Battery Bracket

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Battery Bracket (hereinafter referred to as the "Device"). 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.	September 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 to: 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 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.

Transportation Requirement

⚠

Transport, use and store the Device under allowed humidity and temperature conditions.

Storage Requirement

⚠

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to two or more kinds of power supplies, to avoid damage to the Device.
- Improper use of the battery might result in a fire or explosion.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Install the Device in a well-ventilated place, and do not block its ventilation.

- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- The device must be installed at a height of 2 meters or below.
- If the product has a metal case, we recommend you install it in an environment with a temperature lower than 40℃ (104°F) to avoid overheating and affecting your experience.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Ground the device to protective ground before you power it on.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- This product is professional equipment.
- The Device is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Product Introduction

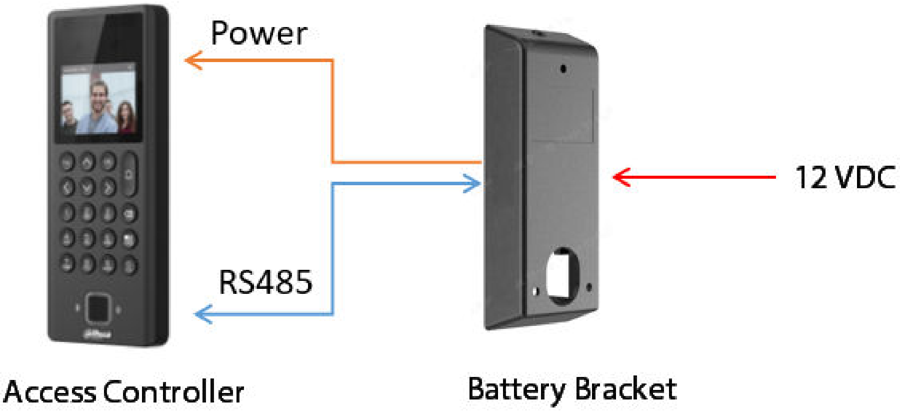
The battery bracket is a dedicated accessory designed for access control systems, providing uninterrupted power supply to all-in-one access control devices. Its core function lies in intelligent power management:

- During normal mains power: Primarily utilizes adapter power while simultaneously charging the battery.
- During power outages: Automatically shifts to backup battery power to sustain device operation.
- Upon power restoration: Reverts back to adapter power and immediately resumes charging the backup battery.

This design effectively addresses continuous operation challenges in unstable power supply scenarios, ensuring devices remain fully functional during brief power outages.

2 Network Diagram

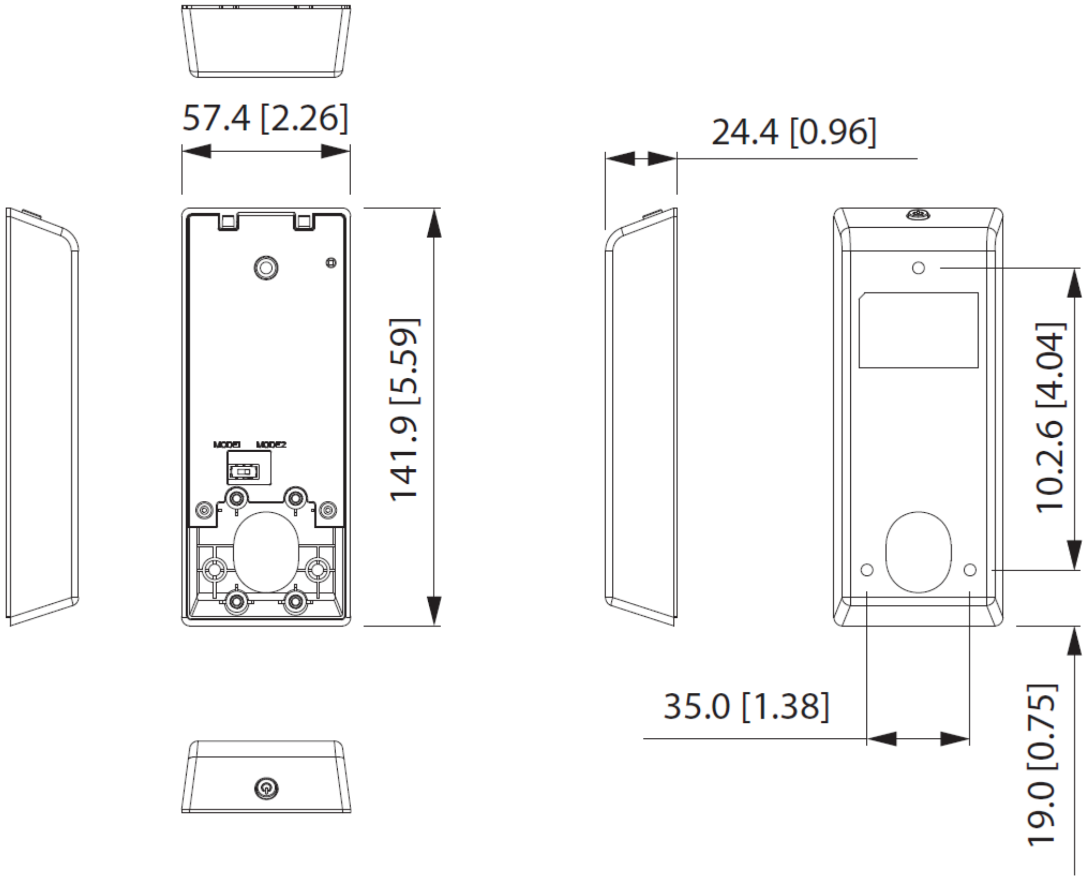
Figure 2-1 Network diagram



3 Dimensions

The figure below provides dimensions when planning the installation of the battery bracket.

Figure 3-1 Dimensions (mm[inch])



4 Appearance

Figure 4-1 Appearance

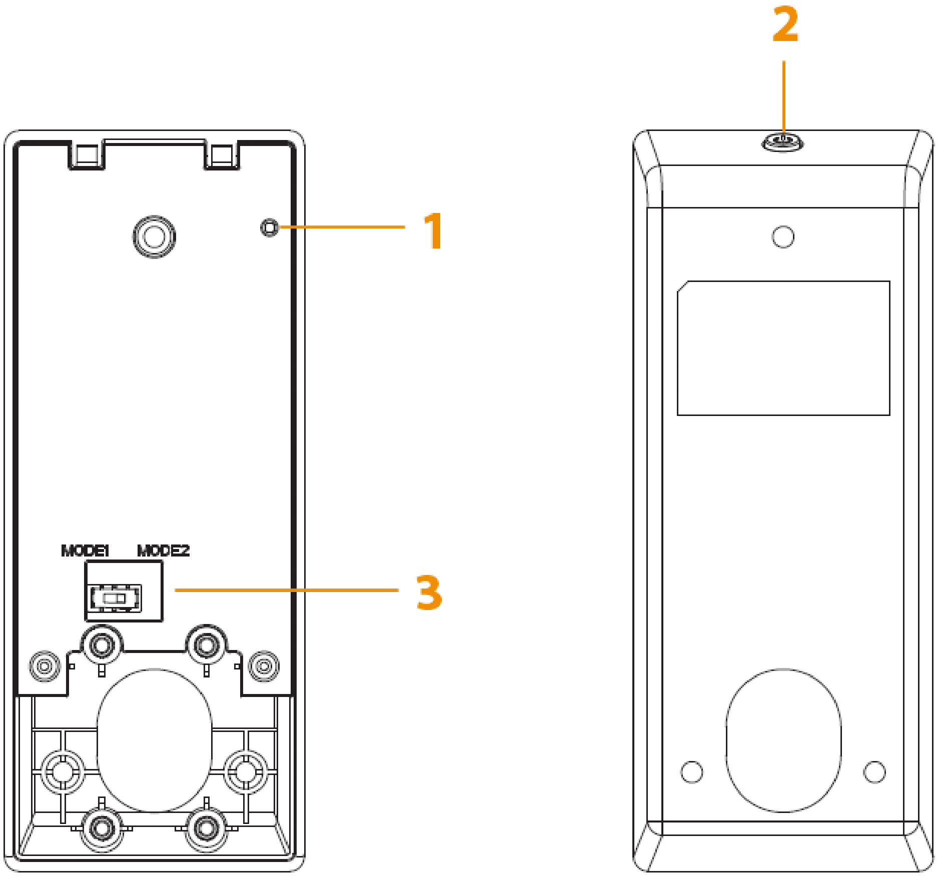


Table 4-1 Parameters description

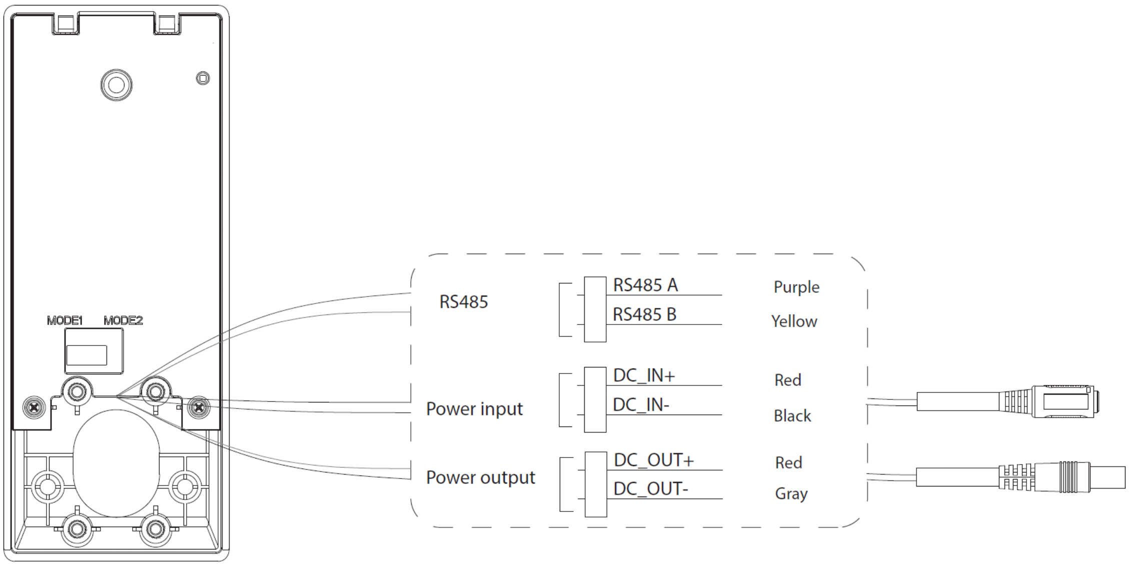
No.	Module Function	Description
1	Indicator	● Solid green: When 12V main power and battery supply power simultaneously. ● Solid red: Only when the battery supplies power. ● Solid blue: In the process of upgrading.

No.	Module Function	Description
2	Power button	● Without 12V main power: Press the power button briefly to turn on the device. ● With 12V main power connected: The device powers on automatically, without the need to press the button. 🕮 Press and hold the button for 3 seconds to power off. The actual powering off might vary depending on the DIP switch settings and whether the main power is connected. See the DIP switch description below for details.
3	DIP switch	● Mode 1: ◇ When 12 VDC main power is connected: The battery bracket and access controller cannot be turned off. ◇ When 12 VDC main power is disconnected: Press and hold the power button for 3 seconds to turn off the battery bracket and access controller. ● Mode 2: ◇ When 12 VDC main power is connected: Press and hold the power button for 3 seconds to turn off access controller. The battery bracket will not be turned off. 🕮 ○ If you want to turn on the access controller again, you need to press the power button. ○ If 12 VDC power is manually disconnected while the battery bracket is on (and the access controller is off), the bracket will automatically switch to battery power—indicated by its LED changing from green to red. The access controller remains powered off during this process. ◇ When 12V main power is disconnected: Press and hold the power button for 3 seconds to turn off both battery bracket and access controller.

5 Installation and Wiring

5.1 Wiring

Figure 5-1 Wiring



5.2 Installation Process

The installation supports in-wall wiring. Here uses model ASI32XXE as an example for illustration.

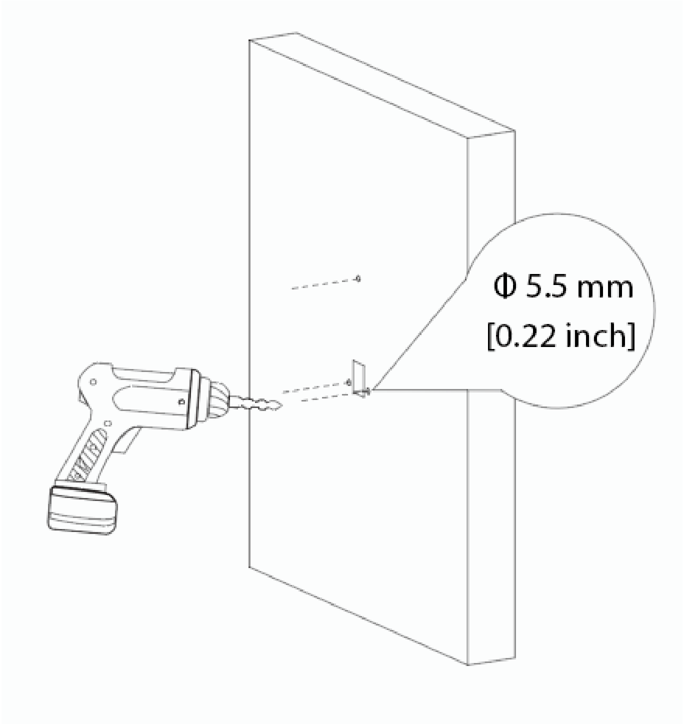
Procedure

Step 1 Level and mark the 3 mounting holes on the mounting surface.

See approximate dimensions in "3 Dimensions" for proper planning and installation.

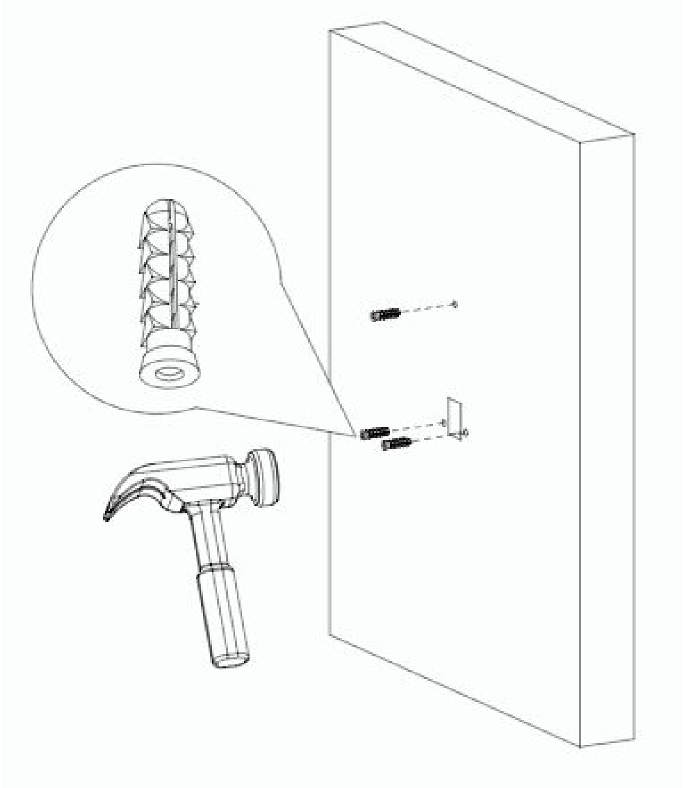
Step 2 Drill the 3 marked mounting holes into the mounting surface, and the put 3 expansion tubes into them.

Figure 5-2 Drill holes (In-wall wiring)



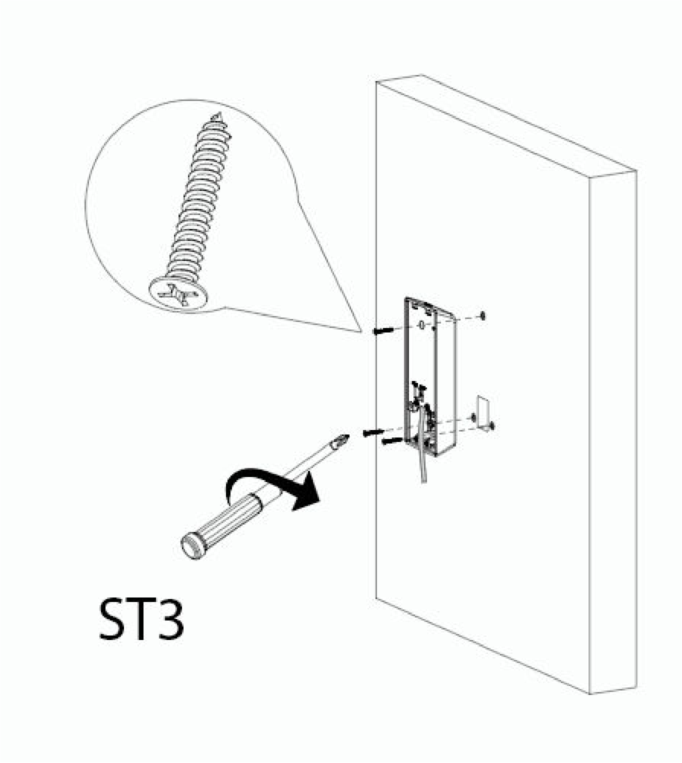
Step 3 Screw 3 expansion screws in the expansion tubes.

Figure 5-3 Screw 3 expansion screws



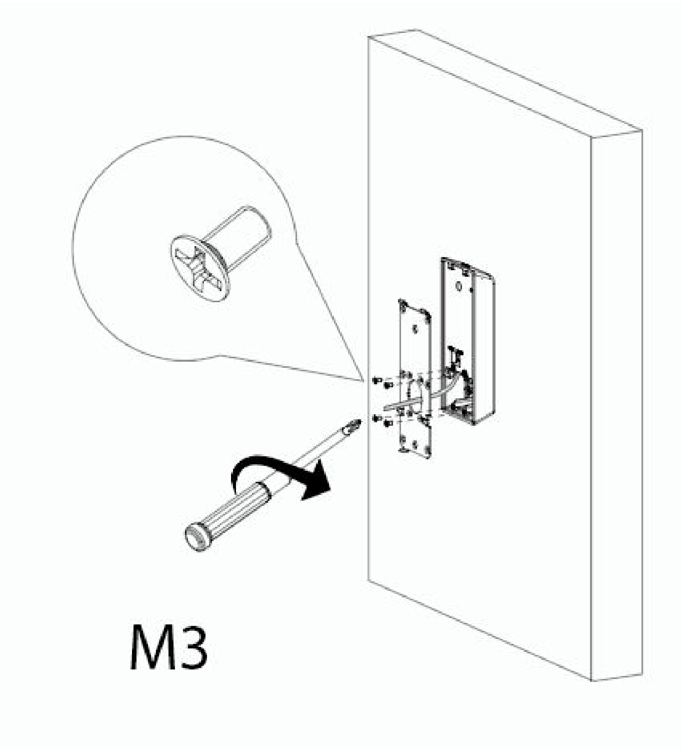
Step 4 Fix the battery bracket on to the wall using ST3 screws.

Figure 5-4 Fix battery bracket



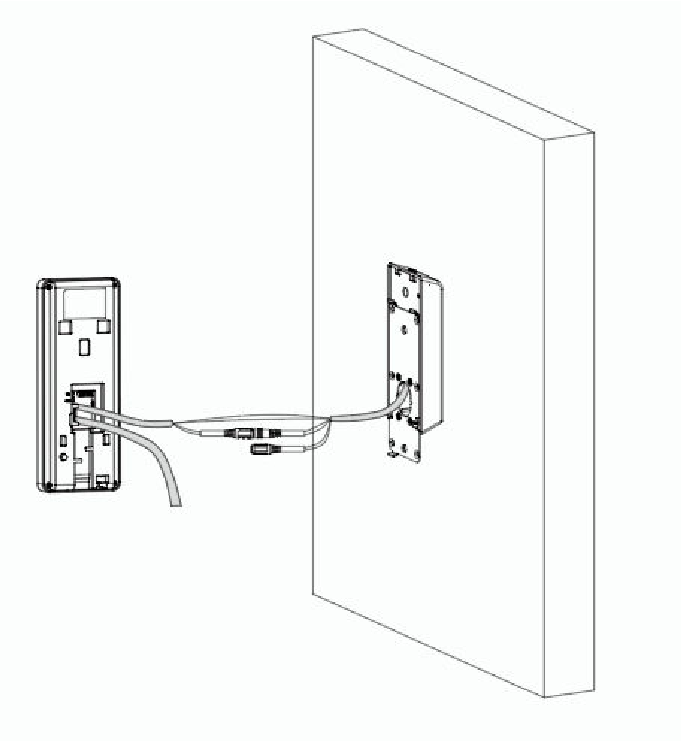
Step 5 Fix the installation bracket on to the battery bracket using 4 M3 screws.

Figure 5-5 Fix the installation bracket



Step 6 Run wires through the wire threading hole and into the opening in the wall.

Figure 5-6 Wiring



Step 7 Attach the access controller on to the battery bracket and then secure them with M2 screws.

Figure 5-7 Attach

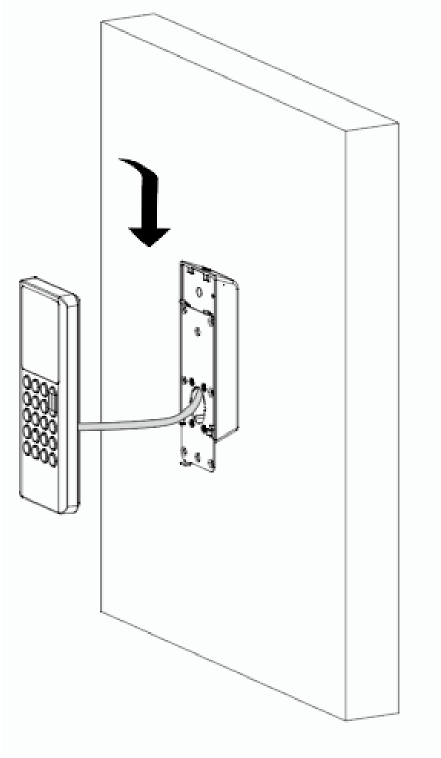
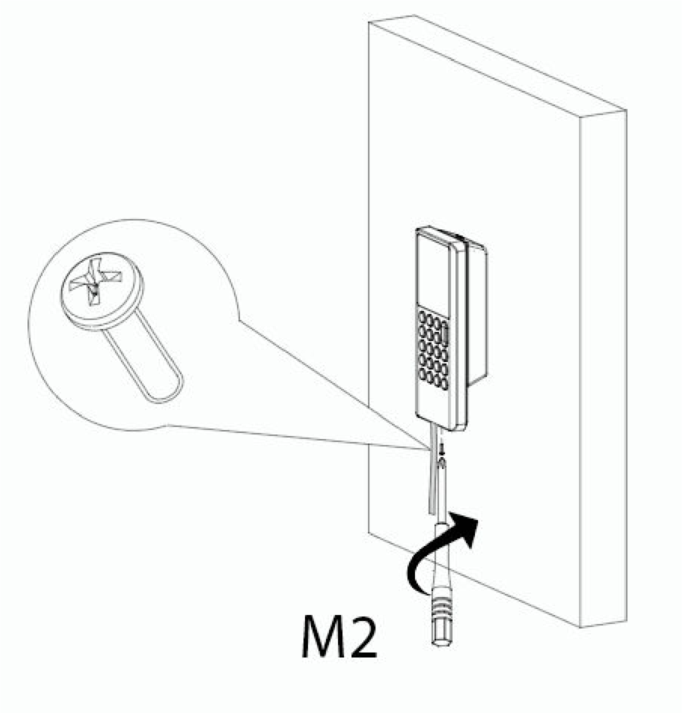
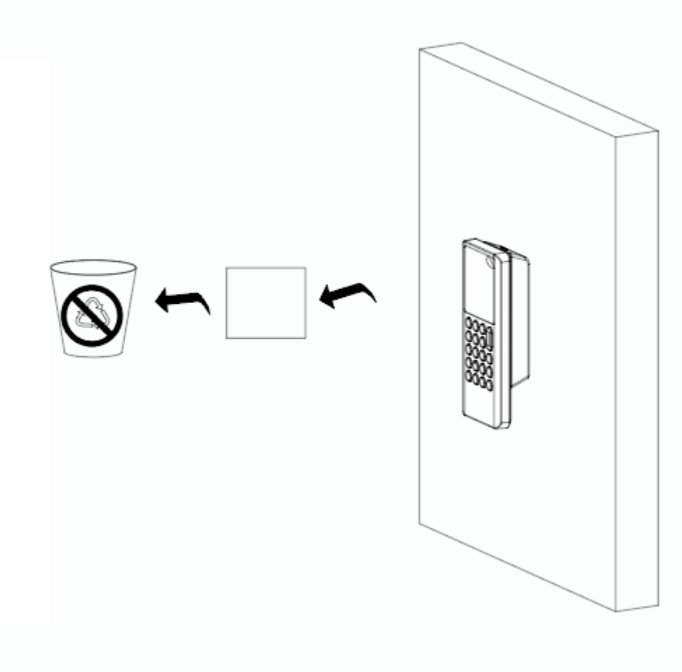


Figure 5-8 Secure



Step 8 Remove the protective film from the access controller.

Figure 5-9 Remove protective film



Appendix 1 Cybersecurity Recommendations

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.