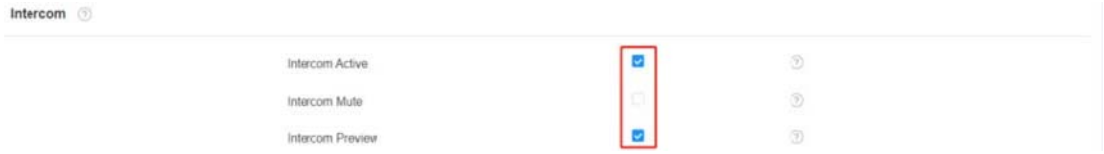
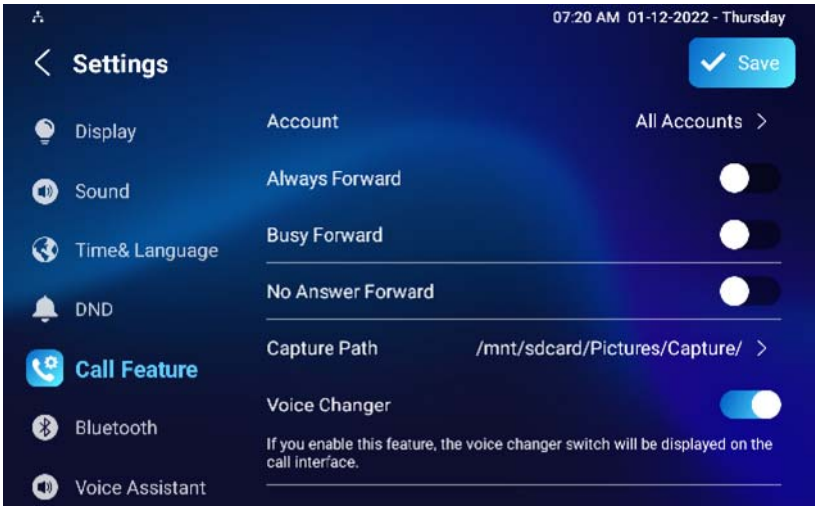


Parameter Set-up:

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

12.11. Voice Changer

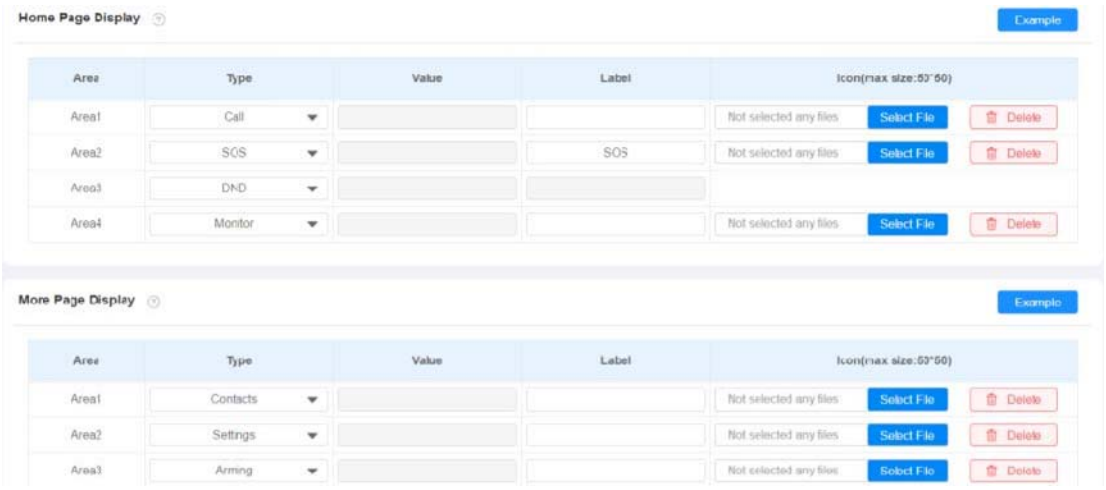
Voice changer help ensures users' privacy and home security. For example, users (especially women and children) can protect themselves by changing their voices when talking to a stranger. Path: **Settings > Call Feature**.



12.12. Emergency Call Setting

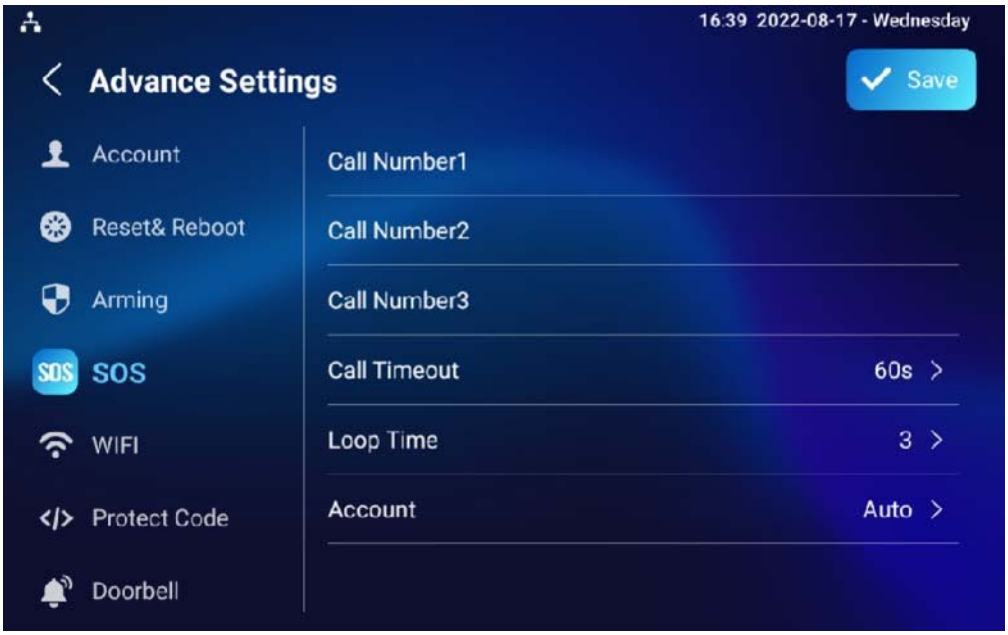
Emergency call is used to call three emergency contacts when you are in urgent status. Especially for the elders and children. To display Emergency call softkey on web **Device > Display Setting >Home Page Display/More Page**

Display interface.



After setup on web , you also need to do the configuration on the device or on the device web interface.

To set it up on the device, go to **Settings >Advance Settings >SOS** screen.

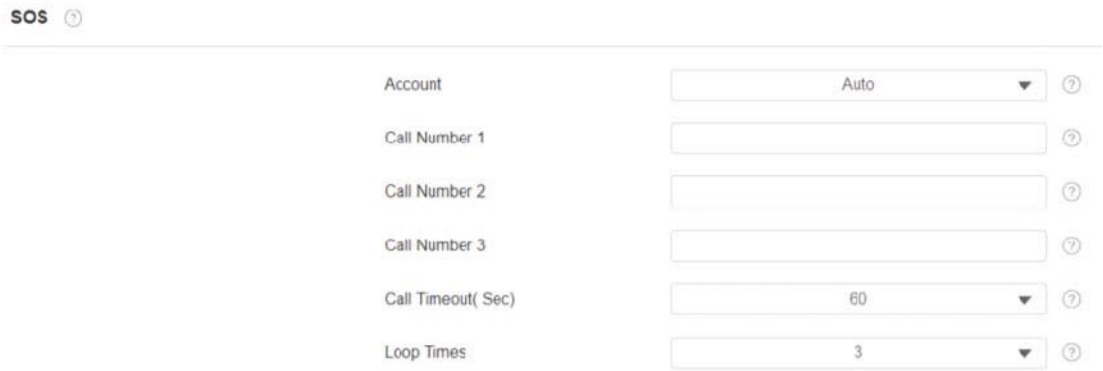


Parameter Set-up:

- **Call Number**: to set up 3 SOS numbers. Once users press **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.

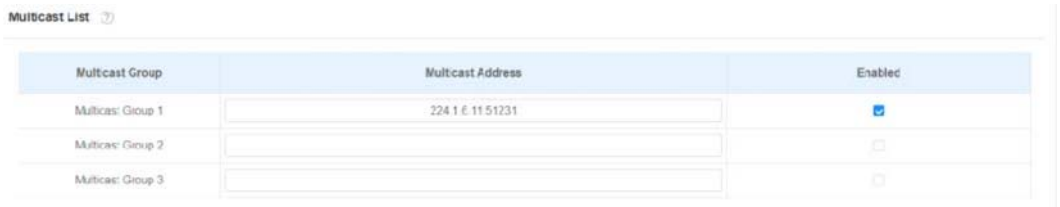
- **Call Timeout**: set up the timeout for each number. Once users call out, if the other side will not answer within the timeout, indoor monitors will continue to call the next number.
- **Loop Times**: set up the call loop times.
- **Account**: select the account from which you want to make SOS calls.

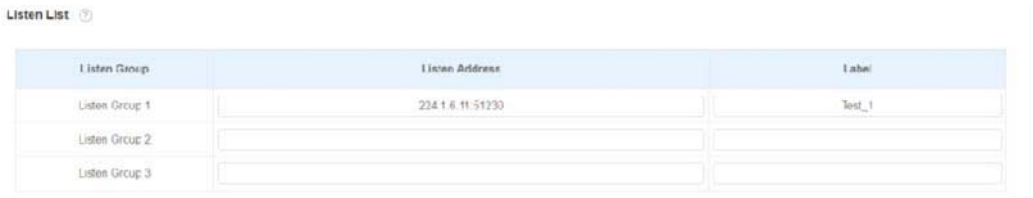
To set it up on the web interface, go to **Device > Intercom > SOS**.



12.13. Multicast Configuration

S567 allows you to conduct one-to-many broadcasting via the multicast function on the web **Device > Multicast > Multicast List** interface.



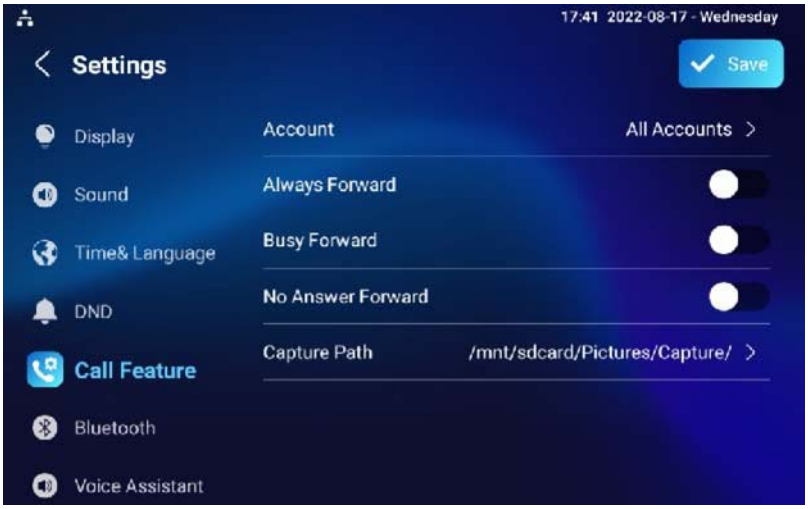


12.14. Call Forwarding Setting

Call Forward is a feature used to redirect an incoming call to a specific third party. Users can redirect the incoming call based on different scenarios. Typically, call forward has three modes: **Always Forward/ No Answer Forward/Busy Forward**.

12.14.1. Call Forwarding Configuration on the Device

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



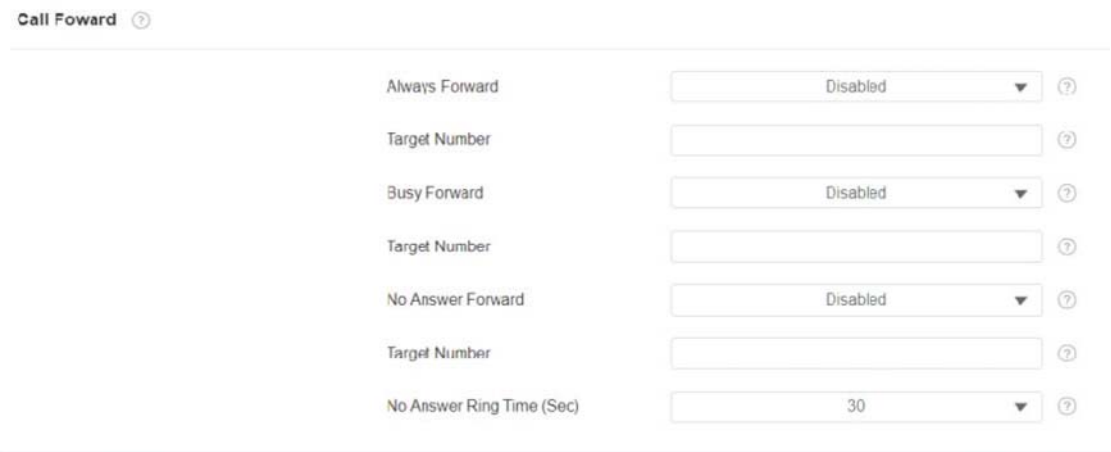
Parameter Set-up:

- **Account:** to choose which account shall implement the call forwarding feature.
- **Always Forward:** to enable Always Forward function; all incoming calls will be automatically forwarded to a specific number.
- **Busy Forward:** to enable Busy Forward function; incoming calls will be forwarded to a specific number if the phone is busy.
- **No Answer Forward**: to enable 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 S567 enables always forward / busy forward / no answer forward.

- **Capture Path:** select the storage location for all the captured pictures.

12.14.2. Call Forwarding Configuration on the Web Interface

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



Parameter Set-up:

- **Always Forward:** to enable Always Forward function; all incoming calls will be automatically forwarded to a specific number.
- **Target Number**: enter the specific forward number if S567 enables always forward.
- **Busy Transfer:** to enable Busy Forward function; incoming calls will be forwarded to a specific number if the phone is busy.
- **Target Number:** enter the specific forward number if S567 enables the busy forward.
- **No Answer Forward:** to enable No Answer forwarding function; incoming calls will be forwarded to a specific number if the phone is not picked up within no answer ring time.
- **Target Number**: enter the specific forward number if S567 enables the **No Answer Forward.**

- **No Answer Ring Time (Sec):** set the no answer time ring time interval from 0-120 seconds before the call is transferred to a designated number.

13. Intercom Message Setting

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

13.1. Manage Messages

You can check, create and clear messages as needed on the S567 indoor monitor **Message** screen. Click **Add** to create a new text message and **Clear** to delete the existing messages.

Parameter Set-up:

- **Notification:** the message from property manager, this feature is only available when using SDMC or Akuvox SmartPlus.
- **Text MSG:** to send or receive or manage the text message here.
- **Owner MSG:** if you enable this feature, and if 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 if nobody answers the incoming call within the preset ring time, it will save the visitor record.

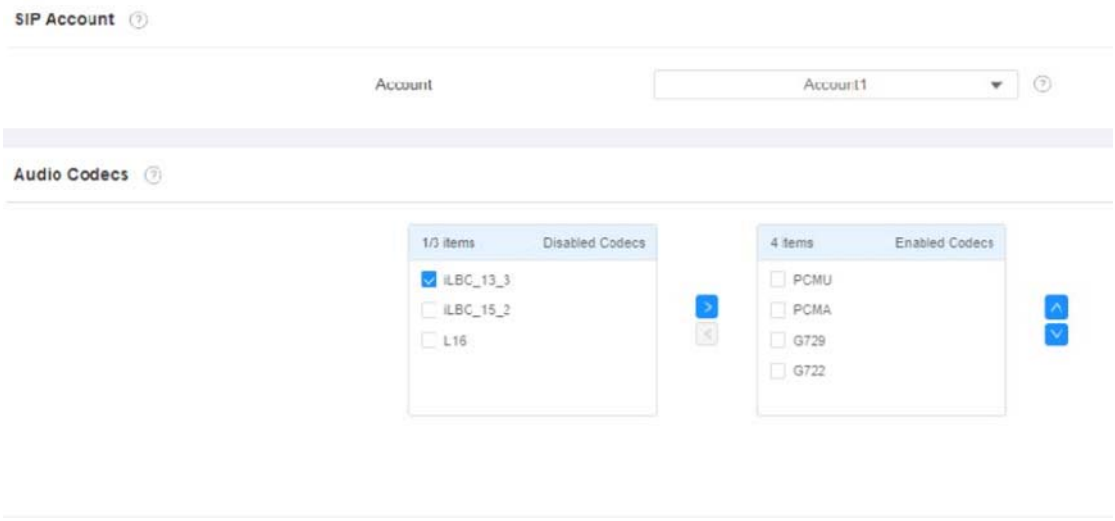
- **Family MSG:** you can record audio messages for your family members.

14. Audio& Video Codec Configuration for SIP Calls

14.1. Audio Codec Configuration

Akuvox indoor monitor supports seven types of Codec (iLBC_13_3, iLBC_15_2, 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.



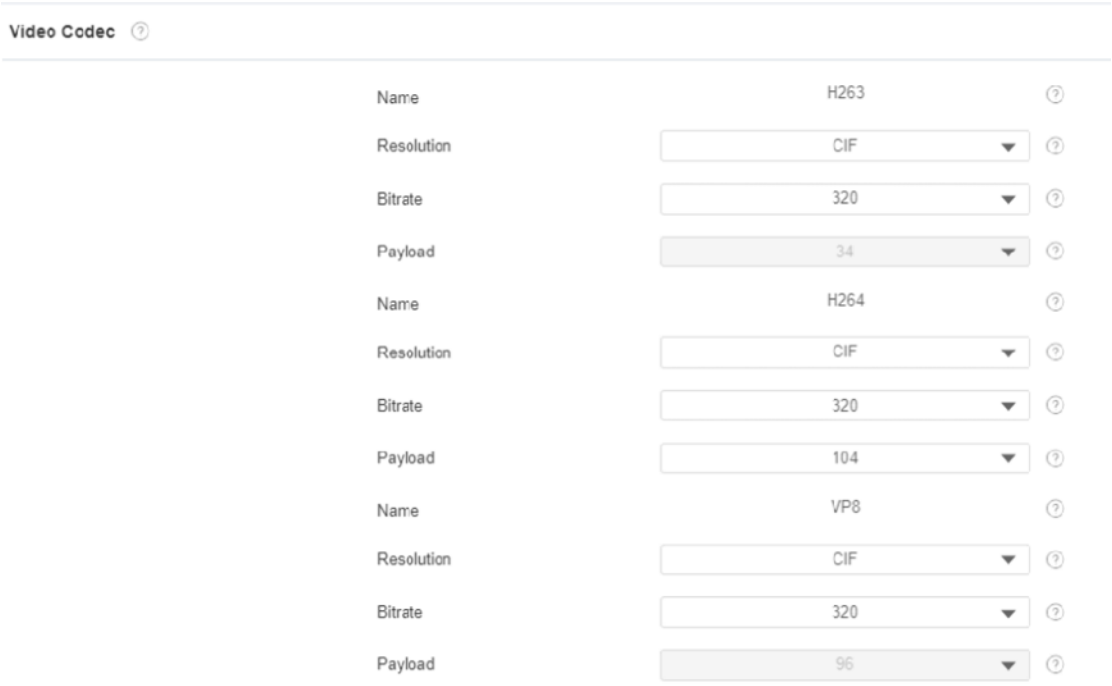
Please refer to the bandwidth consumption and sample rate for the four codec types below:

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

Codec Type	Bandwidth Consumption	Sample Rate
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

14.2. Video Codec Configuration

S567 series supports VP8, H263, H264, and 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 an available video codec and set up the codec parameters.



Parameter Set-up:

- **Name**: check to select the H264 video codec format for the door phone video stream. H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among four options: **QCIF, CIF, VGA, 4CIF, and 720P** according to your actual network environment. The default code resolution is 4CIF.
- **Bitrate:** select the video stream bit rate (ranging from 320-2048). The greater the bitrate, the data transmitted every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048.
- **Payload:** select the payload type (ranging from 90-118) to configure audio/video configuration file. The default payload is 104.

15. Security

15.1. Monitor and Image

15.1.1. Monitor Setting

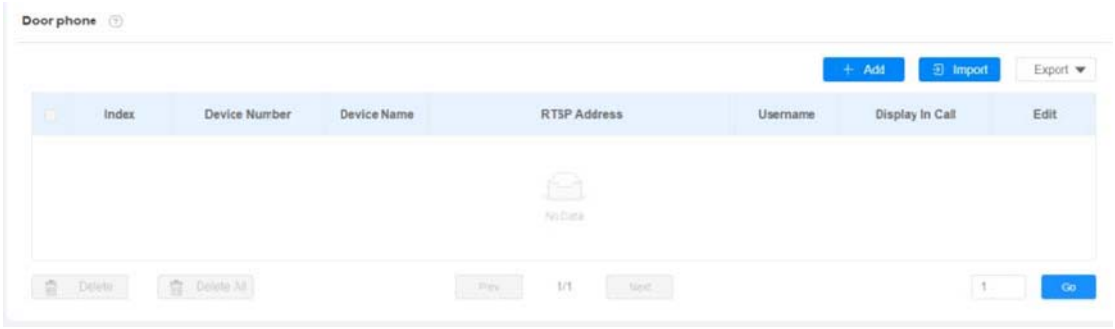
You can configure the monitor setting on the web **Device>Monitor** interface. Enter the IP/SIP number of the door phone in the device number and fill in the device name. Then set up the RTSP address. The RTSP format of the Akuvox door phone is rtsp://deviceIP/live/ch00_0. Enable or disable display in the call. If enabled, when there is an incoming call from the monitor, the video will be displayed.

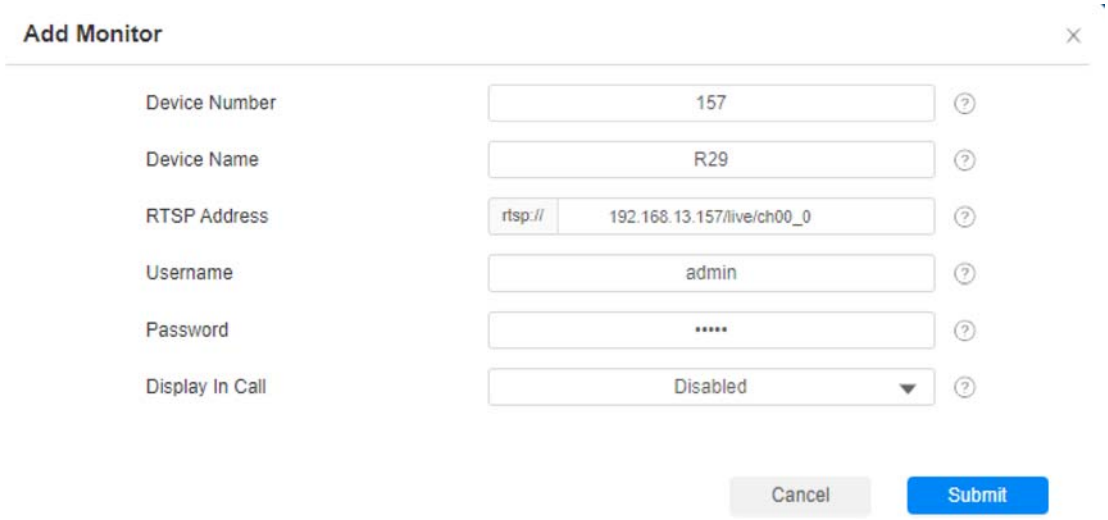
Parameter Set-up:

- **Monitor Display**: select **MultipleWindow** if you want to display four video monitoring channels on the screen. Select **Single** if you want to display only one video monitoring channel.

Note

- You can import and export the monitored device setting via a template in .xml format.

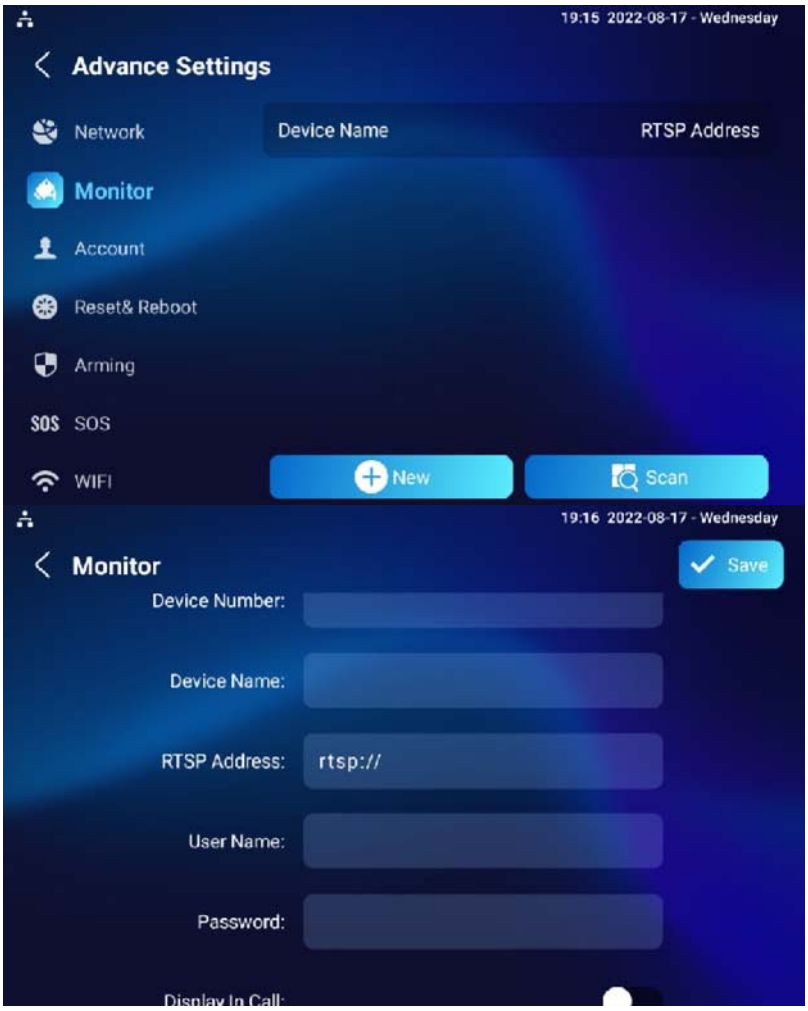




Parameter Set-up:

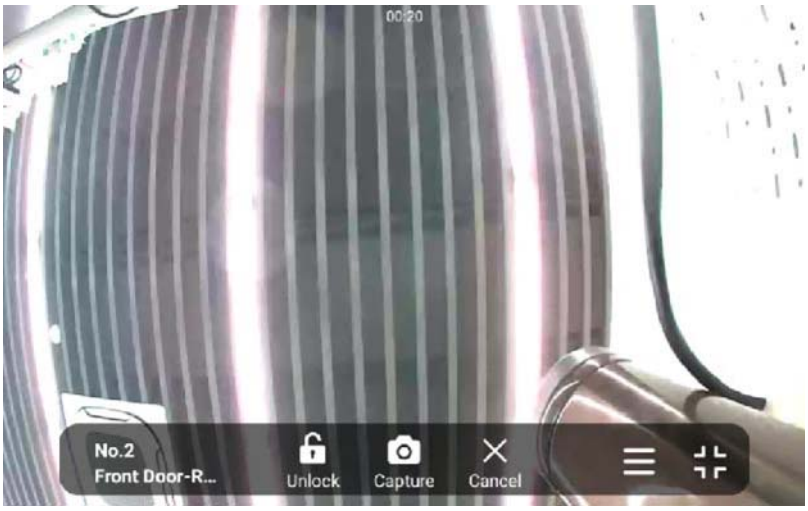
- **Device Number:** type in the monitored device number for identification
- **Device Name:** type in the device name for identification.
- **RTSP Address:** type in the RTSP address of the monitored device. RSTP format: **Device IP address/live/ch00_0**.
- **Username:** type in the username of the monitored device for monitoring authentication.
- **Password:** type in the password of the monitored device for the monitoring authentication.
- **Display In Call:** enable it if you want to display the monitoring video when you are in the call.

You can also set it up on the device:



15.1.2. Video Image Capturing

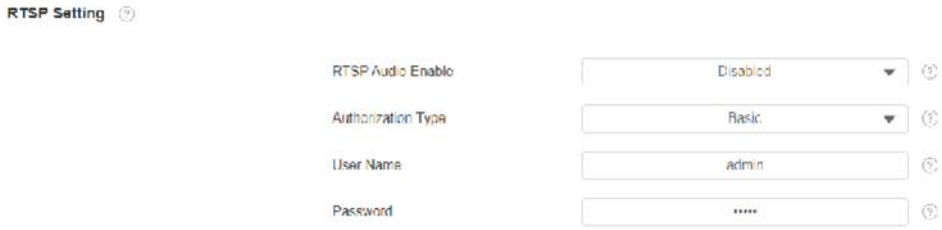
To capture video image by pressing **Monitor>Capture** on the device screen.



15.1.3. RTSP Authentication

You can set the RTSP authentication to allow the indoor monitor to be monitored via RTSP audio stream. For example, you can apply this feature in the baby's room where babies can be monitored on an audio basis for safety.

To set it up, go to **Setting > Basic > RTSP Setting**.



Parameter Set-up:

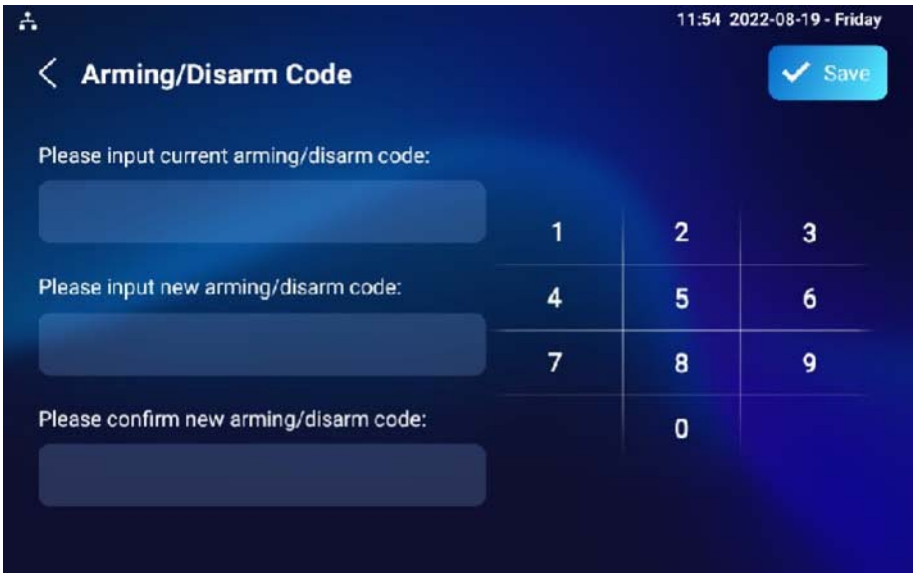
- **RTSP Audio Enable**: enable it if you want to monitor the device via RTSP audio stream.
- **Authorization Type**: select the authorization type (**Basic, Digest**). Select **None** if you allow all types of authorization types for the RTSP audio stream.
- **User Name**: type in the username used for the authentication.
- **Password**: type in the username used for the authentication.

15.2. Alarm and Arming Configuration

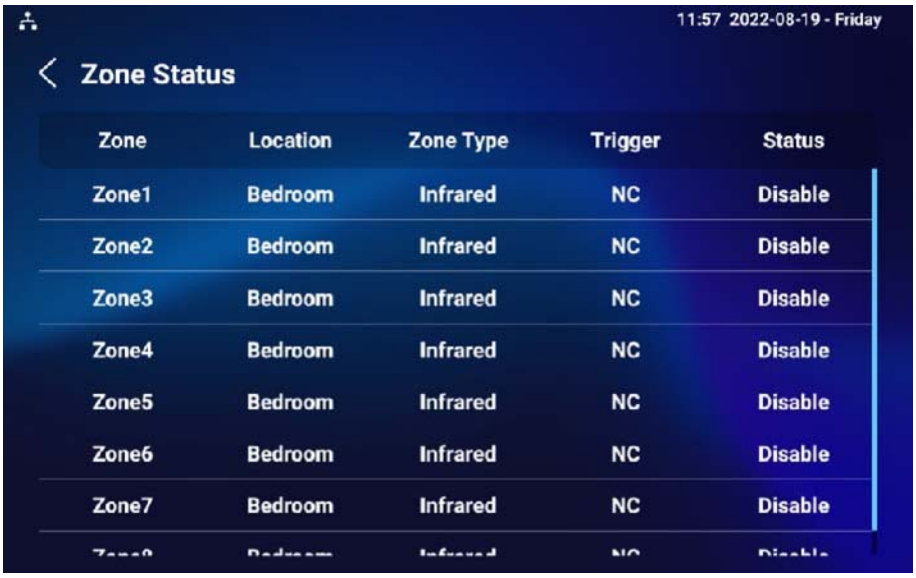
The alarm feature is used to connect some alarm detection devices to protect your home security. Akuvox indoor monitors support 8 alarm connectors which means you can connect 8 different alarm sensors in different rooms of your house. For example, by connecting a smoker sensor in your kitchen. If it detects a gas leak, the indoor monitor will ring up and send the alarm message to the target, like community property.

15.2.1. 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.

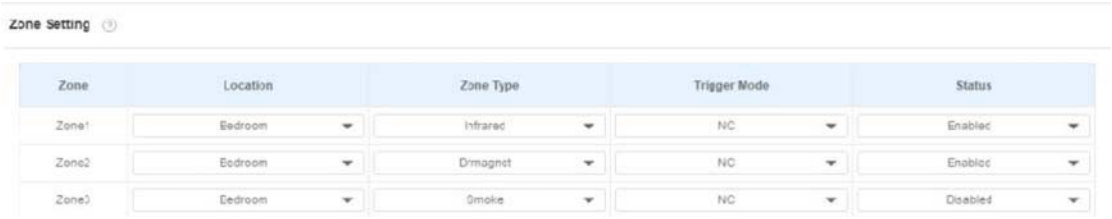


To check the zone status on **Arming > Zone Status** screen.



15.2.2. Configure Alarm and Arming on the Web Interface

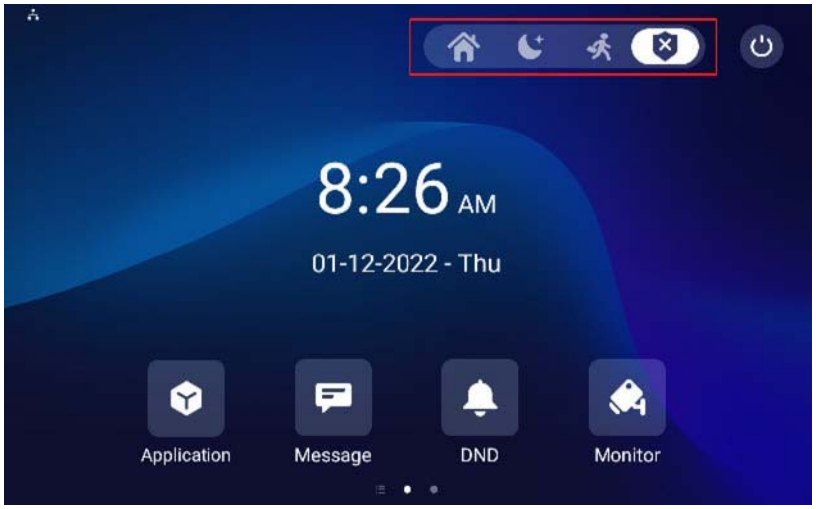
To set up a location-based alarm sensor on the device web **Arming> Zone Setting > Zone Setting** interface.



Parameter Set-up:

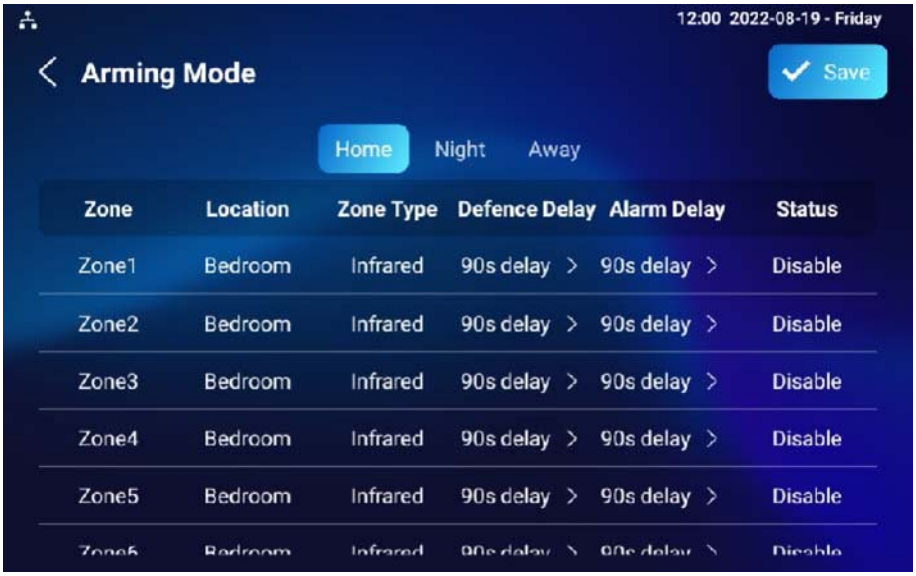
- **Location:** set up the location according to where the alarm sensor is installed. You can select among ten location types: **Bedroom**, **Gate**, **Door,Guest room**, **Hall**, **Window**, **Balcony**, **Kitchen**, **Study,** and **Bathroom**.
- **Zone Type:** set up the alarm sensor types. You can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

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



15.2.3. Configure Location-based Alarm

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



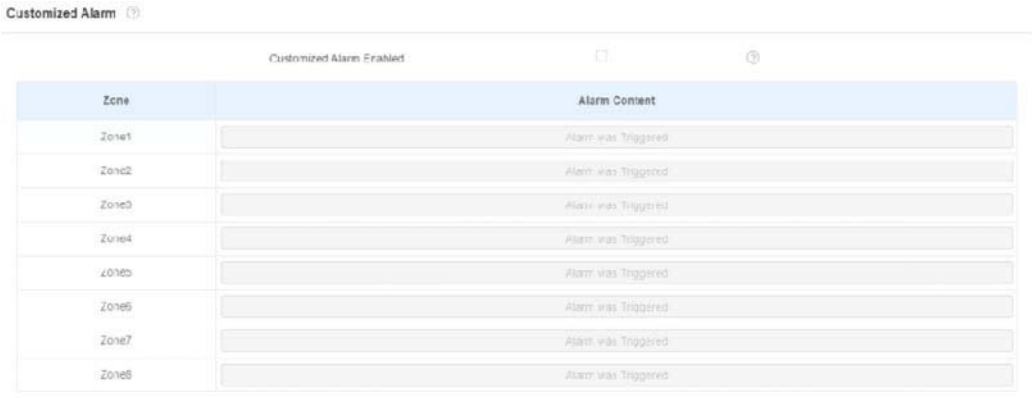
Parameters Set-up:

- **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, 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.

15.2.4. Configure Alarm Text

After the alarm sensor is set up, you are allowed to customize your alarm text shown on the screen when an alarm is triggered on web **Arming> Zone Setting > Zone Setting** interface. Enter the alarm text for the alarm at each

location according to your need.

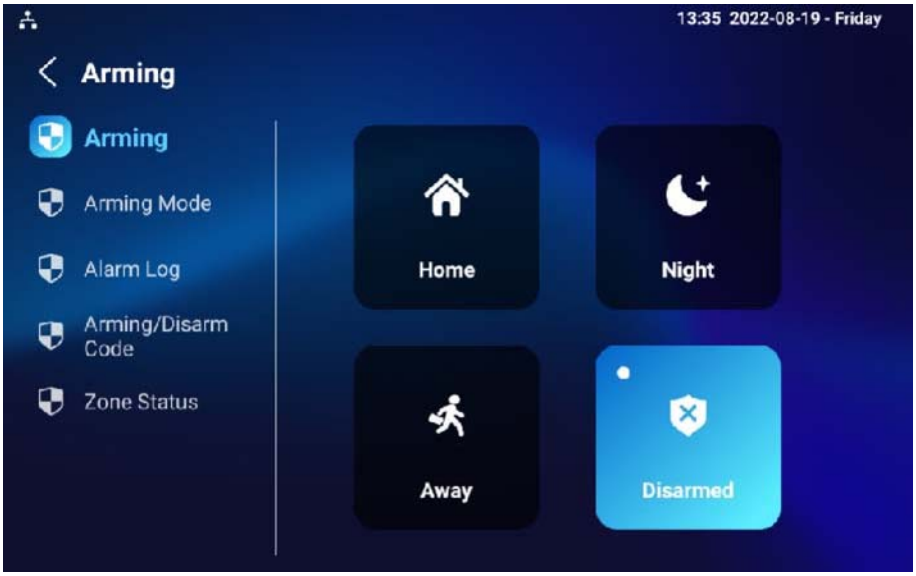


Parameter Set-up:

- **Customized Alarm Enable**: enable the feature before you can type in the customized alarm text.
- **Alarm Context**: type in the alarm text in the specific arming zone. The alarm text will be displayed when an arming is triggered.

15.2.5. Configure Arming Mode

To switch arming mode, disarm the alarm on **Arming** screen by pressing their respective icons. Press **Disarm** icon if you want to clear the Arming Mode.



15.2.6. Configure Alarm Ringtone

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

Note

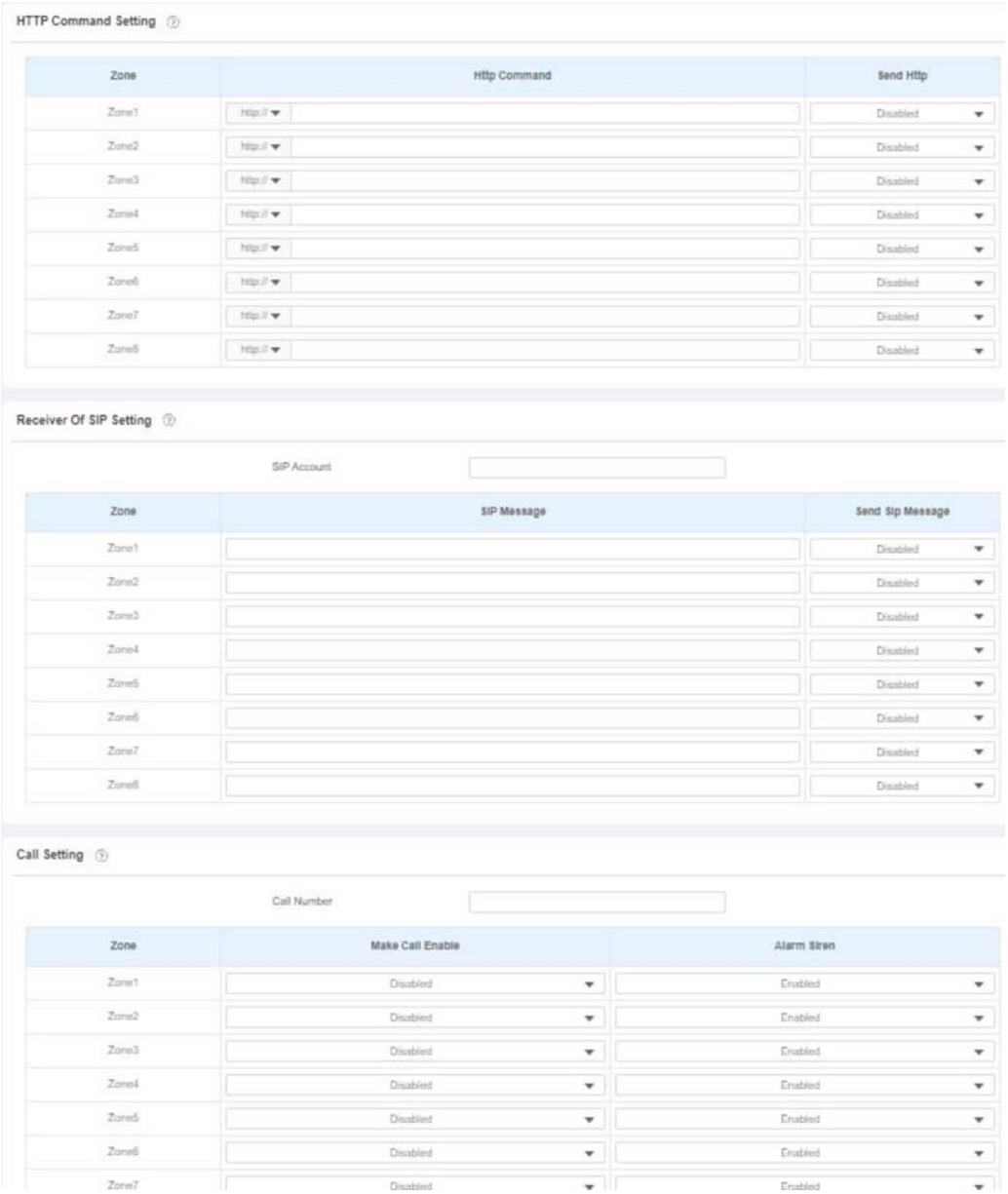
- The file format of customized ringtone should be .wav.

15.2.7. Alarm Action Configuration

The triggering of the alarm sensor can be accompanied by the actions you configured in the forms of HTTP command, SIP Message, Call, Local Relay for different security purposes.

15.2.7.1. Select Alarm Action Types

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



15.2.7.2. Configure Alarm Action via HTTP Command

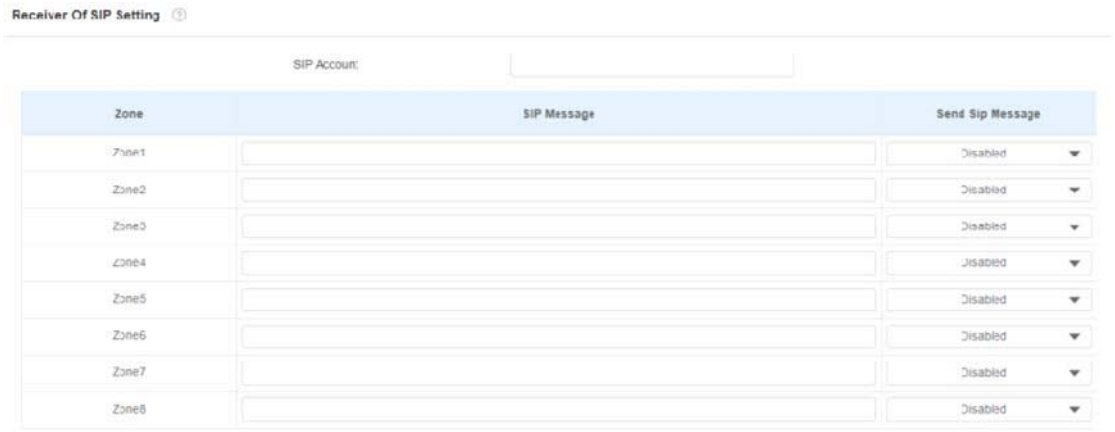
To set up the HTTP Command action, you can click **Enable** in the **Send HTTP** field to enable the actions for the alarm sensor installed in different locations. Then enter the HTTP command provided by the manufacturer of the device on which the action is to be carried.

Parameter Set-up:

- **Send HTTP:** enable it if you want the action to be implemented on a designated third-party device.
- **HTTP Command**: enter the HTTP command provided by third-party device manufacturer.

15.2.7.3. Configure Alarm Action via SIP Message

To set up the SIP message action receiver on the same web interface. Enter the SIP account to which you want to send the configured SIP message as an action when the alarm is triggered.



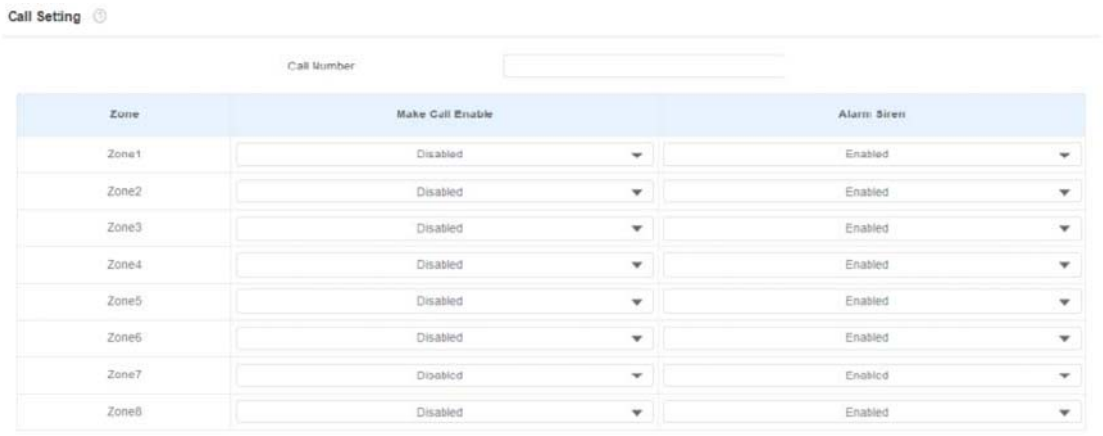
Parameter Set-up:

- **Send SIP Message**: enable it before you can send the customized messages to a designated SIP number or an IP number when the alarm is triggered.

- **SIP message**: type in the message you want to send to the designated SIP number or IP number when the alarm is triggered.

15.2.7.4. Configure Alarm Action via SIP Call

To set up the call action, you can enter the SIP or IP number of the device to be called as an action, then enable **Alarm Siren** for the arming zone as needed.

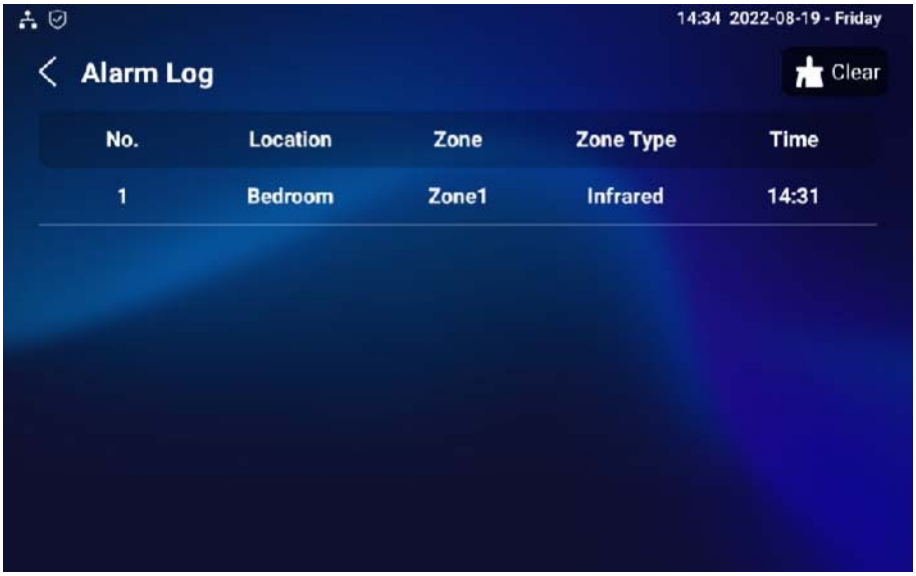


Parameter Set-up:

- **Call Number**: type in the SIP number or IP number to receive the calls when the alarm is triggered.
- **Make Call Enable**: enable it so that a call will go to the designated SIP or IP number when alarm is triggered.
- **Alarm Siren**: enable it if you want to trigger alarm siren on the indoor monitor when the alarm is triggered.

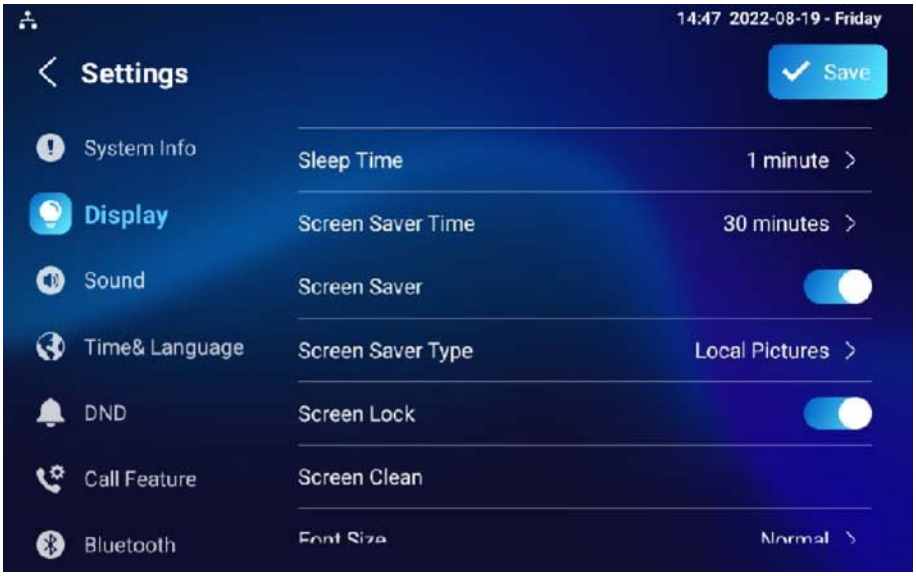
15.2.8. Check Alarm Log

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



15.3. Screen Unlock Setting

You can enable the screen lock function directly on the device **Settings > Display** screen. The device screen will be locked over sleep time. You are required to wake up the device through face recognition (Face ID) or password.



15.3.1. Screen Unlock by PIN code

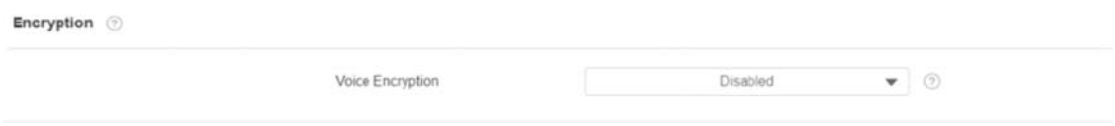
You can unlock the device screen by entering the preset PIN code when the screen is locked.

Note

- The default unlock PIN is 123456.

15.4. Voice Encryption

The encryption function provides you with greater security for the intercom call. The indoor monitor supports three modes of voice encryption: SRTP(Compulsory), SRTP(Optional), and ZRTP(Optional) on the web **Account > Advanced > Encryption** interface.



Parameter Set-up:

- **Voice Encryption:** select encryption mode from four options. If you select **Disable**, 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.

15.5. Remote Control

Remote control function supports configuring a specific server to send HTTP commands or request to the indoor monitor to do some specific action on the web **Device>Relay > Remote Control** interface.

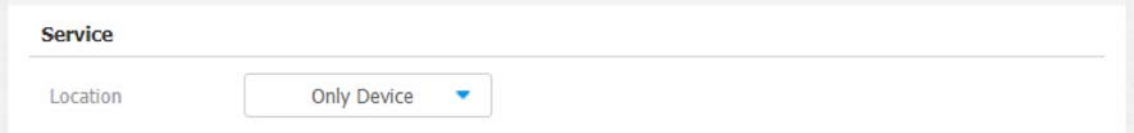
Parameter Set-up:

- **Allowed Access IP List**: set up the server IP address that can be allowed to send the HTTP commands to the indoor monitor.

15.6. Location

You can select the level of protection for the location of the indoor monitor. for example, you can disable the location feature so that no app is allowed to obtain your device location.

To set it up, go to **Security > Advanced > Service**.



Parameter Set-up:

- **Disabled**: select **Disabled** if you do not allow any app to find your device location.
- **Only Device**: the device location can be determined using GPS.
- **High Accuracy**: the device location can be determined via WAN, Bluetooth, or cellular networks.

16. Door Access Control Configuration

16.1. Relay Switch Setting

16.1.1. Local Relay Setting

Local relays in the indoor monitor can be used to trigger relay for the door access and trigger chime bell as needed in different scenarios. 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 two types of the relay, chime bell and open door. **Chime Bell**, when there is a call, the chime bell will ring. **Open door**, when press 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.

16.1.2. Remote Relay Switch Setting

You can use the unlock tab during the call to open the door on web **Phone > Relay > Relay Setting >Remote Relay** interface. You are required to set up the

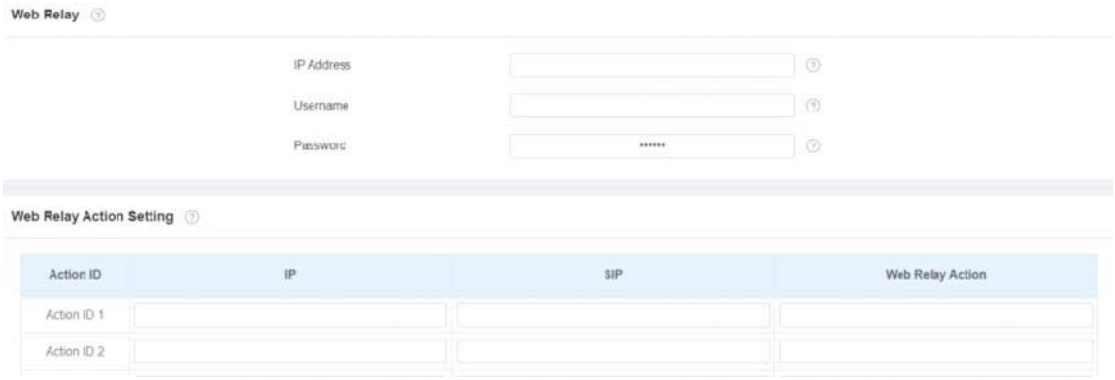
same DTMF code in the door phone and indoor monitor.

Parameter Set-up:

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

16.2. Web Relay Setting

In addition to the relay that is connected to the indoor monitor, you can also control the door access using the network-based web relay. 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.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **IP/SIP:** enter 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, while this setting is optional. And please refer to the example below: http://admin:admin@192.168.1.2/state.xml?relayState=2.

16.3. Door Unlock Configuration

16.3.1. Door Unlock by DTMF Code

DTMF codes can be configured on the web **Account > Advanced > DTMF** interface where you can set up identical DTMF code on the corresponding intercom devices, which allows residents to enter the DTMF code on the soft keypad or press DTMF code attached unlock tab on the screen to unlock the door for visitors etc., during a call.

Parameter Set-up:

- **Type**: select DTMF type among four options: **Inband**, **RFC2833**, **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.

16.3.2. Door Unlock via HTTP Command

You can unlock the door remotely without approaching the device physically for the door access by typing in the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. To do this configuration on web **Intercom > 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
- **Remote Open Relay Via HTTP Allowlist**: enable it and type in, for example, the IP address of the server that you allows to send the HTTP command to the indoor monitor to trigger the local relay.

Note

- DoorNum in the HTTP command above refers to the relay number #1 to be triggered.

16.4. Relay Switch Setting

16.4.1. Local Relay Setting

Local relays in the indoor monitor can be used to trigger relay for the door access and trigger chime bell as needed in different scenarios. 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 two types of the relay, chime bell and open door. **Chime Bell**, when there is a call, the chime bell will ring. **Open door**, when press 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.

16.4.2. Remote Relay Switch Setting

You can use the unlock tab during the call to open the door on web **Phone > Relay > Relay Setting >Remote Relay** interface. You are required to set up the same DTMF code in the door phone and indoor monitor.

Parameter Set-up:

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

16.5. Web Relay Setting

In addition to the relay that is connected to the indoor monitor, you can also control the door access using the network-based web relay. 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.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **IP/SIP:** enter 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, while this setting is optional. And please refer to the example below: http://admin:admin@192.168.1.2/state.xml?relayState=2.

16.6. Door Unlock Configuration

16.6.1. Door Unlock by DTMF Code

DTMF codes can be configured on the web **Account > Advanced > DTMF** interface where you can set up identical DTMF code on the corresponding intercom devices, which allows residents to enter the DTMF code on the soft keypad or press DTMF code attached unlock tab on the screen to unlock the door for visitors etc., during a call.

Parameter Set-up:

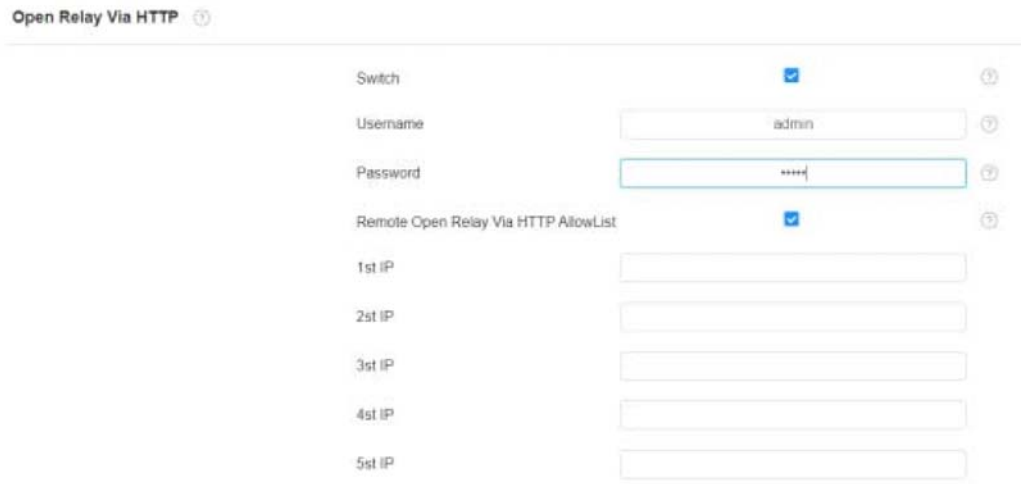
- **Type**: select DTMF type among four options: **Inband**, **RFC2833**, **Info+Inband** and **Info+RFC2833** according to your need.
- **DTMF Code Transport Format**: select it only when the third-party device that receives the DTMF code adopts **Info** transport format. **Info** transfer the DTMF 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.

16.6.2. Door Unlock via HTTP Command

You can unlock the door remotely without approaching the device physically for the door access by typing in the created the HTTP command (URL) on the web browser to trigger the relay when you are not available by the door for the door access. To do this configuration on web **Intercom > 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
- **Remote Open Relay Via HTTP Allowlist**: enable it and type in, for example, the IP address of the server that you allows to send the HTTP command to the indoor monitor to trigger the local relay.

Note

- DoorNum in the HTTP command above refers to the relay number #1 to be triggered.

17. Lift Control

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

17.1. Configure Lift Control

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

Parameter Set-up:

- **Status:** 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.

17.2. Configure Lift Control Prompt

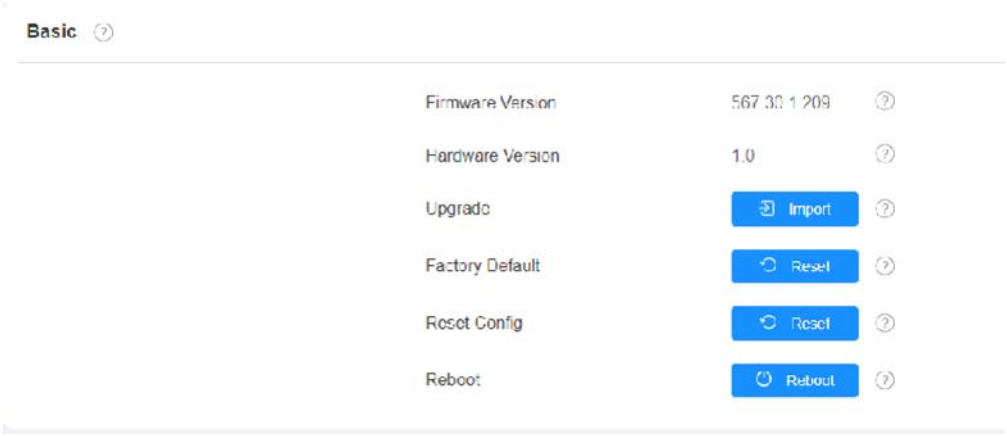
When the lift controller receives the HTTP command, it will give feedback on the current lift status with a prompt. To do this configuration on the web **Device > Lift> Hints** interface. Edit the **HTTP Status Code**, and feedback code

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.

18. Firmware Upgrade

Firmware of different versions for the indoor monitors can be upgraded on the device web **Upgrade > Basic** interface.



Note

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

19. Backup

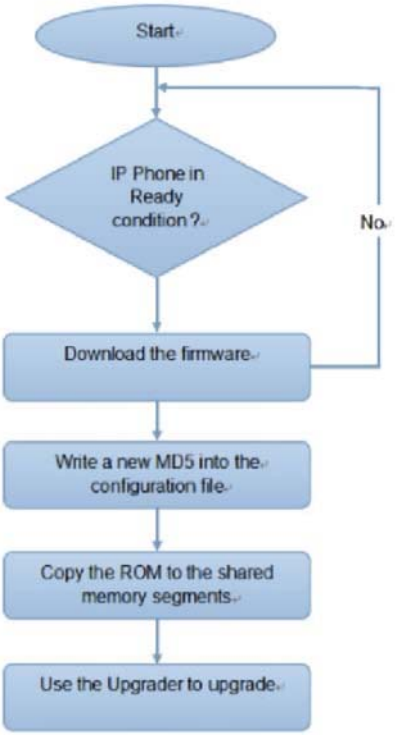
Configuration files can be imported to or exported out of the device to your local PC on the device web **Upgrade > Advanced > Others** interface if needed.

20. Auto-provisioning via Configuration File

20.1. Provisioning Principle

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

Please see the flow chart below:



20.2. 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 other one is the MAC-based configuration provisioning.

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

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

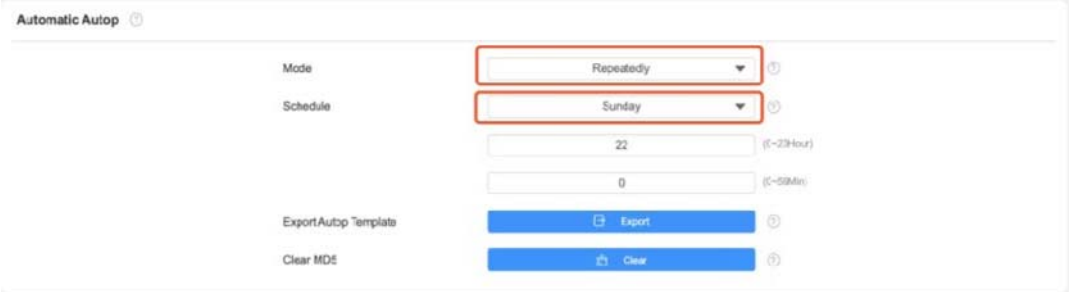
Note

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

20.3. Autop

Akuvox provides you with different Autop methods that enable the indoor monitor to perform provisioning for itself in a specific time according to your schedule. To set up the schedule on device web **Upgrade > Advanced > Automatic Autop** interface.

Please see the picture below:

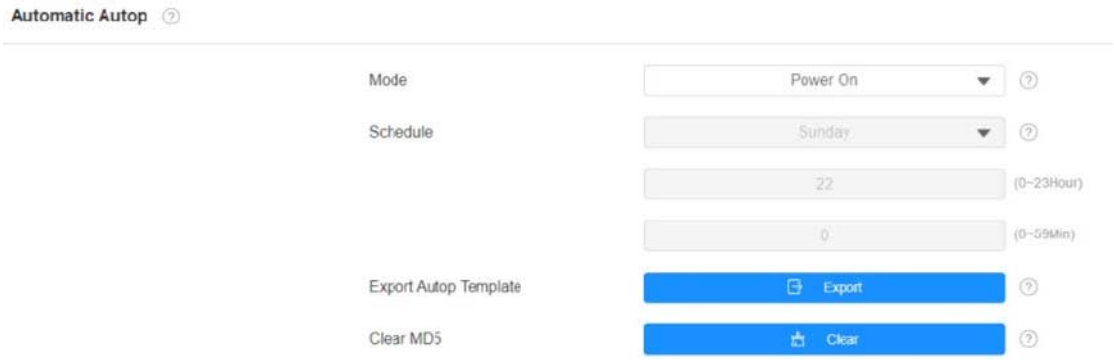


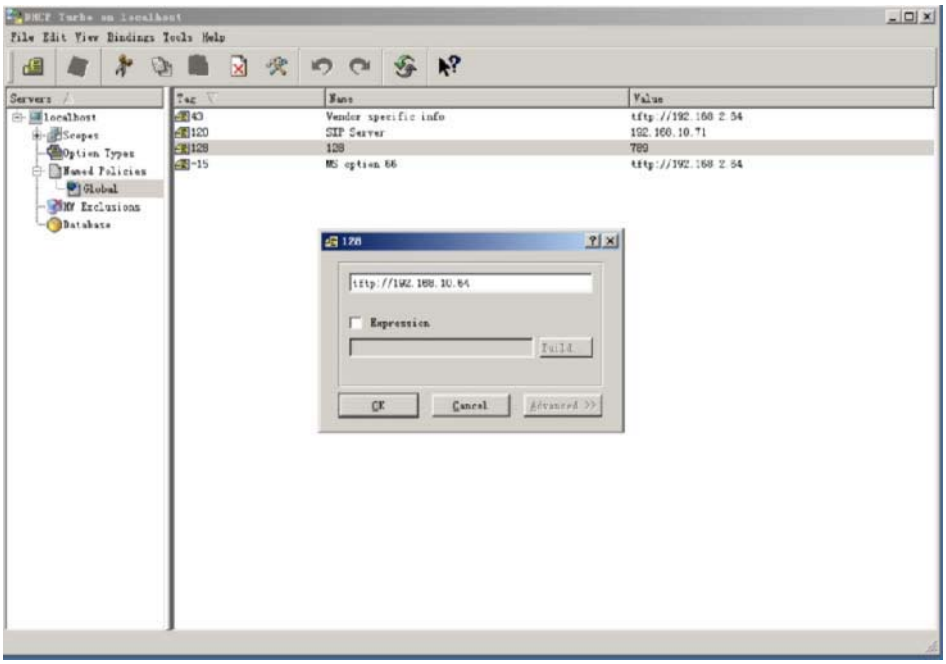
Parameter Set-up:

- **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.

20.4. DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using DHCP option which allows 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 code (range from 128-255), you are required to configure DHCP Custom Option on the web **Upgrade > Advanced > Automatic Autop** interface.





Note

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

ParameterSet-up:

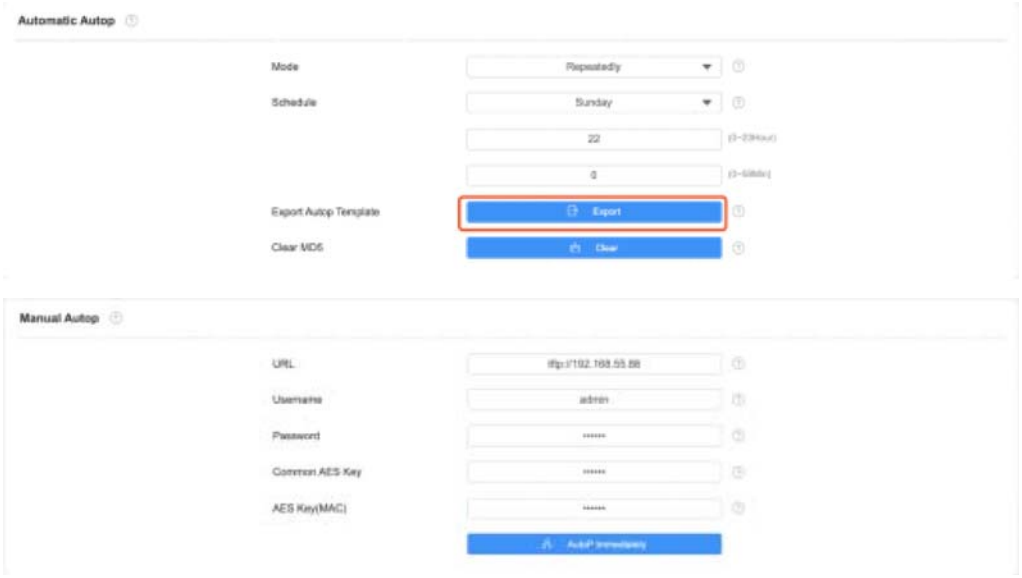
- **Custom Option**: enter the DHCP code that matched with corresponding URL so that device will find the configuration file server for the configuration or upgrading.
- **DHCP Option 66:** if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. 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.**

20.5. Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file on device web **Upgrade > Advanced > Automatic Autop** interface. If an autop schedule is set up, the indoor monitor will perform the auto provisioning on a specific timing according to autop 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.



Parameter Set-up:

- **URL**: set up TFTP, HTTP, HTTPS, FTP server address for the provisioning.
- **User Name**: set up a user name if the server needs an user name to be accessed to otherwise leave it blank.
- **Password**: set up a password if the server needs a password to be accessed to otherwise leave it blank.
- **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 is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

Note

Server Address Format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/(allows anonymous login)

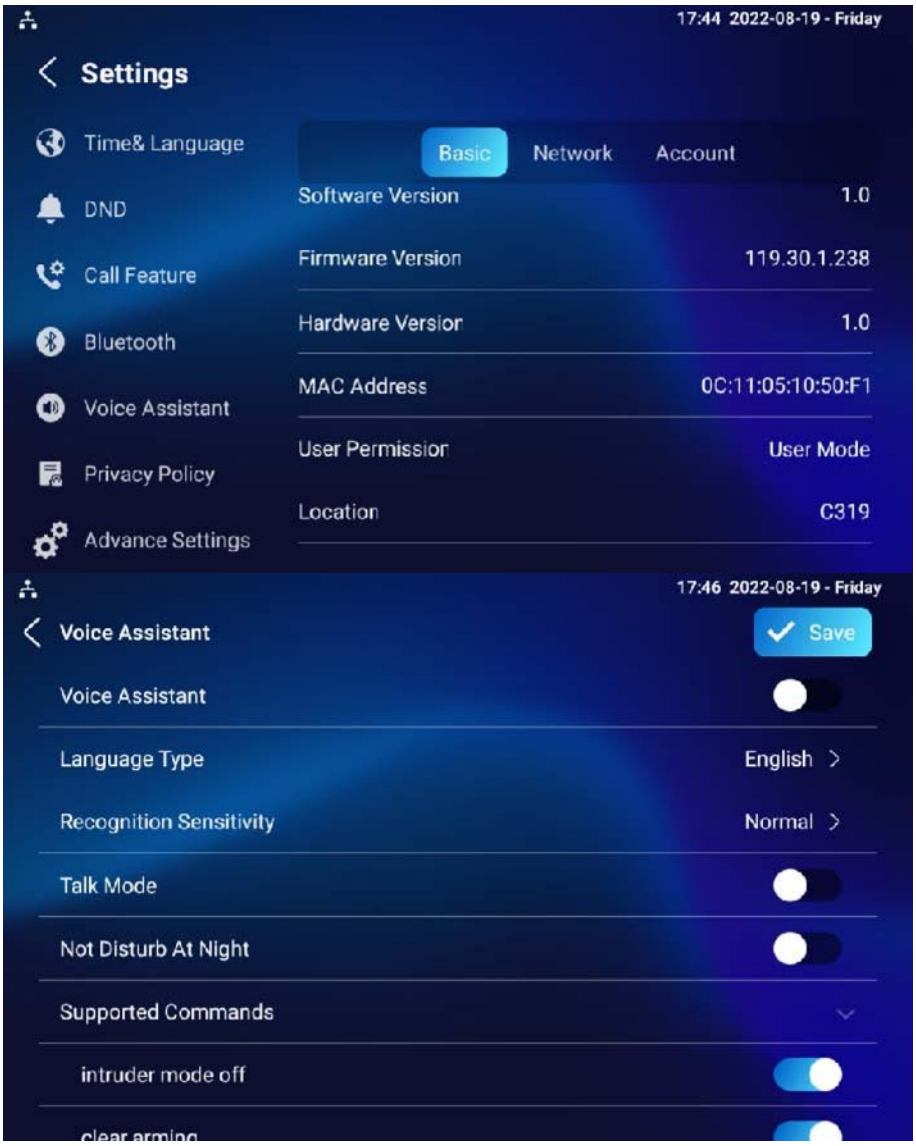
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/(use the default port 80)
- http://192.168.0.19:8080/(use other ports, such as 8080)
- HTTPS: https://192.168.0.19/(use the default port 443)

Note

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

21. Voice Assistant

You can configure voice assistant named **Albert** to perform a variety of functions related to intercom calls, open-door, arming modes, etc. on the device. And you can also set up the specific relay to be triggered by the voice assistant for the door access control. 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

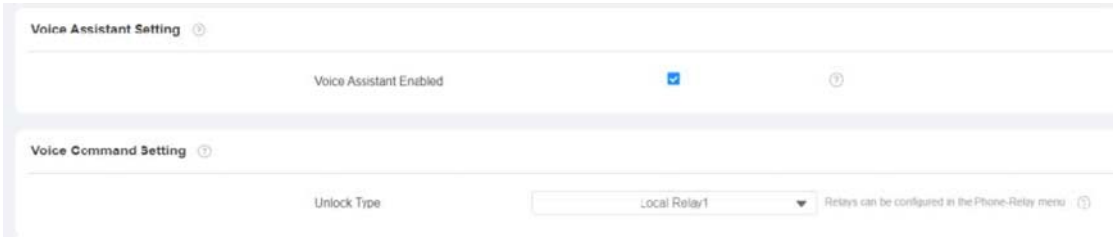
NO	Voice Command	Description	Voice Prompt
			mode is opened, have a nice dream ● Made it, good night ● Started it, sweet dreams!
5	Away mode	Use it when you want to change the arming mode to away mode.	● Sure, away mode is on ● OK, start away mode ● Alright, away mode is opened ● Made it ● Made it, have 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

NO	Voice Command	Description	Voice Prompt
			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 an 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	● Please choose

NO	Voice Command	Description	Voice Prompt
		up in the phonebook.	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 messages.	● Got it, please check ● OK, message is opened, you can write some content 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 the 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 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	Use it when you want to turn off the voice assistant	● See you

NO	Voice Command	Description	Voice Prompt
	down/cancel	function.	● See you later ● Bye ● Good bye ● See you next time ● Bye, best regards ● See you, have a great time
22	Answer Call Permission	Enable it so that you can answer or reject the incoming call via voice assistant by replying **Yes** or **No**.	● The call is coming, do you want to accept it? Yes or No? ● OK, here for you. ● Sure, hung up now.
23	Call Fuzzy Match	Enable it to allow the fuzzy match of the manager calls. For example, if you have multiple manager call contacts: manager1, and manager2, then you will be required to select the specific manager call contact when using **Call manager** voice command.	

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 elect a specific relay to be triggered via voice assistant.

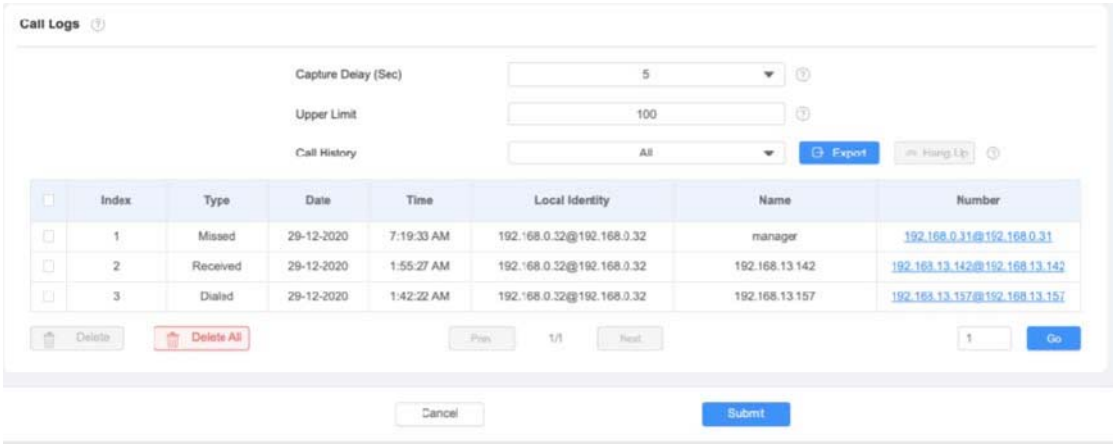


Parameter Set-up:

- **Unlock type:** select the type of relay to be triggered by the voice assistant for the predefined action, for example, door opening.

22. Call Log

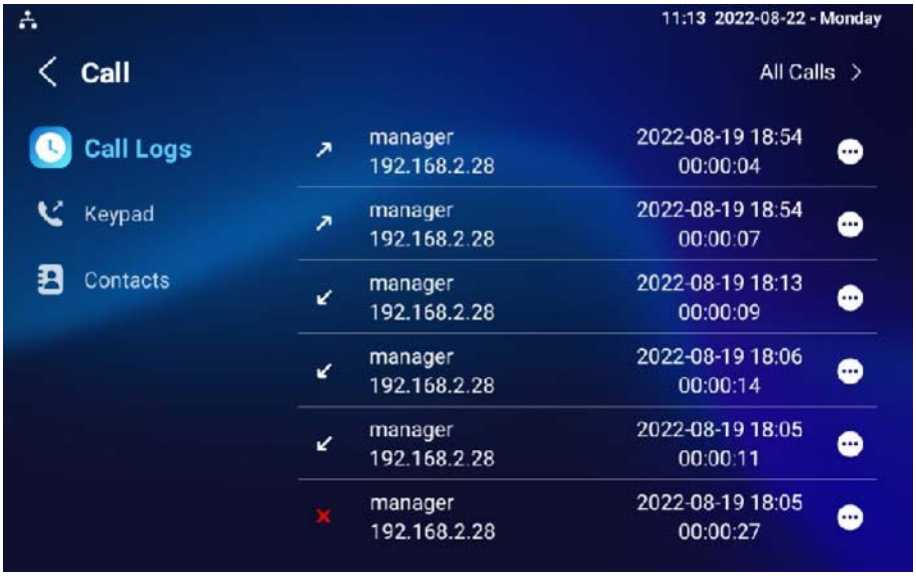
If you want to check on the calls inclusive of the dial-out calls, received calls, and missed calls in a certain period of time, you can check and search the call log on the device web **Contacts > Call Logs** interface and export the call log from the device if needed.



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 (All, Dialed, Received, Missed, Forwarded).
- **Local Identity**: displays the door phone's SIP account or IP number that receives that incoming calls.
- **Name/Number**: select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

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

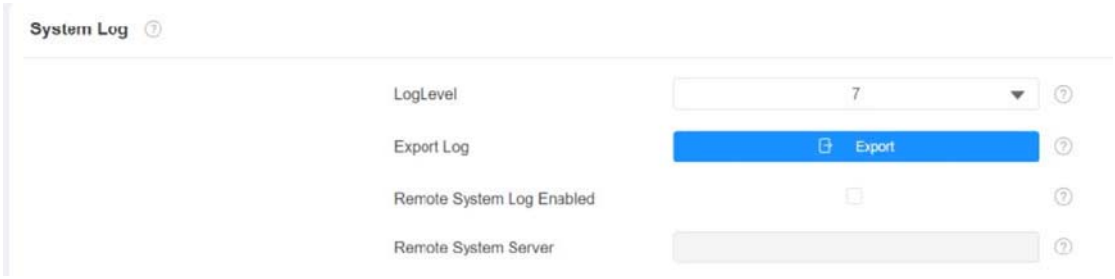

11:13 2022-08-22 - Monday
Call
All Calls
Call Logs
Keypad
Contacts
manager
192.168.2.28
2022-08-19 18:54
00:00:04
manager
192.168.2.28
2022-08-19 18:54
00:00:07
manager
192.168.2.28
2022-08-19 18:13
00:00:09
manager
192.168.2.28
2022-08-19 18:06
00:00:14
manager
192.168.2.28
2022-08-19 18:05
00:00:11
manager
192.168.2.28
2022-08-19 18:05
00:00:27

23. Debug

23.1. System Log for Debugging

23.1.1. Capturing a System Log for Debugging

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



Parameter Set-up:

- **LogLevel**: select log levels from 1 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.

23.2. PCAP for Debugging

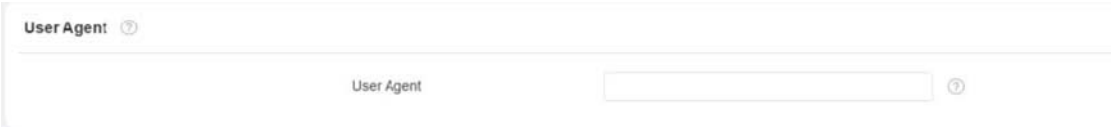
PCAP in Akuvox indoor monitor is used to capture the data package going in and out of the devices for debugging and troubleshooting purpose. You can set up the PCAP on the device web **Upgrade > Diagnosis > PCAP** interface properly before using it.

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.

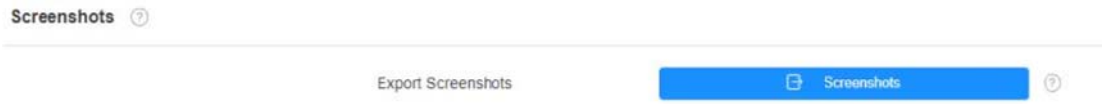
23.3. User Agent

User agent is used for the identification purpose when you are doing analysis on the SIP data packet. To do this configuration on web **Account > Advanced** interface.



23.4. Screenshots

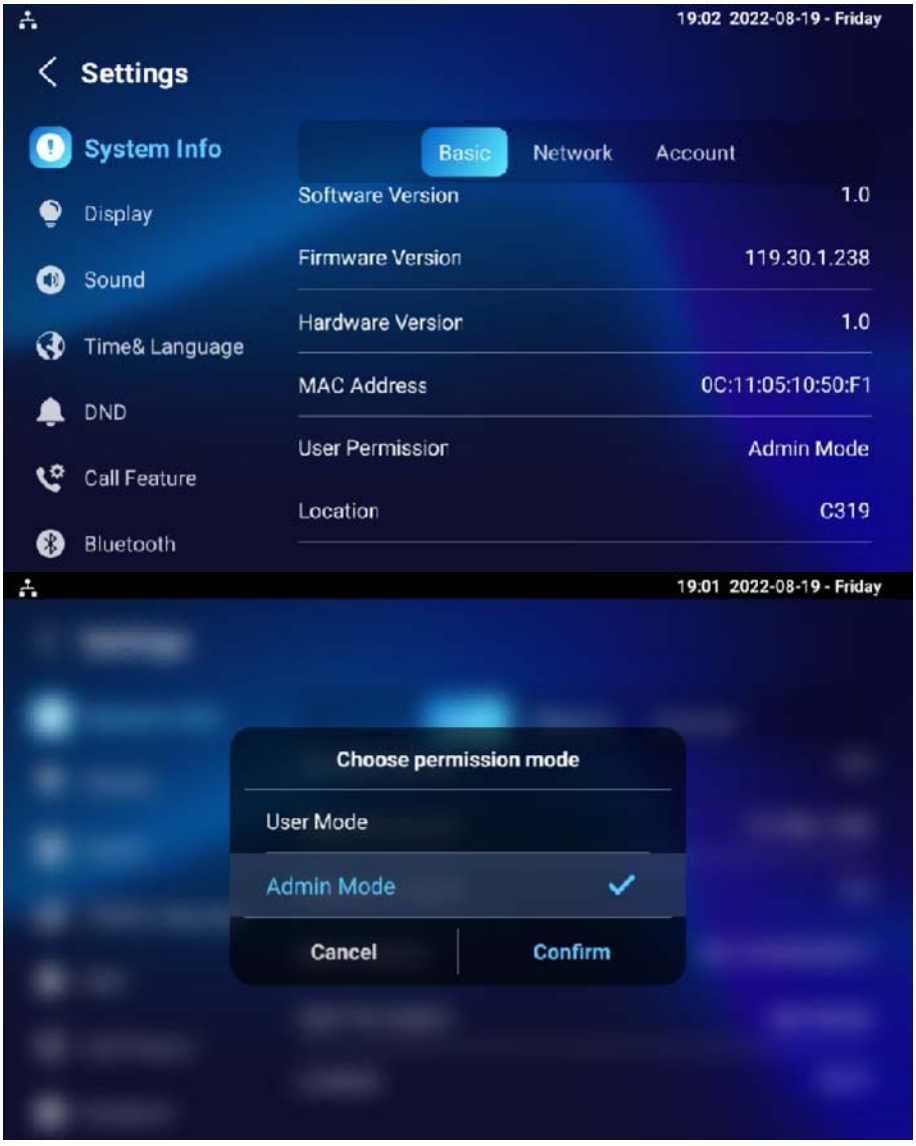
You can take the screenshot of the specific device screen to help with the troubleshooting and so on if needed. To take screenshots, go to **Upgrade > Diagnosis > Screenshots**, then click **Screenshots**.



24. Device Integration with Third Party

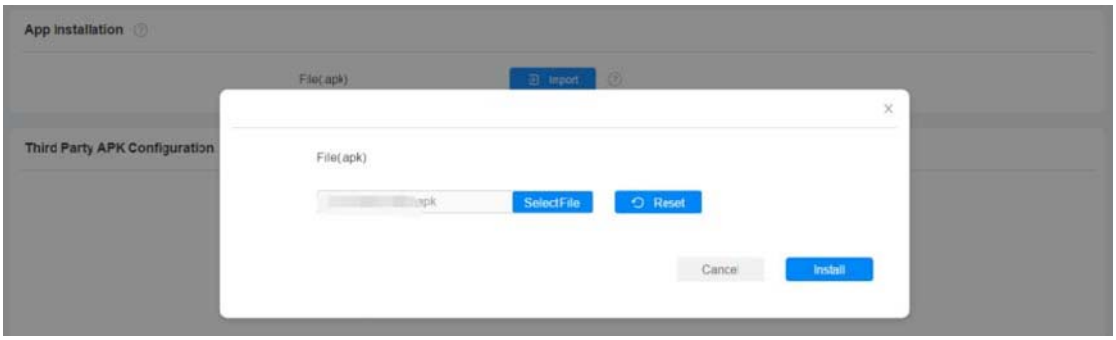
24.1. Enter Applications Screen

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** for confirmation.

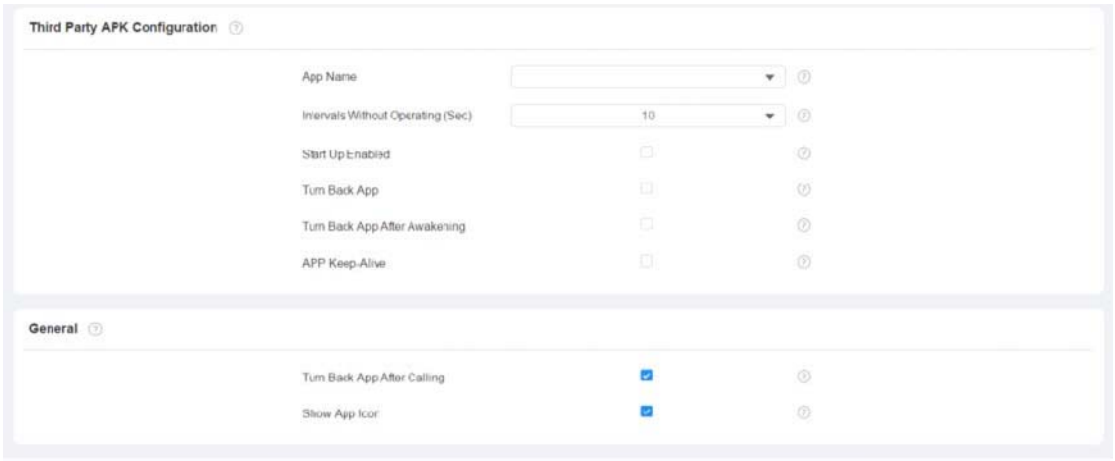


24.2. Install Third-party App

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 the 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:

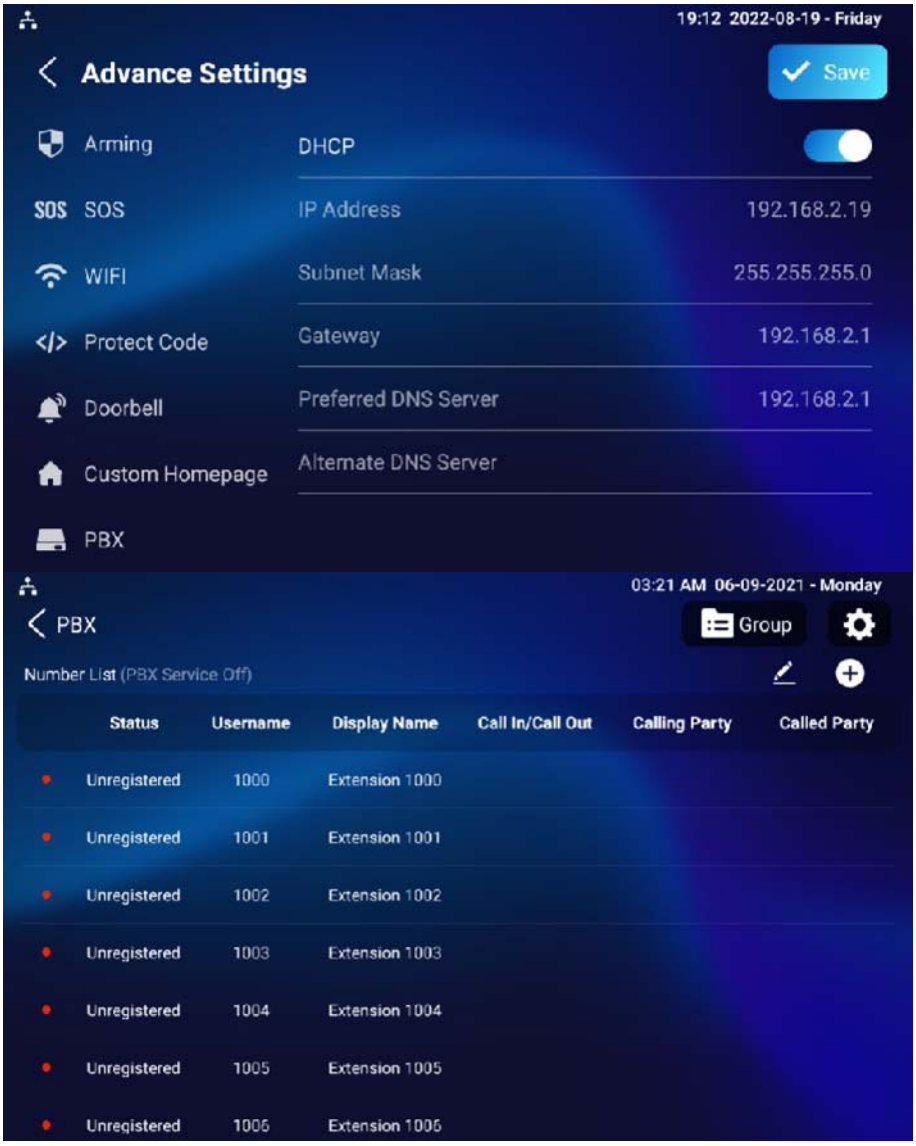
- **App Name**: select the App Name to be configured.
- **Interval Without Operating (Sec)**: tick the check box to set the app returning time-interval when there is no operation on the device.

- **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 of if you want the device to return to the app when the screen is awakened.
- **APP Keep-Alive:** tick the check box of 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.

25. PBX Feature

S567 Android indoor monitor has a built-in PBX server which allows the indoor monitor to serve as an intercom monitor and a SIP PBX, so users do not bother to prepare an extra SIP PBX again. The PBX supports call, forward, transfer, conference, ring group features, and so on. You can set it up on the device screen or web interface.

To set it up on the device, go to **Advanced Settings.**



25.1. PBX Configuration on The Device

Enable the PBX feature on the device **Advance Settings > PBX** screen to check and manage SIP accounts.

25.1.1. Enable PBX Service

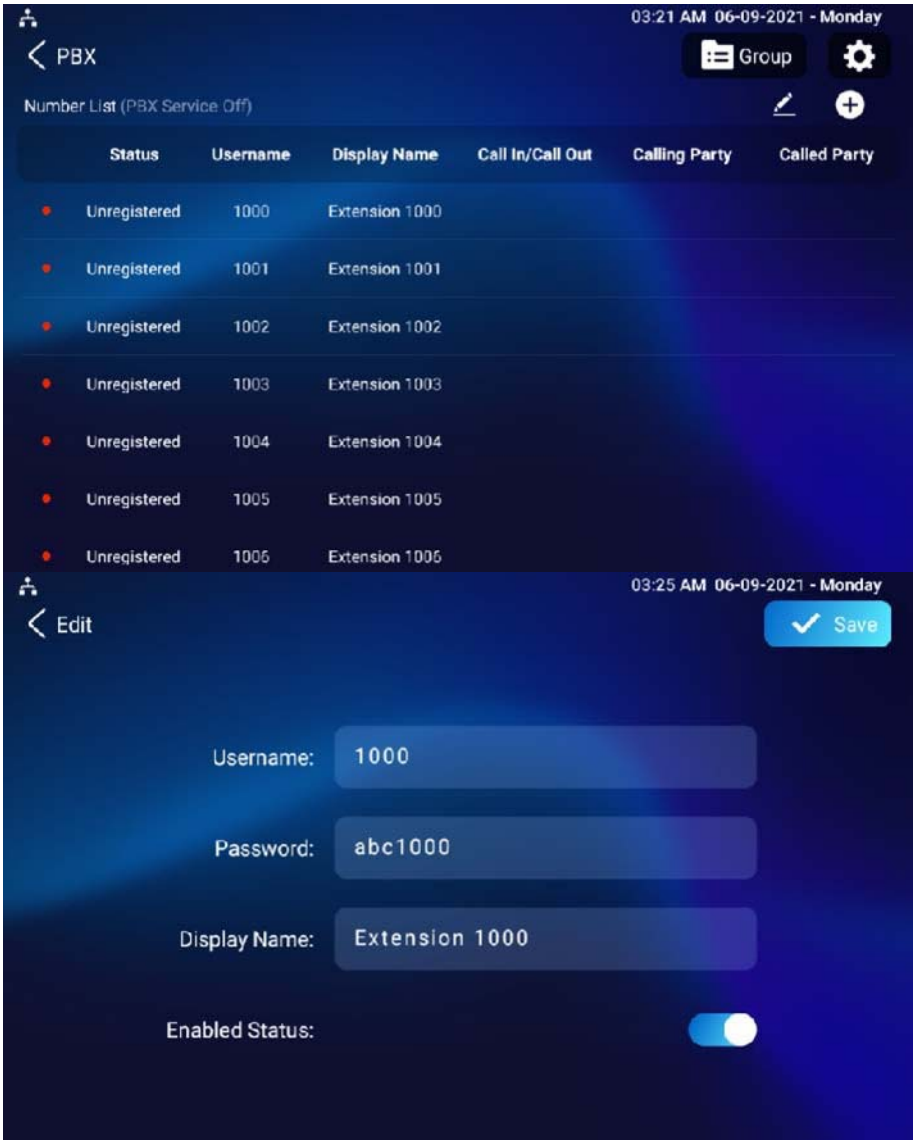
In the PBX interface,tap on the upper right corner to enable the PBX.

Parameter Set-up:

- **Media mode** : select **Default** if the intercom devices are deployed in the same LAN network. Select **Bypass** if the devices are deployed in the different LAN networks where PBX serves as a bridge or a media for the network data transmission.

25.1.2. Manage PBX Accounts

You can check the basic PBX information like PBX server and port and accounts status.



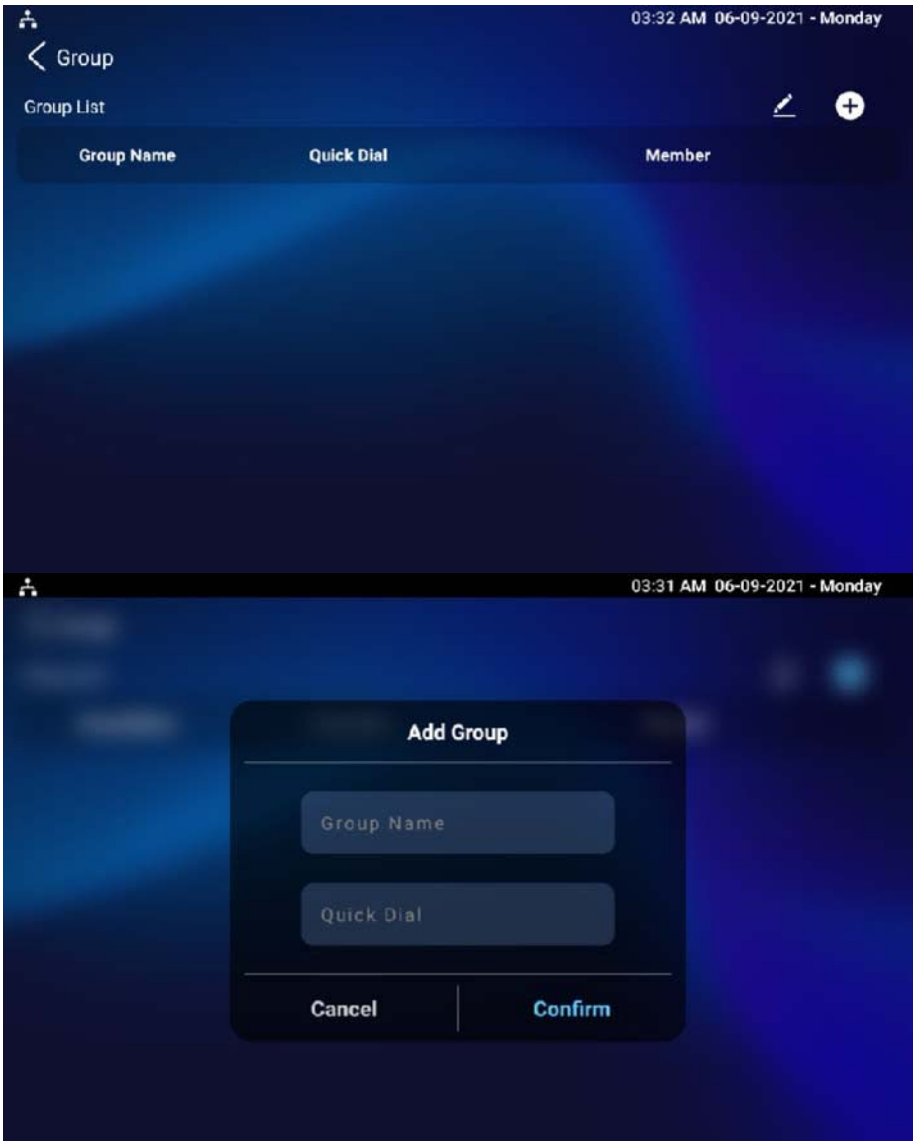
Parameter Set-up:

- **Status:** to show whether the account is registered or not.
- **Username:** to enter the extension number registered onto SIP server.
- **Display Name:** enter the display name of this account, which will be shown on other devices when making calls.
- **Password:** to enter the password of the corresponding users.
- **Enabled Status:** to activate SIP account.
- **Call IN/Call Out:** the calling status of this account.
- **Calling Party:** the calling party number.

- **Caller Party:** the caller party number.

25.1.3. Manage PBX Groups

Click **Group** on the right top corner to add a new ring group or edit the existing group. One number can be added in different ring groups. Once receiving an incoming call, the numbers in one group will be ring up at the same time.

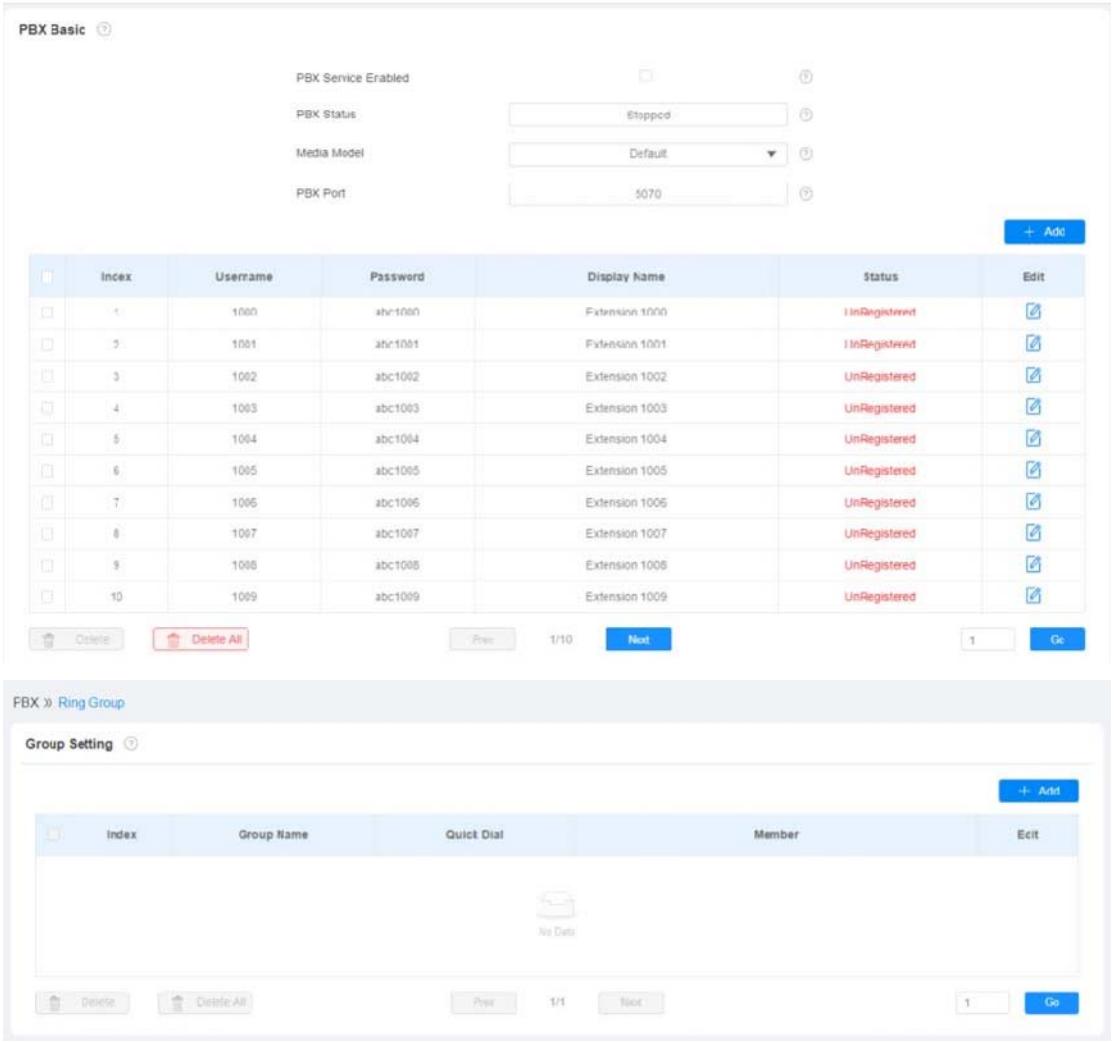


Parameter Set-up:

- **Group Name:** the name of a ring group.
- **Quick Dial:** a number of this ring group.

25.2. PBX Configuration on the Web Interface

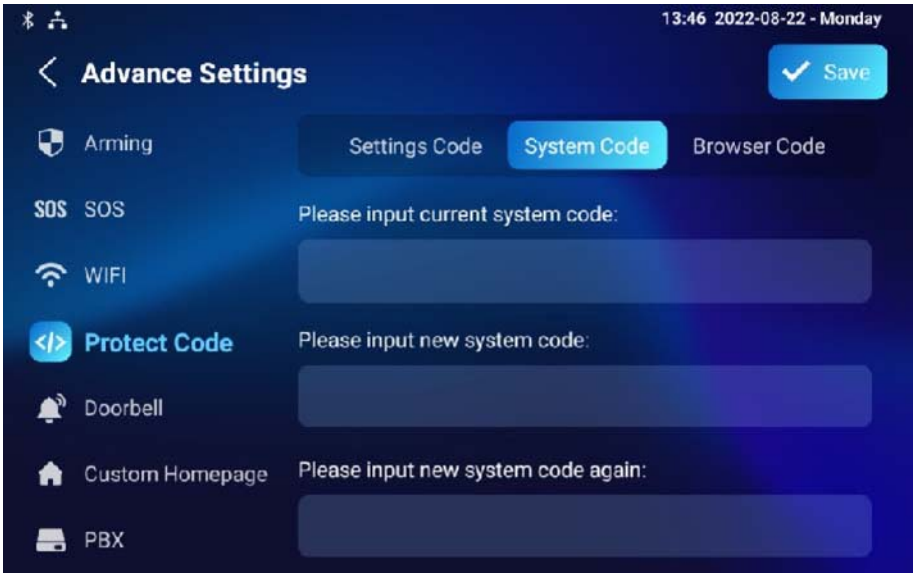
You can do the same configuration on web **PBX > Basic** and **PBX > Ring Group** interface.



26. Password Modification

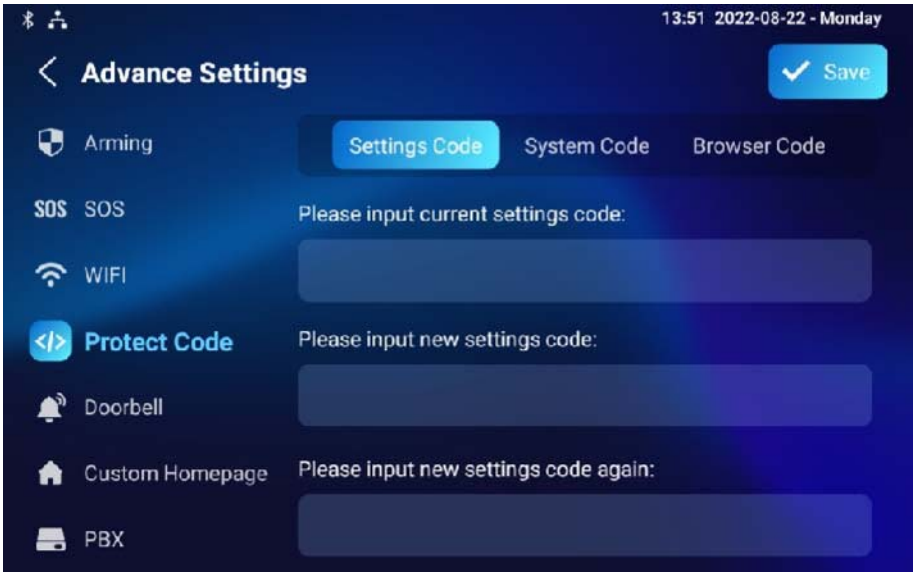
26.1. Modify Device Basic Setting Password

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.



26.2. Modify Device Advanced Setting Password

This password is used to enter the advanced settings of the device, including password settings, account numbers, SOS numbers, network settings, etc. To modify the advanced setting password on device **Settings > Advanced Settings > Protect Code > Setting Code** screen. The default password is 123456.



26.3. Modify Device Web Interface Password

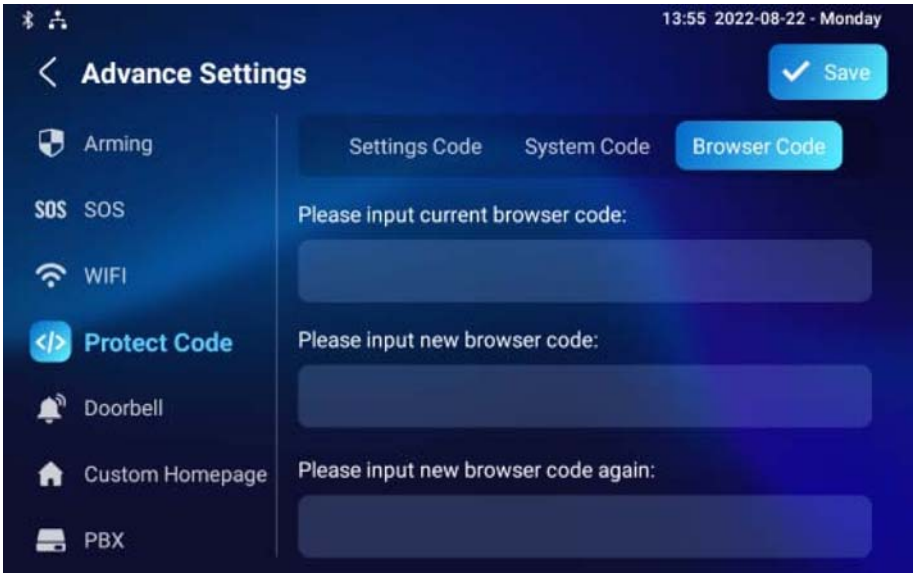
To modify the web interface password, you can do it on the device web **Security>Basic>Web Password Modify interface.** Select **Admin** for the administrator account and **User** for the User Account. Click the **Change Password** tab to change the password.

Note

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

26.4. 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 device **Settings > Advanced Settings > Protected Code > Browser Code** screen. The default password is 123456.


13:55 2022-08-22 - Monday
Advance Settings
Save
Arming
SOS
WIFI
Protect Code
Doorbell
Custom Homepage
PBX
Settings Code
System Code
Browser Code
Please input current browser code:
Please input new browser code:
Please input new browser code again:

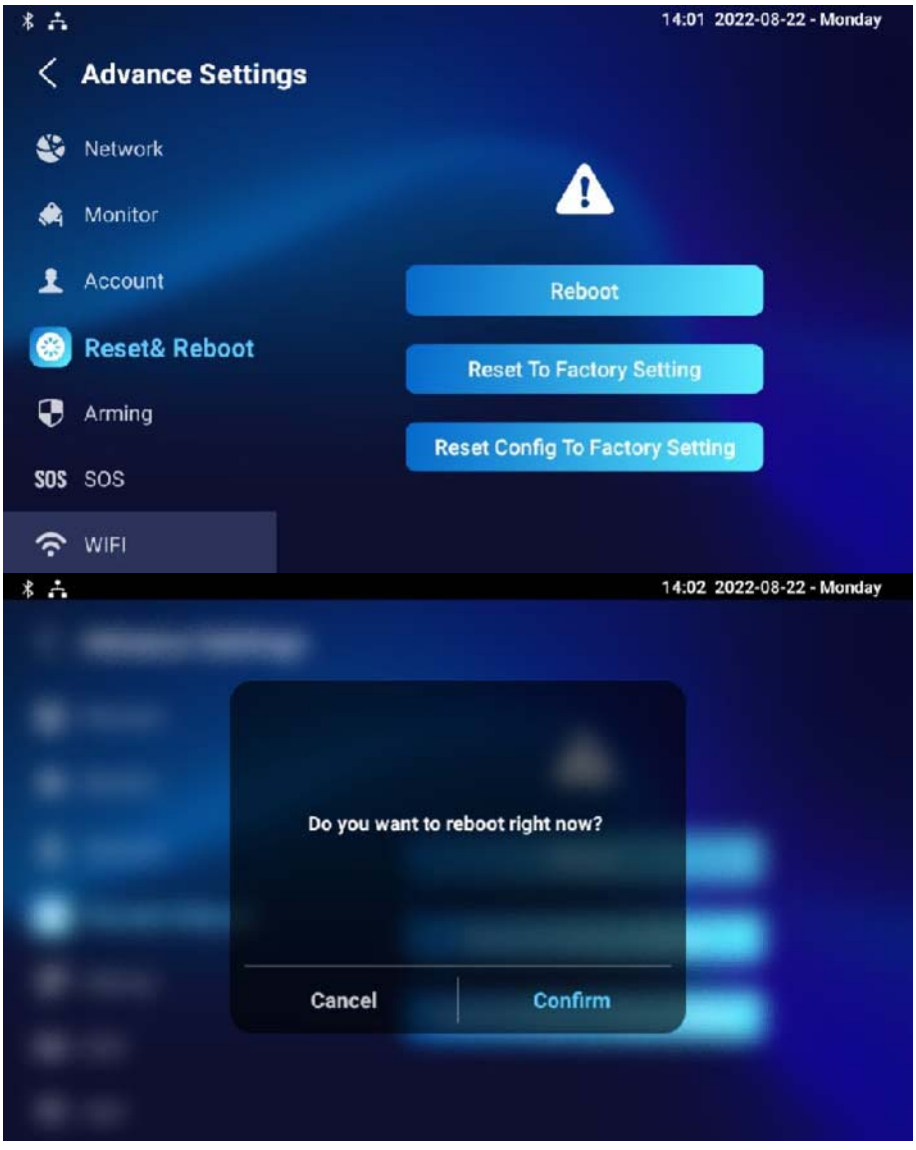
27. System Reboot&Reset

27.1. Reboot

27.1.1. Reboot on the Device

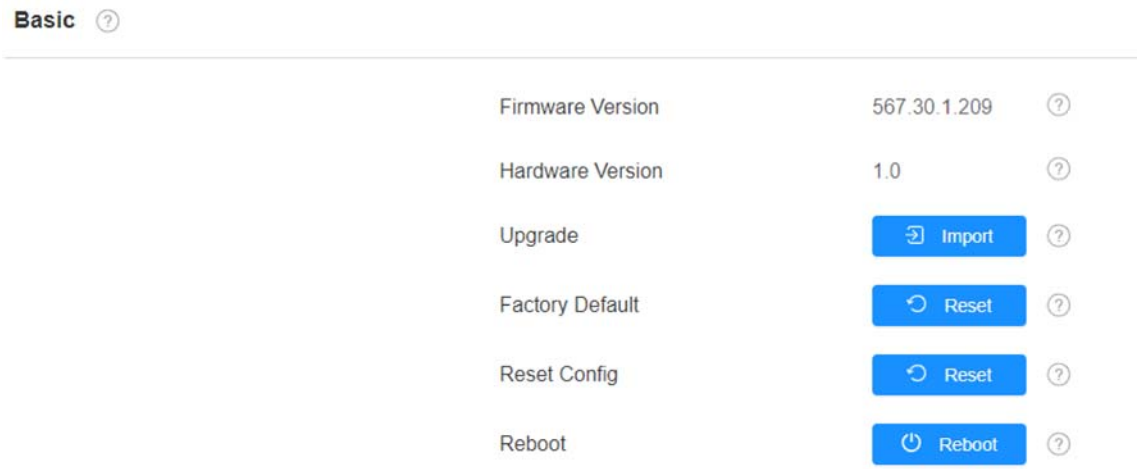
If you want to restart the system setting of the device, you can operate it directly on the device setting screen or on the device web interface.

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

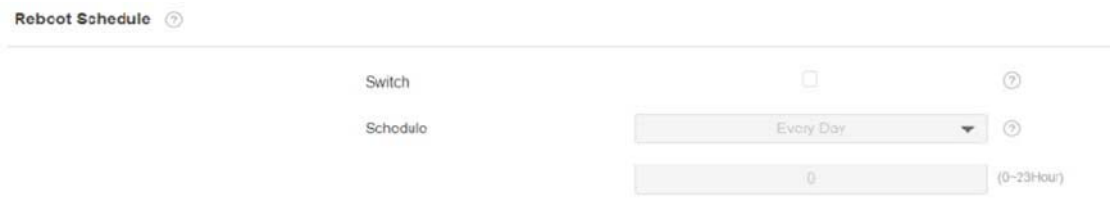


27.1.2. Reboot on the Web Interface

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



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

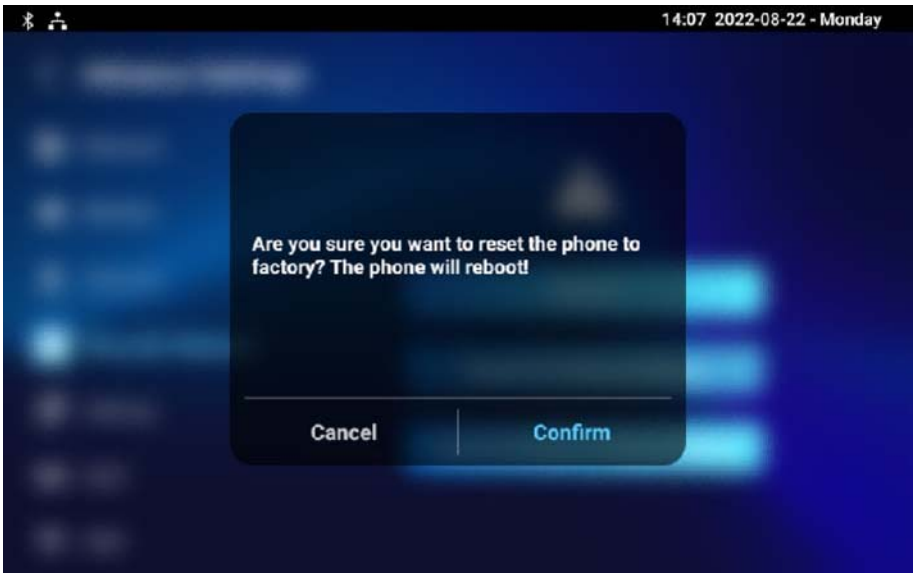


27.2. Reset

27.2.1. 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**

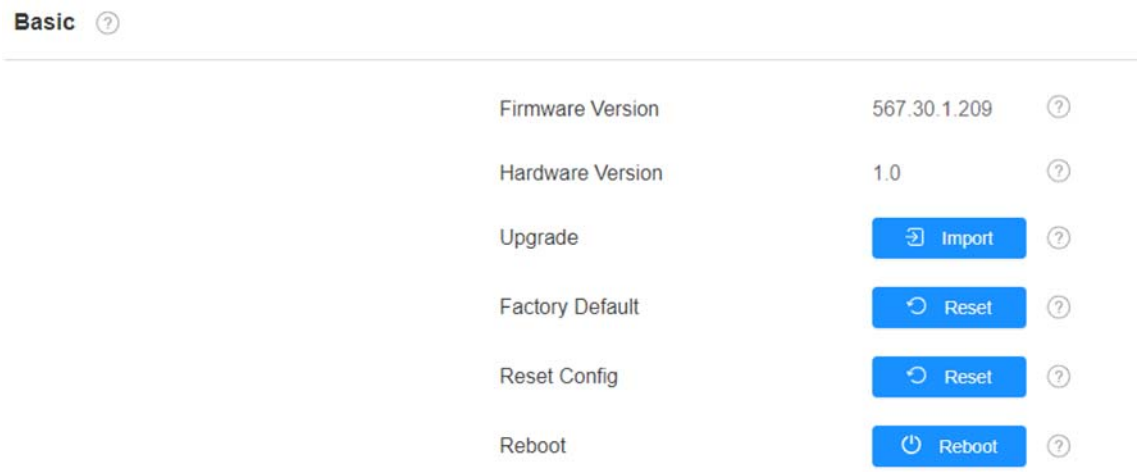
screen.



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.

27.2.2. Reset on the Web Interface

Device system can also be reset on device web **Upgrade > Basic** interface without approaching the device.



If you only want to reset to the configuration file to the factory setting, you can click **Reset Config** on the same page.

28. Abbreviations

ACS: Auto Configuration Server

Auto: Automatically

AEC: Configurable Acoustic and Line Echo Cancelers

ACD: Automatic Call Distribution

Autop: Automatical Provisioning

AES: Advanced Encryption Standard

BLF: Busy Lamp Field

COM: Common

CPE: Customer Premise Equipment

CWMP: CPE WAN Management Protocol

DTMF: Dual Tone Multi-Frequency

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

DND: Do Not Disturb

DNS-SRV: Service record in the Domain Name System

FTP: File Transfer Protocol

GND: Ground

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure Socket Layer

IP: Internet Protocol

ID: Identification

IR: Infrared

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAX: Maximum

POE: Power Over Ethernet

PCMA: Pulse Code Modulation A-Law

PCMU: Pulse Code Modulation μ-Law

PCAP: Packet Capture

PNP: Plug and Play

RFID: Radio Frequency Identification

RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

MPEG: Moving Picture Experts Group

MWI: Message Waiting Indicator

NO: Normal Opened

NC: Normal Connected

NTP: Network Time Protocol

NAT: Network Address Translation

NVR: Network Video Recorder

ONVIF: Open Network Video Interface Forum

SIP: Session Initiation Protocol

SNMP: Simple Network Management Protocol

STUN: Session Traversal Utilities for NAT

SNMP: Simple Mail Transfer Protocol

SDMC: SIP Devices Management Center

TR069: Technical Report069

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TFTP: Trivial File Transfer Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VLAN: Virtual Local Area Network

WG: Wiegand

29. FAQ

Q1: How to obtain IP address of X933/C319?

A1: You can use the display screen to get the IP information, just check the IP address at **Setting, Basic Info**.

You can also use Akuvox IP Scanner to search Akuvox devices in the same LAN network.

Q2: Do Akuvox devices support Opus codec?

A2: For now, only Akuvox Android video IP phone R48G can support Opus audio codec. Door phone and indoor monitor are still not supported.

Q3: What is the resolution of the 7-inch touch screen of X933?

A3: The ratio is 16:10, and the resolution is 1280*800.

Q4: What operating system is X933?

A4: X933 based on Android 9.0.

Q5: Can I install apps at Akuvox indoor monitor ?

A5: Akuvox has indoor monitor based on Linux system and Android system. For Linux system devices (IT80/IT81/C312/C313 series), not possible to install third-party apps. For android system devices (C315/C317/IT83/IT83/X933 series), you can install third-party apps as your wish.

Q6: Can I connect the electrical lock to the indoor monitor?

A6: Akuvox indoor monitor has relay component, so you can connect the electrical lock to indoor monitor.

Q7: Can I communicate with other indoor monitors with the indoor monitor?

A7: Akuvox devices can communicate with each other, no matter whether it is

an indoor monitor, door phone, or IP phone. Of course, indoor monitor can call other indoor monitors, also if you want, you can set other indoor monitors as auto answer mode.

30. Contact Us

For more information about the product, please visit us atwww.akuvox.com or feel free to contact us by

Sales email: sales@akuvox.com

Technical support email: support@akuvox.com

Telephone: +86-592-2133061 ext.7694/8162

We highly appreciate your feedback about our products.

BE	BG	CZ	DK	DE	EE	IE	EL
ES	FR	HR	IT	CY	LV	LT	LU
HU	MT	NL	AT	PL	PT	RO	SI
SK	FI	SE	NO	IS	LI	CH	TR

In all EU memberstates, operation of 5150-5350MHz is restricted to indoor use only.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.