Access Standalone

User's Manual



V1.0.0

Foreword

General

This manual introduces the functions and operations of the Access Standalone (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.
ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
ELECTRIC SHOCK	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
LASER RADIATION	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
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 2024

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: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

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.

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

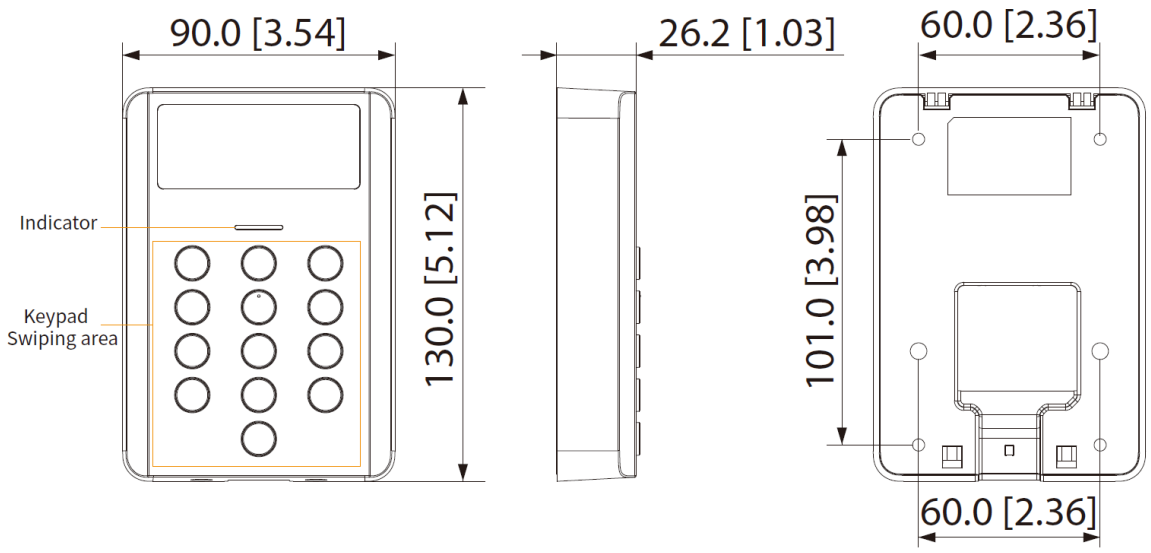
Foreword I
Important Safeguards and Warnings III
1 Product Overview 1
2 Appearance and Dimensions 2
3 Wring and Installation 3
3.1 Installation Environment 3
3.2 Wiring 5
3.3 Installation Process 6
3.3.1 Wall Mount 6
3.3.2 86 Box Mount 7
4 Configuration 9
4.1 Initialization 9
4.2 Main Menu 9
4.3 Prompts 9
4.4 User Management 9
4.4.1 Adding Users 9
4.4.2 Deleting User 10
4.5 Configuring Door Unlock Mode 10
4.6 Configuring Unlock Duration 10
4.7 Configuring Door Sensor 11
4.8 Password Management 11
4.8.1 Changing the Administrator Password 11
4.8.2 Adding Public Password 11
4.8.3 Deleting Public Password 12
4.9 Main Card Management 12
4.9.1 Adding Main Card 12
4.9.2 Deleting Main Card 12
4.9.3 Managing User Cards through Main Card 13
4.10 Configuring Door Timeout Period 13
4.11 Restoring to Factory Settings 13
4.12 Unlocking the Door 13
4.12.1 Unlocking by Card 13
4.12.2 Unlocking by Card + Password 14
4.12.3 Unlocking through Public Password 14
Appendix 1 Security Recommendation 15

1 Product Overview

This product is an access control equipment integrating card reading, configuration and execution. The appearance of the product is simple and fashionable, and it is suitable for office buildings, schools, parks, communities, factories, public venues, business centers, government buildings and other application scenarios.

2 Appearance and Dimensions

Figure 2-1 Appearance and dimensions (unit: mm [inch])



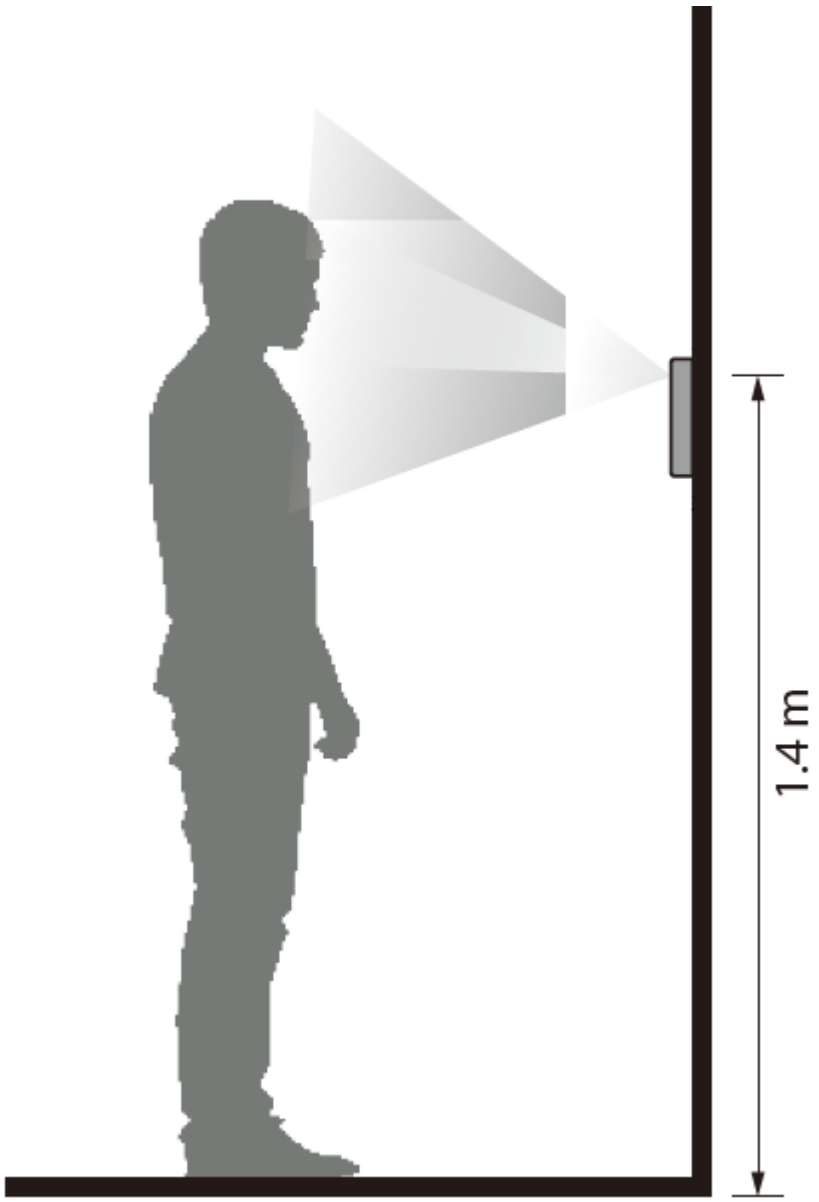
3 Wring and Installation

3.1 Installation Environment

- The light 0.5 meters away from the Access Standalone should be no less than 100 Lux.
- We recommend you install the Access Standalone indoors, at least 3 meters away from windows and doors, and 2 meters away from the light source.
- Avoid backlight, direct sunlight, close light, and oblique light.

Installation Height

Figure 3-1 Installation height requirement



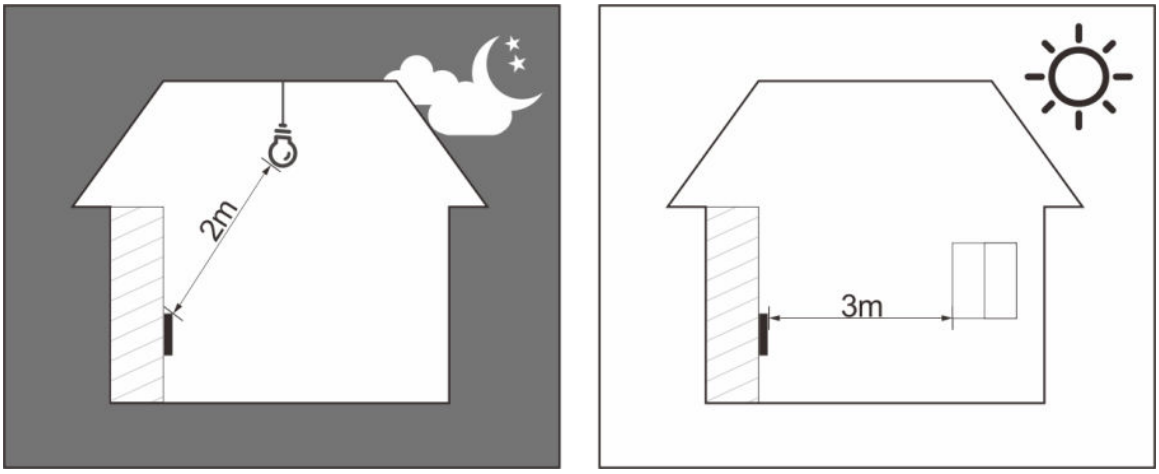
Ambient Illumination Requirements

Figure 3-2 Ambient illumination requirements



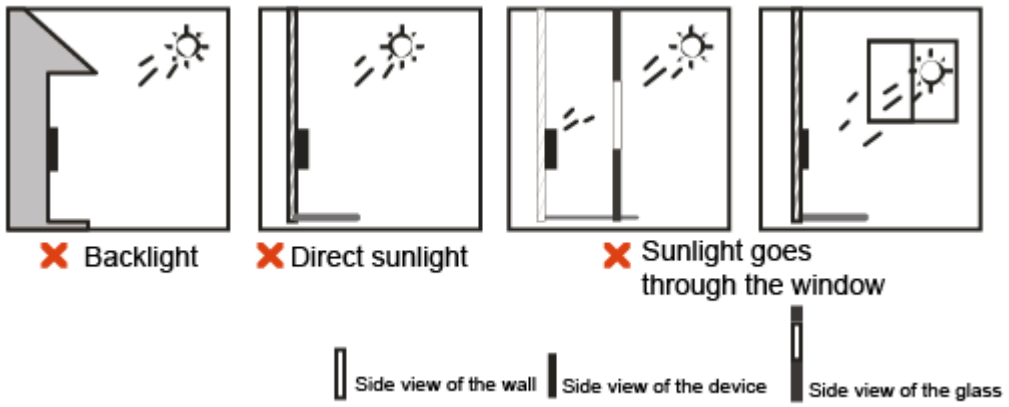
Recommended Installation Locations

Figure 3-3 Recommended installation locations



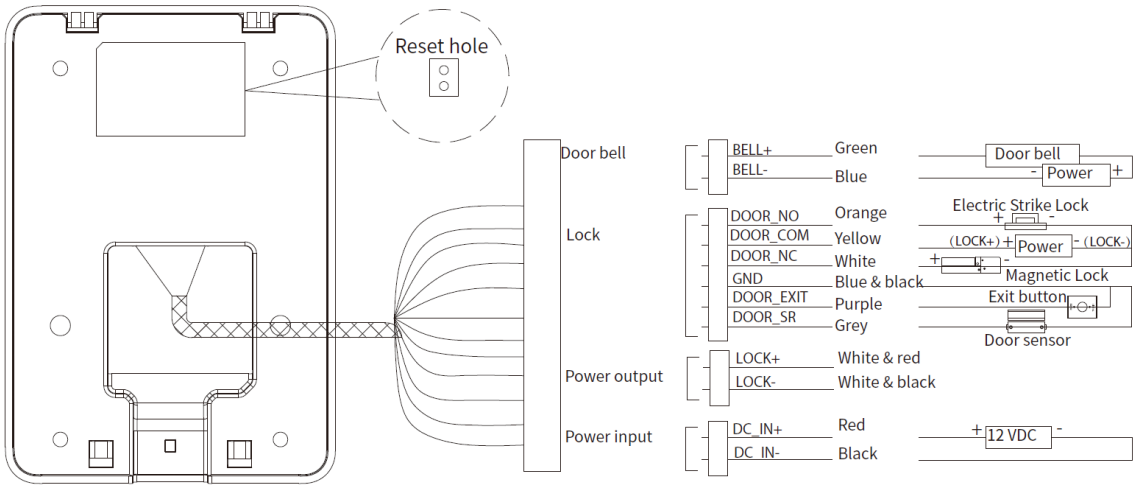
Installation Locations Not Recommended

Figure 3-4 Installation locations not recommended



3.2 Wiring

Figure 3-5 Wiring



The Device (connects lock + and lock-) or a separate power source supplies power for the lock. When the power supply distance exceeds 30 m, it is recommended to supply power for the lock through a separate power source.

- Hardware factory reset: Within 5 minutes after the Device starts, use tweezers to short-circuit the reset hole.
  - ◇ If the short-circuit time is less than 5 seconds, the Device is restored to the factory settings and the user information is retained. All are restored to the factory settings except the user and public password.
  - ◇ If the short-circuit time is no less than 5 seconds, the Device is restored to the factory settings and all information is restored.

Figure 3-6 Lock power supply wiring

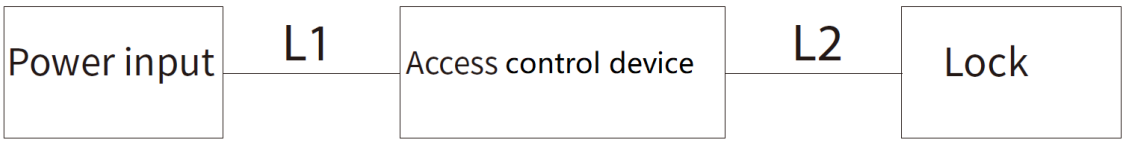


Table 3-1 Cable selection

No.	Name	Recommended model and specification	Maximum power supply distance (17AWG cable, impedance ≤ 2Ω per meter)
L1	Power cord	2-core 17AWG cable	• The Device: L1 cannot exceed 100 m. • The Device and the lock: L1 + L2 no more than 30 m.
L2	Lock wire	2-core 17AWG cable, 4-core 17AWG cable, or category 5e cable	

- If the lock is powered by the Device, it is recommended that the maximum current of the lock should not exceed 1000 mA. The lock supports wide voltage operation, and the allowed minimum operating voltage should not exceed 10 V.
- The wiring distance of L1 and L2 is affected by the voltage of power supply and the specification of power supply cables. In actual construction, the power supply voltage must not be lower than the allowed minimum operating voltage of the access control device and the lock.
- Use category 5e cable (per kilometer impedance ≤ 9 Ω) to supply power for the lock. Except for the signal lines, the rest of lines must be evenly distributed to supply power for the lock to minimize the power loss.

3.3 Installation Process

3.3.1 Wall Mount

Procedure

Step 1 Loosen one screw at the bottom of the Device and remove the back panel.

Step 2 According to the hole position of the back panel, drill 4 holes on the wall and insert expansion tubes into the holes.

For in-wall wiring, you need drill another hole through the wall for wiring purposes.

Step 3 Use the four self-tapping screws (ST3) to fix the back panel to the wall.

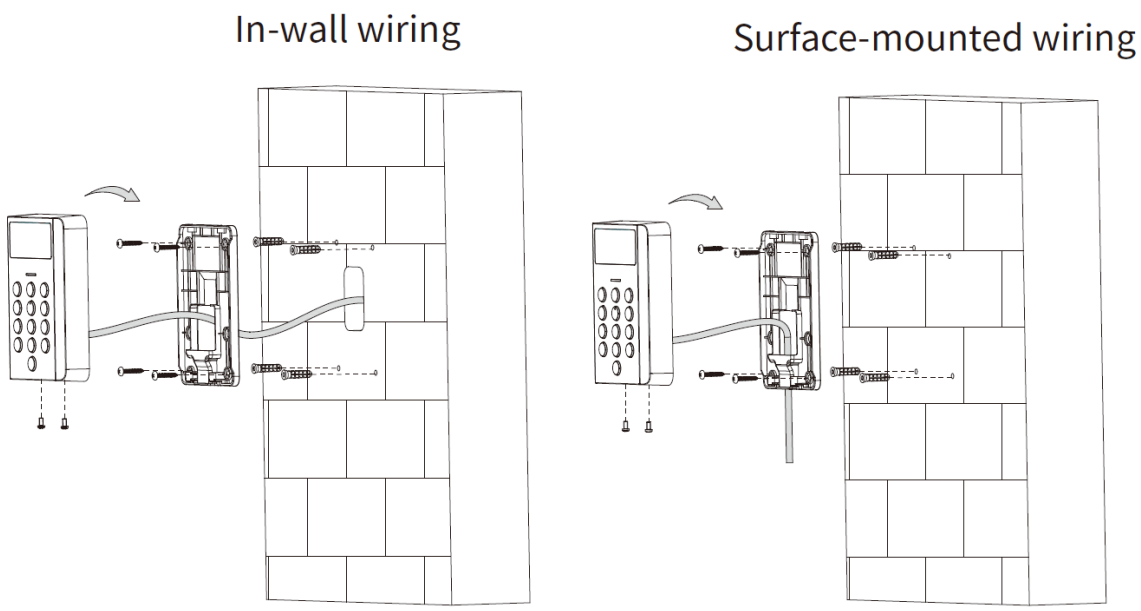
For surface-mounted wiring, pass the wire through the back panel before you fix the back panel to the wall.

Step 4 Wire the Device. For details, see "3.2 Wiring".

Step 5 Attach the Device to the back panel.

Step 6 Screw in two screws from the bottom of the Device securely.

Figure 3-7 Wall mount



3.3.2 86 Box Mount

Procedure

Step 1 Loosen one screw at the bottom of the Device and remove the back panel.

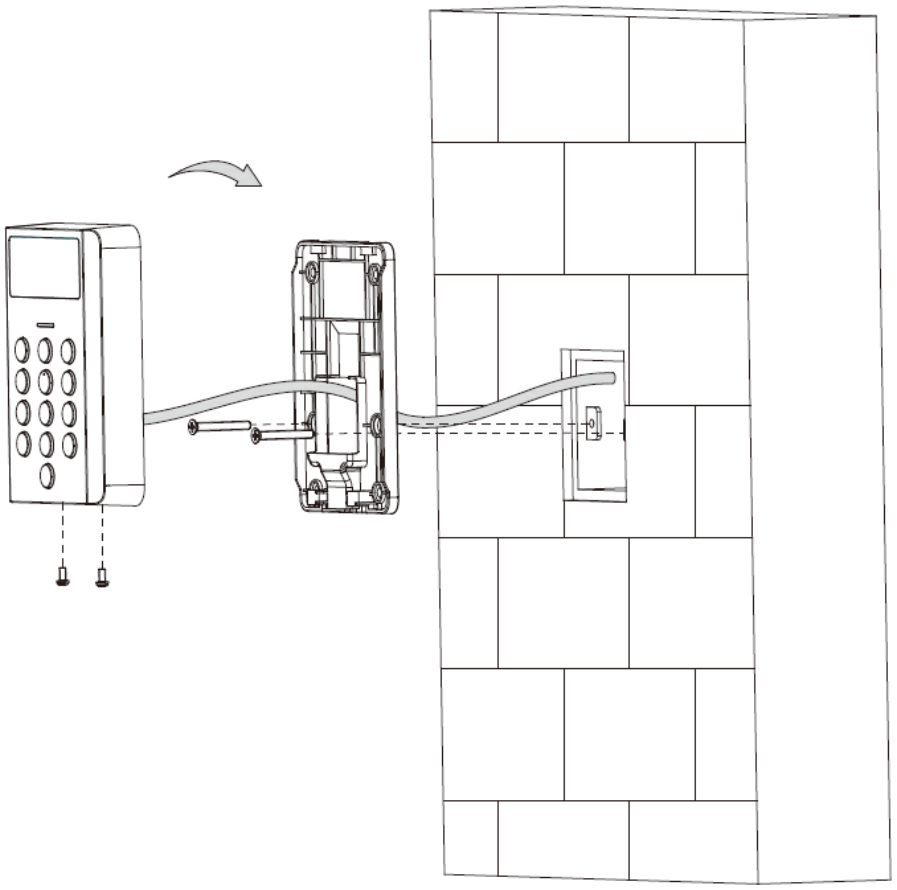
Step 2 Mount the back panel to the 86 box with two M4 screws.

Step 3 Wiring the Device. For details, see"3.2 Wiring".

Step 4 Attach the Device to the back panel.

Step 5 Screw in 2 screws from the bottom of the Device securely.

Figure 3-8 86-box mount



4 Configuration

4.1 Initialization

After the Device is powered on for the first time, you need to set the administrator password. The administrator password is used to enter the main menu of the Device.

Procedure

Step 1 Power on the Device, and the indicator light will flash red slowly.

Step 2 Press **#** , enter the administrator password, and then press **#**.

The password must be 1 to 8 characters in length.

If the indicator light is solid blue, it means the Device is initialized.

4.2 Main Menu

Press **#** , enter the administrator password, and then press **#**.

- The indicator flashes blue, and it means you have entered the main menu.
- The indicator flashes red once, the buzzer generates a beep sound, and then the indicator turns solid blue, which means the password is wrong.

4.3 Prompts

- The indicator flashes green once, and the buzzer makes a beep sound, which means that the operation or access control verification is successful.
- The indicator flashes red once, and the buzzer makes three beep sound, which means that the operation or access control verification failed.
- If the indicator flashes red slowly, it means the Device is not uninitialized.
- If the indicator is solid blue, it means the Device is in the standby status.
- The indicator flashes blue, it means the Device enters the main menu.

4.4 User Management

4.4.1 Adding Users

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **1** and **#** to add users.

Step 3 After swiping the card, press **#** to add the card.

Step 4 Enter the user password, and then press **#**.

If you do not need to set the user password, press **#** to skip it.

The password can be 1 to 8 characters in length.

Step 5 Repeat Step 3 to Step 4 to add more users.

After adding the user, press * to return to the main menu, and then press * to return to the standby status.

4.4.2 Deleting User

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **2** and #.

Step 3 Delete a user.

- Swipe the card, and then press #.

  If you swipe a card that has not been added, the deletion fails.
- Enter 0000, and then press # to delete all users.

After deletion, press * to return to the main menu, and then press * to exit the main menu.

4.5 Configuring Door Unlock Mode

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

Step 2 Press **3** and #.

Step 3 Select the unlock mode.

- Press **0** and # to set unlocking by card.
- Press **1** and # to set unlocking by card and user password.

Step 4 Press * to exit the main menu.

4.6 Configuring Unlock Duration

The door remains open after a defined time after it unlocks, which allows people to pass through.

Procedure

Step 1 Press # , enter the administrator password, and then press #.

Enter the main menu and the indicator flashes blue.

Step 2 Press **4** and #.

Step 3 Enter the time, and then press #.

The value ranges from 1 s to 600 s. The default value is 3 s.

Step 4 Press * to exit the main menu.

4.7 Configuring Door Sensor

After the door sensor is enabled, the door timeout alarm is enabled at the same time by default. If the door stays open after the set door timeout period, the buzzer of the Device generates alarms.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **5** and **#**.

Step 3 Enable or disable the door sensor.

The door sensor is disabled by default.

- Press **0** and **#** to enable the door sensor.
- Press **1** and **#** to disable the door sensor.

Step 4 Press * to exit the main menu.

4.8 Password Management

4.8.1 Changing the Administrator Password

To ensure device security, we recommend that you change the administrator password from time to time.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **0** and **#**.

Step 3 Enter the new password, and then press **#**.

Step 4 Enter the new password again, and then press **#**.

Step 5 Press * to exit the main menu.

4.8.2 Adding Public Password

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **6** and **#**.

Step 3 Enter the public password, and then press **#**.

The password can be 1 to 8 characters in length.



You can add up to 500 public passwords. Repeat step 3 to add more public passwords. Public password cannot be repeated.

Step 4 Press * to exit the main menu.

4.8.3 Deleting Public Password

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **7** and **#**.

Step 3 Enter the public password and press **#**.

Repeat step 3 if you want to delete more public passwords.

Step 4 Press ***** to exit the main menu.

4.9 Main Card Management

4.9.1 Adding Main Card

After adding the main card, you can quickly add and delete other user cards through the main card.

Background Information

The main card cannot be used to unlock the door.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **8** and **#**.

Step 3 Swipe the card, and then press **#**.

User cards that have been added can also be set as main card.

- If a user card is set to main card, it will not be able to unlock the door.
- Only supports one main card. If a new main card is added, the old main card will be overwritten.

Step 4 Press ***** to exit the main menu.

4.9.2 Deleting Main Card

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **9** and **#**.

Step 3 Swipe the card, and the press **#**.

Step 4 Press ***** to exit the main menu.

4.9.3 Managing User Cards through Main Card

If no operation is performed in 3 seconds after you swipe the main card, the Device enters the main card mode, and the Device will determine the corresponding function according to the swipe times of the main card. In the main card mode, the indicator flashes red and blue alternately, and if there is no operation for 10 seconds or you swipe the main card again for one time, it returns to the standby status.

- Add user card: Swipe the main card once, and then swipe the user card to add it. User cards can be added continuously.
- Delete the user card: Swipe the main card twice, and then swipe the user card to delete it. User cards can be deleted continuously.
- Clear all user cards: Swipe the main card 5 times in a row.

4.10 Configuring Door Timeout Period

After the door sensor is enabled, if the door stays open after the set time, the buzzer of the Device will give an alarm.

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu and the indicator flashes blue.

Step 2 Press **10** and **#**.

Step 3 Enter the door timeout period, and then press **#**.

The value range is from 1 s to 9999 seconds. The default value is 60 seconds.

Step 4 Press * to exit the main menu.

4.11 Restoring to Factory Settings

Procedure

Step 1 Press **#** , enter the administrator password, and then press **#**.

Enter the main menu, and the indicator flashes blue.

Step 2 Press **11** and **#**.

Step 3 Restore the Device to factory settings.

- Press **00** and **#** to restore factory settings (retain user information).
- Press **000** and **#** to restore factory settings (restore all information).

4.12 Unlocking the Door

4.12.1 Unlocking by Card

Swipe the user card to unlock the door.



If a user card is set to main card, it will not be able to unlock the door.

4.12.2 Unlocking by Card + Password

If you set the unlock mode to **Card + Password** , swipe the user card and enter the user password, and then press **#** to unlock the door.

4.12.3 Unlocking through Public Password

Enter the public password, and then press **#** to open the door. For details on how to set public passwords, see "4.8.2 Adding Public Password".



Public password can be used to unlock the door in any unlock modes.

Appendix 1 Security Recommendation

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**

   The 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, it is recommended 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 Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.
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**

   It is recommended 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).