Access Control Metal Case

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the Access Control Metal Case (hereinafter referred to as the "Metal Case"). 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.	April 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 Access Control Metal Case, hazard prevention, and prevention of property damage. Read carefully before using the metal case, and comply with the guidelines when using it.

Transportation Requirement

⚠

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

Storage Requirement

⚠

Store the metal case under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the metal case 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 metal case.
- Do not connect the metal case to two or more kinds of power supplies, to avoid damage to the metal case.
- Improper use of the battery might result in a fire or explosion.

⚠

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the metal case in a place exposed to sunlight or near heat sources.
- Keep the metal case away from dampness, dust, and soot.
- Install the metal case on a stable surface to prevent it from falling.
- Install the metal case 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the metal case label.
- The metal case is a class I electrical appliance. Make sure that the power supply of the metal case is connected to a power socket with protective earthing.

Operation Requirements

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the metal case while the adapter is powered on.
- Operate the metal case within the rated range of power input and output.
- Use the metal case under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the metal case, and make sure that there is no object filled with liquid on the metal case to prevent liquid from flowing into it.
- Do not disassemble the metal case without professional instruction.

Contents

1 Product Introduction

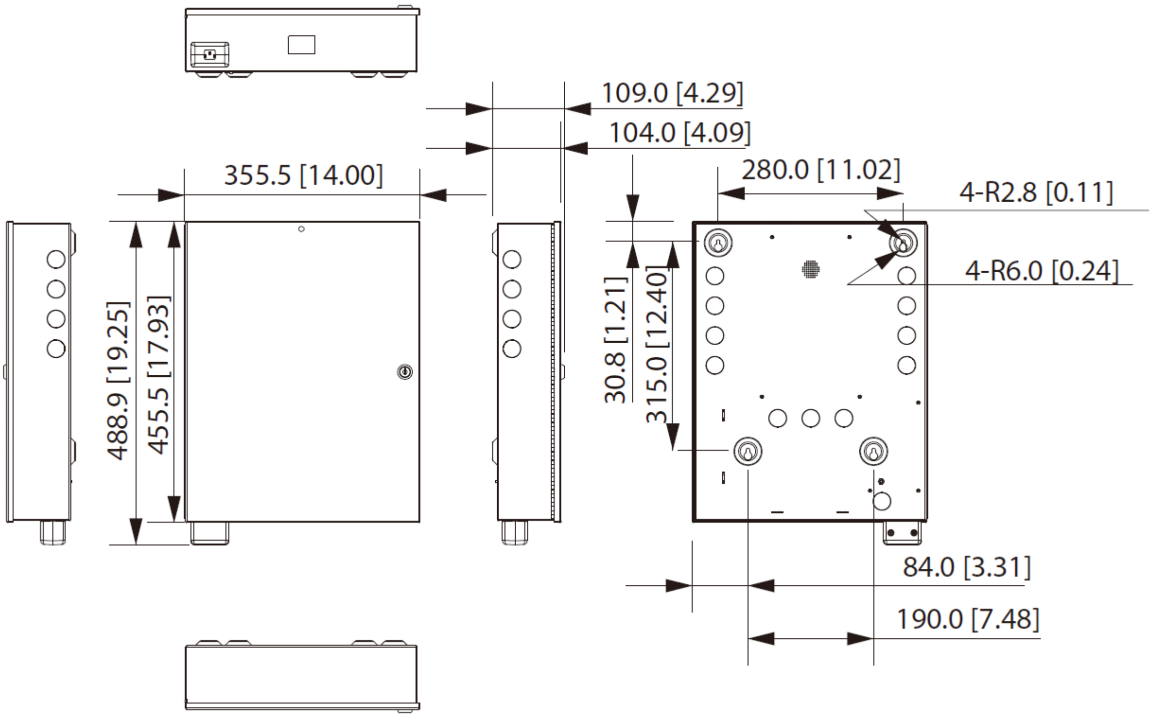
The metal case is designed to house the access controller in a sleek, protective enclosures, which is ideal in commercial parks, communities, and more.

- Made from galvanized steel plate, it is elegant and durable.
- Supports receiving power from mains electricity and its storage battery.
- Built-in air circuit breaker limits the current and protects the device from electricity leakage and short circuits.
- Built-in illuminator.
- Supports firmware update when used with the access controller. This function is only available on select models of access controller.
- Reports multiple types of events such as main electricity failure, mains electricity recovery, and tampering when used with the access controller. This function is only available on select models of access controller.
- Outputs anti-tampering alarms when used with the access controller. This function is only available on select models of access controller.

2 Dimensions

The figure below provides dimensions when planning the installation of the metal case.

Figure 2-1 Dimensions (mm[inch])



3 Appearance

Figure 3-1 Appearance

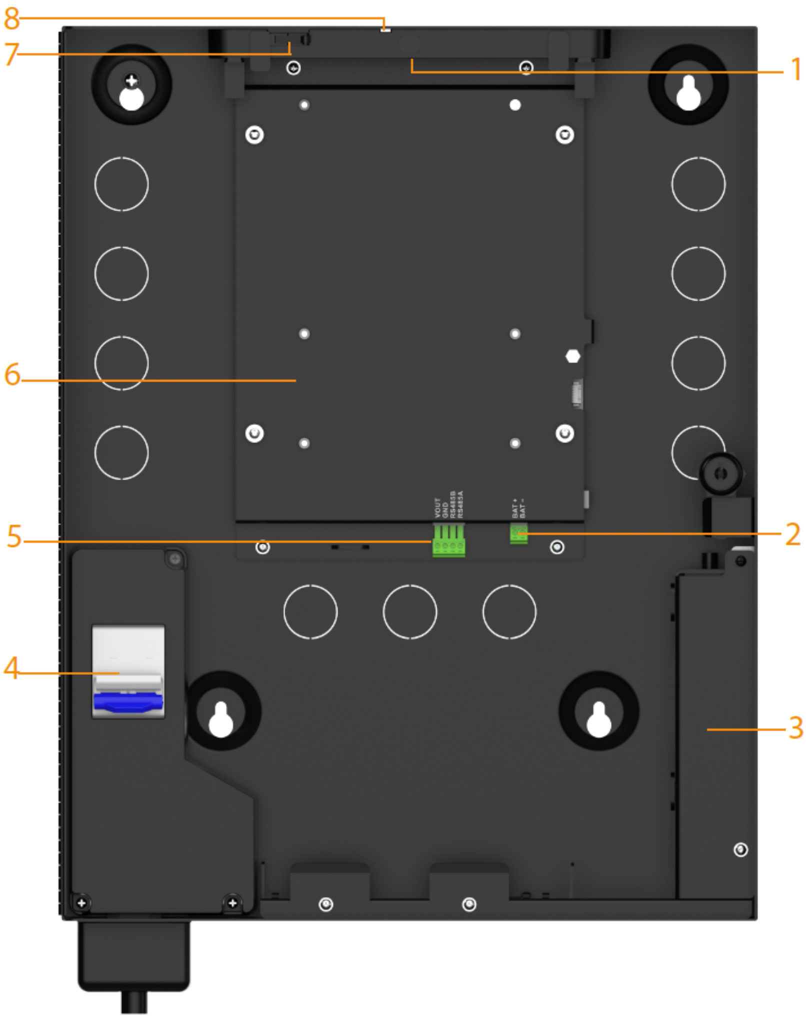


Table 3-1 Parameters description

No.	Module Function	
1	Illuminator	The illuminator light is on when the wall-mount box is opened and off when the box is closed.
2	Storage battery	● BAT+: Power input (12 V, 7 AH) ● BAT-: Grounding
3	Power adapter	Converts the incoming AC (Alternating Current) from your power outlet to a 15 VDC output and the maximum current is 4A. Supplies power to the power transfer board.
4	Circuit breaker	A circuit breaker is an electrical switch designed to protect electrical systems from damage caused by power leakage, short circuit and overloads.

No.	Module Function	
5	RS-485	● RS-485AB: Communicates with access controller ● VOUT: Supplies power to access controller. ● GND: Grounding
6	Power adapter board	Supplies power to and communicates with access controller.
7	Anti-tampering	An tampering alarm is triggered when tampering attacks occur.
8	Power indicator	The indicator is red when the metal case is powered on.

4 Wiring

Figure 4-1 Wring of web-based access controller

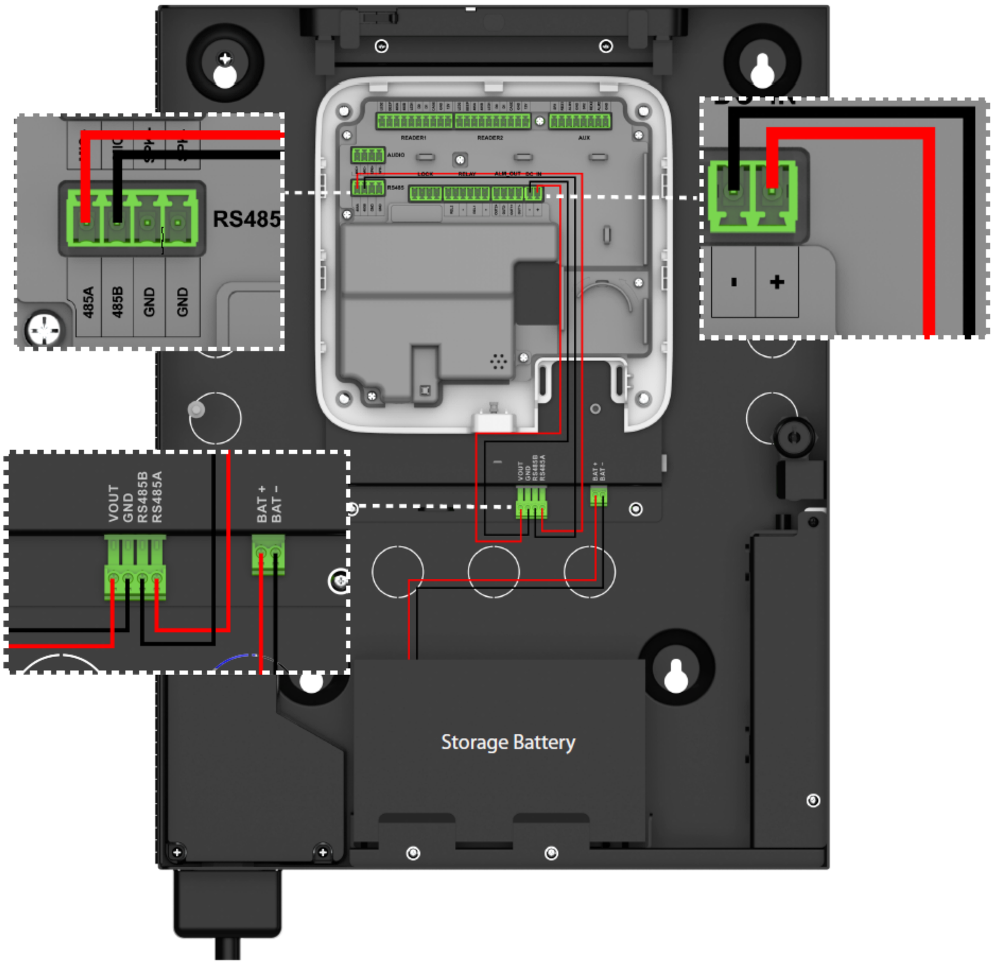


Figure 4-2 Wring of access controller (B) (Long model)

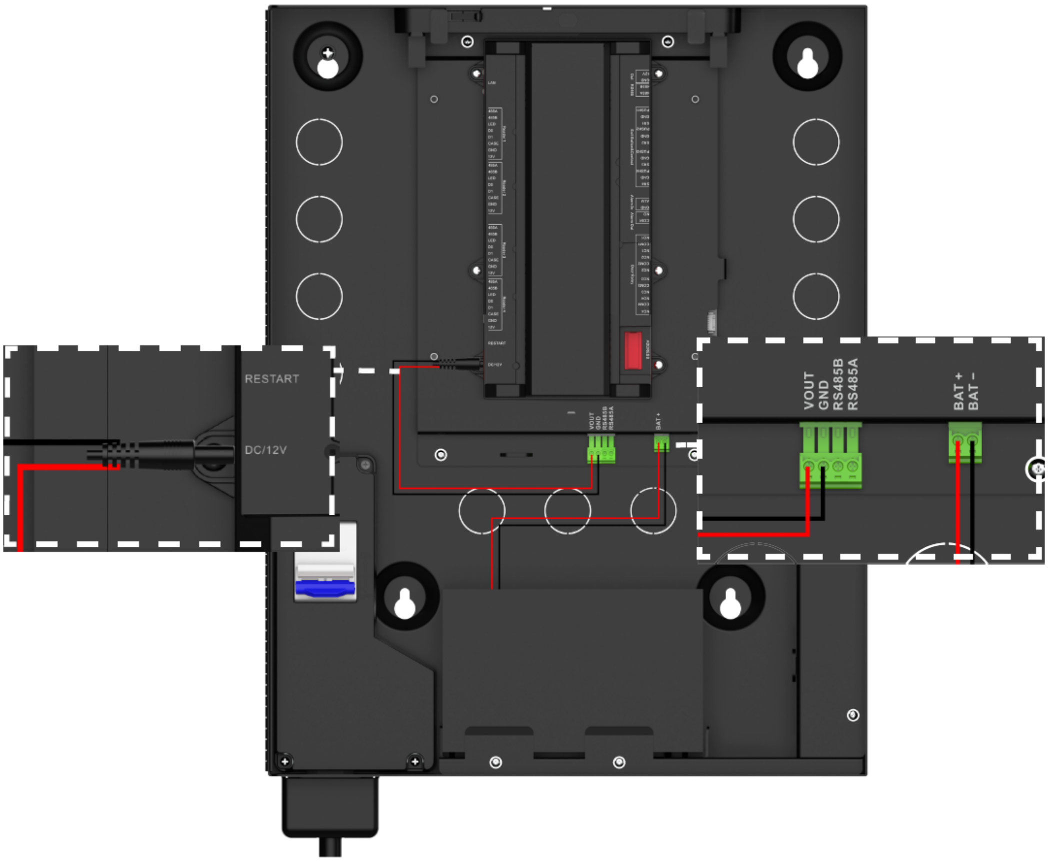
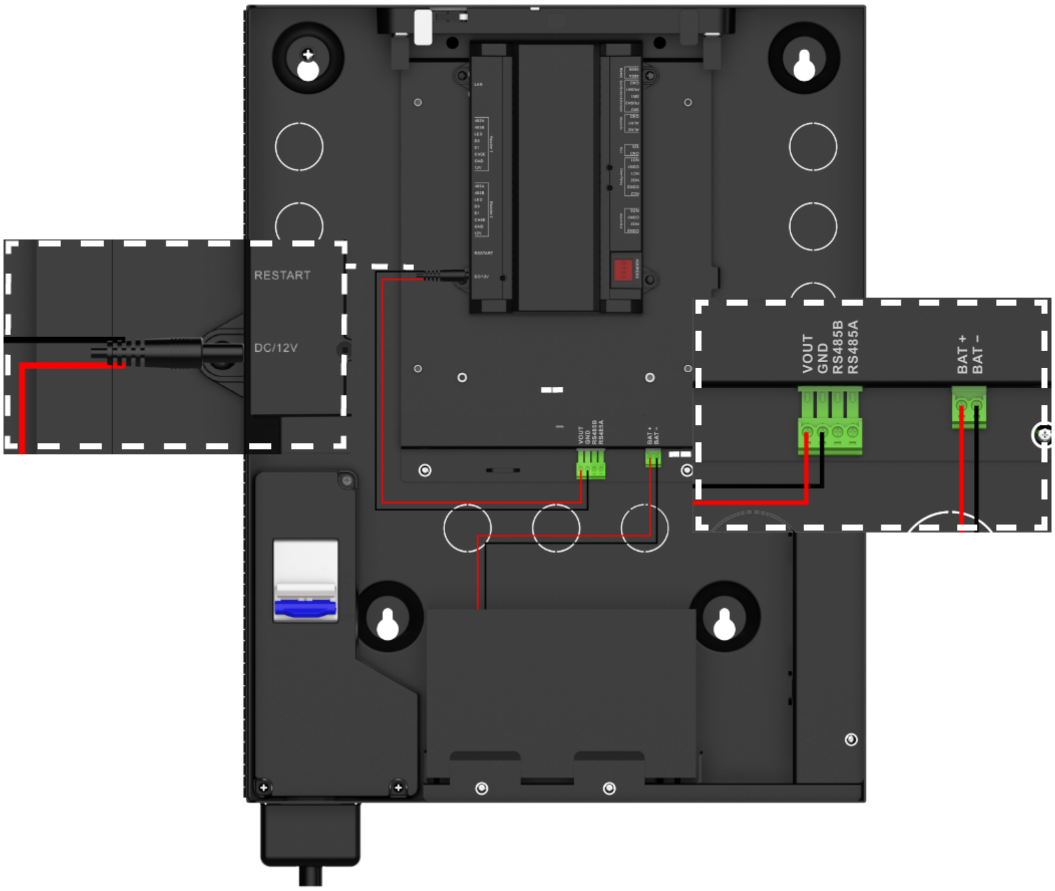


Figure 4-3 Wring of access controller (B) (short model)



5 Installation Process

The installation supports in-wall wiring and surface-mounted wiring. This section uses the in-wall wiring as an example.

Procedure

Step 1 Connect the power cord to the power port on the metal case, and then screw in 2 screws to attach the power cord protector to the metal case.

Step 2 Level and mark the four mounting holes on the mounting surface.

See approximate dimensions in “2 Dimensions” for proper planning and installation.

Step 3 Drill the 4 marked mounting holes into the mounting surface, and the put 4 expansion tubes into them.

Figure 5-1 Drill holes (In-wall wiring)

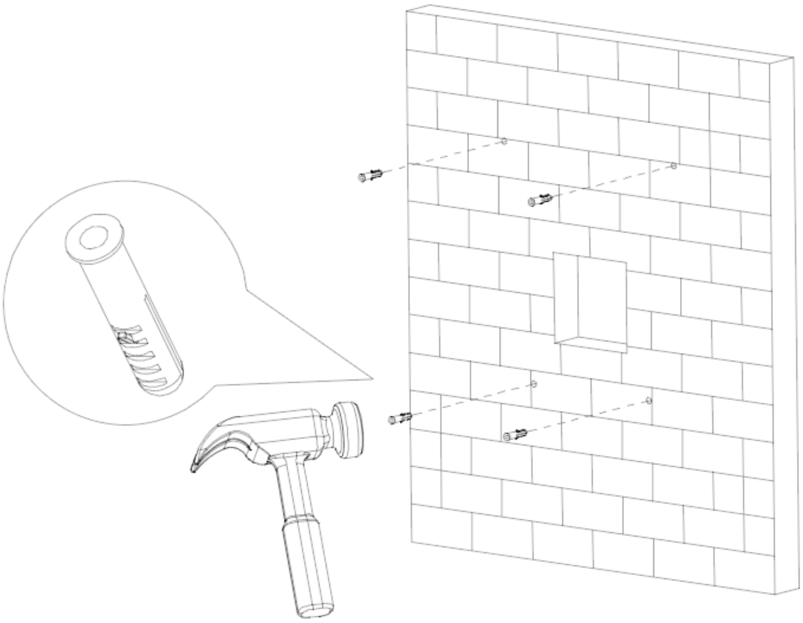
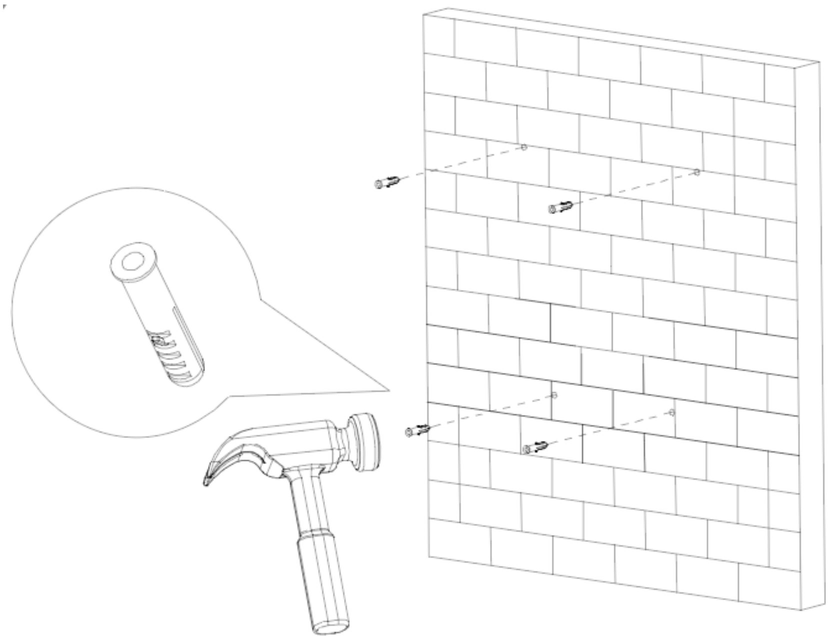
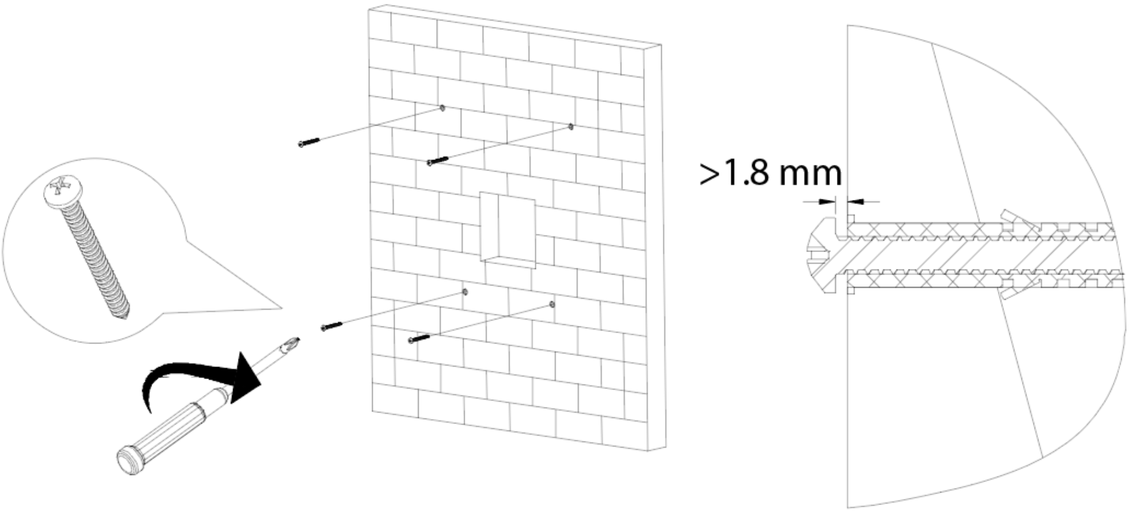


Figure 5-2 Drill holes ((Surface-mounted wiring)



Step 4 Screw 4 expansion screws in the expansion tubes, but leave enough space to hang the metal case.

Figure 5-3 Screw 4 expansion screws



Step 5 Press the edge of a screwdriver against the inner-most KO's stamped edge to gently push the KO away from the metal case.

A "knock out" or "KO" is a partially stamped opening in the metal case for running wires or cables. There will likely be several KOs of different sizes in the metal case. Pick the one that will be easiest to connect wires or cables.

Step 6 Run wires through the knock outs and into the opening in the wall.

Figure 5-4 Remove knock-outs and wire the metal case (In-wall wiring)

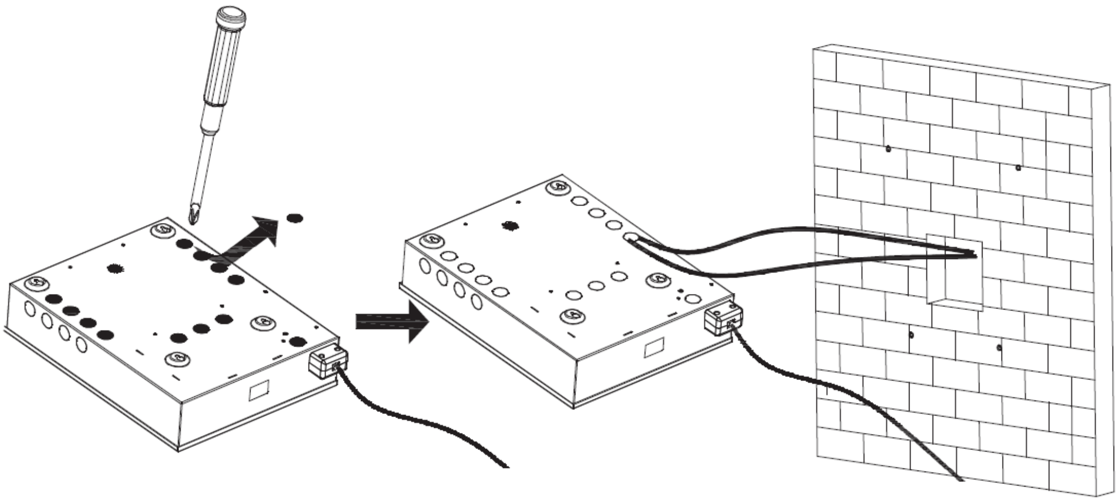
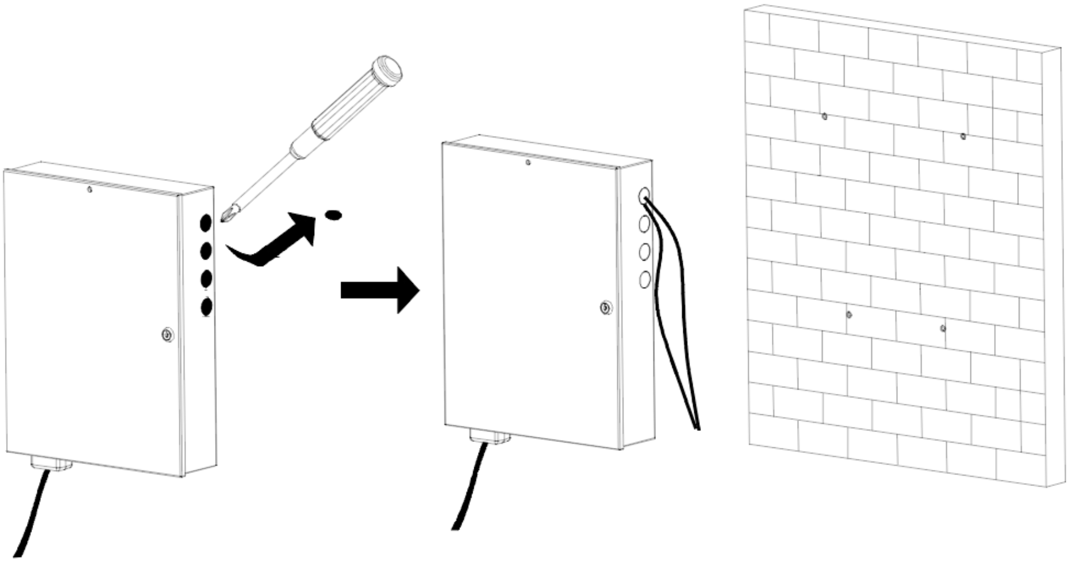


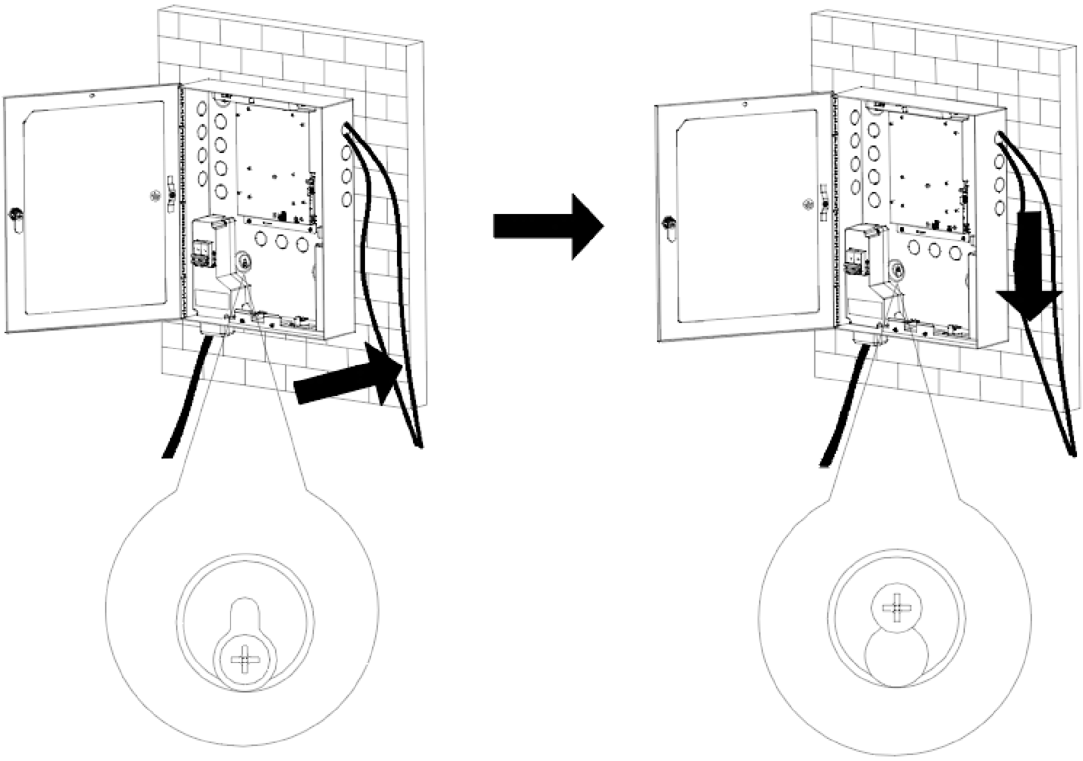
Figure 5-5 Remove knock-outs and wire the metal case (Surface-mounted wiring)



Step 7 Align the 4 keyhole slots on the metal case with the 4 installed screws, and then attach the metal case to the screws.

Step 8 Gently slide the metal case down until all 4 screws are at the top of each keyhole slot.

Figure 5-6 Slide the box downward



Step 9 Tighten the 4 screws and lock the metal case with its key.

6 Configuring on the Webpage

When the metal case works with the access controller, it can connect to the access controller with RS-485, which supports sending events of the metal case to the webpage of the access controller such as anti-tampering events, main electricity failure and mains electricity recovery events. You can also update the system of the metal case through the access controller.

Background Information

This function is only available on select models of the access controller.

Procedure

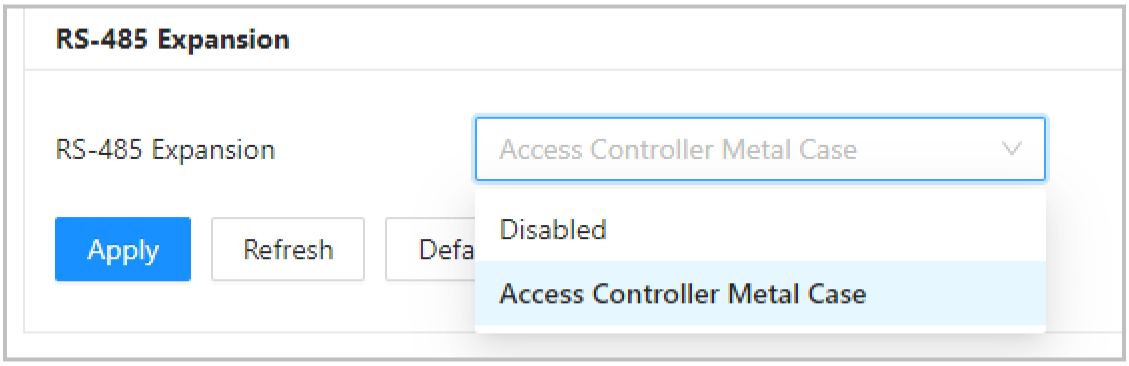
Step 1 Log in to the webpage of the access controller.

Step 2 Go to **Local Device Config** > **Advanced Settings** > **RS-485 Expansion** .

Step 3 Select **Access Controller Metal Case**.

Step 4 Click **Apply**.

Figure 6-1 Configure the metal case on the webpage



RS-485 Expansion

RS-485 Expansion: Access Controller Metal Case

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.