

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



AKUVOX S565 INDOOR MONITOR

Administrator Guide

Thank you for choosing the Akuvox S565 series indoor monitor. This manual is intended for administrators who need to configure the indoor monitor. This manual is written based on firmware version 565.30.10.27, and it provides all the configurations for the functions and features of the S565 series indoor monitor. Please visit the Akuvox forum or consult technical support for any new information or the latest firmware.

Product Overview

- 10"touch screen with 1280x800 resolution
- Stylish industrial design
- Two-way audio communication
- Built-in Wi-Fi(Optional)
- Comply with SIP standard for easy integration with SIP-capable PBXes
- Eight-channel inputs and one built-in relay
- Powered by PoE or external source
- Support US or European electrical wall box mounting
- Desk mount available

Model Specification

Resolution	1280 x 800
Indicator	x1
MIC	x2
Speaker	x1
Wi-Fi (S565W)	802.11b/g/n/ac
Bluetooth	4.0 and above
Ethernet	2 x RJ45
Power Supply	PoE 802.3af or 12VDC/1A
Alarm Input	x8
Door Bell Input	x1
Relay	x1, 30V 2A
RS485	✓
Wiegand Input	X
NFC	X
Reset Button	X
Alarm Zone	8

Introduction to Configuration Menu

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

Akuvox | **S565**

 Homepage

 Status

 Account



 Network



 Device



 Contacts



 Upgrade



 Security



 Settings



 Arming



Breathing Light Status

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



See the indicator light status below:

Status	Color	Light	Description
System status	Blue	ON	The system is working
Power up	White	ON	The system is powered
System booting	Blue	ON	The device is booting
Network	Red	Flashing	Failed to obtain the IP address
Incoming Call	Blue	Flashing	Receiving an incoming call
End a call	Blue	ON	End a call
Screen/System	N/A	OFF	The screen is turned off The device is turned off
Alarm	Red	Flashing	An alarm is triggered
Doorbell	Blue	Flashing	Doorbell is ringing
Upgrade/Reset	Red	Flashing	Upgrading the device Reset the device to the factory setting

Note

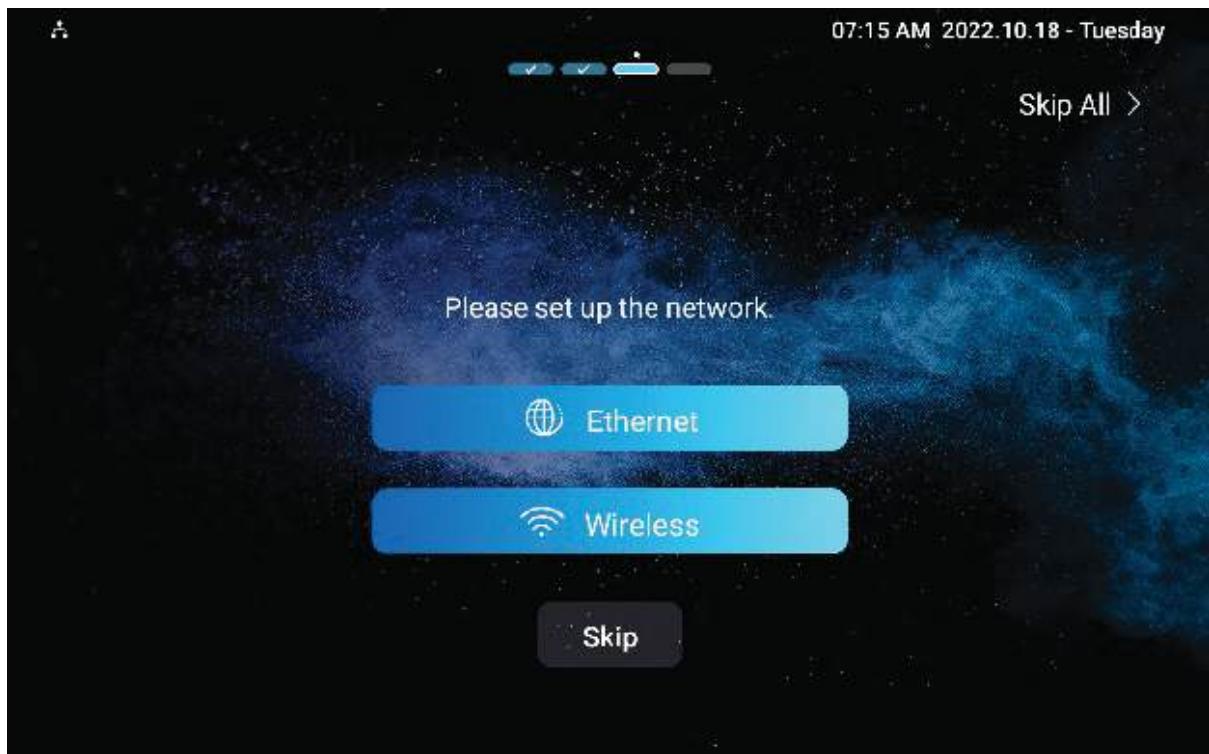
The alarm status light has the highest priority.

Access the Device

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

Device Start-up Network Selection

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

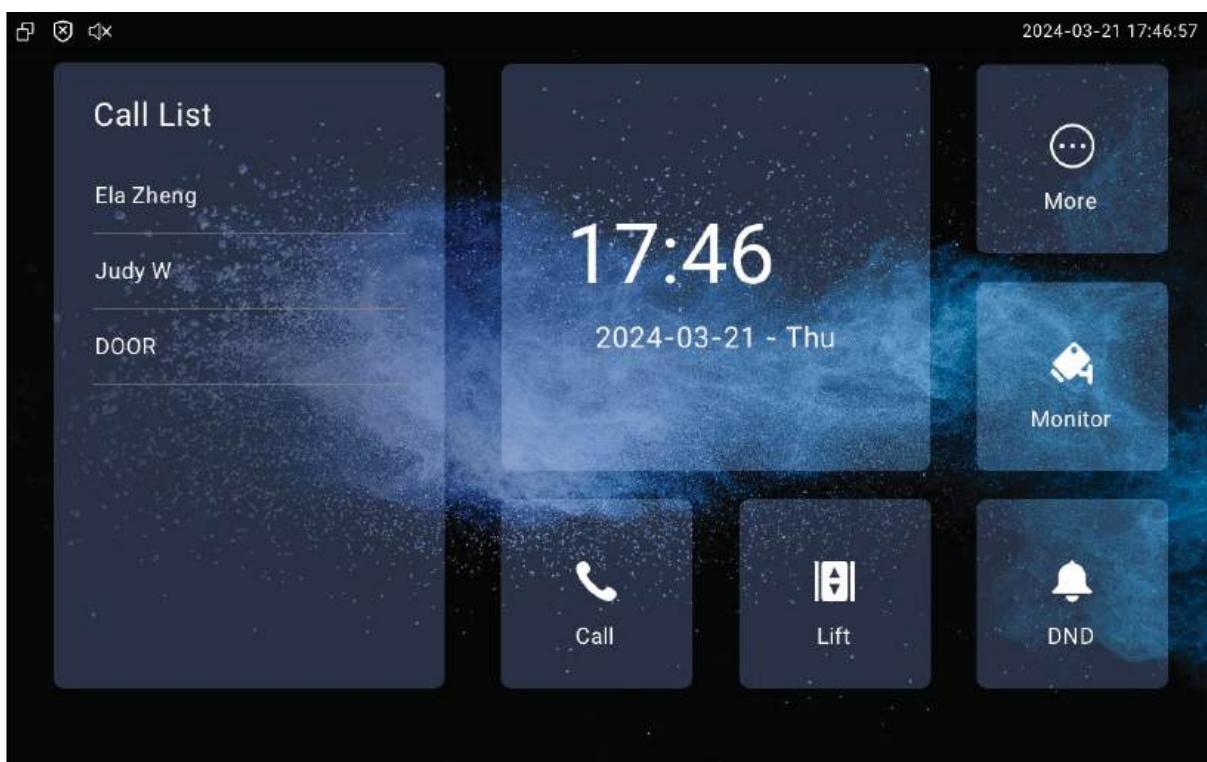
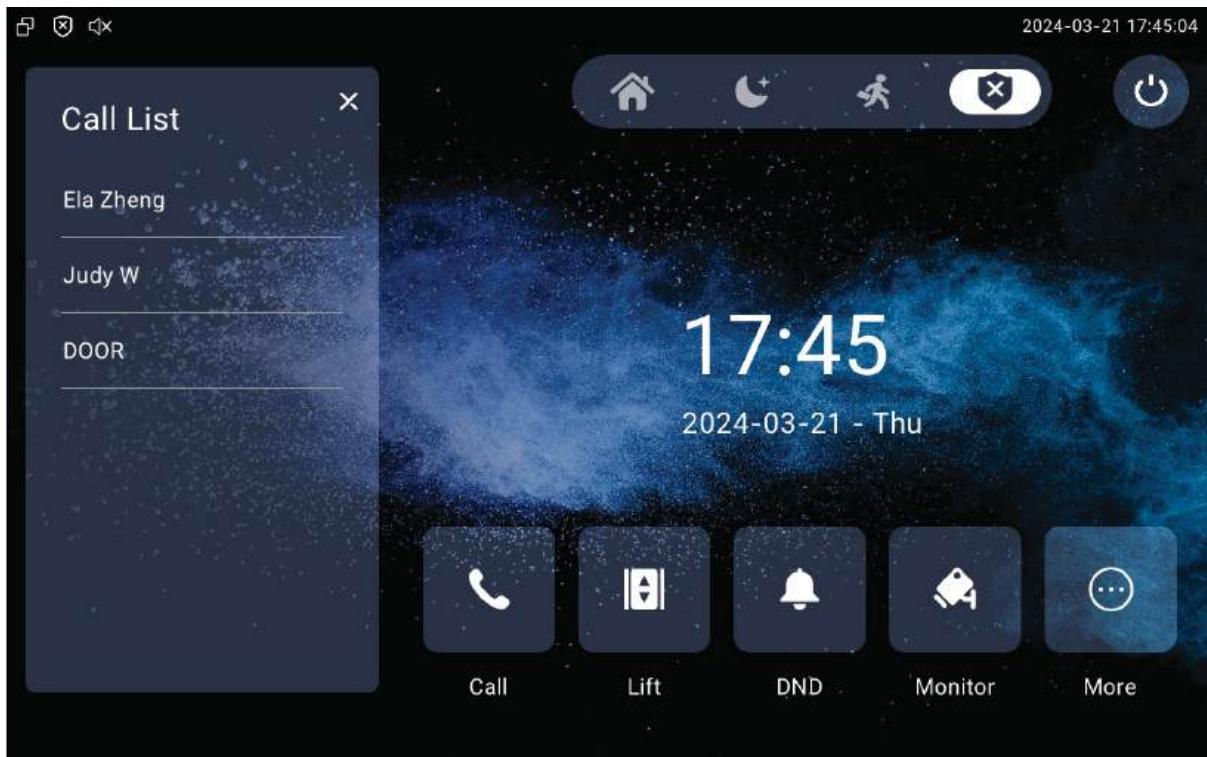


Note

Please refer to [Network Setting & Other Connection](#) for the configuration of the Ethernet and wireless network connection.

Device Home Screen Type Selection

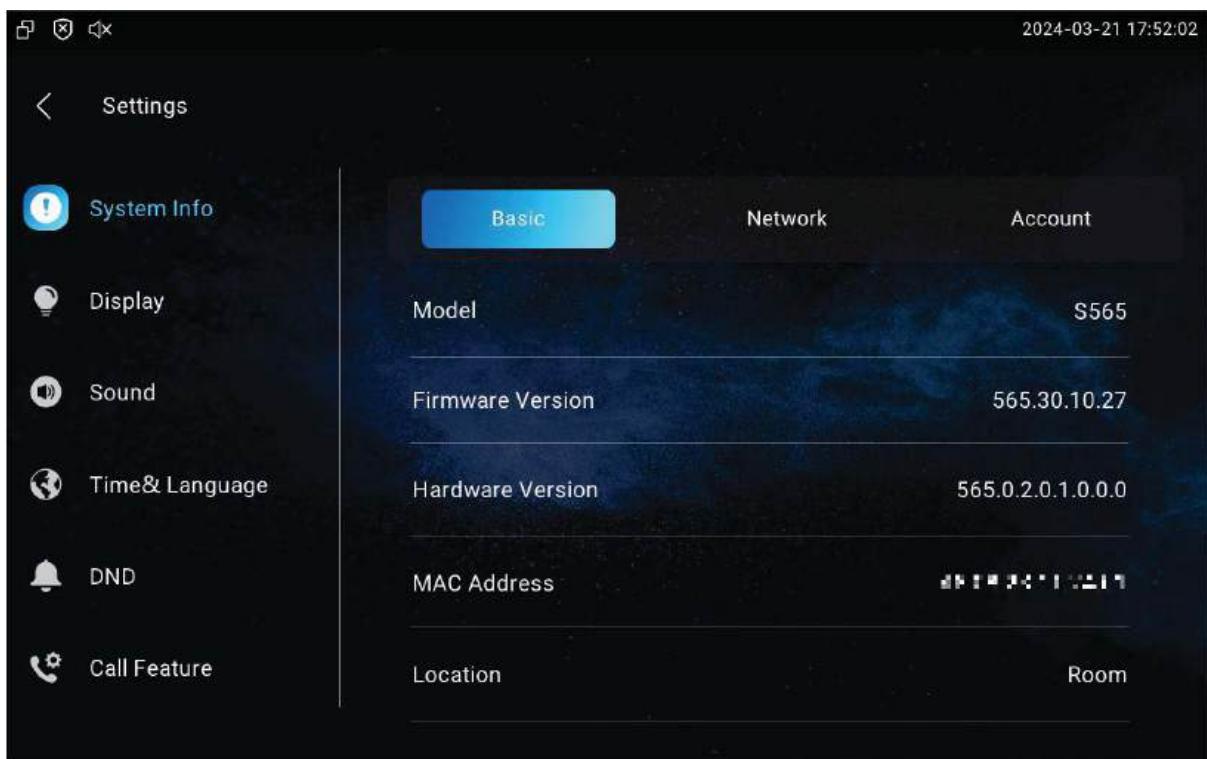
Akuvox indoor monitor supports two different home screen display modes: **Call list simple**, **Classic**. Choose one suitable mode for your scenarios.



Access the Device Settings on the Device

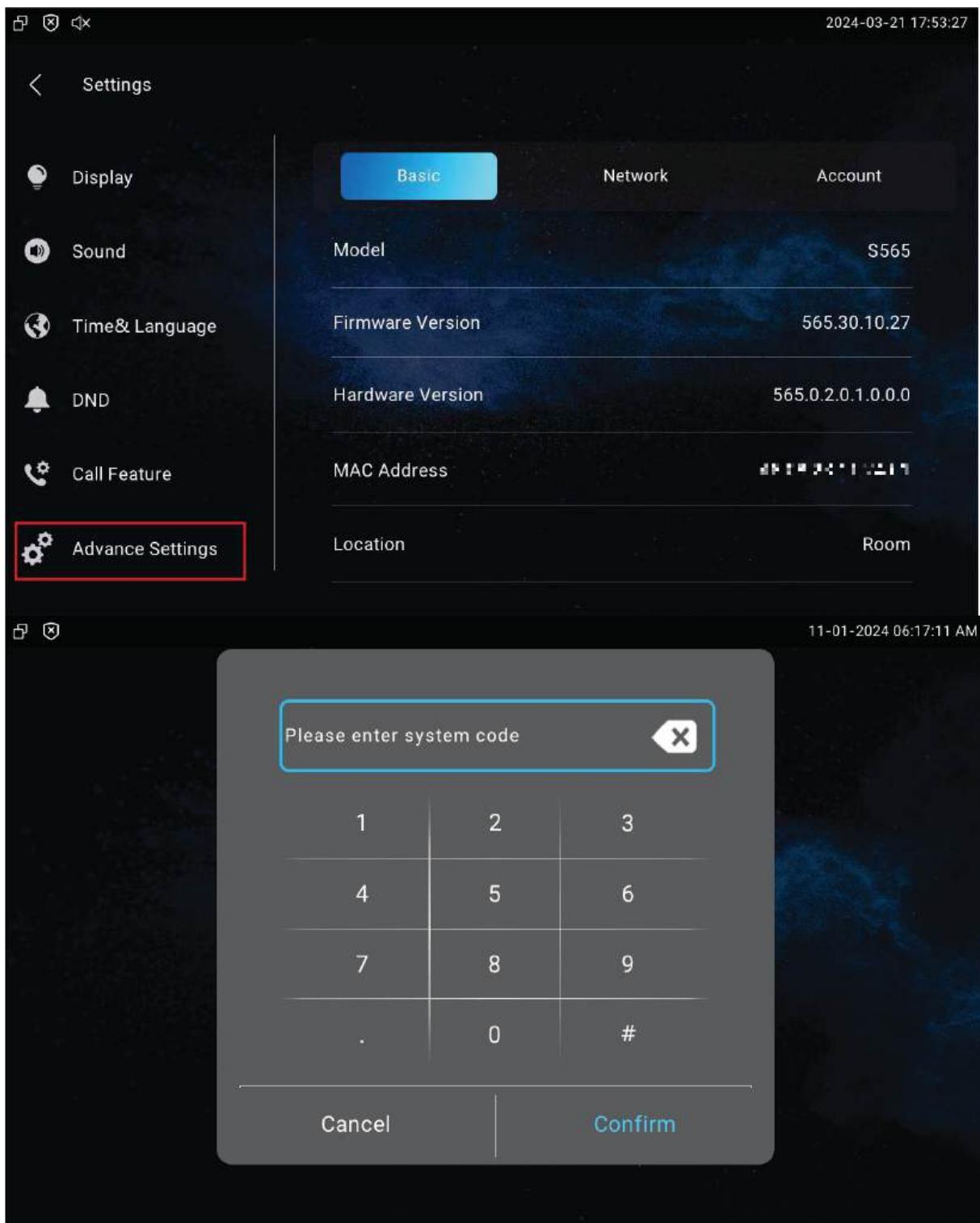
Access Device Basic Settings

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



Access Device Advance Settings

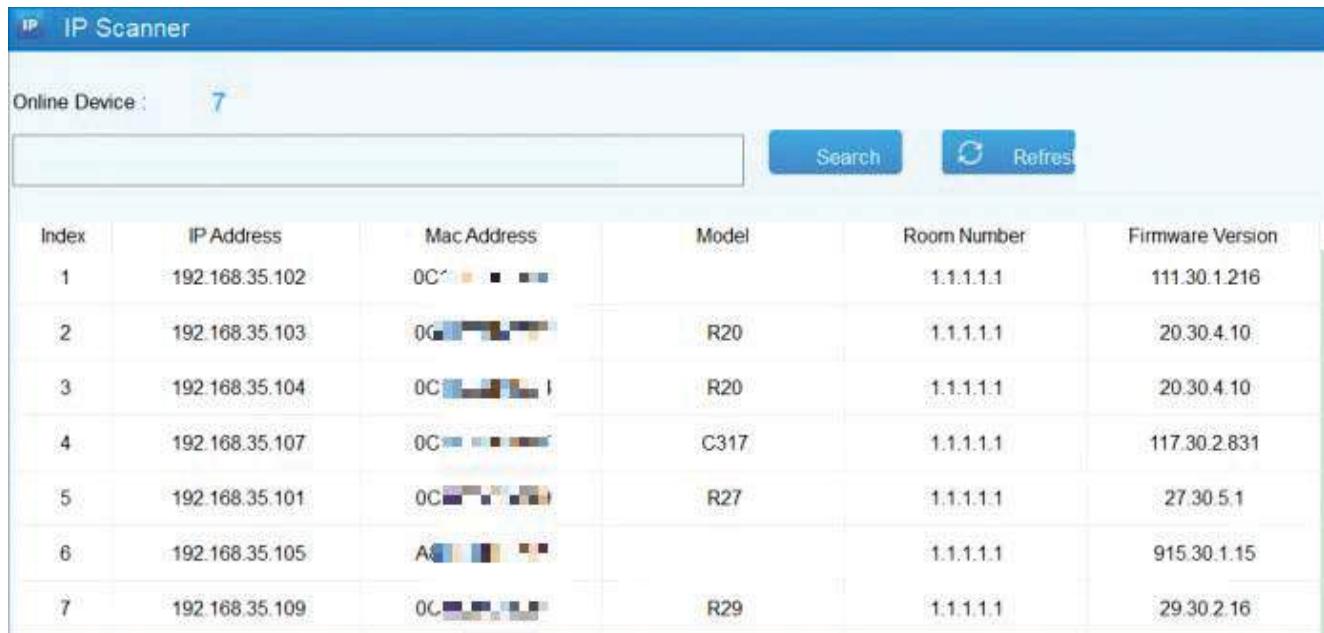
To access the advanced settings, press  and then tap the **Advance Settings**. Press the default password 123456 to enter the advanced settings.



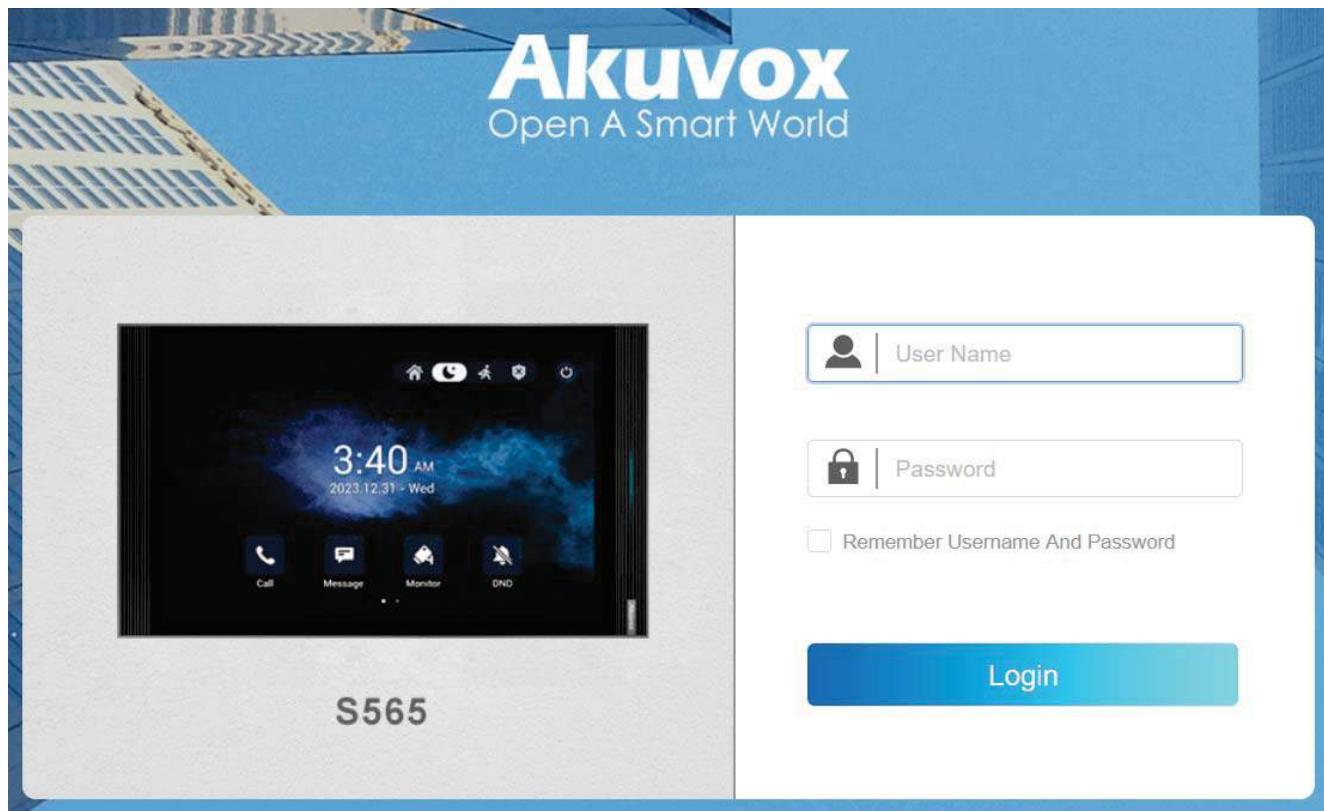
Access the Device Settings on the Web Interface

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

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



Index	IP Address	Mac Address	Model	Room Number	Firmware Version
1	192.168.35.102	0C:xx:xx:xx:xx:xx		1.1.1.1.1	111.30.1.216
2	192.168.35.103	06:xx:xx:xx:xx:xx	R20	1.1.1.1.1	20.30.4.10
3	192.168.35.104	0C:xx:xx:xx:xx:xx	R20	1.1.1.1.1	20.30.4.10
4	192.168.35.107	0C:xx:xx:xx:xx:xx	C317	1.1.1.1.1	117.30.2.831
5	192.168.35.101	0C:xx:xx:xx:xx:xx	R27	1.1.1.1.1	27.30.5.1
6	192.168.35.105	A:xx:xx:xx:xx:xx		1.1.1.1.1	915.30.1.15
7	192.168.35.109	0C:xx:xx:xx:xx:xx	R29	1.1.1.1.1	29.30.2.16



Note

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

Language and Time Setting

Language Setting

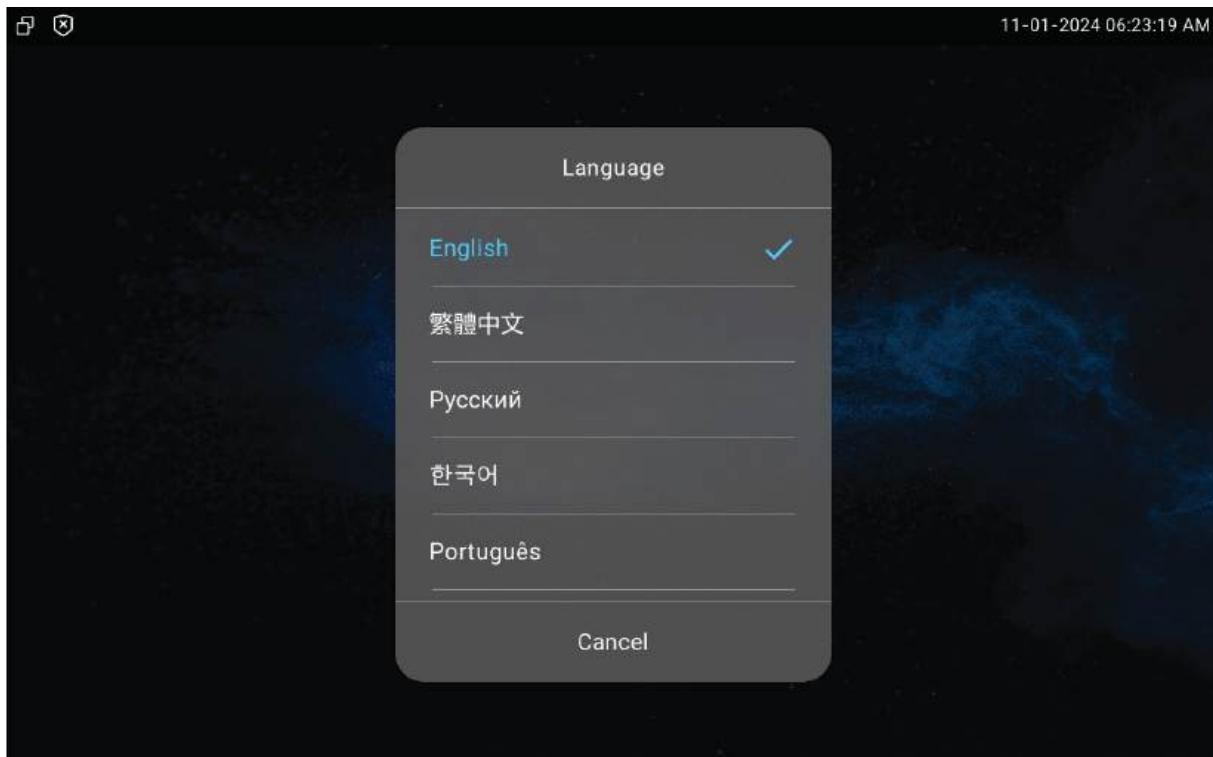
Set up the language during initial device setup or later through the device or web interface according to your preference.

Language Setting on the Device

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

The following languages are supported:

English, Traditional Chinese, Russian, Korean, Portuguese, Spanish, Italian, Dutch, French, German, Hebrew, Turkish, Polish, Japanese, Slovak, Simplified Chinese, Norwegian, Vietnamese, Lithuanian, Czech, and Ukrainian.



Language Setting on the Web Interface

You can switch the web language in the upper right corner.

The following languages are supported:

English, Simplified Chinese, Traditional Chinese, Russian, Portuguese, Spanish, Italian, Dutch, French, German, Polish, and Japanese.



Time Setting

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

Time Setting on the Device Web Interface

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

To set it up, navigate to the web **Device > Time** interface.

Time Setting	
Automatic Date&Time	<input checked="" type="checkbox"/>
Time Format	12-Hour-Format
Date Format	DD-MM-YYYY
Date	11-01-2024
Time	6:41 am
Time Zone	London
NTP	
Preferred Server	0.pool.ntp.org
Alternate Server	1.pool.ntp.org
Update Interval	3600 (>=3600Sec)

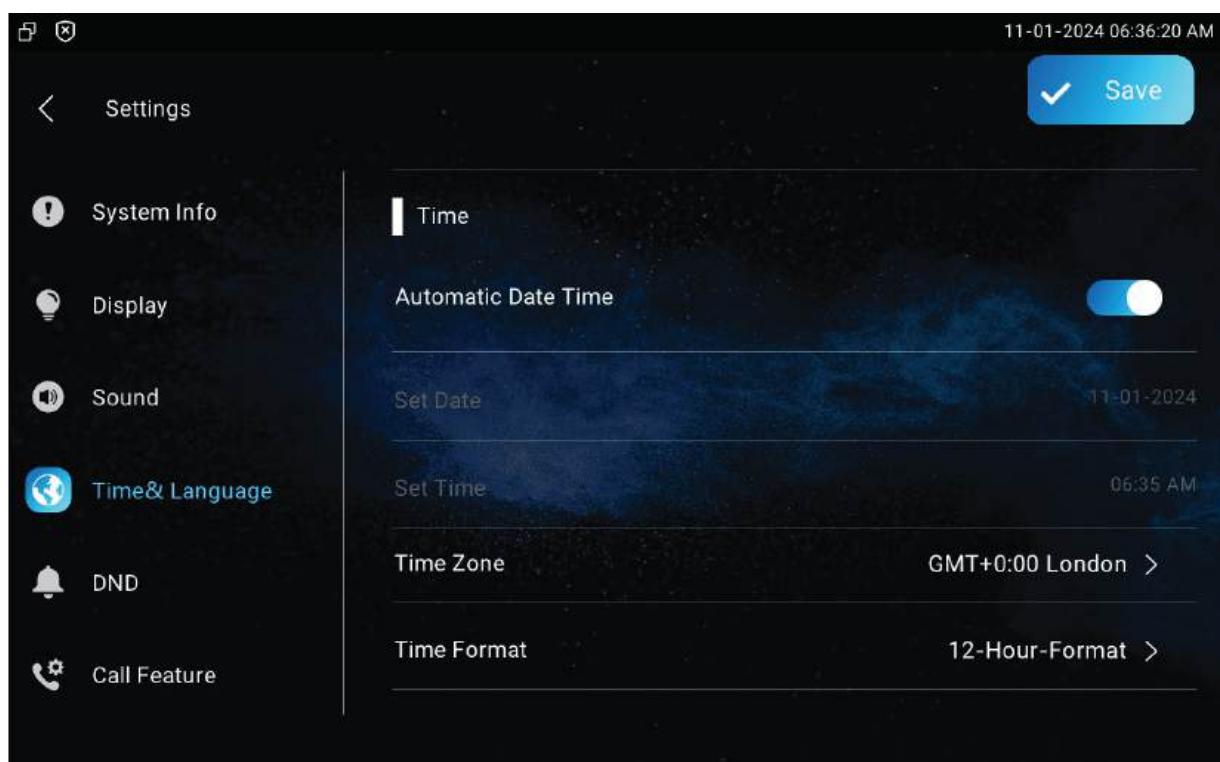
- **Automatic Date & Time:** The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time

Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.

- **Time Format:** 12-hour or 24-hour time format.
- **Date Format:** Select the date format among YYYY/MM/DD, DD-MM-YYYY, DD/MM/YYYY, WW-DD-MM, WW-MM-DD, YYYY-MM-DD, MM-DD-YYYY, MM/DD/YYYY, and WW DD/MM/YYYY.
- **Time Zone:** Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Preferred Server:** The NTP server address.
- **Alternate Server:** The backup server address. When the main NTP server fails, it will change to the backup server automatically.
- **Update Interval:** The time interval that the device sends the request to the NTP server for the time update automatically.

Time Setting on the Device

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



- **Automatic Date Time:** The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date, then enter the time and date and press **Save** to save the setting.
- **Time Zone:** Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Time Format:** The 12-hour or 24-hour time format.
- **Date Format:** Select the date format among YYYY/MM/DD, DD-MM-YYYY, DD/MM/YYYY, WW-DD-MM, WW-MM-DD, YYYY-MM-DD, MM-DD-YYYY, MM/DD/YYYY, and WW DD/MM/YYYY.
- **NTP Server:** The NTP server address. NTP Server 2 is the backup.

Daylight Saving Time

Daylight Saving Time is the practice of advancing clocks (typically by one hour) during warmer months so that darkness falls at a later clock time. You can modify the time parameters to achieve longer evenings or daytime, especially in summer.

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

Daylight Saving Time

Daylight Saving Time Enabled	<input type="button" value="Auto"/>						
OffSet	<input type="button" value="60"/> (-300~300Minutes)						
Update Interval	<input type="button" value="By Date"/>						
Start Time	<table><tr><td>1</td><td>Mon (1~12)</td></tr><tr><td>1</td><td>Day (1~31)</td></tr><tr><td>0</td><td>Hour (0~23)</td></tr></table>	1	Mon (1~12)	1	Day (1~31)	0	Hour (0~23)
1	Mon (1~12)						
1	Day (1~31)						
0	Hour (0~23)						
End Time	<table><tr><td>12</td><td>Mon (1~12)</td></tr><tr><td>31</td><td>Day (1~31)</td></tr><tr><td>23</td><td>Hour (0~23)</td></tr></table>	12	Mon (1~12)	31	Day (1~31)	23	Hour (0~23)
12	Mon (1~12)						
31	Day (1~31)						
23	Hour (0~23)						

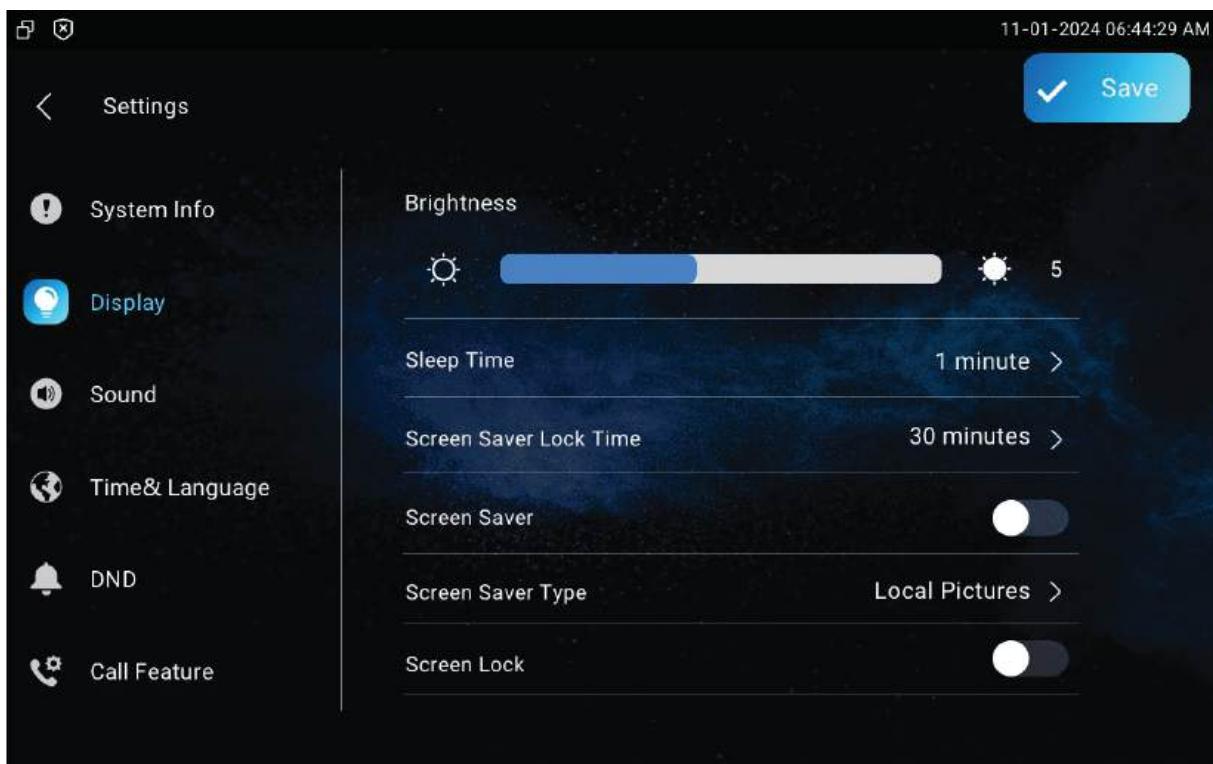
- **Daylight Saving Time Enabled:** Enable or disable daylight saving time. You can also configure it to make the device adjust the daylight saving time automatically.
- **OffSet:** 60 minutes as default, setting the clocks an hour ahead of the standard time.
- **Update Interval:**
 - **By Date** sets the date schedule for daylight saving time.
 - **By Week** sets the schedule for daylight saving time according to the week and month.

Screen Display Configuration

Screen Display Setting on the Device

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

To set it up, navigate to the device **Settings > Display** screen.



- **Brightness:** Move the blue bar to adjust the screen brightness. The default brightness is 5.
- **Sleep Time:** Set the sleep timing based on the screen saver (15 sec to 30 min).
 - If the screen saver is enabled, then the sleep time is the screen saver start time. For example, if you set it as 1 minute, then the screen saver will start automatically when the device has no operation for 1 minute.

- If the screen saver is disabled, then the sleep time is the screen turn-off time. For example, if you set it as 1 minute, then the screen will

be turned off automatically when the device has no operation for 1 minute.

- **Screen Saver Lock Time:** Set the screen saver start time from 15 seconds up to 2 hours.
- **Screen Saver Type:** Local Pictures display pictures uploaded to the indoor monitor as the screen saver.
- **Screen Lock:** The screen lock will lock the screen after the screen turns off. You are required to enter the system code to unlock the screen.

Note

The default password is empty. Tap the ✓ icon on the lock screen to enter the system.

- **Screen Clean:** It allows users to wipe the screen clean without triggering unwanted changes in the settings.
- **Wallpaper:** It is for local wallpaper selection.

Screen Display Setting on the Web Interface

Upload Screen Saver

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

To set it up, navigate to the web **Device > Display Setting > Screen Saver Setting** interface.



- **Screen Saver Type:** Local Pictures display pictures uploaded to the indoor monitor as the screen saver.

Note

- Max size:256K; Format:1280x800 jpg; File name can only contain digits, letters and_.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurs.

Upload Wall Paper

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

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



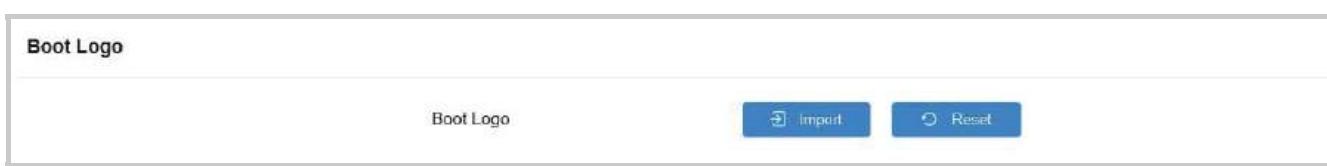
Note

Max size:256K; Format:1280x800 jpg; File name can only contain digits, letters and_.

Upload Device Booting Image

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

To set it up, navigate to the web **Device > Display Setting > Boot Logo** interface.



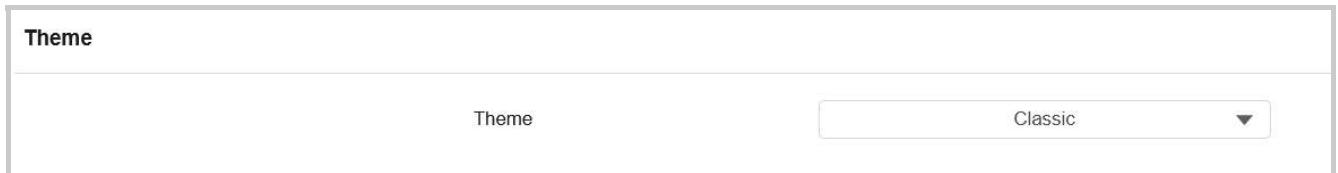
Note

Max size:100K; Format:1280*800 jpg; File name can only contain digits, letters and_.

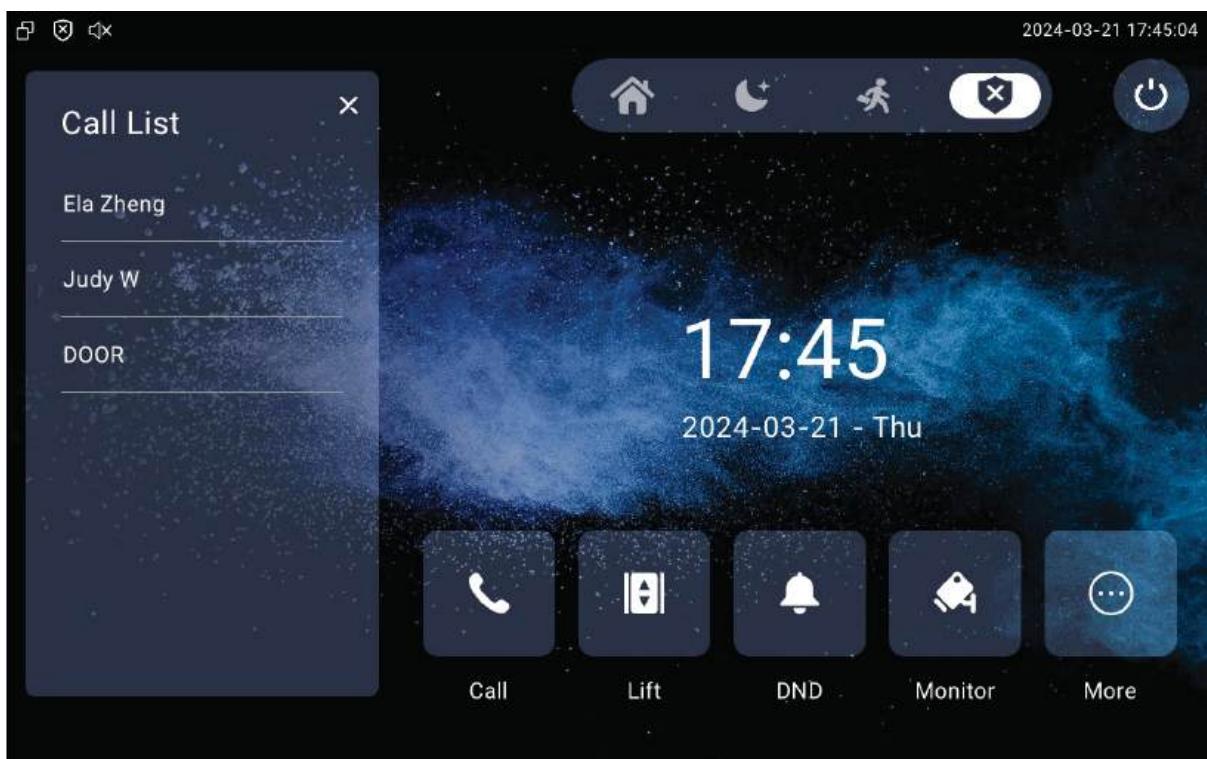
Home Screen Display

You can select the classic or call list simple theme for the home screen display.

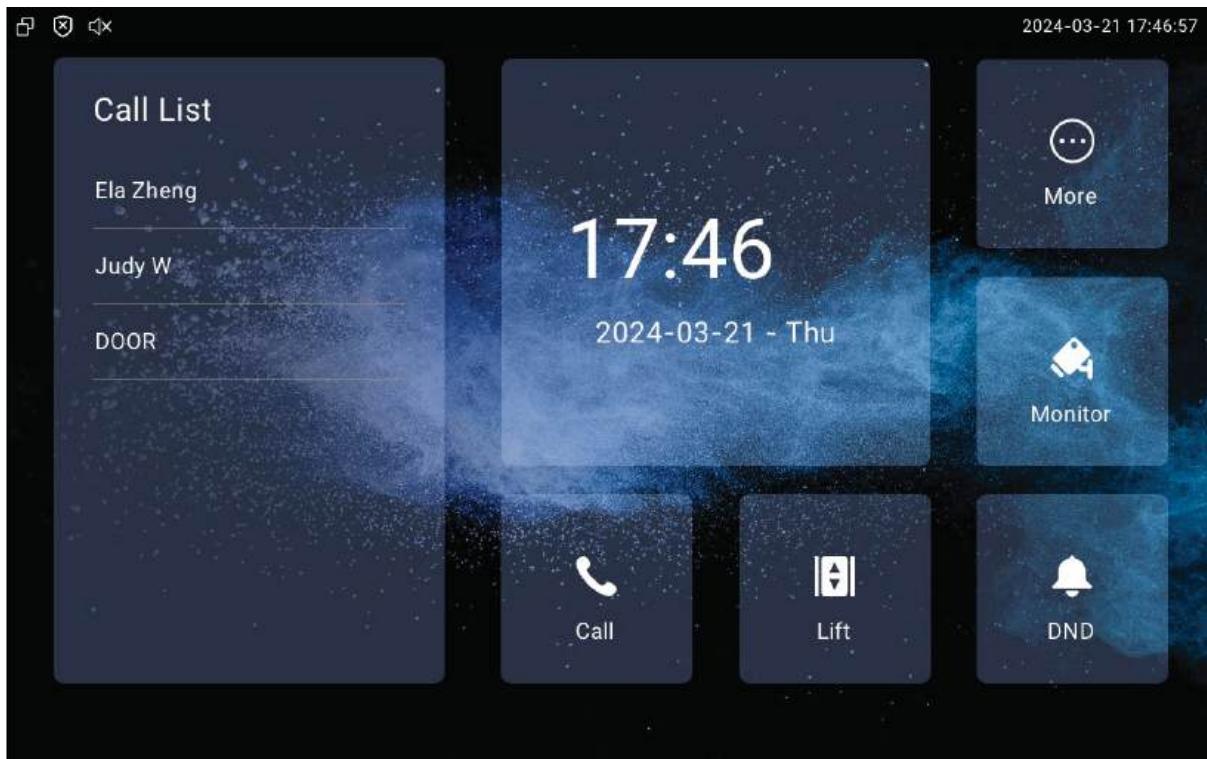
To set it up, go to the web **Device > Display Setting > Theme** interface.



Classic:



Call list simple:



Icon Screen Display Configuration

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

To set it up, navigate to the web **Device > Display Setting > Home Page Display** interface.

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

- Type:** Select the functional icon to be put on the home screen, DND, Message, Contacts, Call, Arming, SOS, Settings, Sound, Display, Status, Relay, Lift, Unlock, Smart Living, Capture Log, Monitor, or All Call.
- Label:** Rename the icon if needed. The DND icon cannot be renamed.
- Icons:** Click to upload the icon picture. The maximum icon size is **100*100**. The picture format can be JPG, JPEG, and PNG.

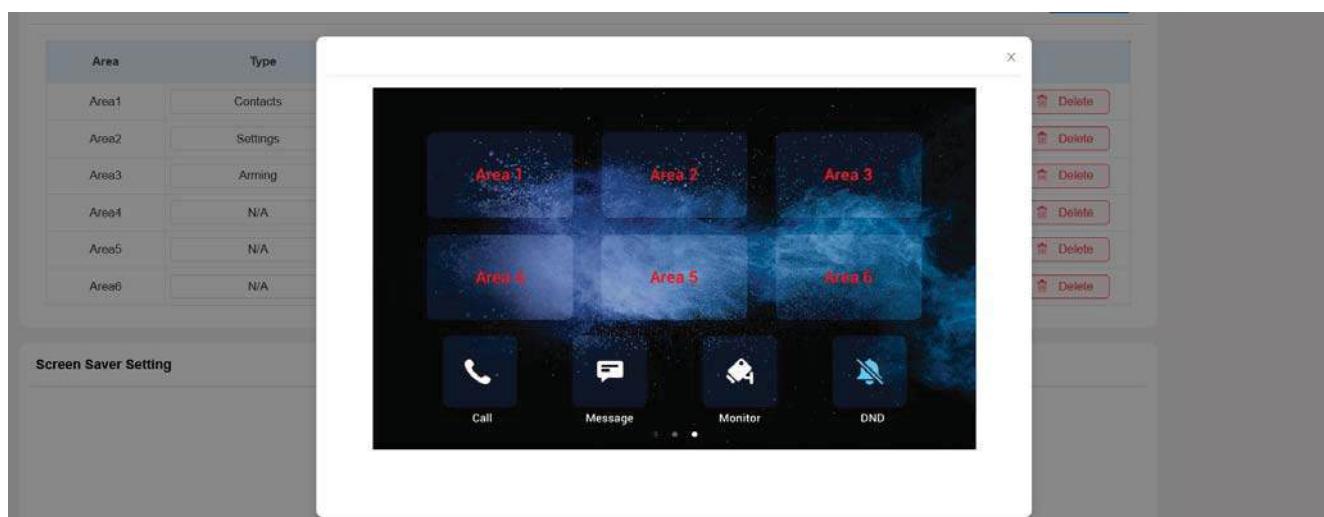
Click **Example** to see the icon layout.



To configure the icons displayed on the More screen, scroll to the **More Page Display** section on the same interface.

More Page Display					Example
Area	Type	Value	Label	Icon(max size:100*100)	
Area1	Contacts		Contacts	Not selected any files	<button>Select File</button> <button>Delete</button>
Area2	Settings		Settings	Not selected any files	<button>Select File</button> <button>Delete</button>
Area3	Arming		Arming	Not selected any files	<button>Select File</button> <button>Delete</button>
Area4	N/A			Not selected any files	<button>Select File</button> <button>Delete</button>
Area5	N/A			Not selected any files	<button>Select File</button> <button>Delete</button>
Area6	N/A			Not selected any files	<button>Select File</button> <button>Delete</button>

Click **Example** to see the icon layout.



Unlock Tab Configuration

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

To set it up, go to **Device > Relay > SoftKey In Talking Page** interface.

Softkey In Talking Page				
Key	Status	Display Name	Type	
Key1	Enabled	Unlock1	Local Relay	
Key2	Enabled	Unlock2	Local Relay	
Key3	Enabled	Unlock3	Local Relay	

- Status:** With the tab enabled, the unlock tab will show on the talking screen.
- Display Name:** Name the unlock tab.
- Type:** The relay trigger type (Local Relay, Remote Relay HTTP, Remote Relay DTMF 1/2/3, Remote Web Relay).

Scroll down to set up unlock tabs on the home screen and more screen on the **Device > Relay > SoftKey in Home or More Page** section.

Softkey In Home Or More Page				
Key	Status	Display Name	Type	
Key	Enabled	Unlock	Remote Relay HTTP1	

- Status:** The unlock button is enabled by default.
- Display Name:** Name the unlock tab.
- Type:** The relay trigger type (Remote Relay HTTP 1-10).

On the same interface, you can set up the unlock tab on the **Monitor screen**:

Softkey In Monitor Page				
Key	Status	Display Name	Type	
Key1	Enabled	Unlock1	Remote Relay HTTP	
Key2	Enabled	Unlock2	Remote Relay HTTP	
Key3	Enabled	Unlock3	Remote Relay HTTP	

- Status:** With the tab(s) enabled, it will show on the monitoring screen.

- **Display Name:** Name the unlock tab.
- **Type:** The relay trigger type (Remote Relay HTTP, Local Relay, Remote Web Relay).

On the same interface, you can set up the unlock tab on the call preview screen:

Softkey In Call-Preview Page				
Key	Status	Display Name	Type	
Key1	Enabled	Unlock1	Remote Relay HTTP	
Key2	Enabled	Unlock2	Remote Relay HTTP	
Key3	Enabled	Unlock3	Remote Relay HTTP	

- **Status:** With the unlock tab enabled, it will appear on the call preview screen.
- **Display Name:** Name the unlock tab.
- **Type:** The relay trigger type(Remote Relay HTTP, Local Relay, Remote Web Relay).

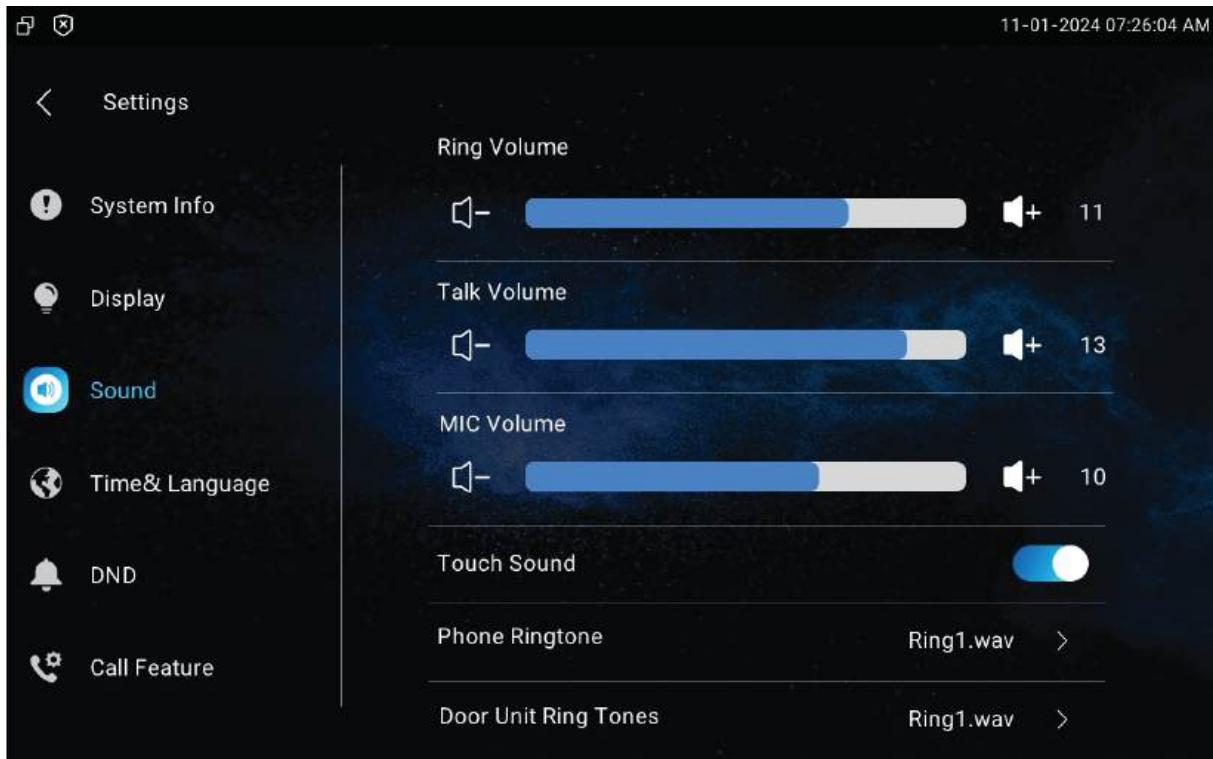
Sound and Volume Configuration

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

Volume Configuration

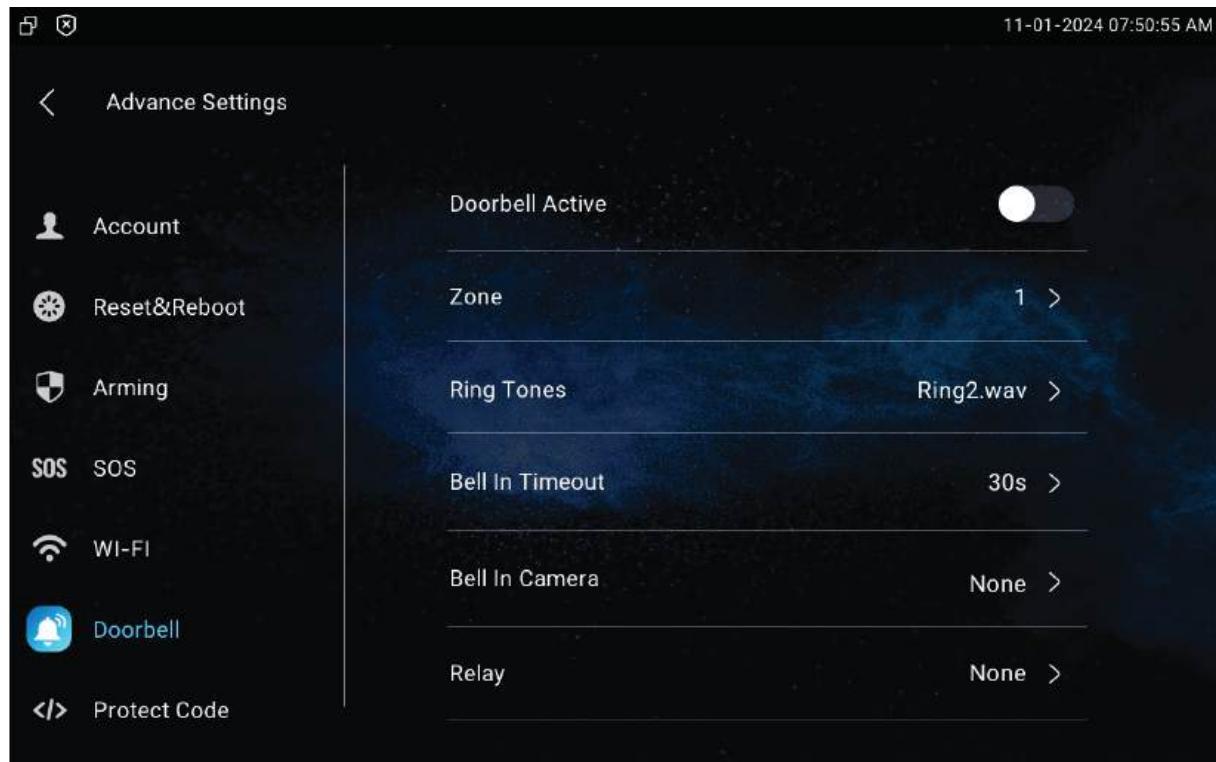
Configure Volume on the Device

To set up the volumes, go to the device **Settings > Sound** screen.



- **Ring Volume:** The incoming call ringtone volume.
- **Talk Volume:** The speaker's volume during the call.
- **MIC Volume:** The mic volume.
- **Touch Sound:** The icon tapping sound.
- **Phone Ringtone:** The ringtone for incoming calls.
- **Door Unit Ring Tones:** The ringtone for the door opening.

You can configure the doorbell sound on the **Settings > Advance Settings > Doorbell** screen.



- **Zone:** The enabling of the doorbell feature will occupy the channel in the selected zone, and the alarm setting in this zone will be disabled.
- **Bell In Timeout:** The doorbell ringing duration from 10 seconds to 5 minutes.
- **Bell In Camera:** Select the camera. The video stream will be displayed on the indoor monitor when the doorbell rings.
- **Relay:** Local relay to be triggered along with the doorbell.

Configure Volume on the Web Interface

Navigate to the web **Device > Audio** interface.

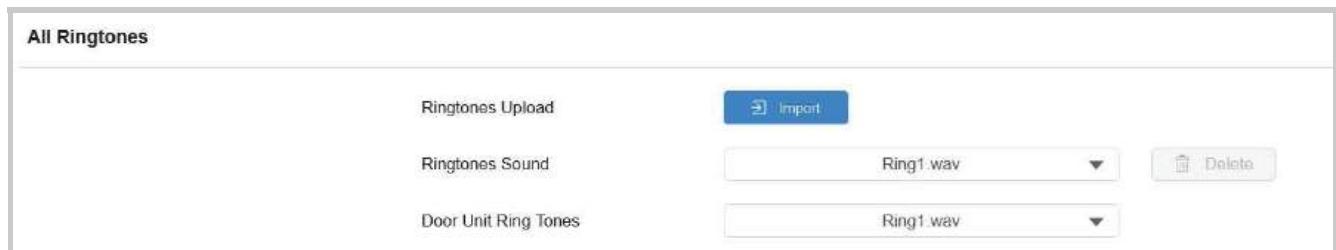
Volume Control			
Mic Volume	10	(1~15)	<input type="text"/>
Ring Volume	11	(0~15)	<input type="text"/>
Talk Volume	13	(1~15)	<input type="text"/>
Touch Sounds	<input checked="" type="checkbox"/>		

- **Mic Volume:** The mic volume.

- **Ring Volume:** The incoming call ringtone volume.
- **Talk Volume:** The speaker's volume during the call.
- **Touch Sounds:** The icon tapping sound.

Upload Ringtones

Navigate to the web **Device > Audio** interface.



- **Ringtones Sound:** The ringtone for incoming calls.
- **Door Unit Ring Tones:** The ringtone for the door opening.

Note

File Format: .wav; Max Size: 250K.

Network Setting & Other Connection

Device Network Configuration

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

Configure Device Network Connection on the Web Interface

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

Network Information		
LAN Port Type		DHCP Auto
Link Status		Connected
IP Address	192.168.36.108	
Subnet Mask	255.255.255.0	
Gateway	192.168.36.1	
Preferred DNS	218.85.152.99	
Alternate DNS	8.8.8.8	

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

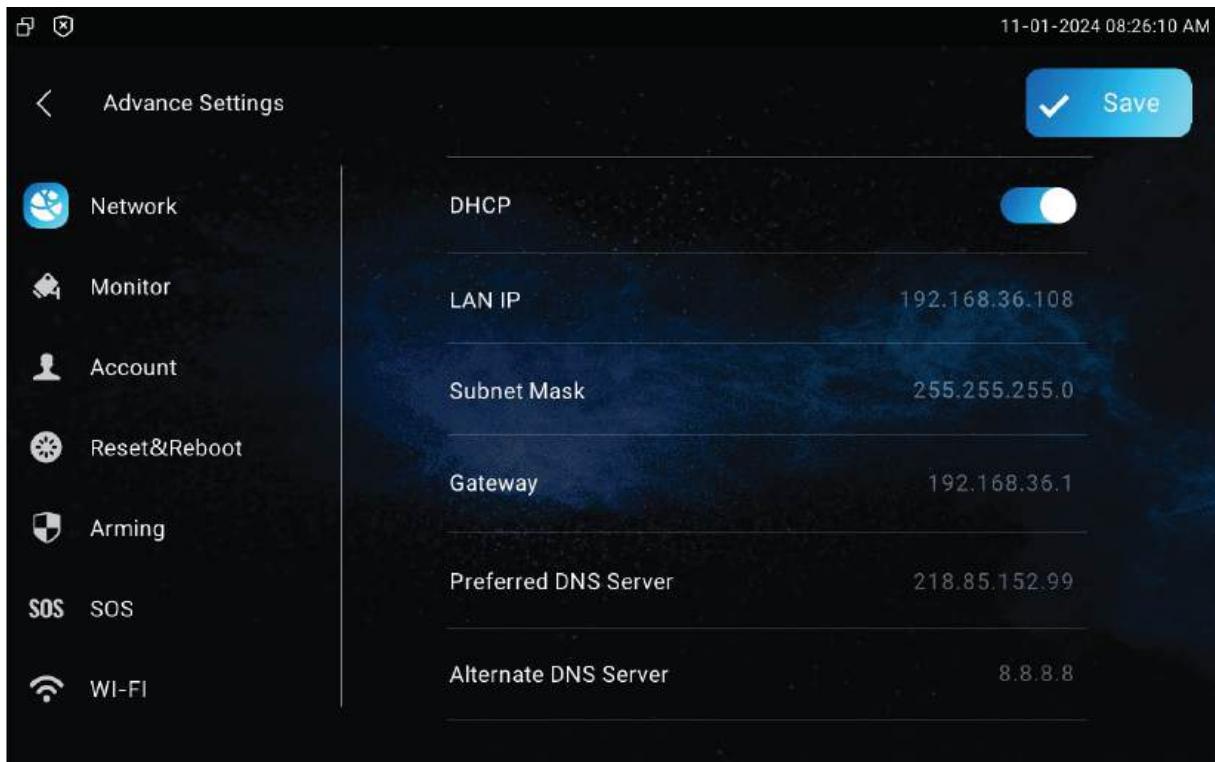
LAN Port	
Type	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Preferred DNS Server	<input type="text"/>
Alternate DNS Server	<input type="text"/>

- Type:

- **DHCP Mode** will enable the indoor monitor to be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
 - **Static IP** allows you to enter the IP address, subnet mask, default gateway, and DNS address manually according to the actual network environment.
- **IP Address:** The IP address when the static IP mode is selected.
 - **Subnet Mask:** The subnet mask according to the actual network environment.
 - **Default Gateway:** The gateway should be set up according to the IP address.
 - **Preferred/Alternate DNS Server:** The preferred and alternate Domain Name Server(DNS). The preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

Configure Device Network Connection on the Device

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



- **DHCP:** DHCP mode is the default network connection. If the DHCP mode is turned on, the device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. If you turn off the DHCP mode, the device will be changed to static IP mode, and then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.
- **LAN IP:** The IP address when the static IP mode is selected.
- **Subnet Mask:** The subnet mask according to the actual network environment.
- **Gateway:** The gateway should be set up according to the IP address.
- **Preferred & Alternate DNS Server:** The preferred and alternate Domain Name Server(DNS). The preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

Device Deployment in Network

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

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

Connect Setting	
Connect Mode	SDMC
Discovery Mode	<input checked="" type="checkbox"/>
Control4 Mode	<input type="checkbox"/>
Device Node	1 1 1 1 1
Device Extension	1 (1~8)
Device Location	Indoor Monitor

- **Connect Mode:** It is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud**, or **None**. **None** is the default factory setting indicating the device is not in any server type.
- **Discovery Mode:** With discovery mode enabled, the device can be discovered by other devices in the network. Uncheck the box if you want to conceal the device.
- **Device Node:** Specify the device address by entering device location info from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.
- **Device Extension:** The device extension number for the device you installed.
- **Device Location:** The location where the device is installed and used.

Device NAT Setting

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

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

NAT	
NAT	<input type="checkbox"/>
Stun Server Address	<input type="text"/>
Port	<input type="text"/> 3478 <small>(1024-65535)</small>

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

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

NAT	
RPort Enabled	<input type="checkbox"/>

- **RPort:** Enable the RPort when the SIP server is in WAN for the SIP account registration.

VLAN Setting

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.

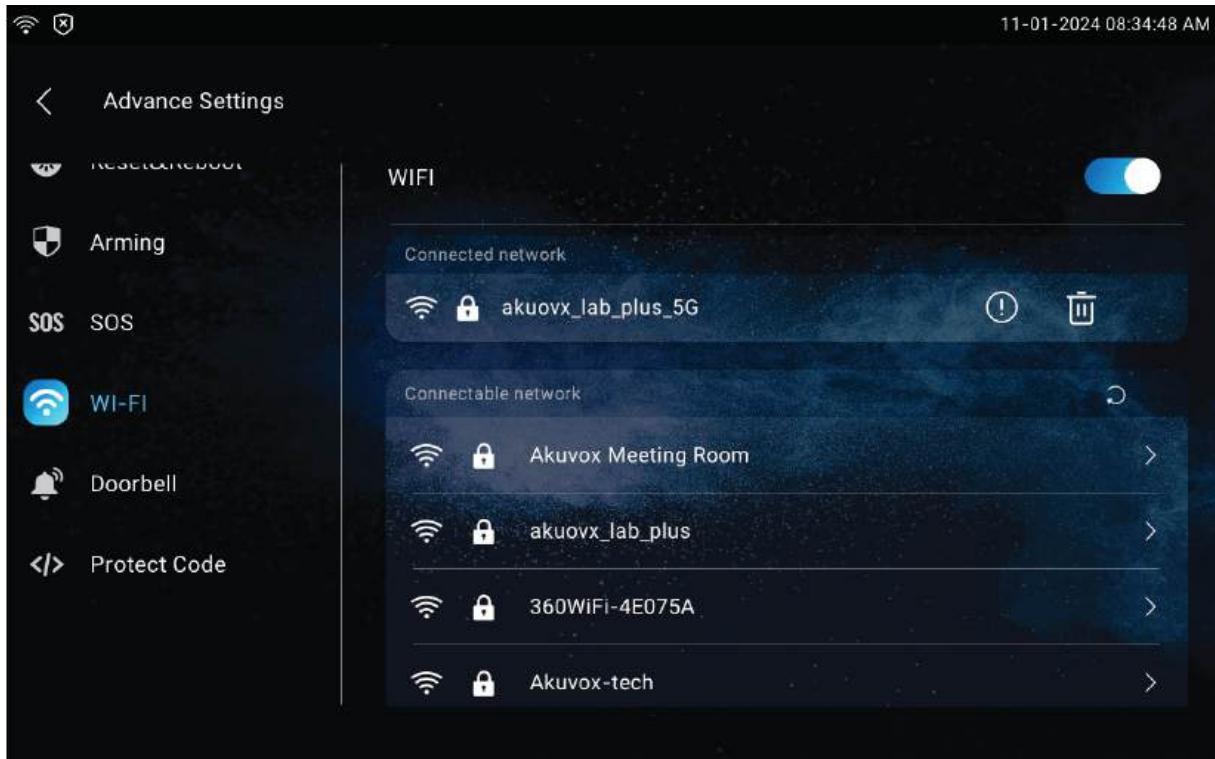
To set it up, navigate to the web **Network > Advanced > VLAN Setting** interface.

VLAN Setting	
VLAN	<input type="checkbox"/>
Priority	<input type="text"/> 0 <small>▼</small>
VLAN ID	<input type="text"/> 1 <small>(1-4094)</small>

- **Priority:** Select VLAN priority for the designated port.
- **VLAN ID:** The VLAN ID for the designated port.

Device Wi-Fi Setting

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

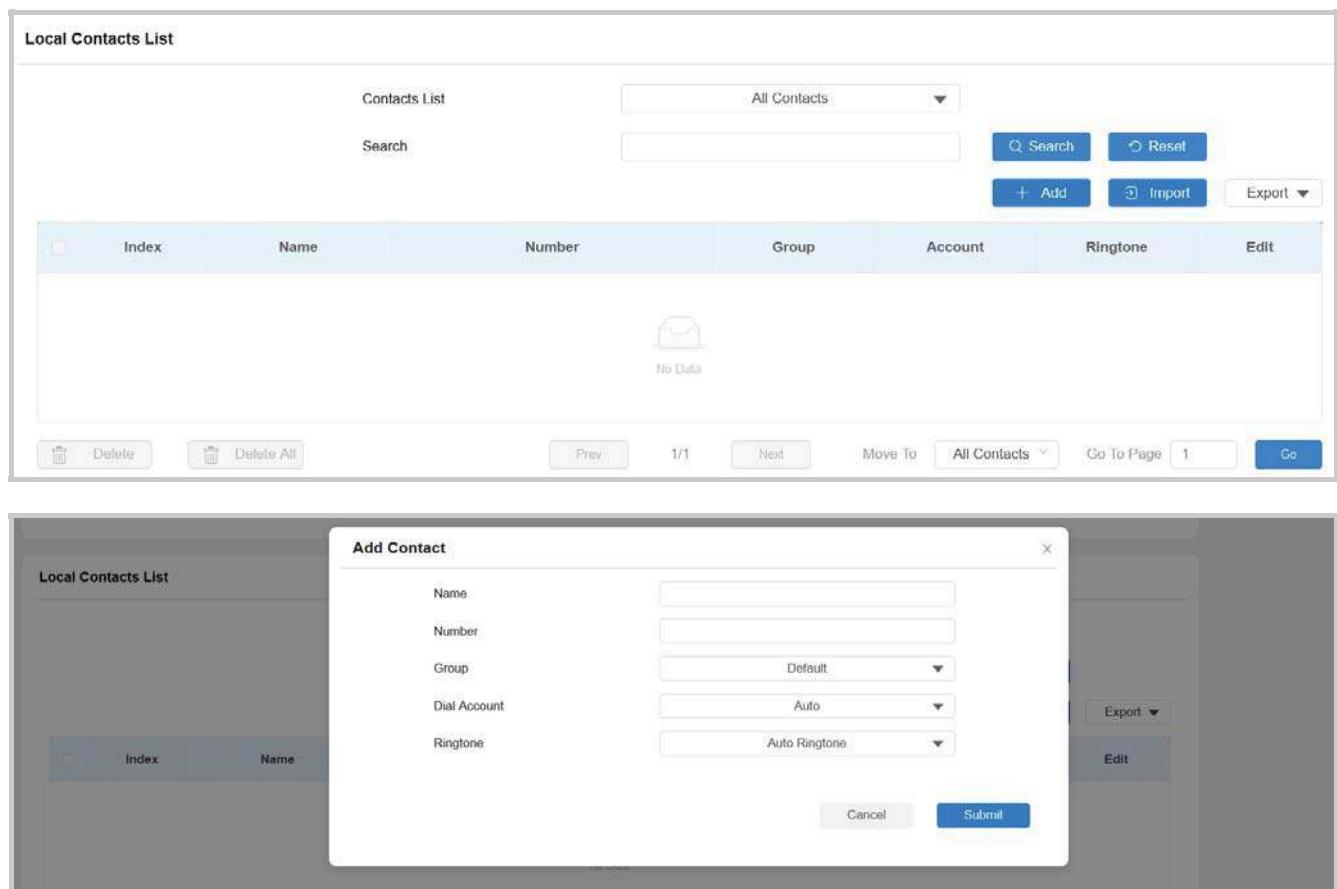


Contacts Configuration

Contacts Configuration on the Web Interface

Add Local Contacts

Add, edit, and search local contacts on the device's web interface. To add contacts, go to **Contacts > Local Contacts > Local Contacts List** interface, then click **+Add**.



The image contains two screenshots of the Akuvox web interface. The top screenshot shows the 'Local Contacts List' page. It features a table with columns: Index, Name, Number, Group, Account, Ringtone, and Edit. The table is currently empty, displaying a 'No Data' message with an envelope icon. Below the table are buttons for 'Delete' and 'Delete All', and navigation links for 'Prev', '1/1', 'Next', 'Move To', 'All Contacts', 'Go To Page 1', and 'Go'. The top of the page has a search bar, a dropdown for 'Contacts List' (set to 'All Contacts'), and buttons for 'Search', 'Reset', '+ Add', 'Import', and 'Export'. The bottom screenshot shows a modal dialog box titled 'Add Contact'. It contains five input fields: 'Name', 'Number', 'Group' (set to 'Default'), 'Dial Account' (set to 'Auto'), and 'Ringtone' (set to 'Auto Ringtone'). At the bottom of the dialog are 'Cancel' and 'Submit' buttons. The background of the dialog is dimmed, showing the 'Local Contacts List' page.

- **Contact List:** All Contacts displays all the contacts in the contact list. BlockList displays the contacts in the blocklist.
- **Search:** Contact name or contact number used to search a contact.
- **Name:** The contact's name to distinguish it from others.

- **Number:** The SIP or IP number of the contact.
- **Group:** Calls from contacts in **Blocklist** will be rejected.
- **Dial Account:** The registered account to make the call, Account 1 or Account 2.
- **Ringtone:** The ringtone for the incoming call from the contact.

Note

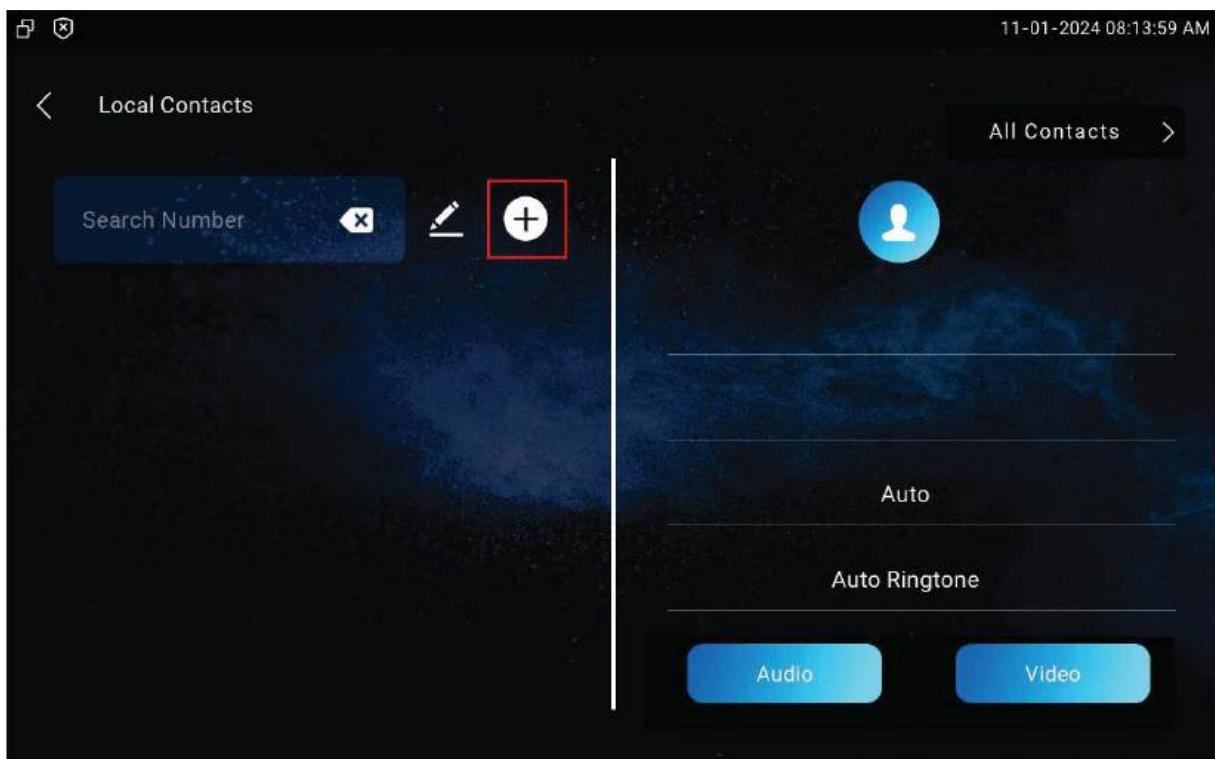
If you want to remove the contact from the blocklist on the web interface, you can change the group to **Default** when editing the contact.

Contacts Configuration on the Device

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

Add Local Contact

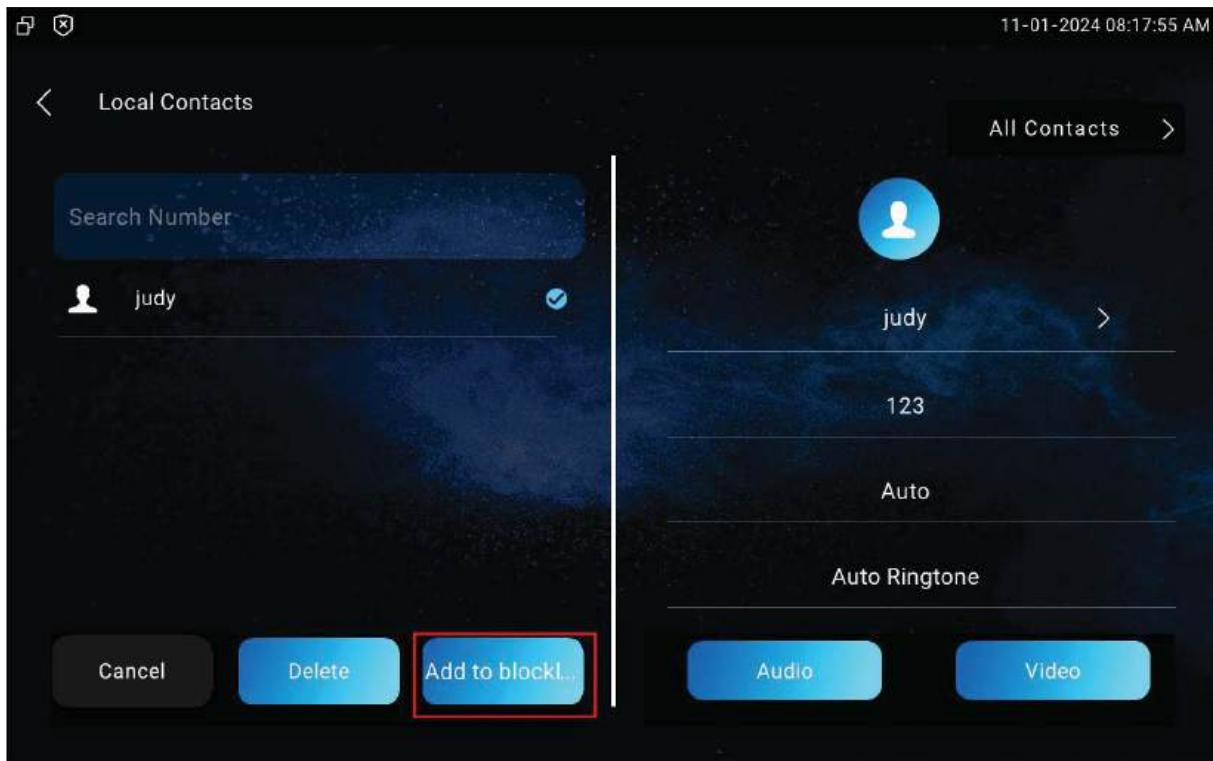
Press the **Add** icon to add a contact.



Block List Setting on the Device

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

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



Import and Export Contacts

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

Navigate to the web **Contacts > Local Contacts > Local Contacts List** interface.



Contact List Display Configuration

Conduct contact display on the web **Contacts > Local Contacts > Contacts List Setting** interface.

Contacts List Setting	
Contacts Sort By	Default ▾
Show Local Contacts Only	Disabled ▾

- **Contacts Sort By:**

- **Default:** The local contacts will be displayed before the contacts from SmartPlus, SDMC, etc.
- **ASCII Code:** The contacts will be displayed in the order based on the first letter of the contact names.
- **Created Time:** The contacts will be displayed by their created time.

- **Show Local Contacts Only:** If enabled, then only the local contacts will be displayed. If disabled, then all the contacts from SmartPlus Cloud, SDMC, and so on will be displayed.

Intercom Call Configuration

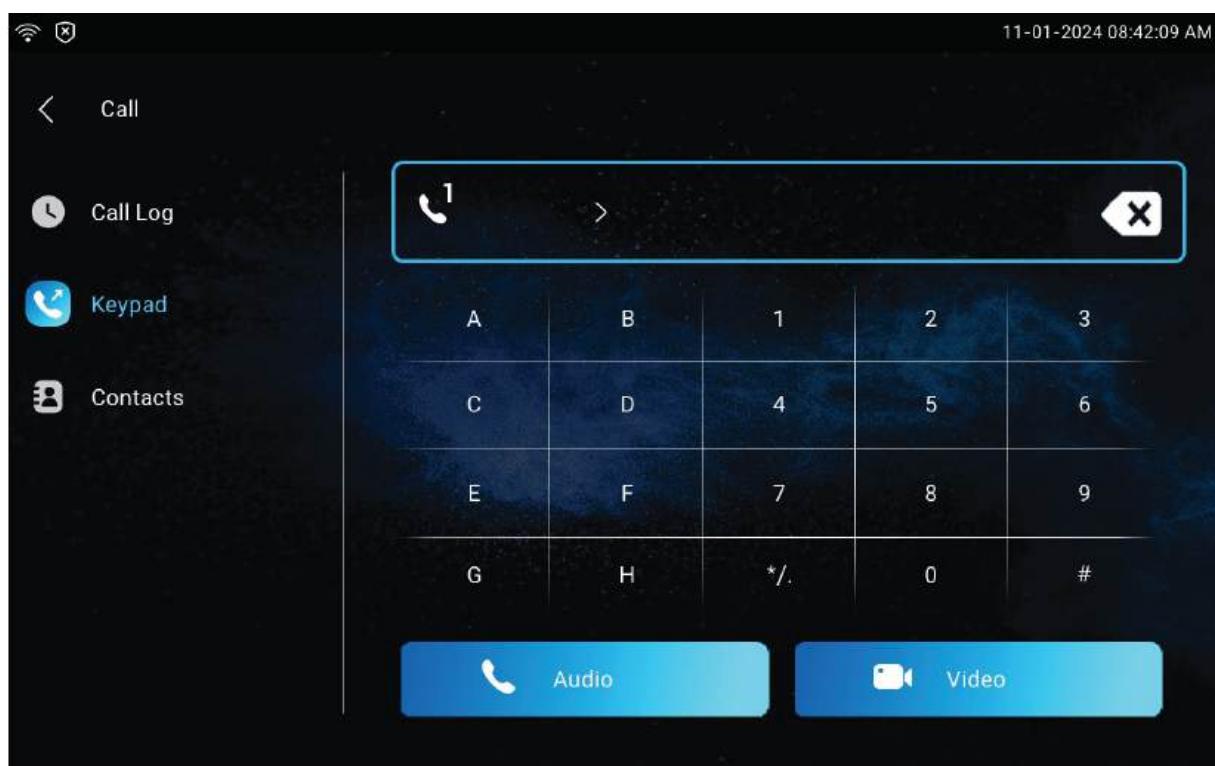
IP Call & IP Call Configuration

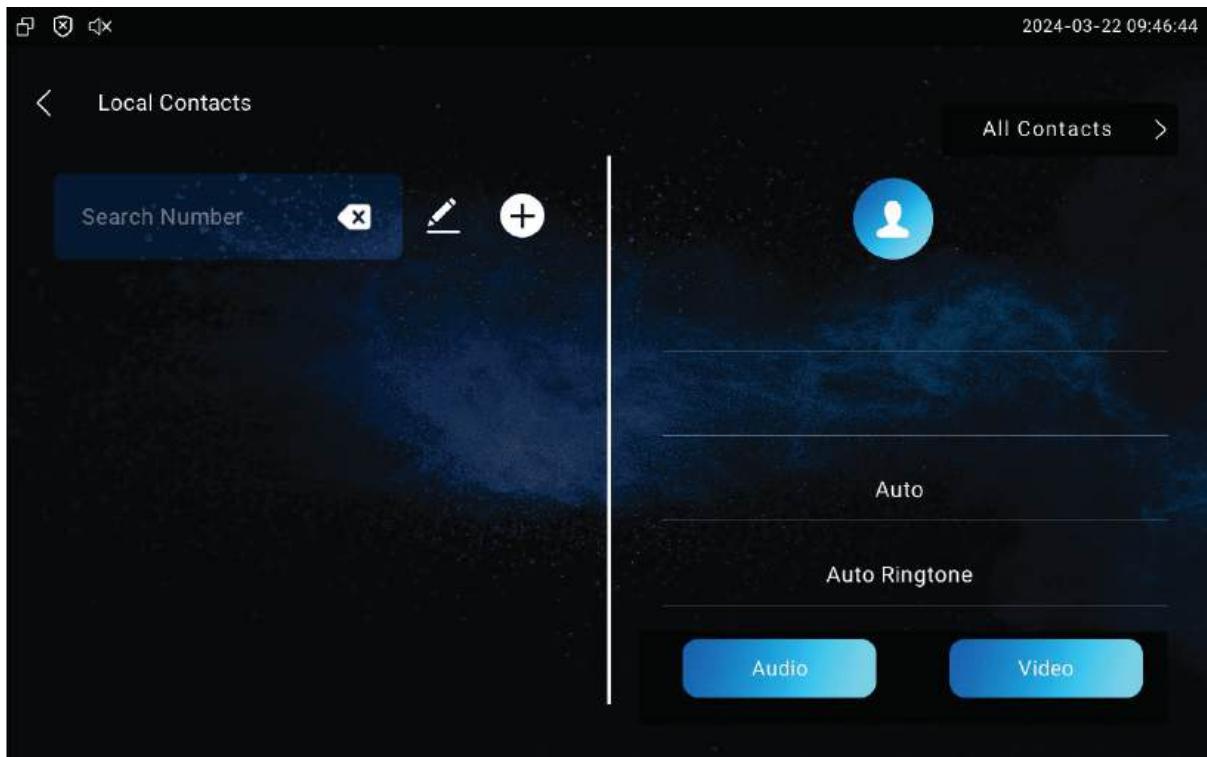
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Make IP Calls

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

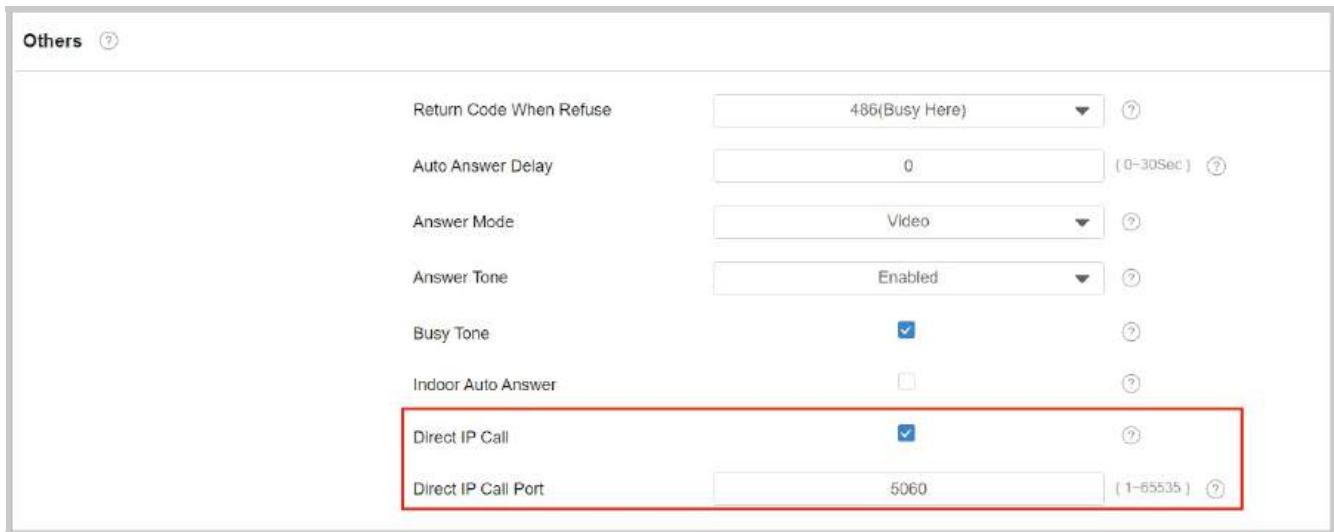
Enter the IP address on the soft keyboard, select the account to make the call, and press the **Audio** or **Video** tab to call out. In addition, users can also make IP calls on the **Contacts > Local Contacts** screen.





IP Call Configuration

Configure the IP call feature and port on the web **Device > Call Feature > Others** interface.



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

SIP Call & SIP Call Configuration

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

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

SIP Account Registration

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

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

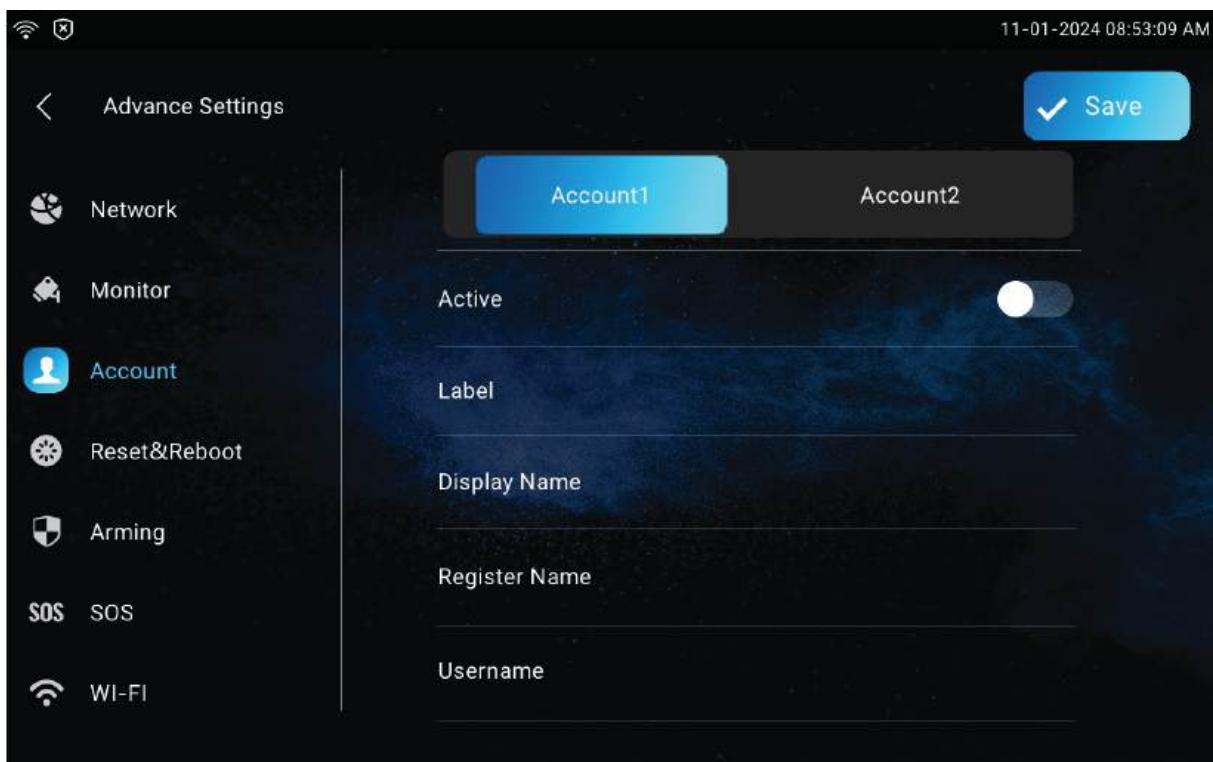
To set it up, navigate to the web **Account > Basic > SIP Account** interface.

SIP Account	
Status	Disabled
Account	<input style="width: 100%; height: 100%;" type="button" value="Account1"/>
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	*****

- **Status:** Display whether the SIP account is registered or not.
- **Account:** The device supports 2 SIP accounts.
 - Account 1 is the default account for call processing. Also, it will be utilized when the Akuvox SmartPlus cloud service is activated.
 - The system switches to Account 2 if Account 1 is not registered.
 - To designate the account to be used for outgoing calls, select the account number for contacts.

- **Account Enabled:** Check to activate the registered SIP account.
- **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.

The SIP account can also be configured on the device **Settings > Advance Settings > Account** screen.



SIP Server Configuration

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

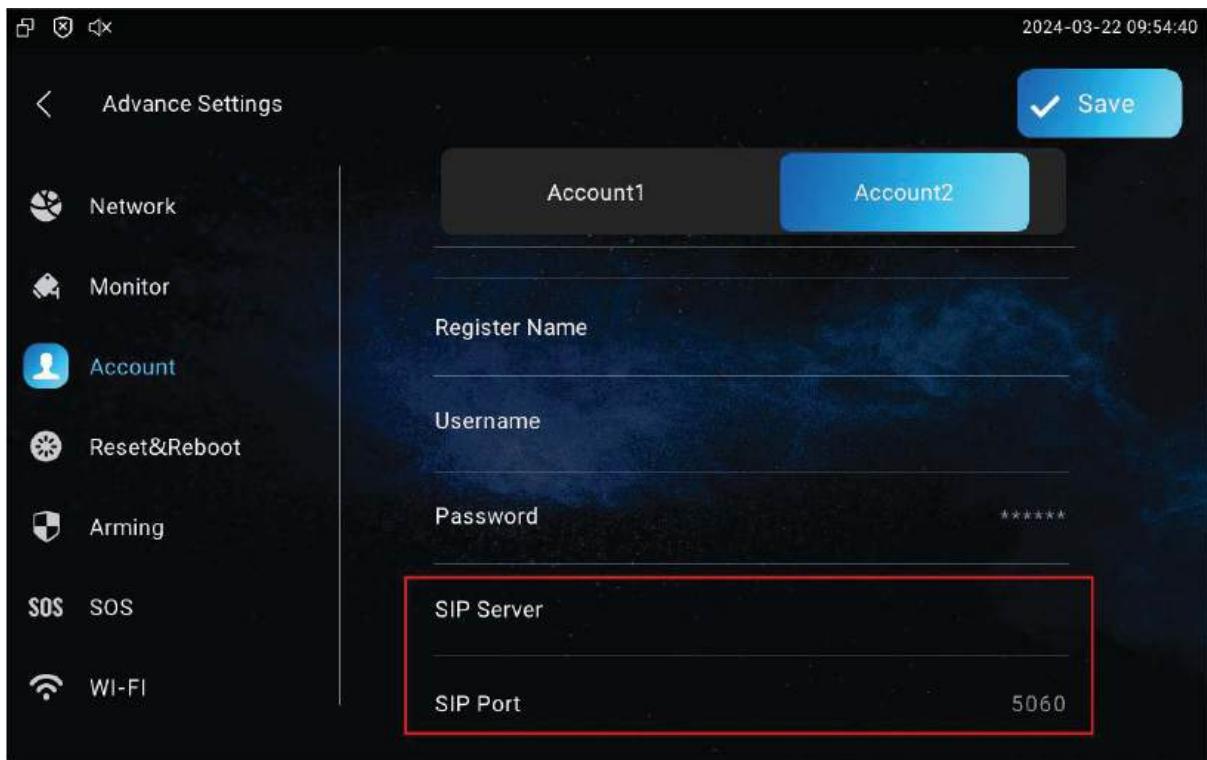
To set it up, navigate to the web **Account > Basic > Preferred SIP Server/Alternate SIP Server** interface or the device **Settings > Advance Settings > Account** screen.

Preferred SIP Server

Sip Server Address	<input type="text"/>
Sip Server Port	5060 <small>(1024~65535)</small>
Registration Period	1800 <small>(30~65535 Sec)</small>

Alternate SIP Server

Sip Server Address	<input type="text"/>
Sip Server Port	5060 <small>(1024~65535)</small>
Registration Period	1800 <small>(30~65535 Sec)</small>



- **SIP Server Address:** The server's IP address number or its URL.
- **SIP Server Port:** The SIP server port for data transmission.
- **Registration Period:** 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 Call DND & Return Code Configuration

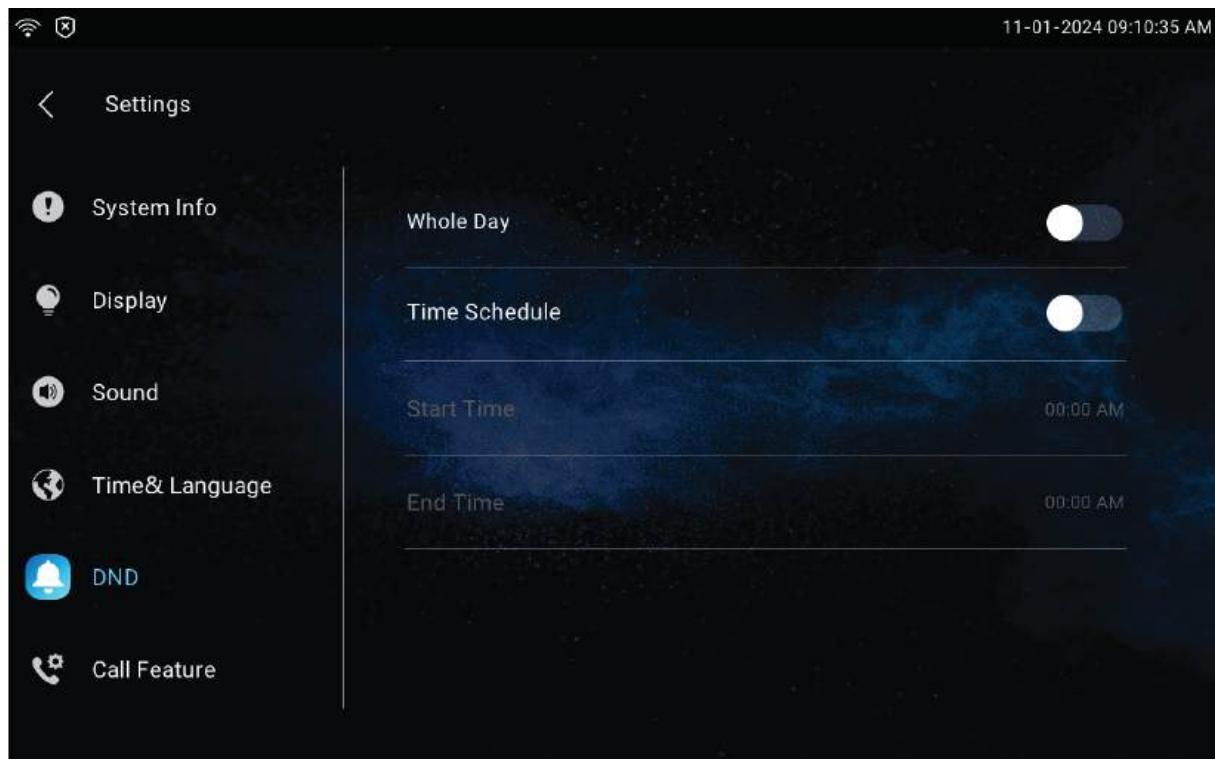
The Do Not Disturb(DND) feature prevents unwanted incoming SIP calls, ensuring uninterrupted focus. It also allows you to set a code to be sent to the SIP server when rejecting a call.

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

DND	
Whole Day	<input type="checkbox"/>
Schedule	<input type="checkbox"/>
DND Start Time	00:00 <input type="button" value=""/>
DND End Time	00:00 <input type="button" value=""/>
Return Code When DND	486(Busy Here) <input type="button" value="▼"/>

- **DND:** Enable **Whole Day** or **Schedule** to turn on the DND function. The DND function is disabled by default.
- **Return Code When DND:** Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

DND can also be set up on the device **Settings > DND** screen.



Outbound Proxy Server Configuration

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

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

Outbound Proxy Server	
Outbound Enabled	<input type="checkbox"/>
Preferred Outbound Proxy Server	<input type="text"/>
Preferred Outbound Proxy Server Port	5060 (1024~65535)
Alternate Outbound Proxy Server	<input type="text"/>
Alternate Outbound Proxy Server Port	5060 (1024~65535)

- Preferred Outbound Proxy Server:** Set 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:** Set 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.

Device Local RTP Configuration

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

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

Set up the device's local RTP on the web **Network > Advanced > Local RTP** interface.

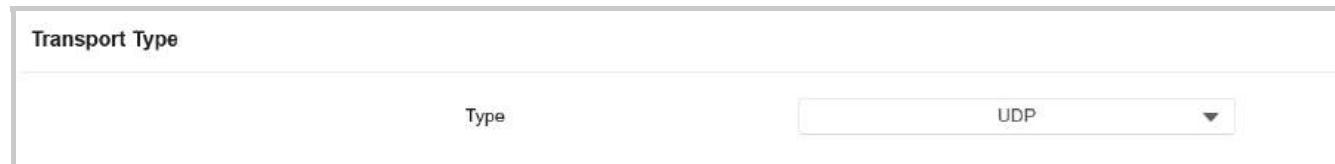
Local RTP	
Starting RTP Port	11800 (1024~65535)
Max RTP Port	12000 (1024~65535)

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

Data Transmission Type Configuration

The device supports three data transmission protocols: User Datagram Protocol(UDP), Transmission Control Protocol(TCP), and Transport Layer Security(TLS).

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



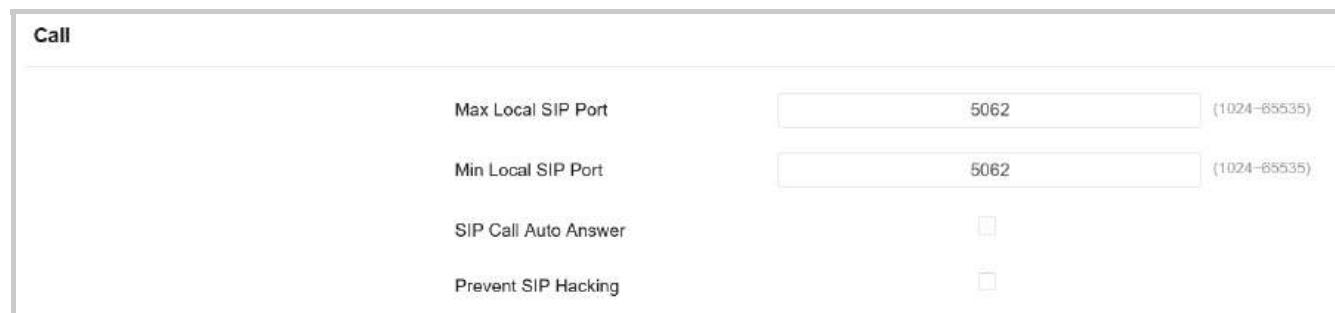
The screenshot shows a configuration interface for 'Transport Type'. At the top, it says 'Transport Type'. Below that is a dropdown menu labeled 'Type' with 'UDP' selected. There is also a small downward arrow icon next to the dropdown.

- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced security or if the other party's server uses TLS. To use it, you need to upload certificates for authentication.

SIP Hacking Protection

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

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



The screenshot shows a configuration interface for 'Call' settings. It includes the following fields:

- Max Local SIP Port: Value 5062, Range (1024-65535)
- Min Local SIP Port: Value 5062, Range (1024-65535)
- SIP Call Auto Answer: A checkbox that is not checked.
- Prevent SIP Hacking: A checkbox that is not checked.

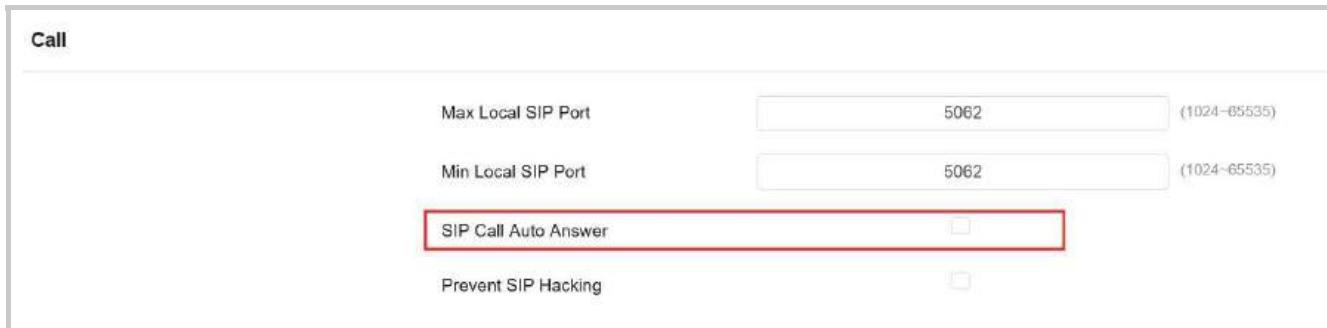
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects user's private and secret information from potential hackers during SIP calls.

Call Settings

Auto-answer Configuration

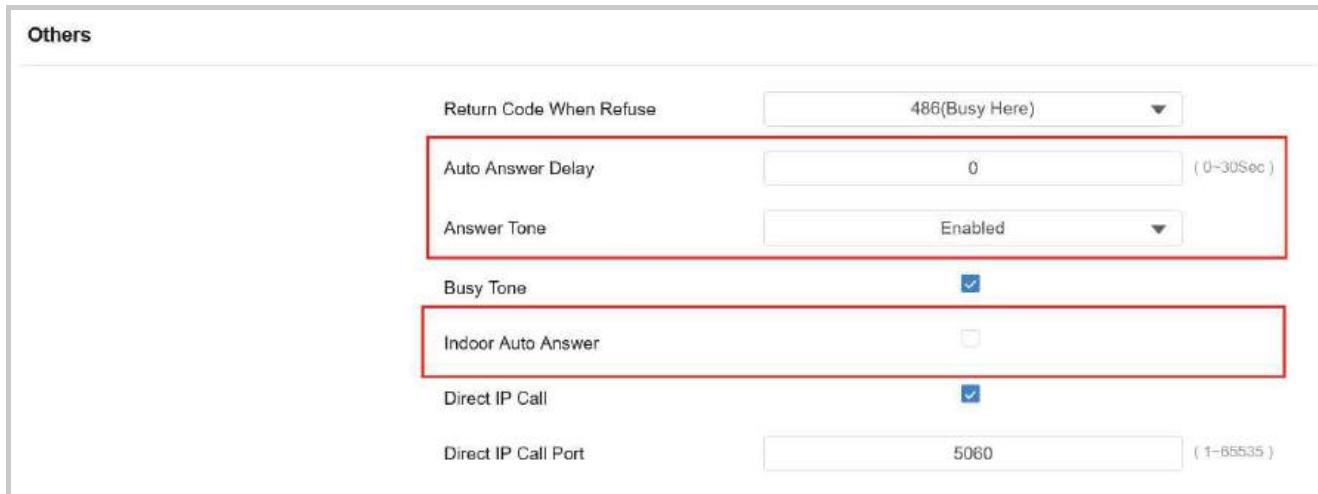
Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention. You can also customize this feature by setting the time duration for auto-answering and choosing the communication mode between audio and video.

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



Max Local SIP Port	5062	(1024-65535)
Min Local SIP Port	5062	(1024-65535)
SIP Call Auto Answer	<input type="checkbox"/>	
Prevent SIP Hacking	<input type="checkbox"/>	

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



Return Code When Refuse	486(Busy Here)	
Auto Answer Delay	0	(0~30Sec)
Answer Tone	Enabled	
Busy Tone	<input checked="" type="checkbox"/>	
Indoor Auto Answer	<input type="checkbox"/>	
Direct IP Call	<input checked="" type="checkbox"/>	
Direct IP Call Port	5060	(1-65535)

- **Auto Answer Delay:** Set the time interval for the call to be automatically picked up after ringing. For example, if you set the delay time to 5 seconds, the device will answer the call automatically after 5 seconds.
- **Answer Tone:** Select the tone for answering calls automatically.
- **Indoor Auto Answer:** Allow calls from other indoor monitors to be answered by the device automatically.

Other Options:

- **Return Code When Refuse:** Decide the code sent to the caller side via the SIP server when rejecting the incoming call.
- **Busy Tone:** Decide whether to sound a busy tone when a call is hung up by the callee.

Auto-answer Allow List Setting

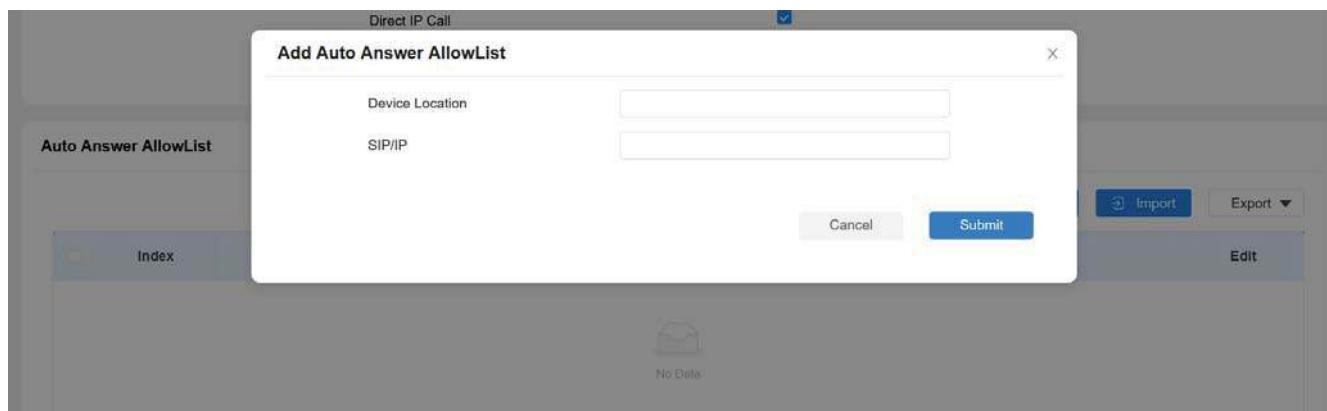
Auto-answer can only be applicable to the SIP or IP numbers that are already added in the auto-answer allow list of your indoor monitor. Therefore, you are required to configure or edit the numbers in the allow list on the web interface.

To set it up, navigate to the web **Device > Call Feature > Auto Answer AllowList** interface.



The screenshot shows a web-based configuration interface for an 'Auto Answer AllowList'. The top navigation bar includes 'Auto Answer AllowList', 'Index', 'Device Location', 'SIP/IP', and 'Edit' buttons. Below this is a table with columns for 'Index', 'Device Location', 'SIP/IP', and 'Edit'. The table body is empty and displays a 'No Data' message with a small envelope icon. At the bottom, there are buttons for 'Delete', 'Delete All', 'Prev', '1/1', 'Next', 'Go To Page 1', and 'Go'.

Click **+Add** to add the device allowed for auto-answer.



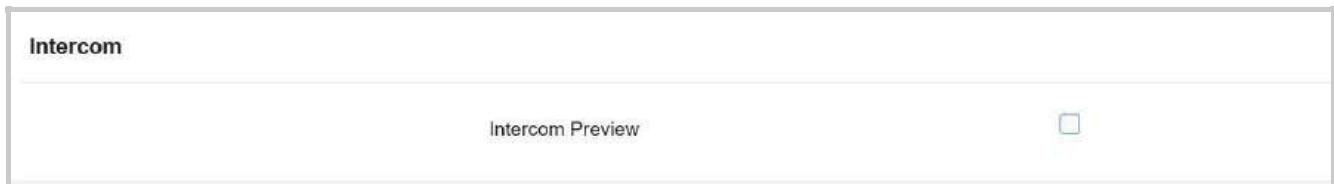
The screenshot shows a 'Add Auto Answer AllowList' dialog box overlaid on a main interface. The dialog has fields for 'Device Location' and 'SIP/IP', both currently empty. It includes 'Cancel' and 'Submit' buttons. The background shows a 'Direct IP Call' section and a 'No Data' message with an envelope icon.

Note

- The supported imported/exported file format is XML or CSV.
- SIP/IP numbers must be set up in the contacts of the indoor monitor before they can be valid for the auto-answer function.

Intercom Setting

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



- **Intercom Preview:** When it is enabled, the group call is not available.

Emergency Call Setting

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

To display the emergency call softkey, you can configure it on the web **Device > Display Setting > Home Page Display/More Page Display** interface.

Home Page Display					Example
Area	Type	Value	Label	Icon(max size:100*100)	
Area1	SOS		SOS	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area2	Message		Message	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area3	DND		DND		
Area4	Monitor		Monitor	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>

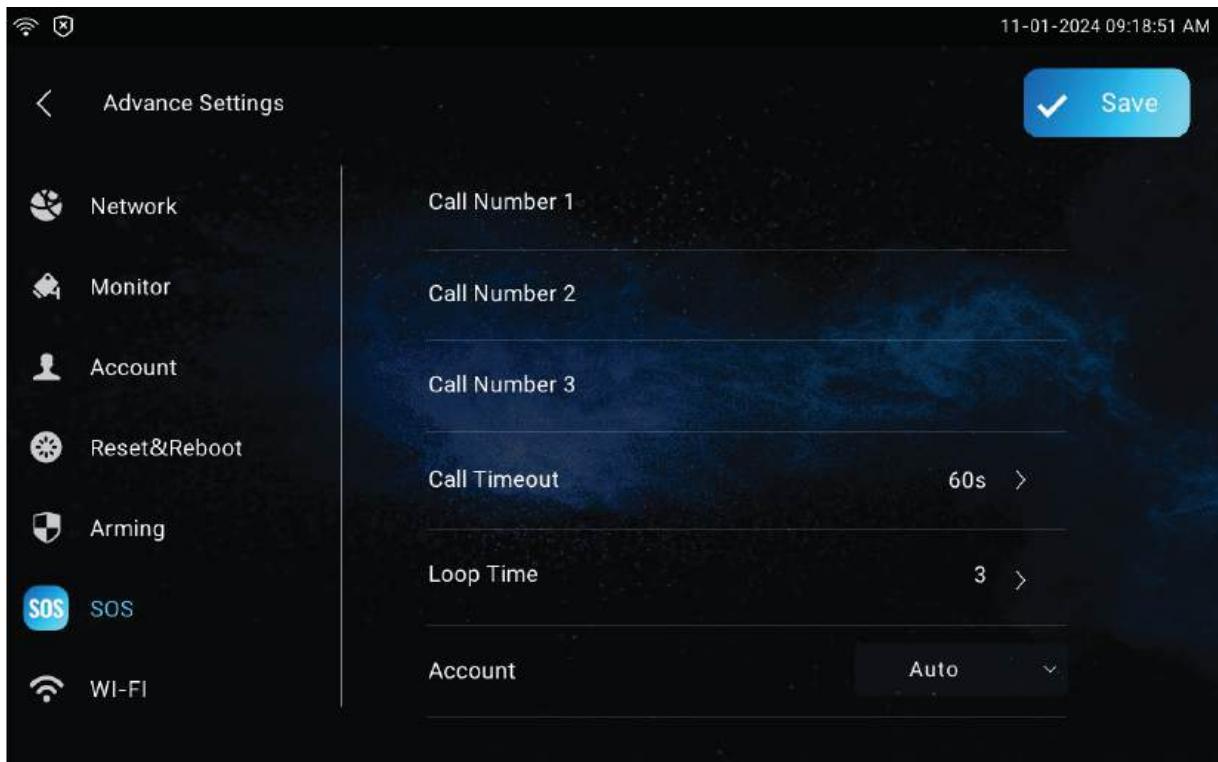
More Page Display					Example
Area	Type	Value	Label	Icon(max size:100*100)	
Area1	SOS		SOS	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area2	Settings		Settings	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area3	Arming		Arming	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>

Then, navigate to the web **Device > Intercom > SOS** interface.

sos	
Account	<input type="button" value="Auto"/>
Call Number 1	
Call Number 2	
Call Number 3	
Call Timeout(Sec)	<input type="button" value="60s"/>
Loop Times	<input type="button" value="3"/>

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

The SOS feature can also be set up on the device **Settings > Advance Settings > SOS** screen.



Multicast Configuration

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

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

Multicast List			
Multicast Group	Multicast Address	Enabled	
Multicast Group 1	224.1.6.11:51230	<input type="checkbox"/>	
Multicast Group 2	224.1.6.11:51231	<input type="checkbox"/>	
Multicast Group 3	224.1.6.11:51232	<input type="checkbox"/>	

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

- **Multicast Address:** The multicast IP address is the same as the listen address.

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

Note

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

Call Forwarding Setting

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

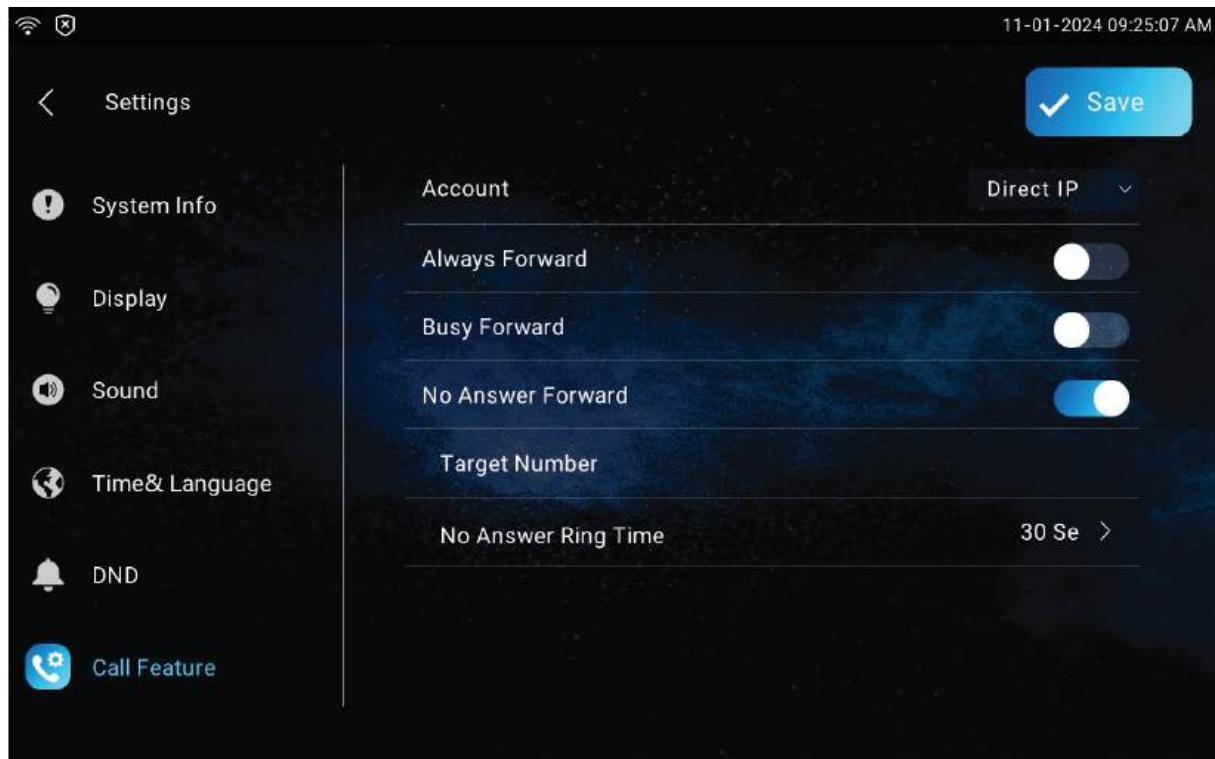
To set it up, go to the web **Device > Call Feature > Call Forward** interface.

Call Forward	
Account	Account1
Always Forward	Disabled
Target Number	
Busy Forward	Disabled
Target Number	
No Answer Forward	Disabled
Target Number	
No Answer Ring Time (Sec)	30

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

- **Target Number:** The specific forward number when Always Forward, Busy Forward, or No Answer Forward is enabled.
- **No Answer Ring Time (Sec):** The time ranges from 0-120 seconds.

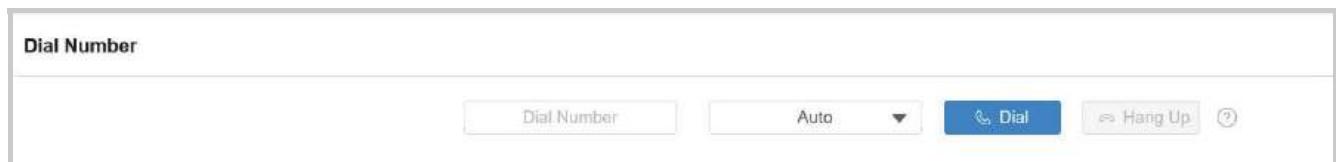
The call forwarding feature can also be set up on the device **Settings > Call Feature** screen.



Web Call

The web call feature allows for making calls via the device's web interface, commonly used for remote call testing purposes.

To set it up, navigate to the web **Contacts > Local Contacts > Dial Number** interface. Enter the contact's SIP or IP number and select the account to dial out.

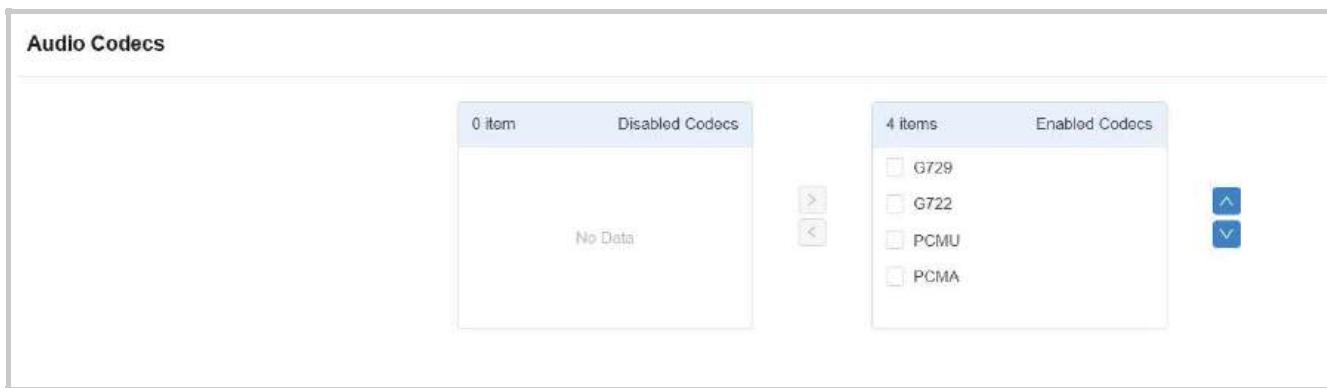


Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

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

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



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

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

Video Codec Configuration

The device supports the H264 codec that provides better video quality at a much lower bit rate with different video quality and payload.

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

Video Codec	
Name	<input checked="" type="checkbox"/> H264
Resolution	720P
Bitrate	2048
Payload	104

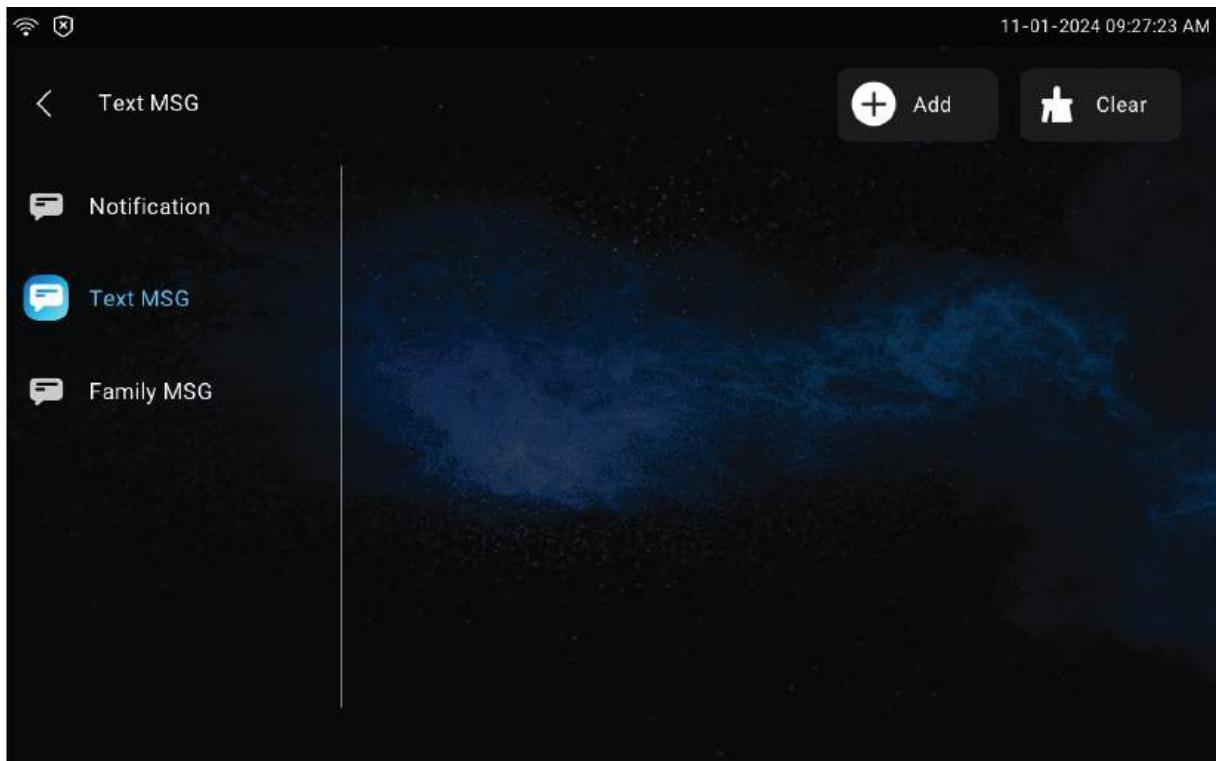
- **Resolution:** The code resolution for the video quality has five options: QCIF, CIF, VGA, 4CIF, and 720P. Select the resolution according to the network environment.
- **Bitrate:** The video stream bit rate ranges from 128-2048. The greater the bitrate, the more data is transmitted every second. Therefore, the video will be clearer. The default bitrate is 2048.
- **Payload:** The payload ranges from 90-119 for the audio/video configuration file.

Intercom Message Setting

Manage Messages

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

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



- **Notification:** The message from property managers, this feature is only available when using SDMC or Akuvox SmartPlus.
- **Text MSG:** To send, receive, or manage the text message.
- **Family MSG:** Audio messages recorded for family members.

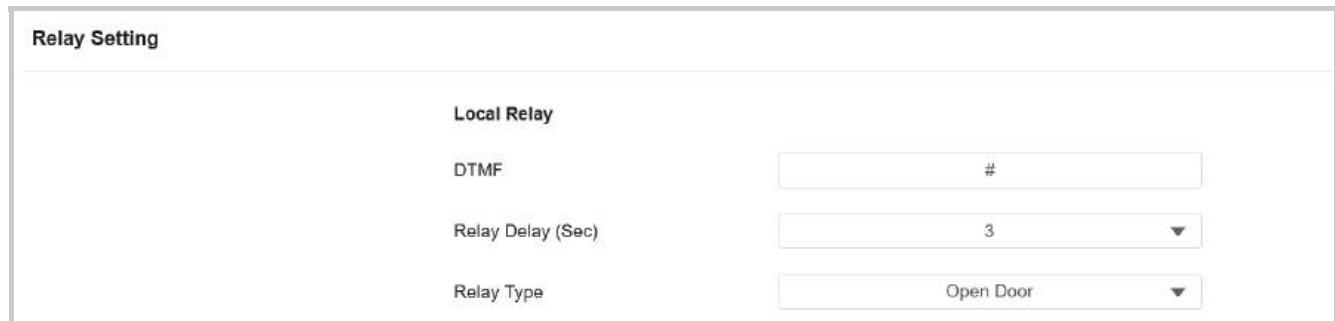
Access Control Configuration

Relay Switch Setting

Local Relay Setting

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

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



The screenshot shows a 'Relay Setting' interface for a 'Local Relay'. It includes fields for DTMF (containing '#'), Relay Delay (Sec) (set to 3), and Relay Type (set to 'Open Door').

- **Relay Delay:** Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains to be opened for 5 seconds before closing.
- **Relay Type:** Relay action type.
 - **Chime Bell Setting:** When there is a call and the relay is triggered, the chime bell will ring.
 - **Open Door:** When the unlock icon is pressed and the relay is triggered, the door will be opened.

Remote Relay Switch Setting

You can use the unlock tab during the call to open the door. And you are required to set up the same DTMF code in the door phone and indoor monitor.

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

Relay Setting

Local Relay	
DTMF	#
Relay Delay (Sec)	3
Relay Type	Open Door
Remote Relay	
DTMF	#
DTMF1 Code	#
DTMF2 Code	#
DTMF3 Code	#

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

Web Relay Setting

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



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

The screenshot shows a software interface for configuring a web relay. The 'Web Relay Setting' section contains fields for IP Address, User Name, and Password. The 'Web Relay Action Setting' section is a table with columns for Action ID, IP, SIP, and Web Relay Action, containing five rows of data.

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

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

Note

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

Door Unlock Configuration

Door Unlock by DTMF Code

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

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

Relay Setting

Local Relay

DTMF	#
------	---

Relay Delay (Sec) 3

Relay Type Open Door

Remote Relay

DTMF	#
DTMF1 Code	#
DTMF2 Code	#
DTMF3 Code	#

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

DTMF

Mode	RFC2833
DTMF Code Transport Format	Disabled
DTMF Payload	101 (96~127)

- **Mode:** Select from the provided options.
- **DTMF Code Transport Format:** there are four options, Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via signaling while other transport format does it via RTP audio packet transmission. Select the DTMF transferring format according to the third-party device.

- **Payload:** It is for data transmission identification ranging from 96-127.

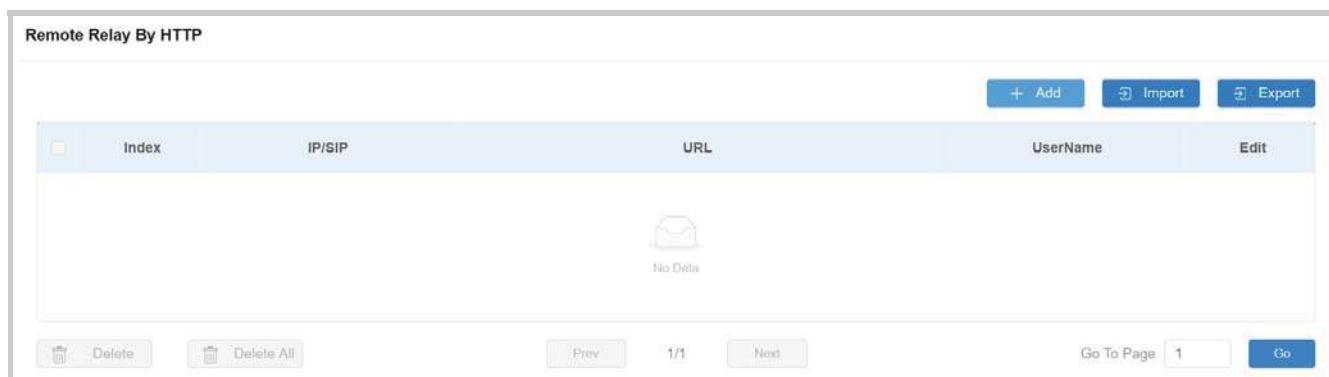
Note

To open the door with DTMF, the intercom devices that send and receive the unlock command must use the same mode and code. Otherwise, the DTMF unlock may fail. See [here](#) for the detailed DTMF configuration steps.

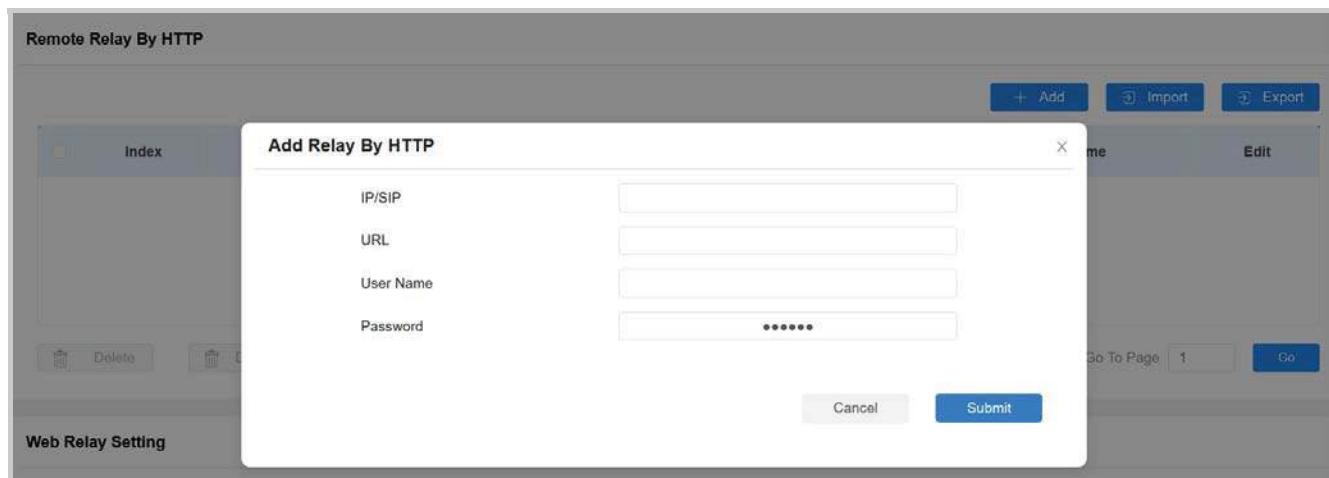
Door Unlock via HTTP Command

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

To set it up, navigate to the web **Device > Relay > Remote Relay By HTTP** interface. Click **+Add**.



Index	IP/SIP	URL	UserName	Edit
 No Data				



IP/SIP	
URL	
User Name	
Password	*****

- **IP/SIP:** Specify the IP or SIP number of the door phone.
- **URL:** Enter the HTTP URL.

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

Tip

Here is an HTTP command URL example for relay triggering.

Door phone's IP **Preset credentials for authentication**
http://192.168.35.127/cgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note

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

Import/Export HTTP Commands

Navigate to the web **Device > Relay > Remote Relay By HTTP** interface. The exported file is in TGZ format. The imported file should be in XML format.

Remote Relay By HTTP				
	Index	IP/SIP	URL	UserName
 Edit				

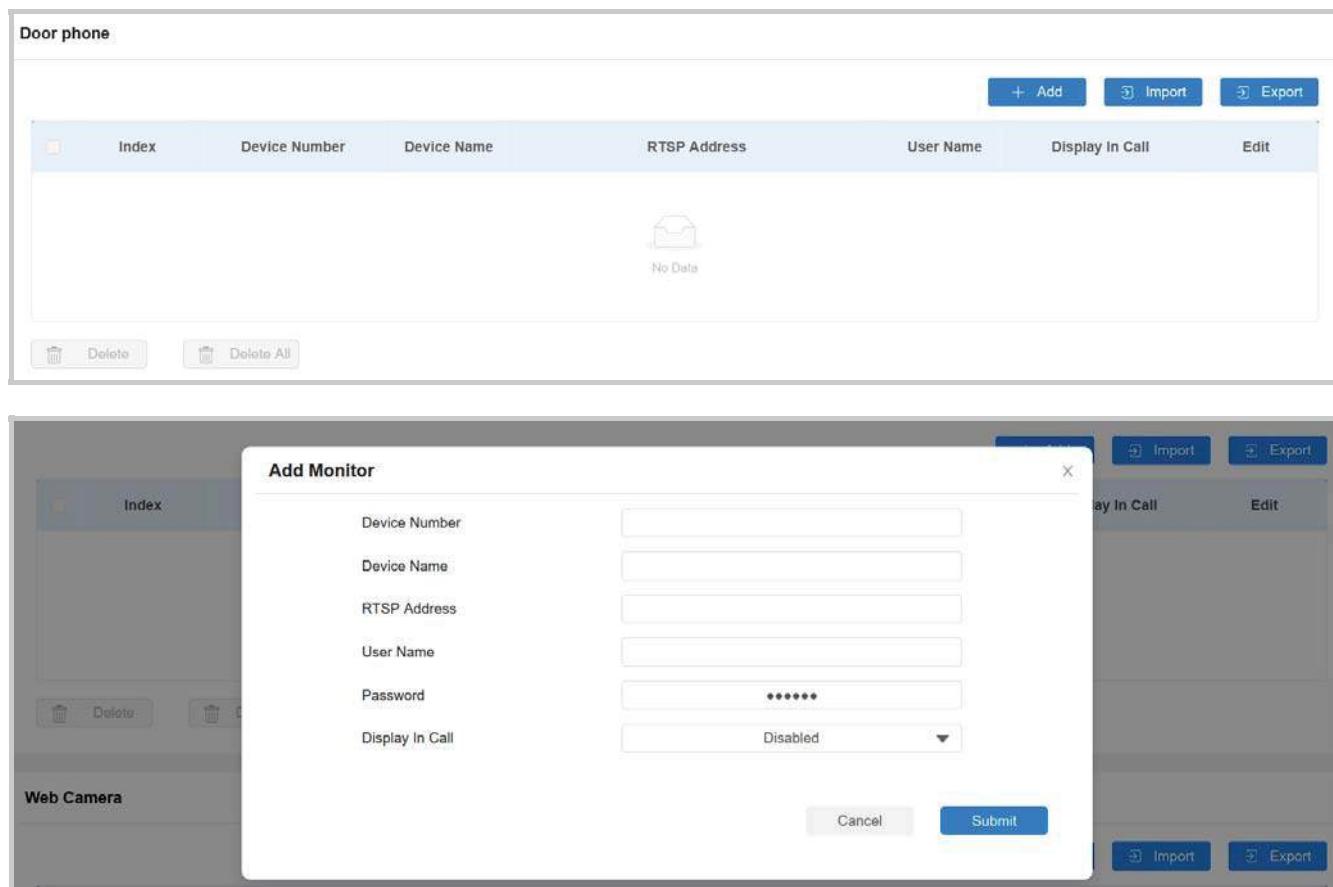
Security

Monitor and Image

Monitor Setting

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

To set it up, navigate to the web **Device > Monitor** interface. Click **+Add** to add a monitor.

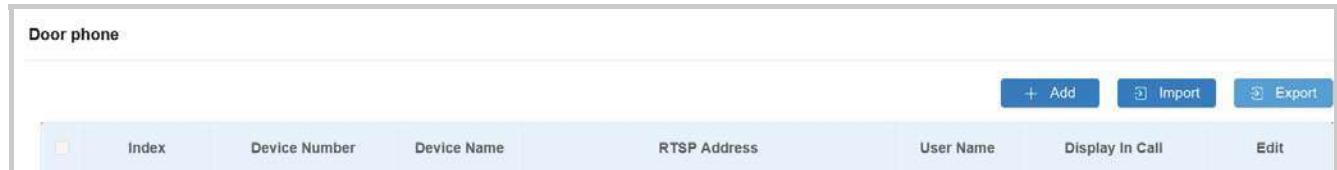


The image shows two screenshots of the Akuvox web interface. The top screenshot displays a table titled 'Door phone' with columns: Index, Device Number, Device Name, RTSP Address, User Name, Display In Call, and Edit. A message 'No Data' is shown in the table area. The bottom screenshot shows a modal dialog box titled 'Add Monitor' with fields for Device Number, Device Name, RTSP Address, User Name, Password (with a masked value), and Display In Call (set to 'Disabled'). The background shows a list of devices under 'Web Camera'.

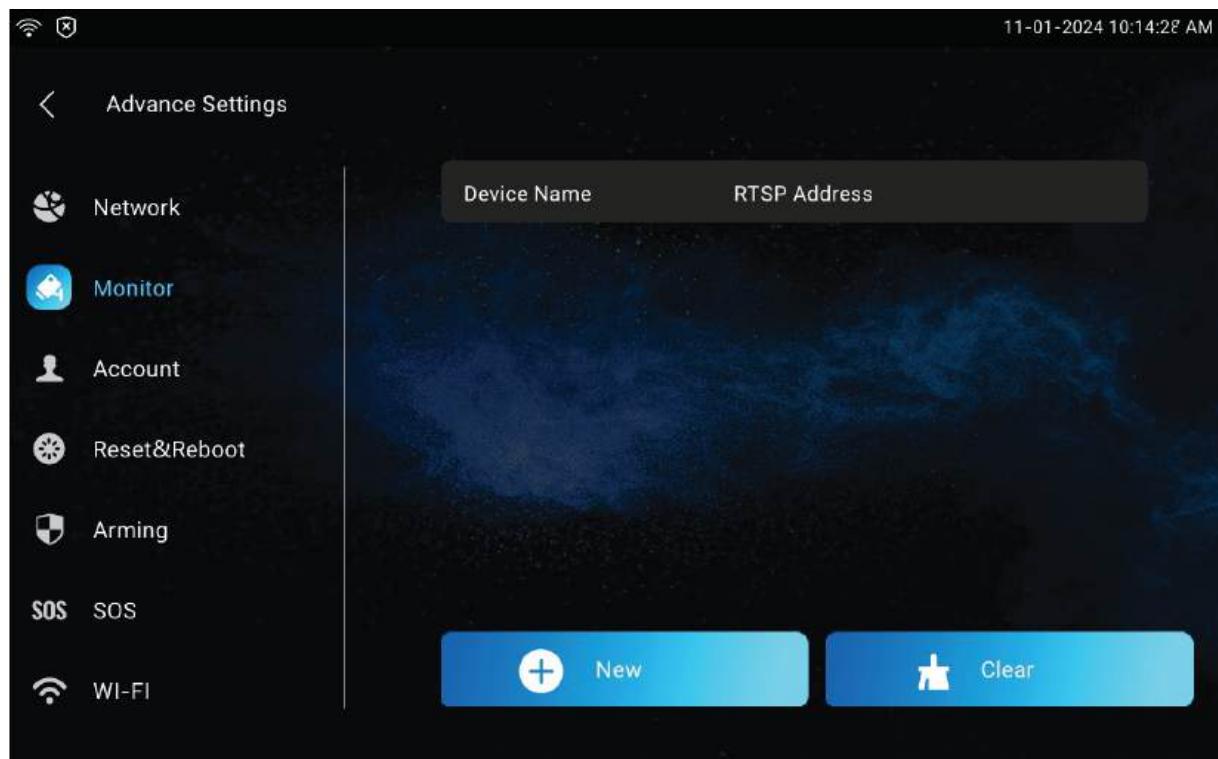
- **Device Number:** The device's SIP/IP number for identification.
- **Device Name:** The device name for identification.
- **RTSP Address:** The RTSP address of the monitoring device. RTSP format: rtsp://Device IP address/live/ch00_0.
- **Username:** The username of the monitoring device for authentication.

- **Password:** The password of the monitoring device for authentication.
- **Display In Call:** Enable it to display the monitoring video during a call.

You can export the monitoring device settings in a TGZ file and import a file in XML format.



Monitor feature can also be set up on the device **Settings > Advance Settings > Monitor** screen.



Web Camera Setting

You can configure the monitor feature for third-party cameras on the web **Device > Monitor > Web Camera** interface.

Index	Device Name	RTSP Address	Edit
No Data			

1/1 1

AddCamera

Device Name	<input type="text"/>
RTSP Address	<input type="text"/>

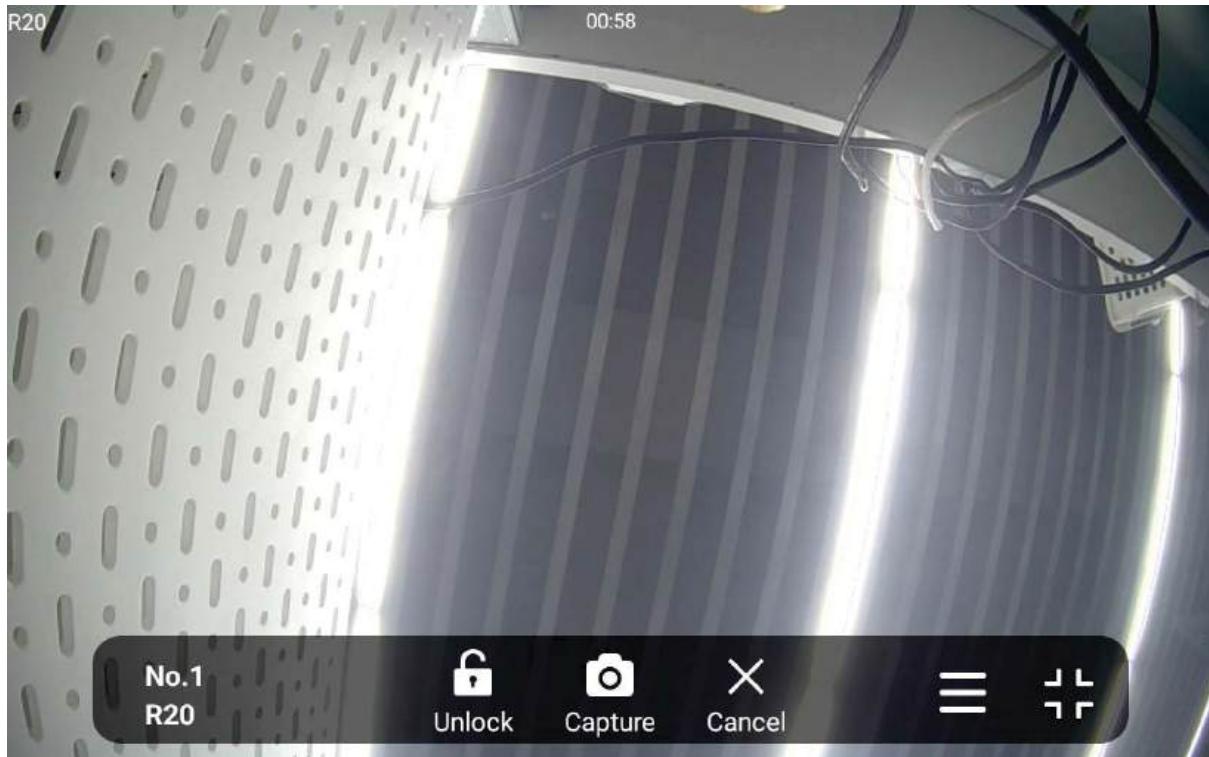
1/1 1

- **Device Name:** Set the name of the third-party camera.
- **RTSP Address:** Set the RTSP URL for the third-party camera.

You can import or export the monitor list in batch on the same interface. The export file is in TGZ format. The imported file only supports the XML format.

Video Image Capturing

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



RTSP Authentication

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

To set it up, navigate to the web **Settings > Basic** interface.

RTSP Setting	
RTSP Audio Enable	Disabled
Authorization Type	Basic
User Name	admin
Password	*****

- **Authorization Type:** There are three options, **Basic**, **Digest**, and **None**. **None** will allow all authorization types for the RTSP audio stream.
- **User Name:** Set the username for the authentication.
- **Password:** Set the password for the authentication.

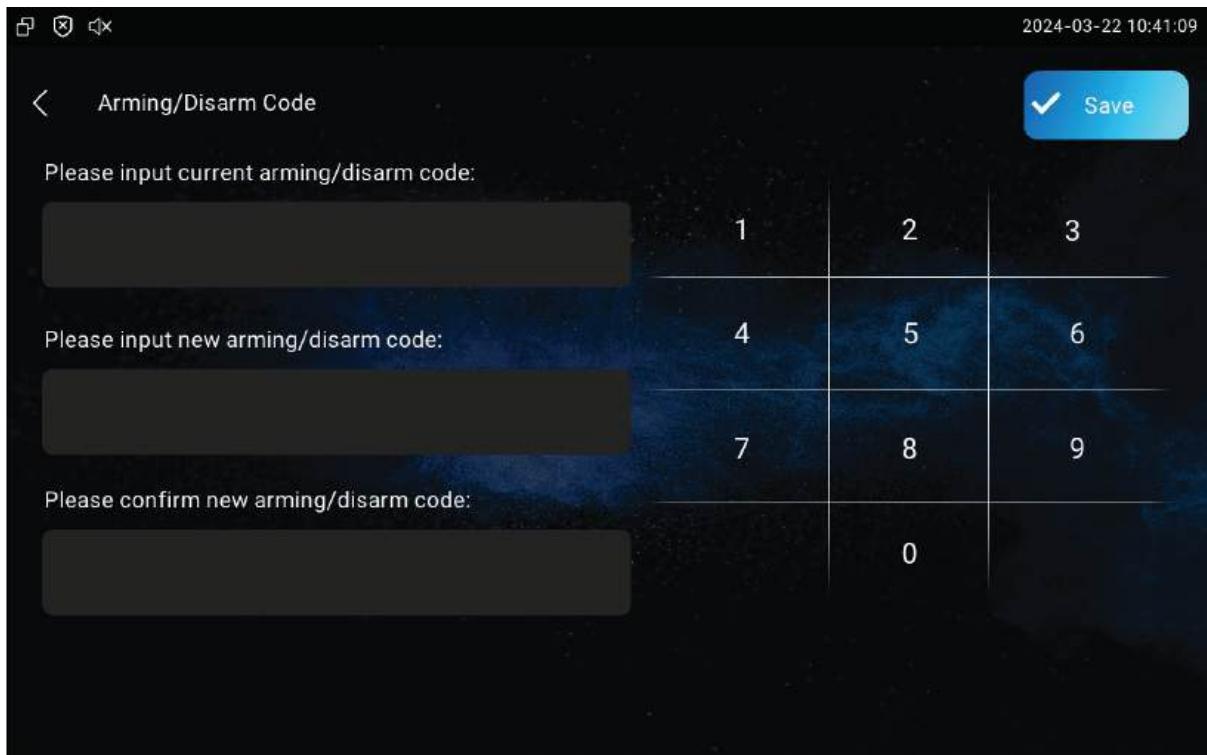
Alarm and Arming Configuration

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

Configure Alarm and Arming on the Device

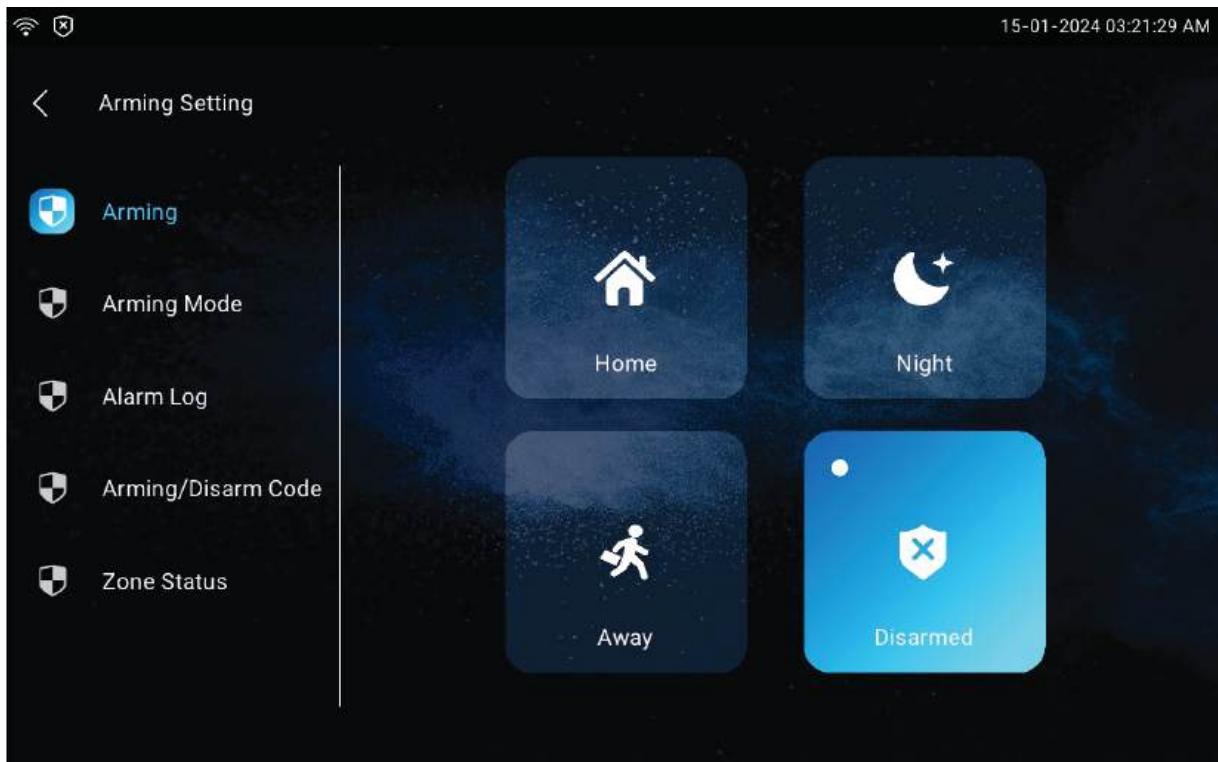
Set up Arming and Disarm Codes

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



Select an Arming Mode

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



Check Zone Status

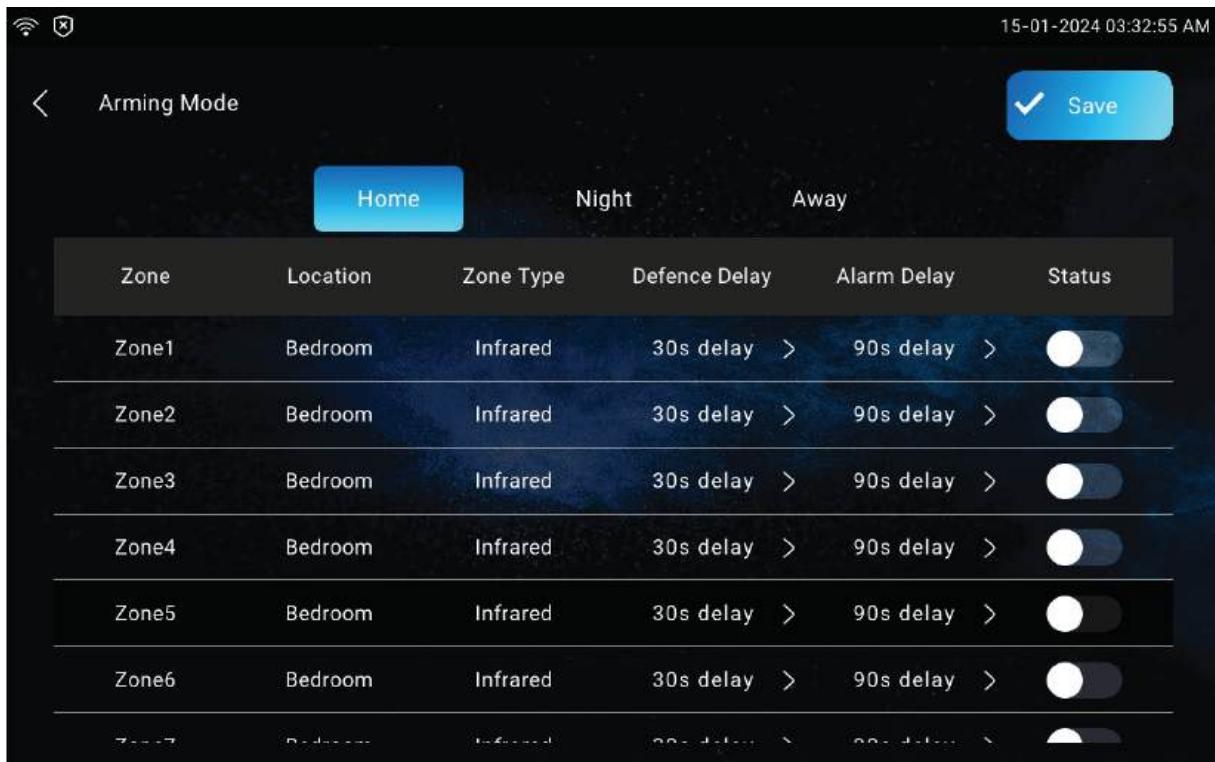
Check the zone status on the Arming > Zone Status screen.

The screenshot shows the 'Zone Status' screen. At the top is a header with icons and the date and time: '2024-03-22 10:43:54'. Below is a table with the following data:

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

Set up Alarm Sensors

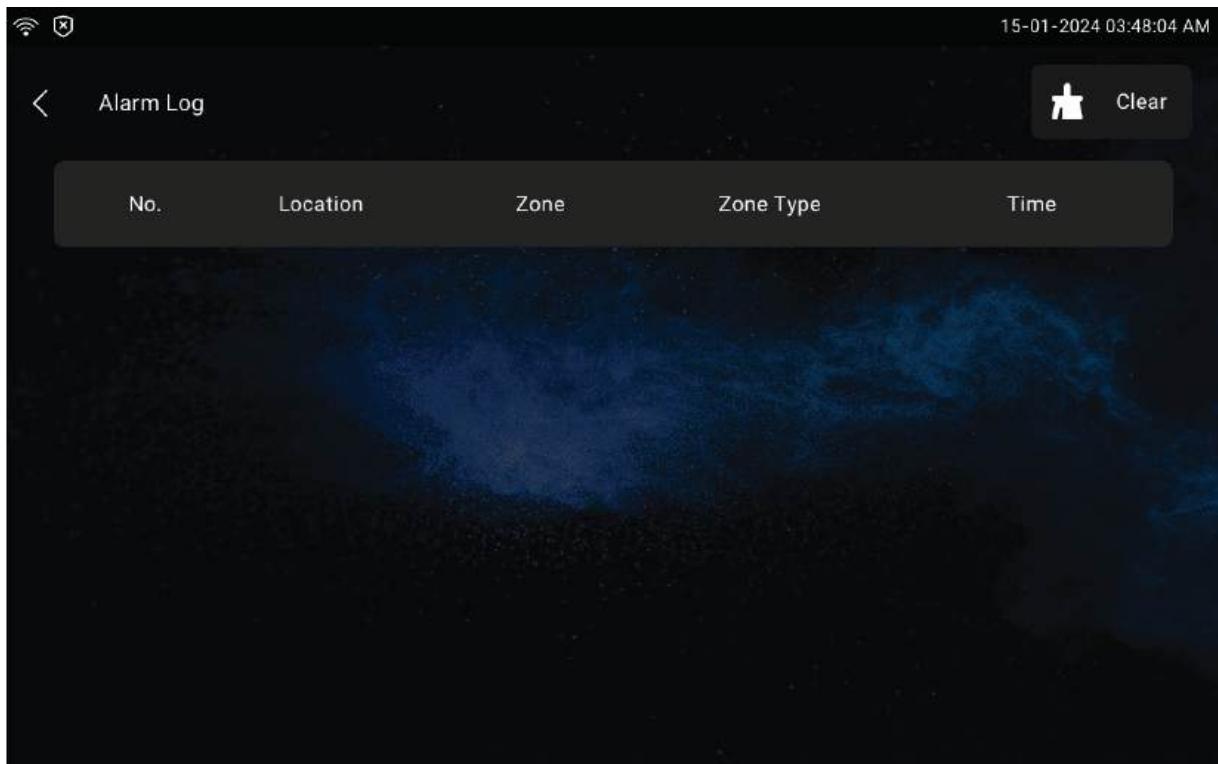
To configure the alarm sensor in different modes, go to the Arming > Arming Mode screen.



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

Check Alarm Logs

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



Configure Alarm and Arming on the Web Interface

Set up Arming and Disarm Codes

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

Disarm Code	
Current Password	<input type="text"/>
New Password	<input type="text"/> length must be 1-10
Confirm Password	<input type="text"/> match with new pwd
Disarm Setting	
Disarm Interval (Sec)	<input type="text"/> Never <input type="button" value="▼"/>

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

Select an Arming Mode

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

Arming Mode

Mode	Disarm
------	--------

Set up Location-based Alarm Sensors

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

Zone Setting

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

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

Set up Alarm Sensors in Different Arming Modes

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

Home						
Zone	Location	Zone Type	Defence Delay		Alarm Delay	Status
Zone1	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone2	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone3	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone4	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone5	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone6	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone7	Bedroom	Infrared	30Sec	▼	90Sec	▼
Zone8	Bedroom	Infrared	30Sec	▼	90Sec	▼

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

Configure Alarm Text

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

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

Customized Alarm		
Customized Alarm Enabled		
Zone		Alarm Content
Zone1		Alarm was triggered
Zone2		Alarm was triggered
Zone3		Alarm was triggered
Zone4		Alarm was triggered
Zone5		Alarm was triggered
Zone6		Alarm was triggered
Zone7		Alarm was triggered
Zone8		Alarm was triggered

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

Alarm Action Configuration

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

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

Configure Alarm Action via HTTP Command

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

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

- **Send HTTP:** Enable it if you want the action to be implemented on a designated third-party device.

- **HTTP Command:** Enter the HTTP command provided by the third-party device manufacturer.

Configure Alarm Action via SIP Message

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

SIP Message Setting

SIP Message Setting		
Zone	SIP Message	Send Sip Message
Zone1	<input type="text"/>	Disabled
Zone2	<input type="text"/>	Disabled
Zone3	<input type="text"/>	Disabled
Zone4	<input type="text"/>	Disabled
Zone5	<input type="text"/>	Disabled
Zone6	<input type="text"/>	Disabled
Zone7	<input type="text"/>	Disabled
Zone8	<input type="text"/>	Disabled

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

Configure Alarm Action via SIP Call

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

Call Setting

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

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

Configure Alarm-Triggered Local Relay

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

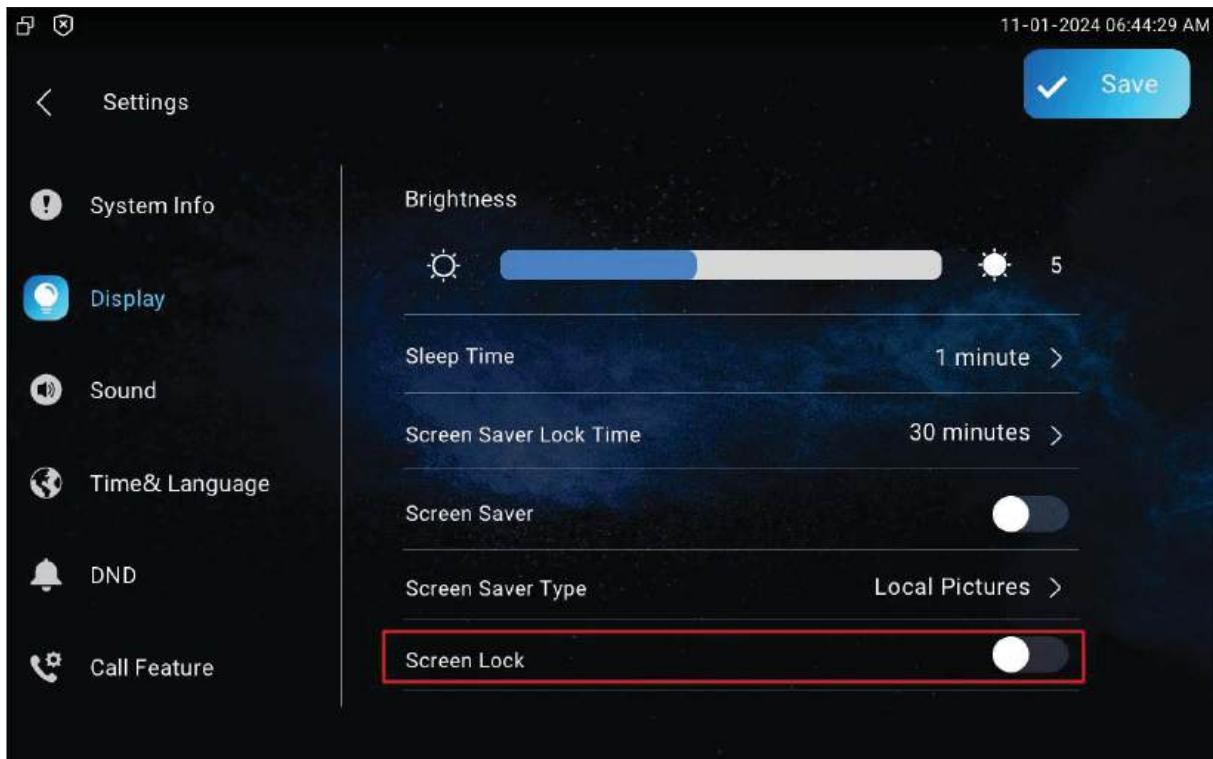
Local Relay

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

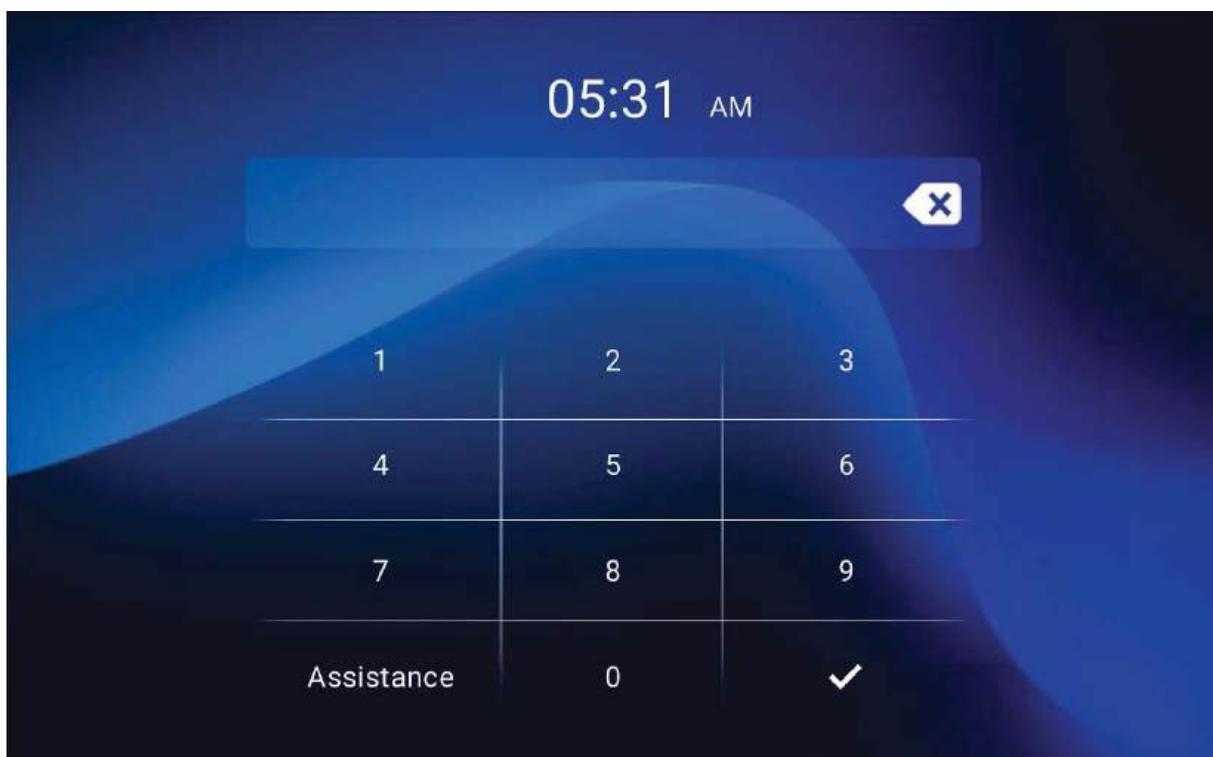
Screen Unlock Setting

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

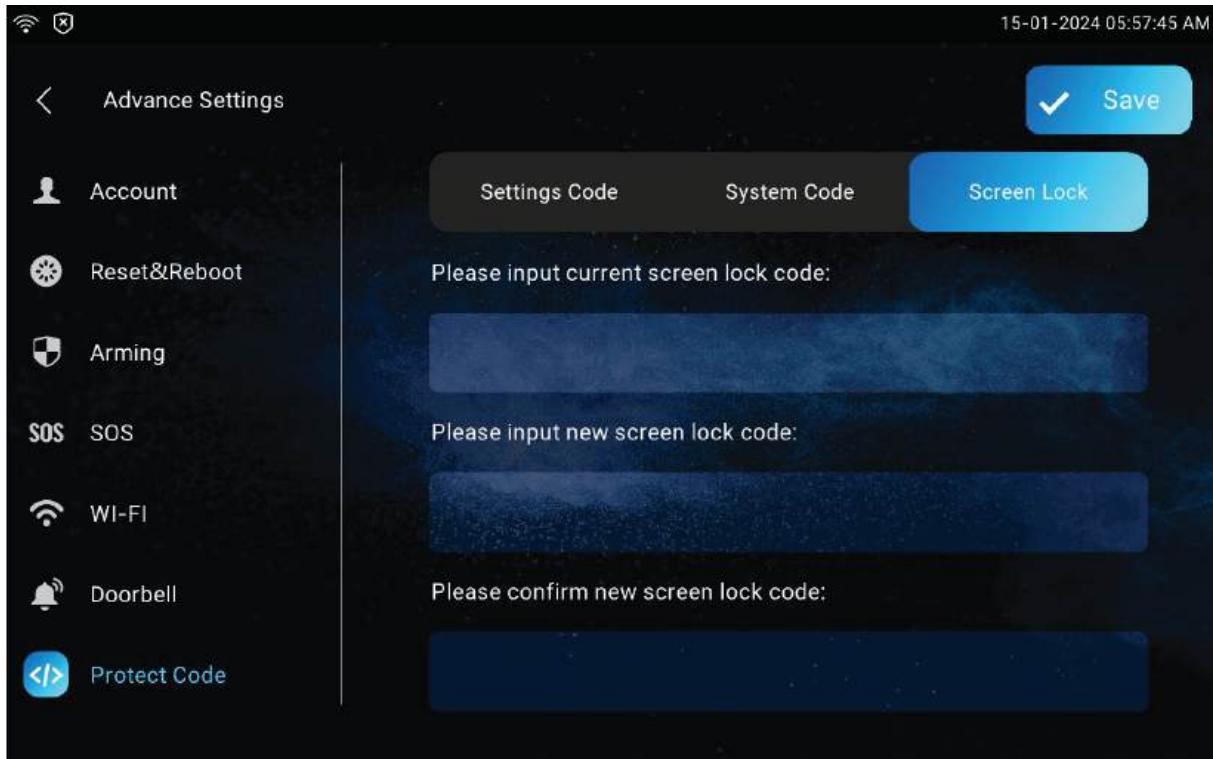
The screen unlock feature can be enabled directly on the device **Settings > Display** screen.



The default PIN code is empty. Tap the ✓ icon to unlock the screen.



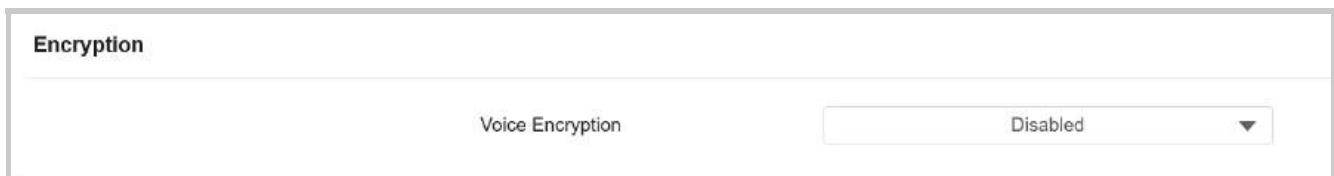
To change the screen lock password, navigate to the device **Settings > Advance Settings > Protect Code > Screen Lock** screen.



Voice Encryption

Secure Real-time Transport Protocol (SRTP) is a protocol derived from the Real-time Transport Protocol (RTP). It enhances the security of data transmission by providing encryption, message authentication, integrity assurance, and replay protection.

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



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

- **ZRTP(Optional):** The protocol that the two parties use to negotiate the SRTP session key.

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.

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

Session Time Out		
Session Time Out Value	300	(60-14400Sec)

Power Output Setting

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

To enable it, navigate to the web **Settings > Basic > Power Output Enable** interface.

Power Output Setting		
Power Output Enable	Disabled	▼

High Security Mode

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

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

High Security Mode		
Enabled	<input checked="" type="checkbox"/>	

Important Notes

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

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

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

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

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

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

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

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

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

Lift Control

Users can summon a lift via the lift control feature.

Configure Lift Control

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

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

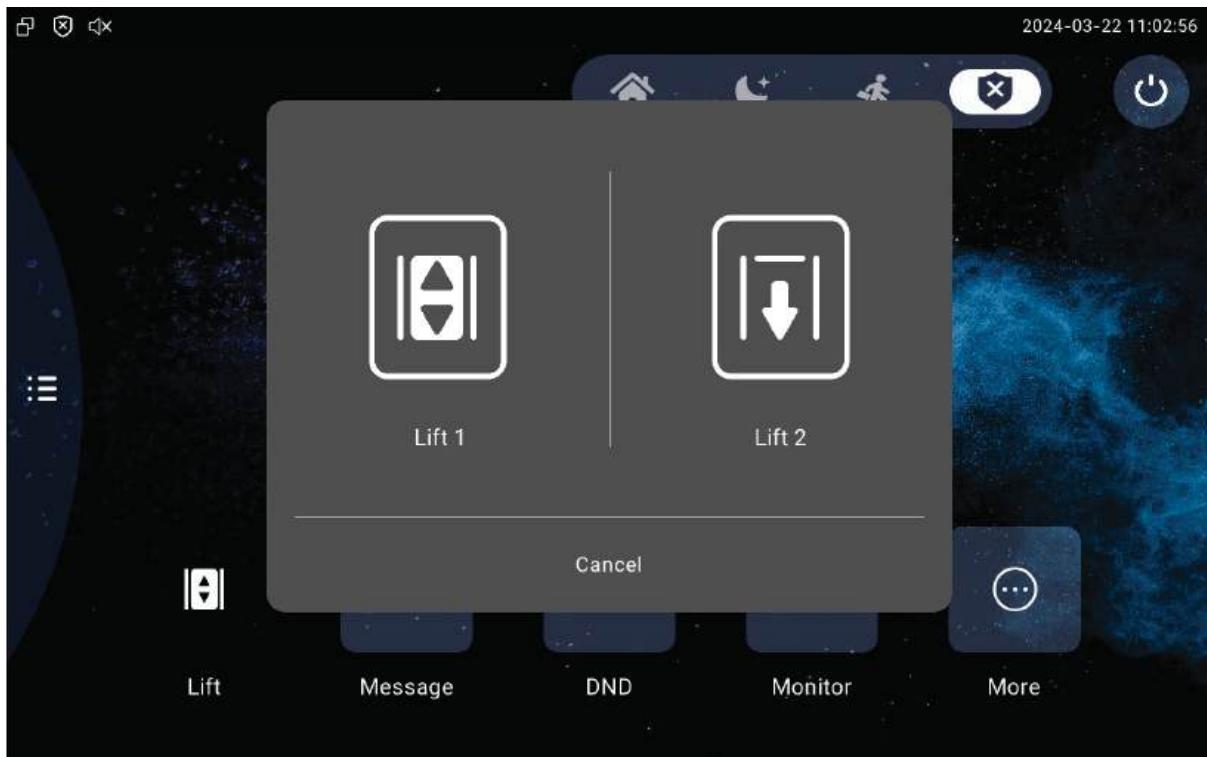
Home Page Display					Example
Area	Type	Value	Label	Icon(max size:100*100)	
Area1	Lift		Lift	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area2	Message		Message	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>
Area3	DND		DND		
Area4	Monitor		Monitor	Not selected any files	<input type="button" value="Select File"/> <input type="button" value="Delete"/>

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

Lift Control					
Name	Status	Icon	Label	Http Command	
Lift1	Disabled	Up	Lift 1	http://	
Lift2	Disabled	Down	Lift 2	http://	

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

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



Configure Lift Control Prompt

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

To set it up, navigate to the web Device > Lift > Hints interface. Click **+Add** to add a prompt and click the **Edit** icon to modify the desired prompt.

The screenshot shows a table titled 'Hints' with the following data:

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

At the bottom of the table, there are buttons for 'Delete' and 'Delete All' (in red), and navigation buttons for 'Prev.', '1/1', 'Next', 'Go To Page' (set to 1), and 'Go'.

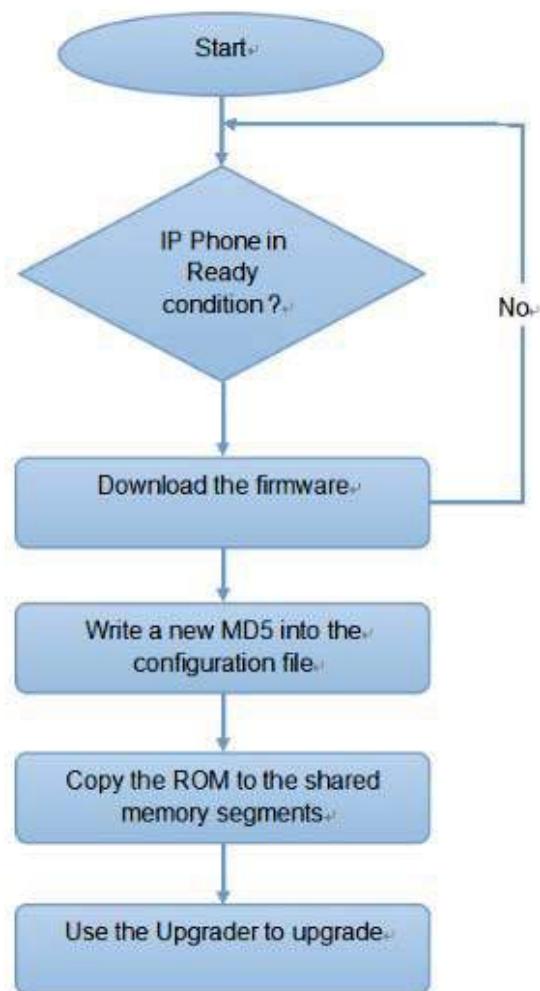
If there are huge amounts of prompts that need to be added, you can click the **Export** tab to export a template and import the file after editing. The export file is in TGZ file and the import file should be in XML file.

Auto-provisioning via Configuration File

Provisioning Principle

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

Please see the flow chart below:



Introduction to the Configuration Files for Auto-Provisioning

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

The difference between the two types of configuration files:

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

Note

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

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

Autop Schedule

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

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

Automatic Autop

Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	 Clear
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:** Combine **Power On** mode and **Repeatedly** mode that will enable the device to perform Autop every time it boots up or according to the schedule.
- **Hourly Repeat:** The device will perform Autop every hour.

Static Provisioning Configuration

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

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

Automatic Autop

Mode: Power On

Schedule: Sunday, 22:00 (0-23Hour), 0 (0-59Min)

Clear MD5: Clear

Export Autop Template: Export

Manual Autop

URL:

User Name:

Password: (*****)

Common AES Key: (*****)

AES Key(MAC): (*****)

AutoP Immediately:

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

Note

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

Tip

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

PNP Configuration

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

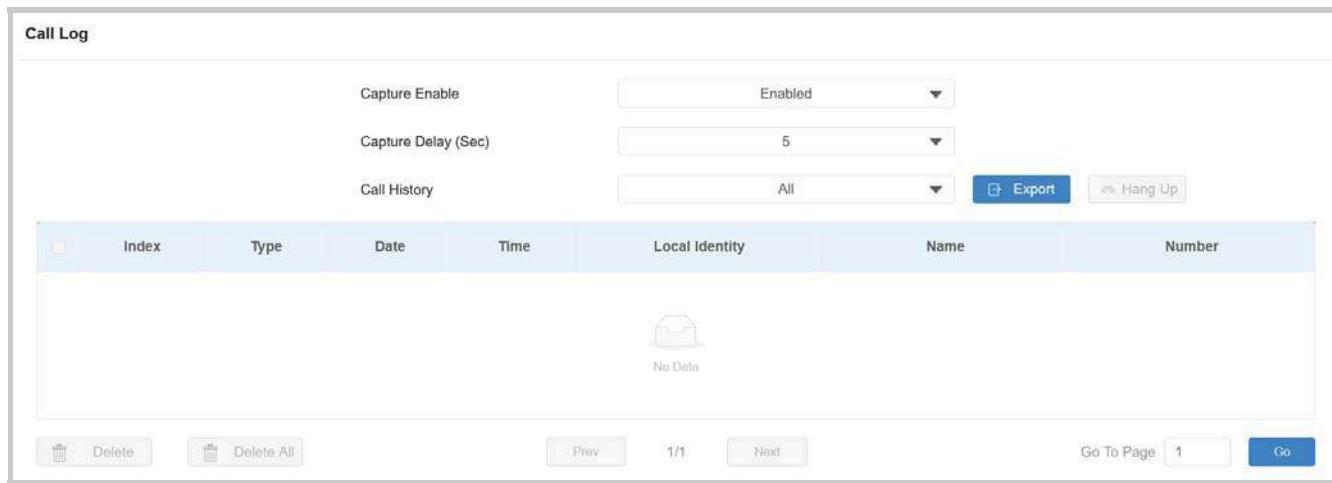
To enable the function, go to the **Upgrade > Advanced > PNP Option** interface.

PNP Option	
PNP Config Enabled	<input checked="" type="checkbox"/>

Call Logs

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

To set it up, navigate to the web **Contacts > Call Log** interface.



Index	Type	Date	Time	Local Identity	Name	Number
No Data						

- **Capture Delay(Sec):** Set the image capturing starting time when the device goes into a video preview.
- **Call History:** There are five types of call history, All, Dialed, Received, Missed, and Forwarded.
- **Local Identity:** Display the device's SIP account or IP number that receives incoming calls.

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



Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

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

Basic

Firmware Version	565.30.10.27
Hardware Version	565.0.2.0.1.0.0.0
Upgrade	 Import
Reset To Factory Setting	 Reset
Reset Config To Factory Setting	 Reset
Reboot	 Reboot

Note

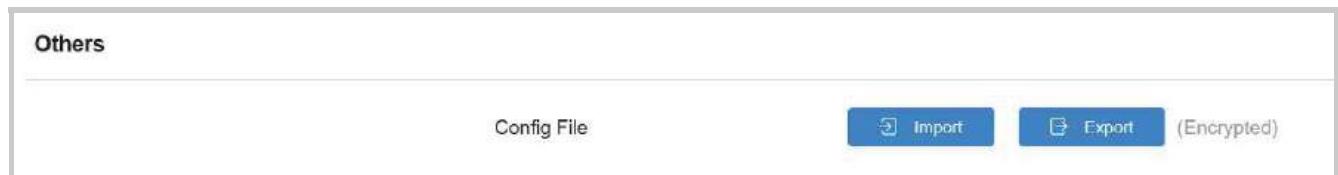
Firmware files should be **.rom** format for the upgrade.

Backup

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

To export the file, navigate to the **Upgrade > Advanced > Others** interface. The export file is in the TGZ file.

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

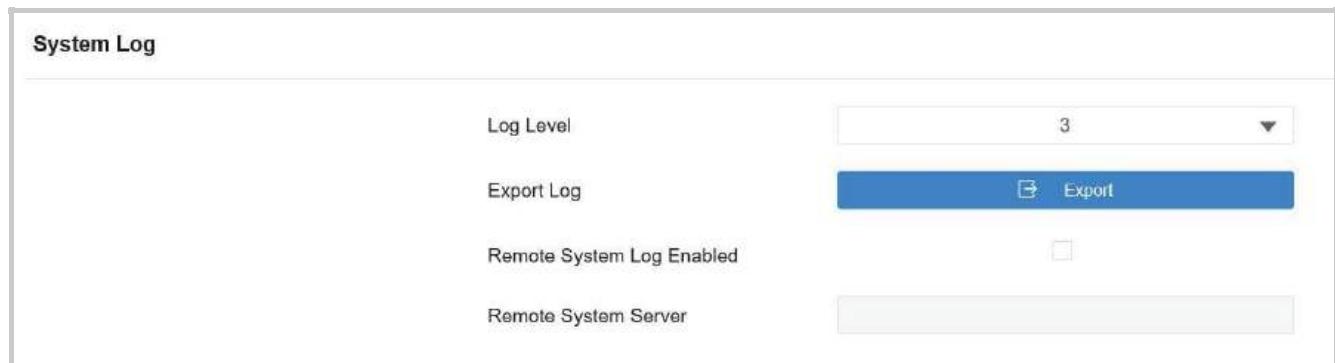


Debug

System Log for Debugging

System logs can be used for debugging purposes.

To set it up, navigate to the web **Upgrade > Diagnosis** interface.

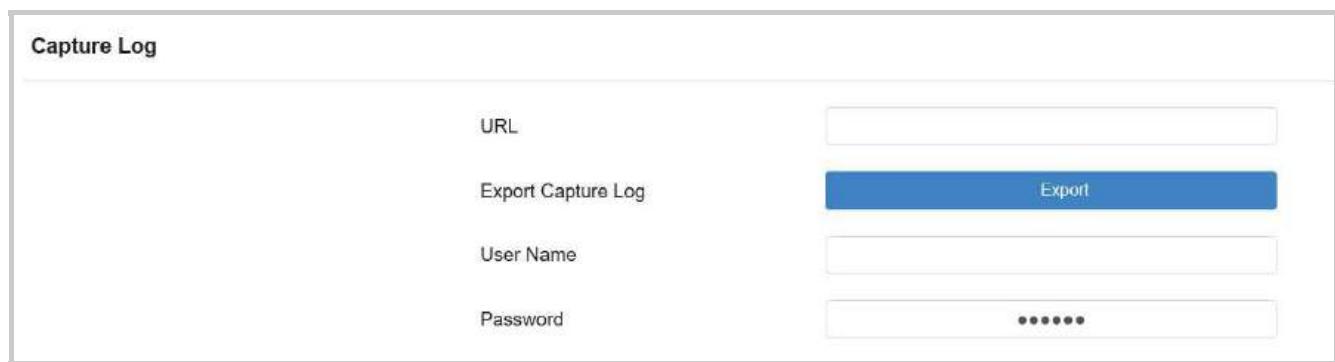


The screenshot shows a 'System Log' configuration page. It includes a dropdown menu for 'Log Level' set to 3, a blue 'Export' button with a file icon, a checkbox for 'Remote System Log Enabled' which is unchecked, and a text input field for 'Remote System Server'.

- **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 will be provided by Akuvox technical support.

Capture Log for Debugging

Navigate to the web **Upgrade > Diagnosis > Capture Log** interface.



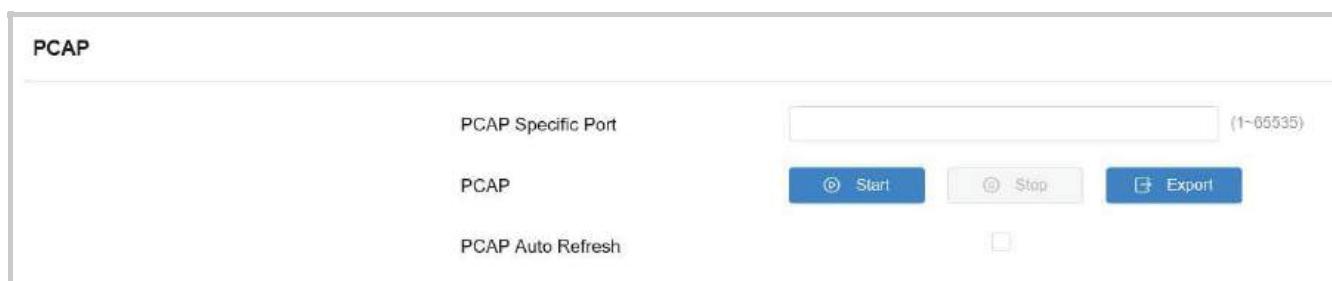
The screenshot shows a 'Capture Log' configuration page. It includes a text input for 'URL', a blue 'Export' button with a file icon for 'Export Capture Log', a text input for 'User Name', and a text input for 'Password' with a masked display.

- **URL:** Set the server address to receive the capture log.
- **Export Capture Log:** Click Export to export the capture log to the local PC.
- **User Name:** Set the username to access the server.
- **Password:** Set the password to access the server.

PCAP for Debugging

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

Navigate to the web **Upgrade > Diagnosis > PCAP interface.**

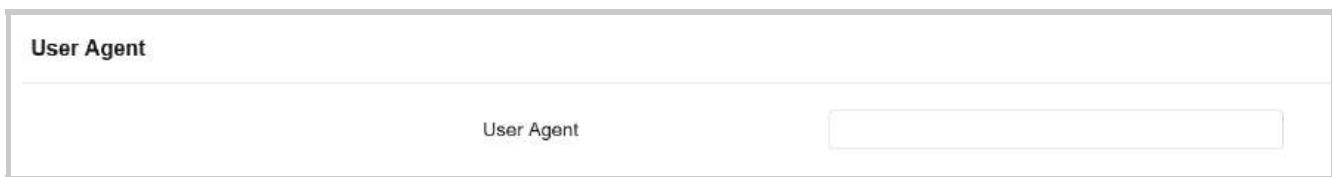


- **PCAP Specific Port:** Select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** 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.

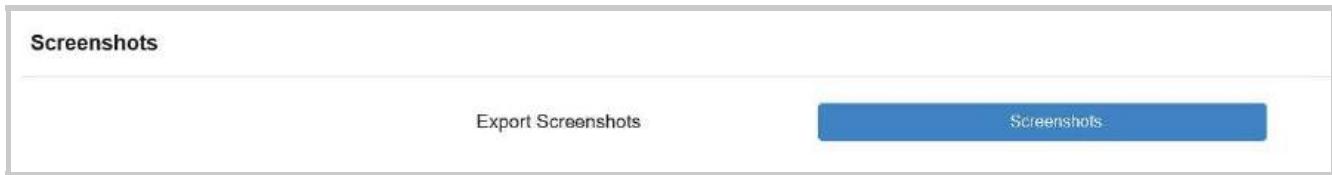
To set it up, go to the web **Account > Advanced > User Agent** interface.



Screenshots

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

To take screenshots, go to **Upgrade > Diagnosis > Screenshots** interface, then click **Screenshots**.



Device Integration with Third Party

Smart Living Setting

You can control the home sensor through an HTTP command. You can add up to 8 control buttons.

Navigate to the web **Device > Smart Living** interface.

Smart Living					
Name	Status	Icon	Label	Http Command	
Button1	Disabled	Scene	Button1	http://	▼
Button2	Disabled	Scene	Button2	http://	▼
Button3	Disabled	Scene	Button3	http://	▼
Button4	Disabled	Scene	Button4	http://	▼
Button5	Disabled	Scene	Button5	http://	▼
Button6	Disabled	Scene	Button6	http://	▼
Button7	Disabled	Scene	Button7	http://	▼
Button8	Disabled	Scene	Button8	http://	▼

- Status:** Enable or disable this button. If disabled, the button won't appear on the home control screen.
- Icon:** If **Scene** is selected, the icon is displayed as . If **Light** is selected, the icon will be .
- Label:** Customize the button display name.
- HTTP command:** Set the HTTP command to trigger the sensor.

Note

To configure Smart Living button, go to the **Device > Display Setting** web interface.

Integration with Control 4

You need to enable the Control 4 mode before you can integrate the device with the Control 4 home center. To enable it, go to **Network > Advanced > Connect Setting** mode.

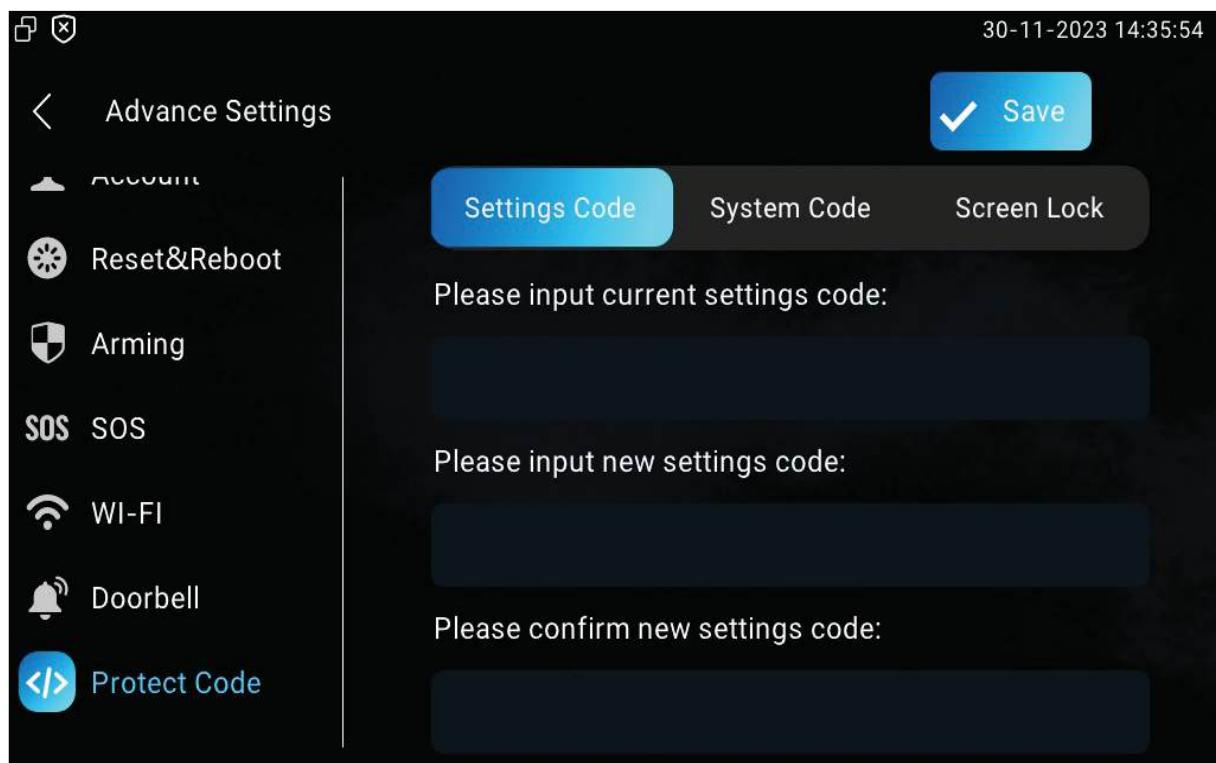
Connect Setting

Connect Mode	SDMC
Discovery Mode	<input checked="" type="checkbox"/>
Control4 Mode	<input type="checkbox"/>
Device Node	1 1 1 1 1
Device Extension	1 (1-9)
Device Location	Indoor Monitor

Password Modification

Modify Device Basic Setting Password

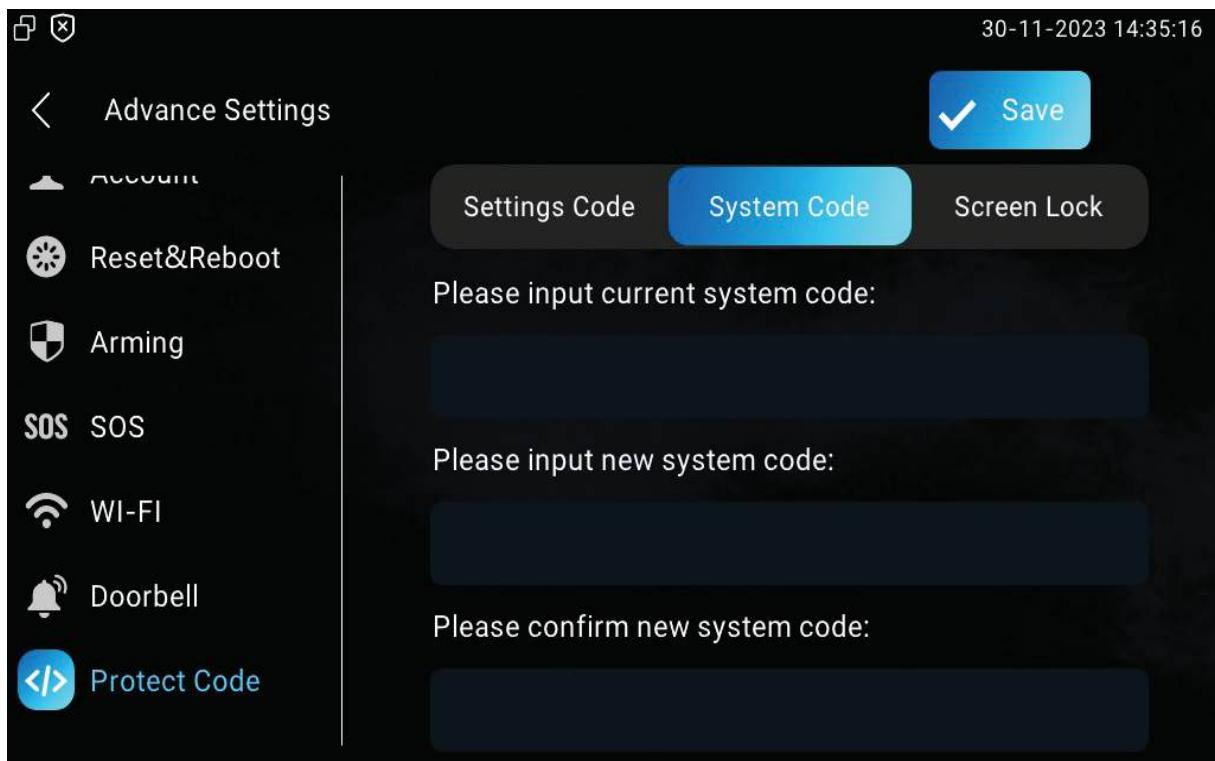
The Settings Code is used to access the device's basic settings. To modify it, go to the **Settings > Advance Settings > Protect Code** screen. The default password is empty.



Modify Device Advance Setting Password

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

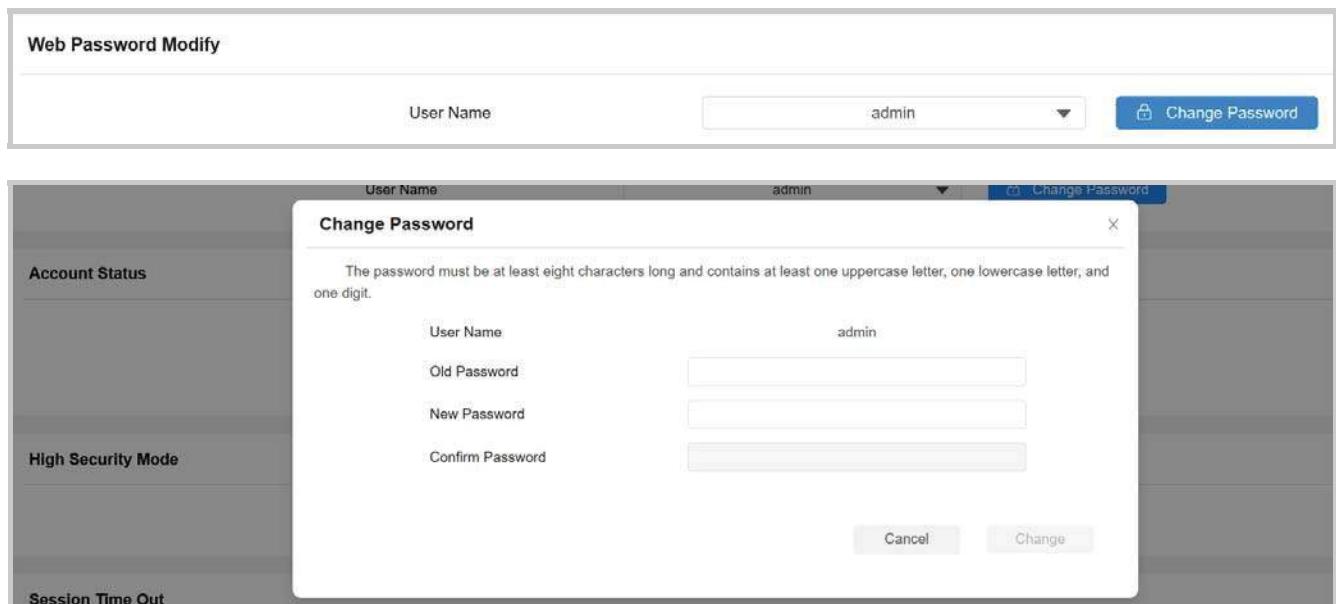
To modify it, navigate to the **Settings > Advance Settings > Protected Code** screen



Modify Device Web Interface Password

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

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



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

Account Status

admin

Enabled

user



Note

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

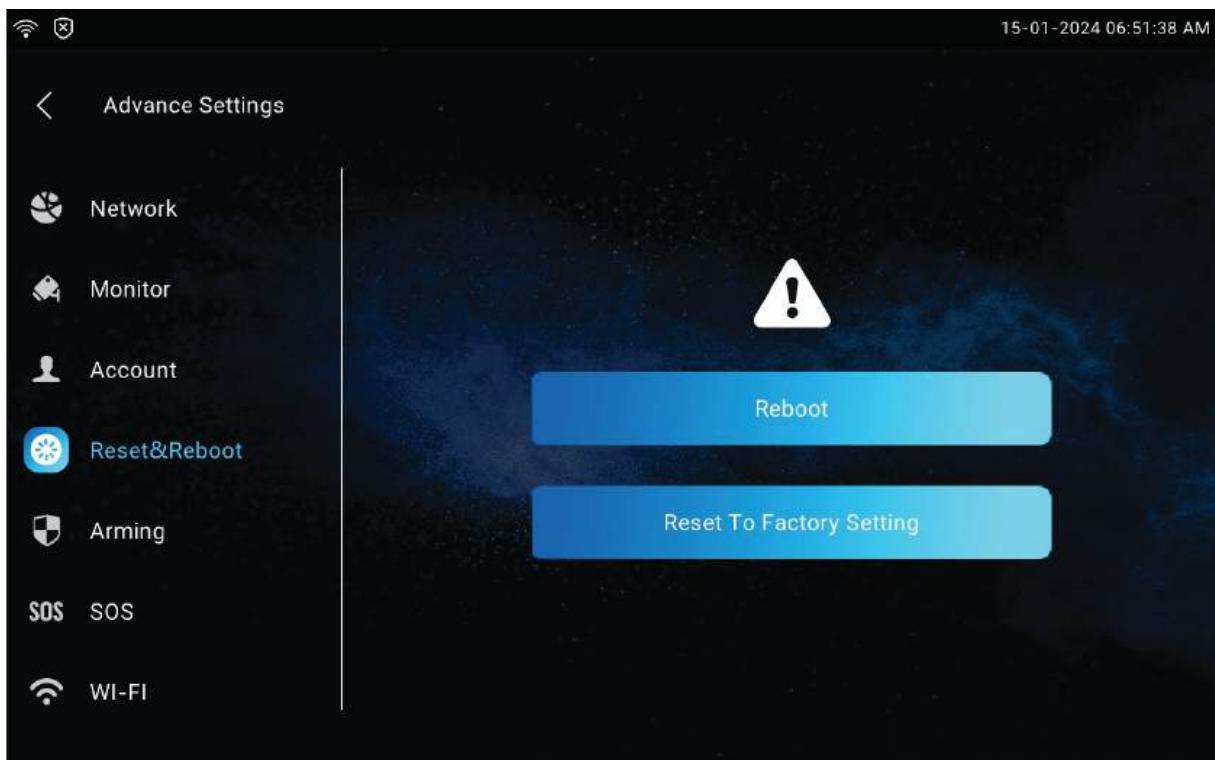
System Reboot & Reset

Reboot

Reboot on the Device

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

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



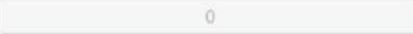
Reboot on the Web Interface

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

Reboot the device on the web **Upgrade > Basic interface**.

Basic	
Firmware Version	565.30.10.27
Hardware Version	565.0.2.0.1.0.0.0
Upgrade	 Import
Reset To Factory Setting	 Reset
Reset Config To Factory Setting	 Reset
Reboot	 Reboot

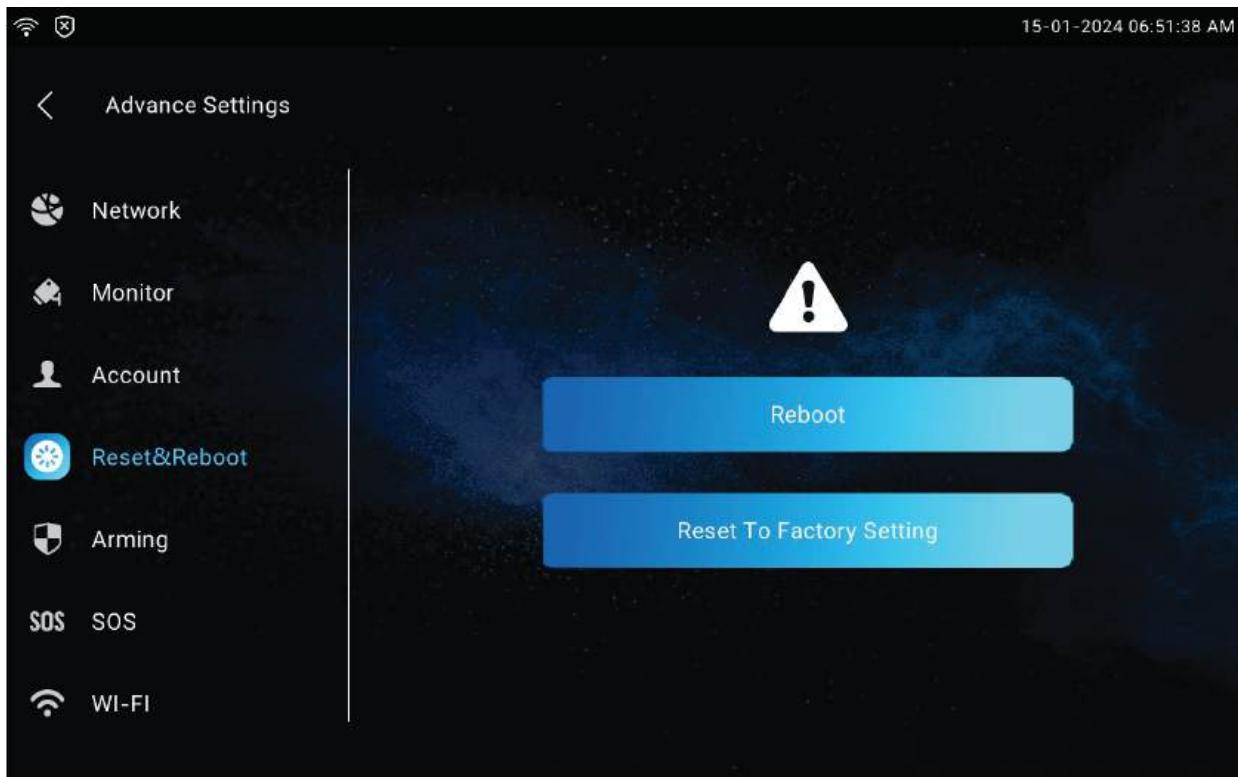
To set up the device restart schedule, go to the **Upgrade > Advanced > Reboot Schedule** interface.

Reboot Schedule	
Mode	<input type="checkbox"/>
Schedule	 Every Day 
	 0 <small>(0-23Hour)</small>

Reset

Reset on the Device

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



Reset on the Web Interface

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

Go to the web **Upgrade > Basic** interface. If you only want to reset the configuration file to the factory setting instead of the whole device system, click **Reset Config To Factory Setting**.

Basic	
Firmware Version	565.30.10.27
Hardware Version	565.0.2.0.1.0.0.0
Upgrade	Import
Reset To Factory Setting	Reset
Reset Config To Factory Setting	Reset
Reboot	Reboot



FCC Caution:

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

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

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

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

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

FCC Radiation Exposure Statement:

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

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

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