Fingerprint Access Controller

FINGKEY ACCESS

User Guide

NITGEN
biometric solutions

`

- Unauthorized reproduction of part or all of this manual’s content in any form is prohibited.
- Product specifications may change without prior notice to improve functionality.
- NITGEN&COMPANY the NITGEN logo are registered trademarks of NITGEN.&COMPANY
- Other names and trademarks belong to respective companies.
- The font used in this product is Naver’s “Nanum”.

NITGEN&COMPANY Customer Service Center

Tel: +82.2.513.2150
Fax: +82.2.513.2191
Email: customer@nitgen.com

NITGEN&COMPANY

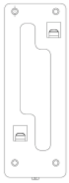
Table of Contents

Chapter 1 Getting Started

Product Component

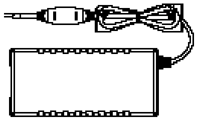
The FingkeyAccess^{TM} includes the following components. For detailed information about installation, see the installation guide. If any of the following items is missing, contact the Customer Support Team.

Terminal



Installation Bracket

Power Cord

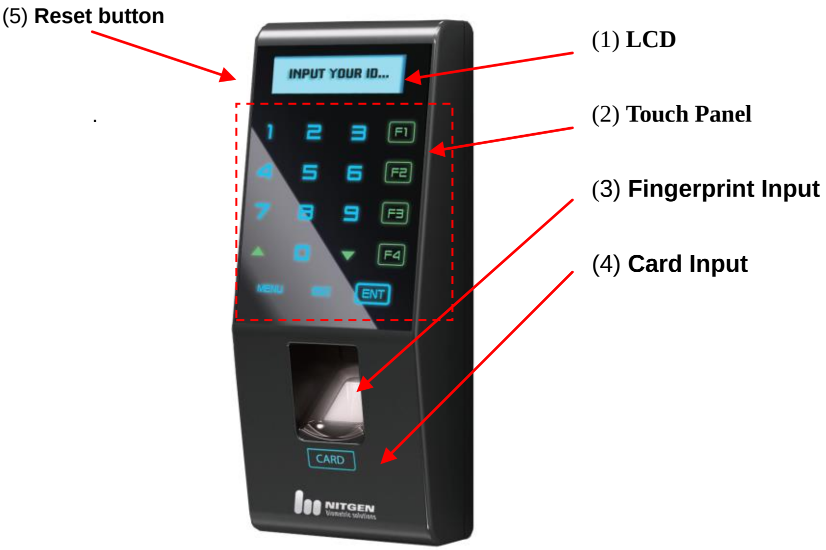


Adapter

Bolts

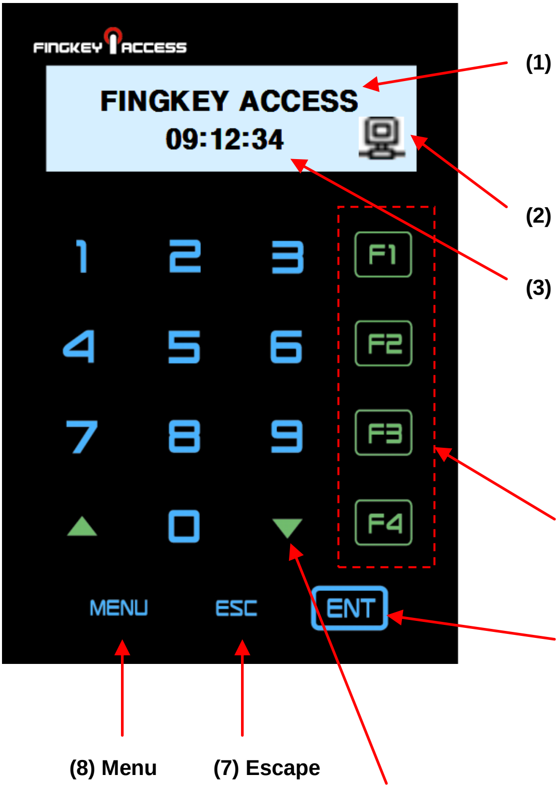
Software CD

Product Description



No.	Name	Description
1	LCD	The user can get information from it
2	Touch Panel	The user can handle all inputs by touching.
3	Fingerprint Input	The user places his/her finger for authentication.
4	Card Input	The user places his/her card for authentication.
5	Reset Button	The user can make the system reset manually.

LCD Display & Touch Pads



(1) Initial message

(2) Network connection status

(3) Time: Displays the present

(4) Function Keys

(5) ENTER Key

(8) Menu

(7) Escape

(6) Cursor Key

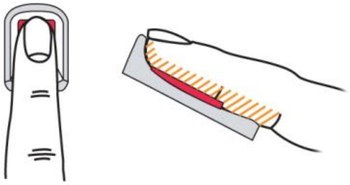
Fingerprint Reading

Scan fingerprints as described below for fingerprint registration and authentication to prevent authentication errors.

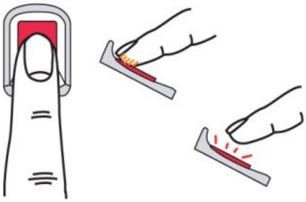
① Maximize the finger area scanned and press evenly (70 ~ 80% of full pressure).

② Place the “core” of the fingerprint at the center of the scanner. The core is usually opposite the whitish half-moon on the bottom of the fingernail. Therefore, place the half-moon part at the center of the scanner when scanning.

○ Correct



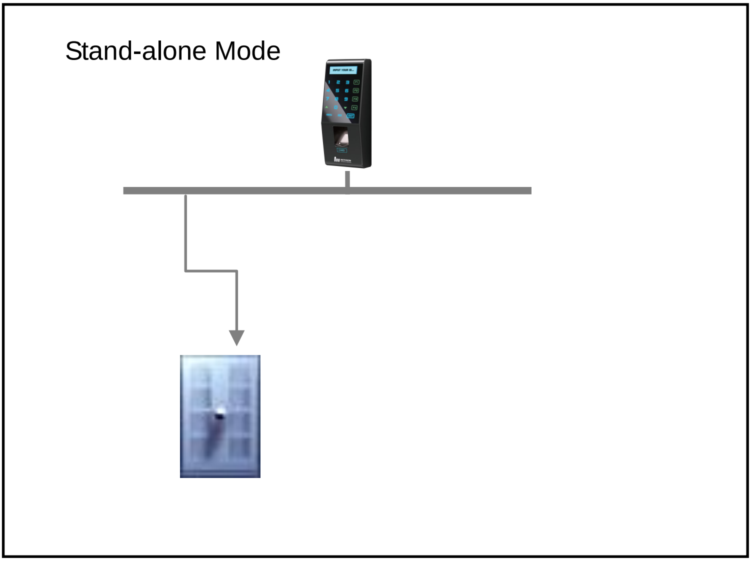
○ Incorrect

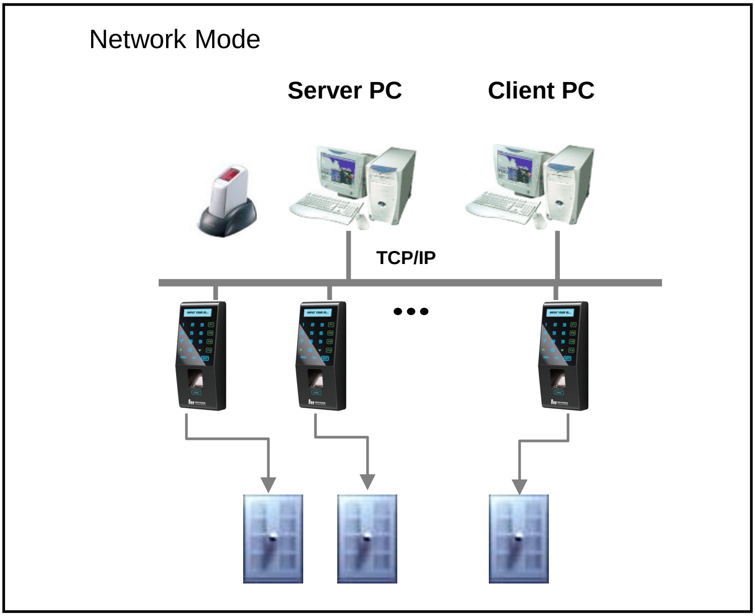


System Configuration

The Access Control Terminal (FingkeyAccess^{TM}) can function either in the network or stand-alone mode. In stand-alone mode, all functions are available and the terminal does not need to be connected to the network. In network mode, multiple terminals are connected to the server through TCP/IP links and the terminals can be managed by the administrator.

To use FingkeyAccess^{TM} in network mode, a server and a management program (AccessManager Professional) must be installed.





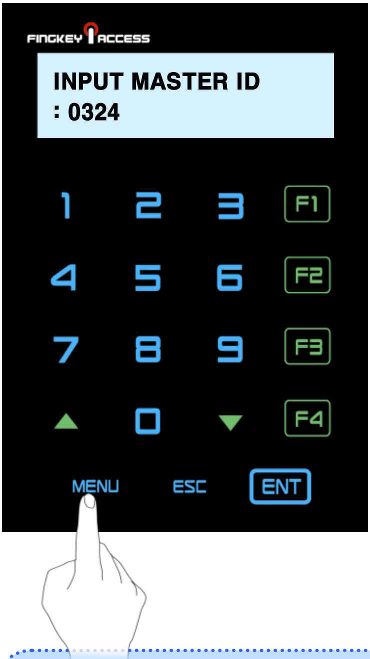
Item	Functions
Server PC	1. Server S/W : AccessManager Professional 2. Terminal management, communication and log data collection 3. User profile and log data DB 4. Authentication
Client PC	1. Client S/W: AccessManager 2. User registration and management 3. Terminal status and event monitoring
Terminal	1. User registration, modification, deletion and checking 2. Warning/Alarm handling 3. Door control

Chapter 2

Administrator menu

Entering Administrator Menu

Terminal users include general users and administrators. General users are only allowed to open the door while the administrator can use the Administrator menu to control the door as well as the terminal's functions.



1. To enter the Administrator menu, touch the "MENU" button at the lower of the touch pad.

2. Input the administrator ID and follow the authentication process. The Administrator menu will be displayed. Because no users have yet been registered, any user can enter the Administrator menu. At least one administrator for should be registered for security purposes.

1. If no administrator was designated and only general users were registered in network mode, all users will be allowed to enter the Management menu.
2. If 1:N authentication is used, an administrator with a registered fingerprint can enter the Administrator menu using fingerprint authentication without entering his ID.

The Administrator menu has seven submenus as shown below.
The following describes each sub menu:

Higher menu		Detailed Menu		Sub menu	
1	User Management	1	User registration		
		2	User info change		
		3	User deletion		
		4	Deletion of all users		
2	Fingerprint sensor setting	1	Security level	1	1:1 mode
				2	1:N mode (Please try menu 3 times after setting number 1)
		2	Capture mode		
		3	Time setting for fingerprint input		
		4	AUTO-ON setting		
		5	1:N time setting	1	Whether to use 1:N time setting or not
				2	Time setting (“time setting” possible only when it is on)
		6	FreeScan		
3	UI setting	1	Language		
		2	Audio		
		3	Button tone		
		4	Function Key Display	Off/Mode1/Mode2	

		5	Menu Timeout		
		6	LCD BL Timeout		
		7	Backlight level		
4	System Setting	1	Log storing		
		2	RF card	1	Off
				2	HID
				3	MIFARE
				4	EM
		3	WIEGAND	1	OFF
				2	26BIT
				3	34BIT
				4	40BIT
		4	Function key setting	Auto T&A / Muti T&A	
		5	Authentication mode		
		6	Time setting		
		7	Terminal mode		
		8	Time zone		
5	Network	1	Terminal ID		
		2	TCP/IP	1	DHCP yes or no?
				2	Terminal IP
				3	Sebnet Mask
				4	Gateway
				5	Server IP
		3	Time limit		
		4	Port setting		
6	Information	1	Number of users		
		2	Firmware version		
7	Factory default	1	DB Format		

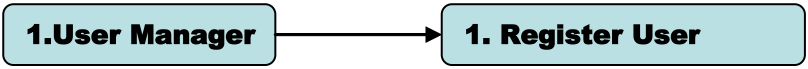
		2	Factory format	
		3	Number of registered fingerprints	
		4	Number of characters in ID	
		5	Reset terminal	

User Management

The administrator can register, delete and change users with the User menu.

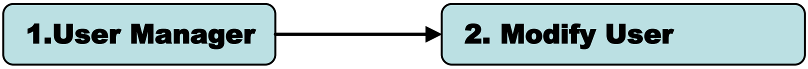
User Registration

The maximum number of users that can be registered is the 20,000 templates. (10,000 uesrs)



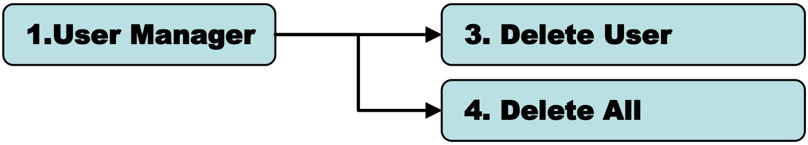
User Change

User IDs are unique and cannot be changed. However, group, privilege, fingerprint, and authentication type can be changed in the "Modify" menu. Users can only be changed in stand-alone mode. In network mode, the server management program must be used to change users.



User Deletion

In network mode, the User menu does not support deletion of certain or all users. The administrator can only delete all users registered at a certain terminal by selecting "Reset → User Data."



Fingerprint Sensor Setting

Settings related to fingerprint sensor options such as security level, fingerprint capture time, capture mode, LFD precision, and sensor brightness can be configured.

Authentication Security Level

The security level is set according to the authentication method. The security level for 1:1 authentication is between 1 and 9, and the default is 5. The security level for 1:N authentication is between 5 and 9, and the default is 8. If the security level is too high, authentication failure rate may rise, and if it security level is too low, the misreading rate may rise. Therefore, the default level should be used. This level applies to all users except those who chose different security levels when registering.

2.FP → **1 Secu .**

Capture Mode

Set whether to distinguish fake fingerprints, to what degree of precision. “Low”, “High”, or “Not in Use” are available.

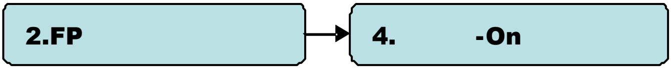
2.FP → **2. Capture**

Authentication Limit Time

The fingerprint input waiting time is between 3 and 9 seconds, and the default is 5 seconds.

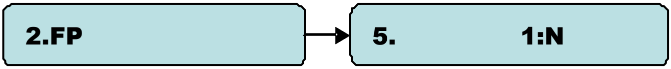
2.FP → **3. Sensor**

Auto-On Setting



1:N Authentication Time

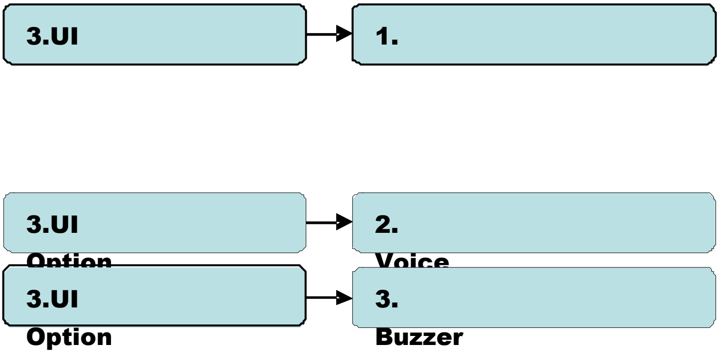
If 1:N authentication is being used, the time can be set during which all user fingerprints are searched. The input value can be between three to nine seconds, with the default being three seconds. If the search fails after the specified time, a “Matching timeout” error will occur.



UI & Sound Setting

Language and Buzzer

The user can change the language, buzzer.



3.UI → 1.

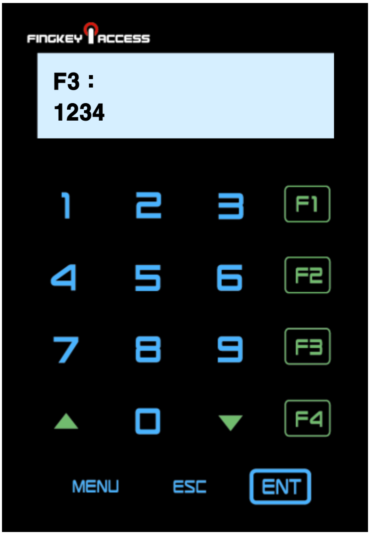
3.UI Option → 2. Voice

3.UI Option → 3. Buzzer

Function Key display mode

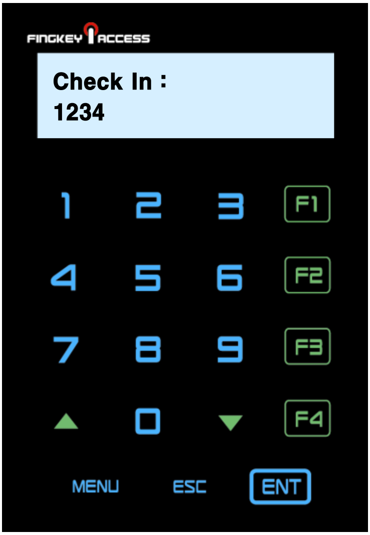
Based on this setting, the display for Function key will be showed differently. For example,

SETTING = OFF



F3 :
1234

SETTING = Mode2



Check In :
1234

The following table shows the message depending on the option of fucntion key display

Option	F1 KEY	F2 KEY	F3 KEY	F4 KEY
Off	F1	F2	F3	F4
Mode1	Clock In	Clock Out	Absense	Return
Mode2	Check In	Check Out	F3	F4

System Setting

Settings related to system such as log storing, RF card, Wiegand, Function key, time, terminal mode and timezone.

Saving Logs

The administrator can save logs that arise during user authentication. To save logs, select “Save Logs” and change “No” to “Yes.” The logs can be checked by selecting “Info” → “Log”, or by using the “AccessManager Professional” program.

4.System Option → **1. LOG**

Card

To use card authentication to authenticate users, do the following.
Select the card type – EM, MIFARE, HID

4.System Option → **2. RF Card**

Wiegand

4.System Option → **3. Wiegand**

It decides whether to use Wiegand communication protocol to send authentication results to a controller

When the result of authentication is succes, The FingkeyAccess™ terminal sends wiegand data as shown below table.

Terminal Mode	Off	None
	26 Bit	Parity(1)+ Facility(8) + ID (16) + Parity(1)
	34 Bit	Parity(1)+ Facility(16) + ID (16) + Parity(1)
	40 Bit	RFcard Site code (16) + RFID (16) + checksum(8)
Reader Mode	Off	None
	26 Bit	Parity(1bit) + 24bit Card CSN + Parity(1bit)
	34 Bit	Parity(1bit) + 32bit Card CSN + Parity(1bit)
	40 Bit	32bit Card CSN + checksum (8bit)

Time and Attendance mode

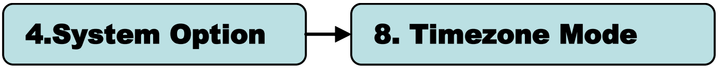
Time and attendance mode, the user must press a function key and perform the user authentication process when opening the door. The entry logs will be sent with the function key data to the server management program.

Depending on the function key, user attendance records can be classified into “Coming to work”, “Leaving work”, “Going out”, and “Returning” for efficient attendance management.

4.System Option → **4. Function Mode**

Time Zone

The “Time Zone” menu is used to restrict or allow entry or to select specific authentication type in terminal during certain time periods. Using this function, you can make timezone function enable or not. For more information, please refer to the Access manager pro user manual.



4.System Option → 8. Timezone Mode

Network Setting

The FingkeyAccess™ terminal can function either in network or stand-alone mode. Wireline networks are supported in the network mode. If the DHCP option is deactivated, the terminal IP, subnet mask, and gateway must be inputted manually. For more information, contact the service team.

Terminal ID

Enter a unique terminal ID between 1 and 2000. The same terminal ID cannot be used in the same server.

5.Network → **1. Terminal ID**

TCP/IP Setting

After selecting network mode, TCP/IP must be configured to connect to the server.

Press “on” in the “DHCP” menu to decide to use DHCP. When using DHCP, enter into the server IP and port information of the server with AccessManager Professional installed.

5.Network → **2. TCP/IP**

Time Limit

Don’t set this value too short.

5.Network → **3. N/W Timeout**

Port Setting

Enter the port number to be used for communication between the server and the terminal. The default value is “7332” and the user can choose between 2000 and 65535. When changing the port data in the terminal, change the communication setting of AccessManager Professional accordingly.

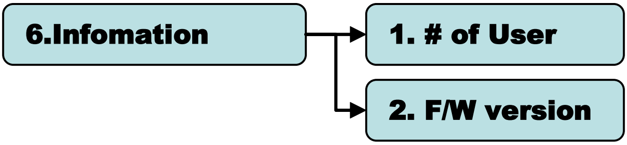
5.Network → **4. Port Setting**

What is DHCP (Dynamic Host Configuration Protocol)?

The DHCP server automatically allocates and manages settings for TCP/IP communication. If DHCP is on, related information such as terminal IP, subnet mask, and gateway are automatically allocated.

Terminal Information Display

The administrator can check the firmware version and number of users.



Factory Default

DB Format

All DB are formatted. When format is completed, the system goes back to the initial screen.

Factory Format

Factory Format is a command to restore all information stored within a terminal into initial values including user DB, option DB, log information and logo. Therefore, the function should be used with an extreme caution.

Fixed Option

In the “Fixed Option” menu, the number of fingerprint scans to be inputted during fingerprint registration and the ID length can be configured. These settings cannot be changed of registered users already exist. To change these settings, the administrator must delete all users registered at the terminal.

To change the number of fingerprint scans required for user fingerprint registration, select “Template Count” and input the number. The default is 2, and the administrator can choose 1 or 2.

Reset Terminal

Terminals can be reset without disassembling. Please choose 『yes』 in a confirmation screen to reset a terminal.

Chapter 3 General User

Door Opening

A user registered at the terminal can open the door in two ways depending on whether 1:N authentication is used.

1:1 Authentication

The user enters his ID and scans his fingerprint, and the scanned fingerprint is compared 1:1 to the registered fingerprint that matches the ID. This method allows for quick authentication.

In 1:1 authentication mode, the user presses “Authentication” on the lower left, and enters his ID. Then, the user continues the authentication process using the registered means – fingerprint, card, or password.

1:N Authentication

In 1:N authentication, the user does not need to input his ID. Instead, the scanned fingerprint is authenticated by searching all fingerprints in the DB. The process is simpler than 1:1 authentication, but if there are a lot of users, it may take more time.

① Fingerprint Authentication

The user is authenticated by scanning his fingerprint without entering his ID.

② Card Authentication

The user is authenticated only by scanning his card without entering his ID.

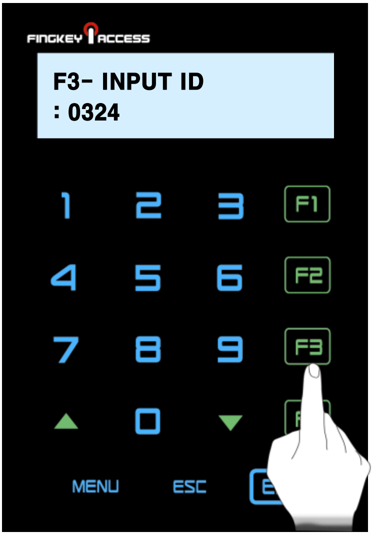
If 1:N authentication is not activated, the user will be asked to input his ID after he presses “Authentication” on the terminal.

In 1:N authentication, the password user is authenticated in the same ways as in 1:1 authentication.

Authentication in Attendance Mode

In attendance mode, all users shall press the functions keys in order to be authenticated. All logs are transmitted to the server. If the users Do not press function keys, the attendance types –coming to office, leaving office, leave, and return –may not be recorded so that the user shall press the function keys in order to be authenticated.

Using Attendance Mode

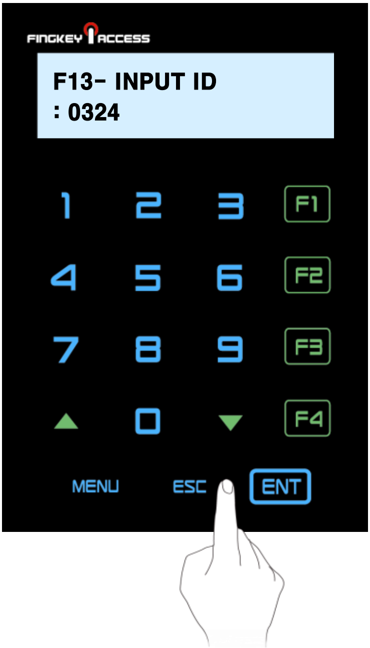


General/Simple

In attendance mode, function keys are displayed on the lower-right of the initial screen.

1. In Simple or General Attendance mode, the user must press a function key and input his ID to be authenticated. Function keys are as follows:
   F1: Coming to work
   F2: Leaving work
   F3: Going out
   F4: Returning

2. After the user presses a function key, the key will be included in the server log data which will be used by the attendance management program.



Using Extended Attendance Mode (Not available)

In Extended Attendance Mode, the initial main screen will be displayed as shown on the left.

1. Select a function key, and press arrow keys to change function number.

2. Enter the user ID and press “Enter” to authenticate.

To use 1:N authentication in attendance mode, enter the attendance key and perform authentication without inputting an ID.

Changing User Information

The administrator can change passwords, fingerprints, and card information of registered users using the terminal's Administrator menu or the server program. To change user information, contact the administrator.

Alphabet User ID

Use the left arrow key to input the alphabtet (LCD displays a "*"), and press key Code to use ther alphabet user id

Key Code	LCD Display	Key Code	LCD Display
*01	A	*02	B
*03	C	*04	D
*05	E	*06	F
*07	G	*08	H
*09	I	*10	J
*11	K	*12	L
*13	M	*14	N
*15	O	*16	P
*17	Q	*18	R
*19	S	*20	T
*21	U	*22	V
*23	W	*24	X
*25	Y	*26	Z

Appendix

Appendix

Troubleshooting

<If fingerprint authentication takes too long>

1. If the terminal uses 1:N authentication in network mode, server overload may occur, resulting in slow authentication and recognition. In this case, a dedicated server should be used.
2. Check if the finger and the sensor are clean. Clean the finger and the sensor. If the user's finger is hurt, the user must register another fingerprint.
3. If the fingerprint is not clean, lower the security level of the user and use the 1:1 authentication method.
4. Input the user's ID in 1:1 mode and check if the user exists.

<If fingerprint is not registered>

If the finger is too dry or humid, fingerprint image quality may be poor and may not register. Dry or moisturize the finger before registering the fingerprint.

<If RF card authentication fails>

1. Check your RF card type matches with the RF option of Terminal.

<If network connection cannot be established>

1. Check if the network setting is correct.
2. Check the TCP/IP setting.

   ① IP address of the server where AccessManager Professional is installed.
   ② The server and the terminal must use the same port.
   ④ Related settings if DHCP is not used.

3. Synchronize the terminal and the server settings.

<If the door does not open after authentication>

1. Check the time period during which access is allowed.
2. Check JP1 jumper status is correct. (refer to install guide)

<If users cannot be registered>

In default configuration, this product operates in network mode which requires a proper network connection for user registration. Check the network connection, or disable network mode to not use the network.

<If the product is unstable or does not function>

1. In the terminal by selecting "Menu" → "Reset" menu.
2. Restart the server if the server management program is in use.
3. If the terminal buttons do not function, restart the terminal by pushing external reset button located right side of terminal.
4. If the problem remains after the above actions are taken, contact the Customer Support Team.

Product Specifications

Item	Description
LCD	128*32 B/W Graphic STN
CPU	400MHz 32Bit RISC
Memory	64MB RAM, 32MB Nand Flash
Sensor	OPP06 Optical, 500DPI(LFD, Auto-On)
Authentication Rate	1:1 – Less than 1 second 1:N -
FAR/FRR	0.001% /0.1%
Number of users	10,000 Users (Two templates per user)
Communication Method	TCP/IP, RS-485, Wiegand
Dimensions	178(L) x 77(W) x 50(H) mm
Power	Input: AC 100V ~ 240V, 50/60 Hz Output: DC 12V, 3A
Door	Dead Bolt, Strike, EM Lock, Automatic Door, Fire Alarm
Temperature/Humidity	IP65 Class, -20 ~ 60℃
Supplementary Features	Buzzer announcement
Encryption	DES / AES

FCC Information

This device complies with part 15 of the FCC Results. Operation is subject to the following two conditions :

(1) This Device may not cause harmful interface, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for CLASS B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try correct the interference by one or more of the following measures:

1.1. Reorient or relocate the receiving antenna.

1.2. Increase the separation between the equipment and receiver.

1.3. Connect the equipment into an outlet on a circuit different from that to which receiver is connected.

1.4. Consult the dealer or experienced radio/TV technician for help.

WARNING

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

"CAUTION : Exposure to Radio Frequency Radiation.

Antenna shall be mounted in such a manner to minimize the potential for human contact during normal operation. The antenna should not be contacted during operation to avoid the possibility of exceeding the FCC radio frequency exposure limit.