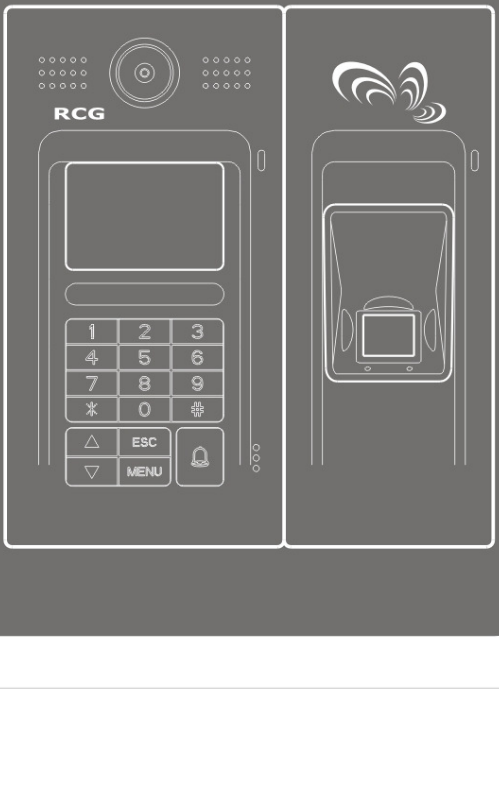
RCG

Biometrics • RFID • Security

i4 FLEXI

Multi-Functional Access Control System

User Menu



RCG i4 Flexi
User Manual V2.5

State：	Third release	version：	2.5
I4Flexi version:	V6.5-071213	SDK version:	DLL_V6.4-071205
		update：	2007-12-17

History

Date	I4Flexi Firmware Version	Dll version	Change
2007-02-08	V3.5-070208	V1.0.070208	First Release
2007-10-18	V4.7-070917	V1.0.060626	Modify 2.4 Enroll Quality Threshold from 65 to 85 Add item 7.1.6 " Verify Safe Rank" Add item 7.1.7 "Enroll Safe Rank" Add item 7.1.8 "Sensitive Rank" Add item 7.1.9 "Enroll Quality"
2007-10-23	v4.9-071019	DLL_v1.020071018	Add item 7.1.10 "Card Reader" Modify 7.2 • Add "Dooropen alarm" Modify 8 • Add "HostDomainName" • Add "Preferred DNS" • Add "Alternate DNS" Modify 8.1.3.1 • Add "Device IP" • Add "Subnet Mask" • Add "Gateway" • Add "Host IP" • Add "Host Port" • Add "MAC Address" • Add "HostDomainName" • Add "Preferred DNS" • Add "Alternate DNS"
2007-11-06	V5.5-071101	DLL_v1.020071030	Modify 7.2 • Add "Exit Button event" • Add "Invalid time zone event" Modify appendix 10 • Add "Door left Alarm"
2007-11-14	V5.5-071101	DLL_v1.020071030	Minor changes in wording
2007-12-17	V6.5-071213	DLL_V6.4-071205	Updated the Main Screen

This is an operating manual for i4 Flexi Access Control & Time Attendance Management System. Every attempt has been made to make it accurate as possible. However, product changes will occur from time to time and please refer to our web site for latest updates. While RCG has attempted to make this document as accurate as possible, we expressly disclaim any and all warranty of accuracy and completeness, and accept no liability for any loss or damage arising from any inaccuracies or omission.

Please send comments to *support@rcg.tv*

Federal Communications Commission (FCC) Statement

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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Trade Name: i4 Flexi
Model No: PTN-100206-01-A

Table of Contents

Conventions

This guide uses the following conventions:

📝	This icon denotes particularly important information.
⚠	This icon denotes precautions to avoid injury, data loss, or a system crash.
♨	This icon denotes precautions to avoid a burn hazard.
⚡	This icon denotes precautions to avoid being electrocuted.

bold Bold text denotes items that you must select or click on in the software, such as menu items and dialog box options. Bold text also denotes parameter names.

Italic Italic text denotes emphasis, a cross reference, or an introduction to a key concept. This font also denotes text that is a placeholder for a word or value that you must supply.

1 About i4 Flexi

i4 Flexi Access Control & Time Attendance Management System is a powerful tool for access control and time attendance management. i4 Flexi adopts with latest optical fingerprint sensor and high-precision fingerprint identification algorithm. With supports of RS485 (converter required) and TCP/IP protocols, it can be implemented as both standalone and networked.

i4 Flexi adopts separate controller and centralized connection board design to enhance security. Tamper alarm will go off if an intruder try to open the device and alarm relay output can be generated.

With its Wiegand Input and Output features, the system can be easily reinforced by just adding an external reader. (Optional Wiegand Input– 26 bit or 34 bit). The i4 Flexi device can also act as a reader to send out Wiegand signal to existing controller. (Optional Wiegand Output feature – 26 bit or 34 bit). This offers more choices to end users.

i4 Flexi boasts an attractive apppearance with changeable casing design. It is easy to operate, ready to implement and embedded with various innovative features. By using high resolution and blue backlit LCD, clear and attractive image can be display. The keypad is made of durable material and so heavy-duty usage is not a problem. Its built-in voice system provides an interactive operation mode.

i4 Flexi can store up to 5,000 fingerprints and supports 1:1 & 1:N identification. Its offers seven verification modes, namely Fingerprint only, Password Only, Card only, fingerprint or password, Card and fingerprint, Card and password, Card and Fingerprint and Password.

1.1 Key Components

i4 Flexi Fingerprint Access Control System has two main components: A Main Unit and a door lock controller.

Main Unit: Manages registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information, and display of prompt information. It consists of fingerprint processor module, LCD, keypad, doorbell button, fingerprint sensor, reset button and casing. The interface of the fingerprint main unit (hereinafter referred to as the "equipment") is shown in the diagram below.

- Product's appearance description

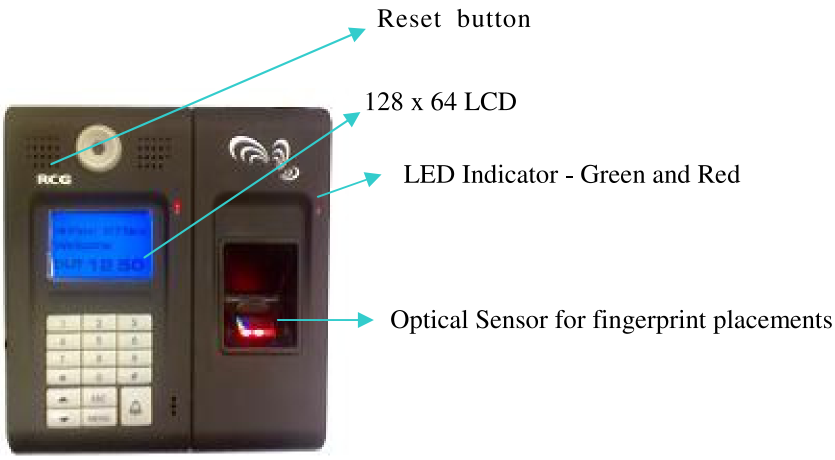

Reset button
128 x 64 LCD
LED Indicator - Green and Red
Optical Sensor for fingerprint placements

Fig. 1 Appearance of i4 Flexi

'#' Enter key: Confirm your present operation

MENU Menu key: Press down the key for seconds to enter the management interface in the initial state

ESC Cancel key: Cancel your present operation

OUT /▲ Scroll up key: Scroll up the menu & **OUT:** Check for off work

IN/▼ Scroll down key: Scroll down the menu & **IN:** Check for on work

'＊' Clear key: Clear the input

🔔 Door bell button (providing dry contact for external door bell)

0 – 9 : Numerical key.

Lock control unit: The control centre of the lock controller. It is also the execution component of the i4 Flexi. It controls the locking and unlocking of the door lock based on the instructions of the fingerprint processor, monitors door lock state of the access control system, and triggers alarm signals in the event of security breaches.

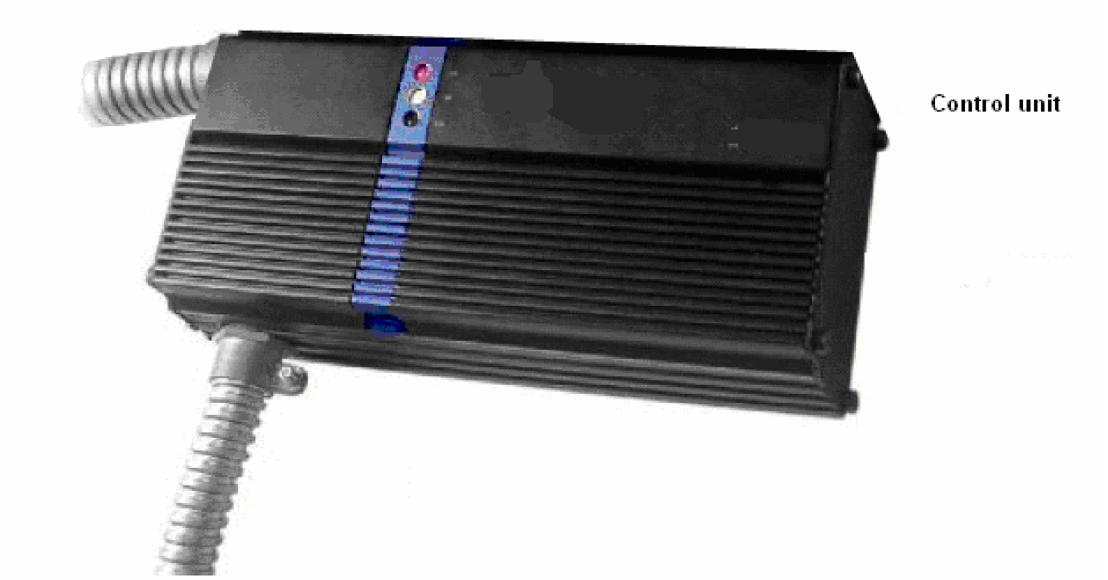


Fig. 2 Lock Control Unit

1.2 Features

1.2.1 Characteristics

1.2.1.1 Enhanced Security

Traditional security systems such as smartcards and keypad locks are not always reliable, given the high incidences of loss and theft. With RCG's fingerprint recognition system, such problems can be easily eradicated. Because biometric technology is known to minimize crime and save time, i4 Flexi is a valuable tool to enhance security.

1.2.1.2 Reliable and stable algorithm

RCG created an unique, proprietary algorithms for i4 Flexi. The algorithms enable i4 Flexi to provide a high degree of fingerprint verification accuracy.

1.2.1.3 Entrance security

In addition to monitoring access control, i4 Flexi maintains a record of all visitors to an area and their time spent on premises. This system makes it possible for human resources and payroll departments to rely on accurate data to compute staff wages.

1.2.1.4 Function keys and log records

i4 Flexi has four programming keys to manage the time and attendance functions. With i4 Flexi, one single terminal can be assigned to manage access control and employees' time and attendance.

1.2.1.5 Low system maintenance cost

Traditional ID systems, such as the smartcard, can incur high long-term costs since replacements are necessary when staff or member cards go missing. i4 Flexi eliminates this long-term cost, given that it relies on employees' own biometry to identify them.

1.2.1.6 One system to control several terminals

One i4 Flexi module can function in standalone mode to monitor access control. i4 Flexi can also connect to other modules compatible with TCP/IP/RS232/RS485 modems to link to a central server. i4 Flexi is equipped with RTC technology, which allows it to log up to 10,000 records and manage access control without the use of an ACU adaptor.

1.3 Support functions

User management

- Register a user (RF, fingerprint, password)
- Delete a user or all users
- Query the number of registered users
- Query the remaining capacity to register new users
- Query ID allocation
- Set a user’s time zone
- View registered ID list
- Transmit user’s data in software terminal

System management

- Configure and read terminal’s time and date
- Change and read security level
- Change Terminal ID
- Configure communication mode (TCP/IP, RS485)
- Receive firmware version
- Change lock operating time

Door mode

- Configure and read door mode (normal/ forced open/ forced close) and time

Log

- Log data contains the function key, entrance time and user ID
- Query log count
- Delete all logs

Authentication

- Terminal Authentication as 1 : 1, 1 : N and Grouping
- Various authentication methods: RF, Password, Fingerprint, RF+FP, RF+PIN, FP+PIN and RF+FP+PIN

Auxiliary function

- Exit button
- Relay in Lock driver
- Transmit case status
- Support voice message
- Transmit door switch status

Alarm function

- Alarm Finger
- Invalid Door Open Alarm
- Tamper Alarm

Note:

1: ‘Standalone’ means that the management, registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information, and display of prompt information can be done once the fingerprint main unit is connected to a power source, and without the use of any networked PC.

1.4 Definitions

User: Users of i4 Flexi can be classified into two groups: User I and User II. User I refers to supervisors, managers, enrollers and normal users of i4 Flexi (hardware), and User II refers to PC software's (DAMS) users ("PC administrator") who can set and administer the data and parameters of i4 Flexi. The roles and responsibilities of the two groups of users are as follows:

1) User I: (User in i4 Flexi access control device)

"Supervisors", "managers", "enrollers" and "normal users" are end-users of i4 Flexi. These users are authorized to perform verification, enquiry and administration. "Normal users" have the authority to use the system only, whereas "supervisors", "managers" and "enrollers" have different levels of authority to administer the equipment.

User authority: The four user types of the equipment have different levels of authority, and are ranked as follows:

Supervisors > managers >enrollers> normal users

Normal users: Normal users do not have the authority to administer the equipment. They can only conduct operations such as access verification.

Enrollers: user who are entitled to enroll new users or delete an existing user in the system. They can't enter the "Menu->2.options" & "Menu->3.Network".

Managers: In addition to the operations that normal users can conduct, managers maintain some administrative authorities except those dedicated to "supervisors". Specifically, "managers" can add, delete, or modify the data of "managers" "enrollers" and "normal users" and they can check the verification logs of any user on the system. They can't enter the "Menu->2.options->1.system opt->5. adv. Opt" & "Menu-> 2. option -> 5. Auto Test" & "Menu -> 3.Network-> 3.com key".

Supervisors: Supervisors have the highest operating authority of the system. In addition to the operations that managers can conduct, supervisors can access the "system administration" of the system to set various setting parameters. Specifically, they can add, delete or modify the data of any user, or delete all the users so that the system reverts to its original empty state. 【Note: It is impossible to modify another supervisor】.

2) User II : (User in DAMS software)

The PC administrator uses PC-based software tool to maintain the data of the access equipment, mainly the outputting and processing of access administration and the verification log, maintenance of access system parameters, and backup and restoring of user data,.

(Note: To access via the PC software, the equipment must be in the standby state to ensure successful connection.)

Empty state: The state in which i4 Flexi is void of any user; either no user data are stored in the main unit terminal (supervisor, administrator, enroller or normal user) or all user data have been deleted.

Standby state: i4 Flexi is idle or is not receiving any input signal from the processor, i.e., no button is pressed . On the LCD screen, only current date and time will be displayed.

Exit button: An optional feature of the i4 Flexi fingerprint access control system. It can be mounted inside a door, and a user can press on the button to unlock the door.

Offline use: With offline use, the fingerprint processor connected to the power supply can perform functions such as registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information and display of prompting information. These jobs can be done without the use of a PC.

Wiegand Output: Wiegand signals plus Wiegand controller may also control the door lock.

Online assistant administration: i4 Flexi provides connection to PC through RS485/TCP/IP, so that customers can administer the access control system, set the various parameters, and backup and restore the user data at the PC. This enables a customer to easily administer multiple access systems.

To successfully achieve communication between the equipment and PC, some parameters of the fingerprint processor have to be set according to the descriptions about “communication” in the following text.

Local alarm: The buzzer inside the fingerprint unit sends out alert sounds alarm.

Remote alarm: i4 Flexi is connected to an alarm in a remote location (such as a security guard office). The alarm goes off in the event of security breaches. People nearby the access system cannot hear the alarm sound.

Alarm finger: When enrolling fingerprints, a user may specify a finger as the alarm finger (fingers not specified as alarm fingers are considered “normal fingers”). When the user applies this finger to conduct “verification for door opening” or “menu logging” operations, the system will produce remote alarm signals. Alarm finger is usually used in duress situations.

Normal door opening: User uses an authorized finger (normal finger or alarm finger) to conduct "verification for door opening" through the access control system, or opens the door via the "exit button". This is called normal door opening.

Invalid door opening: Any door opening action other than normal door opening is called invalid door opening. For instance, someone opens the door using invalid methods such as prying open the door using a crowbar, or unlocks the door with a key (without fingerprint verification or pressing the door release button).

Card, Fingerprint and password verification: i4 Flexi supports verification of card, fingerprint and password separately as well as combined verification of card, fingerprint and password. Separate card/password verification is useful for situations when a user's fingerprint is difficult to register or validate due to its poor quality. The combination of card, fingerprint and password verification can improve the security of the whole system.

Finger relevancy: To enhance the user's level of security, he/she may enroll two normal fingers and a set of two finger relevancies (both enrolled fingers must be used for verification), or register three normal fingers and choose to set two or three finger relevancies (two or three enrolled fingers must be used for verification) . Once finger relevancies are set, the user must pass the verification for all finger relevancies to open the door when conducting fingerprint verification.

FRR: "False Rejection Rate" or FRR is measure of the probability the access system will wrongly reject an access attempt; the system will refuse the access attempt from an authorized user. A smaller percentage value reflects a better system.

FAR: "False Acceptance Rate" or FAR is a measure of the probability the access system will wrongly accept an access attempt; the system will accept the access attempt from an unauthorized user. A smaller percentage value reflects a better system.

1.5 Operating Sensor

When using the fingerprint sensor avoid touching the sensor surface with any sharp or hard object (be careful when installing the device). Always keep the surface clean. For cleaning, dip clean absorbent cotton in water and apply laterally to the stain.

Position of finger placement

To get a clear fingerprint image, place finger closely on sensor in the correct position as shown in the first two diagrams from the left in Fig. 3:

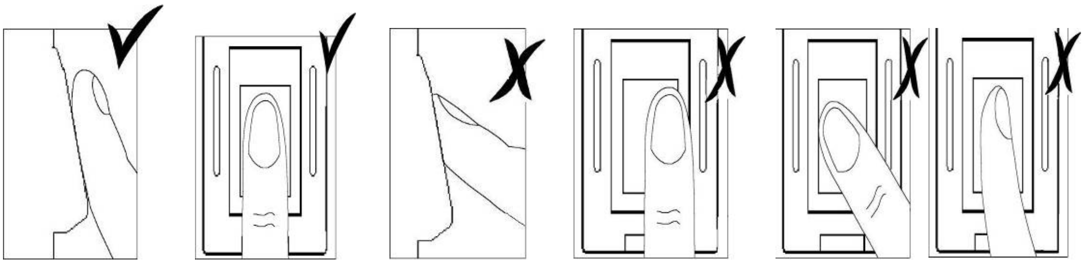


Fig. 3

The first two diagrams show correct finger placement. The other diagrams illustrate incorrect finger placements.

1.6 System Specifications

- Technical specifications

Item	Technical parameter
Type of sensor	Optical sensor
Resolution of sensor	500dpi
Effective area of sensor	18mm×16mm
Dimension of fingerprint processor	156 m (H) X 160 mm (W) X 38 mm (D)
FRR	<= 1 %
FAR	<= 0.0001%
Finger matching time (1:1 matching)	≤0.5S
Verification mode	Fingerprint only, Password Only, Card only, fingerprint or password, Card and fingerprint, Card and password, Card and Fingerprint and Password
Verification mode	1:1, 1:N
Working mode	Standalone or Network
Output	1 x Relay output, 1 x Alarm Relay output
Max user capacity	5000 users (if 1 fingerprints per user)
Max fingerprint capacity	5000 fingerprints (10 fingerprints per user at most)
Max log capacity	50000 logs
Communication Protocol	TCP/IP, RS232, RS485, Wiegand (Input or Output)
Working temperature	0℃ ~ 45℃
Working humidity	RH 20% ~ 80%
Working Voltage	DC 12V
Working Current	400mA
Relay Output (Lock, Alarm)	NC/NO connection, 3A/12Vdc or 120VAC

Time Zone	50
Group	50
Holiday Table	50
User / Group Association	Support
Forced Door Open/Close Schedule	Support
Alarm Type	Tamper Alarm, Alarm on threat (alarm finger), Invalid door open alarm
Wiegand	Support Wiegand input / Wiegand output (26 bit or 34 bit)
Other Features (Optional)	RFID Module
Language	English / Simplified Chinese / Traditional Chinese

2 Tips and precautions

2.1 First setting in initial use

- Change system password to ensure security
- “1111” as the default setting password
- Power up the device after cabling work is completed

2.2 Difficult fingerprints

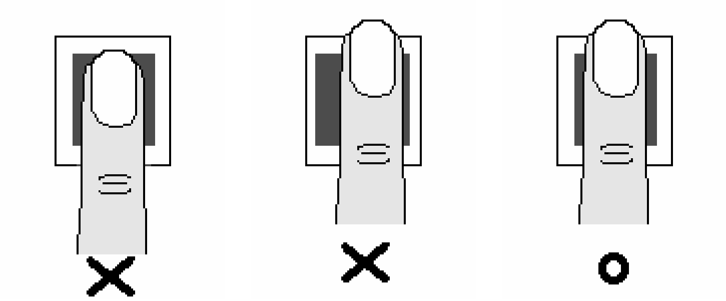
- Remove dirt, ensure fingers are dry and try again
- Maintain finger on sensor for more than one second without moving finger

2.3 Reset i4 Flexi and return to setting status before last trial

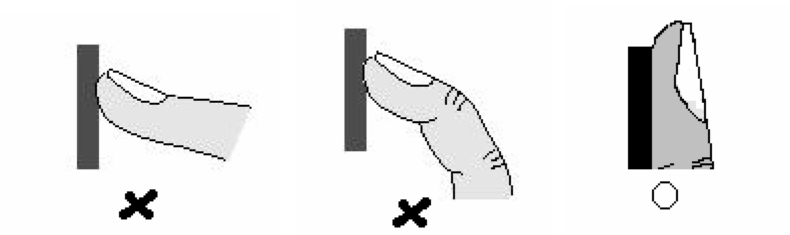
- When i4 Flexi malfunctions without an apparent problem, press the Reset switch to return to setting status before the last trial.
- Contact the i4 Flexi customer support center for assistance

2.4 Right fingerprint registration position

- Correct fingerprint registration position placement
- **During registration**, a quality score will appear for every finger press. For the *mark below 85*, it is recommend to re-registration or use other finger to obtain the better score.



- Correct fingerprint touching placement.



2.5 Cleaning the Sensor

Depending on the amount of use, the sensor window may need to be cleaned periodically.

To clean it, apply the sticky side of a piece of adhesive cellophane tape on the window and peel it away.

Under heavy usage, the window coating on some sensors may turn cloudy from the salt in perspiration. In this case, gently wipe the window with a cloth (not paper) dampened with a mild ammonia-based glass cleaner.

2.6 Sensor Maintenance Warnings

There are several things you should never do when cleaning or using the sensor

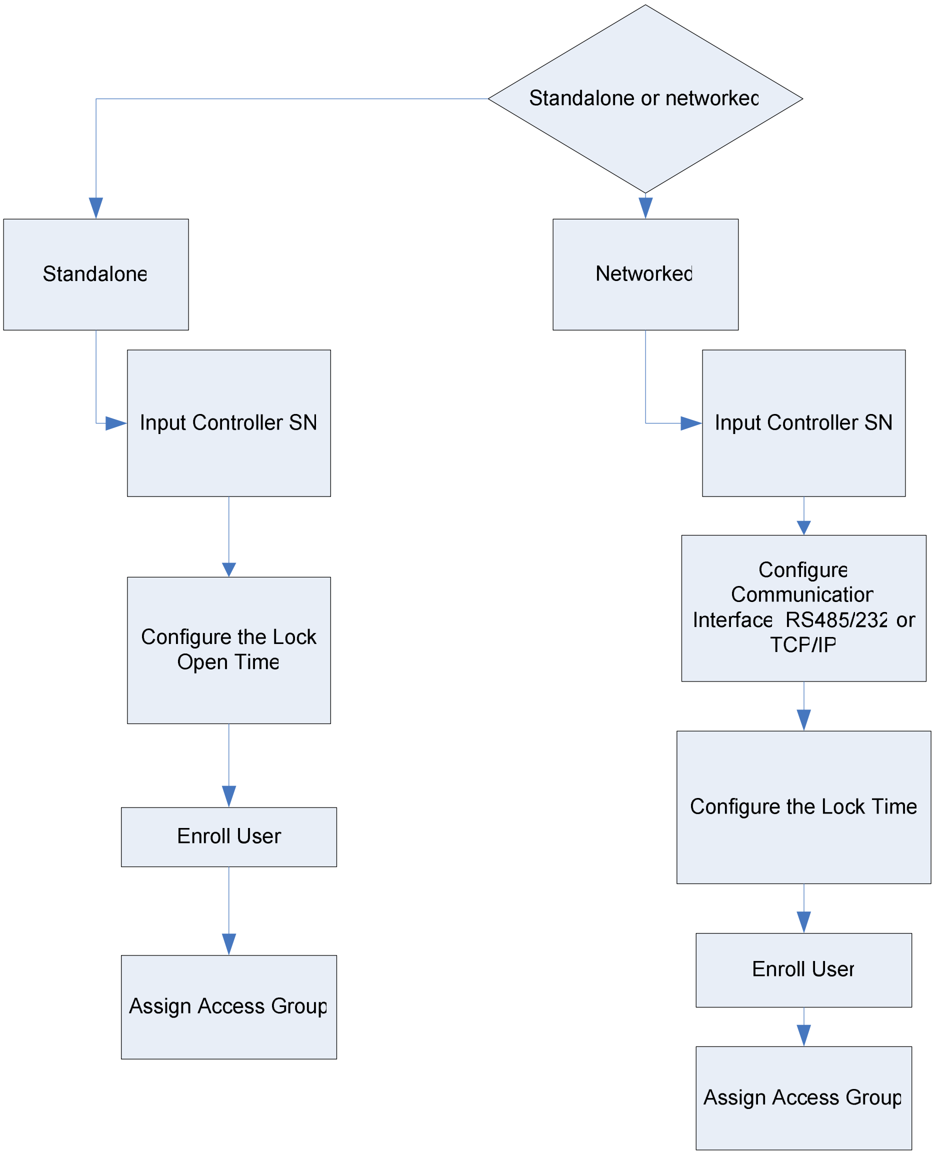
- Do not pour the glass cleaner directly on the sensor window.
- Do not use alcohol-based cleaners.
- Never submerge the sensor in liquid.
- Never rub the window with an abrasive material, including paper.
- Do not poke the window coating with your fingernail or any item, such as a pen.

3 Configuration

3.1 Basic Flow

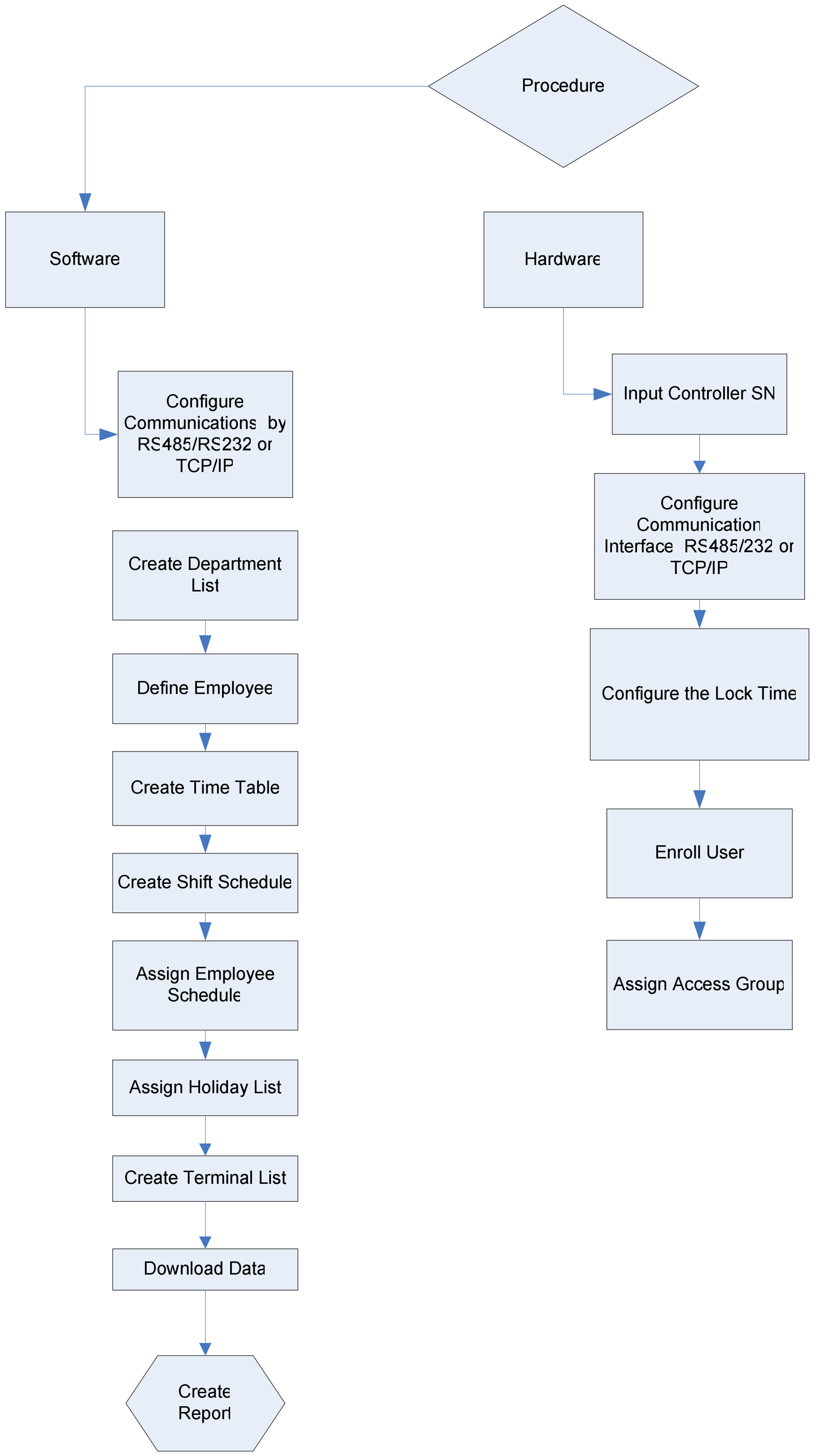
Application for Access Control Configuration

- **Standalone**: The user will operate the i4 Flexi terminal for administration with no data backup capability and the data is stored inside the terminal only.
- **Networked:** The user will connect the i4 Flexi terminal to computer for administration, it is capable to backup the user data, access log and transfer the user data to another new i4 Flexi terminal by using "DAMS" software



Application for Time Attendance Configuration

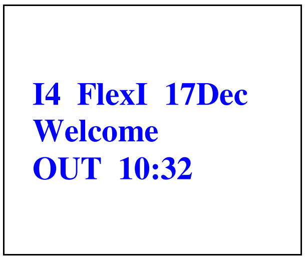
- The user will connect the i4 Flexi terminal to computer for administration; it is capable to calculate time attendance by transfer the user data with "DAMS" software.



3.2 User Registration, Editing, Deletion

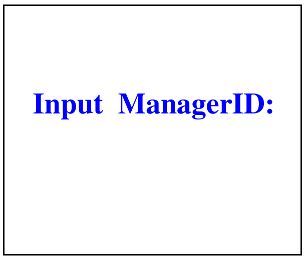
3.2.1 How to enter the administration menu

The administrator menu allows new users to register, edit or delete information. Press "Menu", enter"0" and press "#" to access the administrator mode and then enter '1111' as the initial password.



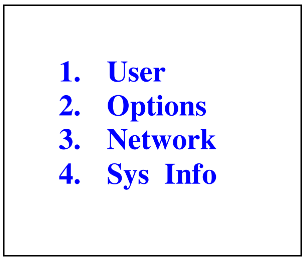
I4 FlexI 17Dec
Welcome
OUT 10:32

The standby screen as show here.



Input ManagerID:

1. Press "Menu" key,



1. User
2. Options
3. Network
4. Sys Info

2. Enter ID "0" and then follow with "#" to confirm and enter "1111" as the initial password.

3.2.2 How to register user

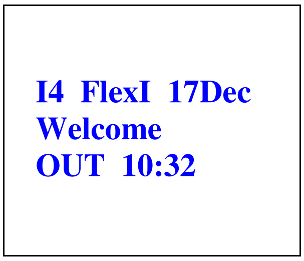
Press "menu", "0" and "#" to input '1111' as the initial password.

First, follow the process "1.User => 1.Add User" and "Add User ID:" appears on screen.

If the ID entered is already in use, "User Exist!" will appear on screen.

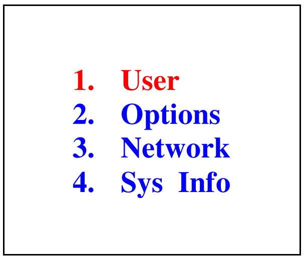
(Maximum number of digit is 8)

How to add new user



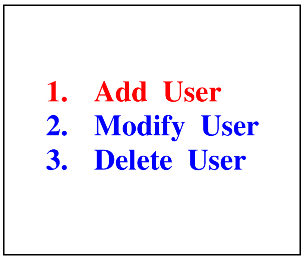
I4 FlexI 17Dec
Welcome
OUT 10:32

1. Press "Menu" key, enter "0" and then follow with "#" to confirm and enter "1111" as the initial password.



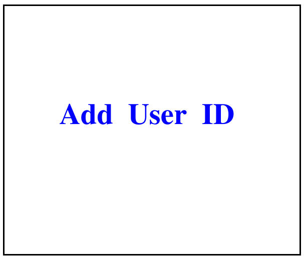
1. User
2. Options
3. Network
4. Sys Info

2. Select "1. user"



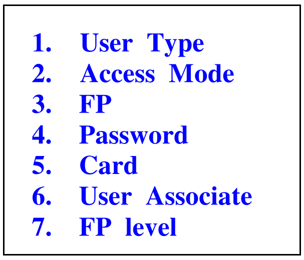
1. Add User
2. Modify User
3. Delete User

3. Select "1.Add user"



Add User ID

4. An "Add User ID" message prompt appears. You are required to input the user ID



1. User Type
2. Access Mode
3. FP
4. Password
5. Card
6. User Associate
7. FP level

5. Enter "Add user " page.

3.2.3 Fingerprint registration

To register a fingerprint, place your finger on the red light sensor after pressing "3. FP" in the "Add user" page (see above). Registration is complete after you register with one of the access factor and press "Esc". The system will then automatically move to the upper menu. To increase authentication rate or register additional fingers, press "2. FP2" and follow the same process required in "1. FP" registration.

.▣ The asterisk (*) appears on the right side of the menu when you save.

1. FP1
2. FP2
3. FP3
4. FP4

1. After pressing "3. FP", FP 1 – 8 is normal finger, FP 9-10 is alarm finger. Select FP ID and place finger on red light sensor

Press Finger…

2. Place finger on red light sensor

Press Again…

3. Place finger on red light sensor one more time

FP Enroll OK!

4. Enroll FP ok. The screen will return to FP page.

1. FP1 *
2. FP2
3. FP3
4. FP4

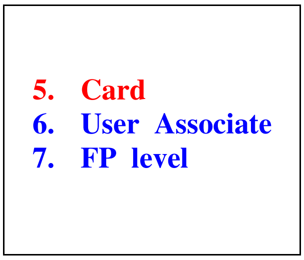
5. The asterisk (*)besides "FP1" indicates successful fingerprint reg istration

Notes 1: Repeat step 1- 4 for another finger

Notes 2: After FP enrollment, a successful registration will be done after access mode assigned – follows section 6.2.6

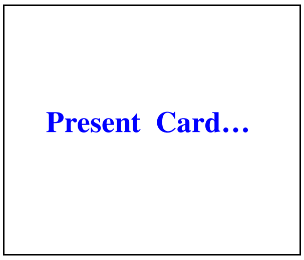
3.2.4 RF Card Registration

First, at the Add user page, (after FP enrollment, press “ESC”). Select “5. Card” for RF Card registration and a “Touch Your Card” message appears on screen. When you complete the RF Card registration, the RF Card “buzzer” will chime. If “One More Time Please!” appears on screen, please repeat the procedure using the same RF card.



5. Card
6. User Associate
7. FP level

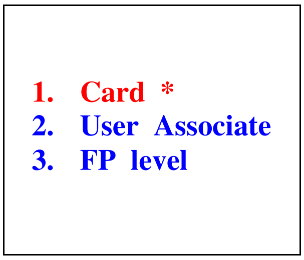
1. Select “5. Card” to see the “Present Card…” message appear on screen.
After you register the RF Card, the RF Card “buzzer” will chime.



Present Card…

2. “RF Enroll Repeat” appears on screen when the card number is already exist in the terminal

Notes: Please check the card status with administrator



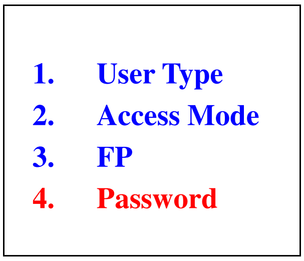
1. Card *
2. User Associate
3. FP level

3. The asterisk (*) shows after “5. Card” to indicate successful RF card registration.

Notes 1: After Card enrollment, a successful registration will be done after access mode assigned – follows section 6.2.6

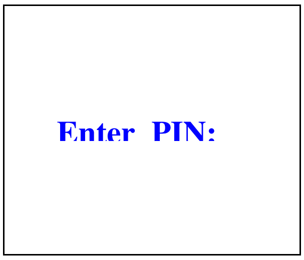
3.2.5 Password registration

To register your password, in the “Add user” page, (after FP enrollment, press “ESC”).please select “4. Password” and the message, “Enter PIN:” will appear on screen. Enter a password between four and eight digits to process registration. If the password does not match, “PIN Set Error” will appear on screen. Enter the correct password and select “2. Access Mode” to complete the registration process.



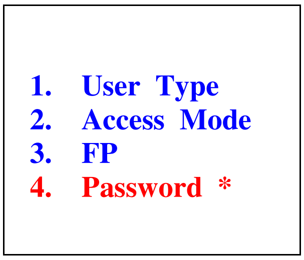
1. User Type
2. Access Mode
3. FP
4. Password

1. Select “4. Password” for password registration and enter your desired password



Enter PIN:

2. Enter password for verification (at least 4 digits and up to 8 digits)



1. User Type
2. Access Mode
3. FP
4. Password *

3. The asterisk (*) shows after “4.Password” to indicate successful PIN registration

Notes 1: After Password enrollment, a successful registration will be done after access mode assigned – follows section 4.2.6

To initiate password authentication, follow the process “2. Access Mode => 3. PIN” with the tick mark (*) by pressing “#” or number “3”. When finished, press “Esc” to save and return to the upper menu.

3.2.6 Activate FP, Card, Password Access Mode

To authenticate an FP, PIN or RF card, follow the process “2. Access Mode=>1. FP, 2. Card & 3. PIN” with the tick mark (*) by pressing “#” or a corresponding number. Press “Esc” to save and return to the upper menu.

1. User Type
2. Access Mode
3. FP
4. Password

1. Select “2.Access Mode”

Notes 1: You must register before being able to select access mode.

1. FP
2. RF
3. PIN
4. RF+FP

2. Select item number to activate the corresponding mode e.g. Press “1. FP, 2. RF & 3.PIN” access mode This makes access mode by either one of the selection.

1. FP *
2. RF *
3. PIN *
4. RF+FP

3. Press “Esc” to save and return to the upper menu

3.2.7 RF Card + Fingerprint

This option is for users who prefer to use an RF card together with fingerprint. It is a high security setting that also confirms identity via the use of an RF card in conjunction with fingerprint recognition.

To register a fingerprint and RF card, select "3. FP" and "5. Card" as the same process for "6.2.3""6.2.4".

Then, to process authentication, follow the process "2.Access Mode=>4.RF +FP" by choosing the tick mark (*) and pressing "*" or "4". Press "Esc" to save and return to the upper menu.

1. User Type **2. Access Mode** **3. FP** **4. Password**	1. Select "3. FP" and "5. Card" to register a fingerprint and RF card
1. FP **2. RF** **3. PIN** **4. RF+FP**	2. Select "2. Access Mode"
1. FP **2. RF** **3. PIN** **4. RF+FP**	3. Select item number to activate the "4. RF+FP" access mode
1. FP **2. RF** **3. PIN** **4. RF+FP ***	4. Press "Esc" to save and return to the upper menu

3.2.8 RF Card + Password

This function is for users who want to use the "RF card together with Password" option, or the high security function to present an RF card and password to confirm their identity.

To register your RF card and Password select "5.Card" and "4.PIN" as the same process for "6.2.4" "6.2.5".

To initiate authentication, follow the process "2. Access Mode => 5. RF +PIN" via tick mark (*) and press "#" or "5". Press "Esc" to save and return to the upper menu.

1. User Type
2. Access Mode
3. FP
4. Password

1. Select "5. Card" and "4. PIN" to register RF card and PIN

1. FP
2. RF
3. PIN
4. RF+FP

2. Select "2. Access Mode" and press" Down Arrow" key to view the following item

5. RF+PIN
6. FP+PIN
7. RF+FP+PIN

3. Select the item number to activate the "5.RF+PIN" access mode

5. RF+PIN *
6. FP+PIN
7. RF+FP+PIN

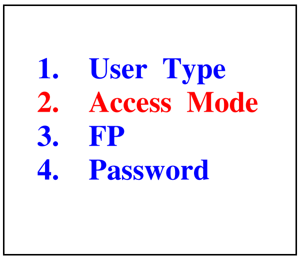
4. Press "Esc" to save and return to the upper menu

3.2.9 FP + PIN

This function is for users who want to use the "FP together with Password" option, or the high security function to present a Fingerprint and password to confirm their identity.

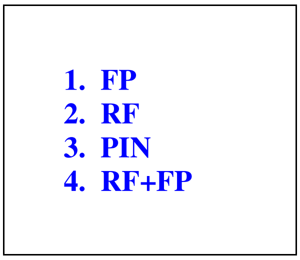
To register your Fingerprint and Password select "3. FP" and "4. Password" as the same process for "6.2.3" and "6.2.5".

To initiate authentication, follow the process "2. Access Mode => 6. FP +PIN" via tick mark (*) and press "#" or "6". Press "Esc" to save and return to the upper menu.



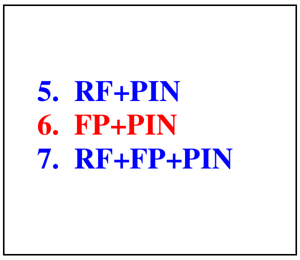
1. User Type
2. Access Mode
3. FP
4. Password

1. Select "5. Card" and "4. PIN" to register RF card and PIN



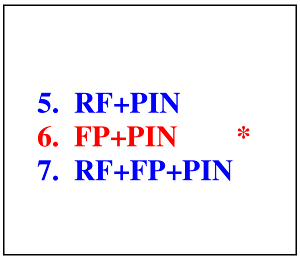
1. FP
2. RF
3. PIN
4. RF+FP

2. Select "2. Access Mode" and press "Down Arrow" key to view the following item



5. RF+PIN
6. FP+PIN
7. RF+FP+PIN

3. Select the item number to activate the "5. RF+PIN" access mode



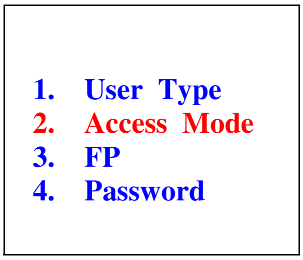
5. RF+PIN
6. FP+PIN *
7. RF+FP+PIN

4. Press "Esc" to save and return to the upper menu

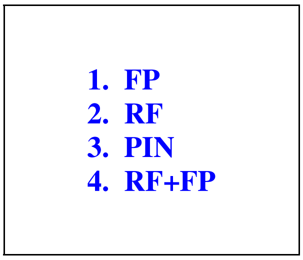
3.2.10 Card + FP + PIN

Users can select this function to confirm identity via “Card+FP+Password” or the high security level with their RF card, Fingerprint and Password.

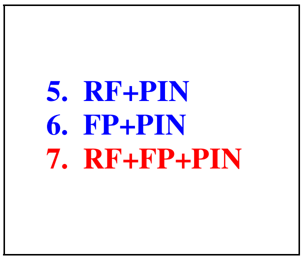
To register a RF card, fingerprint and password, select “3. FP” or “4. Password” and 5. Card” as the same process for “6.2.3”, “6.2.4” and “6.2.5”. To process authentication, follow the process “2. Access Mode=>7. Card +FP+PIN” with the tick mark (*) and press “#” or “7”. Press “Esc” to save and return to the upper menu.



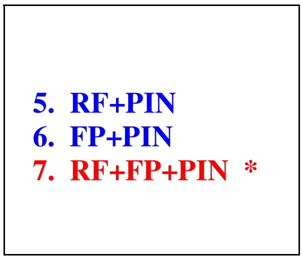
1. Select “5. Card” and “4. PIN” to register RF card and PIN



2. Select “2. Access Mode” and press “Down Arrow” key to view the following item



3. Select the item number to activate the “7. RF+FP+PIN” access mode



4. Press “Esc” to save and return to the upper menu

3.3 Selective authentication method

This function allows users to select one specific authentication process. Users must first register all methods preferred, then select "2. Access Mode" and press the tick mark (*) to choose relevant numbers. To complete the process, users must select "one of the access mode" before "Esc" the screen, otherwise, the user is not register and return to the upper menu.

1. User Type
2. Access Mode
3. FP
4. Password

1. Register all methods and select "2. Access mode"

1. FP *
2. RF
3. PIN *
4. RF+FP

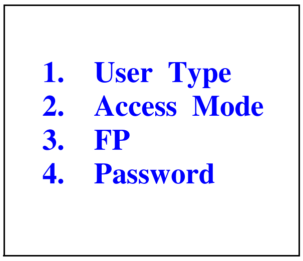
2. Select item number (#) and choose required numbers

1. FP *
2. RF
3. PIN *
4. RF+FP

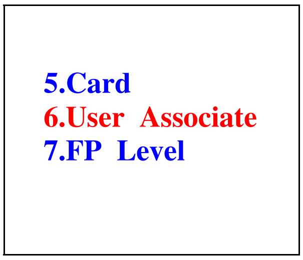
3. Press "ESC" to save and return to the upper menu

3.4 User Association

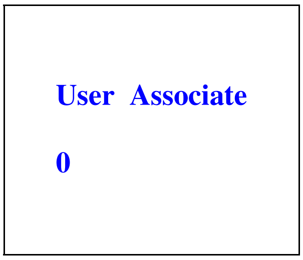
This function allows users to verify with witness by specific user during authentication process. When this function enables, users must first verify its access mode, if the access granted, the system will prompt the associate user to verify his access. If all access is verified, the first user will have access right & event log to the system. To use this function, select "6. User Associate" and press the tick mark (*) to choose relevant numbers.



1. Press "Down Arrow" key at the user page.



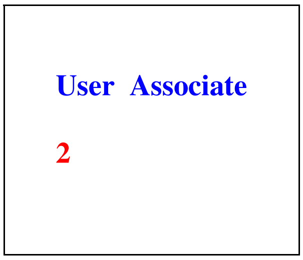
2. Select "6. User Associate"



User Associate

0

3. The default value is "0", means "No User to be associated". e.g. if this user is associated with use ID 2, you may input "2" to this field.



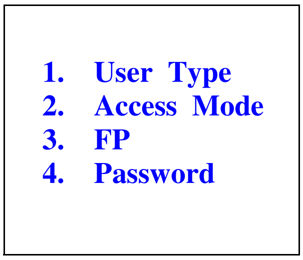
User Associate

2

4. Press "Esc" to save and return to the upper menu

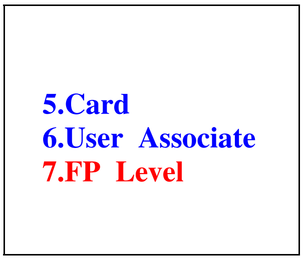
3.5 Set Personal Security Level

This function allows users to change the personal fingerprint verification level. The lower the value provides the lower threshold but the false acceptance rate will be higher. (value from 1 – 5) To use this function, select "7. FP Level" and press the tick mark (#) to choose relevant numbers.



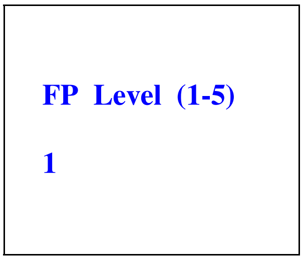
1. User Type
2. Access Mode
3. FP
4. Password

1. Press "Down Arrow" key at the user page.



5.Card
6.User Associate
7.FP Level

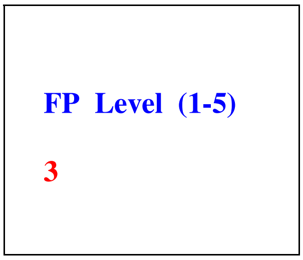
2. Select "7. FP Level"



FP Level (1-5)

1

3. Choose your preferred security levels



FP Level (1-5)

3

4. Press "Esc" to save and return to the upper menu

4 How to change authentication methods

4.1 Search for ID to amend

To change the authentication method, follow the process "1. User => 2. Modify User" until you see "Modify User ID:" appear on screen. Then enter the ID that needs to be amended. To search through the ID list, press "*" until you see the ID list. Use the "ARROW" key to move the cursor and select the required ID from the list. Select "#" to go to editing mode.

1. User
2. Options
3. Network
4. Sys Info

1. Select "1. user"

4. Add User
5. Modify User
6. Delete User

2. Select "2. Modify user"

Modify User ID

3. Enter your user ID, press "*" continuously to retrieve complete ID list and select required ID

4.2 Change authentication methods

To change authentication method select “2. Edit User” to edit. To edit more than one method select (#), if not, delete (press “#” again) to save editing changes, and press “Esc” to save and return to the upper menu.

.▣Tick mark (*) appears when you press “#” or a corresponding number.

1. User Type
2. Access Mode
3. FP
4. Password

1. Select “2. Access Mode”

1. FP *
2. RF
3. PIN *
4. RF+FP

2. Select your desired item to choose authentication method(s)

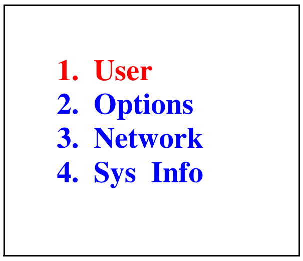
3. Press “Esc” to save and return to the upper menu.

5 User Deletion

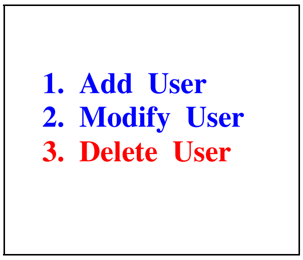
5.1 Delete user

Enter the ID you wish to delete when “Delete User ID:” appears on screen. Then press “Menu1.User=> 3.Delete User” to initiate deletion. When “Yes/No” appears on screen, input the “1. Yes, 2. No” to complete deletion. If the confirmation entered, the screen will display “Delete User, User Deleted”.

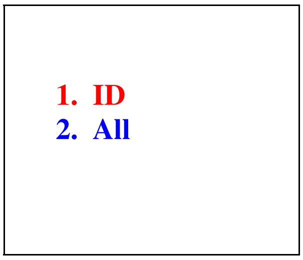
To delete all users, follow the process “1.User=>3.Delete User” until “1. ID” and “2. All” appear on screen. Then, input “2. All” to delete all registered users. When “Yes/No” appears on screen, input the “1. Yes, 2. No” to complete deletion. If the confirmation entered, the screen will display “Delete User, User Deleted”



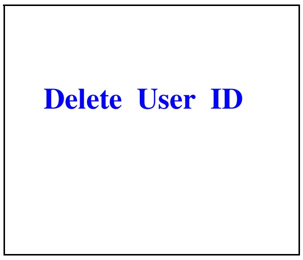
1. Select “1. user”



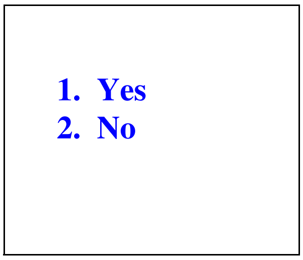
2. Select “3. Delete User”



3. Choose the delete type, “1. ID or 2. All”

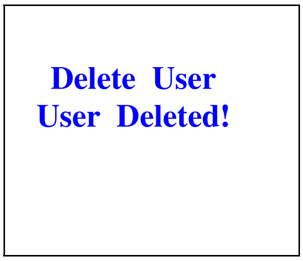


4. Enter your user ID, press “*” continuously to retrieve complete ID list and select required ID



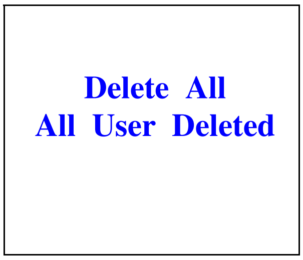
1. Yes
2. No

5. Confirm the user to be deleted



Delete User
User Deleted!

6. The user deleted screen appears & return to upper menu.



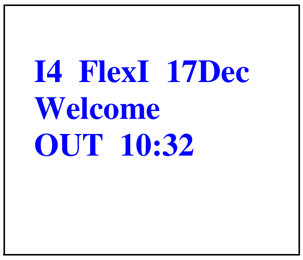
Delete All
All User Deleted

7. If you are choosing “Delete All User” at step 2, the “All Use Deleted” screen appears.

6 Use & Authentication method

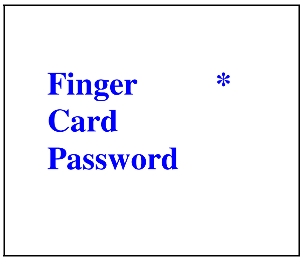
6.1 Fingerprint User

Place your finger on the sensor.



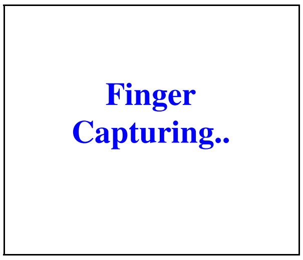
I4 FlexI 17Dec
Welcome
OUT 10:32

1. Standby screen



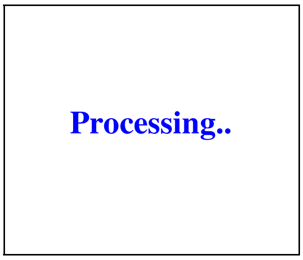
Finger *
Card
Password

2. Place your registered finger on the sensor or input your ID & press “#”.



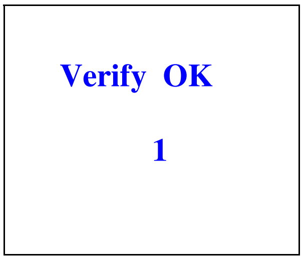
Finger
Capturing..

3. A progress screen “Finger Capturing” appear



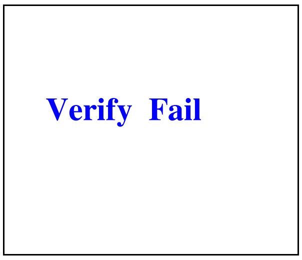
Processing..

4. A progress screen “ Processing..”appear



Verify OK
1

5. A message appears to indicate our fingerprint has our fingerprint has been recognized and your identification verified



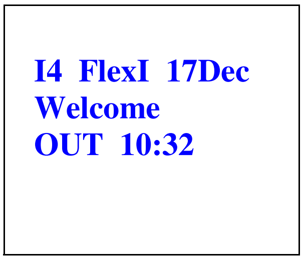
Verify Fail

6. A message shows failure to verify your identification

If authentication fails, please repeat the process.

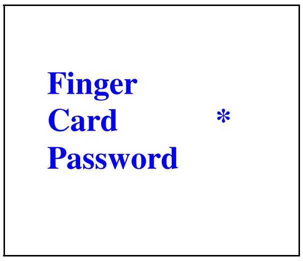
6.2 RF Card Users (do not need to input an ID number)

Place your RF card in the designated section under the fingerprint sensor.



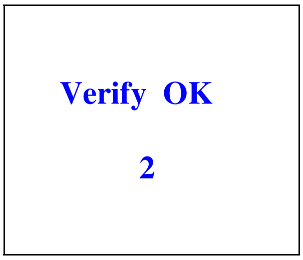
I4 FlexI 17Dec
Welcome
OUT 10:32

1. Ensure that your RF card touches the upper part of the fingerprint sensor



Finger
Card *
Password

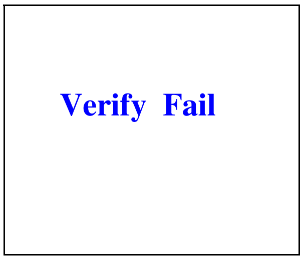
2. Place your registered card on the sensor or input your ID & press “#”.



Verify OK

2

3. A message appears to indicate your RF card has been recognized and your identification verified

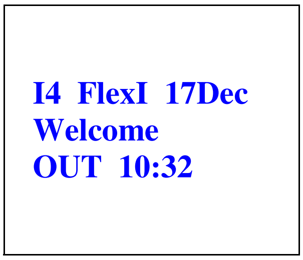


Verify Fail

4. A message shows failure to verify your identification

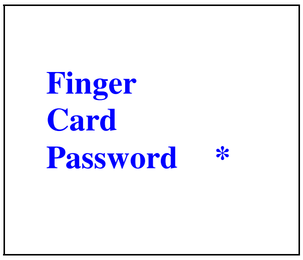
6.3 Password User

Input your user ID, press "#". Enter your password when you see the "Enter Password:" message on screen.



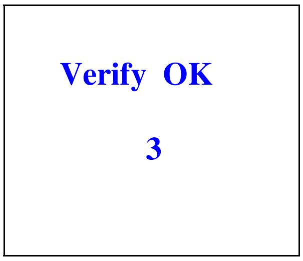
I4 FlexI 17Dec
Welcome
OUT 10:32

1. Input your user ID, press "#"



Finger
Card
Password *

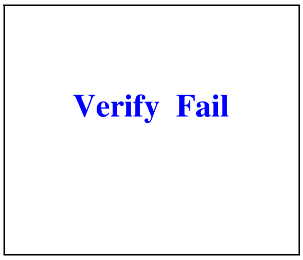
2. Input your password & press "#" to enter.



Verify OK

3

3. A message appears to indicate your password has been recognized and your identification verified



Verify Fail

4. If you enter an incorrect password, a message appears to indicate failure to verify your identification

If authentication fails, please repeat procedure.

6.4 RF Card + Fingerprint, RF Card + Password User

(no need to input ID numbers)

Choose high security level. Authentication is processed when RF card and fingerprint or password match.

6.5 Selectable authentication method user

Select a preferred authentication method. The message "Verify OK" appears on screen when user authorization is confirmed. For example, for Fingerprint & Password registration, users must input their user ID, present a fingerprint and enter the corresponding password.

7 Options

There are six items under the setup "options", namely System Option, Access Module, Event Option, Access Option, Auto Test and FPImageTest. The following sections describes each of these items.

The following steps show how to access the option section

LCD Display	Description
1. User **2. Options** **3. Network** **4. Svs Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "2" to enter Options page.
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	2. Press [Down] key to search for either one of five Options. Press "#" to enter the setting menu of each function

7.1 System Option

The System Option contains Date, Time, Language, Date Format and Advanced Option.

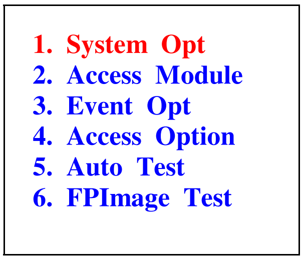
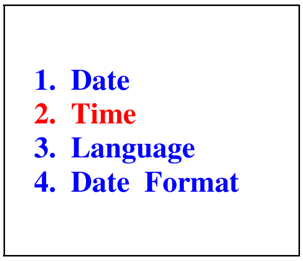
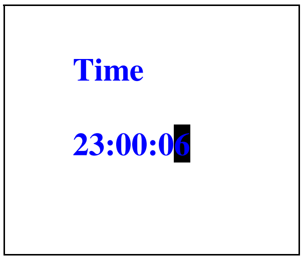
7.1.1 Date

The following steps show how to modify the date on the terminal

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	. In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “1” for System Opt.
1. Date **2. Time** **3. Language** **4. Date Format**	2. Press “1” key to select the Date option.
Date **2006-11-06**	3. Press “Up” and “Down” key to select the field. Input the value and press “#” to save.

7.1.2 Time

The following steps show how to modify the time on the terminal

LCD Display	Description
 1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "1" for System Opt.
 1. Date 2. Time 3. Language 4. Date Format	2. Press "2" key to select the Time option
 Time 23:00:06	3. Press "Up" and "Down" key to select the field. Input the value and press "#" to save.

7.1.3 Language

The following steps show how to modify the language on the terminal

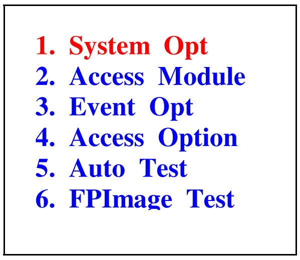
LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	While in the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “1” for System Opt
1. Date **2. Time** **3. Language** **4. Date Format**	2. Press “3” key to select the Language option.
1. English * **2. 简体中文** **3. 繁體中文**	4. Press “Up” and “Down” key to select the field. Press “#” to save. *Notes: The terminal supports three languages, namely, simplified Chinese, traditional Chinese, and English.*

7.1.4 Date Format

The following steps show how to modify the date format on the terminal

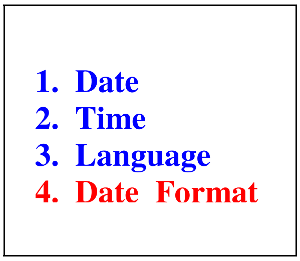
LCD Display

Description

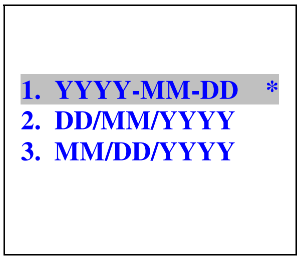


In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page.

1. Press “1” for System Opt.



2. Press “4” key to select the Date Format option



3. Press “Up” and “Down” key to select the field. Press “#” to save.

7.1.5 Advanced Option

The following steps show how to modify the advanced option on the terminal

LCD Display

Description

1. System Opt
2. Access Module
3. Event Opt
4. Access Option
5. Auto Test
6. FPImage Test

While in the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page.

1. Press “1” for System Opt.

5. Adv Option
6. VerifySafeRank
7. EnrollSafeRank
8. SensitiveRank

2. Press “Down” key to reach item “5” key to select the Adv option

1. Reset Opts
2. Del Attlogs
3. Clear All Data
4. Clr Admin Pri
5. 1 to 1 Only
6. Voice

Press Up and Down Key to scroll up or down the screen to select the option.

1. Restore Default: Restore to default setup information. E.g. Date format, Display Lang. to Eng.

2. Delete Logs: Delete all stored logs .

3. Clear all Data: Delete all enrolled fingerprints and logs.

4. Clear Administrator’s right: Change the rights of the administrator to ordinary user.

5. 1 to 1 only: Enable 1:1 matching verification mode

6. Voice: Activate/deactivate phonic hints.

7.1.6 VerifySafeRank

The following steps show how to modify the VerifySafeRank on the terminal

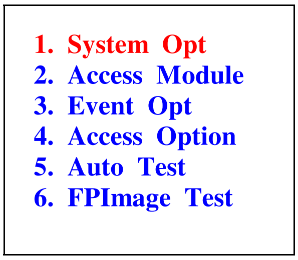
LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	While in the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “1” for System Opt.
5. Adv Option 6. VerifySafeRank 7. EnrollSafeRank 8. SensitiveRank	2. Press “Down” key to reach item “6” key to select the VerifySafeRank option
FP Safety level: 5	3. Input the value and press “#” to save. ➲*Note: Verify Safe Rank: It controls the 1:N matching security level. You can choose a level between 1 and 7. Greater number will provide higher identification security.*

7.1.7 EnrollSafeRank

The following steps show how to modify EnrollSafeRank on the terminal

LCD Display

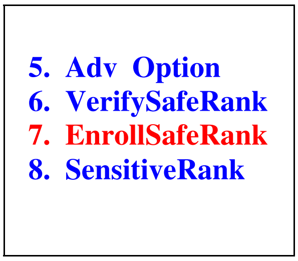
Description



1. System Opt
2. Access Module
3. Event Opt
4. Access Option
5. Auto Test
6. FPImage Test

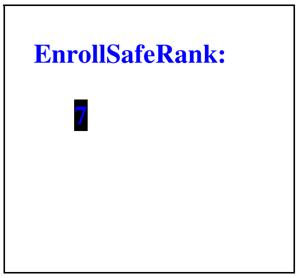
While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page.

1. Press "1" for System Opt.



5. Adv Option
6. VerifySafeRank
7. EnrollSafeRank
8. SensitiveRank

2. Press "Down" key to reach item "7" key to select the EnrollSafeRank option



EnrollSafeRank:

7

3. Input the value and press "#" to save.

➲*Note: Enroll Safe Rank: It controls the fingerprint matching security level in user enrolment. You can choose a level between 1 and 7. Greater number will provide higher quality of fingerprint template.*

7.1.8 SensitiveRank

The following steps show how to modify the SensitiveRank on the terminal

LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "1" for System Opt.
5. Adv Option 6. VerifySafeRank 7. EnrollSafeRank 8. SensitiveRank	2. Press "Down" key to reach item "8" key to select the SensitiveRank option.
SensitiveRank: 6	3. Input the value and press "#" to save. ➲*Note: Sensitive Rank: It controls the image capturing sensitive of fingerprint scanner. You can choose a level between 1 and 7. Lower number will require user to press the scanner with more pressure, hence a better quality of capturing image can be produced.*

7.1.9 EnrollQuality

The following steps show how to modify the EnrollQuality on the terminal

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	While in the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “1” for System Opt.
9. EnrollQuality **10. Card Reader**	2. Press “Down” key to reach item “9” key to select the EnrollQuality option
EnrollQuality: **85**	3. Input the value and press “#” to save. ➲*Note: Enroll Quality: It controls the threshold for accepting captured image in enrolment process. During user enrolment, the system will show the quality of captured image in score and will accept the image with the score higher than or equal to the threshold. You can choose a score between 60 and 100. Greater score will ensure higher quality of fingerprint template.*

7.1.10 Card Reader

The following steps show how to modify the Card Reader on the terminal

LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	While in the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “1” for System Opt.
9. EnrollQuality 10. Card Reader	2. Press “Down” key to reach item “10” key to select the Card Reader option
1. MFCard 2. OEM50	3. Press “Up” and “Down” key to select the field. Press “#” to save. ➲*Notes: With MIFARE version i4 Flexi, it can read MIFARE Standard for setting “MIFARE Card”, While with HID version i4 Flexi, it can read HID iCLASS credentials for setting “OEM50”,*

Access Modules

The following steps show how to modify the date format on the terminal

LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “2” for Access Module (A function to activate/deactivate the access module or not)
1. PIN 2. FP 3. Card	2. Select the item in option.
1. Enable * 2. Disable	3. Press “Up” and “Down” key or Press “1” or “2” to select the field. Press “#” to save.

7.2 Event Option

Alarm Access Log (Alm AccLog): When the log capacity reached the set numerical value, it will automatically sound a warning signal to indicate full capacity. (Max 50000)

Recheck Minute (Recheck Min): If the attendance record of an individual exists in the system within a defined time period (unit: minute), the individual will not be recorded repeatedly.

Notes: '0' is disable, '1' means the same user can only have 1 record within 1 minutes.

Time & Attendance: Select the indication method for IN/OUT status in stand-by screen.

Lock Event: Select whether to store the lock event or not

Access Event: Select whether to store the access event or not

Other Event: Select whether to store the other event or not

Door open alarm: Enable or disable the alarm by setting the valid door opening time

➲*Note: There are 2 kind of event logs for software/SDK to retrieve*

1) *Access Log*
    - *User Transcation Log*
        a) *Normal access log*
        b) *Invalid TZ access log*
    - *Exit Button Log*
        a) *Defined as user ID "0" with remark "ExitBT"*
2) *Manager Log*
    - *Tamper Alarm (Type 1)*
    - *Alarm Finger (Type 2)*
    - *Forced Open Alarm (Type 3)*
    - *Door Left Open Alarm (Type 4)*

The following steps show how to modify the event option in terminal

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "3" for Event Option (A function to configure the event optio n)
1. Alm Acclog **2. Recheck Min** **3. Time&Attend** **4. Lock Event** **5. Access Event** **6. Other Event** **7. Dooropen alarm**	2. Select to the item in option, the following interface appears

Count:

500

3. **Alarm Attendance Log** - Input the number to the field and Press “#” to save.

➲ Note: Max. value is 50000

Min:

1

4. **Recheck Min** - Input the number to the field, and. press “#” to save.

1. Disable
2. Text *
3. Icon

5. **Time & Attend** - Select the interface type and press “#” to save.

1. Enable *
2. Disable

6. **Lock Event, Access Event & Other Event** - Select the function enable or disable, the following interface appears. Press “#” to save.

Dooropensec:

3

7. **Dooropen alarm** - Input the valid door opening time and press “#” to save.

   Notes: Once the door opening time exceeds the preset value, alarm will be triggered. Value “0” means disable this alarm function.

7.3 Access Options

Basic concepts of the Access Options function:

- **Access Options**: Setting a registered user's unlocking time zone and unlocking combination.
- **Define TZ**: is the definition of everyday Time Period that can unlock the door .
- **Define Group (GRP)**: Divides registered users into several groups; grouping is easy and convenient to manage.
- **Effective Time Zone**: Defines Time Zone in which the user currently passes verification.
- **Group Time Zone**: Set group's unlocking time.
- **User Time Zon**e: Set the user's unlocking time.
- **Holiday Schedule**: Set holiday dates and access is denied during holidays.
- **Door Forced Open Schedule:** Set the everyday time zone that can always unlock the door.
- **Door Forced Close Schedule:** Set the everyday time zone that can always lock the door.
- **Access Comb** (Unlocking combination): Defines different unlocking combinations; each combination is composed of different groups.
- **Lock** (Time duration of lock drive): Fingerprint scanner controls the time to open the electronic lock.
- **Period Access** (access mode schedule): Fingerprint scanner will change the access method for all users according the time period.

"Access Options" has *NINE* main functions:

1. **Define TZ** is the minimum time zone unit defined in Access Options. (max. 50 set of time zone that including 3 " time period " per Time zone)
2. **User Profile** allows the user to define the User Access Options, in accordance with his own requirements.
3. **Group Define** is the Group Time Zone that assigning the group time zone. (max. 50 set of group that including TZ per day and 3 set holiday list or holiday TZ)
4. **Holiday Sche** is the list of assigned holiday dates.
5. **Access Comb** is used to define various unlocking combinations; each combination is composed of different groups.
6. **Door For Open** is the time zone unit defined to assign the schedule for always opens.
7. **Door For Close** is the time zone unit defined to assign the schedule for always close.
8. **Lock Open Time** is the length of time the electronic lock remains open per fingerprint scanning.
9. **Period Access** is the time zone to be assigned for changing the access mode for all users.

Operation of access option

The Access Options function is for the settings of a registered user's access time zone and access combination.

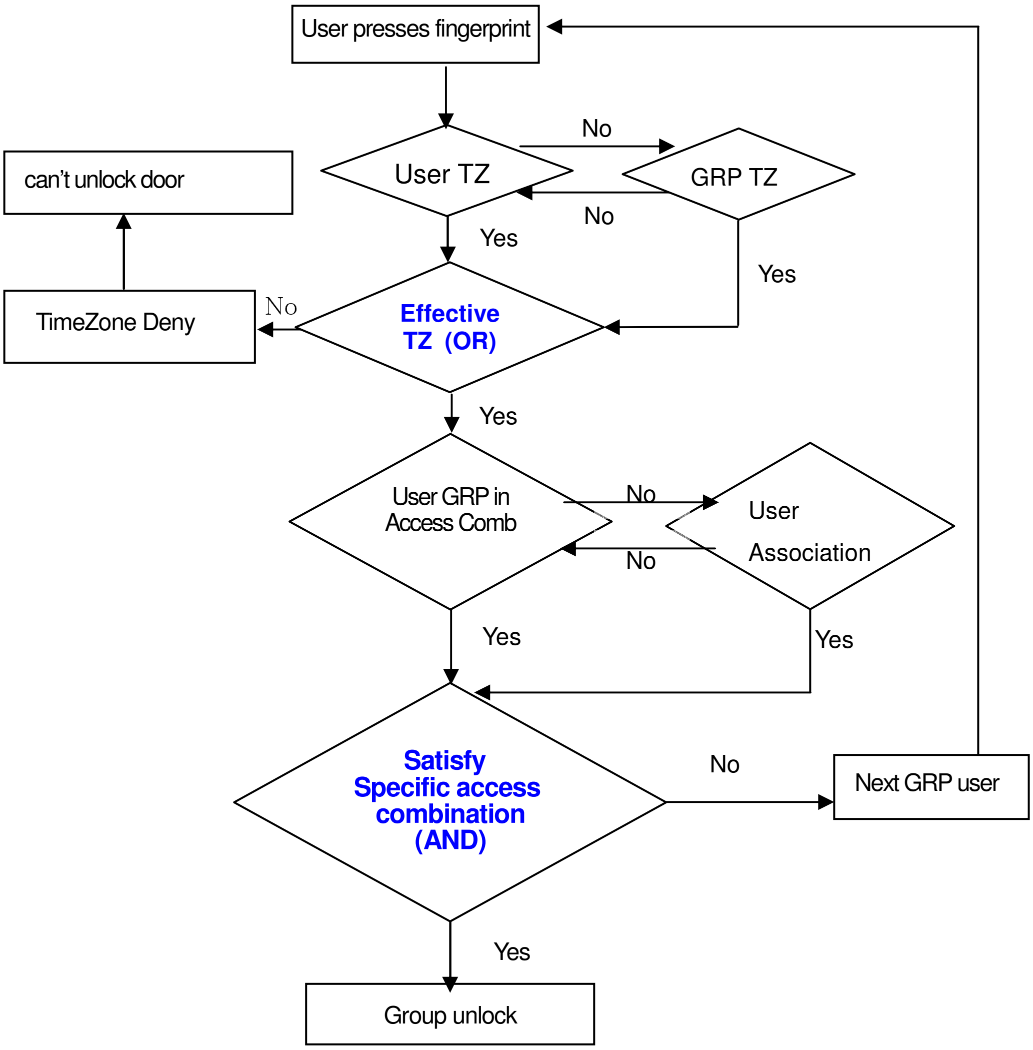
Each user's settings are composed of one grouping to which the user belongs, the user group time zone, and the user time zone. Grouping divides users into a certain group, i.e. group 1, group 2, etc. The user can select a defined time zone in a group per day and holiday list for a group. Also, the time zone contains 4 time periods. The relationship among the four defined time periods is "OR" (i.e. it is only to satisfy any one of the four time periods). In user time zone, the user can select a maximum of three defined time zones that the relationship among the three defined time zones is "OR".

To put it simply, the conditions for a registered user to unlock the door are:

1: The current unlocking time should be within one of the effective time periods in the user time zone or group time zone.
2: The group the user belongs to should be in the user association and access combination (the user with other groups can be in one access combination provided it is required to unlock the door altogether).

The system default for a new registered user is no setting e.g. who can freely access at any time; the default grouping combination is none; and the default group time zone is none. The factory default status for a new registered user is no setting (the system setting will be changed when the user modifies the setting). If the grouping the user belongs to is not included in the grouping combination setting, the user cannot unlock.

Verification flow of operation



7.3.1 Define TZ

Time zone is the minimum time period for Door Access. The whole system can define a maximum of 50 time zones. 4 time regions can be set in each time zone. Each time region is the effective time zone in 24 hours of a day. Each user can set a maximum of 3 time zones. The relationship among these three time zones is “OR”. It is effective as long as the time of verification can meet one of these three time zones. Each time region format of a time zone is HH:MM i.e. the format is according to 24-hour mode and accurate to the minute.

(00:00-00:01) represents all-day forbidden.

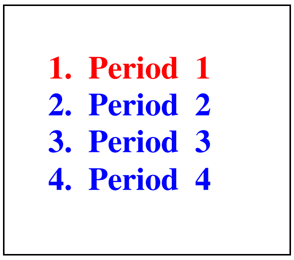
(00:00-23:59) represents effective in this region.

Effective time zone for user to unlock: all-day open (00:00-23:59) or end-time is larger than start-time within a period.

✍Note: System defaults that the time zone is all-day open with no setting here (i.e. new registered user default can unlock door).

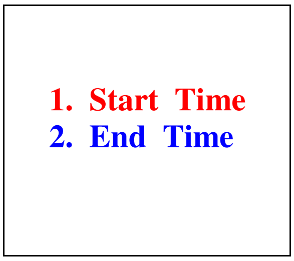
The following steps show how to register a TIME ZONE

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “4” for Access Option (A function to assign access time zone)
1. Define TZ **2. User Profile** **3. Group Define** **4. Holiday Schedule** **5. Access Comb** **6. Door For Open** **7. Door For Close** **8. Lock Open Time** **9. Period Access**	Select the item “1” or use up down arrow to select the item option.
1. Add **2. Edit** **3. Delete**	2. Select “add” to create time zone, “edit” to modify existing time zone or “delete” to erase the time zone created. ➲ Note: in the “edit” or “delete” option, you can key in “*” to list out existing item. In the “delete” option, you can choose delete one by “1. ID” or delete all by”2. All” option.



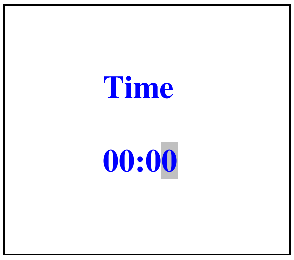
1. Period 1
2. Period 2
3. Period 3
4. Period 4

3. You can input maximum of 4 periods. Press "1" to add "period 1 "time period with starting time & ending time.



1. Start Time
2. End Time

4. Select the "Start Time", and press "#" to enter.



Time

00:00

5. Input the time by 24 hour base. Press "#" to save.

➲ Note: you will stay in the previous page after save. You can set the "End Time". Finally, Press "ESC" to save and return to the upper menu.

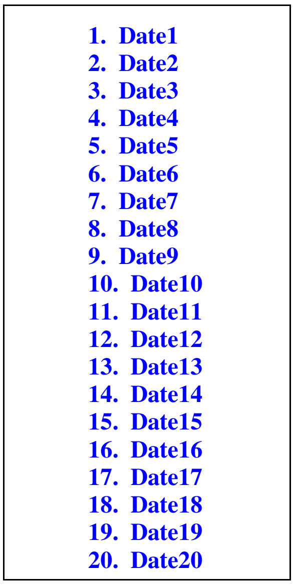
7.3.2 Holiday Schedule

The holiday schedule is a function to assign holiday dates. With the use of holiday, administrator can apply the different group to have different holiday schedule. Thus, during the time on holiday, the system will be according the holiday date with it Time Zone to limit the user to grant access. In addition, the holiday time zone is the time for valid the access. For example, if the holiday set the list no. is 1 with TZ no. 1. That means, the access deny will occur when the day is on the list except the time zone period it can gain access for some period of time.

Each set of holiday is max. Of 20 dates per list and it can be max. of 15 list in holiday schedule.

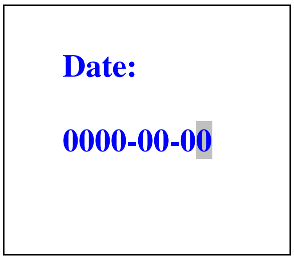
The following steps show how to define Holiday List

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "4" for Access Option (A function to assign access time zone)
1. Define TZ **2. Use Profile** **3. Group Define** **4. Holiday Schedule** **5. Access Comb** **6. Door For Open** **7. Door For Close** **8. Lock Open Time** **9. Period Access**	2. Select the item "4" or use up down arrow to select the item option, the following interface appears
1. Holiday List1 **2. Holiday List2** **3. Holiday List3** **4. Holiday List4** **5. Holiday List5** **6. Holiday List6** **7. Holiday List7** **8. Holiday List8** **9. Holiday List9** **10. Holiday List10** **11. Holiday List11** **12. Holiday List12** **13. Holiday List13** **14. Holiday List14** **15. Holiday List15**	3. Select the list and press "#" to enter (Max. 15 list)



1. Date1
2. Date2
3. Date3
4. Date4
5. Date5
6. Date6
7. Date7
8. Date8
9. Date9
10. Date10
11. Date11
12. Date12
13. Date13
14. Date14
15. Date15
16. Date16
17. Date17
18. Date18
19. Date19
20. Date20

4. Press & select the item. (Max. 20 Date item)



Date:

0000-00-00

5. Input the date to indicate it is holiday.

➲ Note: YYYY-MM-DD

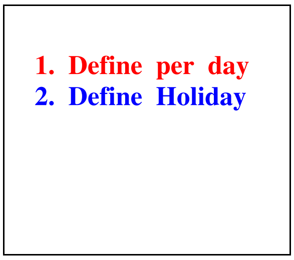
7.3.3 Group Define

The Grouping function can divide users into groups. Furthermore, it can also combine different groups into different unlocking combinations. The grouping management of Access Options is easy and convenient. The system capable to defines max. 50 groups: group 1, group 2, group 3, group 4, and so on. The default for a new registered user is “no group”; the user can be rearranged into another group when necessary.

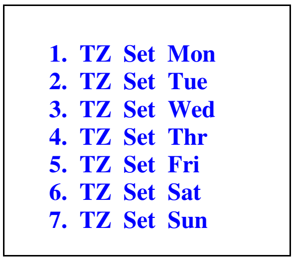
Select the list number of Time Zone that already set in Group Time Zone.
However, after a user resets the group to which he belongs, the user uses the default time zone of the corresponding group. So the default time zone of each group should be defined first.

The following steps show how to define Group

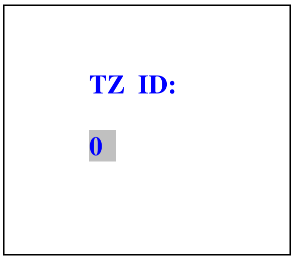
LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “4” for Access Option (A function to assign access time zone)
1. Define TZ 2. Use Profile 3. Group Define 4. Holiday Schedule 5. Access Comb 6. Door For Open 7. Door For Close 8. Lock Open Time 9. Period Access	2. Select the item “3” or use up down arrow to select the item option
1. Add 2. Edit 3. Delete	3. Select “add” to create time zone, “edit” to modify existing time zone or “delete” to erase the time zone created. ➲ Note: in the “edit” or “delete” option, you can key in “*” to list out existing item. In the “delete” option, you can choose delete one by “1. ID” or delete all by”2. All” option.
Group ID: ▇	4. Input the TZ no. and press “#” to enter



5. Press “1” to enter the daily TZ assignment

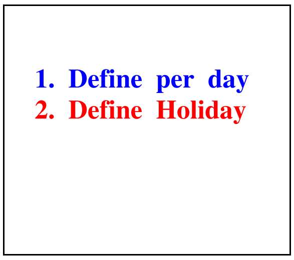


6. Press “1” or one of the day to be modified



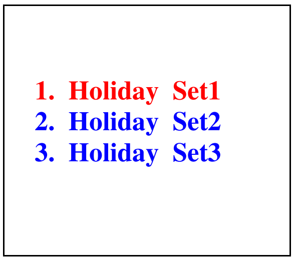
7. Input the TZ for the day you selected. Press “#” to save and return to previous menu.

➲ Note: repeat step 5 for another date TZ setting if any.

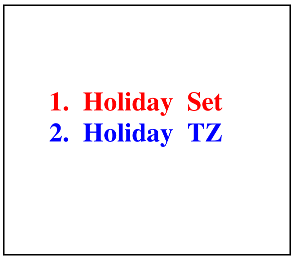


Press “ESC” key to return to previous menu

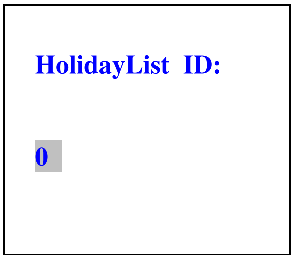
8. Press “2” to define the holiday schedule for this group



9. Select one of the holiday sets (the relationship between them is “or” logic)



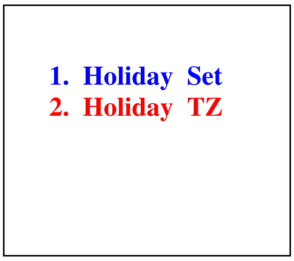
10. Press “1” to assign the Holiday Set no.



HolidayList ID:

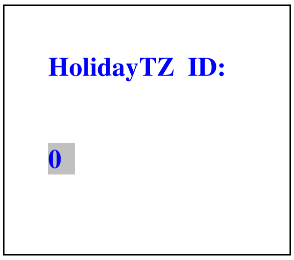
0

11. Input the holiday list no., Press "#" to save and return to previous menu



1. Holiday Set
2. Holiday TZ

12. Press "2" to assign the Holiday TZ



HolidayTZ ID:

0

13. Input the TZ no. and press "#" to save and return to previous menu.

Press "ESC" return to "holiday set" menu
➲ Note: repeat step 8 -12 for another "holiday set" setting if any.

7.3.4 User Profile

The user can define the User Profile Options in accordance with his own requirements.

Enter the menu to check certain user's Access Profile Options status.

User Profile include: (the belonged) grouping setting, user personal time zone, and the user setting (follow by personal TZ or group TZ)

Grouping setting: Divides the registered users into certain groups for the purpose of management.

Use group time zone: To select the user default time access method the user belonged to and either of options "personal TZ" or "group TZ" or "personal and group TZ" (satisfy either of it)

User personal time zone: To set user's unlocking time by selecting list number of time zone.

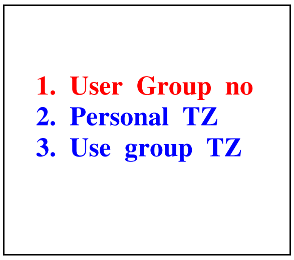
✍Note: Relationships between the use group time zone and the user time zone

The effect of the personal TZ" or "group TZ" or "personal and group TZ" options in the "Use Group Time zone" are as follows:

If the User follows "group TZ" is "selected", then user time zone will automatically be assigned the value of the serial number of time zone of the group belonged to (the group time zone should be set in advance).

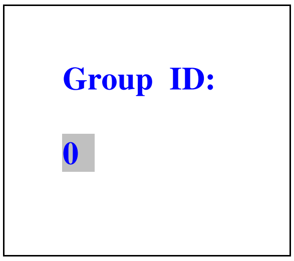
The following steps show how to register a User into a Group

LCD Display	Description
1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test	In the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "4" for Access Option (A function to assign access time zone)
1. Define TZ 2. Use Profile 3. Group Define 4. Holiday Schedule 5. Access Comb 6. Door For Open 7. Door For Close 8. Lock Open Time 9. Period Access	2. Select the item "2" or use up down arrow to select the item option.
ID: ▮	3. Input "user ID" to assign her time zone, press "#" after input the ID.



1. User Group no
2. Personal TZ
3. Use group TZ

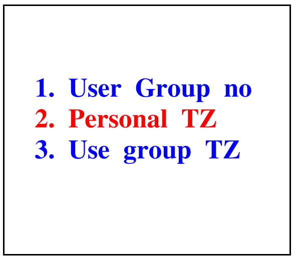
4. Enter “User Profile” and screen displays as follows. Press “1” to assign user belonging group.



Group ID:

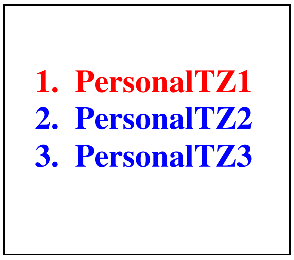
0

5. Input the group ID & press “#” to save and return to previous menu.



1. User Group no
2. Personal TZ
3. Use group TZ

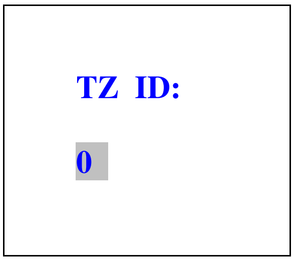
6. Press “2” to assign the Personal TZ



1. PersonalTZ1
2. PersonalTZ2
3. PersonalTZ3

7. Press “1” to assign the Personal time zone with selecting the TZ no.

➲ Note: Max. 3 personal TZ per user.

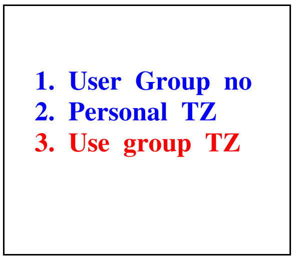


TZ ID:

0

8. Input the TZ no. and press “#” to save and return to previous menu.

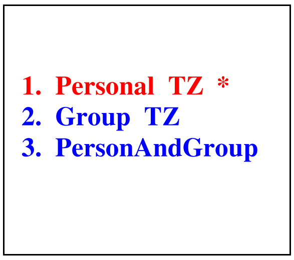
➲ Note: repeat step 7 for another personal TZ setting if any.



1. User Group no
2. Personal TZ
3. Use group TZ

After assigning the personal TZ, press “ESC” to return previous menu.

9. Press “3” to assign “user time access method”, the following interface will show three options.



1. Personal TZ *
2. Group TZ
3. PersonAndGroup

10. You can select “1”, “2”, “3” to assign the user who follows the time access method with personal TZ only, Group TZ only and either “Personal TZ and Group TZ”. Press “ESC” to save and return to the upper menu.

➲ Note: option 3 “person and group” is effective in time zone whether personal or group zone is valid.

7.3.5 Access Combination

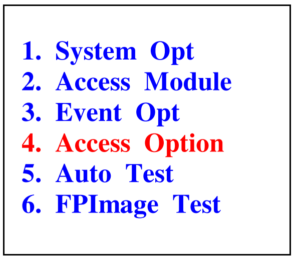
The Access combination is a factor to control the unlocking of the door with multiple users. For example, to access with 2 group user authentication, set a combination list with group 1 or group 2, so that the group 1 user access the door that must verify the authentication with group 2 user.

The Access combination definition is used to define the access combinations where each combination is composed of different groups. The Access combination directly uses group number no matter the user verification sequence between the groups. For example, combination no. 1 have group 1, group 2, group 3, group 4 and group 5; whereas at least one user in each group is required to jointly pass the verification to unlock the door. The system can simultaneously defines a maximum of 5 groups combination and 50 sets combination list where access will be granted if one of them passes the verification.

The following steps show how to register access combination

LCD Display

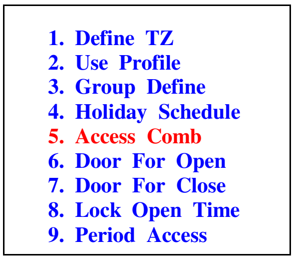
Description



1. System Opt
2. Access Module
3. Event Opt
4. Access Option
5. Auto Test
6. FPImage Test

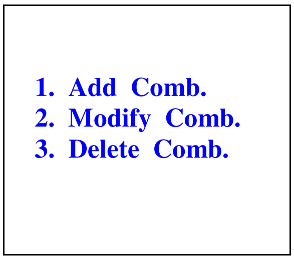
In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page.

1. Press “4” for Access Option (A function to assign access time zone)



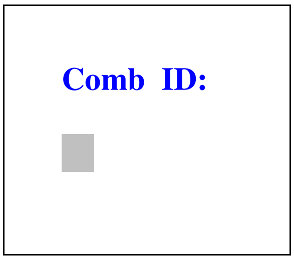
1. Define TZ
2. Use Profile
3. Group Define
4. Holiday Schedule
5. Access Comb
6. Door For Open
7. Door For Close
8. Lock Open Time
9. Period Access

2. Select the item “5” or use up down arrow to select the item option.

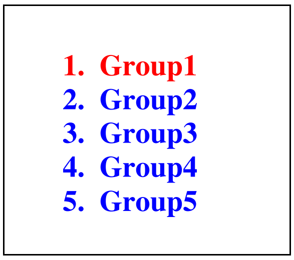


3. Select "add Comb." or press "1" to create combination list, "modify comb." to modify existing time zone or "delete comb." to erase the combination list created.

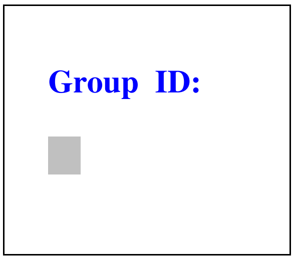
➲ Note: In the "modify" or "delete" option, you can key in "*" to list out existing item. In the "delete" option, you can choose delete one by "1. ID" or delete all by"2. All" option.



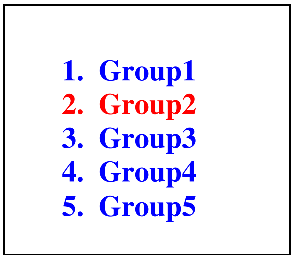
4. Input the ID for combination list, press "#" to save



5. Select the Group 1 or press "1" to assign the combination with the first group no.



6. Input the ID for the group no., press "#" to save and return to previous menu



7. Select the Group2 or press "1" to assign the combination with the second group no.

➲ Note: repeat step 5-6 for another group into the list, if any group to be associated.

➲ Note: The above-mentioned combinations setting indicate that: Group 1 & group 2 is a combination. That makes the user (either one) belonging to group 1 must verify with group 2 user (either one) to gain access

7.3.6 Door Forced Open Schedule

The "Door Forced Open Schedule" is a function to set "always-open" door when enabled with a group time zone. Hence, it will follow a group schedule to always open the door automatically.

The following steps show how to register "door forced open schedule"

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "4" for Access Options (A function to assign access time zone)
1. Define TZ **2. Use Profile** **3. Group Define** **4. Holiday Schedule** **5. Access Comb** **6. Door Forced Open** **7. Door Forced Close** **8. Lock Open Time** **9. Period Access**	2. Select the item "6" or use up down arrow to select the item option
1. Enable **2. Disable**	3. Select "Enable" or press "1" to activate this function, select "Disable" or press "2" to deactivate this function
Group ID: ▨	4. Input the ID for the group no., press "#" to save and return to previous menu ➲ Note: you can press "*" to erase the number.

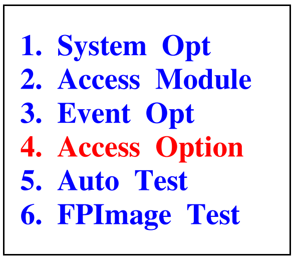
7.3.7 Door Forced Close Schedule

The "Door Forced Close Schedule" is a function to set "always-close" door when enabled with a group time zone. Hence, it will follow a group schedule to always close the door automatically.

The following steps show how to register "door forced close" function

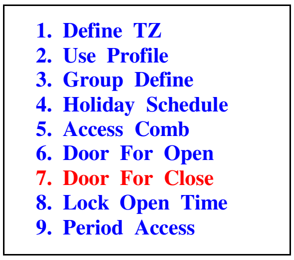
LCD Display

Description

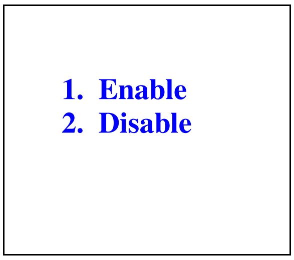


While in the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page.

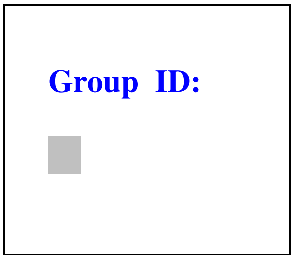
1. Press "4" for Access Options (A function to assign access time zone)



2. Select the item "7" or use up down arrow to select the item option.



3. Select "Enable" or press "1" to activate this function, select "Disable" or press "2" to deactivate this function



4. Input the ID for the group no., press "#" to save and return to previous menu

➲ Note: you can press "*" to erase the number.

7.3.8 Lock Open Time

The “lock Open Time” is a function to modify the lock open time (Max. 50 sec.)

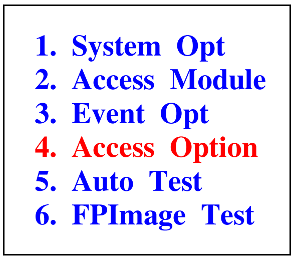
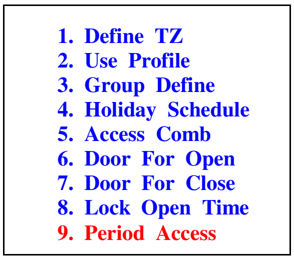
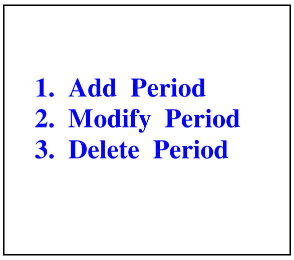
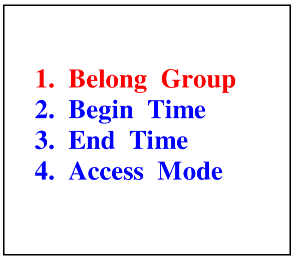
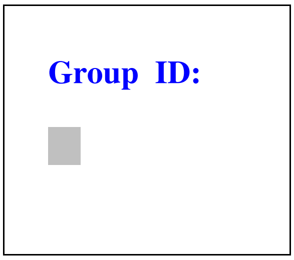
The following steps show how to modify the lock open time

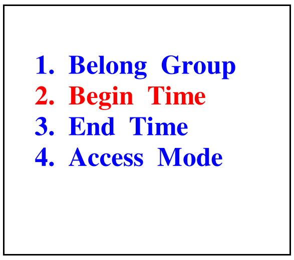
LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “4” for Access Option (A function to assign access time zone)
1. Define TZ **2. Use Profile** **3. Group Define** **4. Holiday Schedule** **5. Access Comb** **6. Door For Open** **7. Door For Close** **8. Lock Open Time** **9. Period Access**	2. Select the item “8” or use up down arrow to select the item option.
SEC: **5**	3. Input the time and press “#” to save and return to previous menu.

7.3.9 Period Access

The "period access" is a function to change group user access mode when the time period. For example, in office hour 09:00 to 18:00, user can use Card only. After the time it will follow his own access mode e.g. FP.

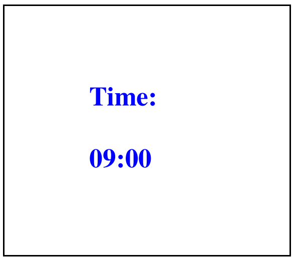
The following steps show how to register a "Period Access" list

LCD Display	Description
 1. System Opt 2. Access Module 3. Event Opt 4. Access Option 5. Auto Test 6. FPImage Test	In the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "4" for Access Option (A function to assign access time zone)
 1. Define TZ 2. Use Profile 3. Group Define 4. Holiday Schedule 5. Access Comb 6. Door For Open 7. Door For Close 8. Lock Open Time 9. Period Access	2. Select the item "9" or use up down arrow to select the item option.
 1. Add Period 2. Modify Period 3. Delete Period	3. Select "add period" or press "1" to create period access, "modify period" to modify existing time zone or "delete comb." to erase the combination list created. ➲ Note: in the "modify" or "delete" option, you can key in "*" to list out existing item. In the "delete" option, you can choose delete one by "1. ID" or delete all by"2. All" option.
 1. Belong Group 2. Begin Time 3. End Time 4. Access Mode	To create the period access, you are required to fill up this 4 item to activate the function. 4. Select "Belong Group" ore press "1" to assign the group user.
 Group ID: ▒	5. Input the ID for the group no., press "#" to save and return to previous menu ➲ Note: you can press "*" to erase the number.

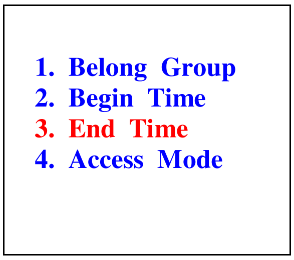


Set this group with the corresponding time period.

6. Select “Begin Time” or press “2” to assign the starting time.

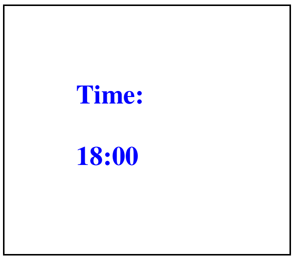


7. Input the time and press “#” key to save and return to previous menu.

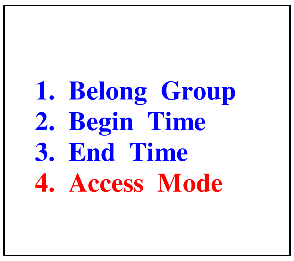


Set this group with the corresponding end period.

8. Select “End Time” or press “3” to assign the starting time.

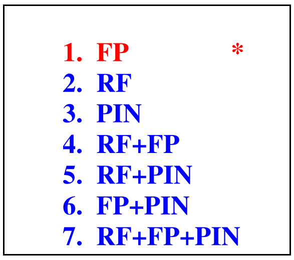


9. Input the time and press “#” key to save and return to previous menu.



Set this group with the corresponding access mode.

10. Select “Access mode” or press “4” to assign the group user.



Set this group with the corresponding access mode.

11. Select “mode” or press item no. to assign the access mode. Press “#” to select and press “ESC” to save and return to previous menu.

7.4 Auto Test

In this option, you can run System device test. In the event of device failure, you can analyze the cause of the device's fault and the devices will be quickly and easily maintained.

It tests the keyboard, LCD, FP sensor, voice and match time. In the course of the test, you should guarantee the stability of the power. Otherwise, the system's hardware is probably damaged;

The following steps show how to run the Auto Test Option in terminal

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	In the standby mode, press the [MENU] key to enter the Setup menu. Press "2" to enter Options page. 1. Press "5" for Auto Test (A function to test the terminal)
1. Run All Test **2. Keyboard Test** **3. LCD Test** **4. FP Sensor Test** **5. Voice Test** **6. Match Time Test**	2. Select the item "1" to run all test or use up down arrow to select the item option.
Keyboard Test **Test Succeed**	3. During the test, the system will prompt for press finger to test the FP sensor or press the key. After all test, a "Test Succeed" appears.
1. Run All Test **2. Keyboard Test** **3. LCD Test** **4. FP Sensor** **5. Voice Test**	4. For the option 2- 4, it is a individual test for troubleshooting purpose **Keyboard test**: press each of key in keypad, the corresponding number disappears **LCD Test**: a screen self-test appears **FP Sensor**: prompt for press finger and a "sensor ok" appears if the sensor is normal **Voice Test**: self-test for voice file. **Match Time Test**: a Fingerprint processing time counter. It can show the processing time to recognize a finger.

7.5 Fingerprint Image Test

In this option, you can enable or disable the test item. In the event of device testing with SDK, you can analyze the device by traffic simulation. Developer can operate the devices quickly and easily maintained.

The following steps show how to run the FPImage Test Option in terminal

LCD Display	Description
1. System Opt **2. Access Module** **3. Event Opt** **4. Access Option** **5. Auto Test** **6. FPImage Test**	In the standby mode, press the [MENU] key to enter the Setup menu. Press “2” to enter Options page. 1. Press “6” for Auto Test (A function to test the terminal)
1. Yes * **2. No**	2. Select “1” for enable this function (A function to test the terminal) 3. Select “2” for disable this function.

8 Network

For i4 Flexi, “Ethernet, RS485” and “Wiegand Input or Output” is simultaneous. However, Ethernet and RS485 are alternatives. If the Ethernet is used, RS485 cannot be used. Likewise, if the RS485 is used, the Ethernet cannot be used.

Terminal ID: The machine number ranges from 1 to 999
Baud rate: The communication speed of the communication with the computer at 19200.
Device IP address: The default IP is 192.168.0.201. You may modify it according to your requirements.
Subnet Mask: The default subnet mask is 255.255.255.0,
Gateway: The default gateway is 192.168.0.200
Host IP: The host computer IP to manage the terminal. You may modify it according to your requirements.
Host Port: The default port number is 8008. Except for special circumstances, this number should not be changed.
Mac Address: Display the MAC address.
HostDomainName: Display the host domain name.
Preferred DNS: The preferred domain name server.
Alternate DNS: The alternate domain name server.
Network speed: The default network speed is 10M, 100M or AUTO detect.
COMM Key: The System default keyword is none, which is optional to be modified. COM Key is a security code when communicate with PC software. Connection established when COM key matched.
Wiegand Output: To assign the Wiegand output type: 26 bit or 34 bit or disable
Wiegand Input: To assign the Wiegand input mode: Out Door Card or In Door Card
Wiegand Content: to assign the Wiegand data content: Card Number or User ID.

⚠ **Warning:** *When RS485 communication used in the outdoor environment, the lightning protection device needs to be installed.*

8.1.1 Terminal ID

To operate terminals in the network users must first choose an ID. Users can select “3. Network =>2.Terminal => new TID“ for as many as 999 terminals and then choose “MENU“ to store data.

The following steps show how to enter network option page

LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press “3” to enter Network page. (A function to set the networking option)
1. Terminal **2. Controller** **3. Network Mode**	2. Press “1” key or select the item with “#” key to enter.
Terminal ID **ID (1-999):** **123**	3. Input the terminal ID and press “#” to save and return to previous menu

8.1.2 Controller SN

To access the Controller SN registration function on the LCD window, go to the stage "3.Network=>2 Controller , => input serial number of controller" and set details.

To activate other communication functions, the main unit sends a register command to the controller. This only needs to be done once for each unit-controller pair. If either the main unit or the controller has been replaced, an error will occur during communications. In such instances, registration should be repeated.

A relay function inside the controller manages the Ethernet cable. During initialization, the Ethernet cable is disconnected, but it becomes connected after registration of the main unit.

The following steps show how to register controller serial number into terminal

LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "3" to enter Network page. (A function to set the networking option)
1. Terminal **2. Controller** **3. Network Mode**	2. Press "2" key or select the item with "#" key to enter. .
ID: **14600003**	3. Input the serial number of controller and press "#" to save and return to previous menu. ➲ Note: The controller serial number is 8 digit number and the label stick at the bottom of controller unit.

8.1.3 Network Mode

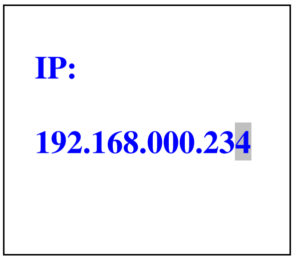
The Network mode option is a function to set the event log output to network or to Wiegand. Also, it is a function to assign the network parameter. In addition, it is an operation mode with "Wiegand" setting:

8.1.3.1 TCP/IP

Select these methods when you use the Internet to access the terminal. Follow the process "3.Network =>3.Network Mode=>2.TCP/IP", press "#" to enter the setup menu.

The following steps show how to register TCP/IP parameter

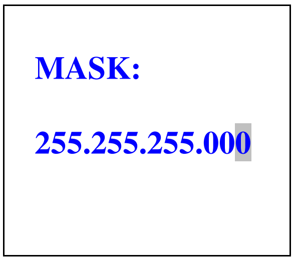
LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "3" to enter Network page. (A function to set the networking option)
1. Terminal **2. Controller** **3. Network Mode**	2. Press "3" key or select the item with "#" key to enter.
1. WiegandOutput **2. TCP/IP** **3. Com Key** **4. WiegContent**	3. Press "2" key or select the item with "#" key to enter. The following interface appears
1. Device IP **2. Subnet Mask** **3. Gateway** **4. Host IP** **5. Host Port** **6. MAC Address** **7. HostDomainName** **8. Preferred DNS** **9. Alternate DNS**	4. Press the key number or select the item with "#" key to enter the setting menu of each function. ➲ Note: Press "#" key to save and return to previous menu after each setting modified.



IP:

192.168.000.234

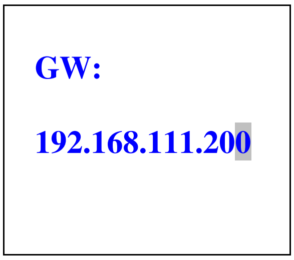
5. **Device IP -** Input the number to the field and Press "#" to save.



MASK:

255.255.255.000

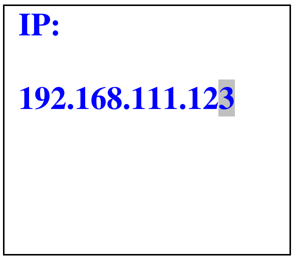
6. **Subnet Mask -** Input the number to the field and Press "#" to save.



GW:

192.168.111.200

7. **Gateway -** Input the number to the field and Press "#" to save.

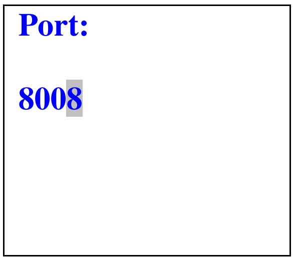


IP:

192.168.111.123

8. **Host IP -** Input the number to the field and Press "#" to save.

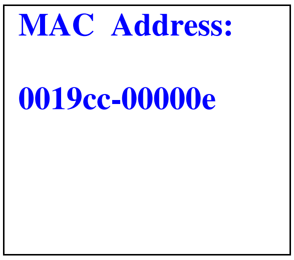
➲ Note: If you want to use the host domain name to retrive the host IP address from DNS server, the host IP in here must be set to 0.0.0.0



Port:

8008

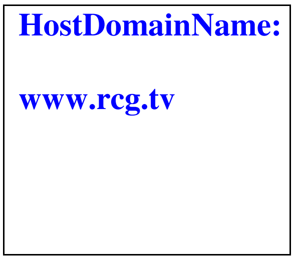
9. **Host Port -** Input the number to the field and Press "#" to save.



MAC Address:

0019cc-00000e

10. **MAC Address –** Display the MAC Address.

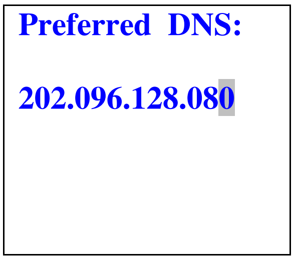


HostDomainName:

www.rcg.tv

11.**HostDomainName-** Display the host domain name.

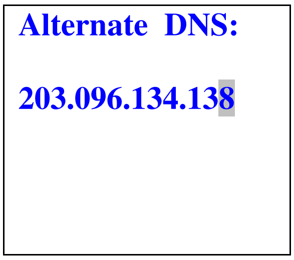
➲ Note: 1) For using the host domain name to retrive the host IP address from DNS server, the host IP in the device must be set to 0.0.0.0
2) The host domain name can be configured by software/SDK.



Preferred DNS:

202.096.128.080

12.**Preferred DNS -** Input the number to the field and Press "#" to save.



Alternate DNS:

203.096.134.138

13.**Alternate DNS –** Input the number to the field and Press "#" to save.

8.1.3.2 Com Key

COM Key is a security code used when communicating with PC software. Connection established when COM key matched

The following steps show how to register COMM key parameter

LCD Display	Description
1. User 2. Options 3. Network 4. Svs Info	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press “3” to enter Network page. (A function to set the networking option)
1. Terminal 2. Controller 3. Network Mode	2. Press “3” key or select the item with “#” key to enter.
1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent	3. Press “3” key or select the item with “#” key to enter.
Key:	4. Input the key (max. 8 digit). ➲ Note: Once the key entered, the server software can establish the connection if the Key inputted here is matched.

8.1.3.3 Wiegand Content

The Wiegand content is a function to select the data content for 1. Card Number, 2. User ID. This enables the Wiegand output data content as card number or user ID, depends on real situation or application.

The following steps show how to select the Wiegand content parameter

LCD Display	Description
1. User 2. Options 3. Network 4. Sys Info	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "3" to enter Network page. (A function to set the networking option)
1. Terminal 2. Controller 3. Network Mode	2. Press "3" key or select the item with "#" key to enter.
1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent	3. Press "4" key or select the item with "#" key to enter.
1. Card 2. User ID	4. Select the option "1" card data or "2" User ID data. . ➲ Note: this enables the Wiegand output data to be card number or user ID.

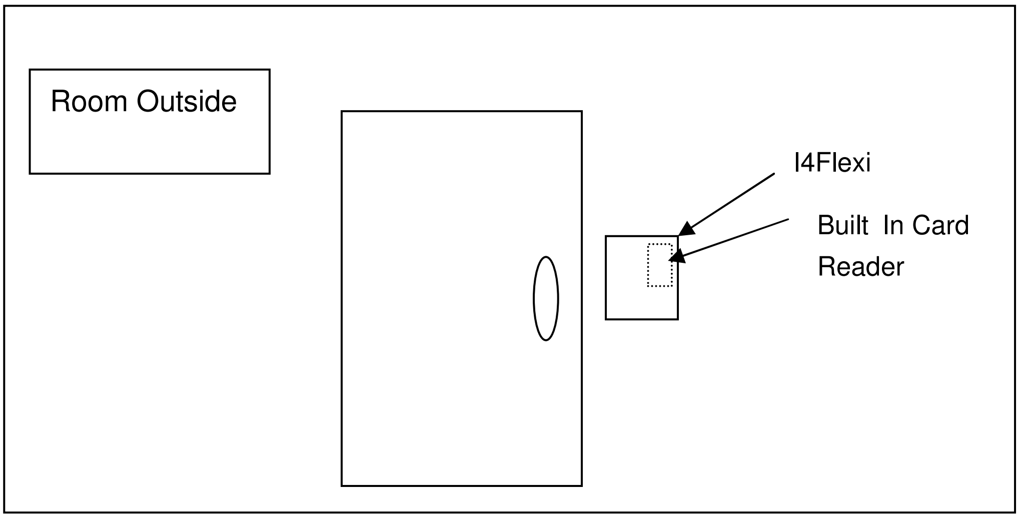
8.1.3.4 Wiegand Input

The Wiegand input is a function to build an application with external reader to form a professional access control. For example, some end user would like to change the front end input to be more accuracy data & enhance security. We may plug the i4 flexi with Access method RF+FP as entrance, while plug a RF reader as exit.

Example 1

(Built-in module, without external Wiegand reader)

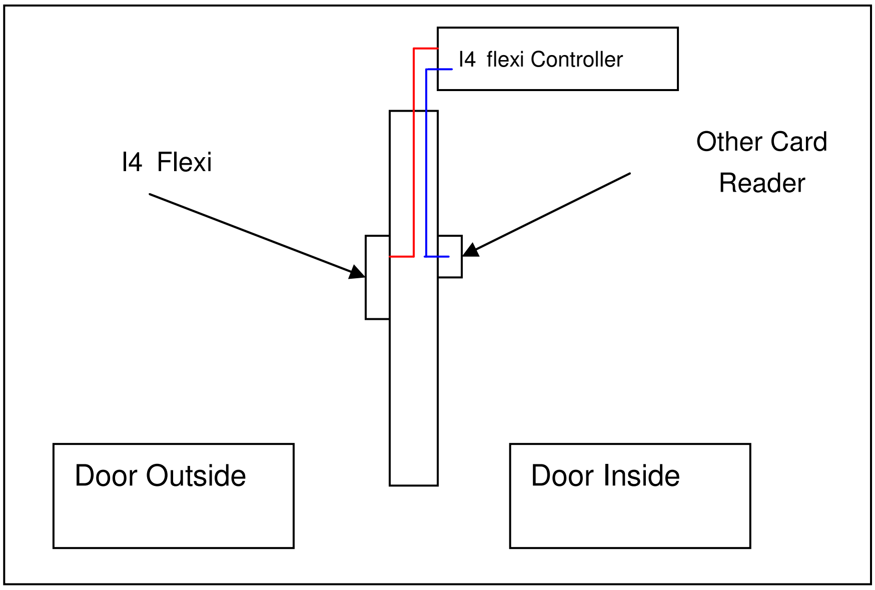
Built-in RF Module Access Module: Follow the User Access Method (FP only, RF only, RF + FP, RF + FP + PIN etc.)



Example 2

(Built-in module + External Wiegand reader) <- ***set the Wiegand Input as "In Door Read Card" mode***

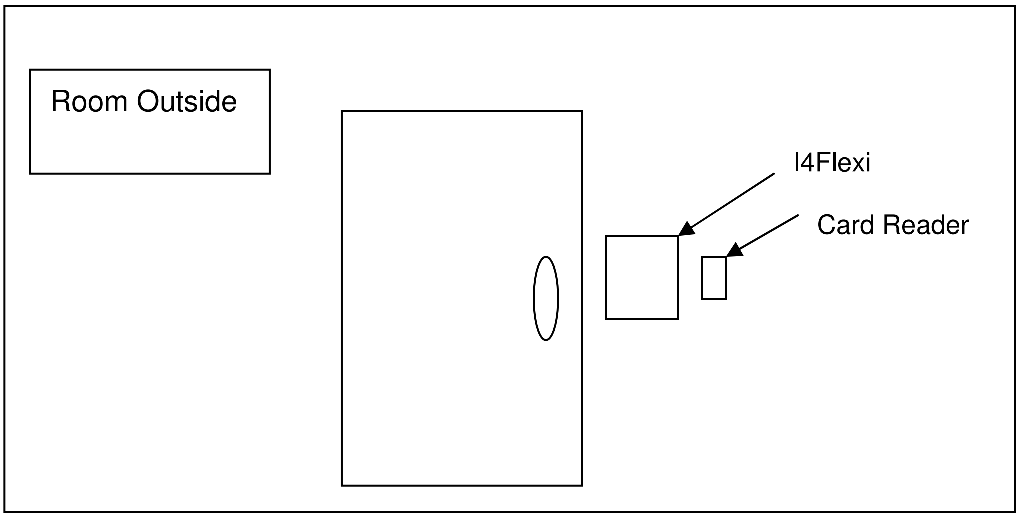
Built-in RF Module Access Module: Follow the User Access Method (FP only, RF only, RF + FP, RF + FP + PIN etc.)
Outside Wiegand Module: ONLY RF



Example 3

(Without built-in RF module, External Wiegand reader only) <- ***set the Wiegand Input as "Out Door Read Card" mode***

External Wiegand reader: Following the User Access Method (FP only, RF only, RF + FP, RF+ FP+ PIN etc.)



Summary

- If you connect with Built-in RF Module only, follow the User Access Method you have preset.

- If you connect external reader only, follow the User Access Method you have preset.

- If you connect with both Built-in RF Module and External Reader, the Built-in RF Module will follow the User Access Method and external Reader must be card only.

The following steps show how to select the Wiegand input mode

LCD Display	Description
1. User **2. Options** **3. Network** **4. Svs Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "3" to enter Network page. (A function to set the networking option)
1. Terminal **2. Controller** **3. Network Mode**	2. Press "3" key or select the item with "#" key to enter.
5. WiegandInput	3. Press "5" key or select the item with "#" key to enter.
1. OutDoorRCard **2. InDoorRCard ***	4. Select the option "1" or "2" for the application installed. ➲ Note: this enables the Wiegand Input mode to be "Out Door Read Card" or " In Door Read Card". (see example 2 or 3 as mentioned above)

8.1.3.5 Wiegand Output

The Wiegand output is a function to export transaction in real time to other access controller following the Wiegand standard 26 bit or 34 bit. When this is enabled, there should be another access controller connected with i4 Flexi's controller via Wiegand connection. It is the easier way to replace the existing card system but remains the aged controller as reporter and compatible aged HR software.

The following steps show how to select the Wiegand Output mode

LCD Display	Description
1. User 2. Options 3. Network 4. Sys Info	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "3" to enter Network page. (A function to set the networking option)
1. Terminal 2. Controller 3. Network Mode	2. Press "3" key or select the item with "#" key to enter.
1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent 5. WiegandInput	3. Press "1" key or select the item with "#" key to enter.
1. 26 Wiegand 2. 34 Wiegand 3. Disable *	4. Select the option "1" or "2" or "3" for the application installed. ➲ Note: this enables the Wiegand Output mode to be "26 bit wiegand output " or " 34 bit wiegand output" or disabled.

9 System Information

The system capacity can be checked by using system information. All the log usage, user usage, free space usage, device name, device serial number, device software version and algorithm version can be checked in the system information.

The following steps show how to view the system information

LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "4" to enter System Info page. (A function to view the terminal status)
1. User Cnt **2. FP Cnt** **3. Att Log** **4. Admin Cnt** **5. Pwd User** **6. System Logs** **7. Free Space Inf** **8. Dev Info**	2. Press [Down] key to search for either one of EIGHT Options. Press "#" to enter the setting menu of [Free Space Info] & [Dev Info] function
1. User Cnt **2. FP Cnt** **3. Att Log** **4. Admin Cnt** **5. Pwd User** **6. System Logs**	3. Provides information on no. of user counts, no. of fingerprint counts, no. of password users, no. of administrator counts, no. of attendance log and no. of supervisory log in the terminal
User Count **5**	For Example, to check no. of user in the terminal 4. Press "1" or select "User Cnt" and press "#" to enter, the following interface appears

9.1.1 Free Space Information

The "free space information" is a function to calculate 'space' available for no. of fingerprint, no. of log and no. of supervisor log.

The following steps show how to view the system information

LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press "4" to enter System Info page. (A function to view the terminal status)
1. User Cnt **2. FP Cnt** **3. Att Log** **4. Admin Cnt** **5. Pwd User** **6. System Logs** **7. Free Space Inf** **8. Dev Info**	2. Press "7" or press [Down] key to search for "free space inf" Options. Press "#" to enter the setting menu of [Free Space Info].
1. FP Cnt **2. Att Log** **3. Super Log**	3. Press "1" to select "FP Cnt", the following interface appears
FP Cnt **4995**	4. It shows the no. of remaining FP space in system and return to previous menu after 2 second

9.1.2 Device Information

The “Device information” is a function to show the default information of the unit, e.g. capacity of FP, Log, supervisor log, manufacturing time, serial number, vendor name, algorithm version and firmware version.

The following steps show how to view the device information

LCD Display	Description
1. User **2. Options** **3. Network** **4. Sys Info**	In the standby mode, press the [MENU] key to enter the Setup menu. 1. Press “4” to enter System Info page. (A function to view the terminal status)
1. User Cnt **2. FP Cnt** **3. Att Log** **4. Admin Cnt** **5. Pwd User** **6. System Logs** **7. Free Space Inf** **8. Dev Info**	2. Press “8” or press [Down] key to search for “free space inf” Options. Press “#” to enter the setting menu of [Dev Info].
1. FP Cnt **2. Att Log** **3. Super Log** **4. Manu Time** **5. Serial Num** **6. Vendor** **7. Alg Version** **8. Firmware Ver**	**Dev info** - shows the device capacity, the date of production, the serial number and the version information. **FP Cnt** – shows the capacity of this terminal for Fingerprint storage limit is 5000. **Att Log** – shows the capacity of this terminal for Attendance log storage limit is 50000. **Super Log** – Shows the capacity of this terminal for supervisory log storage limit is 250 **Manu Time** – Shows the date of production. **Serial Num** – Shows the serial number of this terminal. **Vendor** – Shows the name of the vendor **Alg Version**- Shows the algorithm version of this terminal **Firmware Ver**. – Shows the firmware version of this terminal.

10 Appendix 1 – i4Flexi Alarm Operation

Type of Alarm provided in i4Flexi

1. Tamper Alarm
2. Forced Open Alarm
3. Door Left Alarm
4. Alarm Finger
5. General Purpose Input Alarm

Type	Response Port	Reset Method	Remark
Tamper Alarm	ALARM	Authorized User Verified by any method	Built in
Forced Open Alarm	GPO	Authorized User Verified by any method	Sensor required
Door Left Open Alarm	ALARM	Authorized User Verified by any method	Sensor required
Alarm Finger	ALARM	Authorized User Verified by any method	Default feature
GPI Alarm	GPO	Authorized User Verified by any method	Sensor required

Basically, the alarm raised in i4Flexi will trigger a electrical contact output (either Alarm port or General Purpose Output [GPO] port) for connecting external alarm device. E.g. Siren, Buzzer, Alarm Centre, Auto Dialer.

Example of Alarm

Tamper Alarm

Prize open the i4Flexi Main Unit shell. The Alarm relay is turn ON in the controller alarm port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port <Depends on jumper setting>.

Forced Open Alarm

The "Alarm for Invalid Door Opening" is applied in the system parameters; an alarm will be triggered in the event the user pushes the door open to enter without system verification. The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

Door Left Open Alarm

The "Alarm for Door Left Opening" is applied in the system parameters. This alarm will be triggered when the valid door opening time exceeded. The ALM relay is turn ON in the controller ALM port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

Alarm Finger

The "Alarm Finger" is applied in the system parameters. The fingerprint detected by the system for fingerprint verification upon door opening will be the registered alarm finger verified. The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

General Purpose Input Alarm

The "Alarm for GPI" is applied in the system parameters; an alarm will be triggered in the event the user pushes the sensor (Motion detector, Door Sensor, Output of other device). The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

Warning:

a. The Alarm / GPO Output port relay is limited max. 3A 120VAC current rating.

b. The Door Sensor (DS) / General Purpose Input (GPI) port is supposing

b. The total current rating is subjected to "Power Supply Rating > total system consumption" but limited less than *3A* current. **Failure to do so could result in electric shock leading to serious bodily injury or death.**

Alarm Operation

1. Tamper Alarm

When i4Flexi casing is prizing, it will case the case sensor to turn ON and activate the "tamper alarm" and turns ON corresponding device to operate if any.

Tamper Alarm => make controller "ALM" port" ON => electrical contact ON

Notes: ***RESET ALARM: If the shell is closed properly. The alarm will be off.*

2. Forced Open Alarm

Caution: To enable this feature, a ***"Normal Open Door Sensor (Dry Contact)"*** is required.

The “Alarm for Invalid Door Opening” is applied in the system parameters; an alarm will be triggered in the event the user pushes the door open to enter without fingerprint verification.

Notes: **RESET ALARM: Verification of any authorized finger.

3. Door Left Open Alarm

Caution:

1) To enable this feature, a “Normal Open Door Sensor (Dry Contact)” is Required.

2)The door left time is configured in Menu->2.Option->3.Event Opt->7. Door Open Alarm

The “Alarm for Door Left Opening” is applied in the system parameters; an alarm will be triggered in the event the user left the door open after a period of time.

Notes: **RESET ALARM: Verification of any authorized finger.

4. Alarm Finger

When user the registered alarm finger. System will assume the user is under highjack. GPO port will be trigger.

Caution: To enable the feature, you must ***enroll alarm finger*** into device.
Notes: **RESET ALARM: Verification of any authorized finger.

5. General Purpose Input Alarm

Caution: To enable this feature, a ***“Normal Open Sensor (Dry Contact)***” is required.

The “Alarm for General Purpose Input” is applied in the system parameters; an alarm will be triggered in the event the user pushes the sensor.

Notes: **RESET ALARM: Verification of any authorized finger.

Indicator Light

There are three indicator lights in the Controller:

	Red Light	**Yellow Light**	**Green Light**
Lock Control Unit	Power Connected	Light blinking while traffic with processor	Unlock legally

11 Glossary

User: type of user

Alarm Finger: a finger is defined as special function

Normal Door Open: Authorized verification to open the door

Invalid Door Open: Any door opening action other than Normal door opening

Card, Fingerprint and password verification: authentication mode

Finger relevancy: User security level

FRR: ‘False Rejection Rate”

FAR: “False Acceptance Rate”

DC: Direct Current

GND: -ve or return path, called Ground

Tx: Transmit

Rx :Receive

GPI: General Purpose Input

GPO: General Purpose Output

NO: Normal Open

NC: Normal Close

DS: Door Status

IS: Indoor Switch, (Exit button)

FP: Fingerprint

RF: Radio Frequency Card

PIN: Password

12 Support Information

Web Site	http://www.rcg.tv/support/
Hotline Support	Hong Kong : 852-36696999 Malaysia : +6-03-51248888 Customer Service is available : Monday to Friday 9:00 am – 6:00 pm(local time)
Support Email	support@rcg.tv