Wireless Intercom Siren

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the Wireless Intercom Siren (hereinafter referred to as "the siren"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or

visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Introduction

1.1 Overview

The Wireless Intercom Siren triggers sound and light alarms when it receives alarm signals. It also offers the intercom function, which can be enabled in the DMSS and DoLynk Care mobile app, making it easy for you to communicate with people on your site. The security center can also use the intercom to communicate with your site through the siren.

1.2 Technical Specifications

Please refer to the corresponding technical specifications according to the corresponding models.

Table 1-1 Technical specifications

Type	Parameter	Description	
Port	MIC	Yes	
Audio and Video	Video Intercom	Yes	
Function	Button	1 × panic button, 1 × power button	
	Buzzer	Yes	
	Tamper Alarm	Yes	
	Remote Update	Cloud update	
	Low Battery Alarm	Yes	
	Battery Level Display	Yes	
	Signal Strength	Signal strength detection, RF-HD detection	
Technical Parameter	LED Indicator	Red, blue and green indicators	
	Scenario	Indoor	
	Max. Operating Current	Static current: 18 uA Max current: 1.5 A	
	Alarm current	300 mA	
	Sound and Light Alarm	Yes	
Wireless Parameters	Carrier Frequency	DHI-ARA14-W2(868): 865.34 MHz–868.60 MHz	DHI-ARA14-W2: 433.1 MHz–434.6 MHz
	Transmission Power	DHI-ARA14-W2(868): Limit 25 mW	DHI-ARA14-W2: Limit 10 mW

Type	Parameter	Description	
	Communication Distance	ARA14-W2(868): 1600 m (alarm transmission), 1000 m (intercom)	ARA14-W2: 1200 m (alarm transmission), 800 m (intercom)
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Power Supply	12 VDC/4 × CR123A battery	
	Battery Model	CR123A	
	Standby Time	3 years (when triggered once every 2 weeks and alarms for 120 sec)	
	Power Consumption	0.24 mW (standby)	
	Operating Environment	-10 °C to +55 °C (+14 °F to +131 °F) (indoor)	
	Operating Humidity	10%–90% (RH)	
	Storage Temperature	–10 °C to +55 °C (+14 °F to +131 °F)	
	Storage Humidity	10%–90% (RH)	
	Product Dimensions	133.0 mm × 133.0 mm × 35.5 mm (5.24" × 5.24" × 1.40"）	
	Packaging Dimensions	170 mm × 166 mm × 55 mm (6.69" × 6.54" × 2.71"）	
	Installation	Wall mount	
	Net Weight	377 g (0.83 lb)	
	Gross Weight	507 g (1.12 lb)	
	Casing	PC + ABS	
	Certifications	CE	
	Color	White	
	Anti-corrosion	Basic protection	

2 Checklist

Check the package against the following list. If any of the items are damaged or missing, contact customer service.

Figure 2-1 Checklist

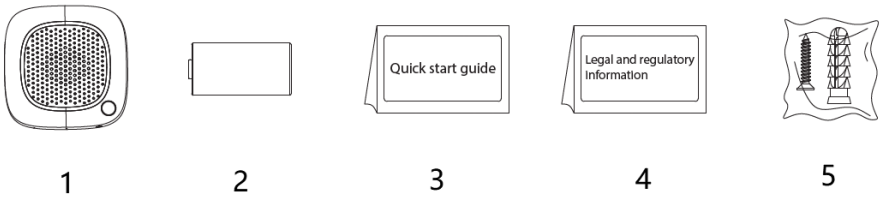


Table 2-1 Checklist

No.	Item	No.	Item
1	Wireless intercom siren	4	Legal and regulatory information
2	CR123A battery × 4	5	Package of screws
3	Quick start guide	-	-

3 Design

3.1 Appearance

Figure 3-1 Appearance

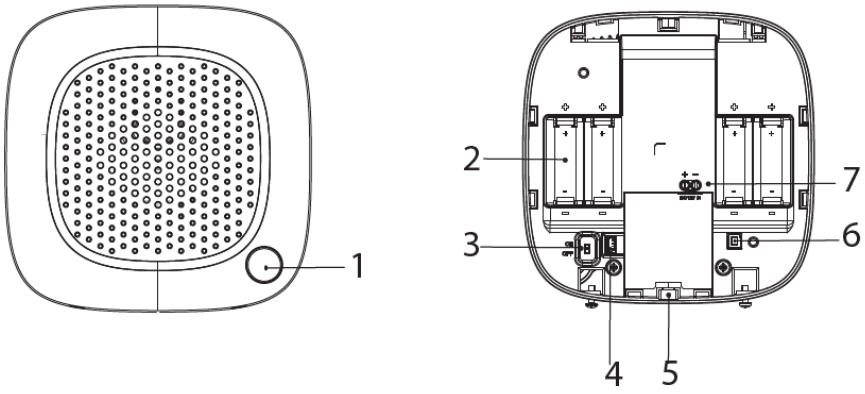
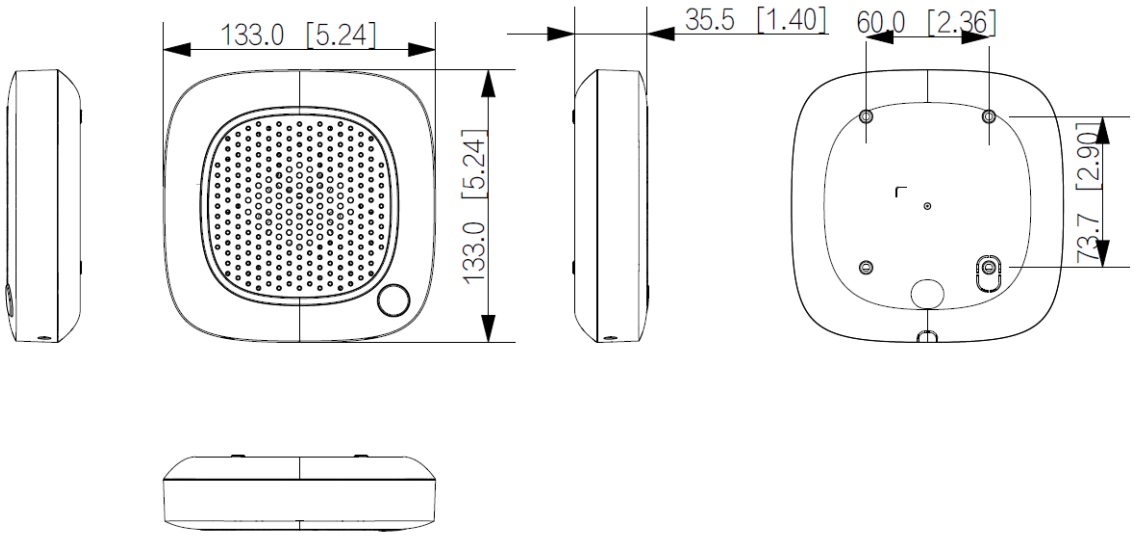


Table 3-1 Structure

No.	Name	Description
1	Panic button	Press to activate an alarm as soon as an intruder or threat is encountered.
2	Battery compartment	Used to place batteries.
3	On/off switch	Turn on or turn off the siren.
4	Serial port	Used for debugging.
5	MIC	Captures audio.
6	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
7	12 VDC power terminal	Insert the 12 VDC power cable. The cable is not included in the package.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])

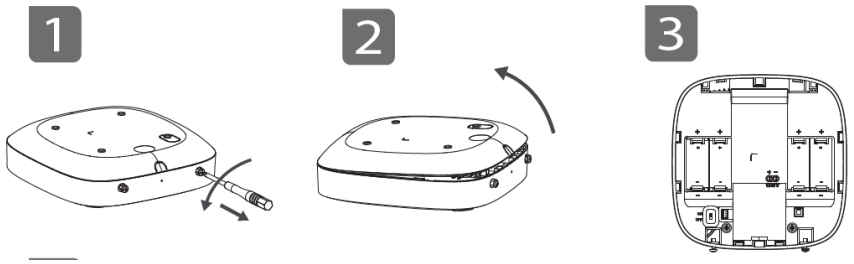


4 Powering On

Procedure

Step 1 Open the front panel of the siren.

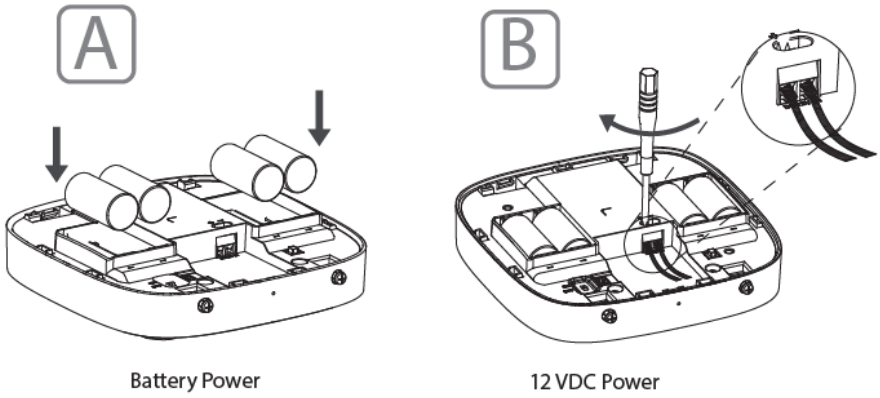
Figure 4-1 Open the front panel



Step 2 Power on the siren through either battery or 12 VDC power.

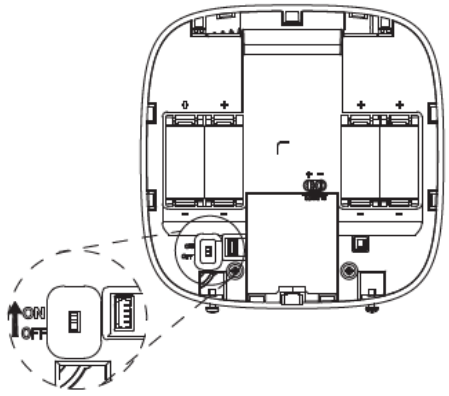
- Battery power: Install four CR123A batteries according to the polarity mark.
- 12 VDC power: Feed the 12 VDC power cable into the case through the power cable knockout.

Figure 4-2 Power on



Step 3 Push the power switch to **ON**.

Figure 4-3 Switch



5 Adding Siren to the Hub

Background Information

Before you connect the siren to the hub, install the DMSS app on your phone. This manual uses iOS as an example.

- Make sure that the version of the DMSS app is 1.99.700 or later, and the hub is V2.000.0000001.0.R.240202 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Procedure

Step 1 Go to the hub screen, and then tap **Peripheral** to add the siren.

Step 2 Tap **+** to scan the QR code at the bottom of the siren, and then tap **Next**.

Step 3 Tap **Next** after the siren has been found.

Step 4 Follow the on-screen instructions and switch the siren to on, and then tap **Next**.

Step 5 Wait for the pairing.

Step 6 Customize the name of the siren, and select the area, and then tap **Completed**.

6 Installation

Prerequisites

Prior to installation, power on the siren, connect it to the hub, and then perform signal strength test and RF-HD test. We recommend that you install the siren in a place with a signal strength and RF-HD of at least 2 bars.

Procedure

Step 1 Loosen the screw at the bottom of the siren to remove the front panel.

Step 2 Set the siren into a horizontal position. Use the spirit level to make sure the siren is horizontal and level.

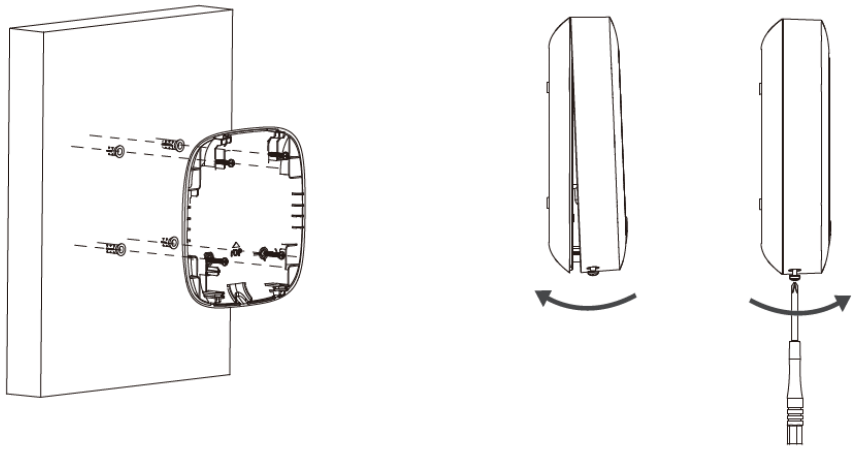
Step 3 Put the expansion bolts into the holes.

Step 4 Align the screw holes on the rear panel with the expansion bolts.

Step 5 Secure the rear panel with self-tapping screws.

Step 6 Tighten the screw at the bottom of the front panel to secure the siren.

Figure 6-1 Installation



7 Configuration

You can view and edit general information of the siren.

7.1 Viewing Status

On the hub screen, select a siren from the peripheral list, and then you can view the status of the siren.

Table 7-1 Status

Parameter	Description
Permanent Deactivate	The status for whether the permanent deactivate function is enabled or disabled. ● : Enable. ● : Only disable tamper alarm. ● : Disable.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the siren. ● : Low. ● : Weak. ● : Good. ● : Excellent. ● : No.
External Power Status	Whether there is a failure alarm for 12 VDC power. ● : Connected. ● : Disconnected.
Battery Level	The battery level of the siren. ● : Fully charged. ● : Sufficient. ● : Moderate. ● : Insufficient. ● : Low.
Tamper Status	The anti-tamper status for the siren. It reacts when a siren is disassembled.

Parameter	Description
Online Status	Online and offline status of the siren. ● : Online. ● : Offline.
Volume	Alarm volume level.
Alarm Duration	Duration of the alarm sound.
Alarm Status Indication	Indicates the alarm status of the siren when the function is enabled.
Arm Indication	Indicates the alarm event through the indicator and sound signal when the function is enabled.
Entering/Exiting Time and Arming/ Disarming Ringtone	The ringtone when entering or exiting arming mode.
Beep Volume	High, medium and low.
Transmit through Repeater	The status of whether the siren forwards peripheral messages to the hub through the repeater.
Program Version	The program version of the siren.

7.2 Configuring the Siren

On the hub screen, select a siren from the peripheral list, and then tap to configure the parameters of the siren.

Table 7-2 Siren parameter description

Parameter	Description
Device Configuration	● View siren name, type, SN and device model. ● Edit siren name, and then tap **Save** to save your configurations.
Area	Select the area to which the siren is assigned.
Zone No.	The zone number assigned to the door detector alarm, which cannot be configured.
Permanent Deactivate	● Tap **Enable** , and then the permanent deactivate function of siren will be enabled. **Enable** is set by default. ● Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages. ● Tap **Disable**, and then the permanent deactivate function of the siren will be disabled.
Control Permissions	Select areas to which the siren will be linked when an alarm is triggered.
External Power Detection	If **External Power Detection** is enabled, power failure alarm messages will be pushed to the DMSS.

Parameter	Description
LED Indicator	**LED Indicator** is enabled by default. If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the siren is functioning normally or not.
Sound Settings	• Configure volume level of the siren sound and ringtone during arming and disarming, and entering and exiting time. Select from low, medium, and high. • **Ringtone configuration** :Enable the function to configure the ringtone audios.
Alarm Duration	Configure the duration of the alarm sound.
Arm Indication	Enable the **Arm Indication** function if you need.
Alarm Status Indication	If **Alarm Status Indication** is enabled, the LED indicator will turn on when an alarm is triggered in an armed area. The LED indicator will flash twice every minute if an area has not been disarmed, and an alarm event ended 30 seconds before. The indicator works when only main power is enabled.
Over-temperature Alarm	Enable the **Over-temperature Alarm** function, and then the alarm will be triggered when the temperature of the area where the water leak detector is installed is higher or lower than the defined one. Tap next to **Over-temperature Alarm** to enable this function. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap **+** or **-** to set the temperature ranges.
Panic Button	• Panic Button: Enable the function and press and hold the button on the front panel of the siren for 3 seconds, alarm messages will be reported. • Link to Siren: When an alarm is triggered, the alarm events are reported with siren linkages. • Link Video: When an alarm is triggered, the alarm events are reported with videos. • Video Channel: Select the video channel to be linked after pressing the panic button.
Intercom Service	Intercom between siren and DMSS app, or between siren and third-party SIP platform.
Beep Volume	Set beep volume during arming and disarming, and enter and exit delay. Select from **High** , **Medium** and **Low**.
Signal Strength Detection	Check the current signal strength.

Parameter	Description
RF-HD Test	Tap **Start Detection** to test the RF-HD signal of the location where the siren is placed.
Siren Test	Tap **Start Detection** to test whether the buzzer works normally. The siren sounds for 5 seconds during the test.
Transmit Power	• Select from high, low, and automatic. • The higher transmission power levels are, the further transmissions can travel, but power consumption increases.
Cloud Update	Update online.

8 Intercom Service

8.1 App Intercom

8.1.1 Configuring Intercom on Hub

You need to configure the intercom services on the hub.

On the **Hub** screen, select **Hub Setting** > **Intercom Service**, and enable **Intercom Service**.

Table 8-1 Intercom setting

Parameter	Description
Intercom Time Limit	When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again. The duration of every intercom session cannot be over 20 minutes.
Intercom	App Intercom: Intercom between the siren and DMSS app. Select the siren assigned to different areas, or select **Do Not Link**.

8.1.2 Configuring Intercom on Siren

Go to the **Device Details** page of the intercom siren, and then tap , and enable **Intercom Service**.

8.1.3 Intercom Commissioning

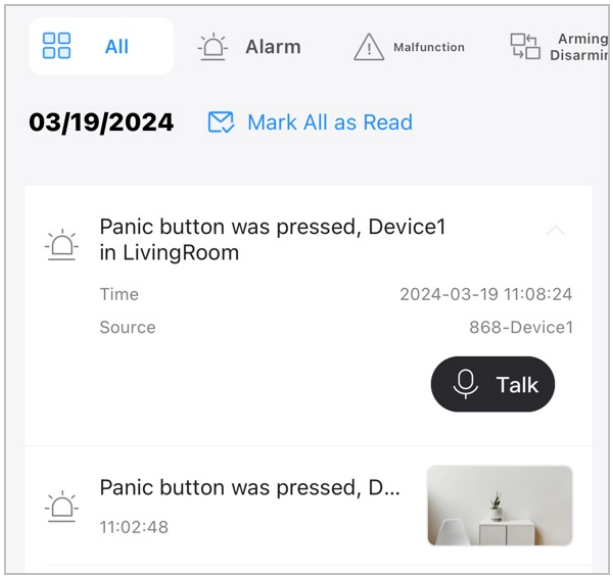
Initiate an intercom session through DMSS app.

Procedure

Step 1 On the home screen, select **Message**.

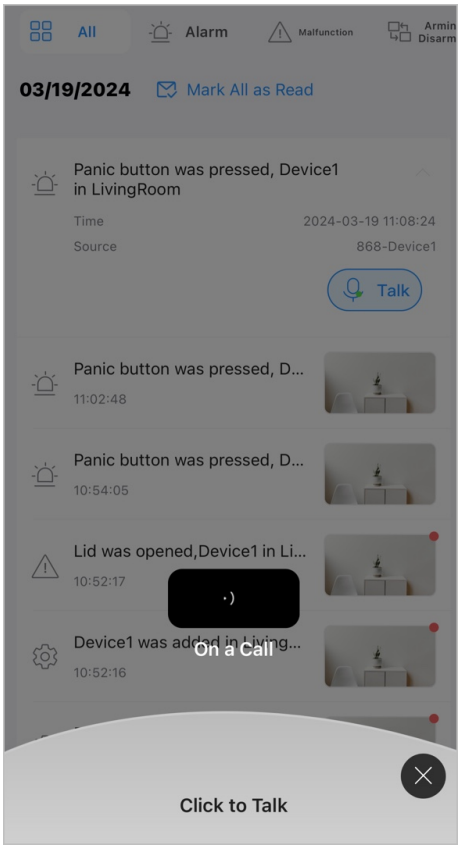
Step 2 Tap an alarm message reported by the siren, and then tap **Talk** to initiate the intercom session.

Figure 8-1 Intercom commissioning



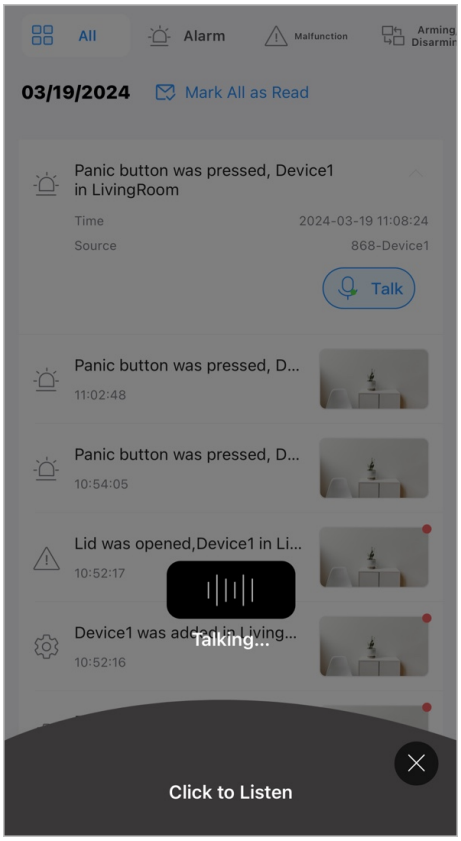
Step 3 Tap **Click to Talk** to start talking to siren.

Figure 8-2 Call



Step 4 (Optional) Tap **Click to Listen** to listen the talking from siren.

Figure 8-3 Talking



8.2 SIP Intercom

You need to configure the intercom services on the hub, and then enable **Intercom Service** on the configuration screen of the siren.

On the **Hub** screen, select **Hub Setting** > **Intercom Service**, and enable **Intercom Service**.

Table 8-2 Intercom setting

Parameter	Description
Intercom Time Limit	When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again. The duration of every intercom session cannot be over 20 minutes.

Parameter	Description
Intercom	SIP Intercom: Intercom between the siren and third party platform. ● Select the siren for intercom. Selection filtered by siren and area are both supported. ● SIP Server Config： ◇ Username/Password: Subject to configuration in third-party platform. ◇ SIP Server Address: Enter the IP address of the third party platform. ◇ SIP Server Port/Local Port: Be consistent with port number of third party platform. ◇ Registration Status: Displays the status for whether the SIP is configured or not.

Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188