Wireless Siren

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.0.1

Foreword

General

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

Model

DHI-ARA12-W2 (868); DHI-ARA12-W2

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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.0.1	Revised arm indication description.	June 2023
V2.0.0	Added a note that the tool is required for removing the back cover of the siren.	August 2022
V1.1.0	● Added technical specifications. ● Updated descriptions of parameters. ● Updated images.	January 2022
V1.0.0	First release.	January 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the siren, hazard prevention, and prevention of property damage. Read carefully before using the siren, and comply with the guidelines when using it.

Operation Requirements

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Installation Requirements

⚠ WARNING

- Connect the PIR to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the PIR.
- Do not connect the PIR to more than one power supply. Otherwise, the PIR might become damaged.

⚠

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the PIR to direct sunlight or heat sources.
- Do not install the PIR in humid, dusty or smoky places.
- Install the PIR in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

1 Introduction

1.1 Overview

Wireless siren is an indoor siren that loudly alarms when an alarm event occurs. It features danger warning and intrusion determent.

1.2 Technical Specifications

This section contains technical specifications of the siren. Please refer to the ones that correspond with your model.

Table 1-1 Technical specifications

Type	Parameter	Description	
Port	Indicator Light	1 × green alarm indicator	
	Button	1 × power button	
Function	Tamper Alarm	Yes	
	Remote Update	Cloud update	
	Search	Signal strength detection	
	Low Battery Alarm	Yes	
Wireless Parameters	Carrier Frequency	DHI-ARA12-W2 (868): 868.0 MHz–868.6 MHz	DHI-ARA12-W2: 433.1 MHz–434.6 MHz
	Transmission Power	DHI-ARA12W2 (868): Limit 25 mW	DHI-ARA12-W2: Limit 10 mW
	Communication Distance	DHI-ARA12W2 (868): Up to 1,000 m (3,280.84 ft) in an open space	DHI-ARA12W2: Up to 800 m (2,624.67 ft) in an open space
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
Temperature	Measuring Range	Indoor: –15 °C to +65 °C (+18.8 °F to +149 °F) Certified temperature:–10°C to +40°C (+14°F to +104 °F)	
	Measuring Precision	± 1 °C (± 33.8 °F)	
	Resolution	1 °C (33.8 °F)	
Technical Parameter	Test Mode	Yes	

Type	Parameter	Description
	Sound Pressure Certified	Volume high 84 db (A)1 m Volume medium 78 db (A)1 m
	Certified Sound	Volume control medium and volume control high
Audio and Video	Volume Control	3 volume levels
General	Power Supply	2 × CR123A batteries
	Battery Voltage	3 VDC
	Min. Voltage	2.5 VDC
	Battery Low Threshold	2.7 VDC
	Battery Restore Threshold	2.75 VDC
	Typical Voltage	3 VDC
	Low Voltage Value	2.7 VDC
	Consumption	Quiescent current 9 uA Max. current 100 mA
	PS Type	Type C
	Battery Life	2.5 years in working status (triggered twice every week and alerts 120 s for each triggering)
	Power Consumption	DHI-ARA12W2 (868): Max. 240 mW DHI-ARA12-W2: Max. 230 mW
	Operating Environment	Indoor: –10 °C to +55 °C (+14 °F to +131 °F) Certified temperature:–10°C to +40°C (+14°F to +104 °F)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	81.0 mm × 81.0 mm × 26.0 mm (3.19" × 3.19" × 1.02")
	Packaging Dimensions	135.0 mm × 98.5 mm × 56.8 mm (5.31" × 3.88" × 2.24")
	Installation	Bracket mount
	Net Weight	105 g (0.23 lb)
	Gross Weight	175 g (0.39 lb)
	Casing	PC + ABS

Type	Parameter	Description
Certifications	DHI-ARA12W2 (868): EN 50131-1: 2006+A2:2017 + A3:2020 EN50131-4:2019 EN50131-6:2017 EN50131-5-3:2017 Security Grade 2 Environmental Class II CE	DHI-ARA12-W2: CE FCC

2 Checklist

Figure 2-1 Checklist

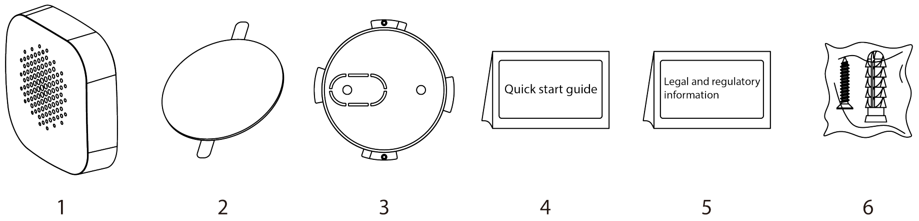


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Siren	1	4	Quick start guide	1
2	Double-sided tape	1	5	Legal and regulatory information	1
3	Back cover	1	6	Screw package	1

3 Design

3.1 Appearance

Figure 3-1 Appearance

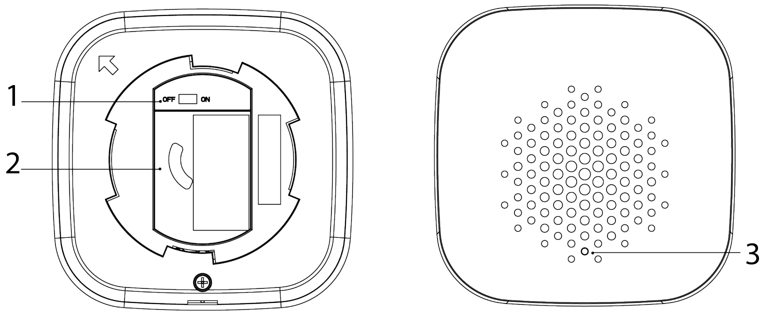
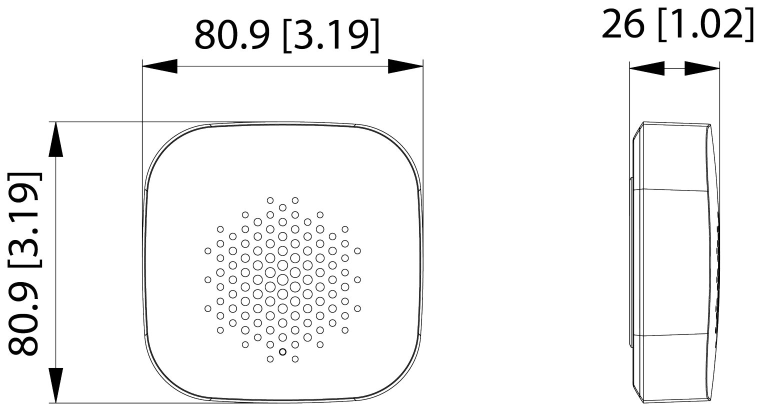


Table 3-1 Structure

No.	Name	Description
1	On/Off switch	Turn on or turn off the switch.
2	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
3	Indicator	● Flashes green quickly: Pairing mode or reduced sensitivity mode. ● Flashes green every second: Alarm event was triggered. ● Solid green for 2 seconds: Pairing successful. ● Slowly flashes green for 3 seconds: Pairing failed. ● Flashes green every 3 seconds: Arming mode.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])



4 Adding the Siren to the Hub

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

Prerequisites

- Make sure that the version of the DMSS app is 1.91or later, and the hub is V1.001.0000000.0.R. 210303 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**.

5 Installation

Prerequisites

Before installation, add the siren to the hub and check the signal strength of the installation location. We recommend installing the siren in a place with a signal strength of at least 2 bars.

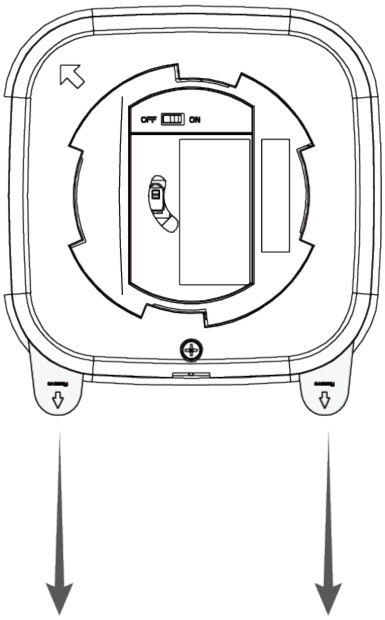
Background Information

The siren supports wall mount.

Procedure

Step 1 Remove the insulation papers on the siren.

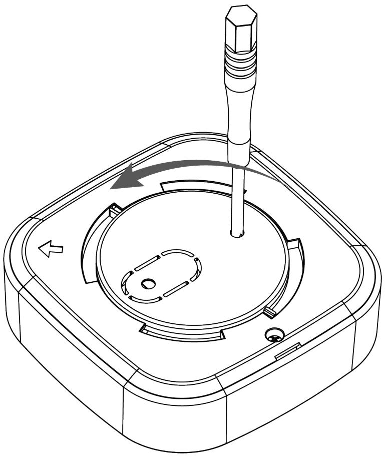
Figure 5-1 Remove the insulating papers



Step 2 If you attached the back cover to the siren too tightly before embedding it in the wall mount, you need to use the screwdriver to remove the back cover first.

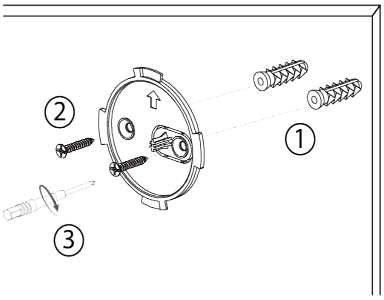
- The siren must not be attached too tightly to the back cover.
- Make sure to use the tool when removing the back cover.

Figure 5-2 Use the screwdriver to remove the back cover



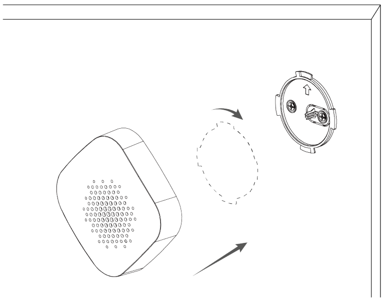
Step 3 Drill 2 holes into the wall according to the hole positions of the siren, and then put the expansion bolts into the holes.

Figure 5-3 Drill holes



Step 4 Attach the siren to the back cover.

Figure 5-4 Attach the siren to the back cover



6 Configuration

You can view and edit general information of the siren.

6.1 Viewing Status

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

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the siren are enabled or disabled. ● ⊙: Enable. ● ⊙: Only disable tamper alarm. ● ⊘: Disable. The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the siren is V1.000.0000001.0.R.20211216 or later.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the siren. ● 📶: Low. ● 📶: Weak. ● 📶: Good. ● 📶: Excellent. ● 📶: No.

Parameter	Value
Battery Level	The battery level of the siren. ● 🟦: Fully charged. ● 🟩: Sufficient. ● 🟨: Moderate. ● 🟧: Insufficient. ● 🟥: Low.
Anti-tampering Status	The tamper mode of the peripheral, which reacts to the detachment of the body.
Online Status	Online and offline status of the siren. ● 🔗: Online. ● ⊘: Offline.
Volume	Alarm volume level.
Alarm Duration	Duration of the alarm sound.
Arm Indication	If enabled, the siren warns about the alarm event by the indicator and sound signal.
Enter/Exit Arming and Disarming Ringtone	The ringtone when entering or exiting arming mode.
Relay Status	The status of whether the siren forwards peripheral messages to the hub through the repeater. 📖 The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.6.R.211215 or later, and the siren is V1.000.0000001.0.R.20211216 or later.
Program Version	The program version of the siren.

6.2 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 6-2 Parameter description of siren

Parameter	Description
Device Configuration	● View siren name, type, SN and device model. ● Edit siren name, and then tap **Save** to save configuration.

Parameter	Description
Area	View the existing area. Add the area that you want to arm, and then tap **Save** to save configuration.
Temporary Deactivate	● Tap **Enable** , and then the function of the 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 function of the siren will be disabled.
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. ● The function is only available when the version of the DMSS app is 1.96 or later, the hub is V1.001.0000000.4.R. 211014 or later, and the siren is V1.000.0000001.0.R. 20210818 or later.
Control Permissions	Select the area over which the siren has control permissions.
Sound Settings	● Configure volume level of the alarm sound. You can select from low, medium, and high. ● Enable **Enter/Exit Arming and Disarming Ringtone** to enable the function of beep during arming and disarming, and enter and exit delay. ● Configure alarm sound. You can select from sound 1, sound 2 and sound 3. Sound 1 is set by default. 📖 The **Alarm Sound** is only available when the version of the DMSS app is 1.97 or later, the hub is V1.001.0000000.6.R. 211228 or later, and the siren is V1.000.0000001.0.R.20211216 or later.
Alarm Duration	● Configure the duration of the alarm sound. ● Select from 3 s to 120 s.
Arm Indication	If enabled, the siren flashes green every three seconds, indicating that the area is armed now.
Signal Strength Detection	Check the current signal strength.
Speaker Test	Tap **Start Detection** to test the volume level of the alarm.

Parameter	Description
Transmit Power	● Select from high, low, and automatic. ● The higher the transmission power, the farther the signal can travel, but the greater the power consumption. 📖 ● If you select **Low**, and then the siren will enter reduced sensitivity mode until you select another option. ● The reduced sensitivity mode is only available when the version of the DMSS app is 1.97 or later, the hub is V1.001.0000000.6.R.211228 or later, and the siren is V1.000.0000001.0.R.20211216 or later.
Cloud Update	Update online.
Delete	Delete the siren. 📖 You can also go to the hub screen, select a siren from the list, and then swipe left to delete it.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.
2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.
2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.
4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.
5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER 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