Akuvox
Open A Smart World

WWW.AKUVOX.COM

S562
INDOOR MONITOR
Administrator Guide

Thank you for choosing the Akuvox S562 series indoor monitor. This manual is intended for the administrators who need to properly configure the indoor monitor. This manual is written based on firmware 562.30.10.115, 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

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

Model Specification

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

Introduction to Configuration Menu

Status: This section gives you basic information such as product information, Network Information, account information, etc.

Account: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & 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.

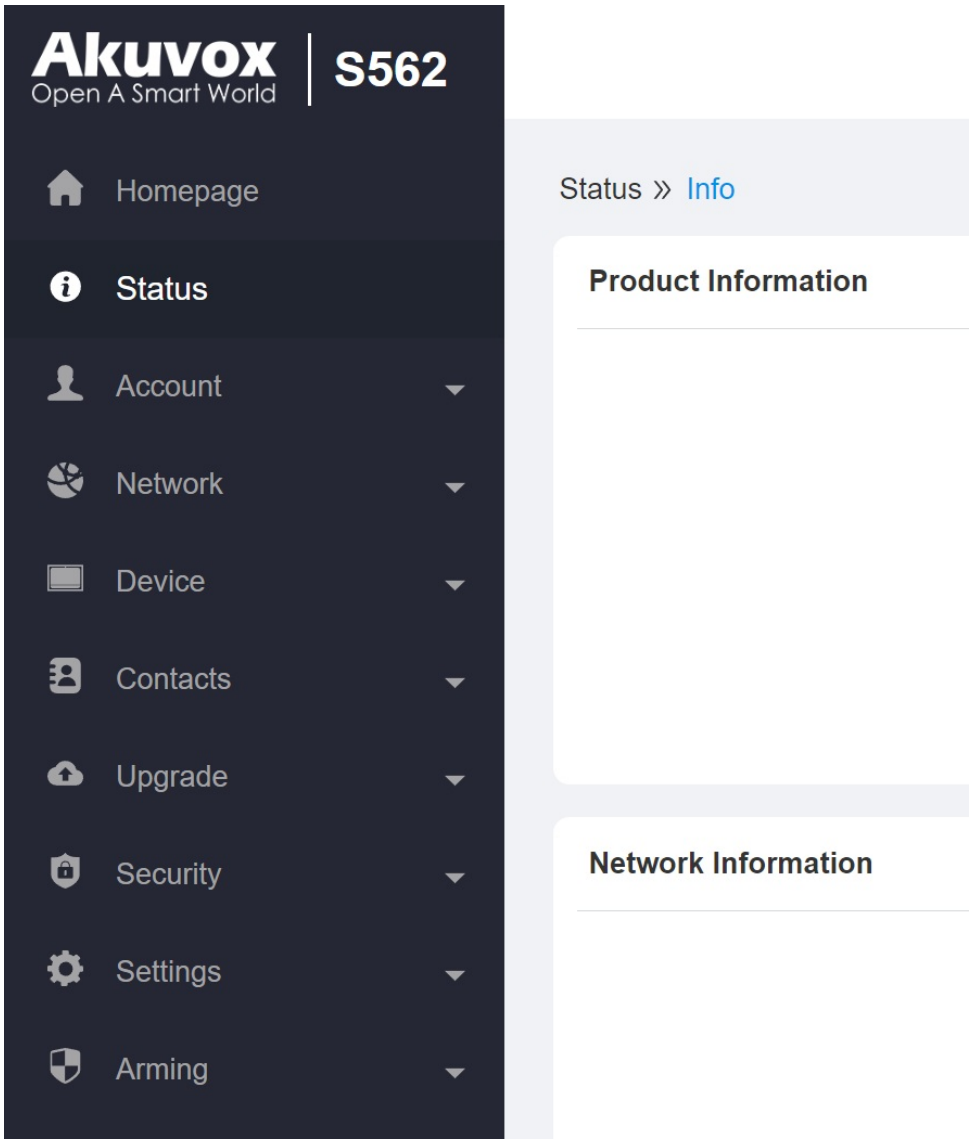
Contacts: This section allows the user to configure the local contact list stored in the device.

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

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

Security: This section is for password modification, account status & session time-out configuration, as well as service location switching.

Settings: This section includes the RTSP and power output.

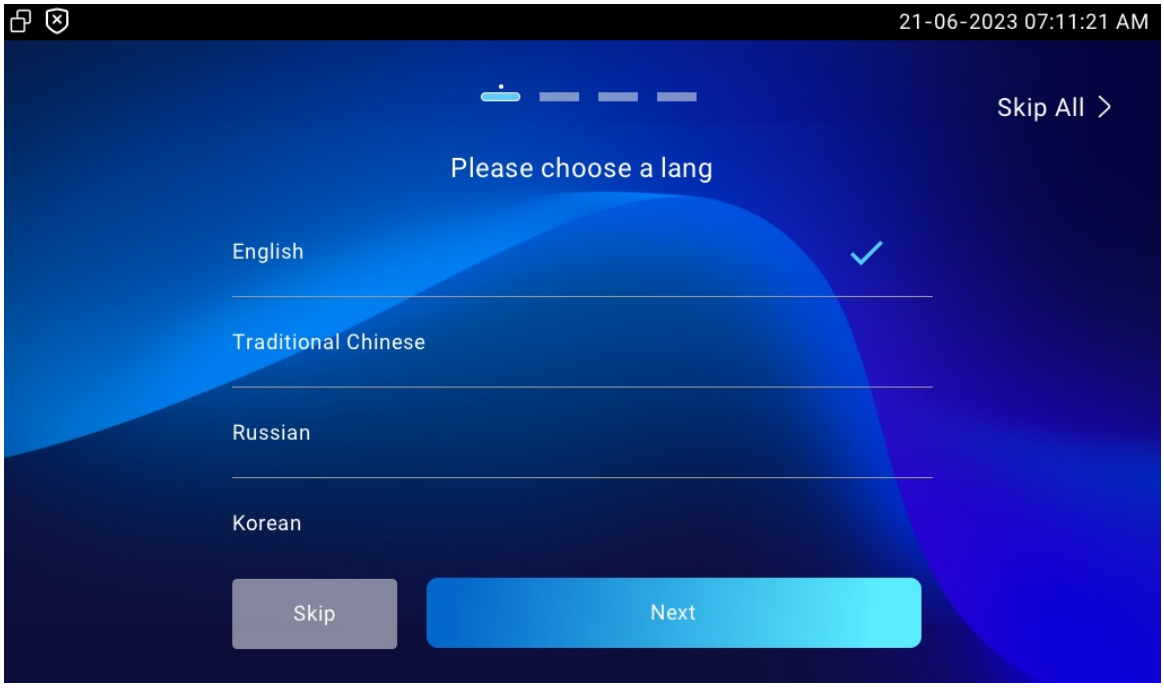

Akuvox
Open A Smart World
S562
Homepage
Status
Account
Network
Device
Contacts
Upgrade
Security
Settings
Arming
Status » Info
Product Information
Network Information

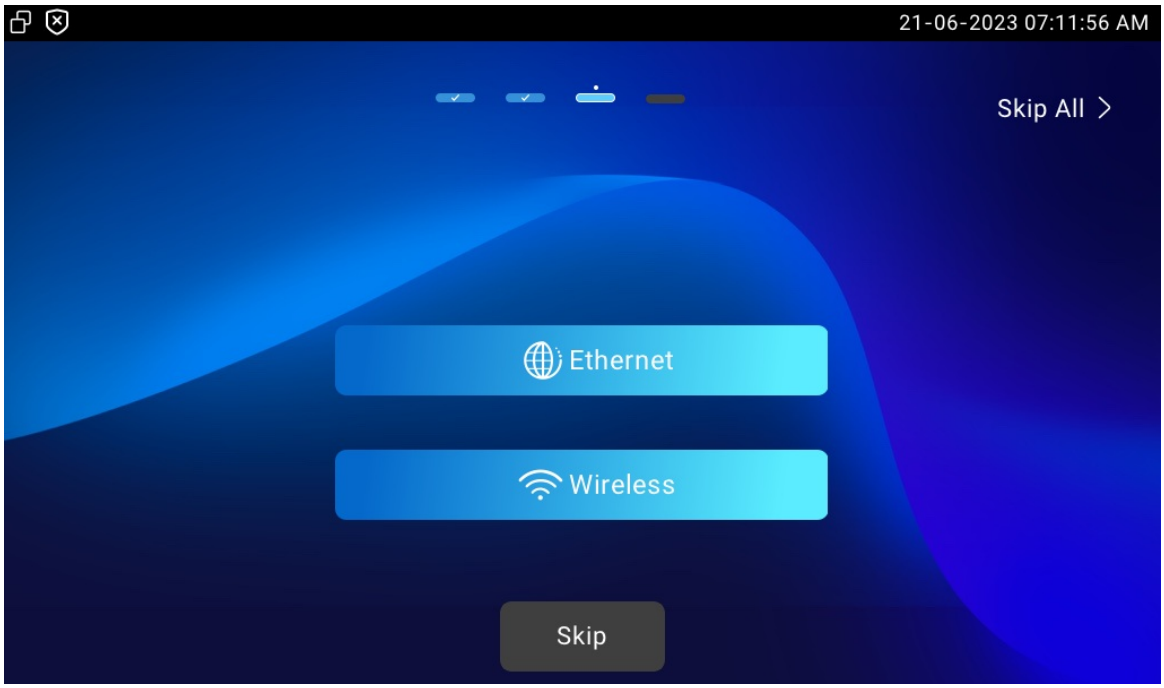
Access the Device

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

Device Start-up Selection

When you first start up the S562 series indoor monitor, you need to perform start-up initialization, which includes a series of settings, such as language, time zone, networking method, and network connection mode. You can also set time, language, and network-related settings later.

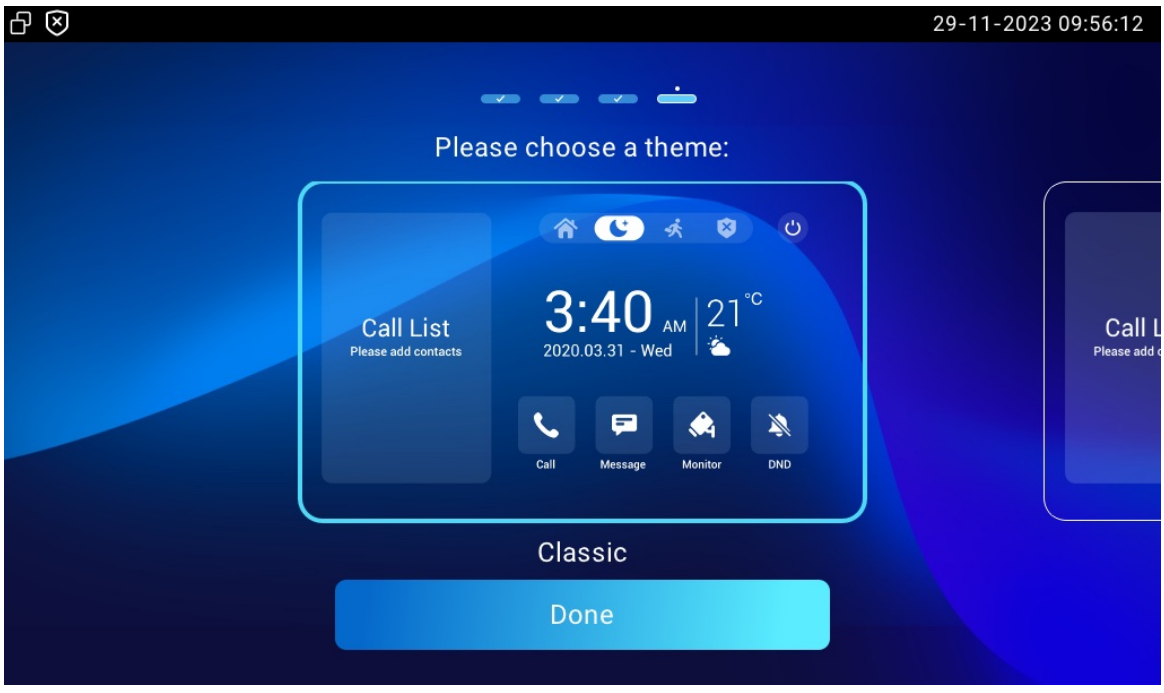


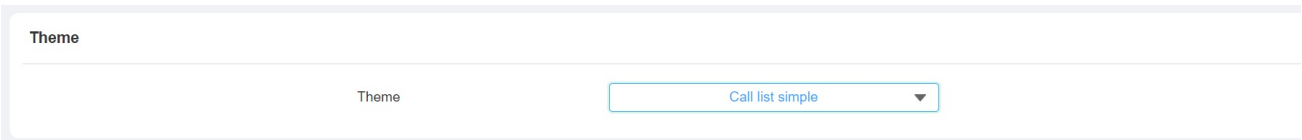


Device Home Screen Type Selection

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

You can select the home screen type on the start-up screen or later configure it on the device web **Device > Display Setting** interface.

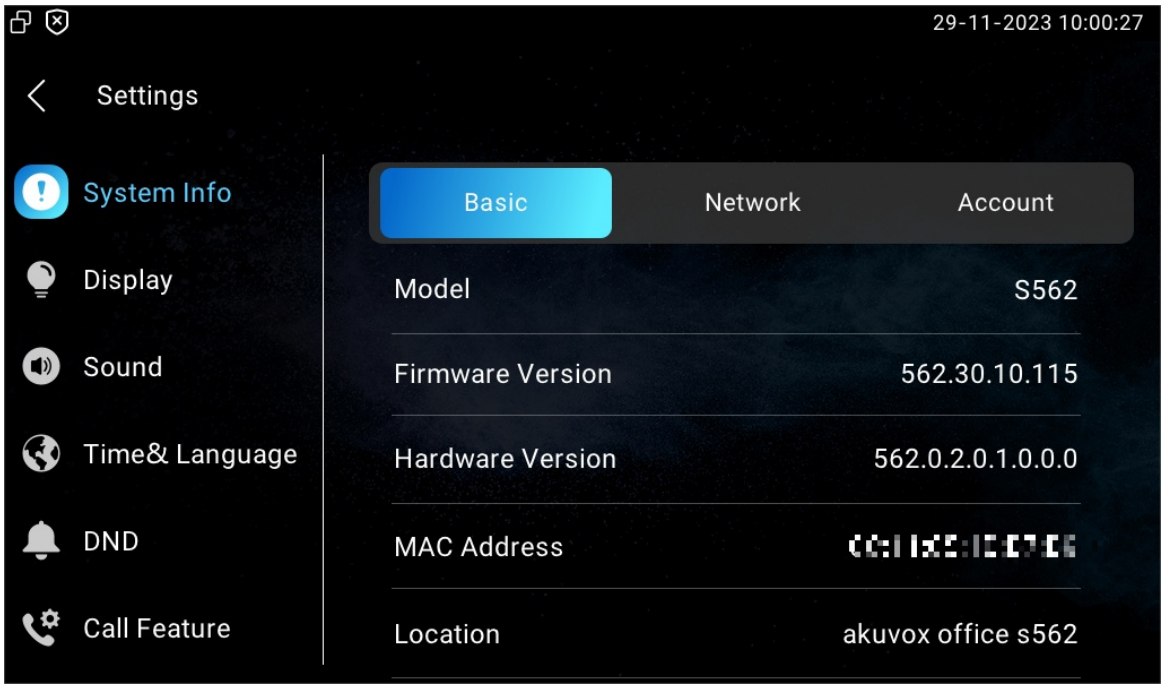




Access the Device Settings on the Device

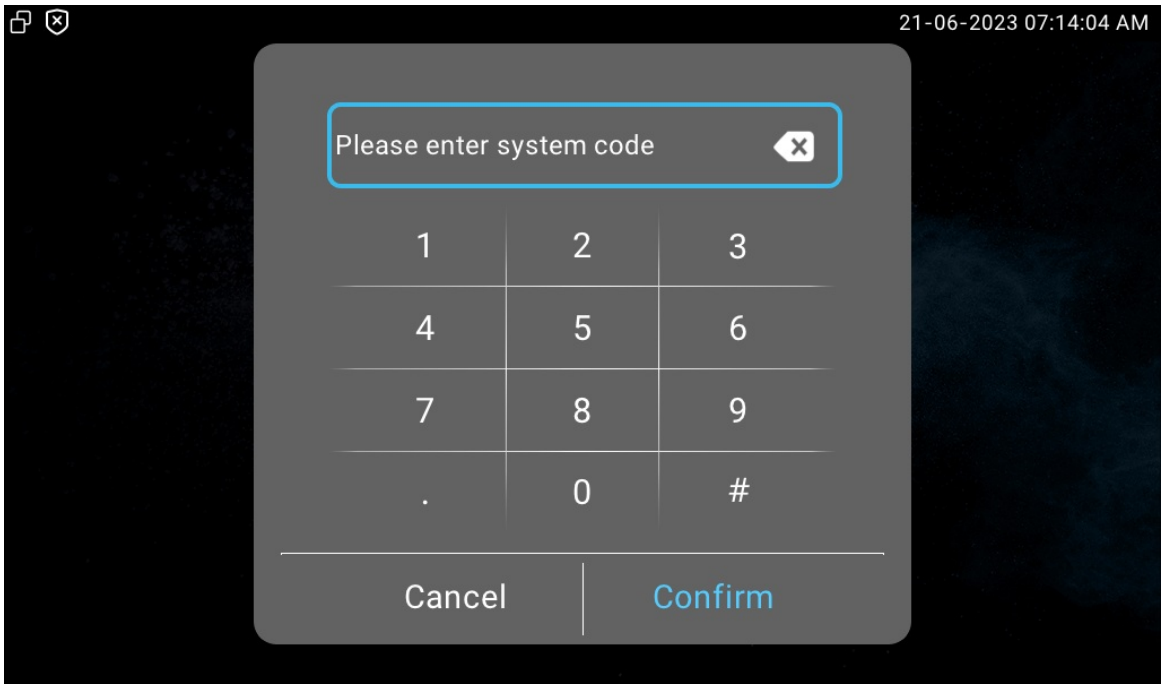
Access Device Basic Settings

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



Access Device Advance Settings

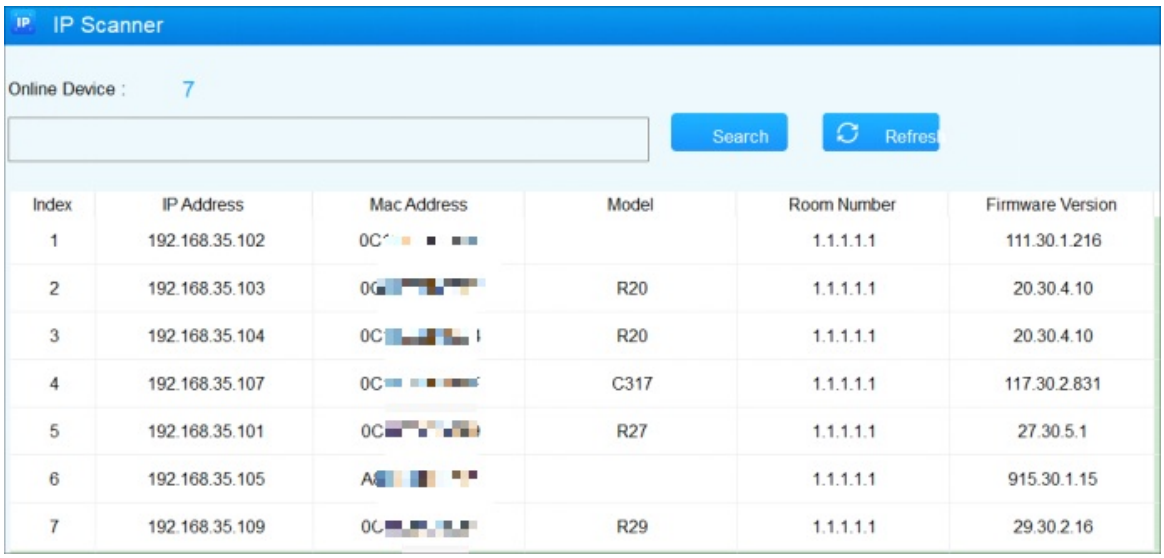
To access the advance settings, press  and then tap Advance Settings. Press the default password 123456 to enter the advance settings.



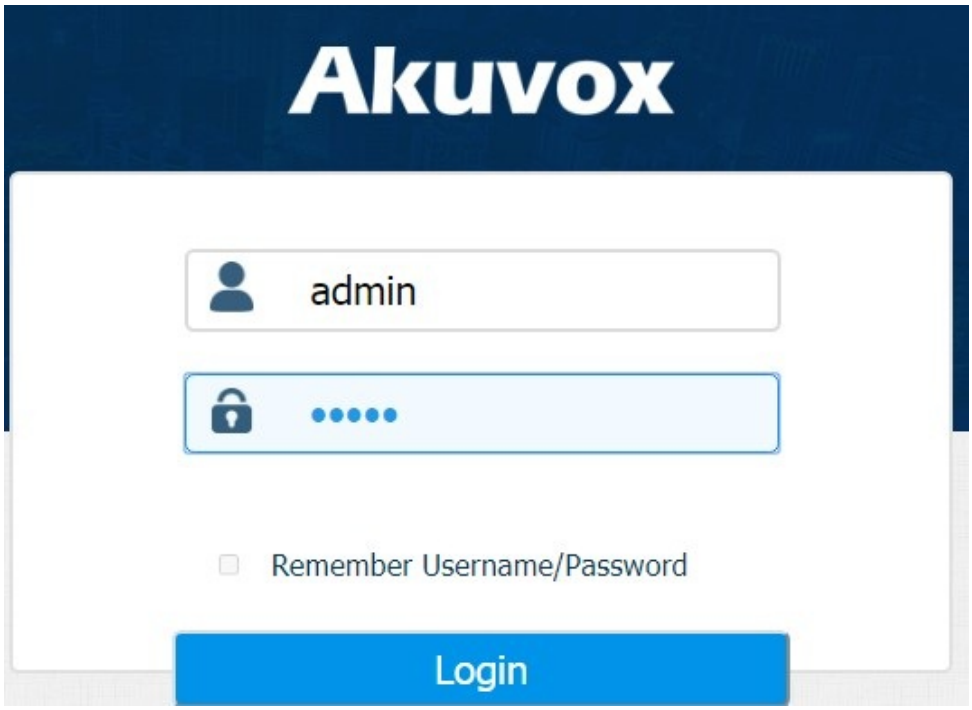
Access the Device Settings on the Web Interface

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

To check the IP address, 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.



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



Note

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

Language and Time Setting

Language Setting

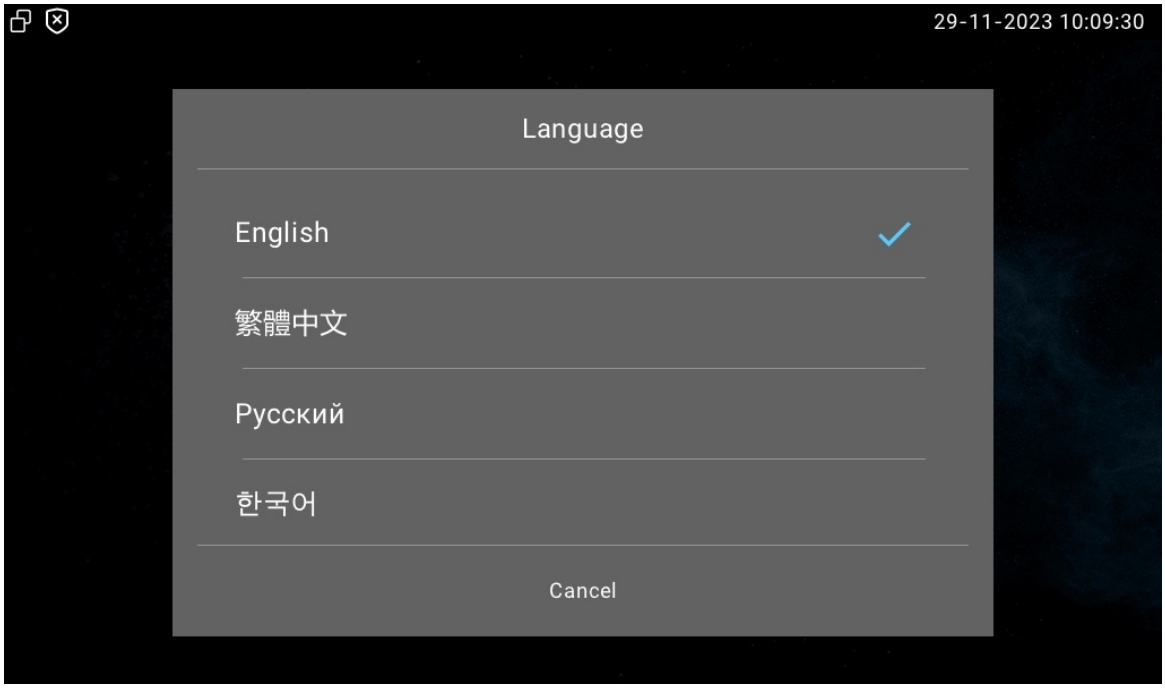
Set up the language during initial device setup or later through the device or web interface according to your preference.

Language Setting on the Device

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

- The device supports the following languages:

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

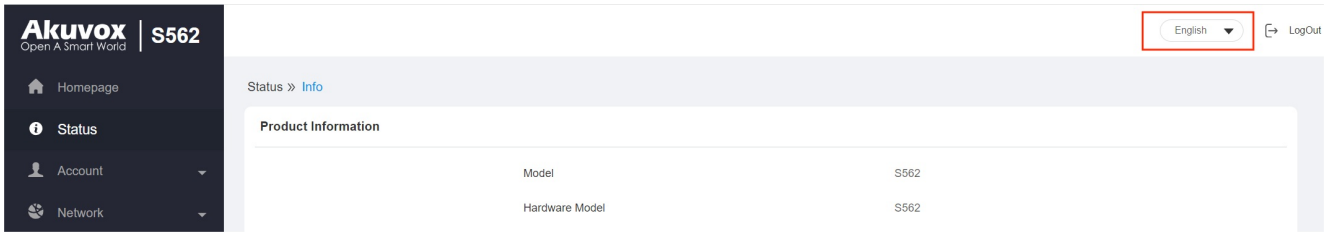


Language Setting on the Web Interface

You can select the device web language in the upper right corner.

- The device web interface supports the following languages when switching browser language:

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

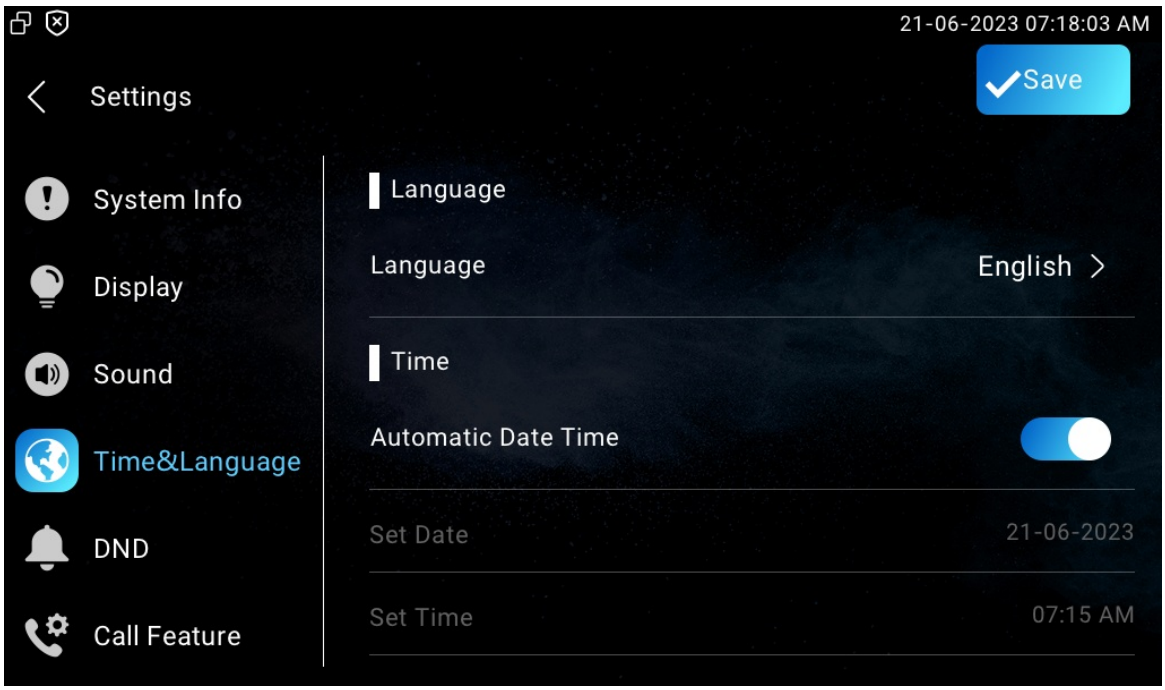


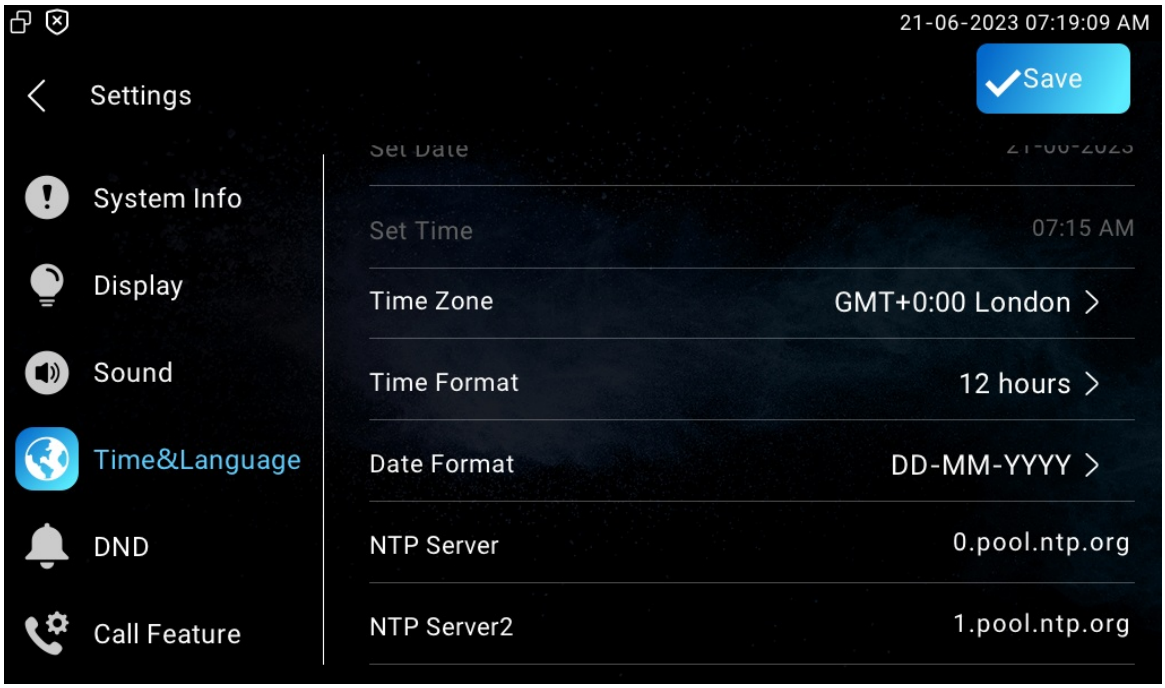
Time Setting

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

Time Setting on the Device

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





Parameter Set-up:

- **Automatic Date Time**: 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 server (NTP). You can also set it up manually by switching off the automatic date, then enter the desired time and date and press the Save tab to save the setting.
- **Time Zone**: the specific time zone selected depending on where the device is used. The default time zone is GMT+0:00.
- **Time Format**: there are two options, 12-hour and 24-hour time format.
- **Date Format**: there are nice options, YYYY/MM/DD, DD-MM-YYYY, DD/MM/YYYY, WW-DD-MM, WW-MM-DD, YYYY-MM-DD, MM-DD-YYYY, MM/DD/YYYY, WW DD/MM/YYYY.
- **NTP Server/NTP Server2**: NTP server address. NTP server 2 is for backup.

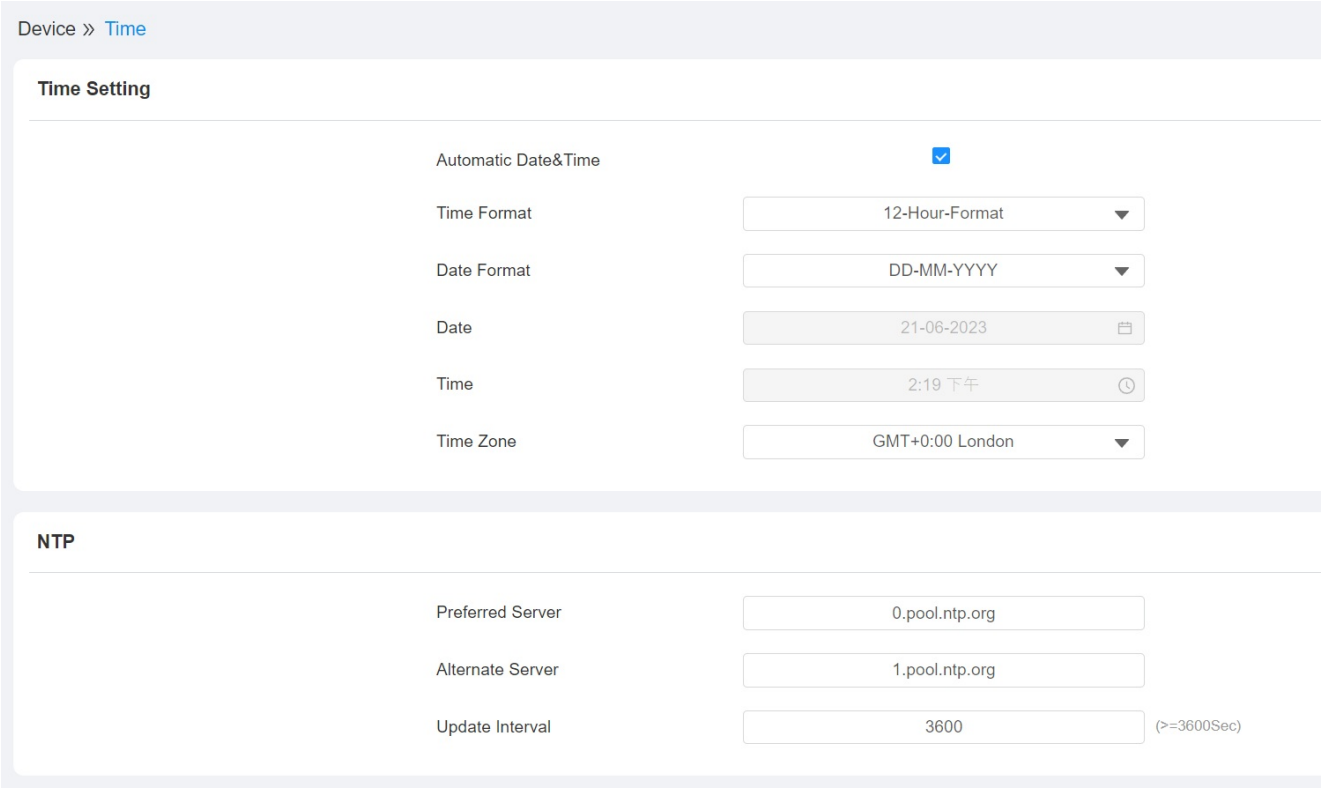
Note

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

Time Setting on the Device Web Interface

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

Navigate to **Device > Time** interface. The parameter configuration is the same as that on the device screen.



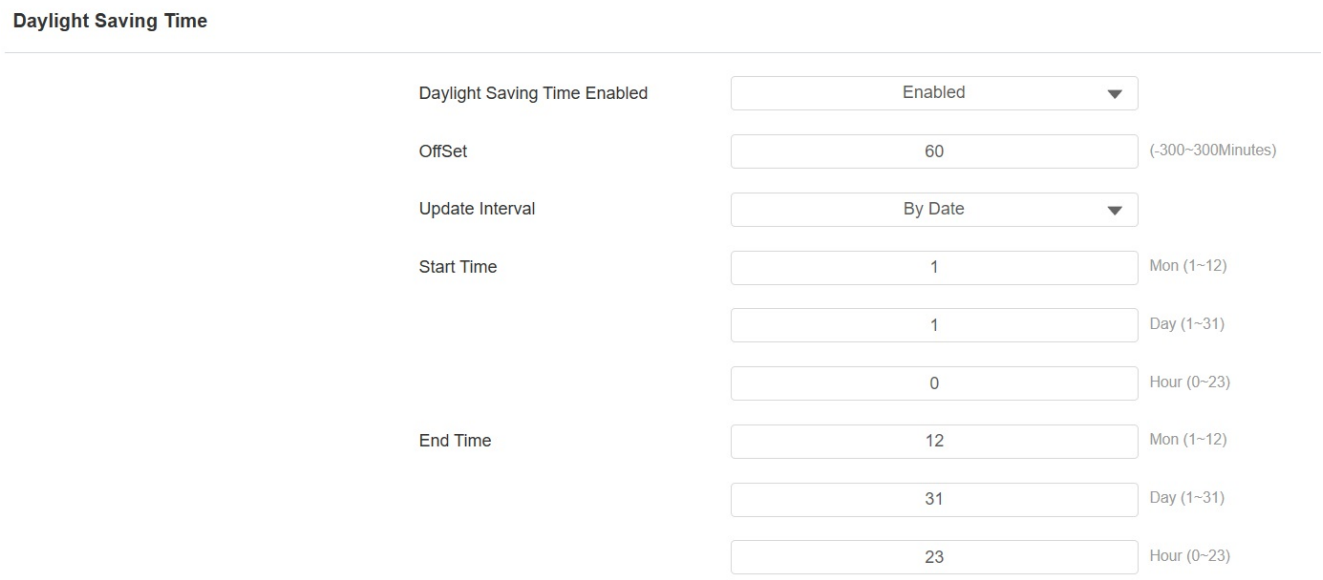
Parameter Set-up:

- **Preferred Server**: the NTP server address.
- **Secondary Server**: the backup server address. When the main NTP server fails, it will change to the backup server automatically.
- **Update Interval**: the interval between two consecutive NTP requests.

Daylight Saving Time

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

To configure it on the **Device > Time** interface.



Parameter Set-up:

- **Daylight Saving Time Enabled**: enable or disable daylight saving time. You can also configure it to make the device adjust the daylight saving time automatically.
- Offset: 60 minutes as default, setting the clocks an hour ahead of the standard time.
- Update Interval: 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 Configuration

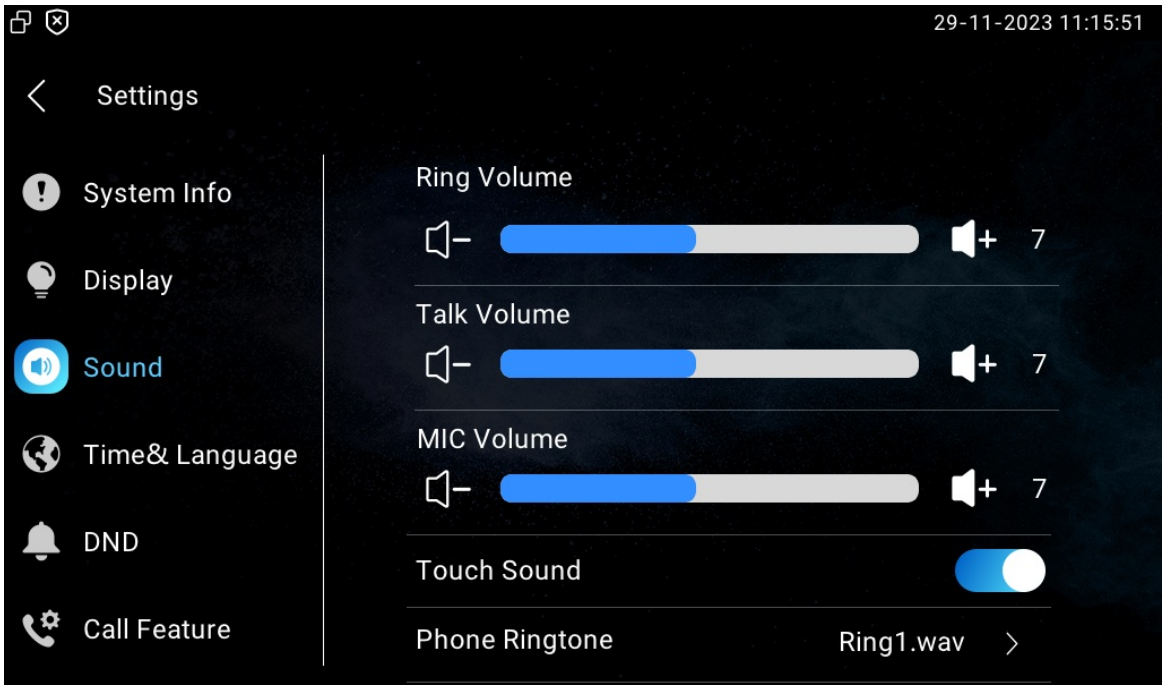
Akuvox indoor monitor provides you with various types of ringtones and volume configurations. You can configure them on the device directly or on the web interface.

Volume Configuration

Configure Volume on the Device

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

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

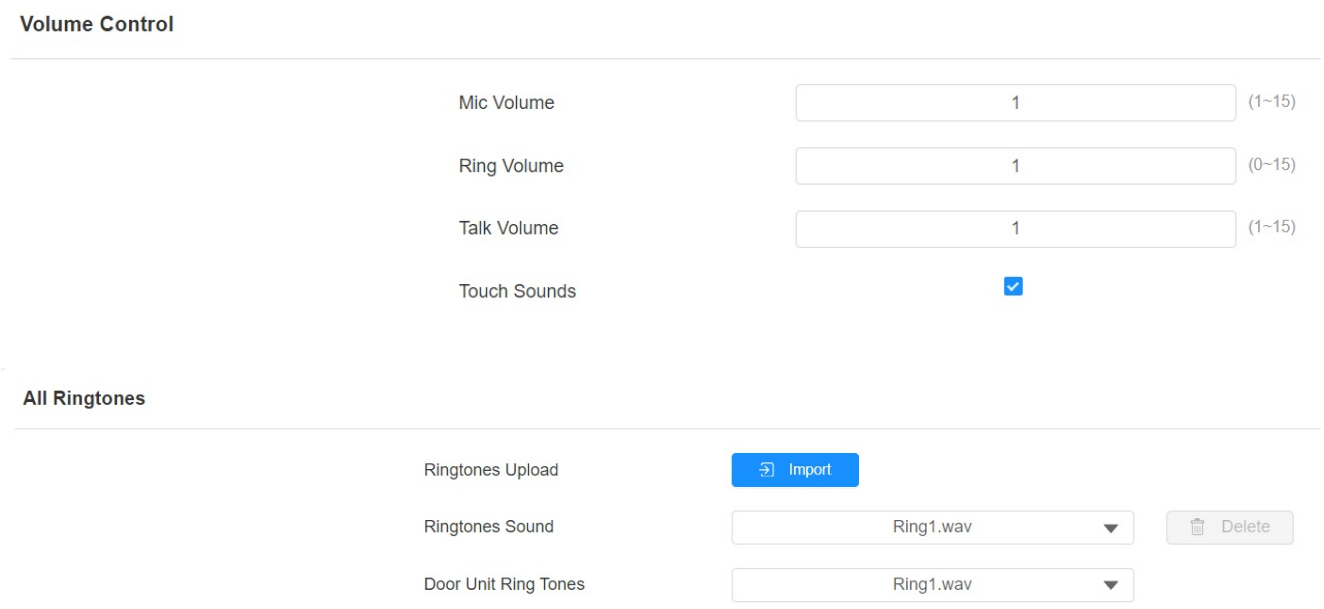


Parameter Set-up:

- **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.

Configure Volume on the Web Interface

You can configure volumes and customize your doorbell sound and alarm ringtone to your preference on the device web **Device > Audio** interface. The volume configuration is the same as that on the device screen.



Parameter Set-up:

- **Door Unit Ring Tones**: the ring tone when receiving calls from Akuvox door units.

Note

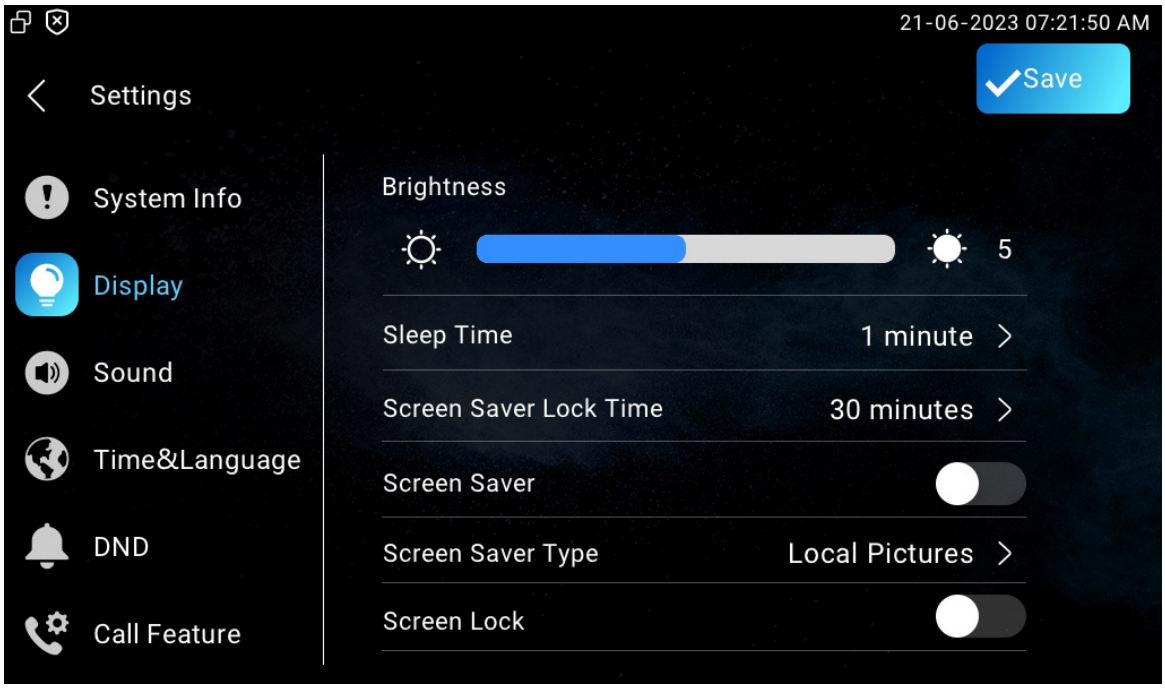
- Ringtone files to be uploaded must be in **.WAV** format with 250K maximum.

Screen Display Configuration

Screen Display Setting on the Device

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

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



Parameter Set-up:

- **Brightness**: move the blue bar to adjust the screen brightness.
- **Sleep Time**: set the sleep time based on the screen saver (15 sec to 30 min).
    - If the screen saver is enabled, then the sleep time is the screen saver start time. For example, if you set it as 1 min, then the screen saver will start automatically when the device has no operation for 1 min.
    - If the screen saver is disabled, then the sleep time is the screen turn-off time. For example, if you set it as 1 min, then the screen will be turned off automatically when the device has no operation for 1 min.
- **Screen Saver Lock Time**: set the screen saver start time from 15 seconds up to 2 hours.
- **Screen Saver**: screen saver starts when the device detects no operation, or no one is

approaching.

- **Screen Saver Type**: **Local Pictures** displays the picture uploaded to the indoor monitor as the screen saver.
- **Screen Lock**: the screen lock will lock the screen after the screen turns off (turn dark). You are required to enter the system code to unlock the screen.
- **Screen Clean**: it allows you to wipe the screen clean without triggering unwanted changes in the settings.
- **Wallpaper**: it is for local wallpaper selection.

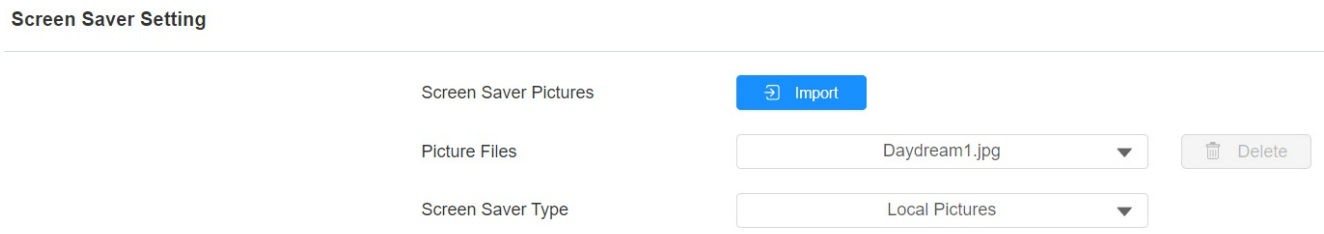
You can also turn off the screen manually.

Screen Display Setting on the Web Interface

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

Upload Screen Saver

You can upload screen-saver pictures on the web **Device > Display Setting > Screen Saver Setting** interface.



Parameter Set-up:

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

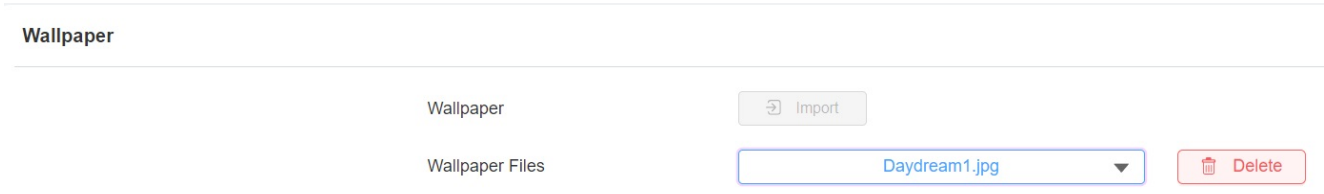
Notes

- The pictures uploaded should be in **1024x600 JPG** format with a maximum of 256K.
- The file name can only contain "_", ".", digits, and letters.
- The previous pictures with a specific ID order will be overwritten when the repetitive designation of pictures to the same ID order occurs.

Upload Wall Paper

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

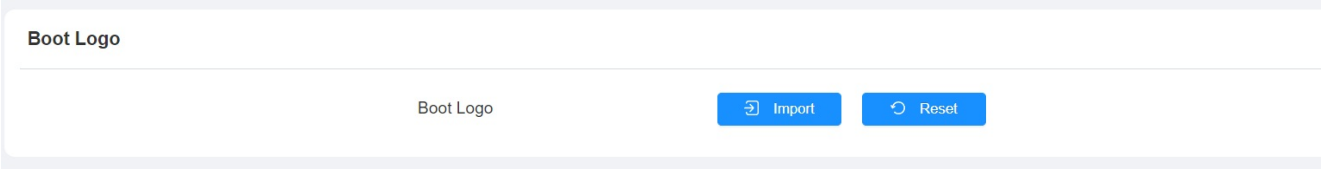
Navigate to **Device > Display Setting > Wallpaper** interface.



Upload Device Booting Image

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

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



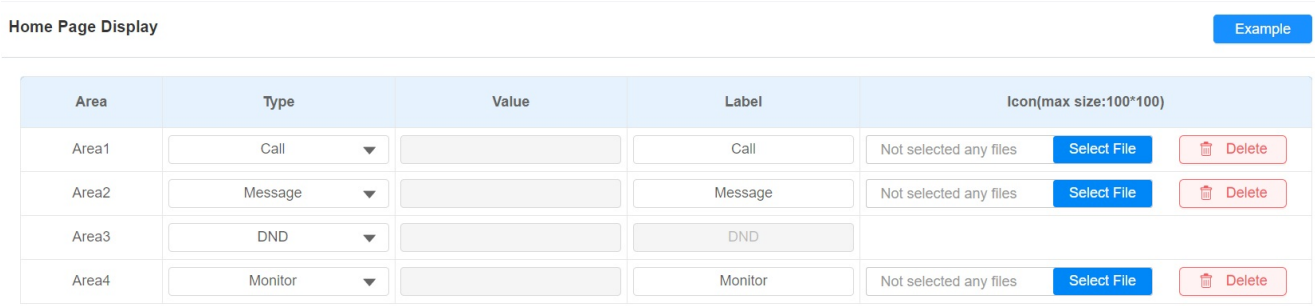
Note

- The pictures uploaded should be in **1024x600 JPG** format with a maximum of 100K.

Icon Screen Display Configuration

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

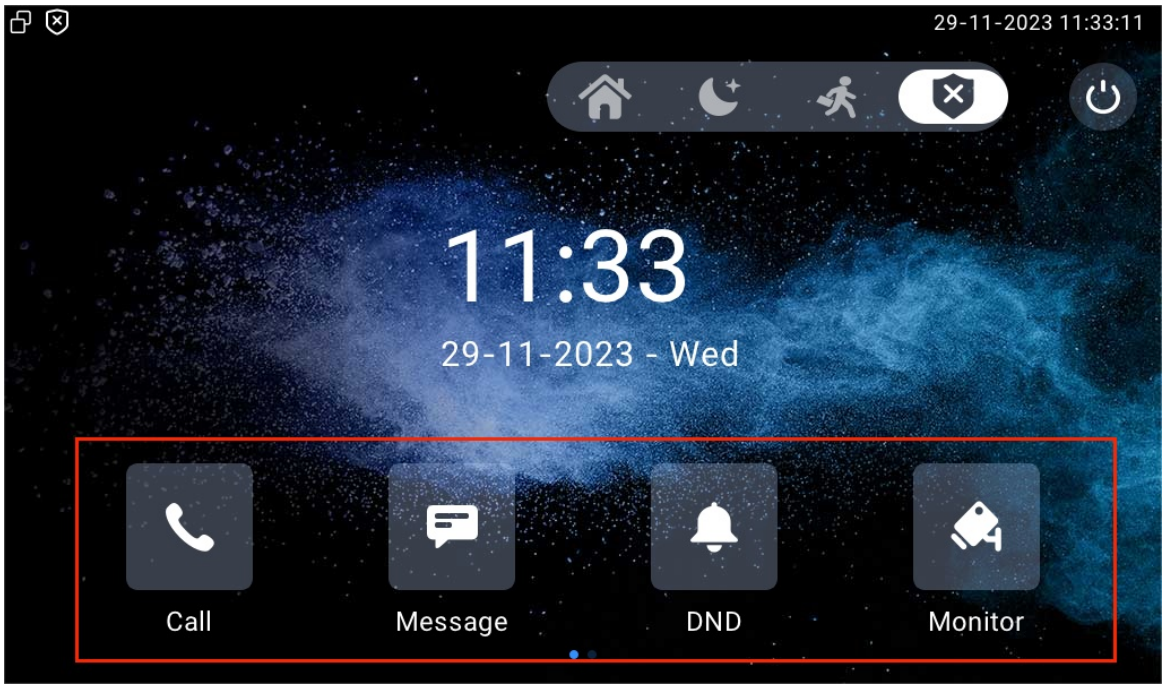
Navigate to **Device > Display Setting**.



Parameter Set-up:

- **Type**: the functional icons you want to put on the home page **(DND, Message, Contacts, Call, Arming, SOS, Settings, Sound, Display, Status, Relay, Lift, Unlock, Smart Living, Capture Log, Monitor, All Call)**.
- **Label**: rename the icon if needed, while the DND icon cannot be renamed.
- **Icons**: click to upload the icon picture. The maximum icon size is **100*100**. The picture format can be JPG, JPEG, and PNG.

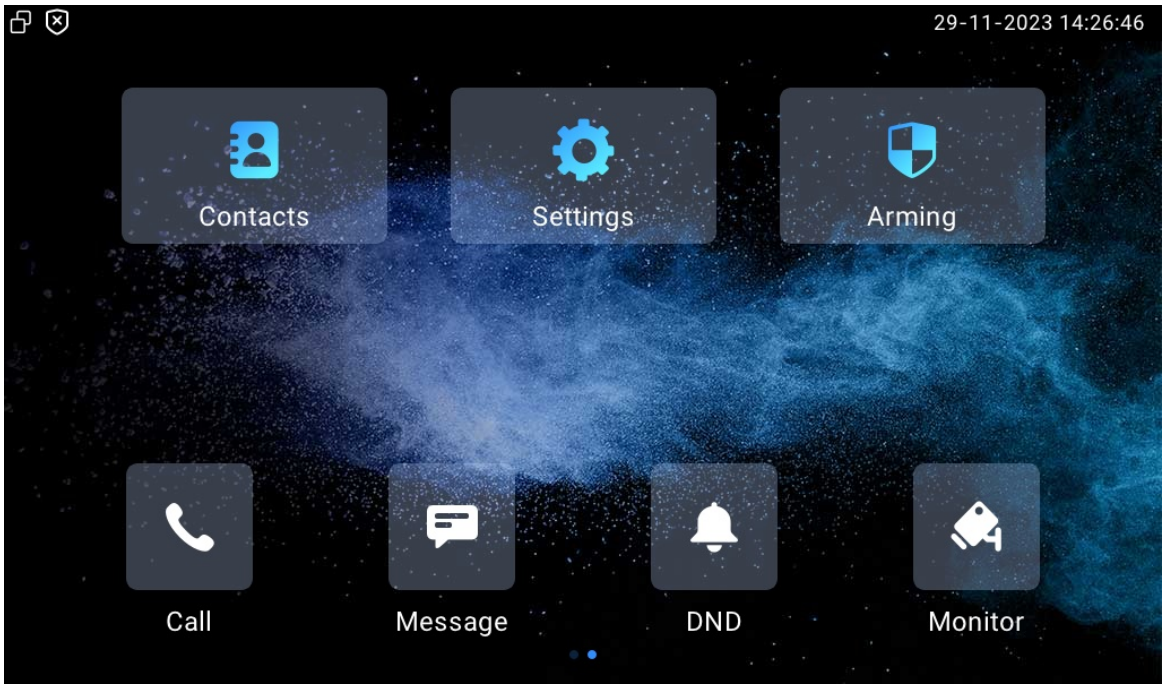
See the four icons on the home screen below:



To configure the icons displayed on **More Page Display** on the same **Device > Display Setting** interface.

More Page Display Example

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



Unlock Tab Configuration

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

Go to **Device > Relay > SoftKey In Talking Page** interface.

Softkey In Talking Page

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

Parameter Set-up:

- **Status**: with the unlock tabs enabled on the talking screen, the unlock tabs will appear during a call.
- **Display Name**: name the unlock tab to distinguish it from others.
- **Type**: the relay trigger type (Local Relay, Remote Relay HTTP, Remote Relay DTMF 1/2/3, Web Relay Action).

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

Softkey In Call-Preview Page

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

Parameter Set-up:

- **Status**: with the unlock tab enabled, it will appear on the call preview screen.
- **Display Name**: name the unlock tab to distinguish it from others.
- **Type**: the relay trigger type. (Remote Relay HTTP, Local Relay, Web Relay Action).

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

Softkey In Home Or More Page

Key	Status	Display Name	Type
Key	Enabled	Unlock	Remote Relay HTTP1

Parameter Set-up:

- **Status**: with the unlock tabs enabled, the unlock tabs will appear during a call.
- **Display Name**: name the unlock tab to distinguish it from others.
- **Type**: the relay trigger type (Remote Relay HTTP 1).

To set up the unlock tab on the **Monitor** screen on the same interface.

Softkey In Monitor Page

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

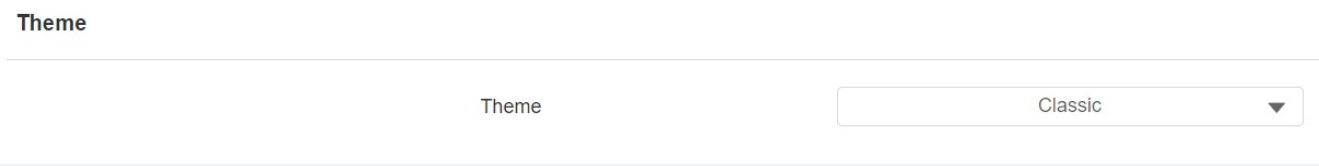
Parameter Set-up:

- **Status**: with the unlock tabs enabled, the unlock tabs will appear on the monitoring screen.
- **Display Name**: name the unlock tab to distinguish it from others.
- **Type**: the relay trigger type (Remote Relay HTTP, Local Relay, Remote Web Relay).

Home Screen Display

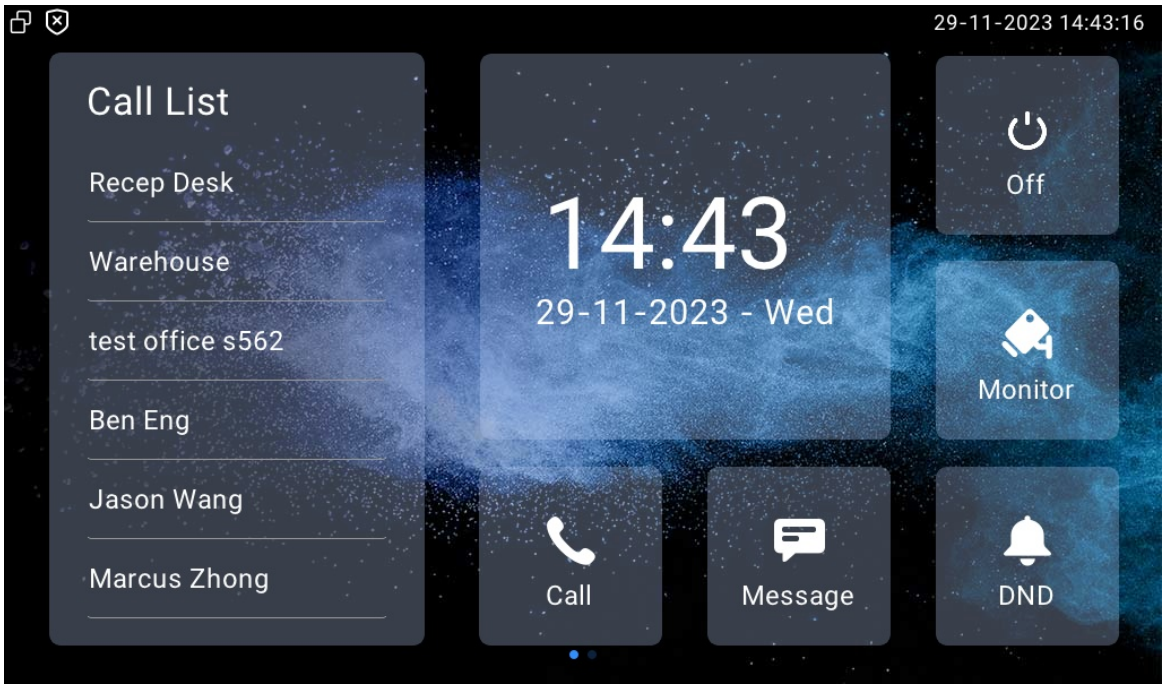
You can select the classic or call list home screen display.

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



Classic Home Screen:

Call List Home Screen:


29-11-2023 14:43:16
Call List
Recep Desk
Warehouse
test office s562
Ben Eng
Jason Wang
Marcus Zhong
14:43
29-11-2023 - Wed
Off
Monitor
Call
Message
DND

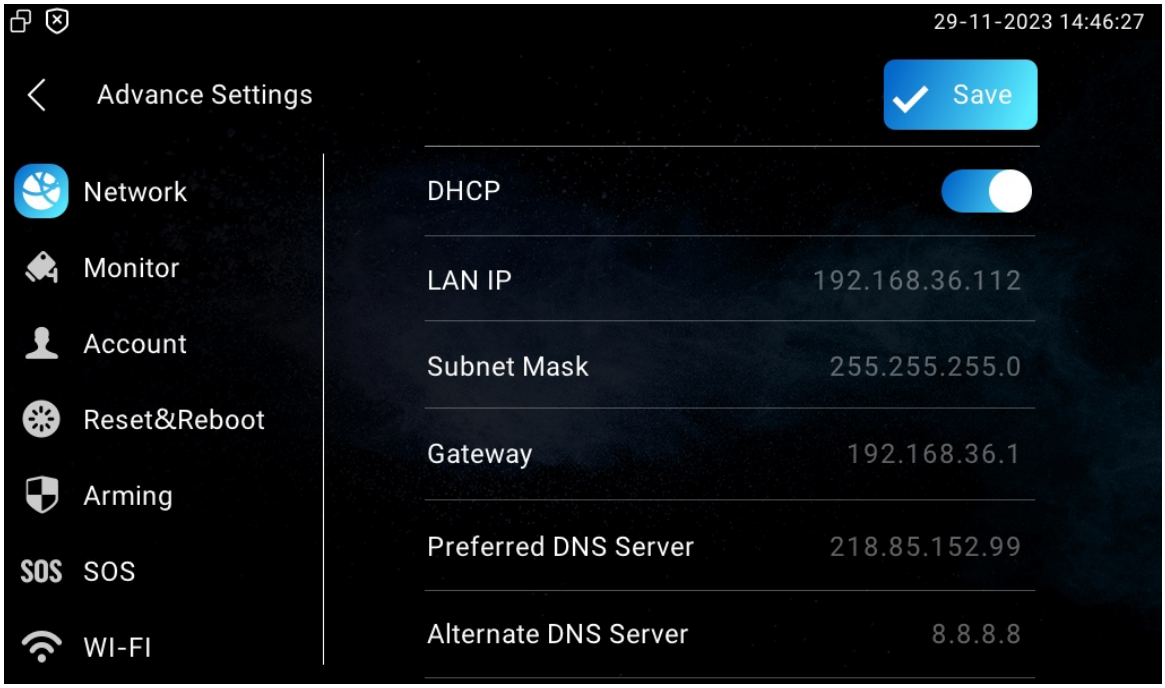
Network Setting

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.

Configure Network Connection on the Device

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



Parameter Set-up:

- **DHCP**: DHCP mode is the default network connection. If the DHCP mode is turned on, then the device will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically. If you turn off the DHCP mode, the device will be changed to static IP mode, and then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to your actual network environment.
- **IP Address**: the IP address when the static IP mode is selected.
- **Subnet Mask**: the subnet mask should be set up according to your actual network

environment.

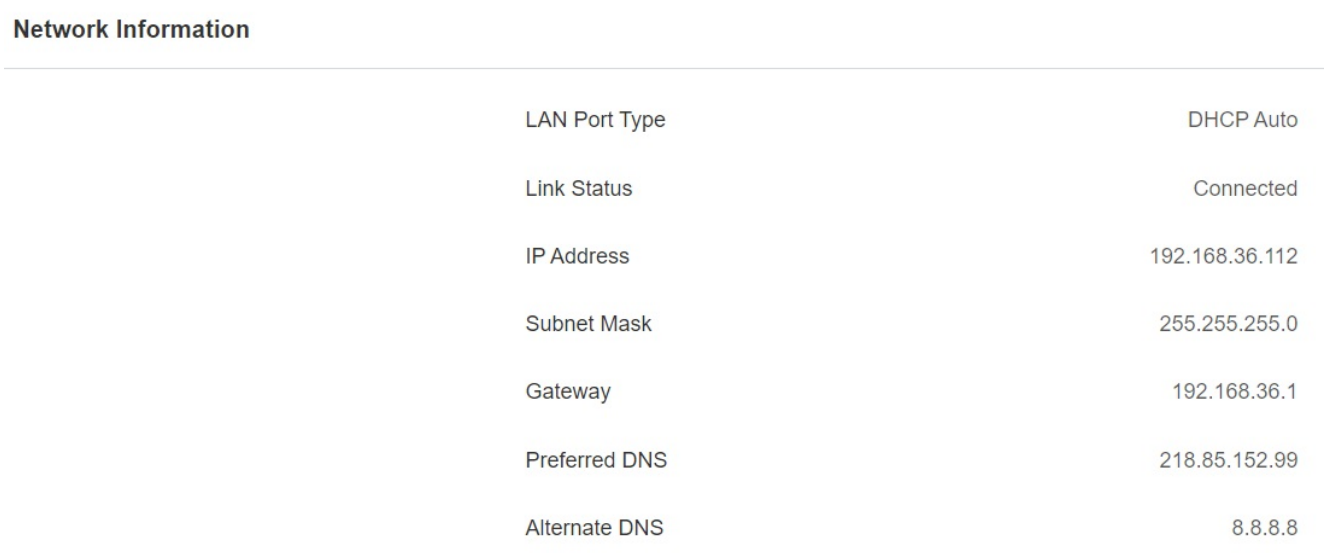
- **Gateway**: the gateway should be set up according to the IP address.
- **Preferred & Alternate DNS Server**: the preferred and alternate Domain Name Server (**DNS**). Preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

Note

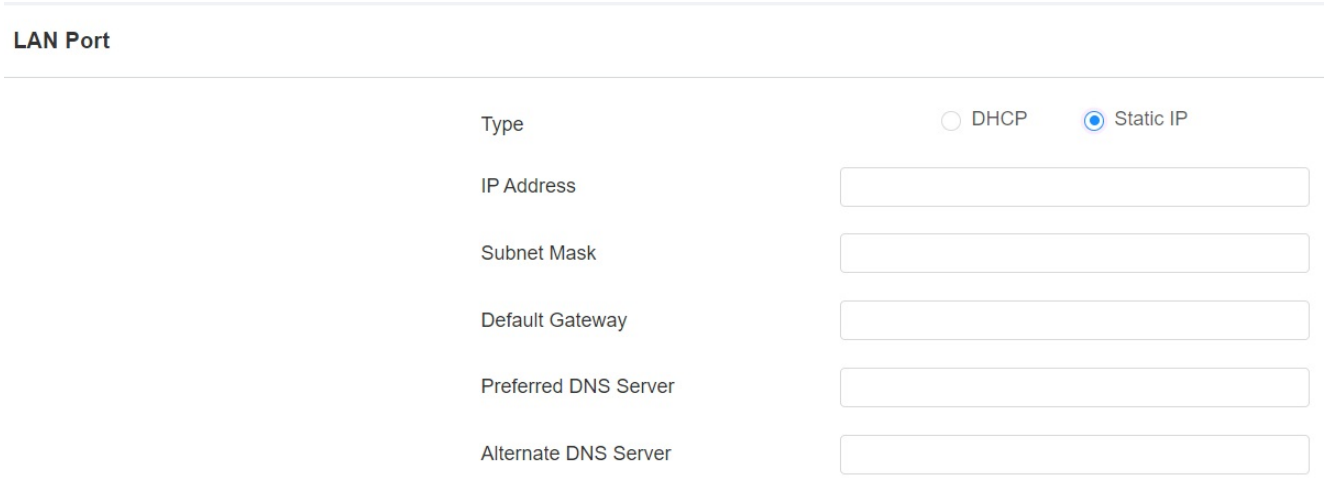
- You can press **System Info**, and then press **Network** on the **Settings** screen to check device network status.
- The default code to enter advance settings is **123456**.

Configure Device Network Connection on the Web Interface

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



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



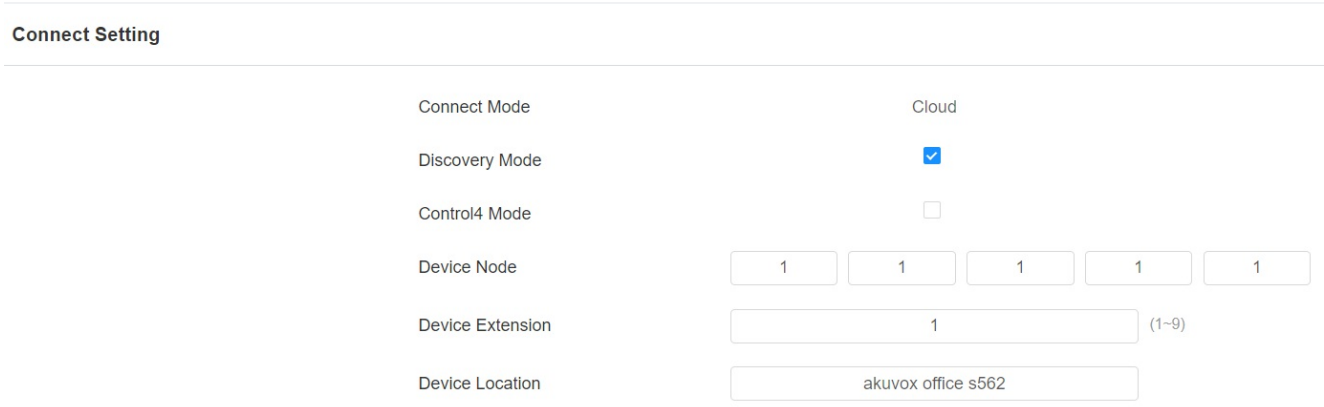
Parameter Set-up:

- **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 your actual network environment.
- **IP Address**: the IP address when the static IP mode is selected.
- **Subnet Mask**: the subnet mask should be set up according to your actual network environment.
- **Default Gateway**: the gateway should be set up according to the IP address.
- **Preferred/Alternate DNS Server**: the preferred and alternate Domain Name Server (**DNS**). Preferred DNS server is the primary DNS address while the alternate DNS server is the secondary one. The device will connect to the alternate server when the primary server is unavailable.

Device Deployment in Network

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

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



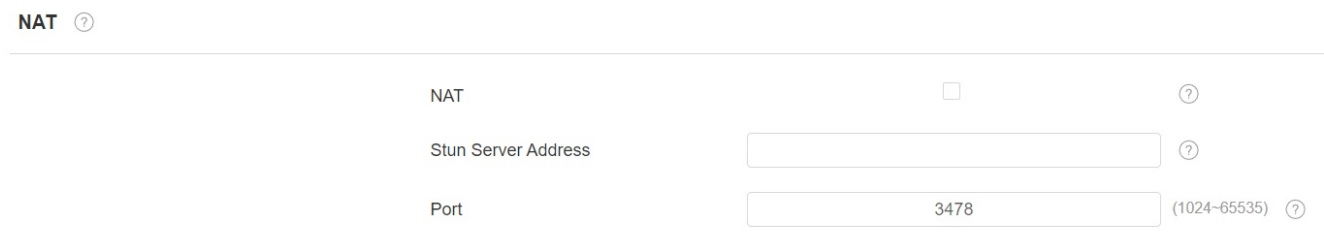
Parameter Set-up:

- **Connect Mode**: it is automatically set up according to the actual device connection with a specific server in the network such as **SDMC**, **Cloud**, and **None**. **None** is the default factory setting indicating the device is not in any server type.
- **Discovery Mode**: with discovery mode enabled, the device can be discovered by other devices in the network. Uncheck the box if you want to conceal the device.
- **Control4 Mode**: enable it to integrate with Control 4 smart home.
- **Device Node**: specifies the device address by entering device location info from the left to the right: Community, Unit, Stair, Floor, and Room in sequence.
- **Device Extension**: the device extension number for the device you installed.
- **Device Location**: the location in which the device is installed and used.

Device NAT Setting

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

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

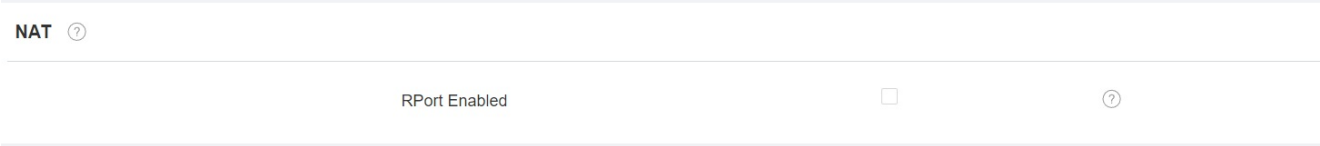


Parameter Set-up:

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

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

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

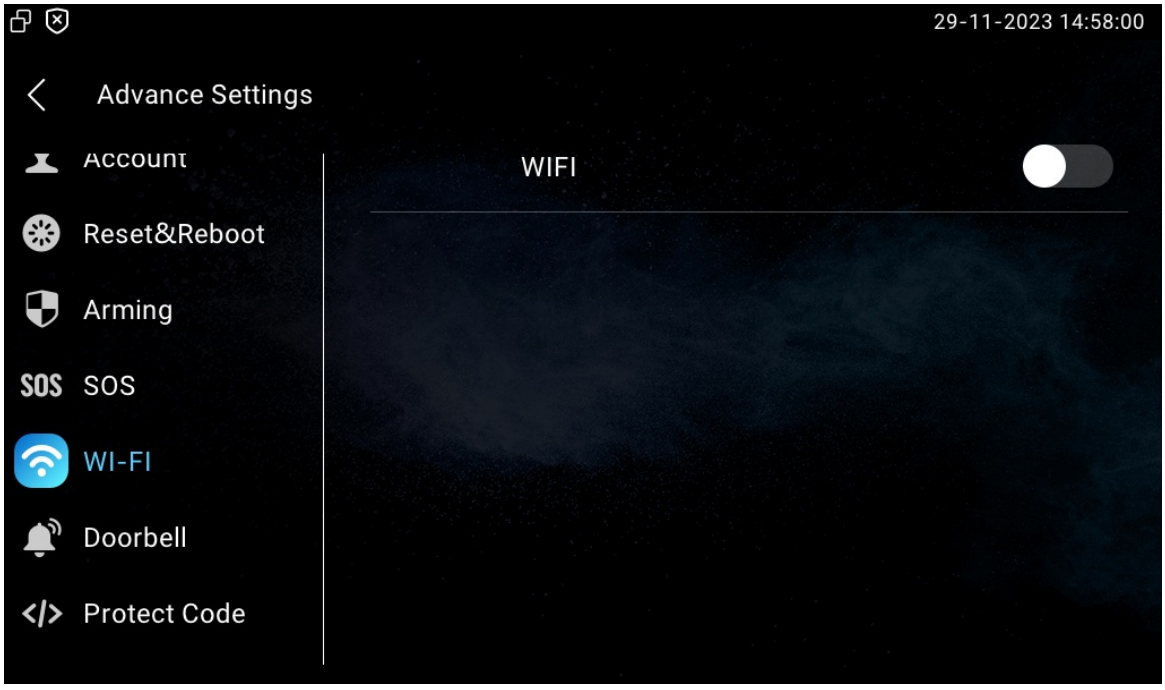


Parameter Set-up:

- **RPort**: enable the RPort when the SIP server is in WAN (**Wide Area Network**) for the SIP account registration.

Device Wi-Fi Setting

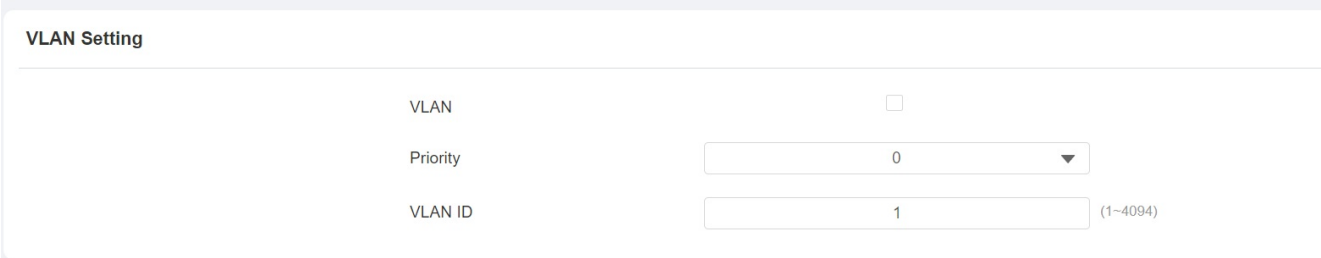
You can set the Wi-Fi on the device screen **Setting > Advanced Settings**.



VLAN Setting

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

To configure the VLAN function on the device web interface **Network > Advanced > VLAN Setting**.



Parameter Set-up:

- **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.

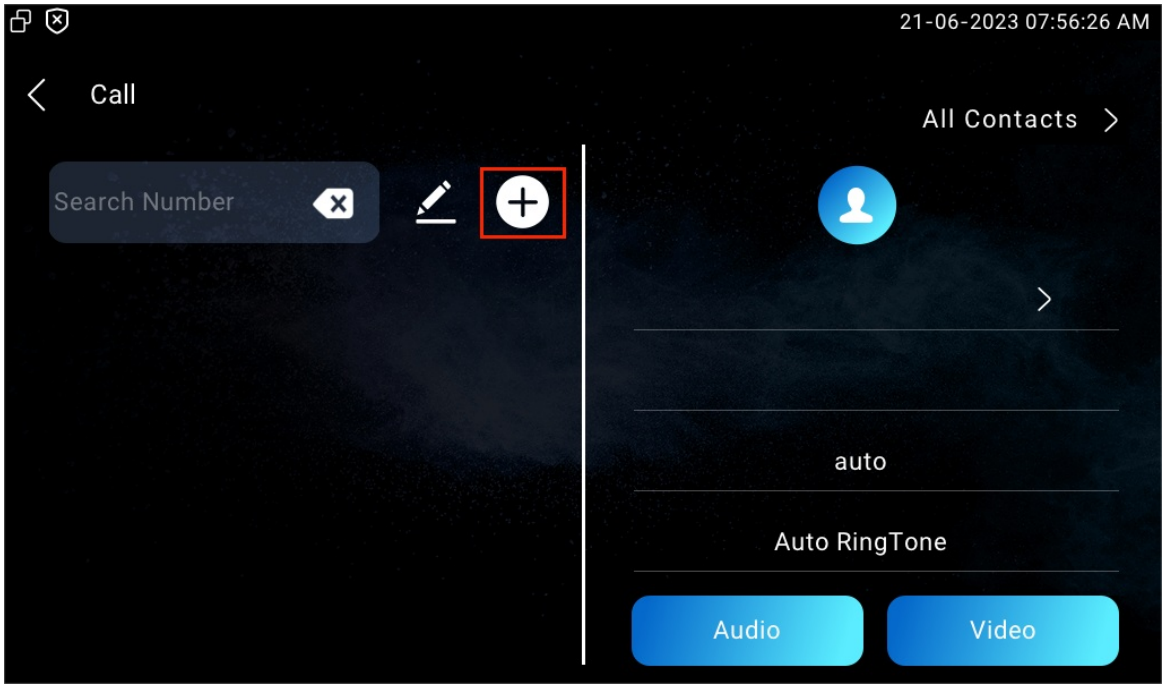
Contacts Configuration

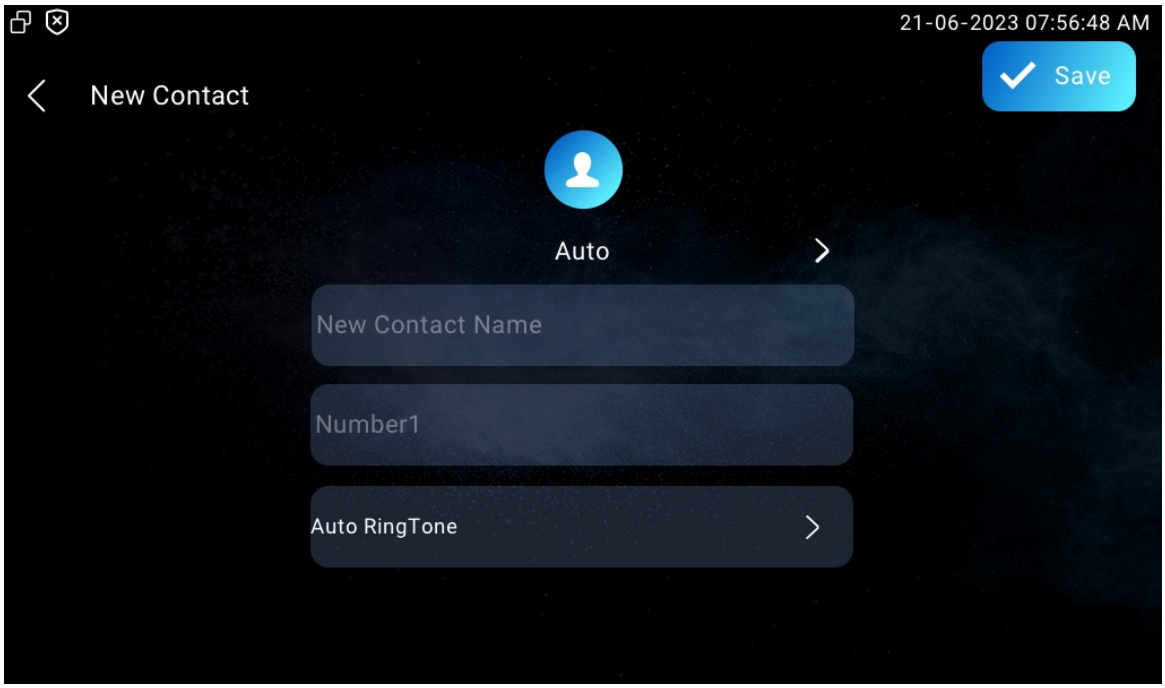
Contacts Configuration on the Device

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

Add Contacts

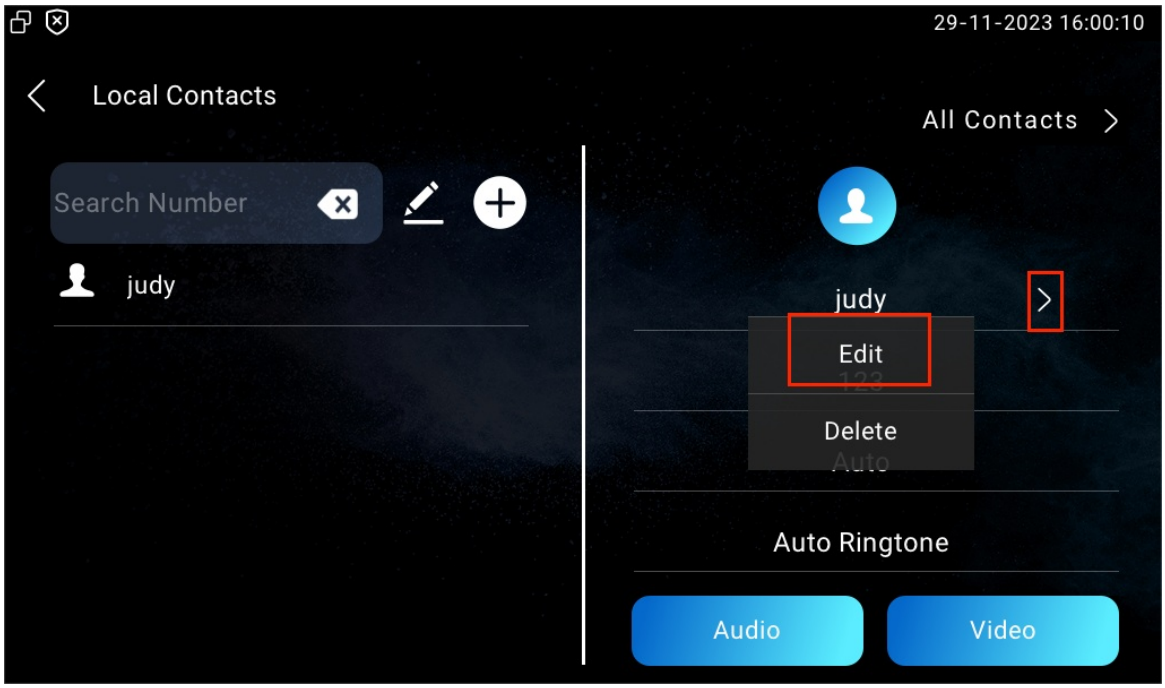
Go to **Contacts > Local Contacts** screen and press the **Add** icon to add a contact.





Edit Contacts

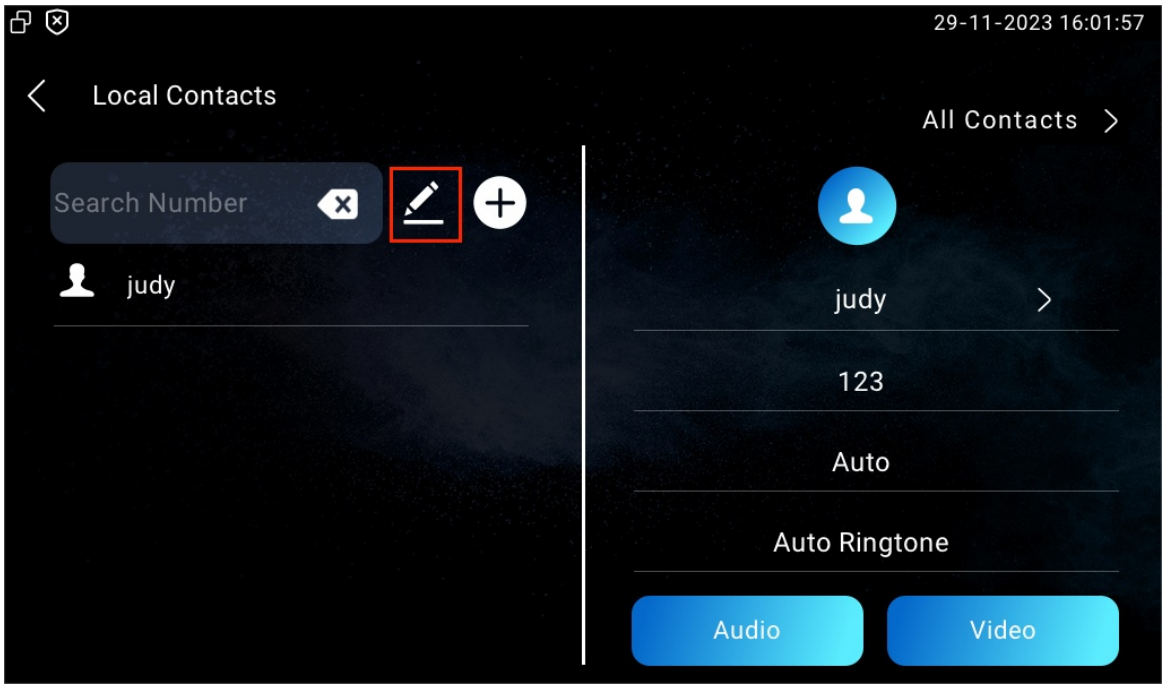
You can check and edit the existing contacts in the contact list. Choose one and click **Edit** to modify.

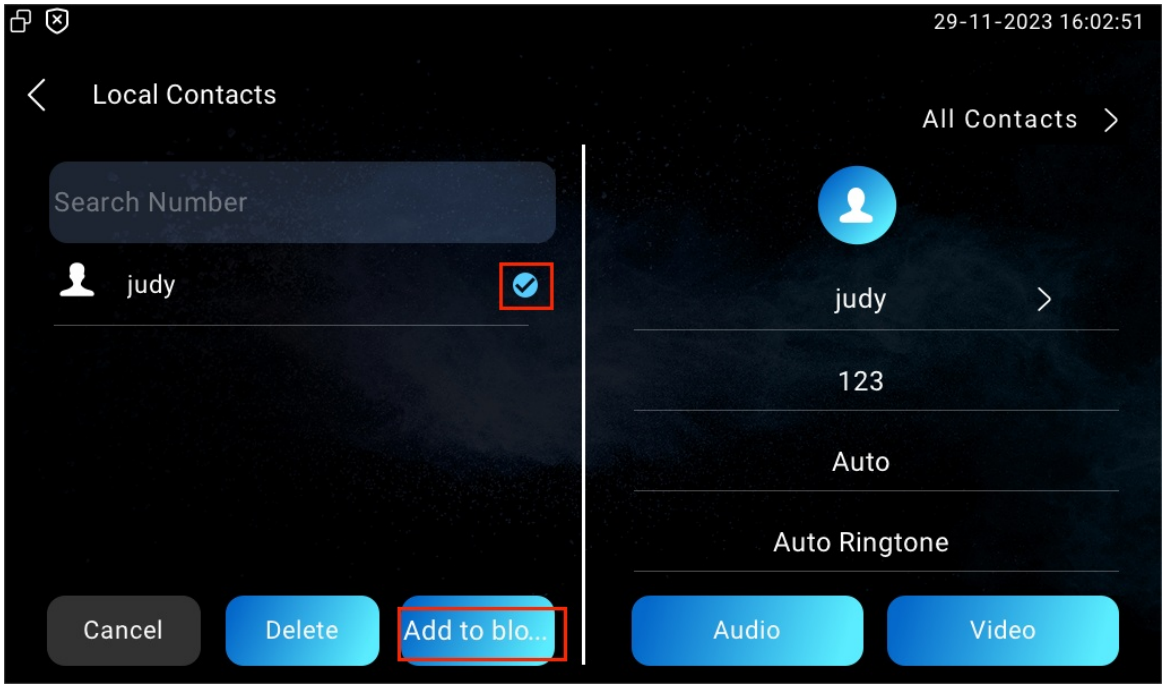


Block List Setting on the Device

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

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





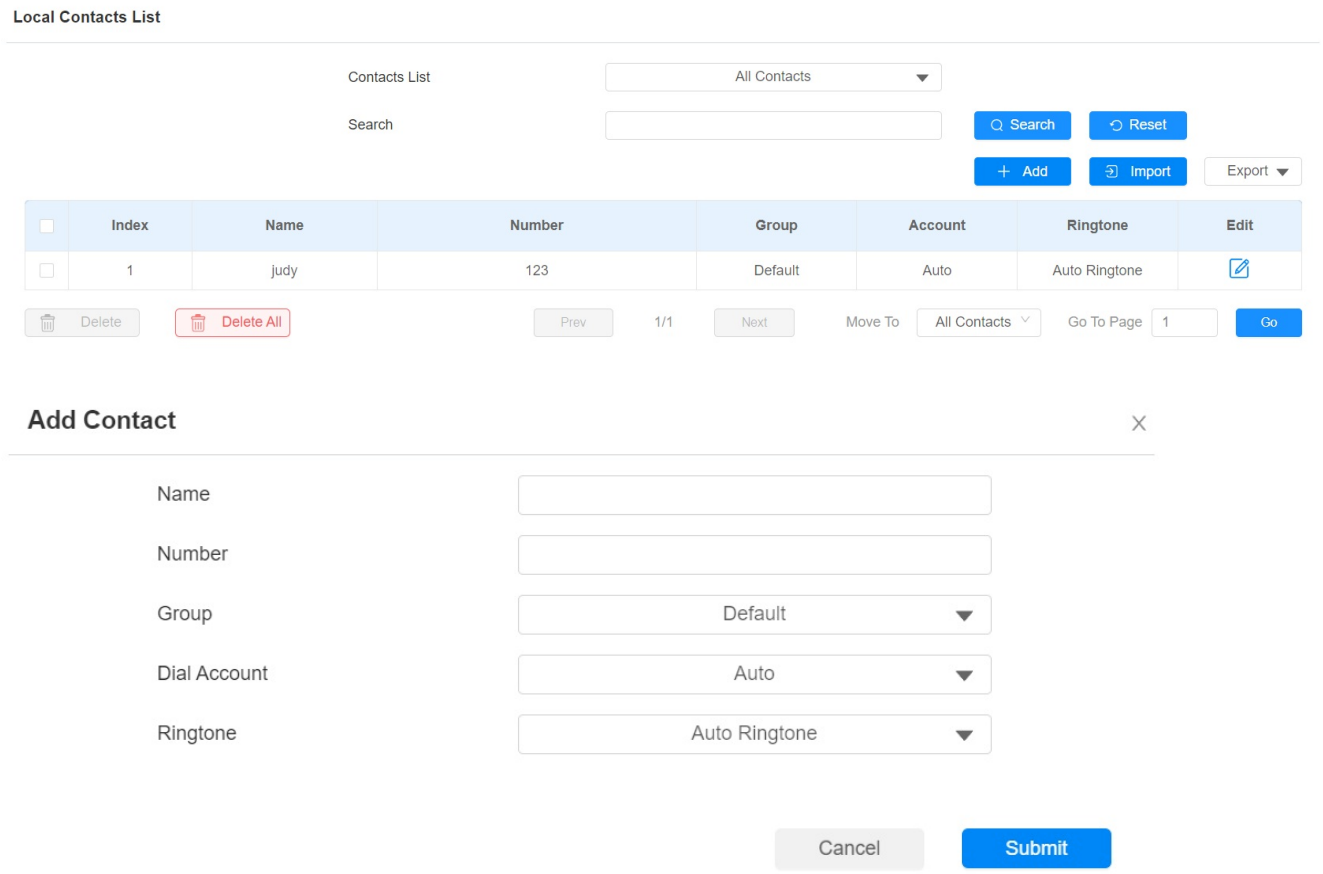
Note

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

Contacts Configuration on the Web Interface

Add Local Contacts

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



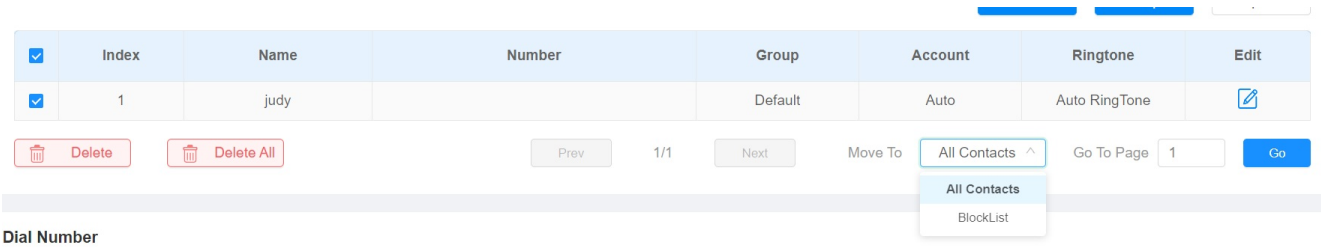
Parameter Set-up:

- **Contact List**: **All Contacts** displays all the contacts in the contact list. **BlockList** displays the contacts in the blocklist.
- **Search**: contact name or contact number used to search a contact.
- **Name**: the contact's name to distinguish it from others.
- **Number**: the SIP or IP number of the contact.
- **Group**: calls from contacts in **BlockList** will be rejected.
- **Dial Account**: the account to make the call, Account 1 or Account 2. When Auto is selected, calls will be made by Account 1 automatically when both accounts are registered.
- **Ringtone**: the ringtone for the incoming call from the contact.

Block List Setting on the Web Interface

You can set the blocklist directly in the contact list on the web interface or set it when editing a contact.

To set it up on **Contacts > Local Contacts > Local Contacts List** interface.

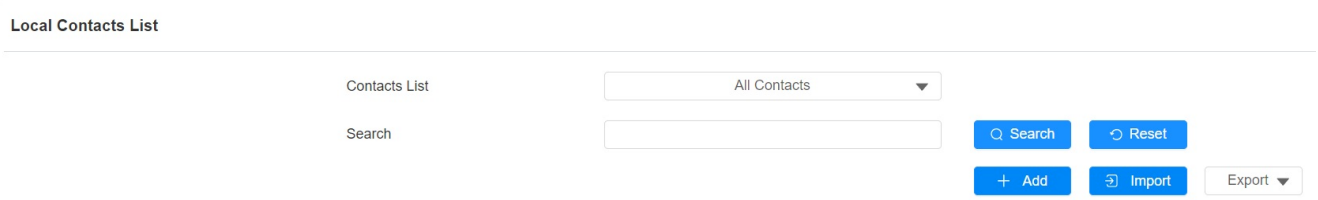


Note

- 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.

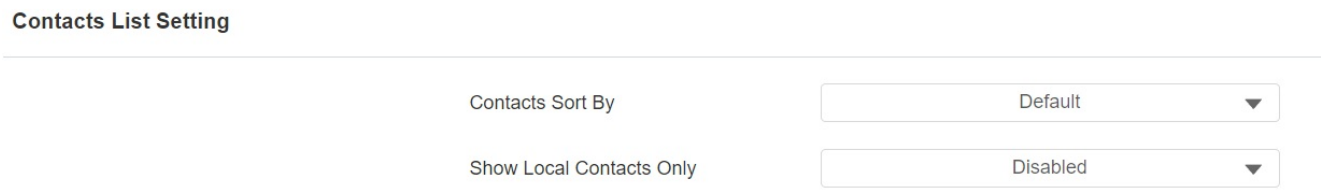
Import and Export Contacts

You can import and export contacts in batch. The file should be in .xml or .csv format. To do so, go to **Contacts > Local Contacts > Local Contacts List** interface.



Contact List Display Configuration

To conduct contact display on web **Contacts > Local Contacts > Contacts List Setting** interface.



Parameter Set-up:

- **Contacts Sort By**: **Default** means the local contacts will be displayed before the contacts from SmartPlus and SDMC, etc. **ASCII Code** means the contacts will be

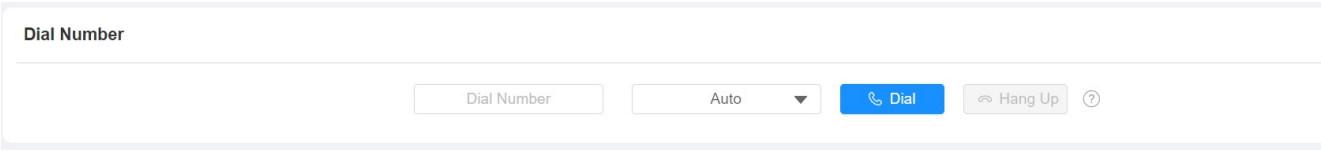
displayed in the order based on the first letter of the contact names. **Created Time** means the contacts will be displayed by their created time.

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

Web Call

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

You can dial out a number using the contact phone number on the web **Contacts > Local Contacts** interface.



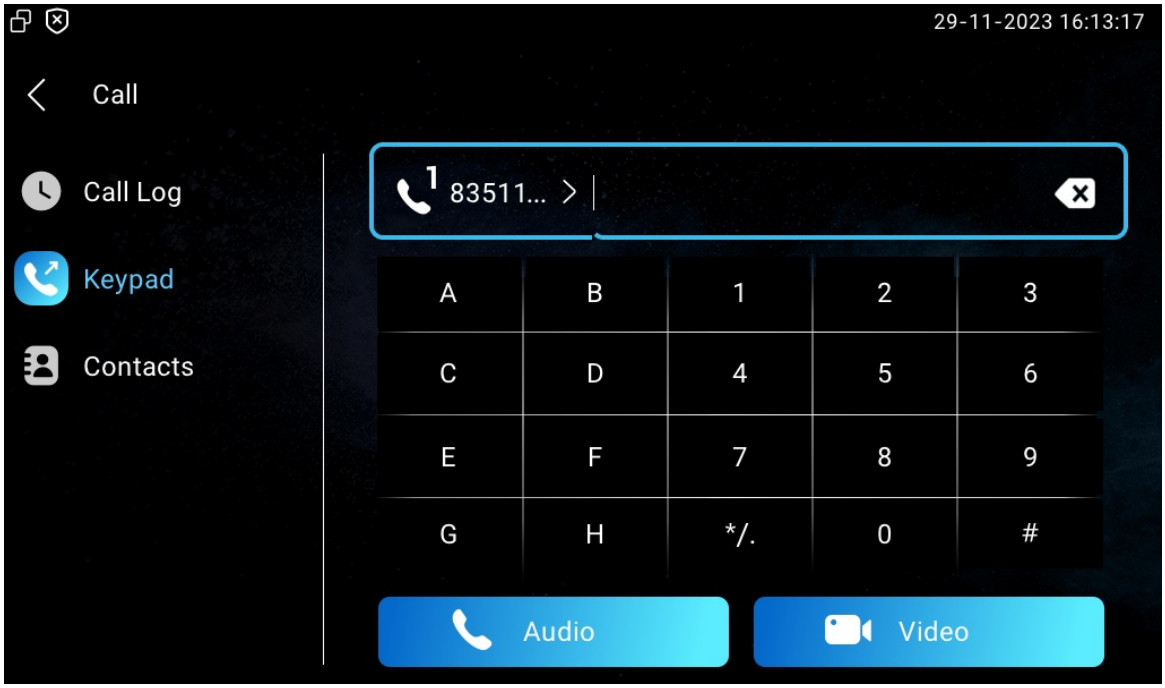
Intercom Call Configuration

IP Call & IP Call Configuration

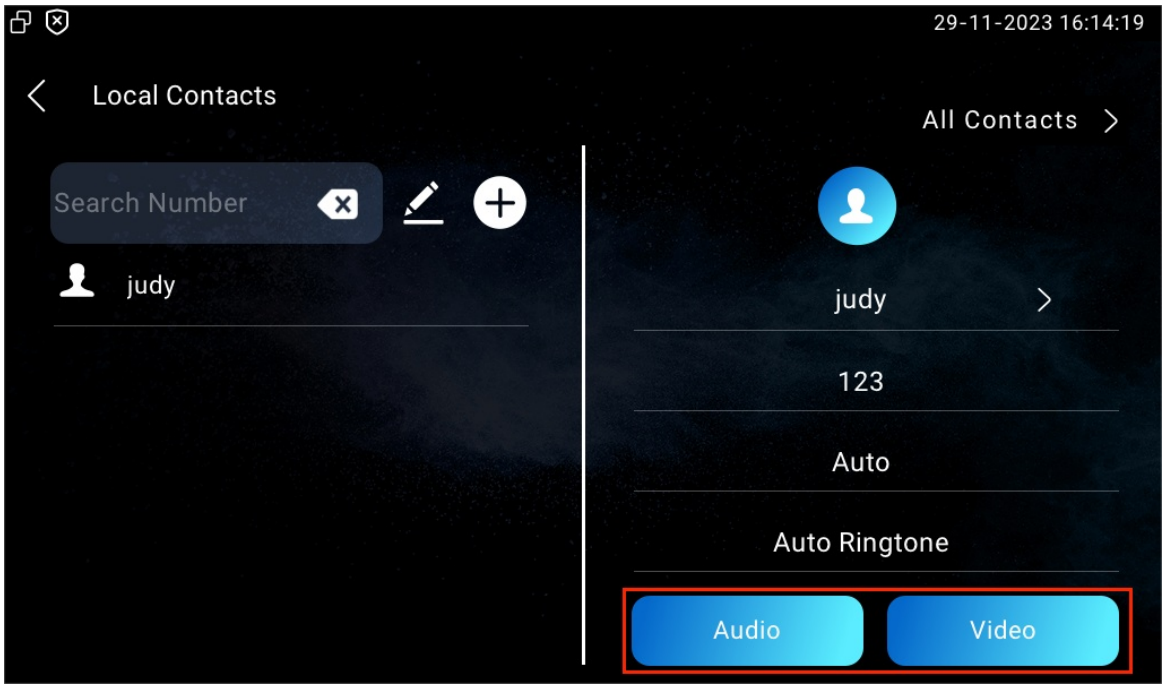
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Make IP Calls

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

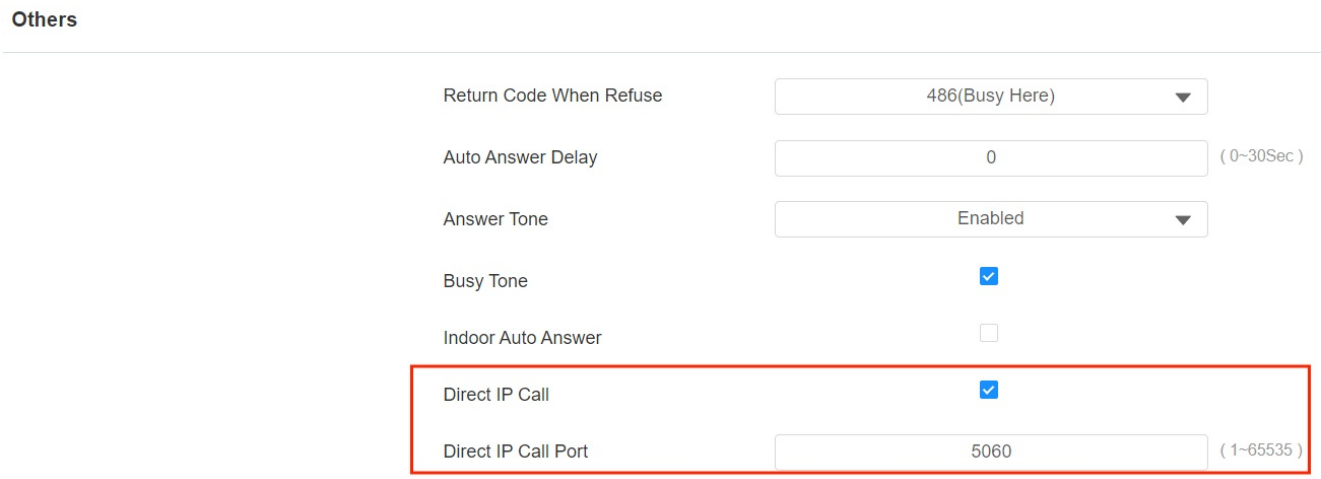


In addition, you can also make IP calls on the **Contacts > Local Contacts** screen.



IP Call Configuration

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



Parameter Set-up:

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

SIP Call & SIP Call Configuration

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

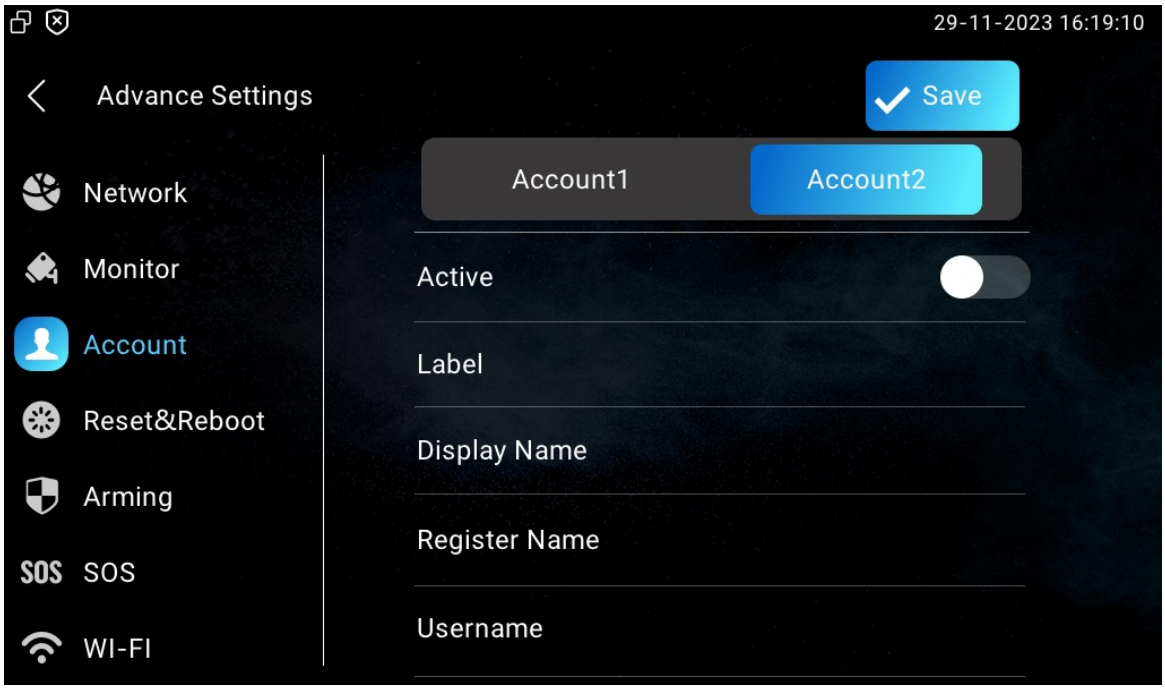
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

SIP Account Registration

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

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

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

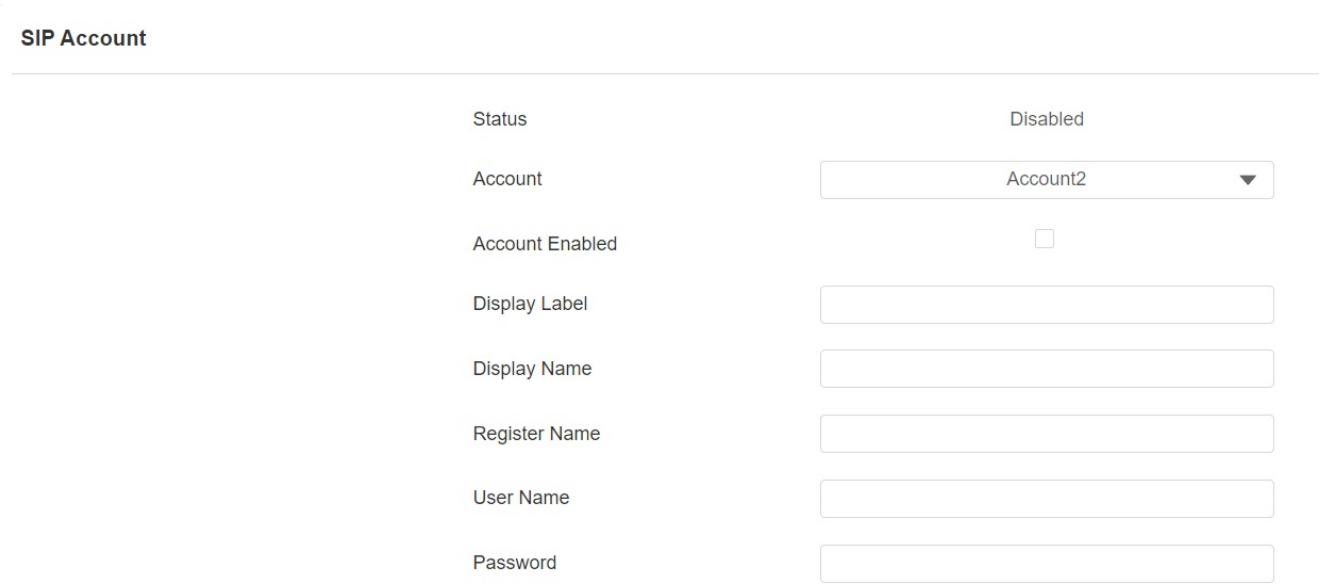


Parameter Set-up:

- **Account1/Account2**: select Account1 or Account2. Account 1 is the default SIP account.
- **Active**: check to activate the registered SIP account.
- **Label**: the device label to be shown on the device screen.
- **Display Name**: the device's name to be shown on the device being called to.

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

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



Parameter Set-up:

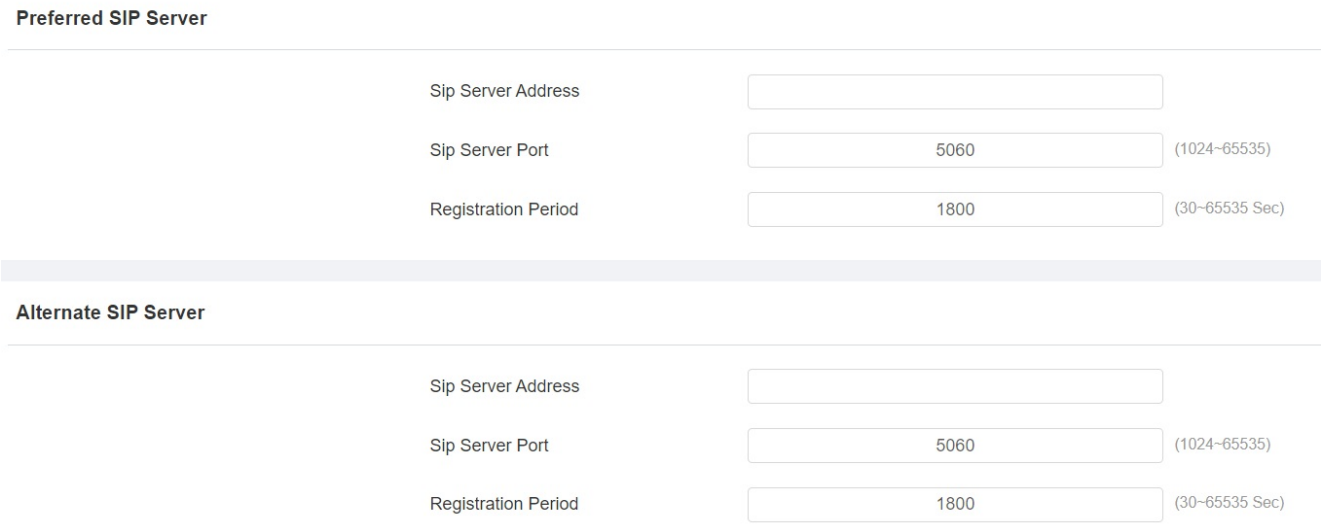
- **Status**: displays whether the SIP account is registered or not.
- **Account**: select Account1 or Account2.
- **Account Enabled**: check to activate the registered SIP account.
- **Display Label**: the device label to be shown on the device screen.
- **Display Name**: the device's name to be shown on the device being called to.

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

SIP Server Configuration

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

To configure it on the device **Settings > Advance Settings > Account** screen or navigate to the web **Account > Basic > SIP Account** interface.



Parameter Set-up:

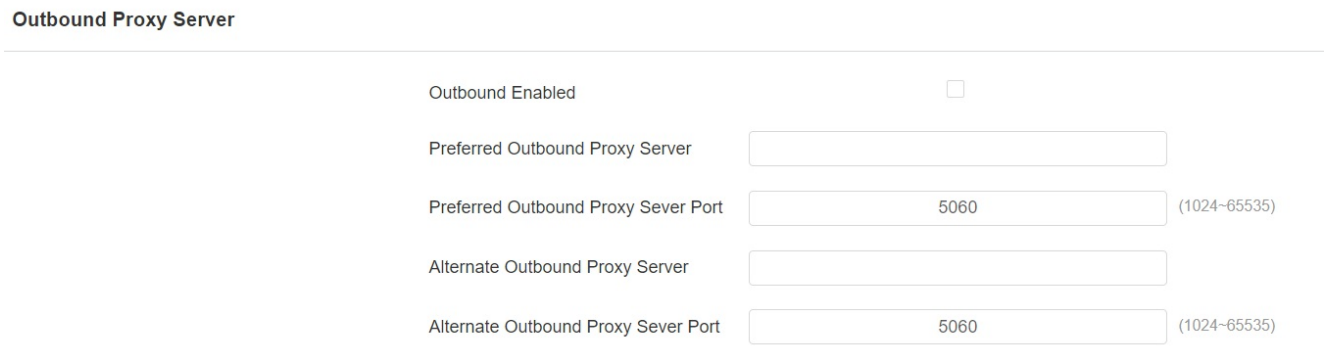
- **Server Address**: the server's IP address or its URL.
- **SIP Server Port**: the SIP server port for data transmission.
- **Registration Period**: the SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The registration period ranges from **120-65535** sec with **1800** by default.

a. To register SIP account for Akuvox indoor monitors, obtain **Server Address** and **Port** from Akuvox indoor monitor PBX screen.
b. To register SIP account for third-party devices, obtain **Server Address** and **Port** from from third-party service provider.

Outbound Proxy Server Configuration

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

Navigate to **Account > Basic** interface.



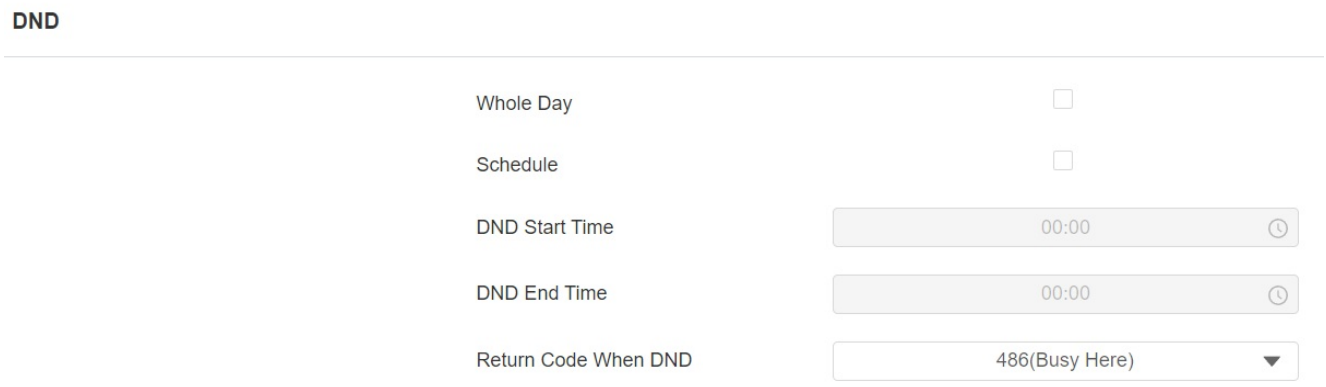
Parameter Set-up:

- **Preferred Outbound Proxy Server**: the IP address of the outbound proxy server.
- **Preferred Outbound Proxy Server Port**: the port number to establish call session via the outbound proxy server.
- **Alternate Outbound Proxy Server**: the IP address for the backup outbound proxy server.
- **Alternate Outbound Proxy Server Port**: the port number to establish 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.

Go to **Device > Call Feature > DND** interface.

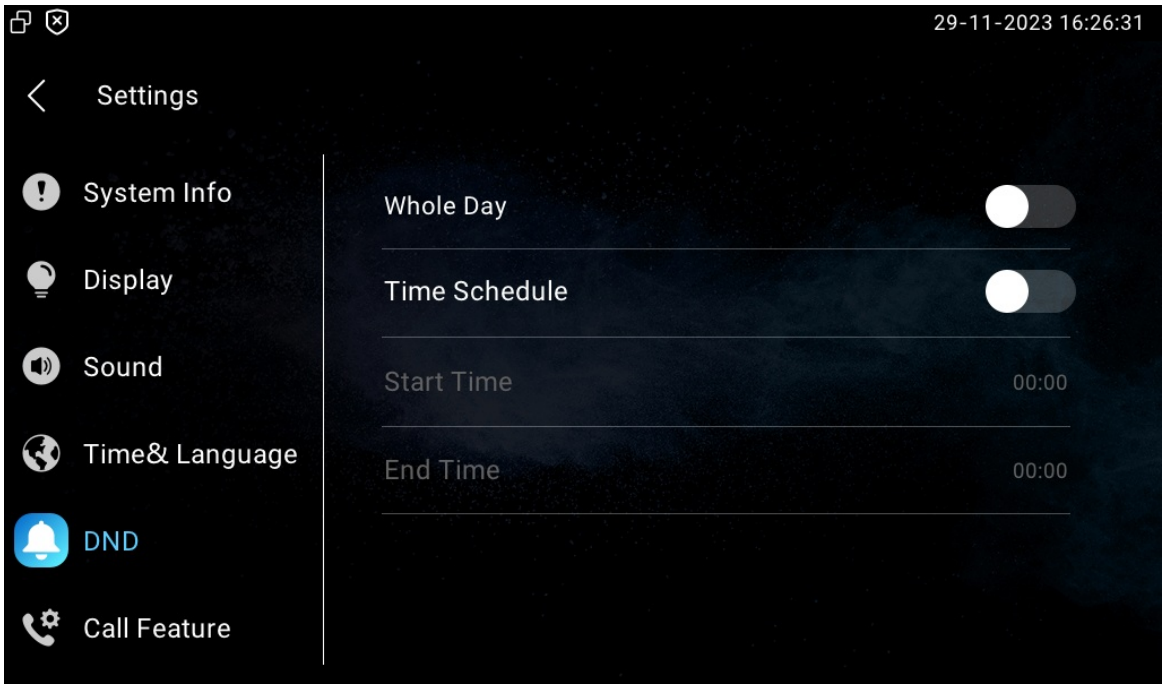


Parameter Set-up:

- **DND**: check **Whole Day** or **Schedule** to enable the DND function. DND function is disabled by default.

- **Return Code When DND**: select what code should be sent to the calling device via SIP server when you reject the incoming calls: **404 for Not Found; 480 for Temporary Unavailable; 486 for Busy Here; 603 for Decline**.

You can also set up DND on the device. Tap **Settings > DND**.

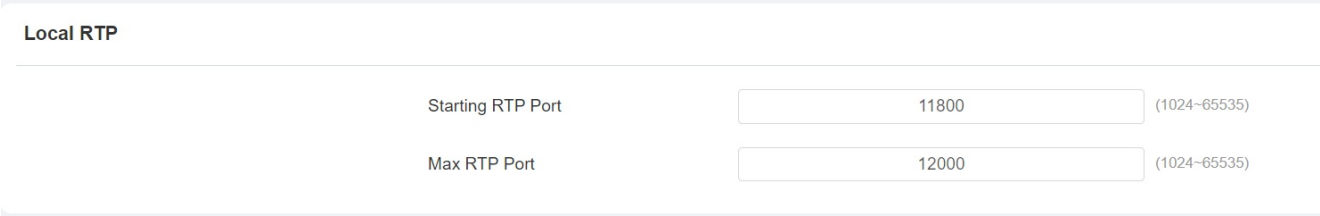


Device Local RTP Configuration

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

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

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



Parameter Set-up:

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

transmission range.

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

Data Transmission Type Configuration

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

To do this configuration on web **Account > Basic > Transport Type** interface.

Parameter Set-up:

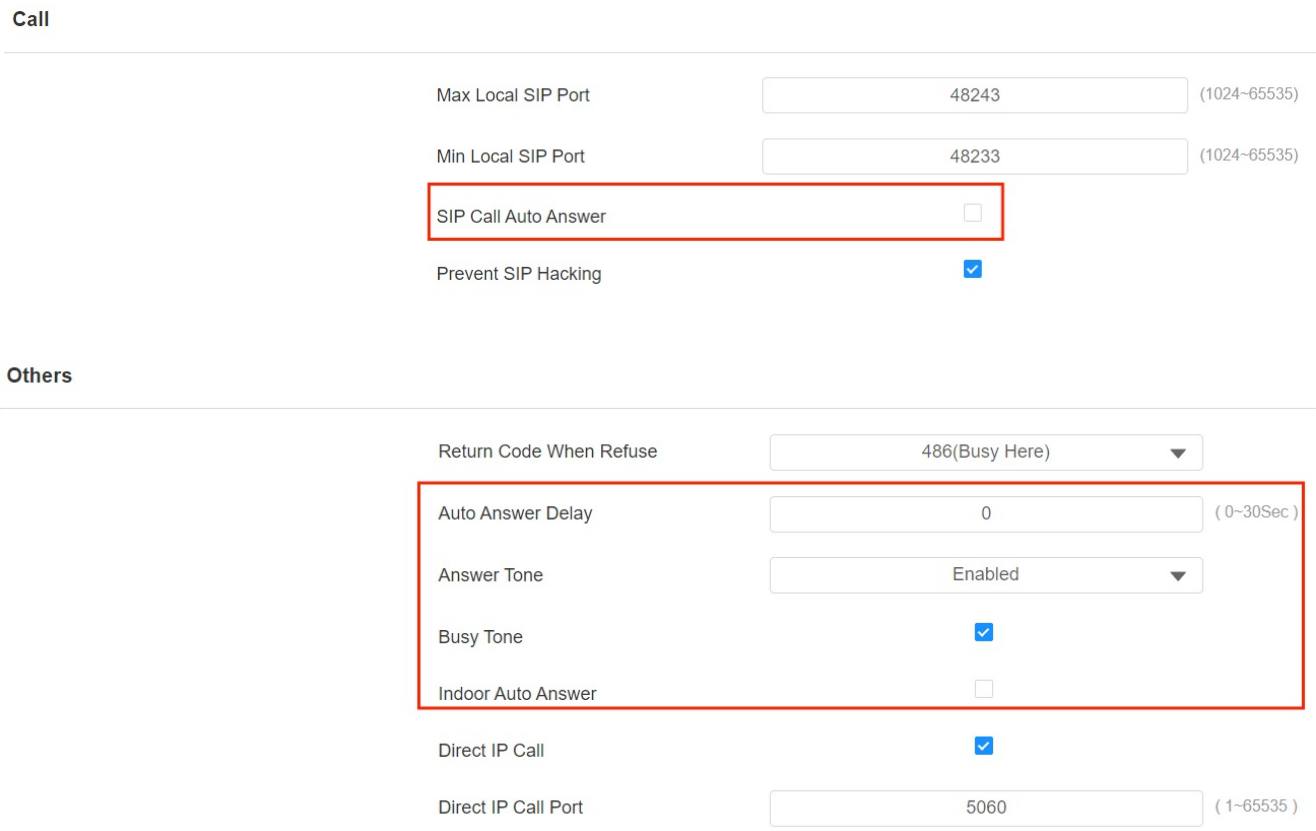
- **UDP**: an unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: a reliable but less-efficient transport layer protocol.
- **TLS**: a secured and reliable transport layer protocol.
- **DNS-SRV**: it is used to obtain a DNS record for specifying the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

Call Setting

Call Auto-answer Configuration

You can define how quickly the device should respond by answering the incoming SIP/IP call automatically by setting up the time-related parameters.

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



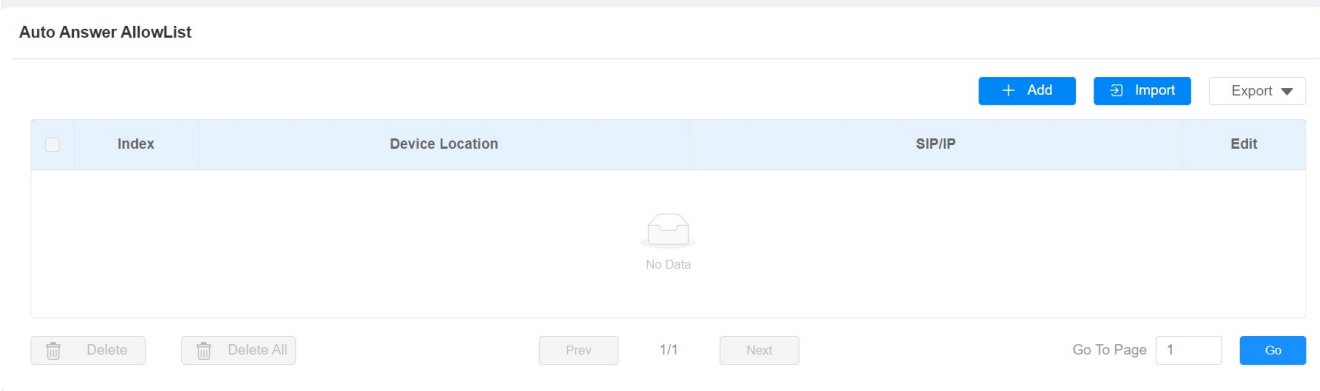
Parameter Set-up:

- **Auto Answer Delay**: the delay time (from 0-30 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Answer Mode**: the video or audio mode for answering the call automatically.
- **Indoor Auto Answer**: allows calls from other indoor monitors to be answered by the device automatically.

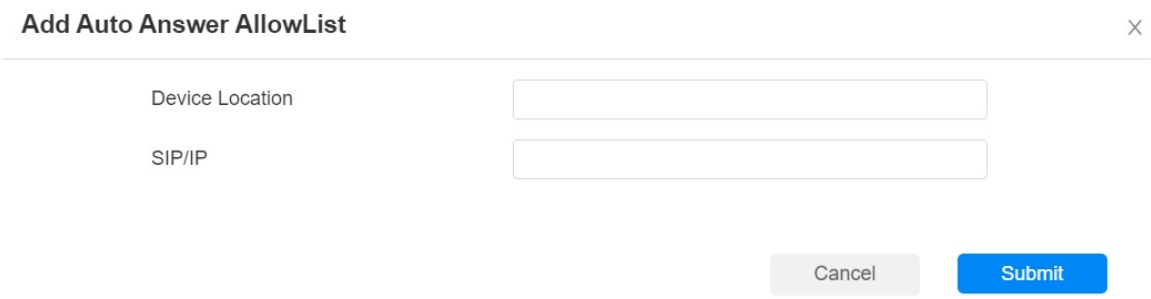
Auto-answer Allow List Setting

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

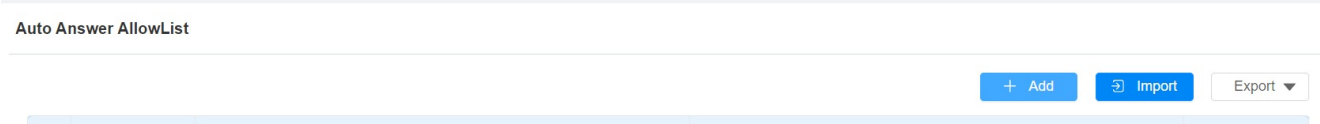
Navigate to the web **Device > Call Feature > Auto Answer AllowList** interface.



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



SIP/IP numbers can be imported to or exported out of the indoor monitor in batch on the web **Device > Call Feature > Auto Answer AllowList** interface.

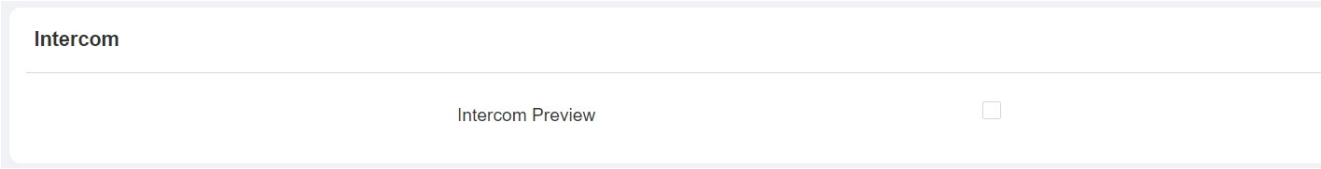


Note

- 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

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



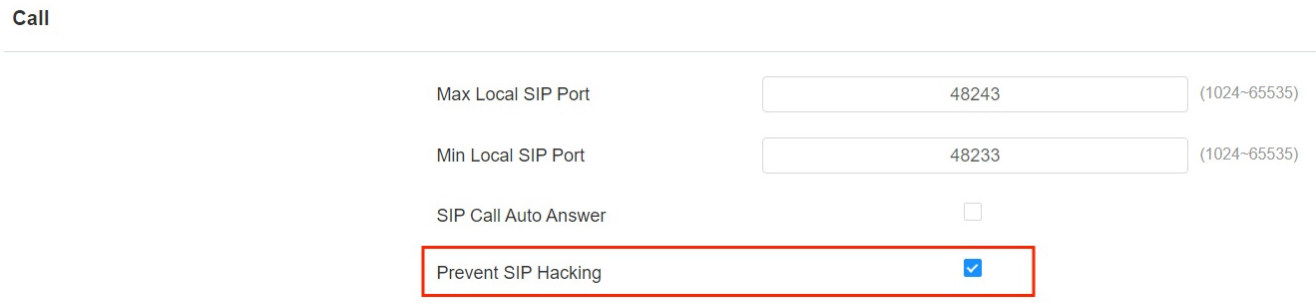
Parameter Set-up:

- **Intercom Preview**: enables the incoming call preview. If it is enabled, the group call is not available.

SIP Hacking Protection

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

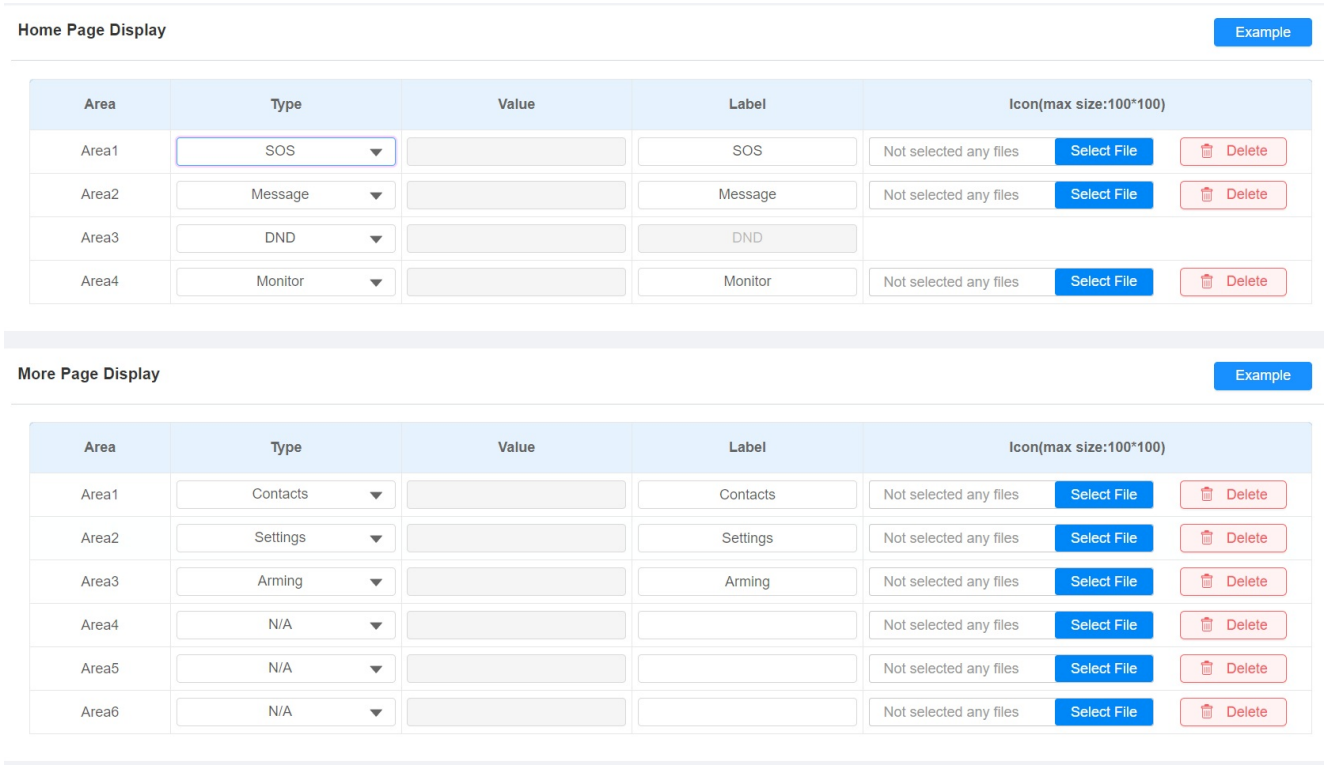
To set it up, go to **Account > Advanced > Call** interface.



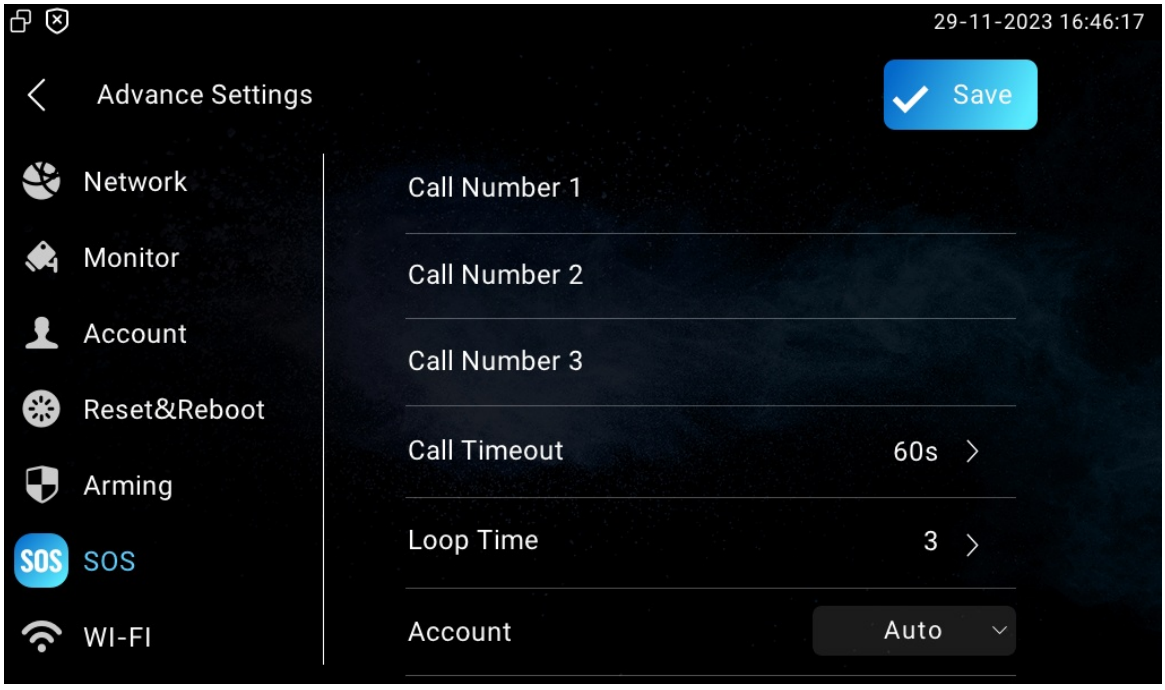
Emergency Call Setting

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

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



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.



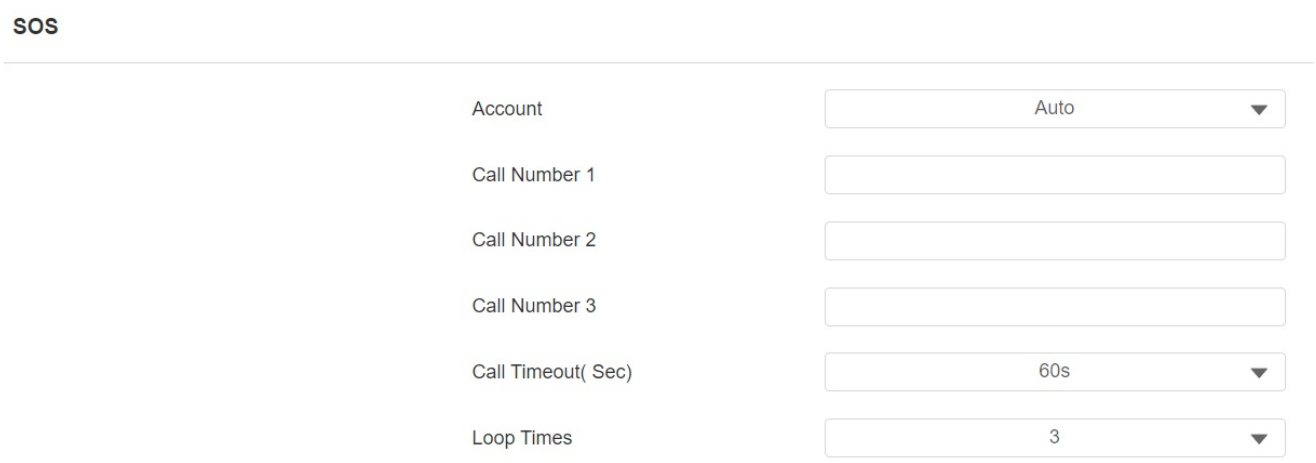
Parameter Set-up:

- **Call Number**: 3 SOS numbers can be set up. Once users press the SOS key on the home

page (the SOS display key shall be set on the web manually), 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 Time**: set up the call loop times.
- **Account**: the account to make SOS calls.

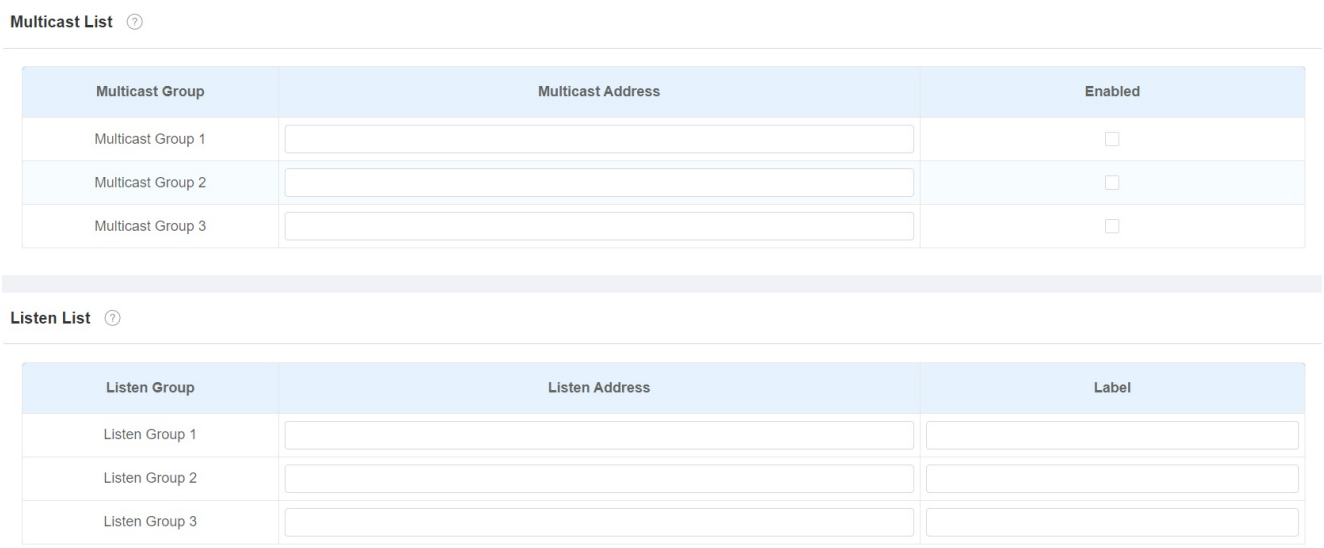
To set it up on the web interface, go to **Device > Intercom > SOS** interface.



Multicast Configuration

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

To configure it on the web **Device > Multicast** interface.



Parameter Set-up:

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

Note

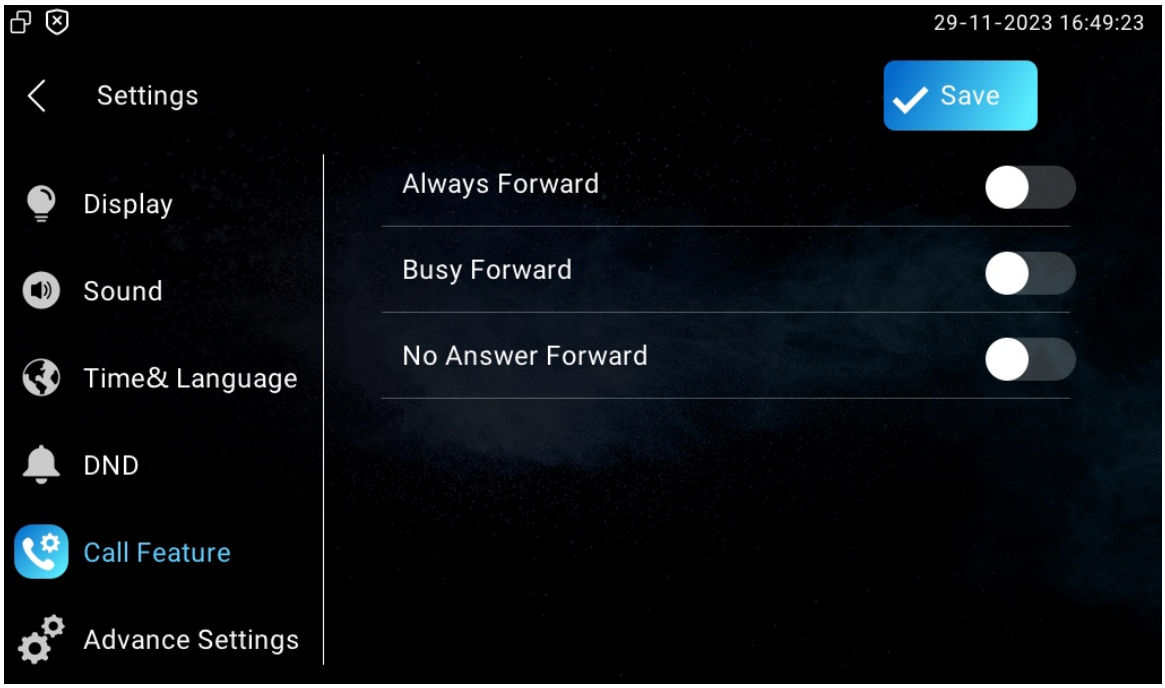
- The multicast address entered should be within the specific range and not all multicast IP addresses are valid. Please consult the Akuvox tech team for more information.

Call Forwarding Setting

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

Call Forwarding Configuration on the Device

To do the configuration on the Device **Settings > Call Feature** screen.

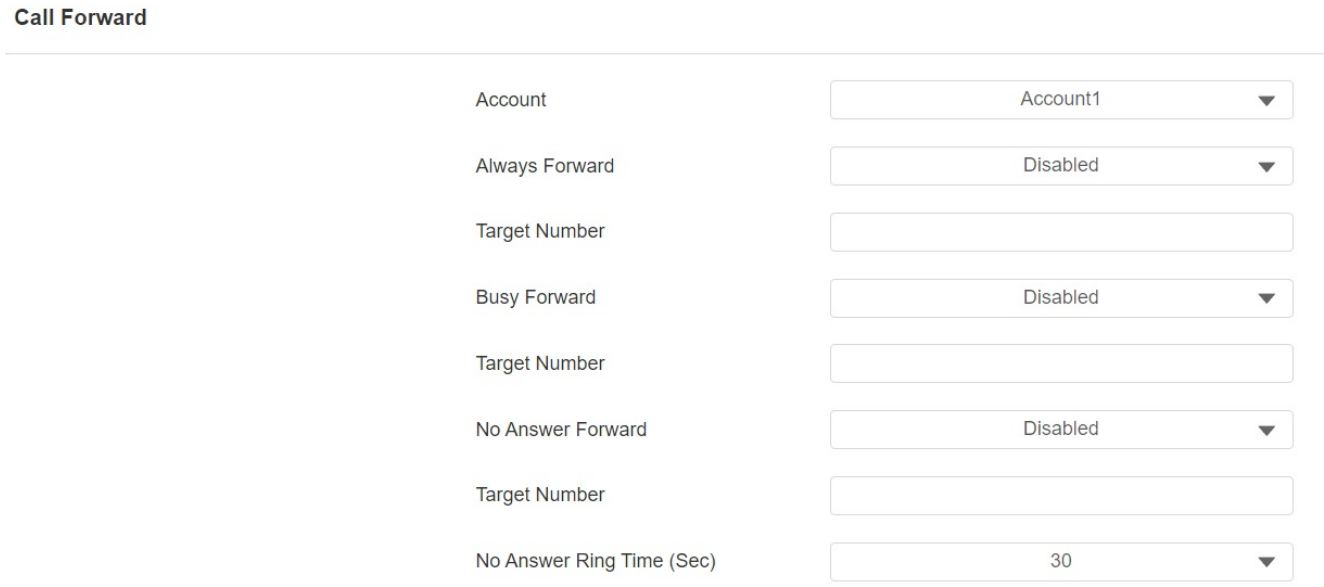


Parameter Set-up:

- **Always Forward**: all incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: incoming calls will be forwarded to a specific number if the device is busy.
- **No Answer Forward**: incoming calls will be forwarded to a specific number if the 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 Forwarding Configuration on the Web Interface

To set up the call forward function on web **Device > Call Feature > Call Forward** interface.



Parameter Set-up:

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

Intercom Message Setting

You can read, create, and delete messages on the **Message** screen.

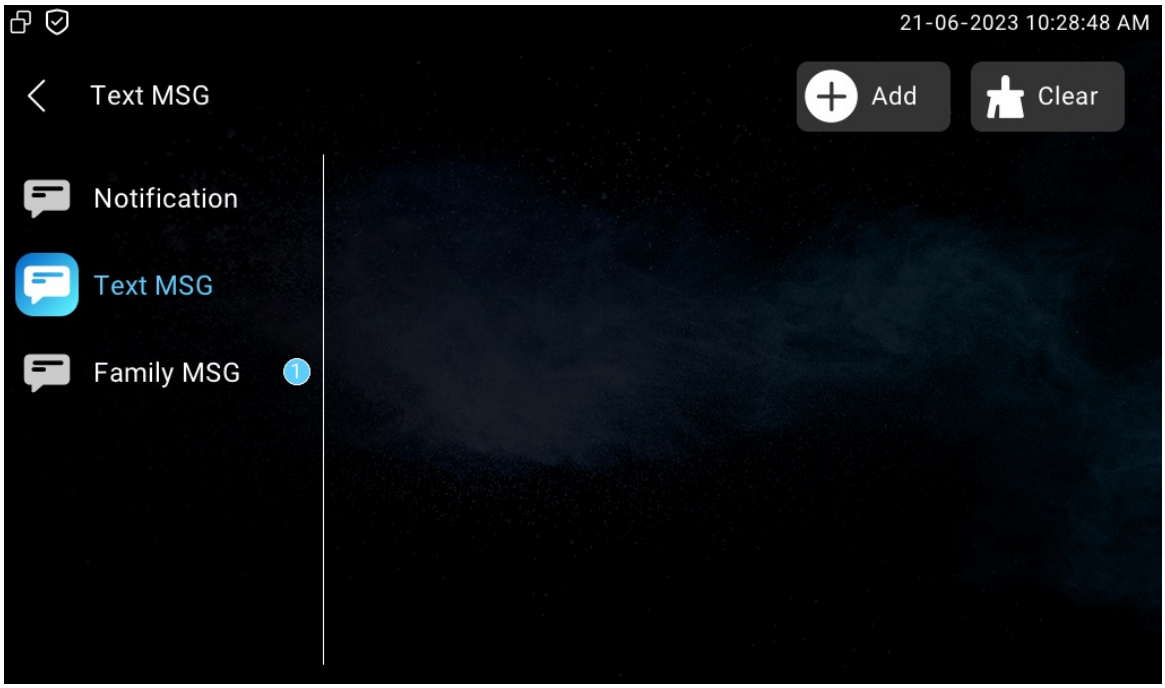
Manage Notification

Messages displayed in Notification are from property managers. This feature is only available when using SDMC or Akuvox SmartPlus.

To configure it, navigate to the **Message > Notification** screen. Press **Clear** to delete the desired notification.

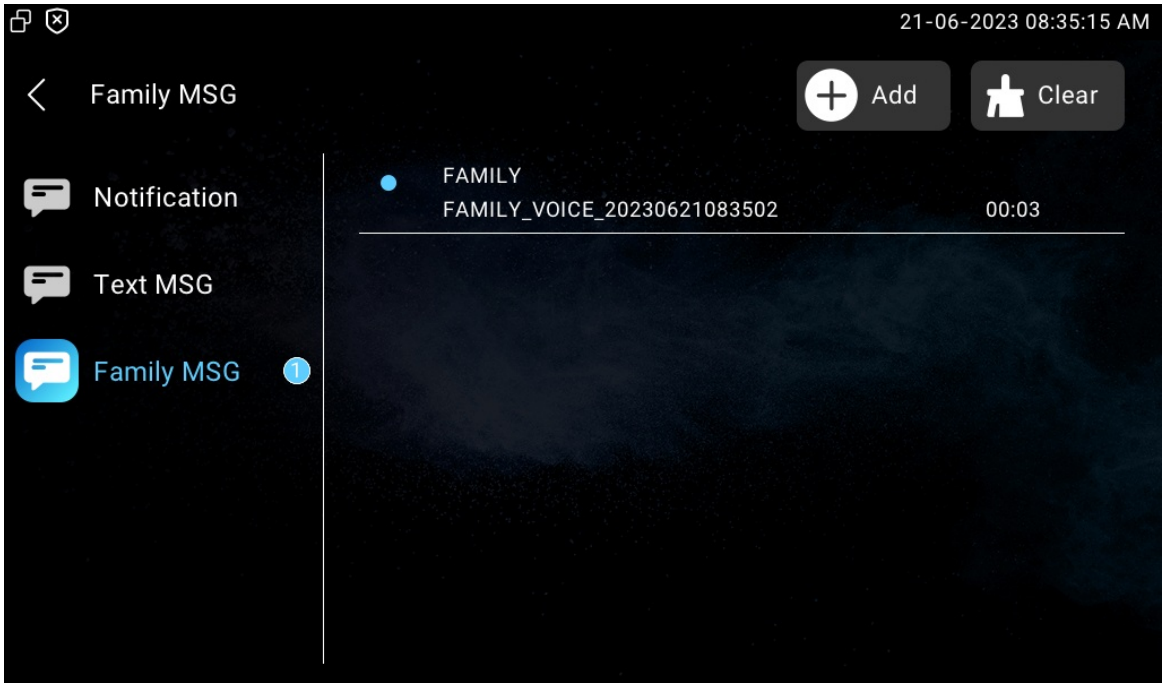
Manage Text Messages

To manage text messages, navigate to **Message > Text MSG** screen. Press **Add** to create a new message and press **Clear** to delete the desired message.



Manage Voice Message

You can create, delete, and view the audio messages of family members recorded on the device screen **Message > Family MSG**. Press **Add** to create a new message and press **Clear** to delete the desired message.

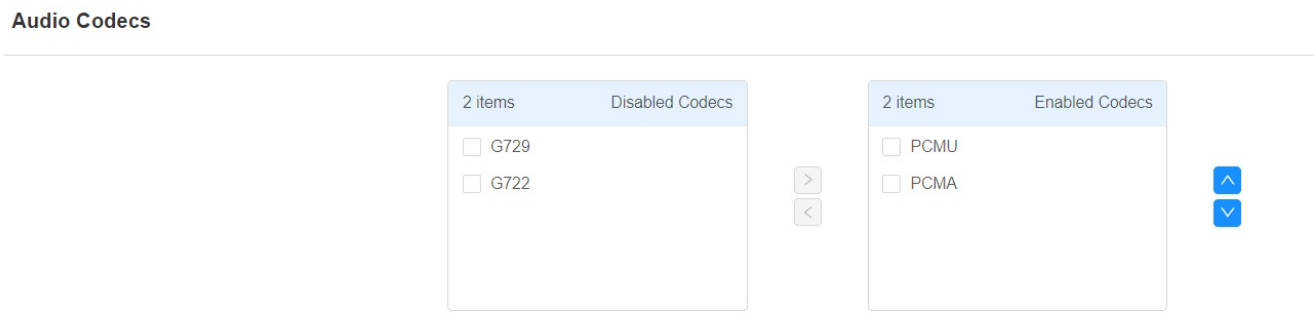


Audio & Video Codec Configuration for SIP Calls

Audio Codec Configuration

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

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



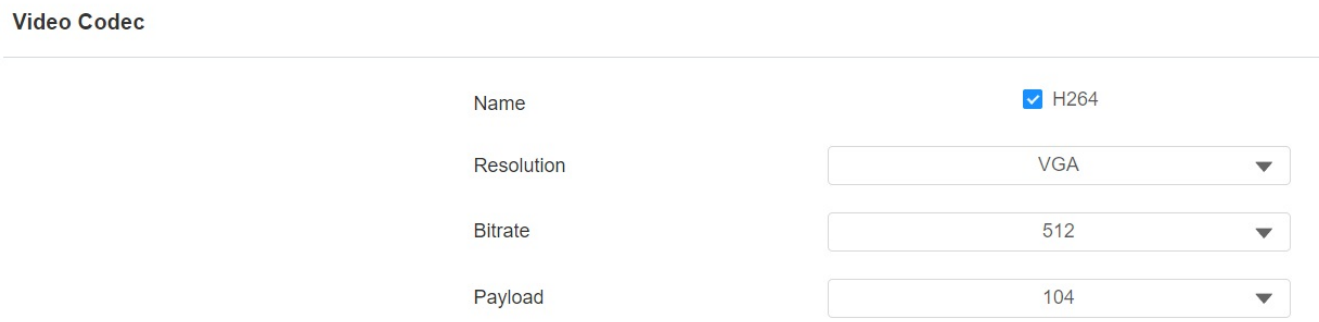
Please refer to the bandwidth consumption and sample rate for the four codec types below:

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

Video Codec Configuration

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

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



Parameter Set-up:

- **Name**: check to select the H264 video codec format for the device video stream. H264 is the video codec by default.
- **Resolution**: the code resolution for the video quality has five options: **QCIF, CIF, VGA, 4CIF**, and **720P**. The default code resolution is **VGA**. Select the resolution according to the network environment.
- **Bitrate**: the video stream bit rate ranges from 128-2048. The greater the bitrate, the more data transmitted every second. Therefore, the video will be clearer. The default code bitrate is **512**.
- **Payload**: the payload ranges from 96-127 for the audio/video configuration file.

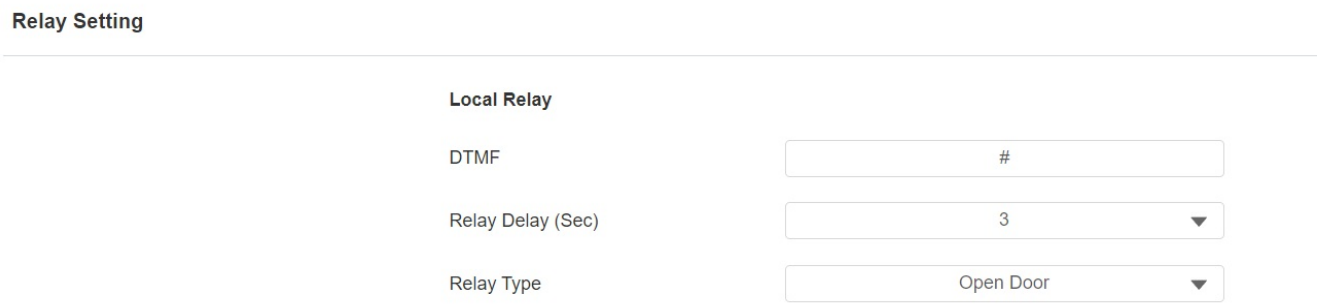
Access Control Configuration

Relay Switch Setting

Local Relay Setting

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

To set it up on the web **Device > Relay > Relay Setting** interface.



Parameter Set-up:

- **DTMF**: the DTMF code to trigger the local relay.
- **Relay Delay**: the delay time after the relay is triggered.
- **Relay Type**: relay action type. There are two types of relay, chime bell and open door.
    - **Chime Bell**: when there is a call, the chime bell will ring.
    - **Open Door**: when the unlock icon is pressed, the door will be opened.

Remote Relay Switch Setting

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

Navigate to the web **Device > Relay > Relay Setting > Remote Relay** interface.

Remote Relay	
DTMF	#
DTMF1Code	#
DTMF2Code	#
DTMF3Code	#

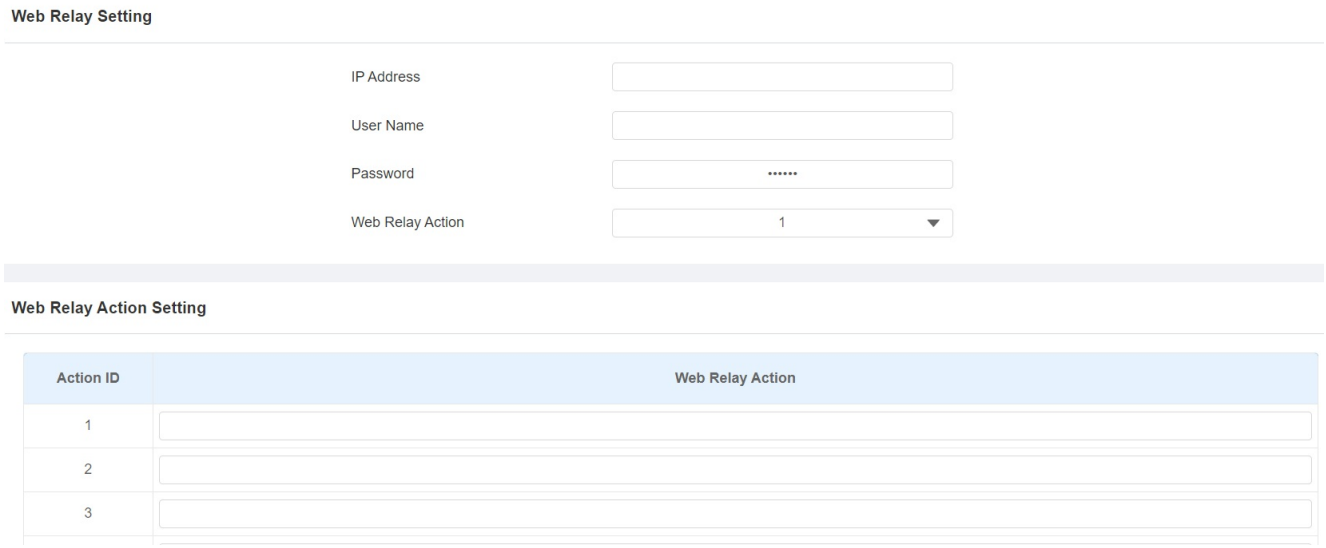
Parameter Set-up:

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

Web Relay Setting

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

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



Parameter Set-up:

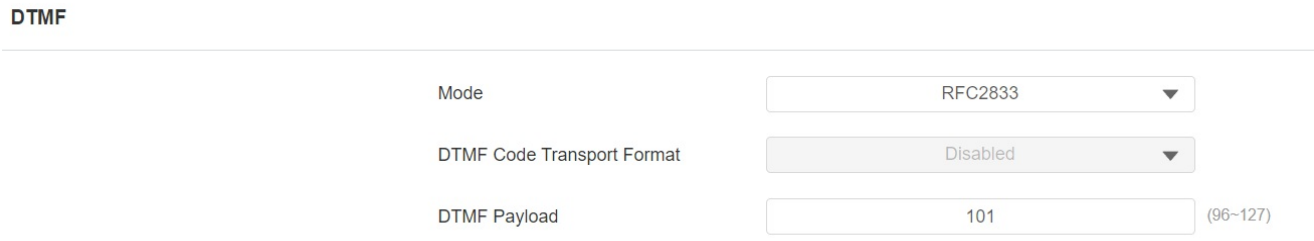
- **Password**: the passwords are authenticated via HTTP and you can define the passwords using HTTP get in Action.
- **Web Relay Action**: the specific web relay action command provided by the web manufacturer for different actions by the web relay. The example format: **state.xml?relayState=2**.
  -If you have not entered the IP address, username, and password, you need to enter the complete HTTP command in such a format: **http://Username:Password@IP address/state.xml?relayState=2**.

Door Unlock Configuration

Door Unlock by DTMF Code

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

Navigate to **Account > Advanced > DTMF** interface.



- **Type**: there are three options, **RFC2833, Info**, and **Info+RFC2833**.
- **DTMF Code Transport Format**: there are four options, **Disable, DTMF, DTMF-Relay**, and **Telephone-Event**. Configure it only when the third-party device that receives the DTMF code adopts the **Info** transport format. **Info** transfers the DTMF code via signaling while other transport format does it via RTP audio packet transmission. Select the DTMF transferring format according to the third-party device.
- **Payload**: it is for data transmission identification ranging from 96-127.

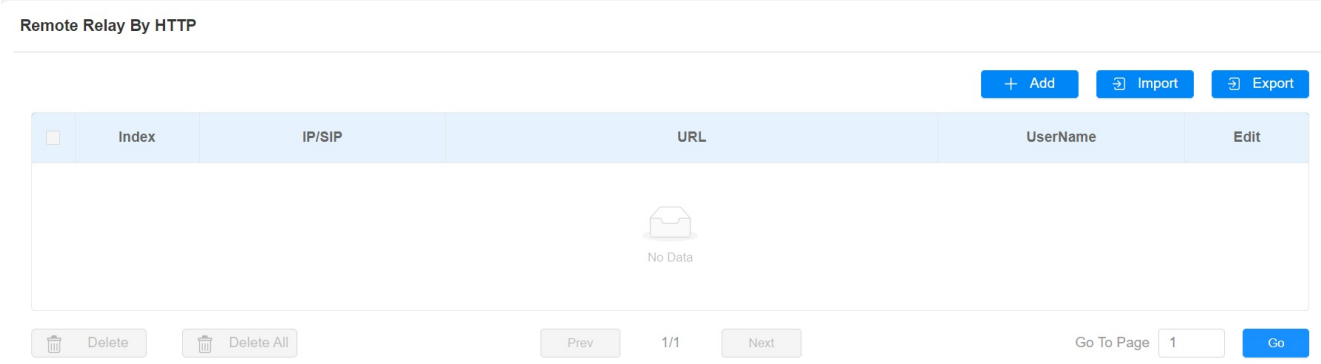
Note

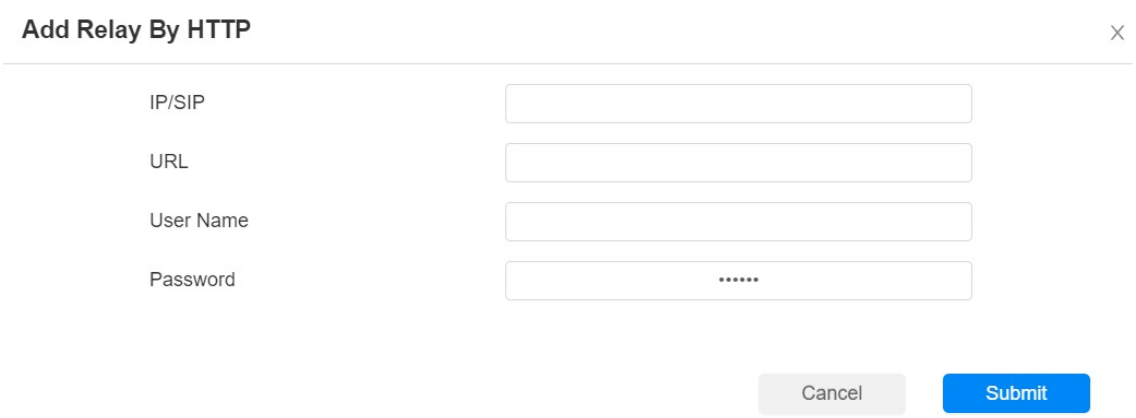
- Please refer to **Relay Switch Setting** for the specific DTMF code setting. Intercom devices involved must be consistent in the DTMF type, otherwise, the DTMF code cannot be applied.

Door Unlock via HTTP Command

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

To do this configuration on web **Device > Relay > Remote Relay by HTTP** interface.





Parameter Set-up:

- **IP/SIP**: the IP address or SIP number of the doorphone.
- **URL**: the HTTP command. Refer to: http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1
- **Username**: customize the username for authentication.
- **Password**: customize the password for authentication.

Note

- DoorNum in the HTTP command above refers to the relay number **#1** to be triggered.
- Devices with high security mode enabled only support new HTTP formats:
  - http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
  - http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1

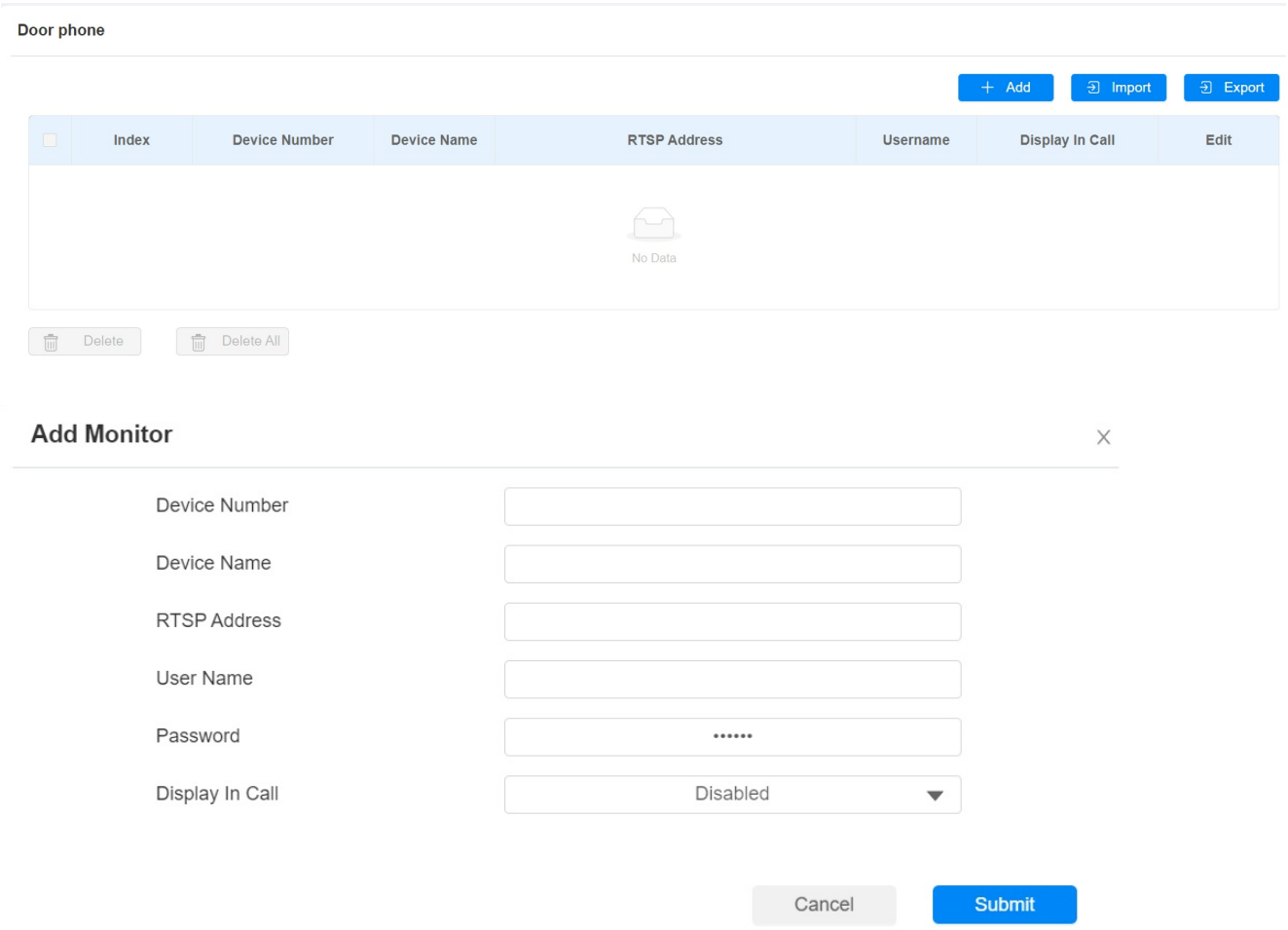
Security

Monitor and Image

Monitor Setting

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

Navigate to **Device > Monitor** interface. Press **+Add** to add a monitor.



Parameter Set-up:

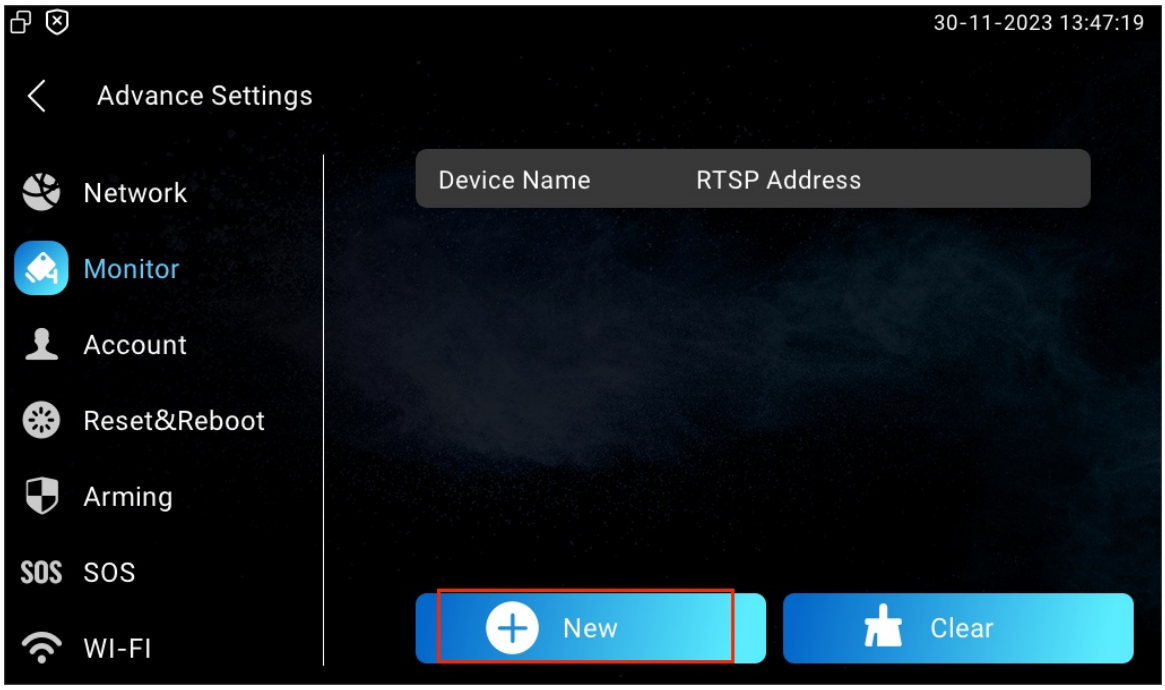
- **Device Number**: the device's SIP/IP number for identification.
- **Device Name**: the device name for identification.
- **RTSP Address**: the RTSP address of the monitoring device. RTSP format: **rtsp://Device IP address/live/ch00_0**.

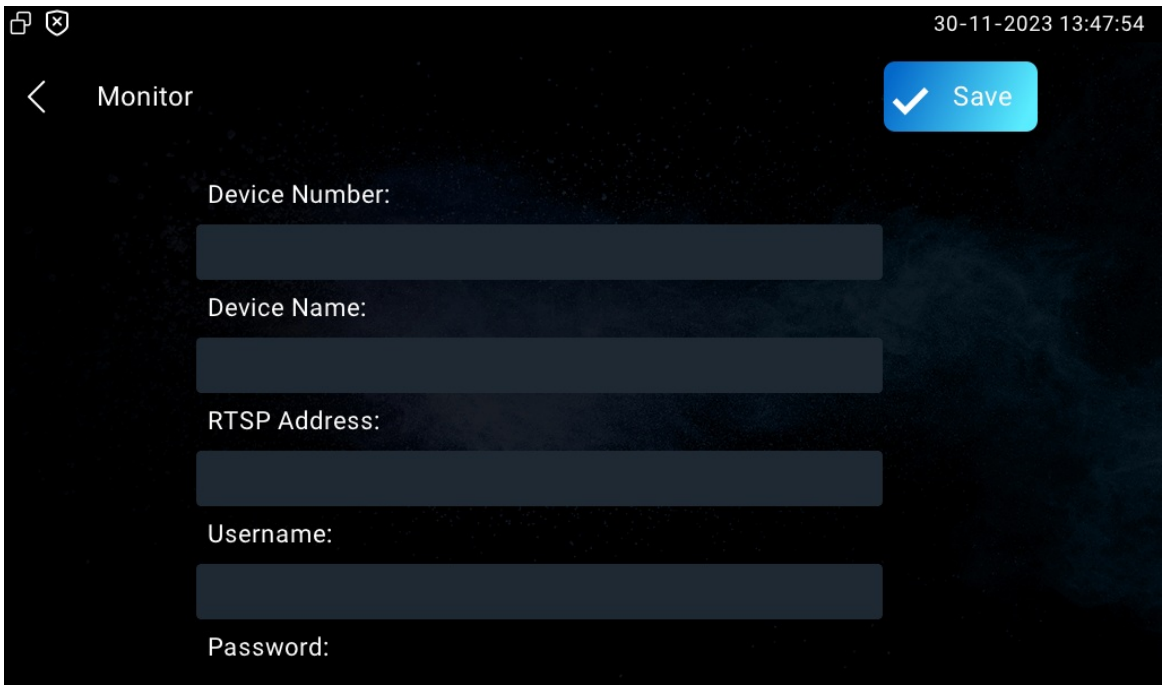
- **Username**: the username of the monitoring device for authentication.
- **Password**: the password of the monitoring device for authentication.
- **Display In Call**: enable it to display the monitoring video during a call.

Note

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

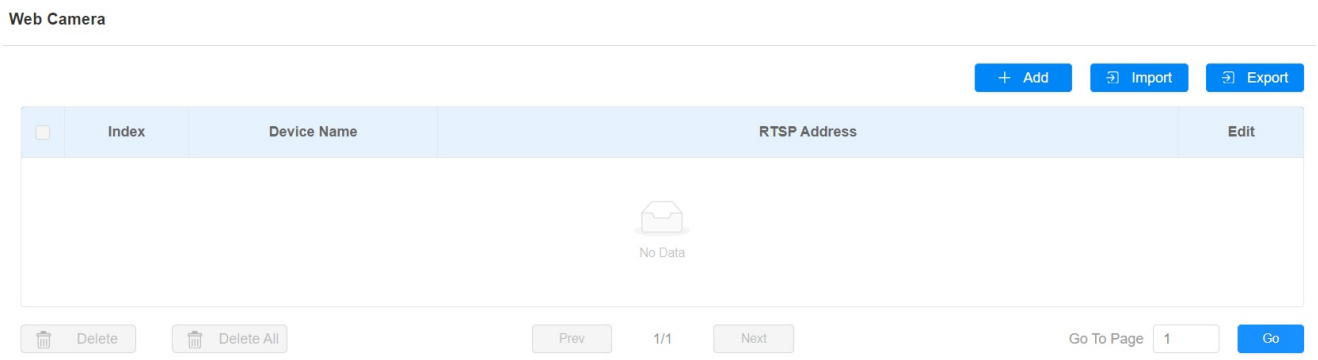
You can also set it up on the device **Settings > Advance Settings > Monitor** screen.





Web Camera Setting

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



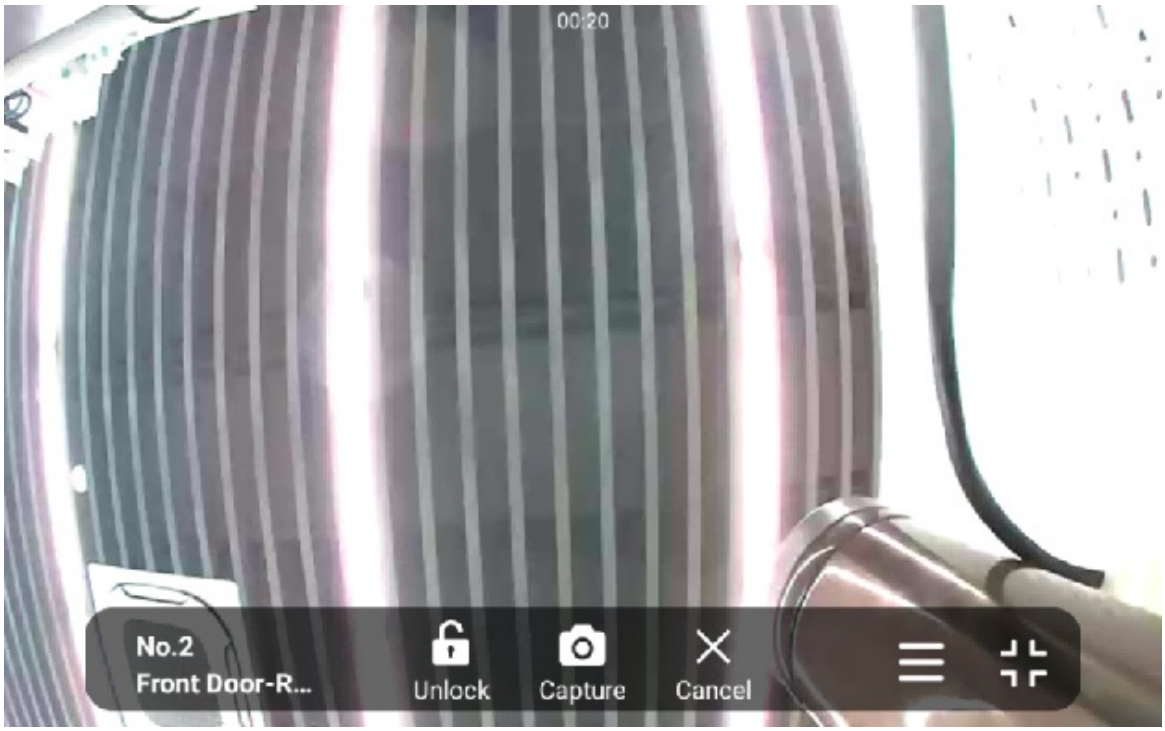
Parameter Set-up:

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

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

Video Image Capturing

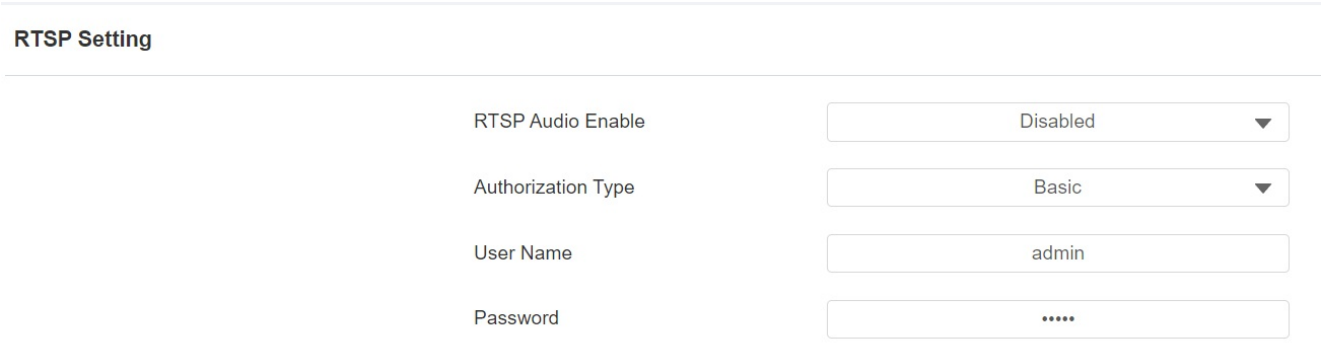
The device lets users take a screenshot during a video call or while using the monitor if they notice anything unusual. To take a screenshot, simply tap the Capture button.



RTSP Authentication

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

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



Parameter Set-up:

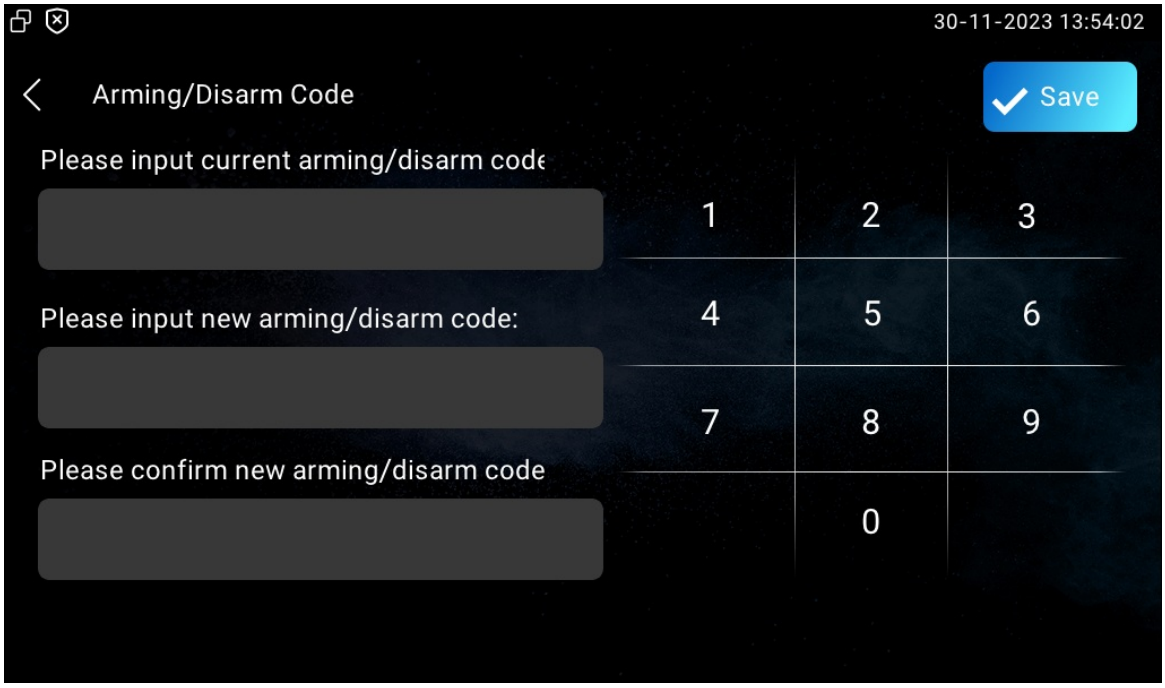
- **Authorization Type**: there are three options, **Basic, Digest** and **None**. **None** will allow all authorization types for the RTSP audio stream.
- **User Name**: the username for the authentication.
- **Password**: the password for the authentication.

Alarm and Arming Configuration

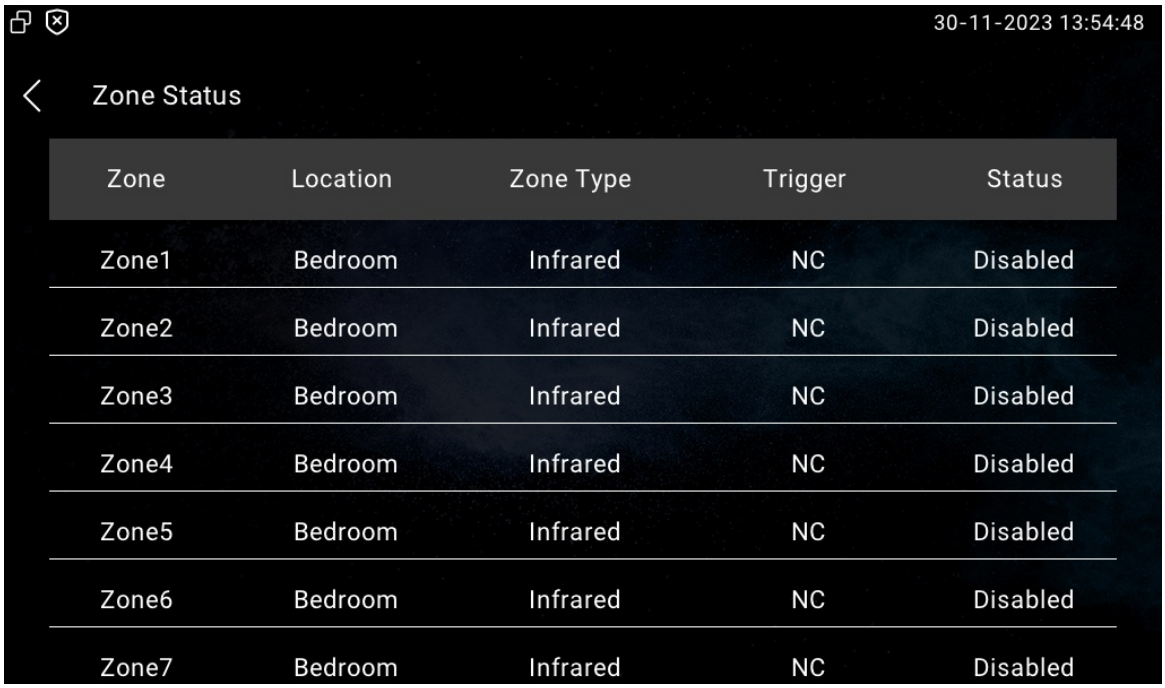
The Arming function is designed to enhance home security by offering three modes with custom zone settings for connected sensors. When armed, the device will sound a siren and notify specific people if a sensor detects something unusual.

Configure Alarm and Arming on the Device

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

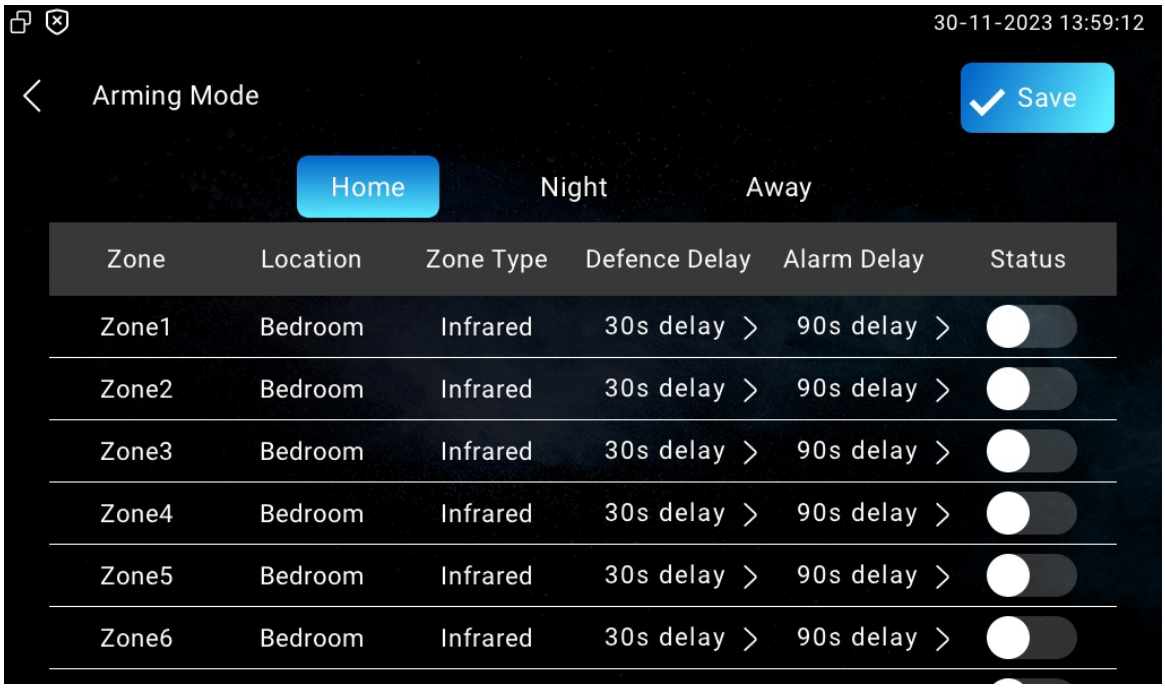


To check the zone status on **Arming > Zone Status** screen.



Configure Location-based Alarm

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



Parameter Set-up:

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

Gas, and **Urgency**.

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

Configure Alarm and Arming on the Web Interface

To set up a location-based alarm sensor on the device web **Arming> Zone Setting** interface.

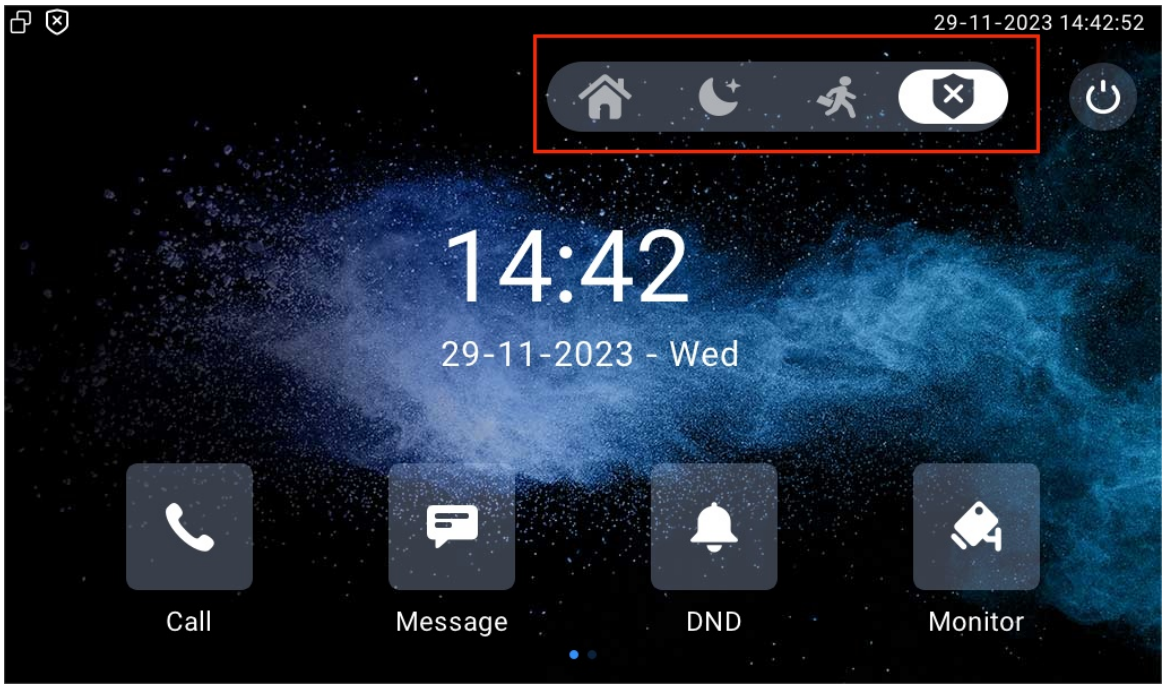
Zone Setting

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

Parameter Set-up:

- **Location**: the location where the alarm sensor is installed. There are ten location types: **Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study**, and **Bathroom**.
- **Zone Type**: the alarm sensor types. There are five sensor types: **Infrared, Drmagnet, Smoke, Gas**, and **Urgency**.
- **Trigger Mode**: set sensor trigger mode between **NC** and **NO** according to your need.
- **Status**: set the alarm sensor status among three options: **Enabled, Disabled**, and **24H**. Select **Enabled** if you want to enable the alarm, however, you are required to set the alarm again after the alarm is disarmed. Select **Disabled** if you want to disable the alarm, and select **24H** if you want the alarm sensor to stay enabled for 24 hours without setting up the alarm manually again after the alarm is disarmed.

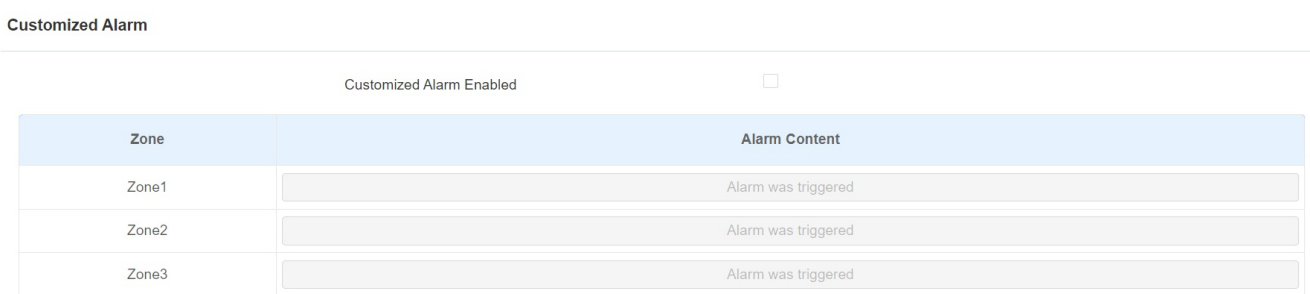
If any of the zones is enabled or set to **24H**, the alarm-related icons will be displayed on the home screen for quick access.



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.

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

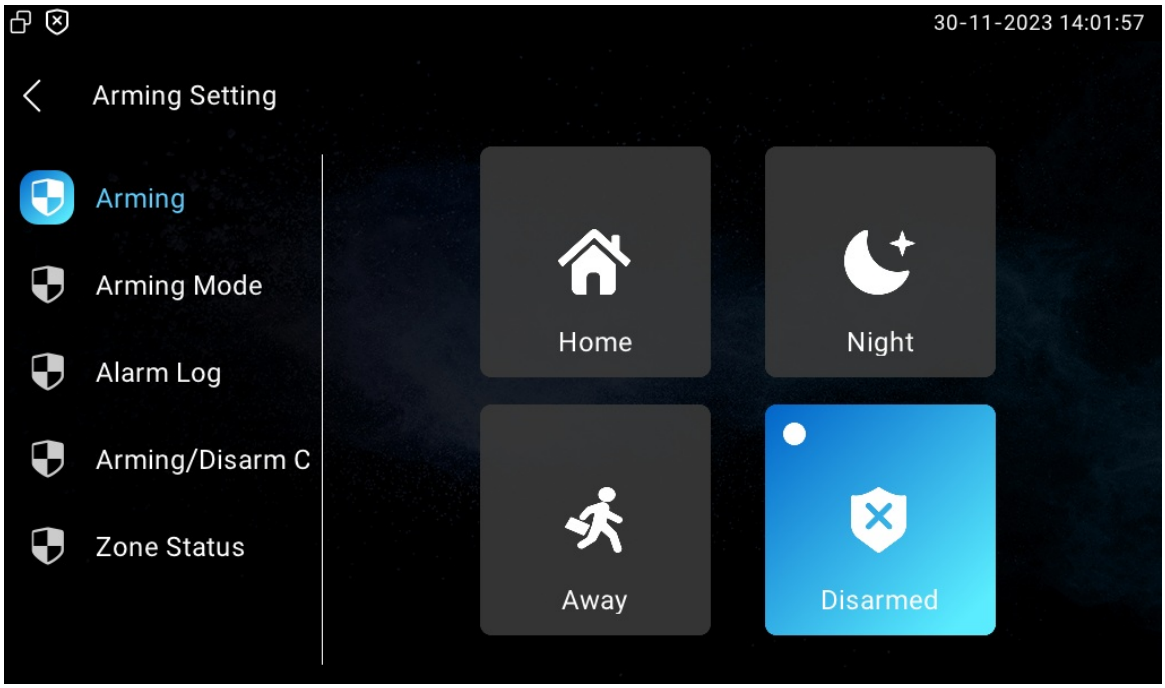


Parameter Set-up:

- **Alarm Context**: the alarm text will display on the device screen when an arming is triggered.

Configure Arming Mode

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



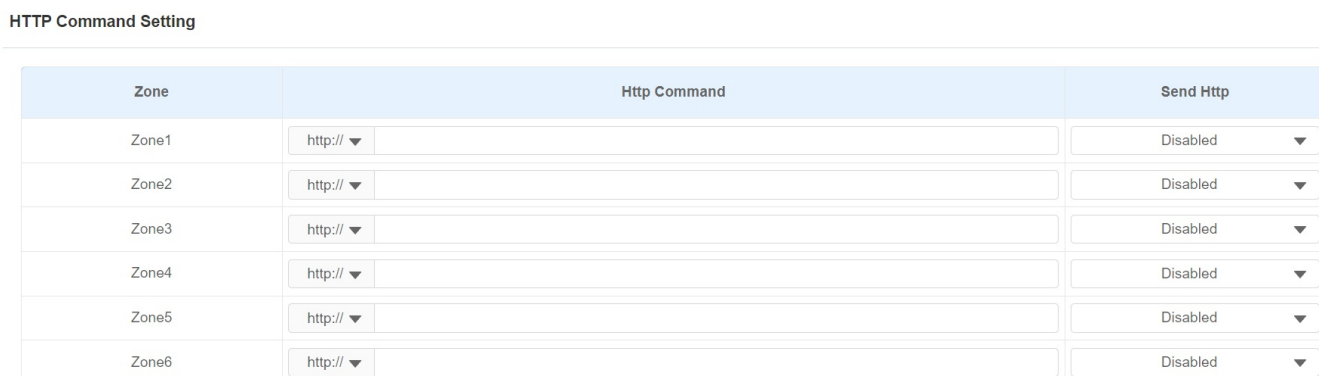
Alarm Action Configuration

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

To select and set up actions on the web **Arming > Alarm Action** interface.

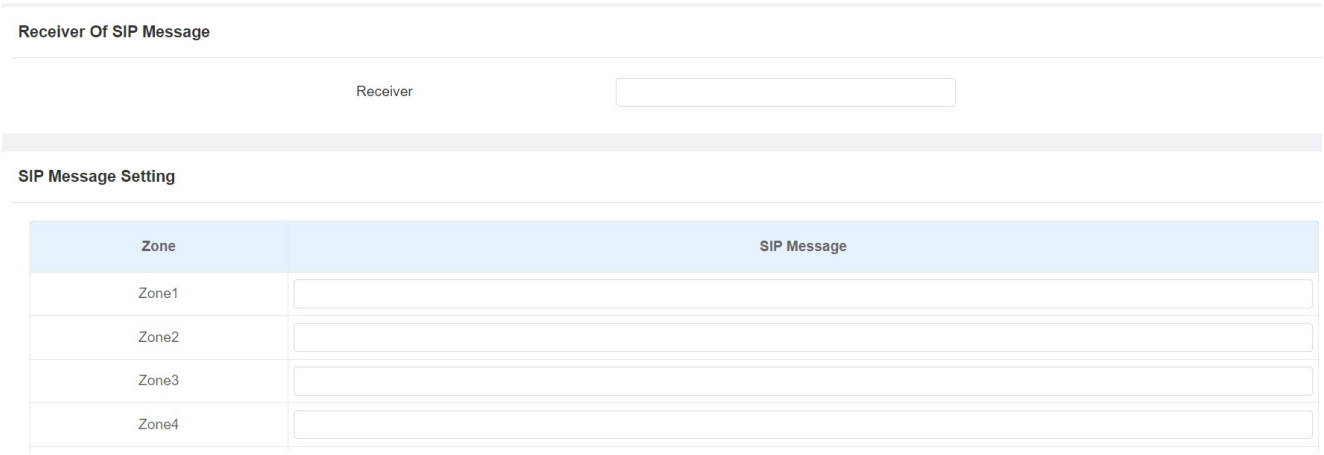
Configure Alarm Action via HTTP Command

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



Configure Alarm Action via SIP Message

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

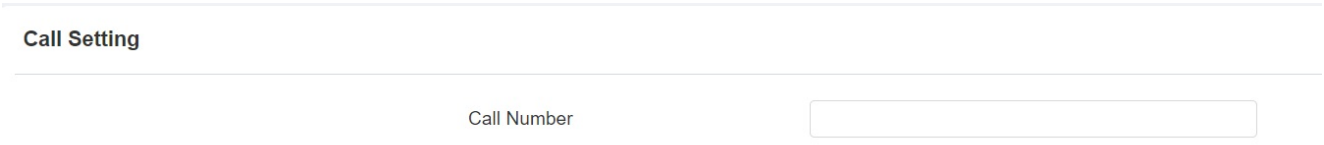


Parameter Set-up:

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

Configure Alarm Action via SIP Call

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

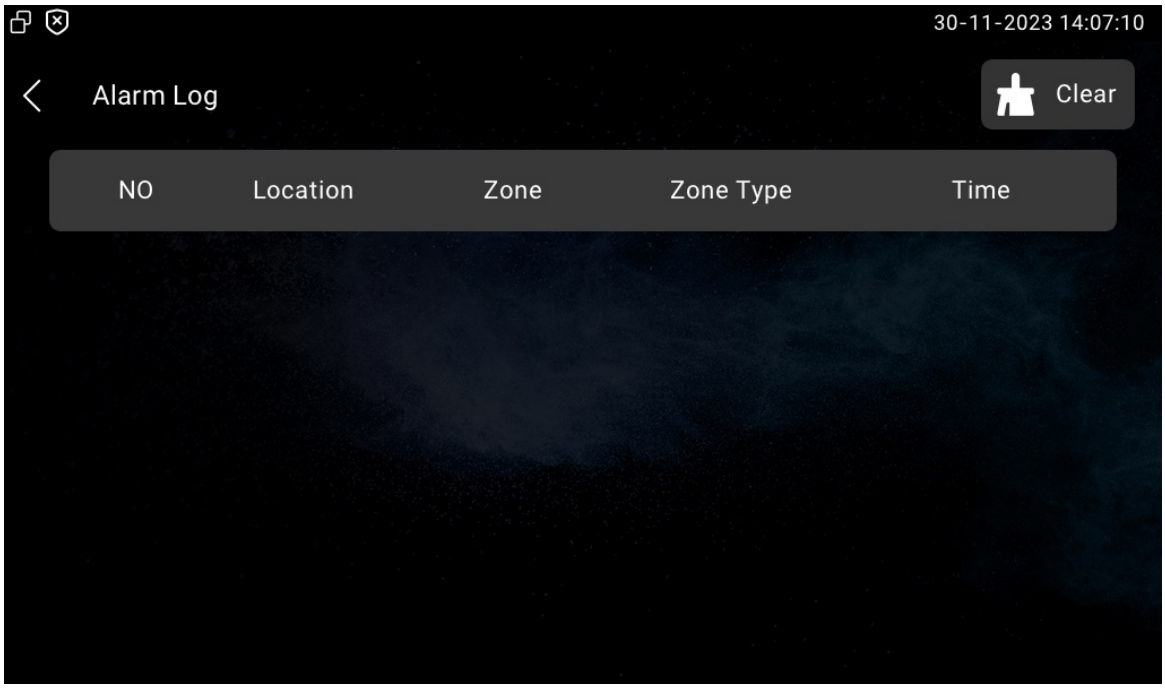


Parameter Set-up:

- **Call Number**: the SIP number or IP number to receive the calls when the alarm is triggered.

Check Alarm Log

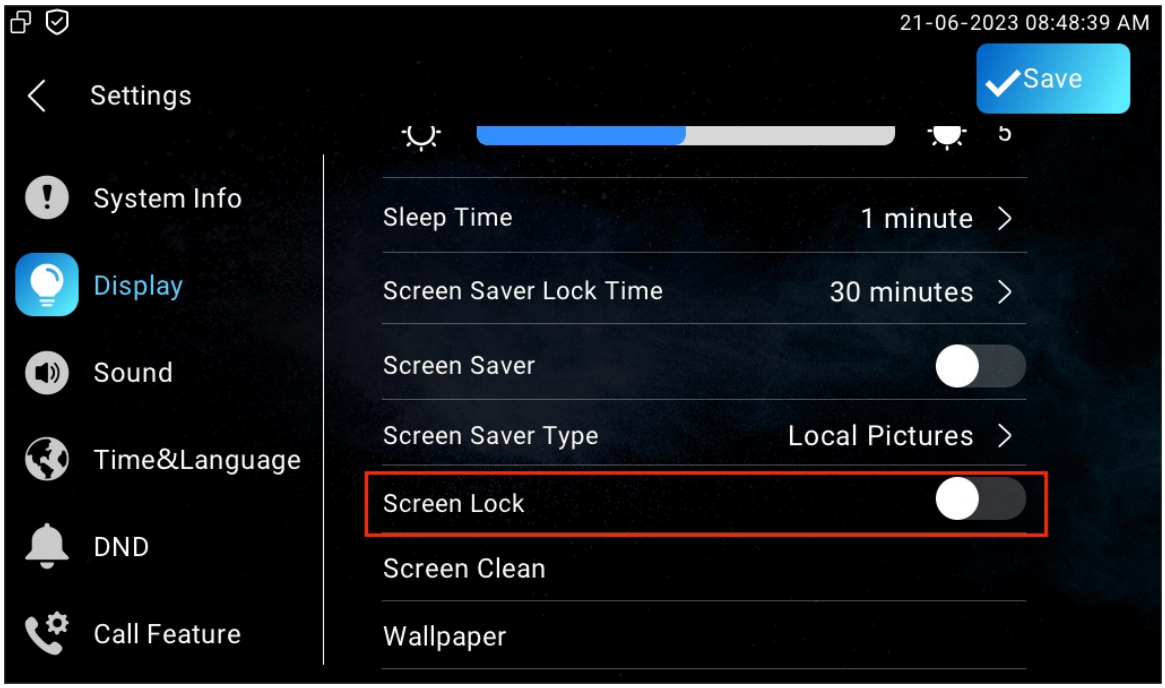
To check alarm logs on the device **Arming > Alarm Log** screen.



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.

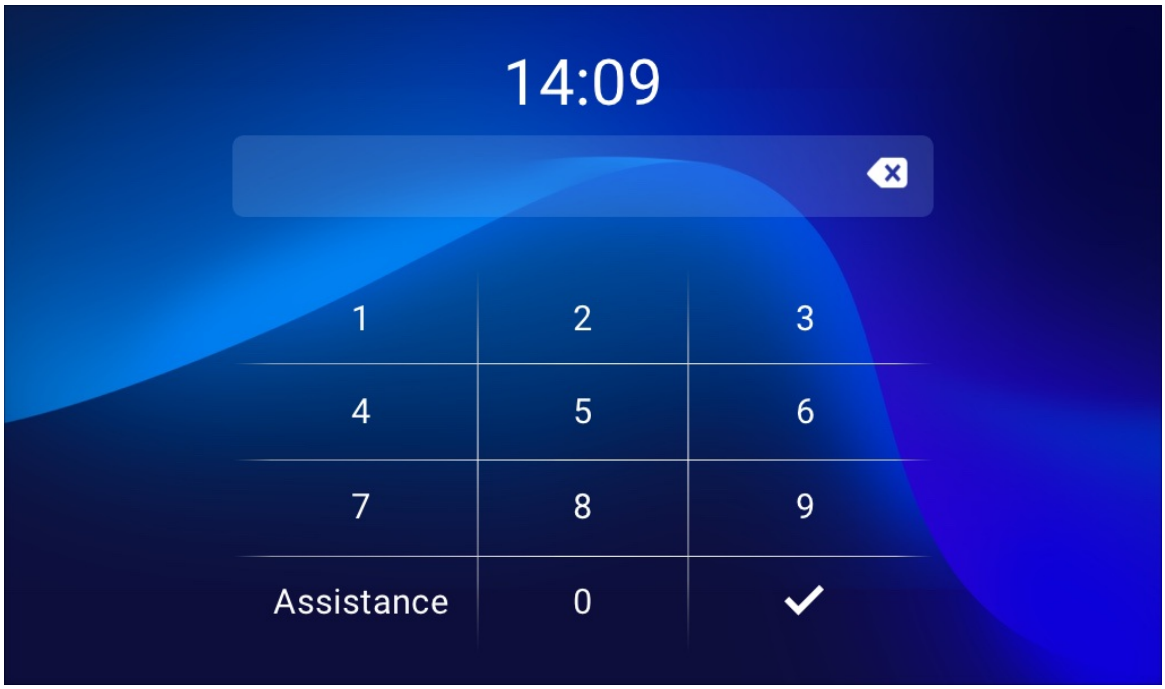
You can enable the screen lock function directly on the device **Settings > Display** screen.



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 **System Code** to change a new password.



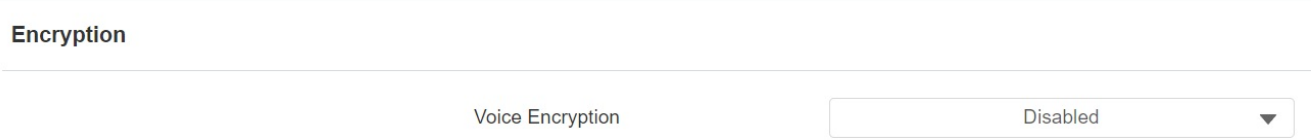
Note

- The default unlock PIN is 123456.

Voice Encryption

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

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



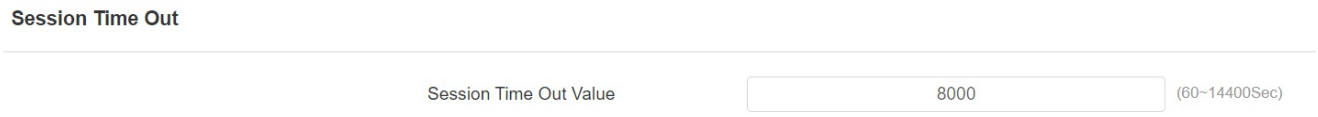
Parameter Set-up:

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

Web Interface Automatic Log-out

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

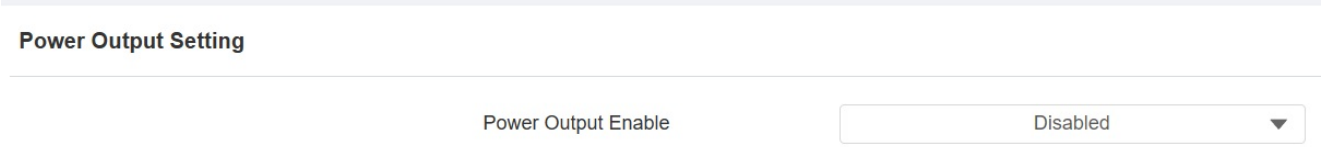
Navigate to **Security > Basic** interface.



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.

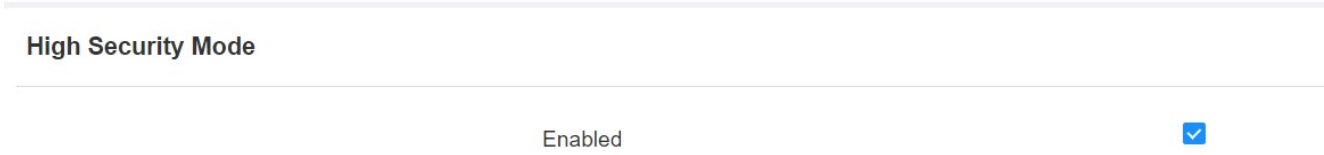
To enable it, go to **Settings > Basic > Power Output Setting** interface.



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 configure this feature on 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.

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

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

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

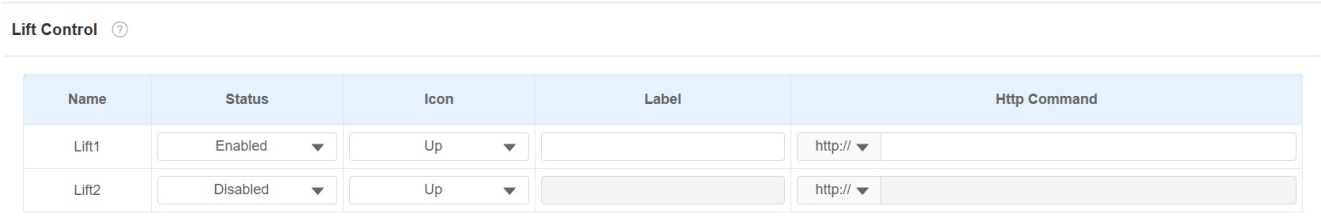
4. It is not allowed to import/export configuration files in tgz. format between a device with the high security mode and another one without it. For assistance with file transfer, please contact Akuvox technical support.

Lift Control

You can summon a lift via the lift control feature.

Configure Lift Control

To enable and set the display status Lift icon on the device web **Device > Lift > Lift Control** interface.



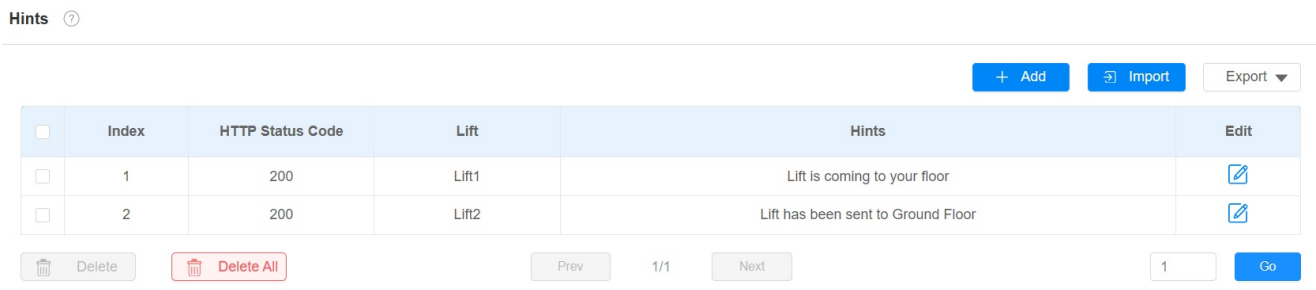
Parameter Set-up:

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

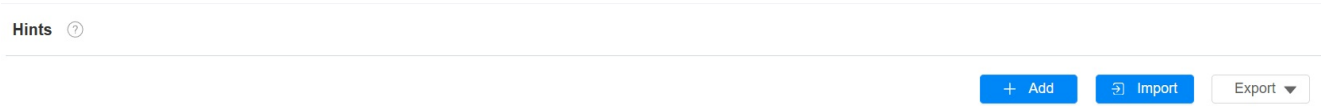
Configure Lift Control Prompt

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

To do this configuration on 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 **Export** tab to export the template and import the file after editing.

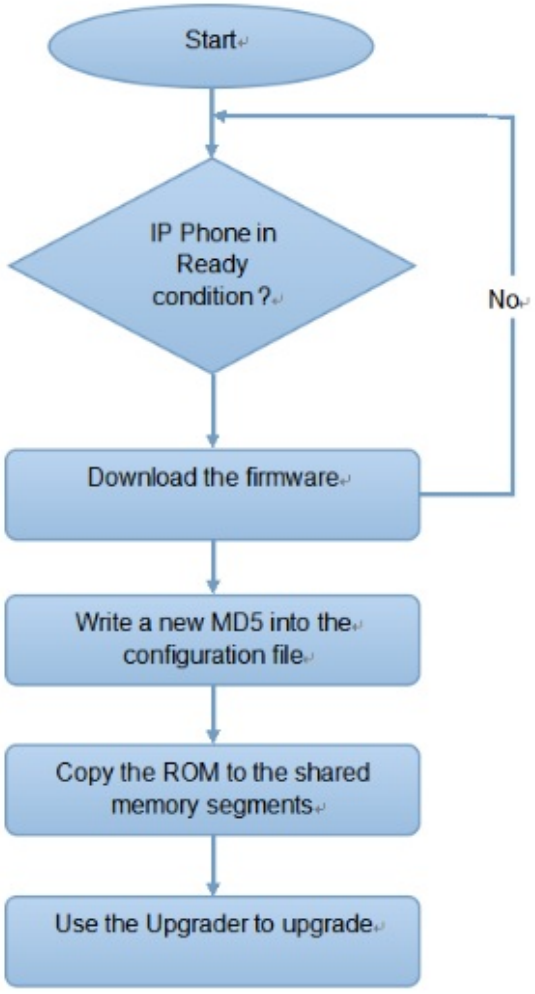


Auto-provisioning

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 intercom devices to access the URL of the address of the third-party server which stores configuration files and firmware, which will then be used to update the firmware and the corresponding parameters on the device.

Please see the flow chart below:



Introduction to the Configuration Files for Auto-Provisioning

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

The difference between the two types of configuration files is shown below:

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

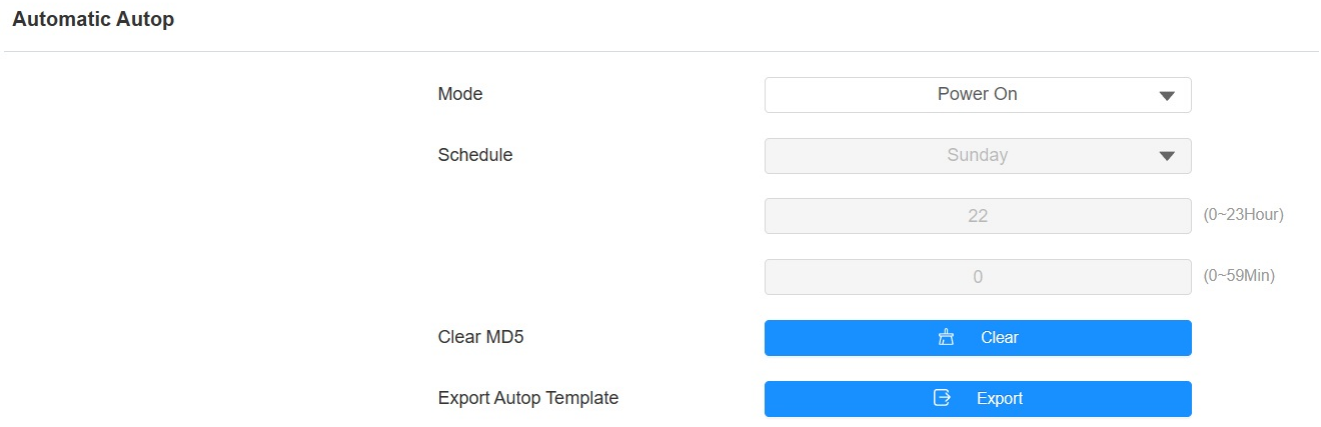
Note

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

Autop Schedule

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

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



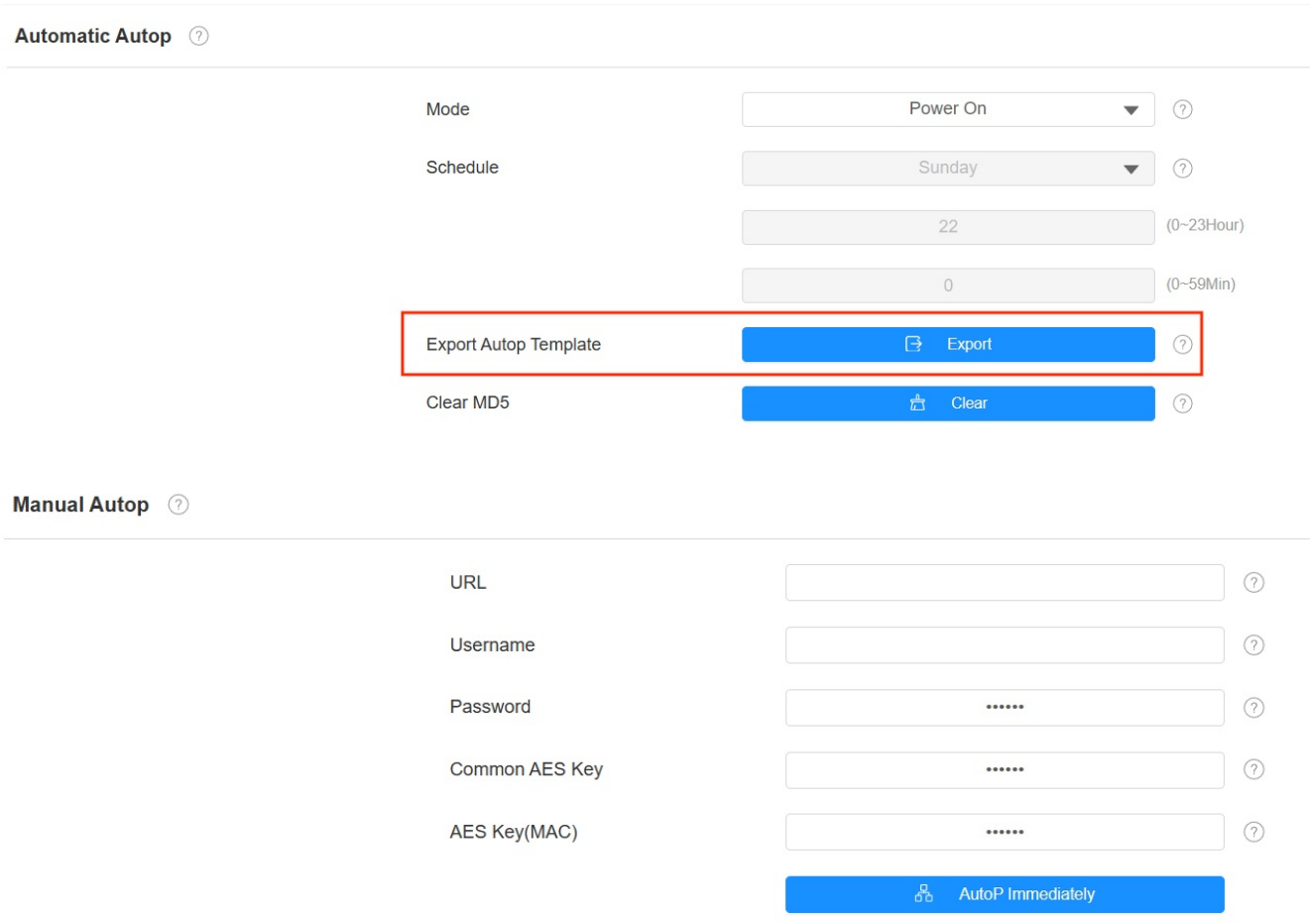
Parameter Set-up:

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

Static Provisioning Configuration

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

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



Parameter Set-up:

- **URL**: TFTP, HTTP, HTTPS, or FTP server address for the provisioning.
- **Username**: set up the username if the server needs a username to be accessed.
- **Password**: set up 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 do not provide the user-specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

PNP Configuration

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

To enable it on the web **Upgrade > Advanced > PNP Option** interface.

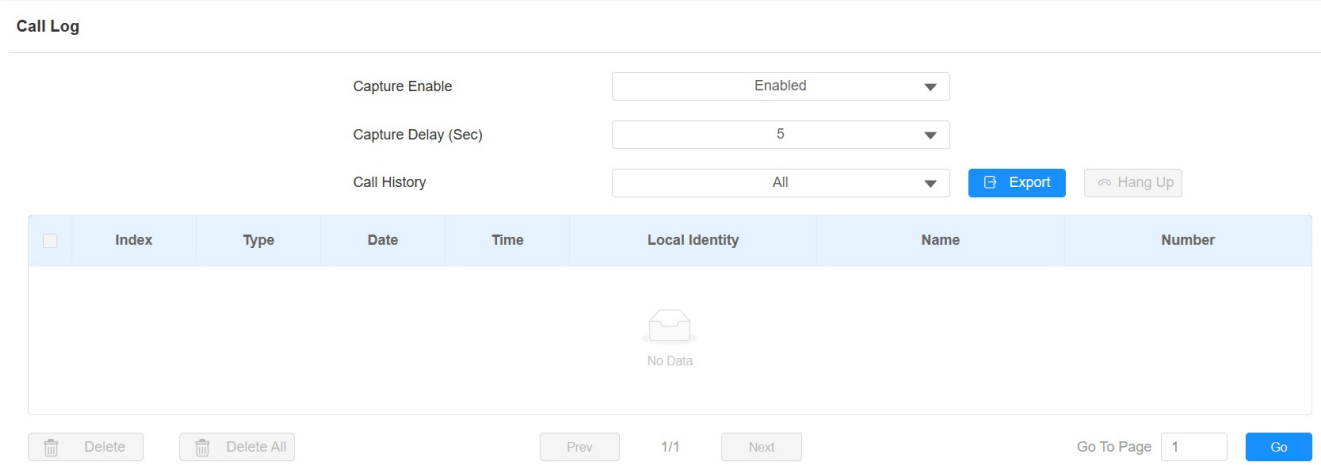
PNP Option

PNP Config Enabled 

Call Logs

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

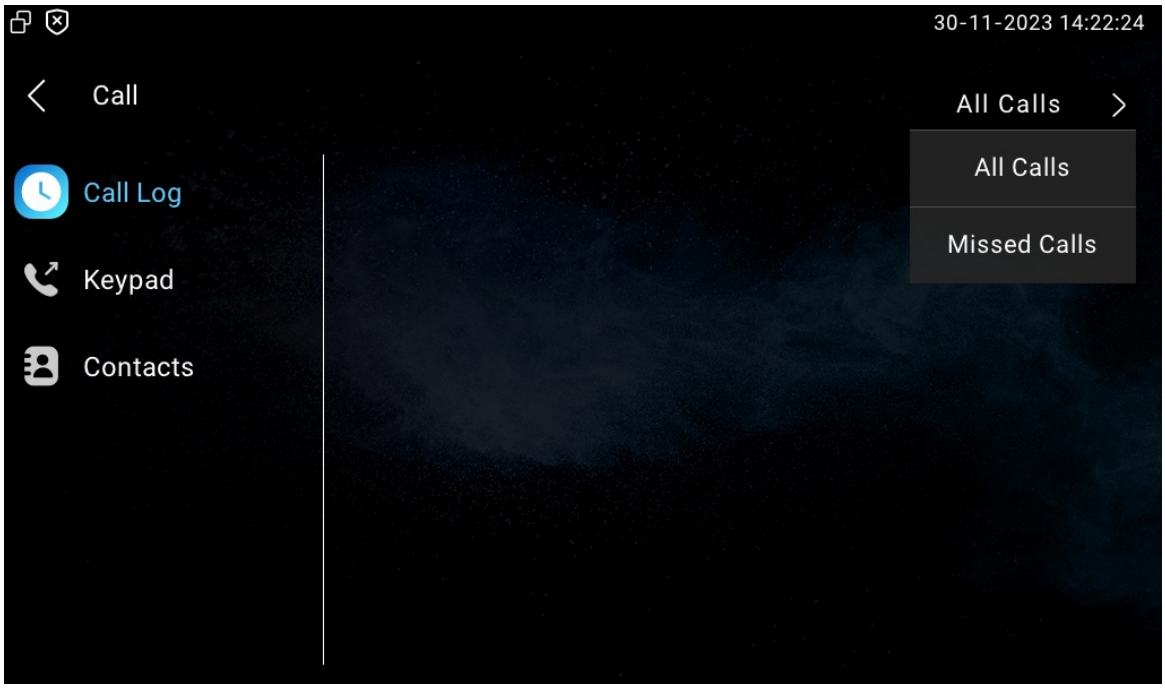
Go to **Contacts > Call Logs** interface.



Parameter Set-up:

- **Capture Delay**: the image capturing starting time when the device goes into a video preview.
- **Upper Limit**: the maximum screenshot storage capacity. When the capacity reaches its limit, the previous screenshots will be overwritten.
- **Call History**: five types of call history, All, Dialed, Received, Missed, and Forwarded.
- **Local Identity**: displays the device's SIP account or IP number that receives the incoming calls.

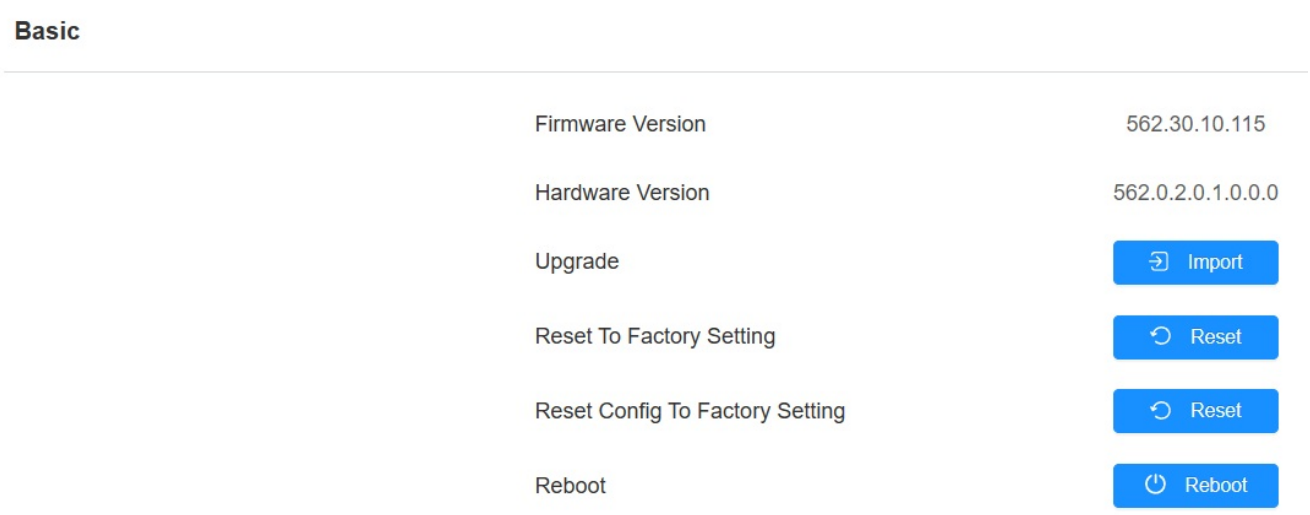
To check call logs on the device, tap **Call > Call Logs**.


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

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Navigate to **Upgrade > Basic** interface.



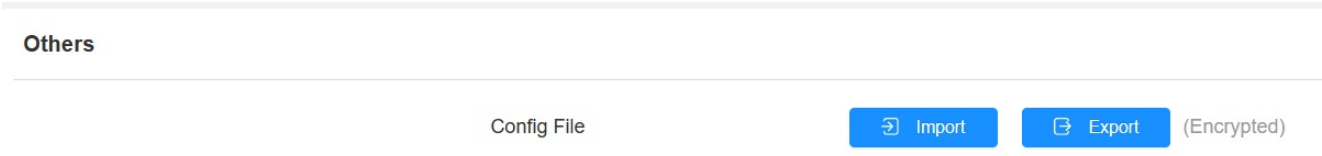
Note

- Firmware files should be .rom format for an upgrade.

Backup

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

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

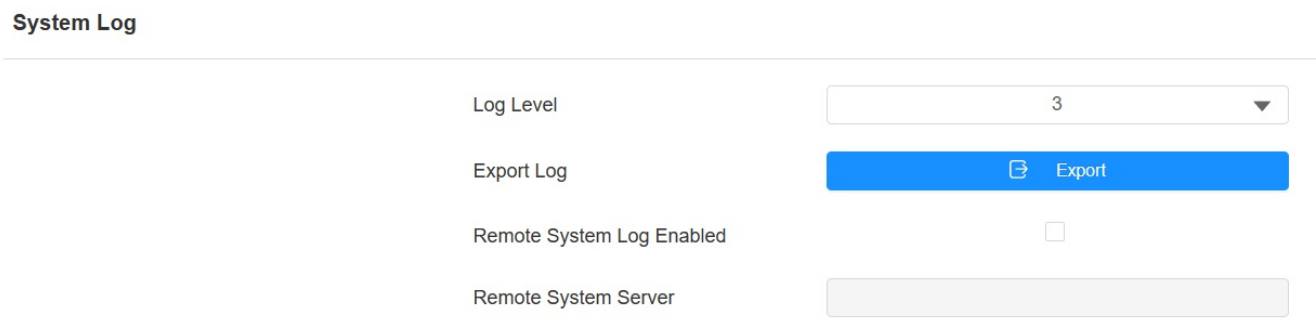


Debug

System Log for Debugging

System logs can be used for debugging purposes.

You can set up the function on the web **Upgrade > Diagnosis > System Log** interface.



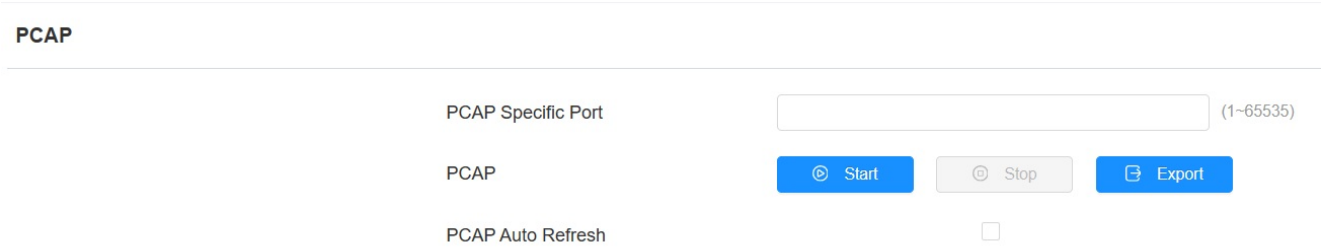
Parameter Set-up:

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

PCAP for Debugging

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

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



Parameter Set-up:

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

User Agent

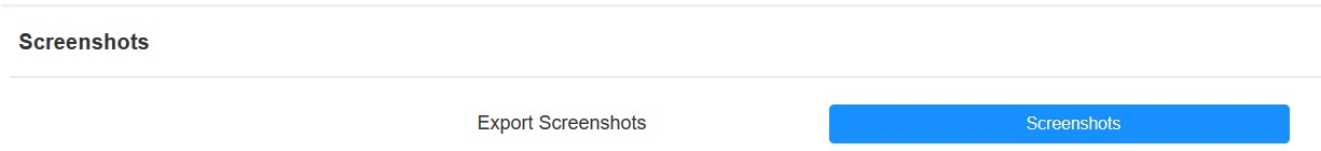
User agent is used for identification purpose when you are analyzing the SIP data packet.

To do this configuration on web **Account > Advanced** interface.

Screenshots

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

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

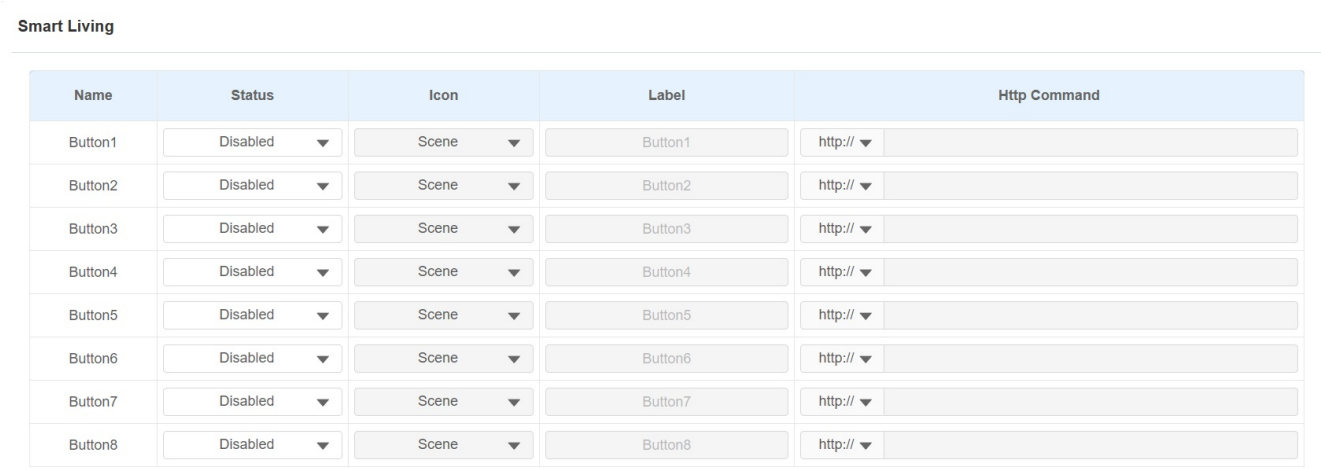


Device Integration with Third Party Device

Smart Living Setting

You can control the home sensor through an HTTP command.

To configure it on the web **Device > Smart Living** interface.



Parameter Set-up:

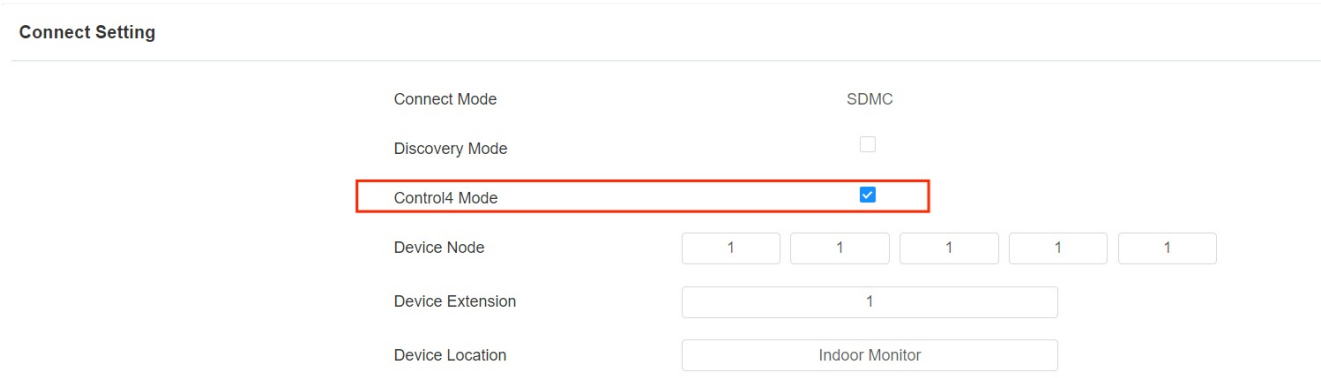
- **Status**: enable or disable this button. If disabled, the button won't appear on the home control page.
- **Icon**: if **Scene** is selected, the icon is displayed as a scene icon. If **Light** is selected, the icon is a light icon.
- **Label**: customize the button display name.
- **HTTP command**: the HTTP command to trigger the sensor.

Note

- To configure Smart Living button on **Device > Display Setting** web interface.

Integration with Control 4

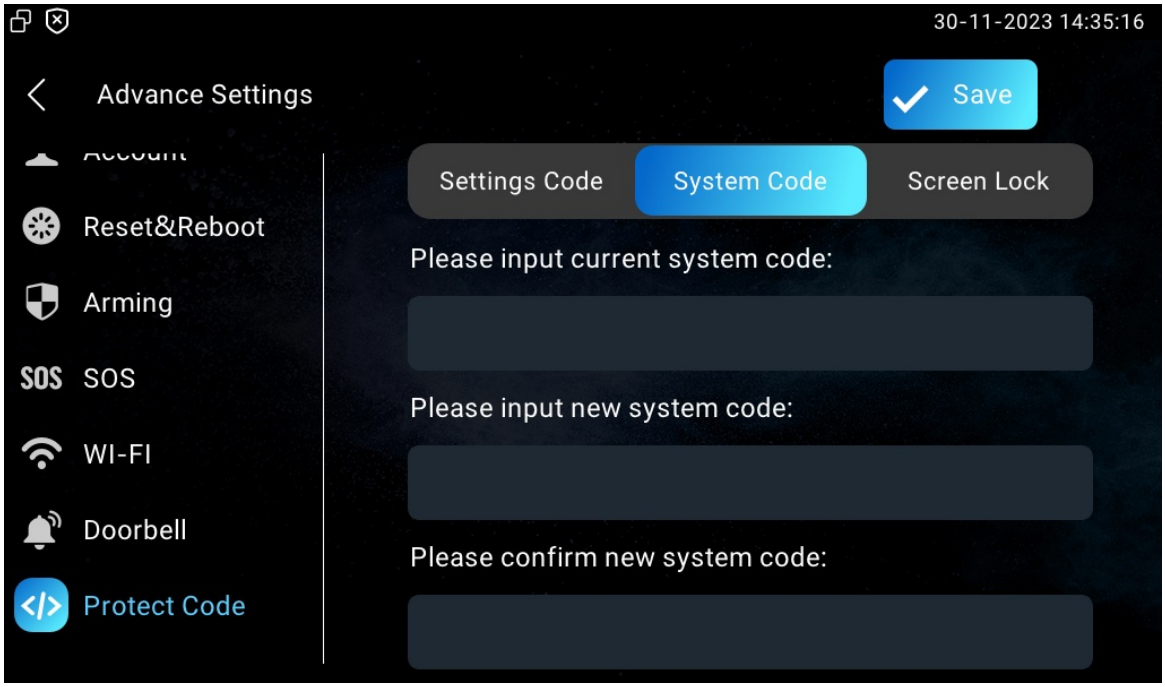
You need to enable the Control 4 mode before you can integrate the device with the Control 4 home center. To enable it, go to **Network > Advanced > Connect Setting** mode.



Password Modification

Modify Device Basic Setting Password

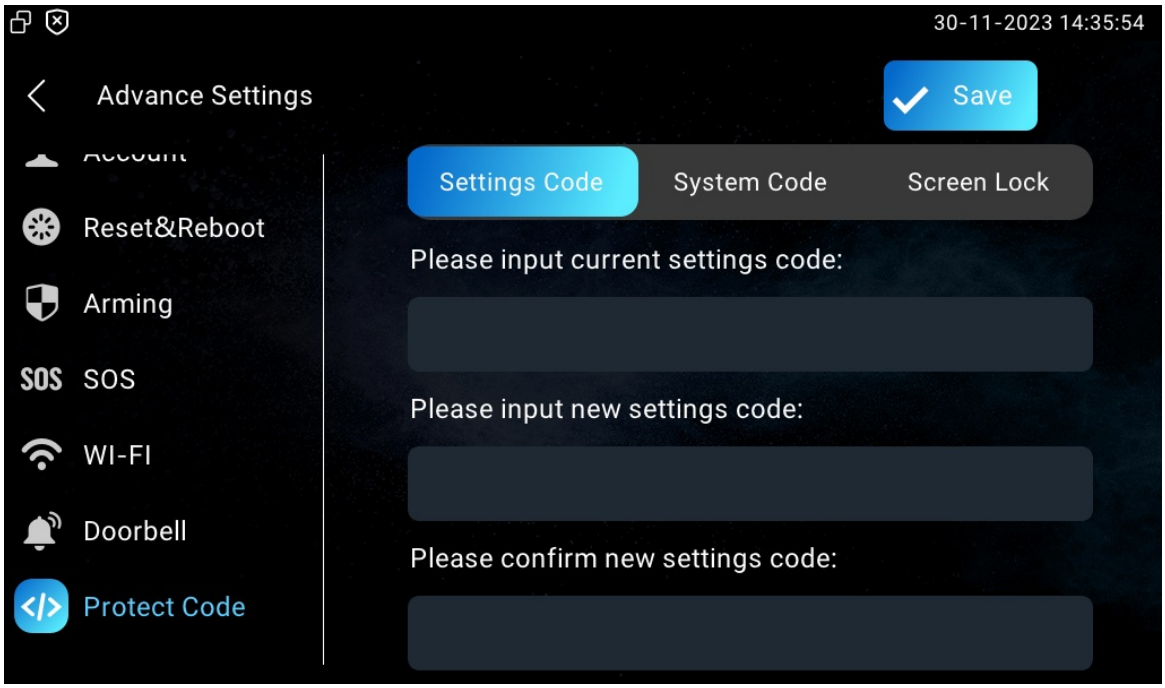
To do the configuration on device **Settings > Advance Settings > Protected Code** screen to choose **System Code** to change a new password. The default password is 123456.



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.

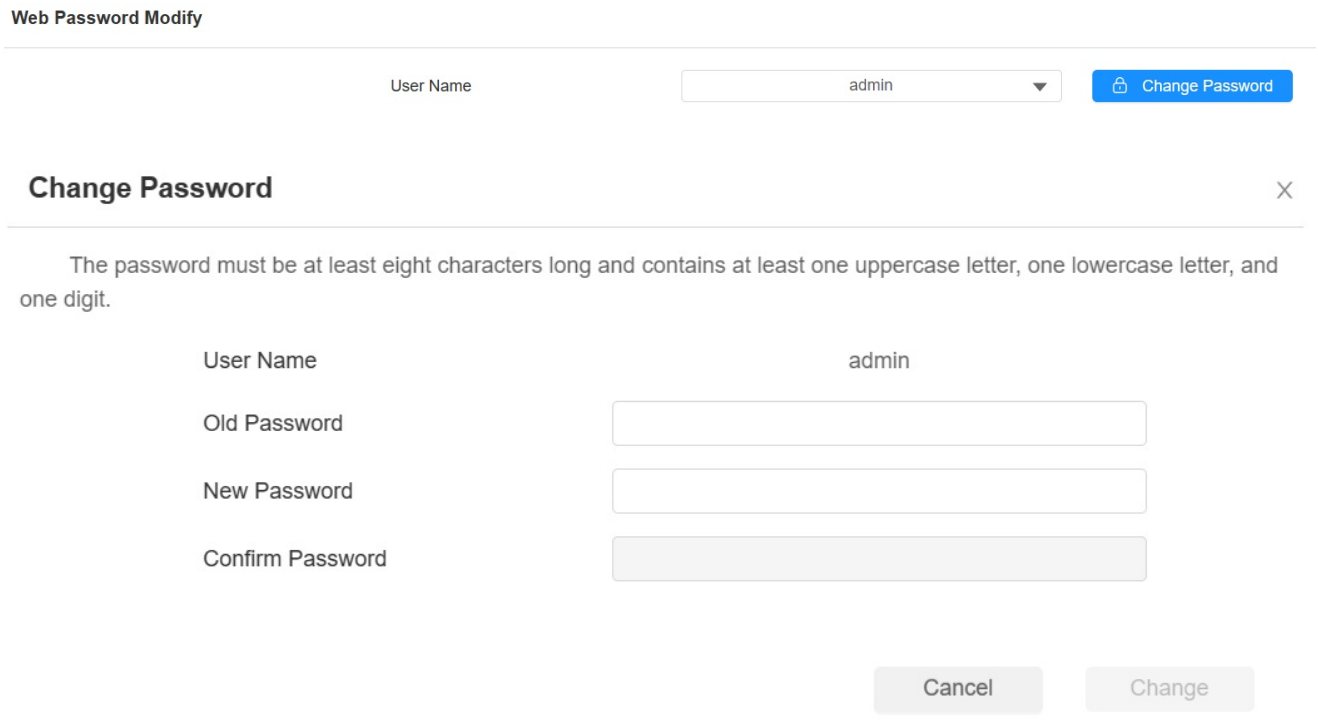
Navigate to **Settings > Advance Settings > Protected Code** screen and choose **Settings Code**.



Modify Device Web Interface Password

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

Navigate to **Security > Basic > Web Password Modify** interface.

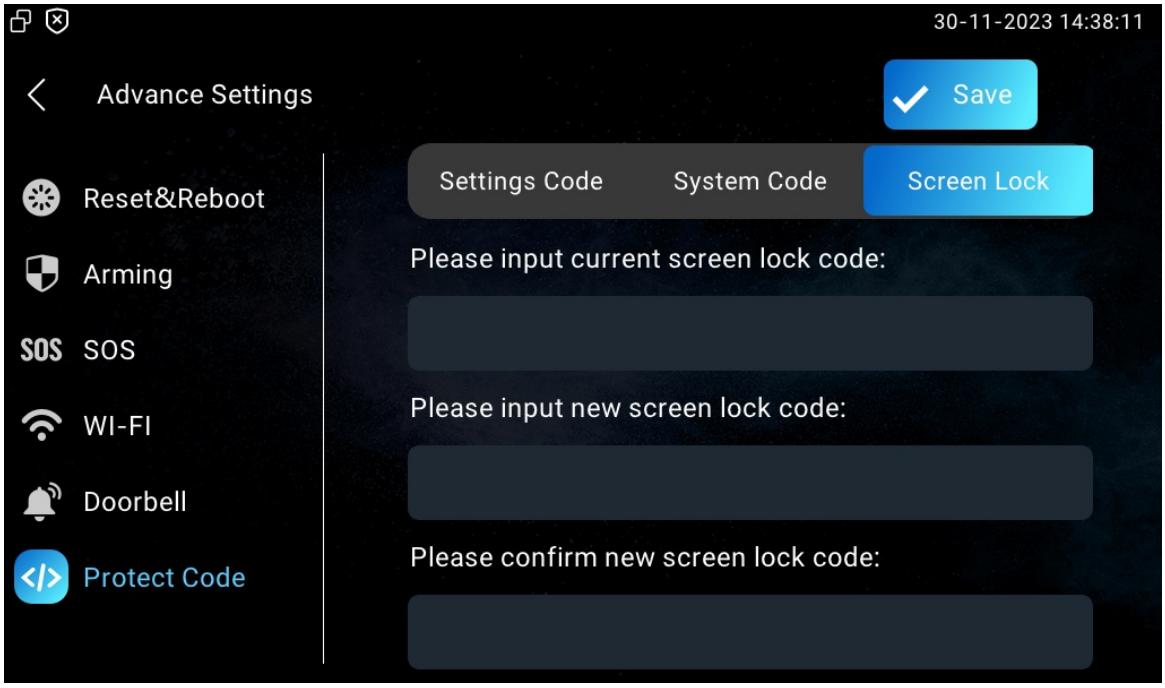


Note

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

Modify Screen Lock Password

Navigate to **Settings > Advance Settings > Protected Code** screen and choose **Screen Lock**.



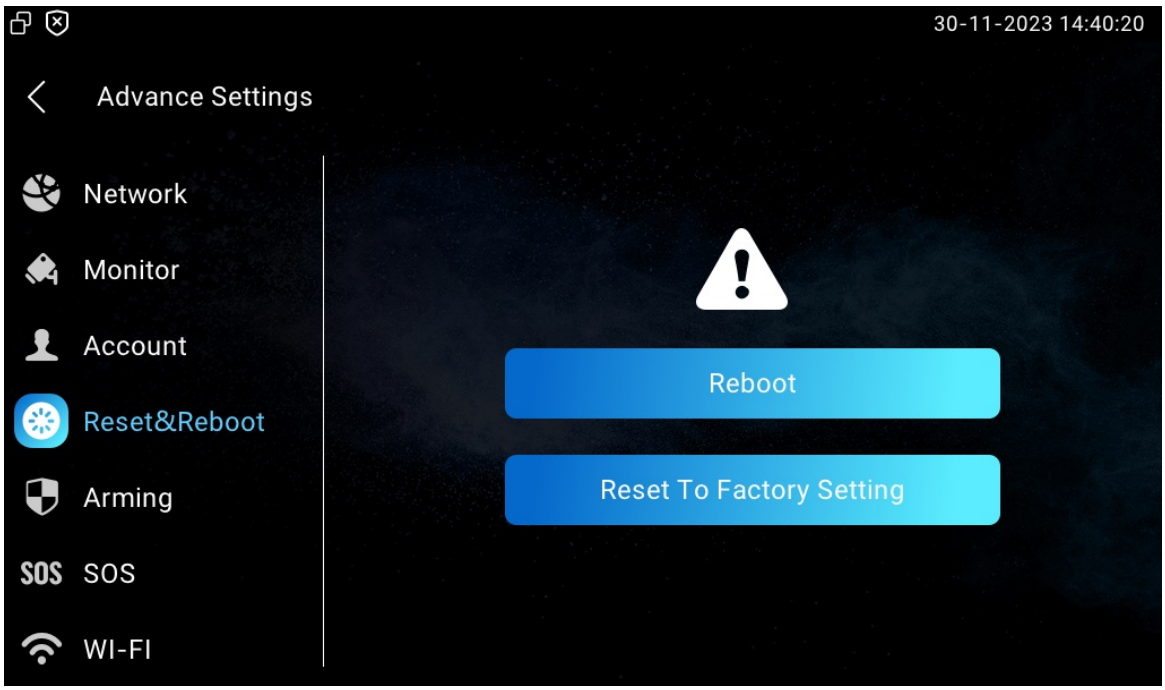
System Reboot & Reset

Reboot

Reboot on the Device

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

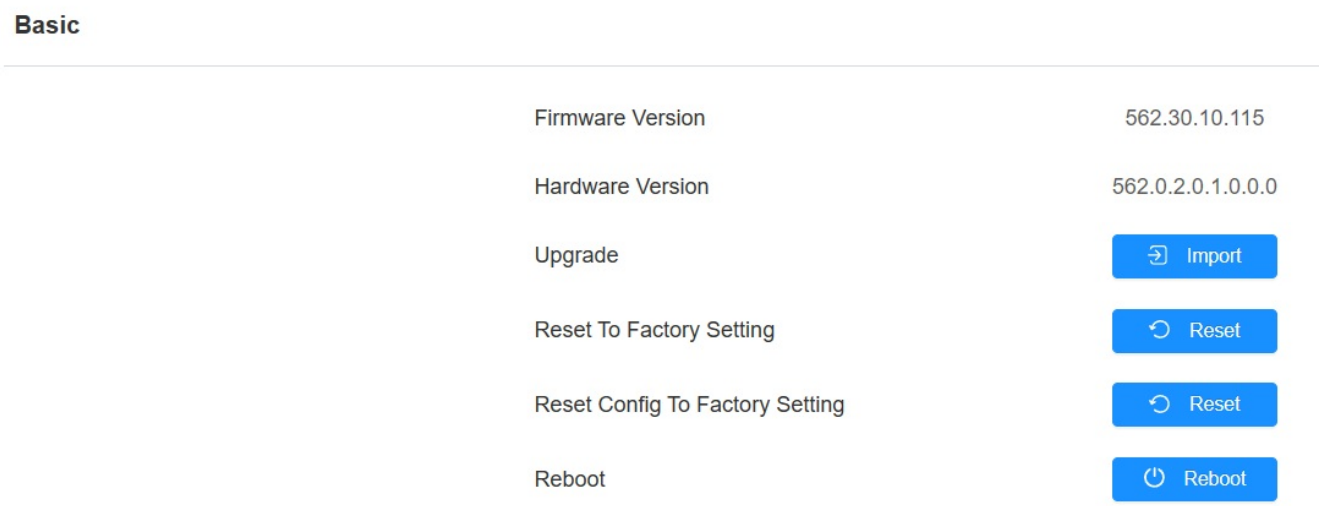
To restart the system on device **Settings > Advance Settings > Reset&Reboot** screen.



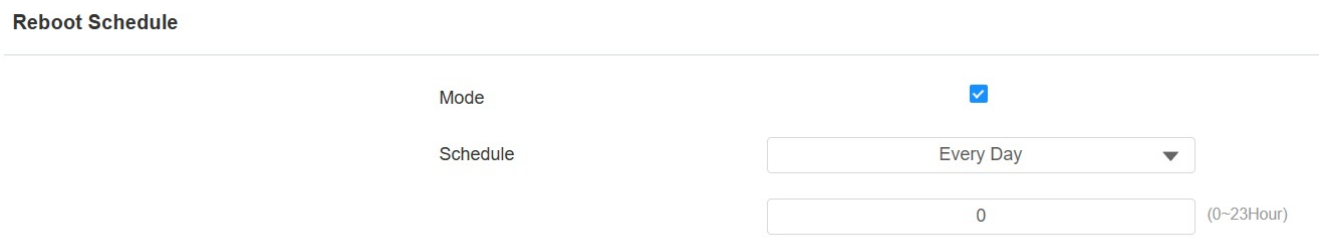
Reboot on the Web Interface

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

To operate it on the device web **Upgrade > Basic** interface.



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

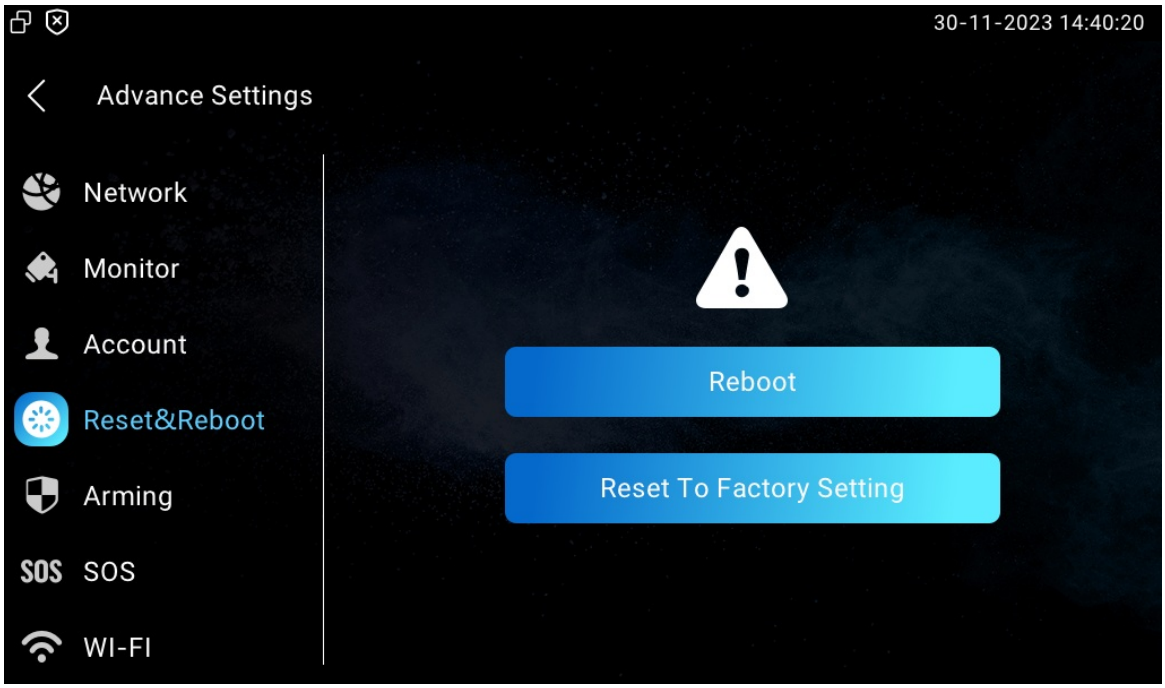


Reset

Reset on the Device

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

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



Reset on the Web Interface

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

To operate it on the device web **Upgrade > Basic** interface.