Alarm Repeater

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.5.0

Foreword

General

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

reference.

Model

DHI-ARA43-W2 (868); DHI-ARA43-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
V1.5.0	Added a procedure to insert the wire into the wire fixing clamp clip.	August 2022
V1.4.0	• Updated technical specifications to meet EN certification standards. • Added a note that the repeater does not support transmitting images from PIR–Camera to the hub. • Updated images of the installation process.	June 2022
V1.3.0	• Added technical specifications. • Updated description of the structure.	February 2022
V1.2.0	Added the hub version.	December 2021

Version	Revision Content	Release Time
V1.1.0	Added app and hub versions.	September 2021
V1.0.0	First release.	August 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 repeater, hazard prevention, and prevention of property damage. Read carefully before using the repeater, 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

- 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

- 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

Alarm repeater is a wireless repeater device that extends the communication range between the alarm hub and other accessories, and forwards messages received from the accessory to the hub. It provides a secondary communication path for accessories, improving the overall stability and reliability of communication of the wireless security system. You can use the DMSS app to manually select a path for accessories or allow the system to automatically select one for them. It is suitable for security use in scenes, such as villas with multiple floors, garages that are far away from residential areas, or office buildings and shops with partitions.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description	
Input / Output	Wireless Zone	32 × wireless peripherals The repeater does not support transmitting images from the PIR–Camera to the hub.	
Port	Storage Battery	Built-in lithium battery	
	Indicator Light	1 that indicates pairing and working	
	Power Switch	1 × power switch	
Function	Tamper Alarm	Yes	
	Remote Update	Cloud update	
	Power Failure Protection for Configured Parameters	Yes	
	Disconnection Detection of External Power Supply	Yes	
	Low Battery Alarm	Yes	
	Search	Signal strength detection	
Wireless	Carrier Frequency	DHI-ARA43-W2 (868): 868.0 MHz–868.6 MHz	DHI-ARA43-W2: 433.1 MHz–434.6 MHz

Type	Parameter	Description	
	Communication Distance	DHI-ARA43-W2 (868): Up to 1,600 m (5249.34 ft) in an open space	DHI-ARA43-W2: Up to 1,000 m (3280.84 ft) in an open space
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
Power Supply	PS Type	Type A	
	Main Power	12 VDC, 1.5 A	
	Battery Capacity	2x 3.6 V/2200 mAh	
	Battery Standby	Battery standby time: Up to 35 h	
	Battery Type	• Battery type: Built-in rechargeable Lithium-ion polymer. • Battery model: 18650	
	Max. current available	0.25 A	
	Power Consumption	Max 3.5 W	
	Current Consumption	• Max 0.25A • Normal 0.05A	
	Low Battery Threshold	3.6 VDC	
	Battery Restore Threshold	3.7 VDC	
	Release Voltage	＜ 3.35.8 V	
	Battery Recharge Time	80% approx. 15 h	
General	Operating Temperature	–10 °C to +55 °C (+14 °F to +131 °F) (indoor)	
	Operating Humidity	10%–90% (RH)	
	Product Dimensions	163.0 mm × 163.0 mm × 32.0 mm (6.42" × 6.42" × 1.26")	
	Packaging Dimensions	219.0 mm × 187.0 mm × 91.0 mm (8.62" × 7.36" × 3.58")	
	Installation	Wall mount; desktop	
	Net Weight	0.32 kg (0.71 lb)	
	Gross Weight	0.74 kg (1.63 lb)	
	Casing	PC + ABS	

Type	Parameter	Description	
	Certifications	EN 50131-1:2006+A2:2017+A3:2020 • EN 50131-3:2009 • EN 50131-6:2017 • EN 50131-5-3:2017 • EN 50131-10:2014 • EN 50136-2:2013 • Security Grade 2 • Environmental Class II • CE	• CE • FCC

2 Checklist

Figure 2-1 Checklist

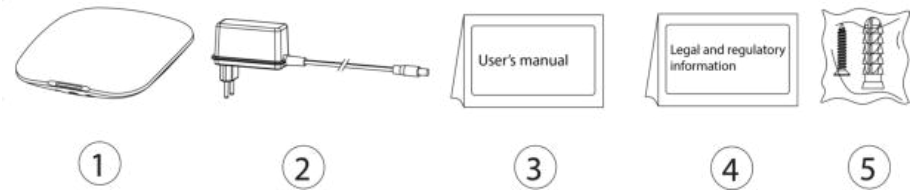


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Alarm repeater	1	4	Legal and regulatory information	1
2	Adapter	1	5	Screw package	1
3	User's manual	1	–	–	–

3 Design

3.1 Appearance

Figure 3-1 Appearance

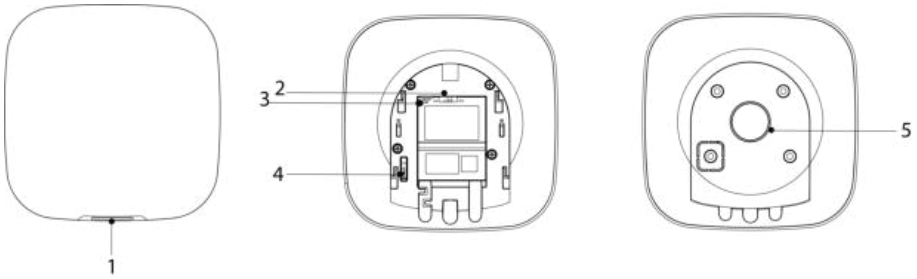
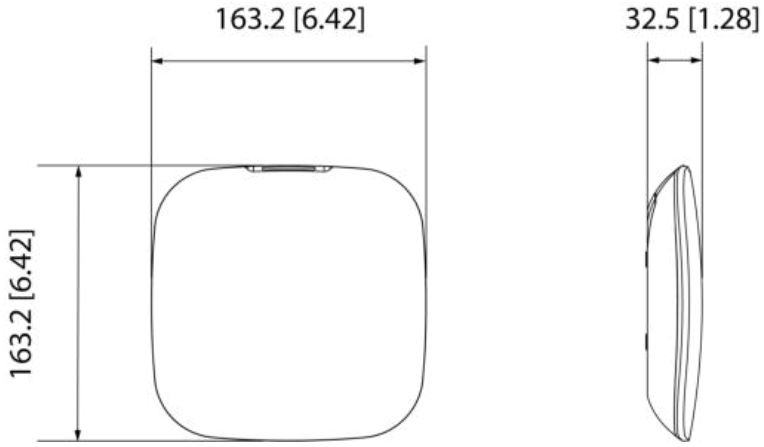


Table 3-1 Structure

No.	Name	Description
1	Indicator	• Solid green: Turned on. • Flashes green: Pairing with the hub.
2	Power switch	Switch to **ON** to turn on the repeater, and **OFF** to turn it off. **OFF** is set by default.
3	Power cable socket	Insert power cable. Powered by 12 VDC power supply.
4	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
5	Back cover	• Back cover closed: Normal status. • Back cover open: If the back cover is opened, the tamper alarm will be triggered.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])



4 Power on

Procedure

Step 1 Loosen the screw to open the repeater.

Figure 4-1 Loosen the screw

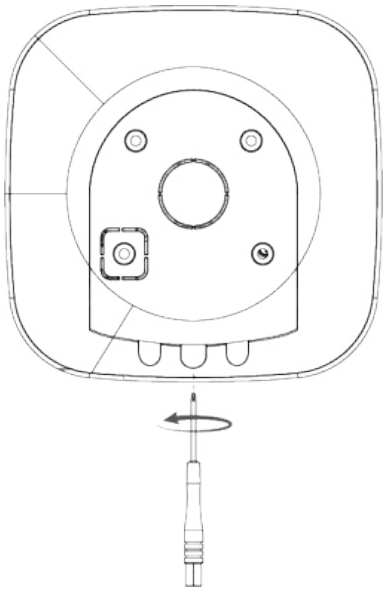
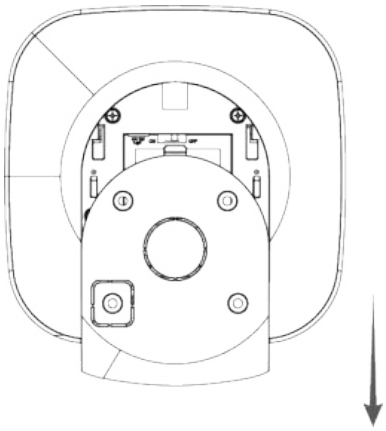
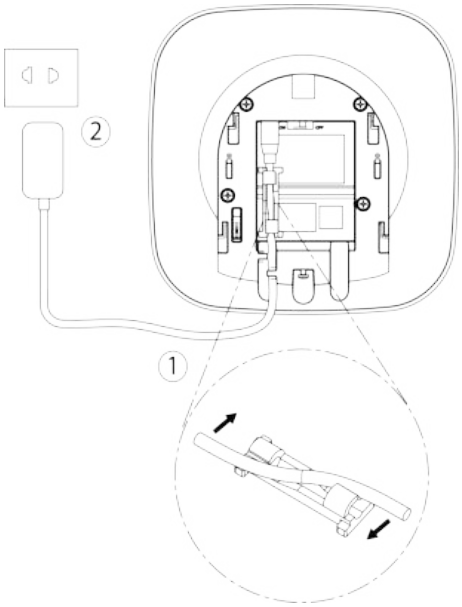


Figure 4-2 Open the repeater



Step 2 Insert the wire into the wire fixing clamp clip and plug it into the repeater to power it on.

Figure 4-3 Power on the repeater



5 Adding the Repeater to the Hub

Before you connect repeater 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 1.94or later, and the hub is V1.001.R.20211215 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 repeater.

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

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

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

Step 5 Wait for the pairing.

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

6 Installation

Prerequisites

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

Background Information

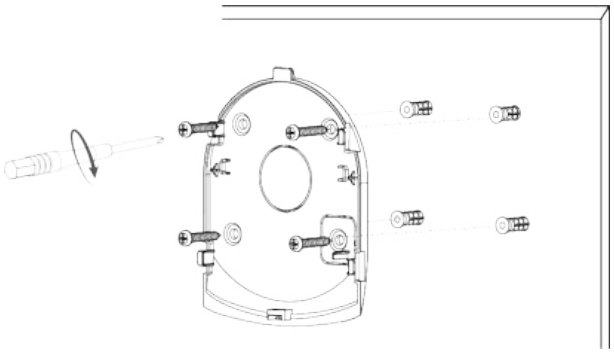
Use the provided screws to mount the repeater in locations accessible for future maintenance.

Mount the repeater in a location that does not have metals and metal objects. Ductwork, wire mesh screens and boxes, and other similar metal based objects will reduce the RF range.

Procedure

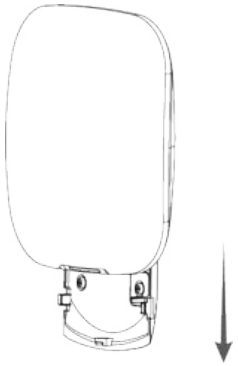
Step 1 Drill four holes into the wall according to the hole positions of the repeater, and then put the expansion bolts into the holes.

Figure 6-1 Drill holes



Step 2 Close the repeater.

Figure 6-2 Close the repeater



Step 3 Secure the repeater with a screw.

Figure 6-3 Secure the repeater

7 Configuration

You can view and edit general information of the repeater.

7.1 Viewing Status

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

Table 7-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the repeater are enabled or disabled. ● : Enable. ● : Only disable tamper alarm. ● : Disable.
Signal Strength	The signal strength between the hub and the repeater. ● : Low. ● : Weak. ● : Good. ● : Excellent. ● : No.
External Power Status	Connection status of the repeater with the power. ● : Connected. ● : Disconnected. If the repeater is powered off, it can work for up to 35 hours.

Parameter	Value
Battery Level	The battery level of the repeater. ● : Fully charged. ● : Sufficient. ● : Moderate. ● : Insufficient. ● : Low. If the battery level is low, the repeater can work for up to 3.5 hours.
Anti-tampering Status	The tamper status of the repeater, which reacts to the detachment of the body.
Online Status	Online and offline status of the repeater. ● : Online. ● : Offline.
Program Version	The program version of the repeater.

7.2 Configuring the Repeater

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

Table 7-2 Parameter description of repeater

Parameter	Description
Device Configuration	● View repeater name, type, SN and device model. ● Edit repeater name, and then tap **Save** to save configuration.
Area	Select the area to which the repeater is assigned.

Parameter	Description
Temporary Deactivate	Tap **Temporary Deactivate** to enable or disable the functions of the repeater. • Tap **Enable** , and then all peripheral messages will be forwarded to the alarm hub. **Enable** is set by default. • Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages. • Tap **Disable**, and then no peripheral messages will be forwarded to the alarm hub through the repeater, and the system will ignore fault messages coming from the repeater.  • If disabled, all the peripherals that were manually set to forward messages through the repeater will be offline. Those selected to automatically send messages to the hub will select another communication path. • Even if you disable the functions of the repeater, the status of the peripherals will be displayed as normal.
LED Indicator	**LED Indicator** is enabled by default. For details on indicator behavior, see "3.1 Appearance".  If LED Indicator is disabled, the LED indicator will remain off regardless of whether the repeater is functioning normally or not.
Peripherals Pairing	Tap **Peripherals Pairing**, and then you can manually set the peripherals to forward messages to the hub through the repeater. • View the status of all the peripherals that are connected to the hub. • In the **To be Paired** list, select a peripheral, and then tap next to the peripheral to manually select a secondary communication path for it. Afterwards, the selected peripheral will be displayed in the **Paired** list.  • The system will automatically select a communication path for the peripherals that were not manually added to the **Paired list** according to the signal strength. Automatic selection for the system is set by default. • If you want the system to automatically select a communication path for the peripheral, you can also go to the **Paired list**, select the peripheral from the list, and then swipe left to delete it.  You can also select > **Peripherals Pairing** to manually set the peripherals to forward messages to the hub through the repeater.

Parameter	Description
Signal Strength Detection	Check the current signal strength.
Transmit Power	• Select from high, low, and automatic. • The higher transmission power levels are, the further transmissions can travel, but power consumption increases.  If you select **Low**, and then the siren will enter reduced sensitivity mode until you select another option.
Cloud Update	Update online. The repeater can forward messages received from the peripheral to the hub even during an online update.  Make sure the hub is disarmed and the repeater is powered up by a 12 VDC power supply.
Delete	Delete the repeater.  If the repeater is deleted, the system will select another communication path for the peripherals that have been manually set to forward messages to the hub through the repeater.  Go to the hub screen, select the repeater from the peripheral 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