UBio-X Face User Guide

Version Eng-1.1

UNION COMMUNITY

Copyright 2000 By UNIONCOMMUNITY Co., LTD.

<Revison History>

Version	Date	Description	Firmware Version
1.0	2020-04-17	Initial Release	0.0.0-61.00-000.01
1.1	2020-06-24	3.6.3 Add the option in Face recognition. - Face size, Multi Face Detection	0.0.0-61.00-000.06

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

<Glossary>

- Admin, Administrator
  - A user who can enter into the terminal menu mode, he/she can register/modify/delete terminal users and change the operating environment by changing settings.
  - If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
  - Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.

- 1 to 1 Verification
  - A user's verification fingerprint (template) is compared to the user's enrollment fingerprint (template) previously registered. The terminal performs 1:1 matches against the user's enrolled template until a match is found.
  - It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

- 1 to N Identification
  - The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
  - Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.

- Authentication level
  - Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
  - The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable 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 Face authentication, FP (fingerprint) authentication, RF (card) authentication or a combination of these methods.
    Example: Face or FP: Authentication with face or fingerprint

- 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.

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

Table of Contents

<Revison History> **2**
<Glossary> **3**
Table of Contents **4**
1. Before use **6**
1.1. Safety Precautions **6**
1.2. Specific names of the terminal **7**
1.3. Windows after operation **8**
1.3.1. Icon 8
1.3.2. Message 9
1.4. Voice sounds in operation **13**
1.5. Beep sound in operation **13**
1.6. How to register and authorize the face properly **13**
2. Product introduction **15**
2.1. Product characteristics **15**
2.2. Product components **17**
2.2.1. Standalone use (Access) 17
2.2.2. Connected with Server (Access, Attendance, Meal management) 17
2.3. Product specification **18**
3. Environment setting **19**
3.1. Checks before setting the environment **19**
3.1.1. Entering the menu 19
3.1.2. Administrator authentication 19
3.1.3. How to enter the menu without administrator authentication 20
3.1.4. How to save the set values 20
3.2. Menu composition **22**
3.3. User Management **25**
3.3.1. Add 25
3.3.1.1. Photo registration 27
3.3.1.2. Name registration 27
3.3.1.4. Face registration 28
3.3.1.5. Password registration 29
3.3.1.6. Card registration 30
3.3.1.7. Authentication option 30
3.3.1.8. Auth type 31
3.3.1.9. Save 31
3.3.2. Delete 32
3.3.3. Modify 33
3.3.4. Delete all 34
3.3.5. View 35
3.4. Network setting **36**
3.5. Application mode **39**
3.5.1. Application 39
3.5.1.1. Access or TnA setting 39
3.5.1.2. Meal setting 40
3.5.2. Function key 41
3.6. System **42**
3.6.1. System 42
3.6.2. Finger 43

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

3.6.3. Face 45
3.6.4. Auth 46
3.6.5. Date/Time 47
3.6.6. Database 48
3.6.6.1. Delete all the users 48
3.6.6.2. Delete setting 49
3.6.6.3. Delete Log 49
3.6.6.4. Delete image log 50
3.6.6.5. Factory init 50
3.7. Terminal 51
3.7.1. Sound 51
3.7.2. Option 52
3.7.3. Input 53
3.7.4. Lock 55
3.7.5. External Device 56
3.8. Display 58
3.8.1. Theme 58
3.8.2. Camera 59
3.8.3. Language 60
3.8.4. Option 61
3.8.5. Message display time 62
3.9. Terminal Info 63
3.9.1. System 63
3.9.2. Terminal 64
3.9.3. Network 65
3.9.4. User 66
3.9.5. Log 67
3.9.6. About 68
3.11. Download the user file 69
3.11.1. Change the voice message 69
4. How to use terminal 70
4.1. How to change Auth mode 70
4.2. How to input user ID 71
4.3. Authentication 71
4.3.1. Face authentication 71
4.3.2. Fingerprint authentication 72
4.3.3. Card authentication 73
4.3.4. Password authentication 73
4.3.5. Multi-mode authentication 74

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

1. Before use

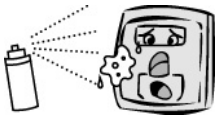
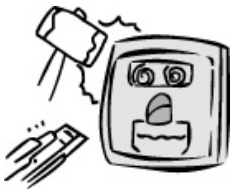
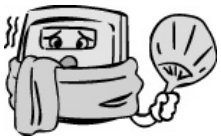
1.1. Safety Precautions

- Warning

Handling with wet hands or allowing liquid to flow into it is prohibited. -> It may cause an electric shock or damage.	Do not place a fire source near the terminal. -> It may cause a fire.
Do not disassemble, repair, or modify the terminal at discretion. -> It may cause an electric shock, fire or damage.	Keep out of reach of children. -> It may cause an accident or damage.

- If the above warning is ignored, it may result in death or serious injury.

- Cautions

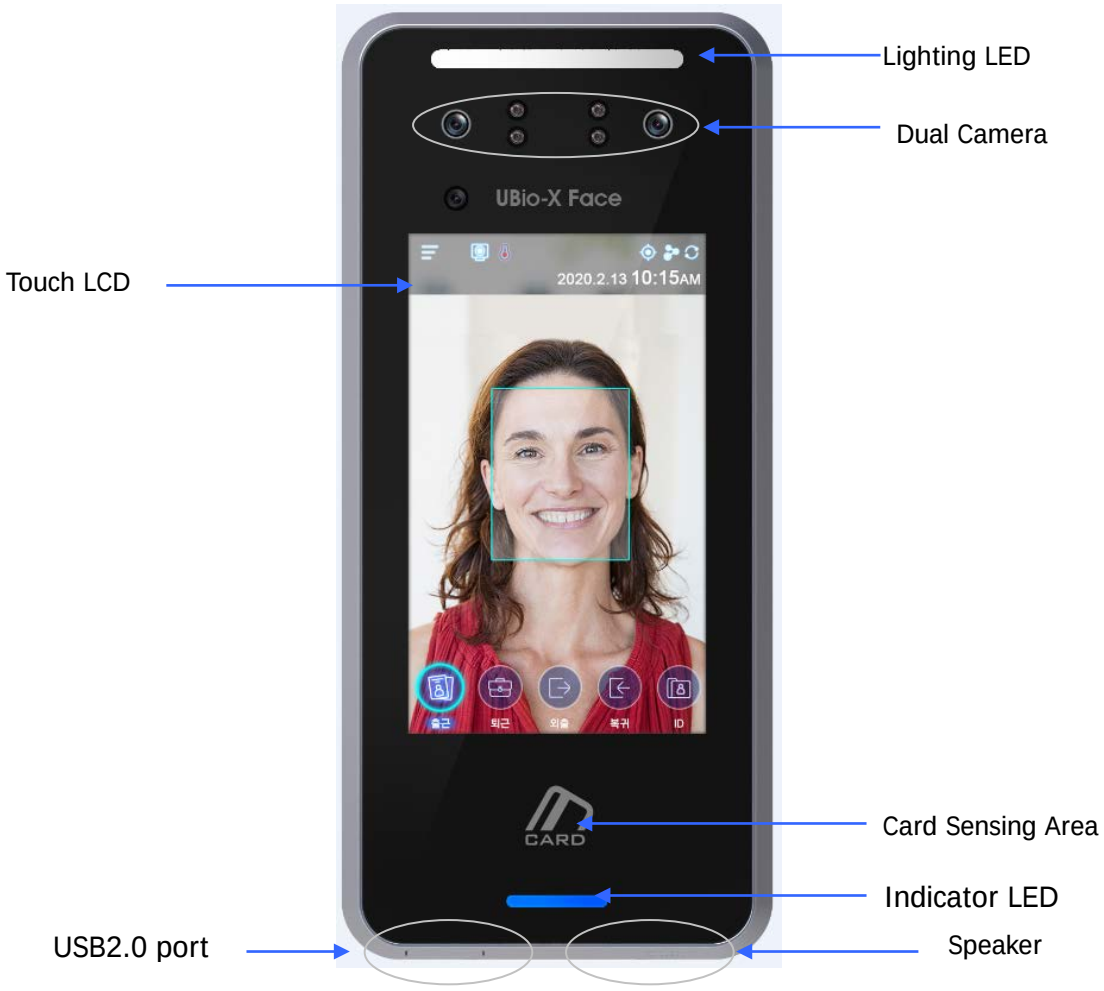
Keep away from direct sunlight -> It may cause deformation or color change.	Avoid high humidity or dust -> The terminal may be damaged.
Avoid using water, benzene, thinner, or alcohol for cleaning -> It may cause an electric shock or fire.	Do not place a magnet close to the terminal. -> The terminal may break down or malfunction.
Do not contaminate the fingerprint input area. -> Fingerprints may not be well recognized.	Avoid using insecticide or flammable spray near the terminal. -> It may result in deformation or color change. 
Avoid impacts or using sharp objects on the terminal. -> The terminal may be damaged and broken. 	Avoid severe temperature changes -> The terminal may be broken. 

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

※ Under no circumstances will UNION COMMUNITY be responsible for accidents or damages caused by inappropriate use of the product without referring to the user manual.

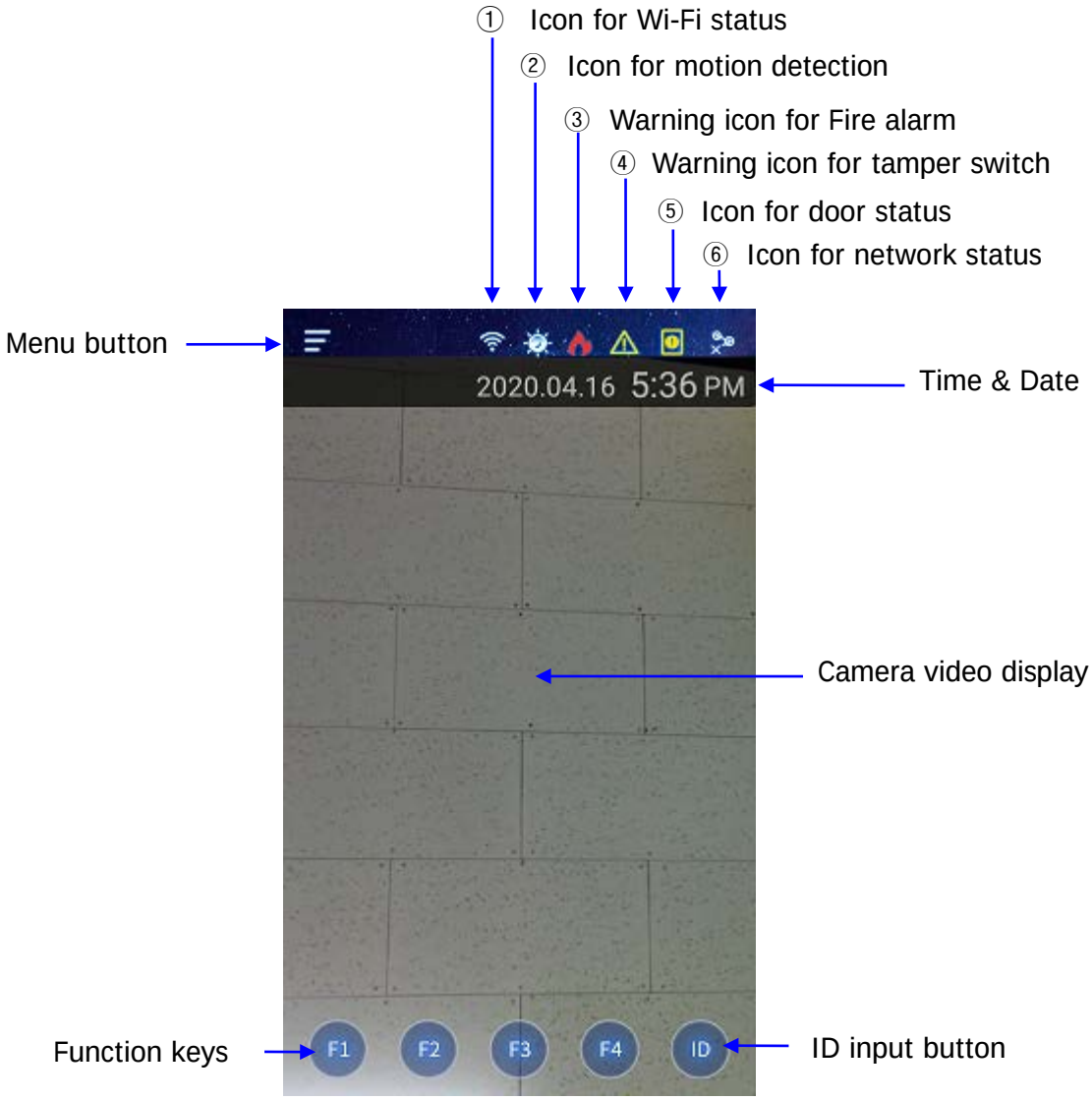
UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

1.2. Specific names of the terminal



UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

1.3. Windows after operation

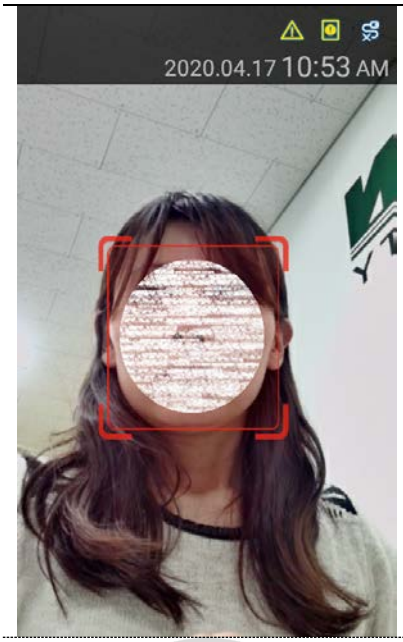
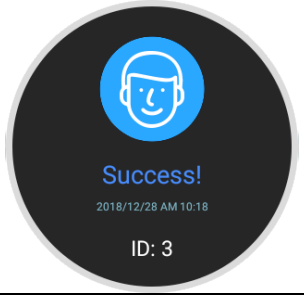


1.3.1. Icon

① Wi-Fi Status	None : There is no connected Wi-Fi dongle. : Wi-Fi connection is not activated : Wi-Fi connection is activated
② Illumination Detection	None : Detect the high illumination status. : Detect the low illumination status

③ Fire Alarm		: Fire Alarm is activated. (on connecting Fire detection sensor)
④ Tamper Switch	None	: Normal status
		: Tamper switch is activated. (Terminal is disassembled.)
⑤ Door Status		: Door status is not sensed.
		: Door is closed.
		: Door is opened.
		: Door is opened abnormally
⑥ Network status		: LAN cable is not connected.
		: Disconnected to the server even if LAN cable is connected.
		: Connected to the server. (Online)

1.3.2. Message

	- Basic Window
	- When authentication is successful

- When authentication is failed

- When unregistered user ID is entered

- When unregistered card is entered

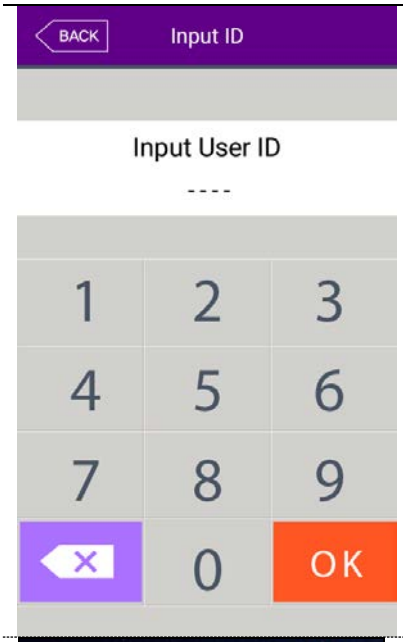
- Passback error when using anti-passback function

- When using for meal management
  When a user tried the authentication more than twice in one meal time when using as meal management

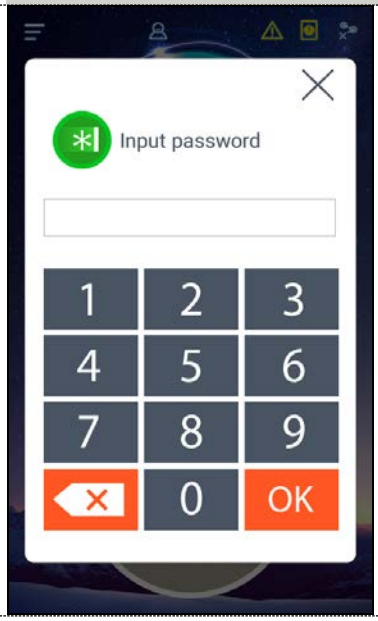
UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

	- When the server does not respond during the authentication attempt to the server - When the network is disconnected during the authentication attempt to the server
	- Registration without authentication right or authentication attempt when the entrance is not permitted
	- When the user is designated in the blacklist
	- When the terminal is set locked
	- When it is not the meal time when set in the meal personnel management

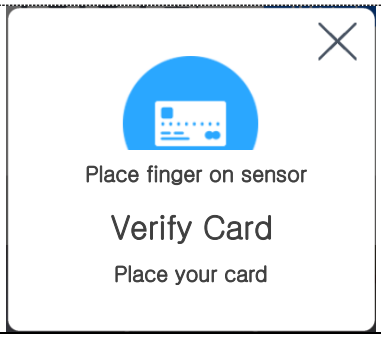
UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr



- The waiting status for the input of user ID



- The waiting status for the input of password



- The waiting status for the input of card

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu,
Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

	- When the terminal program is being upgraded (In this state, you should not turn off the terminal)

1.4. Voice sounds in operation

Operation type	Voice sound
Success to authorize	You are authorized.
Fail to authorize	Please try again.

1.5. Beep sound in operation

Pick	Notice for reading the card or fingerprint	When the card was read When the fingerprint was entered in the fingerprint window
Pi-pick	Notice for fail	When the authentication was failed (at Voice off)
Peek	Notice for Success	When the authentication was successful (at Voice off)

1.6. How to register and authorize the face properly

- Face registration method

  - Maintain the distance between the terminal and face in about 50 cm. (Locate the face in the guide line of LCD window.)
  - Register the face pose along with the guidance. During the shooting, please maintain the attention.
  - When registering the face, register after sweeping your hair up not to hide the eyebrow or lower face with your hair or hat. (On the stand of Passport picture).

- Face authentication method

  Just stare at the camera from the front.

- Notes

  - It is recommended to register and authorize at the location where the terminal is installed.
  - If you pose differently with the registered face, the recognition rate of face can decrease. It is good to locate the full face as much as possible

- The thick glasses frame or sun-glasses can decrease the recognition rate of face

- Cautions in the installation

  - Be sure to install the terminal indoor.
  - Do not install under the light bulb.
  - Not recommended in the circumstance of backlight or direct light.

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

2. Product introduction

2.1. Product characteristics

● Multi-Modal product with which the user can use both face and fingerprint authentication functions together.

● Walk-through product and face authentication is possible by passing and staring at the camera.

● FHD(2M) Display resolution is adapted.

● Live detection feature with Dual Camera (Color & IR)

● RF(125kHz) and Smart Card(13.56MHz) can be used at the same time.

● Easy authentication with the face and fingerprint
  - Can prevent the hazard factors such as forgetting password, losing the card or key, or stealing with the biometrics such as face and fingerprint recognition and increasing the safety with using the person's own bionic information

● Access control management system using LAN
  - Easy expansion by direct applying to the previous network because it communicates with using TCP/IP protocol between the fingerprint recognition terminal and authentication server. High speed with 10/100 Mbps Auto Detect can make it easy to manage and monitor via network.

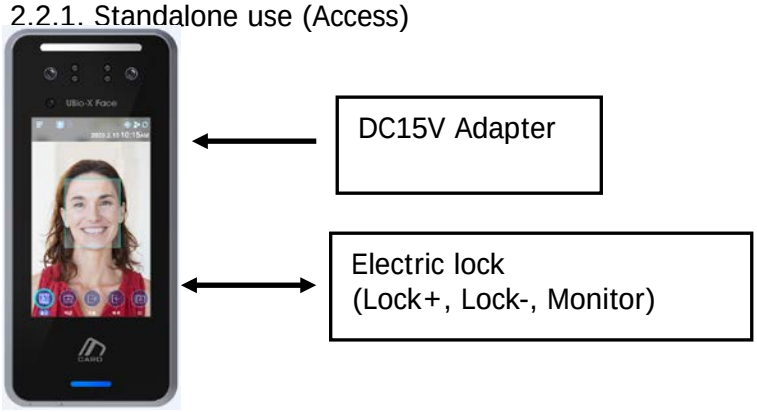
● **Various registration and authentication methods**

Face	Face registration Face authentication
Fingerprint	Fingerprint registration Fingerprint authentication
Card	Card registration Card authentication
Password	Password registration Password authentication
Card or Fingerprint	Card, fingerprint registration Card or fingerprint authentication Fingerprint authentication after ID input
Card & Fingerprint	Card, fingerprint registration Fingerprint authentication after card authentication ID input > Card authentication > Fingerprint authentication
Card or Password	Card, or password authentication Card authentication Password authentication after ID input

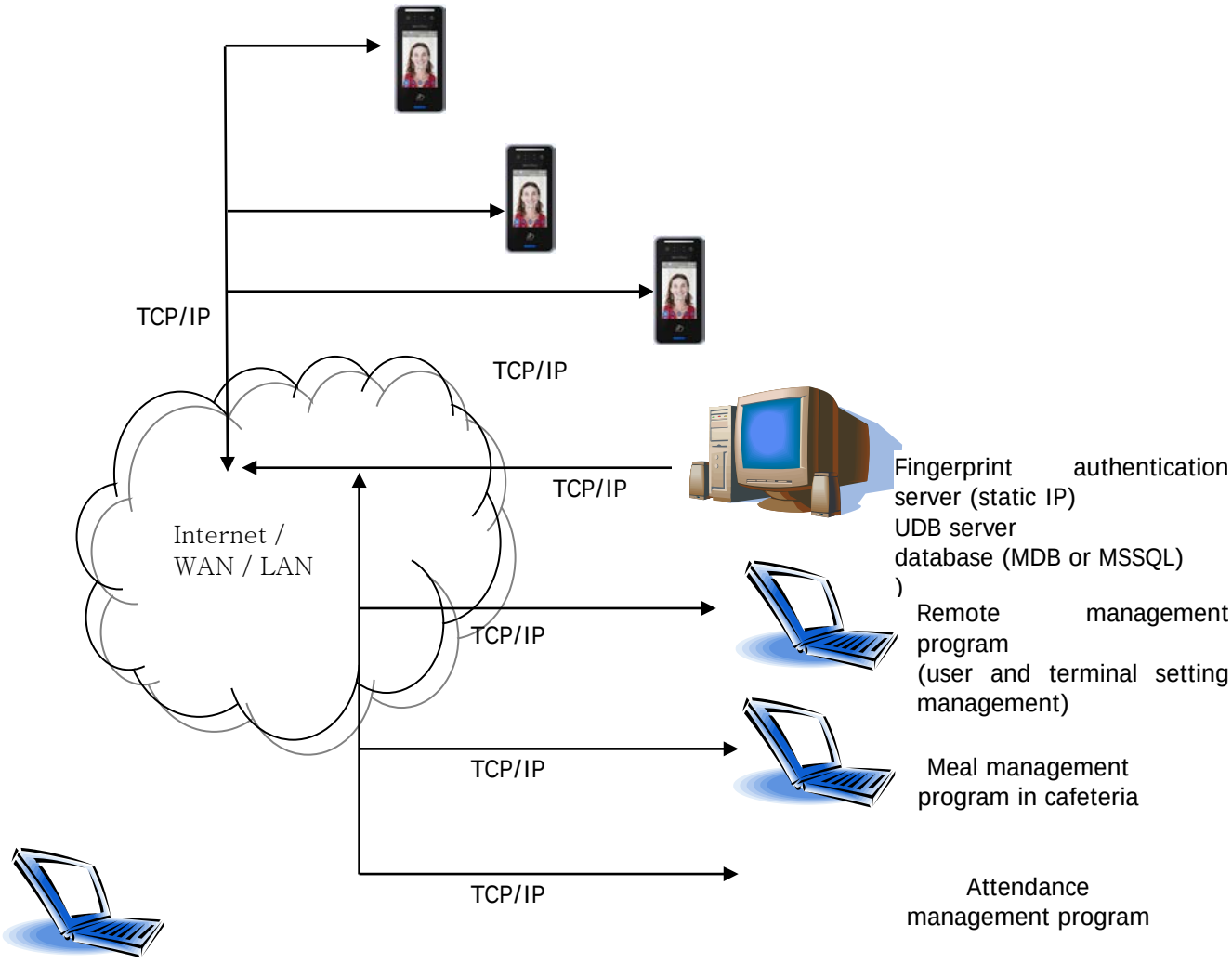
Card & Password	Card, password registration Password authentication after card authentication ID input > Card authentication > Password authentication
Card or Face	Card, face registration Card or face authentication Face authentication after ID input
Card & Face	Card, face registration Face authentication after card authentication ID input > Card authentication > Face authentication
Face or Password	Face, password registration Face authentication ID input> Face authentication > if failed, password authentication
Face & Password	Face, password registration Password authentication after face authentication ID input > Face authentication > Password authentication
Face or Face	Fingerprint, face registration Fingerprint or face authentication ID input > Fingerprint authentication > if failed, face authentication
Card & Face & Password	Card, face, and password registration Face and password authentication after card authentication ID input > Card authentication > Face and card authentication

2.2. Product components

2.2.1. Standalone use (Access)



2.2.2. Connected with Server (Access, Attendance, Meal management)



2.3. Product specification

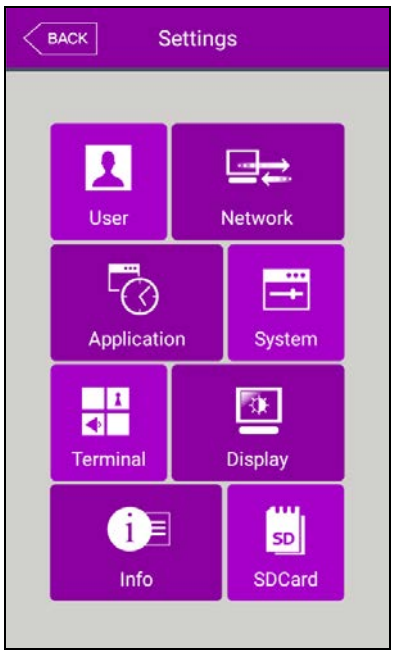
Types	SPEC	REMARK
CPU	1GHz Quad Core CPU	
LCD	5.0 inch Touch LCD(480*800)	
MEMORY	16G Bytes Flash	
	2GBytes RAM	
External SD Card Support	Backup data / FW upgrade	
Camera	Dual Camera (Color & IR)	
Capacity	100,000 User / 100,000 Card 20,000 Face (1:N→1:20,000) 10,000,000 Log / 20,000 Image Log	
Scan Area / Resolution	20 * 20mm / 500 DPI	
Temperature / Humidity	-20 ~ 60℃ / Lower than 90% RH	
AC / DC Adapter	INPUT : Universal AC100 ~ 250V	
	OUTPUT: DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Lock Control	EM, Strike, Motor Lock, Auto Door	
I/O	4 In (1 Exit, 3 Monitor) 2 Out (For Lock Control together)	
Communication Port	TCP/IP (10/100Mbps)	Authentication server communication
	RS-232	Meal ticket printer
	RS-485	Controller communication
	Wiegand In/Out	Card reader or Controller communication
Card Reader	125KHz RF / 13.56MHz Smart simultaneous use (1 Sam socket)	Optional
SIZE	88.0mm * 175.0mm * 43.4mm	

3. Environment setting

3.1. Checks before setting the environment

3.1.1. Entering the menu

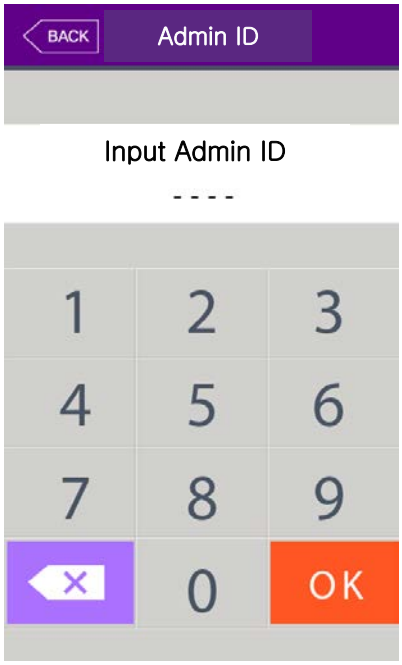
If you click the [ ] icon at the basic window, you can enter the main menu window as follows.



You can enter the subdivision menu by clicking each button.

3.1.2. Administrator authentication

If the administrator is registered, the following administrator authentication window appears first.



▶Administrator authentication

If you enter the administrator ID, the administrator authentication is fulfilled along with the authentication method of the administrator such as card, fingerprint, face, or password.

The administrator authentication only appears when the registered administrator exists. The authentication is fulfilled only once when entering the menu mode and you can access to all the menu until you quit the main menu.

<Fig. 3-2>

3.1.3. How to enter the menu without administrator authentication

It is how to enter the menu when the fingerprint or face authentication is impossible because the administrator card registered in the terminal was lost or there is no administrator.

① Open the cover by removing the bracket at the backside of the terminal

② With the opened cover, connect the 5pin connector number 1 with 3, and 2 with 4 at the bottom of the backside of the terminal.

③ Click the icon at the basic window to enter the administrator authentication window in <Fig. 3-2>, and fill the administrator ID with '0' and click [

] button, then you can enter the menu window.

▶Be sure to remove the connection pin of the connector after modifying the setting value.

3.1.4. How to save the set values

If you click the **[Complete]** button at each menu to save the changed value after the change of settings, the set value of the window is saved and the following message box appears.

▶If there is no changed value, the window is moved to the previous menu.

▶If there is no signal for 30 seconds while changing the set value in the menu, the window is moved to the previous menu.

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

3.2. Menu composition

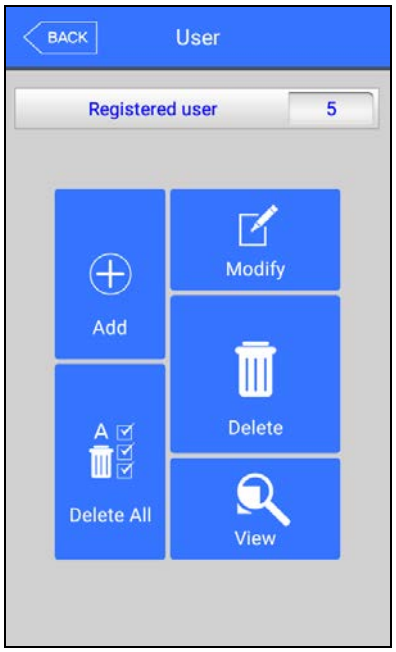
1.User	1. Add 2. Modify 3. Delete 4. Delete All 5. View	
2. Network	IP address	Static IP / DHCP ▶IP address ▶Subnet Mask ▶Gateway
	DNS	▶DNS server 1 ▶DNS server 2
	Server IP	▶Server IP ▶Port
	Terminal ID	▶Terminal ID
3. Application	1. Application	▶Access / TnA / Meal 1. When setting 'Access' or 'TnA' ▶Schedule F1 (Attend) time F2 (Leave) time F3 (Out) time F4 (In) time Access time ▶Blocking Time (0~86400) 2. When setting 'Meal' ▶Schedule Breakfast time Lunch time Dinner time Supper time Snack time □ Allow duplicate
	2. Function key	□ Enable F1 □ Enable F2 □ Enable F3 □ Enable F4 □ ID input
4. System	1. System	▶User ID length [2~8] ▶Authentication: Terminal Only ▶Mandatory Registration □ Face

		□ Fingerprint □ Card □ Password □ Name Number of Fingers [1~10]
	2. Finger	▶1:N Level [3~9] ▶1:1 Level [1~9] ▶Fake Finger Detection ▶FP template format □ Check similar FP □ Multi FP □ Enable 1:N
	3. Face	▶Matching Level [1~4]
	4. Auth	▶Auth Type
	5. Date/Time	▶Time synchronization ▶Display Format ▶Set Date ▶Set Time
	6. Database	1. Delete all users 2. Delete setting 3. Delete Log 4. Delete Image log 5. Factory init
5. Terminal	1. Sound	▶Voice Volume ▶Beep Volume ▶Sound Option
	2. Option	▶Read Card number ▶Card format □ Lock terminal ▶Card reader
	3. Input	▶M0 ▶M1 ▶M2 ▶IO ▶Warn door open (sec) □ Tamper alarm
	4. Lock	▶Lock 1 Option ▶Lock 2 Option ▶Lock 1 duration (ms) ▶Lock 2 duration (ms)
	5. External Device	▶RS232

		▶RS485 ▶Wiegand Site Code Wiegand Output Wiegand Input
6. Display	1. Theme	▶Background
	2. Camera	▶Display Option ▶Save Option □ Save success log □ Save failed log
	3. Language	▶Language
	4. Option	▶Power saving mode ▶Display Option ▶Touch Calibration
	5. Message display time	▶Message Display Time (ms)
7. Info	1. System	▶System Info ▶Disk ▶Ram
	2. Terminal	▶Terminal Info Terminal ID Application Language
	3. Network	▶Network Info MAC <Ethernet> IP
	4. User	▶User
	5. Log	▶Log
	6. About	▶About
8. SD Card	1. Export	1. User Data 2. Event Log 3. System Option 4. Export All 5. Picture
	2. Import	1. User Data 2. System Option
	3. Others	1. Theme 2. F/W Upgrade

3.3. User Management

When you select the **[User]** at the main menu, the following window appears.

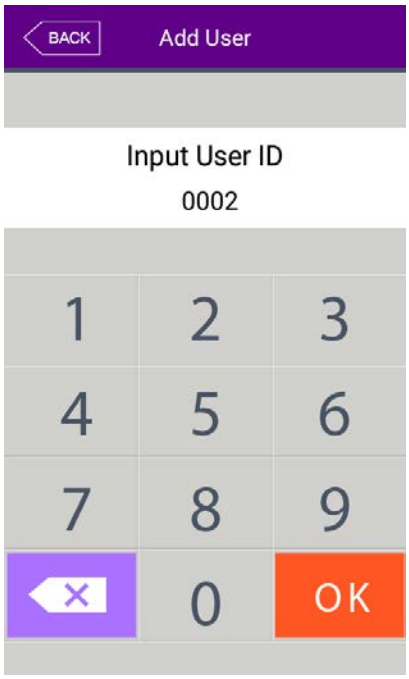


The number of all the users is shown at the top of screen including administrator.

Click **[Add]** button to add the new user, **[Modify]** button to modify the user, **[Delete]** button to delete the specific user, **[Delete All]** button to delete all the users, and **[View]** button to inquire the registered user list.

3.3.1. Add

If you select **[User] -> [Add]** in the main menu, the following screen appears



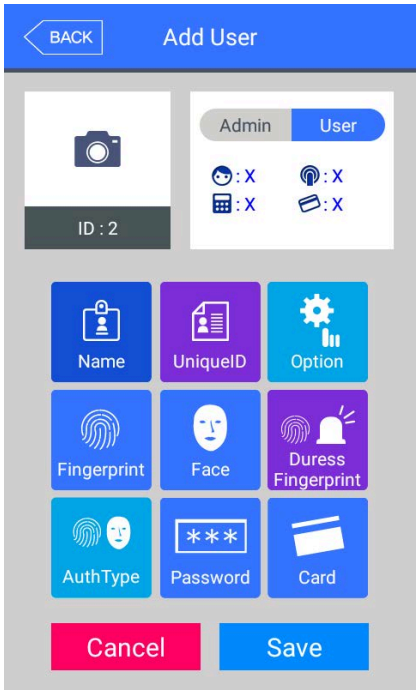
Input the user ID to be registered and click **[OK]** button.

In this case, the ID which can be registered is shown on the screen automatically, so you can register conveniently. If you want to change ID, delete the previous value by clicking [ ] button and input the new value.

Click **[Back]** button to cancel and go back.

.

If you enter ID which is already registered, the failure message appears, and if the ID is not registered, the following screen appears.



The icons in the left side mean as follows

: The number of registered faces

: The number of registered fingerprints (X,1~10)

: Existence of password registration (X: none, O: registered)

: The number of registered cards (X,1~10)

ID : 2 : User ID to be registered

Admin User : User

Admin User : Administrator

Button: Registration with taking a picture of the user.

You can register the name with **[Name]**, employee ID with **[Employee ID]**, fingerprint with **[Fingerprint]**, face with **[Face]**, duress finger with **[Duress FP]**, card with **[Card]**, and password with **[Password]** button. The registration is basically set to be user, and it is can be changed to administrator if you click [Admin] button. Click **[Save]** button to save the registration, and click **[Cancel]** or **[Back]** button to cancel the registration and return.

※ Only user who is registered as administrator can change the operating method of the terminal and can register/modify/delete the information of all the saved users, so be careful to register the administrator.

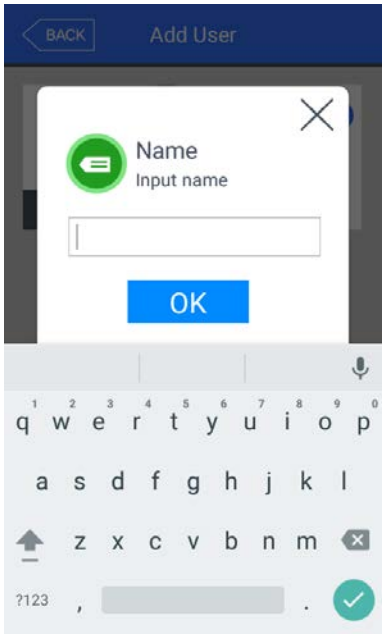
3.3.1.1. Photo registration

Register by clicking [ ] button at the **[Add User]** screen.

Click the **[Save]** button to register with the present camera image.

Click **[Cancel]** or **[Back]** button to cancel the registration and return.

3.3.1.2. Name registration



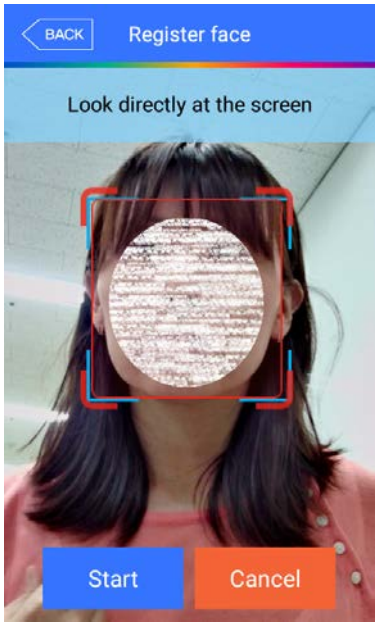
Register by clicking **[Name]** button in the **[Add User]** screen.

After entering name with the keyboard at the bottom, click **[OK]** button.

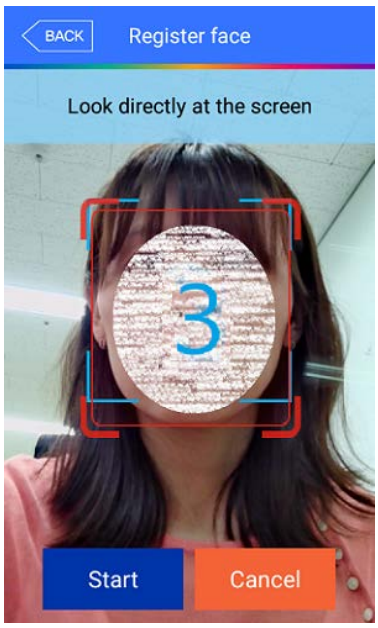
Click the [ ] button to cancel the registration and return.

3.3.1.4. Face registration

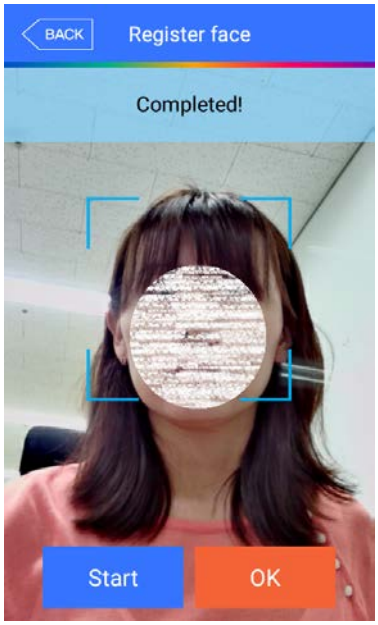
Register with referring ‘1.6. How to register and authorize the face properly’.



① As shown on the left screen, align the red guide that recognizes the face with the center of blue outline and register.



② Press the **[Start]** button to register the face.
As soon as the number on the screen is displayed as 0, the face is registered, so please be caution not to blink the eyes at this moment.

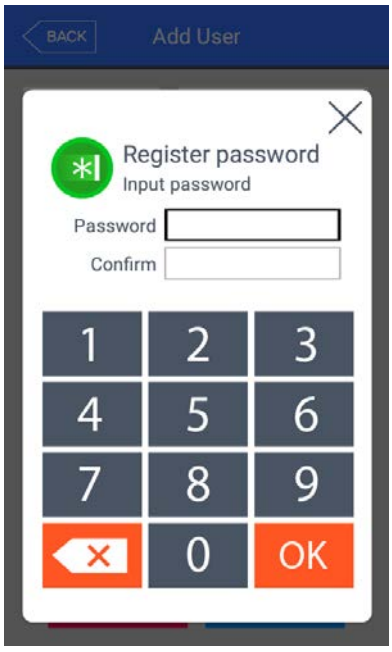


③ When the registration is ended, '**Completed'** message is shown on the screen. If you click [**OK**] button, the face registration is completed and the screen is moved to the previous screen.

If you want to register again, click [**Start**] button to start from the procedure of ②.

※ Basically the feature 'Similar face check" is done at the registration of face but this feature is applied only for the users have the registered face including the Multi Auth users who the option '1:N face use' are activated. So you have to watch out the face users without above condition cannot be verified by the similar face check. (This condition is applied for the feature 'Similar fingerprint check', too.)

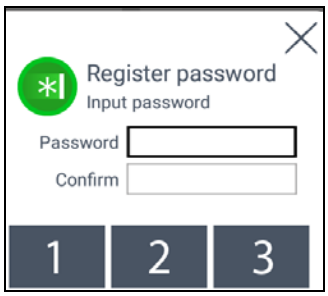
3.3.1.5. Password registration



If you enter the password in 1~8 characters into the password input window and click **[OK]** button, the input focus is moved to the 'password confirm' window at below. Enter the same password again and click **[OK]** button.

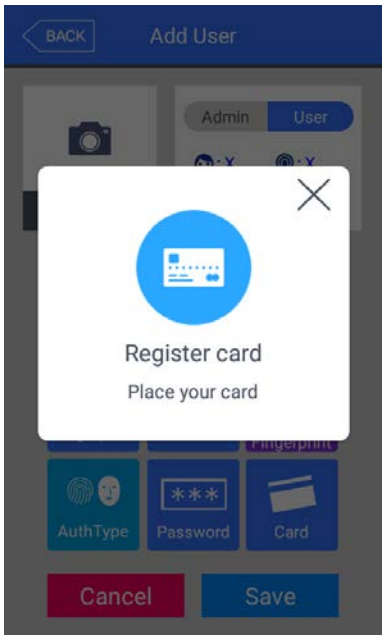
Click [✕] button to cancel and return.

※If you enter the different password in the confirm window, the message "Wrong input!" appears as follows



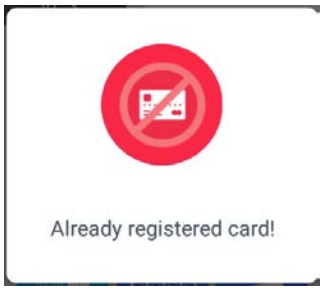
UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

3.3.1.6. Card registration



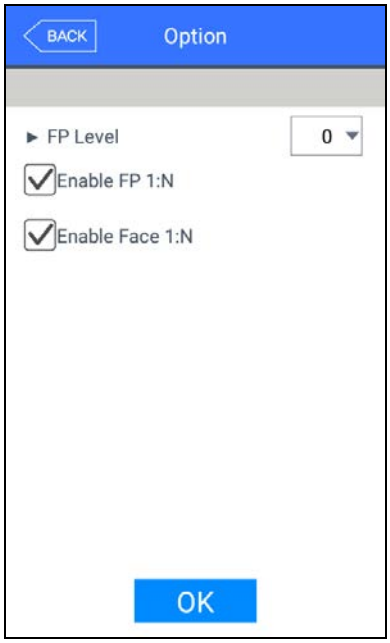
Register with clicking **[Card]** button in the **[Add User]** button. Click [X] button to cancel and return.

※If you entered the card already registered, the following message appears.



※If a user tried over than 10 registrations, the following message appears.

3.3.1.7. Authentication option



▶'FP Level' (Basic setting: '0')

It decides the fingerprint authentication level of each user, and the registered users can have different authentication level by modifying this value. If you set '0', the authentication uses the level of fingerprint authentication.

For example, if you select the "1" for FP Level, this user will be applied with "1" on 1:1 FP Level.

But you select "0" for this level, the user will be applied with the configured 1:1 FP Level on the "System > Finger".

▶'Enable FP 1:N' (basic setting: Registered FP user exist. [v])

If this option is checked, you can authorize only with fingerprint without user ID or card

▶'Enable Face 1:N' (basic setting: Registered Face user exist. [v])

If this option is checked, you can authorize only with face without user ID or card.

3.3.1.8. Auth type

Set by clicking **[Auth type]** at the **[Add User]** window. (But, it can be set when there are more than 2 authentication methods registered)
Click **[Back]** button to cancel and return.
.

This shows all the authentication methods already registered, and the buttons at the lower side shows the buttons **[OR]** / **[AND]** which can be selected. Present authentication method is distinguished with blue color as different as gray color is not selected.
If you click the button **[OK]**, the authentication method is changed and the screen moves to the previous window.
The authentication method icons are represented as follows.

: Face

: Card : Password

※ In case of authentication method, if it is not set, the authentication methods are set to **[OR]** automatically with the current registered authentication methods. (But, there are registerable for 3 authentication methods at maximum and if they are used with Password, it will be limited 2 authentication methods)

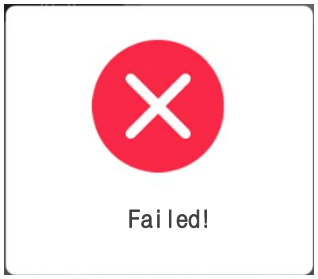
3.3.1.9. Save

Click the **[Save]** button to save when all the registration procedure is finished. At this point, if you click **[Cancel]** or **[Back]** button to return, the user is not saved.

Next is the LCD messages which can appear at the registration procedure.

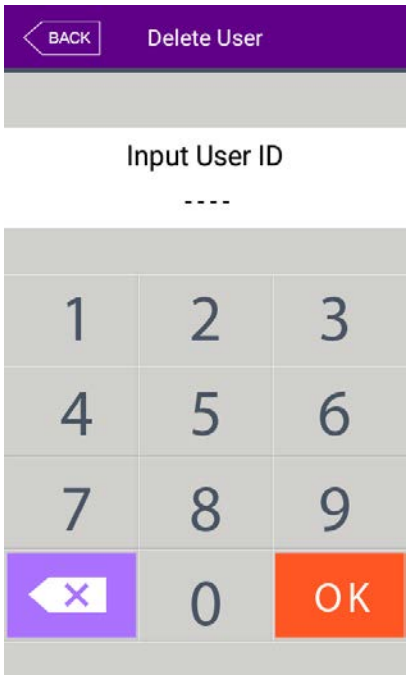
	When you clicked the **[Save]** button, the case registration was successful

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

	When you clicked the **[Save]** button, the case registration was failed : The case none of authentication methods such as fingerprint, face, card, and password is registered.
	When you clicked the **[Auth method]** button, the case none of the authentication method was registered.

3.3.2. Delete

The following window appears if you click **[User]** → **[Delete]** at the main menu.

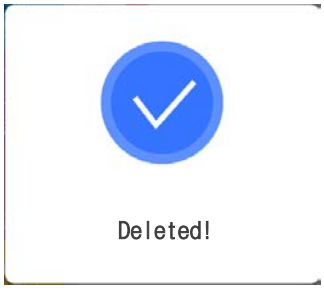
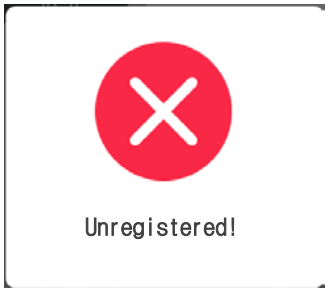


Input the user ID to be deleted and click **[OK]** button.
Click **[Back]** button to cancel and return.

If you input the unregistered ID, the failure message “Unregistered user” appears, and if you input the registered ID, success message “Deleted” appears

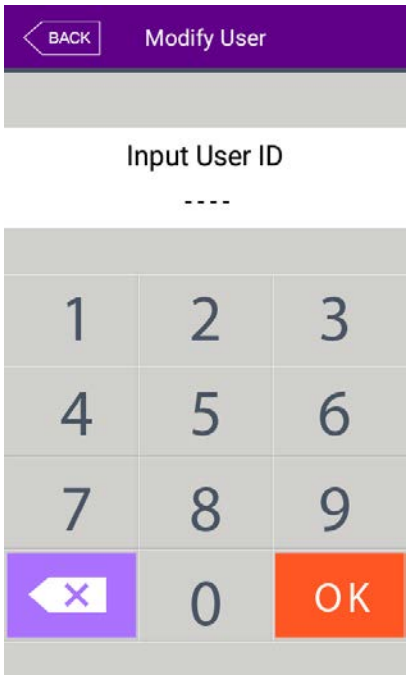
But, the deletion in the terminal is not led to the deletion in the server, so if you want to delete completely, you should delete it also in the server.
It deletes both user and admin, so you should be cautious, and the user registered only in the terminal is cannot be recovered.

The followings are LCD guidance which can appear at the deletion procedure.

	When it is deleted normally.
	When unregistered ID was entered

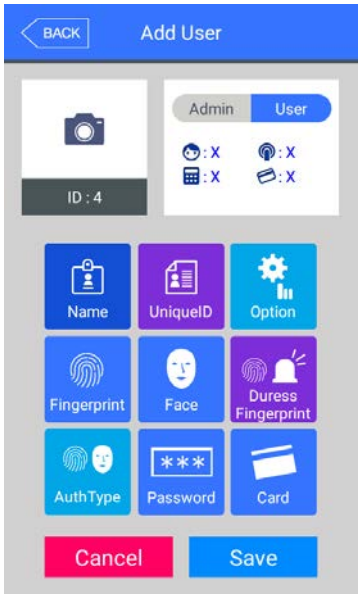
3.3.3. Modify

The following window appears if you click the **[User]** → **[Modify]** in the main menu.



Input the user ID to be modified and click **[OK]** button.
Click **[Back]** button to cancel and return.

The failure message appears if you input the unregistered ID, and if you input the registered ID, the information of registered user is represented as follows



The icons at the left side means as follows.

: The number of registered faces

: The number of registered fingerprints (X,1~10)

: Existence of password registration (1: Registered / X: Not registered)

: The number of registered cards (X,1~10)

ID : 4 : User ID to be registered

Admin User : User

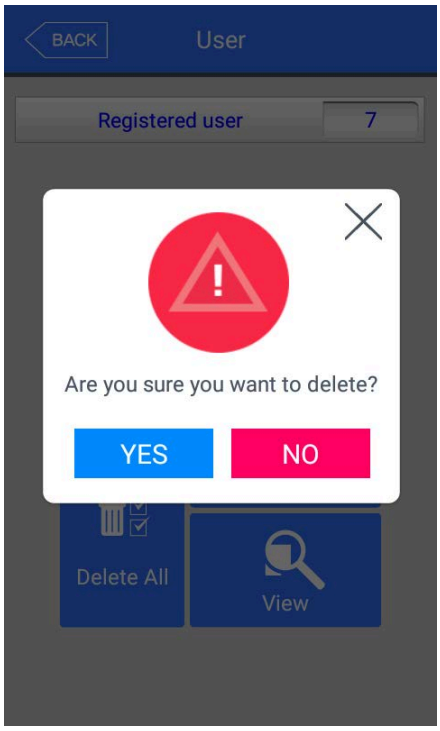
Admin User : Administrator

If you touch the picture, you can register with re-taken picture

The modification method of each item is the same with the user addition, so refer to the '3.3.1. Add'.

3.3.4. Delete all

If you click the **[User]** → **[Delete all]** in the main menu, the following window appears.

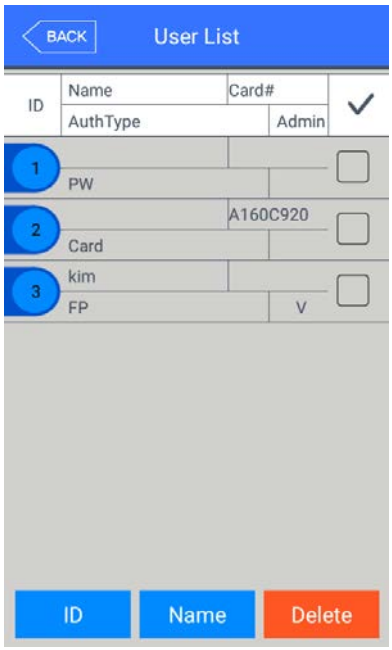


If you want to delete all the users, click **[YES]**, and if you want to cancel, click **[NO]**.

※If you click **[YES]**, the users and admin are deleted, and the restoration is impossible once they are deleted, so be careful.

3.3.5. View

If you click the **[User] -> [View]** in the main menu, all the users registered can be searched as follows.

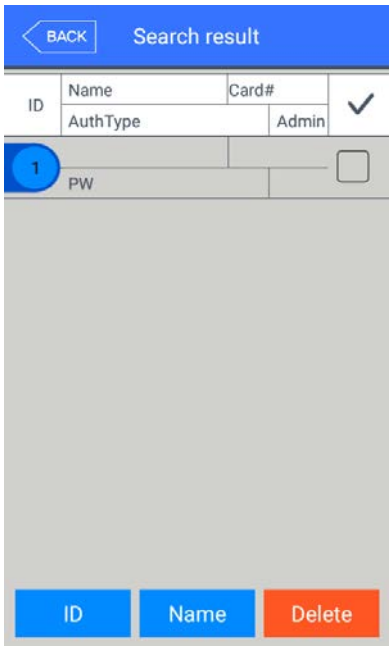


The user list appears by the order of ID, and if you slide the screen upward, you can search the additional user list.
The list appears in the unit of 100 people and if the list is more than 100 people, you can see the previous or next list by clicking **[Back]** or **[NEXT]** button.

▶**[ID]**: If you click the ID of specific user, you can directly move to the modification window of the user.

▶**[Delete]:** If you check the box of the right side and click the **[Delete]** button, you can delete all the checked users at once

If you click **[Back]** button on the top, you can move to the previous '3.3 User management' menu.



▶If you input the User ID by clicking **[ID]** button, the user is searched like in the left picture.
If you click **[Back]** button in this window, you can move to the '3.3. User management' menu.

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

▶**[Name]**: If you input the user name by clicking **[Name]** button, the registered user list including the characters is shown.
If you click **[Back]** button in this window, you can move to the '3.3. User management' menu.

3.4. Network setting

If you select **[Network]** in the main menu, the following window appears.

▶Basic setting: Same with the window at the left side.

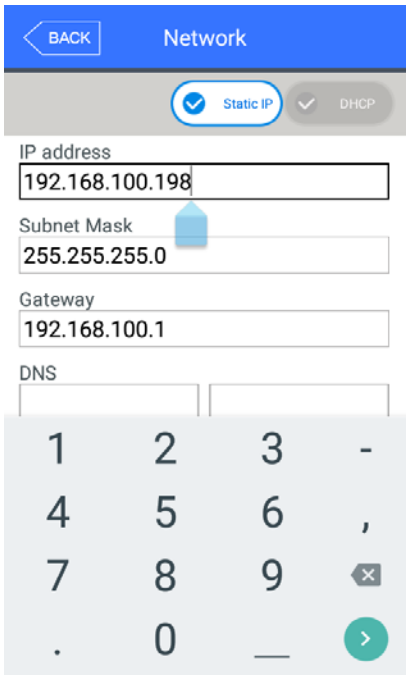
Select the method **[Static IP]** if the static IP is allocated from the connected network, and select **[DHCP]** if the IP is allocated from the DHCP server in the connected network.
.

If you selected **[Static IP]**, set the IP address, subnet mask, and gateway. And if you selected **[DHCP]**, you don't have to set them.

DNS entry is possible instead of IP in the **[Server IP]**, and if you use specific DNS server, input the IP address of **[DNS]** server together. Check "DDNS" when typing DNS in order to type in English.

▶**[Port]**: The basic port value of the authentication server (UNIS server) is '9870', and if you change the value, you should change the server program with the same value, so be cautious.

▶[**Terminal ID**]: It is unique ID used by the terminal to distinguish the terminals and the default value is '1'. It should be the same with the ID of the terminal registered, and the characters can be up to 9 digits.



If you touch the item you want to change, the keypad appears at the bottom.

If the input is finished with the keypad, continue the input by touching [↵] button or the next input window. If you touch the background window which is not the input window, the keypad disappears.

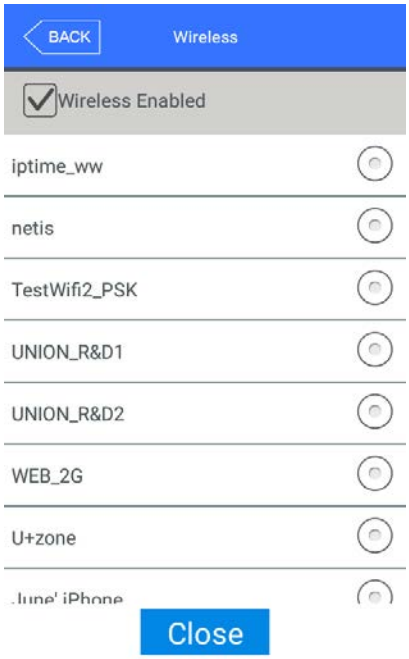
If you want to apply the changes, click **[Save]** button, and return to the previous menu by clicking **[Back]** button.

▶[**Wi-Fi**]

When the Wi-Fi dongle is connected to the USB port on backward of the UBio-X Pro2 device, this icon [Wireless] will be come up automatically on the Network screen as same as left picture.

※ Notes

If you want to apply the Wi-Fi dongle, you have to purchase it from our sales team since we cannot guarantee to cooperate 3rd party Wi-Fi dongle with our device.



When the check box **[Wireless Enabled]** was checked, the AP list around will be scanned automatically as like the left picture.

Selecting the AP name from the AP list, the AP password will be asked and then UBio-X Pro2 device will be connected to this AP when inputting the proper AP password.

If you want to apply the changes, click **[Close]** button, and return to the previous menu by clicking **[Back]** button.

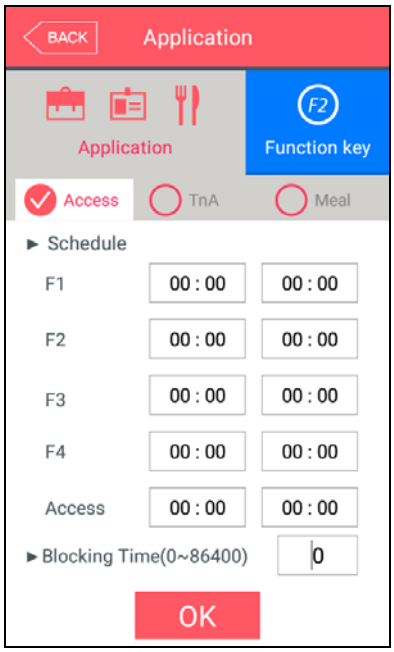
UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr

3.5. Application mode

3.5.1. Application

If you select the **[Application]** in the main menu, the following window appears.
In the application mode, you can select the **[Access / TnA / Meal]** according to the purpose.

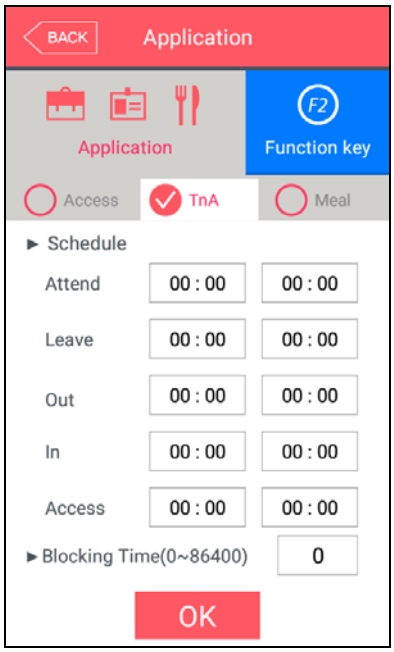
3.5.1.1. Access or TnA setting



It is the screen appearing when you select the Access.

Click **[OK]** button to apply the changes, and click **[Back]** button to cancel and return.

▶Basic setting : Same with the window at the left side.



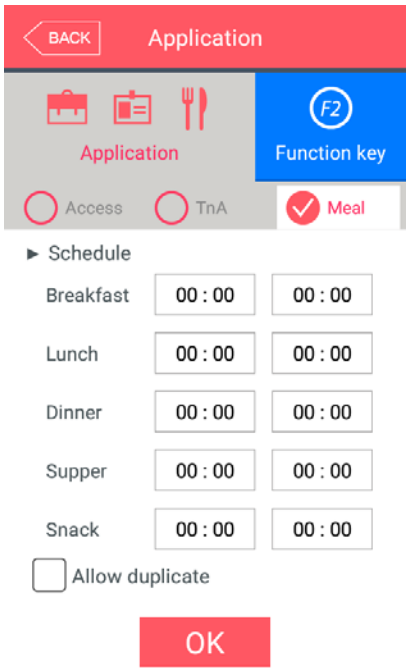
It is the screen appearing when you select the **[TnA]**.

Click the **[OK]** button to apply the changes, and click **[Back]** button to cancel and return.

▶Schedule (00:00~23:59): You can set the time for each authentication mode and if you do not need the function, set '00:00-00:00'.
During the set time, the set mode is always shown unless clicking another function button, and it is convenient for the TnA management because the indication mode is changed to the set authentication mode automatically though another mode was authorized by clicking another function key. The time periods should not be overlapped, but if they are overlapped, the application order is Attend (F1) →Leave (F2) →Out (F3) →In (F4) →Access. If the time is set between 23:00~01:00, it means from 23:00 to the 01:00 the following day.

▶Blocking time (0~86400): This function prevents the same user to authorize again in the set time. There is no restriction if it is set 0, but if it is set bigger than 0, the user can authorize again when the set time (sec) is passed from the previous authentication. It can be set up to 86,400 seconds (24 hours).

3.5.1.2. Meal setting



It is the screen appearing when selecting the meal management.

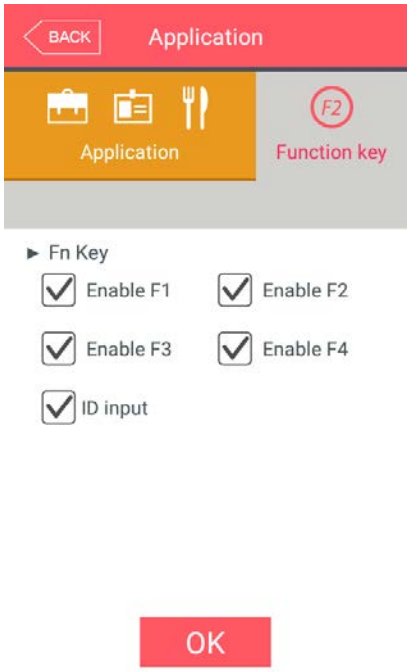
You can set the time period of each meal type.
And if the setting is not needed, set '00:00-00:00'.

▶Allow duplicate : If it is unchecked (☐), each user can authorize once in the one meal, but if it is checked (☑), the multiple authentication is possible regardless of the previous authentications.

Click the **[OK]** button to apply the changes, and click **[Back]** button to cancel and return.

3.5.2. Function key

The following window appears if you select the **[Application]** → **[Function key]** in the main menu.



▶Basic setting: Same with the window at the left side.

▶Fn key

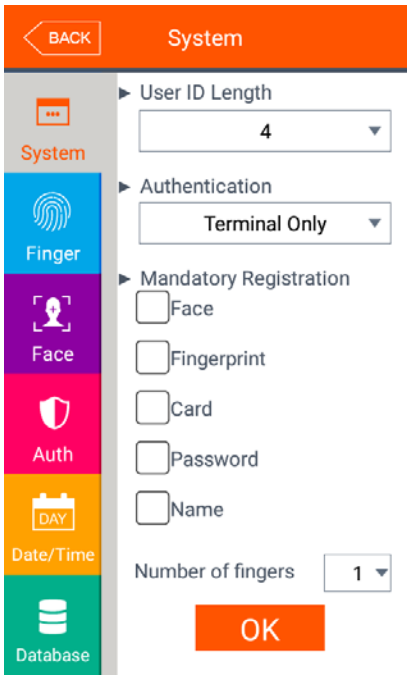
It means the **[F1]** ~ **[F4]**, Access button used to change the authentication mode such as attendance and leaving, and if you click the Fn key, the authentication mode is changed to the mode. Because only the checked buttons are represented on the basic window, you can use with unchecking other function keys when using as device only for the attendance or leaving

Click **[OK]** to apply the set value, and click **[Back]** button to move to the previous menu.

3.6. System

3.6.1. System

The following window appears if you select the **[System]** → **[System]** in the main menu.



▶Basic setting: Same with the window at the left side

▶User ID Length

It sets the length of the user ID, and it can be 2~9 characters and should be the same with the length of the registered ID of the server program. If the ID registered in the server program uses '000075' as a 6 digits ID, set 6.

▶Authentication

It determines the priority of the authentication between the terminal and network server and there are 4 modes "Terminal Only", "Server Only", "Terminal/Server", "Server/Terminal".

[Terminal Only]: It only authorizes the user registered in the terminal.
[Server Only]: It only authorizes the user registered in the server.
[Terminal/Server]: It authorizes the user registered in the terminal as 1:N identification but it authorizes the user in the server as 1:1 verification.
[Server/Terminal]: It authorizes the user registered in server as 1:N identification but if the network between server to terminal was disconnected, it authorizes the user registered in terminal as 1:N identification.

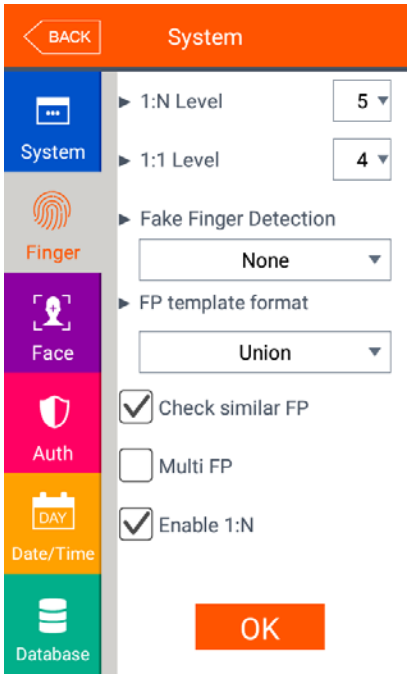
▶Mandatory Registration

It determines the items which should be entered in the user registration, and the user can be registered when all the checked items are entered. The number of registered fingerprints is only valid when the **[Fingerprint]** is checked.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return. If you click the OK button without changing the set value, it is moved to the upper menu directly. Click the menu button at the left side to set additionally.

3.6.2. Finger

The following screen appears if you select the **[System]** -> **[Finger]** in the main menu.



▶Basic setting: Same with the window at the left side

▶1:N Level (3~9)
It is the authentication level used in the 1:N Fingerprint authentication. In case of 1:N authentication, the authentication level is not set for each user, so the authentication level of the terminal is always the standard.

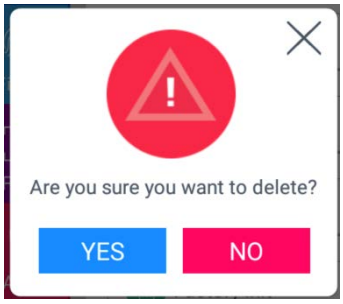
▶1:1 Level (1~9)
It is the authentication level used in the 1:1 Fingerprint authentication. But, in case of the user whose 1:1 authentication level is not set '0' (using the authentication level of the terminal), it follows the 1:1 authentication level of the user.

▶Fake Finger Detection
It sets the LFD level to prevent the fake fingerprint input. The higher level of the LFD level, the preventing function of the fake fingerprint input such as rubber, paper, film, or silicon is strengthened, but the fingerprint also can be hard to enter if the finger is dry too much.

▶FP template format
It determines the format of fingerprint template. When some applications using SDK need another format of the fingerprint, the fingerprint template format of the terminal can be changed. But, if using UNIS server, it should be set the same with the template format of the server.

- Union: It is the default setting and the volume is 400 bytes for each template. It is the most optimized format related with all the functions using fingerprint (1:1 level, 1:N level, authentication speed, and fake fingerprint detection), and the authentication can be fulfilled rapidly and correctly.
- ISO Standard: Fingerprint data is saved as ISO template which is 500 bytes for each template.
- ISO Extended: Fingerprint data is saved as ISO template which is 600 bytes for each template.

If you change the template format of the fingerprint, the following message box appears.



If you click the **[OK]** button, the new format is applied, and if you click the **[Cancel]** button, the format value before the change is maintained.

※ Notes

If you change the fingerprint template format, all the registered fingerprints are deleted, so be cautions.

▶Check similar FP

If it is checked (☑), the re-recognition as another user ID is prevented by checking if the fingerprint is already registered. Similar fingerprints are checked against users who ticked the 1:N option. (100,000 fingerprints limit)

▶Multi FP

If it is checked (☑), all the registered fingerprints should be authorized after the ID (or card) input. If it is checked, the user should input the user ID or card, the option **[Enable 1:N]** will be unchecked (☐) automatically.

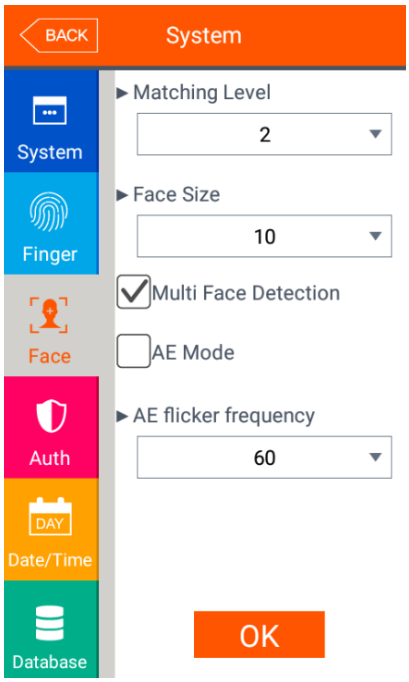
It is the function used when managing the access control of the special area strictly.
For example, if the user with ID '0001' has three fingerprints registered, the user should be authorized with all three fingerprints after entering ID.
In this case, the order of three fingerprints is not important, but if one of the fingerprints is failed to be authorized, the authentication is failed.

▶Enable 1:N

If it is checked (☑), the user can be authorized only with the fingerprint without user ID or card. Though the user is registered by enabling 1:N authentication, in the terminal where the option is not checked, only the 1:1 authentication is possible.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return. If you click **[OK]** button without changing the set value, it is moved to the upper menu automatically.

3.6.3. Face



▶Basic setting: Same with the window at the left side

▶Matching level

It is the level used in face authentication, and it can be set 1~4 levels according to the accordance degree with the registered face. And the authentication is successful when the accordance degree is higher than set authentication level.

If the authentication level is higher, the security level will be higher, but you also can fail to authorize easily due to the high requirement for the accordance level.

▶Face Size (10~400)

Authentication is allowed only when the size of the detected face is larger than the pixel. As the size of the face increases, authentication is possible when approaching at a close distance.

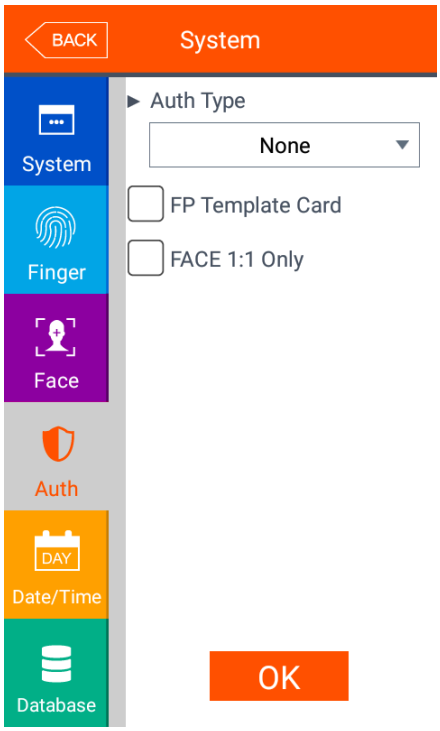
▶Multi Face Detection

When checking (☑) this option, it can detect several faces at once. When unchecking (☐) this option, since the biggest face can be detected, it can be used when one person authenticates at a time such as a speed gate.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return. If you click **[OK]** button without changing the set value, it is moved to the upper menu automatically.

3.6.4. Auth

If you select the **[System]** → **[Auth]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side

▶Auth Type: Select the authentication method of the terminal.

- Card: Though the user is registered with the authentication method requiring the face, fingerprint, or password in addition to the card, the terminal with the checking of the item, the card can authorize by itself. For fingerprint, face or password users, follow the same authentication procedure as per normal to authenticate.

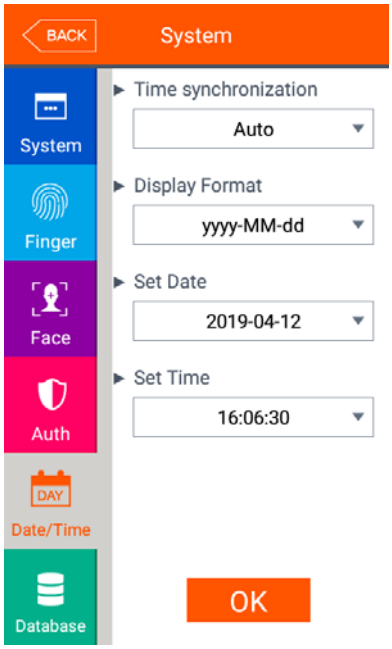
- Fingerprint: Though the user is registered with the authentication method requiring the card, face, or password in addition to the fingerprint, the terminal with the checking of the item, the fingerprint can authorize by itself. For fingerprint, face or password users, follow the same authentication procedure as per normal to authenticate.

- Face: Though the user is registered with the authentication method requiring the card, fingerprint, or password in addition to the face, the terminal with the checking

of the item, the face can authorize by itself. For fingerprint, face or password users, follow the same authentication procedure as per normal to authenticate.

3.6.5. Date/Time

If you select the **[System]** → **[Date/Time]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side

▶Time synchronization

It determines the synchronization method between the present time of terminal and server. If you want automatic synchronization, set **[Auto]**, and if you want manual synchronization, set **[Manual]**.

.

▶Display format

The present time indicating method of the terminal

- yyyy-mm-dd: Order of year, month, and date.
- dd-mmm-yyyy: Order of date, month (English), and year

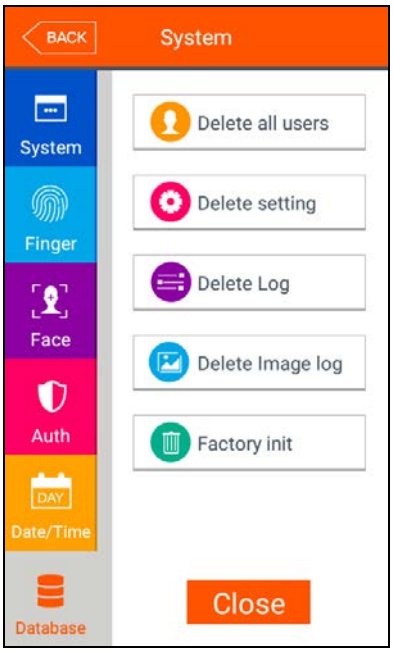
▶Set Date / Set Time

It changes the present time of the terminal. If the server is connected and the [Time synchronization] is set [Auto], you don't have to change since it is synchronized with the server time.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.6.6. Database

If you select the **[System]** → **[Database]** in the main menu, the following window appears.

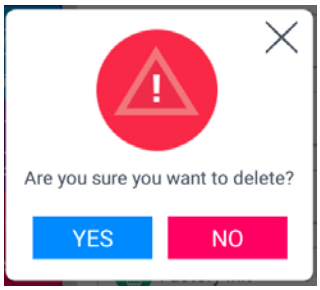


If you want to delete all the users, click **[Delete all users]** button.
If you want to initialize the settings, click **[Delete setting]** button.
If you want to initialize the authentication record, click **[Delete Log]** button.
If you want to delete image log only, click **[Delete image log]** button.
If you want to delete all the data and initialize with the factory setting, click **[Factory init]** button.

If you want to move to the upper menu, click **[Close]** or **[Back]** button.

3.6.6.1. Delete all the users

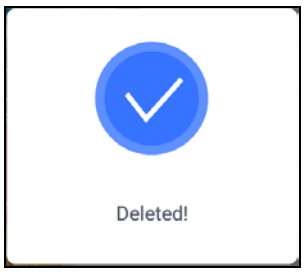
If you select the **[System → [Database] → [Delete all users]** in the main menu, the following window appears.



If you want to delete all users, click **[YES]** button, and if you want to cancel, click **[NO]** or **[X]** button.

If there is no signal for 5 seconds in this state, the message box disappears without deletion.

If deletion is successful by clicking **[YES]**, the following success message box appears.

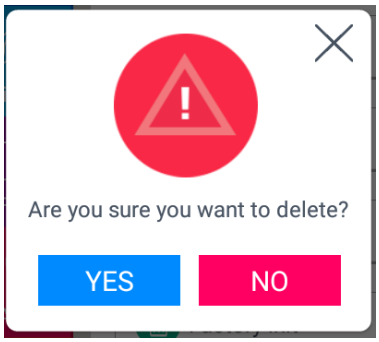


<Fig. 3-5>

In this case, both the users and administrator are deleted, **and the restoration is impossible once the data is deleted.**

3.6.6.2. Delete setting

If you select the **[System] → [Database] → [Delete setting]** in the main menu, the following screen appears.



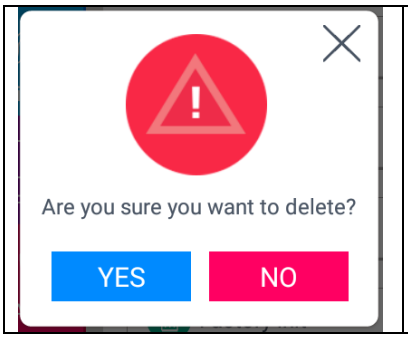
Click **[YES]** button to initialize all the set values, and click **[NO]** or [X] button to cancel.

If there is no signal for 5 seconds in this state, the message box disappears without initialization.

If the deletion is successful by clicking **[YES]**, the success message in <Fig. 3-5> is displayed and the display language and voice is changed to the default value English. All the set value of the terminal besides the MAC address, but the record of the users and authentications is not deleted.

3.6.6.3. Delete Log

If you select the **[System] → [Database] → [Delete log]** in the main menu, the following window appears.



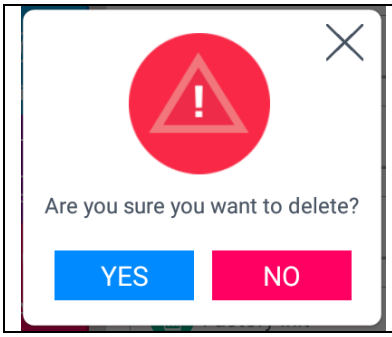
If you want to delete all the authentication record in the terminal, click **[YES]** button, and if you want to cancel, click the **[NO]** or [X] button.

If there is no signal for five seconds in this state, the message box disappears without deletion.

If it is deleted successfully by clicking **[YES]**, the success message in [Fig. 3-5] is displayed. All the authentication log is deleted including image log, **and the restoration after the deletion is impossible.**

3.6.6.4. Delete image log

If you select the **[System] → [Database] → [Delete image log]** in the main menu, the following window appears.



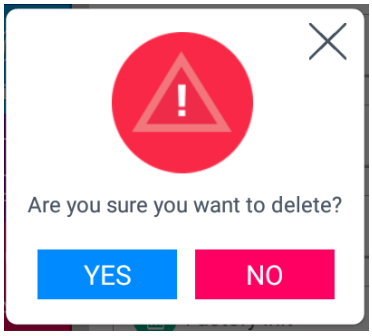
If you want to delete all the authentication record in the terminal, click **[YES]** button, and if you want to cancel, click the **[NO]** or [X] button.

If there is no signal for five seconds in this state, the message box disappears without deletion.

If it is deleted successfully by clicking **[YES]**, the success message in [Fig. 3-5] is displayed. The image saved as a log is only deleted and the authentication log is not deleted.

3.6.6.5. Factory init

If you select the **[System] → [Database] → [Factory init]** in the main menu, the following window appears.



If you want to initialize the terminal in the factory setting, click **[YES]** button, and if you want to cancel, click **[NO]** or [X] button.

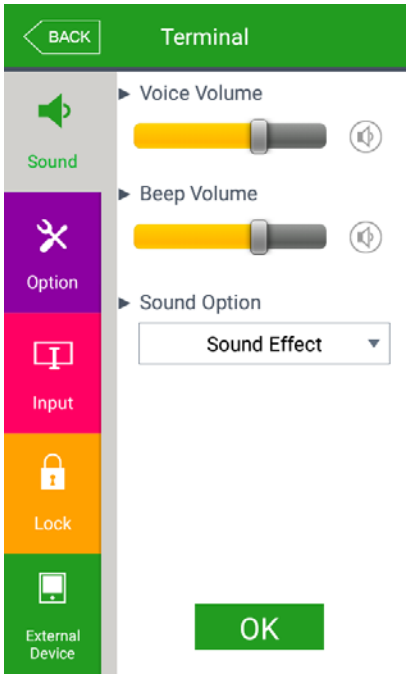
If there is no signal for five seconds in this state, the message box disappears without initialization.

If it is deleted successfully by clicking **[YES]**, the success message in <Fig. 3-5> appears, and the display language and voice is changed to the default value English.
All the set value, users and log information besides the MAC address in the terminal to make the terminal in the factory setting. **The restoration after the deletion is impossible, so be careful.**

3.7. Terminal

3.7.1. Sound

If you select the **[Terminal]** → **[Sound]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side.

▶Voice volume
Scroll from side to side in 0~15 degrees to set the voice volume. If you click the [ ] button at the right side, the voice is played to check the volume.

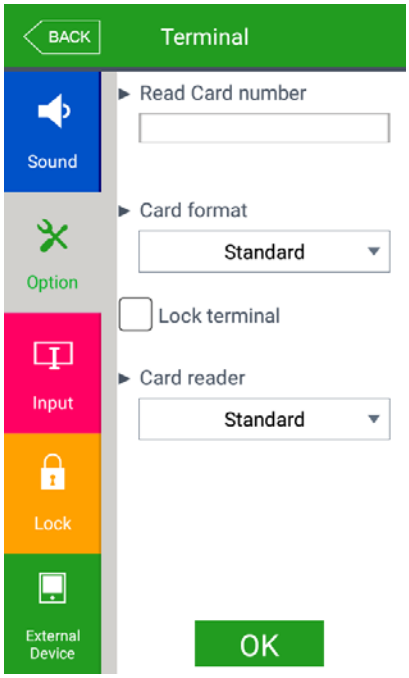
▶Beep volume
Scroll from side to side in 0~3 degrees to set the beep volume. If you click the [ ] button at the right side, the beep sound is played to check the volume.

▶Sound Option
- Sound effect: The sound effect can be output on authentication success or failed.
- User voice: If the user wants to change the voice played when the authentication is successful or failed, the user voice can be played if the user copies the sound into terminal and check the option. The method to copy the sound into the terminal can be referred in 3.10 **[SD card]** → **[Theme]** or [3.11.2 How to change voice sound].
- Saved Voice: The saved voice can be output for authentication success or failed.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return. If you want to set another items, click the menu you want to change at the left side.

3.7.2. Option

If you select the **[Terminal]** → **[Option]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side.

▶Read Card number: If the user put the card on the screen, the card number is displayed on the LCD. You can change the **[Card format]** to check the card number according to the set value.

▶Lock terminal: This function enables the administrator to lock or unlock the terminal directly on the terminal, not on the server program. If it is checked (☑), none can access due to the lock until the administrator unlock the setting.

▶Card reader: You can set Standard or HID iClass and it can recognize the card of setting type.

▶Card format

It determines the representation method of the card number. The card number is changed according to the following settings. So if you have to change the card expression method, you should register the card again.

[RF card example] Card number (5byte): 08h 01h 16h 1Dh D6h

Card format	Card number	Expression
Standard	02207638	(3+5) digits decimal [022(16h)+07638(1DD6h)]
Hexadecimal	0801161DD6	10digits hexadecimal
10 Digit Decimal	0018226646	Posterior 4byte: 10digits decimal (01161DD6h)
3,5 Digit Decimal	02207638	Same with [Standard]
6 Digit Hexadecimal	161DD6	Posterior 3byte: 6digits hexadecimal

[SC card example] Card number (4byte): 52h 9Dh 06h E3h

Card format	Card number	Expression
Standard	529D06E3	8 digits hexadecimal
Hexadecimal	E3069D52	8 digits hexadecimal with changing the order of

		byte
10 Digit Decimal	1386022627	hexadecimal 529D06E3: 10 digits decimal
3,5 Digit Decimal	3808861522	hexadecimal E3069D52: 10 digits decimal
6 Digit Hexadecimal	069D52	Locate the foremost 3bytes backwards.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.7.3. Input

If you select the **[Terminal]** → **[Input]** in the main menu, the following window appears.

▶Basic setting : Same with the window at the left side.

▶M0: It is set when connecting the external access point to the DM0
(When using motor lock, set **[Door open NO]** or **[Door open NC]**.)
-None: When nothing is connected.
-Door open NO or Door open NC: When the door open monitoring pin was connected.
-Fire detection NO or Fire detection NC: When the fire detection sensor is connected.
-Panic detection NO or panic detection NC': When the panic situation detection sensor is connected.
-Emergency detection NO or emergency detection NC': When the emergency situation detection sensor is connected.
→ Set NO/NC according to the state of pin input in detection.

▶M1/M2: Set when connecting the external access point to DM1/DM2
(When using motor lock, set **[Lock NO]** or **[Lock NC]**.)
- None: When nothing is connected.
- Lock NO or Lock NC: When the lock monitoring pin was connected.
- Fire detection NO or Fire detection NC: When the fire detection sensor is connected.
- Panic detection NO or panic detection NC': When the panic situation detection sensor is connected.
- Emergency detection NO or emergency detection NC': When the emergency situation detection sensor is connected.

→ Set NO/NC according to the state of pin input in detection.

▶IO: Set when connecting the external access point to the Exit pin.
- None: When nothing is connected
- Inside Open NO or Inside Open NC: When the exit button was connected
- Fire detection NO or Fire detection NC: When the fire detection sensor is connected.
- Panic detection NO or panic detection NC': When the panic situation detection sensor is connected.
- Emergency detection NO or emergency detection NC': When the emergency situation detection sensor is connected.

→ Set NO/NC according to the state of pin input in detection

▶Warn door open (sec)
This function alarms when set time for door open (5~30 seconds) is passed with the opened door.
If it is set **[0]**, no alarm is ringing, and though you set **[01~04]**, the alarm will ring after 5 seconds.

This function enables the appropriate action to close the door when someone could know that the door is not closed properly by alarming when the door is not closed for specific time.

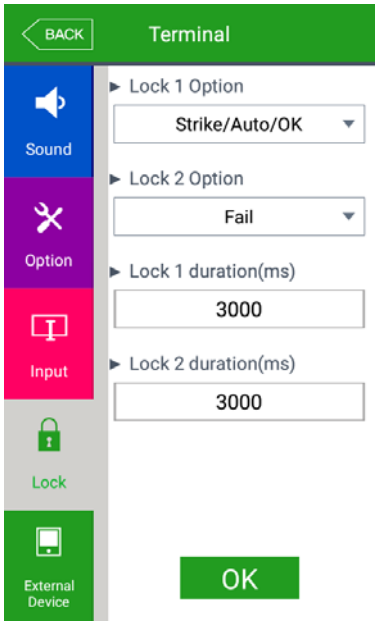
To use the function, the lock must be able to be monitored if it is opened or closed, and the monitoring pin of the lock also should be connected with M0. In addition, the previous M0 also should be set **[Door open NO]** or **[Door open NC]**.

▶Tamper alarm
If it is checked(☑), a warning sound will be played when the terminal is disassembled.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.7.4. Lock

If you select the **[Terminal]->[Lock]** in the main menu, the following windows appears.



▶Basic setting: Same with the window at the left side.

▶Lock 1 Option
- None: When it is not used
- Strike/Auto/OK: When the warning light is connected to indicate the strike type, auto door, or authentication success/failure on Lock1.
- Motor lock 1: When the motor lock is connected.
- Regular notification: When the siren setting of the terminal option was sent to the terminal, it sends the operating signal about it.
- Duress alarm: When the fingerprint registered as a duress FP is authenticated

▶Lock 2 Option
- None: When it is not used
- Strike/Auto/OK: When the warning light is connected to indicate the strike type, auto door, or authentication success/failure on Lock2.
- Motor lock 2: When the motor lock is connected.
- Regular notification: When the siren setting of the terminal option was sent to the terminal, it sends the operating signal about it.
- Duress alarm: When the fingerprint registered as a duress FP is authenticated

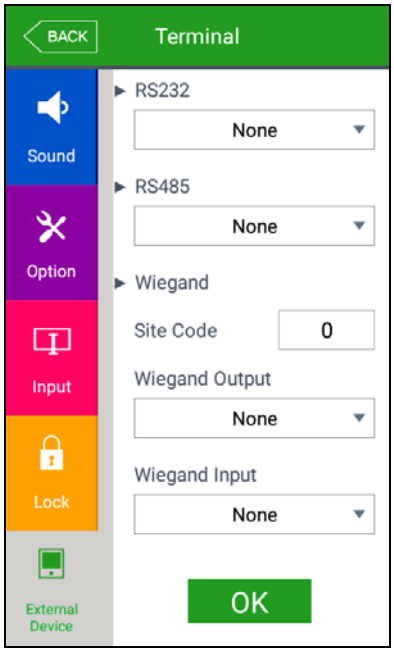
▶Lock 1 duration (ms)
When Lock 1 is set 'Strike/Auto/OK', it determines the signaling time. Because it is set in ms unit, if you want to set 3 seconds, you should set 3000. The strike type means the time until the door is locked again when opening the door after authentication.

▶Lock 2 duration (ms)
It sets the signaling time when Lock 2 is set 'Authentication failure notification'.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return. Because it is set in ms unit, if you want to set 3 seconds, you should set 3000.

3.7.5. External Device

If you select the **[Terminal]** → **[External device]** in the main menu, the following window appears.



▶Basic setting : Same with the window at the left side

▶RS232: It sets the device connected to RS232 port

-None: When there is no device connected to the RS232 port

-Ticket Format1/ Ticket Format2: The authentication result is printed when the authentication is successful. The terminal ID, user ID, authentication time, and authentication mode are printed by the printer connected to the RS232 port.

The printing format differs as per the setting, and when setting as **[Ticket Format2]** the "text for meal printer" which was set from the terminal option, becomes the title on the top side. The printer used to print ticket is "SRP-350" serial type model.

▶RS485: It sets the connecting device to RS485 port.

- None: When there is no device connected to RS485.
- LC010: When LC010 is connected.
- LC015: When LC015 is connected
- Reference: If you set DM0: [Door Open NO] or [Door Open NC], when using LC010, LC015, it gets the status of door open via DM0. If you want to get the status of door open from the controller, you shouldn't set DM0.

▶Site code

It sets the site code value sent in Wiegand output below.

▶Wiegand Output

It is used only when the special controller is equipped running by the Wiegand input. When the authentication is finished, the data of the following format is sent to the Wiegand port of the terminal.

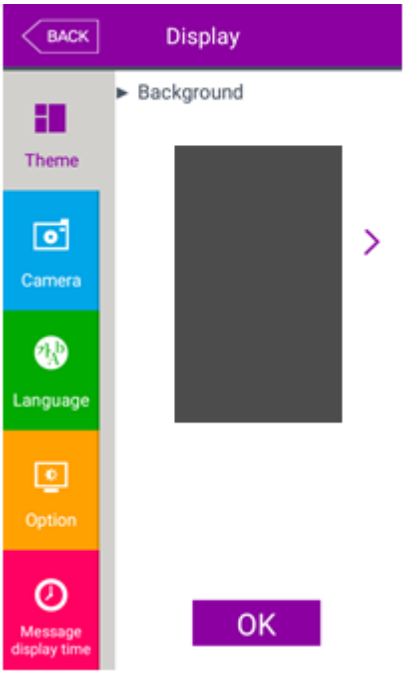
None	General case. It does not use Wiegand out port.
26bit	Because it sends “Site code [1byte] + User ID [2 bytes]”, set the user ID less or equal than 4 digits. Send example) In case of SiteCode:045(2Dh), UID:6543(198Fh) → 1 00101101 0001 1001 10001111 0
34bit	Because it sends “Site code [1 byte] + User ID [3 bytes]”, set the user ID less or equal than 7 digits. But, if the user ID is 8 digits, ignore site code and send only the “User ID [4byte]”. Send example) SiteCode:001(1h), UID:123456(1E240h) → 0 00000001 00000001 11100010 01000000 0
Custom	It is set by the user definition, which only can be set in the server, and the setting type only can be inquired in the terminal.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.8. Display

3.8.1. Theme

If you select **[Display] → [Theme]** in the main menu, the following window appears.

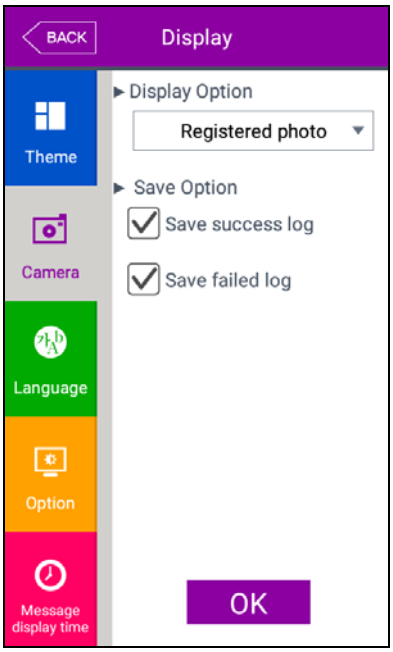


▶Basic setting: Same with the window at the left side.

▶Background
Since the camera is basically displayed, it is not available to select the background.

3.8.2. Camera

If you select the **[Display]** → **[Camera]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side.

▶Display Option

Select the image displayed in the message window of authentication success

- None
- Registered photo
- Authentication method: Image stands for each authentication method

▶Save success log

If it is checked (☑), the camera image is captured as image log when the authentication was successful.

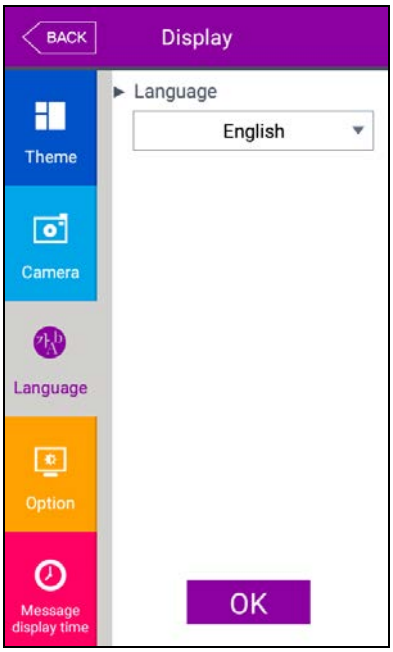
▶Save failed log

When it is checked (☑), the camera image is captured as image log when the authentication was failed.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.8.3. Language

If you select the **[Display]** → **[Language]** in the main menu, the following window appears.



▶Basic setting: 'English'

▶Language

If you change the language and click 'OK' button, the voice message and language are changed to the set language.

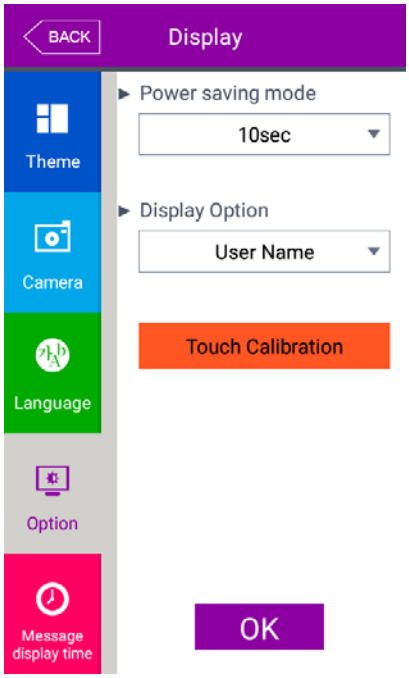
If you want to cancel and move to the upper menu, click **[Back]** button.

※ Supporting languages

English, Korean, Japanese, Portuguese, Chinese(Traditional), French, Chinese(Simplified), Spanish, Polish, Persian, German

3.8.4. Option

If you select **[Display]** → **[Option]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side.

▶Power saving mode (5sec ~ 10min)
If there is no input for set duration, the LCD screen is turned off automatically. But, if you set 'None' the LCD is always turned on.

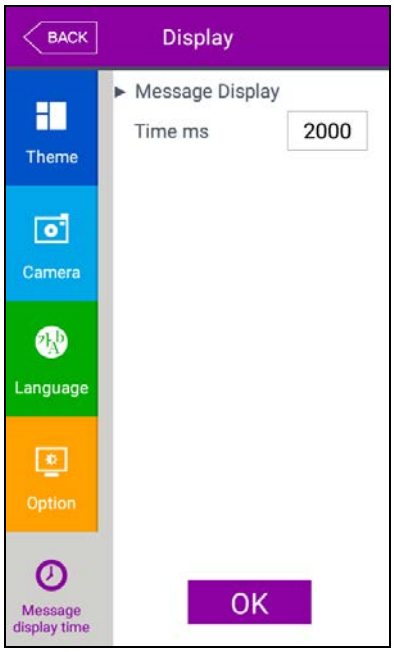
▶Display Option
It sets what will be shown at the LCD screen when the authentication is successful.
- None: The authentication result [Success/Failure] is only represented.
- User ID
-User Name: Representing user ID if it is not registered. (In this case, added "ID" in order to differentiate with name)
- Social No: Representing user ID if it is not registered. (In this case, added "ID" in order to differentiate with employee's number)

▶Touch Calibration
This feature is to calibrate the coordinates of the touch screen.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.8.5. Message display time

If you select the **[Display]** → **[Message display time]** in the main menu, the following window appears.



▶Basic setting: Same with the window at the left side.

▶Message Display (ms)

It sets the time for which the authentication result window to be displayed.

0~5000 is available for the value, and the authentication result window appeared and disappear for the duration.

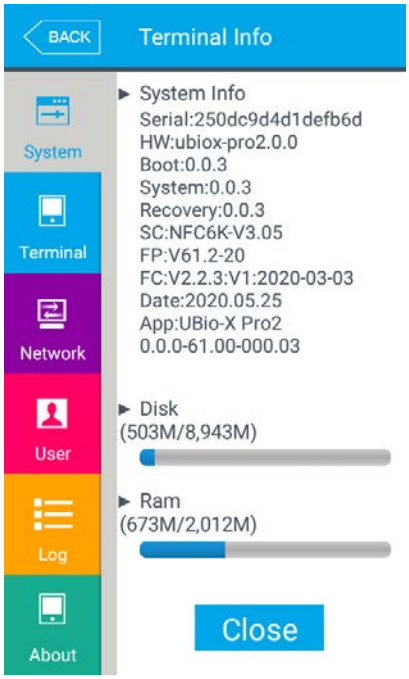
Because it is set in millisecond, if you want to set 2 seconds, you should set 2000.

Click **[OK]** button to apply the set value, and click **[Back]** button to cancel and return.

3.9. Terminal Info

3.9.1. System

If you select the **[Terminal info] → [System]** in the main menu, the following window appears.



▶System info
The hardware and firmware version of terminal is shown.

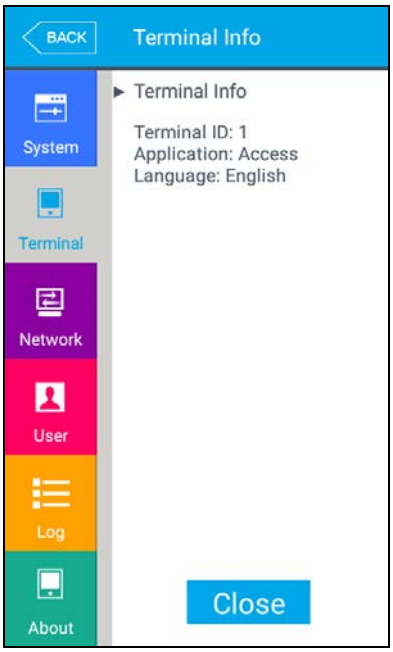
▶Disk (using size / Total size)
It shows the using size of the hard disk.
If the using size is high, it is represented in red.

▶Ram (using size / Total size)
The using size of RAM among the all size is represented.
If the using size is high, it is represented in red...

Click **[Back]** button to finish the inquiry and move to the upper menu. Click the menu on the left side to inquire additional item.

3.9.2. Terminal

If you click the **[Terminal info]** → **[Terminal]** in the main menu, the following window appears.



▶Terminal info

It represents the option setting value of the terminal.

Click **[Close]** or **[BACK]** button to finish the inquiry and move to the upper menu.

3.9.3. Network

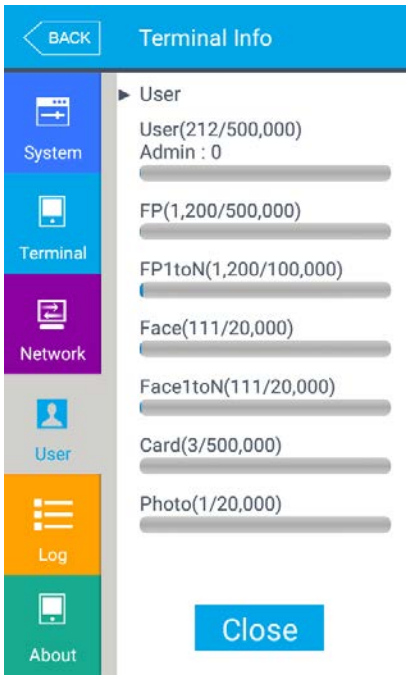
If you select the **[Terminal info] → [Network]** in the main menu, the following window appears.

▶Network info
It shows the setting value of the terminal.

If you want to finish the inquiry and move to the upper menu, click **[CLOSE]** or **[Back]** button.

3.9.4. User

If you select the **[Terminal info]->[User]** in the main menu, the following window appears.



▶User

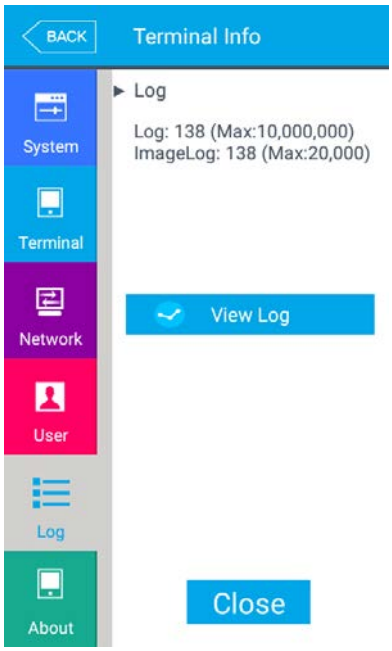
- User: The number of users registered (including administrator)
- Admin: The number of the administrators registered.
- FP: The number of all the fingerprints registered.
- FP 1toN: The number of fingerprints which can be authorized by 1:N.
- Face: The number of the users who registered the face
- Face 1toN: The number of users who can be authorized by 1:N
- Card: The number of cards registered
- Photo: The number of users who registered the picture

(Max means the maximum number of registrations for each item.)

Click the **[Close]** or **[Back]** button to finish the inquiry and move to the upper menu.

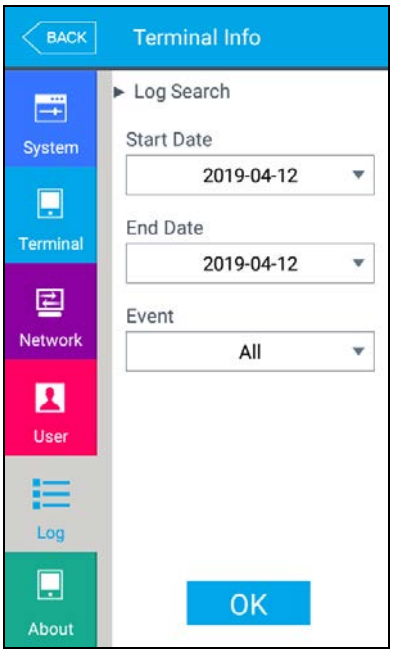
3.9.5. Log

If you select the **[Terminal info] → [Log]** in the main menu, the following window appears.

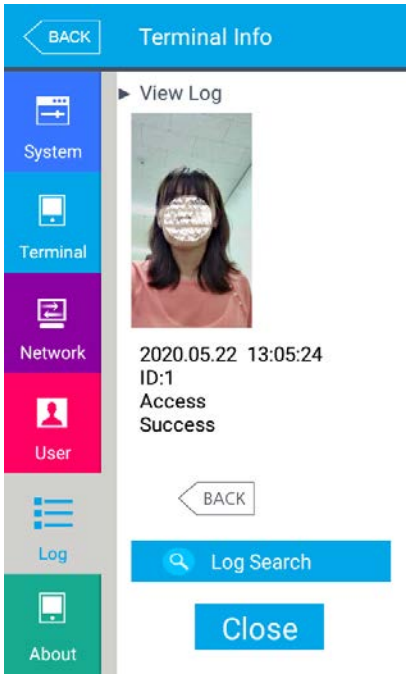


▶Log
Log: The number of logs saved in the terminal
Image Log: The number of image logs saved in the terminal.
(Max means the maximum number of items which can be saved in each item.)

▶View Log
Displays log time and authentication result



▶Log Search
To search log, follow the following steps,
[Terminal Info] → [Log] → [View Log] → [Log Search].
And then set the Start Date, End Date and Event criteria and click **[OK]**.

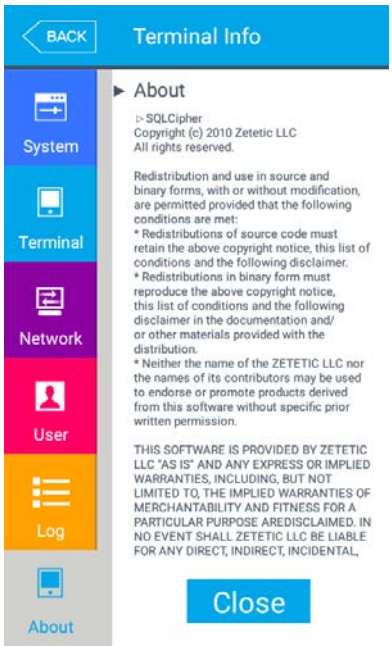


▶View Log
Log search result shows the information such as the date, time, ID and access result (success or failure). Click **[BACK]** or **[NEXT]** button to see the search information.

If you want to finish the inquiry and move to the upper menu, click **[Close]** or **[BACK]** button.

3.9.6. About

If you select the **[Terminal info] -> [About]** in the main menu, the following window appears.



▶About
It shows the license information applied in the terminal.

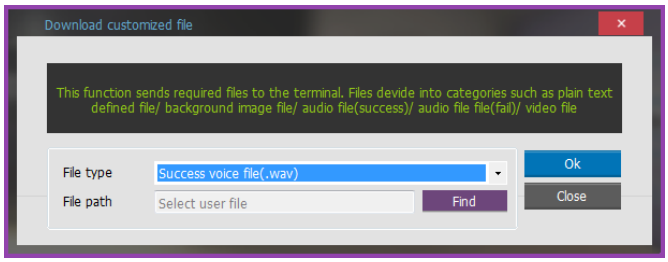
If you want to finish the inquiry and move to the upper menu, click **[Close]** or **[Back]** button.

3.11. Download the user file

If needed, it is the feature that the user can change the voice message.
You can download or change it after downloading the user file from UNIS server program.

3.11.1. Change the voice message

If you select the 'Download customized file' in the UNIS program, the following window appears.



If you select 'Sound file in success (.wav)' as the file type and click 'Send' button after selecting the sound file (.wav or mp3), the terminal selecting window appears. If you select the terminal in the terminal list window and click the 'Send' button again, the file is sent and the result of download appears.

In this time, the file name should be less than 15 letters (English, 15byte) including extension and mp3 format.

In case of sound in failure also can be changed by selecting 'Sound file in failure(.wav)' with the same manner.

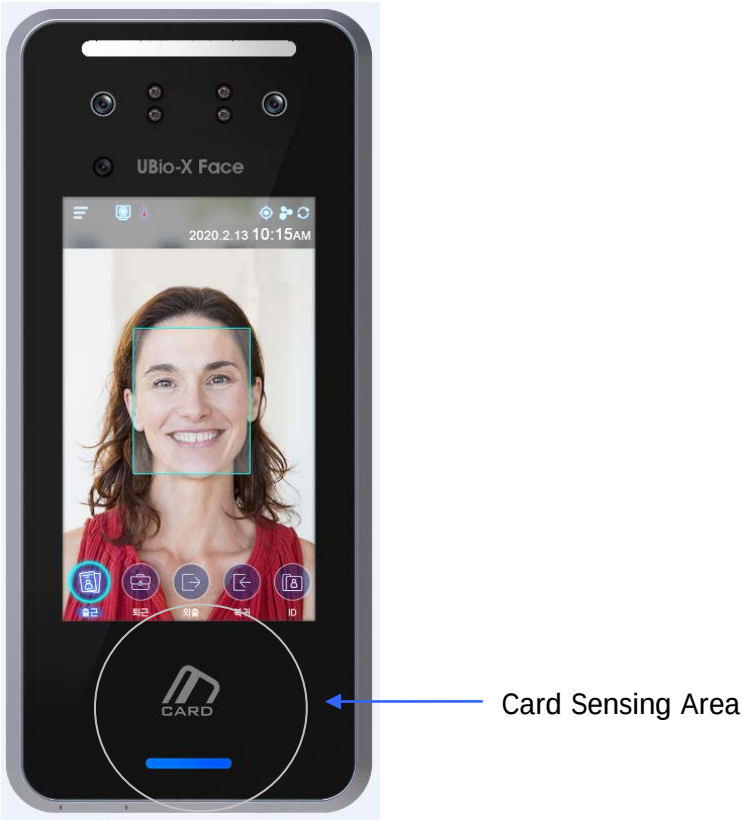
If you want to change back to the basic sound from the user's sound, uncheck the checkbox "User Voice" at the 3.7.1 [**Terminal**] → [**Sound**].

.

4. How to use terminal

The background image and composition of the basic window can be changed according to the administrator's setting. In addition, if the administrator set the screen saver time, the LCD screen is turned off automatically if there is no action for set time, and when the user accessed to the terminal, tried the authentication with fingerprint/card, or touched the main screen, the LCD screen is turned on automatically.

4.1. How to change Auth mode

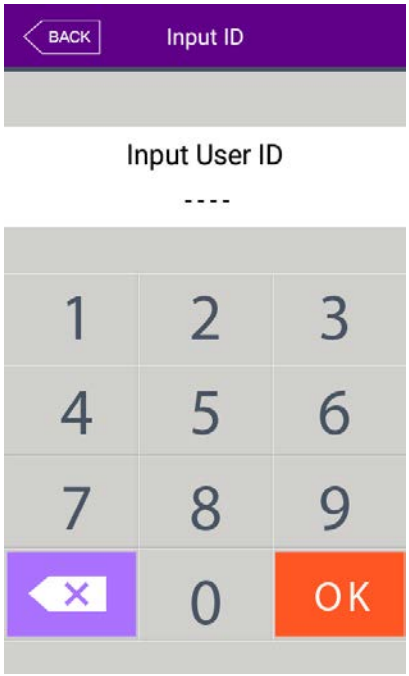


< Fig. 4-1>

Select the function key button among Attend **[F1]**, Leave **[F2]**, Out **[F3]**, In **[F4]** on the screen for choosing the function mode before authentication.

4.2. How to input user ID

If you click the button **[ID]** on the basic window, following the window “Input User ID” as below.



Enter the user ID to be certified and click **[OK]** button, then the input screen of fingerprint, face, card, or password depending on the authentication method of the user.

4.3. Authentication

4.3.1. Face authentication

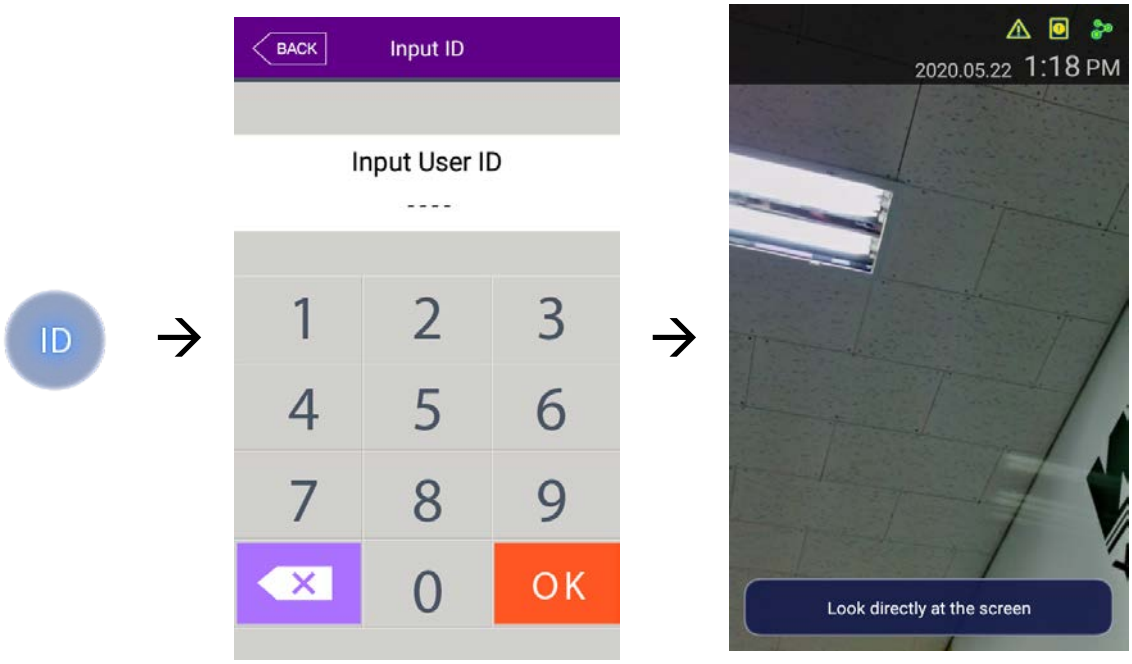
▶1:N authentication (Identification)

Try authentication by staring at the camera so that the face appears on the LCD screen.

▶1:1 Authentication (Verification)

As shown in the following figure, enter your ID first by clicking **[Input ID]** button, and when the face input message appears, locate your face until the LCD guideline is turned blue, and gaze the camera and stop moving.

If the terminal cannot detect the face properly, the 1:1 Authentication will be canceled with the message box is changed to gray after 20 seconds.



4.3.2. Fingerprint authentication

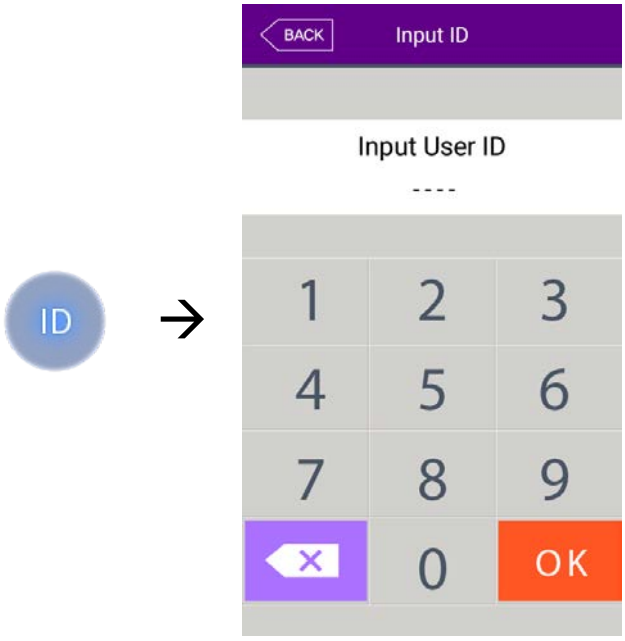
▶1:N Authentication (Identification)

If you put your fingerprint on the fingerprint sensor at the basic window, the fingerprint is entered with the light on the sensor with beeping. Do not take off your finger until the light of the sensor turns off completely.

▶1:1 Authentication (Verification)

As shown in the following figure, enter your ID first by clicking the **[Input ID]** button, and input your fingerprint when the fingerprint entering window appears and the light is turned on at the fingerprint sensor.

Do not take off your finger until the light of the sensor turns off completely.

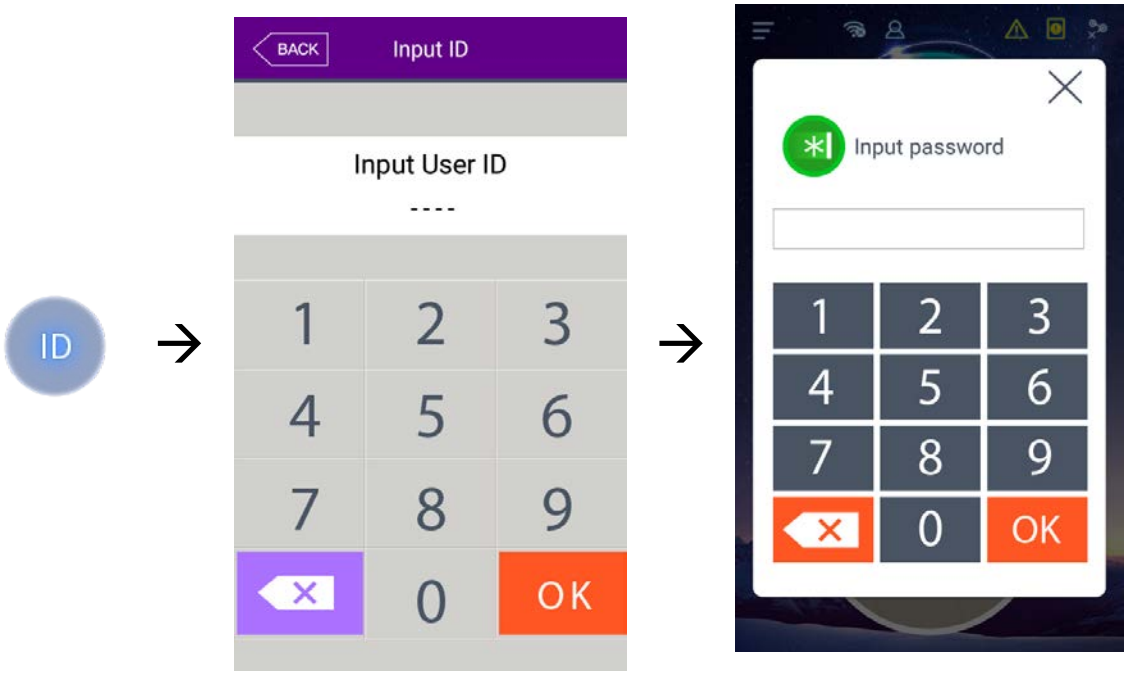


4.3.3. Card authentication

Place the card on the card picture <Fig. 4-1>.

4.3.4. Password authentication

Input your ID by clicking **[ID input]** button as follows and input password when the password input window appears.



4.3.5. Multi-mode authentication

For user who needs to authenticate via more than 2 methods such as –card & fingerprint OR card & fingerprint & face, the preferential precedence of the authentication after the ID is typed is as follows: card→fingerprint→face→password in order.
This type is activated even if face or fingerprint authenticates firstly.

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.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

"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 possibilityof exceeding the FCC radio frequency exposure limit.

Contains FCC ID: 2AEEY-PBLN51822M

UNIONCOMMUNITY Co., Ltd.
Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu, Seoul, Korea (zip code: 05836)
Tel: +82-2-6488-3000, Fax: +82-2-6488-3099,
E-Mail :sales@unioncomm.co.kr; http://www.unioncomm.co.kr