Contents

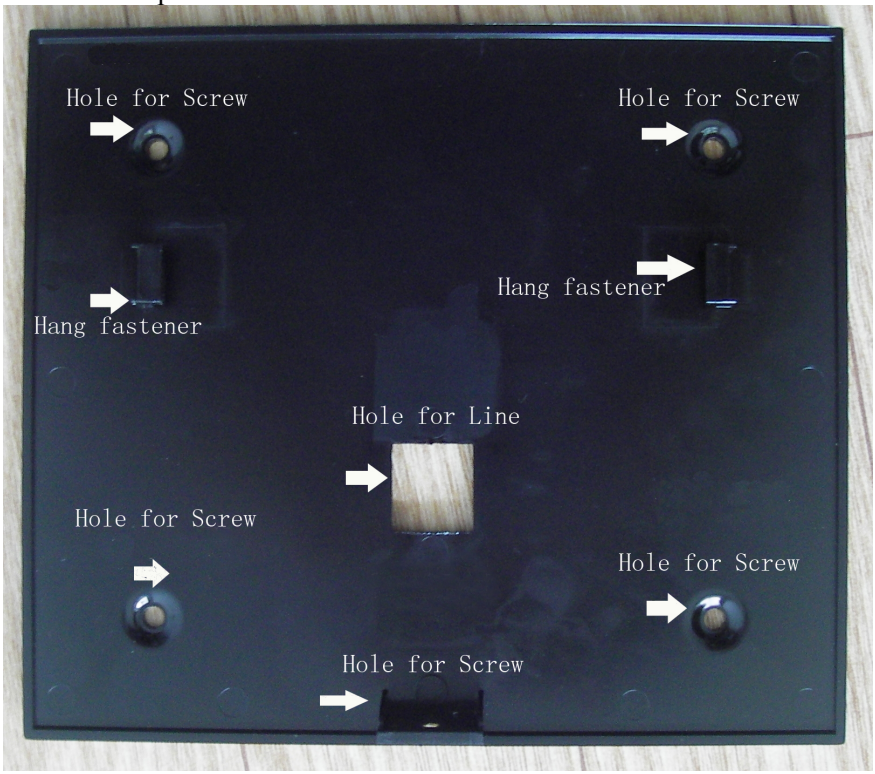
1 Necessary To Know

Don’t install the device under direct strong sunlight. Strong sunlight affects collecting of fingerprint and it may cause failure on the fingerprint authentication.

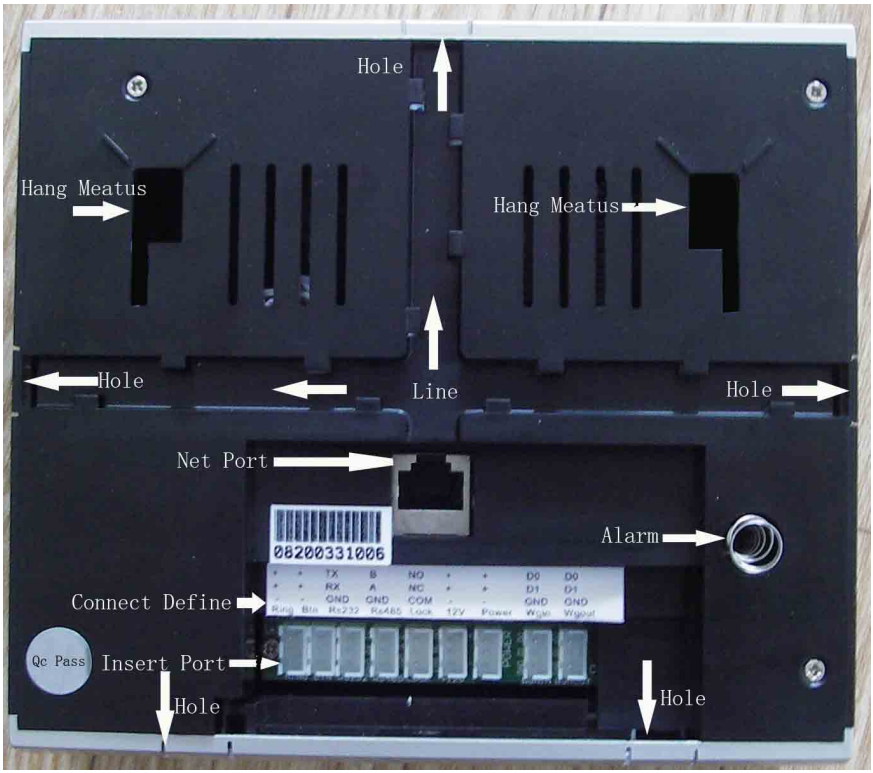
During summer it’s highly recommended not to use outdoor. The device working temperature scope is 0-40^{0}C. Long time using outdoor plus the heat of device itself may lead to slow reaction of device and less pass rate. Once it’s necessary to use outdoor, a sunshade and a set of cooler radiation are recommended.

Loosen off the screw in the middle of back lateral which also has RESET hole, take off mounting panel (for mounting and fixed on the wall), the screw hole shown as below:

For mounting panel, it has 4 holes respective for those screw holes fixed on the wall or other objects. Mounting panel clip to securing the device to be fixed with its panel and cable hole for cable out.



Below is for function flag illustration of device back panel, in which has lead slot, mounting slot, cable hole, wire connection slot, connection define, Ethernet interface and spring of anti-theft alarm.


Hole
Hang Meatus
Hang Meatus
Hole
Line
Hole
Net Port
Alarm
Connect Define
Qc Pass
Insert Port
Hole
Hole

2 Introduction

This chapter contains the common concept & fingerprint pressing way of Z6 series T&A devices.

Here below is the picture of device outlook:

Pic. 1-1 Outlook

Z6

Pic. 1-2 Small keyboard

Keyboard definition:

OK To confirm the current operation;
MENU Under initial status press this key to enter into management Interface
ESC Cancel current operation
▲ Page up
▼ Page down
CALL To control remote doorbell;
0-9 To input digit 1-9

2.1 Basic Concept

It contains the definition & description of basic concepts, including:
- User Enroll
- User Identification
- Safe grade
- User's ID number
- User's grade
- Initial Interface

The two most important functions of Z6 series T&A device are user enroll & user identificaiton.

2.1.1 User Enroll

Enroll is to creat a ID number for the user, and scan the user's same finger for three times to create characteristic code then associate this characteristic code with that ID number. This characteristic code will be treated as a module to store into memory of the device.

By comparing the stored fingerprint module with current finger scanning, it can be confirmed as the identity of the user.

A user who has already enrolled can be realized his/her Time & Attendance function with designated device. The whole process only lasts less than 2 seconds.

For same ID number, at most 10 different fingerprint could be enrolled so the user can have choice of different identification.

In the abstract, every finger of the user should be enrolled so that he/she can still carry out normal enroll with the backup fingers in case he/she get hurts on any finger. Normally it's recommended that at least two fingerprints should be enrolled, like left or right forefinger, thus the user can use any of his/her forefinger to identify and also avoid the identificaiton difficulty caused by forgetting to enroll fingerprint.

2.1.2 User Identification

Whenever the user press his/her fingerprint on the U fingerprint collector or input a ID number then input password or press fingerprint, the whole working process is an identification. And the system will prompt a success or failure result by the end of process and the successful comparison record will be stored into the device.

2.1.3 Safe Grade

Safe Grade is under Menu"Setting – Advanced setting", A safe grade is a balance between "Refust to judge" and "Wrongly judge". "Wrongly judge"is to judge user A's fingerprint as the one of user B, but "Refust to judge is refuse the fingerprint which has already been enrolled on this device.

It can be setup a safe grade suit to all users. Furthermore, for those fingerprints which is hard to identify, it's better to adopt the identificaiton of "ID+fingerprint", namely 1:1 comparison. Therefore the system will only adopt the data of 1:1 safe grade for comparison.

Once the user's finger was worn off or got hurt, the safe grade should be decreased. (Ref. Tab.1-1)

Please pay attention to that, FAR & FRR is mutually interacted, less FAR wil add more FRR and vice versa.

The defaulted safe grade value is 3, the defaulted 1:1 safe grade value is 1. Tab.1-1 is the safe grade setup under different situation.

Tab1-1 Safe Grade Legend

FRR	FAR	Safe Grade 1：N	Safe Grade 1：1
L	H	4	0
M	M	3	3
M	ML	2	2
M	L	1	1

2.1.4 User's ID number

For enrollment, the user will be allocated a ID number. When the user starts to identify his/her fingerprint, this ID number will be used to associated relevant fingerprint characteristic template or password.

ID nmber is input by the small keyboard, but it can also be input by other storage method like RF card (the precondition is that the device should be equipped with RF card reader first)

2.1.5 User's grade

Four user grades for Z6 series T&A device

User: Refer to those who need to pass identity identification for some purpose, for example, the one need to unlock door by device or to be recorded down in/out events.

Enter(Ent.) Manager: Those one who have right to enroll or delete user(s).

General(Gen.) Manager: For all the operation except for advanced setting and not for right of enrolling the user who is superior to the General manager.

Super(Sup.) Manager: The super user who can visit all system function and can also modify all setting of the system.

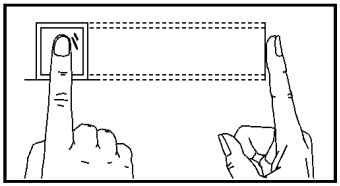
Note: Only when there are't General Manager and Super Manager, the Enter Manager can enroll the above two. The same, when there isn't Super Manager, the General Manager can enroll Sup. Manager. Once there exists more superior manager, the inferior manager can't enroll for hihger manager.

2.1.6 Initial Interface

After the device is powered on, the first interface shown on screen we called it as "Initial Interface". The below is an example:

2.2 The pressing method of fingerprint

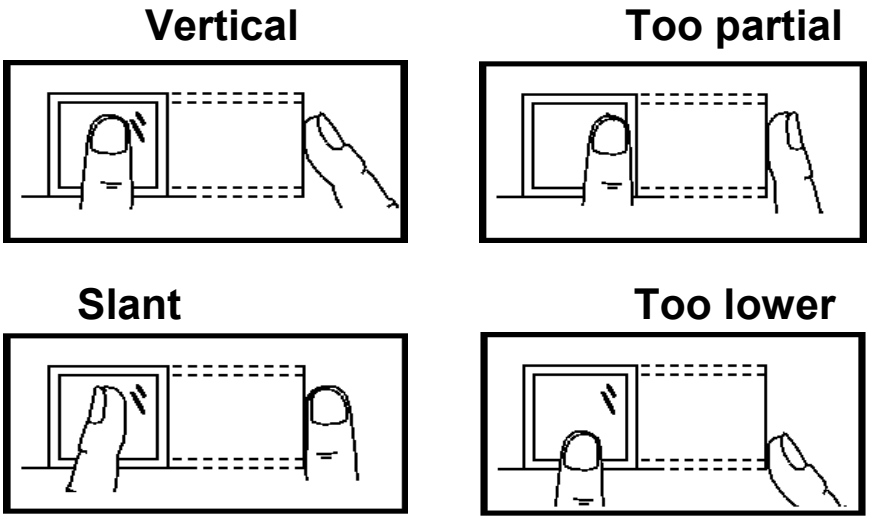
1 Illustraion of correct fingerprint pressing:



Flatly press fingerprint on U fingerprint collector

Try to press fingerprint center to the middle or a little upper of U collector

2 Several wrong pressing method:



Note: Please adopt correct fingerprint pressing method, and we don't undertake the possible less identification result caused by user's inproper operation and we reserve all rights of final explanation and amendment.

3 Enroll & Identification

This chapter contains how to enroll user on the T&A device, plus it also introduces how to identify the consistency of fingerprint enrolled.

It includes:
- User Enroll
- Verify enroll effect
- Backup fingerprint Enroll
- Identity identification
- Prompt of sucessful enrollment

Note: Once new user need to be enrolled, you need to at least act as either Enter Manager or General Manager or Super Manager. Details please refer back to 2.1.5 User Grade.

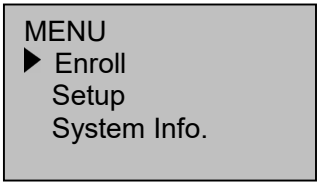
3.1 User Enroll

Once the administrator(Manager) has not been registered, anyone can enroll user.
Once the administrator(Manager) has been registered, you can only enroll user after the authentication of the administrator.

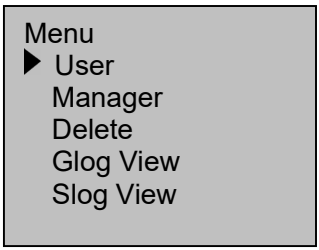
There are 5 enrolling method: Fingerprint enroll, Card enroll, Password enroll, Fingerprint + Password enroll and Fingerprint + Card enroll and they are suit for people of different need. Fingerprint enroll suits for those who have better quality finterprint and it occupies the most part of people. Fingerprint + Password suits to those who can pass fingerprint enroll but have difficulty on authentication and it occupies quite few proportion of people. Card enroll and Password enroll suit to those who can't successfully enroll their fingerprint and it occupies around 1% of people. Fingerprint + Card is similar to Fingerprint + Password but just dedicated for relevant people. Due to different choice and it will go for different submenu.

Once you wish to start user enroll, please first get your identity authentication pass ------ Press "MENU" and press your fingerprint or input password to start identification.
NOTE: Once there is no administrator(Manager) registered, you don't need such identification.

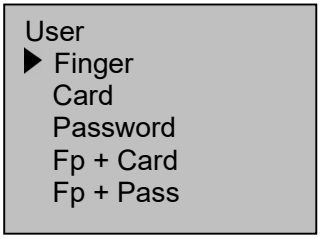
The identification is passed, then it will shown following info. on the screen:



Press OK to enter "Enroll" and the next step interface shown as below:



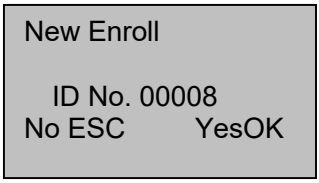
Press OK to enter “User” and the next step interface shown as below:



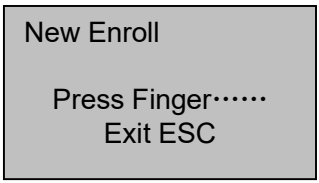
3.1.1 Fingerprint Enroll

（1）Select Finger, press OK to enter next step operation and info. shown as below:

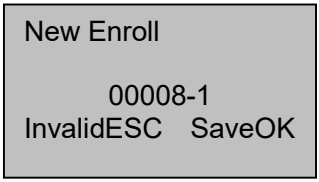
（2）Press “OK” to enter next step operation and info. shown as below:



（3）To input the ID No. you need to enroll in the “ID No.” column (It’s between 1-85534) press “OK” to enter next step operation and info. shown as below:



（4）According to prompt to continuely press same finger for three times, if it succeeds, the info. will be shown like below:

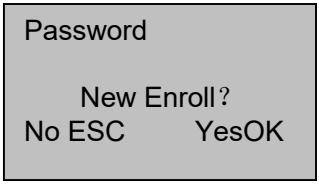


Note：07711-1
The last digit 1 represents the first fingerprint

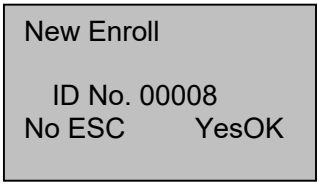
Press “OK” save the fingerprint enrolled just now and fulfill one enroll flow. If it fails, the system will prompt to try again, and back to step (3) to continue to enroll.

3.1.2 Password Enroll

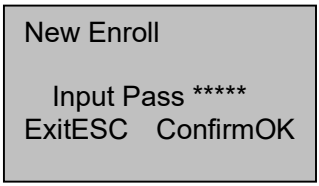
（1）Select Password enroll, press “OK” to confirm and go for next step operation and the info. will be shown as below:



（2）Press “OK” to confirm and go for next step operation and the info. will be shown as below:

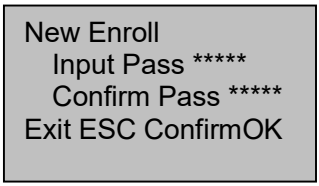


（3）To input the ID No. you need to enroll in the “ID No.” column (It’s between 1-85534) press “OK” to enter next step operation and info. shown as below:

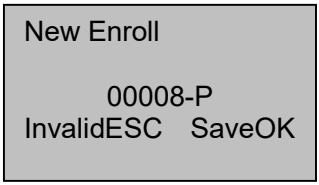


Note: The length of password is 1-4 digits.

（4）To input your password in the “Input Pass” column, press “OK” to enter next step operation and info. shown as below:



（5）To input your password one more time in the “Confirm Pass” column, press “OK” to enter next step operation and info. shown as below:

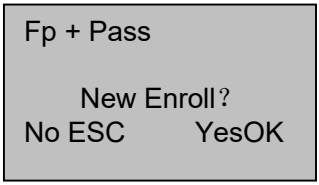


Note：00008-P
The last alphabet P represents Password

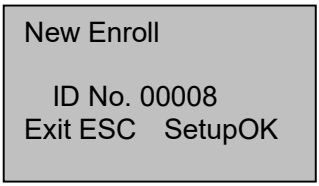
Press “OK” save the registered data just now and thus fulfill one password enroll flow.

3.1.3 Fp + Pass

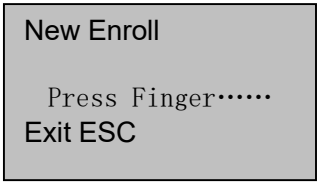
（1）Select “Fp + Pass”,



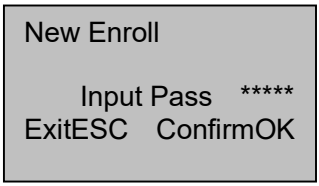
（2）Press “OK” to enter next step operation and info. shown as below:



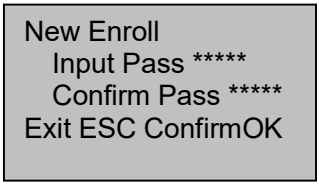
（3）To input the ID No. you need to enroll in the “ID No.” column (It’s between 1-85534) press “OK” to enter next step operation and info. shown as below:



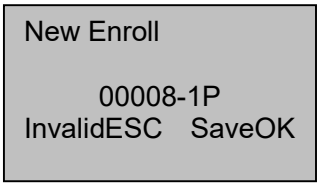
（4）According to prompt to continuely press same finger for three times, if it succeeds, the info. will be shown like below:



（5）To input your password in the “Input Pass” column, press “OK” to enter next step operation and info. shown as below:



（6）To input your password one more time in the “Confirm Pass” column, press “OK” to enter next step operation and info. shown as below:



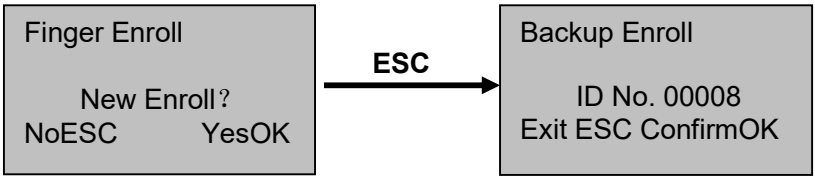
Note：00008-1P

Count backwards to number two is digit “1”, it represents one fingerprint. The last digit P represents Password.

Press “OK” save the registered data just now and thus fulfill one enroll flow of Fp + Pass..

3.2 Backup Enroll

At interface of New Enroll, press”ESC” to cancel new enroll and it will enter into Backup Enroll interface, which is shown as below:



The below setps are same with the one of New Enroll except that “New Enroll” changes as “Backup Enroll” at upper left corner.

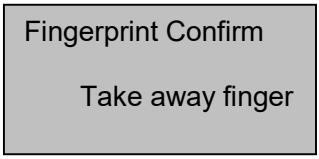
NOTE：For a long term user, it’s wise enough to enroll at least two fingers.

3.3 Identity Identification

During the period of on/off duty, the employee need to make Time & Attendance on the device to create T&A record. There are three defaulted identification modes within the system: Fingerprint Identificaiton, Pass Identificaiton, ID + Fp. Here below are illustrations of above three modes.

3.3.1 Fingerprint Identification

To press fingerprint on initial interface and it will shown like below:



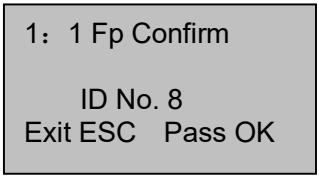
After it's shown around 0.5 seconds, if it succeeds, it will have voice prompt "Thank you" and the screen info. shown as below:

If it fails, it will have voice prompt "Try again" and the screen info. shown as below:

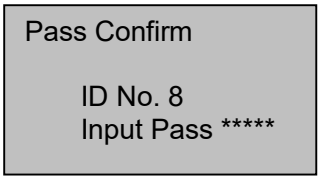
This interface lasts around 0.5 seconds and it will back to initial interface.

3.3.2 Password Identification

To input your ID on initial interface and the screen info. shown as below:

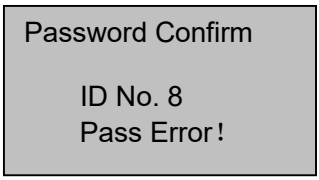


Press “OK” to confirm and the screen info. shown as below:



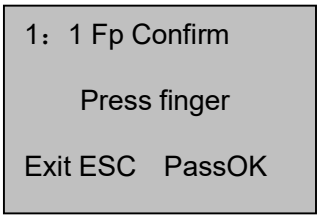
Input correct password and press “OK” to confirm and the screen info. shown as below:

If the password is incorrect, it will have error prompt and the screen info. shown as below:

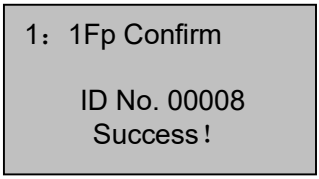


3.3.3 Card + Fp

To swipe card on initial interface and the screen info. shown as below:



To press fingerprint on this interface. Once the fingerprint identification is passed, the screen info. shown as below



3.5 Prompt of successful enrollment

Once the fingerprint enrolled is with good quality and the user's identity identificaiton speed will be very fast, and vice versa. Once the fingerprint enrolled is with bad quality, it will result in "Refuse to judge" or slower identification speed.

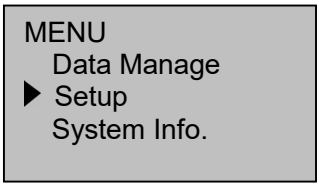
In order to enhance fingerprint enrollment quality, we would like to propose as below:

Tab.2---1 Frequent reasons for error enrollment or poor quallity enrollment

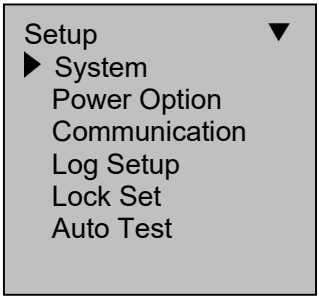
Dry or dirty finger	For dry skin, the better way is to chafe finger with palm because chafing will produce lipid Once the finger is too dry, kindly breathe out to wet finger
Finger pressing is not enough	The user need to flatly press his/her finger on U fingerprint collector
How to choose a finger	Recommend to enroll left/right forefinger or left/right middle finger Better to choose the finger with good quality, no harm or hurt. It's common for the user to chooe forefinger first, but once the forefinger quality is not good, kindly turn to middle finger or ring finer. Once the user's finger is too small then turn to thumb. Once the user prefers to enroll more fingerprint as backup, then turn to the finger which is hard to be harmed or hurted, such as ring finer.
Position of finer-pressing	Guarantee to flatly put finger on the U fingerprint collector and try to occupy the most proportion, not to spot finger vertically, not to knock the finger on quickly and not to glide the finger.
Effect of fingerprint image change	Due to special reason there will be fingerprint image change like desquamation, harm, ect, and it will affect T&A result. Once the user's finger quality is really not good, here it mainly refers to fingerprint desquamation, and it's very possible that one week later the identification is hardly to be passed and need to re-enroll or turn to choose password T&A method.
Other reason	For how great effort the user does, there might exist s very small qty. of people have poor quality fingerprint and can't pass normal identification. Thus it need to consider ID + Fp authentication to decrease 1:1 safe grade or better turn to password T&A method.

4 Setup

On initial interface press “MENU”, after confirm your manage purview, there will be info. shown as below:



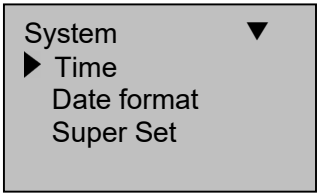
Select”Setup”, press “OK” to go for next step operation and the screen info. shown as below:



Under “Setup” there will five sub-menu as System, Power Option, Communication, Log Setup, Lock Set and Auto Test. Here below is detail explanation of them.

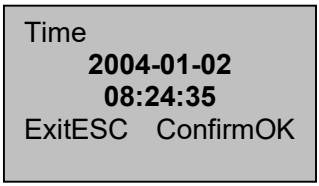
4.1 System

Enter into “System” menu and the screen info. shown as below:



4.1.1 Time

Select “Time”, press “OK” to confirm and the screen info. shown as below:



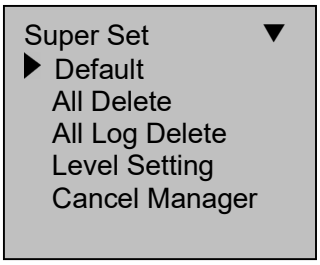
Once the date or time need to be modified, press “▲” or “▼” put cursor on the position need to be modified, then input correct date & time and press “OK” to save.

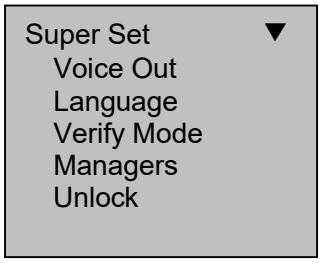
4.1.2 Date Format

Select Year/month/date, or month/date/year or date/month/year or moth/date/year.

4.1.3 Super Set

Select “Super Set”, press “OK” to confirm and the screen info. shown as below:





Press "▲" or "▼" to scroll the screen to select the required item.

4.1.3.1 Default：To make all settings as defaulted EX-Factory status.；

4.1.3.2All Delete：To delete all enrolled fingerprints & records.

4.1.3.3All Log Delete：To delete all records saved in memory chip.

4.1.3.4Level Setting: The higher the level is, the more accurate it will be but with less pass rate.

4.1.3.5Cancel Manager：To cancel all purview of managers and make them as normal user.

4.1.3.6Voice Out：To start voice hint or not.

4.1.3.7Language：To select the language desired.

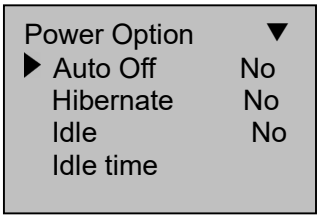
4.1.3.8Verify Mode：To select modes like Fingerprint only, Password only, Card only or any of above two combination.

4.1.3.9Managers：To set up the quantity of managers.

4.1.3.10Unlock：To manage whether to use lock function or not.

4.2 Power Option

Enter into “Poer Option” menu and the screen info. shown as below:



This Z6 product adopts intelligent power option system and supports Auto Off and Hibernate by timing and the like function all which will entend device life at most and meet different requirement of the users.

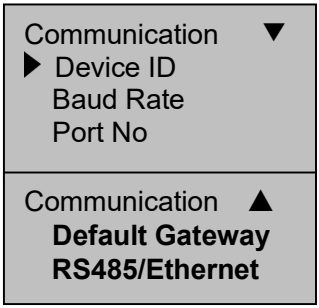
Auto OFF： To automatically power off device in the designated time period.

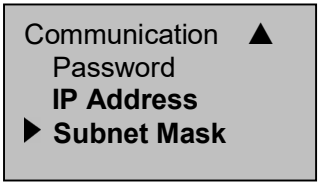
Hibernate： To automatically enter into hibernation status at the designated time and press any key to wake up the device to work again.

Idle & Idle Time: These two function is mutually associated. When Idle Time is 0 and Idle function is closed. When Idle Time is not 0 (the time unit is by minute), for example 1, therefore after 1 minute period and there is no operation, the system will go for Idle status.

4.3 Communication

Enter into “Communication” menu and the screen info. shown as below:





The device has RS232 / RS485 communication interface， TCP/IP is optional， and whether it's standalone or for network usage, it's easy to convenient.

Ethernet function is only available when it has TCP/IP accessory. Z6I and Z6II can simultaneously have function of RS232, RS485 and TCP/IP. However, if it's for Z6II, the user can only choose either Ethernet or RF232/485, it means when Ethernet function is used, there will be no RS232/485 function, same, when RS232/485 function is used, there will be no Ethernet function.

Baud Rate：There will be three options: 9600,38400 and 115200. It's recommend to choose High speed communication for RS232 and lower speed communication for RS485.

Device ID：Code from 1---255；

IP Address：Defaulted IP is 192.168.1.201, and it can be modified based on need.

Ethernet: To adopt TCP/IP to communicate or not.

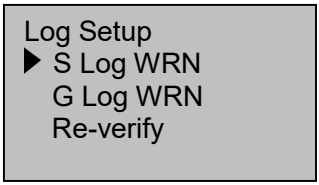
RS232：To adopt RS232 to communicate or not.

RS485：To adopt RS485 to communicate or not.

Connection Pass：A password is required to connect device. It's to avoid illegal connection to ensure device's data.

4.4 Log Setup

Enter into “Log Setup” menu and the screen info. shown as below:



S Log WRN： **When the rest data capacity up to its set value, the device will send out S Log Full warning message.**

G Log WRN: **When the rest in/out log data capacity up to its set value, the device will send out S Log Full warning message.**

Re-verify: **Within set time scope (unit: minute), once there exists someone’s T&A data, thus for the second time, his/her T&A pass result won’t be saved in the system.**

4.5 Access Control

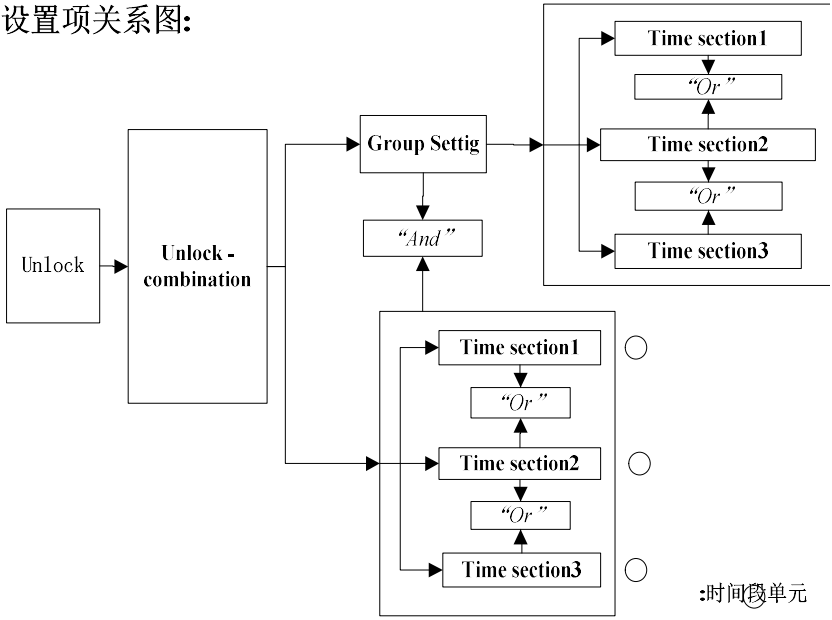
Access Control set up is the settings for unlock time and purview to the users already enrolled. For each user setting, which is composed of three time period setting & one group setting. The relationship between two time periods is “Or”. For group it also has three time periods settings, same, relationship among three time periods is also “Or”. However, for those within the group and user’s time period, their relationship is “and”.

Simply say, if it needs to make the user who enrolled under unlock status, the first step, the group user belongs to must already in a unlock combination (it can also share a combinaiton with other group but it needs to unlock together) second step, current unlock time should be within any of the time period option of user’s access control setting and it is also within any time period of the group user belonged to.

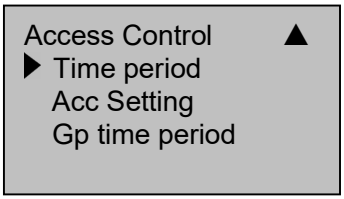
It is defaulted that the user newly enrolled will be the first group and defaulted group combination is alos the first one. Therefore the newly

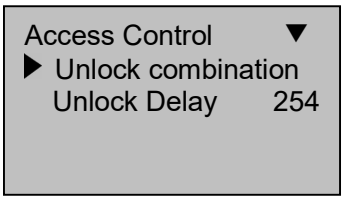
enrolled user is defaulted as unlock status. Once there doesn't exist the user's group in the group combination setting, it means the user is only for attendence and can't unlock door.

设置项关系图:



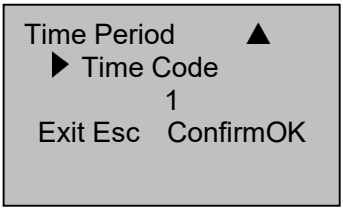
Enter into Access Control menu and the screen info. shown as below:



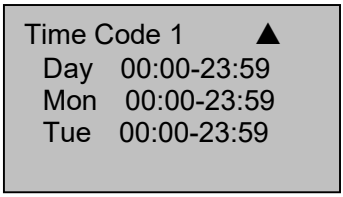


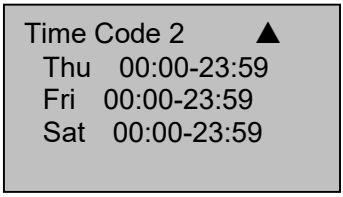
4.5.1 Function definition of Time Period

Time period is the smallest definition period of Access Control setting. For the whole system it can define 50 time periods at most. For each time period it defines the valid time zone within 24 hours a day in a week time, namely 7 time zones in total. The most, each user can setup three time periods, and the relationship among three time periods is “Or”, which means it could be valid whenever the condition can be met any one of three. For each time zone of time period, its format is like HH:MM-HH:MM, namely it could be detailed as the unit of minute in 24 hours. And the end time is earlier than start time （23:57-23:56）it means Forbid all full day, whereas the end time is later than start time （00:00-23:59）it means valid all full day.
Enter into “Time Period” and the screen info. shown as below:



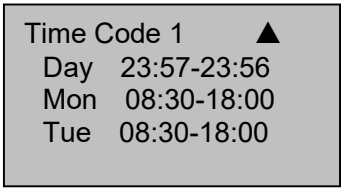
Press “OK” to enter into setting of time code 1 and the screen info. shown as below:

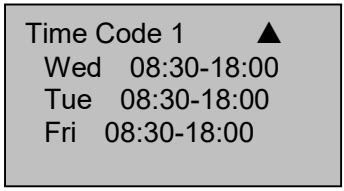




For example：
Definition of time code 1：
It’s not allowed to enter during Saturday and Sunday.
It’s only allow to enter during work time of working days. (Monday to Friday) and the work time is 08:30-18:00

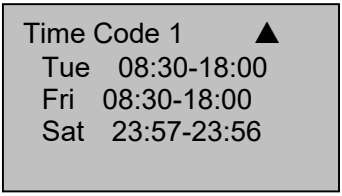
Set up as below”





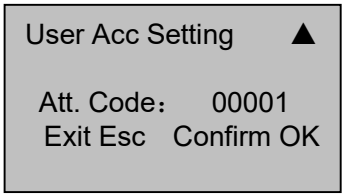
And follow this example to define more time periods and the most it’s allowed to define 50 time periods within the system.

4.5.2 User’s Access Control Setting

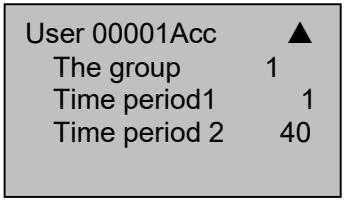


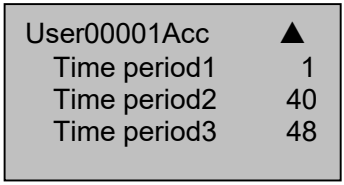
By this menu to check some user’s access control status, which includes his/her group setting and time period setting, the group means which group the user belongs to. And below time period setting can choose from the time codes already set. And the relationship among time periods is “Or” and the relationship between the group and time period is “And”.

Example: Enter into interface of code 00001 and the screen info. shown as below.



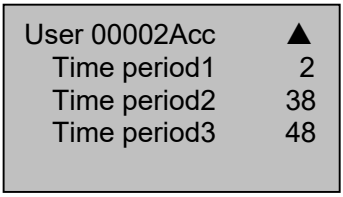
Press “Confirm “ to enter





And the setting for user 00001：
The user belongs to first group and has right to enter within time period of 1,40 and 48.

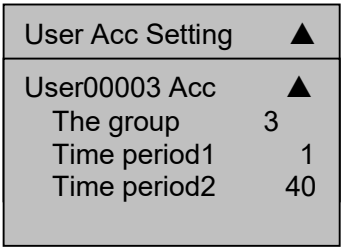
Enter into interface of code 00002 and the screen info. shown as below.
Press “Confirm “ to enter



And the setting for user 00002:

The user belongs to second group and has right to enter within time periods of 2, 38 and 48.

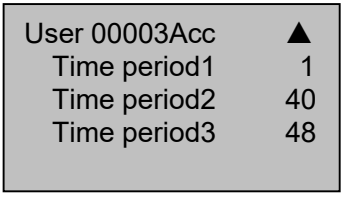
Enter into interface of code 00003 and the screen info. shown as below.



Press “Confirm” to enter.

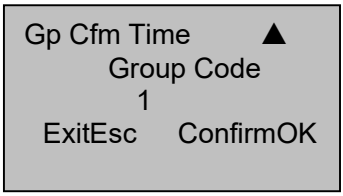
And the setting for user 00003:
The user belongs to group 3 and has right to enter during time period of 1, 40 and 48.

4.5.3 Group Confirm Time Period

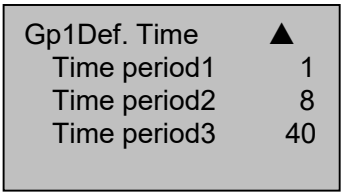


Group definition is to make different groups can be combined as different group combination. It defines 5 groups: 1st group, 2nd group, 3rd group, 4th group and 5th group. The user is defaulted as the 1st group but it’s possilbe to re-designate to other group. It can also defines the defaulted time period of each group. Whenever a user doesn’t be defined concrete time period then it will adopt defaulted one. Once there isn’t any defaulted time period to be defined within such group, then the user can carry out identification & unlock without any time limit.

Enter " Gp Cfm Time" and the screen info. shown as below:



Press "Confirm" to enter:



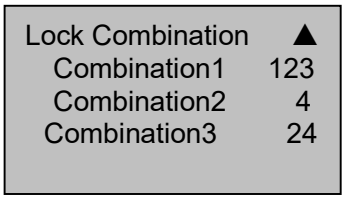
To setup the above code 00001,00002,00003 as 1st group, 2nd group and 3rd group.

4.5.4 Lock combination defintion

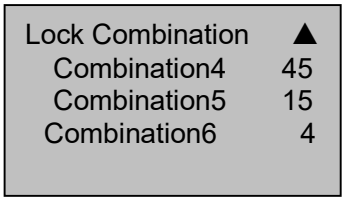
Lock combination is the direct lock control operation. For example, if you wish to make all enrolled users can not unlock, just set all these 10 lock combination as all blank. The defaulted lock combination within the system is "1" (namely the newly enrolled user is defaulted as the one who can unlock)

Lock combination defines it can simultaneously identify the unlocking user's group combination. Lock combination directly defines with group code, and it doesn't consider the sequency of user's identificaton among all groups. For example "123" means the user of 1st group, 2nd group and 3rd group can together to identify and unlock. "4" means it can be unlocked whenever the separate user's identification of 4th group passed. The most the system is allowed to define 10 group combination, any of which is passed will be ok.

Enger into “Lock Combination” and the screen info. shown as below:



By above combination setting we can draw conclusion as below:
1,2,3 is an combination;
4 is an combination
2,4 is an combination
4,5 is an combination
1,5 is an combination



1 When the people of 1st group, 2nd group and 3rd group all present and pass the fingerprint identificaiton and their time period settings is also valid, the door is unlocked;

2 When there is only one person 4th group presents and pass the fingerprint identificaiton and his/her time period settings is also valid, the door is unlocked;

3 When the people of 2nd group and 4th group all present and pass the fingerprint identificaiton and their time period settings is also valid, the door is unlocked;

4 When the people of 1st group and 5th group all present and pass the fingerprint identificaiton and their time period settings is also valid, the door is unlocked;

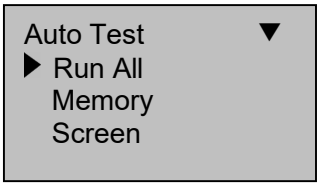
For example: For a bank's bursary, it needs three persons presentation to unlock the door of bursary. The concrete setting is as below:
For the above three persons belong to 2nd,4th and 5th group respectively and have right to unlock in the same time period. Select "Combination 1" to press OK to edit, input 2,4,5 and press ESC to save and exit. Remark: When the combination of 2nd,4th and 5th is set, it can not set combination like "2nd and 4th group", "2nd and 5th group" and "4th and 5th group".

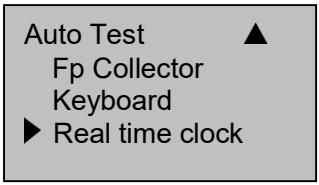
4.5.5 Entrance Delay

It needs to be set up the unlock time of electronic lock which is controlled by T&A device. "0" for turn off its control function. And a scalar unit is 20ms, the most could be set as 254, namely 5.08 seconds. Select this item and press "OK" to enter its setting, input digits on keyboard to input number and press "ESC" to save and exit.

4.6 Auto Test

Enter into "Auto Test" and the screen info. shown as below:



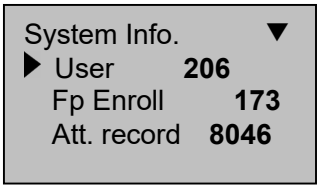


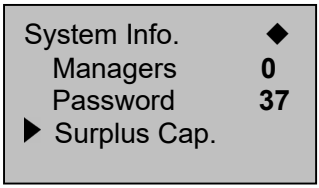
Under this menu option, the user can run all Auto Test on system components. It facilitates the maintenance of the device and also convenient to analyze damaged reason when the device is defective.

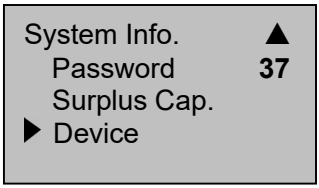
Here it allows to test memory, liquid screen, voice, fingerprint collector, keyboard and clcok. During test, it should be guaranteed the stability of the power supply or else it may do harm on system hardware especially during memory testing.

5 System Info.

Select " System Info." from menu, press "OK" to go for next step operation and screen info. shown as below:

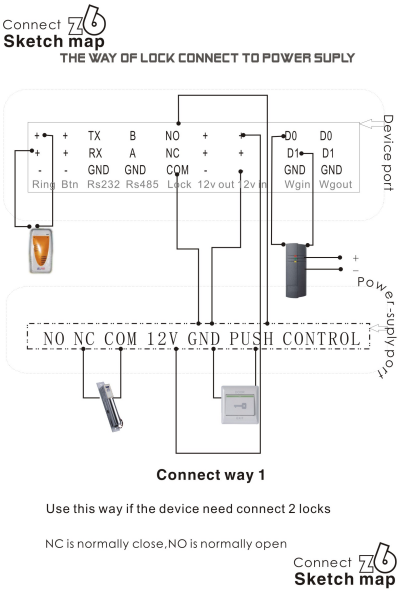






On above screen it has user quantity enrolled, fingerprint quantity, password quantity, manager quantity and Attendance records. For Suplus Cap. it shows how many memory space left. And for Device info. it shows device's capacity, date of EX-factory, serial number and manufacturer info, etc.

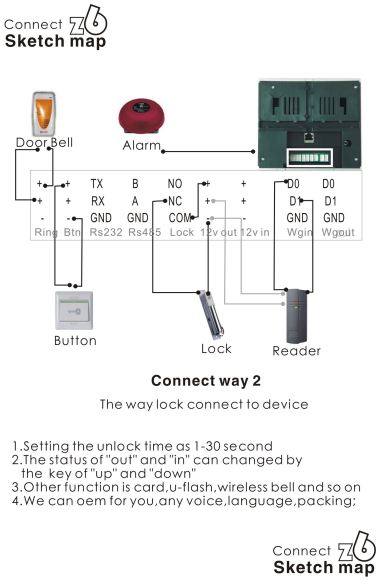
6. Access Control hardware connection Sketch



Connect way 1

Use this way if the device need connect 2 locks

NC is normally close,NO is normally open



Connect way 2

The way lock connect to device

1.Setting the unlock time as 1-30 second
2.The status of "out" and "in" can changed by the key of "up" and "down"
3.Other function is card,u-flash,wireless bell and so on
4.We can oem for you,any voice,language,packing;

This connection sketch map is only access control door connection, for T&A device please just skip it.

7 Maintenance

1 Clean

Sometimes optic lens, keyboard or screen need to cleaned. Due to different outside working environment, it's hard to give an exact cleaning schedule. The below table is an guide which may do some help:

Item	Clean
Keyboard & screen	Whenever it's too dirty and blurry on the surface, it needs cleaning. Details refer to below.
Optic Lens	Don't' clean too frequently. Lens works better with a little lipid.
	Once the lens is shaded or somewhat affects identification of fingerprint, it needs cleaning. Details refer to below.

Tab.5-1 Maintenance Legend

2 Clean keyboard & Liquid Screen

Make sure to turn off the device when it needs to do cleaning on keyboard & liquid screen. Use wet duster cloth or other mild detergent and then dry it.

3 Clean Optic Lens

Follow below suggestion when cleaning Optic Lens:

1) Once it fulls with dust or grit, please blow dust off first;
2) Use adhesive tape to clean display window.
   Warning: Don't use water or other detergent to clean which may do harm on optic lens.
3) To wipe with fine cloth without any floccule and be careful not to hurt lens. Once it has floccule on the lens, to blow it off after the lens becomes dry.