Wireless 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 wireless keypad (hereinafter referred to as the "keypad"). Read carefully before using the device, and keep the manual safe for future reference.

Model

DHI-ARK30T-W2 (868); DHI-ARK30T-W2

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, 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.	April 2022

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 protection, and protection 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

Wireless keypad is used with alarm hub, and supports multiple users, allowing each one to access the alarm security system with their own private passcode. The system also conveniently keeps a log of the operations performed by each user, making it easy to review and analyze usage history. It is ideal for use in villas, shops, apartments and more.

1.2 Technical Specifications

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

Table 1-1 Technical specifications

Type	Parameter	Description	
Function	Indicator Light	4 indicators (communication, arming and disarming, fault, and alarm)	
	Key	15 keys (0–9, *, #, arm, disarm, and home arm)	
	Buzzer	1 × built-in buzzer	
	Arm and Disarm	Passcode; IC card	
	Remote Update	Cloud update	
	Low Battery Detection	Yes	
	Tamper	Yes	
	Measuring Range (Temperature)	–15 °C to +65 °C (+5 °F to +149 °F) (indoor)	
	Measuring Accuracy	1 °C (33.8 °F)	
Wireless	Carrier Frequency	DHI-ARK30T-W2 (868): 868.0 MHz–868.6 MHz	DHI-ARK30T-W2: 433.1 MHz–434.6 MHz
	Communication Distance	DHI-ARD821-W2 (868): Up to 1,600 m (5,249.34 ft) in an open space	DHI-ARD821-W2:Up to 1,200 m (3,937.01 ft) in an open space
	Power Consumption	Max. 2.3 W	
	Communication Mechanism	Two-way	
	Encryption Mode	AES128	
	Frequency Hopping	Yes	
General	Operating Temperature	–10 °C to +55 °C (+14 °F to +131 °F) (indoor)	
	Operating Humidity	10%–90% (RH)	

Type	Parameter	Description
	Power Supply	4 × AA batteries
	Battery Life	3 years (if the device is used to arm and disarm once a day)
	Product Dimensions	146.0 mm × 82.0 mm × 22.6 mm (5.75" × 3.23" × 0.89")
	Packaging Dimensions	180.0 mm × 104.0 mm × 58.0 mm (7.07" × 4.09" × 2.28")
	Installation	Wall mount
	Net Weight	240 g (0.529 lb) (with battery) 145 g (0.32 lb) (without battery)
	Gross Weight	370 g (0.816 lb)
	Certifications	CE

2 Checklist

Figure 2-1 Checklist

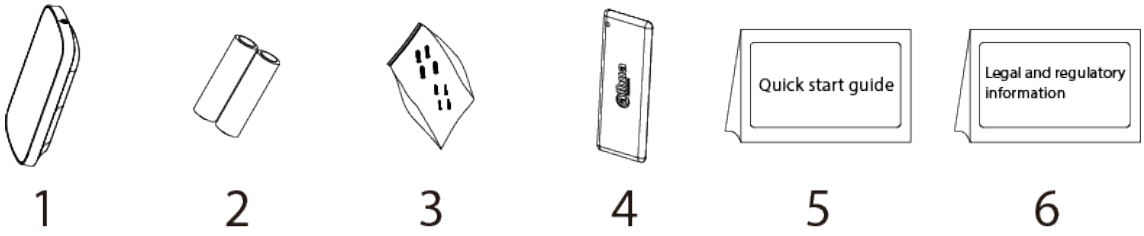


Table 2-1 Checklist

No.	Item Name	Quantity	No.	Item Name	Quantity
1	Keypad	1	4	IC card	2
2	Battery	4	5	Quick start guide	1
3	Screw package	1	6	Legal and regulatory information	1

3 Appearance

Figure 3-1 Appearance

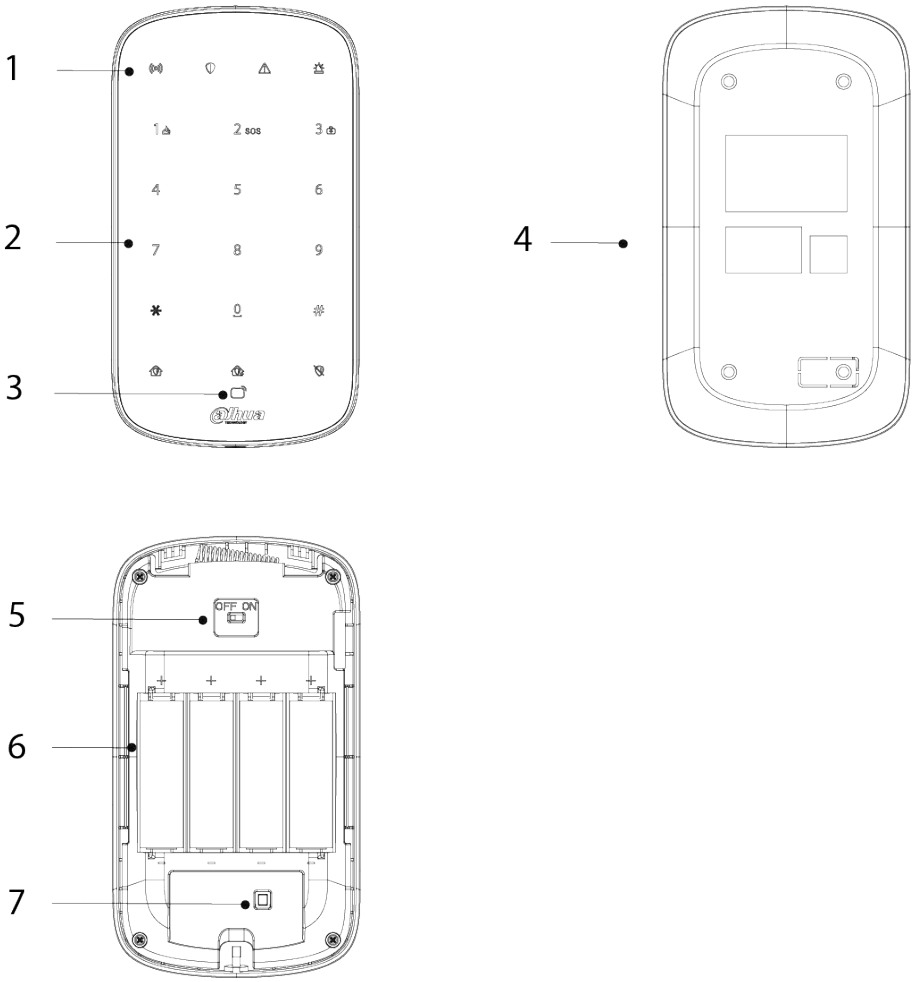


Table 3-1 Structure

No.	Name	Description
1	Indicator	There are four indicators, including communication, arming and disarming, fault, and alarm indicators. ● All indicators are solid for 2 seconds: Powered on. ● All indicators are off: Not enter paring mode. ● Communication indicator status: ◇ Flashes green quickly: Pairing mode. ◇ Sold green for 2 seconds: Pairing successful. ◇ Flashes green 3 times: Pairing fails. ◇ Off: Online. ◇ Flashes green slowly and other indicators are off: Offline. ◇ Flashes green slowly and other indicators are in the normal status: Enters into reduced sensitivity mode. ● Arming and disarming indicator status: ◇ Solid blue: A single or more rooms are armed. ◇ Flashes green 3 times and then off: All rooms are disarmed. ● Fault indicator status: ◇ Flashes yellow: Fault alarms are triggered. ◇ Off: A single or more rooms are armed, or no fault occurs. ● Alarm indicator flashes red: Alarm are triggered.
2	Key	15 keys. ● Numeric keys: 0-9. 1 is also the fire alarm key, 2 emergency alarm key, and 3 medical alarm key. ● #: Search. ● *: Space. ● Home arming. ● : Away arming. ● : Disarming.
3	Card swiping area	Supports IC card recognition. You can swipe your card here.
4	Back cover	When the tamper switch is released, the tamper alarm will be triggered.
5	On/off switch	Turn on or turn off the keypad.
6	4 × Batteries	Insert batteries to power on the keypad.
7	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.

4 Adding the Keypad to the Hub

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

- Make sure that the version of the DMSS app is 1.98 or later, and the hub is V1.001.0000000.8.R.220319 or later.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Step 1 Go to the hub screen, and then tap Accessory 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**.

5 Installation

Prior to installation, add the keypad to the hub and check the signal strength of the installation location. We recommend installing the keypad in a place with a signal strength of at least 2 bars. The keypad supports wall mount.

Step 1 Loosen the screw to open the keypad.

Figure 5-1 Loosen the screw

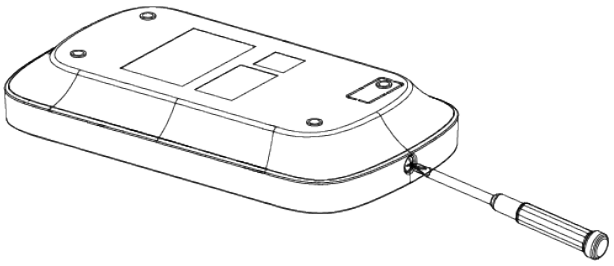
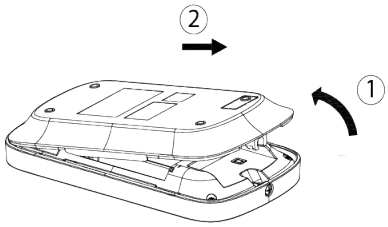


Figure 5-2 Open the keypad

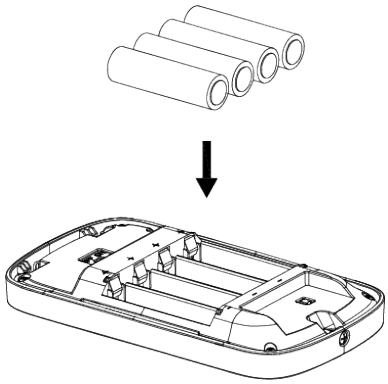


Step 2 Insert four batteries into the keypad.

- If the battery is dead, you need to replace the battery.
- When replacing the battery, make sure that the side marked with "＋" faces the back cover of the keypad.

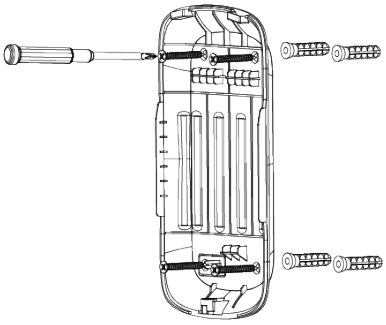
- Make sure to use the same model when replacing the battery to avoid fire or explosion.
- Make sure not to mix the old batteries with new one.

Figure 5-3 Put on the batteries



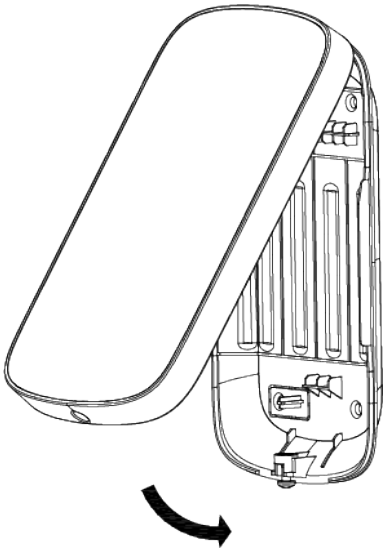
Step 3 Drill four holes in the wall according to the hole positions of the keypad, and then put the expansion bolts into the holes.

Figure 5-4 Drill holes



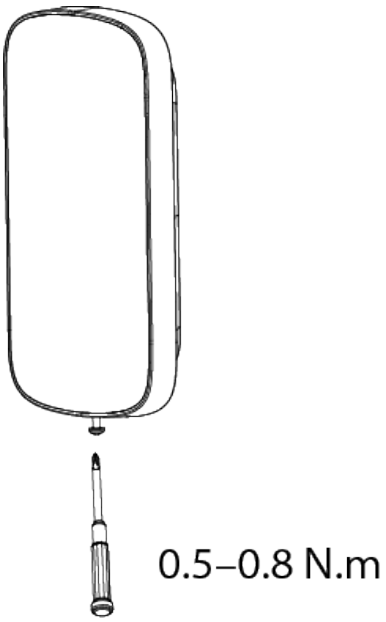
Step 4 Close the keypad.

Figure 5-5 Close the keypad



Step 5 Secure the keypad with screw.

Figure 5-6 Secure the keypad



6 Configuration

You can view and edit general information of the keypad.

6.1 Viewing Status

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

Table 6-1 Status

Parameter	Value
Temporary Deactivate	The status for whether the functions of the keypad are enabled or disabled. ● : Enable. ● : Only disable tamper alarm. ● : Disable.
Temperature	The temperature of the environment.
Signal Strength	The signal strength between the hub and the keypad. ● : Low. ● : Weak. ● : Good. ● : Excellent. ● : No.
Battery Level	The battery level of the keypad. ● : Fully charged. ● : Sufficient. ● : Moderate. ● : Insufficient. ● : Low.
Anti-tampering Status	The tamper status of the keypad, which reacts to the detachment of the body.
Online Status	Online and offline status of the keypad. ● : Online. ● : Offline.
Lock Status	The status for whether the keypad is locked or not. ● : Locked. ● : Unlocked.
Transmit through Repeater	The status of whether the keypad forwards its messages to the hub through the repeater.
Program Version	The program version of the keypad.

6.2 Configuring the keypad

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

Table 6-2 Keypad parameter description

Parameter	Description
Device Configuration	• View keypad name, type, SN and device model. • Edit keypad name, and then tap **Save** to save configuration.
Area	Select the area to which the keypad is assigned.
Control Permissions	Used to set which area the keypad can operate.
Temporary Deactivate	Whether send commands to the alarm hub. • Tap **Enable**, and then the keypad will send commands to the hub. **Enable** is set by default. • Tap **Only Disable Tamper Alarm**, and then the system will only ignore tamper alarm messages. • Tap **Disable**, and then the keypad will not send commands to the hub.
Keypad Config	Enable the keys on the keypad first and set if an event happens. • **Fire Alarm**: Enable by default. After enabling the **Fire Alarm**, when a fire is detected, you need to press and hold the fire key on the keypad for 3 seconds to trigger fire alarms. • **Link Fire Alarm to Siren**: Enable by default. After enabling the function, the siren and the buzzer will be linked when fire alarms are triggered. • **Emergency Alarm**: Enable by default. After enabling the **Emergency Alarm**, when an emergency is detected, you need to press and hold the emergency key on the keypad for 3 seconds to trigger emergency alarms. • **Link Emergency Alarm to Siren**: Enable by default. After enabling the function, the siren and the buzzer will be linked when emergency alarms are triggered. • **Medical Alarm**: Enable by default. After enabling the **Medical Alarm**, when a fire is detected, you need to press and hold the medical key on the keypad for 3 seconds to trigger fire alarms. • **Link Medical Alarm to Siren**: Enable by default. After enabling the function, the siren and the buzzer will be linked when medical alarms are triggered.

Parameter	Description
Keypad Lock Status	Set the number of attempts to enter the wrong passcode and lock time for the keypad. • Enable the keypad lock function first. • For the number of attempts to enter the wrong passcode within 30 minutes, you can select from 3 to 10 times. 5 is set by default. • For the lock time, you can select from 3, 5, 10, 20, 30, 60, 90 and 180 minutes. 3 minutes is set by default.
No Passcode Arming	Set whether you can use the keypad to arm the system without passcode. Disable by default. Enable **No Passcode Arming** function does not meet EN50131-1 certifications.
Transmit Power	Select from high, low, and automatic. The higher transmission power levels are, the further transmissions can travel, but power consumption increases. If you select **Low**, the keypad will enter into reduced sensitivity mode.
Card Reader Config	Enable card reader function and soft encryption function on the keypad. • **Card Reader**: Enable by default. If enabled, the keypad supports card recognition function. If disabled, the card reader function will be turned off. • **Soft Encryption**: Enable by default. If enabled, card information will be encrypted when issuing the card.
Backlight Brightness	Adjust backlit keypad brightness. You can select from **Off**, **Low** and **High**. When battery level is low, the backlight brightness will turn to **Low** automatically.
Buzzer Volume	Configure volume level of the buzzer. Select from **Off**, **Low**, and **High**.
Signal Strength Detection	Test the current signal strength. Signal strength test is not supported when the keypad is in the sleep mode. You can press any key to wake up the keypad.
Cloud Update	Update online.
Delete	Delete the keypad. Go to the hub screen, select the keypad from the accessory list, and then swipe left to delete it.

7 User Management

7.1 Adding Users

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

Only installer and admin users have permission to add users.

Procedure

Step 1 Go to the home screen.

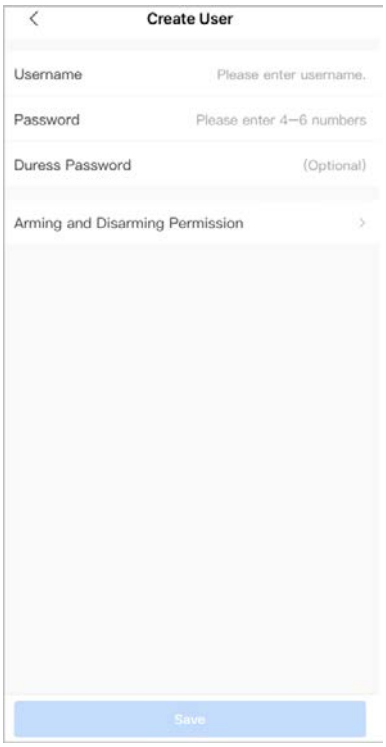
Step 2 Select a hub, and then select ▪▪▪▪ > **Device Details** > **Hub Setting** > **User Manager**.

Step 3 Tap ⊕ to add a user.

Step 4 Enter your username, passcode, and duress passcode, and then select arming and disarming permissions for the room.

- Passcode and duress code must be 4 to 6 digits.
- Duress passcode 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 7-1 Add a user



Step 5 Tap **Save**.

Related Operations

- Deleting a User

On the **User Manager** screen, select the user, and then swipe left to delete the user.

The admin user must be the last to be deleted.

- Modifying User's Information
  On the **User Manager** screen, select the user, and then you can modify user's information, including username, passcode, duress code and arming and disarming permission.

7.2 Adding 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 Manager**.
- Adding the card in the accessory list.

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

7.2.1 Adding Card on the User Manager

Step 1 Go to the home screen.

Step 2 Select a hub, and then select [redacted] > **Device Details** > **Hub Setting** > **User Manager**.

Step 3 Select the user to whom you want to link the card.

Step 4 Tap ⊕.

Step 5 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.

7.2.2 Adding Card in the Accessory List

Step 1 Go to the hub screen.

Step 2 Select **Accessory**.

Step 3 Tap ⊕, and then select **Add Card**.

Step 4 Press any key to wake up the keypad.

Step 5 Place the card near the card swiping area of the keypad to enter to the linking process.

Step 6 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 on adding a user, see "7.1 Adding Users".

Step 7 Tap **Completed**.

8 Operations

8.1 Frequently Used Commands

Following are frequently used commands for the keypad.

Before using the keypad, make sure you have created accounts on the DMSS or COS app.

Table 8-1 Command

Function	Command
Global away arming	Enter the password + + #.
Global home arming	Enter the password + + #.
No passcode arming	Press and hold or .
Global disarming	Enter the password + + #.
Away arming for a single room	Enter the password + * + Room No. + + #.
Home arming for a single room	Enter the password + * + Room No. + + #.
Disarming for a single room	Enter the password + * + Room No. + + #.
Searching for the room status	Enter the password + * + Room No. + #.
Clear	Press and hold #.

8.2 Waking Up the Keypad

Press and hold any key for more than 0.1 seconds to wake up the keypad. When you hear a short beep, and see all the indicator lights are solid, then you can use it.

- If you do not use the keypad for more than 4 seconds, the backlit 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 twice, all the indicator lights will turn off, and then the keypad will enter sleep mode.
- To wake up the keypad when it is offline, the communication indicator will flash green slowly, and other indicator lights, including arming and disarming, fault, and alarm indicators, will turn off.

8.3 Arming

- To arm all the rooms, you can enter the arming commands or swipe the card.

To arm the system without a passcode, you can enable the **No Passcode Arming** function first, and then press and hold or .

- To arm a single room, you can enter the relevant arming command.

  - If the arming is successful, the arming and disarming indicator light will flash blue 3 times slowly, and then will remain solid, with one short beep.
  - If the arming fails because of the potential faults, the arming and disarming indicator light will flash green twice quickly, and then it will go back to the normal status, with one long beep. And if you enter the same arming command again within 30 seconds, or swipe the same card again within 10 seconds, you can force arm the room.
  - If arming fails because of reasons such as using the wrong passcode or invalid card, or allowing people with no permission to use the keypad, the backlit light will flash twice quickly with one long beep.

  By swiping the card, you can only use global away arming.

8.4 Disarming

- If global disarming is successful, the arming and disarming indicator light will flash green 3 times slowly, and then turn off, with 2 short beeps.

  After successfully disarming the system, if there are system faults, the fault indicator light will flash yellow slowly.
- If disarming for a single room is successful, the arming and disarming indicator light will slowly flash green 3 times, and then it will go back to the normal status, with 2 short beeps.
- If disarming fails because of reasons such as using the wrong passcode or invalid card, or allowing people with no permission to use the keypad, the backlit light will flash twice quickly with one long beep.

  - If one or more rooms associated with the card are in the arming status, then all the associated rooms will be disarmed if you swipe the card.
  - If all the rooms associated with the card are in the disarming status, then all the associated rooms will be armed if you swipe the card.

8.5 Searching for the Room Status

You are only allowed to search for the status of a single room.

- If your search is successful, the keypad will beep once, and indicator lights will show the room status.

- The arming and disarming indicator light will glow blue for 6 seconds if the room is armed.
- The arming and disarming indicator light will slowly flash green 3 times slowly if the room is disarmed.
- The fault indicator light is solid on for 6 seconds if there are faults on the peripherals and the hub.
- The alarm indicator light is solid on for 6 seconds if alarm events occur in the room.

- If your search fails because of reasons such as using the wrong passcode or invalid card, or searching for a room that is not associated with the card, the backlit lights will flash 3 times quickly with one long beep. When the beep stops, the indicator light will go back to the normal status.

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.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883