Wireless Multi IO Transmitter

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.1

Foreword

General

This manual introduces the installation, functions and operations of the Wireless Multi IO Transmitter (hereinafter referred to as the "transmitter"). 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
V1.0.1	● Updated the technical specification. ● Added notes for installation.	November 2024
V1.0.0	First release.	September 2024

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 wireless multi IO transmitter, hazard protection, and protection of property damage. Read carefully before using the wireless multi IO transmitter, 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.

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.

⚠

- 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.

Table of Contents

1 Introduction

1.1 Overview

The multi IO transmitter is an integration module for connecting third-party wired detectors and devices to the wireless alarm system. It has 16 wired zones for connecting NC, NO, EOL, 2EOL, and 3EOL devices. It can also support up to 4 outputs and 2 auxiliary power outputs, providing a total power supply of 14.5V/2A.

1.2 Technical Specifications

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

Table 1-1 Technical specification

Type	Parameter	Description	
Port	Alarm Input	Supports local 16-channel alarm input, 1 to 6 channels support pulse detection, and 1 to 16 channels support 0EOL/EOL/2EOL/3EOL	
	Alarm Output	Supports 4 lcoal channels(Max 30 VDC, 3A)	
	Network Mode	Ethernet	
	Network Port	1 × RJ-45 10/100 Mbps Ethernet port; PoE power supply	
Function	Indicator Light	One indicator (indicator status)	
	Button	1 × switch button, 1 × reset button	
	Remote Update	Supports cloud update	
	Tamper	Yes	
Technical	LED Indicator	1 × indicator	
	Scenario	Indoors	
Wireless	Carrier Frequency	DHI-ARM9A4-P-W2(868) :868 MHz	DHI-ARM9A4-P-W2: 433 MHz
	Transmitter Power (EIRP)	DHI-ARM9A4-P-W2(868): limit 25 mW	DHI-ARM9A4-P-W2: limit 10 mW

Type	Parameter	Description	
	Communication Mechanism	Two-way	
	Communication Distance	DHI-ARM9A4-P-W2(868) RF: Up to 1,600 m (5249.34 ft) in an open space	DHI-ARM9A4-P-W2: RF: Up to 1,200 m (3937.0 ft) in an open space
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Power Supply	100-240 VAC, PoE (802.3at)	
	Power Supply Type	Type A	
	Standby Time	Static standby: Up to 30 hrs	
	Power Consumption	220 VAC quiescent current (40 mA Irms) 220 VAC max current@2A load + charge (315 mA Irms) POE quiescent current (125mA) POE max current@0.75A load + charge (612 mA)	
	Operating Temperature	−10 °C to +50 °C (+14 °F to +122 °F)	
	Operating Humidity	10%–90%	
	Product Dimensions	304 mm × 235 mm × 90.8 mm (11.97" × 9.25" × 3.57")	
	Net Weight	1.22 kg (2.69 lb)	
	Gross Weight	1.78 kg (3.92 lb)	
	Installation	Wall mount	
	Casing Material	PC + ABS	
	Appearance	White	
	Protection	IP30	
	Anti-corrosion Level	Basic protection	
	Certifications	CE	
	Storage Temperature	−10 °C to +55 °C (+14 °F to +131 °F)	

Type	Parameter	Description
	Storage Humidity	10%–90%
	Packaging Dimensions	Standalone packaging: 269 mm × 140 mm × 280 mm (10.59" × 0.55" × 11.02") (L × W × H) Protective case packaging: 585 mm × 443 mm × 399 mm (23.03" × 17.44" × 15.71") (L × W × H)

2 Checklist

Figure 2-1 Checklist

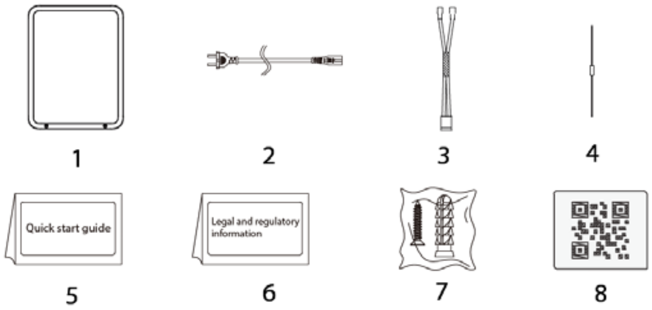


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless multi IO transmitter	1	5	Quick start guide	1
2	Power cable	1	6	Legal and regulatory information	1
3	Battery cable	2	7	Package of screws	1
4	2.2k resistance 6.8k resistance	40 for each	8	QR code	1

3 Design

3.1 Appearance

Figure 3-1 Appearance

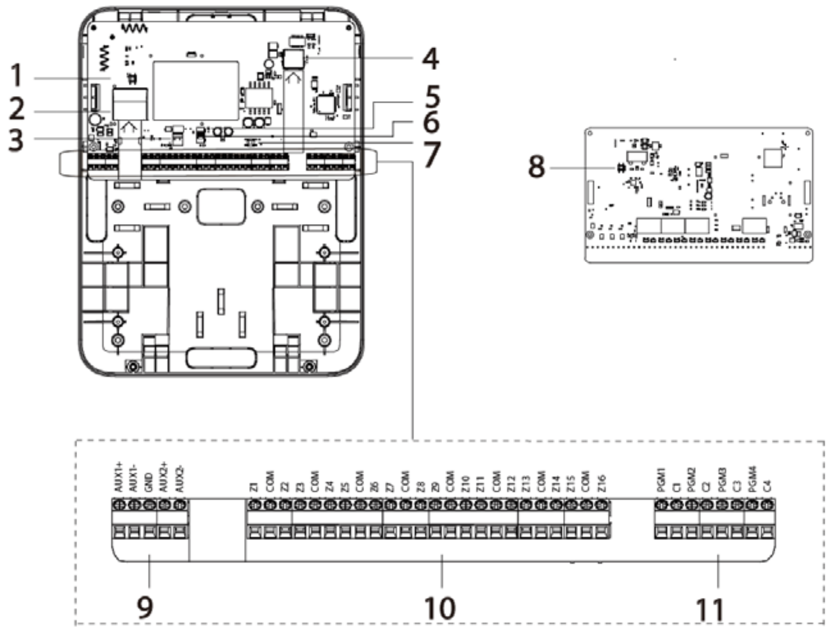


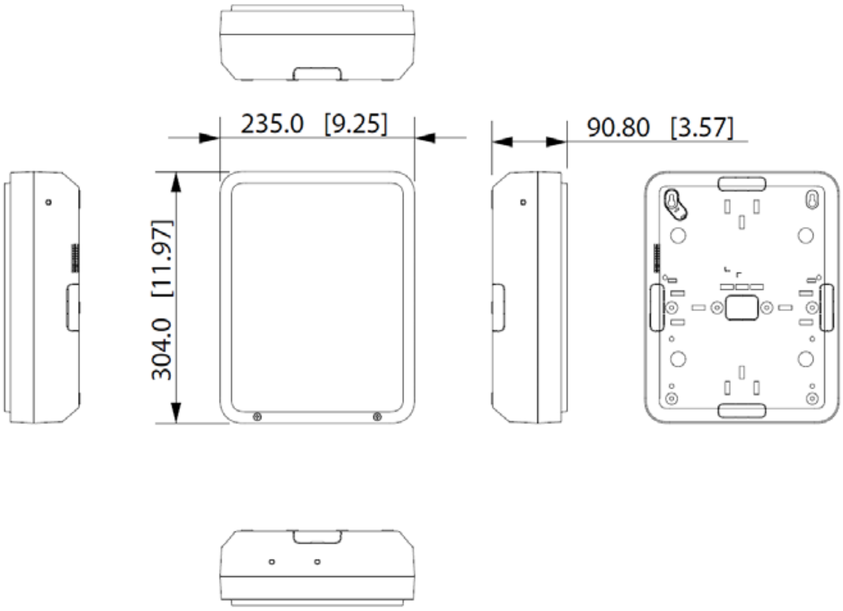
Table 3-1 Structure

No.	Name	Description
1	Case tamper switch	Used to detect any attempts to tamper with or open the case of the transmitter.
2	220 VAC power outlet	Used to power the transmitter.
3	Storage battery terminal	Used to connect the storage battery to the transmitter.
4	Network port (supported on selected models)	Used for the device to send and receive data over a network.
5	LED light	Used as indicator for the transmitter.
6	Power switch	Used to turn on or off the power supply.
7	Reset button (supported on selected models)	Used to restore the transmitter to factory settings.
8	Wall tamper switch	Used to detect any attempts to tamper with or manipulate the transmitter.
9	Auxiliary power output terminal	Used to connect the additional power source for the transmitter.

No.	Name	Description
10	Input terminal	Used to receive input signals or data from various sources and transmit it to the transmitter
11	Output terminal	Used to send output signal of the transmitter to another device.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])

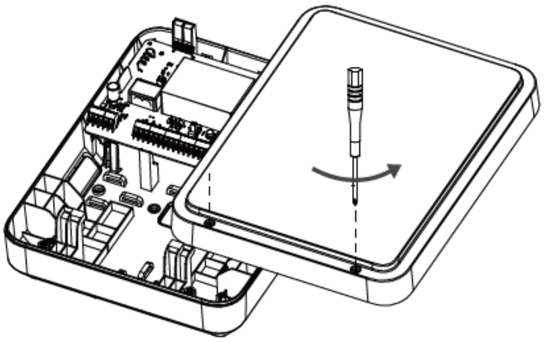


4 Power On

Procedure

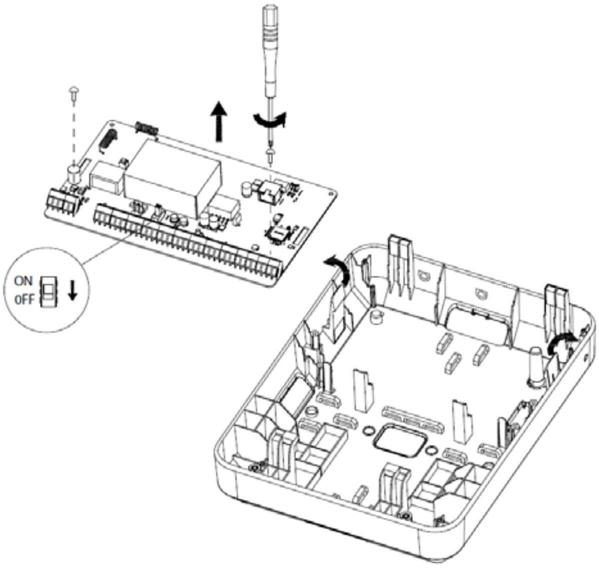
Step 1 Loosen the two screws on the front panel and open it.

Figure 4-1 Remove the front panel



Step 2 Open the buckle and remove the 2 screws on the main board.

Figure 4-2 Main board



5 Installation

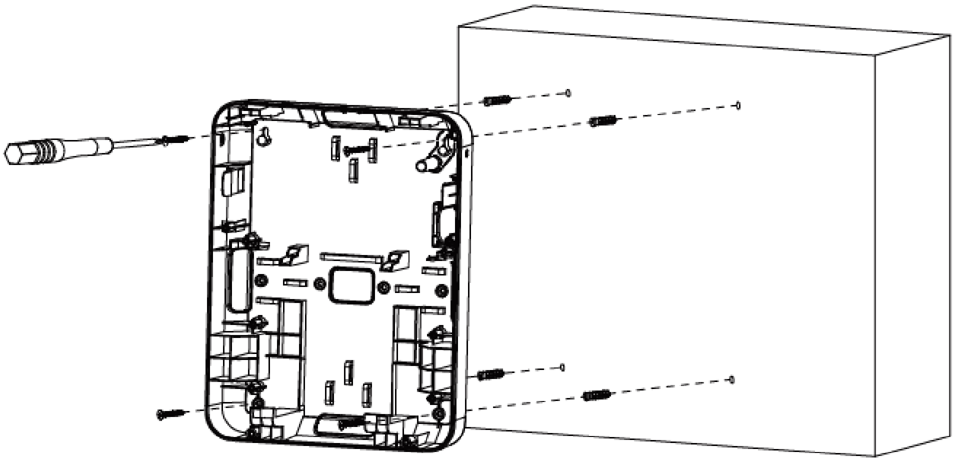
Procedure

Step 1 Use the attached screws to install the rear panel onto the wall.

⚠

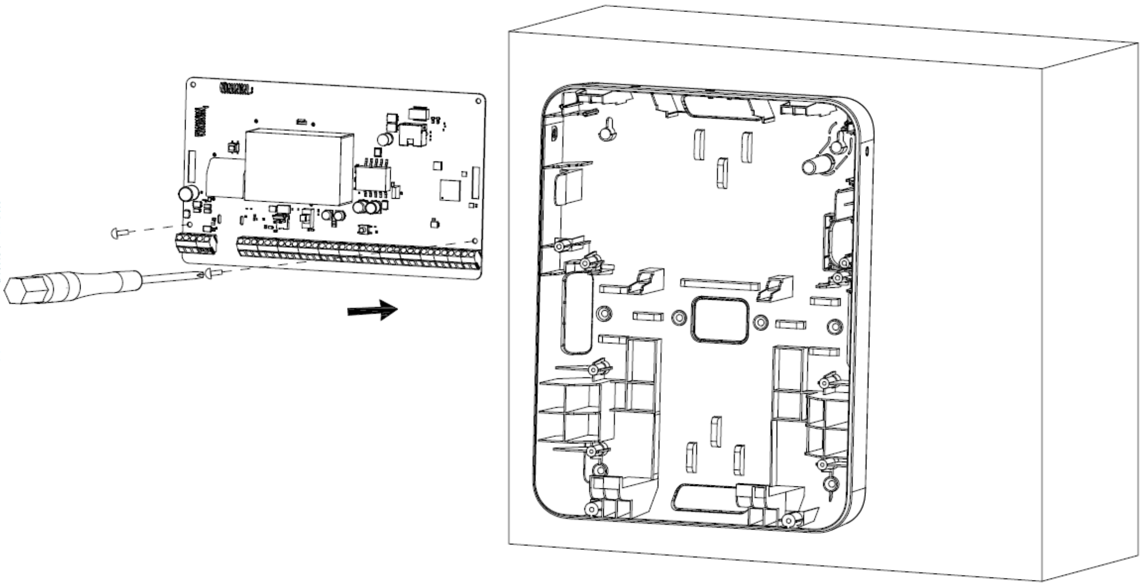
Installation of knock-out holes must be connected to a closed fireproof chamber.

Figure 5-1 Install(1)



Step 2 Install the main board on to the rear panel.

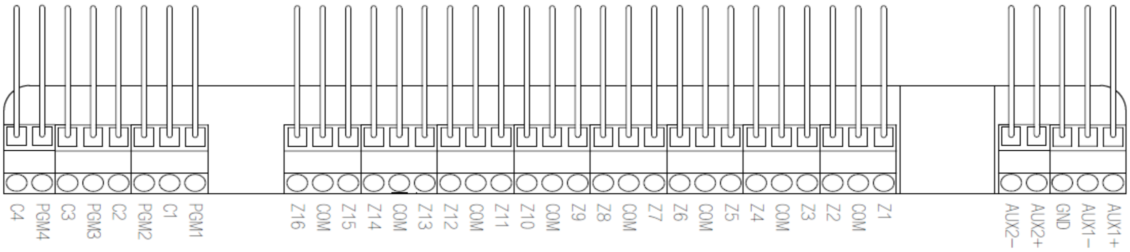
Figure 5-2 Install (2)



Step 3 Complete wiring.

For details, see "6 Wiring".

Figure 5-3 Wiring diagram

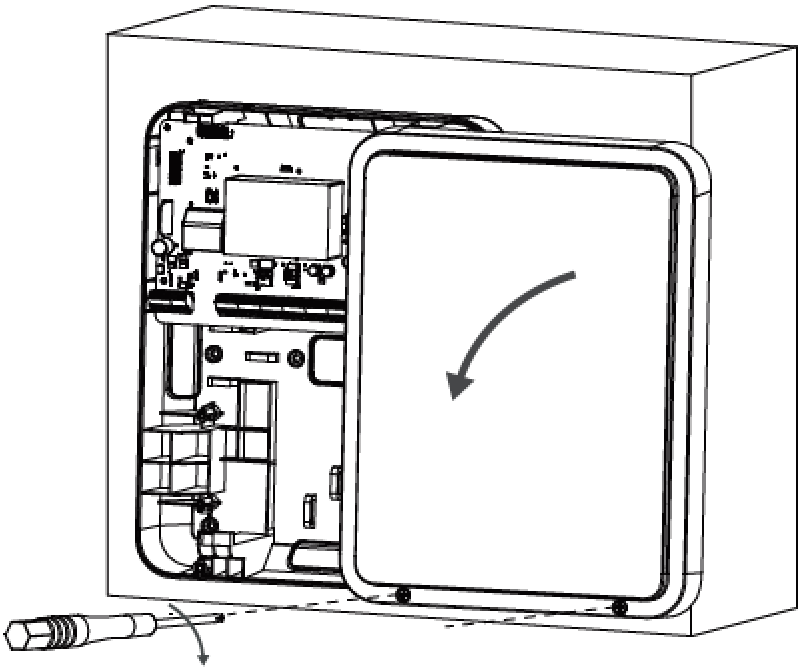


Step 4 Add the transmitter to the alarm hub.

For details, see "7 Adding the Transmitter to the Hub".

Step 5 Install the front panel in to the transmitter and tighten the screws.

Figure 5-4 Install (3)

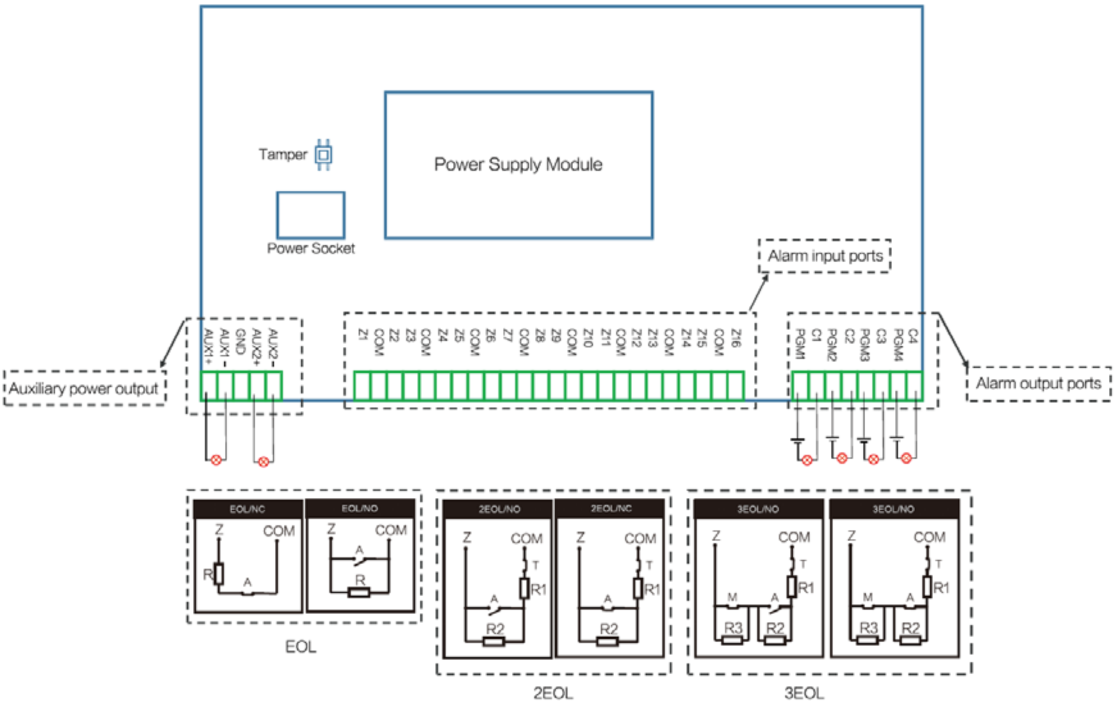


6 Wiring

6.1 Local Alarm Input Cable Connection

The module has 16 local alarm inputs, the corresponding ports are Z1 to Z16. 0EOL,1 EOL, 2 EOL and 3 EOL are available for detectors that are NO and NC. Set the transmitter to 1 EOL when the detector tamper alarm is not required, 2 EOL for tamper alarm and 3 EOL for both tamper and mask alarms.

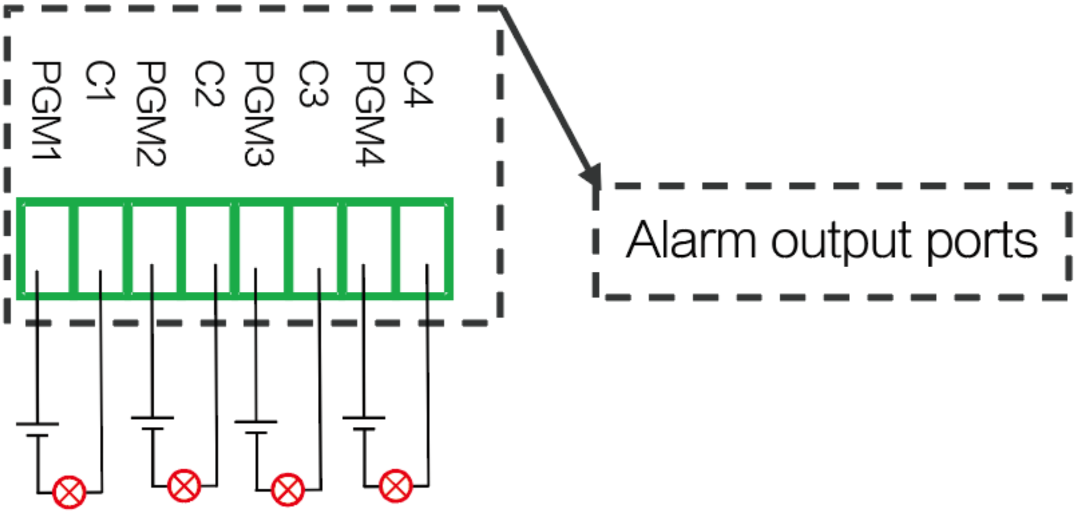
Figure 6-1 Alarm input cable connection



6.2 Local Alarm Output Cable Connection

The transmitter supports 4-channel alarm outputs correspond to ports C1-C4, PGM1-PGM4.

Figure 6-2 Local alarm output cable connection



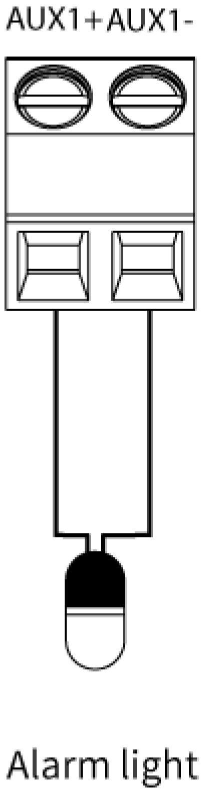
6.3 Auxiliary Output Cable Connection

The transmitter has two auxiliary power outputs, which correspond to AUX1+, AUX1-, GND, AUX2+, and AUX2- ports.

The output power of the 2-ch auxiliary power depends on the power supply mode of the transmitter.

When the module is powered by a 220V AC or 12V 7AH battery, the total output of the two auxiliary power outputs is 14.5V 2A. However, if the module is powered by PoE, the total output of the two auxiliary power outputs is reduced to 14.5V 1A.

Figure 6-3 Auxiliary output connection example



7 Adding the Transmitter to the Hub

Before you connect the transmitter 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 V1.99.800 or later, and DoLynk Care is V2.000.0000002.0 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.

7.1 Airfly Mode

All models of transmitter support adding by airfly.

Procedure

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

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

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

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

Step 5 Wait for the pairing.

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

7.2 Network Mode

Only models that have network ports support adding through network.

Background Information

DHCP is selected by default for the network mode when adding the transmitter. If the operation failed, we recommend that you use Configtool to change the transmitter's IP to a static IP and try adding again.

Procedure

Step 1 On the hub screen, tap **Peripheral**.

Step 2 Tap **+**, select **Add Peripheral**, and scan the QR code on the rear panel of the transmitter, and then tap **Next**.

Step 3 Configure the name and area for the transmitter, and then tap **Next**.

Step 4 Tap **...** on the right top corner of the screen, select **Add Through Network**, and then tap **Next**.

Step 5 Configure the password and confirm it after the transmitter is searched, and then tap **Next**.

Step 6 Wait for the pairing to complete, and then tap **Done**.

8 Configuration

You can view and edit general information of the transmitter.

8.1 Viewing Status

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

Table 8-1 Wireless IO transmitter Status

Modules	Parameter	Value
Wireless IO transmitter	Device No.	Displays the number of the transmitter.
	Bypass	● ⊘:Yes. ● ⊘: Lid only.
	Permanent Deactivation	The status for whether the permanent deactivation of the transmitter 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.
	Signal Strength	The signal strength between the hub and the transmitter. ● 📶 : Low. ● 📶 : Weak. ● 📶 : Good. ● 📶 : Excellent. ● 📶 : No. Only transmitters added through Airfly mode displays signal strength.

Modules	Parameter	Value
	Transmit Through Repeater	● 📡:Yes. ● No icon appears when the 📖 Only transmitters added through Airfly mode supports alarm repeater.
	External Power Status	● 🔗: Connected. ● ⛓: Disconnected.
	Battery Level	The battery level of the transmitter. ● 🟦: Fully charged. ● 🟩: Sufficient. ● 🟨: Moderate. ● 🟧: Insufficient. ● 🟥: Low. ● ❗: No battery.
	Tamper Status	The tamper status of the transmitter, which reacts to the detachment of the transmitter. ⊥ : Open.
	Online Status	Online and offline status of the transmitter. ● 🔗: Online. ● ⛓: Offline.
	Auxiliary Power Output	● Normal: Runs in regular condition. ● Overload: Wiring short circuits or external loads exceeding the specified capacity
	Number of Wired Devices	Displays total number of wired channels on the App on the **Peripheral** screen of the transmitter.
Input Channel	Device No.	Displays the device number of the input.

Modules	Parameter	Value
	Permanent Deactivation	The status for whether the permanent deactivation of the input channel are 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.
	Bypass	● ⊘:Yes. ● Ⓛ: Lid only.
	24 H Protection Zone Status	Active status of the 24 h protection zone. ● 24 : Enable. ● 24 : Disable.
	Home Mode	⌂: Enabled.
	Doorbell	● 🔔: Enabled. ● 🔔: Turned off.
	IPC Linkage	📷: Linked to IPC.
	Input Status	-•-: Normal/lid opened/protection loop shorted/protection loop open/masked.
Output Channel	Bypass	⊘:Yes.
	Permanent Deactivation	The status for whether the permanent deactivation of the output channel are enabled or turned off. ● ⊘ : Yes. The permanent deactivation is enabled. Alarm information will not 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.
	Output Status	● ⏻: On. ● ⏻: Off:

8.2 Configuring the Transmitter

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

Table 8-2 Parameter description

Parameter	Description
Device Configuration	● View the name, type, SN and device model. ● Edit the name, and then tap **Save** to save configuration.
Area	Select the room to which the transmitter 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 transmitter are 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.
Signal Strength Detection	Tap **Start Detection** to check the current signal strength of the transmitter. Make sure that the transmitter is installed in an area with great 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. ◇ Select from high, low, and automatic. ◇ The higher transmission power levels are, the further transmissions can travel, but power consumption increases. ◇ The indicator flashes when setting as **Low**.
User's Manual	View user's manual of the transmitter.

Parameter	Description
Cloud Update	Update the transmitter using cloud service. To update the models with Ethernet, we recommend using the network or manually updating it within the LAN on ConfigTool.

8.3 Adding and Configuring Wired Devices

Adding Wired Devices

1. Connect the detectors to the transmitter properly.
2. Go to the hub screen, and then select **Peripheral**.
3. Tap **Wired Device**, and tap **+** at the top right corner of the screen to add wired devices.

Figure 8-1 Wired device

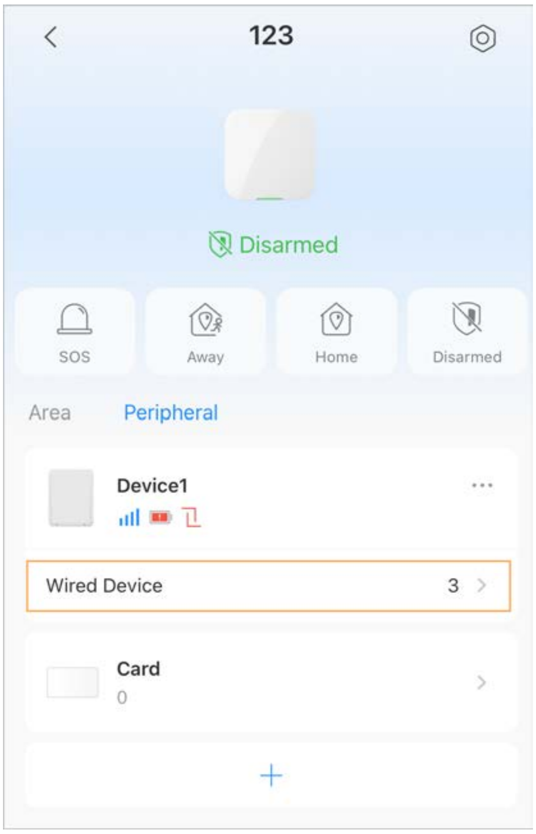
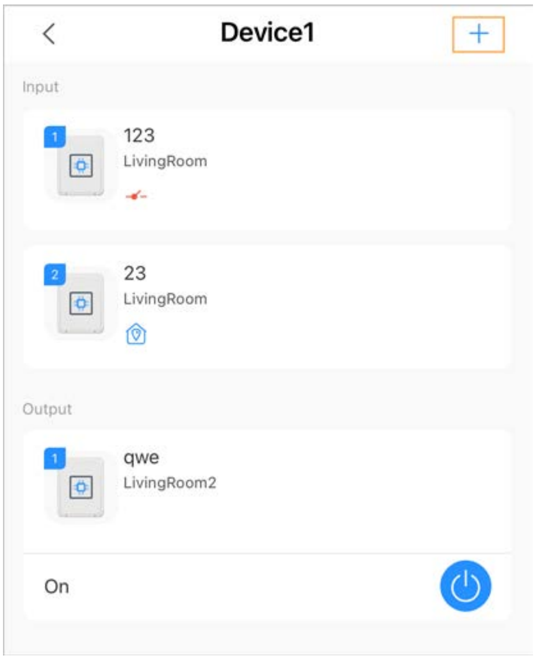


Figure 8-2 Add wired device



- Add input device. Enter the name, select the area, and device type as **Input**, and then select the channel for the input.

  You must select channels between input 1- input 16, which correspond to Z1- Z16 port in the wiring.

- Add output device. Enter the name, select the area, and device type as **Output**, and then select the channel for the output.

  You must select channels between output1- output 4, which correspond to C1- C4 port in the wiring.

Input Device Configuration

On the **Wired Device** screen, tap the input device, and tap ☑ to configure the parameters.

- If the input device is tamper.

Table 8-3 Parameter description

Parameter	**Description**
Name	The name of the input device.
Area	Select the room to which the input is assigned.

Parameter	Description
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 input 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.
External Detector Type	Select **Tamper**.
Contact Type	● Normally Open: Always in an open state. ● Normally Closed: Always in a closed state. ● Pulse: Use changes in pulse to detect the specific event or alarm.
EOLR	Select from **None**, **1**,**2**, **3**.
Resistance Value	When the EOLR is set to **1**, you can configure the resistance value. The available options include 1.1K Ω, 2.2K Ω, 4.7K Ω, 5.6K Ω, 6.8K Ω, and 8.2K Ω. Additionally, custom resistance values ranging from 1 to 15K Ω are also supported."
Alarm and Siren Linkage	Enable it and the siren sounds alarm when the alarm system detects a specific event or alarm condition.

- If the input device is sensor.

Table 8-4 Parameter description

Parameter	Description
Name	The name of the input device.
Area	Select the room to which the input is assigned.

Parameter	Description
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 input 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.
External Detector Type	Select **Sensor**.
Contact Type	● Normally Open: Always in an open state. ● Normally Closed: Always in a closed state. ● Pulse: Use changes in pulse to detect the specific event or alarm.
EOLR	Select from **None**, **1**,**2**, **3**.
Alarm Type	Select from **Intrusion**, **Fire Alarm**, **Medical Help**, **Panic Button**, **Gas Alarm** and **Water Leak**.
Zone Type	● Instant: Takes effect immediately. ● Delay: Takes effect in a customized delay time.You can enable the **Delay Mode under Home Mode**, and the device will be armed and the alarm will not be triggered until the end of customized delay time. 📖 Only after enabling **Home Mode**, the **Delay Mode under Home Mode** function can take effect. ● 24 hr: Takes effect in 24 hours.
Home Mode	When the security system is home armed, the detector will be armed only if the **Home Mode** is enabled.
Doorbell	After it is enabled, when the zone is disarmed and input is enabled, the siren will give off a ding dong sound like a doorbell.

Parameter	Description
Alarm and Siren Linkage	Enable it and the siren sounds alarm when the alarm system detects a specific event or alarm condition.
Alarm and Video Linkage	Enable it and the linked video records video when the alarm system detects a specific event or alarm condition.
Video Channel	After you select the video channel, the linkage video channel will store alarm videos when alarms are triggered.
Detector Test	Tap **Start Detection** to detect the signal strength of the input device.

- If the input device is keyswitch.

Table 8-5 Parameter description

Parameter	Description
Name	The name of the input device.
Area	Select the room to which the input 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 input 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.
External Detector Type	Select **Keyswitch**.
EOLR	Select from **None**, **1**,**2**, **3**.
Resistance Value	When the EOLR is set to **1**, you can configure the resistance value. The available options include 1.1K Ω, 2.2K Ω, 4.7K Ω, 5.6K Ω, 6.8K Ω, and 8.2K Ω. Additionally, custom resistance values ranging from 1 to 15K Ω are also supported."
Control Permissions	Select the areas with control permissions.
Control Mode	Select **Times Opened** or **Keyswitch Status** based on actual needs.

Parameter	Description
Control Type	● When the control mode is set to **Times Opened**, the control type can be set as **Away/Disarm** or **Home/Disarm**. ● When the control mode is set to **Keyswitch Status**, the control type can be set as **Arm**, **Home Mode** or **Disarm**.
Force Arming	It can only take effect when you enable **Arm with Faults** under **System Integrity Check**.

Output Device Configuration

On the **Wired Device** screen, tap the output device, and tap ✎ to configure the parameters.

Table 8-6 Parameter description

Parameter	Description
Name	The name of the output device.
Area	Select the room to which the output 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 output 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.
Output Type	Select **Normally Open** or **Normally Closed**.
Output Mode	● Bistable: Maintain either of its two stable states indefinitely until triggered to switch to the other state. ● Pulse: You can configure the pulse duration. The default is 30 seconds and must not exceed 600 seconds.

Parameter	Description
Scenario Settings	Tap **Create** to configure new scenarios. ● Arming/Disarming Linkage Scenario: The arming or disarming of one or multiple areas will trigger the on/off of the output module. ● Alarm Linkage Scenario: The device alarm will trigger the on/off of the output module. ● Scheduled Linkage Scenario: The output module can be linked based on the configured time.

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