



Alarm Repeater Pro

User Manual



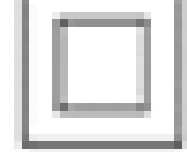
Foreword

General

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

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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.
	Class II equipment

Revision History

Version	Revision Content	Release Time
V1.0.1	Added EN certification descriptions.	May 2026
V1.0.0	First release.	October 2025

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards and Warnings

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

Operation Requirements

**DANGER**

The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- Keep new and used batteries out of reach of children.
- If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
- Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.



- 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**

- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◇ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ Do not connect the power adapter to the device while the adapter is powered on.



- 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.
- Connect class I electrical appliances to a power socket with protective earthing.
- Connect the control panel near an easily accessible socket.
- There will be risk of fire or explosion if the battery is replaced by an incorrect type.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Technical Specifications.....	1
2 Checklist.....	4
3 Design.....	5
3.1 Appearance.....	5
3.2 Dimensions.....	6
4 Installation.....	7
4.1 Installing the Alarm Repeater Pro.....	7
4.2 Adding the Alarm Repeater Pro to the Hub.....	10
5 Configuration.....	12
5.1 Viewing Status.....	12
5.2 Configuring the Alarm Repeater Pro.....	14
Appendix 1 Security Commitment and Recommendation.....	17

1 Introduction

1.1 Overview

The alarm repeater pro extends the distance of wireless communication between peripherals and alarm hub, greatly expanding the coverage of a scene. It also extends the benefits of your security system by allowing more devices to connect to repeaters.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description
Port	Wireless Peripheral	128 wireless peripherals
	Network Mode	Ethernet and Wi-Fi
	Network Port	1 RJ-45, 10 Mbps/100 Mbps Ethernet port
	Storage Battery	One built-in 4,750 mah rechargeable lithium battery
Function	Indicator Light	1 indicator for indicating pairing and working status
	Button	Includes a reset button, power button and AP switch button
	Remote Update	Cloud update
	Low Battery Detection	Yes
	Battery Level Display	Yes
	Tamper	Yes
	Signal Strength	Yes
	Power Failure Protection for Configured Parameters	Yes
	Pairing Mode	Auto/Manual
Technical	Operating Current	220 VAC, 100 mA (max) 220 VAC, 8.6 mA (standby)

Type	Parameter	Description	
Wireless	Carrier Frequency	DHI-ARA46-N-W2(868): Airfly: 865-868.6 MHz RF-HD (normal speed): 865-868 MHz RF-HD (high speed): 2400-2483.5 MHz	DHI-ARA46-N-W2: Airfly: 433.05 - 434.79 MHz RF-HD (normal speed): 433.05 - 434.79 MHz RF-HD (high speed): 2400-2483.5 MHz
	Transmitter Power (EIRP)	Limit 25 mW	Limit 10 mW
	Communication Mechanism	Two-way	
	Communication Distance	DHI-ARA46-N-W2(868): Airfly:2,000 m (6561.68 ft) RF-HD (normal speed):1,600 m (5249.34 ft) RF-HD (high speed): 300 m (984.25 ft)	DHI-ARA46-N-W2: Airfly: 1,600 m (5249.34 ft) RF-HD (normal speed): 1,200 m (3937.01 ft) RF-HD (high speed): 300 m (984.25 ft)
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Power Supply	100–240 VAC, +10% -15%, 50/60 Hz, 0.2 A	
	PS Type	Type A	
	Battery Recharge Time	80% approx. 11 h	
	Battery Restore Threshold	3.7 VDC	
	Battery Low Battery Threshold	3.4 VDC	
	Storage Battery	One built-in 4.750 mah rechargeable lithium battery	
	Standby Time	35 hours (only connected to the Hub through Airfly and normal speed RF-HD) 18 hours (connected to the Hub through Ethernet, Wi-Fi or high speed RF-HD)	
	Power Consumption	22 W (max) 1.9 W (standby)	

Type	Parameter	Description
	Operating Temperature	When battery is not charging: -10 °C to +50 °C (+14 °F to +122 °F) When battery is charging: 0 °C to +45 °C (+32°F to +113 °F)
	Operating Humidity	10%–90% (RH)
	Operating Environment	-10°C +55°C - humidity 95%
	Product Dimensions	174.8 mm × 174.8 mm × 38.3 mm (6.88" × 6.88" × 1.51") (L × W × H)
	Net Weight	510 g (1.12 lb)
	Gross Weight	860 g (1.90 lb)
	Installation	Supports wall mount and desktop mount installation
	Casing Material	PC + ABS
	Certifications	DHI-ARA46-N-W2(868): CE Standards: EN 50131-1:2006+A1:2009+A2:2017+A3:2021 , EN 50131-3:2009, EN 50131-6:2017+A1:2021, EN 50131-5-3:2017, EN50131-10:2014, EN50136-2:2013+A1:2023 Grade 2 Environmental class II
	Storage Temperature	-10 °C to +55 °C (+14 °F to +131 °F)
	Storage Humidity	10%–90% (RH)
	Packaging Dimensions	254 mm × 211 mm × 61 mm (10.00" × 8.31" × 2.40") (L × W × H), standalone in the inner box 524 mm × 508 mm × 442 mm (20.63" × 20.00" × 17.40") (L × W × H), protective case
Wi-Fi	Wi-Fi Standard	IEEE 802.11b/g/n/ax
	Wi-Fi Frequency Range	2400-2483.5 MHz
	Wi-Fi Power Transmission	≤20 dBm@2400-2483.5 MHz

2 Checklist

Figure 2-1 Checklist

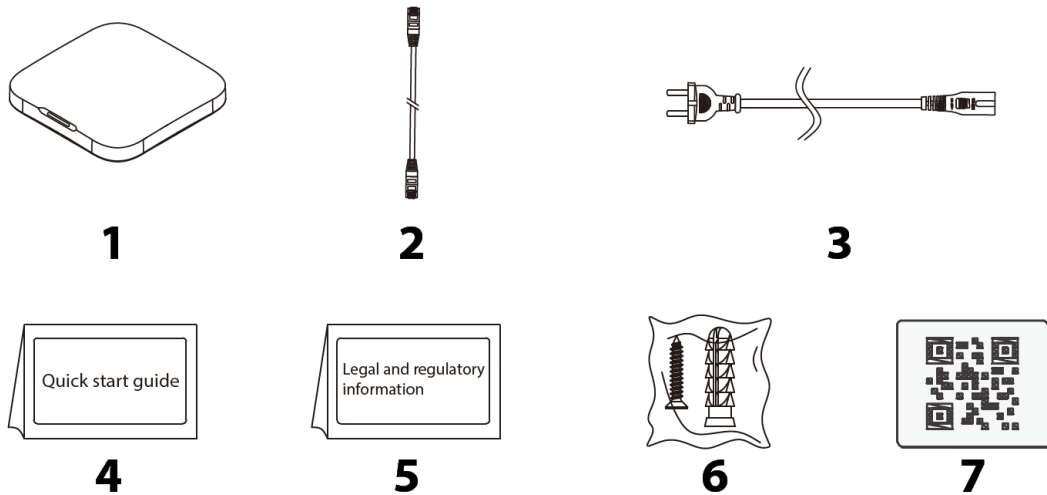


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Alarm repeater pro	1	5	Legal and regulatory information	1
2	Cable	1	6	Package of screws	1
3	Adapter	1	7	QR code	1
4	Quick start guide	1	—	—	—

3 Design

3.1 Appearance

Figure 3-1 Appearance

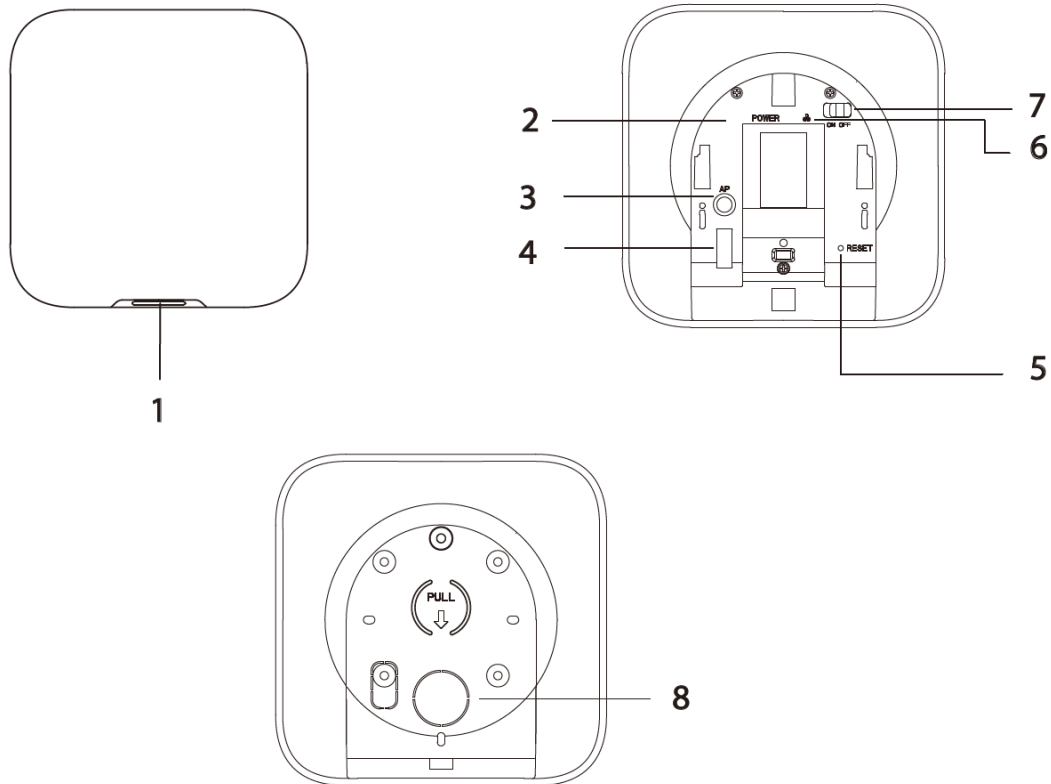


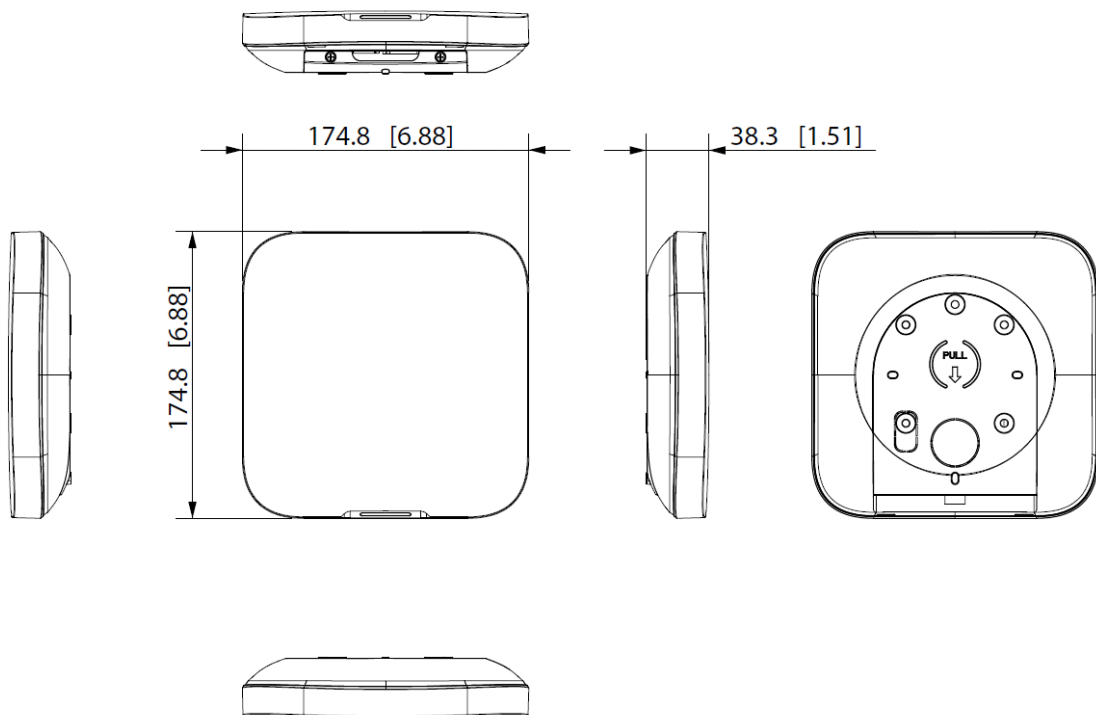
Table 3-1 Structure

No.	Name	Description
1	Indicator	● Solid green: Alarm repeater pro is functioning normally. ● Flashes green: In the pairing mode, the light flashes green. ● Blinks green quickly: Transmission power is set to low, and the light flashes green quicker than that in the pairing mode. ● Solid yellow: Alarm repeater pro is offline. ● Flashes yellow: Alarm repeater pro has a fault, such as tamper detection triggered. ● Flashes blue slowly: Alarm repeater pro is in AP mode; When the repeater is uninitialized and not connected to the hub, it is in the AP mode by default and no indicator is on.
2	Power port	Connects to power supply.

No.	Name	Description
3	AP button	Press and hold the button for 2 seconds to turn on the AP function, and the phone will connect to the hotspot from the hub, and then sync Wi-Fi username and password to the alarm repeater pro. You can also turn off the AP through pressing and holding the button for 2 seconds when AP is enabled.
4	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
5	Reset button	Press and hold the button for 10 seconds to restart the alarm repeater pro and restore to factory default settings.
6	Ethernet cable socket	Connect the hub to the Ethernet.
7	Power switch	Turn on or turn off the alarm repeater pro.
8	Back cover	If the back cover is opened, the tamper alarm will be triggered.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])



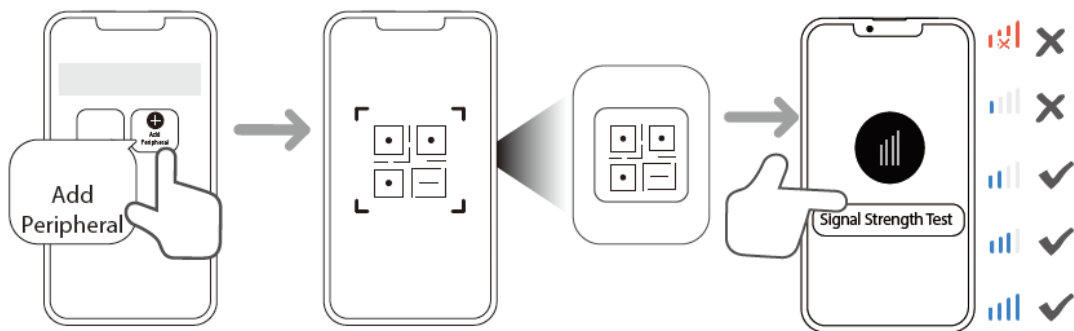
4 Installation

4.1 Installing the Alarm Repeater Pro

Prerequisites

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

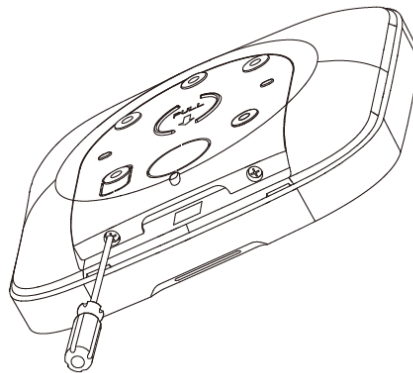
Figure 4-1 Check signal strength



Procedure

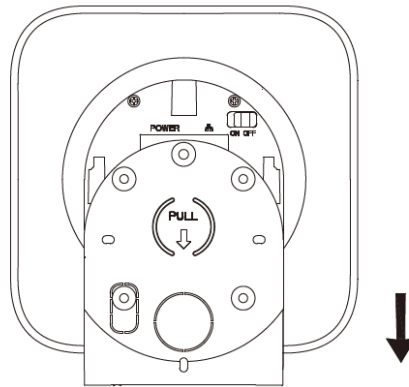
Step 1 Loosen the screw to open the alarm repeater pro.

Figure 4-2 Open the alarm repeater pro



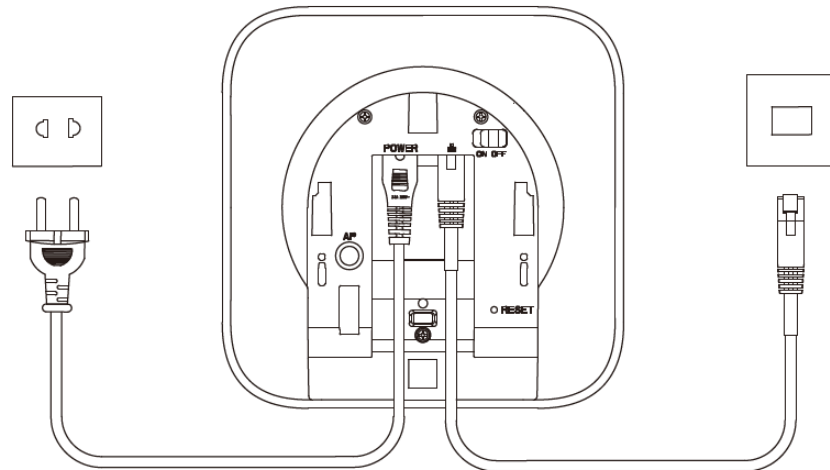
Step 2 Pull down the attachment panel.

Figure 4-3 Pull down attachment panel



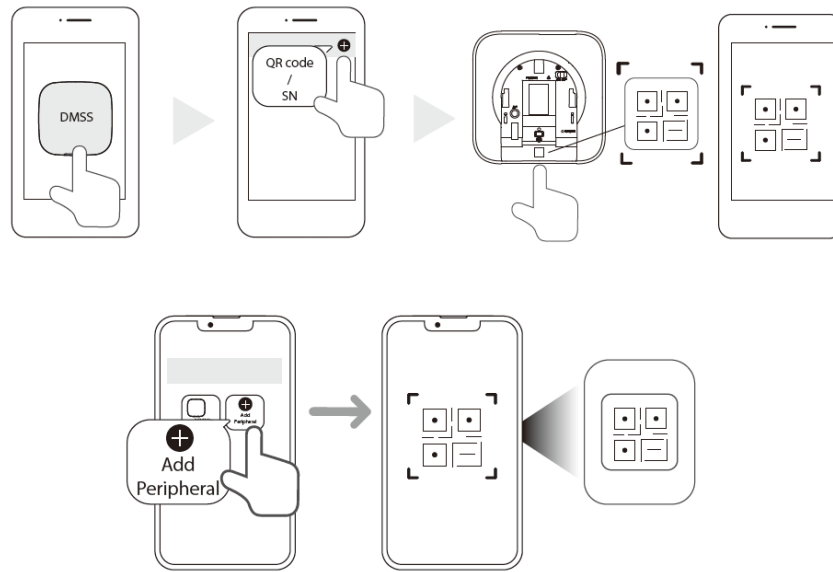
Step 3 Connect the power cable to power on the alarm repeater pro.

Figure 4-4 Power on



Step 4 Add the alarm repeater pro to the hub. For details, see "4.2 Adding the Alarm Repeater Pro to the Hub".

Figure 4-5 Add alarm repeater pro



- Step 5** Confirm the position of the screw holes, and then drill them into the mounting plate. Attach the mounting plate into the wall, and then align the screw holes on the plate with the expansion bolts. Fix the mounting plate with ST4 × 25 mm self-tapping screws.

Figure 4-6 Drill holes

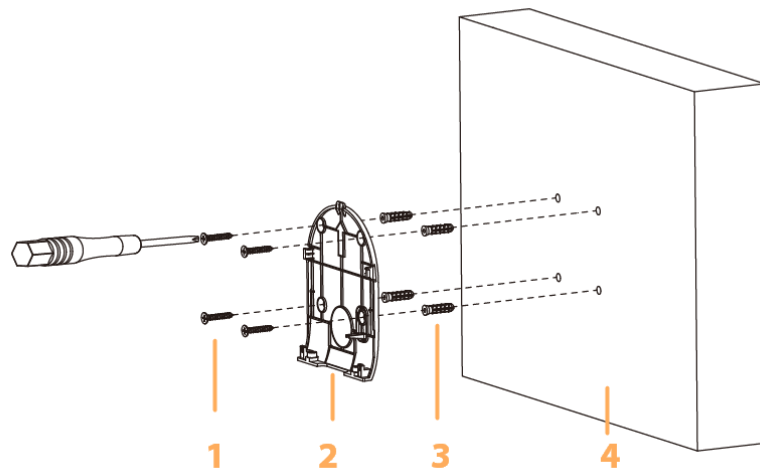
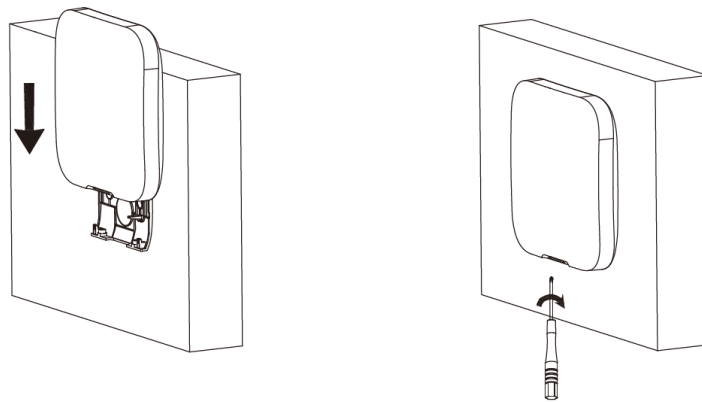


Table 4-1 Installation items

No.	Item Name	No.	Item Name
1	ST4 × 25 mm self-tapping screw	3	Expansion bolt
2	Mounting plate	4	Wall

- Step 6** Put the alarm repeater pro into the mounting plate from top to bottom. Fix the alarm repeater pro and mounting plate with M3 × 8 mm countersunk head screws.

Figure 4-7 Fix the alarm repeater pro



4.2 Adding the Alarm Repeater Pro to the Hub

Before you connect alarm repeater pro to the hub, install the DMSS or DoLynk Care app to your phone. This manual uses iOS as an example.



- Make sure that you have already created an account, and added the hub to DMSS or DoLynk Care.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.
- Make sure that you have performed signal strength test and the alarm repeater pro is installed at a place where it has at least 2 bars of signal.

Adding Through AirFly Mode

You can add the alarm repeater pro to the hub through AirFly mode.

1. Go to the **Devices** screen of the hub, and then select  > **Add Peripheral**.
2. Scan the QR code at the bottom of the alarm repeater pro, and then tap **Next**.
3. Tap **Next** after the alarm repeater pro has been found.
4. Configure the device name for the alarm repeater pro, assign the area for it, and then tap **Next**.
5. Follow the on-screen instructions to flip the switch on the alarm repeater pro from off to on, and its indicator flashes green, and then tap **Next**.
6. Wait for the pairing to finish, and then tap **OK**.

Adding Through Wired Network

You can add the alarm repeater pro to the hub through wired network.

1. Go to the **Devices** screen of the hub, and then select  > **Add Peripheral**.
2. Insert the network cable into the alarm repeater pro. Make sure that the repeater pro and the hub are on the same network. Scan the QR code at the bottom of the alarm repeater pro, and then tap **Next**.

3. Tap ... on the right top corner of the screen, select **Add Through Network**, and then tap **Next**.
4. Wait for the pairing to complete, and then tap **OK**.

Adding Through Wireless Network

You can add the alarm repeater pro to the hub through Wi-Fi.

1. Go to the **Devices** screen of the hub, and then select  > **Add Peripheral**.
2. Scan the QR code at the bottom of the alarm repeater pro, and then tap **Next**.
3. Configure the password and confirm it, and then tap **Next**.
4. Tap **Select Network Config Method**, select **Wi-Fi**.
5. Connect the alarm repeater pro and the hub to the same Wi-Fi hotspot.
6. Wait for the pairing to complete, and then tap **OK**.

5 Configuration

You can view and edit general information of the detector.

5.1 Viewing Status

Detector Icon Description

Introduces the meaning of icons for the alarm repeater pro. You can view these icons on the **Peripheral** list under the hub screen.

Table 5-1 Device icon description

Parameter	Icon	Description
Signal Strength/RF-HD		Low
		Weak
		Good
		Excellent
		No signal
Wi-Fi Signal Strength		Low
		Weak
		Good
		Excellent
		No signal
Battery Level		100%
		80%
		60%
		40%
		20%
Permanent Deactivation		Yes

Parameter	Icon	Description
		Lid only
Bypass		Yes
		Lid only
Tamper		Opened.
Manual Communication Mode for Peripheral		The peripheral is manually added to the alarm repeater pro, and set it as the communication path.

View Detector Status

On the **Devices** screen, select an alarm repeater pro from the peripheral list to go to the **Overview** screen, and then view the status of the alarm repeater pro.

Table 5-2 Status

Parameter	Value
Device No.	Displays the device number of the alarm repeater pro.
Signal Strength	The signal strength between the hub and the alarm repeater pro.
RF-HD	Displays the RF-HD strength between the hub and the alarm repeater pro.
Wi-Fi Signal Strength	Internet connection status of the alarm repeater pro through Wi-Fi. For greater reliability, we recommend installing the alarm repeater pro in places with the signal strength of at least 2 bars.
Wi-Fi	Displays Wi-Fi status of the hub. The types include: - Connected. - Disconnected.
Online Status	Displays online and offline status of the alarm repeater pro.
Battery Level	Displays the remaining battery percentage of the alarm repeater pro.
External Power	- Connected. - Disconnected.
Permanent Deactivation	The status for whether the permanent deactivation of the alarm repeater pro is enabled or turned off. - Yes. The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub. - Lid only. All information, except for tamper alarms will be sent to the alarm hub. - No: The permanent deactivation is turned off. All information will be sent to the alarm hub.

Parameter	Value
Bypass	• Yes: The bypass is enabled. • Lid only: All information, except for tamper alarms will be sent to the alarm hub. • No: All information will be sent to the alarm hub.
Tamper	The tamper status of the alarm repeater pro. The status is triggered when an attempt is made to remove it from its installed position. • Opened. • Closed.
Program Version	The program version of the alarm repeater pro.

5.2 Configuring the Alarm Repeater Pro

On the **Devices** screen, select an alarm repeater pro from the peripheral list to go to the **Settings** screen, and then view the status of the alarm repeater pro.

Table 5-3 Parameter description

Parameter	Description
Device	• View alarm repeater pro name, type, SN and device model. • Edit alarm repeater pro name, and then tap Save to save configuration.
Area	Select the area to which the alarm repeater pro is assigned.
Bypass	• Yes: Bypass is enabled, and information will not be sent to the alarm hub. • Lid only: Tamper only. All information, except for tamper alarms, will be sent to the alarm hub. • No: Bypass is turned off. All information will be sent to the alarm hub.  Bypass will automatically restore after disarming.
Permanent Deactivation	The status for whether the permanent deactivation of the alarm repeater pro is enabled or turned off. • Yes: The permanent deactivation is enabled. Alarm information will not be sent to the alarm hub. • Lid only: All information, except for tamper alarms will be sent to the alarm hub. • No icon appears when the function is configured as No. No means the permanent deactivation is turned off. All information will be sent to the alarm hub.

Parameter	Description
LED Indicator	LED Indicator is enabled by default. Disabling the function will stop the detector from lighting up for alarms, faults, arming, disarming status.  If LED Indicator is disabled, the LED indicator will remain off regardless of whether the alarm repeater pro is functioning normally or not.
Alarm Repeater	- Manual mode: Click + next to the peripheral, and it is manually added to the alarm repeater pro, and select it as the communication path. - Auto mode: The peripherals select the communication path according to the signal strength between the hub and the alarm repeater. For example, if the signal strength of the alarm repeater is better, then the peripheral automatically connects to the alarm repeater pro for communication rather than the hub.
Network	- Ethernet: Configure the IP address, subnet mask, gateway and MAC address of the alarm repeater pro. You can also enable DHCP instead to allow the system automatically assign the information for the alarm repeater pro. Enable Ethernet Failure Detection, and the system detects whether the wire connection between the repeater and the hub is functioning properly. - Wi-Fi: Select the Wi-Fi network from the list, enter the password and tap Add to connect to the Wi-Fi.
Login Info	View the login information of the alarm repeater pro (user name and password). You can modify the password. The user name cannot be edited.
Offline Linkage	- Offline Linkage siren: Enable the function, and when a communication error occurs between the alarm repeater pro and the hub, the alarm signal from the manually connected detector will trigger the siren that is manually added to the repeater. - Offline Linkage scene: Enable the function, and you can select up to 8 alarm linkage scenarios. When the scene is selected, it will remain available even when the hub 2 is offline.
AirFly Error Detection	Enable the function, and the system automatically detects whether the AirFly communication between the repeater and the hub is functioning properly.

Parameter	Description
RF-HD Transmission Speed	Configure the RF-HD transmission rate between the alarm repeater pro and the hub. ● High Speed : Faster data transmission but limited range. It cannot be enabled when the alarm repeater pro is connected to Wi-Fi. ● Normal : Default. With strong wall penetration but slower transmission speed.
RF-HD Test	Tap Start Inspection to check the RF-HD signal strength of the alarm repeater pro and whether the alarm repeater pro has successfully connected to the hub. It helps you to find a location with strong signal to install the alarm repeater pro.
Signal Strength Detection	Test the current signal strength to select an area with great signal to install the alarm repeater pro.
Detector Test	Detect whether the peripheral works.
Transmit Power	● Select from high, low, and automatic. ● The higher the transmission power, the further the signal can travel, but the greater the power consumption.  If you select Low, and then the alarm repeater pro will enter reduced sensitivity mode until you select another option.
Auto Download	Enable the function, and the update package will be automatically downloaded when a new version becomes available.
Firmware Update	Tap to view the current firmware version of the alarm repeater pro. If it is not the latest version, you can update it to the latest.
User's Manual	Tap to view the user manual of the alarm repeater pro.

Appendix 1 Security Commitment and Recommendation

Zhejiang 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 Allowlist

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

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;
- Establish 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 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