

UBio-X Pro User Guide

Version Eng-1.14



UNION
COMMUNITY

Distributed by
genie

Copyright 2000 By Union Community Co., LTD.

<Revision History>

Version	Date	Description	Firmware Version
1.00	2018-12-27	Initial Release	
1.01	2019-02-07	Modification for issues from RQA	
1.02	2019-03-07	Change the screen shot for Terminal Info	
1.03	2019-03-15	Remove the enrollment auto sensitivity Change the screen shots for Meal Management	
1.04	2019-04-15	Add the contents for setting of face authentication trial	
1.05	2019-05-10	Modify the face authentication specification (p21)	
1.06	2019-07-02	Modify the face authentication specification (p21)	
1.07	2019-07-22	3.11.1 Remove the background change category	
1.08	2019-09-05	3.7.5. Add RS485 option in 'External Device'.	
1.09	2019-12-31	3.7.5. Modify RS485 option in 'External Device'.	
1.10	2020-01-08	3.3.1.4. Face registration – Modify the image and contents. 3.6.3. Face – Modify the image and contents. 3.8.1. Theme – Add customized theme.	
1.11	2020-04-14	3.6.3. Face – Modify the image and contents. 3.8.1. Theme – Modify customized theme.	
1.12	2020-09-17	3.6.3. Face – Modify the image and contents. 3.9.1. System – Change the image.	
1.13	2020-10-07	3.5.2. Function key – Add the extended key.	
1.14	2021-04-05	3.3.1.5. Password registration – Add duress password	

< 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.
-

Contents





<Revision History>	2
< Glossary>	3
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
1.7. Proper fingerprint registration and input methods	14
2. Product introduction	16
2.1. Product characteristics	16
2.2. Product components	19
2.2.1. Standalone use (Access)	19
2.2.2. Connected with Server (Access, Attendance, Meal management)	19
2.3. Product specification	20
3. Environment setting	21
3.1. Checks before setting the environment	21
3.1.1. Entering the menu	21
3.1.2. Administrator authorization	21
3.1.3. How to enter the menu without administrator authorization	22
3.1.4. How to save the set values	23
3.2. Menu composition	24
3.3. User Management	27
3.3.1. Add	27
3.3.1.1. Photo registration	29
3.3.1.2. Name registration	29
3.3.1.3. Fingerprint registration	30
3.3.1.4. Face registration	33
3.3.1.5. Password registration	35
3.3.1.6. Card registration	35
3.3.1.7. Options for authorization	37
3.3.1.8. How to set 'AuthType'	37
3.3.1.9. Save	38
3.3.2. Delete	39
3.3.3. Modify	40
3.3.4. Delete all	42
3.3.5. View	42
3.4. Network setting	44
3.5. Application mode	46
3.5.1. Application	46
3.5.1.1. Access or TnA setting	46
3.5.1.2. Meal setting	48
3.5.2. Function key	48
3.6. System	49
3.6.1. System	49
3.6.2. Finger	50
3.6.3. Face	52

3.6.4. Auth	53
3.6.5. Date/Time	54
3.6.6. Database	55
3.6.6.1. Delete all the users.....	55
3.6.6.2. Delete setting	56
3.6.6.3. Delete Log.....	56
3.6.6.4. Delete image log	57
3.6.6.5. Factory init	57
3.7. Terminal	58
3.7.1. Sound	58
3.7.2. Option.....	58
3.7.3. Input	60
3.7.4. Lock.....	62
3.7.5. External Device	63
3.8. Display	65
3.8.1. Theme	65
3.8.2. Camera.....	66
3.8.3. Language	67
3.8.4. Option.....	68
3.8.5. Message display time	69
3.9. Terminal Info.....	70
3.9.1. System	70
3.9.2. Terminal.....	71
3.9.3. Network	72
3.9.4. User.....	73
3.9.5. Log	74
3.9.6. About	75
3.10. SD Card.....	76
3.11. User's file download	78
3.11.1. How to change voice sound	78
4. How to use terminal	80
4.1. How to change Auth mode	80
4.2. How to input user ID	81
4.3. How to authorize	81
4.3.1. Face authorization	81
4.3.2. Fingerprint authorization	82
4.3.3. Card authorization	83
4.3.4. Password authorization	83
4.3.5. Multi-mode authorization	84

1. Before use






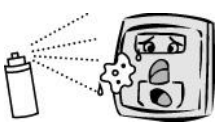

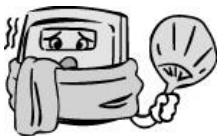
1.1. Safety Precautions

● Warning

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

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

● Cautions

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

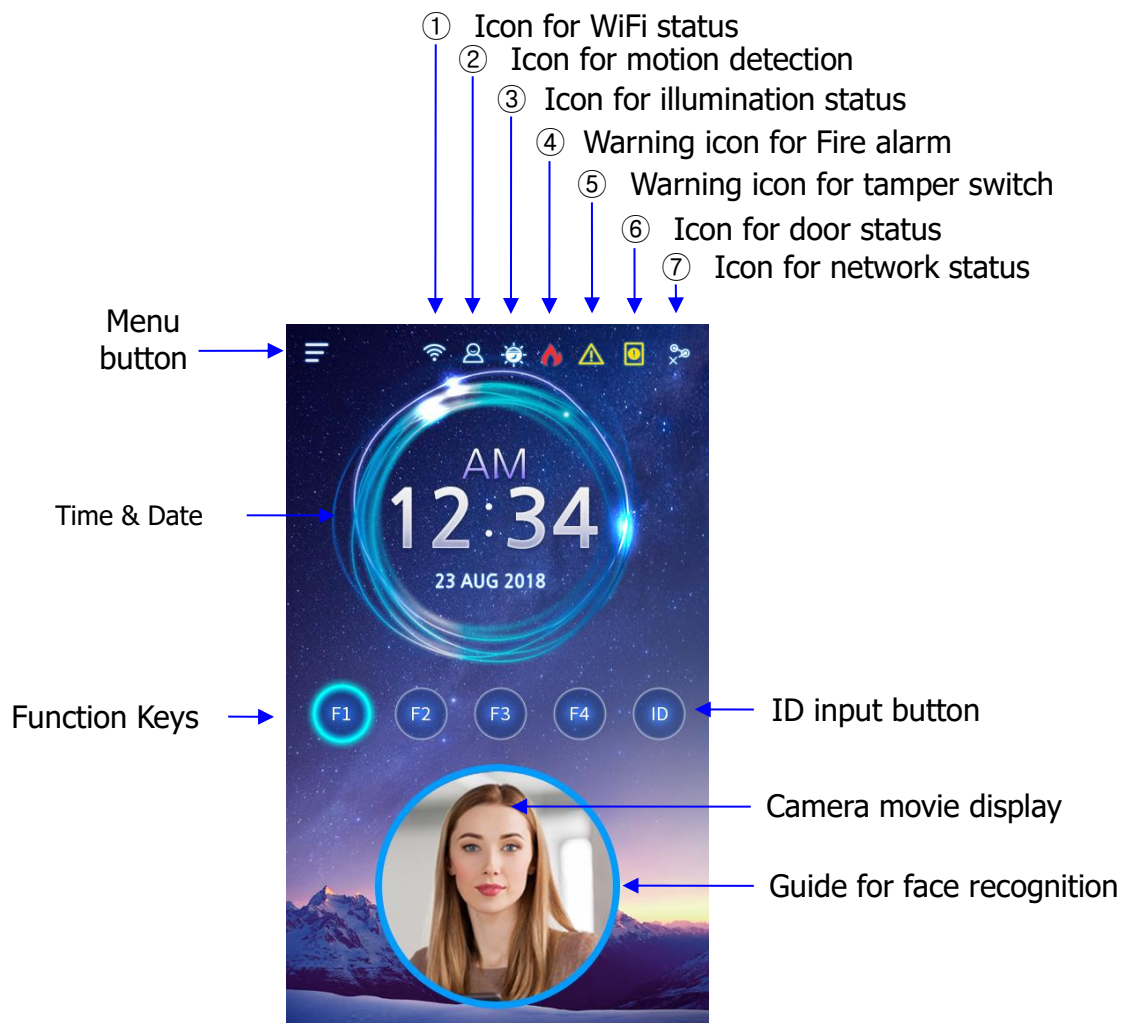
- If the above cautions are ignored, it may result in property loss or human injury.

※ 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.






1.2. Specific names of the terminal











1.3. Windows after operation

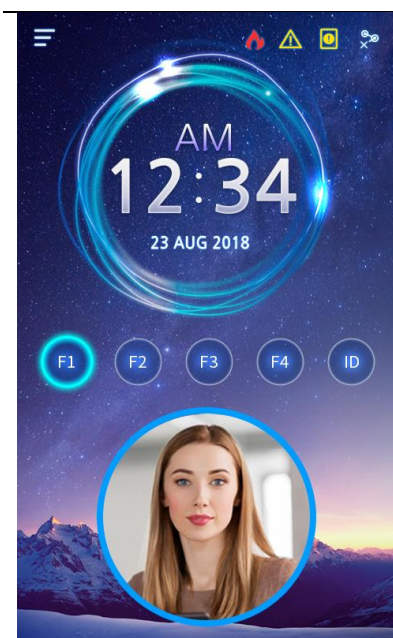


1.3.1. Icon

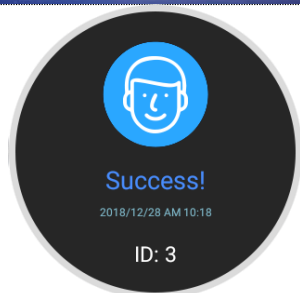
	None	: There is no connected WiFi dongle
① WiFi Status		: WiFi connection is not activated
		: WiFi connection is activated
② Motion Detection	None	: There is not detected any motion
		: Detect the motion
③ Illumination Status	None	: Detect the high illumination status
		: Detect the low illumination status
④ Fire Alarm		: Fire Alarm is activated (on connecting Fire detection sensor)
⑤ Tamper	None	: Normal status

Switch		: Tamper switch is activated (Terminal is disassembled)
⑥ Door Status		: Door status is not sensed
		: Door is closed
		: Door is opened
		: Door is opened abnormally
⑦ Network Status		: There is not connected LAN cable
		: Disconnected to the server even LAN cable is connected
		: Connected to the server (On line)

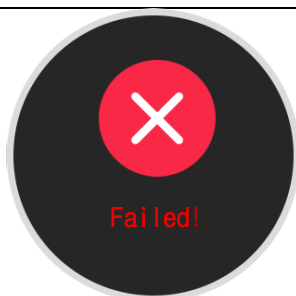
1.3.2. Message



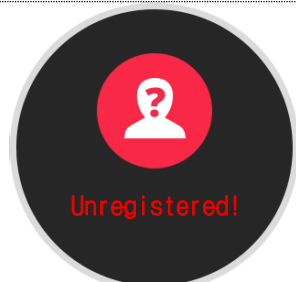
- Basic Window



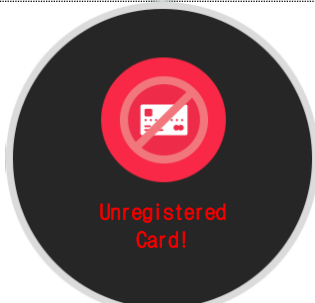
- When authorization is successful



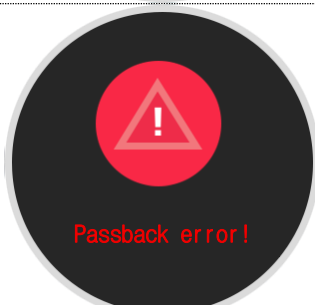
- When authorization is failed



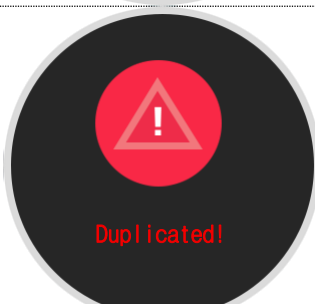
- When unregistered user ID is entered



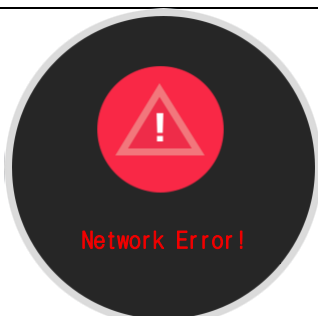
- When unregistered card is entered



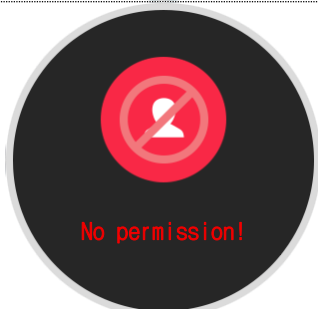
- Passback error when using anti-passback function



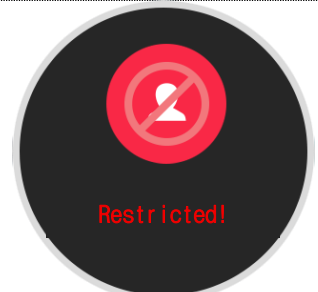
- When a user tried the authorization more than twice in one meal time when using as meal management



- When the server does not respond during the authorization attempt to the server
- When the network is disconnected during the authorization attempt to the server



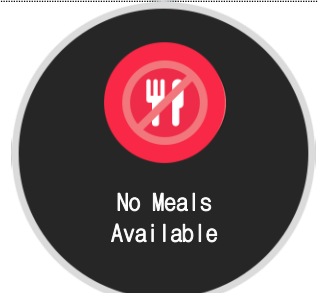
- Registration without authorization right or authorization attempt when the entrance is not permitted



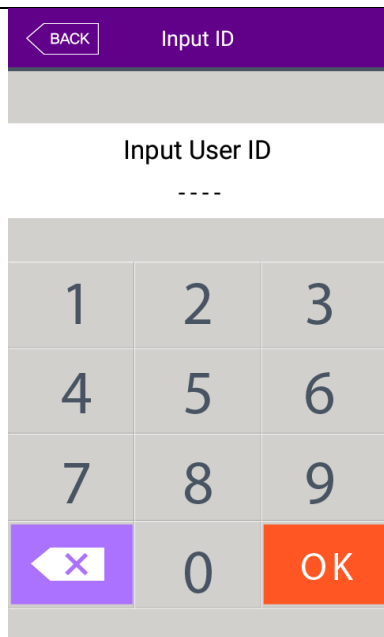
- When the user is designated in the blacklist



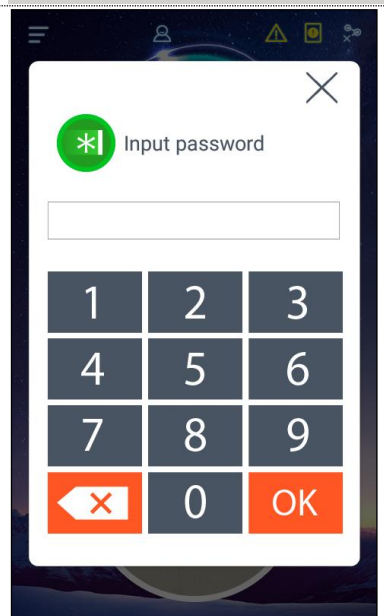
- When the terminal is set locked



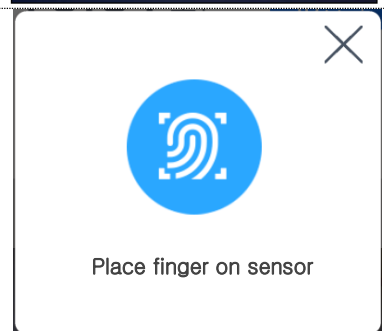
- When it is not the meal time when set in the meal personnel management



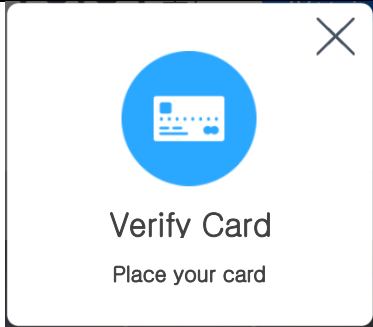
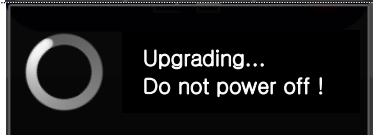
- The state waiting for the input of the user ID



- The state waiting for the input of password



- The state waiting for the input of fingerprint

	<p>- The state waiting for the input of the card</p>
	<p>- When the terminal program is being upgraded (In this state, you should not turn off the terminal)</p>

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 reading card for the or fingerprint	When the card was read When the fingerprint was entered in the fingerprint window
Pi-pick	Notice for fail	When the authorization was failed (at Voice off)
Peek	Notice Success for	When the authorization 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 (Passport picture standard).
 - If you wear the glasses, you should register both pictures with and without glasses. But, if you change your glasses, you should repeat the registration procedures.

- Face authorization method

You can select two modes as the face authorization method.

- Normal mode: When the user gets close within 1.5m, the tilting function of the camera is operated by recognizing the face of user. When the user is within 50~70cm, the face authorization is fulfilled.
- Fixed mode: It has the fastest authorization speed, but because it does not include the tilting function, please locate the user face at the LCD guideline by maintaining the distance between the terminal and user in 50 cm.

- 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.

1.7. Proper fingerprint registration and input methods

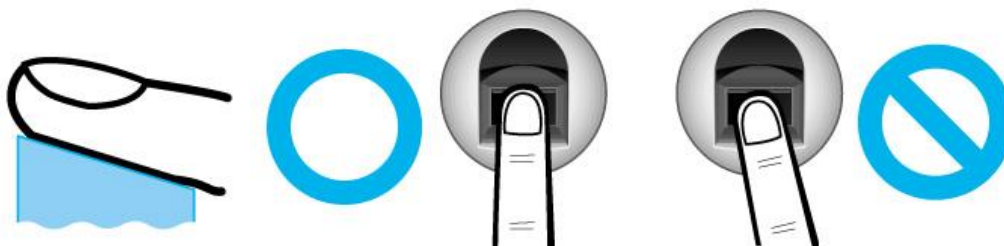
- Correct fingerprint registration methods

Place your index finger on the window just as you do with a finger stamp.

Do not use the tip of the finger.

Make sure the center of your finger touches the window.

(Please be cautious that you may result in low temperature burns when inserting finger.)



- Use your index finger if possible, it is the easiest for orientation and guarantees a stable input method. Using the thumb or baby finger can be awkward and may result in a bad image.
-

- Check if your fingerprint is unclear or damaged.
It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case



- Be aware of certain fingerprint conditions

Depending on the user's fingerprint condition, some fingerprints may not be used or may cause an inconvenience.

- If the fingerprint is damaged or very unclear, then it cannot be recognized. Please use a password instead in this case.
 - **When a finger is dry, breathe on the finger for smooth operation.**
 - For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or very unclear. It is recommended to register their fingerprints every six months.
 - For the elderly, it may not be possible to register their fingerprints if there are too many fine lines on the fingerprints.
 - If fingerprints are very unclear, it may be convenient if you register 2~3 fingerprints.
 - It is recommended that you register more than 2 fingerprints.
-

2. Product introduction

2.1. Product characteristics

- Multi-Modal product with which the user can use both face and fingerprint authorization functions together.
- Superior ability for the face recognition under external light condition (30,000 lux)
- FHD(2M) Display resolution is adapted.
- The face recognition is possible even in the dark place with the illumination sensor and dual camera (color & IR) and saving the discriminable log images.
- RF(125kHz) and Smart Card(13.56MHz) can be used at the same time.
- Easy authorization with the face or 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
- Entrance management system with 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 authorization server. High speed with 10/100 Mbps Auto Detect and easy management and monitoring with network.

● Various registration and authorization methods

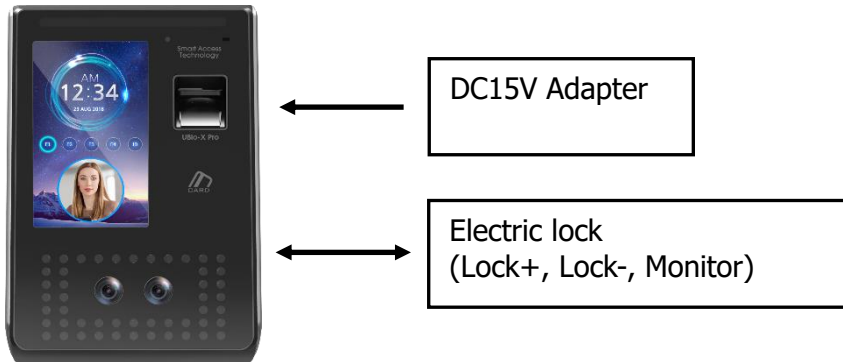
Face	Face registration Face authentication
Fingerprint	Fingerprint registration Fingerprint authentication
Card	Card registration Card authentication
Password	Password registration Password authentication
Card or Fingerprint	Card, fingerprint registration Card or fingerprint authentication Fingerprint 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

	<p>Password authentication after ID input</p>
<p>Card & Password</p>	<p>Card, password registration Password authentication after card authentication ID input > Card authentication > Password authentication</p>
<p>Fingerprint or Password</p>	<p>Fingerprint, password registration Fingerprint authentication Fingerprint authentication after ID input, if failed, password authentication is possible.</p>
<p>Fingerprint & Password</p>	<p>Fingerprint, password registration Password authentication after fingerprint authentication ID input > Fingerprint authentication > Password authentication</p>
<p>Card or Face</p>	<p>Card, face registration Card or face authentication Face authentication after ID input</p>
<p>Card & Face</p>	<p>Card, face registration Face authentication after card authentication ID input > Card authentication > Face authentication</p>
<p>Face or Password</p>	<p>Face, password registration Face authentication ID input > Face authentication > if failed, password authentication</p>
<p>Face & Password</p>	<p>Face, password registration Password authentication after face authentication ID input > Face authentication > Password authentication</p>
<p>Fingerprint or Face</p>	<p>Fingerprint, face registration Fingerprint or face authentication ID input > Fingerprint authentication > if failed, face authentication</p>
<p>Fingerprint & Face</p>	<p>Fingerprint, face registration Face authentication after fingerprint authentication ID input > Fingerprint authentication > Face authentication</p>
<p>Card or Fingerprint or Face</p>	<p>Card, fingerprint, face registration Card or fingerprint or face authentication ID input > Fingerprint authentication > if failed. Face authentication</p>
<p>Card & Fingerprint & Password</p>	<p>Card, fingerprint, and password registration Card and password authentication after card authentication ID input > Card authentication > Password authentication</p>
<p>Card & Face & Password</p>	<p>Card, face, and password registration Face and password authentication after card authentication ID input > Card authentication > Face and card authentication</p>
<p>Card</p>	<p>Card, fingerprint and face registration</p>

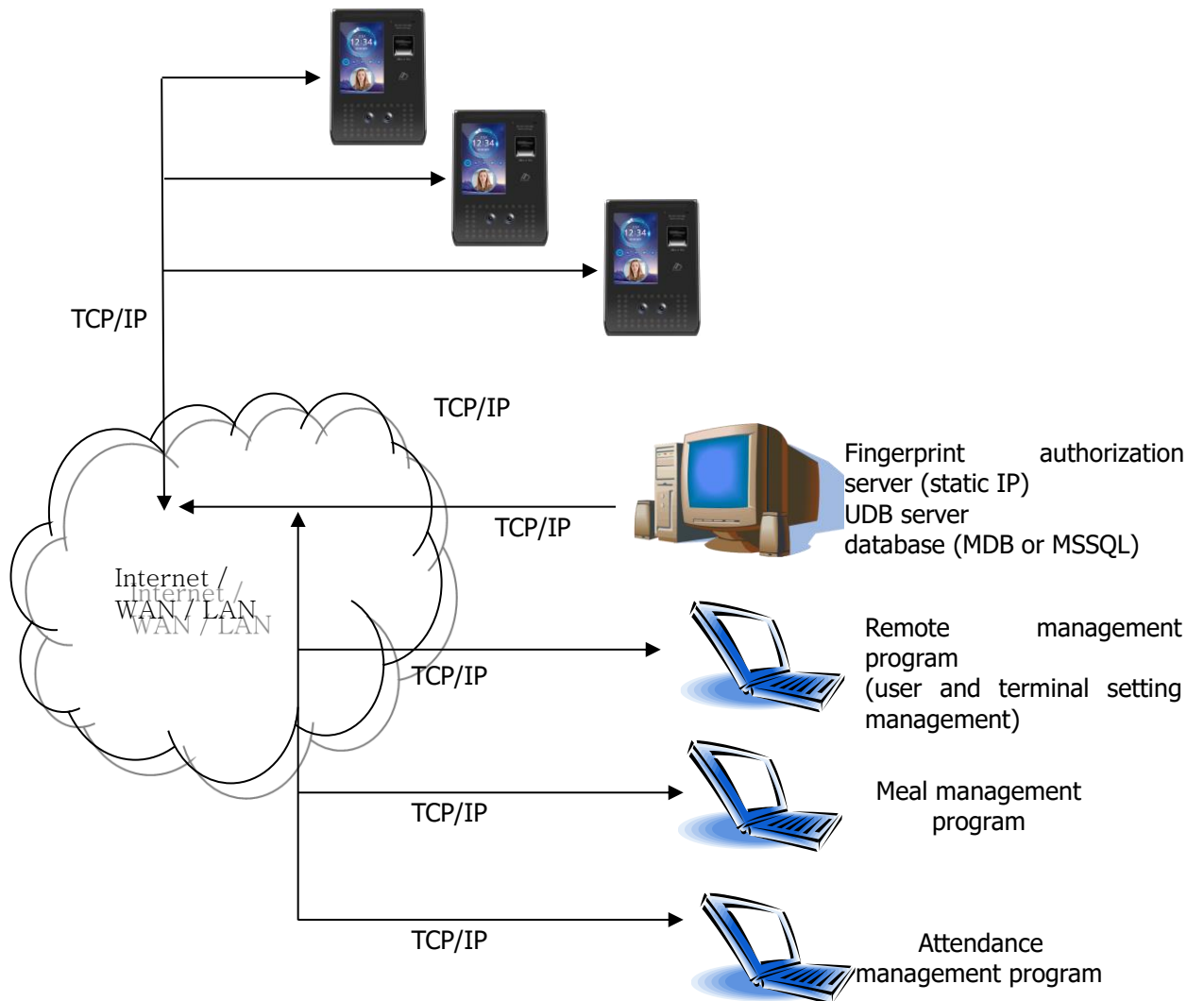
& Fingerprint & Face	Fingerprint and face authentication after card authentication ID input > Card authentication > Fingerprint and face authentication
Fingerprint & Face & Password	Fingerprint, face, password registration Face and password authentication after fingerprint authentication ID input > Fingerprint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

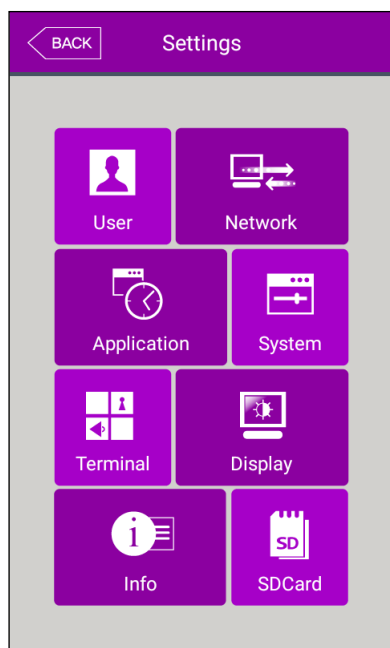
Types	SPEC	REMARK
CPU	1GHz Quad Core CPU	
LCD	5.0 inch Touch LCD(480*800)	
MEMORY	16G Bytes Flash	
	2GBytes RAM	
External SD Card support	Backup data / Upgrade firmware	
Camera	Dual Camera (Color & IR)	
Capacity	500,000 User / 500,000 Card 500,000 Finger (1:N→1:100,000) 200,000 Face (1:N→1:30,000) 10,000,000 Log / 20,000 Image Log	
Fingerprint sensor	Optical	
Scan Area / Resolution	20 * 20mm / 500 DPI	
Temperature / Humidity	-20 ~ 60°C / 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 (Also for Lock Control)	
Communication Port	TCP/IP (10/100Mbps)	Communication with Auth Server
	RS-232	Ticket Printer
	RS-485	Communication with Controller
	Wiegand In/Out	Communication with Card reader or Controller
Card Reader	125KHz RF / 13.56MHz Smart simultaneous use (1 Sam socket) HID 125K Prox card (option) HID iClass Card (option)	option
SIZE	88.0mm * 175.0mm * 43.4mm	

3. Environment setting

3.1. Checks before setting the environment

3.1.1. Entering the menu

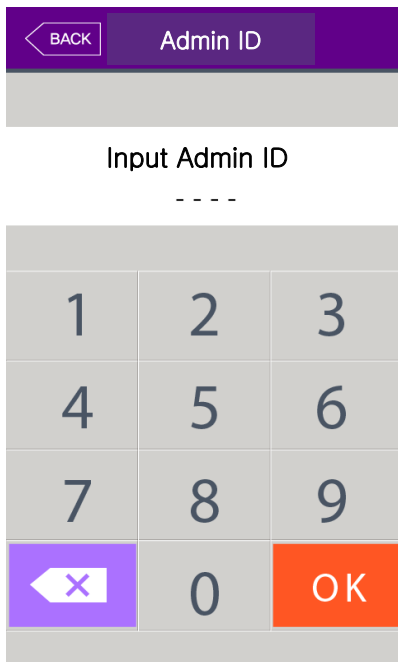
If you click the [⚙️] icon at the basic window, you can enter the main menu window as follows.



You can enter the subdivision menu by clicking each button.

3.1.2. Administrator authorization

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



► Administrator authorization

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

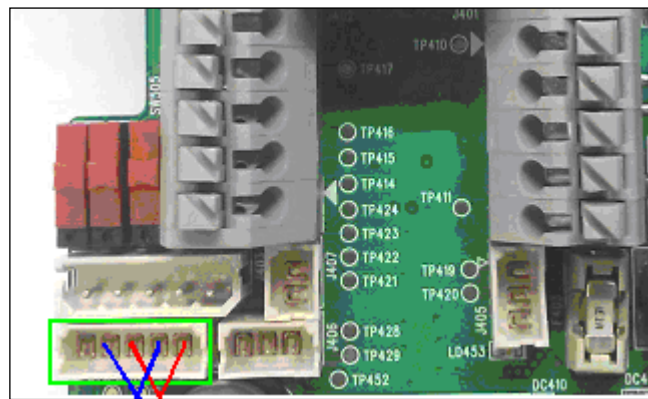
The administrator authorization only appears when the registered administrator exists. The authorization is fulfilled only once when entering the menu mode and you can access to all the menu until you quit the main menu.

<Fig. 3-2>



3.1.3. How to enter the menu without administrator authorization

It is how to enter the menu when the fingerprint or face authorization 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.



<Fig3-3>

- ③ Click the icon  at the basic window to enter the administrator authorization 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.

3.2. Menu composition

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

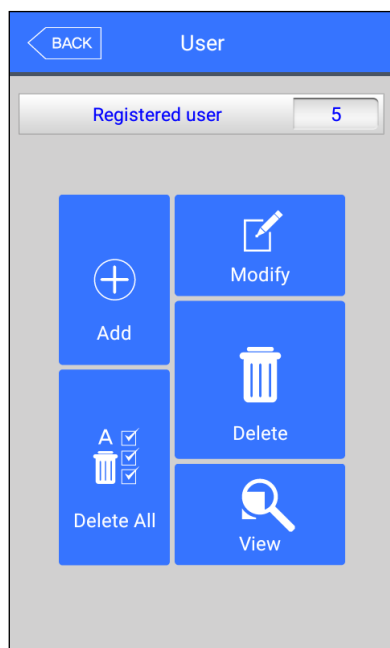
		<ul style="list-style-type: none"> <input type="checkbox"/> Password <input type="checkbox"/> Name Number of Fingers [1~10]
	2. Finger	<ul style="list-style-type: none"> ▶ 1:N Level [3~9] ▶ 1:1 Level [1~9] ▶ Fake Finger Detection ▶ FP template format <ul style="list-style-type: none"> <input type="checkbox"/> Check similar FP <input type="checkbox"/> Multi FP <input type="checkbox"/> Enable 1:N
	3. Face	<ul style="list-style-type: none"> ▶ Matching Level [1~10] ▶ Authentication attempt (1:N) [1~10] ▶ Motion Detection Sensitivity ▶ System Optimization Mode
	4. Auth	<ul style="list-style-type: none"> ▶ Auth Type <ul style="list-style-type: none"> <input type="checkbox"/> FP Template Card <input type="checkbox"/> FACE 1:1 Only
	5. Date/Time	<ul style="list-style-type: none"> ▶ Time synchronization ▶ Display Format ▶ Set Date ▶ Set Time
	6. Database	<ol style="list-style-type: none"> 1. Delete all users 2. Delete setting 3. Delete Log 4. Delete Image log 5. Factory init
5. Terminal	1. Sound	<ul style="list-style-type: none"> ▶ Voice Volume ▶ Beep Volume ▶ Sound Option
	2. Option	<ul style="list-style-type: none"> ▶ Read Card number ▶ Card format <ul style="list-style-type: none"> <input type="checkbox"/> Lock terminal ▶ Card reader
	3. Input	<ul style="list-style-type: none"> ▶ M0 ▶ M1 ▶ M2 ▶ IO ▶ Warn door open (sec) <ul style="list-style-type: none"> <input type="checkbox"/> Tamper alarm
	4. Lock	<ul style="list-style-type: none"> ▶ Lock 1 Option ▶ Lock 2 Option ▶ Lock 1 duration (ms) ▶ Lock 2 duration (ms)

	5. External Device	<ul style="list-style-type: none"> ▶RS232 ▶RS485 ▶Wiegand Site Code Wiegand Output Wiegand Input
6. Display	1. Theme	▶Background
	2. Camera	<ul style="list-style-type: none"> ▶Display Option ▶Save Option <ul style="list-style-type: none"> <input type="checkbox"/> Save success log <input type="checkbox"/> Save failed log
	3. Language	▶Language
	4. Option	<ul style="list-style-type: none"> ▶Power saving mode ▶Display Option ▶Touch Calibration
	5. Message display time	▶Message Display Time (ms)
7. Terminal Info	1. System	<ul style="list-style-type: none"> ▶System Info ▶Disk ▶Ram
	2. Terminal	<ul style="list-style-type: none"> ▶Terminal Info Terminal ID Application Language
	3. Network	<ul style="list-style-type: none"> ▶Network Info MAC <Ethernet> IP
	4. User	▶User
	5. Log	▶Log
	6. About	▶About
8. SD Card	1. Export	<ul style="list-style-type: none"> 1. User Data 2. Event Log 3. System Option 4. Export All 5. Picture
	2. Import	<ul style="list-style-type: none"> 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.

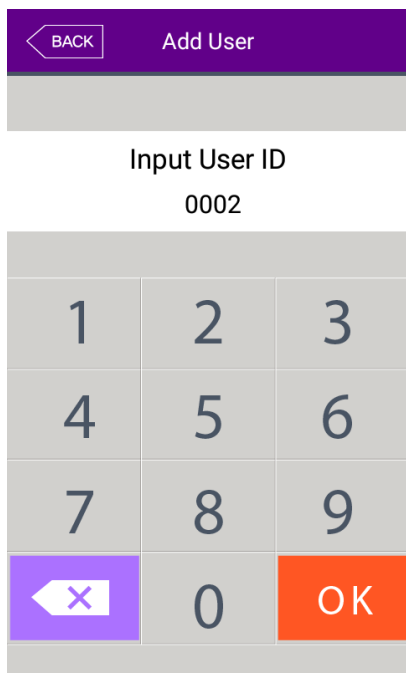


The number of all the users is shown at the top of screen including administrator.

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

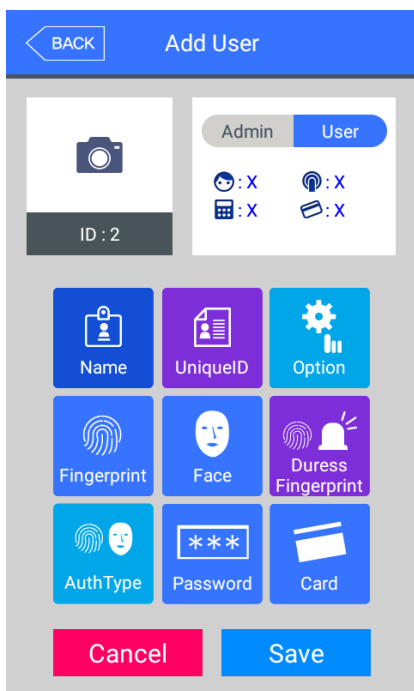


Input the user ID to be registered and click **[OK]** button.

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.



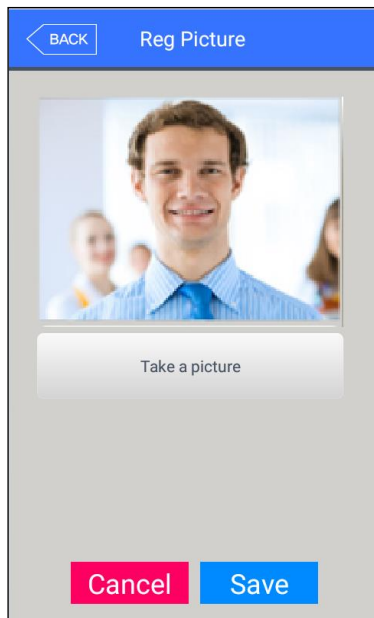
The icons in the left side mean as follows

- : 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 : 4** : User ID to be registered
- : 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

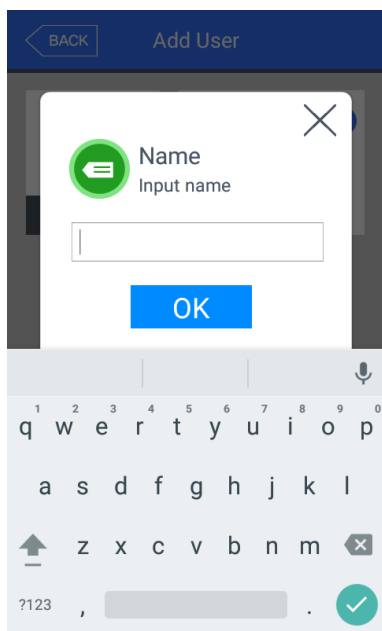


Register by clicking [📷] button at the [Add User] screen

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

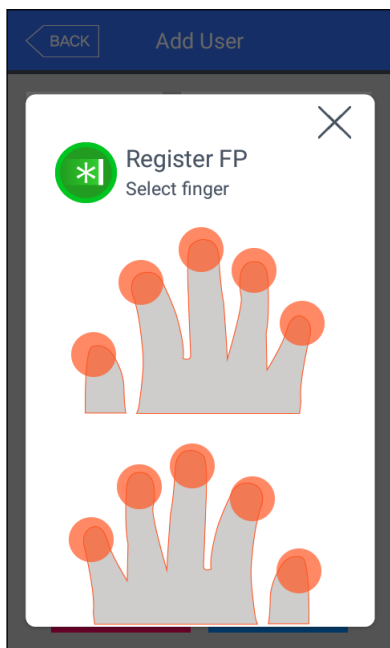


Register by clicking [Name] button in the [Add User] screen.

After entering name with the under keyboard, click [OK] button.

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

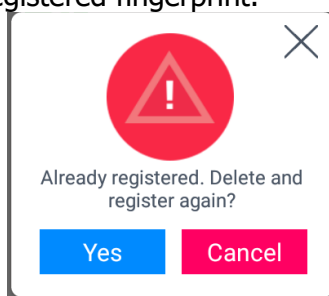
3.3.1.3. Fingerprint registration



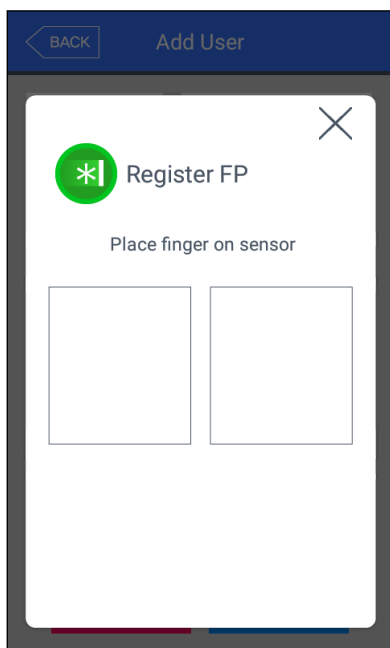
① Register by clicking **[Fingerprint]** button at the **[Add User]** screen.

Click [**X**] button to cancel the registration and return. Choose the finger to be registered when the left screen appears.

※ If you register the multiple fingers, the fingers already registered are represented by blue circle (●). And if the duress fingerprints are represented by violet circle (●). If you select the finger already registered, the following message appears, and if you select the re-registration, you can register again with deleting previously registered fingerprint.



※ When you authenticated with duress FP, the alarm message for Duress can be transferred to the server and you can output the dry contact signal if you set the duress FP alarm from the setting of Lock on the terminal menu. (Refer to 3.7.4.Lock.)

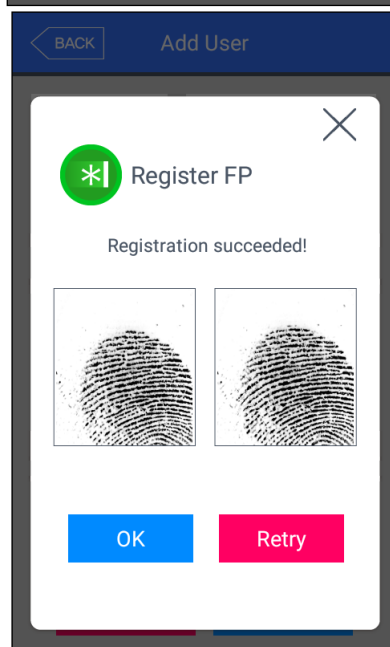


② Enter the fingerprint with referring '1.7 Proper fingerprint registration and input methods'. Enter the fingerprint twice according to the screen instruction as follows.

When the light is turned on at the fingerprint sensor with the message 'Register FP', put your finger on the input screen and wait for 2~3 seconds until the light is turned off.

③ When the message 'Enter the same fingerprint again' appears, enter the same fingerprint again.

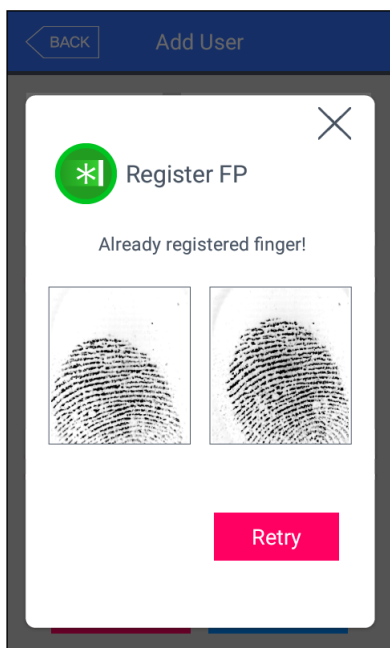
※ In the second fingerprint input after the first fingerprint, you should take off your finger from the screen once and input again.



④ The message of the left side appears when the input is completed. If you click **[OK]** button, the registration is completed and the screen is returned to the upper menu.

If you want to register again, you can click **[Retry]** button and then go through the registration process from ②.

But if you want to cancel the registration, you can click **[X]** button.



If it is similar with the fingerprint already registered, the message "Already registered finger!" appears like the left side, and you can start again from the procedure of ② if you click the **[Retry]** button.

You can click [~~X~~] button to cancel and return to the upper menu.

※ You can register 10 fingerprints at most for one ID, and you cannot register more than 10 IDs.

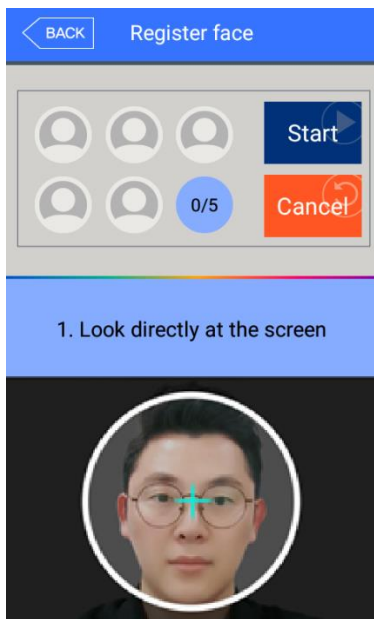
If the registration was failed 2~3 times despite the proper fingerprint registration method, it is recommended to use face, password, or card.

※ The similar fingerprint check on registration should be verified for the registered fingerprints on the terminal side only.

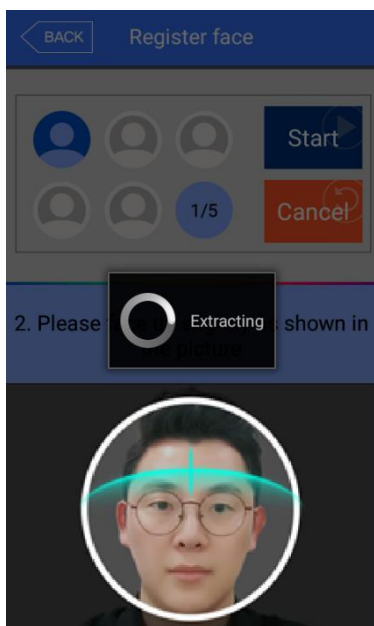
If the same fingerprint was registered from both terminal and server with the different User ID, server does not check the similarity for the retrieved fingerprint from the terminal. In this case, same fingerprint can be authenticated with the different user ID so you have to watch out this.

3.3.1.4. Face registration

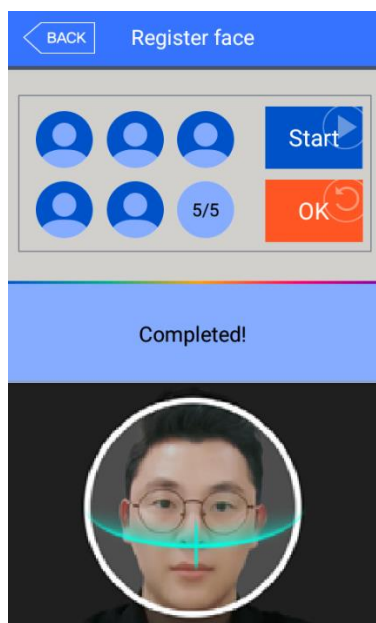
Register with referring '1.6. How to register and authorize the face properly'.



① Press the **[Start]** button to register the face. As shown on the left, align the face with the outline of the face on the screen and place the center of the face on the guide displayed on the screen to register.



② If the face is recognized properly like the left picture, the guide is turned green and the face registration begins. At this point, you should stop not to move the face for better registration.

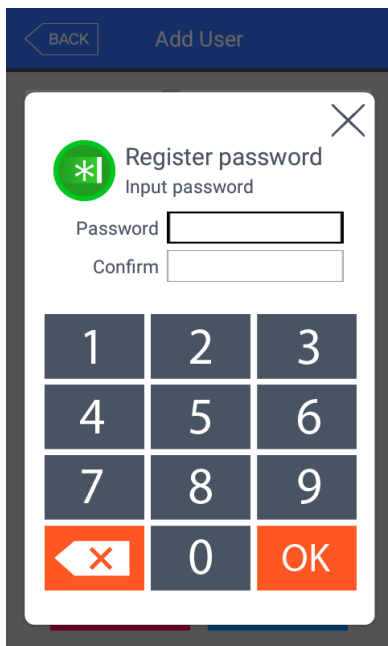


③ When the registration is ended, the message '**Completed!**' appears like the left screen, and if you click the **[OK]** button, the face registration is completed and the screen is moved to the previous screen.

If you want to register again, click the **[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 having the registered face including the Multi Auth users whose 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.)

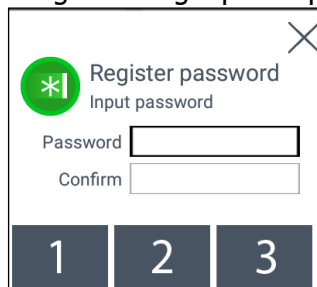
3.3.1.5. Password registration



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 **[X]** button to cancel and return.

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

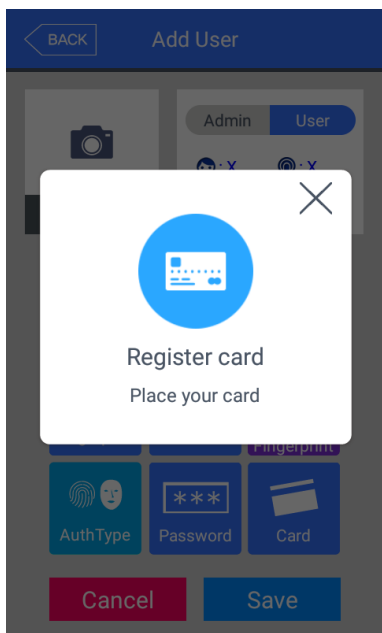


※ Duress password

When entering a password, the authentication is successful even if you enter the password you registered in reverse. But this is an attempt to authenticate threats to the server.

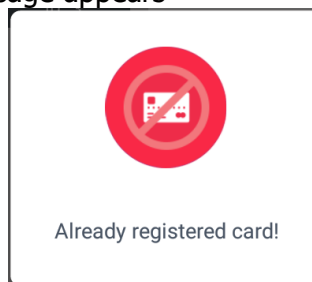
Ex) If the password is 1234, it will be certified as a duress password when entered as 4321.

3.3.1.6. Card registration



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

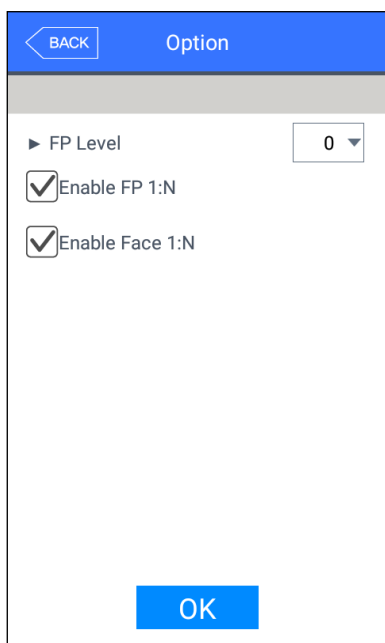
※If you entered the card already registered, the following message appears



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

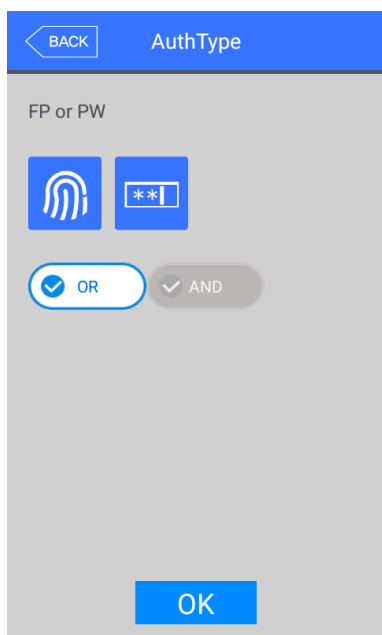


3.3.1.7. Options for authorization



- ▶ 'FP Level' (basic setting: '0')
It decides the fingerprint authorization level of each user, and the registered users can have different authorization level by modifying this value. If you set '0', the authorization uses the level of fingerprint authorization. For example, if you select the "1" for FP Level, this user will 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: if the registered FP user exists, [v])
If this option is checked, you can authorize only with fingerprint without user ID or card
- ▶ 'Enable Face 1:N' (Basic setting: if the registered face user exists, [v])
If this option is checked, you can authorize only with face without user ID or card.

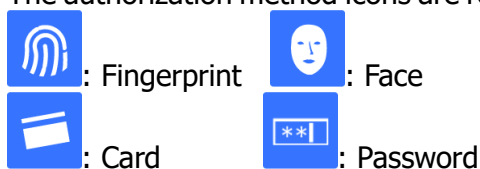
3.3.1.8. How to set 'AuthType'



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

This shows all the authorization methods already registered, and the buttons at the lower side shows the buttons **[OR]** / **[AND]** which can be selected. Present authorization method is distinguished with blue color as different as gray color is not selected.

If you click the button **[Finish]**, the authorization method is changed and the screen moves to the previous window. The authorization method icons are represented as follows.



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

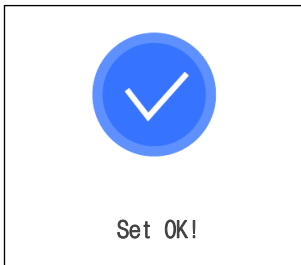
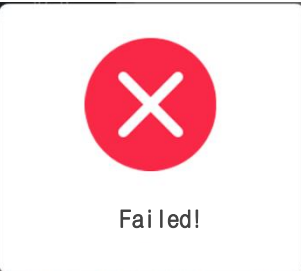

※ (ID or Card) & FP → Card & FP, (ID or Card) & PW → Card & PW,
(ID or Card) & Face → Card & Face, Card & FP & Face & PW → Card & FP & Face will be

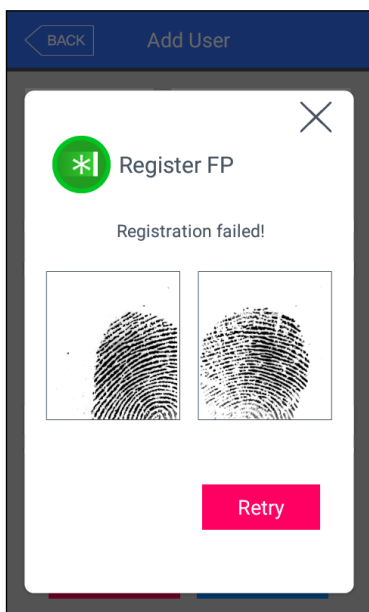
changed automatically.

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.

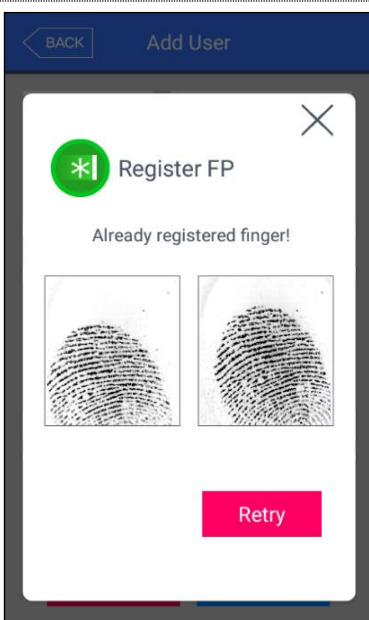
Next is the LCD messages which can appear at the registration procedure.

	<p>When you clicked the [Save] button, the case registration was successful</p>
	<p>When you clicked the [Save] button, the case registration was failed : The case none of authorization methods such as fingerprint, face, card, and password is registered.</p>
	<p>When you clicked the [Auth method] button, the case none of the authorization method was registered.</p>



In **[Register FP]**,

the case you input the different fingerprint at the fingerprint registration.



In **[Register FP]**,

the case you tried to registered the fingerprint already registered. (But, you can input the same fingerprint with the same user ID).

※ If you want to register the same fingerprint in the different ID, you should uncheck the 'System → Fingerprint recognition → preventing the similar fingerprint registration'. But, in this case, because the same fingerprint can be authorized as different ID, it is not suitable for the attendance management.

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

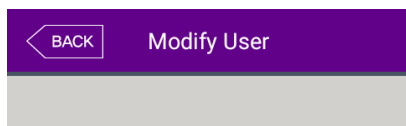
But, the deletion in the terminal is not led to the deletion in the server, so if you want to delete completely, you should delete it also in the server.
The deletion deletes both user and admin, so you should be cautious, and the user registered only in the terminal is cannot be recovered.

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

	<p>When it is deleted normally.</p>
	<p>When unregistered ID was entered</p>

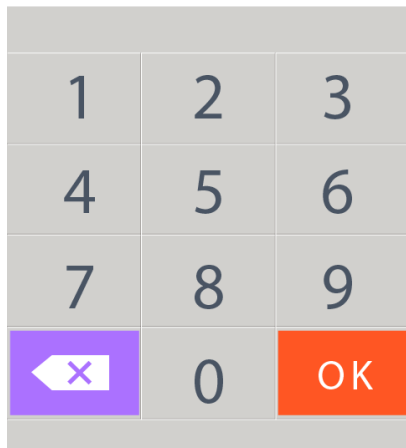
3.3.3. Modify

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

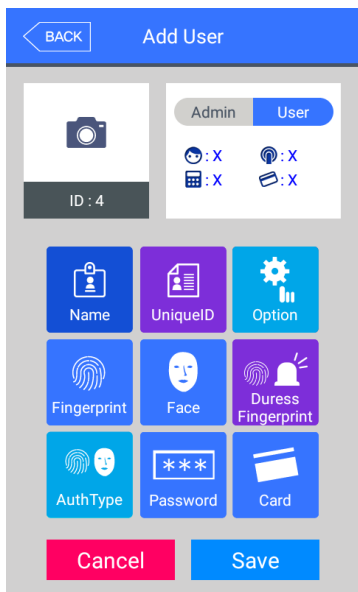


Input the user ID to be modified and click **[OK]** button.
Click **[BACK]** button to cancel and return.

Input User ID



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

: User

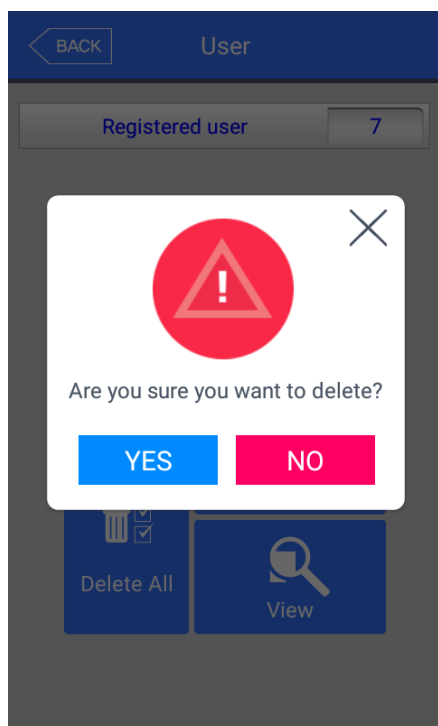
: Administrator

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.

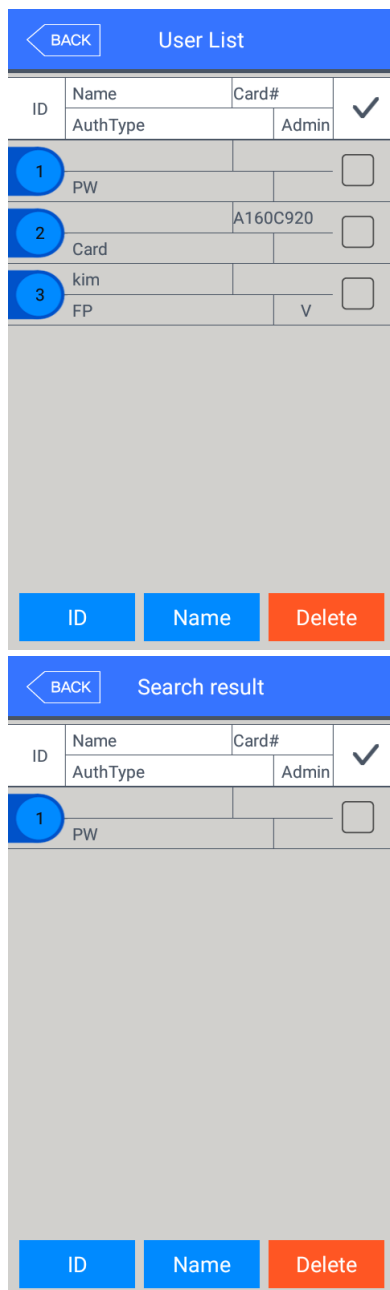


If you want to delete all the users, click **[YES]**, and if you want to cancel, click **[NO]**.

※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.

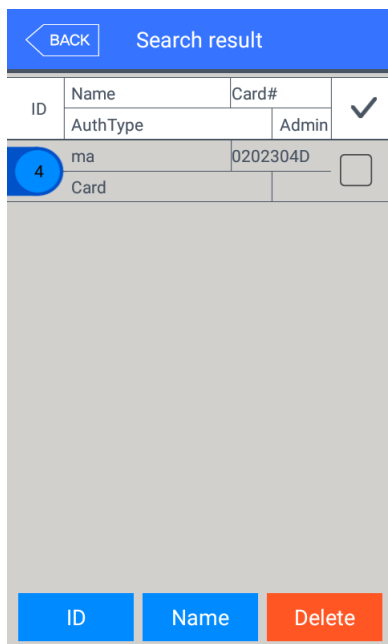
► **[ID]**: If you click the ID of specific user, you can directly move to the modification window of the user.

► **[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.



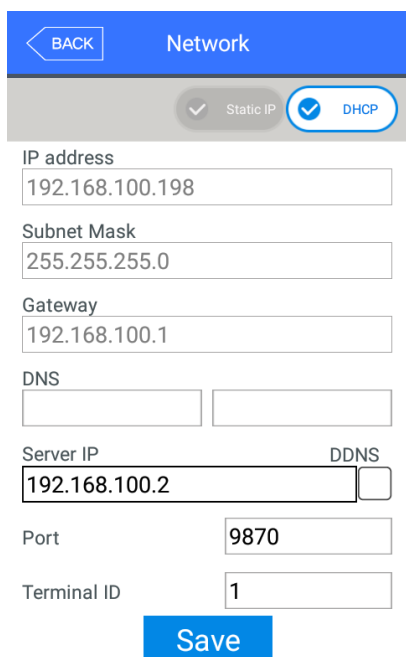
► **[Name]:** If you input the user name by clicking **[Name]** button, the registered user list including the characters is shown.

If you click **[BACK]** button in this window, you can move to the '3.3. User management' menu.

For example, if you searched with "ma", all the users who contain "ma" in their name are searched

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.

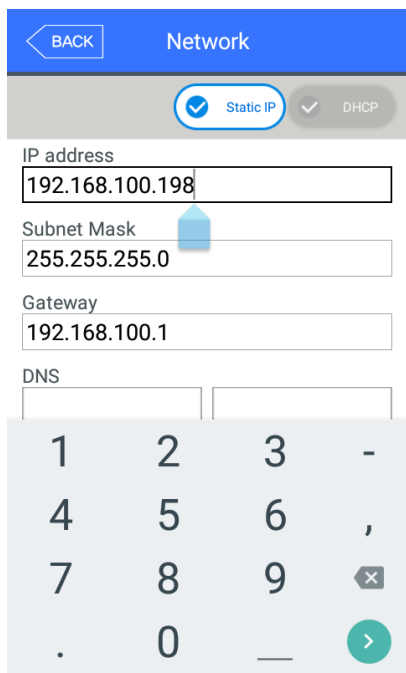
Select the method **[Static IP]** if the static IP is allocated from the connected network, and select **[DHCP]** if the IP is allocated from the DHCP server in the connected network.

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 authorization 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.

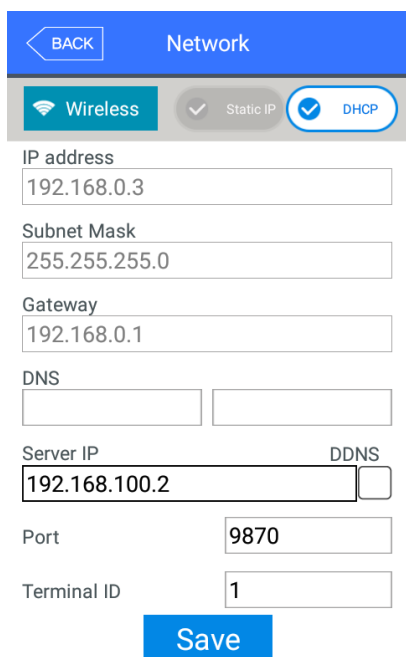


If you touch the item you want to change, the keypad appears at the bottom.

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.

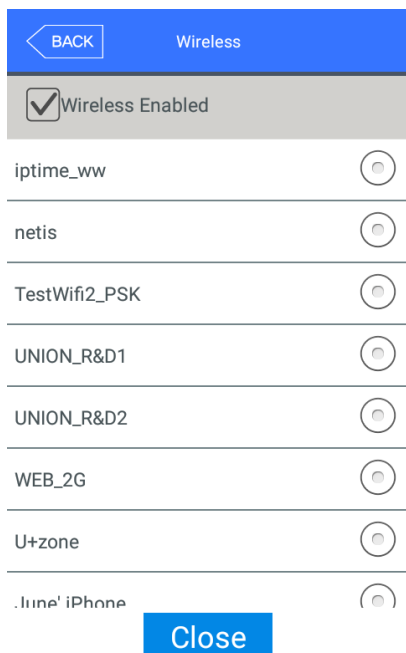
► [WiFi]



When the WiFi dongle is connected to the USB port on backward of the UBio-X Pro 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 WiFi dongle to the UBio-X Pro, you have to purchase it from our sales team because we cannot guarantee to cooperate 3rd party WiFi 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 Pro device will be connected to this AP when inputting the proper AP password.

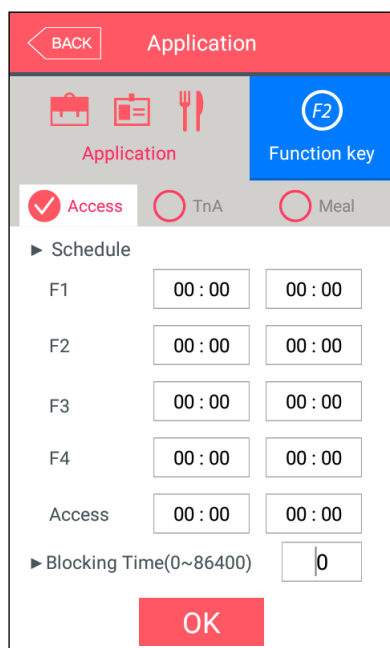
If you want to apply the changes, click **[Close]** button, and return to the previous menu by clicking **[BACK]** button.

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.

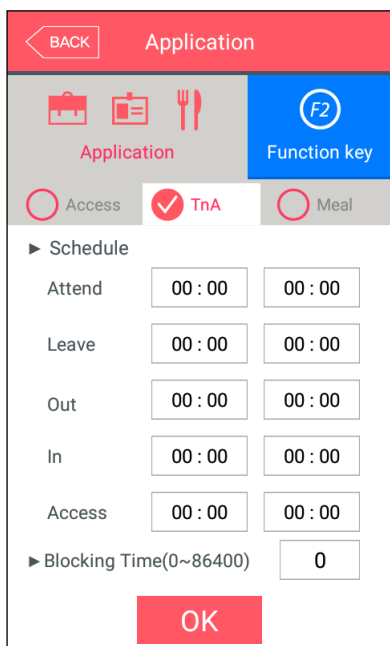
3.5.1.1. Access or TnA setting



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

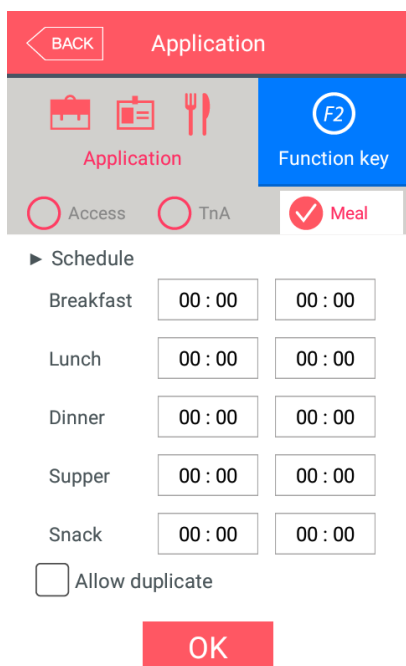


It is the screen appearing when you select the **[TnA]**.

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 authorization 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 authorization 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 authorization. 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.

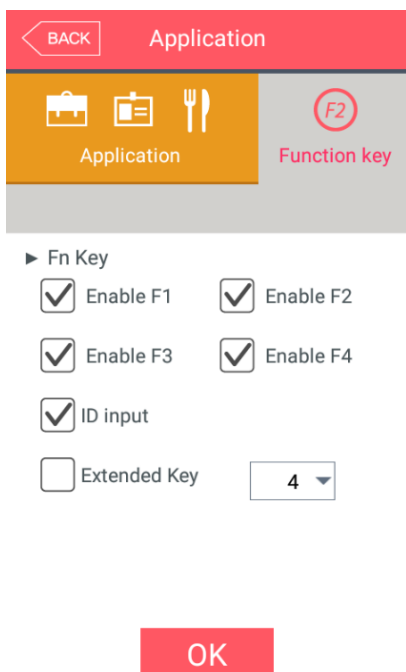
You can set the time period of each meal type. And if the setting is not needed, set '00:00-00:00'.

► Allow duplicate : If it is unchecked () , each user can authorize once in the one meal, but if it is checked () , the multiple authorization is possible regardless of the previous authorizations.

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 authorization mode such as attendance and leaving, and if you click the Fn key, the authorization 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

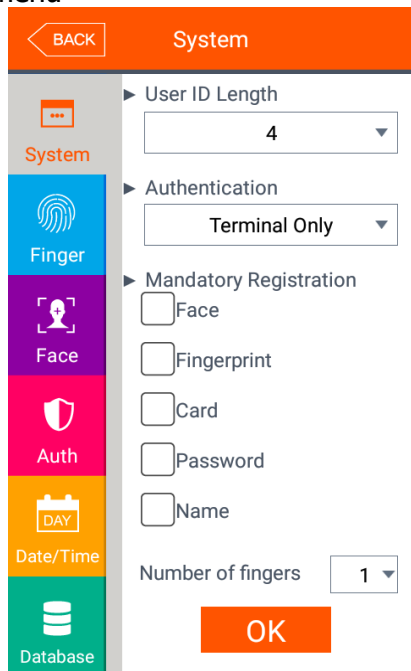
► Extended key
If you need the additional function keys except for the basic function keys **[F1]** ~ **[F4]** and **[Access]**, it can set the additional keys. If you want 'Extended key', check 'Extended key' and set 4, 8, 12, 16, 20, 24, 32, 36, 40.

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 authorization 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.

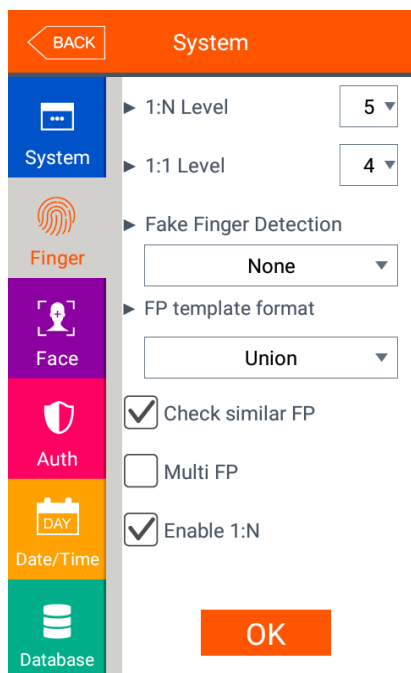
► **Mandatory Registration**

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 authorization level used in the 1: N Fingerprint authorization. In case of 1: N authorization, the authorization level is not set for each user, so the authorization level of the terminal is always the standard.

▶ 1:1 Level (1~9)

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

▶ Fake Finger Detection

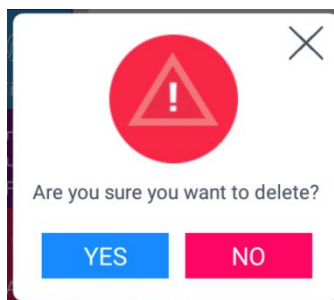
It sets the LFD level to prevent the fake fingerprint input. The higher level of the LFD level, the preventing function of the fake fingerprint input such as rubber, paper, film, or silicon is strengthened, but the fingerprint also can be hard to enter if the finger is dry too much.

▶ 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, authorization speed, and fake fingerprint detection), and the authorization 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 cautious.

▶ **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.

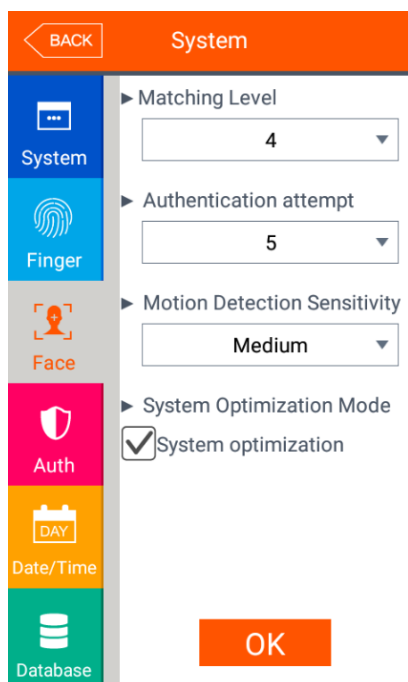
It is the function used when managing the access control of the special area strictly. For example, if the user with ID '0001' has three fingerprints registered, the user should be authorized with all three fingerprints after entering ID. In this case, the order of three fingerprints is not important, but if one of the fingerprints is failed to be authorized, the authorization 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 authorization, in the terminal where the option is not checked, only the 1:1 authorization 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 authorization, and it can be set 1~10 levels according to the matching degree with the registered face. And the authorization is successful when the matching degree is higher than set authorization level.

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

▶ Authentication attempt (1:N): Applied only in terminal authentication (SO)

It shows the authentication result after the set authentication attempt. It can set the value from '1' to '10', and the default setting is '5'. In this case, after '5' authentication attempt, it shows the authentication result.

▶ Motion Detection Sensitivity

It sets the sensitivity of the function to detect the motion and go back from the standby status. Depending on the sensitivity level, it can set 'Low', 'Medium', and 'High'. The default setting is 'Medium'.

▶ System Optimization Mode

It sets the whether to optimize or not of the performance.

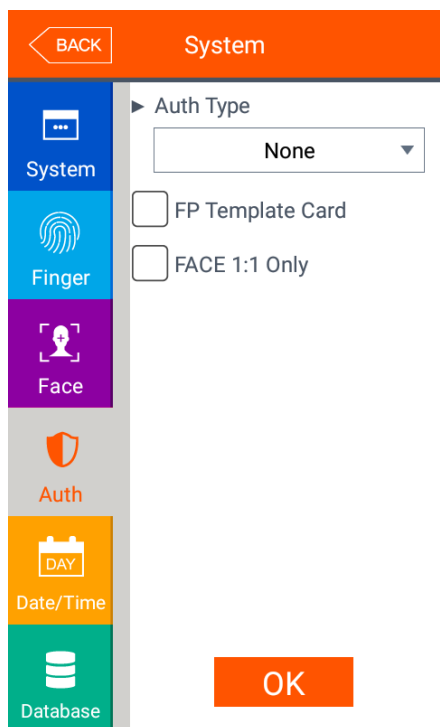
'System optimization' is the default setting.

In the high temperature environment, uncheck this feature.

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 authorization method of the terminal.

- Card: Though the user is registered with the authorization 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 authorization 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 authorization 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.

▶FP Template card

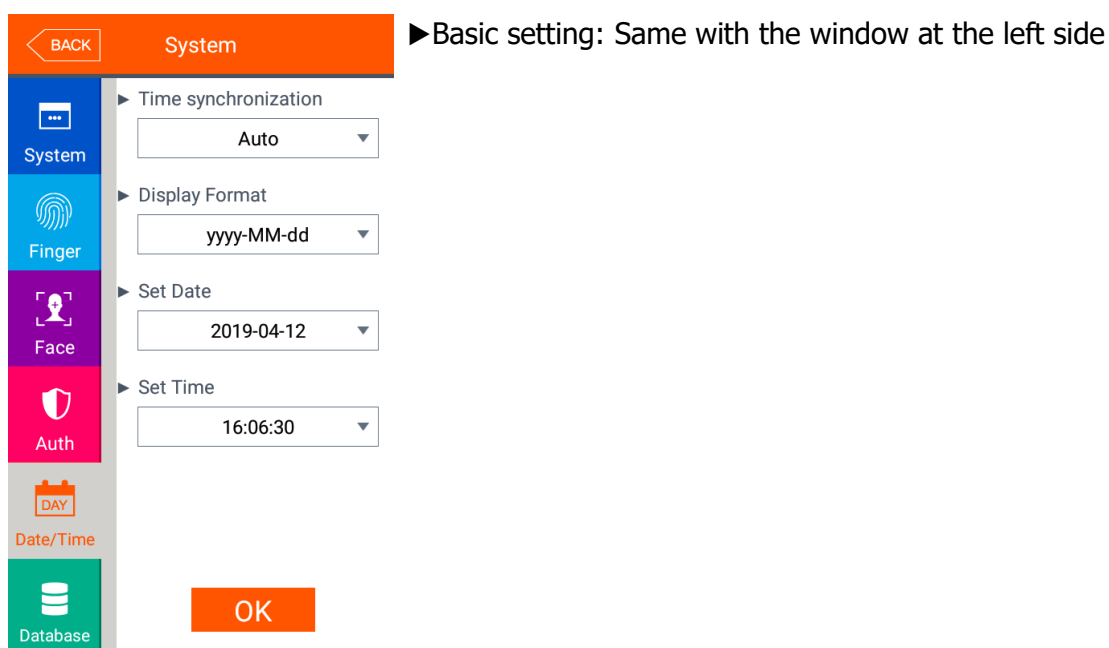
If this option is checked (☑), the option enables the authorization only with the user information in the card and the fingerprint without downloading the user in the terminal. To run this option, the SC card reader must be equipped, and the fingerprint card layout should be set in the server and applied to the terminal.

▶Face 1:1 Only

If this option is checked (☑), face authentication will be worked for 1:1 verification only.

3.6.5. Date/Time

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



▶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

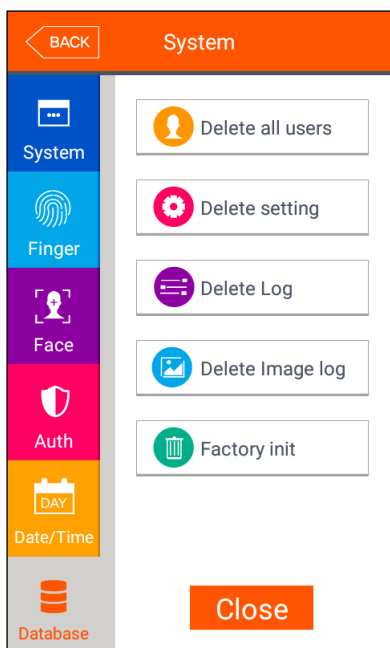
▶Set Date / Set Time

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 because 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 authorization record, click **[Delete Log]** button.

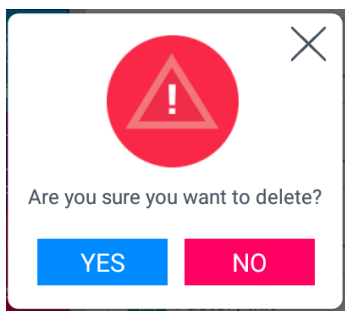
If you want to delete image log only, click **[Delete image log]** button.

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

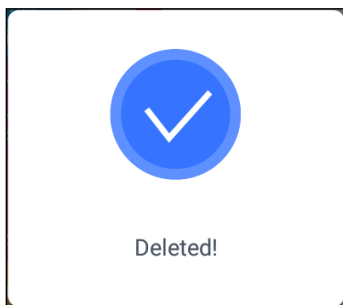
If you select the **[System]** → **[Database]** → **[Delete all users]** in the main menu, the following window appears.



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.

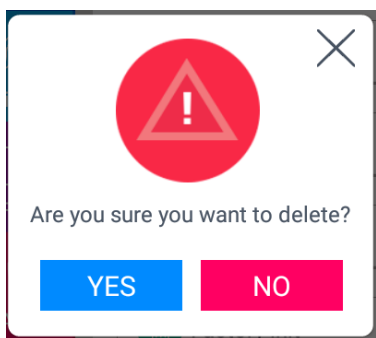


<Fig. 3-5>

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.



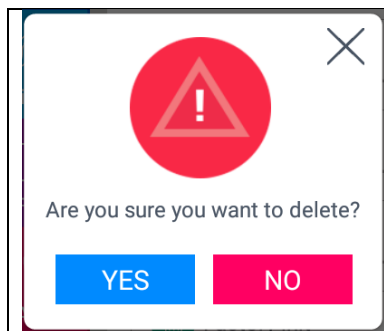
Click **[YES]** button to initialize all the set values, and click **[NO]** or **[X]** button to cancel.

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 authorizations 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.



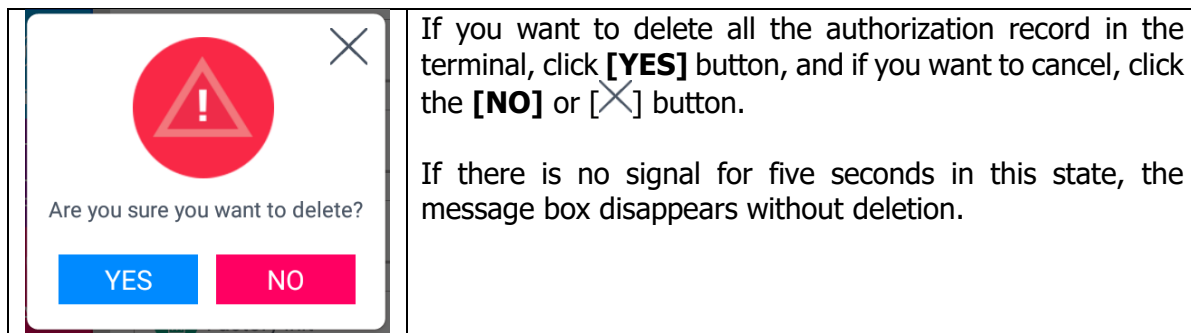
If you want to delete all the authorization record in the terminal, click **[YES]** button, and if you want to cancel, click the **[NO]** or **[X]** button.

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 authorization log is deleted including image log, **and the restoration after the deletion is impossible.**

3.6.6.4. Delete image log

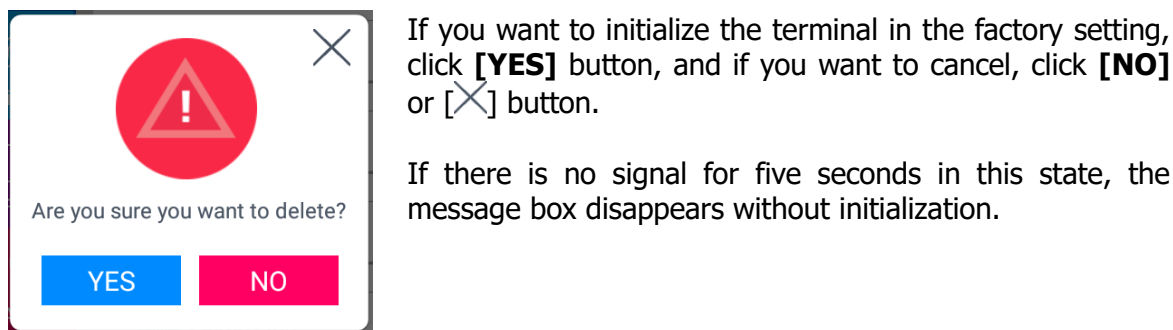
If you select the **[System] → [Database] → [Delete image log]** in the main menu, the following window appears.



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

3.6.6.5. Factory init

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

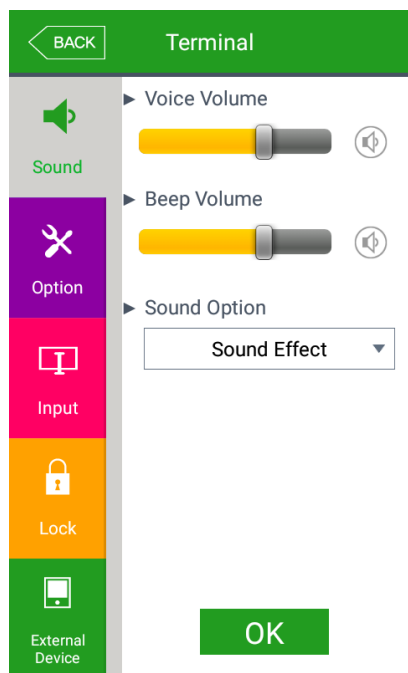


If it is deleted successfully by clicking **[YES]**, the success message in <Fig. 3-5> appears, and the display language and voice is changed to the default value English. All the set value, users and log information besides the MAC address in the terminal to make the terminal in the factory setting. **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 [Speaker] 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 [Speaker] button at the right side, the beep sound is played to check the volume.

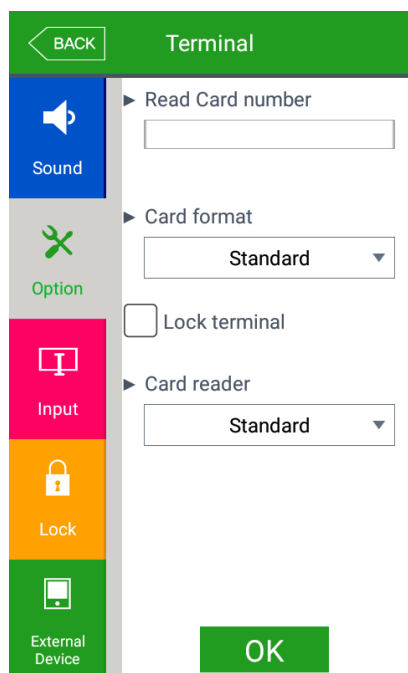
▶ Sound Option

- Sound effect: The sound effect can be output on authorization success or failed.
- User voice: If the user wants to change the voice played when the authorization 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 authorization 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

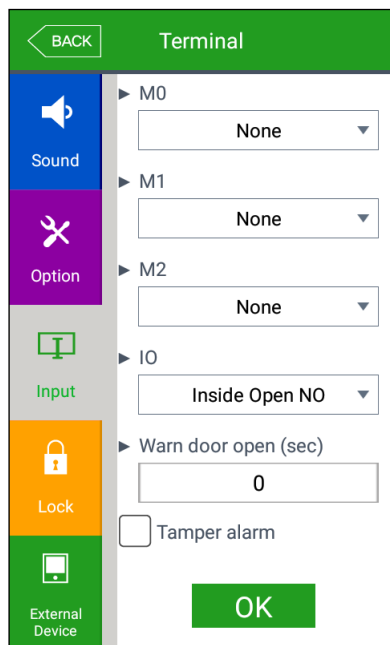
[SC card example] Card number (4byte): 52h 9Dh 06h E3h

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]**.

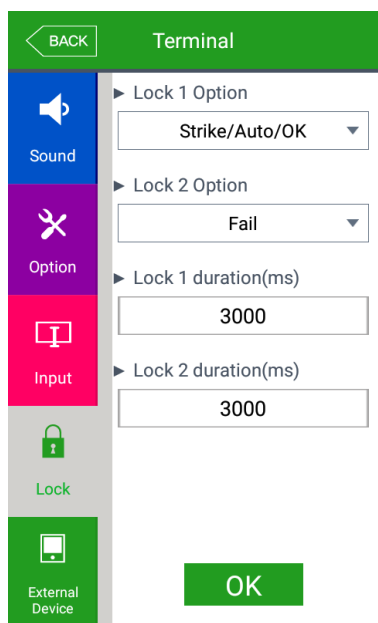
▶Tamper alarm

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 authorization 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 authorization 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 authorization.

► Lock 2 duration (ms)

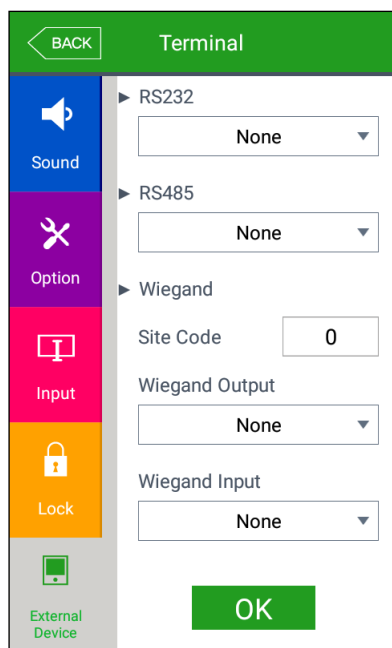
It sets the signaling time when Lock 2 is set 'Authorization failure notification'.

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 authorization result is printed when the authorization is successful. The terminal ID, user ID, authorization time, and authorization 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 use LC010, LC010 and set DM0: 'Door Open NO' or 'Door Open NC', it gets the status of door open via DM0. If you want to get the status of door status 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 authorization 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 byte]", 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 byte]", 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.

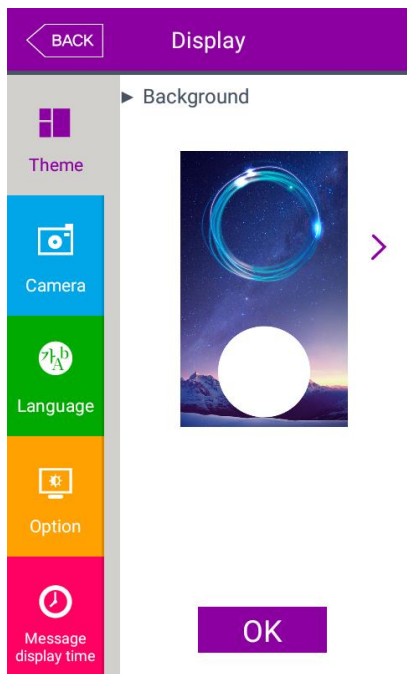
Click **[OK]** button to apply the set value, and click **[BACK]** button to cancel and return.



3.8. Display

3.8.1. Theme

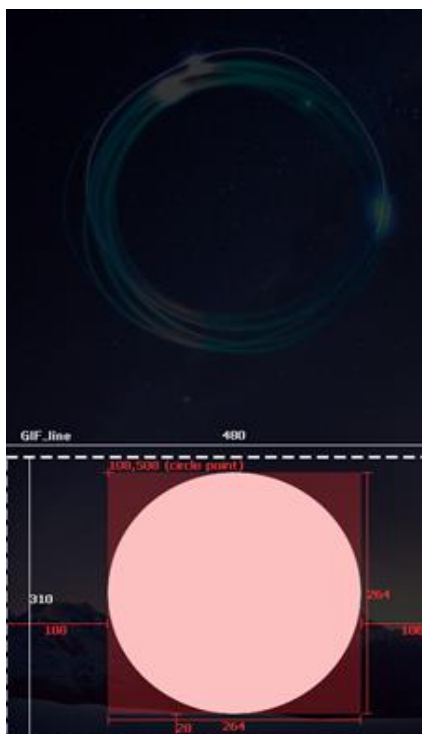
If you select **[Display]** → **[Theme]** in the main menu, the following window appears.



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

▶ Background
It sets the background of the basic window. You can inquire the next image by clicking [>] button.

▶ Customized background



To apply the customized background, you should send both .png and .gif images via the server. If only 1 of image is sent, it is not available to apply the theme and if both 2 images are sent, the theme is automatically applied.

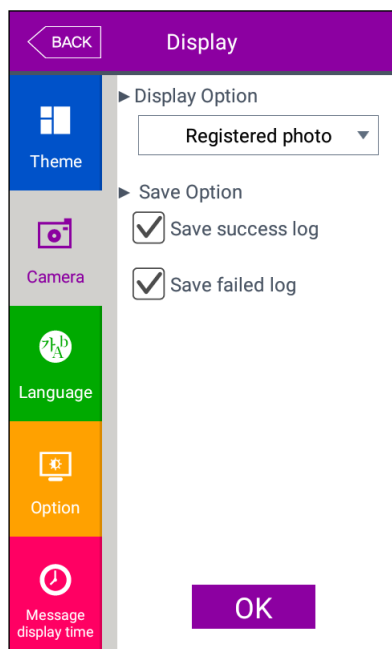
The size of .png and .gif images should be created referring to the left picture and it should not exceed 9MB for maximum.

(※If you apply the wrong image, it is not displayed.)

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.

3.8.2. 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
 Choose the image displayed in the message window of authorization success
 - None
 - Registered user’s picture.
 - AuthType: Image stands for each AuthType

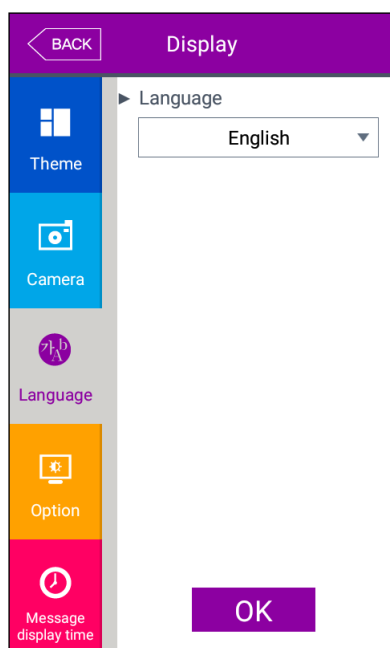
▶ Save success log
 If it is checked (), the camera image is captured as image log when the authorization was successful.

▶ Save failed log
 When it is checked (), the camera image is captured as image log when the authorization 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.

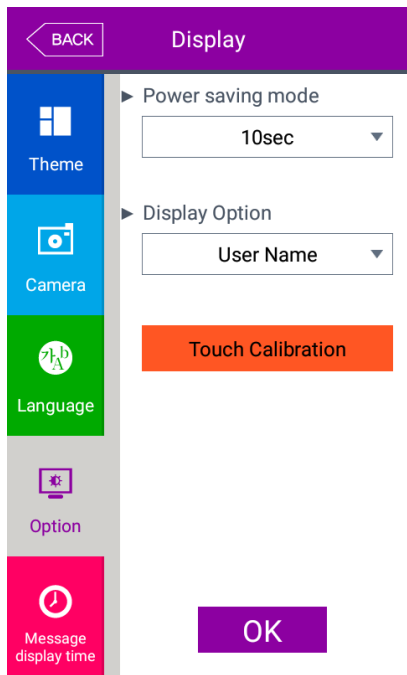
If you want to cancel and move to the upper menu, click **[BACK]** button.

※ 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.

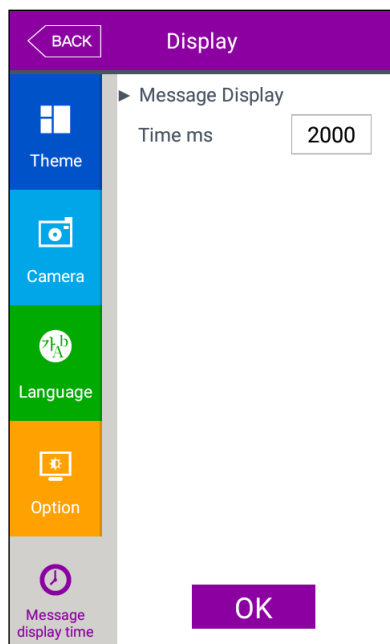
▶ Display Option
 It sets what will be shown at the LCD screen when the authorization is successful.
 - None: The authorization result [Success/Failure] is only represented.
 - User ID
 - User Name: Representing user ID if it is not registered. (In this case, added "ID" in order to differentiate with 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 authorization result window to be displayed.

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

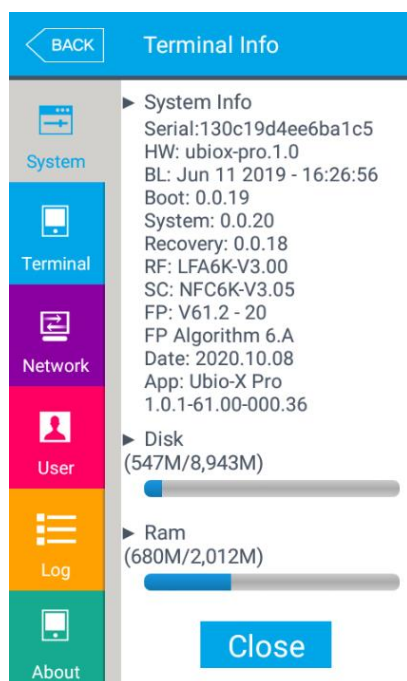
Because it is set in millisecond, if you want to set 2 seconds, you should set 2000.

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 the 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)

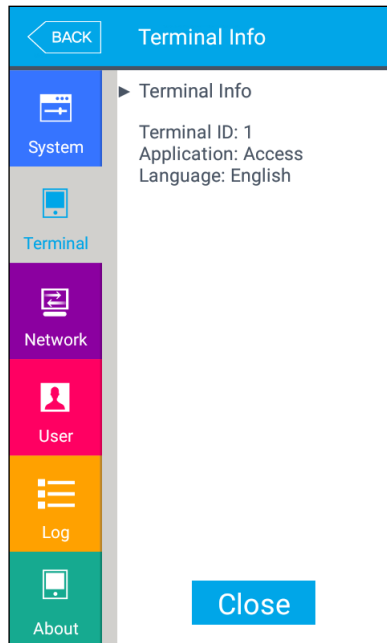
The using size of RAM among the all size is represented.

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.

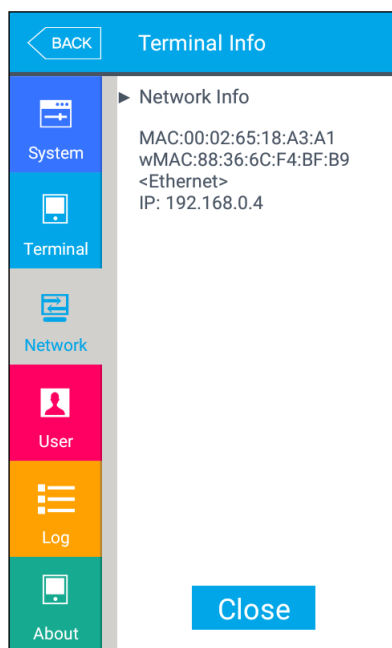


- ▶ Terminal info
It represents the option setting value of the terminal.

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.

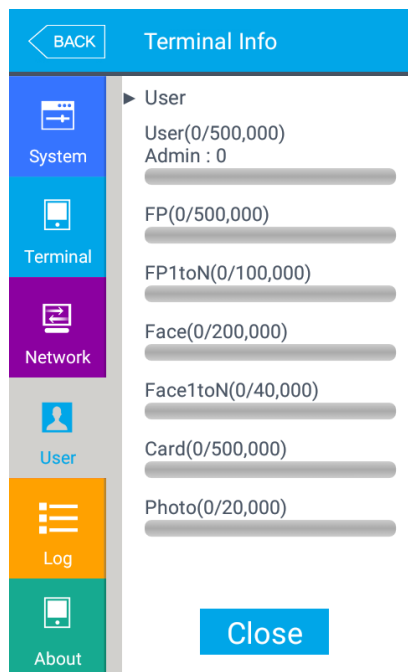


- ▶ Network info
It shows the network setting value of the terminal.

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.



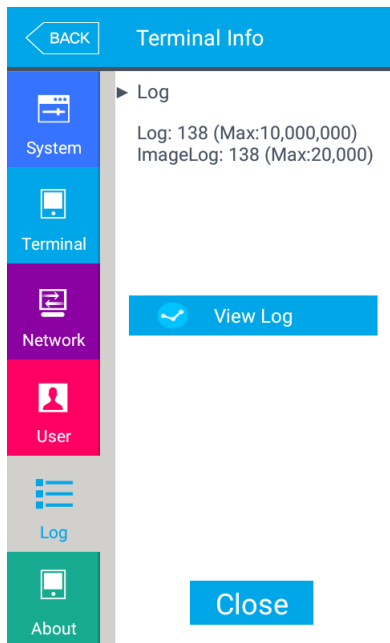
►User

- 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.

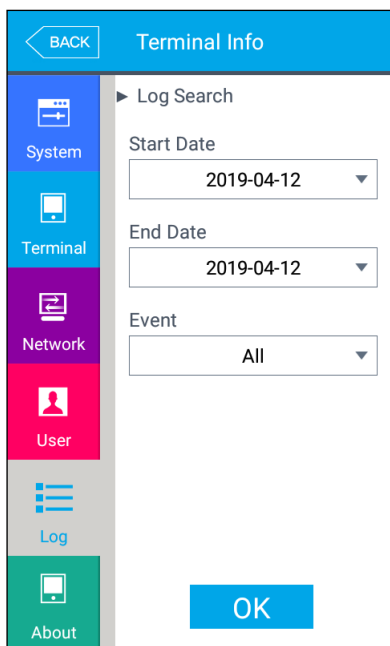
3.9.5. Log

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

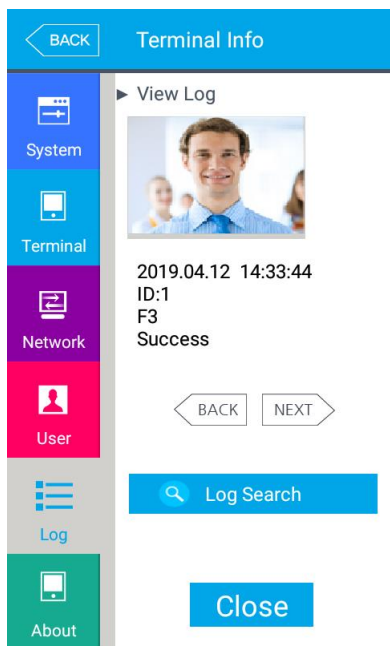


- ▶ **Log**
Log: The number of logs saved in the terminal
Image Log: The number of image logs saved in the terminal.
(Max means the maximum number of items which can be saved in each item.)

- ▶ **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

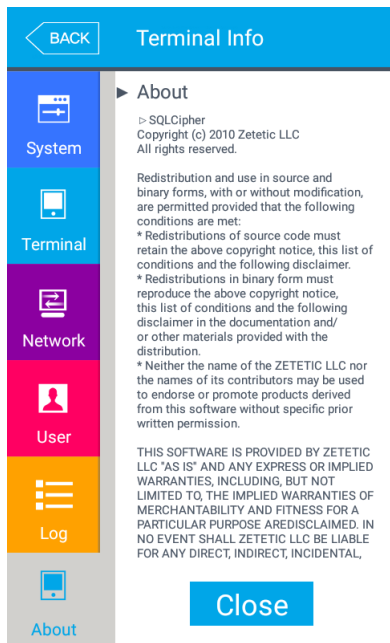
Log search result shows the information such as the date, time, ID and access result (success or failure).

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

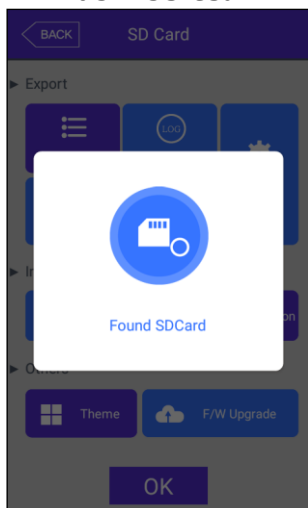
It shows the license information of the Korean font applied to the terminal.

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

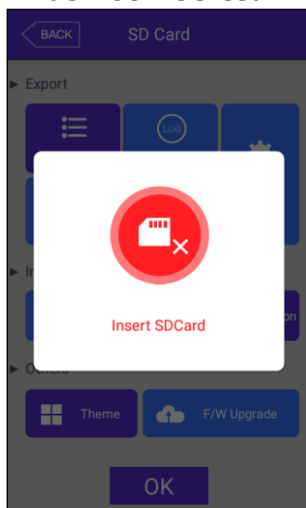
3.10. SD Card

If you select the **[SD Card]** at the main menu, the following screen appears.

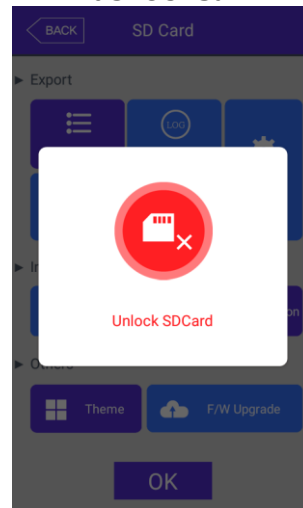
< When the SD Card was inserted >



< When the SD Card was not inserted >

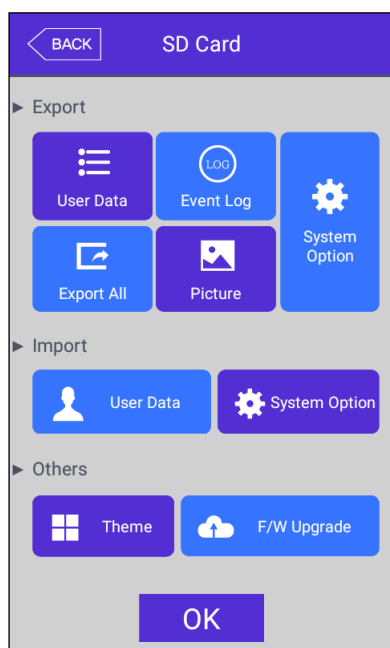


< When the SD Card was locked >



※ It works only if the SD Card is inserted, and it should be inserted with the back side face forward like the figure. (The side of the SD Card should not exceed 32G.)





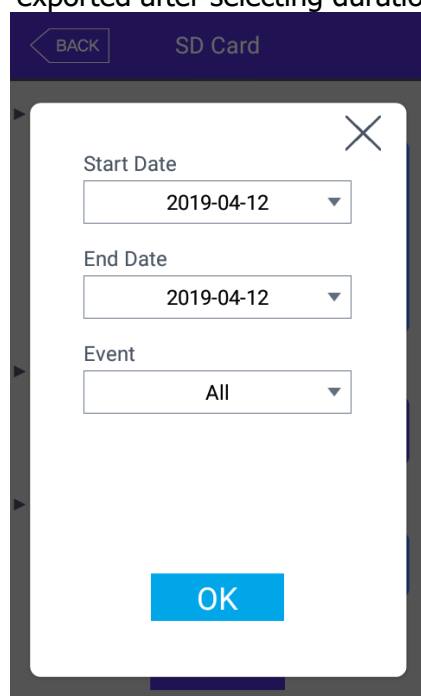
It is the function used for data backup of the terminal by **[Export]**, and you can copy the backup data from the **[Export]** into the terminal again.

► Export

It copies the data from the terminal to the external SD Card.

- User data: It copies the user DB to the folder 'unisuser' on the SD Card.
- System option: The option setting value of the terminal is copied to the folder 'UbioXpro / config'.
- Event log: It copies the authorization log DB to the folder 'UbioXpro / Terminal ID (8 digit) / log' on the SDcard.

Basically, log image couldn't be exported in this option and Period logs can be exported after selecting duration.



- Picture: The image log data is saved in the folder 'Ubioxpro / Terminal ID (8digit) / log / pictures' on the SD Card as jpg file.
- Export all: It can export all things User Data, Event Log, System Option, Picture to the SD Card.

►Import

It copies the data from the SD Card to the terminal.

- User Data: It copies the user DB from the SD Card to the folder 'unisuser' in the terminal.
- System Option: The option setting value of the terminal is copied to the folder 'Ubioxpro / config' in the terminal.

After importing the data, the UBio-X Pro terminal should be rebooted to apply new data & options.

►Others

- Theme: The voice file in the 'Ubioxpro /audio' folder in the SDcard is copied to the terminal. If you want to replace the authorization success (user_ok.mp3) and the authorization fail (user_fail.mp3) message with the user voice, set the name of the user voice file as (user_ok.mp3), (user_fail.mp3) respectively which the user voice will play. And also the checkbox "User Voice" on [3.7.1. Sound] should be checked.

- F/W upgrade: It upgrades the firmware by the SD Card.
(The firmware should be in the 'Ubioxpro' folder on the SD Card.)

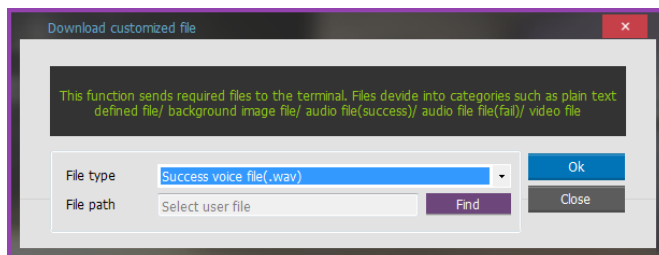
If you want to finish working and move to the upper menu, click the **[OK]** or **[BACK]** button.

3.11. User's file download

If necessary, the user can change the background screen or voice message with this function. It can be fulfilled by copy with SD Card or downloading the user file from the UNIS server program.

3.11.1. How to change voice sound

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 authorization with fingerprint/card, or touched the main screen, the LCD screen is turned on automatically.

4.1. How to change Auth mode

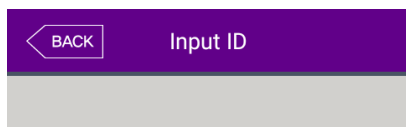


<Fig. 4-1>

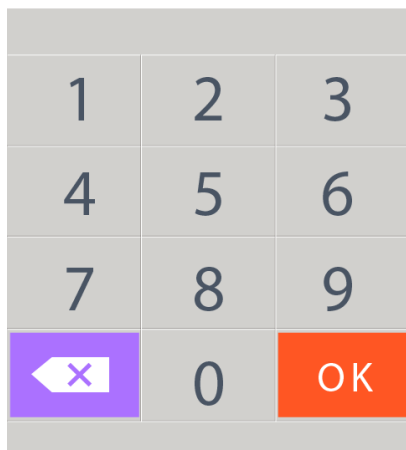
Select the function key button among Attend **[F1]**, Leave **[F2]**, Out **[F3]**, In **[F4]** on the screen for choosing the function mode before authentication.

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.



Input User ID



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

4.3. How to authorize

4.3.1. Face authorization

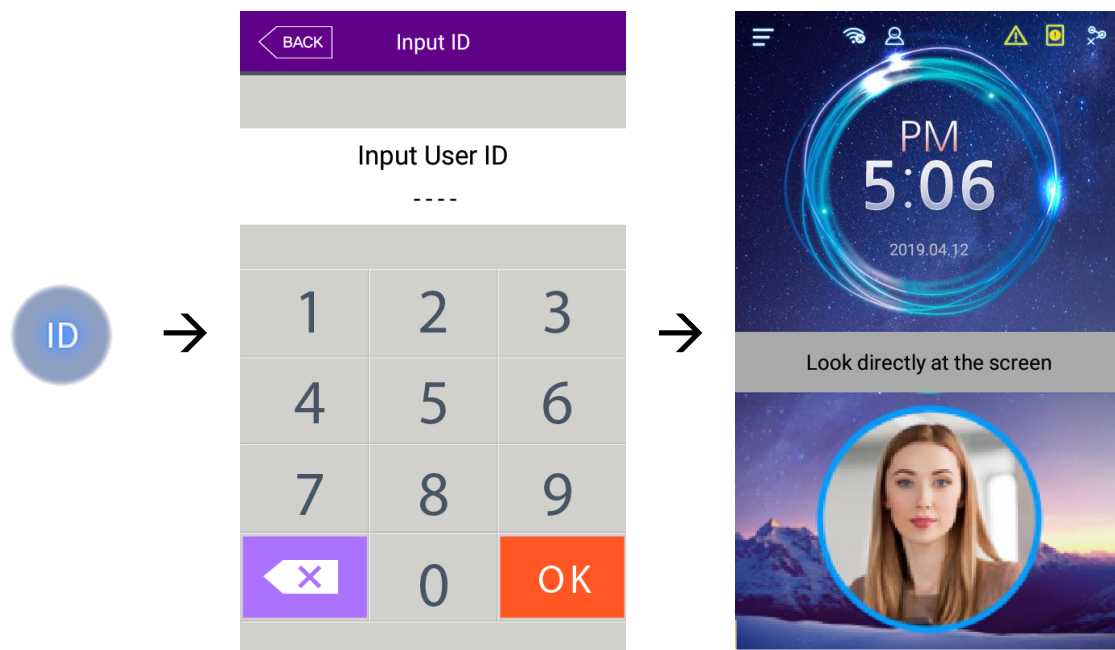
▶ **1:N Authorization (Identification)**

Set the location of your face at the LCD guideline until the guideline is changed blue, and gaze the camera and stop moving to try authorization.

▶ **1:1 Authorization (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 Authorization will be canceled with the message box is changed to gray after 20 seconds.



4.3.2. Fingerprint authorization

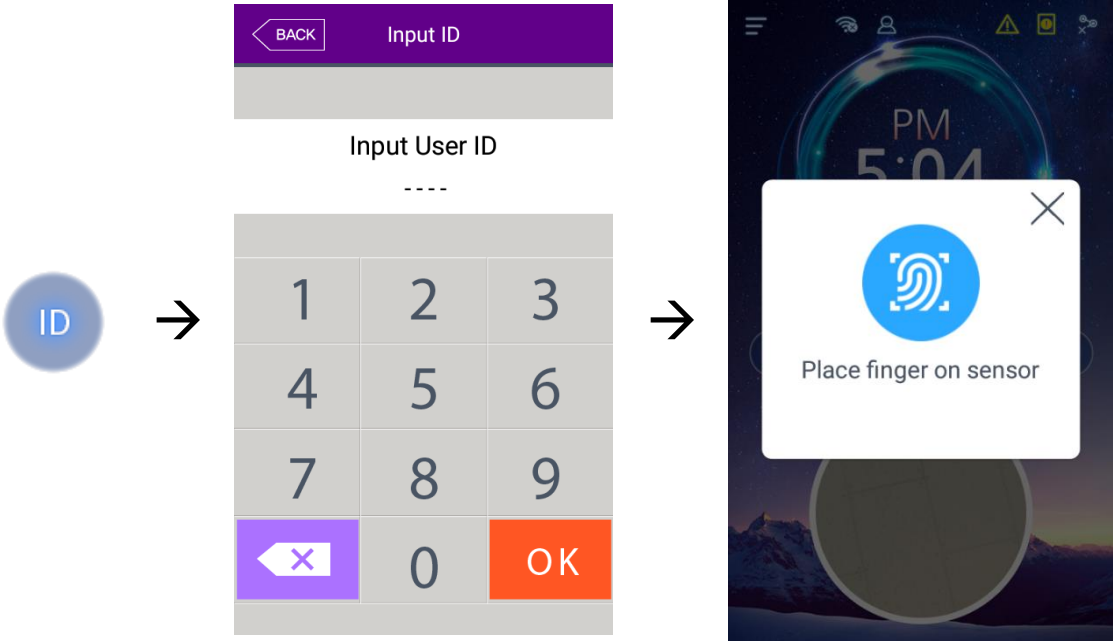
▶ 1:N Authorization (Identification)

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 Authorization (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.

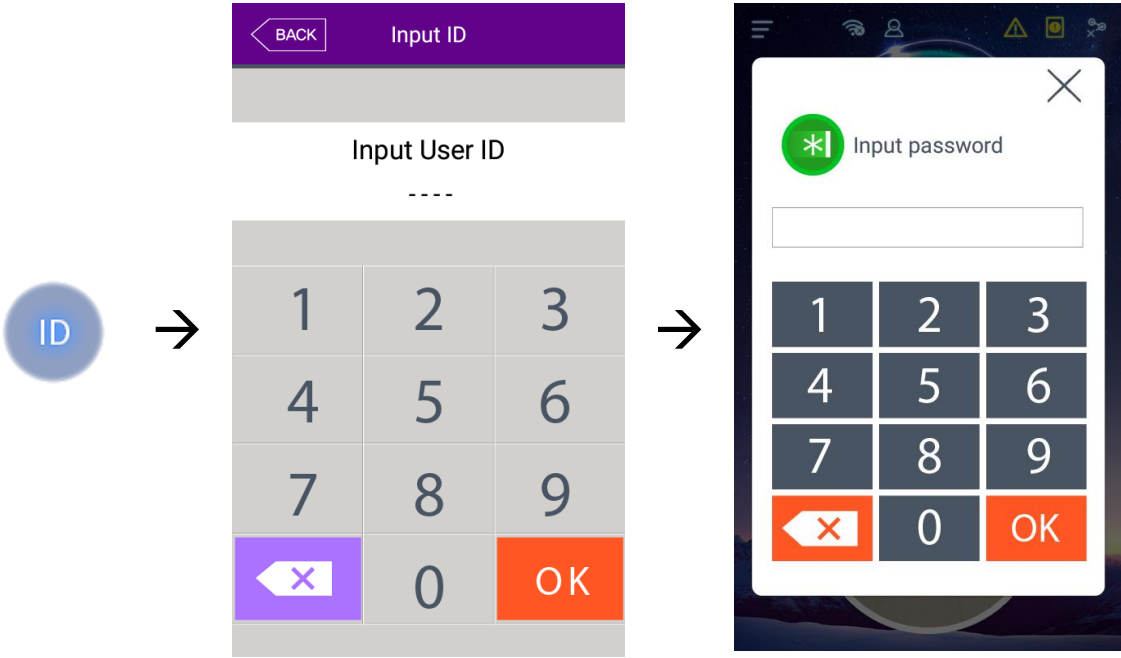


4.3.3. Card authorization

Put the card on the card picture in <Fig. 4-1>

4.3.4. Password authorization

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



4.3.5. Multi-mode authorization

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

It activates even face or fingerprint authenticates firstly.

Distributed by



Trading Address: Unit A8 Caxton Point Business Centre, Caxton Point, Caxton Way, Stevenage, SG1 2XU, UK
Registered Office: c/o Becktech Limited, Terminus Road, Chichester, Sussex, PO19 8DW, UK
Telephone: +44 (0)1707 330 541 | Email: sales@genieproducts.co.uk