IN01 Time & Attendance and Access Control Terminal

USB UNIVERSAL SERIAL BUS

TCP/IP

Colour TFT Screen

User Manual

Version 1.1

Date: November 2011

ZKSoftware®

Advanced Biometric and RFID Solutions

Table of contents

Table of contents...continue 1

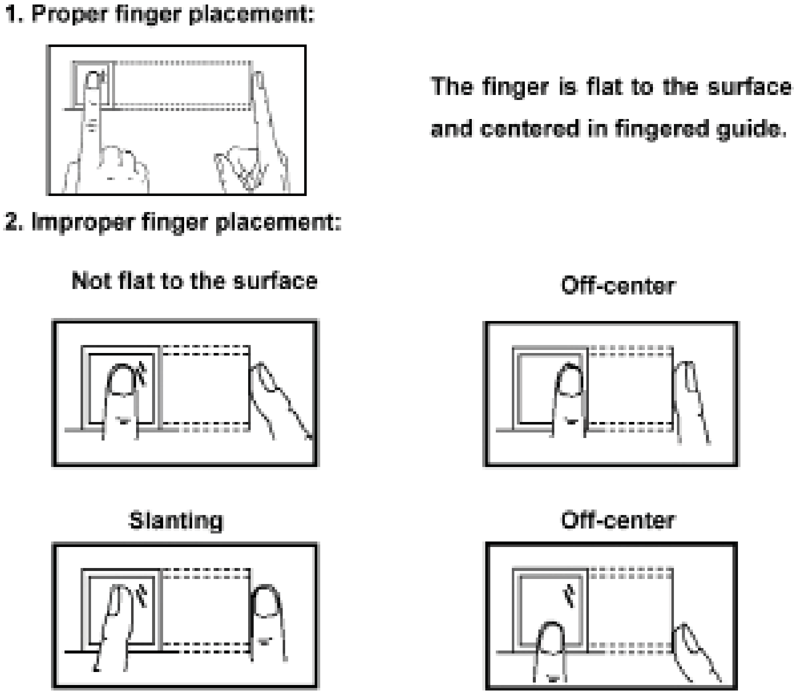
1. Getting started

1.1 Fingerprint Placement

Summary

* Please ensure correct placement of finger on reader.

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).

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

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.

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.

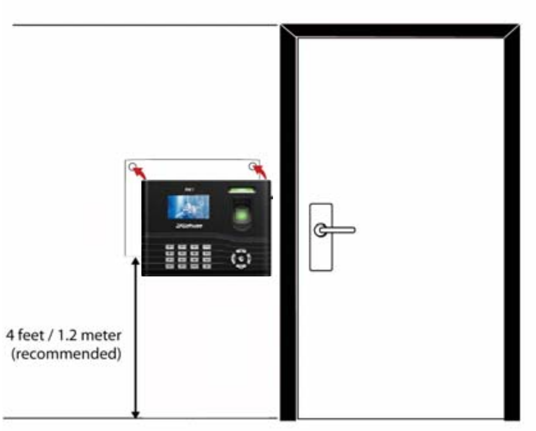
2.2 Important Safeguards

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.

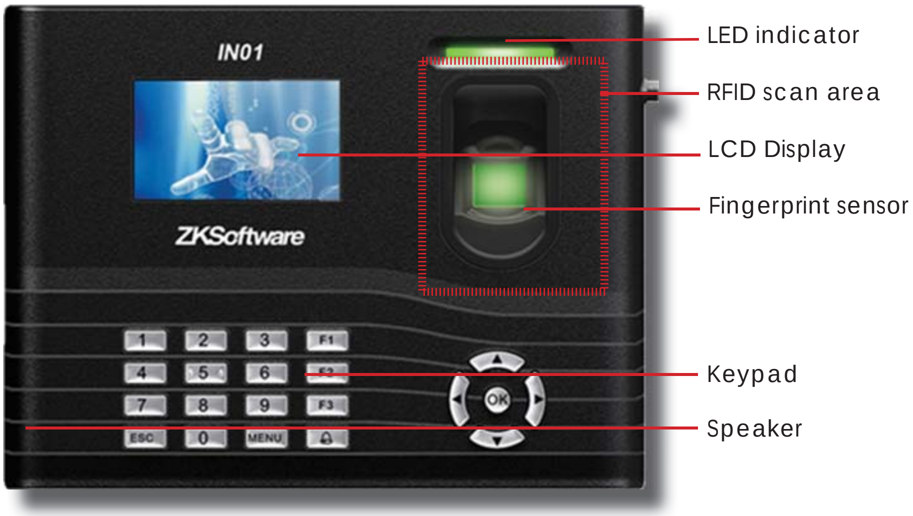
2.2.2 Use of Sensor

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.



2.2.3 Product Appearance

Front view:



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

Summary

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

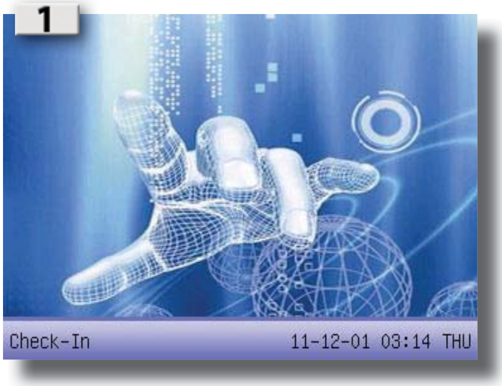
* Ensure the correct date & time on the unit.

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.

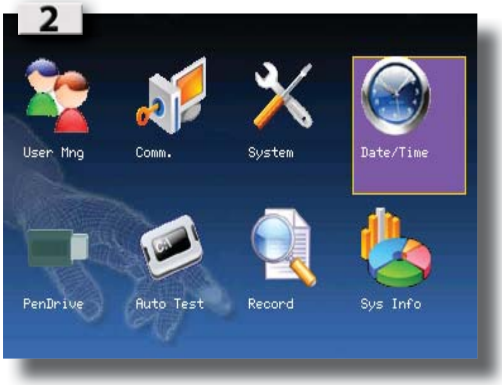
1



Check-In 11-12-01 03:14 THU

- Press M/↵ (menu) once

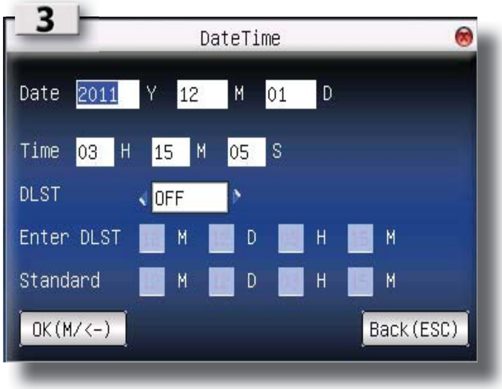
2



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

* Enter the correct date & time in the required fields

3



DateTime

Date 2011 Y 12 M 01 D

Time 03 H 15 M 05 S

DLST OFF

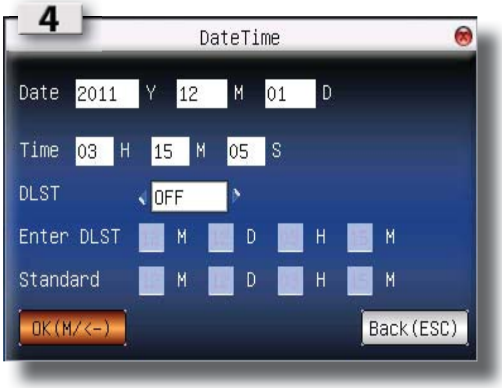
Enter DLST M D H M

Standard M D H M

OK(M/<-) Back(ESC)

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

4



DateTime

Date 2011 Y 12 M 01 D

Time 03 H 15 M 05 S

DLST OFF

Enter DLST M D H M

Standard M D H M

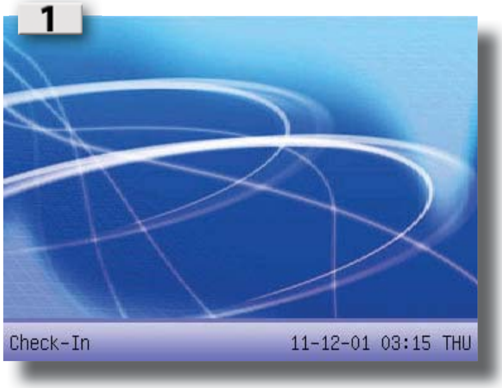
OK(M/<-) Back(ESC)

- Press OK once to confirm settings.

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.

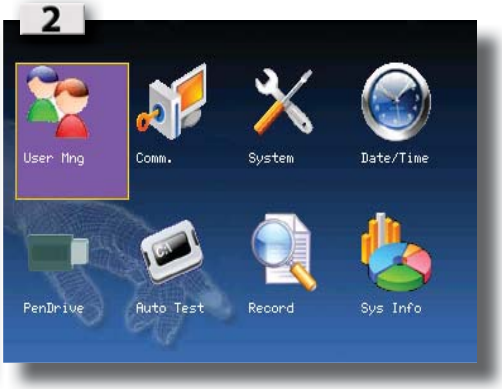
1



Check-In 11-12-01 03:15 THU

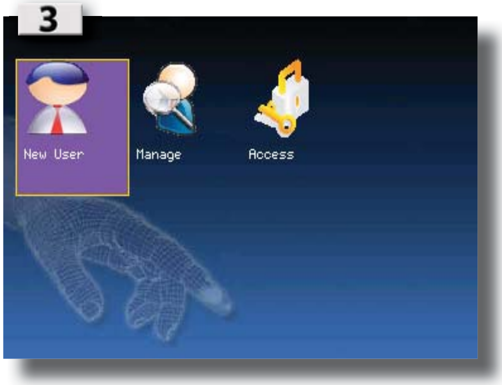
- Press M/↵ (menu) once

2



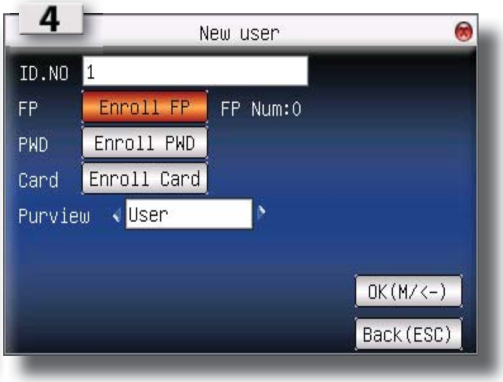
- Press OK (menu) once

3



- Press OK (menu) once

4



New user

ID.NO 1

FP Enroll FP FP Num:0

PWD Enroll PWD

Card Enroll Card

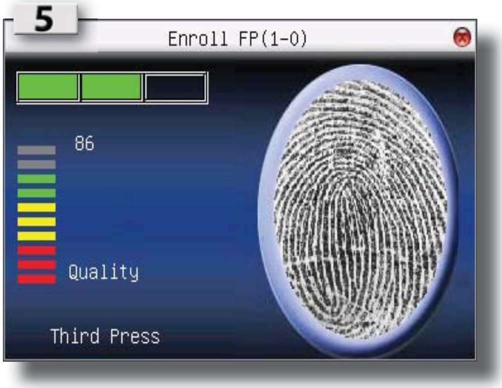
Purview User

OK(M/<-)

Back(ESC)

- Press ▼ 2 times to enrol fingerprint
- Press OK

5



Enroll FP(1-0)

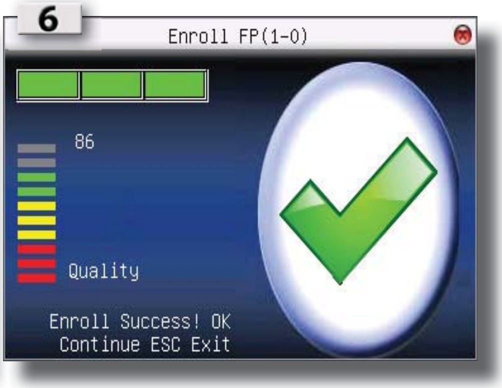
86

Quality

Third Press

- Press desired finger 3x times on sensor to enrol

6



Enroll FP(1-0)

86

Quality

Enroll Success! OK Continue ESC Exit

- Press OK once to enrol more
- Press ESC to exit

Summary

* Ensure to enrol an administrator on the unit.

* FP = Fingerprint

* PWD = Password / pin

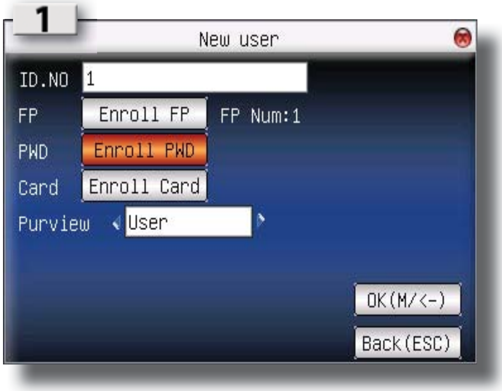
* User = No administrative rights on the unit

* Admin = Full control of unit

* Ensure a good quality fingerprint

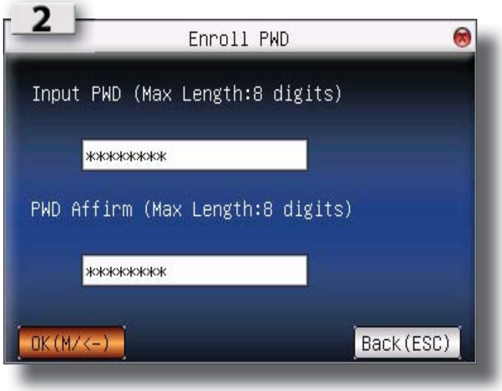
2.6 Password Enrolment

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



ID.NO 1
FP Num:1
Purview User

- Press ▼ 3x times to enrol passowrd

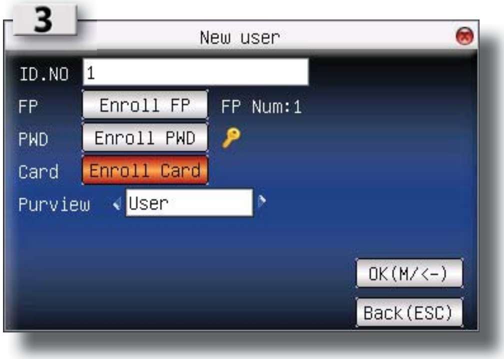


Input PWD (Max Length:8 digits)
****
PWD Affirm (Max Length:8 digits)
****

- Type a numeric password in the fileds
- Press OK to enter

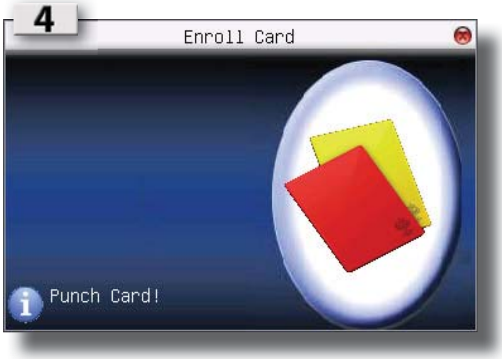
2.7 RFID Card Enrolment

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



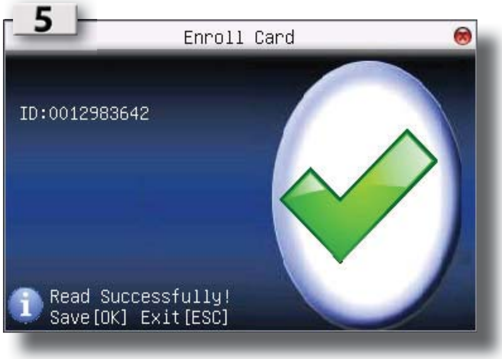
ID.NO 1
FP Num:1
Purview User

- Press ▼ 4x times to enrol a RFID card



Punch Card!

- Punch the card to enrol



ID:0012983642
Read Successfully!
Save[OK] Exit[ESC]

- Confirmation of enrolment
- Press OK to save OR
- Press ESC exit

Summary

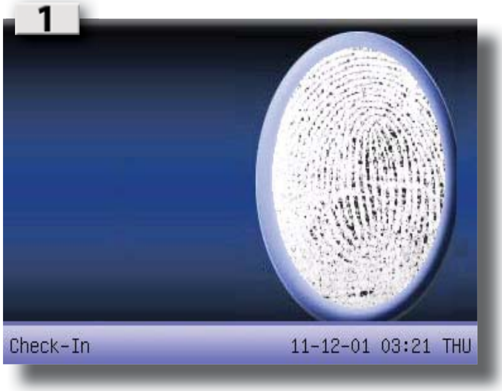
* Password may contain numbers ranging from 1 - 8 digits.

* RFID card is for added security on the unit, or if the user can't use a fringerprint

2.8 Fingerprint & Password Verification

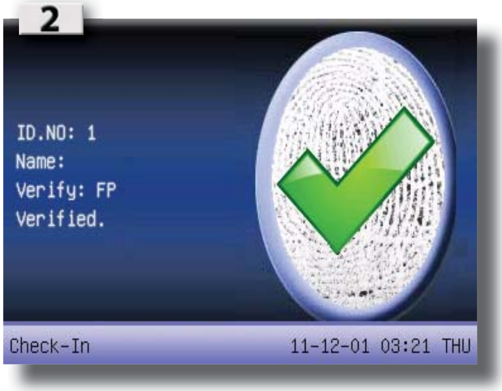
2.8.1 Fingerprint verification

1


Check-In 11-12-01 03:21 THU

- Press fingerprint for verification

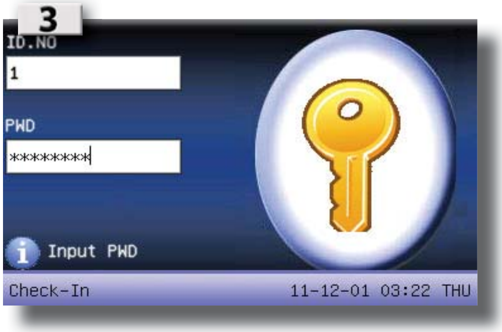
2


ID.NO: 1
Name:
Verify: FP
Verified.

Check-In 11-12-01 03:21 THU

2.8.2 Password verification

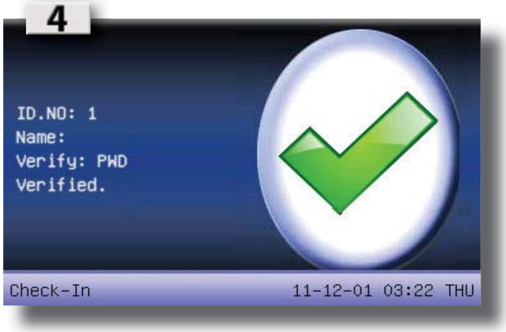
3


ID.NO
1
PWD
****
Input PWD

Check-In 11-12-01 03:22 THU

- Type your password for verification

4

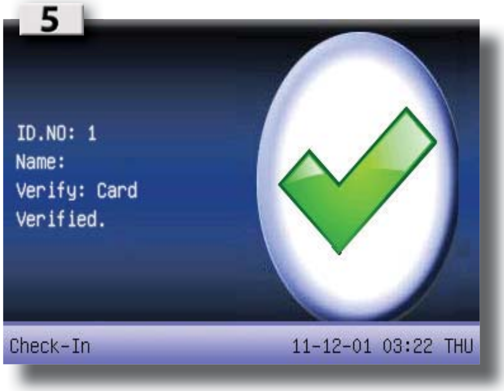

ID.NO: 1
Name:
Verify: PWD
Verified.

Check-In 11-12-01 03:22 THU

- Successful verification

2.8.3 Card verification

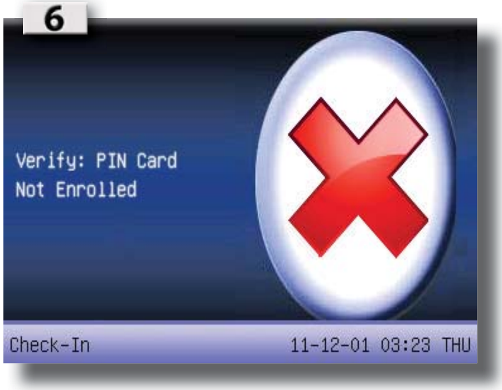
5


ID.NO: 1
Name:
Verify: Card
Verified.

Check-In 11-12-01 03:22 THU

- Punch your card for verification

6


Verify: PIN Card
Not Enrolled

Check-In 11-12-01 03:23 THU

- Declined verification will indicate the image above.

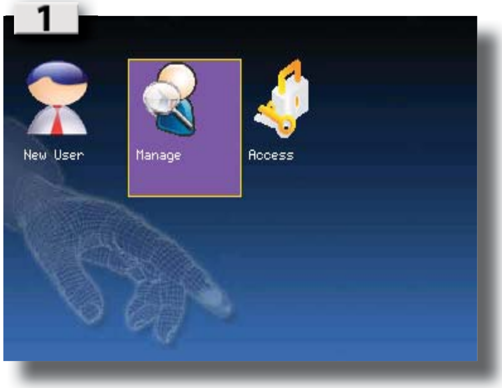
Summary

*Take note of verification screens

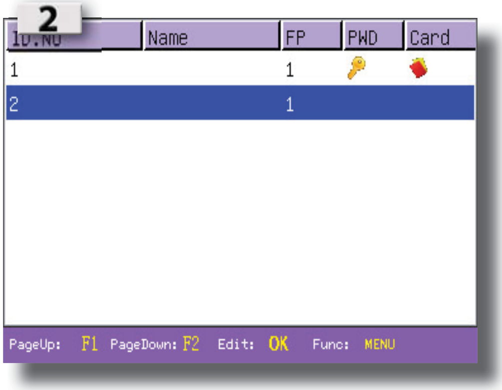
* Declined verification will show on screen.

2.9 Manage Users

2.9.1 Search User

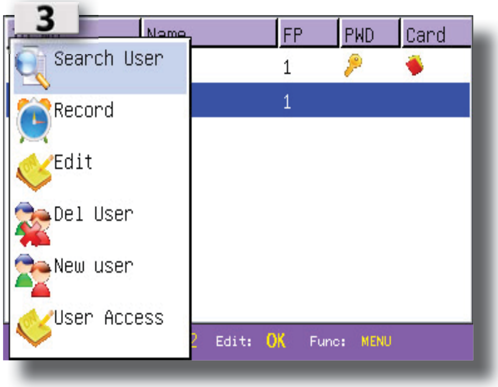


- Press M/↵ (menu) once
- Press OK
- Press ▶ once
- Press OK

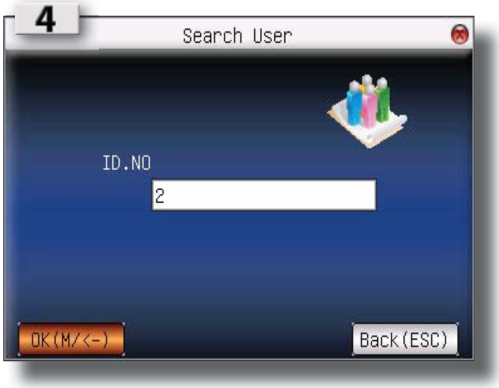


ID.NO	Name	FP	PWD	Card
1		1	🔑	●
2		1		

- Press ▼ to selected user



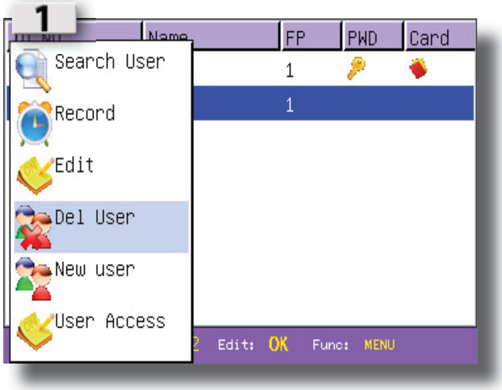
- Press M/↵ (menu) for options window
- Select SEARCH USER
- Press OK



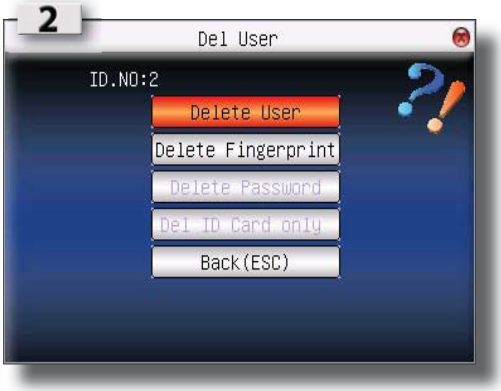
ID.NO 2

- Type in the desired user id to search

2.9.2 Delete user



- Select DEL USER to enter delete options



ID.NO:2

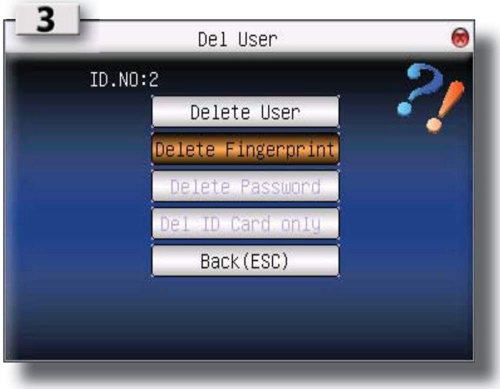
- Delete a single user
- Move down to desired user
- Press OK

Summary

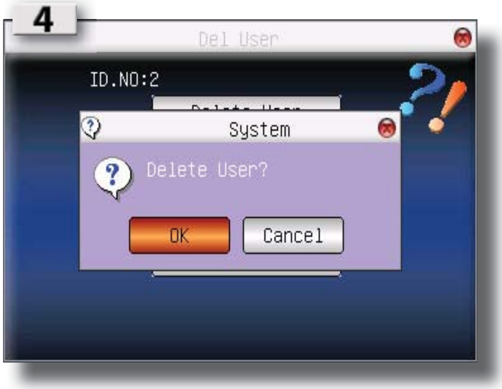
* Take note: Only Administrator can edit / delete users

* Ensure to select correct user ID before deletion

2.9.2 Delete user...continue



- Press ▼ (menu) once to select available options to delete.



Delete User?

- 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.

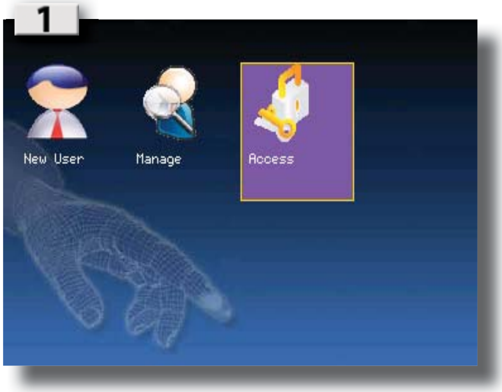
GROUP TIME ZONE	TIME ZONES		
1	2	3	
2			
3			
4			
5			

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

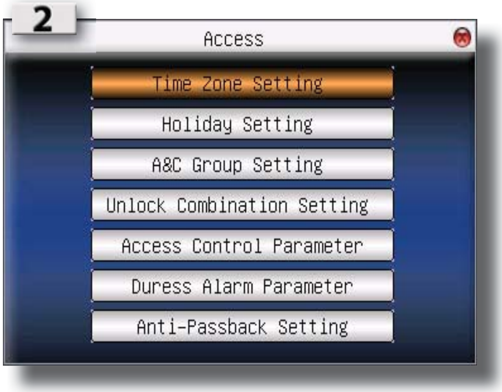
3.2.1 Create a Time Zone

1



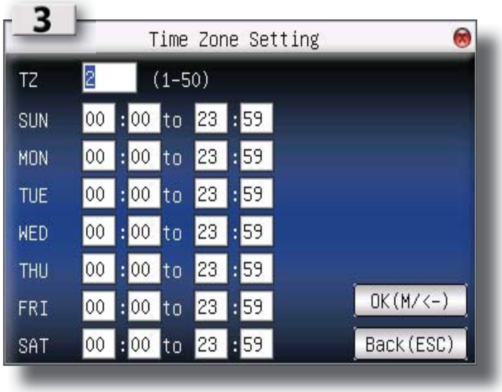
- Press M/↩ (menu) once
- Press OK
- Press ▼ to select ACCESSS
- Press OK

2



- Press OK once

3



Time Zone Setting

TZ 2 (1-50)

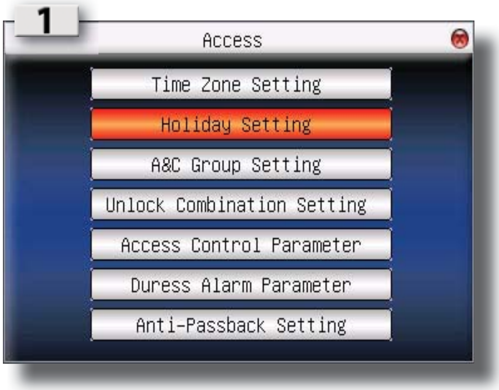
SUN	00	: 00	to	23	: 59	
MON	00	: 00	to	23	: 59	
TUE	00	: 00	to	23	: 59	
WED	00	: 00	to	23	: 59	
THU	00	: 00	to	23	: 59	
FRI	00	: 00	to	23	: 59	OK(M/<-)
SAT	00	: 00	to	23	: 59	Back(ESC)

- Press ▼ to selected field and enter values

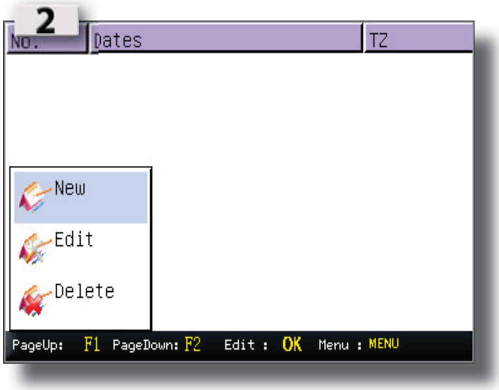
Summary

* Ensure to setup a Time Zone first before assigning users

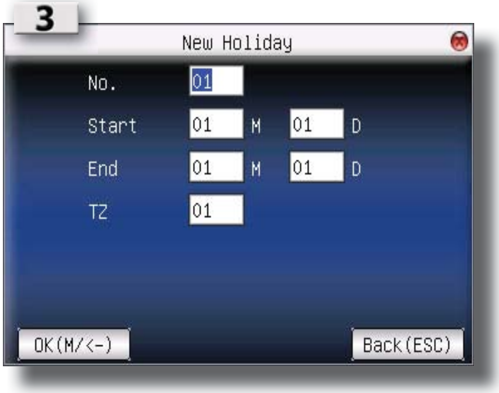
3.2.2 Assign a Holiday Time Zone



- Press ▼ to select HOLIDAY SETTINGS



- Press M/↵ to open options window
- Press OK to create a new settings



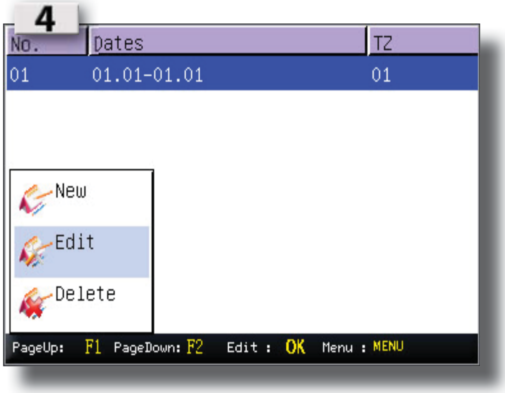
No. 01

Start 01 M 01 D

End 01 M 01 D

TZ 01

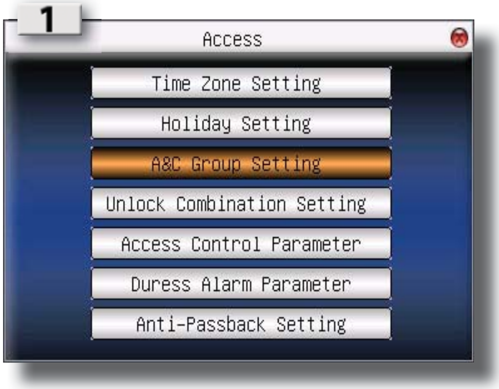
- Insert values
- Press OK to save



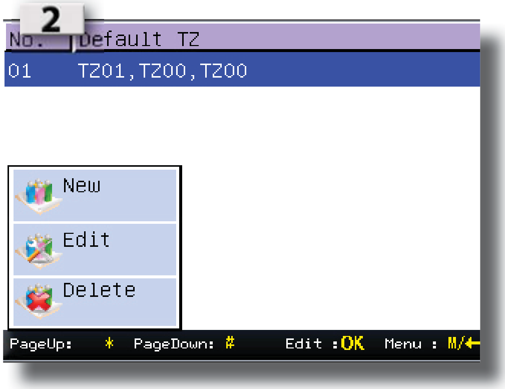
No.	Dates	TZ
01	01.01-01.01	01

- EDIT / DELETE are available to change and delete

3.2.3 Create or Edit a Access Control Group setting



- Press ▼ to select A&C SETTINGS



No.	Default TZ
01	TZ01,TZ00,TZ00

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

Summary

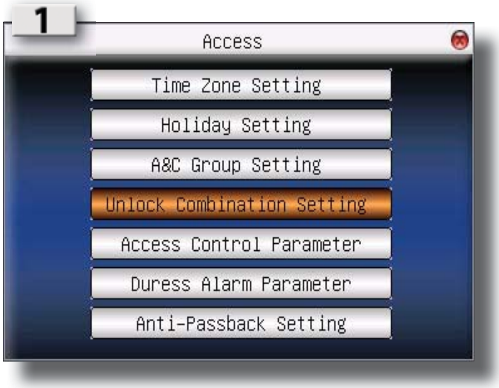
* Ensure to capture all holidays when setting up.

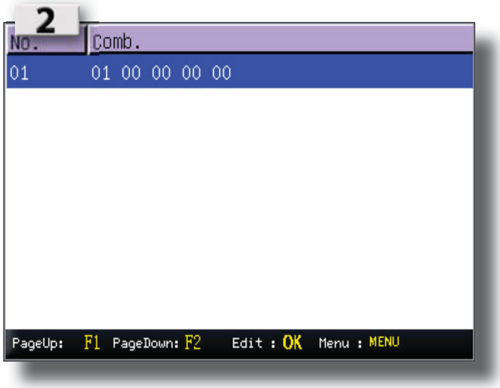
* Recommended to create holiday time zones to deny access, rather than deny access per user for holidays

* 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.





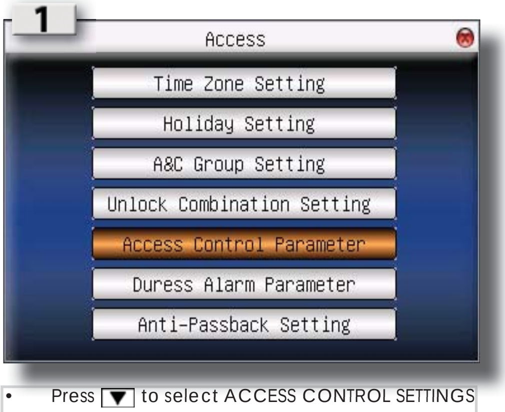
No.	Comb.
01	01 00 00 00 00

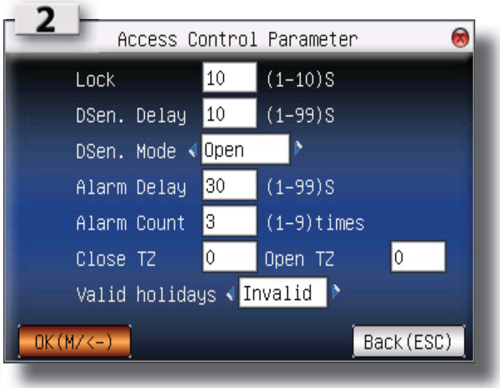
PageUp: F1 PageDown: F2 Edit : OK Menu : MENU

- Press ▼ to select UNLOCK COMB SETTINGS
- Press OK

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

3.2.5 Change Access Control Parameters settings

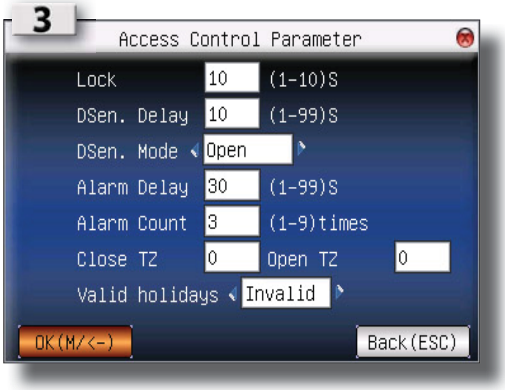




Lock 10 (1-10)S
DSen. Delay 10 (1-99)S
DSen. Mode Open
Alarm Delay 30 (1-99)S
Alarm Count 3 (1-9)times
Close TZ 0 Open TZ 0
Valid holidays Invalid

- Press ▼ to select ACCESS CONTROL SETTINGS
- Press OK

- Press ▼ to select field and change values



Lock 10 (1-10)S
DSen. Delay 10 (1-99)S
DSen. Mode Open
Alarm Delay 30 (1-99)S
Alarm Count 3 (1-9)times
Close TZ 0 Open TZ 0
Valid holidays Invalid

- 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

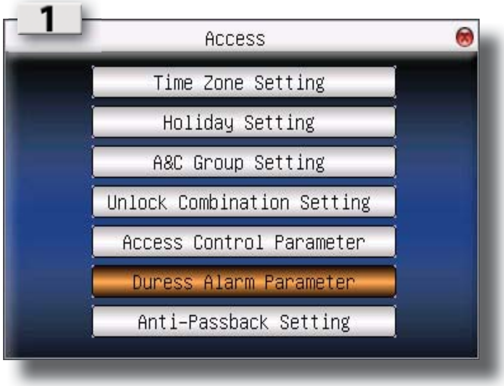
* 2 or more user verification needed before access allowed

* Parameter settings is to change the control of the unit

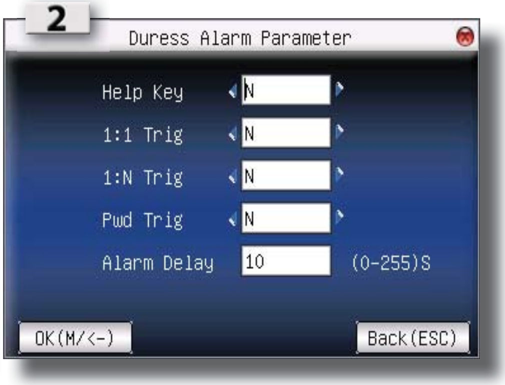
3.2.6 Duress Alarm Parameters

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.

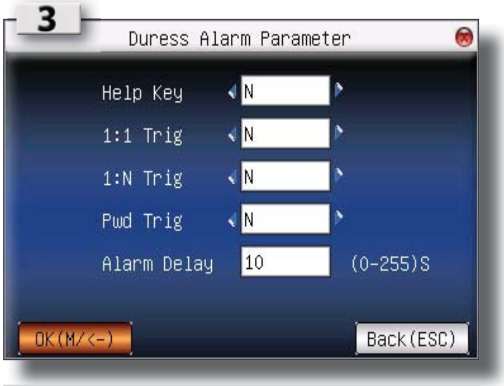


- Press ▼ to select DURESS ALARM SETTINGS
- Press OK



Help Key N
1:1 Trig N
1:N Trig N
Pwd Trig N
Alarm Delay 10 (0-255)S

- Press ▼ to select value field
- Press ◀ ▶ to change options



Help Key N
1:1 Trig N
1:N Trig N
Pwd Trig N
Alarm Delay 10 (0-255)S

- 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.

Summary

* Duress finger enrolment for added security, especially in high risk areas.

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.

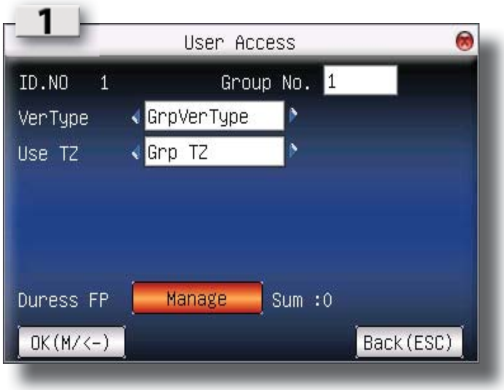
* Enrol 2x or more fingerprints to assign a fingerprint.

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

Define a duress finger...continue

Summary

1


User Access

ID.NO 1 Group No. 1

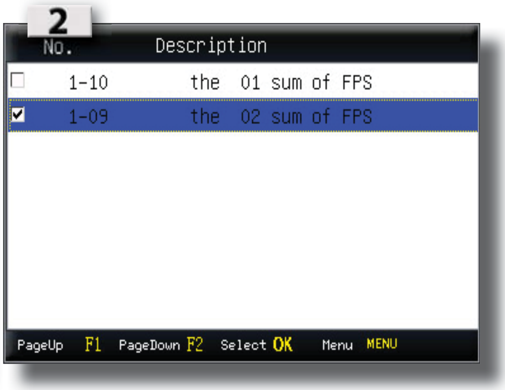
VerType GrpVerType

Use TZ Grp TZ

Duress FP Manage Sum :0

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

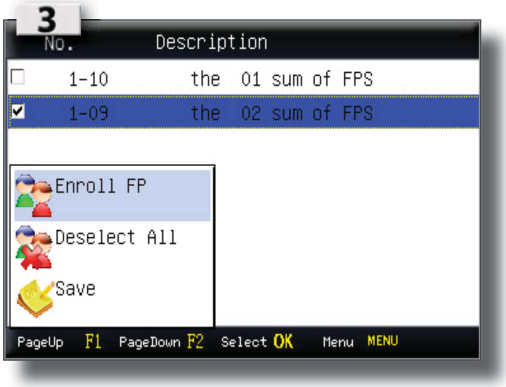
2



	No.	Description
□	1-10	the 01 sum of FPS
☑	1-09	the 02 sum of FPS

- The following screen will display

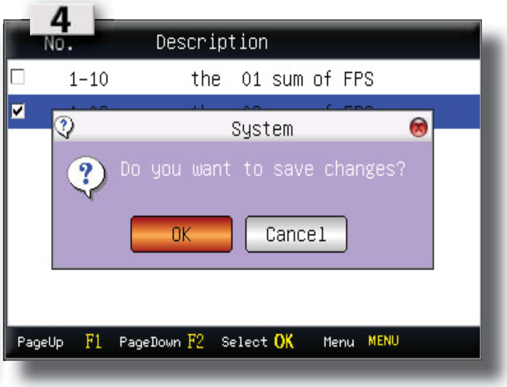
3



	No.	Description
□	1-10	the 01 sum of FPS
☑	1-09	the 02 sum of FPS

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

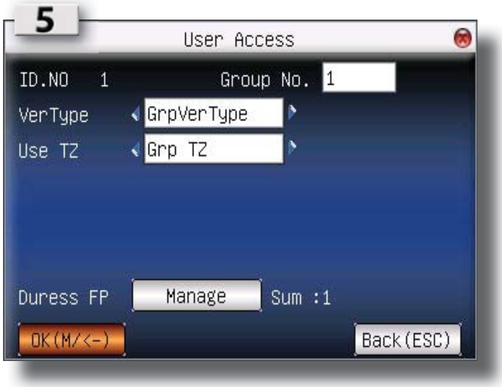
4


System

Do you want to save changes?

- Press OK to save

5


User Access

ID.NO 1 Group No. 1

VerType GrpVerType

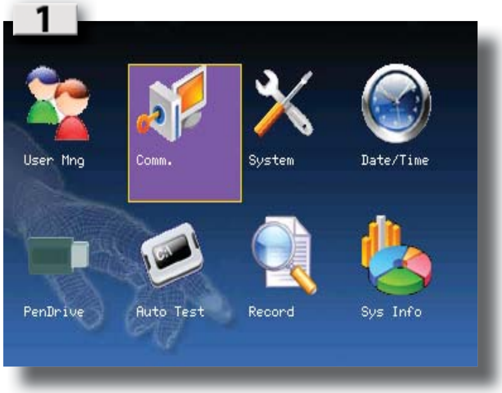
Use TZ Grp TZ

Duress FP Manage Sum :1

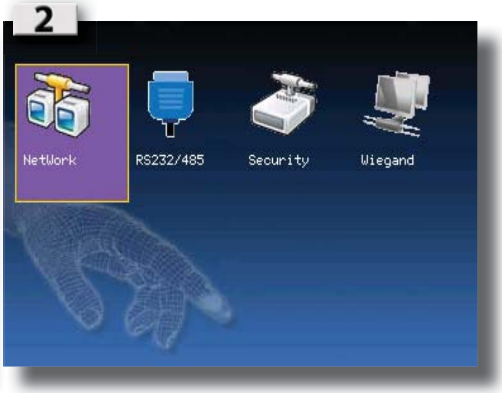
- Press OK to exit

4. Communications

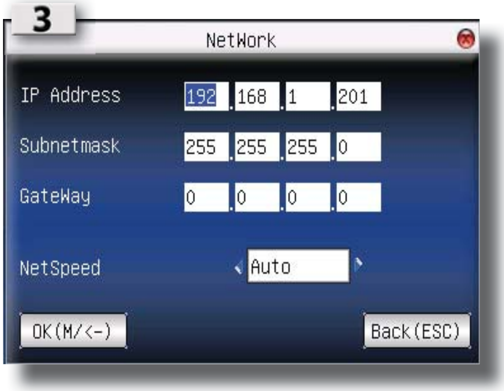
4.1 Network (TCP/IP)

1


- Press [M/↵] once
- Press ▶ once
- Press OK

2


- Press OK on NETWORK

3

NetWork

IP Address 192 168 1 201

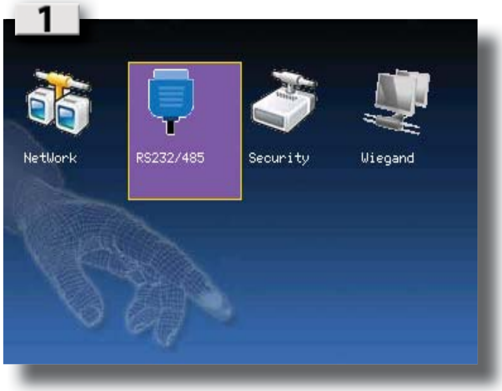
Subnetmask 255 255 255 0

GateWay 0 0 0 0

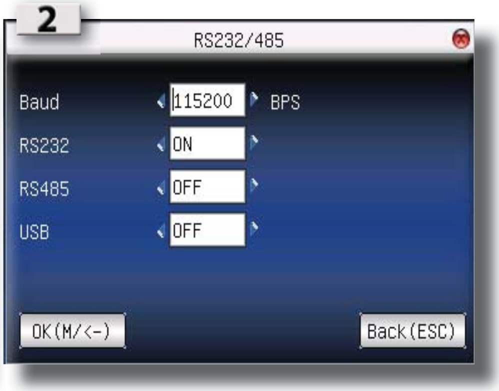
NetSpeed Auto

- Press ▼ to desired field, and complete the values

4.2 RS232 / 485

1


- Press ▶ once to select RS232/485
- Press OK

2

RS232/485

Baud 115200 BPS

RS232 ON

RS485 OFF

USB OFF

- Press ▼ to select field
- Press ◀ ▶ to change values

Summary

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

* Recommended distance

** RS232 = 20m - 60m

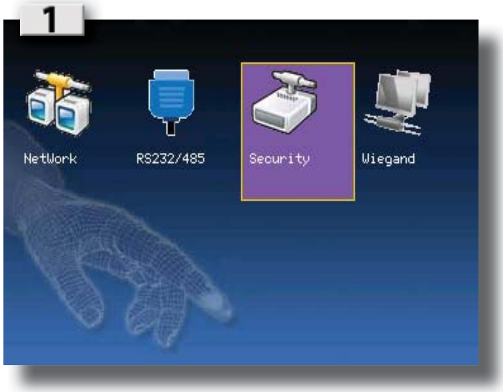
*** Could be affected by distance and power cables running parallel with unit cable

** RS485 = 1000m (max)

*** Could be affected by power cables

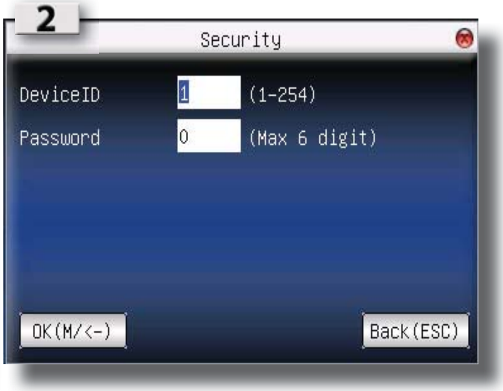
4.3 Security

1



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

2


Security

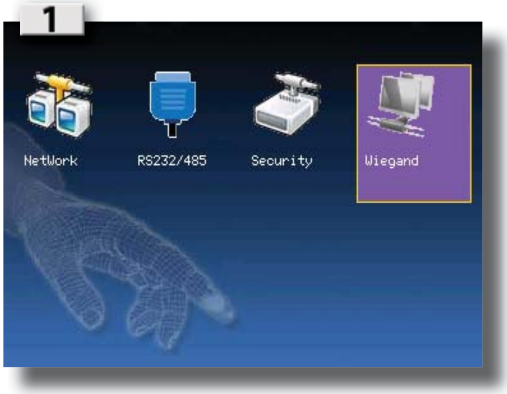
DeviceID 1 (1-254)

Password 0 (Max 6 digit)

- Press ▼ to change values

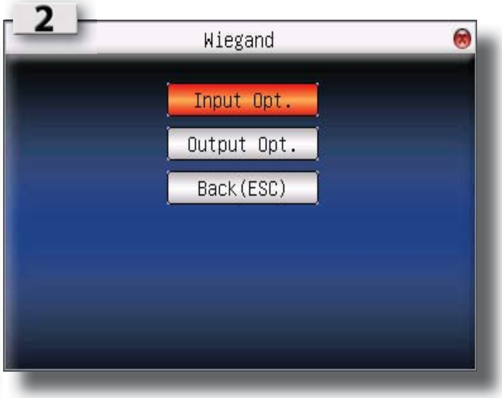
4.4 Wiegand

1



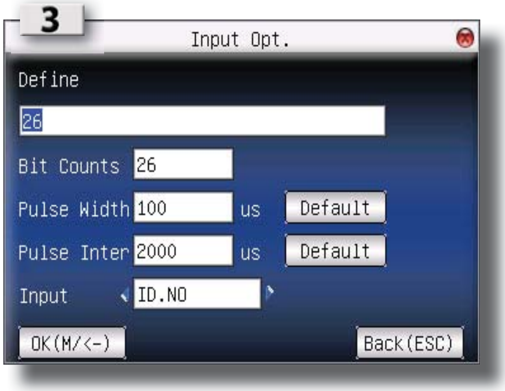
- Press ▶ 3x times to select WIEGAND
- Press OK

2



- Select INPUT OPT

3


Input Opt.

Define

26

Bit Counts 26

Pulse Width 100 us Default

Pulse Inter 2000 us Default

Input ID.NO

- Press ▼ to desired field and enter values
- Press OK to save

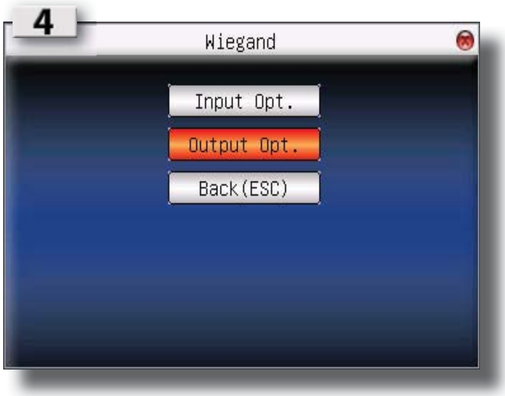
Summary

* Device related password

* Restrict sub-administrator access

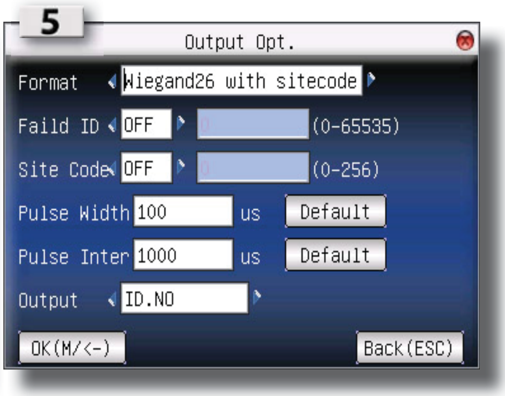
* Use WIEGAND communication port to connect to maglock or turnstiles

4



- Select OUTPUT OPT.

5



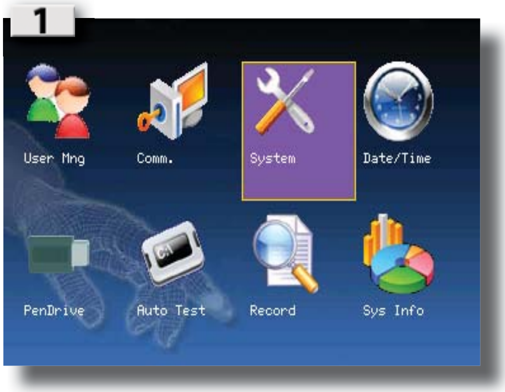
Format Wiegand26 with sitecode
Faild ID OFF (0-65535)
Site Code OFF (0-256)
Pulse Width 100 us
Pulse Inter 1000 us
Output ID.NO

- Press ▼ to select fields
- Press ◀ ▶ to change values or enter values

5. System

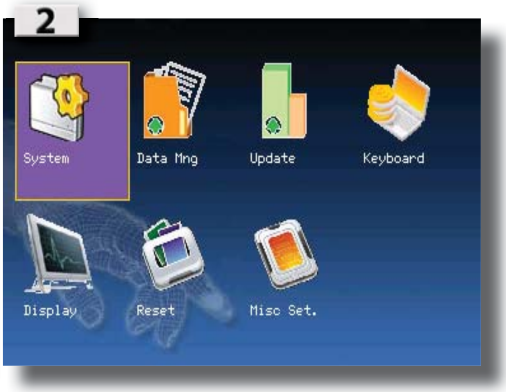
5.1 System settings

1



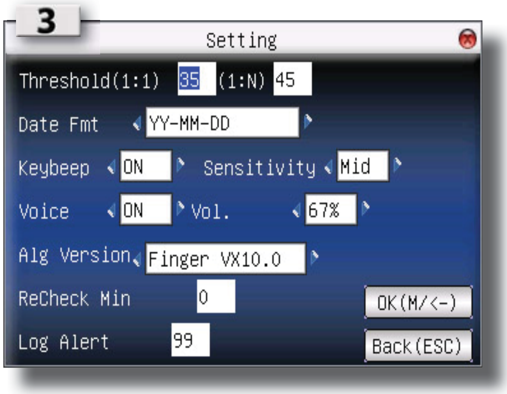
- Press M/↵ once
- Press ▶ 2x times to select SYSTEM

2



- Press OK to enter SYSTEM SETTINGS

3



Threshold(1:1) 35 (1:N) 45
Date Fmt YY-MM-DD
Keybeep ON Sensitivity Mid
Voice ON Vol. 67%
Alg Version Finger VX10.0
ReCheck Min 0
Log Alert 99

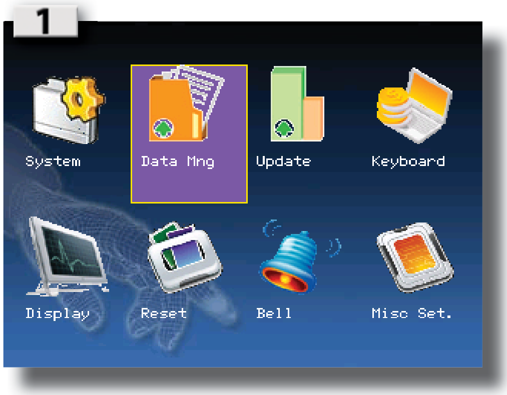
- Press ▼ to scroll down to fields
- Change values

Summary

* Ensure correct system settings before handing over to client.

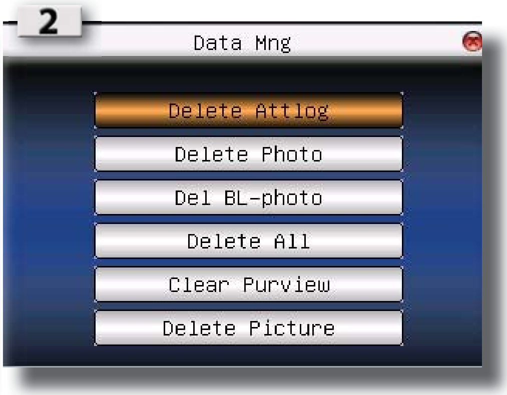
5.2 Data Management

1



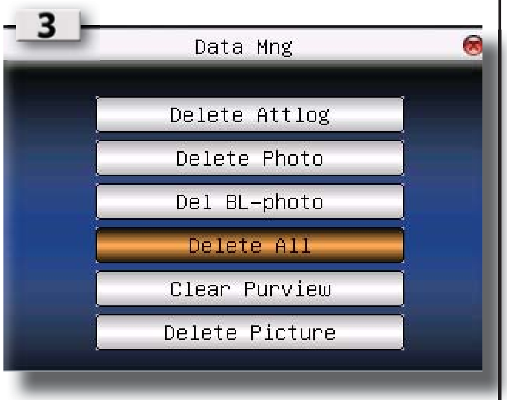
- Press ▶ to select DATA MNG

2



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

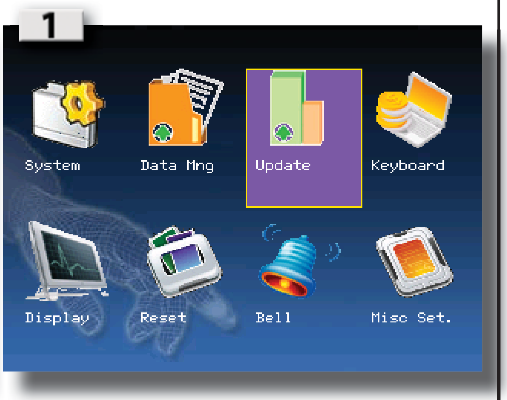
3



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

5.2.1 System Update

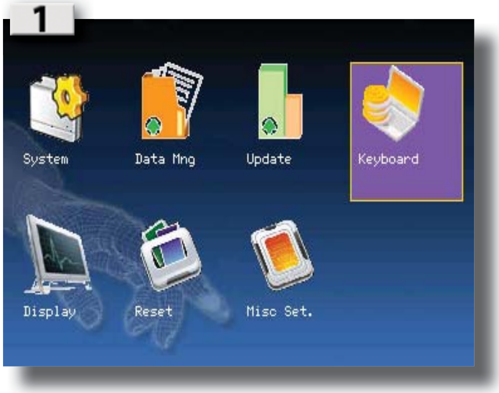
1



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

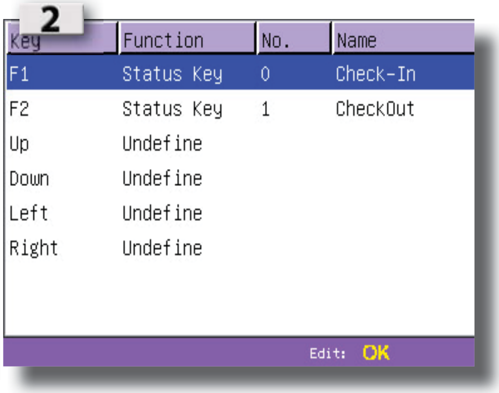
5.3 Keyboard

1



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

2



Key	Function	No.	Name
F1	Status Key	0	Check-In
F2	Status Key	1	CheckOut
Up	Undefine		
Down	Undefine		
Left	Undefine		
Right	Undefine		

Edit: OK

- Press OK to edit selected field

Summary

* Ensure to keep data logs clean, to prevent unit from filling up space.

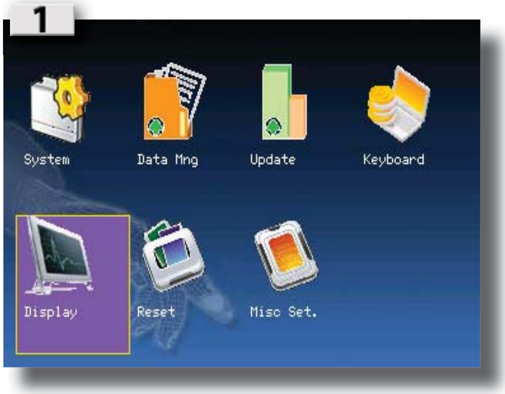
* Ensure to use correct USB drive that is compatible with device.

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

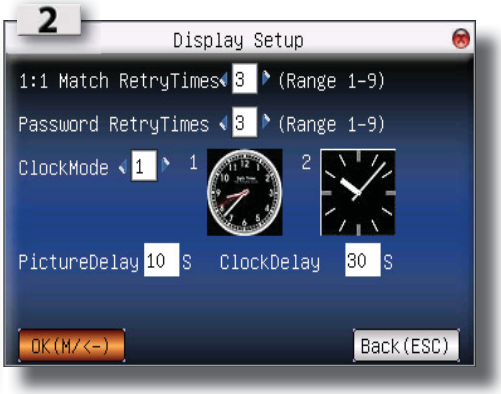
* Assign shortcut for faster access.

* Custom “F” keys to differentiate between access modes

5.4 Display



- Press ▼ to select DISPLAY
- Press OK



1:1 Match RetryTimes ◀ 3 ▶ (Range 1-9)

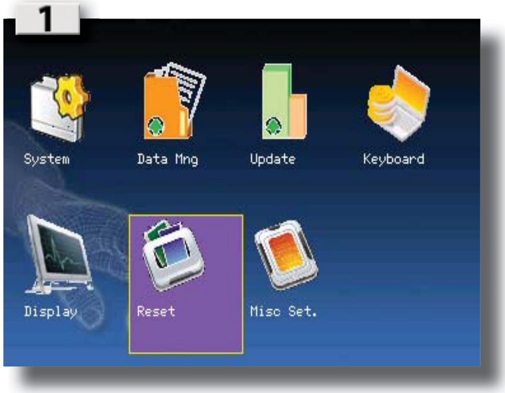
Password RetryTimes ◀ 3 ▶ (Range 1-9)

ClockMode ◀ 1 ▶ 1 2

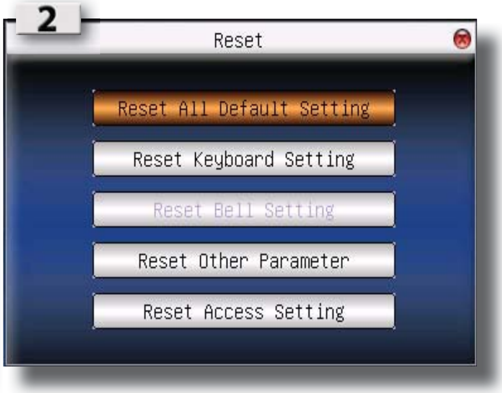
PictureDelay 10 S ClockDelay 30 S

- Press ▼ to select field
- Press ◀ ▶ to change values
- Press OK to save

5.5 System Reset

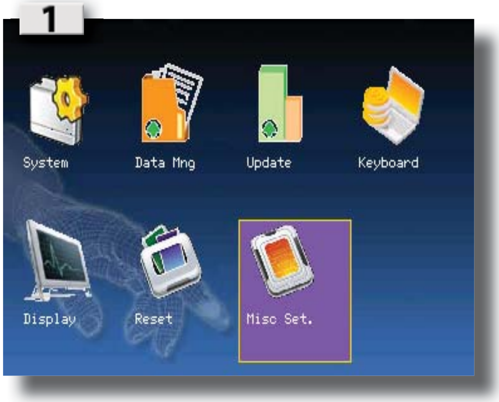


- Press ▶ to select RESET
- Press OK

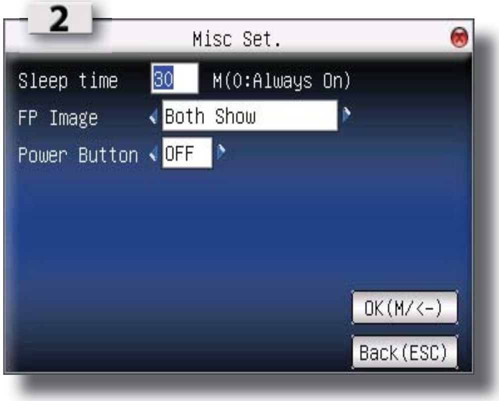


- Select field that needed to be reset
- Press OK to confirm

5.6 Miscellaneous settings



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



Sleep time 30 M(0:Always On)

FP Image ◀ Both Show ▶

Power Button ◀ OFF ▶

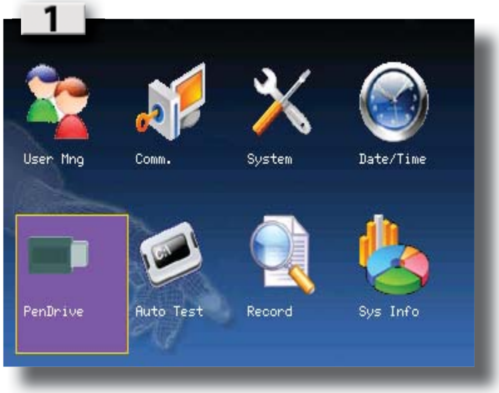
- Press ◀ ▶ to change the value of the desired field or enter text

Summary

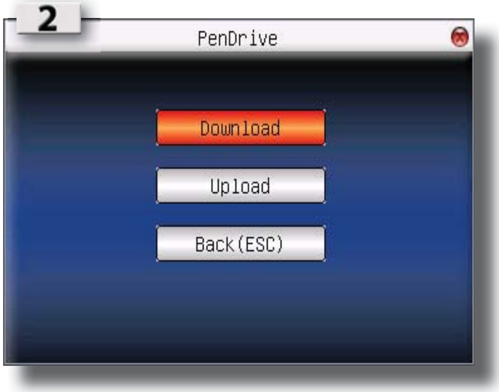
* Reset function are only configuration of unit, and not to delete users

* Ensure device settings are correct when installing the device

5.7 Pendrive (USB)

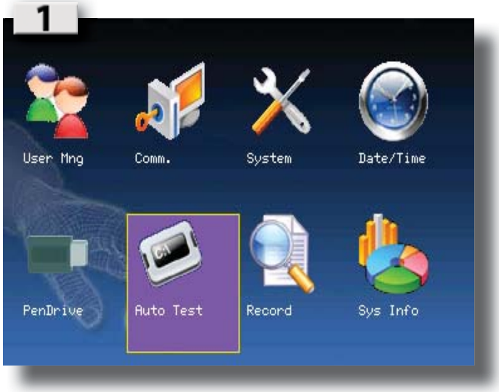


- Select PENDRIVE on the MAIN MENU

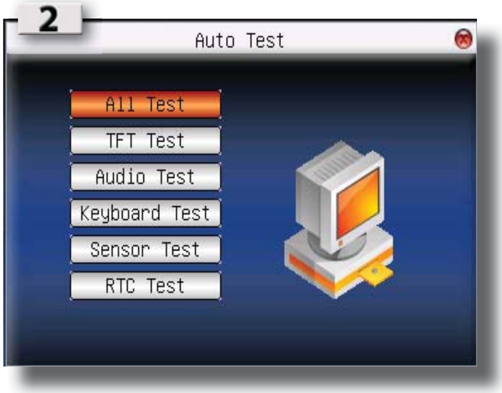


- Insert a PENDRIVE (USB) and select desired option

5.8 Auto Test

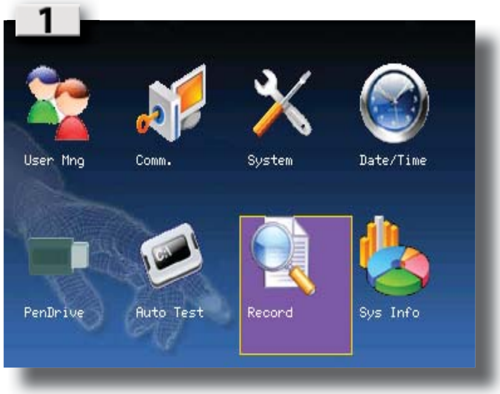


- Select AUTO TEST on the MAIN MENU

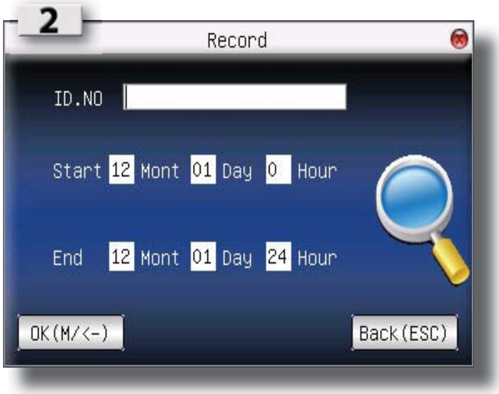


- Select the desired field for testing

5.9 Record



- Select RECORD on the MAIN MENU



ID.NO

Start 12 Mont 01 Day 0 Hour

End 12 Mont 01 Day 24 Hour

- Select option to run desired query on

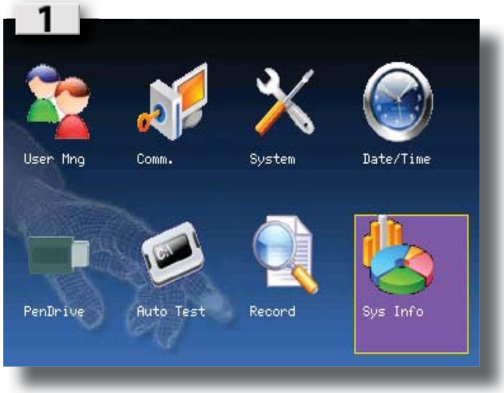
Summary

* Pendrive / USB can be used to upload and download user ID's

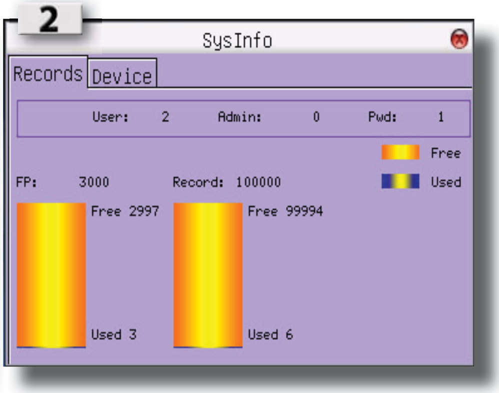
* Ensure to run a AUTOTEST to test all functions on unit

5.10 System Information

Summary



- Select SYS INFO on the MAIN MENU



SysInfo

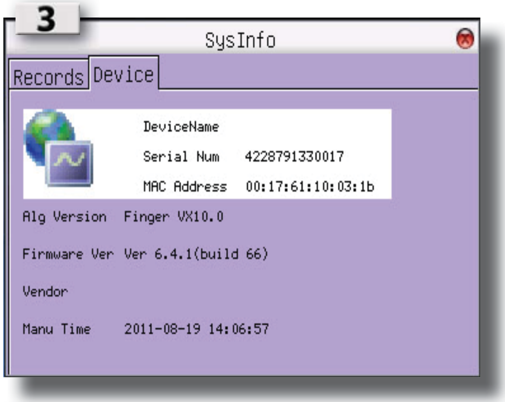
User: 2 Admin: 0 Pwd: 1

FP: 3000 Record: 100000

Free 2997 Free 99994

Used 3 Used 6

- Press ▶ to select desired info page
- RECORD screen



SysInfo

DeviceName

Serial Num 4228791330017

MAC Address 00:17:61:10:03:1b

Alg Version Finger VX10.0

Firmware Ver Ver 6.4.1(build 66)

Vendor

Manu Time 2011-08-19 14:06:57

- DEVICE info screen

5.10.1 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

5.10.2 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

5.10.3 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

5.10.4 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