AC-5000 User Guide

Version eng-1.00

CORPORATION

<Revison History>

Version	Date	Description	Firmware Version
1.00	2011-01-10	Initial Release	10.51.00-000.00

<Glossary>

- Admin (Administrator)
  - As a user who can enter the terminal menu mode, he/she is authorized to register/modify/delete terminal users and change the operating environment by changing the settings.
  - If there is no administrator registered for a terminal, anyone can enter the terminal menu and change the settings. Therefore, it is recommended to register at least one administrator.
  - Special care is required for registration and operation as an administrator has the right to change important environment settings of the fingerprint recognizing unit.

- 1:1 Authentication (1 to 1, Verification)
  - This is a method that authenticates fingerprint with user ID or card entered
  - This method is called 1:1 authentication as only the fingerprint registered in the user ID or card is used for comparison.

- 1:N Authentication (1 to N, Identification)
  - This is a method that searches a corresponding user only with fingerprint.
  - This method is called 1:N authentication as it searches the identical fingerprint from the registered fingerprints without user ID or card entered.

- Security Level
  - This is the level used for fingerprint authentication displayed from 1 to 9 depending on how both fingerprints match against each other. Authentication will be successful only when the identity between both fingerprints is higher than the preset level.
  - The higher the authentication level, the higher the security. Nevertheless, as it requires a relatively high match rate, self-authentication is prone to failure.
  - 1:1 Level: Authentication level used for 1:1 verification.
  - 1:N Level: Authentication level used for 1:N identification.

- Authentication Method
  - This represents the various types of authentication methods including FP (fingerprint) authentication, RF (card) authentication, a combination of these methods.
    Ex) Card or FP: Authentication with card or fingerprint

- Function Keys
  - [F1], [F2], [F3], [F4], and [ENT] keys are available. These keys allow a user to enter the menus or change modes such as office start/leave.

- LFD (Live Finger Detection)
  - This function allows the input of only real fingerprints and blocks the input of imitation fingerprints produced using rubber, paper, film, and silicone.

Table of Contents

<Revison History> **2**
<Glossary> **2**
Table of Contents ..... Error! Bookmark not defined.
1. Before use **5**
1.1. Safety precautions **5**
1.2. Terminal description **6**
1.3. Screen description (during operation) **6**
1.3.1. Icon shown during operation 7
1.3.2. Message shown during operation 7
1.4. LED signal shown during operation **10**
1.5. Keys used during operation **10**
1.6. Voices used during operation **11**
1.7. Buzzer sounds used during operation **11**
1.8. How to register and input fingerprint **11**
2. Product introduction **12**
2.1. Features **12**
2.2. Configuration **15**
2.2.1. Standalone (Access) 15
2.2.2. Connect with PC SERVER (Access, Time & Attendance, Cafeteria) 15
2.3. Specification **16**
3. Environment settings **17**
3.1. Items to be checked before environment settings **17**
3.1.1. Entering menu 17
3.1.2. How to access the menu without administrator verification 17
3.1.3. Change settings 18
3.1.4. Save environment settings 19
3.2. Menu Configuration **21**
3.3. User **23**
3.3.1. Add 23
3.3.2. Delete 27
3.3.3. Modify 28
3.3.4. Delete All 29
3.4. Network **29**
3.4.1. IP 29
3.4.2. Server IP 30
3.4.3. Terminal ID 30
3.5. Application **31**
3.5.1. Application 31
3.5.2. Time Schedule 31
3.5.3. Function Key 33
3.5.4. Extended Key 33
3.5.5. Display 34
3.6. System **35**
3.6.1. System Setting 35
3.6.2. Authentication 35
3.6.3. Fingerprint 37
3.6.4. Language 37
3.6.5. Data Time 38

3.6.6. Database 38
3.7. Terminal 40
3.7.1. Terminal Option 41
3.7.2. Volume Control 41
3.7.3. Door 42
3.7.4. Wiegand 43
3.7.5. Card Reader 44
3.7.6. External Device 45
3.8. Information 45
3.8.1. System Info 46
3.8.2. Network Info 46
3.8.3. Database Info 46
3.8.4. View Log 47
3.8.5. Version Info 47
3.9. Downloading user's file 47
3.9.1. Change background image 47
3.9.2. Change voice message 48
3.9.3. Change user text 48
4. How to use the terminal 50
4.1. Change authentication mode 50
4.2. ID input 50
4.3. Authentication 51
4.3.1. Fingerprint authentication 51
4.3.2. Card authentication 51
4.3.3. Password authentication 51

1. Before use

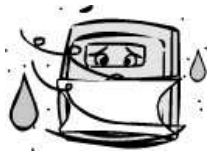
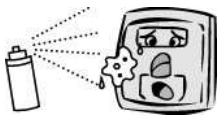
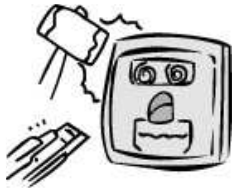
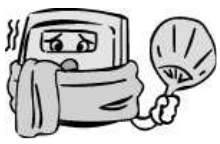
1.1. Safety precautions

- Warning

Do not handle the unit with wet hands and do not allow liquid to flow into it. -> It may cause an electric shock or damage. 	Do not place a fire source near the unit. -> It may cause a fire. 
Do not disassemble, repair, or modify the unit. -> It may cause an electric shock, fire or damage. 	Keep out of children's reach. -> It may cause an accident or damage. 

- If the above warnings are ignored, it may result in death or serious injury.

- Cautions

Keep away from direct sunlight -> It may cause mal-function, deformation or color change of the unit. 	Avoid high humidity or dust ->It may cause the unit to malfunction. 
Avoid using water, benzene, thinner, or alcohol for cleaning the unit. -> It may cause an electric shock or fire. 	Do not place a magnet near the unit. -> The unit may break down or malfunction. 
Avoid getting the fingerprint input area dirty. ->It may prevent the unit from recognizing the fingerprint. 	Avoid using insecticides or flammable sprays near the unit. -> It may result in the deformation or color change of the unit. 
Avoid impact or using sharp objects on the unit. -> The unit may be damaged and broken. 	Avoid installing the unit in a place where temperature severely changes. ->It may cause the unit to malfunction. 

- If the above cautions are ignored, it may result in property loss or human injury.

※ Under no circumstances will Union Community be responsible for the accidents or damages caused by inappropriate use of the product and neglect of the precautions stated in the user guide.

1.2. Terminal description

State Display LED

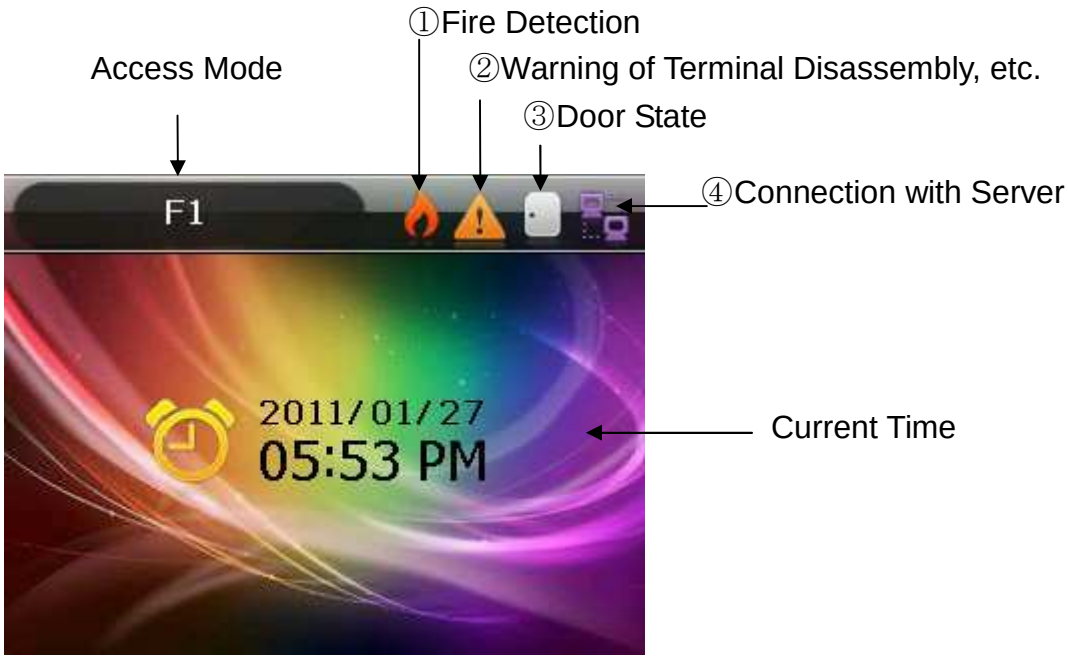
LCD

Fingerprint Sensor

Touch Key
Normally, the figure is invisible as LED is off, but LED is on and the figure is shown when the user touches this area lightly.

Card Input Area

1.3. Screen description (during operation)



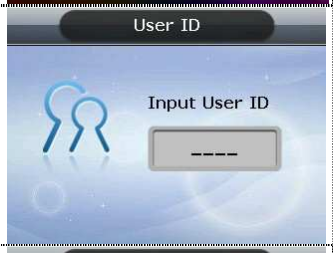
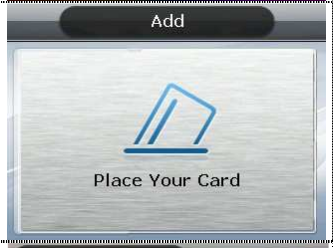
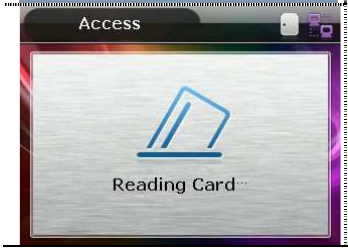
1.3.1. Icon shown during operation

① Fire Detection	None : Normal  : State that fire is detected by fire sensor (subject to the connection with fire sensor)
② Warning	None : Normal  : Abnormal state that terminal is disassembled or door has encountered a problem
③ Door status	 : Door status is unknown  : Door is closed  : Door is opened
④ Connection of Server	None : LAN cable is not connected  : LAN cable is connected, but not yet to the server  : Connected with the server program

1.3.2. Message shown during operation

	- Initial screen of AC5000
	- When authentication is successful
	- When authentication is failed
	- When any unregistered user ID is input - When fingerprint authentication is attempted in the event where the server is not connected and there is no registered fingerprint in the terminal

	- When any unregistered card is input
	- When fingerprint input is failed - When the user took the finger off too fast before the fingerprint is input
	- When Anti-pass back is in error (in the event the user uses the anti-pass back function)
	- When the user attempted two or more times at the same meal time zone (in the event it is used for cafeteria)
	- When there is no response from the server during the attempt of authentication to the server - When network is disconnected during the attempt of authentication to the server
	- When the user is not authorized for authentication even if he/she is being registered or the user attempted authentication when access is not allowed
	- When the terminal is set to Locked

	- When it is not the meal time (in the event it is set to Cafeteria)
	- When the authentication may not be treated as there are too many authentication requests from the terminal during the server authentication.
	- During the status that is waiting for the user ID input
	- During the status that is waiting for the password input of the user
	- During the status that is waiting for the fingerprint input of the user
	- During the status that is waiting for the card input of the user
	- At the time of fingerprint card authentication, it shows the status that the card reads fingerprint data. The user must put the card for 1~2 seconds until the message disappears.

	- When waiting for the response after the user attempted authentication to the server
	- When upgrading the terminal program (Be sure not to power off the terminal during the time the message is output)

1.4. LED signal shown during operation

●	Power	Red	On: Normal Flickering: When the lid is opened or there is any communication error in the connection with LC010
●	Door	Green	On : Door Open Off: Door Close

1.5. Keys used during operation

[0]~[9]	- Keys used for numeric input
[F1]~[F3]	- Keys used for changing the authentication mode
[F4] or [←]	- Used for changing the authentication mode - Used as Delete key for correction when inputting the figure - Used for canceling input and moving to the parent menu in the menu mode
[F4(←)~]	- Means pressing [F4(←)] key for 2 seconds or longer - When input focus is located in the input box, it can cancel the input and exit to the parent menu by pressing this button for 2 seconds or longer
ENT [or MENU]	- Used for modifying the mode - Used for saving the value set in the menu mode or moving to the configuration in the screen
[ENT~]	- Means pressing [ENT] key for 2 seconds or longer - Used for accessing the menu when pressed on the basic screen - When input focus is located in the input box, the user can exit to the parent menu with the current input value saved by pressing it for 2

	seconds or longer - Used to apply the configuration to the current screen in the menu mode and then exit to the parent menu.

1.6. Voices used during operation

Type of operation	Voice
For fingerprint input	Please enter your fingerprint.
When authentication is successful	You are authorized.
When authentication is failed	Please try again.

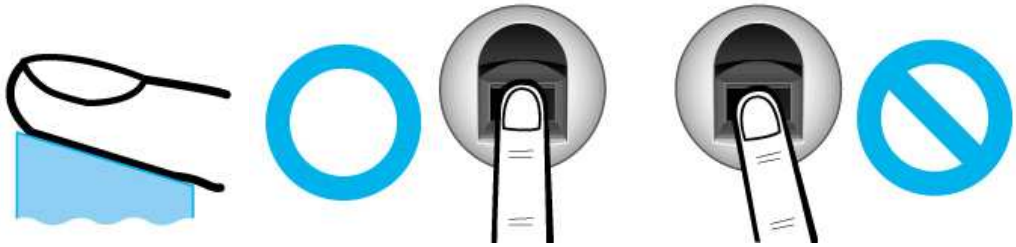
1.7. Buzzer sounds used during operation

Beep	Sound that is generated when a key is pressed or a card is being manipulated	When the key is pressed or card is read; When fingerprint input is completed and the user may take finger off
Be peep	Sound of failure	When authentication is failed or when the user's fingerprint is wrongly input
Brrrrrrp	When standing by for input	When notifying the status of waiting for the user's input of fingerprint or password
Beeeep	Success	When succeeding in authentication or completing the setting work

1.8. How to register and input fingerprint

- How to input fingerprint

  Please input your fingerprint as if you are sealing a document using your forefinger.
  Avoid inputting fingerprint with the fingertip touched lightly in the event of input/registration.
  Be sure that the center of fingerprint correctly touches the fingerprint input area.



- Input the fingerprint of your forefinger if possible.

It will facilitate the accurate and stable input of fingerprint.

- Please check if the fingerprint is not clear or has any scar.
  Too dry or wet fingerprint, ambiguous fingerprint, fingerprint with scar, etc. may not be recognized. In this case, use/register the fingerprint of another finger.

- Precautions related with the user's fingerprint status

  Depending on the fingerprint status, the user may not use fingerprint or suffer inconvenience from its use.

  - This product is the fingerprint recognizing system. Any fingerprint that is damaged or thin may not be used. In such case, the user is required to operate with password.
  - When the finger is in a dry condition, the user is advised to breathe lightly on the finger for a smooth operation.
  - In case of a child, due to small size or tender property of fingerprint, it may be difficult or impossible to use it. Therefore, it is necessary to register the fingerprint every 6 months interval.
  - In case of old people, excessive tiny lines that exist on the fingerprint to be registered may prevent proper registration.
  - It is recommended to register at least 2 fingerprints of the user if possible.

2. Product introduction

2.1. Features

- **Application of POE and Terminal Block – Easy to install**
  - As it supports POE, it can be installed with LAN cable without a separate power cable.
- **Designed in IP65 rainproof specification** – Outdoor installation is possible.
- **Slim and polished design**

- **Easy to install as it is designed in a standing type; Slim and elegant design using** Color LCD and Touch Key

- **Download function of Server – Enables to change background image and voice**
  - Provides a variety of info messages through color LCD and voice; User can download background image and voice from the server according to his/her preference. Especially, the built-in LCD Backlight and Touch key LED enable identifying the screen and manipulating the keys in a dark place.

- **Convenient Auto Sensing Function**
  - Enables to easily perform the operation of authentication by inputting the fingerprint without entering the key separately

- **Easy self-authentication through fingerprint**
  - Prevents the risk of forgetting the password, loss/theft of card or key by adopting fingerprint recognition technology that is biometrics; reinforces the security of self-authentication through the use of own fingerprint

- **Access Management System using the network (LAN)**
  - Communication is carried out between fingerprint recognition device and authentication server using TCP/IP protocol; Allows for easy expansion as it can be applied to the network as it is. 10/100 Mbps Auto Detect ensures high-speed operation; Enables easy management and monitoring through the network

- **Provides a diverse and flexible access management**
  - Provides a perfect control function by granting the right to entrance/access by user group

- **Applicable for various operation methods such as access, time & attendance, cafeteria, etc.**
  - Enables a variety of operation methods depending on the settings of operating method in the terminal menu

- **Abundant capacity for treatment of the server**
  - In the event of managing the persons who enter using the server, it allows to treat almost an unlimited number of persons.

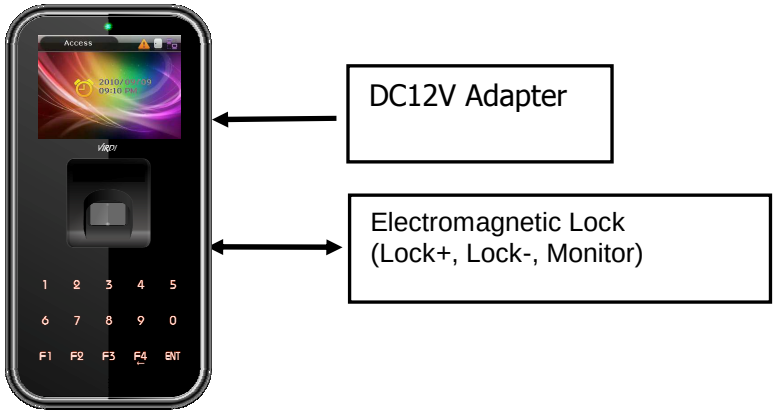
- **Provides a variety of registration and authentication methods**
  There are 12 registration and authentication methods for a general user. Therefore, it is necessary to determine such registration and authentication method before registering a user or administrator.

FP	Fingerprint registration Fingerprint Authentication
PW	Card registration Card authentication
FP or PW	Fingerprint and password registration Password authentication when fingerprint authentication is failed
FP & PW	Fingerprint and password registration Fingerprint authentication and then password authentication
Card	Card registration Card authentication
Card or FP	Card and fingerprint registration

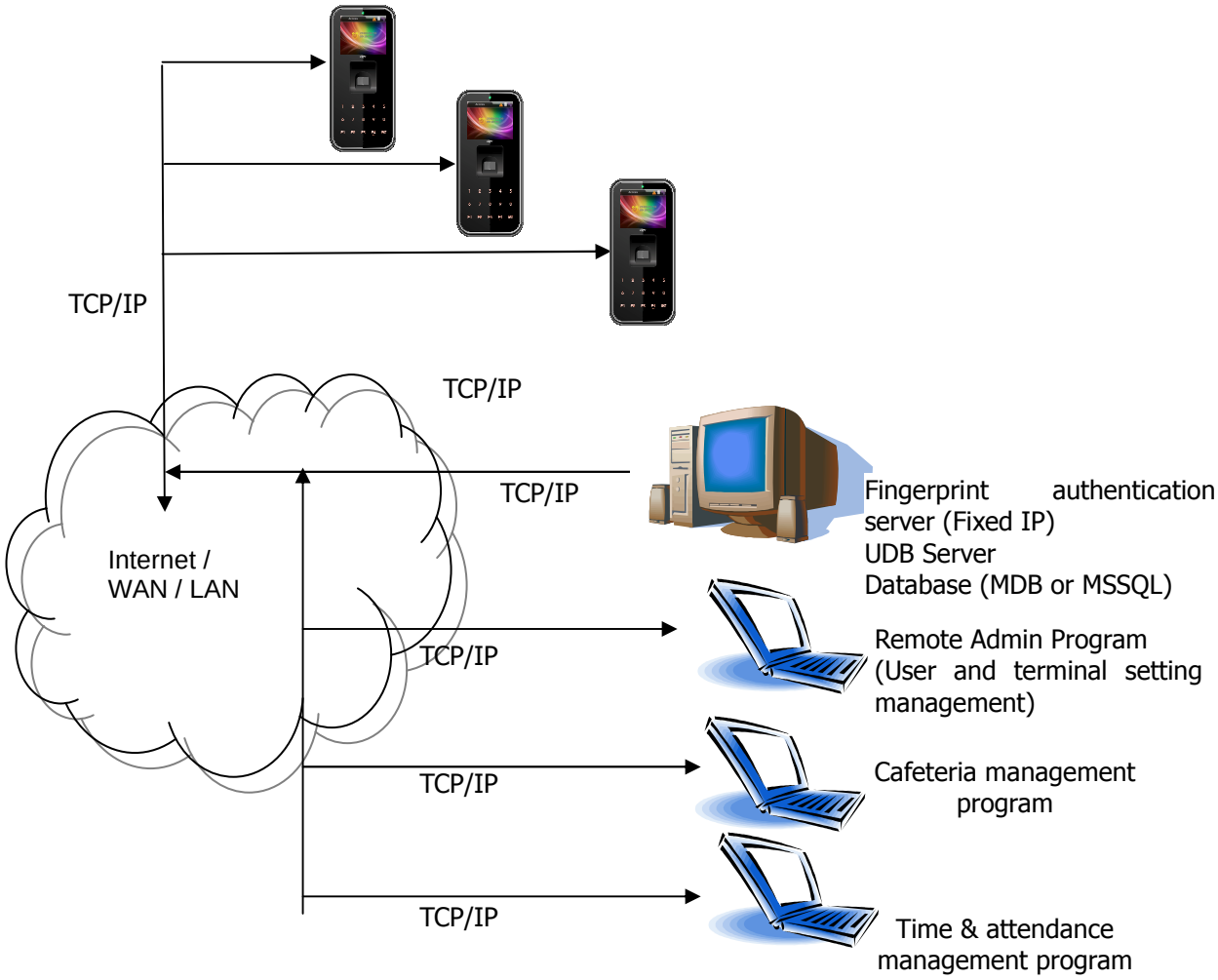
	Card or fingerprint authentication
Card & FP	Card and fingerprint registration Card authentication and then fingerprint authentication
Card or PW	Card and password registration Card or password authentication
Card and PW	Card and password registration Card authentication and then password authentication
(ID or Card) & FP	Card and fingerprint registration ID input and then fingerprint authentication, or card authentication and then fingerprint authentication
(ID or Card) & PW	Card and password registration ID input and then password authentication, or card authentication and then password authentication
Card & PW & FP	Card, password, and fingerprint registration Card authentication and then fingerprint & password authentication

2.2. Configuration

2.2.1. Standalone (Access)



2.2.2. Connect with PC SERVER (Access, Time & Attendance, Cafeteria)



2.3. Specification

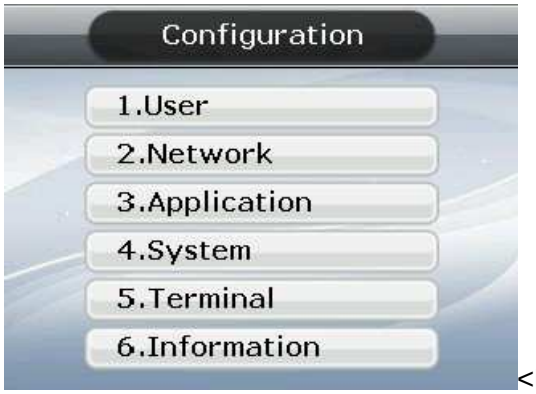
Division	SPEC	REMARK
CPU	32Bit RISC CPU (400MHz)	
Rainproof	**IP65**	
LCD	**2.8” TFT Color (320*240)**	
Touch Key	15key (0~9, F1~F4, Enter)	
MEMORY	32M SDRAM	
	32M FLASH	20,016 User 20,016 Finger 61,439 Log
Fingerprint sensor	Optical	
Authentication speed	Within 1 second	
Scan Area / Resolution	15 * 17mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Temperature / Humidity	-20 ~ 50 / Lower than 90% RH	
POE	**Supports 13W POE**	
AC / DC Adapter	INPUT : Universal AC 100 ~ 250V	
	OUTPUT : DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Lock Control	EM, Strike, Motor Lock, Auto Door	
I/O	3 In (1 Exit, 2 Monitor) 2 Out (Lock Control)	
Communication Port	TCP/IP (10/100Mbps)	Authentication server communication
	RS-232	Meal ticket printer
	RS-485	External device communication
	Wiegand In/Out	Card reader or External device communication
Card Reader	125KHz RF or 13.56MHz Smart (1 SAM Socket)	Option
SIZE	88.0mm * 175.0mm * 43.4mm	

3. Environment settings

3.1. Items to be checked before environment settings

3.1.1. Enter the Menu

Press [ENT] key for two seconds or longer, then the user can access the screen for menu selection as follow;



<Figure 3-1>

User can transfer to each sub menu and have access by pressing the relevant number key. If the admin is already registered, the Verify Admin screen appears as below;

<Figure 3-2>

In compliance with the registered authentication method such as card, fingerprint or password, user can access each menu subject to successful identification after the verification of admin is finished.

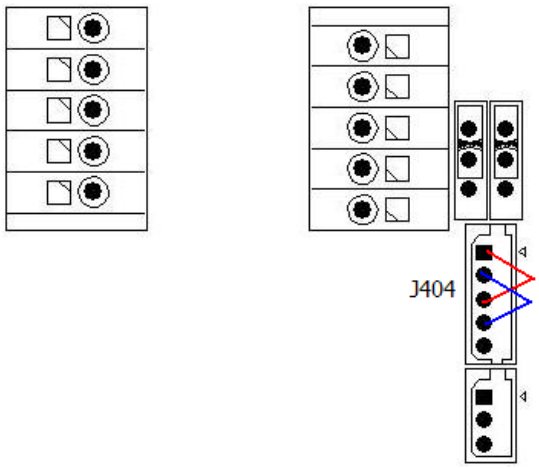
▶ Verify Admin appears only when there is a registered admin. When accessing the menu mode, once being identified, the user is allowed to access all the menus until the user completely exits from the main menu.

3.1.2. How to access the menu without the verification of admin

This is the way of accessing the menu used inevitably when fingerprint authentication is impossible because the user forgot the admin password or lost the card registered on the terminal, or there is no admin.

① Remove the bracket at the backside of the terminal to open the lid.

② With the lid open, as shown in the figure below, connect pin No. 1 with pin No. 3, and pin No. 2 with pin No. 4 of J404 connector respectively at backside.



<Figure 3-3>

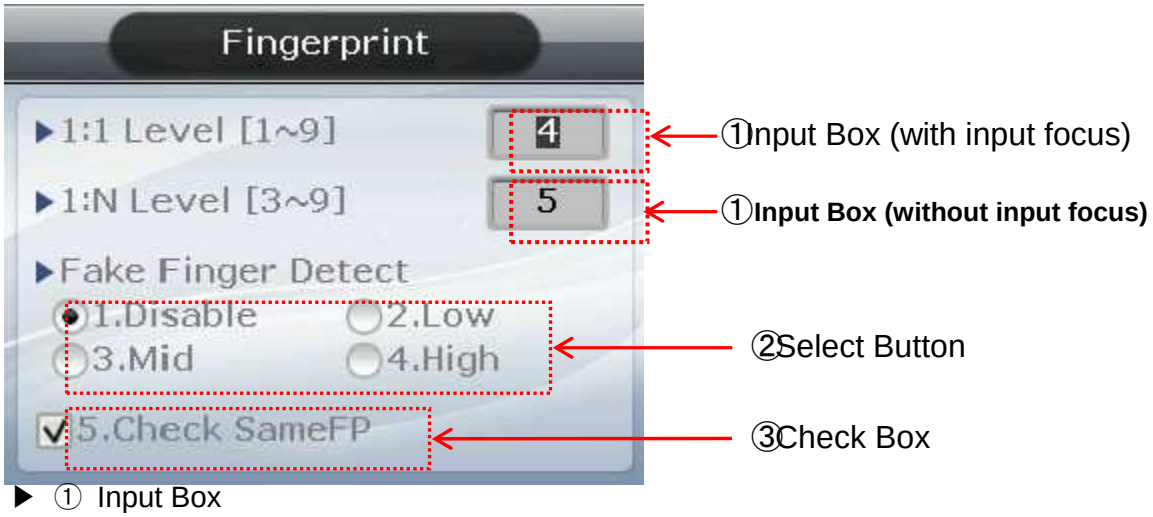
③ Access the menu by pressing [F4(←)]key for 2 seconds or longer, fill Admin ID with '0' on Verify Admin screen in <Figure 3-2>, and then press [ENT]key. The user can then access the menu selected with the buzzer sounding "Brrrrrrp" .

▶ After modifying the configuration, don't fail to get rid of the connected pin of J404 connector.

3.1.3. Modify setvalue

The following are the name and input method by input items.

<Figure 3-4>



▶ ① Input Box

In case of an item where the value is directly input like '1:1 Level', user must delete the existing value with [F4(←)] key when the focus is in the applicable item and then input the new value using [0]~[9] key.

▶ ② Select Button

In case of selecting an item out of the given sample like 'Fake Finger Detect', user must modify the item selection ( ) by pressing the relevant number key, provided that, user must select the item after moving the focus from the input box by pressing [ENT] key if the focus is located at the input box as shown in <Figure 3-5>.

<Figure 3-5> Move Focus (using [ENT] key)

Error!

As shown in the figure at the left, the letter is displayed in a reverse type when the focus is located at input box. As shown in the figure at the right, the applicable letters are displayed in black instead of grey when the focus moved to 'Fake Finger Detect'

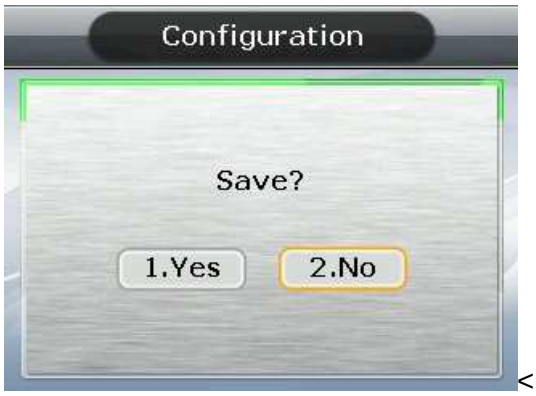
▶ ③ Check Box

In case the user must select whether or not checking like 'Check SameFP', the user can either select ( ) or release ( ) by pressing the relevant key [5]. If it is impossible to select the relevant item, it is displayed in ( )

Press [F4(←)] key to cancel in the course of setting and move to the parent menu. When the focus is located at the input box, [F4(←)] key functions as [DEL] key that deletes the figures one by one. In this case, press [F4(←)] key for two seconds or longer to cancel input and exit to the parent menu. Press [ENT] key for two seconds or longer to save the current configuration and move to the parent menu.

3.1.4. Save environment settings

Press [F4(←)] key in the main menu screen of <Figure 3-1> to save the settings changed, then the following screen will appear.



<Figure 3-6>

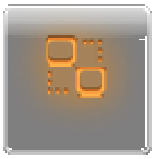
Select [1.Yes] to save the revised contents or [2.No] to cancel it, and then press [ENT] key. If there is no input for a certain period of time in this case, it returns to

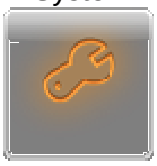
the initial screen.

- If there is no revised contents, it exits from the environment settings menu without the aforementioned process of “Save?”.

- When the settings are changed in the menu, if there is no input for a certain period of time, it exits from the environment setting menu. In this case, if there is any menu revised, it should pass through the “Save?” process. Otherwise, it transfers to the initial screen without saving the revised setting.

3.2. Menu Configuration

1. User 	1. Add 2. Delete 3. Modify 4. Delete All	
2. Network 	1. IP	1. Static IP / 2. DHCP ▶IP Address ▶Subnet Mask ▶Gateway
	2. Server IP	▶Server IP ▶Server Port
	3. Terminal ID	▶Terminal ID ▶Authentication
3. Application 	1. Application	▶Application 1. Access 2. Time & Attendance 3. Cafeteria
	2. Time Schedule	▶F1 Time ▶F2 Time ▶F3 Time ▶F4 Time ▶Access Time □NO Limit (when setting to catering management)
	3. Function Key	□F1 Enabled □F2 Enabled □F3 Enabled □F4 Enabled □Ent Enabled □Auto Sensing
	4. Extended Key	□ Extended Key ▶of Extended Key
	5. Display	▶Background ▶Clock Position □User Voice □User Text

4. System 	1. System Setting	▶UserID Length ▶Display Option
	2. Authentication	▶User GroupIP ▶Enable 1:N ▶Card Only ▶Template On Card ▶Verify Multi-FP ▶Blocking Time (sec.)
	3. Fingerprint	▶1:1 Level [1~9] ▶1:N Level [3~9] ▶Fake Finger Detect □Check SameFP
	4. Language	
	5. Data Time	▶Time Sync ▶Display Time ▶Set Current Time
	6. Database	1. Init Config 2. Delete All Users 3. Clear Log Data 4. Initialize Terminal
5. Terminal 	1. Terminal Option	□Terminal Alarm □Lock Terminal □KeyLed ON
	2. Volume Control	▶Voice Volume ▶Beeper Volume
	3. Door	▶Lock Type ▶Door Monitor ▶Open Duration ▶Warn Door Open
	4. Wiegand	□Bypass ▶Wiegand Out ▶Site Code
	5. Card Reader	▶Card Format ▶Read Card NO.
	6. External Device	▶Printer ▶Lock Controller
6. Information 	1. System Info 2. Network Info 3. Database Info 4. View Log 5. Version Info	

3.3. User

Select “1. User” in the main menu, then the following screen will appear.

Press [1] key to register new user,
[2] key to delete user,
[3] key to modify user, and
[4] key to delete all users.

3.3. 1. Add

◆ Select [ENT~] → [1. User] → [1. Add] ◆ in the basic screen, then the following screen will appear.

Input the user ID to be registered and then press [ENT] key.

In this case, it automatically shows the ID that can be registered on the screen, so the user can easily perform registration. To modify the ID, press [F4(←)] key and delete the existing value and input the new value.

If the user inputs an already registered ID, a failure message will appear. The following screen will appear if the ID is not yet registered.

The icon at left has the meaning as below;

: Authentication type

: Number of fingerprints registered (0~10)

: Number of cards registered (0~10)

: Whether or not password is registered (☑:Registered/☐:Not registered)

As shown on the screen, the user can register by pressing [2] for fingerprint, [3] for card, and [4] for password. Basically, it is registered in the name of the user. Using the keys [7] and [8], the user can modify into the user and the admin. Once the registration is completed, the user can press **[ENT]** to save it. The user must press [F4(←)] key to cancel the registration and exit from the menu.

※ Only the user registered as admin can modify the operating environment of the terminal, and Add/Modify/Delete the information of all the users saved in the terminal.

Therefore, special care is required for the registration of the admin.

3.3.1.1. Auth Type

Delete the existing value by pressing [F4(←)] key, enter one of the 12 authentication types shown on the screen, and then press [ENT] key.

3.3.1.2. FP Register

① **Place finger on the sensor referring to** '1.8. How to register and enter fingerprint'. Fingerprint must be input two times as below in accordance with the guidance on the screen.

When the fingerprint sensor is lit together with the message 'Place Finger on sensor', place the finger on the window for fingerprint input for 2~3 seconds until the light is off.

②When the message 'Place same Finger on sensor' appears, enter once again the fingerprint input just before.

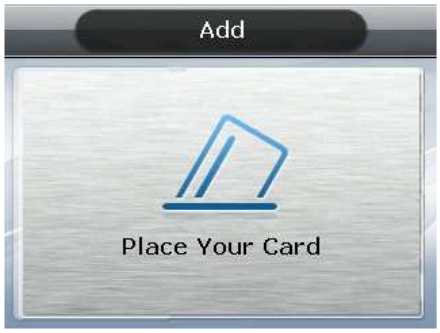
※At the time of entering the fingerprint for the second time, input it again after the user takes the finger off the fingerprint input window.

③ When input is complete, the message at the left will appear together with its image accompanied by quality rating in 0~100.
If the image is not adequate from the visual aspect or any image shows 30 or less, the user is advised to register again.
To register again, start the process from ① by pressing [F4(←)] key until 3 seconds elapse without input or pressing another key. After completion, it moves to the parent menu.

※ Fingerprint registration is available up to 10 per ID. Failure message will appear when registration is attempted in excess of 10.

In case that failure is repeated in spite of the attempts for 2~3 times using the correct fingerprint registration method, the user is advised to use password or card.

3.3.1.3. Card Register



When registration screen appears, put the card on it. If you want to exit without registration, press [F4(←)] key.

3.3.1.4. PW Register

Input the password in 1~8 digits on the password input screen and press [ENT] key. The 'Confirm Password' window will appear again. Input the same password and press [ENT] key.

Press [F4(←)] key for 2 seconds or longer to cancel it and exit.

3.3.1.5. FP Option

As it is the settings related with fingerprint, it is the option that can be changed after registering the fingerprint in advance. If the user selects it with the fingerprint already registered, it only results in the buzzer sound of failure.

▶'1:1 Level' (Initial setting: '0')
It is the item that determines the authentication level for each user registered. By modifying this value, it is possible to determine the authentication level by registered users.
When set to '0', it conducts authentication using 1:1 authentication level of the terminal.

▶Enable 1:N (Initial setting: 'v')
When this option is checked, it is possible to

successfully authenticate using fingerprint without any user ID or card.

3.3.1.6. Save

When registration process is finally completed, press [6] key to save it. In this case, the user is not saved if the user doesn't press [6] key but exits by pressing [F4(←)] key..

The following is the LCD guidance message indicating that the user can exit from the registration process.

	When it is registered normally with [6. Save] key pressed
	When registration is failed with [6. Save] key pressed When the registration means is not registered properly in accordance with the authentication method, for example, the user didn't register any fingerprint after setting it as authentication means, nor register any card after setting it as authentication means.
	In the case of [2. FP Register] When fingerprint image is not in good condition or there is no fingerprint input for 10 seconds after the fingerprint sensor lamp is on At the time of fingerprint registration, when the user didn't input the same fingerprint but inputs a different fingerprint
	In the case of [4. PW Register] When the user inputs a different number during verification after inputting the password

	In the case of [3. Card Register] When the user intends to register a card that has been already registered
	In case of [2. FP Register], when the user intends to register again the fingerprint that has already been registered. ※ If the user wants to register the same fingerprint with other ID again, he/she must release '4. System → 3. Fingerprint → Check SameFP' function. This is, however, not suitable for time & attendance, etc. as the same fingerprints can be authenticated with different IDs at the time of authentication.
	In case of [2. FP Register] or [3. Card Register] When the user attempted registration in excess of the maximum number of registrations (10 each)

3.3.2. Delete

When the user selects ◆ [ENT~] → [1. User] → [2. Delete] in the initial screen ◆, the following screen will appear.

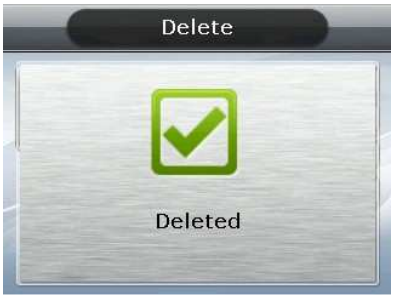
Input the user ID to be deleted, and then press [ENT] key.

When inputting an unregistered ID, the failure message will appear. When inputting a registered ID, the success message will appear.

Deleting from the terminal doesn't mean the deletion from the server. Therefore, it is necessary to delete from the server in order to completely delete it.

Special care should be taken in case of deletion, since deletion is performed regardless of User/Admin. Especially, the user registered in the terminal may not be restored after deletion unless it is registered in the network server.

The following is the LCD information message that may appear during the process of deletion;

	When it is deleted normally
	When the user inputs an unregistered ID

3.3.3. Modify

When the user selects ◆ [ENT~] → [1. User] → [3. Modify] in the initial screen ◆, the following screen will appear.

Press [ENT] key after inputting the user ID to be changed.

When inputting an unregistered ID, the failure message will appear. When inputting a registered ID, the following screen will appear.

The icons at the left are described by their respective meanings on the right.

: Authentication type (FP)

: Number of registered fingerprints (1)

: Number of registered cards (0)

: Whether or not the password is registered (: not registered)

For the changing method, see '3.3.1. Add' as it is the same as shown in the registration method.

3.3.4. Delete All

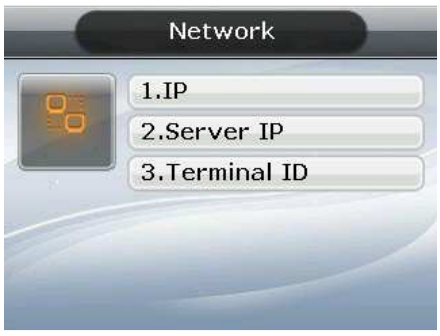
When the user selects ◆ [ENT~] → [1. User] → [4. Delete All] in the initial screen ◆, the following screen will appear.

If the user is sure to delete all users, press [1.Yes] while press [ENT] key after selecting [2.No] to cancel it.

※When the user selects [1.Yes], both user and admin are deleted. Special care should be taken as the deleted user/admin may not be restored after deletion.

3.4. Network

When the user selects “2. Network” in the main menu, the following screen will appear.



Press the applicable key that represents the item to be changed.

3.4.1. IP

When the user selects ◆ [ENT~] → [2. Network] → [1. IP] in the initial screen ◆, the following screen will appear.

At the time of changing IP, delete the existing value using [F4(←)] and then input the new value. The ‘.’ in between the number sequence is created automatically. Ex) input 192 168 010 50 sequentially to input ‘192.168.10.50’.

Select [1] in case of the method that a fixed IP is assigned from the connected network while select [2] in case of the method that there is a DHCP server in the connected network from which IP is assigned. Set IP, Subnet Mask, and Gateway if it is the fixed IP; No need to set them if the user selected a flexible IP.

The user can exit to the parent menu using [ENT~] key to apply the changed value after

finishing the setting while using [F4(←)] key to cancel input during setting. In this case, the user can exit only by pressing the key for 2 seconds or longer if he/she is inputting the value in the input box.

3.4.2. Server IP

When the user selects ◆ [ENT~] → [2. Network] → [1. Server IP] in the initial screen ◆, the following screen will appear.

Set the Server IP and Port.

To change the port, input it after moving the input focus to the server port by pressing [ENT] key.

▶Initial setting
Server Port: '9870'

The basic port value of authentication server is '9870' for UNIS server, while '2201' for Access server. Special care should be taken since changing these values requires the similar changes in the server program.

The user can exit to the parent menu by pressing [ENT~] key to apply the changed value after finishing the setting while pressing [F4(←)~] key to cancel the input value.

3.4.3. Terminal ID

When the user selects ◆ [ENT~] ([2. Network] ([3. Terminal ID] in the initial screen ◆, the following screen will appear.

Set Terminal ID and Authentication.

▶Initial setting
Terminal ID: '1'
Authentication: '2. terminal/server'

Terminal ID is a unique ID used by the authentication server for the purpose of identifying the terminal having '1' as its default value. It must correspond to the entry/exit door ID set in the server program, which can be input in a maximum of 8 digits.

▶ Authentication
This item determines the priority for authentication between terminal and network server. Having '2. Terminal/Server' as its default value, it operates as follow in each mode.

1.Server/Terminal	Authentication is made by the server when it is connected to the server while by the terminal when it is disconnected to the server due to network disturbance, etc.
2.Terminal/Server	Authentication is made by the terminal even if the server is connected and the result of authentication is transferred to the server on a real-time basis.

	However, authentication is made by the server when the input user ID or card is not registered in the terminal. (It doesn't attempt server authentication in case of 1:N fingerprint authentication)
3. Server Only	Although the user is registered in the terminal, authentication is made through the server. Therefore, authentication is not made unless the server is connected.
4. Terminal Only	Only the user registered in the terminal is authenticated. When connected to the server, the authentication result will be transmitted to the server on a real-time basis.

Flexible designation is allowed depending on the circumstance such as the number of terminals connected to the server, the number of users authenticated, or the network error, etc. It is recommended to use '2. Terminal/Server' so that concurrent authentications could be attempted when at least 10 terminals are connected to the server or when network error frequently occurs in general.

3.5. Application

When the user selects '3. Application' in the main menu, the following screen will appear.

Press the applicable key that represents the item to be changed.

3.5.1. Application

When the user selects ◆ [ENT~] → [3. Application] → [1. Application] in the initial screen ◆, the following screen will appear.

Select the operation type of the terminal by pressing the applicable number key.

Press [ENT] key to apply the configuration while [F4(←)] key to cancel it.

3.5.2. Time Schedule

3.5.2.1. Setting to Access / Time & Attendance

When the user selects ◆ [ENT~] → [3. Application] → [2. Time Schedule] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

The user can set the time zone by authentication modes; otherwise, set to '00:00-00:00'..

Input after deleting the existing value using [F4(←)] to change the value.
Input HHMM (Hour/Minute) in the order which can be set from 00:00 to23:59

In the preset time zone, it is always indicated in the preset mode unless the user presses the other function key. Although the user pressed the other function key to authenticate with another mode, terminal display mode is automatically changed into authentication mode, which is suitable for the management of time & attendance.

As shown in the example below, each time zone must be set without being overlapped, but the mode is determined like F1→F2→F3→F4→Access sequentially if they are overlapped.

(Ex) Office start=06:00~09:59, Office leave=17:00~22:00

Exit to the parent menu by pressing [ENT~] key to apply the changed value after finishing the setting while pressing [F4(←)~] key to cancel the input value.

3.5.2.2. . Setting to Cafeteria

▶Initial setting: Identical with the screen at the left

The user can set the time zone by meal types; otherwise, set to '00:00-00:00'.

▶NO Limit

When releasing the check box (☐), each user is allowed for one authentication by meal only, but when the user checks the box (☑) he/she is allowed for several authentications regardless of the existing authentication.

3.5.3. Function Key

When the user selects ◆ [ENT~] → [3. Application] → [3. Function Key] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

Function key means the key including [F1]~[F4], [ENT] used to change the authentication mode such as office start/office leave, etc. When the user presses the function key, authentication mode is changed into the applicable mode. When it is not checked, authentication mode is not changed even though the applicable key is pressed. Therefore, it can be used with the checked other function key released in the event of using it as the terminal exclusively for office start or office leave.

In case of releasing the check box of '6.Auto Sensing', fingerprint sensor doesn't respond even if the user inputs his/her fingerprint on the sensor. In this case, be sure to input the ID or card or fingerprint of the user.

3.5.4. Extended Key

When the user selects ◆ [ENT~] → [3. Application] → [4. Extended Key] in the initial screen ◆, the following screen will appear.

,

▶Initial setting: Identical with the screen at the left

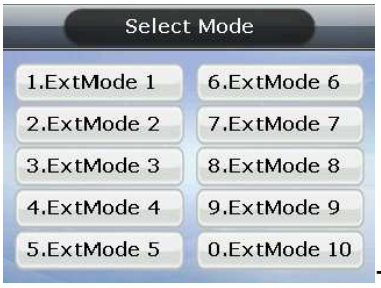
To use the Extended Key, press [1] key and then check '1. Extended Key. The number of extended keys can be set within the range of 1~40.

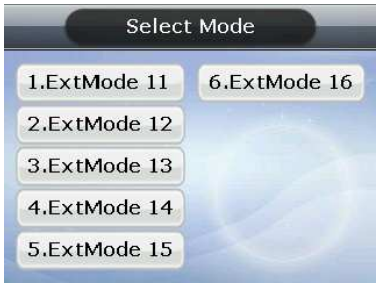
Extended Key is the function that extends the number as required up to 40 when any additional authentication modes are necessary in addition to the basic function key ([F1]~[F4], [ENT]). In this case, the screen for selecting the extended key as below when the user presses the F4 key. Select the applicable mode with [0]~[9] keys.

When the number of extended keys exceeds 10, select them by changing the page with

[F1]~[F4] key.

Ex) In case the number of extended keys is 16, press [F4] key in the initial screen, then the following screen will appear.



→


If the user has to select ExtMode 12, move to the next page with [F2] key and then press [2] key.
Press [ENT] key to exit without selecting the extMode.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

3.5.5. Display

When the user selects ◆ [ENT~] → [3. Application] → [5. Display] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶Background image
The user can change the background image of the initial screen by pressing [1] and [2] keys. Also, the user can set the cycle to 5 seconds or longer to have the background images saved in the terminal displayed sequentially at every preset interval (seconds).

▶Clock Position
Changes the location of the clock appearing on the initial screen

Based on the user's need/preference, he/she can download the voice from Wav file (16bit/8KHz) to change the voice output when authentication is successful or failed. In addition, the user can download the image text in a modified form such as office start or office leave using the specially provided resource file (Excel file). In this case, the user can apply the applicable modified contents when only the boxes of '6. User Voice', and '7. User Text' are checked. For the downloading method, see '3.9.Download customized file'

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.6. System

When selecting ‘4. System’ in the main menu, the following screen will appear.

Press the applicable key that represents the item to be changed.

3.6.1. System Setting

When the user selects ◆ [ENT~] → [4. System] → [1. System Setting] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶ UserID Length

This field sets the length of user ID, which can be changed within the range of 1~9 digits. It must be identical with the length of ID registered in the server program. For example, the user must set it to 6 if the ID registered in the server program is ‘000075’ which is 6 digits.

▶ Display Option

If set to ‘1. None’, it displays the authentication result message only when authentication is successful. If set to ‘2’, it displays the User ID. If set to ‘3’, ‘4’, and ‘5’, it displays the User Name, User Key, and Message respectively on the LCD screen. However, it indicates the ID in case there is no applicable information of the user saved in the terminal.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.6.2. Authentication

When the user selects ◆ [ENT~] ([4. System] [2. Authentication]) in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶User GroupIP

As the method of authentication regarding the initial digit of ID as the same group, it can finish 1:N authentication more quickly if at least 5,000 users are registered.
When this method is checked, it authenticates the fingerprint out of the users whose ID starts with the input letter. If this method is not checked, it considers the input figure as the user ID and attempts 1:1 authentication against the fingerprint of the user with the applicable ID
Ex) Where the user inputs '12' to attempt authentication when the user ID is a 4-digit figure;

If checked (☑), it attempts 1:N authentication among the users having ID '1200'~'1299',

If unchecked (☐), it attempts 1:1 authentication against the fingerprints of the users whose ID is '12'.

▶Enable 1:N

If checked (☑), this option enables to authenticate with fingerprint only without inputting user ID or card. Even if the user is registered with 1:N authentication, only 1:1 authentication is permitted in the terminal where this option is not checked

▶Card Only

If checked (☑), this option enables to authenticate with card only without inputting fingerprint. Even if the user is registered with (Card & FP) or (Card & PW), only authentication with card is permitted in the terminal where this option is checked.

▶Template On Card

If checked (☑), this option enables to authenticate with the user's information and fingerprint recorded in the card without downloading the user in the terminal. In order for this option to be operated, SCcard reader must be mounted without fail and the server must set the terminal that uses fingerprint card.

▶ Verify Multi-FP

If checked (☑), this function has all the registered fingerprints to be authenticated after the user inputs ID (or Card). When this item is set to be checked, the user must input user ID or card without fail. In this case, Enable 1:N is changed into unchecked (☐) automatically.

This function is used for strict access control of the special zone. For example, if the user with ID '0001' is registered with 3 fingerprints, he/she must input ID and complete the authentication for three fingerprints.
In this case, the order of authentication for 3 fingerprints is irrelevant, but the fingerprints should be repeatedly input until authentication is successful. Authentication will fail even at a single occurrence of authentication failure.

▶ Blocking Time (sec)

This is the function that prevents duplicate authentication for the same user within the preset time zone. When set to 0, it has no restriction. However, when set to a value larger than 0, the user can be successful in re-authentication if the preset time (sec) has elapsed after the success of the previous authentication.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.6.3. Fingerprint

When the user selects ◆ [ENT~] → [4. System] → [3. Fingerprint] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶1:1 Level

Authentication level that is used for 1:1 Fingerprint Authentication, provided that, 1:1 authentication level of the relevant user shall apply for the user whose 1:1 authentication level is not set to '0' (using the authentication level of the terminal)

▶1:N Level

Authentication level that is used for 1:N Fingerprint Authentication. In case of 1:N authentication, the authentication level by users is not set and therefore, it is always based on the authentication level of the terminal.

▶ Fake Finger Detect

It presets LFD level that can prevent imitation fingerprint input. When presetting the LFD level to a higher value, it tends to reinforce the function that prevents the input of imitation fingerprint produced with rubber, paper, film, silicone, etc. But even when inputting a real fingerprint, it may not input well if it is in dry condition.

▶ Check SameFP

If checked (☑), it is the function that checks whether or not the fingerprint is already registered during registration so as to prevent overlapped registration of the same fingerprint in another user ID.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.6.4. Language

When the user selects ◆ [ENT~] → [4. System] → [4. Language] in the initial screen ◆, the following screen will appear.

▶Initial setting: '1. English'

When changing the language settings, the voice message and on-screen message are changed into the language set.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.6.5. Data Time

When the user selects ◆ [ENT~] → [4. System] → [5. Data Time] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶ Time Sync

It sets the method that synchronizes the current time of the terminal with the server. To synchronize the terminal time with the server time, set to '1. Auto' to perform it automatically while '2. Manual' to perform it manually.

▶ Display Time

The method of displaying the current time of the terminal set to '1' for 24-hour system and '2' for AM/PM system

▶ Set Current Time

It changes the current time of the terminal. No change is required as it is synchronized with the server time when linked to the server with the aforementioned Time Sync set to '1. Auto'.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

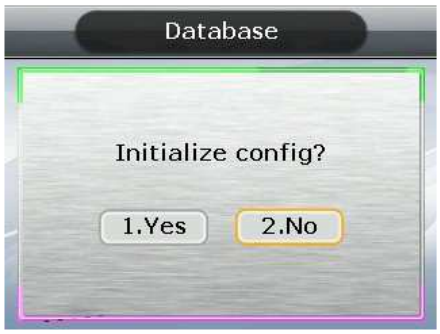
3.6.6. Database

When the user selects ◆ [ENT~] → [4. System] → [6. Database] in the initial screen ◆, the following screen will appear.

Press the following keys;
[1] key to initialize the configuration,
[2] key to delete all users,
[3] key to initialize the authentication record,
and [4] key to initialize the terminal.

3.6.6.1 Init Config

When the user selects ◆ [ENT~] → [4. System] → [6. Database] → [1. Init Config] in the initial screen ◆, the following screen will appear.



Press [1.Yes] key to initialize all configurations while select [2.No] and press [ENT] key to cancel it.

When no value is input for a certain period of time in this state, it returns to the initial screen instead of initialization.

It initializes all the configurations of the terminal except MAC (physical) address but it doesn't delete the user and authentication record.
When the configuration is successfully initialized, it proceeds to the parent menu accompanied by the success buzzer sounds.

3.6.6.2. Delete All Users

When the user selects ◆ [ENT~] → [4. System] → [6. Database] → [2. Delete All Users] in the initial screen ◆, the following screen will appear.

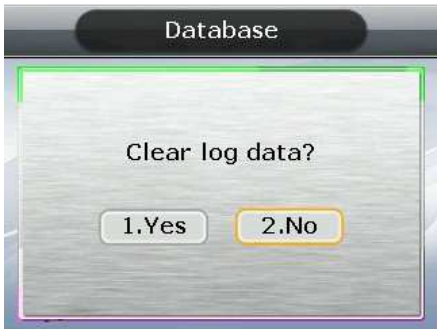
Press [1.Yes] key to delete all users while select [2.No] and press [ENT] key to cancel it.

When no value is input for a certain period of time in this state, it returns to the initial screen instead of deletion.

Both user and administrator are deleted, and the deleted users may not be restored after deletion.
When deletion is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sounds.

3.6.6.3. Clear Log Data

When the user selects ◆ [ENT~] → [4. System] → [6. Database] → [3. Clear Log Data] in the initial screen ◆, the following screen will appear.



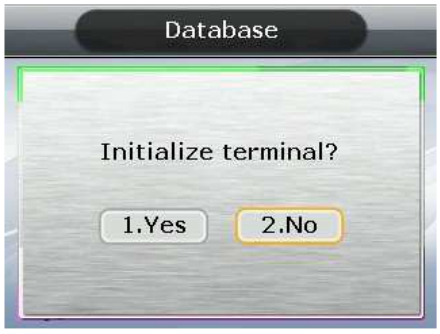
Press [1.Yes] key to delete all the authentication records saved in the terminal while select [2.No] and press [ENT] key to cancel it.

When no value is input for a certain period of time in this state, it returns to the initial screen instead of deletion.

It deletes all the logs related to authentication, and the deleted logs may not be restored after deletion**.**
When deletion is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sounds.

3.6.6.4. Initialize Terminal

When the user selects ◆ [ENT~] → [4. System] → [6. Database] → [4. Initialize Terminal] in the initial screen ◆, the following screen will appear.



Press [1.Yes] key to initialize the terminal to the factory default state while select [2.No] and press [ENT] key to cancel it.

When no value is input for a certain period of time in this state, it returns to the initial screen instead of initialization.

It deletes all the configurations, users, and log information except MAC (physical) address saved in the terminal, restoring it to the factory default state. Special care should be taken as restoration is impossible after it is initialized.
When initialization to the factory default state is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sounds

3.7. Terminal

When selecting '5. Terminal' in the main menu, the following screen will appear.

Press the applicable key that represents the item to be changed

3.7.1. Terminal Option

When the user selects ◆ [ENT~] → [5. Terminal] → [1. Terminal Option] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶Dooropen
Door is opened when pressing '0' key.
It appears only when the terminal is locked. This is option not normally shown.

▶ Terminal Alarm
If checked, (☑), it generates a warning sound when the lid of the terminal is opened.

▶ Lock Terminal
This is the function that the administrator can directly set or release the locking of the terminal through the terminal instead of server program. If checked (☑), it is locked so that no one can access until the administrator releases the settings.

▶ KeyLed ON
If checked (☑), Key LED is always turned ON so that Touch Key is visible.

▶ Dooropen
This is the menu that shows the terminal administrator is allowed to temporarily open the door where the terminal is set to lock in the server.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.7.2. Volume Control

When the user selects ◆ [ENT~] → [5. Terminal] → [2. Volume Control] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

Sets Voice Volume and Beeper Volume.
When set to '0', no voice or buzzer sound is generated.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.7.3. Door

When the user selects ◆ [ENT~] → [5. Terminal] → [3. Door] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶Lock Type
Set to '1' when strike type or automatic door is connected with the terminal while '2' when motor lock is connected to the terminal. In case that no connection is made, it is also set to '1'. Set to '3' when connecting the warning lamp to the lock port to indicate the success or failure of authentication.

▶Door Monitor
Set this function to know the door status
- '3.Disable' – when not checking the door status
- '1.Normal Open': In the case of dead bolt type or automatic door
  (When lock monitoring is open where the door is locked)
- '2.Normal Close': In the case of Strike type
  (When lock monitoring is locked where the door is locked)

▶Open Duration (0.1 sec unit)
It designates the time that the door is opened and closed again when authentication is successful. As it is set to 0.1 second unit, a value of 30 is required to set it to 3 seconds. Strike type refers to the time the door is opened and closed again when authentication is complete.

▶ Warn Door Open (Second unit)
This is the function that enables the terminal to check the time of the door being

opened, and generates a warning sound once it exceeds the preset time (min. 5 sec~ max 30 sec).
When set to '00', warning doesn't sound at all. Even if set to 01~04, it starts sounding when it exceeds at least 5 seconds.

The warning sound is also generated in case the door is not closed unexpectedly within the preset time although the door should be closed. It allows for a proper action to be taken for the door to be closed by informing about the fact that the door is not closed.

To operate this function, the lock must be the one that enables to monitor the door status and the monitoring pin of lock should be connected to the terminal without fail. In addition, such settings are enabled only when the aforementioned Door Monitor is set to '4. Normal Open' or '5.Normal Close'.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.7.4. Wiegand

When the user selects [ENT~] → [5. Terminal] → [4. Wiegand] in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

This is the menu that configures the Wiegand Output.

It is used only when a separate controller operating with Wiegand input is mounted. Upon successful authentication, it transmits the data to the terminal's Wiegand port in the following form;

2.None	This is the normal case; Wiegand Output is not used in this case.
3.26bit	It transmits "Sitecode[1byte] + user ID[2byte]", so the user ID is set to 4 digits or less. Example) In the case of SiteCode:045(2Dh), UID:6543(198Fh), it is transmitted as '1 00101101 0001 1001 10001111 0'
4.34bit	It transmits "Sitecode[1byte] + user ID[3byte]" so the user ID is set to 7 digits or less. In case of an 8-digit user ID, "user ID[4byte]" is transmitted without Sitecode. Example) In the case of SiteCode:001(1h), UID:123456(1E240h), it is transmitted as '0 00000001 00000001 11100010 01000000 0'
5.Custom	It can be set in the server as the settings under the user's definition

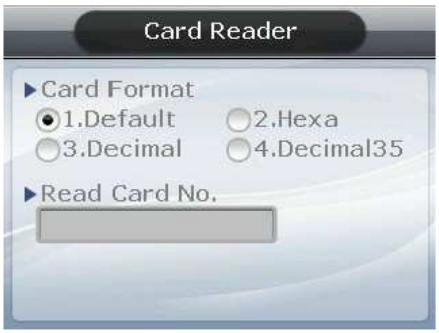
	only. The setting type can only be inquired at the terminal.

However, when Bypass is checked, regardless of Wiegand Out settings, it transmits the data received by Wiegand Input at the time when authentication was successful to the Wiegand Output as it is.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

3.7.5. Card Reader

When the user selects [ENT~] → [5. Terminal] → [5. Card Reader] in the initial screen ◆, the following screen will appear.



▶Initial setting: Identical with the screen at the left

▶ Read Card NO.
When the user puts the card on this screen, the card number will be displayed on the LCD.

▶Card Format
This is the menu that sets the manner of displaying the card number. As shown below, the displayed card number varies depending on the configuration. Therefore, if changing it during operation is unavoidable after it was set during initial installation, the card should be registered again.

RFcard example) Card number (5byte): 08h 01h 16h 1Dh D6h

Card Format	Card Number	Method of Expression
1. Default	02207638	(3+5) digit decimal number [022(16h)+07638(1DD6h)]
2. Hexadecimal number	0801161DD6	10-digit hexadecimal number
3. Decimal number	0018226646	Last 4byte to be expressed in a 10-digit decimal number (01161DD6h)
4. Decimal number 35	02207638	Same as '1. Default'

SCcard example) Card Number (4byte): 52h 9Dh 06h E3h

Card Format	Card Number	Method of Expression
1. Default	529D06E3	Expressing in an 8-digit hexadecimal number
2. Hexadecimal	E3069D52	Expressing in an 8-digit hexadecimal number changing the order of byte

number		
3. Decimal number	1386022627	Hexadecimal number 529D06E3 to be expressed in a 10-digit decimal number
4. Decimal number 35	3808861522	Hexadecimal number E3069D52 to be expressed in a 10-digit decimal number

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.7.6. External Device

When the user selects [ENT~] ([5. Terminal] [6. External Device]) in the initial screen ◆, the following screen will appear.

▶Initial setting: Identical with the screen at the left

▶Printer

If checked ( ), it prints out the authentication result. When set to '1', if authentication is successful, the terminal ID, user ID, authentication time, authentication mode, etc. are printed out through the printer connected to the RS232 (Debug) port of the terminal. The print out type may vary depending on the configuration. When set to 'Format2', it is printed out with the terminal name as the main subject. The printer used is는 "SRP-350" Serial type.

▶ Lock Controller

Set to this function when the user connects a separate device instead of the terminal lock port to control the door. In the event the user directly connected a lock to the terminal, it is set to '4. None', but it is set to '5.LC010' when connected with LC010.

The user can exit to the parent menu using [ENT~] key to apply the changed value after finishing the setting while using [F4(←)] key to cancel input during setting.

.

3.8. Information

When selecting '6. Information' in the main menu, the following screen will appear.

Menu to inquire the setting condition of the terminal.

Press;
[1] key to inquire a variety of optional configurations of the terminal,
[2] key to inquire network configuration such as IP ,
[3] key to inquire the user registration status, etc.
[4] key to inquire log data,
[5] key to inquire firmware version.

3.8.1. System Info

Select ◆ [ENT~] → [6. Information] → [6. System Info] in the initial screen ◆

Press [F4(←)] key to exit to the parent menu.

3.8.2. Network Info

Select ◆ [ENT~] → [6. Information] → [2. Network Info] in the initial screen ◆

Press [F4(←)] key to exit to the parent menu.

3.8.3. Database Info

Select ◆ [ENT~] → [6. Information] → [3. Database Info] in the initial screen ◆

- Registered User: Number of registered users (including administrator)
- Registered Admin: Number of registered administrators
- Max User: Maximum number of users that can be registered
- Registered FP: Number of whole fingerprints that are registered
- Max FP: Maximum number of fingerprints that can be registered

Press [F4(←)] key to exit to the parent menu.

3.8.4. View Log

Select ◆ [ENT~] → [6. Information] → [4. View Log] in the initial screen ◆

- All Log: Number of logs saved in the terminal
- Max Log: Maximum number of logs that can be saved

Press [F4(←)] key to exit to the parent menu.

3.8.5. Version Info

Select ◆ [ENT~] → [6. Information] [5. Version Info] in the initial screen ◆

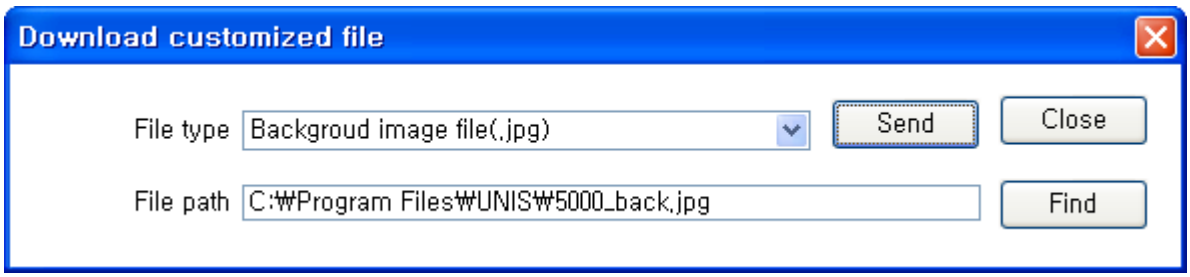
Press [F4(←)] key to exit to the parent menu.

3.9. Downloading user's file

The function allows the user to change background image or voice message when necessary. The user's file can be downloaded from UNIS server program.

3.9.1. Change background image

When selecting 'Download customized file' in UNIS program, the following screen will appear.



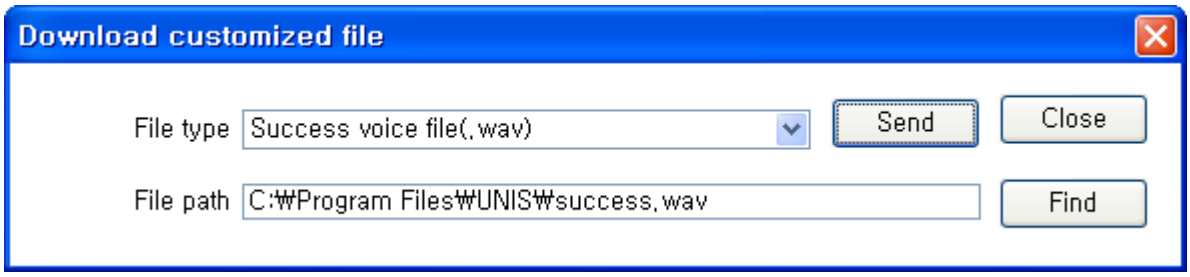
Designate the file as 'Background image file (.jpg)', select the image file (.jpg), and click the 'Send' button, then the terminal select window will appear. When selecting the terminal on the terminal list window and clicking the 'Send' button once again, the file will be transmitted with the downloaded result displayed.

In this case, the file name can be selected up to 15 characters including the extension name with the jpg file in the size of 320*240 only. If any data in a different format is downloaded, the transmission result will be displayed in a version error.

To change background image, the user can directly select it from ‘3.5.5 Display”.

3.9.2. Change Voice Message

When selecting ‘Download customized file’ in UNIS program, the following screen will appear.



Designate the file as ‘Success voice file (.wav)’, select Wav file (.wav) and click the ‘Send’ button, then the terminal select window will appear. When selecting the terminal from the terminal list window and clicking the ‘Send’ button once again, the file is transmitted with the downloaded result displayed.

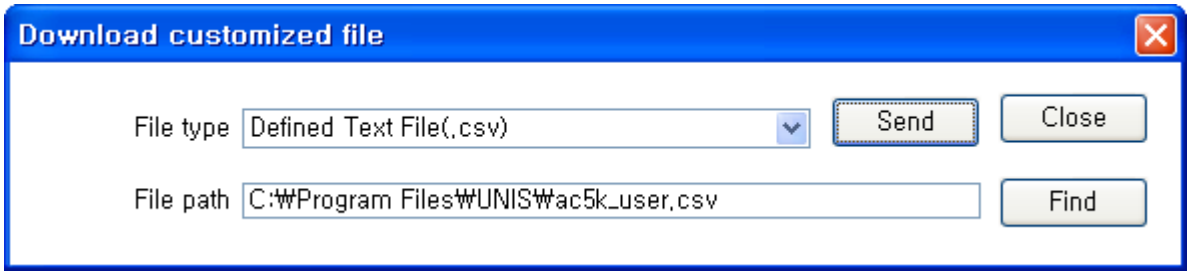
In this case, the file name can be selected up to 15 characters including the extension name with the Wav file in 8KHz, 16bit, in mono form only. If any data in a different format is downloaded, the transmission result will be displayed in a version error.

In the case of the failure voice, designate the file as ‘Fail voice file (.wav)’ and then change it in the same way.

In order to change the user’s defined voice into default voice, release the check mark in the ‘User Voice’ item in ‘3.5.5 Display’.

3.9.3. Change User Text

When selecting ‘Download customized file’ in UNIS program, the following screen will appear.

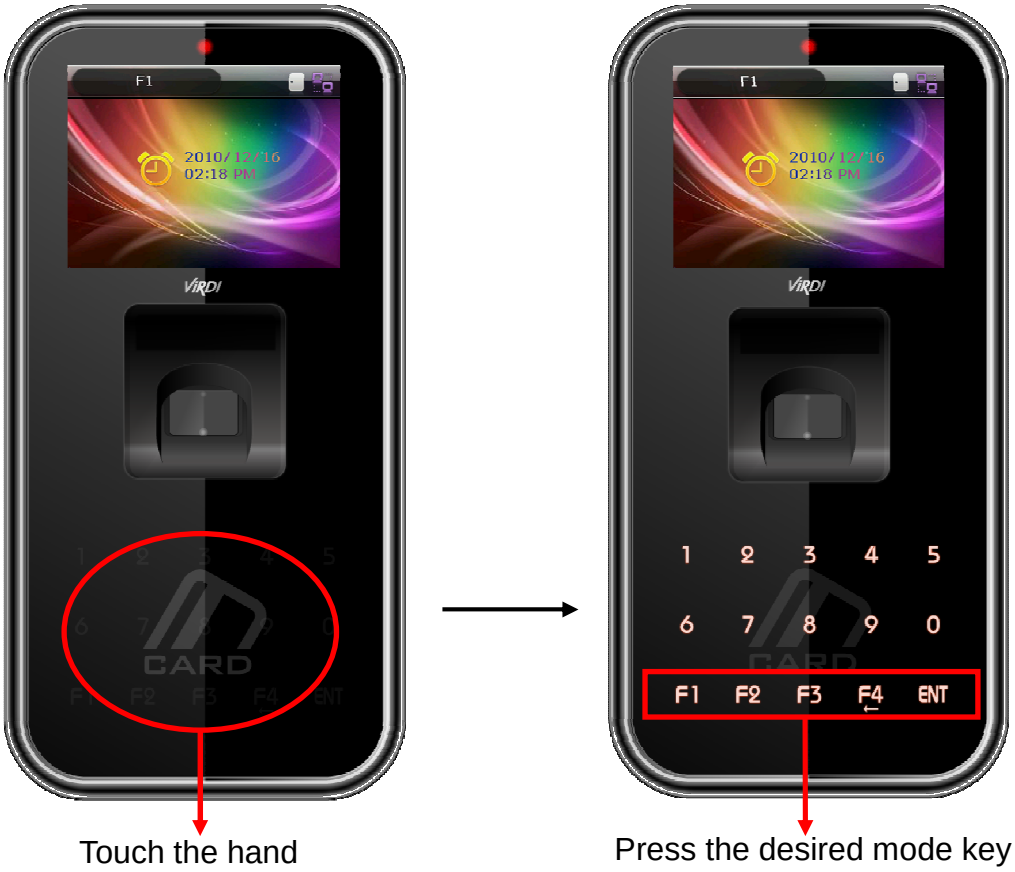


Designate the file as ‘Defined Text File (.csv)’, select CSV file (.csv) and click the ‘Send’ button, then the terminal select window will appear. When selecting the terminal from the terminal list window and clicking the ‘Send’ button once again, the file is transmitted with the downloaded result displayed.
CSV file can be saved and created in the form of csv type after changing the desired text in the Excel (.xls) file provided together with the firmware of the terminal. In order to change it from the user’s defined text to the default text, release the check mark in the

‘User Text’ item in ‘3.5.5 Display’.

4. How to use terminal

4.1. Change of authentication mode



<Figure 4-1>

Normally, it is not visible; but when the user touches the hand on the card input area as shown in the Figure at the left, LED will be powered ON and a keypad will appear as shown in the Figure at the right. When the key is visible, press the desired function key to change into the authentication mode such as office start [F1], office leave [F2], going-out [F3], return [F4], access [ENT], etc.

4.2. ID input

Normally, it is not visible; but as shown in Figure <4-1>, when the user touches the hand on the card input area, LED will be powered ON and a keypad will appear. In this case, ID input screen will appear when the user inputs the figure.

Delete with [F4(←)] key if the figure is wrongly input during the input process.
When pressing [ENT] key after inputting ID, the fingerprint input or password input screen appears depending on the method of user authentication.
However, authentication will fail if a card user inputs ID first. Therefore, be sure to use the card.

4.3. Authentication

4.3.1. Fingerprint Authentication

When placing fingerprint on the fingerprint sensor, buzzer sounds with the sensor lamp ON, and the fingerprint is duly input. Be sure not to take finger off the sensor until the sensor lamp is OFF and the buzzer sounds.
In the case of 1:1 authentication, input ID and press [ENT] key causing the fingerprint sensor to flicker, and then input fingerprint to the fingerprint sensor.

4.3.2. Card Authentication

Touch the card on the figure of the card as shown in <Figure 4-1>.

4.3.3. Password Authentication

Press [ENT] key after inputting ID, then the screen for password input will appear. When a wrong number is input, delete it using [F4(←)] key. Input the password and press [ENT] key.