Your Key to Freedom

iClock 700
Biometric Time & Attendance,
Access Control Terminal

USB UNIVERSAL SERIAL BUS | **TCP/IP**

User Manual

Version 1.1
Date: July 2011

ZKSoftware®
Advanced Biometric and RFID Solutions

Table of contents

Table of contents...continue 1

1. Getting started

1.1 Fingerprint Placement

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

1. Proper finger placement:
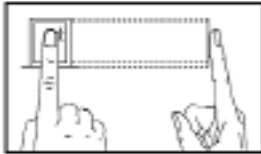
The finger is flat to the surface and centered in fingered guide.

2. Improper finger placement:

Not flat to the surface

Off-center

Slanting

Off-center

Please enrol and verify your fingerprint by using the proper finger placement mode. We shall not be held accountable for any consequences arising out of the degradation in verification performance due to improper user operations. We shall reserve the right of final interpretation and revision of this document.

1.2 Instruction for Card Swipe

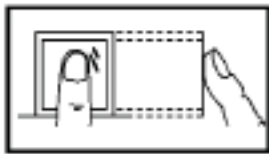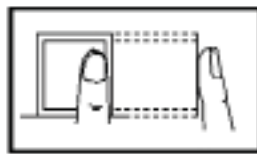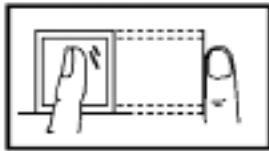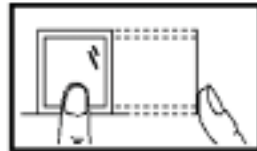This device is supplied with an integrated non-contact RFID (125 MHz) card reader module. By offering multiple verification modes such as fingerprint, RF card and fingerprint + RF card verification, this device can accommodate diversified user needs.

Swipe your card across the sensor area after the voice prompt and remove your card after the device has sensed it. For the swipe area, please see 2.2.3 Product Appearance.

1.3 Precautions

Protect the device from exposure to direct sunlight or bright light, this greatly affects the fingerprint collection and leads to fingerprint verification failure.

It is recommended to use the device under a temperature of 0–50°C so as to achieve the optimal performance. In the event of exposure of the device to the outdoors for long periods of time, it is recommended to adopt sunshade and heat dissipation facilities because excessively high or low temperature may slow down the device operation and result in high false rejection rate (FRR).

When installing the device, please connect the power cable after connecting other cables. If the device does not operate properly, be sure to shut down the power supply before performing necessary inspections. Note that any live-line working may cause damage to the device and the device damage arising out of live-line working falls beyond the scope of our normal warranty.

For matters that are not covered in this document, please refer to related materials including the installation guide, access control software user manual.

Summary

* Please ensure correct placement of finger on reader.

* Ensure to disconnect all power cables, before attempting maintenance.

ZKSoftware®
The Advanced Biometric Solution

2. Introduction of Device

2.1 Overview of Device Functions

As an integrated fingerprint & access control device, our product can be connected with either an electronic lock or an access controller. This device features simple and flexible operations and supports the use of administrators. The screen displays will guide you through all the operations. It supports access control function for a security management and supports multiple communication modes.

2.2 Important Safeguards

2.2.1 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.

2.2.2 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.

4 feet / 1.2 meter (recommended)
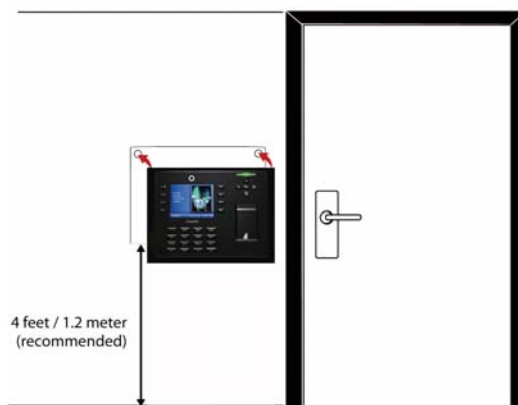
2.2.3 Product Appearance

Front view:

- LED indicator
- RFID scan area
- LCD Display
- Fingerprint sensor
- Keypad
- Speaker

2.3 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.

Summary

* Multiple communication modes

* Do not install in bright light or direct sunlight.

* Recommended height is 1.2m from the floor

The fingerprint terminal provides 4 types of enrolment methods:

- **Fingerprint enrolment**

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

- **Password enrolment**

  For user who has difficulty to enrol fingerprint due to poor fingerprint quality, enrolment of password is recommended. Password enrolment is also suitable for visitors and temporary workers.

- **Fingerprint and password enrolment**

  Under this option, a user can enrol both fingerprint and password at the same time. The user can either use fingerprint or password to report attendance or to gain access.

- **RFID card enrolment**

  Please refer to Chapter 2.7 for RFID Card Function.

2.4 Date / Time Adjustment

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

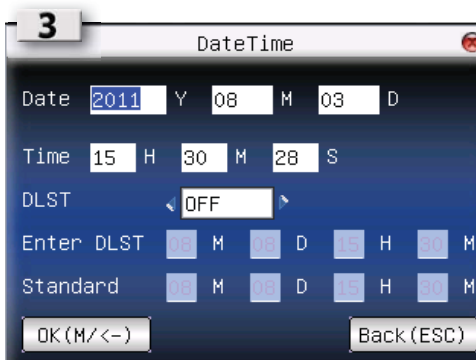Follow the steps shown to access the Date/Time adjustment menu:

- You can insert inputs into the terminals through the keypad. It contains numbers from 0-9, an OK button, an ESC/Cancel button, a Scroll up/down button, a doorbell button and a Menu button.
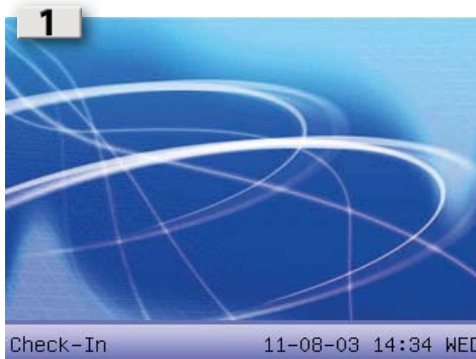
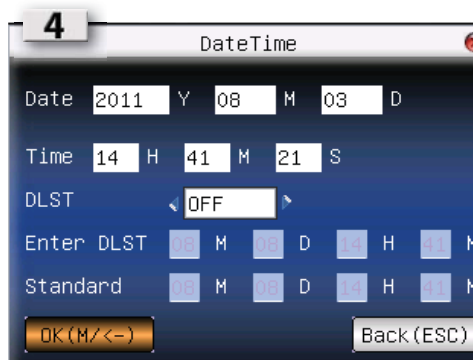
- Press M/↵ (menu) once

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

- Press ▼ to go to the desired field.
- Enter the value using keypads.

- Press OK once to confirm settings.

Summary

* Ensure the correct date & time on the unit.

* Enter the correct date & time in the required fields

2.5 Enrol Administrator / User

Once the fingerprint terminal is switched on, a display on the screen will appear. Enrol 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.

Summary

* Ensure to enrol an administrator on the unit.
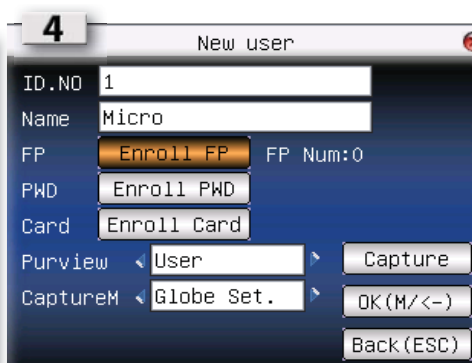
- Press M/↵ (menu) once

- Press OK (menu) once

- Press OK (menu) once

- Press ▼ 2 times to enrol fingerprint
- Press OK

* FP = Fingerprint

* PWD = Password / pin

* User = No administrative rights on the unit

* Admin = Full control of unit
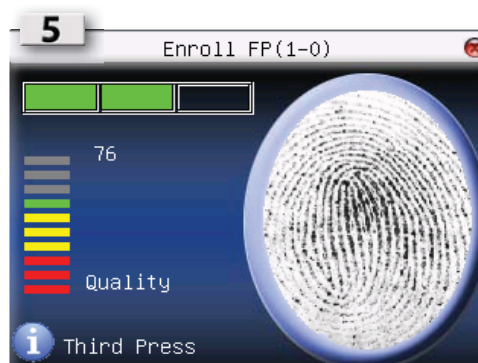
- Press desired finger 3x times on sensor to enrol
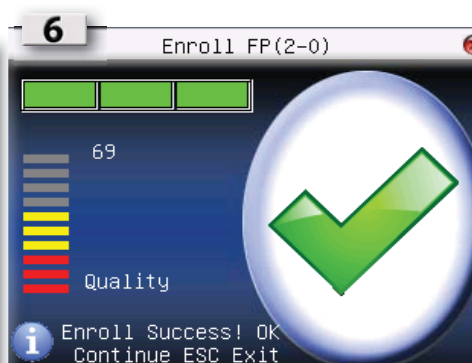
- Press OK once to enrol more
- Press ESC to exit

* Ensure a good quality fingerprint

2.6 Password Enrolment

If a user cannot enrol his fingerprint, he can choose to use passwords. Follow the steps below:

* Password may contain numbers ranging from 1 - 8 digits.
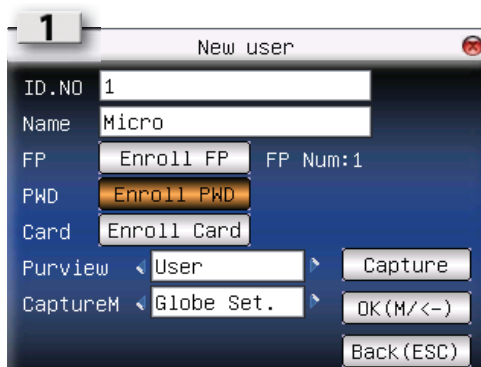
• Press ▼ 3x times to enrol passowrd	• Type a numeric password in the fileds
	• Press OK to enter
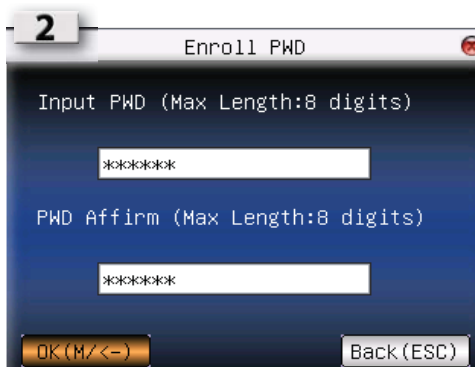
2.7 RFID Card Enrolment

If a user cannot enrol his fingerprint, he can choose to use a RFID Card. Follow the steps below:

* RFID card is for added security on the unit, or if the user can't use a fringerprint
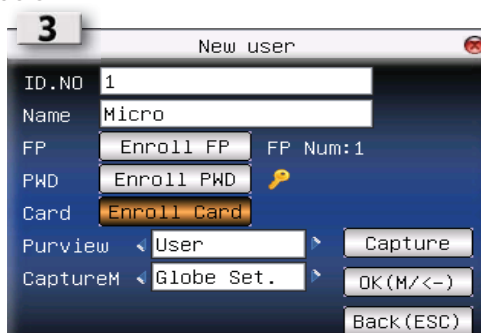
• Press ▼ 4x times to enrol a RFID card	• Punch the card to enrol
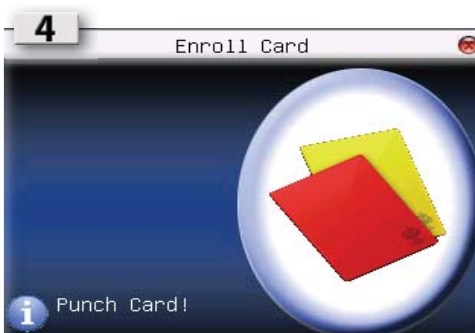
* Confirmation of enrolment

* Press OK to save OR

* Press ESC exit

2.8 Enrolling a Photo ID & Verification

Each enrolled user can enrol a photo ID for confirmation of fingerprint enrolled user.
With every confirmation of fingerprint the unit will display the enrolled ID photo.

Summary

* Photo will accompany user ID when verifying with access (FP or Card)
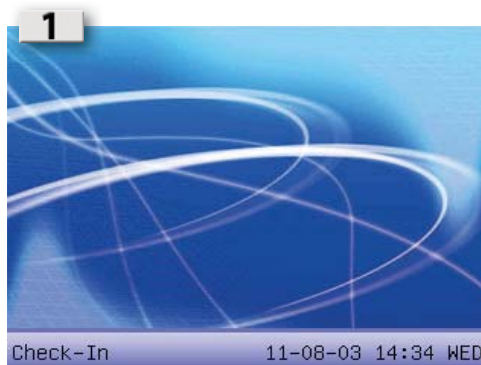
- Press M/↵ (menu) once
- Press OK 2x times
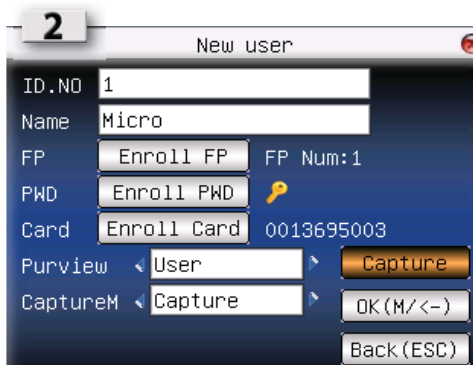
- Press ▼ 7x times to enrol a photo

- Press OK to capture photo
- Press OK after completing capture to exit
- Press CANCEL to re-take the photo

- Press ▼ once
- Press OK to save

2.8.1 Fingerprint Verification with Photo

- Press fingerprint on sensor to verify user

- Verification of fingerprint will display user id photo
- Voice prompt to fiollow : 🗣 "Thank You"

8

2.8.2 Password & Card verification with photo

Summary

* Press number for user ID and then insert PWD for access.

- Press your user id number
- Press OK

- Enter your numeric password
- Press OK
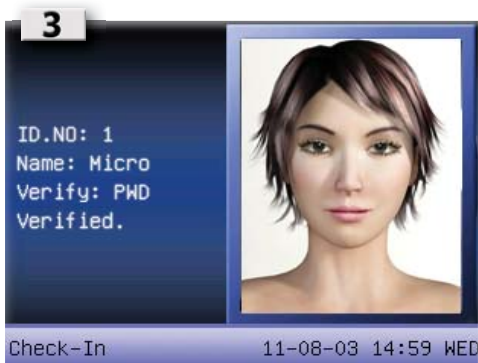
- Photo will verify the user id
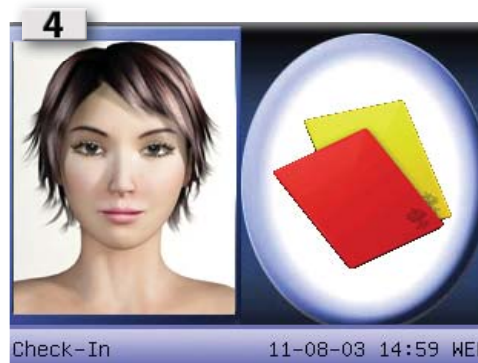
- Swipe your RFID Card
- Photo will verify user id

* Clock display with successful verification

- Incorrect entry via fingerprint / card or password will show error on screen
- Try again

- Successful entry will display clock and time

ZKSoftware®
The Advanced Biometric Solution

2.9 Manage Users

2.9.1 Search User
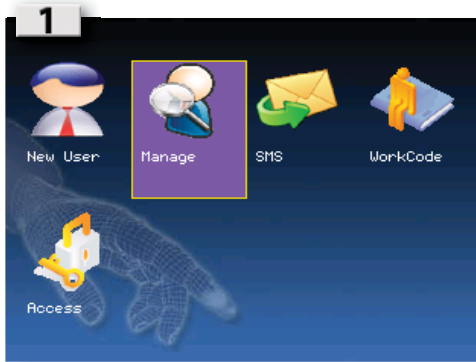
- Press M/↵ (menu) once
- Press OK
- Press ▶ once
- Press OK
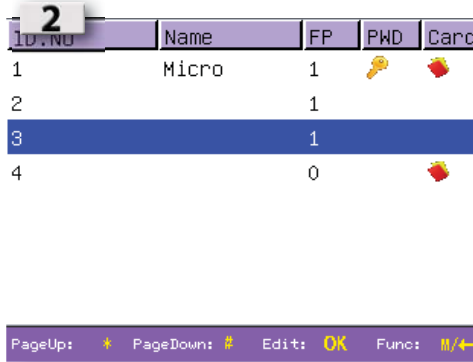
- Press ▼ to selected user
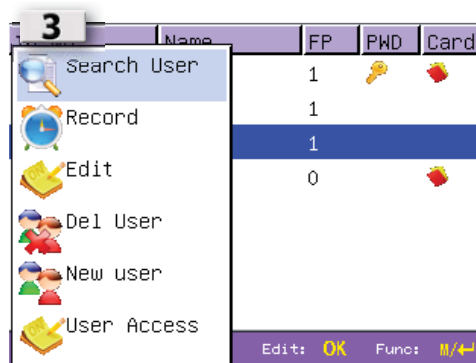
- Press M/↵ (menu) for options window
- Select SEARCH USER
- Press OK
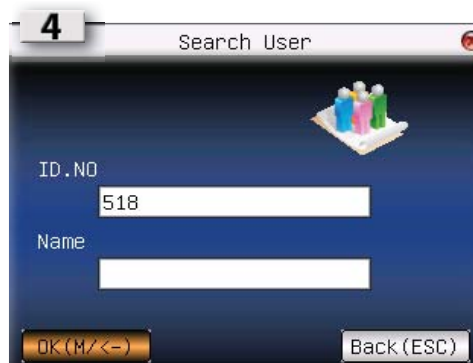
- Type in the desired user id to search

2.9.2 Delete user
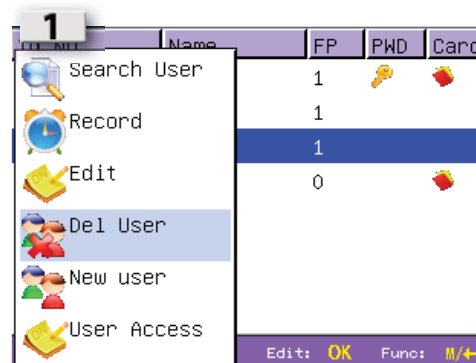
- Select DEL USER to enter delete options

- Delete a single user
- Move down to desired user
- Press OK

Summary

* Take note: Only Administrator can edit / delete users

* Ensure to select correct user ID before deletion

ZKSoftware®
The Advanced Biometric Solution

2.9.2 Delete user...continue

• Press ▼ (menu) once to select available options to delete.	• Press OK to confirm

3. User Access
3.1 Description of User Access

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

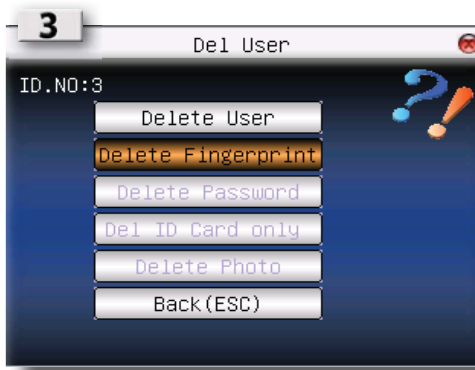| Time Zone	1
SUN	09H00 : 18H00
MON	09H00 : 18H00
TUE	09H00 : 18H00
WED	09H00 : 18H00
THU	09H00 : 18H00
FRI	09H00 : 18H00
SAT	09H00 : 18H00

Time Zone 2 & 3

Variation in access for a period of one week . Table below 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 and 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 employees, therefore they can be grouped together in Group Time Zone, for example Group.

Time Zone	2	3
SUN	23H59 : 00H00	23H59 : 00H00
MON	08H00 : 12H00	14H00 : 18H00
TUE	08H00 : 12H00	14H00 : 18H00
WED	08H00 : 12H00	14H00 : 18H00
THU	08H00 : 12H00	14H00 : 18H00
FRI	08H00 : 12H00	14H00 : 18H00
SAT	23H59 : 00H00	23H59 : 00H00

Summary

* Time Zones can be created for access times to allow access

* Access from 9H00 - 18H00

* Everyday of the week

* TZ 2 : Access from 8H00 to 12H00 during week

* No weekend access

* TZ 3 : Access from 14H00 to 18H00 during week

* No weekend access

Group Time Zones

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.

Summary

GROUP TIME ZONE	TIME ZONES		
1	2	3	
2			
3			
4			
5			

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.

3.2 Assign a user to a Time Zone

3.2.1 Create a Time Zone

* Press M/↵ (menu) once

* Press OK

* Press ▼ to select ACCESSS

* Press OK

* Press OK once

* Ensure to setup a Time Zone first before assigning users
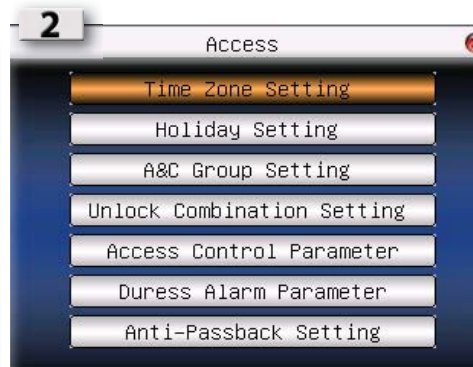
* Press ▼ to selected field and enter values

3.2.2 Assign a Holiday Time Zone
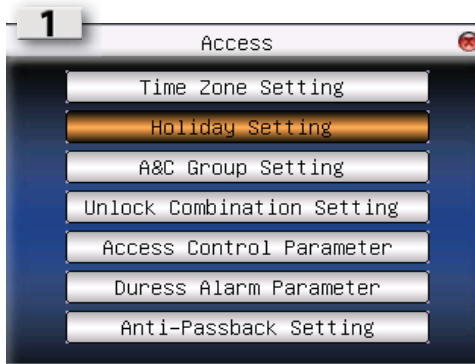
1

```
Access                        ⊗
   Time Zone Setting
   Holiday Setting
   A&C Group Setting
   Unlock Combination Setting
   Access Control Parameter
   Duress Alarm Parameter
   Anti-Passback Setting
```

- Press ▼ to select HOLIDAY SETTINGS

2

```
No.  Dates                    TZ

        New
        Edit
        Delete

PageUp:  *  PageDown: #   Edit : OK   Menu : M/←
```
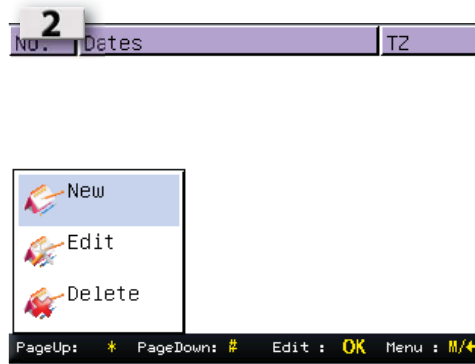
- Press M/↵ to open options window
- Press OK to create a new settings

3

```
       New Holiday            ⊗
No.      01
Start    01  M   01  D
End      01  M   01  D
TZ       01

OK(M/<-)              Back(ESC)
```
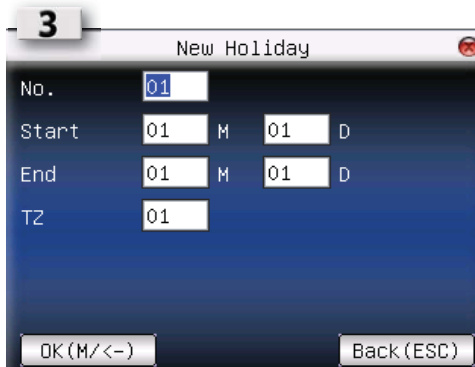
- Insert values
- Press OK to save

4

```
No.  Dates                    TZ
01   01.01-01.01              01

        New
        Edit
        Delete

PageUp:  *  PageDown: #   Edit : OK   Menu : M/←
```
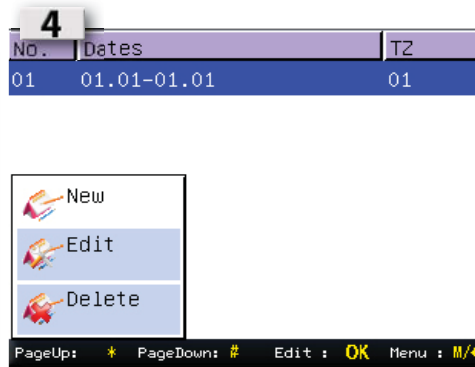
- EDIT / DELETE are available to change and delete

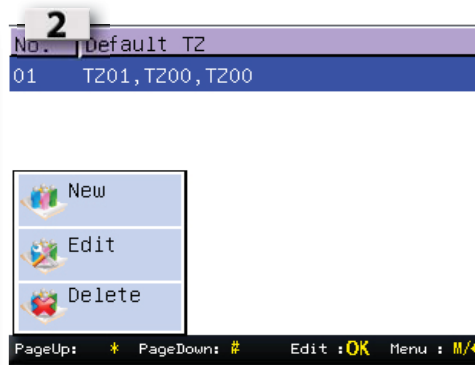## 3.2.3 Create or Edit a Access Control Group setting

1

```
Access                        ⊗
   Time Zone Setting
   Holiday Setting
   A&C Group Setting
   Unlock Combination Setting
   Access Control Parameter
   Duress Alarm Parameter
   Anti-Passback Setting
```
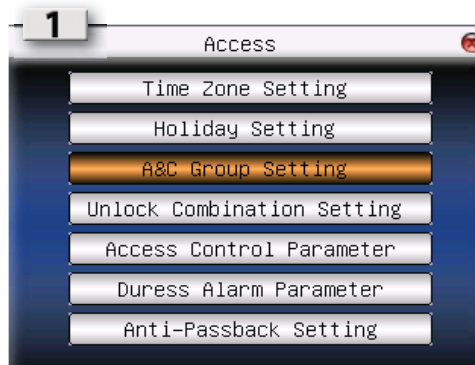
- Press ▼ to select A&C SETTINGS

2

```
No.  Default TZ
01   TZ01,TZ00,TZ00

        New
        Edit
        Delete

PageUp:  *  PageDown: #   Edit : OK   Menu : M/←
```

- Press M/↵ to open options window
- Note that Time Zone is already available
- NEW / EDIT / DELETE options are available

Summary

* Ensure to capture all holidays when setting up.

* Recommended to create holiday time zones to deny access, rather than deny access per user for holidays

* Delete is only available when a new group is created. There must always be a group active.

3.2.4 Unlocking Combination settings

Combo settings are for extra added security, where more than ons user need to sign in before access is granted.
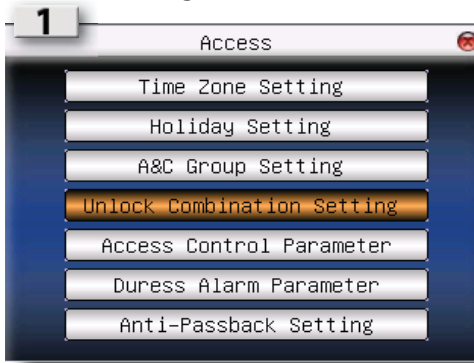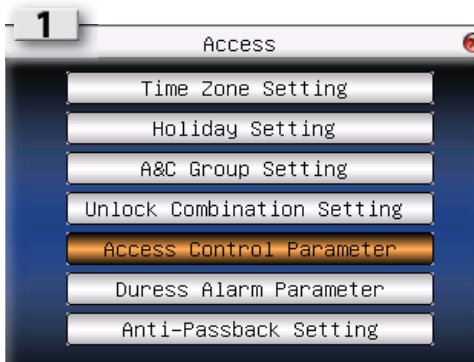

• Press ▼ to select UNLOCK COMB SETTINGS

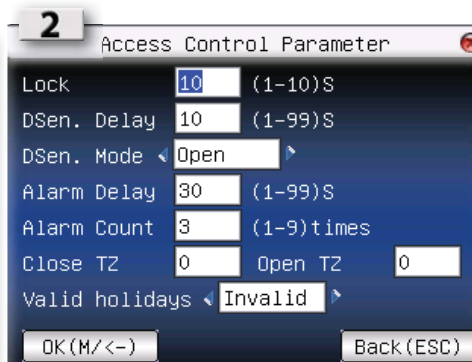• Press OK
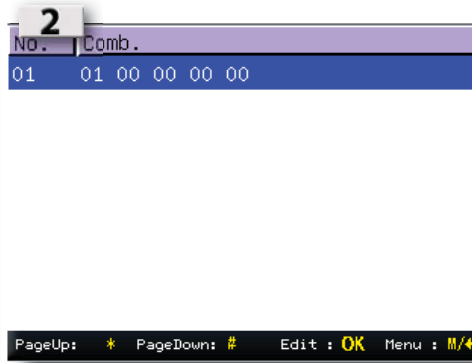
• Press M/↵ (menu) for NEW / EDIT / DELETE options

3.2.5 Change Access Control Parameters settings

• Press ▼ to select ACCESS CONTROL SETTINGS

• Press OK

• Press ▼ to select field and change values

• Press OK to save.

• **Lock (1-10s) :**
  To adjust the unlocking time after verification.

• **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.

• **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.

• **Alarm Delay (1-99s) :**
  To delay the reader from triggering alarm system.

• **Alarm count (1-9 ti mes) :**
  To adjust the maximum verification failures of users. When the maximum is reached, reader will trigger alarm system.

• **Close TZ :**
  Door is always locked during the predefined time period, so users cannot gain access after verification.

• **Open TZ :**
  Door is always unlocked during the predefined time period, so users do not need to verify their identities but can gain access.

• **Valid holidays :**
  Choose Valid to enable the holiday settings. Choose Invalid to disable the holiday settings.

Summary

* Combo settings for added security

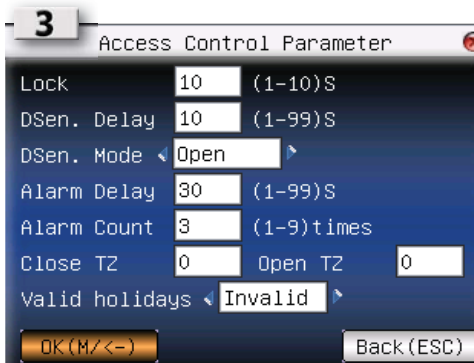* 2 or more user verification needed before access allowed

* Parameter settings is to change the control of the unit

3.2.6 Duress Alarm Parameters

The fingerprint reader will trigger alarm system after a duress fingerprint is verified sucessfully. It is advisable :
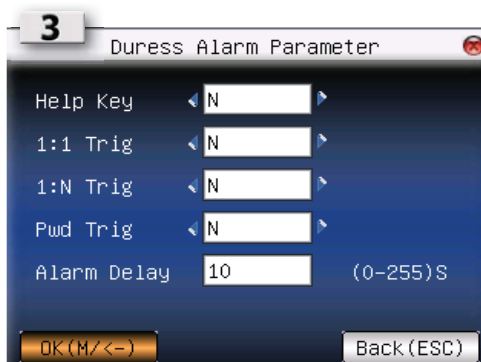
- 1 to use different fingers to do daily clocking mechanism and to trigger duress alarm

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

Summary
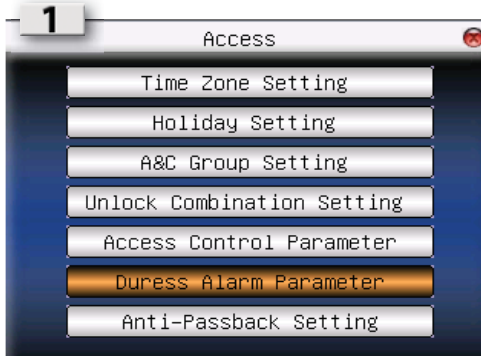
- Press ▼ to select DURESS ALARM SETTINGS

- Press OK
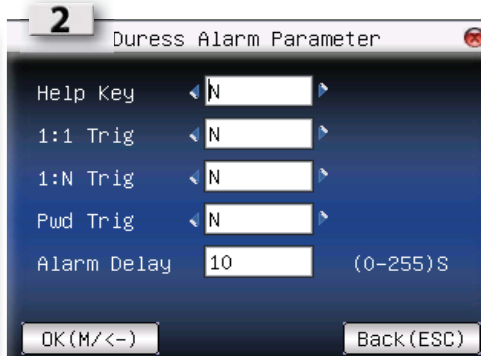
- Press ▼ to select value field

- Press ◄ ► to change options

- Press OK to save

- **Help key :**
  Select [Yes] to enable. Hold the for 3 second followed by the fingerprint verification. Successful verification will trigger alarm system.

- **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: N fingerprint verification process will trigger alarm system.

- **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.

- **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.

- **Alarm delay :**
  To delay the reader to trigger alarm system after verification.

3.2.7 Define a Duress Finger

If users would like to use different fingers for daily clocking and to trigger duress alarm, users must enrol 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.
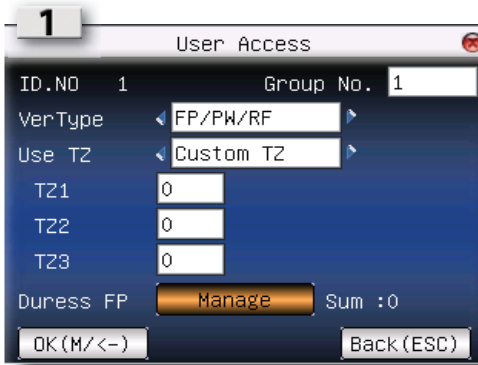
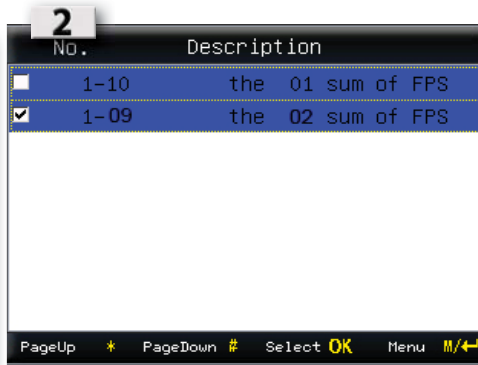Follow the steps on the next page to define duress finger.

* Enrol 2x or more fingerprints to assign a fingerprint.

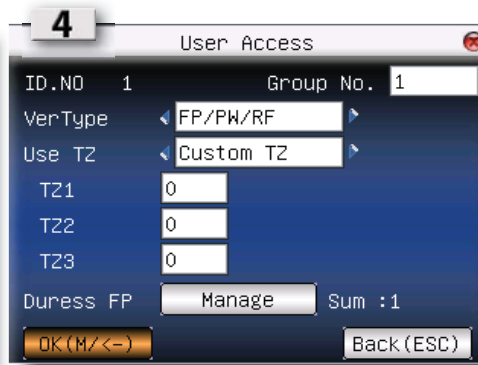* Assign index finger for daily clocking, and thumb for duress finger.

Define a duress finger...continue

- Press OK on USR MNG, ▶ to MANAGE
- Select user id for change
- Press M/↵, USER ACCESS
- Select MANAGE

- Press M/↵ (menu) once
- Select ENROL FP
- Follow instructions
- ESC to exit

- Press ESC
- Press OK to c

- Press OK to exit

3.2.8 Work Codes

This terminal is providing work code feature. The work code feature allows user to key in predefined 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:

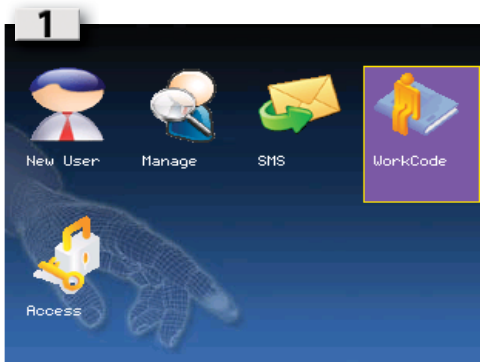| REASON	WORK CODE
Engineer	100
Welder	200
Packer	300
Receiving	400
Dispatch	500

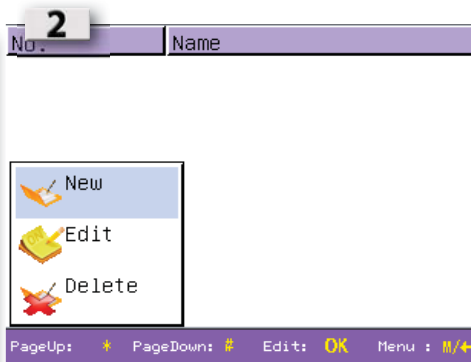* Workcodes can be customised.

* Advisable to use software to adjust workcodes

Create and assign work codes

Summary
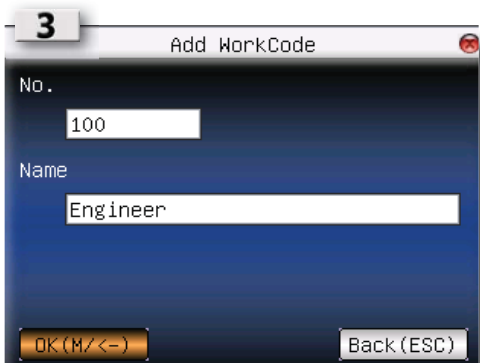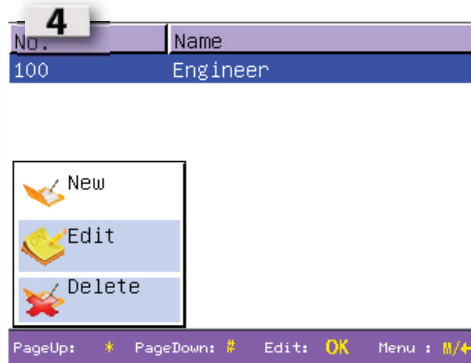
*Create / Edit workcodes

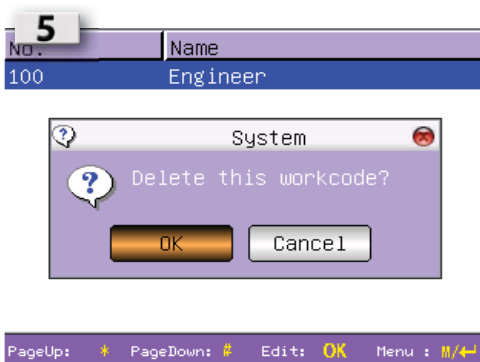- Press OK on USR MNG
- Press ▶ 3x times
- Press OK on WORKCODE

- Press M/↵ for options window
- Select NEW to create workcode

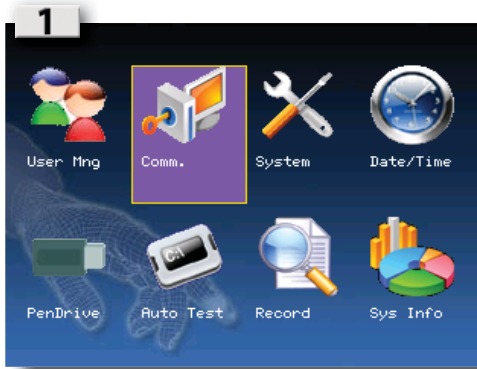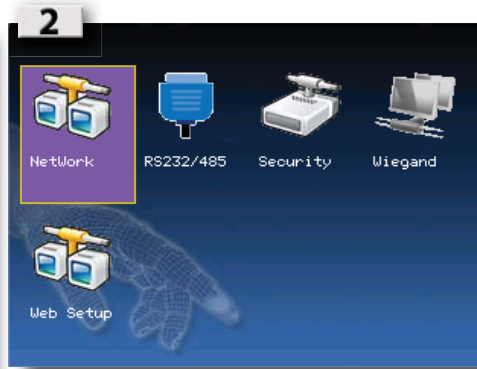- Complete the fields

- EDIT / DELETE available for changes

NOTE :

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

- If you wish to delete confirm with OK

17

4. Communications

4.1 Network (TCP/IP)

- Press M/ᶜ once
- Press ▶ once
- Press OK

- Press OK on NETWORK

- Press ▼ to desired field, and complete the values

* Ensure to assign a static address, units will not work on DHCP

4.2 RS232 / 485

- Press ▶ once to select RS232/485
- Press OK
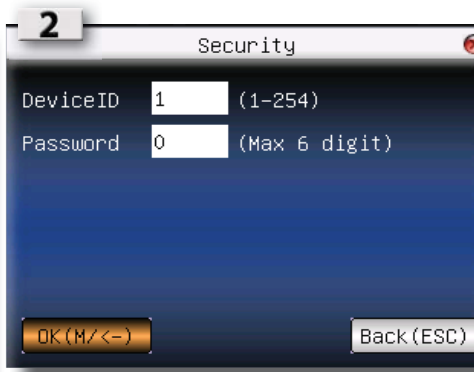
- Press ▼ to select field
- Press ◀ ▶ to change values

* Recommended distance

** RS232 = 20m - 60m

*** Could be affected by distance and power cables running parallel with unit cable

** RS485 = 1000m (max)

*** Could be affected by power cables

18

4.3 Security

* Device related password

* Restrict sub-administrator access

- Press ▶ 2x times to select SECURITY
- Press OK

- Press ▼ to change values

4.4 Wiegand

* Use WIEGAND communication port to connect to maglock or turnstiles

- Press ▶ 3x times to select WIEGAND
- Press OK

- Select INPUT OPT

Input Opt.

Define

26

Bit Counts	26	
Pulse Width	100	us	Default
Pulse Inter	2000	us	Default
Input	◄ ID.NO ►	

OK(M/<-)   Back(ESC)
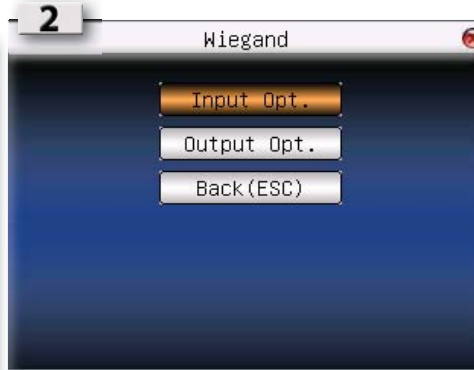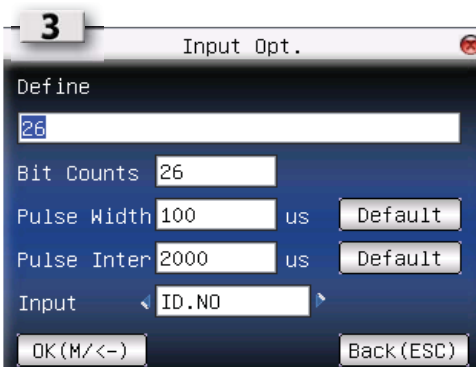
- Press ▼ to desired field and enter values
- Press OK to save

ZKSoftware®
The Advanced Biometric Solution
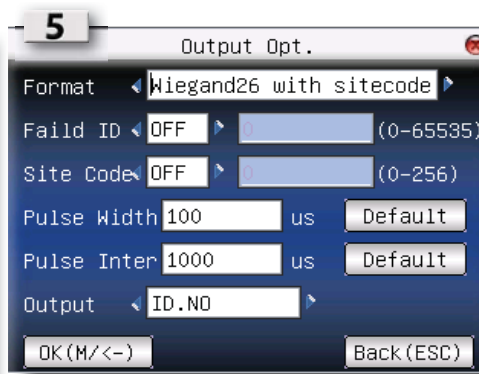
• Select OUTPUT OPT.	• Press ▼ to select fields • Press ◄ ► to change values or enter values

4.5 Web Setup

• Press ▼ to select WEB SETUP	• Press ▼ to select fields to change values
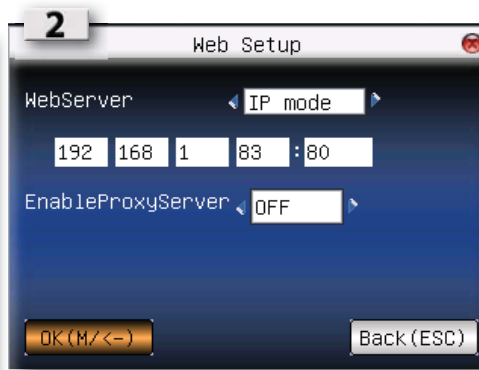
[English]
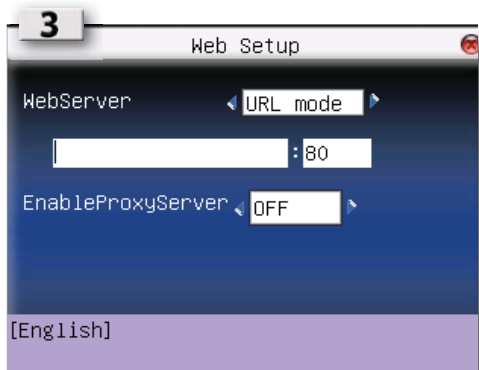
• Fill in the fields as requested

20

5. System

5.1 System settings
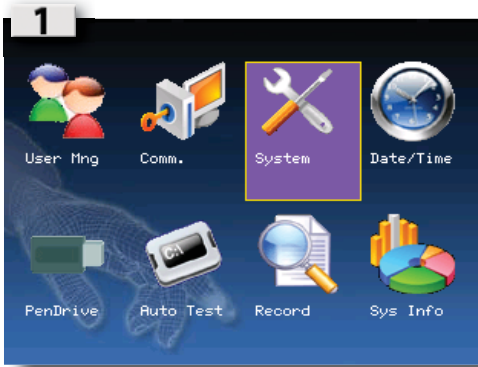
- Press M/↵ once
- Press ▶ 2x times to select SYSTEM

- Press OK to enter SYSTEM SETTINGS

- Press ▼ to scroll down to fields
- Change values

5.2 Data Management

- Press ▶ to select DATA MNG

- Press OK on a delete function
- Press OK to confirm

21

5.2.1 System Update

- Insert PENDRIVE(USB) with latest firmware on, before accessing this function

Data Mng (3)

Delete Attlog
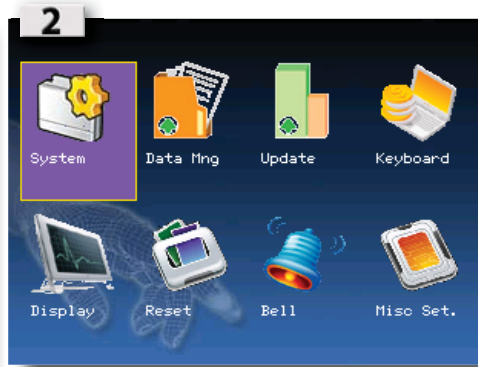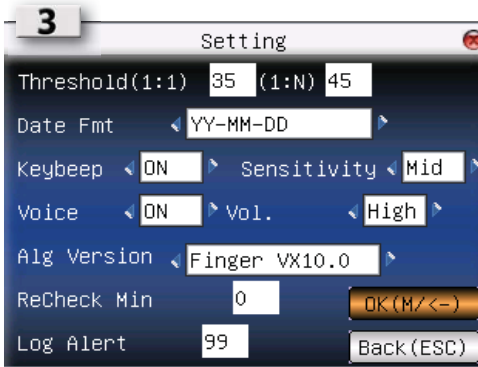Delete Photo
Del BL-photo
Delete All
Clear Purview
Delete Picture

- Press ▼ to select desiired option
- Press OK to confirm

Summary

* System update - ensure to have latest firmware loaded on USB before this function will activate

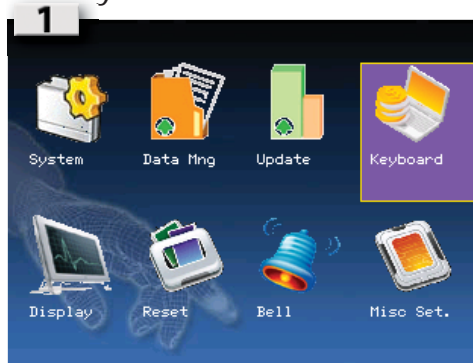* Custom "F" keys to dif-firentiate between access modes

5.3 Keyboard

- Press ▶ 3x times to select KEYBOARD
- Press OK

Key	Function	No.	Name
F1	Status Key	0	Check-In
F2	Status Key	1	CheckOut
F3	Status Key	2	BreakOut
F4	Status Key	3	Break-In
F5	Status Key	4	OT-IN
F6	Status Key	5	OT-OUT
F7	Undefine		
F8	Undefine		

PageUp: *   PageDown: #   Edit: OK
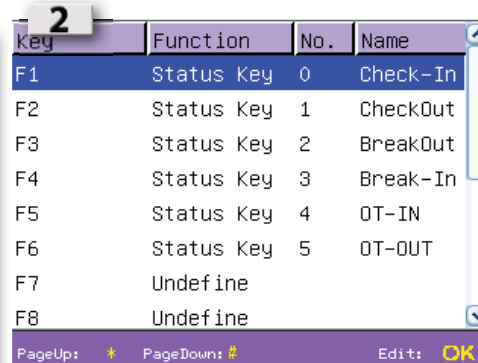
- Press OK to edit selected field

5.4 Display
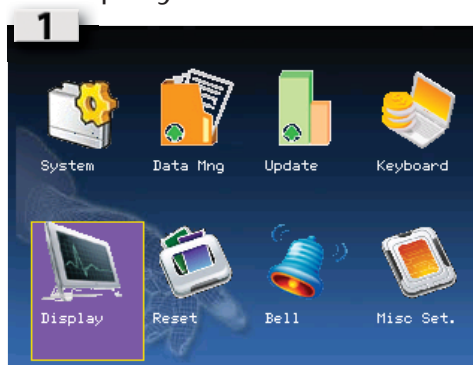
- Press ▼ to select DISPLAY
- Press OK

Display Setup

1:1 Match RetryTimes ◀ 3 ▶ (Range 1-9)
Password RetryTimes ◀ 3 ▶ (Range 1-9)
ClockMode ◀ 1 ▶   1   2
PictureDelay 10 S   ClockDelay 10 S
CaptureMode ◀ Capture ▶

OK(M/<-)   Back(ESC)
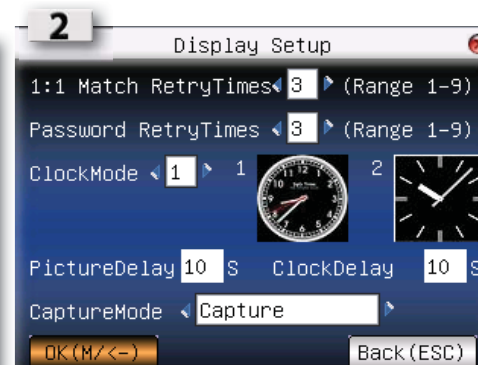
- Press ▼ to select field
- Press ◀ ▶ to change values
- Press OK to save

22

5.5 System Reset
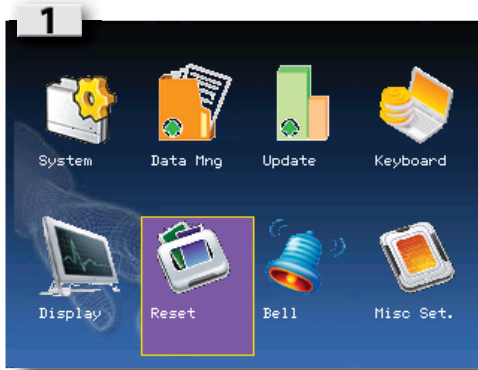
- Press ▶ to select RESET
- Press OK

- Select field that needed to be reset
- Press OK to confirm

5.6 Bell

- Press ▶ 2x times to select BELL
- Press OK
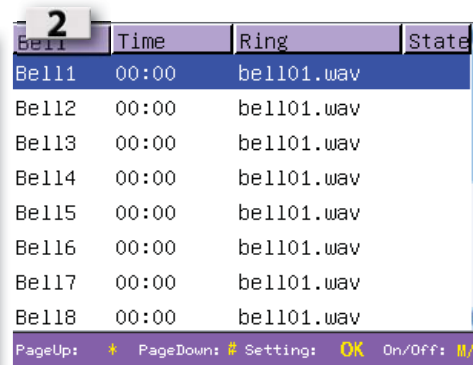
- Press OK to edit the field

- Press ◀ ▶ to change values or enter values
- Press OK to save

- Display will indicate change with a BELL in the STATE field

Summary

* Reset function are only configuration of unit, and not to delete users

* Notification bell for time breaks (lunch / tea / etc)

23

5.7 Miscellaneous settings

Misc Set.

Sleep time	30	M(0:Always On)
Video Set.	Adjust Video	
FP Image	Both Show	
Power Button	OFF	
Language	ENG	

OK(M/<-)

Back(ESC)

- Press ▶ 3x times to select MISC SET
- Press OK

- Press ◀ ▶ to change the value of the desired field or enter text

5.8 Pendrive (USB)

PenDrive

Download

Upload

Back(ESC)

- Select PENDRIVE on the MAIN MENU
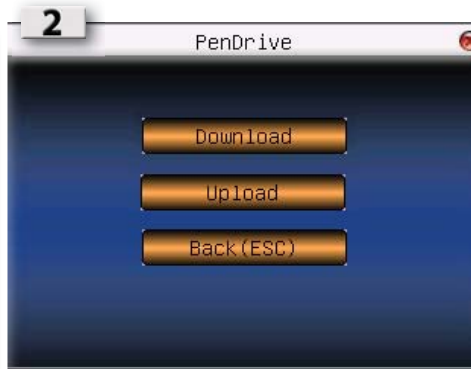
- Insert a PENDRIVE (USB) and select desired option

5.9 Auto Test

Auto Test

All Test

TFT Test

Audio Test

Keyboard Test

Sensor Test

RTC Test

- Select AUTO TEST on the MAIN MENU

- Select the desired field for testing

Summary

* Ensure device settings are correct when installing the device
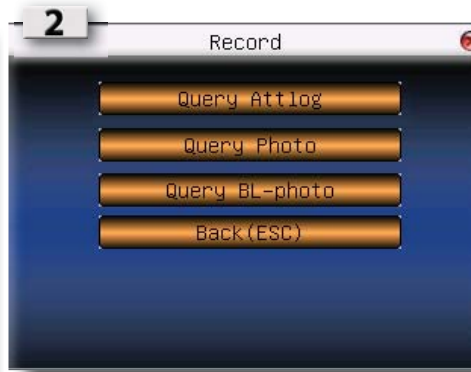
* Pendrive / USB can be used to upload and download user ID's

* Ensure to run a AUTOTEST to test all functions on unit

5.10 Record

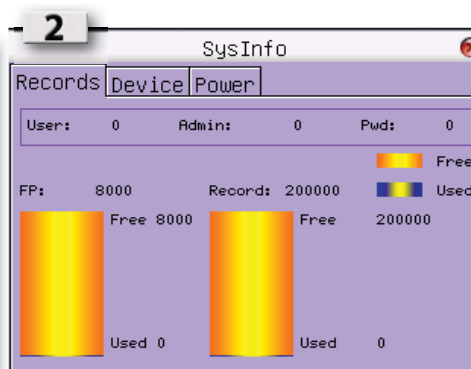- Select RECORD on the MAIN MENU

- Select option to run desired query on
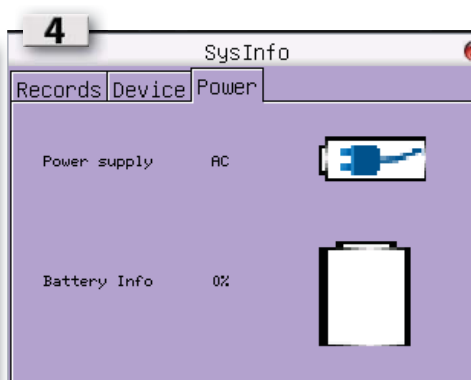
5.11 System Information

- Select SYS INFO on the MAIN MENU

- Press ▶ to select desired info page

- RECORD screen

- DEVICE info screen

- POWER info screen

25

5.11.1 Number of Password Users Available in the Terminal (Password User)

Users can do verification using PIN password and a combination of fingerprint and password. To find out how many users are using password:

• Press Menu > Sys Info > Password User > View the number

5.11.2 Number of Time Scanners Have Been Used for Verification (S Logs)

S logs stands for scanner logs, which means the number of times the scanner has been used for verification, regardless of whether it is successful or not. To view the scanner logs:

• Press Menu > Sys Info > Record > Amount of transactions USED / FREE

5.11.3 Free Space Information (Free Space)

Find out the information about availability of space in your terminal through this function.

• Press Menu > Sys Info > Free Space > Free = number available

5.11.4 Device Information (Dev Info)

Find out the information about your terminal through this function. Press Menu > Sys Info > Dev Info > View the info

Information available includes:

• **AttLog (10k)**: Shows the number of attendance logs that can be stored in the terminal, for example for AttLog (10k) 12 means 10,000 x 12 = 120,000

• **S Logs**: Shows the number of Scanner Logs available for the terminal.

• **Manufactured Time (Manu Time)**: The date and time when the terminal was produced is displayed when you press Manu Time

• **Serial Number of the Terminal (Serial Num)**: The Serial number is pasted on the back of the terminal but in case the sticker is damaged, this is where you can retrieve the serial number.

• **Manufacturer:** Get the name of the manufacturer of the terminal here.

• **Device Name**: All models have different names. If you don't know the name of the terminal that you are having, get it here.

• **Algorithm Version**: This is where you can find terminal's algorithm version.

• **Firmware Version**: Support sometimes require a firmware version to resolve some support issues. The version and date of the version is released is provided here. **For example**: Ver 6.20 Aug 19 2009

• **View MAC**: This feature is a security feature of the products. Linking Software to the terminal requires the correct MAC address. Without availability of MAC address, the software will not be activated correctly. All products are supplied with the correct MAC address to ease communication. This is also to hinder people from using the software with a different hardware brand. An example of a MAC address is 00:0A:5D F1 BE 57.

• Press Menu > Sys Info > Dev Info > View MAC

ZKSoftware®
The Advanced Biometric Solution