Table of Contents

Akuvox R49G Guard Phone Administrator Guide

About This Manual

Akuvox

Open A Smart World

WWW.AKUVOX.COM

AKUVOX R49G
GUARD PHONE
Administrator Guide

Thank you for choosing the Akuvox R49 guard phone. This manual is intended for administrators who need to properly configure the R49 guard phone. This manual applies to the 49.30.10.55 version, and it provides all the configurations for the functions and features of the guard phone. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Changelog

What's new in version 49.30.10.55:

- Support configuring the outbound proxy server.
- Support disabling the alarm feature.
- Support automatically recording videos and audio when the device makes calls.

The following optimization requires the device's connection to the SmartPlus Cloud.

- Support displaying the door-opening source(guard phone) on the SmartPlus App when users open doors on the device.
- Optimized call logs.

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

Indicator Light Status

No.	Indicator Light Type	Indicator Light Status
1	**Power Indicator Light**	● When the device is powered on the light will turn on . ● When the device starts on normally, the light will be on. ● When the device is powered off, the light will turn off .
2	**Network Connection indicator light**	● When the device is powered on but is not connected to the network, the light will be off. ● When the the device is powered on and the network is connected, the light will turn on immediately. ● When the device network is disconnected, the light will turn off. (the light will be turn on when the network is reconnected).
3	**Call Indicator Light**	● When there is no missing call or unread messages and the device is in stand-by status, the light will be off. ● When there is no missing call or unread messages and the device is in receiving incoming calls status, the light will be flickering. ● when there is no missing call or unread messages and the device is in dialing out status, the light will stay on. ● when there is no missing call or unread messages and the device is in dialing out status while receiving a incoming call, the light will be flickering. ● when there is no missing call or unread messages and the device is in calling status, the light will stay on. ● when there is missing call or unread messages and the device is in calling status while receiving a incoming call, the light will be flickering. ● when there is missing call or unread messages and the device is in stand-by status, the light will be flickering. ● when there is missing call or unread messages and the device is in dialing out status, the light will be flickering. ● when there is missing call or unread messages and the device is receiving an incoming call , the light will be flickering. ● when there is missing call or unread messages with new missing calls and unread messages, the light will be flickering.

Product Overview

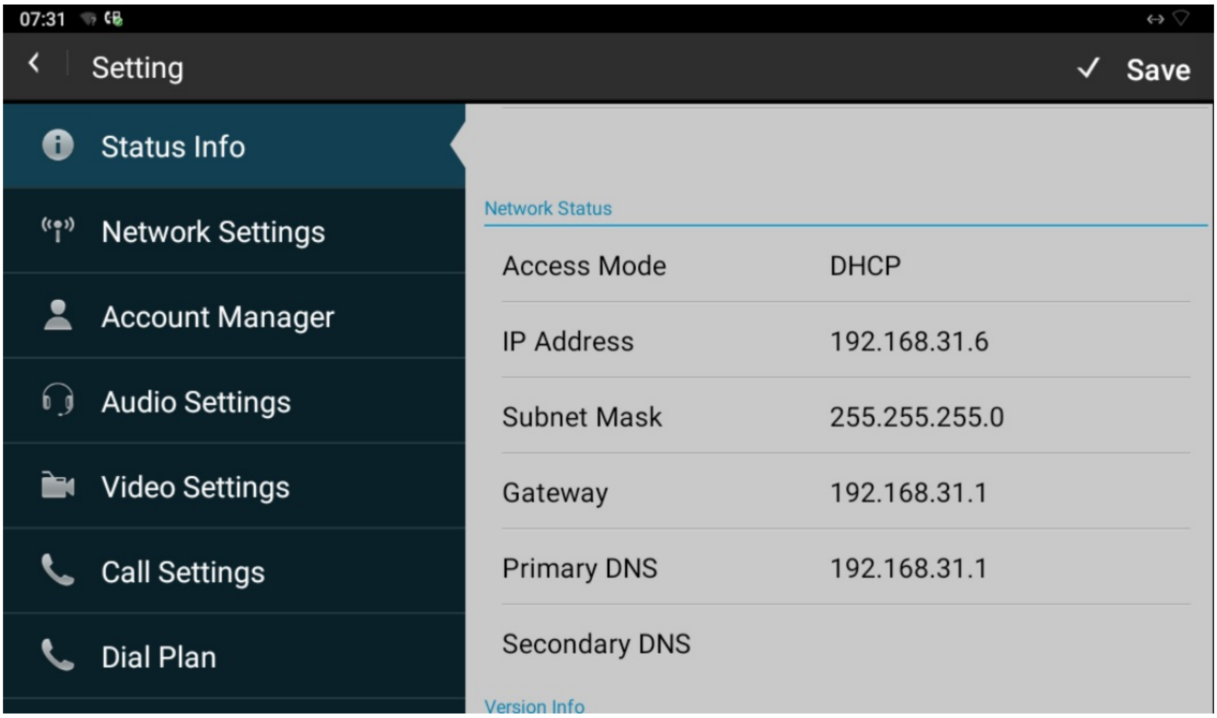
The cloud-based R49G guard phone can be deployed and maintained on the SmartPlus platform along with Akuvox door phones, indoor monitors, and the SmartPlus app incorporated with the guard phone as a whole in the community management. With the R49G guard phone, users will be able to build up the connection with door phones, indoor monitors, and the SmartPlus app in terms of making intercom calls, monitoring door phones, dealing with alarms triggered by the indoor monitors in a community, and receiving SOS messages. Moreover, R49G allows users to send notifications to the door phones and SmartPlus apps, create their local contacts in the devices, and set up monitoring locally.

Access the Device

The device’s system settings can be accessed directly or on the device's web interface.

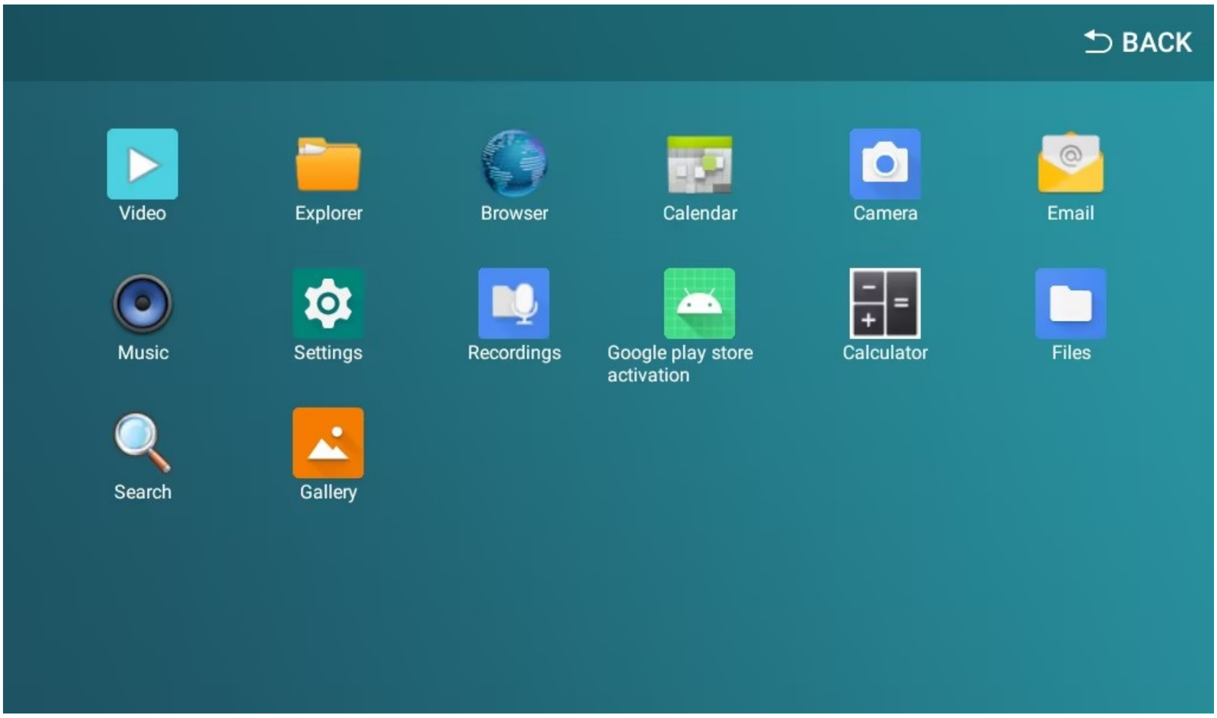
Access the Device Settings

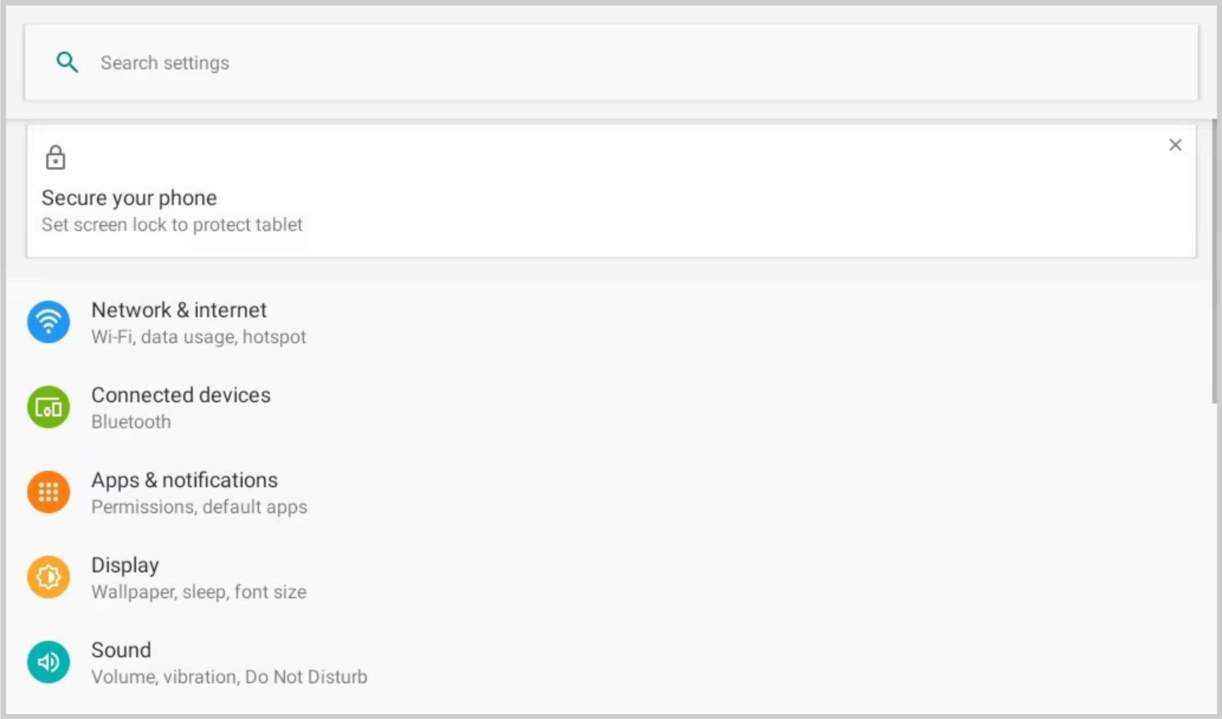
Tap ⚙ on the device home screen to enter the settings screen.



Access Mode	DHCP
IP Address	192.168.31.6
Subnet Mask	255.255.255.0
Gateway	192.168.31.1
Primary DNS	192.168.31.1
Secondary DNS	

Tap ⊞ on the device home screen and tap **Settings** to enter the advanced settings screen.

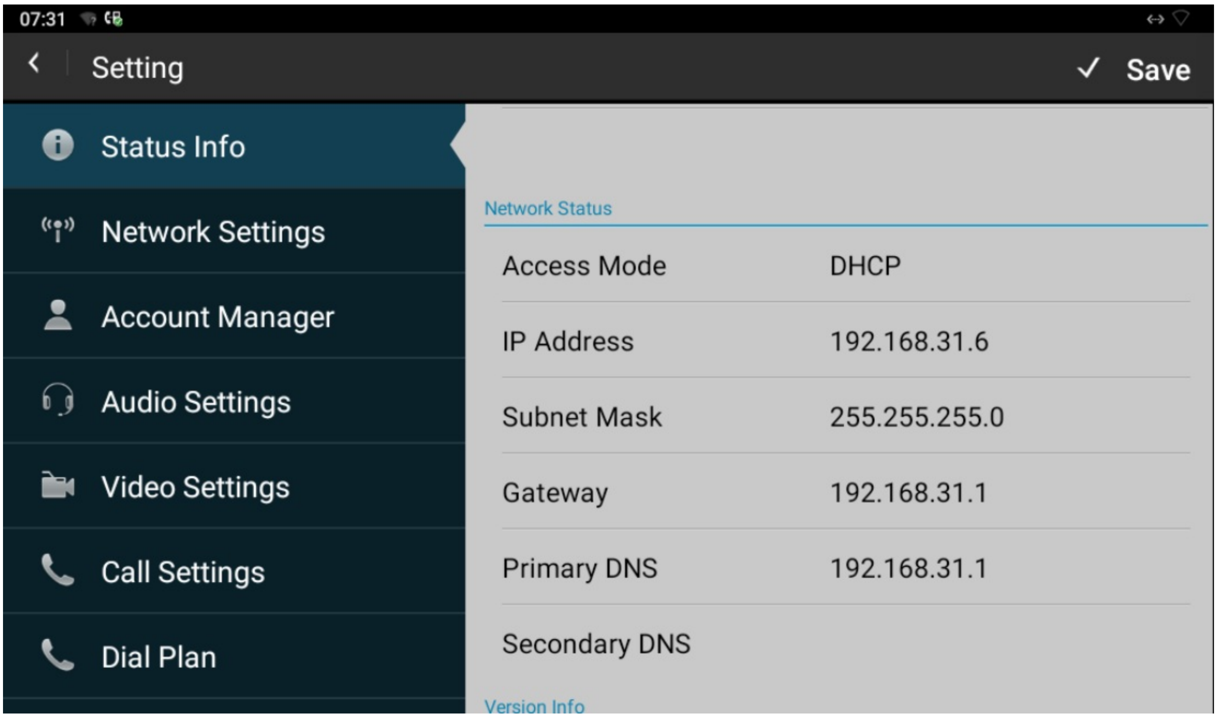



Search settings
Secure your phone
Set screen lock to protect tablet
Network & internet
Wi-Fi, data usage, hotspot
Connected devices
Bluetooth
Apps & notifications
Permissions, default apps
Display
Wallpaper, sleep, font size
Sound
Volume, vibration, Do Not Disturb

Access the Device’s Web Settings

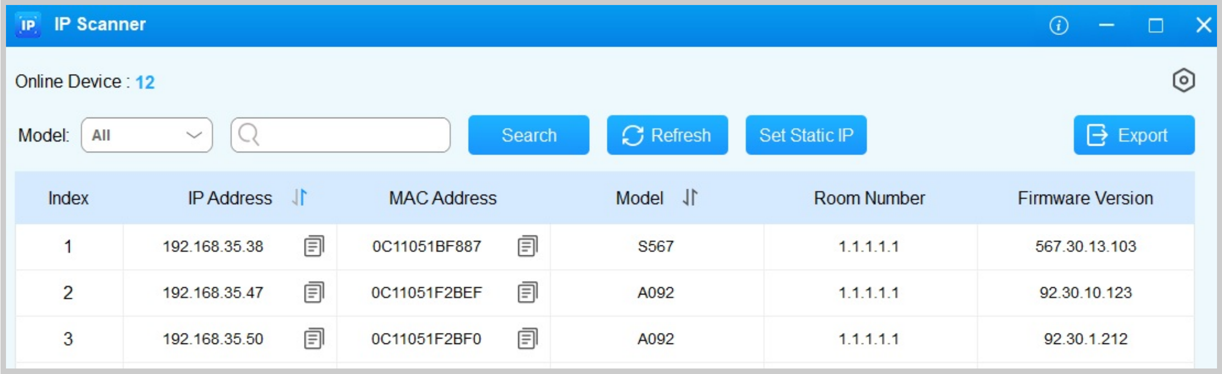
You can enter the device IP address in the web browser to log in to the device web interface.

Check the device IP on the **Settings > Status Info > Network Status** screen.



Access Mode	DHCP
IP Address	192.168.31.6
Subnet Mask	255.255.255.0
Gateway	192.168.31.1
Primary DNS	192.168.31.1
Secondary DNS	

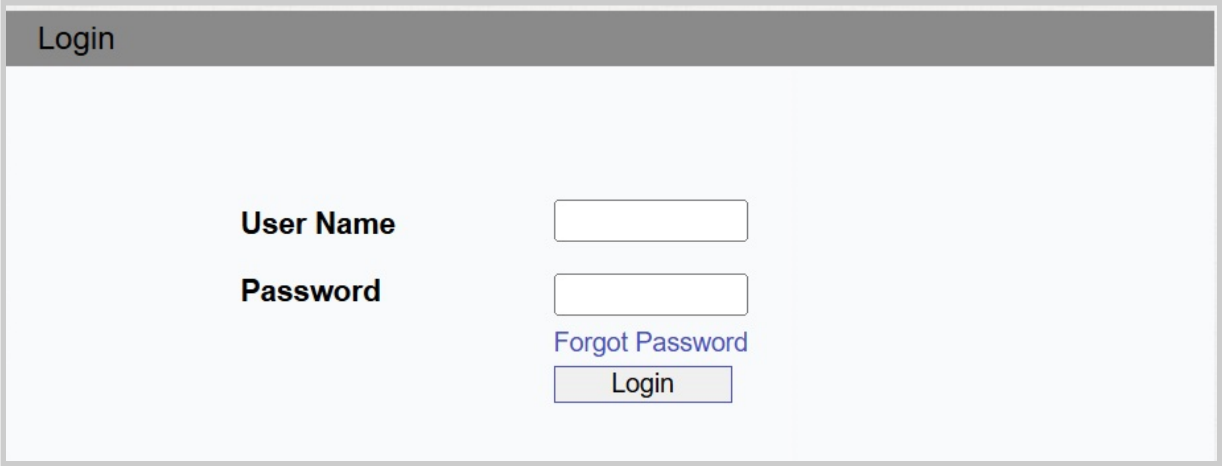
Or, search the device IP with the IP scanner on the same LAN network. Click **Refresh** to update the list.



Online Device : 12

Index	IP Address	MAC Address	Model	Room Number	Firmware Version
1	192.168.35.38	0C11051BF887	S567	1.1.1.1.1	567.30.13.103
2	192.168.35.47	0C11051F2BEF	A092	1.1.1.1.1	92.30.10.123
3	192.168.35.50	0C11051F2BF0	A092	1.1.1.1.1	92.30.1.212

The initial username and password are **admin,** and please be case-sensitive to the usernames and passwords entered.

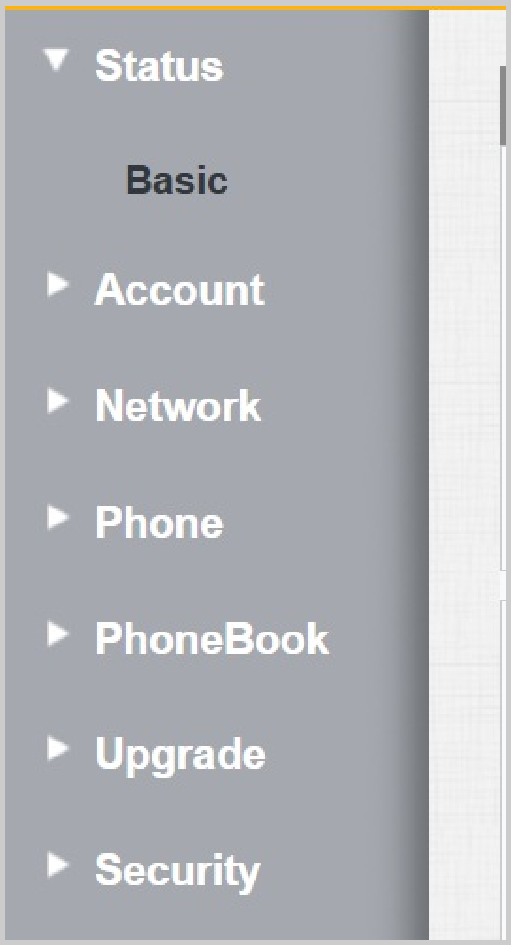


Note

- Download IP scanner: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- See the detailed guide: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Google Chrome browser is strongly recommended.
- Your computer should be on the same network as the device.

Introduction to the Configuration Menu

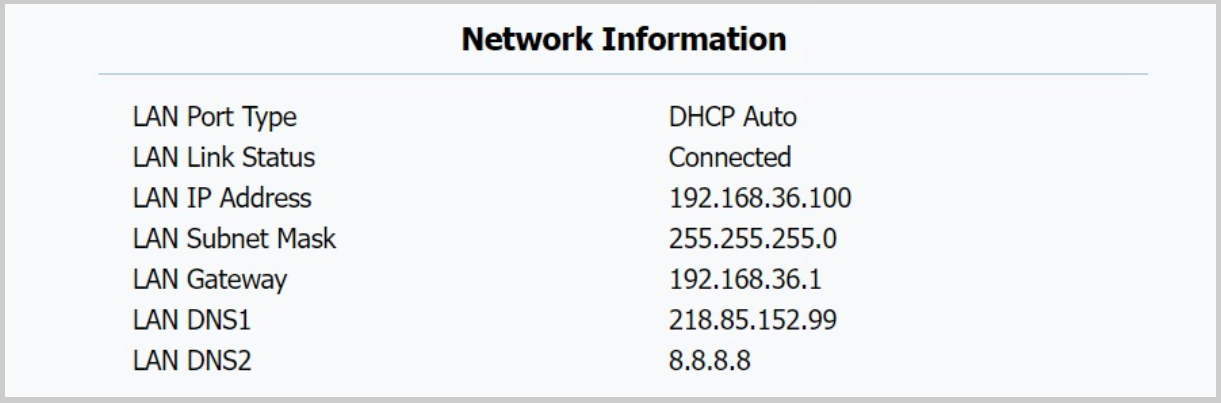
- **Status:** This section gives you basic information, such as product information, network information, account information, etc.
- **Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, etc.
- **Network:** This section mainly deals with DHCP & static IP settings, RTP port settings, device deployment, etc.
- **Phone**: This section covers time and language settings, volume control, call features, lift control, etc.
- **PhoneBook**: This section is for contact management.
- **Upgrade**: This section covers device upgrade, auto-provisioning, maintenance, etc.
- **Security**: This section covers web password modification, auto-answer allowlist, certificates upload, etc.



Network Setting

Device Network Status

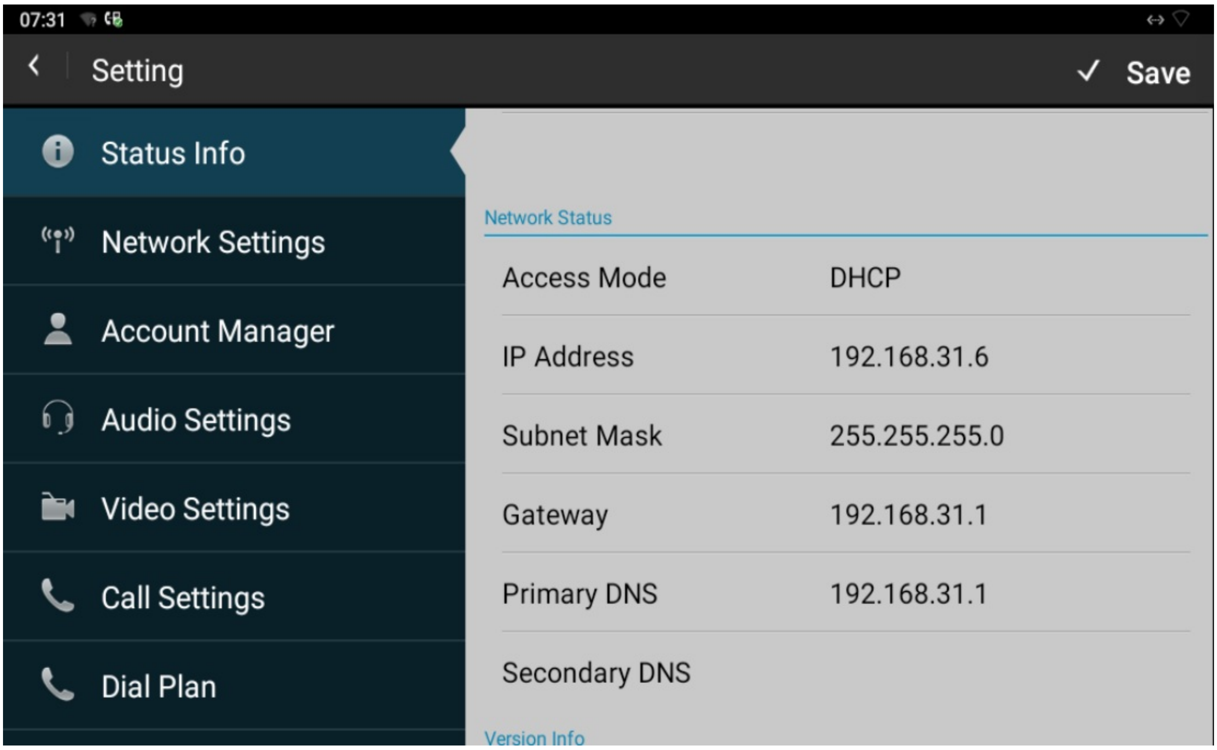
To check network status, navigate to the web **Status > Basic** interface.



Network Information

LAN Port Type	DHCP Auto
LAN Link Status	Connected
LAN IP Address	192.168.36.100
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

To check the network status on the device, navigate to the **Settings > Status Info > Network Status** screen.



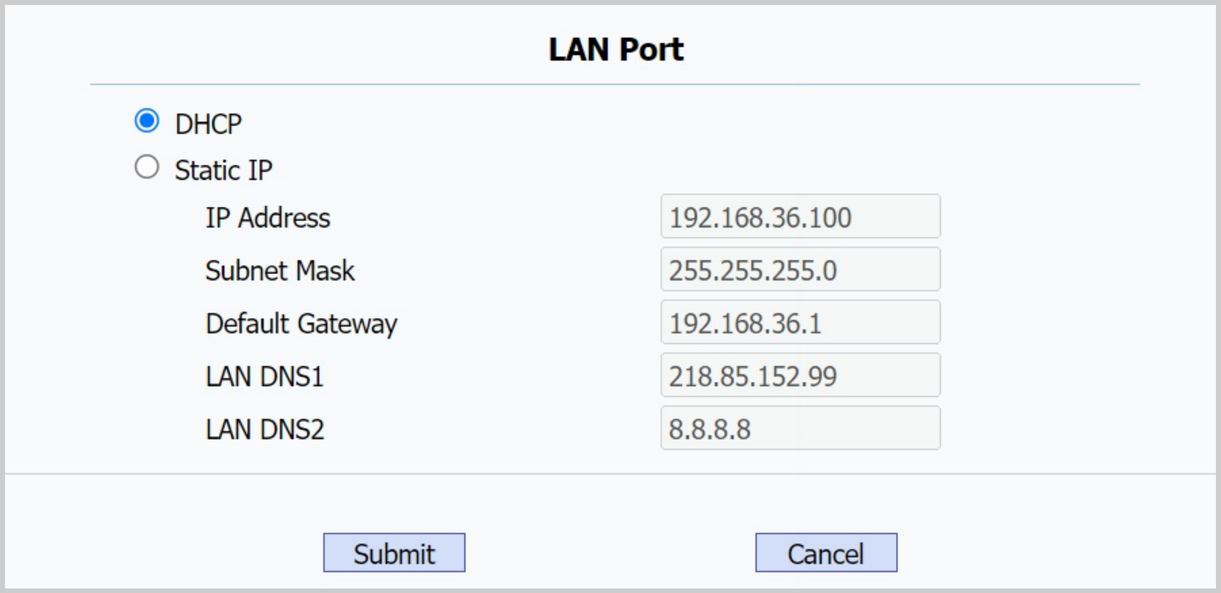
Network Status

Access Mode	DHCP
IP Address	192.168.31.6
Subnet Mask	255.255.255.0
Gateway	192.168.31.1
Primary DNS	192.168.31.1
Secondary DNS	

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.

Set it up on the web **Network > Basic** interface.



LAN Port

● DHCP

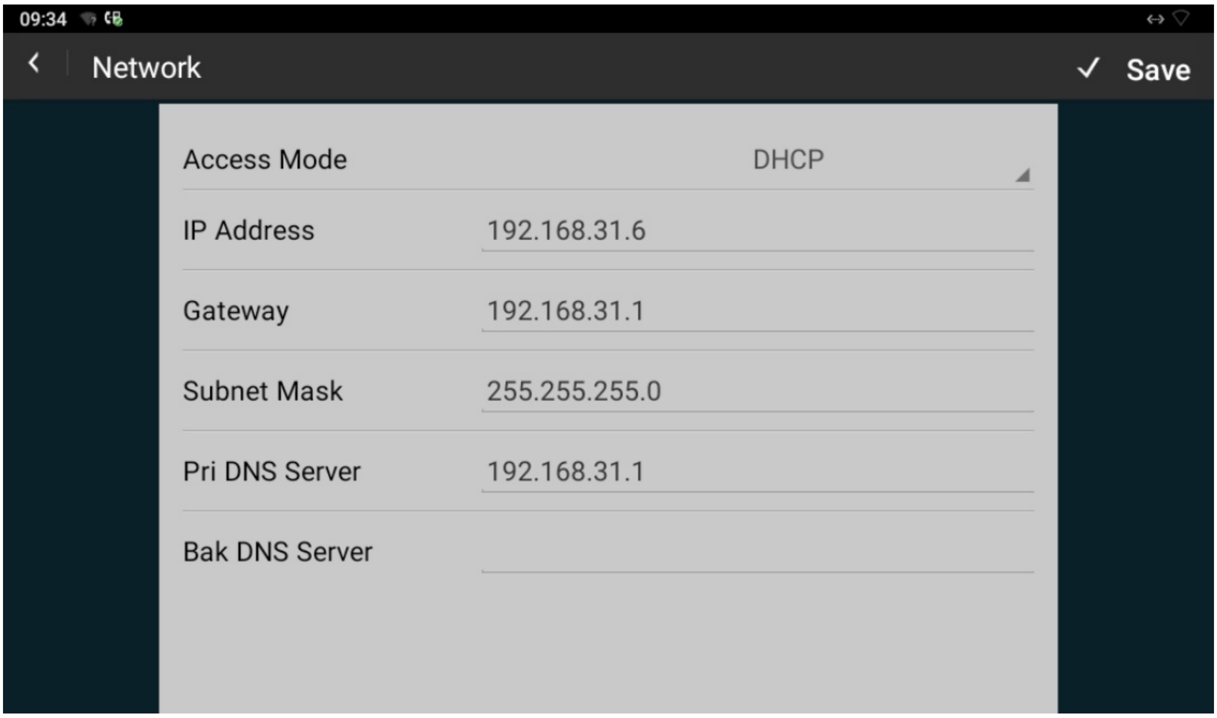
○ Static IP

IP Address	192.168.36.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.36.1
LAN DNS1	218.85.152.99
LAN DNS2	8.8.8.8

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

- **LAN DNS1/2**: Domain Name System(DNS) is the overall system or network that handles the translation of domain names (like www.example.com) into IP addresses (like 192.0.2.1), which computers use to identify each other on a network. The device connects to the alternate DNS server when the primary one is unavailable.

The device network can also be configured on the **Settings > Network Settings** screen.

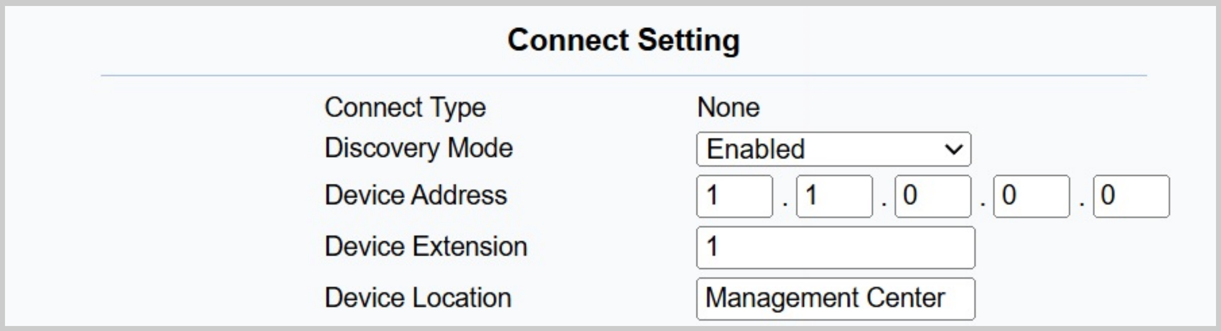


Access Mode	DHCP
IP Address	192.168.31.6
Gateway	192.168.31.1
Subnet Mask	255.255.255.0
Pri DNS Server	192.168.31.1
Bak DNS Server	

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.

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


Connect Setting

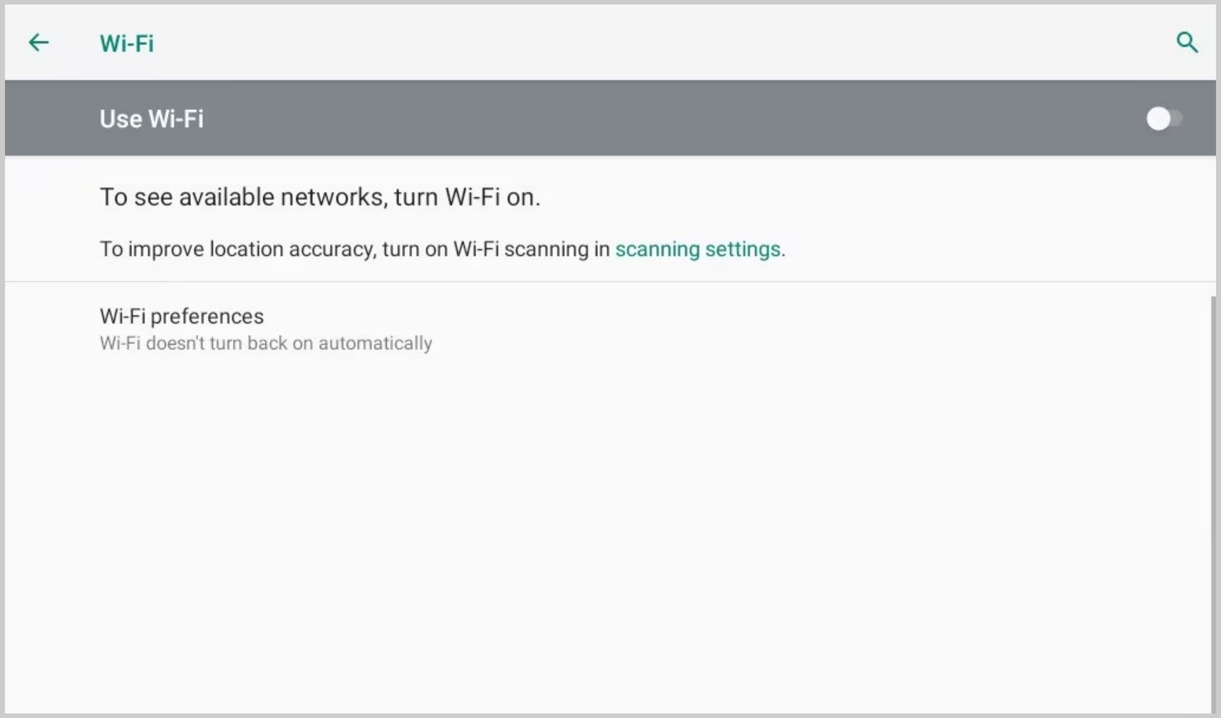
Connect Type	None
Discovery Mode	Enabled
Device Address	1 . 1 . 0 . 0 . 0
Device Extension	1
Device Location	Management Center

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

- **Discovery Mode**: Enabled by default. Available for the None server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.
- **Device Address**: Available for the None server mode. It can be used to call the device. Specify the device address by entering device location information from left to right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for the None server mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location where the device is installed and used.

Wi-Fi Connection

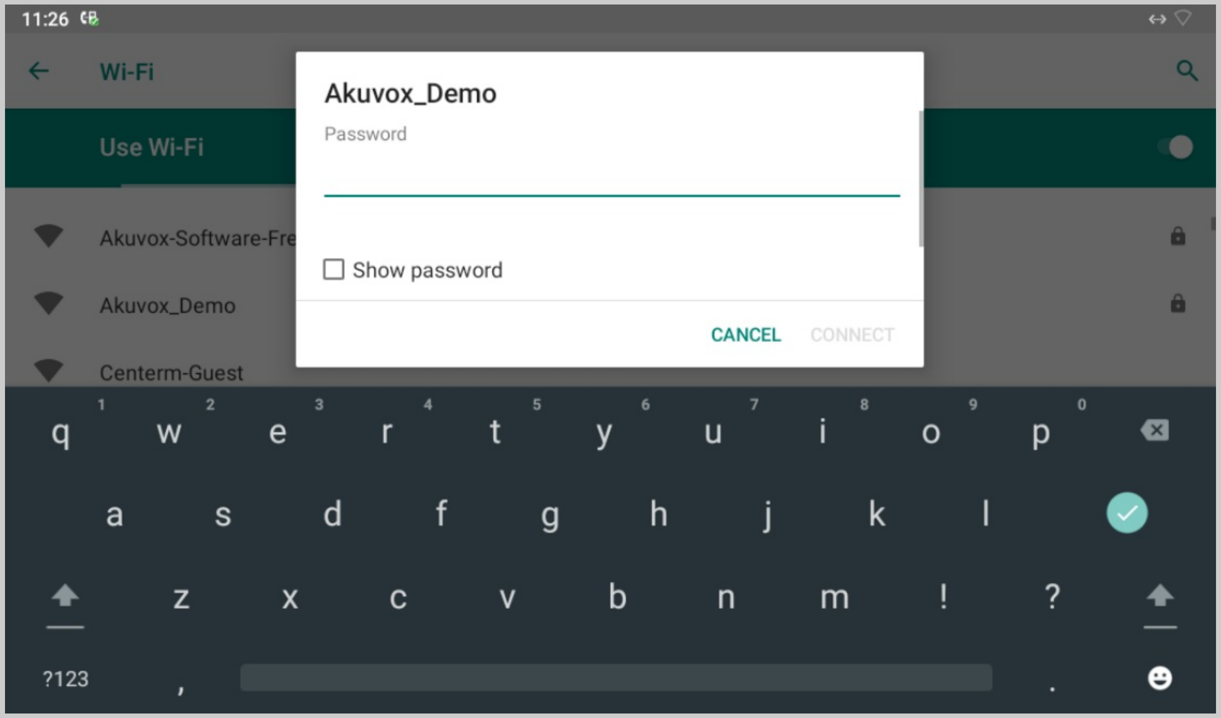
In addition to a wired connection, the device also supports a Wi-Fi connection. Slide down on the home screen and long-press on the Wi-Fi icon to enter the settings screen.



To see available networks, turn Wi-Fi on.

To improve location accuracy, turn on Wi-Fi scanning in scanning settings.

Wi-Fi preferences
Wi-Fi doesn't turn back on automatically



Akuvox_Demo
Password

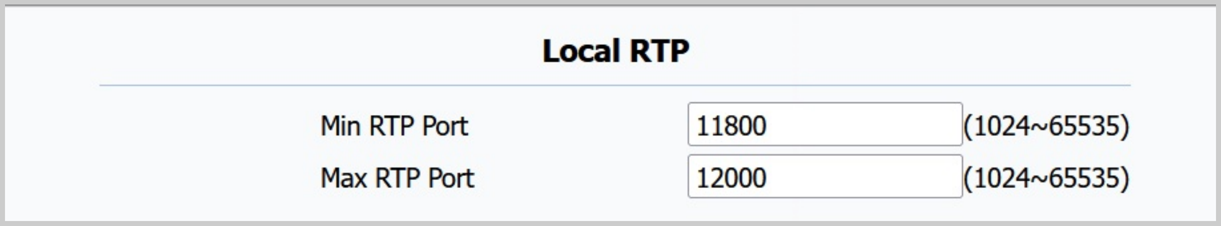
□ Show password

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.

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



Local RTP

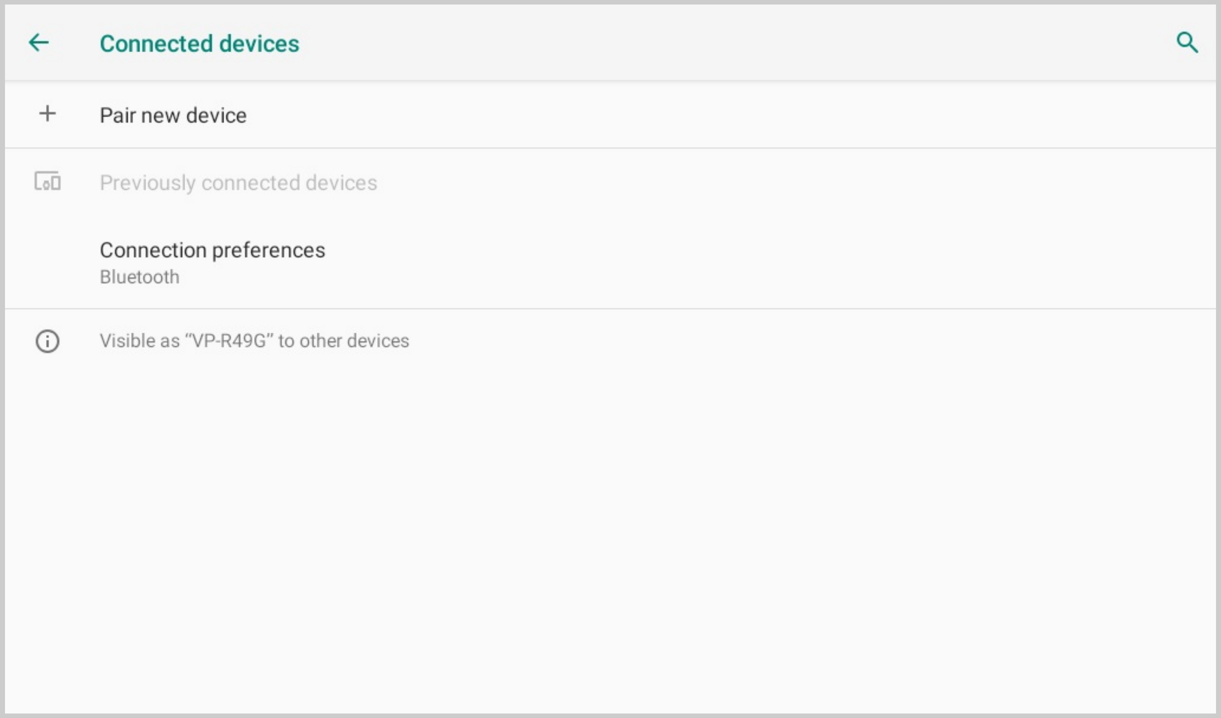
Min RTP Port	11800	(1024~65535)
Max RTP Port	12000	(1024~65535)

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

Bluetooth Configuration

To connect via Bluetooth, enable the Bluetooth function on the device to establish connections with other Bluetooth-enabled devices for file transfer and calls. Slide down on the home screen and long-press the Bluetooth icon to access the settings.

Tap **Pair new device** to establish connections.



Connected devices

+ Pair new device

Previously connected devices

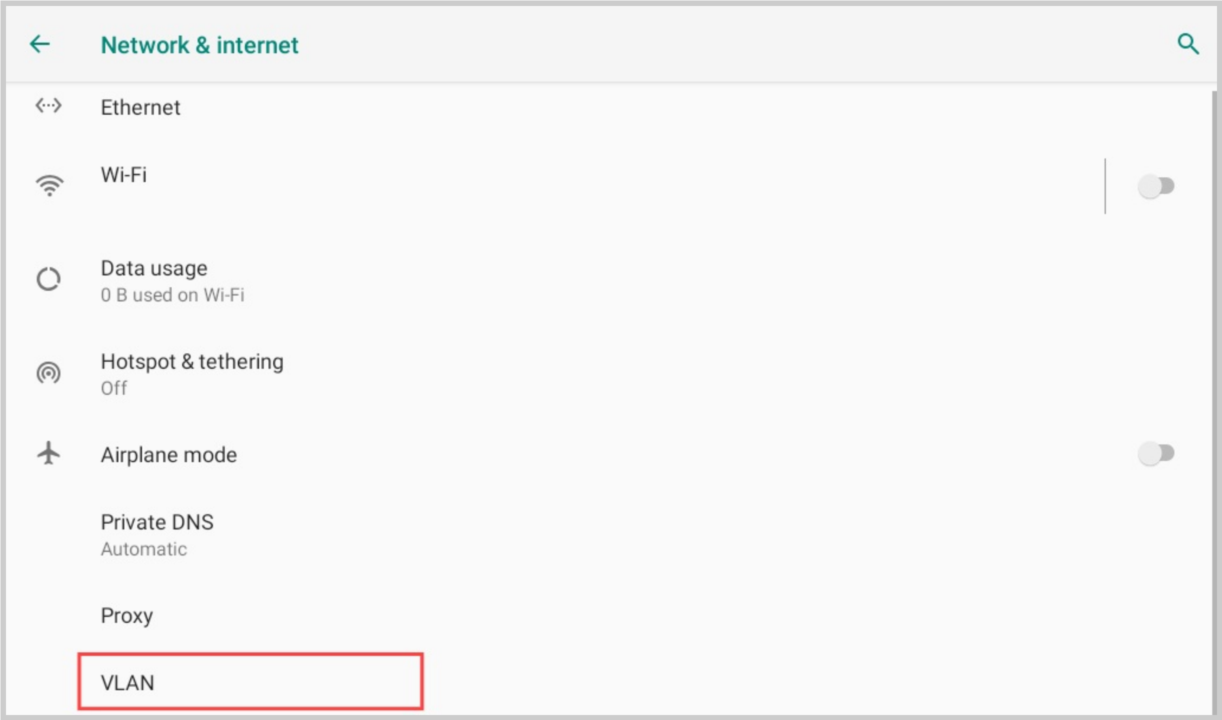
Connection preferences
Bluetooth

ⓘ Visible as "VP-R49G" to other devices

Device VLAN Configuration

A Virtual Local Area Network (VLAN) is a logical group of nodes from the same IP domain, regardless of their physical network segment. It separates the layer 2 broadcast domain via switches or routers, sending tagged packets only to ports with matching VLAN IDs. Utilizing VLANs enhances security by limiting ARP attacks to specific hosts and improves network performance by minimizing unnecessary broadcast frames, thereby conserving bandwidth for increased efficiency.

Tap ⊞ **> Settings > Network & Internet > VLAN** on the device screen.



Network & internet

Ethernet

Wi-Fi

Data usage
0 B used on Wi-Fi

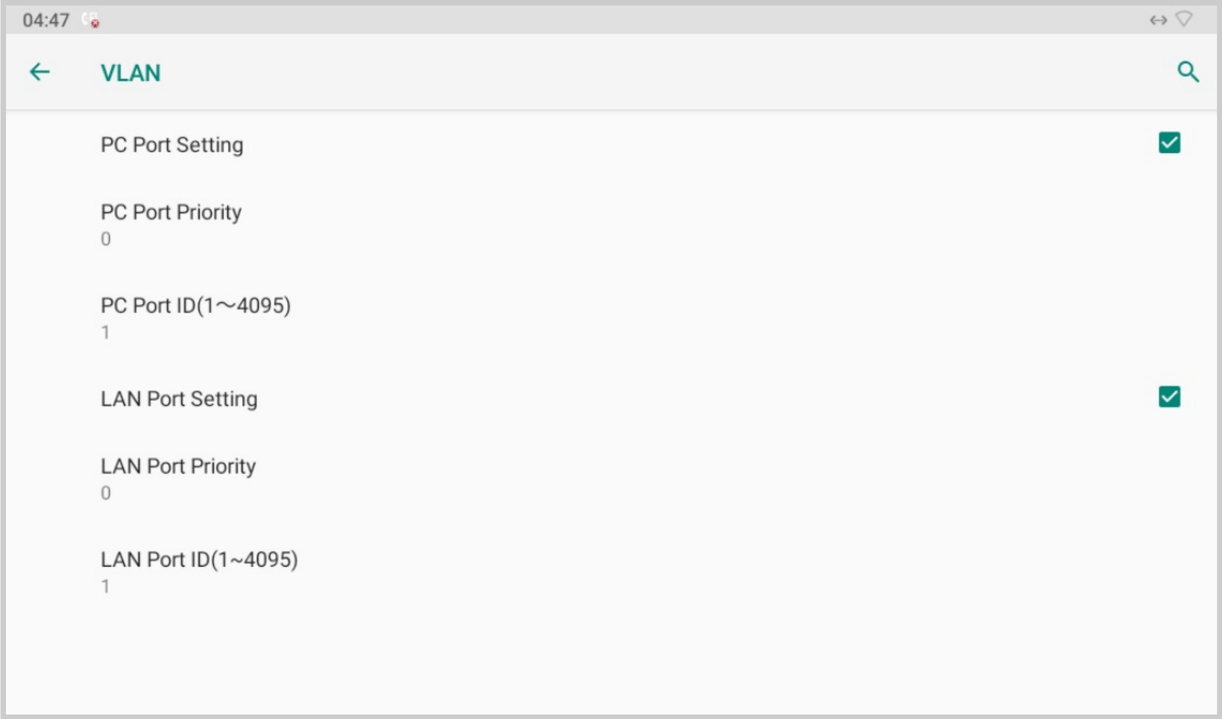
Hotspot & tethering
Off

Airplane mode

Private DNS
Automatic

Proxy

VLAN



04:47

VLAN

PC Port Setting ☑

PC Port Priority
0

PC Port ID(1~4095)
1

LAN Port Setting ☑

LAN Port Priority
0

LAN Port ID(1~4095)
1

- **PC Port Setting**: Enable it to connect the device to the VLAN network from the PC port on the device. R49 has two types of ports for the network connection: one is the PC port and the other is the LAN port. If you set the PC port for the VLAN network connection and connect the device to the network from the device's LAN port, then the setting will not be valid. The value is 0 by default.
- **PC Port Priority**: Select the PC port priority from 0-9. The higher the number is, the higher priority will be given to the VLAN in terms of sending out the data packets to the devices in the VLAN when network congestion occurs.
- **PC Port ID (1-4095)**: This parameter does not need to be filled in by the users. The ID is 1 by default.
- **LAN Port Setting**: Enable it to connect the device to the VLAN network from the LAN port on the device. R49 has two types of ports for the network connection: one is the PC port and the other is the LAN port. If you set the LAN port for the VLAN network connection and connect the device to the network from the device's PC port, the setting will not be valid. The value is 0 by default.
- **LAN Port Priority**: Select the PC port priority from 0-9. The higher the number is, the higher priority will be given to the VLAN in terms of sending out the data packets to the devices in the VLAN when network congestion occurs.

- **LAN Port ID (1-4095)**: Leave this field blank, as this parameter does not need to be filled in by the users. The ID is 1 by default.

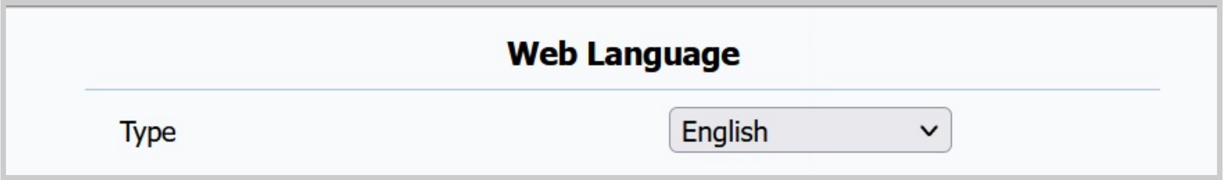
Language and Time

Language

Select languages on the web **Phone > Time/Lang** interface.

The device supports the following web languages:

English, Simplified Chinese, Traditional Chinese, Russian, Czech, Portuguese, Spanish, Dutch, French, German, Polish, Turkish, Japanese, and Ukrainian.

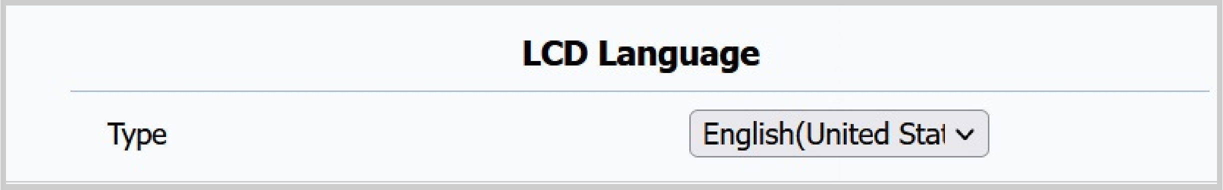


Web Language

Type: English

The device supports the following LCD languages:

English, German, Spanish, French, Italian, Dutch, Russian, Iranian, Simplified Chinese, Traditional Chinese, Japanese, Czech, and Ukrainian.

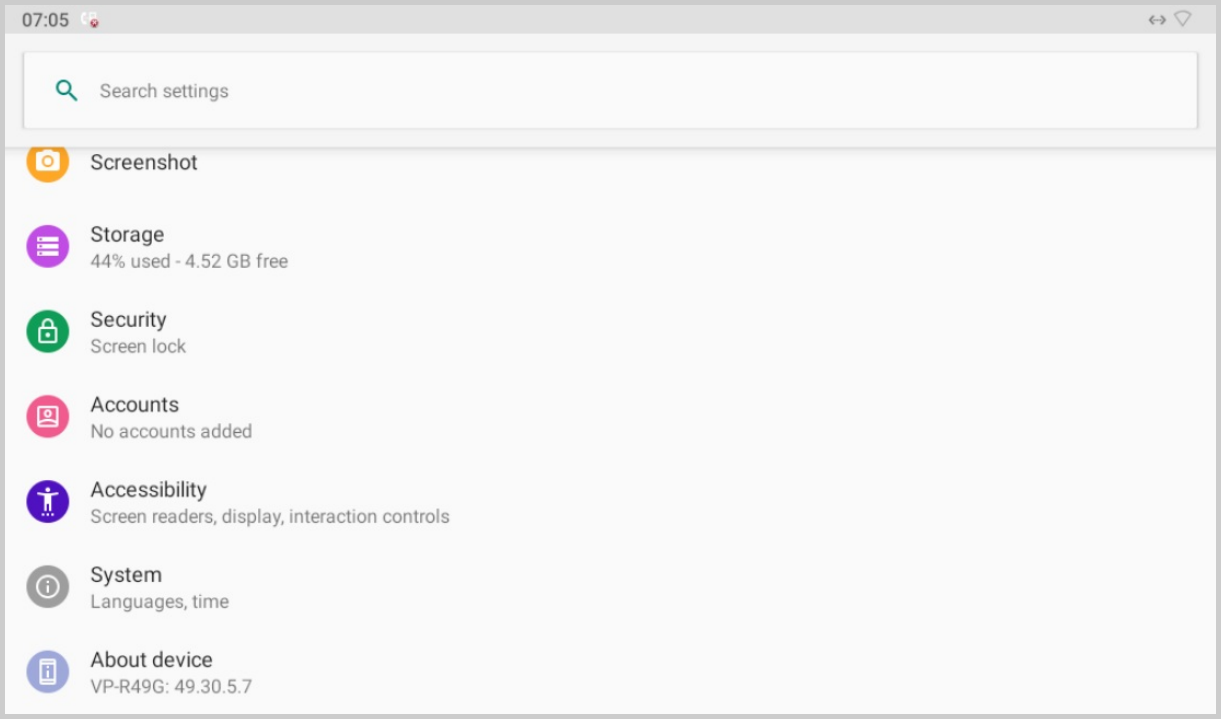


LCD Language

Type: English(United Stat

Languages can also be set on the device by tapping ⊞ **> Settings > System**. Then, tap **Languages & Input**.

Tap **Add a language** to add a new language; switch the LCD language by long-pressing the desired one and moving it to the top.


07:05

Search settings

Screenshot

Storage
44% used - 4.52 GB free

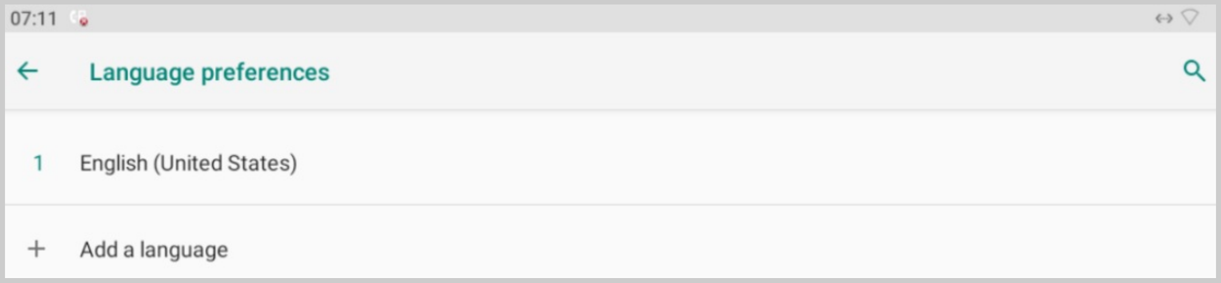
Security
Screen lock

Accounts
No accounts added

Accessibility
Screen readers, display, interaction controls

System
Languages, time

About device
VP-R49G: 49.30.5.7


07:11

Language preferences

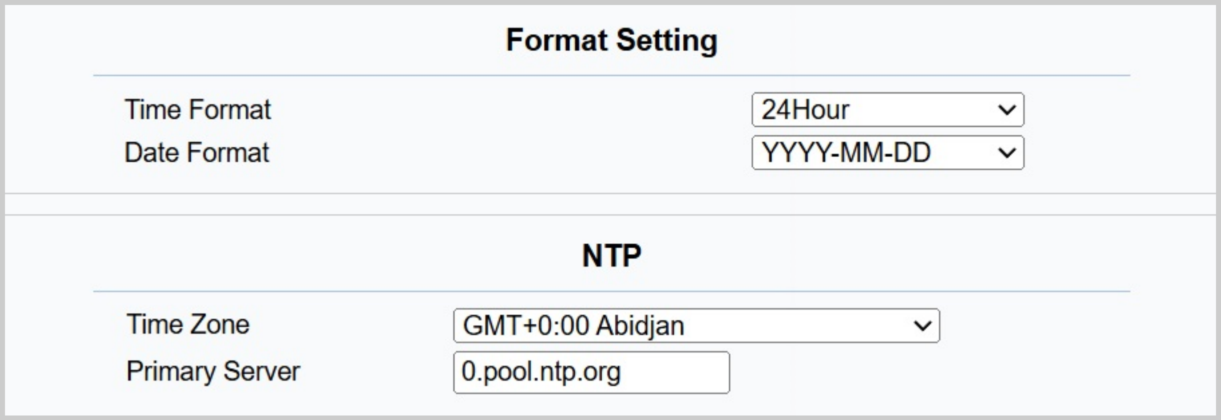
1 English (United States)

+ Add a language

Time

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

Set it up on the web **Phone > Time/Lang** interface.


Format Setting

Time Format	24Hour
Date Format	YYYY-MM-DD

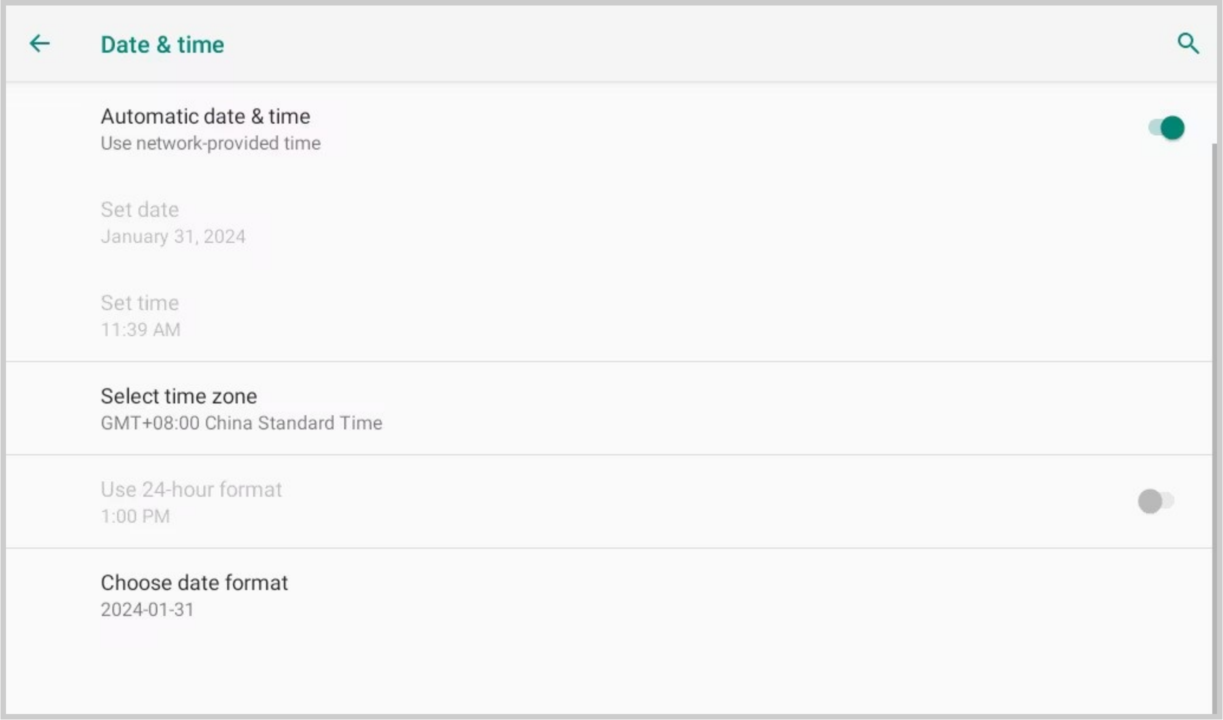
NTP

Time Zone	GMT+0:00 Abidjan
Primary Server	0.pool.ntp.org

- **Time Format**: 12-hour or 24-hour.

- **Date Format**: Select from the available options.
- **Time Zone**: Select the specific time zone based on where the device is used.
- **Primary Server**: The NTP server address.

Time can also be configured on the device ⊞ **> Settings > System > Date & Time** screen.



Date & time

Automatic date & time
Use network-provided time

Set date
January 31, 2024

Set time
11:39 AM

Select time zone
GMT+08:00 China Standard Time

Use 24-hour format
1:00 PM

Choose date format
2024-01-31

- **Automatic Date & Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Select Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Choose Date Format**: Select the desired date format.

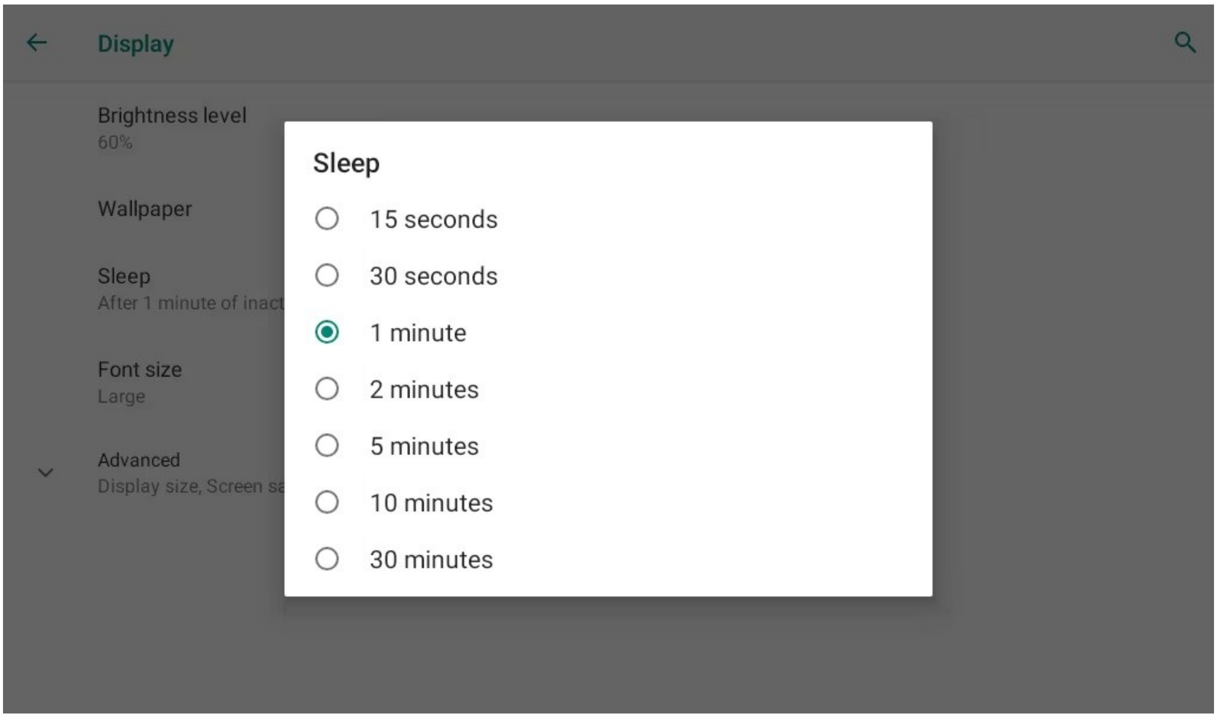
Screen Display

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

Sleep Mode

You can set the timing for the device to go into sleep mode. For example, if you set it to 1 minute, then the device will go into sleep mode when there is no operation for 1 minute.

Tap ⊞ **> Settings > Display > Sleep** on the device screen.



Display

Brightness level
60%

Wallpaper

Sleep
After 1 minute of inact

Font size
Large

Advanced
Display size, Screen sa

Sleep

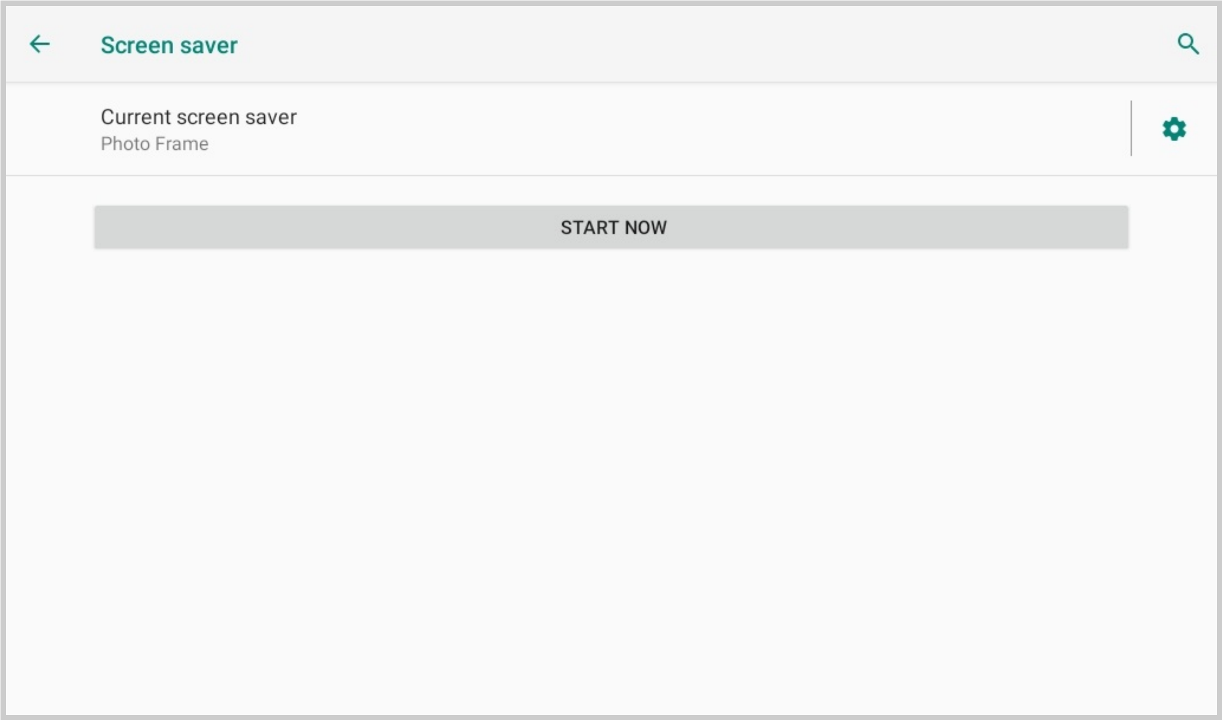
- ○ 15 seconds
- ○ 30 seconds
- ● 1 minute
- ○ 2 minutes
- ○ 5 minutes
- ○ 10 minutes
- ○ 30 minutes

Screensaver

The screensaver will be displayed after the device goes into sleep mode.

Tap ⊞ **> Settings > Display > Screen saver.** Select the desired screensaver type.

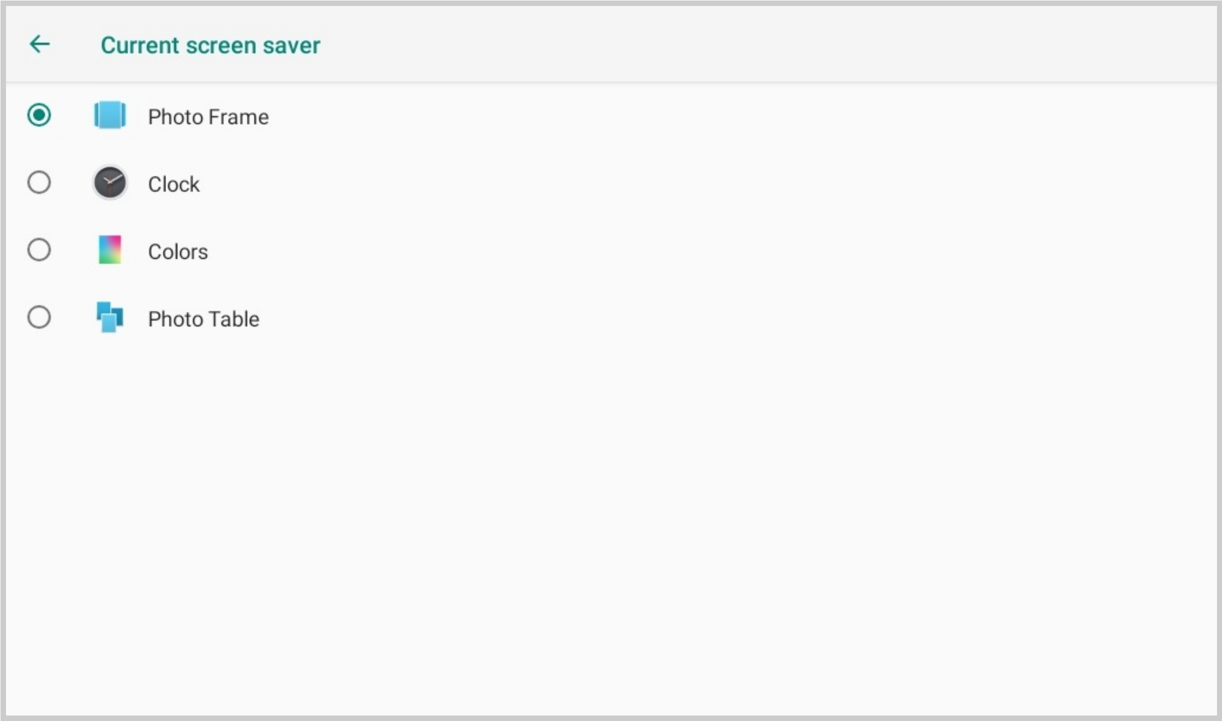
- Tap **START NOW** to display the screensaver right away.
- Tap ⚙ to select pictures as the screensaver.



Screen saver

Current screen saver
Photo Frame ⚙

START NOW



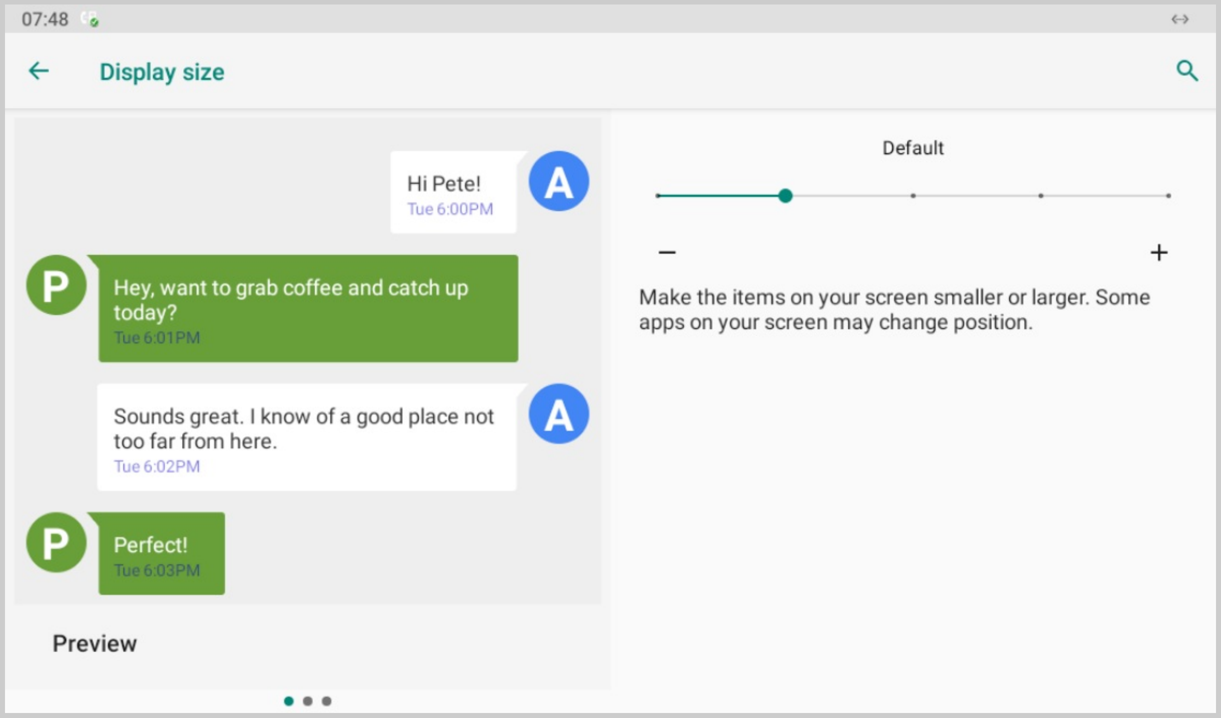
Current screen saver

● Photo Frame
○ Clock
○ Colors
○ Photo Table

Text Size

Users can amplify everything shown on the screen to see everything on the screen with greater ease.

Tap ⊞ **> Settings > Display > Display size.**

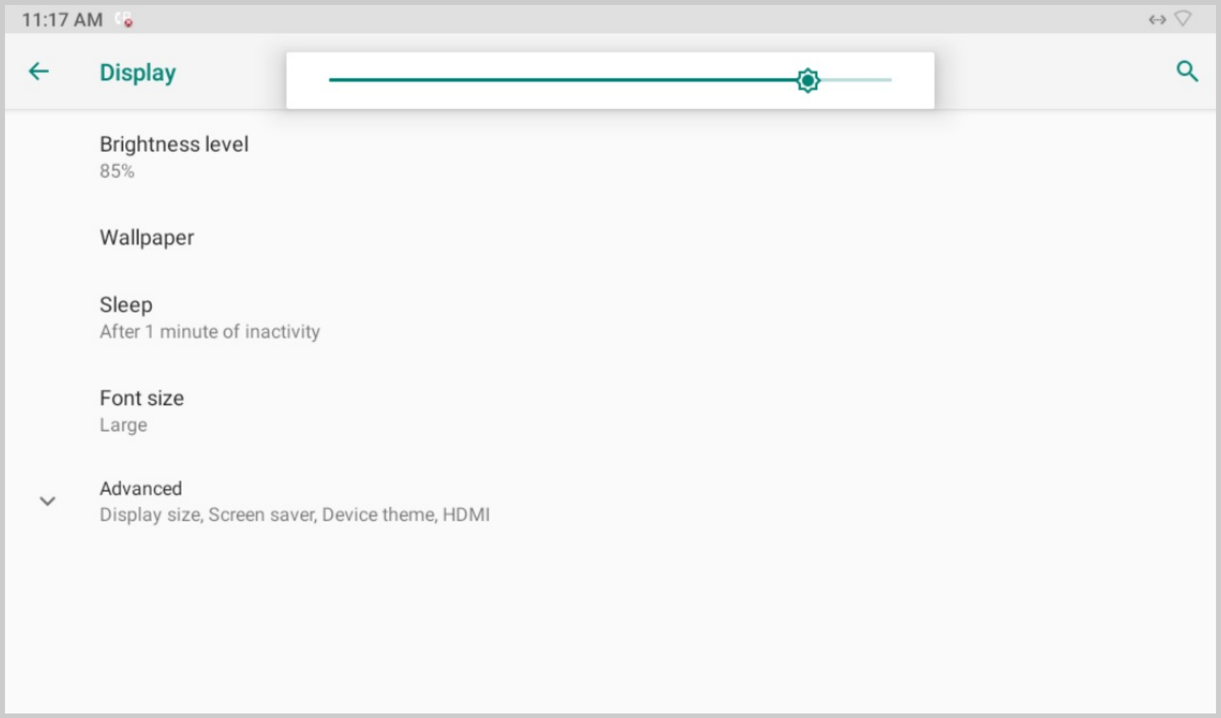


07:48
Display size
Hi Pete!
Tue 6:00PM
Hey, want to grab coffee and catch up today?
Tue 6:01PM
Sounds great. I know of a good place not too far from here.
Tue 6:02PM
Perfect!
Tue 6:03PM
Preview
Default
−
+

Make the items on your screen smaller or larger. Some apps on your screen may change position.

LCD Screen Brightness

Tap ⊞ **> Settings > Display** to enter the settings screen. Tap **Brightness Level** to adjust the brightness.



Brightness level
85%

Wallpaper

Sleep
After 1 minute of inactivity

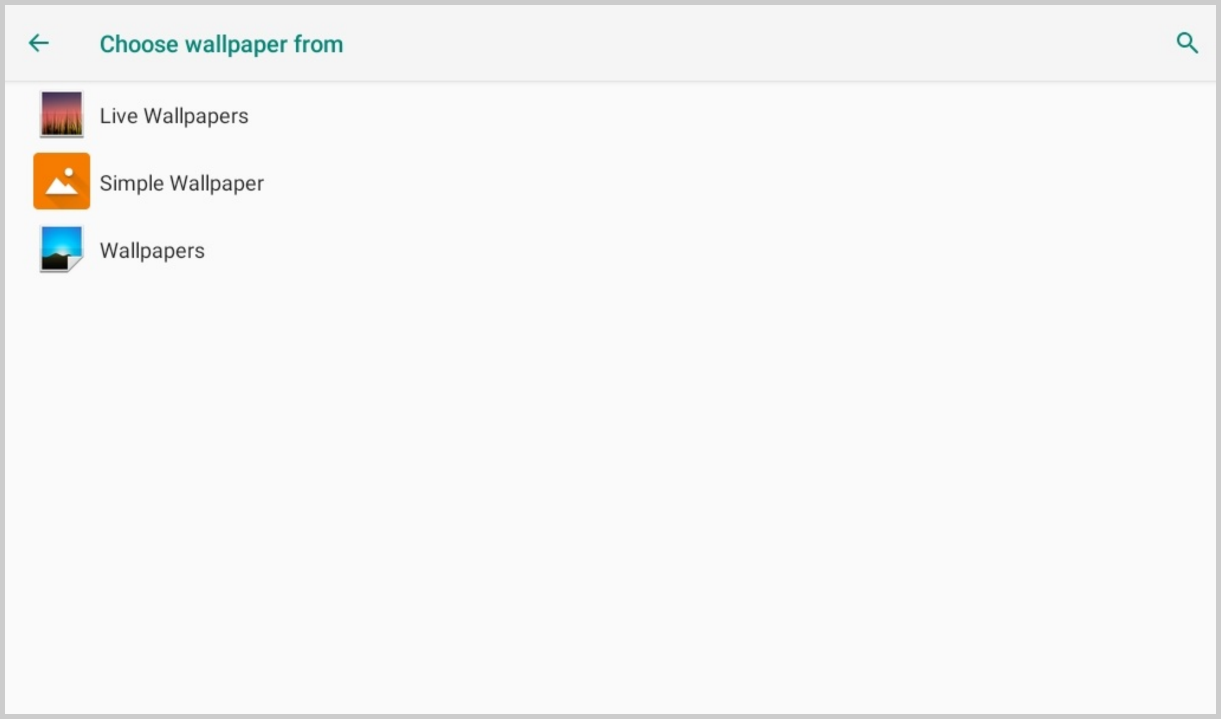
Font size
Large

Advanced
Display size, Screen saver, Device theme, HDMI

Wallpaper

The wallpaper will appear when the device goes into sleep mode or the lock screen status.

Tap ⊞ **> Settings > Display > Wallpaper** on the device screen.



Choose wallpaper from

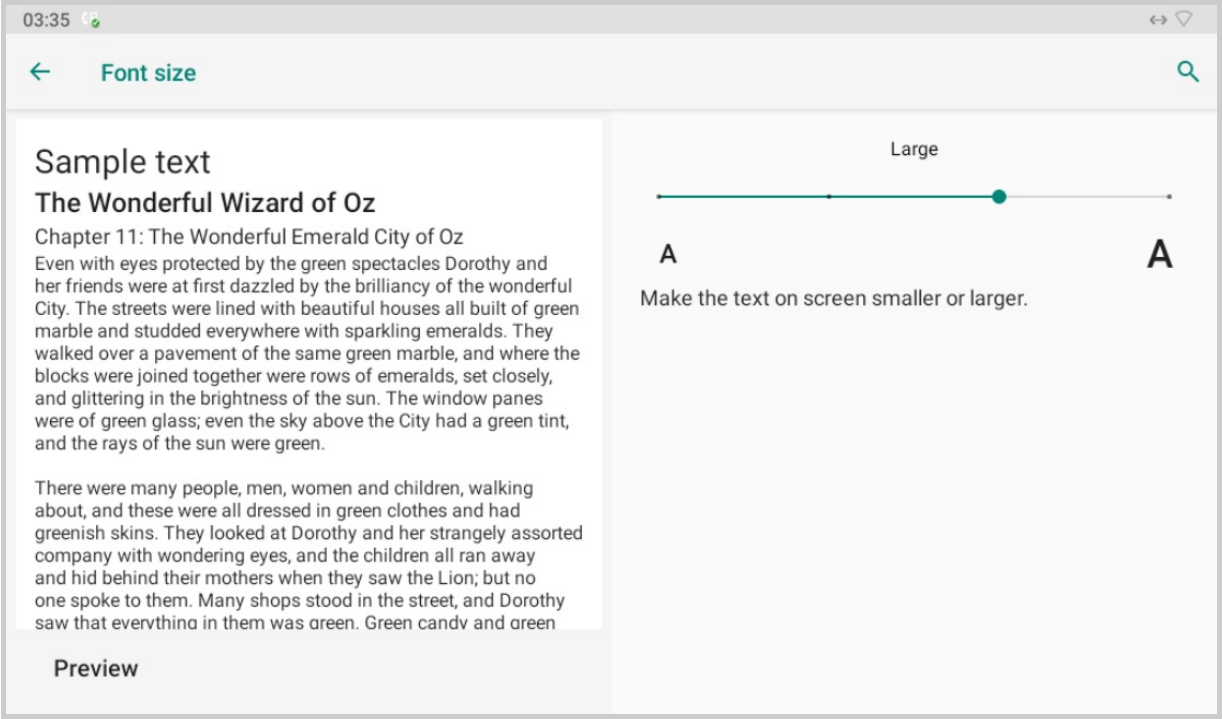
Live Wallpapers

Simple Wallpaper

Wallpapers

Font Size

Tap ⊞ **> Settings > Display > Font Size** on the device screen.



03:35

Font size

Sample text

The Wonderful Wizard of Oz

Chapter 11: The Wonderful Emerald City of Oz

Even with eyes protected by the green spectacles Dorothy and her friends were at first dazzled by the brilliancy of the wonderful City. The streets were lined with beautiful houses all built of green marble and studded everywhere with sparkling emeralds. They walked over a pavement of the same green marble, and where the blocks were joined together were rows of emeralds, set closely, and glittering in the brightness of the sun. The window panes were of green glass; even the sky above the City had a green tint, and the rays of the sun were green.

There were many people, men, women and children, walking about, and these were all dressed in green clothes and had greenish skins. They looked at Dorothy and her strangely assorted company with wondering eyes, and the children all ran away and hid behind their mothers when they saw the Lion; but no one spoke to them. Many shops stood in the street, and Dorothy saw that everything in them was green. Green candy and green

Preview

Large

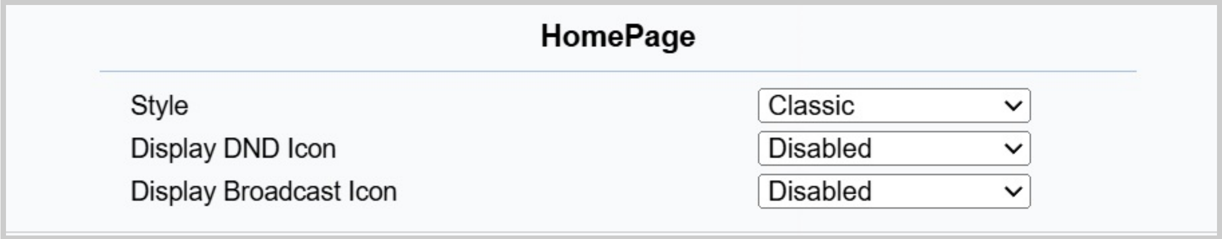
A A

Make the text on screen smaller or larger.

Home Screen Display

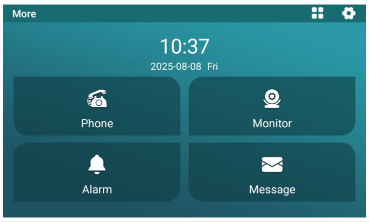
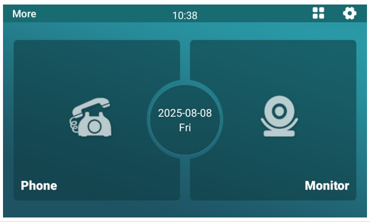
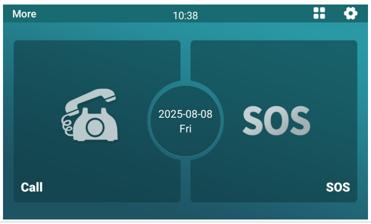
You can choose the home screen display among three options: **Classic, Only Phone And Monitor**, and **Home Care**.

Set it up on the web **Phone > Preference > HomePage** interface.



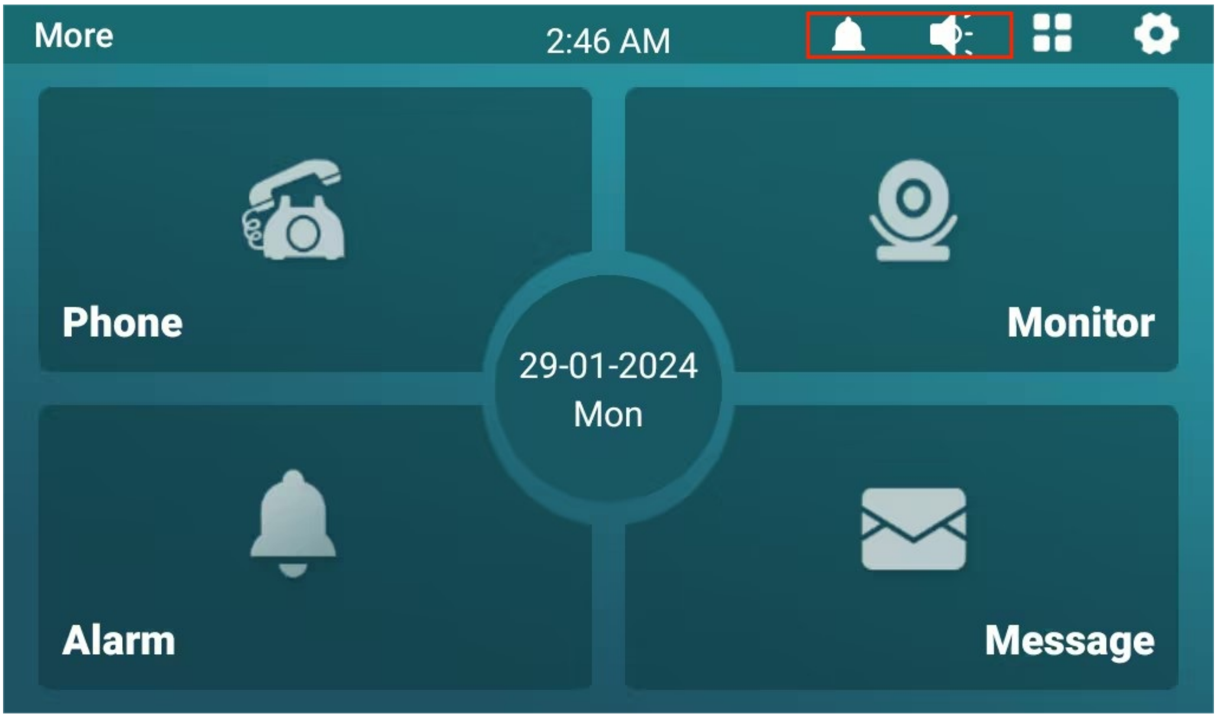
HomePage

Style	Classic
Display DND Icon	Disabled
Display Broadcast Icon	Disabled

Classic	Only Phone & Monitor	Home Care
 More 10:37 2025-08-08 Fri Phone Monitor Alarm Message		

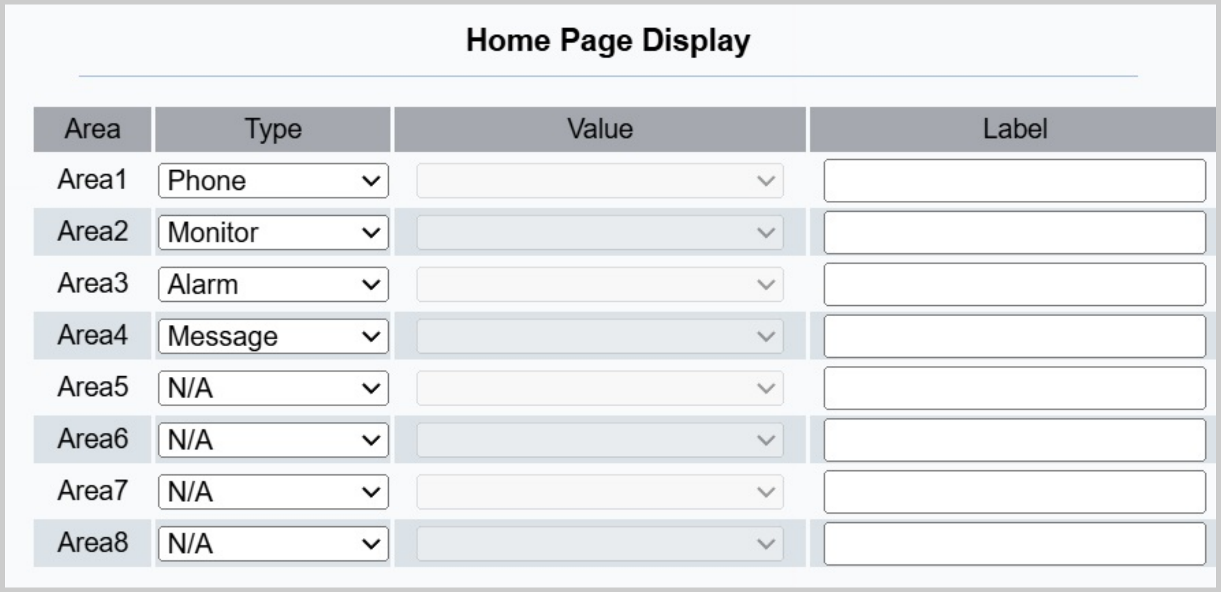
- **Display DND Icon**: Enable it to display the DND icon 🔔 on the home screen.

- **Display Broadcast Icon**: Enable it to display the broadcast icon 🔈 on the home screen.



Classic Style

In Classic style, you can choose the tabs to be displayed.



Home Page Display

Area	Type	Value	Label
Area1	Phone		
Area2	Monitor		
Area3	Alarm		
Area4	Message		
Area5	N/A		
Area6	N/A		
Area7	N/A		
Area8	N/A		

- **Type**: Select the functional icon to be displayed on the home screen.
- **Value**: Choose the unlock command when the Unlock type is selected.

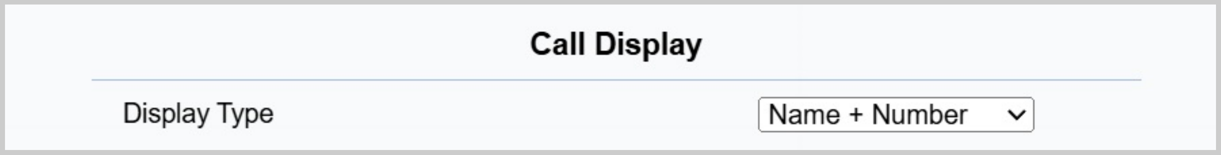
- **Label**: Name the icon.

> **Note**
>
> See Door Access Control Configuration chapter for setting up HTTP command.

Contact Display on the Call Screen

You can choose how to display contacts on the Call screen.

Set it up on the **Phone > Preference > Call Display** interface.



Call Display

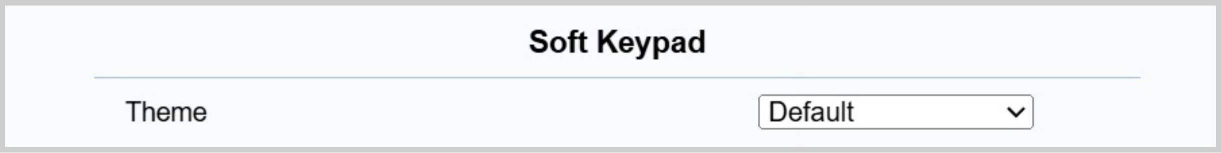
Display Type: Name + Number

- **Display Type**:
  - **Name+Number**: The contact name and number will be displayed.
  - **Name**: Only the contact name will be displayed.

Keypad Display

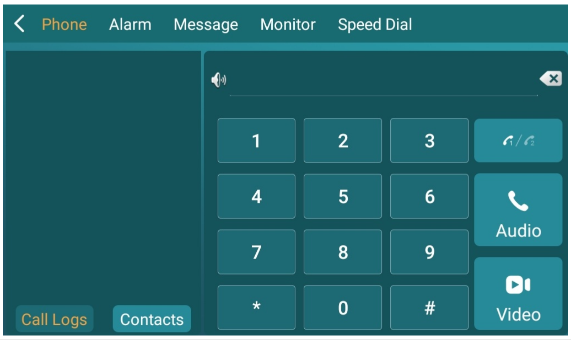
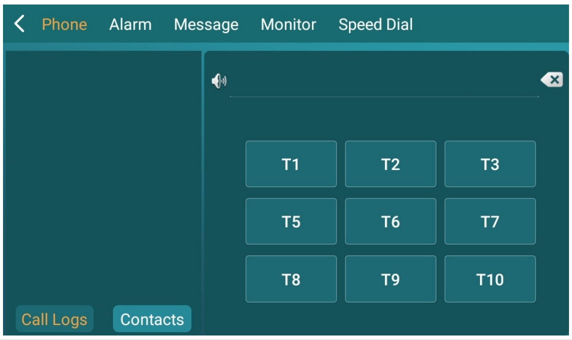
The device has two keypad display modes catering to different needs.

Set it up on the **Phone > Preference** interface. When Alphanumeric is selected, you can name each key.



Soft Keypad

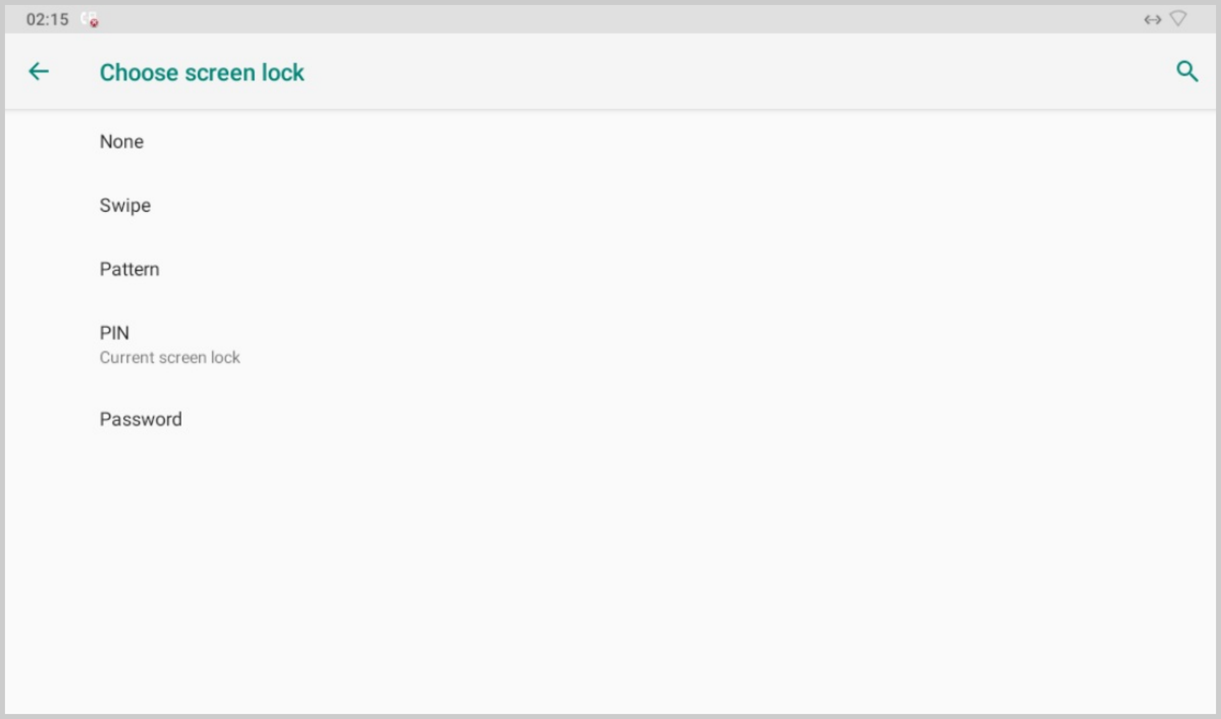
Theme: Default

Default	Alphanumeric
 Phone Alarm Message Monitor Speed Dial 1 2 3 4 5 6 7 8 9 * 0 # Audio Video Call Logs Contacts	 Phone Alarm Message Monitor Speed Dial T1 T2 T3 T5 T6 T7 T8 T9 T10 Call Logs Contacts

Screen Lock Setting

You can set up a screen lock on the guard phone for security.

Tap ⊞ **> Settings > Security > Screen Lock** on the device screen.



Choose screen lock

None

Swipe

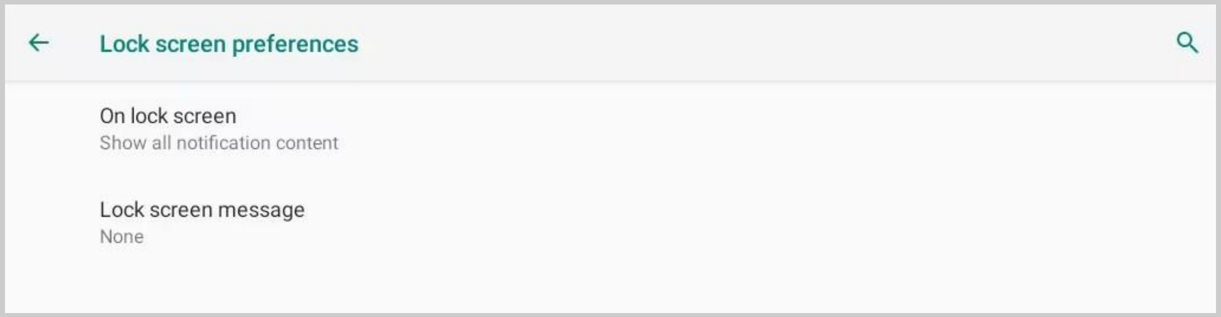
Pattern

PIN
Current screen lock

Password

- **None**: Disable the screen lock function.
- **Swipe**: Swipe upward on the screen to unlock the screen.
- **Patten**: Set up the pattern for the screen unlock.
- **PIN**: Set up the screen unlock PIN code.
- **Password**: Set up the password for the screen unlock.

Screen Lock Message and Notification



On lock screen
Show all notification content

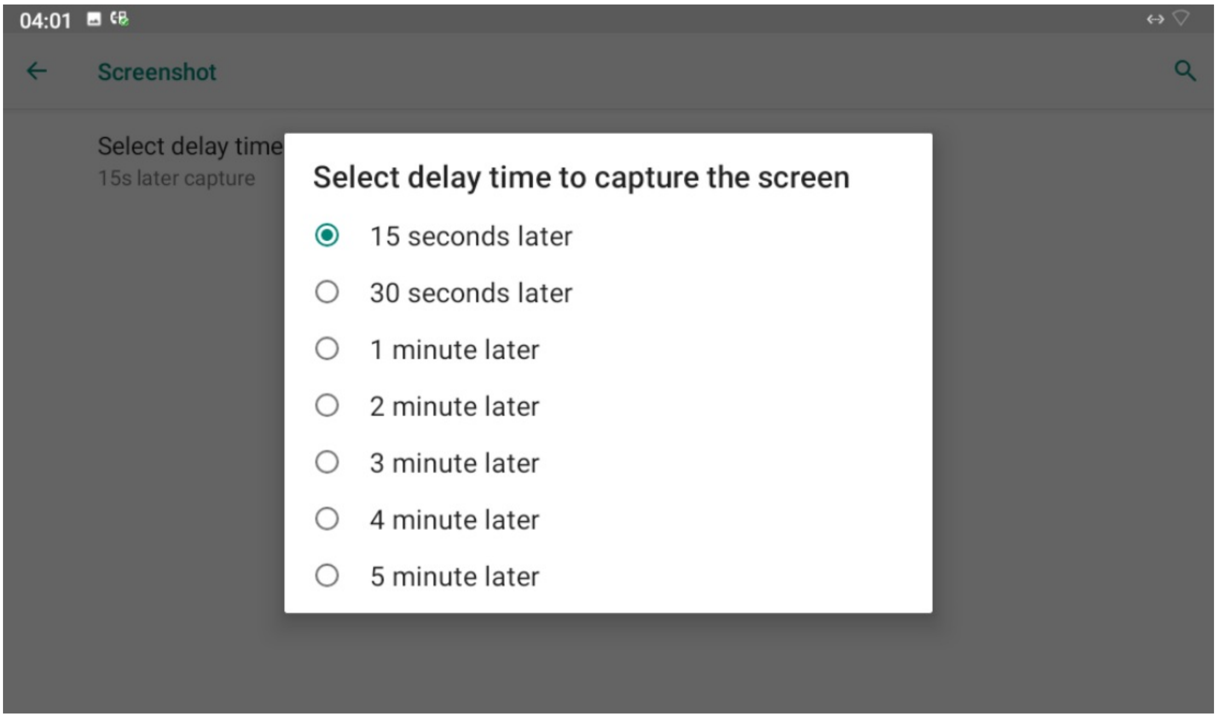
Lock screen message
None

- **On lock screen:**
  - **Show all notification content**: All notifications will be displayed on the lock screen.
  - **Don’t show notifications at all**: All notifications will NOT be displayed on the lock screen.
- **Lock screen message**: Customize the message shown on the lock screen.

Screenshot

You can set up a delay time for the device screen capturing, for example, if you set it as 30 seconds later, then the device will start capturing the current device screen automatically after 30 seconds for one time.

Tap ⊞ **> Settings > Screenshot** on the device screen.



04:01

Screenshot

Select delay time
15s later capture

Select delay time to capture the screen

● 15 seconds later

○ 30 seconds later

○ 1 minute later

○ 2 minute later

○ 3 minute later

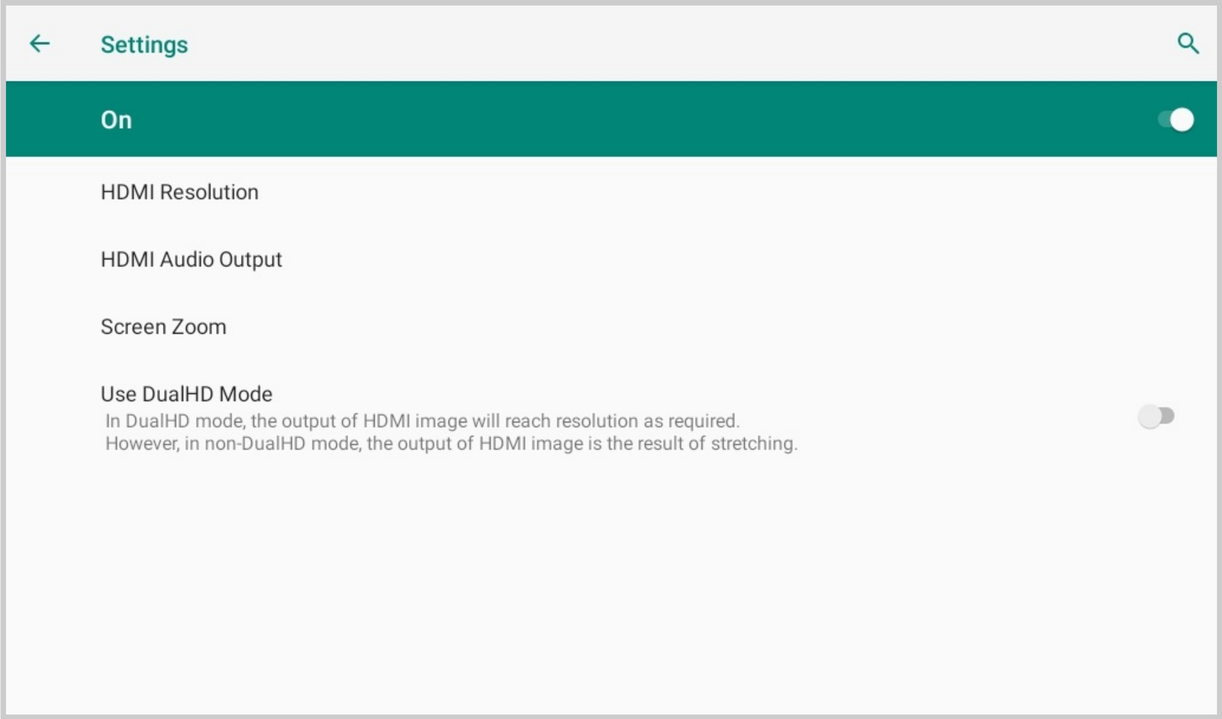
○ 4 minute later

○ 5 minute later

HDMI Settings

The device can project via the HDMI interface, and you can configure the relevant parameters.

Tap ⊞ **> Settings > Display > HDMI** on the device screen.



Settings

On

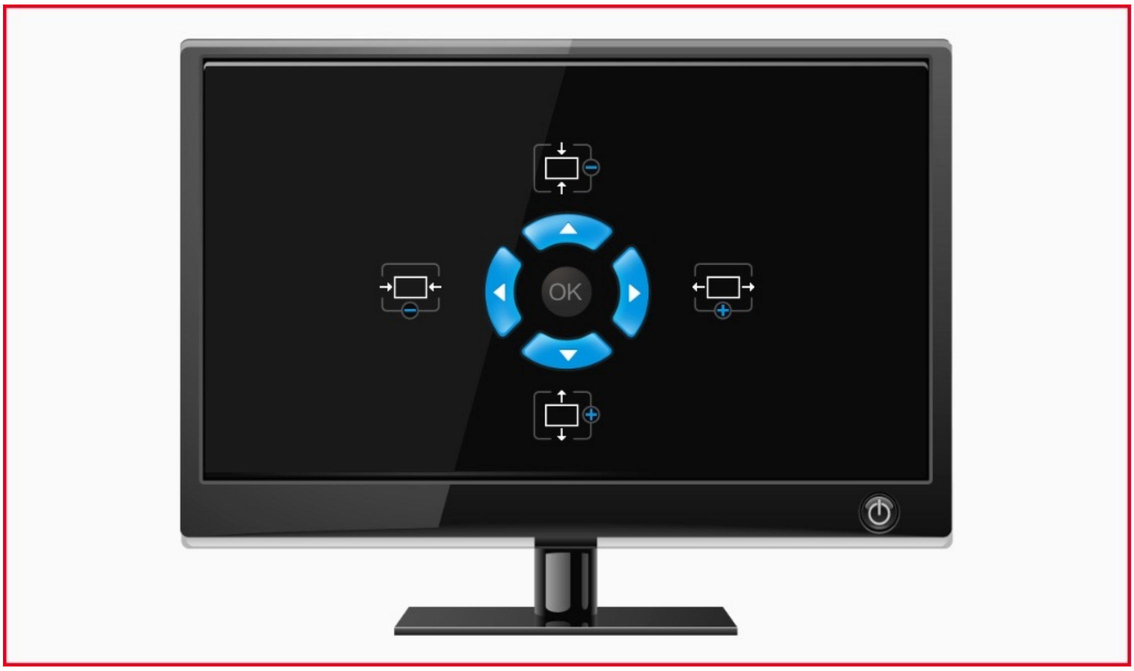
HDMI Resolution

HDMI Audio Output

Screen Zoom

Use DualHD Mode
In DualHD mode, the output of HDMI image will reach resolution as required.
However, in non-DualHD mode, the output of HDMI image is the result of stretching.

- **HDMI Resolution**: Choose the desired resolution from 1080P, 720P, 576P, and 480P.
- **HDMI Audio Output**: Choose the audio output in HDMI, the phone, or both.
- **Screen Zoom**: Tap to adjust the projection display.

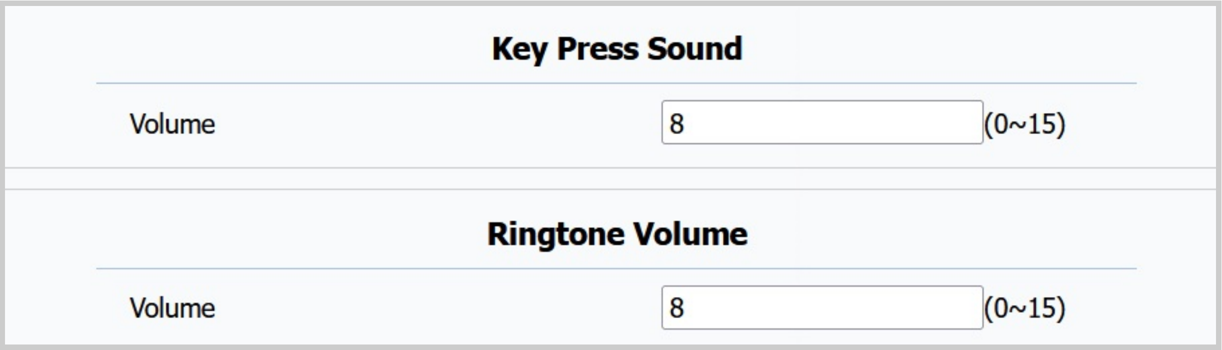


- **Use DualHD Mode**: This feature allows the HDMI output to display images at the required resolution. In contrast, Non-DualHD Mode stretches the image, which may lead to lower image quality.

Sound and Volume

The device provides various types of ringtones and volume configurations. You can configure them on the device directly or on the web interface.

Set it up on the web **Phone > Preference** interface.



Key Press Sound

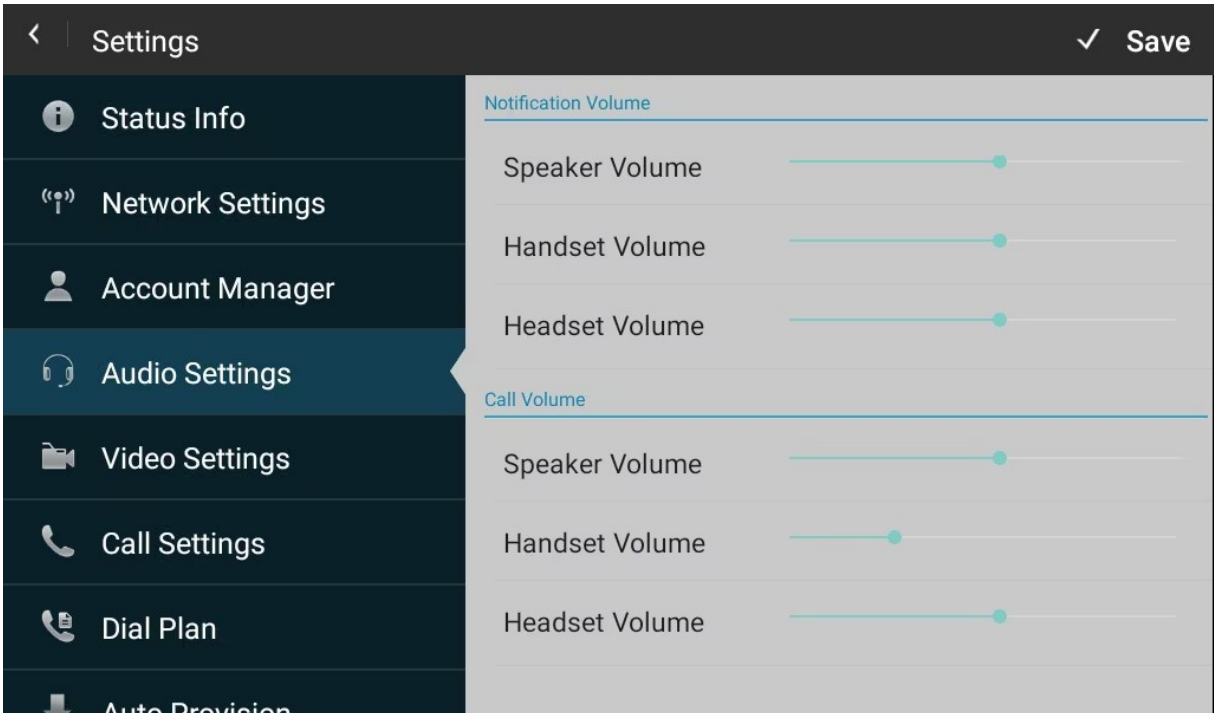
Volume 8 (0~15)

Ringtone Volume

Volume 8 (0~15)

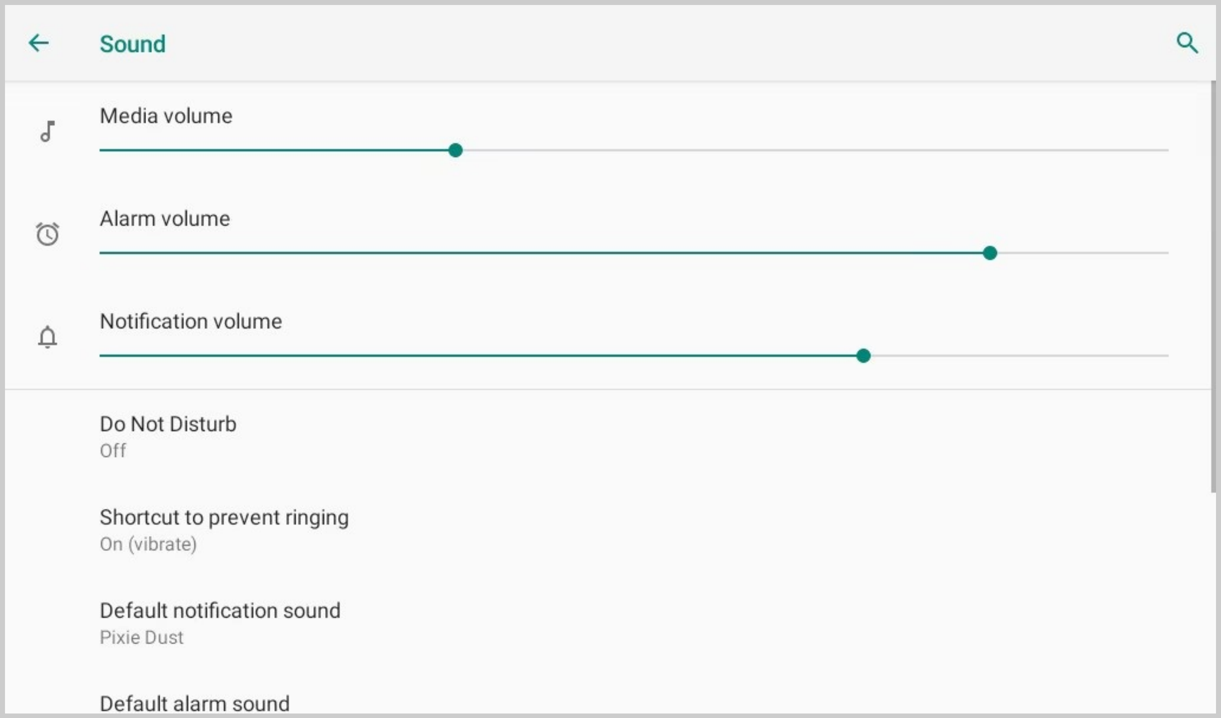
- **Keypad Press Sound**: The volume of pressing keys. The default is 8.
- **Ringtone Volume**: The ringtone for incoming calls. The default is 8.

Configure the tone and talk volumes on the ⚙ **> Audio Settings** screen.



- **Notification Volume**: The volume of the ringtone when there is an incoming call with the device in the speaker, handset, or headset mode.
- **Call Volume**: The volume during talking with the device in the speaker, handset, or headset mode.

Sound and volume can also be configured on the ⊞ **> Settings > Sound** screen.



Sound

Media volume

Alarm volume

Notification volume

Do Not Disturb
Off

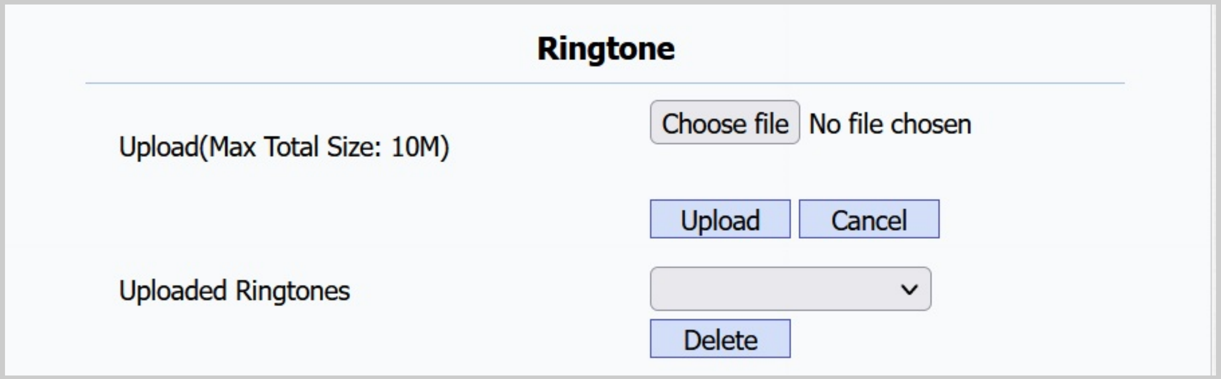
Shortcut to prevent ringing
On (vibrate)

Default notification sound
Pixie Dust

Default alarm sound

Upload Ringtones

You can upload ringtones on the web **Phone > Preference > Ringtone** interface.



Ringtone

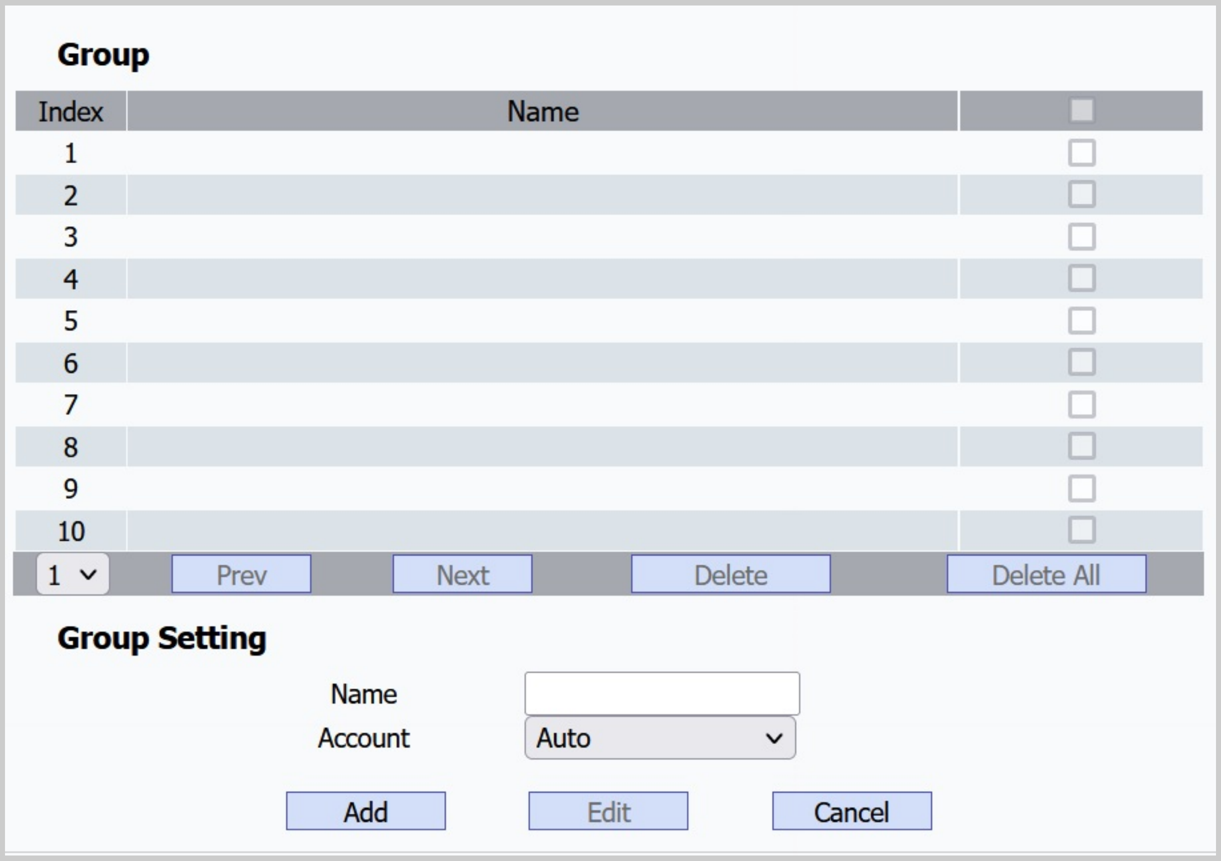
Upload(Max Total Size: 10M)	Choose file No file chosen Upload Cancel
Uploaded Ringtones	Delete

Contacts Configuration

Contact Group

You can create and edit a contact group for the contacts. The contact group will be used when you are adding a user.

To create and edit a contact group, navigate to the web **PhoneBook > Local Book > Group** interface.



Group

Index	Name	□
1		□
2		□
3		□
4		□
5		□
6		□
7		□
8		□
9		□
10		□

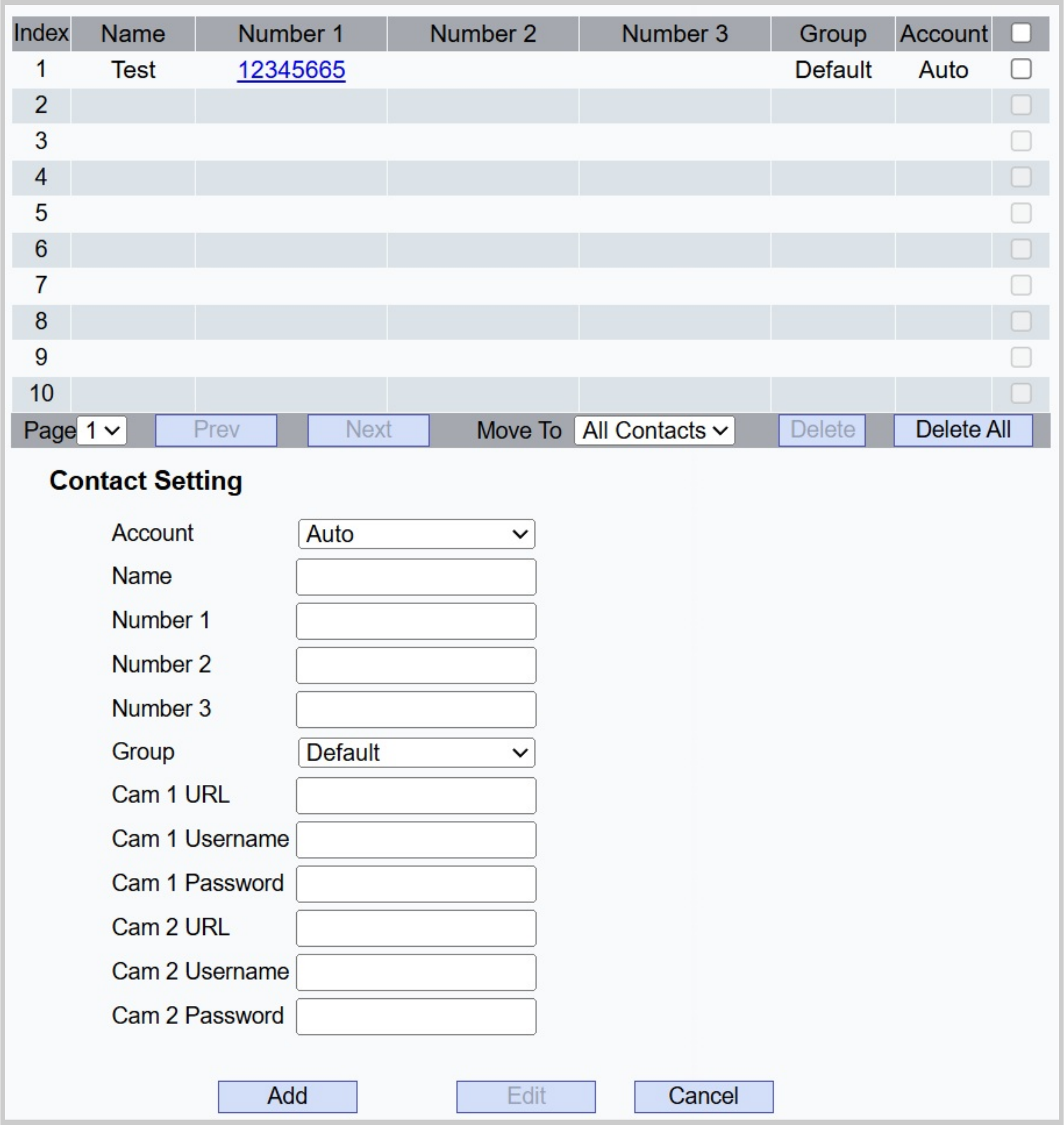
Group Setting

Name

Account: Auto

Add a Contact

Add a contact on the **PhoneBook > Local Book** > **Contact Setting** interface.



Index	Name	Number 1	Number 2	Number 3	Group	Account	□
1	Test	12345665			Default	Auto	□
2							□
3							□
4							□
5							□
6							□
7							□
8							□
9							□
10							□

Contact Setting

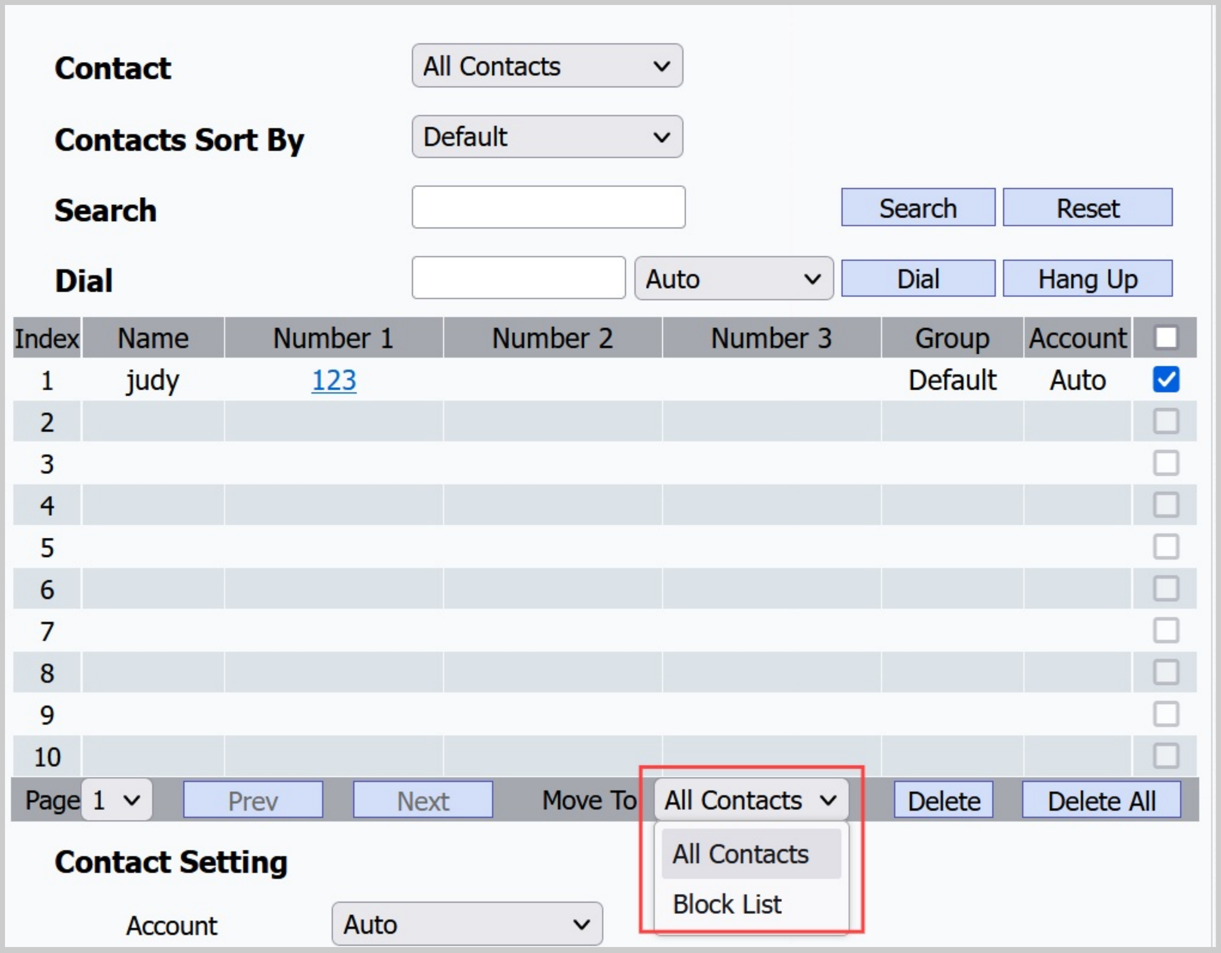
Account	Auto
Name	
Number 1	
Number 2	
Number 3	
Group	Default
Cam 1 URL	
Cam 1 Username	
Cam 1 Password	
Cam 2 URL	
Cam 2 Username	
Cam 2 Password	

- **Account**: Select the dial account from which to call the contact.
- **Name**: Customize the contact name.
- **Number 1/2/3**: Type in the IP or SIP number.
- **Group**: Assign the contact to a default or self-created group.
- **Cam URL:** Enter the RTSP URL for video preview. The format is *rtsp://Device IP address/live/ch00_0*.
- **Cam Username**: Enter the username for authentication.
- **Cam Password**: Enter the password for authentication.

Blocklist Contact

The calls from contacts in the blocklist will be rejected. You can blocklist a contact when editing it.

Set it up on the **PhoneBook > Local Book** interface.



Contact	All Contacts
Contacts Sort By	Default
Search	
Dial	Auto

Index	Name	Number 1	Number 2	Number 3	Group	Account	☐
1	judy	123			Default	Auto	☑
2							☐
3							☐
4							☐
5							☐
6							☐
7							☐
8							☐
9							☐
10							☐

Page 1 Move To All Contacts

Contact Setting

Account Auto

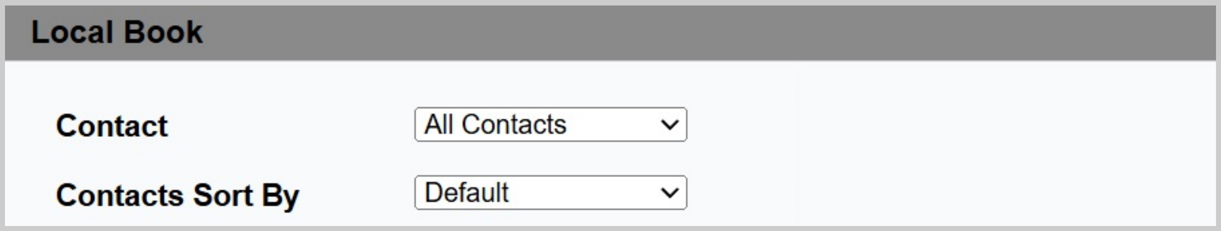
Note

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

Set it up on the web **PhoneBook > Local Book** interface.



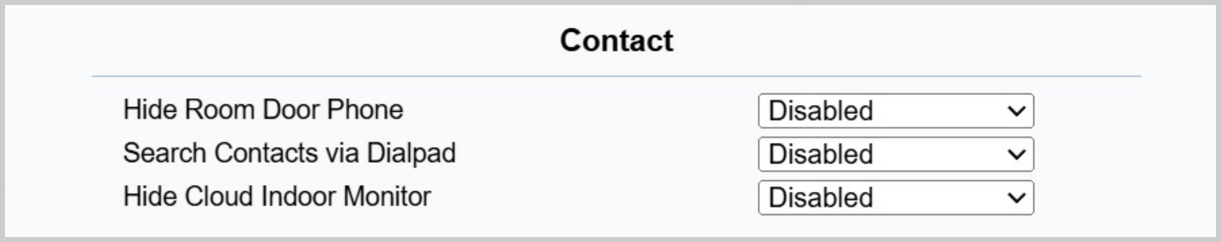
Local Book

Contact: All Contacts

Contacts Sort By: Default

- **Contact**: Display all contacts, contacts from the blocklist, or contacts from the self-created group.
- **Contacts Sort By**:
  - **Default**: The local contacts will be displayed before those from SmartPlus, SDMC, etc.
  - **ASCII Code**: The contacts will be displayed in order based on the first letter of the contact names.
  - **Created Time**: The contacts will be displayed by their created time.
  - **Room Number**: The contacts will be displayed based on the room numbers configured on the SmartPlus Cloud.

Besides, you can further set up contact display on the **Phone > Preference** interface.



Contact

Hide Room Door Phone: Disabled

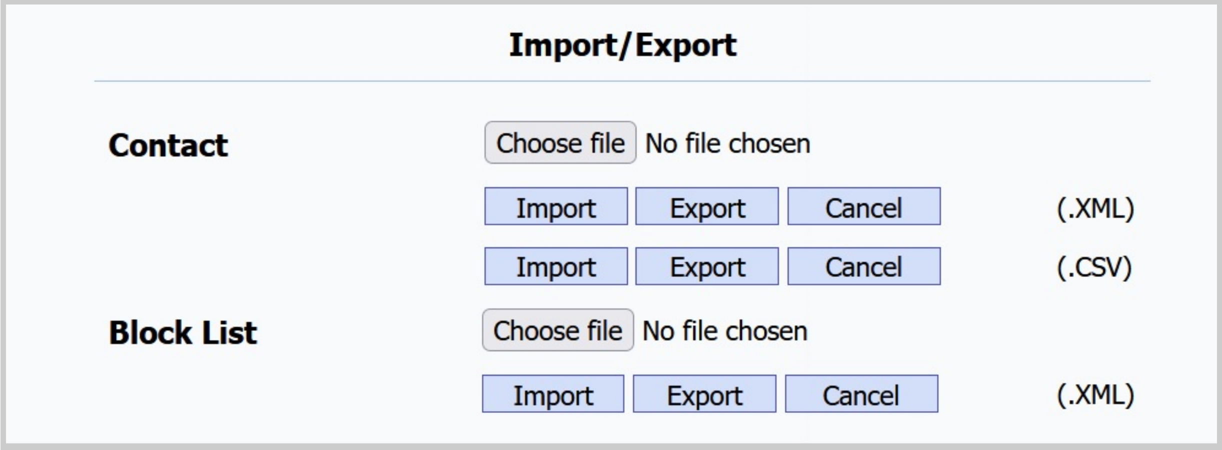
Search Contacts via Dialpad: Disabled

Hide Cloud Indoor Monitor: Disabled

- **Hide Room Door Phone**: Set whether to display the door phone in the same room issued from SDMC or SmartPlus Cloud. When enabled, users will not see the door phone's name in the contact list or monitoring list.
- **Search Contacts via Dialpad**: Set whether to display the search box for searching for the desired contact. When enabled, pressing any number will redirect to the contact searching screen.
- **Hide Cloud Indoor Monitor**: Set whether to display the indoor monitor in the same room issued from the SmartPlus Cloud.

Contacts Import and Export

When the contacts become so many that you can not afford to manage each contact one by one manually, you can import and export the contacts in batches on the device's web **PhoneBook > Local Book** interface.



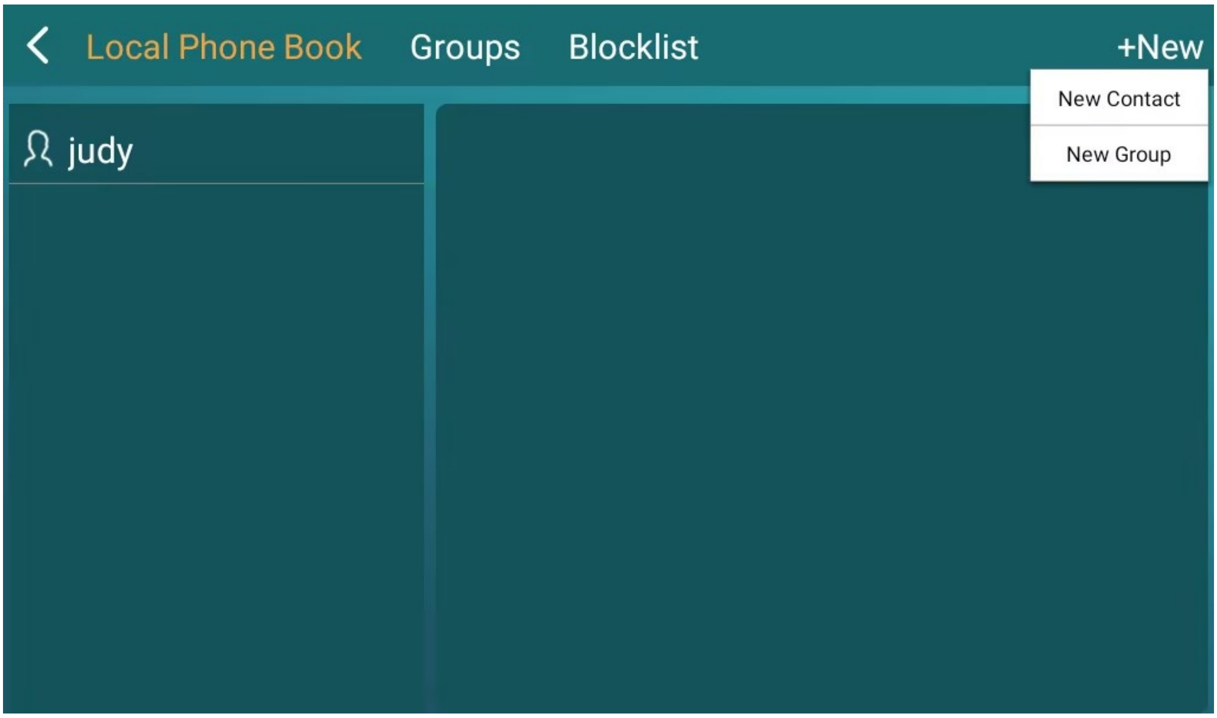
Import/Export

Contact	Choose file No file chosen	
	Import Export Cancel	(.XML)
	Import Export Cancel	(.CSV)
Block List	Choose file No file chosen	
	Import Export Cancel	(.XML)

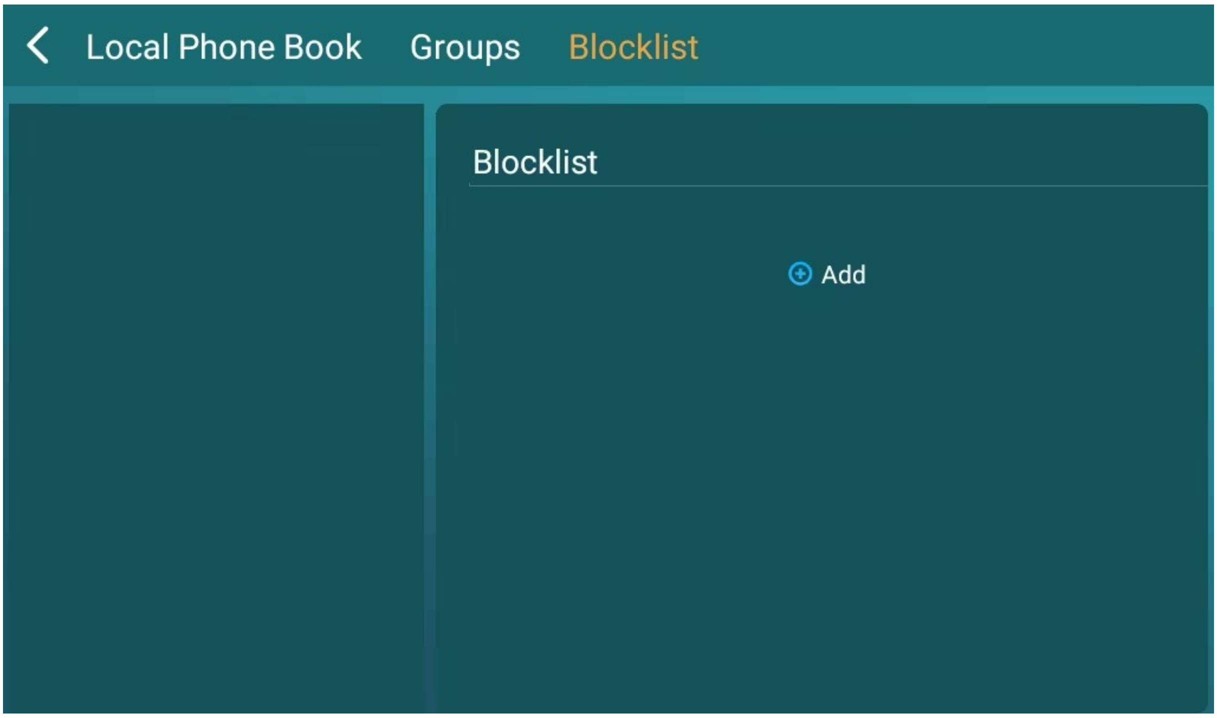
Contacts Configuration on the Device

You can create contacts and contact groups directly on the device.

Tap **More** in the upper left corner of the home screen and tap **+New** to create new contacts or new groups.



Tap **Blocklist** and **+Add** to blocklist a contact.



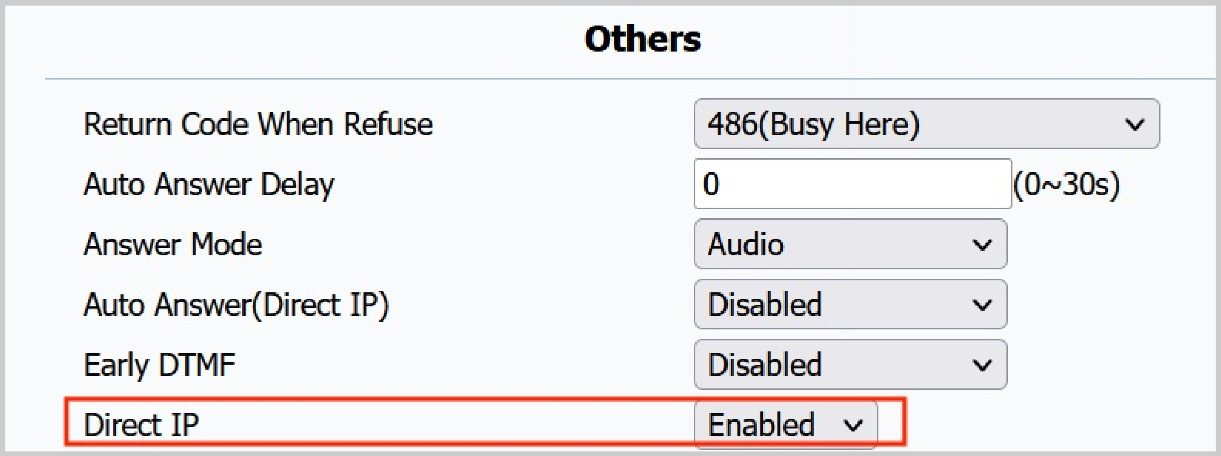
Local Phone Book
Groups
Blocklist
Blocklist
Add

Intercom Call Configuration

IP Call Configuration

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

To enable the direct IP call feature, navigate to the web **Phone > Call Feature > Others** interface.



Others

Return Code When Refuse	486(Busy Here)
Auto Answer Delay	0 (0~30s)
Answer Mode	Audio
Auto Answer(Direct IP)	Disabled
Early DTMF	Disabled
Direct IP	Enabled

SIP Call Configuration

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

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

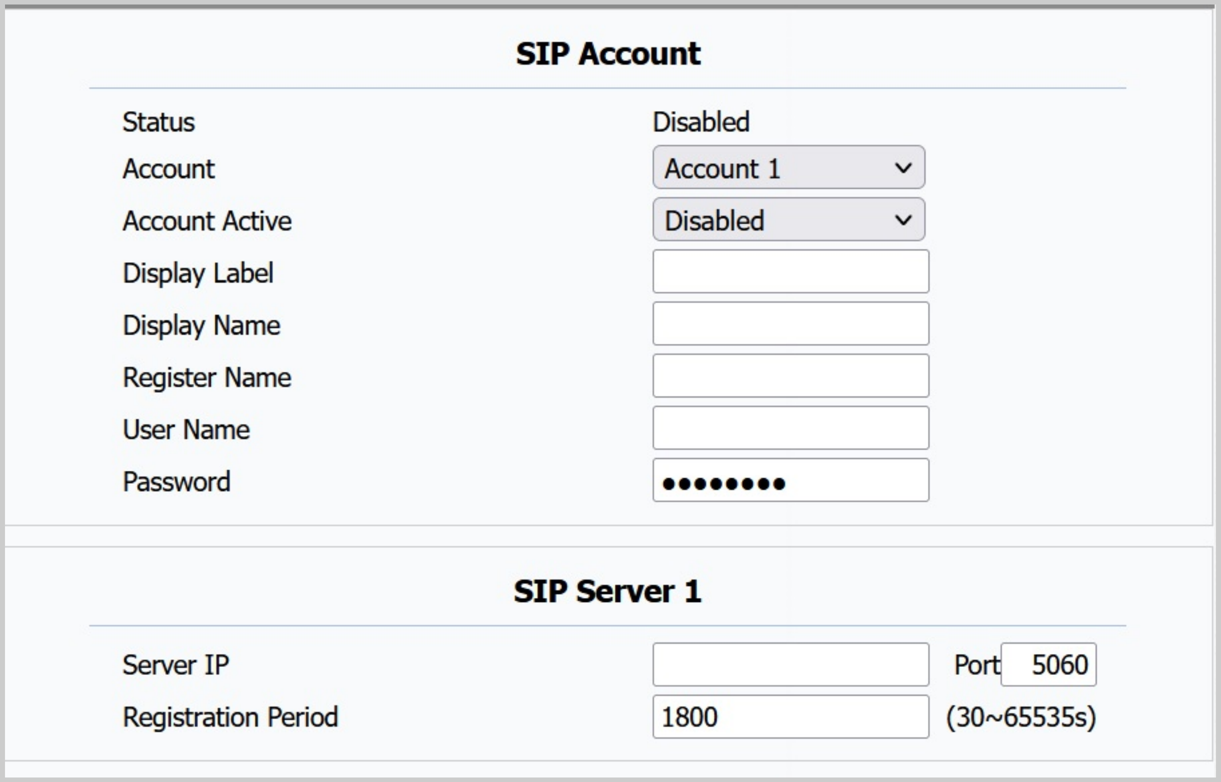
SIP Account Registration

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

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

Click here to view the SIP account registration example.

Navigate to the web **Account > Basic** interface.



SIP Account

Status	Disabled
Account	Account 1
Account Active	Disabled
Display Label	
Display Name	
Register Name	
User Name	
Password	••••••••

SIP Server 1

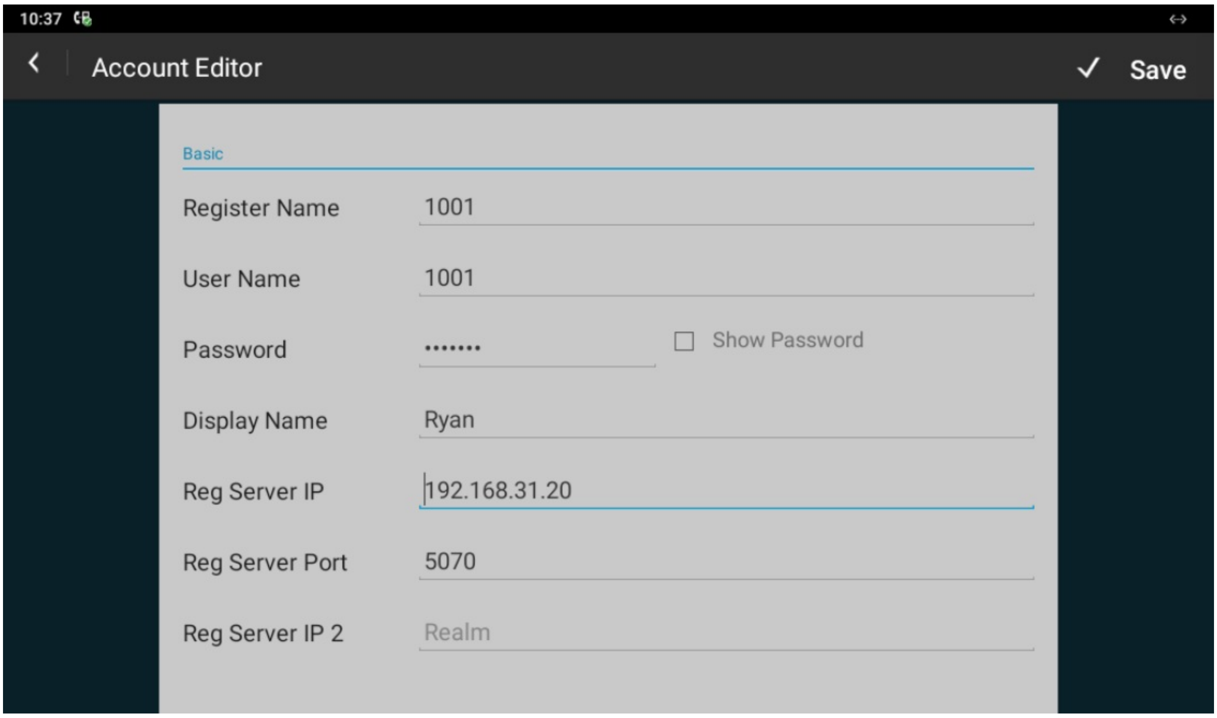
Server IP		Port 5060
Registration Period	1800	(30~65535s)

- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** The device supports 2 SIP accounts. Choose the account for configuration.
  - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus Cloud service is activated.
  - The system switches to Account 2 if Account 1 is not registered.
  - To designate the account to be used for outgoing calls, select the account number for contacts or dial plan prefixes in their settings.

- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same as the username from the PBX server.
- **User Name:** Same as the username from the PBX server for authentication.
- **Password:** Same as the password from the PBX server for authentication.

- **Server IP:** Specify the SIP account registration server port. The default is 5060. You can find the port information on the indoor monitor's PBX screen or from third-party server providers.
- **Registration Period**: Set up the SIP account registration period. SIP re-registration will start automatically if the account registration fails during the registration period. The default registration period is 1800, ranging from 30-65535s.

SIP accounts can also be set up on the device ⚙ **> Account Manager** screen. Tap Account 1 or Account 2 to configure it.



10:37

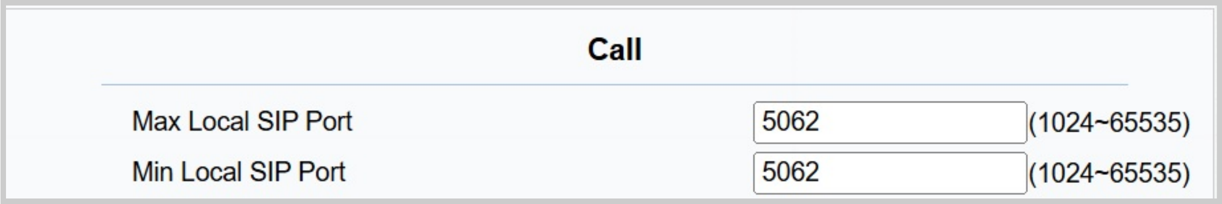
Account Editor ✓ Save

Basic

Register Name	1001
User Name	1001
Password	••••••• □ Show Password
Display Name	Ryan
Reg Server IP	192.168.31.20
Reg Server Port	5070
Reg Server IP 2	Realm

Configure SIP Ports for SIP Calls

You can set up a SIP port range for making SIP calls on the web **Account > Advanced > Call** interface.



Call

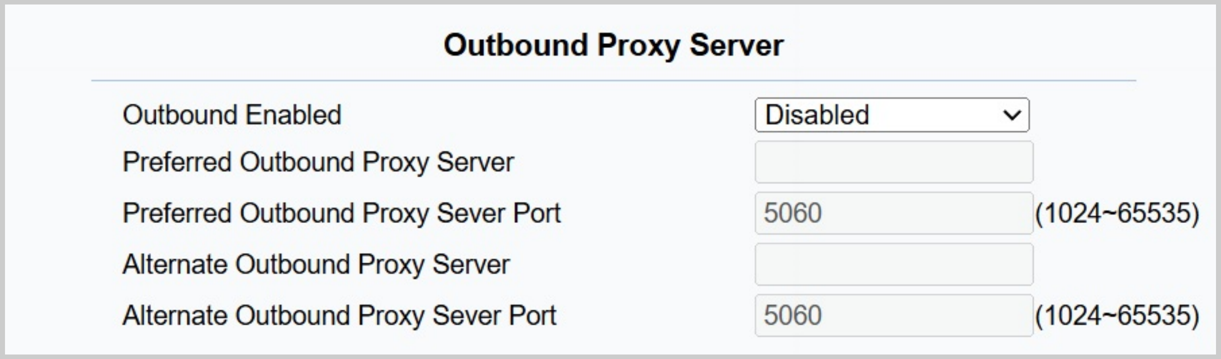
Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)

- **Max Local SIP Port**: The maximum SIP port ranges from 1024 to 65535. The default port value is 5062.
- **Min Local SIP Port**: The minimum SIP port ranges from 1024 to 65535. The default port value is 5062.

Outbound Proxy Server

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission.

Set it up on the web **Account > Basic > Outbound Proxy Server** interface.



Outbound Proxy Server

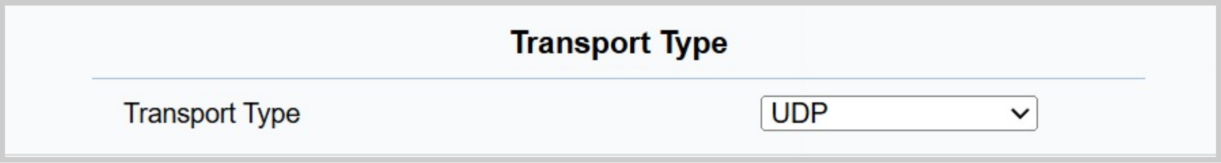
Outbound Enabled	Disabled	
Preferred Outbound Proxy Server		
Preferred Outbound Proxy Sever Port	5060	(1024~65535)
Alternate Outbound Proxy Server		
Alternate Outbound Proxy Sever Port	5060	(1024~65535)

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

Data Transmission Type

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

Set it up on the web **Account > Basic** interface.



Transport Type

Transport Type	UDP

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.

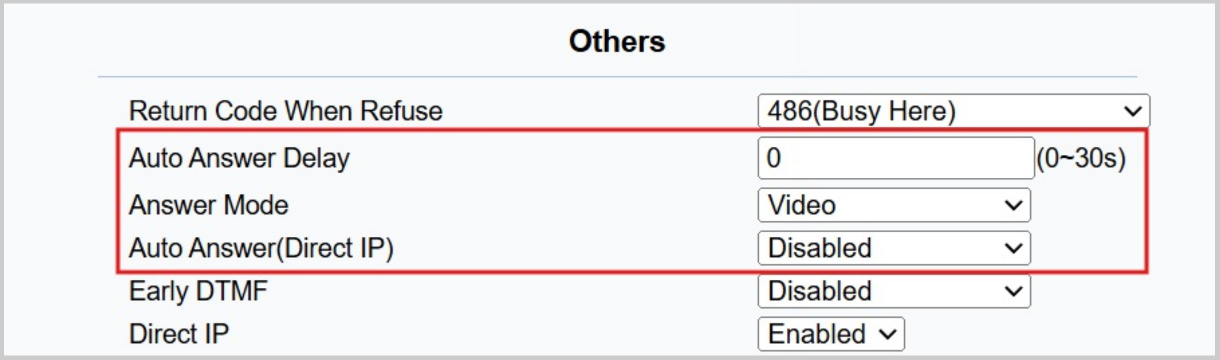
- **TLS:** An encrypted and secure transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.
- **DNS-SRV:** A DNS service record defines the location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

Call Settings

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.

Set it up on the web **Phone > Call Feature > Others** interface.

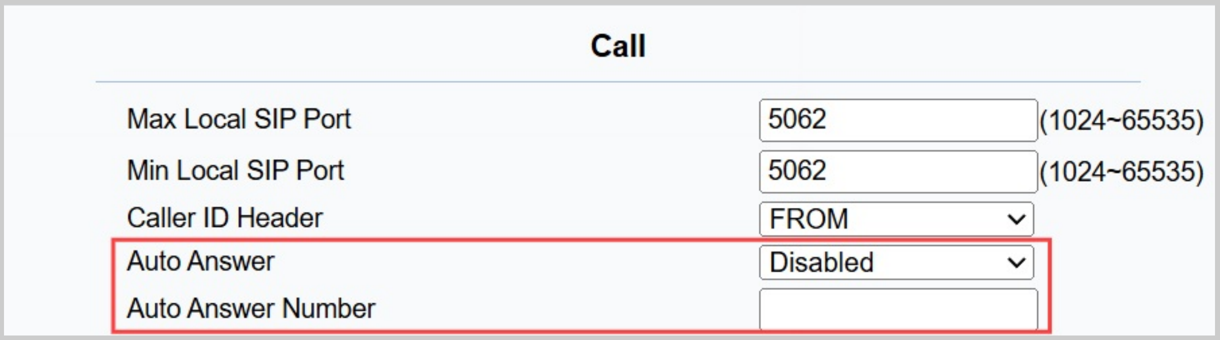


Others

Return Code When Refuse	486(Busy Here)
Auto Answer Delay	0 (0~30s)
Answer Mode	Video
Auto Answer(Direct IP)	Disabled
Early DTMF	Disabled
Direct IP	Enabled

- **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 to 1 second, then the call will be answered in 1 second automatically.
- **Answer Mode**: The video or audio mode for answering the call automatically.
- **Auto Answer(Direct IP)**: The setting applies to IP calls.

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



Call

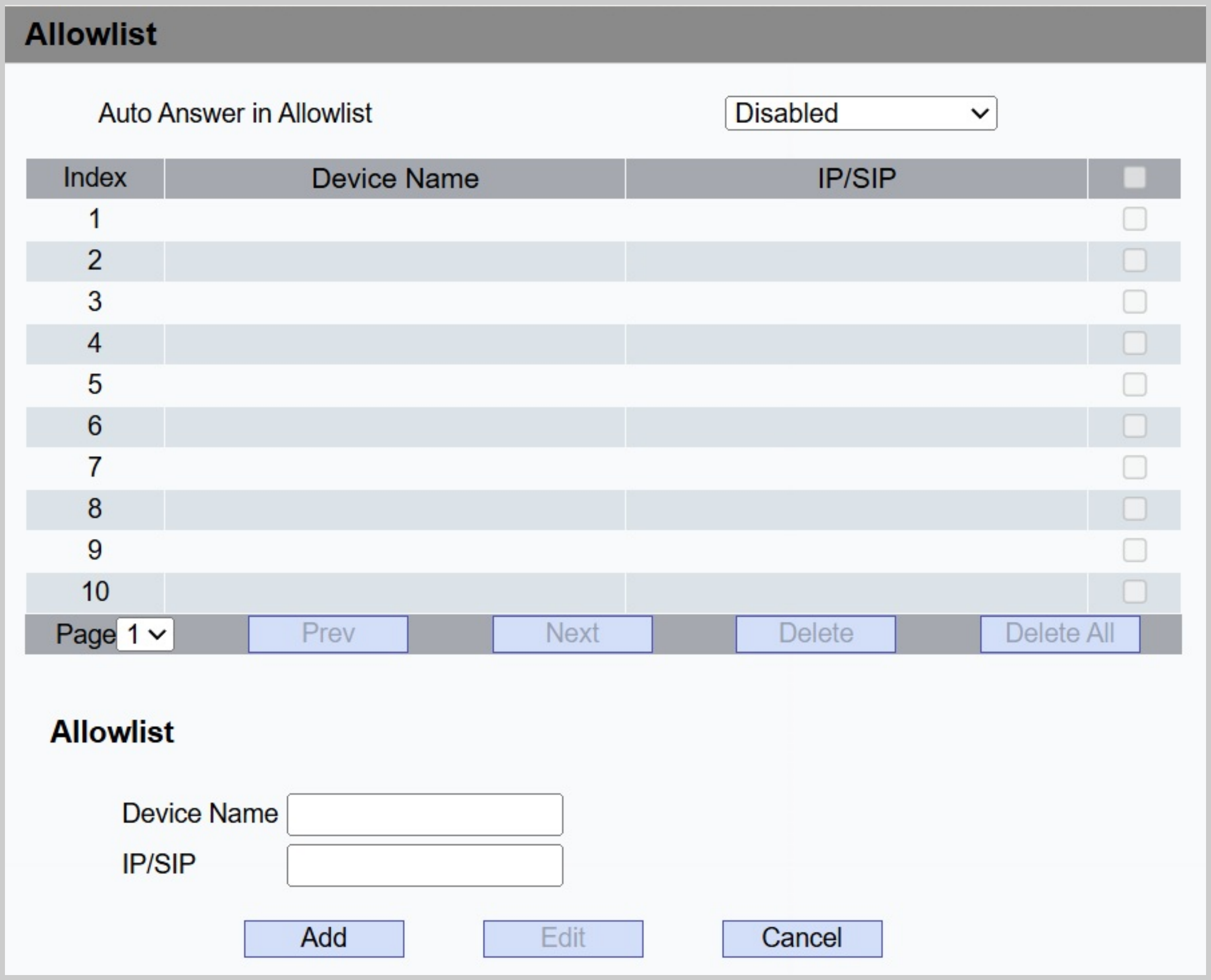
Max Local SIP Port	5062 (1024~65535)
Min Local SIP Port	5062 (1024~65535)
Caller ID Header	FROM
Auto Answer	Disabled
Auto Answer Number	

- **Auto Answer**: The setting applies to SIP calls.
- **Auto Answer Number**: Enter the SIP number of the caller whose call will be answered automatically.

Auto-answer Allowlist

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

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



Allowlist

Auto Answer in Allowlist: Disabled

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

Page 1

Allowlist

Device Name:

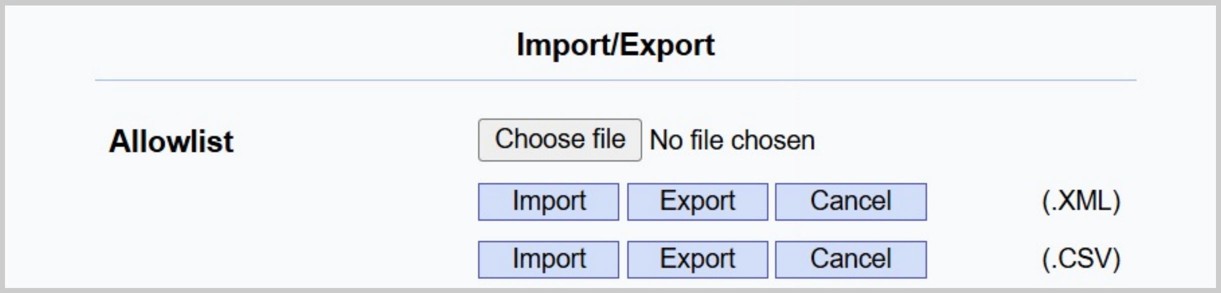
IP/SIP:

- **Auto Answer in Allowlist**: Turn on/off the feature.
- **Device Name**: Specify the allowed device’s name.
- **IP/SIP**: Enter the allowed device’s SIP or IP number.

Auto-answer Allowlist Import and Export

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

Set it up on the **Security > Allowlist** interface. The supported file formats are XML and CSV.



Import/Export

Allowlist: Choose file No file chosen

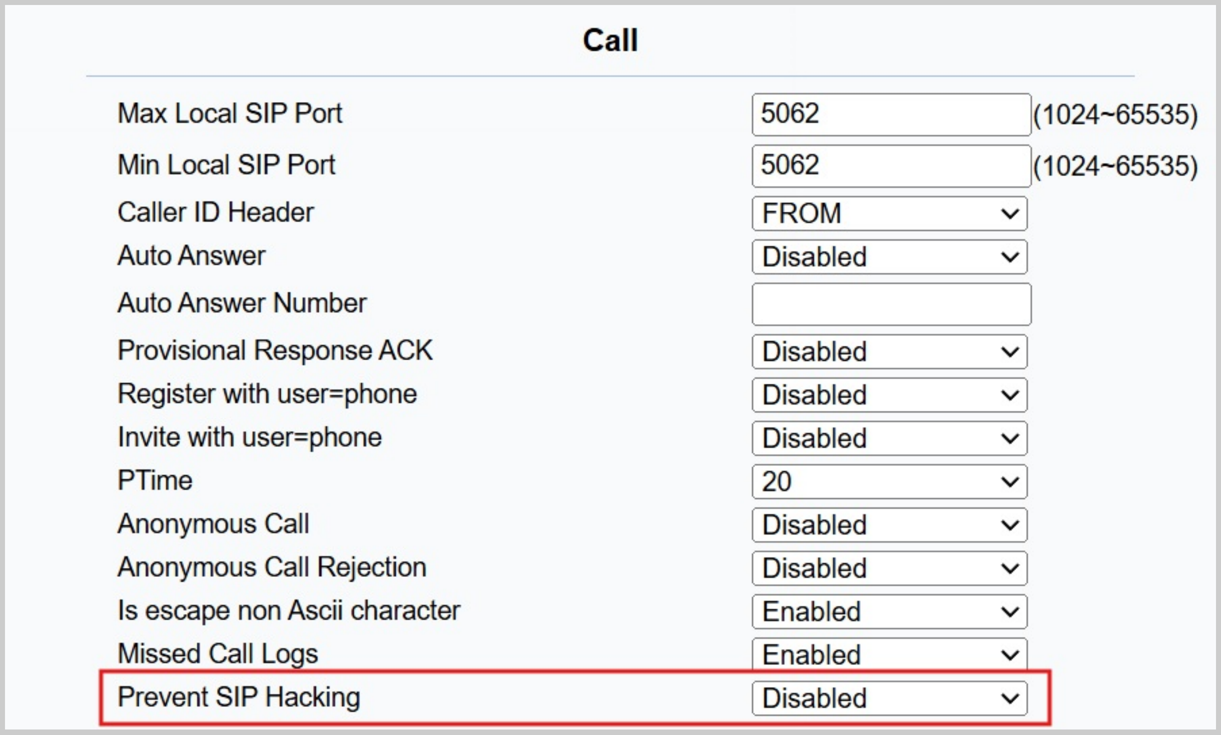
Import Export Cancel (.XML)

Import Export Cancel (.CSV)

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.

Enable the feature on the web **Account > Advanced > Call** interface.



Call

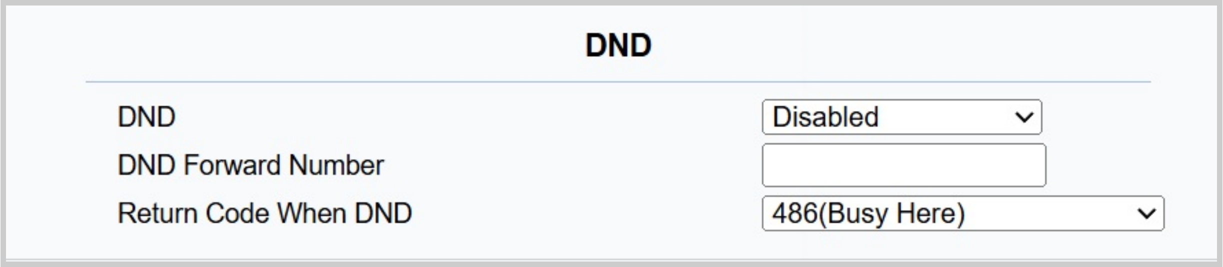
Max Local SIP Port	5062	(1024~65535)
Min Local SIP Port	5062	(1024~65535)
Caller ID Header	FROM	
Auto Answer	Disabled	
Auto Answer Number		
Provisional Response ACK	Disabled	
Register with user=phone	Disabled	
Invite with user=phone	Disabled	
PTime	20	
Anonymous Call	Disabled	
Anonymous Call Rejection	Disabled	
Is escape non Ascii character	Enabled	
Missed Call Logs	Enabled	
Prevent SIP Hacking	Disabled	

- **Prevent SIP Hacking**: Enable to activate this feature during SIP calls. This feature is only available for SIP calls.

DND

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.

Set it up on the web **Phone > Call Feature > DND** interface.



DND

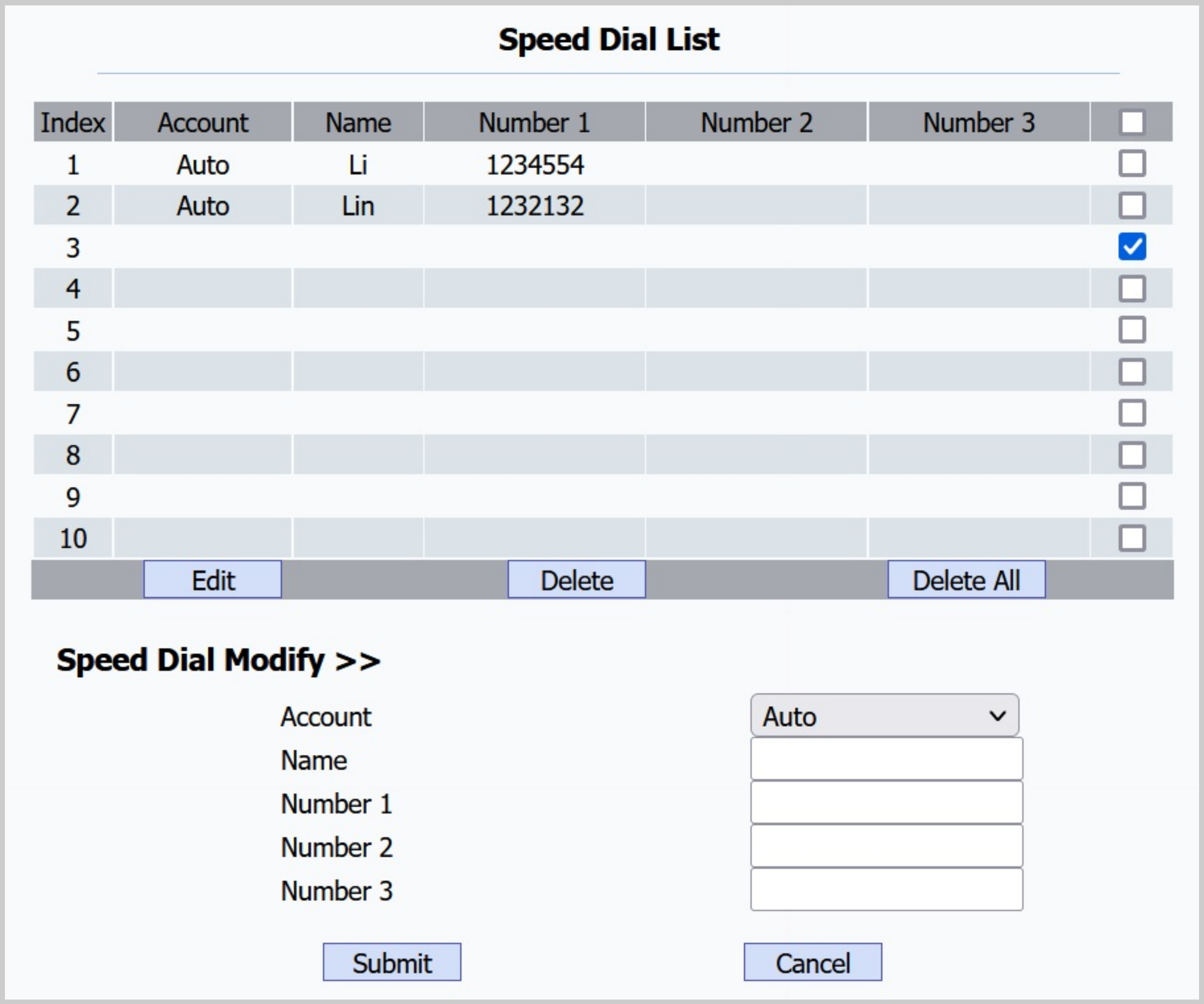
DND	Disabled
DND Forward Number	
Return Code When DND	486(Busy Here)

- **DND Forward Number**: When the device refuses the call, the call will be forwarded to the number.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

Speed Dial

Speed dial allows users to make speedy calls by pressing the contacts on the speed dial screen.

Set it up on the web **Phone > Speed Dial** interface.



Speed Dial List

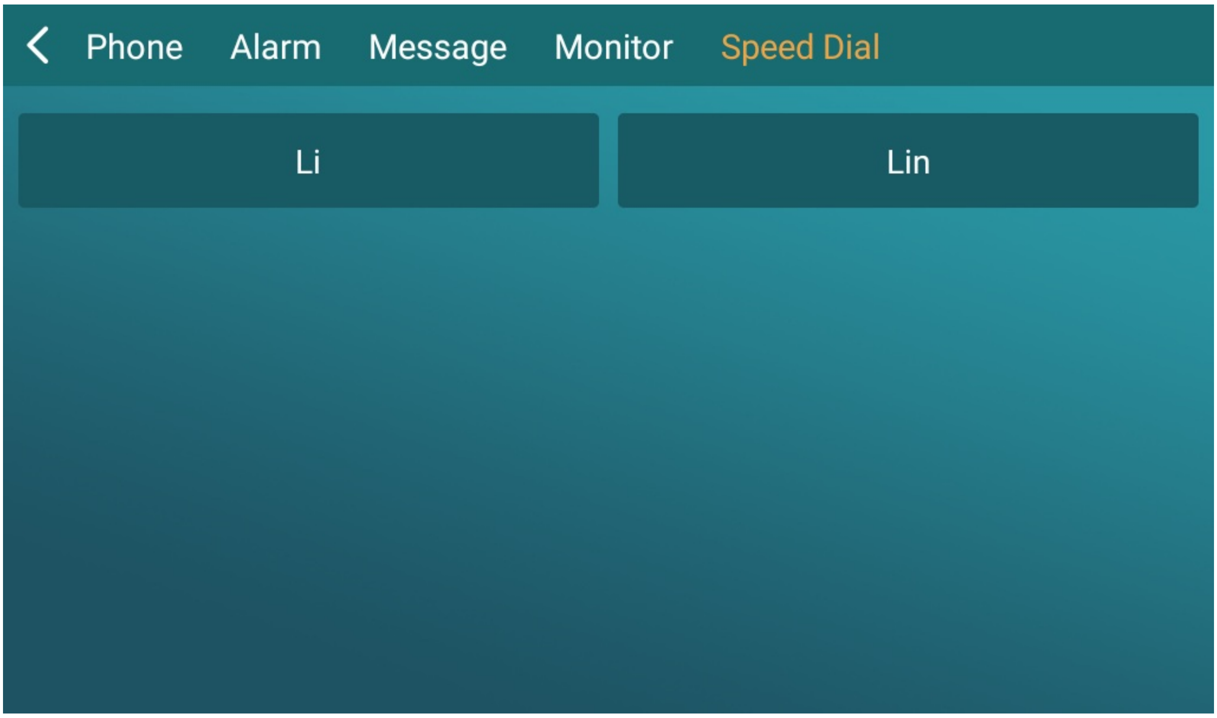
Index	Account	Name	Number 1	Number 2	Number 3	□
1	Auto	Li	1234554			□
2	Auto	Lin	1232132			□
3						☑
4						□
5						□
6						□
7						□
8						□
9						□
10						□

Speed Dial Modify >>

Account	Auto
Name	
Number 1	
Number 2	
Number 3	

- **Account**: The account to make the speed dial call.
- **Name**: The contact name.
- **Number 1/2/3**: The contact’s IP or SIP number. One contact can have three numbers at most. When users press the contact on the Speed Dial screen, three numbers will be called simultaneously.

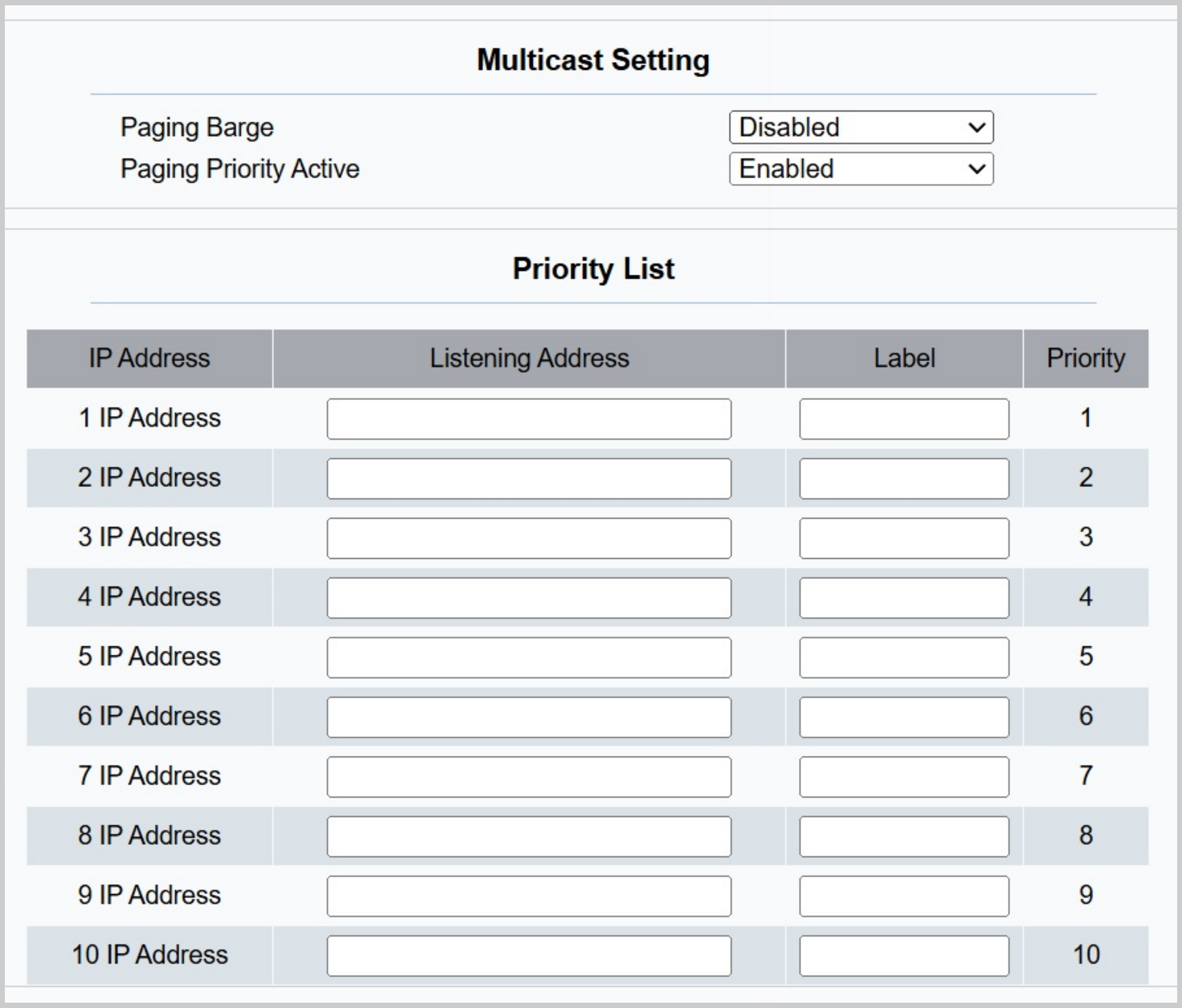
To call the speed dial number, tap a random option among Phone, Alarm, Message, and Monitor. Then, tap **Speed Dial**.



Multicast

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

Set it up on the web **Phone > Multicast** interface.



Multicast Setting

Paging Barge	Disabled
Paging Priority Active	Enabled

Priority List

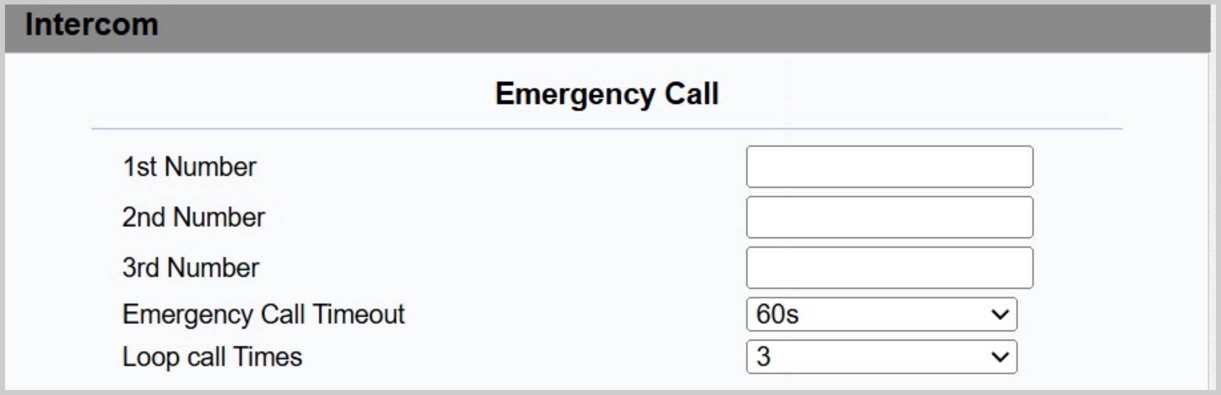
IP Address	Listening Address	Label	Priority
1 IP Address			1
2 IP Address			2
3 IP Address			3
4 IP Address			4
5 IP Address			5
6 IP Address			6
7 IP Address			7
8 IP Address			8
9 IP Address			9
10 IP Address			10

- **Paging Barge**: Multicast, or how many multicast calls have a higher priority than SIP call. If you disable it, the SIP call will have high priority.
- **Paging Priority Active**: Multicast calls are called in order of priority or not.
- **Listening Address:** Enter the multicast IP address. The multicast IP address needs to be the same as the listening part, and the multicast port cannot be the same for each IP address. Multicast IP addresses are from 224.0.0.0 to 239.255.255.255.
- **Label**: The name to be shown on the calling screen.

Emergency Call

SOS numbers need to be set up before users can make SOS calls. You can set up a maximum of three SOS numbers, which can be initiated automatically when pressing SOS on the home screen when an emergency occurs.

Set it up on the web **Phone > Intercom** interface.



Intercom

Emergency Call

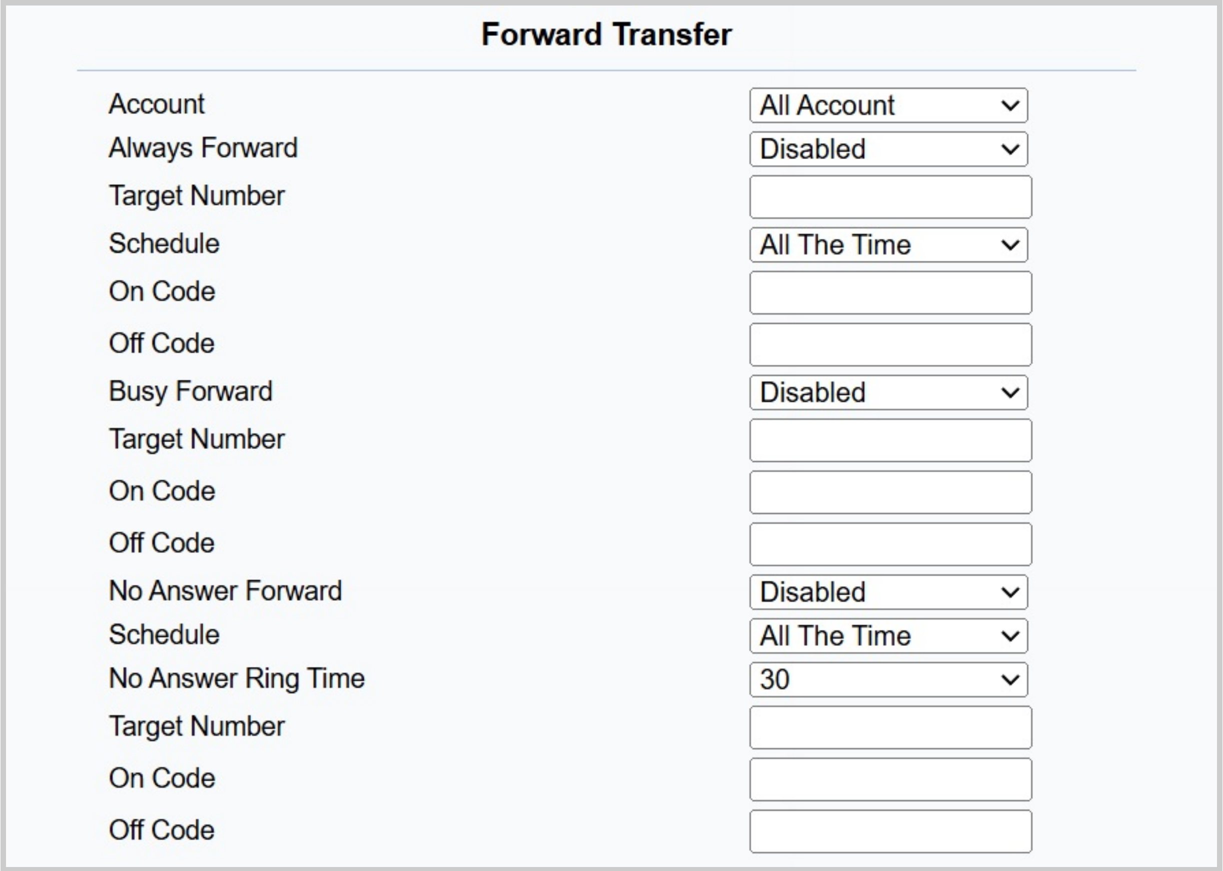
1st Number	
2nd Number	
3rd Number	
Emergency Call Timeout	60s
Loop call Times	3

- **Number:** Set up three SOS numbers, which will be called when pressing SOS on the device's home screen.
- **Emergency Call Timeout:** Set up the timeout for each number. Once users call out, if the other side does not answer within the timeout, the device will continue to call the next number.
- **Loop Call Times**: Set up the call loop times.

Call Forwarding

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

Set it up on the **Phone > Call Feature > Forward Transfer** interface.

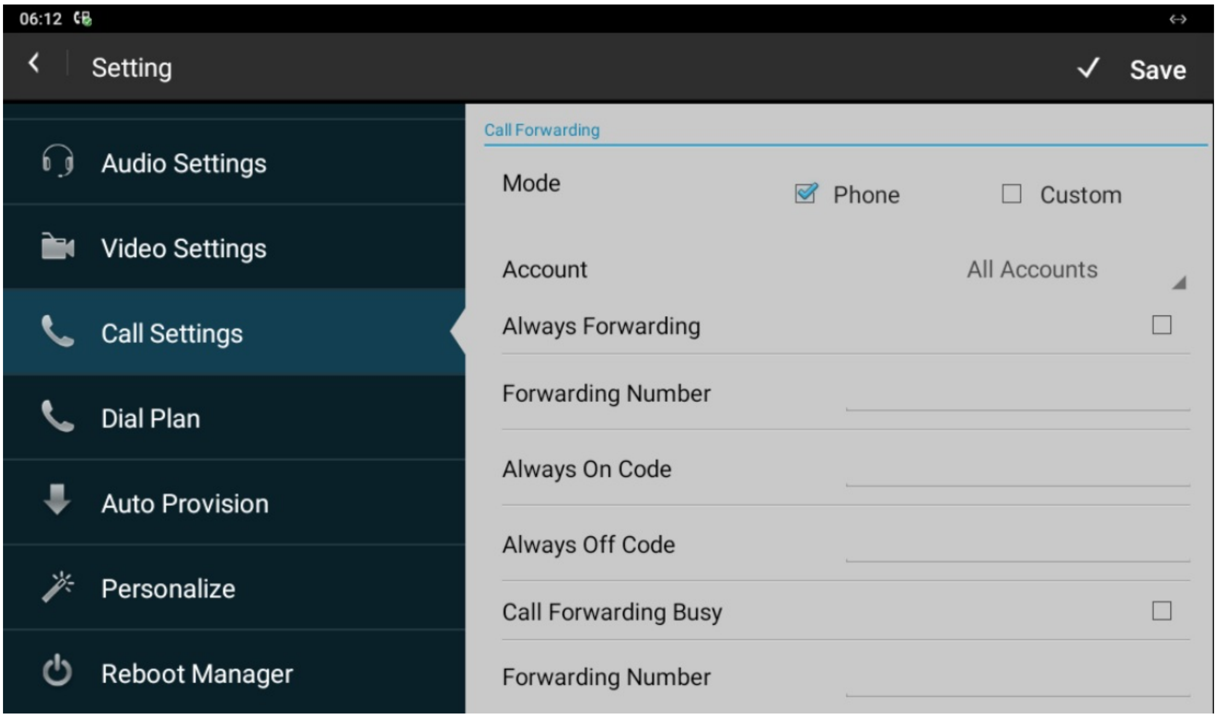


Forward Transfer

Account	All Account
Always Forward	Disabled
Target Number	
Schedule	All The Time
On Code	
Off Code	
Busy Forward	Disabled
Target Number	
On Code	
Off Code	
No Answer Forward	Disabled
Schedule	All The Time
No Answer Ring Time	30
Target Number	
On Code	
Off Code	

- **Account**: Choose the registered account to implement the call forwarding feature.
- **Always Forward**: All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: Incoming calls will be forwarded to a specific number if the phone is busy.
- **No Answer Forward**: Incoming calls will be forwarded to a specific number if the phone is not picked up within the no-answer ring time.
- **Target Number**: Enter the specific forward number when the R49 guard phone enables always forward / busy forward / no answer forward.
- **On/Off Code**: The code sent to the SIP server to turn on/off the call forwarding feature.

Call forwarding can also be set up on the device ⚙ **> Call Settings** screen.



Call Forwarding

Mode ☑ Phone □ Custom

Account All Accounts

Always Forwarding □

Forwarding Number

Always On Code

Always Off Code

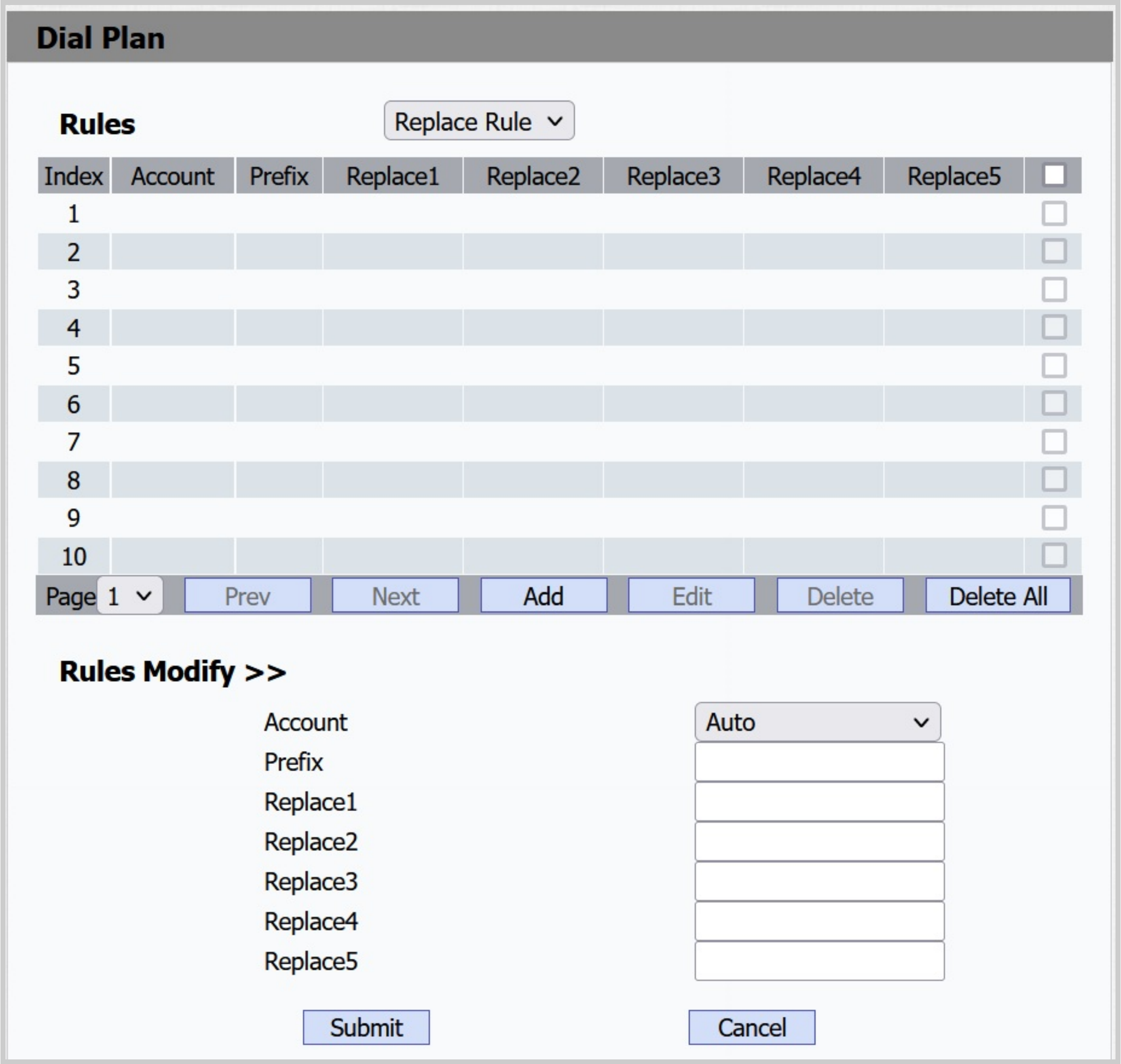
Call Forwarding Busy □

Forwarding Number

Quick Dial By Number Replacement

The dial number replacement feature simplifies long and complex dial numbers of the device, providing shorter and more user-friendly alternatives for making calls. It allows the substitution of multiple dial numbers, such as IP addresses or SIP numbers, with a single, simplified number.

Set it up on the **Phone > Dial Plan** interface. Click **Add**.



Dial Plan

Rules: Replace Rule

Index	Account	Prefix	Replace1	Replace2	Replace3	Replace4	Replace5	□
1								□
2								□
3								□
4								□
5								□
6								□
7								□
8								□
9								□
10								□

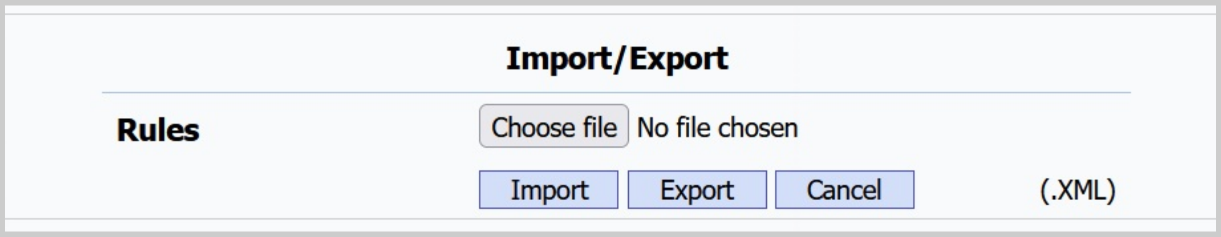
Page 1

Rules Modify >>

Account	Auto
Prefix	
Replace1	
Replace2	
Replace3	
Replace4	
Replace5	

- **Account**: Choose the account for dial number replacement. By default, it is set to Auto, which means calls will go out from the registered account. You can select either Account 1 or Account 2 to make the call. If both accounts are registered, it will use Account 1 by default.
- **Prefix**: The short number that replaces the dial number.
- **Replace**: Enter the dial number(s) to be replaced. For example, if you replace five original dial numbers with a common short number, such as 101, then the five intercom devices with the dial number will be called at the same time when users dial 101.

You can import or export the quick dial numbers on the same interface. The file supported is XML.



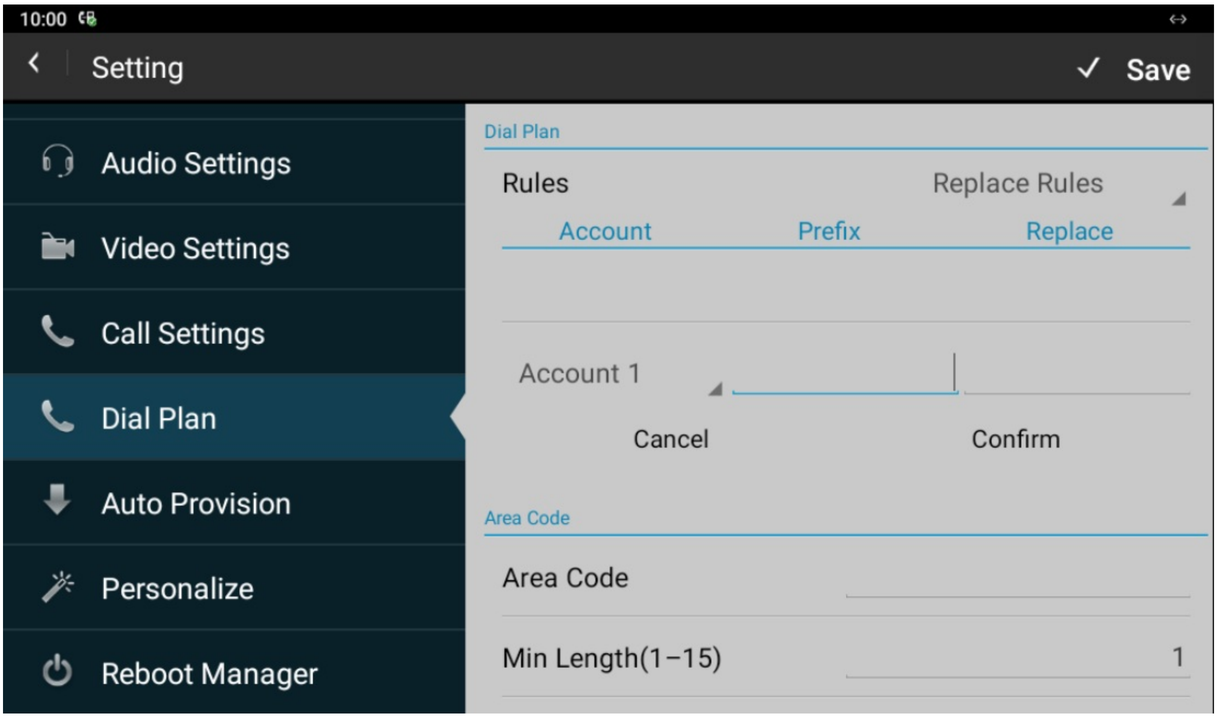
Import/Export

Rules

Choose file No file chosen

Import Export Cancel (.XML)

Quick dial can also be set up on the device ⚙ **> Dial Plan** screen.



10:00

Setting ✓ Save

Audio Settings
Video Settings
Call Settings
Dial Plan
Auto Provision
Personalize
Reboot Manager

Dial Plan

Rules: Replace Rules

Account	Prefix	Replace

Account 1

Cancel Confirm

Area Code

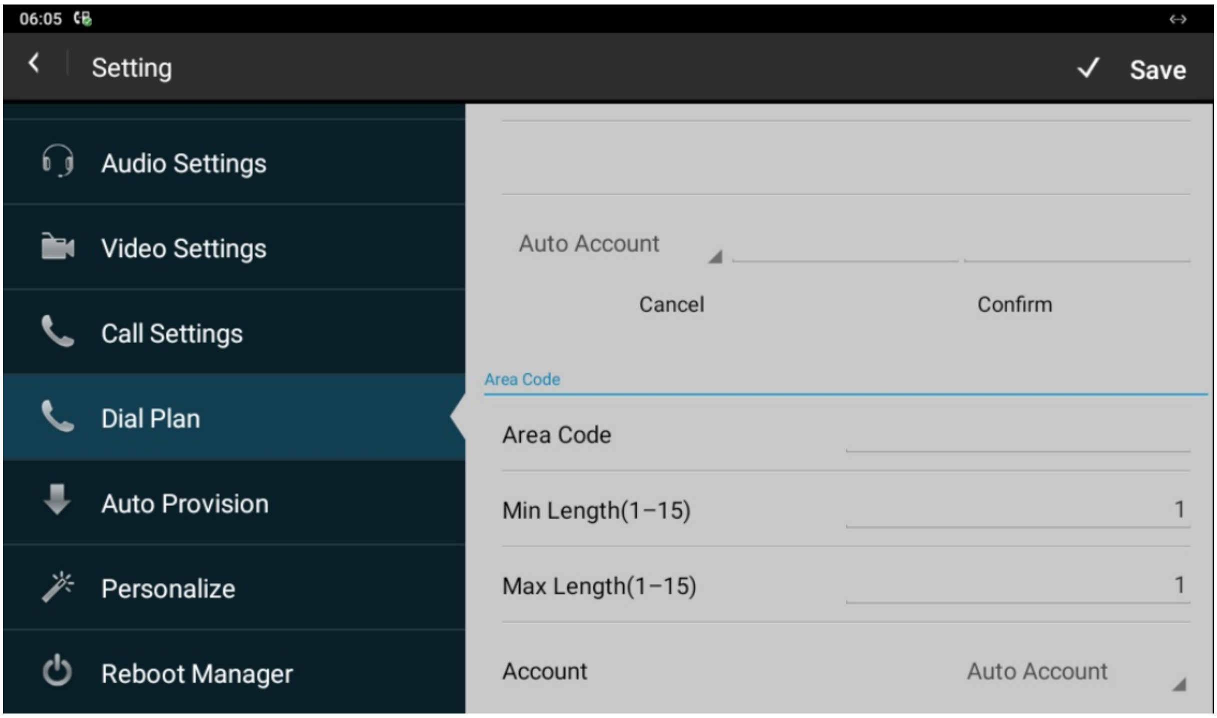
Area Code:

Min Length(1–15): 1

Area Code

Area codes are also known as NPAs (Numbering Plan Areas). They usually indicate different geographical areas within one country. If the entered numbers match the predefined area code rule, the phone will automatically prefix the outgoing number with the area code.

Set it up on the device ⚙ **> Dial Plan > Area Code** screen.



Auto Account

Area Code

Area Code

Min Length(1–15) 1

Max Length(1–15) 1

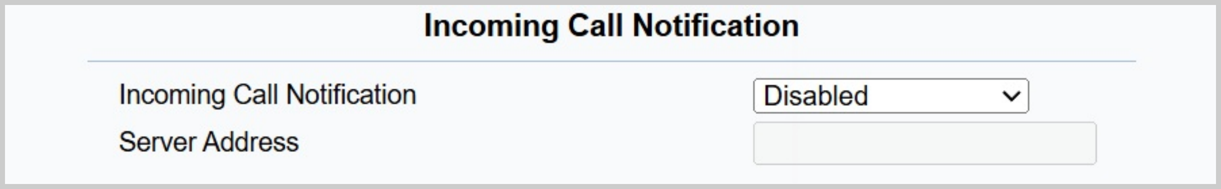
Account Auto Account

- **Min Length (1-15)**: Set the minimum length of the SIP number.
- **Max Length(1-15)**: Set the maximum length of the SIP number
- **Account**: Select the account for which you want to apply the area code function.

Incoming Call Notification

The device can send the calling contact's information to a third-party server in the HTTP URL format.

Set it up on the **Phone > Call Feature** interface.



Incoming Call Notification

Incoming Call Notification: Disabled

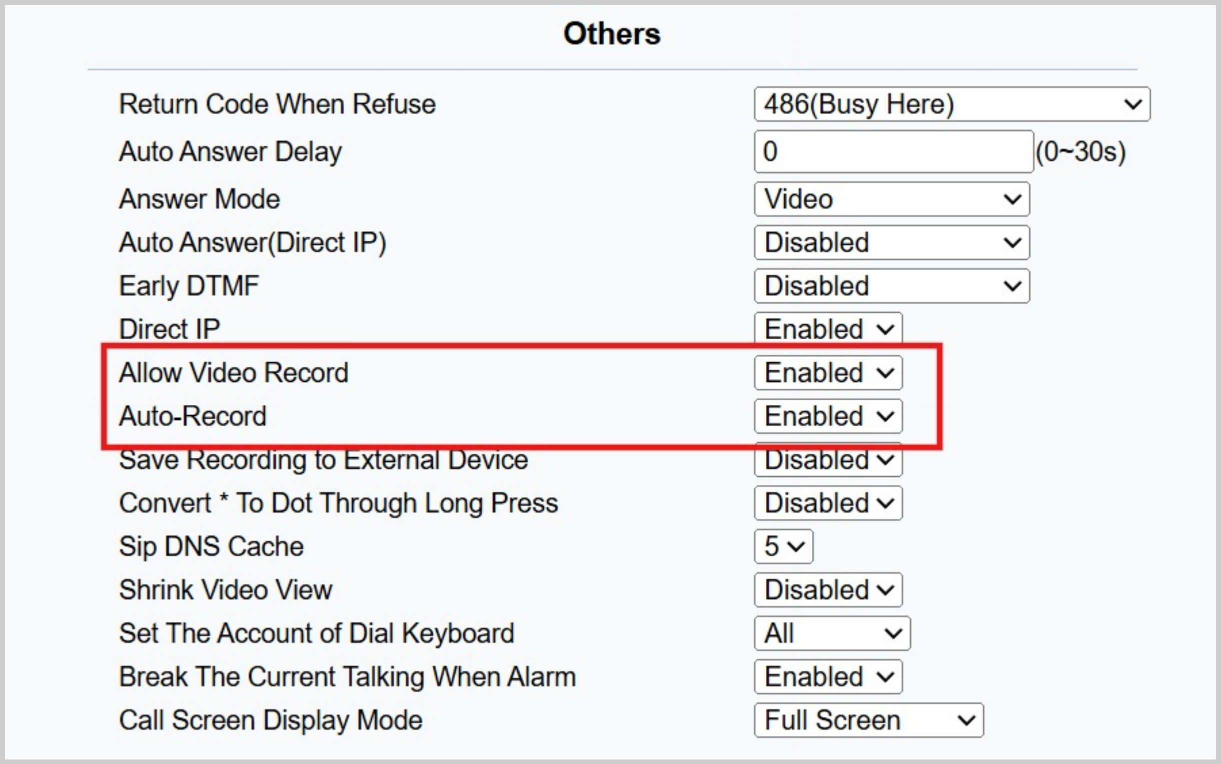
Server Address:

- **Incoming Call Notification**: Turn on/off the feature. It is disabled by default.
- **Server Address**: The address of the third-party server.

Auto-record when Making Calls

The device can automatically record videos and audio when it calls other devices.

To set this up, go to the **Phone > Call Feature > Others** interface.

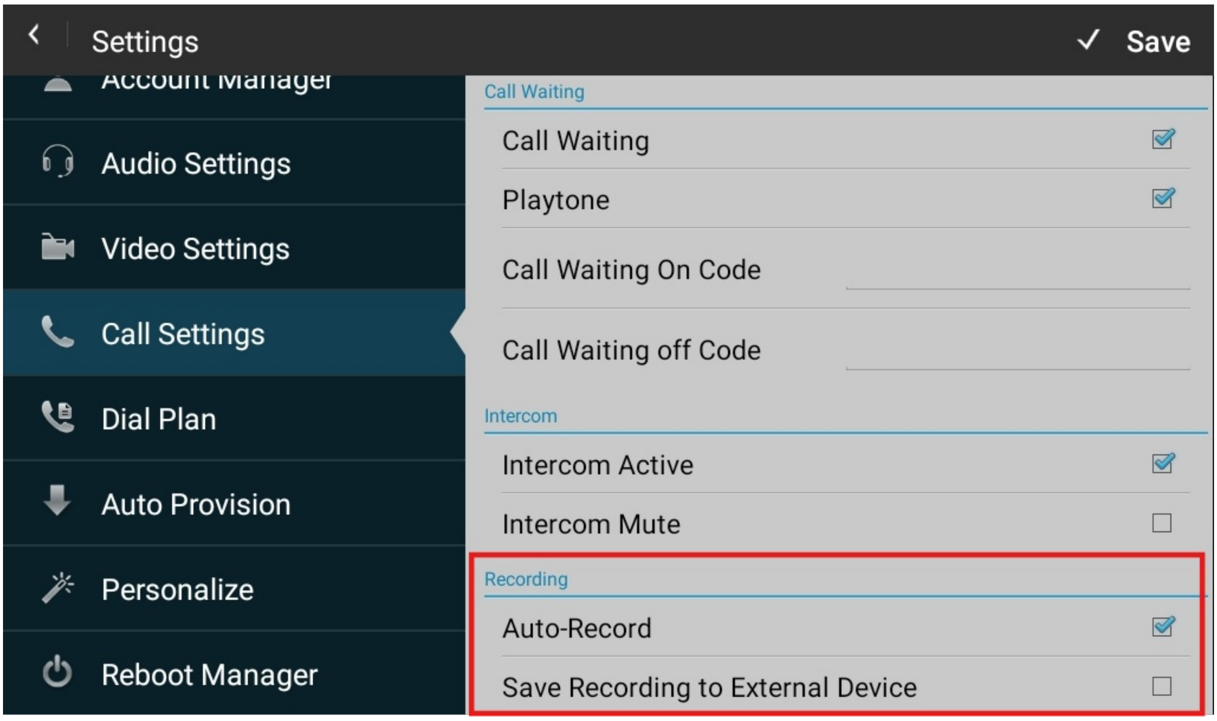


Others

Return Code When Refuse	486(Busy Here)
Auto Answer Delay	0 (0~30s)
Answer Mode	Video
Auto Answer(Direct IP)	Disabled
Early DTMF	Disabled
Direct IP	Enabled
Allow Video Record	Enabled
Auto-Record	Enabled
Save Recording to External Device	Disabled
Convert * To Dot Through Long Press	Disabled
Sip DNS Cache	5
Shrink Video View	Disabled
Set The Account of Dial Keyboard	All
Break The Current Talking When Alarm	Enabled
Call Screen Display Mode	Full Screen

- **Allow Video Record**: It is disabled by default. When enabled, the device will automatically start recording a video when it calls other devices. During the call, users can tap ⏺ to stop the recording.
- **Auto-Record**: It is disabled by default. When enabled, the device will automatically start recording audio when it calls other devices.

You can also set this feature by tapping ⚙ **> Call Settings**. Scroll to the bottom.



Call Waiting

- Call Waiting ☑
- Playtone ☑
- Call Waiting On Code
- Call Waiting off Code

Intercom

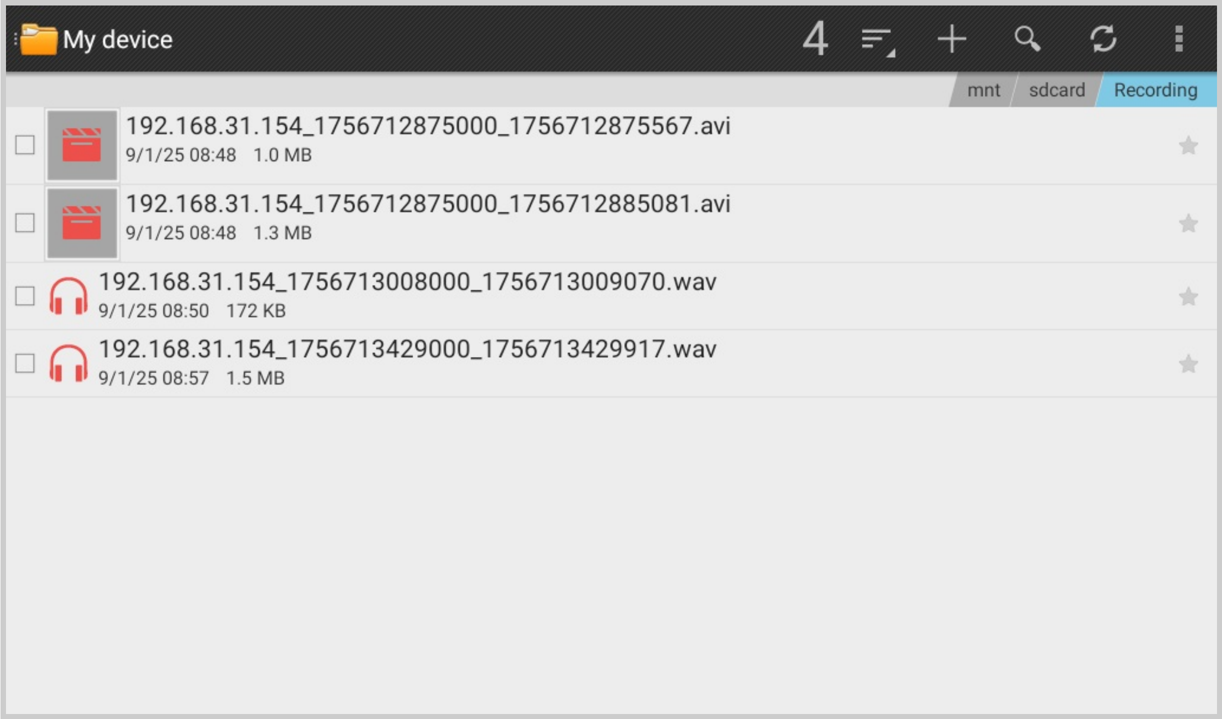
- Intercom Active ☑
- Intercom Mute ☐

Recording

- Auto-Record ☑
- Save Recording to External Device ☐

- **Save Recording to External Device**: When checked, recorded files will be saved to the external device instead of the internal folder.

You can check the recorded files by tapping ⊞ **> Recordings**.

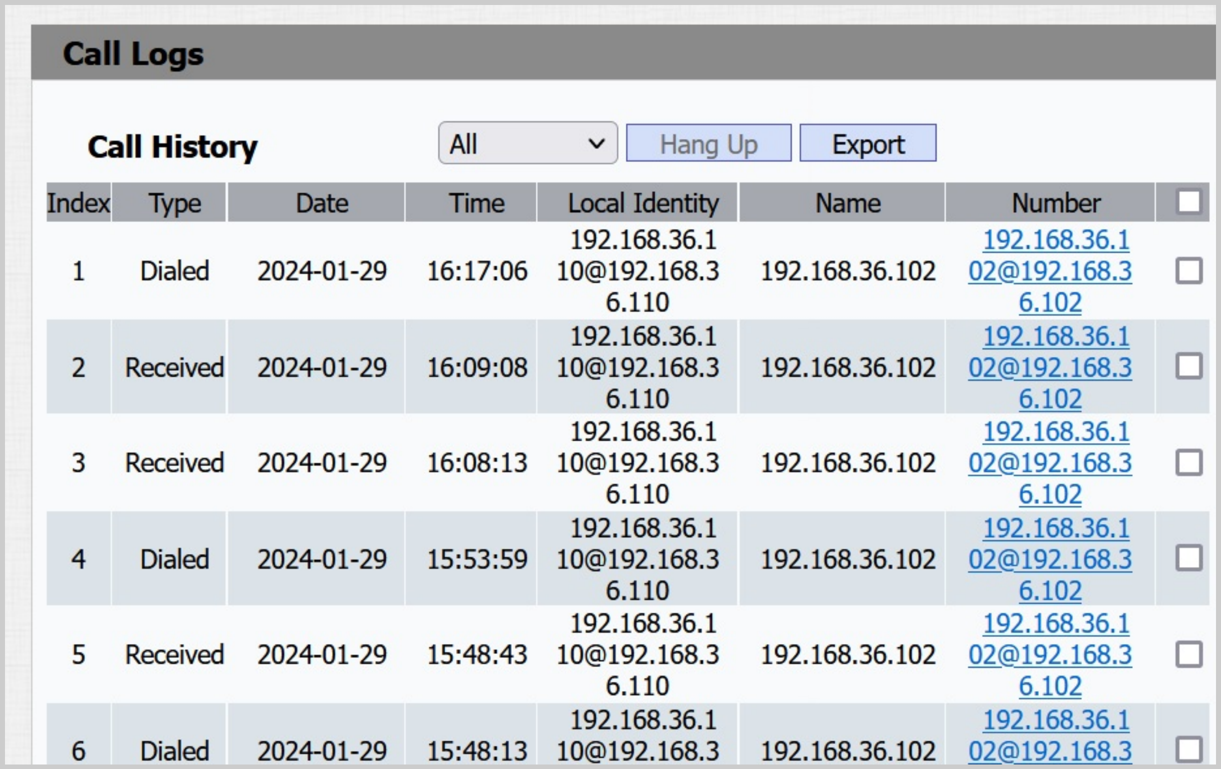


☐	192.168.31.154_1756712875000_1756712875567.avi	9/1/25 08:48	1.0 MB
☐	192.168.31.154_1756712875000_1756712885081.avi	9/1/25 08:48	1.3 MB
☐	192.168.31.154_1756713008000_1756713009070.wav	9/1/25 08:50	172 KB
☐	192.168.31.154_1756713429000_1756713429917.wav	9/1/25 08:57	1.5 MB

Call Logs

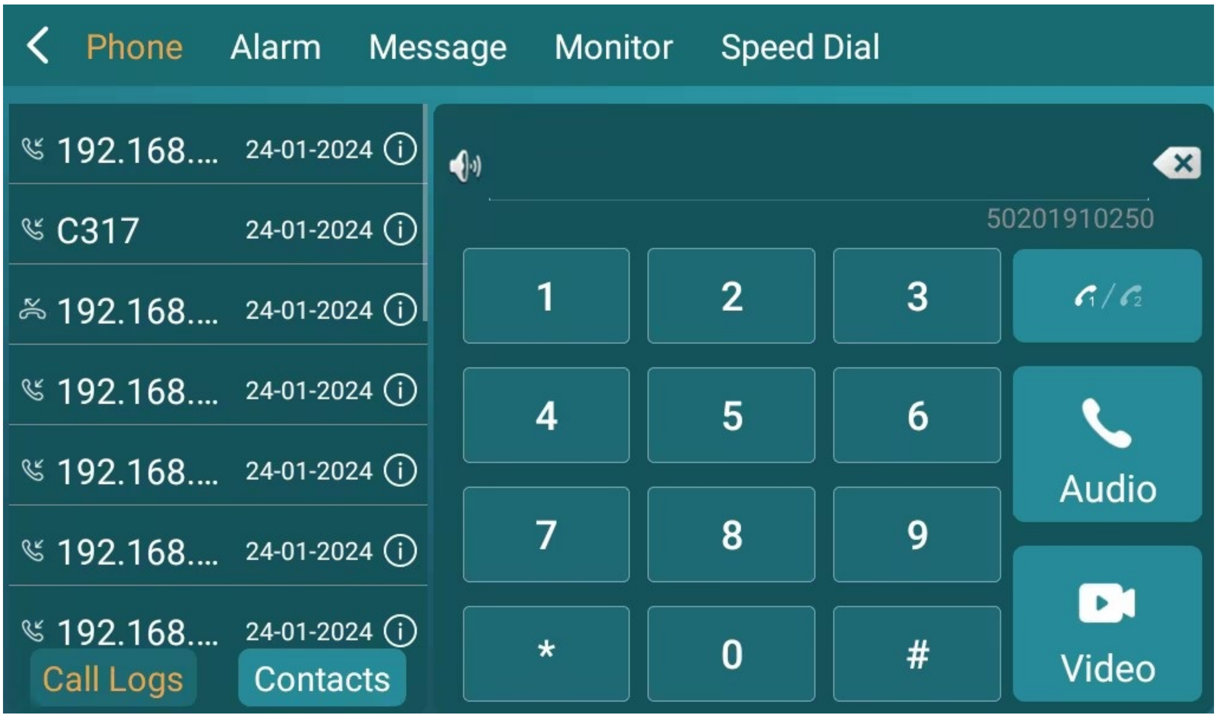
To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

Check call logs on the web **PhoneBook > Call Logs** interface.



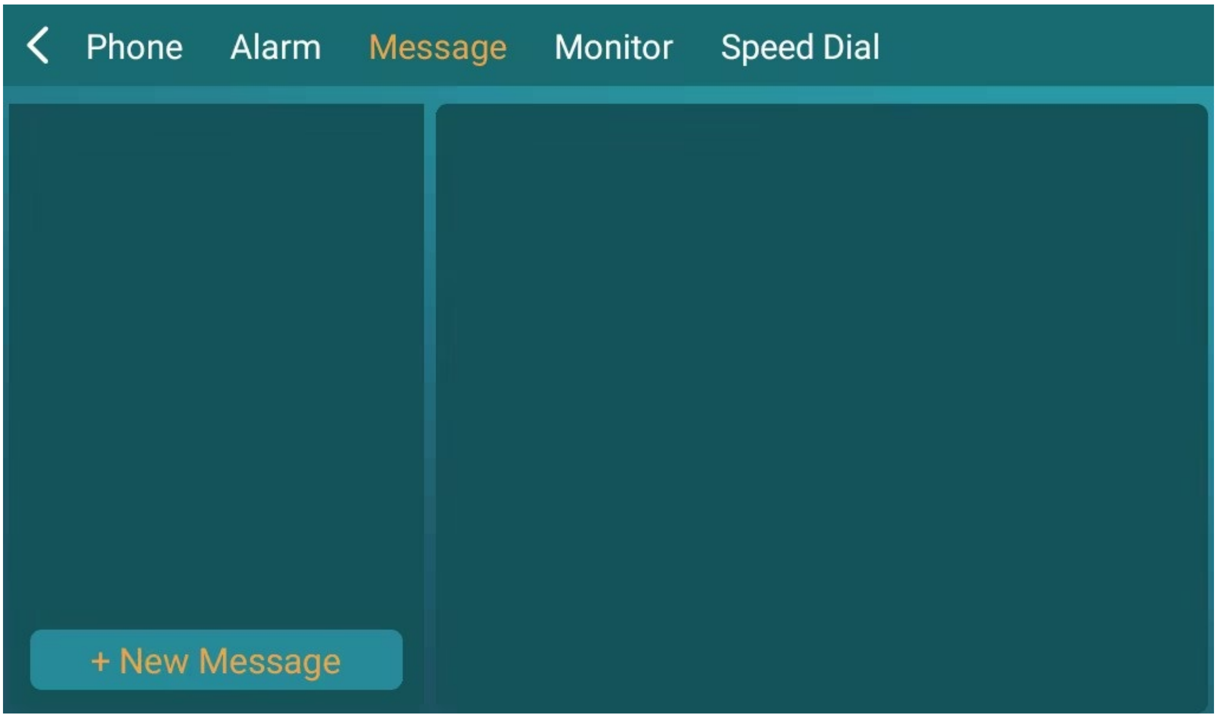
Index	Type	Date	Time	Local Identity	Name	Number	□
1	Dialed	2024-01-29	16:17:06	192.168.36.110@192.168.36.110	192.168.36.102	192.168.36.102@192.168.36.102	□
2	Received	2024-01-29	16:09:08	192.168.36.110@192.168.36.110	192.168.36.102	192.168.36.102@192.168.36.102	□
3	Received	2024-01-29	16:08:13	192.168.36.110@192.168.36.110	192.168.36.102	192.168.36.102@192.168.36.102	□
4	Dialed	2024-01-29	15:53:59	192.168.36.110@192.168.36.110	192.168.36.102	192.168.36.102@192.168.36.102	□
5	Received	2024-01-29	15:48:43	192.168.36.110@192.168.36.110	192.168.36.102	192.168.36.102@192.168.36.102	□
6	Dialed	2024-01-29	15:48:13	192.168.36.110@192.168.3	192.168.36.102	192.168.36.102@192.168.3	□

Call logs can also be checked on the device’s **Phone** screen.

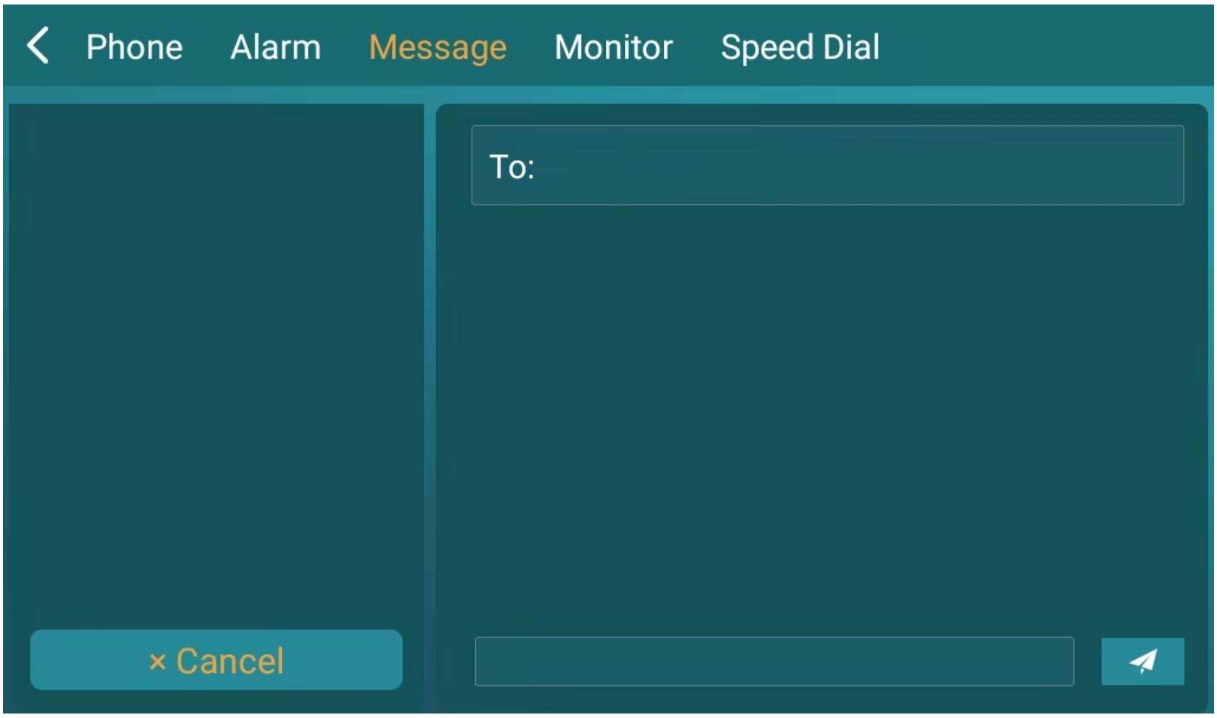

Phone
Alarm
Message
Monitor
Speed Dial
192.168.... 24-01-2024
C317 24-01-2024
192.168.... 24-01-2024
192.168.... 24-01-2024
192.168.... 24-01-2024
192.168.... 24-01-2024
192.168.... 24-01-2024
Call Logs
Contacts
50201910250
1
2
3
4
5
6
7
8
9
*
0
#
Audio
Video

Intercom Message

You can check, create, and clear messages on the **Message** screen. Press **Message** to create a new text message and press **Delete** to delete the existing messages.



Tap **+New Message**.


Phone
Alarm
Message
Monitor
Speed Dial
To:
× Cancel

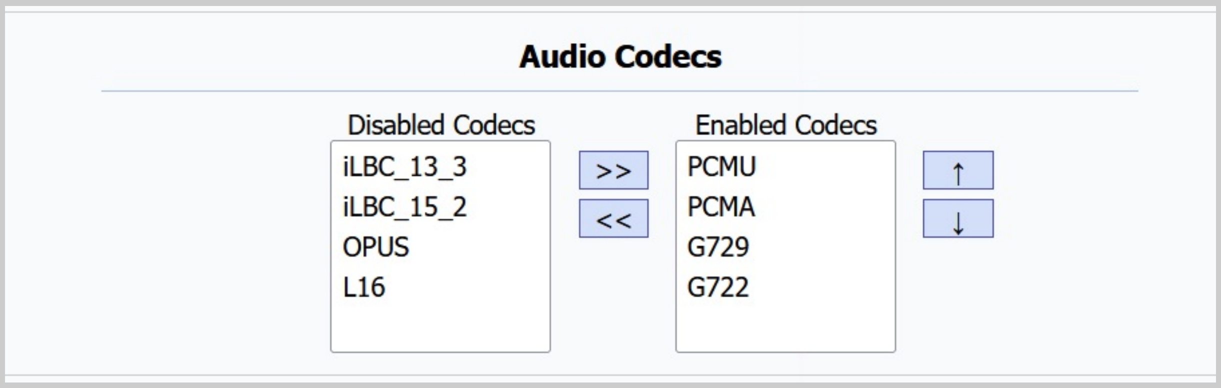
Audio & Video Configuration

Audio Codec Configuration

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

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

To set it up, navigate to the web **Account > Advanced > Audio Codecs** interface.



Audio Codecs

Disabled Codecs	Enabled Codecs
iLBC_13_3	PCMU
iLBC_15_2	PCMA
OPUS	G729
L16	G722

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

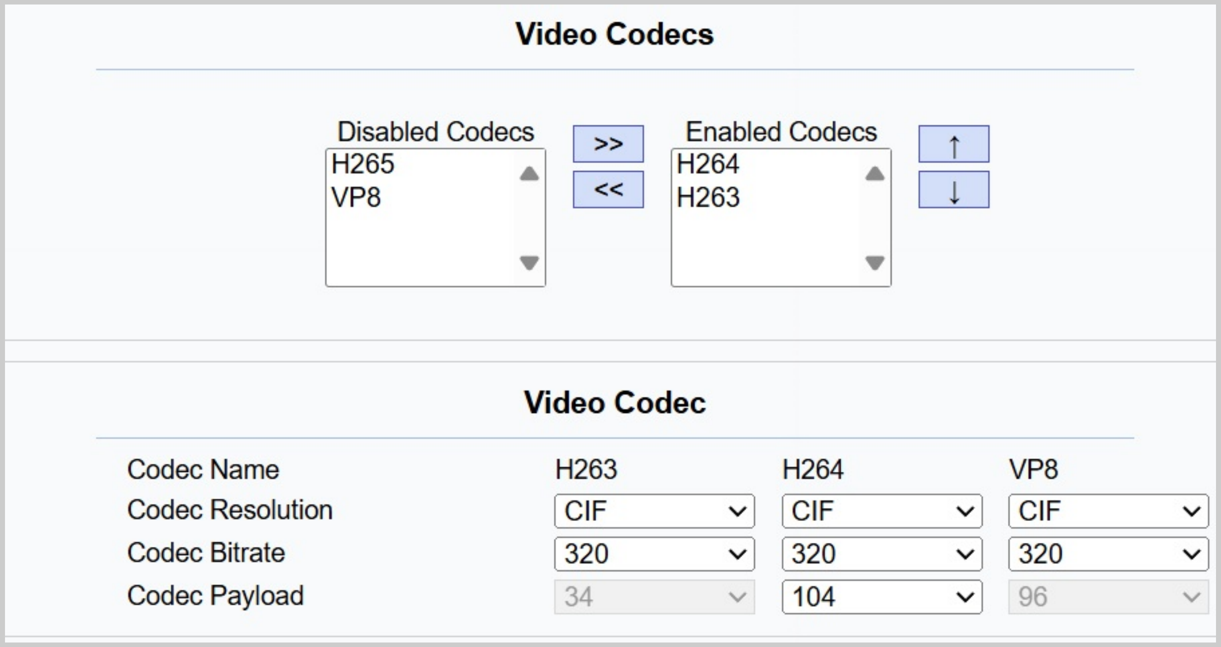
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ
iLBC_13_3	8,16 kbit/s	13.3kHZ
iLBC_15_2	8,16 kbit/s	15.2kHZ
L16	128 kbit/s	variable
OPUS	154.4 kbit/s	48kHZ

Video Codec Configuration

Video Codec for SIP Calls

The device supports the H263, H264, H265, and VP8 codecs. Choose the desired codec based on the network environment.

Set it up on the web **Account > Advanced > Video Codecs** interface.



Video Codecs

Disabled Codecs: H265, VP8

Enabled Codecs: H264, H263

Video Codec

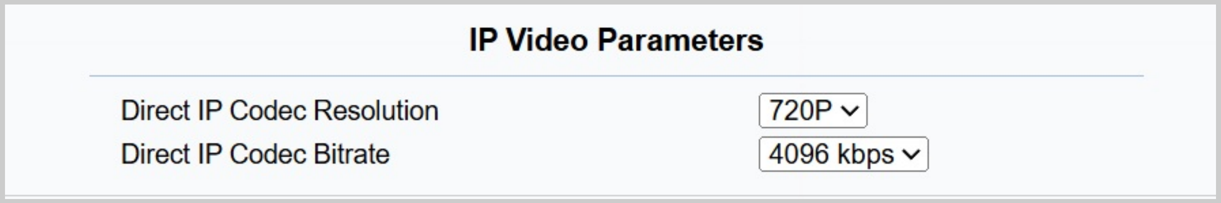
Codec Name	H263	H264	VP8
Codec Resolution	CIF	CIF	CIF
Codec Bitrate	320	320	320
Codec Payload	34	104	96

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

Video Codec for IP Calls

You can select the IP call video quality by selecting the proper codec resolution according to the network condition.

Set it up on the **Phone > Call Feature** interface.



IP Video Parameters

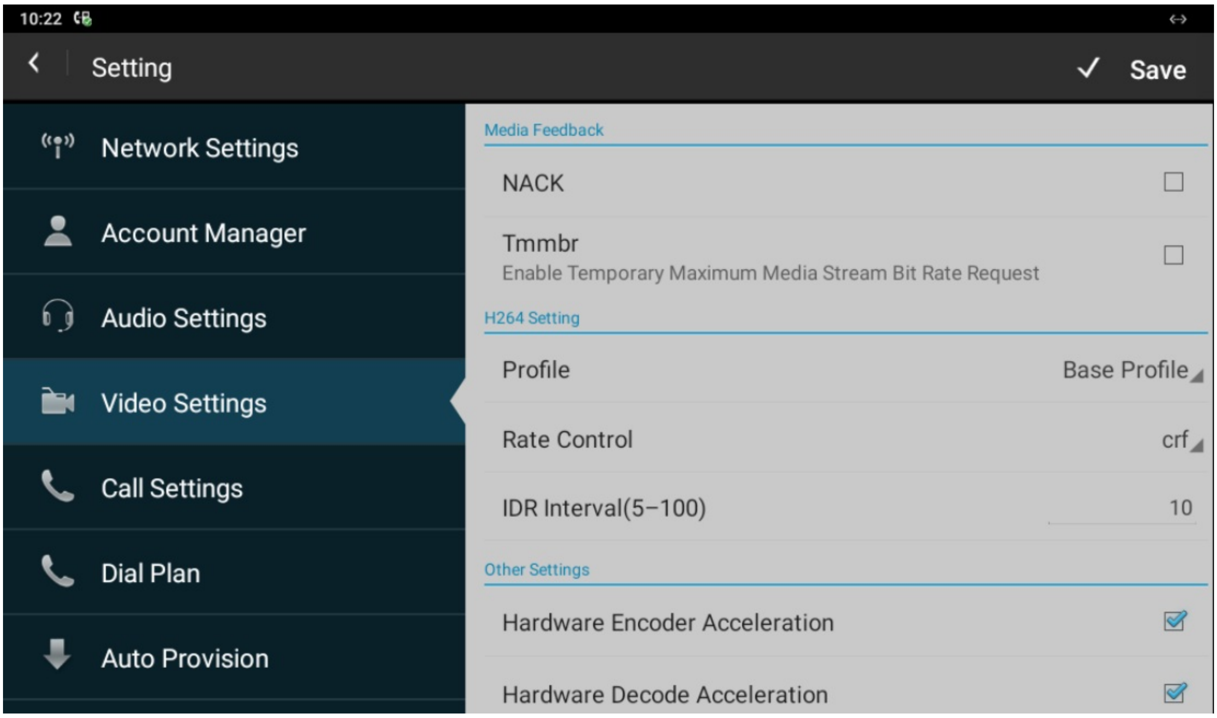
Direct IP Codec Resolution: 720P

Direct IP Codec Bitrate: 4096 kbps

- **Direct IP Codec Resolution**: Select the resolution from the provided options. The default is 720P(1280×720 pixels).
- **Direct IP Codec Bitrate**: The video stream bitrate ranges from 128 to 4096 kbps. The default bitrate is 4096.

H264 Setting

You can also set up H264 video codec on the ⚙ **> Video Settings** screen.



10:22

Setting ✓ Save

Media Feedback

NACK □

Tmmbr □
Enable Temporary Maximum Media Stream Bit Rate Request

H264 Setting

Profile Base Profile

Rate Control crf

IDR Interval(5–100) 10

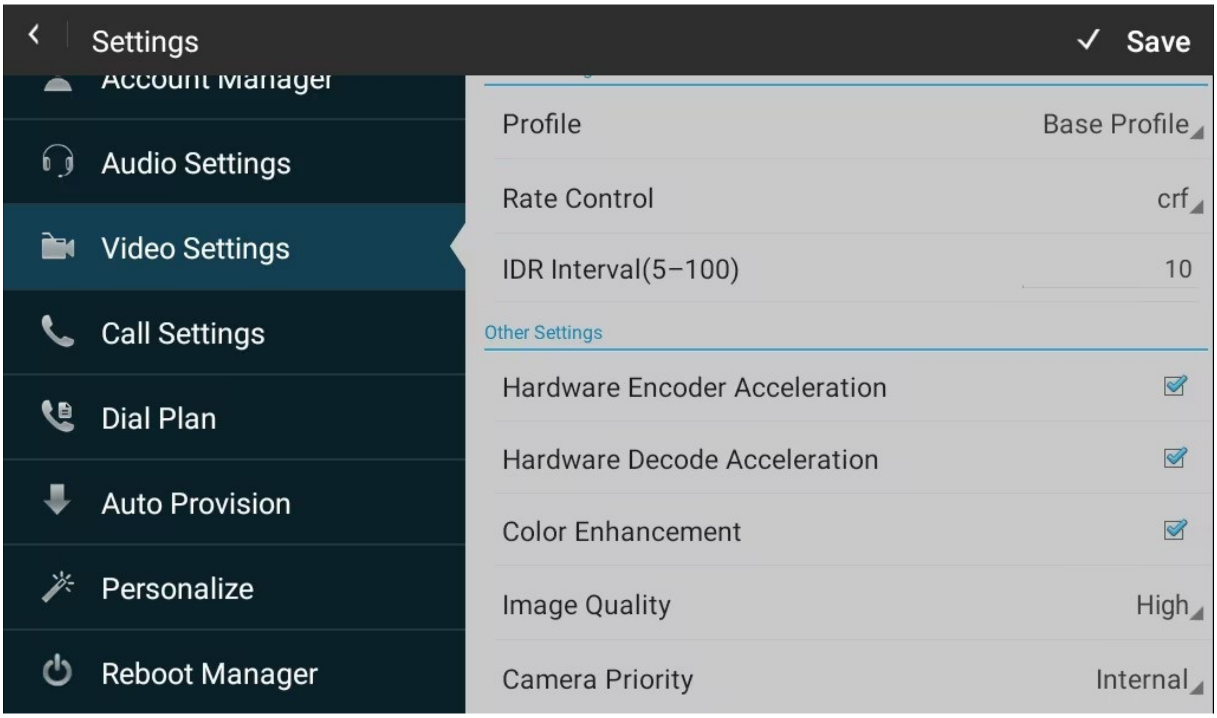
Other Settings

Hardware Encoder Acceleration ☑

Hardware Decode Acceleration ☑

- **Profile**: Select the video code profile level; the higher the profile is, the more complex and efficient the encoding will be. Base Profile is the default setting.
- **Rate Control**: Used to control the encoding bitrate.
- **IDR Intervals(5-100)**: IDR means Instantaneous Decoding Refresh. It is used to control the process of coding and decoding.

Other video settings can be configured on the same screen.



Settings ✓ Save

Profile Base Profile

Rate Control crf

IDR Interval(5–100) 10

Other Settings

Hardware Encoder Acceleration ☑

Hardware Decode Acceleration ☑

Color Enhancement ☑

Image Quality High

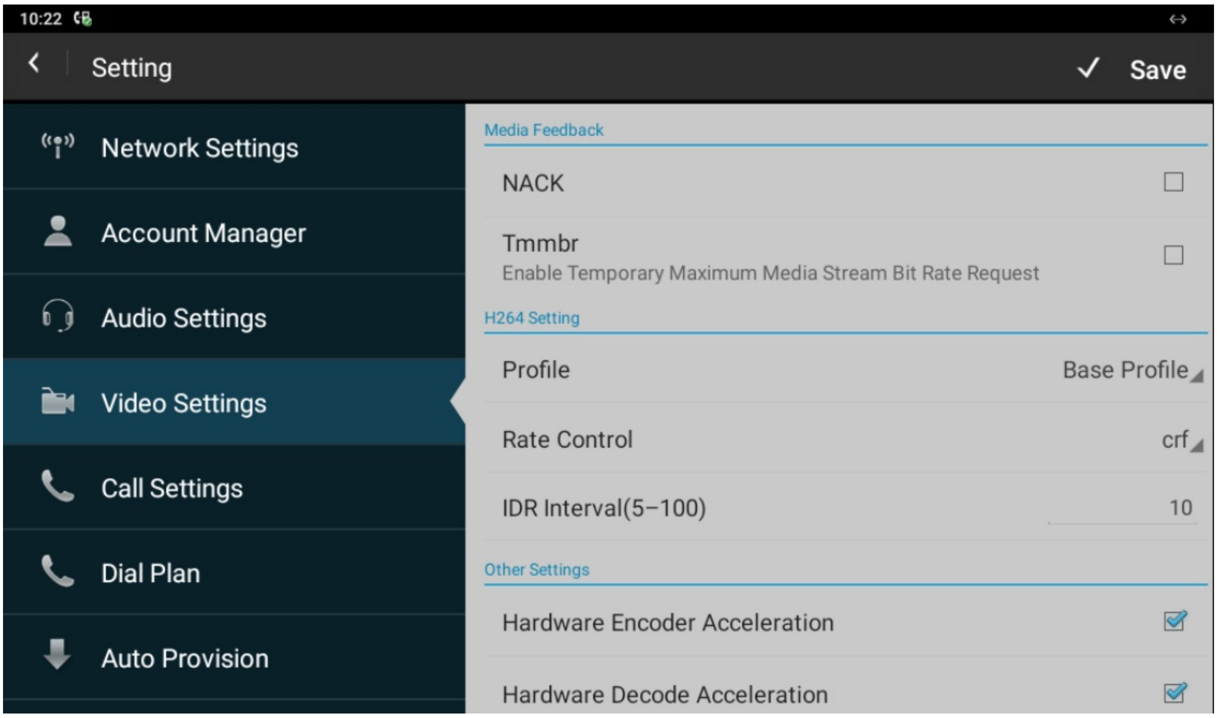
Camera Priority Internal

- **Hardware Encode Acceleration**: Enable it to turn on the function to accelerate video encoding on a hardware basis.
- **Hardware Decode Acceleration**: Enable it to turn on the function to accelerate the video decoding on a hardware basis. This function is disabled by default.
- **Color Enhancement**: Enable it to increase the phone display color. Enabled by default.
- **Image Quality**: Users can select Low, Middle, or High modes that determine the encoded picture quality.
- **Camera Priority**: Decide whether the internal or external has a higher priority.

Media Feedback

To ensure smooth and continued data transmission for the video call, you are required to set both Negative Acknowledgement(NACK) and Temporal Max Media Bitrate Request(Tmmbr).

Navigate to the device ⚙ > **Video Settings** screen.



Media Feedback

NACK □

Tmmbr □
Enable Temporary Maximum Media Stream Bit Rate Request

H264 Setting

Profile Base Profile

Rate Control crf

IDR Interval(5-100) 10

Other Settings

Hardware Encoder Acceleration ☑

Hardware Decode Acceleration ☑

- **NACK**: Used to reinforce the data transmission during the video call. It can be used to prevent losing data packets in a weak network environment when discontinued and mosaic video images occur.

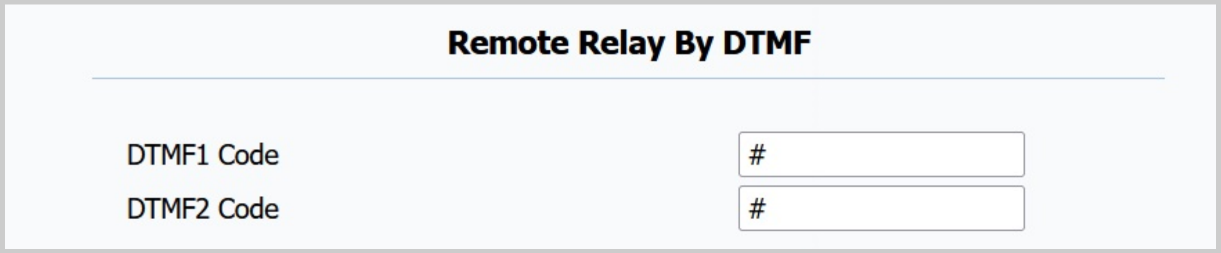
- **Tmmbr**: Used to indicate the maximum bitrate that the receiver can take.

Door Access Control Configuration

Open the Door via DTMF

Users can use the unlock tab during the call to open the door. You are required to set up the same DTMF code in the door phone and the guard phone.

Set it up on the web **Phone > Remote Relay > Remote Relay By DTMF** interface.



Remote Relay By DTMF

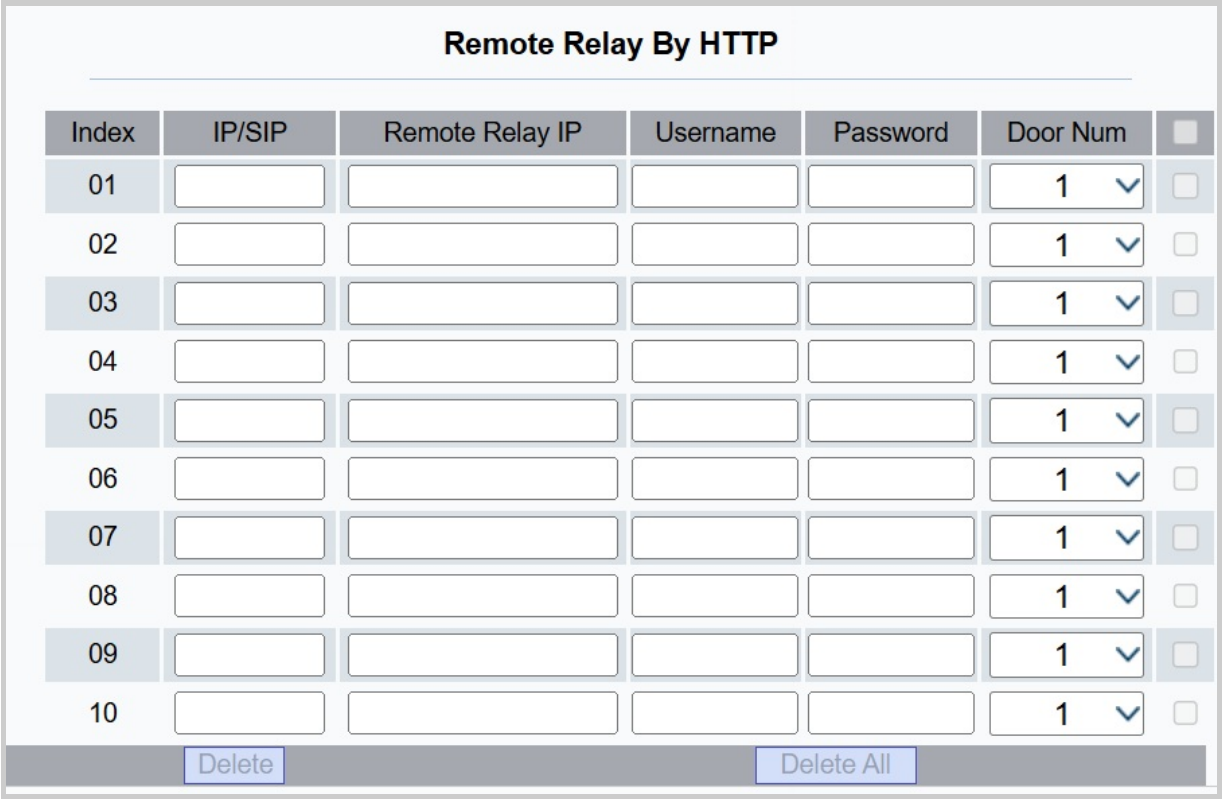
DTMF1 Code	#
DTMF2 Code	#

- **DTMF1/2 Code**: Set the DTMF code for the remote relay, which is # by default.

Open the Door via HTTP Command

The device supports remote door opening via an HTTP command. Simply enable this feature and input the HTTP command (URL) for the device. This will trigger the relay connected to another intercom device, e.g., a door phone, and open the door.

Set it up on the **Phone > Remote Relay > Remote Relay By HTTP** interface.



Remote Relay By HTTP

Index	IP/SIP	Remote Relay IP	Username	Password	Door Num	☐
01					1	☐
02					1	☐
03					1	☐
04					1	☐
05					1	☐
06					1	☐
07					1	☐
08					1	☐
09					1	☐
10					1	☐

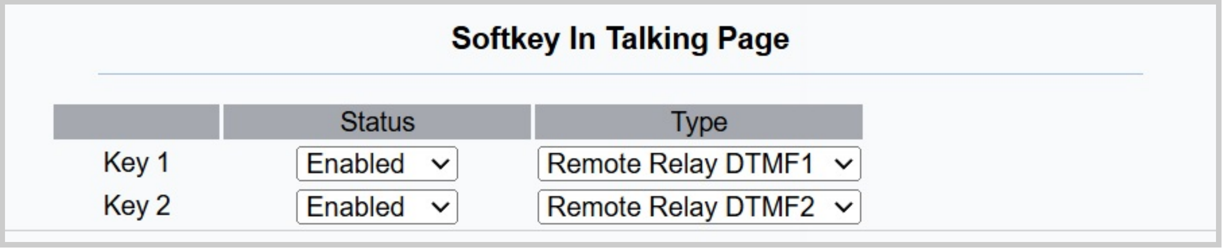
- **IP/SIP**: Enter the IP address or SIP account to trigger a certain remote relay by sending an HTTP message.
- **Remote Relay IP**: Specify the IP of the door phone.
- **Username**: Enter the username the same as that configured on the door phone's web interface.
- **Password**: Enter the password the same as that configured on the door phone's web interface.
- **Door Num**: Check the relay to be triggered. DoorNum1 corresponds to Relay A; DoorNum2 corresponds to Relay B, and so on.

> **Note**
> Please refer to **Open the Door via HTTP Command** for detailed configuration.

Unlock Key Configuration

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

Navigate to the web **Phone > Remote Relay > Softkey In Talking Page** interface.

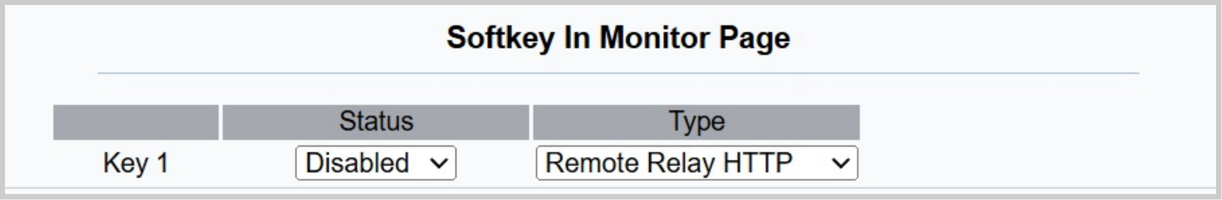


Softkey In Talking Page

	Status	Type
Key 1	Enabled	Remote Relay DTMF1
Key 2	Enabled	Remote Relay DTMF2

- **Status**: With the unlock tabs enabled on the talking screen, the unlock tabs will appear during a call.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up the unlock tab on the Monitor screen.

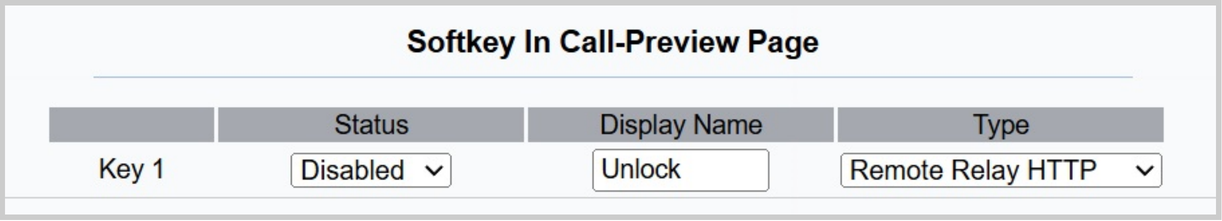


Softkey In Monitor Page

	Status	Type
Key 1	Disabled	Remote Relay HTTP

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

To set up the unlock tab on the call preview screen on the same interface.



Softkey In Call-Preview Page

	Status	Display Name	Type
Key 1	Disabled	Unlock	Remote Relay HTTP

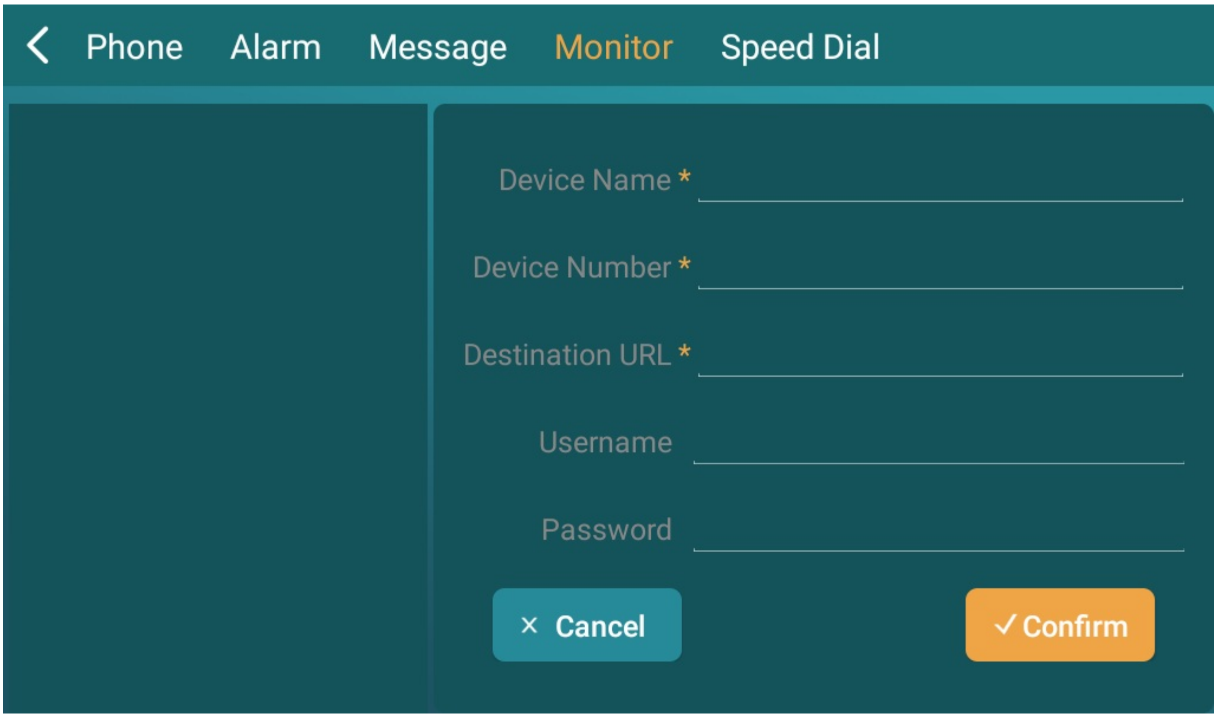
- **Status**: With the unlock tab enabled, the unlock tab will appear on the monitoring screen.
- **Display Name**: Name the key.
- **Type**: Select the relay trigger type according to the actual setup.

Security

Monitor Settings

You can use RTSP to watch a live video stream from other intercom devices on the device.

Tap **Monitor** on the home screen and tap **+New Monitor**.

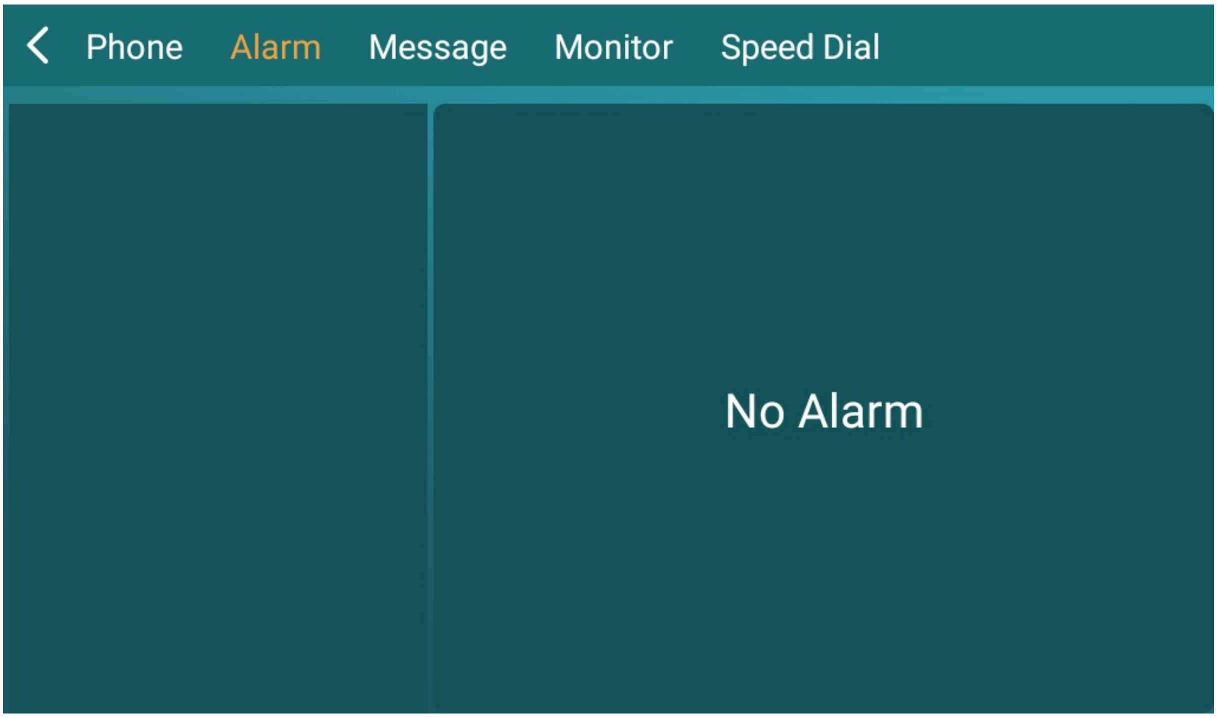


- **Device Number**: The device's SIP/IP number for identification.
- **Device Name**: The device name for identification.
- **Destination Address**: The RTSP address of the monitoring device. RSTP format: rtsp://Device IP address/live/ch00_0.
- **Username**: The username of the monitoring device for authentication.
- **Password**: The password of the monitoring device for authentication.

Alarm

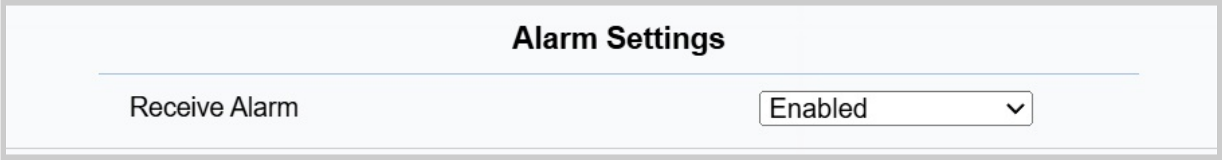
You can check, clear, and deal with the alarms triggered by the device.

Tap **Alarm** on the device home screen.



No Alarm

If you do not want to receive alarms on the device, you can disable the alarm feature on the **Phone > Preference > Alarm Settings** interface.



Alarm Settings

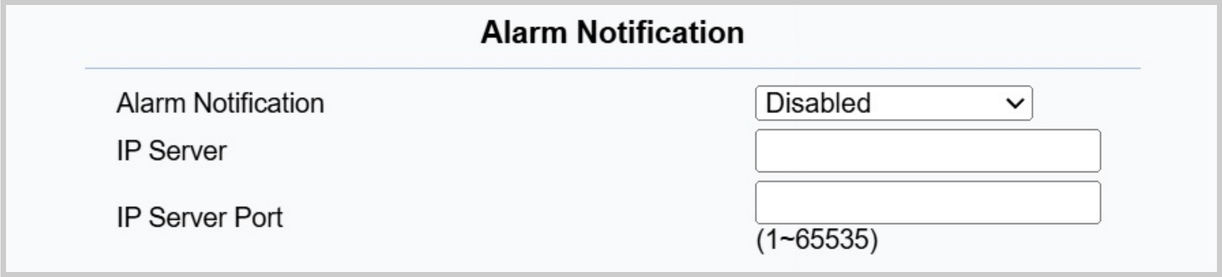
Receive Alarm	Enabled

- **Receive Alarm**: It is enabled by default.

Alarm Notification

The device supports sending alarm notifications in HTTP URL format to a third-party property management system.

Set it up on the **Phone > Preference** interface.



Alarm Notification

Alarm Notification	Disabled
IP Server	
IP Server Port	(1~65535)

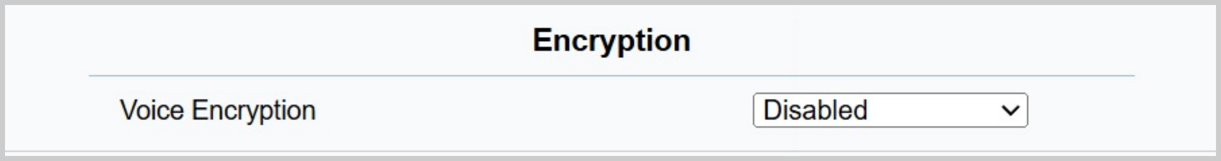
- **Alarm Notification**: Turn on/off the feature.

- **IP Server**: The designated third-party server address. The HTTP message contains the information: device name, triggered zone, alarm type, area, and alarm time.
- **IP Server Port**: The third-party server's port number.

Voice Encryption

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

Set it up on the web **Account > Advanced > Encryption** interface.



Encryption

Voice Encryption: Disabled

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

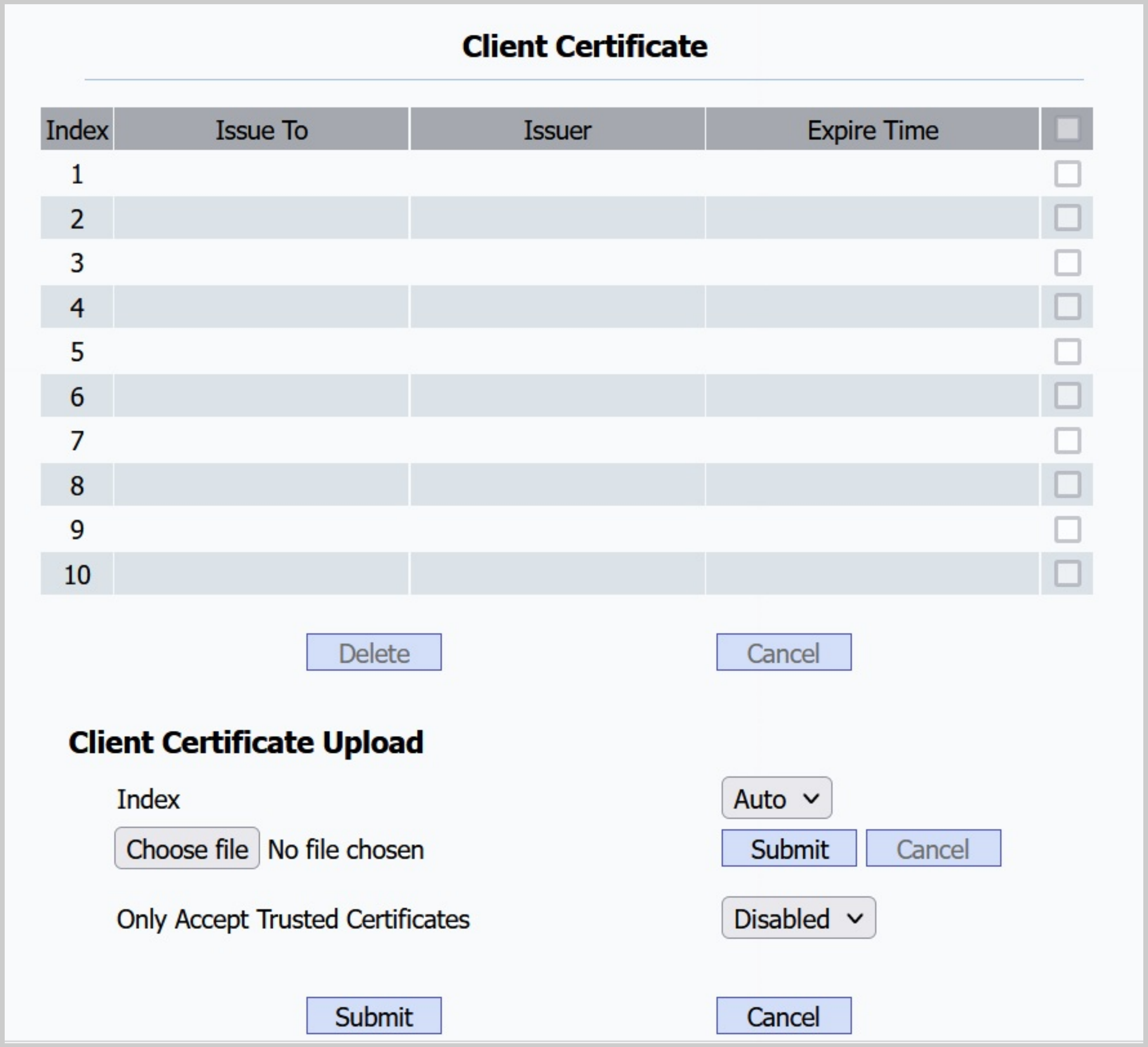
Client Certificate Setting

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

Client Certificate

This certificate verifies the server to the device when they want to connect using SSL. The device verifies the server's certificate against its client certificate list.

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



Client Certificate

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

Delete Cancel

Client Certificate Upload

Index: Auto

Choose file No file chosen Submit Cancel

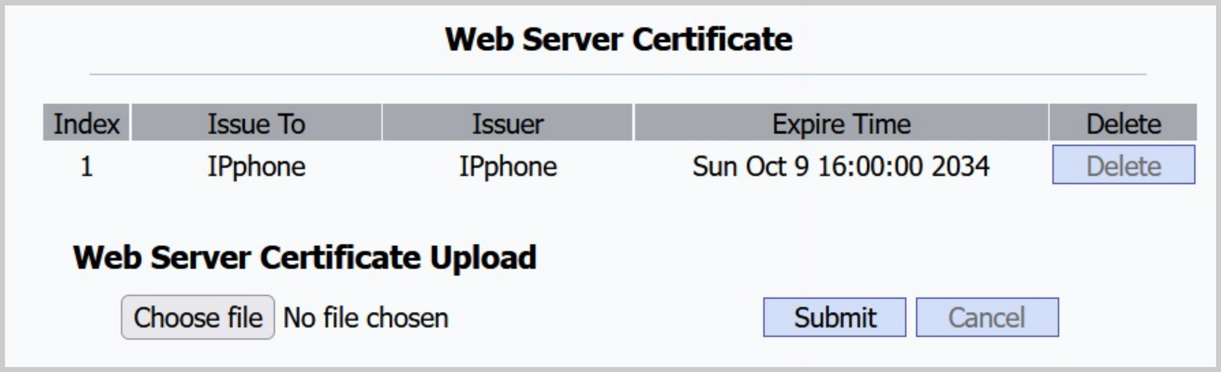
Only Accept Trusted Certificates: Disabled

Submit Cancel

Web Server Certificate

It is a certificate sent to the client for authentication when the client requests an SSL connection with the Akuvox device. Please upload the certificates in accepted formats.

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



Web Server Certificate

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

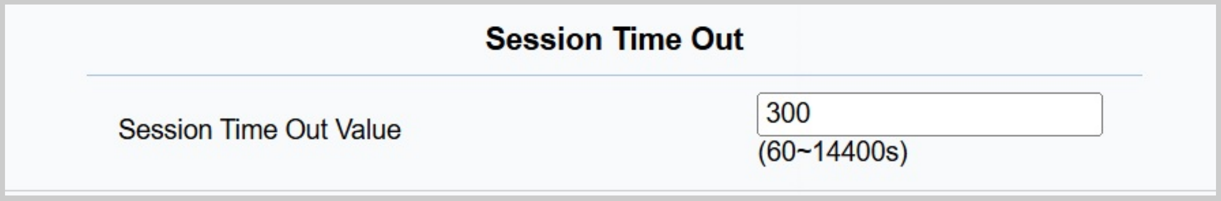
Web Server Certificate Upload

Choose file No file chosen Submit Cancel

Web Interface Automatic Log-out

You can set up the web interface's automatic log-out timing, requiring re-login by entering the user name and the passwords for security purposes or for the convenience of operation.

Set it up on the **Security > Basic > Session Time Out** interface.



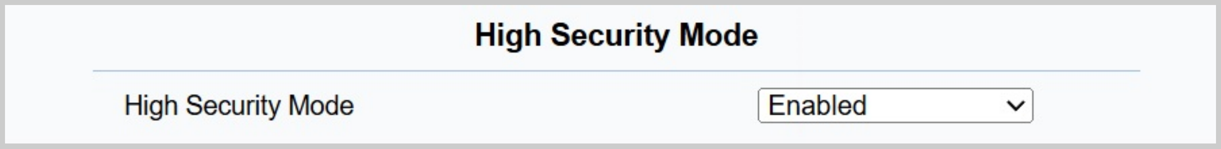
Session Time Out

Session Time Out Value: 300 (60~14400s)

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.

Enable/disable it on the **Security > Basic > High Security Mode** interface.



High Security Mode

High Security Mode: Enabled

Important Notes

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

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

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

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

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

- 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

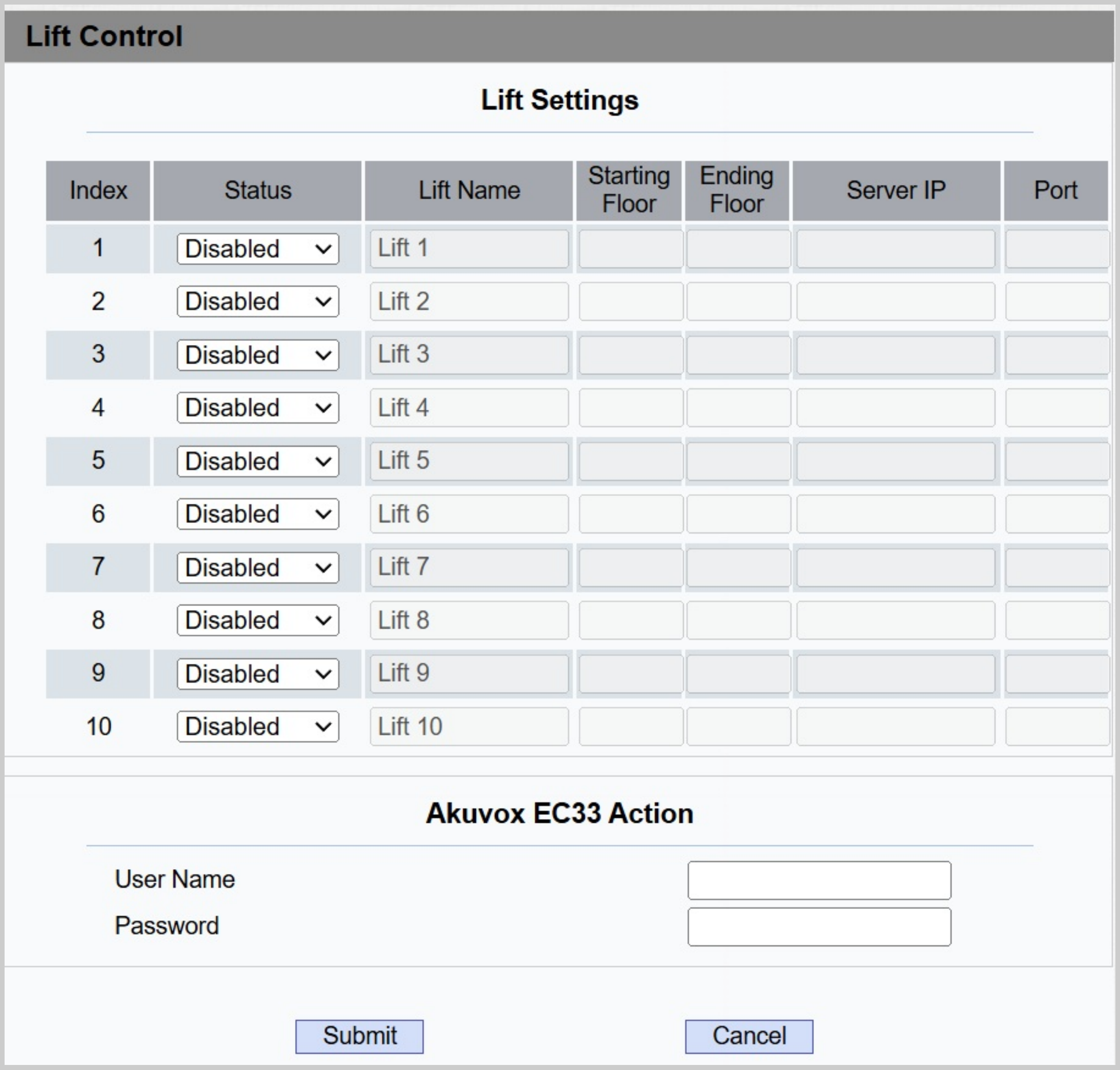
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Lift Control

Residents can summon and send the lift by simply tapping on the Akuvox guard phone.

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

Set it up on the **Phone > Lift Control** interface.



Lift Control

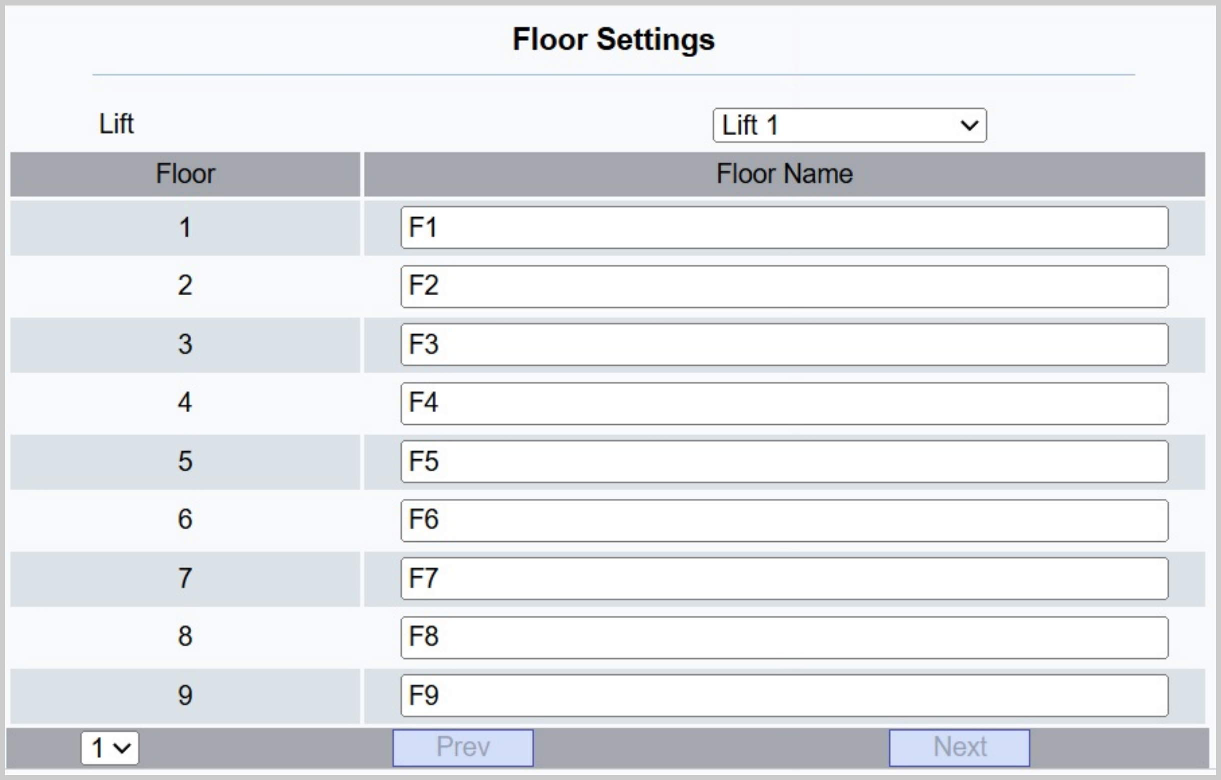
Lift Settings

Index	Status	Lift Name	Starting Floor	Ending Floor	Server IP	Port
1	Disabled	Lift 1				
2	Disabled	Lift 2				
3	Disabled	Lift 3				
4	Disabled	Lift 4				
5	Disabled	Lift 5				
6	Disabled	Lift 6				
7	Disabled	Lift 7				
8	Disabled	Lift 8				
9	Disabled	Lift 9				
10	Disabled	Lift 10				

Akuvox EC33 Action

User Name

Password



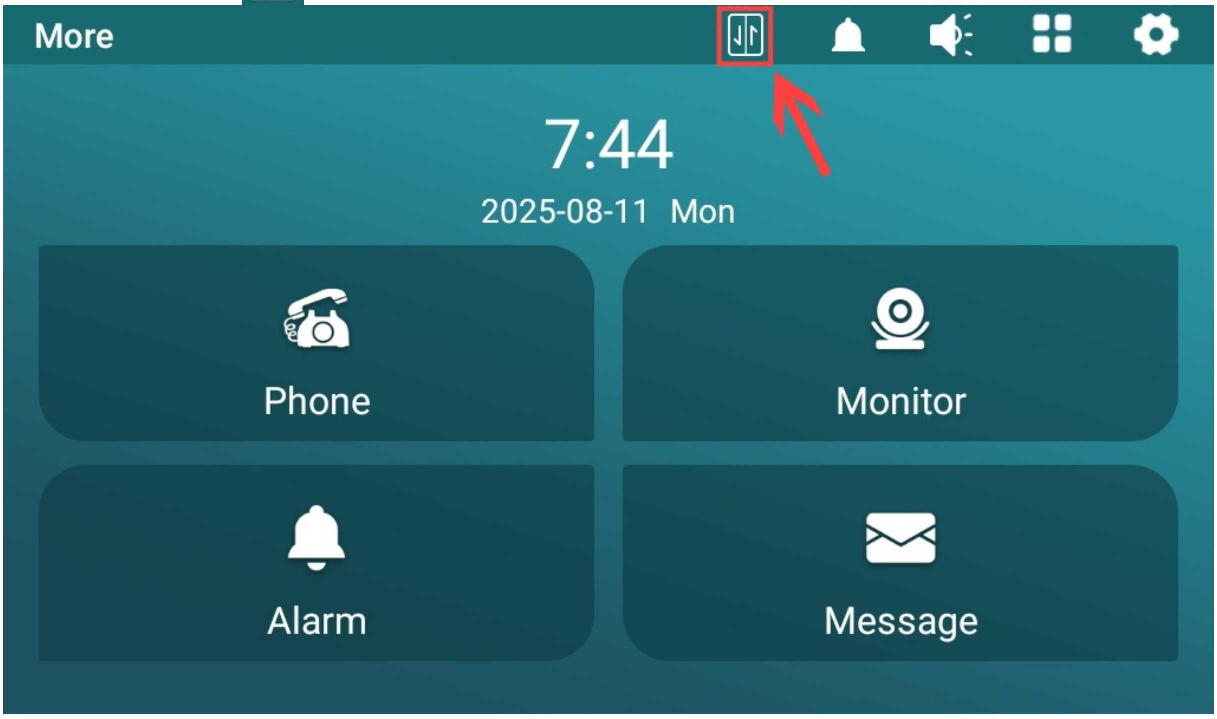
Floor Settings

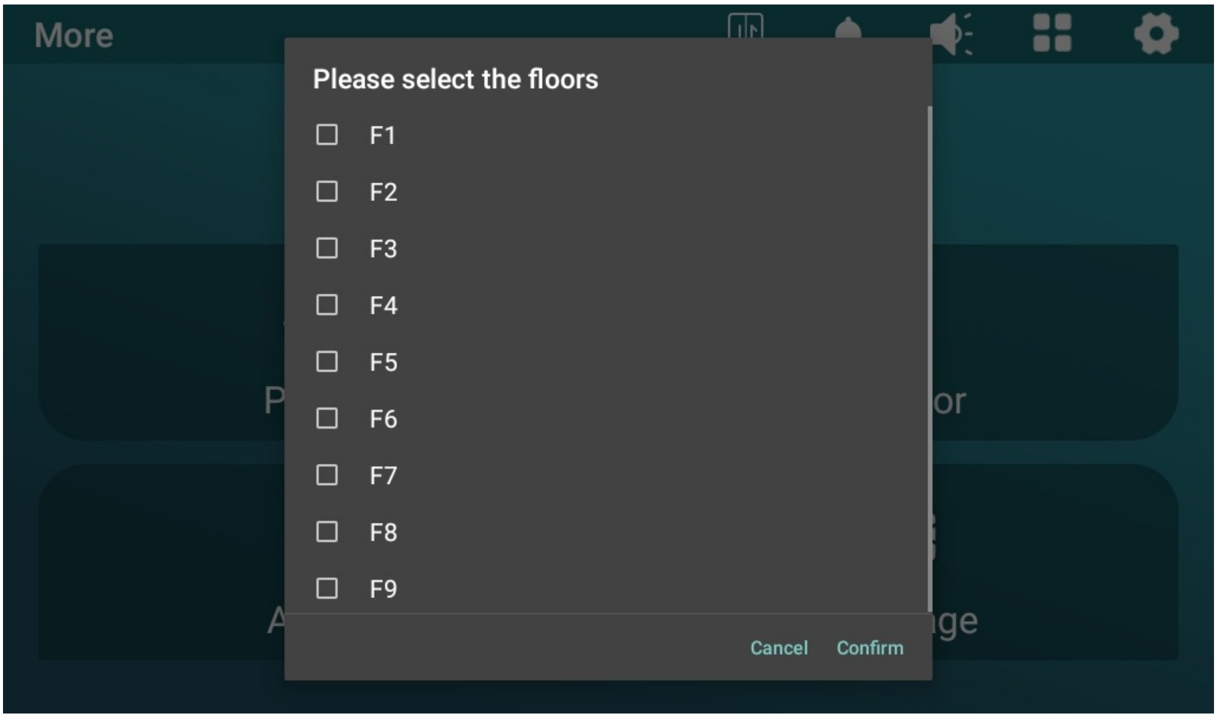
Lift: Lift 1

Floor	Floor Name
1	F1
2	F2
3	F3
4	F4
5	F5
6	F6
7	F7
8	F8
9	F9

- **Status**: Enable/disable the lift. When enabled, set up **Floor Settings**. You can name each floor.
- **Lift Name**: Name the lift.
- **Starting Floor**: Set the lift control starting floor(-5-128). It cannot be 0.
- **Ending Floor**: Set the lift control ending floor(-5-128). It cannot be 0.
- **Server IP**: The IP address of EC33.
- **Port**: The port of EC33.
- **Username**: The username set in EC33 for authentication.
- **Password**: The password set in EC33 for authentication.

Users can tap and select the target floor.





Please select the floors

□ F1

□ F2

□ F3

□ F4

□ F5

□ F6

□ F7

□ F8

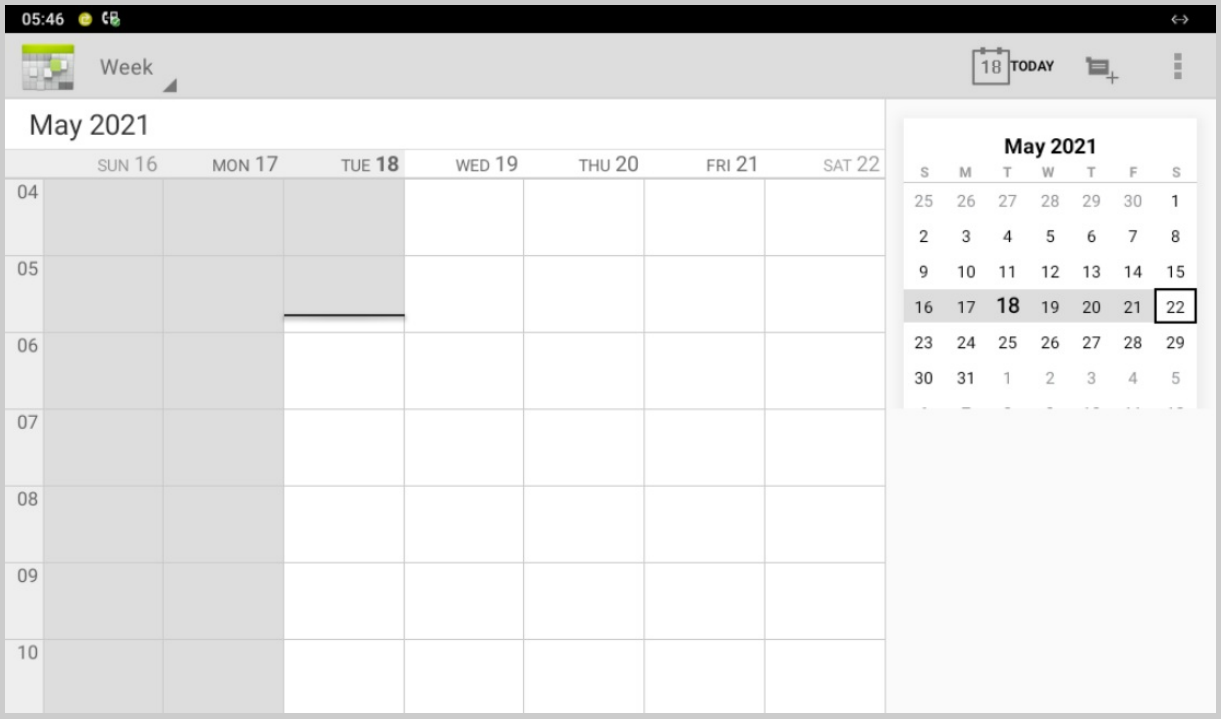
□ F9

Applications

Calendar

Users can set up the events and agenda in the calendar.

Navigate to the ⊞ **> Calendar** screen.



Camera

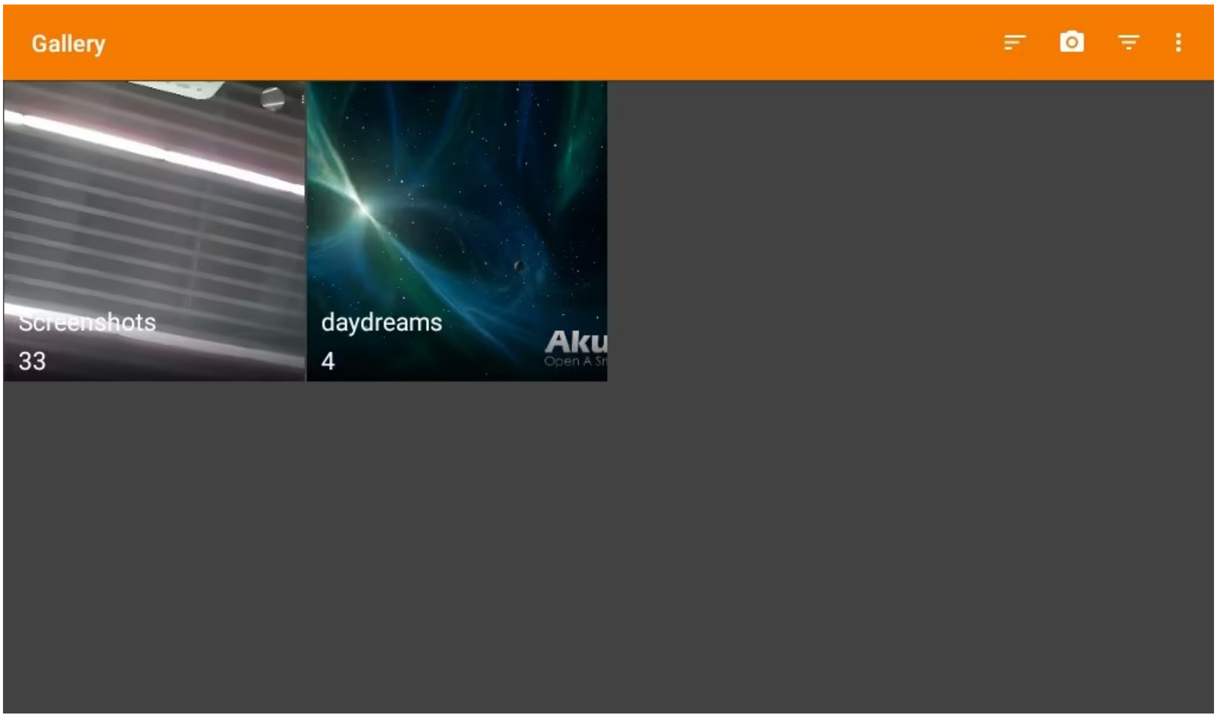
R49G has installed a camera in the front, which allows users to take pictures as needed.

Navigate to the ⊞ **> Camera** screen.

Gallery

In the Gallery, all the screenshots, pictures, and videos taken can be checked, edited, deleted, and shared.

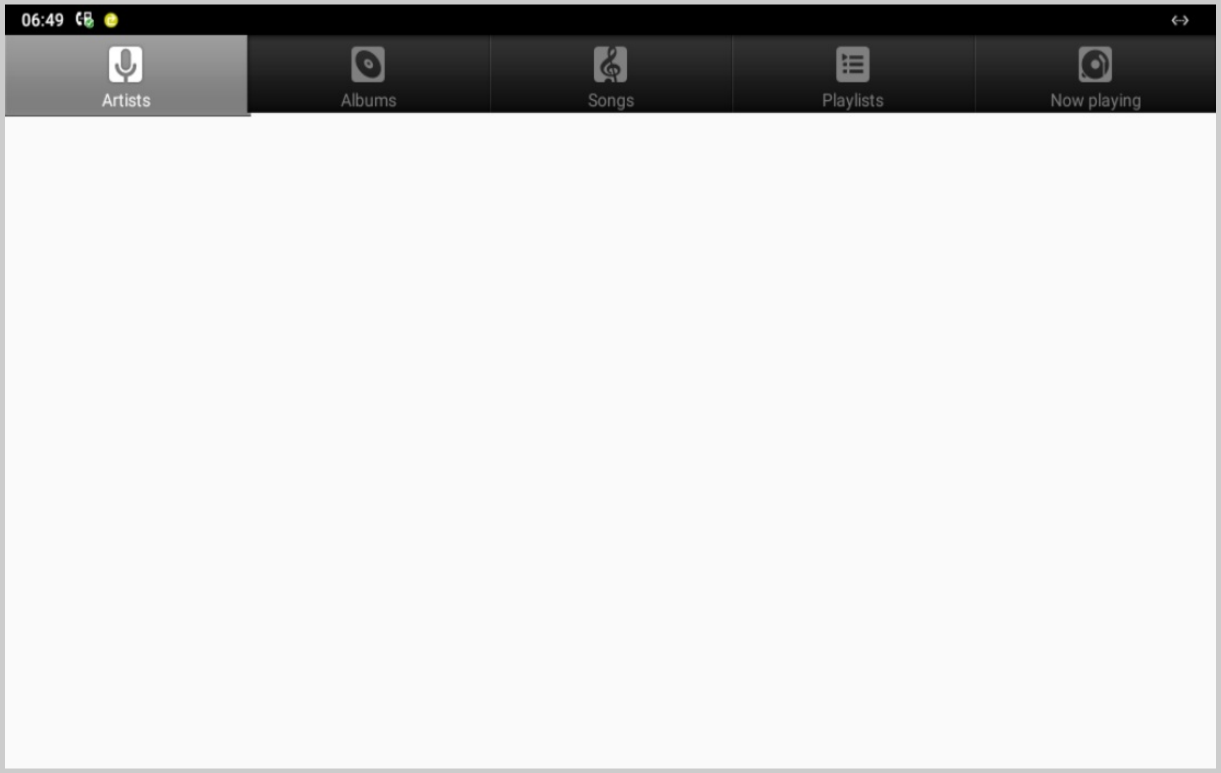
Navigate to the ⊞ > **Gallery** screen.



Music

R49G can also serve as a music player. Users can play music by Artist, Album, Songs, and Playlist, and check on the music being played.

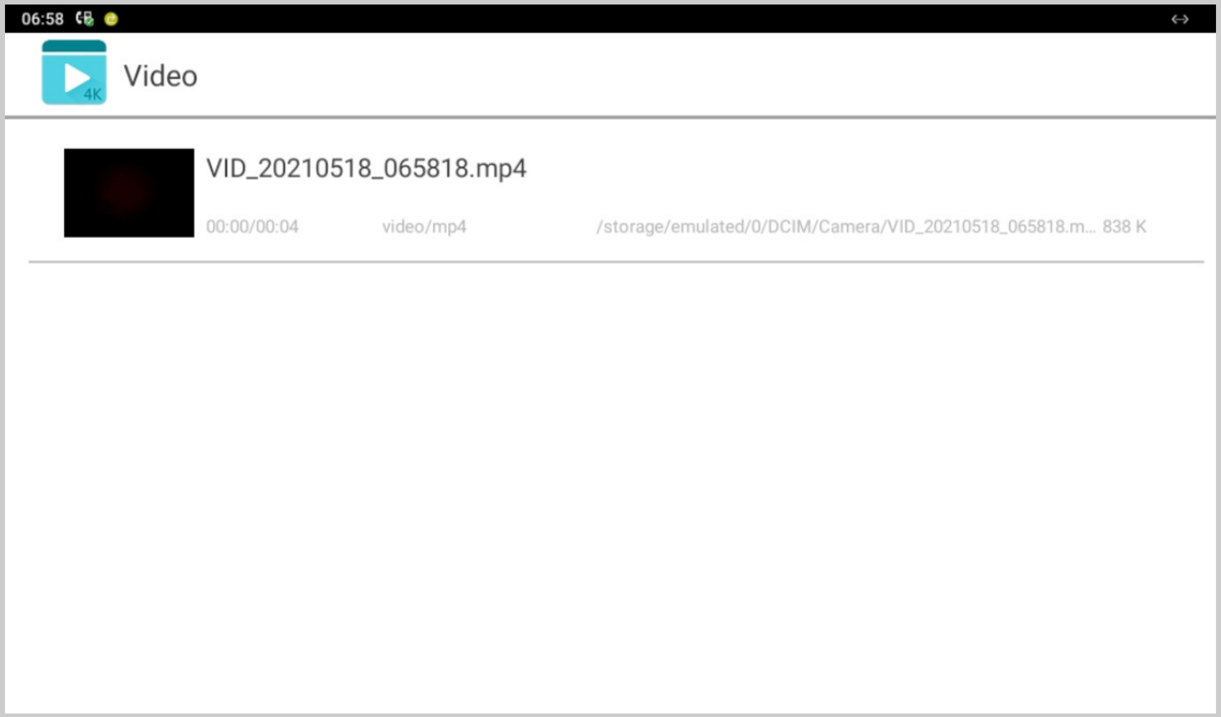
Navigate to the ⊞ **> Music** screen.



Video

Users can check, delete, and play the video stored in the guard phone.

Navigate to the ⊞ **> Video** screen.



06:58

Video

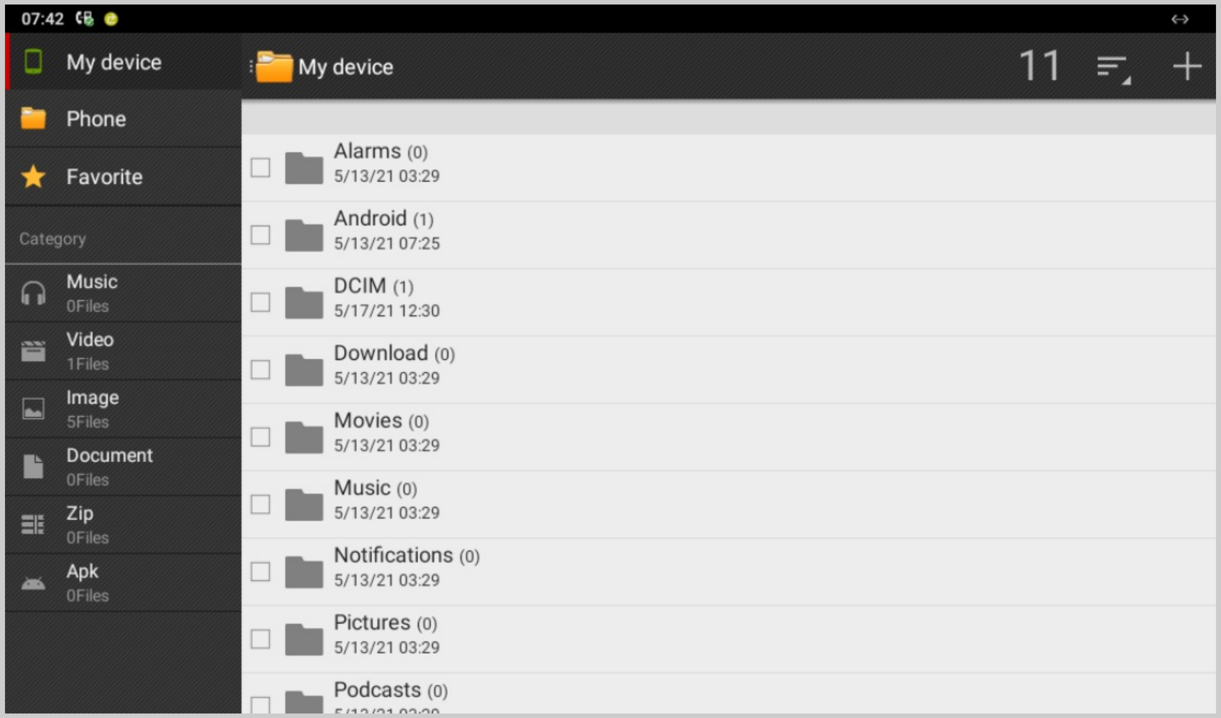
VID_20210518_065818.mp4

00:00/00:04 video/mp4 /storage/emulated/0/DCIM/Camera/VID_20210518_065818.m... 838 K

Explorer

Explorer in the R49G serves as a file manager that allows users to manage all types of files stored in the device. Users can search, check, sort, delete, copy, and paste the files in the Explorer as needed.

Navigate to the ▦ **> Explorer** screen.



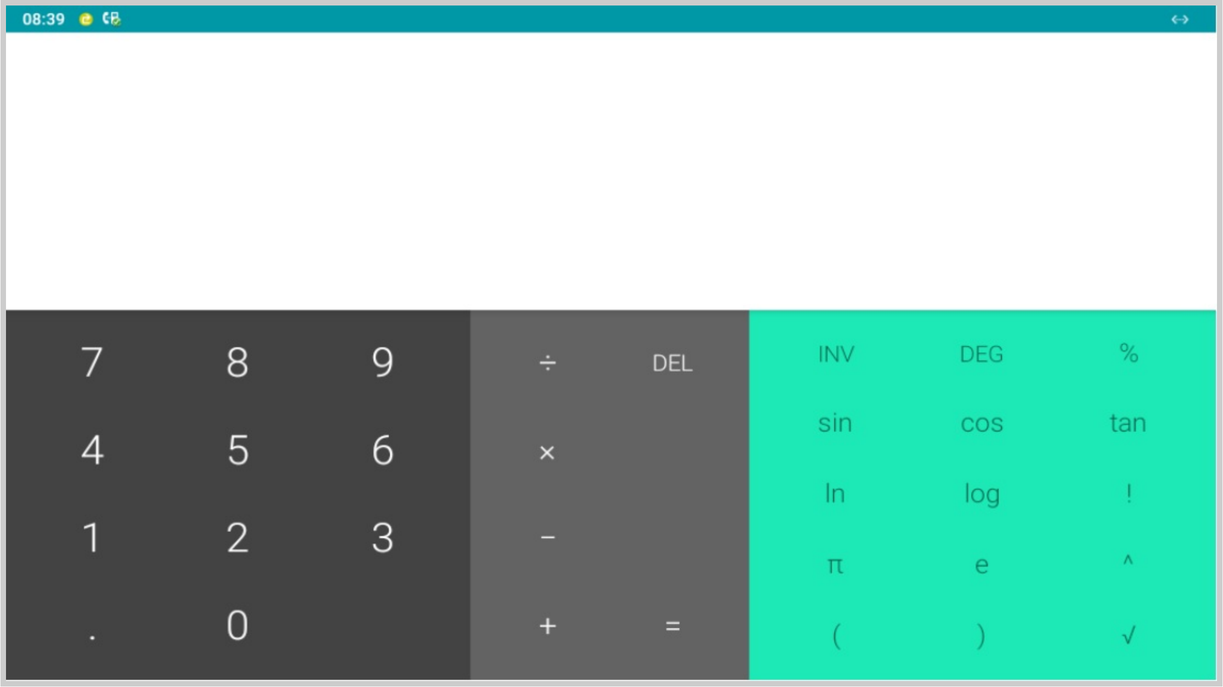
07:42

My device	My device 11
Phone	□ Alarms (0) 5/13/21 03:29
Favorite	□ Android (1) 5/13/21 07:25
Category	□ DCIM (1) 5/17/21 12:30
Music 0Files	□ Download (0) 5/13/21 03:29
Video 1Files	□ Movies (0) 5/13/21 03:29
Image 5Files	□ Music (0) 5/13/21 03:29
Document 0Files	□ Notifications (0) 5/13/21 03:29
Zip 0Files	□ Pictures (0) 5/13/21 03:29
Apk 0Files	□ Podcasts (0)

Calculator

The calculator in the device allows users to do the calculation.

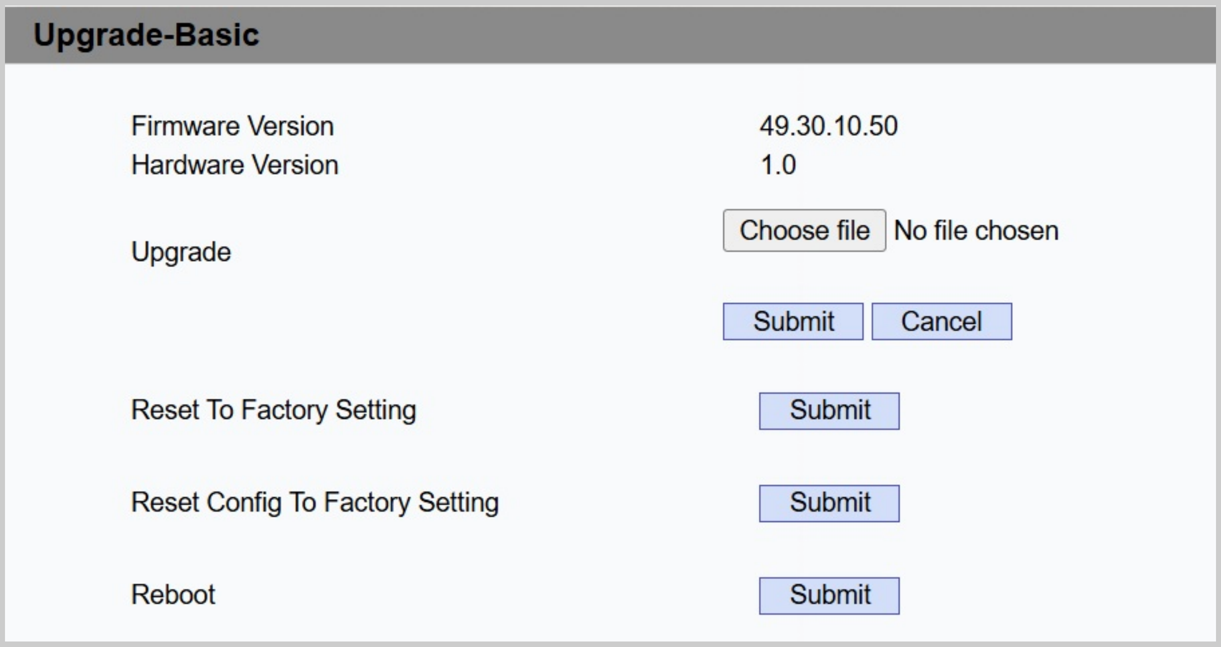
Navigate to the ⊞ **> Calculator** screen.



Firmware Upgrade

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

Click **Choose file** to select the upgrade firmware from the local PC.



Upgrade-Basic

Firmware Version	49.30.10.50
Hardware Version	1.0
Upgrade	Choose file No file chosen

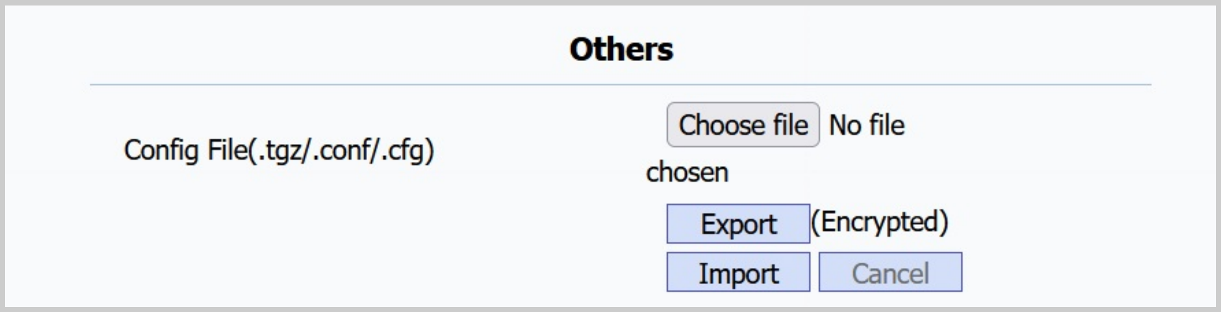
Note

- The upgrade file should be in .ZIP format.
- Click here to download the latest firmware and check changelog.

Backup

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

Navigate to the web **Upgrade > Advanced > Others** interface.



Others

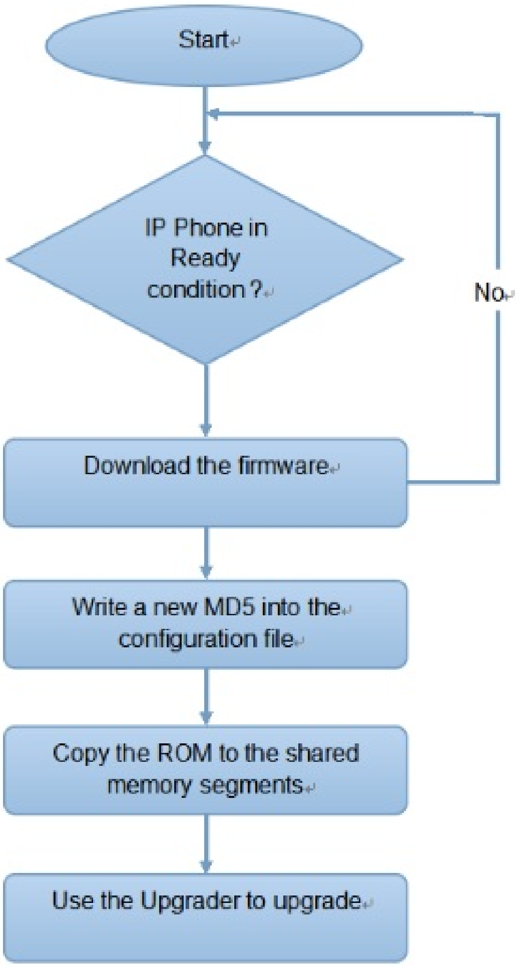
Config File(.tgz/.conf/.cfg) Choose file No file chosen

Auto-provisioning

Provisioning Principle

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

Please see the flow chart below:


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

Introduction to the Configuration Files

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

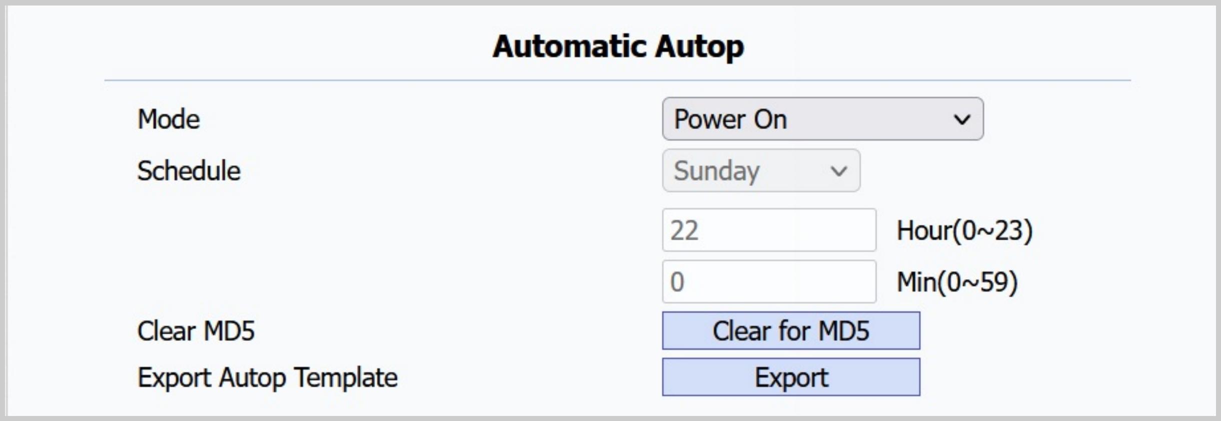
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

Autop Schedule

Akuvox provides you with different Autop methods that enable the device to perform provisioning for itself at a specific time according to your schedule.

Set it up on the **Upgrade > Advanced > Automatic Autop** interface.



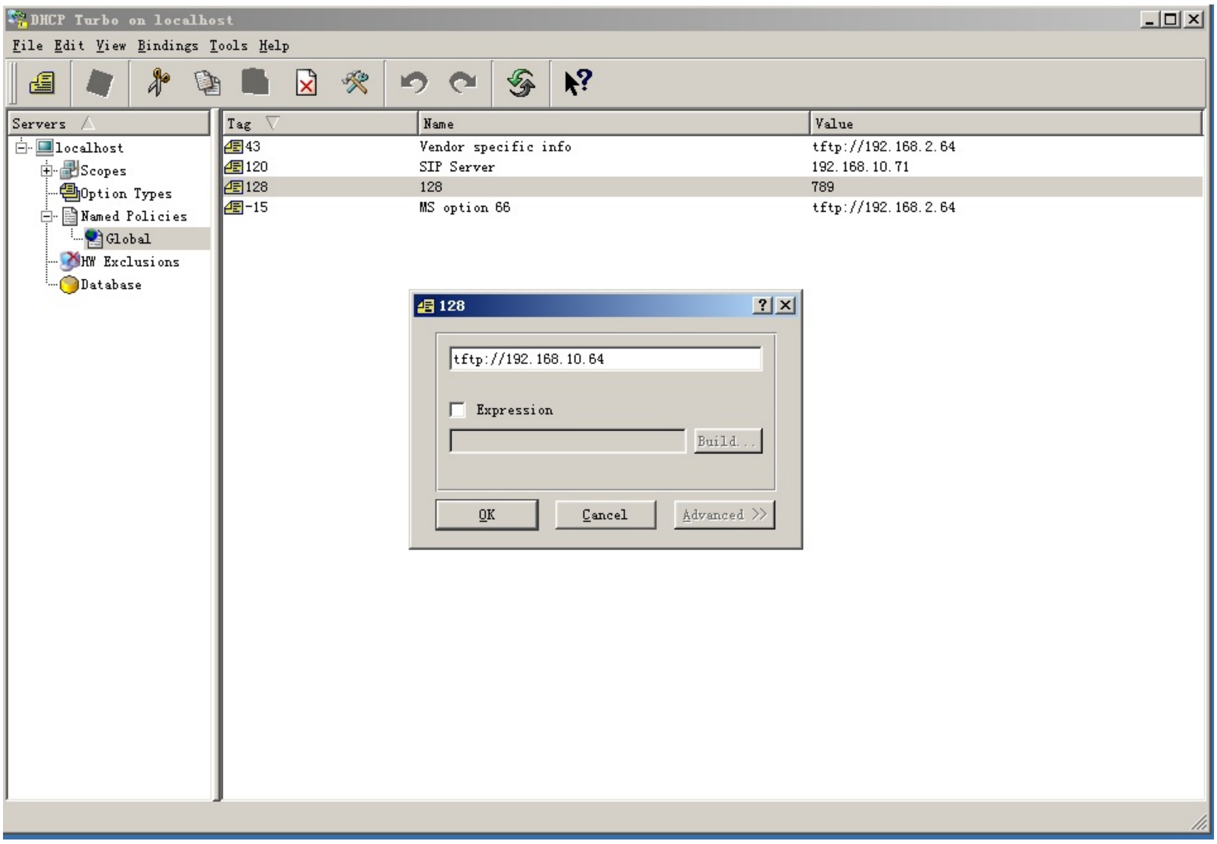
Automatic Autop

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

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

DHCP Provisioning

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.



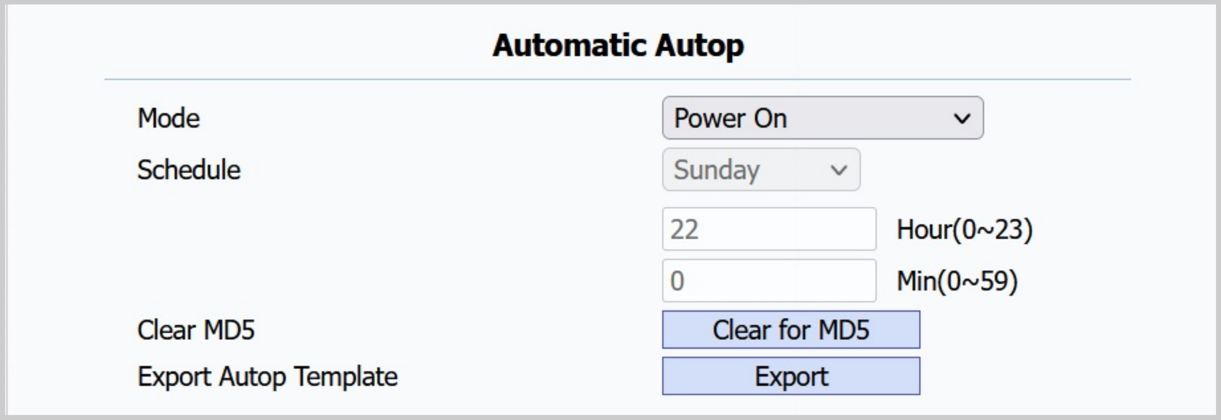
Tag	Name	Value
43	Vendor specific info	tftp://192.168.2.64
120	SIP Server	192.168.10.71
128	128	789
-15	MS option 66	tftp://192.168.2.64

tftp://192.168.10.64

Note

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

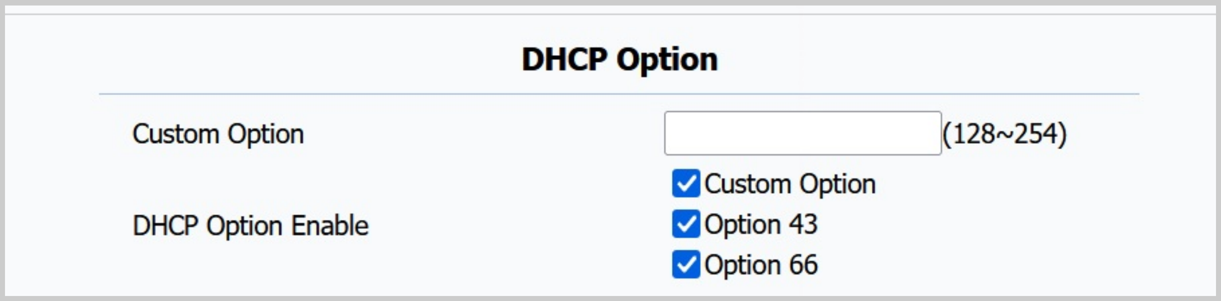
To set up DHCP Autop with **Power On** mode and export Autop Template to edit the configuration, navigate to the web **Upgrade > Advanced > Automatic Autop** interface.



Automatic Autop

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

Then set up the DHCP Option on **Upgrade > Advanced > DHCP Option** interface.



DHCP Option

Custom Option (128~254)

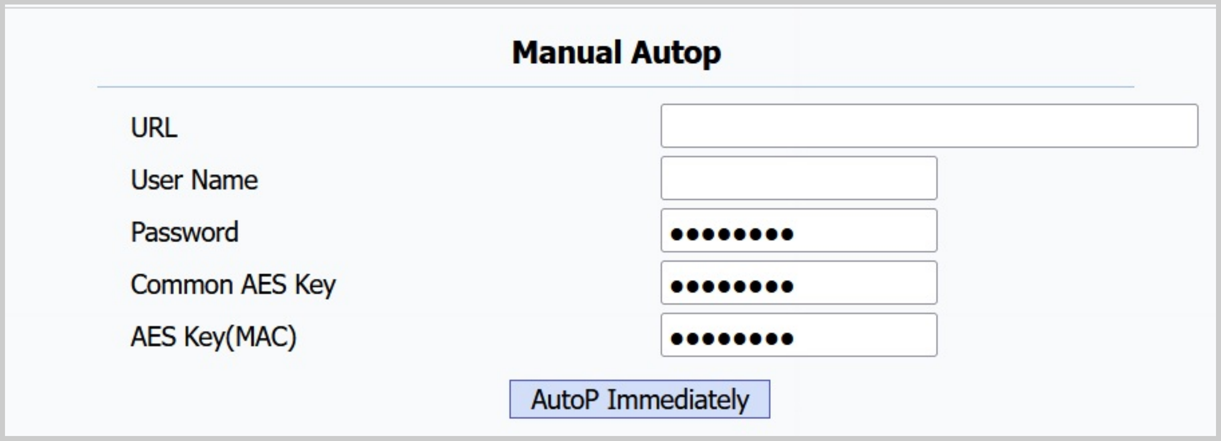
DHCP Option Enable ☑ Custom Option ☑ Option 43 ☑ Option 66

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

Static Provisioning

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

Download the template on **Upgrade > Advanced > Automatic Autop**, and set up the Autop server on **Upgrade > Advanced > Manual Autop**.



Manual Autop

URL	
User Name	
Password	●●●●●●●●
Common AES Key	●●●●●●●●
AES Key(MAC)	●●●●●●●●

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

Note

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

Tip

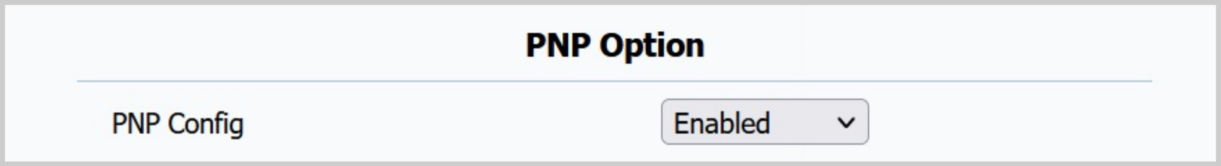
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

Click here to watch the configuration video.

Enable it on the **Upgrade > Advanced > PNP Option** interface.



PNP Option

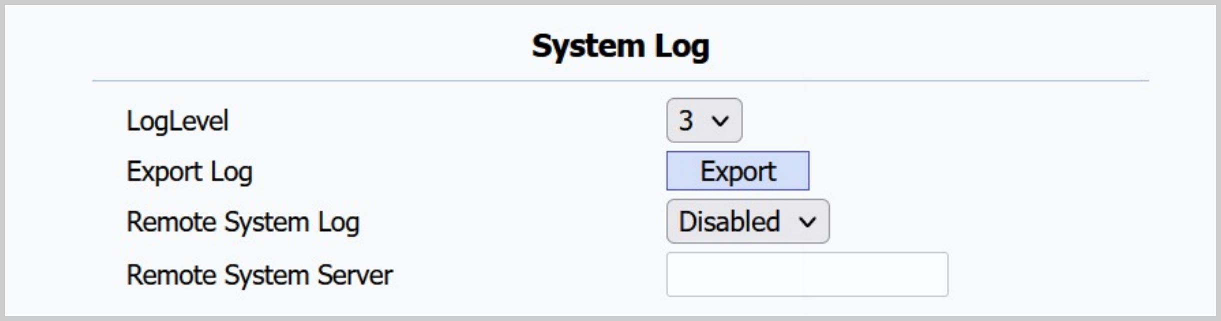
PNP Config: Enabled

Debug

System Log for Debugging

System logs can be used for debugging purposes.

Set it up on the **Upgrade > Advanced > System Log** interface.



System Log

LogLevel: 3

Export Log: Export

Remote System Log: Disabled

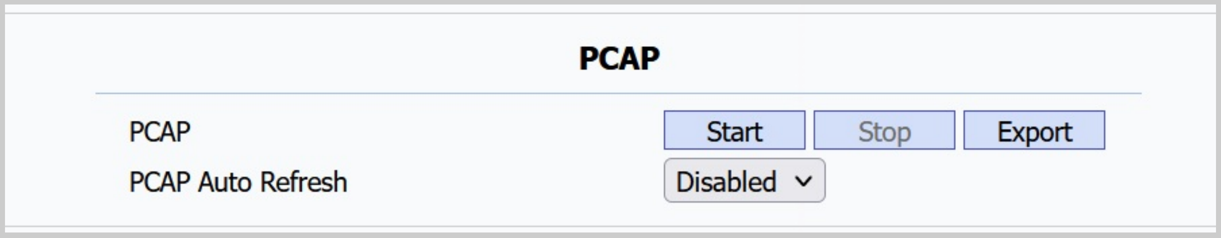
Remote System Server:

- **Log Level**: Log level ranges from 1 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is **3**. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Server**: The remote server address to receive the system log. It will be provided by Akuvox technical support.

PCAP for Debugging

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

Set it up on the **Upgrade > Advanced > PCAP** interface.



PCAP

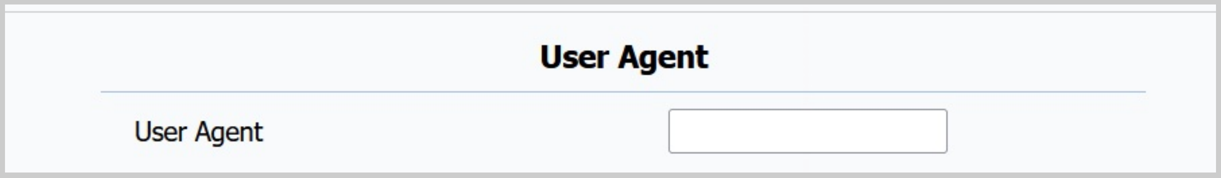
PCAP Auto Refresh: Disabled

- **PCAP**: Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: When enabled, the PCAP will continue to capture data packets even after the data packets reach 50M maximum in capacity. When disabled, the PCAP will stop data packet capturing when the data packets reach the maximum capturing capacity of 1MB.

User Agent

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

Set it up on the **Account > Advanced > User Agent** interface.



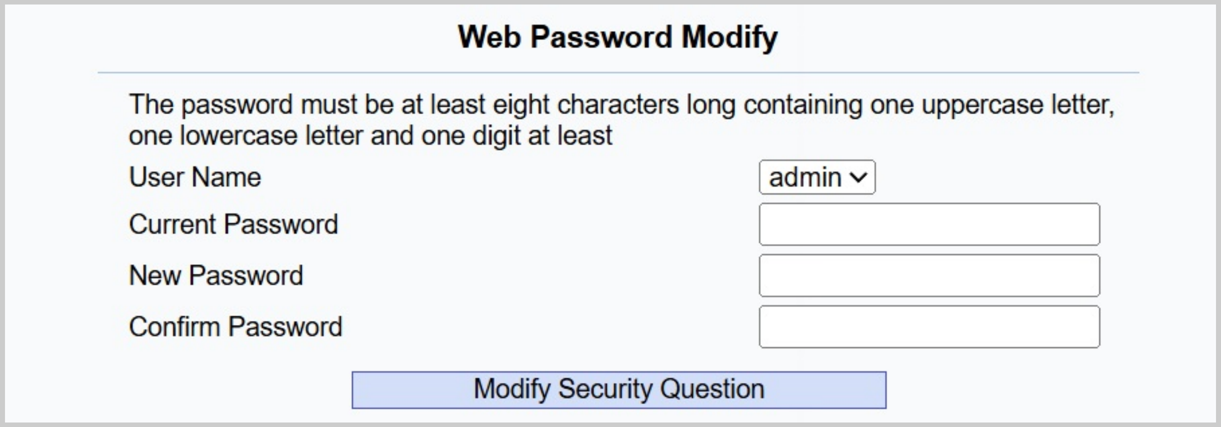
User Agent

User Agent

Password Modification

Modify Device Web Interface Password

Navigate to the web **Security > Basic > Web Password Modify** interface. Select **admin** or **user** to modify web passwords for the desired role.



Web Password Modify

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

User Name	admin
Current Password	
New Password	
Confirm Password	

Note

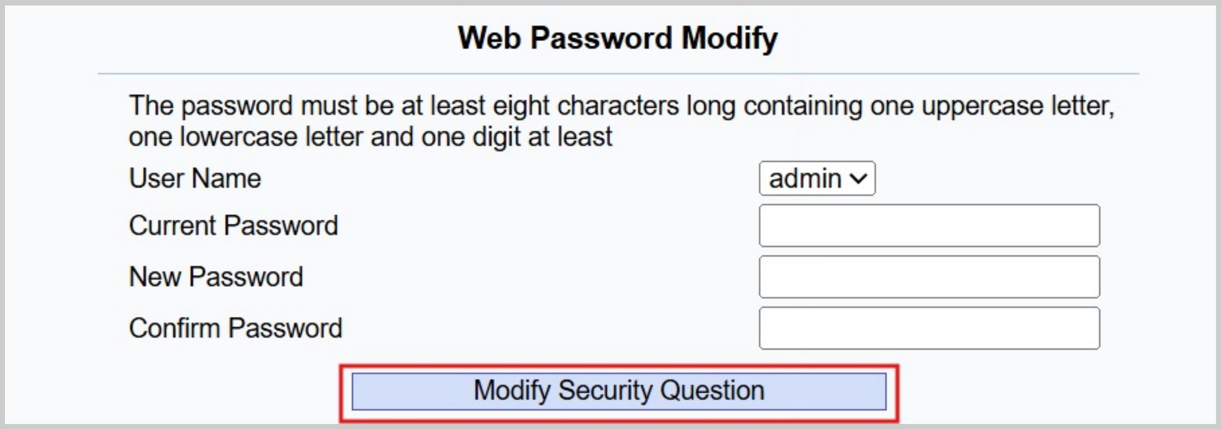
There are two accounts, one is admin, its password is admin, the other is user, and its password is user.

Modify Security Questions

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

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

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

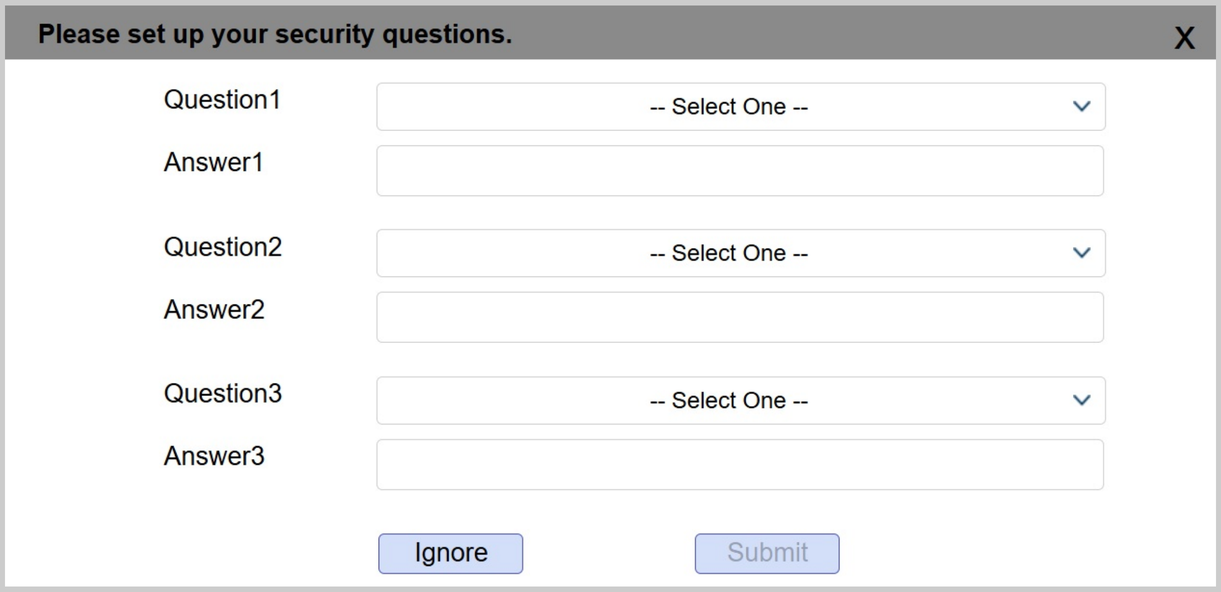


Web Password Modify

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

User Name	admin
Current Password	
New Password	
Confirm Password	

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



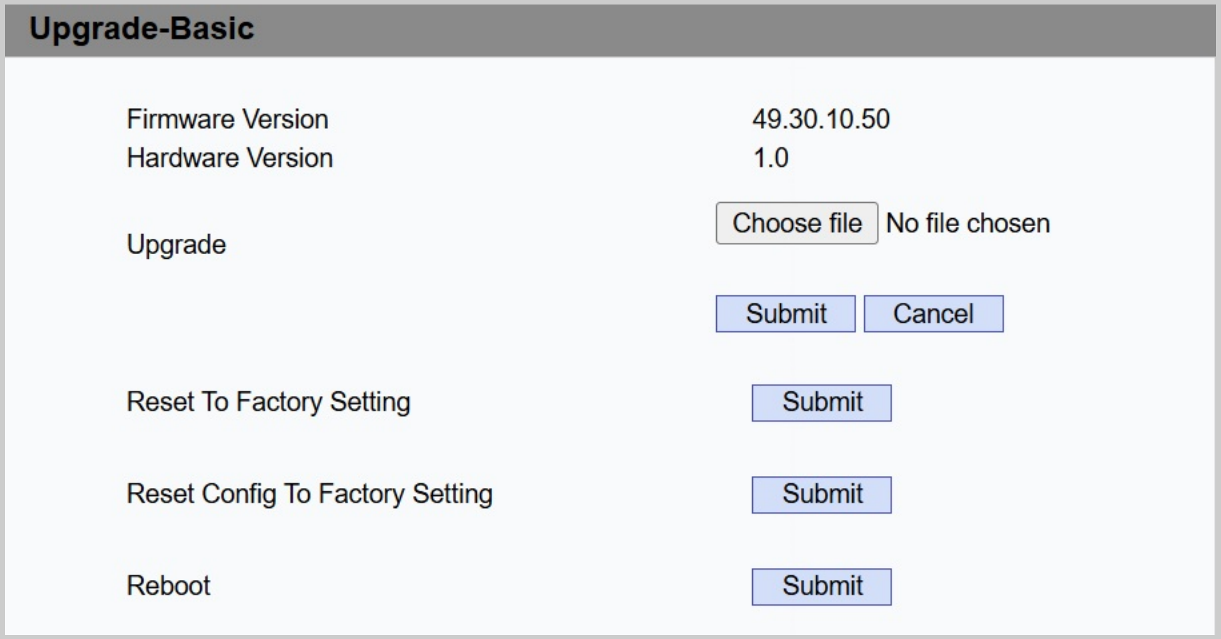
Please set up your security questions.

Question1	-- Select One --
Answer1	
Question2	-- Select One --
Answer2	
Question3	-- Select One --
Answer3	

System Reboot & Reset

Reboot

Navigate to the web **Upgrade > Basic** interface. Click **Reboot**.

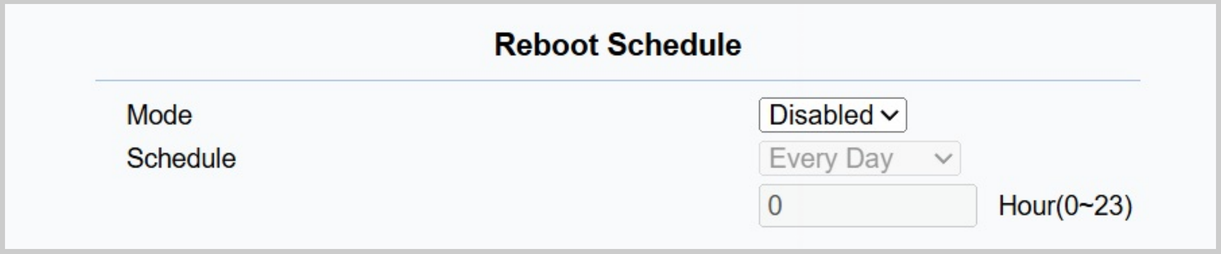


Upgrade-Basic

Firmware Version	49.30.10.50
Hardware Version	1.0
Upgrade	Choose file No file chosen Submit Cancel
Reset To Factory Setting	Submit
Reset Config To Factory Setting	Submit
Reboot	Submit

You can set up a schedule for the device to be restarted.

Navigate to the web **Upgrade > Advanced > Reboot Schedule** interface.



Reboot Schedule

Mode	Disabled
Schedule	Every Day 0 Hour(0~23)

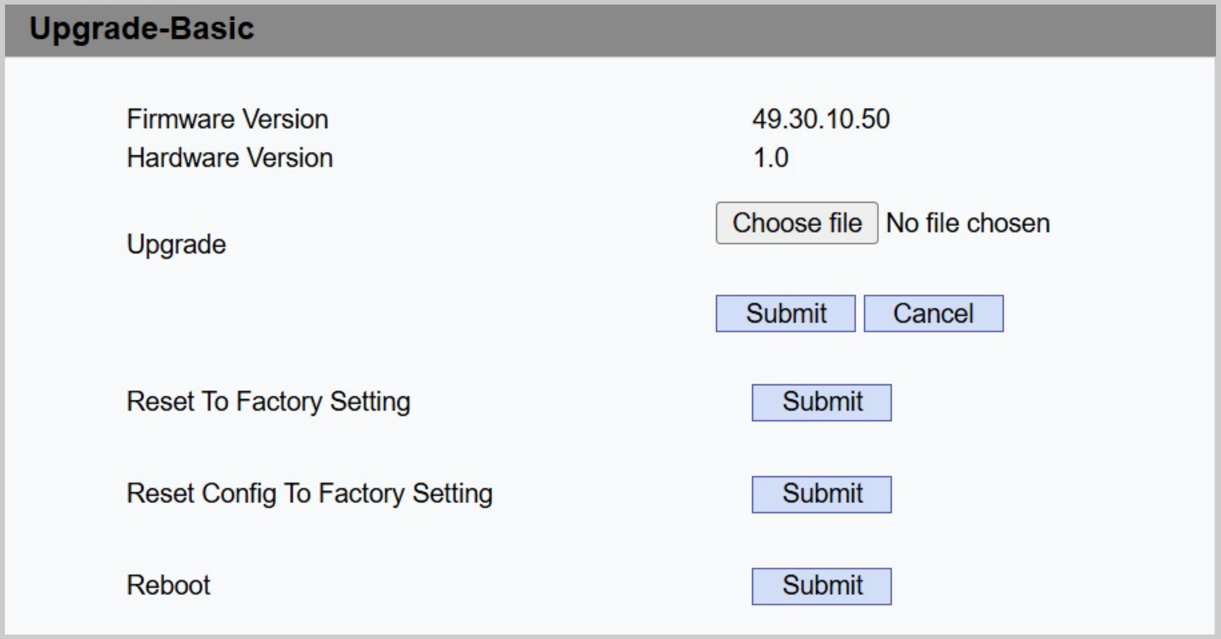
Reset

Reset the device on the **Upgrade > Basic** interface.

The device provides two reset options:

- **Reset to Factory Setting**: Reset all data to the factory default.

- **Reset Config To Factory Setting**: Retain the user data, such as schedules and call logs.

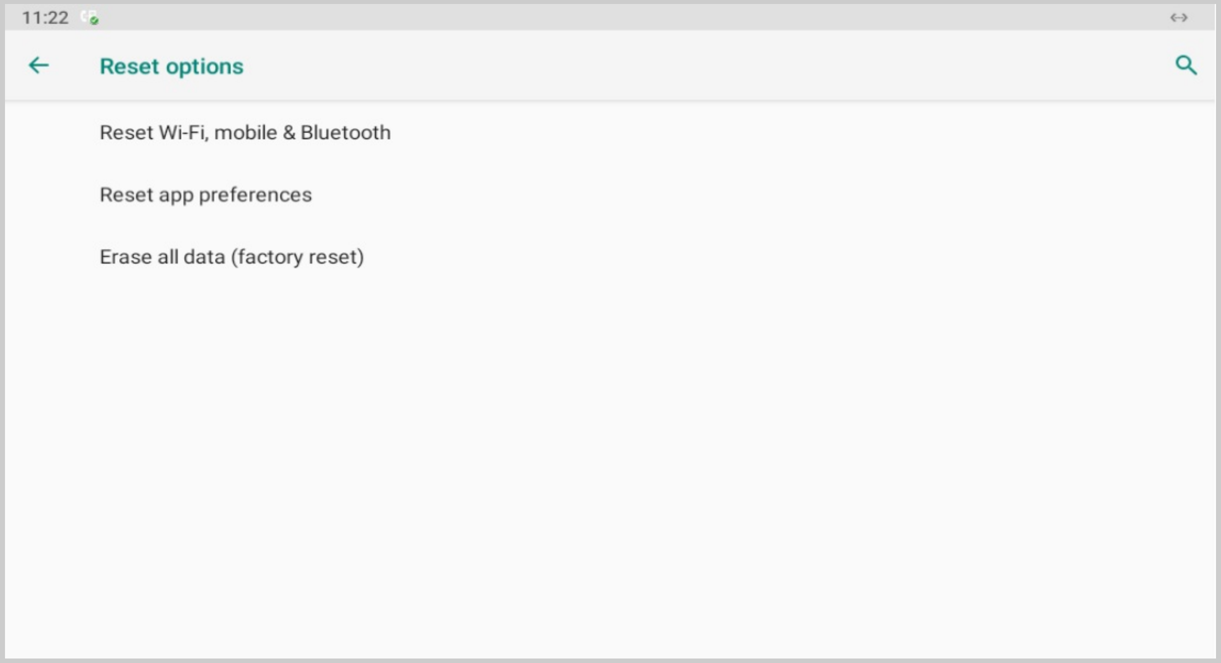


Upgrade-Basic

Firmware Version	49.30.10.50
Hardware Version	1.0
Upgrade	Choose file No file chosen Submit Cancel
Reset To Factory Setting	Submit
Reset Config To Factory Setting	Submit
Reboot	Submit

The device can also be reset directly on the screen.

Tap ⊞ **> Settings > System > Reset options.**



11:22

Reset options

Reset Wi-Fi, mobile & Bluetooth

Reset app preferences

Erase all data (factory reset)