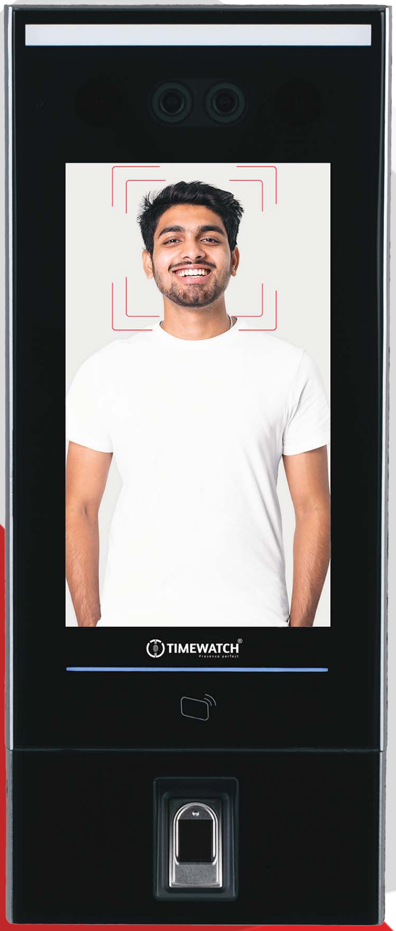
TIMEWATCH®

Presence perfect



Face Recognition Device

TrueFace1L-FP

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation and basic operations of the Face Recognition Access Controller (hereinafter referred to as the "Access Controller"). 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.	July 2023

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

Transportation Requirement

⚠

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

Storage Requirement

⚠

Store the Access Controller under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Do not connect the power adapter to the Access Controller 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 Controller to two or more kinds of power supplies, to avoid damage to the Access Controller.
- 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 Controller in a place exposed to sunlight or near heat sources.
- Keep the Access Controller away from dampness, dust, and soot.
- Install the Access Controller on a stable surface to prevent it from falling.
- Install the Access Controller 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 Controller label.
- The Access Controller is a class I electrical appliance. Make sure that the power supply of the Access Controller is connected to a power socket with protective earthing.

Operation Requirements

⚠

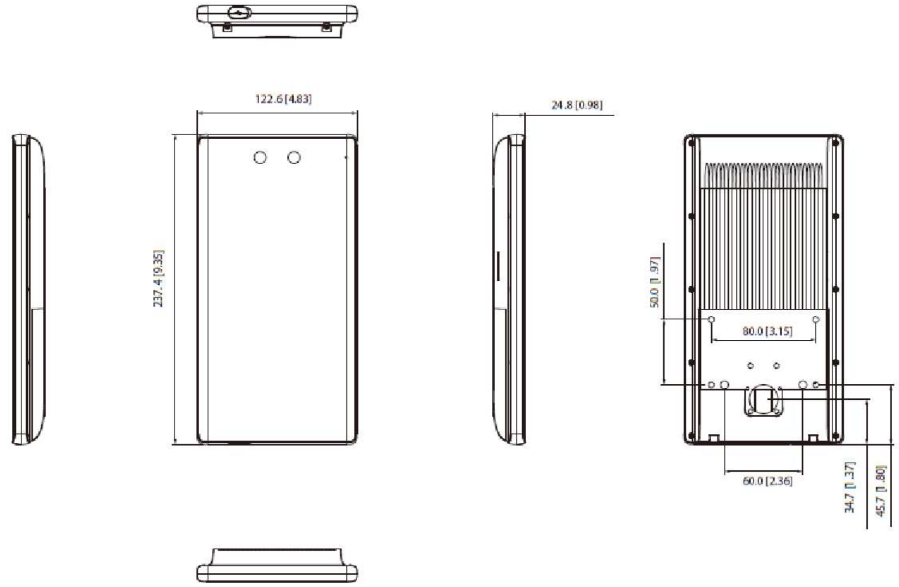
- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Access Controller while the adapter is powered on.
- Operate the Access Controller within the rated range of power input and output.
- Use the Access Controller under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Access Controller, and make sure that there is no object filled with liquid on the Access Controller to prevent liquid from flowing into it.
- Do not disassemble the Access Controller without professional instruction.
- This product is professional equipment.
- The Access Controller is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Appearance

The front appearance might differ depending on different models of the Access Controller. Here we use the Wi-Fi model as an example.

Figure 1-1 Structure (Unit: mm [inch])

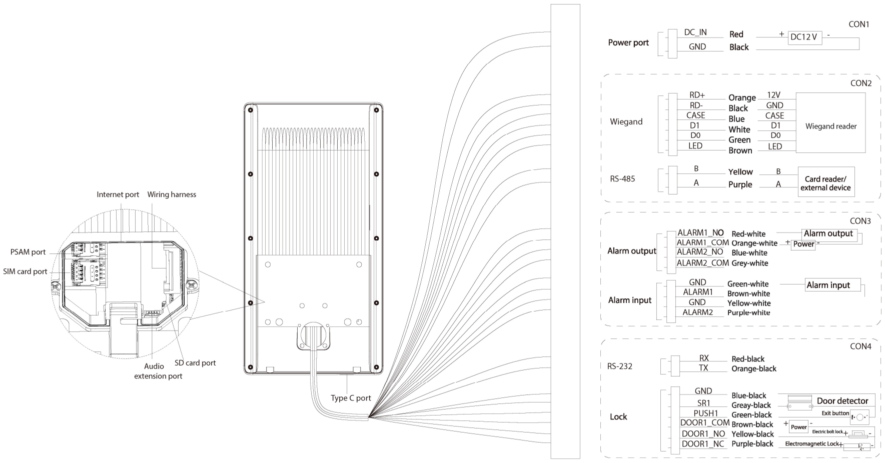


2 Wiring and Installation

2.1 Wiring

The access controller needs to be connected to devices like sirens, readers, and door contacts.

Figure 2-1 Cable connections



📖

- The back panel of the Access Controller has SIM card port, Internet port, audio extension port, SD card port and wiring harness. Ports might differ depending on different models of Access Controller.
- If you want to connect an external speaker, an audio adapter cable is required.
- The load capacity of type C port is 5 V 500 mA.
- The load capacity of RD+ and RD- port is 12 V 200 mA.

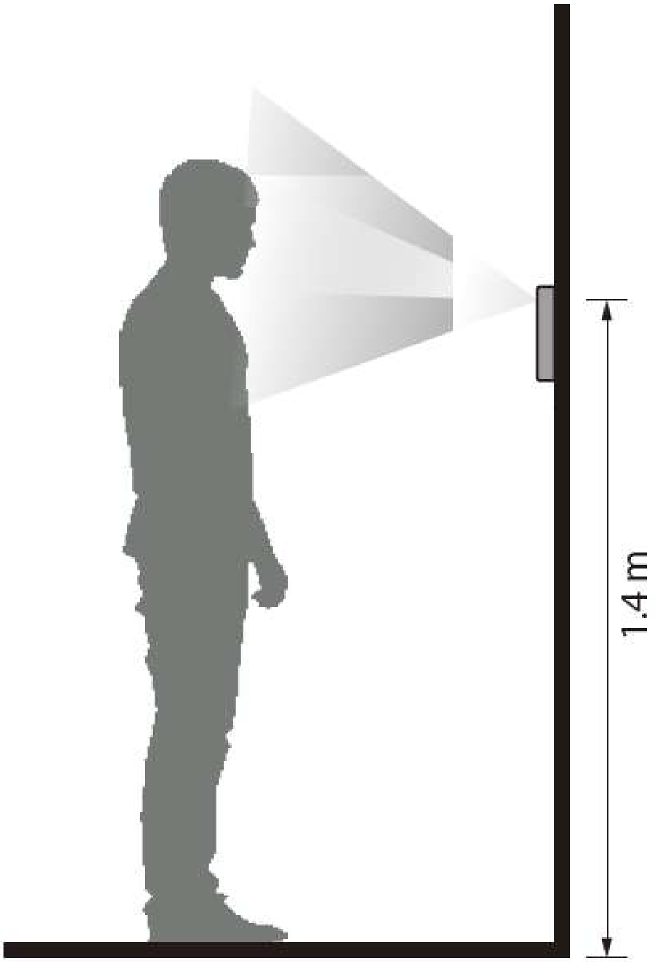
2.2 Installation Requirements

📖

- The light at the 0.5 meters away from the access controller should be no less than 100 Lux.
- We recommend you install the Access Controller 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.

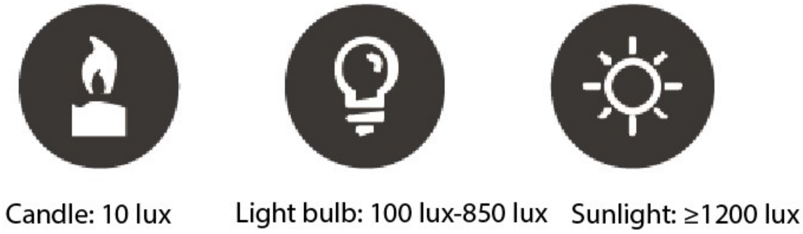
Installation Height

Figure 2-2 Installation height requirement



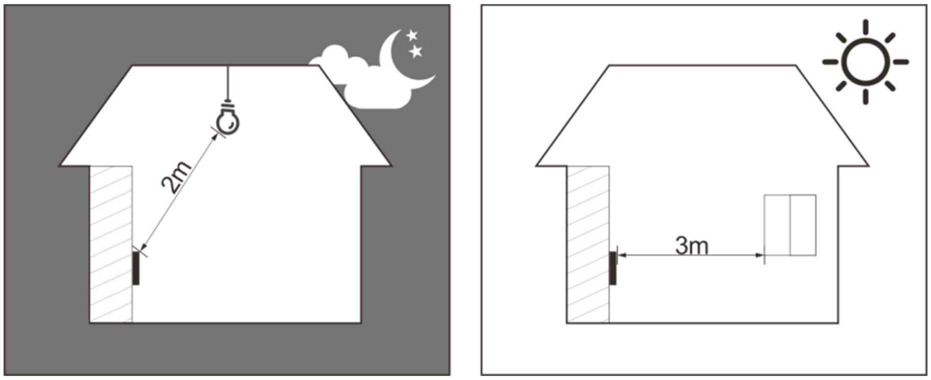
Ambient Illumination Requirements

Figure 2-3 Ambient illumination requirements



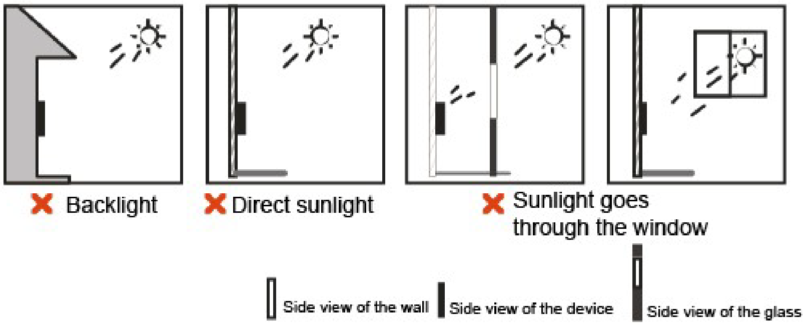
Recommended Installation Location

Figure 2-4 Recommended installation location



Installation Location Not Recommended

Figure 2-5 Installation location not recommended



2.3 Installation Process

The Access Controller has four installation methods: wall mount, floor bracket mount, turnstile mount and 86 case mount. This section only introduces wall mount and 86 case mount. For details of floor bracket mount and turnstile mount, please refer to user's manual of corresponding devices.

2.3.1 Wall mount

Procedure

Step 1 According the holes' position of the bracket, drill four holes and one cable outlet in the wall. Put expansion bolts in the holes.

Step 2 Remove the sheet metal at the bottom of the bracket.

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

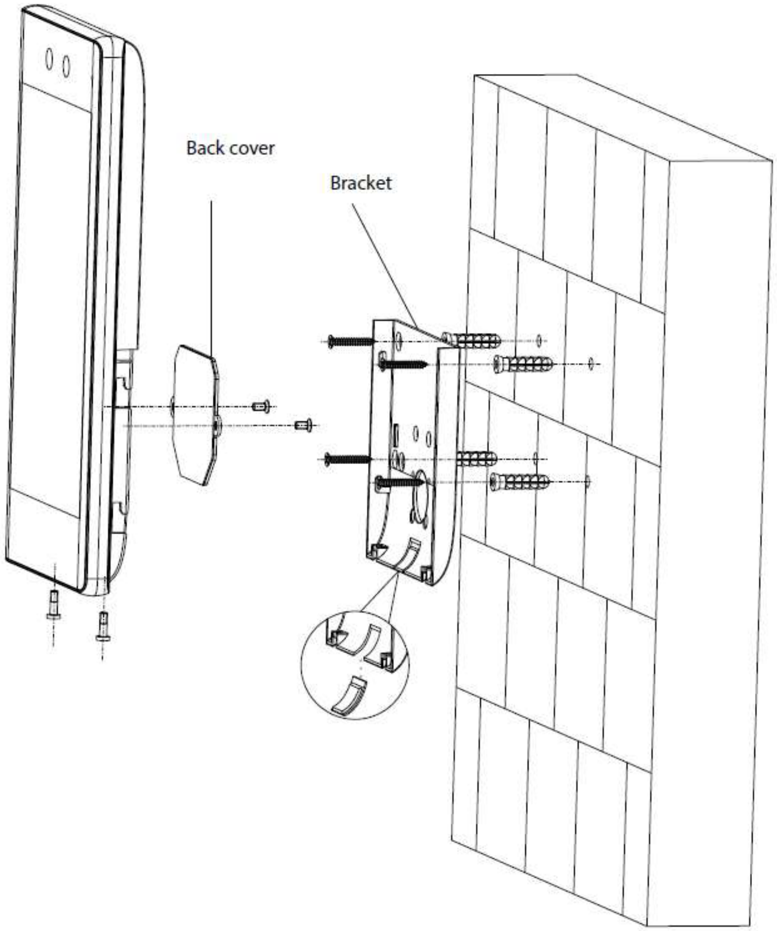
Step 4 Wire the Access Controller. For details, see "2.1 Wiring".

Step 5 Use two screws to fix the back cover to the Access Controller.

Step 6 Fix the Access Controller on the bracket.

Step 7 Screw in two screws securely at the bottom of the Access Controller.

Figure 2-6 Wall mount



2.3.2 86 Box Mount

Procedure

Step 1 Put an 86 case in the wall at an appropriate height.

Step 2 Fasten the bracket to the 86 case with two screws.

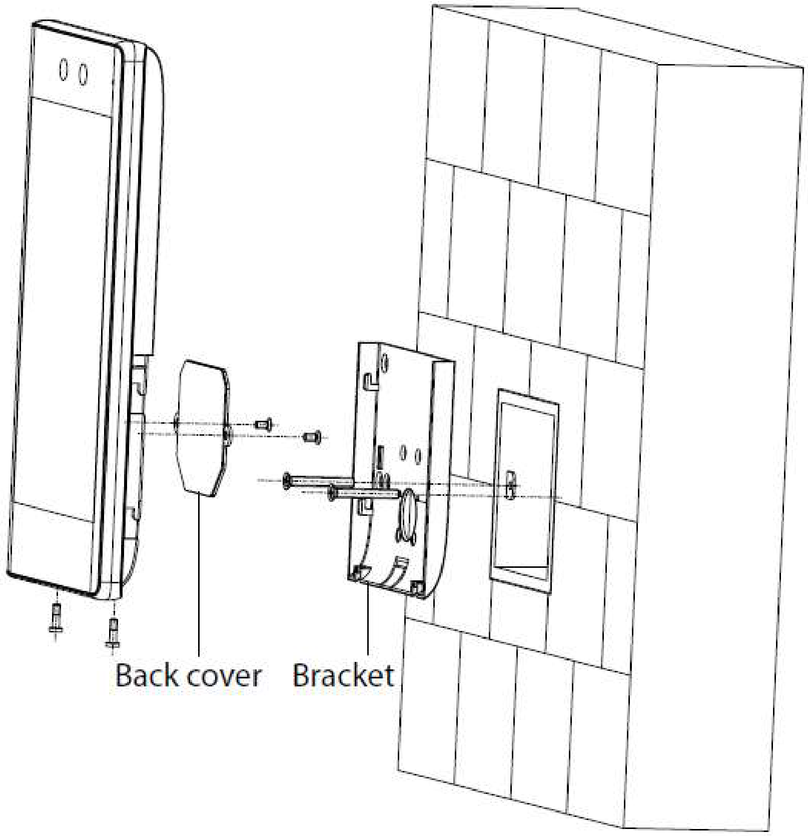
Step 3 Wire the Access Controller. For details, see "2.1 Wiring".

Step 4 Use two screws to fix the back cover to the Access Controller.

Step 5 Fix the Access Controller on the bracket.

Step 6 Screw in two screws securely at the bottom of the Access Controller.

Figure 2-7 86 case mount



3 Local Configurations

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

3.1 Initialization

For the first-time use or after restoring factory defaults, you need to select a language on Access Controller, and then set the password and email address for the admin account. You can use the admin account to enter the main menu of the Access Controller and its webpage.

🕮

- If you forget the administrator password, send a reset request to your registered e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

3.2 Logging In

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

Background Information

- admin account: Can log in to the main menu screen of the Access Controller, but does not have door access permissions.
- Administrator account: Can log in to the main menu of the Access Controller and has door access permissions.

Procedure

Step 1 Press and hold the standby screen for 3 seconds.

Step 2 Select a verification method to enter the main menu.

- Face: Enter the main menu by face recognition.
- Fingerprint: Enter the main menu by using fingerprint.

  🕮

  Fingerprint function is only available on select models.
- Card Punch: Enter the main menu by swiping card.
- PWD: Enter the user ID and password of the administrator account.
- admin: Enter the admin password to enter the main menu.

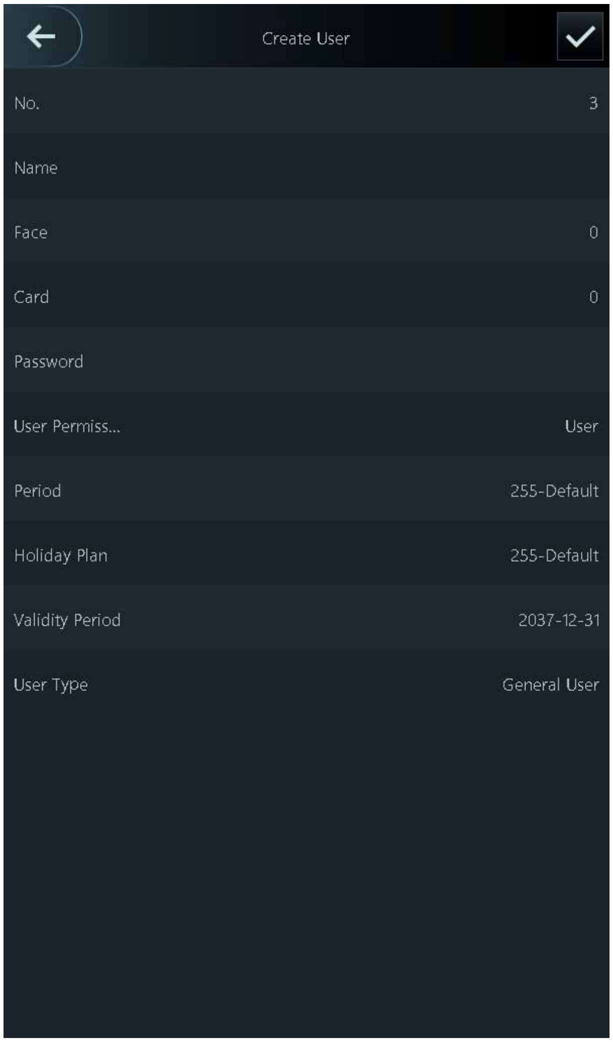
3.3 Adding Users

Procedure

Step 1 On the Main Menu , select Person Management > Create User .

Step 2 Configure the parameters on the interface.

Figure 3-1 Add new user



No. 3

Name

Face 0

Card 0

Password

User Permiss... User

Period 255-Default

Holiday Plan 255-Default

Validity Period 2037-12-31

User Type General User

Table 3-1 Parameters description

Parameter	Description
No.	The No. is like employee ID, which can be numbers, letters, and their combinations, and the maximum length of the No. is 32 characters.

Parameter	Description
Name	The name can have up to 30 characters (including numbers, symbols, and letters).
FP	Register fingerprints. A user can register up to 3 fingerprints, and you can set a fingerprint to the duress fingerprint. An alarm will be triggered when the duress fingerprint is used to unlock the door. 📖 Fingerprint function is only available on select models. We do not recommend you set the first fingerprint as the duress fingerprint. One user can only set one duress fingerprint. Fingerprint function is available if the Access Controller supports connecting a fingerprint extension module.
Face	Position your face inside the frame, and a face image will be captured automatically. You can register again if you are not satisfied with the outcome.
Card	A user can register up to 5 cards at most. Enter your card number or swipe your card, and then the card information will be read by the access controller. You can enable the Duress Card function. An alarm will be triggered if a duress card is used to unlock the door. 📖 One user can only set one duress card.
Password	Enter the user password. The maximum length of the password is 8 digits. The duress password is the unlock password + 1. For example, if the user password is 12345, the duress password will be 12346. A duress alarm will be triggered when a duress password is used to unlock the door.
User Permission	User : Users only have door access or time attendance permissions. Admin : Administrators can configure the Access Controller besides door access and attendance permissions.
Period	People can unlock the door or take attendance during the defined period.

Parameter	Description
Holiday Plan	People can unlock the door or take attendance during the defined holiday.
Validity Period	Set a date on which the door access and attendance permissions of the person will be expired.
User Type	General User : General users can unlock the door. Blocklist User : When users in the blocklist unlock the door, an blocklist alarm will be triggered. Guest User : Guests can unlock the door within a defined period or for certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door. Patrol User : Patrol users can take attendance on the Access Controller, but they do not have door permissions. VIP User : When VIP unlocks the door, service personnel will receive a notification. Other User : When they unlock the door, the door will stay unlocked for 5 more seconds. Custom User 1/Custom User 2 : Same with general users.
Department	Select departments, which is useful when configuring department schedules. 🕮 This function is only available on select models.
Schedule Mode	Department Schedule: Apply department schedules to the user. Personal Schedule: Apply personal schedules to the user. 🕮 ◇ This function is only available on select models. ◇ If you set the schedule mode to department schedule here, the personal schedule you have configured for the user in Attendance > Schedule Config > Personal Schedule become invalid.

Step 3 Tap ☑

4 Web Configurations

On the web interface, you can also configure and update the Access Controller.

Web configurations differ depending on models of the Access Controller.

4.1 Initialization

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

Prerequisites

Make sure that the computer used to log in to the webpage is on the same LAN as the Access Controller.

Procedure

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

We recommend you use the latest version of Chrome or Firefox.

Step 2 Select a language on Access Controller.

Step 3 Set the password and email address according to the screen instructions.

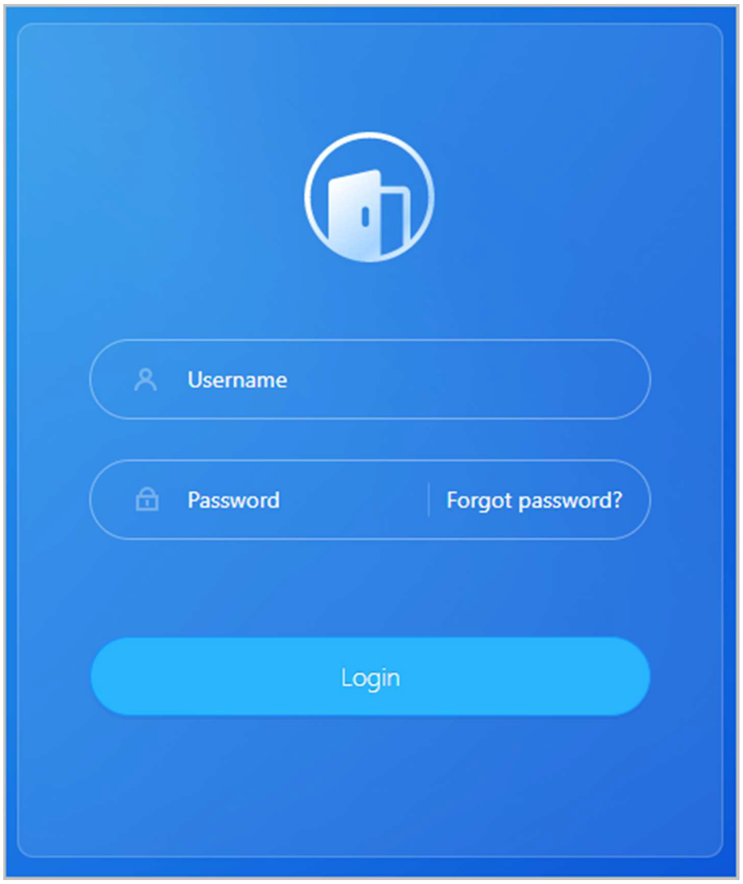
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.
- Keep the password safe after initialization and change the password regularly to improve security.

4.2 Logging In

Procedure

Step 1 Open a browser, enter the IP address of the Access Controller in the Address bar, and press the Enter key.

Figure 4-1 Log in



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? For details,

Step 3 Click Login .

Appendix 1 Important Points of Face Registration

Before Registration

- Glasses, hats, and beards might influence face recognition performance.
- Do not cover your eyebrows when wearing hats.
- Do not change your beard style greatly if you use the Device; otherwise face recognition might fail.
- Keep your face clean.
- Keep the Device at least 2 meters away from light source and at least 3 meters away from windows or doors; otherwise backlight and direct sunlight might influence face recognition performance of the access controller.

During Registration

- You can register faces through the Device or through the platform. For registration through the platform, see the platform user manual.
- Make your head center on the photo capture frame. The face image will be captured automatically.

📖

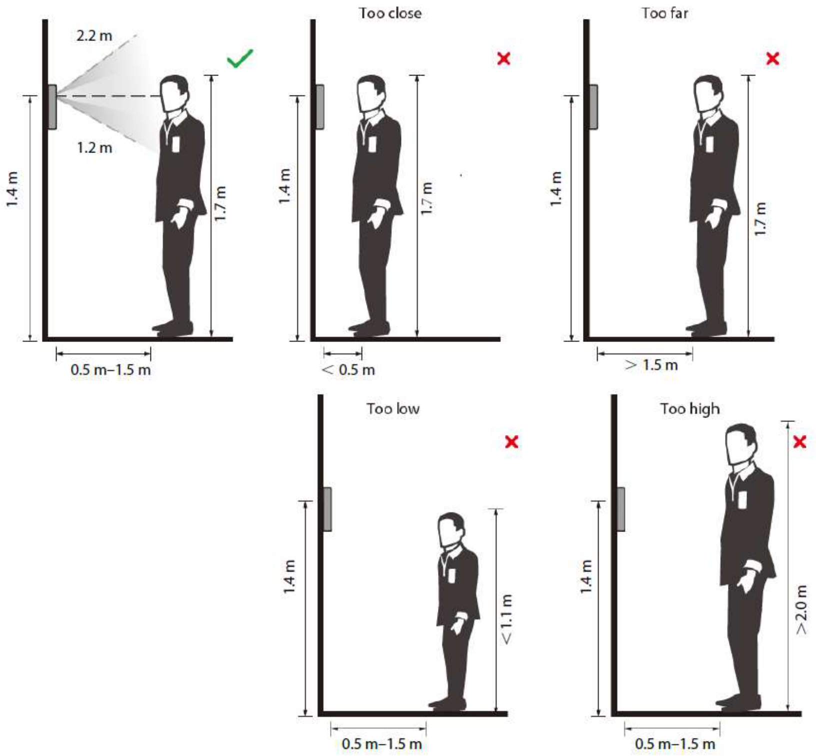
- Do not shake your head or body, otherwise the registration might fail.
- Avoid 2 faces appear in the capture frame at the same time.

Face Position

If your face is not at the appropriate position, face recognition accuracy might be affected.

The face position below is for reference only, and might differ from the actual situation.

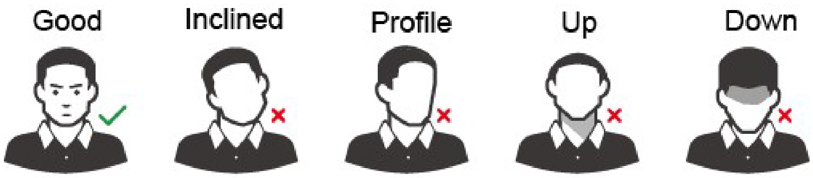
Appendix Figure 1-1 Appropriate face position



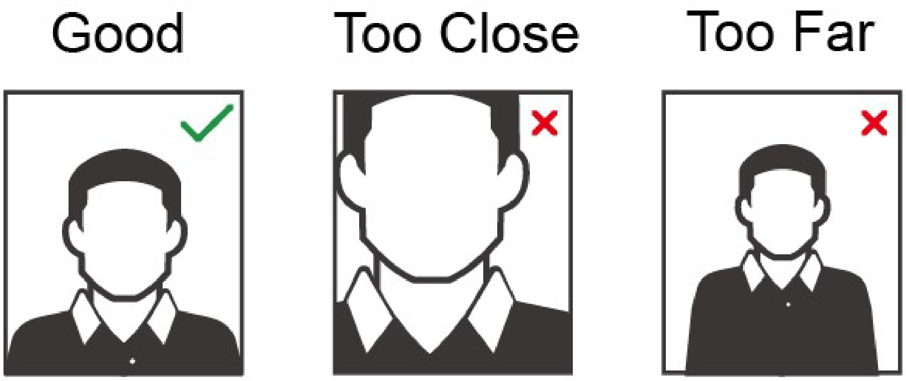
Requirements of Faces

- Make sure that the face is clean and forehead is not covered by hair.
- Do not wear glasses, hats, heavy beards, or other face ornaments that influence face image recording.
- With eyes open, without facial expressions, and make your face toward the center of camera.
- When recording your face or during face recognition, do not keep your face too close to or too far from the camera.

Appendix Figure 1-2 Head position



Appendix Figure 1-3 Face distance



- When importing face images through the management platform, make sure that image resolution is within the range from 150 × 300 pixels to 600 × 1200 pixels. It is recommended that the resolution be greater than 500 × 500 pixels, the image size be less than 100 KB, and the image name and person ID be the same.
- Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area, and the aspect ratio does not exceed 1:2.

Appendix 2 Important Points of Intercom Operation

The Device can function as VTO to realize intercom function.

Prerequisites

The intercom function is configured on the Device and VTO.

Procedure

Step 1 On the standby screen, tap 📞

Step 2 Enter the room No, and then tap .📞

Appendix 3 Important Points of Fingerprint Registration Instructions

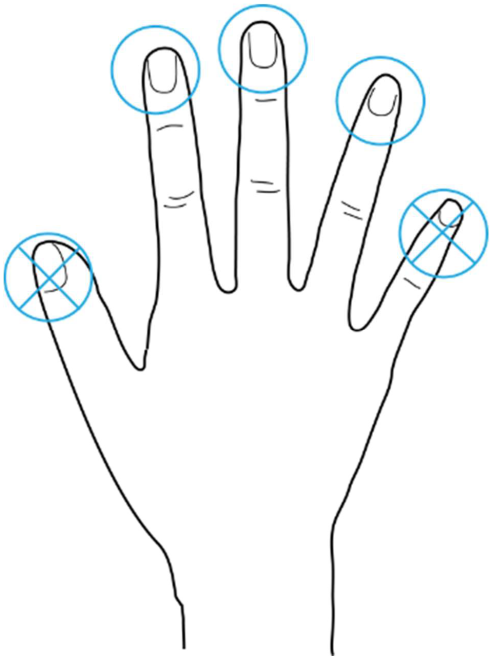
When you register the fingerprint, pay attention to the following points:

- 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

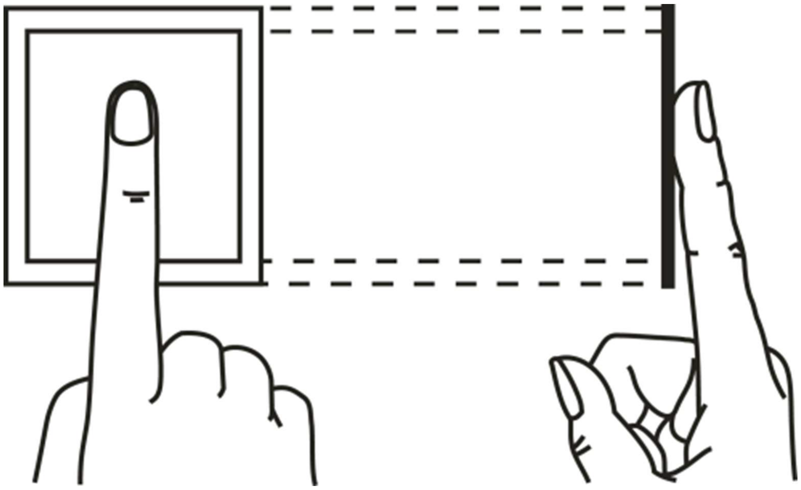
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 3-1 Recommended fingers

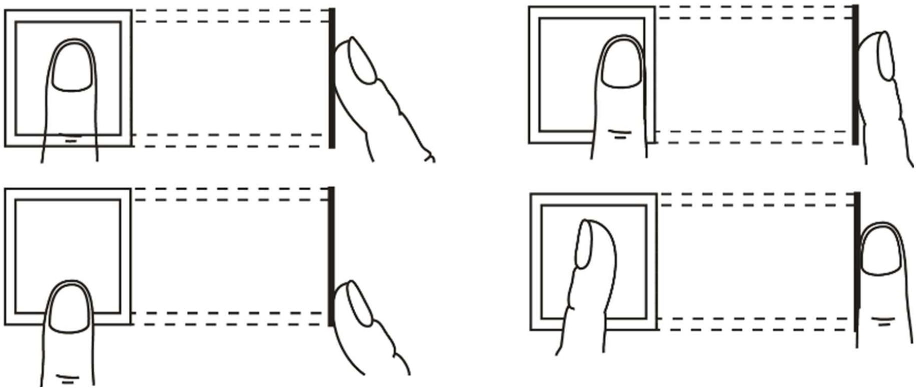


How to Press Your Fingerprint on the Scanner

Appendix Figure 3-2 Correct placement



Appendix Figure 3-3 Wrong placement



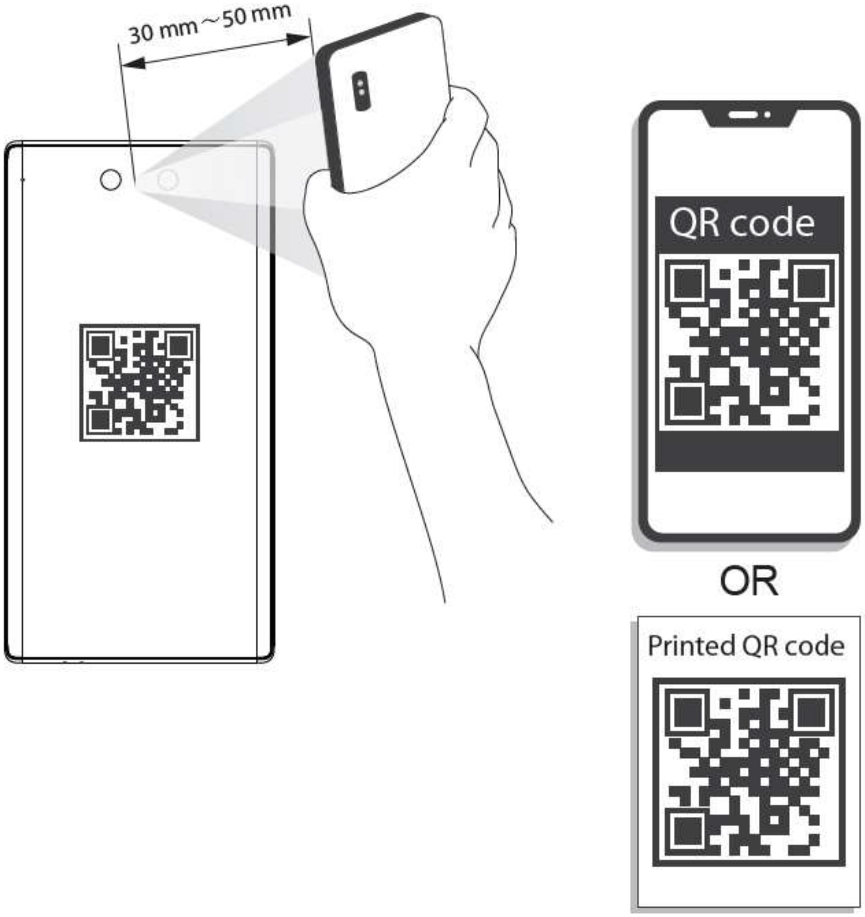
Appendix 4 Important Points of QR Code Scanning

Place the QR code on your phone at a distance of 30 mm–50 mm away from the QR code scanning lens. It supports QR code that is larger than 30 mm × 30 mm and less than 128 bytes in size.

📖

- QR code detection distance differs depending on the bytes and size of QR code.
- Make sure the QR code is aligned with the lens, and avoid direct sunlight.

Appendix Figure 4-1 QR code scanning



Appendix 5 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

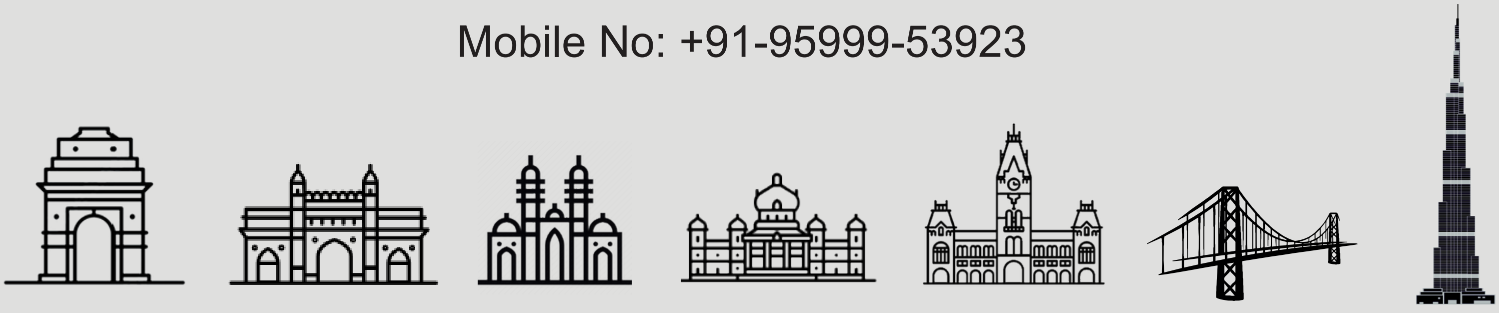
It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

TIMEWATCH®

Presence perfect

Contact Us

D-162, Okhla Industrial Area, Phase-I, Delhi 110020
Email: sales@timewatchindia.com
Phone: +91-11-41916615
Mobile No: +91-95999-53923



www.timewatchindia.com