Akuvox

Table of contents

Akuvox S562 Series Indoor Monitor Administrator Guide

About This Manual 9

Product Overview 11

Changelog 12

Model Specification 13

Introduction to Configuration Menu 14

Access the Device 16

- Device Start-up Network Selection 16
- Device Home Screen Type Selection 16
- Access the Device Settings 17
  - Access Device Basic Settings 18
  - Access Device Advance Settings 18
- Access the Device Web Settings 19

Language and Time 22

- Language 22
  - On the Device 22
  - On the Web Interface 23

Time 23
On the Device 23
On the Web Interface 24
Daylight Saving Time 25
Sound and Volume 27
On the Device 27
On the Web Interface 28
Upload Tones 29
Bell Setting 29
Screen Display 31
On the Device 31
On the Web Interface 33
Upload Screen Saver 34
Upload Wallpaper 35
Upload Device Booting Image 35
Home Screen Display 35
Home Screen Tab Display 37
Unlock Tab Configuration 38
Function Display on the Settings Screen 40
Temperature Display Setting 41

Network Setting 43
Device Network Configuration 43
On the Device 43
On the Web Interface 44
Device Deployment in Network 46
Device NAT Setting 48
Device Web HTTP Setting 49
Device Wi-Fi Setting 49
VLAN Setting 50
SNMP Setting 51
Contacts Configuration 52
On the Device 52
Add Local Contacts 52
Edit Contacts 53
Blocklist Contacts 54
On the Web Interface 56
Add Local Contacts 56
Import and Export Contacts 57
Contact List Display 57
Intercom Call Configuration 59

IP Call Configuration 59
Make IP Calls 59
IP Call Setup 60
SIP Call Configuration 61
SIP Account Registration 61
SIP Server Configuration 63
Outbound Proxy Server 65
SIP Call DND & Return Code Configuration 65
Device Local RTP 66
Data Transmission Type 67
SIP Hacking Protection 67
Call Setting 69
Auto-answer Configuration 69
Auto-answer Allowlist Setting 70
Intercom Preview 72
Emergency Call 72
Multicast 74
Call Forwarding 75
On the Device 75
On the Web Interface 76

Call Logs 78
Intercom Message Setting 80
Manage Messages 80
Audio & Video Codec Configuration for SIP Calls 81
Audio Codec Configuration 81
Video Codec Configuration 82
Access Control Configuration 83
Local Relay 83
Remote Relay 84
Web Relay 85
Door-opening Configuration 87
Unlock by DTMF Code 87
Unlock via HTTP Command 89
Security 92
Monitor and Image 92
Monitor Setting 92
Web Camera Setting 95
View Monitoring Streams 96
Monitor Lock 97
RTSP Authentication 99

Alarm and Arming Configuration 100
Set up Location-based Alarm Sensors 100
Select an Arming Mode 102
Set up Alarm Sensors in Different Arming Modes 103
Set up the Disarm Codes 104
Check Zone Status 105
Check Alarm Logs 106
Configure Alarm Text 107
Configure Alarm Ringtone 107
Alarm Action Configuration 108
HTTP Command 108
SIP Message 108
SIP Call 109
Local Relay 110
Screen Unlock Setting 110
Screen Unlock by PIN Code 111
Voice Encryption 112
Web Interface Automatic Log-out 113
Power Output Setting 113
High Security Mode 114

Lift Control 116
Set Lift Control Icon 116
Set Lift Control Prompt 117
Integration with Third-party Devices 118
Smart Living Setting 118
Integration with Control4 119
Integration via External Relay 120
Auto-provisioning 122
Provisioning Principle 122
Configuration Files for Auto-Provisioning 123
Autop Schedule 124
Static Provisioning 124
PNP Configuration 126
Firmware Upgrade 127
Backup 129
Debug 130
System Log for Debugging 130
PCAP for Debugging 130
Remote Debug Server 131
User Agent 132

Capture Log 132
Web Call 132
Screenshots 133
Network Detection 133
Password Modification 135
Modify Device Basic Setting Password 135
Modify Device Advance Setting Password 135
Modify Device Web Interface Password 136
Modify Security Questions 137
System Reboot & Reset 139
Reboot 139
Reset 140

Akuvox

About This Manual

Akuvox
Open A Smart World

WWW.AKUVOX.COM



S562
INDOOR MONITOR
Administrator Guide

Akuvox

Thank you for choosing the Akuvox S562 series indoor monitor. This manual is intended for administrators who need to properly configure the indoor monitor. This manual is written based on firmware 562.30.16.144, and it provides all the configurations for the functions and features of the S562 series indoor monitor. Please visit the Akuvox website or consult technical support for any new information or the latest firmware.

Product Overview



The device can be connected to the Akuvox door phone for audio/video communication, unlocking, and monitoring. Residents can communicate with visitors via audio/video calls, and the system supports remote door opening. It is more convenient and safer for residents to check the visitor's identity through its video preview function. S562 series is often applied to scenarios such as villas, apartments, and buildings.

Changelog

What's new in version 562.30.16.144:

- Support the integration with Akuvox LED11.
- Support the Monitor Lock feature.
- Support selecting Remote Relay by HTTP as the unlock type .

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

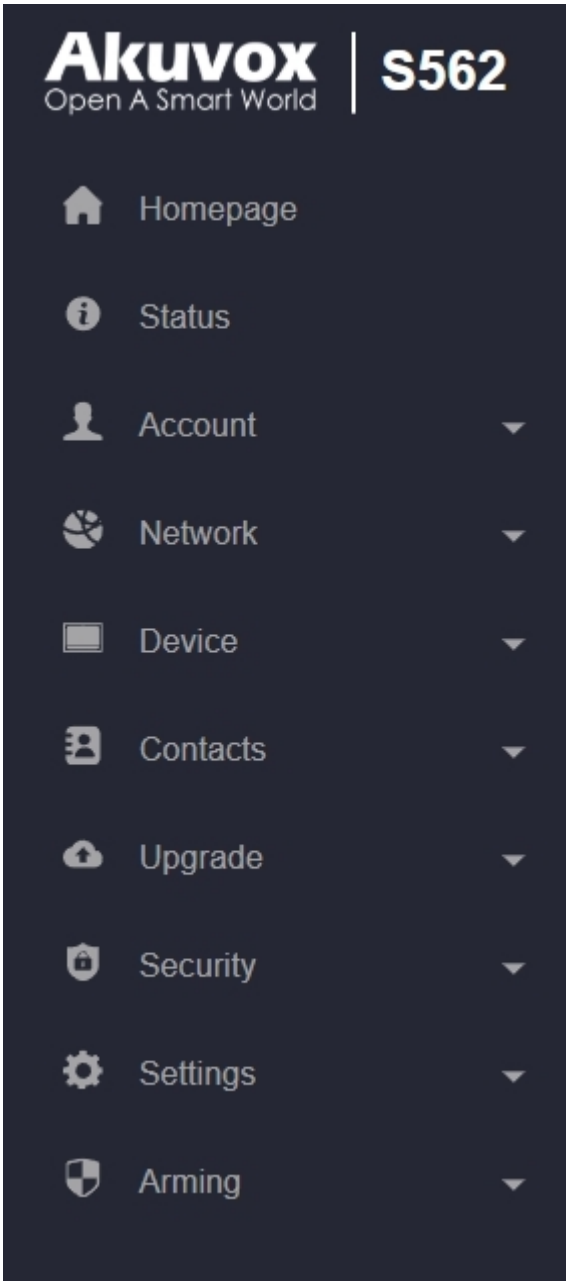
Model Specification

Model	S562
Touch Screen	✓
Resolution	1024x600
Wi-Fi	IEEE 802.11 b/g/n
Bluetooth	×
NFC	×
RS485	1
Alarm In	8

> **Note**
>
> Click here to download the device's datasheet.

Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network information, account information, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.
- **Network**: This section mainly deals with DHCP & Static IP settings, RTP port settings, device deployment, etc.
- **Device**: This section includes time & language, call feature, screen display, multicast, audio intercom feature, monitor, relay, lift import & export, door log, and web relay.
- **Contacts**: This section includes local contacts configuration and call logs.
- **Upgrade**: This section covers firmware upgrade, device reset and reboot, configuration file auto-provisioning, and PCAP.
- **Security**: This section is for password modification, account status, high-security mode switch, and session time-out configuration.
- **Settings**: This section includes the RTSP and power output.
- **Arming**: This section covers the configuration of arming zone, arming mode, disarm code, and alarm action.


Akuvox
Open A Smart World
S562
Homepage
Status
Account
Network
Device
Contacts
Upgrade
Security
Settings
Arming

Access the Device

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

Device Start-up Network Selection

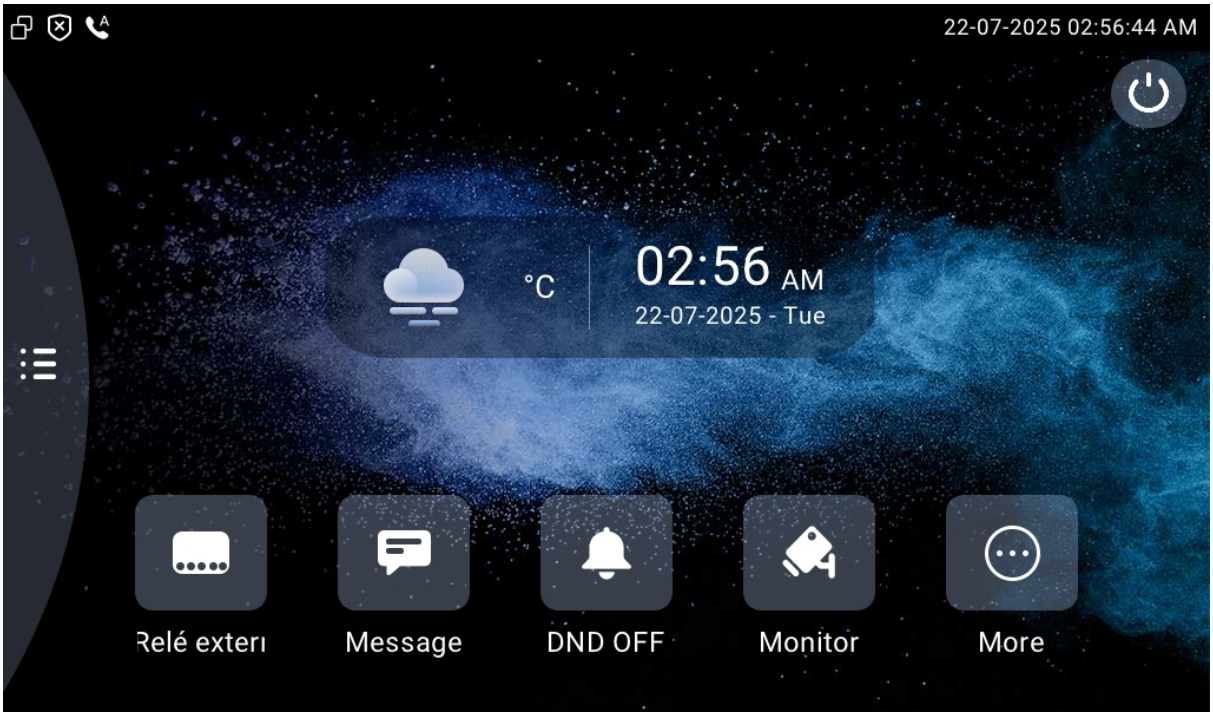
After the device boots up initially, you are required to select the network connection for the device. You can either select Ethernet or Wireless network connection.

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

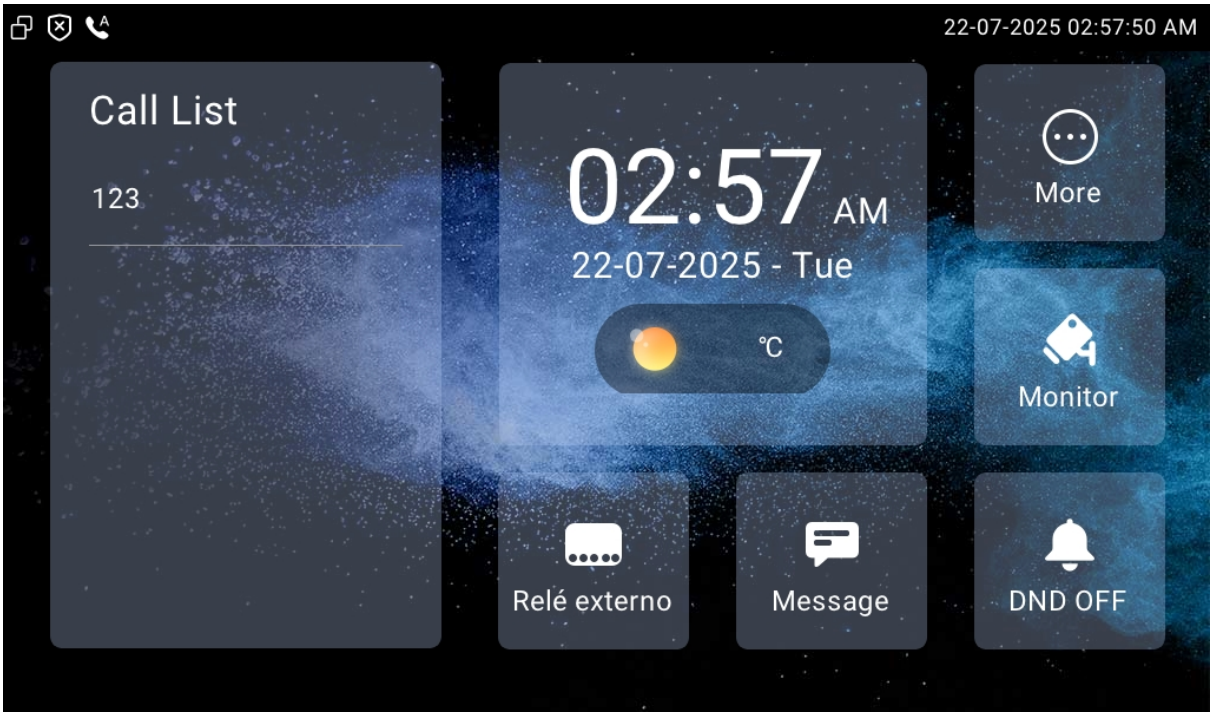
Device Home Screen Type Selection

Akuvox indoor monitor supports two different home screen display modes: **Call list simple** and **classic**.

Choose one suitable mode on the device start-up screen, or configure it on the device's web interface.



Classic

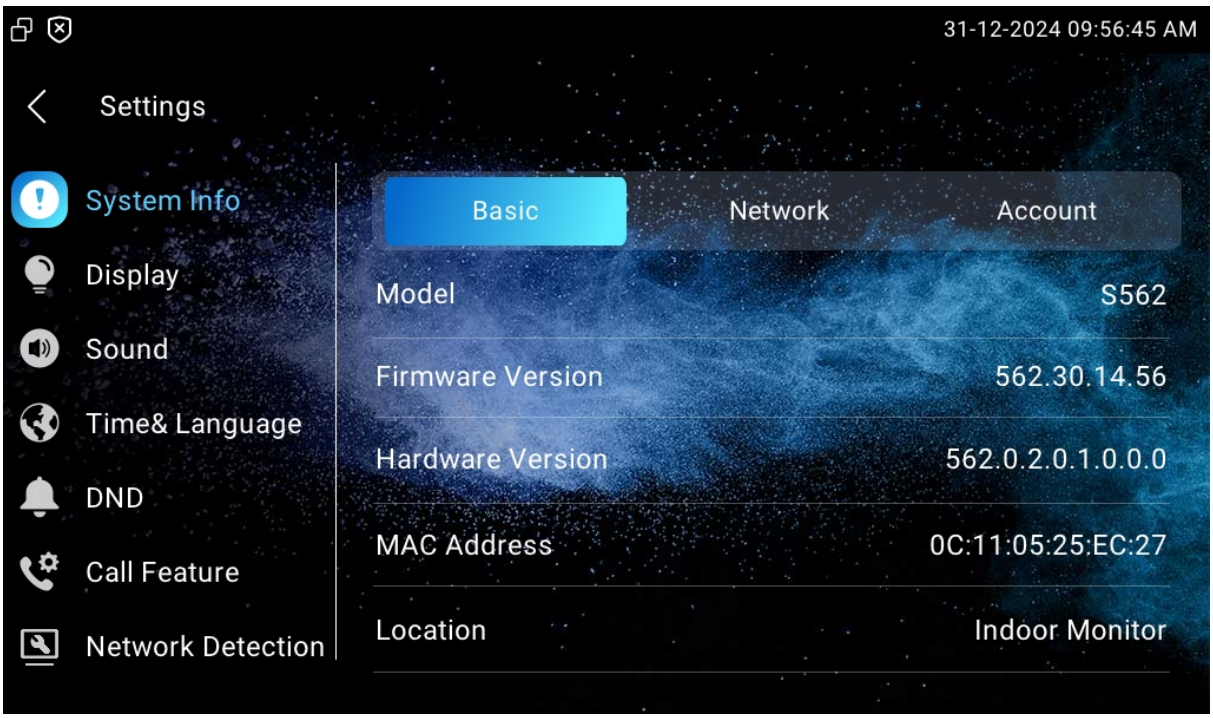


Call list simple

Access the Device Settings

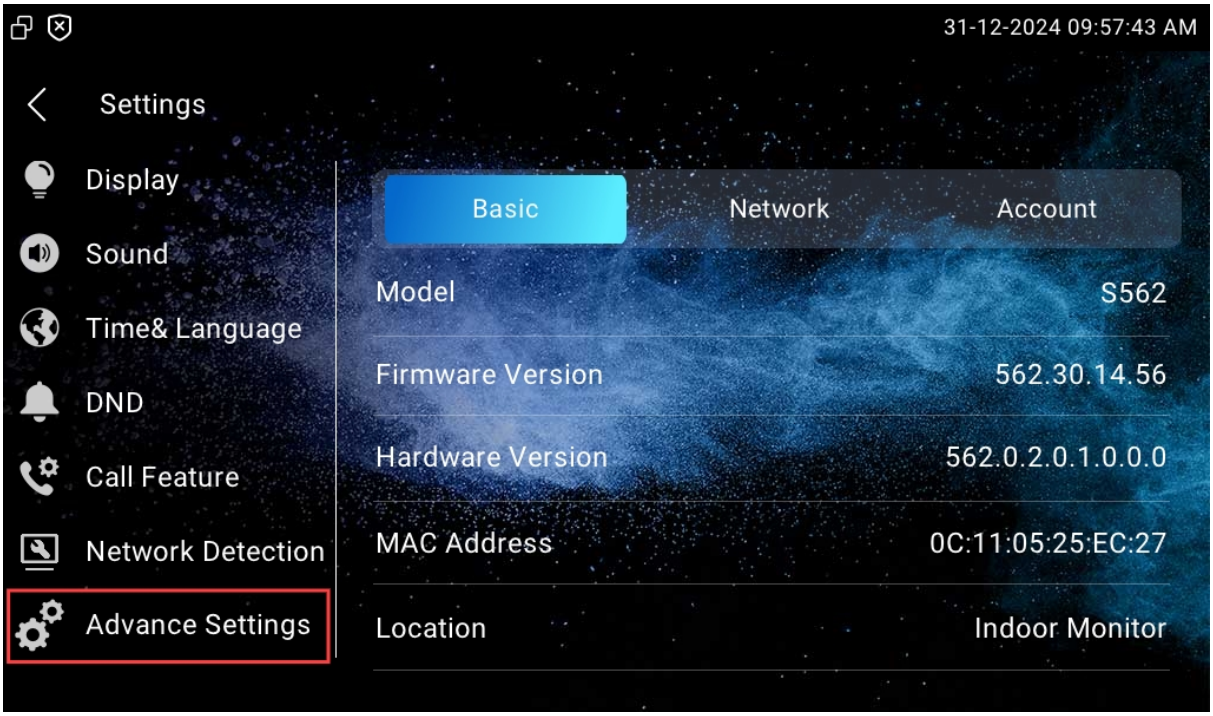
Access Device Basic Settings

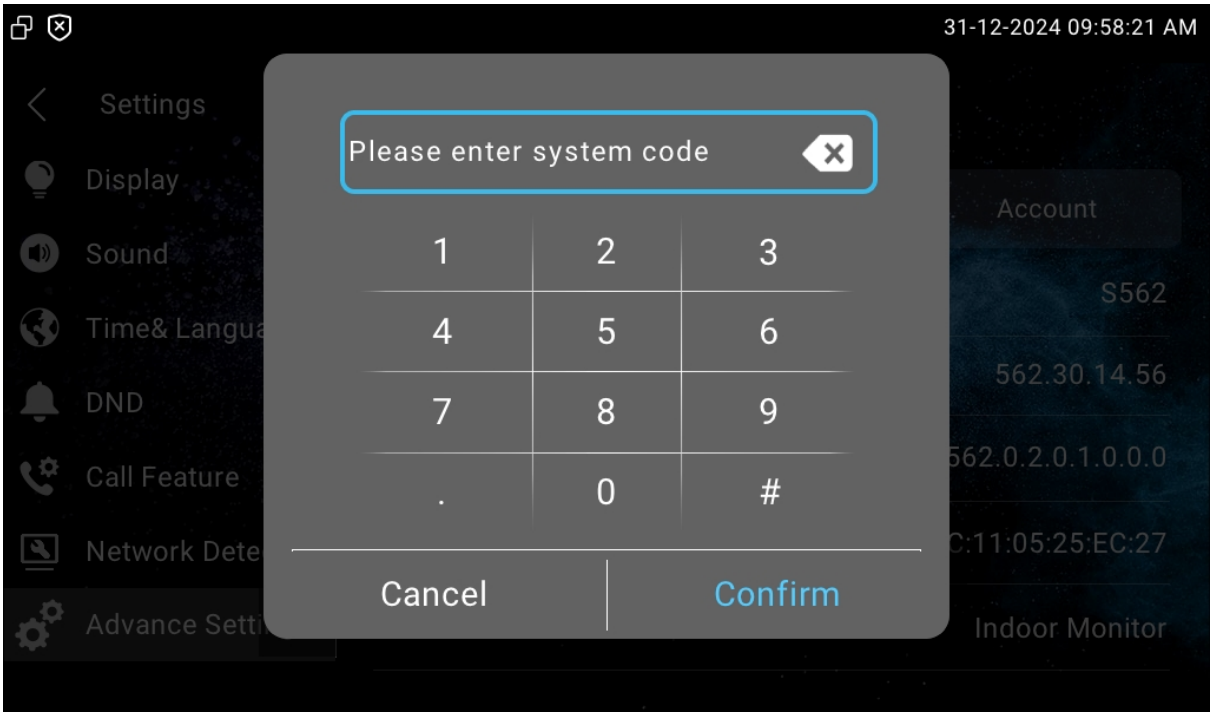
You can access the device's basic and advanced settings to configure different types of functions as needed. To access the device's basic settings, tap **More > Settings.**



Access Device Advance Settings

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

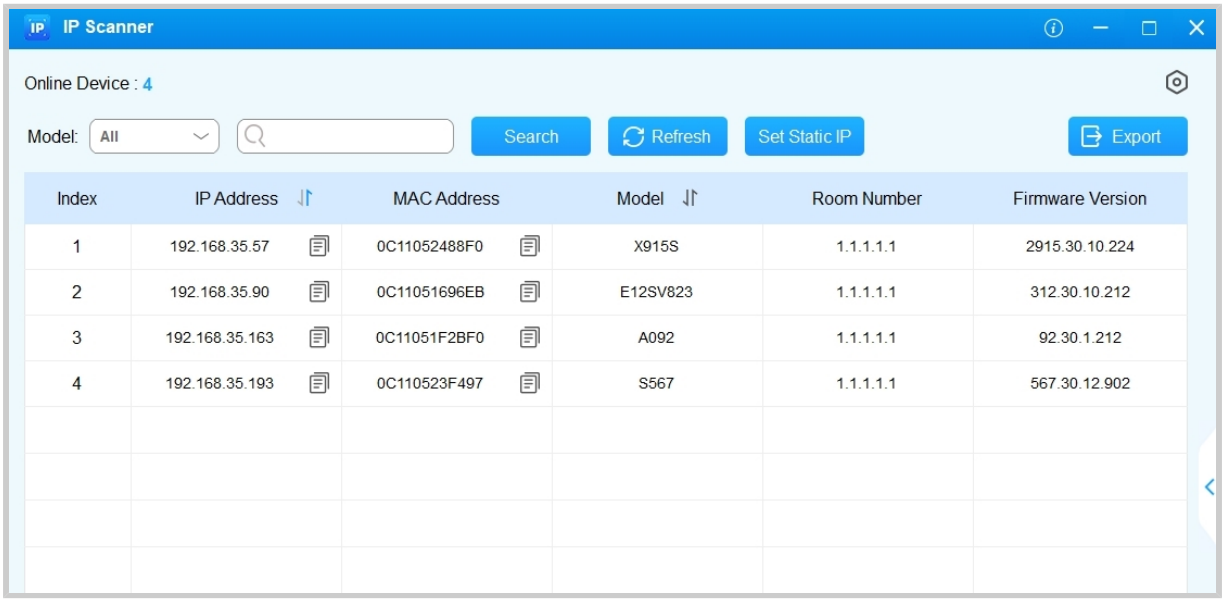




Access the Device Web Settings

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

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





Note

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

Language and Time

Language

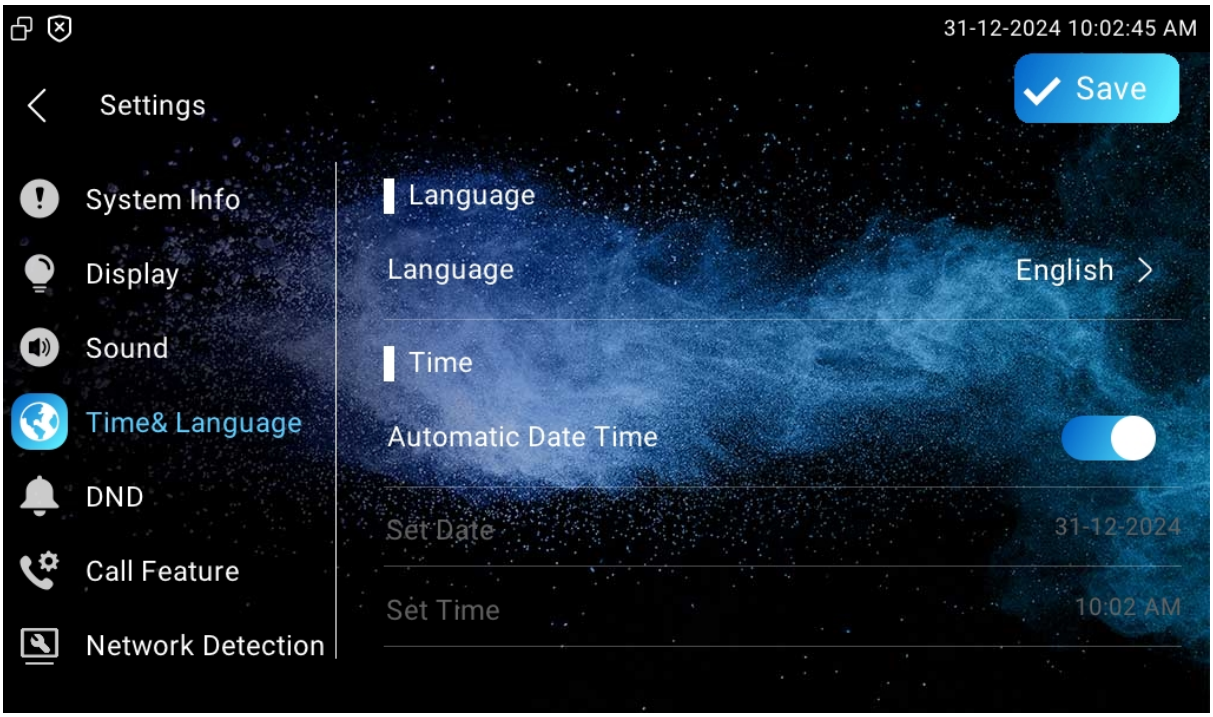
Set up the language during initial device setup or later through the device or web interface according to your preference.

On the Device

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

The device supports the following languages:

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



On the Web Interface

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

The device web interface supports the following languages:

- English, Simplified Chinese, Traditional Chinese, Russian, Korean, Portuguese, Spanish, Italian, Dutch, French, German, Polish, Turkish, Japanese, Vietnamese, Arabic, and Bosnian.



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

The device supports the following languages:

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

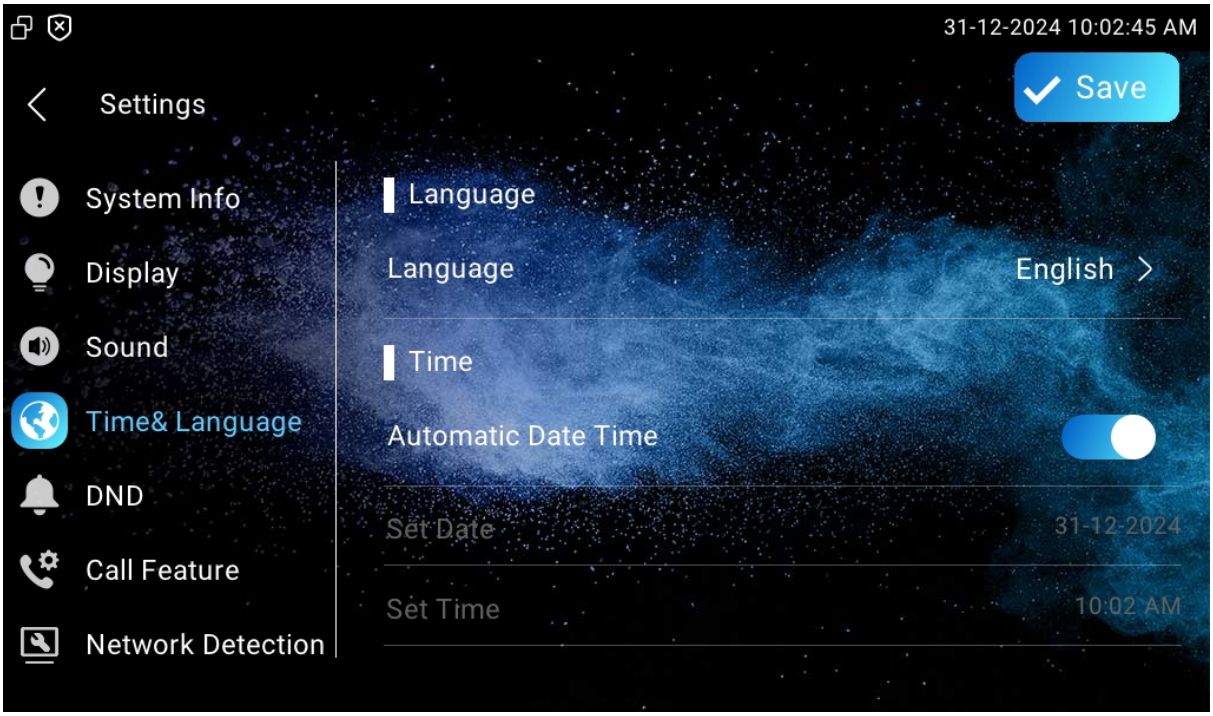


Time

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

On the Device

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

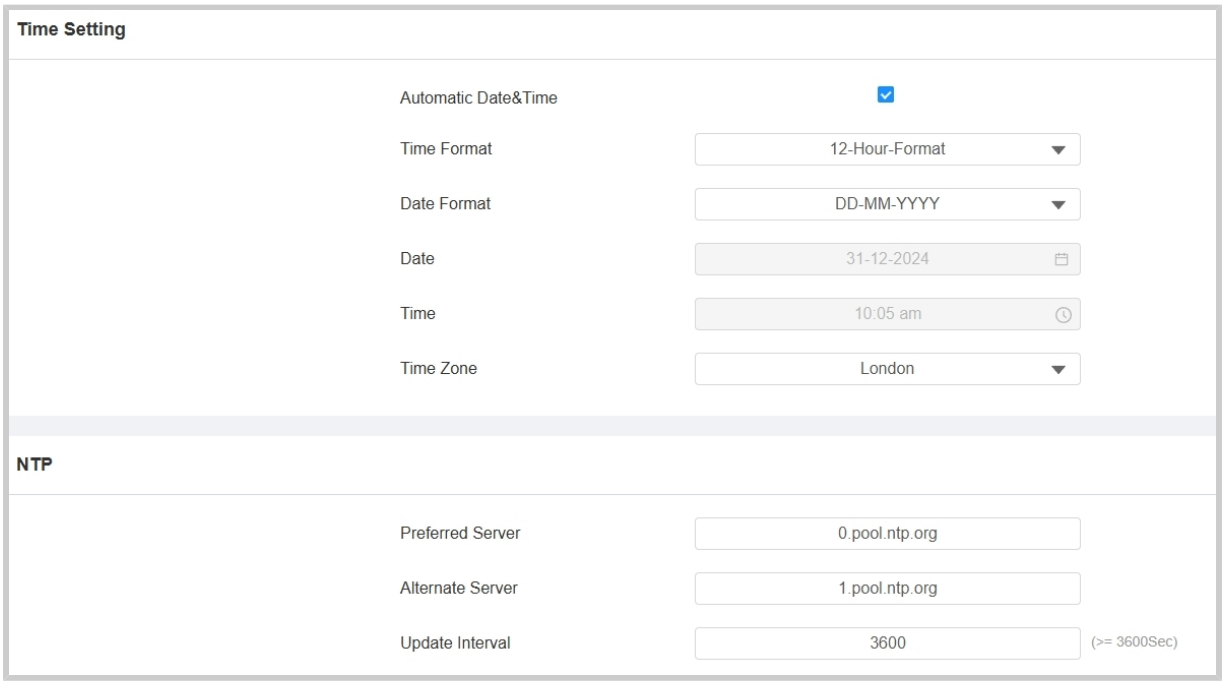


- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the time and date.
- **Time Zone**: Select the specific time zone depending on where the device is used. The default time zone is GMT+0:00.
- **Date Format**: Select the date format from the available options.
- **Time Format**: Select a 12-hour or 24-hour time format.
- **NTP Server 1/2**: Enter the NTP server address. NTP server 2 is the backup.

On the Web Interface

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

Navigate to **Device > Time** interface.

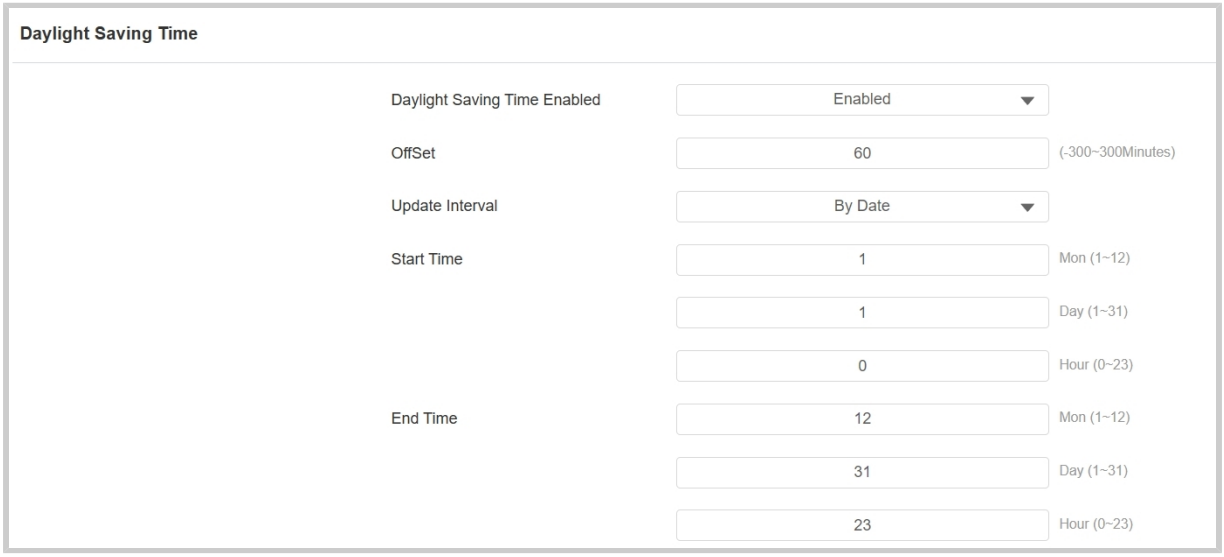


- **Automatic Date Time**: The automatic date is switched on by default, which allows the date & time to be automatically set up and synchronized with the default time zone and the Network Time Protocol(NTP) server. You can also set it up manually by switching off the automatic date and entering the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

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.

Set it up on the **Device > Time** interface.



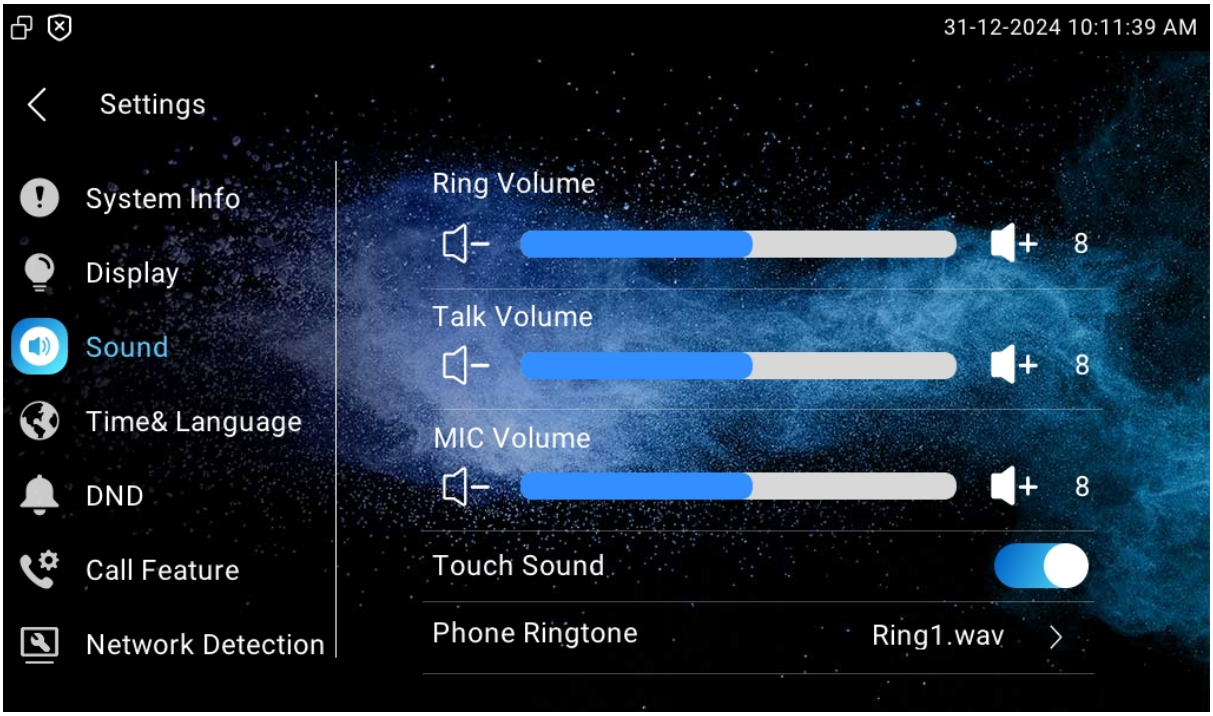
- **Daylight Saving Time Enabled**: Enable or disable the feature. **Auto** means that the device adjusts the daylight saving time automatically.
- **Offset**: 60 minutes as default, setting the clocks an hour ahead of the standard time.
- **Update Interval**: There are two options: **By Date** and **By Week**. 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.

Sound and Volume

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

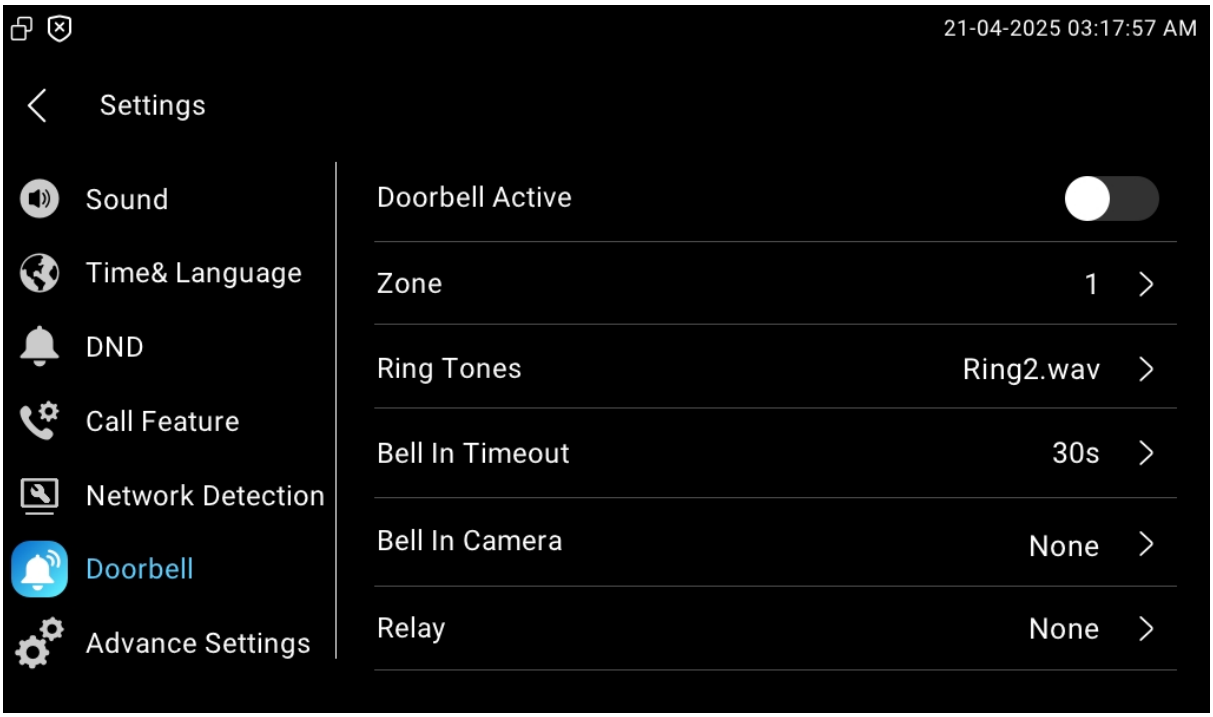
On the Device

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



- **Ring Volume**: The incoming call ringtone volume.
- **Talk Volume**: The speaker volume during the call.
- **Mic Volume**: The mic volume.
- **Touch Sound**: The icon tapping sound.
- **Phone Ringtone**: The ringtone for incoming calls.
- **Notification Sound**: The ringtone for the incoming messages.
- **Door Unit Ring Tones**: The tone sounds when the indoor monitor receives calls from a door phone.

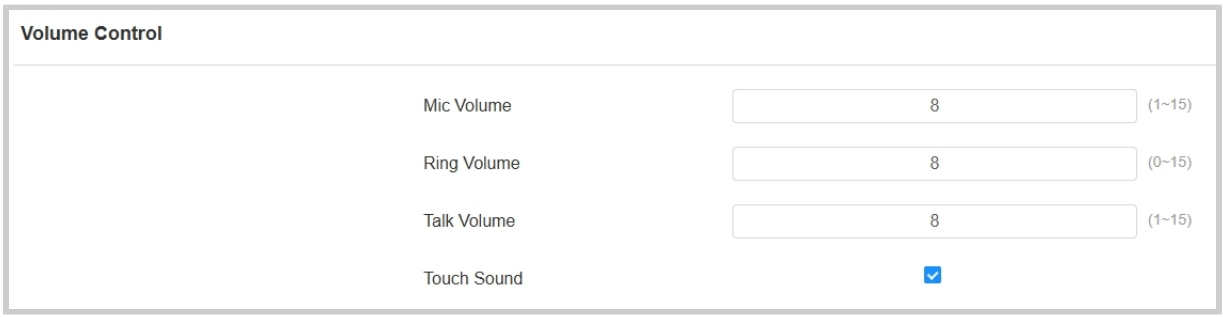
You can configure the doorbell sound and select the local relay to be triggered along with the doorbell on the **Settings > Doorbell** screen.



- **Zone**: Set which zone(IO port) is used for doorbell connection.
- **Ring Tones**: Select the doorbell sound.
- **Bell In Timeout:** Set the doorbell duration(from 10 seconds to 5 minutes).
- **Bell In Camera**: Select the camera to be triggered along with the doorbell.
- **Relay**: Select the local relay to be triggered along with the doorbell.

On the Web Interface

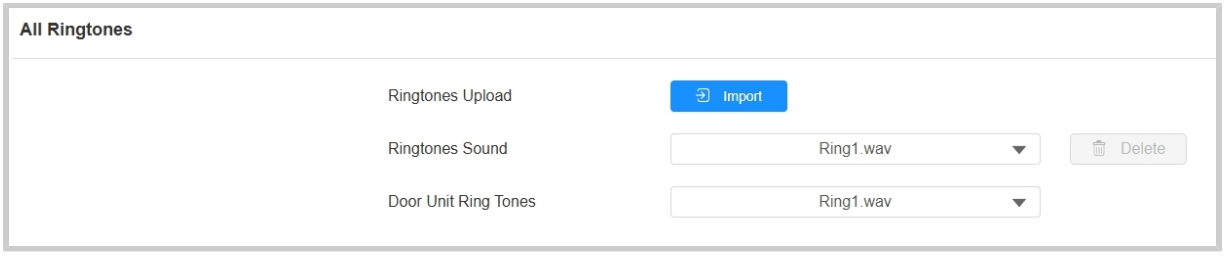
You can configure volumes on the **Device > Audio** interface.



- **Mic Volume**: The mic volume.
- **Ring Volume**: The incoming call ringtone volume.
- **Talk Volume**: The speaker volume during the call.
- **Touch Sound**: The icon tapping sound.

Upload Tones

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

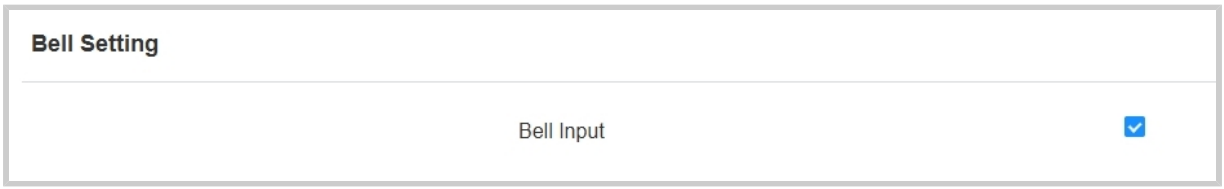


> **Note**
>
> The files to be uploaded should be in WAV format with a maximum of 250K.

Bell Setting

You can enable/disable the use of the bell input port.

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



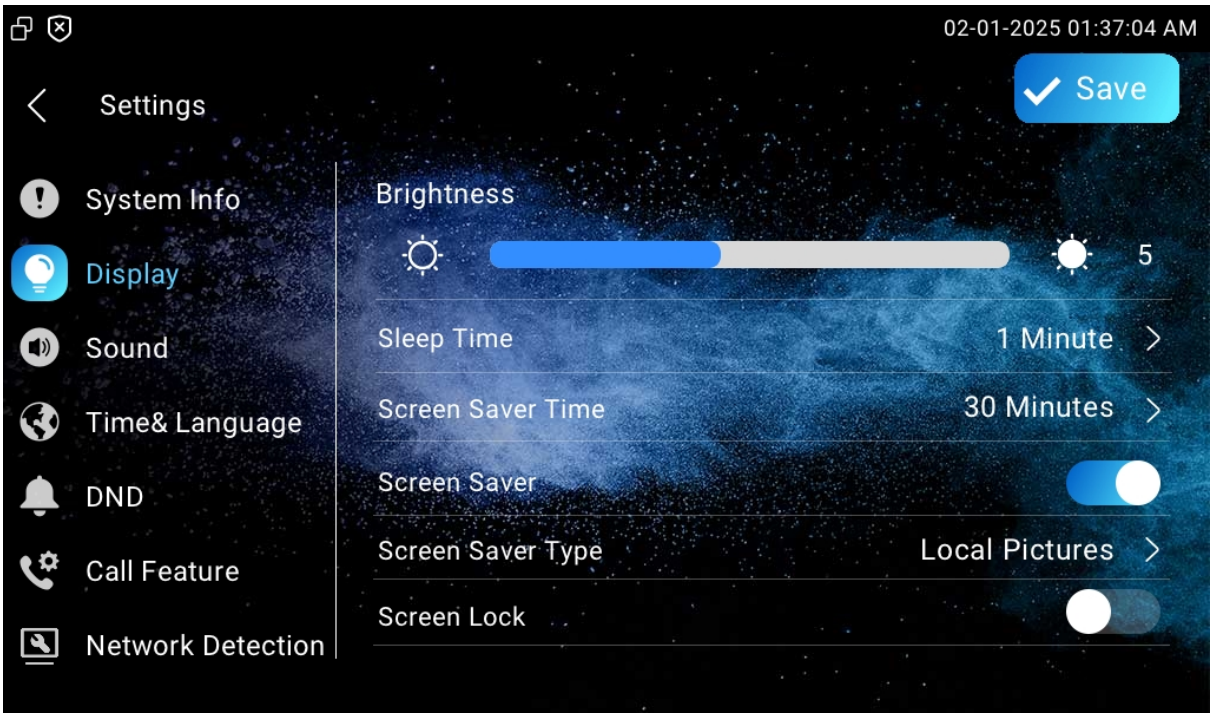
- **Bell Input**: It is enabled by default. When disabled, the doorbell trigger prompt will not display on the indoor monitor.

Screen Display

On the Device

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

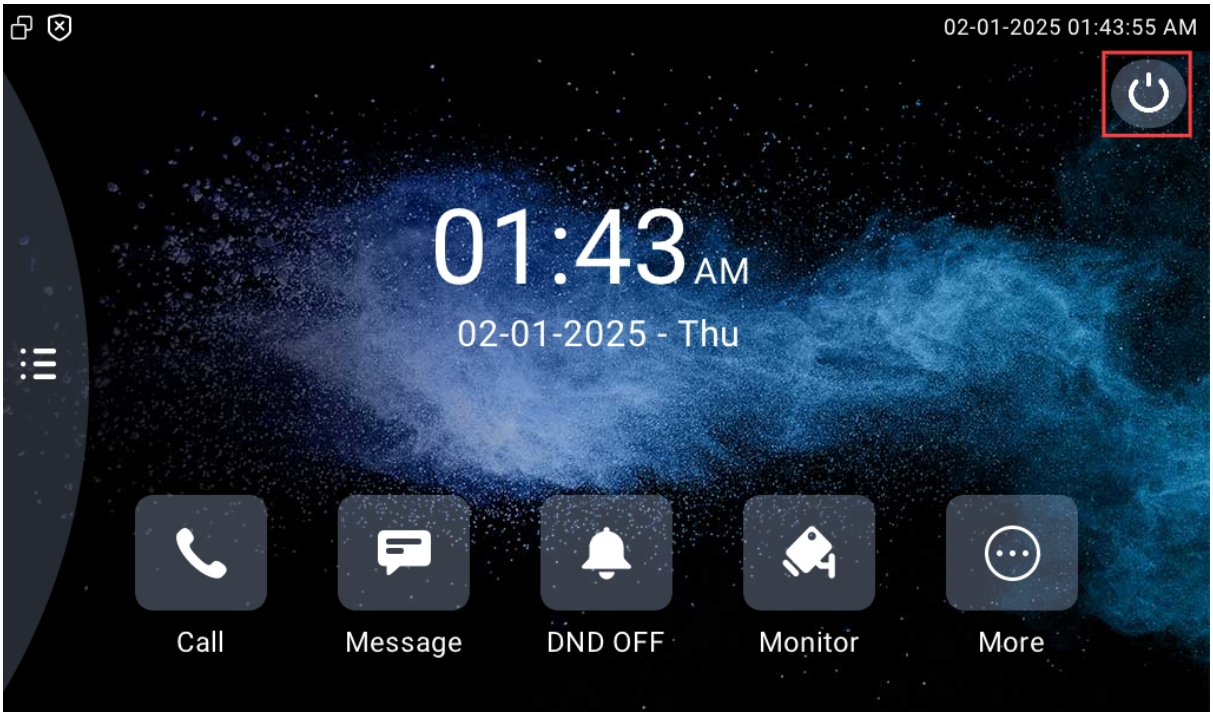
Set up the screen display on the **Settings > Display** screen.



- **Brightness**: Move the blue bar to adjust the screen brightness. The default brightness is **145**.
- **Sleep Time**: Set the sleep timing based on the screen saver (15 seconds to 30 minutes).
  - If the screen saver is enabled, the sleep time here is the screen saver start time. For example, if you set it to 1 minute, the screen saver will start automatically when the device has no operation for 1 minute.

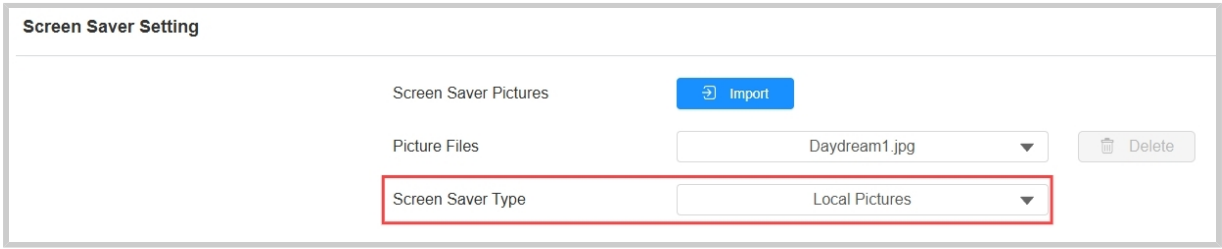
  - If the screen saver is disabled, the sleep time here is the screen turn-off time. For example, if you set it to 1 minute, the screen will be turned off automatically when the device has no operation for 1 minute.
- **Screen Saver Time**: The time for displaying the screensaver.
- **Screen Saver**: Determine whether to display the screensaver when the device goes into sleep mode.
- **Screen Saver Type**:
  - **SDMC Pictures:** Display pictures uploaded to the SDMC.
  - **Local Pictures:** Display pictures uploaded to the indoor monitor as the screen saver.
  - **SDMC + Local Pictures:** Display pictures uploaded to the SDMC or the indoor monitor as the screen saver.
  - **Clock:** Display the clock as the screen saver.
- **Screen Lock**: Lock the screen after the screen is turned off(turn dark). You are required to enter the code to unlock the screen. The initial password is empty. Tap ✓ to unlock the screen.
- **Screen Clean**: Allow users to wipe the screen clean without triggering unwanted changes in the settings.
- **Wallpaper**: It is for local wallpaper selection.

You can also turn off the screen manually.



On the Web Interface

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



- **Screen Saver Type**:
  - **SDMC Pictures:** Display pictures uploaded to the SDMC.
  - **Local Pictures:** Display pictures uploaded to the indoor monitor as the screen saver.
  - **SDMC + Local Pictures:** Display pictures uploaded to the SDMC or the indoor monitor as the screen saver.
  - **Clock:** Display the clock as the screen saver.

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



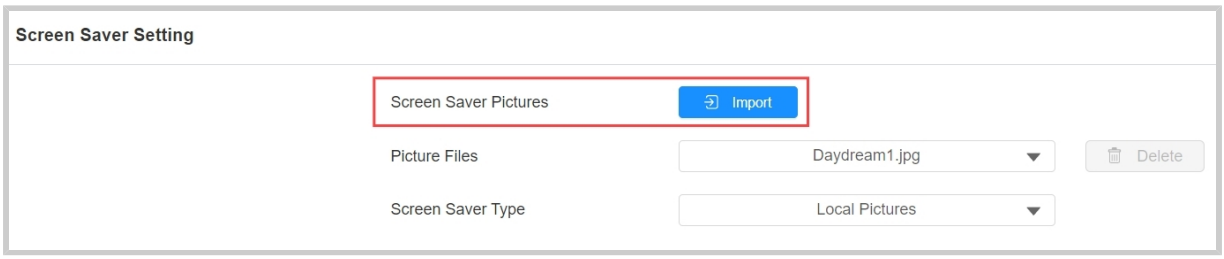
- **Sleep Time**: If the screen saver is enabled, the sleep time is the screen saver's start time. For example, if you set it as 1 minute, the screen saver will start automatically when the device has no operation for 1 minute. If the screen saver is disabled, the screen will be turned off automatically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

Upload Screen Saver

You can upload screen-saver images individually or in batches to the device via the web interface, enhancing visual experience or serving publicity purposes.

Set it up on the web **Device > Display Setting > Screen Saver Setting** interface.

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



- **Screen Saver Pictures**: Max size: 256K; Format:1024x600 jpg; File name can only contain digits, letters, and "_".

> **Note**
>
> - Previous pictures with the same ID will be overwritten if they are designated again.
> - The file name should not exceed 127 characters.

Upload Wallpaper

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

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



- **Wallpaper**: Max size: 256K; Format:1024x600 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.

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



- **Boot Logo**: Max size:100K; Format:1024*600 jpg; File name can only contain digits, letters, and "_".

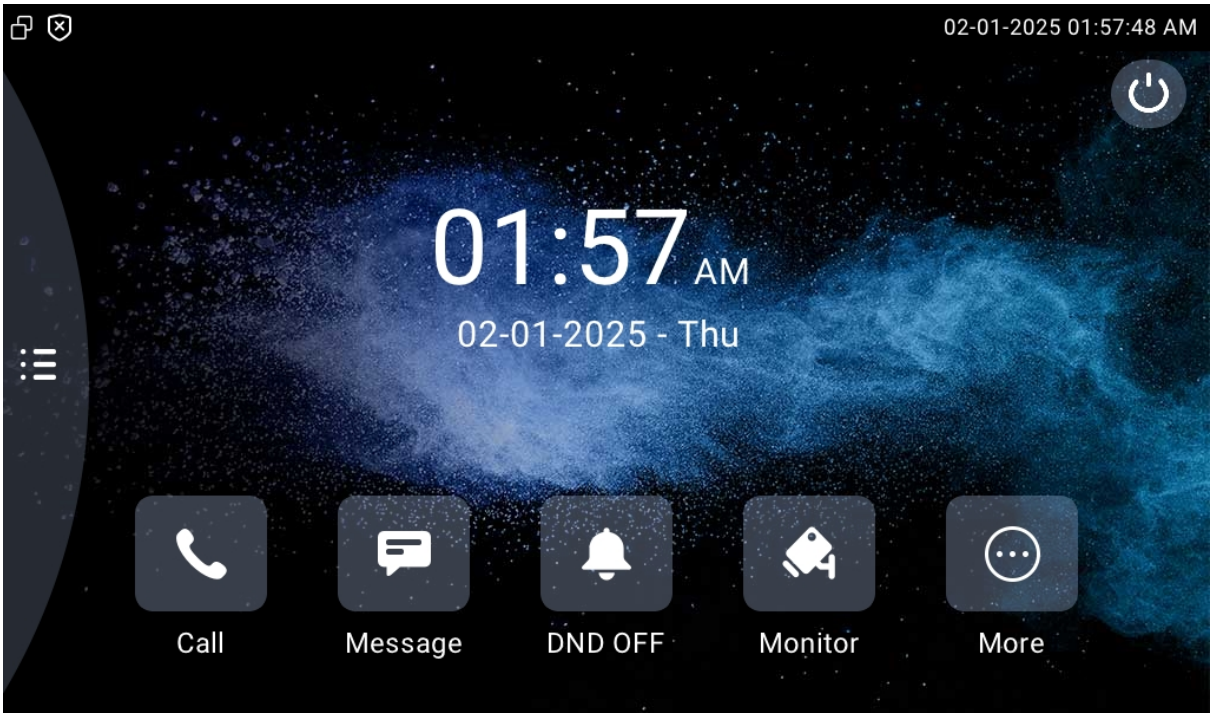
Home Screen Display

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

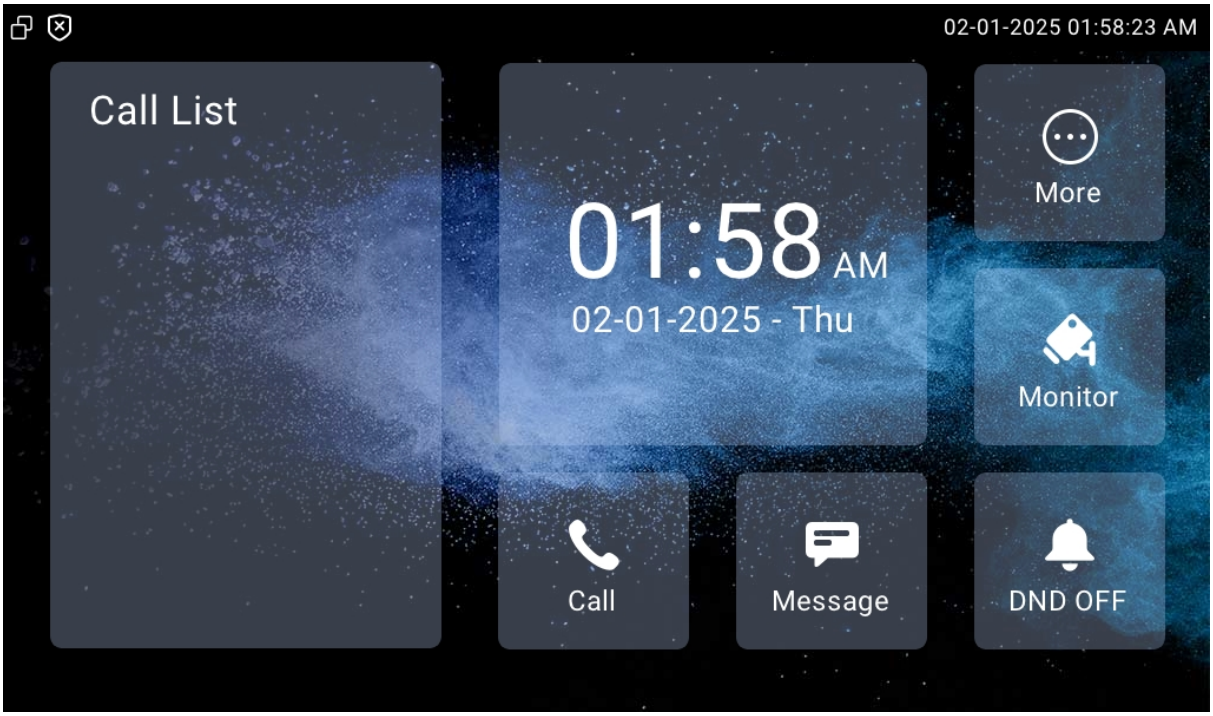
Go to **Device > Display Setting > Theme** interface.



Classic Home Screen:



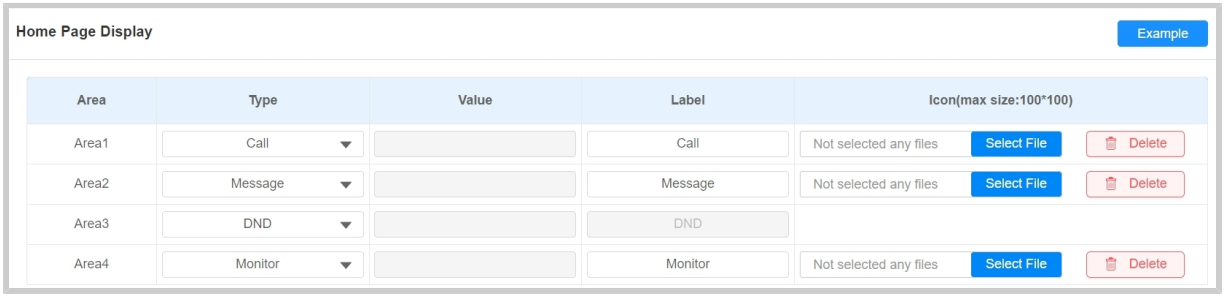
Call List Home Screen:



Home Screen Tab Display

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

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



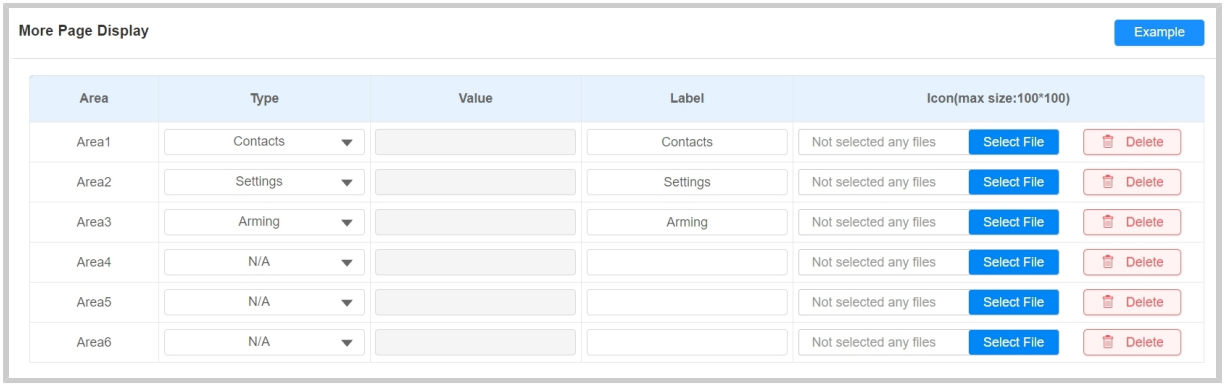
- **Type**: Select the functional icon to be displayed on the home screen.

- **All Calls/All Calls 1-3**: Tap to initiate multicast calls.

  When **All Calls** is selected and more than one multicast group is configured, users can choose the desired group after tapping All Calls. All Calls 1-3 correspond to the multicast groups 1 to 3.
- **Label**: Name the icon. The DND icon cannot be renamed.
- **Type**: Click to upload the icon picture. The maximum icon size is 100*100. The picture format can be JPG, JPEG, or PNG.

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

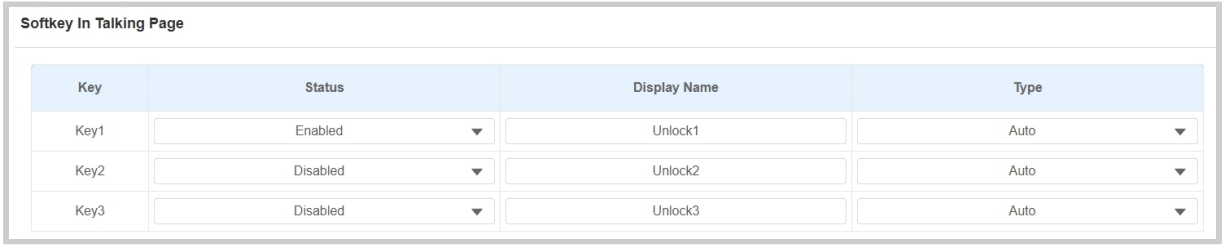
Configure the icons displayed on **More Page Display** on the same interface.



Unlock Tab Configuration

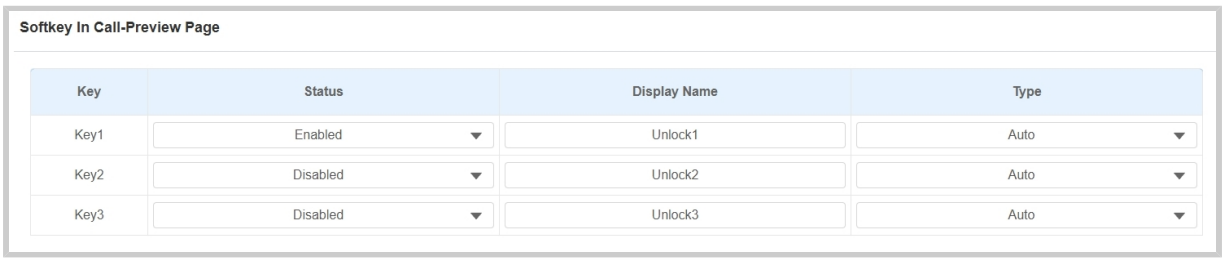
You can customize the unlock tab and select the relay type on the talking, monitor, and call preview screen for the door opening.

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



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

Scroll down to set up the unlock tab on the **Call Preview** screen.



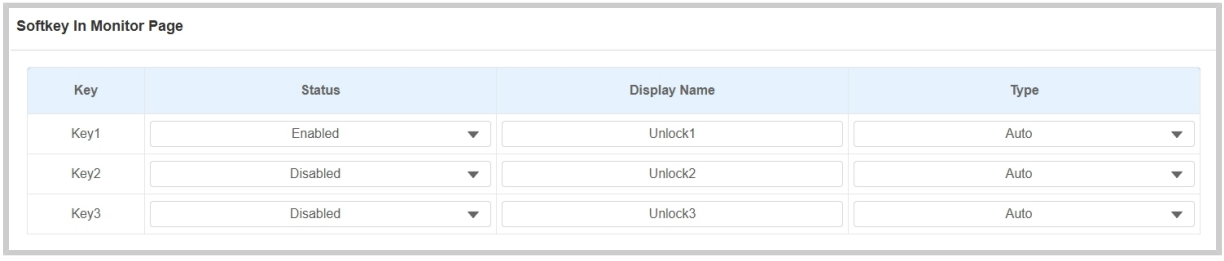
- **Status**: With it enabled, the unlock tab will be displayed on the call-preview screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up unlock tabs on the home screen and more screens.



- **Status**: It is enabled by default.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

Scroll down to set up unlock tabs on the **Monitor** screen.



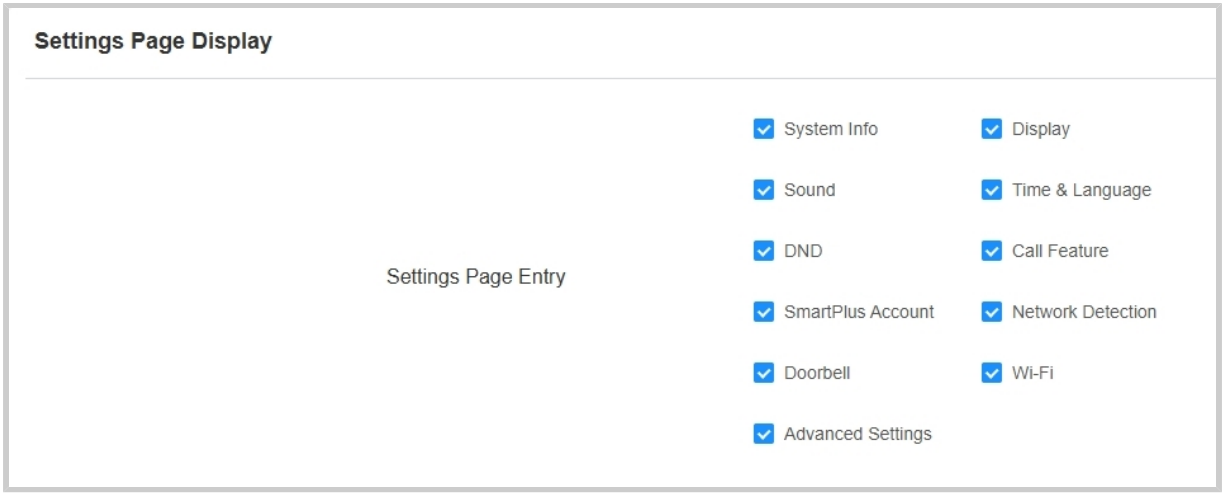
- **Status**: With it enabled, the unlock tab will be displayed on the monitoring screen.
- **Display Name**: Name the unlock tab.
- **Type**: Select the relay trigger type according to the actual setup.

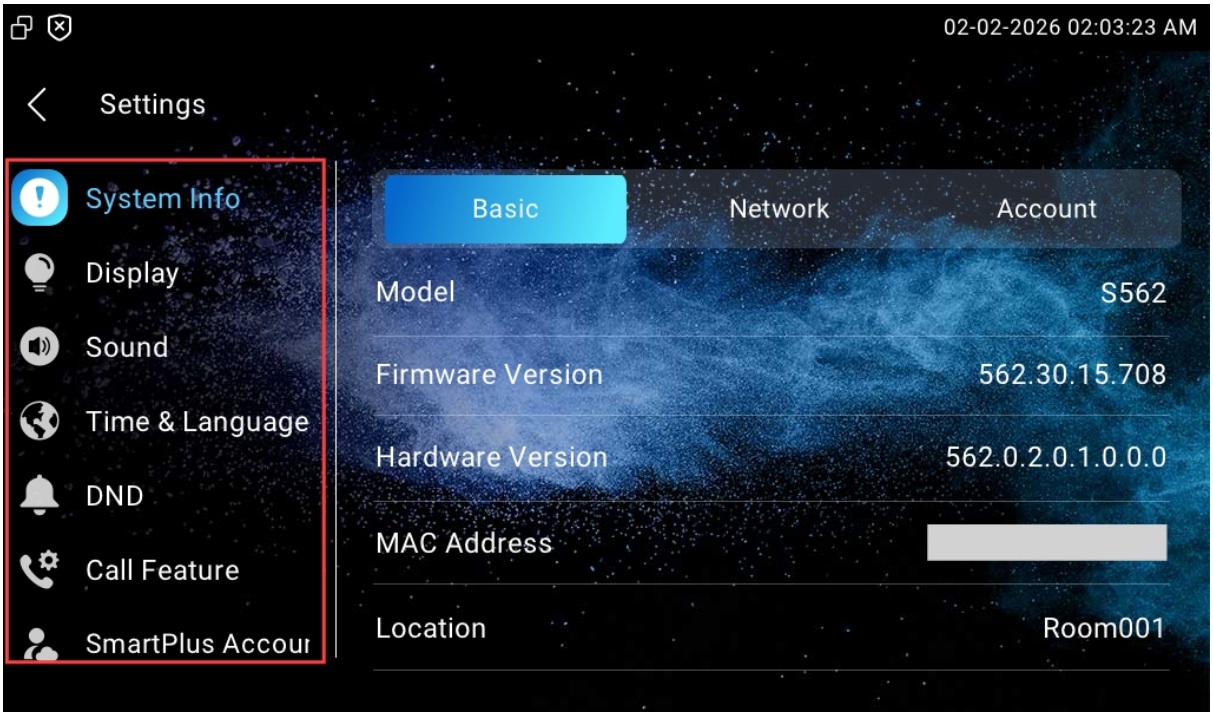
> **Note**
>
> Please refer to the Access Control Configuration chapter for different unlock types setup.

Function Display on the Settings Screen

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

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



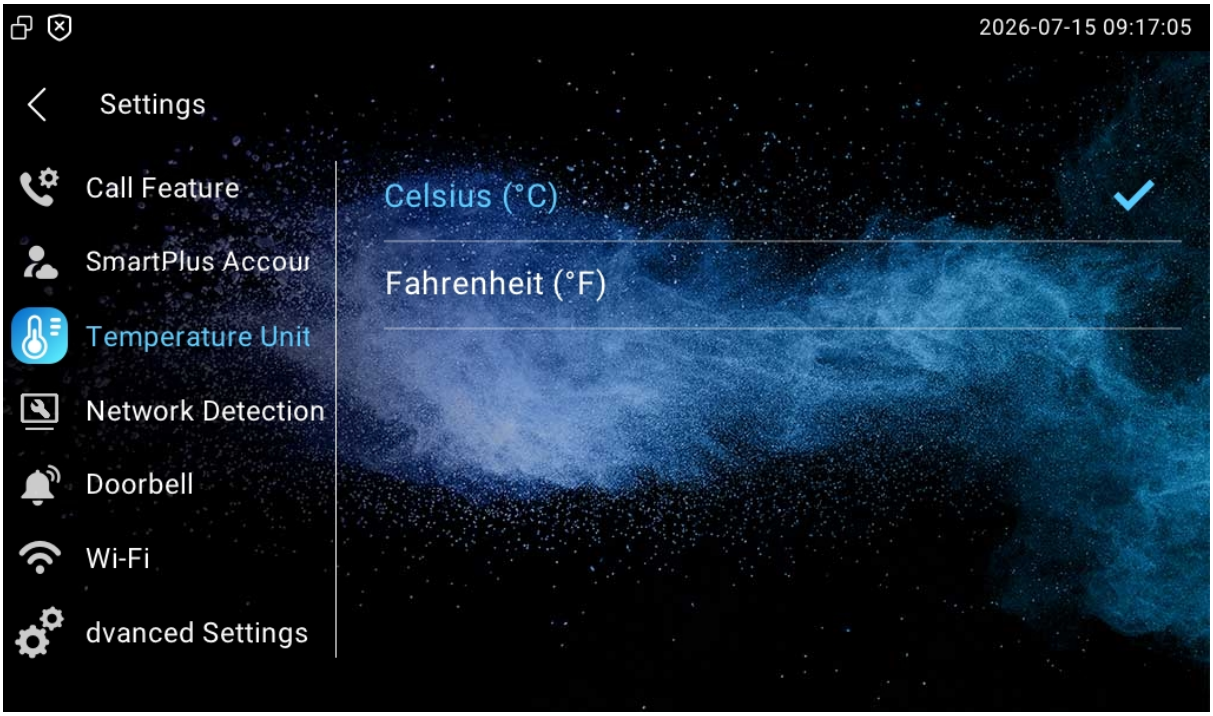


Temperature Display Setting

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

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

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



Note

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

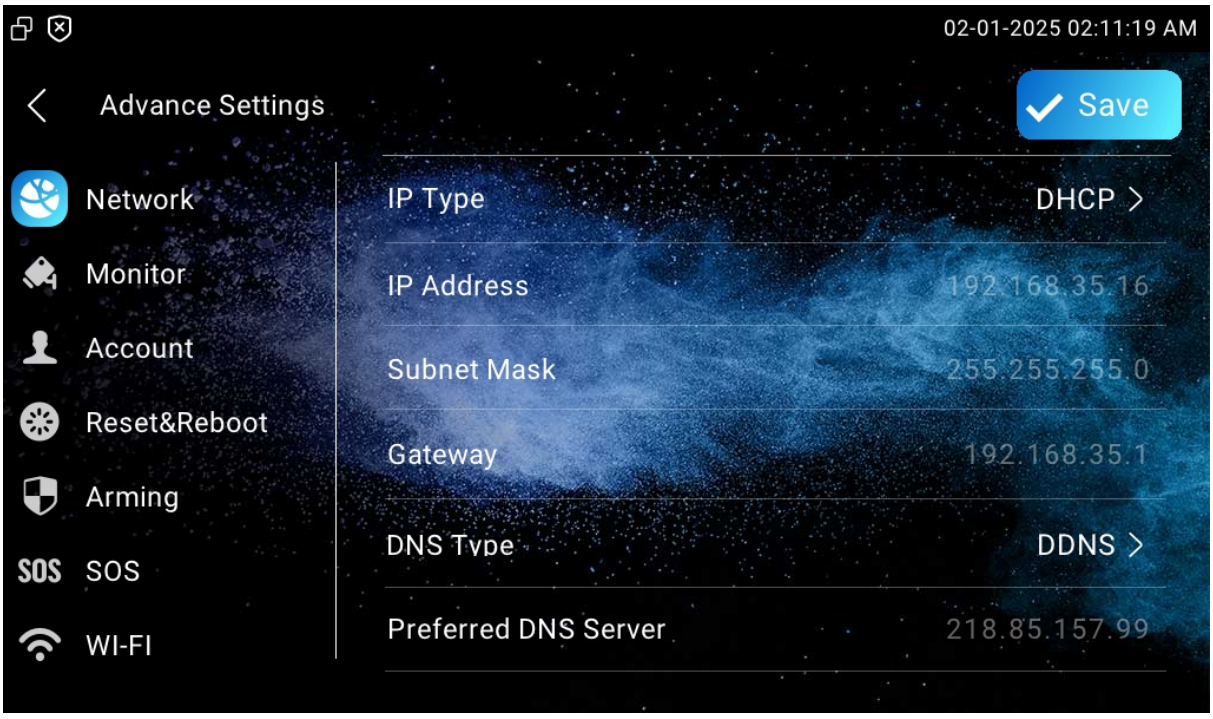
Network Setting

Device Network Configuration

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

On the Device

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



- **IP Type:** DHCP mode is the default network connection. The device will be assigned by the DHCP server with an IP address, subnet mask, default gateway, and DNS server address automatically. In static IP mode, the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to the actual network environment.

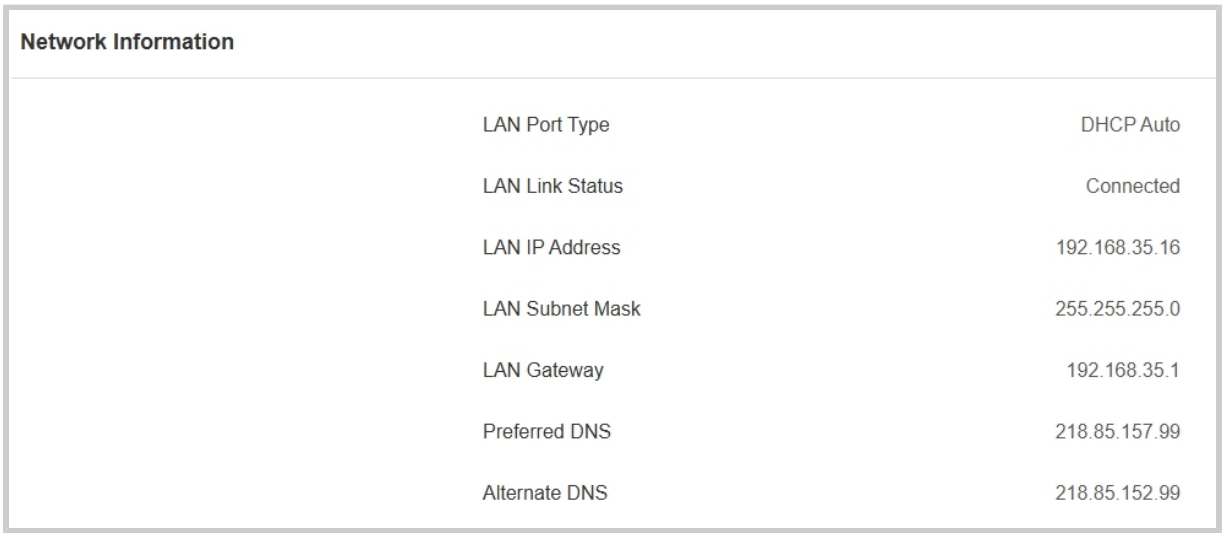
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.
- **Subnet Mask**: A subnet mask tells your device which IP addresses are part of your local network and which ones are not.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

Note

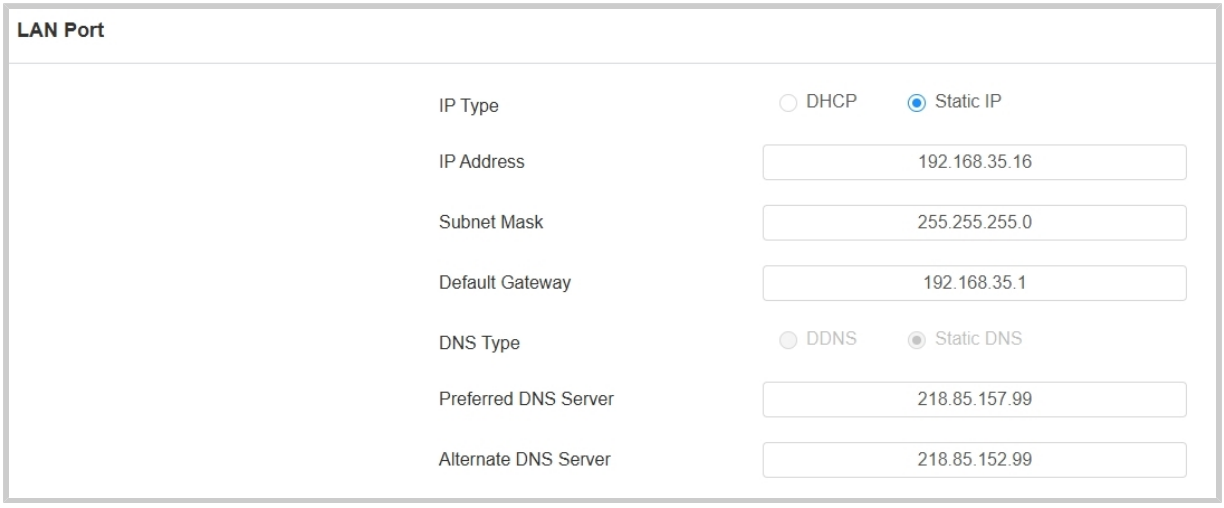
- You can press System Info and then press Network on the Settings screen to check the device's network status.
- The default code to enter advanced settings is 123456.

On the Web Interface

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



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



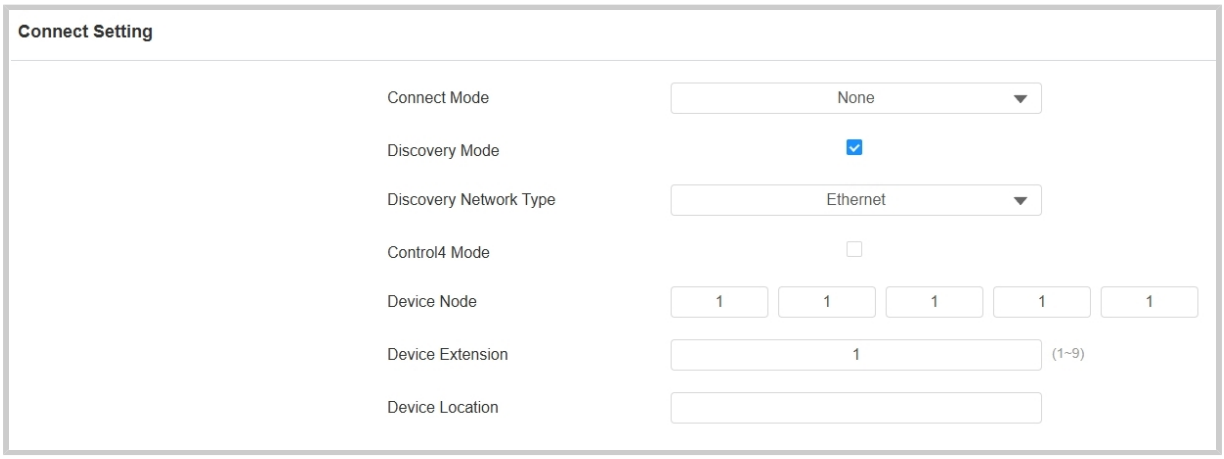
- **IP Type**:
  - **DHCP** mode will enable the indoor monitor to be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS address automatically.
  - **Static IP** allows you to enter the IP address, subnet mask, default gateway, and DNS address manually according to the actual network environment.
- **IP Address**: Set up the IP address when the static IP mode is selected. To access the device's web settings, your computer should be on the same local network as the device.

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

Device Deployment in Network

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

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



- **Connect Mode**: You can set up the connect mode according to the device connection with a specific server in the network, such as **SDMC**, **Cloud,** or **None**.

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

- **Discovery Mode**: Enabled by default. Available for **None** server mode. The device can be discovered by other devices in the network. When disabled, the device will be concealed and not be discovered by other devices.

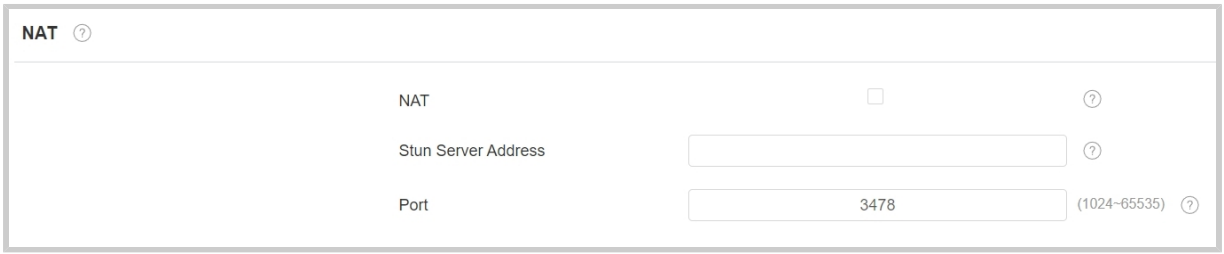
- **Discovery Network Type**: Specify the preferred network connection, WLAN or Ethernet. It is Ethernet by default. When Ethernet is unavailable, the device will automatically switch to a WLAN connection and vice versa.
- **Control4 Mode:** Enable this option for integration with the Control4 smart home.
- **Device Node**: Available for **None** server mode. It can be used to call the device. Specify the device address by entering device location information from the left to the right: Community, Building, Unit, Floor, and Room in sequence.
- **Device Extension**: Available for **None** server mode. The device extension number ranges from 0 to 10.
- **Device Location**: The location in which the device is installed and used. Available for **None** server mode.

Device NAT Setting

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

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

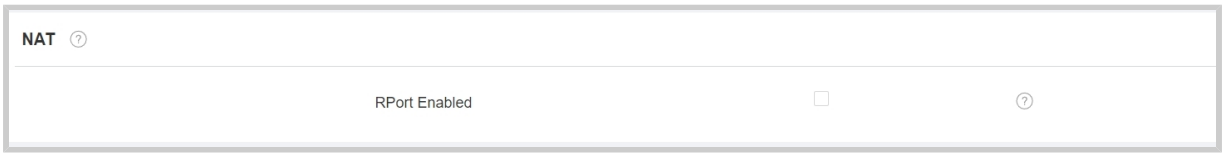
To set up NAT, go to **Account> Basic > NAT** interface.



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

- **Port**: Set the SIP server port.

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



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

Device Web HTTP Setting

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

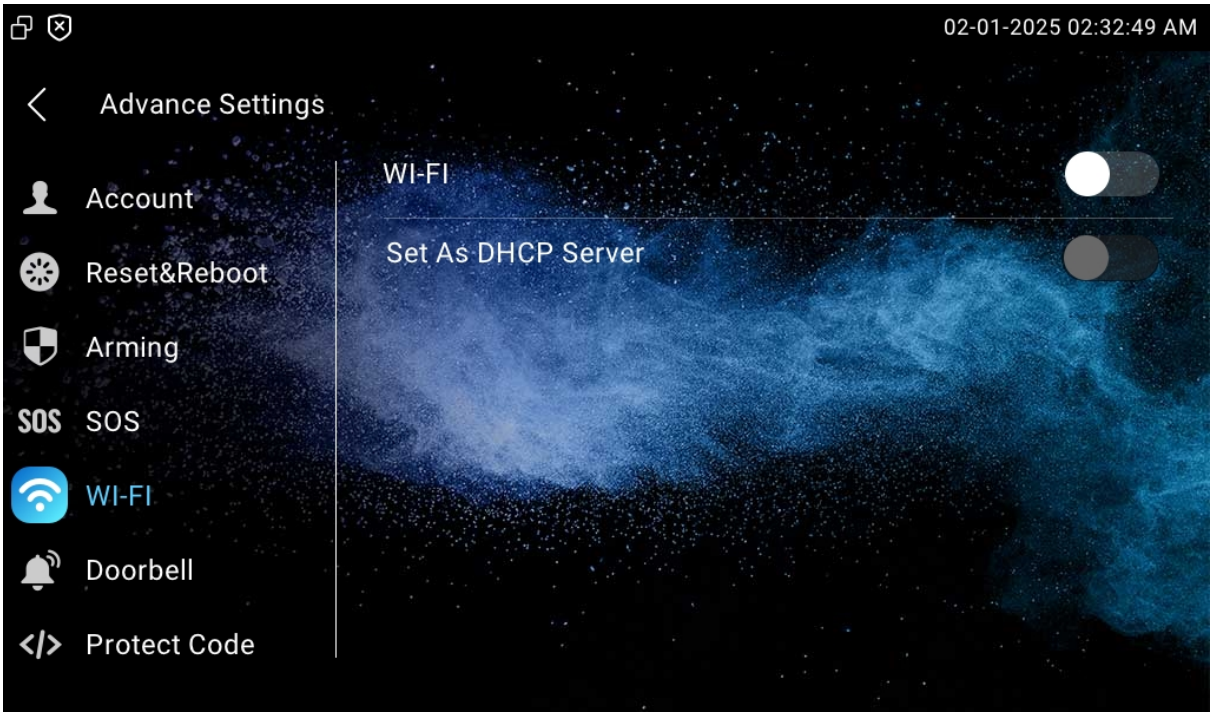
Set it up on the **Network > Advanced > Web Server** interface.



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

Device Wi-Fi Setting

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

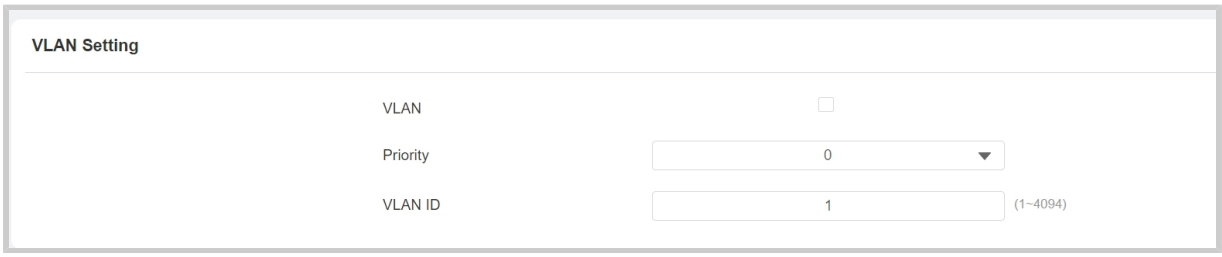


- **Set As DHCP Server**: Use the Wi-Fi as the DHCP server.

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.

Set it up on the **Network > Advanced > VLAN Setting** interface. You can also set it up on the **Settings > Advance Settings > Network** screen.



- **Priority**: VLAN Priority lets you assign a priority to outbound packets containing the specified VLAN-ID (VID). Packets containing the specified VID are marked with the priority level configured for the VID classifier.
- **VLAN ID**: The same VLAN ID as the switch or router.

SNMP Setting

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

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



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

Contacts Configuration

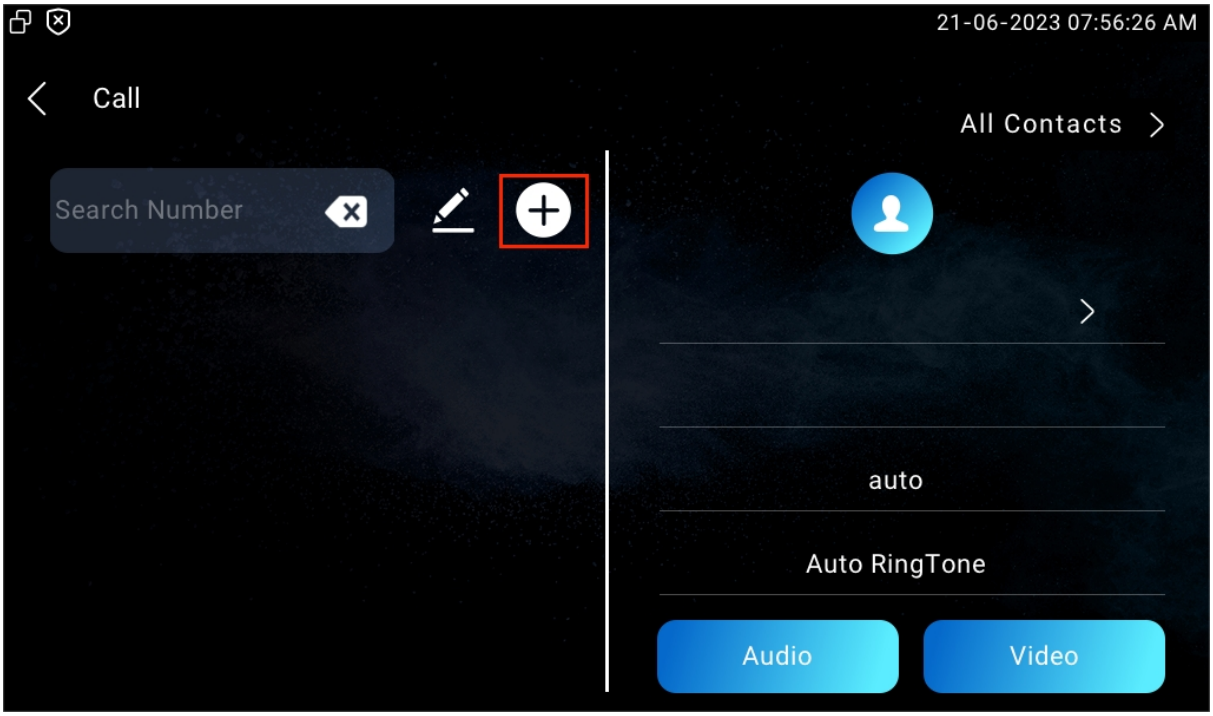
The local contact information is used to initiate SIP or IP calls to other intercom devices. You can group the contact information to facilitate group calls. Moreover, you can add the camera URL of the target device, allowing users to view its live stream during a call or a call preview.

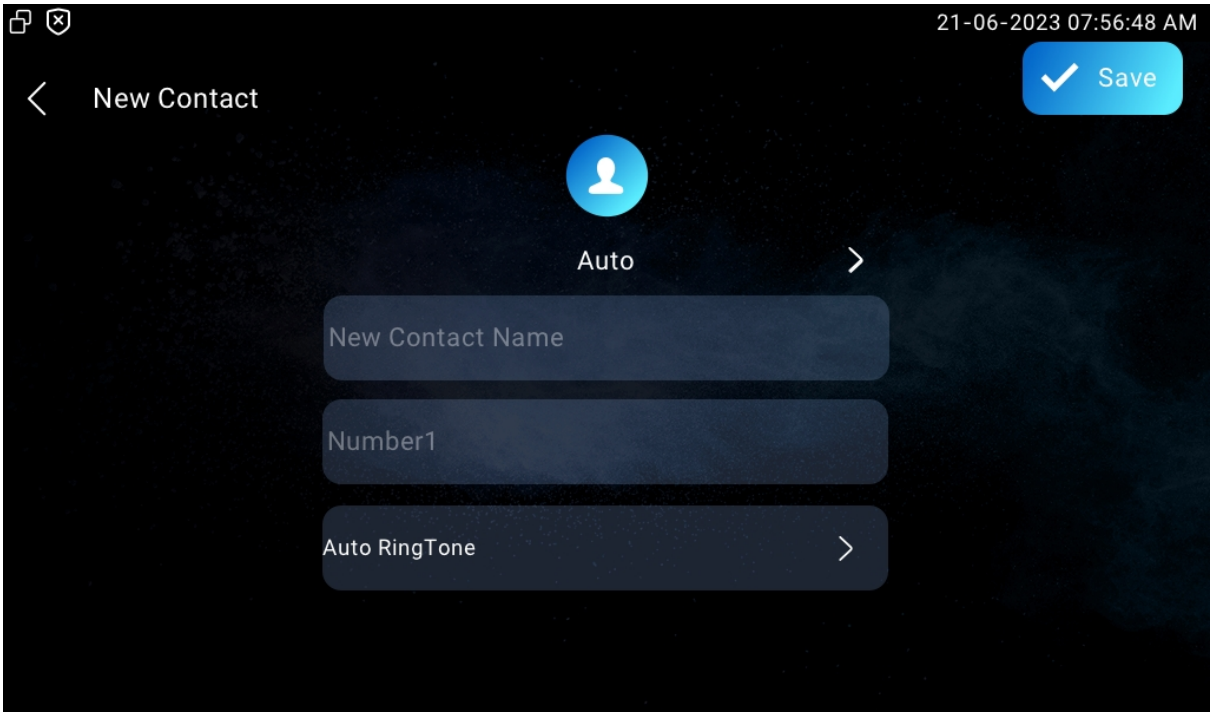
On the Device

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

Add Local Contacts

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

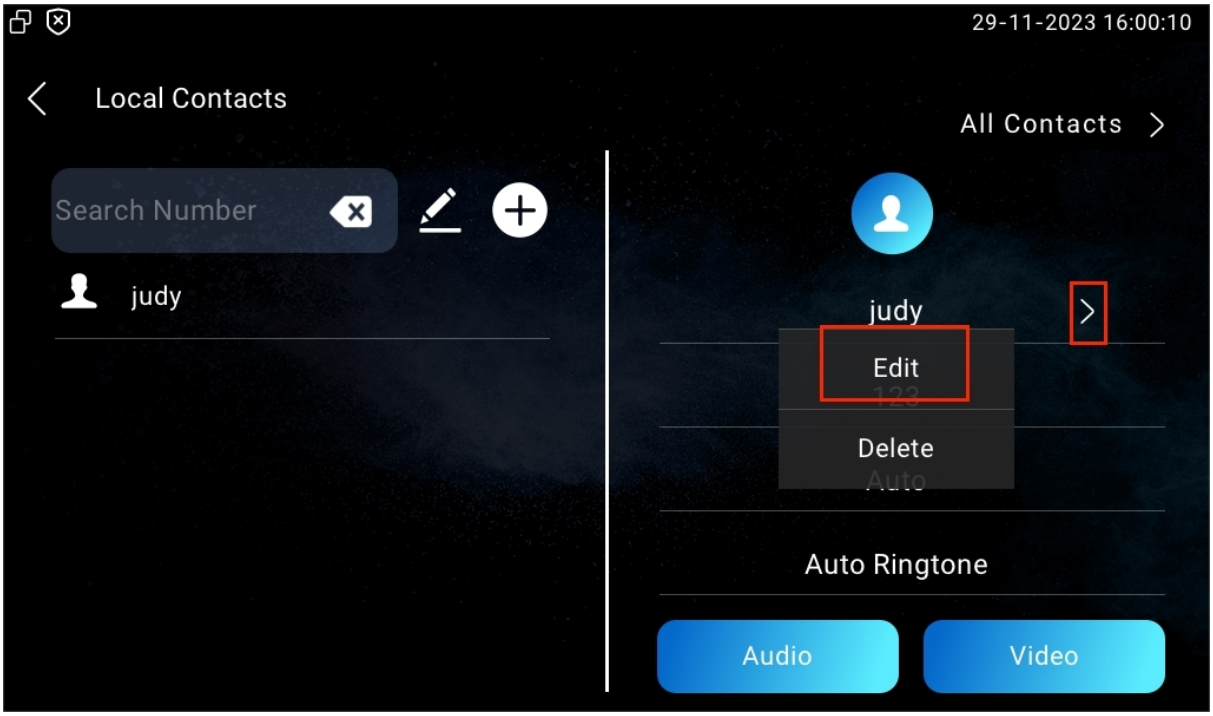




- **Account**: The account to make the call, Account 1 or Account 2. **Auto** will adopt the registered account to make the call. If both accounts are registered, account 1 is the default option.
- **New Contact Name**: Name the contact to distinguish it from others.
- **Number**: The IP or SIP number.
- **Auto Ringtone**: The phone ringtone for incoming calls.

Edit Contacts

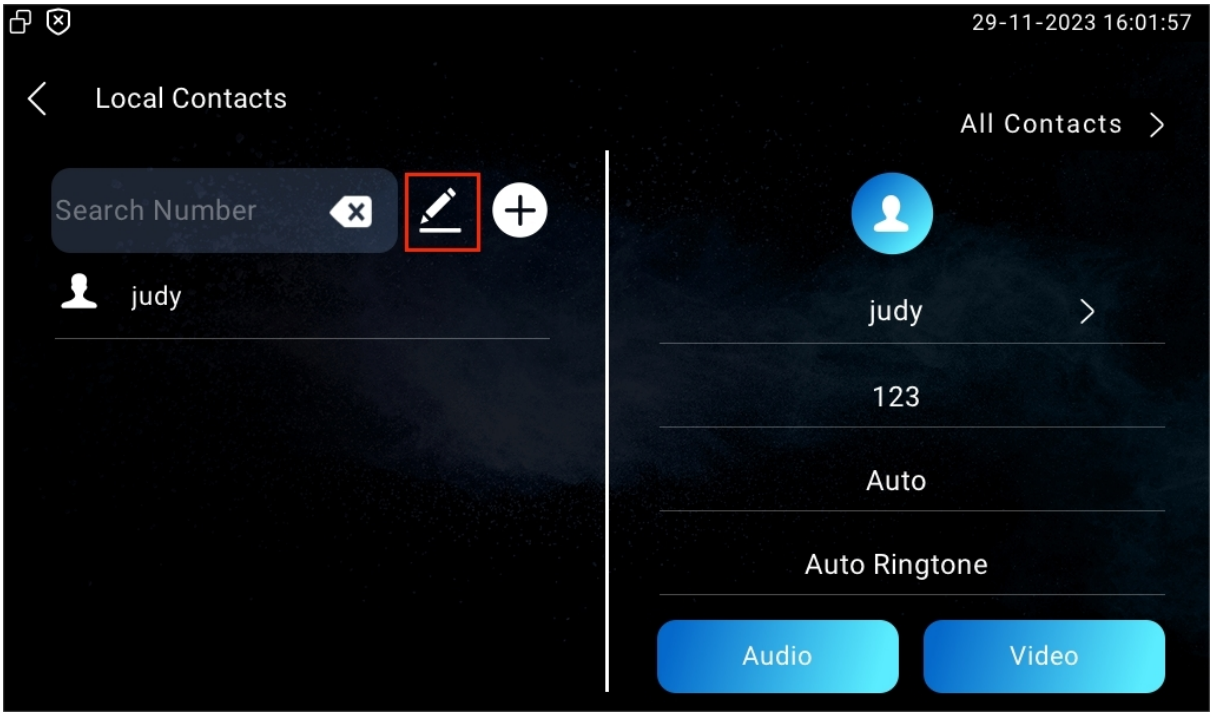
You can check and edit the existing contacts in the contact list. Choose one and click **Edit** to modify.

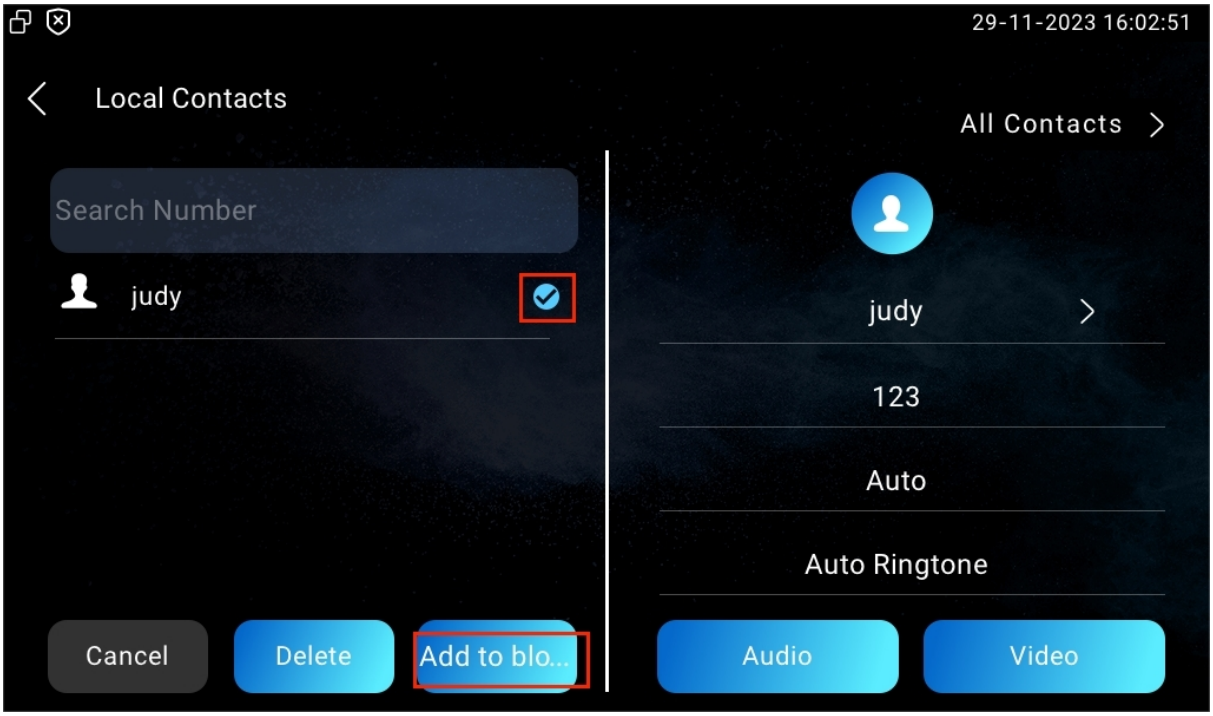


Blocklist Contacts

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

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





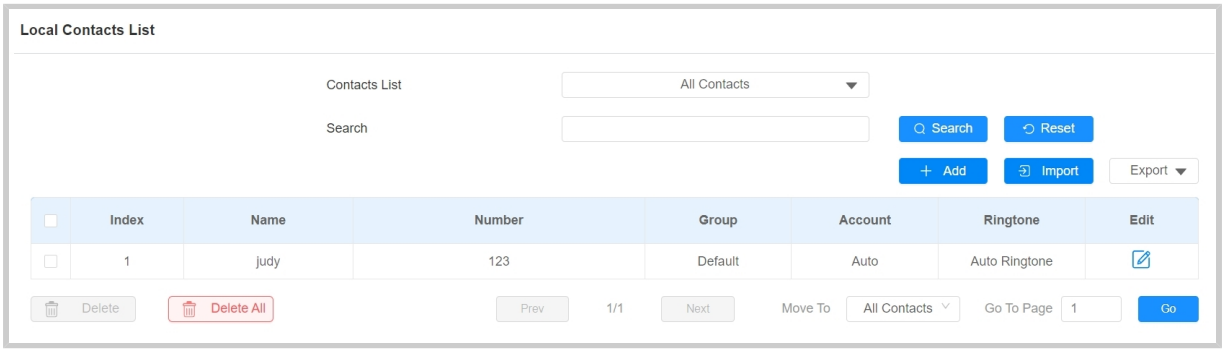
Note

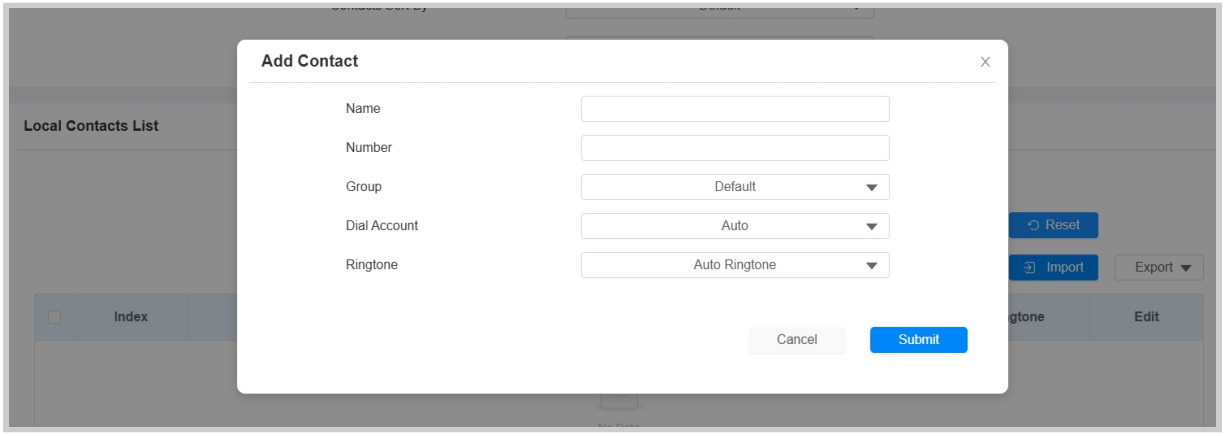
You can delete contacts regardless of whether it is in Blocklist.

On the Web Interface

Add Local Contacts

You can add, edit, and search local contacts on the device's web interface. To add contacts, go to **Contacts > Local Contacts > Local Contacts List** interface, then click **+Add**. You can add up to 500 contacts.





- **Contacts List**: **All Contacts** displays all the contacts in the contact list. **Blocklist** displays the contacts in the blocklist.
- **Search**: Search a contact by its name or number.
- **Name**: The contact's name to distinguish it from others.
- **Number**: The SIP or IP number of the contact.
- **Group**: Calls from contacts in **Blocklist** will be rejected.
- **Dial Account**: The account to make the call, Account 1 or Account 2.

- **Ringtone**: The ringtone for the incoming call from the contact.

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

Import and Export Contacts

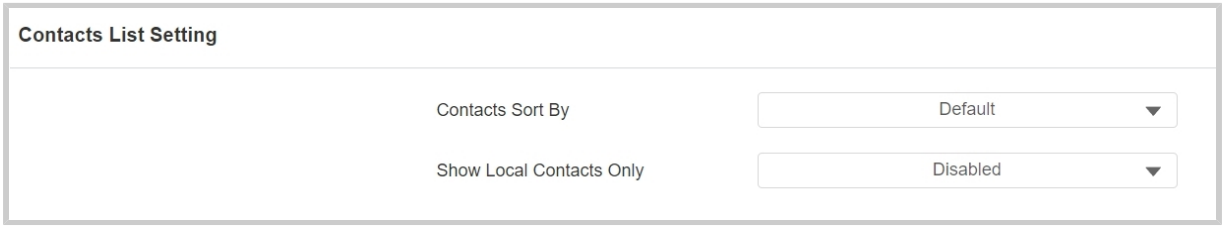
You can import and export contacts in batch. The file should be in .xml or .csv format.

To import or export contacts, go to **Contacts > Local Contacts > Local Contacts List** interface.



Contact List Display

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



- **Contacts Sort By**:
  - **Default**: The local contacts will be displayed before those from SmartPlus, SDMC, etc.
  - **ASCII Code**: The contacts will be displayed in order based on the first letter of the contact names.

  - **Created Time**: The contacts will be displayed by their created time.
- **Show Local Contacts Only**: If enabled, only the local contacts will be displayed. If disabled, all the contacts from SmartPlus Cloud, SDMC, and so on will be displayed.

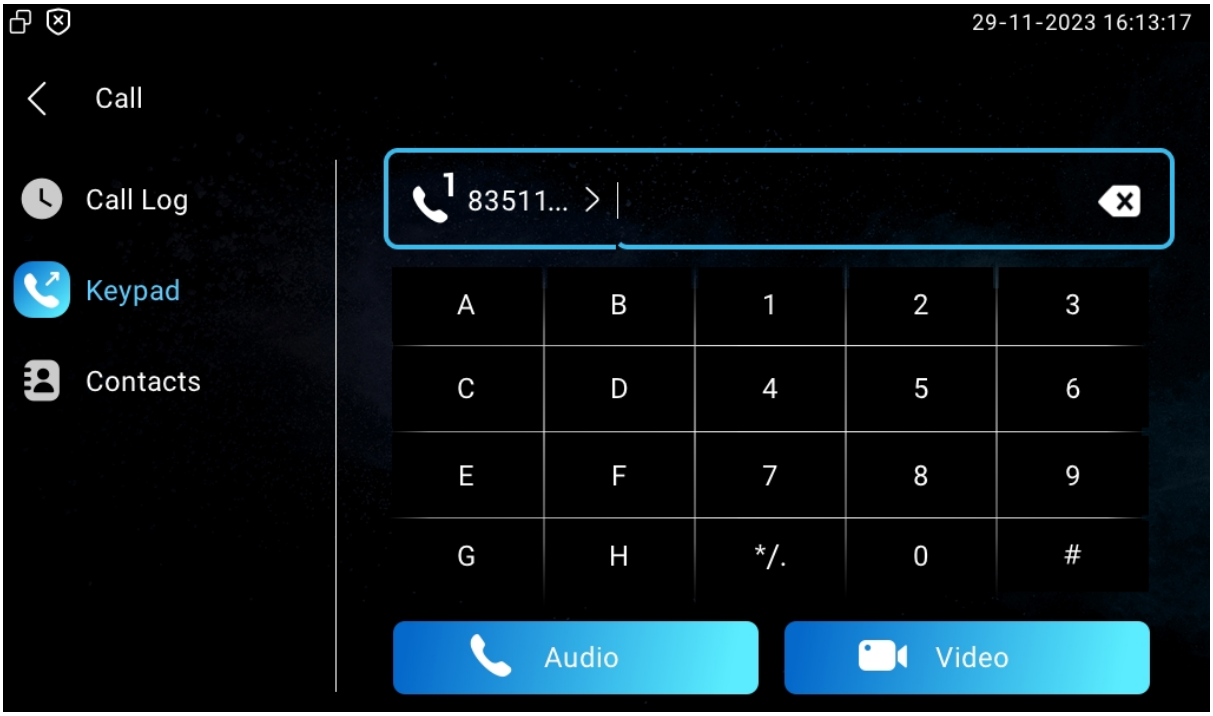
Intercom Call Configuration

IP Call Configuration

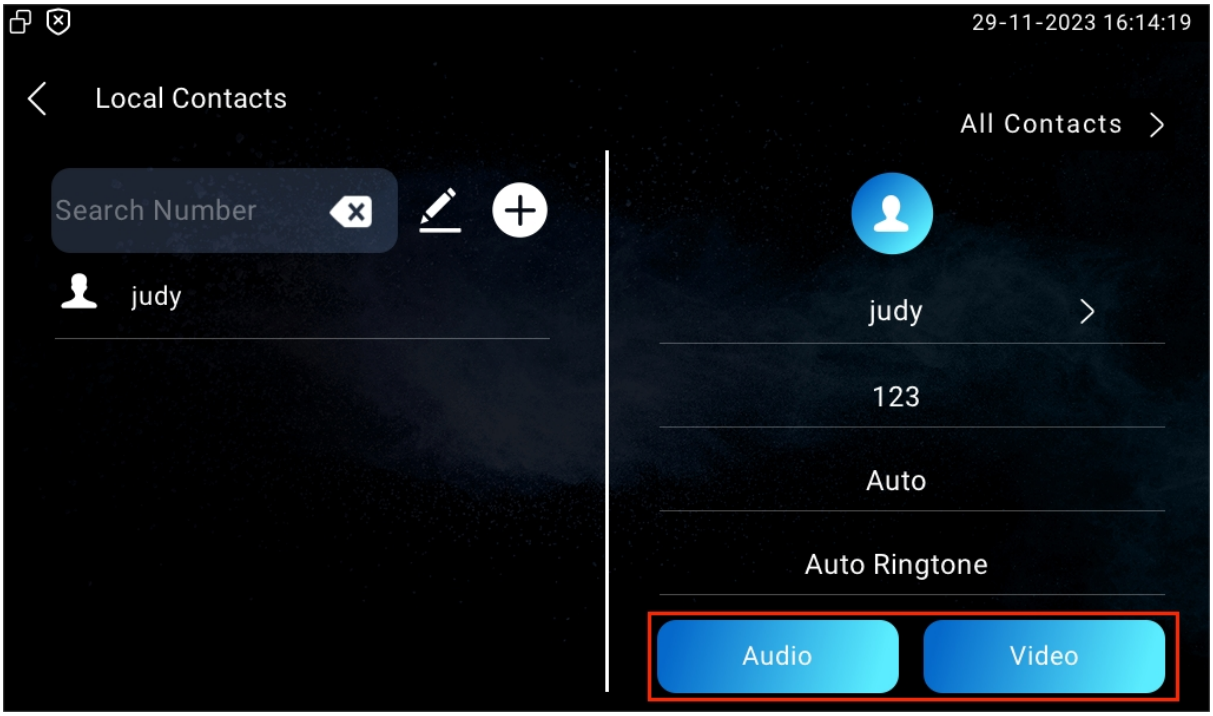
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Make IP Calls

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

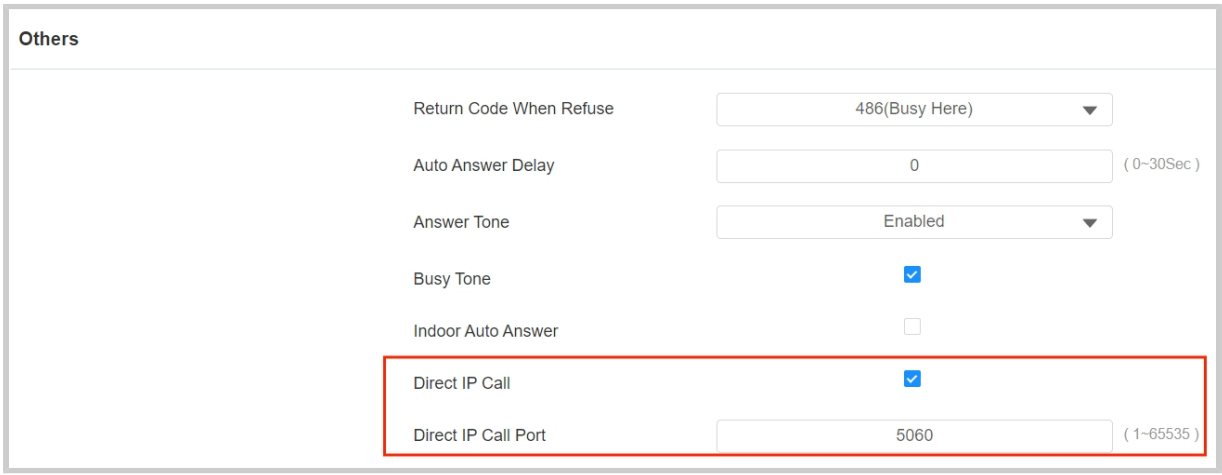


In addition, you can also make IP calls on the **Contacts > Local Contacts** screen.



IP Call Setup

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



- **Direct IP Call**: If you do not allow direct IP calls to be made on the device, you can untick the check box to terminate the function.

- **Direct IP Call Port**: Set the port for direct IP calls. The default is 5060, with a range from 1-65535. If you enter a value within this range other than 5060, ensure consistency with the corresponding device for data transmission.

SIP Call Configuration

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

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

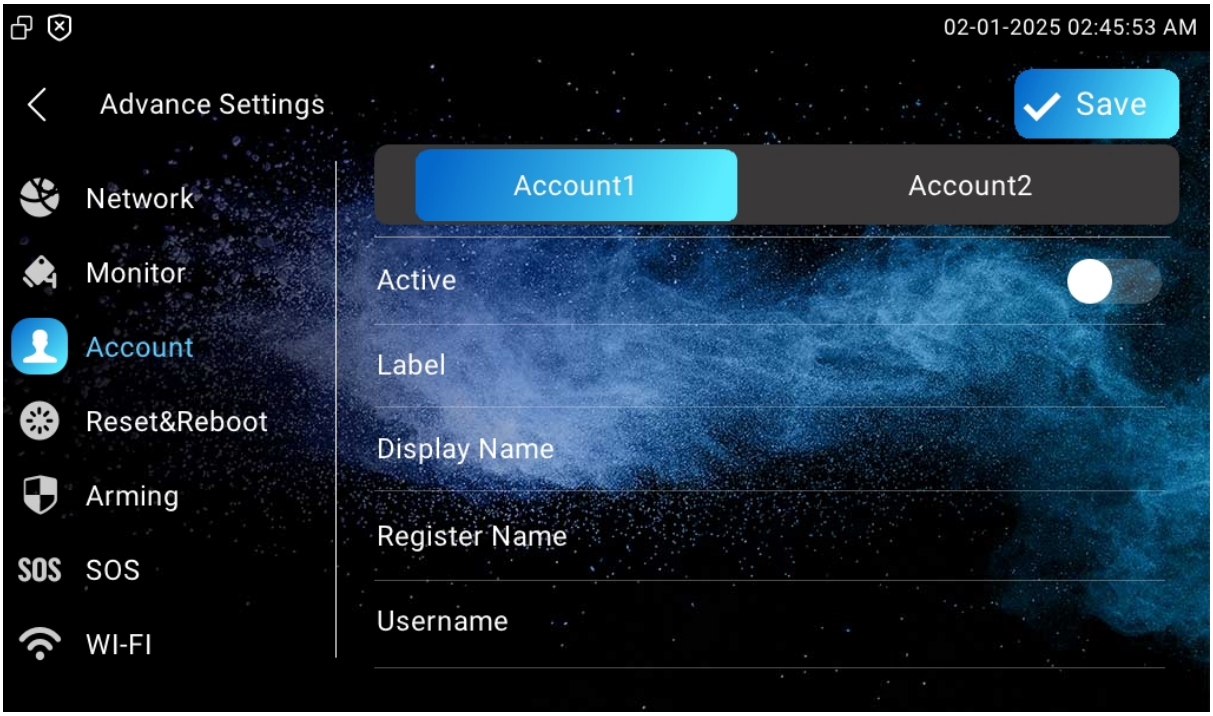
SIP Account Registration

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

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

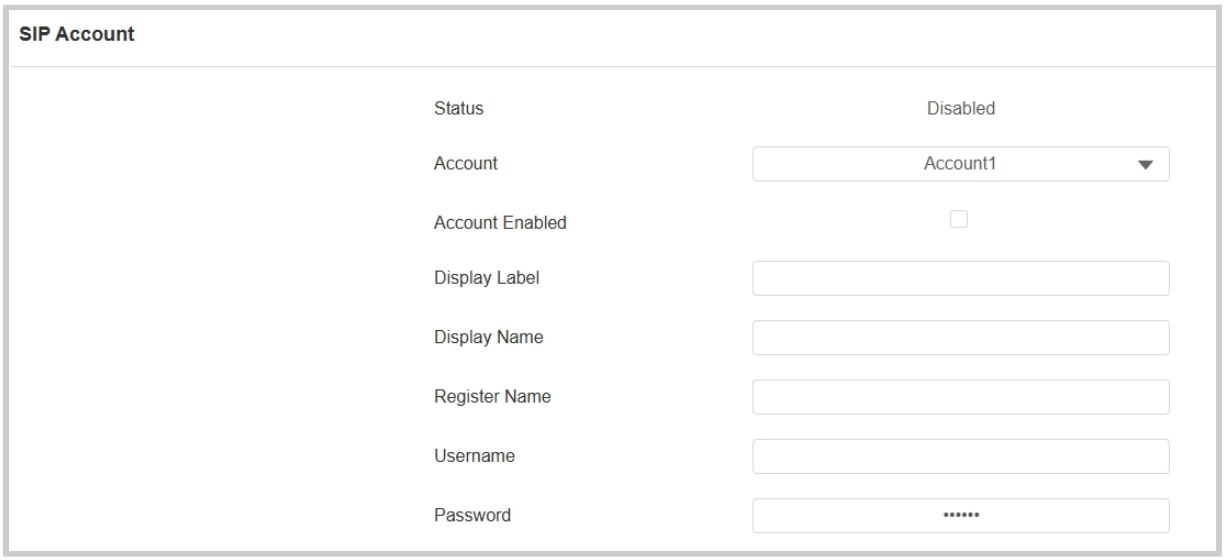
Click here to view the SIP account registration example.

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



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

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



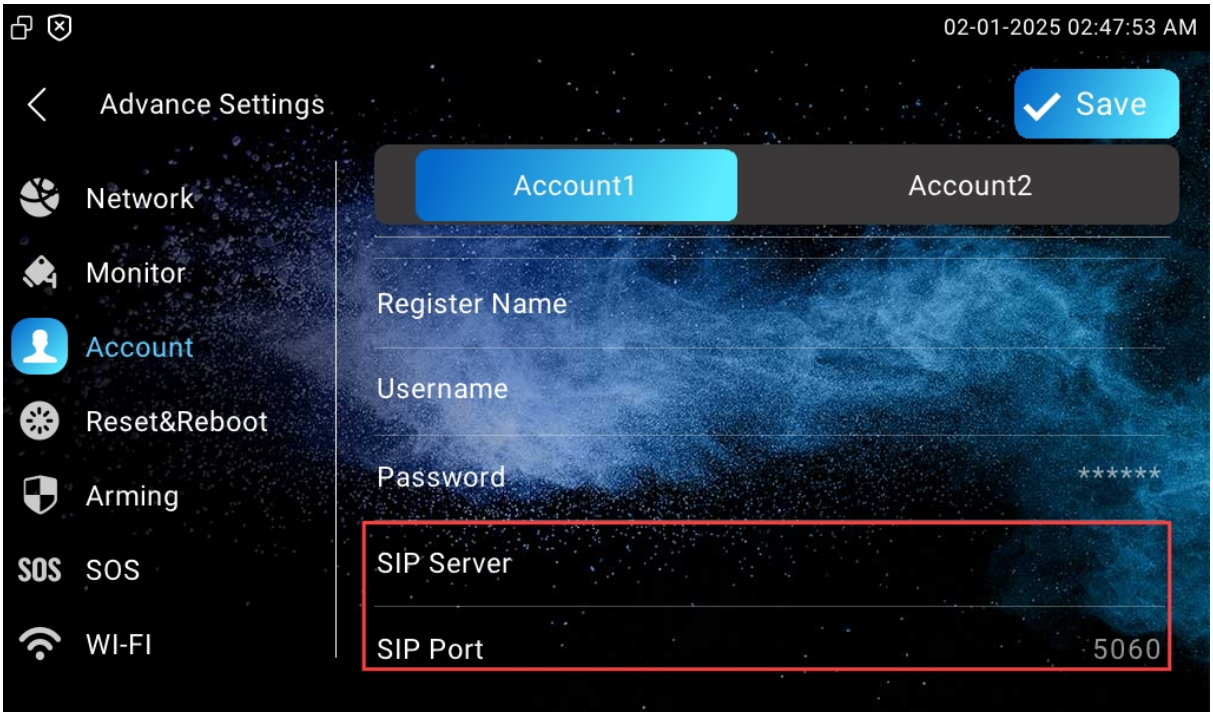
- **Status:** Indicate whether the SIP account is registered or not.
- **Account:** Choose the account for configuration.
- **Display Label:** The label of the device.
- **Display Name:** The designation for Account 1 or 2 to be shown on the device itself on the calling screen.
- **Register Name:** Same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

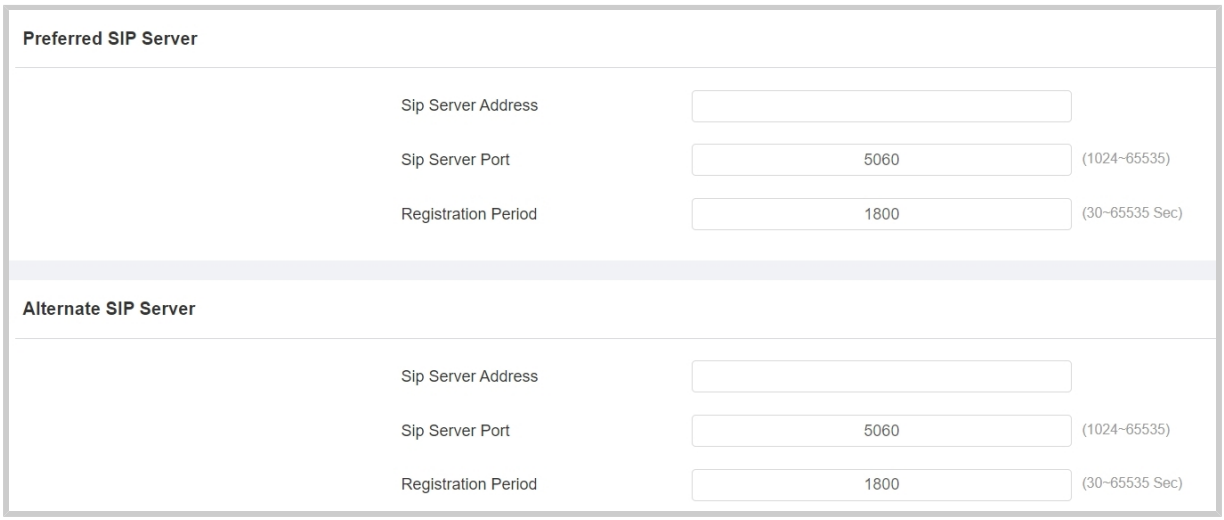
> **Tip**
>
> When the device is connected to the SmartPlus Cloud, the display label, register name, and username will show its SIP number.

SIP Server Configuration

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

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



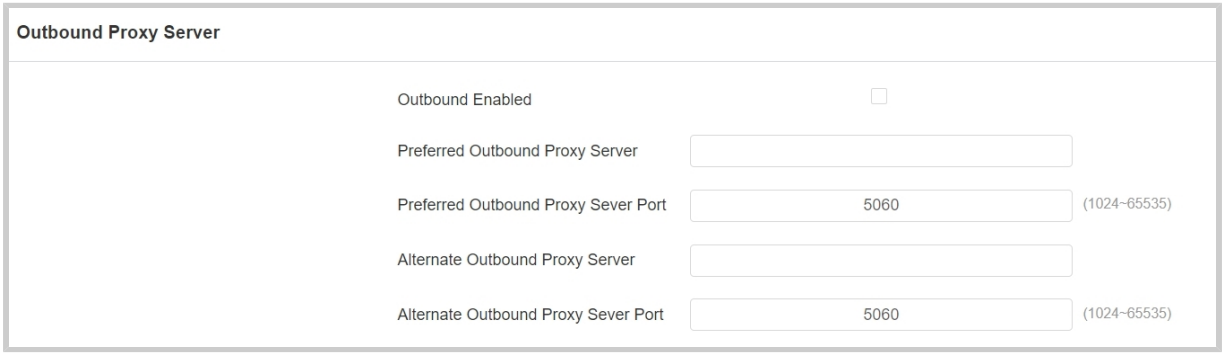


- **SIP Server Address**: Enter the server's IP address or its domain name.
- **SIP Server Port**: Specify the SIP server port for data transmission.
- **Registration Period**: Define the time limit for SIP account registration. Automatic re-registration will initiate if the account registration fails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

Outbound Proxy Server

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

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

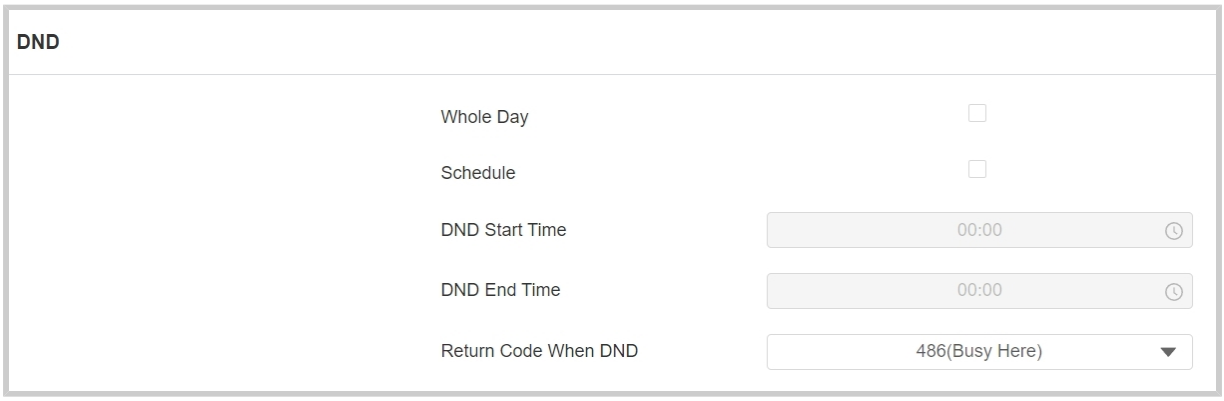


- **Preferred Outbound Proxy Server**: Enter the SIP proxy IP address.
- **Preferred Outbound Proxy Server Port**: Set the port for establishing a call session via the outbound proxy server.
- **Alternate Outbound Proxy Server**: Enter the SIP proxy IP address to be used when the main proxy malfunctions.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

SIP Call DND & Return Code Configuration

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

To set it up, go to **Device > Call Feature > DND** interface. You can also set up DND on the device. Tap **Settings > DND**.



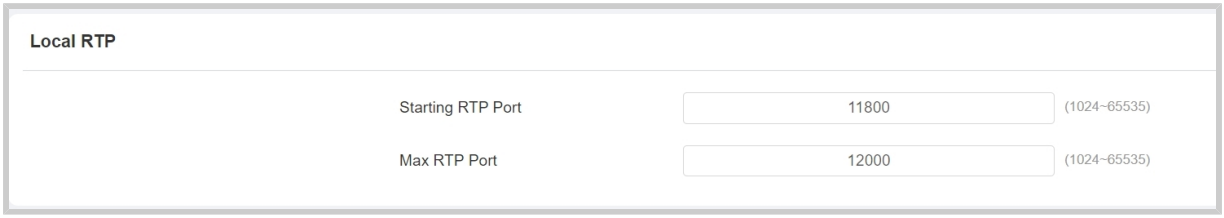
- **DND**: Check **Whole Day** or **Schedule** to enable the DND function. The DND function is disabled by default.
- **Schedule**: Determine the DND period by selecting DND Start Time and DND End Time.
- **Return Code When DND**: Specify the code sent to the caller via the SIP server when rejecting an incoming call in DND mode.

Device Local RTP

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

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

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



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

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

Data Transmission Type

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

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

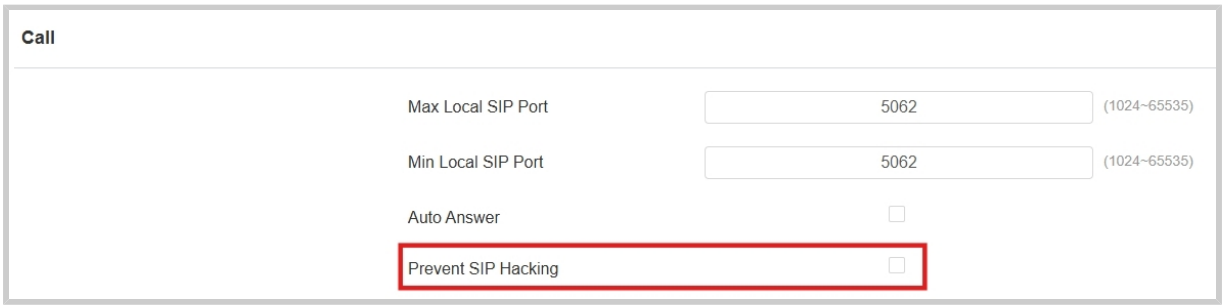


- **UDP:** An unreliable but very efficient transport layer protocol. It is the default transport protocol.
- **TCP:** A less efficient but reliable transport layer protocol.
- **TLS:** An encrypted and secured transport layer protocol. Select this option if you wish to encrypt the SIP messages for enhanced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

SIP Hacking Protection

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

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



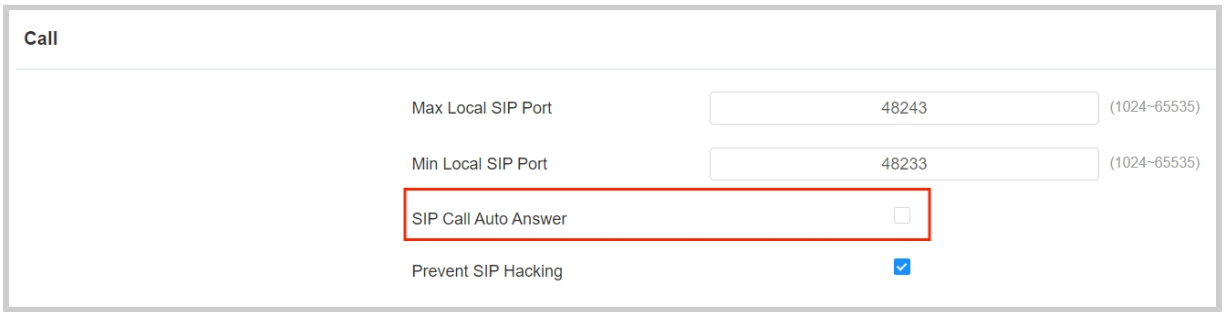
- **Prevent SIP Hacking:** Activate this feature to only receive calls from contacts in the whitelist. This protects users' private and secret information from potential hackers during SIP calls.

Call Setting

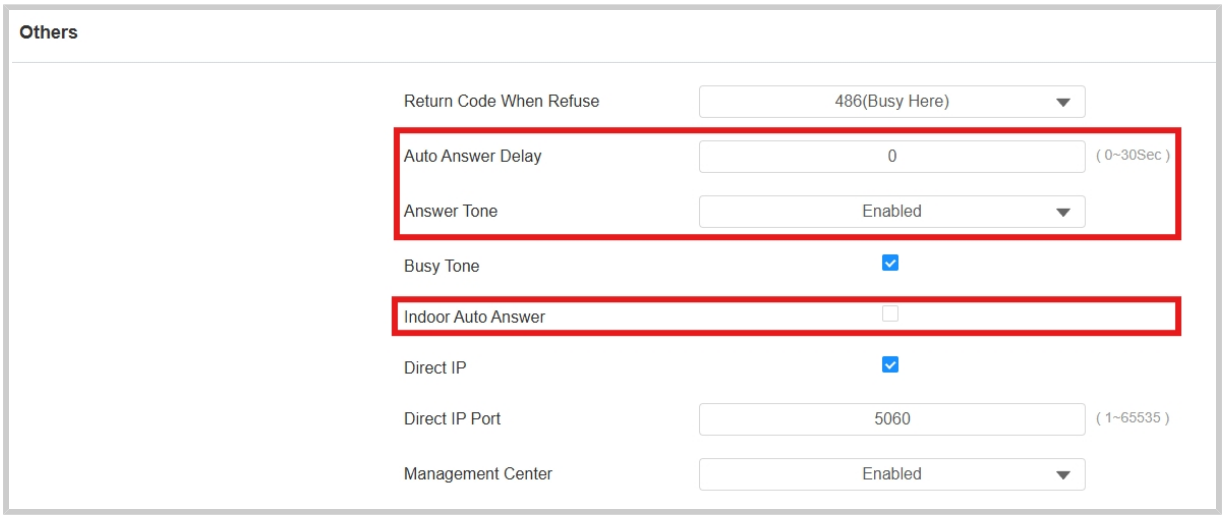
Auto-answer Configuration

Auto-answer feature allows the device to automatically pick up incoming calls without any manual intervention.

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



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



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

- **Indoor Auto Answer**: Allow calls from other indoor monitors to be answered by the device automatically.

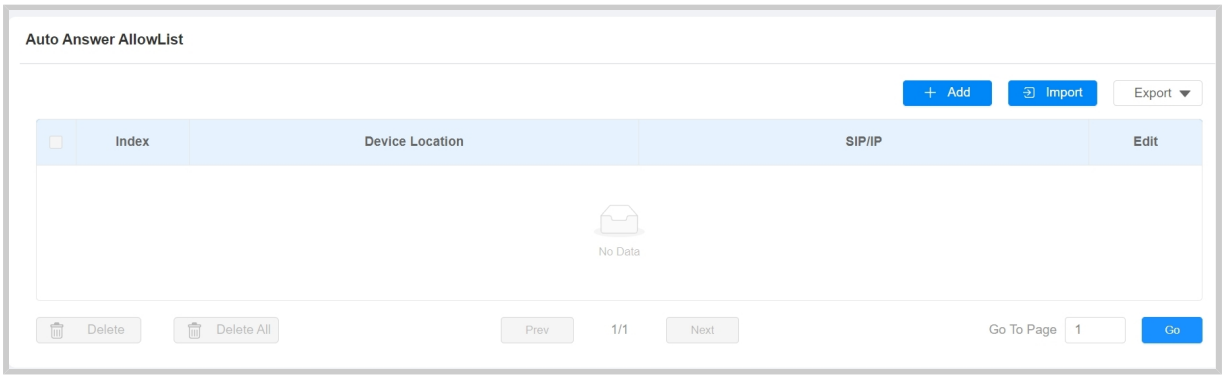
Other Options:

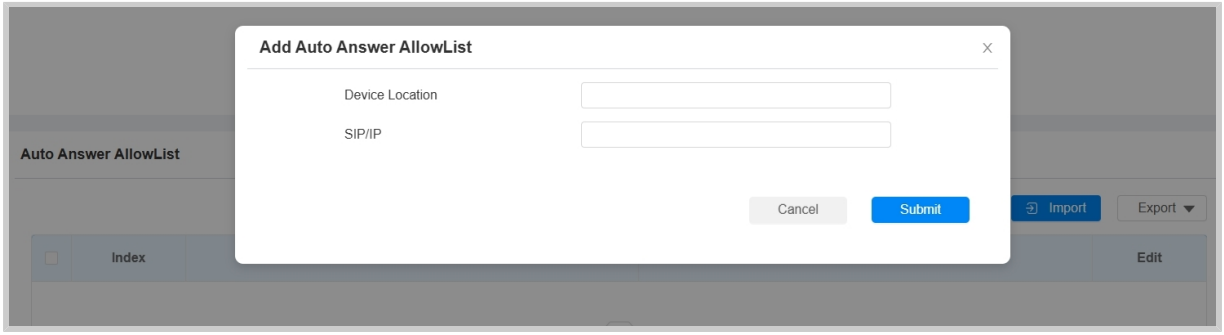
- **Return Code When Refuse**: Decide the code sent to the caller side via the SIP server when rejecting the incoming call.
- **Busy Tone**: Decide whether to sound a busy tone when a call is hung up by the callee.
- **Management Center**: Decide whether to generate the contact labeled Management Center.
  - When the device is deployed on the SmartPlus Cloud, the cloud system will issue the SmartPlus Property Manager App and the guard phone R49 as a contact labeled Management Center. When this function is disabled, the PM App and guard phone will be displayed as contacts separately.
  - When the device is deployed on the SDMC, SDMC is shown as Management Center on the device screen. When the function is disabled, no contacts will be displayed as Management Center.

Auto-answer Allowlist Setting

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

To set it up, go to the **Device > Call Feature > Auto Answer AllowList** interface. Click **+Add** to add the allowed device.





- **Device Location**: Specify the allowed device's name or location.
- **SIP/IP**: Enter the allowed device's SIP or IP number.

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

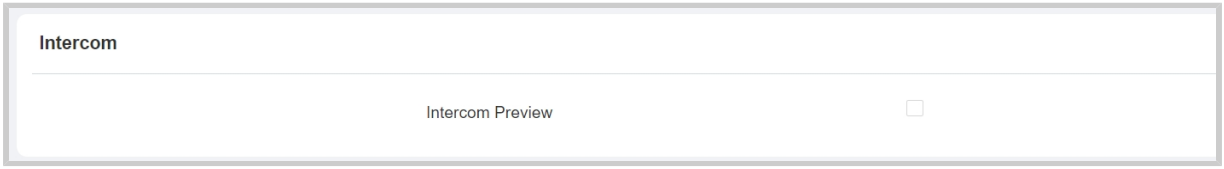


Note

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

Intercom Preview

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

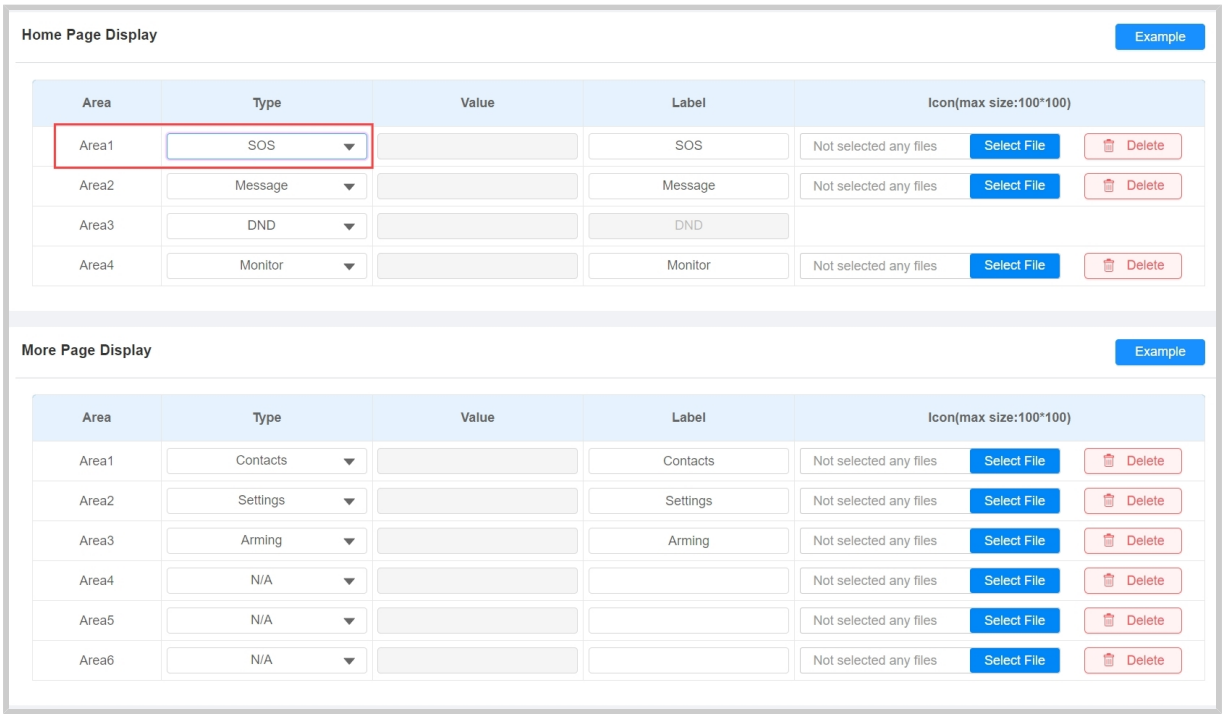


- **Intercom Preview**: It is disabled by default. When it is enabled, the group call is not available. Enabling **Intercom Preview** option or not depends on whether the other party features RTSP.
  - For devices without RTSP: Enable this option. The indoor monitor will automatically answer incoming calls and display the live stream on the preview screen.
  - For devices with RTSP: Disable this option, as RTSP already provides real-time audio and video for intercom preview.

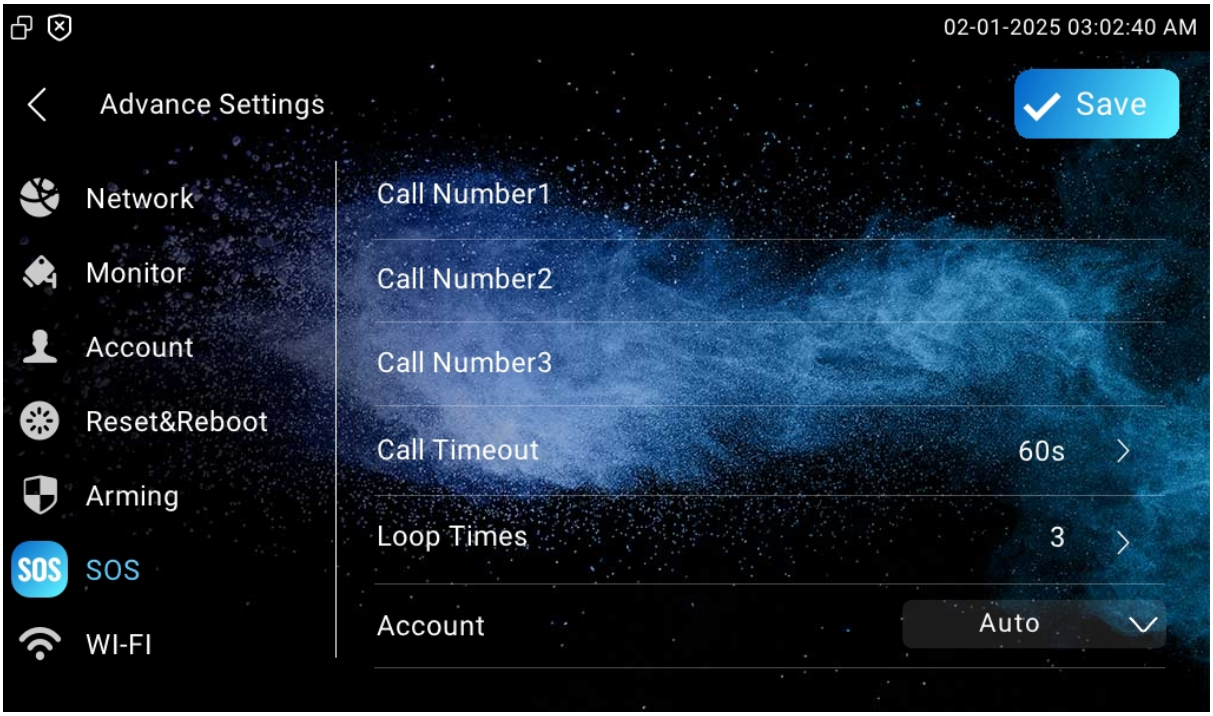
Emergency Call

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

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

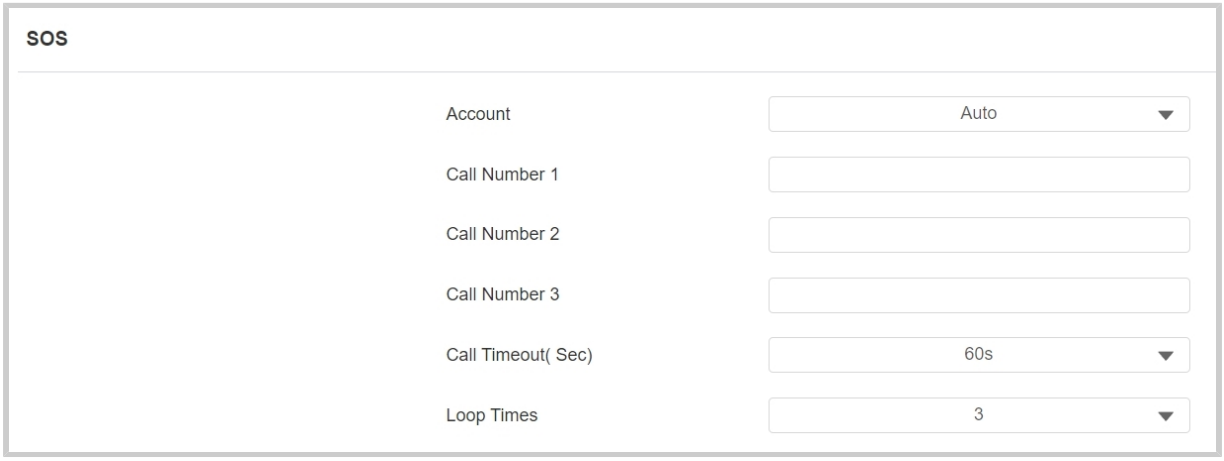


You also need to set up specific parameters on the device or the device web interface. To set it up on the device, go to **Settings > Advance Settings > SOS** screen.



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

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

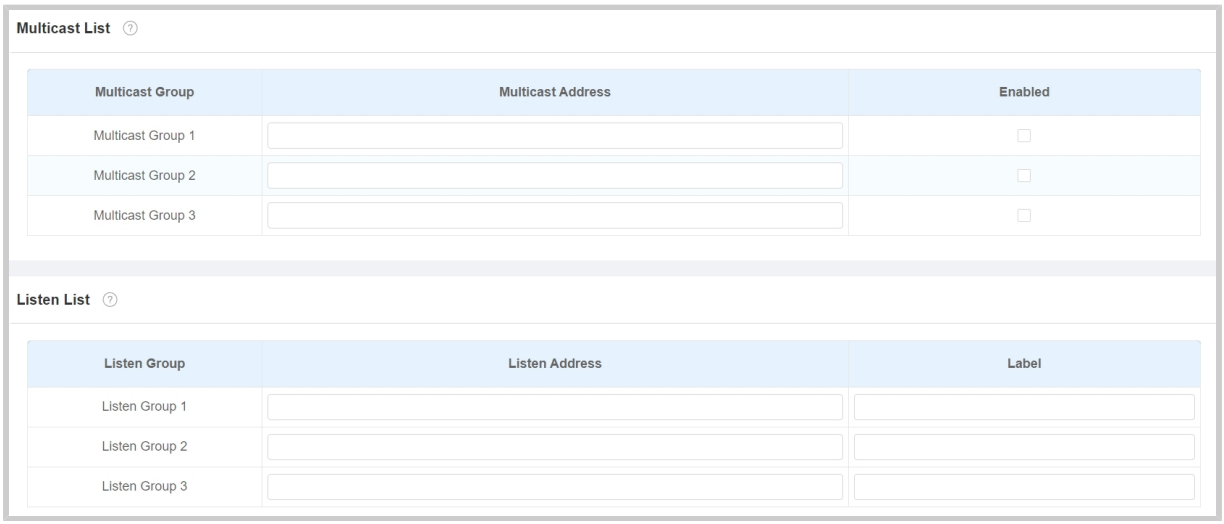


Multicast

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

Click here to watch the demonstration video.

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



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

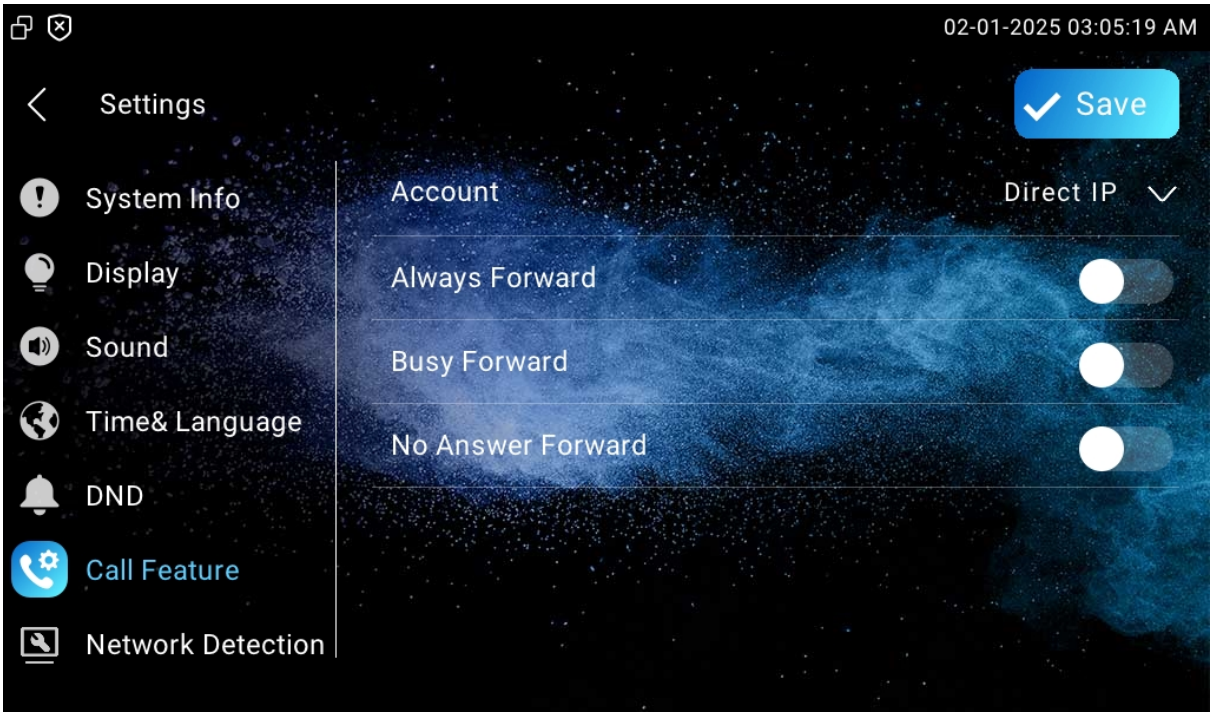
> **Note**
>
> The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult Akuvox tech team for more information.

Call Forwarding

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

On the Device

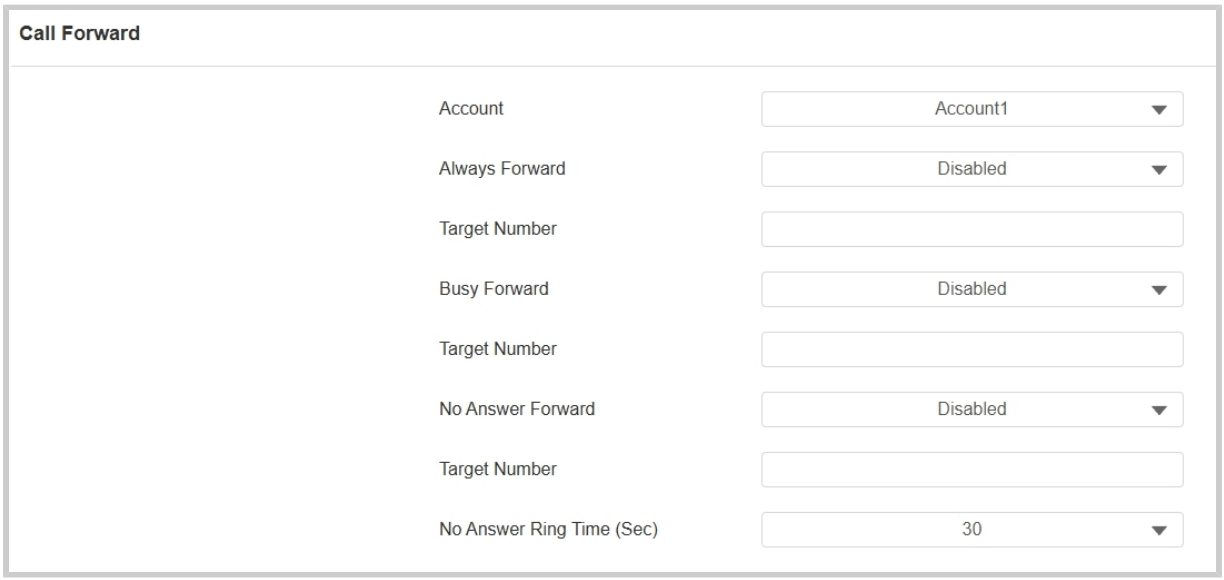
To set it up, go to the device **Settings > Call Feature** screen.



- **Account**: The account or direct IP call to implement the call forwarding feature.
- **Always Forward**: All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: Incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward**: Incoming calls will be forwarded to a specific number if the call is not picked up within no answer ring time.
- **Target Number**: Specify the forward number when Always Forward, Busy Forward, or No Answer Forward is enabled.
- **No Answer Ring Time(Sec)**: The time ranges from 0-120 seconds. This option appears when No Answer Forward is enabled.

On the Web Interface

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

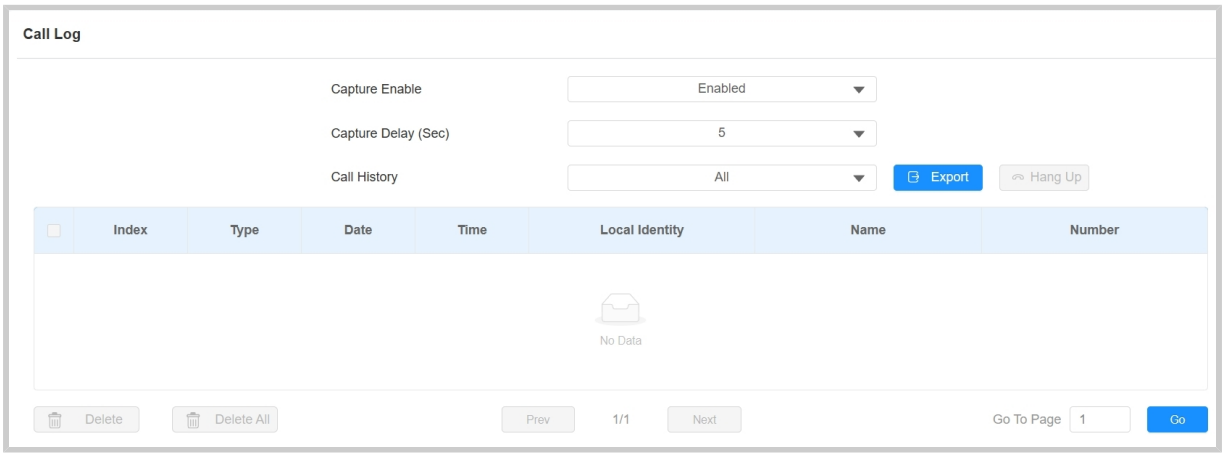


- **Account**: The account or direct IP call to implement the call forwarding feature.
- **Always Forward**: All incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: Incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward**: 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. This option appears when No Answer Forward is enabled.

Call Logs

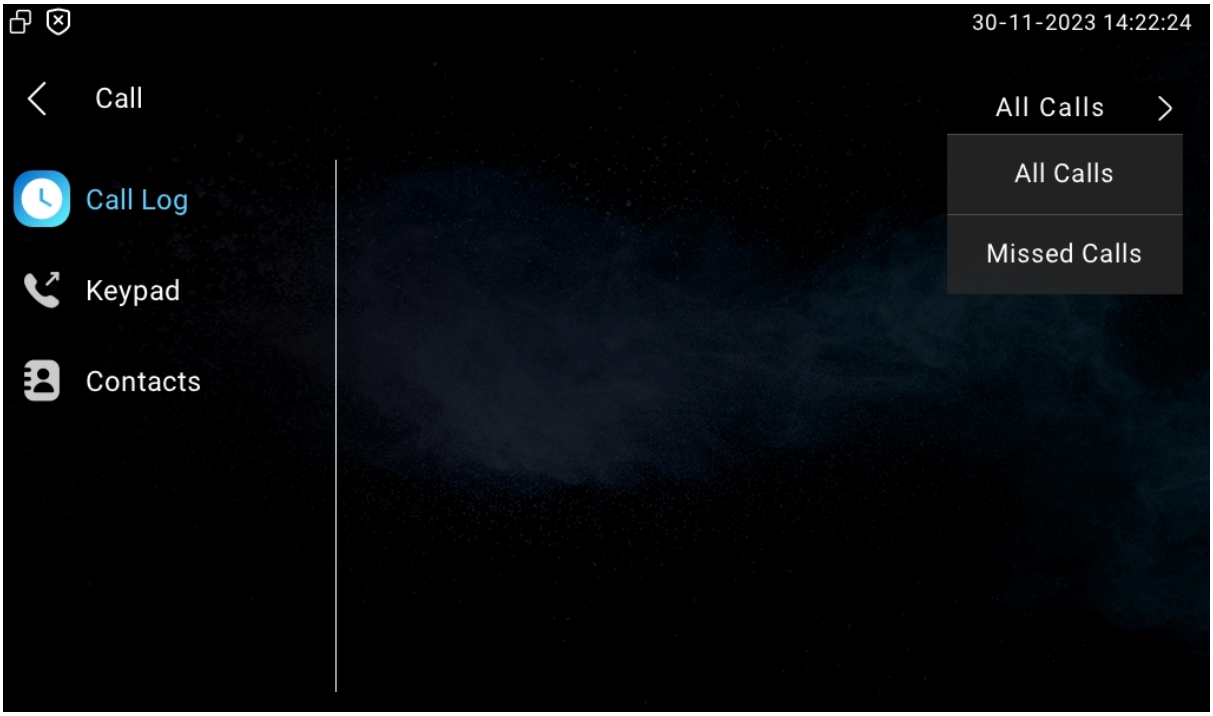
To check calls—including dial-out, received, and missed calls—within a specific period, you can view the call log on the device's web interface. If needed, you can also export the call log from the device.

To set it up, go to the **Contacts > Call Logs** interface. The device supports up to 100 local call logs.



- **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 Log**.

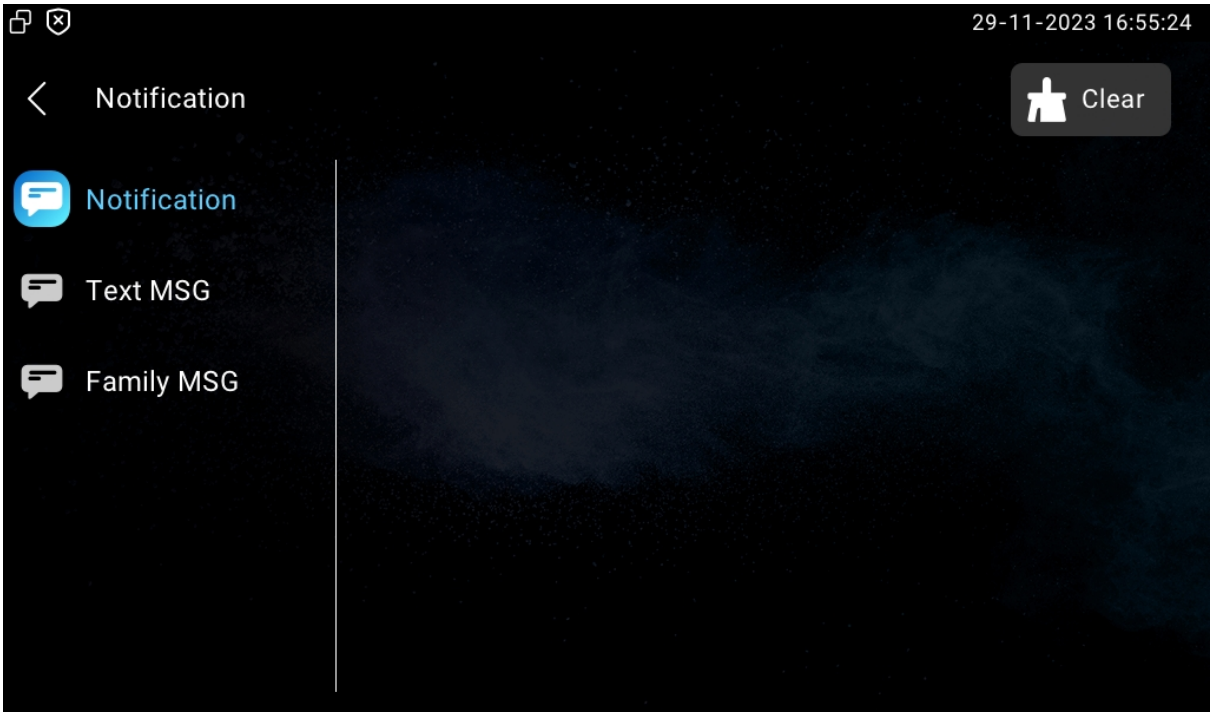

30-11-2023 14:22:24
Call
All Calls
Call Log
Keypad
Contacts
All Calls
Missed Calls

Intercom Message Setting

Manage Messages

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

Tap **+Add** to create a message and tap **Clear** to delete messages. The device can store up to 100 messages.



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

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

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

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



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

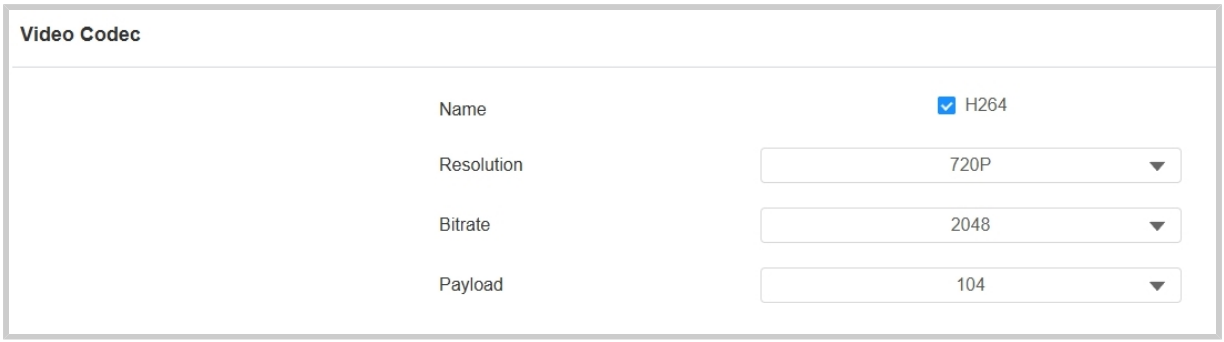
Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ

Codec Type	Bandwidth Consumption	Sample Rate
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Video Codec Configuration

The door phone 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, go to the web **Account > Advanced > Video Codecs** interface.



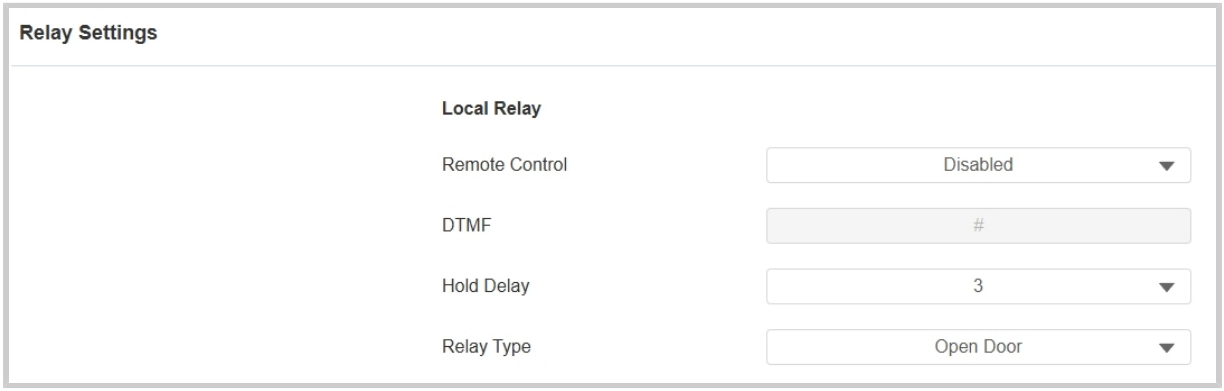
- **Resolution**: Specify the code resolution for the video quality. The default is 720P(1280X720 pixels).
- **Bitrate**: Select the video stream bitrate. It varies by the resolution. The default is 2048.
- **Payload**: The payload ranges from 90-119 for the audio/video configuration file.

Access Control Configuration

Local Relay

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

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



- **Remote Control**: Decide whether to control the indoor monitor's relay remotely by another intercom device. It is disabled by default.
- **DTMF**: The DTMF code to trigger the local relay.
- **Hold Delay(Sec)**: Determine how long the relay stays activated. For example, if set to 5 seconds, the relay remains open for 5 seconds before closing.
- **Relay Type**:
  - **Chime Bell Setting**: The relay is triggered when the indoor monitor receives calls, and the doorbell rings.
    - When the call is picked up, rejected, or hung up, the relay resets.
    - The relay trigger time is not limited to **Hold Delay** when the doorbell rings. It follows the settings on the Doorbell screen.

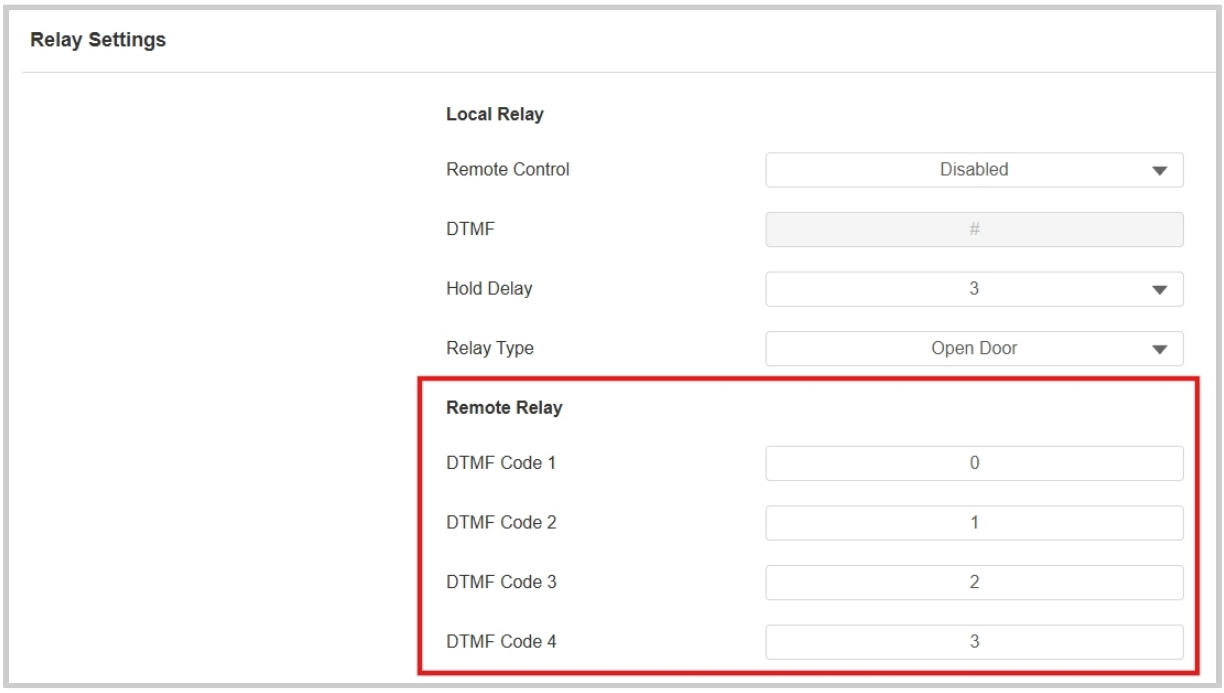
- **Open Door**: The relay is triggered when users open the door, such as by pressing the Unlock key and remotely opening via an HTTP command. In this case, the relay trigger time is not limited to the **Hold Delay**.

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

Remote Relay

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

Set it up on the web **Device > Relay > Relay Setting > Remote Relay** interface.



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

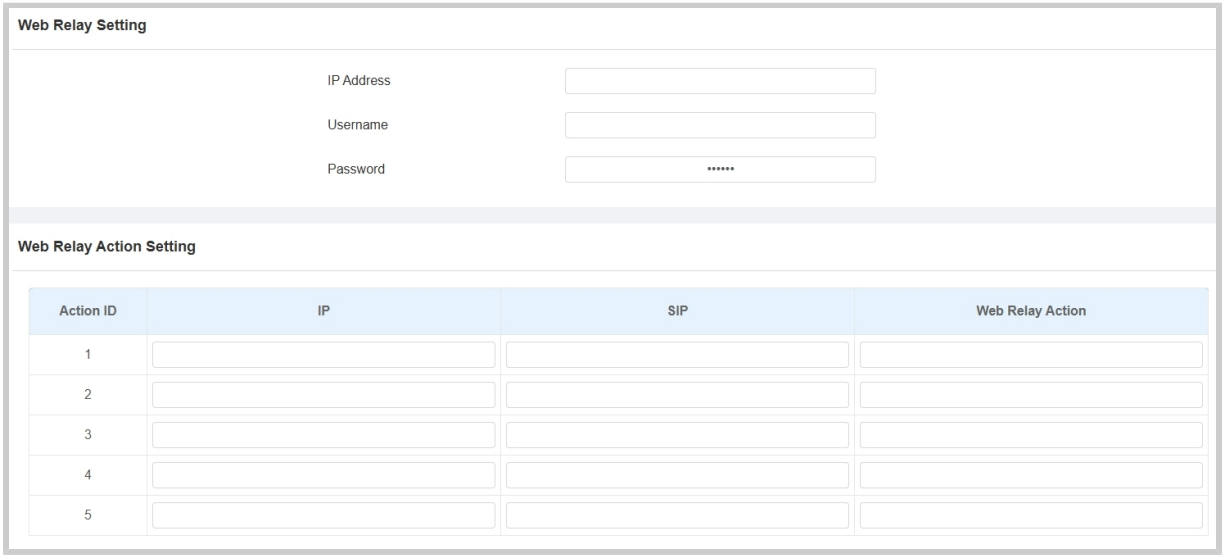
Web Relay

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



Click here to view how to set up web relay.

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



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

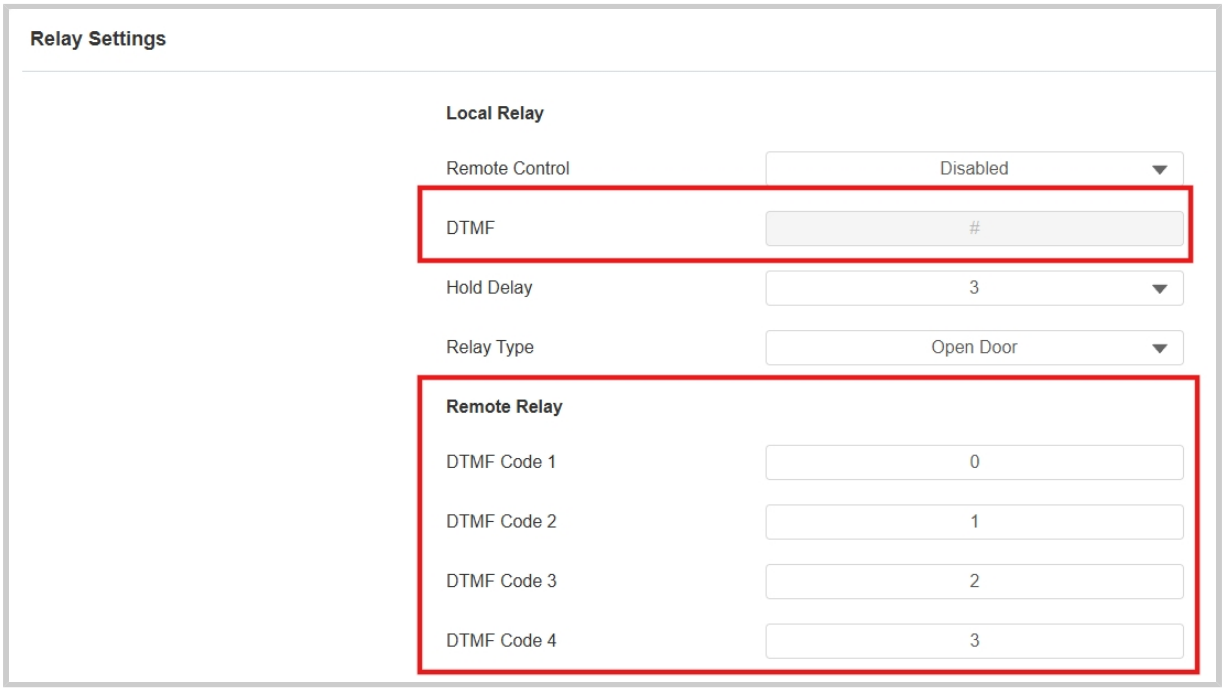
> **Note**
>
> If the URL includes full HTTP content(e.g., http://admin:admin@192.168.1.2/state.xml?relayState=2), it doesn't rely on the IP address that you entered above. However, if the URL is simpler (e.g., "state.xml?relayState=2"), the relay uses the entered IP address.

Door-opening Configuration

Unlock by DTMF Code

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

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



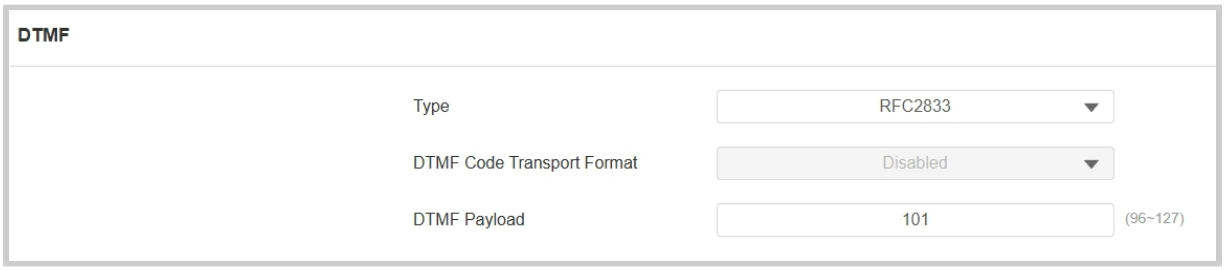
DTMF Transport Type

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

DTMF Type Differences:

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

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



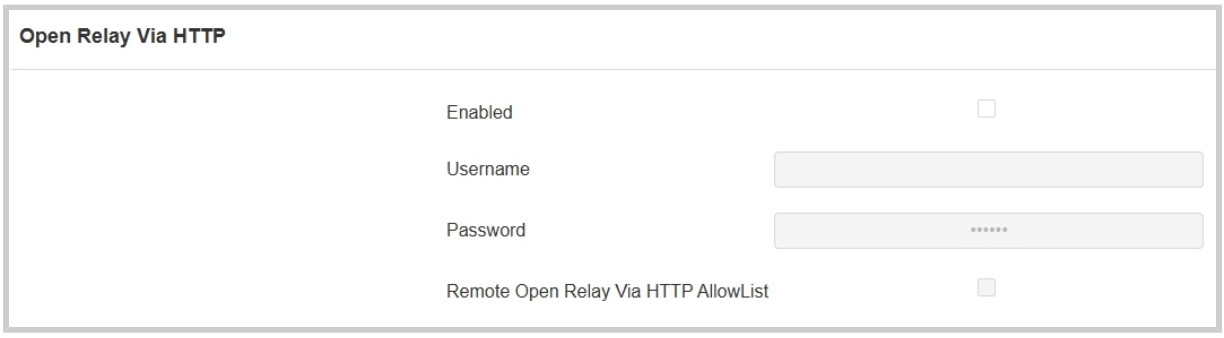
- **Type**: Select from the provided options.
- **DTMF Code Transport Format**: There are four options: Disabled, DTMF, DTMF-Relay, and Telephone-Event. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via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

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

Unlock via HTTP Command

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

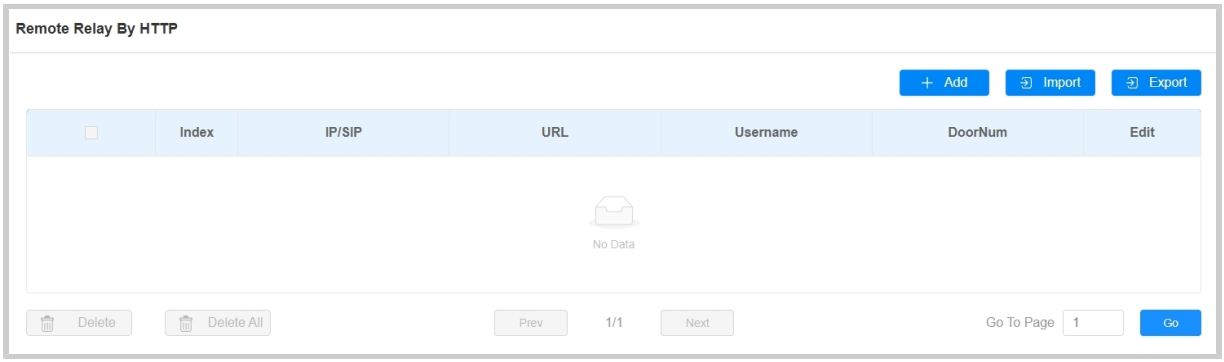
To set it up, go to the web **Device > Relay > Open Relay via HTTP** interface.



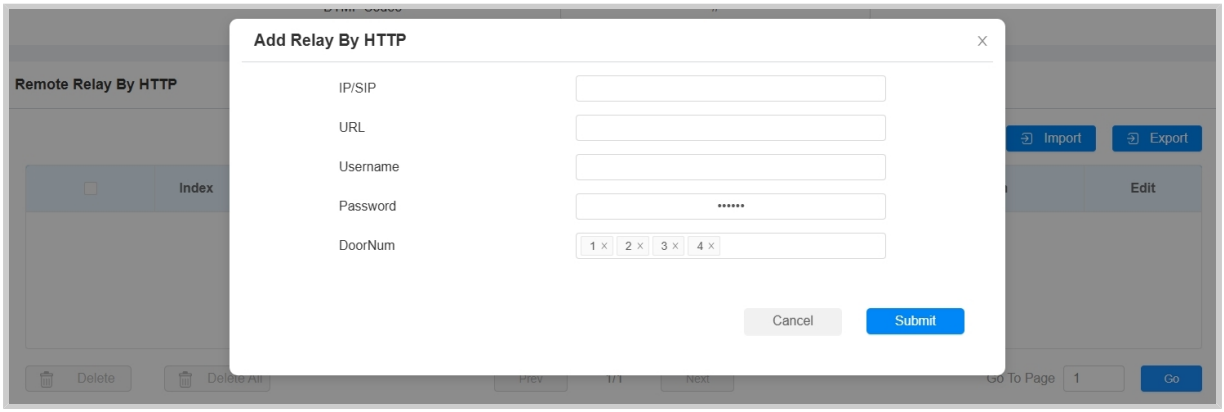
- **Username**: Set a username for authentication in HTTP command URLs.
- **Password**: Set a username for authentication in HTTP command URLs.
- **Remote Open Relay Via HTTP AllowList**: Enable it and type in the IP address of the server that you allow to send the HTTP command to the indoor monitor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

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

You can also set up HTTP commands to remotely control relays connected to door phones. Go to the web **Device > Relay > Remote Relay By HTTP** interface.



Click **Add** to add an HTTP command.



- **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 configured on the door phone's web interface.
- **Password**: Enter the password the same as that configured on the door phone's web interface.
- **DoorNum**: Specify the door to be opened.

Tip

Here is an HTTP command URL example for relay triggering.



Note

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

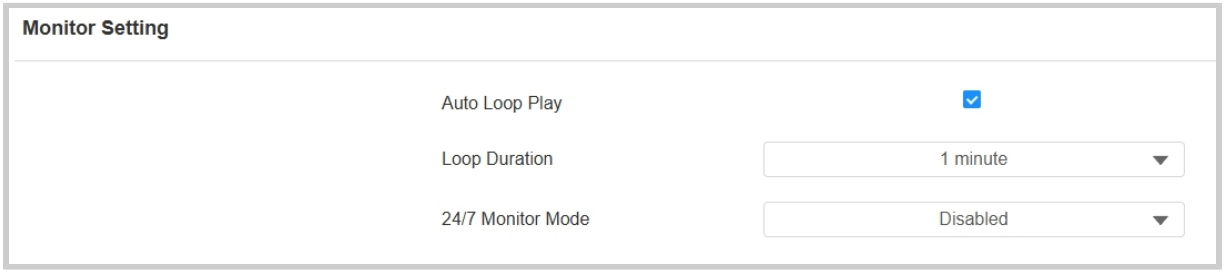
Security

Monitor and Image

Monitor Setting

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

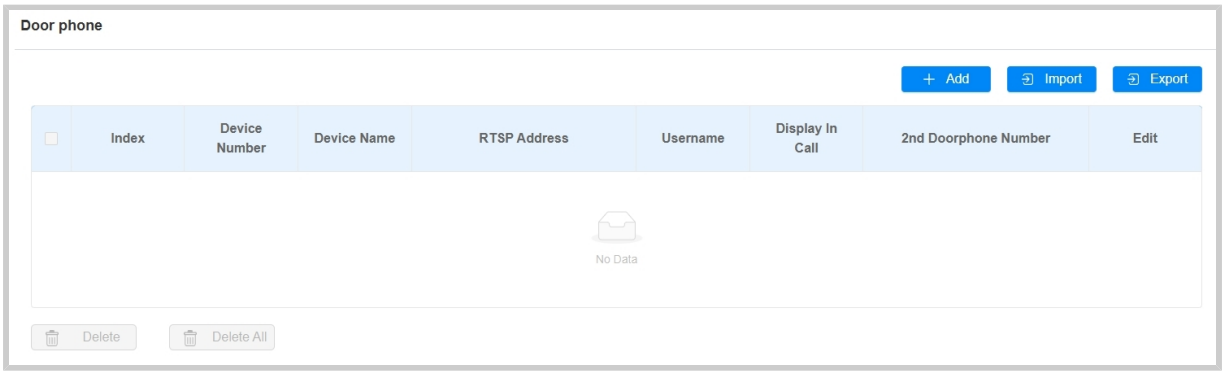
To set it up, go to the **Device > Monitor** interface.

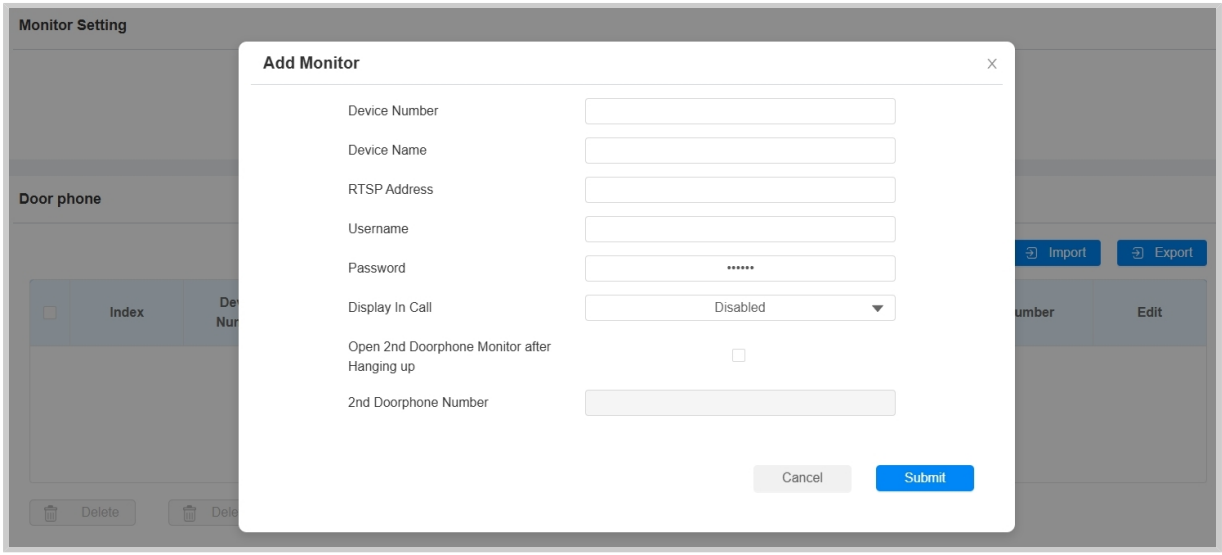


- **Auto Loop Play**: Set whether to play all monitoring streams in rotation.
- **Loop Duration**: The duration of playing each monitoring stream. The default is 1 minute.
- **24/7 Monitor Mode**: When enabled, the indoor monitor displays the monitoring screen for 6 hours, then plays a 10-second screensaver before resuming the monitoring stream. This feature ONLY applies to door phones added via local RTSP.

> **Note**
>
> If devices are deployed on SmartPlus Cloud, the video stream from door phones is limited to 3 minutes and is not controlled by the 24/7 Monitor Mode.

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

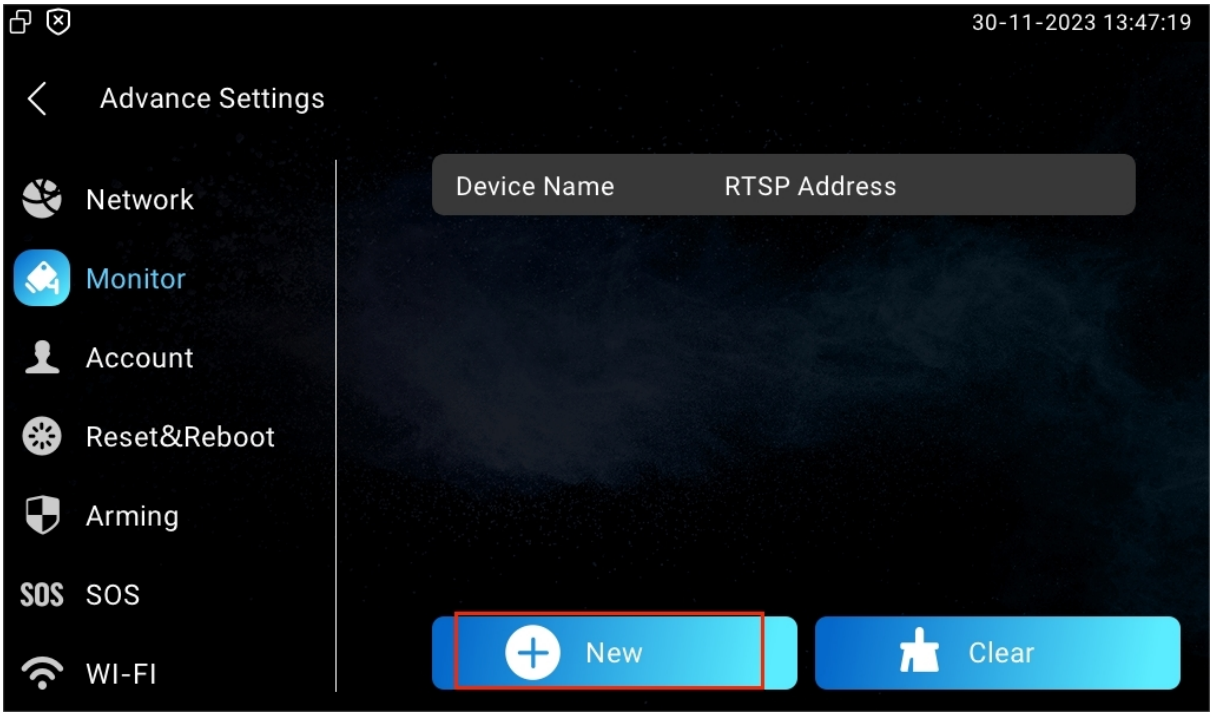


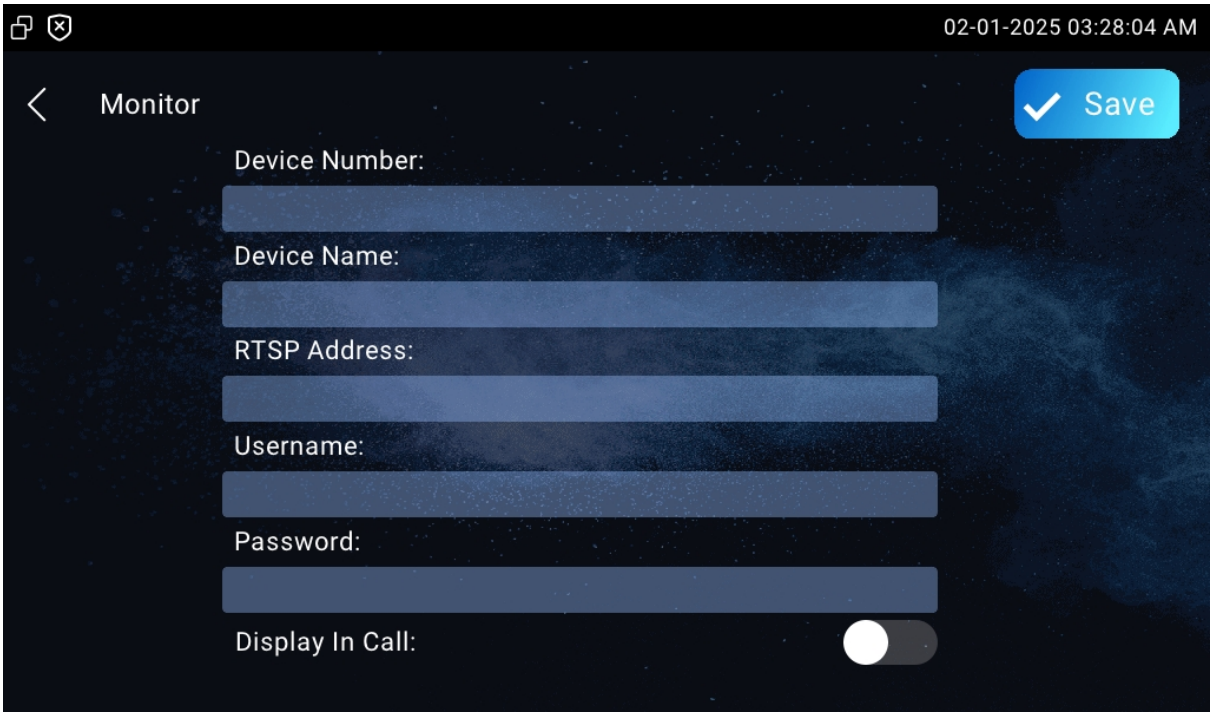


- **Device Number**: The device's SIP/IP number for identification.
- **Device Name**: The device name for identification.
- **RTSP Address**: The RTSP address of the monitoring device. RTSP format: *rtsp://Device IP address/live/ch00_0.*
- **Username**: The username of the monitoring device for authentication.
- **Password**: The password of the monitoring device for authentication.
- **Display In Call**: Enable it to display the monitoring video during a call.
- **Open 2nd Doorphone Monitor after Hanging up**: Disabled by default. If enabled, when a call ends between the indoor monitor and the door phone (the added monitor), the indoor monitor will automatically display the live stream from the 2nd door phone.
- **2nd Doorphone Number**: SIP or IP number of the 2nd door phone.

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

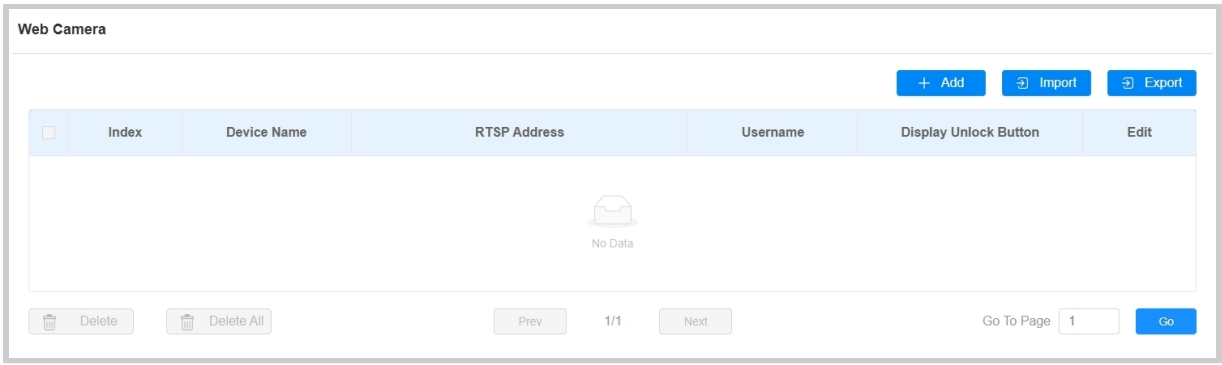
You can also set it up on the device **Settings > Advance Settings > Monitor** screen.



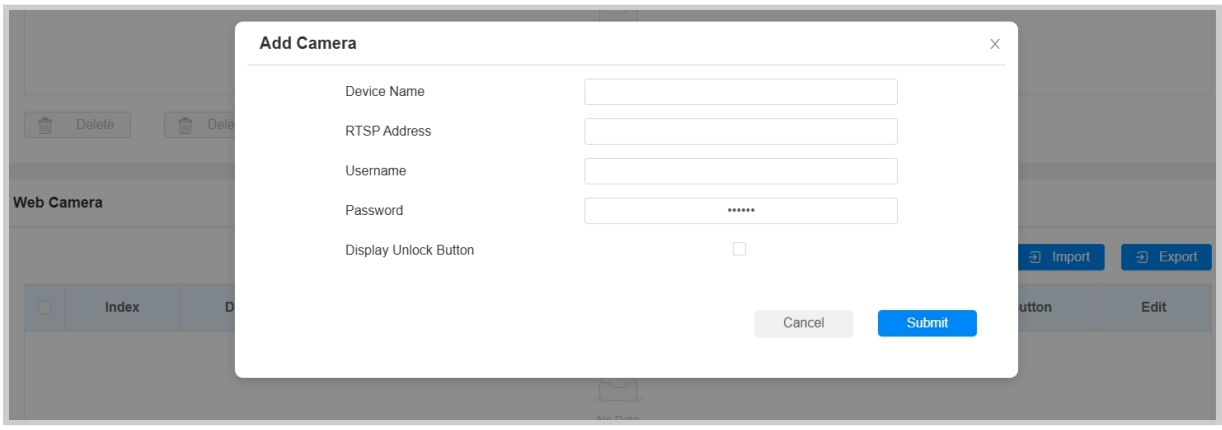


Web Camera Setting

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



Click **Add** to add a camera.



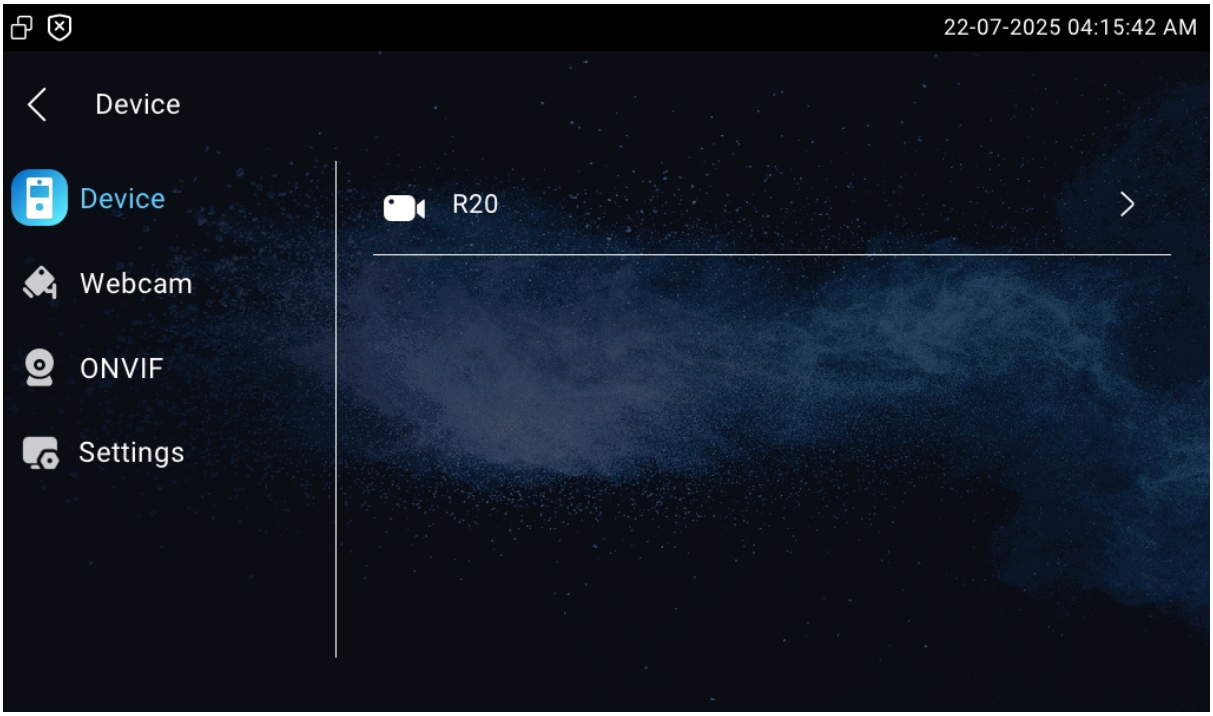
- **Device Name**: The name of the third-party camera.
- **RTSP Address**: The RTSP URL for the third-party camera. Confirm it with the third-party service provider.
- **Username**: The username of the monitoring device for authentication.
- **Password**: The password of the monitoring device for authentication.
- **Display Unlock Button**: Disabled by default. Set whether to display the Unlock tab when viewing the live stream from the third-party camera.

You can also import or export the monitor list in batch on the same interface. The import file only supports the **.xml** format.



View Monitoring Streams

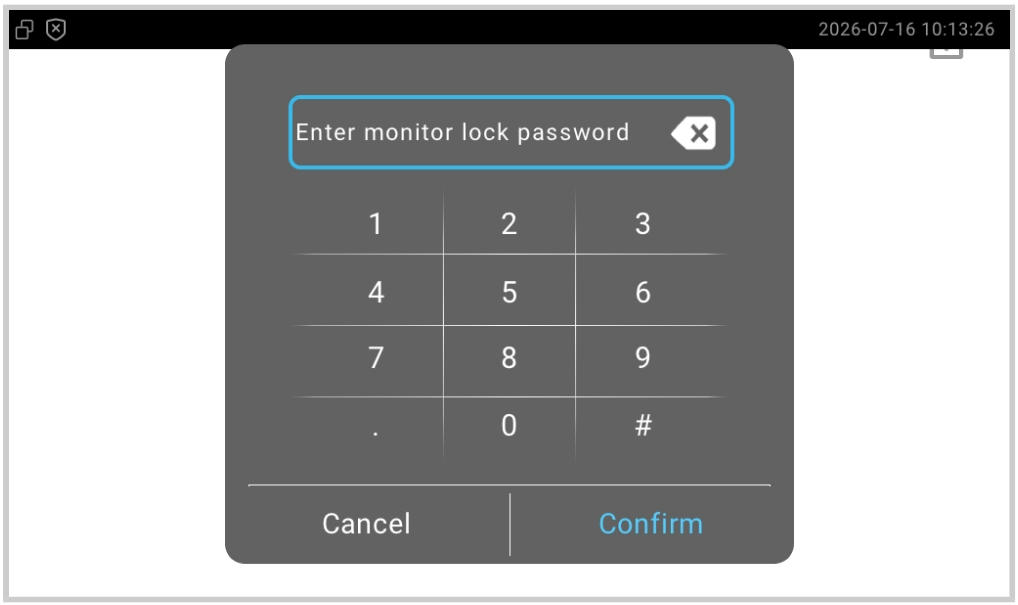
After adding the monitored device's RTSP URL, tap **Monitor** on the home screen and tap the device name to view the stream.

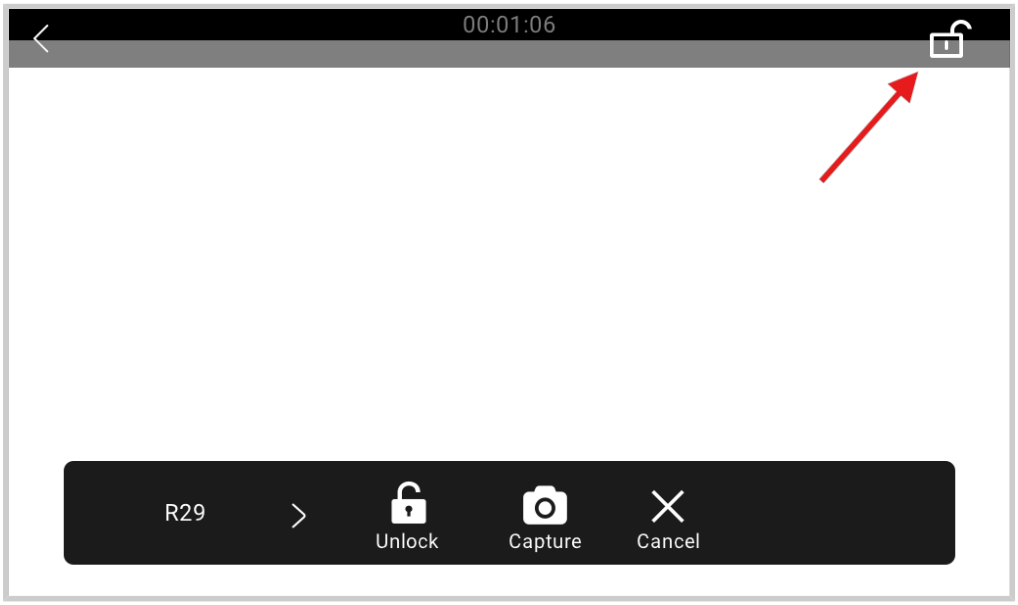


Monitor Lock

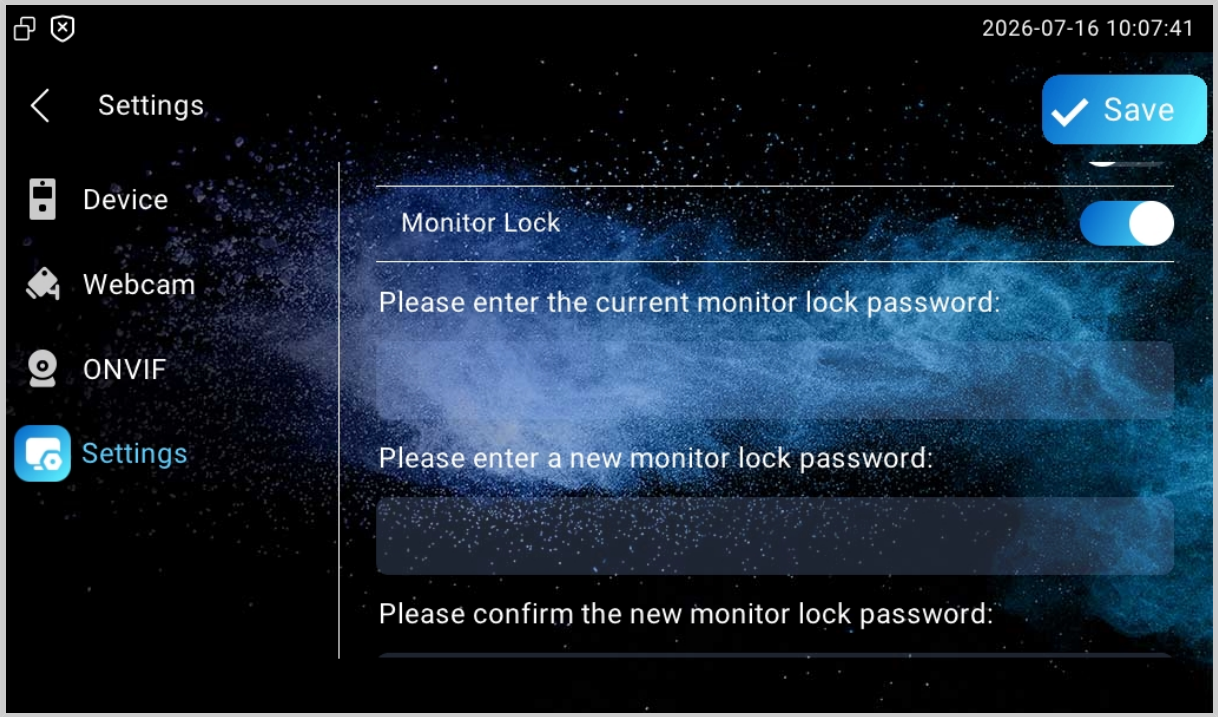
Monitor Lock restricts access to the live view controls by requiring password verification. When enabled, all on-screen controls and the Back button are hidden, and a lock icon is displayed in the upper-right corner.

After the correct password is entered, the screen is unlocked. Tapping the unlocked icon locks the screen again.





To set it up, go to **Monitor > Settings** on the device's screen.

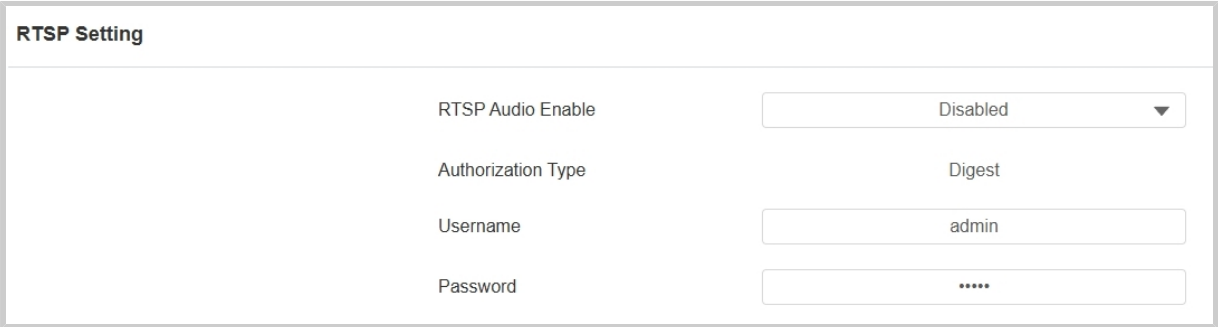


- **Monitor Lock**: Enable/disable the feature.
- **Password**: Set the password required to unlock the live view screen. The password is empty by default.

RTSP Authentication

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

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



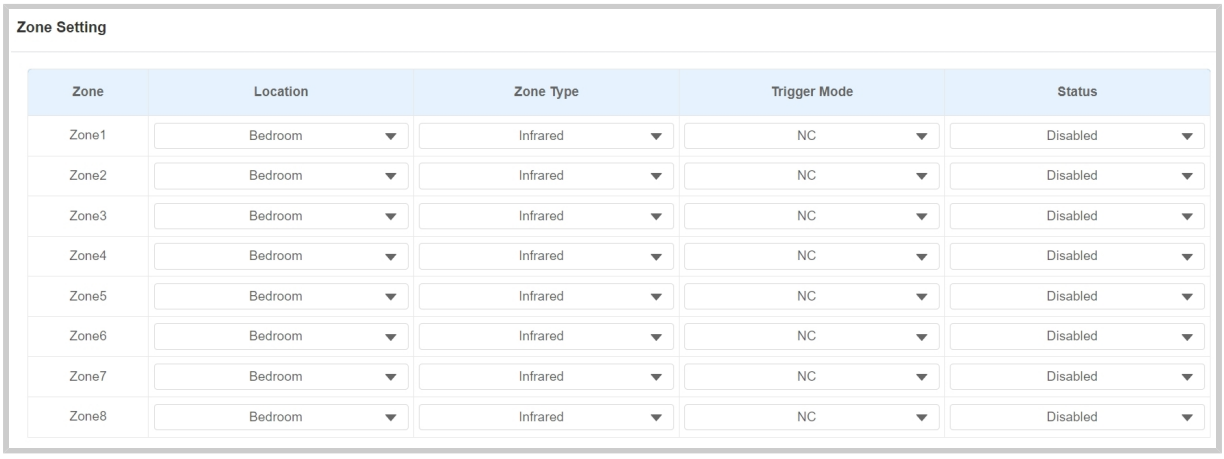
- **RTSP Audio Enable**: Enable it if you want to monitor the device via RTSP audio stream.
- **Authorization Type**: It is Digest by default.
- **User Name**: Set the username for the authentication.
- **Password**: Set the password for the authentication.

Alarm and Arming Configuration

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

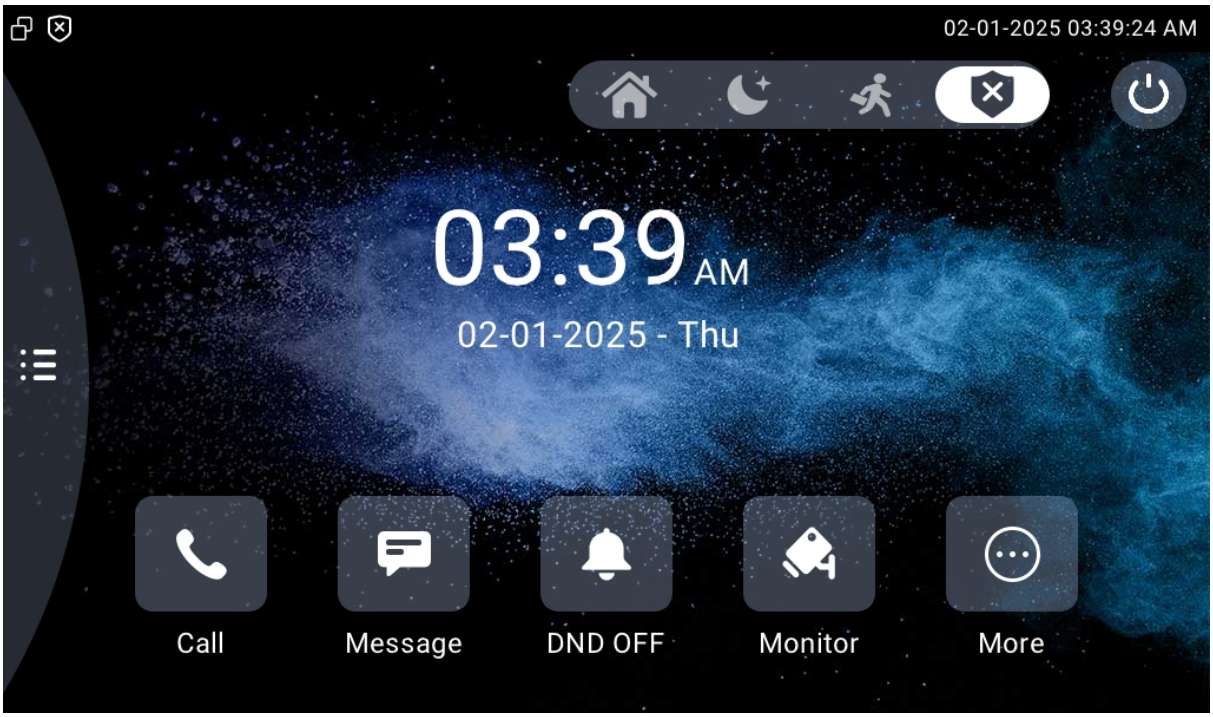
Set up Location-based Alarm Sensors

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

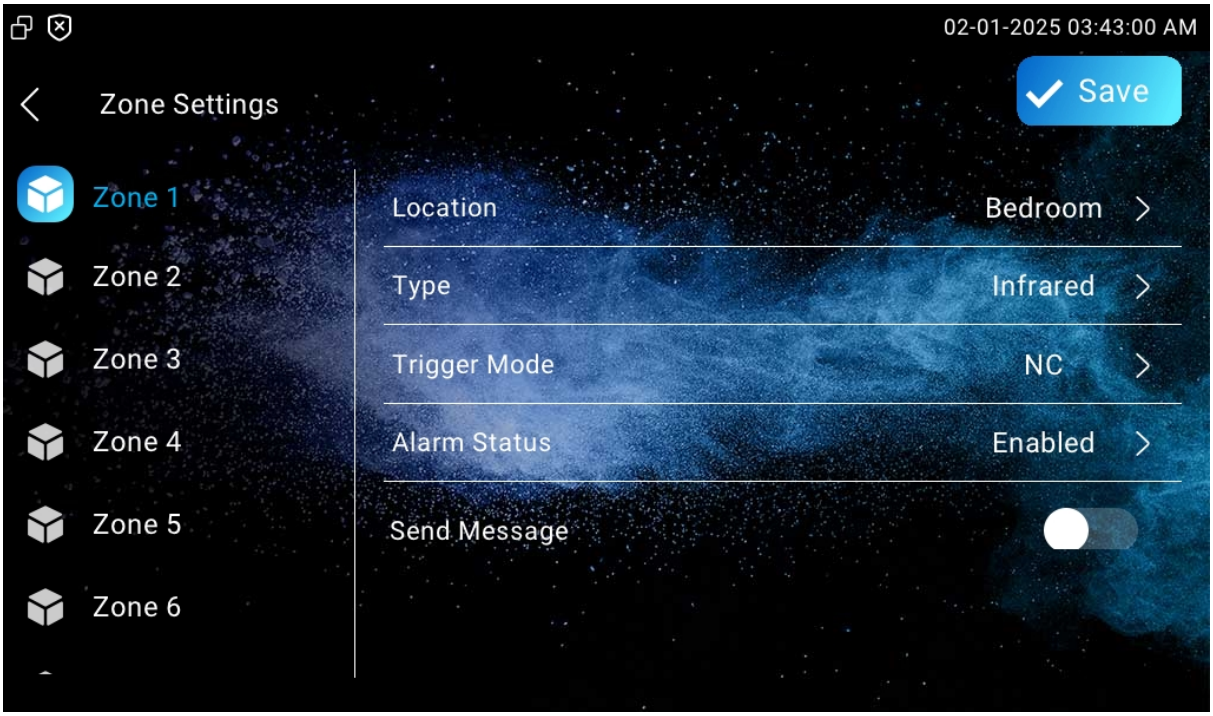


- **Location**: Indicate where the alarm sensor is installed. There are ten location types: Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study, and Bathroom.
- **Zone Type**: The alarm sensor types. There are six sensor types: Infrared, Drmagnet, Smoke, Gas, Urgency, and Motion.
-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

- **Status**: Set the alarm sensor status among three options: Enabled, Disabled, and 24H.
  - **Enabled**: The alarm needs to be set again after disarming.
  - **Disabled**: Disarm the alarm.
  - **24H**: The alarm sensor will stay enabled for 24 hours without setting up the alarm manually again after the alarm is disarmed. If any of the zones is enabled or set to **24H**, the alarm-related icons will be displayed on the home screen for quick access.

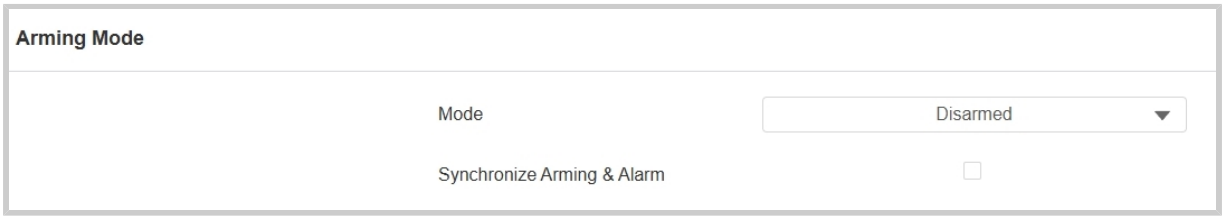


You can also set up alarm sensors on the **Settings > Advance Settings > Arming** screen.



Select an Arming Mode

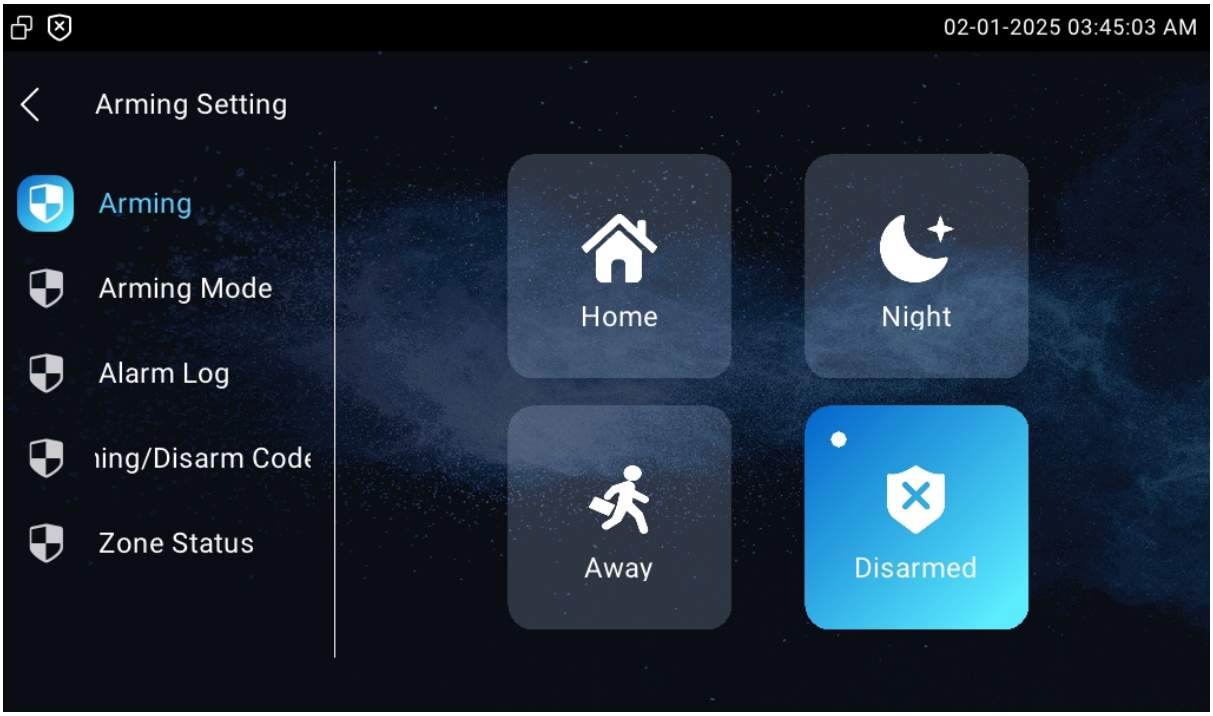
To select an arming mode, go to the **Arming > Arming Mode** interface.



- **Synchronize Arming & Alarm**: It is disabled by default. When enabled, the device synchronizes arming and alarms with other indoor monitors in the same room (if deployed on SmartPlus Cloud) or within the same node (if deployed on SDMC or on-premise).

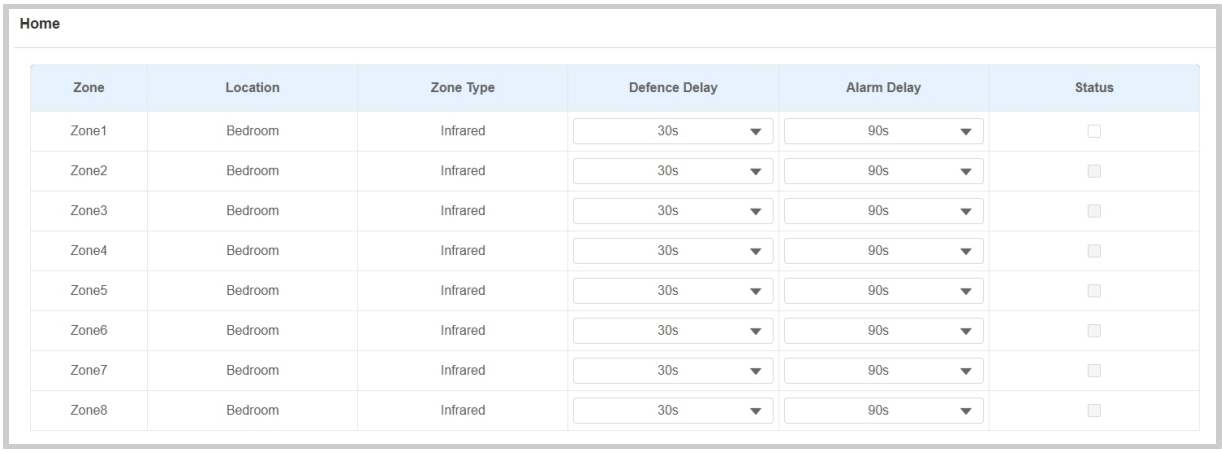
After displaying the Arming tab on the device screen, users can switch arming mode on the Arming screen.

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



Set up Alarm Sensors in Different Arming Modes

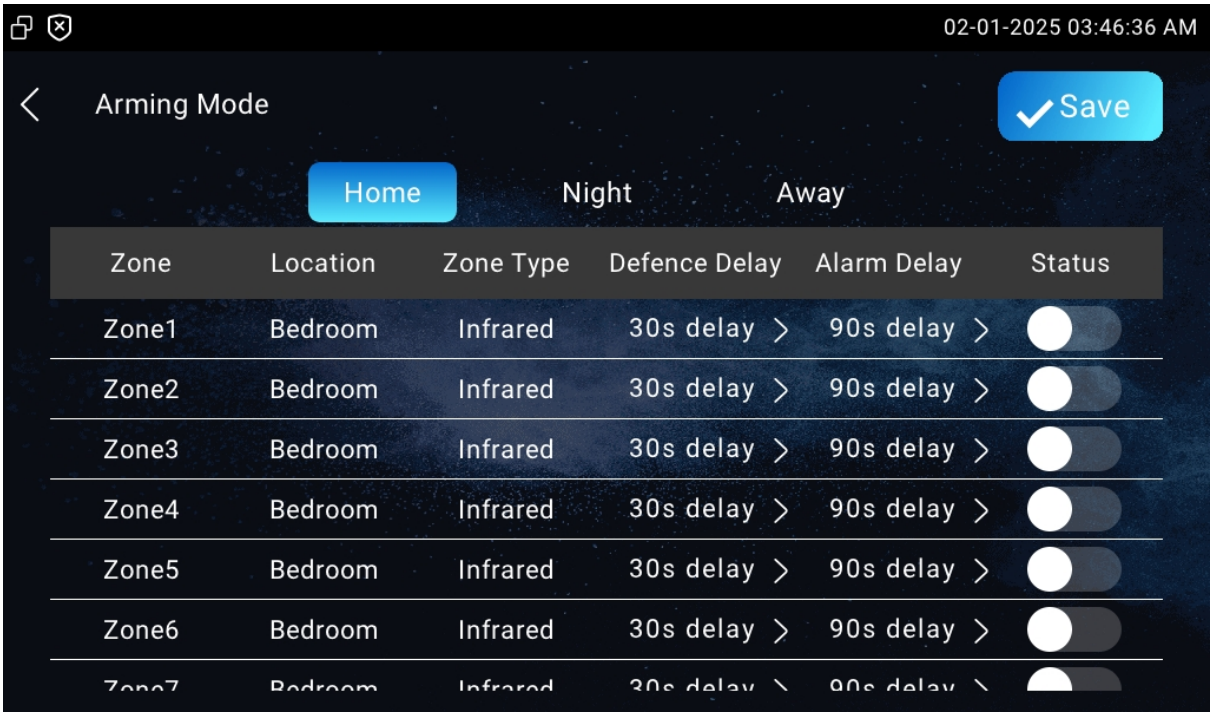
To configure the alarm in different modes, go to the **Arming > Arming Mode** interface.



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

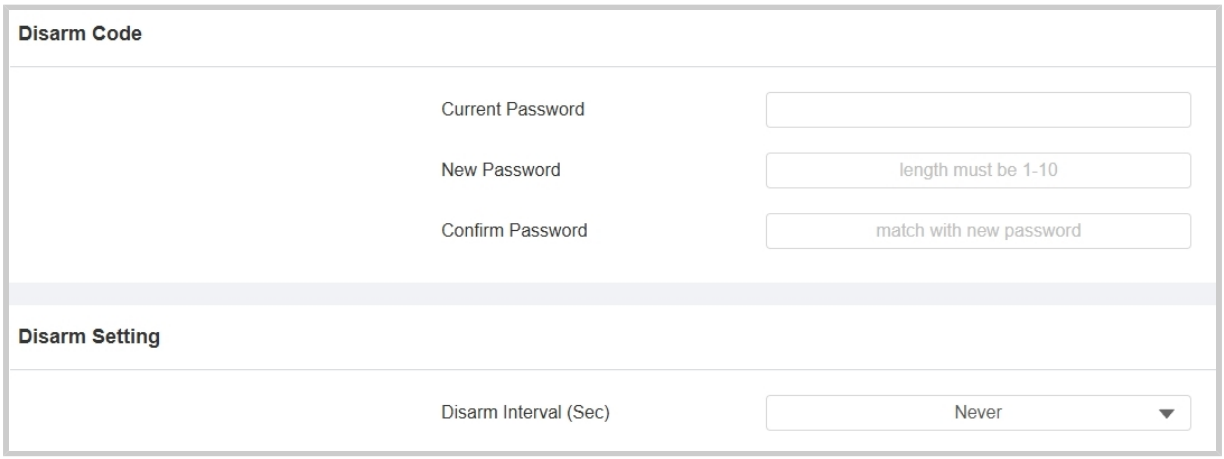
- **Defence Delay**: It means when users change the arming mode from other modes, there will be 30 seconds delay time to get activated.
- **Alarm Delay**: It means when the sensor is triggered, there will be 90 seconds delay time to announce the notification.
- **Status**: Enable or disable Arming Mode on the corresponding zone.

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



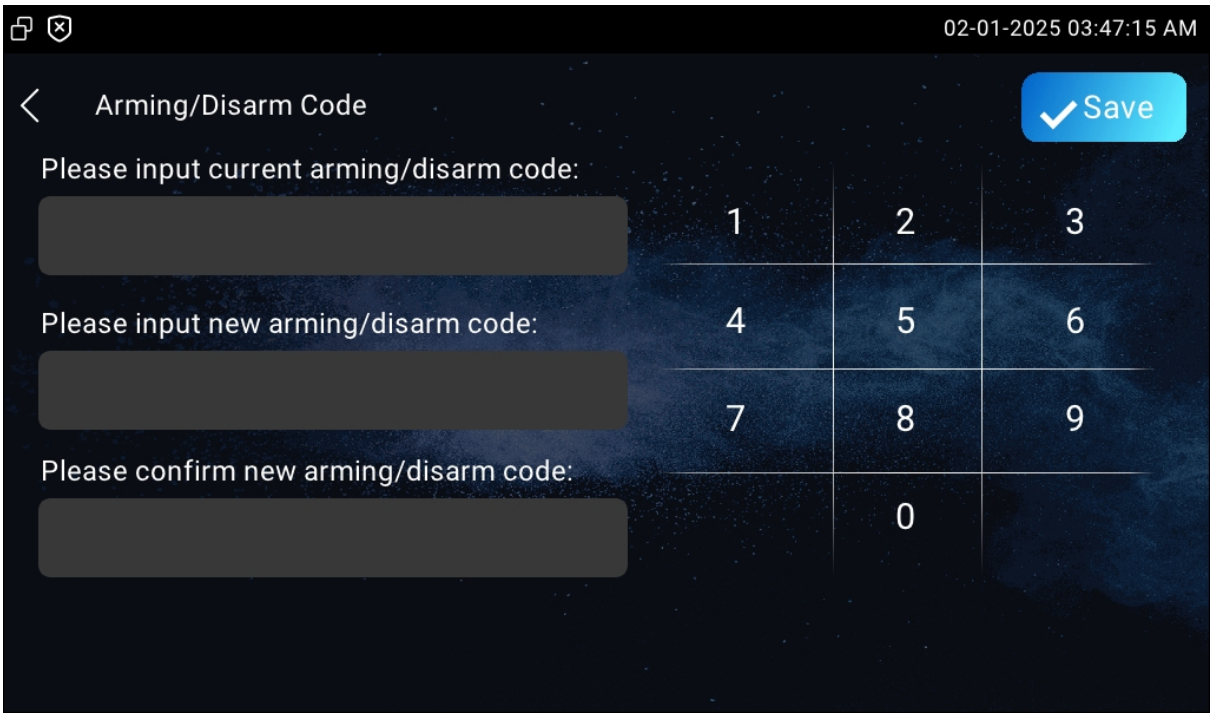
Set up the Disarm Codes

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



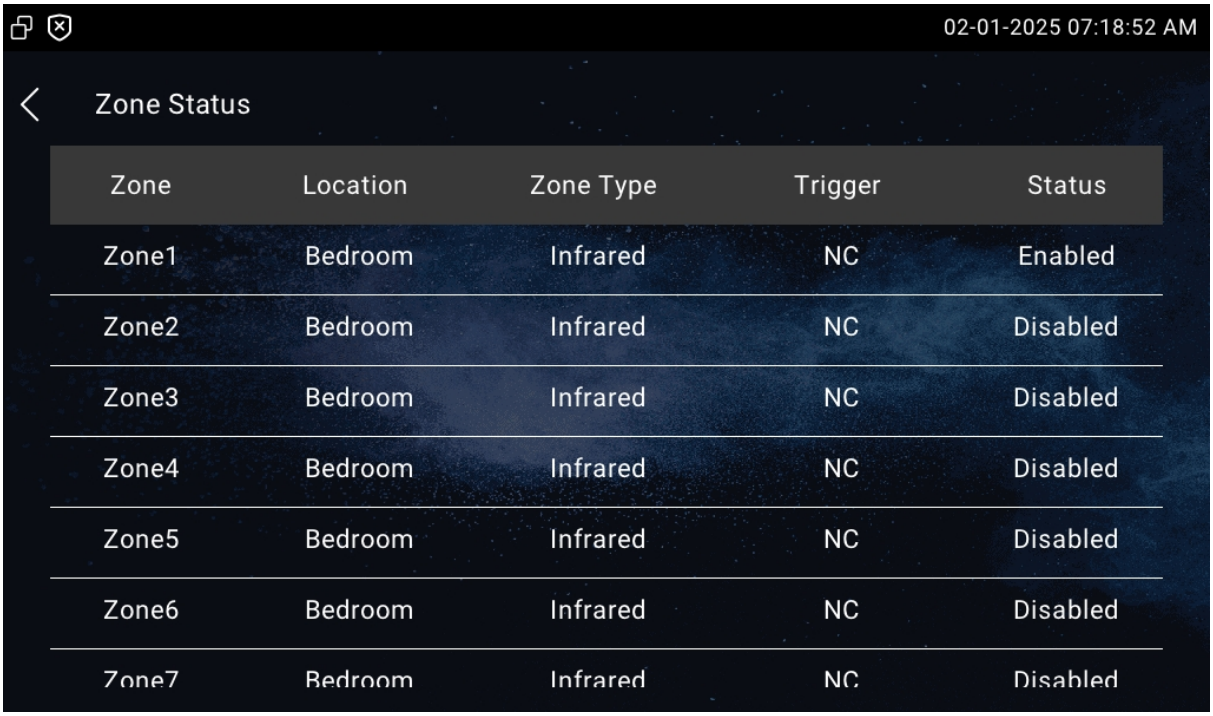
- **Disarm Interval(Sec)**: Set the alarm sound duration after the alarm is triggered.

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



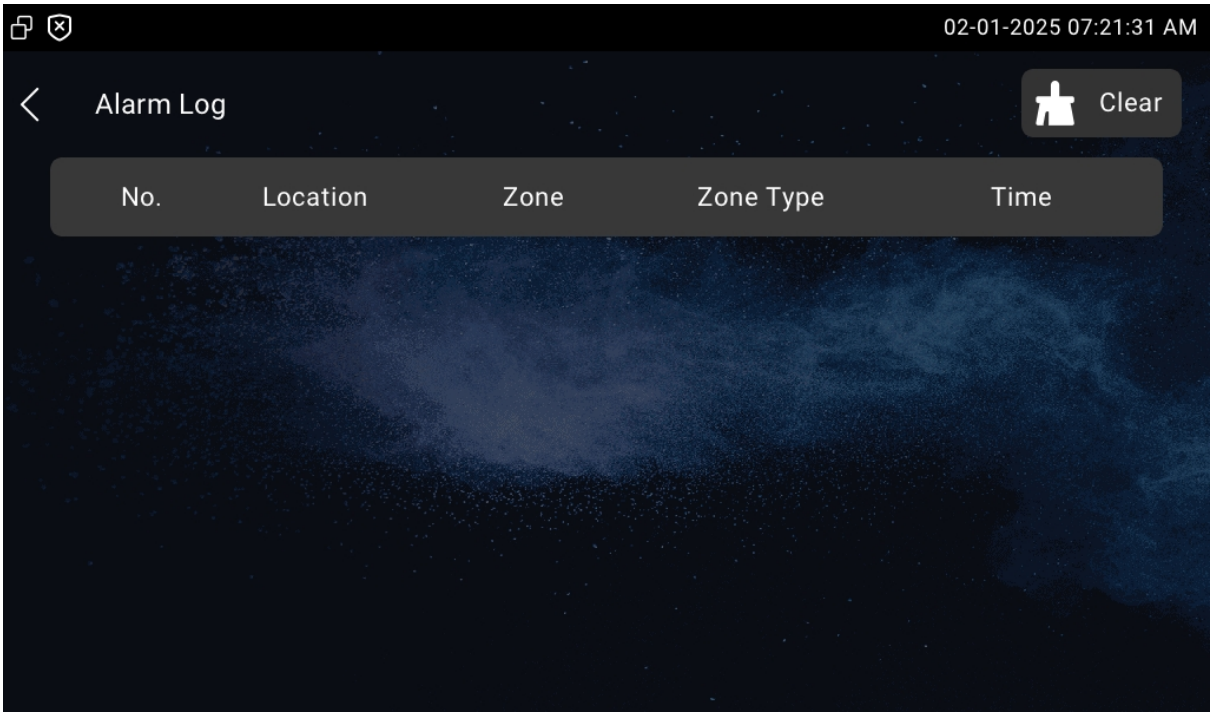
Check Zone Status

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



Check Alarm Logs

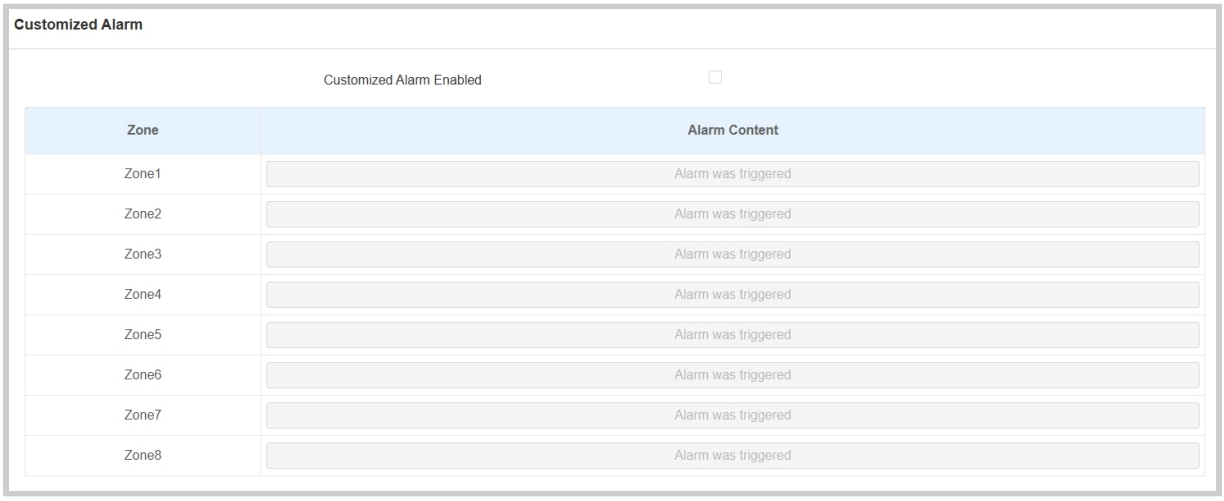
Check the alarm log on the **Arming > Alarm Log** screen.



Configure Alarm Text

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

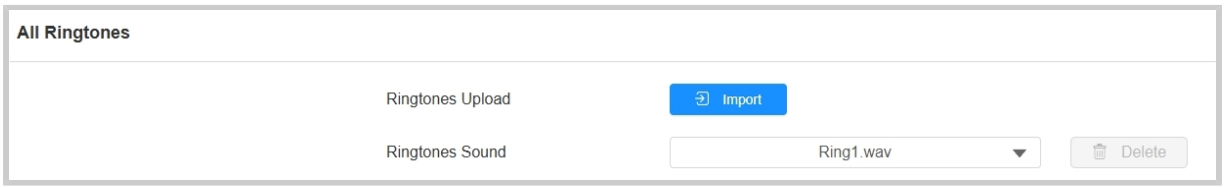
To set it up, navigate to the web **Arming > Zone Setting > Customized Alarm** interface.



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

Configure Alarm Ringtone

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



> **Note**
>
> The audio file should be WAV format with a maximum size of 250KB.

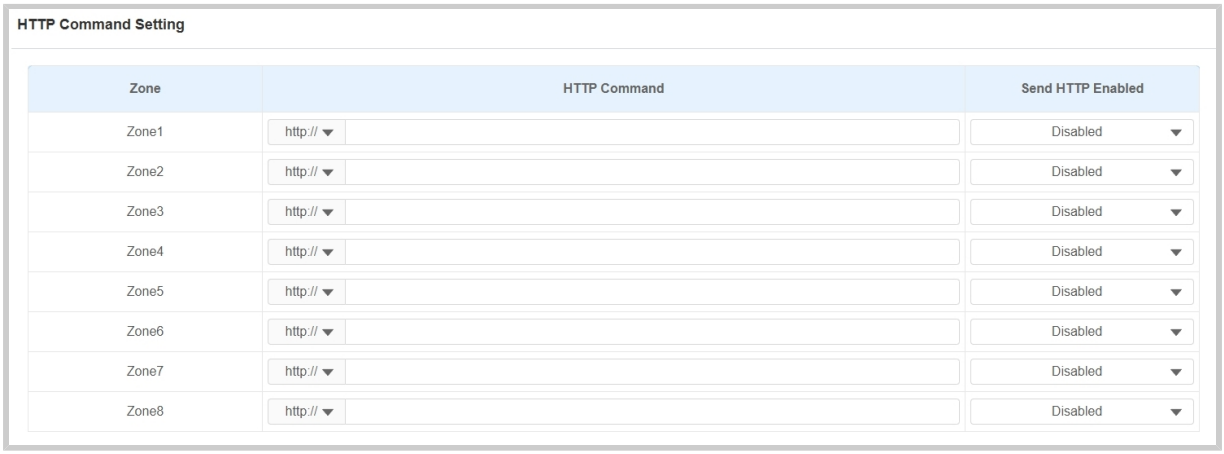
Alarm Action Configuration

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

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

HTTP Command

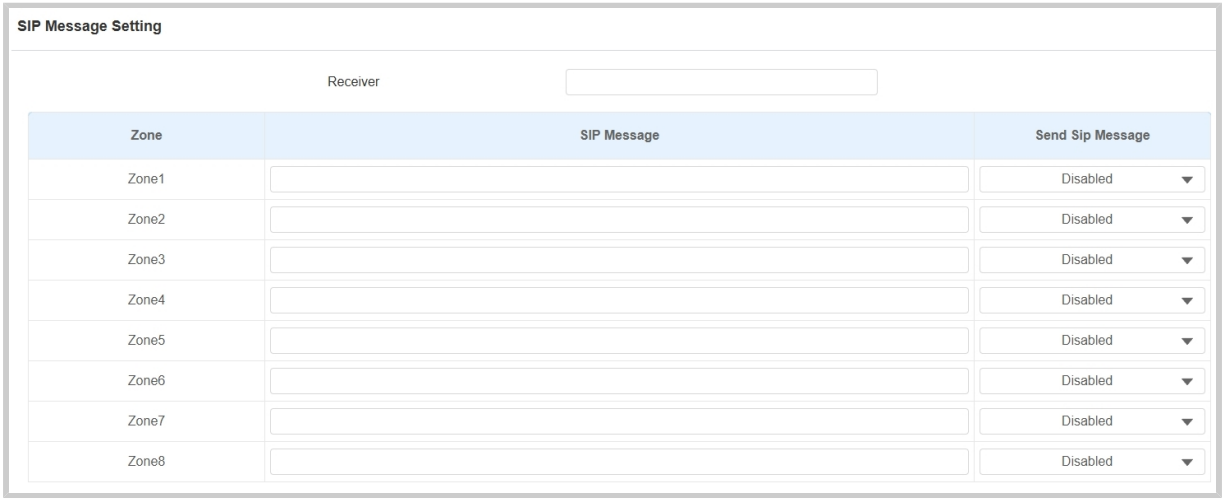
To set up the HTTP command action, you can select **Enabled** in the **Send HTTP** field to enable the actions for the alarm sensor installed in different locations. Then enter the HTTP command provided by the device manufacturer on which the action is to be carried.



- **Send HTTP Enabled**: 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.

SIP Message

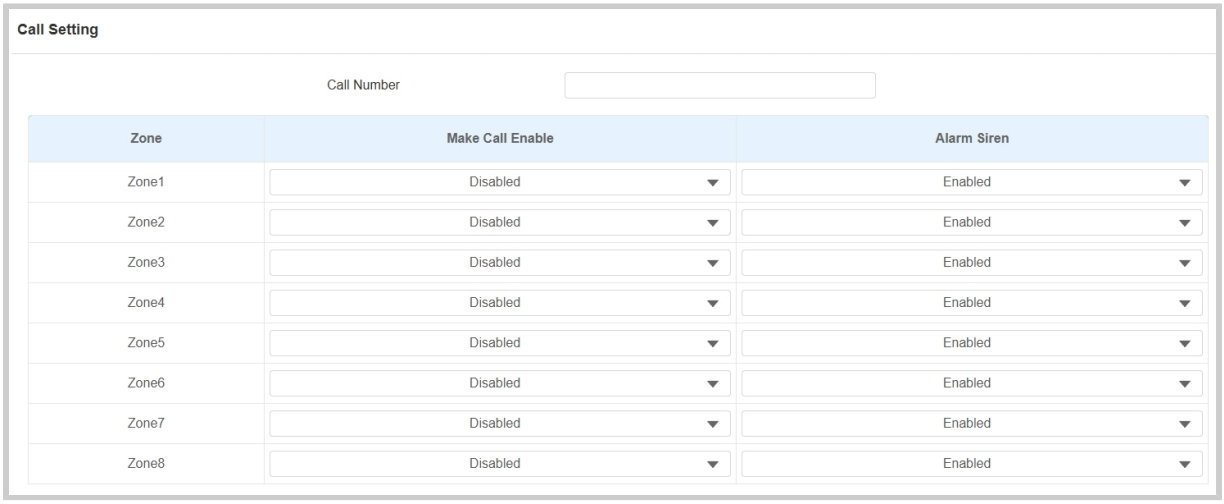
The device can send messages to a designated device when the alarm is triggered. To set this up, enter a SIP number or IP address along with the message content.



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

SIP Call

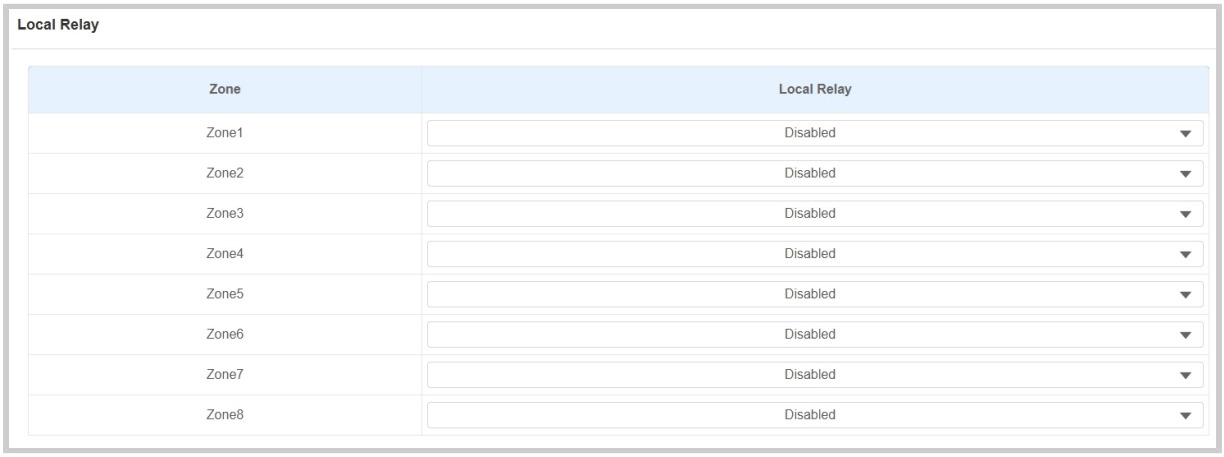
To enable the device to make a call when the alarm is triggered, enter the SIP or IP number of the called party. Additionally, you can allow the indoor monitor to sound a siren simultaneously.



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

Local Relay

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

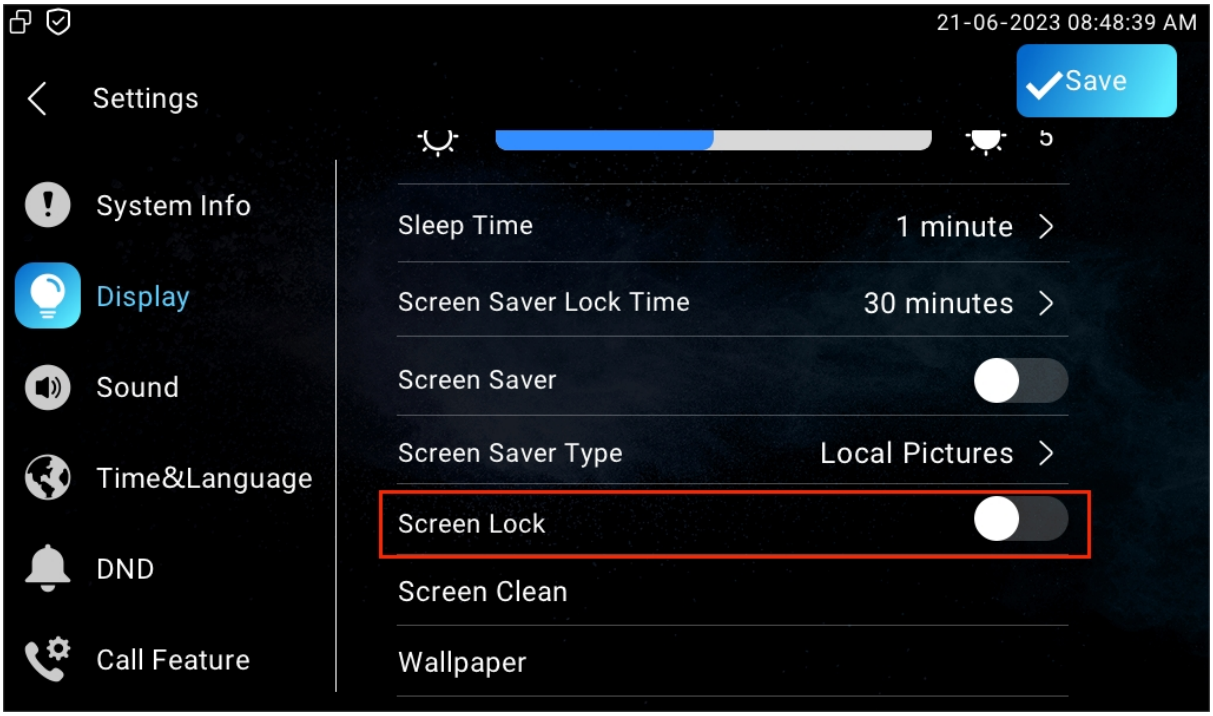


- **Local Relay**: Enable it if you want the local relay to be triggered with the sensor.

Screen Unlock Setting

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

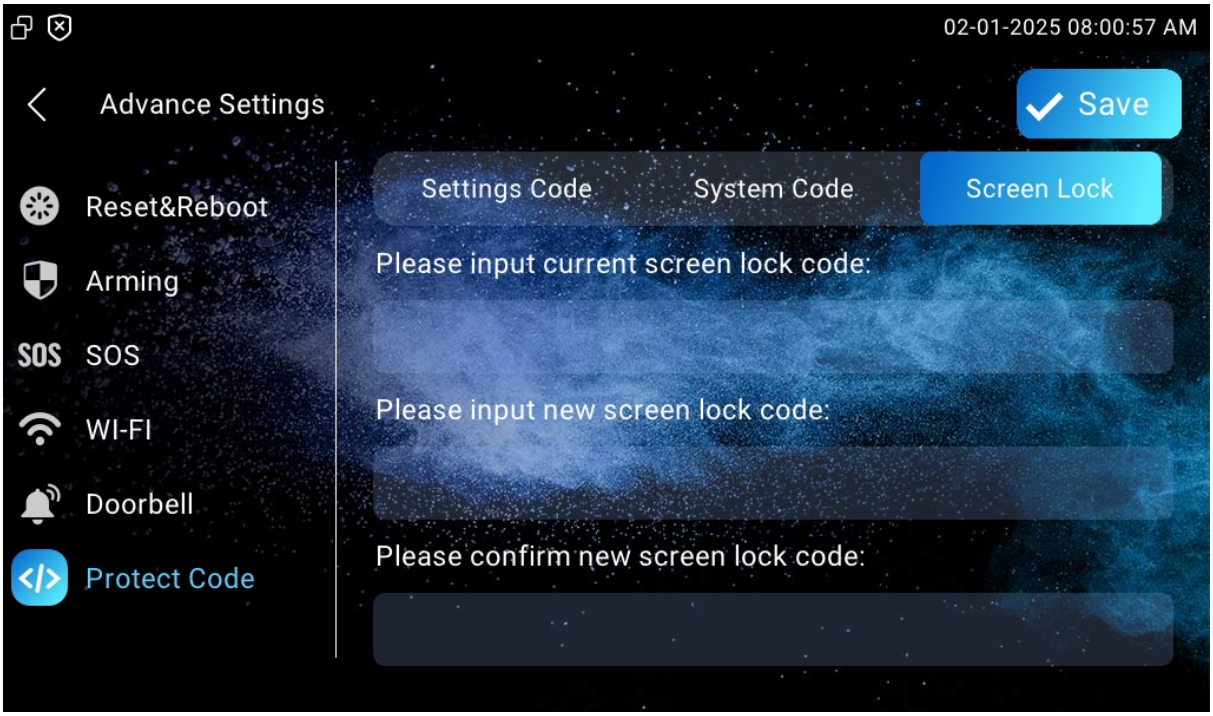
You can enable the screen lock function directly on the device **Settings > Display** screen.



Screen Unlock by PIN Code

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

Navigate to the **Settings > Advance Settings > Protected Code** screen and select **Screen Lock** to change a new password.



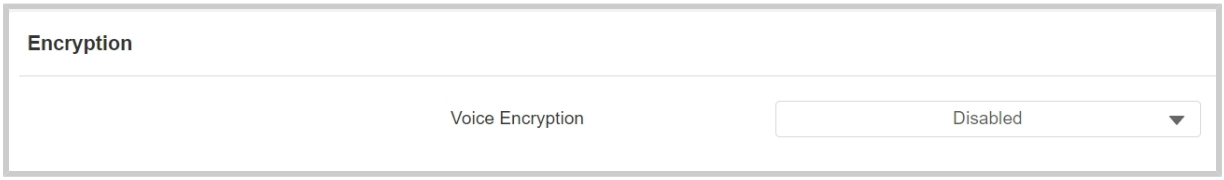
Note

The initial password is empty. Tap ✓ to unlock the screen.

Voice Encryption

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

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



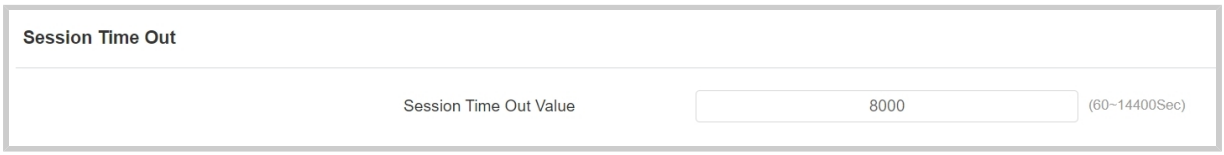
- **Voice Encryption**:
  - **Disabled**: The call will not be encrypted.
  - **SRTP(Compulsory)**: All audio signals(technically speaking it is RTP streams) will be encrypted to improve security.

- **SRTP(Optional)**: Encrypt the voice from the caller. If the caller also enables SRTP, the voice signals will also be encrypted.
- **ZRTP(Optional)**: The protocol that the two parties use to negotiate the SRTP session key.

Web Interface Automatic Log-out

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

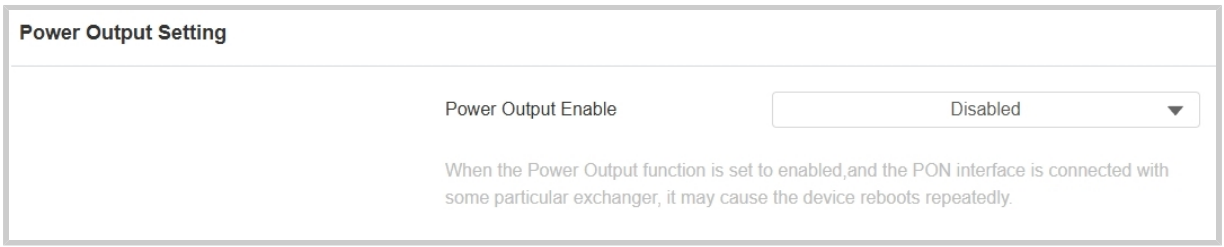
To set it up, go to the web **Security > Basic > Session Time Out** interface.



Power Output Setting

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

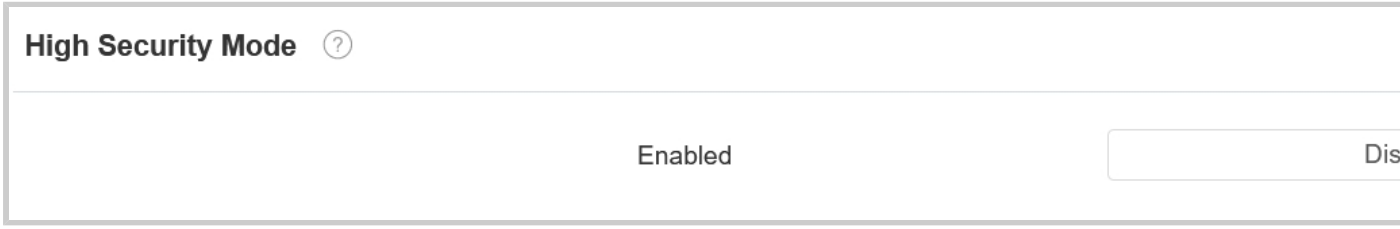
To enable it, go to **Settings > Basic > Power Output Setting** interface.



High Security Mode

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

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



Important Notes

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

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

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

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

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

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

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

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

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

Lift Control

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

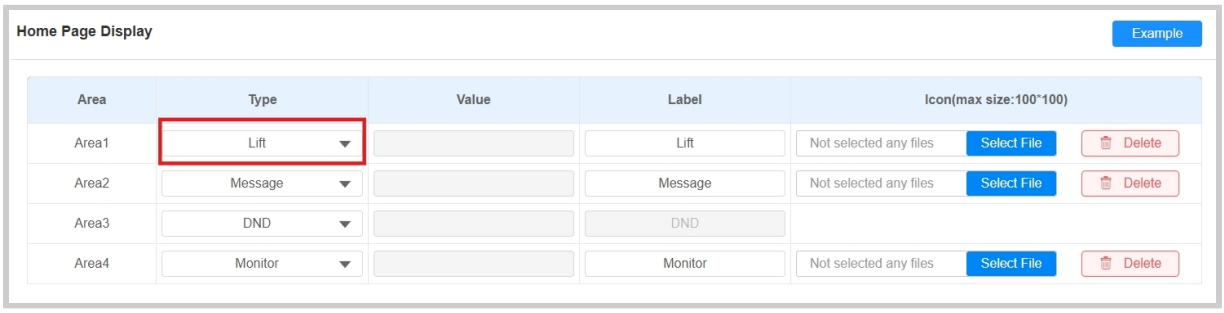
To achieve this function, you need to set up the lift control feature on both the indoor monitor and the lift controller EC33.

Click here to view the configuration steps.

Set Lift Control Icon

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

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



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

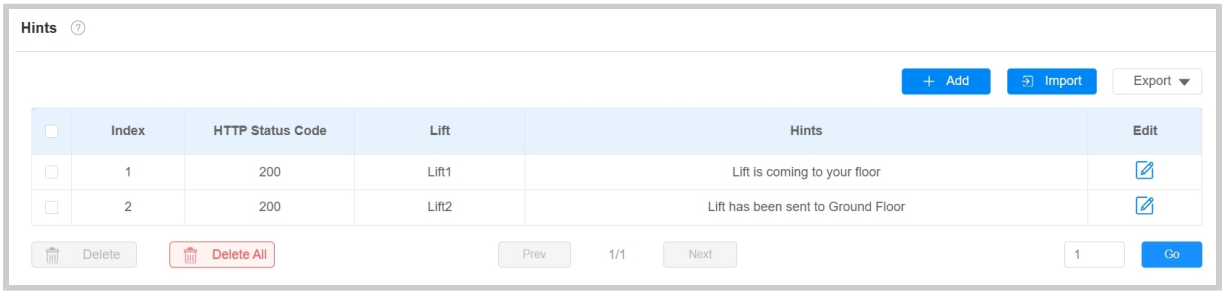


- **Status**: Enable or disable the lift button.
- **Icon**: Decide the button icon.
- **Label**: Name the button.
- **HTTP Command**: Select http:// or https:// for the head of the HTTP command and enter the HTTP command.

Set Lift Control Prompt

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

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



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

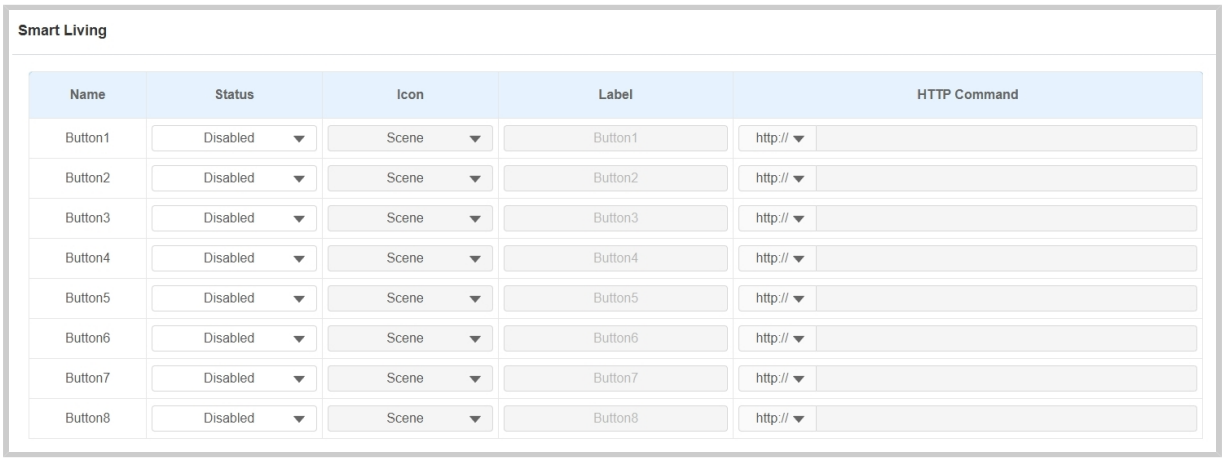


Integration with Third-party Devices

Smart Living Setting

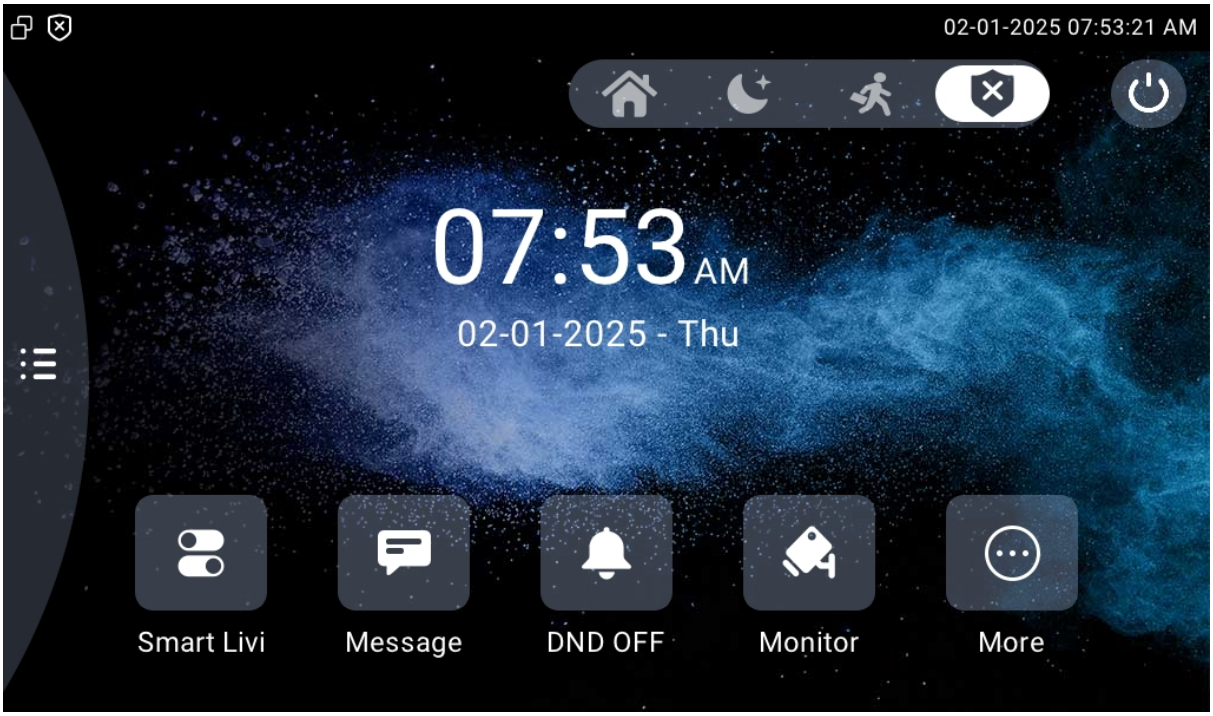
You can control the home sensor through an HTTP command.

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



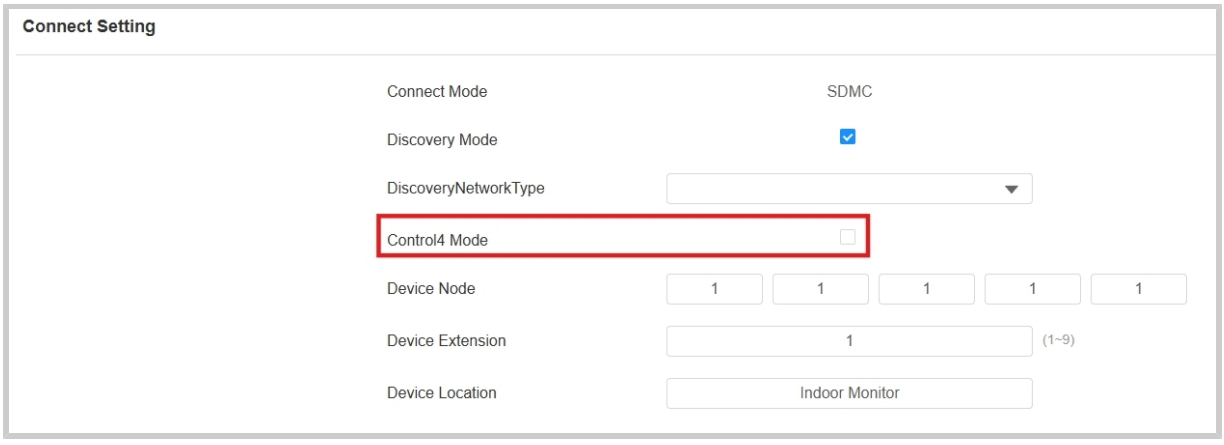
- **Status**: Enable or disable this button. If disabled, the button won't appear on the home control page.
- **Icon**: Select the preferred icon image.
- **Label**: Customize the button display name.
- **HTTP command**: The HTTP command to trigger the sensor.

> **Note**
>
> Set the Smart Living button to be displayed on the **Device > Display Setting** interface before using this feature.



Integration with Control4

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.



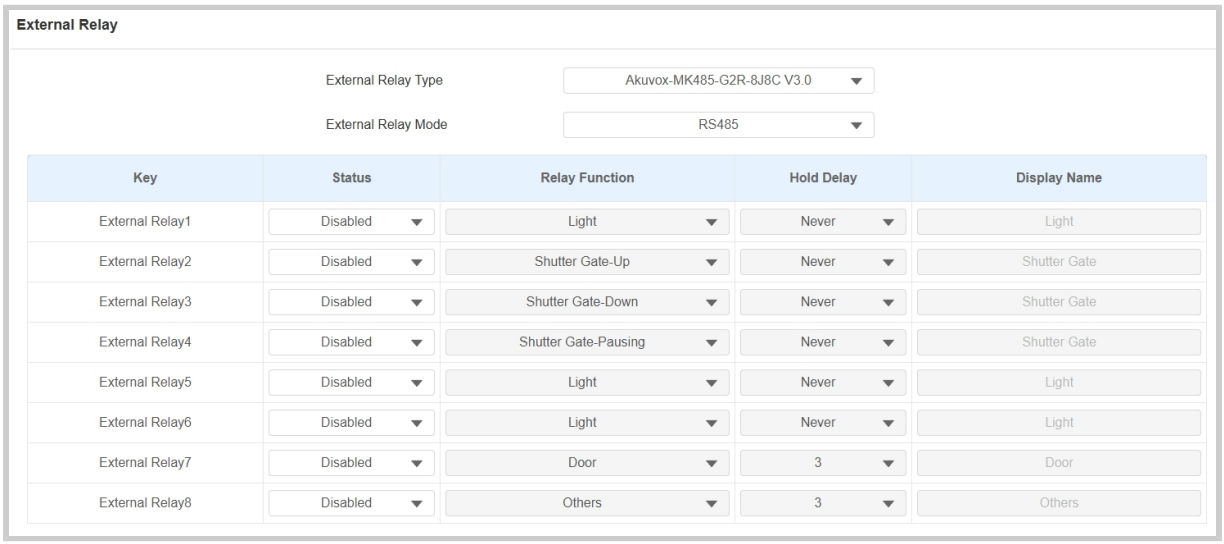
Note

Click here to view the detailed integration steps with Control4.

Integration via External Relay

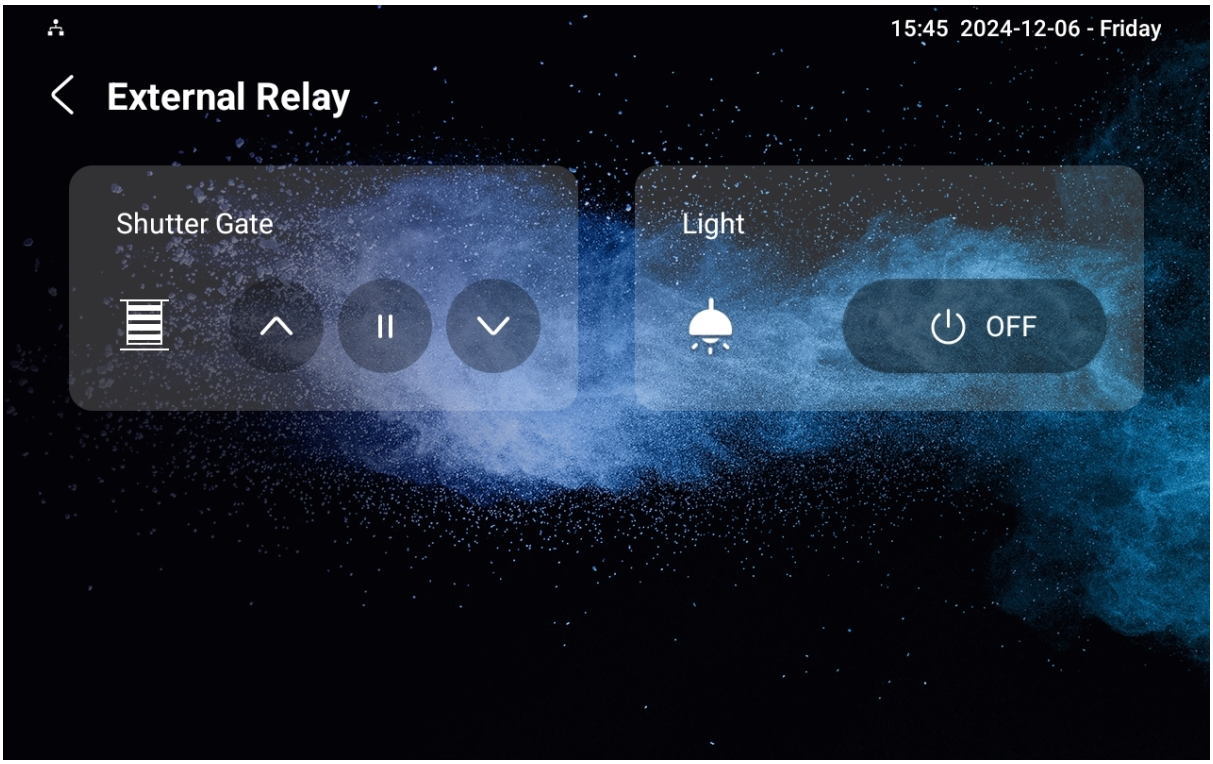
Users can control akubela or third-party smart home devices on the indoor monitor through an external relay controller.

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



- **External Relay Type**: Select the external relay type.
  - **None:** No external relay device is connected.
  - **Akuvox MK485:** Select when the indoor monitor is connected to the Akuvox MK485.
  - **RSAC-C1-R8:** Select when the indoor monitor is connected to the akubela RSAC-C1-R8 relay controller via RS485.
  - **LED11:** Select when the indoor monitor is connected to LED11.
- **External Relay Mode**: Select the external relay mode.
- **Status**: Enable/disable the relay.
- **Relay Function**: Set the relay function based on the smart home devices connected.
- **Hold Delay**: Specify the relay reset time from 1 to 60 seconds. **Never** means it keeps activated once it is triggered. By default, it is 3 seconds for Door and Others relay functions and Never for other functions.

- **Display Name**: Set the tab's name displayed on the indoor monitor's External Relay screen.



Note

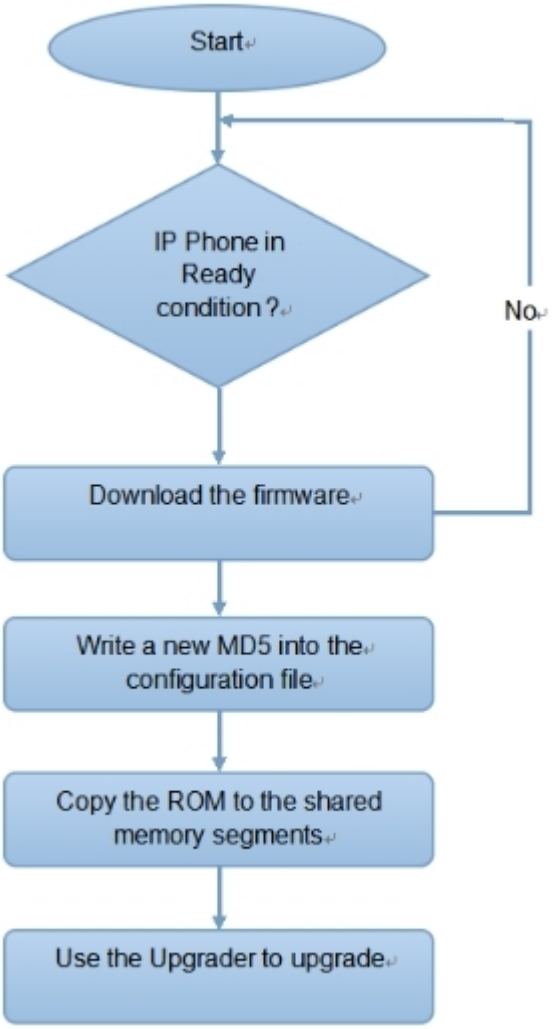
- To display the External Relay button on the home screen, set it up on the **Device > Display Setting** interface.
- Click here to view the detailed configuration of the external relay feature.

Auto-provisioning

Provisioning Principle

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

Please see the flow chart below:



Configuration Files for Auto-Provisioning

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

Differences:

- **General Configuration Provisioning**:

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

- **MAC-Based Configuration Provisioning**:

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

Note

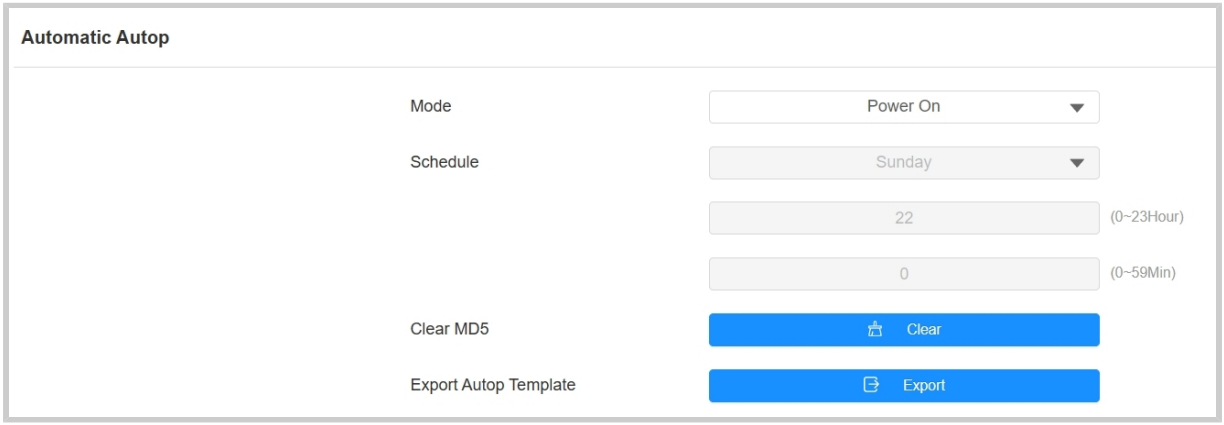
- Configuration files must be in CFG format.
- The name of the general configuration file for batch provisioning varies by model.
- The MAC-based configuration file is named after its MAC address.
- Devices will first access general configuration files before the MAC-based ones if both types are available.

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

Autop Schedule

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

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

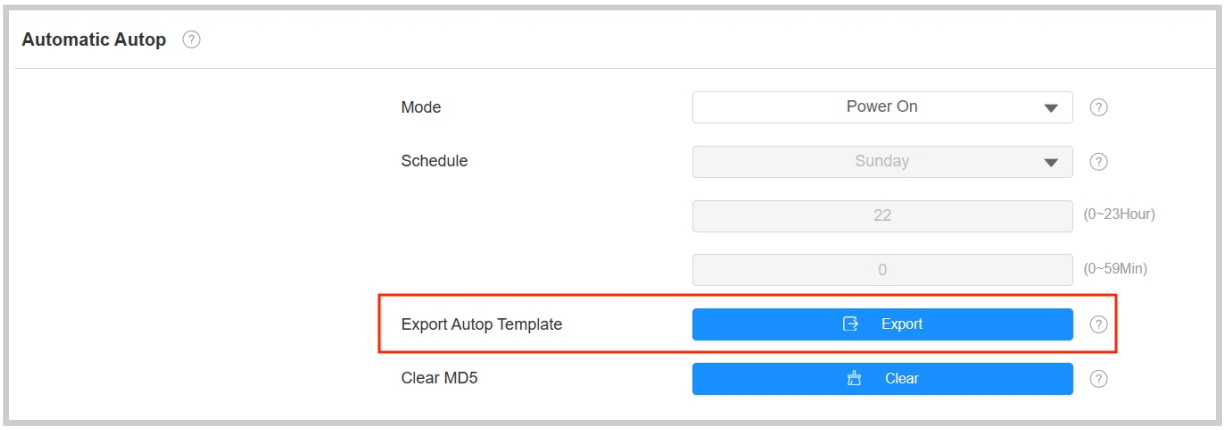


- **Mode**:
  - **Power On**: The device will perform Autop every time it boots up.
  - **Repeatedly**: The device will perform Autop according to the schedule you set up.
  - **Power On + Repeatedly**: Combine **Power On** mode and **Repeatedly** mode, which will enable the device to perform Autop every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

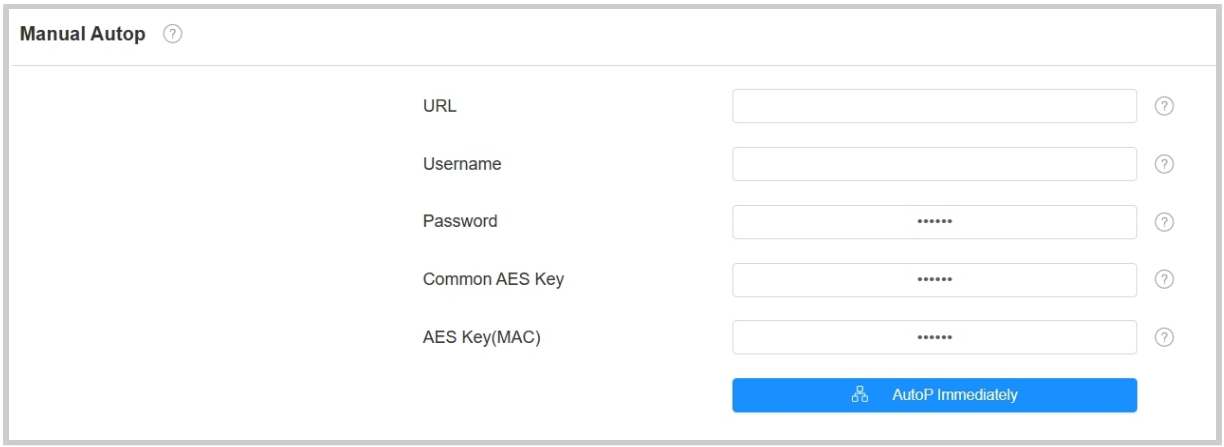
Static Provisioning

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

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



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



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

Note

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

Tip

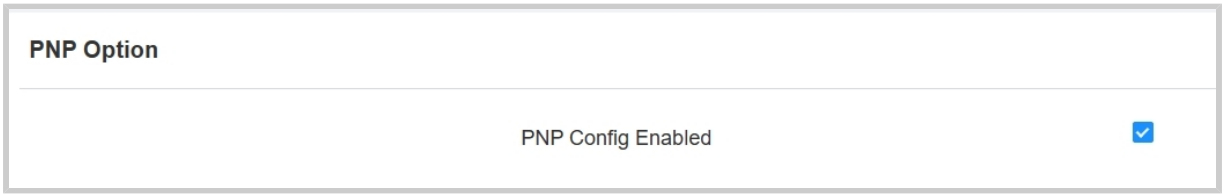
Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

Click here to watch the configuration video.

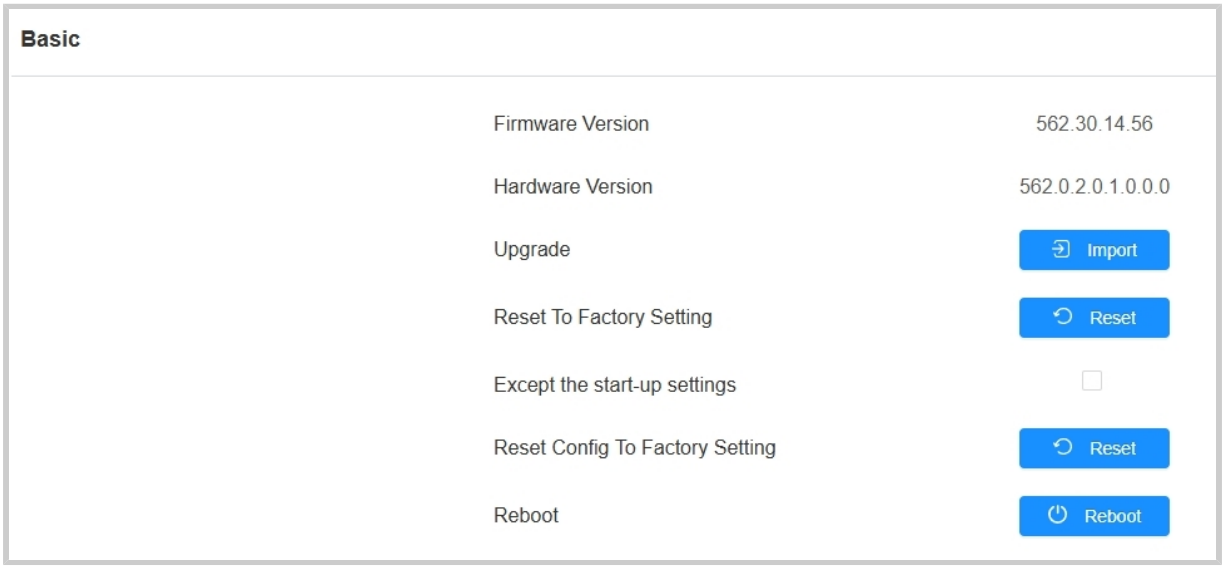
To enable the function, go to the **Upgrade > Advanced > PNP Option** interface.



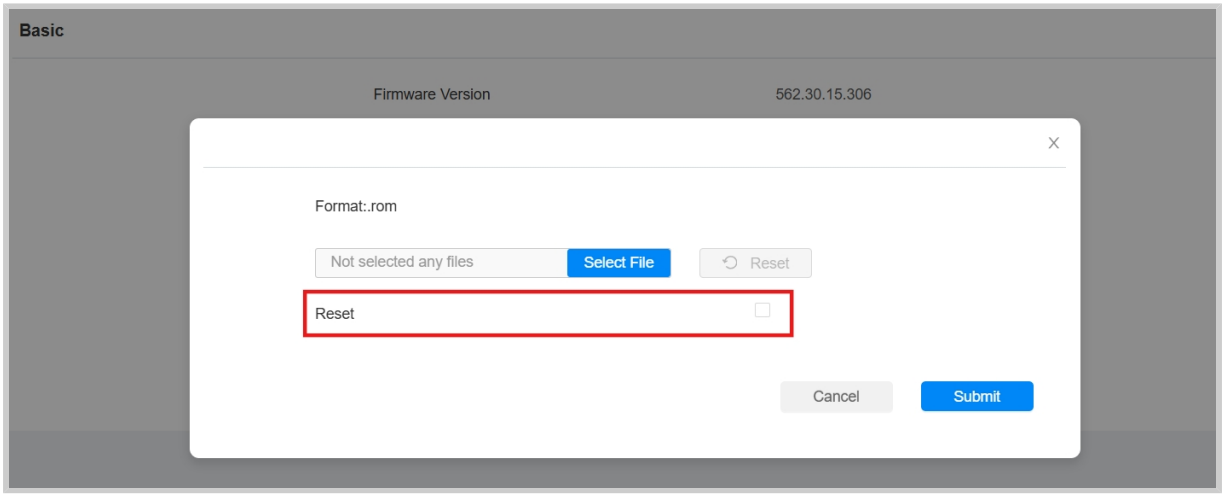
Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

To upgrade the device, navigate to the **Upgrade > Basic** interface. Click **Import** to upload the upgrade file.



If you want to reset the device while upgrading, check the **Reset** box. After the upgrade, the device will be reset to the factory settings.



Note

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

Backup

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

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

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

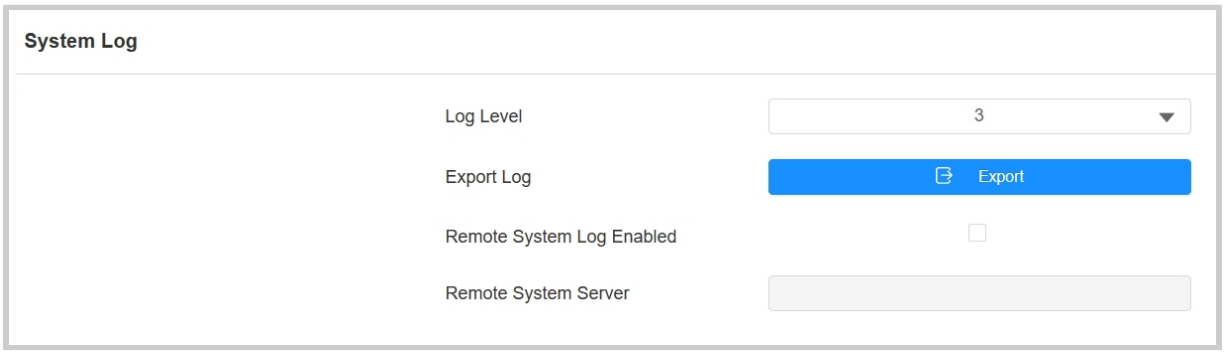


Debug

System Log for Debugging

System logs can be used for debugging purposes.

If you want to export the system log to a local PC or a remote server for debugging, you can set up the function on the web **Upgrade > Diagnosis > System Log** interface.

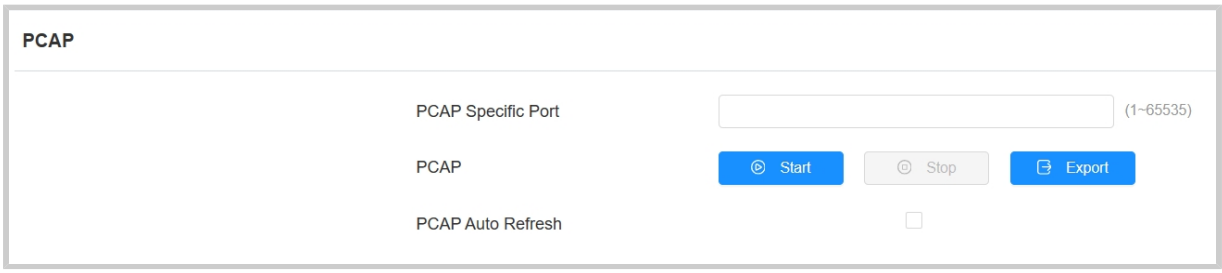


- **Log Level**: Log level ranges from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purposes. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: Click the **Export** tab to export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

PCAP for Debugging

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

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

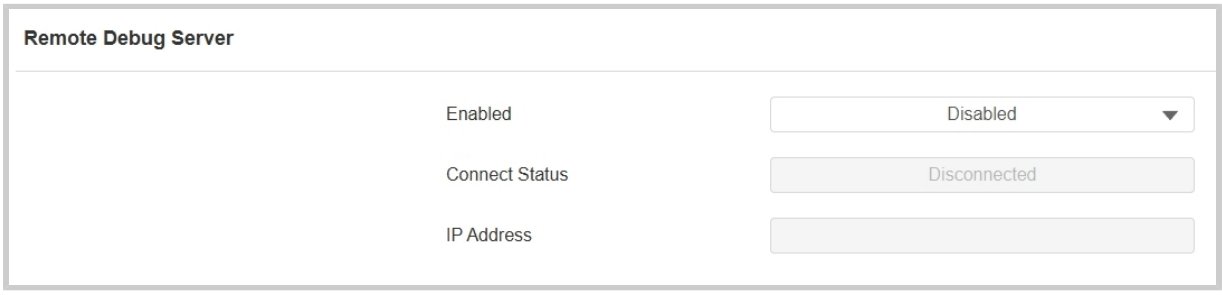


- **PCAP Specific Port**: Select the specific port from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: Click the **Start** tab and **Stop** tab to capture a certain range of data packets before clicking the **Export** tab to export the data packets to your local PC.
- **PCAP Auto Refresh**: When enabled, the PCAP will continue to capture data packets even after the data packets reach 50 MB in capacity. When disabled, the PCAP will stop data packet capturing when the data packets reach the maximum capturing capacity of 1MB.

Remote Debug Server

When the device is having a problem, you can use the remote debug server to access the device log remotely for debugging purposes.

Set it up on the **Upgrade > Diagnosis** interface.

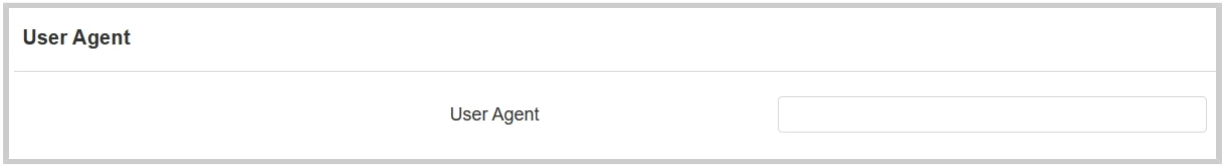


- **Connect Status**: Indicate the remote debug server's connection status.
- **IP**: Specify the server's IP address.

User Agent

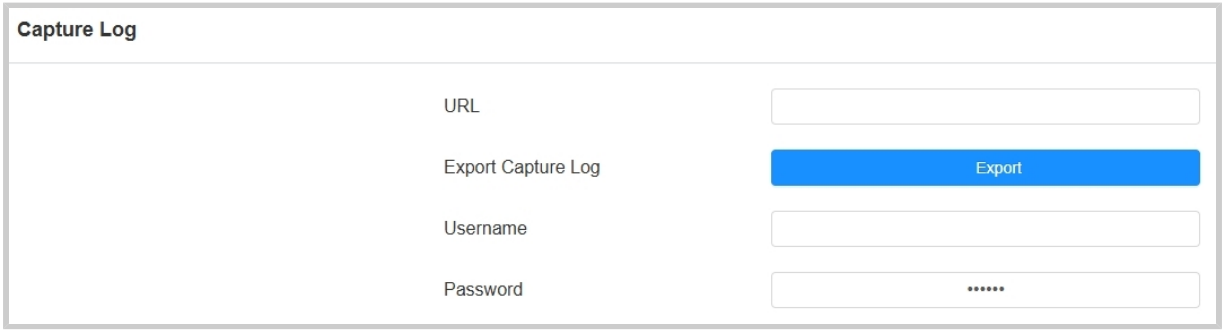
User agent is used for identification purpose when you are analyzing the SIP data packet.

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



Capture Log

You can set up a remote server to receive the device's capture log on the **Upgrade > Diagnosis > Capture Log** interface.

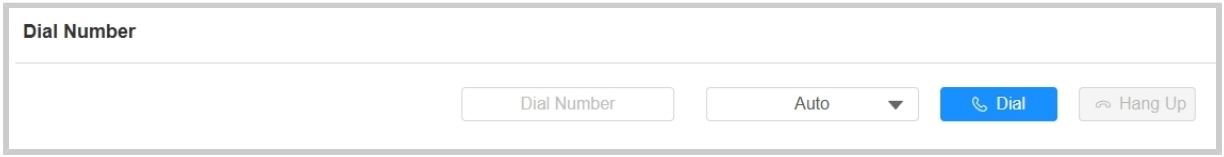


- **URL**: Set the server address to receive the capture log.
- **Export Capture Log**: Click Export to export the capture log to the local PC.
- **User Name**: Set the username to access the server.
- **Password**: Set the password to access the server.

Web Call

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

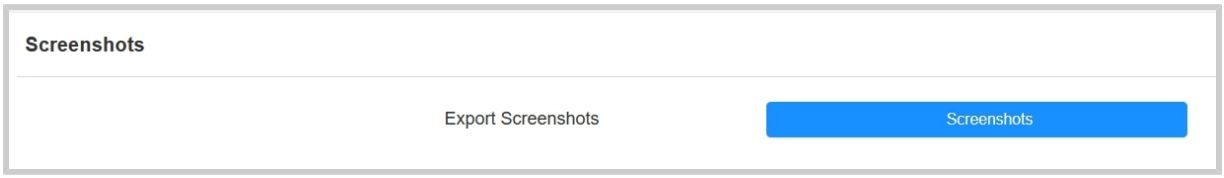
To set it up, navigate to the **Contacts > Local Contacts > Dial Number** interface. Enter the target number and select the account to dial out.



Screenshots

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

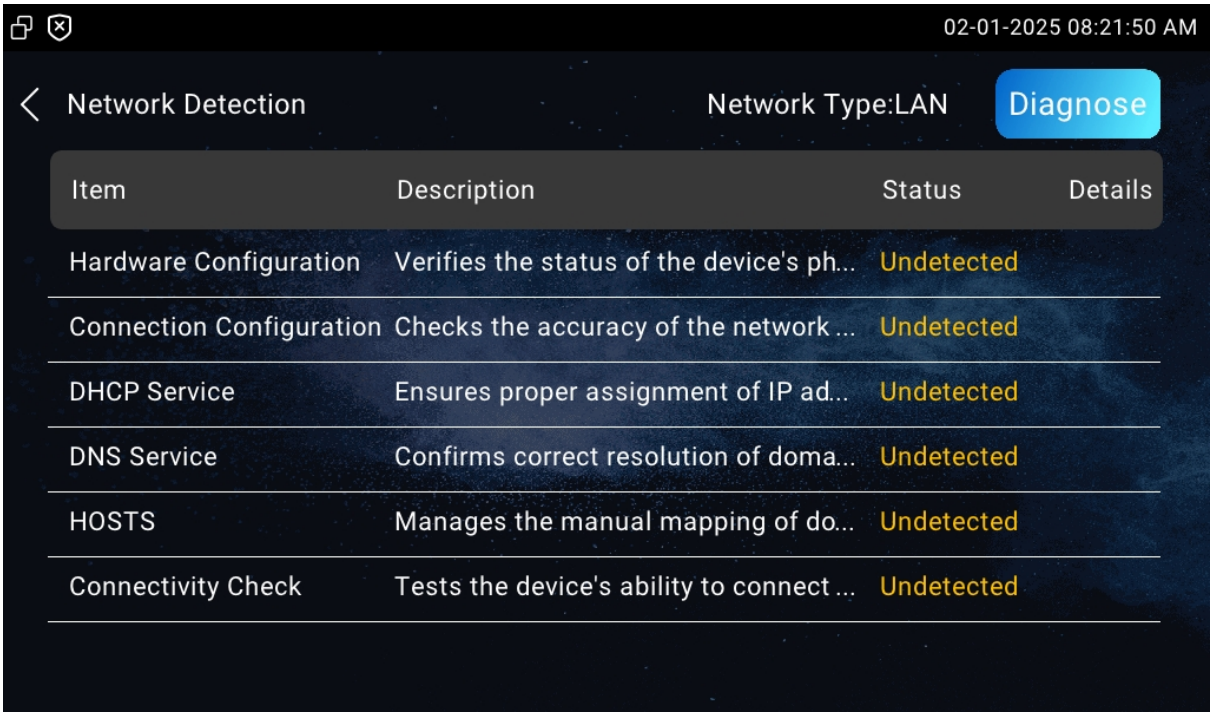
To take screenshots, go to **Upgrade > Diagnosis > Screenshots** interface, then click **Screenshots**.



Network Detection

You can use the network detection feature to quickly troubleshoot network problems.

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



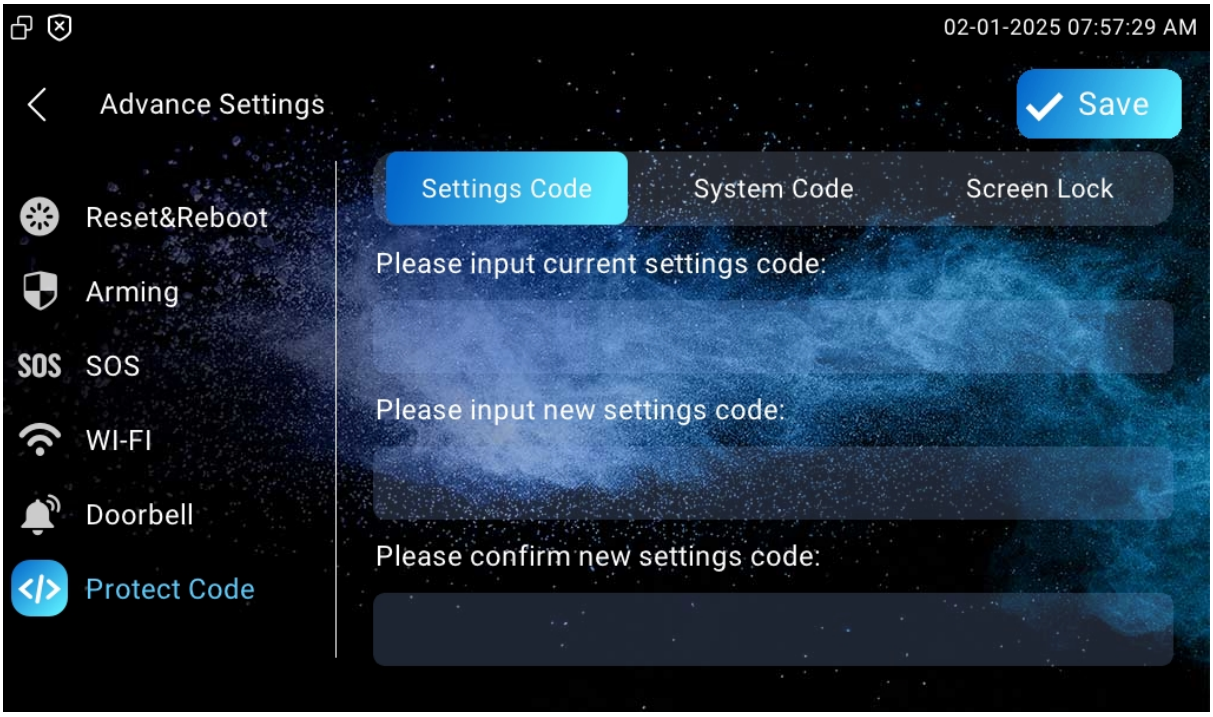
- **Diagnose**: Tap to start detection.
- **Status**: Display a loading icon when the detection starts; display ✓ for normal results and **X** for abnormal results.
- **Details**: Tap to view the detection details.

Password Modification

Modify Device Basic Setting Password

Settings Code is used to access the device's basic settings. The default is 123456.

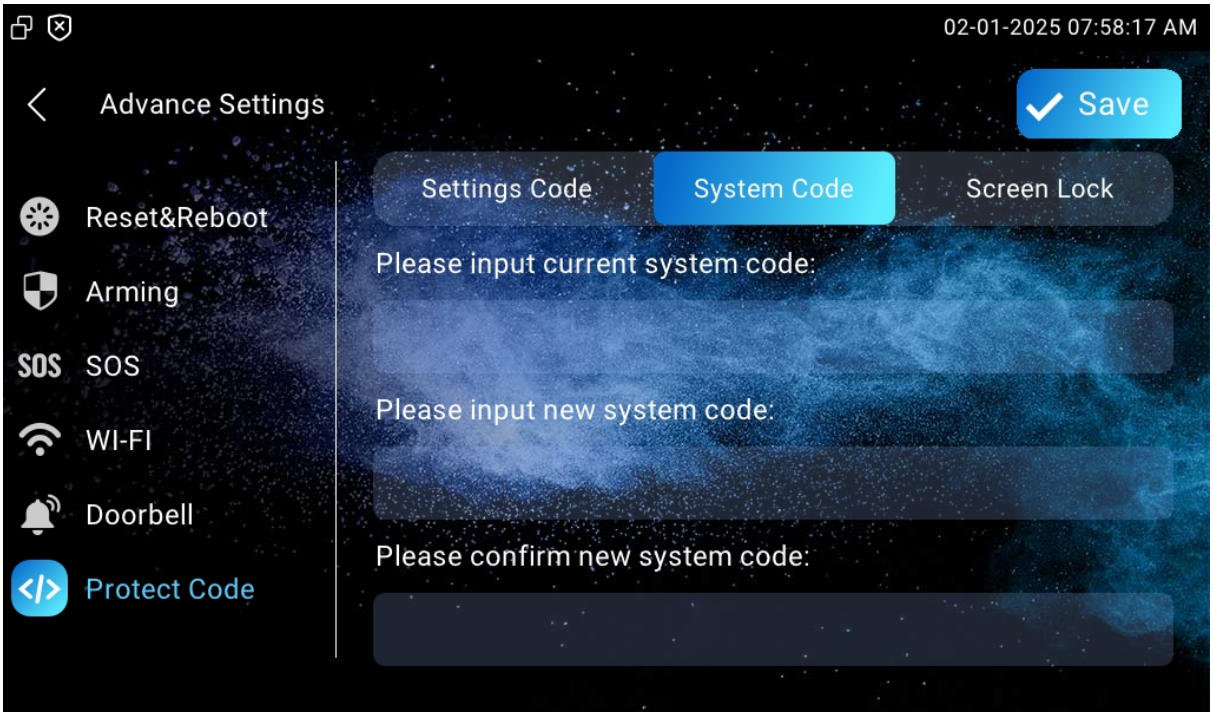
To modify it, go to the **Settings > Advance Settings > Protect Code** screen and select **Settings Code**.



Modify Device Advance Setting Password

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

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

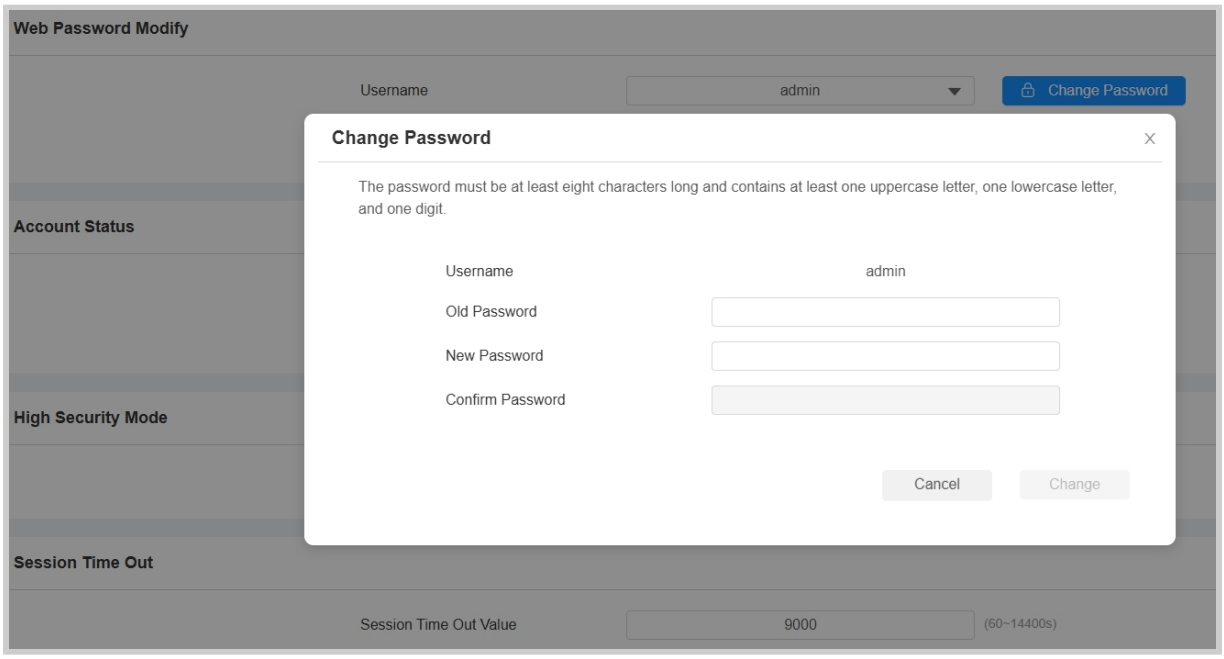


Modify Device Web Interface Password

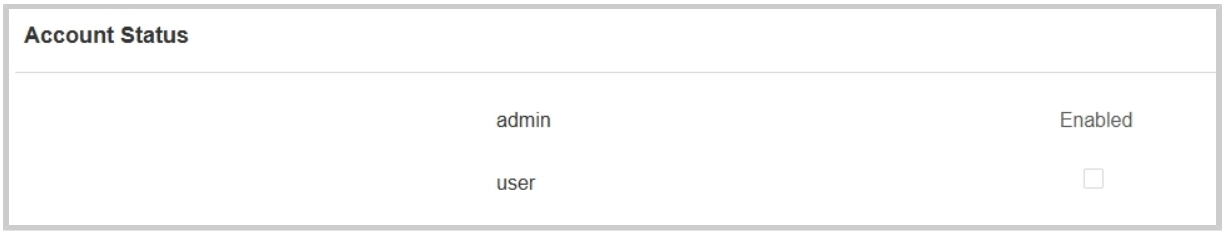
Select **Admin** for the administrator account and **User** for the user account. Click the **Change Password** tab to change the password.

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





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



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

Modify Security Questions

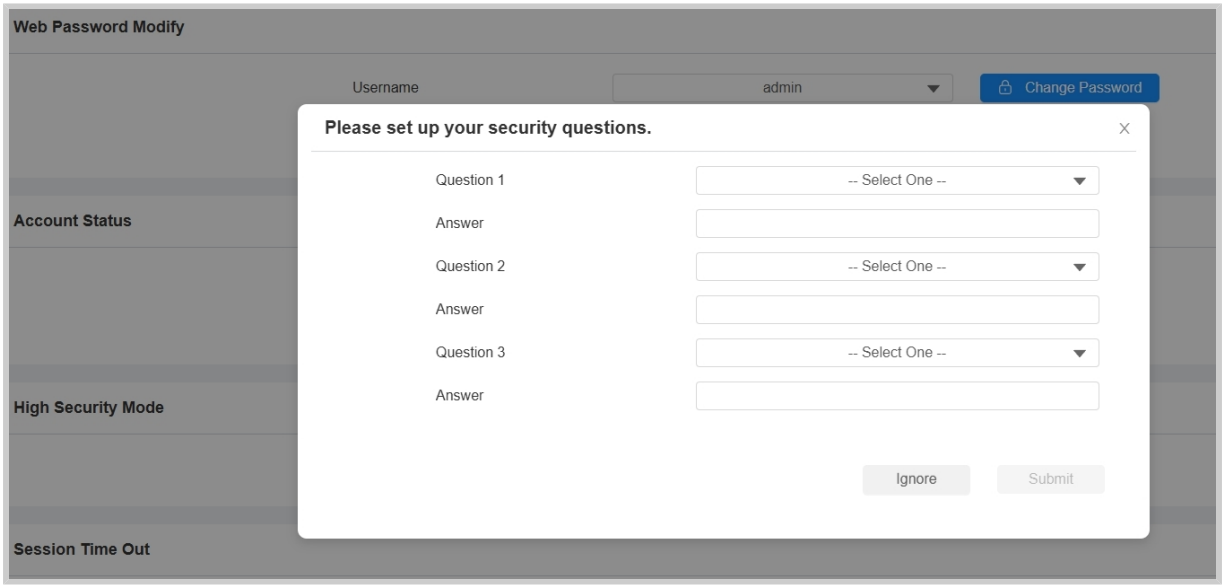
Security questions allow you to reset the web password if you forget it. After setting up the security questions, you can click "Forget Password" on the login interface, enter the answers, and a password reset window will pop up.

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

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



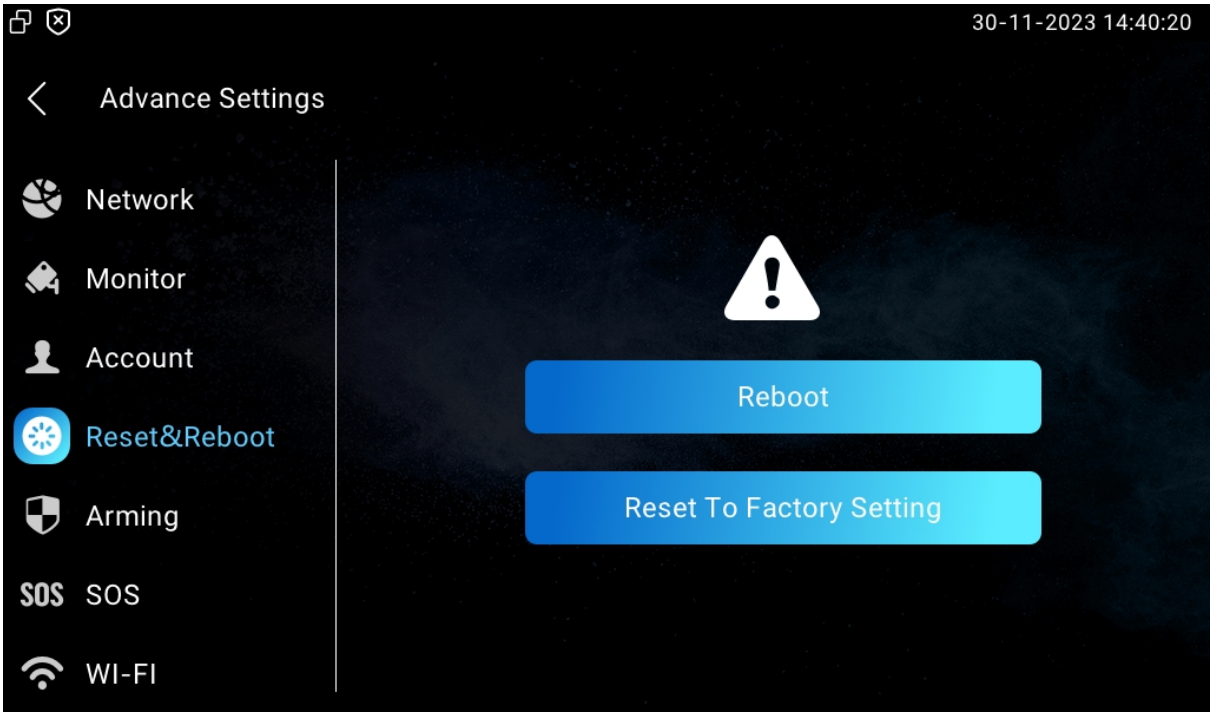
You are required to fill in the correct password before setting the new password.



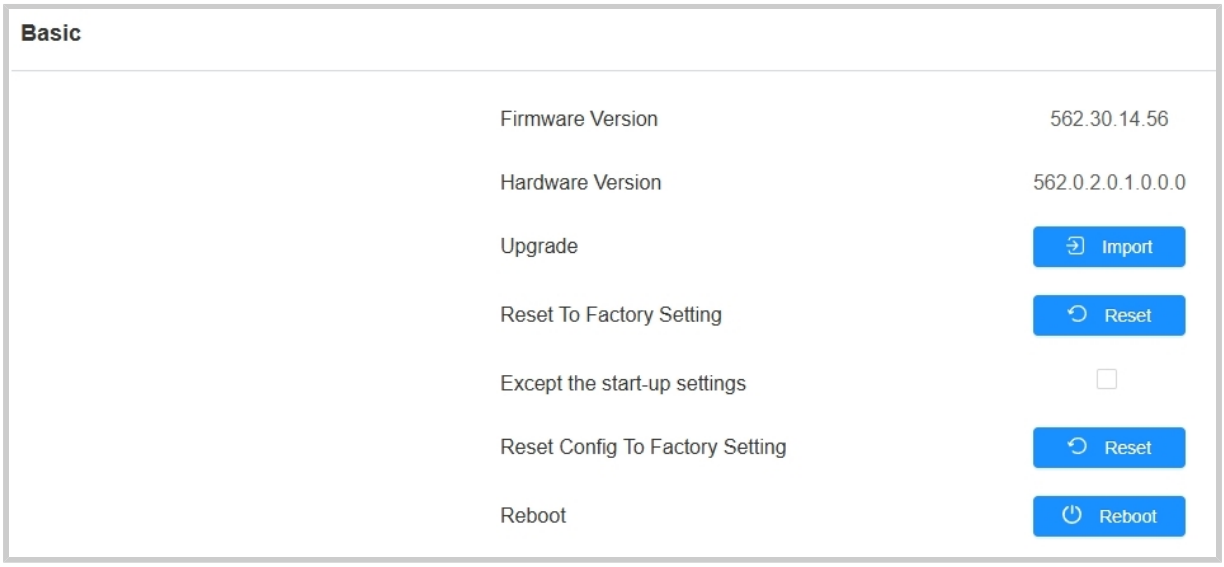
System Reboot & Reset

Reboot

You can reboot the device on its **Settings > Advance Settings > Reset&Reboot** screen.



Or, go to the **Upgrade > Basic** interface.



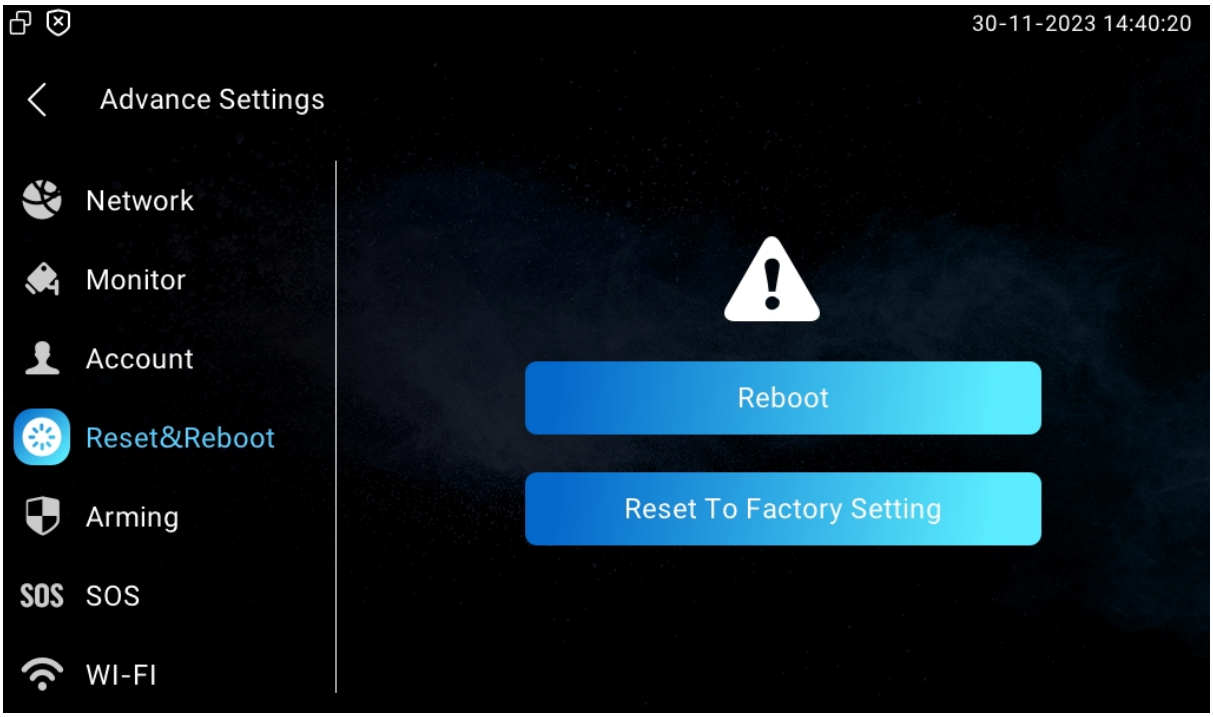
Besides, you can set up a reboot schedule to make the device restart at designated times.

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



Reset

You can reset the device on its **Settings > Advance Settings > Reset&Reboot** screen.

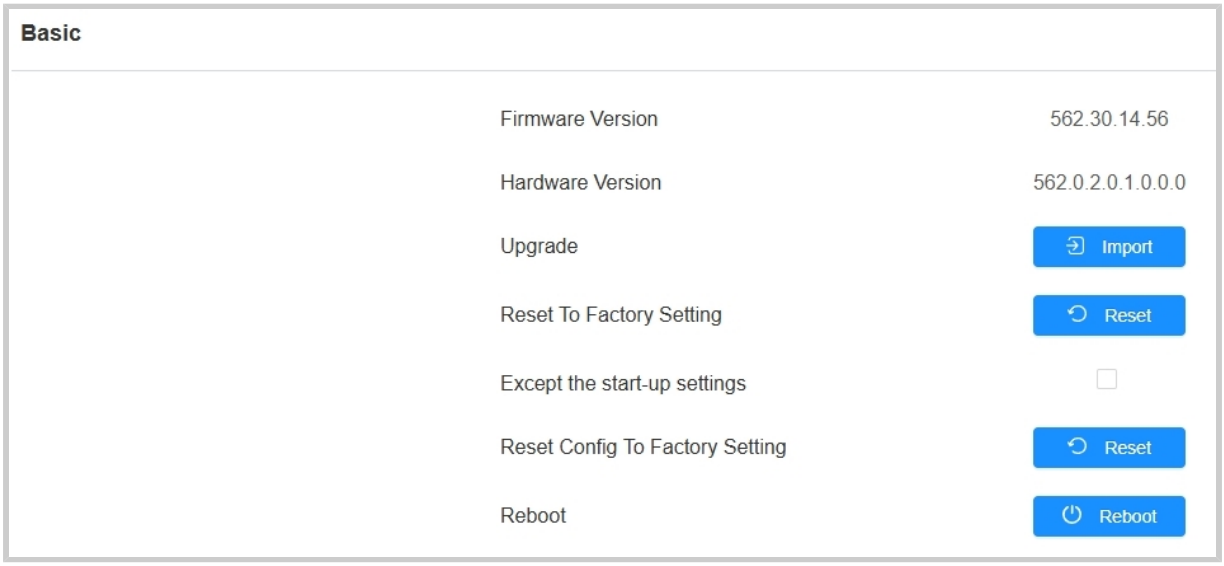


Or, go to the **Upgrade > Basic** interface.

The device provides two reset options:

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

- **Reset Config to Factory Setting**: Retain the user data, such as the RF cards, face data, schedules, and call logs.



- **Except the start-up settings**: Check to retain the initial settings, such as network and time zone.