Wireless LCD Keypad

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the LCD keypad (hereinafter referred to as the "keypad"). 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
V1.0.0	First release.	February 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, audio 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 keypad, hazard prevention, and prevention of property damage. Read carefully before using the keypad, 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 Product Overview

The LCD keypad is paired with the Alarm Hub 2, featuring an LCD screen and high-decibel buzzer. It supports one-button alarm activation for multiple scenarios and offers the convenience of arming and disarming through card swiping.

1.2 Technical Specification

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

Table 1-1 Technical specification

Type	Parameter	Description	
Function	Indicator Light	4 indicators (External power supply, arming/disarming, fault, and alarm)	
	Button	20 buttons (10 digital buttons and 10 function buttons)	
	Buzzer	2 × built-in buzzer	
	Arm and Disarm	Password; IC/desfire card	
	Remote Update	Cloud update	
	Signal Strength	Signal strength detection	
	Measuring Range (Temperature)	–10 °C to +55 °C (+14 °F to +131 °F)	
Technical	Operating Current	1.6 A (Max), 20 uA (Standby) (Battery 3 V); 0.77 A (Max), 1.6 mA (Standby) (12 VDC)	
Wireless	Carrier Frequency	DHI-ARK30C-RW2(868): 865.34 MHz–868.60 MHz	DHI-ARK30C-RW2: 433.1 MHz–434.6 MHz
	Transmitter Power (EIRP)	DHI-ARK30C-RW2(868): Limit 25 mW	DHI-ARK30C-RW2: Limit 10 mW
	Communication Mechanism	Two-way	
	Communication Distance	DHI-ARK30C-RW2(868): 1,600 m (5249.34 ft) (alarm transmission)	DHI-ARK30C-RW2:1,200 m (3937.01 ft) (alarm transmission)
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Language	Yes	
	Power Supply	12 VDC/4 × CR123A battery	

Type	Parameter	Description
	Battery Model	CR123A
	Standby Time	3 years (the heartbeat cycle is set as 1 minute by default. It will last 3 years if it is operated 2 times per day, with each interval lasting 1 minute.) 2 years (When the relevant function is enabled, the heartbeat cycle is set as 1 minute by default. It will last 2 years if it is operated 2 times per day, with each interval lasting 1 minute.)
	Power Consumption	4.8 W (Max), 0.20 mW (Standby) 4.8 W (Max), 0.33 mW (Standby, When the relevant function is enabled)
	Operating Temperature	-10 °C to +55 °C (+14 °F to +131 °F) (indoor)
	Operating Humidity	10%–90% (RH)
	Product Dimensions	170.0 mm × 129.0 mm × 31.2 mm (6.69" × 5.08" × 1.23")
	Net Weight	390 g (0.86 lb)
	Gross Weight	665 g (1.47 lb)
	Installation	Wall mount
	Casing Material	PC + ABS
	Appearance Color	White
	Certifications	CE
	Anti-corrosion Level	Basic Protection
	Storage Temperature	–10 °C to +55 °C (+14 °F to +131 °F)
	Storage Humidity	10%–90% (RH)
	Packaging Dimensions	214.0 mm × 162.0 mm × 57.0 mm (8.43" × 6.38" × 2.24")

2 Checklist

Please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

Figure 2-1 Checklist

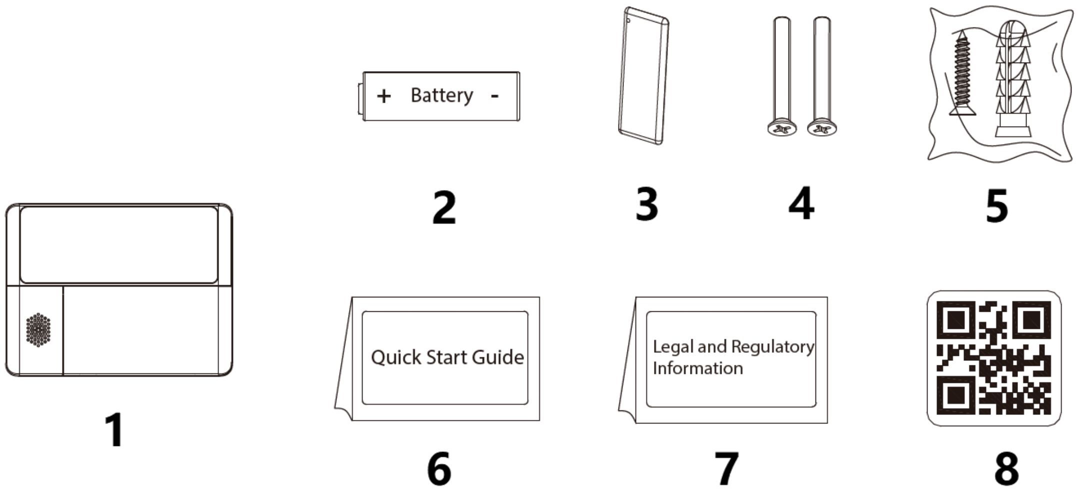


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Wireless LCD keypad	1	5	Package of screws	1
2	Battery	1	6	Quick start guide	1
3	IC card	1	7	Legal and regulatory information	1
4	Long screws	2	8	QR code	1

3 Design

3.1 Appearance

Figure 3-1 Appearance

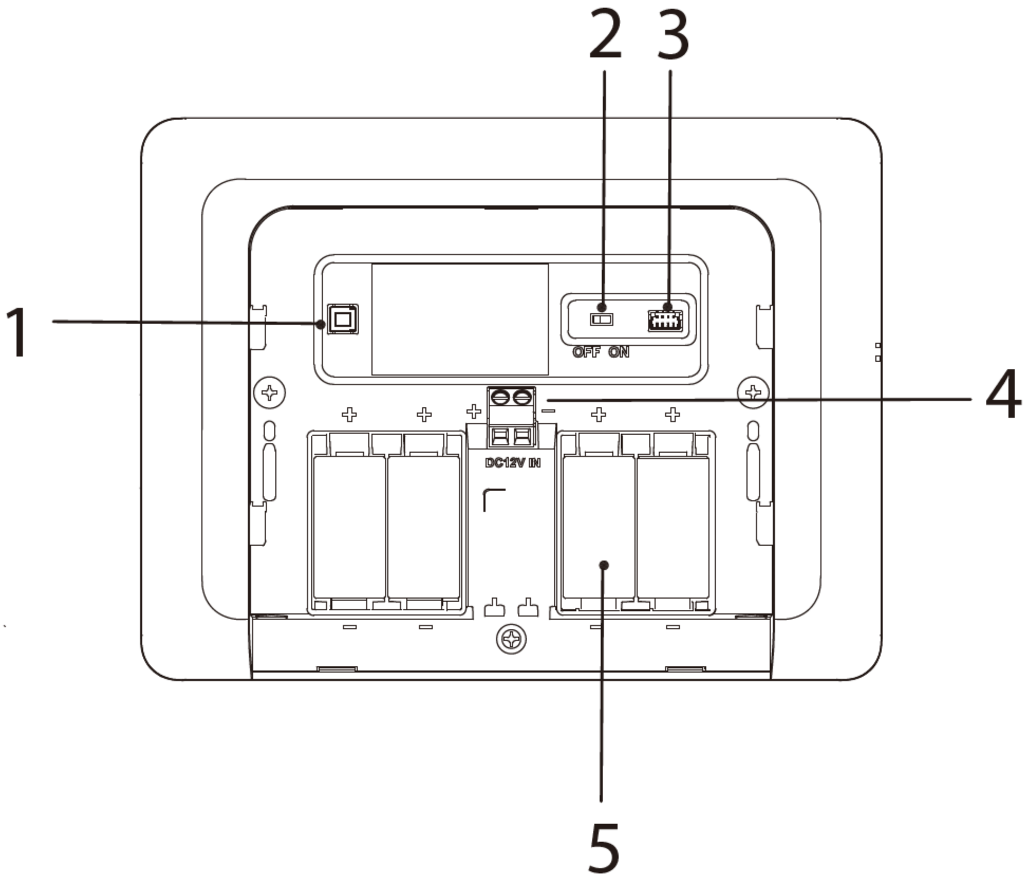
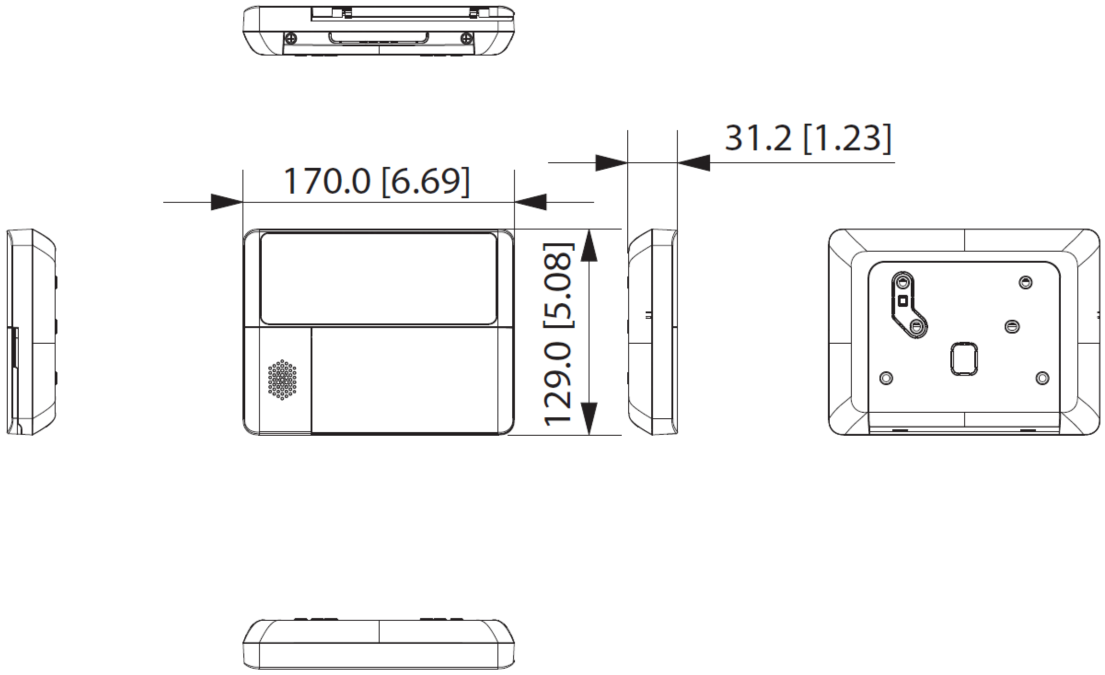


Table 3-1 Structure

No.	Name	Description
1	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
2	Power switch	Used to turn on or off the power supply.
3	Debug port	Used to connect to debuggers or other diagnostic tool.
4	12 VDC power terminal	Insert the 12 VDC power cable.
5	Battery compartment	Used to place batteries.

3.2 Dimensions

Figure 3-2 Dimensions(mm[inch])



4 Installation

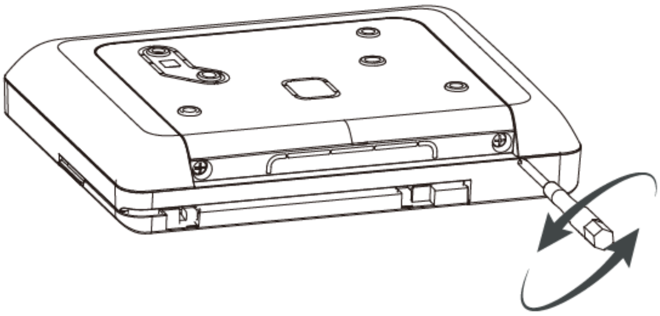
Power on the keypad, connect it to the hub, perform signal strength test, and then install the keypad onto the wall.

4.1 Powering on the Keypad

Procedure

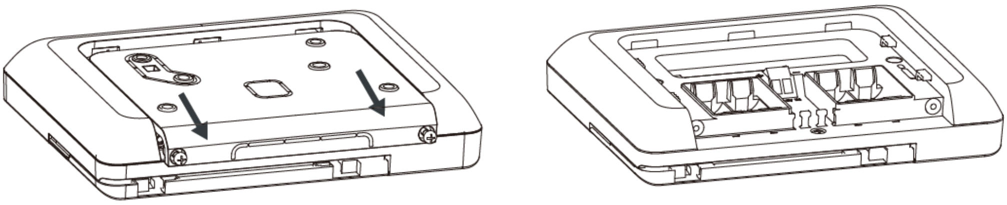
Step 1 Use a Phillips screwdriver to open the anti-loosening screws at the bottom of keypad on both sides.

Figure 4-1 Open the anti-loosening screws



Step 2 Open the mounting plate.

Figure 4-2 Open mounting plate



Step 3 Insert the batteries or connect to external power supply.

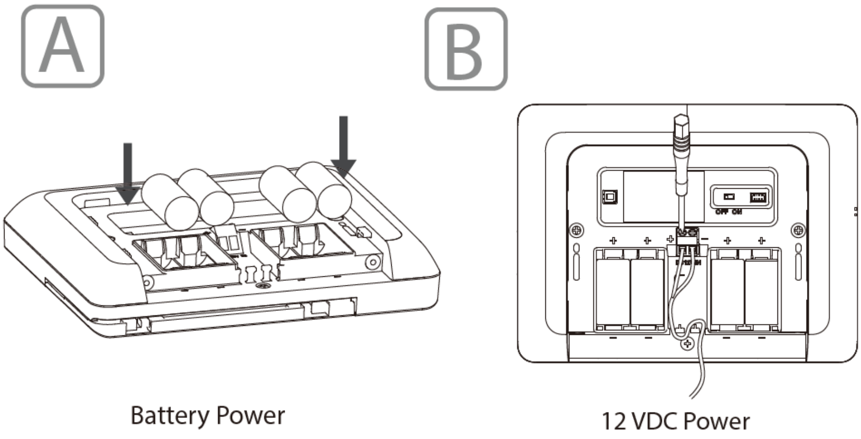
- Battery power: Place the 4 batteries in the compartment in the correct direction.

  ◇ When inserting the batteries, make sure that they are all charged to the same level.

  ◇ When inserting the batteries, align the "+" symbols on the battery to those on the LCD keypad.

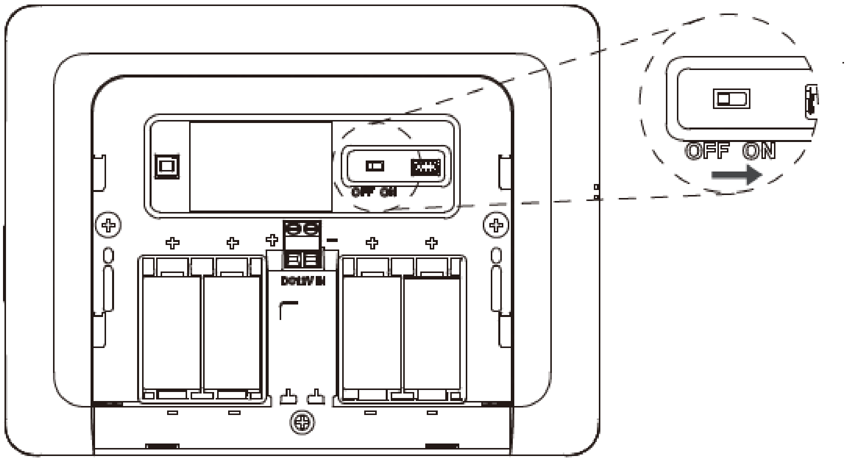
- 12 VDC power: Insert the power cable into the socket according to the "+" and "-" symbols molded on the panel. Use a Phillips screwdriver to tighten it.

Figure 4-3 Insert batteries or connect to power



Step 4 Switch the power to the "ON" position.

Figure 4-4 Switch to "ON"



4.2 Adding Keypad to Hub

Background Information

Before you connect the keypad 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 V1.99.850 or later, the DoLynk Care app is V2.50 or later, and the hub is V2.000.0000005.0.R.250106 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 keypad.

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

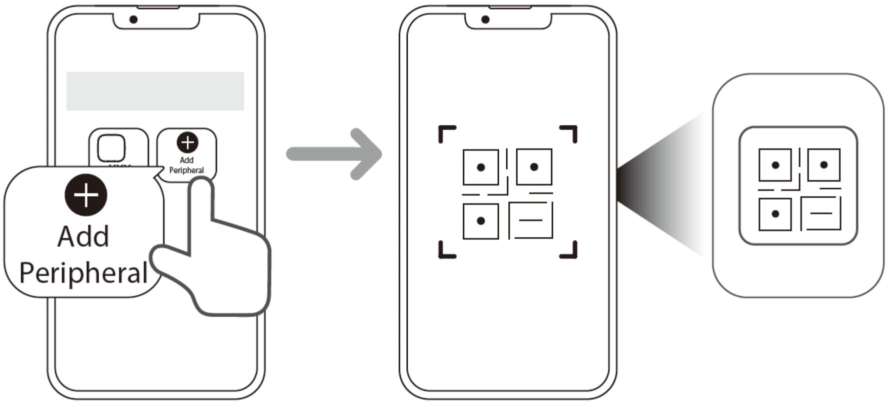
Step 3 Tap **Next** after the keypad has been found.

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

Step 5 Wait for the pairing.

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

Figure 4-5 Add keypad to Hub



4.3 Detecting Signal Strength

Procedure

Step 1 Install the keypad in a place with great signal strength.

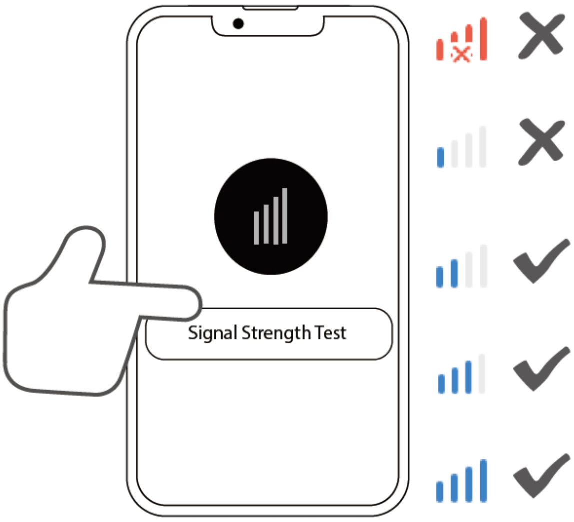
Step 2 Open the DMSS app, select a hub on the **Home** screen, and then select a keypad on the **Devices** > **Settings** screen.

Step 3 Tap **Signal Strength Detection** to check the current signal strength of the keypad.

⚠

The signal strength must be at least 2 bars.

Figure 4-6 Detect signal strength



4.4 Installing Keypad

4.4.1 Wall-Mount Installation

Procedure

Step 1 Loosen the screw at the bottom of the keypad to remove the front panel.

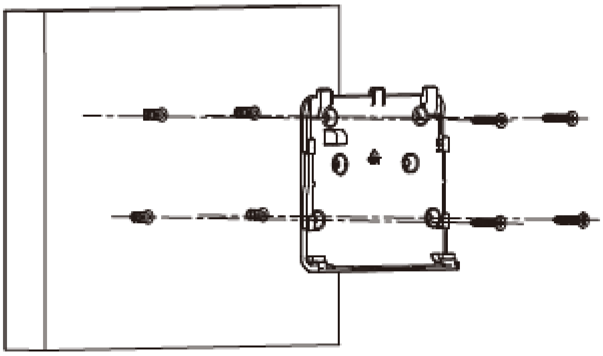
Step 2 Set the keypad into a horizontal position. Use the spirit level to make sure the keypad is horizontal and level.

Step 3 Put the expansion bolts into the holes.

Step 4 Align the screw holes on the rear panel with the expansion bolts.

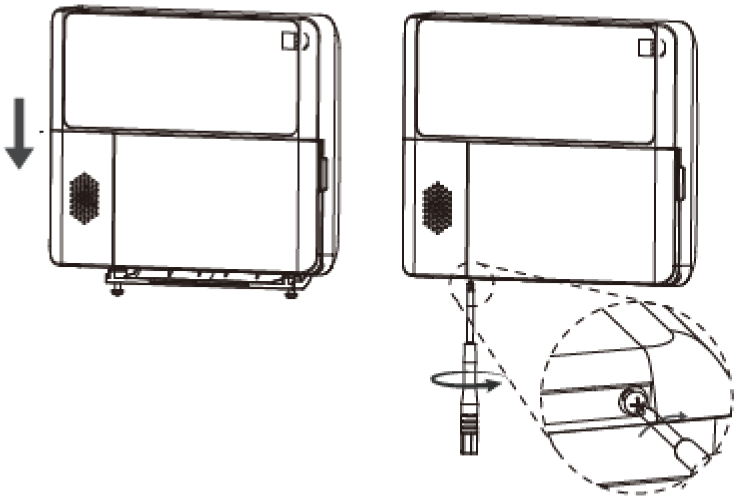
Step 5 Secure the rear panel with self-tapping screws.

Figure 4-7 Installation



Step 6 Tighten the screw at the bottom of the front panel to secure the keypad.

Figure 4-8 Secure the keypad



4.4.2 86 Box Installation

Install the keypad using the 86 box.

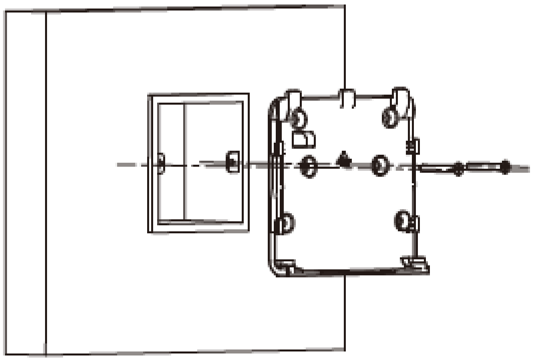
Procedure

Step 1 Loosen the screw at the bottom of the keypad to remove the front panel.

Step 2 Insert the 86 box into the holes and secure it with screws.

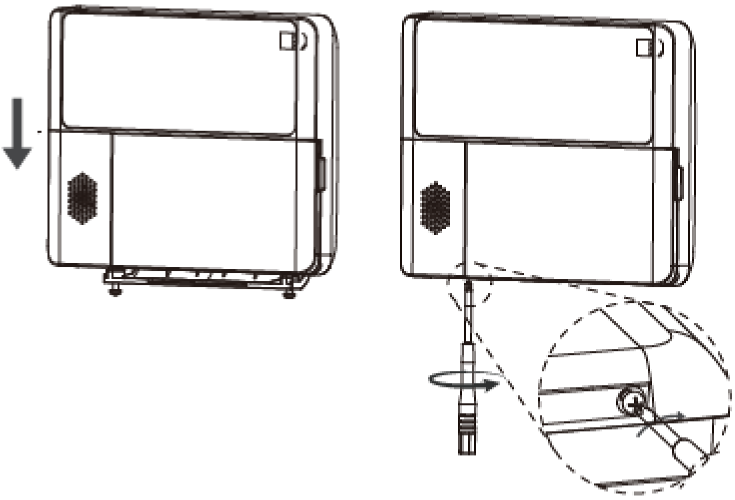
Step 3 Fix the real panel on to the 86 box and secure the rear panel with self-tapping screws.

Figure 4-9 Installation



Step 4 Attach the front panel to the real panel, and tighten the screw at the bottom of the front panel to secure the keypad.

Figure 4-10 Secure the keypad



5 Configuration

5.1 Viewing Status

On the **Home** screen, select a hub, and then select a keypad, go to **Devices** > **Overview** screen of the hub to view the status of the keypad.

Table 5-1 Status

Parameter	Description
Device No.	Displays the number of the keypad.
Temperature	Displays the temperature of the keypad. The temperature has a tolerance of ± 3 °C, and the measurement accuracy is 1 °C.
Signal Strength	The signal strength between the hub and the keypad. ● 📶: Low. ● 📶: Weak. ● 📶: Good. ● 📶: Excellent. ● 📶✕: No.
Online Status	Online and offline status of the keypad. ● Online. ● Offline.
Battery Level	The battery level of the keypad.
External Power	Displays whether the external power is connected. Only after you have enabled **External Power Detection**, the status of external power can be displayed. ● Disconnection. ● Connected.
Permanent Deactivation	The status for whether the permanent deactivation of the keypad is enabled or turned off. ● Yes. ● Lid only. ● No.

Parameter	Description
Bypass	Whether bypass is enabled or not. Once enabled, all information will not be sent to the alarm hub. ● Yes. ● Lid only. ● No.
Tamper	The tamper status of the keypad, which reacts to the detachment of the keypad. ● Opened. ● Closed.
Lock Status	The lock status of the keypad. ● Unlock. ● Locked.
Doorbell	The doorbell status of the keypad. ● Enabled. ● Disabled.
Repeater	Whether transmission through repeater is supported. ● Yes. ● No.
Program Version	Displays the latest version of the keypad program.

5.2 Configuring the Keypad

On the **Home** screen, select a hub, and then select a keypad on the **Devices** > **Settings** screen of the hub to configure the keypad.

Table 5-2 Parameter description

Parameter	Description
Device	● View the name, type, SN of the device. ● Edit the name, and then tap **OK** to save configuration.
Area	Select the room to which the keypad 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.

Parameter	Description
Permanent Deactivation	The status for whether the permanent deactivation of the keypad 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.
Control Permissions	Configure the rooms that the keypad can control. You can select **All Areas** to have the permissions of all the areas under the hub, or select the specific area for the keypad to control.
Alarm Button	Enable the keys on the keypad first and set if an event happens. ● Fire alarm: Press and hold the fire key on the keypad for 3 seconds to trigger fire alarm after enabling this function. ● Link fire alarm to siren: The fire alarm is sent to siren after enabling this function. ● Panic alarm: Press and hold the SOS key on the keypad for 3 seconds to trigger panic alarm after enabling this function. ● Link panic alarm to siren: The panic alarm is sent to siren after enabling this function. ● Medical alarm: Press and hold the medical key on the keypad for 3 seconds to trigger medical alarm after enabling this function. ● Link medical alarm to siren: The medical alarm is sent to siren after enabling this function.
Keypad Lock Status	● Lock: Configure the lock duration and the number of wrong attempts after enabling this function. The default is 5 minutes, and you can configure from 3 to 180 minutes. ● Password attempts: Configure the number of attempts allowed if you enter a wrong password within 30 minutes. The default number is 5 times, and you can configure from 3 to 10 times. ● Lock time: Configure the time to automatically lock the keypad after the allowed attempts expired.
Arm Without Password	You can arm the keypad without entering the password.
Alarm Details	Enable the function to receive alarm details. You can configure the alarm duration. The default is 120 seconds, and you can configure from 0 to 180 seconds.

Parameter	Description
Card	Enable the **Card Reader** function, and the keypad can use card recognition function. ● Type: IC card or DESFire card. ● Soft encryption: Card information will be encrypted when issuing the card. ● NFC: Tap the card against the keypad without swiping. ● Operation mode: Select **Easy** or **Standard**. In the easy mode, you can swipe the card to arm or disarm the linked areas. In the standard mode, swiping card is equivalent to entering the password.
Sound Settings	● Play sound for arming and disarming: Enable the function to play sound when arming and disarming. ● Play sound for delay time: Enable the function to play sound when delay time. ● Play sound for scheduled arming and disarming: Enable the function to play sound for scheduled arming and disarming. ● Volume: Adjust the volume for arming and disarming, delay time, and scheduled arming and disarming from low to high. ● Key sound: Adjust the sound from low to high. You can select **Off** to turn off the sound. ● Alarm sound: Adjust the sound from low to high. You can select **Off** to turn off the sound. ● Doorbell sound: Adjust the sound from low to high. You can select **Off** to turn off the sound.
External Power Detection	If **External Power Detection** is enabled, power failure alarm messages will be pushed to the DMSS.
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 keypad 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. The range is between -10 and 55°C.
Backlight Brightness	Select from **Closed** , **Low** and **High** to adjust the backlight brightness of the keypad operating screen. ⚠ Selecting the **High** mode will reduce the battery life. Be cautious with your selection.
LED Indicator	Indicators for alarms, fault and arming/disarming status on the keypad. 🕮 Turning off the function will stop the indicators of the keypad from lighting up for alarms, faults and arming/disarming statuses.

Parameter	Description
Signal Strength Detection	Tap **Start Detection** to check the current signal strength of the keypad. Make sure that the keypad 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 keypad.
Firmware Update	Update the keypad firmware using cloud service.

6 User Management

6.1 Adding Users

You can add, modify, or delete keypad users when it is disarmed.

Background Information

Only installer and admin users have permission to add users.

Procedure

Step 1 Go to the home screen.

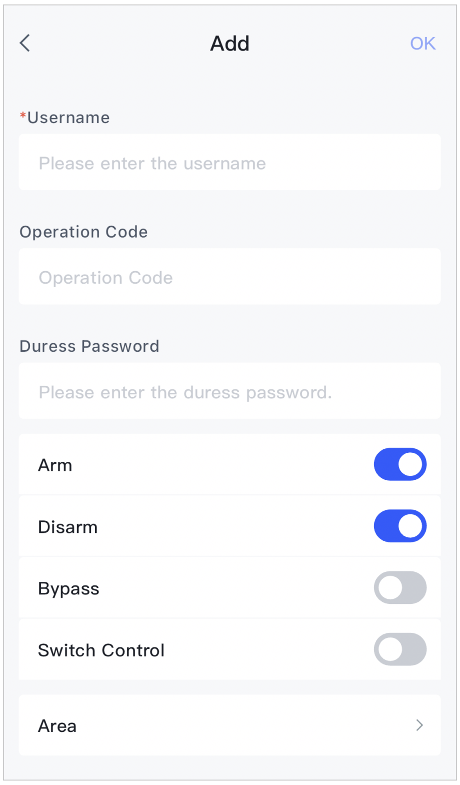
Step 2 Select a hub, and then select **Device Details** > **Settings** > **Hub Setting** > **User Management**.

Step 3 Select **Keypad User** , and then click **Add** to add a user.

Step 4 Enter your user name, operation code (password), and duress password, select the arm, disarm, bypass permissions, and then select the area to be controlled.

- Password and duress code must be 4 to 6 digits.
- Duress password is optional.
- Up to 32 users can be created. The first created user is the admin user by default. All the permissions are available to them.

Figure 6-1 Add a user



Step 5 Tap **OK**.

Related Operations

- Deleting a user

  On the **Keypad User** screen, select the user, and then tap **Delete User**.

  The admin user must be the last to be deleted.

- Modifying user information

  On the **Keypad User** screen, select the user, and then you can modify user's information, including user name, operation code, and duress code.

6.2 Adding Cards

The method for adding IC cards is the same as that for adding DESFire cards. The following example illustrates how to add an IC card.

You can add, modify, or delete the card when the keypad is disarmed. There are 2 ways to add the card.

- Adding the card on the **User Management**.
- Adding the card in the peripheral list.

Only installer and admin users have permission to add the card.

6.2.1 Adding Cards on the User Management

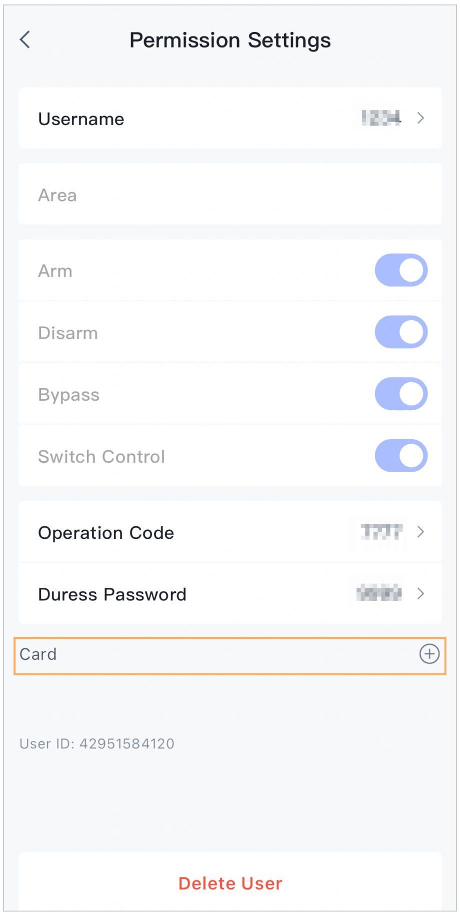
Procedure

Step 1 Go to the home screen.

Step 2 Select a hub, and then select **Device Details** > **Settings** > **Hub Setting** > **User Management**.

Step 3 On the **Keypad User** screen, select the user to whom you want to link the card, and tap **+** next to **Card**.

Figure 6-2 Add card



Permission Settings

Username [redacted]

Area

Arm

Disarm

Bypass

Switch Control

Operation Code [redacted]

Duress Password [redacted]

Card ⊕

User ID: 42951584120

Delete User

Step 4 Press any key to wake up the keypad, and then place the card near the card swiping area of the keypad to enter to the linking process within 30 seconds.

If the card information is successfully recognized, the card ID will be displayed on the app, and the keypad will beep once. After you save the configurations, the card will have the user's permissions.

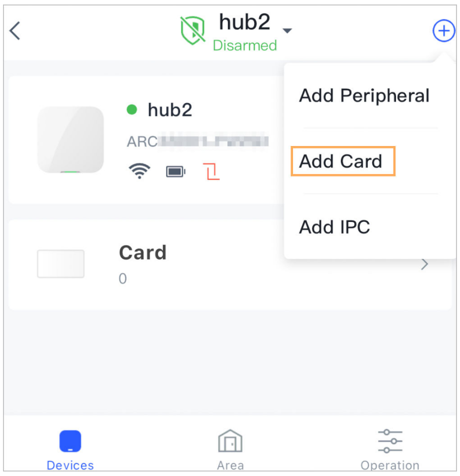
Up to 8 cards can be linked to a user.

6.2.2 Adding Cards in the Peripheral List

Procedure

Step 1 Go to the **Devices** screen of the hub, and then select ⊕ > **Add Card**.

Figure 6-3 Add card



Step 2 Press any key to wake up the keypad.

Step 3 Place the card near the card swiping area of the keypad to enter to the linking process.

Step 4 On the **Linked User** screen, you can select whether to create a new user, or link the card to the added user.

If you select to create a new user, tap **Create User**. For details, see "6.1 Adding Users".

Step 5 Tap **OK**.

7 Operation

7.1 Frequently Used Commands

Following are frequently used commands for the keypad.

- Before using the keypad, make sure you have created accounts on the DMSS.
- Before using **Standard** mode, you must have selected the **Standard** in **Card** function module on DMSS. For details, see"5.2 Configuring the Keypad".
- The duress code and password of the keypad are configured on the **Hub Setting** > **User Management** screen of the DMSS. For details, see"6.1 Adding Users".

Table 7-1 Command

Function	Command
Global Away Arming	● When the keypad is in **Standard** mode: ◇ When the system is in fault: Enter the password/swipe card +⌂ + ⌂. ◇ When the system is not in fault: Enter the password/swipe card +⌂. In the **Standard** mode, swiping the card is equivalent to entering the password. You can swipe the card instead if you do not want to enter the password. ● When the keypad is in **Simple** mode: ◇ When the system is not in fault: Swipe the card. ◇ When the system is in fault: Swipe the card, and then swipe it again. In the **Simple** mode, swiping the card is equivalent to arming when the keypad has been disarmed; and is equivalent to disarming when the keypad has been armed.
Global Stay Arming	● When the system is in fault: Enter the password/swipe card +⌂ + ⌂. ● When the system is not in fault: Enter the password/swipe card +⌂. In the **Standard** mode, swiping the card is equivalent to entering the password. You can swipe the card instead if you do not want to enter the password.
Area Away Arming	● When the system is in fault: Enter the password/swipe card +*+Area No.+*+Area No...+*...+⌂+⌂. ● When the system is not in fault: Enter the password/swipe card +*+Area No.+* +Area No...+*...+⌂.

Function	Command
Area Stay Arming	● When the system is in fault: Enter the password/swipe card +*+Area No.+*+Area No...+*...+⌂+⌂. ● When the system is not in fault: Enter the password/swipe card +*+Area No.+*+Area No...+*...+⌂.
Global Disarming	● When the keypad is in **Standard** mode: ◇ If the system displays fault prompt: Enter the password/swipe card +⊘ to go back to the home screen. ◇ If the system displays fault prompt: Enter the password/swipe card +⊘, and wait a while/press return key to go back to the home screen. In the **Standard** mode, swiping the card is equivalent to entering the password. You can swipe the card instead if you do not want to enter the password. ● When the keypad is in **Simple** mode: ◇ If the system displays fault prompt, swipe the card to go back to the home screen. ◇ If the system displays fault prompt, swipe the card, and wait a while/press the return key to go back to the home screen. In the **Simple** mode, swiping the card is equivalent to disarming.
Area Disarming	Enter the password/swipe card +*+ Area No.+*+Area No.+...+*...+⊘. In the **Standard** mode, swiping the card is equivalent to entering the password. You can swipe the card instead if you do not want to enter the password.
Duress Disarming	Enter the duress password + ⊘.
Bypass	1. Enter the password/swipe card + ⊟ (press and hold for 3 seconds). In the **Standard** mode, swiping the card is equivalent to entering the password. You can also swipe card instead if you do not want to enter the password. 2. Press ←↑↓→ to select the zone to be bypassed or cancel bypass, and then press **Enter**. ● If the zone has been bypassed, pressing **Enter** means cancel bypassing. ● If the zone has not been bypassed or in tamper only mode, pressing **Enter** means bypassing.

Function	Command
Output Control	1. Enter the password/swipe card + ⊟⊟. In the **Standard** mode, swiping the card is equivalent to entering the password. You can also swipe card if you do not want to enter the password. 2. Press ←↑↓→ to select the output to be enabled, and then press **Enter**. ● If the output is closed, pressing **Enter** means opening it. ● If the output is opened, pressing **Enter** means closing it.
Status Query	View the hub status, peripheral status, hub version information and keypad version information. 1. Enter the password/swipe card, and then press and hold #🔧 for 3 seconds. In the **Standard** mode, swiping the card is equivalent to entering the password. You can also swipe card instead if you do not want to enter the password. 2. Press **Enter** to go to the directory page. Press ←↑↓→ to select from **Hub Status**, **Peripheral Status**, **Hub Info** and **Keypad Info**. 3. Press **Enter** to go to the details page.

7.2 Waking Up the Keypad

Press any key on the keypad to wake up the keypad.

- If you do not use the keypad for more than 4 seconds, the backlight LCD display will be dim, and the status of the indicator light will remain the same.
- If you do not use the keypad for more than 12 seconds, the keypad will beep once, all the indicator lights will turn off, and then the keypad will enter sleep mode.

7.3 Arming and Disarming

The indicator displays blue if arming is successful. If disarming is successful, the indicator will flash green and then turn off.

7.4 One-tap Alarm

Press and hold the fire/emergency/medical alarm button for 3 seconds to trigger alarm. The alarm indicator light flashes red if the one-tap alarm is successful.

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 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;
   - 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