Access Standalone

Quick Start Guide



V1.0.2

Foreword

General

This manual introduces the installation and operations of the Access Standalone. 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
V1.0.1	Updated the manual.	November 2022
V1.0.0	First Release.	October 2022

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 Standalone, hazard prevention, and prevention of property damage. Read carefully before using the Access Standalone, and comply with the guidelines when using it.

Transportation Requirement



Transport, use and store the Access Standalone under allowed humidity and temperature conditions.

Storage Requirement



Store the Access Standalone under allowed humidity and temperature conditions.

Installation Requirements



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

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Structure 1

2 Wiring and Installation 2

2.1 Wiring 2

2.2 Installation Requirements 3

2.3 Installation Process 5

2.3.1 Wall mount 5

2.3.2 86 Box Mount 6

3 Local Configurations 7

3.1 Initialization 7

3.2 Adding New User 7

4 Web Configurations 10

4.1 Initialization 10

4.2 Logging In 10

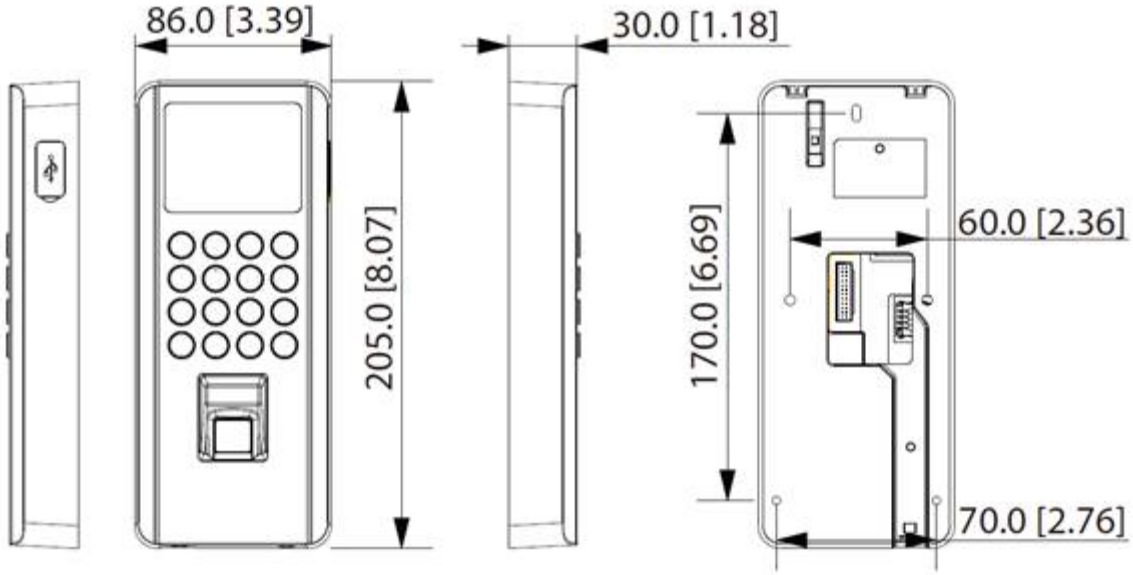
Appendix 1 Important Points of Fingerprint Registration Instructions 12

Appendix 2 Cybersecurity Recommendations 14

1 Structure

The front appearance might differ depending on different models of the Access Standalone.

Figure 1-1 Structure of Access Standalone (fingerprint model) (Unit: mm [inch])



2 Wiring and Installation

2.1 Wiring

Figure 2-1 Wiring of Access Standalone (ASI22XXJ)

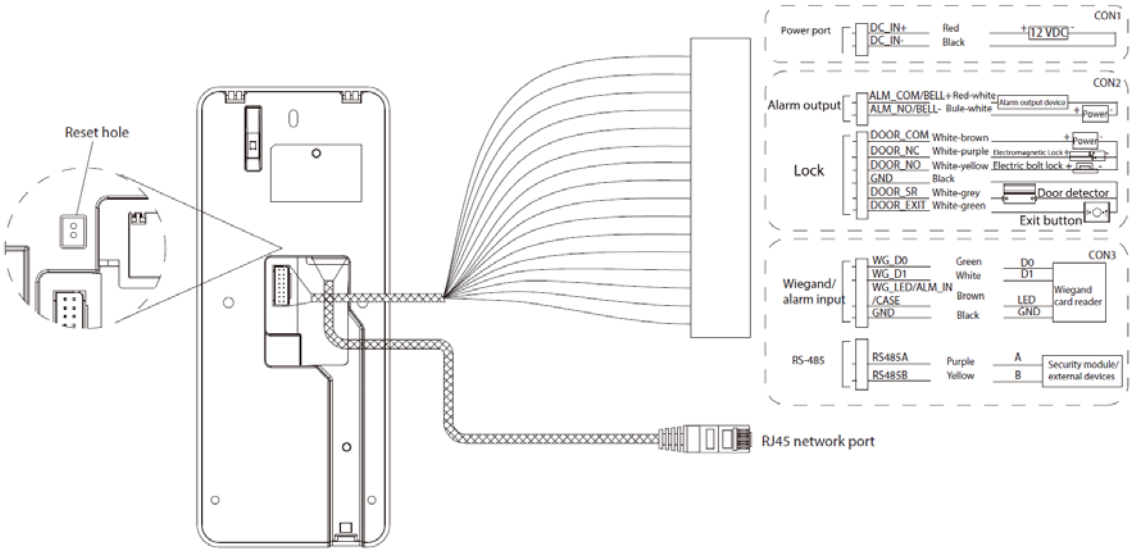
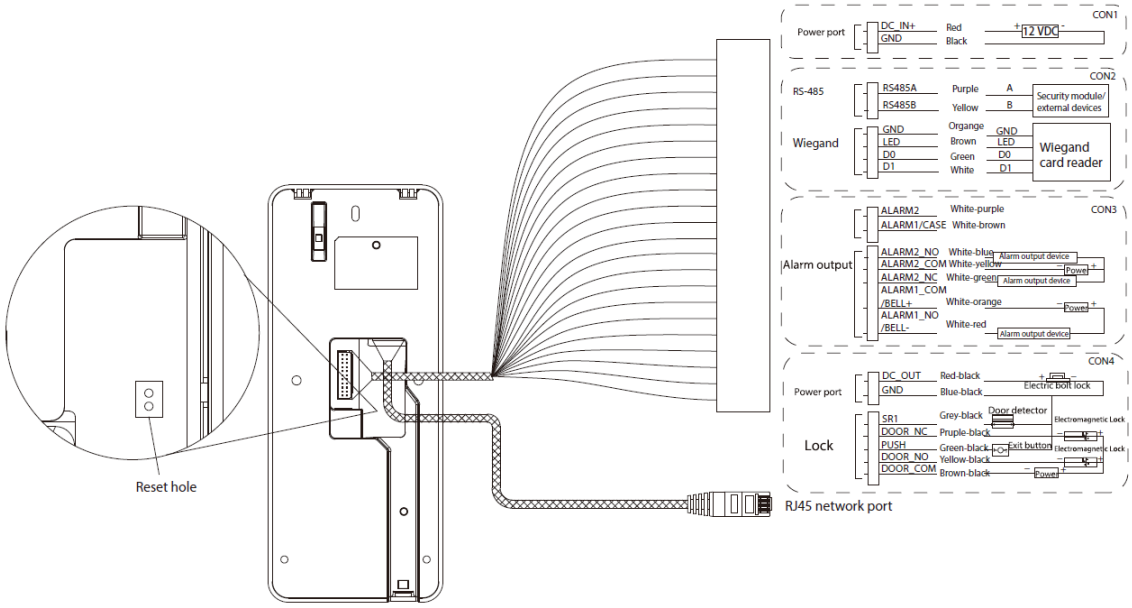


Figure 2-2 Wiring of Access Standalone (ASI22XXJ-(D)PW)



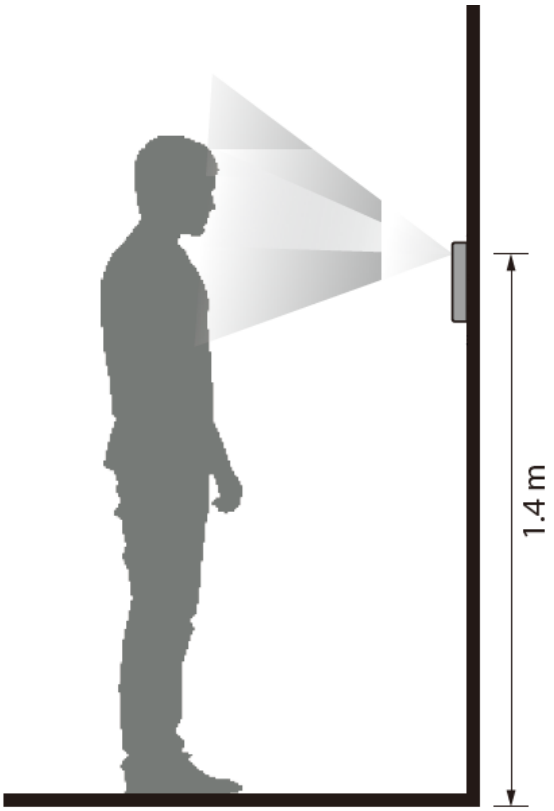
- For alarm output, connect the alarm device ALARM2_NC or ALARM2_NO according to the type of the alarm output devices.
- For door lock, connect the lock to DOOR_NC or DOOR_NO according to the type of the lock.
- Certain wires can be used for different purposes. On the webpage of the Access Standalone, select **Config Mgmt.** > **Interface Config**, and then you can set the function of ports.

2.2 Installation Requirements

- 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 2-3 Installation height requirement



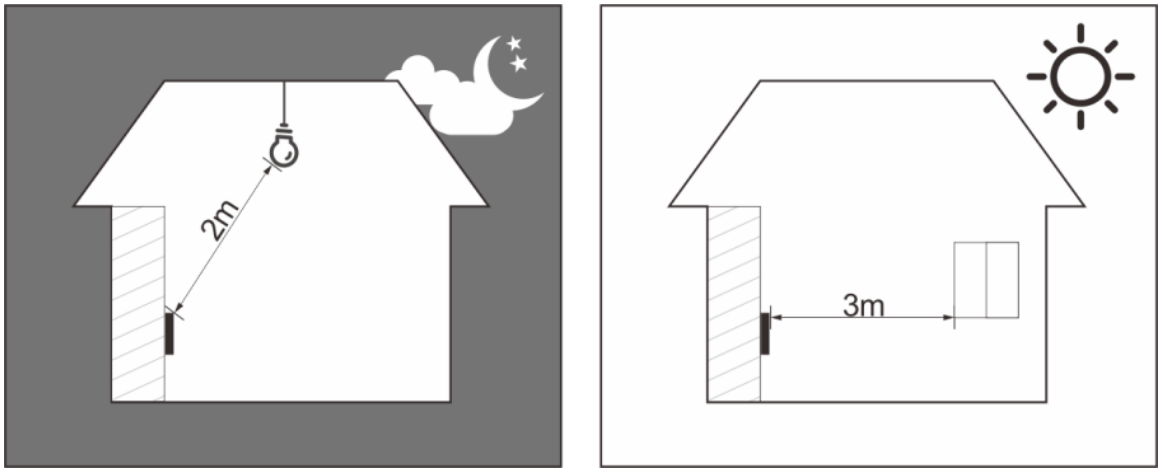
Ambient Illumination Requirements

Figure 2-4 Ambient illumination requirements



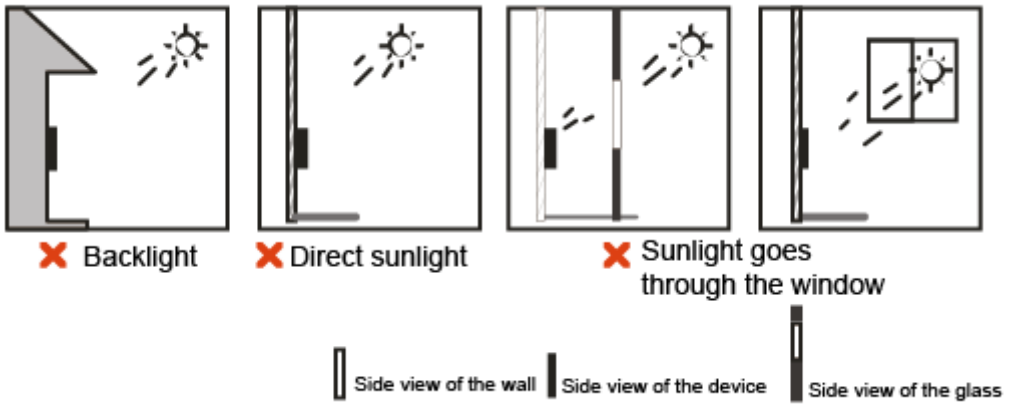
Recommended Installation Locations

Figure 2-5 Recommended installation locations



Installation Locations Not Recommended

Figure 2-6 Installation locations not recommended



2.3 Installation Process

The Access Standalone supports 2 installation methods: wall mount and 86 case mount. The recommended installation height is 1.2 m–1.6 m.

2.3.1 Wall mount

Procedure

Step 1 Unscrew the 2 screws at the bottom of the Access Standalone, and then remove the back bracket.

Step 2 According to the holes' position of the back bracket, drill 3 holes, and then put expansion bolts in the holes.

Drill 1 cable outlet in the wall if you use in-wall wiring.

Step 3 Use the 3 screws to fix the bracket to the wall.

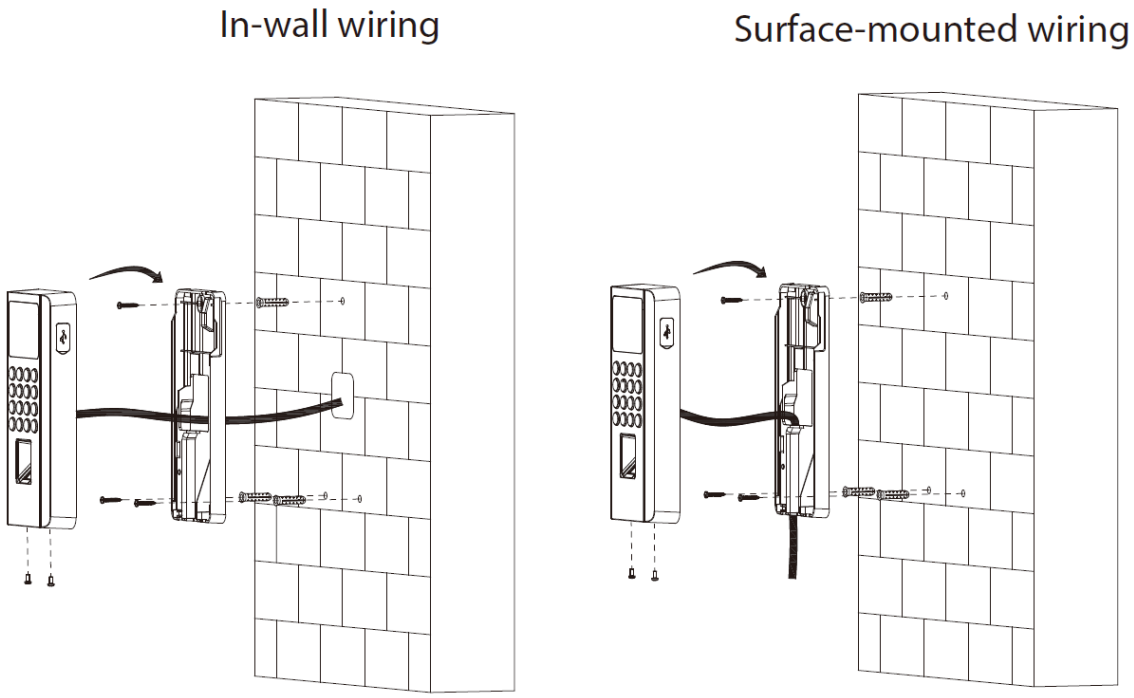
For surface-mounted wiring, pass the wires through the back bracket first, and then fix the back bracket to the wall.

Step 4 Wire the Access Standalone. For details, see "2.1 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 2-7 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.

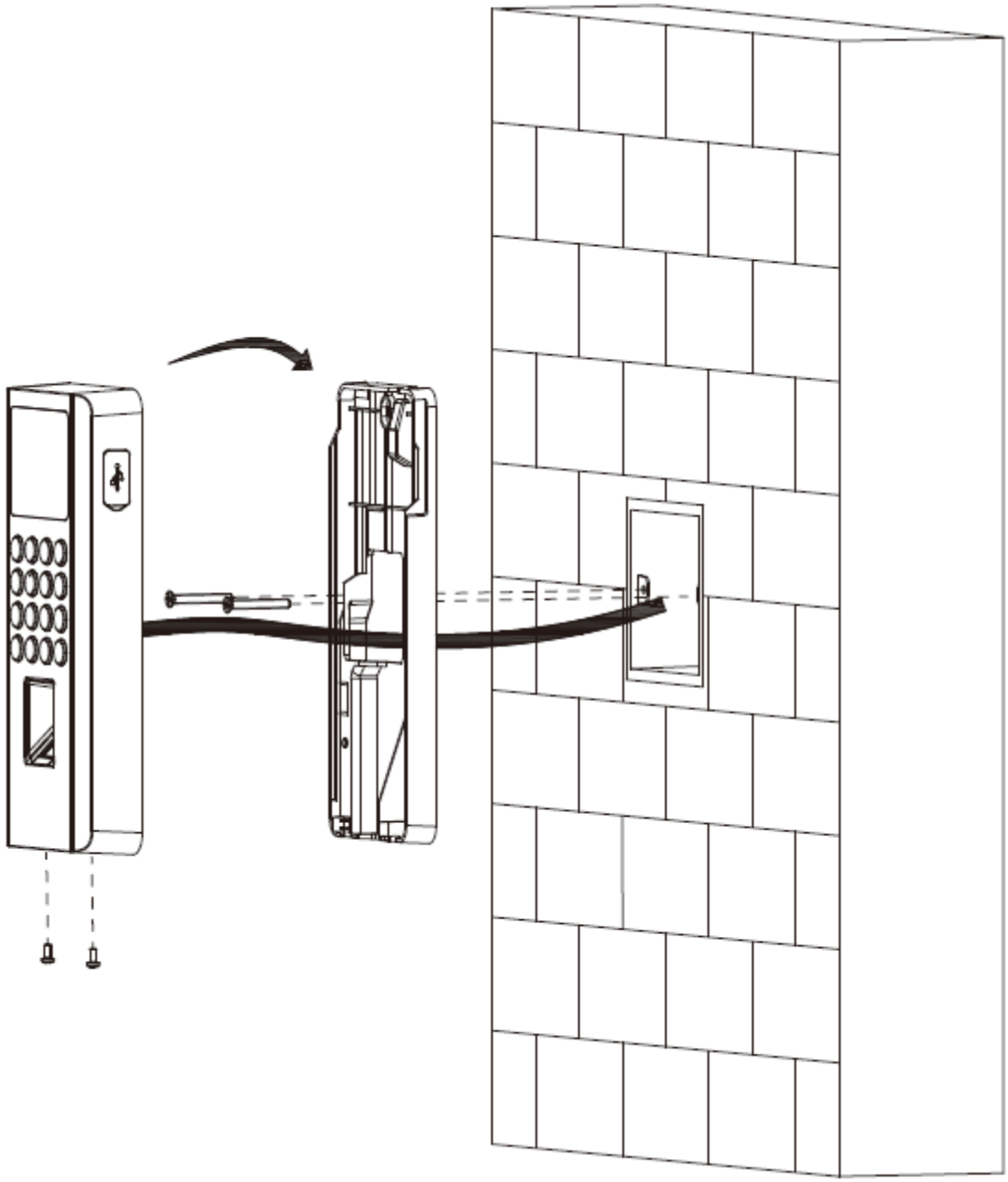
Step 3 Fasten the bracket to the 86 box with 2 screws.

Step 4 Wire the Access Standalone. For details, see "2.1 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

Local operations might differ depending on different models of Access Standalone.

3.1 Initialization

For the first-time use or after restoring factory defaults, you need to set a password and email address for the admin account. You can use the admin account to log in to the main menu screen of the Access Standalone and its webpage.

Figure 3-1 Initialization



- 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.
- If you forget the administrator password, send a reset request to your linked e-mail address.

3.2 Adding New User

Procedure

Step 1 Tap【∧】or【∨】to select on the standby screen, and then tap **OK**.

Step 2 Log in with the administrator account, and then select **User** > **New User**.

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

Figure 3-2 Add a new user



Step 3 Configure the parameters.

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).
Fingerprint	Each user can add up to 3 fingerprints. Follow the on-screen instructions 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 you set the first fingerprint as the duress fingerprint. ● Only Access Standalone of fingerprint model supports 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.
PWD	Enter password to unlock the door. The maximum length of the ID digits is 8.
Permission	You can select a user permission for the new user. ● Normal users only have door unlock permission. ● Administrators can configure the Access Standalone and unlock the door.
Period	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 Date	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**: Paroling users can have their attendance tracked, but they have no unlocking permissions. • **VIP**: When VIP unlock the door, service personnel will receive a notification. The VIP user is 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 4 After you have configured all the parameters, tap **Esc**.

Step 5 Tap **OK** to save the changes.

4 Web Configurations

You can access the webpage of the Access Standalone through your computer or phone, and configure or update the Access Standalone.

Web configurations differ depending on models of the Access Standalone.

4.1 Initialization

Initialize the Access Standalone when you log in to the webpage for the first time or after the Access Standalone is restored to the factory defaults.

Prerequisites

Make sure that the computer or the phone is on the same LAN as the Access Standalone.

Procedure

Step 1 Open a web browser, and go to the IP address (the default address is 192.168.1.108) of the Access Standalone.

You can log in to the web with Chrome or Firefox.

Step 2 Enter and confirm the password, enter an email address, and then click **Completed**.

- 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.
- Keep the password safe after initialization and change the password regularly to improve security.
- If you want to reset the administrator password by scanning the QR code, you need the linked email address to receive the security code.

4.2 Logging In

Procedure

Step 1 Open a web browser, go to the IP address of the Access Standalone.

Step 2 Enter the user name and password.



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

Step 3 Click **Login**.

Appendix 1 Important Points of Fingerprint Registration Instructions

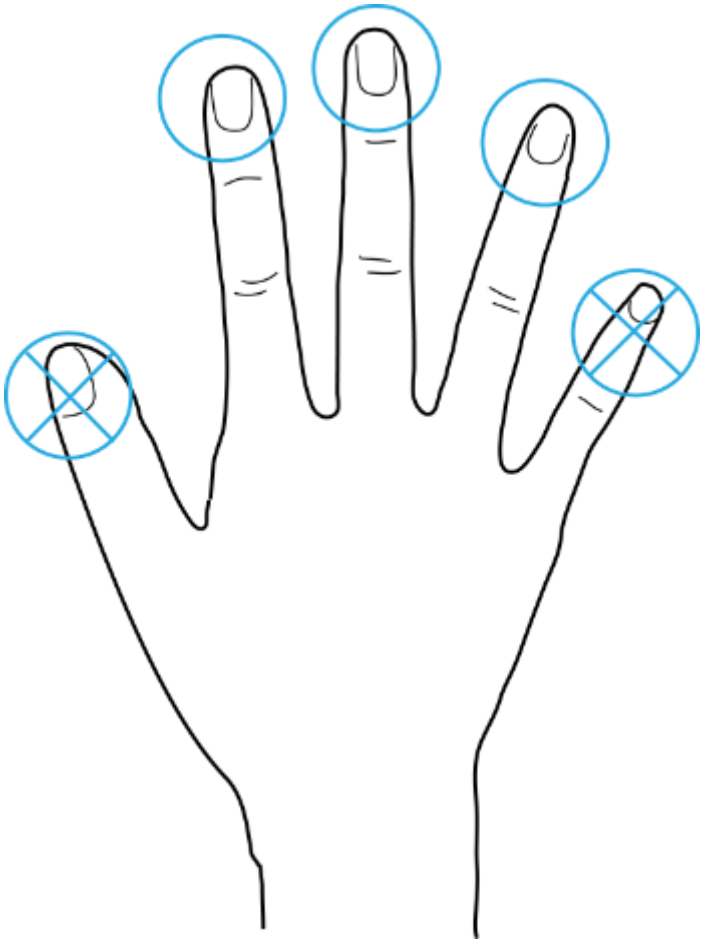
When you register the fingerprint, pay attention to the following points:

- 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

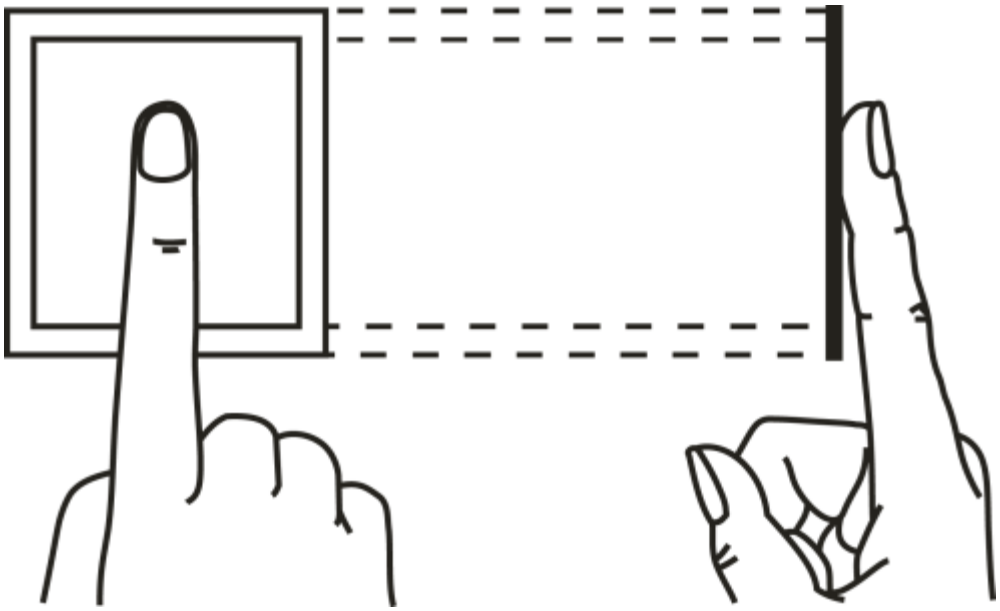
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

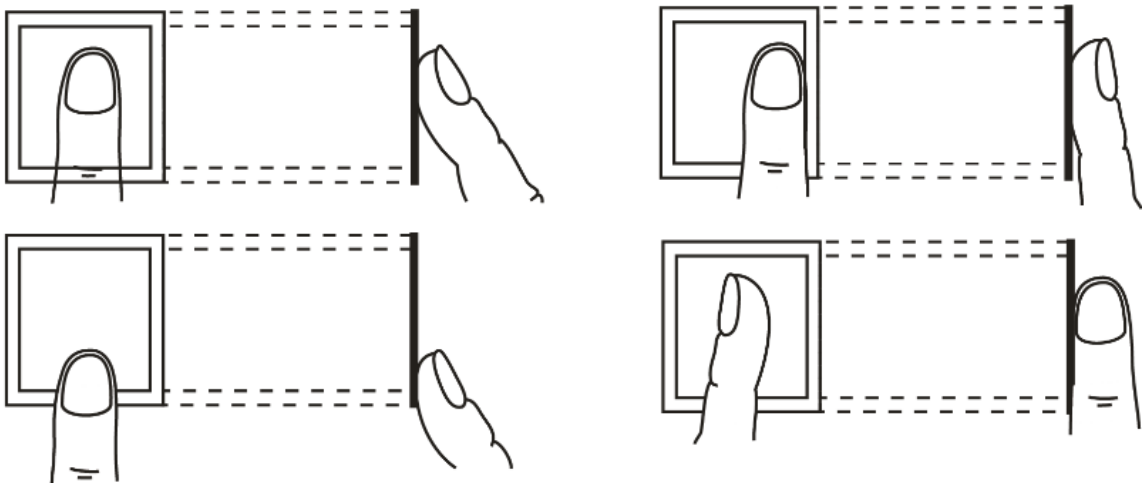


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct placement



Appendix Figure 1-3 Wrong placement



Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters.
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
   - Do not contain the account name or the account name in reverse order.
   - Do not use continuous characters, such as 123, abc, etc.
   - Do not use overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the"auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.