



Ultra Speed
Fingerprint
Recognition
Algorithm

KJ-3500
USER
MANUAL

VER. 1.05
ENGLISH
www.ekjtech.co.kr

FCC Statement

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.
OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

- 1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

"Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment."

FCC RF

INTERFERENCE STATEMENT

NOTE:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



1. Getting Started

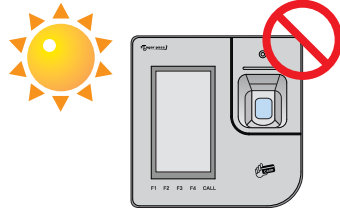
2. Understanding Device

3. Operating Menu

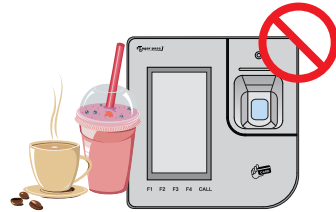
CAUTIONS

Before using this device, read and follow all instructions for safety.

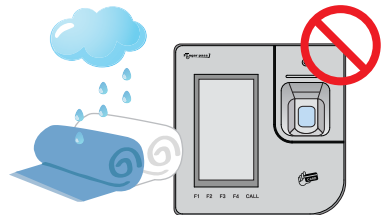
CAUTIONS



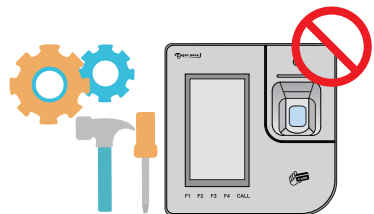
Keep out of direct sunlight and heat radiation sources.



Shall not be exposed to dripping or splashing and no objects filled with liquids, such as vases, shall be placed on the products.



When cleaning, do not use liquid solvent or wet cloth. Wipe with soft cloth.



Never disassemble or modify this device in any way.
(KJ Tech is not liable for problems caused by unauthorized modification or attempted repair)

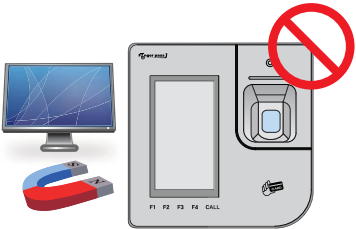


KJ-3500
USER MANUAL ver.1.05
www.ekjtech.co.kr

CAUTIONS

Before using this device, read and follow all instructions for safety.

CAUTIONS



Do not install this device near by TV, monitor or magnetic interference.



If the product fails to operate normally, contact the authorized dealer or service senter.



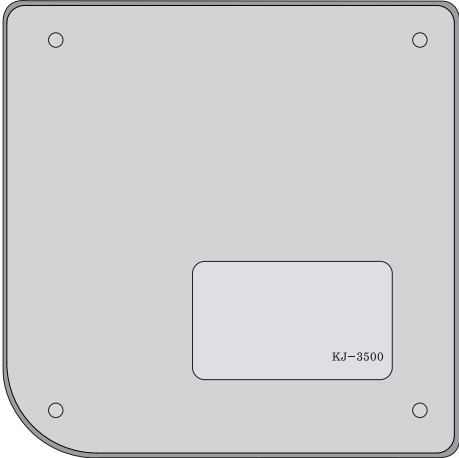
INCLUDED ITEMS

This system comes with the following components.

INCLUDED ITEMS

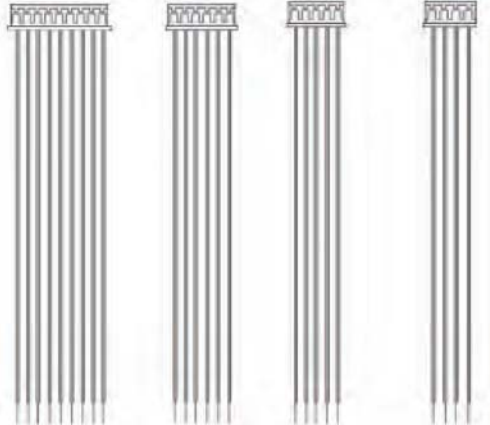


KJ-3500



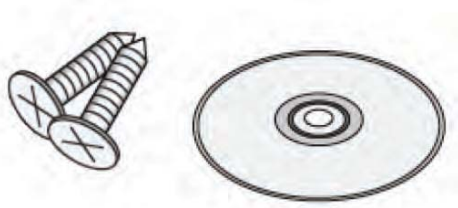
Bracket

Cable



9PIN
6PIN
5PIN
4PIN
(Power, 485 CON)

Screw / Program CD



For bracket 4ea T3x20mm
For KJ-3500(L) 2ea M3x6mm



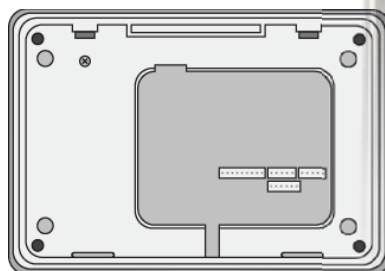
PARTS AND THEIR FUNCTIONS

PARTS AND THEIR FUNCTIONS

Color TFT LCD
Displays time, device status, user list and UI for operation.

Touch Pad
Key button for operation.

Connector
For cable connection.



LED
Light on for system status.

Fingerprint sensor
Used to register or identify the user.

Function Key
selects the events for T&A, Enter, Exit, or navigate The menu.

Speaker
Outputs sounds effect & voice.

E1 E3 E3 E4 CVTT

USB
For USB memory.



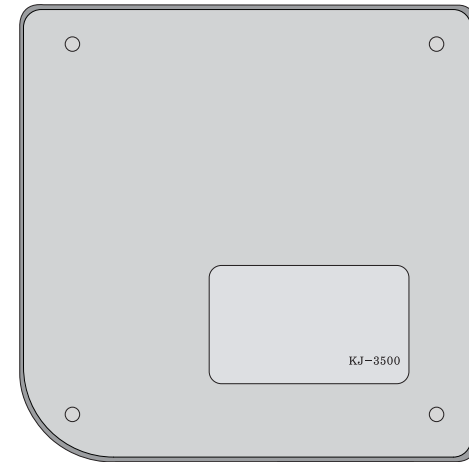
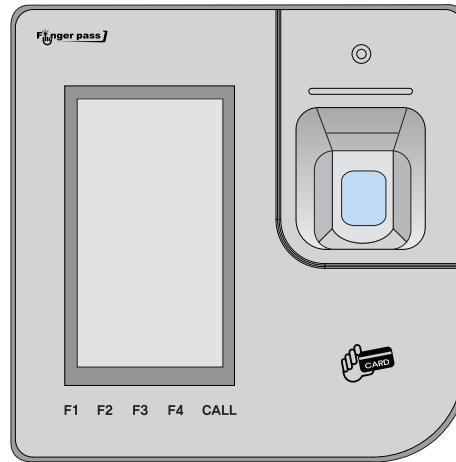
DIMENSIONS

DIMENSIONS

W:165mm

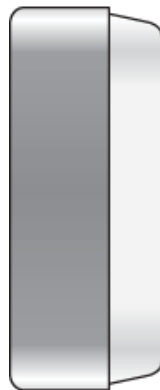
W:149.8mm

H:115mm



H:92.8mm

49mm



FINGERPRINT REGISTRATION

FINGERPRINT REGISTRATION

Place the finger on the sensor as seen in below in the proper way.

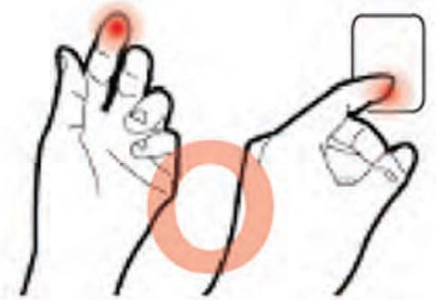
Place the entire area of your finger firmly to the sensor.



You have to register fingerprint in proper way to enhance recognition rate.
Recommended to use finger which has no damage.
Recommended to register more than two fingerprint in case.



Proper way



Improper way.



VERIFICATION MODE

VERIFICATION MODE

Verification mode can be setup
in verification mode
(Settings>Basic>Verification Mode)

CARD



ID(PIN)



FD(Finger Print)



KJ-3300 supports various type of access mode : Combination of Fingerprint, Card and ID(PIN)



FUNCTIONS KEY

Function Key is usually used for Time & Attendance.
The admin is able to setup a certain definition to a function key in the program (F1 = Sing in) The admin is able to find out the users attendance records.

ID Authentication Scheme F1~F4 + 0~9

1. Press Function Key (F1~F4) only or Press numbers after Function Key .
2. Input ID used to enter.

CARD Authentication Scheme F1~F4 + 0~9

1. Press Function Key (F1~F4) only or press numbers after Function Key .
2. Present the card to enter.

FD Authentication Scheme F1~F4 + Fingerprint

1. Press Function Key (F1~F4) only or Press numbers after Function Key .
2. Place Finger Print to enter.

KJ-3500 SYSTEM DIRECTORY ON KEY

KJ-3500 SYSTEM DIRECTORY ON KEY

USER 1.Enroll 2.Delete 3.Set Temp ID

SETTING 1.Basic 2.Advanced 3.AC Setting 4.Communication 5.Schedule 6.Log Setting

USB MEMORY 1.Download General Log 2.Download All General Log 3.Download Management Log
4.Download All Management Log 5.Download User Info 6.Upload User Info
7.Upgrade Firmware

SYSTEM INFO 1.Memory 2.Device Info 3.Advanced

TEST 1.Test All 2.Test Memory 3.Test LCD 4.Test Sound (AUTO) 5.Test Sound (MANUAL)
6.Test Sensor 7.Test Keyboard 8.Test RTC 9.Test Case Status 10.Test Card Reader



KJ-3500 SYSTEM DIRECTORY ON KEY

SETTING 1.Basic 2.Advanced 3.AC Setting 4.Communication 5.Schedule 6.Log Setting

Basic

- 1.Time
- 2.Date
- 3.Date Format
- 4.Language
- 5.Use Busytone detection
- 6. Set Phone Numbers

Advanced

- 1.Verification Mode
- 2.ID Mask
- 3.Use Tamer Alram
- 4.Use Touch Sensor
- 5.Celibrate Senseor
- 6.Restore Factory Settings
- 7.Clear General Log
- 8.Clear Management Log
- 9.Clear Enroll Date

AC Settings

- 1.Define Timezone
- 2.User Timezone
- 3.Lock Type
- 4.Lock Door Release Time
- 5.Door Open Warning
- 6.Re-access Count
- 7.Re-access Limit Time
- 8.Wiegand Format
- 9.Anti-Passback



KJ-3500 SYSTEM DIRECTORY ON KEY

SETTING 1.Basic 2.Advanced 3.AC Setting 4.Communication 5.Schedule 6.Log Setting

Communication

- 1.Device ID
- 2.Baudrate
- 3.TCP/IP Settings
 - DHCP
 - IP Antipass
 - Subnet Mask
 - Default Gateway
 - Port
 - Mac Address
- 4.Communication Password

Schedule

- 1.Set Tmode
- 2.Ring Settings
- 3.Auto Door
- 4.Auto Funckey
- 5.None-Relat Funckey
- 6.Day Light
- 7.Holiday
- 8.Funckey Alarm
- 9.Idle Settings

Log Setting

- 1.Management Log Warning
- 2.General Log Warning





1. Getting Started

2. Understanding Device

3. Operating Menu

DISPLAYS

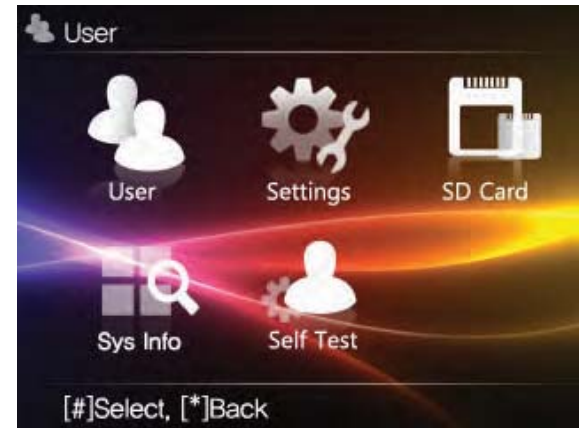
DISPLAYS

These displays are primary screens.



Verification Mode

Date and Time



User Menu



User Enroll Menu



Settings Menu



MEMU NAVIGATION BUTTONS

MEMU NAVIGATION BUTTONS

- F1** Move Forward
- F2** Move Backward
- *** To previous menu
- F4** Home Screen
- #** Select the Menu



ACCESS TO THE SYSTEM MENU 1

ACCESS TO THE SYSTEM MENU 1

Default condition and admin is not registered.



***** > 1 2 3 4 > **#** > Menu Screen

1. Press ***** Button.
2. After "1 2 3 4", Press **#** Button
3. Succeed to access system menu
4. Move between menus using **F1** or **F2** button



1. Getting Started

2. Understanding Device

3. Operating Menu

ACCESS TO THE SYSTEM MENU 2

ACCESS TO THE SYSTEM MENU 2

Only when admin is registered. Refer to “Admin Registration Part” for admin registration.

When admin ID is incorrect, access to the system menu is denied.

When admin ID is not registered anyone can be access to system menu.

So it is highly recommended to register admin More than one.

Unless stated otherwise instructions in this manual starts from system menu.

Admin is registered already.



* > Admin ID > # > Verify Fingerprint or CD > Main menu

1. Press * Button.
2. Press Registered admin ID and *
3. Verify fingerprint or CD of the above ID
4. Succeed to access system menu.
5. Move between menus using F1 or F2 button.
Press * Button at the bottom left corner to return home Screen.



REGISTER

When ADMIN is not registered

***** > 1234 > **#** > User > Enroll

1. Press ***** button
2. After “1 2 3 4”, press **#** button (Access to the system menu)
3. Select “User” and press **#** button
4. Select “Enroll” and press **#** button
5. Input password(USER ID) and set up the privilege;
User or Admin.
(After User ID, press **F1** and set the privilege using the **#** and **F1** button)
6. Register fingerprints and/or card
(Refer to p. 16, Menu Navigation Buttons)

REGISTER

Default admin ID is 1234.
When the new admin is registered,
1234 does not work anymore.

Tip : In case of the absence of
the admin, multiple admin is
recommended

REGISTER

When ADMIN is not registered

* > Admin ID > Admin verification > User . Enroll

1. Press * button
2. After “Admin ID”, press # button
3. Verify Fingerprint or CD of the above Admin ID
(Access to the system menu)
4. Select “Enroll” and press # button
5. Input password(USER ID) and set up the privilege ; User or Admin.
(After User ID, press F1 and set the privilege using the # and F1 button)
6. Register fingerprints and/or card
(Refer to p. 16, Menu Navigation Buttons)



USER REGISTRATION

If doesn't need 2nd fingerprint or CARD, it is possible to skip this process

USER REGISTRATION

1. Access to the system menu
(Refer to P. 17 or P. 18 for access to the system menu)
2. Go to "User" > "Enroll" > **#** to process
3. Input password ("User ID") and **#**
4. Register 1st fingerprint
5. Scan fingerprint 3times for one registration
6. Complete the registration of 1st fingerprint
7. Press ***** button and back to no. 4
(If want to register one fingerprint only, press F4 button an back to home screen)
8. Select 2nd fingerprint
9. Scan 2nd fingerprint three times
10. Complete fingerprint registration
(If want to register fingerprint only, press **F4** button an back to home screen)
11. Press ***** button and back to no. 4 for Card
12. Select Card
13. Present the card and read card data
14. Press **#** button
15. Complete registration
- 16 Press **F4** and back to home screen



ADMIN REGISTRATION

If doesn't need 2nd fingerprint or CARD, it is possible to skip this process

ADMIN REGISTRATION


1. Access to the system menu
(Refer to P. 17 or P. 18 for access to the system menu)
2. Go to "User" > "Enroll" > # to process
3. Input password ("User ID") and #
4. Move to privilege using F1 or F2 and select "Admin" using
(Privilege F1 > # > Admin > F1 > # > OK > F1 > #)
5. Move to OK and press
6. Register 1st fingerprint
7. Scan fingerprint three times
8. Complete the registration of 1st fingerprint
(If want to register one fingerprint only, press F4 button an back to home screen)
9. Press * button and back to no. 6 to register 2nd fingerprint and repeat the same process
10. Select 2nd fingerprint
11. Scan 2nd fingerprint three times
12. Complete fingerprint registration
(If want to register fingerprint only, press F4 button an back to home screen)
13. Press * button and back to no. 6 for Card
14. Select Card
15. Present the card and read card data
16. Press # button
17. Complete the registration
18. Press F4 and back to home screen



DELETE

Same as registration process, it is able to delete 1st fingerprint, 2nd fingerprint and card in each. If wish to delete all 3data, select "Delete All" and corresponding ID is deleted

DELETE




1. Access to the system menu
(Refer to P. 17 or P. 18 for access to the system menu)
2. Select "User"
3. Select "Delete"
4. Input password ("User ID") to delete
5. Place fingerprint or Card to delete
(If want to delete both fingerprint and card of the ID, select Delete All.
6. Press  button after selection
7. "Yes" and complete the delete



SET TEMP ID

Temp ID cannot be an Admin and not use fingerprint Admin can determine access times of Temp ID (min. 1 ~ max. 9)
Access times are expired, Admin can revert it.
emp ID leaves log data
Pre-registered ID is not used as a temp ID.

SET TEMP ID

1. Access to the system menu
(Refer to P. 17 or P. 18 for access to the system menu)
2. Press  button
3. Select “User”
4. Select “Set Temp ID”
5. Input Temp ID (upto 8 digits) and press 
6. Input access admission times with this temp ID and press 
(Min. 1, Max. 9)
7. Complete setup temp ID.



KJ-3500

SETTING 1.Basic 2.Advanced 3.AC Setting 4.Communication 5.Schedule 6.Log Setting

Basic

- 1.Time
- 2.Date
- 3.Date Format
- 4.Language
- 5.Use Busytone detection
- 6. Set Phone Numbers

Advanced

- 1.Verification Mode
- 2.ID Mask
- 3.Use Tamer Alram
- 4.Use Touch Sensor
- 5.Celibrate Senseor
- 6.Restore Factory Settings
- 7.Clear General Log
- 8.Clear Management Log
- 9.Clear Enroll Date

AC Settings

- 1.Define Timezone
- 2.User Timezone
- 3.Lock Type
- 4.Lock Door Release Time
- 5.Door Open Warning
- 6.Re-access Count
- 7.Re-access Limit Time
- 8.Wiegand Format
- 9.Anti-Passback



KJ-3500

SETTING 1.Basic 2.Advanced 3.AC Setting 4.Communication 5.Schedule 6.Log Setting

Communication

- 1.Device ID
- 2.Baudrate
- 3.TCP/IP Settings
 - DHCP
 - IP Antipass
 - Subnet Mask
 - Default Gateway
 - Port
 - Mac Address
- 4.Communication Password

Schedule

- 1.Set Tmode
- 2.Ring Settings
- 3.Auto Door
- 4.Auto Funckey
- 5.None-Relat Funckey
- 6.Day Light
- 7.Holiday
- 8.Funckey Alarm
- 9.Idle Settings

Log Setting

- 1.Management Log Warning
- 2.General Log Warning



BASIC

1. Time

Set-up the time of the device

Device' s time is applied to the time of the event. So it is important the accurate time.

2. Date

Setup the date of the device.

3. Date Format (YYYY-MM-DD)

Define date format at home screen

4. Language (Korean/English)

Choose the language

5. Use Busy tone detection (No/Yes)

If the silent exceeds 1minute, the phone disconnected automatically.

Even visitors activate interphone, it returns standby mode and recommend to use.

6. Set Phone Numbers

When interphone is connected, the receivers can remote control the door with pass word.

Only registered phone numbers are able to control the door and available max. 100 phone numbers.



ADVANCED

1. Verification Mode

Depends on the security level, it is able to adjust the verification mode.

2. ID mask

When the user input ID, it hides user ID as xxxxxx and enhance the security.

3. Use Tamer Alarm

When it detects tamper, it activate alarm.

4. Use Touch Sensor

If touch sensor is on, sensor lights off in normal condition and lights on when the user touch the sensor only.

5. Calibrate Sensor

Optical sensor perceive surroundings and optimize the brightness.
When use this function, it has to block extraneous light.

6. Restore Factory Settings

Reset all settings to the default

7. Clear General Log

Delete all general log data

8. Clear Management Log

Delete all management log data

9. Clear Enroll Data

Delete entire user data including fingerprint, card data and it is unrecoverable

VERIFICATION MODE

1. ANY MODE : Access granted with any form of authorization
2. FINGER : Fingerprint Only - No access with ID or Card
3. CD OR FP
4. ID&FP OR CD
5. ID&FP OR ID&CD
6. ID &FP OR CD & FP
7. OPEN : Always Open (Fail Safe Mode)
8. CLOSE : Always Closed (Fail-Secure Mode) - No access with any form of authorization
9. CD : Card Only - No access with ID or Fingerprint
10. ID OR FP : ID or Fingerprint only - No access with Card
11. ID OR CD : ID or Card Only - No access with Fingerprint
12. ID & CD : Both ID and Card required for access - must punch in ID before Card authentication
13. CD & FP : Both Card and Fingerprint required for Access
 - Card must be authorized before fingerprint authentication
14. ID & FP : Both ID and Fingerprint required for Access
 - must punch in ID before fingerprint authentication
15. ID & CD & FP : all three formats needed for access

AC SETTINGS

1. Define Timezone : Able to set-up 256 timezones.
(Refer to Software (Guardian) manual 7.3 Time Zone set-up.

2. User Timezone : Able to allocate 2 time zone for each user. 0 for [All Time] and 257 for [None Time].

3. Lock Type : NC or NO Set up door lock type

4. Lock Door Release Time : Default 3sec. Available to adjust between 1 ~ 99sec.

5. Door Open Warning : Once door open, if the door remains open over setting condition, it activates alarm

6. Reaccess Count : No, 0~ 9 Limit reaccess count between no., 0 ~ 9times.

7. Reaccess Limit Time : Limit reaccess time between no. 0 ~ 600minutes.

8. Wiegand Format : 26,34,35,37,64
Designate wiegand output format 26,34,35,37, or 64.
Read all wiegand data regardless of wiegand settings

9. Anti-Passback : No / Yes
Anti-passback activates through external wiegand input.
If there is two controllers for enter and exit, re-enter is allowed only it has exit event data
(EX : Public Parking lot, Restricted Area, Membership center)

COMMUNICATIONS SETTINGS

1 .Device ID (1 ~ 999)

Device ID ranges between 1 ~ 999.

When many devices are connected in one network, each device must have unique address.

2. Baud rate : 115200 bps

RS-485 Communication speed

3. TCP/IP Settings

– DHCP : No/ Yes

Choose DHCP on or off

– IP Address : 192.168.1.224

Setup IP Address

– Subnet Mask : 255.255.255.0

Setup subnet mask

– Default Gateway : 192.168.1.1

Setup default gateway

– Port : 5005

Setup TCP Port

– MAC Address

Displays MAC Address of the device

To connect device with software (Guardian) by TCP/IP (LAN),
it must set-up IP Address, Subnet Mask, Gateway,

(All the above data is for reference only and an confirm the details in network environment of the PC to connect)

4. Communication Password

If the communication password is not correct, it is impossible to communicate with the software

SCHEDULE

1. Set Tmode

Setup the door mode and it is converted automatically according to the time and schedule.

Refer to Software (Guardian) manual 7-4 controller

Special function/ Door mode how to setup the door mode

2. Ring Settings

Setup the bell ring schedule.

Refer to Software (Guardian) manual 7-4 controller

Special function / Bell Time how to setup the bell rings

3. Auto Door

Setup the operation time of the automatic door

Refer to Software (Guardian) manual 7-4 controller

Special function

Auto Door how to setup the auto door.

4. Auto Funckey

At the designated date and time, the corresponding key is set-up as default.

Refer to Software (Guardian) manual 7-4 controller

Special function

auto F-Key how to setup the auto F-Key.

5. None-Relay Funckey

Setup none-relay Funckey and buzzer alarm key.

Refer to Software (Guardian) manual 7-4 controller

Special function

No act F-Key how to setup the No Act F-key.

SCHEDULE

6. Day Light

Setup the daylight.

Refer to Software (Guardian) manual 7-4 controller

Special function

Daylight how to setup Daylight.

7. Holiday

Holiday settings must comply with the day of the week

Refer to Software (Guardian) manual 7-4 controller

Holiday setup

8. Funckey Alarm

Once input the alarm key and succeed to identify, it activates buzzer alarm or relay alarm.

9. CD2 Auto Funckey

Input card data to the external reader by Wiegand, and succeed to identify, it is used to save the event..

If a controller is connected to a reader, this function gives a function key to the external reader automatically, thus a an automatically setup function key is given to a user who is authorized from an external reader. Events of user entries from the reader are stored. (Ex. For time & attendance)

10. Idle Settings

LCD power cut off : 0 ~ 60minutes

IDLE mode : 0 ~ 60minutes

LOG SETTINGS

1. Management Log Warning (0 ~ 100)

If the management log exceeds the setting value, it alarms

2. General Log Warning

If the management log exceeds the setting value, it alarms

USB MEMORY

Insert USB memory into the slot at the bottom of the device and up/download the events data and update the firmware i

Download General log
Download new general events

Download All General log
Download all general events

Download Management log
Download new management events

Download All Management log
Download all management events

Download User Info
Download user data

Upload User info
Upload user data

Upgrade Firmware
Update Firmware



MEMORY

1. User :User numbers which is enrolled in the device

2. Fingerprint : Template numbers which is enrolled in the device

3. ID Card : ID Card numbers which is enrolled in the device

4. General Log : General log (access event) numbers

5. Management Log : Management log (system event) numbers

DEVICE INFO

Device info is set from the manufacturer and the user cannot edit this info.

1. Release Date : Displays the device release date
2. Serial Number : Displays the device serial number
3. Manufacturer : Displays the device manufacturer
4. Product Name : Displays the device Name
5. Product Type : Displays the device Type
6. Engine Version : Displays the engine version
7. Firmware Version: Displays the firmware version



ADVANCED

- 1.View General Log : Search and view the general access event
- 2.View Management Log : Search and view the system management event
- 3.View User info : Search and view the numbers of the fingerprint and card

SELF TEST

Test All : Test overall status and functions of the device

Test Memory : Test memory and takes 1 ~ 2 minutes . After test, it reboots and displays the result

Test LCD : Test LCD

Test Sound (Auto) : Test Voice announcement automatically. If there is no voice chip, it finishes quickly

Test Sound (Manual) : Test Voice announcement manually.

Test Sensor : Test Finger sensor

Test Keyboard : Test keyboard

Test RTC : Test RTC

Test Case Status : Test the status of the case

Test Card Reader : Test the card reading