Access Control Card Reader

User's Manual

V1.0.0

Foreword

General

This manual introduces the functions and operations of the access control card reader (hereinafter referred to as "the Device").

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
📖 **NOTE**	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	October 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The following contents are about the proper ways of using the Device, preventing dangers and property damage when it is in use. Read the manual carefully before using the Device, strictly abide by the manual and properly keep it for future reference.

- A non-switch mode linear DC power supply is recommended for the best reading distance.
- Power supply distance should not exceed 100 m; otherwise, it is recommended to use a dedicated power supply.
- For the Device to work properly, make sure that the input voltage is between 12V ± 10%.
- Connect the device and access controller with cable of RVVP0.5 or above.
- If installed outdoors or at places with high humidity or water leakage, it is recommended to install with a waterproof cover.
- To reduce the noise from long distance transmission, the shielding cover of the transmission cable should be common-grounded with the Device and the access controller.

Table of Contents

1 Introduction

As a key part of the access control system, the Device can read fingerprints and various kinds of cards and send the information to the access controller for verification. It is applicable to industrial zones, office buildings, schools, factories, stadiums, CBD, residential area, government properties, etc.

1.1 Features

- PC material and acrylic panel with an ultra-thin and waterproof design.
- Supports reading IC (Mifare) and ID (only supported by certain models) cards in a non-contact way.
- Supports communication through RS485 and Wiegand (only supported by certain models).
- Supports online update.
- Supports tamper alarm.
- Built-in buzzer and indicator light.
- Built-in watchdog to ensure device stability.
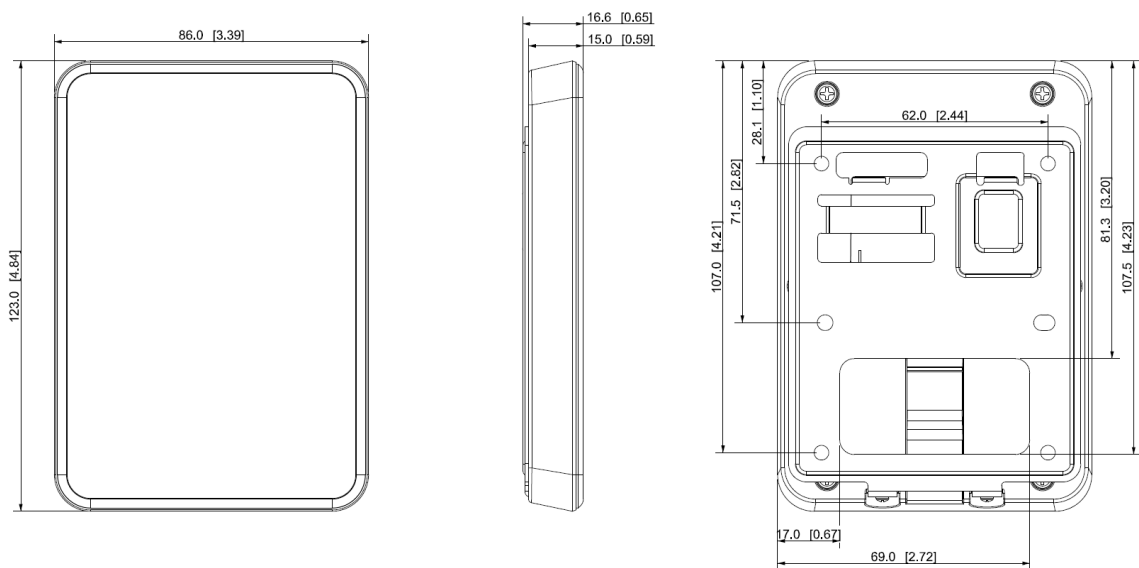- Safe and stable with overcurrent and overvoltage protection.

Functions may vary according to the model, and the actual functions of the model shall prevail.
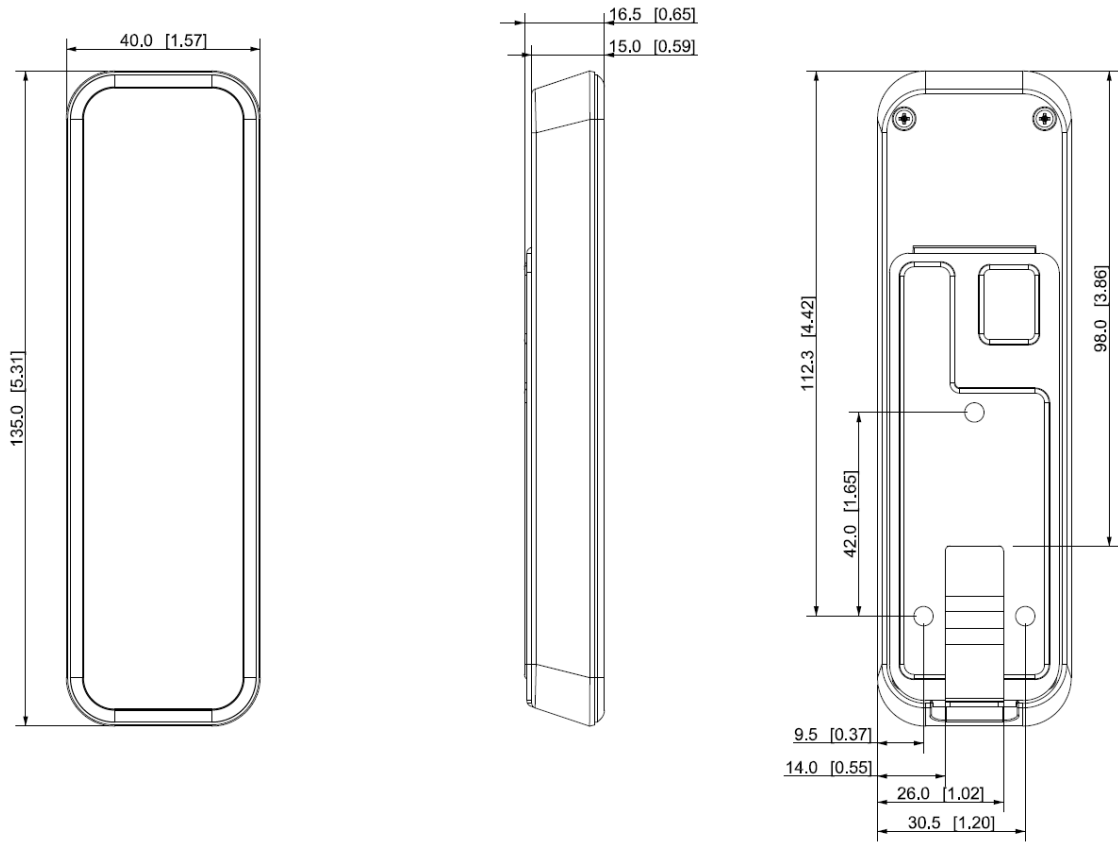
1.2 Dimensions

1.2.1 86 Box Model

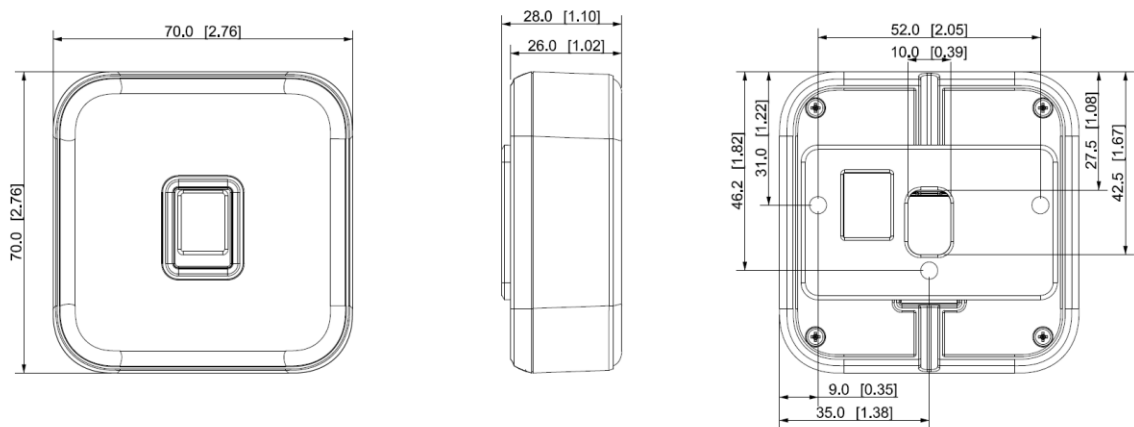Figure 1-1 Dimensions of the 86 box model (mm [inch])

1.2.2 Slim Model

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

1.2.3 Fingerprint Model

Figure 1-3 Dimensions of the fingerprint model (mm [inch])

2 Installation

2.1 Cable Connection

8-core Cables for the 86 Box and Slim Models

Figure 2-1 Cable connection description (1)

Color	Port	Description
Red	RD+	PWR (DC +12V)
Black	RD–	GND
Blue	CASE	Tamper alarm signal
White	D1	Wiegand transmission signal (effective only when using Wiegand protocol)
Green	D0	Wiegand transmission signal (effective only when using Wiegand protocol)
Brown	LED	Wiegand responsive signal (effective only when using Wiegand protocol)
Yellow	RS485_B	RS485_B
Purple	RS485_A	RS485_A

5-core Cables for the Fingerprint Model

Table 2-2 Cable connection description (2)

Color	Port	Description
Red	RD+	PWR (DC +12V)
Black	RD–	GND
Blue	CASE	Tamper alarm signal
Yellow	RS485_B	RS485_B
Purple	RS485_A	RS485_A

When connecting cables, select either the RS485 or Wiegand cable.

Figure 2-3 Cable specification and length

| Device Type	Connection Method	Length
RS485 card reader	Connect to the RS485 port with a cat 5e Ethernet cable, and each wire must be within 10Ω.	100 m (328.08 ft)
Wiegand card reader	Each wire must be within 2Ω.	80 m (262.47 ft)

2.2 Installation

The recommended installation height (from the center of the Device to the ground) is 130 cm – 150 cm (51.18" – 59.06"), and should not be over 200 cm (78.74").

2.2.1 Installing the 86 Box Model
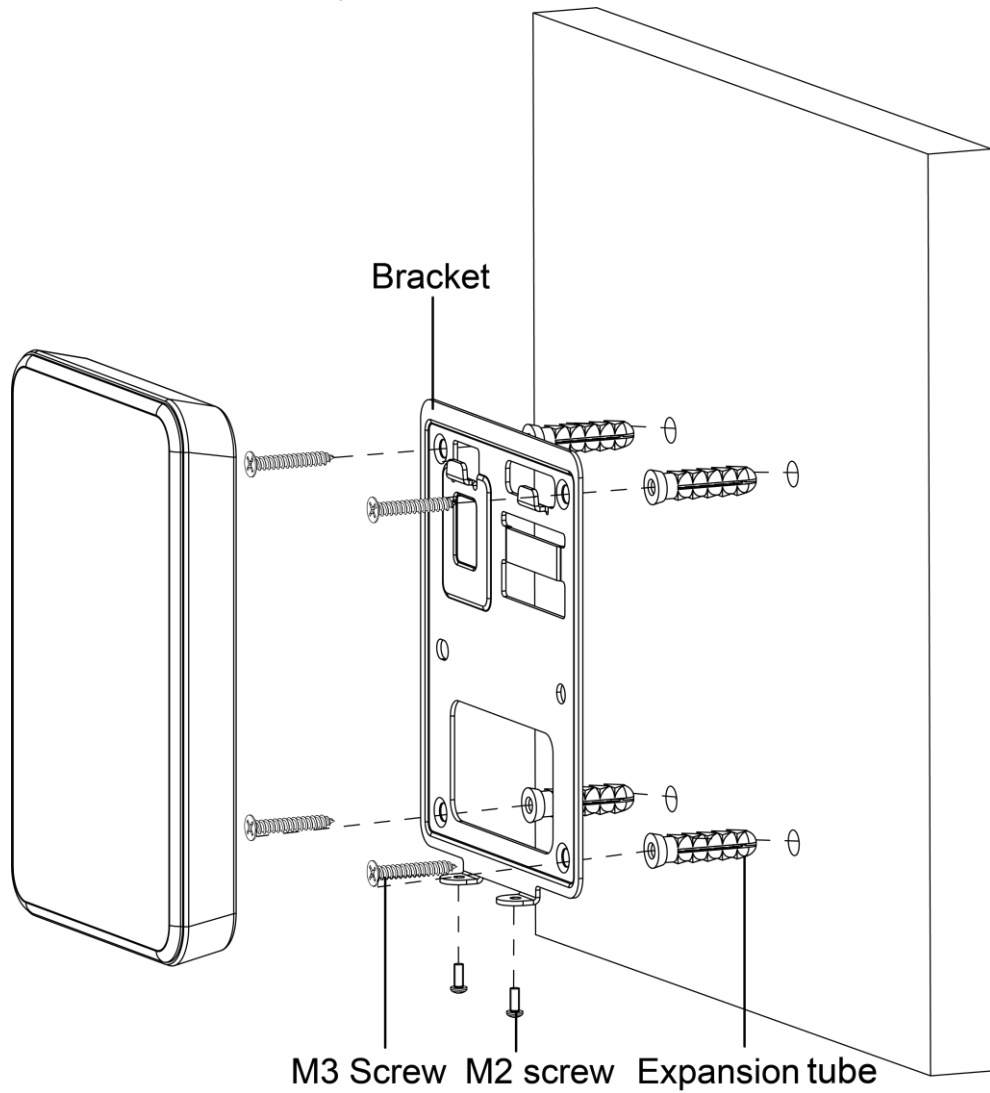
With an 86 Box

Figure 2-1 Install with an 86 box
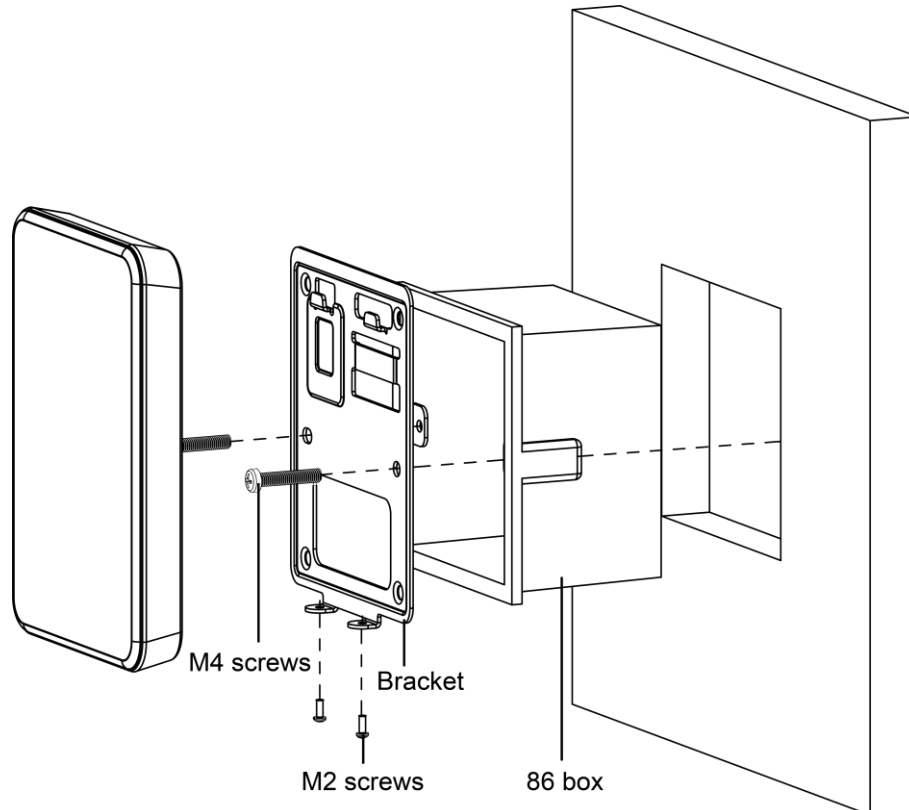
Step 1 Fit the 86 box into the wall.
Step 2 Connect the wires of the Device and put them inside the 86 box.
Step 3 Use two M4 screws to fix the bracket to the 86 box.
Step 4 Fix the Device onto the bracket from top down.
Step 5 Use two M2 screws to fix the Device onto the bracket.

Wall Mount

Bracket

M3 Screw M2 screw Expansion tube

Step 1 Drill holes on the wall. See Figure 1-1 for the positions.
Step 2 Put four expansion bolts into the holes.
Step 3 Connect the wires of the Device and put them inside the wall.
Step 4 Use two M3 screws to fix the bracket on the wall.
Step 5 Fix the Device onto the bracket from top down.
Step 6 Use two M2 screws to fix the Device onto the bracket.

2.2.2 Installing the Slim Model
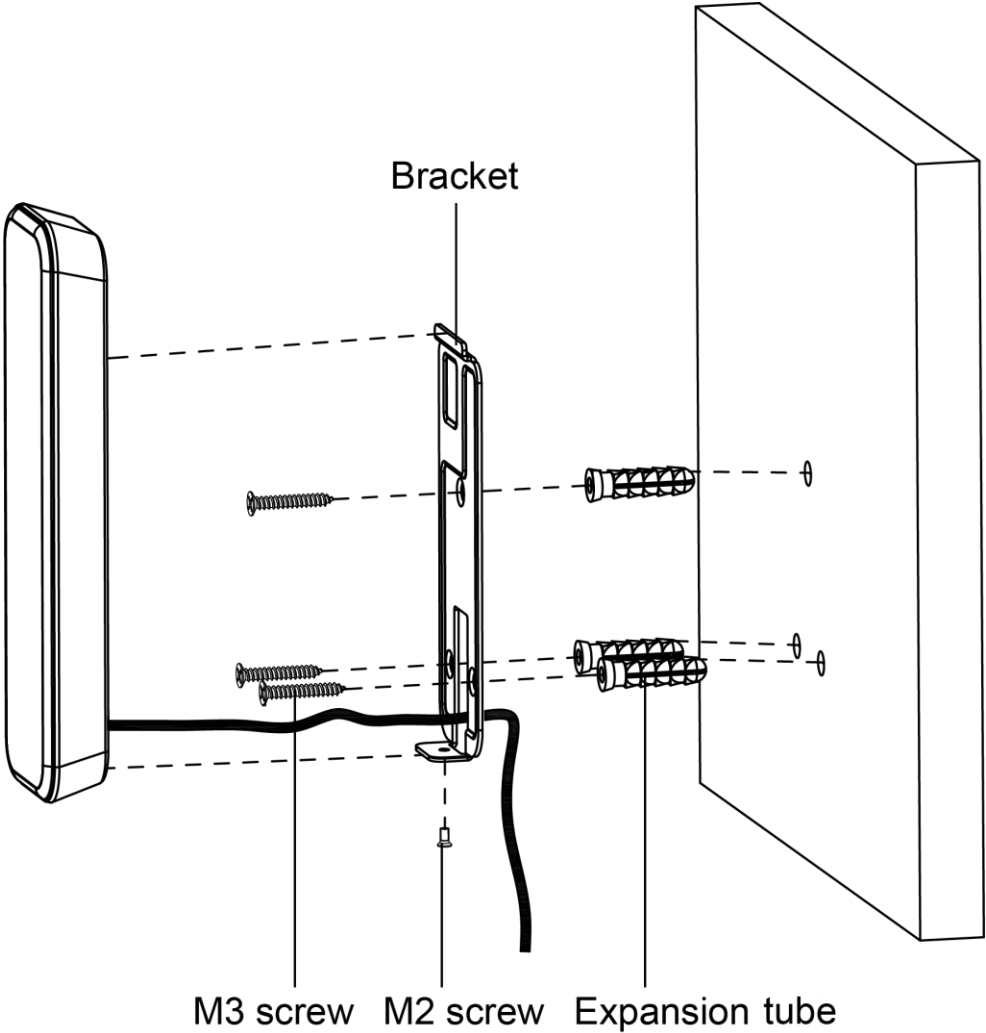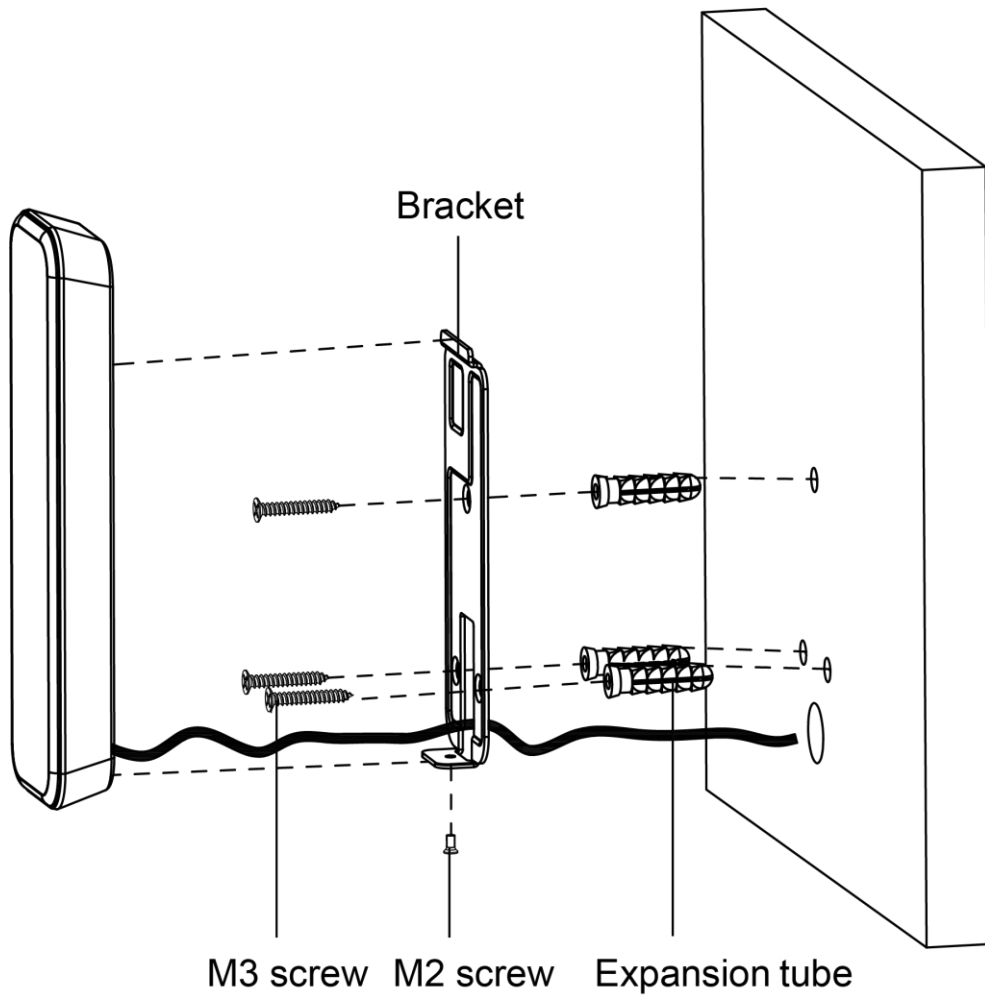
Figure 2-3 Surface mount

Bracket

M3 screw   M2 screw   Expansion tube

Figure 2-4 Flush mount

Bracket

M3 screw   M2 screw   Expansion tube

Step 1 Drill holes on the wall. See Figure 1-2 for the positions.
Step 2 Put three expansion bolts into the holes.
Step 3 Connect the wires of the Device and run them through the cable outlet of the bracket.
Step 4 (Optional) Put the wires inside wall.
Step 5 Use three M3 screws to fix the bracket on the wall.
Step 6 Fix the Device onto the bracket from top down.
Step 7 Use one M2 screw to fix the Device onto the bracket.

2.2.3 Installing the Fingerprint Model
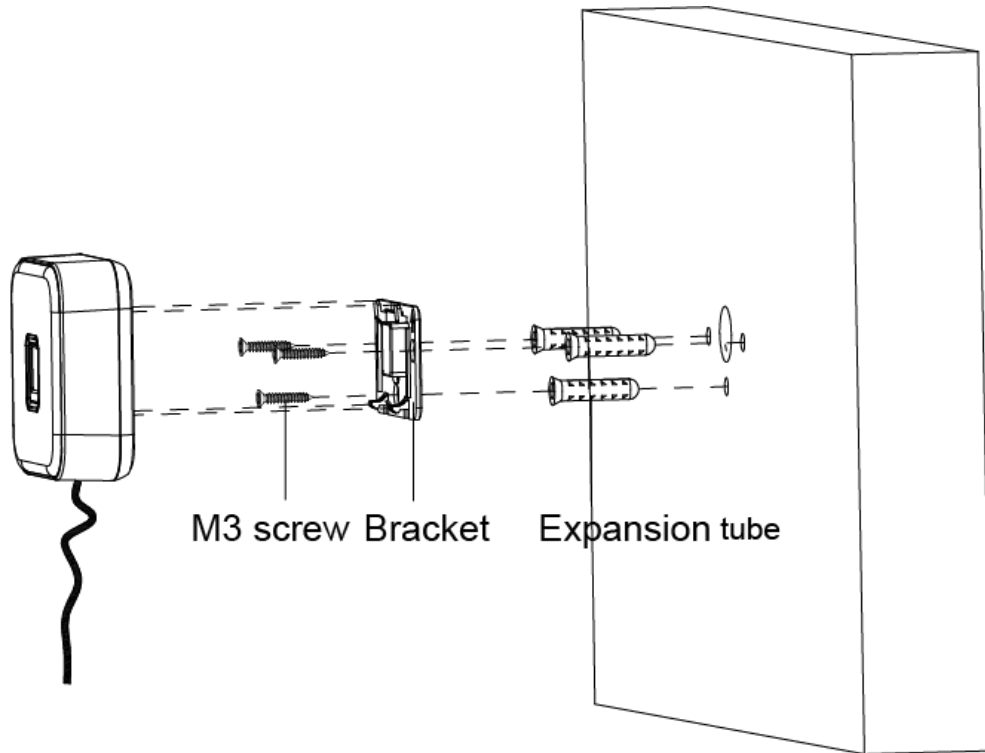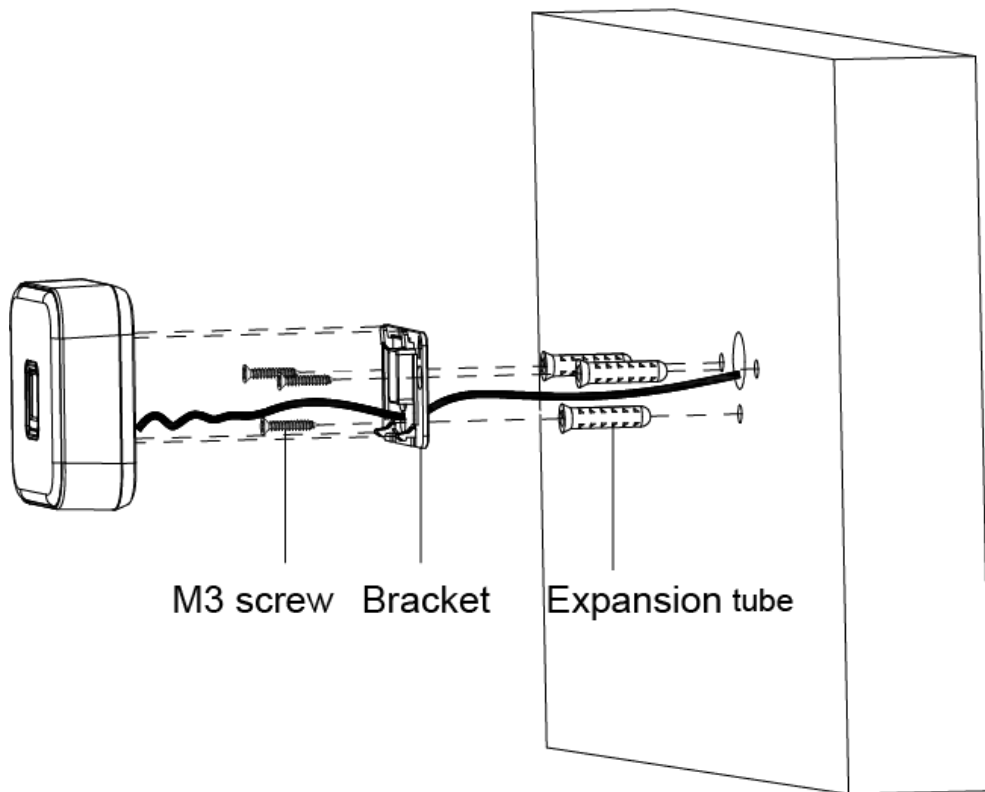
Figure 2-5 Surface mount

M3 screw Bracket Expansion tube

Figure 2-6 Flush mount

M3 screw Bracket Expansion tube

Procedure

Step 1 On the wall, drill three holes for expansion bolts and one hole for the wires. See Figure 1-3 for the positions.

Step 2 Put three expansion bolts into the holes.

Step 3 Use three M3 screws to fix the bracket on the wall.

Step 4 Connect the wires of the Device.
Step 5 (Optional) Put the wires inside the wall.
Step 6 Fix the Device onto the bracket from top down.
Step 7 Press the Device hard toward the arrow direction until you hear a "click", and the installation completes. See the following figure.
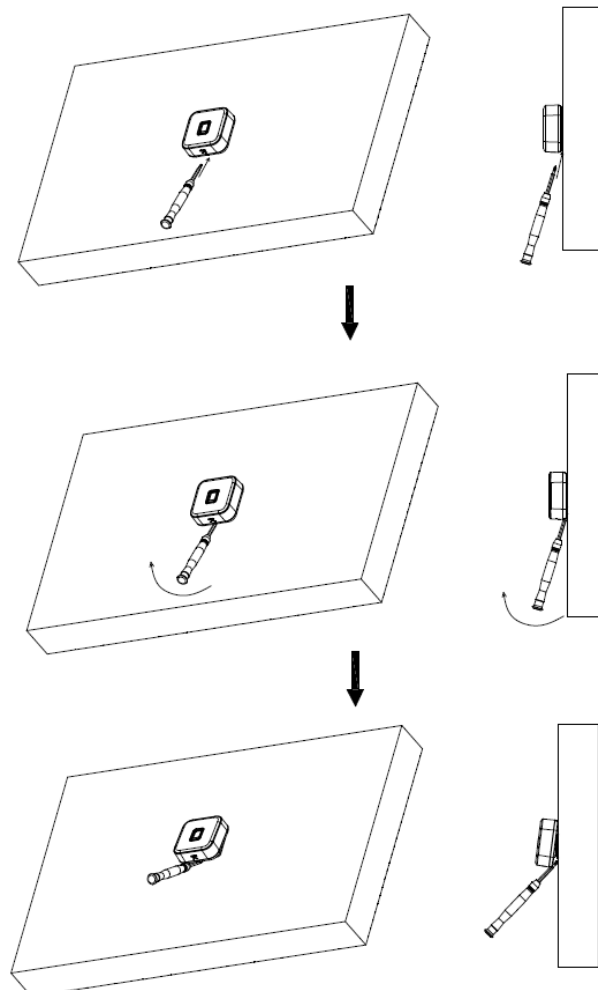
Figure 2-7 Press the Device hard until you hear a "click"
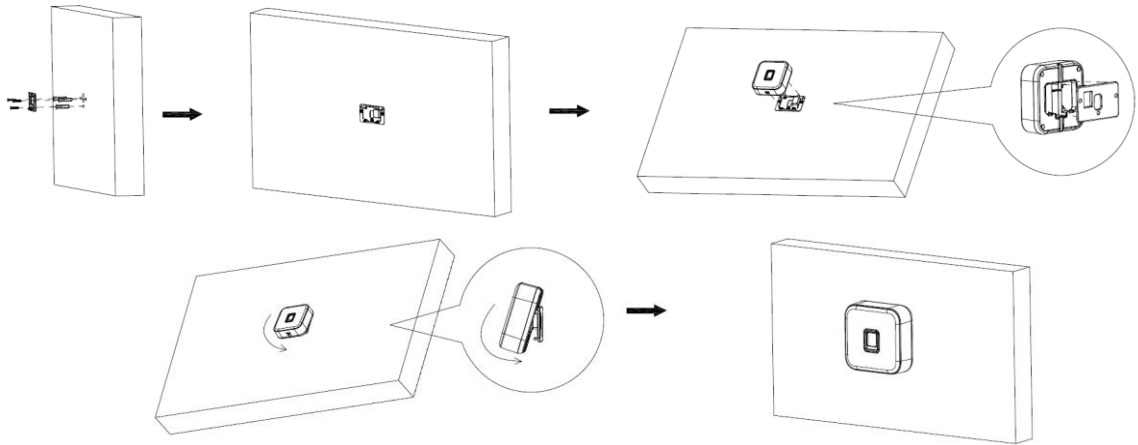
Related Operation

To unbuckle the Device from the wall, insert the provided screwdriver in the cable outlet on the bottom, pry the Device open toward the arrow direction until you hear a "click".

Figure 2-8 Unbuckle the Device

3 Sound and Light Prompt

After powered on, the Device will buzz once and the indicator is solid blue, which means the Device is working properly.

⚠️

The Device can only read one card at a time. When multiple cards stack together, it cannot work properly.

3.1 86 Box and Slim Models

The sound and light prompt of the 86 box and slim models are the same.

Table 3-1 Sound and light prompt description

Situation	Sound and Light Prompt
Power on	Buzz once; The indicator is solid blue.
Removing the Device	Long buzz for 15 seconds.
Pressing buttons	Short buzz once.
Alarm triggered by the controller	Long buzz for 15 seconds.
RS485 communication and use an authorized card	Buzz once; The indicator flashes green once, and then turns to solid blue as standby mode.
RS485 communication and use an unauthorized card	Buzz four times; The indicator flashes red once, and then turns to solid blue as standby mode.
Abnormal 485 communication and use an authorized/unauthorized card	Buzz three times; The indicator flashes red once, and then turns to solid blue as standby mode.
Wiegand communication and use an authorized card	Buzz once; The indicator flashes green once, and then turns to solid blue as standby mode.
Wiegand communication and use 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 completed.

3.2 Fingerprint Model

Table 3-2 Sound and light prompt description

Situation	Sound and Light Prompt
Device Power-on	Buzz once; The indicator is solid blue.
Removing the Device	Long buzz for 15 seconds.

Situation	Sound and Light Prompt
Alarm linkage triggered by the controller	Long buzz for 15 seconds.
485 communication and use an authorized card	Buzz once; The indicator flashes green once, and then turns to solid blue as standby mode.
485 communication and use an unauthorized card	Buzz four times; The indicator flashes red once, and then turns to solid blue as standby mode.
Abnormal 485 communication and use an authorized or unauthorized card/ fingerprint.	Buzz three times; The indicator flashes red once, and then turns to solid blue as standby mode.
485 communication and a fingerprint is recognized	Buzz once.
485 communication and use an authorized fingerprint	Buzz twice with 1 second interval; The indicator flashes green once, and then turns to solid blue as standby mode.
485 communication and use an unauthorized fingerprint	Buzz once, and then four times; The indicator flashes red once, and then turns to solid blue as standby mode.
Fingerprint operations, including adding, deleting and synchronization	The indicator flashes green.
Exiting fingerprint operations, including adding, deleting and synchronization	The indicator is solid blue.
Software updating or waiting for update in BOOT	The indicator flashes blue until update is complete.

4 Device Update

4.1 SmartPSS AC

Use SmartPSS AC to update the Device through the access controller.
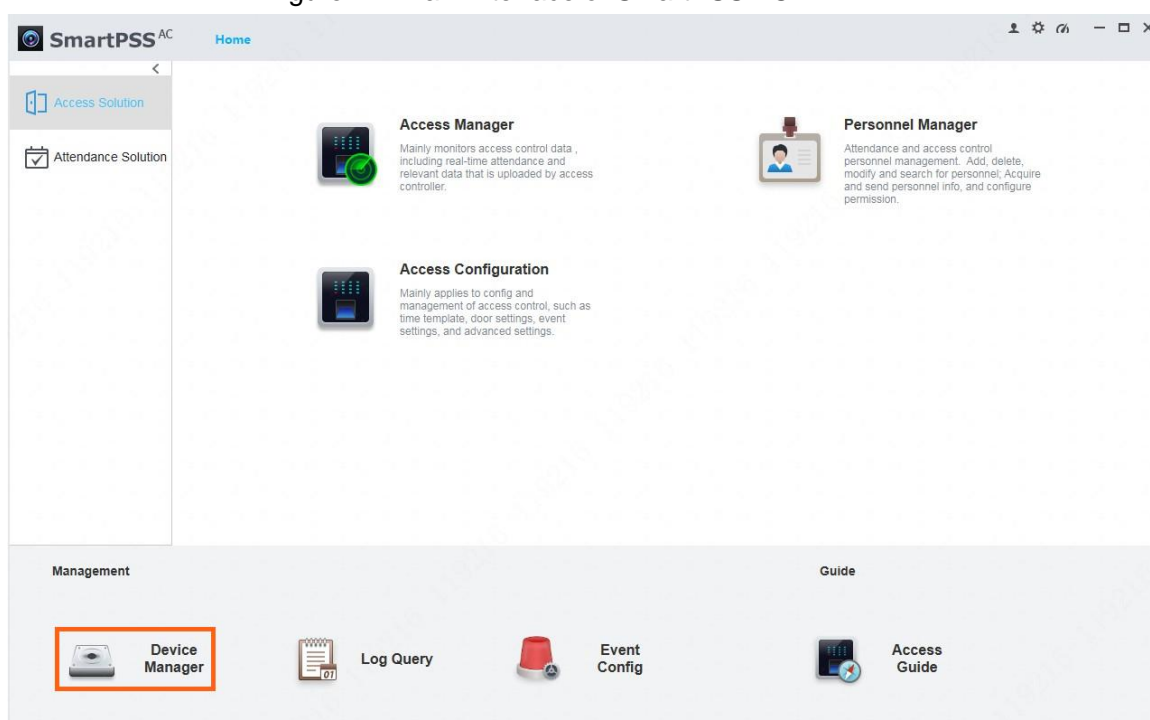
Prerequisites
- The Device and access controller are connected and powered on.
- SmartPSS AC is installed on your PC.

Procedure

Step 1   Log in to SmartPSS AC, and then select **Device Manager**.

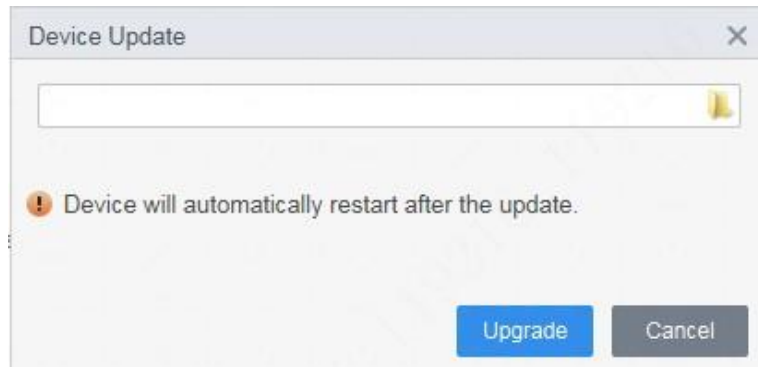Figure 4-1 Main interface of SmartPSS AC

Step 2   Click .

Figure 4-2 Select the access controller

☑	No.	Name ▲	IP	Device Type	Device Model	Port	Channel Number	Online Status	SN	Operation
☑	1	Device01	171.2.101.80	Access Controller	ASC2208C-S	37777	0/0/8/8	● Online	6H029E1YAJ5FD7D	🖉 ⚙ ⇨ 🗑

Step 3   Click and to select the update file.

Figure 4-3 Device update

Step 4 Click **Upgrade.** The indicator of the Device flashes blue until update is completed, and then the Device automatically restarts.

4.2 Configuration Tool

Use the Configtool to update the Device through the access controller.
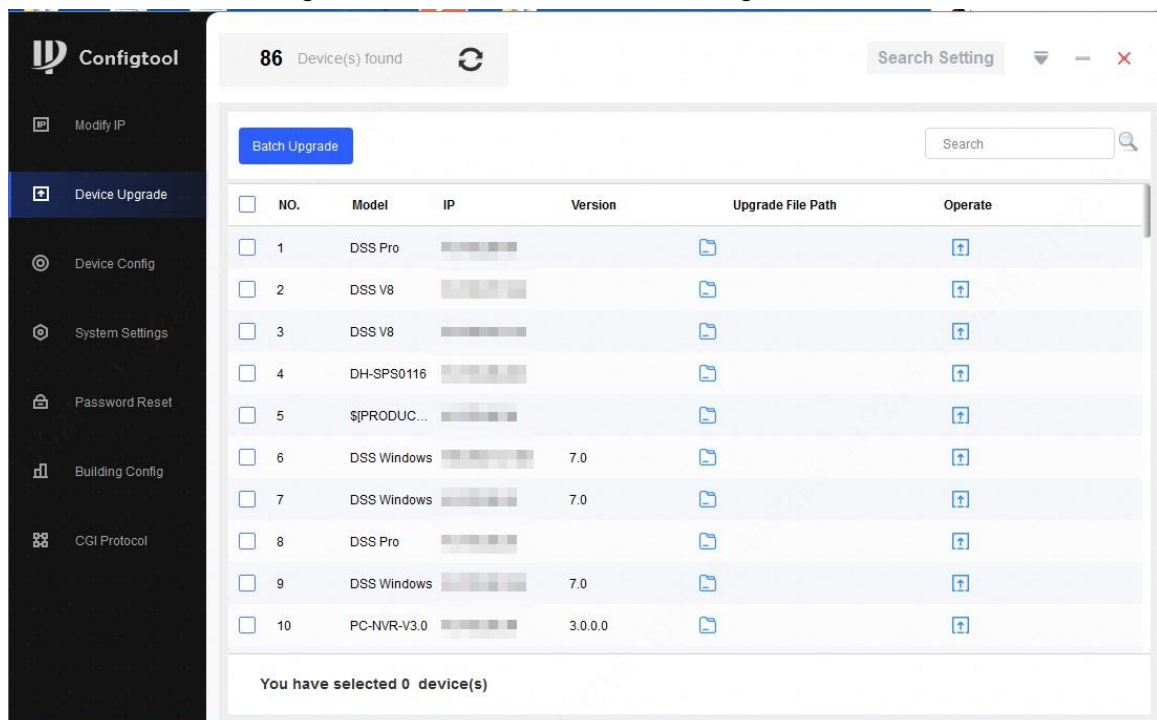
Prerequisites
- The Device and access controller are connected and powered on.
- The Configtool is installed on your PC.

Procedure
Step 1   Open the Configtool and select **Device upgrade**.

Figure 4-4 Main interface of the Configtool

Step 2   Click 📁 and select the update file for each access controller, and then click ⬆.
Step 3   Click **Batch Upgrade.** The indicator of the Device flashes blue until update is completed, and then the Device automatically restarts.

Figure 4-5 Batch update

	NO.	Model	IP	Version	Upgrade File Path	Operate
☐	16	VTH5422H		4.500.0000000.0.R 🗀		⬆
☐	17	VTS5340B		4.500.0000000.5.R 🗀		⬆
☐	18	ASI7214Y-V3		1.000.0000006.3.R 🗀		⬆
☐	19	VTH5422H		4.500.0000000.0.R 🗀		⬆
☐	20	DH-ASI7223...		1.000.0000002.5.R 🗀		⬆
☐	21	VTH2421F		4.500.0000000.5.R 🗀		⬆
☐	22	VTH5441G		4.500.0000000.4.R 🗀		⬆

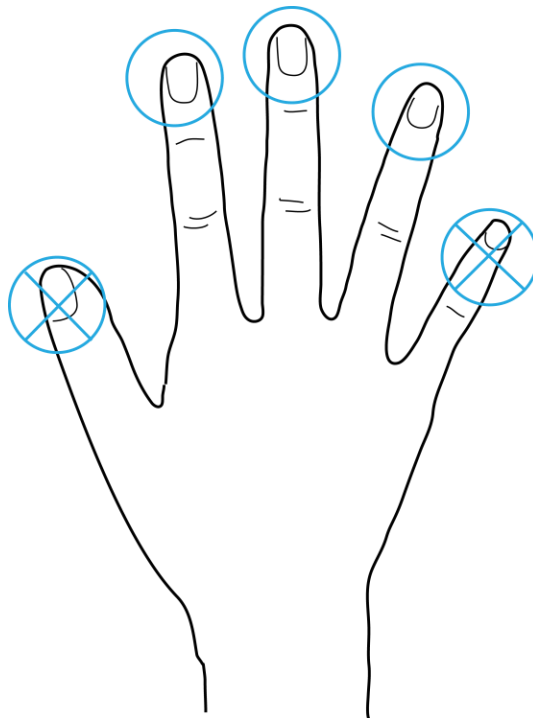# Appendix 1 Fingerprint Collecting Instruction

Notice

- Make sure that your fingers are clean and dry before collecting your fingerprints.
- Do not expose the fingerprint scanner to high temperature and humidity.
- If your fingerprints are worn or unclear, use other methods including password and card.

Recommended Fingers

Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the capturing center easily.
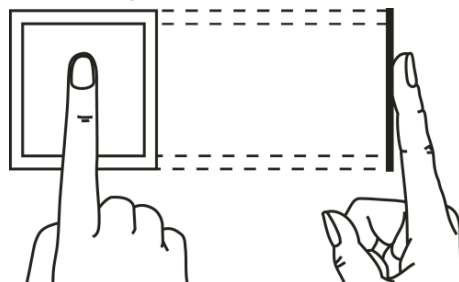
Appendix Figure 1-1 Recommended fingers

Correct Way of Pressing Your Finger

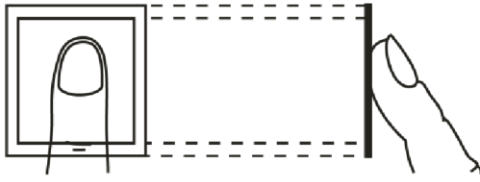Press you finger to the fingerprint collecting area, and align the center of your fingerprint to the center of the collecting area.
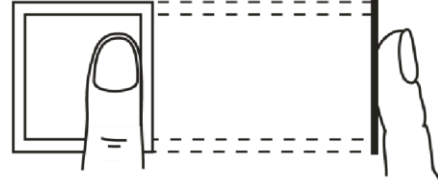
Appendix Figure 1-2 Correct way
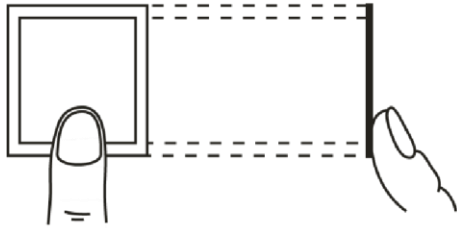
Appendix Figure 1-3 Incorrect ways

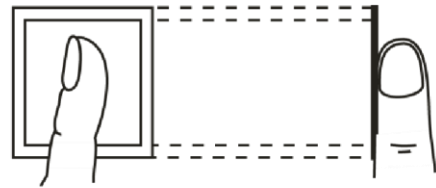Fingerprint not entirely
on the collecting area

Fingerprint not on the
center of the collecting area

Fingerprint not on the
center of the collecting area

Fingerprint not on the
collecting area

Appendix 2 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 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.