

AC-5000 User Guide

Version eng-1.00



***VIRDI* GSS**
Advanced Biometrics Security Solutions

<Revision History>

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

<Glossary>

- Admin (Administrator)
 - A user who can enter the terminal menu mode. They are authorised to register/modify/delete terminal users and alter 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 rights to change important environmental settings of the fingerprint recognition unit.
- 1:1 Authentication (1 to 1, Verification)
 - This is a method that authenticates fingerprints together with a user ID or card.
 - This method is called 1:1 authentication as only the fingerprint registered for the user ID or card is used for comparison.
- 1:N Authentication (1 to N, Identification)
 - This is a method that searches for a corresponding user only with fingerprint.
 - This method is called 1:N authentication as it searches for the identical fingerprint, from the registered fingerprints, without a user ID or card being 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 is only successful when the similarity 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, including FP (fingerprint) authentication, RF (card) authentication or a combination of these methods.
Example: 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 times.
- 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



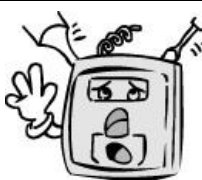

<Revision History>	2
<Glossary>	2
Table of Contents	3
1. Before Use	4
1.1. Safety Precautions	5
1.2. Terminal Description	5
1.3. Screen Description (During Operation)	6
1.3.1. Icons Shown During Operation	6
1.3.2. Message Shown During Operation	7
1.4. LED Signal Shown During Operation	10
1.5. Keys Used 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	14
2.2.1. Standalone (Access)	14
2.2.2. Connect with PC SERVER (Access, Time & Attendance, Cafeteria) ..	14
2.3. Specification	15
3. Environment Settings	16
3.1. Items to be checked before environment settings.	16
3.1.1. Enter the Menu.	16
3.1.2. How to access the menu without the Admin verification.	17
3.1.3. Modify Set Values	18
3.1.4. Save Environment Settings	19
3.2. Menu Configuration.....	20
3.3. User	22
3.3. 1. Add	22
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	32
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	36
3.6.3. Fingerprint	37
3.6.4. Language.....	38
3.6.5. Date Time	38
3.6.6. Database	39

3.7. Terminal	41
3.7.1. Terminal Option	41
3.7.2. Volume Control	42
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	46
3.8.1. System Info	46
3.8.2. Network Info	46
3.8.3. Database Info	47
3.8.4. View Log	47
3.8.5. Version Info	47
3.9. Downloading User's File	48
3.9.1. Change Background Image	48
3.9.2. Change Voice Message	48
3.9.3. Change User Text	49
4. How to use the Terminal	49
4.1. Change of 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


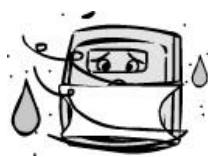



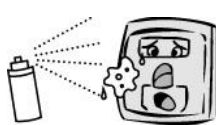

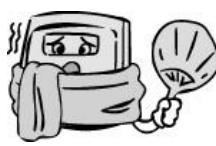
1.1. Safety Precautions

● Warning

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

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

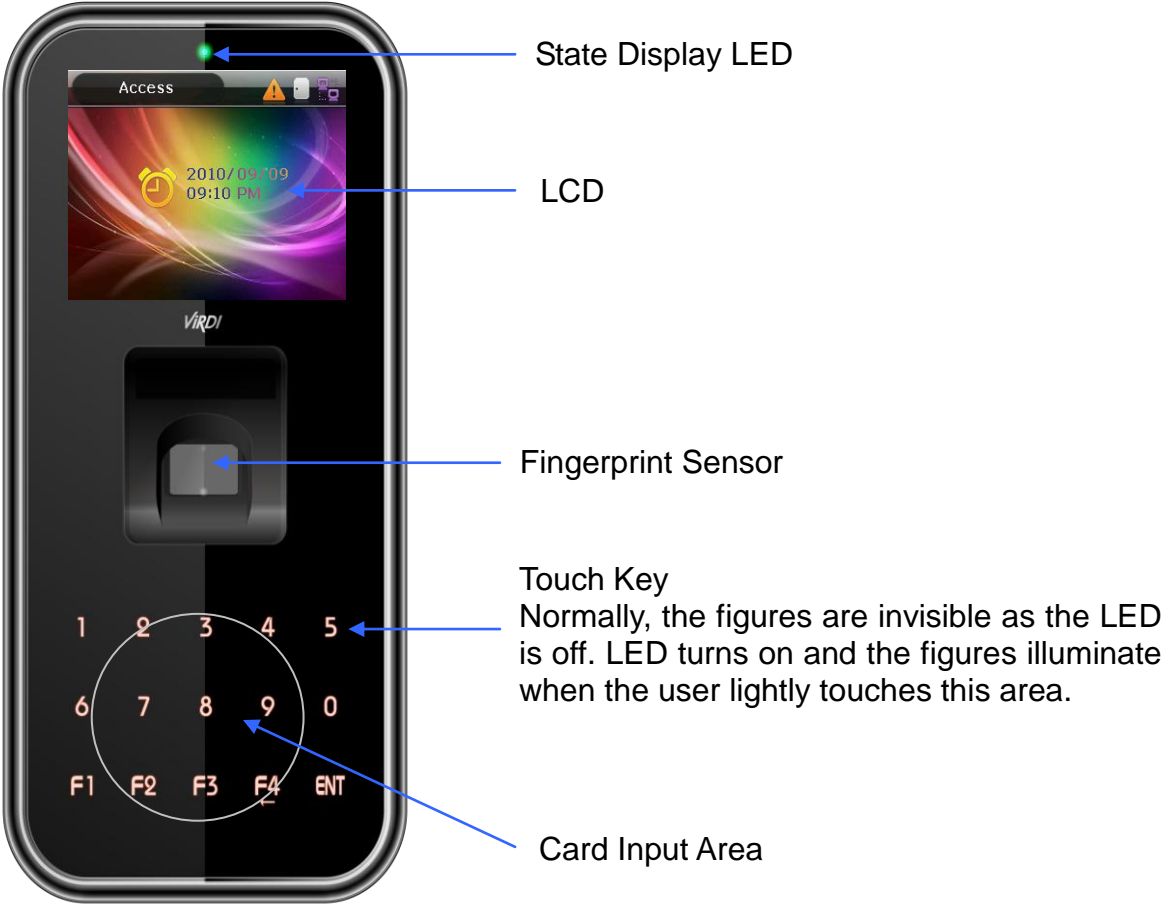
● Cautions

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

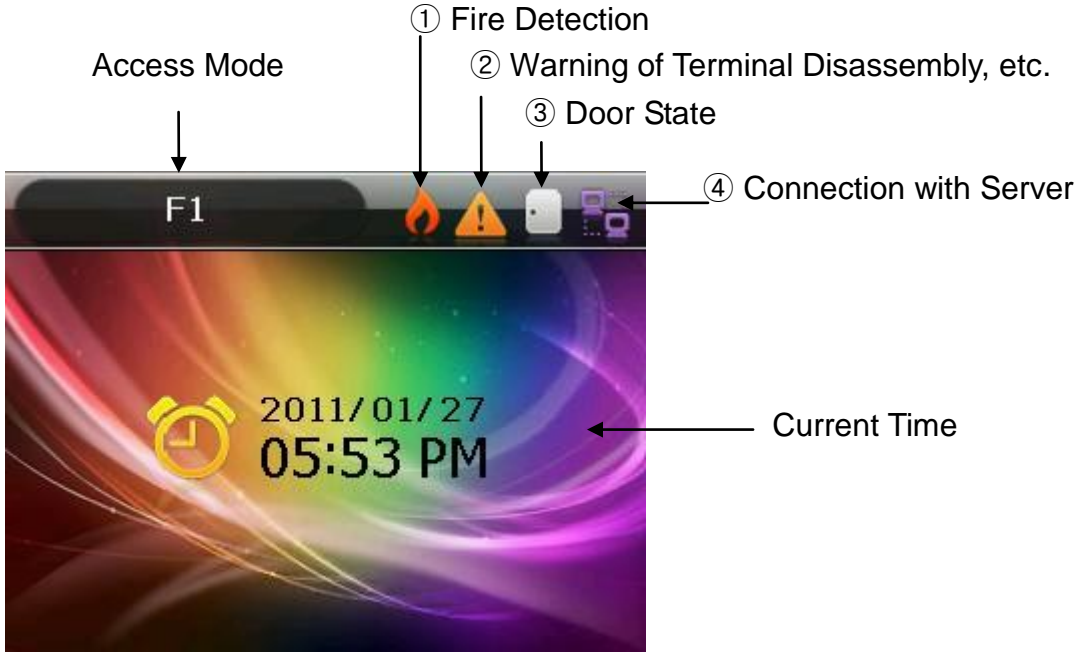
- If the above cautions are ignored, it may result in property damage or human injury.

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

1.2. Terminal Description










1.3. Screen Description (During Operation)


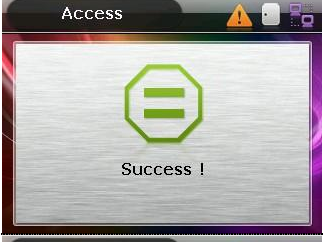
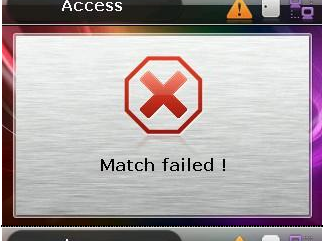
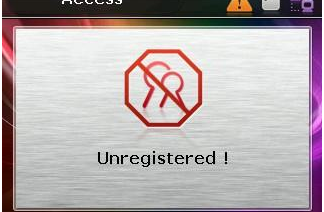




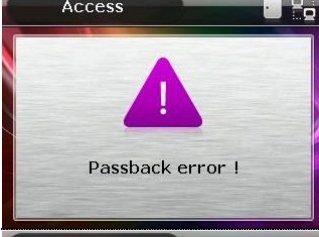

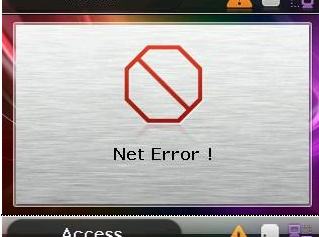
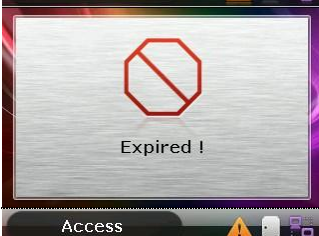
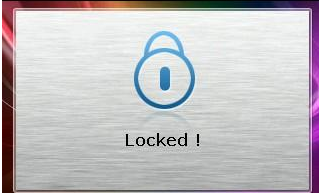
1.3.1. Icons Shown During Operation

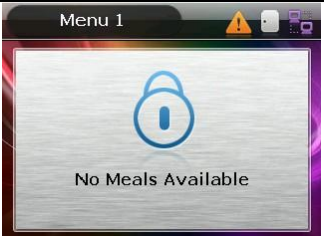
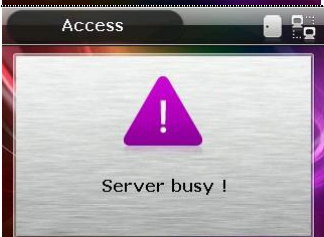


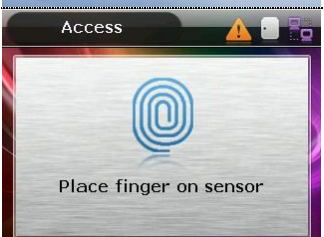
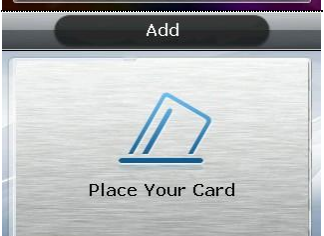
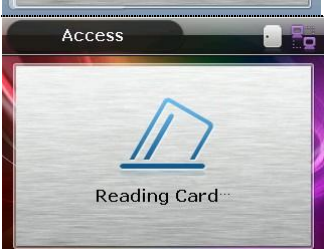
① Fire Detection	None : Normal
------------------	---------------

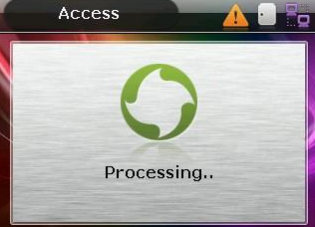

		: State when fire is detected by a fire sensor (subject to the appropriate fire sensor connection).
② Warning	None	: Normal.
		: Abnormal state when terminal is disassembled or door has encountered a problem.
③ Door Status		: Door status is unknown.
		: Door is closed.
		: Door is open.
④ Connection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

1.3.2. Message Shown During Operation

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

	<ul style="list-style-type: none">- When any unregistered card is input.
	<ul style="list-style-type: none">- When fingerprint input has failed.- If the user removed their finger too quickly before the fingerprint was identified.
	<ul style="list-style-type: none">- When Anti-Pass Back is in error (if the anti-pass back function is being used).
	<ul style="list-style-type: none">- If a user made two or three attempts at the same meal time zone (if being used for cafeteria operation).
	<ul style="list-style-type: none">- If there is no response from the server when attempting authentication to the server.- When network is disconnected during an authentication attempt to the server.
	<ul style="list-style-type: none">- When the user is not authorised for authentication, even if they are registered, or the user attempted authentication when access is not allowed.
	<ul style="list-style-type: none">- When the terminal is set to Locked.

	<ul style="list-style-type: none"> - When it's not a meal time (if being used for Cafeteria operation).
	<ul style="list-style-type: none"> - When the authentication cannot be processed due to too many server authentication requests from the terminal.
	<ul style="list-style-type: none"> - Show the waiting status for a user's ID input.
	<ul style="list-style-type: none"> - Status waiting for password input from the user.
	<ul style="list-style-type: none"> - Status waiting for fingerprint input from the user.
	<ul style="list-style-type: none"> - Status waiting for card input from the user.
	<ul style="list-style-type: none"> - During fingerprint card authentication, it shows the status when the card reads fingerprint data. The user must position the card for 1~2 seconds until the message disappears.

	<ul style="list-style-type: none"> - When waiting for a response, after the user attempted authentication by the server.
	<ul style="list-style-type: none"> - When upgrading the terminal program. Make sure the terminal is not powered off while this message is being output.

1.4. LED Signal Shown During Operation

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

1.5. Keys Used During Operation

[0]~[9]	- Keys used for numeric input.
[F1]~[F3]	- Keys used for changing the authentication mode.
[F4] or [←]	<ul style="list-style-type: none"> - Used for changing the authentication mode. - Used as the Delete key for correction when numerics are input. - Used for cancelling input, and moving to a parent menu in menu mode,
[F4(←)~]	<ul style="list-style-type: none"> - Means press the [F4 (←)] key for 2 seconds or longer. - When input cursor is located in the input box, it cancels the input and exits to the parent menu if pressed and held for 2 seconds or longer.
ENT [or MENU]	<ul style="list-style-type: none"> - Used for modifying the mode. - Used for saving the values set in menu mode, or moving to the screen configuration.
[ENT~]	<ul style="list-style-type: none"> - Means press the [ENT] key for 2 seconds or longer. - Used for accessing the menu when pressed on the initial screen - When input cursor is located in the input box, the user can exit to the parent menu with the current input value saved by pressing the button for 2 seconds or longer.

	- Used to apply the configuration to the current screen in menu mode and then exiting 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 authorised.
When authentication has failed	Please try again.

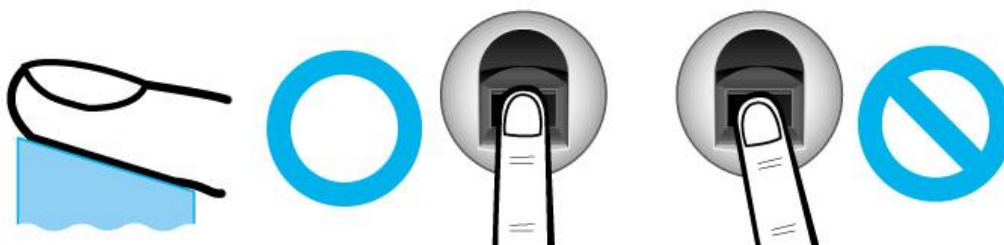
1.7. Buzzer Sounds Used During Operation

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 their finger off.
Be peep	Sound of failure	When authentication has 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.
Beeeeeep	Success	When succeeding in authentication or completing the settings.

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 your fingerprint with the fingertip touched lightly at input or registration. Make sure the centre of your fingerprint correctly touches the fingerprint input area.



- If possible input the fingerprint of your forefinger.

- It facilitates accurate and stable fingerprint input.
- Check to see if the fingerprint is clear and without any scars.
A too dry or wet fingerprint, ambiguous fingerprint, fingerprint with a scar, etc. may not be recognised. In such cases, use/register the print from a different finger.



- Precautions related to 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 a fingerprint recognition system. Any fingerprint that is damaged or thin may not be used. In such cases, the user should operate with a password.
- If a finger is in a dry condition, we advise breathing lightly on the finger for a smooth operation.
- For children, due to their small size and the tender properties of their fingerprints, it may be difficult or impossible to use their fingerprints. It is necessary to register their fingerprint at 6 monthly intervals.
- In cases of old people, excessive tiny lines existing on their fingerprints may prevent proper registration.
- It is recommended, if possible, to register at least 2 fingerprints from every user.

2. Product Introduction

2.1. Features

- **PoE and Terminal Block – Easy to install**
 - As PoE is supported, it can be installed with a LAN cable and doesn't need a separate power cable.
- **Designed to IP65 rainproof specification** – Outdoor installation is possible.
- **Slim and polished design**
 - Easy to install as it is designed as a standalone type; Slim and elegant design using Colour LCD and Touch Keys

● **Download Server Functions – Change the LCD background image and voice**

- Provides a variety of information messages via the colour LCD screen and voices. You can download background images and voice messages from the server; according to your preferences. Also, the built-in LCD Screen Backlight and Touch Key LED's allow the screen to be read and keys to be operated in dark conditions.

● **Convenient Auto Sensing Function**

- Enables easy authentication operations to be performed by inputting a fingerprint without separately entering a key.

● **Easy Fingerprint Self-Authentication**

- Prevents risks associated with forgetting a password, loss/theft of a card or key by using biometric fingerprint recognition technology; reinforces the security of self-authentication through the use of your own fingerprint.

● **Access Management System Using a Network (LAN)**

- Communication is carried out between the fingerprint recognition device and authentication server using TCP/IP protocol, and allows for easy expansion as it can be applied to the network as is. 10/100 Mbps Auto Detection ensures high-speed operation. Enables easy management and monitoring via the network.

● **Provides a Diverse and Flexible Access Management**

- Provides a perfect control function by granting entrance/access rights by user group.

● **Applicable for Various Operations such as, Access, Time & Attendance, Cafeteria, etc.**

- Enables a variety of operational methods depending on the settings in the terminal menu.

● **Abundant Server Capacity**

- The system allows an almost unlimited number of people to be managed by the server.

● **Provides a Variety of Registration and Authentication Methods**

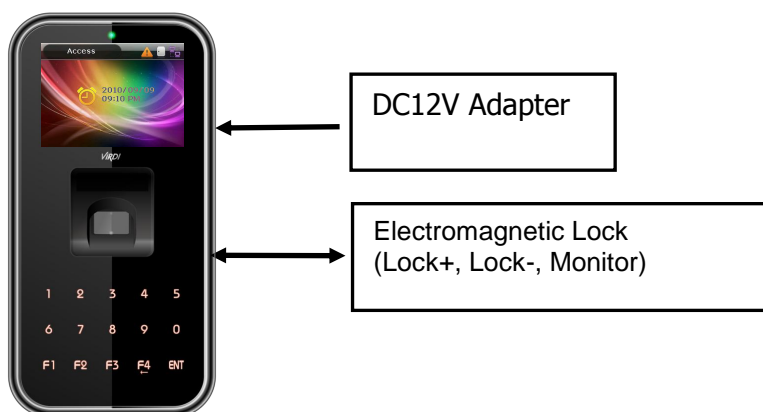
There are 12 registration and authentication methods for general use. Therefore, it's necessary to determine which registration and authentication method to use before registering a user or administrator.

FP	Fingerprint Registration Fingerprint Authentication
PW	Card Registration Card Authentication
FP or PW	Fingerprint and Password Registration Password Authentication when Fingerprint Authentication fails
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

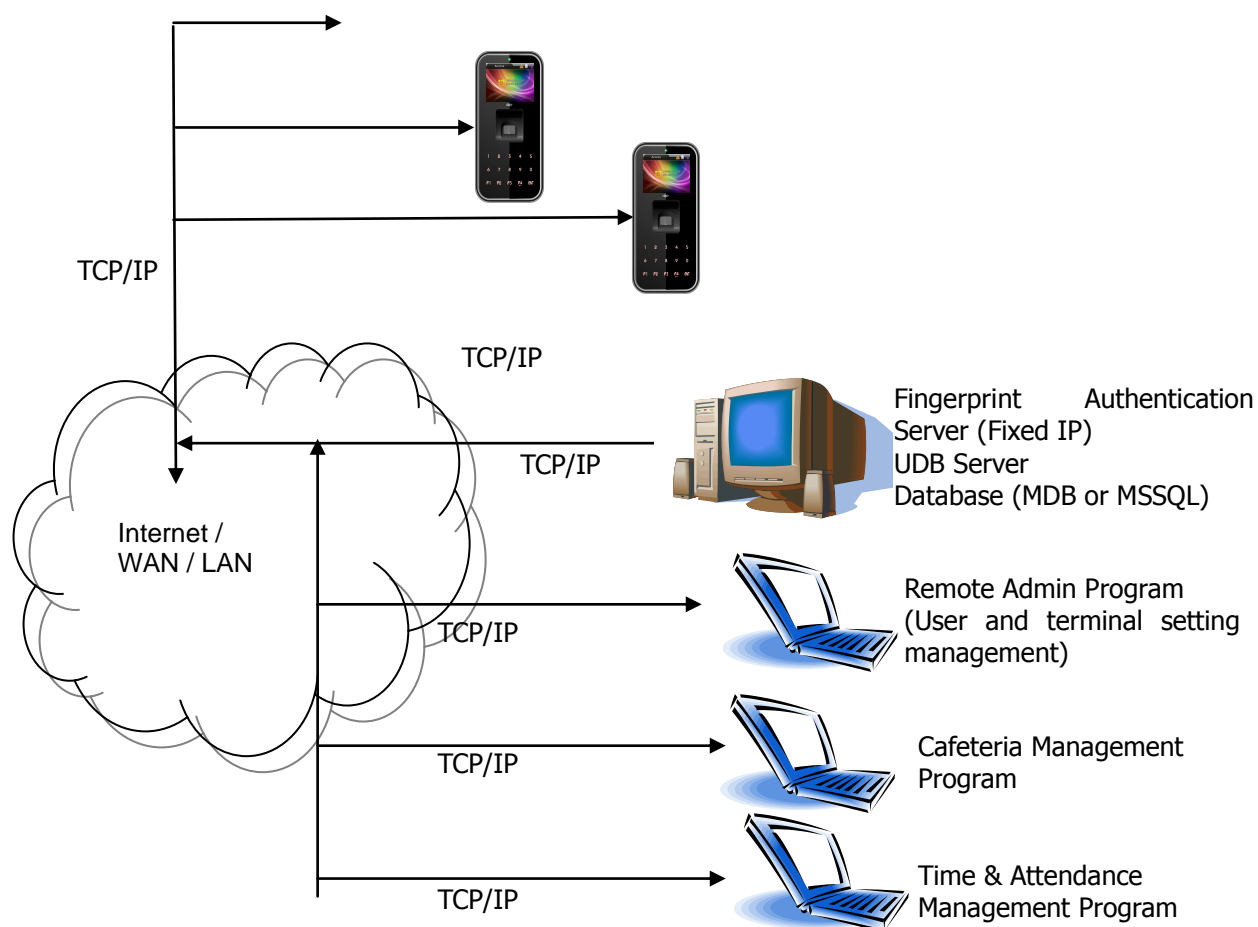
	Card Authentication and then Fingerprint Authentication
Card or PW	Card and Password Registration Card or Password Authentication
Card and PW	Card and Password Registration Card Authentication and then Password Authentication
(ID or Card) & FP	Card and Fingerprint Registration ID Input and then fingerprint 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

Item	Specification	Remarks
CPU	32-bit RISC CPU (400MHz)	
Environmental	IP65	
LCD Screen	2.8" TFT Colour (320*240)	
Touch Keys	15 keys (0~9, F1~F4, Enter)	
Memory	32M SDRAM	20,016 User 20,016 Finger 61,439 Log
	32M FLASH	
Fingerprint Sensor	Optical	
Authentication Speed	Less Than 1 Second	
Scan Area / Resolution	15 * 17mm / 500 DPI	

FRR / FAR	0.1% / 0.001%	
Temperature / Humidity	-20 °C ~ +50 °C Lower than 90% RH	
PoE	Supports 13W PoE	
AC / DC Adapter	INPUT: Universal AC 100 ~ 250V	Option DC 24V
	OUTPUT: DC 12V	
	UL, CSA, CE Approved	
Lock Control	EM, Strike, Motorised 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
Dimensions	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 the [ENT] key and hold for two seconds or longer. The user can now access the screen for menu selection, as follows:



<Figure 3-1>

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



<Figure 3-2>

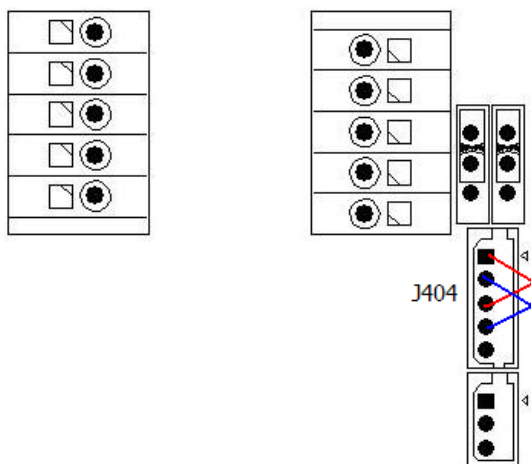
In adherence with the registered authentication method, such as card, fingerprint or password, users can access each menu - subject to successful identification - after the admin verification has finished.

- ▶ Verify Admin appears only if there is a registered Admin User. When accessing menu mode, after being identified, the user is allowed to access all the menus until they completely exit from the main menu.

3.1.2. How to access the menu without the Admin verification.

This is the way to access the menu if fingerprint authentication is impossible, or because the user forgot the admin password, or lost the card registered on the terminal, or there is no Admin.

- ① Remove the bracket on the rear of the terminal to open the lid.
- ② With the lid open, as shown in the figure below, connect pin 1 to pin 3, and pin 2 to pin 4 of connector J404.



<Figure 3-3>

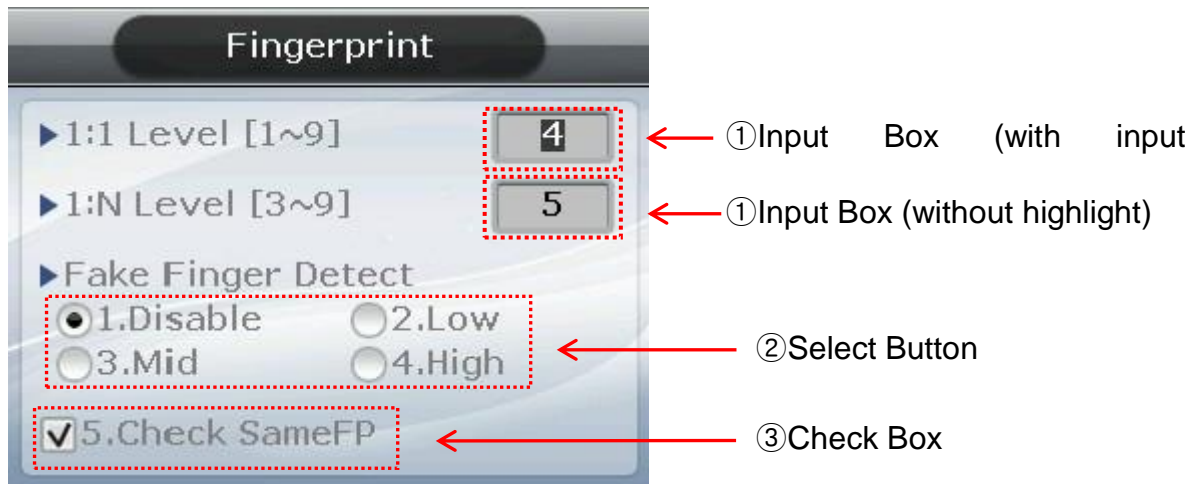
- ③ Access the Configuration Menu by pressing and holding the [F4(←)] key for 2 seconds or longer. Go to 1. User and Verify Admin screen <Figure 3-2> will be shown. Fill the Admin ID with '0000' and press the [ENT] key. The user can now

access the Menu and delete the admin or delete all users.

- ▶ After modifying the configuration, remember to remove the wires from the connected pins on the J404 connector.

3.1.3. Modify Set Values

The following are the names and input methods for setting items.
<Figure 3-4>



▶ ① Input Box

For items where the value is directly input, such as the '1:1 Level', users must delete the existing value using the [F4 (←)] key when the applicable item is highlighted. Then input the new value using the [0] ~ [9] keys.

▶ ② Select Button

For items such as 'Fake Finger Detect', the user should modify the selection (●) by pressing the relevant numeric key, provided the item is first highlighted. Move the highlighting in the input box by pressing the [ENT] key - if the highlight is located in the input box as shown in <Figure 3-5>.

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



As shown in the figure on the left, the number is displayed in reverse colour when the highlight is in the input box. In the figure on the right, the applicable letters are displayed in black instead of grey when the highlight moves to 'Fake Finger Detect'.

▶ ③ Check Box

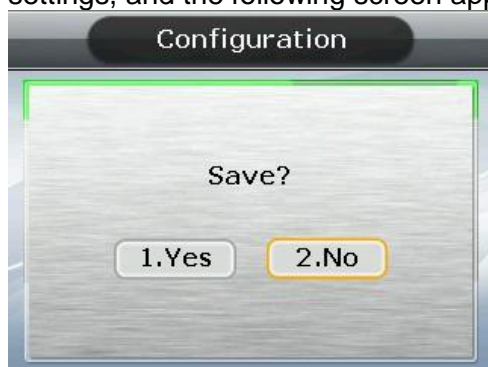
The user must select whether or not to check 'Check SameFP'. The user can either

select (✓) or release it (□) by pressing the relevant key [5]. It's impossible to select this item, if it's displayed as (✗).

Press the [F4 (←)] key to cancel, while setting, and move back to the parent menu. When the highlight is located at the input box the [F4 (←)] key functions as a [DEL] key, which deletes figures one by one. Press the [F4 (←)] key for two seconds, or longer, to cancel input and exit to the parent menu. Press the [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 the [F4 (←)] key in the main menu screen of <Figure 3-1> to save the changed settings, and the following screen appears:






<Figure 3-6>


Select [1.Yes] to save the new configuration or [2.No] to cancel it. Then press the [ENT] key. In this instance, if, after a period of time there is no input the system returns to the initial screen.



- If there is no new content, the system exits from the environment settings menu without the aforementioned "Save" process.
- When the settings are changed in the menu, and if there is no input after a certain period of time, the system exits from the environment setting menu. In which case, if there is any revised menu, it should pass through the "Save" process. Otherwise, it transfers to the initial screen without saving the revised settings.

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	<ul style="list-style-type: none"> ▶ F1 Time ▶ F2 Time ▶ F3 Time ▶ F4 Time ▶ Access Time <input type="checkbox"/> NO Limit (when setting to catering management)
	3. Function Key	<ul style="list-style-type: none"> <input type="checkbox"/> F1 Enabled <input type="checkbox"/> F2 Enabled <input type="checkbox"/> F3 Enabled <input type="checkbox"/> F4 Enabled <input type="checkbox"/> Ent Enabled <input type="checkbox"/> Auto Sensing
	4. Extended Key	<ul style="list-style-type: none"> <input type="checkbox"/> Extended Key ▶ of Extended Key
	5. Display	<ul style="list-style-type: none"> ▶ Background ▶ Clock Position <input type="checkbox"/> User Voice <input type="checkbox"/> User Text

4. System 	1. System Setting	<ul style="list-style-type: none"> ▶ UserID Length ▶ Display Option
	2. Authentication	<ul style="list-style-type: none"> ▶ User GroupIP ▶ Enable 1:N ▶ Card Only ▶ Template On Card ▶ Verify Multi-FP ▶ Blocking Time (sec.)
	3. Fingerprint	<ul style="list-style-type: none"> ▶ 1:1 Level [1~9] ▶ 1:N Level [3~9] ▶ Fake Finger Detect <input type="checkbox"/> Check SameFP
	4. Language	
	5. Data Time	<ul style="list-style-type: none"> ▶ Time Sync ▶ Display Time ▶ Set Current Time
	6. Database	<ol style="list-style-type: none"> 1. Init Config 2. Delete All Users 3. Clear Log Data 4. Initialise Terminal

5. Terminal 	1. Terminal Option	<input type="checkbox"/> Terminal Alarm <input type="checkbox"/> Lock Terminal <input type="checkbox"/> KeyLed ON
	2. Volume Control	▶ Voice Volume ▶ Beeper Volume
	3. Door	▶ Lock Type ▶ Door Monitor ▶ Open Duration ▶ Warn Door Open
	4. Wiegand	<input type="checkbox"/> 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, and the following screen appears:



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

3.3. 1. Add

◆ Select [ENT~] → [1. User] → [1. Add] ◆ in the basic screen, and the following screen appears:



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

Automatically shows the ID to be registered on the screen, so the user can easily perform registration. To modify the ID, press the [F4 (←)] key and delete the existing value and input the new value.

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



The icon on the left mean, as shown 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 registers 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 as user or admin. Once the registration is complete, the user can press [ENT] to save it. The user must press the [F4 (←)] key to cancel the registration and exit from the menu.

※ Only a user registered as Admin can modify the operating environment of the terminal, and Add/Modify/Delete the information about all users saved in the terminal. Therefore, special care is required when registering Admin.

3.3.1.1. Auth Type



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

3.3.1.2. FP Register



① **Place finger on the sensor** - refer to '1.8. How to register and enter fingerprint'. Fingerprint must be input twice, as below, in conjunction with the on screen guidance.

When the fingerprint sensor is lit and the message "Place Finger on sensor" is displayed, place a finger on the window for fingerprint input - for 2~3 seconds - until the light goes off.



② When the message 'Place same Finger on sensor' is displayed, enter the fingerprint input once again.

※ When entering the fingerprint for the second time, make sure the user has taken their finger off the fingerprint input window after the first read.



③ When input is complete the message at the left appears, together with the images accompanied by their quality rating from 0~100.

If the image is not adequate from a visual aspect, or any image shows 30 or less, the user is advised to register again.

To register again, start the process from step ① by pressing [F4 (←)] key until 3 seconds elapse without input or pressing another key. After completion, the system moves to the parent menu.

※ Fingerprint registration is available for up to 10 per ID. A failure message appears when registration is attempted in excess of 10 times.

If repeated failure is observed after 2~3 attempts when 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 the [F4 (←)] key.

3.3.1.4. PW Register



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

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



3.3.1.5. FP Option

This is the setting related to fingerprints, and 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 failure buzzer sound.



► '1:1 Level' (Initial setting: '0')

Is the item that determines the authentication level for each registered user. By modifying this value, it is possible to determine the authentication level per registered user.

When set to '0', it conducts authentication using the 1:1 authentication level of the terminal.






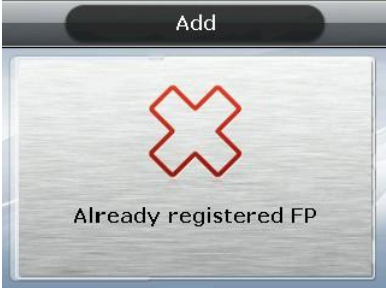
► Enable 1:N (Initial setting: 'v')


When this option is checked, it's possible to successfully authenticate using a fingerprint without any user ID or card.

3.3.1.6. Save

When the registration process is complete, press the [6] key to save it. The user settings are not saved if the user doesn't press [6] key and exits by pressing the [F4 (←)] key.

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

 <p>The screen shows a green checkmark icon and the text 'Registration Completed'.</p>	<p>When registered normally with [6. Save] key pressed.</p>
 <p>The screen shows a red 'X' icon and the text 'Registration Failed'.</p>	<p>When registration failed after [6. Save] key pressed.</p> <p>Means the user is not registered properly in accordance with the authentication method. For example, the user didn't register any fingerprint after setting it as the authentication method, nor registered a card after setting it as the authentication method.</p>
 <p>The screen shows a red 'X' icon and the text 'Fingerprint registration failed !'.</p>	<p>In the case of [2. FP Register]</p> <p>When fingerprint image is not in a good condition or there is no fingerprint input within 10 seconds of the fingerprint sensor lamp being on.</p> <p>At the time of fingerprint registration, when the user didn't input the same finger, but input a different finger.</p>
 <p>The screen shows a red 'X' icon and the text 'Password registration failed'.</p>	<p>In the case of [4. PW Register]</p> <p>When the user inputs a different number during password confirmation.</p>
 <p>The screen shows a red 'X' icon and the text 'Already registered card'.</p>	<p>In the case of [3. Card Register]</p> <p>When the user tried to register a card that has already been registered.</p>
 <p>The screen shows a red 'X' icon and the text 'Already registered FP'.</p>	<p>In case of [2. FP Register], when the user tried to register a fingerprint that has already been registered.</p> <p>※ If the user wants to register the same fingerprint with another ID again, they must the release '4. System → 3. Fingerprint → Check SameFP' function. This is, however, not suitable for Time & Attendance as the same fingerprints could be authenticated with</p>

	different ID's.
	<p>In case of [2. FP Register] or [3. Card Register]</p> <p>When the user attempted registration in excess of the maximum number of allowed registrations (10 each).</p>

3.3.2. Delete

Select ♦ [ENT~] → [1. User] → [2. Delete] in the initial screen ♦, and the following screen appears:



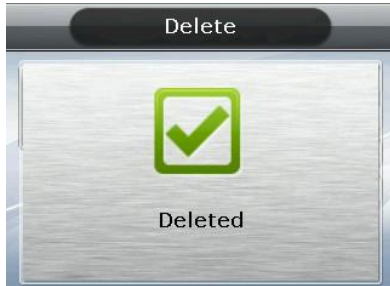
Input the user ID to be deleted, and then press the [ENT] key.

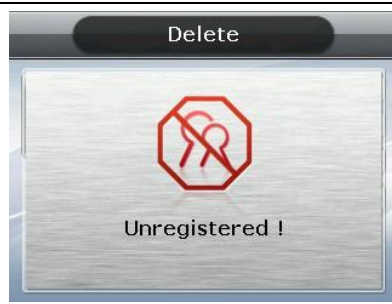
When inputting an unregistered ID, a failure message will appear. When inputting a registered ID, a success message will appear.

Deleting from the terminal doesn't mean deletion from the server. Therefore, it is necessary to delete from the server to make the deletion complete.

Special care should be taken when deleting, since deletion is performed regardless of User/Admin. In particular, the user registered in the terminal may not be restored after deletion unless registered on the network server.

The following are the LCD information messages that appear during the deletion process:

	When deleted normally.
---	------------------------



When the user inputs an unregistered ID.

3.3.3. Modify

Select ◆ [ENT~] → [1. User] → [3. Modify] in the initial screen ◆, and the following screen appears:



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

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



The icons on the left are described with 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 method of changing, see '3.3.1. Add' as it is the same as shown in the registration method.

3.3.4. Delete All

Select **◆** [ENT~] → [1. User] → [4. Delete All] in the initial screen **◆**, and the following screen appears:



If the user is sure they want to delete all users, press [1.Yes] and press [ENT] key. Select [2.No] to cancel.

※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

Select “2. Network” in the main menu, and the following screen appears:



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

3.4.1. IP

Select **◆** [ENT~] → [2. Network] → [1. IP] in the initial screen **◆**, and the following screen appears:



When changing IP, delete the existing values using [F4 (←)] and then input the new values. The ‘.’ in between the number sequence is created automatically. Example: input 192 168 010 50 sequentially to input ‘192.168.10.50’.

Select [1] when a fixed IP address is assigned to the connected network and select [2] in cases where there is a DHCP server in the connected network which is assigning the address. Set IP, Subnet Mask, and Gateway if it is a fixed IP. There’s no need to set the address if the user selected a flexible IP address.

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

after finishing the settings, or use the [F4 (←)] key to cancel input during setting. In this case, the user can only exit by pressing the key for 2 seconds or longer if they are inputting value in the input box.

3.4.2. Server IP

Select ♦ [ENT~] → [2. Network] → [1. Server IP] in the initial screen ♦, and the following screen appears:



Set the Server IP and Port.

To change the port, move the input highlight to the server port by pressing the [ENT] key.

- ▶ Initial Setting
Server Port: '9870'

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

You can, after finishing setting and to apply the new value, exit to the parent menu by pressing the [ENT~] key. Pressing the [F4 (←)~] key cancels the input value.

3.4.3. Terminal ID

Select ♦ [ENT~] [2. Network] [3. Terminal ID] on the initial screen ♦, and the following screen appears:



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 as a maximum of 8 digits.

► Authentication

This determines the priority for authentication between terminal and the network server. Having '2. Terminal/Server' as its default value, operation is as follows in each mode:

1.Server/Terminal	Authentication is made by the server when it's connected to the network, and by the terminal when it is disconnected from the server due to network disturbance, etc.
2.Terminal/Server	Authentication is made by the terminal, even if the server is connected, and authentication result 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 via the server. Therefore, authentication cannot be performed unless the server is connected.
4. Terminal Only	Only users registered in the terminal are authenticated. When connected to the server, the authentication results are 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 network errors etc. It is recommended to use '2. Terminal/Server' so concurrent authentications can be attempted if 10> terminals are connected to the server, or if frequent network errors occur.

3.5. Application

Selecting '3. Application' in the main menu causes the following screen to appear:



Press the applicable key representing the item to be changed.

3.5.1. Application

Select ◆ [ENT~] → [3. Application] → [1. Application] in the initial screen ◆, and the following screen appears:



Select the terminal operation type by pressing the applicable numeric key.

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

3.5.2. Time Schedule

3.5.2.1. Setting to Access / Time & Attendance

Select ◆ [ENT~] → [3. Application] → [2. Time Schedule] in the initial screen ◆, and the following screen appears:



► Initial setting: Identical with the screen on the left.

The user can set the time period for authentication mode; otherwise, set to '00:00-00:00'.

Input after deleting the existing value using [F4 (←)] to change the value.

Input HHMM (Hour/Minute) in order - can be set from 00:00 to 23:59

In a preset time period, it's always shown in the preset mode unless the user presses another function key. Although the user pressed the other function key to authenticate with another mode the terminal display mode automatically changes to authentication mode, which is suitable for the management of time & attendance.

As shown in the example below, each time period must be set without overlapping; the mode is determined F1→F2→F3→F4→Access sequentially if they do overlap.

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



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

3.5.2.2. . Setting to Cafeteria



► Initial setting: Identical with the screen on the left.

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

► NO Limit

Clear the check box (☐) , and each user is allowed one authentication by meal only. If you check the box (☒) they are allowed several authentications regardless of the existing authentication.

3.5.3. Function Key

Select ♦ [ENT~] → [3. Application] → [3. Function Key] in the initial screen ♦ , and the following screen appears:



► Initial setting: Identical with the screen on the left.

Function key refers to the keys [F1]~[F4], [ENT] & [Auto Sensing] used to change the authentication mode, such as office start/office leave etc. If you press a function key the authentication mode changes to the applicable mode. When a box is not checked, authentication mode does not change even if the applicable key is pressed.

If the '6.Auto Sensing' check box is cleared the fingerprint sensor doesn't respond, even if the user inputs their 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

Select ♦ [ENT~] → [3. Application] → [4. Extended Key] in the initial screen ♦ , and the following screen appears:

,

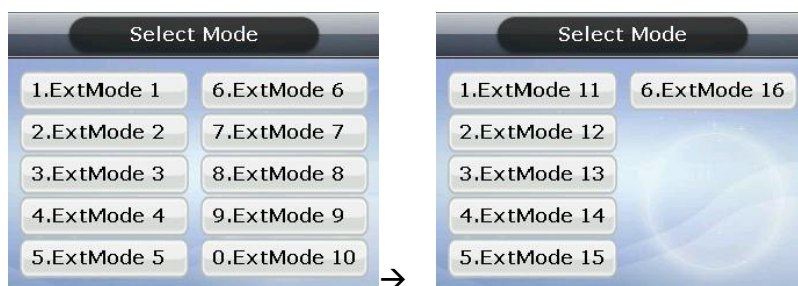


► Initial setting: Identical with the screen on the left

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

Extended Key is a function which extends the number of additional authentication modes (up to 40 as required) in addition to the basic function keys ([F1]~[F4], [ENT]). The screen for selecting the extended keys, when the user presses the F4 key, is shown below. Select the applicable mode with [0]~[9] keys. If the number of extended keys exceeds 10, select them by changing the page with the [F1]~[F4] keys.

Example: If the number of the extended keys is 16, press [F4] key in the initial screen, and the following screen appears



If you want to select ExtMode 12, move to the next page with the [F2] key and then press the [2] key.

Press the [ENT] key to exit without selecting an ExtMode.

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

3.5.5. Display

Select ◆ [ENT~] → [3. Application] → [5. Display] on the initial screen ◆, and the following screen appears:



► Initial setting: Identical with the screen on the left

► Background image

You can change the background image shown on the initial screen by pressing the [1] and [2] keys. Also, you 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 need/preference, you can download a voice from a Wav file (16bit/8KHz) to change the voice output when authentication is successful or has failed. Additionally, you 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 only when the boxes of '6. User Voice' and '7. User Text' are checked. For the download method, see '3.9.Download customised file'

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

3.6. System

Selecting '4. System' in the main menu causes the following screen to appear:



Press the applicable key representing the item to be changed.

3.6.1. System Setting

Select ◆ [ENT~] → [4. System] → [1. System Setting] in the initial screen ◆, and the following screen appears:



► Initial setting: Identical with the screen on 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 to 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 long.

► 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.

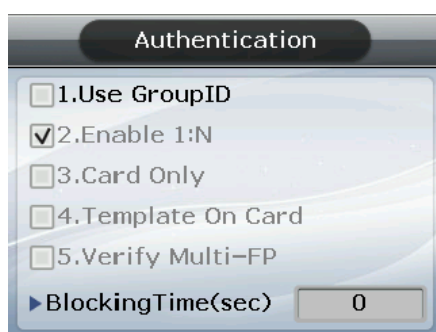
However, it indicates the ID in case there is no applicable information of the user saved in the terminal.

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

3.6.2. Authentication

Select ◆ [ENT~] ([4. System] [2. Authentication]) in the initial screen ◆, and the following screen appears:

► Initial setting: Identical with the screen on the left



► User GroupID

The method of authentication where the initial digit of an ID relates to a group. It completes 1:N authentication faster when more than 5,000 users are registered.

When this method is checked, it authenticates the fingerprint from users whose ID starts with the same 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

Example: Where the user inputs '12' to attempt authentication when the user ID is a 4-digit figure;

If checked (☒) , 1:N authentication is attempted from users having ID '1200'~'1299',

If unchecked (☐) , 1:1 authentication is attempted from fingerprints of users whose ID is '12'.

► Enable 1:N

If checked (☒) , this option enables fingerprint only authentication 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 card only authentication 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 authentication 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 and the server must set which terminal uses that 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 checked, the user must, without fail, input user ID or card. In this case, Enable 1:N is automatically changed to unchecked (☐) .

This function is used for strict access control to special zones. For example, if the user with ID '0001' is registered with 3 fingerprints they must input ID and complete the authentication for three fingerprints.

In this case, the order of authentication for the 3 fingerprints is irrelevant, but the fingerprints should be repeatedly input until authentication is successful. Authentication will fail on a single occurrence of authentication failure.

► Blocking Time (sec)

This function prevents duplicate authentication for the same user within the preset time period. 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 the [ENT~] key to apply the changed values. Use the [F4 (←)] key to cancel input during setting.

3.6.3. Fingerprint

Select ♦ [ENT~] → [4. System] → [3. Fingerprint] in the initial screen ♦ , and the following screen appears:



► Initial setting: Identical with the screen on the left.

► 1:1 Level

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

► Fake Finger Detect

It presets LFD level to prevent imitation fingerprint input. Pre-setting the LFD level to a higher value tends to reinforce the function, preventing the input of imitation

fingerprints produced with rubber, paper, film, silicone, etc. But when inputting a real fingerprint, it may not read well.

► Check SameFP

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

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

3.6.4. Language

Select ◆ [ENT~] → [4. System] → [4. Language] in the initial screen ◆, and the following screen appears:



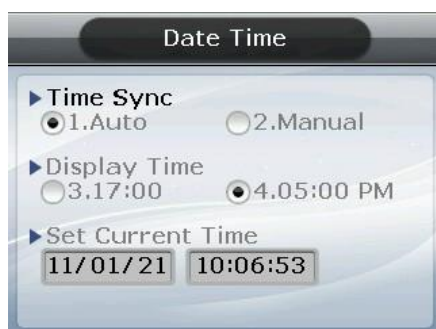
► Initial setting: '1. English'

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

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

3.6.5. Date Time

Select ◆ [ENT~] → [4. System] → [5. Date Time] in the initial screen ◆, and the following screen appears:



► Initial setting: Identical with the screen on the left.

► Time Sync

Sets the method which synchronises the current time of the terminal with the server. To synchronise the terminal time with the server time, set to '1. Auto' to perform it automatically, while '2. Manual' is for manual setting.

► Display Time

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

► Set Current Time

Changes the current time of the terminal. No change is required if it's synchronised and linked with the server time and with the aforementioned Time Sync set to '1. Auto'.

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

3.6.6. Database

Select ◆ [ENT~] → [4. System] → [6. Database] in the initial screen ◆, and the following screen appears:



Press the following keys:

[1] key to initialise the configuration.

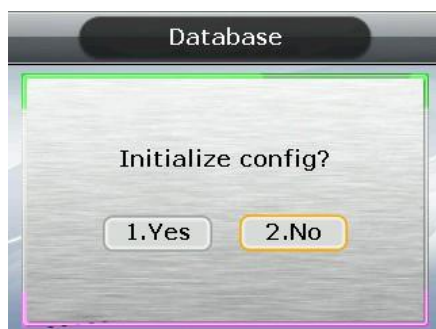
[2] key to delete all users.

[3] key to initialise the authentication record.

and [4] key to initialise the terminal.

3.6.6.1 Init Config

Select ◆ [ENT~] → [4. System] → [6. Database] → [1. Init Config] in the initial screen ◆, and the following screen appears:



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

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

Initialises 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 initialised, it proceeds to the parent menu accompanied by the success buzzer sound.

3.6.6.2. Delete All Users

Select ◆ [ENT~] → [4. System] → [6. Database] → [2. Delete All Users] in the initial screen ◆, and the following screen appears:



Press the [1.Yes] key to delete all users, or select [2.No] and press the [ENT] key to cancel.

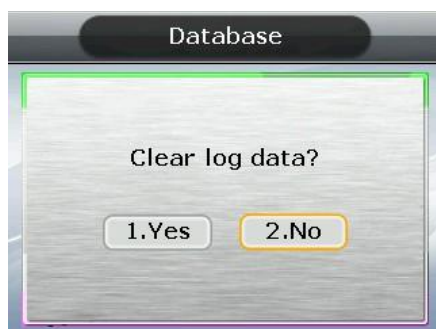
If no value is input for a certain period of time in this state, it returns to the initial screen instead of deleting.

Both user and administrator are deleted, and the deleted users cannot be restored after deletion.

When deletion is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sound.

3.6.6.3. Clear Log Data

Select ♦ [ENT~] → [4. System] → [6. Database] → [3. Clear Log Data] in the initial screen ♦, and the following screen appears:



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

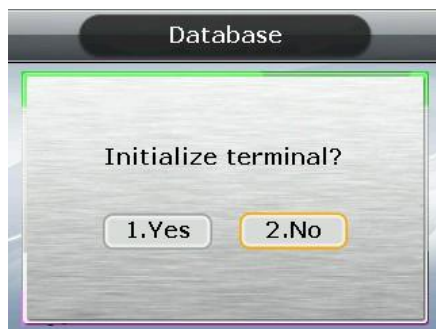
If no value is input for a certain period of time in this state, it returns to the initial screen instead of deleting.

Deletes all logs related to authentication, and the deleted logs cannot be restored after deletion.

When deletion is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sound.

3.6.6.4. Initialise Terminal

Select ♦ [ENT~] → [4. System] → [6. Database] → [4. Initialise Terminal] in the initial screen ♦, and the following screen appears:



Press the [1.Yes] key to initialise the terminal to the factory default state, or select [2.No] and press the [ENT] key to cancel.

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

Deletes all the configurations, users, and log information, except MAC (physical) address saved in the terminal, restoring them to factory default state. Special care should be taken as restoration is impossible after initialisation.

When initialisation to the factory default state is successfully completed, it proceeds to the parent menu accompanied by the success buzzer sound.

3.7. Terminal

Selecting '5. Terminal' in the main menu causes the following screen to appear:



Press the applicable key representing the item to be changed.

3.7.1. Terminal Option

Select ♦ [ENT~] → [5. Terminal] → [1. Terminal Option] in the initial screen ♦, and the following screen appears:



► Initial setting: Identical with the screen on the left

► Door open

Door opens when the '0' key is pressed. Appears only when the terminal is locked. This option is not normally shown.

► Tamper Alarm

If checked, (☑), a warning sound is generated when the lid of the terminal is opened.

► Lock Terminal

This is the function the administrator can directly set or release the locking of the

terminal via the terminal rather than server program. If checked (☒) , it is locked so no one can access until the administrator releases the setting.

► KeyLed ON

If checked (☒) , Key LED is always turned ON so the Touch Keys are visible.

► Door open

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

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

3.7.2. Volume Control

Select ♦ [ENT~] → [5. Terminal] → [2. Volume Control] in the initial screen ♦ , and the following screen appears:



► Initial setting: Identical with the screen on 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 the [ENT~] key to apply the changed values. Use the [F4 (←)] key to cancel input during setting.

3.7.3. Door

Select ♦ [ENT~] → [5. Terminal] → [3. Door] in the initial screen ♦ , and the following screen appears:



► Initial setting: Identical with the screen on the left.

► Lock Type

Set to '1' when strike type or automatic door is connected to the terminal, or '2' when

motorised lock is connected to the terminal. If no connection is made, it is set to '1'. Set to '3' when connecting a 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 or automatic door (when lock monitoring is open and the door is locked).
- '2.Normal Close': In the case of Strike (when lock monitoring is locked and the door is locked).

► Open Duration (0.1 sec unit)

Designates the time the door is opened and closed again when authentication is successful. As it is set to 0.1 second per 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 function enables the terminal to check the time the door opens, and generate 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. If set between 01~04, it only starts sounding after 5 seconds have elapsed.

The warning sound is also generated in cases where the door is unexpectedly not closed within the preset time; although the door should be closed. This warning allows proper action to be taken for the door to be closed.

To use this function, the lock must be the one that enables the monitoring of the door door status, and the monitoring pin of the lock should be connected to the terminal. 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 the [ENT~] key to apply the changed values. Use the [F4 (←)] key to cancel input during setting.

3.7.4. Wiegand

Select [ENT~] → [5. Terminal] → [4. Wiegand] in the initial screen ◆, and the following screen appears:



► Initial setting: Identical with the screen on the left

This menu configures the Wiegand Output.

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:

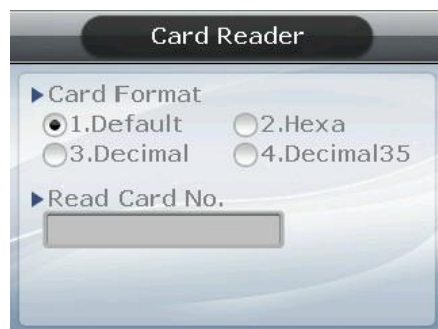
2.None	This is the normal case. Wiegand Output is not used.
3.26bit	Transmits "Sitecode[1byte] + user ID[2byte]", so the user ID is set to 4 digits or less. Example: For SiteCode:045(2Dh), UID:6543(198Fh), is transmitted as '1 00101101 0001 1001 10001111 0'
4.34bit	Transmits "Sitecode[1byte] + user ID[3byte]" 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), is transmitted as '0 00000001 00000001 11100010 01000000 0'
5.Custom	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 Inport at the time when authentication was successful to the Wiegand Output as it is.

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

3.7.5. Card Reader

Select [ENT~] → [5. Terminal] → [5. Card Reader] in the initial screen ◆, and the following screen appears.



► Initial setting: Identical with the screen on the left.

► Read Card No.

When the user puts the card on the screen, the card number is displayed on the LCD.

► Card Format

This is the menu that sets the way the card number is displayed. 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

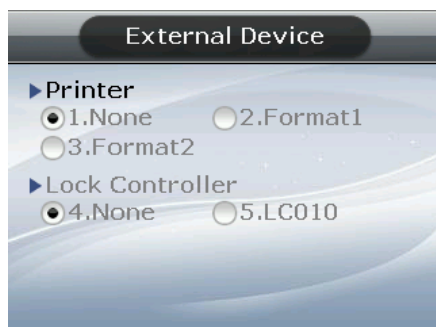
Card Format	Card Number	Method of Expression
1. Default	529D06E3	Expressed as an 8-digit hexadecimal number
2. Hexadecimal number	E3069D52	Expressed as an 8-digit hexadecimal number changing the order of byte
3. Decimal number	1386022627	Hexadecimal number 529D06E3 to be expressed as a 10-digit decimal number
4. Decimal number 35	3808861522	Hexadecimal number E3069D52 to be expressed as a 10-digit decimal number

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

3.7.6. External Device

Select [ENT~] ([5. Terminal] [6. External Device]) in the initial screen ◆, and the following screen appears.

► Initial setting: Identical with the screen on 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 is "SRP-350" Serial type.

► Lock Controller

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

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

3.8. Information

Select '6. Information' in the main menu and the following screen appears:



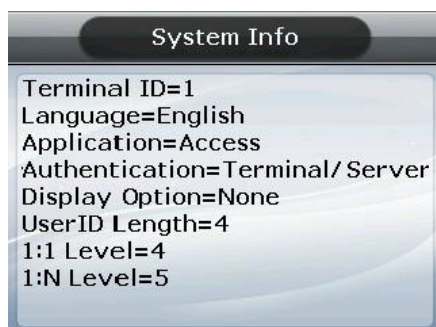
Menu to view the terminal settings.

Press;

- [1] key to view various terminal configurations.
- [2] key to view network configuration, such as IP.
- [3] key to view the user registration status, etc.
- [4] key to view log data.
- [5] key to view firmware version.

3.8.1. System Info

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



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

3.8.4. View Log

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

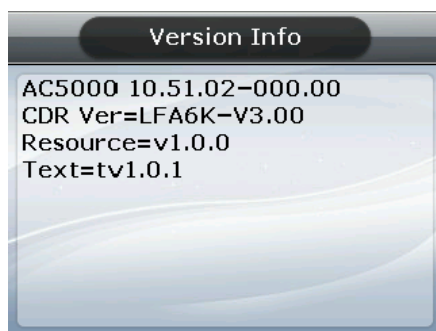


- All Log: Number of logs saved in the terminal.
- Max Log: Maximum number of logs that can be saved.

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

3.8.5. Version Info

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



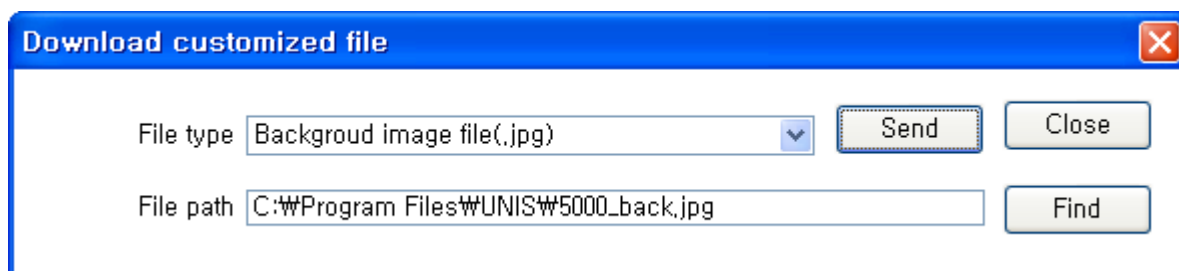
Press the [F4 (←)] key to exit to the parent menu.

3.9. Downloading User's File

This function allows the user to change background image or voice message. User files can be downloaded from UNIS server program.

3.9.1. Change Background Image

When selecting 'Download customised file' in the UNIS program, the following screen appears:



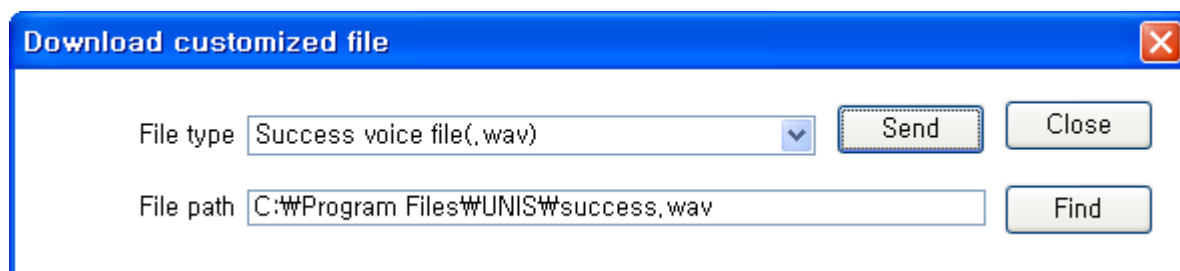
Designate the file as 'Background image file (.jpg)', select the image file (.jpg), and click the 'Send' button. The terminal select window will appear. Select the terminal on the terminal list window and click the 'Send' button again. The file will be transmitted with the downloaded result displayed.

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

To change the background image, you can directly select it from '3.5.5 Display'.

3.9.2. Change Voice Message

When selecting 'Download customised file' in UNIS program, the following screen appears:



Designate the file as 'Success voice file (.wav)', select Wav file (.wav) and click the 'Send' button. The terminal select window will appear. Select the terminal from the terminal list window and click the 'Send' button again. The file is transmitted with the downloaded result displayed.

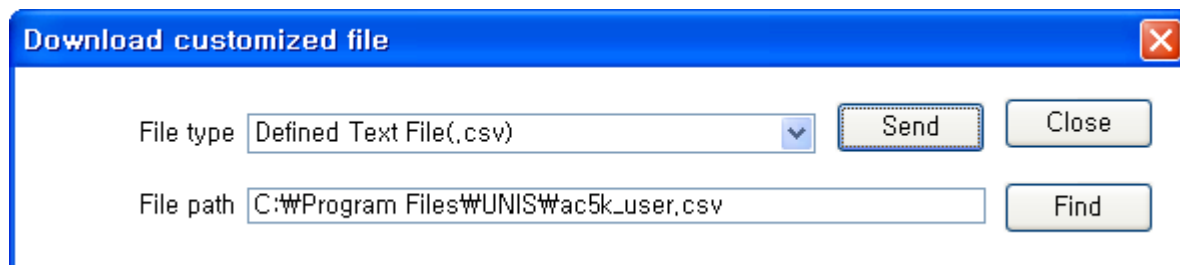
The file name can be up to 15 characters, including the extension name, with the Wav file in 8KHz 16-bit mono form only. If any data in a different format is downloaded, the transmission result will be displayed as a version error.

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

To change the user's defined voice into the 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 customised file' in UNIS program, the following screen appears:

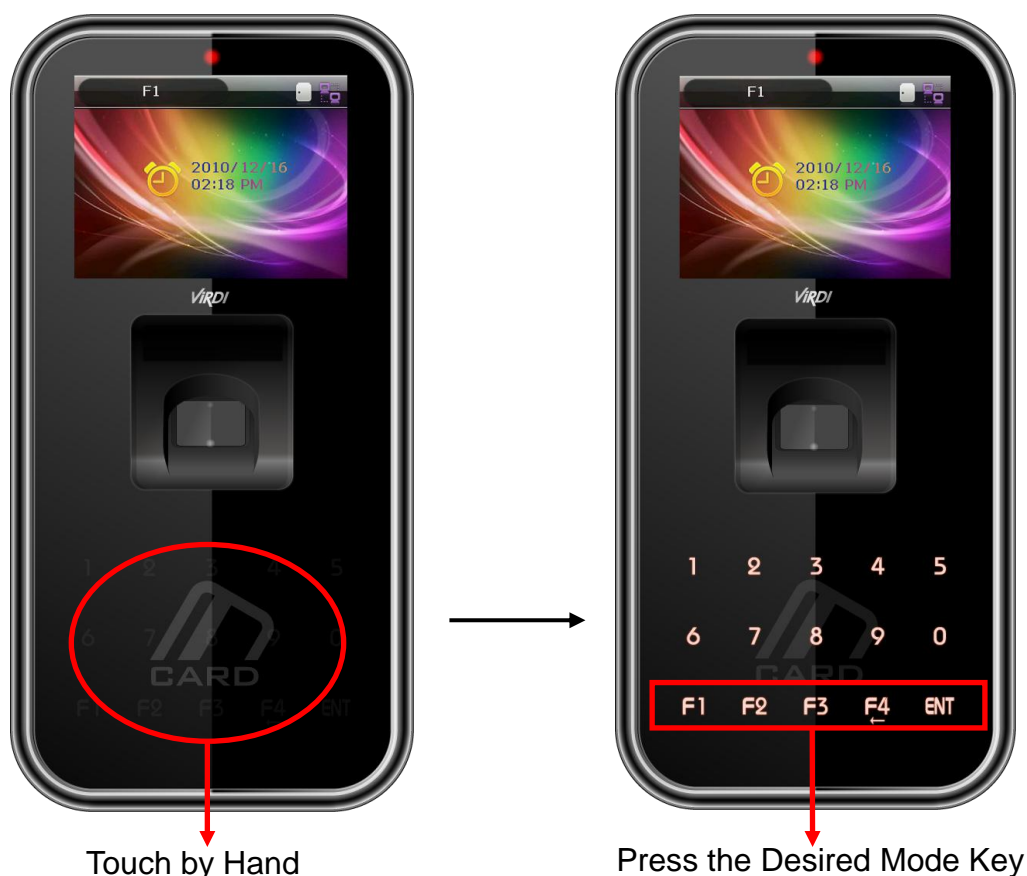


Designate the file as 'Defined Text File (.csv)', select CSV file (.csv) and click the 'Send' button. The terminal select window will appear. Select the terminal from the terminal list window and click the 'Send' button again. The file is transmitted with the downloaded result displayed.

CSV file can be created and saved as a csv file type after changing the desired text in the Excel (.xls) file provided with the terminal firmware. To change 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 the Terminal

4.1. Change of Authentication Mode

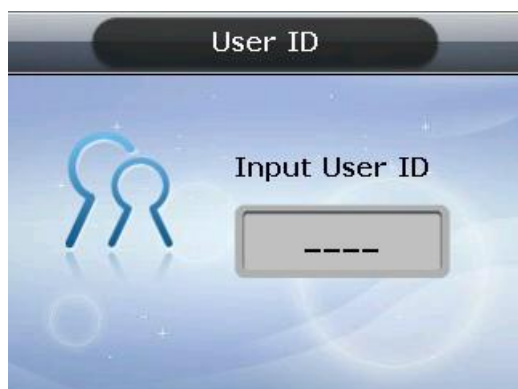


<Figure 4-1>

Normally it's not visible, but when the user touches their hand on the card input area - as shown in the Figure at the left – the LED's are powered ON and the keypad appears - as shown in the Figure at the right. When the keys are visible, press the desired function key to change 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's not visible, but as shown in Figure <4-1>, when the user touches their hand on the card input area, the LED's are powered ON and the keypad appears. In this case, ID input screen appears when the user inputs their ID.



Delete with the [F4 (←)] key if a figure is wrongly input during the input process. Pressing the [ENT] key, after inputting ID, causes the fingerprint input or password input screen to appear; 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 a fingerprint on the sensor, a buzzer sounds with the sensor lamp ON, and the fingerprint is duly input. Be sure not to take your 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 the [ENT] key which causes the fingerprint sensor to flicker. Then input the fingerprint via the 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 the [ENT] key after inputting ID, and the screen for password input appears. When a wrong number is input, delete it using the [F4 (←)] key. Input the password and press the [ENT] key.