



Security at Fingertips

User Manual

2.4" TFT AC Terminal
Installation Guide & Quick Start Guide

Contents

Safety Precautions	----->	1
1. Packing List	----->	2
2. Overview of the Operation Panel	----->	3
3. System Structure	----->	4
4. The Installation of Device	----->	5
5. Quick Start Guide	----->	10
6. Others	----->	19

Safety Precautions

Thank you for using our products. Please read this manual carefully before using this product for a comprehensive understanding so as to avoid causing unnecessary damages to the product.

○ Important Notes

- Do not place the device under strong light.
- Use regulated **12V DC** power source (separately purchased and recommend using Uninterrupted Power Supply with backup battery option considering of power failure).
- Do not place the device in a vulnerable location where it might be subjected to vandalism.

○ Before Installation

1. Prior to beginning installation, cut off all power to prevent personal injury and damage to the device and peripheral equipment.
2. Connect the ground wire first, in order to prevent electro-static damage to the device.
3. Connect **12V DC** power supply to the device at last. If the device does not operate properly, always cut off power to it before examining/dismantling. Be advised that wiring the device while power is on may cause damage to the terminal. Possible resulting damage from not powering off the device prior to wiring is not covered by manufacturer's warranty.
4. Mount the device at a comfortable height, typically between **1.4~1.5** meter from the ground.
5. After installation, remove protective film from the device display and fingerprint sensor.
6. To prevent being accidentally locked out while testing the exit button, keep a person on the inside of the door.
7. Run the auto-test function to confirm that installation is successful.
8. In order to maximize the life of the device, use the auto-sleep functions, sleep time could be set in the system parameter menu.
9. The rated voltage of the device is **DC 12V**, and the rated current is **300mA**. If the incorrect voltage is used, the device may be damaged or may not operate the electric door lock (if attached).
10. Improper wiring may cause the device's main circuit board and fingerprint sensor to burn out. Resulting damage from improper wiring is not covered under manufacturer's warranty.

11. Only use supplied transformer and cord. Do not attempt extending the cord by cutting and splicing.
12. If using RS485 mode of communication with PC, use specialized RS485 cables and powered RS232/485 converter. If the RS485 cable length exceeds **100** meters, we recommend using a 120 Ω terminator.
13. Refer to the user handbook and operating instructions for further information.

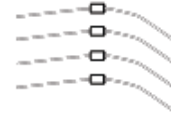
1. Packing List



Access Device



1 Screwdriver



4 Diodes (FR107)



1 Star Screw

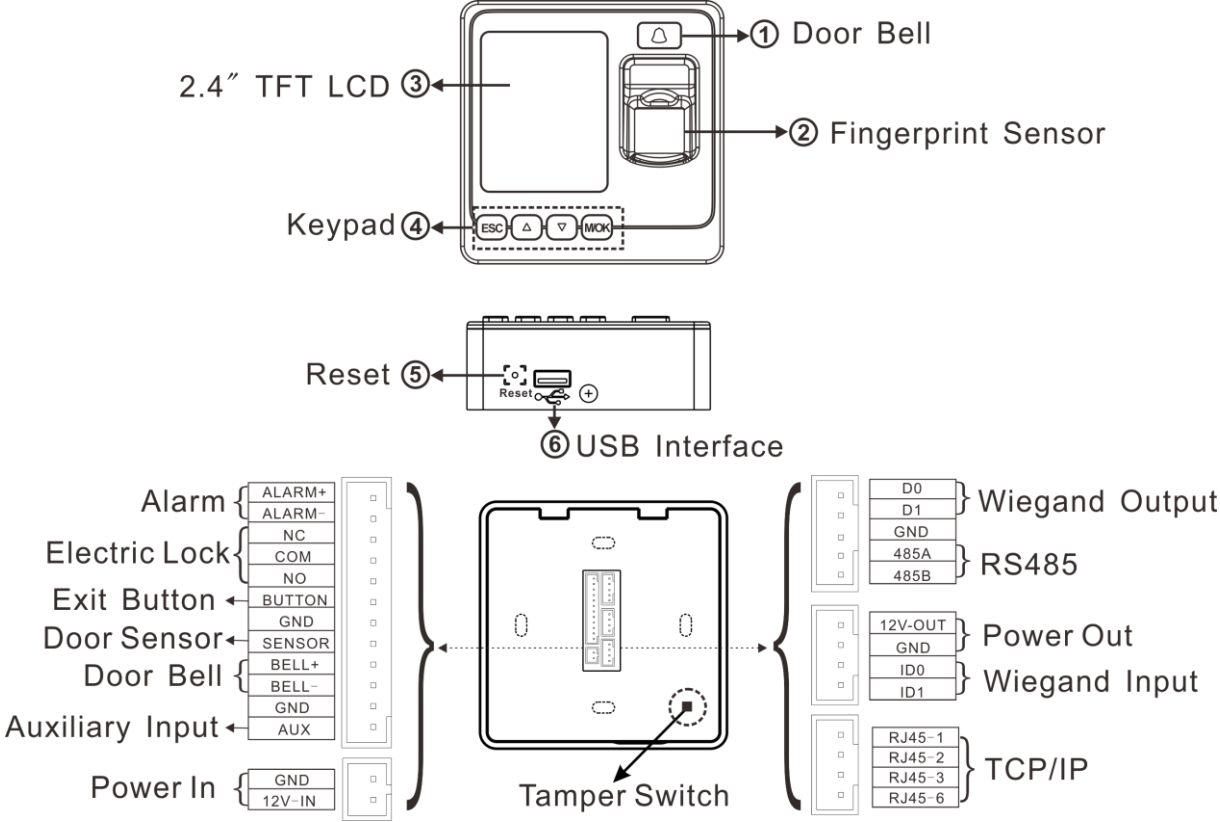


4 Screws & Wall Plugs



CD

2. Overview of the Operation Panel

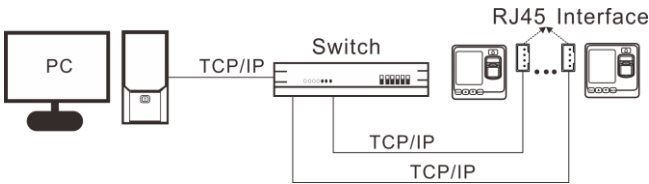


3. System Structure

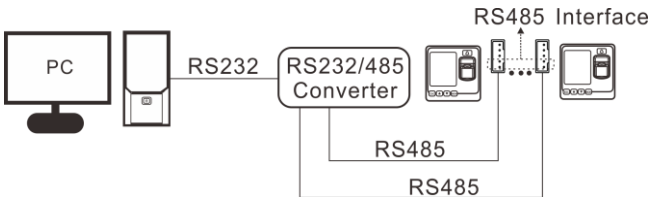
Directly connect with PC through TCP/IP



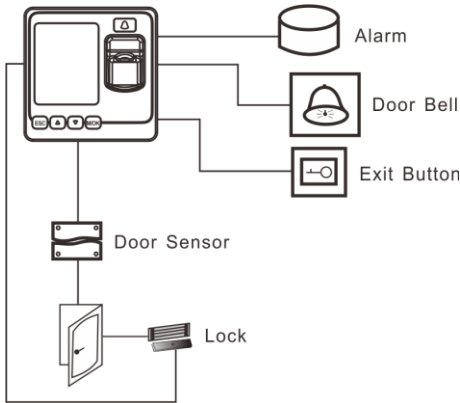
Connect with PC through TCP/IP network



Connect with PC through RS485 network

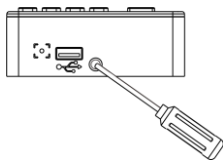


The diagram of system construction

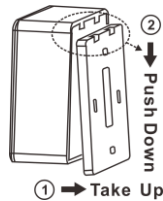


4. The Installation of Device

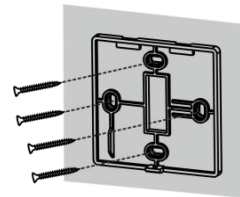
i . Install Device



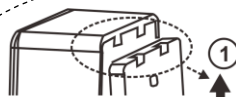
1. Remove the screw on the bottom of device.



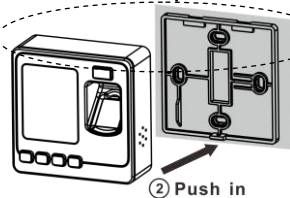
2. Take out the *Back Cover*.



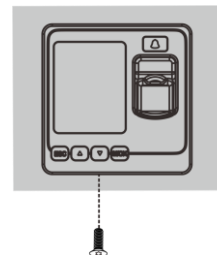
3. Fix the *Back Cover* on the wall with provided screws.



Insert



4. Fix the device on the *Back Cover*.



5. Fixing the screw.

ii. Connect with peripheral equipment

 **Caution:** Please make sure the power is cut off before wiring; otherwise it is possible to damage the device badly.

● Door Sensor Connection

● Exit Button Connection

● Alarm Connection

● Door Bell Connection

● Lock Connection

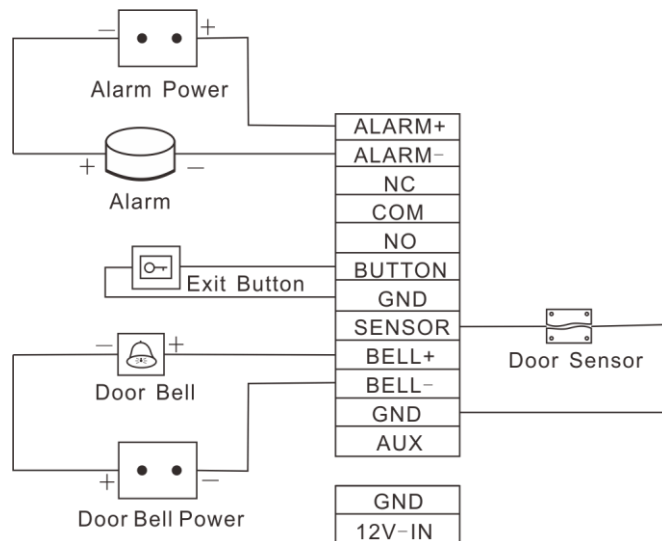
Selecting door lock: The choice of lock depends firstly on the door-electric strikes or bolts, magnetic locks, turnstiles or barriers are all options depending firstly on the architecture and secondly on the required resistance to attach. Please consult your supplier for more info.

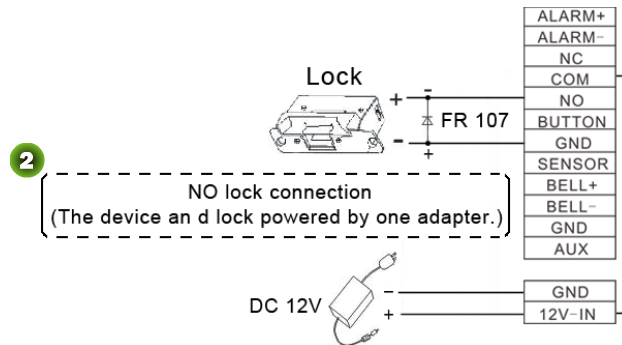
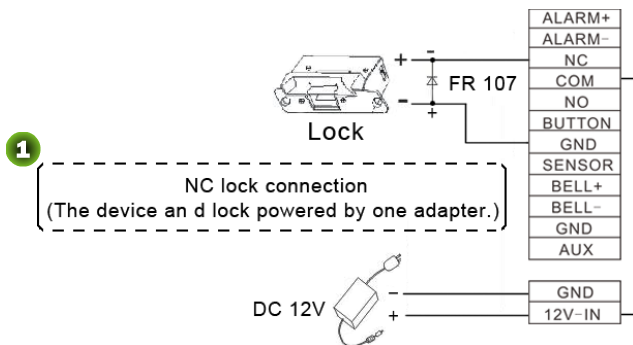
Connect with electric lock: After the user verified the identity, the device will output the unlock signal. The device supports NO (Normally Open) LOCK and NC (Normally Close) LOCK.

NO LOCK: the door is normally open at power on, so it closes the door at power off.

NC LOCK: the door is normally closed at power on, so it opens the door at power off.

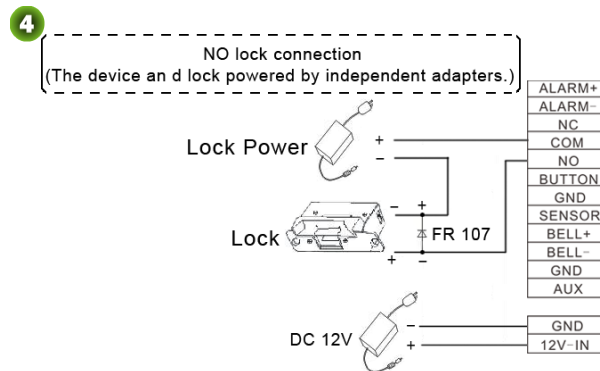
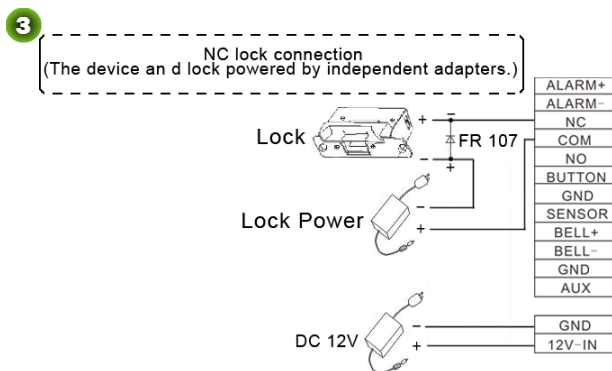
The device can supply power directly to a door lock, please refer to **Figure 1, 2**. (Ensure that proper voltages are applied to the lock terminals and check on the current ratings of the locks.)





However, in the following three scenarios, it is recommended that the door lock has an independent power source, and is NOT powered by the device; shown as **Figure 3, 4**.

- If the door lock voltage is not **12V DC** then provides separate power to the door lock.
- If the door lock runs on **12V DC**, but requires more than **1A** (amp), then provide separate power to the door lock.
- If the distance between the device and door lock is greater than **15** feet, then provide separate power to the door lock.



- **RS485 Connection**

RS-485 systems using a bus structure configuration connect the driver to the receiver. As shown as **Figure 5**.

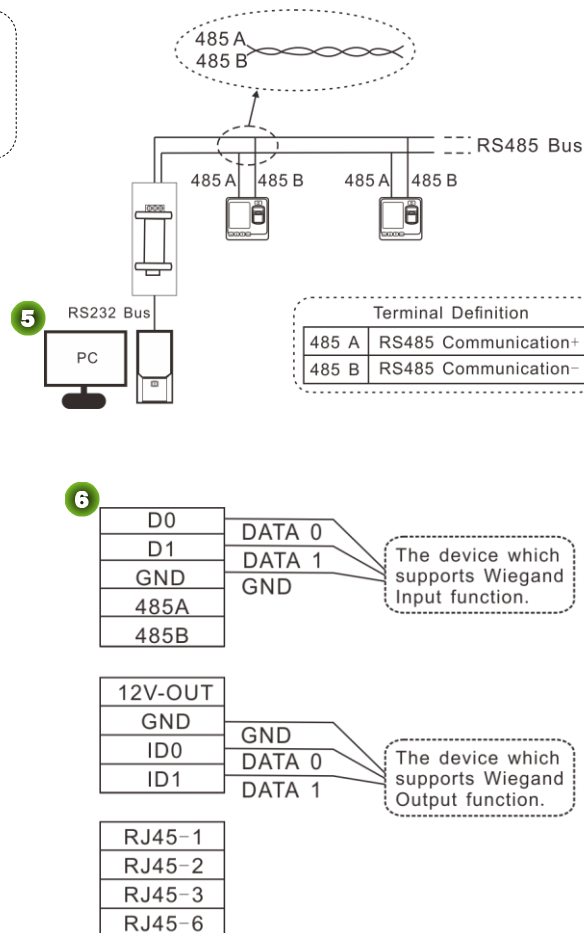
- **Wiegand Function**

Wiegand Output: This device provides standard Wiegand 26 output, which can be used as reader. The distance from the controller to device cannot be more than 15 meter (If the signal must be transferred much further or there is a strong interference around, please adopt a Wiegand signal amplifier. For detail, please see **Figure 6**.)

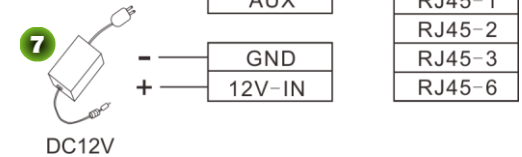
Wiegand Input: The device has Wiegand input function, can connect the external card reader. Device and card reader can be installed respectively inside and outside of the door, control the lock together, control out & in. (For detail, please see **Figure 6**.)



 **Note:** No matter the device is powered by access controller or not, the ground ports of them have to be properly together to ensure the Wiegand transfer reliable.



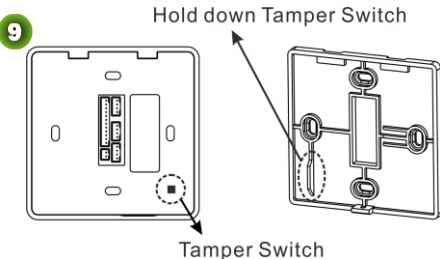
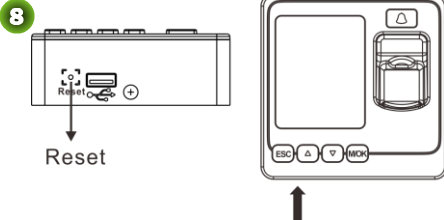
- **Power Connection:** Shown as **Figure 7.**



iii. Test and examine after installation

Make a test and examine prior to power on, inspect whether the lock driver is OK or not.

1. The green LED begins to glitter after power up.
2. Enter **[Main menu] > [System] > [Auto Test]**.
3. Enter **[Main menu] > [User Mng] > [New User] > [Enroll FP]**, Enroll a fingerprint, and use the fingerprint to test access system and door lock.
4. If there is no any problem. Please delete this enrolled fingerprint.



iv. Reset and Tamper Switch

Reset: Due to operation error or other accidents, which leads the device failed to work, you can restart device through reset button.

To reset the device use a small tool (e.g., pin or paperclip) to push in the reset button (labeled **Reset**, shown as **Figure 8**) located on the underside of the device.



Note: it does NOT erase any stored data (i.e. templates, transactions, settings). This information will be available as soon as power is restored.

Tamper Switch is located on the back of the device (**Shown as Figure 9**), when the device detects it is being "tampered" with, it will send an alarm signal.

If the administrator was lost, you can wait about 30 seconds (there is a short beep tip) after the device is disassembled from the wall, then press the tamper switch three times to access the device menu.

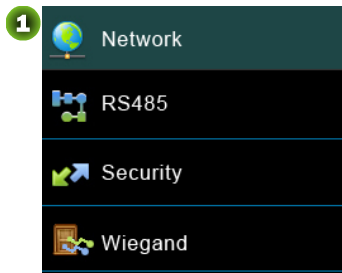
5. Quick Start Guide



Press & hold **(MOK)** key to enter the **Main menu** interface; include **User Management (User Mng)**, **Access Setting (Access)**, **Communication Setting (Comm.)**, **System Setting (System)**, **Data Management (Data Mng)** and **U Disk Management (U Disk)**.

I . Communication Setting

Press & hold  key to enter the **Main menu** interface, press  key to select [**Comm.**] sub-menu, and then press  key to enter the **Communication Setting (Comm.)** Interface, shown as **Figure 1**.



Network: Set IP address (The default value is 192.168.1.201), **Subnet mask** (The default value is 255.255.255.0) and **Gate Way** (The default value is 192.168.1.254) for device.

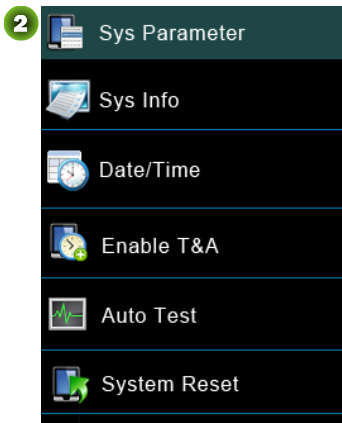
RS485: Set the baud rate for the communication between the device and PC.

Security: Set Device ID and password for the connection between the device and PC. The default password is 0 (that is, no password).

Wiegand: To configure Wiegand Function.

II . System Setting

Press & hold  key to enter the **Main menu** interface, press  key to select [**System**] sub-menu, and then press  key to enter the **System Setting (System)** Interface, shown as **Figure 2**.



Sys Parameter: Set **Threshold (1:1)**, **Match Threshold (1:N)**, **Date Format**, **Sleep time**, whether enable **Key tones/Voice** and adjust **Volume** as required.

Date/Time: Set device's Date and Time as required.

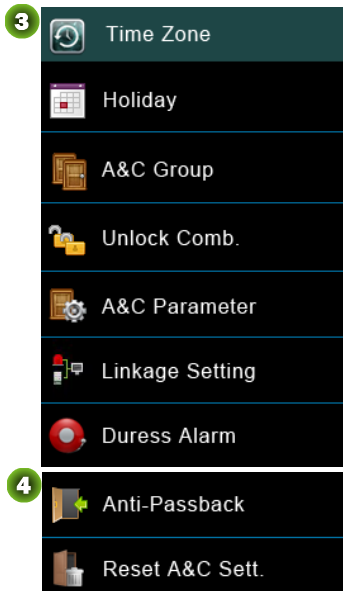
Enable T&A: Enable/Disable **T&A Status** and **Auto Switch** function as required. In additional, you can set the auto switch time for each status.

Auto Test: **TFT Test**, **Sensor Test** and **RTC Test**.

System Reset: Restore all system parameters to factory default settings.

III. Access Setting

- Press & hold  key to enter the **Main menu** interface, press ▼ key to select [**Access**] sub-menu, and then press  key to enter the **Access Setting (Access)** Interface, shown as **Figure 3, 4**.



Time Zone: Add **Time Zones** for device. The device controls access according to the Time Zones.

Holiday: Add access holiday, and select Access Time Zone for it.

A&C Group: Access Group refers to one selected Time Zone or several selected Time Zones that can be opened by verification. (**Note:** The A&C Group must be set under **Access Setting**.)

Unlock Comb.: Add Unlock Combination for device.



Note: The total number of users in the access group must be equal to or smaller than 5.

A&C Parameter: Set **Lock(S)**, **Door Sensor Delay(S)**, **Door Sensor Mode** (Open, Close or No), **Alarm Delay(S)**, **Alarm Count** (times), **Close/Open Time Zone** and whether **valid holidays**.

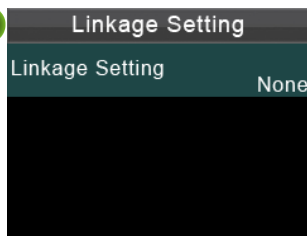
Linkage Setting: The specific setting method, please see **Linkage Setting**.

Duress Alarm: Set the duress alarm delay time as required.

Anti-Passback: Set anti-passback function for device.

Reset A&C Sett.: Reset all the Access Setting to factory defaults and then restart device automatically.

5



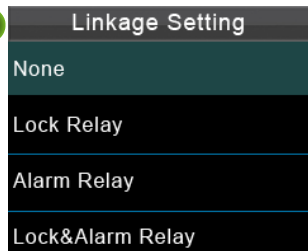
○ Linkage Setting

The device supports Auxiliary Input function. On receiving the linkage signals, the device will perform related linkage operations accordingly.

1. In the **Access Setting** interface, press ▼ key to select [**Linkage Setting**] sub-menu, and then press **MOK** key to enter the **Linkage Setting** interface; shown as **Figure 5**.
2. Press **MOK** key to enter the modify linkage setting interface, shown as **Figure 6**.
3. Press ▼ key to move the cursor to select linkage type, and then press **MOK** key to save and return to the previous interface.

- ✧ **Lock Relay:** The lock is opened after the device receives the linkage signal.
- ✧ **Alarm Relay:** An alarm is triggered after the device receives the linkage signal.
- ✧ **Lock & Alarm Relay:** The lock is opened and an alarm is triggered after the device receives the linkage signal.

6

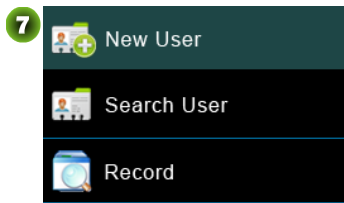


○ Cancel Linkage

Press & hold **MOK** key to enter the **Main menu** interface. The **Cancel linkage?** message will display on the screen. Press **MOK** key to confirm and cancel linkage.

IV. User Management

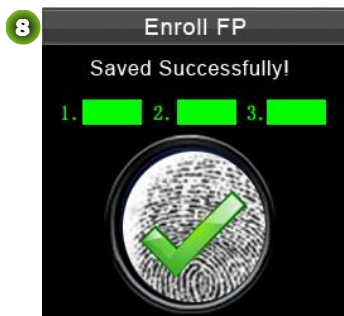
- Press & hold **MOK** key to enter the **Main menu** interface, press ▼ key to select [**User Mng**] sub-menu, and then
- press **MOK** key to enter the **User Management (User Mng)** Interface, shown as **Figure 7**.



New User: Input **ID No.** (The max length is 9.), **PSW** (The max length is 6.) and **Card** (Optional), set **Purview** (User or Admin).

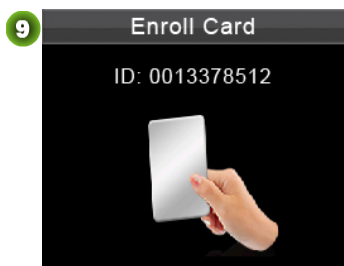
Search User: Input **ID No.** and press **[MOK]** key to search the corresponding user; and then Edit/ Delete user or set User Access as required.

Record: Input **ID No.** and **Month** and press **[MOK]** key to query attendance logs of the user with the specified ID in the specified month.



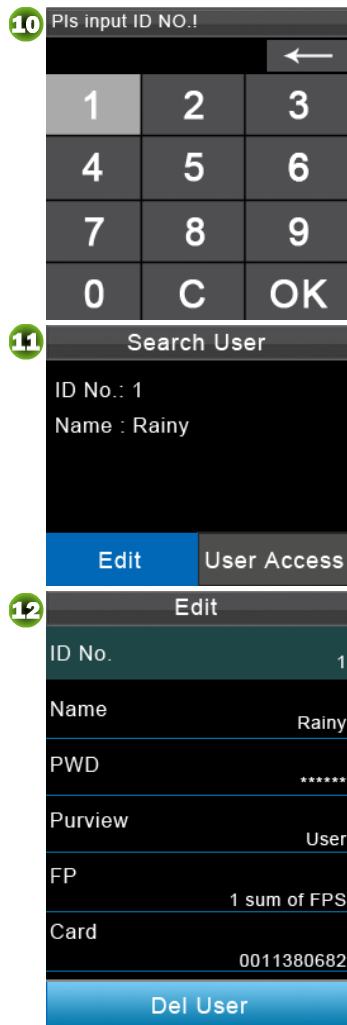
○ Enroll Fingerprint

1. In the **New User** interface, press **▼** key to move the cursor and select **[FP]**, and press **[MOK]** key to enter the **Enroll FP** interface.
2. According to the operation prompt information, place finger on the Fingerprint Sensor properly. Place the same finger on the Fingerprint Sensor for three consecutive times correctly until enrollment succeeds, and then return to the **New User** interface automatically.
3. Press **[ESC]** to exit, save user information according to the operation prompt box.



○ Enroll Card (Optional)

1. In the **New User** interface, press **▼** key to move the cursor and select **[Card]**, and press **[MOK]** key to enter the **Enroll Card** interface.
2. According to the operation prompt information, punch card at the punch area (at the Fingerprint Sensor; after enrollment succeed, return to the **New User** interface automatically.
3. Press **[ESC]** to exit, save user information according to the operation prompt box.



○ Search User

1. In the **User Mng** interface, press ▼ key to move the cursor and select [**Search User**], and press **MOK** key, the interface shown as **Figure 10**.
2. Press ▲/▼ to move the cursor on the desire numeric and then press **MOK** key to confirm and enter numeric. (**Note:** You can press ▲/▼ to move the cursor on the ← button, and then press **MOK** key to delete the incorrect input.)
3. After input **ID No.**, press ▲/▼ to move the cursor on [**OK**] button, and then press **MOK** key to search the corresponding user, shown as **Figure 11**.

○ Edit User

Edit the added user. (**Note:** In the **Search User** interface, press **MOK** key to enter the Edit interface, the specific operation are same as **New User** (Add User).

○ Delete User

1. In the **Edit** interface, press ▼ key to move the cursor and select [**Del User**] sub-menu, shown as **Figure 12**.
2. Press **MOK** key to enter the **Del User** interface, press ▼ key to move the cursor to select delete type (Delete Password, Del ID Card only, Delete Fingerprint or Delete User), and then press **MOK** key to confirm and carry out the corresponding delete operation.



Note:

- (1) Based on the information registered by a user, the device displays the optional operation types. For example, if the user does not register the password, the option **Delete Password** is not available.
- (2) If **Del User** is selected, the user's fingerprint, password, and ID card (optional) information will be deleted.

13

User Access	
ID No.	1
Group No.	1
Use TZ	Grp TZ
Duress FP	1 sum of FPS
VerType	GrpVerType

○ User Access Setting

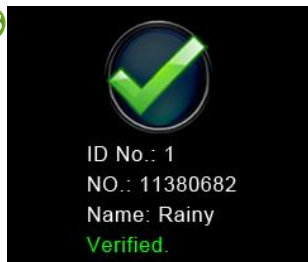
1. In the **Search User** interface, press ▼ key to select [**User Access**], press **MOK** key to enter the **User Access** setting interface, shown as **Figure 13**.
2. Set the Group No., Use Time Zone and select Duress FP as required.

V. User Verification

14



15

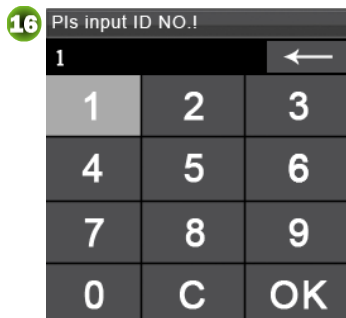


○ Using Fingerprint / Card(Optional) to Verify

Place finger on the Fingerprint Sensor properly or punch card in the punch area (at the Fingerprint Sensor); after verification succeed, the interface shown as **Figure 14** (Fingerprint Verification), **15** (Card Verification).

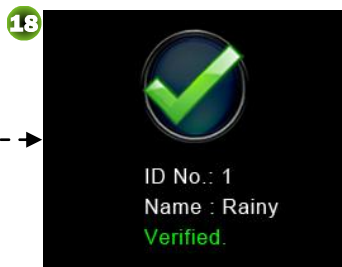
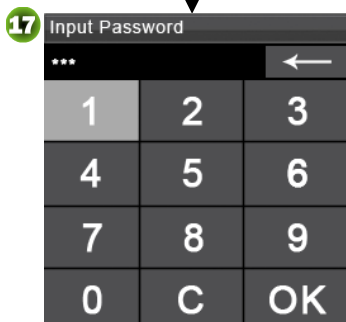


Note: The card verification is an optional function.



○ Password Verification

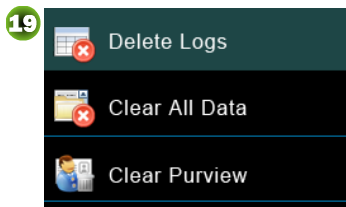
1. In the initial interface, press **MOK** key to enter the **Input ID NO.** interface; input **ID NO.**, shown as **Figure 16**. (The specific input method, please see **Search User**.)
2. Press **▲/▼** key to move the cursor on **[OK]** button, and then press **MOK** key to confirm and enter the **Input Password** interface.



3. Input password (The specific input method is same as input **ID NO.**), shown as **Figure 17**.
4. Press **▲/▼** key to move the cursor on **[OK]** button, and then press **MOK** key to confirm; after verification succeed, the interface shown as **Figure 18**.

VI. Data Management

- Press & hold **MOK** key to enter the **Main menu** interface, press **▼** key to select **[Data Mng]** sub-menu, and then press **MOK** key to enter the **Data Management (Data Mng)** interface, shown as **Figure 19**.



Delete Logs: Delete all attendance logs.

Clear All Data: Delete all attendance logs, user information, and Time Zone, Holiday, A&C Group, Unlock Combination settings.

Clear Purview: Set all the administrators to ordinary users.

VII. U Disk Management

Press & hold **MOK** key to enter the **Main menu** interface, press **▼** key to select [**U Disk**] sub-menu, and then press **MOK** key to enter the **U Disk Management** interface, shown as **Figure 20**.



Download Attlog: Download all attendance logs to the U Disk. And then import logs into the **Access 3.5** software through **Import Data From USB disk** function, and then view Access Report as required.

Download User: Download all user information to the U Disk.

Upload User: Upload user information (stored in U Disk) into the device.

Update: You can upgrade the device firmware through this menu; an upgrade file is needed in the U Disk.

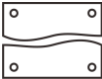
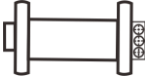
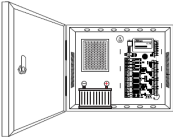
VIII. View Access Report

1. Connect the device to the network.
2. Run **Access3.5** software.
3. Add the device to the software, download logs from device (you can use the U Disk to download logs too), and then analyze logs and view the access report as required.

Bundled *Access3.5 Security System* is unique software. For detailed operations, refer to **Access3.5 software user manual** in the CD.

6. Others

The following equipments are needed for an access control system but are not included in the standard package.

Name	Picture	Name	Picture
PC		Lock	
Door Sensor		Exit Button	
Alarm		485 Convertor	
Access Control Panel		Network Cable	
Door Bell			



#24,Shambavi Building, 23rd Main, Marenahalli,
JP Nagar 2nd Phase, Bangalore - 560078
Phone: 91-8026090500 | Email : sales@esslsecurity.com
www.esslsecurity.com