Wireless Input Expander

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.0

Foreword

General

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

Model

DHI-ARM320-W2; DHI-ARM320-W2(868)

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
V1.0.0	First release.	May 2023

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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements

⚠

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

Installation Requirements

⚠ WARNING

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

⚠

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

Table of Contents

1 Introduction

1.1 Overview

The wireless input expander is a conversion device that connects third-party detectors to Dahua wireless hub. When the alarm of the third-party detector is triggered, the Expander sends the signal to the Hub through RF, and then the hub reports it to the platform. Different alarm types can be configured on the DMSS app, depending on the types of connected detectors. The expander has a built-in triaxial accelerometer to prevent the device from movement. An input channel is also provided to connect the tamper port of the third-party detectors. The Expander is powered by dry batteries, and can also provide power supply for detectors connected to it.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description
Port	Alarm Input	2 (1 for alarm and 1 for anti-tampering)
	Auxiliary Power Output	3.3 V, up to 10 mA
Function	Button	1 × power button
	Remote Update	Cloud update
	Signal Strength	Signal strength detection
	Measuring Range (Temperature)	−10 °C to +55 °C (+14 °F to +131 °F) (indoor)
Technical	Sensor	Triaxial accelerometer
	LED Indicator	1 × green alarm indicator
	Scenario	Indoor
	Operating Current	45 uA (with 1 min heartbeat, normally open mode, charge not being provided for other devices and device moved alarm not enabled)
	Alarm Current	50 mA
Wireless	Carrier Frequency	● DHI-ARM320-W2(868): 868.0 MHz–868.6 MHz ● DHI-ARM320-W2: 433.1 MHz–434.6 MHz

Type	Parameter	Description
	Transmit Power	● DHI-ARM320-W2(868): 14 dBm ● DHI-ARM320-W2: 9 dBm
	Communication Mechanism	Two-way
	Communication Distance	● DHI-ARM320-W2(868): Up to 1600 m (5249.34 ft) in an open space ● DHI-ARM320-W2: Up to 1300 m (4265.10 ft) in an open space
	Encryption Mode	AES128
	Frequency Hopping	Yes
General	Power Supply	3 × CR123A battery
	Battery Model	CR123A
	Battery Life	5 years (without providing charge for other devices)
	Power Consumption	Max. 150 mW (without providing charge for other devices)
	Operating Temperature	–10 °C to +55 °C (+14 °F to +131 °F) (indoor)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	102 mm × 39 mm × 21.5 mm (4.02" × 1.54" × 0.85")
	Net Weight	77 g (0.17 lb)
	Gross Weight	135 g (0.30 lb)
	Installation	Surface mount, or mount inside a third-party device
	Certifications	CE
	Anti-corrosion Level	Basic Protection
	Packaging Dimensions	95 mm × 43 mm × 139 mm (3.74" × 1.69" × 5.47")

2 Checklist

Figure 2-1 Checklist

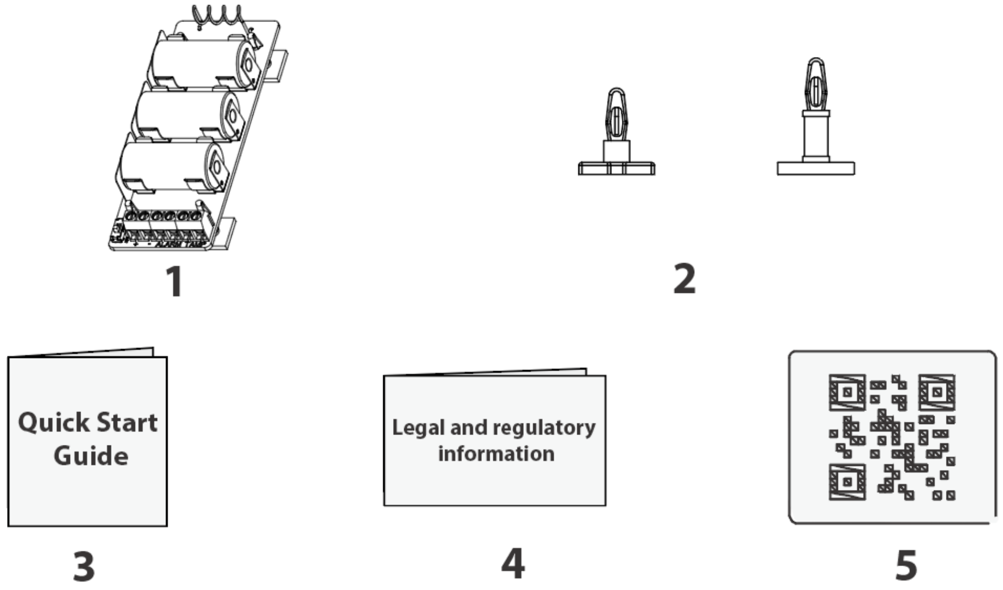


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless input expander	1	4	Legal and regulatory information	1
2	Space supporter	8	5	QR code	1
3	Quick start guide	1	—	—	—

3 Design

3.1 Appearance

Figure 3-1 Appearance

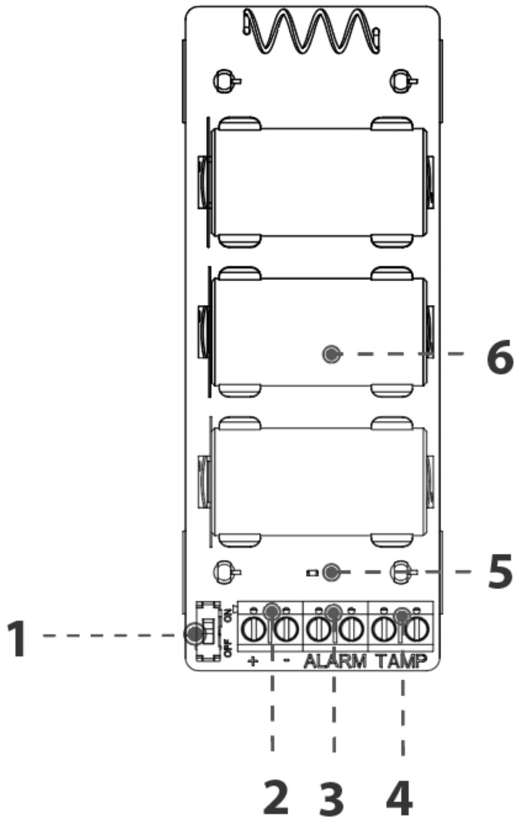
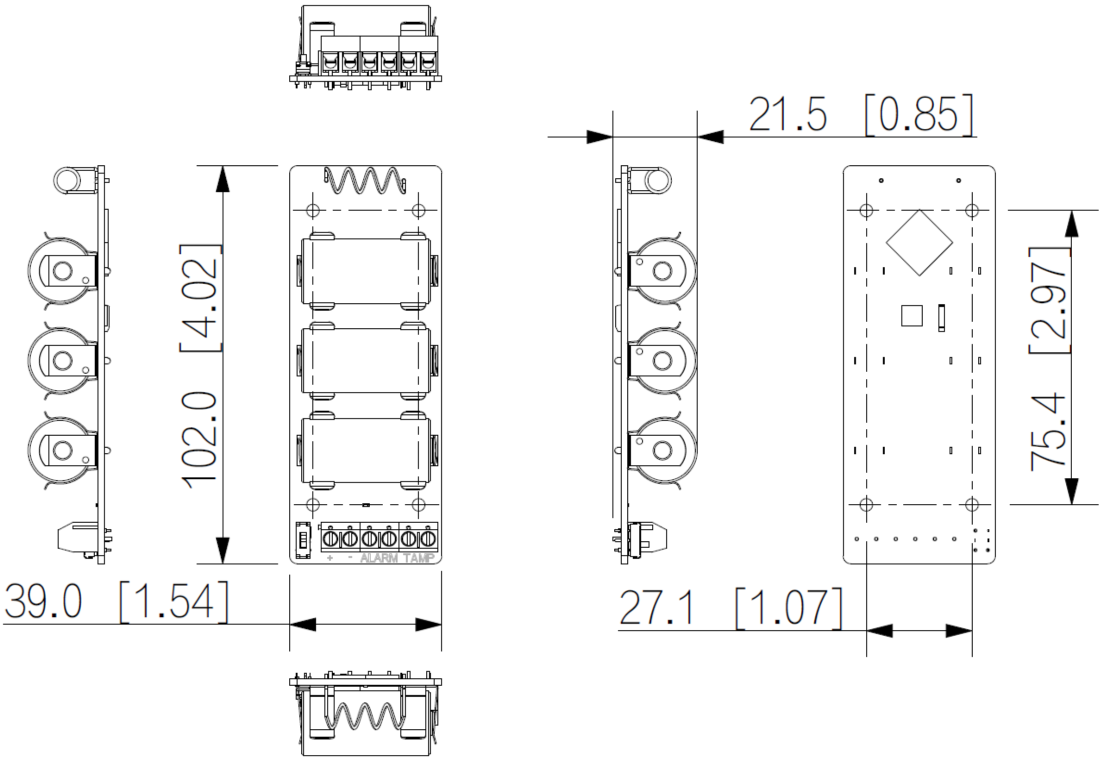


Table 3-1 Port description

No.	Name	Description
1	On/off switch	● Upper button: Power on. ● Lower button: Power off.
2	Power output port	● **+**: Positive pole. ● **-**: Negative pole.
3	Alarm input	Alarm input port that connects an alarm device.
4	Tamper input	The alarm is triggered when the device is detached.
5	Indicator	—
6	Battery	—

3.2 Dimensions

Figure 3-2 Dimensions (Unit: mm[inch])



4 Adding Expander to the Hub

Background Information

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

📖

- Make sure that the version of the app is 1.99.420 or later, and the hub is V1.001.0000006.0.R.230404 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 Expander.

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

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

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

Step 5 Wait for the pairing.

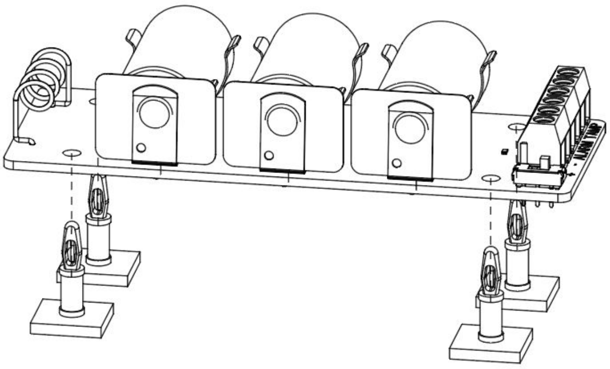
Step 6 Customize the name of the Expander, and select the area, and then tap **Completed**.

5 Installation

Procedure

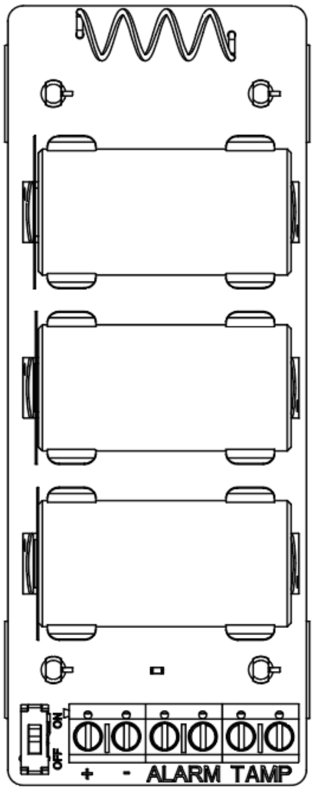
Step 1 Insert four space supporters into the board of the Expander.

Figure 5-1 Space supporters



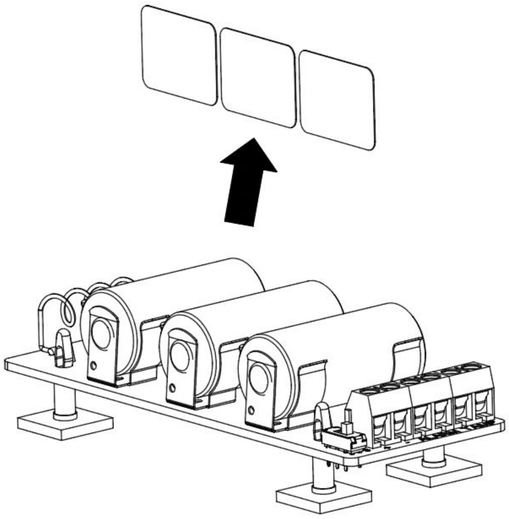
Step 2 Fix the device onto a flat surface.

Figure 5-2 Flat surface



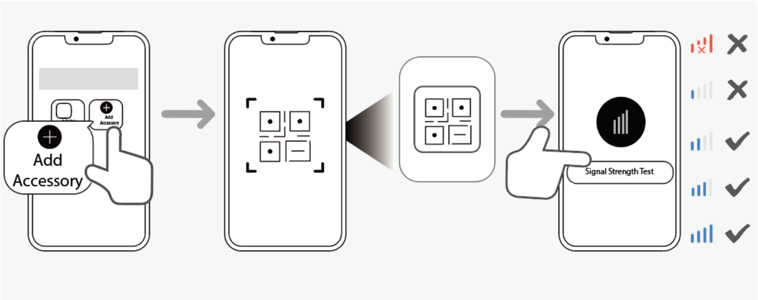
Step 3 Remove the mylar film.

Figure 5-3 Remove mylar film



Step 4 Add the Wireless Input Expander to the Hub, and check the signal strength of the installation location.

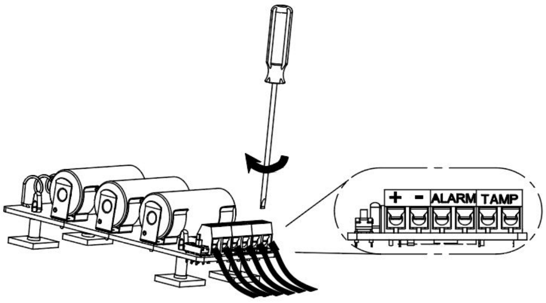
Figure 5-4 Test strength



Step 5 Complete the wiring of 6 ports.

After the wiring, switch the On/Off switch to see whether the device works.

Figure 5-5 Wiring



6 Configuration

6.1 Viewing Status

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

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the expander are enabled or disabled. ● ⊙: Enable. ● ⊘: Disable. 📖 Make sure that the version of the app is 1.99.420 or later,and the hub is V1.001.0000006.0.R.230404 or later.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the expander. ● 📶: Low. ● 📶: Weak. ● 📶: Good. ● 📶: Excellent. ● 📶: No.
Battery Level	The battery level of the expander. ● 🟦: Fully charged. ● 🟩: Sufficient. ● 🟨: Moderate. ● 🟧: Insufficient. ● 🟥: Low.
External Device Tamper Status	Displays **On** or **Off**.

Parameter	Value
Online Status	Online and offline status of the expander. ● 🔗: Online. ● ⛓: Offline.
Entering Delay Time	Entrance delay time.
Exiting Delay Time	Exit delay time.
24 H Protection Zone Status	Active status of the 24-hour protection zone. ● 24: Enable. ● 24: Disable.
Transmit through Repeater	The status of whether the expander forwards its messages to the hub through the repeater. Make sure that the version of the app is 1.99.420 or later,and the hub is V1.001.0000006.0.R.230404 or later.
Doorbell Status	The status of whether the chime function is enabled. ● !: Disabled. ● ✓: Enabled.
External Input	The status for whether the external input function of the expander is working normally or not. ● ⊸ : Normal. ● ⊸ : Abnormal.
Movement Alarm	The status of whether the movement alarm is enabled. ● □ :Disabled. ● □ : Enabled.
Program Version	The program version of the expander.

6.2 Configuring the Expander

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

Table 6-2 Parameter description

Parameter	Description
Device Configuration	● View expander name, type, SN and device model. ● Edit expander name, and then tap **Save** to save configuration.
Area	Select the area to which the expander is assigned.
Zone. No	The zone number assigned to the door detector alarm, which cannot be configured.
Temporary Deactivate	● Tap **Enable** , and then the function of the siren will be enabled so that information will be sent to the alarm hub. **Enable** is set by default. ● Tap **Disable**, and then the function of the siren will be disabled, and information will not be sent to the alarm hub.
LED Indicator	**LED Indicator** is enabled by default. 📖 If **LED Indicator** is disabled, the LED indicator will remain off regardless of whether the detector is functioning normally or not.
24 H Protection Zone	● If **24 H Protection Zone** is enabled, even the system is disarmed, the expander can be armed and detects motion. ● If **24 H Protection Zone** is disabled, only when the system is armed, the expander can be armed and detects motion. The Expander will not be armed immediately, it will begin before the end of the ping interval of the hub-detector (60 seconds by default). 📖 You can go to the hub's screen to configure the ping interval of the hub-detector. For details, see the user's manual of the hub.
Home Mode	Enable the home mode, and then the selected accessories under the hub will be armed.
Delay Mode under Home Mode	Enable the **Delay Mode under Home Mode**, the selected accessory under the hub will be armed and the alarm will not be triggered until the end of customized delay time. 📖 Only enable **Home Mode** first can **Delay Mode under Home Mode** take effect.

Parameter	Description
Delay Time	● The system provides you with time to leave or enter the protection zone without alarm. ◇ **Delay Time for Entering Arming Mode** : When you enter the zone, if you do not disarm the system before the delay ends, an alarm will be triggered. 📖 Make sure that the delay time for entering arming mode is no longer than 45 seconds in order to comply with EN50131-1. ◇ **Delay Time for Exiting Arming Mode** : When you are in the zone and arm the system, if you do not leave the zone before the delay ends, an alarm will be triggered. ● Select from 0 s to 120 s. 📖 The arming mode will be effective after the delay time.
Siren Linkage	When an alarm is triggered, the accessories will report the alarm events to the hub and alert with siren.
Alarm-video Linkage	When an alarm is triggered, the accessories will report the alarm events to the hub and then will be linked with videos.
Video Channel	Select the video channel as needed.
External Input	● **Alarm Type** : Select from the alarm list. ● **External Input** : Select from **Normally Open**, **Normally Closed** and **Pulse**.
External Tamper	● **External Tamper** : Tap to enable the function. ● **Cable Connection** : Select from **Normally Open** and **Normally Closed**.
Movement Alarm	The expander detects the movement every 5 seconds. When the detected acceleration of device movement reaches a certain threshold, a movement alarm will be triggered with the LED indicator flashes. ● Tap ○ next to the **Movement Alarm** to enable the movement alarm. ● Tap ○ next to **Link Movement Alarm to Siren** to enable the siren function. 📖 The siren can only be enabled when the movement alarm is enabled.

Parameter	Description
External Power Supply	● **Always Open** :The Expander will always provide external power supply for other devices. ● **Disabled while Disarmed** : When the Expander is disarmed, the external power supply function is disabled. ● **Always Disabled** : The Expander would not provide external power supply for other devices. 📖 ● If the expander is always open for external power supply, then the battery lifespan will be shortened. ● The external power supply supported is 3.3 V.
Chime	After enabling, when the area is disarmed, if the door detector is opened, the indoor siren will be triggered.
Over-temperature Alarm	Tap ○ next to **Over-temperature Alarm** to enable this function, and then the alarm will be triggered when the temperature of the area where the water leak detector is installed is higher or lower than the defined one. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap **+** or **-** to set the temperature ranges.
Signal Strength Detection	Test the current signal strength.
Detector Test	Tap **Start Detection** to test the status of the device. 📖 ● The detector test will not begin immediately. It will begin before the end of the ping interval of the hub-detector (60 seconds by default). ● You can configure the hub-detector ping interval on the hub.
Transmit Power	● Select from high, low, and automatic. ● The higher the transmission power, the farther the signal can travel, but the greater the power consumption. 📖 ● If you select **Low**, the expander will enter into reduced sensitivity mode. ● We recommend you selecting **Low** when installing the device to test the signal strength of the installation location, and then adjusting to **High** or **Automatic**. ● The indicator flashes when setting as **Low**. ● Make sure that the version of the app is 1.99.420 or later, and the hub is V1.001.0000006.0.R.230404 or later.
Cloud Update	Update online.

Parameter	Description
Delete	Delete the expander. Go to the hub screen, select the accessory from the list, and then swipe left to delete it.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

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

    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**

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

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

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

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

More information

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

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