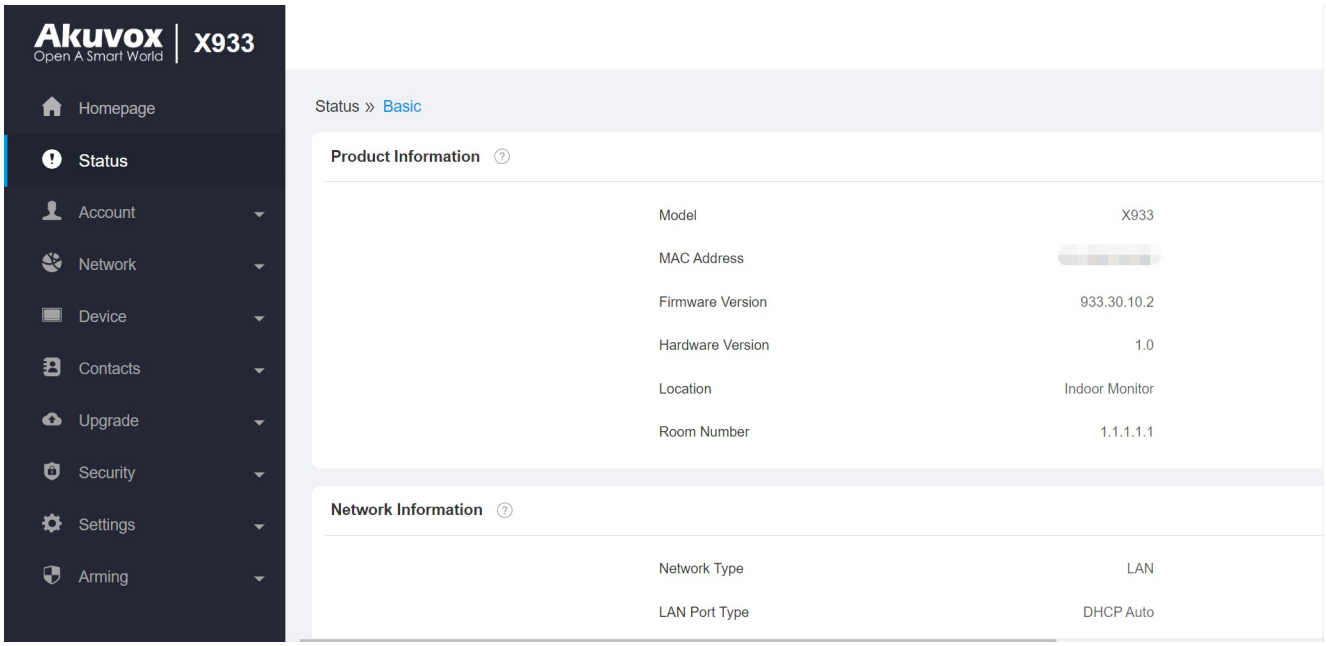
Introduction to Configuration Menu

- **Status**: This section gives you basic information such as product information, network Information, account information, etc.
- **Account**: This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio&video codec, DTMF, session timer, etc.
- **Network**: This section mainly deals with DHCP&Static IP setting, RTP port setting, device deployment, etc.
- **Device**: This section includes time, language, call feature, dial management, data import&export, door log, and web relay.
- **Contacts**: This section allows the user to configure the local contact list stored on the device.
- **Upgrade**: This section covers Firmware upgrade, device reset&reboot, configuration file auto-provisioning, and PCAP.
- **Security**: This section is for Password modification, account status & session time-out configuration, as well as service location switching.
- **Settings**: This section includes the RTSP & voice assistance setup.
- **Arming**: This section covers the configuration including arming zone setting, arming mode, disarm code, and alarm action.

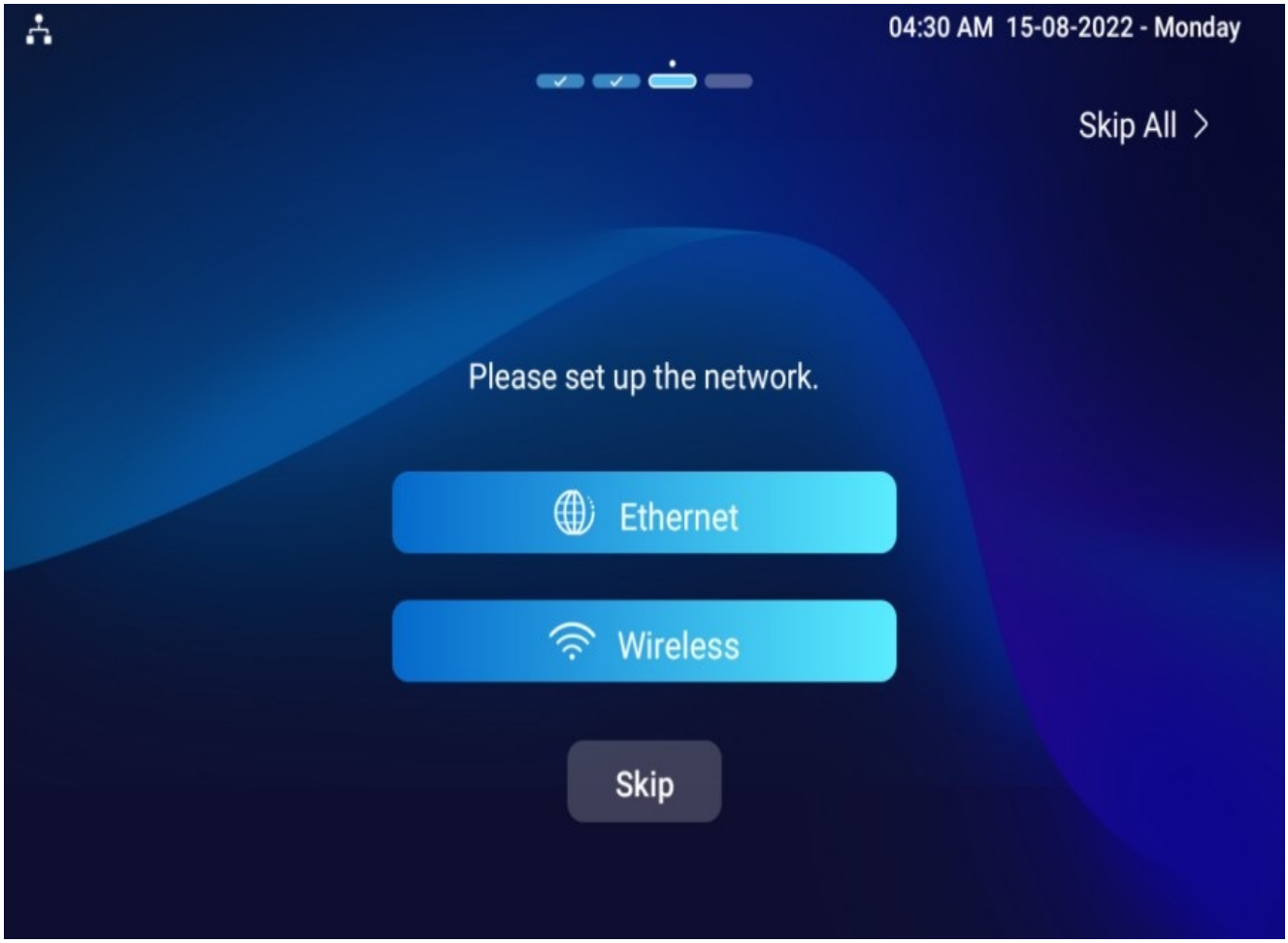

Akuvox
Open A Smart World
X933
Homepage
Status
Account
Network
Device
Contacts
Upgrade
Security
Settings
Arming
Status » Basic
Product Information
Model
X933
MAC Address
Firmware Version
933.30.10.2
Hardware Version
1.0
Location
Indoor Monitor
Room Number
1.1.1.1.1
Network Information
Network Type
LAN
LAN Port Type
DHCP Auto

Access the Device

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

Device Start-up Network Selection

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



Note

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

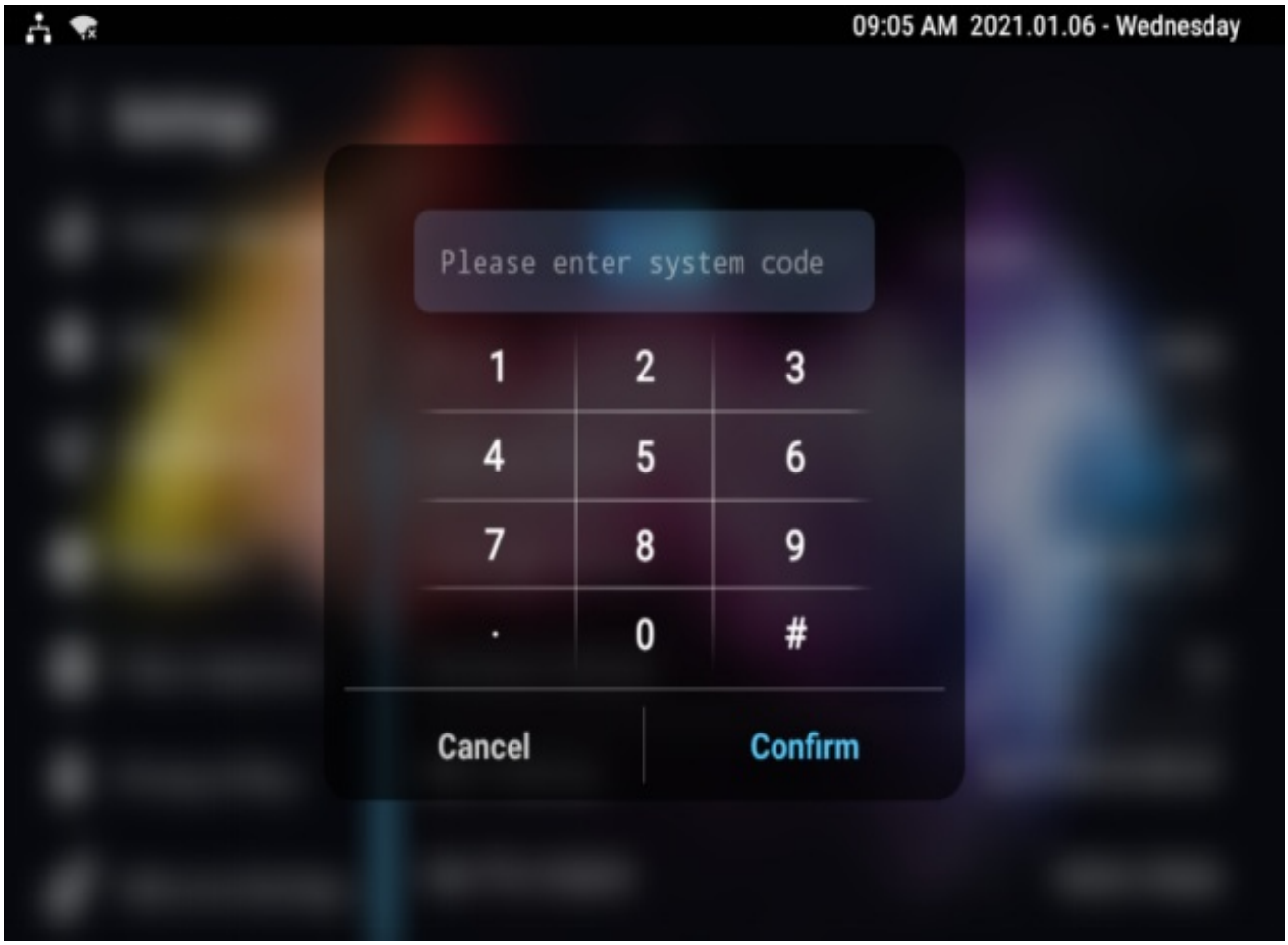
Access the Device Setting on the Device

Access Device Basic Setting

To access the device basic setting by pressing **Setting** icon. To checking the basic information like MAC, firmware and ect.

Access Device Advance Setting

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



Access the Device Setting on the Web Interface

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

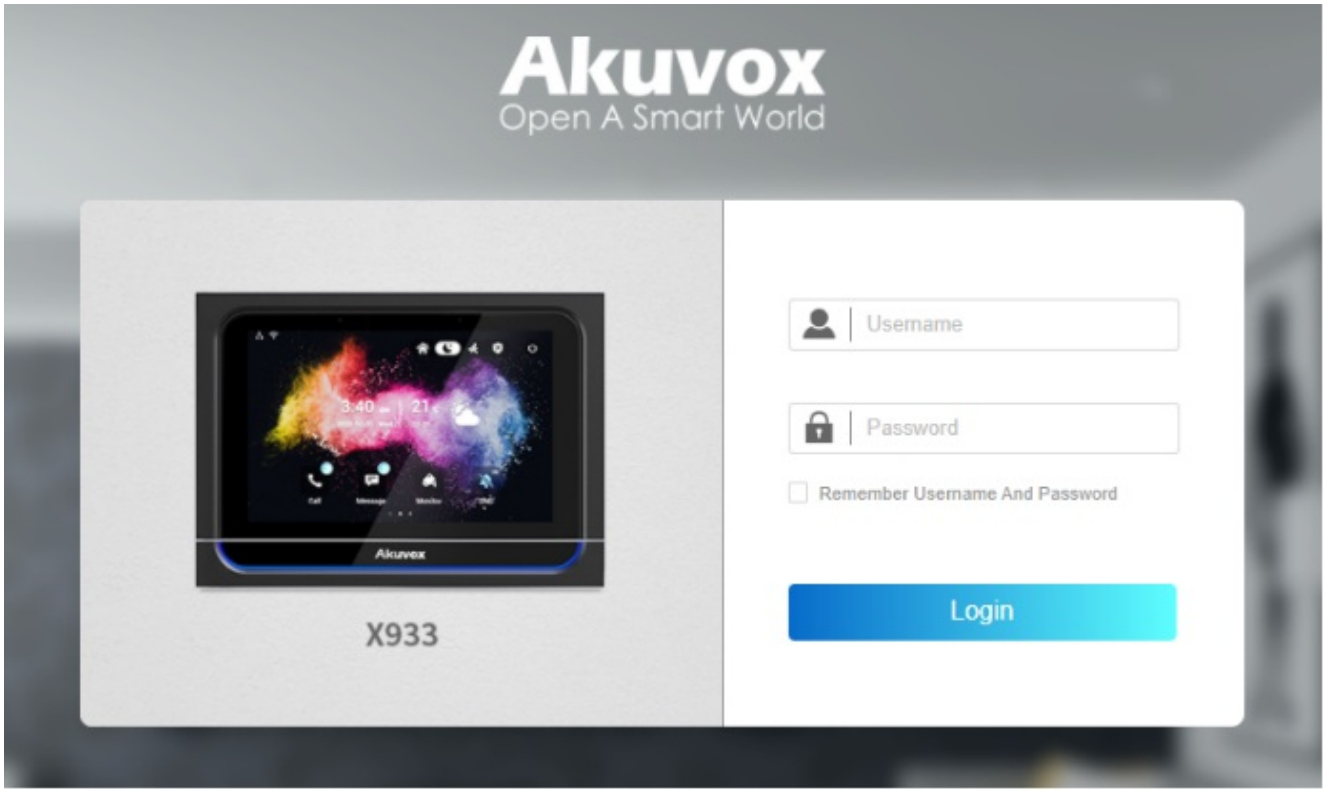
You can check device IP on device **Setting > System Info > Network** screen. Or searching by IP scanner tool which in the same LAN with the devices.

IP Scanner

Online Device : 7

Search Refresh

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.

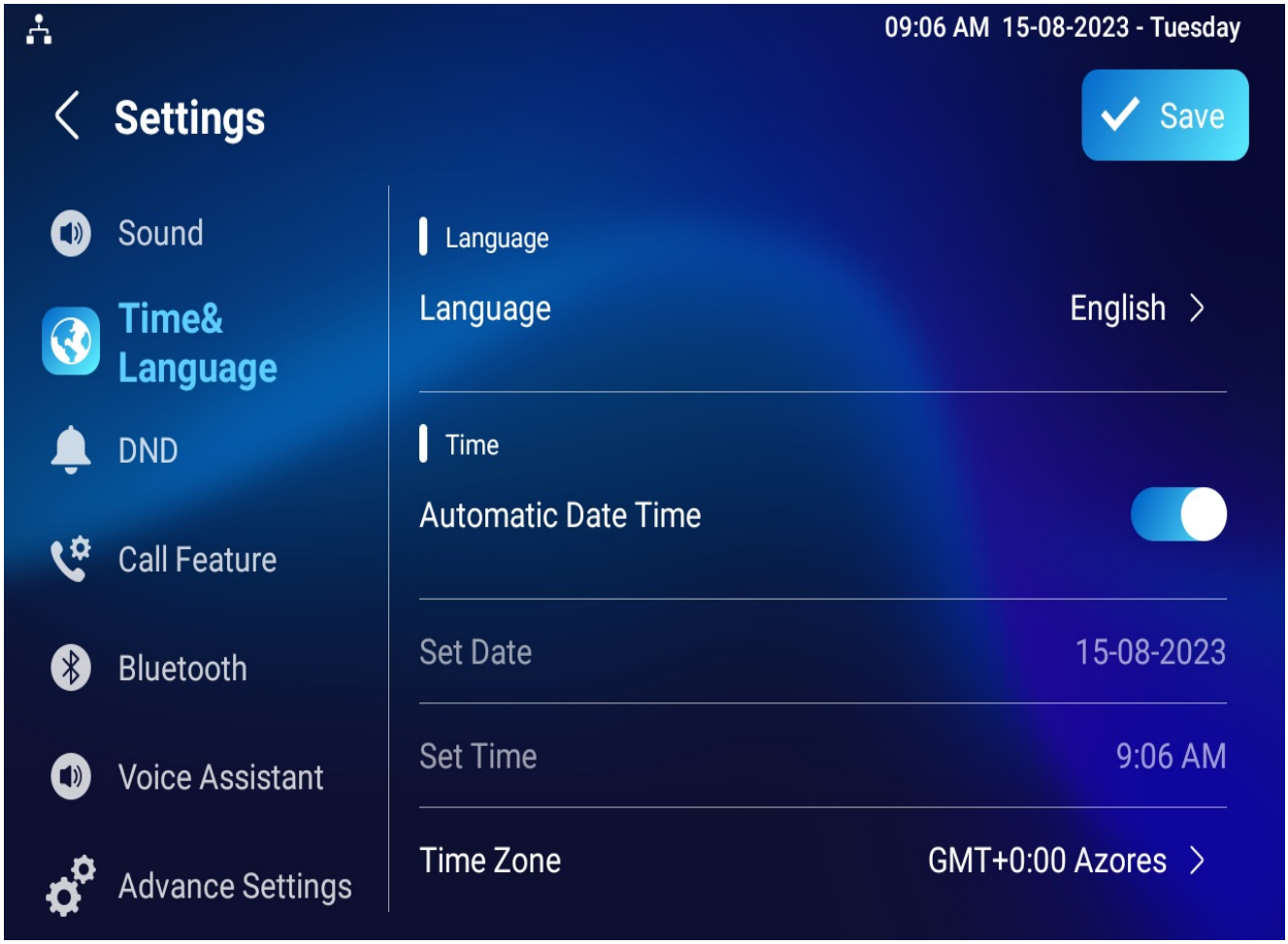
Language and Time Setting

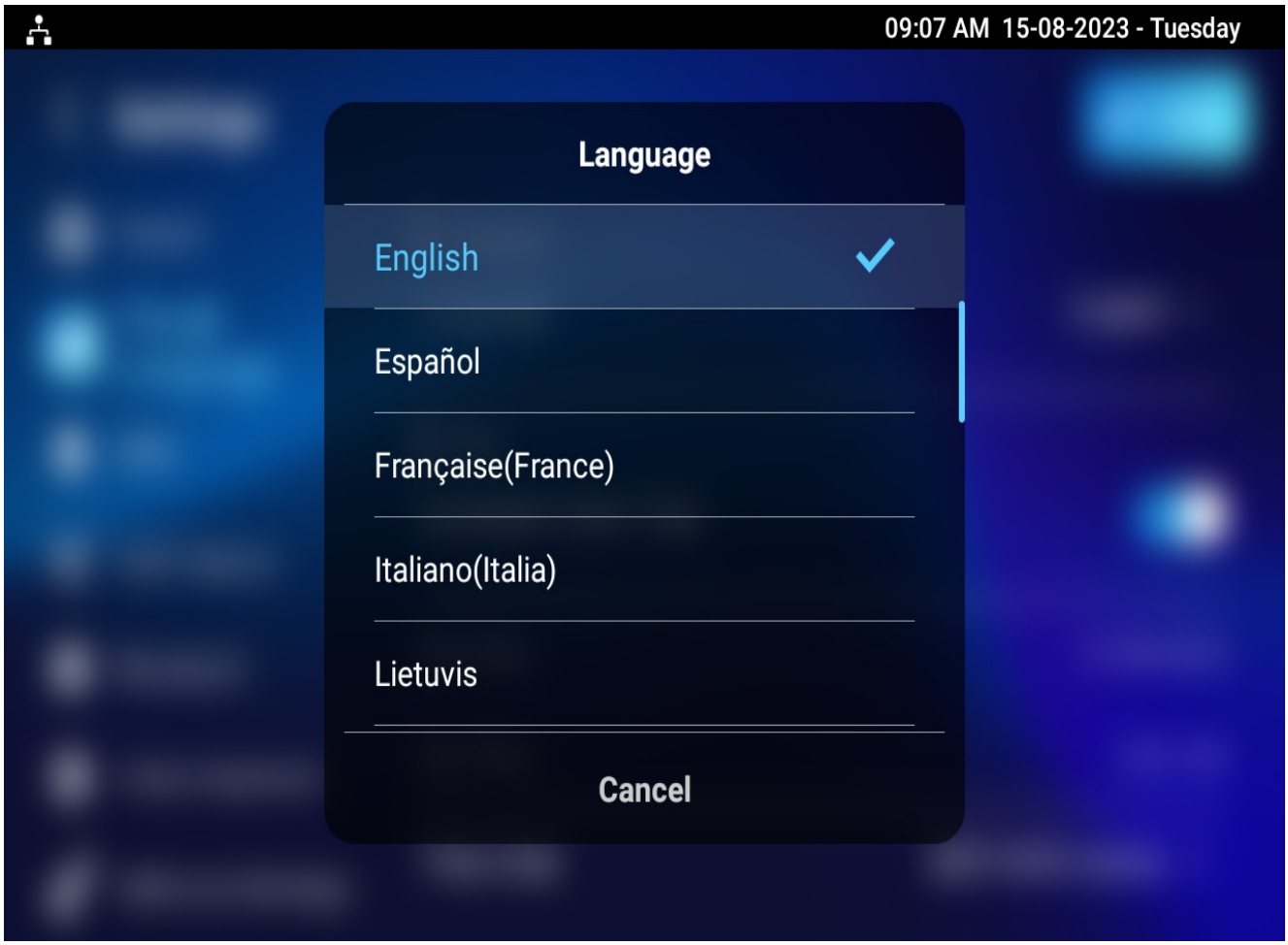
Language Setting

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 configure the language display on the device **Setting > Time&Language** screen.



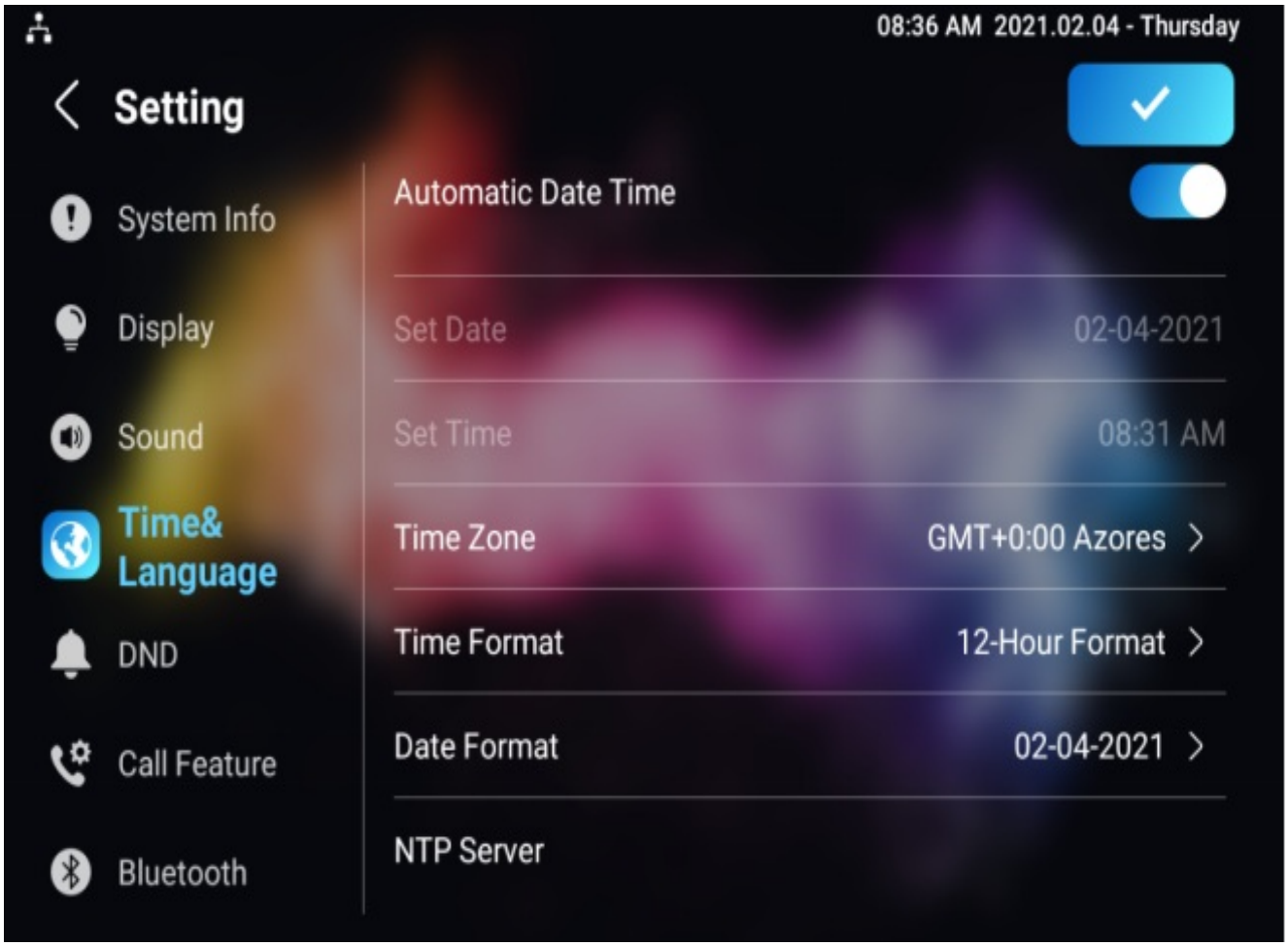


Time Setting

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

Time Setting on the Device

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



Parameter Set-up:

- **Automatic Date**: 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 NTP server (Network Time Protocol). You can also set it up manually by checking off the square box and then entering the time and date you want and pressing the Save tab to save the setting.
- **Time Zone**: select the specific time zone depending on where the device is used. The default time zone is GMT+0.00.
- **Date Format**: select the date format as you like among the 6 format options. The 6 formal options are **Y-M-D, Y/M/D, D-M-Y, D/M/Y, M-D-Y, M/D/Y.**
- **Time Format**: select 12-hour or 24-hour time format as you like.
- **NTP Server**: enter the NTP server you obtained in the NTP server field.

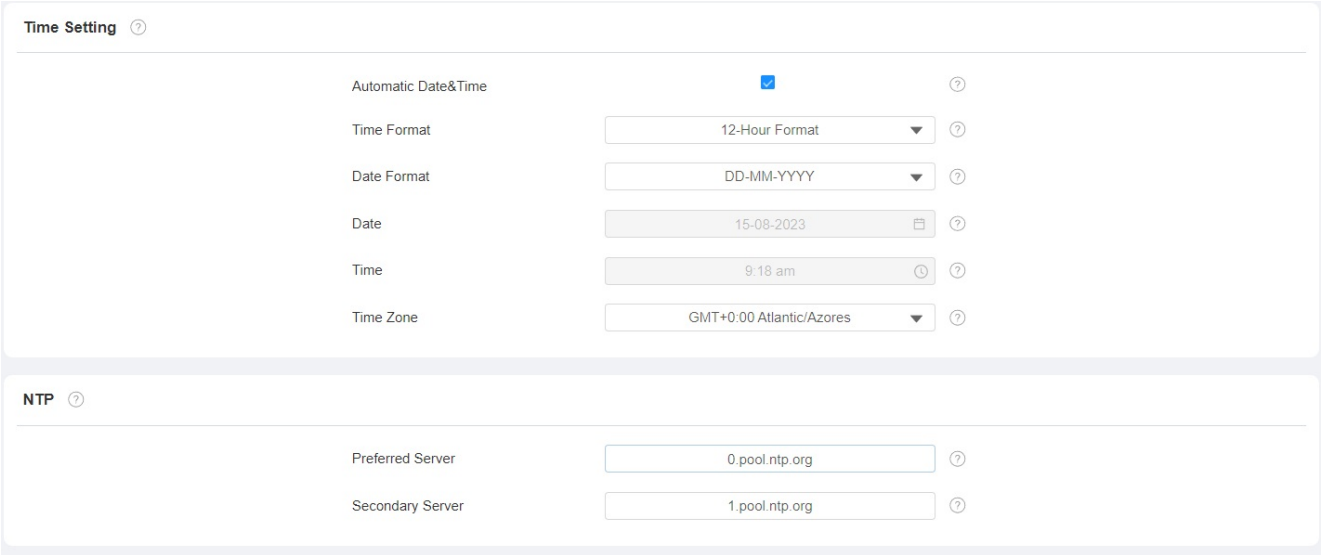
Note:

- When the **Automatic Date&Time** toggle switch is toggled off then parameters related to the NTP server will become uneditable. And when the switch is toggled on, then time and date will be denied editing.

Time Setting on the Device Web Interface

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

Navigate to **Device >Time** interface.



Parameter Set-up:

- **NTP Server**: enter the NTP server you obtained in the NTP server field.

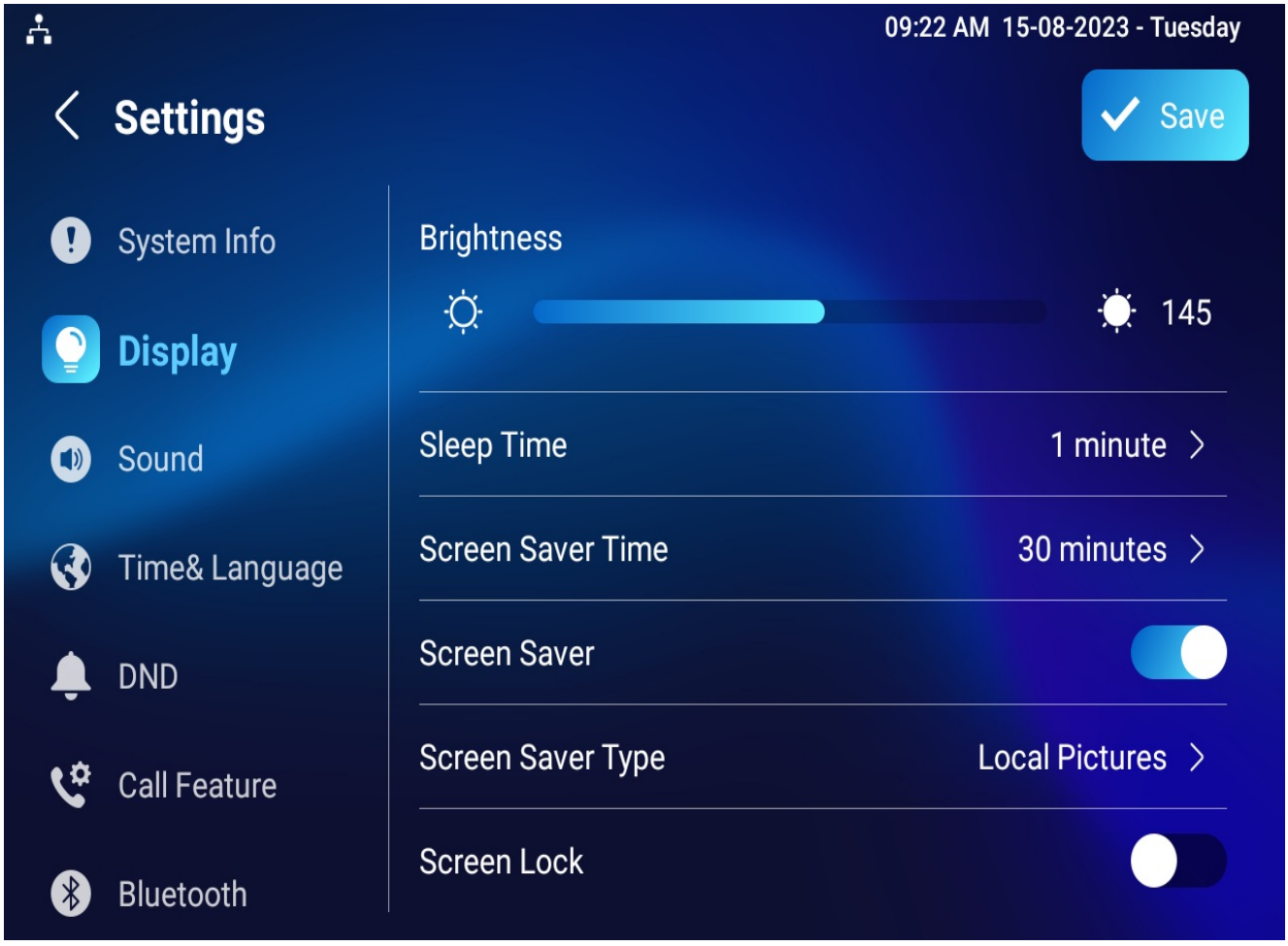
Screen Display Configuration

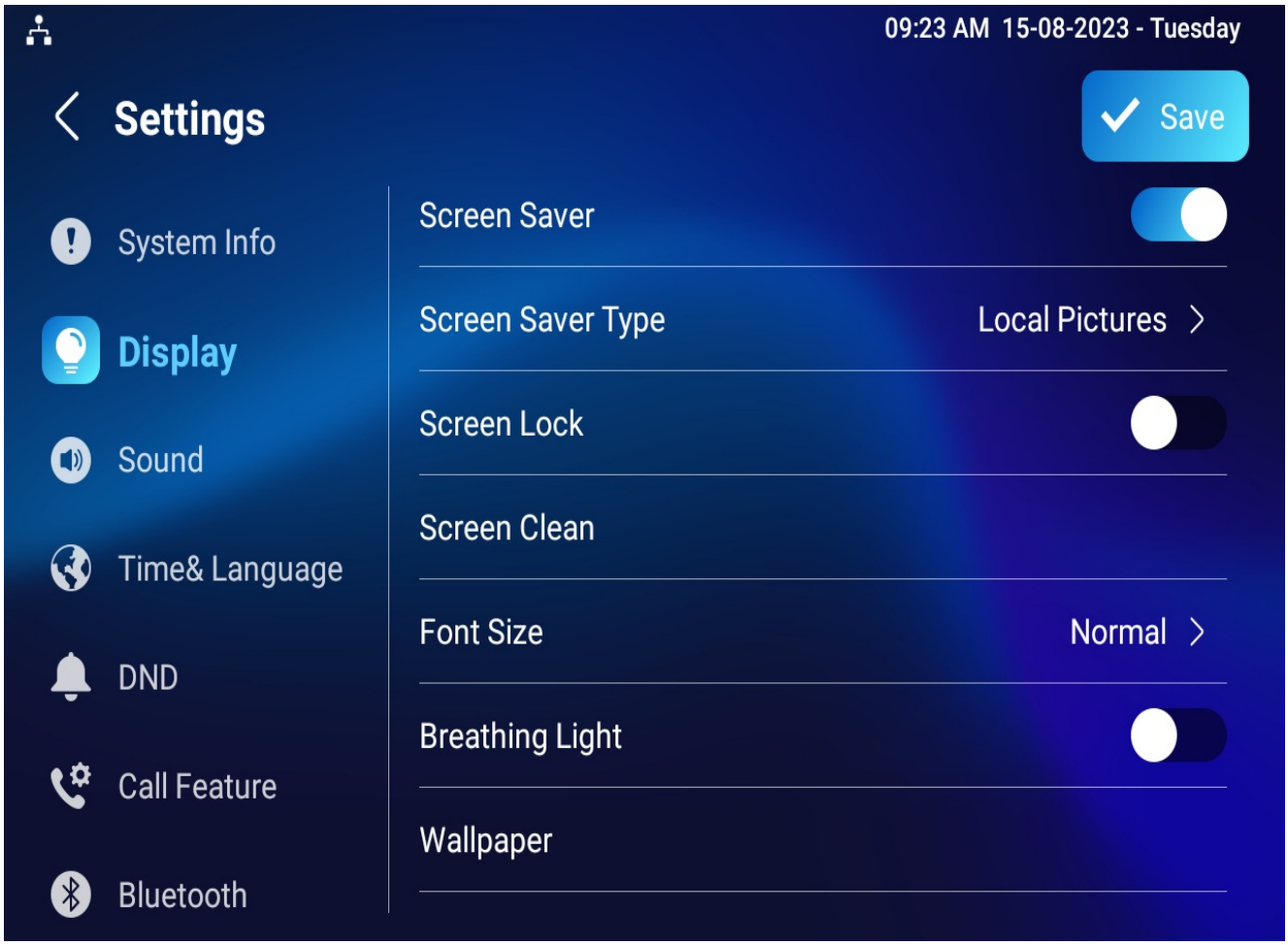
The device allows you to enjoy a variety of screen displays to enrich your visual and operational experience through customized settings to your preference.

Screen Display Setting on the Device

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

To do this configuration on device **Setting > Display** screen.





Parameter set-up:

- **Brightness**: move the bar to adjust the screen brightness. The default brightness is "145".
- **Sleep Time**: set the timing for the device screen to be turned off. You can select the timing among seven options: **15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes**, and **30 minutes**. For example, if you set it as 1 minute then the screen will be turned off if there is no operation on the device for 1 minute. However, if you turn on the function, then the device screen will not be turned off until the screen saver display reaches its configured time duration.
- **Screen Saver Time**: set the time duration for the screen saver among 9 options: **15seconds, 30seconds, 1minute, 2minutes, 5minutes, 10minutes, 30 minutes, 1 hour**, or **2 hours**. Screen saver starts when the device detects no operation, or no one is approaching.
- **Screen Saver**: tick the square box to enable the screen saver function.
- **Screen Saver Type**: select screen saver type among 7 options: **SDMC Pictures, Local Pictures, SDMC+Local Pictures, SDMC Videos, Local Videos, SDMC+Local Videos, Clock**.

Details for the screen saver types are shown below:

NO.	Screen Saver Type	Type Description
1	SDMC Pictures	Display pictures from SDMC as the screen saver.
2	Local Pictures	Display picture uploaded to the indoor monitor as the screen saver.
3	SDMC+Local Pictures	Display pictures from SDMC and the indoor monitor in rotation as the screen saver.
4	SDMC Videos	Display videos from SDMC as the screen saver.
5	Local Videos	Display videos from the indoor monitor as the screen saver
6	SDMC+Local Videos	Display videos from SDMC and the door phone in rotation as the screen saver.
7	Clock	Display the clock as the screen saver.

- **Screen Lock**: tick the screen lock if you want to lock the screen after the screen is turned off (turn dark). You are required to enter the system code to unlock the screen or you can unlock the screen by facial recognition.
- **Screen Clean**: press **Screen Clean** first before you start wiping the screen clean. And this helps you avoid unwanted changes in the settings incurred while you are wiping the screen.
- **Font Size**: select the font size among four options **Small, Normal, Large**, and **Huge** according to your need.
- **Breathing Light**: move the toggle switch to enable the breathing light.
- **Wallpaper**: click to select the local wallpaper.

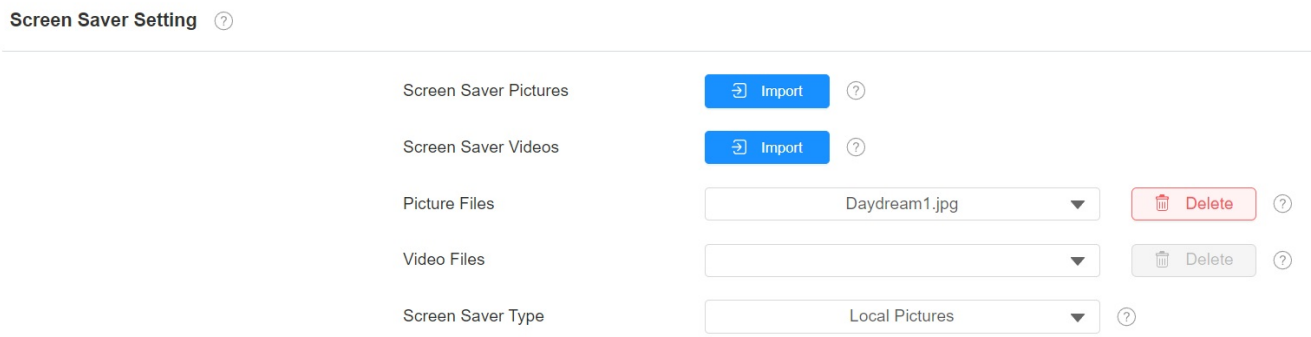
Screen Display Setting on the Web Interface

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 separately or in batches to the device and to the device web interface for publicity purposes or for a greater visual experience.

Navigate to **Device > Display Setting > Screen Saver Setting**



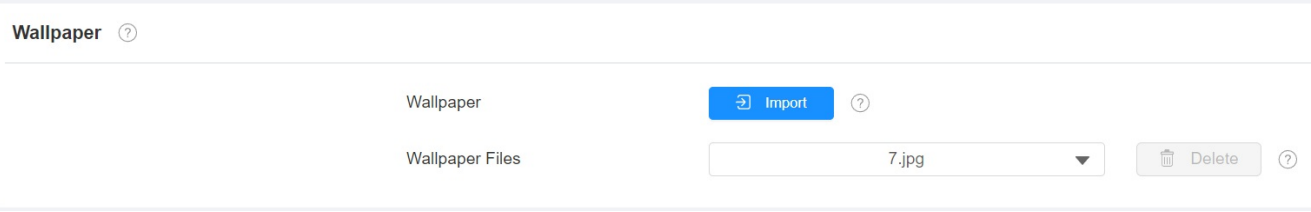
Note:

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

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 > Wall Paper**



Note:

- The pictures uploaded should be in JPG, JPEG, or PNG format with 2M maximum.

Upload Device Booting Image

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

You can go to **Device > Display Setting> Boot Logo**.

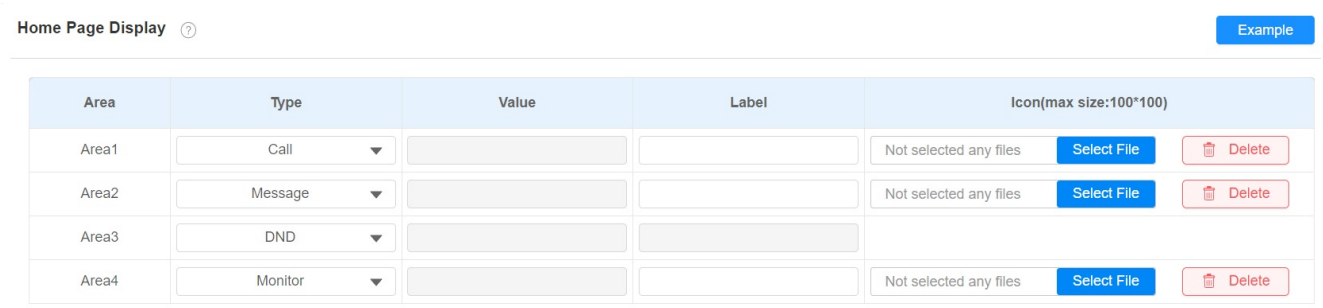
Note:

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

Icon Screen Display Configuration

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

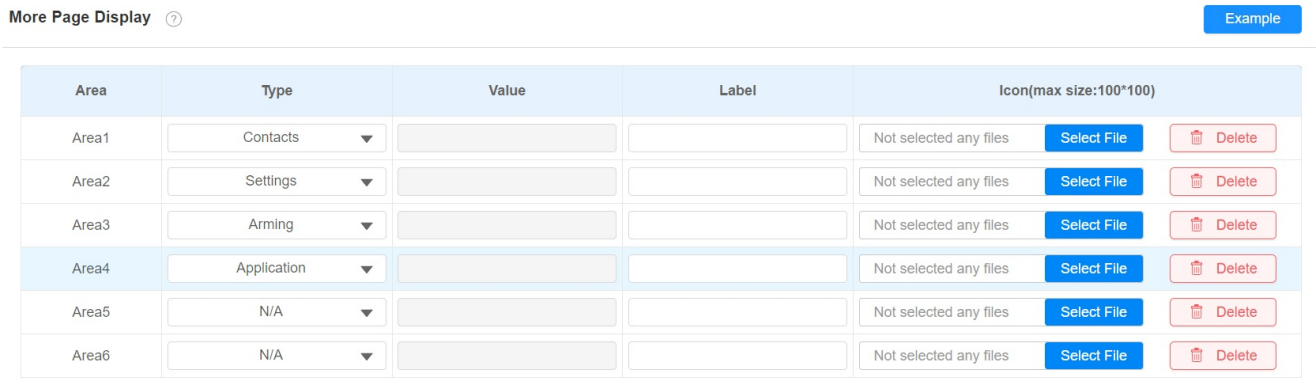
To set it up, go to **Device > Display Setting > Home Page Display** interface.



Parameter Set-up:

- **Type**: click to select among eighteen icon options: **DND, Message, Contact, Call, System info, Setting, Arming, SOS, Browser, Custom APK, Monitor, Lift, Relays, Unlock, All calls, Control4 Unlock, Application, N/A** is selected, the icon display in the corresponding area will disappear.
- **Value**: **select** the value if you select the icon type **Custom APK** and **Browser**. For example, when you select **Custom APK**, choose **Home Center** in the corresponding **Value** field before the APK icon can be displayed on the home screen. If **Browser** is selected, you are required to enter the URL of the browser before the browser icon can be displayed. while the value is not applicable to other icon types.
- **Label**: click to rename the icon if you need, while DND icon cannot be renamed.
- **Icons**: click to select the picture to be uploaded as the icon to be displayed. The maximum icon size is 50 * 50.The picture format can be JPG, JPEG and PNG.

To configure the more icon display on **More Page Display** on the same interface.



Note:

- You can configure 4 icons in 4 areas on the home screen.
- You can configure 6 icons in 6 areas on the **More** screen.

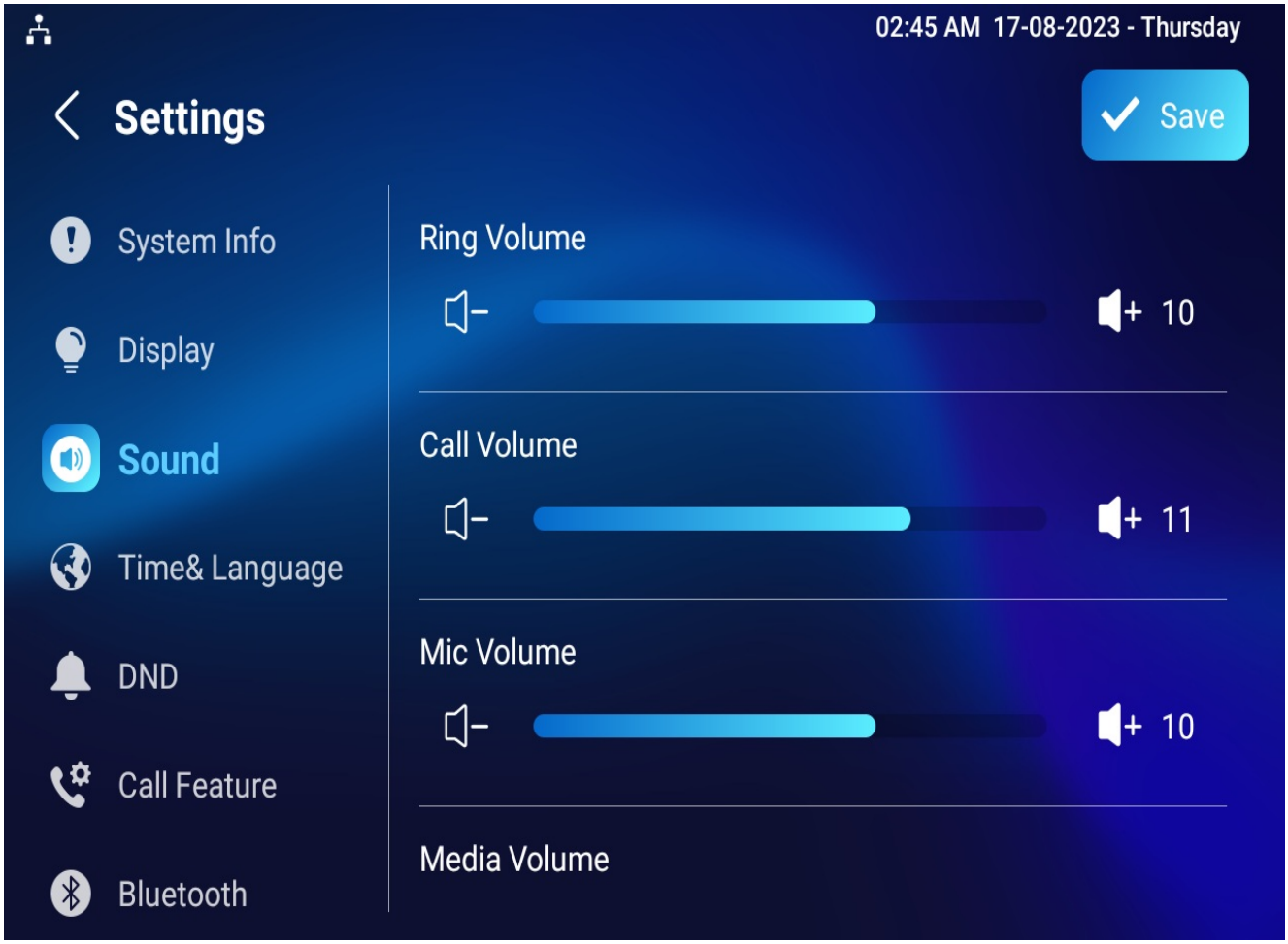
Sound and Volume Configuration

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

Volume Configuration

Configure Volume on the Device

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



Parameter Set-up:

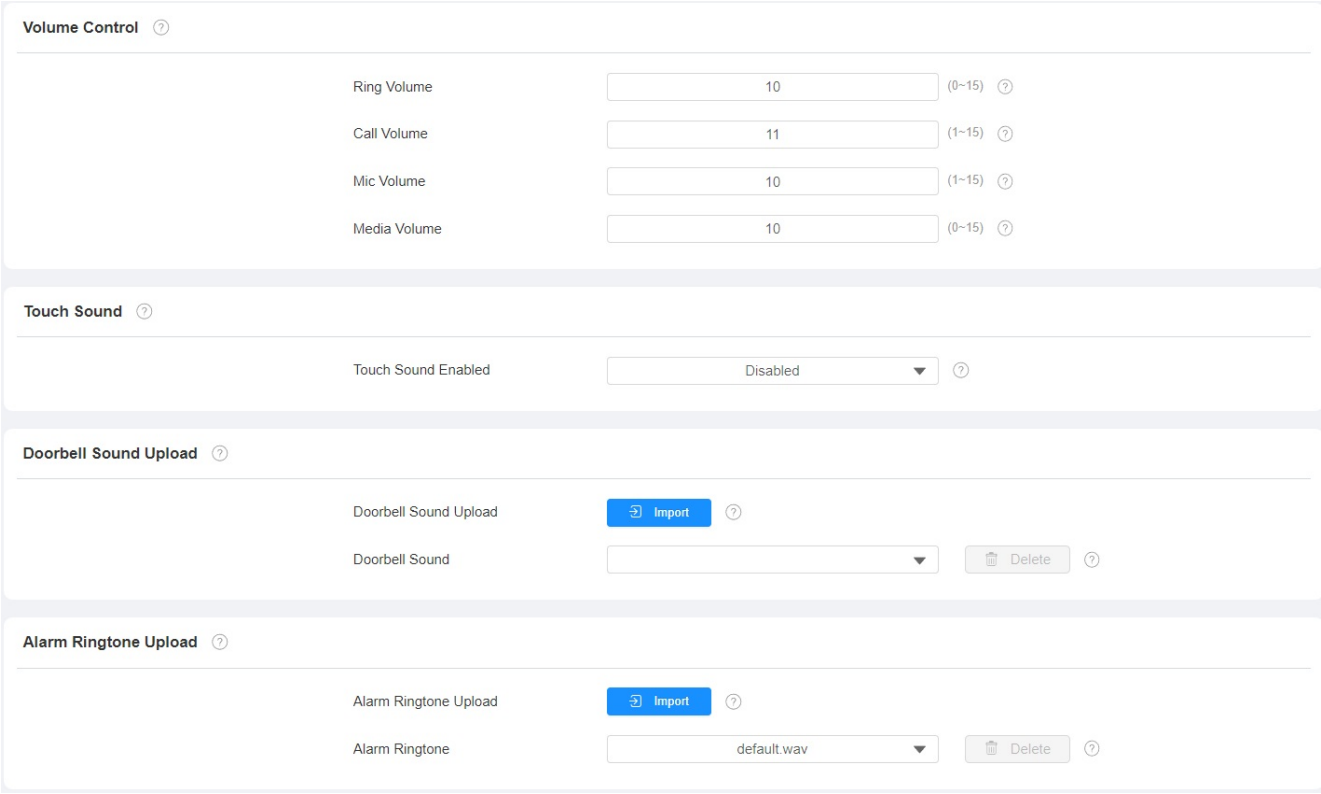
- **Ring Volume**: adjust the incoming call ringtone volume.
- **Call Volume**: adjust the speaker volume during the call.
- **Mic Volume**: adjust the volume of your voice to be heard.
- **Media Volume**: adjust the volume for the video screen saver.

- **Phone Ringtone**: select ringtone for incoming calls.
- **Notification Sound**: select ringtone for the incoming messages.

Configure Volume on the Web Interface

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

Go to **Device > Audio > Volume Control** interface.



Note:

- Doorbell Sound and Alarm Ringtone files to be uploaded must be **.WAV** or **MP3** format. No limitation on the file size.

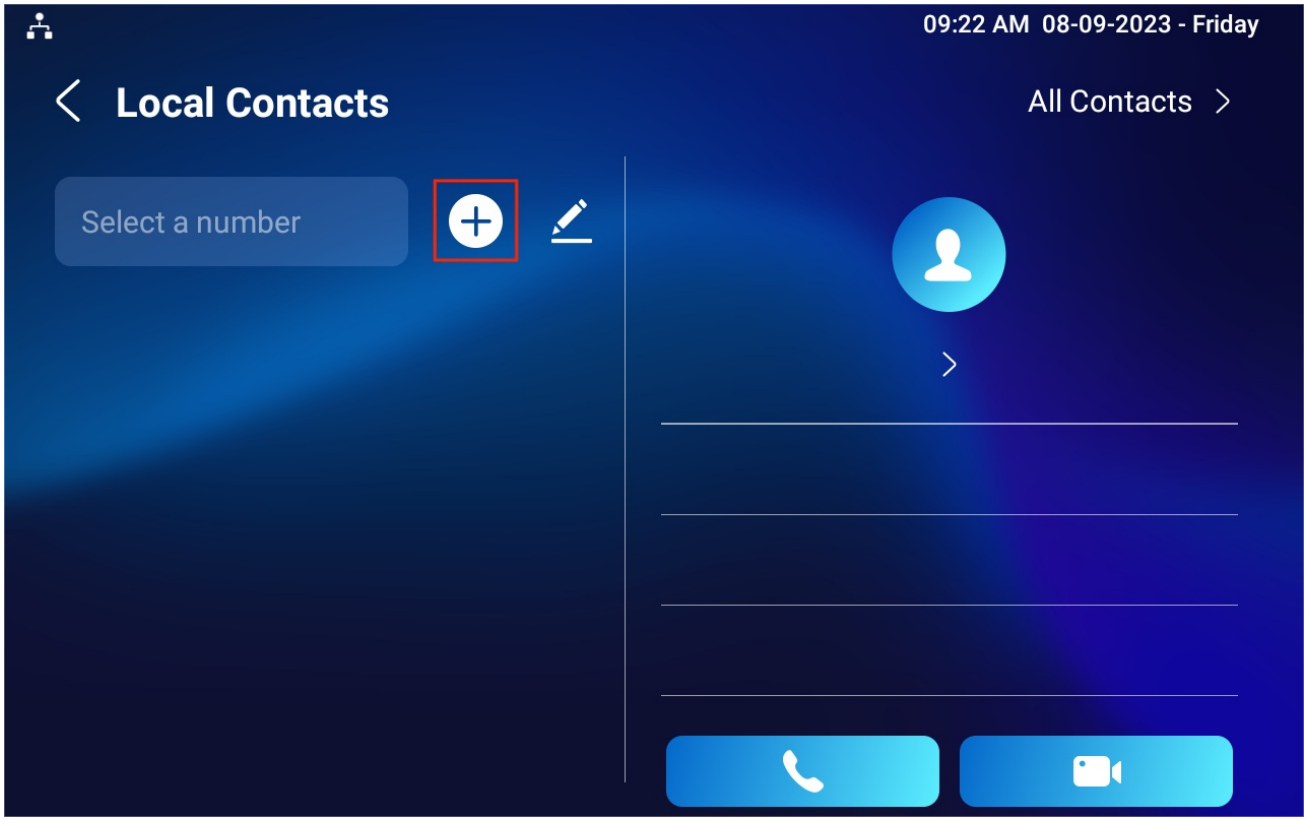
Phone Book Configuration

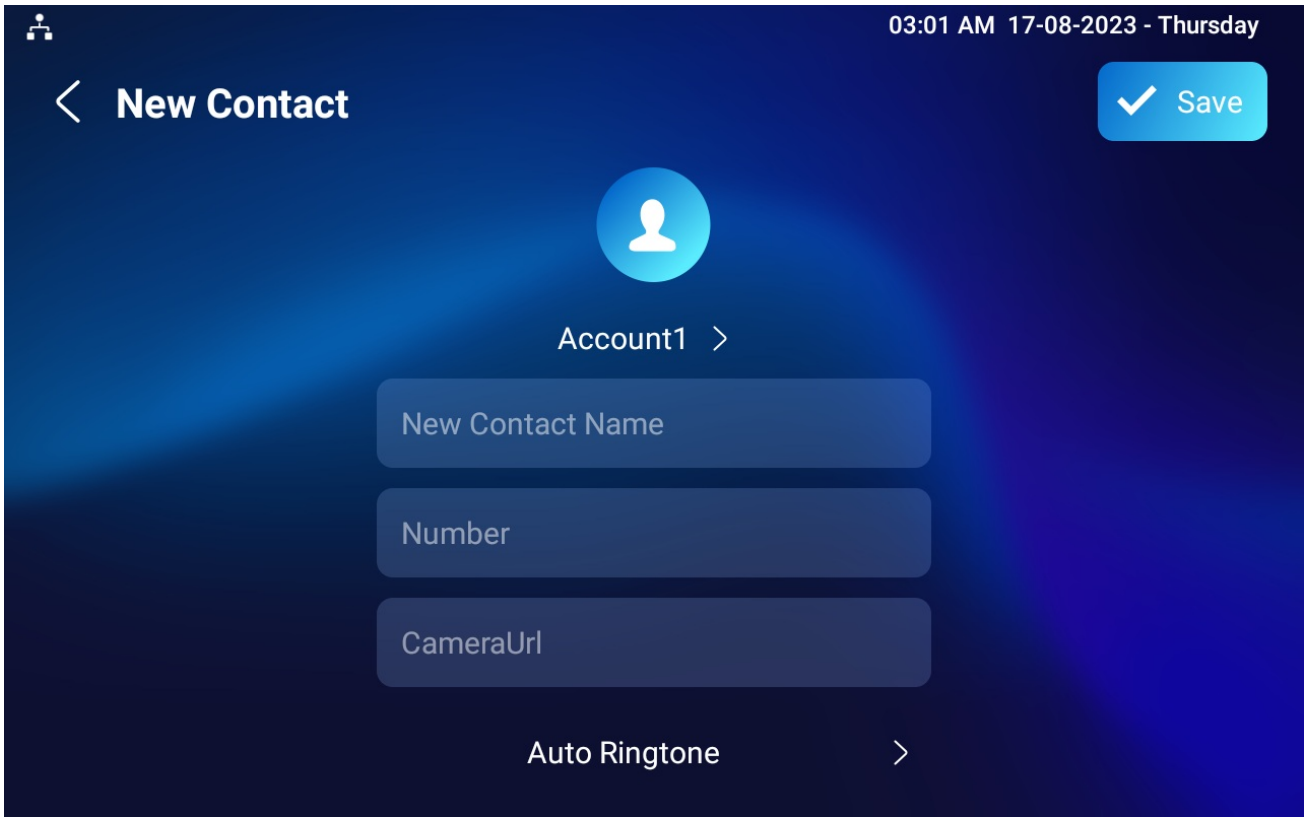
Phone Book Configuration on the Device

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

Add Contact

Go to **Contacts > Local Contacts** screen, and then press the **Add** icon.





Parameter Set-up:

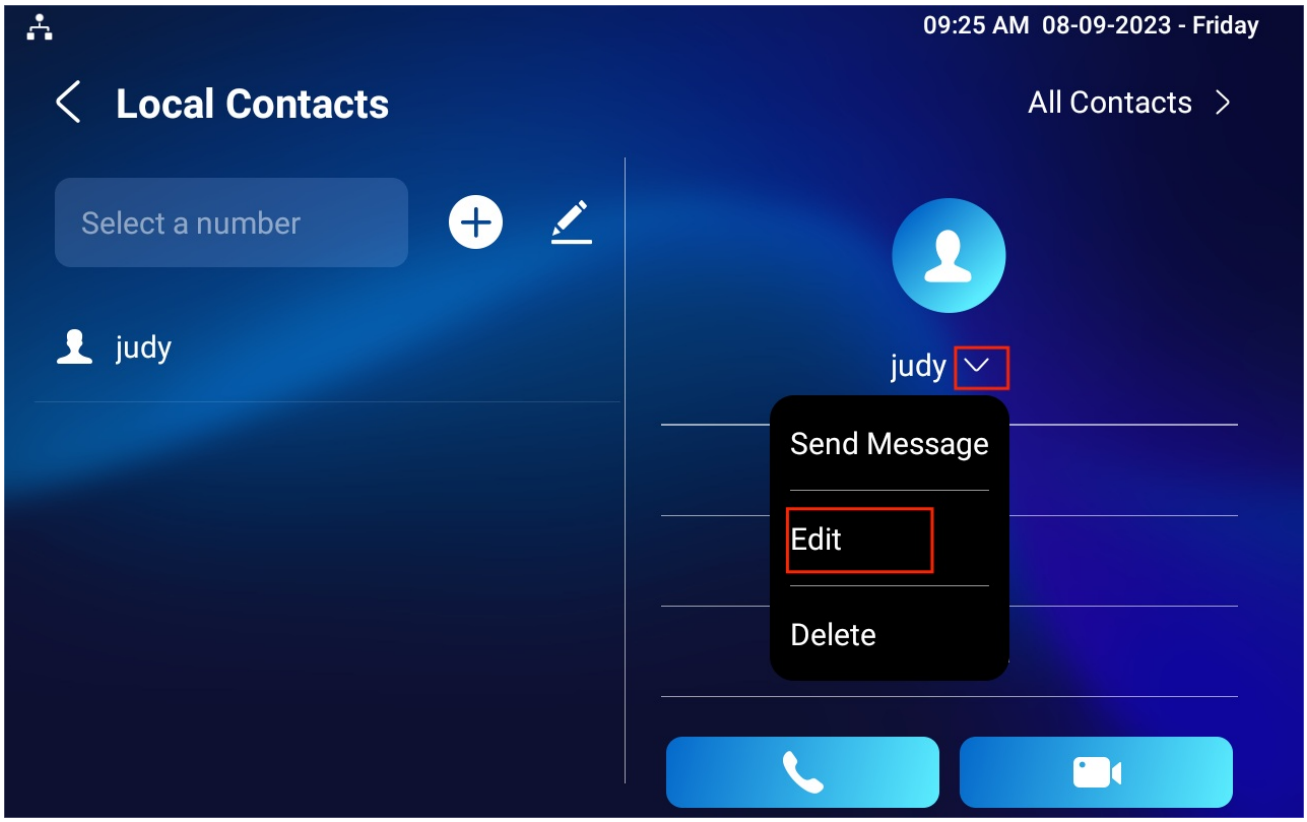
- **Account1**: select which account to dial out, Account 1 or Account 2.
- **New Contact Name**: enter the name.
- **Number**: enter the IP or SIP number.
- **CameraUrl**: enter the RTSP URL for video preview.

Note:

- Akuvox device RTSP URL format is **rtsp://device IP/live/ch00_0**. if you use a third-party device, please confirm the URL format with third-party service providers.

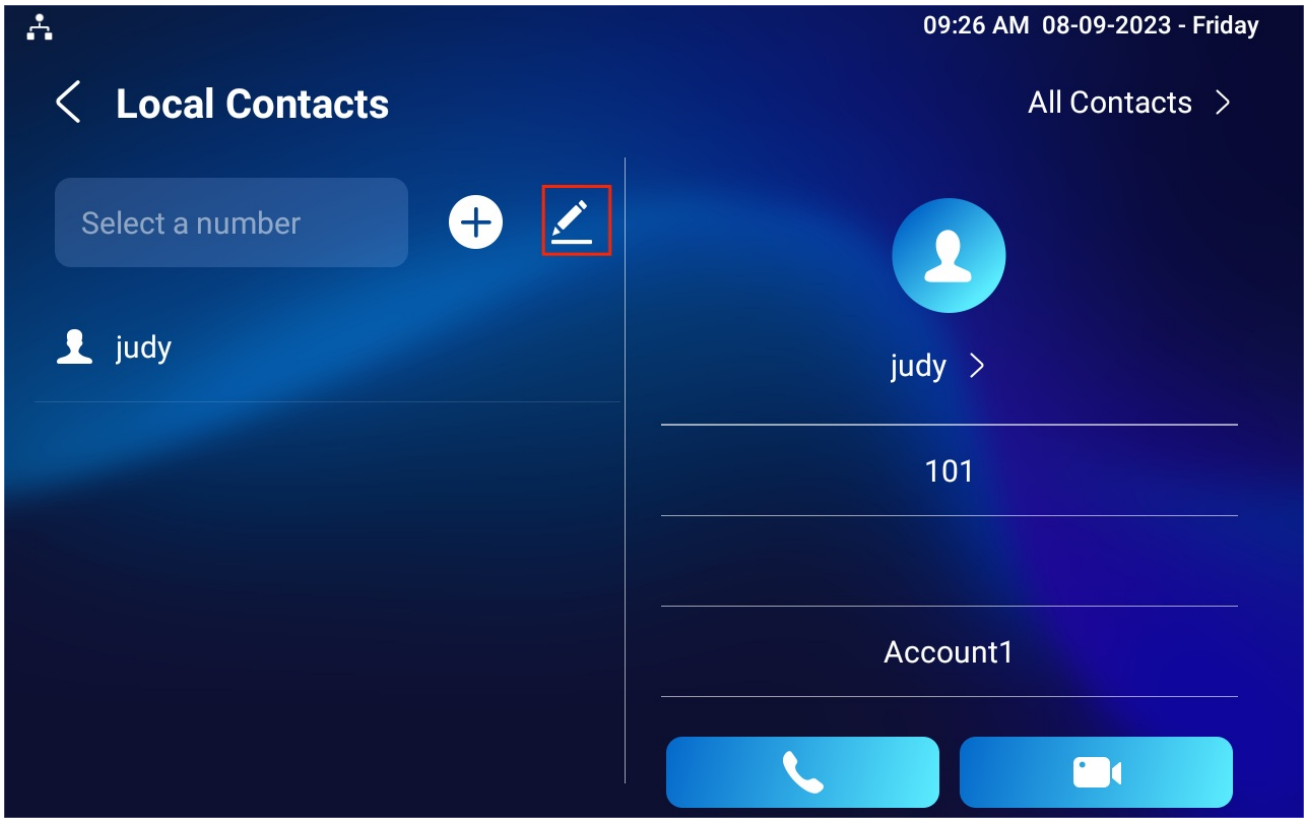
Edit Contact

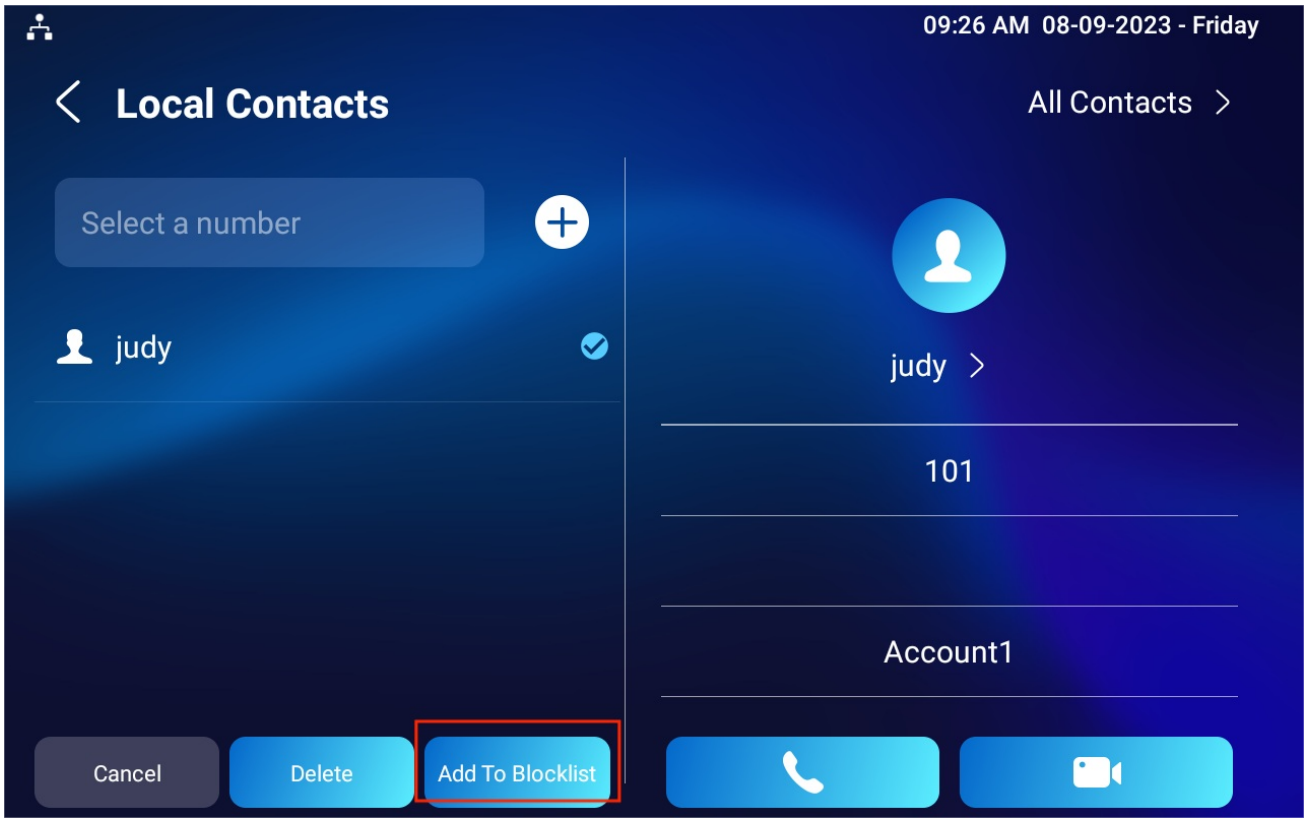
You can check and edit the existing contacts in the phonebook list. Choose one and press **Edit** to modify.



Block List setting on the device

Choose which contact on the contact list you want to be added to the blocklist. Press the **Edit** icon first and then **Add To Blocklist**.





Note:

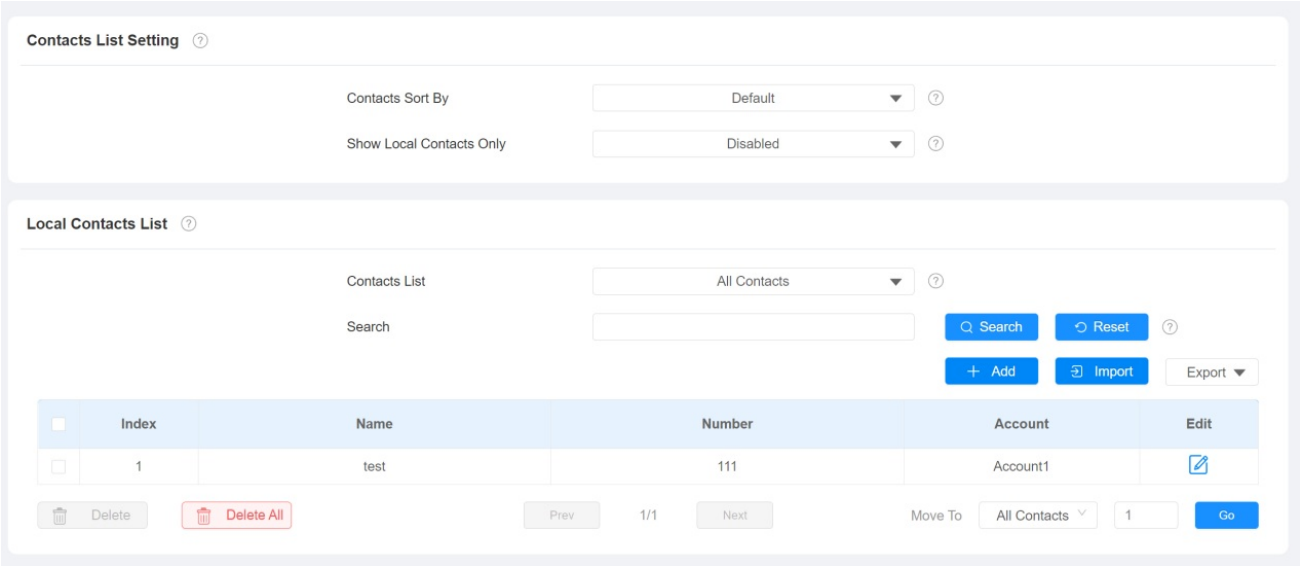
- You can delete contacts regardless of whether it is on the **All Contacts** screen or the **Blocklist** screen.

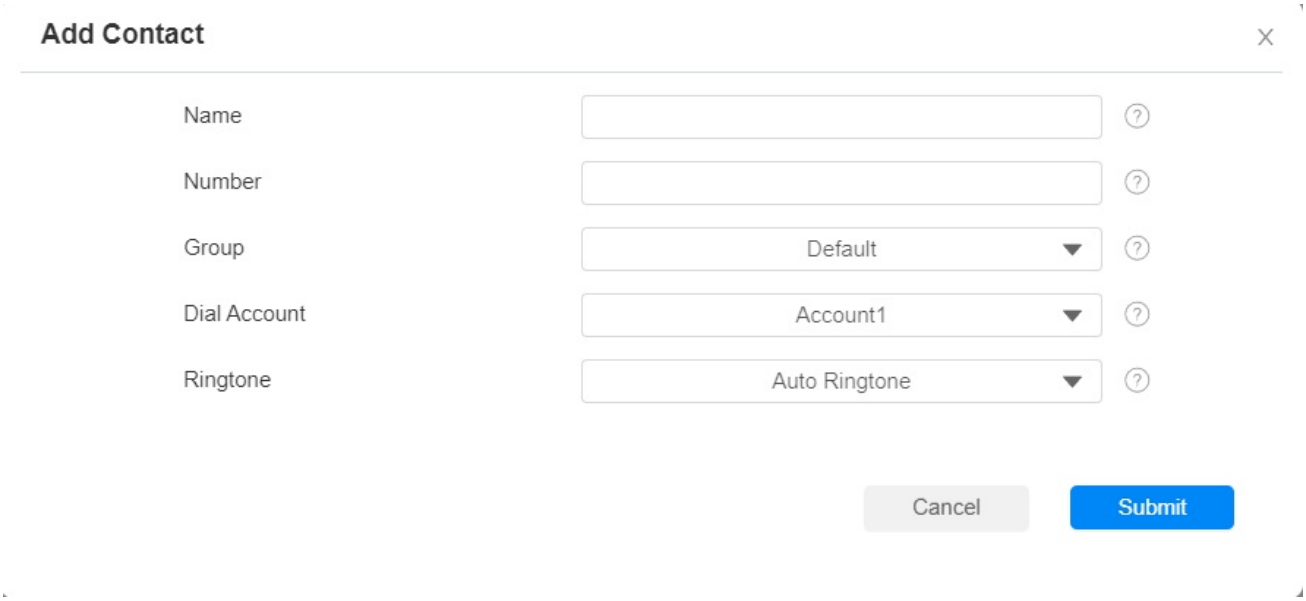
Phone Book Configuration on the Web Interface

Contact Configuration

To conduct contact configuration on the web interface. The existing contacts will show in the below list after they are added. Press + Add to add a contact.

Go to **Contacts > Local Contacts > Local Contacts List**.





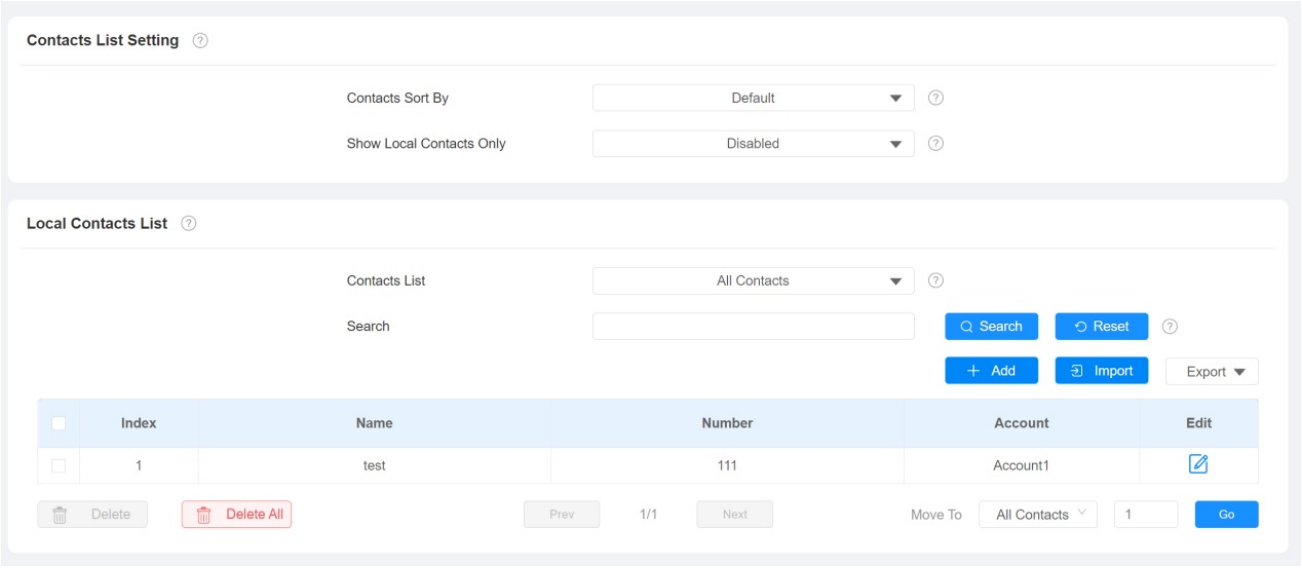
Parameter set-up:

- **Name**: enter the contact name.
- **Number**: enter the contact number (SIP or IP number).
- **Group**: select Default or Blocklist group.
- **Dial Account**: select Account 1 or Account 2.
- **Ringtone**: select the ringtone to hear when receiving the call from the contact.

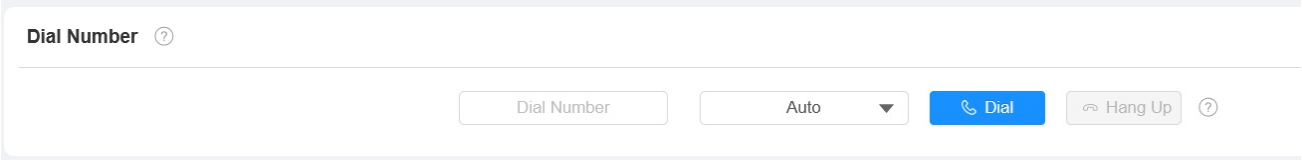
Contact Management

You can search, display, edit, and delete the contacts in your contacts list on the web.

Go to **Contacts > Local Contacts > Local Contacts List**. Press  to edit a contact.



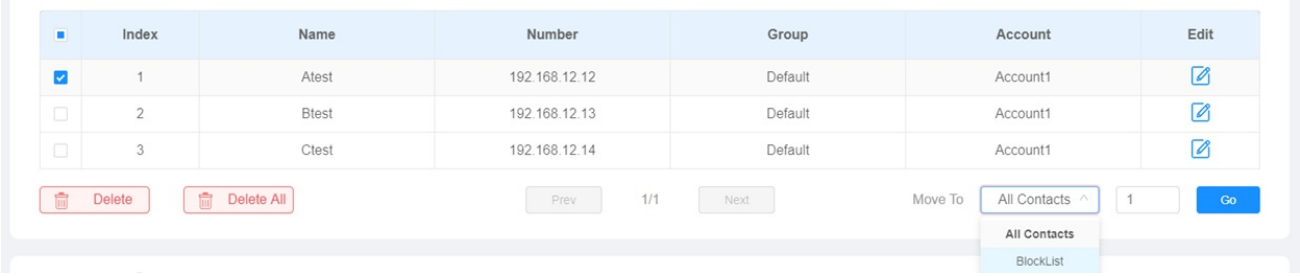
You can dial out using the contact phone number on **Contacts > Local Contacts > Dial Number** interface.

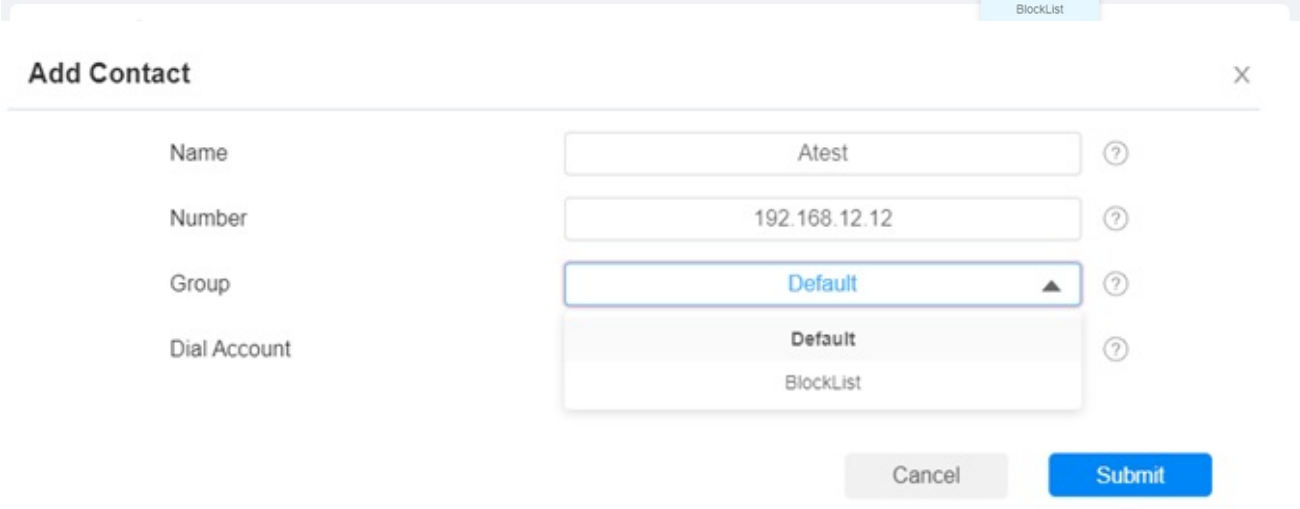


Block List Setting on the Web Interface

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

Go to **Contacts > Local Contacts**.





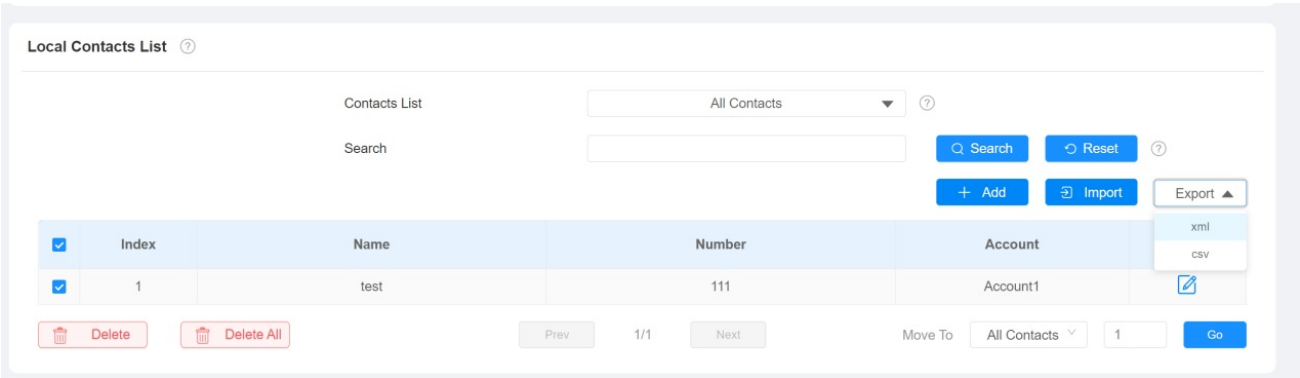
Note:

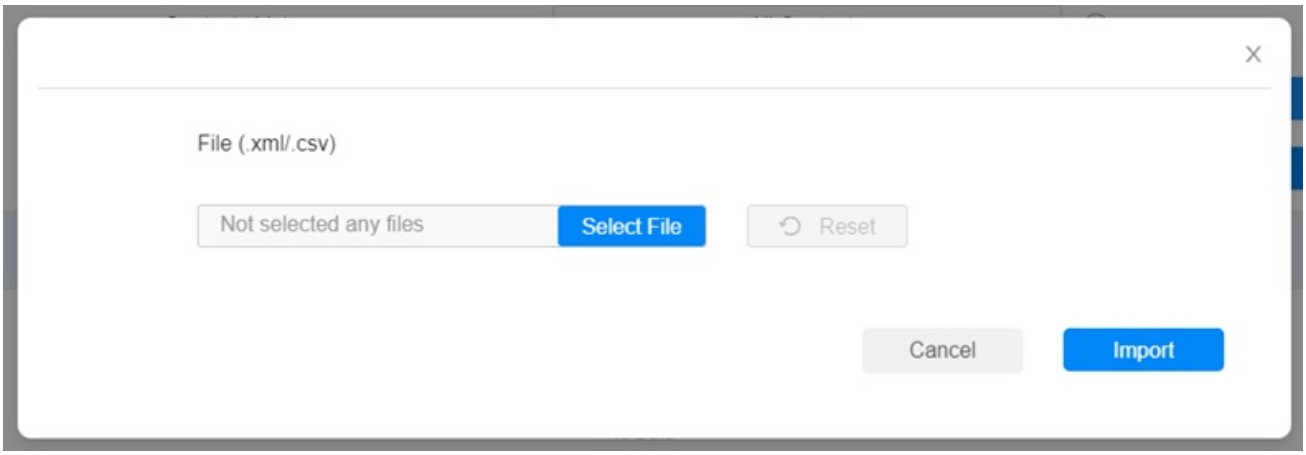
- If you want to remove the contact from the blocklist on the web interface, you can change the group to **Default** when editing the contact.

Contacts Import and Export on the Web Interface

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

Go to **Contacts > Local Contacts > Local Contacts List** interface.





Note:

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

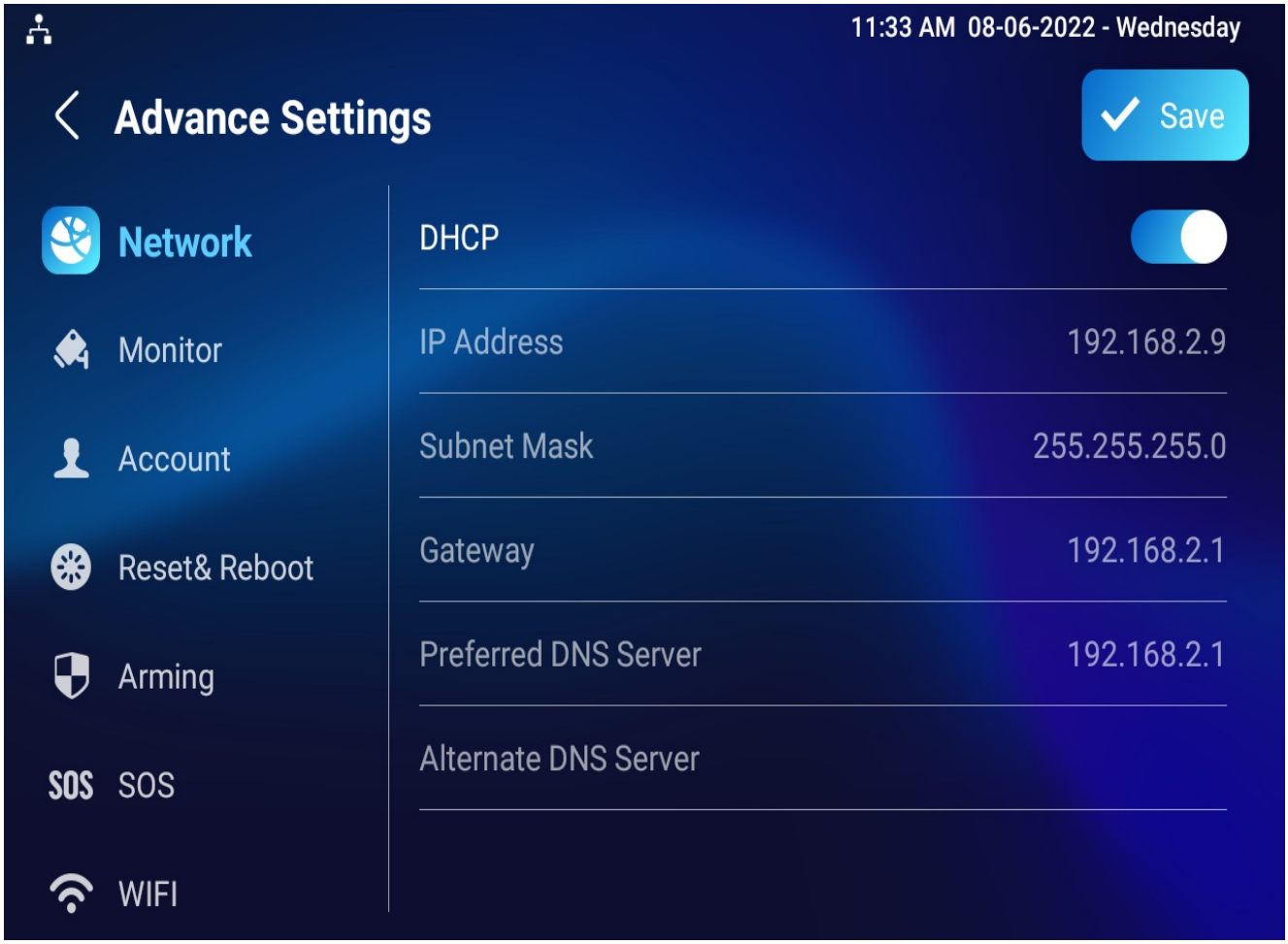
Network Setting & Other Connection

Device Network Configuration

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

Configure Device Network Connection on the Device

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



Parameter Set-up:

- **DHCP**: select the **DHCP** mode by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the device will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS

server address automatically.

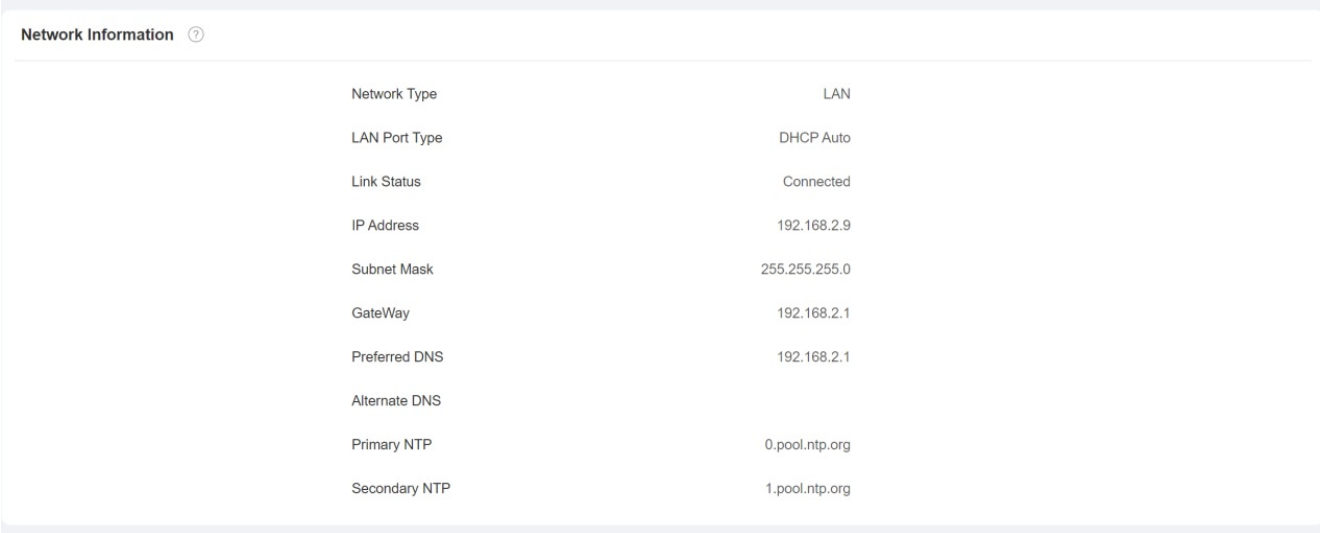
- **Static IP**: select the static IP mode by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to your actual network environment.
- **IP Address**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Preferred&Alternate DNS Server**: set up a preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address while the alternate DNS server is the secondary server address and the device will connect to the alternate server when the primary DNS server is unavailable.

Note:

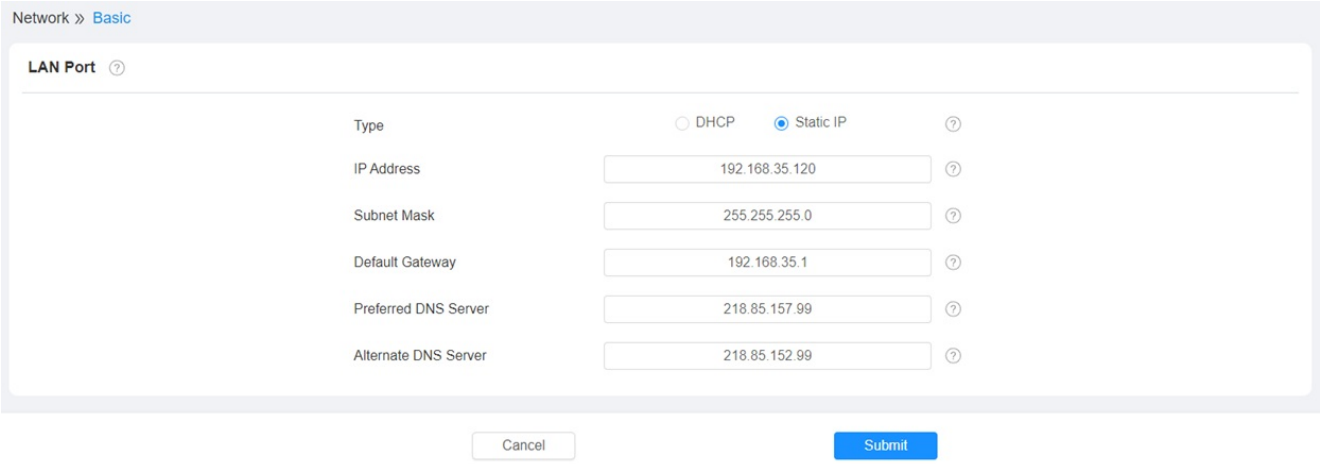
- You can press **System Info** and then press **Network** tab on the **Settings** screen to check the device network status.
- The default system code to enter advanced settings is **123456**.

Configure Device Network Connection on the Web Interface

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



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



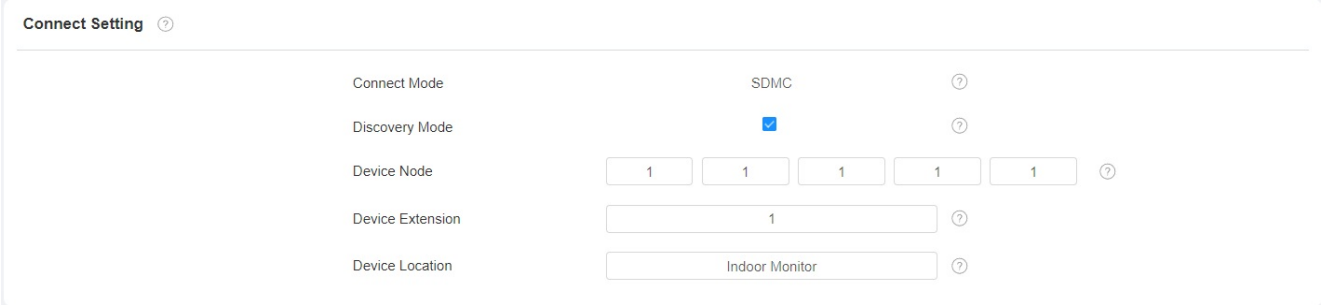
Parameter Set-up:

- **DHCP**: select the DHCP mode by checking the DHCP box. DHCP mode is the default network connection. If the DHCP mode is selected, then the indoor monitor will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP**: When static IP mode is selected, 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**: set up the IP address if the static IP mode is selected.
- **Subnet Mask**: set up the subnet mask according to your actual network environment.
- **Default Gateway**: set up the correct gateway according to the IP address.
- **Preferred/Alternate DNS Server**: set up DNS (**Domain Name Server**) according to your actual network environment. Preferred DNS Server is the primary DNS server address while the **Alternate DNS Server** is the secondary server address and the door phone connects to the alternate DNS server when the preferred DNS server is unavailable.

Device Deployment in Network

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

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



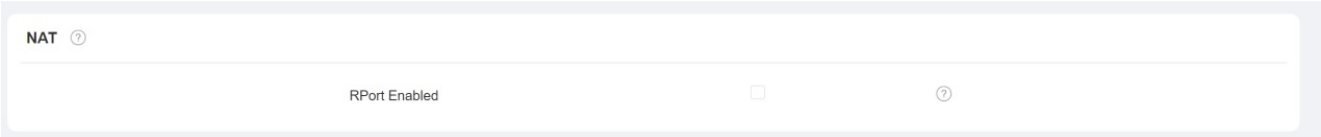
Parameter Set-up:

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

Device NAT Setting

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

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



Parameter Set-up:

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

Device Bluetooth Setting

Device Bluetooth Pairing

After X933 series indoor monitors turn on the Bluetooth on the device **Settings > Bluetooth** screen, it can be paired with other devices via Bluetooth.

Device Bluetooth Data Transmission

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

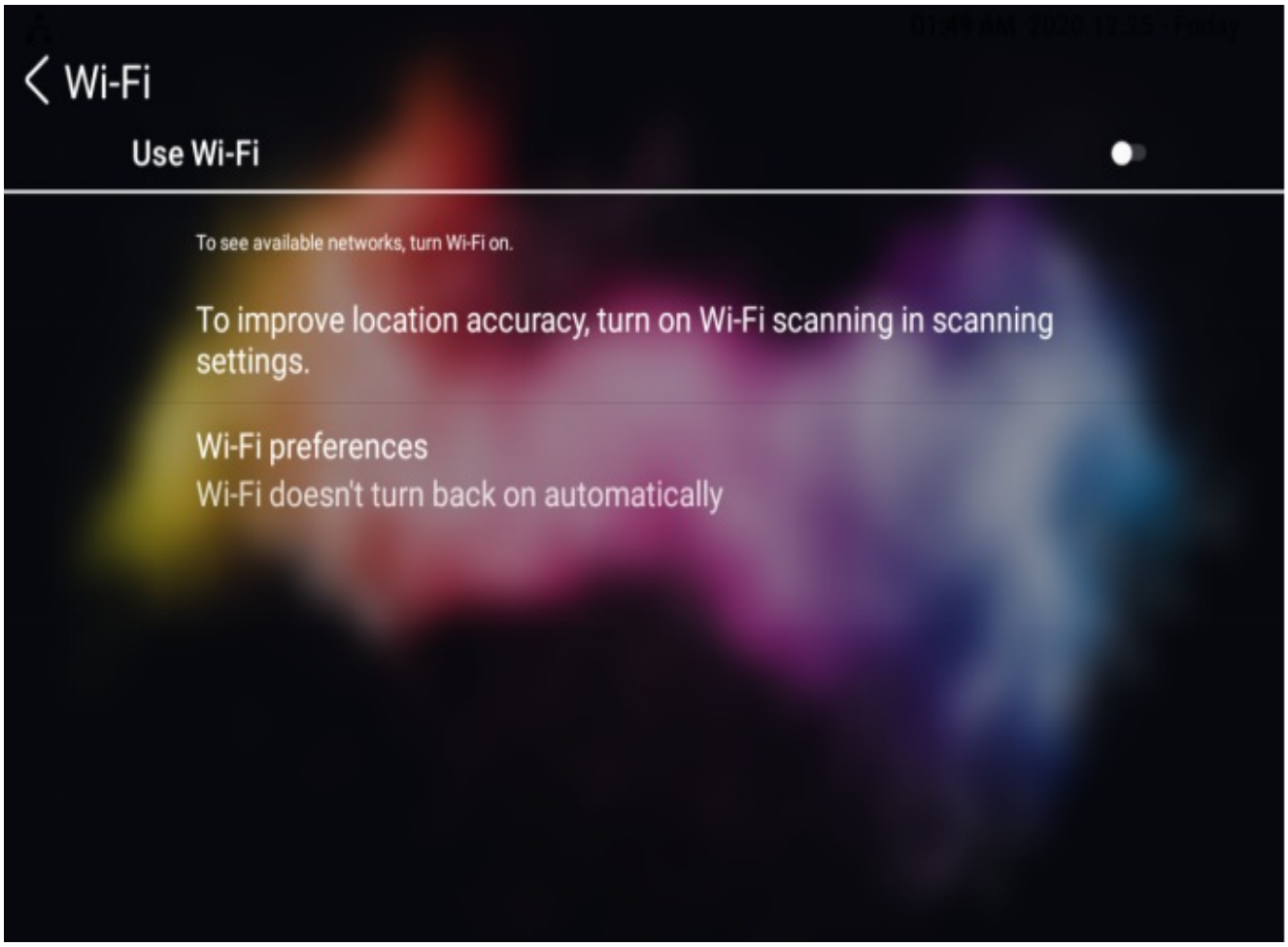

06:30 AM 17-08-2023 - Thursday
Bluetooth
On
Device name
X933
Previously connected devices
Pair new device
When Bluetooth is turned on, your device can communicate with other nearby Bluetooth devices.

Note:

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

Device Wi-Fi Setting

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



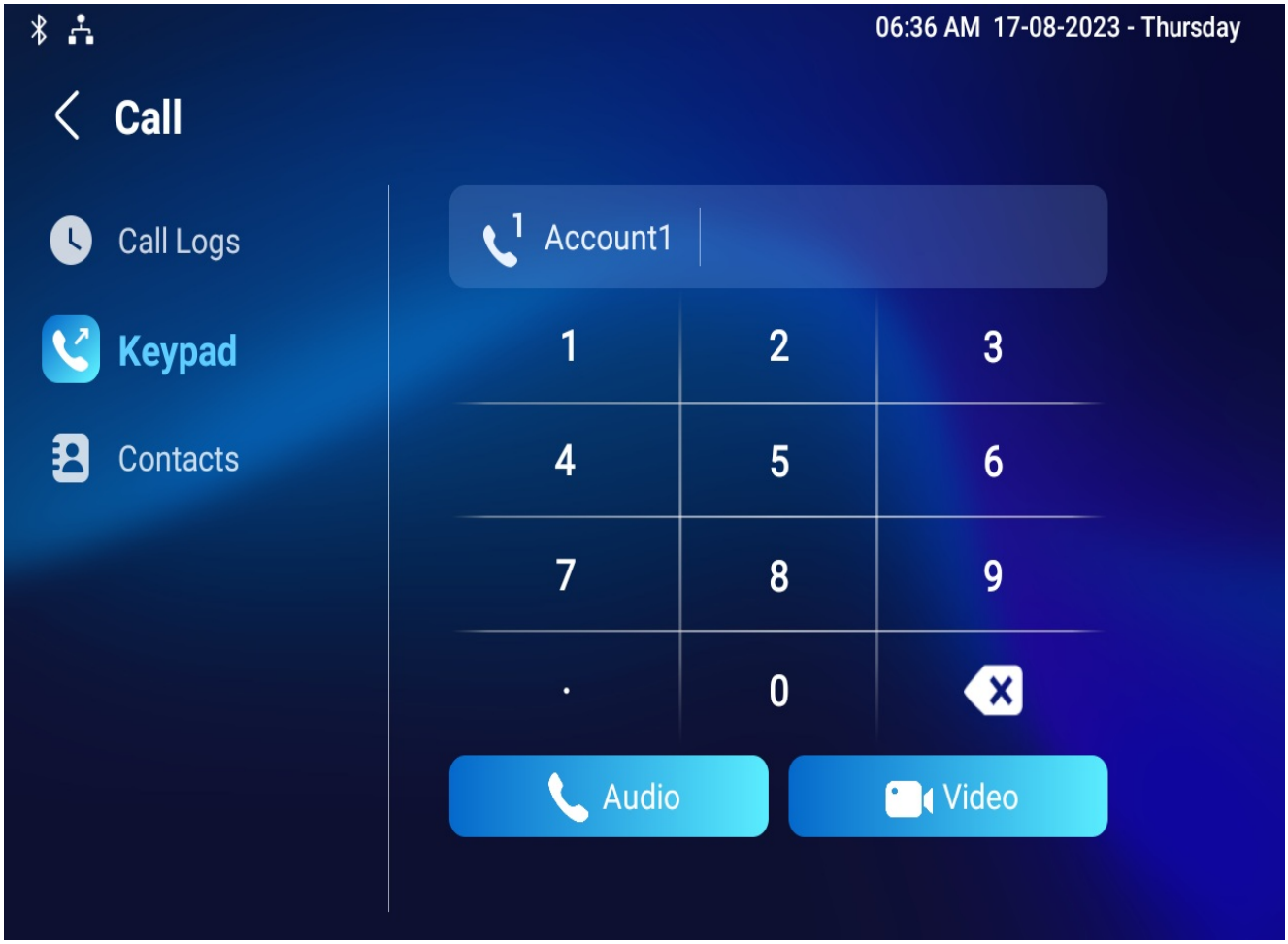
Intercom Call Configuration

IP Call & IP Call Configuration

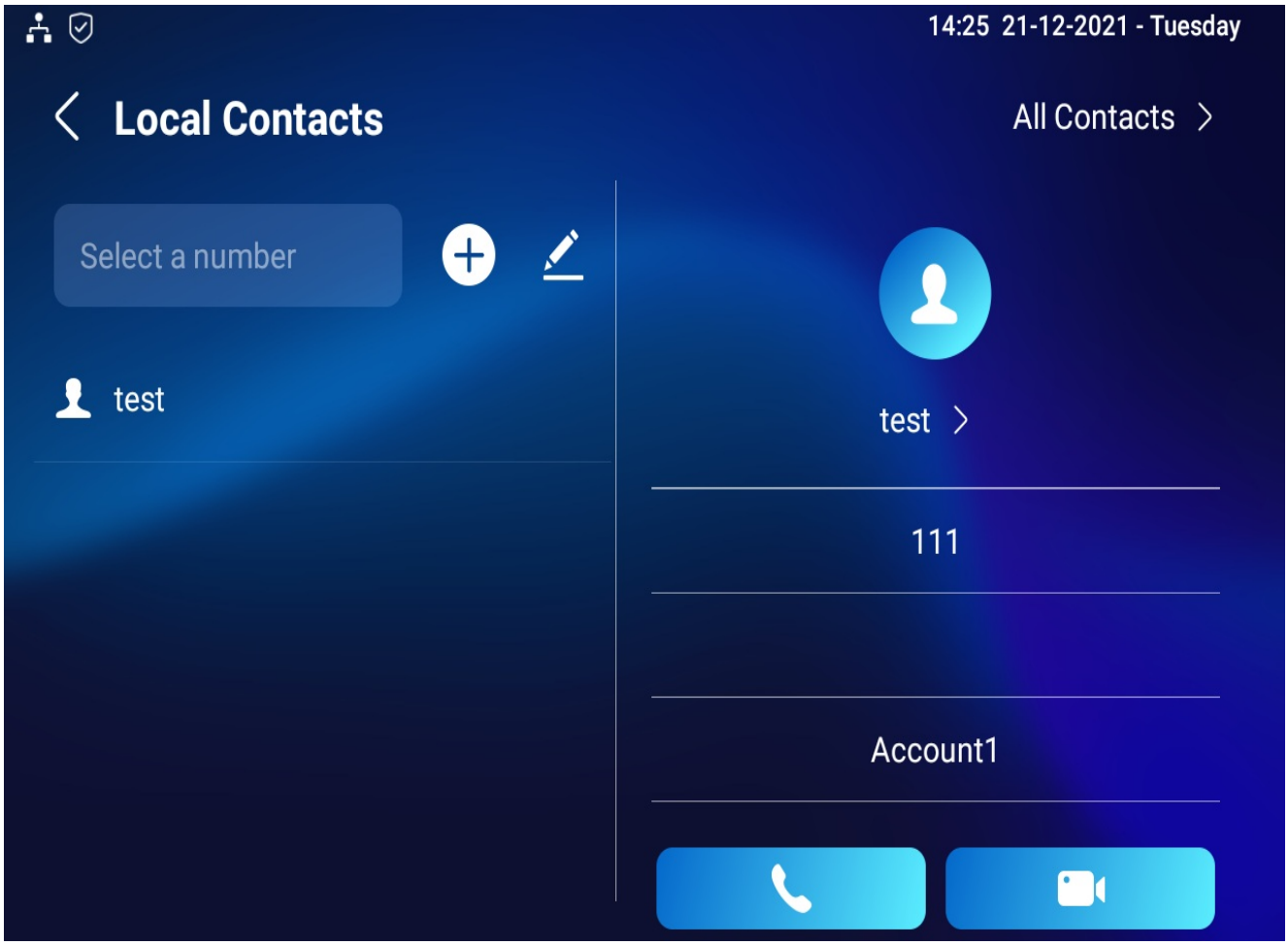
An IP call is a direct call between two intercom devices using their IP addresses, without a server or a PBX. IP calls work when the devices are on the same network.

Make IP Calls

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

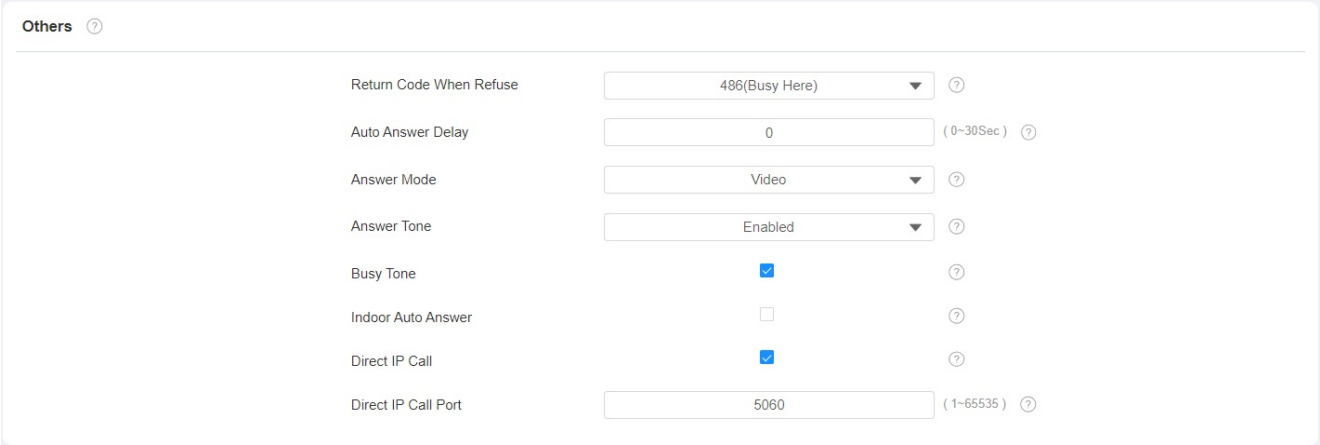


In addition, you can also make IP calls on the **Local Contacts** screen.



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**: tick the check box to enable the direct IP call. For example, if you do not allow direct IP call 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 the port range from 1-65535. If you enter any values within the range other than the 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

SIP Call & SIP Call Configuration

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

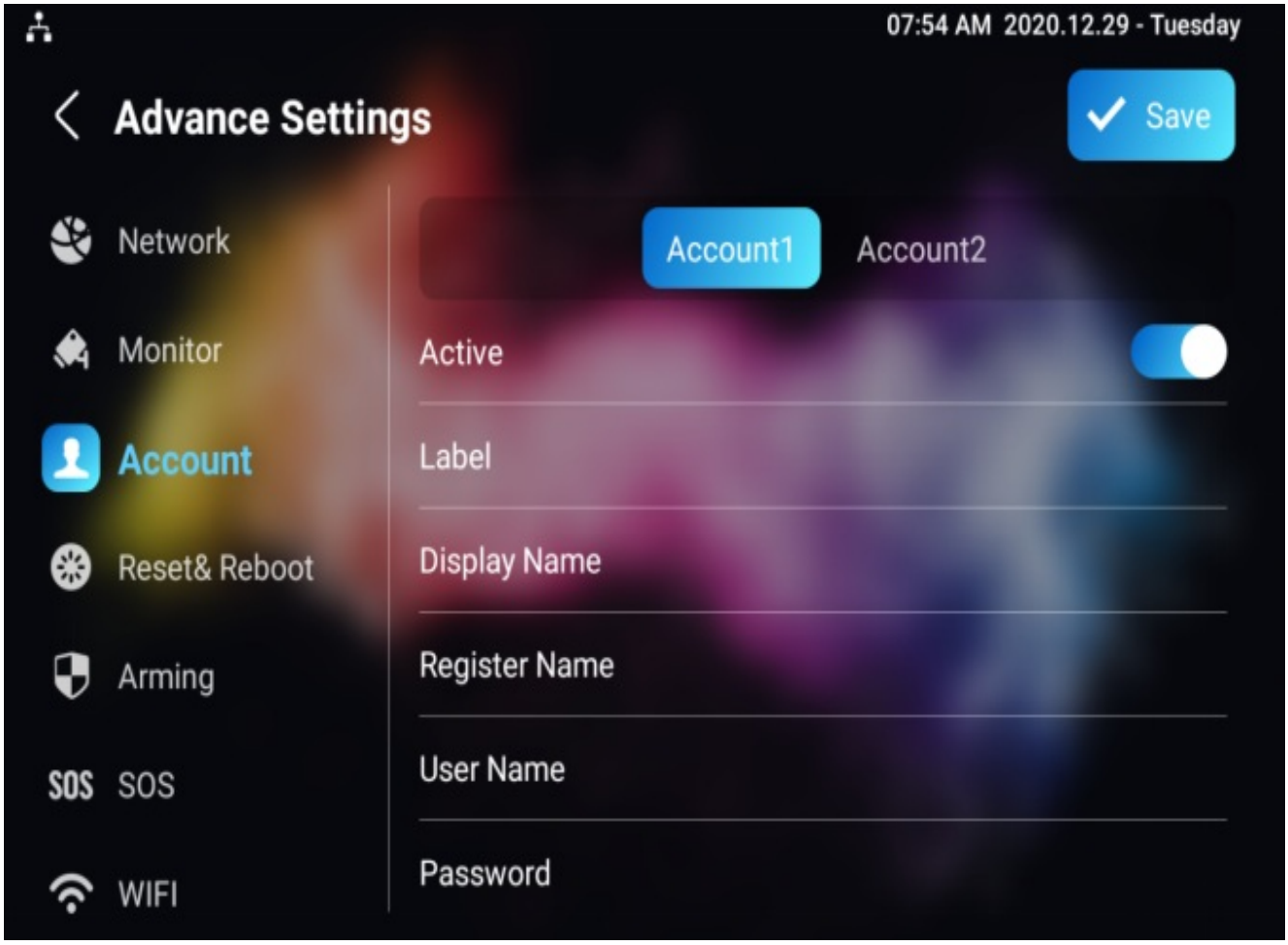
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

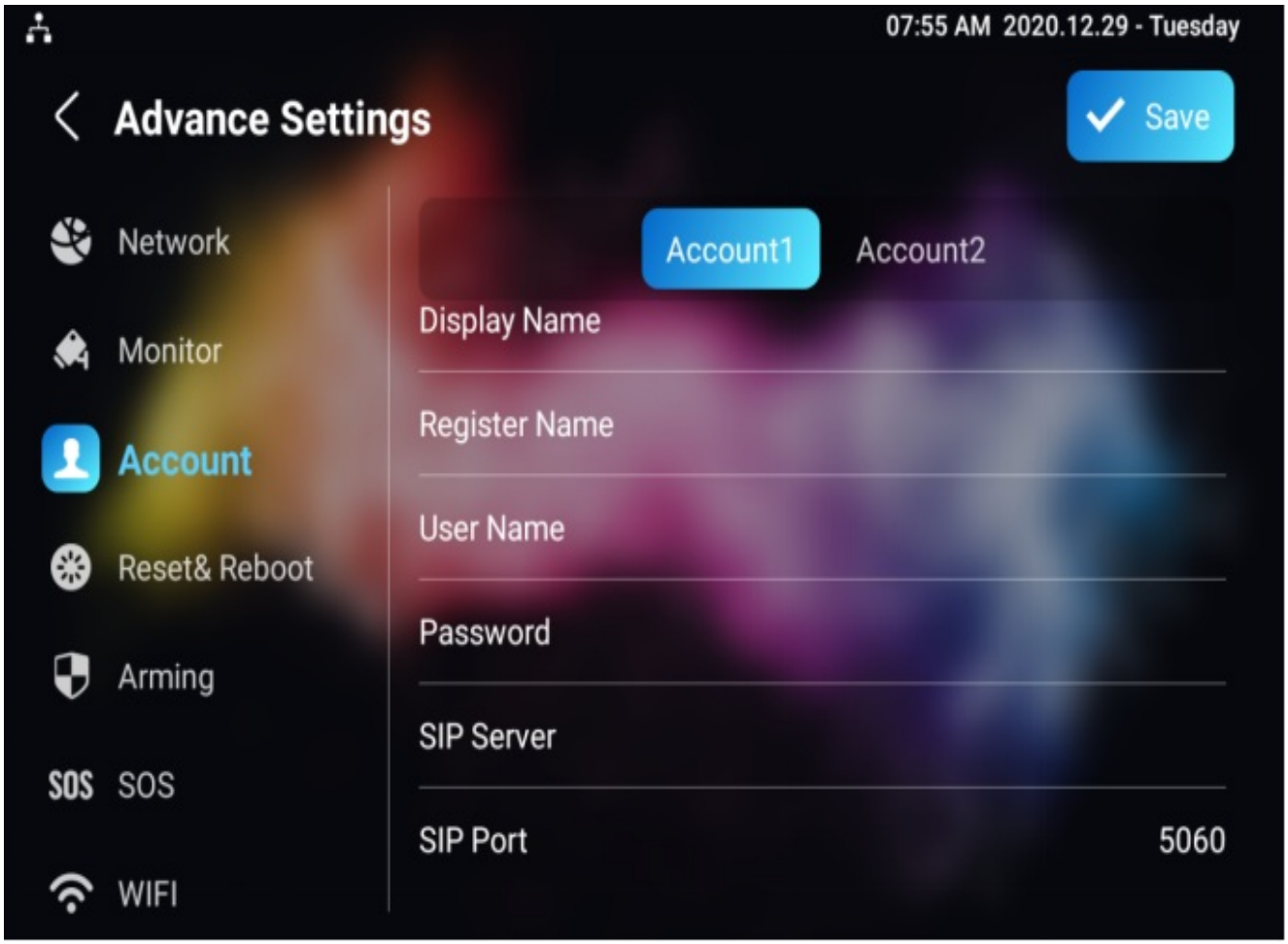
SIP Account Registration

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

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

To configure the SIP account on the device **Settings > Advance Settings > Account** screen. If you register a SIP account from a third-party device, obtain the **Register Name, User Name**, **Password**, **SIP Server**, and **SIP Port** from the third-party SIP service provider.

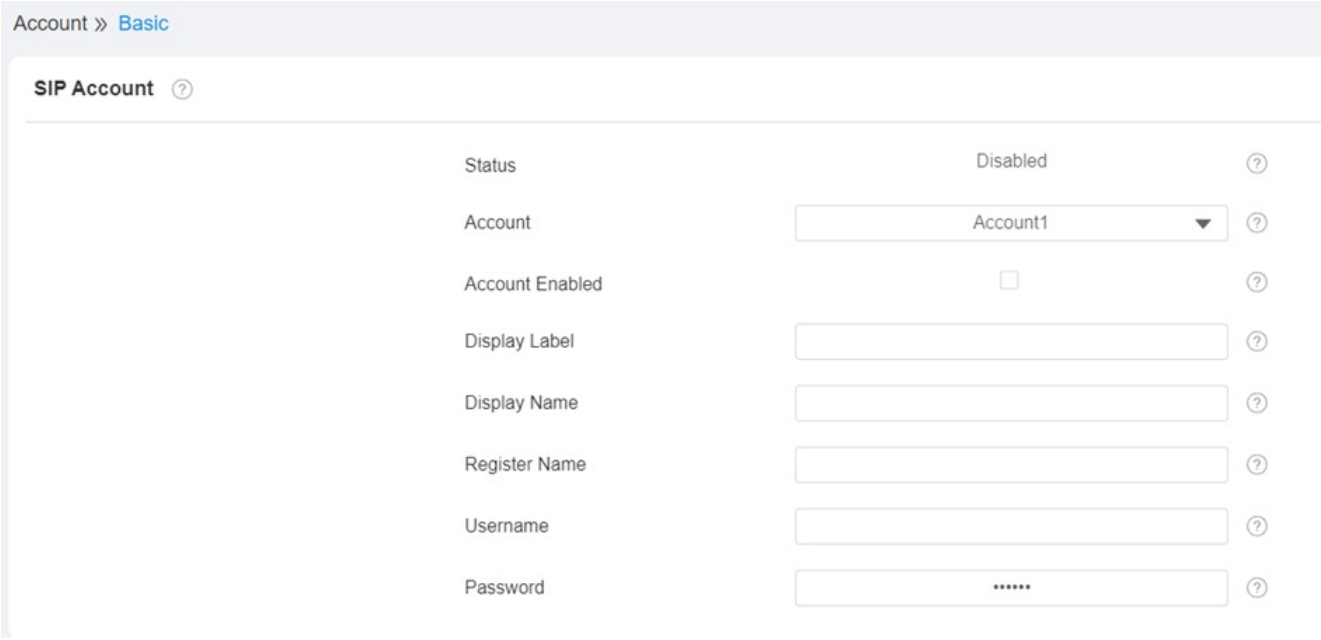




Parameter Set-up:

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

The parameter settings for SIP account registration can be configured on the **Account Settings** screen and they can also be configured on the device web **Account > Basic > SIP Account** interface. If you register a SIP account from a third-party device, obtain the **Register Name, User Name**, and **Password** from the third-party SIP service provider.



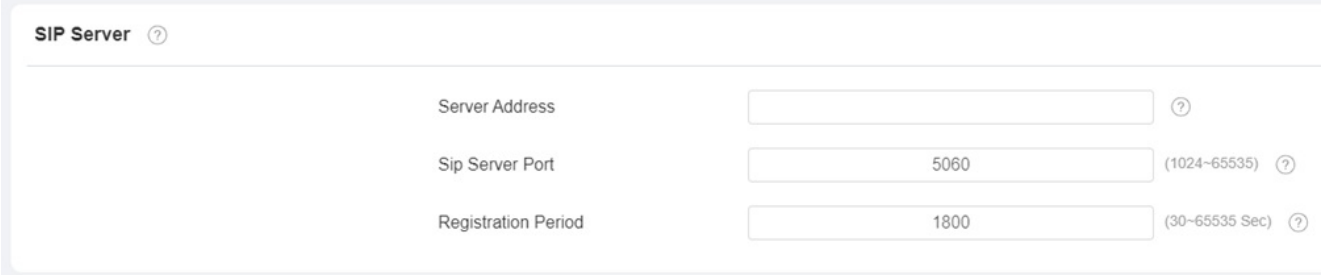
Parameter set-up:

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

SIP Server Configuration

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

To perform the SIP account setting on the Web **Account > Basic > SIP Server** interface.



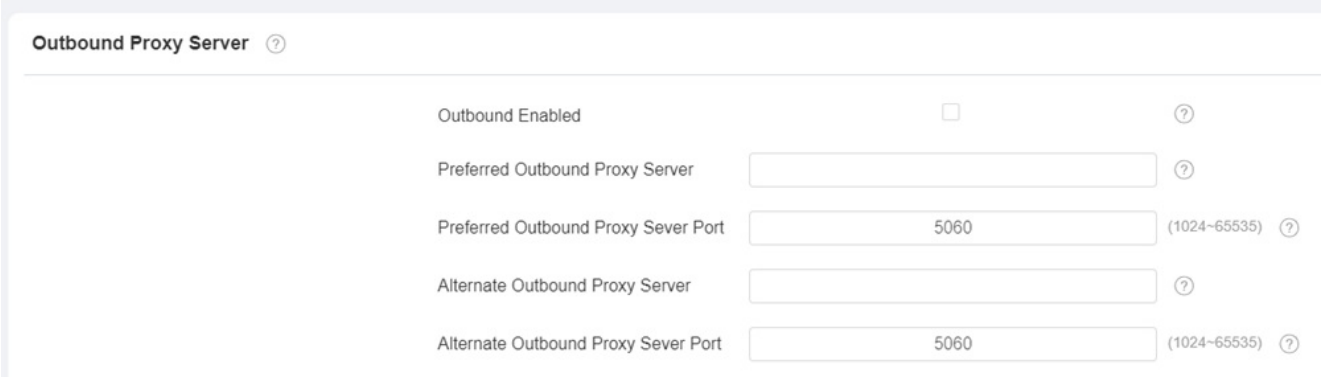
Parameter Set-up:

- **Server Address**: enter the server's IP address or its URL.
- **Sip Server Port**: set up SIP server port for data transmission.
- **Registration Period**: set up SIP account registration time pan. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is "**1800**", ranging from **30-65535s**.

Outbound Proxy Server configuration

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

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



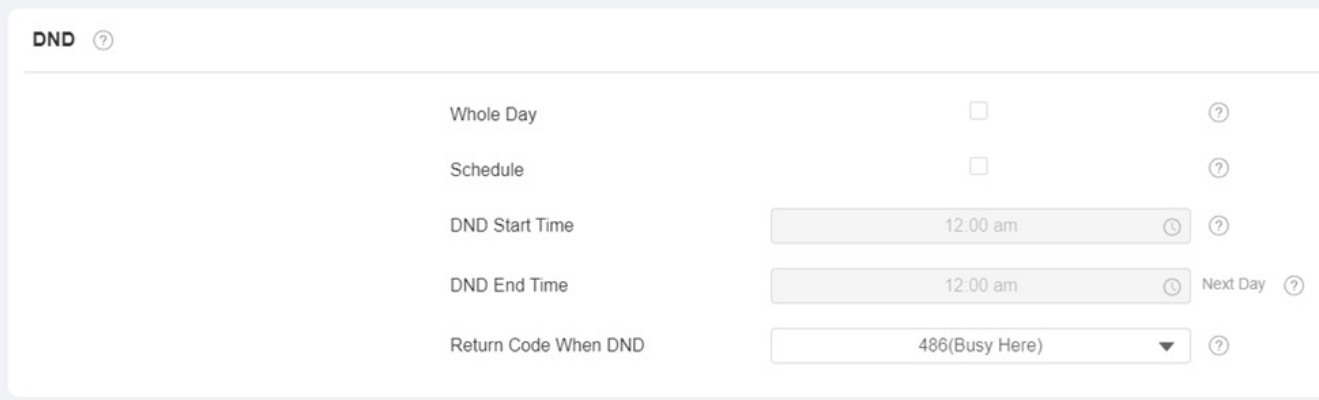
Parameter Set-up:

- **Preferred Outbound Proxy Server**: enter the SIP address of the outbound proxy server.
- **Preferred Outbound Proxy Port**: enter the port number for establishing call sessions via the outbound proxy server.
- **Alternate Outbound Proxy Server**: set up backup server IP for the backup outbound proxy server.
- **Alternate Outbound Proxy Port**: enter the port number for establishing call sessions 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:

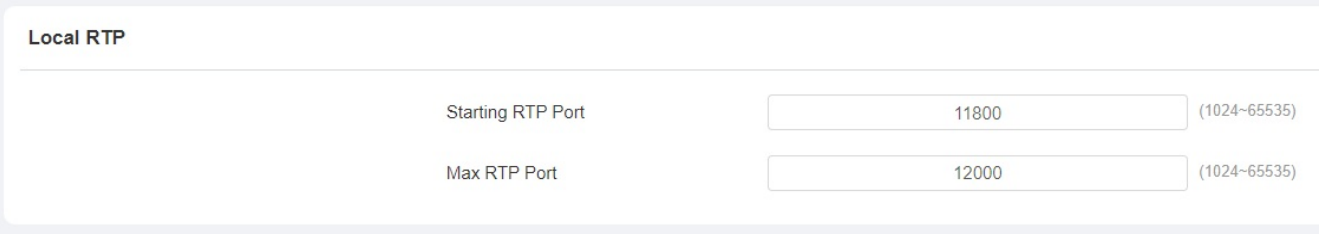
- **DND**: check **Whole Day** or **Schedule** to enable the DND function. DND function is disabled by default.
- **Return Code When DND**: select what code should be sent to the calling device via the SIP server. **404 for Not Found; 480 for Temporary Unavailable; 486 for Busy Here**; and **603 for Decline**.

Device Local RTP configuration

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

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

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



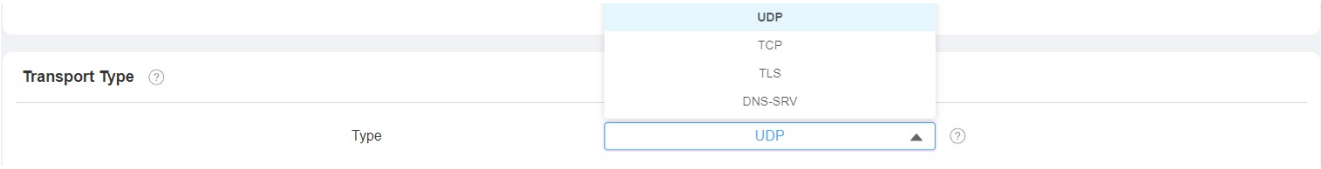
Parameter set-up:

- **Starting RTP Port**: enter the port value in order to establish the start point for the exclusive data transmission range.
- **Max RTP Port**: enter the port value in order to establish the 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**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for Reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain DNS record for specifying the location of services. And SRV not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

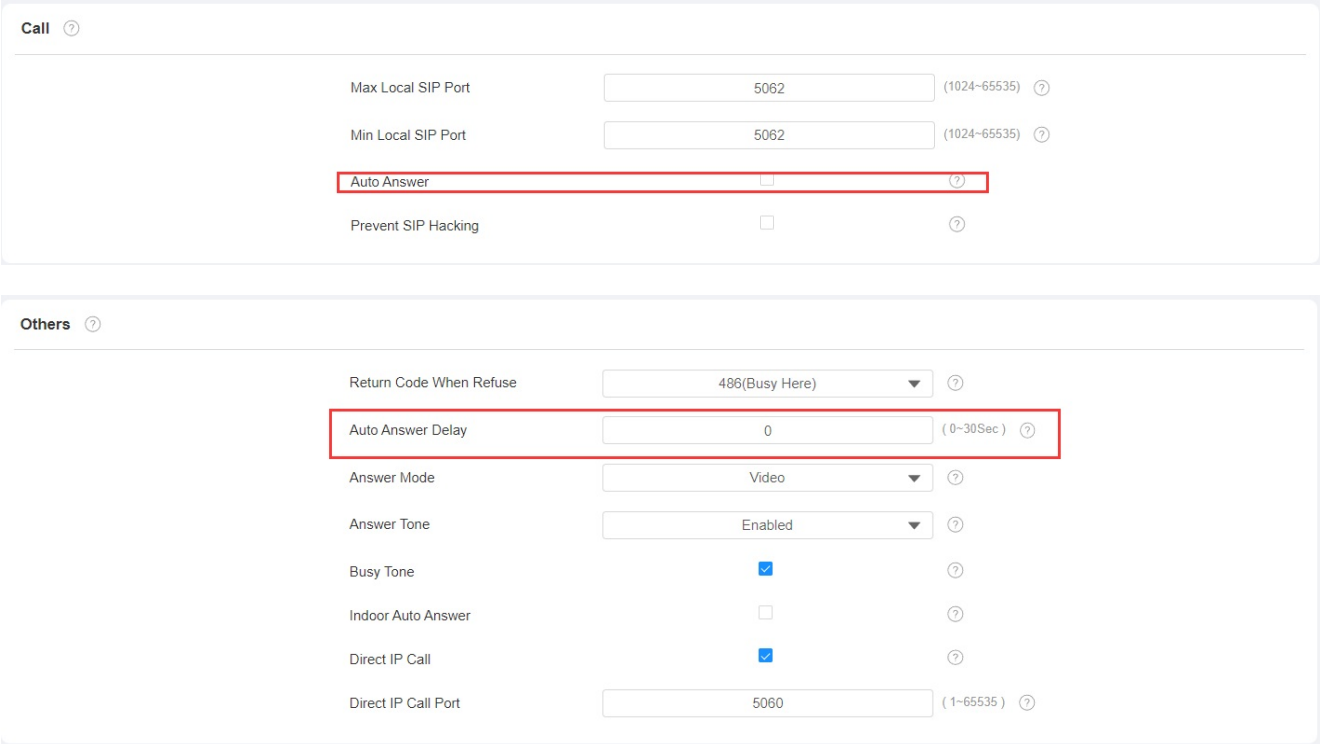
Call Setting

Call Setting

The indoor monitor will auto-answer all incoming calls if call auto-answer is enabled and receive a live stream if live stream is enabled.

Call Auto-answer Configuration

To do the configuration on web **Account > Advanced > Call > Auto Answer** and **Device > Call Feature > Others** interface.



Parameter Set-up:

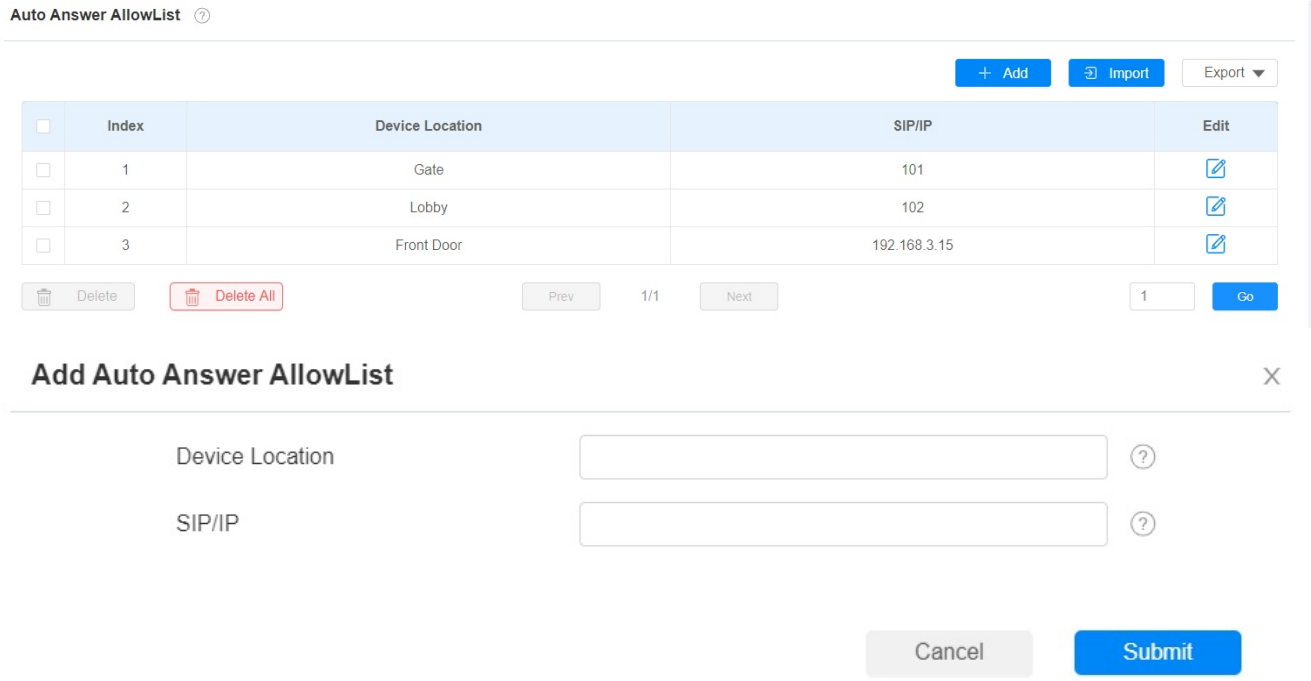
- **Auto Answer**: turn on the **Auto Answer** function by ticking the square box.
- **Auto Answer Delay**: set up the delay time (from 0-30 sec.) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Answer Mode**: set up the video or audio mode you preferred for answering the call automatically.
- **Indoor Auto Answer**: turn on the **Auto Answer** function for calls from other indoor

monitors by ticking the check box.

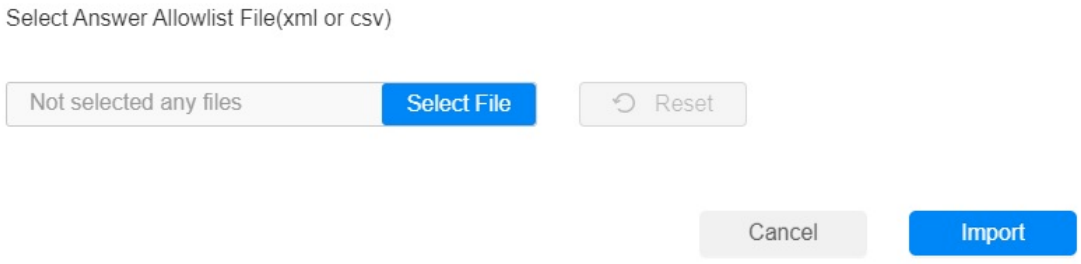
Auto-answer Allow List Setting

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

Go to **Device > Call Feature > Auto Answer AllowList** interface. Click **Add**.



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



Note:

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

Live Stream Setting

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

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

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

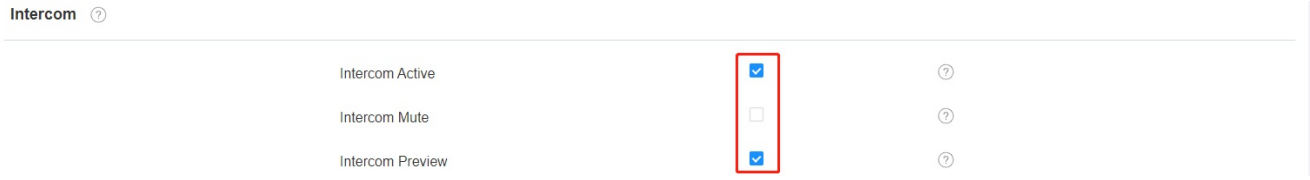
- If we receive the coming call as a video call at the X933 side, a two-way video conversation will be built, both caller and callee can be seen.
- If we receive the coming call as an audio call at the X933 side, a one-way video conversation will be built, only the live streaming from the caller can be seen.

Note:

- Only devices with camera module have this feature.

Intercom Active, Mute and 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.



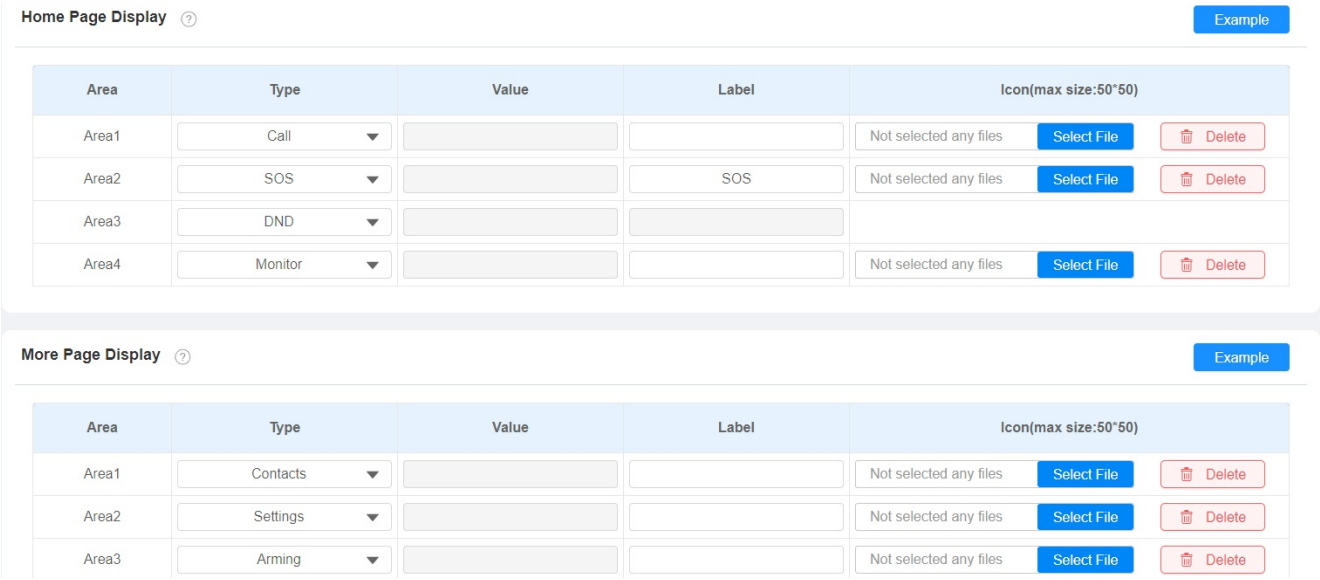
Parameter Set-up:

- **Intercom Active**: tick the check box to enable or disable the intercom function.
- **Intercom Mute**: tick the check box to mute the voice from the callee side and vice versa.
- **Intercom Preview**: tick the check box to enable the incoming call preview function. If enabling intercom preview, the group call is not available.

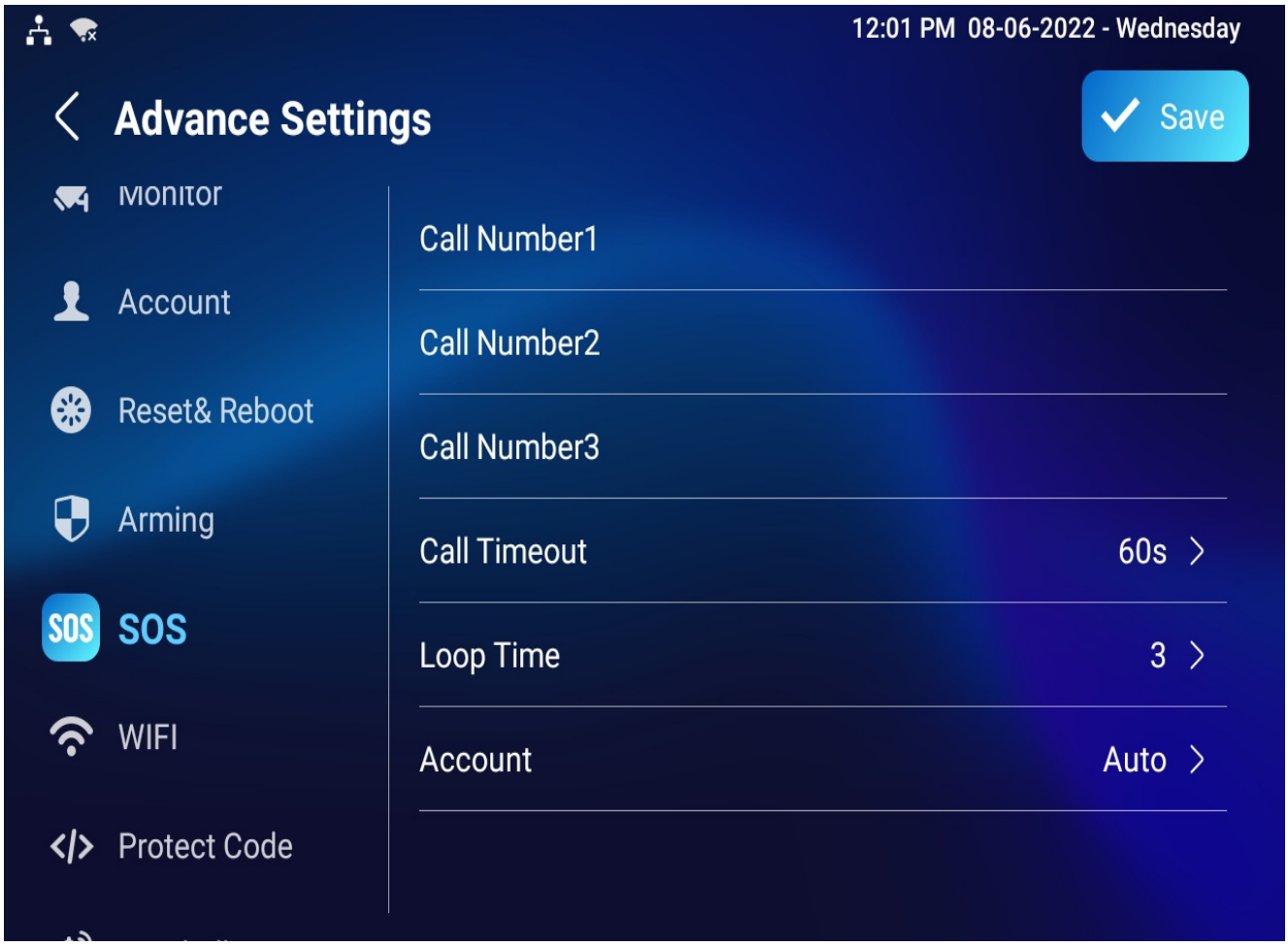
Emergency Call Setting

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

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



After setup on web, you also need to do the configuration on device **Settings > Advance Settings > SOS** screen.



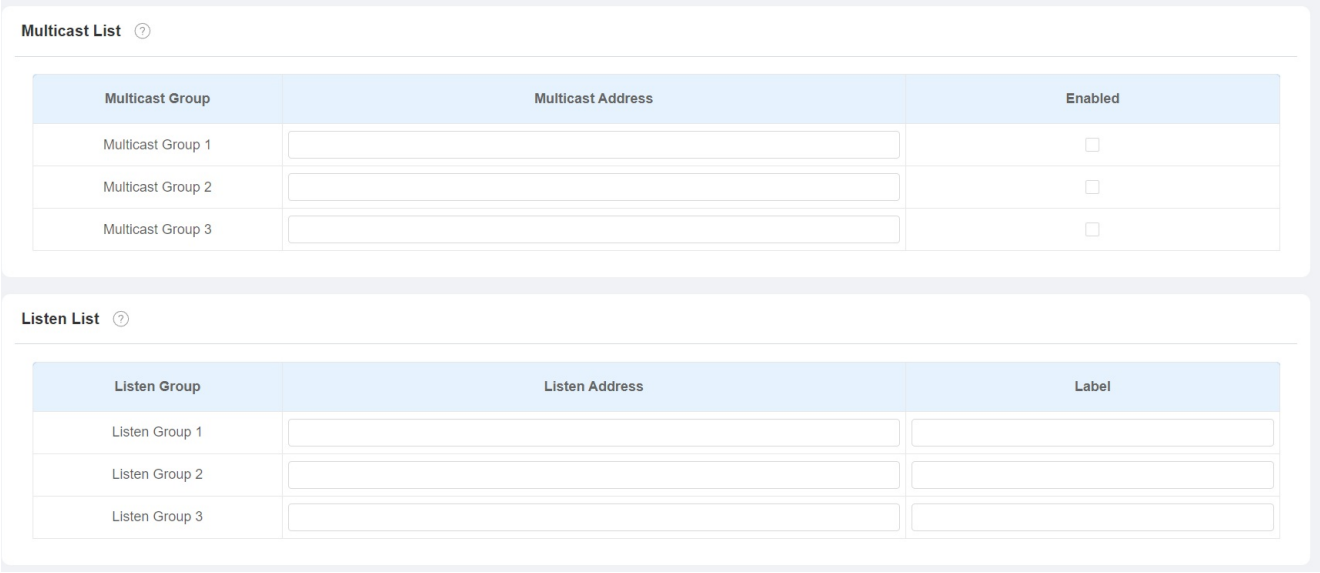
Parameter Set-up:

- **Call Number**: to set up 3 SOS numbers. Once users press the SOS key on the home page (SOS display key shall be set on the web manually), indoor monitors will call out the number in order.
- **Call Timeout**: set up the timeout for each number. Once users call out, if the other side does not answer within the timeout, indoor monitors will continue to call the next number.
- **Loop Times**: to set up the call loop times.

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.

Go to **Device > Multicast > Multicast List** interface.



Parameter Set-up:

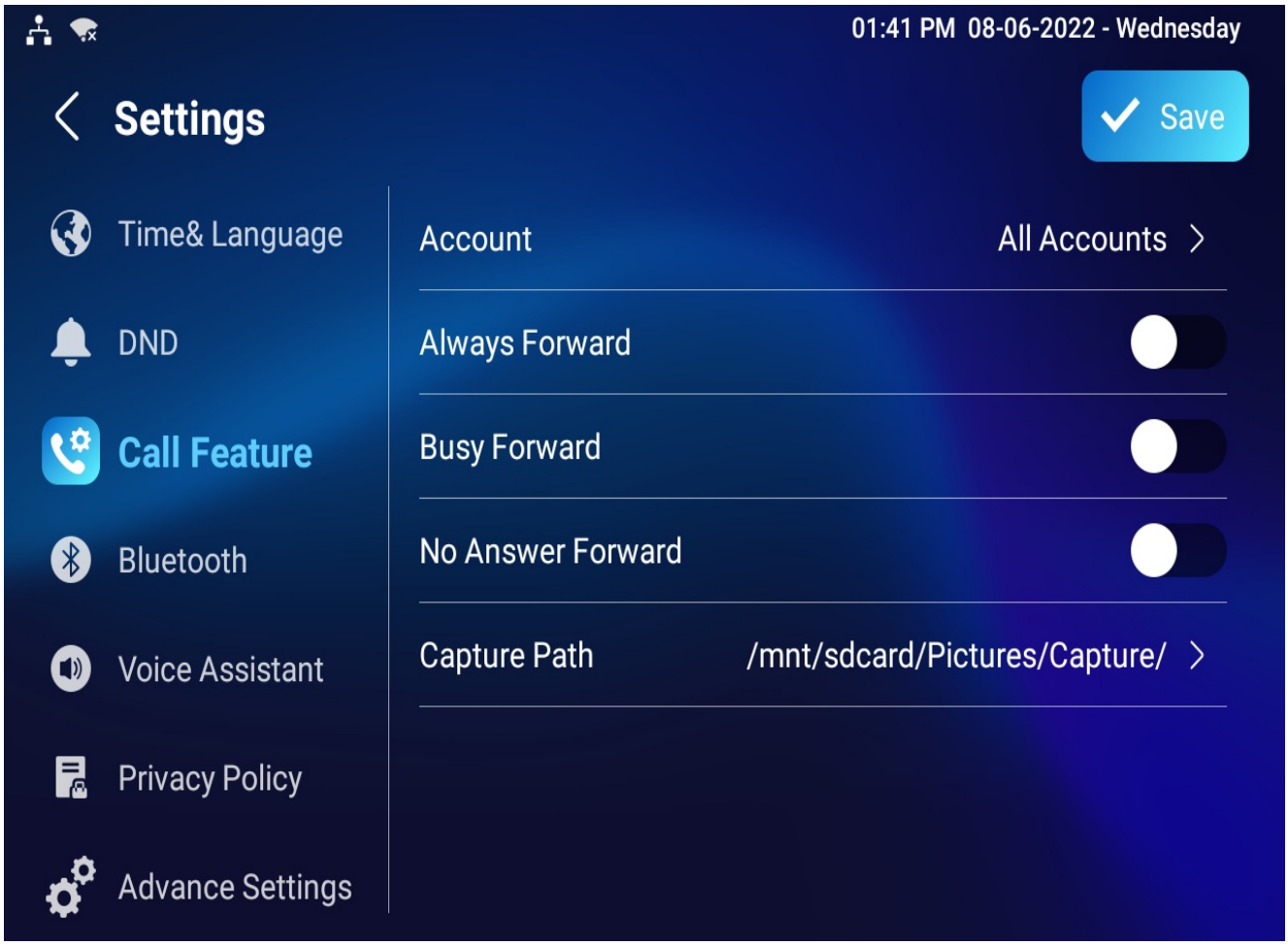
- **Multicast Address**: Enter the multicast address (Range: 224.0.0.0 – 239.255.255.255) when the device serves as the caller.
- **Listen Address**: Enter the multicast address (Range: 224.0.0.0 – 239.255.255.255) when the device serves as the callee.

Call Forwarding Setting

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

Call Forwarding Configuration on the Device

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

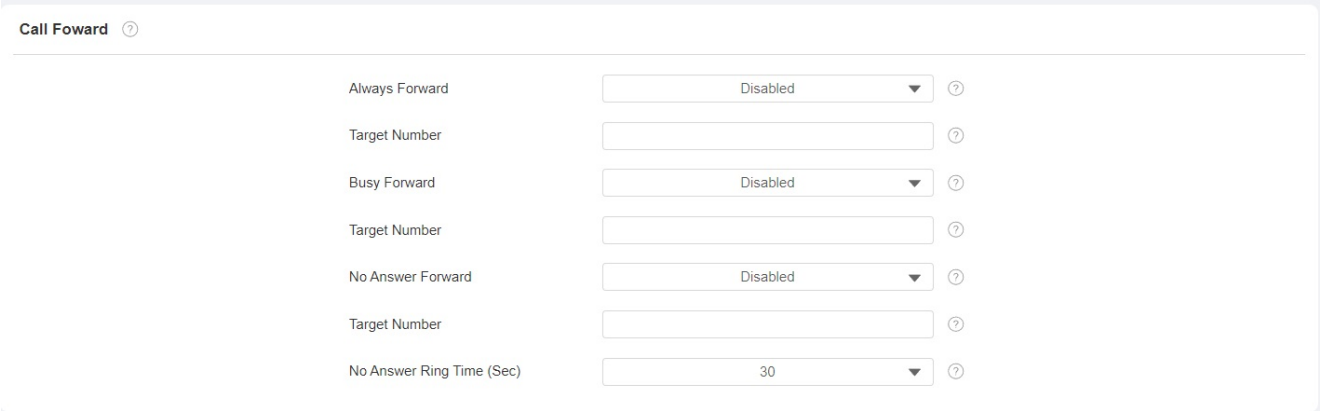


Parameter Set-up:

- **Account**: to choose which account shall implement the call forwarding feature.
- **Always Forward**: to enable the **Always Forward** function; all incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: to enable the **Busy Forward** function; incoming calls will be forwarded to a specific number if the phone is busy.
- **No Answer Forward**: to enable the **No Answer Forward** function; incoming calls will be forwarded to a specific number if the phone is not picked up within no answer ring time.
- **Target Number**: to enter the specific forward number if the indoor monitor enables **Always Forward / Busy Forward / No Answer Forward**.
- **Capture Path**: select the storage location for all the captured pictures.

Call Forwarding Configuration on the Web Interface

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



Parameter Set-up:

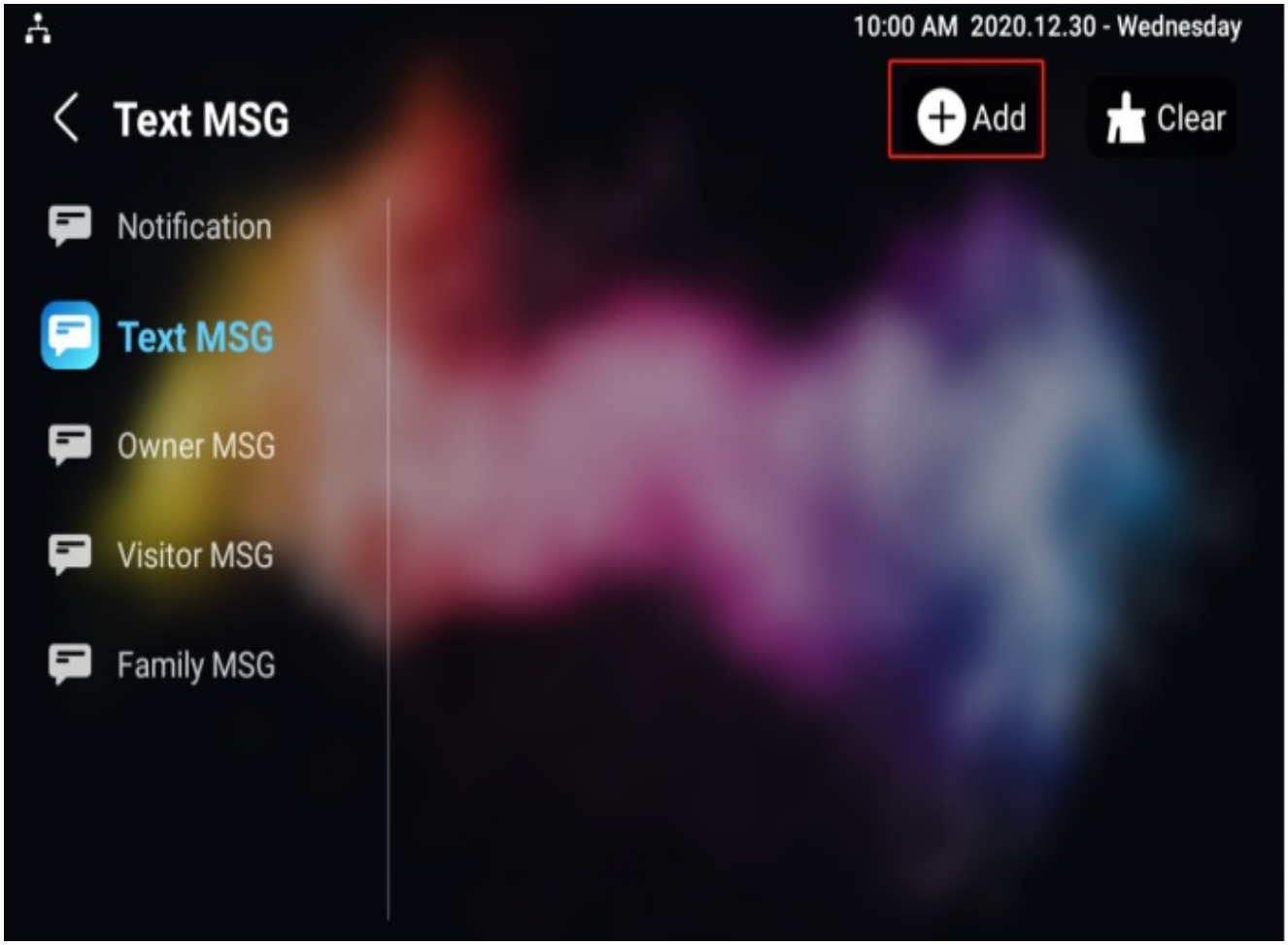
- **Always Forward**: to enable the **Always Forward** function; all incoming calls will be automatically forwarded to a specific number.
- **Busy Forward**: to enable the **Busy Forward** function; incoming calls will be forwarded to a specific number if the phone is busy.
- **No Answer Forward**: to enable the **No Answer Forward** function; incoming calls will be forwarded to a specific number if the phone is not picked up within no answer ring time.
- **Target Number**: to enter the specific forward number if the indoor monitor enables **Always Forward / Busy Forward / No Answer Forward**.
- **No Answer Call Ring Time (Sec)**: to set no answer time interval from 0-120 seconds before the call is transferred to a designated number.

Intercom Message Setting

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

Manage Messages

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



Parameter Set-up:

- **Notification**: the message from the property manager, this feature is only available when using SDMC or Akuvox SmartPlus.
- **Text MSG**: to send, receive or manage the text message here.
- **Owner MSG**: if you enable this feature, and nobody answers the incoming call within the pre-configured ring time, the visitor will hear the owner's audio message.
- **Visitor MSG**: if you enable the visitor message feature, and nobody answers the

incoming call within the pre-configured ring time, it will save the visitor record.

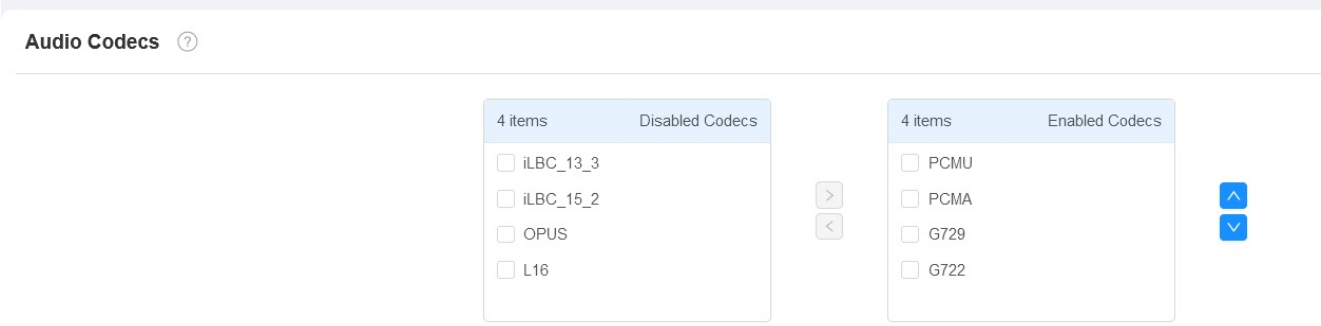
- **Family MSG**: you can record the audio messages for your family members.

Audio& Video Codec Configuration for SIP Calls

Audio Codec Configuration

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

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

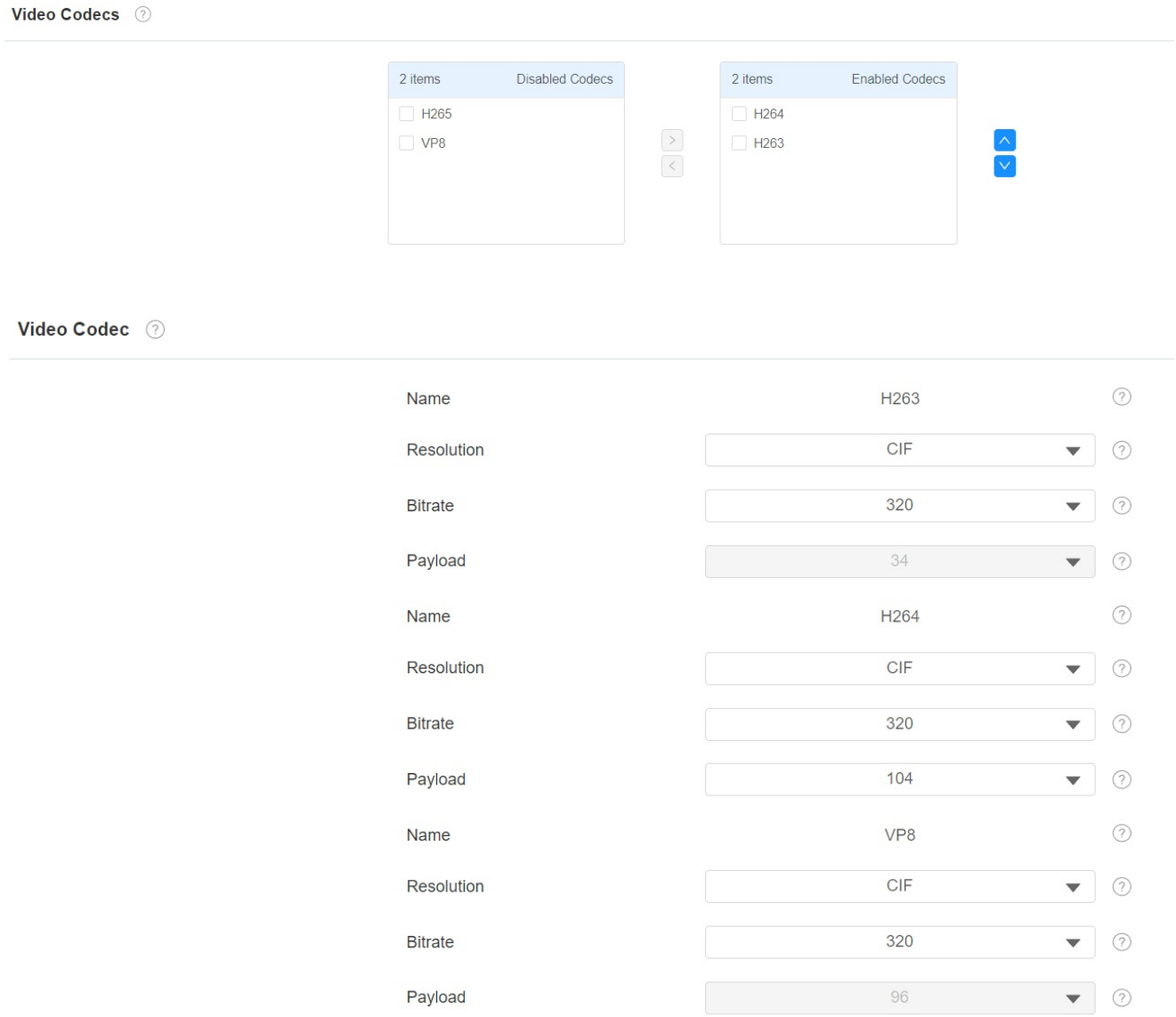


Please refers to the bandwidth consumption and sample rate for the codec types below:

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

Video Codec Configuration

X933 series supports VP8, H263, H264, H265 codec that provides a better video quality at a much lower bit rate with different video quality and payload. To do the configuration on web **Account > Advanced > Video Codecs** interface. Choose available video codecs and set up the codecs parameters.



Parameter Set-up:

- **Name**: Display the video code type for the device.
- **Resolution**:
  - Select the code resolution for H263 among three options: **QCIF, CIF, 4CIF**.
  - Select the code resolution for H264 among five options: **QCIF, CIF, 4CIF, VGA, 720P**.
  - Select the code resolution for VP8 among five options: **QCIF, CIF, 4CIF, VGA, 720P**.
- **Bitrate**: select the video stream bit rate for H263 (ranging from 128-512).

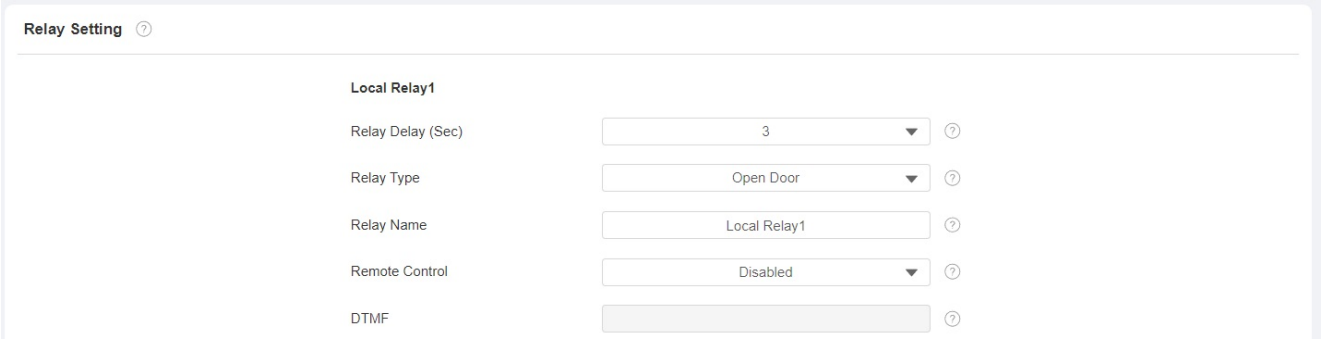
Door Access Control Configuration

Relay Switch Setting

Local Relay Setting

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

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



Parameter Set-up:

- **Relay Delay**: set the relay delay time after the relay is triggered.
- **Relay Type**: set relay action type. There are three types of the relay, chime bell setting, open door and other switchs(reset by event). **Chime Bell**, when there is a call, the chime bell will ring. **Open door**, when pressing the unlock icon, the local relay will be opened.
- **Remote Control**: enable it to trigger local relay by DTMF and vice versa.
- **DTMF**: set the DTMF to trigger the local relay when you enable **Remote Control**.

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.

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

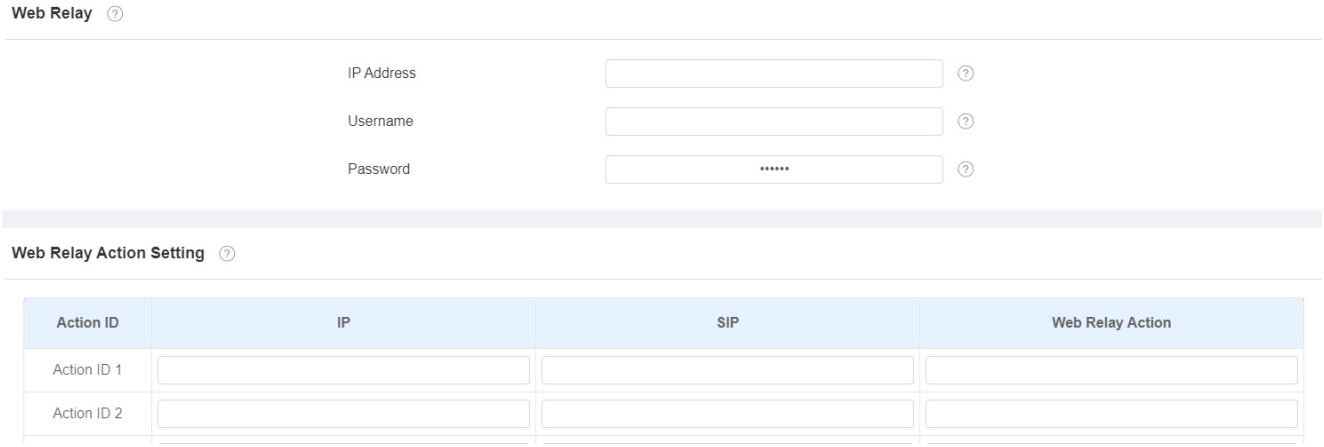
Parameter Set-up:

- **DTMF Code**: to set 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 device can use a web relay to either control a local relay, or a remote relay somewhere else on the network.

To do this configuration on web **Device > Relay > Web Relay** interface.



Parameter Set-up:

- **IP address**: enter the web relay IP address.
- **User Name**: enter the User name provided by the web relay manufacturer.
- **Password**: enter the password provided by the web relay manufacturer. The passwords are authenticated via HTTP and you can define the passwords using "HTTP get" in Action.
- **IP/SIP**: the relay extension information, which can be an IP address or SIP account of an intercom device such as an indoor monitor, so that the specific action command will be sent when unlock is performed on the intercom device. This setting is optional.
- **Web Relay Action**: 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**.

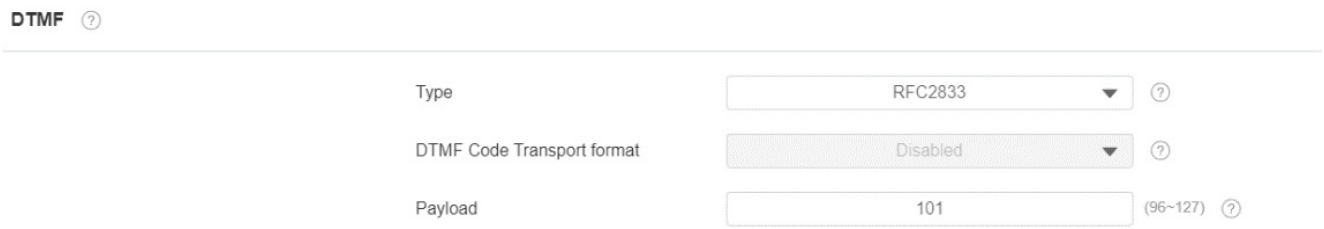
  -If you have not entered the IP address, username, and password, you need to enter the complete HTTP command in such a format: **http://Username:Password@IP address/state.xml?relayState=2**.

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.

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



Parameter Set-up:

- **Type**: select DTMF type among **Inband, RFC2833, Info, Info+Inband** and **Info+RFC2833** according to your need.
- **DTMF Code Transport Format**: select it only when the third-party device that receives the DTMF code adopts Info transport format. Info transfer the DTMF code via signaling while other transport format does it via RTP audio packet transmission. You can select the DTMF transferring format according to the third-party device (**DTMF, DTMF-Relay, Telephone-Event**). For example, select **Telephone-Event** if the third-party device adopts the telephone-event. Select among four options: **Disable, DTMF, DTMF-Relay, Telephone-Event** according to your need.
- **Payload**: select payload 96-127 for data transmission identification.

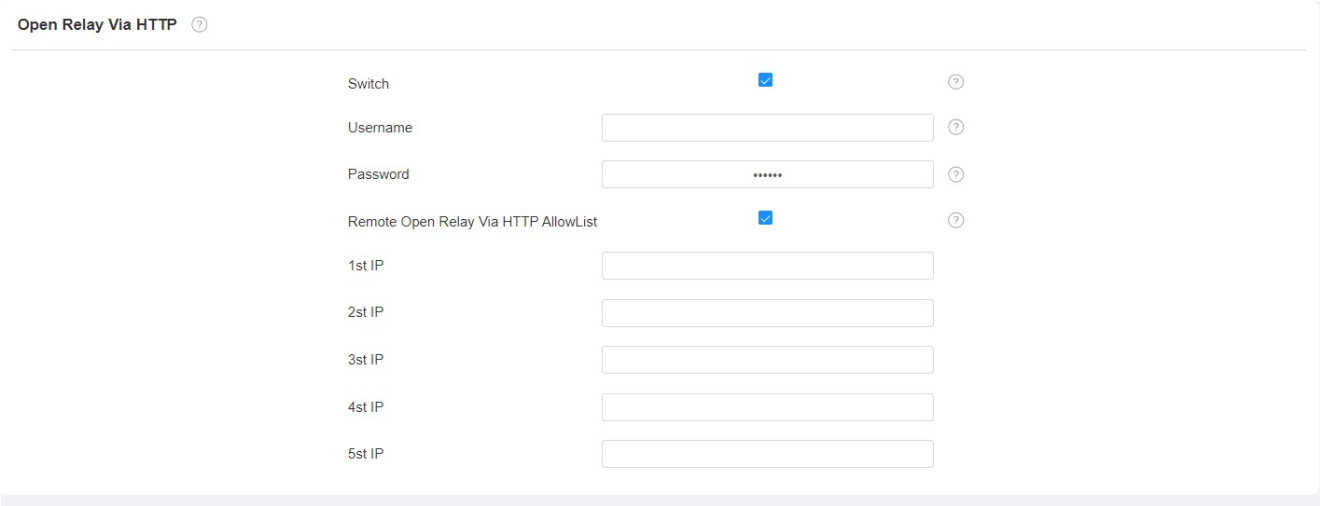
Note:

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

Door Unlock via HTTP Command

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

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



Parameter Set-up:

- **Switch**: Enable it to allow the relay to be triggered remotely using HTTP command.
- **Username**: Enter the device username to be used as a part of the HTTP command to trigger the local relay. For example, admin.
- **Password**: Enter the device password to be used as part of the HTTP command to trigger the local relay. For example, 12345.

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

Note:

- DoorNum in the HTTP command above refers to the relay number #1 to be triggered.
- The device with high security mode enabled only supports new formats. Please refer to **Security**.

Lift Control

You can summon lift at home via the lift control feature.

Configure Lift Control

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

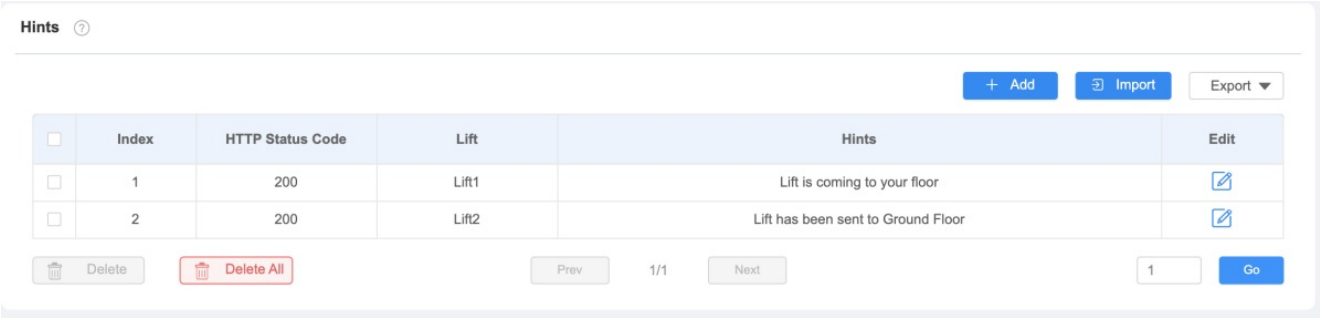
Parameter Set-up:

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

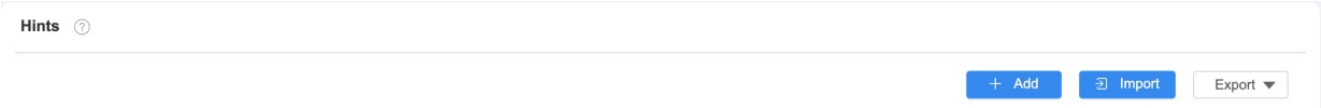
Configure Lift Control Prompt

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

To do this configuration on web **Device > Lift> Hints** interface. Edit the **HTTP Status Code**, and feedback code from the lift control board.



If there are huge amounts of Prompts that need to be added, you can click **Export** tab to export a template, after editing to import/export.

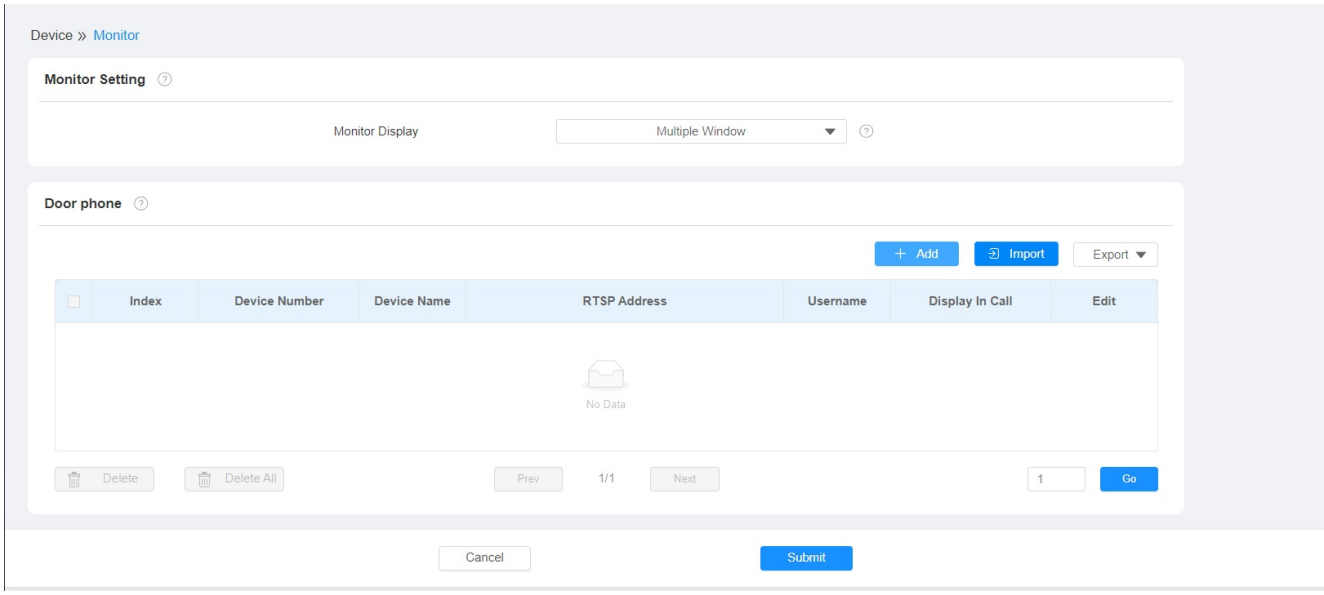


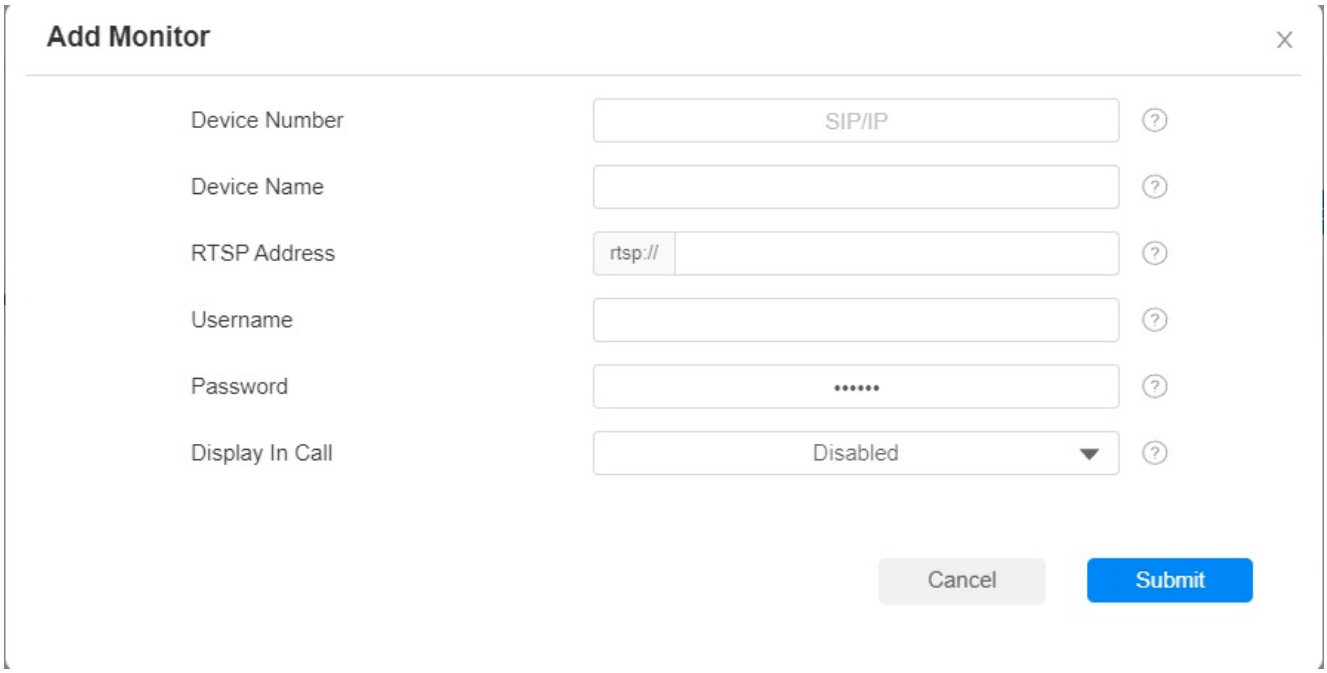
Security

Monitor and Image

Monitor Setting

You can configure the monitor setting on the web **Device > Monitor** interface.





Parameter Set-up:

- **Device Number:** enter the IP/SIP number of Akuvox door phone or third-party device.

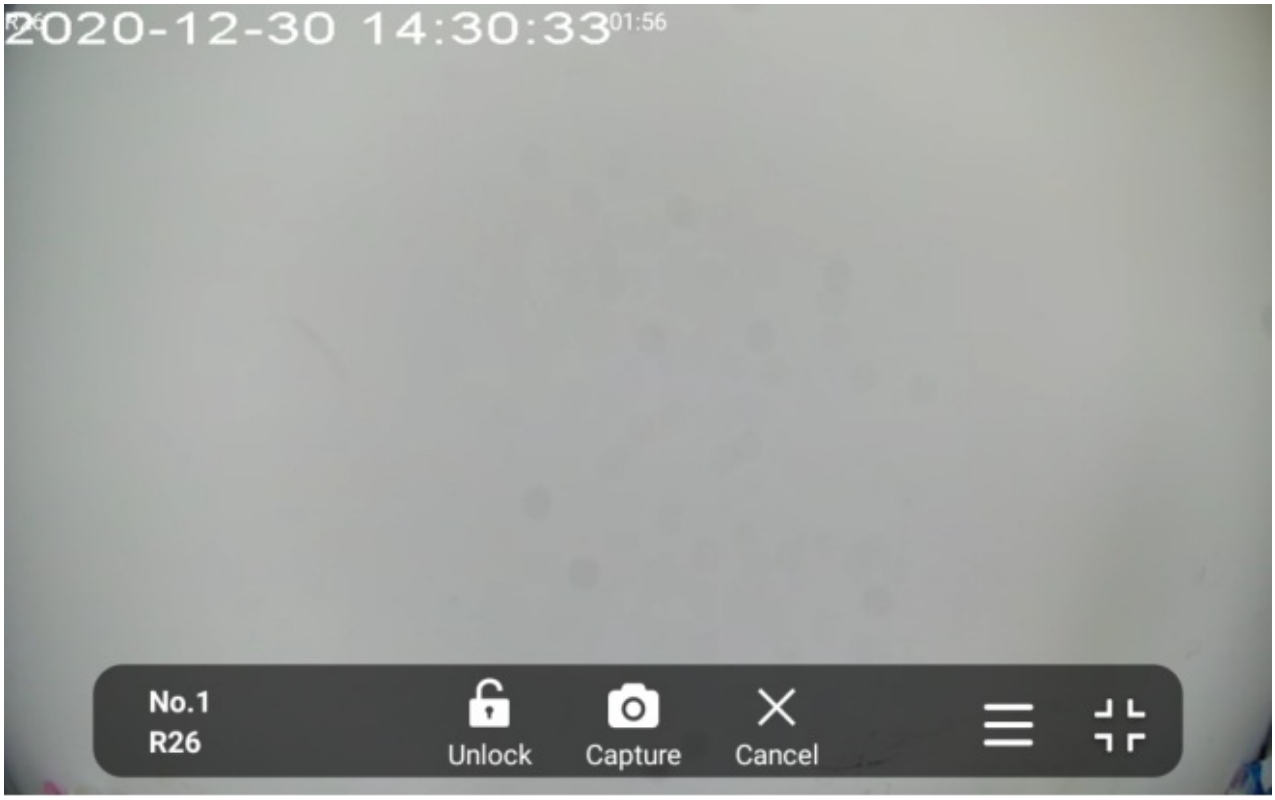
- **Device Name**: name the device to distinguish it from others.
- **RTSP Address**: set up the RTSP address. The RTSP format of the Akuvox door phone is rtsp://deviceIP/live/ ch00_0. If it is a third-party device, you need to obtain the RTSP format from the third-party device service provider.
- **Username**: enter the username shown on the door phone's RTSP interface for authentication.
- **Password**: enter the password shown on the door phone's RTSP interface for authentication.
- **Display in Call**: If enabled, when there is an incoming call from the monitor, the video will be displayed.

Note

- If you want to add a third-party camera for monitoring, you need to obtain the **RTSP format**, **Username**, and **Password** from the third-party device service provider.

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.

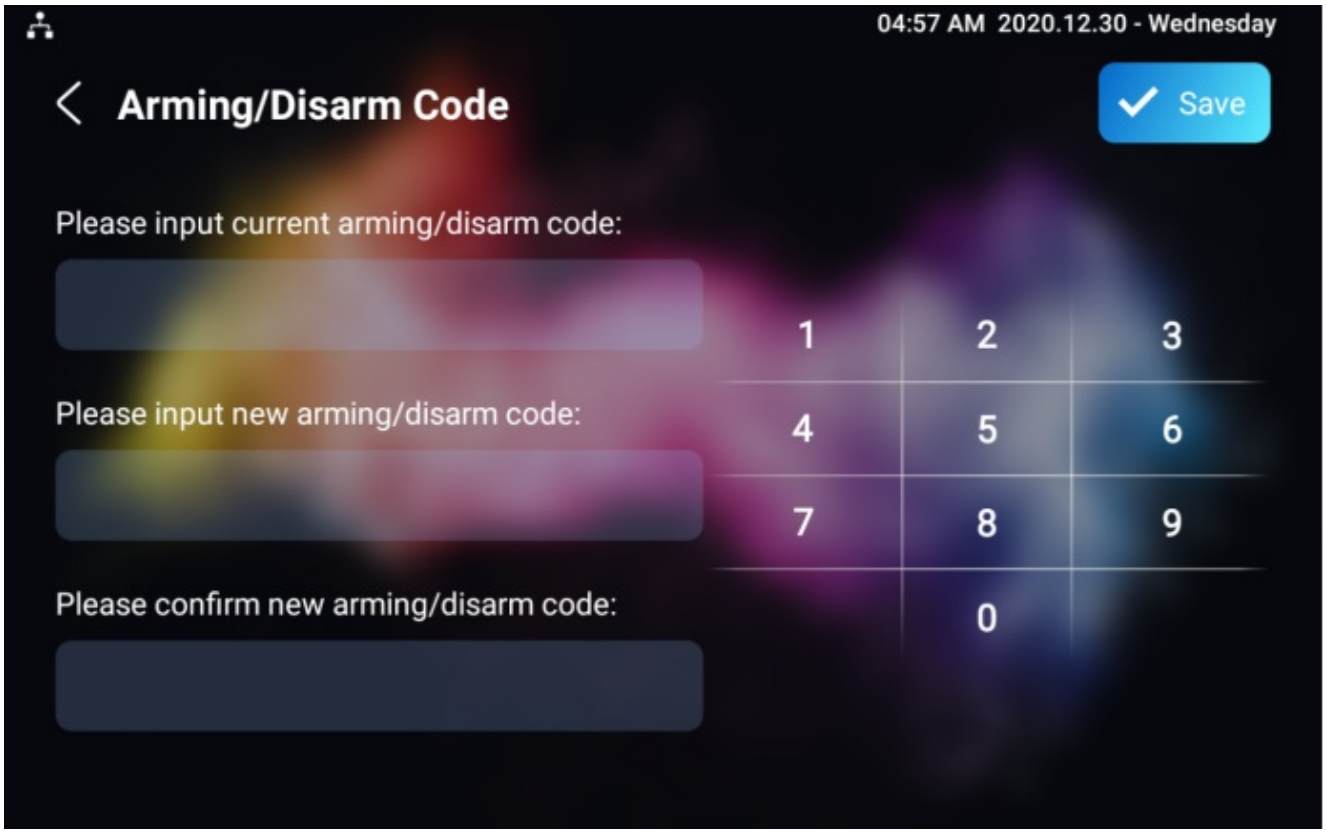


Alarm and Arming Configuration

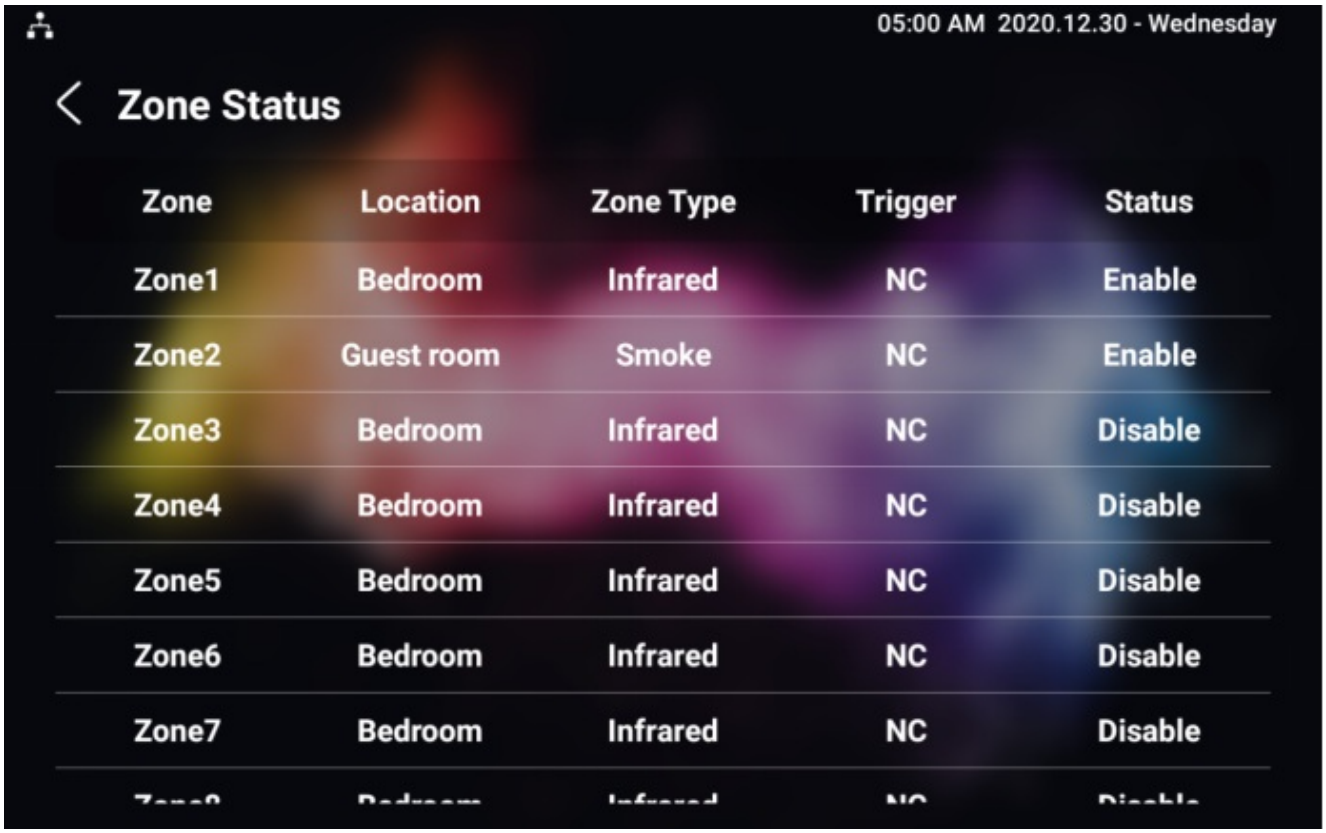
The Arming function is designed to enhance home security by offering three modes with custom zone settings for connected sensors. When armed, the device will sound a siren and notify specific people if a sensor detects something unusual.

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.

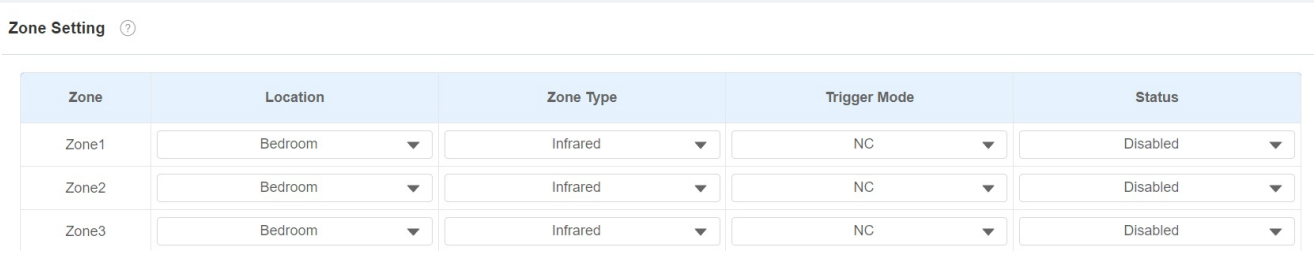


To check the zone status on **Arming > Zone Status** screen.



Configure Alarm and Arming on the Web Interface

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



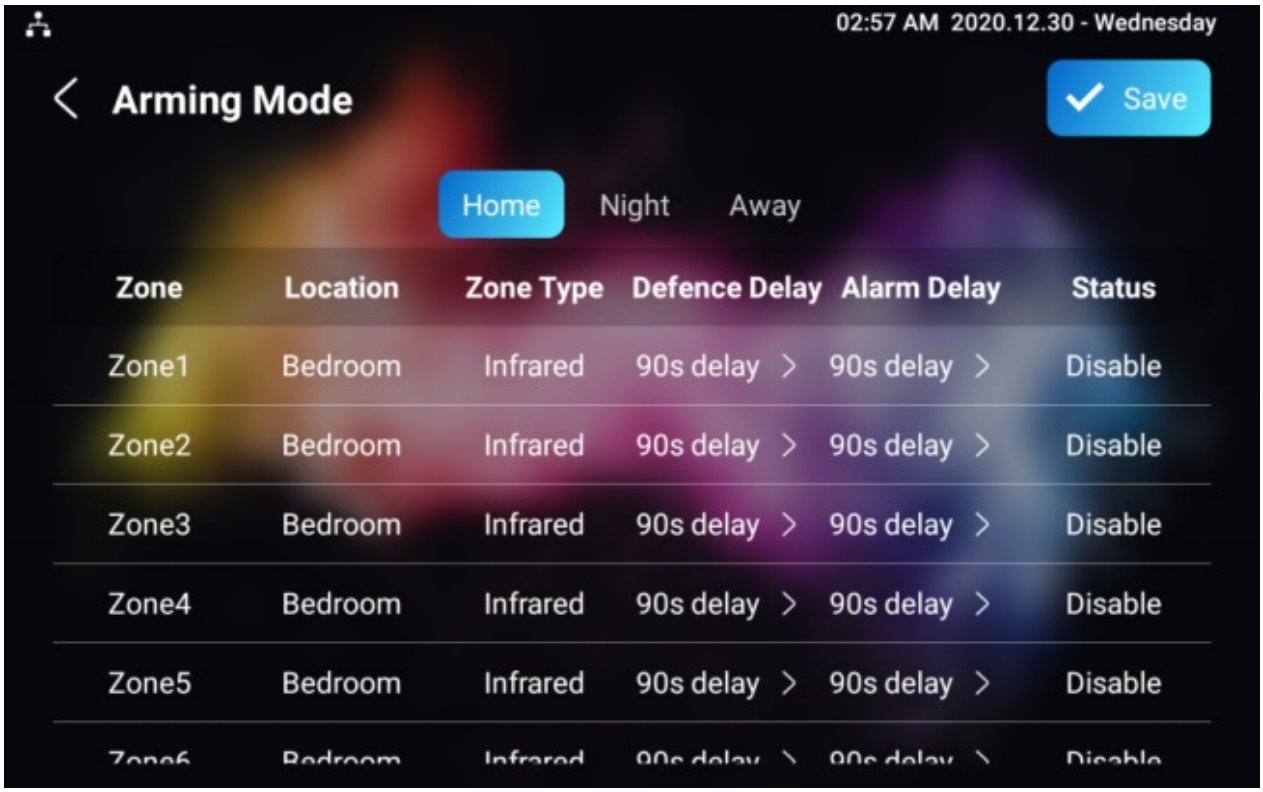
Parameter Set-up:

- **Location**: set up the location according to where the alarm sensor is installed. You can select among ten location types: **Bedroom, Gate, Door, Guest room, Hall, Window, Balcony, Kitchen, Study** and **Bathroom**.
- **Zone Type**: set up the alarm sensor types. You can select among five sensor types: **Infrared Drmagnet, Smoke, Gas, Urgency**.
- **Trigger Mode**: set sensor trigger mode between **NC** and **NO** according to your need.
- **Status**: set the alarm sensor status among three options: **Enable, Disable**, and **24H**. Select **Enable** if you want to enable the alarm, however, you are required to set the alarm

again after an alarm is disarmed. Select **Disable** if you want to disable the alarm, and select **24H** if you want the alarm sensor to stay enabled for 24 hours without needing to set up the alarm manually again after the alarm is disarmed.

Configure Location-based Alarm

Configure the alarm sensor in the same way you do on the web interface on the Arming screen.



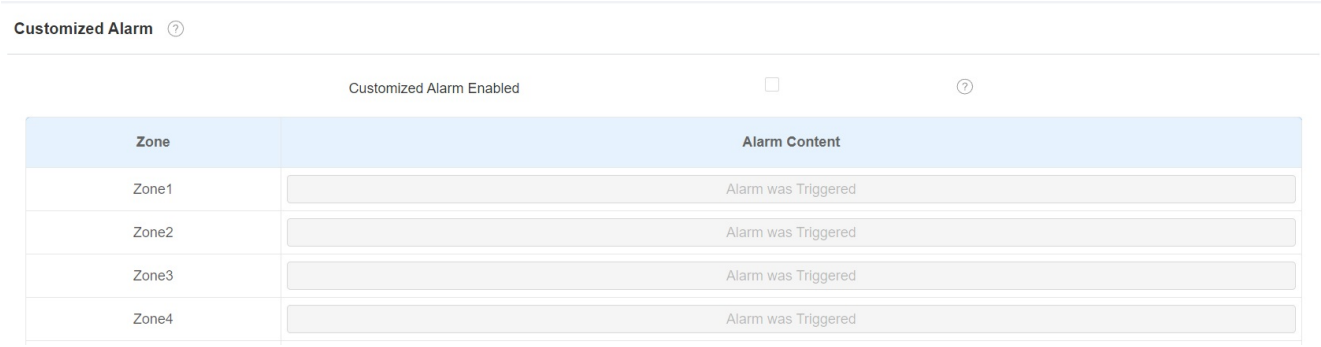
Parameters set up:

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

Configure Alarm Text

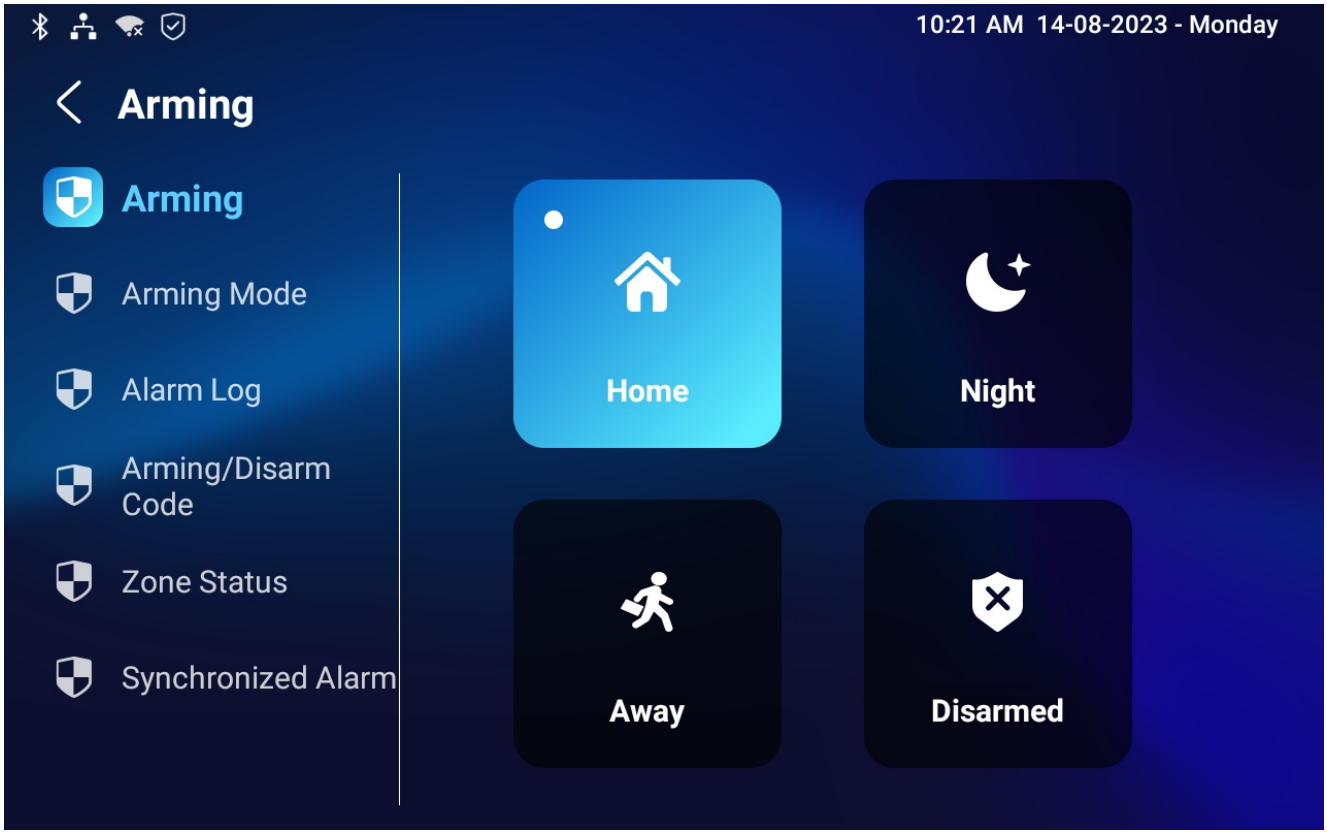
Once the alarm sensor is configured, you can access the device's web interface to personalize the alert content displayed on the screen when an alarm is triggered.

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



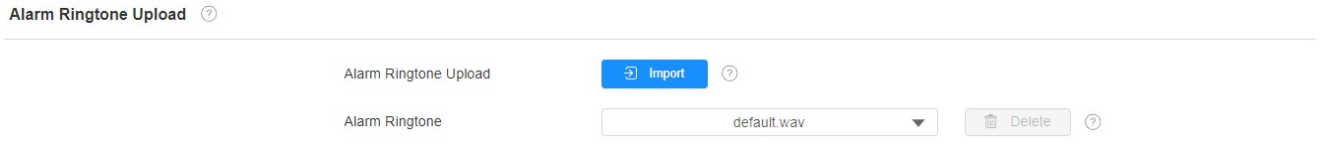
Configure Arming Mode

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



Configure Alarm Ringtone

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



Note:

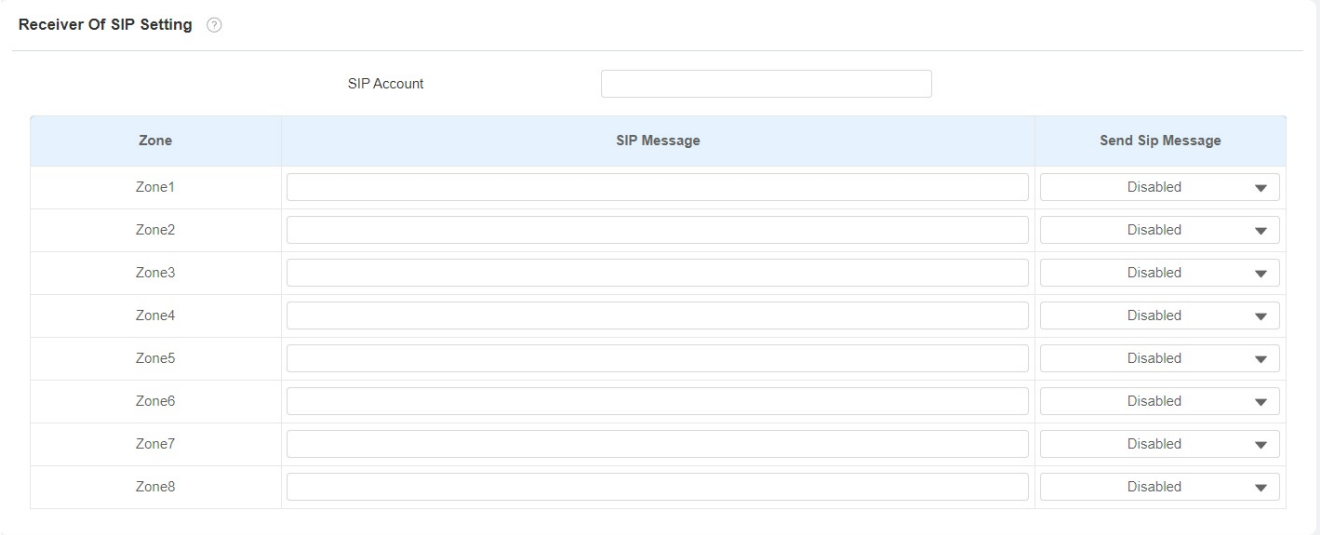
- The file format of the customized ringtone should be .wav.

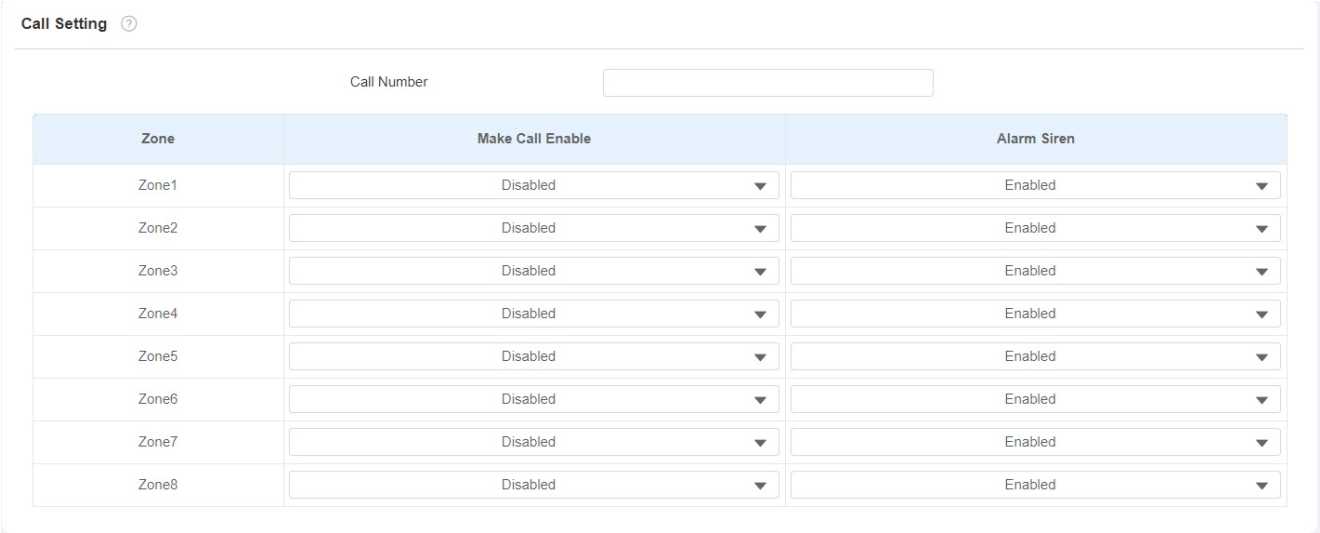
Alarm Action Configuration

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

Select Alarm Action Types

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





Parameter Set-up:

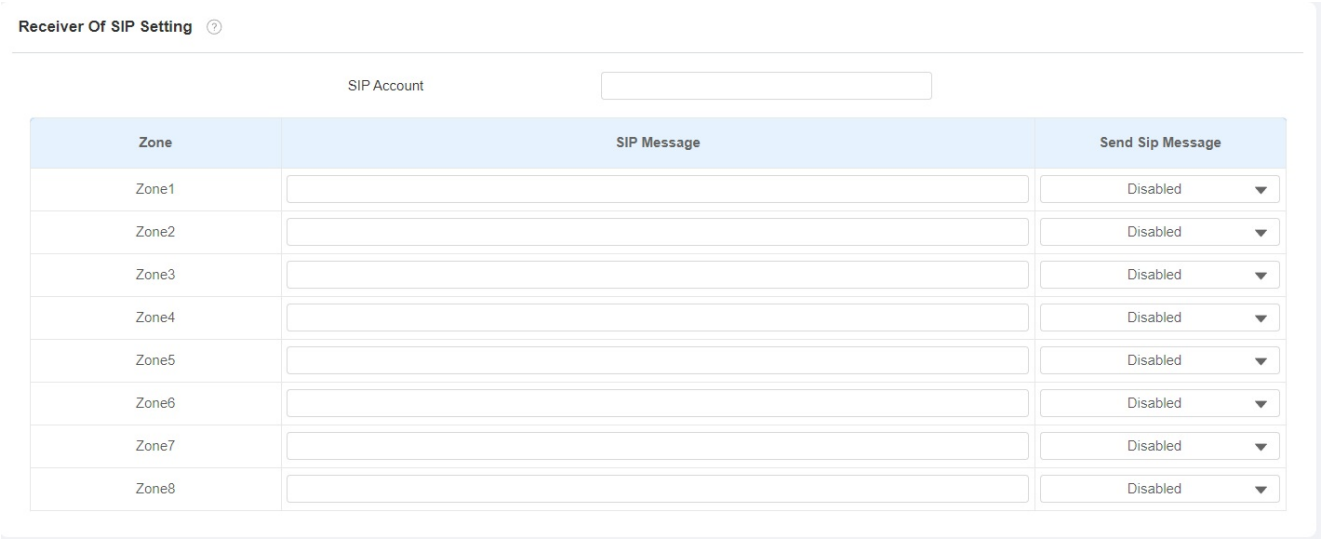
- **HTTP Command**: enable the HTTP command if you want the action to be implemented on a designated third-party device.
- **SIP Message**: enable SIP message if you want the SIP message to be sent to a designated SIP account as an action. This feature should be enabled by using Autop.
- **Call**: enable call if you want to make a call to a designated SIP or IP number.

Configure Alarm Action via HTTP Command

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

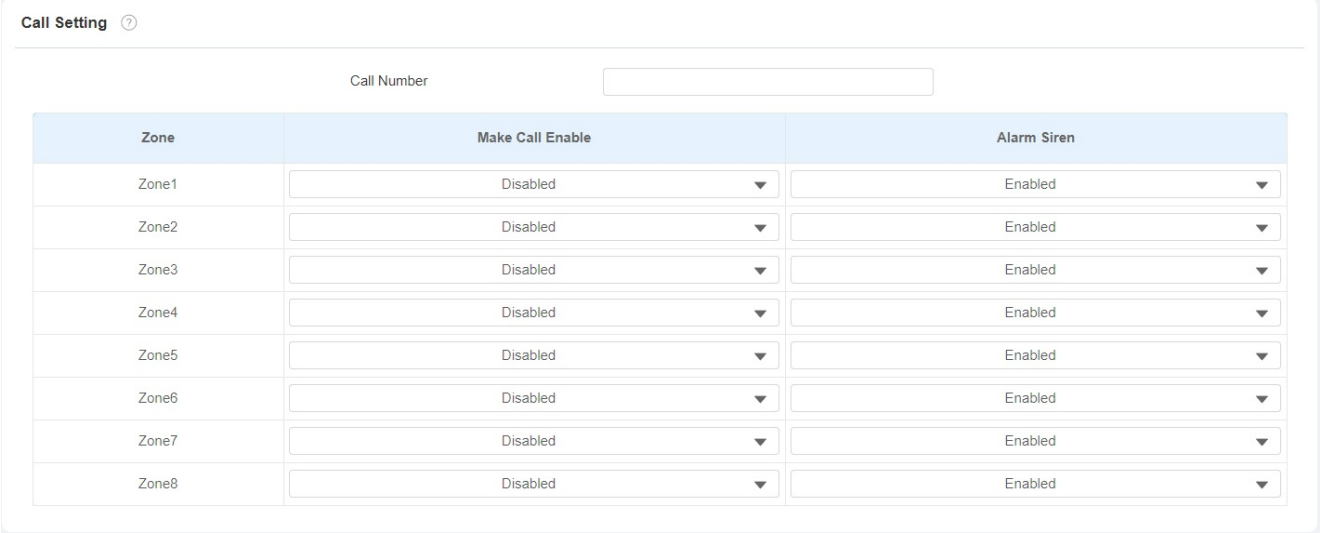
Configure Alarm Action via SIP Message

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.



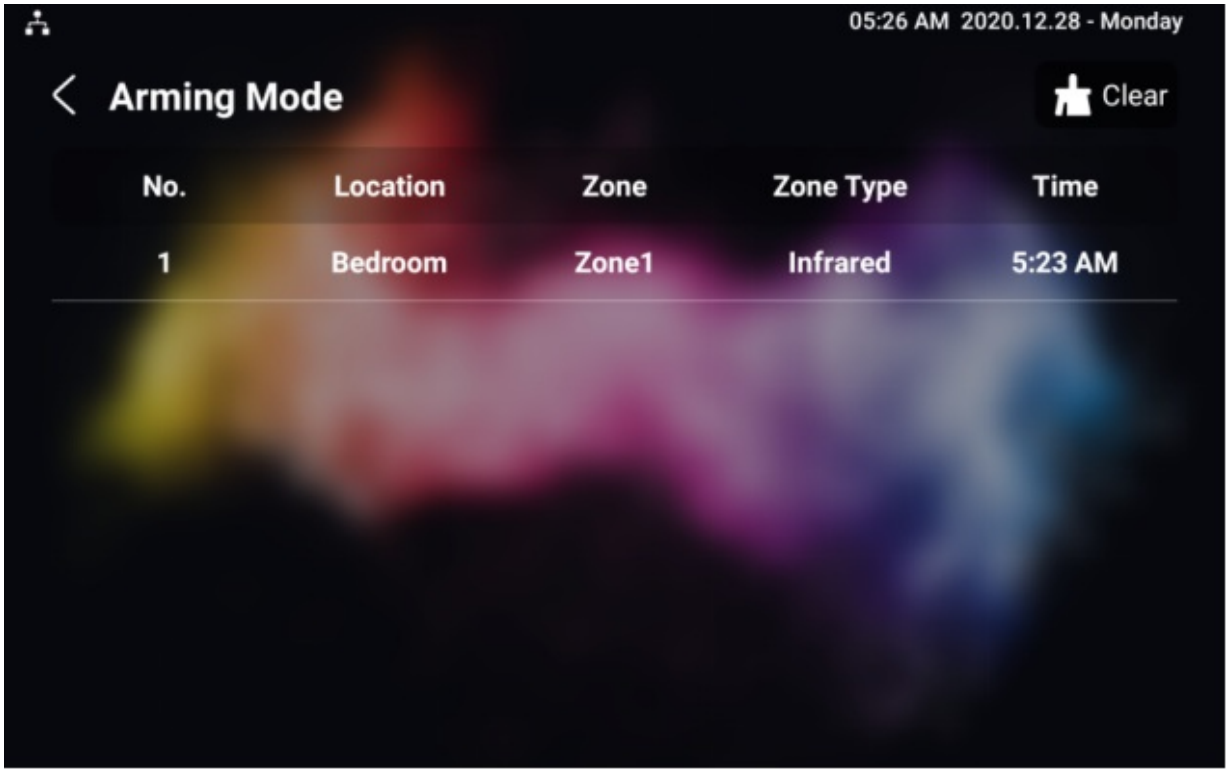
Configure Alarm Action via SIP Call

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.



Check Alarm Log

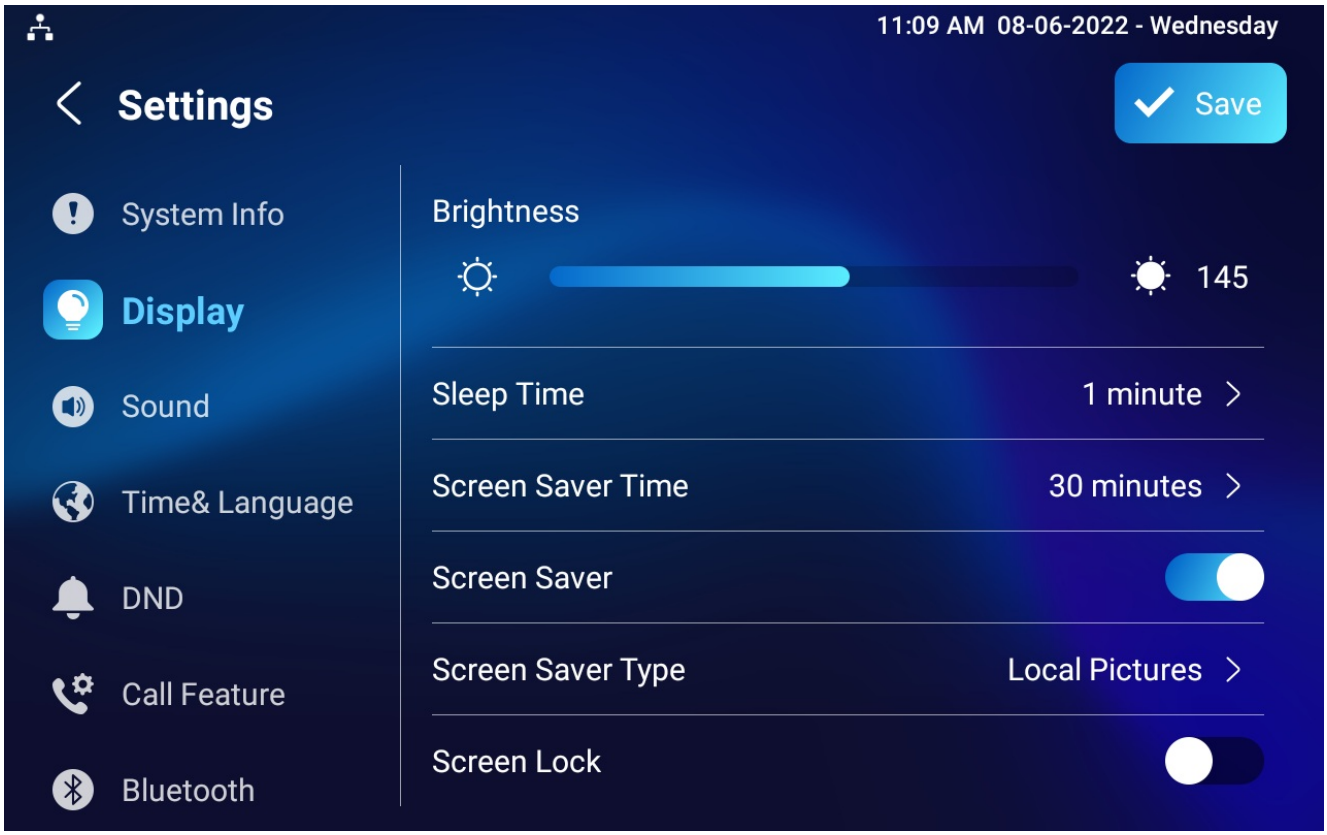
To check alarm log on device **Arming > Arming Log** screen.



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.

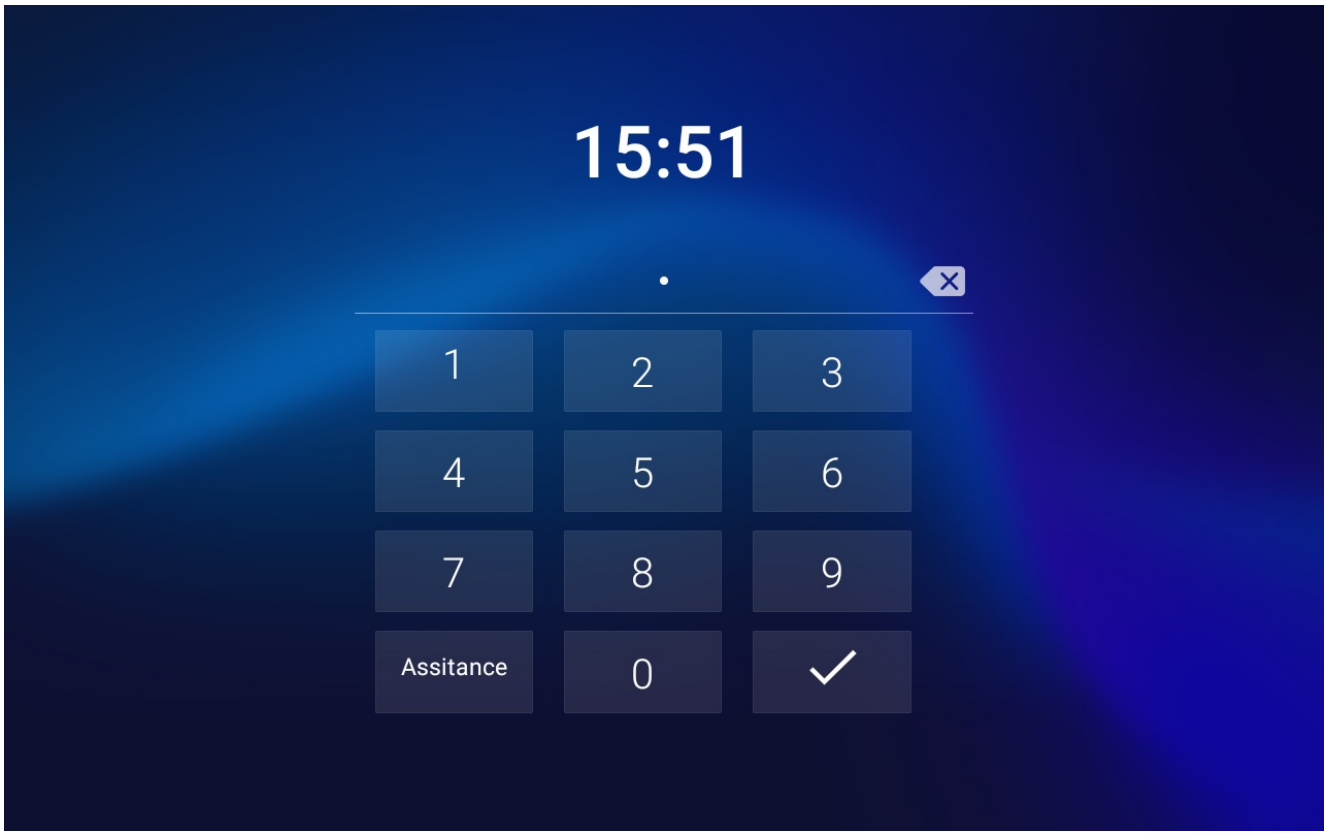
You can enable screen lock function directly on the device **Settings > Display** screen.



Screen Unlock by PIN code

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

Navigate to the **Settings > Advanced Settings > Protected Code** screen and select **System Code** to change a new password.



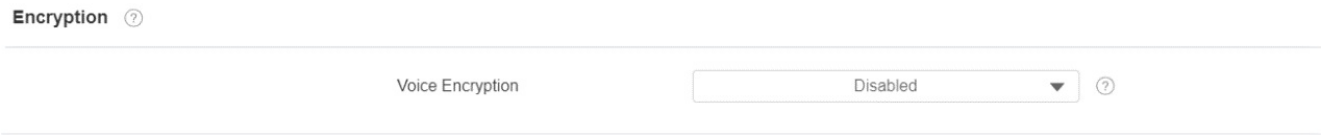
Note:

- 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**: select encryption mode from four options. If you select to disable it, the call will not be encrypted. **SRTP(Compulsory)**, all audio signals (technically speaking it is RTP streams) will be encrypted to improve security. **SRTP(Optional)**, encrypts voice from the called party, if the called party also enables SRTP, the voice signals will also be encrypted. **ZRTP(Optional)** is the protocol that the two parties use to negotiate the SRTP

session key.

Remote Control

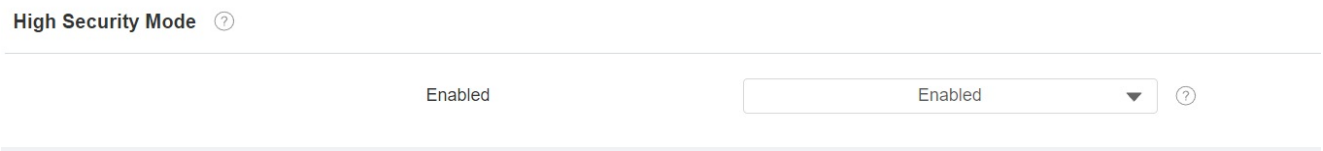
The remote control function allows a specific server to send HTTP commands or requests to the indoor monitor for actions like unlocking a local relay.

Navigate to **Device > Relay > Remote Control** 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**.



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:

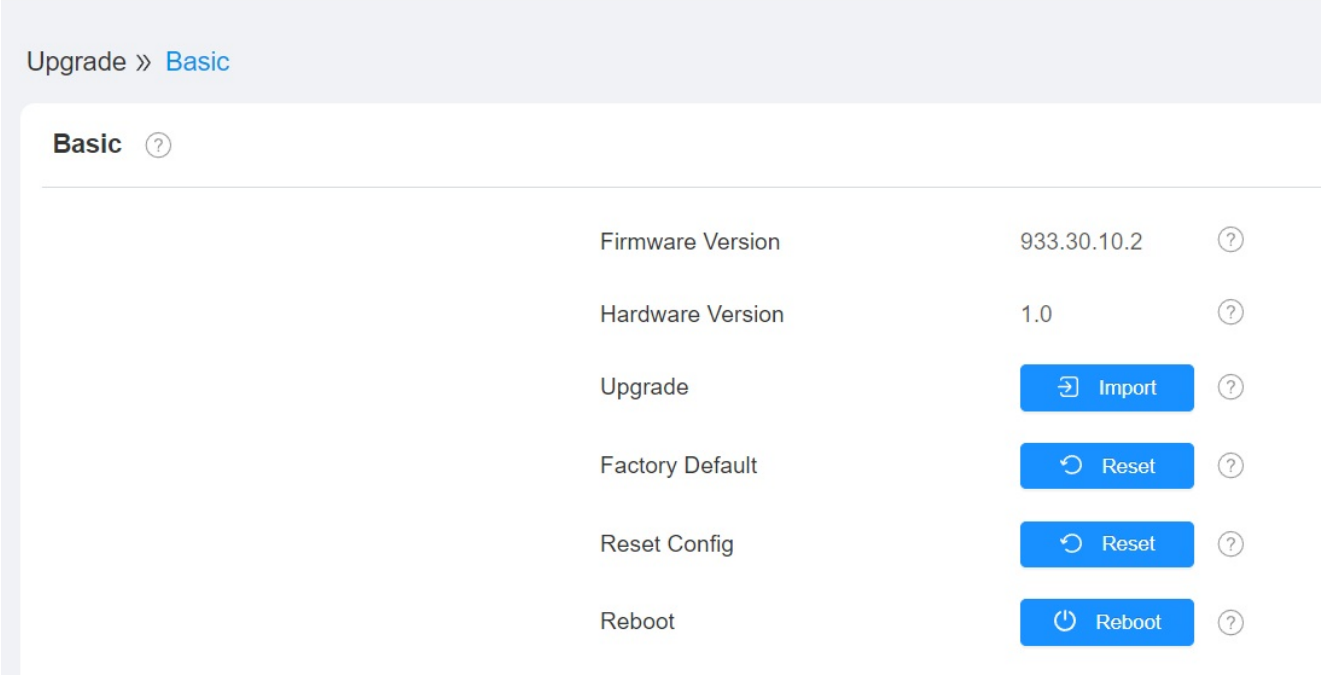
- l http://deviceIP/fcgi/do?
  action=OpenDoor&UserName=username&Password=password&DoorNum=1

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.

Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Go to **Upgrade > Basic** interface.



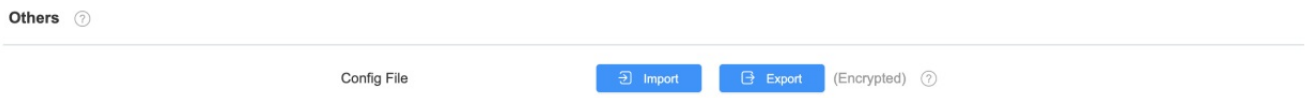
Note:

- Firmware files should be .zip format for the upgrade.

Backup

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

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

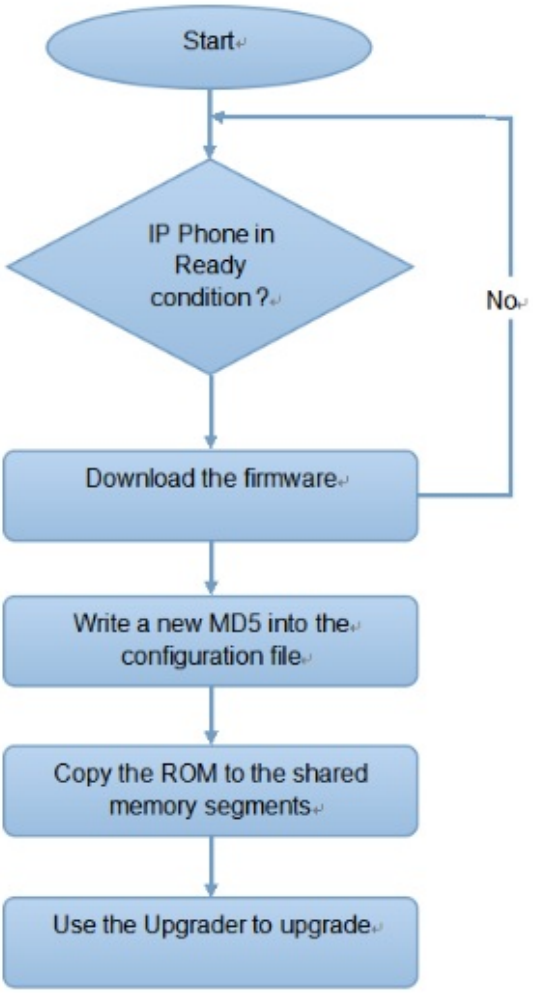


Auto-provisioning via Configuration File

Provisioning Principle

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

Please see the flow chart below:



Introduction to the Configuration Files for Auto-Provisioning

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

The difference between the two types of configuration files:

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

Note

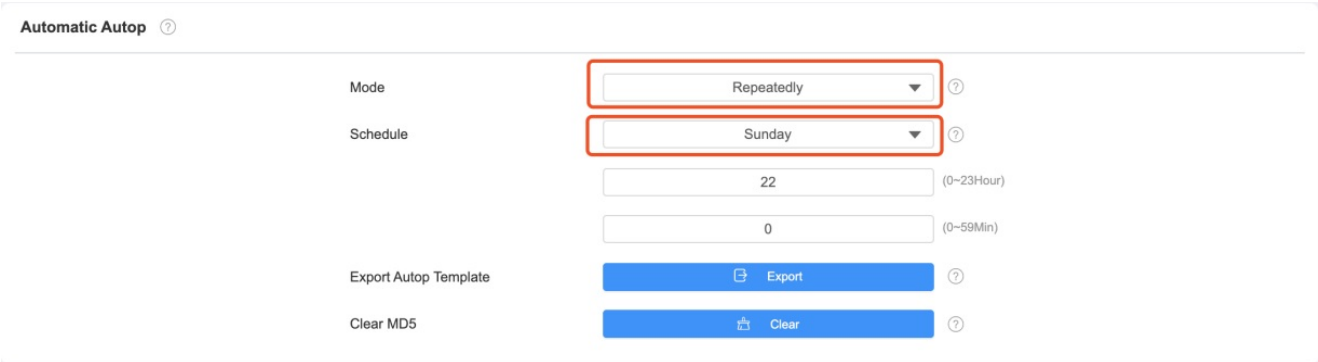
- The configuration file should be in CFG format.
- The general configuration file for the in-batch provisioning varies by model.
- The MAC-based configuration file for the specific device provisioning is named by its MAC address.
- If a server has these two types of configuration files, devices will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

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

Autop Schedule

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

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

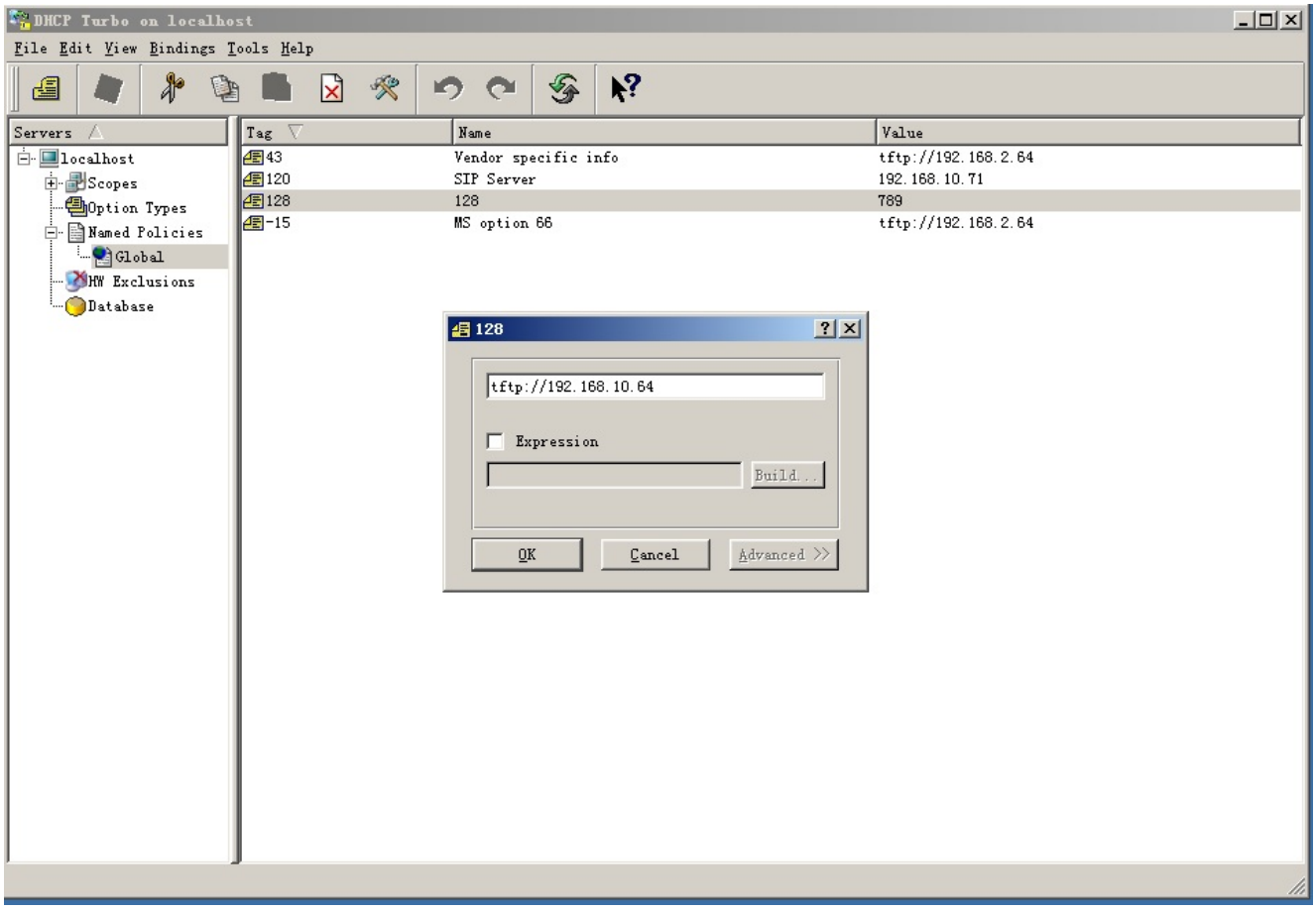


Parameter Set-up:

- **Power On**: select Power on, if you want the device to perform Autop every time it boots up.
- **Repeatedly**: select Repeatedly, if you want the device to perform autop according to the schedule you set up.
- **Power On + Repeatedly**: select Power On + Repeatedly if you want to combine 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**: select Hourly Repeat if you want the device to perform Autop every hour.

DHCP Provisioning Configuration

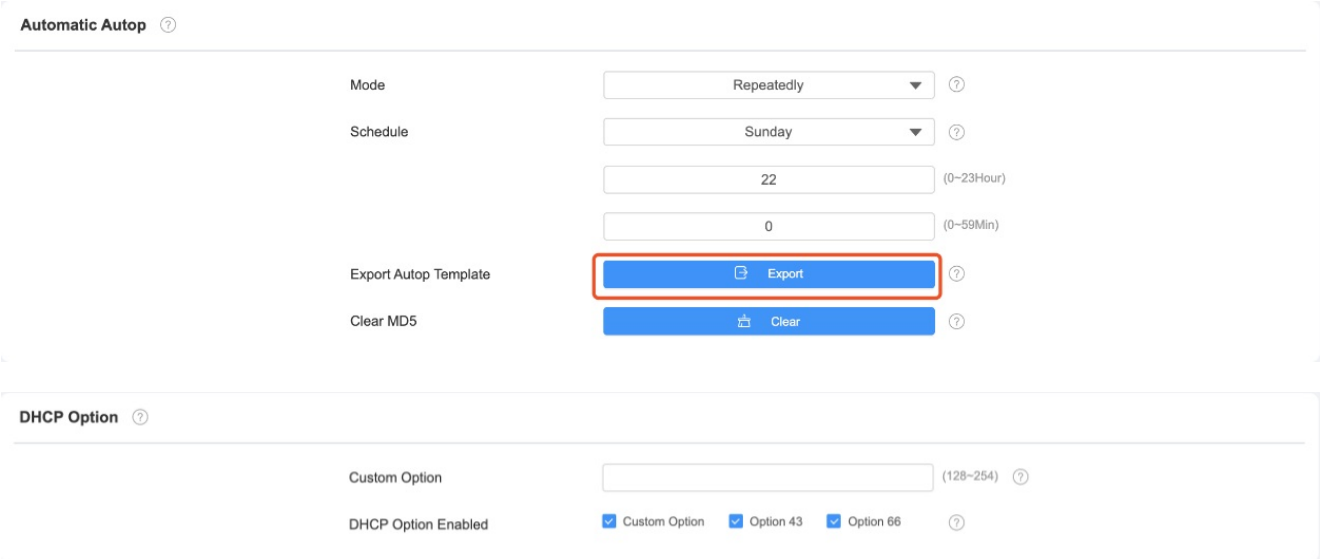
Auto-provisioning URL can also be obtained using the DHCP option which allows the device to send a request to a DHCP server for a specific DHCP option code. If you want to use **Custom Option** as defined by users with option codes ranging from 128-255), you are required to configure DHCP Custom Option on the web interface.



Note

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

Navigate to **Upgrade > Advanced** interface.



Parameter Set-up:

- **Custom Option**: enter the DHCP code that matched with corresponding URL so that device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66**: If none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for the option 66 with the update server URL in it.
- **DHCP Option 43**: If the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the update server URL in it.

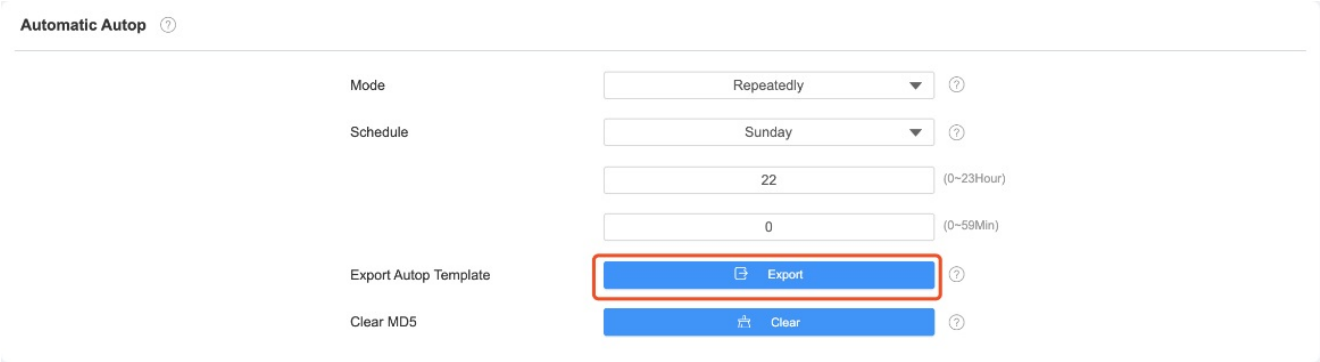
Note

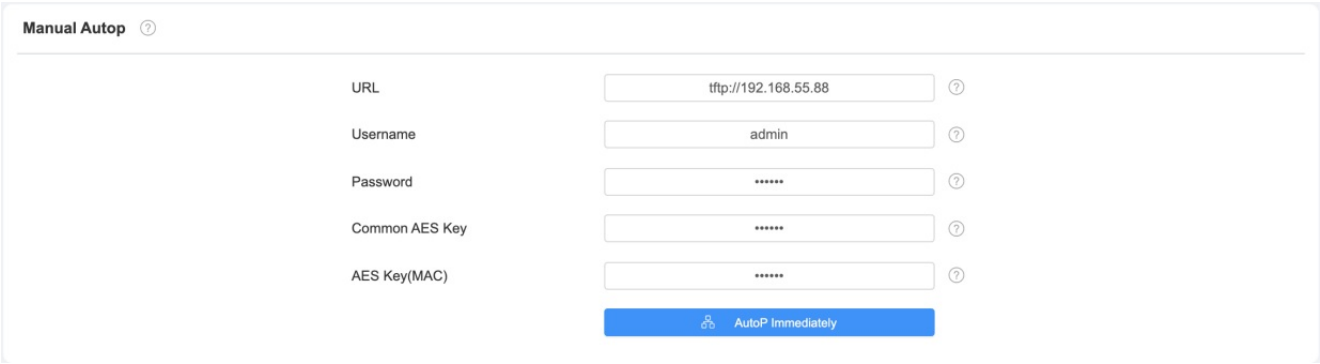
- The general configuration file for the in-batch provisioning is with the format **cfg** taking R29 as an example, r000000000029.cfg (10 zeros in total while the MAC-based configuration file for the specific device provisioning is with the format MAC_Address of the device.cfg, for example, **0C110504AE5B.cfg**.

Static Provisioning Configuration

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

Go to web **Upgrade > Advanced > Automatic Autop** interface.





Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, FTP server address for the provisioning.
- **User Name**: set up the user name if the server needs a user name to be accessed to.
- **Password**: set up the password if the server needs a password to be accessed to.
- **Common AES Key**: set up AES code for the intercom to decipher general Auto Provisioning configuration file.
- **AES Key (MAC)**: set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

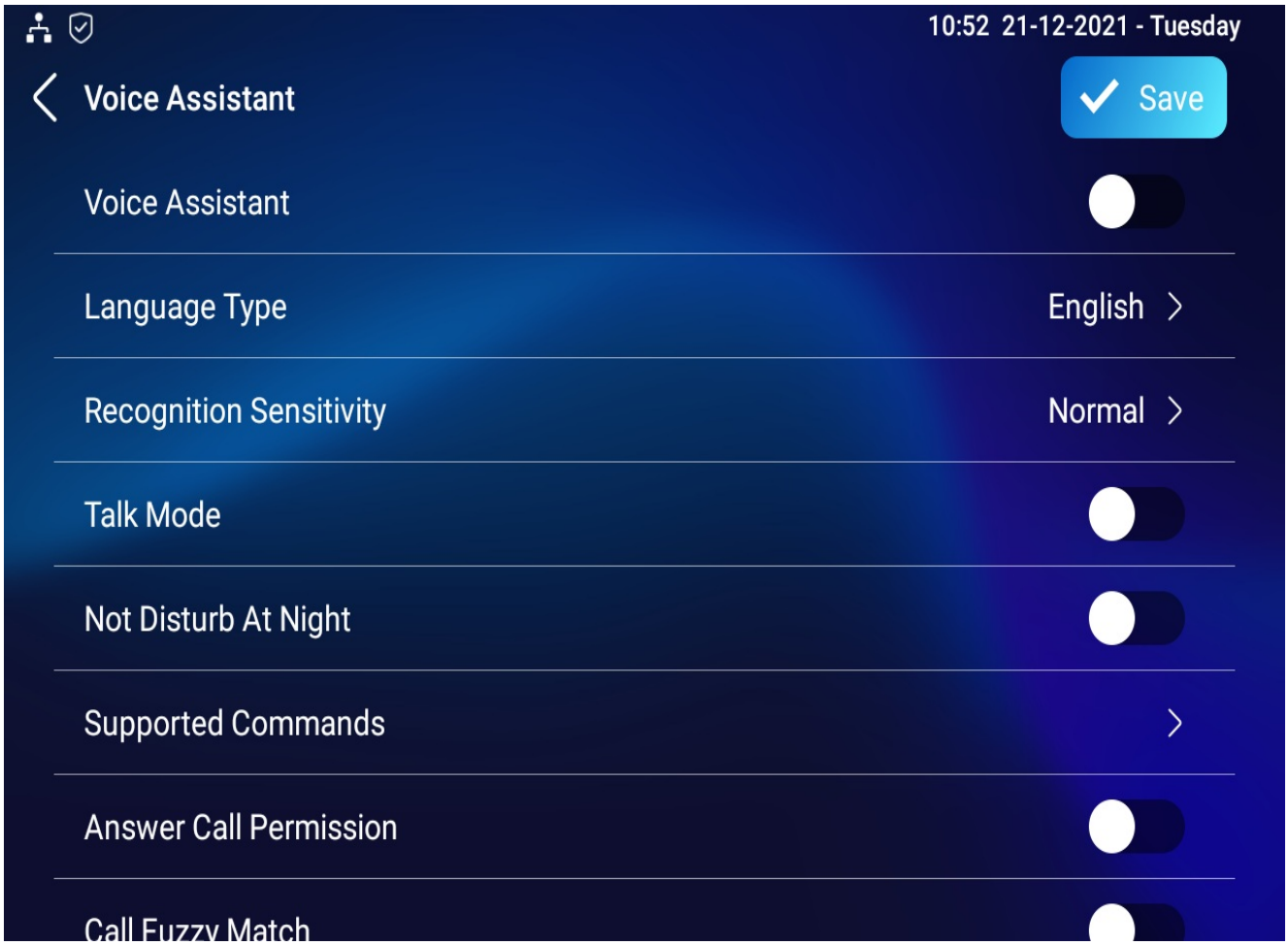
Note

- AES, as one type of encryption, should be configured only when the config file is encrypted with AES.
- Server Address Format:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/ (allows anonymous login)
    ftp://username:password@192.168.0.19/(requires a user name and password)
  - HTTP: http://192.168.0.19/ (use the default port 80)
    http://192.168.0.19:8080/ (use other ports, such as 8080)
  - HTTPS: https://192.168.0.19/ (use the default port 443)
- Akuvox does not provide user specified server. Please prepare TFTP/FTP/HTTP/HTTPS server by yourself.

Voice Assistant

Albert is a voice assistant from Akuvox. It can help you with intercom calls, door opening, arming modes, and other functions. As for the door access control, you can choose which relay to activate by this voice assistant.

To configure the voice assistant on device **Settings > Voice Assistant** screen.



Parameter Set-up:

- **Language Type**: select the language according to your need.
- **Recognition Sensitivity**: adjust the voice assistance recognition sensitivity among **Low, Normal**, and **High** according to your need.
- **Talk Mode**: move the toggle switch to the right if you want to enable the talk mode. When the **Talk Mode** is enabled, the voice assistant will stay on to receive your voice commands for 30 seconds without your needing to call **Albert** again to wake up the voice assistant, while if you disable it, the voice assistant will be wake up again for each voice command.
- **Not Disturb At Night**: move the toggle switch to the left to enable the function. This

function is applied when you want the voice assistant to stay silent while carrying out what it is made to do according to your voice commands.

- **Supported Command**: enable or disable the voice commands according to your need.

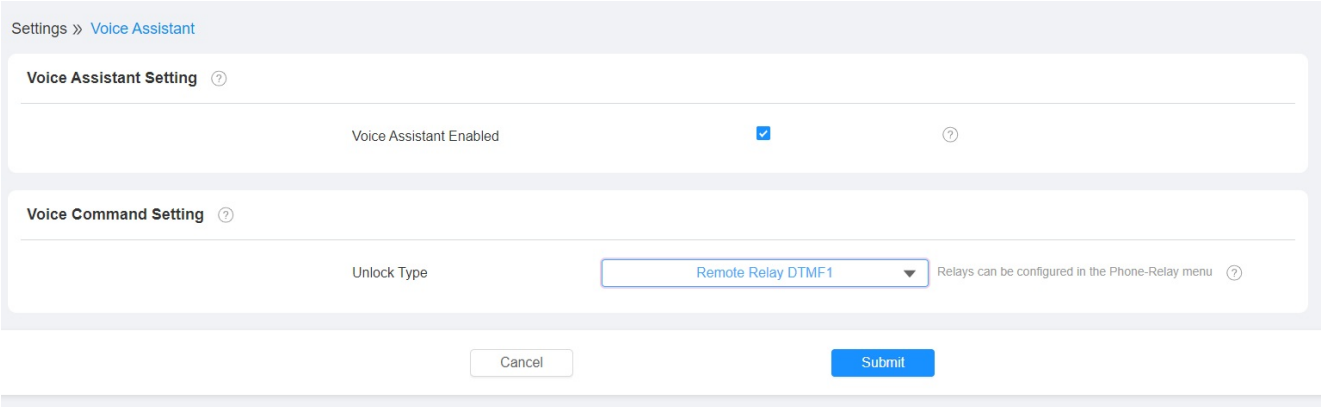
Please see the voice command details below:

NO	Voice Command	Description	Voice Prompt
1	Intruder mode off	Use it when you want to clear the arming mode when the arming alarm is triggered. (you are required to enter the disarm password in the pop-out window initiated by the voice assistant)	Please Input Password
2	Clear arming	ibid	ibid
3	night mode	Use it when you want to change the arming mode to night mode	• Started it, sweet dreams! • Made it, good night • Sure, sleep mode is on • OK, start sleep mode, have a good night Alright, sleep mode is opened, have a nice dream
4	sleep mode	Use it when you want to change the arming mode to sleep mode	• Sure, sleep mode is on • OK, start sleep mode, have a good night • Alright, sleep mode is opened, have a nice dream • Made it, good night • Started it, sweet dreams!
5	away mode	Use it when you want to change the arming mode to away mode	• Sure, away mode is on • OK, start away mode • Alright, away mode is opened • Made it • Made it, have a good day • Done, away mode is started
6	home mode	Use it when you want to change the arming mode to home mode	• Sure, home mode is on • OK, start home mode • Alright, home mode is opened • Made it • Done, home mode is started
7	open door	Use it when you want to open the door	• Sure, the door is open • The door is open for you • No problem, open the door • Opened, always here for you Yep, door is opened now
8	open the door	Use it when you want to open the door	• Sure, the door is open • The door is open for you • No problem, open the door • Opened, always here for you Yep, door is opened now

9	disable DND	Use it when you want to disable the DND mode	• Yes, closed it for you • Welcome back, DND is off • DND is closed, to mingle with the world • Sure, DND is off
10	enable DND	Use it when you want to enable the DND mode	• OK, DND is on • Done, enjoy yourself • DND is on, feel your inner peace • Turn on it now
11	emergency	Use it when you want to dial SOS number	• Got it, calling SOS as soon as possible • OKay, be relaxed, making a emergency call now • Calling ambulance now • Calling SOS now, please hold on • God bless you, calling emergency now • Hold on please, calling emergency right now • Take it easy, calling emergency right now
12	help me	ibid	ibid
13	call manager	use it when you want to call "manager" you name set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
14	call staff	use it when you want to call "stuff" you named and set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
15	call carer	use it when you want to call "carer" you named and set up in the phonebook	• Please choose one for calling • Sorry I didn't get that
16	open message	use it when you want to check text message.	• Got it, please check • OK, message is opened, you can write some contents to send • Message is ready for you • already opened it for you
17	open monitor	use it when you want to check monitor	Got it , please check
18	homepage	use it when you want to go to home screen	• Home page is already for you. Already got it for you
19	enable mute	use it when you want to mute your voice on the indoor monitor so that the caller or callee will be not be able to hear you.	• OK, mute is on • Done, enjoy yourself • Mute is on, feel your inner peace • Set it now
20	disable mute	use it when you want to unmute your voice on the indoor monitor so that the caller or callee will be able to hear you.	• Sure, mute is off • Mute is closed, to mingle with the world • Welcome back, mute is off • Yes, closed it for you
21	shut down/cancel	Use it when you want to turn off the voice assistant function.	• See you • See you later • Bye • Good bye • See you next time • Bye, best regards • See you, have a great time

- **Answer Call Permission**: enable it when you so that you can answer or reject the incoming call via voice assistant by replay **Yes** or **No**.
- **Call Fuzzy Match**: Enable it to allow fuzzy matching of the contact name, for example, if you have Tom and Tomy in your phonebook, then Tomy will also appear when you call Tom, and you are required to select the right contact manually.

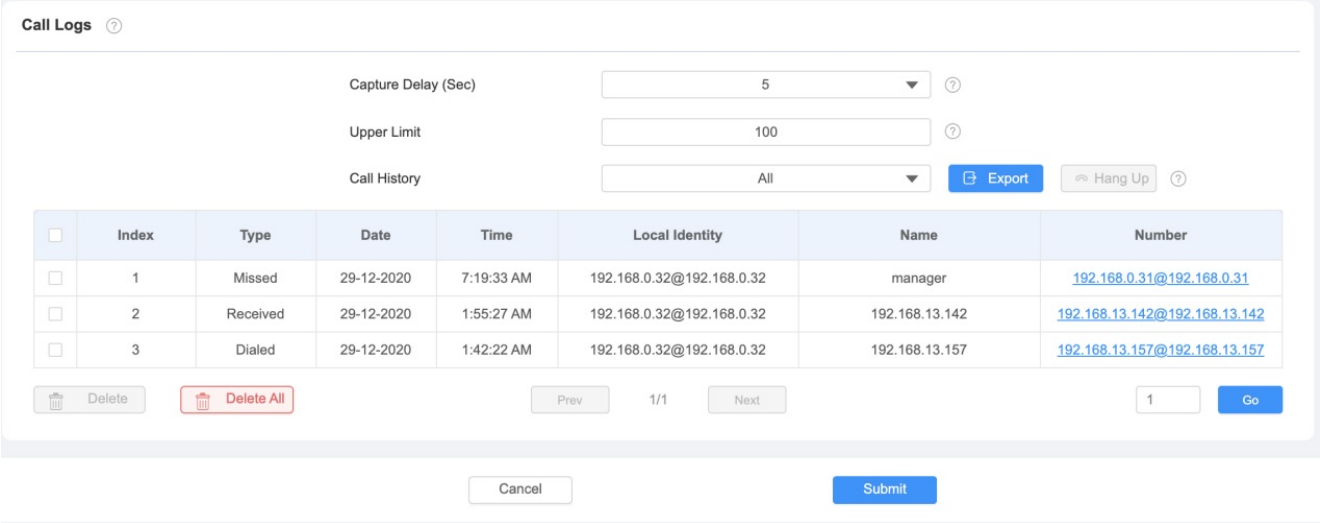
To enable the voice assistant and set the voice assistant-controlled relay on the web **Settings > Voice Assistant > Voice Assistant Setting** interface, you can tick the check box to enable the voice assistant function. Then go to **Voice Command Setting** to select a specific relay to be triggered via voice assistant.



Call Log

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

Navigate to **Contacts > Call logs** interface.



Parameter Set-up:

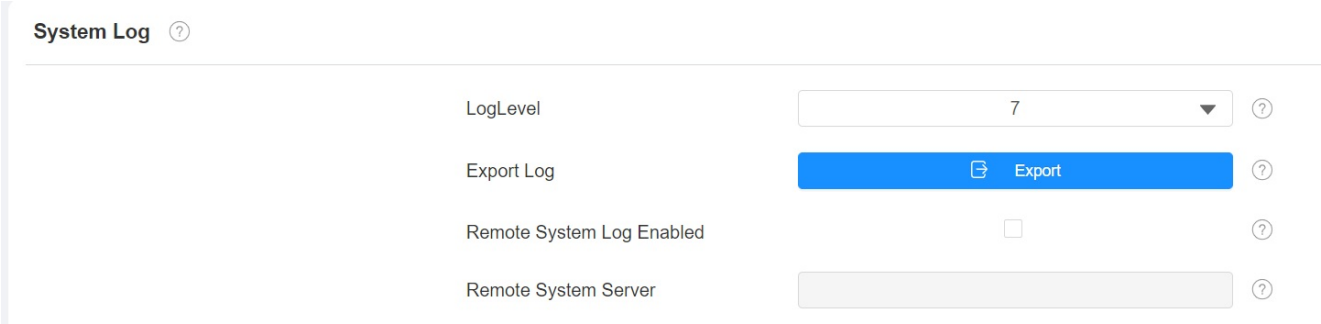
- **Capture Delay**: set the image capturing starting time when the device goes into video preview.
- **Upper Limit**: set the maximum screenshot storage capacity, when the capacity is reached the previous screenshots would be overwritten.
- **Call History**: select call history among four options: **All**,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

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.



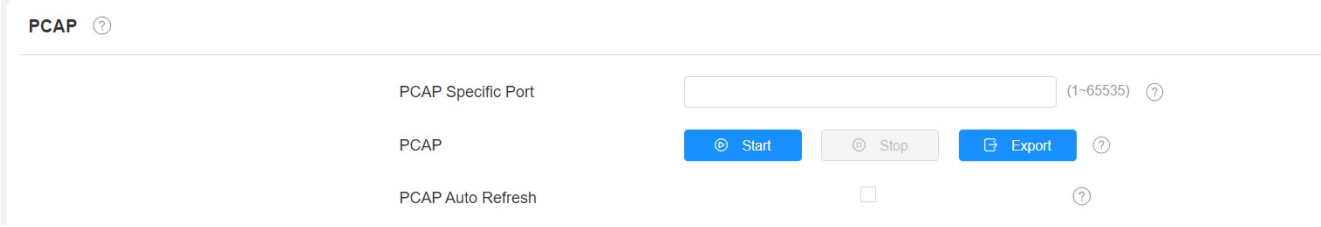
Parameter Set-up:

- **Log Level**: select log levels from 0 to 7 levels. You will be instructed by Akuvox technical staff about the specific log level to be entered for debugging purpose. The default log level is 3. The higher the level is, the more complete the log is.
- **Export Log**: click the **Export** tab to export temporary debug log file to a local PC.
- **Export Debug Log**: click the **Export** tab to export debug log file to a local PC.
- **Remote System Log**: select **Enable** or **Disable** if you want to enable or disable the remote system log.
- **Remote System Server**: enter the remote server address to receive the system log and the remote server address will be provided by Akuvox technical support.

PCAP for Debugging

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

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



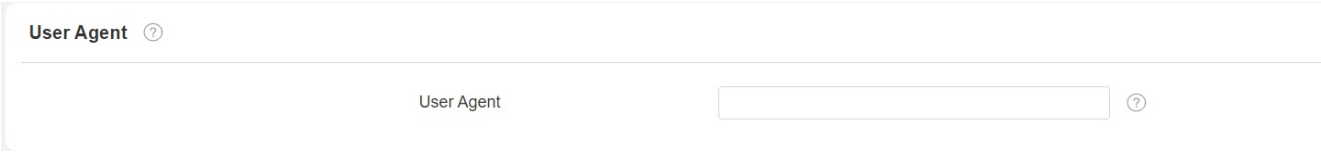
Parameter Set-up:

- **Specific Port**: select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP**: click **Start** tab and **Stop** tab to capture a certain range of data packets before clicking **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh**: select **Enable** or **Disable** to turn on or turn off the PCAP auto fresh function. If you set it as **Enable**, then the PCAP will continue to capture data packets even after the data packets reached their 50M maximum in capacity. If you set it as **Disable**, the PCAP will stop data packet capturing when the data packet captured reaches 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.

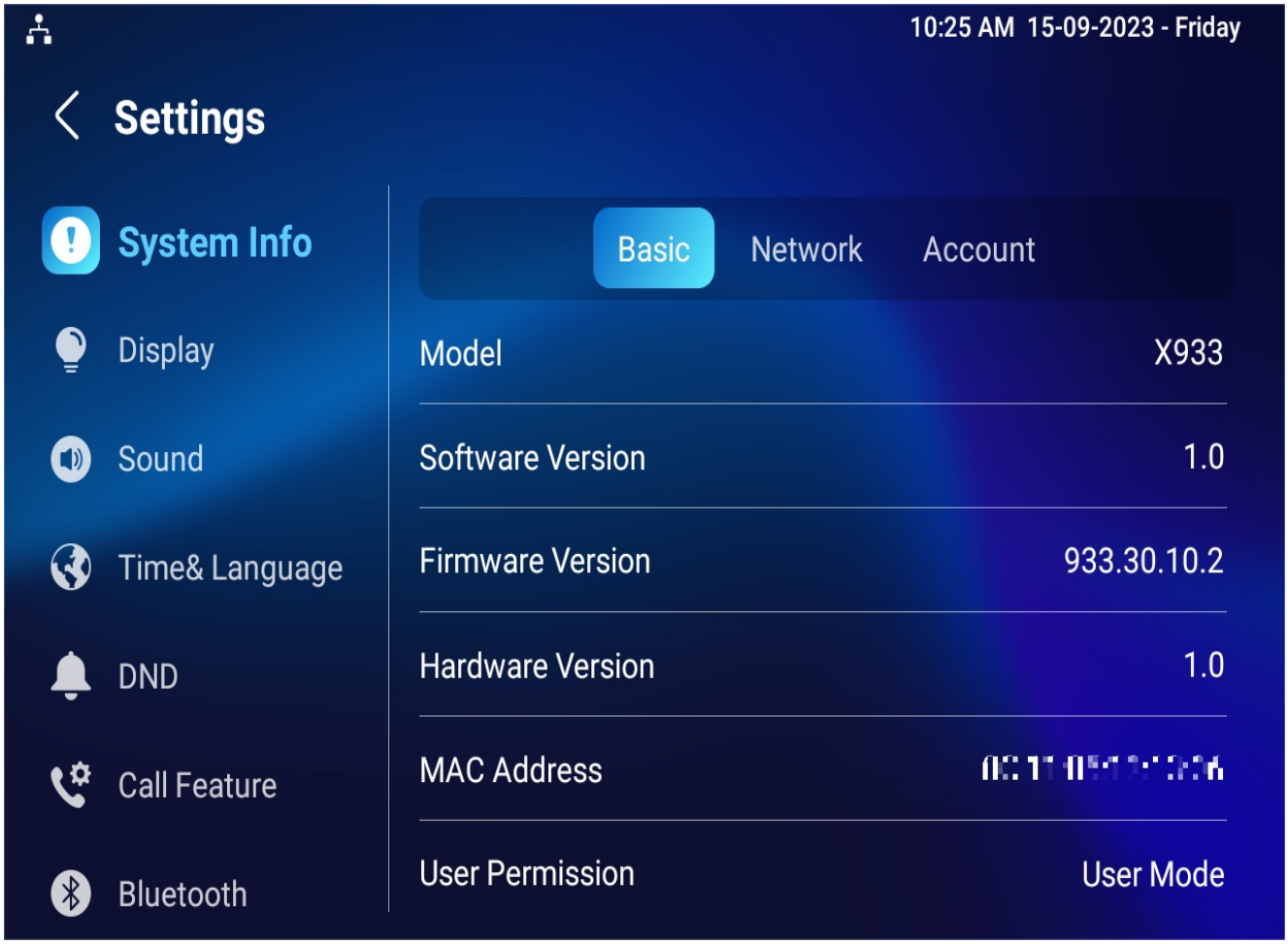


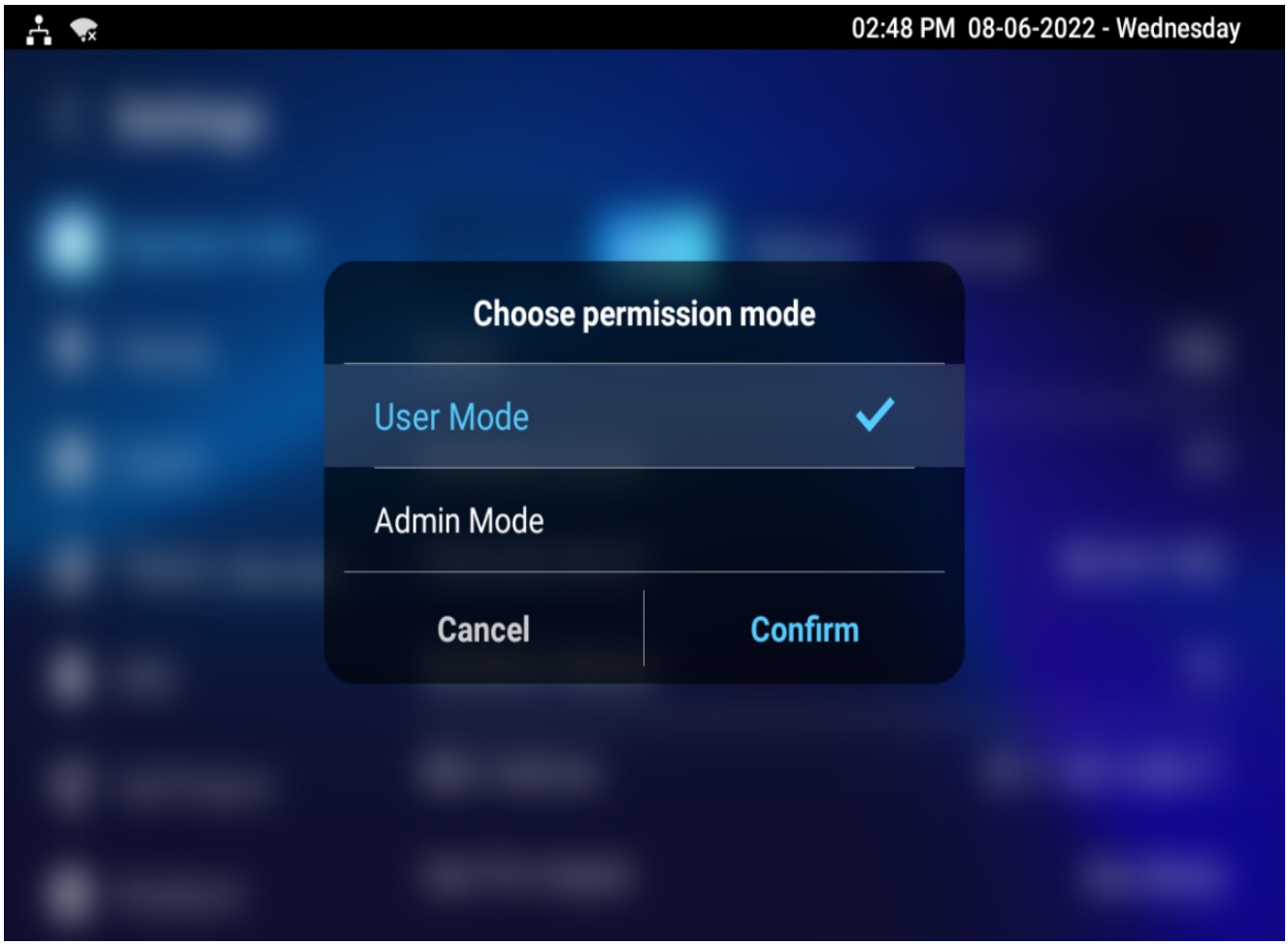
Device Integration with Third Party

Enter Applications Screen

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

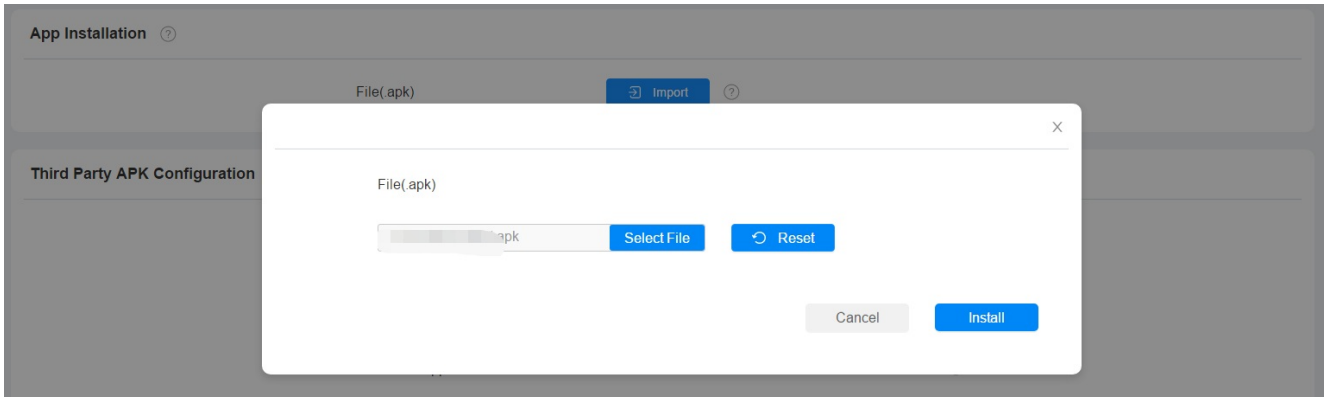
To do the configuration on device **Settings > System Info** interface. You can press on **User Mode** 10 times and press **Admin Mode** and press **Confirm**.



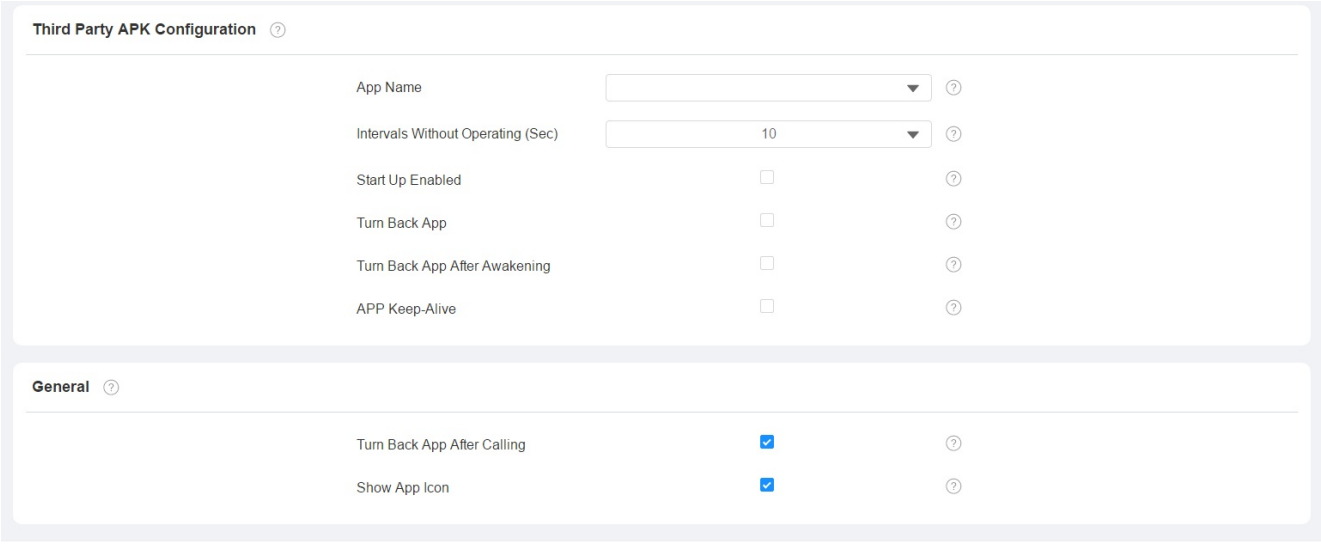


Install Third-party App

You can install the third-party App to your device on the device web **Device >Third-party APK** interface. Choose a suitable .apk file from PC to upload. If you want to clear the apk file uploaded, click **Reset**.



To configure the installed third-party app, you can click **App Name** field to select the specific name of the installed APK files for configuration. Then tick the check boxes of the each field for specific configuration you need.



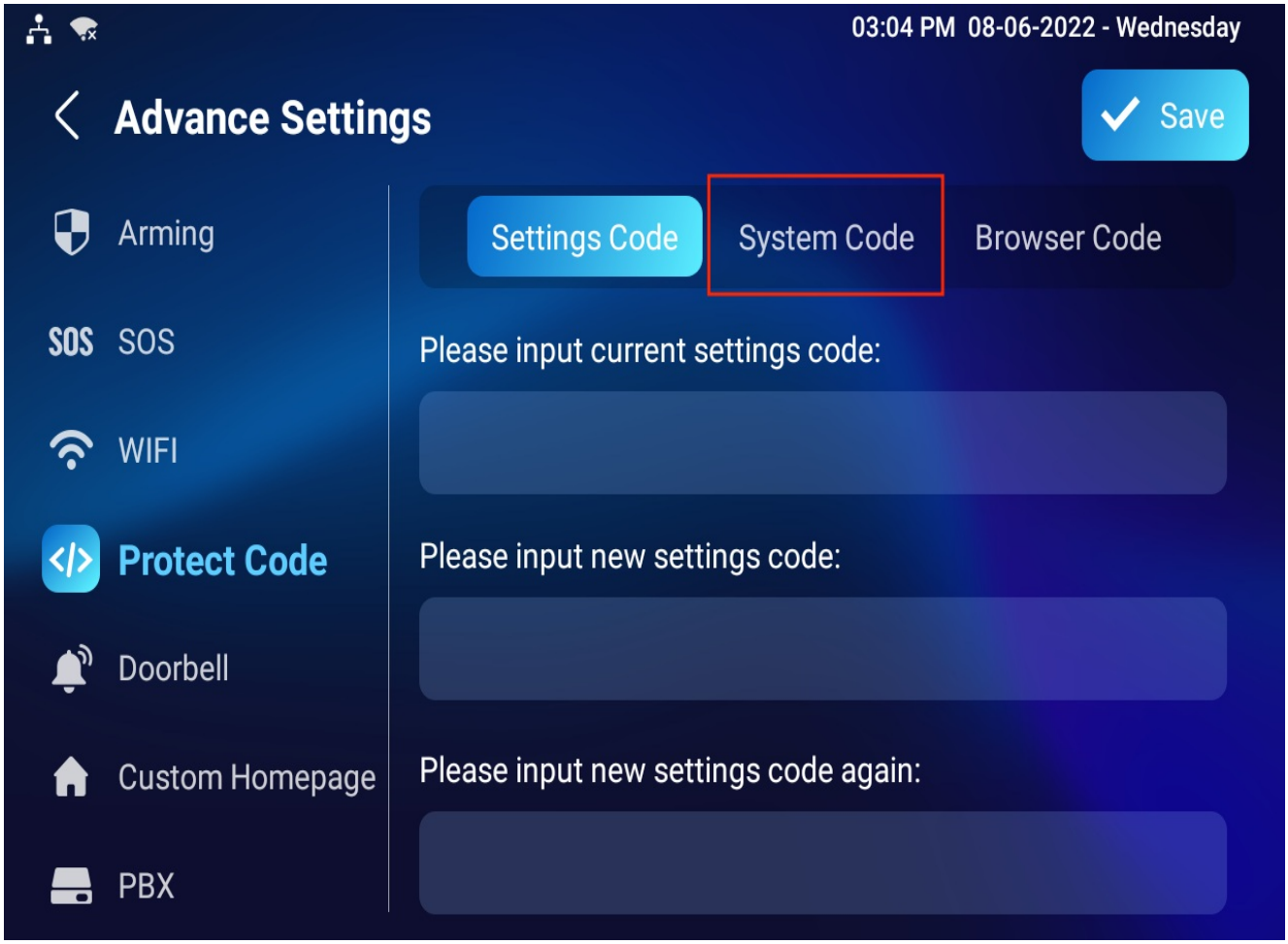
Parameter Set-up:

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

Password Modification

Modify Device Basic Setting Password

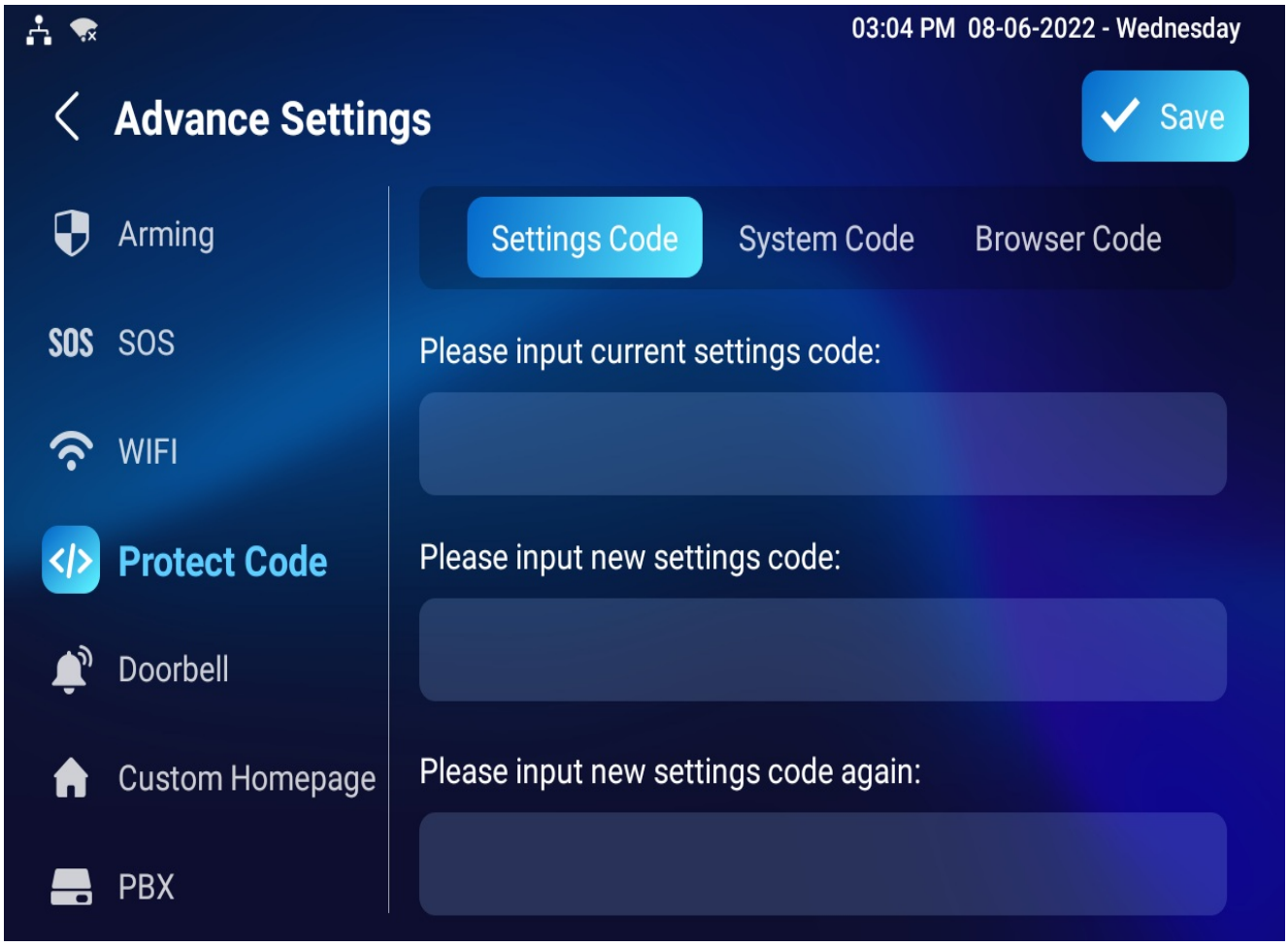
To do the configuration on device **Settings > Advanced Settings > Protected Code** screen to choose **System Code** to change a new password. The default password is 123456.



Modify Device Advanced Setting Password

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

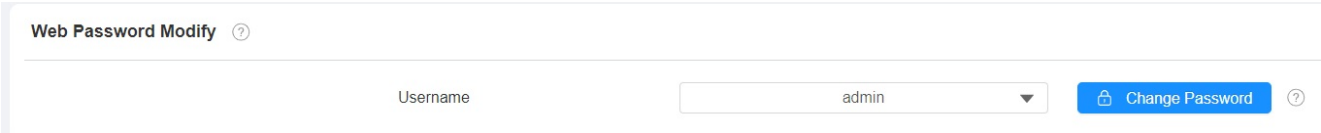
To set it up on the device, go to **Setting > Advanced Settings > Protect Code > Setting Code** screen.



Modify Device Web Interface Password

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

To set it up on the device web, go to **Security > Basic > Web Password Modify** interface.



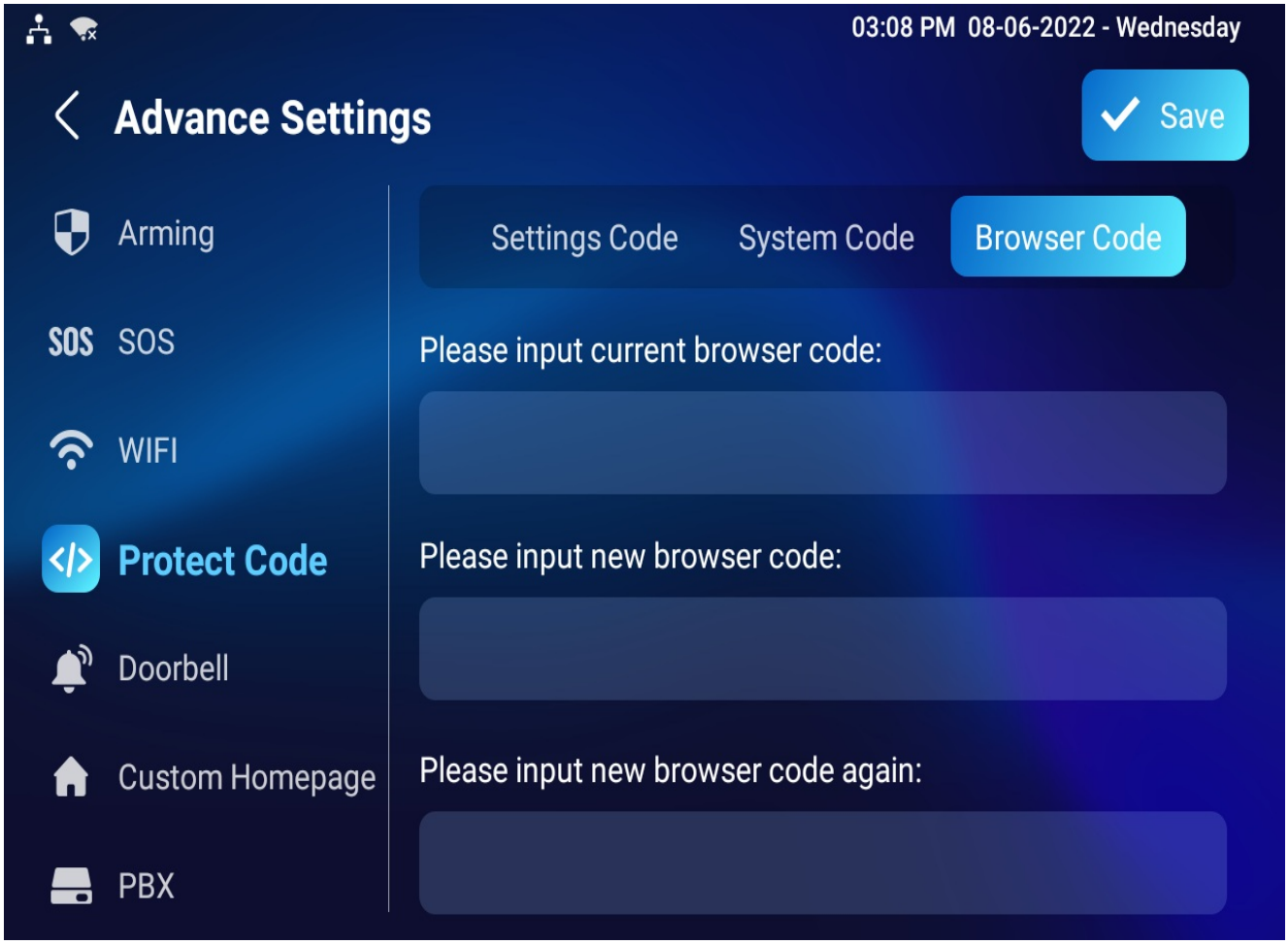
Note

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

Modify Browser Password

This password is used to lock the browser on the device in case someone abuses the browser for any unwanted application. You can do this configuration on the device screen. The default password is 123456.

You can do this configuration on device **Settings > Advanced Settings > Protected Code > Browser Code** screen.



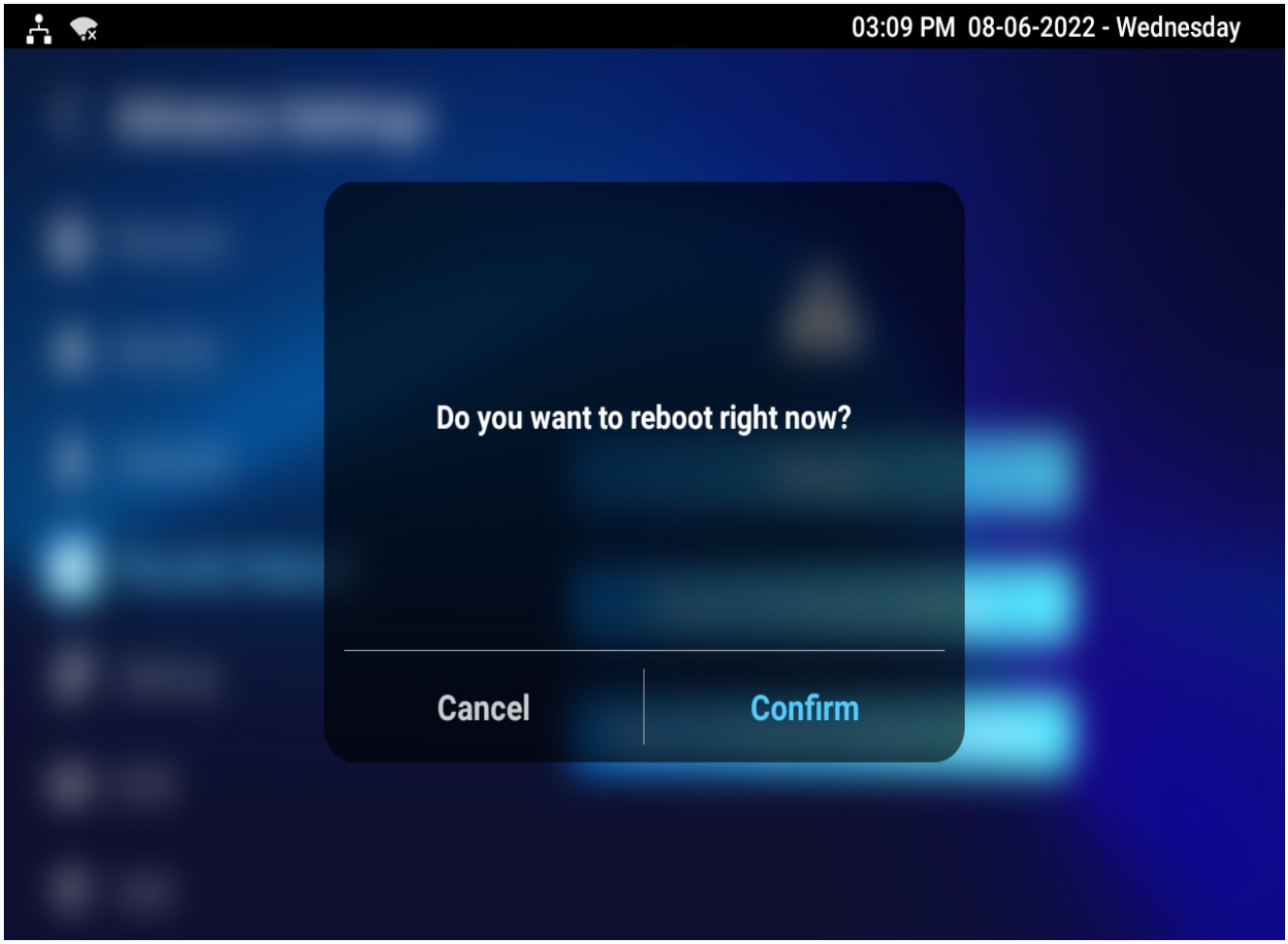
System Reboot&Reset

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.

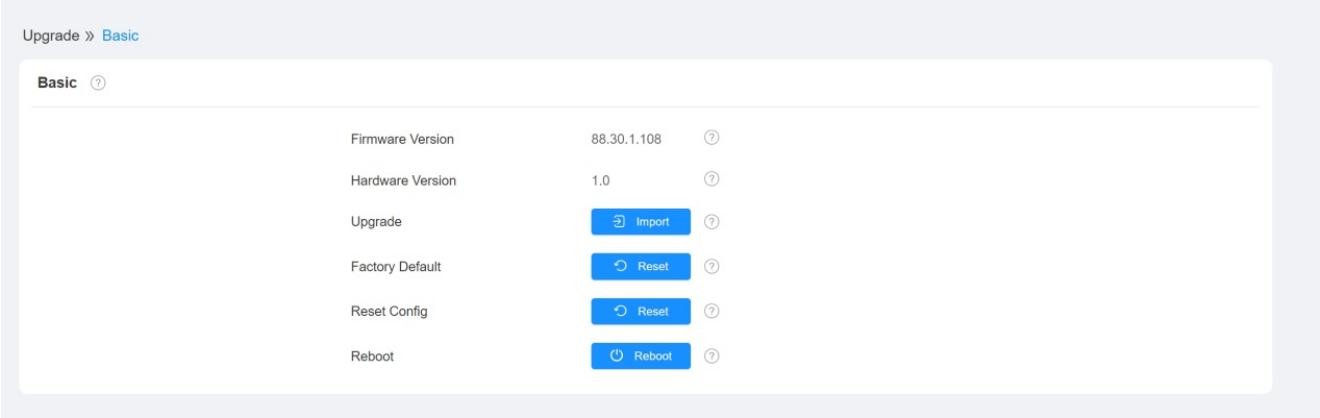
To restart to the system setting on device **Settings > Advance Settings > Reset&Reboot** screen.



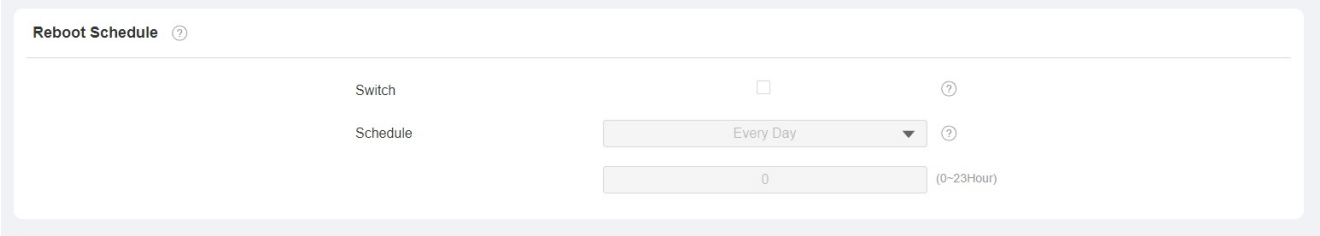
Reboot on the Web Interface

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 reboot on **Upgrade > Basic** interface.



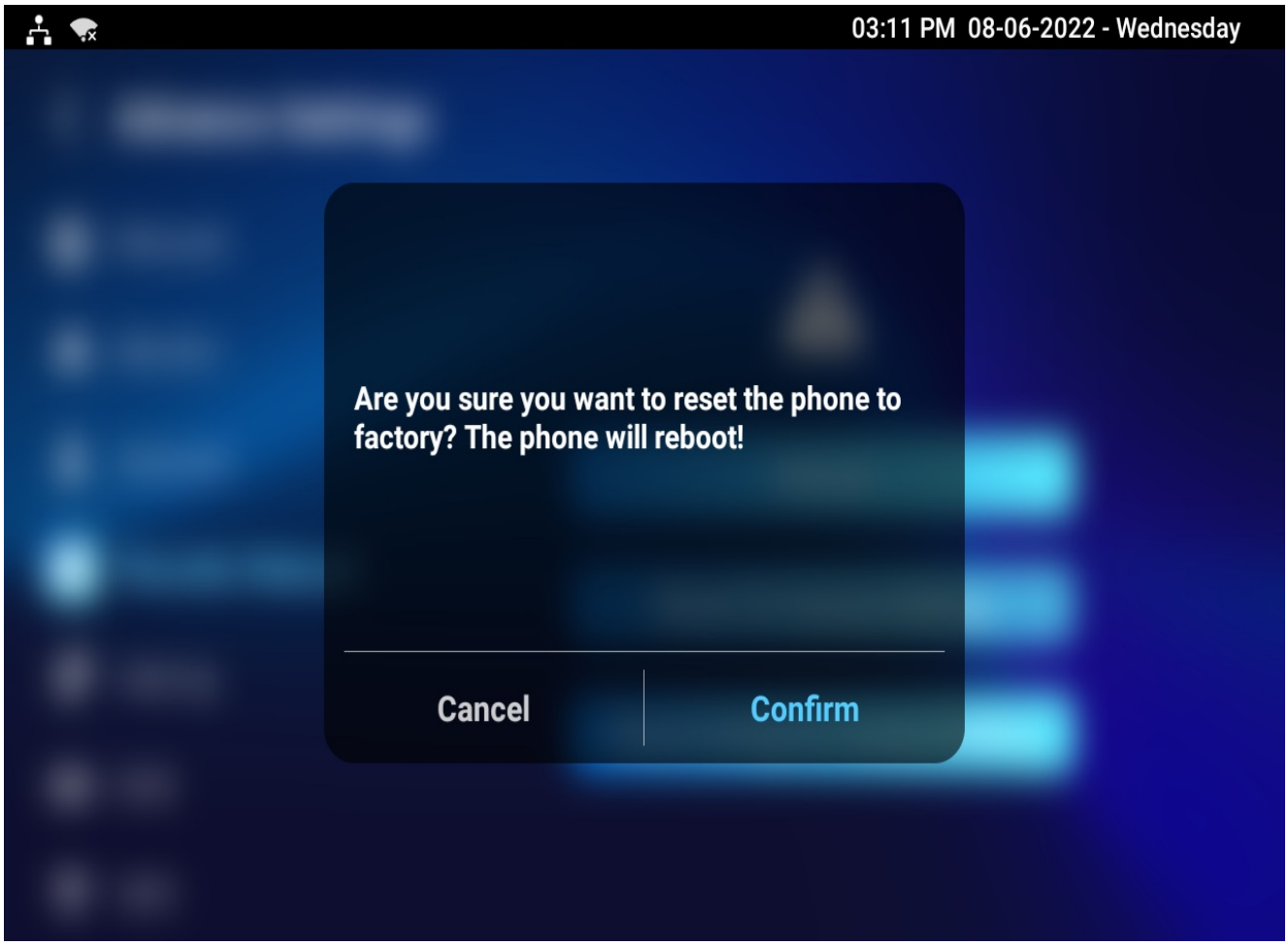
To set up the device restart schedule on web **Upgrade > Advanced > Reboot Schedule** interface.



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



Reset on the Web Interface

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

Navigate to **Upgrade > Basic** interface.