USER MANUAL

BR1200

Version: 1.0

Date: February 2019

Important Statement

Thank you for choosing our product. Before using this product, please read this user manual carefully to avoid risks of danger to the users of this product or those nearby and damaging the device. Follow these instructions to ensure that your product functions properly and completes verifications in a timely manner.

Unless authorized by our company, no group or individual shall take excerpts of or copy all or part of these instructions nor transmit the contents of these instructions by any means.

The products described in this manual may include software that is copyrighted by our company and its possible licensors. No one may copy, publish, edit, take excerpts of, decompile, decode, reverse-engineer, rent, transfer, sublicense, or otherwise infringe upon the software's copyright unless authorized by the copyright holder(s). This is subject to relevant laws prohibiting such restrictions.

As this product is regularly updated, we cannot guarantee exact consistency between the actual product and the written information in this manual. Our company claims no responsibility for any disputes that arise due to differences

About This Manual

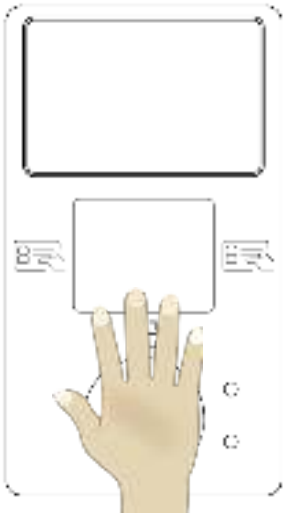
- This manual mainly introduces operating the user interfaces and menu functions of 2.4 Inch color screen devices.
- The product images in this manual may not be exactly inconsistent with your product; the actual product's display shall prevail.
- The functions with ★ symbol are optional.

Table of Contents

1. Notes before use

1.1 Enrollment and Verification of palm ★

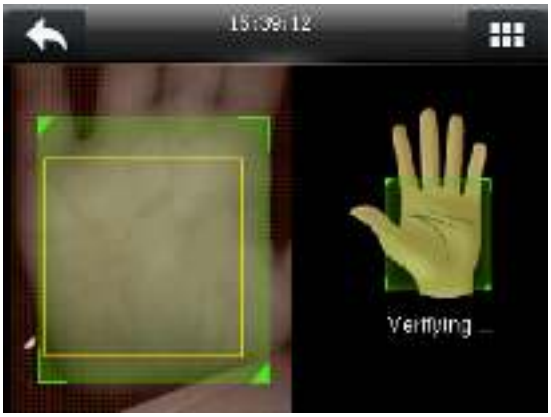
- **How to correctly enroll the palm**



Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device. Fingers naturally open.

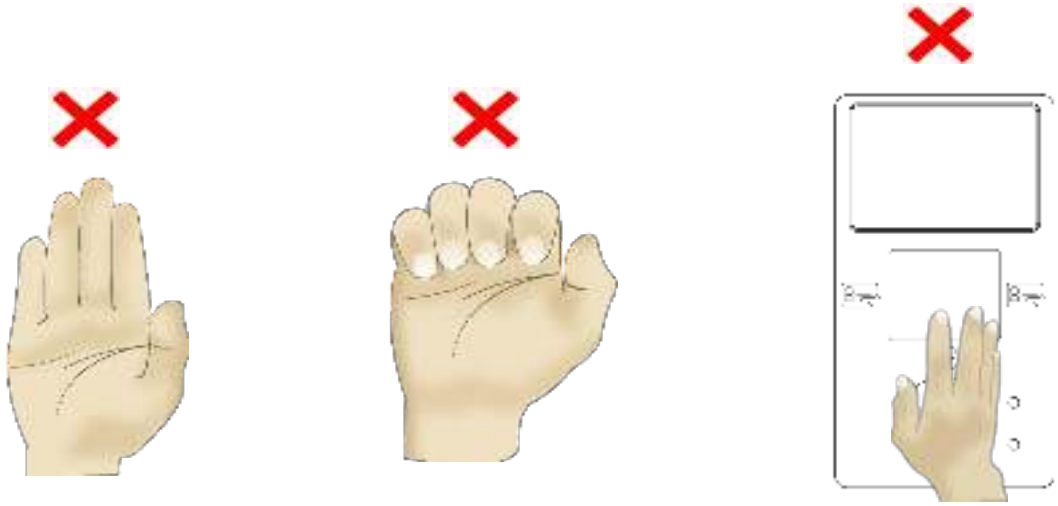
During enrollment locate your palm at the center of the screen, and follow the screen tips "Focus the center of the palm inside the green box". The user needs to move forward and backward to adjust the palm position during the palm registration.

- **Verification**



Place your palm in the green area parallel to the device with space between the fingers.

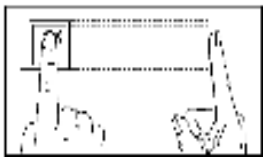
- **Incorrect palm gestures**



1.2 Method of Fingerprint registration ★

It is recommended to use the **index finger, middle finger** or **ring finger**; avoid using the thumb and little finger.

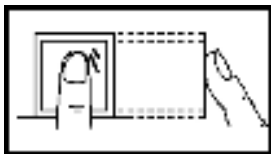
- **Correct way to press the fingertip onto the sensor:**



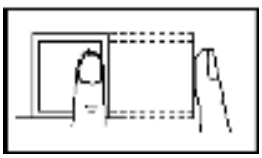
Press the fingertip horizontally onto the fingerprint sensor; the center of the fingertip should be placed on that of the sensor.

- **Wrong ways to press the fingertip onto the sensor:**

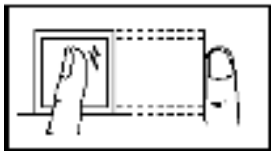
Pressing vertically onto the sensor



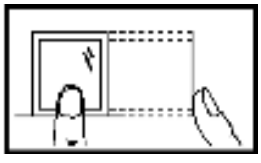
Pressing on the side of the sensor



Tilting while pressing onto the sensor



Pressing too low onto the sensor

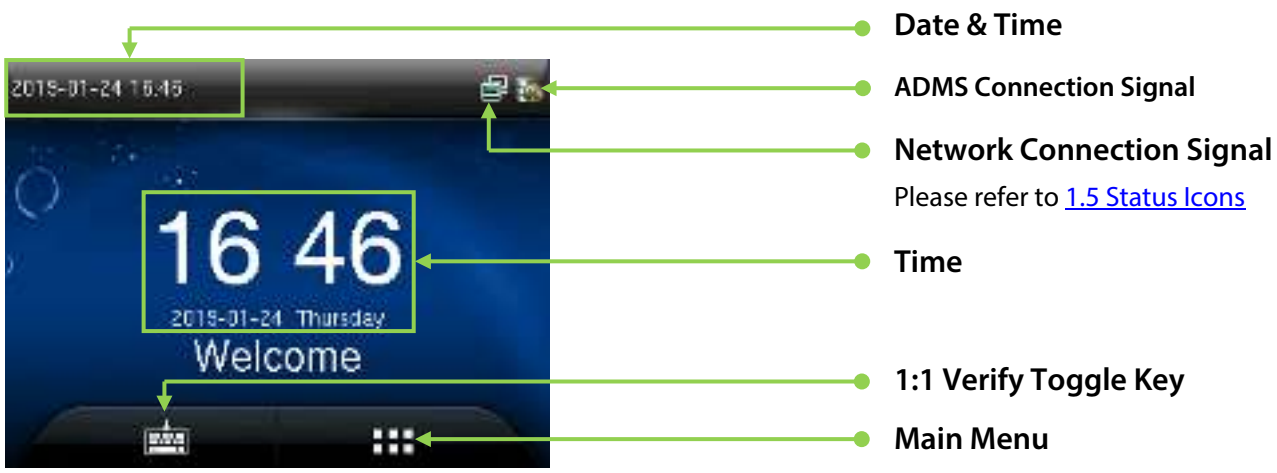


1.3 Use of Touch Screen

Touch the screen with one of your fingertips or the top of the forward edge of a fingernail, as shown in the following figure. A broad point of contact may lead to inaccurate pointing.

1.4 Initial Interface

When the device is turned on, the initial interface is shown as below:

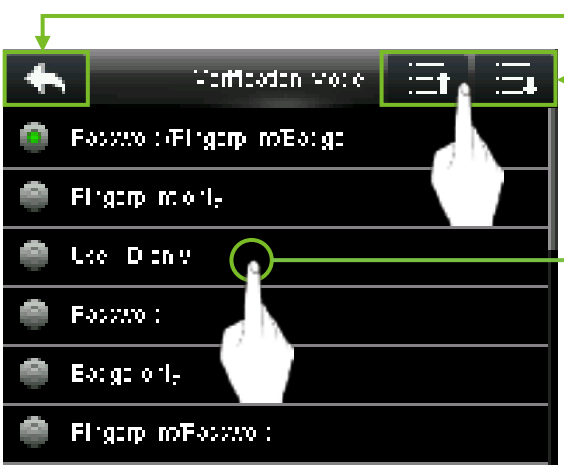


1.5 Status Icons

Status Icon	Name	Descriptions
	Ethernet	Indicates that the connection to Ethernet has been established.
		Indicates that the Ethernet is disconnected.
	ADMS server	The connection between device and ADMS server is successful.
		The connection between device and ADMS server is failed.
		The communication data of ADMS are being transmitted.

1.6 Touch Operations

- **Basic Operations**



Return and Save

Page Up and Page Down

Click the line where the menu option is located to select the option and then automatically return to the previous interface.

Note: During operations, after registering or modifying user information or setting parameters, you need to tap **Return/Save** to make the settings take effect. If timeout and no operations on the interface, the system returns to the main interface without saving registration, user information modification or parameter settings.

- **Soft Keypad**

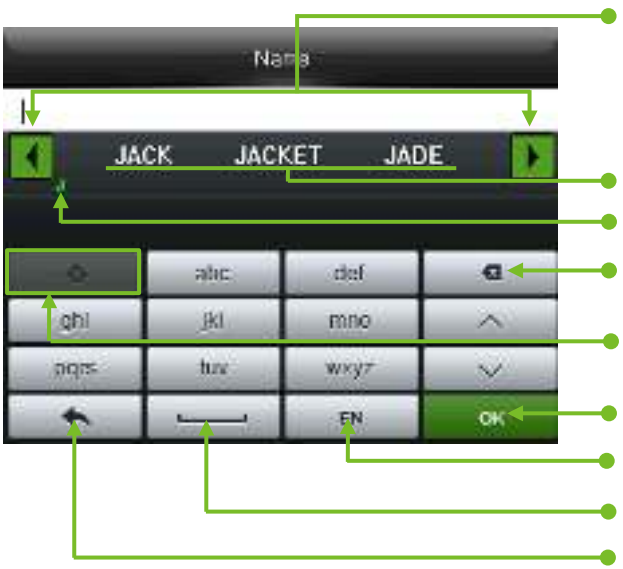
Content display area

Clearing previous entry

Confirming the entry

Return key

- **Letter Keypad**



Tap for text rummage leftwards and rightwards

Text suggestion area

Enter the content display area

Clearing previous entry

Tap to switch to the uppercase keypad

Confirming the entry and returning

Tap to switch to the Letter, digital and symbol keypad

Space key

Return key

- **Digital and Symbol Keypad**

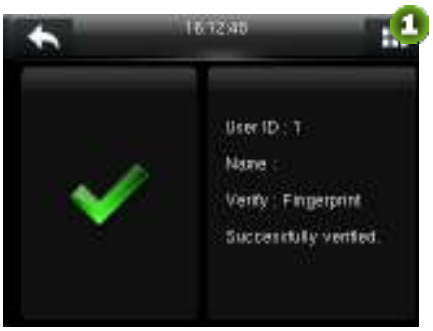
1.7 Verification Modes

1.7.1 Fingerprint Verification ★

- **1 : N Fingerprint Verification**

Under this fingerprint verification method, a fingerprint collected by the sensor is verified with all fingerprints stored in the device.

Please use the correct way to press the fingertip onto the fingerprint sensor (for detailed instruction, please refer to 1.2 Method of Fingerprint registration).



Verification Succeeds.

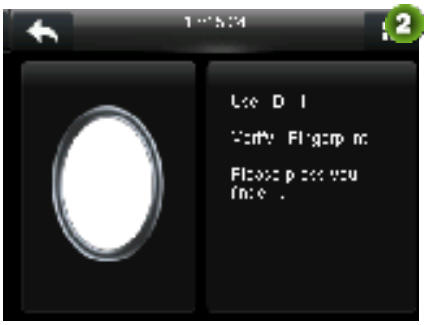
Verification Fails.

- **1 : 1 Fingerprint Verification**

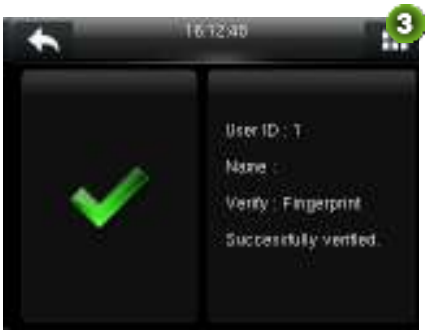
Under this fingerprint verification method, a fingerprint collected by the sensor is verified with the fingerprint matched to the entered user ID. Please use this method when difficulty is encountered during 1:N fingerprint verification.

Press  **on the screen to enter 1:1 Verify Mode.**

Enter your ID and tap **[OK]**.



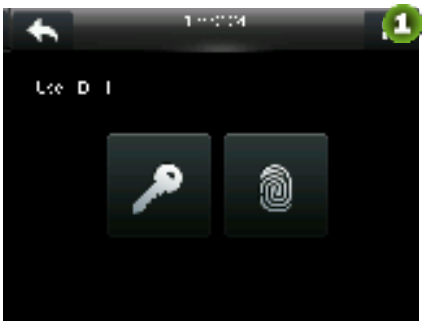
Press your fingerprint for verification.



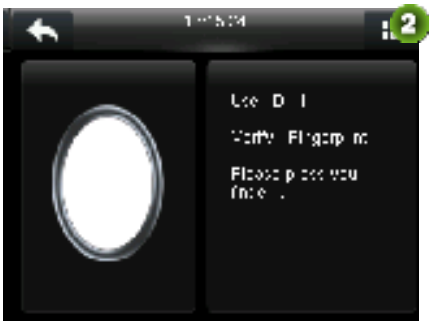
Verification Succeeds.

Verification Fails.

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap **[OK]**.



Tap the Fingerprint icon to access the fingerprint verification



Press your finger onto the fingerprint scanner to scan your fingerprint for verification. The result is displayed as above.

Remarks:

1. Type the user ID when the device is on the initial interface and press **[OK]** button. If "No enrolled data!" is displayed, this means the user ID does not exist.
2. When the device displays "please press your finger again", press your finger again onto the fingerprint sensor. The device allows users to retry twice by default. Retry times can be set as per 7.3 Fingerprint Parameters. If verification still fails after 2 attempts, the system will exit to the initial interface.

1.7.2 Palm Verification ★

- **1 : N Palm Verification**

Under this palm verification method, a palm collected by the sensor is verified with all palms stored in the device.

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device. The device will automatically detect as palm verification mode.

- **1 : 1 Palm Verification**

Under this palm verification method, a palm collected by the sensor is verified with the palm matched to the entered user ID. Please use this method when difficulty is encountered during 1:N palm verification.

Press  **on the screen to enter 1:1 Verify Mode.**

Enter your ID and tap **[OK]**.

Press your palm for verification.

Verification Succeeds.

Verification Fails.

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap **[OK]**.

Tap the Palm icon to access the palm verification interface.

Place your palm in the palm multi-mode collection area, such that the palm is placed parallel to the device. The result is displayed as above.

1.7.3 Password Verification

Under this verification method, the entered password is verified with the password of the entered user ID.

Press  **on the screen to enter 1:1 Verify Mode.**

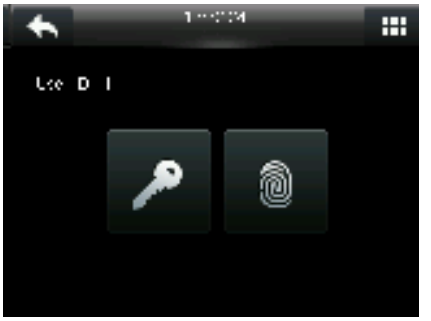
Enter your ID and tap **[OK]**.

Input the Password and press **[OK]**.

Verification Succeeds

Verification Fails

If you have registered multiple verification modes, the following interface appears after you enter your ID and tap **[OK]**.



Tap the Key icon to access the password verification interface.

The verification result is displayed as above.

Note: If you have registered only the password, you will access the password verification interface directly after entering your ID. If you have registered in multiple verification modes, the icons of

registered verification modes are displayed, just as the above figure showing that Password, Fingerprint or Palm have been registered.

1.7.4 Card Verification ★

Card function is optional, only products with a built-in card module are equipped with card verification function.

Swipe the ID card or Mifare card ★ above the card area (the card must be registered first).

Verification Succeeds.

Verification Fails.

1.7.5 QR Code Verification ★

QR Code is processed as the card number. When a new user registers the card number, in addition to swiping the card, QR Code can also be used for registration.

Note: You can use the QR code generator to convert the card number into a QR code for registration.

Scan the QR code at the camera area for verification (the QR code must be registered first).

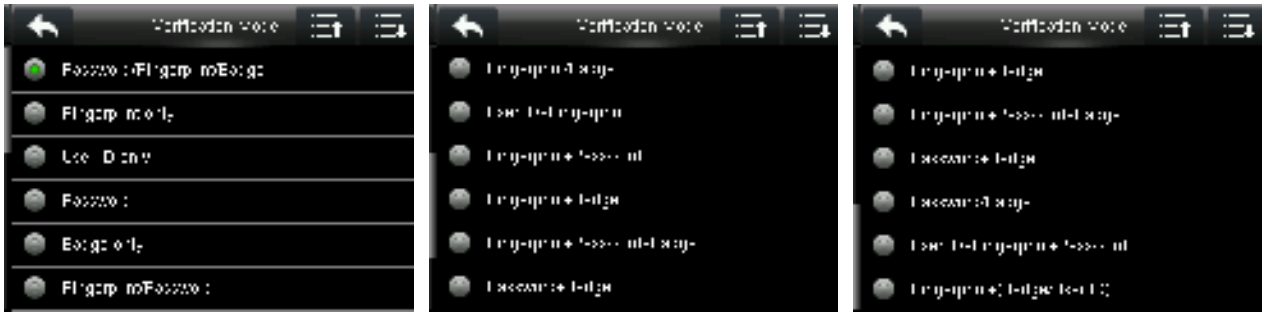
Verification Succeeds

Verification Fails

Remarks: When the verification mode is card, it includes card verification and QR code verification by default.

1.7.6 Combined Verification

In order to meet the needs of some access control occasions with high security and in consideration of the diversity of access control, the device provides a wide range of verification modes, which can be combined as required for individual users and user groups. The device supports 15 combinations verification modes, as shown in the following figure.



Note:

"/" means Or, and "+" means And.

In combination verification mode, you must register required verification information, otherwise the verification may fail. For example if user A uses **Fingerprint Registration** but the verification mode is **Password**, this user will never pass verification.

The following takes **Fingerprint + Password** as an example to introduce the combination verification mode.

Press your finger onto the fingerprint scanner to scan your fingerprint for verification. The result is displayed as above.

The password entry interface pops up after verification passes. Enter the password and tap [**OK**].

Fingerprint + Password verification succeeds.

Fingerprint + Password verification fails.

☺ **Remarks:** The combination verification is available only if corresponding verification modes are selected. You can set it in the following way:

When the device is in standby mode, press  on the screen to open the Main Menu, press **Access Control** > **Access Control Options** > **Verification Mode** to enter the **Verification Mode** setting interface.

2. Main Menu

When the device is in standby mode, press to open the Main Menu.

- **User Management:** It can add new users. Contains basic information of registered users, including user ID, name, user role, fingerprint, palm★, badge number★ (**ID card, QR code and MiFare** are optional), password, user expiration rule and access control role.
- **Device Settings:** It is used to set user roles for gaining access to the menu and editing options.
- **Comm. Settings:** It is used to set the related parameters of the communication between the device and PC, including ethernet parameters such as IP address etc., Serial Comm, PC connection and cloud server settings.
- **System Settings:** It will set related parameters of the system, set date & time, set access logs, palm parameter and fingerprint parameters★ and reset to factory settings.
- **Personalize:** It will set interface display.
- **Data Mgt.:** It is used to clear, backs up, or restores related data in the device.
- **Access Control:** It will set the parameters of the control lock and access control devices, including parameters of access control, time schedule, holidays, combined verification.
- **Attendance Search:** It will search for the records stored in the device after successful verification.
- **Auto Test:** It will automatically test different module's functions, including the LCD, fingerprint sensor and clock RTC test.
- **System Information:** It is for checking device capacity, device and firmware information.

3. Adding User

When the device is on the initial interface, press button > **User Management** > **New User** to enter **New User** setting interface. You need to input User ID and name, choose User Role, register Fingerprint and Badge Number, set Password and set Access Control Role.

3.1 Entering a User ID

The device automatically assigns user IDs for personnel, starting from "1". The user ID can also be manually entered.

Press **User ID**.

Enter your ID and press **[OK]** to save and exit.

The user ID entry is completed.

Note:

1. The user ID may contain 1-9 digits by default. If you want to expand the number of digits, please consult our pre-sales technical support personnel.
2. During the initial registration, you can modify your ID, which cannot be modified after registration.

3.2 Entering a User Name

Press **Name**.

Enter your name and press **[OK]** to save and exit.

The name entry is completed.

Note: A user name may contain 1-12 characters by default.

3.3 Setting the User Role

There are two types of user accounts: the normal users and the super administrator. If there is already a registered administrator, the normal users have no rights to manage the system and may only access authentication verifications. The administrator owns all management privileges.

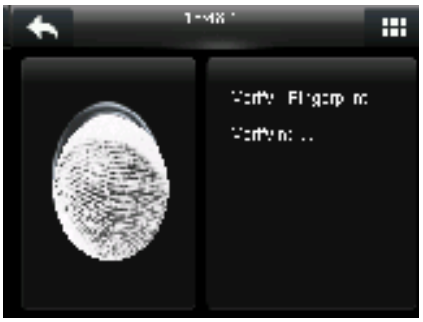
Press **User Role**.

Select a user role.

User role selection is completed.

If the selected user role is the Super Admin, the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered. The following is an example of accessing the main menu as the super administrator by fingerprint authentication.

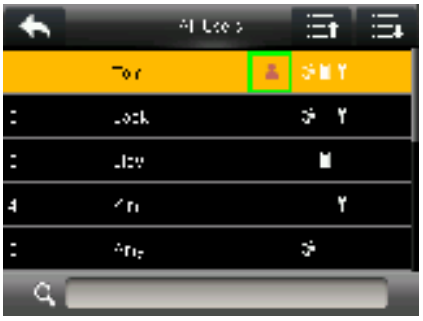
Press ⊞ button.



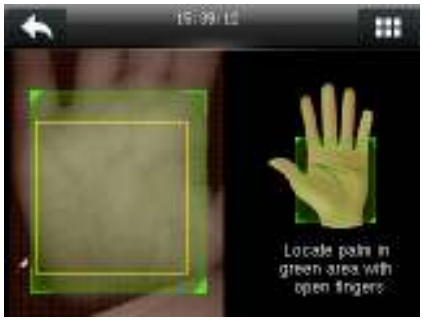
Press the fingerprint of the super administrator for authentication.

The user may access the main menu directly after successful authentication.

Example: In the below interface, the user with User ID 1 is a super admin.



3.4 Palm Template Registration ★

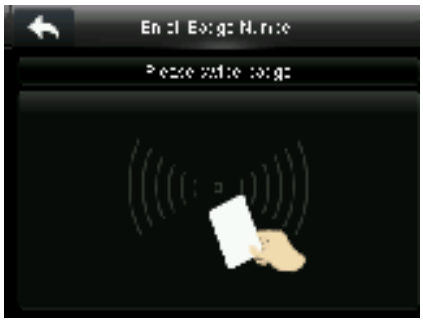


Follow the interface instructions and move back and forth to position your palm within the green frame.

The system will automatically return to the **New User** interface after successful registration.

3.5 Card Number Registration ★

Press **Badge Number**.



Place your badge close to the card swiping area.

Successful registration of card number.

The system will automatically return to the **New User** interface.

If the card has already been registered, the prompt "Error! Badge already enrolled" will appear.

Note: QR Code can also be used for registration here. You can use the QR code generator to convert the card number into a QR code for registration.

3.6 Password Registration

Press **Password**.

Enter the password and press **[OK]**.

Enter the password again and press **[OK]**.

The system will automatically return to the **New User** interface after successful registration.

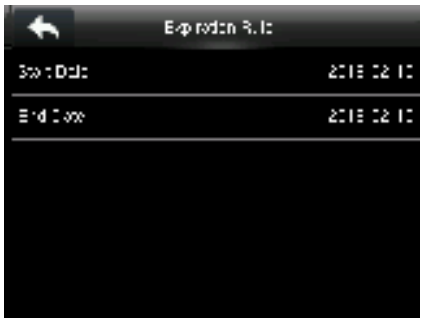
If the two entered passwords are different, the prompt "Password not match" will appear.

Note: The password may contain one to eight digits by default.

3.7 Setting Expiration Date

The device can set the period of validity of the user. When the period of validity passes, the access control permission of the user will be invalid.

Press **User Expiration Rule**.



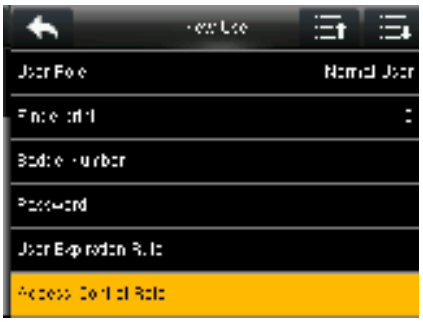
Set the start date and end date.

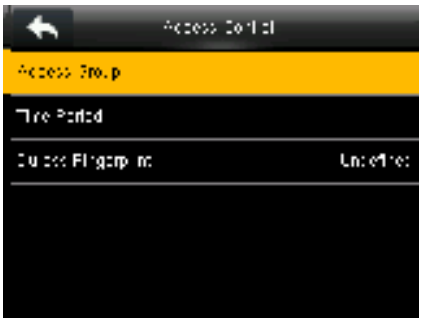
Adjust the date by "+" and "-", and press **[OK]** after setting.

3.8 Setting the Access Control Rights

Access control option is used to set door access for all the personnel. It includes access group setting, Time period, and Duress fingerprint management.

Press **Access Control Role**.





3.8.1 Access Group

Access Group: To allocate different access control groups to users for management. New users will belong to Group 1 as per default settings, but they can be reallocated to other groups.

Press **Access Group**.

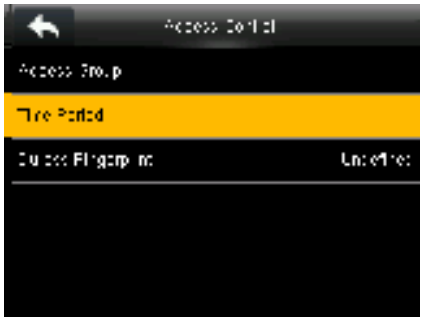
Enter the belonged group and press **[OK]**.

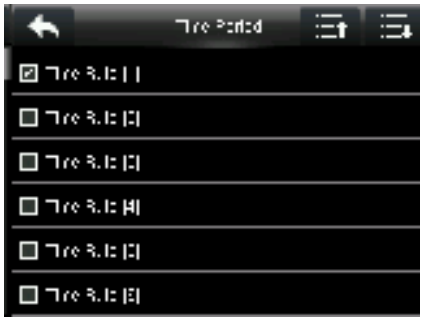
The system will automatically return to the **Access Control** interface.

3.8.2 Time Period

Choose whether to apply the time period for this user, yes by default.(**Note:**Time rules can be set in the management of access control. Up to 50 time rules can be set. For specific setting methods, please refer to "10.2 Time Rule Settings".)

Press **Time Period**.



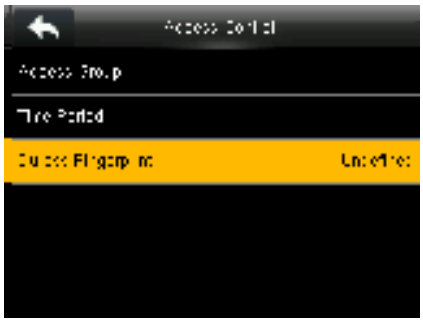


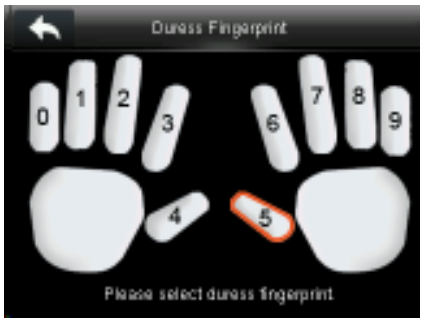
Note: In the list of "Time Rules", click and select time rules (multiple choices are available, means selected);Click the button, save and return to the previous interface.

3.8.3 Duress Fingerprint

Duress Fingerprint: User can choose one or more registered fingerprint(s) as Duress Fingerprint. When verifying through duress fingerprint, duress alarm will be triggered.

Press **Duress Fingerprint**.





Example: Among those registered fingerprints (6, 7, 8), choose the 8th fingerprint as the duress fingerprint.

4. User Management

When the device is on the initial interface, press button > **User Management** > **All Users** to enter **All Users** interface.

Note: The users are sorted by ID number, with indicating the super administrator.

4.1 Searching for a User

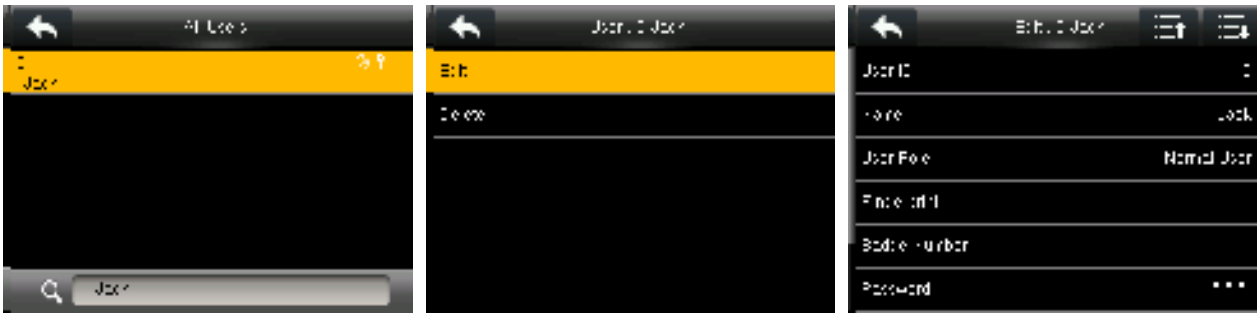
Tap the search bar on user list and enter the retrieval keyword. The system automatically finds the users related to entered keyword.

Note: The retrieval keyword can be ID, surname, given name or full name.

4.2 Editing a User

After selecting a user through 4.1 Searching for a User, choose the user from the list and click **[Edit]** to enter the user editing interface.

Or when the device is on the initial interface press button > **User Management** > **All Users** > Select a user > Click **Edit** to enter the user editing interface.



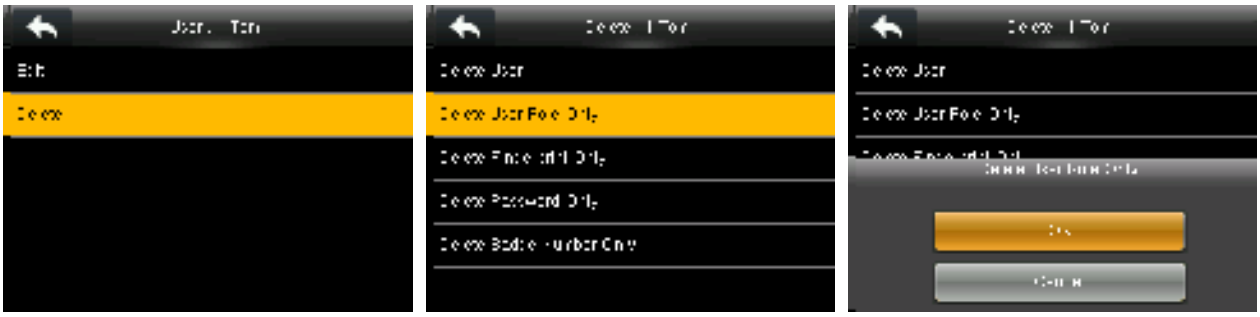
Note: The operation of editing a user is the same as that of adding a user except that the ID cannot be modified in editing a user.

4.3 Deleting a User

After selecting a user through 4.1 Searching for a User, choose the user from the list and click **[Delete]** to enter the user editing interface.

Or when the device is on the initial interface press button > **User Management** > **All Users** > Select a user > Click **Delete** to enter the user deleting interface.

Select the user information to be deleted and click **OK**.



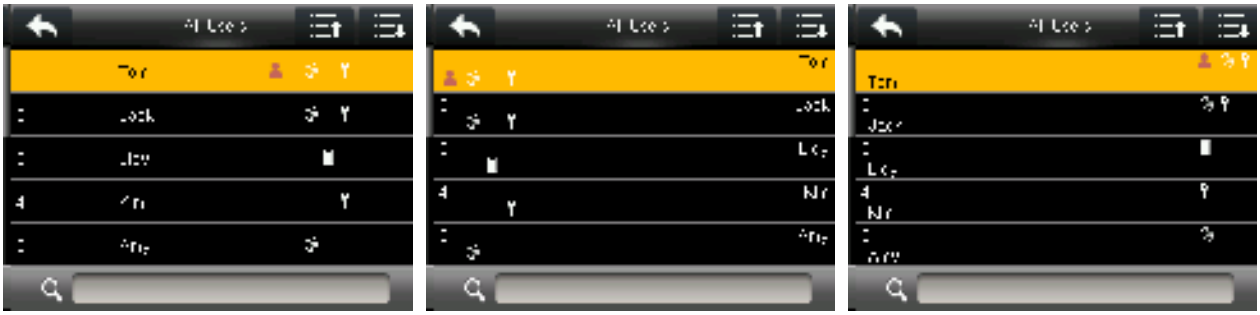
Note:

1. When deleting a user, you can choose to delete partial information such as the privilege, fingerprint, badge number or password of the user. If you select **Delete User**, all information of this user is deleted.
2. After the privileges of the super administrator is deleted, the super administrator becomes a common user, without super administrator privileges any more.

4.4 User Display Style

When the device is on the initial interface, press button > **User Management** > **Display Style** to enter the **Display Style** setting interface.

Display Styles are shown as below:



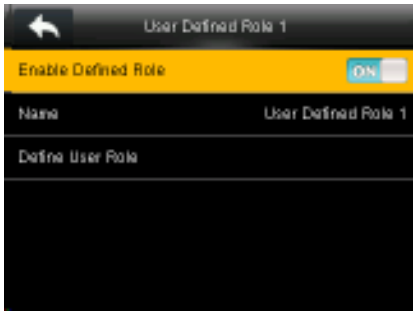
Single Line Style **Multiple Line** **Mixed Line**

5. User Role

When the device is on the initial interface, press button > **Device Settings** to enter **User Role** setting interface. Setting user rights of operating the menu (a maximum of 3 roles can be set). When user role is enabled, in **[User Management]** > **[New User]** > **[User Role]**, you can allocate suitable user role to each user.

- **Role:** Super user needs to allocate different rights to new users. To avoid setting rights for each user one by one, you can set user roles to categorize different permission levels in user management.

1.Tap any item to set a defined role.interface.



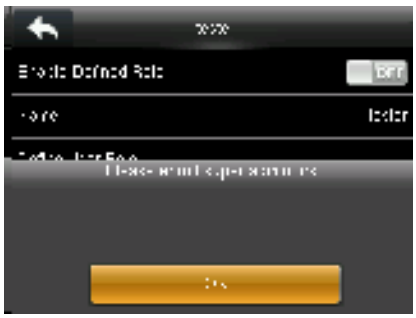
2. Tap **Enable Defined Role** to enable this defined role.

3. Tap **Name** to enter the role name.

4. The system returns to the **User Defined Role** interface.

5. Tap **Define User Role** to assign privileges to the role.

6. The role definition is completed.



Note: During privilege assignment, the main menu is on the left and its sub-menus on the right. You only need to select the features in sub-menus. If no super administrator is registered in the device, the following prompt appears after you tap **Enable Defined Role**.

6. Comm. Settings

6.1 Ethernet Settings

When the device is on the initial interface, press button > **COMM. Settings** > **Ethernet** to enter the **Ethernet** setting interface.

The parameters below are the default values, please adjust them according to the actual network.

- **IP Address:** The factory default value is192.168.1.201, please adjust them according to the actual network situation.
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 0.0.0.0
- **DNS:** 0.0.0.0
- **TCP COMM. Port:** 4370
- **DHCP:** Dynamic Host Configuration Protocol, which dynamically allocate IP addresses for clients via the server. **If DHCP is enabled, IP cannot be set manually.**
- **Display in Status Bar:** If enabled, it will display the network icon on the status bar.

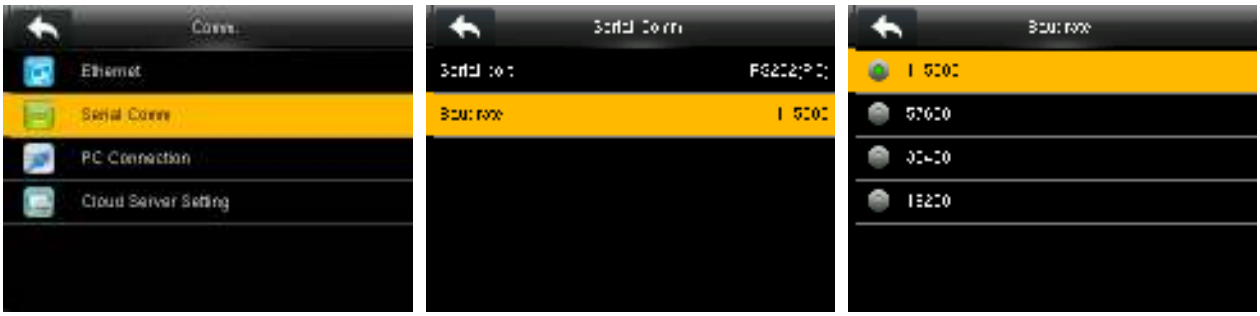
6.2 Serial Comm. Settings

When the device is on the initial interface, press button > **COMM. Settings** > **Serial Comm** to enter **Serial Comm** interface.

- **Turning On / OFF RS232/RS485 Function**

Remarks: Three functions; RS485 communication, RS232 communication, and connection with 485 Reader cannot be used at the same time. Only one function can be operated at a time.

- **Baudrate Settings**



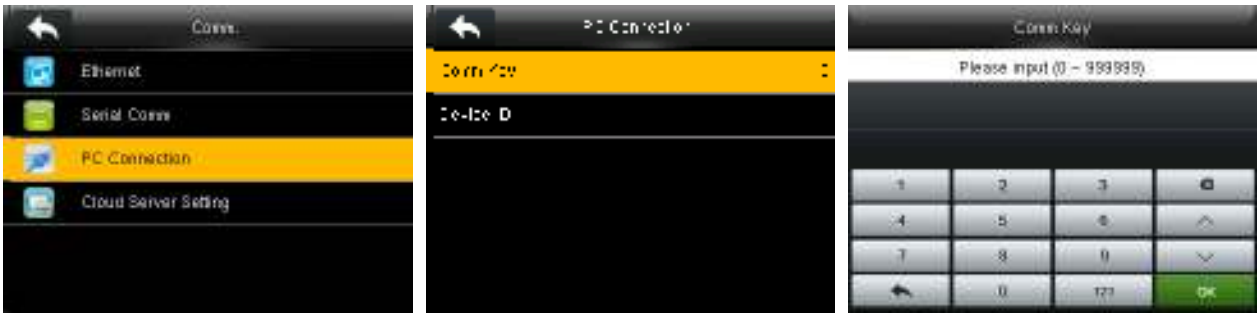
Baudrate: It is the rate of the communication with PC. There are 4 types of baud rate: 115200 (default), 57600, 38400 and 19200. The higher is the baud rate, the faster is the communication speed, but also the less reliable. In general, a higher baud rate can be used when the communication distance is shorter; when the communication distance is longer, choosing a lower baud rate would be more reliable.

6.3 PC Connection

- **Comm key Settings**

To improve security of data, **Comm Key** need to be set for the communication between the device and PC.

If a **Comm Key** is set in the device, the connection password needs to be entered when the device is connected to the PC software, so that the device and software can communicate.

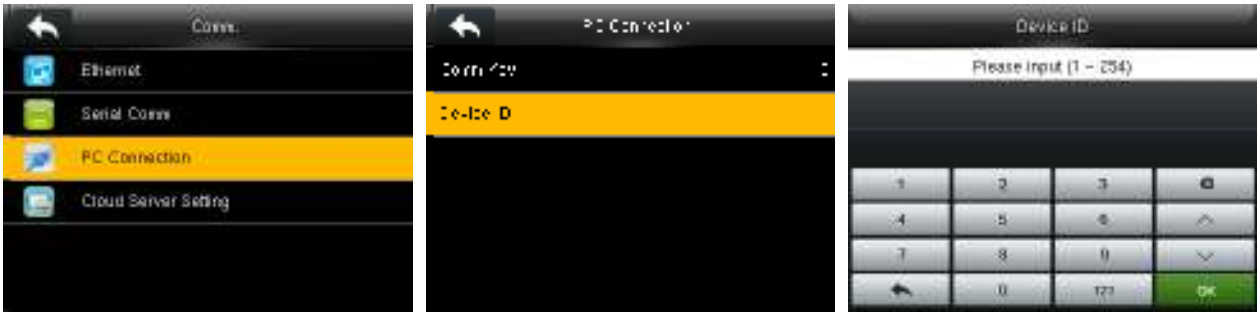


When the device is on the initial interface, press button > **COMM. Settings** > **PC Connection** > **Comm Key** to enter the **Comm Key** setting interface.

Comm Key: The default password is 0 (means no password). **Comm Key** can be from 1 to 6 digits and ranges from 0 to 999999.

- **Device ID Settings**

If the communication method is RS232/RS485 for a device, then inputting the device ID in the software communication interface is required.



When the device is on the initial interface, press button > **COMM. Settings** > **PC Connection** > **Device ID** to enter the **Device ID** setting interface.

Device ID: Input number for the device, ranging from 1 to 254.

6.4 Cloud Server Setting

This option is used to connect with ADMS server, such as IP address and port settings, and whether to enable proxy server etc.

When the device is on the initial interface, press button > **COMM. Settings** > **Cloud Server Setting** to enter the **Cloud Server Setting** interface. When the Web server is connected successfully, the main interface will display the logo.

- **Enable Domain Name:** When this function is enabled, the domain name mode is http://....., such as http://www.XYZ.com. XYZ denotes the domain name when this mode is on; when this mode is disabled, enter the IP address format in XYZ.
- **Server Address:** IP address of the ADMS server.
- **Server Port:** Port used by the ADMS server.
- **Enable Proxy Server:** Method of enabling proxy. To enable a proxy, please set the IP address and port number of the proxy server. Entering method of proxy IP and server address is same like above.

7. System Settings

7.1 Date and Time Settings

When the device is on the initial interface, press button > **System Settings** > **Date Time** to enter the date/time setting interface. It includes setting date, time, 24-hour clock and date format. When reset to factory settings, the date format will be restored as (YYYY-MM-DD).

Remarks: When reset to factory settings, the device's date/time will not be restored (if the date/time is set as "18:30 on January 1, 2020", after settings are reset, the date/time will stay at 18:30 on January 1, 2020).

7.2 Access Logs Setting

When the device is on the initial interface, press button > **System Settings** > **Access Logs Setting** to enter **Access Logs Setting** setting interface.

- **Access Logs Warning:** When the remaining recording capacity becomes lesser than the set value, the device will automatically prompt warning message. It can be disabled or set to a value ranged from 1 to 9999.

- **Circulation Delete Access Records:** It is the number of access logs allowed to be deleted at a time when the maximum storage is attained. It can be disabled or set to a value ranging from 1 to 999.
- **Confirm Screen Delay(s):** It is the duration for displaying the verification information interface after verification. The value ranges from 1 to 9 seconds.

7.3 Fingerprint Parameters

When the device is on the initial interface, press button > **System Settings** > **Fingerprint** to enter the **Fingerprint** setting interface.

- **1:1 Match Threshold:** Under 1:1 Verification Method; it is a value of similarity required, between the verifying fingerprint and the user's registered fingerprint. The value of similarity must be greater than this value to get successful verification.
- **1:N Match Threshold:** Under 1:N Verification Method, it is a value of similarity required, between the verifying fingerprint and all the registered fingerprints of the user. The value of similarity must be greater than this value to get successful verification.
- **FP Sensor Sensitivity:** It is used to set the sensitivity of fingerprint collection. It is recommended to use the default level "**Medium**". When the environment is dry, the fingerprint detection becomes slow, you can set the level to "**High**" to raise the sensibility; when the environment is humid, it gets hard to identify the fingerprint, you can set the level to "**Low**".
- **1:1 Retry Times:** In 1:1 Verification or Password Verification, users might forget the registered fingerprint or password, or presses the finger improperly. To reduce the process of re-entering user ID, retrying is allowed; the number of retries can be within 1 ~ 9.
- **Fingerprint Image:** To set whether to display the fingerprint image on the screen during registration or verification. Four choices are available.

7.4 Reset to Factory Settings

It can reset data, such as communication settings and system settings to factory settings.

When the device is on the initial interface, press ⊞ button > **System Settings** > **Reset** > **OK** to finish the reset setting.

Remark: When resetting to factory settings, the date and time will not be affected. For example, if the device date and time are set as "18:30 on January 1, 2020", the date and time will remain unchanged after resetting to factory settings.

8. Personalize Settings

8.1 User Interface Settings

When the device is on the initial interface, press button > **Personalize** > **User Interface** to set **User Interface.**

- **Wallpaper:** Select the wallpaper of the main screen as required, you can find wallpapers of various styles in the device.
- **Language:** Select the language of device as required.
- **Menu Screen Timeout (s):** When there is no operation in the menu interface and the time exceeds the set value, the device will automatically exit to the initial interface. You can disable it or set the value from 60 to 99999 seconds.

Remark: If **[Disabled]** is chosen, the system will not exit the menu interface even when there is no operation. Disabling this function is not recommended due to excessive power consumption and insecurity.

- **Idle Time To Slide Show(s):** When there is no operation in the initial interface and the time exceeds the set value, a slide show will be shown. It can be disabled (set to "**None**") or set to 3 ~ 999 seconds.
- **Slide Show Interval(s):** This refers to the interval between displaying different slide show pictures. It can be disabled or set to 3 ~ 999 seconds.
- **Idle Time To Sleep(m):** When there is no activity in the device and the set Sleep Time is attained, the device will enter standby mode. Press any key or finger to cancel standby mode. You can disable this function, or set the value to 1~999 minutes. If this function is turned to

[Disabled], the device will not enter standby mode.

Remark: Disabling this function is not recommended due to excessive power consumption.

- **Main Screen Style:** It will set the position of clock & status key and will set display style.

9. Data Mgt.

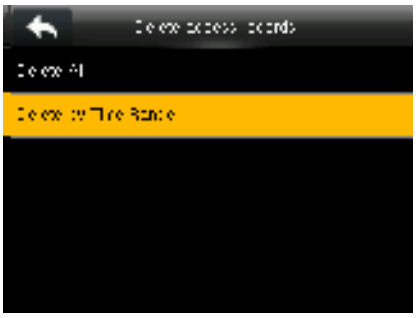
9.1 Deleting Data

To manage data in the device, which includes deleting attendance data, deleting all data, deleting admin role and deleting screen savers etc.

When the device is on the initial interface, press button > **Data Mgt.** > **Delete Data** to enter the **Delete Data** settings interface.

- **Delete access records:** To delete all access records data in the device.
- **Delete All Data:** To delete all user information, fingerprints and access logs etc.
- **Delete Admin Role:** To make all Administrators become Normal Users.
- **Delete Access Control:** To delete all access data.
- **Delete Wallpaper:** To delete all wallpapers in the device.
- **Delete Screen Savers:** To delete all screen savers in the device.
- **Delete Backup Data:** To delete all backup data.

Note: When deleting the attendance record, attendance picture or blacklist picture, you can select Delete All or Delete by Time Range. When Delete by Time Range is selected, you need to set the time range for data deletion.

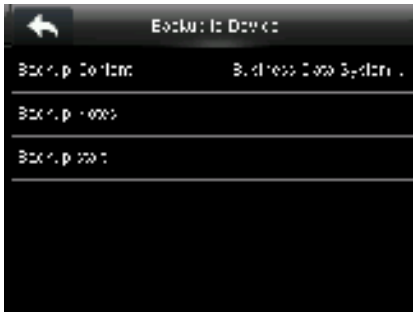


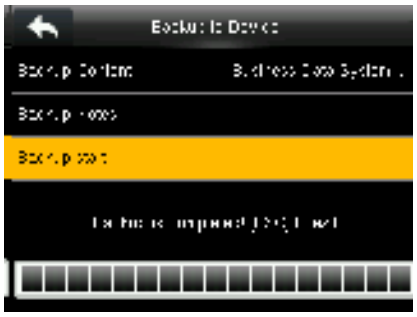
Select **Delete by Time Range**.

Set the time range and tap **Confirm (OK)**.

9.2 Data Backup

To back up the business data, or configuration data to the device.





When the device is on the initial interface, press button > **Data Mgt.** > **Backup Data** > **Backup to Device** > **Backup Content** > choose content to be backed up (**Business Data** / **System Data**) > edit **Backup Notes** (This step is optional.) > **Backup Start** to start backup. Restarting the device is not needed after backup is completed.

9.3 Data Restoration

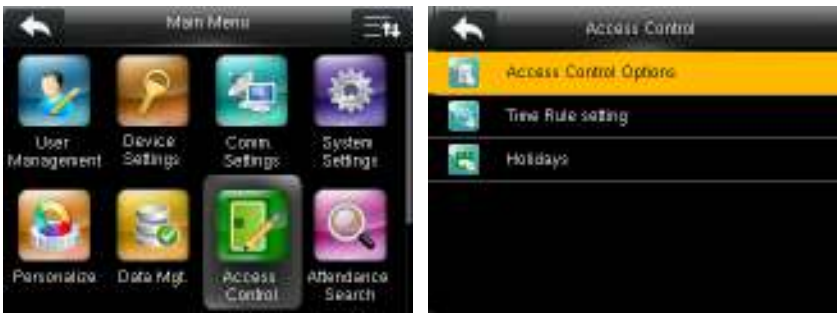
To restore the data in the device to the device.

- **Restore from USB disk:**

In the initial interface, press ⋮⋮⋮ > **Data Mgt.** > **Restore Data** > **Restore from Device** > **Content** > choose content to be restored (**Business Data** / **System Data**) > **Start Restore** > select **Yes** to start restoring. After restoration completes, click **[OK]** to automatically restart the device.

10. Access Control

Access Control option is used to set the Time Schedule, Holidays, Combined Verification etc., and the related parameters for the device to control the lock and other devices.



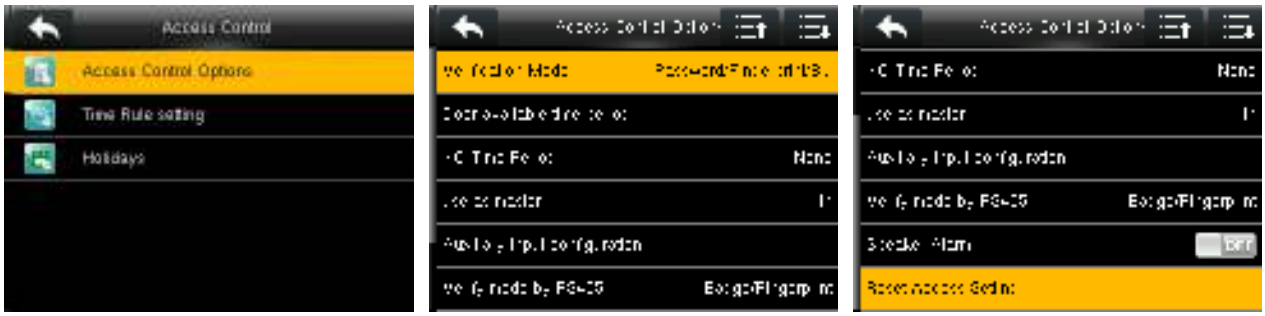
When the device is on the initial interface, press button > **Access Control** to enter the **Access Control** setting interface.

To gain access, the registered user must meet the following conditions:

1. User's access time must fall within the user's personal time zone or group time zone.
2. User's group must be in the access combo (when there are other groups in the same access combo, verification of members of those groups is also required to unlock the door).

The system defaults to the first group of newly registered users, and the default time rule is "1". If the user modifies the relevant Settings of access control, the system will change with the user's modification.

10.1 Access Control Options Settings



When the device is on the initial interface, press button > **Access Control** > **Access Control Options** to enter the **Access Control Options** setting interface.

- **Verification Mode:** The device supports 15 combinations verification modes. According to the need to choose, can choose as: password/fingerprint/badge, fingerprint only, user ID only, password, badge only, fingerprint/password, fingerprint/badge, user ID + fingerprint, fingerprint + password, fingerprint + badge, fingerprint + password + badge, password + badge, password/badge, user ID + fingerprint + password and fingerprint + (badge / user ID).

  Remarks:

  1. "/" means "or". "+" means "and".
  2. In a combined verification mode, the corresponding verification information must be registered first. For example: When User A registers fingerprint only, and the [Verification Mode] is set as "Password + Badge", User A will not pass verification.

- **Door available time period:** It is used to limit the time the user can open the door.
- **NO Time Period:** It is used to set a time period for Normally Open, so that the door is always unlocked during this period.
- **Use as master:** While configuring the master and slave devices, you may set the state of the master as **Out** or **In**.

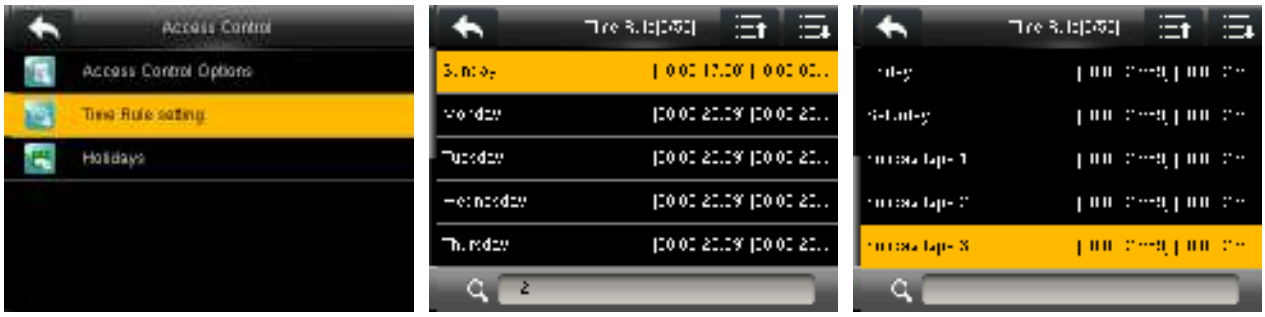
  Out: A record of verification on the master device is a check-out record.

  In: A record of verification on the master device is a check-in record.
- **Auxiliary input configuration:** To set the **Aux output/Lock open time** and **Aux Output type** for the device with auxiliary connector. **Aux Output type** includes **None**, **Trigger door open**, **Trigger Alarm**, and **Trigger Door open and Alarm**.
- **Verify mode by RS485:** It is the verification mode used by the device when it is the master unit. This option will be displayed only if RS485 reader function is enabled.
- **Speaker Alarm:** When the **[Speaker Alarm]** is enabled, the speaker will sound an alarm when the device is being dismantled.
- **Reset Access Setting:** It will reset the parameters of door lock delay, door sensor delay, door sensor type, door alarm delay, retry times to alarm, NC time period, NO time period, valid holidays, speaker alarm, Anti-Passback direction, device status, duress function, alarm on 1:1 match, alarm on 1: N match, alarm on password and alarm delay. However, the content of the Access Data Deletion in **[Data Mgt.]** will not be affected.

10.2 Time Rule Settings

Time Rule is the minimum time unit of access control settings; at most 50 **Time Rule** can be set for the system. Each **Time Rule** consists of 7 time sections (a week) and 3 holiday time schedules,, and each time section is the valid time within 24 hrs.

You may set a maximum of 3 time periods for every time schedule. The relationship among these time periods is "or". When the verification time falls in any one of these time periods, the verification is valid. The time period format is HH:MM-HH:MM in the 24-hour system with precision to minute.

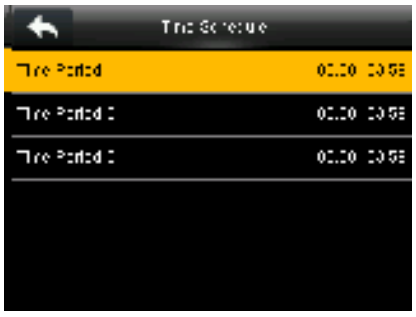


When the device is on the initial interface, press button > **Access Control** > **Time Rule setting** to enter the **Time Rule setting** interface. The default **Time Rule** No. is 1 (whole-day valid), which can be edited.

- **Editing a Time Rule**

A super administrator may edit time rules as needed. The detailed operation is as follows:

Input time rule number (such as "2"), the time rule (2) will be located automatically, select a time schedule (such as "Monday").



Select "Time Period 1/2/3" and enter time period setting interface.

Set "Start Time" and "End Time" as required, after setting, press **[Confirm(OK)]** to save and exit.

Prompt: You can set the "Start Time" and "End Time" by press ▲/▼.

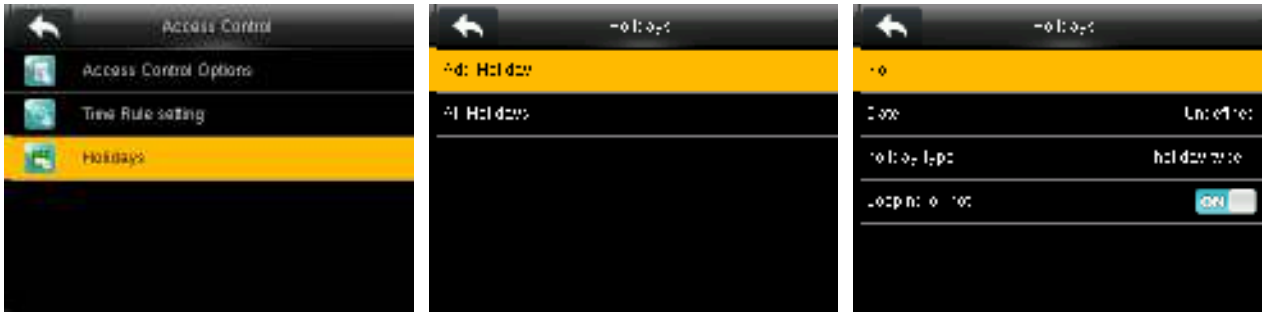
You can set other time schedules as required after setting time schedule for Monday, and then press button to exit.

Notes:

1. When the end time is earlier than the start time (for example, 23:57-23:56), this means closing all day long. When the end time is later than the start time (for example, 00:00-23:59), this means that this time period is valid.
2. **Valid Time Period:** 00:00-23:59 (Whole-day valid) or when the end time is later than the start time (for example, 08:00-23:59).
3. By default, time rule 01 indicates full-day opening (00:00-23:59).

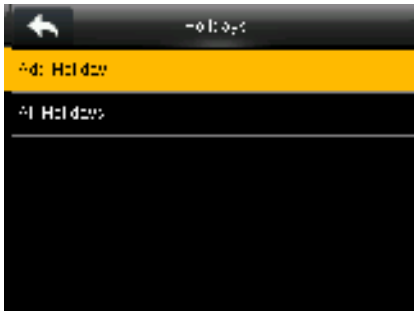
10.3 Holidays Settings

Add access control holidays for the device and set time periods on holidays as needed. The device controls the access control on holidays according to the holiday settings.



When the device is on the initial interface, press button > **Access Control** > **Holidays** to enter the **Holidays** interface.

10.3.1 Adding Holiday



Press **Add Holiday**.

Press **Date**.

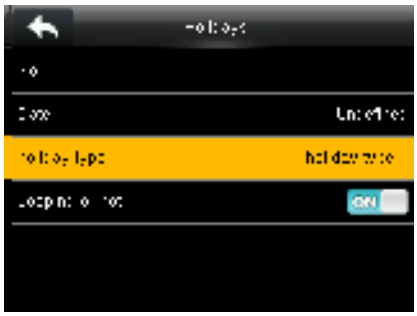
Set date for the added holiday, press **[Confirm(OK)]** to save and exit.

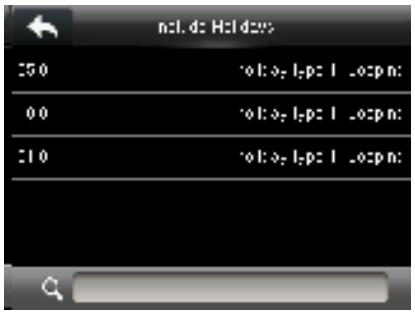
The holiday parameters are set as follows:

- **No.:** The device automatically assigns a number to a holiday. You can also select **[No.]** and enter the No. interface. Enter a holiday No. as needed and press **[OK]** to save the settings and return to the **Holidays** interface.

Note: A holiday No. ranges from 1 to 24.

- **Date:** Set the date of a holiday. Press ▲/▼ to set the date. Then, press **[Confirm(OK)]** to save the settings and return to the **Holidays** interface.
- **Holiday Type:** Select access time schedule for holiday. Time period for holiday type 1/2/3 can be edited in time rule. For details about editing methods, please refer to 10.2 Time Rule Settings.





- **Looping or not:** The default value of Looping or not is **[ON]**. You can press button to switch between **[ON]** and **[OFF]**.

For fixed holidays every year, for example, the New Year's Day is January 1, Looping or not can be

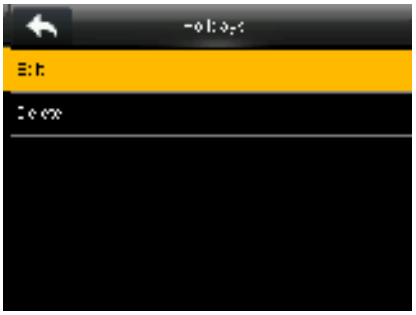
set to **[ON]** for them. For unfixed holidays every year, for example, the Mother's Day is the second Sunday of May, the specific dates are uncertain and Looping or not can be set to **[OFF]** for them.

For example, when the date of a holiday is set to January 1, 2010 and holiday type is set to holiday type 1, the access control on January 1 is conducted according to the time period settings of holiday type 1 rather than the time period settings of Friday.

10.3.2 All Holidays

Press **All Holidays**.

Select a holiday to enter **Holidays** setting interface.

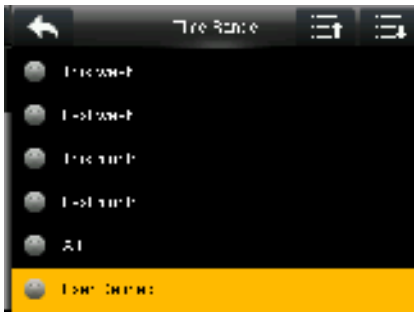


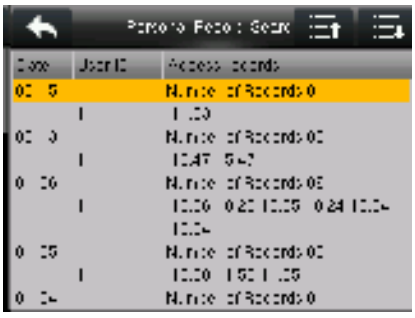
Edit or delete the holiday.

Remarks: The methods of editing or deleting a holiday are the same as those of editing or deleting a user and are not described here.

11. Attendance Search

When users verify successfully, attendance records are saved in the device. This function enables users to check attendance logs.

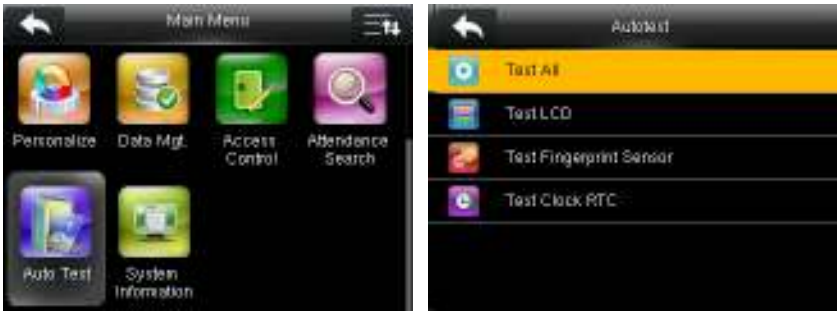




When the device is on the initial interface, press ▦ button > **Attendance Search** > enter **User ID** (if no ID is entered, all user records will be searched) > select **Time Range**, the corresponding attendance logs will be shown.

12. Autotest

To automatically test whether all modules in the device, functions properly or not. It includes the LCD, fingerprint sensor and RTC (Real-Time Clock).



When the device is on the initial interface, press button > **Autotest** to enter the **Autotest** interface.

- **Test All:** It is used to test LCD, fingerprint sensor and RTC. During the test, touch the screen to continue to the next test, or else press button to exit the test.
- **Test LCD:** It is used to test the display effect of LCD screen by displaying full color, pure white, and pure black. During the test, touch the screen to continue to the next test, or else press button to exit the test.
- **Test Fingerprint Sensor:** It is used to test check if the collected fingerprint image is clear or not. When pressing fingerprint on the sensor, the image will be displayed on the screen. Press button to exit the test.
- **Test Clock RTC:** It will test the Real-Time Clock for the proper and accurate functioning of clock by checking the stopwatch. Touch the screen to start counting time, and press it again to stop counting, to see if the stopwatch counts time accurately. Press button to exit the test.

13. System Information

It checks data capacity, device and firmware information.

When the device is on the initial interface, press button > **System Information** to enter the **System Information** interface.

Device Capacity **Device Info** **Firmware Info**

- **Device Capacity:** It displays the number of registered users, administrators, passwords, fingerprints ★, badges ★ and attendance logs, also checks the total storage of users, fingerprints ★, badges ★ and attendance records.
- **Device Info:** It displays the device name, serial number, MAC address, fingerprint algorithm, platform information, MCU version and manufacturer.
- **Firmware Info:** It displays the firmware version, Bio service, push service ★, standalone service, Dev service and system version.

Remark: The display of Device Capacity, Device Info and Firmware Info on the system information interface of different products may vary; the actual product shall prevail.

14. Troubleshooting

- Fingerprint sensor can't read and verify the fingerprint effectively.

  - Check if the fingertip is wet, or the fingerprint sensor is wet or dusty.
  - Clean the fingertip and the fingerprint sensor and try again.
  - If the fingertip is too dry, blow air onto it and try again.

- "Invalid time zone" is displayed after verification.

  - Contact Administrator to check if the user has the privilege to gain access within that time Schedule.

- Failed to gain access after successful verification.

  - Check whether the user privilege is set correctly.
  - Check whether the lock wiring is correct.

- The Tamper Alarm rings.

  - Check if the device and the back plate are fixed together properly; if not, the tamper switch on the back of the device will be triggered and raises an alarm. Warning sign  will be shown on the top right corner on the interface. To get the alarm sound, the speaker should be ON in setting **Access Control** > **Access Control Options** > **Speaker Alarm**.

Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the hybrid biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition devices for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.
2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.
3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.
4. For any dispute involving the human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products for police use, or development tools support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

The law of the People's Republic of China has the following regulations regarding the personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.
2. The personal dignity of citizens of the People's Republic of China is inviolable.
3. The home of citizens of the People's Republic of China is inviolable.
4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The biometric products actually provide adequate protection for your identity under a high security environment.

Environment-Friendly Use Description

Parts Name	Names and Concentration of Toxic and Hazardous Substances or Elements					
	Pb	**Hg**	**Cd**	**Cr6+**	**PBB**	**PBDE**
Power line	X	O	O	O	O	O
PCB components	X	O	O	O	O	O
Structural components	O	O	O	O	O	O
This form is made according to the provisions of SJ/T 11364.						
O：Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in GB/T 26572.						
X： Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in GB/T 26572						
Due to the different models, the products may not include all of the above parts except the host. Please refer to the actual sales of the product.						
 This mark number indicates that the environment friendly use period of the product under normal use is 15 years. Some parts may also have an environment friendly use period, please refer to its mark number.						

ZK Building, Wuhe Road, Gangtou, Bantian, Buji Town,
Longgang District, Shenzhen China 518129

Tel: +86 755-89602345

Fax: +86 755-89602394

www.zkteco.com