

## About This Manual



[WWW.AKUVOX.COM](http://WWW.AKUVOX.COM)



# S562

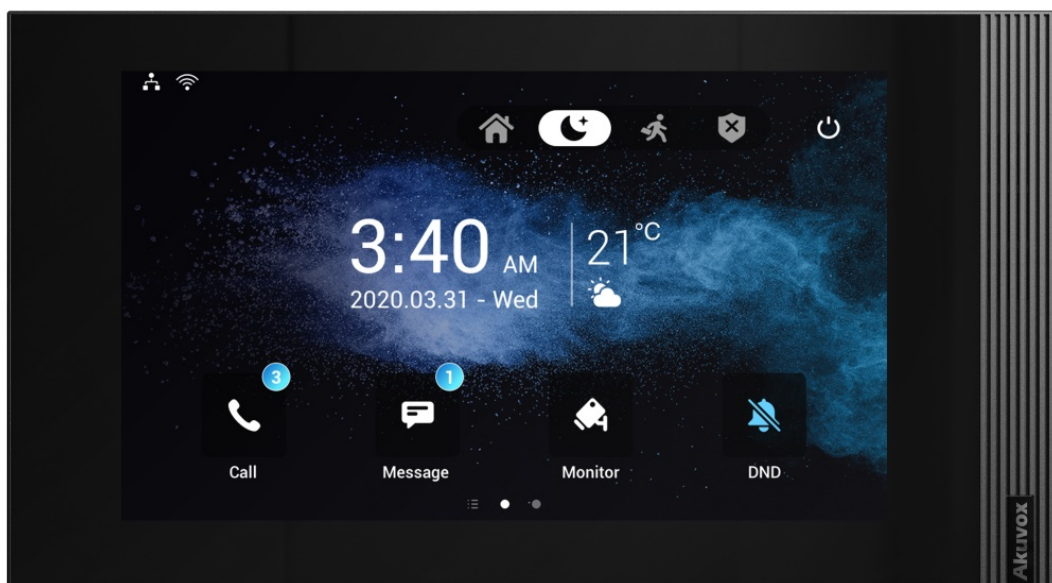
# INDOOR MONITOR

## Administrator Guide

Thank you for choosing the Akuvox S562 series indoor monitor. This manual is intended for the administrators who need to properly configure the indoor monitor. This manual is written based on firmware 562.30.10.115, and it provides all the configurations for the functions and features of the S562 series indoor monitor. Please visit the Akuvox website or consult technical support for any new information or the latest firmware.

## Product Overview

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



## Model Specification

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

# Introduction to Configuration Menu

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

**Account:** This section concerns the SIP account, SIP server, proxy server, transport protocol type, audio & video codec, DTMF, session timer, etc.

**Network:** This section mainly deals with DHCP & Static IP settings, RTP port settings, device deployment, etc.

**Device:** This section includes time & language, call feature, screen display, multicast, audio intercom feature, monitor, relay, lift import & export, door log, and web relay.

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


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

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

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



**Settings:** This section includes the RTSP and power output.



 Homepage



 Status



 Account 



 Network 


 Device 

 Contacts 

 Upgrade 

 Security 

 Settings 

 Arming 

Status » [Info](#)

### Product Information

---

### Network Information

---

# Intercom Call Configuration

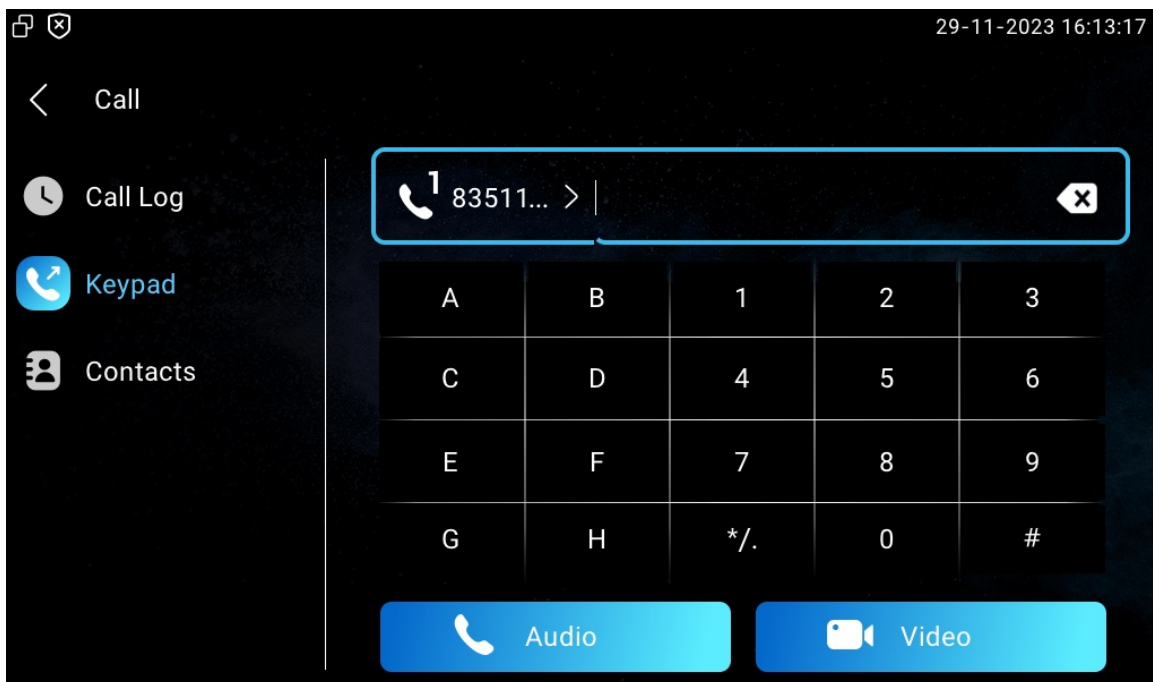
## IP Call & IP Call Configuration

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

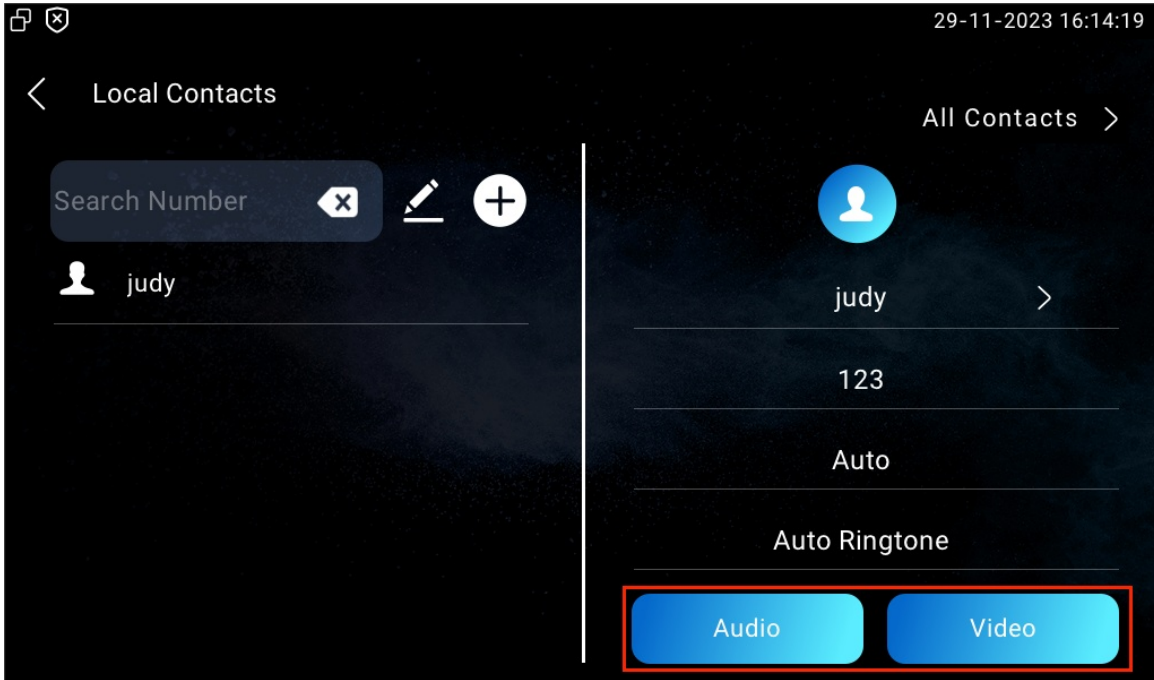
### Make IP Calls

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

Enter the IP address you wish to call on the soft keyboard, select the account to make the call, and press the **Audio** or **Video** tab to call out.



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



## IP Call Configuration

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

Others

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

### Parameter Set-up:

- **Direct IP Call:** if you do not allow direct IP calls to be made on the device, you can uncheck the check box to terminate the function.
- **Direct IP Call Port:** the direct IP call port is 5060 by default with a port range of 1-65535. If you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission.



## SIP Call & SIP Call Configuration

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

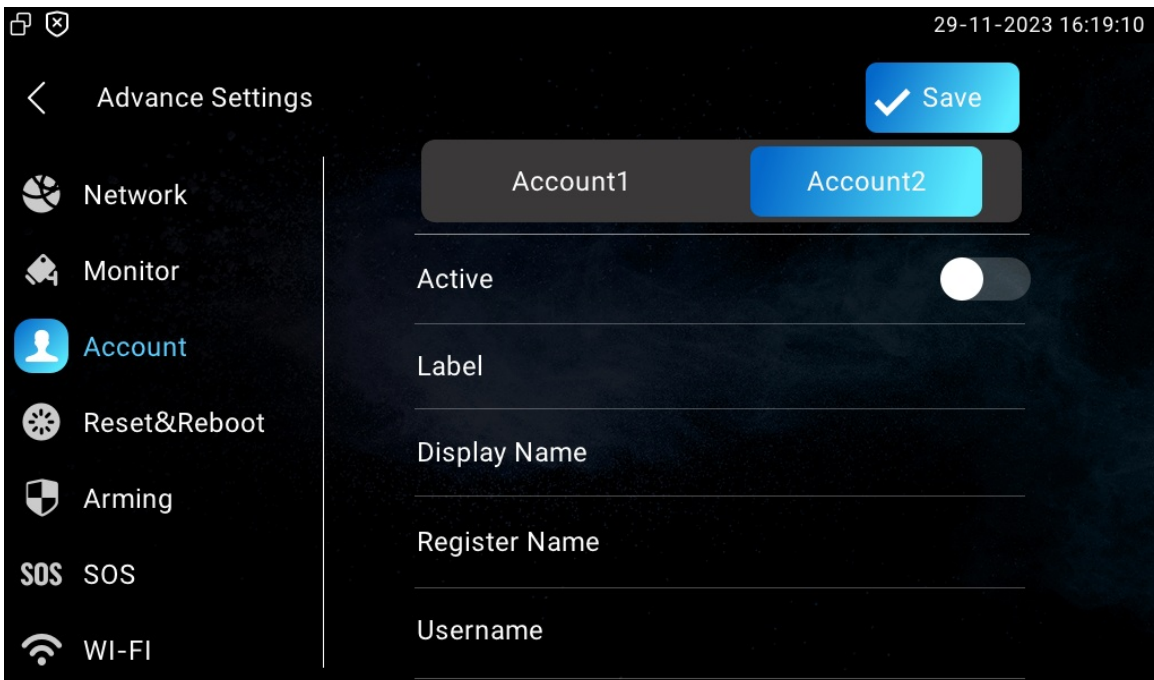
A SIP call uses SIP to send and receive data between SIP devices, and can use the internet or a local network to offer high-quality and secure communication. Initiating a SIP call requires a SIP account, a SIP address for each device, and configuring SIP settings on the devices.

## SIP Account Registration

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

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

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



### Parameter Set-up:

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

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

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

#### SIP Account

Status	Disabled
Account	Account2 ▼
Account Enabled	<input type="checkbox"/>
Display Label	<input type="text"/>
Display Name	<input type="text"/>
Register Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>

#### Parameter Set-up:

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

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

## SIP Server Configuration

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

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

Preferred SIP Server

---

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

---

Alternate SIP Server

---

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

### Parameter Set-up:

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

a. To register SIP account for Akuvox indoor monitors, obtain **Server Address** and **Port** from Akuvox indoor monitor PBX screen.

b. To register SIP account for third-party devices, obtain **Server Address** and **Port** from from third-party service provider.

## Outbound Proxy Server Configuration

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

Navigate to **Account > Basic** interface.

### Outbound Proxy Server

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

#### Parameter Set-up:

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

## SIP Call DND & Return Code Configuration

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

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

### DND

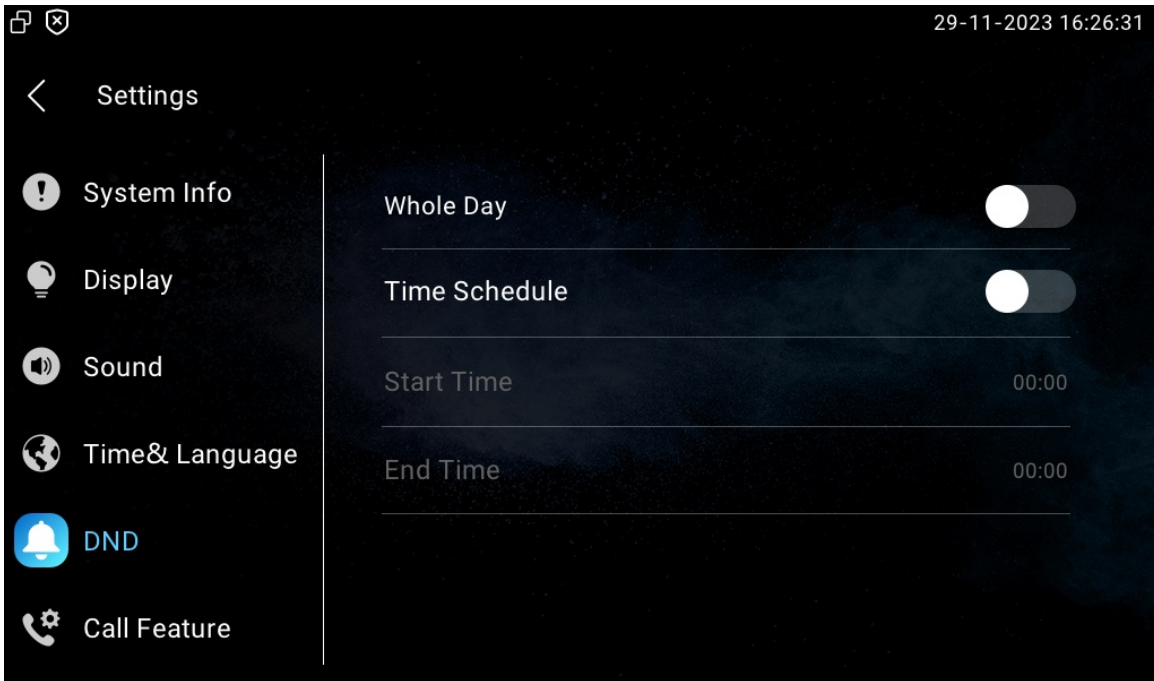
Whole Day	<input type="checkbox"/>
Schedule	<input type="checkbox"/>
DND Start Time	<input type="text" value="00:00"/>
DND End Time	<input type="text" value="00:00"/>
Return Code When DND	<input type="text" value="486(Busy Here)"/>

#### Parameter Set-up:

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

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

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



## Device Local RTP Configuration

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

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

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

Local RTP		
Starting RTP Port	<input type="text" value="11800"/>	(1024-65535)
Max RTP Port	<input type="text" value="12000"/>	(1024-65535)

### Parameter Set-up:

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

transmission range.

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

## Data Transmission Type Configuration

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

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

Transport Type

Type

TCP

### Parameter Set-up:

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

# Security

## Monitor and Image


### Monitor Setting

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

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

Door phone

+ Add Import Export

<input type="checkbox"/>	Index	Device Number	Device Name	RTSP Address	Username	Display In Call	Edit
 No Data							

Delete Delete All

---

#### Add Monitor X

Device Number	<input type="text"/>
Device Name	<input type="text"/>
RTSP Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>
Display In Call	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Disabled"/> ▼

Cancel Submit

#### Parameter Set-up:

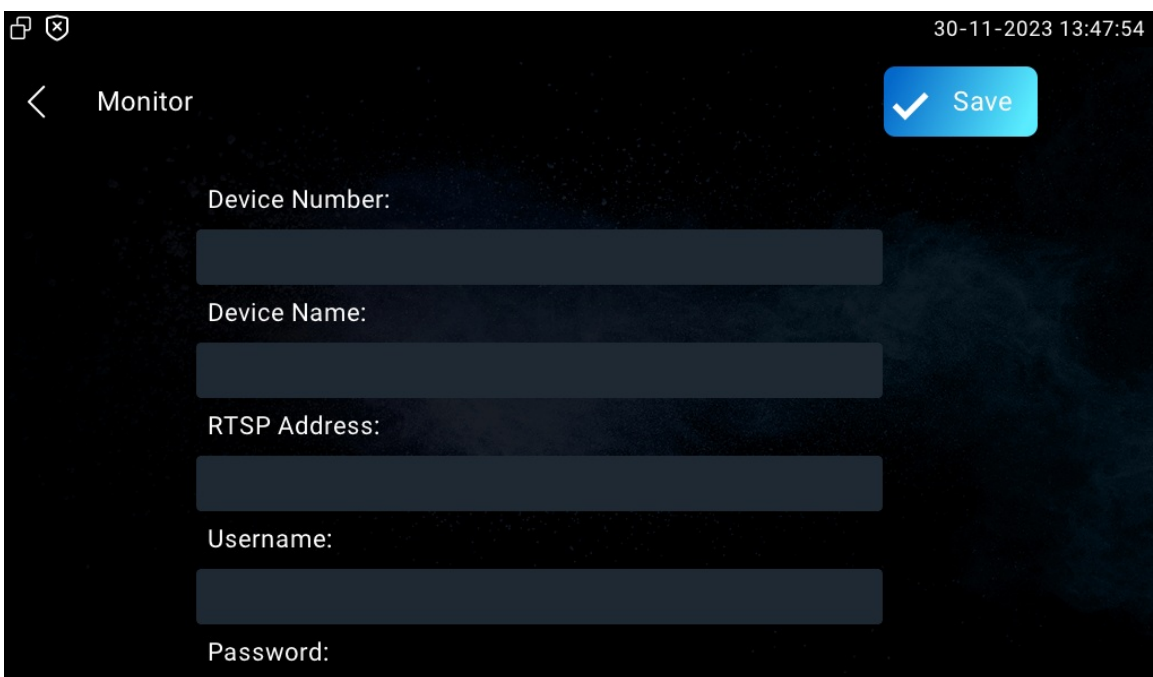
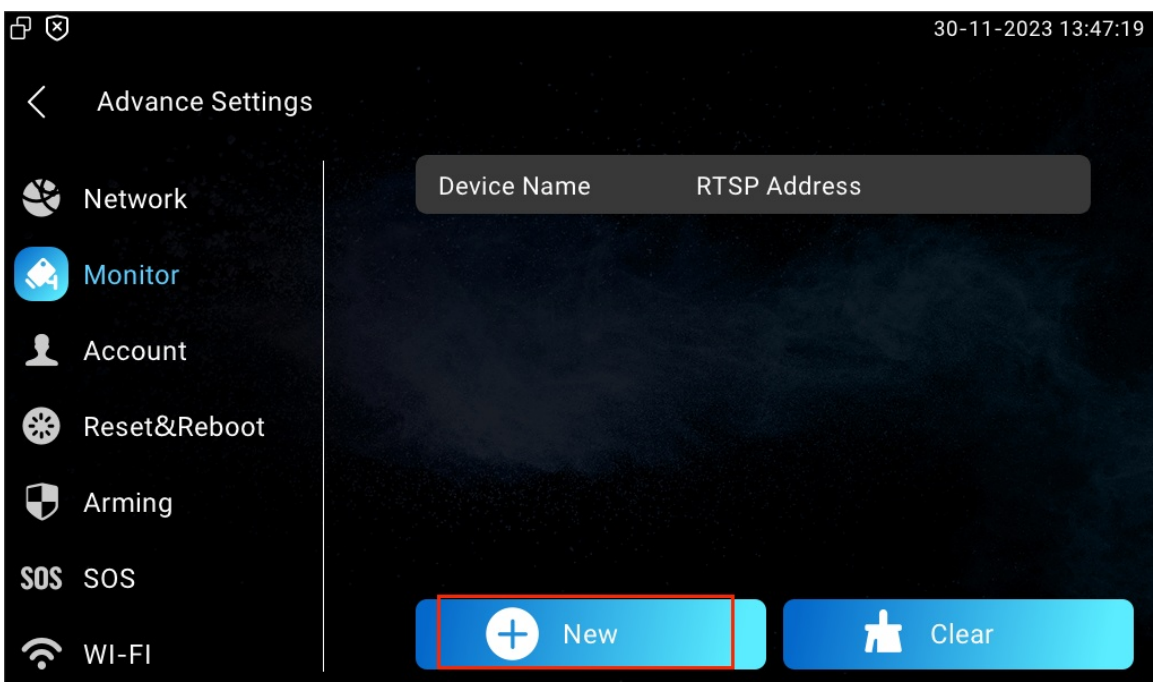
- **Device Number:** the device's SIP/IP number for identification.
- **Device Name:** the device name for identification.
- **RTSP Address:** the RTSP address of the monitoring device. RTSP format: **rtsp://Device IP address/live/ch00\_0.**

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

### Note

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

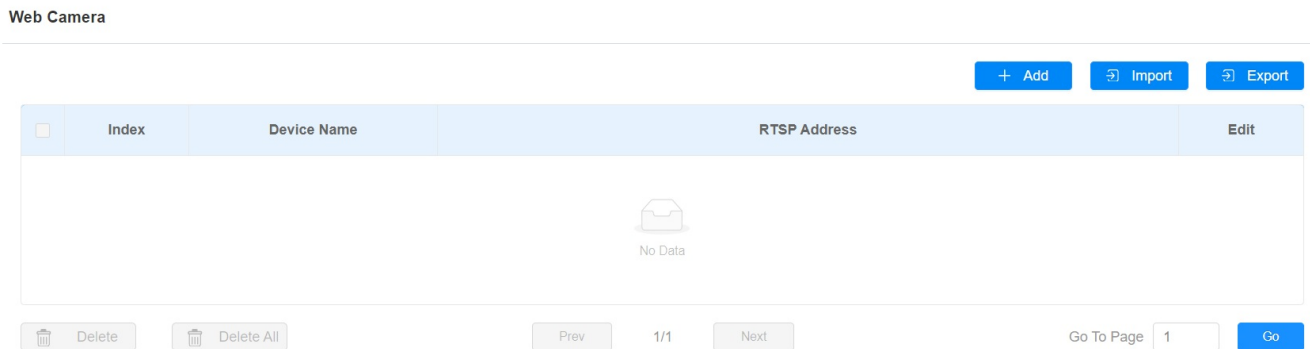
You can also set it up on the device **Settings > Advance Settings > Monitor** screen.





## Web Camera Setting

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



### Parameter Set-up:

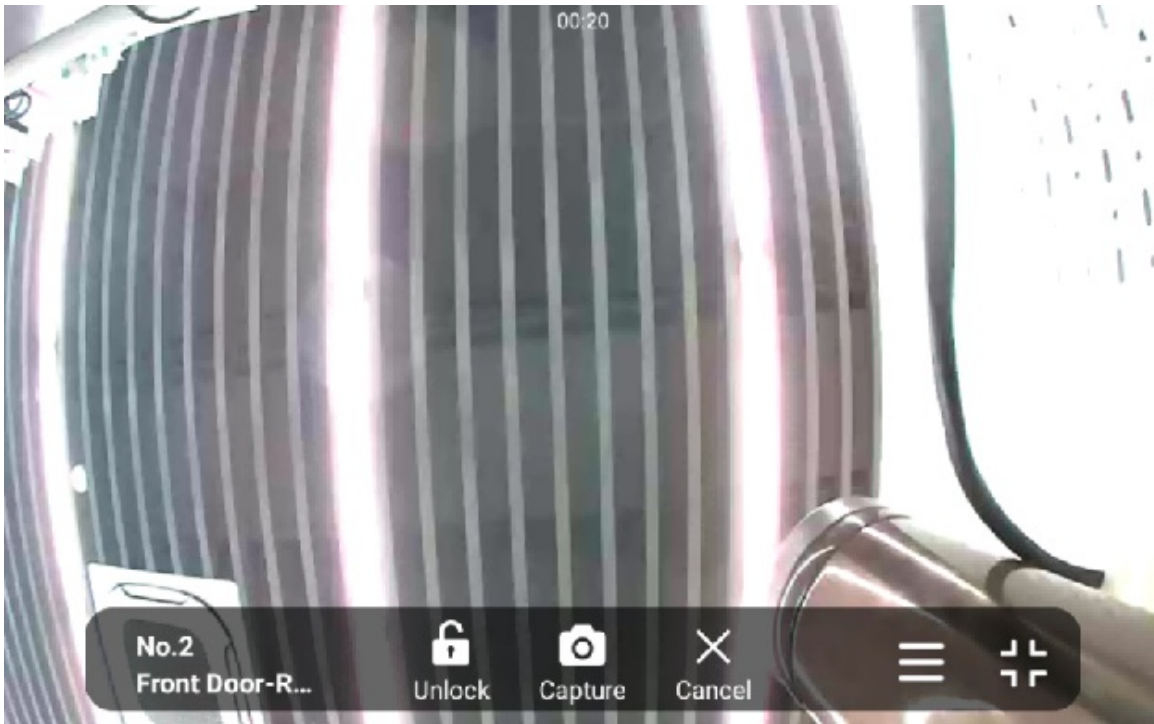
- **Device Name:** the name of the third-party camera.
- **RTSP Address:** the RTSP URL for the third-party camera.

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



## Video Image Capturing

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



## RTSP Authentication

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

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

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

### Parameter Set-up:

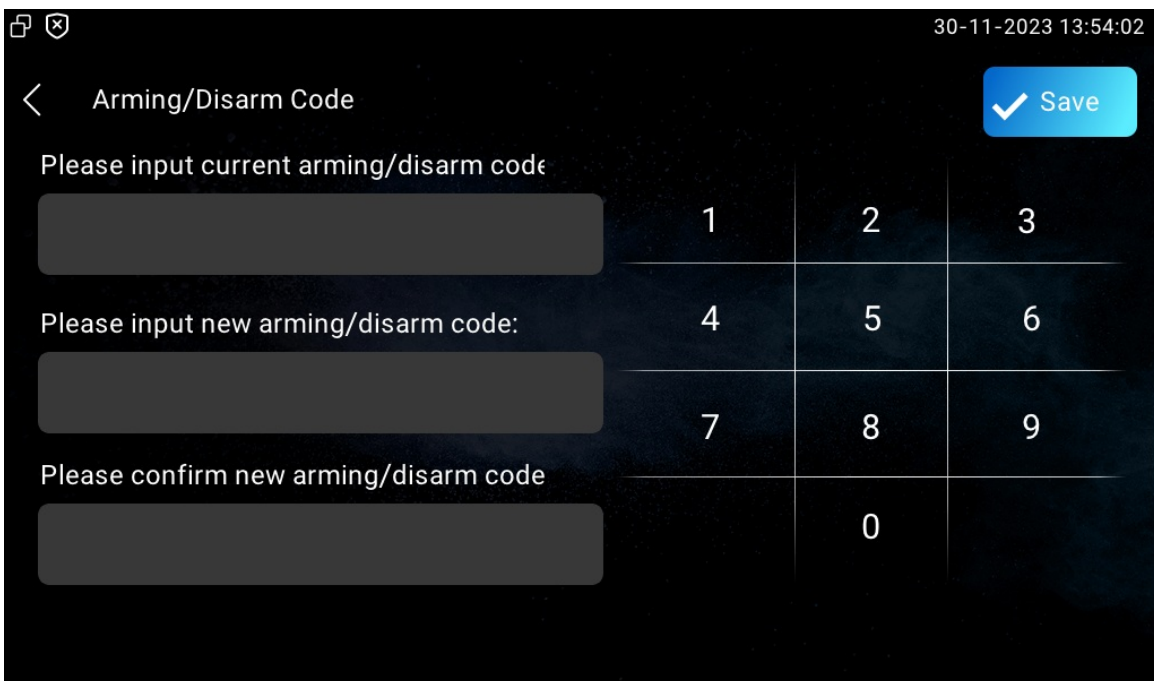
- **Authorization Type:** there are three options, **Basic**, **Digest** and **None**. **None** will allow all authorization types for the RTSP audio stream.
- **User Name:** the username for the authentication.
- **Password:** the password for the authentication.

## Alarm and Arming Configuration

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

### Configure Alarm and Arming on the Device

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



The screenshot shows the 'Arming/Disarm Code' configuration screen. At the top right, the date and time are '30-11-2023 13:54:02'. A blue 'Save' button with a checkmark is in the top right corner. The screen contains three input fields for codes, each with a corresponding row of numbers on a keypad:

Please input current arming/disarm code	1	2	3
Please input new arming/disarm code:	4	5	6
Please confirm new arming/disarm code	7	8	9
		0	

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

30-11-2023 13:54:48

< Zone Status

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

## Configure Location-based Alarm

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

30-11-2023 13:59:12

< Arming Mode Save

Home
Night
Away

Zone	Location	Zone Type	Defence Delay	Alarm Delay	Status
Zone1	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>
Zone2	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>
Zone3	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>
Zone4	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>
Zone5	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>
Zone6	Bedroom	Infrared	30s delay >	90s delay >	<input type="checkbox"/>

### Parameter Set-up:

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

**Gas, and Urgency.**

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

## Configure Alarm and Arming on the Web Interface

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

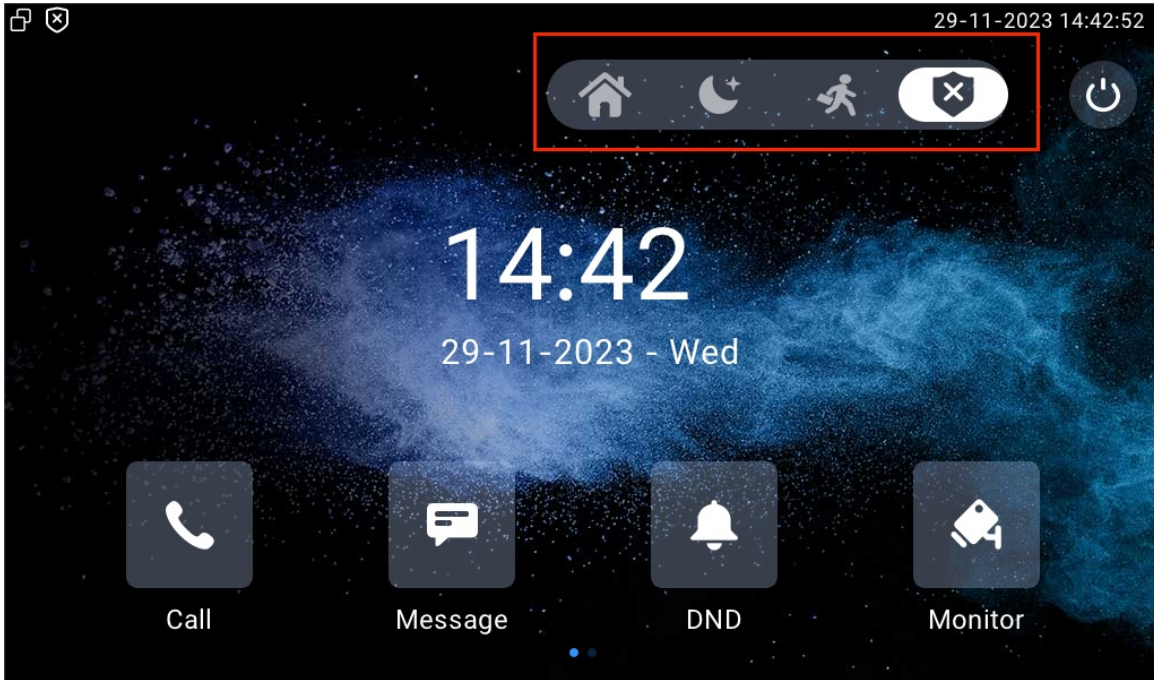
Zone Setting

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

### Parameter Set-up:

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

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



## Configure Alarm Text

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

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

### Customized Alarm

Customized Alarm Enabled

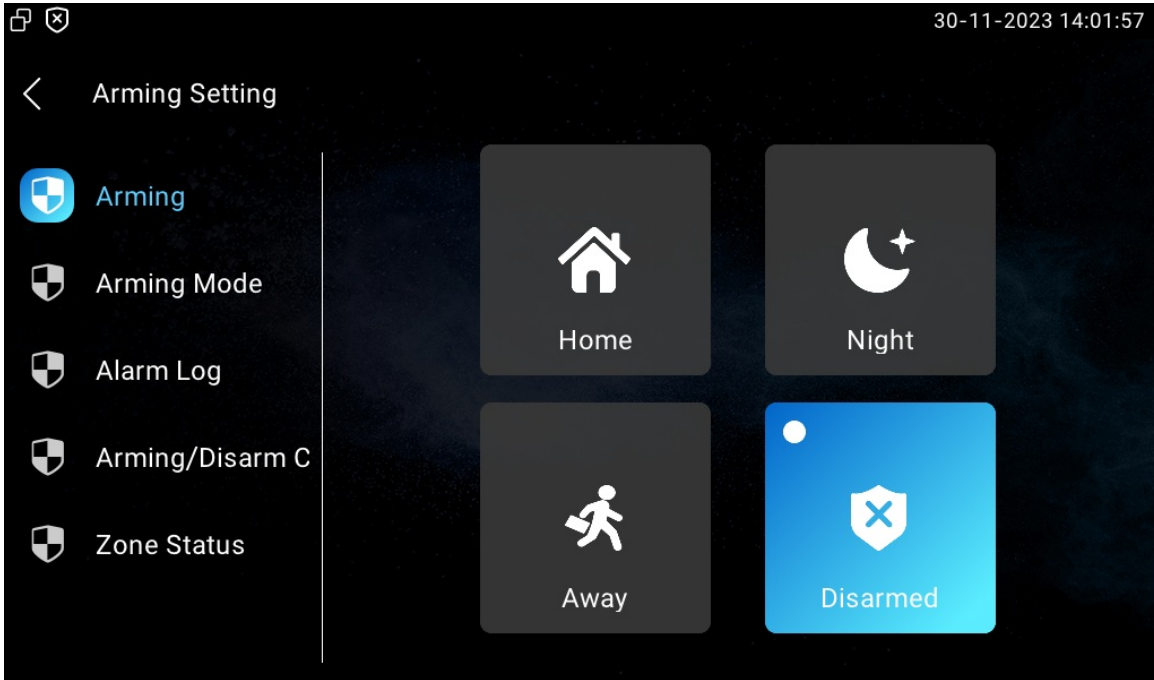
Zone	Alarm Content
Zone1	Alarm was triggered
Zone2	Alarm was triggered
Zone3	Alarm was triggered

### Parameter Set-up:

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

## Configure Arming Mode

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



## Alarm Action Configuration

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

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

### Configure Alarm Action via HTTP Command

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

HTTP Command Setting

Zone	Http Command	Send Http
Zone1	http:// <input type="text"/>	Disabled <input type="button" value="v"/>
Zone2	http:// <input type="text"/>	Disabled <input type="button" value="v"/>
Zone3	http:// <input type="text"/>	Disabled <input type="button" value="v"/>
Zone4	http:// <input type="text"/>	Disabled <input type="button" value="v"/>
Zone5	http:// <input type="text"/>	Disabled <input type="button" value="v"/>
Zone6	http:// <input type="text"/>	Disabled <input type="button" value="v"/>

### 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.

---

Receiver Of SIP Message

---

Receiver

---

SIP Message Setting

---

Zone	SIP Message
Zone1	<input type="text"/>
Zone2	<input type="text"/>
Zone3	<input type="text"/>
Zone4	<input type="text"/>

### Parameter Set-up:

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

## Configure Alarm Action via SIP Call

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

---

Call Setting

---

Call Number

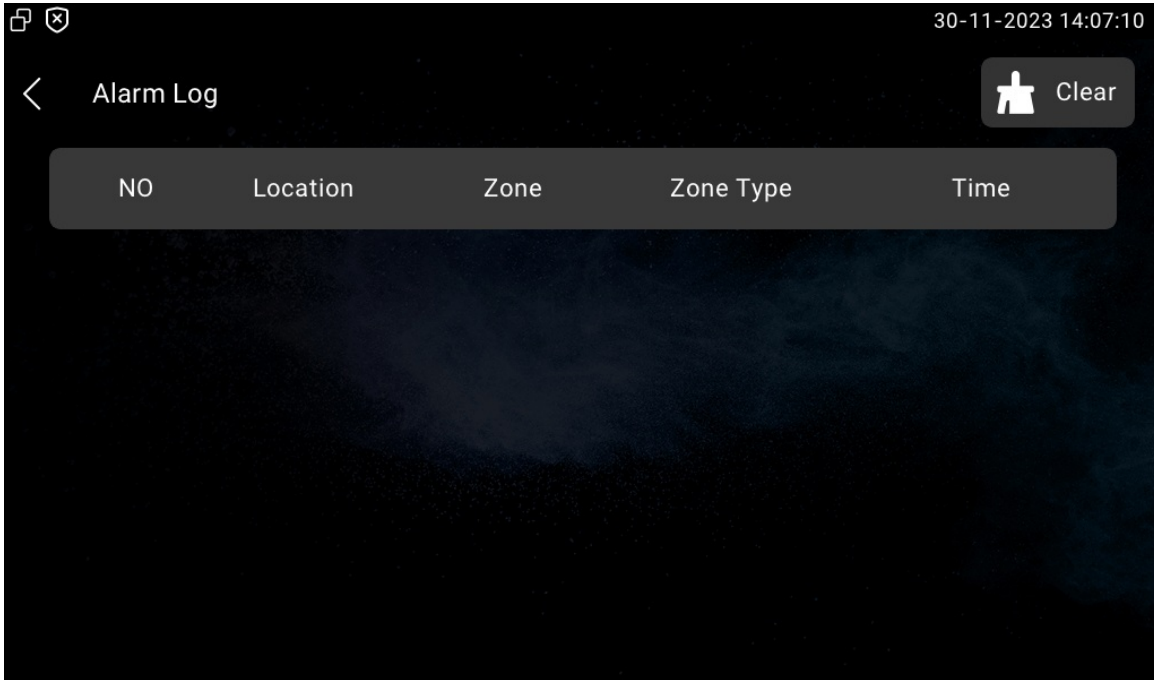
### Parameter Set-up:

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

## Check Alarm Log

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

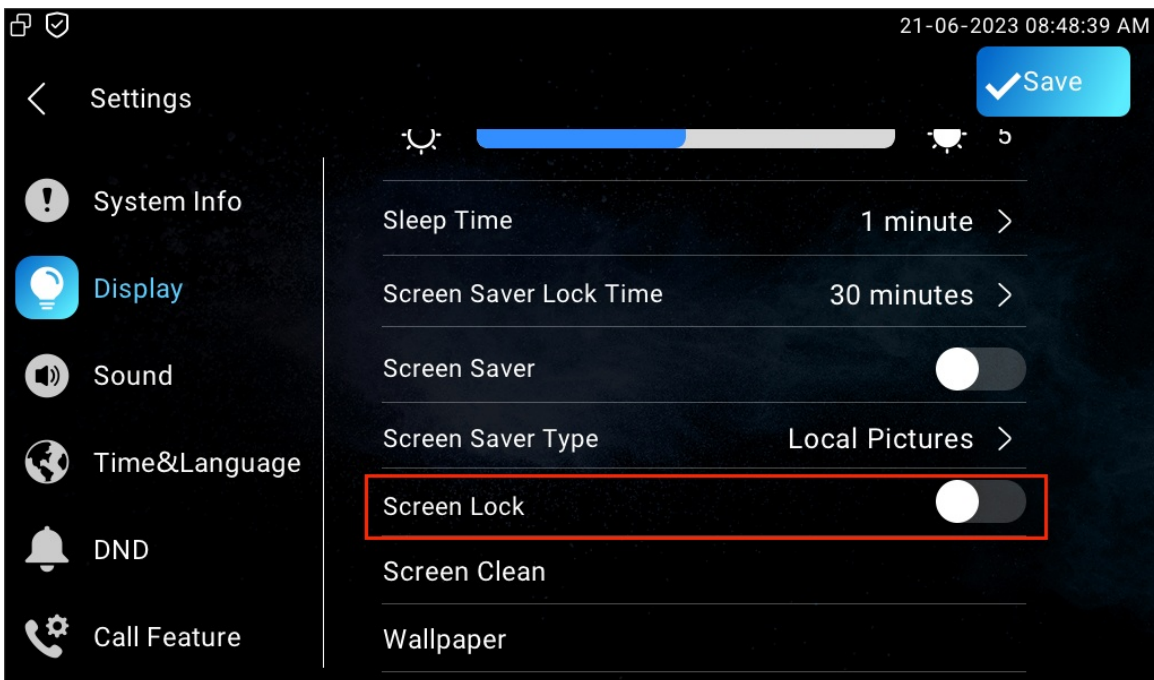




## Screen Unlock Setting

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

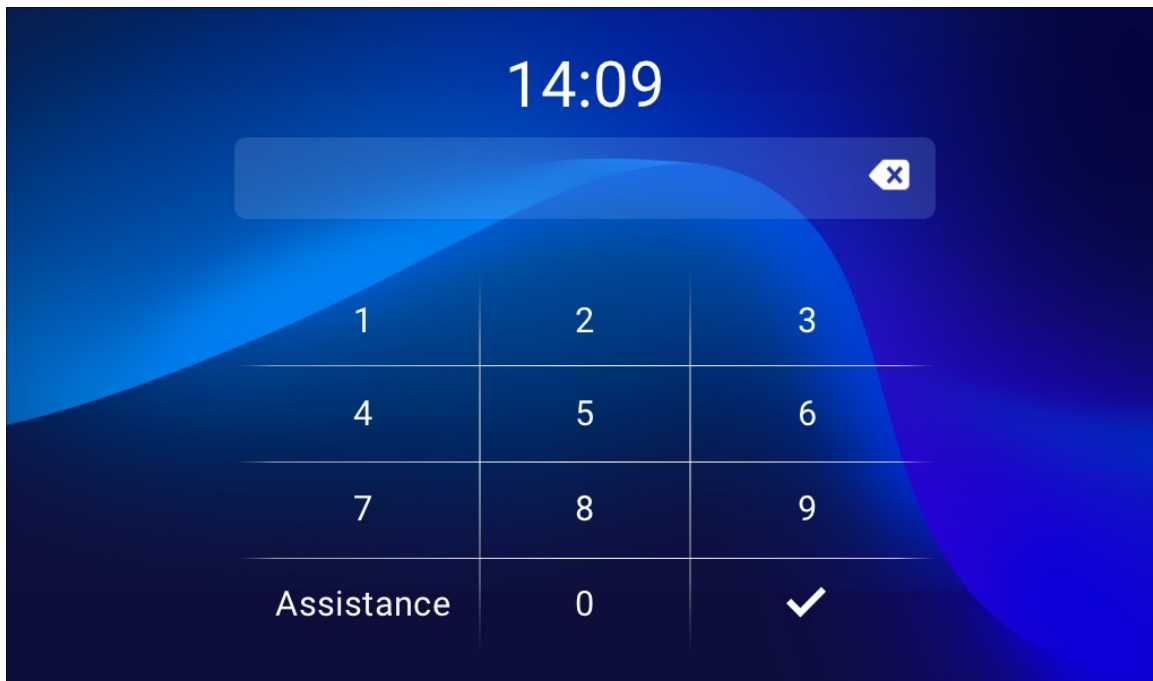
You can enable the screen lock function directly on the device **Settings > Display** screen.



## Screen Unlock by PIN Code

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

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



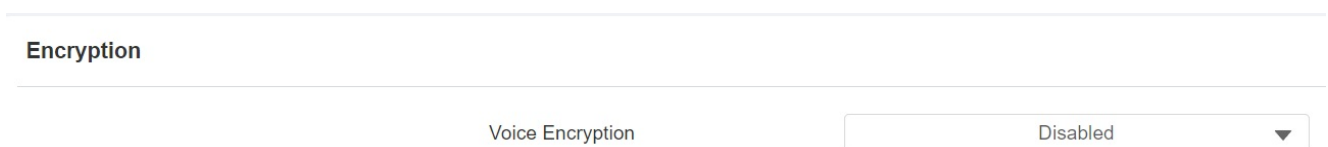
### Note

- The default unlock PIN is 123456.

## Voice Encryption

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

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



**Parameter Set-up:**

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

## Web Interface Automatic Log-out

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

Navigate to **Security > Basic** interface.

### Session Time Out

Session Time Out Value

8000

(60~14400Sec)

## Power Output Setting

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

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

### Power Output Setting

Power Output Enable

Disabled

## High Security Mode

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

To configure this feature on the web **Security > Basic > High Security Mode** interface.

---

## High Security Mode

---

Enabled



### Important Notes

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

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

·PC Manager: 1.2.0.0

·IP Scanner: 2.2.0.0

·Upgrade Tool: 4.1.0.0

·SDMC: 6.0.0.34

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

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

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

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

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

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

# Lift Control

You can summon a lift via the lift control feature.

## Configure Lift Control

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

Lift Control ?

Name	Status	Icon	Label	Http Command
Lift1	Enabled <span>▼</span>	Up <span>▼</span>		http:// <span>▼</span>
Lift2	Disabled <span>▼</span>	Up <span>▼</span>		http:// <span>▼</span>

### Parameter Set-up:

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

## Configure Lift Control Prompt

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

To do this configuration on the web **Device > Lift > Hints** interface. Click the **Edit** icon to modify the desired prompt.

Hints ?

+ Add Import Export ▼

<input type="checkbox"/>	Index	HTTP Status Code	Lift	Hints	Edit
<input type="checkbox"/>	1	200	Lift1	Lift is coming to your floor	<a href="#">✎</a>
<input type="checkbox"/>	2	200	Lift2	Lift has been sent to Ground Floor	<a href="#">✎</a>

Delete Delete All Prev 1/1 Next 1 Go

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

---

Hints ⓘ

---

[+ Add](#) [📄 Import](#) [Export ▼](#)

# Call Logs

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


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

Call Log

Capture Enable

Capture Delay (Sec)

Call History  [Export](#) [Hang Up](#)

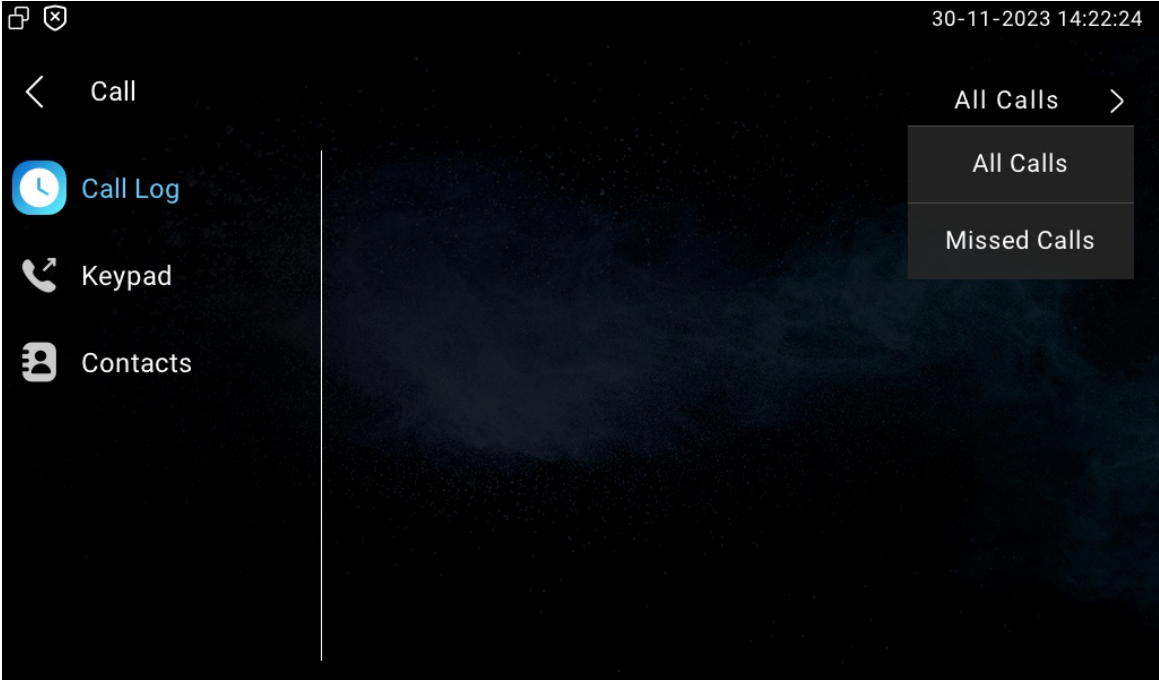
<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number
 No Data							

[Delete](#) [Delete All](#) [Prev](#) 1/1 [Next](#) Go To Page  [Go](#)

## Parameter Set-up:

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

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









# Firmware Upgrade

Akuvox devices can be upgraded on the device web interface.

Navigate to **Upgrade > Basic** interface.

## Basic

---

Firmware Version	562.30.10.115
Hardware Version	562.0.2.0.1.0.0.0
Upgrade	 Import
Reset To Factory Setting	 Reset
Reset Config To Factory Setting	 Reset
Reboot	 Reboot

### Note

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

# Backup

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


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


---

Others

---

Config File

 Import

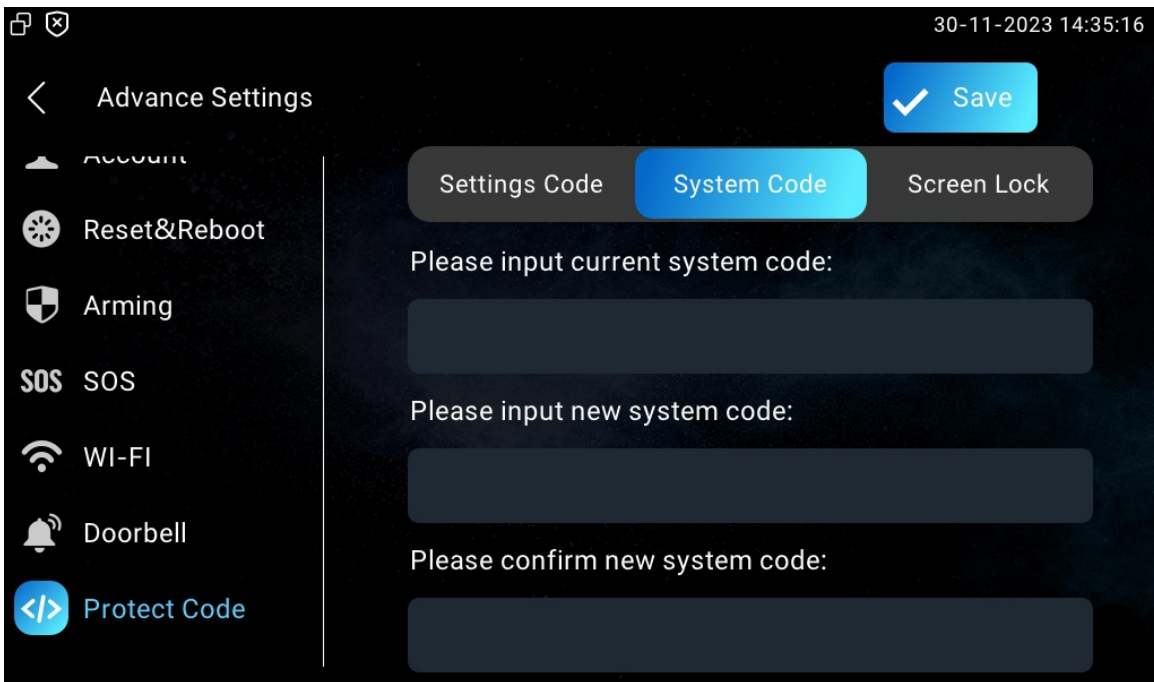
 Export

(Encrypted)

# Password Modification

## Modify Device Basic Setting Password

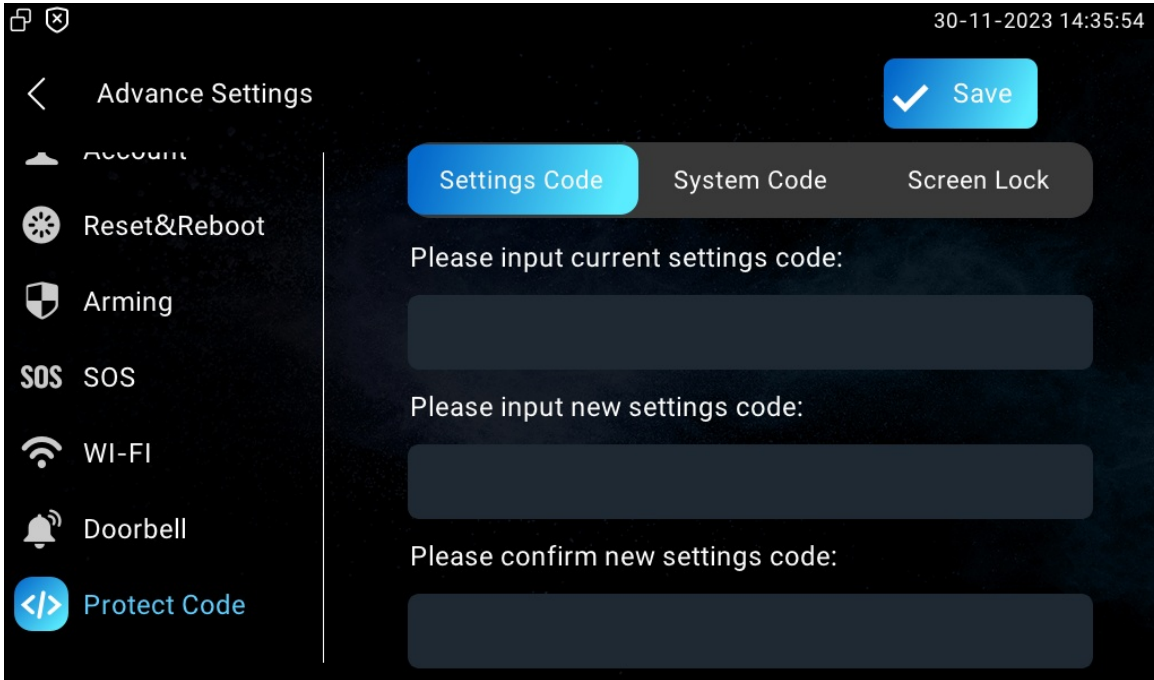
To do the configuration on device **Settings > Advance Settings > Protected Code** screen to choose **System Code** to change a new password. The default password is 123456.



## Modify Device Advance Setting Password

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

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



## Modify Device Web Interface Password

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

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

### Web Password Modify

User Name

admin

Change Password

### Change Password

X

The password must be at least eight characters long and contains at least one uppercase letter, one lowercase letter, and one digit.

User Name

admin

Old Password

New Password

Confirm Password

Cancel

Change

### Note

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

## Modify Screen Lock Password

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

