Access Reader

LXK101-BD

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the access reader. 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.
📖 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	October 2024

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 reader, hazard prevention, and prevention of property damage. Read carefully before using the Card Reader, and comply with the guidelines when using it.

Transportation Requirement

⚠

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

Storage Requirement

⚠

Store the access reader under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the access reader 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 Access Controller.
- Do not connect the access reader to two or more kinds of power supplies, to avoid damage to the access reader.
- 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 access reader in a place exposed to sunlight or near heat sources.
- Keep the access reader away from dampness, dust, and soot.
- Install the access reader on a stable surface to prevent it from falling.
- Install the access reader 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 access reader label.
- The access reader is a class I electrical appliance. Make sure that the power supply of the access reader 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 access reader while the adapter is powered on.
- Operate the access reader within the rated range of power input and output.
- Use the access reader under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the access reader, and make sure that there is no object filled with liquid on the access reader to prevent liquid from flowing into it.
- Do not disassemble the access reader without professional instruction.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Introduction 1

- 1.1 Features 1
- 1.2 Appearance 1
  - 1.2.1 86 Box Model 1
  - 1.2.2 Slim Model 2

2 Ports Overview 3

3 Installation 4

- 3.1 Installing the 86 Box Model 4
- 3.2 Installing the Slim Model 5

4 Sound and Light Prompt 8

5 Unlocking the Door 9

6 Updating the System 10

- 6.1 Updating through X Station 10
- 6.2 Updating through X Portal 10

Appendix 1 Security Recommendation 11

1 Introduction

1.1 Features

- PC material and acrylic panel with a slim and waterproof design.
- Supports non-contact card reading.
- Supports IC card (Mifare) reading, ID card reading (only for the access reader with ID card reading function), and QR code reading (only for the access reader with QR code reading function).
- Supports communication through RS–485 and Wiegand (fingerprint access reader and QR code reader only support RS–485).
- Supports online update.
- Supports tamper alarm.
- Built-in buzzer and indicator light.
- Built-in watchdog to ensure access reader stability.
- Safe and stable with overcurrent and overvoltage protection.

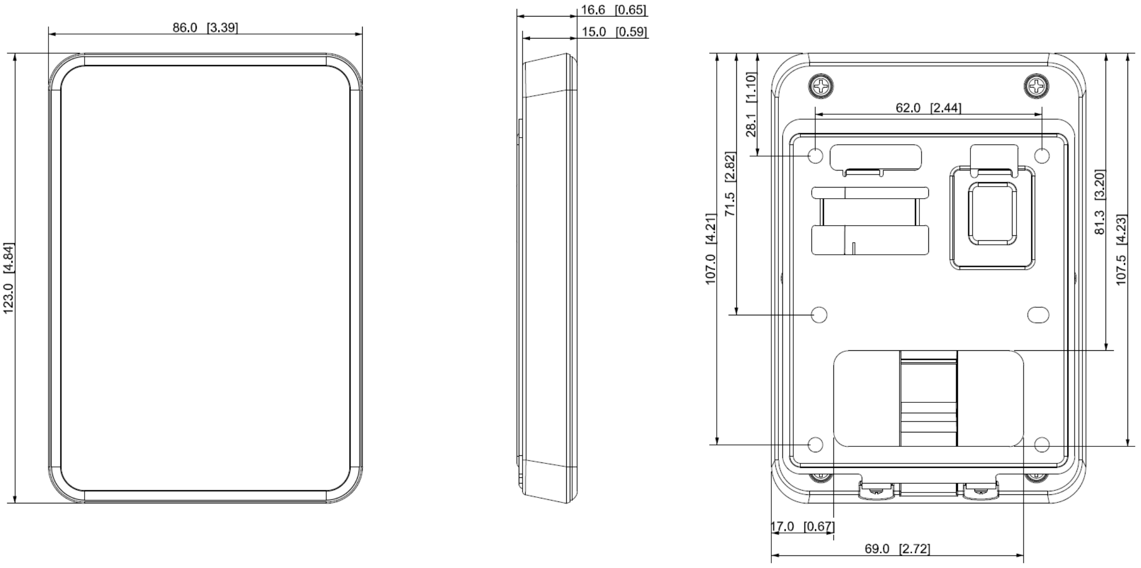
Functions might vary according to different models.

1.2 Appearance

The access reader can be divided into 86 box model, slim model, and fingerprint mode according to their appearances.

1.2.1 86 Box Model

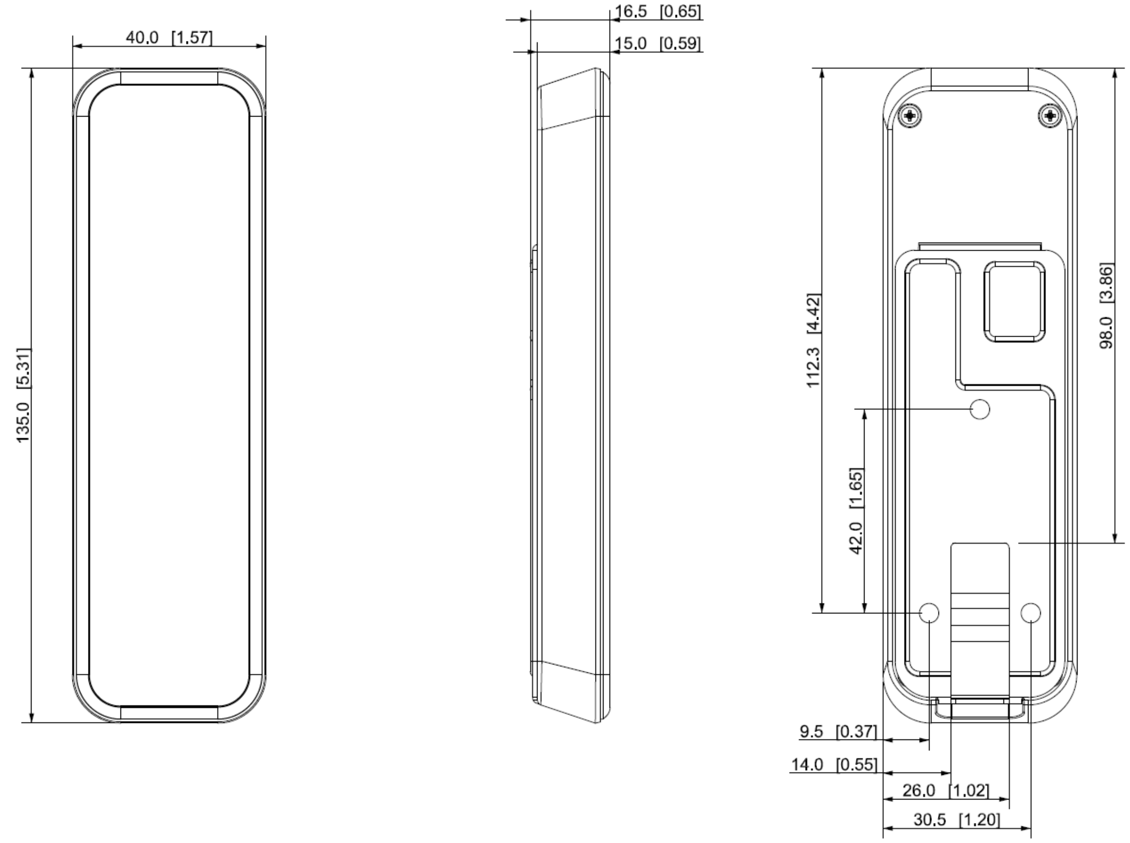
Figure 1-1 Dimensions of the 86 box model (mm [inch])



The 86 box model can be further divided into QR code access reader, and general card reader according to their functions.

1.2.2 Slim Model

Figure 1-2 Dimensions of the slim model (mm [inch])



2 Ports Overview

Use RS–485 or Wiegand to connect the access reader.

8-core Cables for the 86 Box and Slim Models

Table 2-1 Cable connection description

Color	Port	Description
Red	RD+	PWR (12 VDC)
Black	RD–	GND
Blue	CASE	Tamper alarm signal
White	D1	Wiegand transmission signal (effective only when using Wiegand protocol)
Green	D0	
Brown	LED	Wiegand responsive signal (effective only when using Wiegand protocol)
Yellow	RS–485_B	
Purple	RS–485_A	

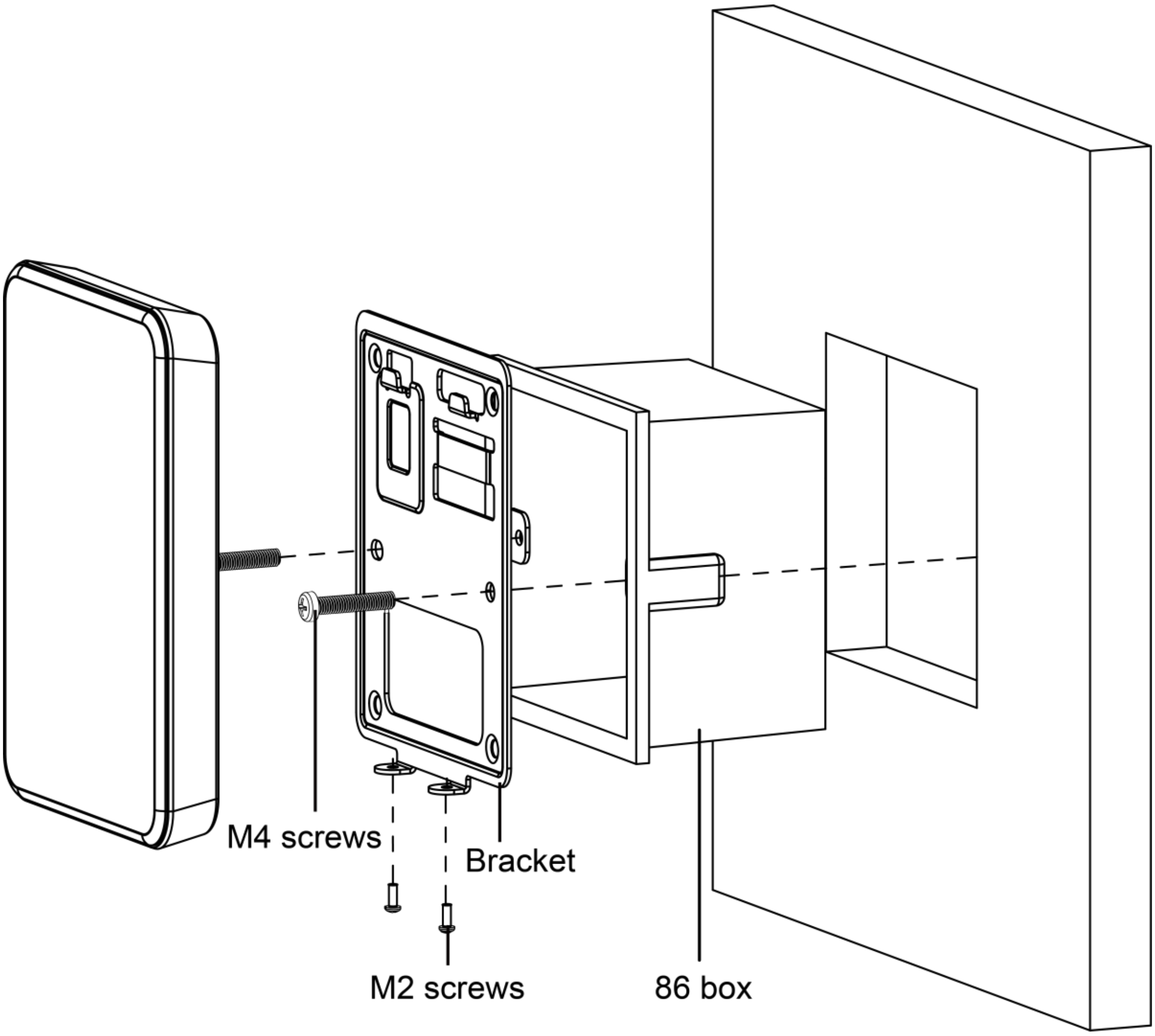
3 Installation

3.1 Installing the 86 Box Model

Box mount

1. Mount the 86 box to the wall.
2. Wire the access reader, and put the wires inside the 86 box.
3. Use two M4 screws to attach the bracket to the 86 box.
4. Attach the access reader to the bracket from top down.
5. Screw in 2 screws on the bottom of the access reader.

Figure 3-1 Wall mount

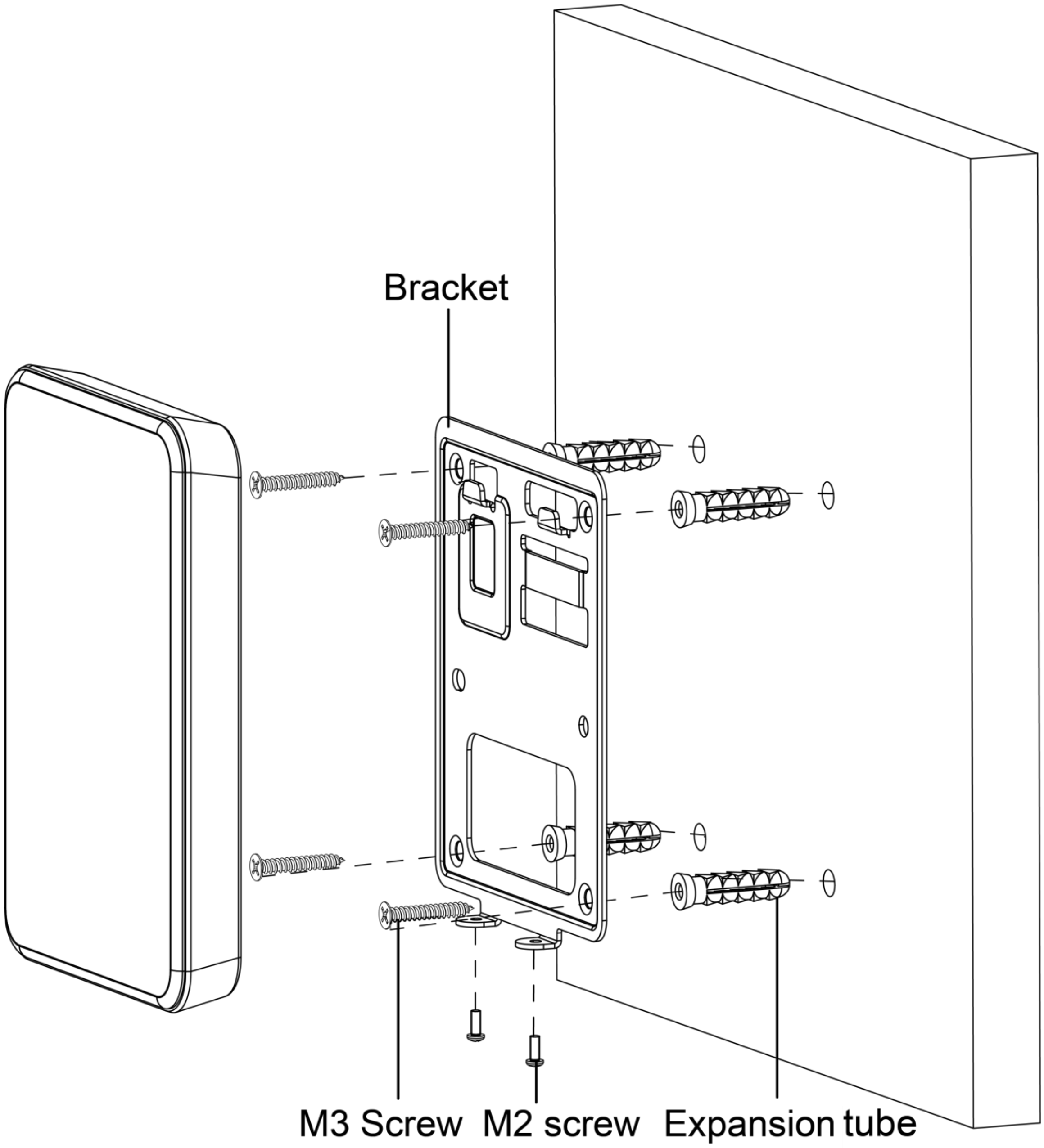


Wall mount

1. Drill holes on the wall.

2. Put 4 expansion bolts into the holes.
3. Wire the access reader through the slot of the bracket.
4. Use two M3 screws to mount the bracket on the wall.
5. Attach the access reader to the bracket from top down.
6. Screw in 2 screws on the bottom of the access reader.

Figure 3-2 Wall mount



3.2 Installing the Slim Model

Procedure

Step 1 Drill 4 holes and one cable outlet on the wall.

📖

For surface-mounted wiring, cable outlet is not required.

Step 2 Put 3 expansion bolts into the holes.

Step 3 Wires of the access reader, and pass the wires through the slot of the bracket.

Step 4 Use three M3 screws to mount the bracket on the wall.

Step 5 Attach the access reader to the bracket from top down.

Step 6 Screw in one M2 screw on the bottom of the access reader.

Figure 3-3 In-wall wiring

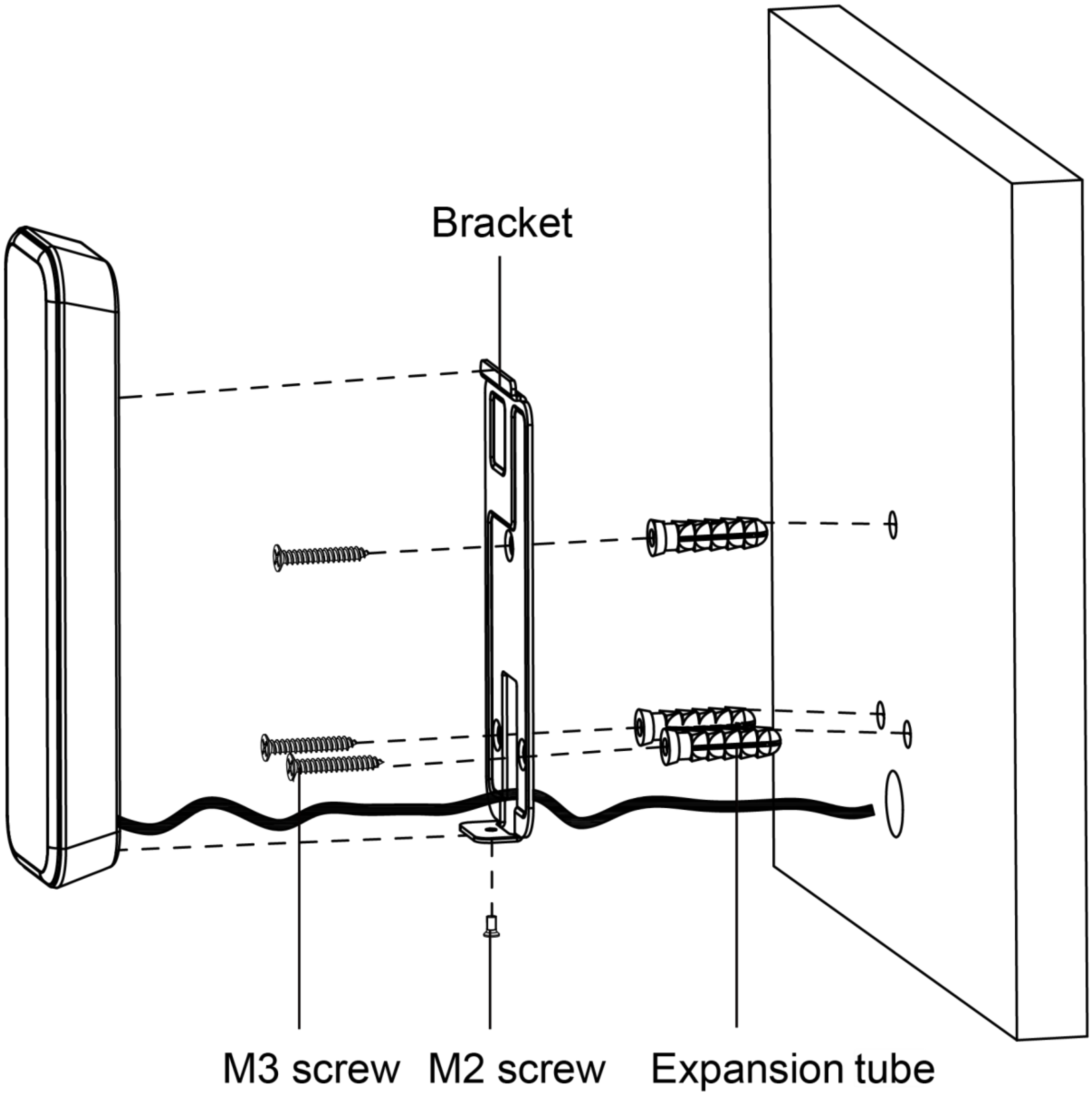
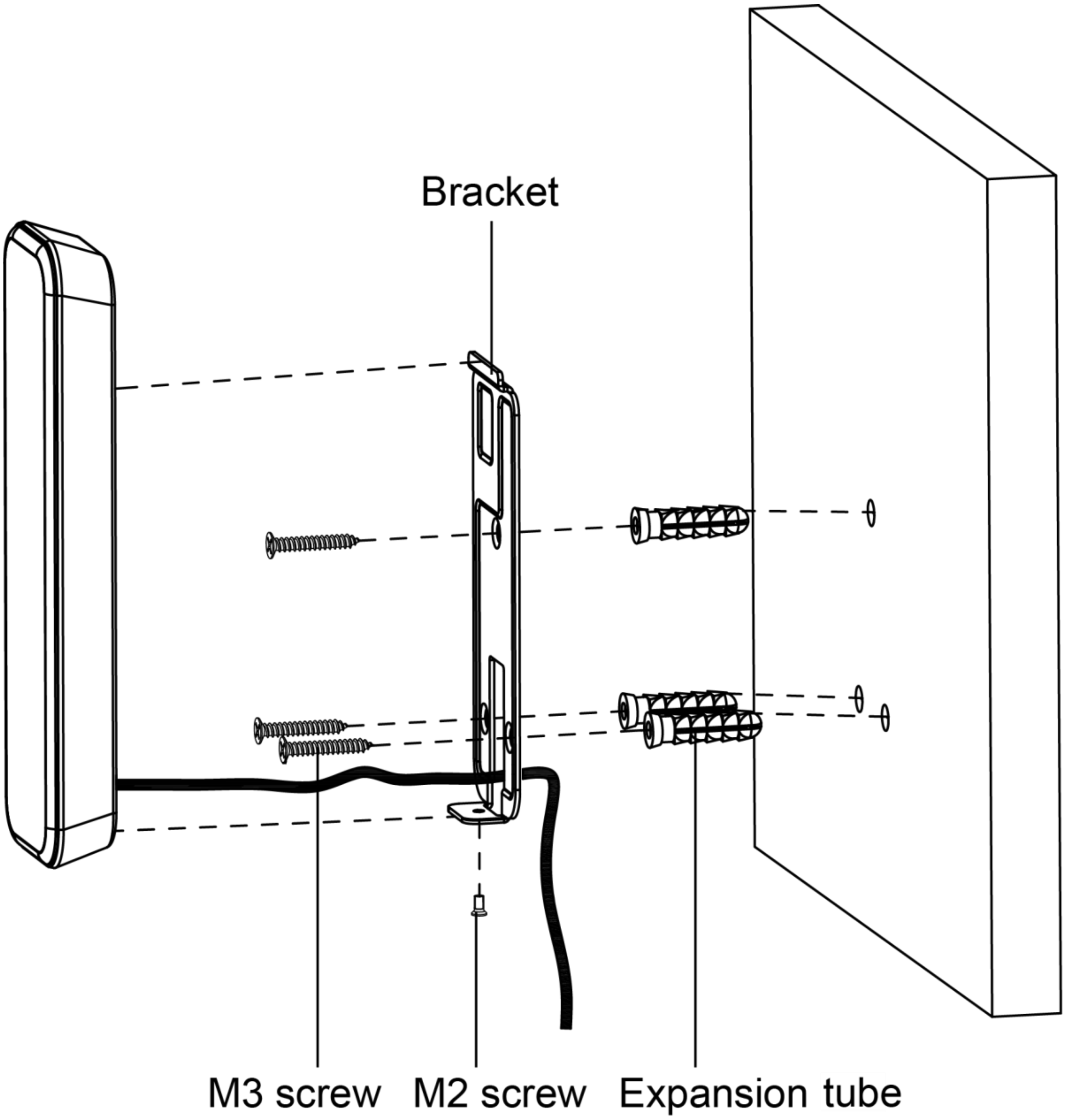


Figure 3-4 Surface mounted wiring



4 Sound and Light Prompt

86 Box and Slim Models

Table 4-1 Sound and light prompt description

Situation	Sound and Light Prompt
Power on.	Buzz once. The indicator is solid blue.
Removing the access reader.	Long buzz for 15 seconds.
Pressing buttons.	Short buzz once.
Alarm triggered by the controller.	Long buzz for 15 seconds.
RS–485 communication and swiping an authorized card.	Buzz once. The indicator flashes green once, and then turns to solid blue as standby mode.
RS–485 communication and swiping an unauthorized card.	Buzz four times. The indicator flashes red once, and then turns to solid blue as standby mode.
Abnormal 485 communication and swiping an authorized/unauthorized card.	Buzz three times. The indicator flashes red once, and then turns to solid blue as standby mode.
Wiegand communication and swiping an authorized card.	Buzz once. The indicator flashes green once, and then turns to solid blue as standby mode.
Wiegand communication and swiping an unauthorized card.	Buzz three times. The indicator flashes red once, and then turns to solid blue as standby mode.
Software updating or waiting for update in BOOT.	The indicator flashes blue until update is complete.

5 Unlocking the Door

Swipe card on the access reader to open the door.

For access reader with keypad, you can also unlock the door by entering the user ID and password.

- Unlock the door through public password: Enter the public password, and then tap **#**.
- Unlock the door through user password: Enter the user ID and tap **#**, and then enter the user password and tap **#**.
- Unlock the door through card + password: Swipe card, enter the password, and then tap **#**.

If the password is correct, the indicator is green and the buzzer sound once. If the password is incorrect, the indicator is red, and the buzzer sounds 4 times (RS-485 communication) or sounds 3 times (Wiegand communication or no signal line is connected).

6 Updating the System

6.1 Updating through X Station

Prerequisites

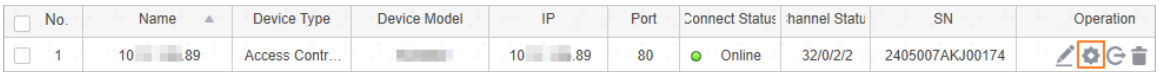
- The access reader was added to the access controller through RS-485 wires.
- The access controller and access reader are powered on.

Procedure

Step 1 Install and log in to X Station, and then select **Device Manager**.

Step 2 Click ⚙.

Figure 6-1 Select the access controller



□ No.	Name ▲	Device Type	Device Model	IP	Port	Connect Status	hannel Statu	SN	Operation
□ 1	10[redacted].89	Access Contr...	[redacted]	10[redacted].89	80	● Online	32/0/2/2	2405007AKJ00174	✎ ⚙ ⟲ 🗑

Step 3 Click ☁ and 📁 to select the update file.

Step 4 Click **Upgrade.**

The indicator of the access reader flashes blue until the update is completed, and then the access reader automatically restarts.

6.2 Updating through X Portal

Prerequisites

- The access reader was added to the access controller through RS-485 wires.
- The access controller and access reader are powered on.

Procedure

Step 1 Install and open the X Portal, and then select **Device upgrade**.

Step 2 Click 🗋 of an access controller, and then click ⬆.

Step 3 Click **Upgrade**.

The indicator of the access reader flashes blue until update is complete, and then the access reader automatically restarts.

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).