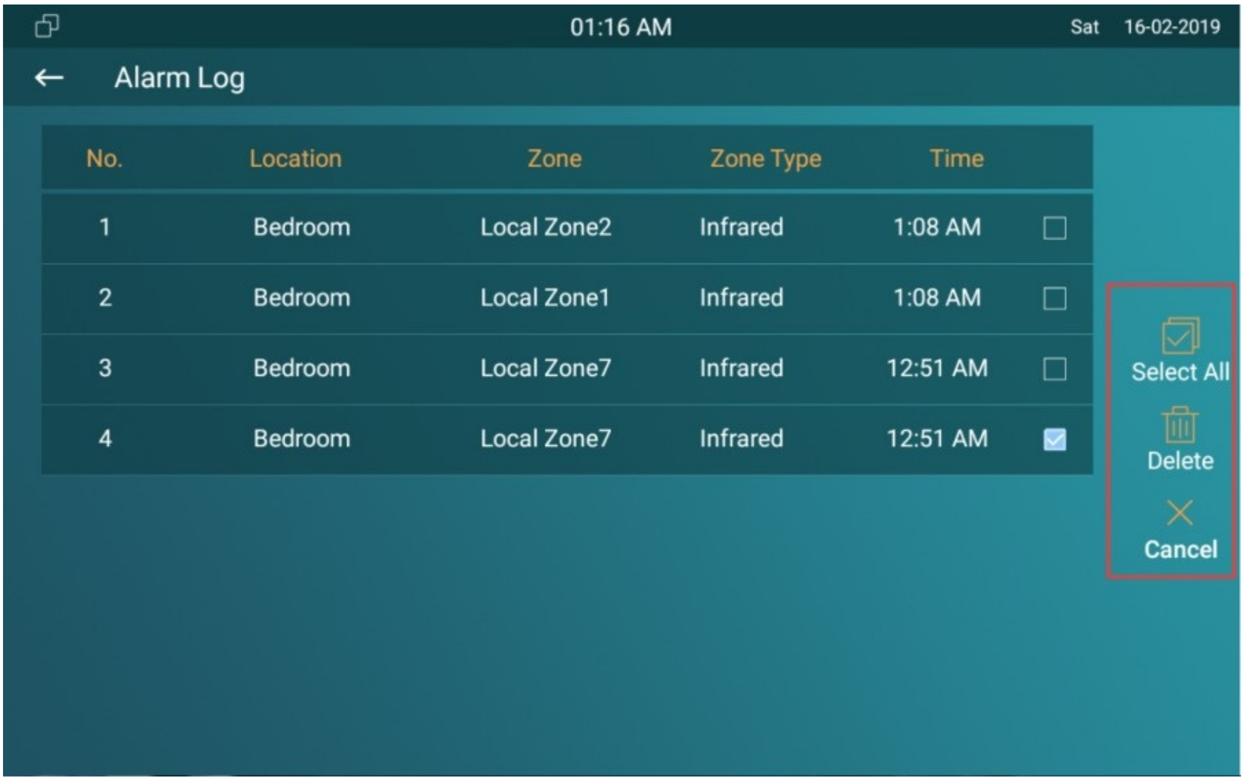
	Make Call	Alarm Siren
Zone 1	Disabled	Enabled
Zone 2	Disabled	Enabled
Zone 3	Disabled	Enabled

Parameter Set-up:

- **Make Call**: enable it so that a call will go to the designated SIP or IP number when alarm is triggered.
- **Alarm Siren**: enable it if you want to trigger alarm siren on the indoor monitor when the alarm is triggered.

Check Alarm Log

To check alarm log on device **Arming > Alarm Log** screen. To delete the existing alarm log by clicking the right-side operation icon.



01:16 AM Sat 16-02-2019

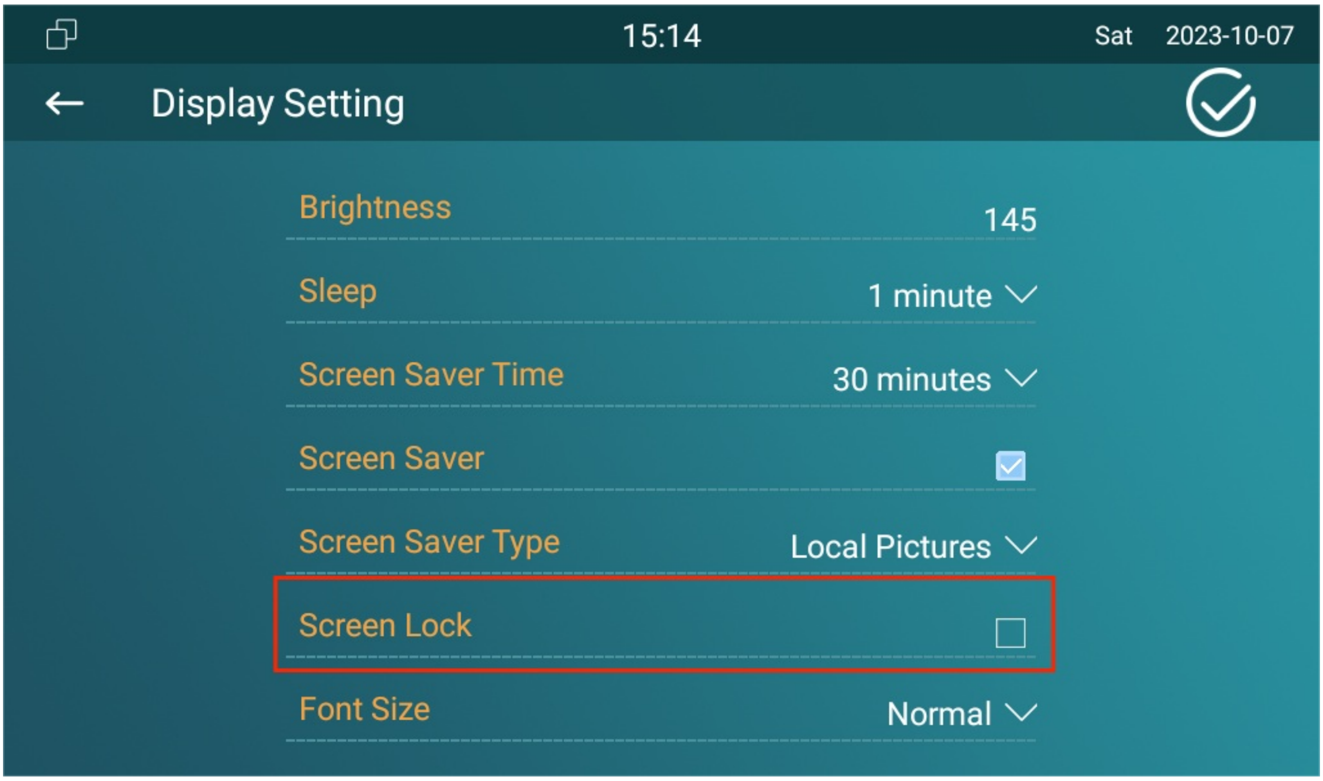
Alarm Log

No.	Location	Zone	Zone Type	Time	
1	Bedroom	Local Zone2	Infrared	1:08 AM	□
2	Bedroom	Local Zone1	Infrared	1:08 AM	□
3	Bedroom	Local Zone7	Infrared	12:51 AM	□
4	Bedroom	Local Zone7	Infrared	12:51 AM	☑

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



15:14 Sat 2023-10-07

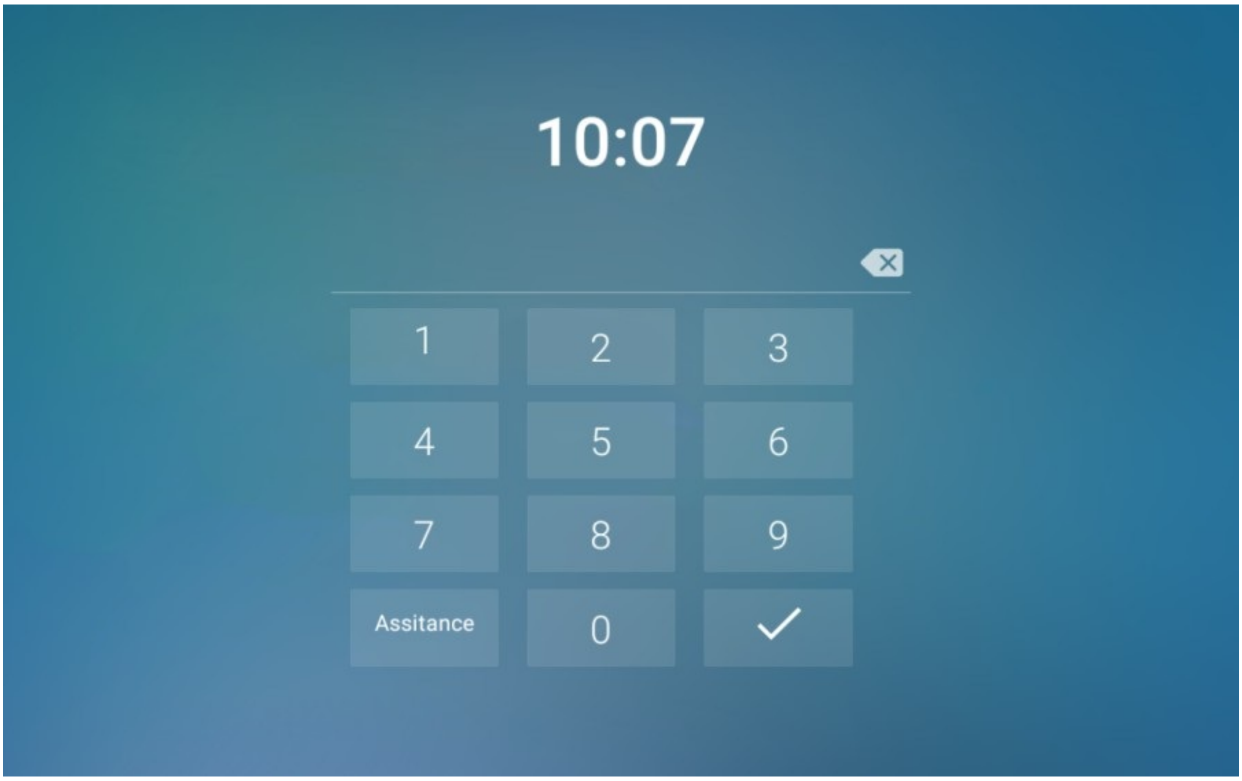
Display Setting

Brightness	145
Sleep	1 minute
Screen Saver Time	30 minutes
Screen Saver	☑
Screen Saver Type	Local Pictures
Screen Lock	□
Font Size	Normal

Screen Unlock by PIN Code

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

Navigate to the **Advance Settings** > **System Code** screen to change a new password.



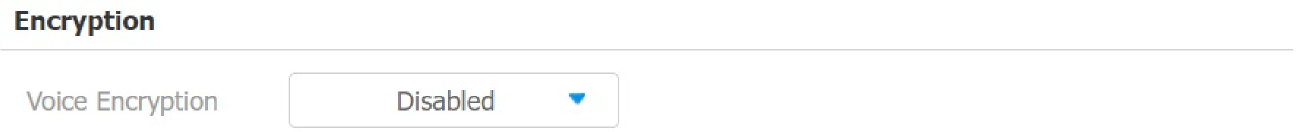
Note

- The default unlock PIN is 123456.

Voice Encryption

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

Go to **Account** > **Advanced** > **Encryption** interface.



Encryption

Voice Encryption: Disabled

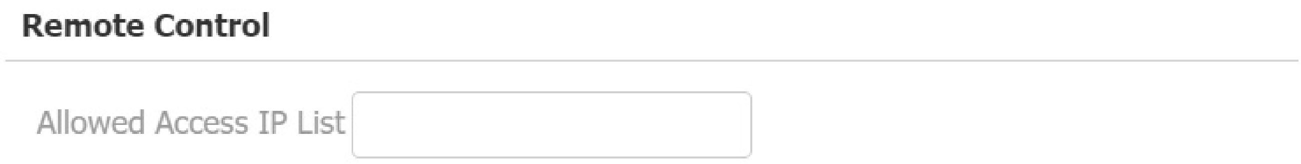
Parameter Set-up:

- **Voice Encryption**: select encryption mode from four options. If you disable it, 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)**, encrypts voice from the called party, if the called party also enables SRTP, the voice signals will also be encrypted.**ZRTP(Optional)** is 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.

Navigate to **Phone** > **Call Feature** > **Remote Control** interface.



Remote Control

Allowed Access IP List

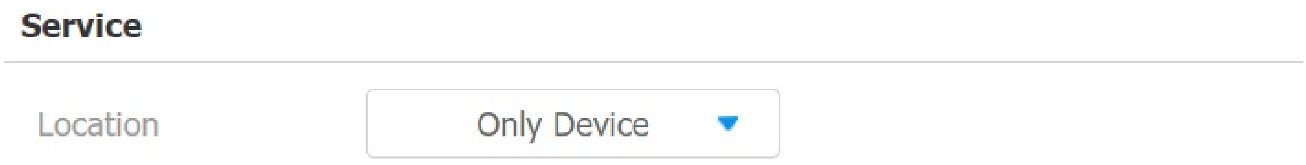
Parameter Set-up:

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

Location

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

To set it up, go to **Security** > **Advanced** > **Service.**



Service

Location: Only Device

Parameter Set-up:

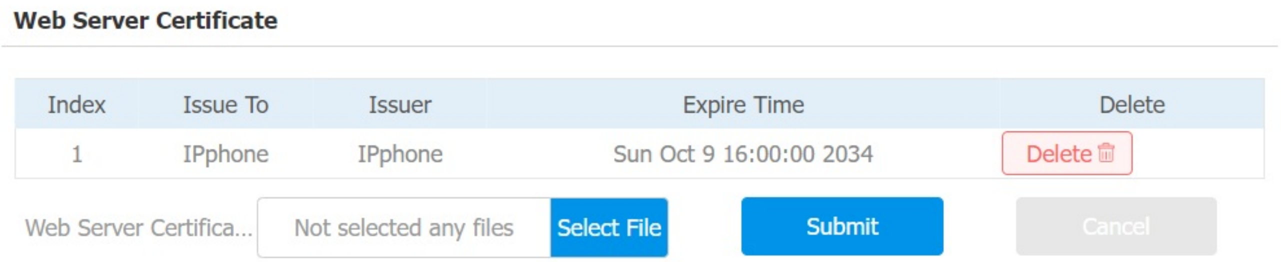
- **Disabled**: select **Disabled** if you do not allow any app to find your device location.
- **Only Device**: the device location can be determined using GPS
- **High Accuracy**: the device location can be determined via WAN, Bluetooth, or cellular networks.

Client Certificate Setting

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

Web Server Certificate

To upload web server certificate on the device web interface **Security > Advanced > Web Server Certificate**.

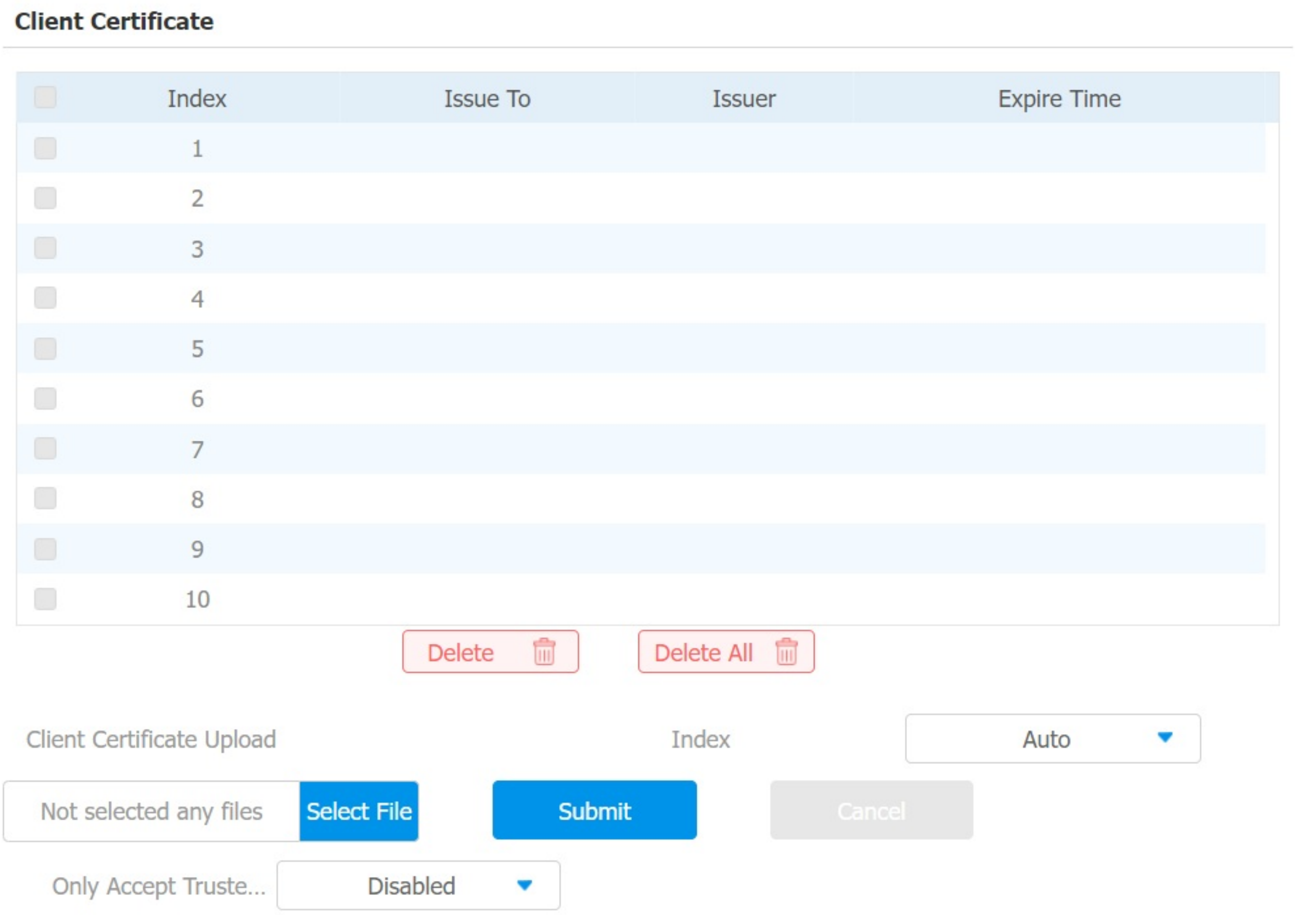


Web Server Certificate

Index	Issue To	Issuer	Expire Time	Delete
1	IPphone	IPphone	Sun Oct 9 16:00:00 2034	Delete

Client Certificate

To upload and configure client certificates on the same page.



Client Certificate

□	Index	Issue To	Issuer	Expire Time
□	1			
□	2			
□	3			
□	4			
□	5			
□	6			
□	7			
□	8			
□	9			
□	10			

Client Certificate Upload

Index: Auto

Not selected any files

Only Accept Truste...: Disabled

Parameter Set-up:

- **Index**: select the desired value from the drop-down list of Index. If you select **Auto**, the uploaded certificate will be displayed in numeric order. If you select values from **1** to **10**, the uploaded certificate will be displayed according to the value selected.

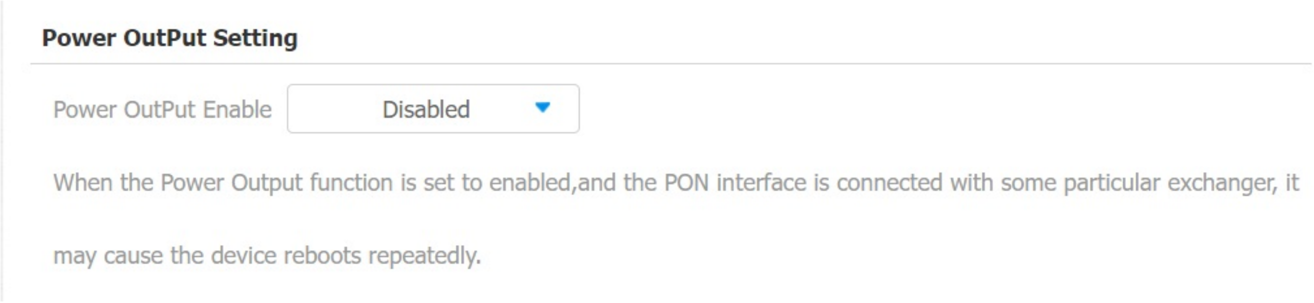
- **Select File**: click **Select file** to browse the local drive, and locate the desired certificate (*.pem only).

- **Only Accept Trusted Certificates**: if you select **Enabled**, as long as the authentication success, the device will verify the server certificate based on the client certificate list. If you select **Disabled**, the device will not verify the server certificate no matter whether the certificate is valid or not.

Power Output Setting

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

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



Power OutPut Setting

Power OutPut Enable: Disabled

When the Power Output function is set to enabled,and the PON interface is connected with some particular exchanger, it may cause the device reboots repeatedly.

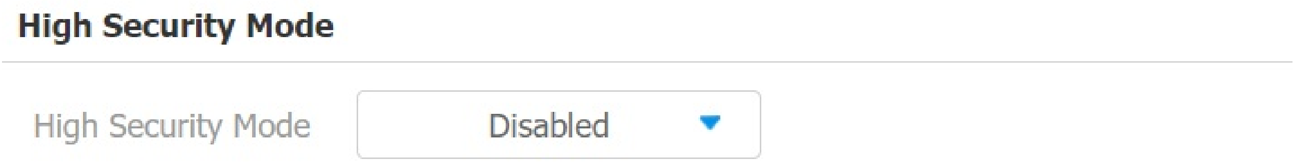
Note

- When the **Power Output** function is enabled, and the PON interface is connected with some particular exchangers, it may cause the device to reboot repeatedly.

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 configure this feature on the web **Security > Basic > High Security Mode** interface.



High Security Mode

High Security Mode: 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.

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

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

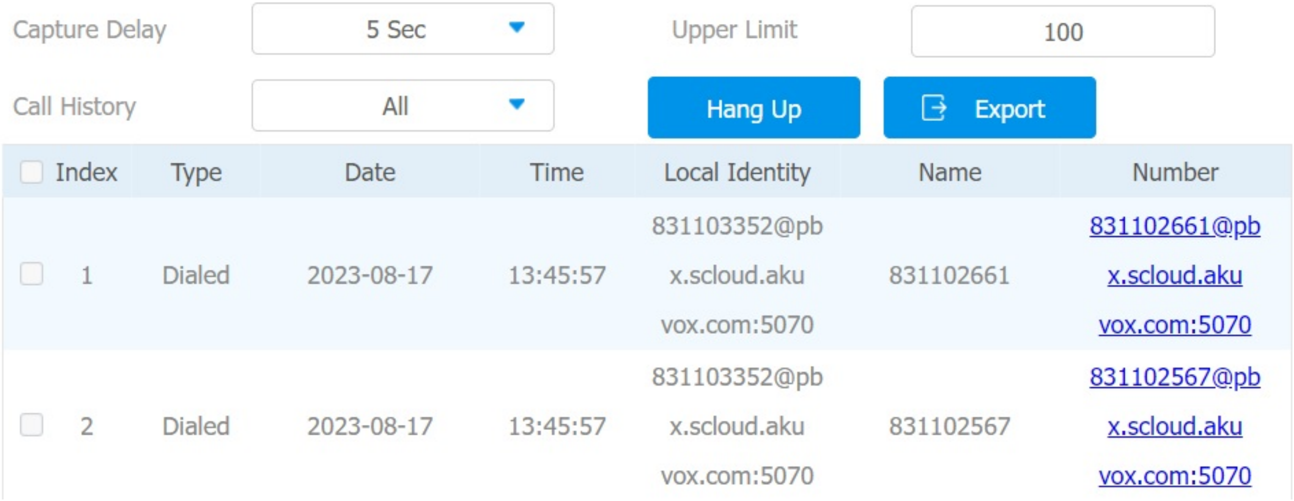
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Call Log

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

You can also set up the call-related picture capturing if needed.

Go to **Contacts > Call Log** interface.



Capture Delay: 5 Sec

Upper Limit: 100

Call History: All

□ Index	Type	Date	Time	Local Identity	Name	Number
□ 1	Dialed	2023-08-17	13:45:57	831103352@pbx.scloud.akuvox.com:5070	831102661	831102661@pbx.scloud.akuvox.com:5070
□ 2	Dialed	2023-08-17	13:45:57	831103352@pbx.scloud.akuvox.com:5070	831102567	831102567@pbx.scloud.akuvox.com:5070

Parameter Set-up:

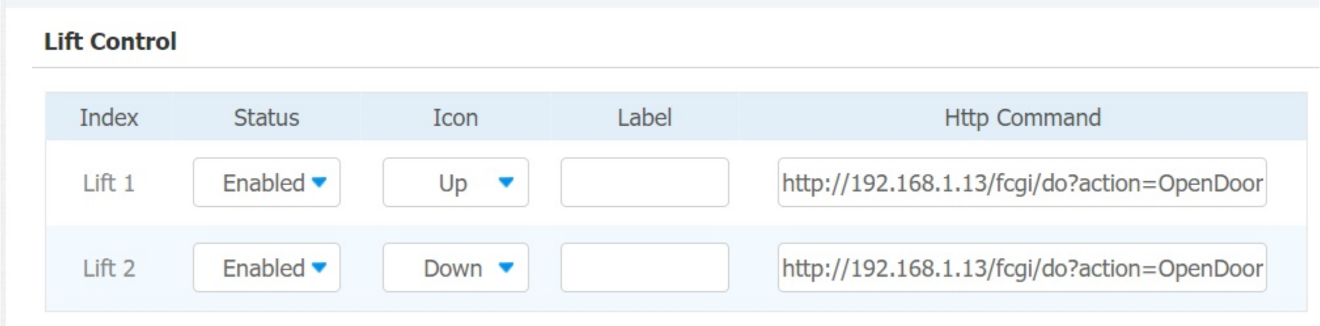
- **Capture Delay**: set the image capturing starting time when the device goes into video preview.
- **Upper Limit**: set the maximum screenshot storage capacity. When the capacity is reached, the previous screenshots will be overwritten.
- **Call History**: select call history among **All, Dialed, Received, Forwarded**, and **Missed** for the specific type of call log to be displayed.

Lift Control

You can summon a lift via the lift control feature.

Configure Lift Control

To enable and set the **Lift** icon on device web **Phone > Lift > Lift Control** interface.



Lift Control

Index	Status	Icon	Label	Http Command
Lift 1	Enabled	Up		http://192.168.1.13/fcgi/do?action=OpenDoor
Lift 2	Enabled	Down		http://192.168.1.13/fcgi/do?action=OpenDoor

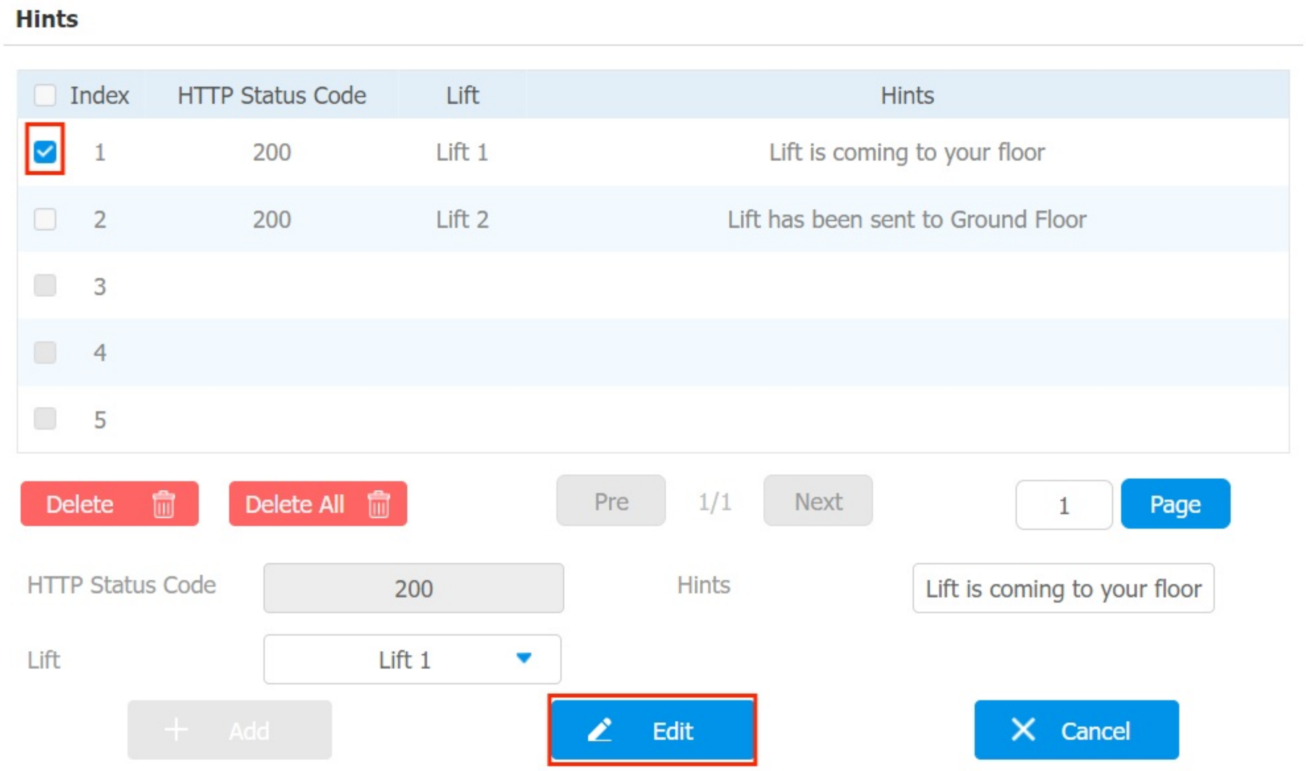
Parameter Set-up:

- **Status**: click to enable or disable the lift button.
- **Icon**: click to select icon for the button.
- **Label**: enter the title for the button.
- **HTTP Command**: select http:// or https:// for head of http command and enter http command.

Configure Lift Control Prompt

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

To do this configuration on web **Phone > Lift > Hints** interface. Click **Edit** icon to save the configuration.

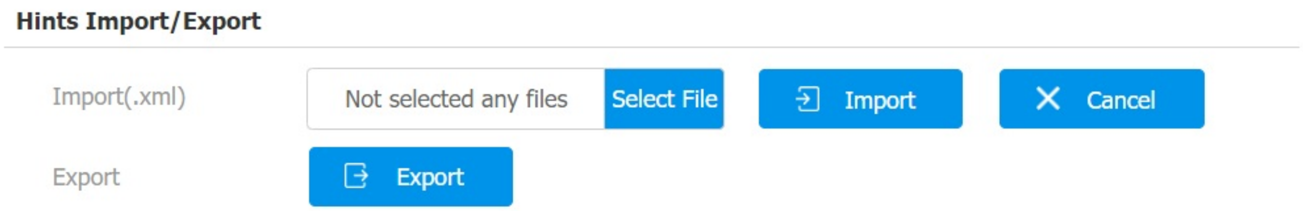


Hints

□	Index	HTTP Status Code	Lift	Hints
☑	1	200	Lift 1	Lift is coming to your floor
□	2	200	Lift 2	Lift has been sent to Ground Floor
□	3			
□	4			
□	5			

HTTP Status Code	200	Hints	Lift is coming to your floor
Lift	Lift 1		

If there are huge amounts of prompts that need to be added, you can click **Export** tab to export a template on the same page. After editting the file, import it to the web.



Hints Import/Export

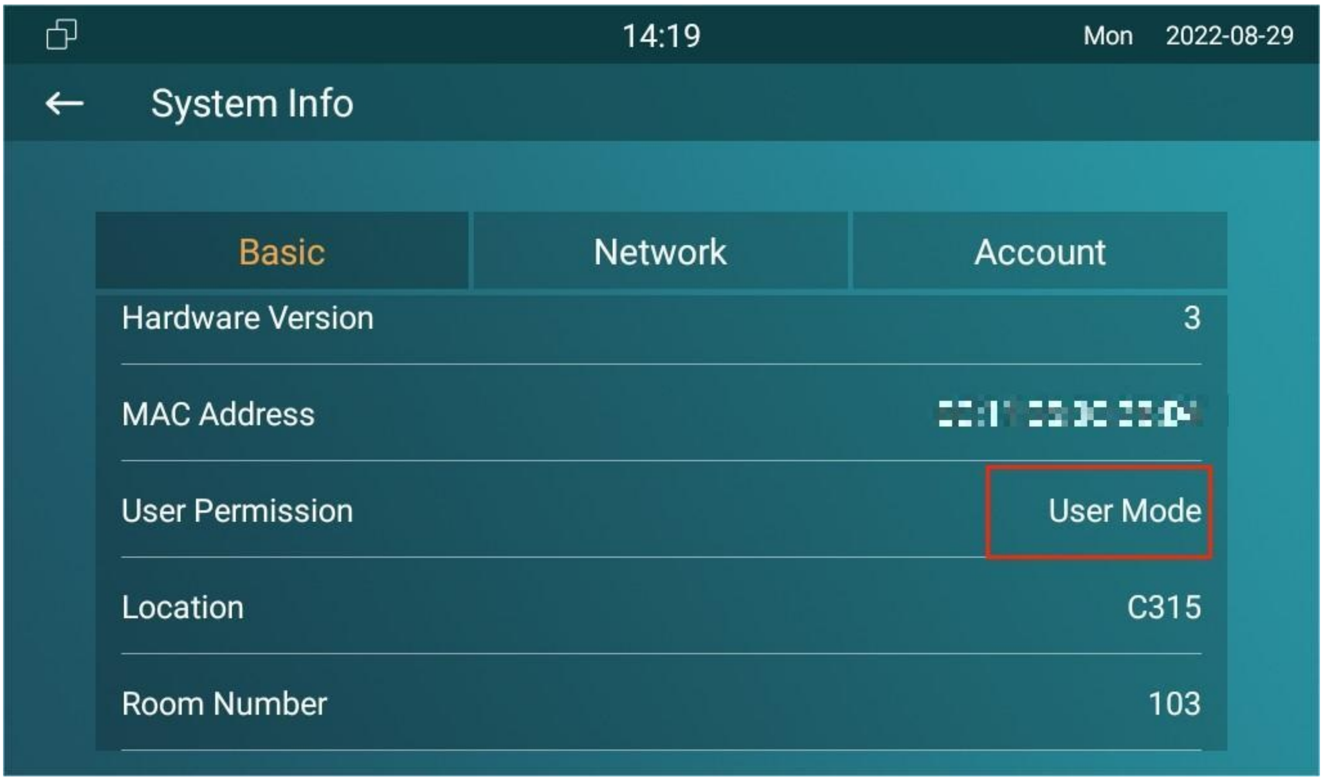
Import(.xml)	Not selected any files
Export	

Device Integration with Third Party

Enter Applications Screen

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

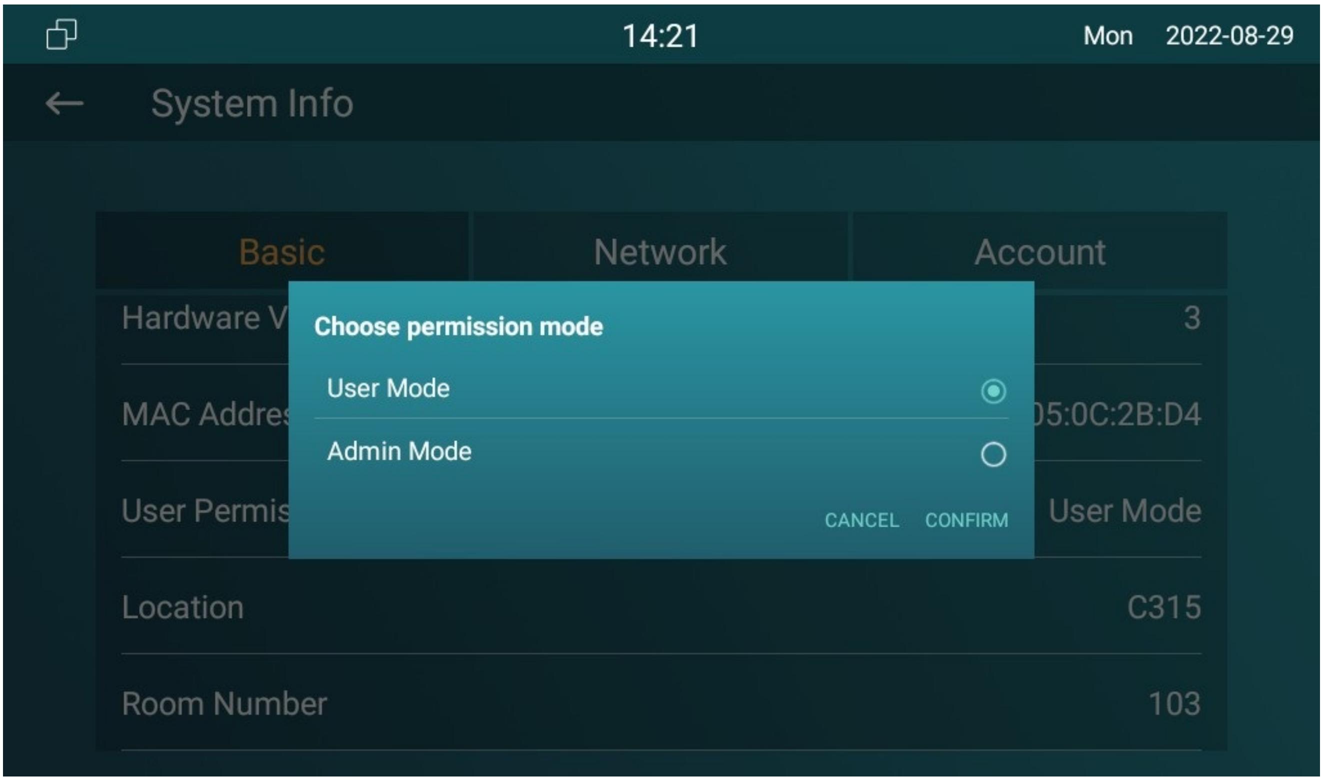
To do the configuration on device **Settings > System Info** screen. You can press on **User Mode** 10 times and press **Admin Mode**, and then **Confirm**.



14:19 Mon 2022-08-29

System Info

Hardware Version	3
MAC Address	[redacted]
User Permission	User Mode
Location	C315
Room Number	103



14:21 Mon 2022-08-29

System Info

Basic	Network	Account

Hardware V	3
MAC Addres	05:0C:2B:D4
User Permis	User Mode
Location	C315
Room Number	103

Choose permission mode

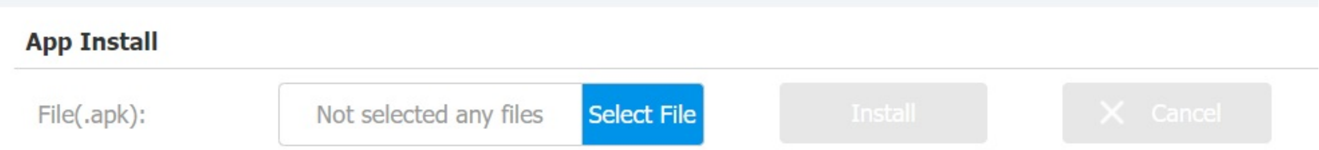
User Mode ●

Admin Mode ○

CANCEL CONFIRM

Install Third-party App

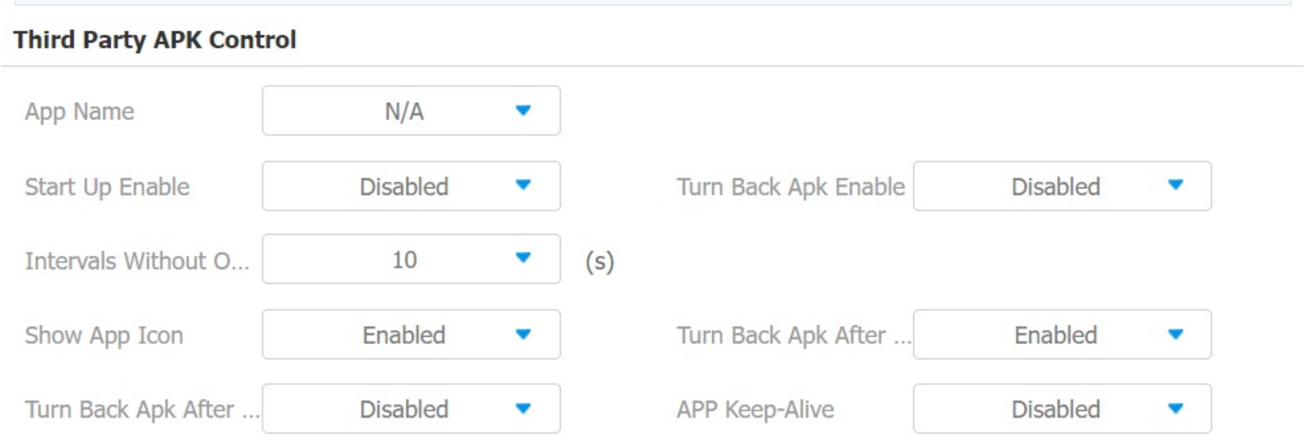
You can install the third-party app to your device on the device web **Phone > App** interface. Choose a suitable .apk file from the PC to upload.



App Install

File(.apk): Not selected any files

To configure the installed third-party app on the web **Phone > Key/Display > Third Party APK Control** interface, you can click **App Name** to select the installed APK files for configuration. Then, enable or disable each field for the specific configuration you need.



Third Party APK Control

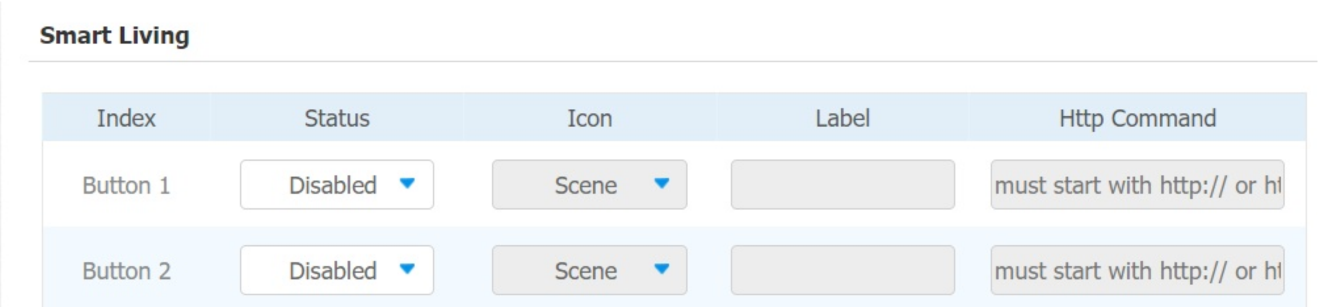
App Name	N/A		
Start Up Enable	Disabled	Turn Back Apk Enable	Disabled
Intervals Without O...	10 (s)		
Show App Icon	Enabled	Turn Back Apk After ...	Enabled
Turn Back Apk After ...	Disabled	APP Keep-Alive	Disabled

Parameter Set-up:

- **App Name**: select the app to be configured.
- **Interval Without Operating (Sec)**: enable it to set the app returning time interval when there is no operation on the device.
- **Start Up Enable**: enable it if you want the app to run automatically when the device is turned on.
- **Turn Back App After Awakening**: enable it if you want the device to return to the app when the screen is awakened.
- **APP Keep-Alive** : enable it if you want the app to stay running without being turned off.
- **Turn Back App After Calling**: enable it if you want the app to return automatically after finishing a call (this feature applies to all the apps).
- **Show App Icon**: enable it if you want the app icon to be displayed on the screen.

Smart Living Setting

You can control the home sensor through an HTTP command on the device web **Phone > Smart Living** interface.



Smart Living

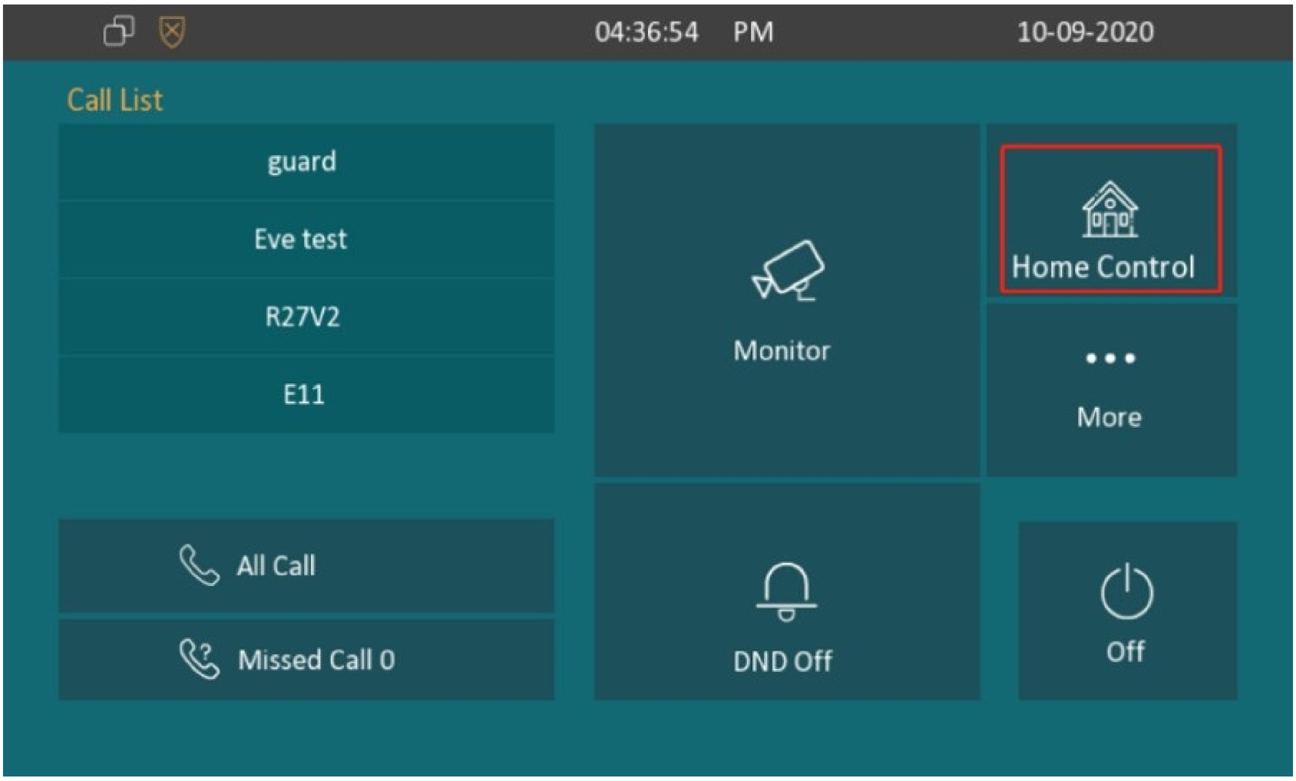
Index	Status	Icon	Label	Http Command
Button 1	Disabled	Scene		must start with http:// or ht
Button 2	Disabled	Scene		must start with http:// or ht

Parameter Set-up:

- **Status**: enable or disable this button. If disabled, the button will not appear on the home control page.
- **Icon**: select **Scene** or **Light**. If **Scene** is selected, the icon is displayed as a scene icon. Select **Light**, the icon is a light icon.
- **Label**: it is used to customize the button display name.

- **HTTP command**: set up the HTTP command to trigger the sensor.

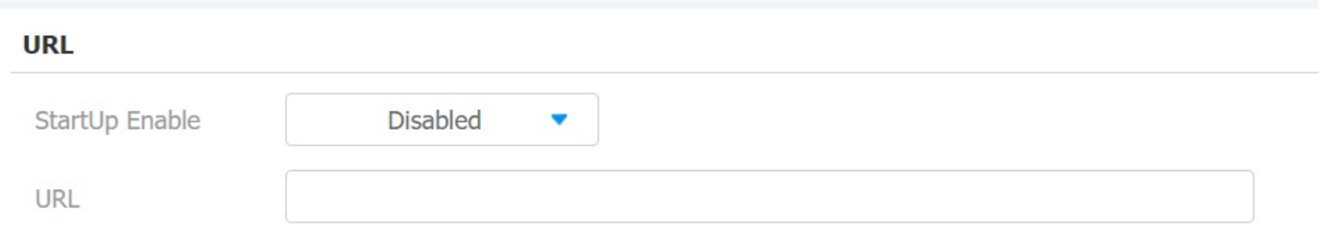
> **Note**
>
> - To configure Smart Living button on **Phone** > **Key/Display** interface.



Display Third-party Webpage after Booting Up

If you want the device screen to go to any third-party servers or the third-party webpage after the device's boot-up, you can type in their URL.

To set it up, you can go to **Phone** > **Web View** > **URL**.

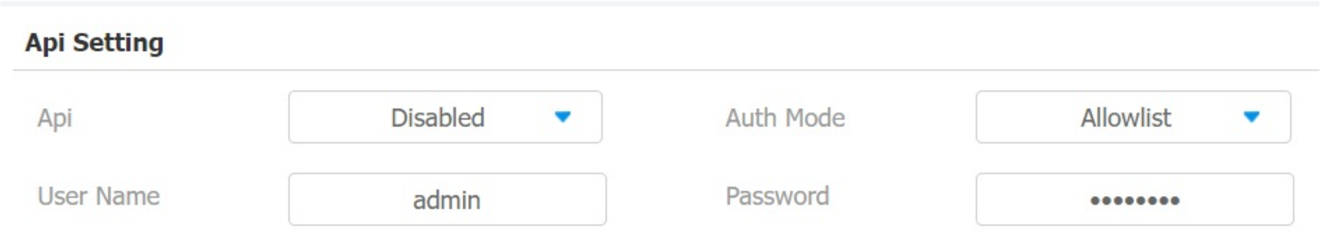

URL

StartUp Enable	Disabled
URL	

Third-party Integration via API

To allow the third-party devices to integrate with the indoor monitor, you need to set up API authentication by setting up a username and password. You also need to select the authentication code for the API-based integration.

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



Api Setting

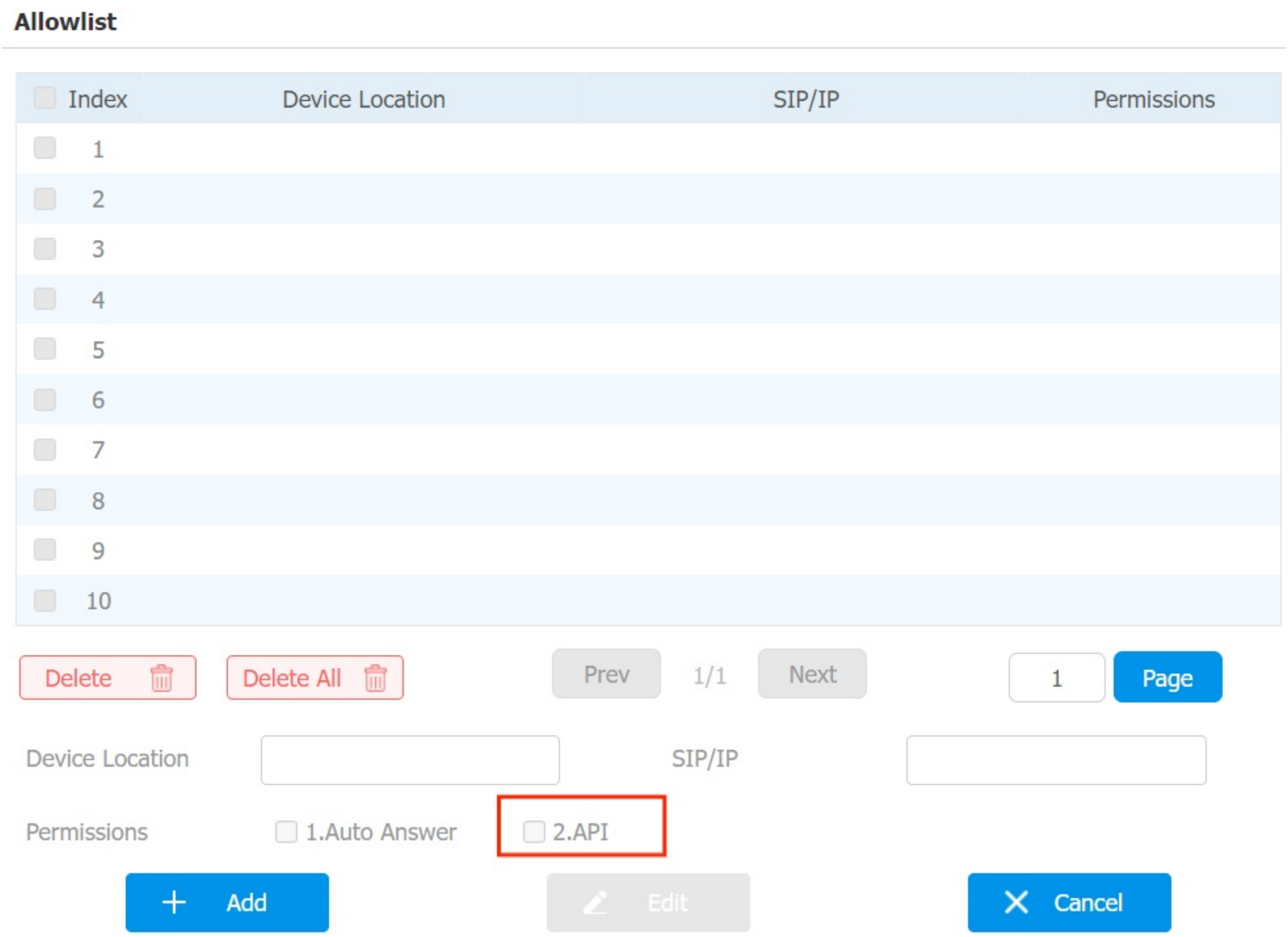
Api	Disabled	Auth Mode	Allowlist
User Name	admin	Password	••••••••

Parameter Set-up:

- **API**: enable the API if you allow the device to be integrated with the third-party devices via API.
- **Auth Mode**: select the authentication mode.
  - **Allowlist**: select it when you only allow the device in the allow list to integrate with the indoor monitor.
  - **Digest**: select it when you apply the **Digest** mode for the third-party integration.
  - **None**: select none if all the devices are allowed to integrate with the indoor monitor with all forms of the authentication mode.
- **User Name**: type in the username used for the authentication.
- **Password**: type in the password used for the authentication.

Before the API integration, you need to enable the API permission and create allow list by entering the location and IP address of the device to be integrated with the indoor monitor.

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



Allowlist

□ Index	Device Location	SIP/IP	Permissions
□ 1			
□ 2			
□ 3			
□ 4			
□ 5			
□ 6			
□ 7			
□ 8			
□ 9			
□ 10			

Device Location

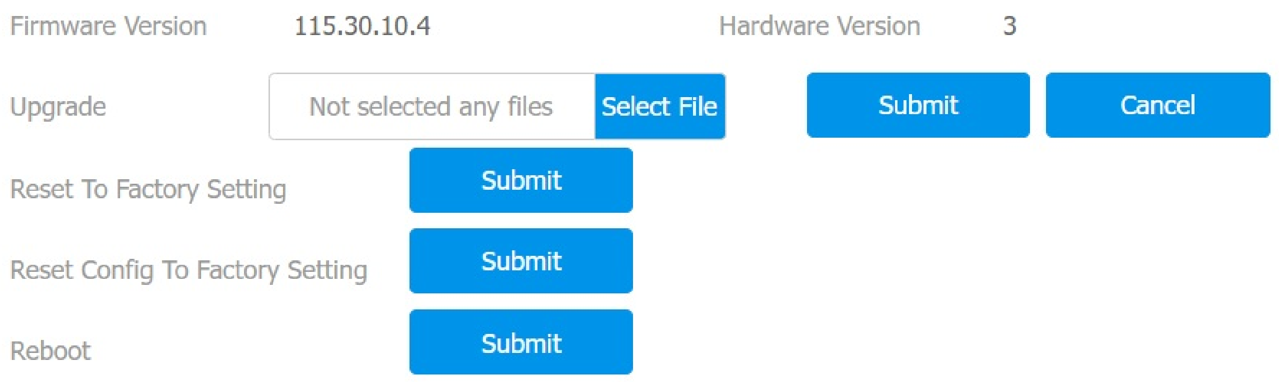
SIP/IP

Permissions □ 1.Auto Answer □ 2.API

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Firmwares of different versions for the indoor monitors can be upgraded on the device web **Upgrade > Basic** interface.



Firmware Version 115.30.10.4

Hardware Version 3

Upgrade: Not selected any files

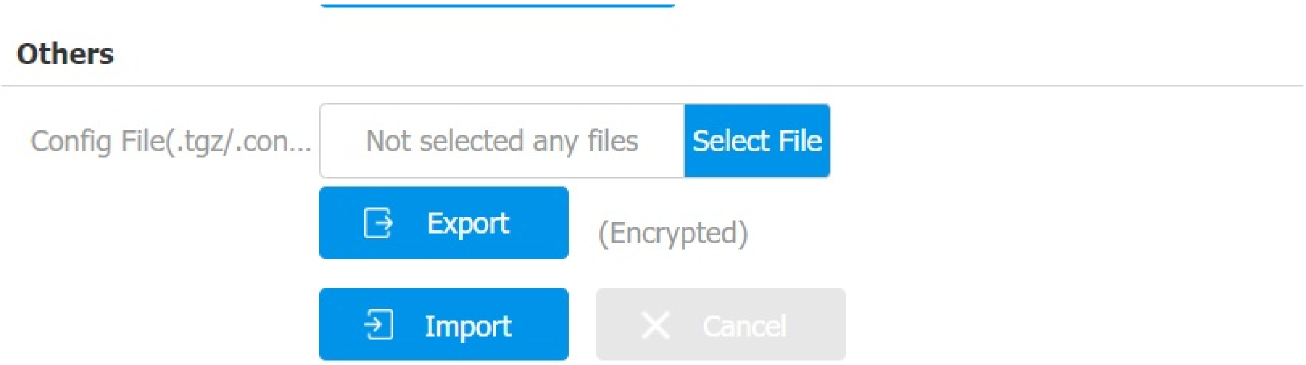
Note

- Firmware files should be **.zip** format for an upgrade.

Backup

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

Navigate to **Upgrade** > **Advanced** > **Others** interface if needed.

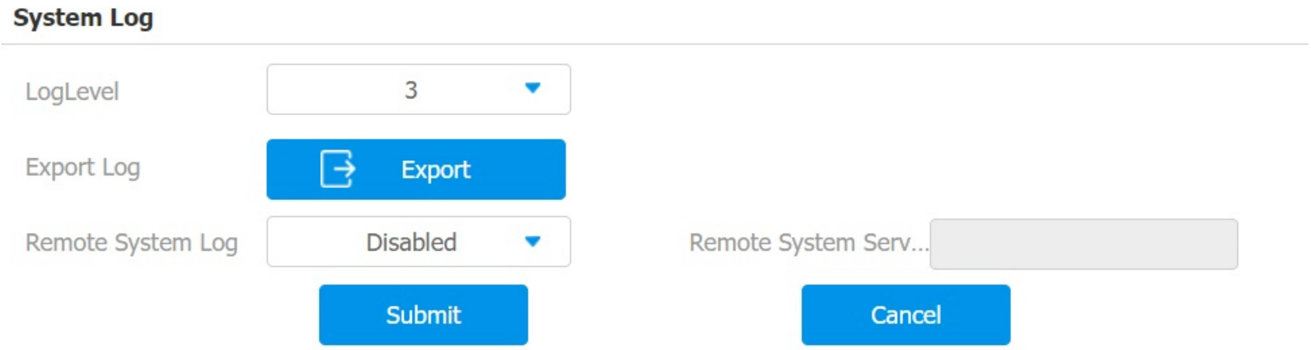


Debug

System Log for Debugging

System logs can be used for debugging purposes.

Go to **Upgrade > Diagnosis > System Log** interface.



System Log

LogLevel: 3

Export Log: Export

Remote System Log: Disabled

Remote System Serv...:

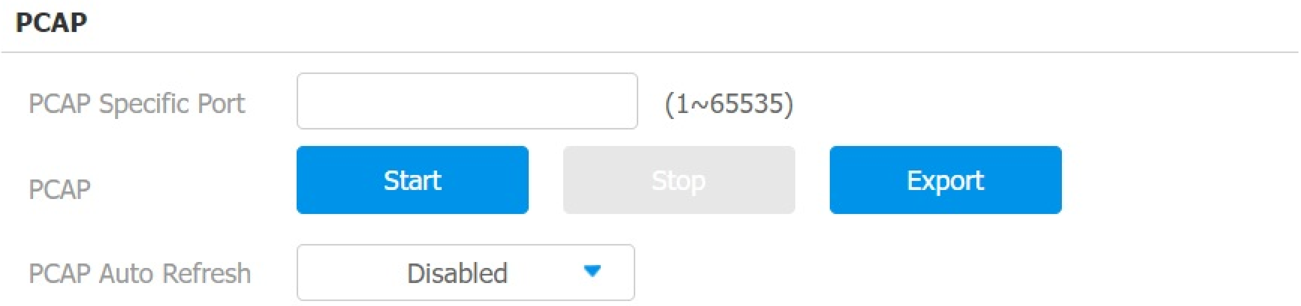
Parameter Set-up:

- **Log Level**: select log levels from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. 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 the temporary debug log file to a local PC.
- **Remote System Server**: enter the remote server address to receive the device and the remote server address 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.

You can set up the PCAP on the device web **Upgrade > Diagnosis > PCAP** interface properly before using it.



PCAP

PCAP Specific Port (1~65535)

PCAP

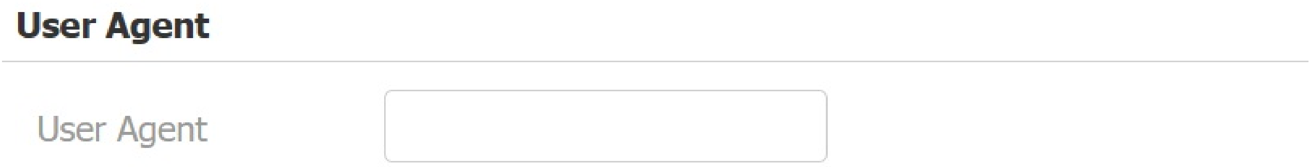
PCAP Auto Refresh: Disabled

Parameter Set-up:

- **PCAP Specific Port**: select the specific ports 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 **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: if you set it as **Enabled**, then the PCAP will continue to capture data packets even after the data packets reach their 50M maximum in capacity. If you set it as **Disabled**, the PCAP will stop data packet capturing when the data packets captured reach the maximum capturing capacity of 1MB.

User Agent

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



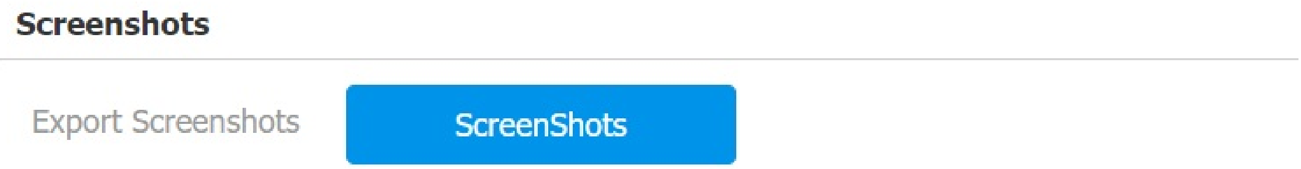
User Agent

User Agent

Screenshots

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

Go to the web **Upgrade > Advanced > Screenshots** interface.



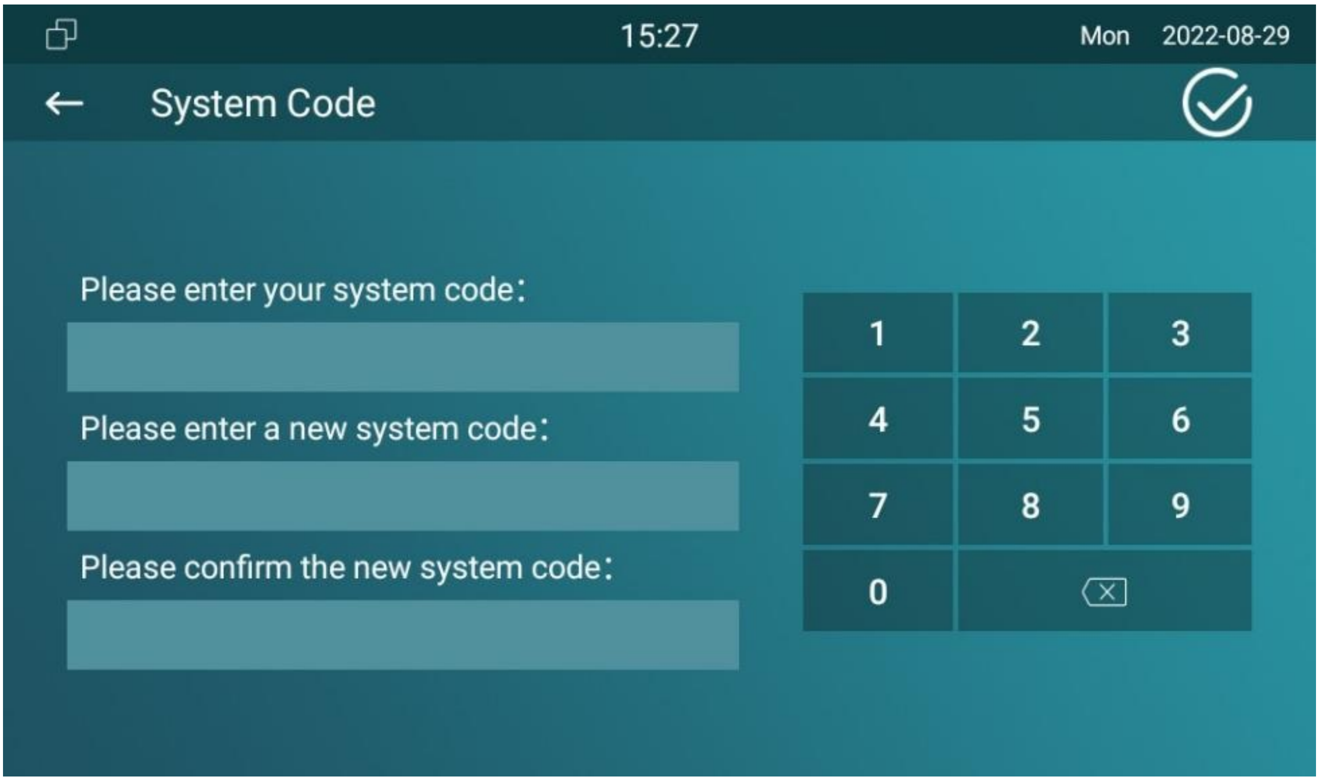
Screenshots

Export Screenshots

Password Modification

Modify Device Basic Settings Password

To do the configuration on the device **Advance Settings > System Code** screen to change a new password. The default password is 123456.



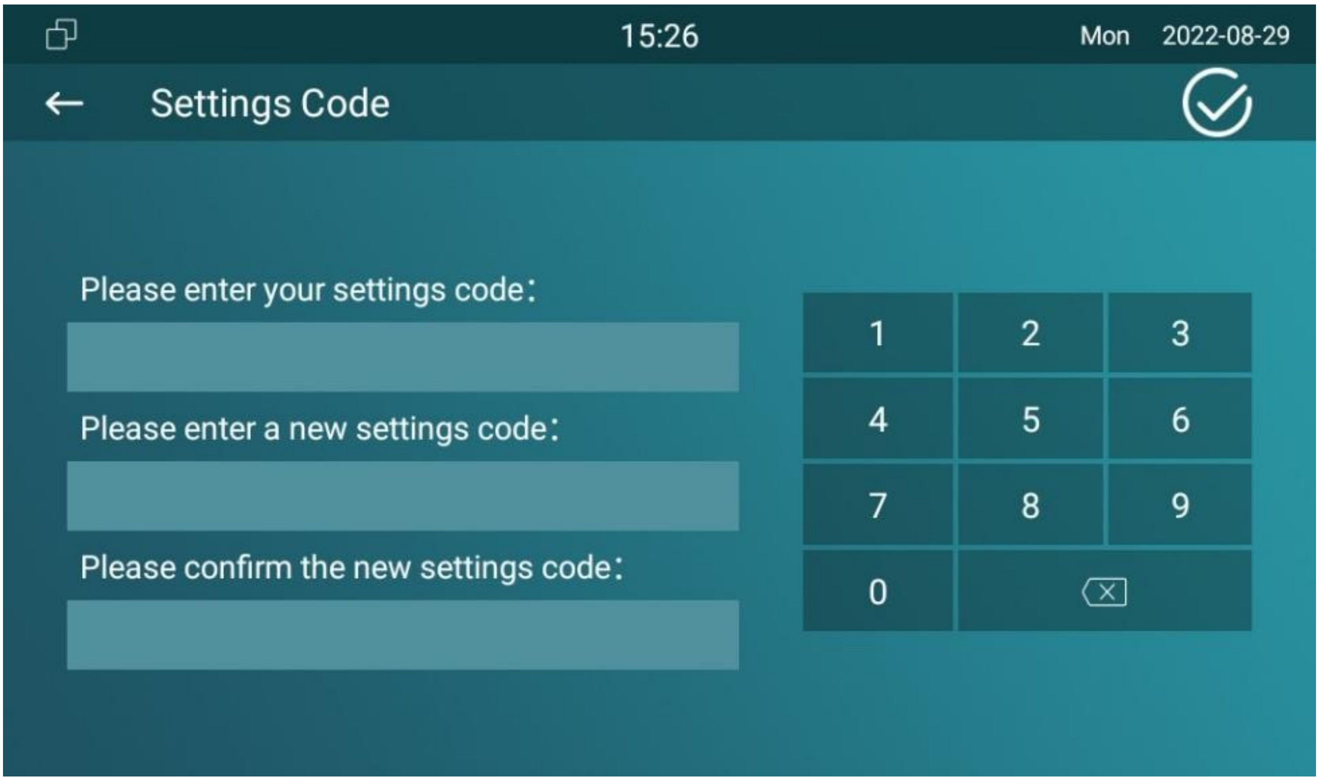
Please enter your system code:

Please enter a new system code:

Please confirm the new system code:

Modify Device Advance Settings Password

This password is used to enter the advance settings of the device, including password settings, account numbers, SOS numbers, network settings, etc. To modify the advanced setting password on the device **Advanced Settings > Setting Code** screen. The default password is 123456.



15:26 Mon 2022-08-29

Settings Code

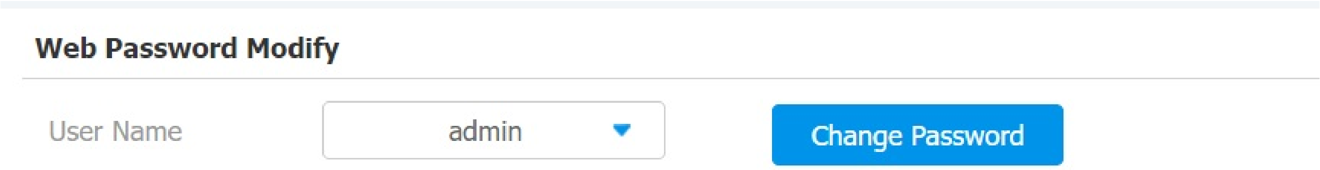
Please enter your settings code:

Please enter a new settings code:

Please confirm the new settings code:

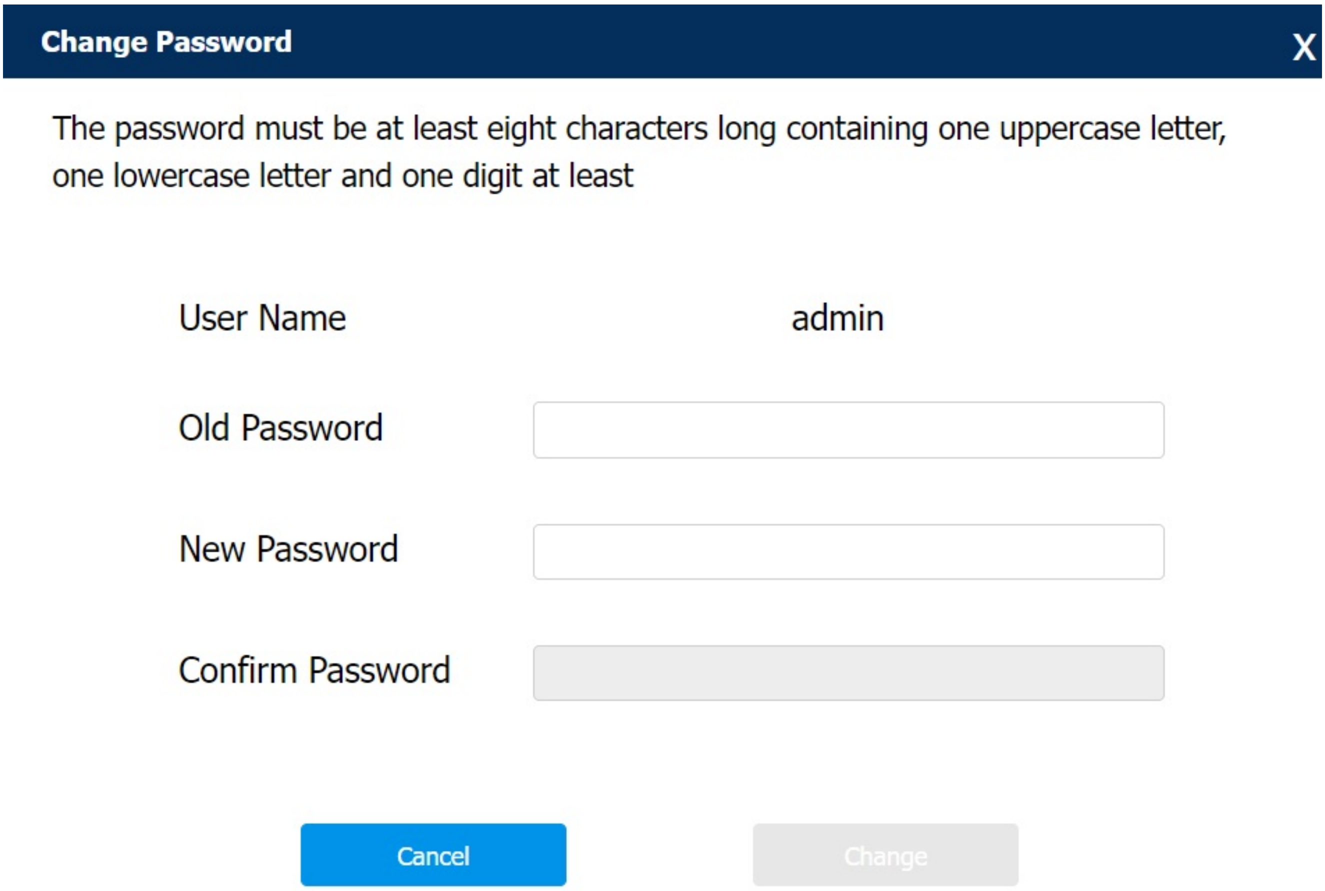
Modify Device Web Interface Password

To modify web interface password, you can do it on device web **Security > Basic > Web Password Modify** interface. Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.



Web Password Modify

User Name: admin



Change Password

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

User Name admin

Old Password

New Password

Confirm Password

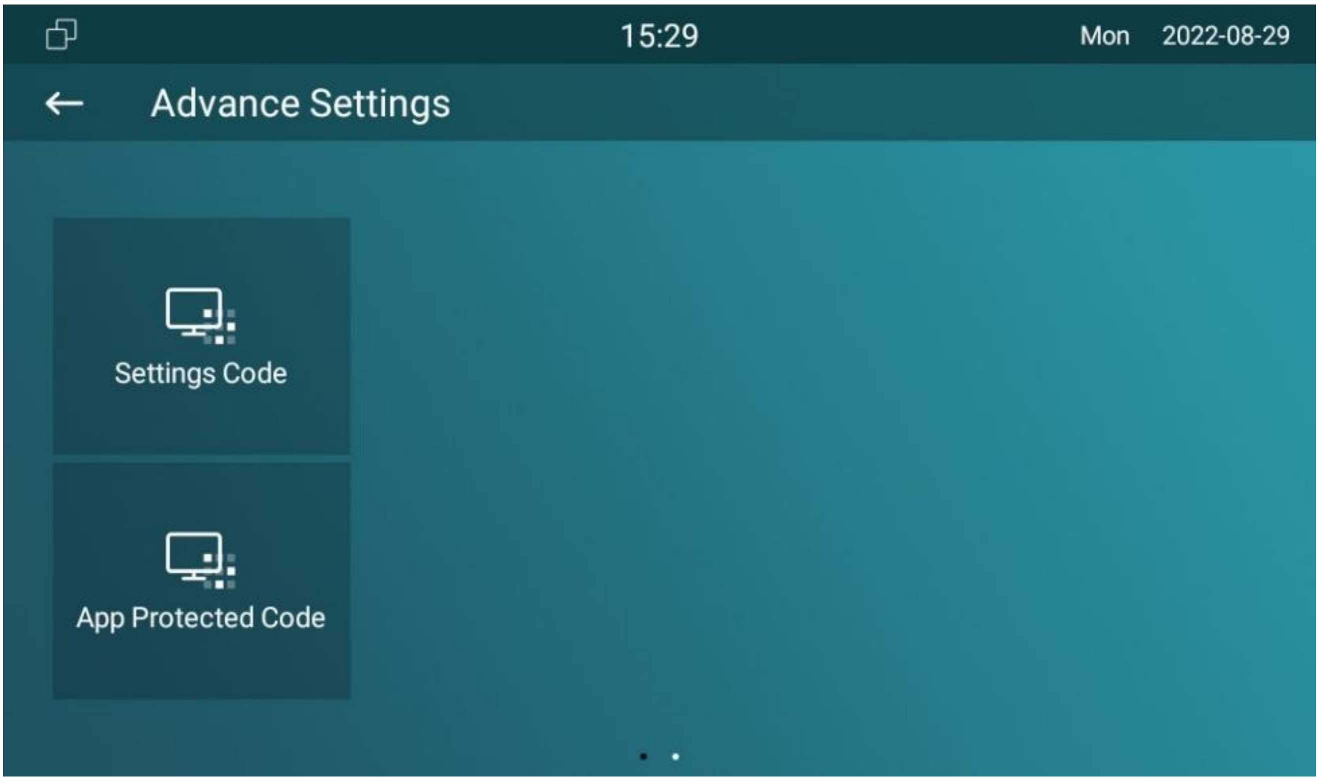
Note

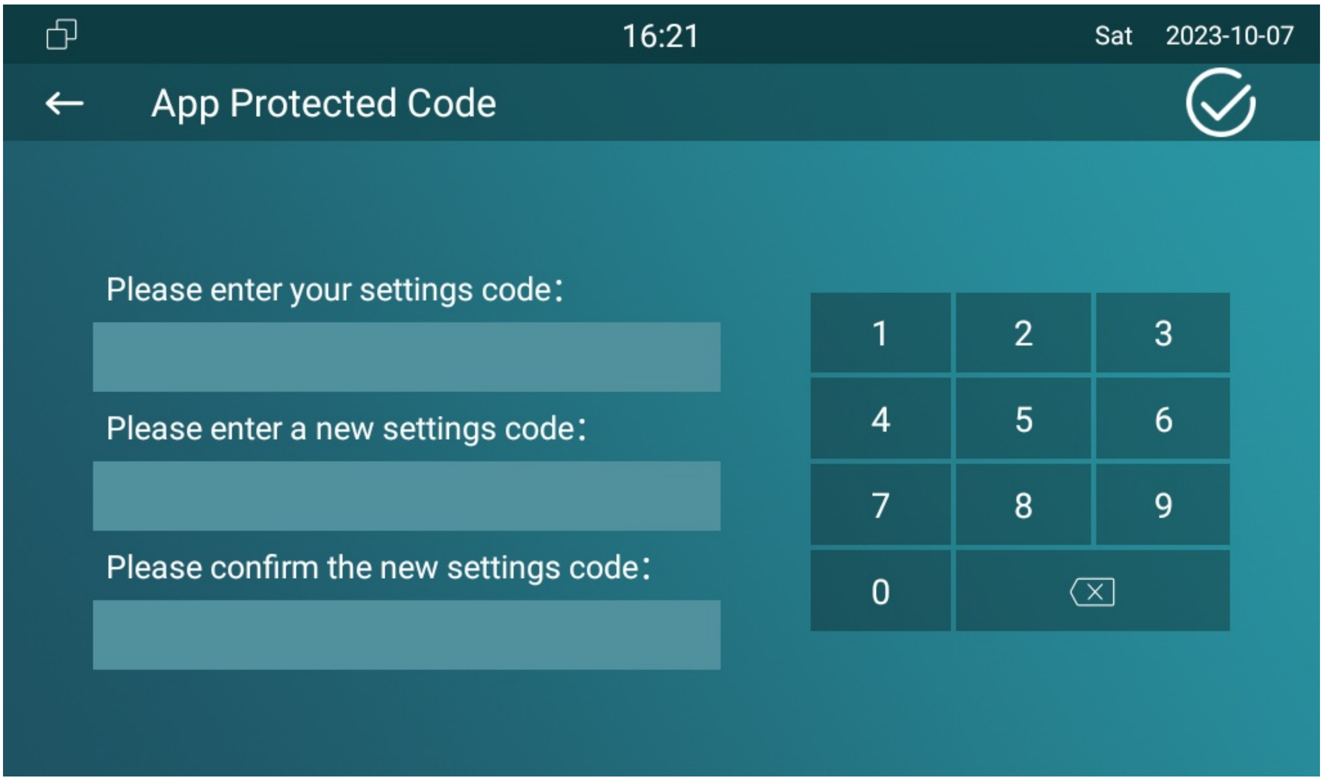
- There are two accounts, one is admin, its password is admin, the other is user, its password is user.

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.

Go to **Advance Settings > App Protected Code** screen.





App Protected Code

Please enter your settings code：

Please enter a new settings code：

Please confirm the new settings code：

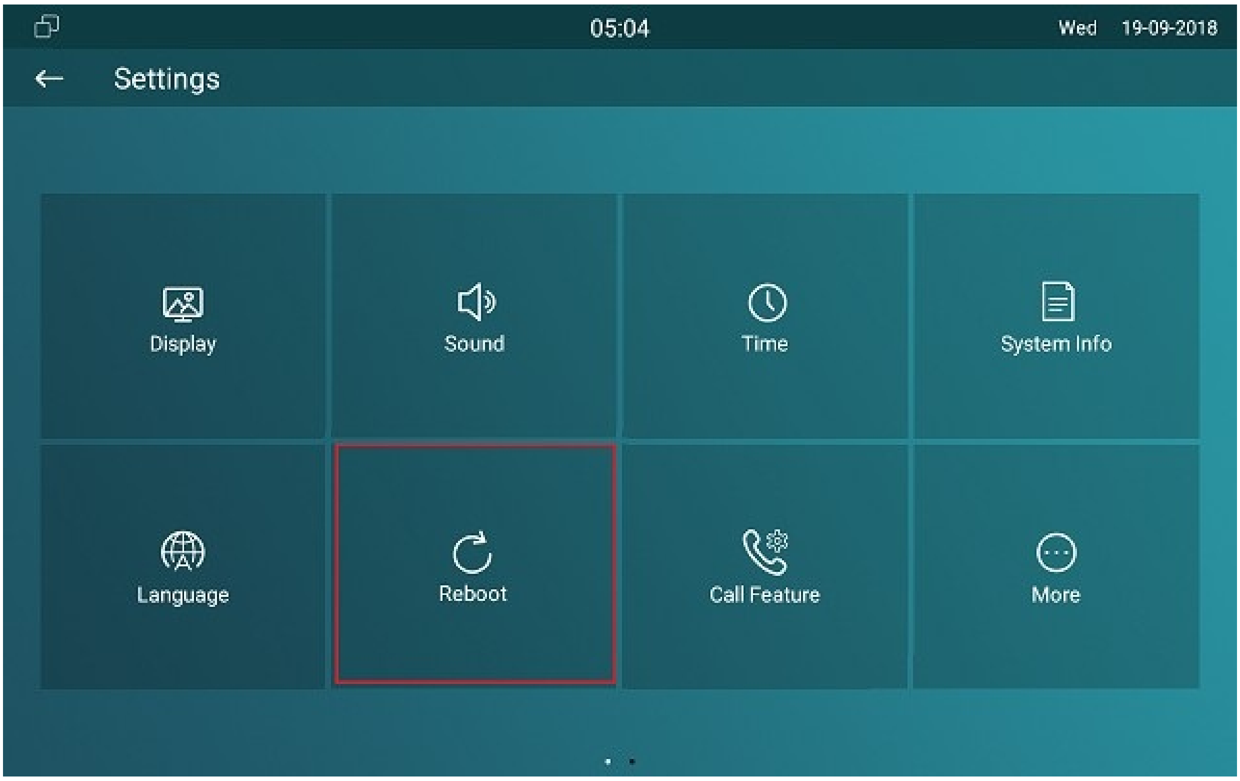
System Reboot & Reset

Reboot

Reboot on the Device

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

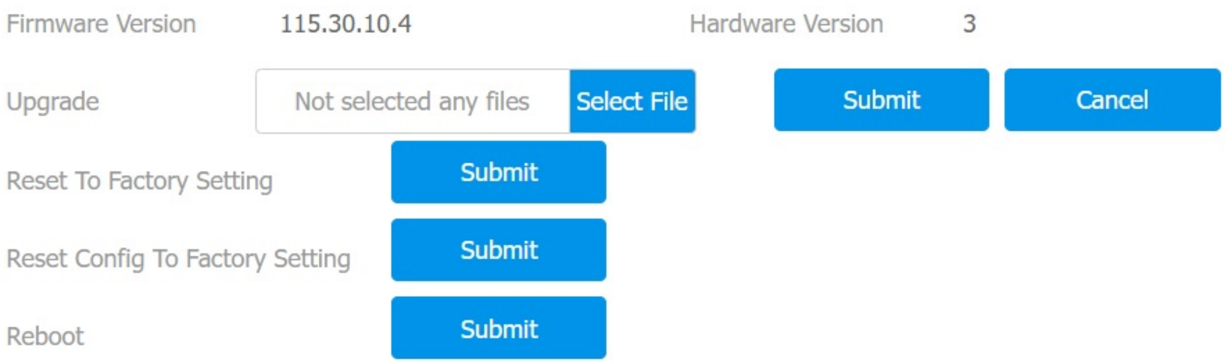
To reboot to the system setting on device **Settings >Reboot** screen.



Reboot on the Web Interface

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

To reboot the device on the web **Upgrade > Basic** interface.



Firmware Version 115.30.10.4 Hardware Version 3

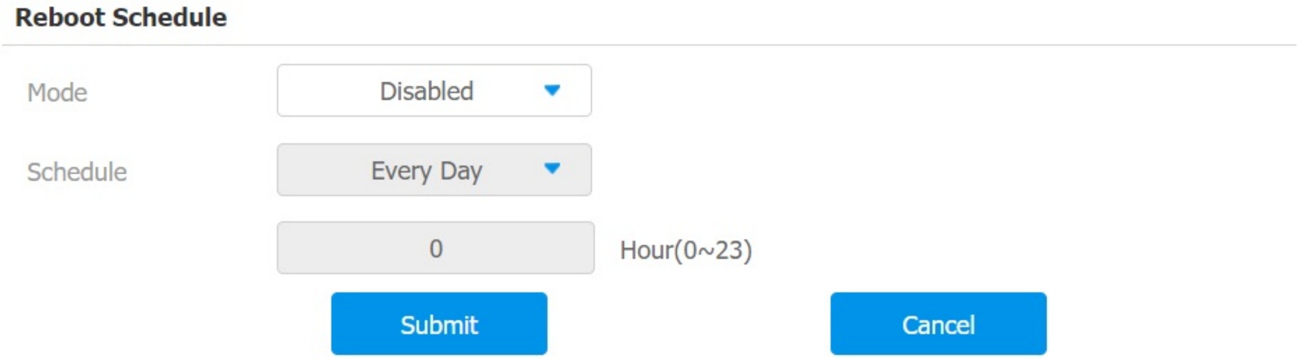
Upgrade: Not selected any files

Reset To Factory Setting

Reset Config To Factory Setting

Reboot

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



Reboot Schedule

Mode: Disabled

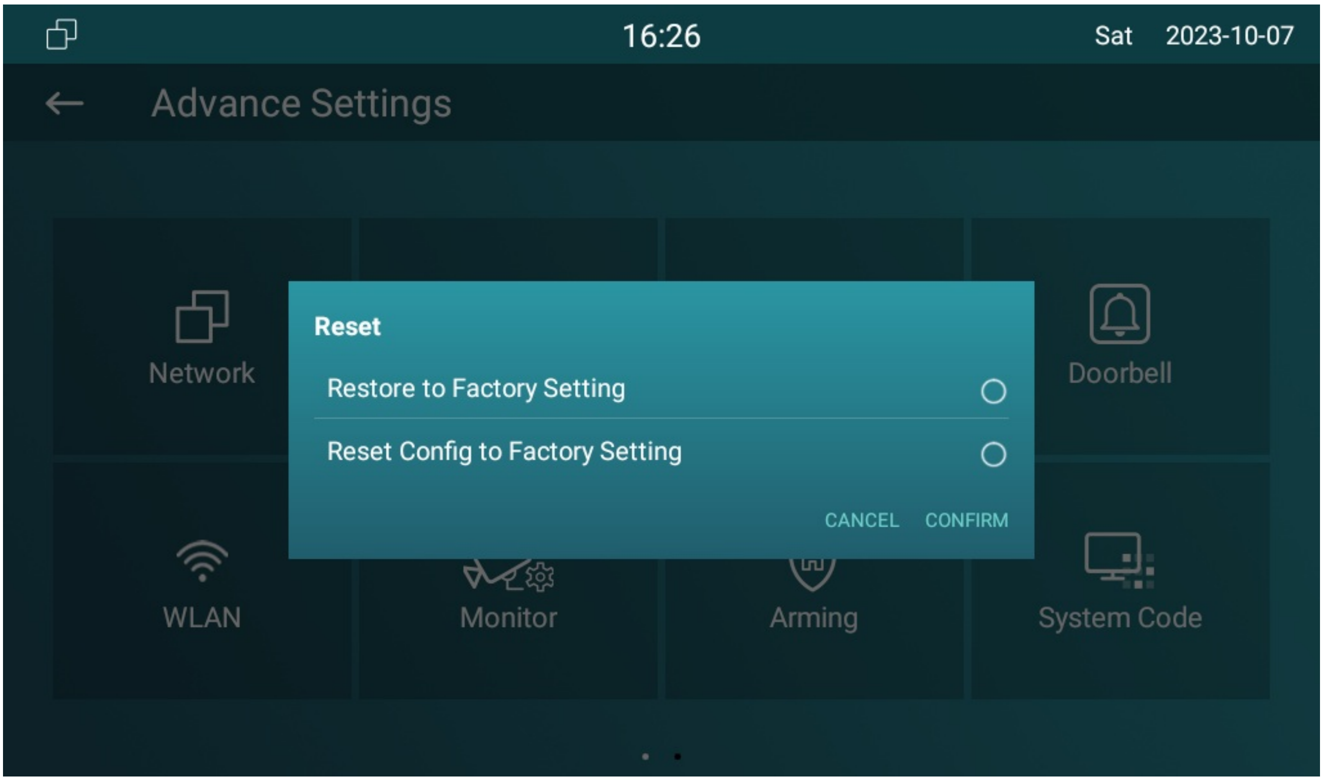
Schedule: Every Day

0 Hour(0~23)

Reset

Reset on the Device

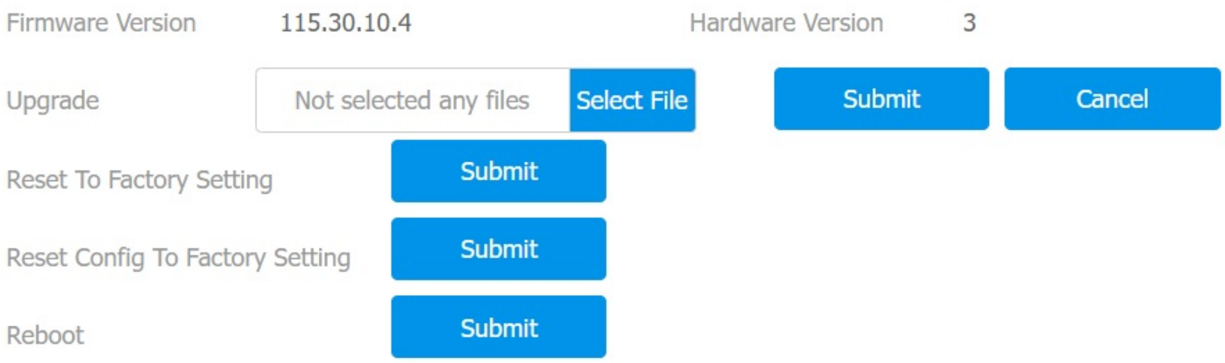
If you want to reset the whole device system to the factory setting, you can operate it directly on the device **Settings > Advance Settings** screen. If you only want to reset the configuration file to the factory setting instead of the whole device system, you can press **Reset Config to Factory Setting**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



Reset on the Web Interface

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

Go to **Upgrade > Basic** interface.



Firmware Version 115.30.10.4

Hardware Version 3

Upgrade Not selected any files