FINGERTEC

TA100C TA100TC Q2i/TA200Plus i-Kiosk 100

USER MANUAL

Color Multimedia Fingerprint Time Attendance
& Access Control System

FINGERTEC WORLDWIDE SDN BHD

For enquiries on technical matters, please forward the email to
support@fingertec.com

CONTENTS

IMPORTANT SAFEGUARDS

INSTALLATION LOCATION

Do not install terminal in areas which are exposed to bright sunlight or rain, as the fingerprint readers are not designed to work in those areas. Bright light will interfere with reading of the sensor and fingerprint readers are not waterproof or vandal proof. It is recommended to protect your fingerprint terminal with enclosure.

Go to http://accessory.fingertec.com to view the enclosure and other accessories.

USE OF SENSOR

Do not abuse the fingerprint sensor by scratching the surface, contacting the sensor's surface with heat, pressing hard during placement of fingerprint for verification. Clean the sensor occasionally with cellophane tape to maintain the performance of the sensor.

INTRODUCTION TO TERMINAL

TA100C Series

TA100C TA100TC

A fingerprint verification terminal is designed to record time and attendance by using biometrics trait, fingerprint. It is to replace the conventional punch card system as well as other card systems for time & attendance function. The fingerprint terminals are capable of recognizing the recorded fingerprint templates in seconds and therefore, have been successful in eliminating buddy-punching activity, one of the major problems in human resource management.

TA100C Series terminals are able to store fingerprint templates from 1,500 for TA102C to 2,800 for TA103C depending on the series chosen. It is also able to record from 100,000 transactions with TA102C and 120,000 transactions with TA103C, at any given time and those transactions can be downloaded and cleared up using the management software TCMS V2. TA100C Series also offers TA103C-R, fingerprint time & attendance system with RFID card function, TA100TC- touch screen system with card function and TA100TC-R, color multimedia system with card function.

Q2i/TA200 Plus

The Q2i / TA200 Plus is the revolutionary product of time attendance and door access, designed with colored screen TFT display for vivid color presentation.

Storage capacity of Q2i / TA200 Plus is 3000 fingerprint templates and 120000 transaction logs, and it offers multiple methods of verification which include fingerprint, password and RFID card for user convenience. Q2i / TA200 Plus understands the needs of today's working environment which requires multi-tasking.

Fingerprint enrolment of every user shall be done once and these templates are downloadable into TCMS V2 software for backup and they are transferable to other terminal for verification.

Every time a registered user gets verified at the readers, date and time of the transaction is stored as a transaction log. These logs can be downloaded into TCMS V2 software for reports and further analysis. Download process can be done via TCP/IP connection, USB flash disk (pen drive), RS232 connection, or RS485 connection.

i-Kiosk 100

The i-Kiosk 100 is the revolutionary product of time attendance and door access, designed with colored screen TFT display for vivid color presentation.

Storage capacity of i-Kiosk 100 is 3000 fingerprint templates and 120000 transaction logs, and it offers multiple methods of verification which include fingerprint, password and RFID card for user convenience. i-Kiosk 100 understands the needs of today's working environment which requires multi-tasking.

Fingerprint enrollment of every user shall be done once and these templates are downloadable into software for backup and they are transferable to other readers for verification.

Every time a registered user gets verified at the terminal, date and time of the transaction is stored as a transaction log. These logs can be downloaded into software for reports and further analysis. Download process can be done via TCP/IP connection, USB flash disk (pen drive), RS232 connection, or RS485 connection.

SPECIFICATION




Model	TA100C	TA100TC	Q2i/TA200 Plus	i-Kiosk 100
Display area (inch)	3.0 TFT screen		3.5 TFT screen	
Color resolution	65k			
Surface finishing	Acrylonitrile Butadiene Styrene (ABS)			
Fp Storage	1500		3000	
Transaction log	50000		120000	
Connection available	TCP/IP, RS232, RS485, USB flash disk, USB host-client		TCP/IP, RS232, RS485, USB flash disk, USB host-client, Wiegand 26-bits input/output	
Card terminal	RFID card terminal (default)			
Sensor	Optical scanner			
Terminal default language ***Optional language**	English Arabic / Indonesian / Spanish / Chinese Simplified / Chinese Traditional / French /German / Malay / Russian / Farsi / Portuguese / Thai / Italian / Vietnamese / Turkish			

COMPLETE PACKAGE

TA100C Series

1 • Fingerprint Terminal
2 • Software & Video Guide CD
3 • USB Extension
4 • A Packet of Bolts
5 • DC 5V Power Adapter
6 • Siren Cable
7 • Screwdriver
8 • Cable Protector

Q2i/TA200 Plus

1 • Fingerprint Terminal
2 • Software & Video Guide CD
3 • USB Extension
4 • A Packet of Bolts
5 • DC 12V Power Adapter
6 • TCP/IP Connector Jack
7 • Screwdriver
8 • RFID Card (5pcs)
9 • Wire Connector

i-Kiosk 100

1 • Fingerprint Terminal
2 • Software & Video Guide CD
3 • USB Extension
4 • A Packet of Bolts
5 • DC 12V Power Adapter
6 • TCP/IP Connector Jack
7 • Screwdriver
8 • RFID Card (5pcs)
9 • Wire Connector

MATERIALS PROVIDED

- Quick Start Guide
- Hardware User Manual
- Software User Manual
- Video Guide for Software and Hardware
- Sample of Enrollment Form

NOTE

USB port for data transfer

USB PORT

To upload/download user information, password, fingerprints and transaction logs via USB flash disk.

BASIC FEATURES

TA100C Series | TA100C

L.E.D DISPLAY

The L.E.D display has two lights.
Green - The terminal is in standby mode or to indicate that user has been successfully verified.
Red - To indicate that user verification has failed.

COLOR LCD

Screen that displays instruction and status of terminal.

SPEAKER

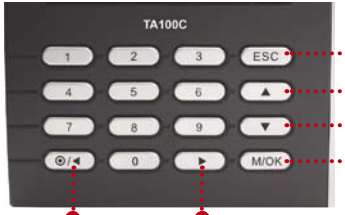
To prompt user with result of verification and information.

OPTICAL SCANNER

For user to place finger for enrollment or verification.

KEYPADS

Keys from 0-9, alphabets Power on/off button, Escape/Cancel button, Menu/Enter button, backspace button, left ◀ button, right ▶ button.



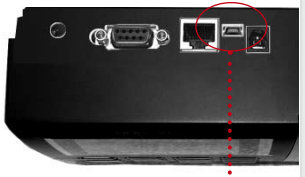
L.E.D DISPLAY
The L.E.D display has two lights.
Green - The terminal is in standby mode or to indicate that user has been successfully verified.
Red - To indicate that user verification has failed.

COLOR LCD
Screen that displays instruction and status of terminal.

SPEAKER
To prompt user with result of verification and information.

OPTICAL SCANNER
For user to place finger for enrollment or verification.

NOTE



USB port for data transfer

USB PORT
To upload/download user information, password, fingerprints and transaction logs via USB flash disk.

KEYPADS
Keys from 0-9, alphabets Power on/off button, Escape/Cancel button, Menu/Enter button, backspace button, left ◄ button, right ► button.

Q2i/TA200 Plus

L.E.D DISPLAY
The L.E.D display has two lights.
Green - The reader is in standby mode or to indicate that user has been successfully verified.
Red - To indicate that user verification has failed.

COLOR LCD
Screen that displays instruction and status of terminal.

FUNCTION KEYS
Shortcut keys to enter specific command to terminal.

OPTICAL SCANNER
For user to place finger for enrollment or verification.

NAVIGATION KEYS
To navigate and to input command to terminal.

SPEAKER
To prompt user with result of verification and information.

CARD
RFID card induction area.

NOTE

USB PORT
To upload/download users information, password, fingerprints and transaction logs via USB flash disk.

USB port for data transfer

KEYPADS
Keys from 0-9, alphabets Power on/off button, Escape/Cancel button, Menu/Enter button, backspace button, asterisk (*) button, hash (#) button.

Escape
Menu/Enter
Backspace
Power On/Off
Asterisk
Hash

NOTE

USB port for data transfer

USB PORT
To upload/download users information, password, fingerprints and transaction logs via USB flash disk.

COLOR LCD
Screen that displays instruction and status of terminal.

L.E.D DISPLAY
The L.E.D display has two lights.
Green - The terminal is in standby mode or to indicate that user has been successfully verified.
Red - To indicate that user verification has failed.

NAVIGATION KEYS
To navigate and to input command to reader.

FUNCTION KEYS
Shortcut keys to enter specific command to reader.

SPEAKER
To prompt user with result of verification and information.

RFID CARD
RFID card induction area.

OPTICAL SCANNER
For user to place finger for enrollment or verification.

KEYPADS
Keys from 0-9, alphabets Power on/off button, Escape/Cancel button, Menu/Enter button, backspace button, asterisk (*) button, hash (#) button.

- Asterisk | Hash
- Menu/Enter | Escape
- Backspace | Power On/Of

USING THE FINGERPRINT TERMINAL

This chapter will guide on how to use the fingerprint terminal effectively. To get a good reading every time, initial fingerprint enrollment must be done properly.

The fingerprint terminal provides 4 types of enrollment method:

1 **FINGERPRINT ENROLLMENT**
User enrolls his fingerprint template into a terminal and the template will be used for future verifications.

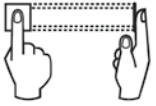
2 **PASSWORD ENROLLMENT**
For user who has difficulty to enroll fingerprint due to poor fingerprint quality, enrollment of password is recommended. Password enrollment is also suitable for visitors and temporary workers.

3 **FINGERPRINT AND PASSWORD ENROLLMENT**
Under this option, a user can enroll both fingerprint and password at the same time. The user can either use fingerprint or password to report attendance or to gain access.

4 **RFID CARD ENROLLMENT**
Please refer to Chapter 3 for RFID Card Function.

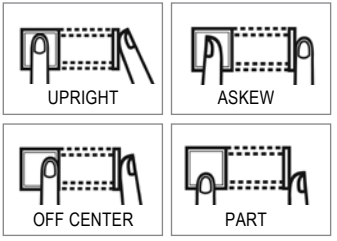
TIPS FOR BEST FINGERPRINT ENROLLMENT

WHAT YOU SHOULD DO



Place finger flat on the fingerprint sensor. Make sure the finger's midpoint is placed at the center of the fingerprint sensor.

WHAT YOU SHOULD NOT DO



1 **USE INDEX FINGER**
Index finger is smaller than thumb and it can be comfortably placed on the sensor. The use of thumb is not recommended because the center points might not be placed properly on the sensor, hence cannot be read by the sensor.

2 **MAKE SURE THE FINGER IS NOT WET, TOO DRY, INJURED OR DIRTY**
The finger needs to be slightly moist to enable the sensor to read the minutiae points on the fingerprint.

3 **PLACE THE CENTER POINTS OF YOUR FINGER AT THE CENTER OF THE SENSOR**
The center points of a finger is an area where there is a swirl and the center points must be properly placed on the sensor during enrollment.

4 **DON'T PRESS HARD AT THE SENSOR, JUST PLACE YOUR FINGER ON THE SENSOR**
The sensor is reading minutiae points of your finger and placing a finger properly on the sensor will prompt the sensor to read those points. Pressing your finger hard on the sensor is not necessary.

5 **DON'T DO ENROLLMENT UNDER BRIGHT LIGHT OR DIRECT SUNLIGHT**
It is important to note that bright light or sunlight could interfere with reading of the sensor. Avoid placing the terminal under direct sunlight or bright light to avoid difficulty in enrollment and future verification.

INITIAL SET UP OF THE FINGERPRINT TERMINAL

DATE / TIME ADJUSTMENT

When first installing a fingerprint terminal, it is important to set the correct date and time.

Follow the steps shown to access the Date/Time adjustment menu:

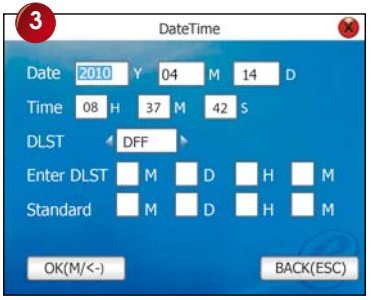
1

Press M /↵ once.

2

Press ▶ 3 times to go to Date/Time.
Press OK once.

3



Press ▼ to go to the desired column.
Enter value using keypads.
Press OK once to confirm setting.

DLST stands for Daylight Saving Time. Please enter the date and time in the given column to use this feature.

- **DLST**
  Enter date and time for daylight saving starts.
- **Standard**
  Enter date and time to return to standard.

NOTE

Not applicable to TA100C.

4

Press OK once to save setting.

5

Press Esc twice to return to the main menu.

ENROLLMENT

To assist in fingerprint enrollment, we have designed a form for the administrator to use to keep track of the enrollment details or you can design your own form to suit to your company's requirements.

User Enrollment Template Form for Terminal

Terminal ID: _____

No.	User ID	Employee No.	Name	Department	IC No.	No. of Fingers Enrolled	Date Registered	Note	Signature

SAMPLE

ENROLLMENT OF SUPERVISOR / ADMINISTRATOR

Once the fingerprint terminal is switched on, a display on the screen will appear. Enroll a supervisor or an administrator, who is the in-charge person to administer the fingerprint templates and the transaction data in the terminal. Choose trustworthy people for this particular role.

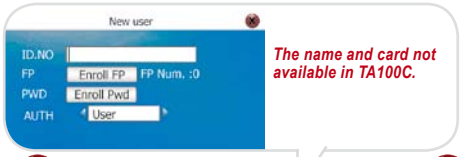
1

Press M /↵ once.

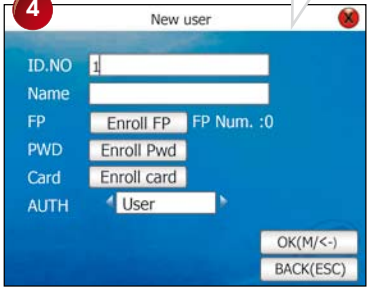
2

Press OK once.

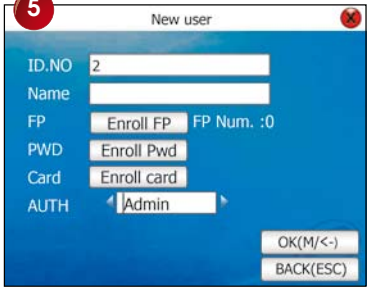
Press **OK** once. *The Access icon only available in i-Kiosk 100 and Q2i.*



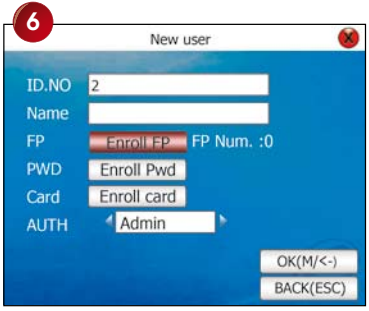
The name and card not available in TA100C.



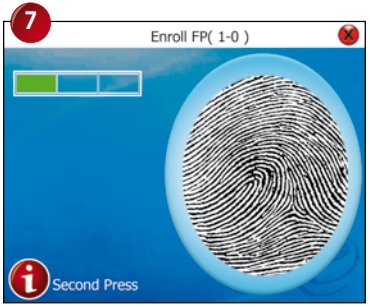
Assign user ID of the administrator.



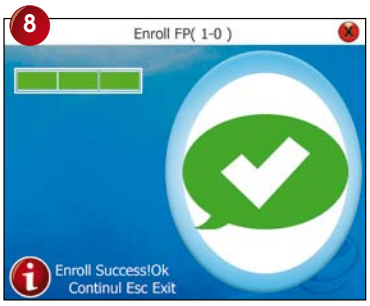
Press ▼ 5 times.
Press ▶ once to select Admin.



Press ▼ 2 times to Enroll FP and press **OK**.



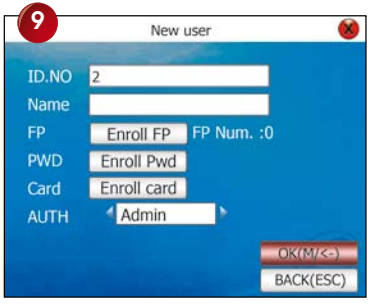
Place center point of fingerprint properly on the scanner. Place finger 3 times during enrollment. Read page 12 for tips on fingerprint scanning technique.



Press **OK** once to save enrollment.
Press **Esc** once to end enrollment.

ENROLLMENT OF NORMAL USER

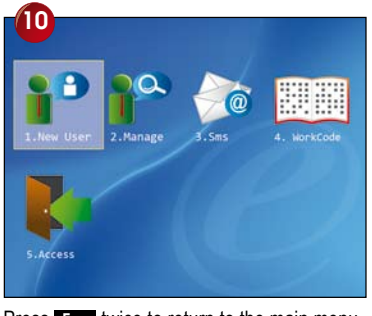
A normal user is only allowed to use terminal for identity verification, and he does not have any other authorities to access the system. To add a normal user, follow the steps shown.



Press **OK** once to save.

Press **M /↵** once.

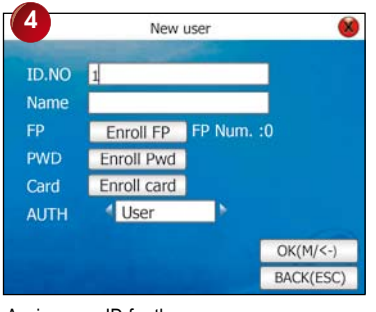
Press **OK** once.



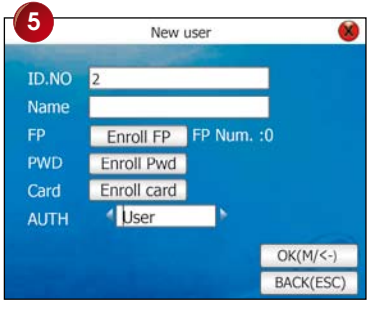
Press **Esc** twice to return to the main menu.

The Access icon only available in i-Kiosk 100 and Q2i.

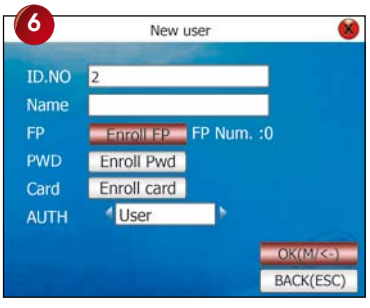
Press **OK** once.



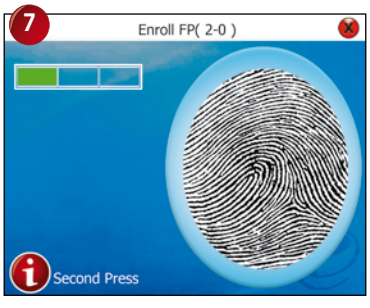
Assign user ID for the user.



Press ▼ 5 to AUTH. Press ▶ once to select user.

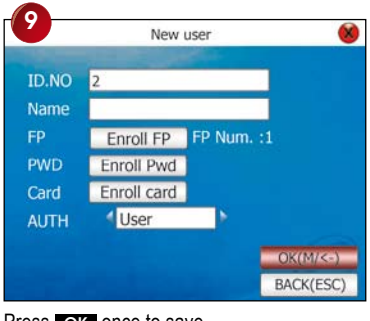


Press ▲ 3 times to Enroll FP and press OK.

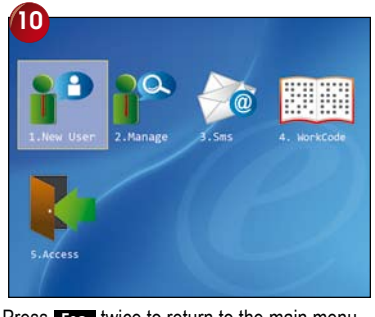


Place center point of fingerprint properly on the scanner. Place finger 3 times during enrollment.

Press OK once to save enrollment.
Press Esc once to end enrollment.



Press OK once to save.



Press Esc twice to return to the main menu.

To enroll more users, repeat the steps above.

FINGERPRINT VERIFICATION

Terminal supports 2 types of fingerprint verification method. User can choose either method to verify his fingerprint at the terminal. 2 types of fingerprint verification methods are:

- 1 to Many (1:N) fingerprint matching

Place the enrolled finger properly on the fingerprint sensor.

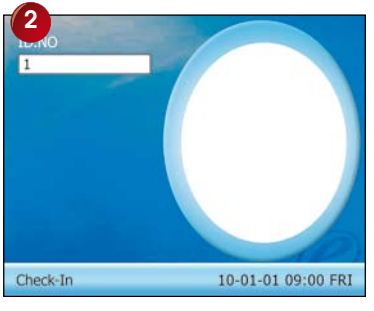
Wait a second before removing the finger from the fingerprint sensor.

The terminal verifies user, displays the ID and prompts “Verified”

If verification failed, the terminal prompts, “Try again please!”

- 1 to 1 (1:1) fingerprint matching

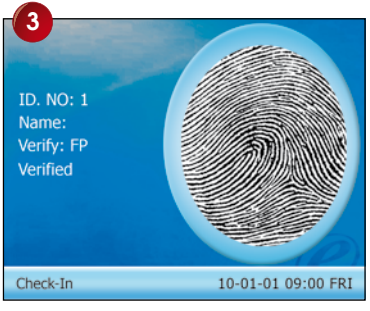
Enter the user ID using keypad.



Place the enrolled finger properly on the fingerprint sensor.

PASSWORD ENROLLMENT

For user who cannot enroll his fingerprint, he can choose to use passwords. Follow the steps below:



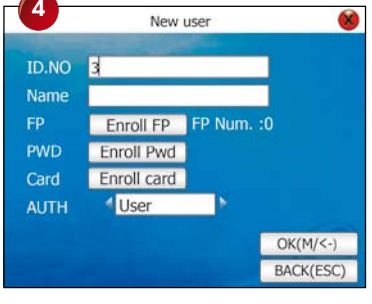
The terminal verifies user, displays the ID and prompts “Verified”.

If verification failed, the terminal prompts, “Try again please!”

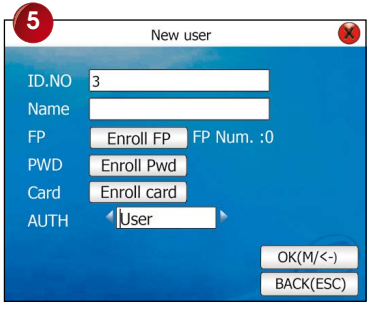
Press M /↵ once.

Press OK once.

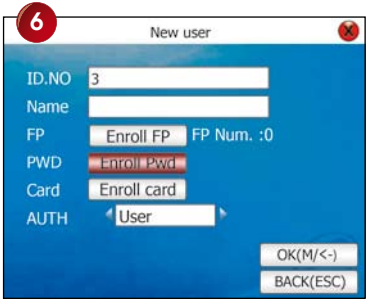
Press OK once.



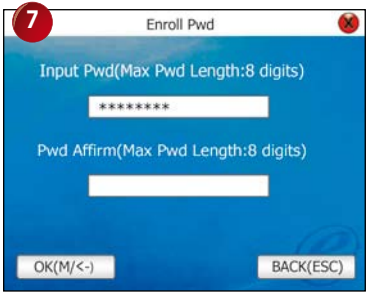
Assign user ID using keypads, for example 3.



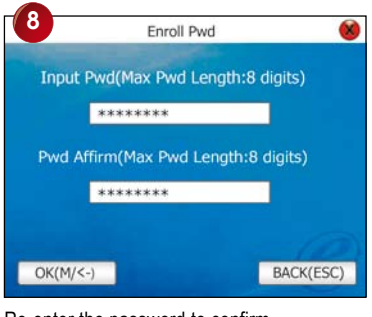
Press ▼ 5 times.
Press ▶ once to select user.



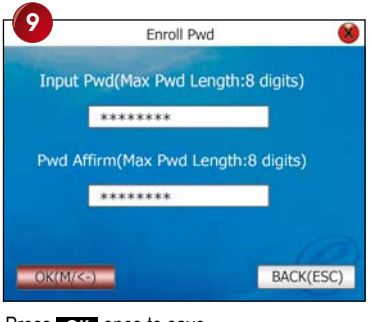
Press ▲ twice to Enroll Pwd and press OK.



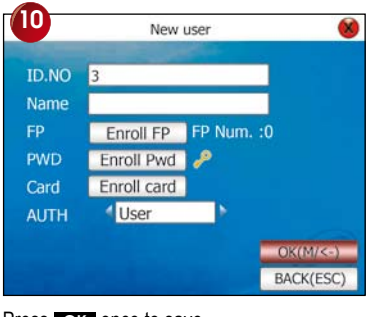
Enter password maximum 8 digits.
Press ▼ once.



Re-enter the password to confirm.



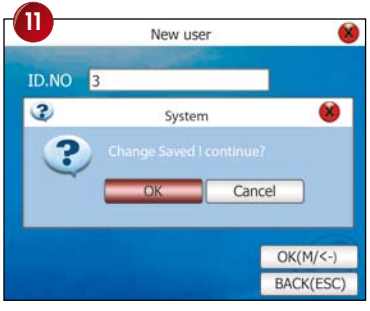
Press OK once to save.



Press OK once to save.

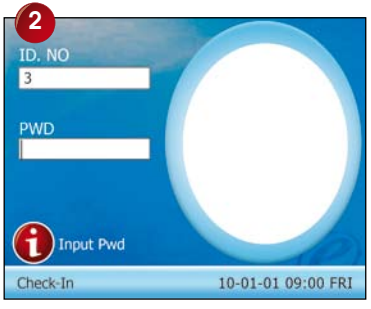
PASSWORD VERIFICATION

User with password enrollment can always use password to report attendance or gain access from the terminals.

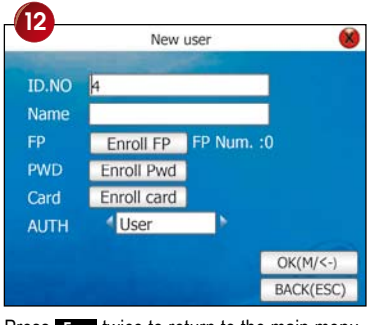


Press **OK** once to save.

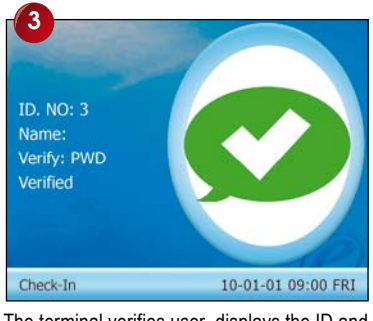
Enter the user and press **OK** .



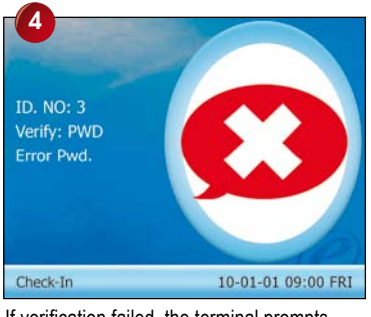
Enter password and press **OK** .



Press **Esc** twice to return to the main menu.



The terminal verifies user, displays the ID and prompts “Verified”.



If verification failed, the terminal prompts, “Try again please!”.

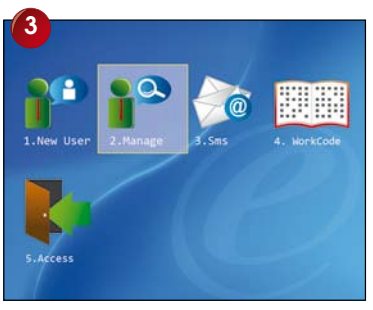
DELETING USERS

The system also allows deletion of user from the system. This is important as employees come and go. Therefore, for those who had left the company, their fingerprint templates or records must be deleted from the system to avoid any misuse of the system. Only an administrator or a supervisor has the rights to delete user.

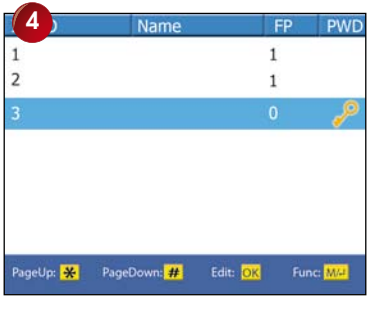
Follow the steps shown to delete users.

Press M /↵ once.

Press OK once.



Press ▶ once to go to Manage and press OK.



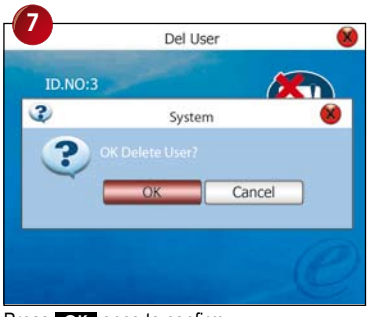
Press ▼ to choose user ID to delete.
Press M /↵ once.

Press ▼ 3 times to go to Del User and press OK .

NOTE

Remember to select the correct User ID for deletion.

Press **OK** once to delete user.



Press **OK** once to confirm.

Press **Esc** 3 times to return to the main menu.

The reader supports enrollment of RFID Card. User can report time attendance and gain access by using RFID card. At the same time, users with fingerprint or password enrollment can add RFID card as well.

Each RFID card has a unique ID. During enrollment this Card ID will be read from the RFID card and stored in the reader. During verification the reader will match the ID in the card to the ID stored in the reader.

RFID CARD

Each RFID card user must register his RFID card to the reader.

To enroll user with RFID card, follow the steps shown:

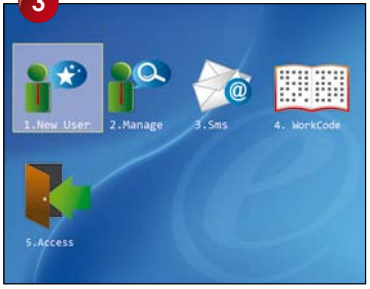
1

Press M /↵ once.

2

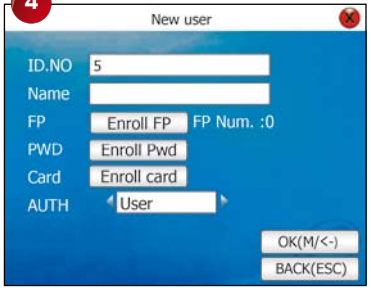
Press OK once.

3

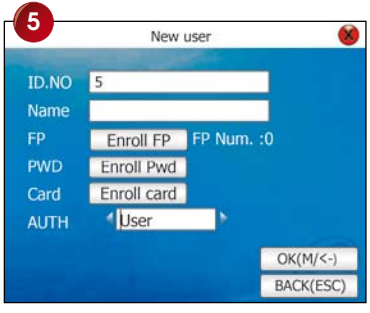


Press OK once.

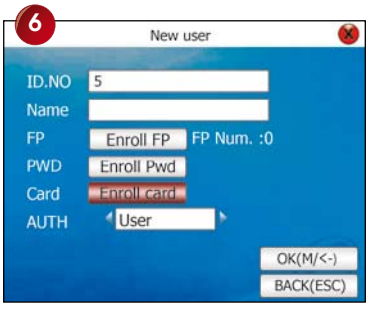
4



Assign user for example 5.

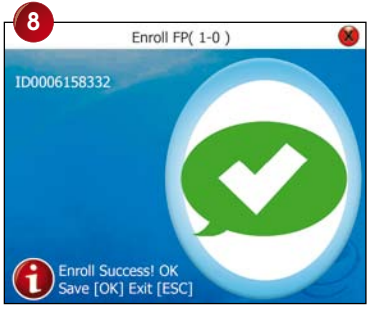


Press ▼ 5 times.
Press ► once to select user.

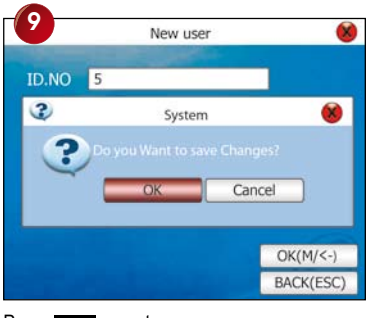


Press ▲ once to Enroll Card and press OK.

Wave RFID card at the induction area to read the card.



The Card ID is captured and displayed on the screen. Press OK once to save.

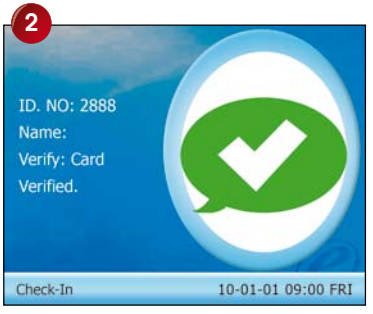


Press OK once to save.
Press Esc twice to return to the main menu.

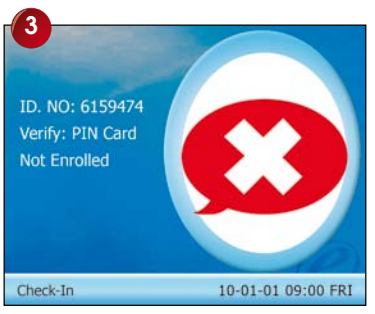
VERIFICATION WITH RFID CARD

RFID card user can do verifications at the reader by using the following combinations:
To enable this operation, configure option “Card Only” in Advance Option to “Yes”

Place RFID card at the induction area.



The Card ID and the User ID are shown on the screen, and the reader prompts, “Thank you”



If verification failed, the screen shows “Not Enrolled” and prompts, “Invalid ID”

BRIEF INTRODUCTION TO ACCESS OPTIONS

Access option function setting is the settings of user's accessibility to certain doors. It is known as Time Zone. A combination of time zones is known as Group Time Zone. There are a total of 50 time zones available in the reader. Below are some examples of Time Zone configurations and combinations of Time Zones.

TIME ZONE 1

CONSTANT ACCESS TIME FOR A PERIOD OF ONE WEEK.

Table 1.1 is showing the time zone 1 detailed schedule where users are only allowed access from 9am to 6pm from Monday to Sunday.

Time zone	1
SUN	09:00-18:00
MON	09:00-18:00
TUE	09:00-18:00
WED	09:00-18:00
THU	09:00-18:00
FRI	09:00-18:00
SAT	09:00-18:00

Table 1.1 Time Zone 1

TIME ZONE 2

VARIATION IN ACCESS FOR A PERIOD OF ONE WEEK.

Table 1.2 is showing the time zone 2 where users are allowed to access from 8am to 12pm from Monday to Friday but denied any access on the weekends.

TIME ZONE 3

VARIATION IN ACCESS FOR A PERIOD OF ONE WEEK.

Table 1.2 also is showing the time zone 3 where users are allowed to access from 2pm to 6pm from Monday to Friday but denied any access on the weekends.

The Time Zone 2 and Time Zone 3 belongs to the same group of employee, therefore they can be grouped together in Group Time Zone, for example Group Time Zone 1.

Time zone	2	3
SUN	23:59-00:00	23:59-00:00
MON	08:00-12:00	14:00-18:00
TUE	08:00-12:00	14:00-18:00
WED	08:00-12:00	14:00-18:00
THU	08:00-12:00	14:00-18:00
FRI	08:00-12:00	14:00-18:00
SAT	23:59-00:00	23:59-00:00

Table 1.2 Time Zones 2 & 3

There are a total of 5 Group Time Zones available for use.

Every new registered user belongs to Time Zone 1. Default grouping combination is Group 1 and default Group Time Zone 1.

Group time zone	Time zones		
1	2	3	
2			
3			
4			
5			

Table 1.3 Group Time Zones

Under a condition where Group 1 and Time Zone 1 are in factory default status, new registered user defaults in unlocking status. If the grouping of that user does not include in grouping combination setting, then user can only record time attendance but cannot unlock the door.

Access option has 6 main functions

1. **TIME ZONE SETTING**
   To define time zone 1 to 50.
2. **HOLIDAY SETTINGS**
   To define time zone for holiday.
3. **GROUP TIME ZONES SETTINGS**
   To define group time zones, a group can support up to 3 different time zones.
4. **UNLOCK COMBINATION SETTINGS**
   To define different time zone combinations, and each combination is composed of different groups.
5. **ACCESS CONTROL PARAMETERS**
   To define lock/unlock parameters
6. **DURESS ALARM PARAMETERS**
   To define duress alarm parameters.

FUNCTION DESCRIPTION DEFINITION OF TIME ZONE

TIME ZONE
Range of time specified for access options. The system can define a maximum of 50 time zones. Each user can set a maximum of 3 times zones.

TIME REGION
A certain period of time with a format of HH: MM–HH:MM, operates in 24-hr format and accurate to the minutes. For each time zones, 7 time regions can be set.

ALL DAY ACCESS
00:00 to 23:59, reader allows user to access anytime in a day.

FORBIDDEN TIME ZONE
23:59 to 00:00, reader blocks users to access anytime in a day.

All new enrolled users are automatically assigned to Time Zone 1. It is recommended not to change any settings in Time Zone 1.

For example, Users are allowed to access from 8:30am – 6:00pm during work time from Monday to Friday. Saturday and Sunday are off day and users are not allowed for any entry. Follow the steps to configure time zones.

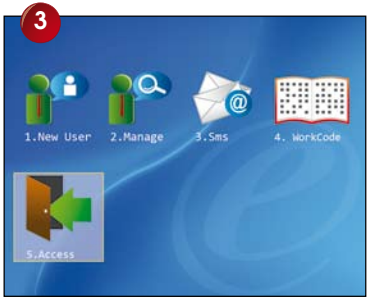
1

Press M /↵ once.

2

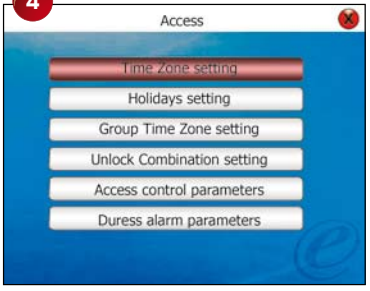
Press OK once.

3



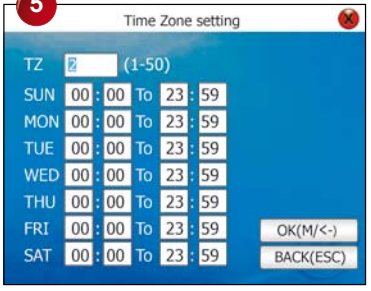
Press ▼ once to choose Access and press OK .

4



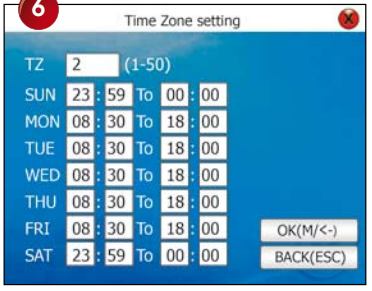
Press OK once.

5

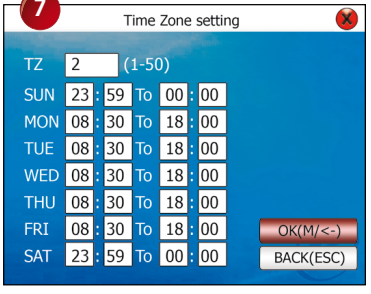


Enter time zone (vary from 1 to 50)

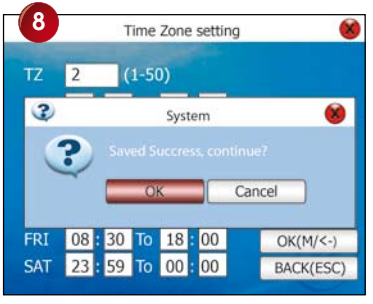
6



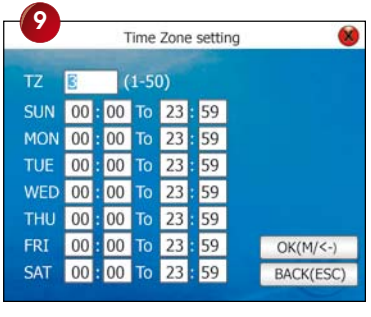
Press ▼ to go to the desired column.
Enter time into the desired day.



Press **OK** once to save.



Press **OK** once to confirm.



Press **Esc** 4 times to return to the main menu.

The configured time zone is saved and reader is allowed to set the next time zone. A total of 50 time zone is available and each user can use up to 3 time zones.

After time zones settings are configured, these time zones shall be included in the Group Time Zones for the configuration to take effects.

DEFINITION OF GROUPING FUNCTION

Grouping function can segregate users into group and combine different groups into different unlocking combinations. The function provides convenience to grouping management of Access Options. The grouping function can combine as many unlocking combinations as possible from the five groups. New registered user default belongs to Group 1 but the users in Group 1 can be relocated into another group.

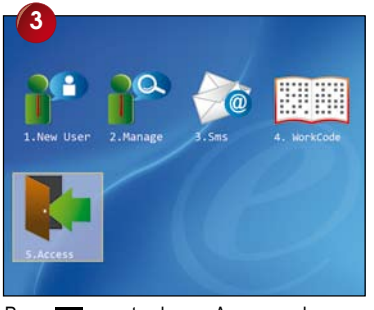
For example,

Here are 3 time zones, TZ1, TZ2 and TZ3. And now all 3 time zones group into group time zone 2.

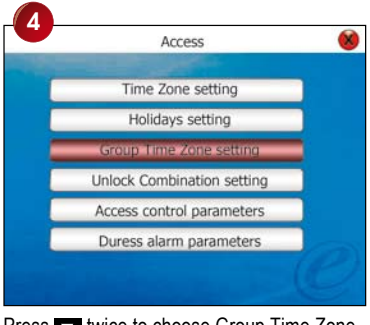
Follow the steps to configure group time zone,

Press M /↵ once.

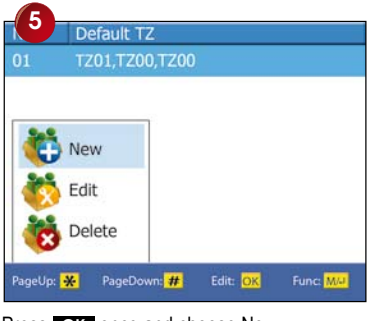
Press OK once.



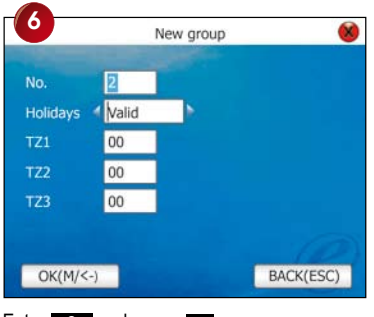
Press ▼ once to choose Access and press OK .



Press ▼ twice to choose Group Time Zone settings and press OK once.

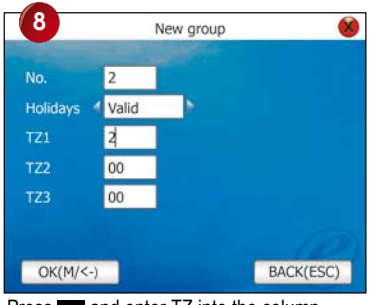


Press OK once and choose New.

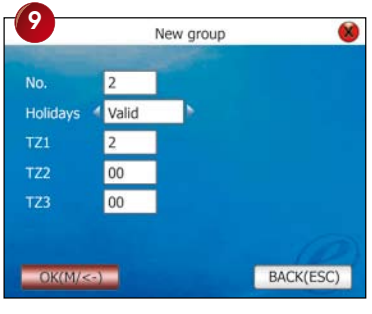


Enter 2 and press ▼ .

Press ▶ to choose Holiday as Valid.



Press ▼ and enter TZ into the column.
Repeat to press ▼ to next column for next the time zone.



Move to **OK** and press **OK** to save setting.

Press **OK** once to confirm.
Press **Esc** 4 times to return to main menu.

DEFINITION OF USER ACCESS SETTINGS

User Access Options is to process correlative setting according to user's requirements.

ENTER ACCESS OPTIONS MENU TO CHECK USER'S ACCESS OPTIONS STATUS.

User Access Options include user grouping setting, use group time zone and user time zone.

GROUPING divides registered users into several groups making them managable.

USE GROUP TIME ZONE is whether the user uses default time zone of the belonged group.

USER TIME ZONE is for user to set user's unlocking time, and select number of time zone already being set.

For example,

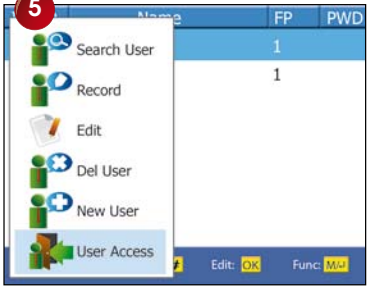
User ID 00001 is assigned to Group Time Zone 2. Follow the steps to assign user into group time zone.

Press M /↵ once.

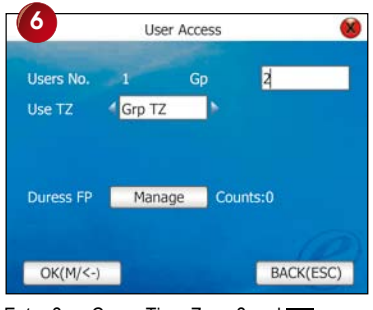
Press OK once.

Press ▶ once to choose Manage and press OK .

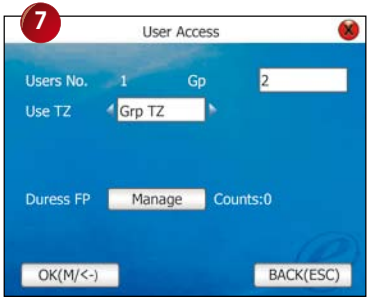
Press ▼ to select the user ID 00001 and press M /↵ button.



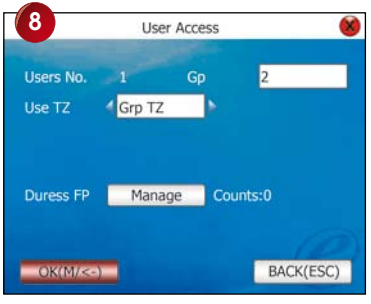
Press ▼ to choose User Access and press OK .



Enter 2 as Group Time Zone 2 and ▼ .



Press ▶ to choose Grp TZ.



Press ▼ twice and press OK .

Press Esc 3 times to return to the main menu.

DEFINITION OF HOLIDAY SETTINGS

User access time can control reader during holiday. The access time zone might vary during holiday and the time zone for holiday can be preset.

During configuration of the time zone for holiday, the time range for the time zone is time to block users to gain access.

Example,

Users are allowed to access during holiday from 8:00 to 12:00. Therefore, you must configure in time zone as below

13:00 – 23:59

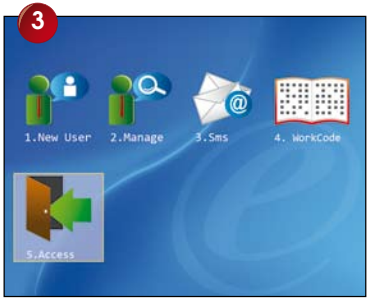
This is the time range to block users to gain access from the reader. Please kindly take note, time zone for holiday has a different concept than the normal time zone.

EXAMPLE OF SETTINGS

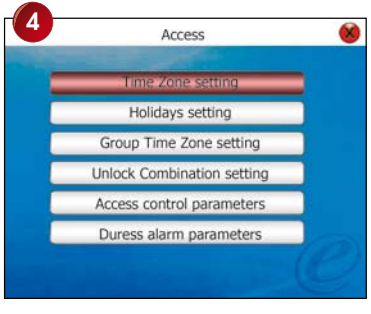
Select a public holiday for example 1st May. The reader is set to disallow any access during holiday. Follow the steps shown to configure holiday settings.

Press M /↵ once.

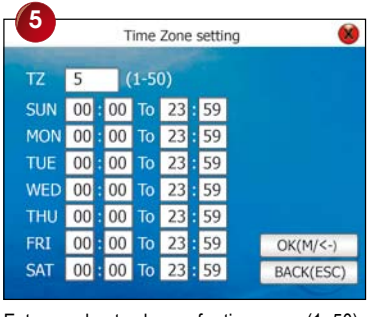
Press OK once.



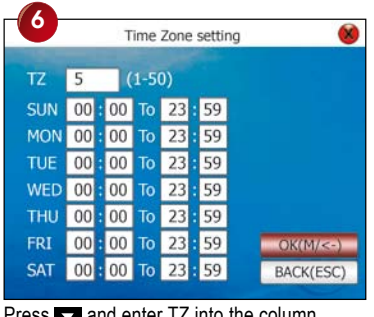
Press ▼ once to select Access.



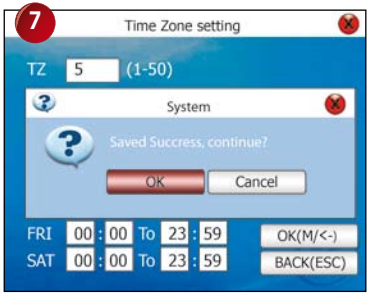
Press OK once to choose Time Zone settings.



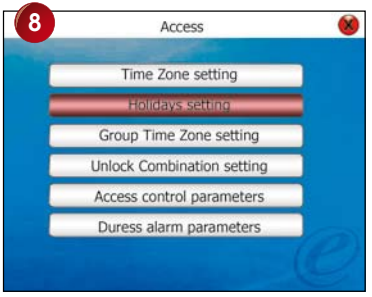
Enter a value to choose for time zone (1~50), for example 5. Press OK once.



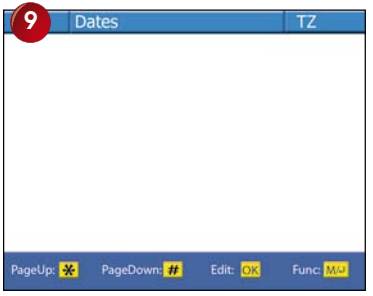
Press ▼ and enter TZ into the column. Repeat to press ▼ to go to the next column for the next time range.



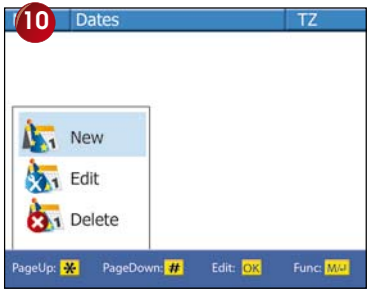
Press **OK** once to save settings.
Press **Esc** once to return to the previous page.



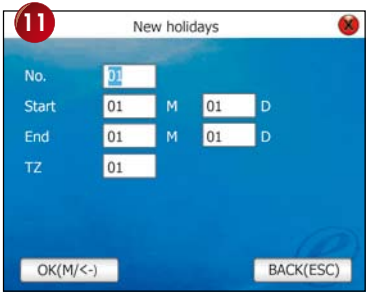
Press ▼ to choose Holiday settings.



Press **M /↵** once.

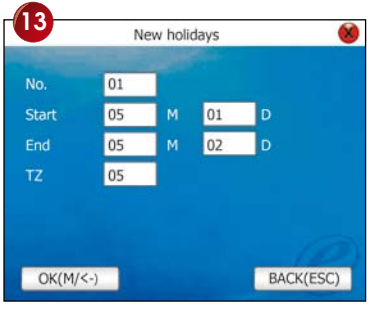


Press **OK** once to choose NEW.



Enter number of holiday, for example 1.

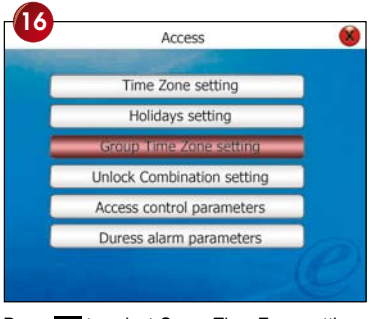
Press ▼ to enter date range of holiday.



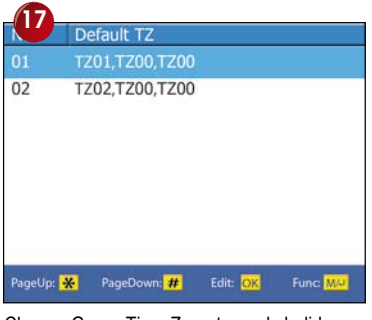
Preset time zone for holiday in Time Zone settings, for example 5.

Move to **OK** and press **OK** to save settings.

Press **Esc** to return to the previous page.



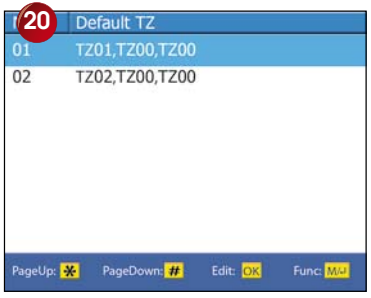
Press ▼ to select Group Time Zone setting and press **OK** .



Choose Group Time Zone to apply holiday, for example 1. Press **OK** once.

Under holiday column, press ► to change to Invalid.

Press **OK** once.



Press **Esc** 4 times to return to the main menu.

USER UNLOCK COMBINATION SETTINGS

In order to allow user to use different time zone groups, please set the followings accordingly:

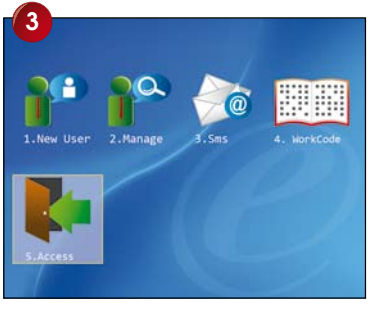
- Comb1 value set to 1
- Comb2 value set to 2
- Comb3 value set to 3
- Comb4 value set to 4
- Comb5 value set to 5

ACCESS CONTROL PARAMETERS

This page allows administrator to configure accessibility of readers. There are total 8 options ready for configuration. Follow the steps to enter to access control parameters.

Press **M /↵** once.

Press **OK** once.



Press ▼ once choose for Access.

Press ▼ 4 times to choose Access Control Parameters and press OK.

Options available and their functions

1. **LOCK (1-10S)**
   To adjust the unlocking time after verification.
2. **DSEN. DELAY (1-99S)**
   To delay door sensor from triggering alarm system when door is not closing. This function only works when a door sensor is attached to the reader.
3. **DSEN MODE**
   To choose the type of door sensor attached to the reader. There are NO (normally opened) and NC (normally closed) available. Choose NONE if no door sensor is attached.
4. **ALARM DELAY (1-99S)**
   To delay the reader from triggering alarm system.
5. **ALARM COUNT (1-9 TIMES)**
   To adjust the maximum verification failures of users. When the maximum is reached, reader will trigger alarm system.
6. **CLOSE TZ**
   Door is always locked during the predefined time period, so users cannot gain access after verification.
7. **OPEN TZ**
   Door is always unlocked during the predefined time period, so users do not need to verify their identities but can gain access.
8. **VALID HOLIDAYS**
   Choose Valid to enable the holiday settings. Choose Invalid to disable the holiday settings.

DURESS ALARM PARAMETERS

The fingerprint reader will trigger alarm system after a duress fingerprint is verified successfully. It is advisable

1 to use different fingers to do daily clocking mechanism and to trigger duress alarm

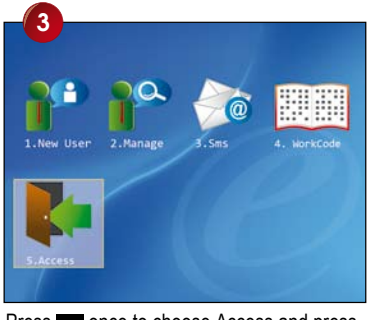
OR

2 to use different verification to do daily clocking mechanism and to trigger duress alarm.

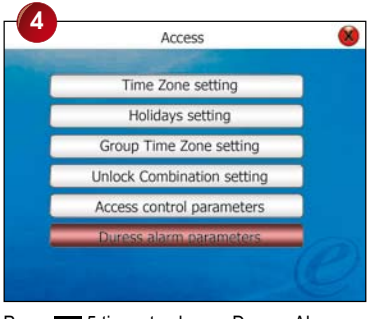
Follow the steps shown to configure duress alarm parameters:

Press M /↵ once.

Press OK once.



Press ▼ once to choose Access and press OK .



Press ▼ 5 times to choose Duress Alarm Parameters and press OK .

Options available and their functions

If users would like to use the same fingerprint for daily clocking and to trigger duress alarm, administrator must enable either one of the following functions.

1. **HELP KEY**
   Select **[Yes]** to enable. Hold the ▼ for 3 second followed by the fingerprint verification. Successful verification will trigger alarm system.
2. **1:1 TRIG**
   Select **[Yes]** to enable. Enter user ID followed by fingerprint verification to trigger alarm system. During daily clocking mechanism, all users use 1:N fingerprint verification. All 1:1 fingerprint verification process will trigger alarm system.
3. **1:N TRIG**
   Select **[Yes]** to enable. Place finger on scanner for fingerprint verification to trigger alarm system. During daily clocking mechanism, all users use 1:1 fingerprint verification. All 1:N fingerprint verification process will trigger alarm system.
4. **PWD TRIG**
   Select **[Yes]** to enable. Enter user ID and password for verification to trigger alarm system. During daily clocking mechanism, all users use fingerprint verification. Any password verification process will trigger alarm system.
5. **ALARM DELAY**
   To delay the reader to trigger alarm system after verification.

If user would like to enroll another finger to trigger duress alarm, please disable all of the above option.

Please see the next page to learn to enroll/define a finger to trigger duress alarm.

TO DEFINE DURESS FINGERPRINT

If users would like to use different fingers for daily clocking mechanism and to trigger duress alarm, users must enroll with more than 1 fingerprint (2 or above).

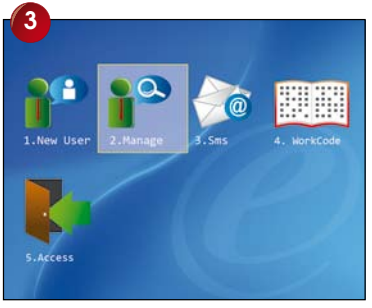
Example, index finger for daily clocking activities and thumb as duress finger.

When duress finger is used for verification, it will trigger alarm system as well. Administrator does not need to enable any of the verification methods in Duress Alarm Parameters.

Follow the steps shown to define duress finger.

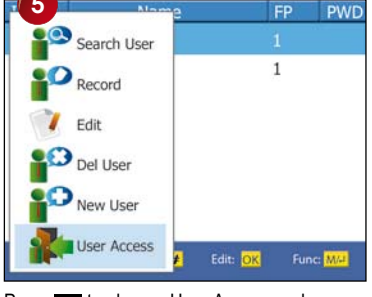
Press M /↵ once.

Press OK once.

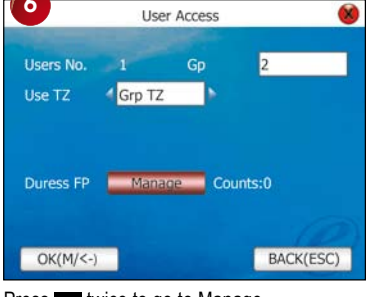


Press ▶ to choose Manage and press OK .

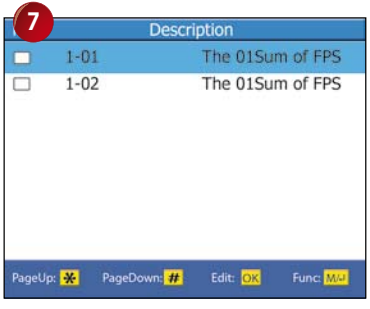
Press ▼ to choose the user ID and press M /↵ .



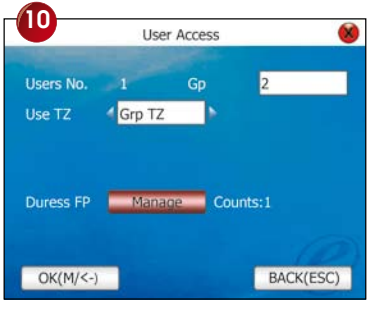
Press ▼ to choose User Access and press OK .



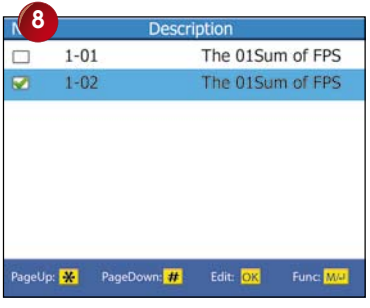
Press ▼ twice to go to Manage.



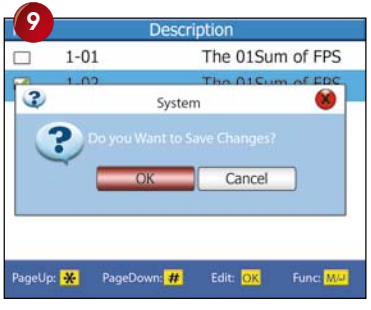
Press **OK** once to select the enrolled fingerprint as duress finger.



Move to **OK** and press **OK** once to save settings. Press **Esc** 3 times to return to the main menu.



Press ▼ to choose the fingerprint to use as duress finger, and press **OK** . User ID–01: first enrolled fingerprint. User ID–02: second enrolled fingerprint.



Press **Esc** once to end process.
Press **OK** once.

USB PEN DRIVE

If terminal is installed far from a PC or encountering cabling problem that is causing disruption of data download, user can transfer data via USB flash disk (pen drive).

To use USB pen drive with terminal, plug in your USB pen drive and follow the steps shown.

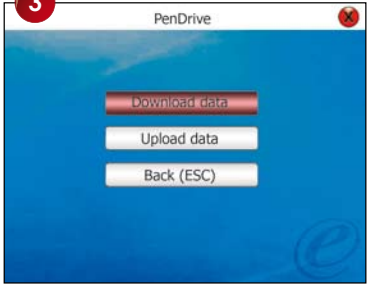
1

Press M /↵ once.

2

Press ▼ to Pen Drive.

3



Press OK once.
Choose the option by OK button.
Unplug USB flash disk when process complete.

The functions of the USB flash disk include:

1. **DOWNLOAD RECORD**
   To download transaction logs from terminal into USB pen drive.
2. **DOWNLOAD USER**
   To download users from terminal into USB pen drive.
3. **DOWNLOAD SMS**
   To download all short messages stored inside terminal into USB pen drive.
4. **UPLOAD USER**
   To upload users from USB pen drive to terminal.
5. **UPLOAD PICTURE**
   To upload users' pictures from USB pen drive to terminal.
6. **UPLOAD SMS**
   To upload predefined short messages from USB pen drive to terminal.
7. **UPLOAD THEME**
   To upload new theme to terminal. Please refer to ***http://user.fingertec.com*** to learn to configure theme and upload to terminal.

WORK CODES

This terminal is providing work code feature. The work code feature allows user to key in a predefined number after fingerprint or password verification. User will key in a number after fingerprint or password verification. User will key in related work codes to show purpose of their clocking data.

Table below is showing examples of work code function predefined by number:

Reasons	Work code
Check In	00
Check out	01
OT start	04
Done	05
Sick leave	10
Half day leave	12
Emergency leave	11
Meeting client	20
Outstation	21

These numbers are predefined by user in the software and represent different reasons, such as “10” for sick leave, “11” for emergency leave.

TO DEFINE WORK CODE

1

Press M /↵ once.

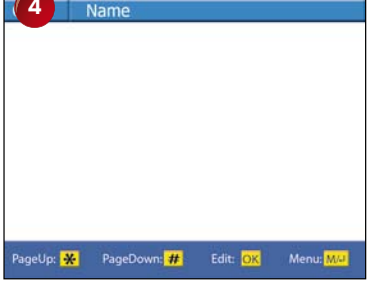
2

Press OK once.

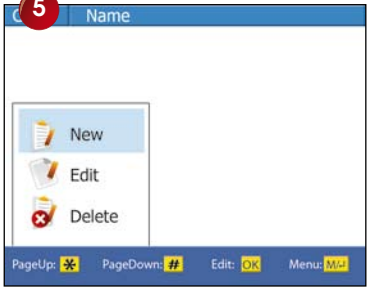
3

Press ▶ to choose Work Code and press OK button.

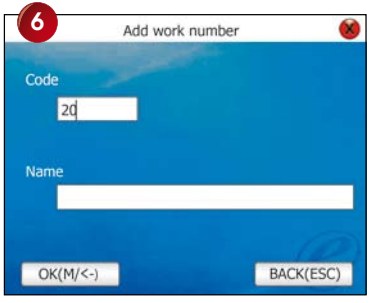
4



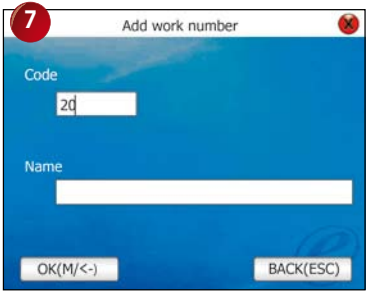
Press M /↵ once.



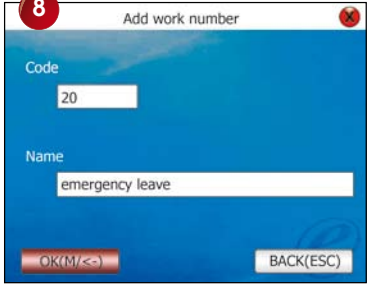
Choose NEW and press **OK** .



Enter number to represent work code.



By using the T9 input method, input the name of work code.



Press **OK** once to save all settings.

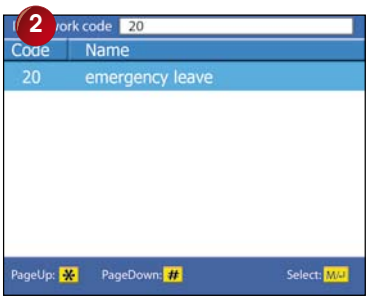
Press **Esc** 3 times to return to the main menu.

NOTE

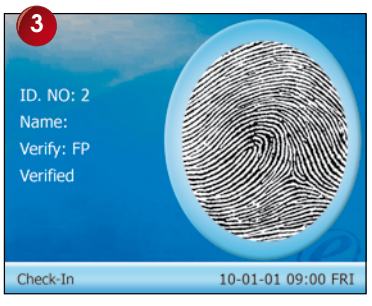
It is recommended to define work codes from the software rather than from the hardware because the process is easier.

TO VERIFY WITH WORK CODE

Press * once.



Enter work code value and press OK once.



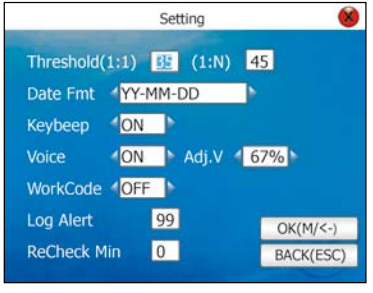
Verify your identity by your enrollment type.

SYSTEM OPTIONS

System options enable users to configure the followings:

- System
- Data
- Update
- Keyboard
- Display
- Power
- Reset
- Bell

SYSTEM



Threshold (1:1)
To configure the sensitivity of the optical scanner 1:1 matching. Range 0~50, recommended 35.

Threshold (1:N)
To configure the sensitivity of the optical scanner for 1:N matching. Range 0~50, recommended 45.

- Date format: To change the date display format.
- Keybeep: To enable or disable the keypad sound.
- Voice: To enable or disable greeting voice of terminal.
- Adj. V: To adjust the volume of greeting voice.
- Work code: To enable/disable work code function.

Log alert
To instruct terminal to alert user if the transaction storage is less than as configured, default is 99.

Recheck min
To instruct terminal to update transaction logs of all users in a time interval, default is 10 minutes.

DATA

Clear record
To delete all transaction logs stored inside the terminal.

Clear all
To delete all users information and transaction logs stored inside the terminal.

Clear admin
To clear administrator privilege in the terminal.

Delete picture
To delete picture of users stored inside the terminal.

UPDATE

This option is to allow installer to update the firmware version of terminal. Firmware is stored inside the USB flash disk and plug to the terminal. The updated process will run after you press **OK** for this option.

KEYBOARD

Key	Function	Code	Name
F1	Status Key	0	Check-In
F2	Status Key	1	Check-In
F3	Status Key	2	Break-Out
F4	Status Key	3	Break-Out
F5	Status Key	4	OT-IN
F6	Status Key	5	OT-OUT
F7	Undefine		
F8	Undefine		

PageUp: * PageDown: # Edit: M/↵

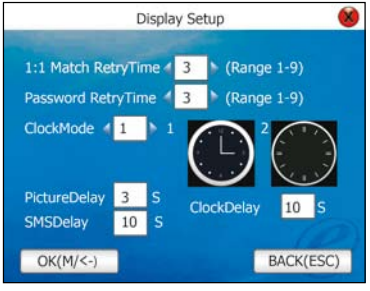
This option is to configure shortcut key for Status key, Work code, View SMS or Help Key for function key F1, F2, F3, F4, F5, F6, F7 and F8.

Key	Function	No.	Name
Backspace	Status Key	0	Check-In
Right	Status Key	1	CheckOut
ESC	Status Key	2	BreakOut
UP	Status Key	3	Break-In
M/OK	Status Key	4	OT-IN
Down	Status Key	5	OT-OUT
0	WorkCode		

Edit: M/OK

Applicable to TA100C only.

DISPLAY



1:1 match retry times
To set the maximum number of tries when user is using 1:1 fingerprint verification method. The terminal triggers alarm system when user tries more than as configured. Range 1 to 9.

Password retry times
To set the maximum number of tries when user is using password verification method. The terminal triggers alarm system when user tries more than as configured. Range 1 to 9.

Clock mode
To choose the display mode of clock.

Picture delay
To configure the picture delay time, range 1 to 99 sec.

Clock delay
To configure the clock delay time, range 1 to 99 sec.

SMS delay
To configure the short messages delay time, range 1 to 999 sec.

RESET

This option is to reset terminal back to default factory settings.

CAUTION

Once the terminal is reset, all information will be lost.
Back up all your important files!!

BELLS

This option is to configure schedule bells of terminal to trigger siren, total of 56 schedules. To define schedules bells:

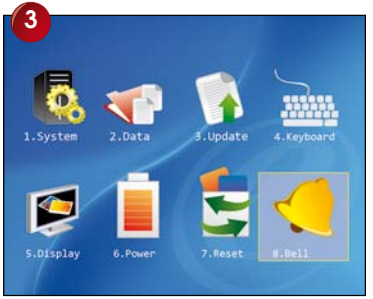
1

Press M /↵ once.

2

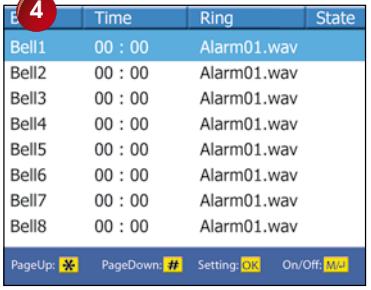
Press ► to choose System and press OK .

3



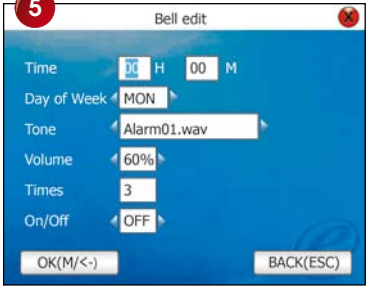
Press ► to choose Bells and press OK .

4



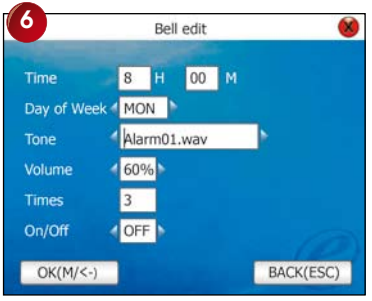
Press ▼ to go to the desired schedule bells press OK , for example Bell 1.

5

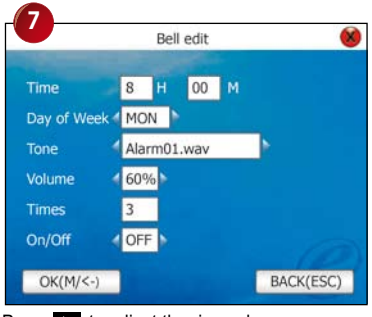


Enter value to adjust times should the bell ring. Press ▼ to proceed. Press ► to define day to trigger the bell, example Monday. Press ▼ to proceed.

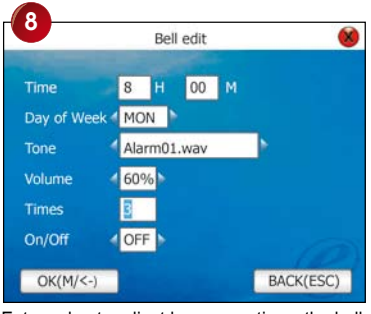
6



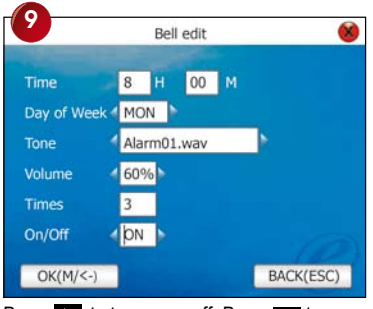
Press ► to choose the sound of bell. Press ▼ to proceed.



Press ► to adjust the ring volume.
Press ▼ to proceed.

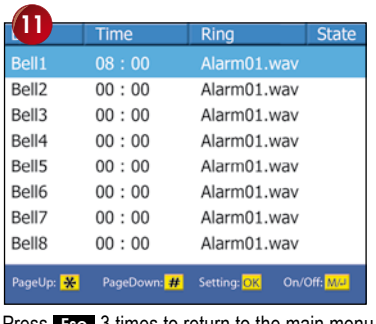


Enter value to adjust how many times the bell will ring for example 3. Press ▼ to proceed.



Press ► to turn on or off. Press ▼ to proceed.

Press OK to save settings.



Press Esc 3 times to return to the main menu.

To enable/disable the fingerprint image display on screen when user is scanning finger.

Neither show
To not show image for enrollment or verification

Both show
Show image during enrollment or verification

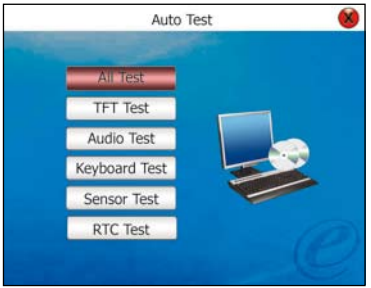
Enroll show
Show image during enrollment only

Match show
Show image during verification only

AUTO TEST

This option is recommended to run the installer. Installer can run the test from terminal to diagnose or analyze.

1. **ALL TEST**
   To run a complete cycle of test to all components of terminal.
2. **TFT TEST**
   To run test of TFT screen.
3. **AUDIO TEST**
   To run test of audio of terminal.
4. **KEYBOARD TEST**
   To run test of the keypad.
5. **SENSOR TEST**
   To run test of the optical scanner.
6. **RTC TEST**
   To run test of the real time clock in terminal.

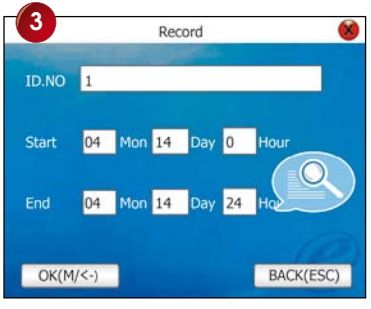


RECORD

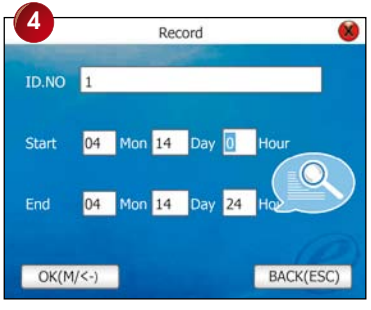
This is to allow administrator to view the transaction logs of users. Administrator needs to enter the user ID, start date and finish date to proceed.

Press M /↵ once.

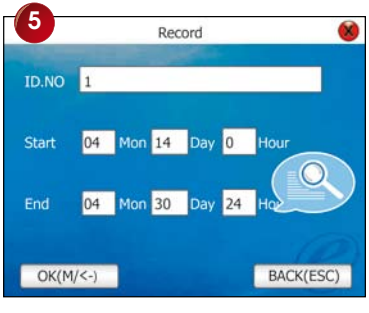
Press ▶ to choose Record and press OK .



Enter user ID and press ▼ .

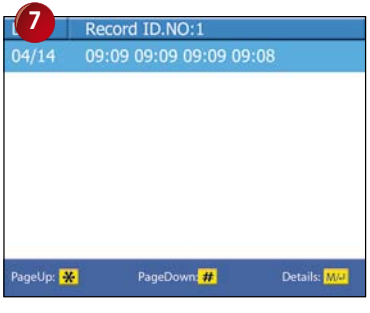


Enter start date and press ▼ .



Enter end date and press ▼ .

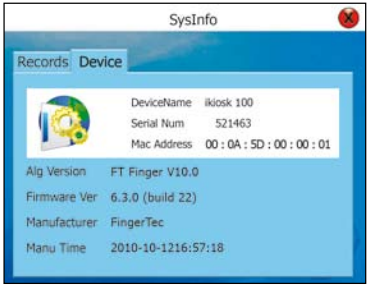
Press OK once.



Transaction logs found and displayed on screen. Press Esc times to return to the main menu.

SYSTEM INFO

This option is to allow installer to check the information of terminal, such as storage, firmware, algorithm etc.



SHORT MESSAGE DISPLAY

This option allows administrator to input message to view by individual or all users after verification. To configure short message.

1

Press M /↵ once.

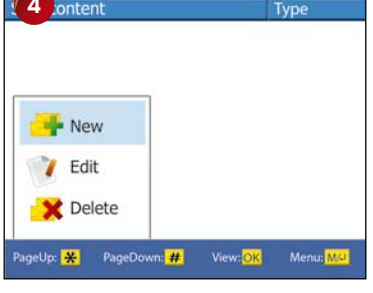
2

Select User and press OK .

3

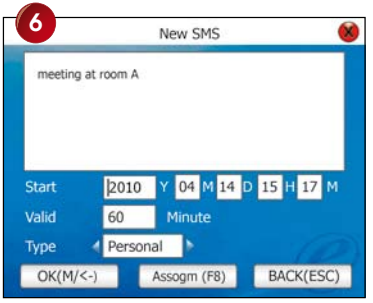
Press ► to choose SMS and press OK .

4



Press M /↵ once. Choose new and press OK .

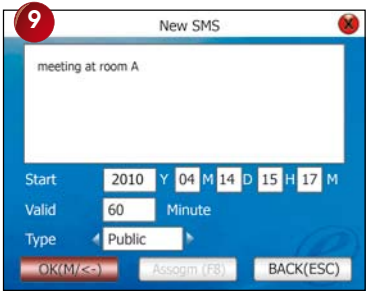
Enter the contents of short message by T9 input method. Press ▼ to proceed.



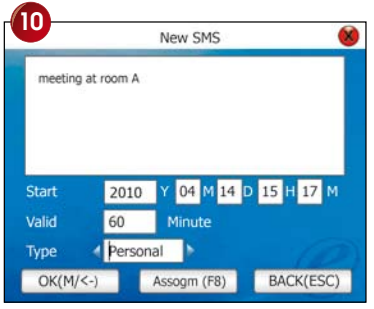
Enter the start time for message to be displayed. Press ▼ to proceed.

7 Enter the valid time for message to be viewed, for example 60 minutes. Press ▼ to proceed.

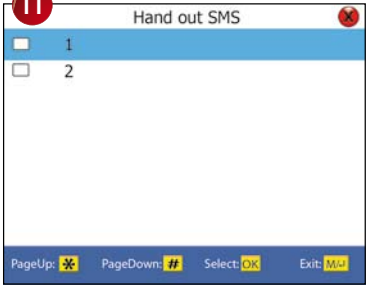
8 Press ► to choose recipient of the message.
Public: Message display to all users after verification.
Personal: Message only display to selected users only.
Reserved: Message saved but not display to any users.



If Public or Reserved is selected, press **OK** to save settings. Press **Esc** 3 times to return to the main menu.



If Personal is selected, press F8 to proceed.



Press **OK** to choose user to display message. You can choose multi users. Press **Esc** once to exit. Press **OK** once to save settings. Press **Esc** 3 times to return to the main menu.

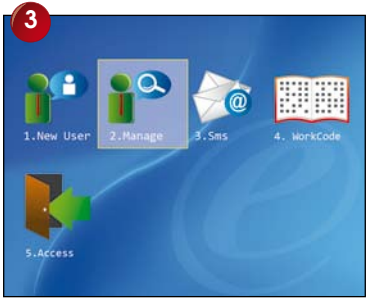
T9 INPUT METHOD

Administrator can enter alphabets, symbols or numbers during configuration at the reader, for example the user name, the content of short messages, etc. Administrator needs to use T9 input method to enter information.

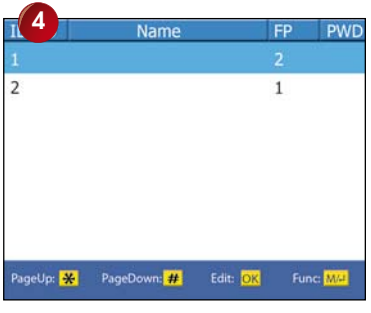
For example, To input user name by T9 Input Method:

Press M /↵ once.

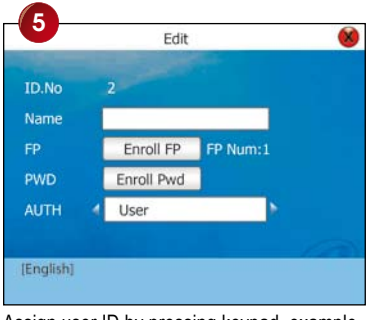
Press OK once.



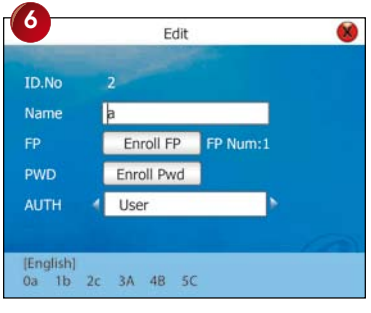
Press ► to select Manage.



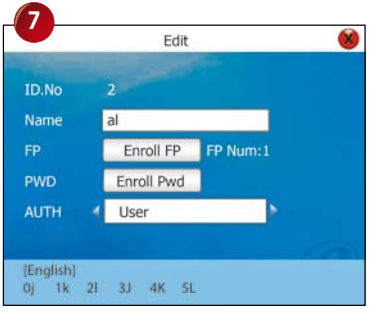
Press ▼ to select the user ID and press OK .



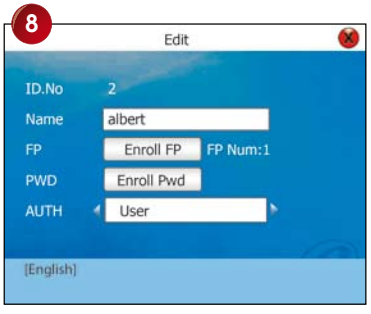
Assign user ID by pressing keypad, example 2. Press * once to start T9 input.



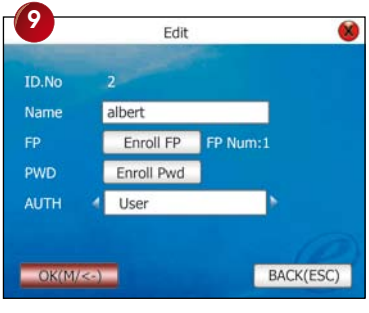
Press 2 and select 0 for letter a.



Press 5 and select 4 for letter K. Repeat the process to input.



Press OK once to save.



Press ▼ 4 times. Press OK once to save.

Press Esc 3 times to return to the main menu.

This Chapter is meant for qualified installer only. The installation of terminal shall be handled by a well-trained installer. If you are not a qualified installer, you can ignore this Chapter or this Chapter serves as reference for all types of connections available for the terminal only.

CONNECTIONS AVAILABLE

TA100C Series

1. TCP/IP PORT
This port is for connection in LAN environment. A straight RJ45/CAT. 5E cable should be plugged here to connect to a network switch/hub. A crossover RJ45 cable is for direct connection to a PC's network port.

2. USB PORT
To upload/download user information, password, fingerprint and transaction logs via USB flash disk.

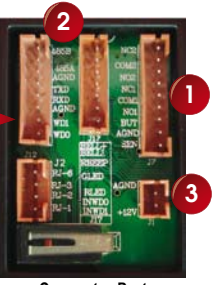
3. RS232/RS485 PORT
The port is for connection of RS232/RS485 communication type.
RS232 is a serial communication cable connecting from this port at one end to a serial port of a PC at another end.
RS485 cable extender should be connected to this port and the other of the cable should be connected to an optional RS232/RS485 Data Converter before it can be connected to the serial port of a PC.

4. POWER ADAPTER PORT
This port is for the power connection. Plug the power adapter here.

Q2i/TA200 Plus

Back of TA200 Plus

Back of Q2i



Connector Port

1. ACCESS CONTROL CONNECTION
To link reader with door lock systems and alarm system.

2. COMMUNICATION CONNECTION
TCP/IP Connection to provide TCP/IP communication to computer via LAN cable.
RS232 Connection to provide RS232 communication to computer via RS232 cable.
RS485 Single Connection to provide RS485 communication to computer via RS485 cable.
RS485 Network Connection to provide RS485 communication to computer via RS485 network.

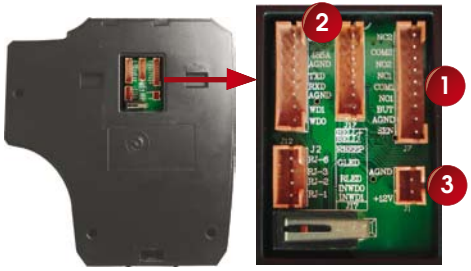
3. POWER SUPPLY CONNECTION
To provide DC 12V to reader to operate.

4. TCP/IP PORT
TCP/IP port to provide TCP/IP communication to the computer via LAN cable.

5. DC12V POWER
DC12V power input to provide power to the terminal.

POWER SUPPLY CONNECTION

i-Kiosk 100



Back of Reader　　Connector Port

1. ACCESS CONTROL CONNECTION

To link reader with door lock systems and alarm system.

2. COMMUNICATION CONNECTION

TCP/IP Connection to provide TCP/IP communication to computer via LAN cable.

RS232 Connection to provide RS232 communication to computer via RS232 cable.

RS485 Single Connection to provide RS485 communication to computer via RS485 cable.

RS485 Network Connection to provide RS485 communication to computer via RS485 network.

3. POWER SUPPLY CONNECTION

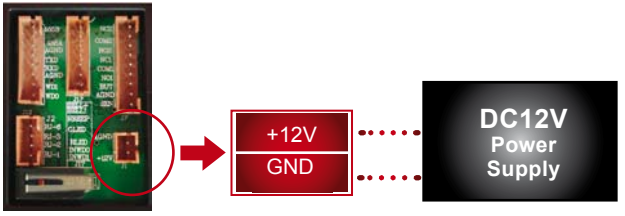
To provide DC 12V to reader to operate.

TA100C Series

DC 5V power adapter　　TA100C Terminal　　Power Button

1. Connect DC 5V power adapter to the terminal.
2. Turn on the power supply.
3. Press the power button to switch on or shutdown the terminal.

Q2i/TA200 Plus　　i-Kiosk 100



Connector Port　　Connector Pin

1. Connect DC 12V power supply to reader.
2. Turn on the power supply, the reader will start.

COMMUNICATIONS CONNECTION

The terminal can be connected to the computer by 4 ways.

TCP/IP CONNECTION

Please follow the steps shown to configure to connect via TCP/IP.

1

Press M /↵ once.

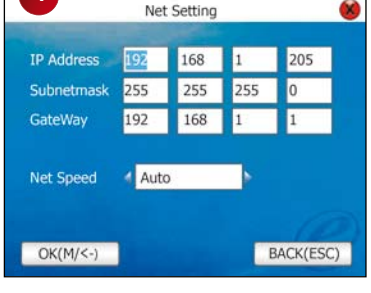
2

Press ▶ to Comm.
Press OK once.

3

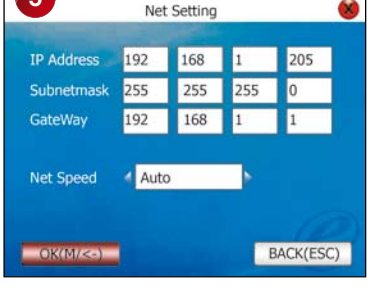
Select Network and press OK .

4

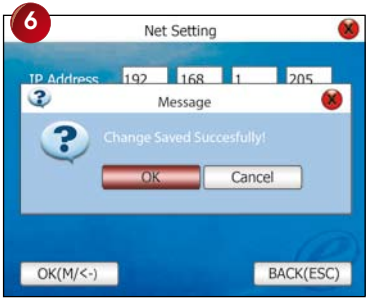


Enter the desired value.

5



Press OK to save settings.



Press **OK** to confirm.

Press **Esc** twice to return to the main menu.

8. Power off the reader.
9. Plug network plug into the network port of reader and network point.
10. Turn on power and continue to configure Security (see Security on page 68 for more details).

In this page you will need to enter the values.

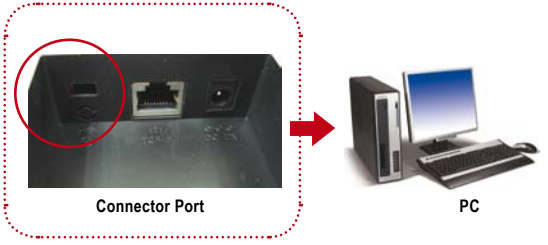
IP address
To enter the IP address of the terminal to suit into the network environment.

Subnet mask
To enter the subnet mask of the network environment.

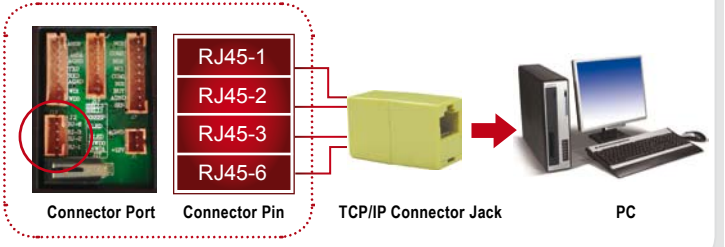
Gateway
To enter the gateway of the network environment.

Netspeed
To select the network speed of the terminal, 10M, 100M or Auto. Recommended to use Auto.

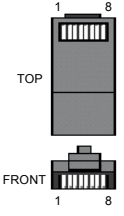
TA200 Plus



Q2i / i-Kiosk 100



Ethernet 10/100Base-T Crossover Cable



This cable can be used to cascade hubs or for connecting two Ethernet stations back-to-back without a hub. It works with both 10Base-T and 100Base-TX.

Joint 1 Pin			Joint 2 Pin
TX+	1	3	RX+
TX-	2	6	RX-
RX+	3	1	TX+
RX-	6	2	TX-

Ethernet 10/100Base-T Straight Thru Cable

This cable will work with both 10Base-T and 100Base-TX and is used to connect a network interface card to a hub or network outlet. These cables are sometimes called “whips”.

ConnectorPin		Cable Color Connector		
TX+	1	White/Orange	1	TX+
TX-	2	Orange	2	TX-
RX+	3	White/Green	3	RX+
	4	Blue	4	
	5	White/Blue	5	
RX-	6	Green	6	RX-
	7	White/Brown	7	
	8	Brown	8	

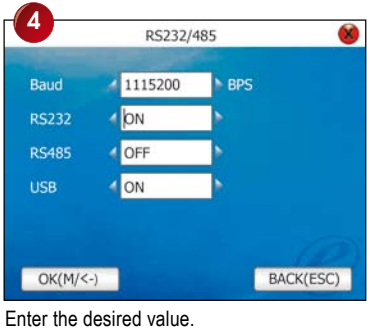
RS232 CONNECTION

Please follow the steps shown to configure RS232.

Press M /↵ once.

Press ▶ to Comm.
Press OK once.

Select RS232/485 and press OK .



Enter the desired value.

Press OK to save settings.

Press OK to confirm.

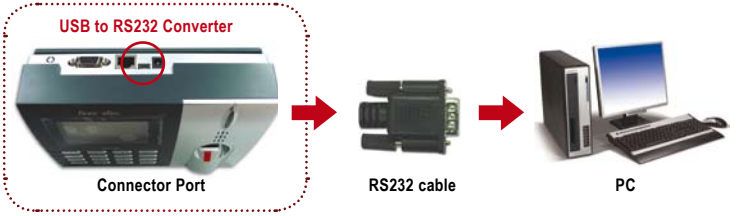
Press **OK** twice to return to the main menu.

8. Power off the terminal.
9. Plug RS232 cable into terminal and computer.
10. Turn on power and continue to configure Security (see Security on page 68 for more details).

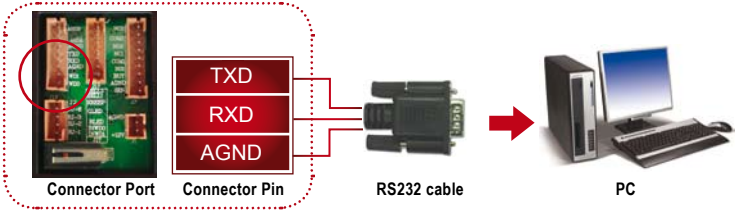
In this page you will need to enter the value.

Baud - To define the baudrate of the connection.
RS232 - Select Yes to enable.
RS485 - Select No to disable.
USB - Select Yes to enable.

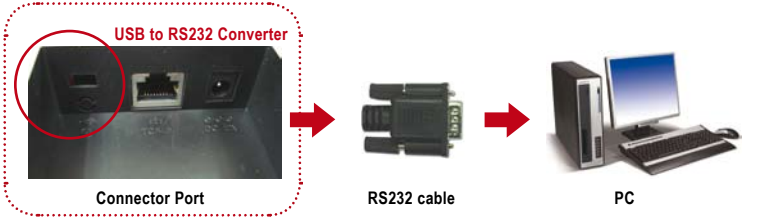
TA100C Series



Q2i / i-Kiosk 100



TA200 Plus



RS485 CONNECTION

Please follow the steps shown to configure RS485.

Press M /↵ once.

Press ► to Comm.
Press OK once.

Select RS232/485 and press OK .

Enter the desired value.

Press OK to save settings.

Press OK to confirm.

7

Press **Esc** twice to return to the main menu.

8 Power off the terminal.

9 Plug RS485 cable to data converter then into terminal and computer.

10 Turn on power and continue to configure Security (see Security on page 68 for more details).

In this page you will need to enter the value.

Baud To define the baudrate of the connection.

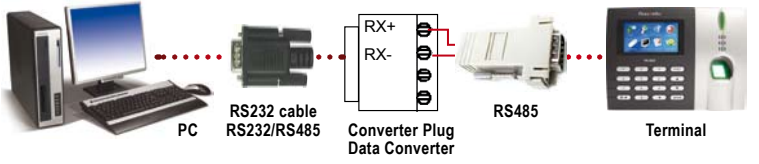
RS232 Select Yes to enable.

RS485 Select No to disable.

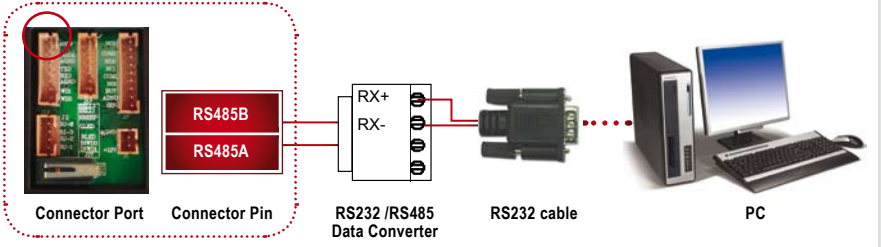
USB Select Yes to enable.

RS485 SINGLE CONNECTION

TA100C Series

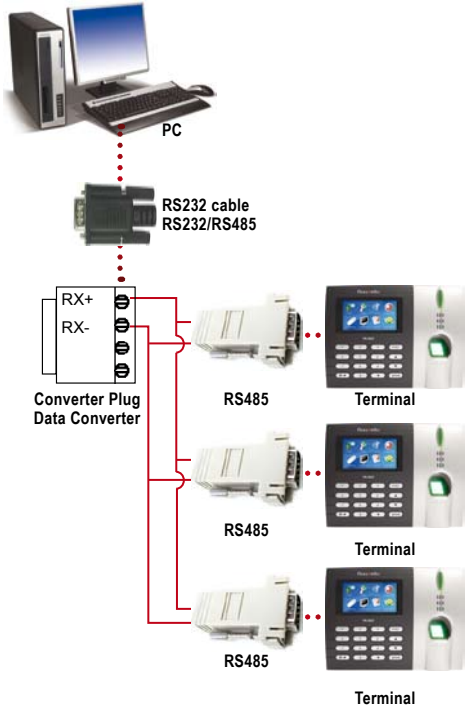


Q2i / i-Kiosk 100

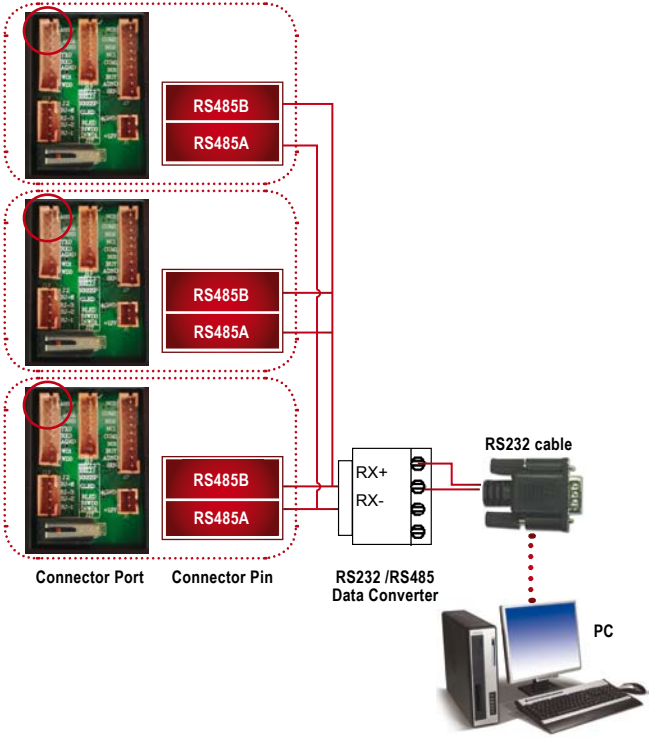


RS485 NETWORK CONNECTION

TA100C Series



Q2i / i-Kiosk 100



SECURITY

You need to define the followings after you select your communication method.

DEVICE ID

This is the ID of the terminal for the software to recognize and connect to it. It starts from 1 to 254. Please make sure you define the Device ID after you configured the communication method. The Device ID of the terminal must match with the ID in the software or the connection will fail.

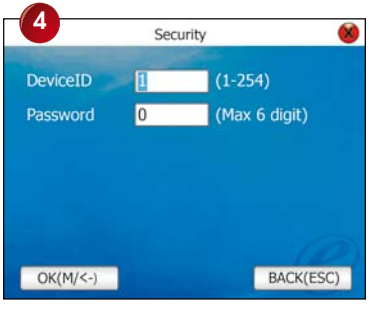
PASSWORD

This is the security password for software to connect to the terminal. Please always keep it as default, 0 because the software comes with product key and activation code for security purpose.

Press M /↵ once.

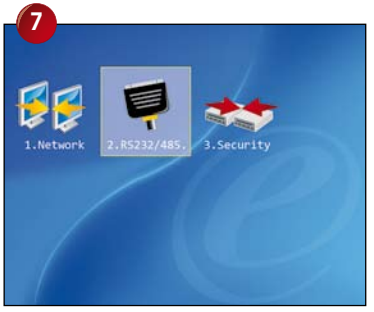
Press ► to Comm. Press OK once.

Select Security and press OK .

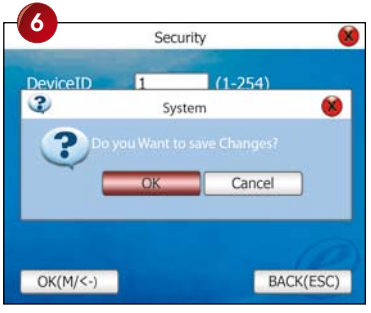


Enter the desired value.

Press **OK** to save settings.



Press **Esc** twice to return to the main menu.



Press **OK** to confirm.

8 Restart the terminal.

Appendix • TROUBLESHOOTING

1. How to power on and shut down the terminal?
   To power on, press the ON/OFF button once. To shut down, press and hold the ON/OFF button for 3 second.

2. I cannot connect the terminal to the PC. Every time I try, the software prompts "Unable to connect" message. What should I do?
   Please check communication settings in **Menu > Option > Comm.** Opt. Please see more details in page 60, Connection to Computer.

3. The terminal has difficulty recognizing my fingerprint. It takes many tries before I am verified. What should I do?
   Please make sure that your finger is not too oily or too dirty because the oil and dirt will cover the minutiae points of the fingerprints, thus making reading difficult. Make sure the terminal is not facing direct sunlight because it will disturb the reading of the sensor. To deal with light interference, cover the reading area when you want to verify your fingerprint. If this occurred often, kindly ask for re-registration.

4. Alarm goes off every time when I place finger on the sensor. Why did such thing occur and what should I do?
   The finger you used was defined as a duress finger. Once a duress finger is verified, it will trigger the terminal to activate the alarm. To undefine your finger as a duress finger, follow these steps: **Menu > Option > Access options > Duress Option > Duress FP > Undef Duress FP > Enter your user ID.**

5. When the terminal is turned on, the red LED is blinking all the time. Is there any problem with the terminal?
   There is nothing wrong with the terminal. The red LED blinks to indicate terminal is on standby. When a fingerprint is verified, the LED will turn green to indicate successful verification.

6. The terminal is accidentally turned off by a staff. Would we lose all the transaction data and fingerprints in that terminal?
   All transaction data and fingerprints in the terminal is safe in the event of power shutdown because all the information is stored in the memory of the terminal. This information can only be deleted via software or it can be manually purged in Advance option.

7. How to define the short message and assign it to certain users?
   Refer to page 54 for instructions to define short messages. The easier way to define the short message is by using software.

8. Do I need to clear the unwanted or outdated short messages in the terminal?
   Not necessary, as those messages will be deleted automatically after the predefined time period has expired.

9. During enrollment I heard "duplicate finger". Why was that?
   The "duplicate finger" voice message is to alert user if the enrolling finger is found to have existed in the terminal. User must use other finger to enroll.

10. I waved my RFID card to a terminal but it did not respond. What could be the reason?
    Please make sure that your RFID card is registered to the terminal before you use it. Please also make sure that your user ID is assigned into the verification group that supports RFID card.

11. Do I need to stop the USB pen drive like we usually do when used in computer before we could unplug it from the terminal?
    Not necessary because once download or upload operation is completed, it is safe for you to remove the USB pen drive from the terminal.

For technical tips and manuals in other languages, refer to **http://user.fingertec.com**