

Access Standalone

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the access standalone device (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.	December 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°C (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

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Structure.....	1
2 Wiring and Installation.....	2
2.1 Environment Requirements.....	2
2.2 Wiring.....	4
2.3 Installation.....	6
2.3.1 Wall Mount	6
2.3.2 86 Box Mount.....	7
3 Local Configurations.....	9
3.1 Initialization.....	9
3.2 Logging in to the Main Menu.....	9
3.3 Adding Users.....	11
4 Web Configurations.....	14
4.1 Logging in to the Webpage.....	14
4.2 Logging in to the Phone Webpage.....	14
Appendix 1 Important Points of Fingerprint Registration Instructions.....	16
Appendix 2 Security Recommendation.....	18

1 Structure

Figure 1-1 Structure

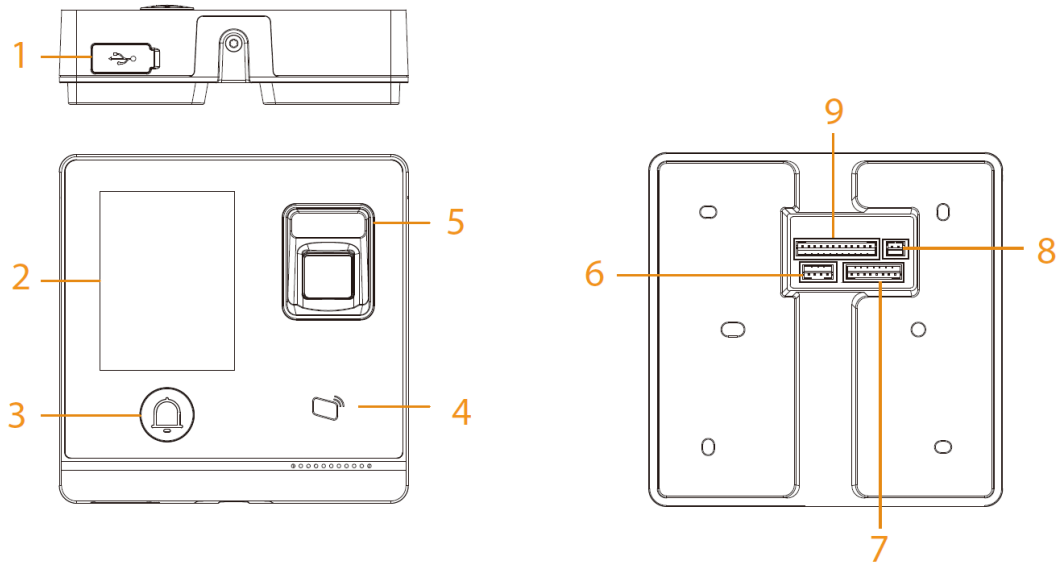


Table 1-1 Port description

No.	Name
1	USB port
2	Screen
3	Bell button
4	Card swiping area
5	Fingerprint sensor
6	Network cable port
7	Functional cable port 2
8	Power input cable port
9	Functional cable port 1

2 Wiring and Installation

2.1 Environment Requirements

- The illumination 0.5 m from the device should not be less than 100 lux.

Figure 2-1 Installation Environment



Candle: 10 lux



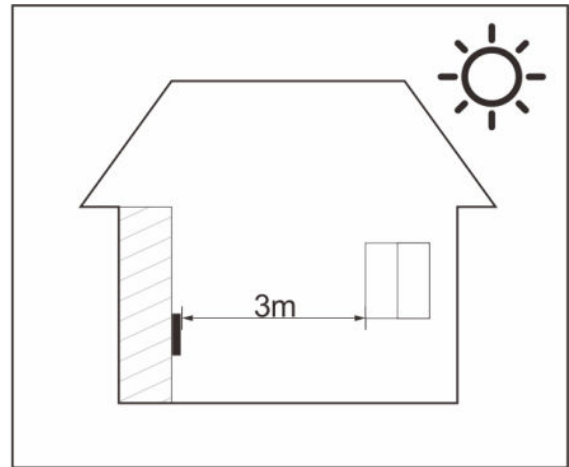
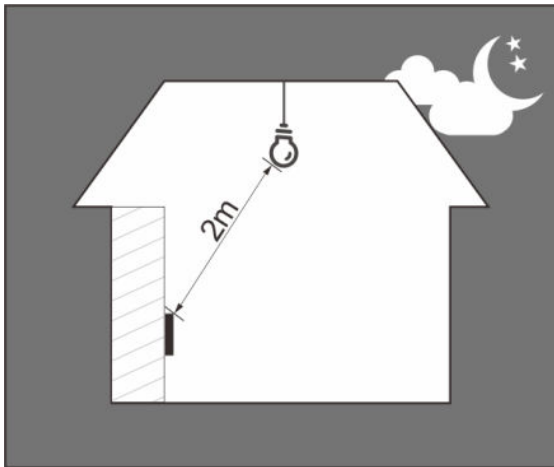
Light bulb: 100 lux - 850 lux



Sunlight: ≥ 1200 lux

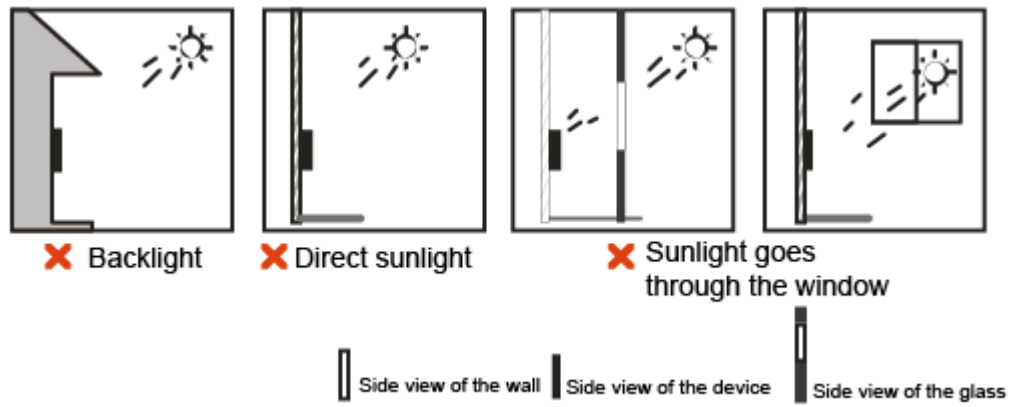
- We recommend installing the device indoors, 3 m away from the windows or doors, and 2 m away from any light source.

Figure 2-2 Installation Position



- Do not expose the device to backlight, sunlight, or place it near any light.

Figure 2-3 Places not recommended



2.2 Wiring

Figure 2-4 Cable introduction

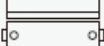
Function cable port 1	Power Input	Black	DC_IN-		12 VDC
		Red	DC_IN+		
	Alarm Input	Gray	GND		Sensor
		White & Brown	ALM_IN		
	Alarm Output	White & Gray	ALM_COM		Siren
		White & Blue	ALM_NO		
	Doorbell Output	White & Orange	BELL+		Doorbell
		White & Red	BELL-		
	Lock	Gray	GND		Exit button
		Green & Black	DOOR_EXIT		Door detector
		Gray & Black	DOOR_SR		
		Brown & Black	DOOR_COM		Normally closed electromagnetic lock
		Purple & Black	DOOR_NC		Normally open electric strike lock
		Yellow & Black	DOOR_NO		
Function cable port 2	RS-485	Purple	RS485A		RS-485 card reader
		Yellow	RS485B		Door security module
	Wiegand	Green	WG_D0		Wiegand card reader
		White	WG_D1		
		Brown	WG_LED		
		Blue	CASE		Card Reader Tamper
	Power Output	Gray	DC_OUT-		
		Red	DC_OUT+		

Figure 2-5 Wiring

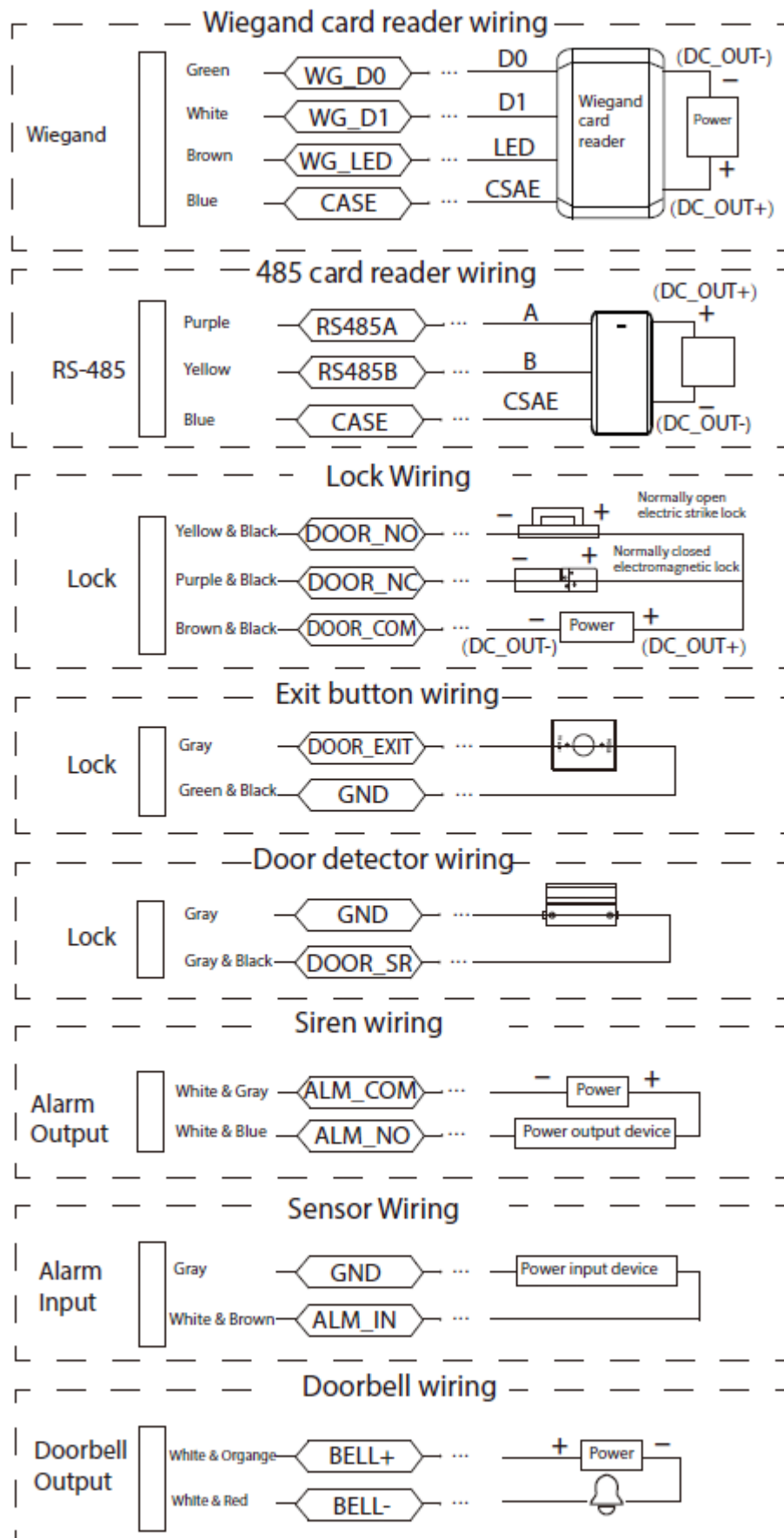
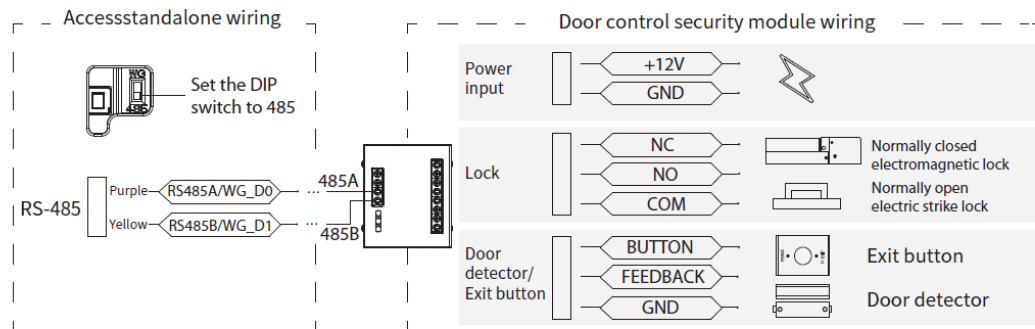


Figure 2-6 Wiring for door control security module



- If you have selected **Door Security Module** in **Communication Settings > Serial Port Config > RS-485 Settings**, a compatible door control security module must be purchased, and the module requires an external power supply.
- When the door control security module is enabled, the device's exit button and lock control linkage for door opening will be invalid.
- For details of door lock wiring, see the lock user manual.

2.3 Installation

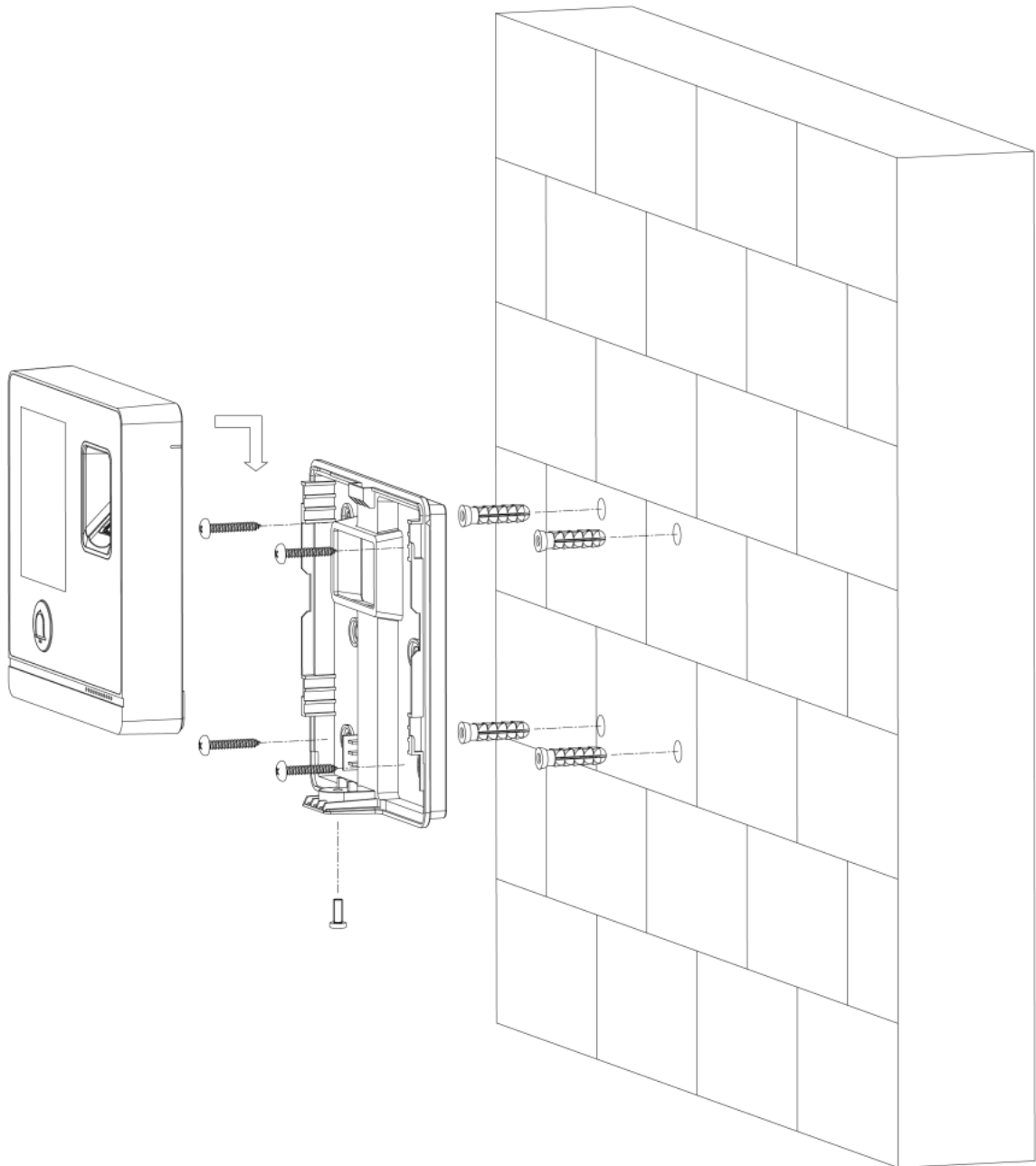
The standalone supports wall mount installation and 86 box mount installation.

2.3.1 Wall Mount

Procedure

- Step 1 Use the 4 screws to fix the bracket to the wall.
- Step 2 Wire the access standalone. For details, see "2.2 Wiring".
- Step 3 Use 1 screw to fix the back cover to the access standalone.
- Step 4 Fix the access standalone on the bracket.
- Step 5 Screw in 1 screw securely at the bottom of the access standalone.

Figure 2-7 Wall mount

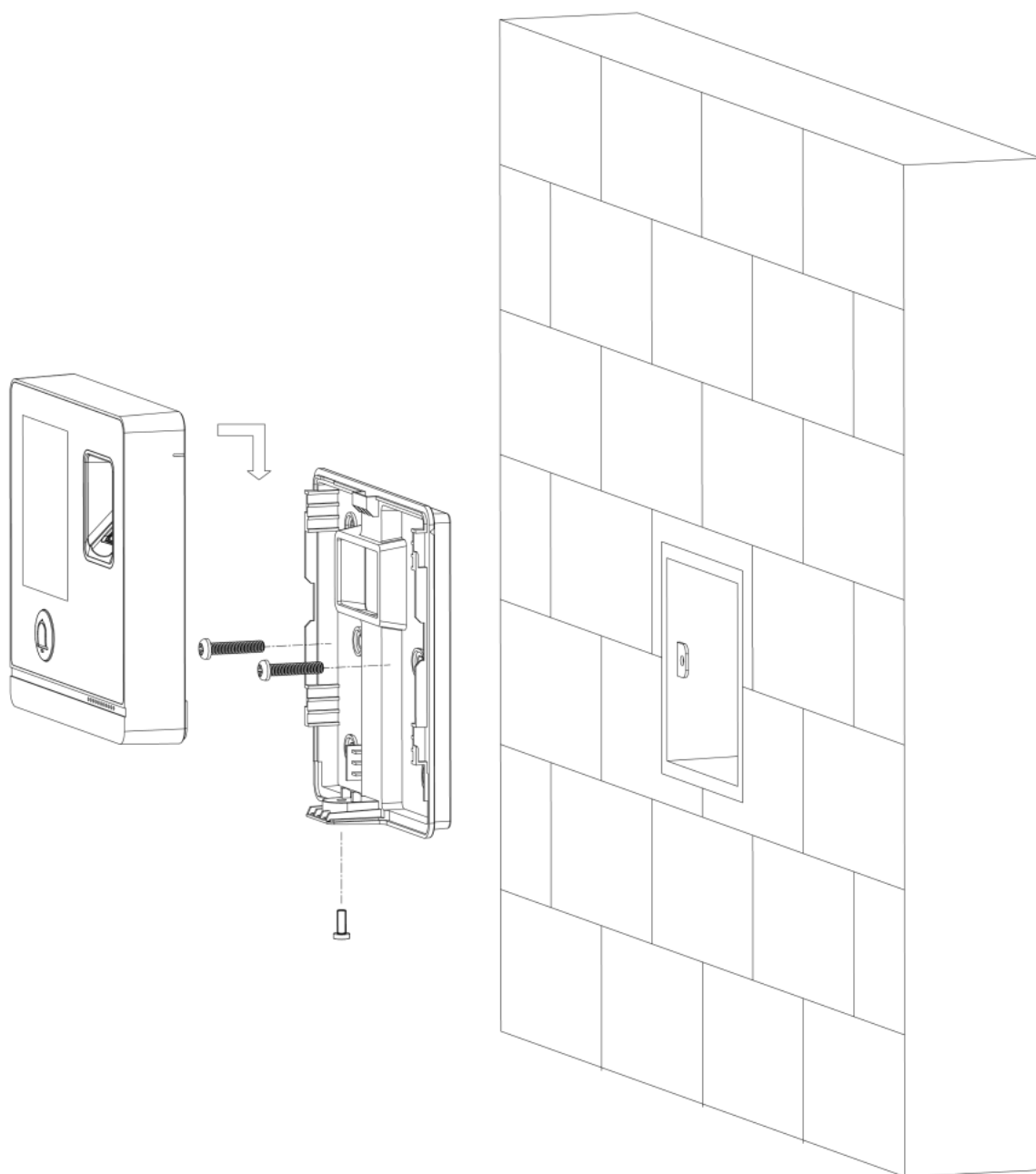


2.3.2 86 Box Mount

Procedure

- Step 1 Unscrew the 2 screws at the bottom of the access standalone, and then remove the back bracket.
- Step 2 Put an 86 box in the wall at an appropriate height.
- Step 3 Fasten the bracket to the 86 box with 2 screws.
- Step 4 Wire the access standalone. For details, see "2.2 Wiring".
- Step 5 Fix the access standalone on the bracket.
- Step 6 Screw in 2 screws securely at the bottom of the access standalone.

Figure 2-8 86 box mount



3 Local Configurations

3.1 Initialization

For first-time use or after restoring factory defaults, you need to set a password and associate your email address for the admin account. You also need to set the time zone of the access standalone. You can use the admin account to log in to the main menu of the access standalone, configure the access standalone, and log in to the web browser and SmartPSS Lite.



- If you forget the administrator password, send a reset request to your reserved Email address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: Upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

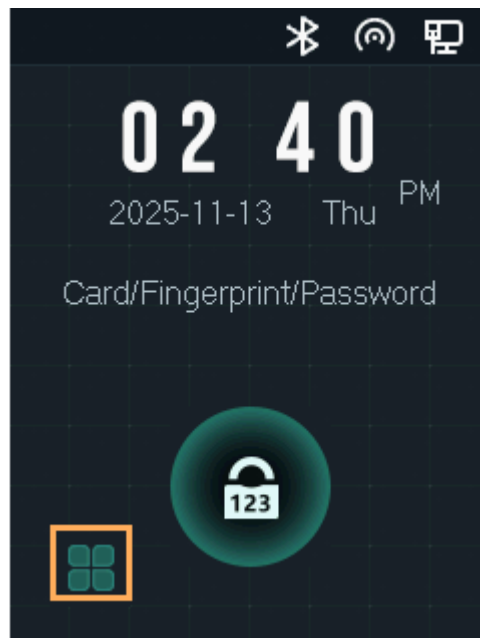
3.2 Logging in to the Main Menu

Log in to the main menu to configure the access standalone. Only admin account and administrator account can enter the main menu of the access standalone. For the first-time use, use the admin account to enter the main menu screen and then you can create the other administrator accounts.

Procedure

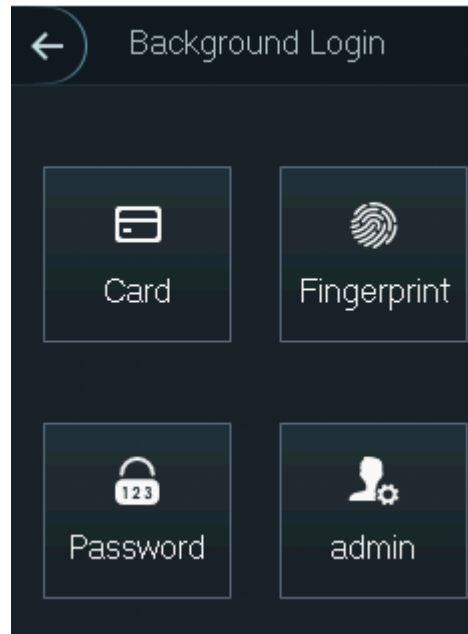
Step 1 On the standby screen, tap .

Figure 3-1 Standby screen



Step 2 Select verification methods.

Figure 3-2 Verification methods



- Fingerprint: After successfully recognizing the administrator's fingerprint, you can go to the main menu.



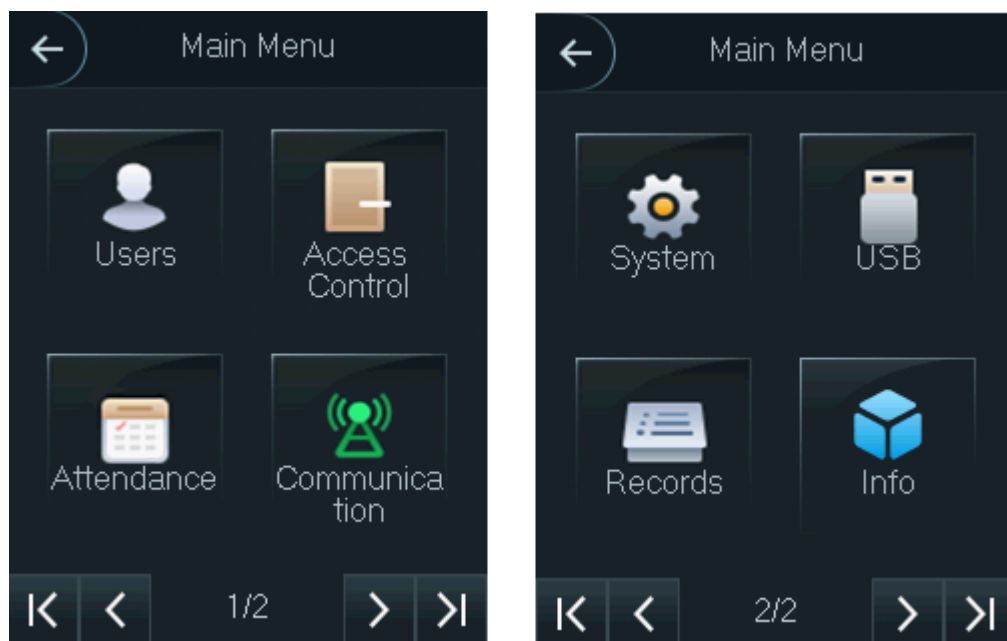
Only supported on select models.

- Card swipe: After successfully recognizing the administrator's card, you can go to the main menu.
- Password: Enter the administrator's ID and password to go to the main menu.
- Admin: Enter the admin password to go to the main menu.

Results

After successful authentication, you can go to the device's main menu.

Figure 3-3 Main menu



3.3 Adding Users

Procedure

Step 1 Log in with the administrator account, and then select **Users > User List**.



The screens in this manual are only for reference, and might differ from the actual product.

Step 2 Tap  at the top-right corner, and then configure user parameters.

Figure 3-4 Add users

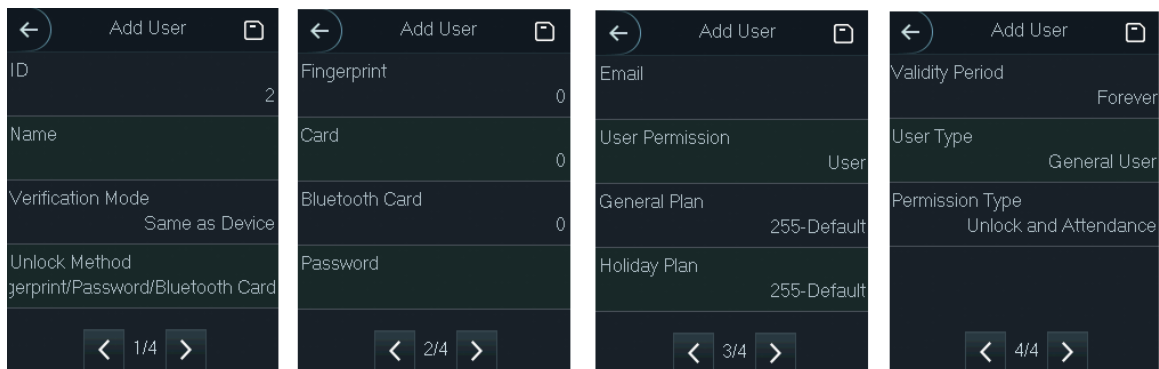


Table 3-1 Description of user parameters

Parameter	Description
ID	Each user ID is unique. It can be 18 characters of numbers, letters, or their combination.
Name	Enter the name (a maximum of 32 characters, including numbers, symbols, and letters).
Verification Mode	Supports configuring verification methods for each personnel.
Unlock Method	- Same as Device: The personnel will use the device's configured verification method for authentication. - Custom: The personnel will be authenticated using the custom methods. Select Custom, and select Unlock Method, tap OK. Select Combinational Element and Combination Method.  ◇ The custom unlock method only supports local device authentication and does not work with external card readers. ◇ If the custom verification method conflicts with the device's default method, the custom configuration takes priority.

Parameter	Description
Fingerprint	Each user can add up to 3 fingerprints. Follow the on-screen prompts and voice prompts to add fingerprints. You can enable the duress fingerprint function under each fingerprint. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress fingerprint.  • We do not recommend setting the first fingerprint as the duress fingerprint. • Only certain models support the fingerprint function.
Card	You can register 5 cards for each user. On the card registration page, swipe your card on the card reader, and then the card information will be read by the Device. You can enable the duress card function on the card registration page. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress card.
Bluetooth Card	You can register 5 Bluetooth cards for each user. On the card registration page, select request through Email or registration code to register your Bluetooth card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is adding 1 based on the last digit of the unlock password. For example, if the user password is 12345, the duress password will be 12346; if the user password is 789, and then the duress password is 780. A duress alarm will be triggered when a duress password is used to unlock the door.
Email	Enter the email that is used for password reset.
Permission Type	You can select a user permission for the new user. • Normal users only have door unlock permission. • Administrators can configure the Device and unlock the door.
General Plan	A user can only have door access within the defined period. The default value is 255, which means no period is configured.
Holiday Plan	A user can only have door access within the scheduled holidays. The default value is 255, which means no holiday plan is configured.
Valid Period	Define a period during which the user has door access control.

Parameter	Description
User Type	● General: General users can unlock the door normally. ● Blocklist: When users in the blocklist unlock the door, service personnel receive a notification. ● Guest: Guests can unlock the door within a defined period or for a certain number of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. ● Patrol: Patrolling users can have their attendance tracked, but they have no unlocking permissions. ● VIP: When VIP users unlock the door, they are not restricted by unlock modes, such as Multi-card and Time Section. ● Others: When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/2: Same as General.

Step 3 Press **Esc** , and then press **OK** to save the settings.

4 Web Configurations

The access standalone supports configuring network and access control parameters through the webpage on a mobile phone or computer. For details, see the corresponding user manual. This section introduces only the methods to log in to the webpage and phone webpage.

4.1 Logging in to the Webpage

Procedure

Step 1 Open a browser, enter the IP address of the access standalone in the **Address** bar, and press the Enter key.

Step 2 Enter the user name and password.



- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can click **Forget password?** to reset password.

Step 3 Click **Login**.

4.2 Logging in to the Phone Webpage

Prerequisites

Make sure that the phone used to log in to the webpage is on the same LAN as the access standalone.

Procedure

Step 1 Open a browser, and then enter to the IP address of the access standalone.

You can log in to the webpage through the following 3 methods:

- The phone and the access standalone are in the same LAN. Open the browser on the phone, and then enter the IP address.
- The phone and the access standalone are in the same LAN. Scan the QR code through **Communication Settings** > **Network Settings** > **Wi-Fi** on the webpage of your phone.
- Connect the hotspot of the Device on your phone. On the main screen of the device, tap the upper-right corner to go to **Wi-Fi AP** screen. Scan the IP address QR code through the browser on your phone, or in the browser of your phone, enter the IP address that is displayed in the **Wi-Fi AP** screen.

You can also select **Communication Settings** > **Network Settings** > **Wi-Fi AP** to go to the main menu.



Wi-Fi and Wi-Fi AP are available on select models.

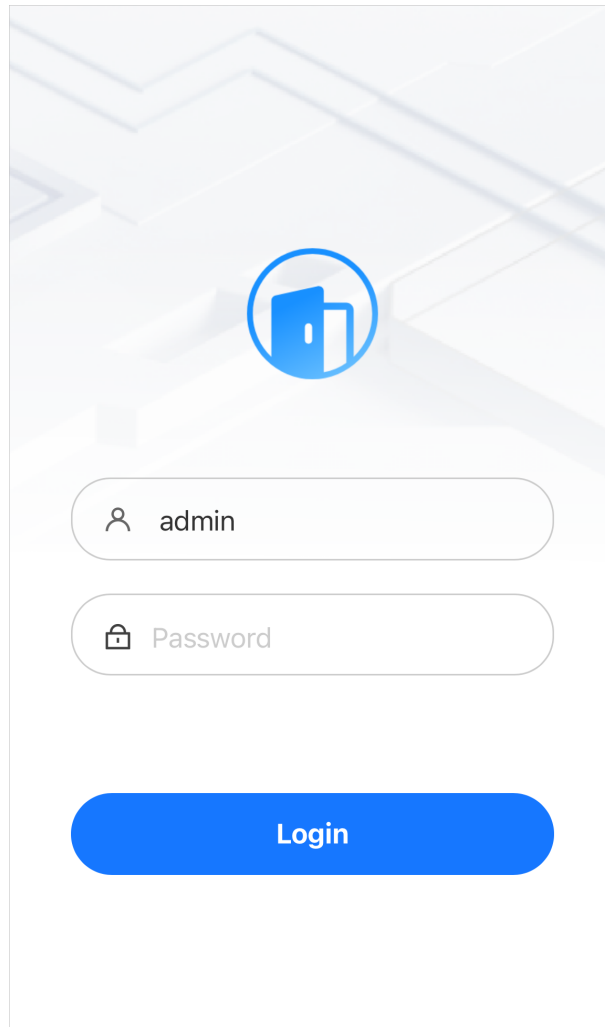
Step 2 Enter the user name and password.

Click  next to the password to view it.



- The default administrator name is admin, and the password is the one you set up during initialization. We recommend you change the administrator password regularly to increase security.
- If you forget the administrator login password, you can reset the password through the webpage on the computer.

Figure 4-1 Login page

The image shows a login page with a light gray background featuring a subtle geometric pattern. At the top center is a blue circular icon containing a white stylized building or folder symbol. Below this icon are two input fields: the first contains the text 'admin' preceded by a small person icon, and the second contains the text 'Password' preceded by a small lock icon. At the bottom of the form is a large, rounded blue button with the word 'Login' in white text.

Step 3 Tap **Login**.

Appendix 1 Important Points of Fingerprint Registration Instructions

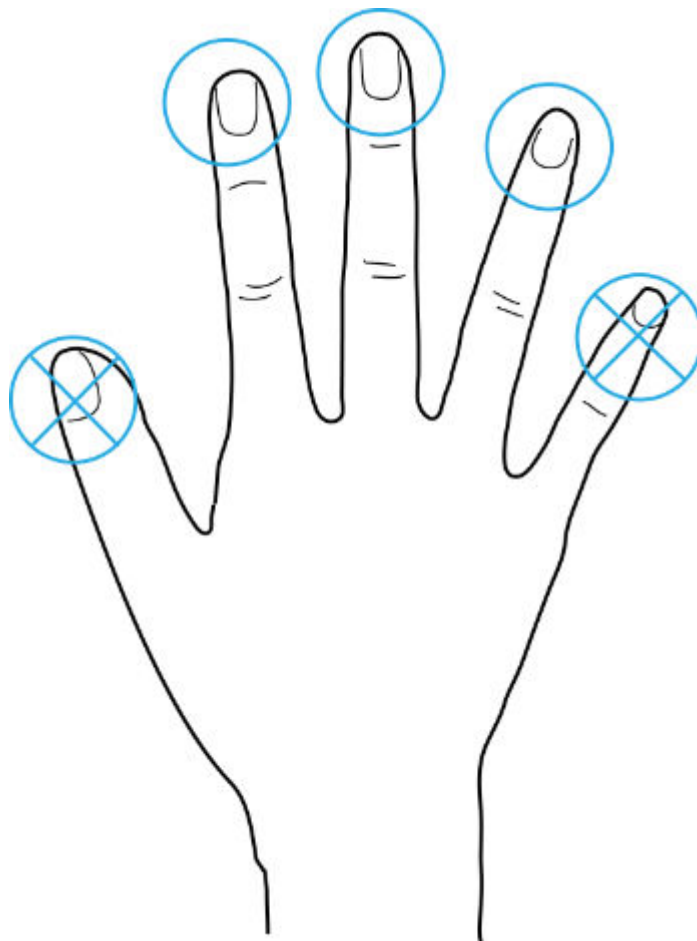
When you register the fingerprint, pay attention to the following points:

- Make sure that your fingers and the scanner surface are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

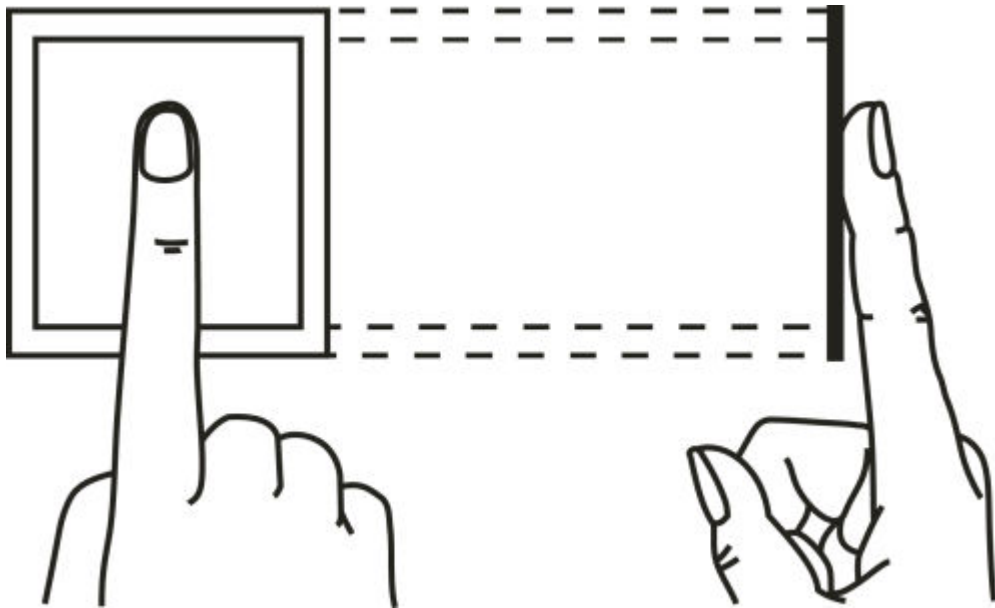
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

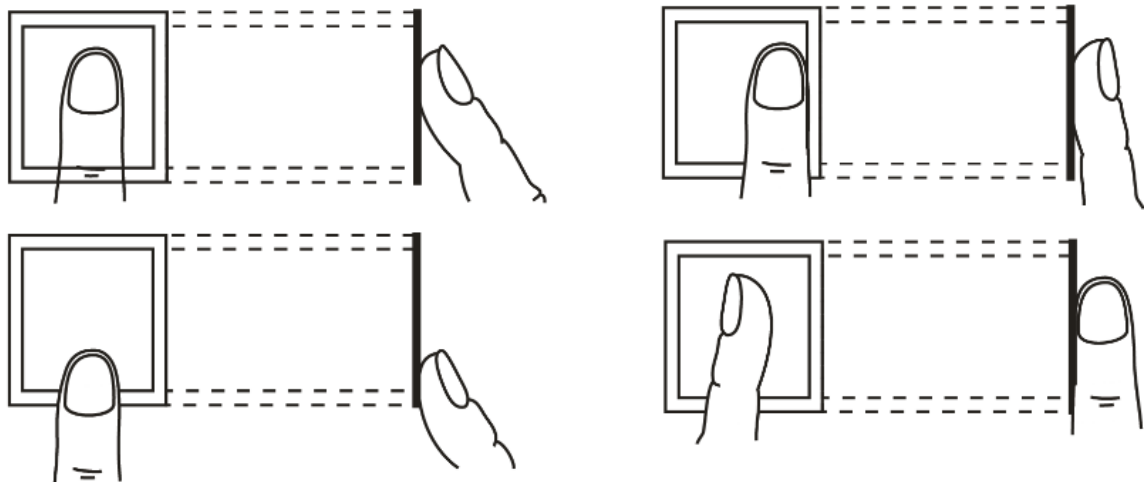


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 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 logout function

The account logout 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 Allowlist**

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

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;
- Establish 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).