Face Recognition Access Controller

User's Manual

V1.0

Foreword

General

This manual introduces the functions and 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.

About the Manual

- The manual is for reference only.
- The manual will be updated according to the latest laws and regulations of related jurisdictions.
- 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.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.

FCC Warning

FCC

1. This device complies with Part 15 of the FCC Rules.
   Operation is subject to the following two conditions:
   (1) This device may not cause harmful interference.
   (2) This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. I f this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator &your body.

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.

Installation Requirements

- 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.
- 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.
- 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.

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.
- This equipment is not suitable for use in locations where children are likely to be present.

Table of Contents

1 Overview

1.1 Introduction

The access controller is an access control panel that supports unlock through faces, passwords, fingerprint, cards, QR code, and their combinations. Based on the deep-learning algorithm, it features faster recognition and higher accuracy. It can work with management platform which meets various needs of customers.

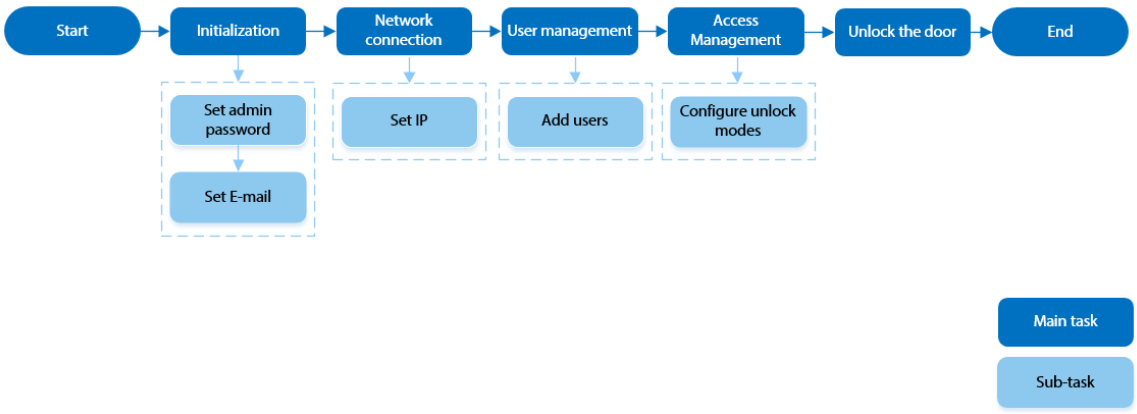
1.2 Features

- 4.3 inch glass touch screen with a resolution of 272 × 480.
- 2-MP wide-angle dual-lens camera with IR illumination and DWDR.
- Multiple unlock methods including face, IC card and password.
- Supports 6,000 users, 6,000 faces, 6,000 passwords, 6,000 fingerprints, 10,000 cards, 50 administrators, and 300,000 records.
- Recognizes faces 0.3 m to 1.5 m away (0.98 ft-4.92 ft); face recognition accuracy rate of 99.9% and the 1:N comparison time is 0.2 s per person.
- Supports improved security and to protect against the device being forcefully opened, security module expansion is supported.
- TCP/IP and Wi-Fi connection.
- PoE power supply.
- IP65.

2 Local Operations

2.1 Basic Configuration Procedure

Basic configuration procedure



2.2 Standby Screen

You can unlock the door through faces, passwords, and IC CARD.

If there is no operation in 30 seconds, the Access Controller will go to the standby mode.

This manual is for reference only. Slight differences might be found between the standby screen in this manual and the actual device.

2.3 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 the web-page.

NOTE: 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 ' " ; : &).

2.4 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 has no door access permission.
- Administration 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.
- 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.

2.5 User Management

You can add new users, view user/admin list and edit user information.

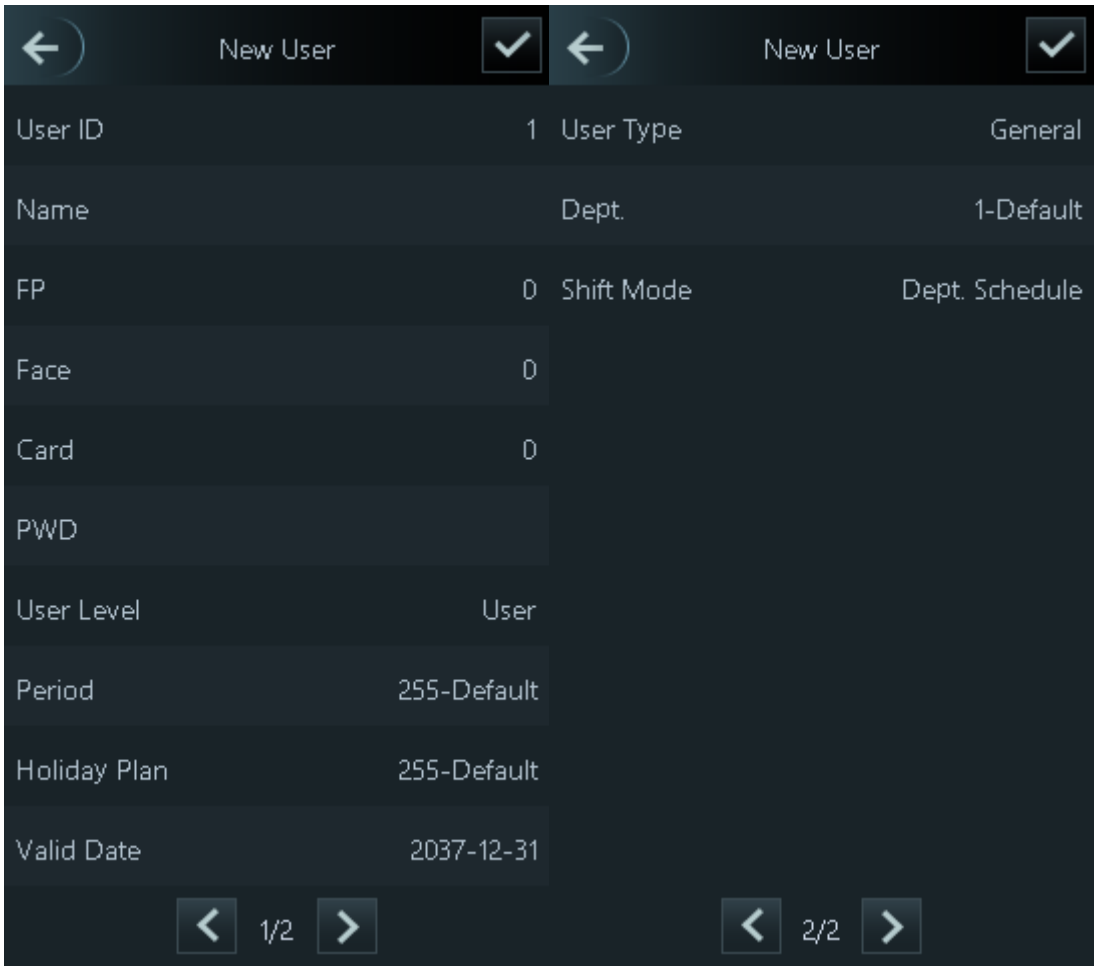
2.5.1 Adding New Users

Procedure

Step 1 On the **Main Menu**, select **User** > **New User**.

Step 2 Configure the parameters on the interface.

Add new user



Parameters description

Parameter	Description
User ID	Enter user IDs. The IDs can be numbers, letters, and their combinations, and the maximum length of the ID is 32 characters. Each ID is unique.
Name	Enter name with at most 32 characters (including numbers, symbols, and letters).
Face	Make sure that your face is centered on the image capturing frame, and an image of the face will be captured and analyzed automatically.
Card	A user can register five 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.
PWD	Enter the user password. The maximum length of the password is 8 digits.

Parameter	Description
User Level	You can select a user level for new users. ● **User**: Users only have door access permission. ● **Admin**: Administrators can unlock the door and configure the access controller.
Period	People can unlock the door only during the defined period.
Holiday Plan	People can unlock the door only during the defined holiday plan.
Valid Date	Set a date on which the access permissions of the person will be expired.
User Type	● **General**: General users can unlock the door. ● **Blocklist**: When users in the blocklist unlock the door, service personnel will receive a notification. ● **Guest**: 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**: Patrol users will have their attendance tracked, but they have no unlocking permissions. ● **VIP**: When VIP unlock the door, service personnel will receive a notice. ● **Others**: When they unlock the door, the door will stay unlocked for 5 more seconds. ● Custom User 1/Custom User 2: Same with general users.
Dept.	Set departments.
Shift Mode	Select shift modes.

Step 3 Tap .

2.5.2 Viewing User Information

You can view user/admin list and edit user information.

Procedure

Step 1 On the **Main Menu**, select **User** > **User List**, or select **User** > **Admin List**.

Step 2 View all added users and admin accounts.

- : Unlock through password.
- Unlock through swiping card.
- : Unlock through face recognition.

Related Operations

On the **User** screen, you can manage the added users.

- Search for users: Tap and then enter the username.
- Edit users: Tap the user to edit user information.
- Delete users
  - ◇ Delete individually: Select a user, and then tap .

- Delete in batches:
  - On the **User List** screen, tap to delete all users.
  - On the **Admin List** screen, tap to delete all admin users.

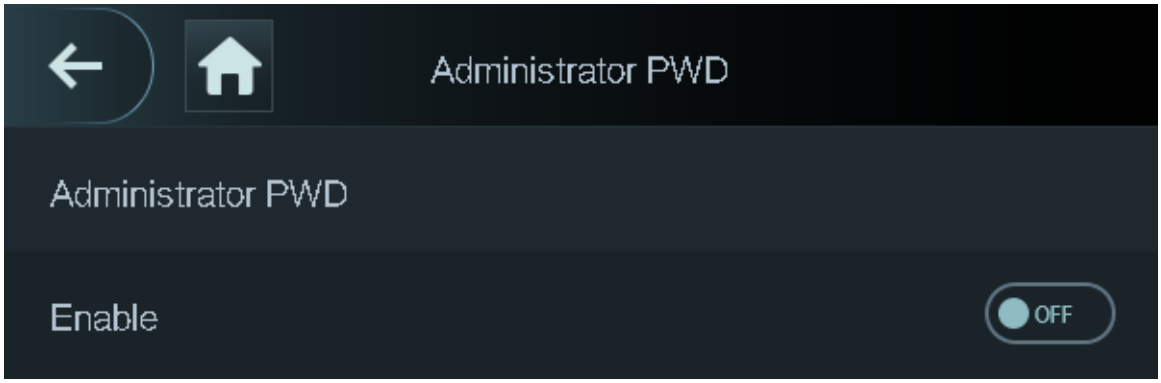
2.5.3 Configuring Administrator Password

You can unlock the door by only entering the admin password. Admin password is not limited by user types. Only one admin password is allowed for one device.

Procedure

Step 1 On the **Main Menu** screen, select **User** > **Administrator PWD**.

Set admin password



Step 2 Tap **Administrator PWD**, and then enter the administrator password.

Step 3 Tap .

Step 4 Turn on the administrator function.

2.6 Network Communication

Configure the network, serial port and Wiegand port to connect the Access Controller to the network.

2.6.1 Configuring IP

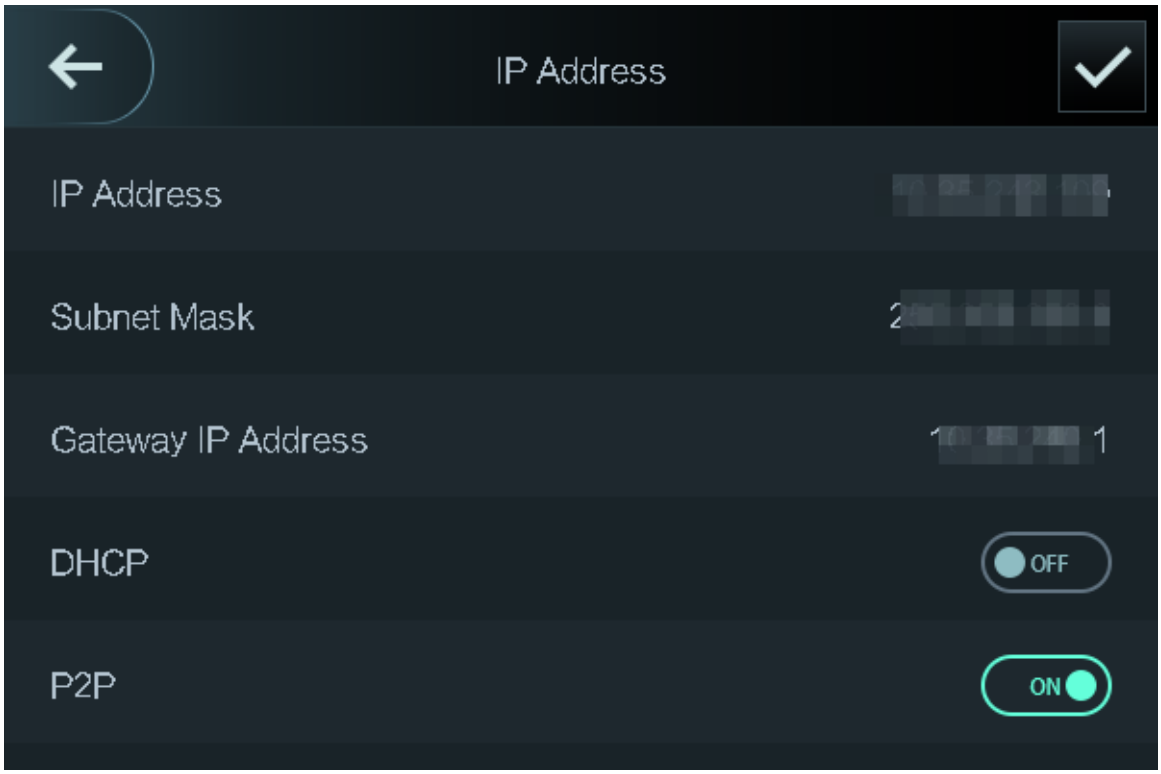
Set IP address for the Access Controller to connect it to the network. After that, you can log in to the webpage and the management platform to manage the Access Controller.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Network** > **IP Address**.

Step 2 Configure IP Address.

IP address configuration



IP configuration parameters

Parameter	Description
IP Address/Subnet Mask/Gateway Address	The IP address, subnet mask, and gateway IP address must be on the same network segment.
DHCP	It stands for Dynamic Host Configuration Protocol. When DHCP is turned on, the Access Controller will automatically be assigned with IP address, subnet mask, and gateway.
P2P	P2P (peer-to-peer) technology enables users to manage devices without applying for DDNS, setting port mapping or deploying transit server.

2.6.2 Configuring Wi-Fi

You can connect the Access Controller to the network through Wi-Fi network.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Network** > **WiFi**.

Step 2 Turn on Wi-Fi.

Step 3 Tap to search available wireless networks.

Step 4 Select a wireless network and enter the password.

If no Wi-Fi is searched, tap **SSID** to enter the name of Wi-Fi.

Step 5 Tap .

2.6.3 Configuring Serial Port

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Serial Port**.

Step 2 Select a port type.

- Select **Reader** when the Access Controller connects to a card reader.
- Select **Controller** when the Access Controller functions as a card reader, and the Access Controller will send data to the Access Controller to control access.
  Output Data type:
  - ◇ Card: Outputs data based on card number when users swipe card to unlock door; outputs data based on user's first card number when they use other unlock methods.
  - ◇ No.: Outputs data based on the user ID.
- Select **Reader (OSDP)** when the Access Controller is connected to a card reader based on OSDP protocol.
- Security Module: When a security module is connected, the exit button, lock will be not effective.

2.6.4 Configuring Wiegand

The access controller allows for both Wiegand input and output mode.

Procedure

Step 1 On the **Main Menu**, select **Connection** > **Wiegand**.

Step 2 Select a Wiegand.

- Select **Wiegand Input** when you connect an external card reader to the Access Controller.
- Select **Wiegand Output** when the Access Controller functions as a card reader, and you need to connect it to a controller or another access terminal.

Wiegand output

Description of Wiegand output

Parameter	Description
Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. ● **Wiegand26**: Reads three bytes or six digits. ● **Wiegand34**: Reads four bytes or eight digits. ● **Wiegand66**: Reads eight bytes or sixteen digits.
Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
Pulse Interval	
Output Data Type	Select the type of output data. ● **User ID**: Outputs data based on user ID. ● **Card No.**: Outputs data based on user's first card number, and the data format is hexadecimal or decimal.

2.7 Access Management

You can configure door access parameters, such as unlocking modes, alarm linkage, door schedules.

2.7.1 Configuring Unlock Combinations

Use card, face or password or their combinations to unlock the door.

Background Information

Unlock modes might differ depending on the actual product.

Procedure

Step 1 Select **Access** > **Unlock Mode** > **Unlock Mode**.

Step 2 Select unlocking methods.

Step 3 Tap +**And** or **/Or** to configure combinations.

- **+And**: Verify all the selected unlocking methods to open the door.
- **/Or**: Verify one of the selected unlocking methods to open the door.

Step 4 Tap ☑ to save changes.

2.7.2 Configuring Alarm

An alarm will be triggered when abnormal access events occur.

Procedure

Step 1 Select **Access** > **Alarm**.

Step 2 Enable the alarm type.

Description of alarm parameters

Parameter	Description
Anti-passback	Users need to verify their identities both for entry and exit; otherwise an alarm will be triggered. It helps prevents a card holder from passing an access card back to another person so they gain entry. When anti-passback is enabled, the card holder must leave the secured area through an exit reader before system will grant another entry. ● If a person enters after authorization and exits without authorization, an alarm will be triggered when they attempt to enter again, and access is denied at the same time. ● If a person enters without authorization and exits after authorization, an alarm will be triggered when the they attempt to enter again, and access is denied at the same time.
Duress	An alarm will be triggered when a duress card, duress password or duress fingerprint is used to unlock the door.
Intrusion	When door sensor is enabled, an intrusion alarm will be triggered if the door is opened abnormally.
Door Sensor Timeout	A timeout alarm will be triggered if the door remains unlocked longer than the defined door sensor timeout, which ranges from 1 to 9999 seconds.
Door Sensor On	Intrusion and timeout alarms can be triggered only after door sensor is enabled.

2.7.3 Configuring Door Status

Procedure

Step 1 On the **Main Menu** screen, select **Access** > **Door Status**.

Step 2 Set door status.

- **NO**: The door remains unlocked all the time.
- **NC**: The door remains locked all the time.
- **Normal**: If **Normal** is selected, the door will be unlocked and locked according to your settings.

2.7.4 Configuring Lock Holding Time

After a person is granted access, the door will remain unlocked for a defined time for them to pass through.

Procedure

Step 1 On the **Main Menu**, select **Access** > **Lock Holding Time.**

Step 2 Enter the unlock duration.

Step 3 Tap ✓ to save changes.

individuals or departments, and then employees must follow the established work schedules.

Procedure

Step 1 Select **Attendance** > **Schedule**.

Step 2 Set works schedules for individuals.

1. Tap **Personal Schedule**
2. enter the user ID, and then tap ☑.
3. On the calendar, select the date, and then configure shifts.
   You can only set work schedules for the current month and the next month.
   - 0 indicates break.
   - 1 to 24 indicates the number of the pre-defined shifts.
   - 25 indicates the business trip.
   - 26 indicates the leave of absence.
4. Tap ☑.

Step 3 Set works schedules for the department.

1. Tap **Dept Schedule**.
2. Tap a department, set shifts for a week.

- 0 indicates break.
- 1 to 24 indicates the number of the pre-defined shifts.
- 25 indicates the business trip.
- 26 indicates the leave of absence.

Department shifts

The defined work schedule is in one-week cycle and will be applied to all employees in the department.

Step 4 Tap ☑.

2.7.5 Configuring Verification Interval Time

the employee repeats punch-in/out within a set time, the earliest punch-in/out will be recorded.

Procedure

Step 1 Select **Attendance** > **Schedule** > **Verification Interval Time(s)**.

Step 2 enter the time interval, and then tap ✓.

2.8 System

2.8.1 Configuring Time

Configure system time, such as date, time, and NTP.

Procedure

Step 1 On the **Main Menu**, select **System** > **Time**.

Step 2 Configure system time.

Description of time parameters

Parameter	Description
24-hour System	The time is displayed in 24-hour format.
Date Setting	Set up the date.
Time	Set up the time.
Date Format	Select a date format.

Parameter	Description
DST Setting	1. Tap **DST Setting** 2. Enable DST. 3. Select **Date** or **Week** from the **DST** Type list. 4. Enter start time and end time. 5. tap ✓.
NTP Check	A network time protocol (NTP) server is a machine dedicated as the time sync server for all client computers. If your computer is set to sync with a time server on the network, your clock will show the same time as the server. When the administrator changes the time (for daylight savings), all client machines on the network will also update. 1. Tap **NTP Check**. 2. Turn on the NTP check function and configure parameters. ● **Server IP Address**: Enter the IP address of the NTP server, and the Access Controller will automatically sync time with NTP server. ● **Port**: Enter the port of the NTP server. ● **Interval (min)**: Enter the time synchronization interval.
Time Zone	Select the time zone.

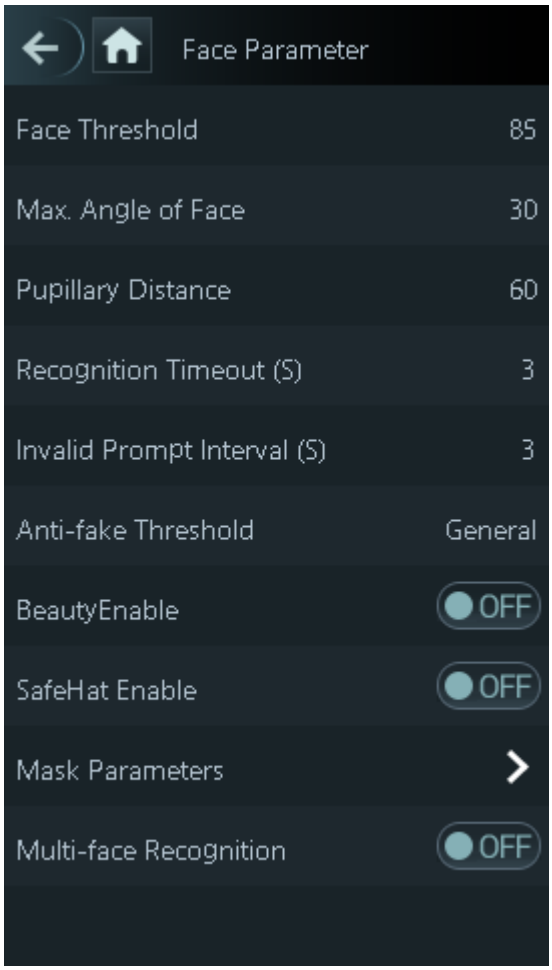
2.8.2 Configuring Face Parameters

Procedure

Step 1 On the main menu, select **System** > **Face Parameter**.

Step 2 Configure the face parameters, and then tap ✓.

Face parameter



Description of face parameters

Name	Description
Face Threshold	Adjust the face recognition accuracy. Higher threshold means higher accuracy.
Max. Angle of Face	Set the maximum face pose angle for face detection. Larger value means larger face angle range. If the face pose angle is out of the defined range, the face detection box will not appear.
Pupillary Distance	Face images require desired pixels between the eyes (called pupillary distance) for successful recognition. The default pixel is 45. The pixel changes according to the face size and the distance between faces and the lens. If an adult is 1.5 meters away from the lens, the pupillary distance can be 50 px-70 px.
Recognition Timeout (S)	If a person with access permission has their face successfully recognized, the Access Controller will prompt face recognition success. You can enter the prompt interval time.
Invalid Face Prompt Interval (S)	If a person without access permission attempts to unlock the door for several times in the defined interval, the Access Controller will prompt face recognition failure. You can enter the prompt interval time.

Name	Description
Anti-fake Threshold	Avoid false face recognition by using a photo, video, mask or a different substitute for an authorized person's face. ● Close: Turns off this function. ● General: Normal level of anti-spoofing detection means higher door access rate for people with face masks. ● High: Higher level of anti-spoofing detection means higher accuracy and security. ● Extremely High: Extremely high level of anti-spoofing detection means extremely high accuracy and security.
BeautyEnable	Beautify captured face images.
SafeHat Enable	Detects safehats.
Mask Parameters	● Mask mode: ◇ **No detect**: Mask is not detected during face recognition. ◇ **Mask reminder**: Mask is detected during face recognition. If the person is not wearing a mask, the system will remind them to wear masks, and access is allowed. ◇ **Mask intercept**: Mask is detected during face recognition. If a person is not wearing a mask, the system will remind them to wear masks, and access is denied. ● Mask Recognition Threshold: Higher threshold means higher mask detection accuracy.
Multi-face Recognition	Supports detecting 4 face images at the same time, and the unlock combinations mode become invalid. The door is unlocked after any one of them gain access.

2.8.3 Setting Volume

You can adjust the volume of the speaker and microphone.

Procedure

Step 1 On the **Main Menu**, select **System** > **Volume**.

Step 2 Select **Beep Volume** or **Mic Volume**, and then tap + or − to adjust the volume.

2.8.4 (Optional) Configuring Fingerprint Parameters

Configure fingerprint detection accuracy. Higher value means that higher threshold of similarity and higher accuracy. This function is only available on Access Controller that supports fingerprint unlock.

Procedure

Step 1 On the **Main Menu**, select **System** > **FP Parameter**.

Step 2 Tap + or − to adjust the value.

2.8.5 Screen Settings

Configure screen off time and logout time.

Procedure

Step 1 On the **Main Menu**, select **System** > **Screen settings**.

Step 2 Tap **Logout Time** or **Screen Off Timeout**, and then tap + or − to adjust the time.

2.8.6 Restoring Factory Defaults

Procedure

Step 1 On the **Main Menu**, select **System** > **Restore Factory**.

Step 2 Restore factory defaults if necessary.

- **Restore Factory**: Resets all configurations and data.
- **Restore Factory (Save user & log)**: Resets configurations except for user information and logs.

2.8.7 Restart the Device

On the **Main Menu**, select **System** > **Reboot**, and the Access Controller will be restarted.

2.8.8 Configuring the Language

Change the language on the Access Controller. On the **Main Menu**, select **System** > **Language**, select the language for the Access Controller.

2.9 USB Management

You can use a USB to update the Access Controller, and export or import user information through USB.

- Make sure that a USB is inserted to the Access Controller before you export data or update the system. To avoid failure, do not pull out the USB or perform any operation of the Access Controller during the process.
- You have to use a USB to export the information from an Access Controller to other devices. Face images are not allowed to be imported through USB.

2.9.1 Exporting to USB

You can export data from the Access Controller to a USB. The exported data is encrypted and cannot be edited.

Procedure

Step 1 On the **Main Menu**, select **USB** > **USB Export**.

Step 2 Select the data type you want to export, and then tap **OK**.

2.9.2 Importing From USB

You can import data from USB to the Access Controller.

Procedure

Step 1 On the **Main Menu**, select **USB** > **USB Import**.

Step 2 Select the data type that you want to export, and then tap **OK**.

2.9.3 Updating System

Use a USB to update the system of the Access Controller.

Procedure

Step 1 Rename the update file to "update.bin", put it in the root directory of the USB, and then insert the USB to the Access Controller.

Step 2 On the **Main Menu**, select **USB** > **USB Update**.

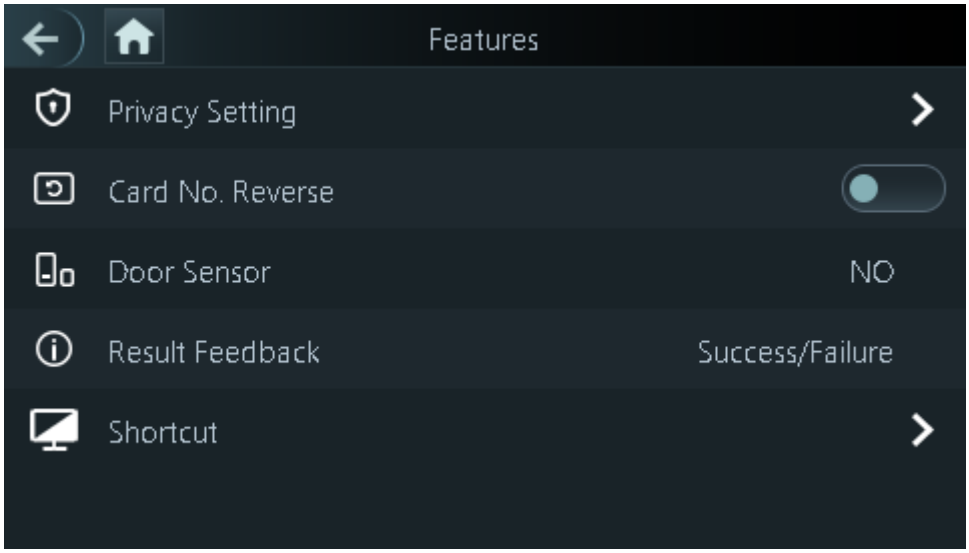
Step 3 Tap **OK**.

The Access Controller will restart when the updating completes.

2.10 Configuring Features

On the **Main Menu** screen, select **Features**.

Features



Description of features

Parameter	Description
Private Setting	• PWD Reset Enable: You can enable this function to reset password. The PWD Reset function is enabled by default. • HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication over a computer network. When HTTPS is enabled, HTTPS will be used to access CGI commands; otherwise HTTP will be used. When HTTPS is enabled, the access controller will restart automatically. • CGI: Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. The CG I is enabled by default. • SSH: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. • Capture Photos: Face images will be captured automatically when people unlock the door. The function is enabled by default. • Clear Captured Photos: Delete all automatically captured photos.
Card No. Reverse	When the Access Controller connects to a third-party device through Wiegand input, and the card number read by the Access Terminal is in the reserve order from the actual card number, you need to turn on the **Card No. Reverse** function.
Door Sensor	NC: When the door opens, the circuit of the door sensor circuit is closed. NO: When the door opens, the circuit of the door sensor circuit is open. Intrusion and overtime alarms are triggered only after door detector is turned on.
Result Feedback	• Success/Failure: Only displays success or failure on the standby screen. • Only Name: Displays user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. • Photo&Name: Displays user's registered face image, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied. • Photos&Name: Displays the captured face image and a registered face image of a user, user ID, name and authorization time after access granted; displays not authorized message and authorization time after access denied.

Parameter	Description
Shortcut	Select identity verification methods on the standby screen. ● Password: The icon of the password unlock method is displayed on the standby screen.

2.11 Unlocking the Door

You can unlock the door through faces, passwords, fingerprint, cards, and more.

2.11.1 Unlocking by Cards

Place the card at the swiping area to unlock the door.

2.11.2 Unlocking by Face

Verify the identity of an individual by detecting their faces. Make sure that the face is centered on the face detection frame.

2.11.3 Unlocking by User Password

Enter the user ID and password to unlock the door.

Procedure

Step 1 Tap on the standby screen.

Step 2 tap **PWD Unlock**, and then enter the user ID and password.

Step 3 Tap **Yes**.

2.11.4 Unlocking by Administrator Password

Enter only the administrator password to unlock the door. The access controller only allows for one administrator password. Using administrator password to unlock the door without being subject to user levels, unlock modes, periods, holiday plans, and anti-passback except for normally closed door. One device allows for only one admin password.

Prerequisites

The administrator password was configured. For details, see: Configuring Administrator Passwor.

Procedure

Step 1 Tap on the standby screen.

Step 2 Tap **Admin PWD**, and then enter the admin password.

Step 3 Tap .

2.12 System Information

You can view data capacity and device version.

2.12.1 Viewing Data Capacity

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view storage capacity of each data type.

2.12.2 Viewing Device Version

On the **Main Menu**, select **System Info** > **Data Capacity**, you can view the device version, such as serial No., software version and more.