

# UBio-X Slim(For Virdi)

## User Guide

---

Version Eng-2.3



**Union**  
biometrics

Copyright 2026 By Union Biometrics Co., LTD.

## <Revision History>

| Version | Date       | Description                                                                       | Firmware Version |
|---------|------------|-----------------------------------------------------------------------------------|------------------|
| 1.0     | 2020-04-21 | Release                                                                           |                  |
| 1.2     | 2021-10-18 | Delete DNS Content                                                                |                  |
| 1.3     | 2021-12-06 | Change Card Menu Description, Add Bluetooth Version                               |                  |
| 1.4     | 2021-12-20 | p.33 Card Content Revision, Addition of Alpeta Terminology                        |                  |
| 1.5     | 2021-12-29 | Menu Image Update, Firmware Download Content Revision                             |                  |
| 1.6     | 2022-08-25 | Addition of AIN2, Mobile Card Menu                                                |                  |
| 1.7     | 2023-06-15 | Addition of FN Update Menu                                                        |                  |
| 1.8     | 2023-08-25 | Addition of External Reader                                                       |                  |
| 1.9     | 2023-10-19 | Addition of LAN Cable Icon                                                        |                  |
| 2.0     | 2024-06-18 | Addition of Priority Input for Function Keys                                      |                  |
| 2.1     | 2024-07-29 | Addition of Guidance Message When Adding or Modifying Fingerprints After Deletion |                  |
| 2.2     | 2024-12-02 | Addition of WiFi Function                                                         |                  |
| 2.3     | 2025-02-04 | Addition of WiFi Icon and AP List Screen                                          |                  |

## < Glossary >

- Admin (Administrator)

- A user who can access the device's menu mode and has the authority to register, modify, or delete device users, as well as change operational settings to adjust the device's operating environment.
- If no administrator is registered on the device, anyone can access the device menu and change settings. Therefore, it is strongly recommended to register at least one administrator.
- Administrators have the authority to modify critical settings of the fingerprint device, so special care must be taken during their registration and management.

- 1 to 1, Verification

- A method in which a fingerprint is authenticated after entering the user ID or card.
- This is called 1:1 authentication, as only the fingerprint of the user registered with the user ID or card is compared.

- 1 to N, Identification

- A method that identifies the user using only a fingerprint.
- This is called 1:N authentication, as the system searches for a matching fingerprint among all registered fingerprints without requiring a user ID or card.

- Authentication Level

- The level used during fingerprint authentication, ranging from 1 to 9 based on the degree of fingerprint match. Authentication is successful only if the similarity between the two fingerprints meets or exceeds the set authentication level.
- A higher authentication level increases security, but since it requires a higher degree of fingerprint match, the likelihood of authentication failure for the rightful user also increases.
- 1:1 Authentication Level: The authentication level used during 1:1 authentication.
- 1:N Authentication Level: The authentication level used during 1:N authentication.

- LFD (Live Finger Detection): Fake Fingerprint Prevention Function

- A function that allows only real fingerprints to be recognized and prevents the use of fake fingerprints made from materials such as rubber, paper, film, or silicone

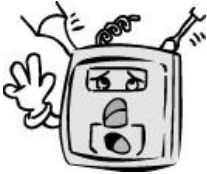
## Table of Contents

|                                                                      |    |
|----------------------------------------------------------------------|----|
| <Revision History> .....                                             | 2  |
| < Glossary > .....                                                   | 3  |
| 1. Before Use .....                                                  | 5  |
| 1.1. Safety Precautions .....                                        | 5  |
| 1.2. Terminal Component Names.....                                   | 7  |
| 1.3. LCD Screen Layout.....                                          | 8  |
| 1.4. Voice and Sound Effect Guidance During Operation .....          | 9  |
| 1.5. Proper Fingerprint Registration and Authentication Method ..... | 9  |
| 2. Product Overview .....                                            | 11 |
| 2.1. Product Features .....                                          | 11 |
| 2.2. System Diagram .....                                            | 11 |
| 2.3. Product Specifications .....                                    | 13 |
| 3. Environmental Settings .....                                      | 15 |
| 3.1. Pre-Check Before Environmental Settings .....                   | 15 |
| 3.2. Menu Structure .....                                            | 17 |
| 3.3. User .....                                                      | 21 |
| 3.4. Network .....                                                   | 26 |
| 3.5. Auth .....                                                      | 30 |
| 3.6. System.....                                                     | 38 |
| 3.7. Initialization.....                                             | 47 |
| 3.8. UI.....                                                         | 48 |
| 3.9. Information.....                                                | 52 |
| 3.10. USB.....                                                       | 59 |
| 4. How to Use the Terminal .....                                     | 64 |
| 4.1. How to open the door.....                                       | 64 |
| 4.2. How to authenticate in TNA Mode .....                           | 67 |

## 1. Before Use

### 1.1. Safety Precautions

- Warning

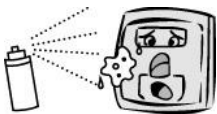
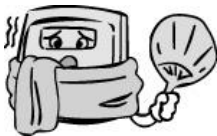
|                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Do not operate the terminal with wet hands or allow water or other liquids to enter the terminal.</p> <p>→ This may cause malfunction or electric shock.</p>  | <p>Do not place open flames or heat sources near the terminal.</p> <p>→ This may cause a fire.</p>                                       |
| <p>Do not disassemble, repair, or modify the terminal on your own.</p> <p>→ This may cause malfunction, electric shock, or fire.</p>                           | <p>Keep children from handling the terminal carelessly.</p> <p>→ There is a risk of injury to children or damage to the terminal.</p>  |

- Failure to follow the indicated precautions may result in death or serious injury.

- Caution

|                                                                                                                                                                                                                                      |                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Do not install the terminal in a location exposed to direct sunlight.</p> <p>→ This may cause malfunction, deformation, or discoloration.</p>  | <p>Do not install the terminal in areas with high humidity or excessive dust.</p> <p>→ This may cause malfunction.</p>  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## UBio-X Slim User Guide

|                                                                                                                                                                                                                                           |                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Do not clean the terminal by directly spraying water or wiping with benzene, thinner, alcohol, etc.<br/>→ This may cause electric shock or fire.</p>  | <p>Keep magnets away from the terminal.<br/>→ This may cause malfunction or damage.</p>                                     |
| <p>Do not dirty the fingerprint sensor.<br/>→ The terminal may fail to recognize fingerprints correctly.</p>                                             | <p>Do not spray insecticides or flammable sprays on the terminal.<br/>→ This may cause deformation or discoloration..</p>   |
| <p>Do not subject the terminal to impact or allow sharp objects to touch it.<br/>→ This may damage the product and cause malfunction.</p>              | <p>Do not install the terminal in locations with extreme temperature fluctuations.<br/>→ This may cause malfunction.</p>  |

- Failure to follow the indicated precautions may result in injury or property damage.
- We are not responsible for accidents or damage resulting from use that does not follow the instructions in this manual.

## 1.2. Terminal Component Names



### 1.3. LCD Screen Layout



#### 1.3.1 Status Icon

|                   |      |                                                         |
|-------------------|------|---------------------------------------------------------|
| Network           |      | : Standalone Mode                                       |
|                   |      | : Connected to Server Program                           |
|                   |      | : Not Connected to Server Program                       |
|                   |      | : LAN Cable Not Connected                               |
|                   |      | : WiFi Connected                                        |
|                   |      | : WiFi Not Connected                                    |
| Fire Detection    | None | : Normal                                                |
|                   |      | : Fire Detected (via External Device or Server Program) |
| Warning Indicator | None | : Normal                                                |
|                   |      | : Abnormal Terminal Status (Tamper Switch Activated)    |
| Door Status       |      | : Door Closed                                           |
|                   |      | : Door Open                                             |
|                   |      | : Door Not in Use                                       |
|                   |      | : Forced Door Open Warning                              |
|                   |      | : Door Open Time Elapsed Notification                   |

## 1.4. Voice and Sound Effect Guidance During Operation

| Operation Type                    | Voice Guidance Message   |
|-----------------------------------|--------------------------|
| When Authentication is Successful | You are authorized       |
| When Authentication Fails.        | Please try again         |
| Waiting for Fingerprint           | Please place your finger |
| Waiting for Card                  | Please place your card   |
| When Entering ID                  | Please insert your ID    |
| When Entering Password            | Please enter your ID     |

### 1.4.1 Beep or Sound Effects During Operation

|                       |                    |                                                    |
|-----------------------|--------------------|----------------------------------------------------|
| Beep + Error Tone     | In Case of Failure | When Authentication Fails and Voice is Disabled    |
| Beep + Ding Dong Tone | In Case of Success | When Authentication Succeeds and Voice is Disabled |

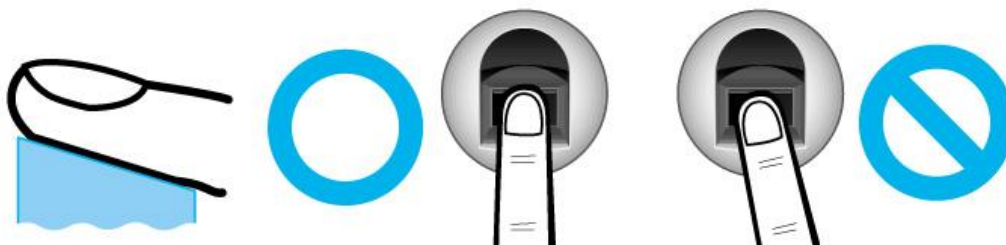
## 1.5. Proper Fingerprint Registration and Authentication Method

- Correct Fingerprint Input Method

Use your index finger and place it as if you are stamping your fingerprint.

Lightly touching the sensor with only the fingertip is not a correct method for registration or input.

Make sure the very center of your fingerprint touches the fingerprint sensor.



- Use the fingerprint of the index finger whenever possible.

Using the index finger ensures accurate and stable fingerprint input.

- Check whether the fingerprint is unclear or has any cuts or injuries.

Fingerprints that are excessively dry or moist, blurred, or have cuts or injuries are difficult to recognize.

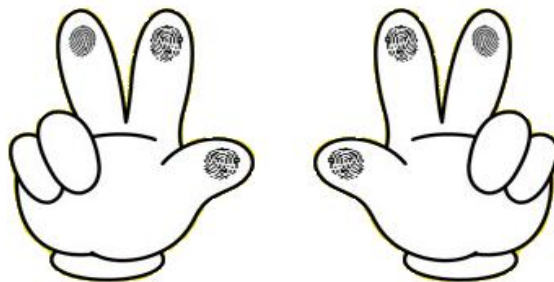
In such cases, register the fingerprint of another finger.



- **Precautions Based on Fingerprint Condition**

Depending on the condition of the user's fingerprint, fingerprint recognition may be unavailable or may function with reduced reliability.

- If the fingerprint is damaged or fragile, fingerprint authentication cannot be used, and card-based authentication must be used instead.
- **If the hands are dry, exhaling onto the finger can improve recognition performance.**
- For children, fingerprint recognition may be difficult or impossible if the fingerprints are too small or fragile. It is recommended to re-register fingerprints every six months.
- For elderly users, fingerprint registration may fail if the fingerprint has deep wrinkles.
- It is recommended to register at least two fingerprints per user whenever possible.
- To improve fingerprint recognition accuracy, it is recommended to use six fingers (both thumbs, index fingers, and middle fingers) as shown in the figure whenever possible.



## 2. Product Overview

### 2.1. Product Features

- A multi-modal authentication product that supports fingerprint, user card, or password.
- The built-in camera flash enables face detection in low-light environments.
- The ambient light sensor automatically activates the flash in low-light environments.
- RF (125 kHz) / Smart Card (13.56 MHz) (optional)
- Access control system using TCP/IP or Wi-Fi (optional) connected to the server database.
- Various registration and authentication methods

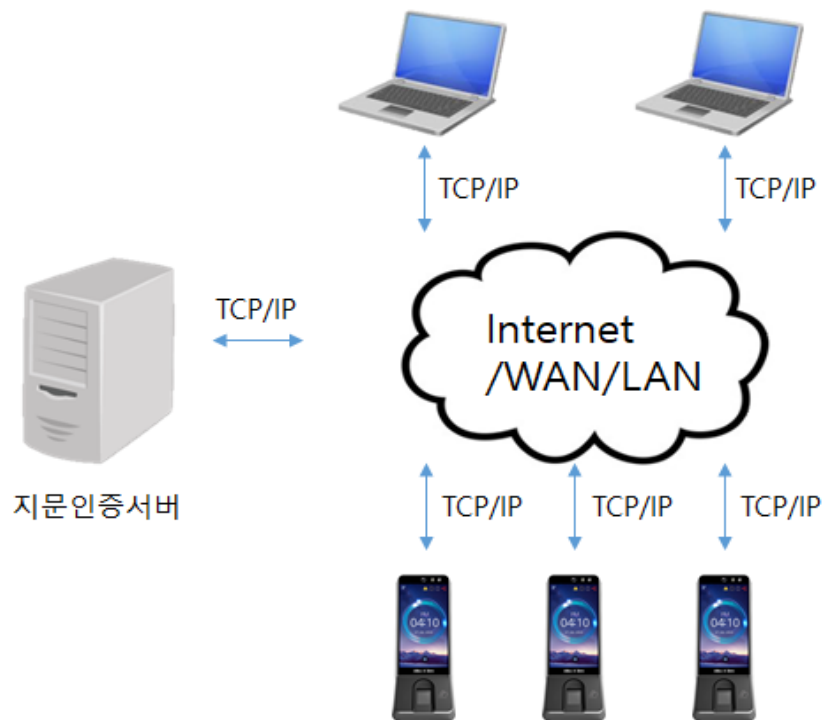
|                    |                                                                             |
|--------------------|-----------------------------------------------------------------------------|
| Fingerprint        | Fingerprint registration / Fingerprint authentication                       |
| Card               | Card registration / Card authentication                                     |
| Password           | Password registration / Password authentication                             |
| OR Authentication  | Successful if any one of the configured authentication methods is satisfied |
| AND Authentication | Successful only if all configured authentication methods are satisfied      |

### 2.2. System Diagram

#### 2.2.1. Standalone Use (Access Control)



2.2.2. Connected to PC Server (Access Control and Attendance)



## 2.3. Product Specifications

| Method                 | Specification                                                                          | Remarks                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| CPU                    | 1.4 GHz Quad-Core                                                                      |                                                                                                            |
| LCD                    | 4.95-inch Touch LCD (480 × 854)                                                        |                                                                                                            |
| Memory                 | eMMC 8 GB Flash                                                                        |                                                                                                            |
|                        | 2 GB RAM                                                                               |                                                                                                            |
| External USB Support   | Data backup / Firmware upgrade                                                         |                                                                                                            |
| Camera                 | Still color images (1600 × 1200)                                                       |                                                                                                            |
| Camera Flash Sensor    | Ambient light sensor, flash                                                            |                                                                                                            |
| Number of Users        | 500,000 users / 500,000 cards (Server: 200,000)<br>10,000,000 logs / 50,000 image logs | If the number of users exceeds 100,000 or logs exceed 100,000, the boot time may take more than 3 minutes. |
| Temperature / Humidity | -20°C ~ 60°C / Below 90% RH                                                            |                                                                                                            |
| AC / DC Adapter        | Input: Universal AC 100~250V                                                           |                                                                                                            |
|                        | Output: DC 12~24V, 3.5A                                                                |                                                                                                            |
|                        | Certifications: UL, CSA, CE                                                            |                                                                                                            |
| Lock Control           | EM, Strike, Motor Lock, Auto Door                                                      |                                                                                                            |
| I/O                    | 4 Inputs (1 Exit Button, 3 Monitor)<br>2 Outputs (Lock 1, Lock 2)                      |                                                                                                            |
| Communication Ports    | TCP/IP (10/100Mbps)                                                                    | Authentication Server Communication                                                                        |
|                        | RS-232                                                                                 | Meal Ticket Printer                                                                                        |
|                        | RS-485                                                                                 | Controller Communication                                                                                   |
|                        | Wiegand Input/Output                                                                   | Card Reader or Controller Communication                                                                    |

**UBio-X Slim User Guide**

|             |                                                                                                          |                  |
|-------------|----------------------------------------------------------------------------------------------------------|------------------|
| Card Reader | 125 kHz RF / 13.56 MHz Smart Card<br>HID 125 kHz Proximity Card (Optional)<br>HID iClass Card (Optional) | Optional         |
| Dimensions  | 80 × 195.6 × 23.5 mm (Normal)<br>/ 54.67 mm (Max)                                                        | Includes Bracket |

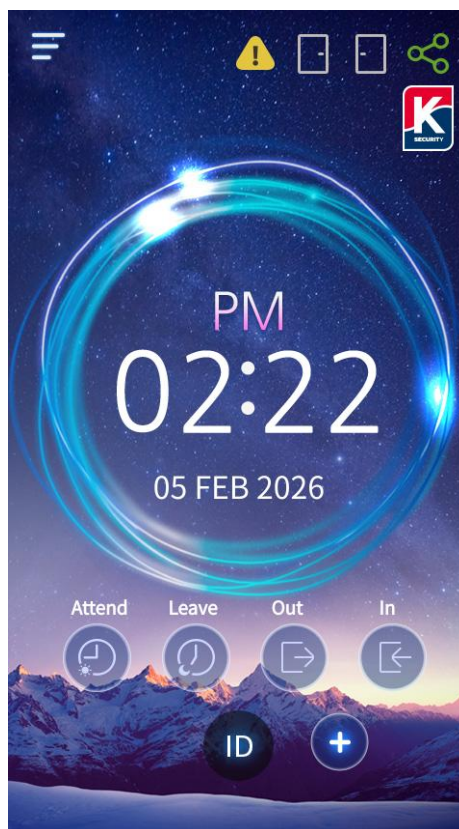
### 3. Environmental Settings

#### 3.1. Pre-Check Before Environmental Settings

##### 3.1.1. Enter Administrator Menu

- Terminal users are classified as either general users or administrators.

|               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| General User  | A user granted permission only to unlock the door                                             |
| Administrator | A user who can control the door and access all terminal functions through the management menu |



- To access the management menu, press the menu button at the top-left corner with your hand.

- On the ID input screen, enter the administrator ID and perform authentication according to the registered authentication method to access the management menu.

Since no users are registered at the time of product shipment, anyone can freely access the management menu.

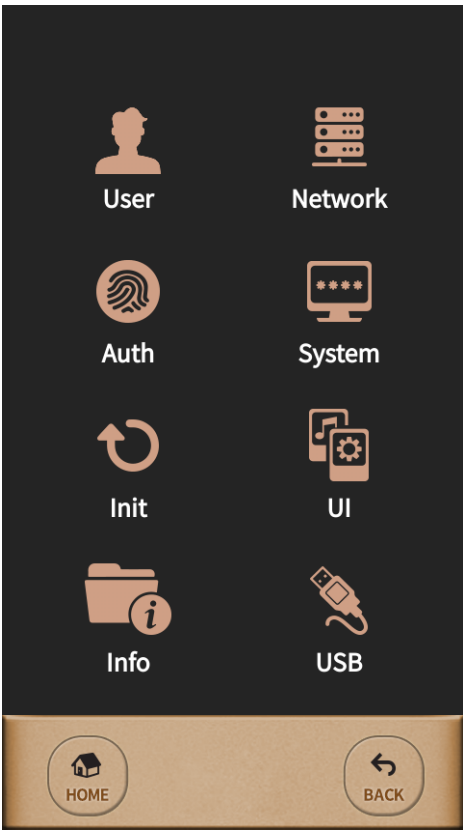
For security, at least one administrator must be registered.



1. In network mode, if only general users are registered without designating an administrator through the server management program, all users can access the management menu.
2. When using 1:N authentication, a registered administrator can access the management menu directly by fingerprint input without entering an ID.

3.2. Menu Structure

The management menu consists of seven sections, with the main functions as follows:



| Category | Subcategory | Description    | Default Value |
|----------|-------------|----------------|---------------|
| User     | Register    |                |               |
|          | Modify      |                |               |
|          | Delete      |                |               |
|          | List        |                |               |
|          | Delete All  |                |               |
| Network  | Basic       | Network Type   | Ethernet      |
|          |             | Terminal ID    | 1             |
|          |             | Server Address | 192.168.0.2   |
|          |             | Port Number    | 9870          |
|          |             | Ping Interval  | 10 seconds    |
|          |             | AP List        |               |
|          | TCP/IP      | Use DHCP       | Not Use       |
|          |             | IP Address     | 192.168.0.3   |

**UBio-X Slim User Guide**

|        |              |                          |               |
|--------|--------------|--------------------------|---------------|
|        |              | Subnet Mask              | 255.255.255.0 |
|        |              | Gateway                  | 192.168.0.1   |
| Auth   | Basic        | 1:1 Authentication Level | 4             |
|        |              | 1:N Authentication Level | 5             |
|        |              | Fingerprint 1:N Allowed  | USE           |
|        |              | Authentication Order     | Terminal Only |
|        | TNA          | TNA Mode                 | TNA           |
|        |              | F1                       | 00:00         |
|        |              | F2                       | 00:00         |
|        |              | F3                       | 00:00         |
|        |              | F4                       | 00:00         |
|        |              | Access                   | 00:00         |
|        | Meal         | Breakfast                | 00:00         |
|        |              | Lunch                    | 00:00         |
|        |              | Dinner                   | 00:00         |
|        |              | Late-Night Meal          | 00:00         |
|        |              | Snack                    | 00:00         |
|        |              | Allow Duplicates         | Not Use       |
|        | Log          |                          |               |
|        | Function Key | Function Key Mode        | Not Use       |
|        |              | Forced Function Key      | Not Use       |
| System | Sensor       | Capture Timeout          | 5 seconds     |
|        |              | LFD Accuracy             | Not Use       |
|        |              | Camera Usage             | Not Use       |
|        |              | Camera Flash             | 1             |
|        | Card         | Card Type                |               |
|        |              | Card Format              | Not Use       |
|        |              | Wiegand Type             | Card Number   |
|        |              | Transmission Data        |               |
|        |              | Site Code                | Not Use       |
|        |              | TOC (Template On Card)   | Not Use       |
|        |              | External Reader          |               |
|        |              | Card Read                | Door1         |
|        | Door         | Door Selection           | Door          |

**UBio-X Slim User Guide**

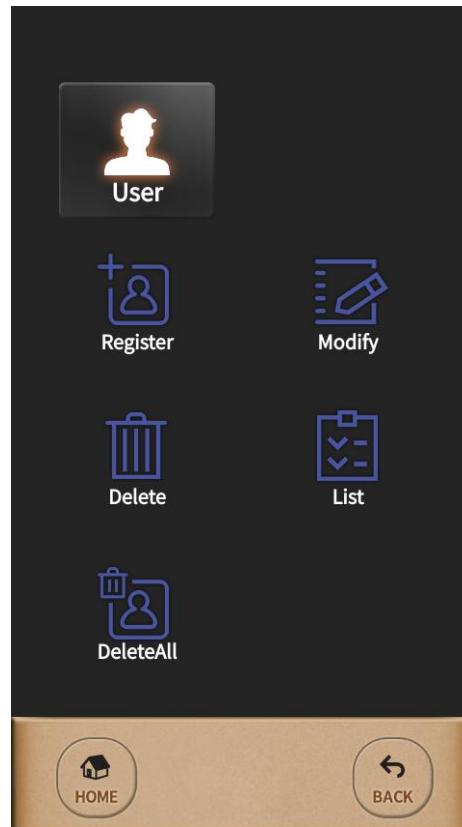
|                |               |                                 |               |
|----------------|---------------|---------------------------------|---------------|
|                |               | Door Function                   | Success       |
|                |               | Authentication Result Signal    | 5 seconds     |
|                |               | Lock Open Time                  | 20 seconds    |
|                |               | Door Warning Time               | Normal Close  |
|                |               | Door Control Type               | Not Use       |
|                | RS485         | RS-485 Type                     | 0             |
|                |               | RS-485 ID                       | 2             |
|                | Optional      | Number of Fingerprint Templates | 5 seconds     |
|                |               | ID Length                       | 4             |
|                |               | Log Storage                     | Yes           |
|                |               | Display User Name               | Yes           |
|                |               | Result Display Duration         | 1 Seconds     |
|                |               | Tamper Alarm                    | Mute          |
|                | Mobile Card   | BLE RSSI                        | 5             |
|                |               | BLE Power                       | 4             |
| Initialization | Delete User   |                                 |               |
|                | Delete Logs   |                                 |               |
|                | Reset Options |                                 |               |
|                | Restart       |                                 |               |
|                | Factory Reset |                                 |               |
|                | TnA Reset     |                                 |               |
| UI             | Sound         | Sound Type                      | Effect Only   |
|                |               | Volume                          | 1             |
|                | Display       | Language                        | English       |
|                |               | LCD Brightness                  | 3             |
|                |               | Main Display                    | Digital Clock |
|                |               | Idle Time                       | 3 Minutes     |
|                |               | Screensaver                     |               |
|                |               | Date                            | System Date   |
|                |               | Time                            | System Time   |
|                |               |                                 |               |
| Information    | Version       | Mac Address                     |               |
|                |               | App Version                     |               |
|                |               | Resource Version                |               |

**UBio-X Slim User Guide**

|     |                 |                                   |  |
|-----|-----------------|-----------------------------------|--|
|     |                 | Kernel Version                    |  |
|     |                 | Filesystem Version                |  |
|     |                 | Card Module Version               |  |
|     |                 | Compile Date                      |  |
|     |                 | Touch Sensor Version              |  |
|     | Option          | Terminal ID                       |  |
|     |                 | Attendance Mode                   |  |
|     |                 | Card Type                         |  |
|     |                 | Network Type                      |  |
|     |                 | IP Address                        |  |
|     |                 | Version (App, Kernel, Filesystem) |  |
|     | User            | Number of Administrators          |  |
|     |                 | Number of Users                   |  |
|     |                 | Number of Fingerprints            |  |
|     |                 | Number of Fingerprint 1:N         |  |
|     |                 | Number of Cards                   |  |
|     | Log             | Number of Transmitted Logs        |  |
|     |                 | Number of Untransmitted Logs      |  |
|     |                 | Number of Image Logs              |  |
|     |                 |                                   |  |
|     |                 |                                   |  |
| USB | User Download   |                                   |  |
|     | User Upload     |                                   |  |
|     | Log Download    |                                   |  |
|     | Firmware Update |                                   |  |
|     | FN Update       |                                   |  |

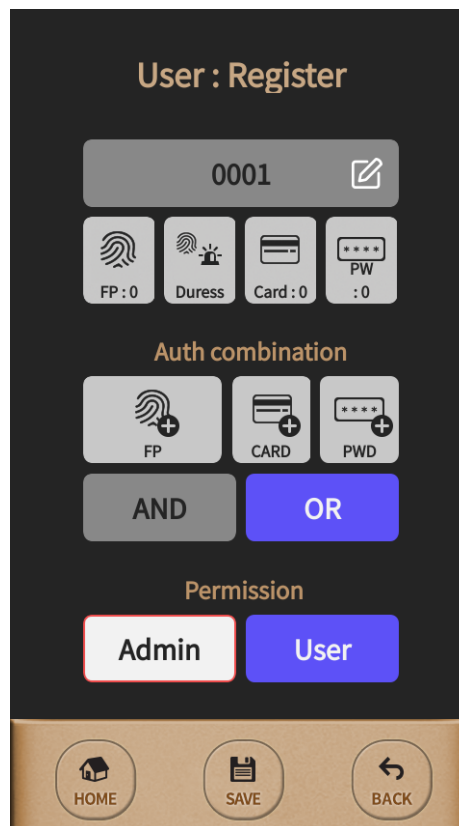
### 3.3. User

When **[User]** is selected from the main menu, the following window appears. Administrators can use the User menu to perform overall user management tasks, such as registering, deleting, modifying, and searching for users.



### 3.3.1. User Registration

- The maximum number of registrable users on the terminal is 200,000 fingerprint templates for fingerprint users, and up to 500,000 for RF card or password users. For example, if 200,000 fingerprint templates are registered for 10,000 users on the terminal, an additional 490,000 password or card users can be registered.



- To register a user, go to the Management Menu → **User** → press the **Register** button.
- Press the **"Enter ID"** button and enter the user ID you want to register.
- In the **Permissions** section, pressing the **Administrator** button changes the user's permission. Press the button to set the desired permission as either **General User** or **Administrator**.
- A **duress fingerprint** can be registered.

If a duress fingerprint is registered, authenticating with the registered duress fingerprint in an emergency situation will notify the server of the incident.



Administrators and general users are granted the following permissions:

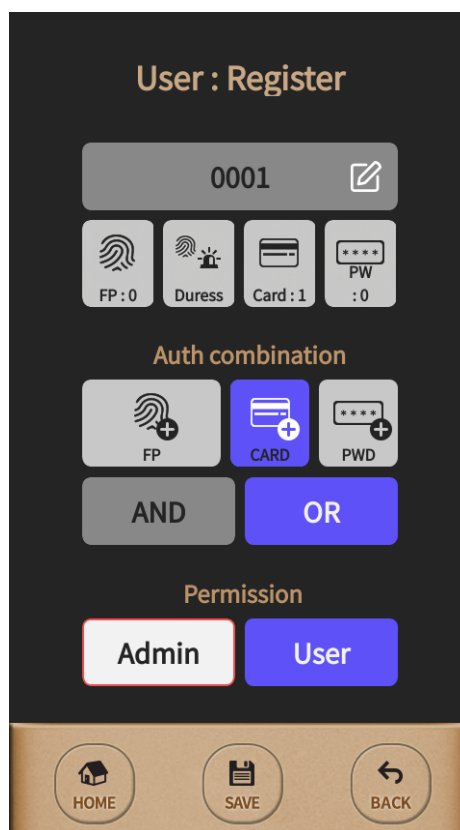
- **General User:** Door control only
- **Administrator:** Door control + access to the management menu

To complete user registration, at least one of the following authentication methods—fingerprint, password, or card—must be registered.

Register at least one of the authentication methods below, select the authentication combination method, and press the **“Save”** button to finish registering the user.

### 3.3.2. Modify User

- The user ID is a unique identifier and cannot be changed. Other information, such as fingerprints, duress fingerprints, cards, passwords, and authentication methods, can be freely modified in the **Modify User** menu.



- Press the **“Modify User”** button, enter the user ID you want to modify, and then press the **“Enter”** button to display the user’s registration information.
- Select the information you want to change—**Group**, **Permission**, or **Authentication Method**—modify the values, and then press the **“Save”** button to store the changes.
  - With OR authentication, a combination of any two methods among fingerprint, card, password, and mobile card is supported.



- ✓ For mobile card users, an **MC** icon appears next to the password image.  
If a mobile card is not used, the icon does not appear.  
Users with a mobile card cannot select the AND authentication combination.
- ✓ If you want to add or change a fingerprint after deleting an existing fingerprint in **Modify User**, first delete the existing fingerprint, press the **"Save"** button to store the changes, and then select **Modify User** again to add the new fingerprint.

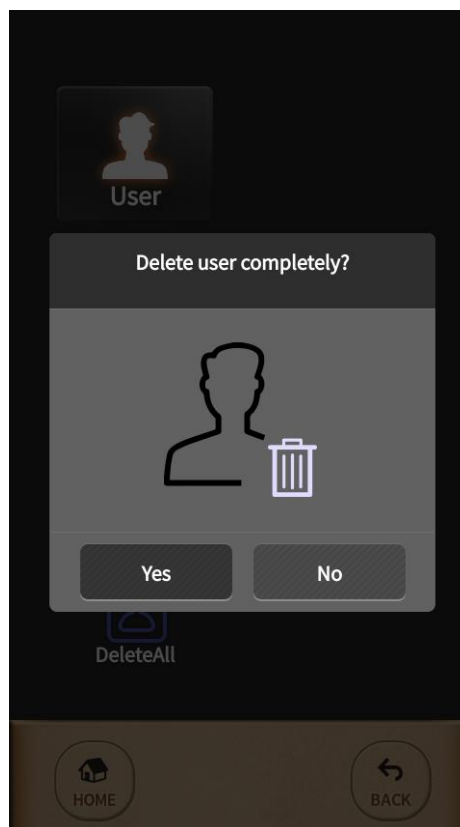
### 3.3.3. Delete User

Enter the user ID to delete and select the **[Yes]** button.

To cancel and return, select the **Close** button.

If an invalid or unregistered ID is entered, an error message will appear.

If a valid or already registered ID is entered, a confirmation window will appear as shown below.



#### 3.3.4. User List

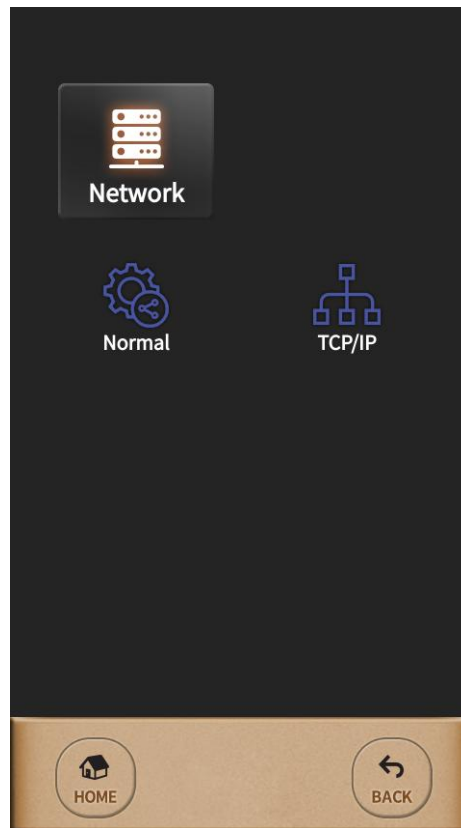
Registered users on the terminal can be searched using the **User List** and **User Verification** menus.

#### 3.3.5. Delete All Users

All users registered on the terminal can be deleted.

### 3.4. Network

When **[Network]** is selected from the main menu, the following window appears.



Network settings are divided into **Basic Settings** and **TCP/IP Settings**.

### 3.4.1. Basic

The UBio-X Slim terminal can operate in two modes: **Network Mode** and **Standalone Mode**. Network Mode is further divided into **Wired Network (Ethernet)** and **Wireless Network**.

The screenshot displays the 'Network : Normal' configuration interface. It features a dark background with white text. The title 'Network : Normal' is at the top. Below it, there are five rows of configuration fields: 'Type' with a dropdown menu showing 'Ethernet', 'Terminal ID' with a text box containing '1', 'Server Address' with a text box containing '17.17.17.2', 'Port Number' with a text box containing '9003', and 'Ping Period' with a text box containing '10'. At the bottom of the screen, there is a light-colored bar containing three circular buttons labeled 'HOME', 'SAVE', and 'BACK'.

- Network Type

The network type is divided into Not Use (Disabled), Ethernet (Wired Network), and Wi-Fi (Wireless Network).

When the network is set to Not Use, the terminal operates in Standalone Mode, functioning independently without connecting to a network.

In this case, authentication is performed by searching only the terminal's internal database. Ethernet and Wi-Fi are Network Modes, where the terminal is connected to the network and operates in conjunction with the UNIS and Alpeta programs.

- Terminal ID

The Terminal ID is a unique identifier for the device. Enter the desired ID within the range 1–99,999,999.

It cannot duplicate the ID of another terminal on the same server.

- Server Address

Enter the IP address of the server where UNIS or Alpeta is installed.

- Port Settings

Enter the port information used for communication between the server and the terminal.

- Ping Interval

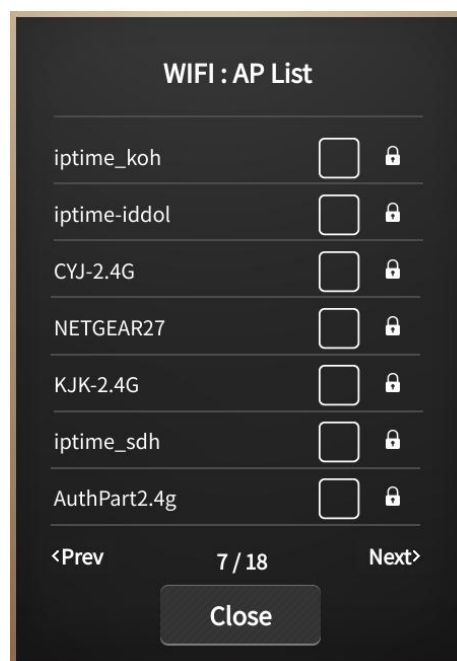
This function checks the communication status between the terminal and the server.

The default value is 10 seconds Ping.

- AP List

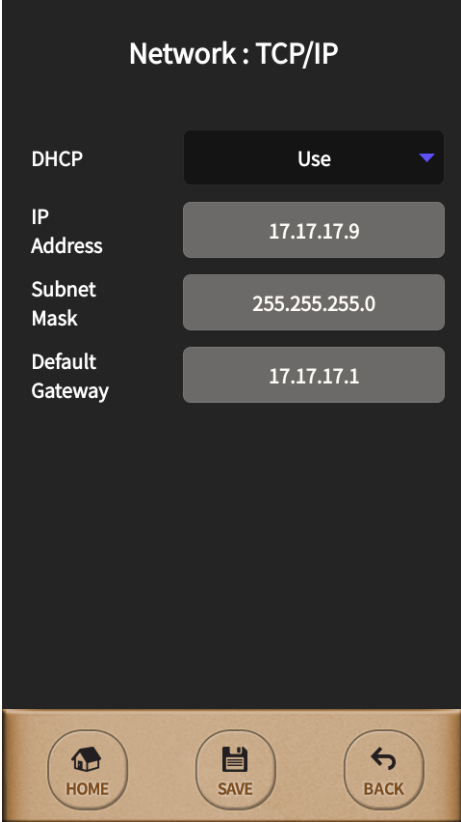
This menu appears when the network type is set to Wi-Fi (Wireless Network).

Select the Wi-Fi network you want to connect to from the displayed list.



### 3.4.2. TCP/IP

If the terminal is set to **Network Mode**, the **TCP/IP settings** must be completed to ensure proper connection with the server.



| Network : TCP/IP |               |
|------------------|---------------|
| DHCP             | Use ▼         |
| IP Address       | 17.17.17.9    |
| Subnet Mask      | 255.255.255.0 |
| Default Gateway  | 17.17.17.1    |

HOME SAVE BACK

- DHCP

In the menu, press the **“Use”** button to enable or disable DHCP.

If DHCP is enabled, the terminal automatically obtains its IP address, which cannot be changed manually.

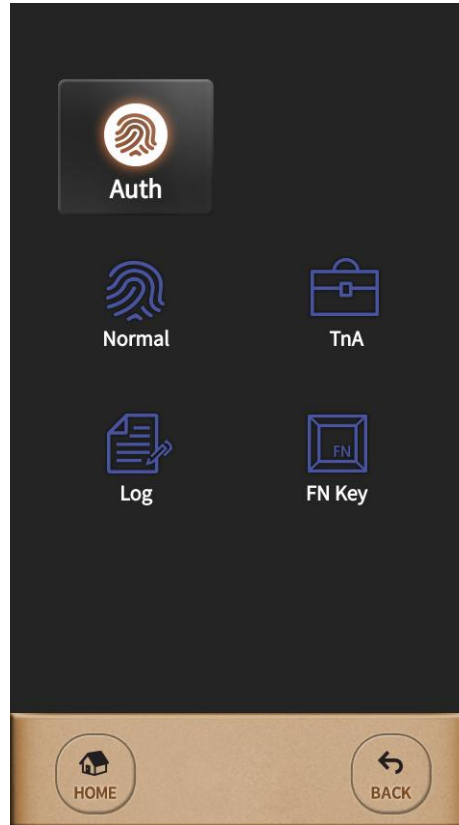
If DHCP is disabled, you must manually enter the terminal's **IP address**, **Subnet Mask**, and **Gateway**.

For this information, contact your IT administrator.

### 3.5. Auth

When **[Auth]** is selected from the main menu, the following window appears.

This menu allows you to configure authentication options, attendance mode, and card usage.



### 3.5.1. Basic

This menu allows you to configure authentication options, attendance mode, and card usage.

Auth : Normal

Verify Level 4

Identify Level 5

Enable FP 1:N Use ▼

Auth Sequence Terminal -> Server ▼

HOME SAVE BACK

- Authentication Security Level

Set the security level according to the authentication method.

- For **1:1 authentication**, the input range is **1–9**, with a default of **4**.
- For **1:N authentication**, the input range is **5–9**, with a default of **5**.

A security level that is too high may increase authentication failure rates, while a level that is too low may increase false acceptance rates.

It is recommended to use the default values.

This setting applies to all users for whom a security level has not been individually specified during registration.

- 1:1 / 1:N Authentication Method Settings

The UBio-X Slim supports two authentication methods: 1:1 and 1:N.

In 1:1 authentication, the user enters their ID before performing authentication.

In 1:N authentication, no ID is entered; the terminal searches all registered users to perform authentication.

Use 1:1 when faster authentication speed is required, and 1:N when a simpler authentication process is preferred.

- Authentication Order

The authentication order determines how the terminal operates when connected to the network and integrated with the PC software, UNIS.

There are four types of authentication methods:

|                  |                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Server->Terminal | Server authentication is performed first.<br>If the network is disconnected, user authentication is performed locally on the terminal. |
| Server Only      | Only server authentication is performed.                                                                                               |
| Terminal->Server | Authentication is first performed on the terminal.<br>If it fails, server authentication is then performed.                            |
| Terminal Only    | Authentication is performed only on the terminal.                                                                                      |

### 3.5.2. TNA

#### 3.5.2.1 TNA Mode

Auth : TnA

|          |         |         |
|----------|---------|---------|
| TnA Mode | TnA ▼   |         |
| Attend   | 00:00 ▼ | 00:00 ▼ |
| Leave    | 00:00 ▼ | 00:00 ▼ |
| In       | 00:00 ▼ | 00:00 ▼ |
| Out      | 00:00 ▼ | 00:00 ▼ |
| Access   | 00:00 ▼ | 00:00 ▼ |

HOME SAVE BACK

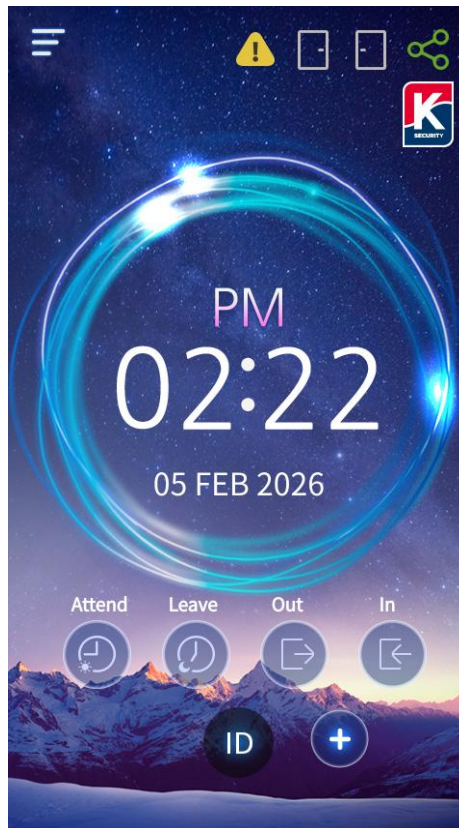
When Attendance Mode is enabled, users must press a function key before performing authentication to open the door.

The corresponding access log, along with the function key, is transmitted to the server management program.

By using function keys, user attendance status—such as Attend, Leave, Out, and In—can be distinguished, allowing for more efficient attendance management.

In Function Key Mode (3.5.4), the default value is Not Use. When Normal Mode is selected, the settings are applied as follows.

Attend (F1) / Leave (F2) / Out (F3) / In (F4)



When **Expand Mode** is selected, a “+” icon is displayed as shown below.

(ExtMode1 ~ ExtMode40)



### 3.5.2.2 Meal

The screenshot shows a mobile application interface for 'Auth : TnA'. The 'TnA Mode' is set to 'Meal'. Below this, there are six rows for meal types: Breakfast, Lunch, Dinner, Supper, and Snack. Each row has two time selection fields, both currently set to '00:00'. At the bottom, there is an 'Allow duplicate' option set to 'Not Use'. A navigation bar at the very bottom contains three buttons: 'HOME' (house icon), 'SAVE' (floppy disk icon), and 'BACK' (back arrow icon).

| TnA Mode        | Meal    |       |
|-----------------|---------|-------|
| Breakfast       | 00:00   | 00:00 |
| Lunch           | 00:00   | 00:00 |
| Dinner          | 00:00   | 00:00 |
| Supper          | 00:00   | 00:00 |
| Snack           | 00:00   | 00:00 |
| Allow duplicate | Not Use |       |

When Meal Mode is enabled, time periods can be set for each meal type.

If no time setting is required, set it to 00:00–00:00.

- **Allow Duplicates:** When enabled, multiple authentications are allowed regardless of previous authentication results.  
Press the **Save** button to apply the setting.

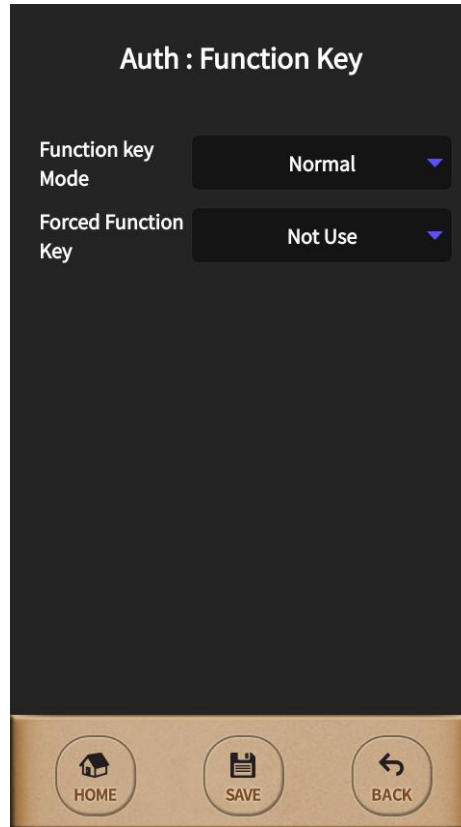
3.5.3. Log

This function allows you to view user authentication log information on the terminal.



### 3.5.4. Function Key

Function Key Mode supports the extension of Attendance Mode when Attendance Mode is in use



The default value is **Not Use**, and the terminal supports **Normal** and **Expand** modes.

In **Normal Mode**, F1 / F2 / F3 / F4 buttons appear on the main screen.

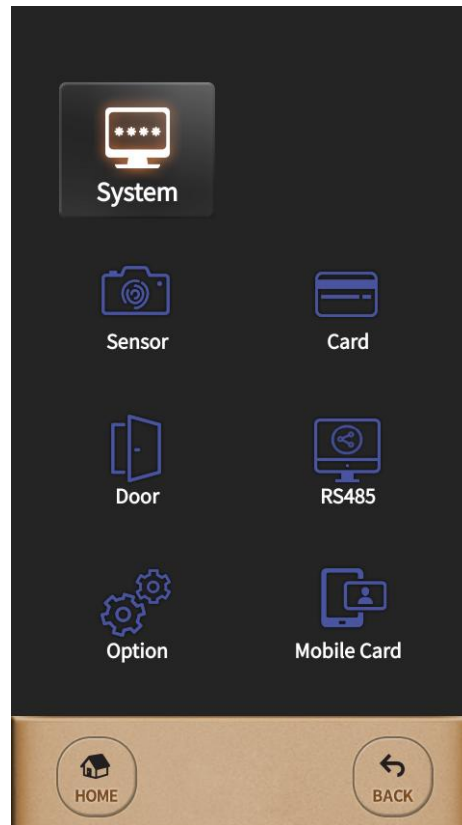
In **Expand Mode**, a “+” icon appears on the main screen. Selecting it opens the expanded function key input screen.

### 3.5.5. Forced Function Key

Forced Function Key is a feature that requires users to press a function key (F1 / F2 / F3 / F4) before authentication.

### 3.6. System

This menu allows you to configure sensor settings, card settings, and door options. When [System] is selected from the main menu, the following window appears.



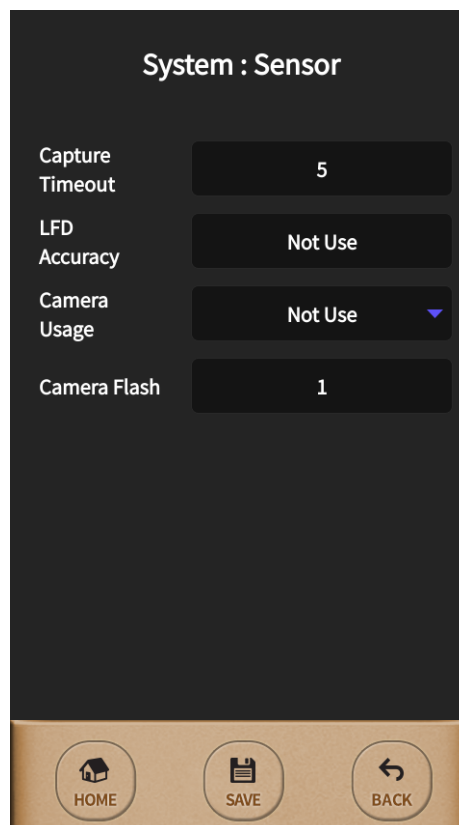
### 3.6.1. Sensor

This menu allows you to configure fingerprint capture time, LFD (Liveness Detection) accuracy, camera usage, and camera flash options.

It is used to set fingerprint sensor options related to authentication.

When the default sensor settings of the terminal are changed, the new options are applied to all users who do not have individual sensor settings during registration.

Enabling the camera allows the system to record photo logs.



- Fingerprint Capture Timeout

This is the waiting time for fingerprint input during capture.

The range is 1–9 seconds, and the default value is 5 seconds.

- LFD (Live Finger Detection) Accuracy

This menu is used to enable or disable fake fingerprint detection and to set its level.

Select the desired option from 0 to 3: Not Use (0), Low (1), Medium (2), or High (3).

- Camera Usage

You can configure whether the camera is used and under which conditions photos are taken.

- Success: A photo is taken when authentication succeeds.
- Fail: A photo is taken when authentication fails.
- All: A photo is taken for both successful and failed authentications.
- Not Use: No photo is taken; instead, a fingerprint image or the image corresponding to the authentication type is displayed.

- Camera Flash

The flash can be adjusted in 4 levels (0–3).

It is activated when the surrounding environment becomes dark, as detected by the ambient light sensor.

Higher levels increase the LED brightness.

### 3.6.2. Card

These settings are used when card authentication is enabled for terminal user verification.

System : Card

|                 |             |
|-----------------|-------------|
| Card Type       | MIFARE      |
| Card Format     | Default     |
| Wiegand Type    | Not use     |
| Send Data       | Card Number |
| Site Code       |             |
| TOC             | Not Use     |
| External Reader | Not Use     |
| Card Read       |             |

HOME SAVE BACK

- Card Type

During boot, the terminal automatically detects the card reader module and displays the recognized card module type.

The recognized module type is displayed as "MIFARE", "EM or HID", or "iClass".

- Card Format

This menu specifies the format in which the read card number is displayed.

- Hexa: Displays the card number in hexadecimal.

- Decimal: Displays the card number in decimal.

For devices with an RF (low-frequency) card reader, setting Hexa\_1 will display EM card numbers as 16-byte hexadecimal values.

- Wiegand Type

This setting allows you to enable Wiegand output and select the bit format.

For MIFARE card modules, select 34-bit.

For EM 26-bit cards, select 26-bit.

- Transmission Data

This setting determines what data is sent through the Wiegand output: Card Information, User ID, or Unique ID.

User ID: When selected, the 4-digit user ID is transmitted upon successful authentication.

Card Number: When selected, the authenticated user's card information is transmitted.

Unique ID: When selected, the authenticated user's Unique ID is transmitted. (Unique IDs can be configured in Alpeta.)

- Site Code

This setting is only applicable when Transmission Data is set to User ID.

You can select the output as 26-bit or 34-bit:

26-bit: Enter a value from 0 to 255.

34-bit: Enter a value from 0 to 32,767.

- TOC (Template On Card)

You can choose whether to enable or disable TOC.

- External Reader

When Wiegand Card is selected, Wiegand authentication is performed as "Card OR", regardless of the chosen authentication combination (AND/OR).

- Card Read

When a card is presented to the terminal in the Card menu, the card data is displayed according to the card format currently applied in the terminal.

### 3.6.3. Door

The Door menu options serve two main purposes. The first is to control up to two doors, and the second is to support additional functions by connecting fire alarms or lighting alarms.

System : Door

|                |              |
|----------------|--------------|
| Door Selection | Door1        |
| Function       | Not Use      |
| Result Signal  | Success      |
| Lock Open Time | 5 Sec        |
| Door Warn Time | 20 Sec       |
| Door Control   | Normal Close |
| AIN2           | Not Use      |

HOME SAVE BACK

- Door Selection

You can select either Door 1 or Door 2.

- Door Function

You can set the following options: Not Use, Door (for normal door operation), Fire Alarm, Panic Alarm, or Motor Lock.

- ❖ Note for BLC010

When using BLC010, set Door 1 function to Door (for normal door operation).

If Door 1 is set to Not Use, monitoring will not function properly.

- ❖ If Door 1 is set to Motor Lock, Door 2 will automatically also be set to Motor Lock, and vice versa.

When Motor Lock is enabled, the Result Signal, Lock Open Time, and Door Warn Time settings for Door 2 are ignored.

- ❖ The AIN2 setting can be used as a Panic Alarm for the rear connector AIN2.

- Authentication Result Signal

You can configure the lock to operate based on the authentication result.

Success: The lock opens when authentication is successful.

Fail: The lock opens when authentication fails.

- Lock Open Time

Sets the duration for which the lock control output signal is maintained.

- Door Open Warning Time

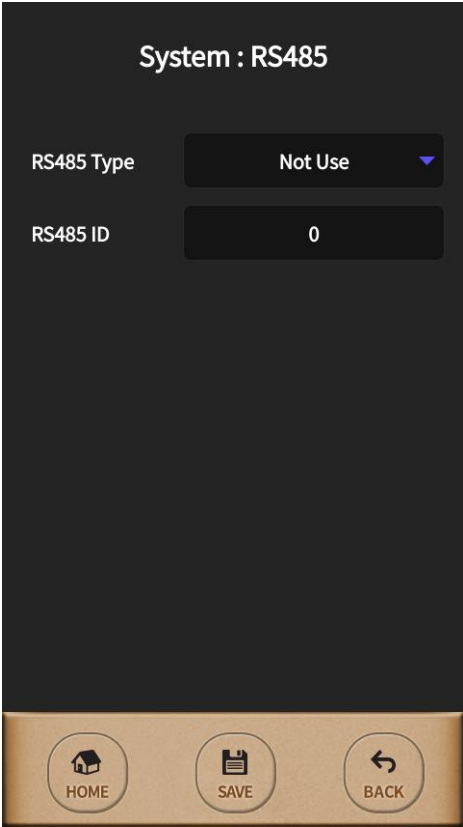
Sets the duration after which a warning is issued if the door remains open.

- Door Status Type

Sets the door control status to NC (Normally Closed) or NO (Normally Open).

### 3.6.4 RS485

This function allows communication with external devices through the RS-485 interface.



- RS-485 Function Selection

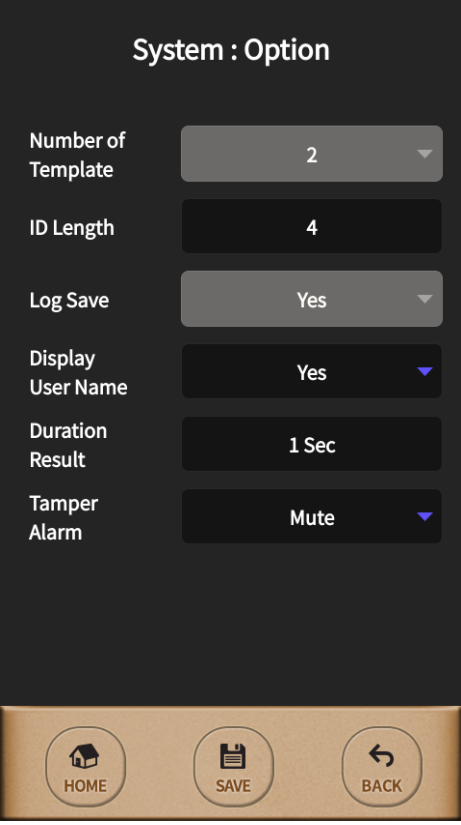
You can select options such as Not Use or BLC010 (External Reader).

- RS485 ID

When using RS-485 communication, the device ID can be set from 0 to 7.

### 3.6.5 Options

In Options, you can configure settings such as the number of fingerprint templates registered per user and the ID length.



The screenshot shows a mobile application interface titled "System : Option". It contains several settings, each with a label and a value in a dropdown menu:

- Number of Template: 2
- ID Length: 4
- Log Save: Yes
- Display User Name: Yes
- Duration Result: 1 Sec
- Tamper Alarm: Mute

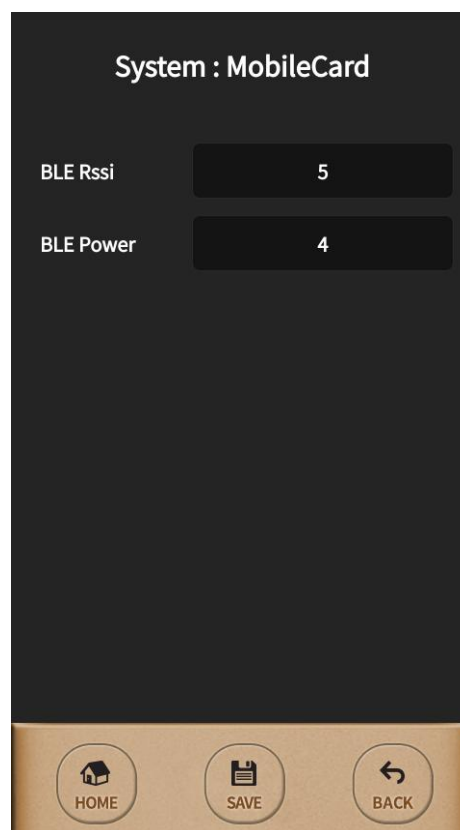
At the bottom of the screen, there is a navigation bar with three icons: a house icon labeled "HOME", a floppy disk icon labeled "SAVE", and a back arrow icon labeled "BACK".

- Number of Fingerprint Templates  
The default value is 2.
- ID Length  
The default value is 4, and the input range is 4 to 8.
- Log Storage  
Configures whether authentication logs are stored.
- Display User Name  
Sets whether the user name is displayed upon successful authentication (Enable/Disable)

- Authentication Result Display Time  
Sets the duration for which the authentication result screen is displayed (1 second ~ 20 seconds)
- Tamper Alarm Mute  
Sets whether the tamper warning sound is muted or enabled (Mute / Enable)

### 3.6.6. Mobile Card

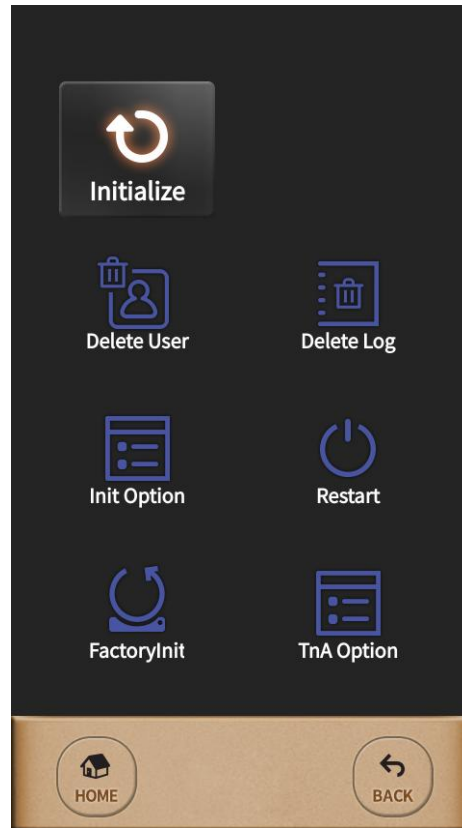
This is set when using Mobile Card authentication during terminal user authentication.



- BLE Rssi  
Sets the reception sensitivity of the mobile card. (Range: 1–10)
- BLE Power  
Sets the transmission power of the mobile card. (Range: 1–16)

### 3.7. Initialization

When [Initialization] is selected from the main menu, the following screen appears.

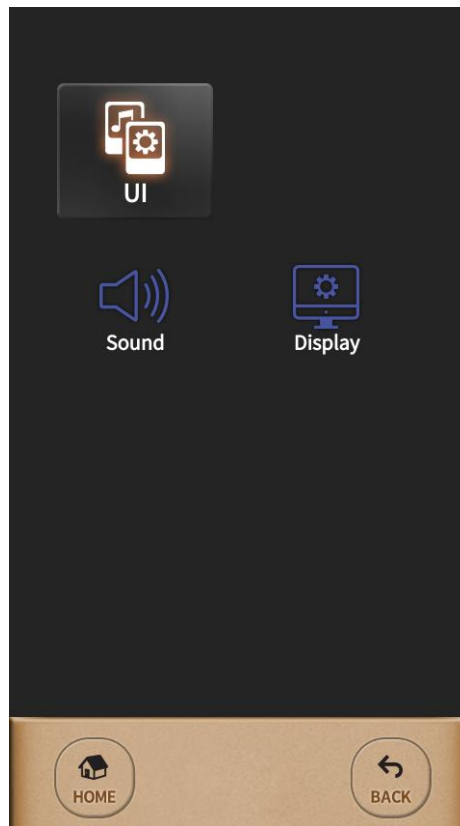


This menu restores the device to its factory default settings, including all registered users, log information, and options. Use caution when performing initialization, as it will completely erase the device database.

- User Delete: Resets all users.
- Log Delete: Clears all logs.
- Option Initialize: Resets all options.
- Restart: Restarts the device.
- Factory Reset: Restores factory settings.
- TnA Initialize: Resets attendance and meal time settings.

### 3.8. UI

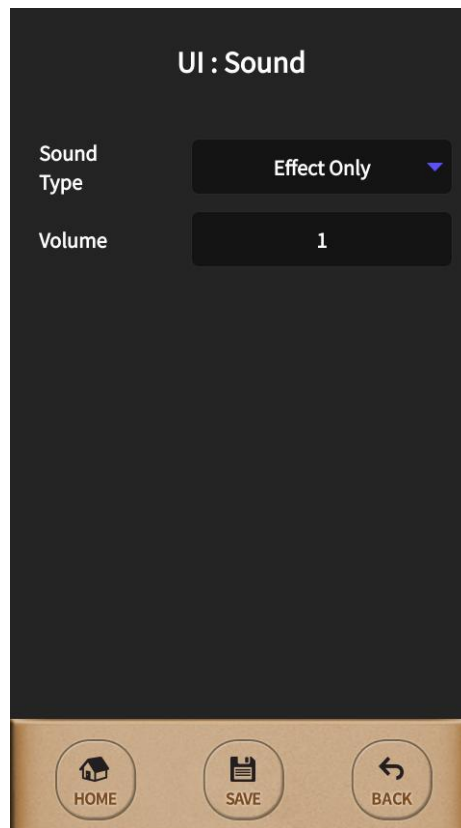
When [UI] is selected from the main menu, the following window appears.



The terminal's initial screen background, display language, time, and sound can be freely customized according to the user's preferences

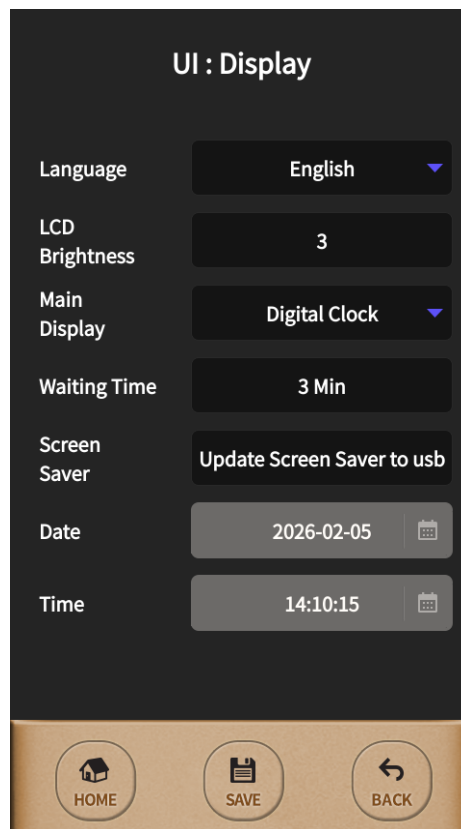
### 3.8.1. Sound

You can turn voice prompts and sound effects on or off, and adjust the volume.



- ✓ Voice Only: Voice only
- ✓ Effect Only: Sound effects only
- ✓ All: Both voice and sound effects
- ✓ Not Use: Disabled

### 3.8.2. Display



- **Language**  
Press the Language button to select the language to be displayed on the screen  
(Available languages: English, Korean, French, Spanish, Portuguese, Indonesian, Persian, Japanese, Russian, Arabic, Chinese, Thai, Hindi; default is English)
- **LCD Brightness**  
The LCD brightness can be set from 1 to 5, with the default value being.
- **Main Display**  
You can choose between Digital Clock and Custom Image for the wallpaper.  
User images can be changed from the UNIS and Alpeta servers.  
Supported formats: JPG, PNG, BMP. The image size should be 480 × 854, and the file name must be within 11 characters (numbers and English letters are supported).

- Waiting Time

If there is no input for the set duration, the configured screensaver will activate.

(Range: 0–5 minutes, default: 3)

- Screensaver

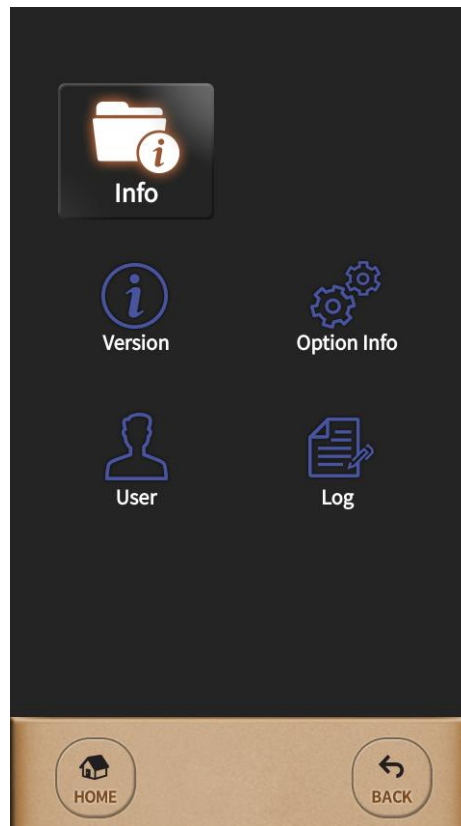
Save up to 5 screensaver images you want to apply in the USB path UbioXslim/screensaver/ and rename them as bg1.jpg, bg2.jpg, bg3.jpg, bg4.jpg, and bg5.jpg. After inserting the USB into the terminal, press the "Update Screensaver from USB" button to apply the screensaver images stored on the USB to the terminal.

- Date & Time

You can set the terminal's date and time. This function is available in Standalone mode only.

### 3.9. Information

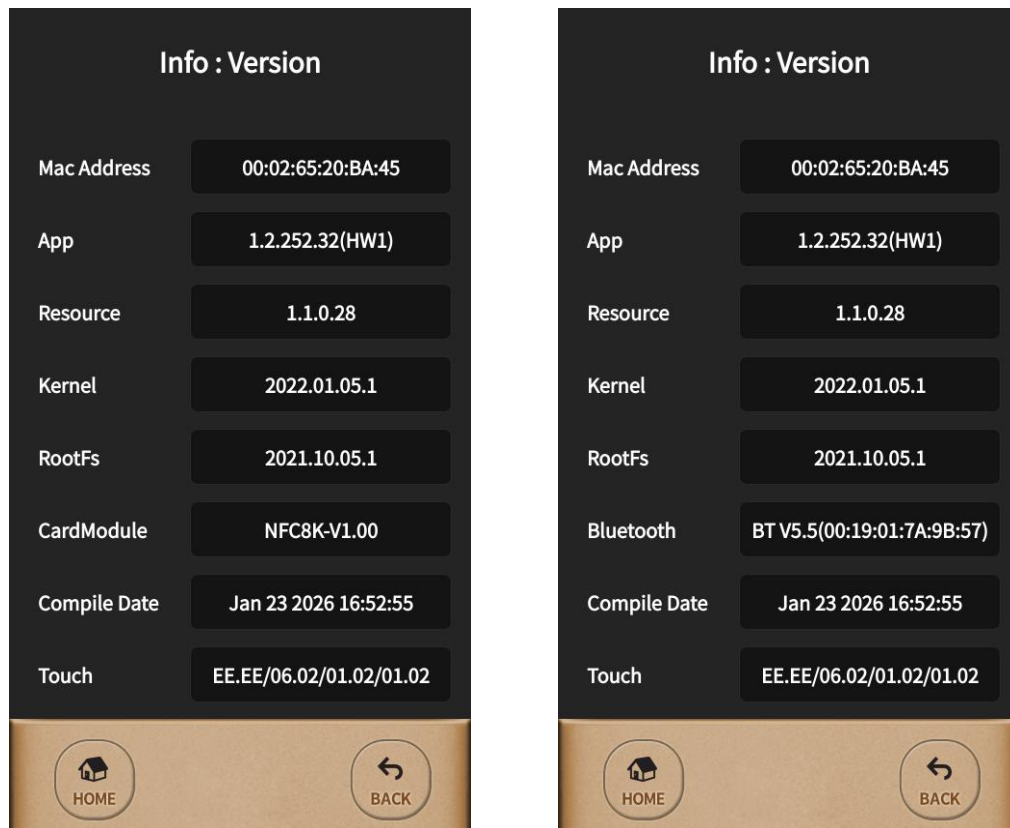
When [Info] is selected from the main menu, the following screen appears.



On the terminal information screen, you can select Version, Option Info, User, or Log to view the terminal's information. In this menu, you can only view the information; no changes can be made.

### 3.9.1. Version

You can view the version information.



- Mac Address  
Displays the MAC address.
- App  
Displays the App version.
- Resource  
Displays the Resource version.
- Kernel  
Displays the Kernel version.
- RootFs  
Displays the Filesystem version.

- CardModule

Displays the Card Module version.

When the Card Module version is selected, the Bluetooth version is displayed. The display toggles between the Card Module version and the Bluetooth version.

If the terminal does not have a Bluetooth module or does not support Bluetooth, the Bluetooth version will not be shown.

- Compile Date

Displays the App compile date.

- Touch

Displays the Touch Sensor Firmware version.

### 3.9.2. Option Info

Displays the Option Information.

The screenshot shows a mobile application interface titled "Info : Option Info". It displays a list of system parameters in a table-like format. At the bottom, there are two circular navigation buttons labeled "HOME" and "BACK".

| Info : Option Info |                                         |
|--------------------|-----------------------------------------|
| Terminal ID        | 1                                       |
| TnA Mode           | TnA                                     |
| Card Type          | MIFARE                                  |
| Network Type       | Ethernet                                |
| IP Address         | 17.17.17.9                              |
| Version            | 1.2.252.32-2022.01.05.1<br>2021.10.05.1 |
| FP Version         | FP Algorithm 6.D                        |

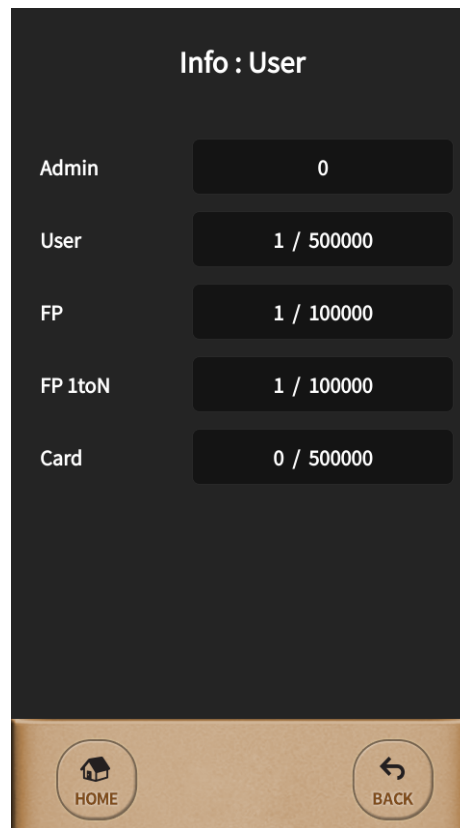
- Terminal ID  
Displays the Terminal ID.
- TnA Mode  
Displays the TnA (Time and Attendance) mode.
- Card Type  
Displays the card type.
- Network Type  
Displays the network type.
- IP Address  
Displays the IP address.

- Version

Displays the App version / Kernel version / Filesystem version.

### 3.9.3. Info User

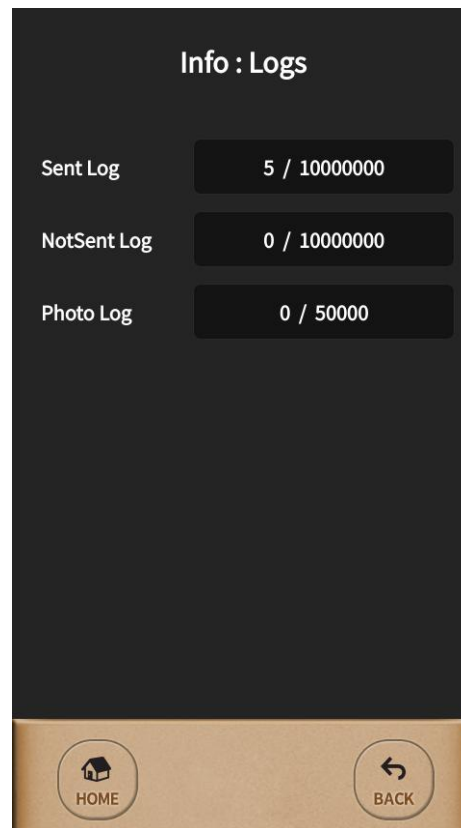
Displays User information.



- Admin  
Displays the number of administrators.
- User  
Displays the number of users.
- FP  
Displays the number of fingerprints.
- FP 1 to N  
Displays the number of 1:N fingerprints.
- CARD  
Displays the number of cards.

### 3.9.4. Info Logs

Displays log information.



- Sent Log  
Displays the number of transmitted logs.
- NoSent Log  
Displays the number of untransmitted logs.
- Photo Log  
Displays the number of photo logs.

### 3.10. USB

Connect a USB memory to the terminal to upload or download user information or download log information.

❖ Please use FAT32 format for the USB file system.

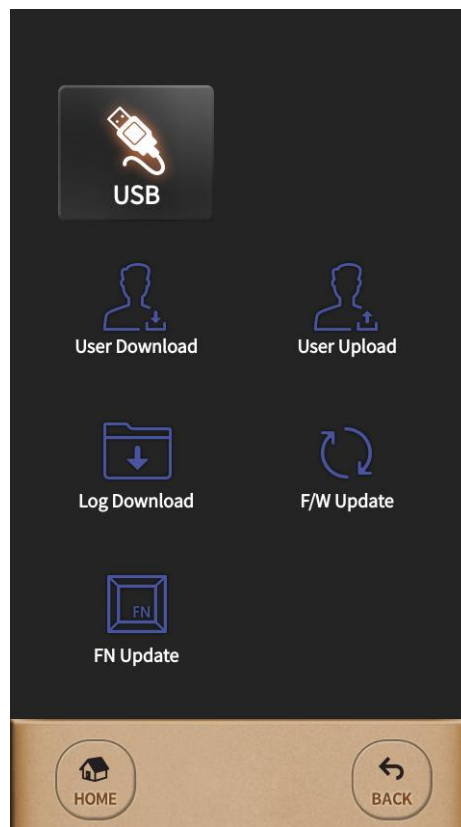
Using an NTFS file system may cause failures when downloading user or log files, and uploads may also fail.

❖ Due to system differences, the time may vary when downloading and checking users or logs.

Example: Current time 15:00 when downloading users

- On Windows, it appears as 06:00
- On Linux, it appears as 15:00

When [USB] is selected from the main menu, the following window appears.



### 3.10.1. User Download

When the User Download button is pressed, if a USB memory is not detected, an error message is displayed. Otherwise, a popup appears asking whether to proceed with the download. Selecting Yes saves all terminal user information to the USB memory in the unisuser directory with the file name format \*.dat (e.g., 0000.dat, 0001.dat, 0002.dat).

After the download is complete, unmount the USB memory.

If you want to download or upload users again, please disconnect and reconnect the USB memory. This file can be read by UNIS and saved to the server.

### 3.10.2. User Upload

When the User Upload button is pressed, if a USB memory is not connected or there is no file named unisuser, an error message will appear. Otherwise, a popup will ask whether to proceed with the upload.

By selecting Yes, the \*.dat files in the unisuser folder on the USB memory are read, and the user data is uploaded to the terminal. If a user ID already exists in the terminal, that user's information will not be overwritten.

After the upload is complete, unmount the USB memory. If you need to download or upload users again, disconnect and reconnect the USB memory.

### 3.10.3. Log Download

When downloading the terminal's log information to a USB memory, you can choose to download all logs or only unsent logs.

All Logs Download: Saves all logs from the terminal to the USB memory, regardless of whether the terminal is in Network Mode or Standalone Mode.

You can select Event Log, Picture Log, or All Log for download.

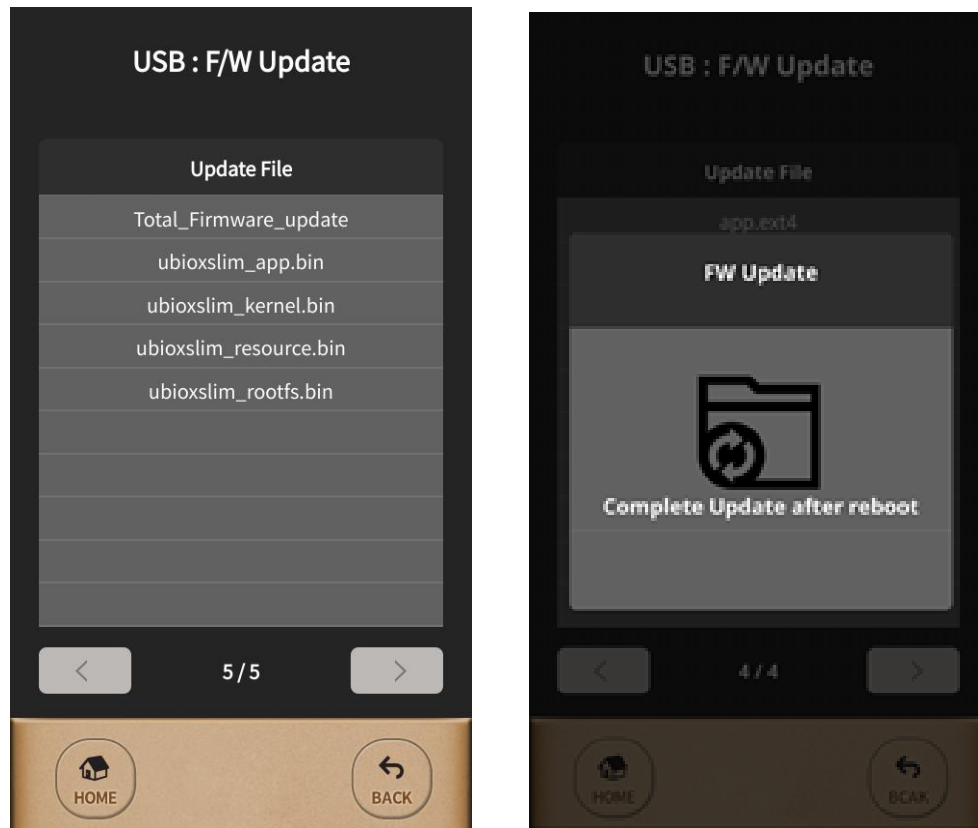
The log data is saved in the log folder on the USB memory with the file name LOG.dat.

Logs stored on the USB can be imported into UNIS and saved to the server.

After the download is complete, unmount the USB memory. If you need to download logs again, disconnect and reconnect the USB memory.

### 3.10.4. F/W Update

Set the FW file to update from the list. The update will proceed as shown in the screen below, and the terminal will reboot after completion.



If you want to download app.ext4, resource.ext4, rootfs-unioncomm\_t7.ext4, and ulmage.unioncomm\_t7 at once, press Total\_Firmware\_update in the list window to update all files simultaneously.

The Total\_Firmware\_update option will only appear if all four files (app.ext4, resource.ext4, rootfs-unioncomm\_t7.ext4, ulmage.unioncomm\_t7) exist on the USB memory. If even one of the four files is missing, Total\_Firmware\_update will not appear.

\*\*\*Starting from firmware version 1.2.0.1 installed on the terminal, the file names have changed to:

- *ubioxslim\_app.bin*
- *ubioxslim\_resource.bin*
- *ubioxslim\_kernel.bin*
- *ubioxslim\_rootfs.bin*

The Total\_Firmware\_update option will only appear if all four files exist on the USB.

⚠ Important: Do not rename any of the distributed files. If the file names are changed and an update is attempted, the terminal may fail to operate properly.

### 3.10.5. FN Update

When you press the FN Update button:

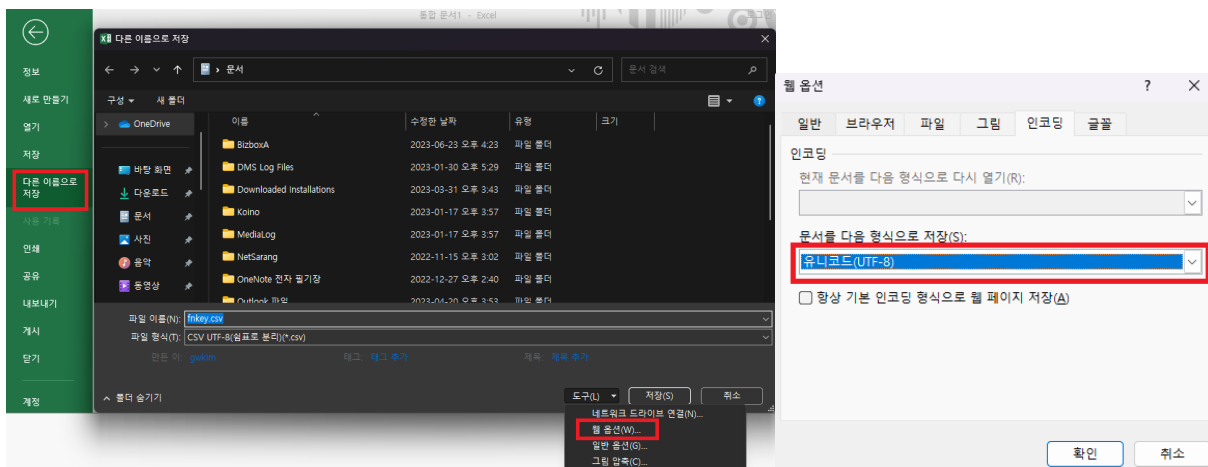
- If a USB memory is not connected or the file named fnkey.csv is not present, an error popup will appear.
- If the fnkey.csv file exists, the Function Key names on the terminal will be updated.

Details about fnkey.csv:

- Function Keys are separated by commas (,).
- Each Function Key name can have a maximum of 20 characters.

Example: Key1,Key2,Key3,Key4,Key5

- The CSV file must be in UTF-8 encoding format; other encodings are not supported.



## 4. How to Use the Terminal

### 4.1. How to open the door

There are two supported methods for opening the door for users registered on the terminal, depending on whether 1:N authentication is enabled.

- **1:1 Authentication**

This method requires entering a pre-registered ID first, then providing a fingerprint. The entered fingerprint is compared 1:1 with the fingerprint registered for that ID.

- 1:1 authentication allows fast verification regardless of the number of users.
- To use 1:1 authentication, press the "Authenticate" button at the bottom right, enter the ID, and then authenticate using the registered method(s) (fingerprint, card, or password).



- **1:N Authentication**

This method allows the user to authenticate without entering an ID. The device scans the presented fingerprint (or other registered authentication method) against all registered fingerprints in the system.

The authentication process is simpler since users don't need to input their ID.

However, if there are many registered users, the authentication time may be slightly longer.

### 1) Fingerprint Authentication

The registered fingerprint is entered on the fingerprint reader without entering an ID for authentication.



## 2) Card authentication

Authenticate by presenting a registered card at the card reader without entering an ID.



If the ID must be entered when pressing the "Authenticate" button on the terminal's main screen, make sure that the 1:N authentication option in the terminal settings is turned off.



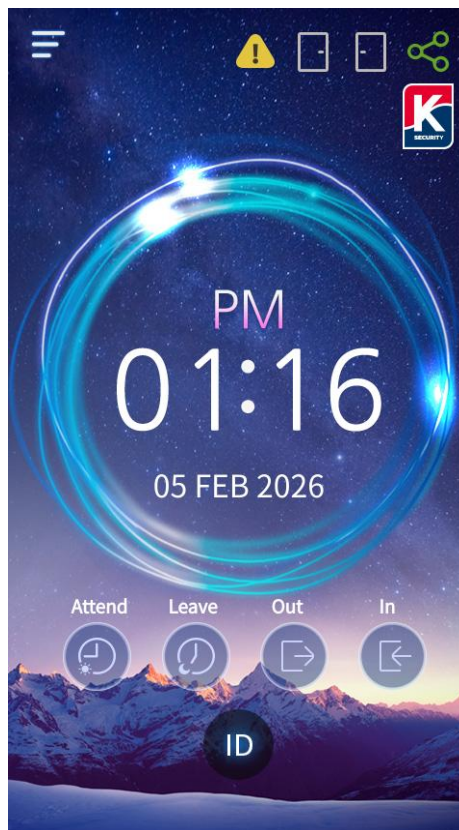
For users using a password in 1:N authentication, the process is the same as the 1:1 authentication method.

#### 4.2. How to authenticate in TNA Mode

When the terminal is set to Time & Attendance (TnA) mode, users must press the Function Key before performing authentication for the entry/exit. Only then will the Function Key log be transmitted to the server.

If the Function Key is not pressed, the system may not correctly record the user's work status, such as Attendance, Leave, Out, or In, so users must follow the administrator's instructions and always press the Function Key before authentication.

In TNA mode, the main screen initially displays the labels and icons for Attend, Leave, Out, and In at the bottom.



Tip : To use 1:N authentication in TNA mode, perform authentication immediately after entering the attendance key, without entering an ID in the ID input field.

## FCC Compliance Information

This device 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.