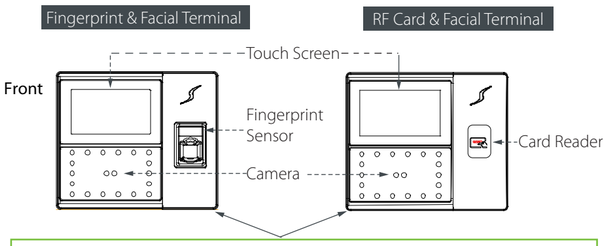
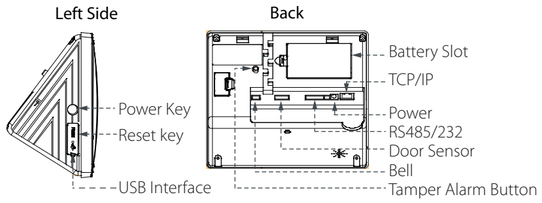
1. Overview



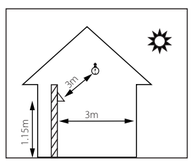


Tamper Alarm Button: Once the tamper alarm button is released, the system make will a warning sound and the ⚠ will be displayed in the status bar of the initial interface. There will be no alarm signal while the button is pressed.

NOTE: Not all products have the function with ★, the real product shall prevail.

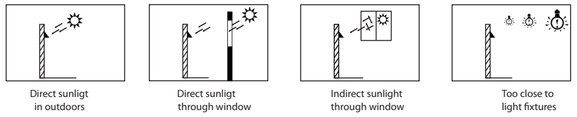
2. Installation Environment

1) Recommended Installation Location

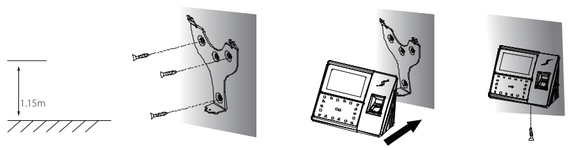


Install the device indoors at least 10 feet (3m) away from windows, and 6.5 feet (2m) from light fixtures.
It is not recommended to install it near windows or outdoors.

2) Locations Unrecommended



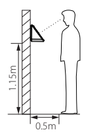
3. Installation Steps



1) Put the mounting template sticker onto the wall, and drill holes according to the mounting paper.
2) Fix the back plate onto the wall using wall mounting screws.
3) Insert the device into back plate.
4) Use security screw to fasten the device to back plate.

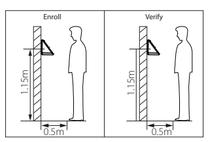
4. Cautions on Using Face Recognition Device

1) Recommended Standing Position



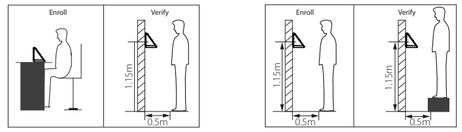
For user heights between 1.5m to 1.8m, it is recommended to install the device at 1.15m above ground (may be modified according to user average height).

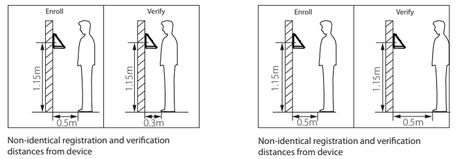
a. Recommended Registration and Verification Position



Recommended Procedures (as shown in the left image):
During registration and verification procedures, the position of device should not be changed to prevent reduction in verification preciseness. If it is necessary to move the device, its vertical height should not be changed.

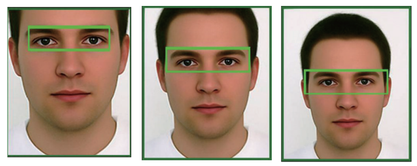
b. Factors Affecting the Preciseness of Verification





2) Registration

a. During registration, it is required to adjust your upper body to fit your eyes into the green frame on the screen.



b. During verification, it is required to show your face in the center of the screen and fit your face into the green frame in the screen.

5. Quick Flows

Enroll Administrator and Users → Communication Settings → Punch/Verify → View Records

1) Enroll Administrator and Users

a. Enroll Administrator (Main Menu→ User Management→New User)

User ID: Enroll user ID; it supports 1-9 digits of numbers.
Name: Enroll name; it supports 1-12 digits of any characters.
Use Role: Select the user role between Normal User and Super Admin.
Fingerprint ★: Enroll a fingerprint or fingerprints.
Face: Enroll a face according to the prompts of screen and voice.
Badge Number★: Enroll a badge by swiping a badge.
Password: Enroll the password; it supports 1-9 digits of numbers.
User Photo: Enroll the user photo which will be displayed after verification .
Access Control Role: Set the Access Conrtol parameters of a user.

Access Control Setting (Main Menu→Access Control):

Access Control Options: Including Door Lock Delay, Door Sensor Delay, Door Sensor Type, Door Alarm Delay, Retry Times to Alarm, NC / NO Time Period etc.
Time Schedule: Schedule Doors' opening time, 50 time zones are available to define.
Holidays: Set special time zones for holidays.
Access Groups: Set to manage employees in groups.
Combined Verification: Set various groups into a combined access group to achieve multi-verification.
Duress Options: Set duress function options.

b. Enroll Normal Users (same steps with enrolling adminnistrator except the "User Role" option.)

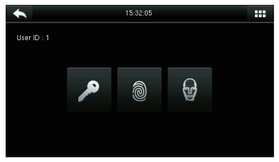
2) Communication Settings (Main Menu→Communication)

Ethernet: The device can communicate with PC via the Enthernet parameters.
Serial Comm: The device can communicate with PC via the serial port according to the parameters you set.
PC Connection: Set the password and device ID so that you can connect the device with software in PC.
Cellular Data Network★: When the device is applied on a dial-up network, ensure that the device is within the coverage of the mobile network signals (GPRS/3G).
ADMS Setting★: Settings used for connecting with ADMS server.
Wi-Fi Setting★: The device provides a Wi-Fi module, which can be built in the device mould or externally connected, to enable data transmission via Wi-Fi and establish a wireless network environment.
Wiegand Setup: Set wiegand-out parameters.

3) Verification (1:1 verification mode for example)

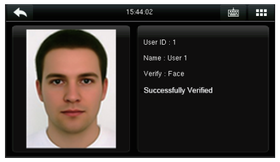
Click 1:1 to enter 1:1 verification mode on initial interface.

Enter User ID and press [OK].

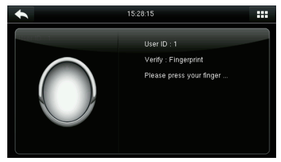


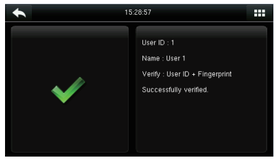
When multi-verification mode is registered, please choose the verify mode as the figure above: password, fingerprint and face.

a. Face Verification Mode

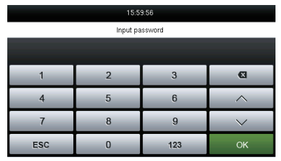


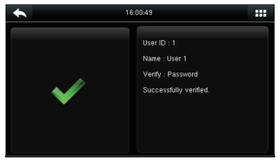
b. Fingerprint Verification Mode





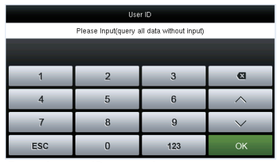
c. Password Verification Mode



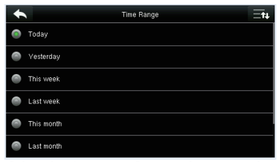


4) Viewing Attendance Records

a. View records in the device (Main Menu→Attendance Search→Attendance Records)



Enter the user ID to search.



Select the time range for attendance record query.

Tap the record in green to view its details.

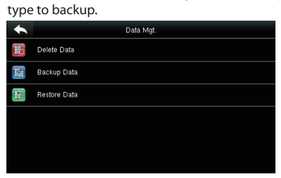
The above figure shows the details of this record.

b. View records on computer (Main Menu→USB Manager→Download→Attendance Data)

Insert the usb disk correctly, download the attendance data to the disk, then upload that from the disk to your computer. The downloaded data is named "Device Serial Number.dat", you can open and view it.

6. Backup Data

To avoid deleting data by misoperation, you can backup data to local or usb disk at any time.
Enter Main Menu→Data Management→Backup Data, select the saving type and data type to backup.



Select the content to be backed up.

7. Other Settings

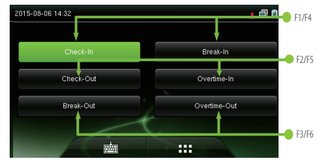
a. Date Time (Main Menu→System→Date Time)

Set the date, time and time format for the device.

b. Shortcut Key Mappings (Main Menu→Personalize→Shortcut Key Mappings)

Shortcut keys can be defined as punch state keys or menu function key. When the device is on the main interface, pressing the set shortcut key will display the attendance state or enter the menu operation interface.

Tap the shortcut key to be set



Tap the main interface to show the shortcut menu.

8. Troubleshootings

1. The face cannot be recognized by the device in verification.
Solutions
a. Check if your facial expression, standing posture and distance during verification are the same with that in enrollment.
b. Check if the device is under direct sunlight or near the windows.

2. Verification fails as user wears glasses during verification but not in face enrollment.
Solution
You can enroll your face wearing glasses in the first or second time of face capturing, since the device supports 3 times of capturing face templates.

3. The device makes a misjudgment in verification.

Solution
There is a certain probability of misjudgment. You can re-enroll your face.

Quick Start Guide

4.3-inch Touch Screen & Facial Attendance Terminal

Version: 1. 0