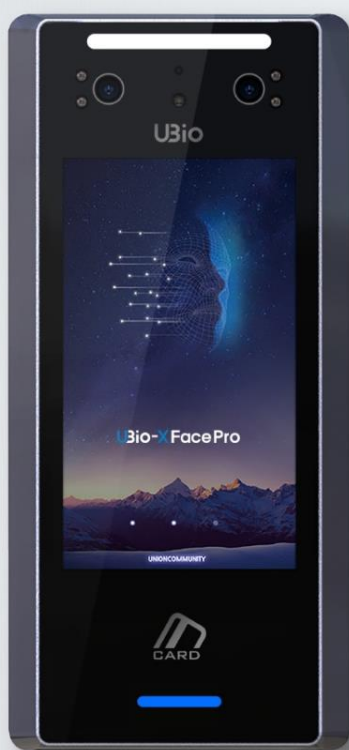




Revision History

Version	Date	Description	Firmware Version
1.0	2023-08-23	Initial Release	
1.1	2024-03-12	5.3.4. Addition of UBio-Core	0.0.0-61.01-000.42
1.2	2025-02-14	5.2.3. Addition of extended key to function key 5.5.2. Addition of Chinese(Traditional) language	0.0.0-61.01-000.51

Explanation of Term

Admin, Administrator

- The term refers to users who have the authority to enter the terminal's menu mode, register/modify/delete terminal users, and change operational settings.
 - Administrators have the authority to change crucial environmental settings of the fingerprint recognition device, so extra caution is required for registration and operation.
- * If there is no registered administrator on the terminal, anyone can enter the terminal menu and change settings. Therefore, it is strongly recommended to **register at least one administrator**.

1 to 1, Verification

- The system authenticates the user's fingerprint only by comparing it after entering the user ID or card and fingerprint.

1 to N, Identification

- This is an authentication method that identifies the matching fingerprint from the registered fingerprints without requiring user ID or card input.

Authentication Levels

- The level used in fingerprint authentication, displayed in steps from 1 to 9 based on the degree of matching fingerprints. During authentication, the match level between the two fingerprints must be higher than the set authentication level for successful authentication.
- Higher authentication levels can provide increased security but may require a relatively high match rate, increasing the likelihood of authentication failure during self-verification.

* 1:1 Authentication Level: The authentication level used in 1:1 authentication.

* 1:N Authentication Level: The authentication level used in 1:N authentication.

Authentication Method

- This refers to various forms of authentication methods created by combining Face authentication, FP (Fingerprint) authentication, and RF (Radio Frequency) authentication.

* Example: Face or FP - Authentication using either Face or Fingerprint.

LFD (Live Finger Detection)

- It allows only actual fingerprints to be input and prevents the input of dummy fingerprints made from materials such as rubber, paper, film, silicone, etc.

Table of Contents

Revision History		1
Explanation of Term		2
Table of Contents		3
Chapter 1	Pre-use Verification	4
01	Cautions	5
	Cautions in Installation	6
02	Terminal Specific Names	7
03	Sound/Screen Guidance	8
	Sound	8
	Buzzer Sound	8
	Screen	8
	Icon	9
	Message	10
04	Correct Registration and Authentication Methods	16
	Face	16
	Finger	17
	QR	18
05	Pre-checks Before Environmental Configuration	19
	Administrator Authentication	19
	Menu Structure and Navigation	19
	Entering the Menu Without Administrator Authentication	25
	Saving Configuration Settings	25
Chapter 2	Product Description	26
01	Product Composition	27
	Components	27
	Cables	28
02	System Configuration Diagram	29
	Standalone Usage	29
	Connection to PC Server	29
03	Specifications	30
Chapter 3	Administor	31
01	User Management	32
02	Enrollment	32
	Face	34
	Password	35
	Card	35
	Finger	36
	QR Code	37
	Save	38
03	Modify	39
04	Delete	39
05	View	40

Chapter 4		Authentication	41
01	Authentication Options		42
02	Authentication Methods		42
	Providing Various Registration and Authentication Methods		43
Chapter 5		Settings	44
01	Network		45
02	Application		46
	Access / TnA		46
	Meal		47
	Function Key		47
03	System		48
	System		48
	Face		48
	Auth		50
	UBio-Core		50
	Date / Time		53
	Database		53
	Finger		55
04	Terminal		57
	Sound		57
	Option		58
	Input		59
	Lock		60
	External Device		61
	ETC. (Thermal)		62
05	Display		63
	Camera		63
	Language		64
	LCD Option		64
	Message display time		65
06	Info		65
07	USB		68
Chapter 6		Terminal Usage Instructions	69
01	Change Authentication Mode		70
02	ID Input		70
03	Authentication		71
	Face		71
	Finger		71
	Card		72
	QR Code		72
	Password		72
	Multi		72

Chapter 1

Pre-use Verification

01	Cautions	5
	Cautions in Installation	6
02	Terminal Specific Names	7
03	Sound/Screen Guidance	8
	Sound	8
	Buzzer Sound	8
	Screen	8
	Icon	9
	Message	10
04	Correct Registration and Authentication Methods	16
	Face	16
	Finger	17
	QR	18
05	Pre-checks Before Environmental Configuration	19
	Administrator Authentication	19
	Menu Structure and Navigation	19
	Entering the Menu Without Administrator Authentication	25
	Saving Configuration Settings	25

Warning



Do not operate the device with wet hands or allow liquids to enter the device.

-> There is a risk of malfunction and electric shock.



Do not disassemble, repair, or modify the device arbitrarily.

-> There is a risk of malfunction, electric shock, and fire.



Prevent children from touching the device recklessly.

-> There is a risk of child safety accidents or malfunctions.



Do not place flammable objects near the device.

-> It may cause a fire.

Caution



Do not install in places exposed to direct sunlight.

-> There is a risk of and concerns about deformation and malfunction discoloration.



Do not install in places with high humidity or a lot of dust.

-> There is a risk of malfunction.



Do not dirty the fingerprint input area.

-> The fingerprint cannot be recognized correctly.



Avoid giving impacts to the device or letting sharp objects come into contact with it.

-> Product breakage may cause malfunctions.



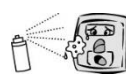
Do not clean by spraying water directly or wipe with benzene, thinner, alcohol, etc.

-> There is a risk of electric shock and fire.



Do not place magnetic objects close to the device.

-> There is a risk of malfunction.



Do not spray insecticides or flammable sprays on the device.

-> There is a concern about deformation and discoloration.



Do not install in places with extreme temperature changes.

-> There is a risk of malfunction.

-> Be cautious of burns when using the product.

- If the displayed precautions are not followed, there may be a risk of injury or property damage to the user.

※ We are not responsible for accidents and damages that occur due to the failure to use the product as instructed in the user manual.

I Cautions in Installation

- Install at a height of 135cm from the bottom of the product body.
- Do not install it under a light with an incandescent bulb.
- In addition, it is recommended to adjust the installation location in an environment where strong light is directly shining on the face recognition camera.
- It is not recommended in an environment with backlight or direct sunlight.
- When installing the product in a place where the illuminance exceeds 30,000 lux, the installation location must be changed or measures must be taken to provide shade to the recognition device.
- Do not install the same product in near locations (within 50cm).
- Comply with the installation height. The recognition rate may decrease due to the angle of the face when installed in a low or high location.
- If the wall is uneven, the tamper may not be detected properly.
- In the case of a place where people are near around or waiting for an elevator, use it by reducing the face recognition distance.
- When installed on speed gates, ensure that the viewing area does not overlap with neighboring gates during operation, and adjust the width of the verification area as needed to prevent users standing at neighboring gates from being mis-authenticated.

- If the displayed precautions are not followed, there may be a risk of injury or property damage to the user.

※ We are not responsible for accidents and damages that occur due to the failure to use the product as instructed in the user manual.

02 | Terminal Specific Names

Chapter 1

Pre-use Verification



*** XScan : Optional devices with fingerprint, QR reader**

- To register and authenticate fingerprints, XScan (optional) must be installed
- For detailed installation instructions for the product, please refer to the UNION biometrics website (<http://unionbiometrics.com>).

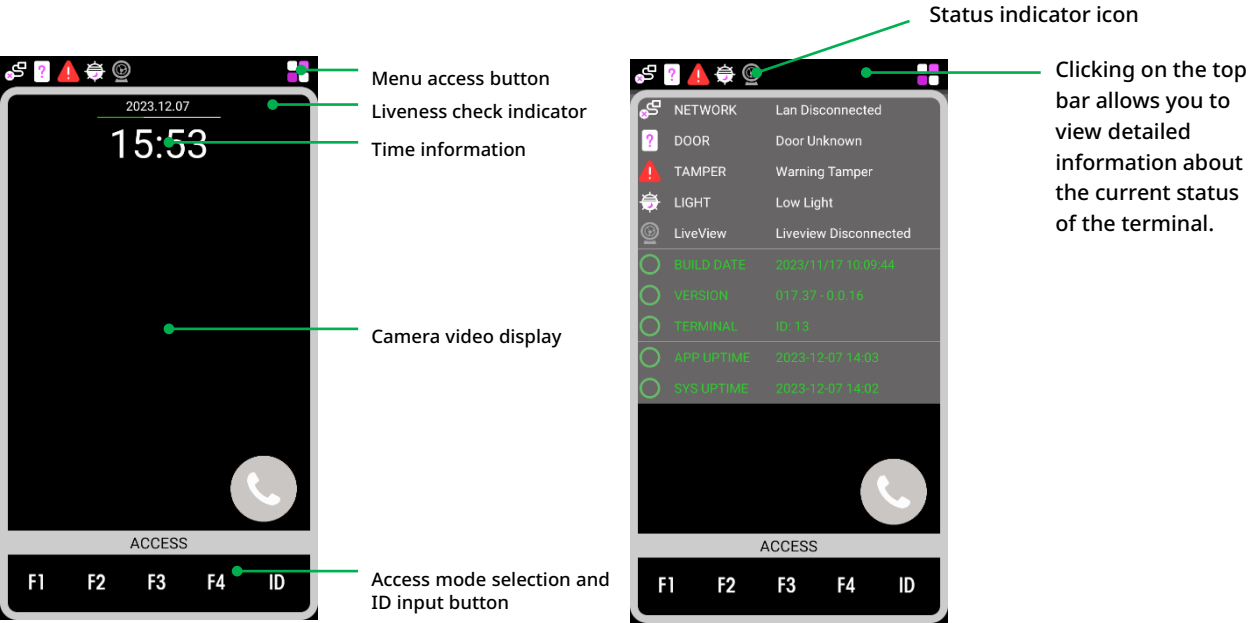
I Sound

Voice guidance	Motion detection
You are authorized.	Upon successful authentication
Please try again.	Upon authentication failure

I Buzzer Sound (mute volume)

Voice guidance	Motion detection
'Beep'	- When a card is read - When a fingerprint is entered into the fingerprint reader
'Bee Beep'	Upon authentication failure
'Bee~ep~'	Upon successful authentication

I Screen

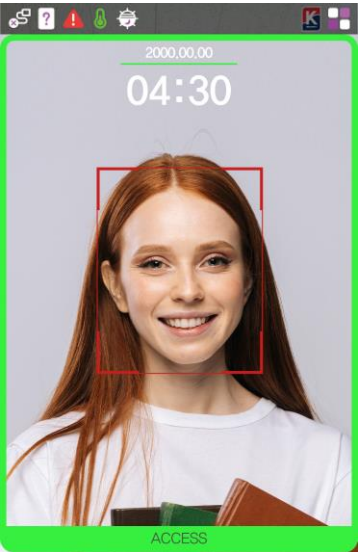


Icon

icon	info	icon	info
	Offline state, not connected to the internet		LAN cable disconnected
	Connected to the internet		Not connected to the server program
	Low-light detection state		Connected to the server program
	Fire sensor detected state (Fire detection on the terminal)		Heat detection sensor connection failure
	Fire sensor detected state (Fire detection from the server)		Heat detection sensor connection normal
	Terminal disassembled state (Tamper switch activated state)		Continuous unlock state (State where continuous unlocking is configured from the server)
	Door status unknown		Continuous unlock state (Scheduled unlocking state)
	Door closed		Warning sound (fire alarm)
	Door open		Warning sound (tamper alarm)
	Door abnormal state (forced entry)		Warning sound (forced entry)
	Door abnormal state (continuous door opening)		Warning sound (continuous door opening)
	XScan connection status		Warning sound (emergency alert by the server)

I Message

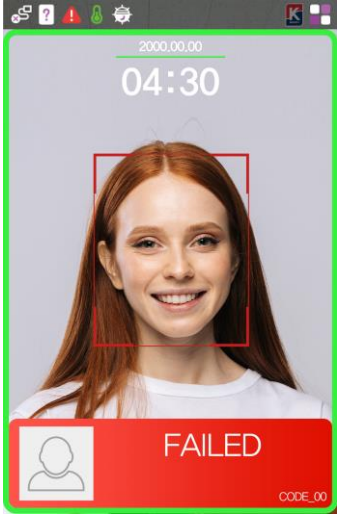
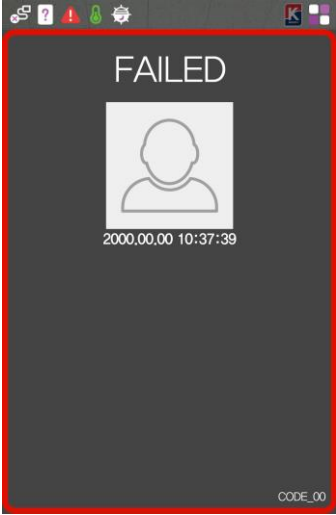
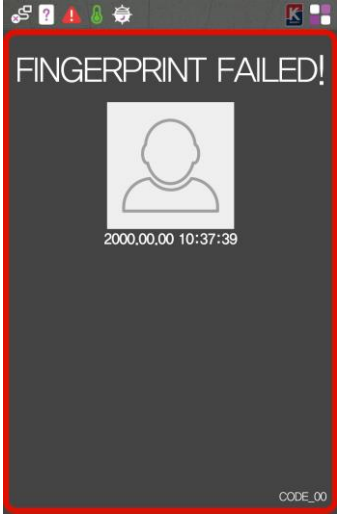
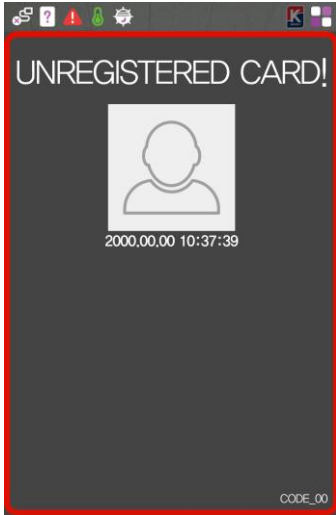
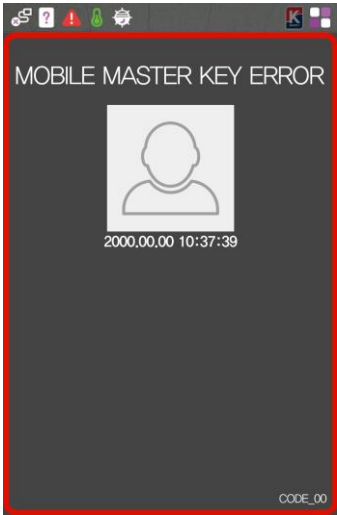
Main Screen

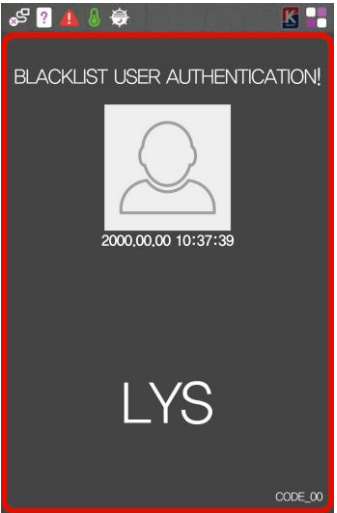


Message when authentication succeed

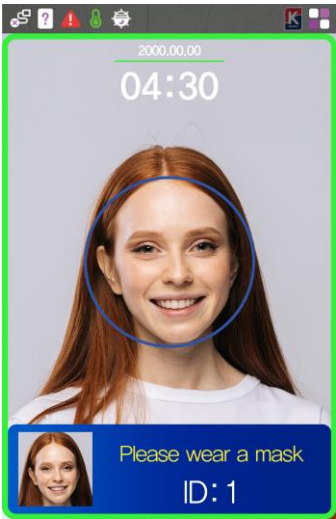
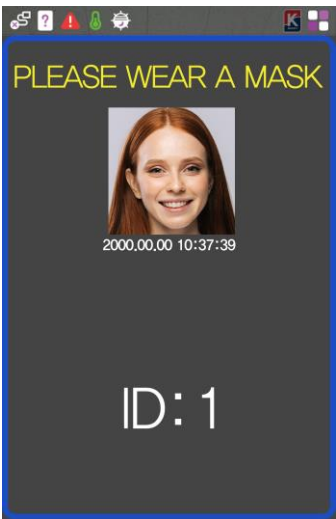
action	Bottom Popup (Default Setting)	List Popup	Whole Popup
Screen	The image shows the main screen of the 'I Message' app with a bottom popup. The popup is blue and contains the text 'SUCCESS' in yellow and 'ID: 2' in white. There is a small thumbnail of the woman's face to the left of the text.	The image shows the main screen of the 'I Message' app with a list popup. The popup is blue and contains four thumbnails of the woman's face, each labeled with the number '2'.	The image shows the whole screen of the 'I Message' app. The screen is dark blue and contains the text 'SUCCESS' in white at the top, a small thumbnail of the woman's face in the middle, and the text 'ID: 2' in white at the bottom.

Message when authentication failed

action	Bottom Popup (Default Setting)	List Popup, Whole Popup, Authentication method except Face	Fingerprint input Failure
Screen			
action	Bottom Popup (Default Setting)	List Popup, Whole Popup, Authentication method except Face	If the Mobile Master Key is not correct
Screen			

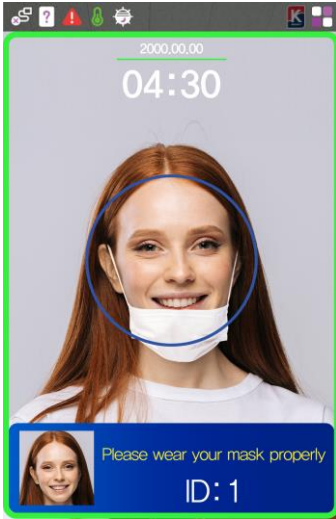
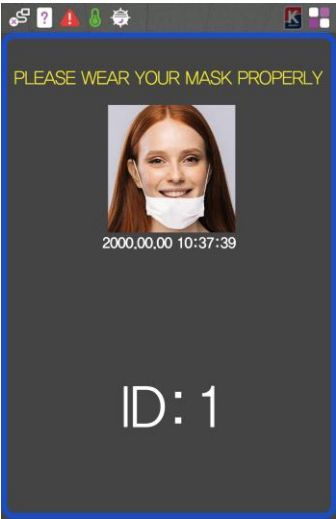
action	Antipassback Error	Duplicate authentication in Meal's same time zone	No response/disconnected when authenticating in the server
Screen	 The screen displays 'ANTIPASSBACK ERROR!' at the top, a user icon in the center, the timestamp '2000.00.00 10:37:39' below the icon, 'ID: 1' at the bottom, and 'CODE_00' in the bottom right corner.	 The screen displays 'DUPLICATE AUTHENTICATION FAILED!' at the top, a user icon in the center, the timestamp '2000.00.00 10:37:39' below the icon, 'ID: 1' at the bottom, and 'CODE_00' in the bottom right corner.	 The screen displays 'NETWORK ERROR!' at the top, a user icon in the center, the timestamp '2000.00.00 10:37:39' below the icon, 'ID: 1' at the bottom, and 'CODE_00' in the bottom right corner.
action	No authentication authority or unavailable access time	Blacklist user authentication	Face too close in authentication
Screen	 The screen displays 'NOT AUTHORIZED!' at the top, a user icon in the center, the timestamp '2000.00.00 10:37:39' below the icon, 'ID: 1' at the bottom, and 'CODE_00' in the bottom right corner.	 The screen displays 'BLACKLIST USER AUTHENTICATION!' at the top, a user icon in the center, the timestamp '2000.00.00 10:37:39' below the icon, 'LYS' at the bottom, and 'CODE_00' in the bottom right corner.	 The screen shows a live face scan of a woman. A blue circle indicates the face is too close. A red banner at the bottom contains a white exclamation mark icon and the text 'Please step backward'.

Message for not wearing a mask properly * The design changes based on the selected popup type.

action	Bottom Popup (Default Setting)	List Popup	Whole Popup
Screen			

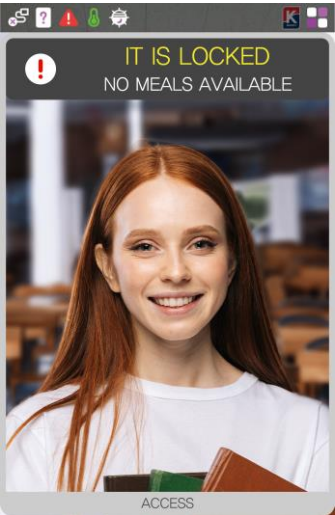
No text is displayed in the popup, only the voice "Please put on your mask".

Message for not wearing a mask properly * The design changes based on the selected popup type.

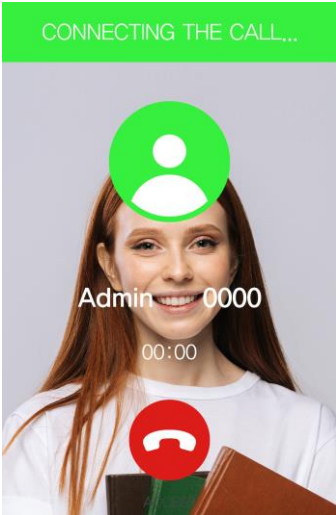
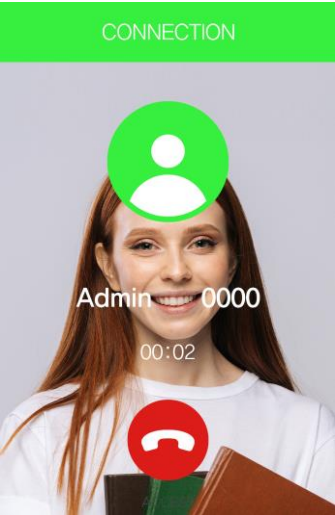
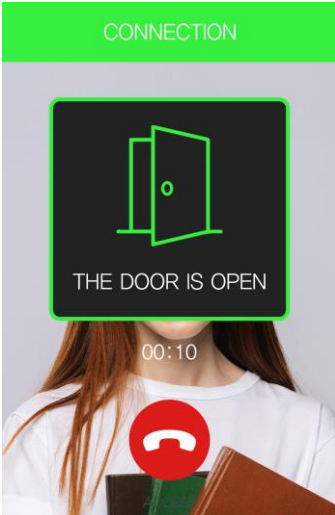
action	Bottom Popup (Default Setting)	List Popup	Whole Popup
Screen			

No text is displayed in the popup, only the voice "Please put on your mask".

Message when Locked

action	Terminal locked	Not meal time in meal management setting
Screen		

Video Intercom Message

action	Video Intercom Connection trial	Video Intercom Connection Success	Video Intercom Connection door open
Screen			

Message when Locked

action	Waiting for user id input	Waiting for password input	Waiting for FP input
Screen	BACKINPUT ID INPUT USER ID 123 456 789 ←0OK	2024 06 2514:14 ✖ Input password 123 456 789 ←0OK ACCESS F1F2F3F4ID	2024 07 0114:25 ? ✖ Place finger on sensor F1 F1F2F3F4ID
action	Waiting for card input	Upgrading device program	
Screen	2024 06 2515:14 ? ✖ VERIFY CARD Place your card ACCESS F1F2F3F4ID	2024 06 2518:20 Upgrading... Do not power off ! ACCESS	

Do not power off power until 'Upgrading.. Do not power off !' ends.

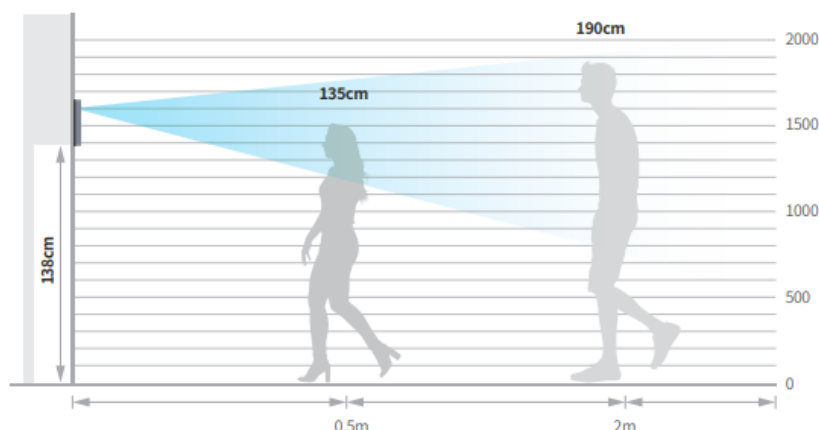
I Face

Face Registration method

- Please maintain a distance of about 50cm between the terminal and your face. Position your face within the guidelines on the LCD screen and register your facial pose according to the instructions.
- Ensure that your face, including the lower part of your face with eyebrows, is not covered by hats, masks, eye patches, hair, etc.
- Keep still and gaze directly at the camera during the capture.

Correct face registration and authentication methods

- Authenticate yourself from a distance of 50 to 200cm away from the device.
- Do not tilt your head up or down. Register one person at a time unless specified otherwise.
- When the positioning guide appears, authenticate your face according to the instructions.
- Ensure that your eyebrows and the lower part of your face are visible to the device.
- Failure to follow the instructions may result in a longer or failed facial authentication process, so please adhere to the on-screen guidance.



Considerations during registration

- You can also register with a photo at the level of an official ID picture taken within the last 3 months.
- Look directly at the camera and maintain a neutral expression (a natural face with closed lips).
- Capture your face aligned with the guidelines displayed on the screen.
- Ensure that the contours of your entire face, including eyes, eyebrows, forehead, nose, mouth, and jawline, are clearly visible.
- Capture the photo against a plain, bright background with no other faces or objects.
- When registering with a photo, ensure that the minimum size is at least 200 x 200 pixels.

Considerations during authentication

- It is recommended to register and authenticate at the installation location of the terminal.
- Taking different poses from the registered face may decrease the facial recognition accuracy.
- Positioning the face frontally is preferable.
- Thick eyeglass frames or sunglasses can obscure eye features, leading to a reduction in facial recognition accuracy.
- If eyebrows are covered by hair or glasses, facial authentication may fail.
- Covering a significant portion of the face with hair or a mask can reduce facial recognition accuracy.
- After installing the recognition device, please remove the protective film before registering and authenticating your face, as the protective film may cause a decrease in recognition accuracy.

※ If there are changes in style (dyeing, eyeglass frames, bangs, etc.), re-registration is recommended.

I Finger

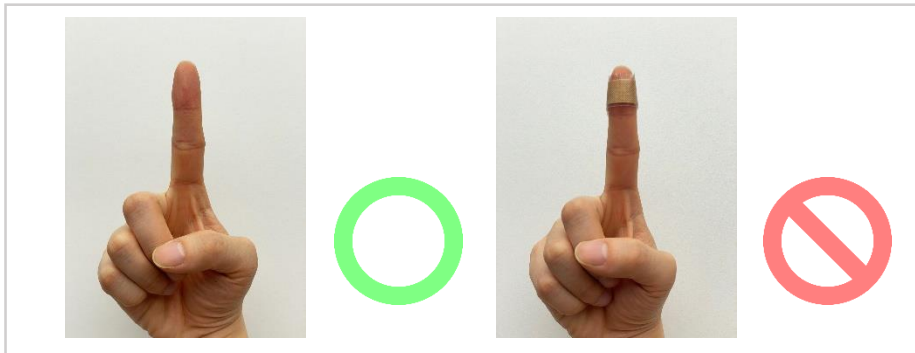
* To register and authenticate fingerprints, XScan (optional) must be installed.

Correct fingerprint registration method

- Please use your fingertip to press as if leaving a fingerprint.
(Entering by lightly touching with only the fingertip is not the correct registration/input method.)
- Ensure that the exact center of the fingerprint touches the fingerprint input area.



- If your fingerprint is excessively dry or moist, blurred, or has injuries, it may be difficult to recognize. In such cases, please register a fingerprint from a different finger.



Considerations during registration

- This product, when fingerprint recognition is impaired or fingerprints are delicate, cannot use fingerprints, and you must operate it with a password.
- For the elderly, if there is severe wrinkling on the fingerprint to be registered, there may be cases where registration is not possible.
- It is recommended to register two or more fingerprints for users if possible.
- For children, if the fingerprint size is too small or delicate, usage may be difficult or impossible, and it is necessary to re-register fingerprints every 6 months.

Precautions for Authentication

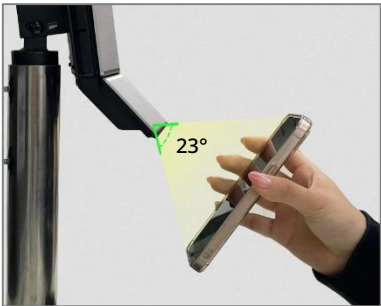
- Please input a fingerprint similar to the one registered with the corresponding finger.
- Be cautious of the risk of frostbite during fingerprint input.
- If your hands are dry, blowing warm air onto them can help with smooth operation.

I QR

* To register and authenticate using QR, XScan (optional) must be installed.

Correct QR registration method:

- Adjust the angle to make the QR code visible to the terminal.
- Maintain a moderate distance, neither too close nor too far.



<Authentication possible angle
23 degrees>



<Height 45mm ~ 175mm>



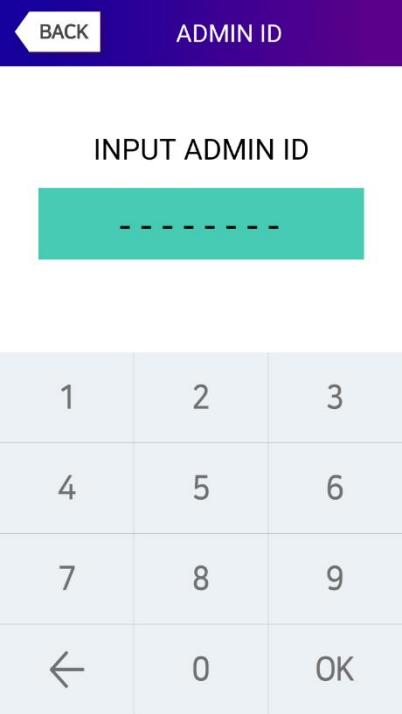
<Error based on wrist angle>

Types of QR codes that can be registered

Barcode Type	Scanner Engine (EM3396)	Barcode Type	Scanner Engine (EM3396)
1D	Code 128	1D	UCC-EAN-128
	EAN-13		GS1 Data bar
	EAN-8		Matrix 2 of 5
	Code 39		Code 11
	UPC-A		Industrial 2 of 5
	UPC-E		Plessey
	Code bar		MSI-Plessey
	Interleaved 2 of 5	2D	PDF417
	ITF-6		ECC200
	ITF-14		ECC000
	ISBN		ECC050
	Code 93		ECC080
	UCC-EAN-128		ECC100
	GS1 Data bar		ECC140
	Matrix 2 of 5		QR Code
	Code 11		Chinese Sensible Code

I Administrator Authentication

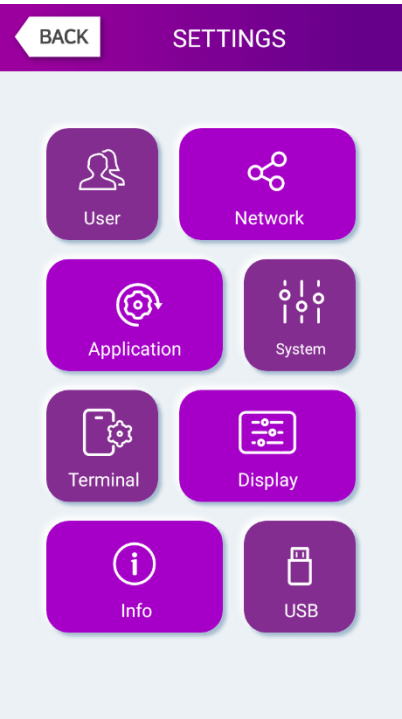
If an administrator is registered, the following administrator authentication screen will appear first.



- ① When entering the administrator ID, authenticate the administrator using the method specified for that administrator, such as card, fingerprint, face, or password. Upon successful authentication, you can access each menu.
- ② Administrator authentication appears only if there is a registered administrator.
- ③ Administrator authentication is required only once when entering menu mode, and access to all menus is possible until completely exiting from the main menu.

* If only card (mobile card), only fingerprint, or both card (mobile card) and fingerprint are included in the authentication methods, you can access the menu without entering an ID during authentication.

I Menu Structure and Navigation



Pressing the [] icon on the main screen enters the main menu screen on the left.

> You can enter each submenu by pressing the respective button.

Menu Configuration

Name	Details	
1. User	1. Add 2. Modify 3. Delete 4. Delete All 5. View	
2. Network	IP address	Static IP / DHCP / Ethernet ▶ IP address ▶ Subnet Mask ▶ Gateway ▶ DDNS
	DNS Server	▶ DNS Server1 ▶ DNS Server2
	Server IP	▶ Server IP ▶ Port
	Terminal ID	▶ Terminal ID
3. Application	1. Applictaiion	▶ Access / TnA / Meal 1. When setting 'Access' or 'TnA' ▶ Schedule F1 (Attend) time F2 (Leave) time F3 (Out) time F4 (In) time Access time ▶ Blocking Time 2. When setting 'Meal' ▶ Schedule Breakfast time Lunch time Dinner time Supper time Snack time ▶ Allow duplicate

Name	Details	
	2. Function key	▶ Enable F1 ▶ Enable F2 ▶ Enable F3 ▶ Enable F4 ▶ ID Input
4. 시스템	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] ▣ Face Finger Detection ▶ Check similar FP ▶ Multi FP ▶ Enable 1:N
	3. Face	▣ Verified distance ▣ Mask Detection ▣ AE flicker frequency ▣ Face Popup Type ▶ Anti Spoofing ▶ Enable 1:N ▶ Multi Face Detection
	4. Auth	▣ Auth Type
	5.. UBio-Core	▣ Live View ▣ Intercom
	6. Date/Time	▣ Time synchronization ▣ Display Format ▣ Set Date ▣ Set Time

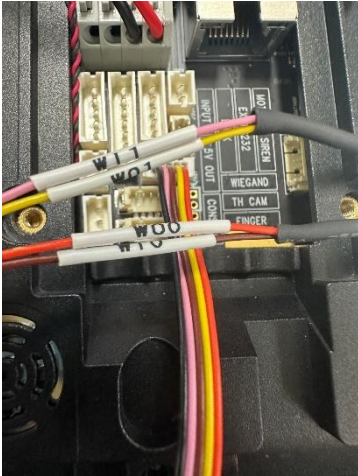
Name	Details	
5. Terminal	7. Database	1. Delete all users 2. Delete setting 3. Delete Log 4. Delete Image log 5. Factory init 6. Reboot 7. Restart App
	1. Sound	▶ Voice Volume ▶ Beep Volume ▶ Sound Option
	2. Option	▶ Read Card number ▶ Card format ▶ Card reader ▶ Ble Rssi ▶ Ble TxPower ▶ Lock terminal
	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 ▶ RS485 ▶ Wiegand Site Code Wiegand Output Wiegand Input ▶ External Device

Name	Details	
	6. ETC.(Thermal)	▶ Thermal Camera Use ▶ Display ▶ Operation Setting
6. Display	1. Camera	▶ Save Option ▶ Save success log ▶ Save failed log ▶ Save Option
	2. Language	▶ Language
	3. Option	▶ Power saving mode ▶ Display Option ▶ Touch Calibration
	4. Message display time	▶ Message Display Time (ms)
7.	1. System	▶ System Info ▶ Disk ▶ Ram
	2. Terminal	▶ Terminal Info Terminal ID/Application/Language/Stored Voice AccessControl Info View Schedule Info View
	3. Network	▶ Network Info MAC WMAC <Ethernet> IP
	4. User	▶ User
	5. Log	▶ Log Info
	6. About	▶ About

Name	Details	
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 Option
	3. Others	1. Theme 2. F/W Upgrade

I Entering the Menu Without Administrator Authentication

In case of losing the registered administrator card on the terminal or when there is no administrator for fingerprint or face authentication, here is a method to enter the menu.



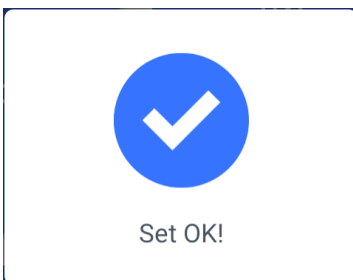
<Figure 1>

- ① Remove the bracket on the back of the terminal to open the cover.
- ② In the open cover state, connect the bottom 5-pin connectors on the back of the device as shown below: connect 1 and 3, and connect 2 and 4.
- ③ On the main screen, press the [] icon to enter the administrator authentication screen in <Figure 1>. Fill in the administrator ID as '00000000' (the length of the user ID) and press the [] button to enter the menu screen.
 - ☛ Press 0 as many times as the length of the user ID to be recognized as "00000000."

> After modifying the settings, be sure to disconnect the connector pins.

I Saving Configuration Settings

After making changes to the settings, pressing the [Complete] button in each menu to save the changes will display a message box like the one below.



> If there are no changes, it will exit to the previous menu screen.

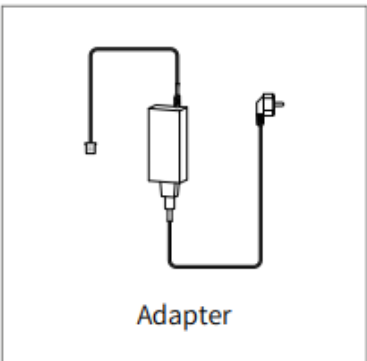
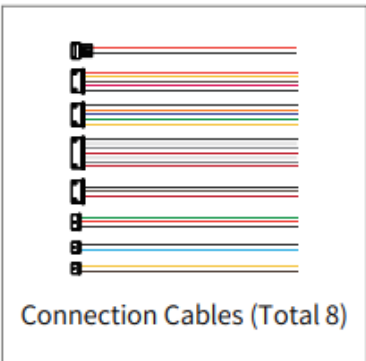
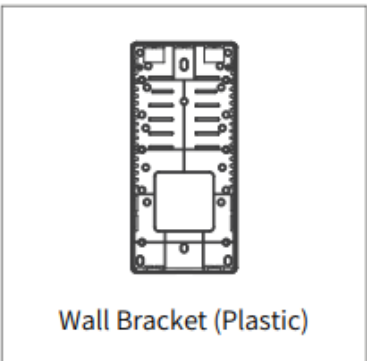
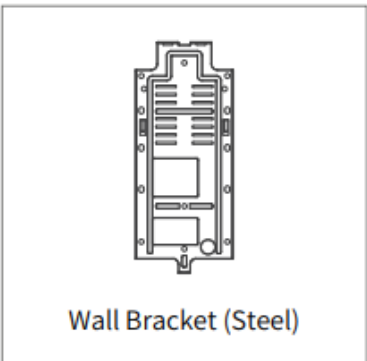
> If there is no input for 30 seconds while changing the settings in the menu, it will exit to the previous menu.

Chapter 2

Product Description

01	Product Composition	27
	Components	27
	Cables	28
02	System Configuration Diagram	29
	Standalone Usage	29
	Connection with PC Server	29
03	Specifications	30

I Components



Warning

- Components may vary depending on the installation environment.
- XScan is a separate optional product and is not included in the components.
- For information on product installation, please visit the UNION biometrics website (<https://unionbiometrics.com/>) and check the installation guide.

I Cables

Power Adapter



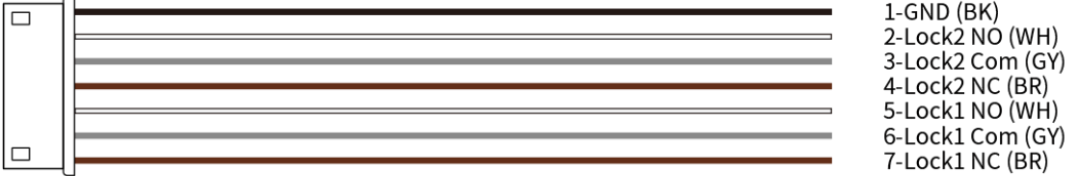
Wiegand



Lock Status



Lock



RS-232



Light Bar



5V Out



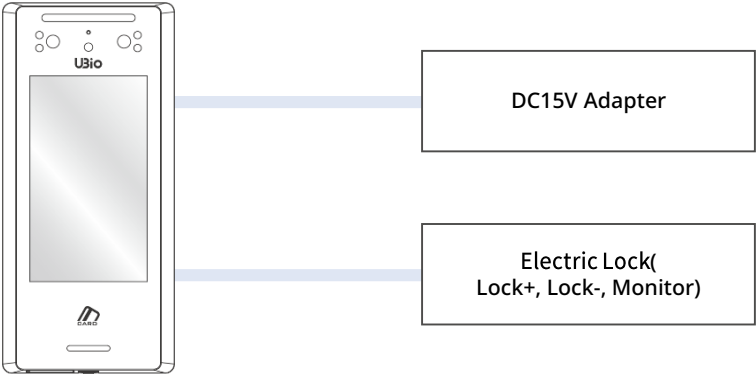
Motor Cable



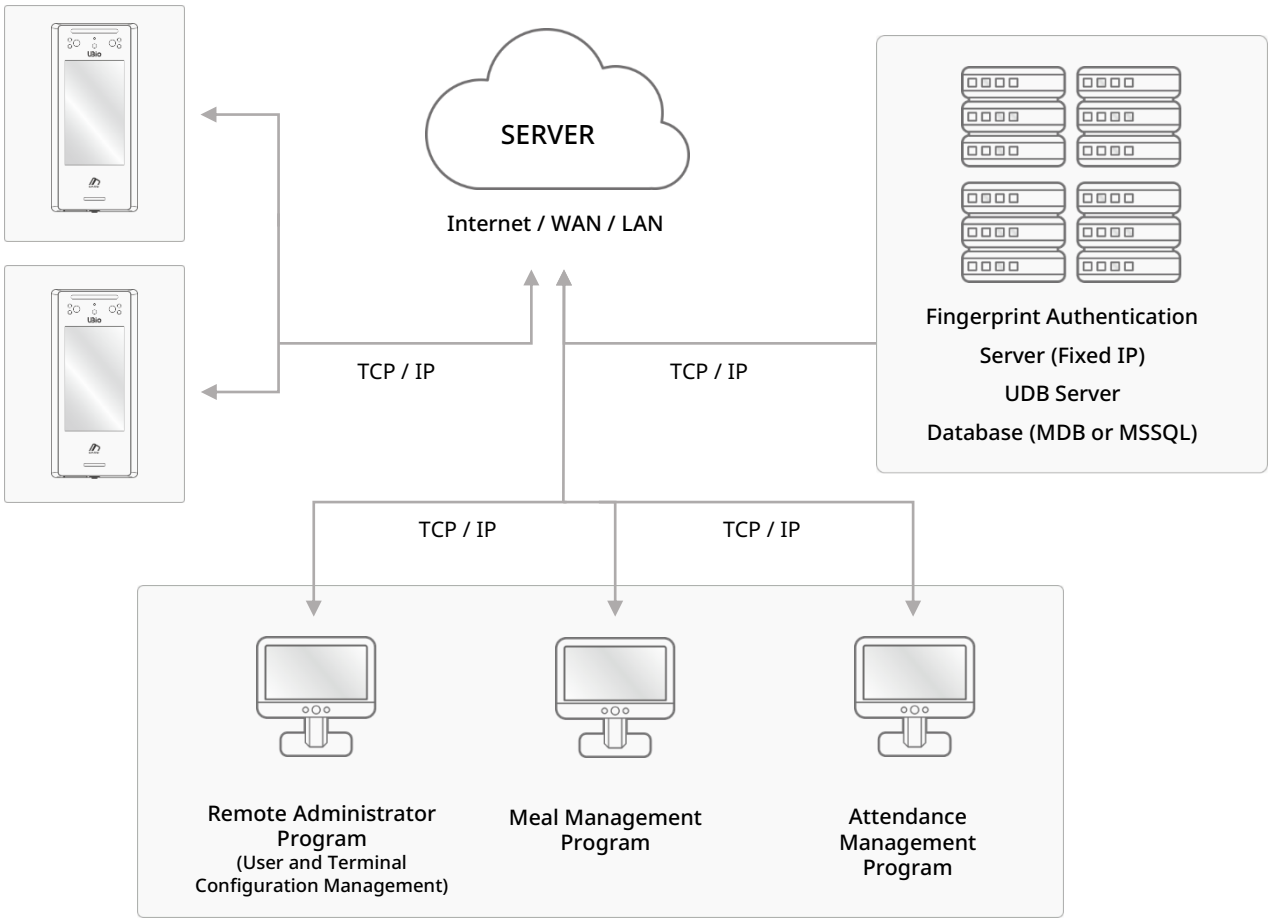
02 | System Configuration Diagram

Product Description

I Standalone Usage (entry/exit)



I Connected to PC Server (access control, attendance, meal management)



03 I Specifications

Category	Spec	Remark
CPU	Cortex A53 Quad Core 1.8GHz)	
LCD	5" 720 x 1280	
MEMORY	eMMC 16GByte	
	LPDDR4 / 4GByte x 1EA	
External Type C USB Supprot	Data Backup / FW Upgrade	
Camera	Dual Camera (Color & IR)	
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 (Lock Control double use)	
Communication Port	TCP/IP (10/100/1000Mbps)	Authentication Server Communication
	RS-232	Meal Ticket Printer
	RS-485	Controller Communication
	Wiegand In/Out	Card Reader or Controller Communication
Card Reader	125KHz EM & 13.56MHz Smart Card Reader, ISO14443A/B, MiFare, MiFare Plus, Felica, ISO15693	
SIZE	91.96 x 199.96 x 21 (mm)	

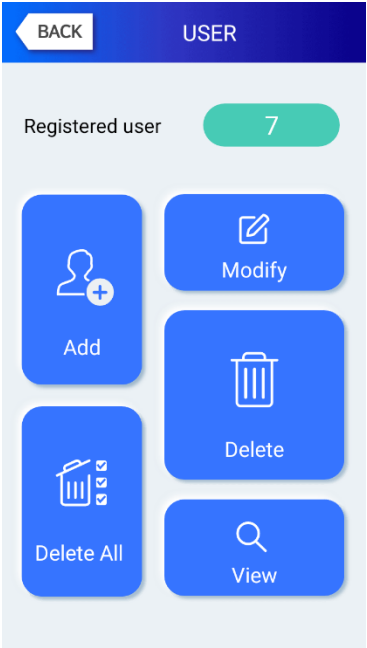
Chapter 3

Administrator

01	User Management	32
02	Enrollment	32
	Face	34
	Password	35
	Card	35
	Finger	36
	QR Code	37
	Save	38
03	Modify	39
04	Delete	39
05	View	40

01 | User Management

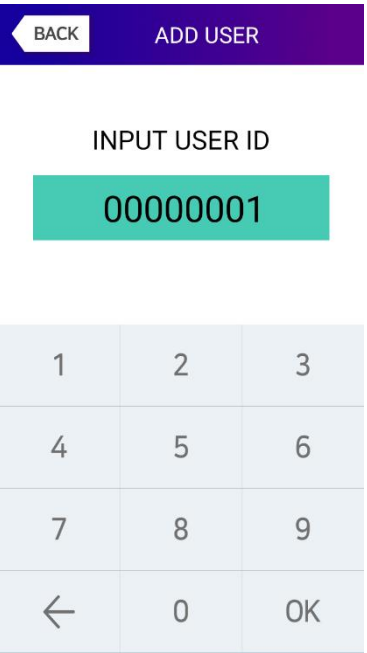
When you select [User] from the main menu, the following screen appears.



> The total number of registered users, including administrators, is displayed at the top of the screen.

Button	Action Type
Add	Add New User
Modify	Modify User
Delete	Delete User with a specific ID
Delete All	Delete All Users, including administrators
View	View the list of registered users

02 | Enrollment



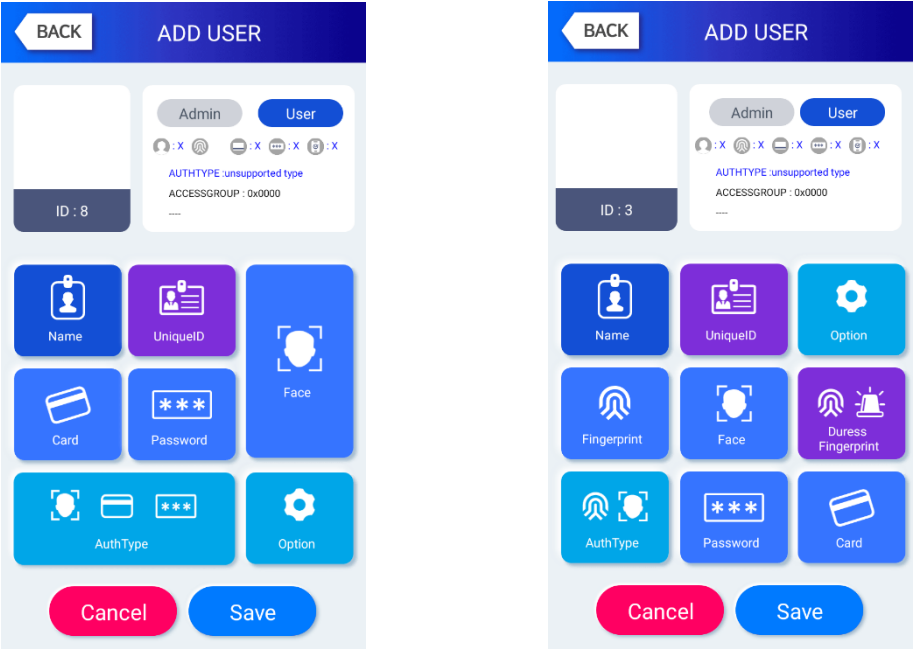
You can register information for a new user.

- ① In [User], press the [Add] button.
- ② Enter the user ID to be registered and press [OK].
The automatically generated available ID will be displayed on the screen, making it convenient for registration.

* To change the ID, press the [] button to delete the existing value and enter a new one.

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

- ③ If you enter an ID that is already registered, a failure message will appear. If you enter an ID that is not yet registered, the following screen will appear.



<When XScan is not attached>

<When XScan is attached>

> The above icons have the following meanings :

Icon	Meaning
	Facial registration status (X: Not registered, 1: Registered)
	Number of registered fingerprints (X, 1~10)
	Password registration status (X: Not registered, 1: Registered)
	Number of registered cards (X, 1~10)
	Mobile key registration status (X: Not registered, 1: Registered)
User	User
Admin	Administrator

- ④ To complete the registration and save, press the **[Save]** button. To cancel the input and exit, press the **[Cancel]** or **[BACK]** button.

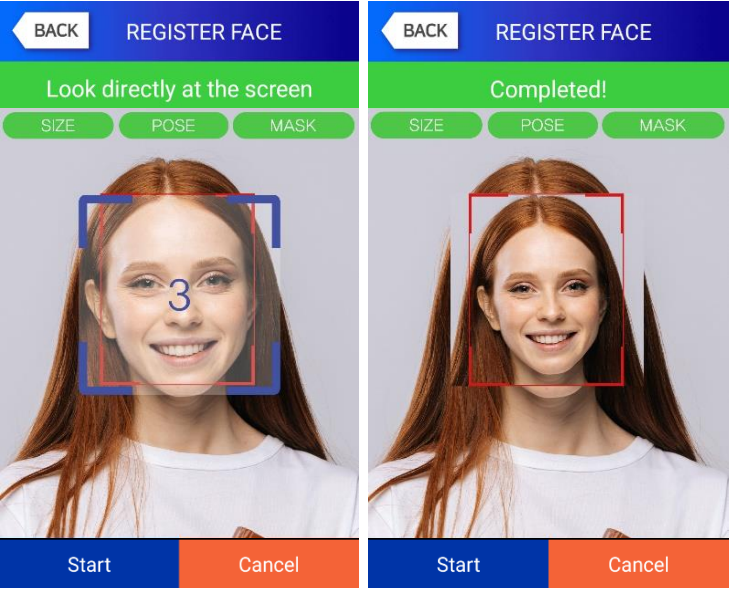
※ By default, it is registered as a regular user, and by pressing the **[Admin]** button, you can change to an administrator.

※ Only users registered as administrators can change the operation method of the terminal and register/modify/delete information for all users stored in the terminal. Therefore, be cautious about administrator registration.

※ When booting, the presence of the XScan device is determined, and if the device is not present, the fingerprint registration menu is not available on the registration page.

I Face

Please refer to the 'Correct Registration and Authentication Methods' for registration.



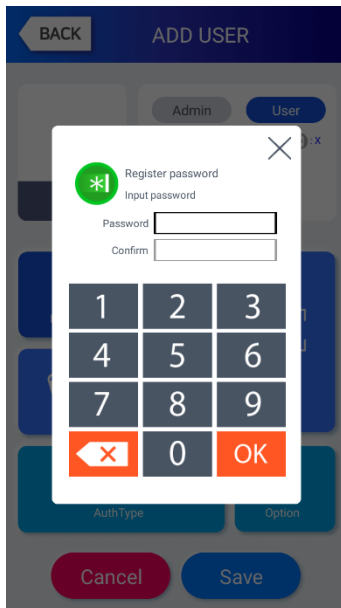
- ① Align your face with the red guide that recognizes the face and the blue outline in the center, as shown on the left screen, and proceed with registration.
- ② Press the **[Start]** button to start facial registration. Avoid blinking when the number on the screen is displayed as 0 because it indicates that the face is registered at that moment.
- ③ When registration is complete, a message saying **"Completed!"** will be displayed, as shown on the left screen. Press the **[OK]** button to complete facial registration and return to the previous screen.

If you want to register again, press the **[Start]** button and start the process from step ② above.

Guidance screen in case of registration failure

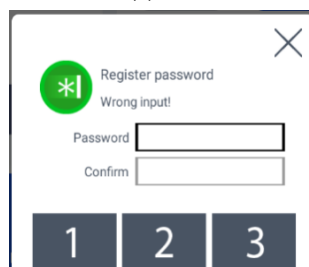
Case	If the face registration size is too small	If the face registration size is too large	When wearing a mask during registration
Guidance Screen			

I Password



- ① If you enter a password of 1 to 8 characters in the password entry window and press the [OK] button, the input focus moves to the 'Password Confirmation' window below.
- ② Enter the same password again and press the [OK] button. To cancel and exit, press the [X] button.

※ After entering the password, if a different number is entered during confirmation, the message "Wrong input" will appear as below.

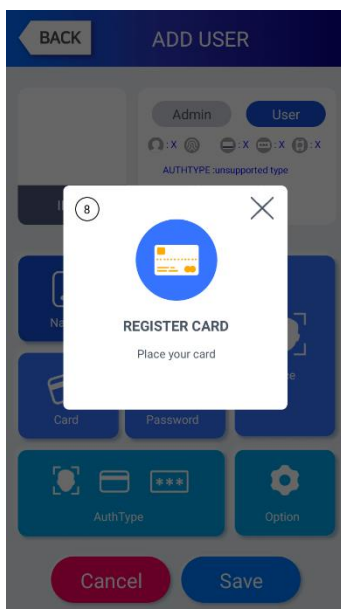


Threatening Password (Server integration is required)

If the registered password is entered in reverse order during password entry, authentication is successful, but it notifies that it is an attempt at coercion authentication to the server.

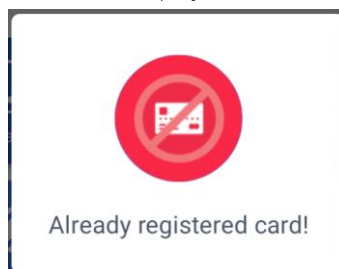
Ex) If the password is 1234, entering 4321 will authenticate it as a coercion password.

I Card



- ① Press the [Card] button on the [ADD USER] screen to register. To exit without registering, press the [X] button.

※ If a card that is already registered is entered, the message below will be displayed..

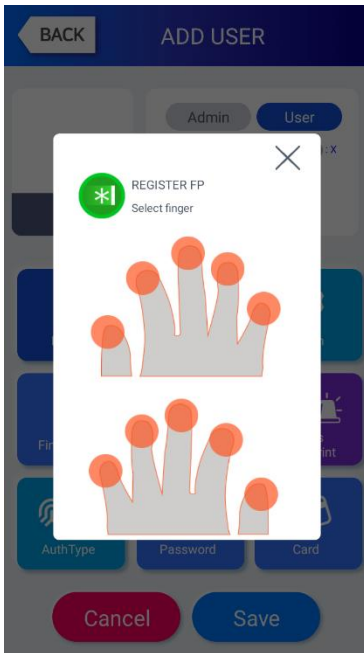


※ If an attempt is made to register more than 10 cards per user, the following message will be displayed.



I Finger

* To register and authenticate fingerprints, XScan (optional) must be installed..



- ① On the [ADD USER] screen, press the [Fingerprint] button to register. To cancel the registration and exit, press the [X] button in the top right corner.
- ② When the screen below appears, select the finger to register.

* If you are registering multiple fingers, already registered fingers will be indicated with a blue circle [●], and duplicated threat fingerprints will be indicated with a purple circle [●]. If you select an already registered finger, the following message will be displayed. Choosing to re-register will erase the existing fingerprint and allow you to register again.

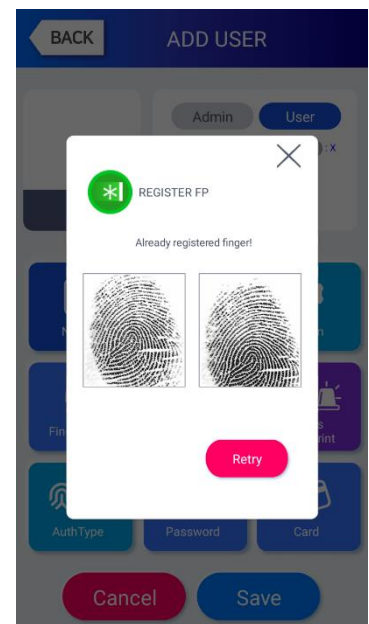
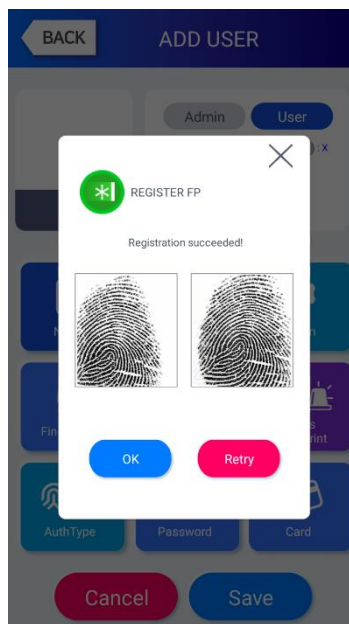
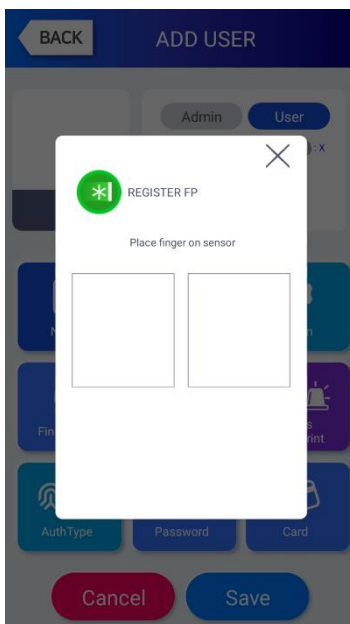
Threatening Password (Server integration is required)

- ① When authenticating with the threat fingerprint, authentication success is achieved, but it notifies the server of an attempt to authenticate with a threat fingerprint.

※ Authenticating a finger registered as a threat fingerprint sends an alarm message to the server. If you set Threat Situation Notification in 5.4.4.Lock Settings, you can provide a contact signal.

- ② Refer to '**1.4 Correct Fingerprint Registration and Input Method**' and input the fingerprint. Enter the fingerprint twice following the on-screen instructions.
When the message '**Enter fingerprint**' appears and the light on the fingerprint sensor turns on, place your finger on the sensor and wait for about 2-3 seconds until the light turns off, then remove your finger.
- ③ When the message '**Enter the same fingerprint again**' appears, re-enter the fingerprint you just input.
※ For the second fingerprint input after the first one, you must lift your finger from the fingerprint input window and then input it again.
- ④ Once the input is complete, the following message will appear. Press the [OK] button to complete the registration and return to the main menu.

If the entered fingerprint is similar to an already registered fingerprint, a message such as "**Similar to an already registered fingerprint**" will appear. In this case, press the [Retry] button to start the process again from ②.



If you want to register again, press the [Retry] button to restart the process from ② mentioned above. To cancel, press the [X] button to exit.

Precautions for fingerprint registration

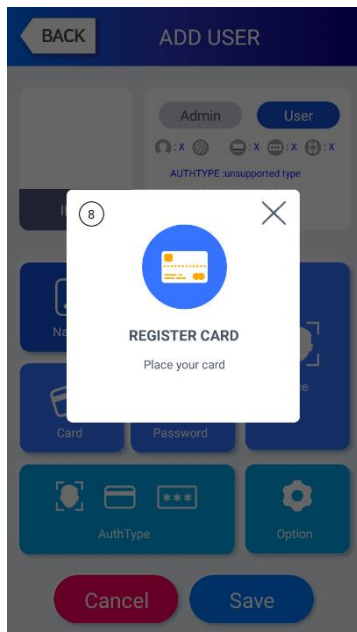
- You can register up to 10 fingerprints per ID, and exceeding this limit is not allowed.
- If repeated attempts using the correct fingerprint registration method (2-3 times) fail, it is recommended to use facial recognition, a password, or a card.

※ Note that the similarity check during fingerprint registration only checks against fingerprints registered on the device. If the same user registers on both the device and UNIS with different IDs and then transfers the user from UNIS to the device, the similarity check may not be performed, and each ID may authenticate successfully independently. Please be aware of this situation.

※ If XScan is installed later, it is necessary to download fingerprint users again from the server.

QR Code

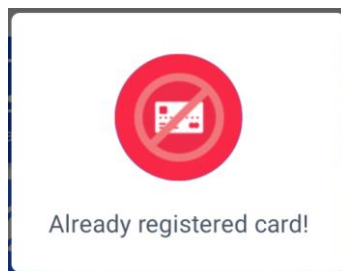
* To register and authenticate fingerprints, XScan (optional) must be installed.



① Press the [Card] button on the [Add User] screen to register a card.

If you want to exit without registering, press the [X] button.

※ If you enter a card that is already registered, the following message will be displayed..



※ If you attempt to register more than 10 cards per user, the following message will be displayed.



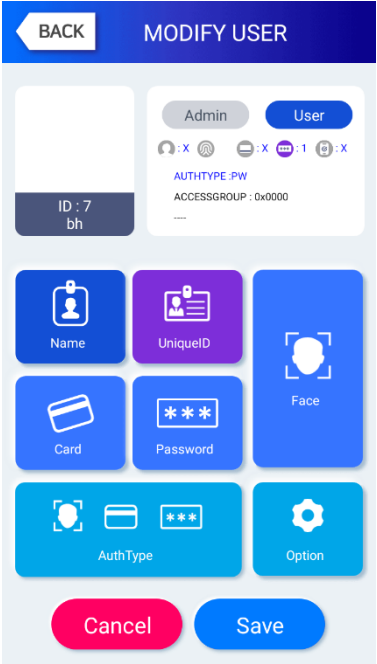
I Save

If the registration process is complete, press the [Save] button to save. If you exit without pressing the [Save] button by pressing [Cancel] or [BACK], the user will not be saved.

Here are possible LCD messages that may appear during the registration process:

	When the [Save] button is pressed If registration is successful
	When pressing the [Save] button When user registration fails: Fails if none of the authentication methods (fingerprint, face, card, password) are registered
	When pressing the [Auth Type] button When there are no registered authentication methods.
	When [registering fingerprints] When registering fingerprints and entering different fingerprints without repeating the same fingerprint.
	When [registering fingerprints] When attempting to register the same fingerprint again. (However, it is possible to input the same fingerprint for different user IDs.) ※ To register the same fingerprint for different user IDs, you must disable the 'Prevent Similar Fingerprints' function in 'System → Fingerprint Recognition.' In this case, the same fingerprint can authenticate with different user IDs, so it may not be suitable for attendance management, etc.

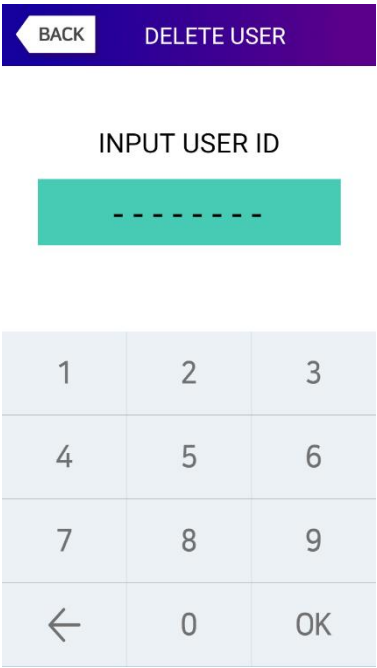
03 | Modify



- ① In the main menu, select [User] → [Modify].
- ② Enter the user ID to be modified and press the [OK] button. To cancel and exit, press the [BACK] button.
- ③ If an unregistered ID is entered, a failure message will be displayed, and if a registered ID is entered, the information of the registered user will be displayed as follows:
 - > The left icons have the following meanings:

Icon	Meaning
	Facial registration status (X: Not registered, 1: Registered)
	Number of registered fingerprints (X, 1~10)
	Password registration status (X: Not registered, 1: Registered)
	Number of registered cards (X, 1~10)
	Mobile key registration status (X: Not registered, 1: Registered)
	The user ID to be registered
	User
	Administrator

04 | Delete



Enter the user ID to delete and press the [OK] button. To cancel and exit, press the [BACK] button.

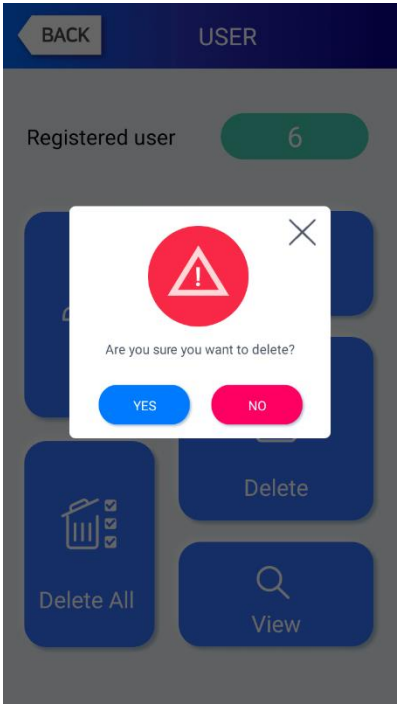
If an unregistered ID is entered, the screen will display a failure message, "Unregistered!". If a registered ID is entered, a success message, "Deleted!", will be displayed.

However, deleting from the terminal does not mean it is deleted from the server. To completely delete, you must also delete it from the server.

During deletion, there is no distinction between user/administrator, so caution is required. If a user is deleted only from the terminal without being registered on the network server, it cannot be recovered, so please be careful.

The following are LCD guidance messages that may appear during the deletion process.

	Successful deletion
	Entering an unregistered ID



Delete All

If you select [User] → [Delete All] from the main menu, the following screen will appear.

To confirm the deletion of all users, press [Yes]. To cancel, press [No].

※ If you select [Yes], all users and administrators will be deleted, and **recovery will be impossible afterward. Please exercise caution.**

05 | View

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



The user list is displayed in ID order, and by touching the screen from bottom to top, you can continue to view the user list behind.

The list is presented in units of 100, and if there are more than 100 users, you can use the [BACK] or [NEXT] buttons to scroll through the previous or next lists.

Button	Motion detection
ID (Displayed on the list)	If you touch the ID section of a specific user on the list, you can directly move to the screen for changing that user's information.
Delete	After checking the checkboxes on the right, pressing the delete button allows you to delete the selected users all at once.
ID	Entering the user ID will display the corresponding user on the left side of the screen.
Name	Pressing the button and entering the user name will display a list of users registered with names containing the entered string.

Pressing the [BACK] button on this screen will return you to the [User] menu.

Ex) if you search for "j", all users with names containing "j" will be displayed as shown on the left screen.

Chapter 4

Authentication

01	Authentication Options	42
02	Authentication Methods	42
	Providing Various Registration and Authentication Methods	43

01 | Authentication Options

Chapter 4

Authentication



> 'FP Level' (Basic Setting : '0')

The item determining the fingerprint authentication level for each user. You can change this value to set different authentication levels for registered users.

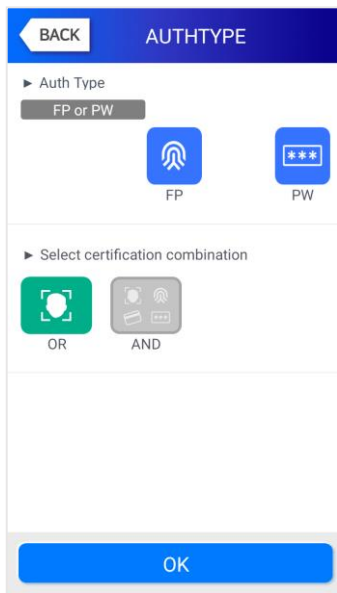
If set to '0,' the terminal uses the 1:1 fingerprint authentication level. For example, selecting fingerprint authentication level 1 means that the user will use level 1 for 1:1 authentication.

If set to 0, the system will use the 1:1 level value in the system settings → fingerprint recognition menu for 1:1 authentication.

> Enable FP 1:N (Basic Setting : Fingerprint is already registered[v])

If this option is checked, authentication is possible with just a fingerprint, without the need for a user ID or card.

02 | Authentication Methods



On the **[Add]** screen, press the **[Auth Type]** button to configure it. (However, this setting is only available if at least one authentication method is registered.)

To exit without making changes, press the **[BACK]** button.

Display all registered authentication methods and select the usage status by pressing each button. The **[OR]** / **[AND]** buttons below determine whether to authenticate the selected authentication methods with OR combination or AND combination. The selected authentication methods are highlighted in blue, and the ones that are registered but not in use are displayed in gray.

Press the **[OK]** button to confirm the changes in authentication methods and return to the previous screen.

The icons for authentication methods are displayed as follows:



: Fingerprint



: Face



: Card



: Password



: Mobile Card

※ If you do not configure the authentication method, it will automatically be set to the OR combination of the existing registered authentication methods.

(However, you can select up to a maximum of 3 authentication methods, and the OR combination with the password is limited to a maximum of 2.)

※ When using a mobile card, only OR combination is possible.

I Providing Various Registration and Authentication Methods

Face	Face registration / Face authentication
FP	FP registration / FP authentication
Card	card registration / card authentication
PW	PW registration / PW authentication
Card or FP	card, FP registration / card or FP authentication / FP authentication after entering ID
Card & FP	card, FP registration / After card authentication, FP authentication / ID input card authentication, then FP authentication
Card or PW	card, PW registration / card authentication / Password authentication after entering ID
Card and PW	card, PW registration / Authenticate your password after card authentication / Enter your ID and authenticate your password after authenticating your card
FP or PW	FP, PW registration / FP authentication / FP authentication after entering ID, password authentication possible if failed
FP & PW	FP, PW registration / Password authentication after FP authentication / After entering your ID and verifying your FP, you can also authenticate your password.
Card or Face	Card, Face registration / Card or Face authentication / Face authentication after entering ID
Card & Face	Card, Face registration / After card authentication, face authentication / ID input After card authentication, face authentication
Face or PW	Face, PW registration / Face authentication / Face authentication after entering ID, password authentication if failed
Face & PW	Face, PW registration / Password authentication after face authentication / After entering ID, face authentication and then password authentication
FP or Face	FP, Face registration / FP or Face authentication / FP authentication after entering ID, face authentication if failed
FP & Face	FP, Face registration / After FP authentication, face authentication / After entering ID, FP authentication and then face authentication
Card or FP or Face	card, FP, Face registration / Card or FP or Face authentication / FP authentication after entering ID, face authentication available if failed
Card & Face & PW	card, Face, PW registration / After card authentication, face and password authentication / After ID input card authentication, face and password authentication
Card & FP & Face	card, FP, Face registration / After card authentication, FP and face authentication / After ID input card authentication, FP and face authentication
FP & Face & PW	FP, Face, PW registration / After FP authentication, face and password authentication / After entering ID and FP authentication, face and password authentication
Mobile Card	Mobile card authentication
Card or Mobile Card	card registration / card or mobile card authentication / Card authentication after entering ID, mobile card authentication possible in case of failure
Mobile Card or FP	FP registration / Mobile card or FP authentication / FP authentication after entering ID
Mobile Card or Face	Face registration / Mobile card or Face authentication / Face authentication after entering ID
Mobile Card or PW	PW registration / Mobile card or PW authentication / PW authentication after entering ID
Mobile Card or FP or Face	FP, Face registration / Mobile card or FP or Face authentication / FP authentication after entering ID, face authentication available if failed
Card or Mobile Card or Face	card, Face registration / card or Mobile card or Face authentication / Face authentication after entering ID
Card or Mobile Card or FP	card, FP registration / card or Mobile card or FP authentication / FP authentication after entering ID

- ※ When using a mobile card, only OR combination is possible.
- ※ In OR conditions that include both cards and mobile cards, the card and mobile card combination is excluded from 1:1 authentication attempts.
- ※ QR registration and authentication methods are the same as cards.
- ※ To use fingerprints and QR, XScan must be purchased separately.

Chapter 5

Settings

01	Network	45
02	Application	46
	Access / TnA	46
	Meal	47
	Function Key	47
03	System	48
	System	48
	Face	48
	Auth	50
	UBio-Core	50
	Date / Time	53
	Database	53
	Finger	55
04	Terminal	56
	Sound	56
	LCD Option	57
	Input	59
	Lock	60
	External Device	61
	ETC. (Thermal)	62
05	Display	63
	Camera	63
	Language	64
	Option	64
	Message display Time	65
06	Info	65
07	USB	68

Field	Value
IP address	192.168.0.3
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
DNS	168.126.63.1
Server IP	192.168.0.2
DDNS	☐
Port	9870
Terminal ID	1

Selecting **[Network]** from the main menu displays the corresponding screen.

If you are using a static IP assigned within the connected network, choose **[Static IP]**. If the network has a DHCP server to allocate IP addresses, select **[DHCP]**.

In the case of **[Static IP]**, you need to configure the terminal's IP address, subnet mask, and gateway. If you have selected **[Dynamic IP]**, there is no need to configure these settings.

For **[Server IP Address]**, enter the IP address of the server. However, if you are using the DDNS provided by our company, check the DDNS option and enter the assigned information. If the terminal has 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'. If you decide to change this value, make sure to update the server program with the same value. Exercise caution when altering this setting to ensure compatibility with the server program.

[Terminal ID] : The authentication server utilizes a unique ID to distinguish terminals, with the default value being '1'. This ID must match the one registered in the server program and can be entered with a maximum of 9 digits.

When entering the item ends, start input by touching the [>] button or the next input. After typing, the keypad will disappear when you touch the rest of the screen, not the input screen.

AP Name	Selection
skkim_netis	☐
netis_cyj	☐
iptime-iddol	☐
netis	☐
iptime_SW_1	☐
UnionSW2B	☐
kth	☐
UNION_R&D1	☐
netis_wee	☐
test	☐

Wireless LAN

When you select the **[Wifi Enabled]** checkbox, you can view the results of scanning the surrounding AP (Access Point) list as shown in the image.

After selecting the desired AP to connect to, a password input window will appear. Once you correctly enter the password, you will be able to connect to that AP and use WiFi. Note that when the wireless LAN is enabled, using a static IP is not possible.

After completing the settings, press the **[Close]** button or **[BACK]** button to exit to the upper menu.

02 I Application

When you select [Application] from the main menu, the screen below will appear.
Choose the operational mode based on your intended purpose among [Access / TnA / Meal].

To apply the changes after modifying the settings, press the [Complete] button. If you wish to cancel and return to the upper menu, press the [BACK] button.

I Access / TnA

The screen that appears when you select [Application] → [Access] or [TnA] from the main menu.

BACK

APPLICATION

Application

F2

Function key

Access

TnA

Meal

Schedule

F1

00:00 ~ 00:00

F2

00:00 ~ 00:00

F3

00:00 ~ 00:00

F4

00:00 ~ 00:00

Access

00:00 ~ 00:00

Blocking Time(0~86400)

0

OK

BACK

APPLICATION

Application

F2

Function key

Access

TnA

Meal

Schedule

Attend

00:00 ~ 00:00

Leave

00:00 ~ 00:00

Out

00:00 ~ 00:00

In

00:00 ~ 00:00

Access

00:00 ~ 00:00

Blocking Time(0~86400)

0

OK

[Schedule(00:00~23:59)] : You can set the time for each authentication mode, and if not needed, set it as '00:00-00:00'.

[Blocking Time] : This feature prevents the same user from re-authenticating within the specified time. If set to 0, there is no restriction. However, if set to a value greater than 0, the user must wait for the specified time (in seconds) to elapse after a successful authentication before re-authenticating. You can set this value up to a maximum of 86,400 seconds (24 hours).

Precautions

- During the configured time periods, the system will always display in the set mode unless another function button is pressed. Even if you authenticate in a different mode by pressing another function button, the display mode will automatically switch to the configured authentication mode after the authentication is completed. This is convenient for attendance management.
- Each time period must be configured not to overlap. If there is an overlap, the modes will be determined in the order of configuration: Clock In (F1) -> Clock Out (F2) -> Go Out (F3) -> Return (F4) -> Access.
- If a time range is set as 23:00~01:00, it means from 23:00 until 01:00 the next day.

I Meal

The screen that appears when you select [Application] -> [Meal] from the main menu.

You can set the time periods for each meal type, and if not needed, set it as '00:00-00:00'.

[Allow Duplication]

- If unchecked (☐), each user can authenticate for each meal type only once.
- If checked (☒), users can authenticate multiple times regardless of previous authentications.

I Function Key

The screen that appears when you select [Application] -> [Function Key] from the main menu.

Fn Key

[F1]~[F4] and [Access] buttons are used to change authentication modes such as Clock In/Out. Pressing a function button switches the authentication mode accordingly. Only the checked buttons are displayed on the default screen, so when using a terminal dedicated to Clock In or Clock Out, you can uncheck other function keys for ease of use.

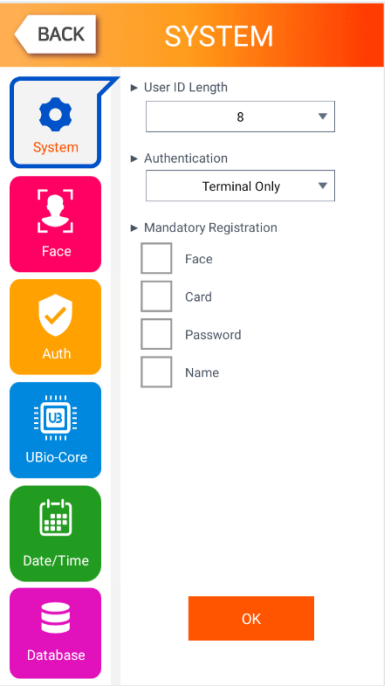
If you check the "Extended Key", you can add more authentication mode in addition to the default buttons.

※ If you are not using all the function keys, the access popup window at the bottom will not be displayed.

03 | System

I System

When you select [System] -> [System] from the main menu, the following screen will appear.



> **User ID Length**

This section allows you to set the length of the user ID, ranging from 2 to 8 characters. It must match the length of the ID registered in the server program. For example, if the ID registered in the server program is '000075' with a length of 6 characters, set it to 6.

> **Authentication**

An item determining the authentication priority between the terminal and the network server. It supports terminal-only and terminal/server hybrid modes.

[Terminal / Server] : If authentication fails for a user registered on the terminal, the system will attempt authentication with the server.

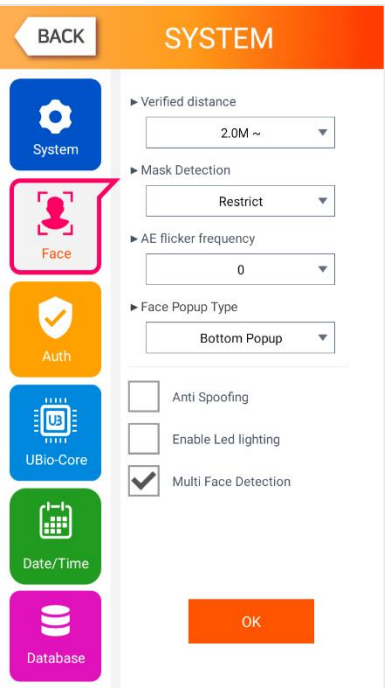
[Terminal Only] : Attempts authentication for a user registered on the terminal.

> **Mandatory Registration**

Setting the mandatory input items when registering a user. Checked items must be entered to register a user. The number of registered fingerprints is valid only when [Fingerprint] is checked, and when registering user fingerprints, you must enter at least the selected number of fingerprints or more.

To continue setting other items, press the button for the corresponding menu item on the left.

I Face



> **Verified distance**

* The authentication distance may vary depending on the size of the user's face.

- AntiSpoofing Enable/Disable: Set the authentication distance for different user heights (~0.6M, ~0.9M, ~1.2M, ~1.5M, ~1.7M, 2.0M~).

> **Mask Detection**

- None : Not checking for mask wearing.
- Guide : Provides guidance with yellow text (Not wearing/wearing improperly) and proceeds with authentication success.
- Guidance through text (Not wearing - red/Improper wearing - yellow) and handles authentication failure only when not wearing a mask.
- High-Restrict : Guidance with red text (Authentication failure).

* **Types of Guidance Messages**

Guidance Message	Motion detection
Please wear a mask	When not worn.
Please wear the mask properly.	In case of improper wearing (covering only the mouth).

> **AE flicker frequency**

- When installing the terminal indoors, if there is flickering in the camera image under specific lighting, setting this option to 50 or 60 can improve the symptoms.

> **Face Popup Type**

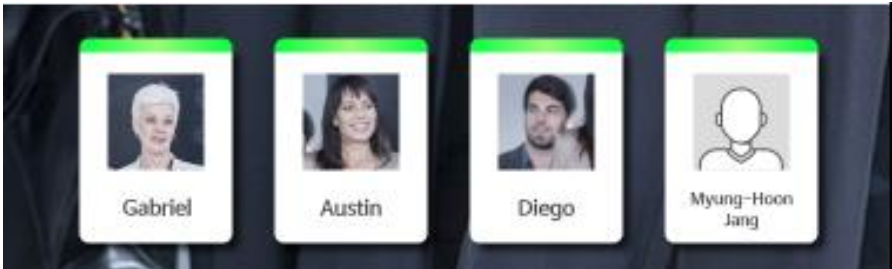
Popup types are applied for face authentication.

Precautions

- When using the Anti-Spoofing option or terminal cameras, regardless of the popup type, if authenticating with a card or fingerprint, the entire popup will be applied.

List Popup

When face authentication is performed, the authentication results are displayed in a list format. (However, it's important to note that when using the list popup type, the function key features are not available. Additionally, regardless of the user display option selection [ID/Name/Employee Number], the results will be displayed by ID.)



Bottom Popup

When face authentication is performed, the authentication results are displayed at the bottom of the terminal screen..



Full Popup

When face authentication is performed, the authentication results are displayed across the entire terminal screen.

> **Anti Spoofing**

Activates the counterfeit face detection feature.

> **Enable Led lighting**

If it is determined to be a low-light environment by the illuminance sensor, the Flash LED at the top is turned on to assist in face recognition and capture of face photo logs.

> **Multi Face Detection (Configurable when AntiSpoofing is disabled.)**

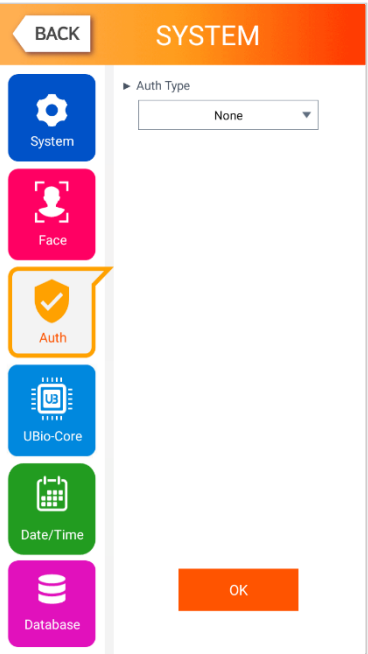
When the option is activated, multiple faces are detected. When the option is deactivated, only the face of the person closest to the terminal is detected.

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

If you press the [OK] button without changing the settings, it directly returns to the upper menu.

I Auth

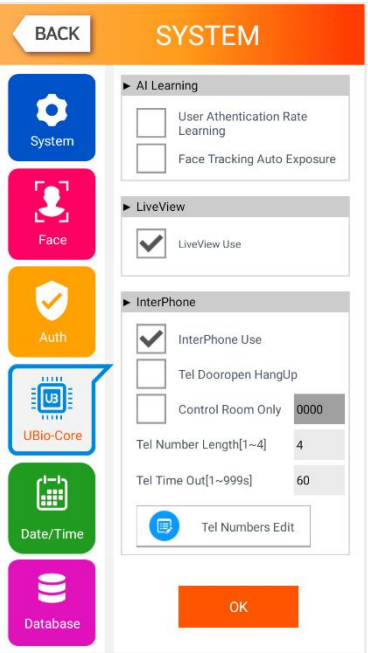
When you select [System] -> [Auth] from the main menu, the following screen will appear.



- > Auth Type : Selects the authentication method for the terminal.
- Card : Even if a user is registered with multiple authentication methods such as card, face, fingerprint, and password, when this option is selected on the terminal, authentication can be done with just the card. Users with fingerprint, face, or password need to authenticate using their respective authentication methods.
- FP : Even if a user is registered with multiple authentication methods such as card, face, fingerprint, and password, when this option is selected on the terminal, authentication can be done with just the fingerprint. Users with card, face, or password need to authenticate using their respective authentication methods.
- Face : Even if a user is registered with multiple authentication methods such as card, face, fingerprint, and password, when this option is selected on the terminal, authentication can be done with just the face. Users with card, fingerprint, or password need to authenticate using their respective authentication methods.

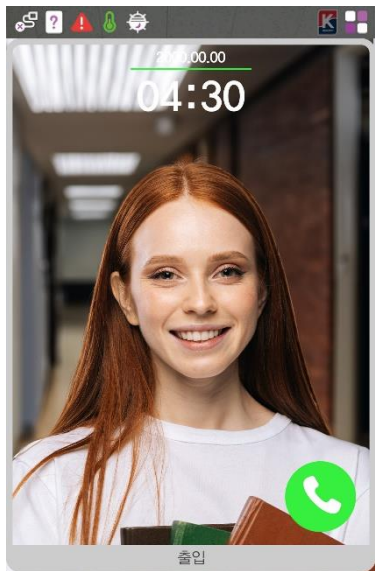
I UBio-Core

When you select [System] -> [UBio-Core] from the main menu, the following screen will appear.



- > **AI Learning**
 - User Authentication Rate Learning: A feature that displays an alarm popup to re-register a user if their average authentication rate drops.
 - Face Tracking Auto Exposure : Auto exposure operates by tracking the face.
- > **LiveView**
 - LiveView Use: The server can live-check the view illuminated on the terminal.
- > **InterPhone**
 - A feature that allows external visitors or individuals without a card to request entry and, in such cases, the internal control room or staff can be contacted via voice call to remotely open the entry door.
 - InterPhone Use : This function is used for voice calls during checks, and the sub-functions can be utilized.
 - Tel Dooropen HangUp: Setting to automatically end the call if the door opens successfully when attempting to open the door via VMonitor.

- Control Room Only : A feature that attempts to directly connect to the control room's call number when the phone button on the screen is pressed.
- Tel Number Length [1~4] : Setting for the number of digits in the phone number to be called (choose from 1 to 4 digits).
- Tel Time Out [1~999s] : Setting for how many seconds to forcibly disconnect the call after entering the phone number to be called.



> Intercom

- Enables the intercom feature on the device that is connected to the server.

Enabling the intercom feature allows you to use the intercom feature with users who have the Video Intercom program installed. - Every 1 minute, the intercom information (extension number) set in the video intercom program is synchronized with the terminal and displayed in the terminal phone number list.

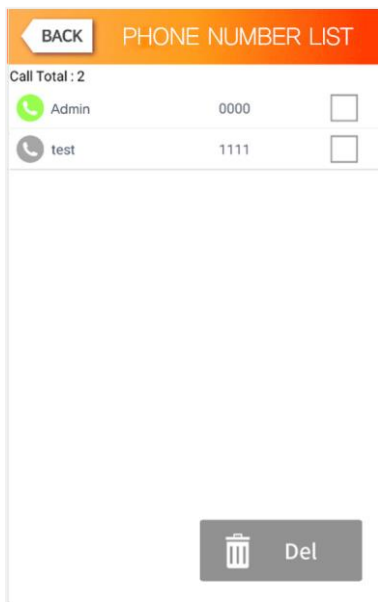
- Use intercom: Checked to use for voice calls, sub-functions are available.

- Hang up when door is opened: Set whether to automatically hang up when the door is opened normally when VMonitor tries to open the door.

- Control room only: When the call button is pressed on the screen, it immediately attempts to dial the control room call number.

- Call duration [5~999s]: You can specify the intercom call duration from a minimum of 5 seconds to a maximum of 999 seconds. The default value is 60 seconds. On door opening If the hang up feature is disabled, the call will remain connected after the door is opened for the set call duration after the door is opened.

When using the intercom feature, 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 (if checked for the management room only) the call is connected immediately.



> Phone number Edit

You can see which extensions are connected to the video intercom program and available for calls, and which extensions are disconnected and unavailable for calls. You can select and delete extensions that are no longer in use



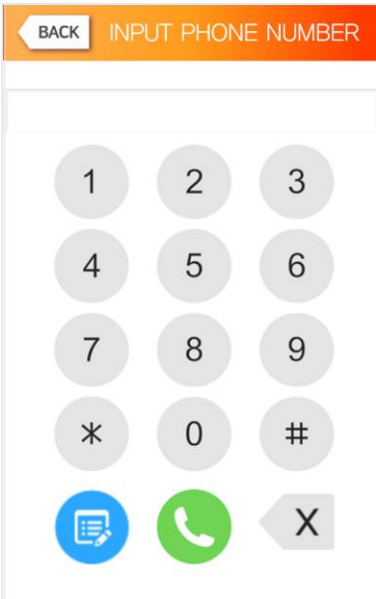
: The phone number where VMonitor can currently be reached



: The phone number where Vmonitor currently cannot be reached



: Select the list you want to delete from the phone list and use it to delete it.



> Input Phone number

When you touch the intercom button on the main screen, you will be taken to the phone number entry screen.



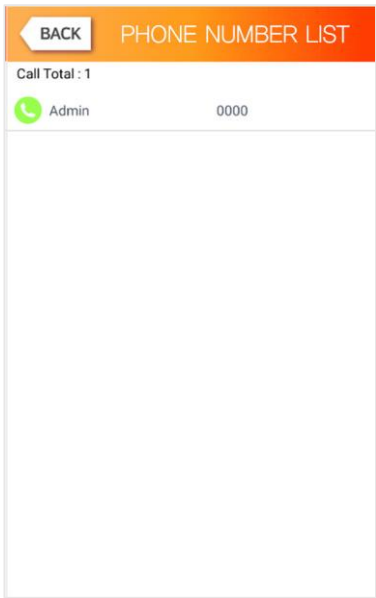
: Move to the phone number list screen



: Request Intercom with entered phone number.



: Delete the number you entered by one digit

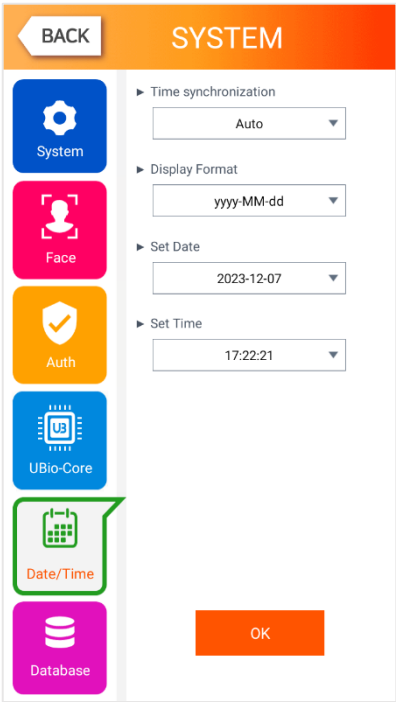


> Phone number list

You can see which extensions are automatically synchronized. Select an extension then it will be automatically dialed, and when you press the call button, it will try to connect the call.

I Date / Time

When you select [System] -> [Date/Time] from the main menu, the following screen will appear.



- > Time synchronization

This setting determines how to synchronize the current time of the terminal with the server. To synchronize automatically with the server time, choose [Auto]; to do it manually, choose [Manual].
- > Display Format

This setting determines how the current time on the terminal is displayed:

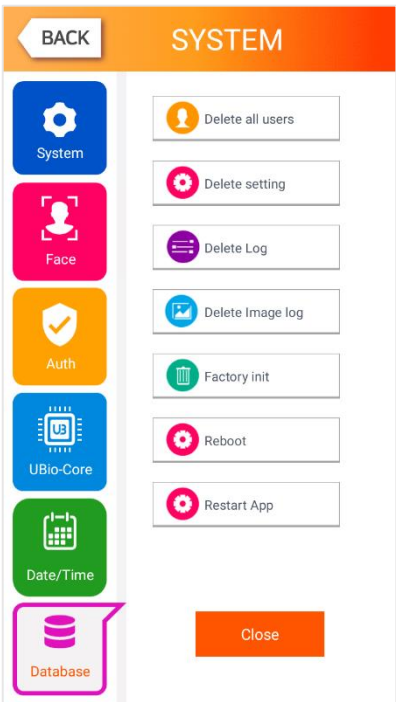
 - yyyy-mm-dd : Displays in the order of year, month, day.
 - dd-mm-yyyy : Displays in the order of day, month (in English), year.
- > Set Date / Set Time

Changes the current time on the terminal. If the server is connected and [Time synchronization] above is set to [Auto], there is no need to change it as it will be synchronized with the server time.

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

I Database

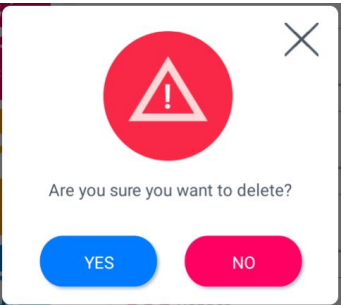
When you select [System] -> [Database] from the main menu, the following screen will appear.



Button	Motion detection
Delete all users	When deleting all users
Delete setting	When initializing settings
Delete Log	When resetting authentication records
Delete Image log	When deleting only the image log
Factory init	When deleting all data and resetting to factory default
BACK	When moving to the upper menu
Reboot	When rebooting the system
Restart App	When restarting the app

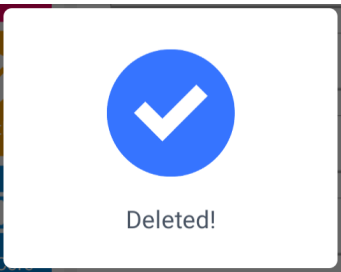
Delete all users

When you select [System] → [Database] → [Delete all users] in the main menu, the following screen will appear.



To delete all users, press the [Yes] button. To cancel, press the [No] or [X] button.

If there is no input within 5 seconds in this state, the deletion will be canceled, and the message box will disappear.



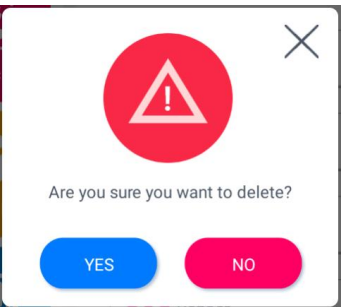
If you successfully press [Yes] to delete, the following success message box will appear.

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

< Figure 2 >

Delete setting

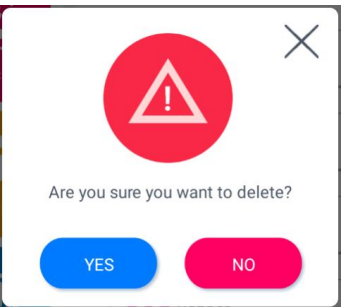
When you select [System] → [Database] → [Delete settings] in the main menu, the following screen will appear.



To delete all users, press the [Yes] button. To cancel press the [No] or [X] button.

If there is no input within 5 seconds in this state, the deletion will be canceled, and the message box will disappear.

If you click[Yes] button and successfully delete it, the success message in [Figure 2] will be displayed, and the display language and voice will be changed to their initial values in English. Initializes all settings on the device except for the Mac (physical) address and [fingerprint template format], but does not delete the user and authentication history.



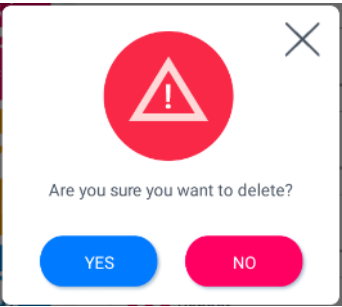
To delete all users, press the [Yes] button. To cancel, press the [No] or [X] button.

If there is no input within 5 seconds in this state, the deletion will be canceled, and the message box will disappear.

If you click Yes and delete it successfully, the success message in [Figure 2] will be displayed. Delete all authentication logs, including image logs, and after they are deleted, **recovery is not possible after deletion.**

Delete Image log

When you select [System] → [Database] → [Delete Image log] in the main menu, the following screen will appear.



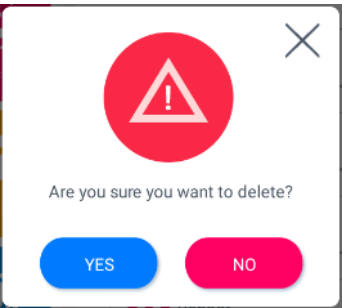
To delete all image logs stored on the terminal, press the [Yes] button. To cancel, press the [No] or [X] button.

If there is no input within 5 seconds in this state, the deletion will be canceled, and the message box will disappear.

If you successfully press [Yes] to delete, a success message, as shown in <Figure 2>, will be displayed. Only the images stored as logs will be deleted, and the authentication logs themselves will not be deleted.

Factory Init

When you select [System] → [Database] → [Factory Init] in the main menu, the following screen will appear.



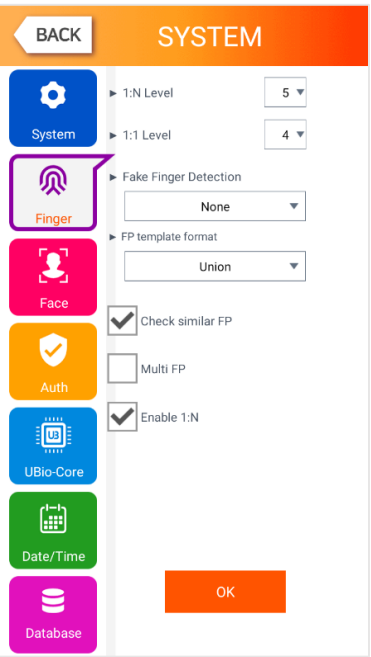
To reset the terminal to its factory default state, press the [Yes] button. To cancel, press the [No] or [X] button.

If there is no input within 5 seconds in this state, the reset will be canceled, and the message box will disappear.

If you successfully press [Yes] to reset, a success message, as shown in <Figure 2>, will be displayed. The display language and voice will be set to the default value, English. All settings, users, and log information stored on the terminal, except for the MAC (physical) address, will be deleted, restoring the terminal to its factory state. After the reset, **recovery is not possible, so exercise caution.**

I Finger * To register and authenticate fingerprints, you need to install XScan (optional).

When you select [System] → [Finger] in the main menu, the following screen appears.



> 1: N Level (3~9)

This is the authentication level used for 1:N fingerprint authentication. In the case of 1:N authentication, where individual user authentication levels are not set, it always follows the authentication level of the terminal.

> 1:1 Level (1~9)

This is the authentication level used for 1:1 fingerprint authentication. However, for users whose 1:1 authentication level is not set to '0' (using the terminal's authentication level), it follows the specified 1:1 authentication level for that user.

> Face Finger Detection

Set the Level of LFD (Live Finger Detection) to prevent spoof fingerprint input. The higher the LFD Level, the more robust the prevention of input from fake fingerprints made of materials such as rubber, paper, film, silicone, etc. However, extremely dry real fingerprints may not be detected well even during actual fingerprint input.

> FP template format (Changing fingerprint template format information results in the deletion of all existing users.)

Configure the format of the fingerprint template you want to use. When some applications using the SDK require a different format of fingerprint templates, you can change the fingerprint template format on the terminal. However, if you are using a server, you must **set the template format to match the one configured on the server**.

- Union: It is currently set to the default configuration, with a size of 400 bytes per template. This format is optimized for all fingerprint-related functions, including 1:1 level, 1:N level, authentication speed, and spoof fingerprint detection, providing the most accurate and fast authentication.
- ISO Standard: Fingerprint data is stored in ISO templates with a size of 500 bytes per template.

➤ Check similar FP

When checked (☒), this feature prevents the re-registration of the same fingerprint under a different user ID during fingerprint registration, ensuring that a fingerprint is not registered multiple times with different user IDs. The system checks for similar fingerprints against users who have the 1:N option enabled, with a limit of 50,000 fingerprints.

> Multi FP

When checked (☒), this feature requires entering the user ID (or card) and authenticating all registered fingerprints. Enabling this option automatically unchecks (☐) [Allow 1:N Matching], as it necessitates entering the user ID or card. This functionality is useful for strict access control in specific areas.

Ex) if a user with ID '0001' has three registered fingerprints, entering the ID requires authenticating all three fingerprints. The order of authenticating the three fingerprints doesn't matter, but all three must be successfully authenticated. If any one fails, the overall authentication fails.

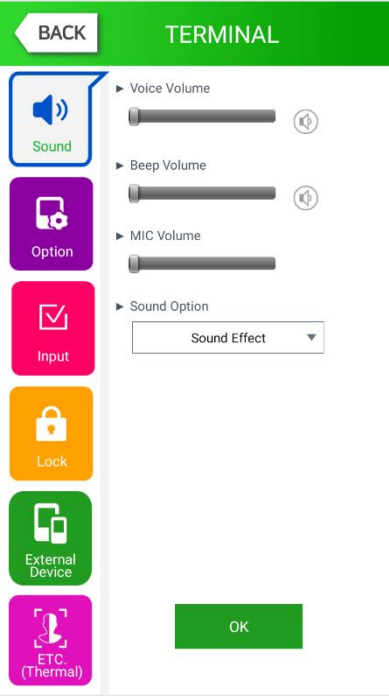
> Enable 1:N

When checked (☒), this option enables authentication using only fingerprints without requiring the entry of user ID or card. Even if a user is registered with 1:N matching allowed, when this option is unchecked, only 1:1 matching is possible on the terminal.

04 | Terminal

I Sound

When you select [Terminal] → [Sound] in the main menu, the following screen appears.

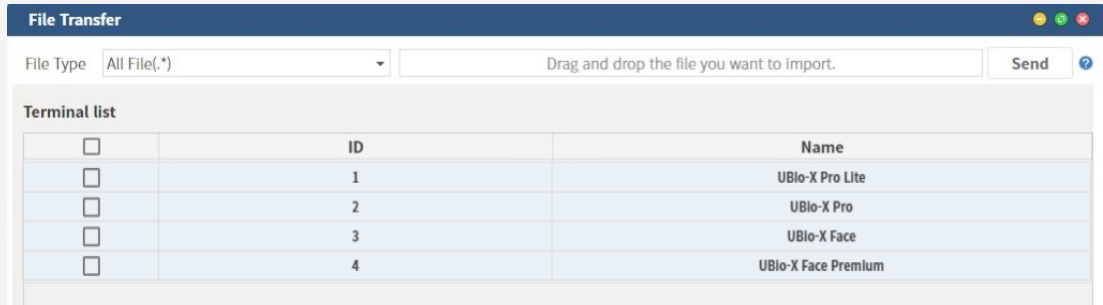


- > Voice Volume
Scroll left and right from 0 to 15 to set the voice volume. Press the [🔊] button on the right to play the voice and confirm the volume.
- > Beep Volume
Scroll left and right from 0 to 3 to set the buzzer volume. Press the [🔊] button on the right to trigger the buzzer and confirm the volume.
- > Sound Option
 - Sound Effect : A sound effect will play upon successful or failed authentication.
 - User Voice : The user's copied voice will play upon successful or failed authentication.
 - Stored Voice : Pre-saved audio will play upon successful or failed authentication.

To apply the settings, press the [OK] button. To cancel and return to the previous menu, press the [BACK] button. If you want to continue configuring other items, press the corresponding menu button on the left.

Voice message change

When you select 'User File Transfer' in the program, the following window will appear.



Specify the file type as either 'Success Voice File (.wav)' or 'Failure Voice File (.wav),' select the voice file (.wav or .mp3), and press the 'Transfer' button. A terminal selection window will appear. After selecting the terminal in the terminal list window, press the 'Transfer' button again to send the file, and the download result will be displayed.

To revert from custom voice to the default voice, uncheck the 'Use Voice' option in [Terminal] -> [Sound].

- The filename must be within 15 characters, including the extension (15 bytes in English), and only mp3 files can be transmitted.
- You can also change the voice message in [USB] → [Theme].

I Option

When you select [Terminal] → [Option] from the main menu, the screen below will appear.

BACK

TERMINAL

Sound

Option

Input

Lock

External Device

ETC (Thermal)

Read Card number

Card format

Card reader

Ble Rssi

Ble TxPower

Lock terminal

Standard

Standard

3

2

☐

OK

- > Read Card Number
- On this screen, when you present the card, the card number will be displayed on the LCD. You can view the card number based on the settings by changing the [Card format] below.
- > Lock terminal
- If the [Server Program] is not used, there is a feature where administrators can directly set or release the lock on the terminal. When checked (☒), the system enters a locked state where no one can enter until the administrator releases the lock.
- > Card reader
- It will only recognize cards of the standard type.
- > Card format
- This configures the display method for card numbers. Since the card number varies according to the set values as shown below, it is essential to configure it during the initial installation. If it becomes necessary to change it during operation, you will need to re-register the cards.

RF Card Ex) Card Number(5byte) : 08h 01h 16h 1Dh D6h

Card format	Card Number	Display Method
Standard	02207638	Display as a (3+5)-digit decimal number [022(16h)+07638(1DD6h)]
Hexadecimal	0801161DD6	Display as a 10-digit hexadecimal number
10 Digit Decimal	0018226646	Display the last 4 bytes as a 10-digit decimal number (01161DD6h)
3,5 Digit Decimal	02207638	Same as [Standard]
6 Digit Hexadecimal	161DD6	Display the last 3 bytes as a 6-digit hexadecimal number

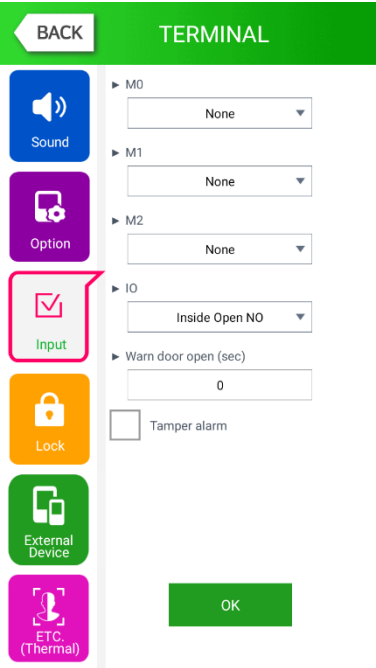
SC Card Ex) Card Number(4byte) : 52h 9Dh 06h E3h

Card format	Card Number	Display Method
Standard	529D06E3	Display as an 8-digit hexadecimal number
Hexadecimal	E3069D52	Display as an 8-digit hexadecimal number with reversed byte order
10 Digit Decimal	1386022627	Display the hexadecimal number 529D06E3 as a 10-digit decimal number
3,5 Digit Decimal	3808861522	Display the hexadecimal number E3069D52 as a 10-digit decimal number
6 Digit Hexadecimal	069D52	The first 3 bytes are reversed in position.

- > Ble Rssi
- Adjusts the reception sensitivity of the BLE module. A higher value increases the recognition distance.
- > Ble TxPower
- Adjusts the RF output power of the BLE module. A higher value increases the recognition distance."
- To apply the settings, press the [OK] button. To cancel and return to the upper menu, press the [BACK] button.

I Input

When you select [Terminal] → [Input] from the main menu, the screen below will appear.



- > M0: When connecting external contacts to DM0, configure the settings. (When using the motor lock, set it to either [Door Open State NO] or [Door Open State NC])
 - Not in use: When nothing is connected.
 - Door Open State NO or Door Open State NC: When the door open state monitoring pin is 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 based on the state of the pin when detection occurs.
- > M1/M2: When connecting external contacts to DM1/DM2, configure the settings. (When using the motor lock, set it to either [Lock Locked State NO] or [Lock Locked State NC])
 - Not in use: When nothing is connected.

- Lock Locked State NO or Lock Locked State NC: When the lock locked state monitoring pin is 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 based on the state of the pin when detection occurs.

- > IO: When connecting external contacts to the Exit pin, configure the settings.
 - Not in use: When nothing is connected.
 - Inside Open NO or Inside Open NC: When the Exit button is 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 based on the state of the pin when detection occurs.

> Door Open Warning Time (in seconds)

This feature checks the time the door is open using the terminal and, if it remains open for a duration exceeding the set time (0 or a minimum of 5 seconds to a maximum of 60 seconds), activates an alert sound. Setting it to [0] disables the alert sound entirely, and even if it is set to [01~04], the alert sound will only start after a minimum of 5 seconds has passed.

If the door does not close within the set time but should close within that time, an alert sound will be triggered. This serves as a notification that the door has not closed as intended, allowing for appropriate measures to ensure that the door closes properly.

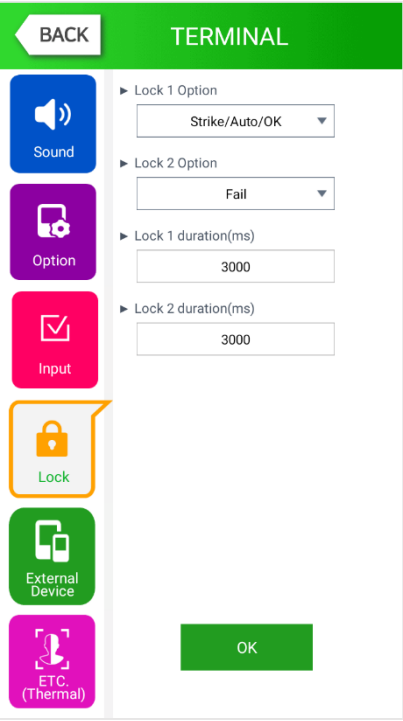
To use this feature, the lock must be monitored to determine whether it is currently open or closed. The monitoring pin of the lock must also be connected to M0. Additionally, the M0 setting should be [Door Open State NO] or [Door Open State NC].

> Terminal Disassembly Warning Sound

When checked (☒), an alert sound will be triggered if the terminal is disassembled.

I Lock

When you select [Terminal] → [Lock] from the main menu, the screen below will appear..



Lock1 Option

- None: When not in use.
- Strike / Auto / Authentication Success Notification: When connected to Lock1 with a strike type, automatic door, or a beacon for indicating authentication success/failure.
- Motor Lock 1: When connected to Motor Lock.
- Schedule alarm: When the server sends a siren setting for the terminal option, it sends an operation signal.
- Duress: When authenticated with a coercion fingerprint.

Lock2 Option

- None: When not in use.
- Authentication Failure Notification: When connected to Lock2 with a beacon for indicating authentication failure.
- Motor Lock 2: When connected to Motor Lock.
- Schedule alarm: When the server sends a siren setting for the terminal option, it sends an operation signal.
- Duress: When authenticated with a coercion fingerprint.

> Lock 1 duration (ms)

When Lock 1 is set to 'Strike / Auto / Authentication Success Notification,' specify the signal duration time. Since it is set in milliseconds, if you want to set it to 3 seconds, you should set it to 3000. The strike type indicates the time until the door is locked again after opening it following authentication.

> Lock 2 duration (ms)

When Lock 2 is set to 'Authentication Failure Notification,' specify the signal duration time. Since it is set in milliseconds, if you want to set it to 3 seconds, you should set it to 3000.

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

I External Device

When you select **[Terminal]** → **[External Device]** from the main menu, the screen below will appear.

The screenshot shows the 'EXTERNAL DEVICE' configuration screen. It features a green header bar with a 'BACK' button and the title 'TERMINAL'. A sidebar on the left contains icons for various settings: Sound, Option, Input, Lock, External Device (which is highlighted with a green border), and ETC (Thermal). The main content area is divided into sections for different communication protocols: RS232 (set to 'QR Card'), RS485 (set to 'None'), Wiegand (with 'Site Code' set to '0', 'Wiegand Output' set to 'None', and 'Wiegand Input' set to 'None'), and External Reader (set to 'None'). An 'OK' button is located at the bottom right of the main content area.

- > RS232 : Configure the device connected to the RS232 port
 - None: When no device is connected to the RS232 port.
 - Ticket Output 1 / Ticket Output 2: Prints authentication results on the printer upon successful authentication. The terminal ID, user ID, authentication time, authentication mode, etc., are printed on the printer connected to the RS232 port. The print format may vary based on the settings. When set to [Ticket Output 2], the "Text for Ticket Printer" configured in the server's terminal options is printed as the top title. The printer used for ticket printing is the "SRP-350" Serial model.
 - QR Card: Allows the use of QR codes as authentication cards, similar to standard authentication cards. Up to 24 characters are supported.
- > RS485 : Configure the device connected to the RS485 port
 - None: When no device is connected to the RS485 port.
 - LC010: When LC010 is connected.
 - LC015: When LC015 is connected.
 - Replay I/O: When connected to an elevator controller.
 - OSDP: When connected to a controller that supports OSDP.
 - Note: (When using LC010, LC015, if DM0 is set to [Door Open State NO] or [Door Open State NC], DM0 will receive door open state inputs. If the controller wants to receive door open state inputs, DM0 should not be configured.)

> Site cord
Set the Site code value transmitted during Wiegand Output.

> Wiegand Output
This is only used when a separate controller operated by Wiegand input is installed. After authentication is completed, the terminal's Wiegand port transmits data in the following format:

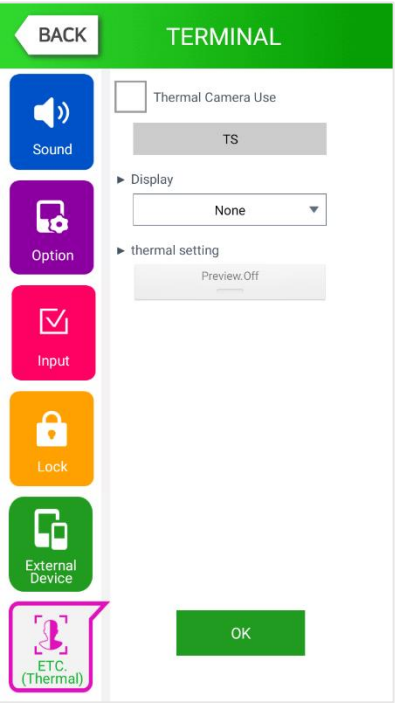
Not in use	In typical cases, the Wiegand Out port is not used.
26bit	Since it transmits 'Sitecode[1 byte] + User ID[2 bytes],' set the User ID to be 4 digits or less. Example of transmission: SiteCode: 045 (2Dh), UID: 6543 (198Fh) → 1 00101101 0001 1001 10001111 0
34bit	Since it transmits 'Sitecode[1 byte] + User ID[3 bytes],' set the User ID to be 7 digits or less. However, if the User ID is 8 digits, it ignores the Sitecode and transmits only 'User ID[4 bytes].' Example of transmission: SiteCode: 001 (1h), UID: 123456 (1E240h) → 0 00000001 00000001 11100010 01000000 0
User-defined	The settings based on user customization are only configurable by the server, and the terminal can only query the setting type.

- > External Reader
- This is used when a Wiegand reader is connected inside the access door where the terminal is installed.
- Not in use: When there is no card reader connected to the Wiegand port.
 - Wiegand Card: Cards input through Wiegand are considered as if they were read by a separate reader connected inside the access door. Users who use card-only authentication, regardless of other authentication methods such as face/ fingerprint/password and combination authentication, authenticate only with a card. Mask checks, door open checks, and photo logs are not performed.

To apply the settings, press the **[OK]** button. To cancel and return to the upper menu, press the **[BACK]** button.

I ETC. (Thermal)

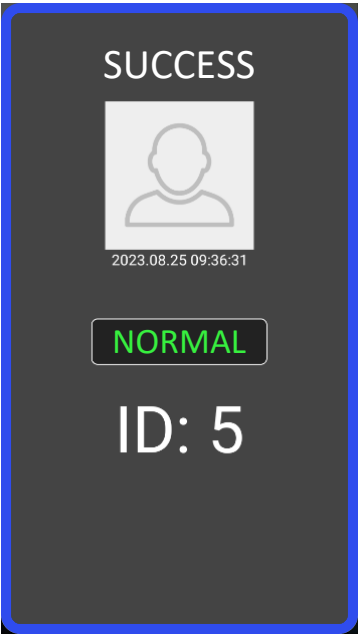
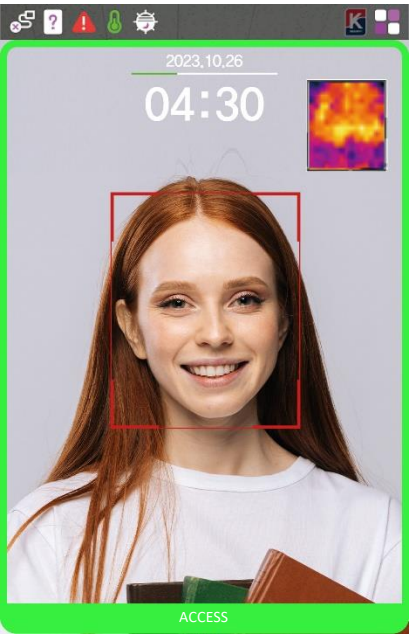
When you select [Terminal] → [ETC. (Thermal)] from the main menu, the screen below will appear.



- > Thermal Camera Use
If you check (☒), you can use a thermal imaging camera.
[TS (Terminal-i2)]
- > Display
You can choose between Celsius, Fahrenheit, or not displaying it.
* If you choose not to display, the authentication result window will show four options.

Auth Results	Info
LOW	If the temperature is below 30°C
HIGH	If the temperature exceeds 42°C
Success	If the temperature is 30°C or higher and below the set heating temperature
Failure	If the temperature exceeds the set heating temperature

- > Thermal setting
 - If you turn on the Preview button (☒ Preview.On), the thermal camera's preview video will be displayed in the top right corner of the main screen.



While the thermal check is in progress, you can view the preview video of the thermal camera in the top right corner.

This product is an additional device designed to screen for elevated skin temperature in a non-specific population.

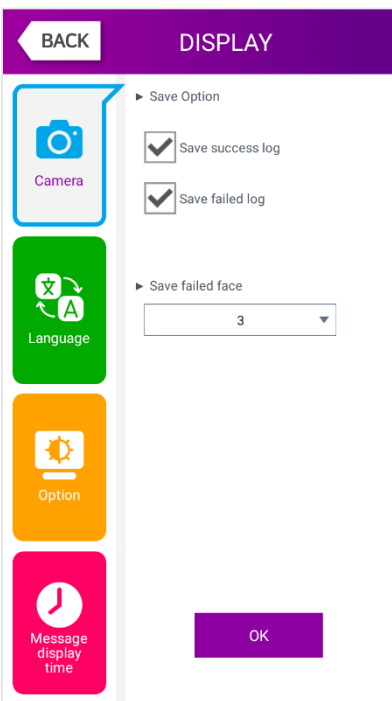
This device allows for a quick check to determine whether the skin surface temperature of the subject exceeds the normal skin surface temperature threshold. However, it cannot confirm diseases or viruses. Therefore, individuals screened in the first stage must undergo a secondary examination through medical devices, and appropriate follow-up measures should be taken.

1. It is recommended to operate the product with the sensor parallel to the face.
(A deviation of 1 degree may occur if the face position is not parallel.)
2. Deviations may occur depending on the type of lighting.
(Possible deviations in places with incandescent lamps, halogens, quartz tungsten halogens, etc.)
3. Obstructions or accessories covering the face may cause errors.
(Glasses, hats, covering the forehead with bangs, headbands, etc.)
4. Please move objects that can reflect infrared on the background facing the sensor of the product.
(Glass, mirrors, metal surfaces, etc.)
5. Errors may occur if there is air conditioning or cooling equipment in the installation location.
(Near air conditioning ventilation or near fans for building air conditioning.)
6. It is recommended to install and operate within the temperature range of 20 to 24 degrees Celsius and humidity range of 10% to 50%.
7. It is recommended to perform thermal detection for only one person at a time.
8. For accurate temperature measurement, it is recommended to use a black body along with the product.
9. Infrared cameras can be used after the algorithm is loaded.

05 I Display

I Camera

When you select [Display] → [Camera] from the main menu, the screen below will appear.



> Save success log

When checked(☒), if authentication is successful, the camera image is captured and saved as an image log.

> Save failed log

When checked(☒), if authentication fails, the camera image is captured and saved as an image log.

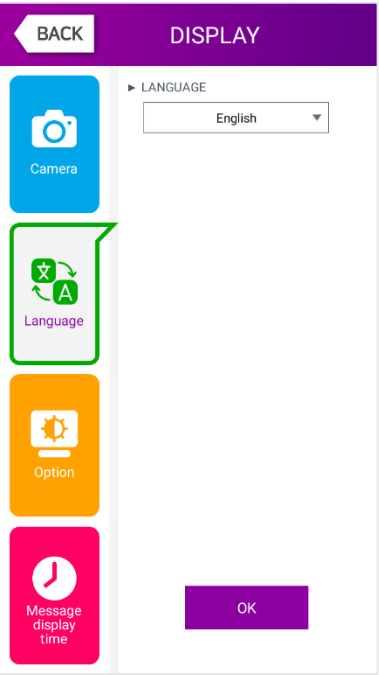
> Save failed face

0: Failure logs not saved, no popup for unregistered user authentication failure.

1-5: If an unregistered user stays in front of the camera for more than the specified seconds, failure logs are saved. A popup for unregistered user authentication failure is displayed.

I Language

When you select [Display] → [Language] from the main menu, the screen below will appear.

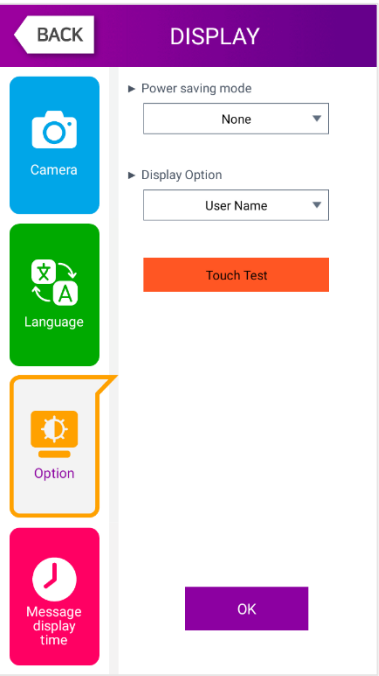


- > Default Setting: 'English'
- > Language
After changing the language, press the 'Done' button to switch the voice messages and on-screen messages to the selected language.

To cancel and return to the main menu, press the [BACK] button.
- ※ Supported Languages
English, Korean, Japanese, Portuguese, French, Spanish, Polish, Persian, German, Turkish, Vietnamese, Thai, Arabic, Chinese(Traditional)
- ※ For common languages, there may be parts expressed in English instead of the selected language.

I Option

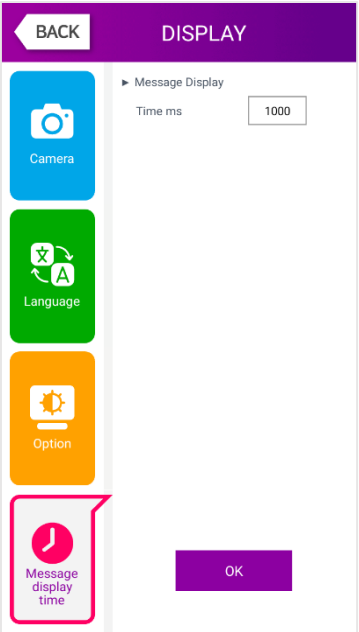
When you select [Display] → [Option] from the main menu, the screen below will appear.



- > Power Saving Mode Settings (5 seconds ~ 10 minutes)
If there is no input for the set duration, the LCD screen will automatically turn off. However, if set to 'Disabled,' the LCD will remain on at all times.
- > User Display Options
Configure the content to be displayed on the LCD screen upon successful authentication.
 - None: Displays only the authentication result [Success/Failure].
 - User ID
 - User Name: If not registered, displays the User ID (In this case, "ID:" is added for differentiation from the name).
 - Employee Number: If not registered, displays the User ID (In this case, "ID:" is added for differentiation from the employee number).
- > Touch Calibration
This function allows you to calibrate the coordinates of the touchscreen.

I Message display time

When you select **[Display]** → **[Message display time]** from the main menu, the screen below will appear.

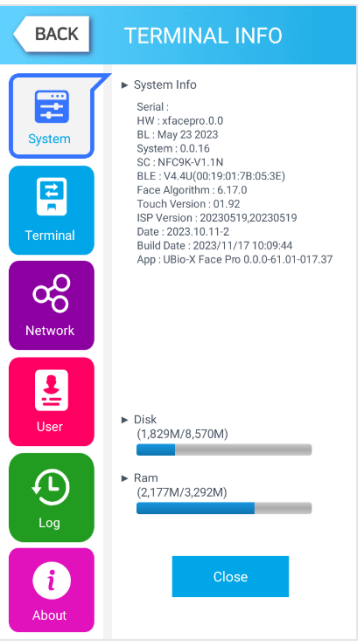


> Message Display (ms)

Sets the time for which the authentication result window will be displayed.

You can set it from 0 to 5000, and the authentication result window will appear and disappear after the configured time. Since it is in milliseconds, if you want to set it to 2 seconds, you would enter 2000.

06 I Info



System Info

> System Info

Displays the hardware and firmware version of the terminal device.

> Disk(Usage/Total)

Displays the usage of storage space. When the usage increases, it is indicated in red.

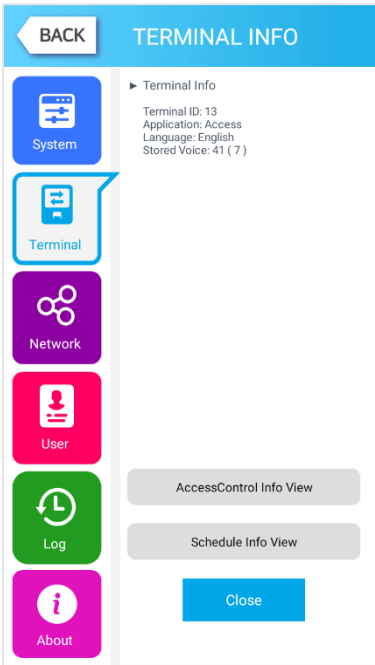
> Ram(Usage/Total)

Total RAM: Displays the amount of RAM that is in use.

If the memory usage increases, it is indicated in red.

To finish the inquiry and return to the main menu, press the **[BACK]** button.

If you wish to continue checking other items, press the corresponding menu item button on the left.



Terminal Info

> Terminal Info

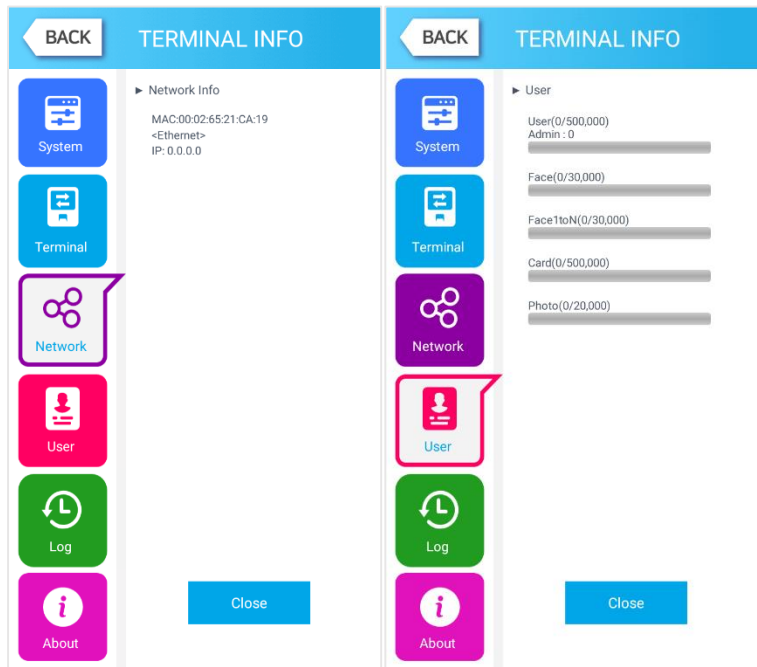
Displays the option settings of the terminal device.

- Viewing Access Group Information

Displays the access group information configured on the terminal device.

- Viewing Schedule Information

Displays the schedule information configured on the terminal device.



Network Info

> Network Info

Displays the network configuration settings of the terminal device.

User Info

> User Info

- User : The number of registered users.(Including administrators)
- Admin: The number of registered administrators.
- FP: The total number of registered fingerprints.
- FP1toN: The number of fingerprints capable of 1:N authentication.

- Face: The number of users with registered facial data.
- Face1toN: The number of users capable of 1:N facial authentication.
- Card: The number of registered cards.
- Photo: The number of users with registered photos.
(The maximum represents the maximum registration limit for each category).



Log Info

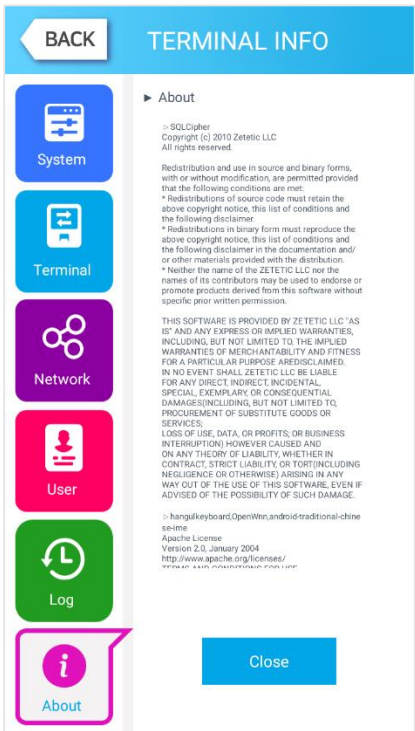
- > Log Info

Log: The number of logs stored on the terminal.
Image Log: The number of image logs stored on the terminal.
(The maximum represents the maximum storage limit for each category.)
- > View Log

Shows the log time and authentication status, starting from the most recent log.
- > Log Search

Press the **[Info]** → **[Log]** → **[View Log]** → **[Log Search]** buttons, set the start date, end date, event conditions, and press the **[OK]** button to search for logs.
- > Search result

The log search results include information such as date, time, ID, and access status (success or failure), allowing you to review the details.



About.

- > About

Displays the license information applied to the terminal device.
To finish the inquiry and return to the main menu, press the **[Close]** or **[BACK]** button.

> Export

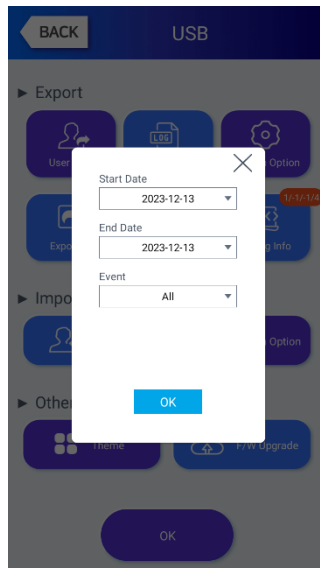
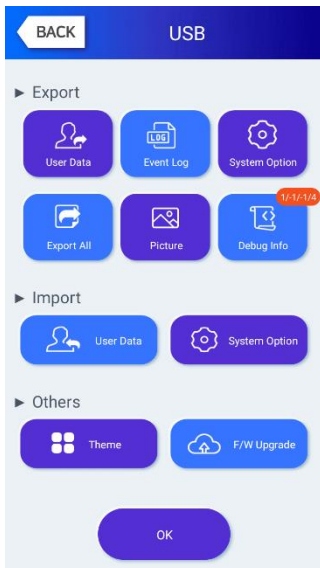
- User Data : Copies the user database to the 'unisuser' folder on the C-type USB.
- System Option : Copies the terminal's option settings to the 'UbioXfacePro/fconfig' folder.
- Event Log : Copies authentication logs to the 'UbioXfacePro/DeviceID(8 digits)/log' folder on the C-type USB. (Image logs are not copied.) You can specify a period to copy event logs.
- Debug Info : Exports terminal debugging information to the "Debug Info" folder.
- Picture : Saves image logs as .jpg files in the 'UbioXfacePro/DeviceID (8 digits)/log/pictures' folder on the C-type USB.
- Export All : Copies user data, system options, event logs, and image logs to the corresponding folder on the C-type USB.

> Import

- User Data : Copies the user database saved on the C-type USB ('unisuser' folder) to the terminal.
- System Option : Copies the terminal's option settings saved on the C-type USB ('UbioXfacePro/fconfig' folder) to the terminal.

> Others

- Theme : Copies audio files from the 'UbioXfacePro/audio' folder on the C-type USB to the terminal. If you want to replace the authentication success (user_ok.mp3) and failure (user_fail.mp3) messages with custom user voices, specify the custom voices with the mentioned file names and copy them. To play custom voices, check the "Enable User Voice" option in [3.7.1. Sound].
- F/W Upgrade : Upgrades firmware from the C-type USB. (The firmware should be located in the 'UbioXfacePro' folder on the C-type USB.)



<Figure 3>

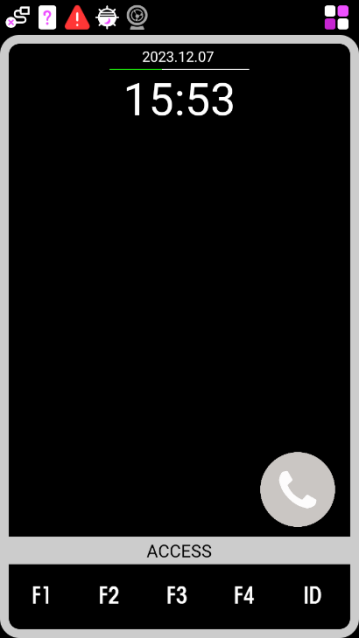
- ※ This operation is only possible when a C-type USB is inserted, and it should be inserted with the back facing forward, as shown in the <Figure 3>. (C-type USBs with a size of 32GB or less can be used.)
- ※ This function is used to back up the data of the terminal through [**Export**], and you can copy the backed-up data back to the terminal through [**Import**].
- ※ If you have executed [**Import**], you need to reboot the terminal to apply the new database or settings.

Terminal Usage Instructions

01	Change Authentication Mode	70
02	ID Input	70
03	Authentication	71
	Face	71
	Finger	71
	Card	72
	QR Code	72
	Password	72
	Multi	72

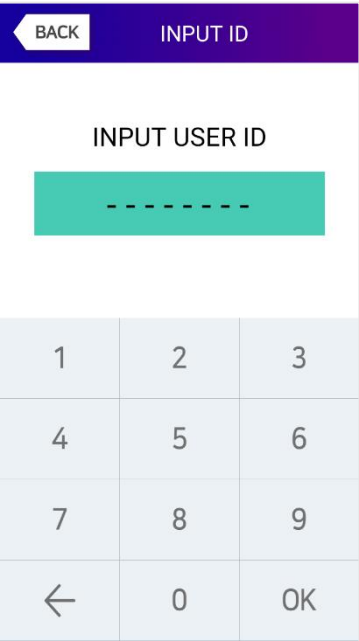
01 | Change Authentication Mode

The background image and layout of the default screen can be changed according to the administrator's settings. Additionally, if the administrator has set a screensaver time, the LCD screen will automatically turn off after the specified time without any activity on the terminal. When a user subsequently accesses the terminal, attempts authentication with fingerprint/card, or touches the main screen, the LCD screen will automatically activate.



To change the authentication mode, click on the screen to display the buttons for Clock In [F1], Clock Out [F2], Go Out [F3], and Return [F4]. Press the corresponding button to switch to the desired authentication mode.

02 | ID Input

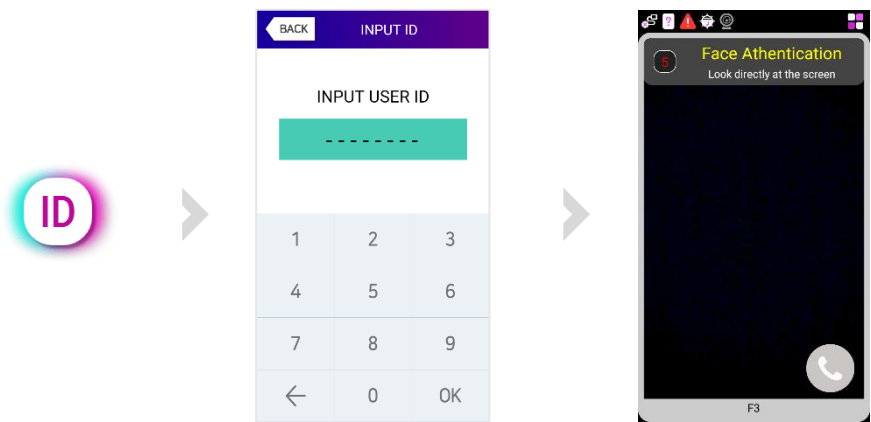


To enter the ID, click on the screen to display the **[ID]** button. Press the **[ID]** button, and the ID input window will appear as follows:

Enter the user's ID to authenticate, and after pressing the **[OK]** button, the authentication method screen will appear based on the user's authentication method, such as fingerprint input, face input, card input, or password input.

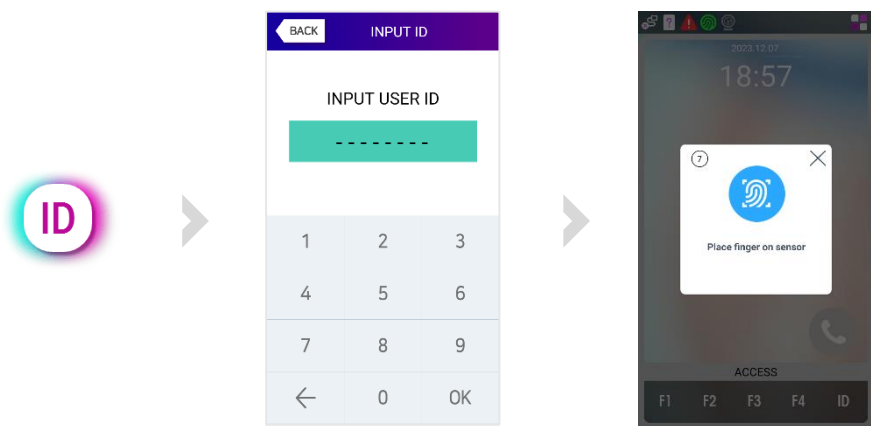
I Face

- > 1:N Authentication
Staring at the camera, attempt authentication for facial recognition, and the LCD screen will display your face for verification.
- > Enter ID and attempt authentication
Press the [Enter ID] button as shown below, and when you input the ID, the facial input message box changes to blue, displaying the message "Look straight at the screen."
Adjust the position of your face until the LCD guidelines turn blue, then gaze at the camera and momentarily stop any movement until it becomes blue.
If facial input fails, the message box will revert to gray after 20 seconds, and the 1:1 authentication will be canceled.



I Finger

- * To register and authenticate fingerprints, XScan (optional) must be installed..
- > 1:N Authentication
On the default screen, when you place your fingerprint on the fingerprint sensor, the buzzer will sound, the sensor light will turn on, and it will begin capturing the fingerprint. Do not remove your finger until the light on the fingerprint sensor is completely turned off.
- > Enter ID and attempt authentication
Press the [Enter ID] button as shown below, enter your ID first, and then the fingerprint input window will appear. Place your fingerprint on the sensor when the light is on. Do not remove your finger until the light on the fingerprint sensor is completely turned off and the fingerprint input window below disappears.



I Card

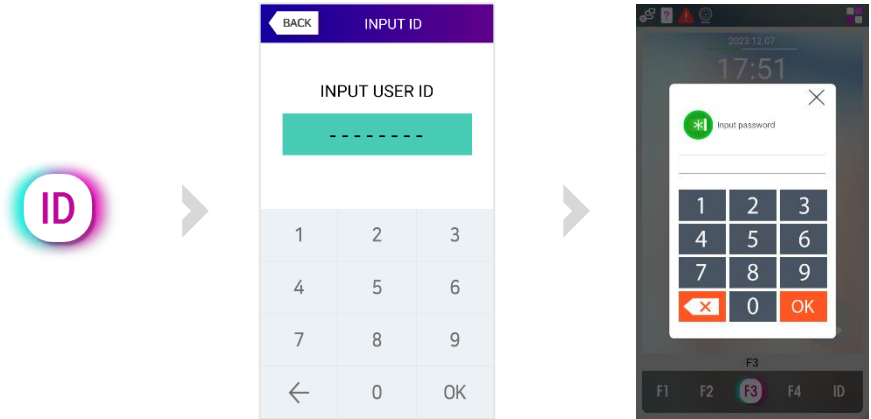
Place the card at the card authentication location on the terminal. (Refer to the terminal name illustration)

I QR Code* To register and authenticate fingerprints, XScan (optional) must be installed.

Place the QR code at the card authentication location on the terminal. (Refer to the terminal name illustration)

I Password

Press the [Enter ID] button as shown below, enter your ID first, and when the password input window appears, enter the password.



- > Coercive Password Authentication

Entering the registered password in reverse order during password input will result in successful authentication, similar to coercive fingerprint recognition. However, it will notify the administrator that it is an attempt at coercive authentication.

Ex 1) If the password is 1234, entering 4321 will result in coercive password authentication.

Ex 2) If the password is a consecutive number like 1111, it will not apply.

Ex 3) If the password is a symmetrical number like 1221, it will not apply.

Ex 4) If the password is a single-digit number like 1, it will not apply.

I Multi

- > If the authentication combination is "AND."

For users who need to authenticate using multiple methods (such as card & fingerprint, card & fingerprint & face, etc.), if the ID is entered first, the authentication priority is in the order of (card → fingerprint → face → password). It will still work even if face or fingerprint is authenticated first.
- > If the authentication combination is "OR."

If it is only a card or only a mobile card, it operates using the card method during 1:1 authentication. However, in the case of an OR condition that includes both card and mobile card, you cannot use both card and mobile card as authentication means during 1:1 authentication attempts.

※ If using a mobile card, only OR combinations are allowed.

FCC Compliance Information

Virdi / UBio-X Face Pro

This terminal complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
 (1) This device may not cause harmful interference.
 (2) This device must accept any interference received, including interference that may cause undesired operation.

UBio-X Face Pro

Have any questions?

- If you have any questions about the content of this product, please contact UNION biometrics.
- Our UNION biometrics team is available 24 hours a day to answer your calls.
- Share with us any questions or inconveniences you may have while using the service, then we will discuss this in detail and resolve them quickly.