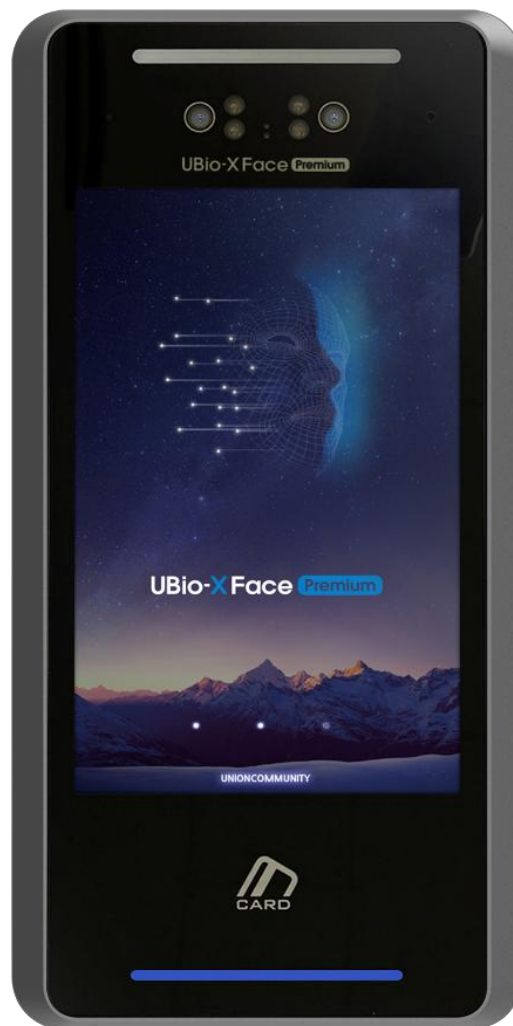


UBio-X Face Premium User's Guide

Version Eng-1.26



<Revision History>

Version	Date	Description	Firmware Version
1.0	2022-02-18	Initial Release	
1.1	2022-06-13		
1.2	2022-07-05	Correction.	000.04
1.2	2022-07-27	Enable Face list pop-up update.	
1.2	2022-08-12	Anti-Spooping related modifications.	
1.3	2022-08-22	Added the AE flicker frequency menu.	
1.4	2022-09-02	1.3.2 Real-time check of icon and terminal details Add Table of Contents 3.7.4 Addition of unregistered users to access 3.7.6 Add ETC. (Deterioration) 3.9.2 Change Image and Add Description	
1.5	2022-11-09	3.6.3 Modifying the menu related to facial recognition	
1.6	2022-12-06	1.3.1 Temper related icons, adding comments	
1.7	2023-02-15	Complement the description when it is more than 24 digits related to the QR card.	
1.8	2023-02-24	3.6.3 Face recognition Changing the Menu Image Face recognition - AE Mode, face authentication pop-up type, Add Multiple Face Detection	
1.9	2023-04-10	3.7.2. Terminal Options Fixed to Card Reader Standard 3.7.6. ETC. (Deterioration) Secure with thermal camera TS	000.31
1.10	2023-05-11	3.8.1 Camera Add save description if face authentication fails	
1.11	2023-05-25	1.3.2 Real-time check of icon and terminal details Modify Image and Description 3.2 Modify Menu Configuration 3.6.4 Authentication Change image and add First Function Key description Changing the manual capture image by changing the default value	
1.12	2023-06-08	1.3.3 Add Message Guide Table of Contents and Descriptions 3.6.3.Face recognition –Face authentication pop-up type Add list pop-up description	

1.13	2023-06-22	3.6.6 Add Database App Restart Menu	
1.14	2023-06-28	3.6.4 Delete Authentication First Function Key	
1.15	2023-07-13	3.7.6 Correcting typos	
1.16	2023-08-11	Adding Descriptions at Administrator Authentication Add Authentication Com Description Add Mobile Card Condition Description 2.1 Product Features -> Authentication combination Card & Fingerprint & Face Duplicated 3.1.2 Add Administrator Authentication Ps-> Mobile Card 3.2 Menu Configuration -> [4. System]->Adding App Restart to Database Access 3.2 Menu Configuration -> [7. Terminal Information] ->Adding voice stored in terminal information in terminal items 3.3.3 Change-> Delete the phrase "If you touch a picture, you can take a picture again and register it" (not implemented) 3.8.2 Language->Supported Language->English / Korean / Japanese / Portuguese / French / Spanish / Polish / German / Turkish / VietNAmese / Thai / Arabic Correct 4.3.5 multi-authentication-> "Card and mobile card cannot be used as authentication means when attempting 1:1 authentication under or conditions that include cards and mobile cards."	
1.17	2023-08-16	Add face size description when using anti-spoofing	
1.18	2023-08-25	Add UBio-X Face Pro Applied Content	
1.19	2023-08-28	Change photos according to menu, add wireless LAN	
1.20	2023-08-29	Change the Authenticated Distance menu and change the top bar picture	
1.21	2023-09-15	Corrects the same for UBio-X Face Pro changes	
1.22	2023-11-06	Added Camera Calibration feature.	
1.23	2024-01-31	UBio-Core feature integration	000.49

1.24	2025-08-01	Add AEMode	
1.25	2025-09-15	Add breathalyzer	
1.26	2025-11-06	Add to Europe	

< Glossary >

● Administrator (Admin, Administrator)

- A user who can enter the terminal menu mode, which is authorized to register/modify/delete the user of the terminal and change the operating environment through setting changes.
- If there is no registered administrator on the terminal, anyone can enter the terminal menu and change the settings, so we **recommend that you register at least one administrator**
- Administrators have the right to change important preferences for fingerprint recognition terminals, so special attention is required to register and operate.
- **Europe-oriented products are forced to set up an administrator, and the administrator's means of authentication must use at least two and AND conditions.**

● 1:1 Verification (1 to 1, Verification)

- How to authenticate your fingerprint after entering your user ID or card
- It is called 1:1 authentication because it compares only the fingerprints of the user ID or the user registered on the card.

● 1:N Verification (1 to N, Identification)

- It is a method of finding the user with only a fingerprint.
- It is called 1:N authentication because it is a method of finding the same fingerprint as the input fingerprint among registered fingerprints without user ID or card input.

● Authentication level

- The level used for fingerprint authentication is displayed in steps from 1 to 9 depending on the degree of fingerprint matching, and authentication is successful only when the degree of matching between the two fingerprints is higher than the set authentication level.
- The higher the level of authentication, the higher the security, but the higher the probability of authentication failure during self-authentication because it requires a relatively high match rate.
- 1:1 authentication level: The authentication level used for 1:1 authentication.
- 1:N authentication level: This is the authentication level used for 1:N authentication.

● Authentication Method

- Face (face) authentication, FP (fingerprint) authentication, RF (card) authentication, and various types of authentication methods made by each combination.
Yes) Face or FP: Authenticate with face or fingerprint.

● Live Finger Detection (LFD): Fingerprint Protection

- It allows you to input only real fingerprints and prevents the input of fake fingerprints made of rubber, paper, film, and silicone

Table of Contents

< Revision History>	
< Glossary >	4
Table of Contents	5
1. Check before use.....	7
1.1. Safety Precautions.....	7
1.1.1 Installation Height and Authentication Range	8
1.1.2 Installation Precautions.....	8
1.2. Specific names of the terminal (XScan fitted appearance)	9
1.3. Screen guide for operation.....	10
1.3.1 Icon Guide	11
1.3.2 Real-time check of icon and terminal details	12
1.3.3. Message Guide	12
1.4. Voice Guidance During Operation	25
1.5. Information on the buzzer that comes out during operation	25
1.6. Proper face registration and authentication methods.....	25
1.7. Proper fingerprint registration and input method	26
2. Product Introduction	27
2.1. Product features	28
2.2. Configuration Diagram	31
2.2.1. Standalone (Access).....	31
2.2.2. Connected with Server (Access, Attendance, Meal management)	31
2.2.3. Product Specifications.....	32
3. Configuration settings	33
3.1. Pre-Environmental Settings Confirmation	33
3.1.1. Enter the menu	33
3.1.2. Administrator Authentication	34
3.1.3. How to enter the menu without administrator authentication	35
3.1.4. Saving Settings.....	35
3.2. Menu configuration.....	36
3.3. User Management	39
3.3.1. Add	40
3.3.1.1. Name Registration.....	42
3.3.1.2. Fingerprint Registration	43
3.3.1.3. Face Registration	46
3.3.1.4. Password Registration	46
3.3.1.5. Card Registration	48
3.3.1.6. Authentication Option	49
3.3.1.7. Auth Type	50
3.3.1.8. Save.....	51
3.3.2. Delete	52
3.3.3. Modify.....	53
3.3.4. Delete All	54
3.3.5. View.....	55
3.4. Network Settings.....	56
3.5. Application Mode	58
3.5.1. Application Mode	58
3.5.1.1. Access or TNA setting	58
3.5.1.2. Meal Setting	59
3.5.2. Function keys	59
3.6. Systems.....	60

3.6.1. System	60
3.6.2. Finger	61
3.6.3. Face	63
3.6.4. Authentication	65
3.6.5. UBio-Core	67
3.6.6. Setting the current time	72
3.6.7. Database	73
3.6.7.1. Delete All Users	73
3.6.7.2. Delete Settings	74
3.6.7.3. Delete log data	74
3.6.7.4. Delete Image Logs	75
3.6.7.5. Delete All	75
3.6.7.6. Reboot	76
3.6.7.7. Restarting the app	76
3.7. Terminal Settings	76
3.7.1. Sound	76
3.7.2. Terminal Option	77
3.7.3. Input Settings	80
3.7.4. Lock	81
3.7.5. External Device	83
3.7.6. ETC(Thermal)	85
3.8. Display	87
3.8.1. Camera	87
3.8.2. Language	89
3.8.3. LCD Option	90
3.8.4. Message display time	91
3.9. System	92
3.9.1. System	92
3.9.2. Terminal Information	93
3.9.3. Network	93
3.9.4. User	94
3.9.5. Log	95
3.9.6. About	96
3.10. USB	97
3.11. Download User Files	100
3.11.1. Change voice message	100
4. How to use terminal	100
4.1. How to change auth mode	101
4.2. How to input the user ID	101
4.3. Authentication	102
4.3.1. Face Authentication	102
4.3.2. Fingerprint Authentication	103
4.3.3. Card Authentication	104
4.3.4. Password authentication	104
4.3.5. Multi Authentication	105

1. Check before use

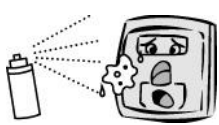
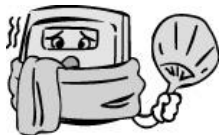
1.1. Precautions for Safety

● Warning

Do not operate the terminal with wet hands or allow liquids such as water to enter the terminal. ->The risk of failure and electric shock There is.		Do not leave fire source near the terminal. -> It can cause fire.	
Do not disassemble, repair, or modify the product arbitrarily. -> There is a risk of failure, electric shock,		Keep out of reach of children. -> It may cause an Accident or damage.	

- Failure to comply with what is indicated may result in death or serious injury to the user.

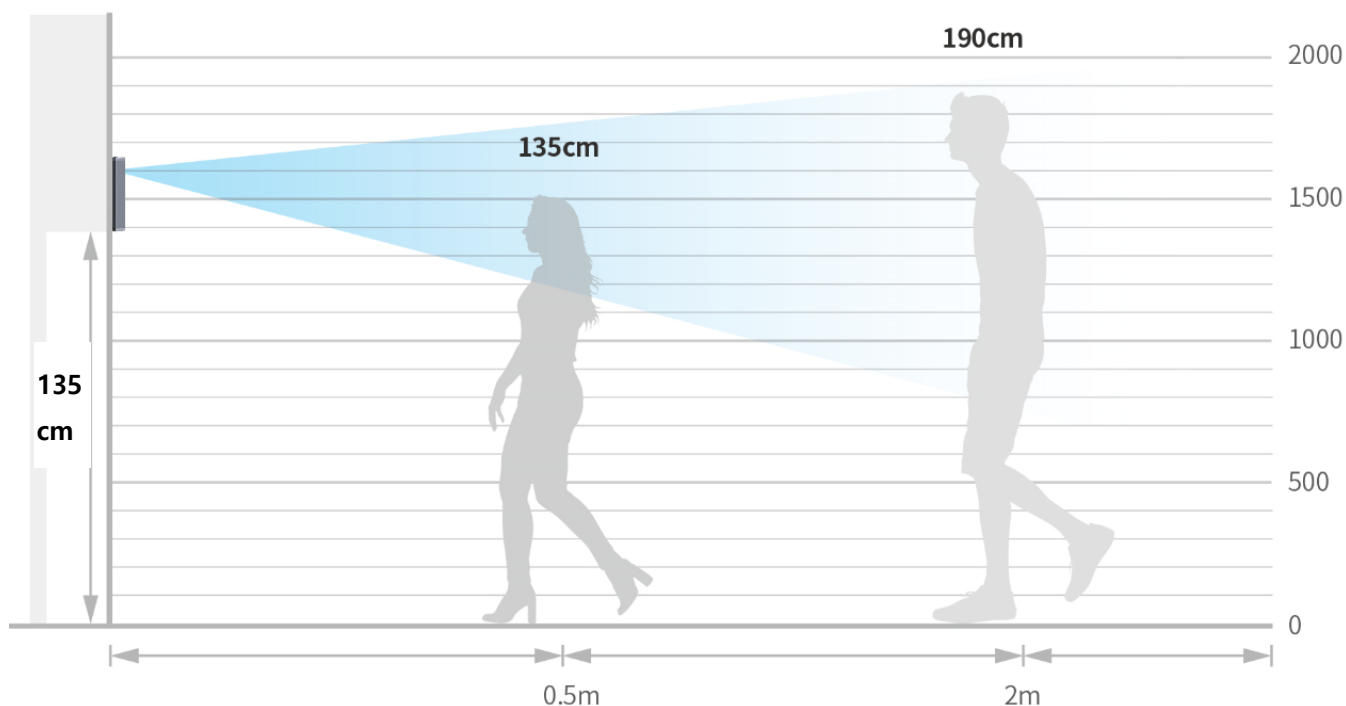
● Caution

Do not install in a place exposed to direct sunlight. ->There is a risk of malfunction, and there is a risk of deformation and discoloration.		Do not install it in a place with a lot of moisture or dust. ->There is a risk of failure.	
Do not spray water directly to clean or wipe with benzene, thinner, alcohol, etc. ->There is a risk of electric shock and fire.		Keep magnets away from the instrument. -> There is a risk of failure and malfunction.	
Do not contaminate the fingerprint access. ->Fingerprints cannot be recognized correctly.		Do not spray the terminal with insecticides or flammable sprays. ->There is a risk of deformation and discoloration.	
Do not shock the instrument or touch any sharp objects. ->The product may be damaged and cause a failure.		Do not install in places with severe temperature changes. ->There is a risk of failure. -> Be careful of burns when using the product	

- Failure to comply with what is indicated may result in injury or property damage to the user.

※ We will not be responsible for accidents and damages caused by not using it according to the contents of the instruction manual.

1.1.1 Installation Height and Authentication Range



1.1.2 Installation Precautions

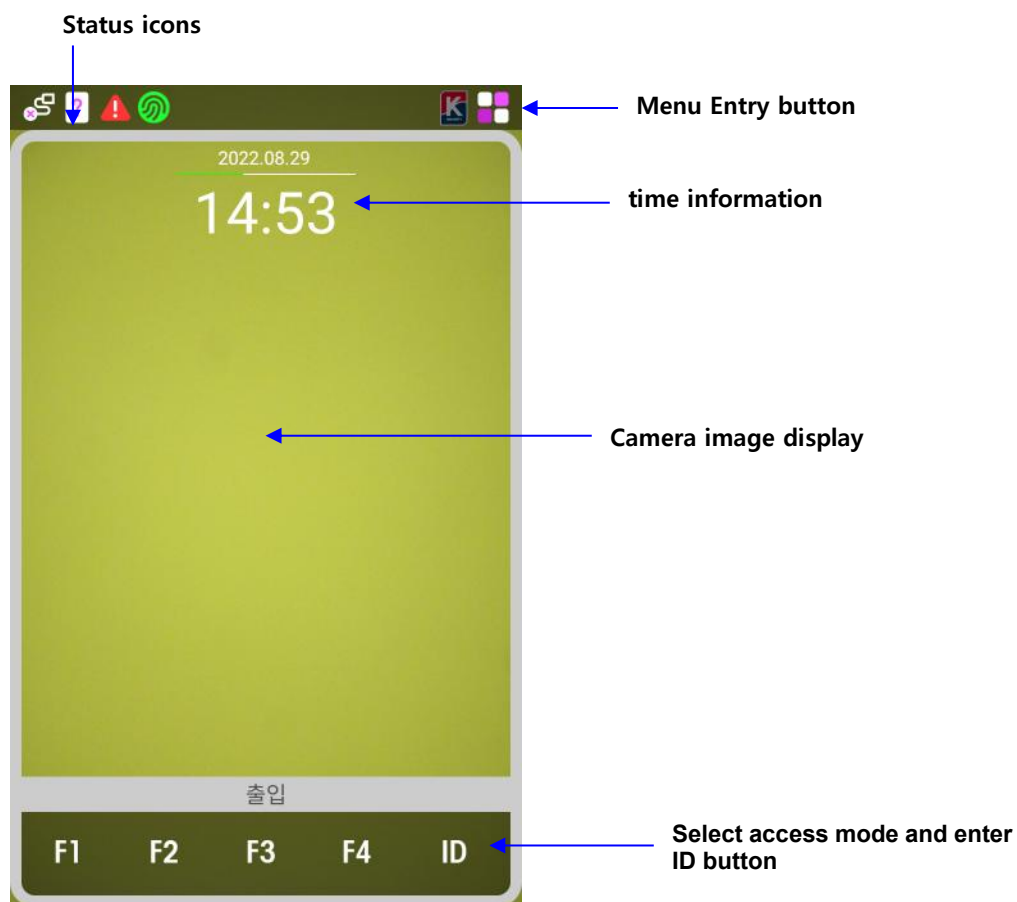
- Please install the device at a height of 135 cm from the bottom of the product.
- Do not install the device under lighting that uses incandescent bulbs.
so, it is recommended to adjust the installation location if strong lighting directly illuminates the face recognition camera.
- Installation is not recommended in environments with backlight or direct sunlight.
- When installing the product in locations where illumination exceeds 30,000 lux, appropriate measures such as adjusting the installation position or providing shade for the device should be taken.
- Do not install identical products within 50 cm of each other.
- Follow the recommended installation height. Installing the device too high or too low may reduce recognition performance due to face angle variations.
- If the wall surface is uneven, the tamper function may not operate properly.
- In locations where people may linger or wait (such as near elevators), it is recommended to reduce the face recognition distance.
- When installed on speed gates, ensure that the view area does not overlap with adjacent gates. If necessary, adjust the authentication area width to prevent false recognition of users standing near adjacent gates.

1.2. Specific names of the terminal (XScan fitted appearance)

◆ XScan: Optional terminal with fingerprint, QR reader



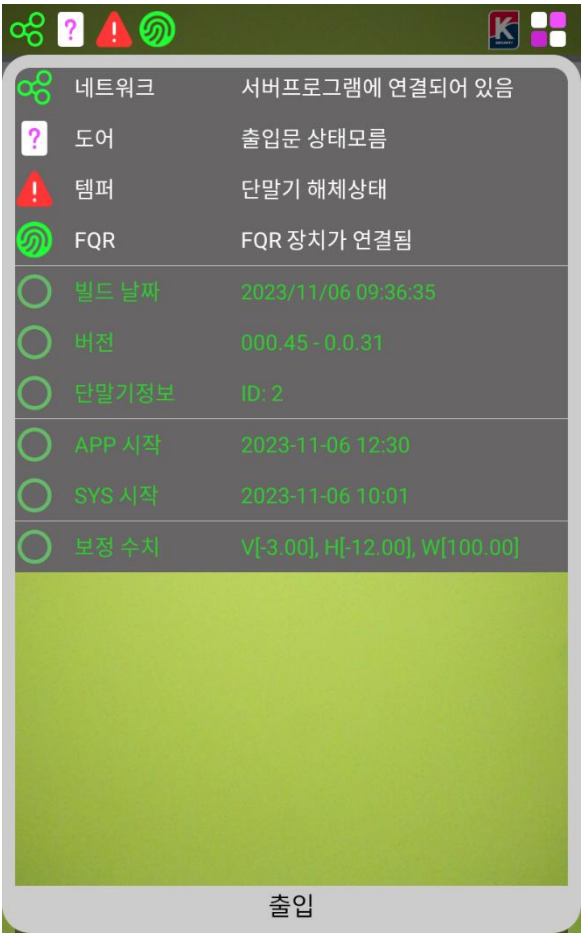
1.3. Information on the screen that comes out when it's operational



1.3.1 Icon Guide

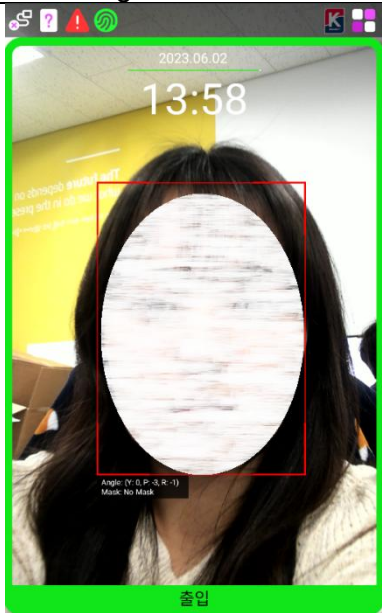
	Unconnected to the Internet		LAN wire not connected
	Internet connection status		Not connected to server program
	Low light detection status		Connected to a server program
	Fire sensor detected status (Fire detection on the appropriate terminal)		Poor connection to thermal sensor
	Fire sensor detected status (Fire detection from server)		Thermal sensor connection normal
	Terminal disassembly status (Magnet type temperature switch operation state)		Lock Status Continuous Unsetting Status (Continuous Open is set on the server)
	Terminal disassembly status (Electric Temper Switch Operation Status)		Lock Status Continuous Unsetting Status (Schedule Open)
	Do not know the status of the door		Warning sound (fire alarm)
	Door closed		Warning sound (Delete terminal warning sound)
	Door open		Warning Tone (Forced Intrusion)
	Door abnormality (Forced intrusion)		Warning tone (continuous door open)
	Door abnormality (Continuous door open)		Alert sound (emergency alert sound by server)
	XScan connection status		Live view in operation
	Live view not in operation		

1.3.2 Real-time check of icon and terminal details

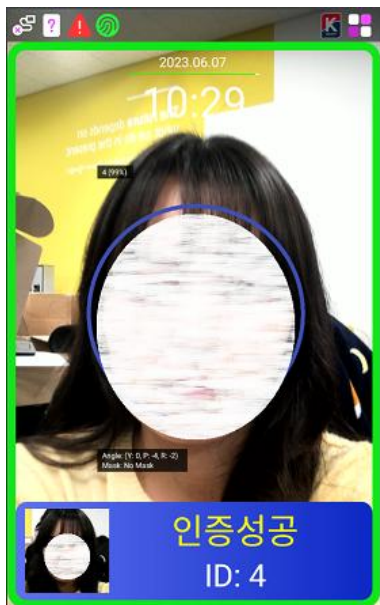


Click the top bar to see detailed information about the terminal's status.
(The XScan status is marked when the XScan is installed.)

1.3.3. Message Guide



- Default screen



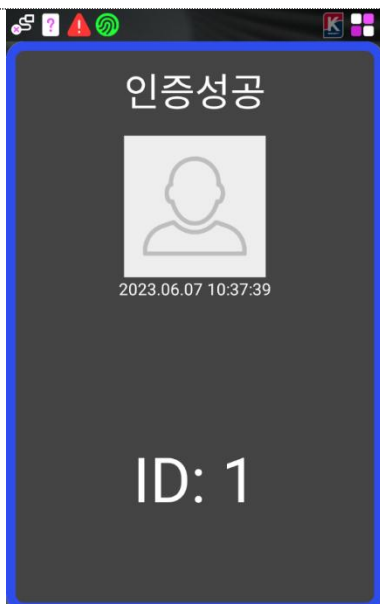
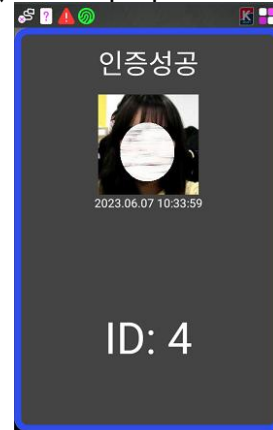
- Upon successful authentication (for face authentication)
: The design changes depending on the pop-up type selected.

<- For the bottom pop-up (default setting)

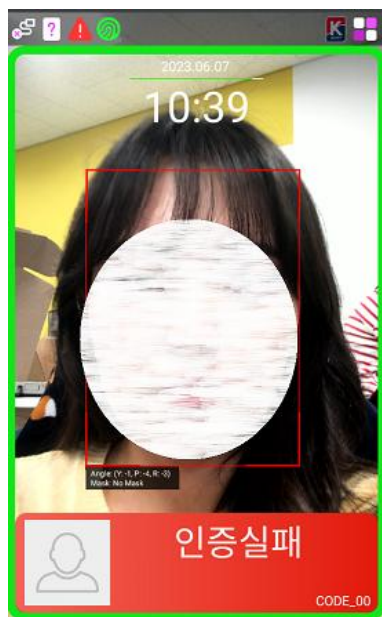
↓ List Pop-up



↓ Full Pop-up

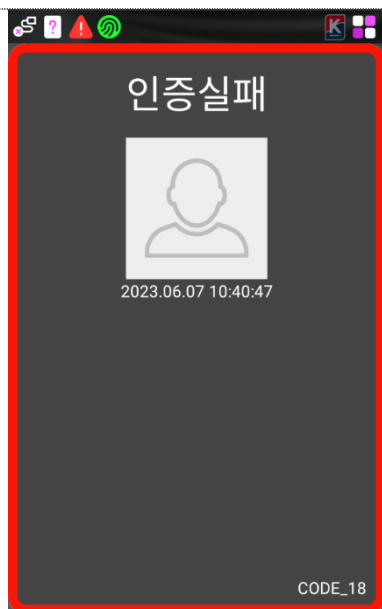
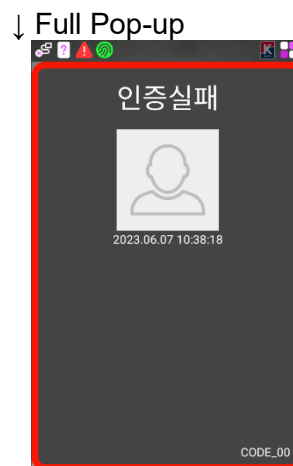
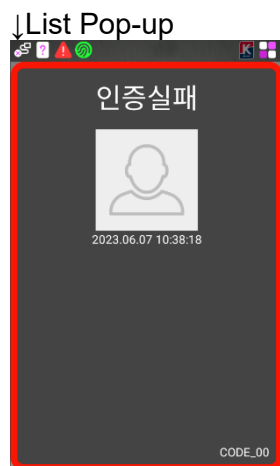


- Upon successful authentication (For authentication methods other than face)

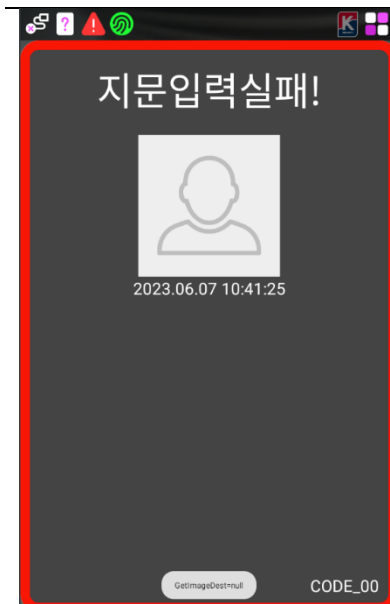


- If authentication fails (for face authentication)
: The design changes depending on the pop-up type selected.

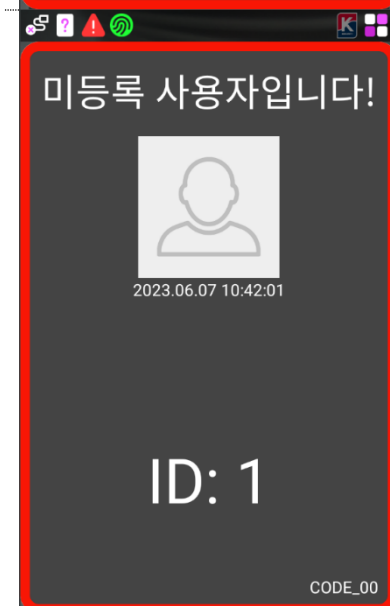
<- For the bottom pop-up (default)



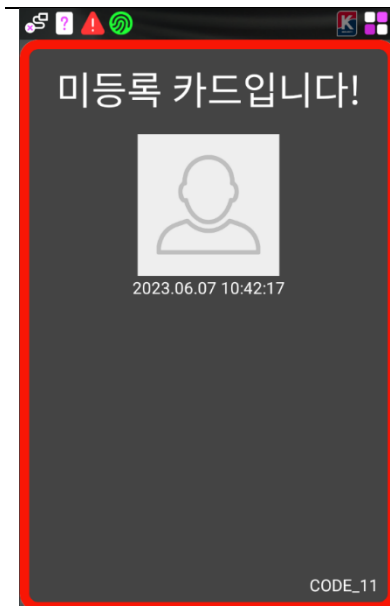
- In case of authentication failure (For authentication methods other than face)



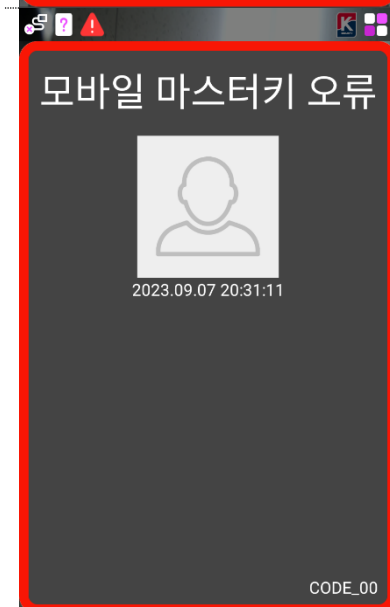
- In case of fingerprint input failure



- If you enter an unregistered user ID



- If you enter an unregistered card



- In case of mobile master key error
(If the mobile master key is not correct)



- In case of a pass-back error when using the anti-pass-back function



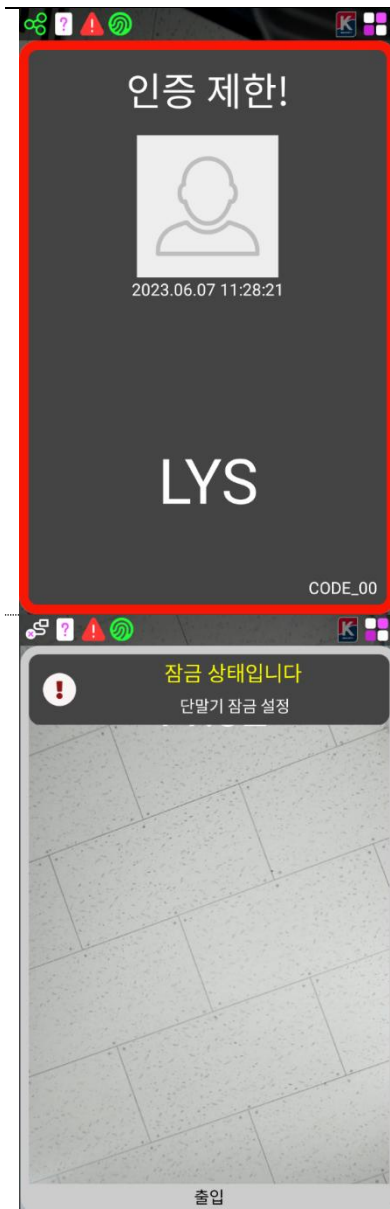
- When used as meal management
Users attempt to authenticate more than once at the same time of meal in one case



- If there is no response from the server while attempting server authentication
- Network connection is lost while attempting a server authentication

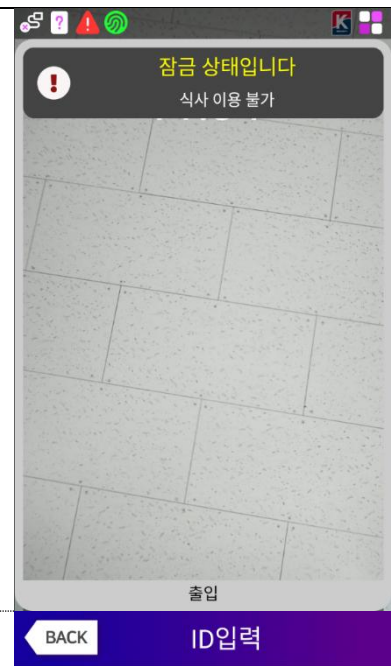


- Registered but not authorized to authenticate
- Attempt to authenticate when it is not accessible



- The user is blacklisted

- If you set the terminal locked



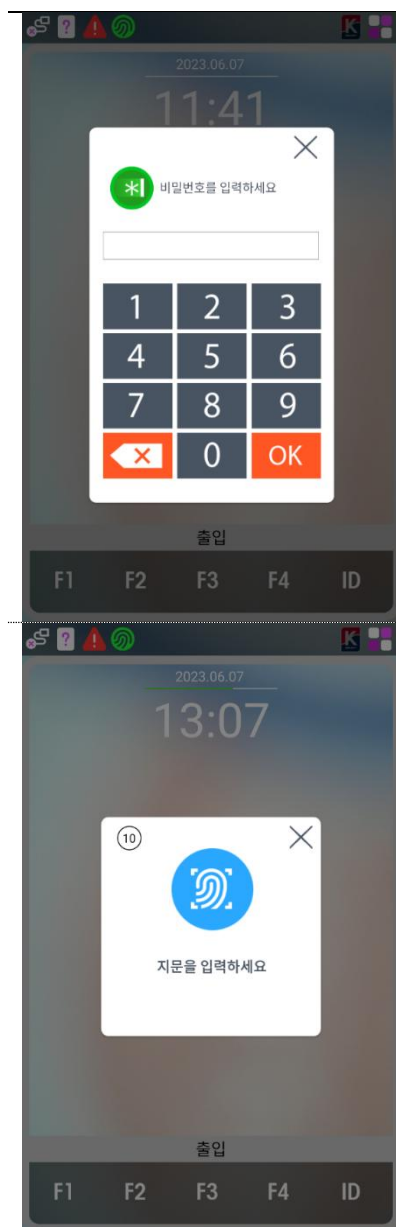
- If it is not mealtime when setting it as meal management

사용자 ID를 입력하세요



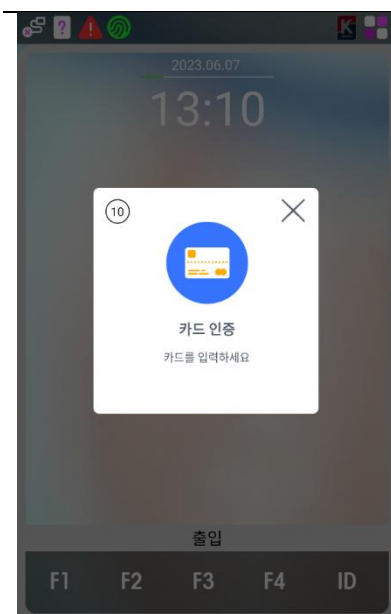
1	2	3
4	5	6
7	8	9
←	0	OK

- Waiting for User ID access

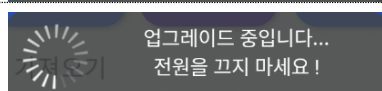


- Waiting for password access

- Waiting for fingerprint access



- Waiting for card access



- When upgrading a terminal program
(Do not power off the terminal when it is outputting this message.)



Authentication is successful if the criteria for determining fever symptoms (37.5°C) are less than the criteria



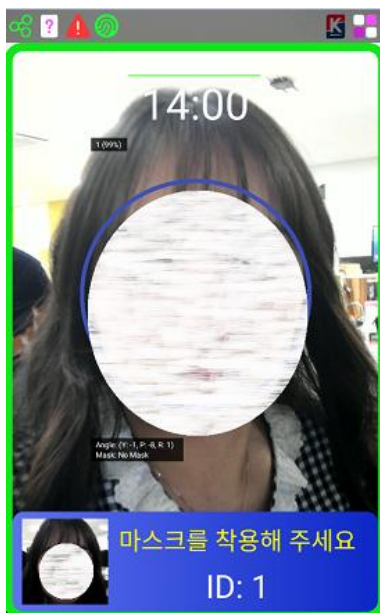
Authentication failure if fever symptoms exceed the criteria (37.5°C)



- If the distance is too close to the face authentication

Message without mask

: The design changes depending on the pop-up type selected.



<- For the bottom pop-up (default)

- List pop-up:



- Full pop-up:



No messages are displayed in the pop-up
Only "Please wear a mask" audio is output.

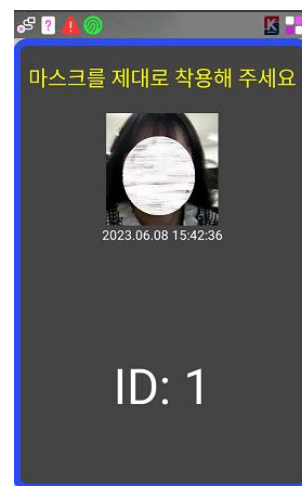
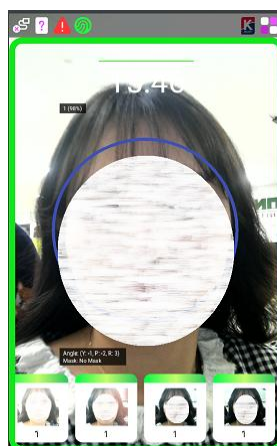
Message when you don't wear a mask properly
e.g.) On the chin

: The design changes depending on the pop-up type selected.



<- For the bottom pop-up (default)

- List pop-up: - Full pop-up:



No words are displayed in the pop-up
Only "Please wear a mask properly" audio is output.

1.4. Voice guidance during operation

Operation Classification	Voice guidance
Authentication Success	You are authorized
Authentication Failure	Please try again

1.5. Information on the buzzer that comes out during operation

Voice volume off situation	Beep	Notification sound when reading a fingerprint or card	- If you read the card - If you enter a fingerprint in the fingerprint window
	Be-Beep	Authentication Failure	If authentication fails
	Beep	Authentication Success	If authentication succeeds

1.6. Proper face registration and authentication methods

- How to register your face
 - Keep the distance between the terminal and the face at approximately 50 cm. (Position the face into the guidelines of the LCD screen)
 - Follow the instructions to register your face pose. However, please keep the movement stationary when taking registration photos.
 - For face registration, register after sweeping up the lower part of your face, including the eyebrows, so that they are not covered by your hat or hair. (Based on passport photos)
- Precautions for Face Registration
 - You can register (recommended) directly using the terminal or with photos of good quality within the last 3 months.
 - Staring straight ahead (natural face with mouth closed) take pictures of your face according to the guidelines displayed on the screen.
 - Make sure that the entire face, including eyes, eyebrows, forehead, nose, mouth, and jawline, comes out well.
 - The background should be taken on a bright, solid background without other people's faces or objects.
 - Face registration proceeds without obstacles that may interfere with extracting facial feature points such as masks, hats, mufflers, and excessive accessories.
 - The minimum size must be at least 200 x 200 pixel when registering as a photo.

※ When registering a face, a similar face check is performed, and the feature is checked only among users whose face is included in the user's authentication combination (the same applies when registering a fingerprint)

※ When registering your face, we recommend that you register your appearance in normal times.

※ If there is a change in style (dye, eyeglass frame, bangs, etc.), we recommend re-registration.

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

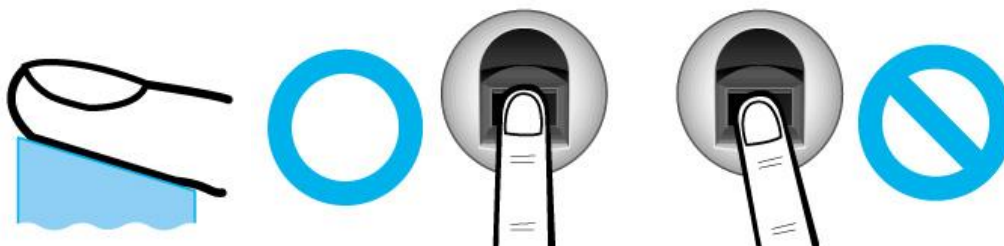
- How to authenticate your face
You can stare at the camera from the front.
- Restrictions for Face Authentication
 - Facial recognition is a biological technology that is affected by ambient illumination and should be installed and used in an environment where the effect of illumination is minimized, and it is best to register/authenticate at the place where the recognizer is installed.
 - Posing differently from your registered face or changing your appearance can reduce your face recognition rate.
 - If you raise or lower your head during face authentication, face authentication may fail, so you need to look straight ahead and authenticate.
 - Thick eyeglass frames or sunglasses can reduce facial recognition because they cover the feature points around the eyes.
 - Face authentication may fail if your eyebrows are covered by hair or glasses.
 - Covering a large portion of your face with hair or a mask can reduce your facial recognition rate.
 - After installing the terminal, remove the product's protective film and use it when registering and authenticating the face. The protective film will cause a decrease in recognition rate.

1.7. Proper fingerprint registration and access method

◆ **For fingerprint registration and authentication, an optional XScan must be installed.**

- How to enter the correct fingerprint

If possible, use your index finger to enter it as if you are stamping your hand.
It is not a valid registration/entering method to enter just the fingertips.
Ensure that the center of the fingerprint touches the fingerprint input.
(Be careful as there is a risk of low-temperature burns when entering fingerprints.)



- Please enter the fingerprint of the index finger as much as possible.

You can enter your fingerprints accurately and reliably with your index finger.

- Make sure the fingerprints are not clear or there are wounds.
Excessively dry or wet fingerprints, blurry fingerprints, and fingerprints with wounds are difficult to recognize. In this case, register the fingerprint of the other finger.

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics



- Points to Note for User Fingerprint Status

Depending on the user's fingerprint status, the fingerprint may not be available or inconvenient to use.

- This product is a fingerprint recognition system, and if the fingerprint is damaged or soft, the fingerprint cannot be used and must be operated with a password.
- **If your hands are dry, blow it and use it** to operate smoothly.
- For children, if the size of the fingerprint is too small or too thin, it may be difficult or impossible to use, and a new fingerprint needs to be registered every six months.
- In the case of the elderly, if the balance is severe in the fingerprint to be registered, it may not be registered.
- It is recommended that you register more than one fingerprint of the user, preferably.

2. Product Introduction

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

2.1. Product Features

- Multi-Modal products that can use both face and fingerprint authentication
- Walk-through products allow you to authenticate your face by staring at the camera
- Apply resolution with FHD (5M) image
- Dual Camera (Color & IR) with Live Detection
- RF (125 kHz) with Smart Card (13.56 MHz) Reader
- Easy self-authentication through face or fingerprint
 - The use of biometric technology (biometrics), facial recognition and fingerprint recognition technology, can prevent the risk of forgetting passwords, loss of cards or keys, or theft, and strengthen security by using one's own biometric information
- Access Management System Using Network (LAN)
 - Since the fingerprint recognizer and the authentication server communicate using the TCP/IP protocol, it can be applied to the existing network as it is, making it easy to expand. 10/100 Mbps Auto Detect ensures fast speed, as well as ease of management and monitoring over the network
- **Provide various registration and authentication methods**

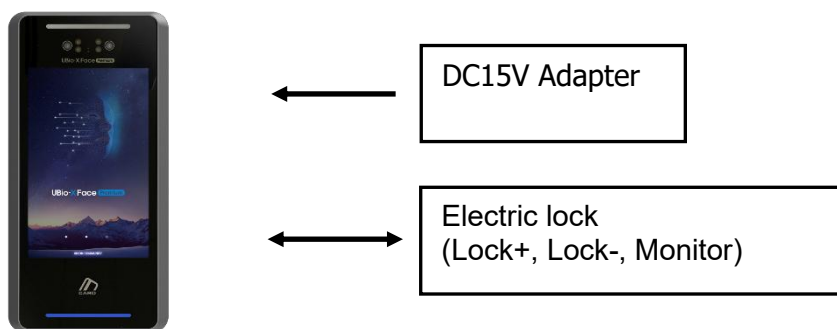
The face	Face registration Face verification
Fingerprints	Fingerprint registration fingerprint authentication
Card	Card registration Card Authentication
Password	Password registration password authentication
Card OR fingerprint	Card, Fingerprint Registration Card or fingerprint authentication Fingerprint authentication after ID input
Card & Fingerprint	Card, Fingerprint Registration Card authentication and fingerprint authentication ID input card authentication and fingerprint authentication
Card OR password	Card, password registration Card Authentication Authenticate password after entering ID
Card & password	Card, password registration Card authentication and password authentication ID input card authentication and password authentication
Fingerprint OR password	Fingerprint, password registration fingerprint authentication

	Fingerprint authentication after ID input, password authentication in case of failure
Fingerprint & Password	Fingerprint, password registration Fingerprint authentication and password authentication ID input fingerprint authentication and password authentication
Card OR face	Card, Face Registration Card or Face Authentication Face authentication after ID input
Card & face	Card, Face Registration Card authentication and face authentication ID input card authentication and face authentication
Face or password	Face, password registration Face verification Face authentication after ID input, password authentication in case of failure
Face & password	Face, password registration Face authentication and password authentication ID input, face authentication, and password authentication
Fingerprint or face	Fingerprint, Face Registration Fingerprint or Face Authentication Fingerprint authentication after ID input, face authentication in case of failure
Fingerprint & face	Fingerprint, Face Registration Fingerprint authentication and face authentication After entering ID, fingerprint authentication, and face authentication
Card OR fingerprint OR face	Card, Fingerprint, Face Registration Card or fingerprint or face authentication Fingerprint authentication after ID input and face authentication in case of failure
Card & Fingerprint & Password	Register your card, fingerprint, password After card authentication, even fingerprints and passwords After ID input card authentication, fingerprint and password authentication
Card & face & password	Card, face, password registration After card authentication, even face and password authentication After ID input card authentication, even face and password authentication
Card & fingerprint & face	Card, Fingerprint, Face Registration After card authentication, fingerprint and face authentication After ID input card authentication, fingerprint and face authentication
Fingerprint & face & password	Fingerprint, face, password registration After fingerprint authentication, even face and password

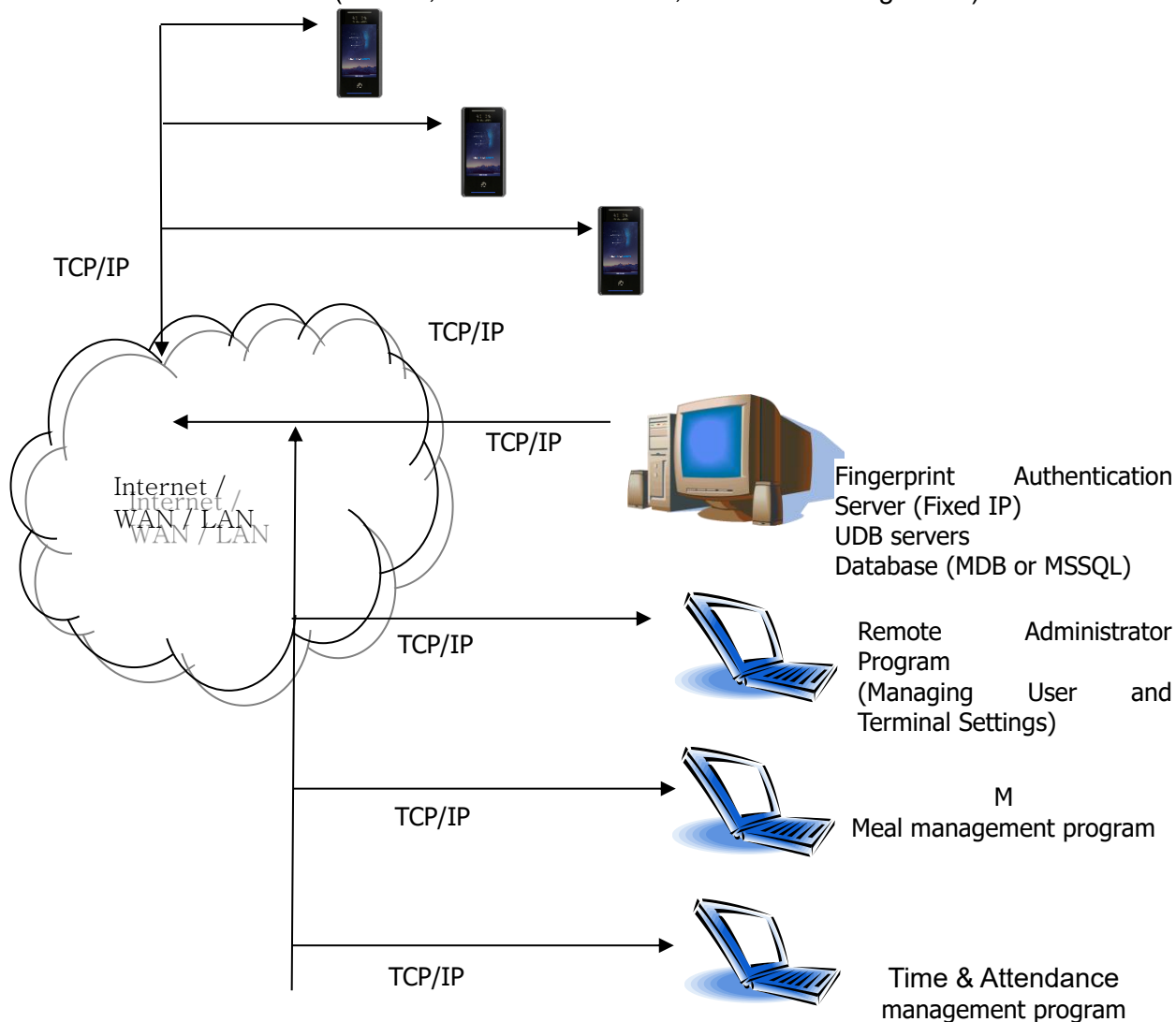
	authentication ID input fingerprint authentication and face and password authentication
Mobile card	Mobile card authentication
Card OR mobile card	Card registration Card or mobile card authentication Card authentication after ID input, mobile card authentication in case of failure
Mobile Card OR Fingerprint	Fingerprint registration Mobile card or fingerprint authentication Fingerprint authentication after ID input
Mobile card OR face	Face registration Mobile card or face authentication Face authentication after ID input
Mobile card OR Password	Password registration Mobile card or password authentication Authenticate password after entering ID
Mobile card OR fingerprint OR face	Fingerprint, Face Registration Mobile card or fingerprint or face authentication Fingerprint authentication after ID input and face authentication in case of failure
Card OR mobile card OR face	Card, Face Registration Card or mobile card or face authentication Face authentication after ID input
Card OR mobile card OR fingerprint	Card, Fingerprint Registration Card or mobile card or fingerprint authentication Fingerprint authentication after ID input

2.2. Configuration Diagram

2.2.1. Standalone (Access)



2.2.2. Connect with PC server (access, Time & Attendance, and meal management)



2.3. Product Specifications

Division	SPEC	REMARK
CPU	Cortex A53 Quad Core 1.8GHz)	
LCD	8" 800 x 1280	
MEMORY	eMMC 16GByte	
	LPDDR4 / 4GByte x 1EA	
External USB support	Data Backup / FW Upgrade	
Camera	Dual Camera (Color & IR)	
Number of users	500,000 User / 500,000 Card Finger 1:1 -> 500,000 / 1:N -> 50,000 Face 30,000 10,000,000 Log / 20,000 Image Log	
Fingerprint sensor	Optical	options
Scan Area / Resolution	13 * 14.8mm / 500 DPI	
Temperature / Humidity	-20 ~ 60°C / Lower than 90% RH	
AC / DC Adapter	INPUT : Universal AC100 ~ 250V	
	OUTPUT : DC 15V / (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 (Used with Lock Control)	
Communication Port	TCP/IP (10/100Mbps)	Authentication Server Communication
	RS-232	A meal ticket printer
	RS-485	Controller communication
	Wiegand In/Out	Card reader or Controller communication
Card Reader	125KHz EM/HID & 13.56MHz Smart Card Reader, ISO14443A/B, MiFare, MiFare Plus, Felica, ISO15693, DESFire EV1/EV2, SE iCLASS (Option)	options
SIZE	143.3 x 289.5 x 23.8 (mm)	

3. Configuration Settings

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>



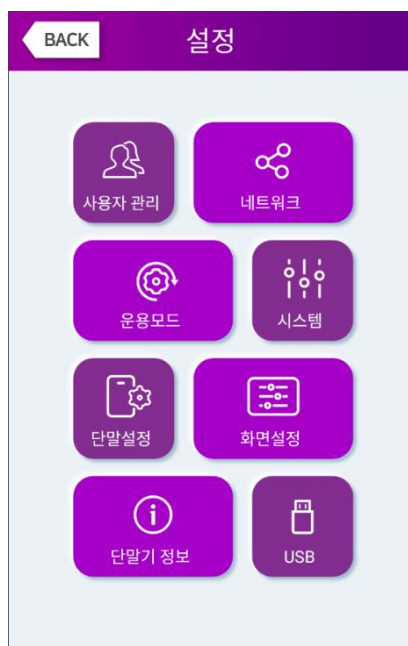
3.1. Pre-Environmental Settings Confirmation

3.1.1. Enter the menu

Press the [] icon on the main screen to enter the main menu screen as shown below.

For European-oriented products, pressing the menu icon in the absence of an administrator will take you to the screen where you set the administrator. If you have an administrator, go through administrator authentication and then enter the menu screen. And send a notification to the server if administrator authentication fails.

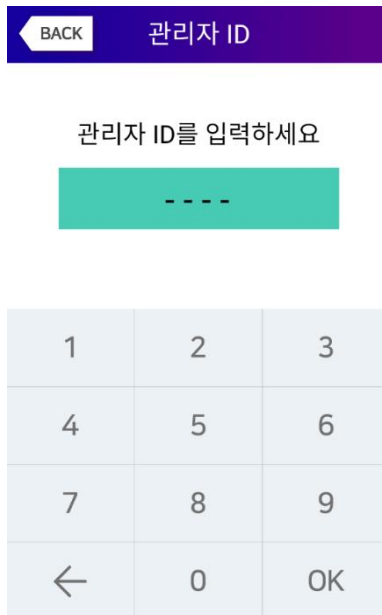
If authentication fails more than 5 times, access is not allowed for 5 seconds.



Movements to each submenu can be entered by pressing the corresponding button

3.1.2. Administrator Authentication

If the administrator is registered, the administrator authentication screen will appear first, as shown below.



1	2	3
4	5	6
7	8	9
←	0	OK

▶ Administrator authentication

When you enter an administrator ID, you authenticate the administrator with a card, fingerprint, face, or password, depending on how that administrator authenticates. Once the authentication is successful, you can enter each menu.

Administrator authentication appears only if you have a registered administrator. When entering the menu mode, it is authenticated only once, and access to all menus is possible until completely exiting the main menu.

ps) Only card (mobile card), only fingerprint or card (mobile card) or if fingerprint is included in the authentication method, you can access the menu at the time of authentication without entering your ID.

3.1.3. How to enter the menu without administrator authentication

This is a way to enter the menu if you lose the manager card registered in the terminal or if you cannot authenticate your fingerprint or face because there is no manager

- ① Remove the bracket on the back of the terminal to keep the lid open
- ② With the lid open, connect the lower 5 pin connectors 1 and 3, and 2 and 4 pins on the back of the terminal as shown below



<Figure 3-2>

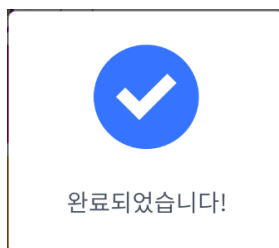
- ③ Press the icon on the main screen to  enter the administrator authentication screen of <Figure 3-2>, fill the administrator ID with '00000000' (user ID length) and press the  to enter the menu screen.

▶ 0 must be pressed by the length of the user ID to be recognized as "00000000".

- ▶ Make sure to remove the connector connection pin after modifying the setting value

3.1.4. Saving Settings

If you click **the Finish** button on each menu to save the changes after changing the settings, the settings on the screen are saved and a message box appears as shown below.



- ▶ If there are no changes, you will be moved to the previous menu screen.
- ▶ If there is no input for 30 seconds while you are changing the settings in the menu, you will exit to the previous menu.

3.2. Menu Configuration

1. User	1. Add 2. Modify 3. Delete 4. Delete All 5. View	
2. Network	IP address	Fixed IP / DHCP / Wireless LAN (optional) ▶ IP address ▶ Subnet mask ▶ Gateway
	DNS server	▶ DNS Server 1 ▶ DNS Server 2
	Server IP	▶ Server IP ▶ Port
	Terminal ID	▶ Terminal ID
3. Application	1. Operation mode	▶ Access / TNA management / Meal management 1. Access or TNA ▶ Schedule F1 (Attend) time F2 (Leave) time F3 (Out) time F4 (In) time access time ▶ Blocking Time 2. Meal management ▶ Schedule Breakfast time Lunch time Dinner time Supper time Snack time ▶ Duplication allowed
	2. Function Key Settings	☐ Enable F1 ☐ Enable F2 ☐ Enable F3 ☐ Enable F4 ☐ ID input
4. System	1. System	▶ User ID length [2~8] ▶ Authentication: Terminal/server, terminal only ▶ Mandatory Registration ☐ Face ☐ Card

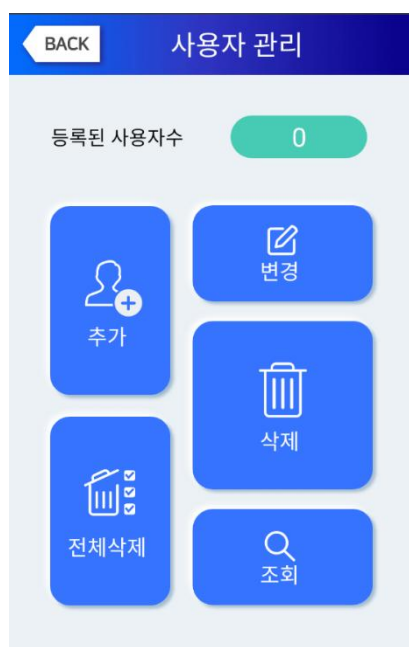
		☐ Password ☐ Name
	2. Finger	▶ 1:N level [3~9] ▶ 1:1 level [1~9] ▶ Fake finger Detection ▶ FP template format ☐ Check similar FP ☐ Multi FP ☐ Enable 1:N
	3. Face	▶ Verified distance ▶ Mask Detection ▶ AE flicker frequency ▶ AE Mode ▶ Enable Face list pop-up ☐ Anti-spoofing ☐ Using LED Lighting ☐ Multiple face detection
	4. Auth	▶ Terminal authentication method
	5. UBio-Core	☐ Live View ☐ Intercom ☐ Control Room Only Phone number length Call Time ▶ Tel Numbers Edit
	5. Date/Time	▶ Time synchronization ▶ Display Format ▶ Set Date ▶ Set Time
	6. Database	1. Delete All Users 2. Delete Setting 3. Delete Log 4. Delete Image Log 5. Factory Init 6. Reboot 7. Restart app
5. Terminal	1. Sound	▶ Voice Volume ▶ Beep Volume ▶ Sound Option
	2. Terminal Options	▶ Read Card number ▶ Card Format ▶ Card reader ▶ Ble Rssi ▶ Ble TxPower ☐ Lock terminal

	3. Input	▶ M0 ▶ M1 ▶ M2 ▶ IO ▶ Warn door open (sec) ☐ Tamper alarm
	4. Lock	▶ Lock1 Option ▶ Lock2 Option ▶ Lock1 duration (ms) ▶ Lock2 duration (ms)
	5. External Device	▶ RS232 Options ▶ RS485 Options ▶ Wiegand Site Code ▶ Wiegand Output ▶ Wiegand Input ▶ External Reader
	6. ETC. (Thermal)	☐ Thermal Camera Use ▶ thermal mode ▶ Display ▶ Fever temperature ▶ Thermal setting
6. Display	1. Camera	▶ Save Option ☐ Save success log ☐ Save failed log ▶ Save failed face ▶ Camera ISP (Gamma) ▶ Camera calibration
	2. Language	▶ Language
	3. LCD Options	▶ Power saving mode ▶ Display Option ▶ Touch calibration
	4. Message display time	▶ Message display Time (ms)
7. Info	1. System	▶ System Info ▶ Disk ▶ Ram
	2. Terminal	▶ Terminal info - Terminal ID/Application/Language /Stored Voice ▶ Access Control Info View ▶ Schedule Info View
	3. Network	▶ Network info

		MAC <Ethernet> IP
	4. User	▶ User
	5. Log	▶ Log
	6. About	▶ About
8. USB	1. Export	1. User Data 2. Event Log 3. System Option 4. Export All 5. Picture 6. Debug Info
	2. Import	1. User Data 2. System Options
	3. Others	1. Theme 2. F/W Upgrade

3.3. User Management

When you select **[User]** from the main menu, the screen below appears.



Displays the total number of registered users, including administrators, at the top of the screen

To add a new user, click **Add** button
 To change the user, click **Change** button,
 To delete a user with a specific ID, click **Delete** button,
 To delete all users, click **Delete All** button,
 To view the list of registered users, click **View** button.

3.3.1. Add

If you choose **User Management [Add]** from→ the main menu, the screen below appears



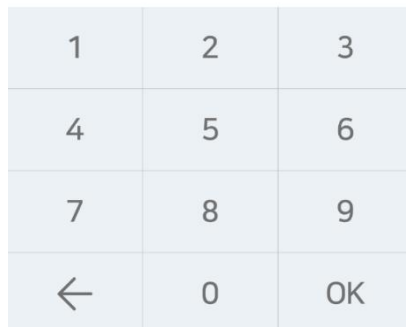
Enter the user ID you want to register and click the **OK** button.

사용자 ID를 입력하세요

0001

In this case, it automatically shows the ID that can be registered on the screen, so you can register conveniently. To change the ID, click the [] button  to delete and enter the existing value.

To cancel and exit, press the **[BACK]** button.



If you enter an ID that is already registered, you will receive a failure message, and if it is an ID that is not registered, you will see the screen below.



Each icon on the left has a meaning below

-  : Number of registered faces
-  : Number of registered fingerprints (X,1-10)
-  : Password registration status (X: not registered, 1: registered)
-  : Number of registered cards (X, 1-10)
-  : Whether the mobile key is registered (X: not registered, 1: registered)

사용자 : Users
관리자 : Administrator

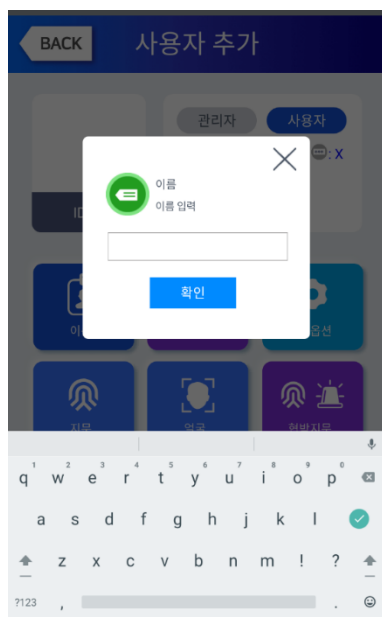


<Additional XScan Options>

You can register by clicking [name], [employee number], [fingerprint] for fingerprint registration, [threat fingerprint], [face] for face registration, [card] for card registration, and [password] for password. By default, you are registered as a user, and you can change to an administrator by pressing the **Administrator** button. Press the **Save button** to save after registration is complete or **Cancel** or **Back** to exit.

※Only the user registered as an administrator can change the operation method of the terminal and register/change/delete the information of all users stored in the terminal, so care must be taken in registering the administrator.

3.3.1.1. Name Registration

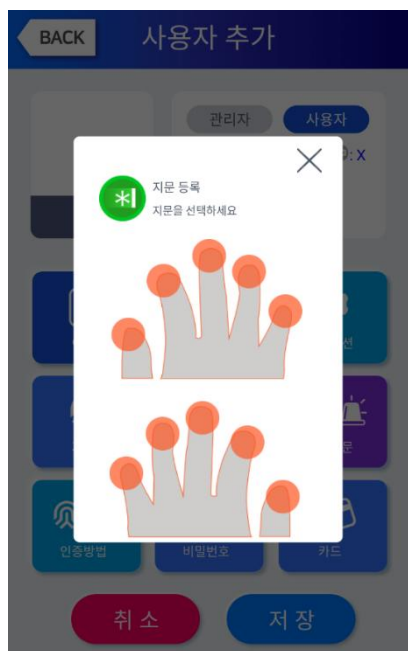


On the **Add User** screen, click **Name** to register.

Type a name using the keyboard shown below and press the OK button.

To unregister and exit, press the [X] button.

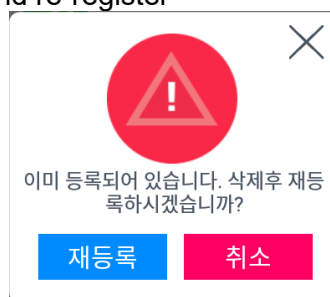
3.3.1.2. Fingerprint registration



① On the **Add User** screen, click **Fingerprint** to register. To unregister and exit, press the [X] button.

When the left screen appears, select the finger you want to register

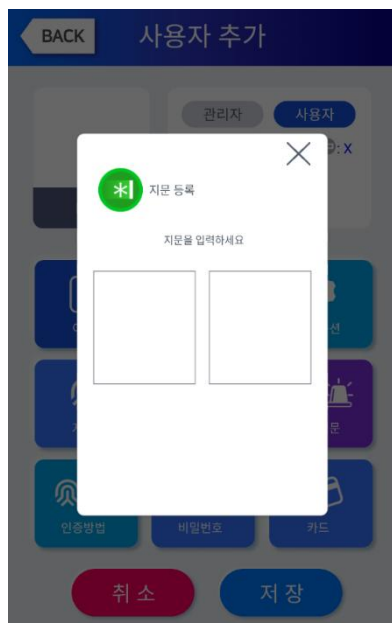
※ If multiple fingers are registered, the fingers already registered will be shown in a blue circle (●) and the double threatening fingerprint will be shown in a purple circle (●). If you select an already registered finger, you will see the following message, and if you select Re-register, you can clear the existing registered fingerprint and re-register



※ Threatening fingerprints **(requires server interworking)**

Authentication is successful when authenticating with threatening fingerprints, but the server notifies that it is a threat authentication attempt.

※ If you authenticate the finger registered as a threat fingerprint, you can send an alarm message to the server and give a contact signal if you set it to threat situation notification in 3.7.4.Lock setting

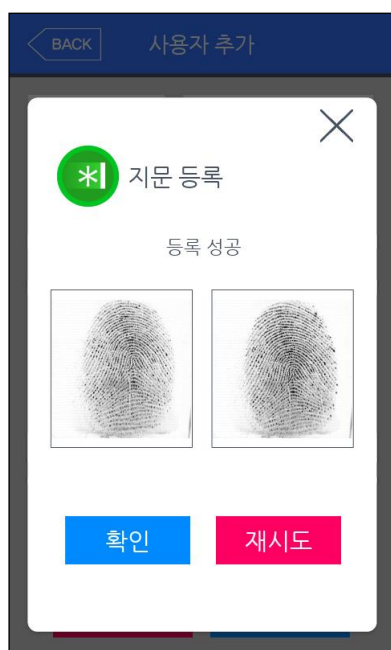


② Refer to '1.7. Proper fingerprint registration and access method' to enter your fingerprint. Fingerprints are entered twice according to the screen guidance as follows.

Please enter your fingerprint When the fingerprint sensor lights up with the message "", put your finger on the fingerprint input window and wait 2-3 seconds for the light to go out before removing your finger.

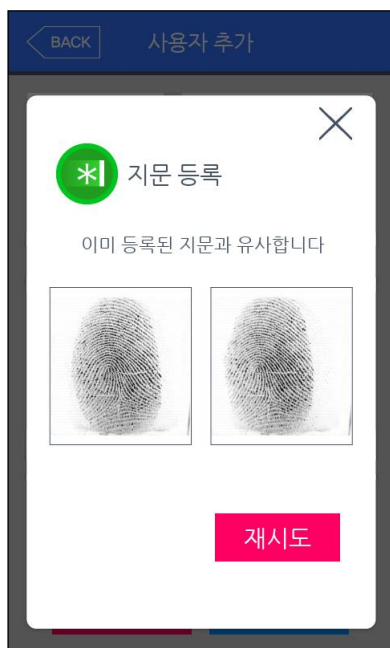
③ Please enter the same fingerprint again If you receive the message "", type the fingerprint you just entered

※When entering the second fingerprint after entering the first fingerprint, you must remove the finger from the fingerprint input window and re-enter it.



④ When the input is complete, a message such as the one on the left appears. Press **the OK** button to complete the registration and go to the parent menu.

To re-register, press **the [retry]** button to restart the above process, and to cancel, press the [X] button to exit



If the fingerprint is similar to the fingerprint already registered, the message "It is similar to the fingerprint already registered" appears as shown on the left, in which case you can restart the process from ② by pressing the **retry** button.

To cancel, press the [X] button to exit the top menu

※Up to 10 fingerprints can be registered per ID, and more than 10 fingerprints cannot be registered.

According to the correct fingerprint registration method, it is recommended to use a face, password, or card if repeated attempts fail two or three times.

※When registering a fingerprint, a similar fingerprint check is performed only on the fingerprint registered in the terminal.

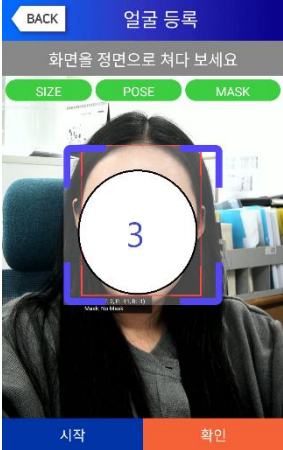
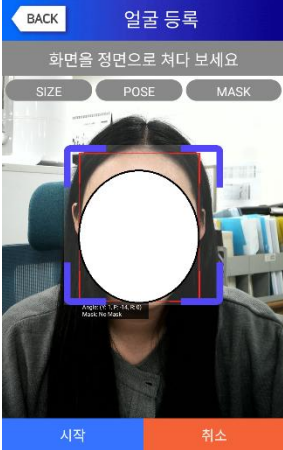
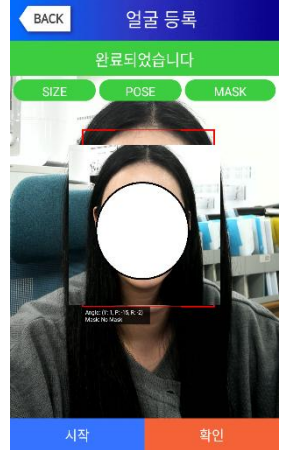
If the same user registers with a different ID on the terminal and UNIS, respectively, then UNIS

When sending a user to a terminal, it is stored without checking a similar fingerprint. It should be noted that in this case, authentication success may be achieved with different IDs.

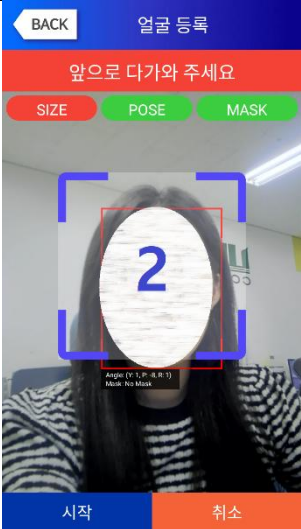
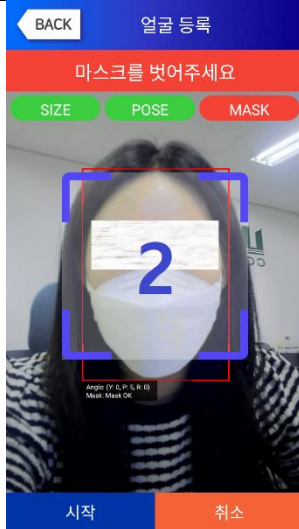
※If XScan is installed later, the fingerprint user must be downloaded from the server again.

3.3.1.3. Face Registration

Please refer to "1.6. Proper face registration and authentication method"

		
① A red guide that recognizes the face, as shown on the left screen, is outlined in blue in the center	② Click the Start button to register your face. As soon as the number on the screen is displayed as 0, your face will be registered, so make sure you don't blink at this moment. Follow the line and proceed with the registration.	③ When you finish registering, the message "Completed" is displayed as shown on the left screen, and when you press the OK button, your face registration is complete and you go to the previous screen.

If you want to re-register, press the **Start** button to start over from the process ② above

 <Face registration size is Small case >	 <Face registration size is If it's too big >	 <Wear a mask If you are registering >
--	---	--

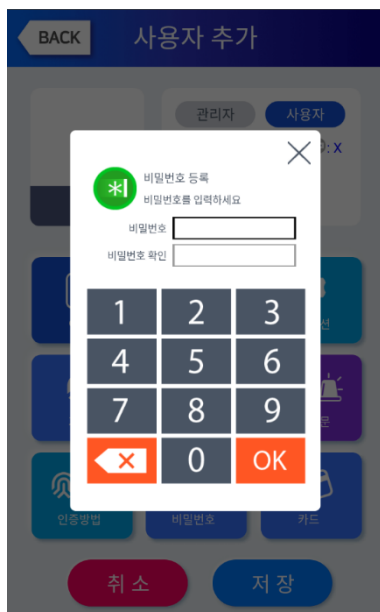
3.3.1.4. Password Registration

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

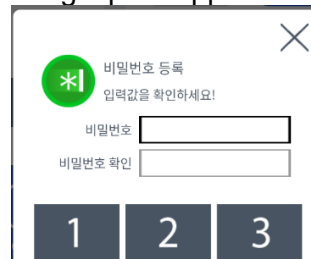
Union
biometrics



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



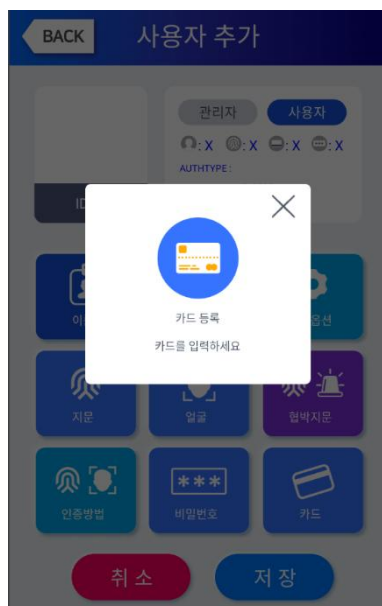
※ Threat password **(requires server interworking)**

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.

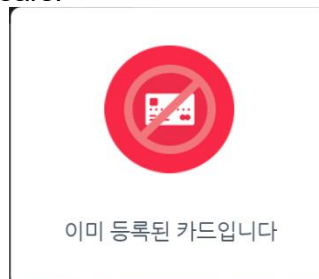
Ex) If the password is 1234, it will be certified as a duress password when entered as 4321.

3.3.1.5. 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.

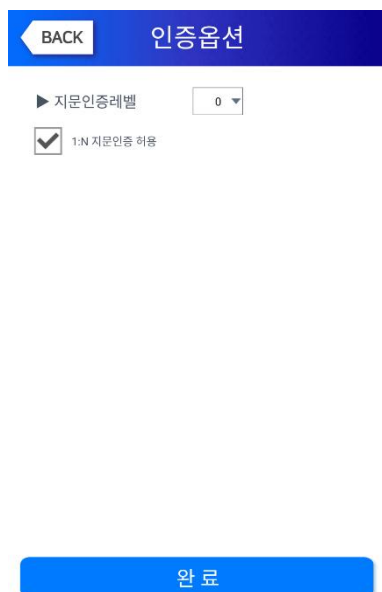
※If you entered the card already registered, the following message appears.



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

등록가능 개수를 초과하였습니다!

3.3.1.6. Authentication Option



▶ FP Level' (Basic setting: '0')

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

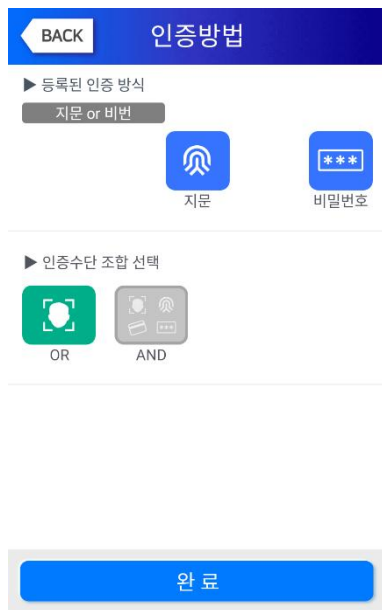
For example, if you select the "1" for FP Level, this user will be applied with "1" on 1:1 FP Level.

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

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

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

3.3.1.7. Auth Type



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

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



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

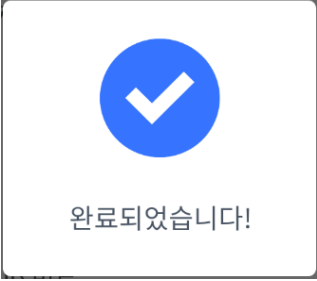
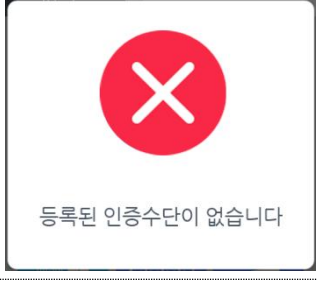
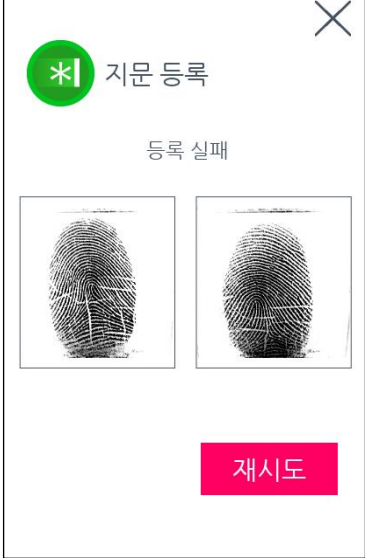
※Only OR combination is possible when using a mobile card.

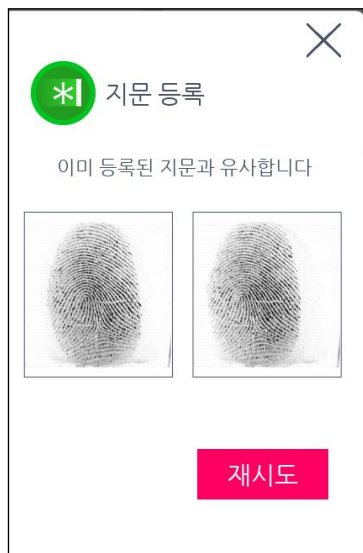
※In the case of European-oriented products, make sure that there are two or more authentication means by the administrator and that AND conditions are selected.

3.3.1.8. Save

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

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

	When you press the [Save] button the case registration was successful
	When you press [Save] button User registration fails : The case none of authentication methods such as fingerprint, face, card, and password is registered
	When you press [Auth method] button the case none of the authentication method was registered.
	In [Register FP], the case you input the different fingerprint at the fingerprint registration



In [Register FP],

the case you tried to register 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 time & 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, the 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 in the server.

It deletes both user and admin, so you should be cautious, and the user registered only in the terminal cannot be recovered.

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

 삭제되었습니다!	If deleted normally
 미등록 사용자입니다!	If you enter an unregistered ID

3.3.3. Modify

※ If you change existing data, the old data is immediately deleted. Please make sure to check the contents before changing

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

BACK
사용자 변경

사용자 ID를 입력하세요

1	2	3
4	5	6
7	8	9
←	0	OK

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

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



Each icon on the left has a meaning below

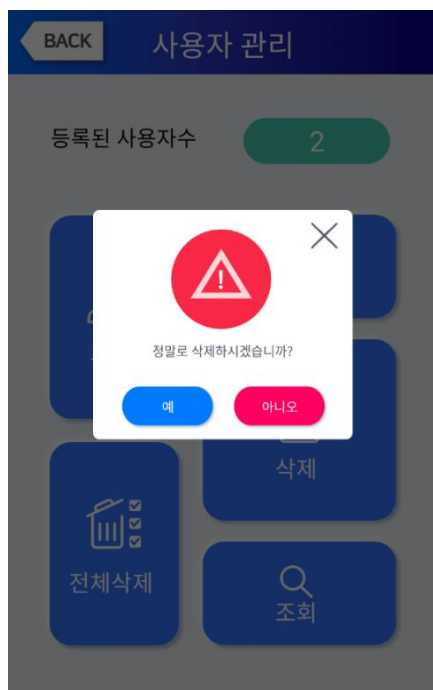
- : Number of registered faces
- : Number of registered fingerprints (X, 1-10)
- : Password registration status (X: not registered, 1: registered)
- : Number of registered cards (X, 1-10)
- : Whether the mobile key is registered (X: not registered, 1: registered)
- ID : 4** : User ID to register

사용자 : Users
관리자 : Administrator

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.

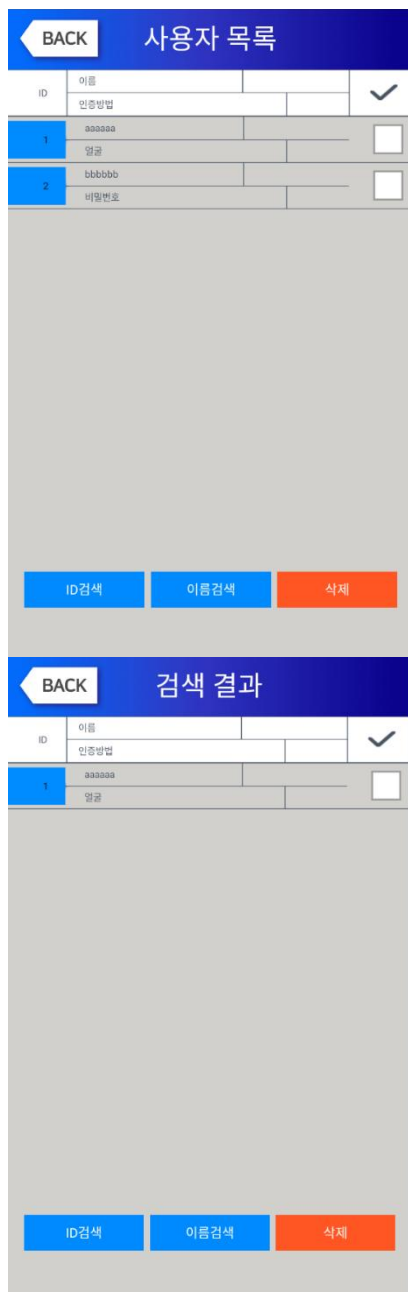


If you want to delete all the users, click **[YES]**, and if you want to cancel, click **[NO]**

※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 select [User Management] → [View] from the main menu, you can view the list of all registered users as shown below.



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.

► **[ID search]** : 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.

Ex) If you search 'm', all the users including 'm' are searched as the left picture.

3.4. Network Settings

※ **Wireless LAN is optional and only Tp-link products can be linked.**

If you select **[Network]** from the main menu, the screen below 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.

In **[Server IP Address]**, enter the server's IP address. However, if you are using DDNS provided by us, you must check DDNS ☐ to enter the information you received, and if your device is a [Static IP], you must enter at least one DNS server address.

► **[Port]**: The default port value for the authentication server (Alpeta server) is '9003', and if you change this value, the server program must change it to the same value, so be careful when changing it.

► **[Terminal ID]**: A unique ID used by the authentication server to distinguish terminals,

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

default is '1'. It must match the ID of the terminal registered by the server program and can be entered up to 9 digits.

Touch the item you want to change, and the keypad keyboard will appear at the bottom

When you are done entering the item using the keypad, continue to enter by touching the [>] button or the next input window. If you touch the desktop instead of the input window after the input is finished, the keypad disappears

Press the **Finish** button to apply the changed value after setting, or the **Back** button to cancel exiting the parent menu.

►[Wireless LAN] (Optional)

Select the Enable Wireless LAN check box to view the results of scanning the surrounding AP list as shown in the figure.

When you select the AP you want to connect to, a password access window appears. If you enter your password correctly, you will be able to access the AP and use WiFi, and you will not be able to use Static IP when you activate the wireless LAN.

After the setup is complete, press the Close button or the Back button to exit the parent menu.

3.5. Application mode

3.5.1. Application

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

In the application mode, you can select the **[Access / TNA / Meal]** according to the purpose.

3.5.1.1. Access or TNA setting

It is the screen appearing when you select the Access.

Click **[OK]** button to apply the changes, and click

[BACK] button to cancel and return.

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

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

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

- ▶ Schedule (00:00~23:59): You can set the time for each authentication mode and if you do not need the function, set '00:00-00:00'.

During the set time, the set mode is always shown unless clicking another function button, and it is convenient for the TNA management because the indication mode is changed to the set authentication mode automatically though another mode was authorized by clicking another function key. The time periods should not be overlapped, but if they are overlapped, the application order is Attend (F1) → Leave (F2) → Out (F3)

◇ In (F4) → Access. If the time is set between 23:00~01:00, it means from 23:00 to the 01:00 the following day.

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

3.5.1.2. Meal Setting

It is the screen appearing when selecting the meal Management.

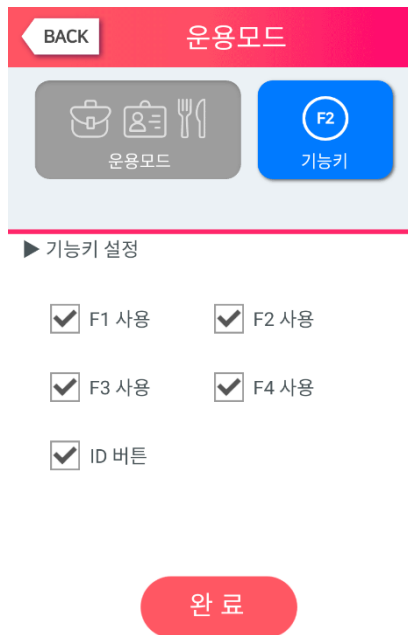
You can set the time period of each meal type. And if the setting is not needed, set '00:00-00:00'.

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

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

3.5.2. Function keys

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



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

▶ Fn Key

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

If you check 'Extended Key', you can add the authentication mode except for the existing key.

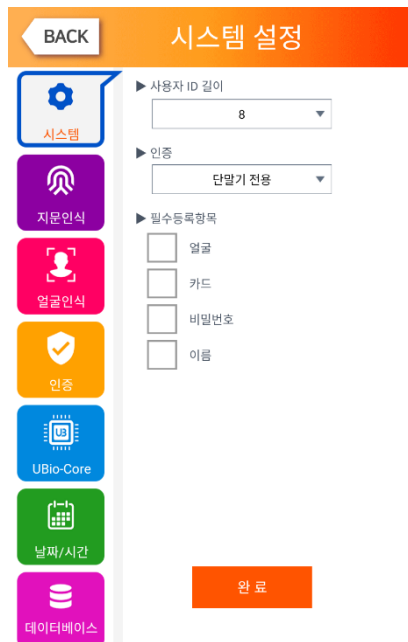
※ If you do not use the entire function key, the access pop-up window will not be displayed at the bottom

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

3.6. Systems

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 2~8 characters and should be the same with the length of the registered ID of the server program. If the ID registered in the server program uses '000075' as a 6 digits ID, set 6.

▶ Authentication

It determines the priority of the authentication between the terminal and network server and there are 2 modes "Terminal/Server", and "Terminal Only".

[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.

[Terminal Only]: It only authorizes the user registered in the terminal.

► Mandatory Registration

Items checked in this menu are required fields during user registration. Only users who have entered all required items can be registered.

The number of registered fingerprints is valid only when [Fingerprint] is checked, and at least the selected number of fingerprints must be enrolled when registering a user.

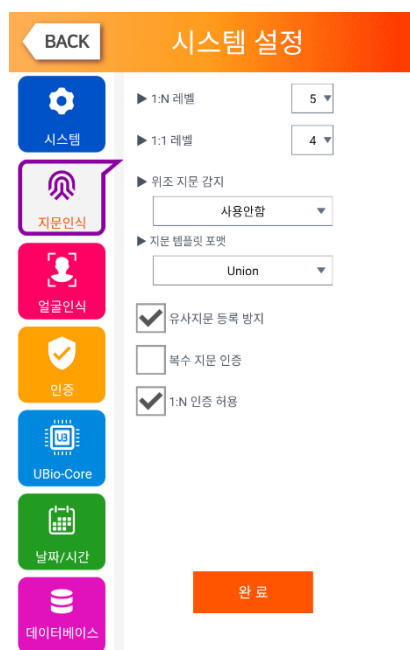
To apply the settings, click the [OK] button. To cancel and return to the previous menu, click the [BACK] button.

If you click [OK] without changing any settings, you will return to the previous menu.

To continue configuring other items, click the corresponding menu item on the left.

3.6.2. Finger

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



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

► 1: N Level (3~9)

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

► 1:1 Level (1~9)

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

► Fake Fingerprint Detection

Sets the LFD level to prevent false fingerprint input. The higher the LFD level, the stronger the input prevention function of fake fingerprints made of rubber, paper, film, silicone, etc., but even when entering actual fingerprints, too dry fingerprints may not be input well.

► Fingerprint template format

(Changing the fingerprint template format information will delete the entire existing user.)

Sets the format of the fingerprint template that you want to use. If some applications using SDK require a different format of fingerprint template, you can change the format of the fingerprint template on your terminal. However, if you use a server, you must **set it the same as the template format set on the server**

- Union: is currently the default setting and has a size of 400 bytes per template. All features using fingerprints (1:1 level, 1:N level, authentication speed, fake fingerprint

detection, etc.) can be authenticated more accurately and quickly in the most optimized format.

- ISO Standard: Fingerprint data is stored as an ISO template with a size of 500 bytes per template.

► Check similar FP registration

It is a function that checks whether a fingerprint is already registered when registering a fingerprint to prevent re-registration with a different user ID by duplicating the same fingerprint. ☒ Pseudo-fingerprints are checked up to 100,000 fingerprint limits for users whose fingerprint 1: N option is checked

► Multiple FP authentication

It is a function that requires you to enter an ID (or card) and authenticate all registered fingerprints when ☒ checking (). If this item is set to check, [Allow 1: N Authentication] will automatically change to Uncheck () ☐ because you must enter your User ID or card.

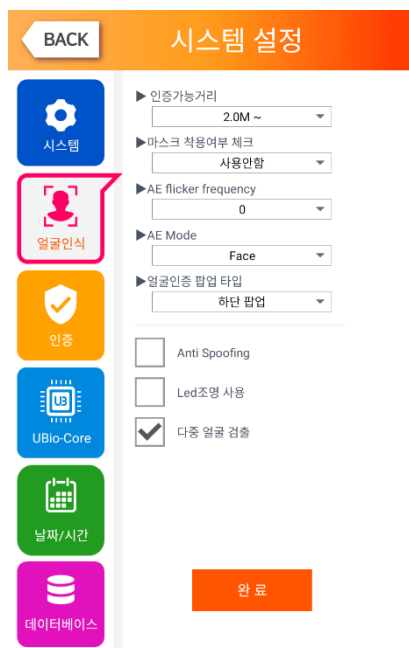
It is a function used to strictly manage access control in a special area,
For example, if a user with ID '0001' has three fingerprints registered, the user must enter the ID and authenticate all three fingerprints.
In this case, the authentication order of the three fingerprints is irrelevant, but they will continue to receive the fingerprints until all three are authenticated, and if they fail at least once, the authentication will fail.

► Enable 1: N authentication

An option that allows authentication with only a fingerprint without ☒ user ID or card input at check (), even if the user is registered with 1:N authentication permission, only 1:1 authentication is possible on terminals that are not checked.

To apply the settings, cancel the **Finish** button, and press **the Back** button to move to the parent menu. Press the Finish button without changing the settings to go directly to the upper menu.

3.6.3. Face



▶Preference: Same as the screen on the left

* However, in the case of fingerprint recognition items, they only appear when a fingerprint sensor is installed

▶ Authenticable distance (maximum distance recommended 2m)

***Depending on the user's face pixel, the verifiable distance is Difference may occur**

- AntiSpoofing enabled:
(~0.6M, ~0.9M, ~1.2M to 1.5M, ~1.7M, ~2.0M) Set the verifiable distance.

- AntiSpoofing disabled:
(~0.6M, ~0.9M, ~1.2M~1.5M, ~1.7M, 2.0M~) Set the verifiable distance.

▶Check whether a mask is worn or not

- Do not use: Do not check whether the mask is worn
- Notice: Only guidance with yellow phrases (worn/worn status/defective status) is completed and authentication is processed
- Restrictions on Access: Guide to the text (Worn-Red/Disappointed-Yellow)
Process authentication failure only when not worn
- Strong access restrictions: Red phrases (authentication failure)

* Information type

- When Not Worn: Please wear a mask
- If you are not wearing it properly (only covering your mouth): Please wear a mask properly

▶AE flicker frequency

If you install the terminal indoors

If the camera image blinks under a particular light, the option is 50 or

Setting it to 60 can improve symptoms.

▶AE Mode

Determines the (Auto **Exposure**) method.

Full: Auto exposition is operated based on the full screen.

Face: Track the face to activate auto exposition.

Center: auto exposer operates based on the center of the screen.

Auto (**recommended for use in backlit environments**):

Automatically adjust the brightness to make the subject visible in a backlight environment.

▶Face authentication pop-up type

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

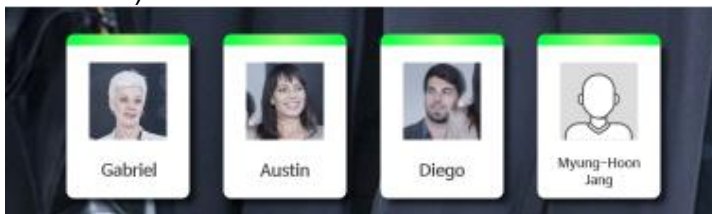
The pop-up type applies to face authentication.
(However, if you use the Anti-Spoofing option or use a thermal camera
List pop-ups and bottom pop-ups are not available.)

- List pop-up

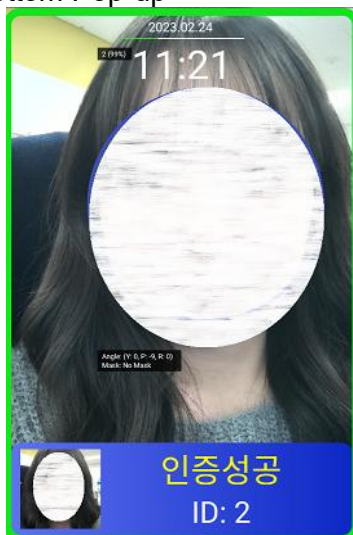
When authenticating the face, the authentication result is shown in the form of a list.

(However, when using the list pop-up type, the function key function is not available,

It is displayed as an ID regardless of the user display option [ID/Name/Employee Number] selection.)

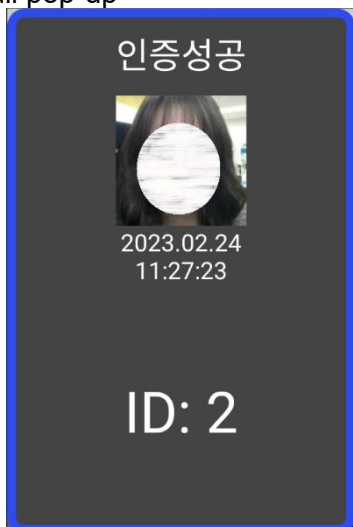


- Bottom Pop-up



When you authenticate your face,
The authentication results are displayed at the
bottom of the terminal screen.

- Full pop-up



When you authenticate your face,
The authentication results are displayed
throughout the terminal screen.

▶Anti Spoofing

Enables anti-spoofing fake face detection.

Face size 40 (0.6 m) to 15 (2 m) limit when using anti-spoofing

▶Using LED Lights

If the illuminance sensor determines that it is a low-light environment, turn on the Flash LED at the top to recognize the face and helps you obtain a log of face photographs.

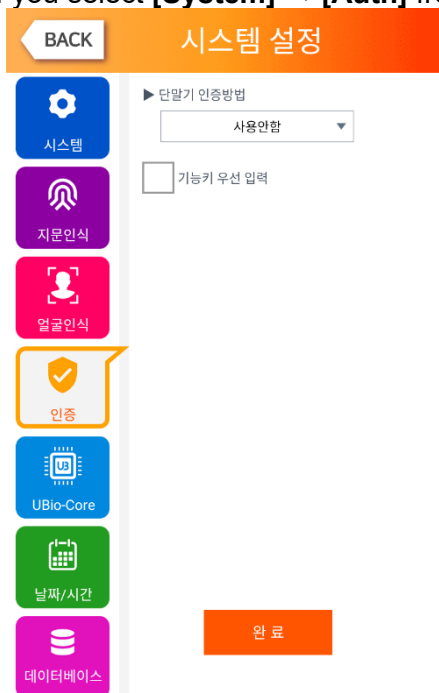
▶Multiple face detection (**can be set when not using AntiSpoofing**)

Multiple faces will be detected if the option is enabled, and if the option is disabled Only the face of the person closest to the terminal is detected.

To apply the settings, cancel the **Finish** button, and press **the Back** button to move to the parent menu. Press the Finish button without changing the settings to go directly to the upper menu.

3.6.4. Authentication

If you select **[System]** → **[Auth]** from the main menu, the screen below will appear.



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

* However, in the case of fingerprint recognition items, they only appear when a fingerprint sensor is installed

► Terminal auth Type : Select the terminal's authentication method.

- Card: Even if the user is registered as an authentication method that requires the authentication of the face, fingerprint and password together with the card, the terminal with this option can be authenticated with the card alone. In the case of fingerprint, face, and password users, they authenticate according to the user authentication method.
- Fingerprint: Even if the user is registered as an authentication method that requires the authentication of the card, face and password together with the fingerprint, the terminal with this option can be authenticated with the fingerprint alone. Card, face, and password users authenticate according to the user authentication method.
- Face: Even if the user is registered as an authentication method that requires the user to authenticate the card, fingerprint, and password with the face, the terminal with this option can authenticate with the face alone. Card, fingerprint, and password users authenticate according to the user authentication method.

► Enter function keys first

When checking, you must first select the function key [F1-F4] before authenticating. To apply the settings, cancel the **Finish** button, and press **the Back** button to move to the parent menu. Press the Finish button without changing the settings to go directly to the upper menu.

3.6.5. UBio-Core

The UBio-Core Service is supported in UBio Alpeta Standard version or later, and the UBio-Core license can be activated through UBio Alpeta.

- If you select **[System]** → **[UBio-Core]** from the main menu, the screen below will appear.

▶Preference: Same as the screen on the left

* However, in the case of fingerprint recognition items, they only appear when a fingerprint sensor is installed

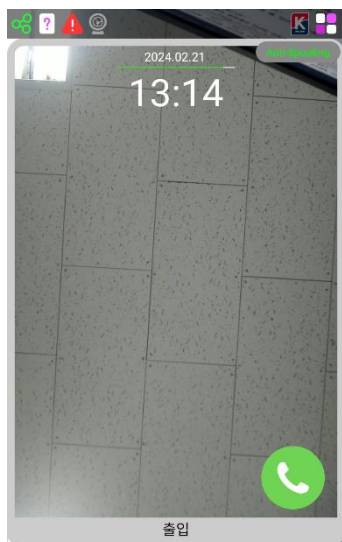
▶Use Live View

Enables the live view functionality of the terminal that is connected to the server. The VMS Server (VURIX) dashboard installed on the same network allows you to view real-time images in front of the door.

▶Using Video Intercom

Enables the intercom function of the terminal connected to the server. When you enable the intercom function, you can use the intercom function with users who have installed the video intercom program.

Every one minute, the terminal synchronizes with the intercom information (extensions) set in the video intercom program and appears in the phone number list of the terminal.



When using the intercom function, The intercom button is activated in the lower right corner of the main screen. When selecting the intercom button, the phone number input screen is displayed, or the call is connected immediately (when checking the management room only)

▶ Hang up when the door opens

When you use the door-open feature in the video intercom, the call is terminated automatically.

▶ Management Office Only

Call the video intercom program user with the administration office-only extension '0000'. If the video intercom program extension is registered as a number other than '0000', I can't get through to the call.

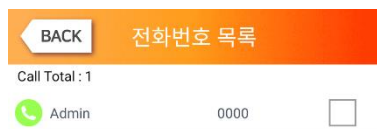
▶ Call time

You can specify the intercom call time from a minimum of 5 seconds to a maximum of 999 seconds. The default is 60 seconds. If the Hang Up Call feature is disabled when the door is opened, the call connection is maintained for the set call time after the door is opened.

▶ Edit phone number

Go to the Phone Number List screen. The call is connected to the video intercom program. You can check the status of the extension number that you can't call because it's disconnected from the available extension.

Select an extension that you are no longer using, such as deleting video intercom programs and you can delete it.



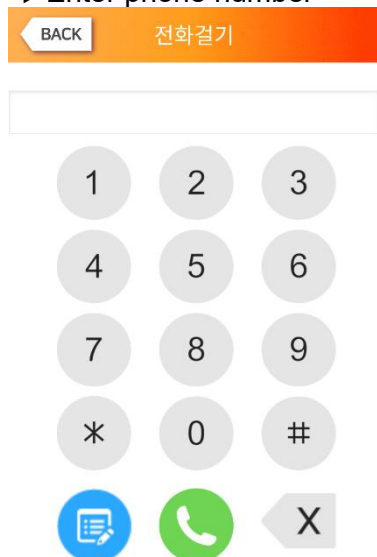
 : Phone number that is currently available to talk to the video intercom

 : Phone number that is currently unavailable to the video intercom

 Del : Use to delete a list from a phone list by selecting the list you want to delete



▶ Enter phone number



When the intercom button is touched on the main screen, it is moved to the phone number input screen. If Administration Room Only is selected in Settings, try to connect to the video intercom as soon as possible



Go to the Phone List screen

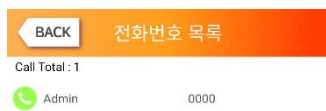


Make an intercom request to the number you entered

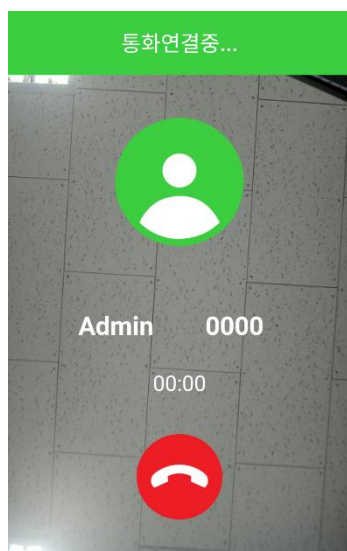


Delete the entered number one digit at a time

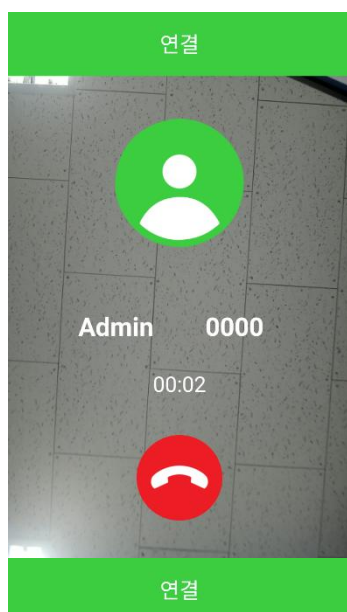
▶ Phone number list



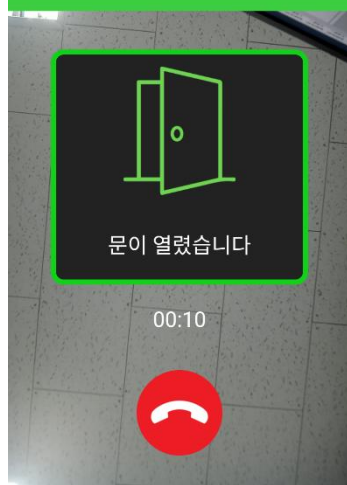
You can check the extension that is automatically synchronized. If you select an extension, you will automatically enter the number, and if you press the call button, you will try to connect to the call.



Video intercom connection attempt screen



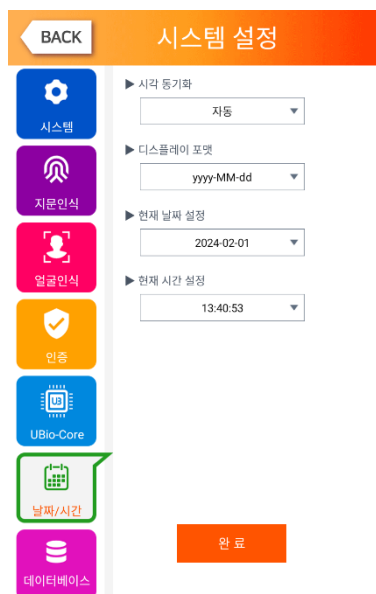
Video Intercom Connection Success Screen



Video intercom door opening screen

3.6.6. Setting the Current Time

If you select **[System]** → **[Date/Time]** from the main menu, the screen below will appear.



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

* However, in the case of fingerprint recognition items, they only appear when a fingerprint sensor is installed

▶ Time synchronization

Set how to synchronize the current time of the terminal with the server. Set **it to Auto** to synchronize with the server time automatically or **Manual** to Manual.

▶ Display Format

In a way to display the current time of the terminal

- yyyy-mm-dd : Display in the order of year, month, and day
- dd-mm-yyyy : Display in order of day, month, and year

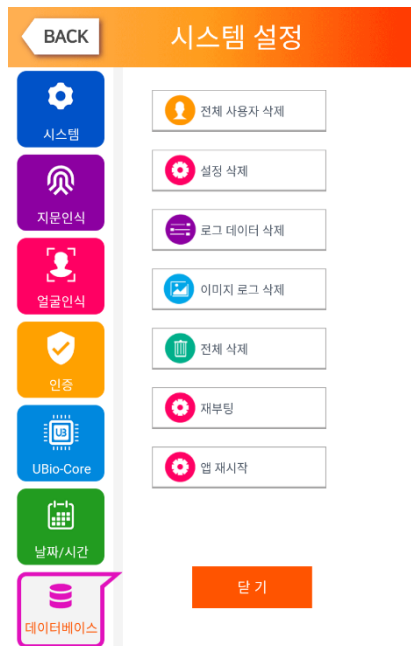
▶ Set date/Set time

Change the current time of the terminal. If the server is connected and **the above Visual Synchronization is set to Auto**, it will synchronize with the server time and you do not need to change it.

To apply the settings, cancel the **[Finish]** button, and press **the [Back]** button to move to the parent menu.

3.6.7. Database

If you select [System] → [Database] from the main menu, the screen below will appear.



* However, in the case of fingerprint recognition items, they only appear when a fingerprint sensor is installed

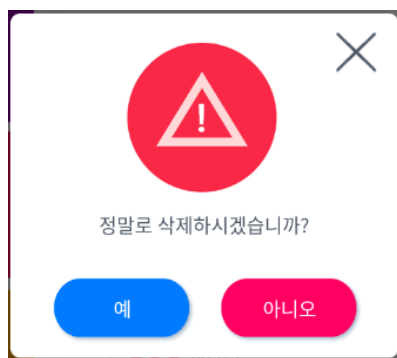
To delete all users, click **the Delete All Users** button,
If you want to initialize the settings, click **the Delete Settings** button,
If you want to initialize your authentication history, click **the Delete Log Data** button,
To delete the image log only, click **the Delete Image Log** button,
Click **the Delete Full** button to delete the entire data and bring it to factory initialization state.

Press **the Close or Back** button to move to the parent menu.

Reboot: Reboot the system.
[App Restart] : Restart the app.

3.6.7.1. Delete All Users

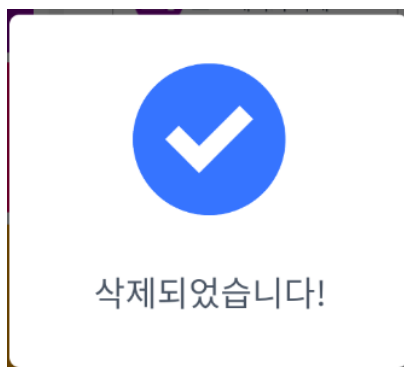
If you select **[System] → [Database] → [Delete All Users]** from the main menu, the screen below will appear.



To delete all users, click **the [Yes]** button,
Press **the [No] or [X]** button to cancel.

If there is no input for five seconds in this state, the message box disappears without deleting it.

If you click **[Yes]** and delete it successfully, a success message box appears as below

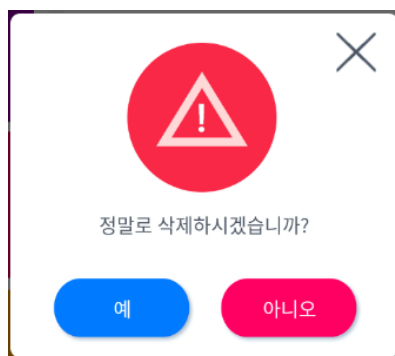


<Figure 3-5>

In this case, both users and administrators are deleted, **and recovery is not possible after deletion.**

3.6.7.2. Delete Settings

If you select **[System] → [Database] → [Delete Settings]** from the main menu, the screen below will appear.



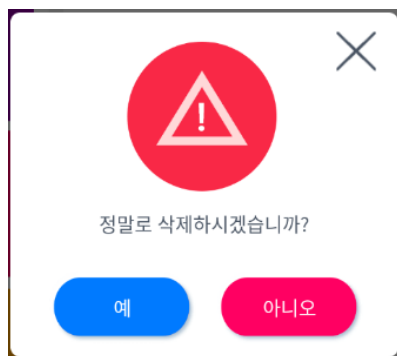
To reset all settings, click the **[Yes]** button, Press the **[No]** or **[X]** button to cancel.

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

If it is successfully deleted by pressing **[Yes]**, the success message in Figure 3-5 will be displayed and the display language and voice will be changed to the initial English value. Initializes all settings on the terminal except for the MAC (physical) address and the [fingerprint template format], but does not delete the user and authentication history.

3.6.7.3. Delete log data

If you select **[System] → [Database] → [Delete Log Data]** from the main menu, the screen below will appear.



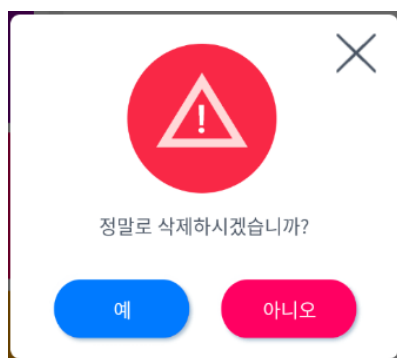
Click the **[Yes]** button to delete all authentication records stored on the terminal, **or the No** or **[X]** button to cancel.

If there is no input for five seconds in this state, the message box disappears without deleting it.

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

3.6.7.4. Delete Image Logs

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



Click the **[Yes]** button to delete all image logs stored on the terminal, **or the No** or **[X]** button to cancel.

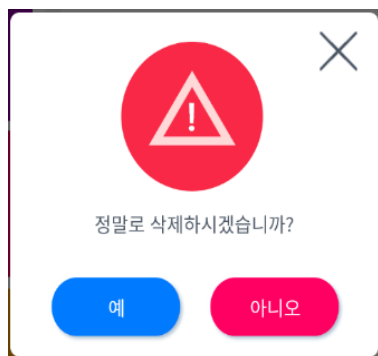
If there is no input for five seconds in this state, the message box disappears without deleting it.

If you click **[Yes]** and delete it successfully, the success message in Figure 3-5 will be displayed.

Only images saved as logs are deleted, not the authentication log itself.

3.6.6.5. Delete All

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



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

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

If it is deleted successfully by clicking **[YES]**, the success message in <Fig. 3-5> appears, and the display language and voice is changed to the default value English.

All the set value, users and log information besides the MAC address in the terminal to make the terminal in the factory setting. **The restoration after the deletion is impossible, so be careful.**

3.6.7.6. Reboot

"Reboot the system. Please wait a moment..." After the message comes out, the terminal measures It will be booted.

3.6.7.7. Restarting the App

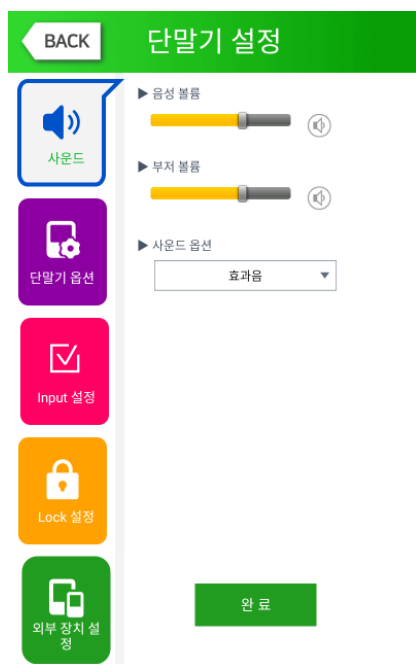
"Reboot the app. Please wait a moment..." After the message comes out, only the terminal app will be restarted.

※ If you are heading to Europe, you will be forced to re-register the manager because the factory initialization and deletion of the entire user will also delete the manager.

3.7. Terminal Settings

3.7.1. Sound

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



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

▶ Voice volume

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

▶ Beep volume

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

▶ Sound Option

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

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

3.7.2. Terminal Options

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

Set the display method of the card number. The card number varies depending on the setting value as follows, so set it up at the time of initial installation, and if it is unavoidable to change during operation, you must re-register the card

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

card format	Card number	How to display
Standard	02207638	(3+5) Indicate in decimal place [022(16h)+07638(1DD6h)]
Hexadecimal	0801161DD6	Display in 10-digit hexadecimal
10 Digit Decimal	0018226646	Display the last 4 bytes in 10-digit decimal numbers (01161DD6h)
3,5 Digit Decimal	02207638	Same as [Standard]
6 Digit Hexadecimal	161DD6	Display the last 3 bytes in 6-digit hexadecimal

SC card example) Card number (4 bytes): 52h 9Dh 06h E3h

card format	Card number	How to display
Standard	529D06E3	Displayed in 8-digit hexadecimal
Hexadecimal	E3069D52	Replace the Byte order to display in 8-digit hexadecimal
10 Digit Decimal	1386022627	Display hexadecimal 529D06E3 in decimal
3,5 Digit Decimal	3808861522	hexadecimal E3069D52 in decimal
6 Digit Hexadecimal	069D52	Place the first 3 bytes upside down

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

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

►Ble Rssi

Sets the reception sensitivity of the Ble module.

The larger the value, the greater the recognition distance.

►Ble TxPower

Sets the RF output strength of the Ble module.

The larger the value, the greater the recognition distance.

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

3.7.3. Input Settings

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

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

- 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 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 open 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 on the left side.

►Lock1 Option

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

►Lock2 Option

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

►Lock 1 duration (ms)

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

►Lock 2 duration (ms)

It sets the signaling time when Lock 2 is set 'Authentication failure notification'. Because it is set in ms unit, if you want to set 3 seconds, you should set 3000. Click **[OK]** button to apply the set value, and click **[BACK]** button to cancel and return.

3.7.5. External Device

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

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

► **RS232 Option:** Set up the terminal that connects to the RS232 port

- Disabled: If no terminal is connected to the RS232 port
- TicketFormat 1/ TicketFormat 2: Prints the authentication result to the printer upon successful authentication. The printer connected to the RS232 port prints the terminal ID, user ID, authentication time, and authentication mode.

TicketFormat 1 :

Terminal mode, equipment number, employee number, employee name, authentication date, serial number, meal classification

TicketFormat 2 :

Equipment number, employee number, employee name, authentication date

The print format varies depending on the settings, and when set to [Ticket Output 2], the "text for meal printer" set through the server's terminal option is output as the top title. The printer used to print tickets is a model of the "SRP-350" Serial type.

- QR card: QR code can be used in the same way as authentication card
It can be used up to 24 digits. (Please note that reading QR codes of 24 digits or more may lead to errors if 24 digits are the same.)
- Breathalyzer: If the authentication is successful, the breathalyzer connected to the RS232 port will be used to measure the breathalyzer, and the result of the measurement will determine the accessibility.

► **RS232:** It sets the device connected to RS232 port

- None: When there is no device connected to the RS232 port
- Ticket Format1/ Ticket Format2: The authentication result is printed when the authentication

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

is successful.

The terminal ID, user ID, authentication time, and authentication mode are printed by the printer connected to the RS232 port.

Ticket Format 1 :

Terminal mode, equipment number, employee number, employee name, authentication date, serial number, meal classification

Ticket Format 2 :

Equipment number, employee number, employee name, authentication date

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.

- QR Card: QR Code can be used in the same way as the authentication method card and can be used up to 24 digits.

- Breathalyzer: If authentication is successful, a breathalyzer test is performed using a breathalyzer connected to the RS232 port, and entry is determined based on the test results.

►RS485 Option: Set up the terminal that connects to the RS485 port

- None: When there is no device connected to RS485
- LC010: When LC010 is connected.
- LC015: When LC015 is connected
- Replay I/O: When the elevator controller is connected
- MCP040: When MCP040 product is connected
- OSDP: When an OSDP-enabled controller is connected.
- Reference: If you set DM0: [Door Open NO] or [Door Open NC], when using LC010, LC015, it gets the status of door open via DM0. If you want to get the status of door open from the controller, you shouldn't set DM0

►Site Code

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

►Wiegand Output

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

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

► External Reader

A function that allows the Wiegand reader to operate differently on the main terminal inside the door to which the terminal is connected

- None: Set to use the main terminal registered user authentication method as it is
 - Wiegand card
 - : Features that can be used differently from the registered user authentication method of the main terminal
- The card entered through Wiegand is considered a separate reader connected to the inside of the door, and users who use the card with other authentication methods such as face/fingerprint/password and combination authentication will be authenticated only with the card, without mask check, thermal check, or photo log.

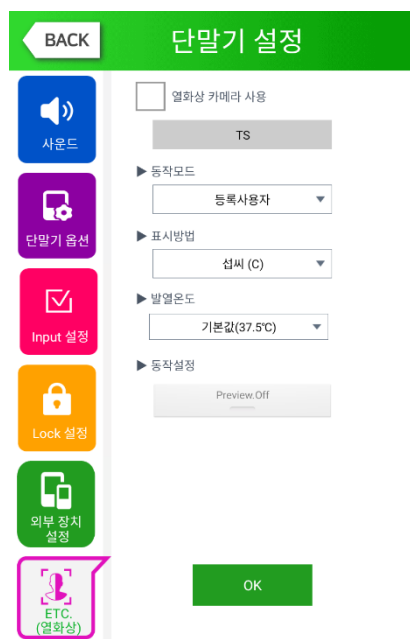
To apply the settings, cancel the **[Finish]** button, and press **[Back]** button to move to the upper menu.

3.7.6. ETC. (Thermal)

This product is an additional device to primarily screen whether the skin temperature rises for an unspecified number of people. It can be quickly checked whether the skin surface temperature of the test target is higher than the normal skin surface temperature reference value, so that many people can be quickly tested. However, since the disease or virus cannot be confirmed, the primary screening test subject must perform a secondary test through a medical device to take follow up measures.

- (1) It is recommended that the sensor and the face of the product be installed and operated in parallel.
(If the face position is not parallel, an error of 1 degree may occur.)
- (2) Errors may occur depending on the type of lighting.
(Errors may occur where incandescent lamps / halogens / quartz tungsten halogens are installed)
- (3) An error may occur if there are accessories or obstacles that cover the face.
(Glasses / hat / bangs covering the forehead / headband, etc.)
- (4) Move an object that can reflect infrared rays in the background that the sensor of the product sees.
(Glass/Mirror/Metal surface, etc.)
- (5) If there is an air conditioner or cooling device in the installation location, an error may occur.
(An error occurs when near a blower for air conditioning or air conditioning in a building.)
- (6) It is recommended to install and operate within the temperature range of 20°C to 24°C / 10% to 50% humidity.
- (7) It is recommended that only one person detects heat at a time.
- (8) For accurate temperature measurement, it is recommended to use a black body together.

If you select **[Terminal]** -> **[ETC(Thermal)]** in the main menu, the following window appears.



- ▶ Basic setting: Same with the window at the left.
- ▶ Thermal Camera Use
Thermal cameras are available when checking (☑)[TS(Thermal-i2)].

▶ Operation Mode

Operation Mode	Description
Registered User	Authentication and temperature measurement for registered users only
Unregistered Users	Measurement of body temperature for registered and unregistered users

▶ Display

- You can choose between Celsius, Fahrenheit, or None.
- * If you select None, the authentication results pane displays four.

Authentication Results	Description
LOW	Temperatures below 30°C
HIGH	Temperature exceeding 42°C
Success	30°C or higher and below the set heating temperature
Failed	Temperature exceeding the set heating temperature

▶ Heating temperature

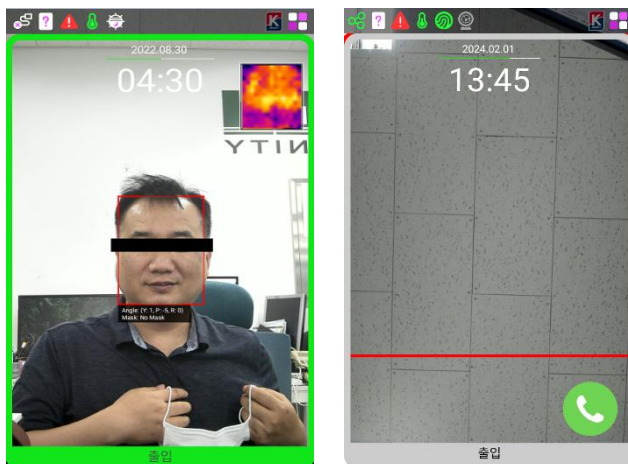
- The heating temperature standard can be selected from 37.0°C to 38.5°C.
If the measured temperature is higher than the heating temperature reference, it is measured with the message 'Authentication Failure'
The temperature is displayed in the Authentication Results window.

▶ Thermal Settings

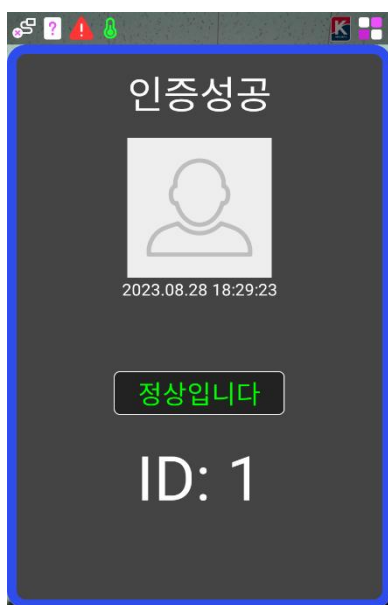
Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)
Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com
<http://www.unionbiometrics.com>

- When the Preview button () is turned on, the Preview image of the thermal imaging camera is displayed in the upper right corner of the main screen.
- When the guide button is turned on, a red guideline appears on the main screen

To apply the settings, cancel the **[Finish]** button, and press **[Back]** button to move to the parent menu.



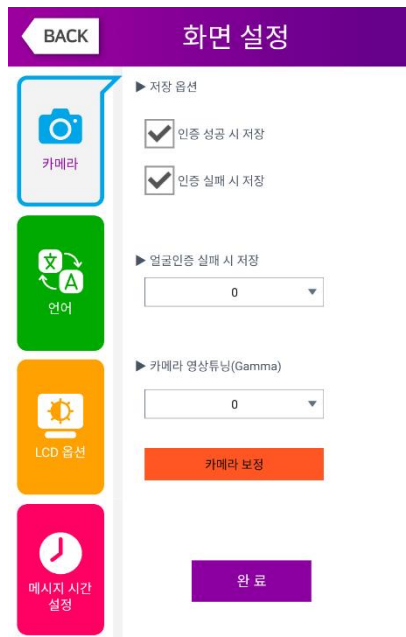
During the heat check, you can also watch the thermal imaging camera preview video at the bottom right.



3.8. Display

3.8.1. Camera

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



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

▶ Display Option

Select the image displayed in the message window of authentication success

- None

- Registered photo

- Authentication method: Image stands for each authentication method

▶ Save success log

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

▶ Save failed log

If it is checked (☒) the camera image is captured as image log when the authentication was failed.

▶ Save failed face

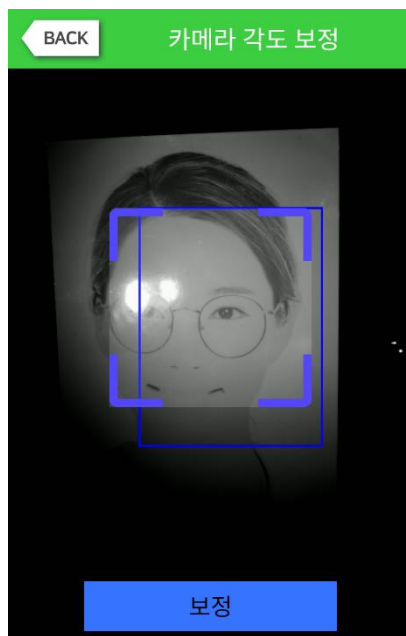
0: The failed log is not saved.

1~5: An unregistered user stares at the screen of terminal for more than the set time (1~5), the failed log is saved.

▶ Camera ISP (Gamma)

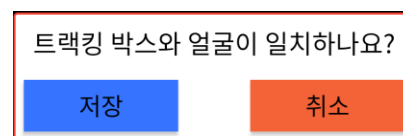
0~4: Sets the value of the camera Gamma, and the larger the value, the brighter the image.

◆ CAUTION: If the image is too bright, it may affect authentication, so be careful when using it.



▶ Camera calibration

When you look straight ahead and press the correction button, the "Save, Cancel" screen appears as shown below.



The face and tracking box (blue solid box)

Check if it matches your face and click Save

The corrected values are stored and corrected from the next authentication

The coordinates are applied.

● Caution: When there is more than one person or no person on the screen, the following warning message is displayed and only one person must be on the screen.



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

3.8.2. 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.

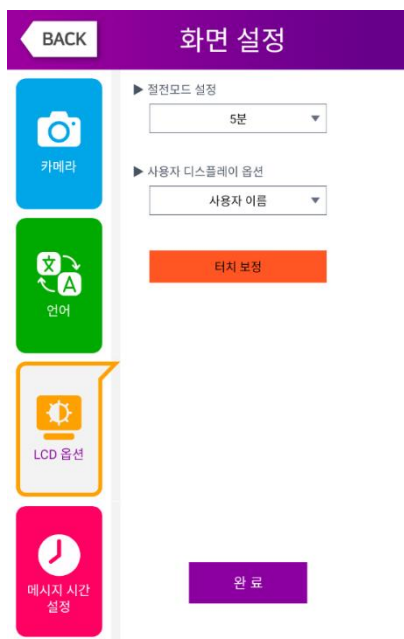
※ Supporting languages

English, Korean, Japanese, Portuguese, French, Spanish, Polish, Persian, German, Turkish, Vietnamese, Thai, Arabic

※ In the case of a common language, there is a part that is expressed in English rather than a set language.

3.8.3. LCD Options

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



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

▶ Power saving mode (5sec ~ 10min)

If there is no input for set duration, the LCD screen is turned off automatically. But, if you set 'None' the LCD is always turned on.

▶ Display Option

It sets what will be shown at the LCD screen when the authentication is successful.

-None: The authentication result [Success/Failure] is only represented.

- User ID

- User Name: Representing user ID if it is not registered. (In this case, added "ID" to differentiate with name)

- Social No: Representing user ID if it is not registered. (In this case, added "ID" to differentiate with employee's number)

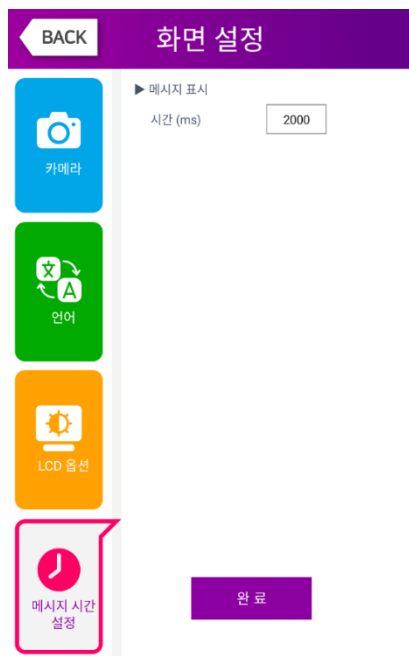
▶ Touch Calibration

This feature is to calibrate the coordinates of the touch screen.

To apply the settings, cancel the **[Finish]** button, and press **[Back]** button to move to the upper menu.

3.8.4. Message display time

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



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

► Message Display (ms)

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

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

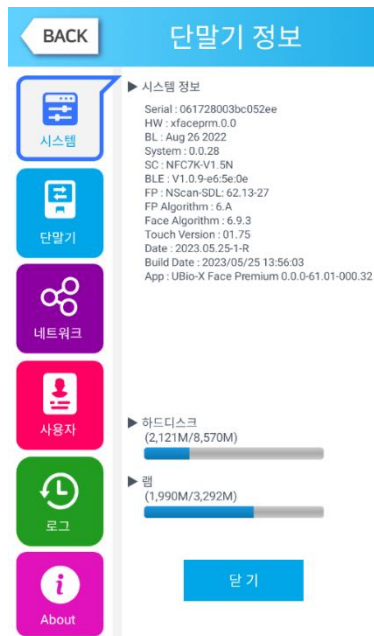
Because it is set in millisecond, if you want to set 2 seconds, you should set 2000.

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

3.9. System

3.9.1. System

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



▶ System info

The hardware and firmware version of terminal is shown

▶ 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.

▶ 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 Information

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



▶ Terminal info

It represents the option setting value of the terminal.

▪ Access Control Info View

Displays access group information set on your device.

▪ Schedule Info View

Displays schedule information set on your device.

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

3.9.3. Network

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



▶ Network info

It shows the setting value of the terminal.

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

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

3.9.4. User

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



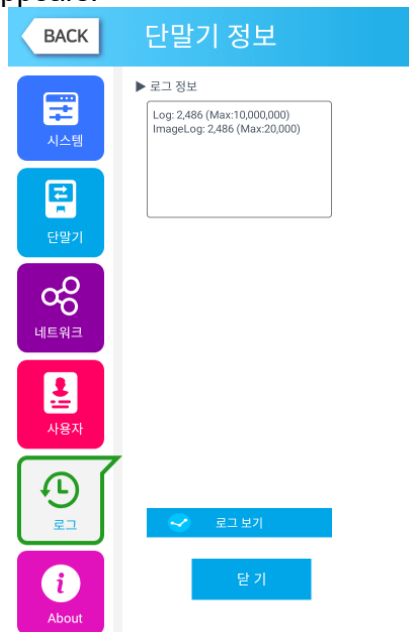
▶ User

- 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

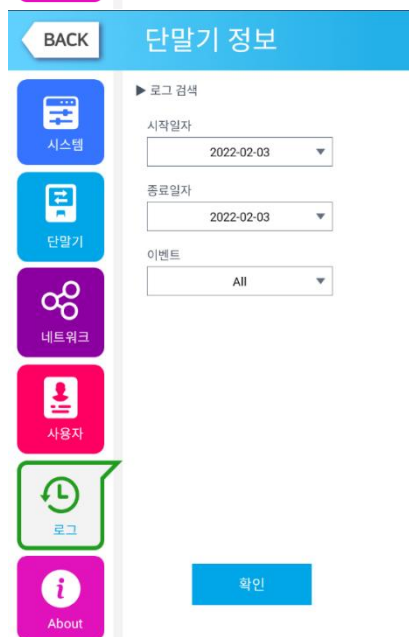
Log: The number of logs saved in the terminal

Image Log: The number of logs saved in the terminal

The number of logs saved in the terminal

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

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

3.9.6. About

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



► About

It shows the license information applied in the terminal.

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

3.10. USB

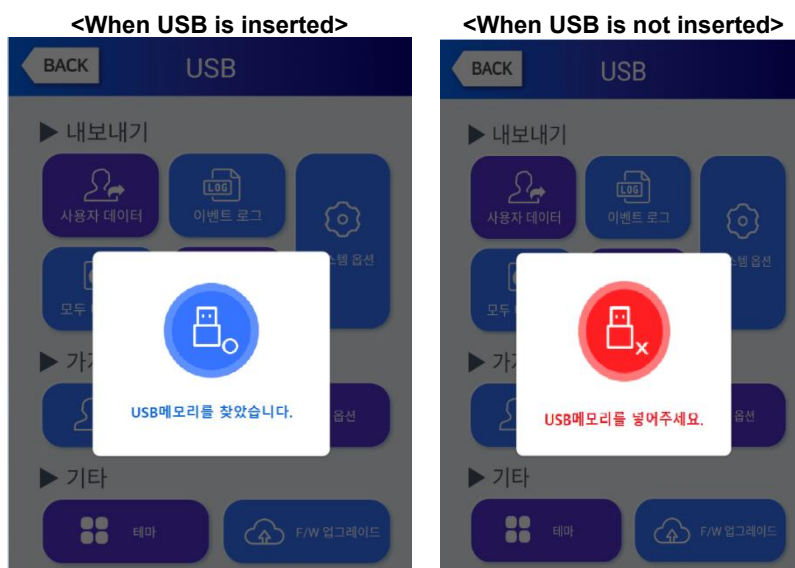
Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

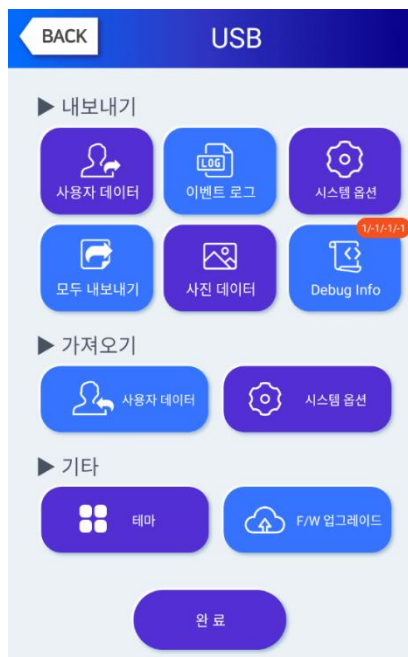


If you select **[USB]** from the main menu, the following screen appears.



※ Work can only be done when USB is inserted, and the back side must be inserted forward as shown in the picture below. (The size of the USB should not exceed 32G.)





It is the feature to back up the data of the terminal via [Export]. You can copy the back-up data to the terminal via [Import].

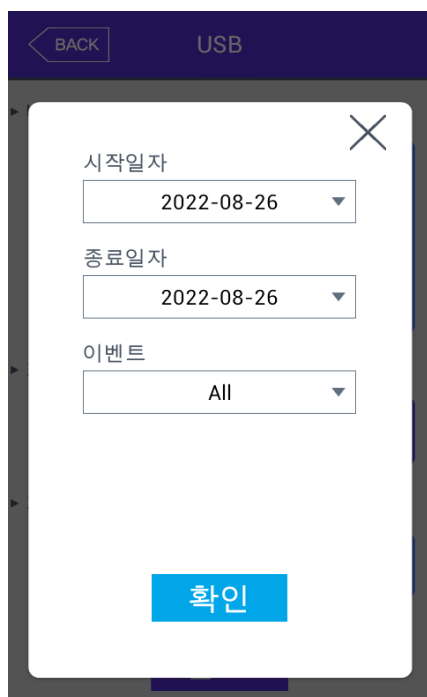
▶ Export

It copies the data from the terminal to the external USB. - User data: It copies the user DB to the folder 'unisuser' in USB.

- System option: The option setting value of the terminal is copied to the folder 'UbioXfacePremium/config'.

- Event Log: Copy the authentication log to the 'UbioXfacePremium/Terminal ID (8 digits)/log' folder on the USB. (Images (face photos) taken during authentication are not included in the event log.) You can copy the event log by specifying a period.

- Debug Info: Exports terminal debugging information to the "Debug Info" folder.



- Picture: The image log data is saved in the folder 'UbioXfacePremium / Terminal ID (8 digits) / log / pictures' in USB as jpg file.
- Export all: It can export all things User Data, Event Log, and image log to USB.

▶ Import

It copies the data from the USB to the terminal.

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

After importing the data, you should reboot the terminal to apply the new DB or setting value.

▶ Others

- Theme: The voice file in the 'UbioXfacePremium/audio' folder in the USB is copied to the terminal.

If you want to replace the authentication success (user_ok.mp3) and the authentication 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.

*How to upgrade

: You can proceed by selecting the upgrade through the FW upgrade item at the bottom of the USB menu.

※ Caution: Upgrade FW (app, system) and card and fingerprint firmware together

- F/W Upgrade:

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

Upgrade firmware from Type C USB (App, System)

(Firmware must be in the Type C USB 'UbioXfacePro folder)

- Card Upgrade:

The card firmware must be in the Type C USB ('UbioXfacePro/Card') folder.

- Fingerprint upgrade method (**Xcan option**):

The fingerprint firmware must be in the Type C **USB** ('UbioXfacePro/Card') folder.

To finish the task and go to the upper menu, press **[Finish]** or **[BACK]** button.

3.11. Download User Files

It is a function that allows the user to change the voice message if necessary. You can copy using USB or download and change user files from the server program.

3.11.1. Change Voice Messages

If you select the 'File Transfer' in our server program, the following window appears.

	ID	Name
☐	1	UBio-X Pro Lite
☐	2	UBio-X Pro
☐	3	UBio-X Face
☐	4	UBio-X Face Premium

If you select 'Sound Voice File (.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 'Fail Voice File (.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 the terminal

Union Biometric Co., Ltd. / 641-4 Daemyung Bellion 12th floor, Munjeong-dong, Songpa-gu, Seoul (058-036)

Tel : 02-6488-3000 , Fax : 02-6488-3099, E-Mail : sales@unionbiometrics.com

<http://www.unionbiometrics.com>

Union
biometrics

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

4.1. How to change Auth mode



<Fig 4-1>

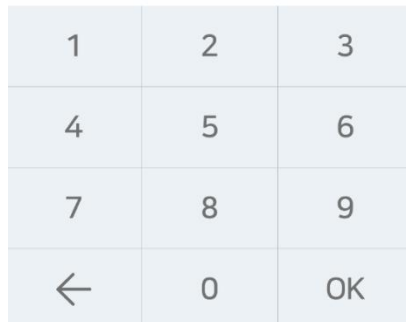
Select the function key button among Attend [F1], Leave [F2], Out [F3], In [F4] on the screen for choosing the function mode before authentication.

4.2. How to input user ID

If you click the button [ID] on the basic window, following the window "Input User ID" as below



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



4.3. Authentication

- For European products, the administrator account cannot be authenticated using a single authentication method according to the security policy.
- Two or more authentication methods must be authenticated by combining them with AND conditions.
- The policy is enforced by the system and is enforced when changing administrator settings or accessing assets.
- Commonly applied.

4.3.1. Face Authentication

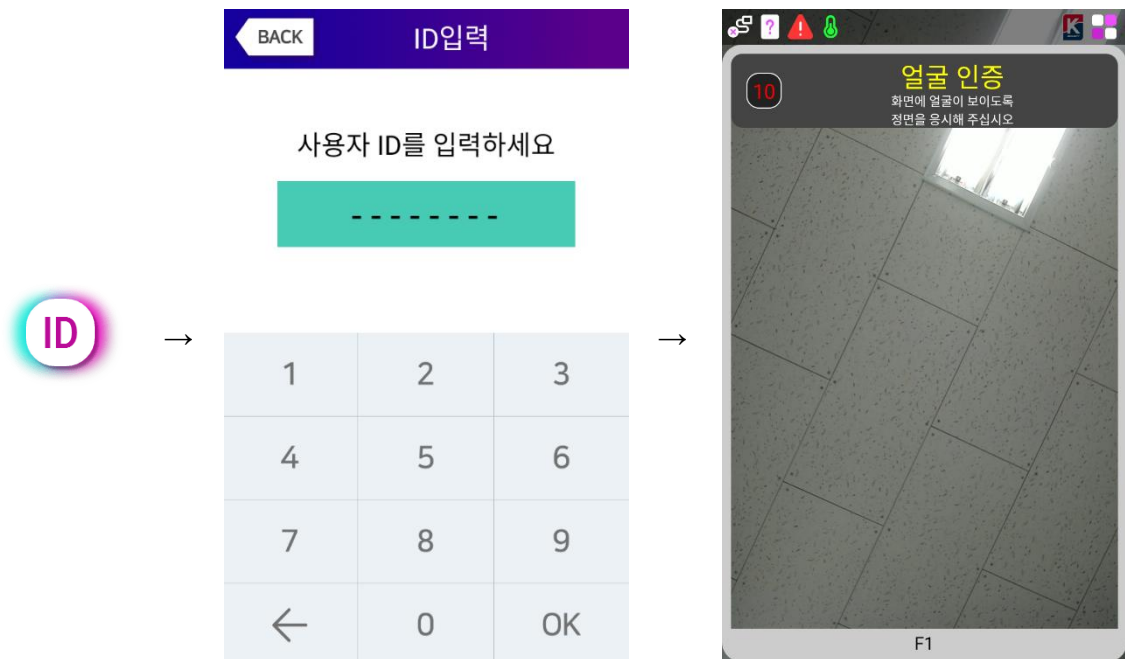
▶ 1:N Authentication

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

▶ 1:1 Authentication

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

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



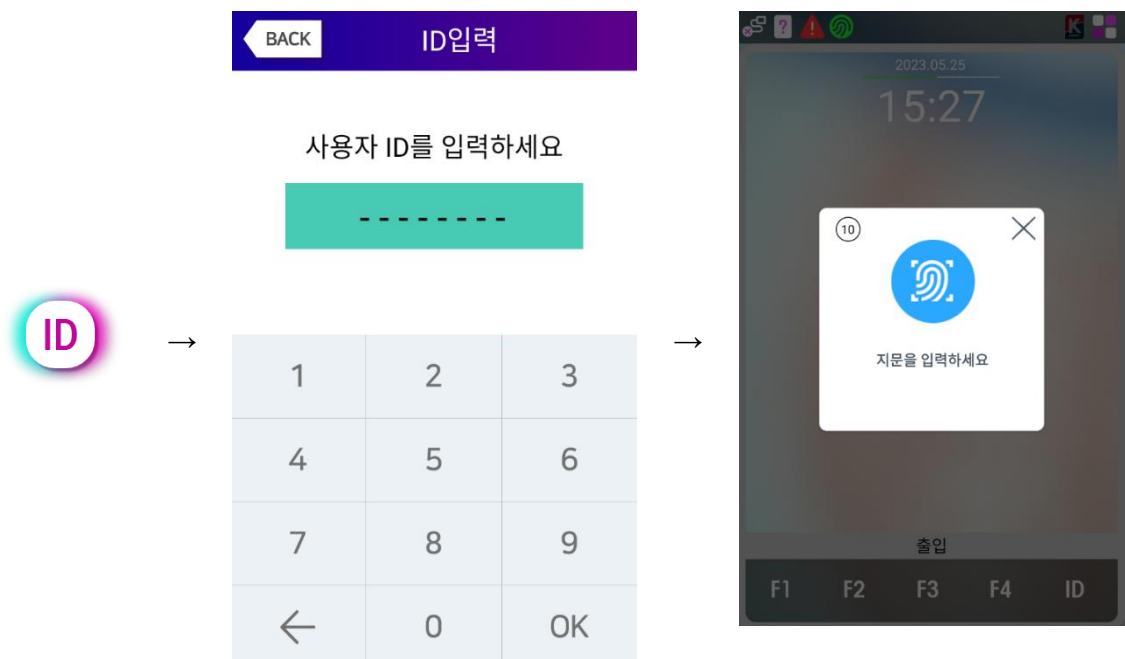
4.3.2. Fingerprint authentication

▶ 1:N Authentication

When you touch a fingerprint to the fingerprint sensor on the main screen, a buzzer sounds and the sensor lights up and receives the fingerprint. Do not release your fingers until the light on the fingerprint sensor is completely off.

▶ 1:1 Authentication

Press the [Input ID] button to enter the ID first, as shown in the figure below, and then enter the fingerprint when the fingerprint sensor lights up. Do not take off your finger until the light of the sensor turns off completely.

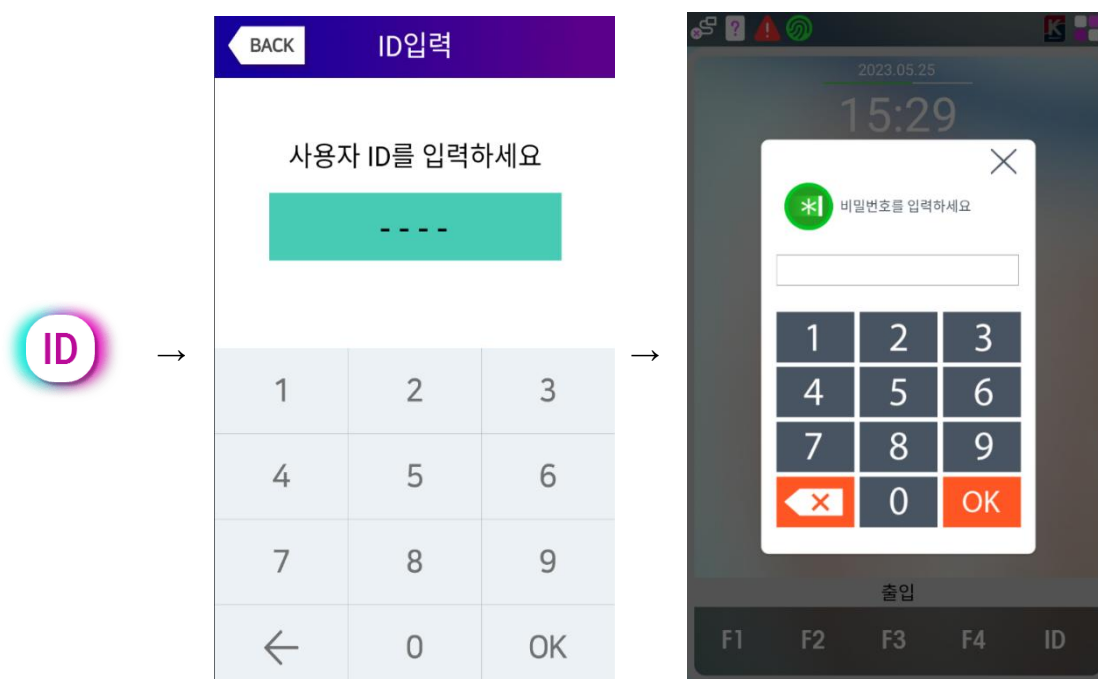


4.3.3. Card Authentication

Attach the card to the terminal's card authentication location (see terminal name picture)

4.3.4. Password Authentication

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



► Duress password authentication.

When entering a password, entering the registered password in reverse order will inform the administrator that the authentication is successful, but it is an attempt to authenticate the duress in the same way as the duress fingerprint.

Example 1) If the password is 1234, if you authenticate it with 4321, you can authenticate the duress password.

Example 2) It doesn't apply if the password is a continuous number like 1111.

Example 3) It doesn't apply even if the password is a symmetric number like 1221.

Example 4) If the password is a single digit number like 1, it doesn't apply.

4.3.5. Multi-authentication

For user who needs to authenticate via more than 2 methods such as –card & fingerprint OR card & fingerprint & face, the preferential priority of the authentication after the ID is typed is as follows: (card-> fingerprint -> face -> password) in order.

This type is activated even if face or fingerprint authenticates firstly.

- If the authentication combination is or

In the case of only card and only mobile card, it operates by card method at 1:1 authentication.

Card and mobile card cannot be used as a means of authentication when attempting 1:1 authentication under or conditions that include card and mobile card.

※Only OR combination is possible when using a mobile card.

FCC Compliance Information

Virdi / UBio-X Face Premium

This device complies with Part 15 of the FCC regulations.

Operation is subject to the following two conditions:

- (1) This terminal does not cause harmful interference.
- (2) This terminal accepts any interference, including interference that may cause undesired operation.