

# UBio-X Slim User Guide

---

Version Eng-1.3



**UNION**  
COMMUNITY

Distributed by  
**genie**

---

Copyright 2000 By Union Community Co., LTD.

## &lt;Revision History&gt;

Version	Date	Description	Firmware Version
0.1	2019-03-15	Initial Release	
0.2	2019-03-25	Modified some words.	
0.3	2019-04-25	Modified the menu titles according to terminal's menu modes.	
0.4	2019-05-17	Added the explanation of USB user and log download.	
0.5	2019-06-05	Modified the explanation of USB and added the feature of motor lock.	
0.6	2019-06-21	Added the voice message of the password.	
0.7	2019-06-28	Added the default value of the information in menu.	
0.8	2019-07-10	-Added the explanation of auto TNA, encryption, voice and language. -Added the feature of factory reset.	
0.9	2019-08-09	Add the comment of image display about authentication result depending on the authentication type. (pg.26)	
1.0	2019-09-23	Added the comment of camera flash. (pg.27)	
1.1	2019-10-11	Added the explanation of log download and USB unmount.	
1.2	2019-10-30	Added the feature to use the user's photo.	
1.3	2019-12-06	Added the method to update App, Resource, Kernel and Rootfs file at one time.	

---

## <Glossary>

- Admin, Administrator
  - A user who can enter into the terminal menu mode, he/she can register/modify/delete terminal users and change the operating environment by changing settings.
  - If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
  - Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.
  
- 1 to 1 Verification
  - Authenticate the user's fingerprint after inserting his user ID or swiping his registered Card.
  - It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.
  
- 1 to N Identification
  - The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
  - Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.
  
- Authentication level
  - Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
  - The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable to failure.
  - 1:1 Level: Authentication level used for 1:1 verification
  - 1:N Level: Authentication level used for 1:N identification
  
- LFD (Live Finger Detection)
  - This function allows the input of only real fingerprints and blocks the input of imitation fingerprints produced using rubber, paper, film, and silicone.

---

**UNIONCOMMUNITY Co., Ltd.**

**Addr : 12F, Munjeong Daemyeong Valeon bldg, 127 Beobwon-ro Songpa-gu,  
Seoul, Korea (zip code : 05836)**

**Tel : +82-2-6488-3000 , Fax : +82-2-6488-3099,**

**E-Mail : [sales@unioncomm.co.kr](mailto:sales@unioncomm.co.kr); <http://www.unioncomm.co.kr>**



## Contents

<Revision History> .....	2
<Glossary> .....	3
<b>1. Before use</b> .....	<b>5</b>
1.1. Safety Precautions .....	6
1.2. Specific names of the terminal .....	6
1.3. LCD Display Composition .....	7
1.3.1 Status Icons.....	8
1.4. Voice and Beep sounds in operation.....	9
1.4.1 Beep or Sound effect in operation.....	9
1.5. Proper fingerprint registration and input methods.....	9
<b>2. Product introduction</b> .....	<b>10</b>
2.1. Product characteristics .....	10
2.2. Product components .....	11
2.2.1. Standalone use (Access).....	11
2.2.2. Connected with Server (Access, Attendance) .....	12
2.3. Product specification.....	13
<b>3. Environment setting</b> .....	<b>14</b>
3.1. Checks before setting the environment .....	14
3.1.1. Entering the menu by Administrator .....	14
3.2. Menu composition .....	15
3.3. User.....	17
3.3.1. Register .....	18
3.3.2. Modify.....	19
3.3.3. Delete .....	20
3.3.4. List.....	21
3.3.5. Card Only .....	21
3.4. Auth.....	22
3.4.1. Normal.....	22
3.4.2. TnA.....	23
3.4.3. Timezone.....	24
3.4.4. Log .....	24
3.5. System .....	25
3.5.1. Sensor .....	25
3.5.2. Card .....	26
3.5.3. Door .....	27
3.5.4. RS485 .....	28
3.5.5. Option.....	28
3.5.6. Information .....	29
3.6. Network.....	29
3.6.1. Normal.....	30
3.6.2. TCP/IP .....	31
3.7. UI.....	31
3.7.1. Sound .....	32
3.7.2. Display.....	33
3.8. USB .....	33
3.8.1. User Download .....	34
3.8.2. User Upload.....	34
3.8.3. Log Download.....	34
3.8.4. F/W Update .....	35

---

3.9. Initialize..... 35

4. How to use terminal ..... 36




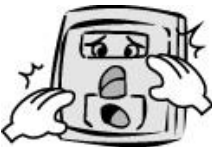
4.1. How to open the door ..... 36

4.2. How to punch for TnA..... 38

# 1. Before use






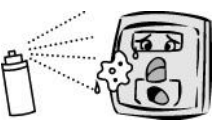

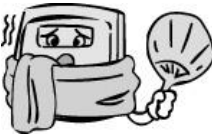
## 1.1. Safety Precautions

### ● Warning

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

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

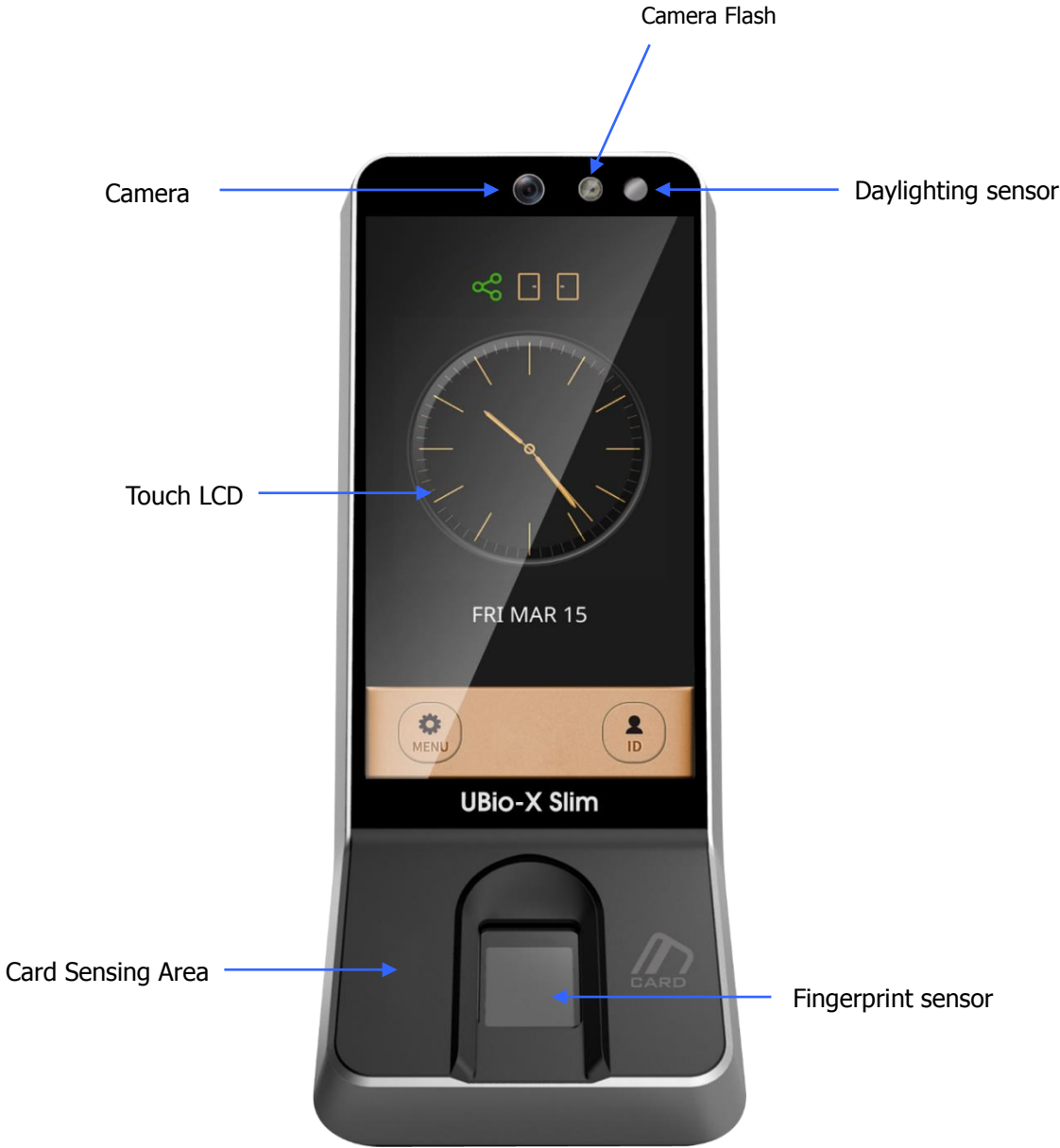
### ● Cautions

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

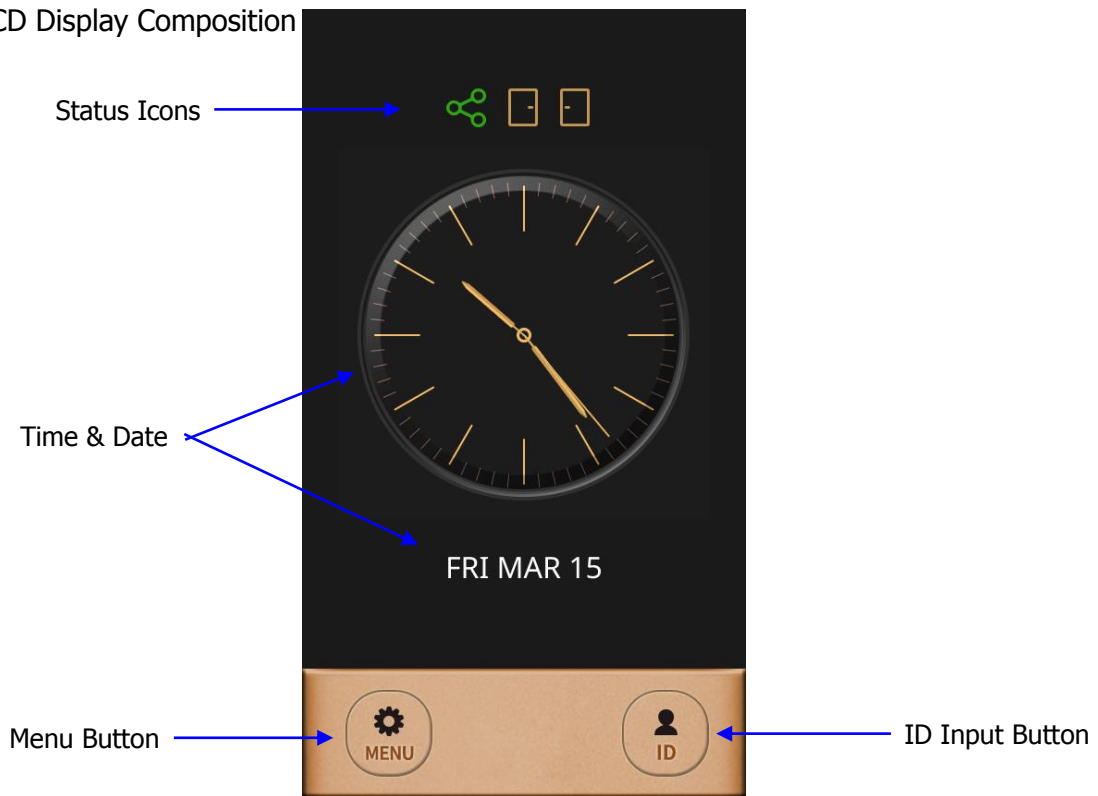
- If the above cautions are ignored, it may result in property loss or human injury.

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











1.2. Specific names of the terminal



1.3. LCD Display Composition



1.3.1 Status Icons

Network Status		: Standalone Mode (Non-networking Mode)
		: Connected to the server (On line)
		: Disconnected to the server (Off line)
Fire Alarm	None	: Normal Status
		: Fire Alarm is activated. (by the Fire switch or by Server program)
Tamper	None	: Normal Status
		: Abnormal Status (Tamper switch is activated.)
Door Status		: Door is closed.
		: Door is opened.
		: Door is opened abnormally.
		: Door is not used.
		: Door is forcedly open.



1.4. Voice and Beep sounds in operation

Operation type	Voice sound
Success to authorize	You are authorized
Fail to authorize	Please try again
Waiting for FP input	Please place your finger.
Waiting for card input	Please place your card.
When entering ID	Please insert your ID.
When entering the password	Please enter your ID.

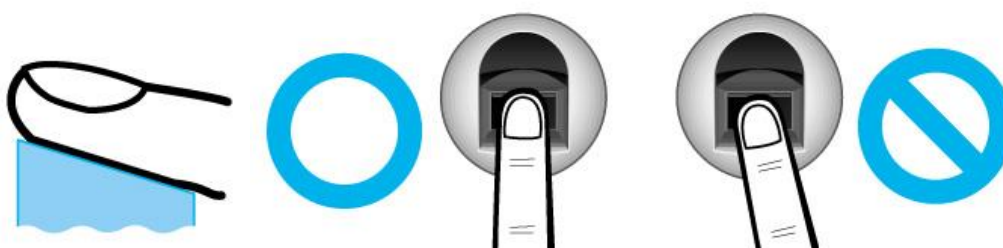
1.4.1 Beep or Sound effect in operation

Pi-pick error tone +	Notice for fail	When the authorization was failed (at Voice off)
Peek Ding-dong +	Notice for Success	When the authorization was successful (at Voice off)

1.5. Proper fingerprint registration and input methods

- Correct fingerprint registration methods

Place your index finger on the window just as you do with a finger stamp.  
 Do not use the tip of the finger.  
 Make sure the center of your finger touches the window.



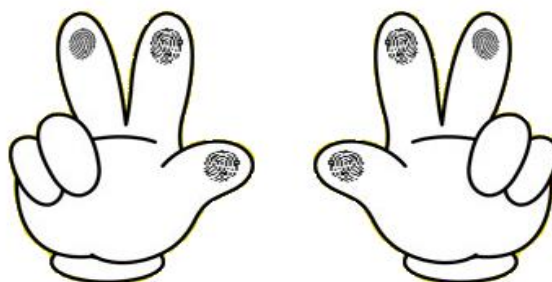
- Use your index finger if possible, it is the easiest for orientation and guarantees a stable input method.
- Check if your fingerprint is unclear or damaged.  
 It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case.



- Be aware of certain fingerprint conditions

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

- If the fingerprint is damaged or very unclear, then it cannot be recognized. Please use the RF Card instead in this case.
- **When a finger is dry, breathe on the finger for smooth operation.**
- For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or very unclear. It is recommended to register their fingerprints every six months.
- For the elderly, it may not be possible to register their fingerprints if there are too many fine lines on the fingerprints.
- It is recommended that you register more than 2 fingerprints.
- In order to increase the fingerprint authentication rate, it is recommended to use six of the ten fingers as illustrated above. (Both thumbs, forefingers, middle fingers).



## 2. Product introduction

### 2.1. Product characteristics

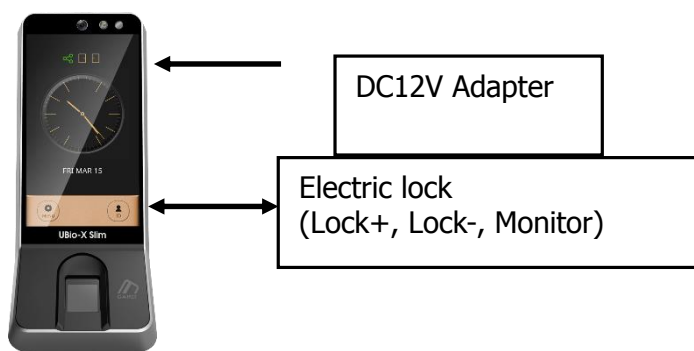
- Multi-Modal product with which the user can use fingerprint, Card or Password authorization functions together.
  - Built-in Camera Flash can detect the real human face or a picture.
-

- Camera Flash can be activated automatically by the Daylighting sensor.
- RF Card (125 kHz)
- Smart Card (13.56MHz)
- This is Access Control System can be cooperated with Server Database by TCP/IP or Wi-Fi (optional).
- Various registration and authorization methods

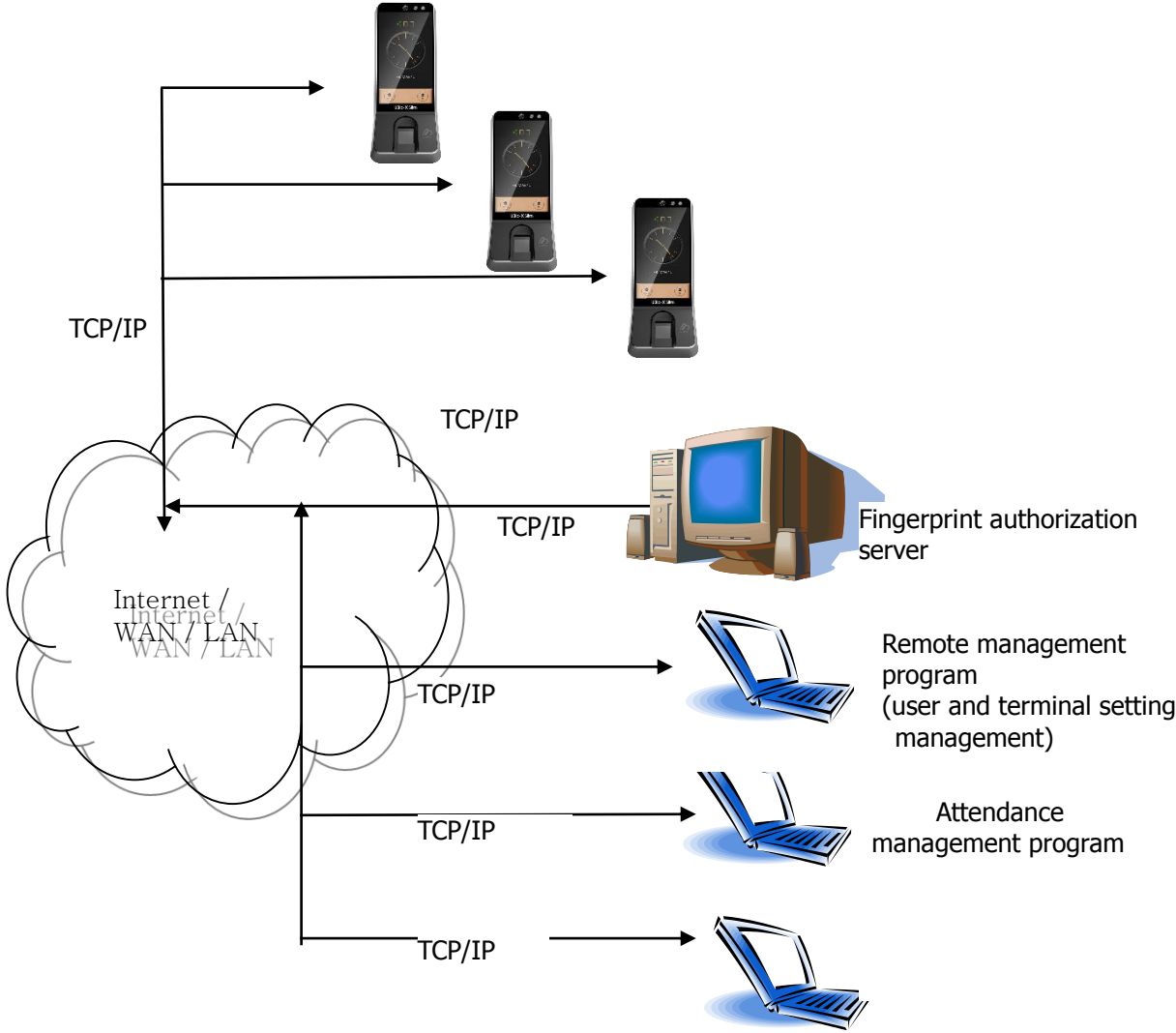
Fingerprint	Fingerprint registration Fingerprint authorization
Card	Card registration Card authorization
Password	Password registration Password authorization
'OR' Combination Authentication	To be authorized successfully, one method among the registered should be authorized.
'AND' Combination Authentication	To be authorized successfully, all registered Auth methods should be authorized.

2.2. Product components

2.2.1. Standalone use (Access)



2.2.2. Connected with Server (Access, Attendance)



## 2.3. Product specification

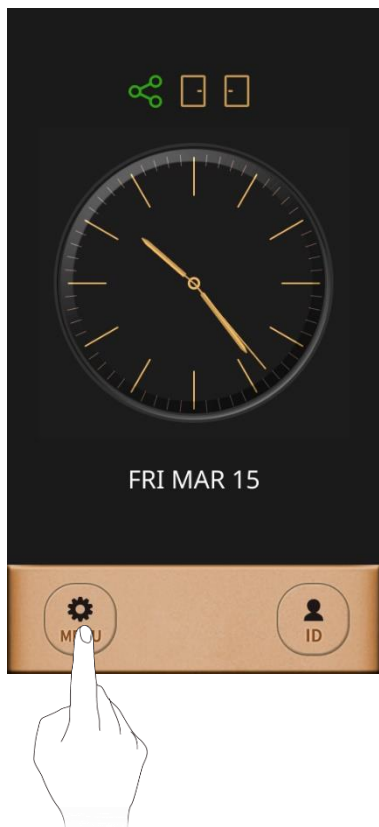
Types	SPEC	Remarks
CPU	1.4GHz Quad Core CPU	
LCD	4.95 inches Touch LCD(480*854)	
Memory	eMMC 8G Bytes Flash	
	2GByte RAM	
External USB support	Backup data / Upgrade firmware	
Camera	Still Capture Image Color (1600x1200)	
Camera Flash Sensor	Daylighting Flash Control	
Capacity	500,000 Users / 500,000 Cards (Server: 200,000) 10,000,000 Logs / 50,000 Image logs	100,000 Users / In case of more than 100,000 users, the booting time takes more than 3 mins.
Temperature / Humidity	-20 ~60°C / Lower than 90% RH	
AC / DC Adapter	INPUT : Universal AC100 ~ 250V	
	OUTPUT : DC 12V ~ 24V 3.5A	
	UL, CSA, CE Approved	
Lock Control	EM, Strike, Motor Lock, Auto Door	
I/O	4 In (1 Exit, 3 Monitors) 2 Out (Lock 1, Lock 2)	
Communication Port	TCP/IP (10/100Mbps)	Communication with Auth Server
	RS-232	Ticket Printer
	RS-485	Communication with Controller
	Wiegand Input / Output	Communication with Card reader or Controller
Card Reader	125KHz RF / 13.56MHz Smart HID 125K Prox card (Optional) HID iClass card (Optional)	Option
Dimension (mm)	80 X 195.6 X 23.5(Normal) / 54.67(Max)	Including Bracket

### 3. Environment setting

#### 3.1. Checks before setting the environment

##### 3.1.1. Entering the menu by Administrator

Terminal users include general users and administrators. General users are only allowed to open the door while the administrator can use the Administrator menu to control the door as well as the terminal's functions.



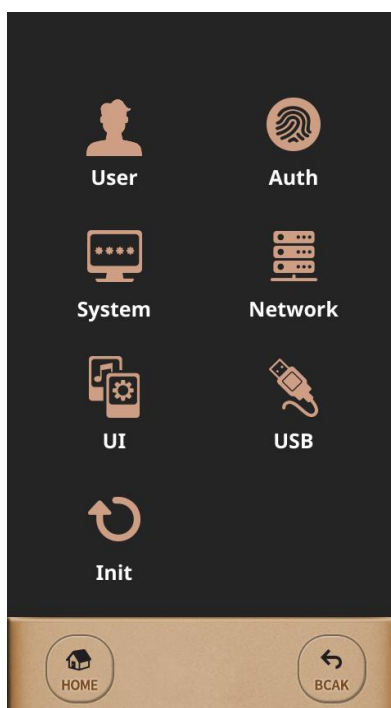
1. To enter the menu, touch the [MENU] button at the lower of the touch pad.
2. Input the administrator ID and follow the authentication process. The Administrator menu will be displayed. Because no users have yet been registered, any user can enter the Administrator menu. At least, one administrator should be registered for security purposes.

**TIP**

1. If no administrator was designated and only general users were registered in network mode, all users will be allowed to enter the management menu.
2. If 1:N authentication is used, an administrator with a registered fingerprint can enter the administrator menu using fingerprint authentication without entering his ID.

### 3.2. Menu composition

The Administrator menu has seven submenus as shown below. The following describes each sub menu:



1. User	<ol style="list-style-type: none"> <li>1. Register</li> <li>2. Modify</li> <li>3. Delete</li> <li>4. List</li> <li>5. Card Only</li> </ol>	
2. Auth	1. Normal	<ul style="list-style-type: none"> <li>▶ 1:1 Auth Level (Default : 5)</li> <li>▶ 1:N Auth Level (Default : 8)</li> <li>▶ Auth Type (Default : Use Identify (1:N Auth))</li> <li>▶ Auth Order (Default : Terminal → Server)</li> </ul>
	2. TnA	<ul style="list-style-type: none"> <li>▶ TnA Type (Default : Not Use)</li> <li>▶ Auto TnA (Default : Not Use)</li> <li>▶ TnA only (Default : Not Use)</li> </ul>
	3. Timezone	
	4. Log	

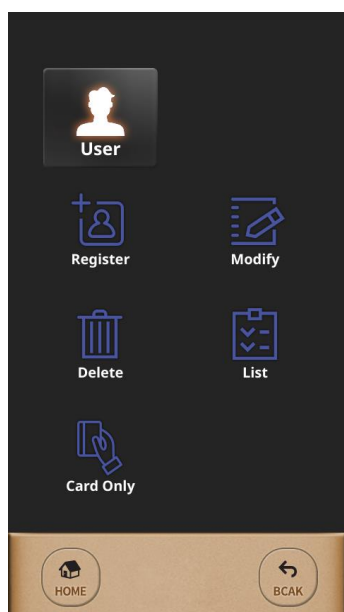
3. System	1. Sensor	<ul style="list-style-type: none"> <li>▶ Capture Timeout (Default : 5 seconds)</li> <li>▶ LFD Accuracy (Default : Not Use)</li> <li>▶ Camera Usage (Default : Not Use)</li> <li>▶ Camera Flash (Default: 1)</li> </ul>
	2. Card	<ul style="list-style-type: none"> <li>▶ Card Type (Default : Not Use)</li> <li>▶ Wiegand Type (Default : Not Use)</li> <li>▶ Send Data (Default : Card Number)</li> <li>▶ Site Code</li> </ul>
	3. Door	<ul style="list-style-type: none"> <li>▶ Door Selection (Default : Door1)</li> <li>▶ Function (Default : Door)</li> <li>▶ Result signal (Default : Success)</li> <li>▶ Lock Open Time (Default : 5 seconds)</li> <li>▶ Door Warn Time (Default : 20 seconds)</li> <li>▶ Door Control (Default : Normal Close)</li> </ul>
	4. RS485	<ul style="list-style-type: none"> <li>▶ RS485 Type (Default : Not Use)</li> <li>▶ RS485 ID (Default : 0)</li> </ul>
	5. Option	<ul style="list-style-type: none"> <li>▶ Number of Template (Default : 2)</li> <li>▶ ID length (Default : 4)</li> <li>▶ Log Save (Default : Yes)</li> <li>▶ Display User Name (Default : Yes)</li> <li>▶ Duration Result (Default : 1 second)</li> <li>▶ Tamper Alarm (Default : Mute)</li> </ul>
	6. Information	<ul style="list-style-type: none"> <li>▶ Terminal ID (Default : 1)</li> <li>▶ Number of User / Template (0/0)</li> <li>▶ Number of Admin. (0)</li> <li>▶ TnA Mode (Not Use)</li> <li>▶ Card Type (Not Use)</li> <li>▶ Network Type (Ethernet)</li> <li>▶ IP Address (192.168.0.3)</li> <li>▶ Version (Firmware – Kernel version / File system version)</li> </ul>
4. Network	1. Normal	<ul style="list-style-type: none"> <li>▶ Type (Default : Ethernet)</li> <li>▶ Terminal ID (Default : 1)</li> <li>▶ Server Address (Default : 192.168.0.2)</li> <li>▶ Port Number (Default : 7332)</li> <li>▶ Encrypt (Default : DES)</li> <li>▶ Ping Period (Default : 10 seconds)</li> </ul>
	2. TCP/IP	<ul style="list-style-type: none"> <li>▶ DHCP (Default : Not Use)</li> <li>▶ IP Address (Default : 192.168.0.3)</li> <li>▶ Subnet Mask (Default : 255.255.255.0)</li> <li>▶ Default Gateway (Default : 192.168.0.1)</li> <li>▶ Primary DNS</li> </ul>
5. UI	1. Sound	<ul style="list-style-type: none"> <li>▶ Sound Type (Default : Effect Only)</li> <li>▶ Volume (Default : 1)</li> </ul>



	2. Display	<ul style="list-style-type: none"> <li>▶Language (Default : English)</li> <li>▶LCD Brightness (Default : 3)</li> <li>▶Main Display (Default : Analog Clock)</li> <li>▶Waiting Time (Default : 3 Min)</li> <li>▶Screen Saver</li> <li>▶Date (Default : System Date)</li> <li>▶Time (Default : System Time)</li> <li>▶User Picture (Default : No)</li> </ul>
6. USB	1. User Download	
	2. User Upload	
	3. Log Download	
	4. F/W Update	
7. Initialize	1. Delete User	
	2. Delete Log	
	3. Init Option	
	4. Restart	

### 3.3. User

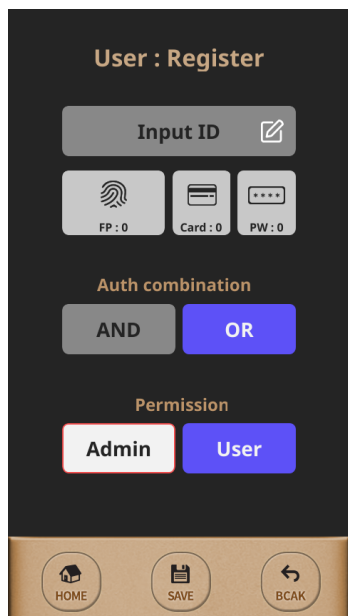
When you select the **[User]** at the main menu, the following window appears.



The administrator can register, delete, modify, and search for the user by using the [User] menu.

### 3.3.1. Register

The maximum number of users to enroll to the terminal are 200,000 templates for FP users but Card users or PW user can be enrolled up to 500,000 users. For example, when 10,000 users have 200,000 FP templates totally stored on the terminal, 490,000 users can register with the Card or PW additionally.



1. To register a new user to the terminal, select [Menu] → [User] → [Register] in order.
2. Insert the User ID you want to register after pressing the button "Input ID".
3. When selecting the button [Admin] from [Permission], this user's authority will be changed. Basically, there are two buttons to select the user's privilege between administrator and normal user.

The first registered user from terminal will be an administrator automatically.

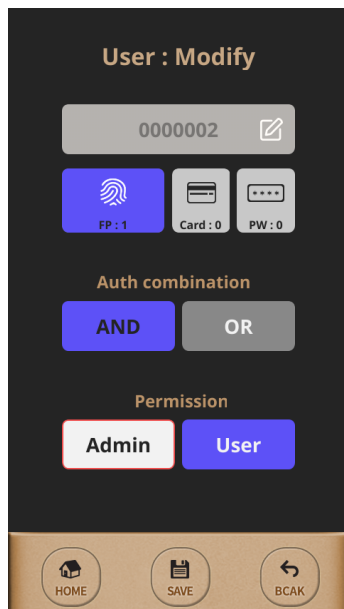
Administrator and normal user have the different authority as below.

- User : Only control the access door.
- Admin : Access door + Enter the menu mode of terminal

To finish registration of user from the terminal, at least more than one Auth method should be registered among 'FP', 'Card', and 'PW'. And then the user will be registered when pressing the button [SAVE] after selecting 'Auth combination'.

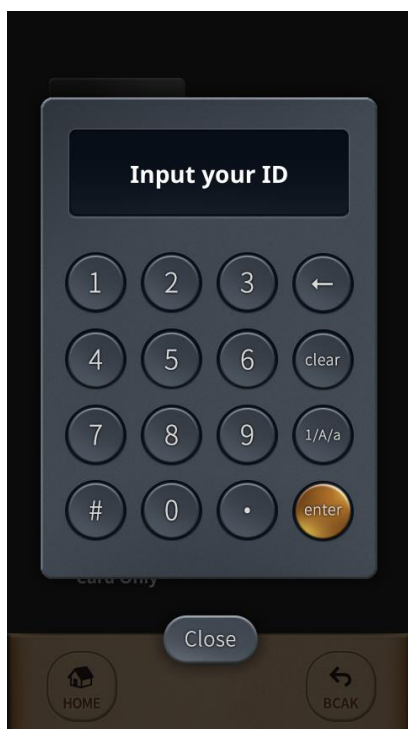
### 3.3.2. Modify

When modifying the registered user from the terminal, 'Group', 'Permission', 'FP', 'Card', 'PW', 'Auth combination' can be modified freely except 'User ID' because it is a unique identifying number so that it couldn't be modified after registration. And also it is possible on Standalone mode which the network type is 'Not Use'. So you have to modify the registered user from the Server software on Network mode.



1. To modify the registered user from the terminal, select [Menu] → [User] → [Modify] in order. And then the user information will be shown as left picture after inserting the User ID to modify.
2. To finish modification of user info from the terminal, press the button [SAVE] after modifying the user info.

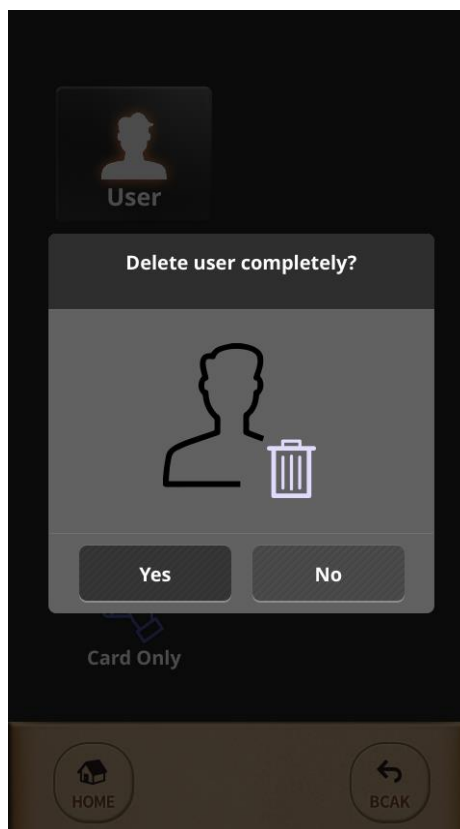
### 3.3.3. Delete



The user ID to delete and select [Yes] button. Select [Close] button to delete and go back.

If inserting the invalid user ID or unregistered user ID, the error message is displayed.

If inserting the valid ID or registered ID, the message is displayed as below.

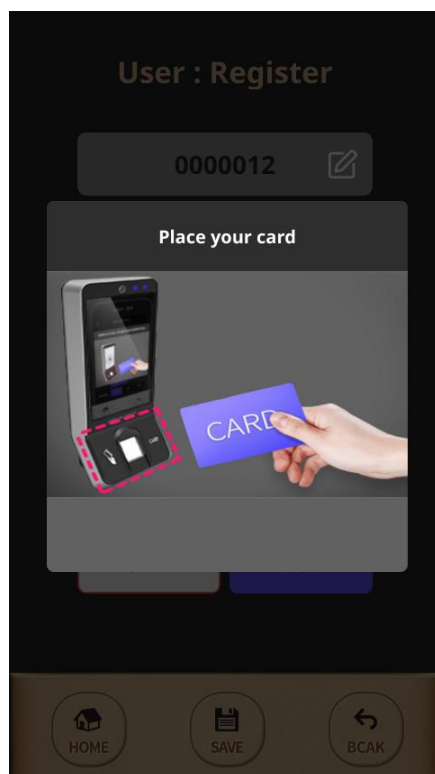


### 3.3.4. List

To query the registered user list from the terminal, select [Menu] → [User] → [List] in order.

### 3.3.5. Card Only

The model "UBio-X Slim" realizes more convenient to control the door by Card only without using fingerprint or password. The button [Card Only] is used easier to enroll the card users continuously but this feature should be worked under network mode.



To enroll the card users seamlessly from the terminal, select [Menu] → [User] → [Card Only] in order.

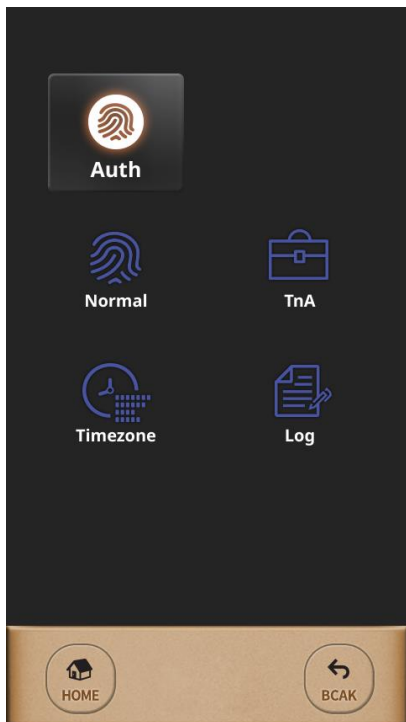
And then the message "Place your card" will be shown as left picture.

If swiping new card to the terminal, the card user can be enrolled easily as creating a new User ID automatically.

To authorize with the registered card, you can swipe the card from the terminal without inserting User ID.

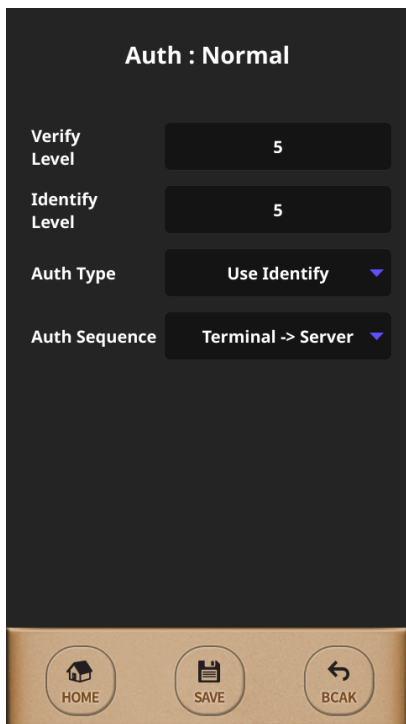
### 3.4. Auth

Select [Menu] → [Auth] in order from the terminal, the below picture will be shown.



This menu is to set the auth-related option, TNA mode and whether to use the card.

#### 3.4.1. Normal



##### Verify Level / Identify Level

Security Level for FP is adjustable per each Auth Type. For Verify Level (1:1), default is 5 but it can be selected from 1 to 9. For Identify Level (1:N), default is 8 but it can be selected from 5 to 9. If the security Level is too higher, FRR (False Rejection Rate) is more increasing but if it is too lower, FAR (False Acceptance Rate) is more increasing. So, please use the default value if not special case. These are applied to all users except the user has the individual setting on registration.

##### Auth Type

The model "UBio-X Slim" supports both 1:1 and 1:N Auth Types. When using 1:1, insert the User ID or swipe his registered card before placing his registered finger. But using 1:N, place your finger without input User ID or swipe the Card because matching the fingerprint against all user data. However, if you want to be authenticated faster, to use 1:1 is better than to use 1:N even 1:N is more convenient than 1:1.

##### Auth Sequence

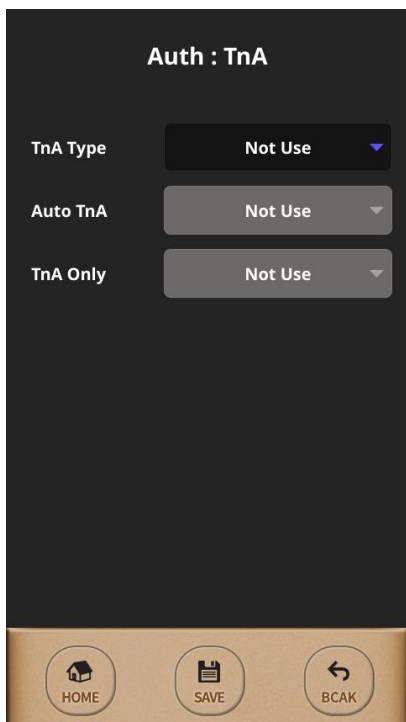
There are 4 Auth Sequence modes in "UBio-X Slim". And these are operated with Server software, Access Manager Professional program.

- Server → Terminal : Authentication starts by Server and if it is

not searched, authentication will be started by Terminal automatically.

- Server Only : Authentication should be done by Server only.
- Terminal → Server : Authentication starts by Terminal and if it is not searched, authentication will be started by Server automatically..
- Terminal Only : Authentication should be done by Terminal only.

### 3.4.2. TnA



When using TnA mode, the user should press the Function key before authentication, and then the authentication log will be transferred with the pressed function key number.

It makes the TnA feature manage efficiently when pressing each Function key for employee’s situation.

There are three TnA types in “UBio-X Slim” and it is selectable among ‘Simple’, ‘Normal’, and ‘Expand’.

‘Simple’ type has 2 Function keys, ‘Normal’ type has 4 Function keys, and ‘Expand’ type supports the multiple Function keys up to 63keys.

The ‘Simple’ type has ‘Attend / Leave’ and ‘Normal’ type has ‘Attend / Leave / Out / In’, whose function keys are fixed.

In case of the ‘Expand’ type, you can set the function keys freely depending on S/W requirement that you connect.

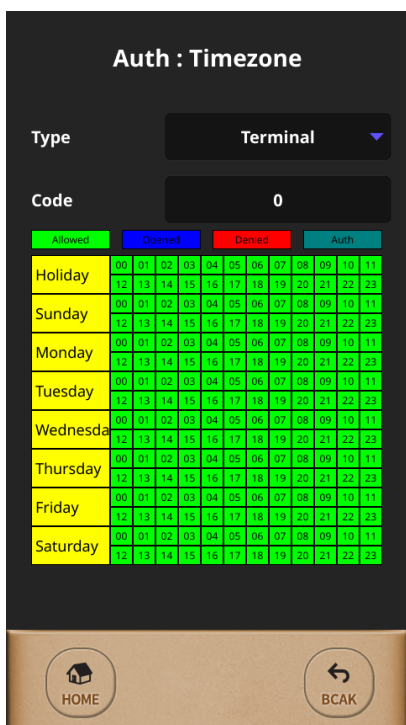
In case of ‘Auto TnA, authentication is performed with the selected type when the function key is input. If not, authentication is performed with the function key value type previously input.

If you only want to allow access through TnA authentication, go to [TnA Only] > select ‘Use’. In this case, you should select the function key to open the door.

When finishing the setting, select [SAVE] button to save the current setting value.

\*When you set ‘Use’ in [TnA Only], please be caution that it doesn’t perform the authentication process if you don’t press the function key.


### 3.4.3. Timezone



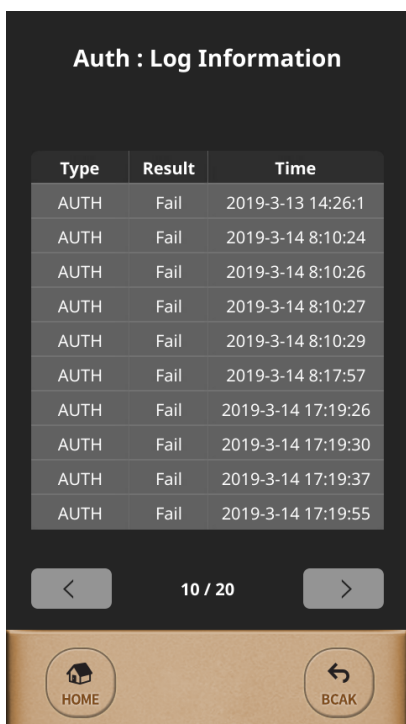
If using the feature terminal's timezone, it is possible to grant to access or deny to access per each period or per each time. But this feature can be used to set the door access on Network mode only.

It is possible to set the timezone for each terminal or for each user with selecting the button [Type].

The time table consists of Day and Time as the left picture and it can be checked all the terminal's timezone or a specific user's timezone.

 Caution for setting the timezone  
The timezone is only set through Access Manager Professional and it is not possible to set it from the terminal.

### 3.4.4. Log

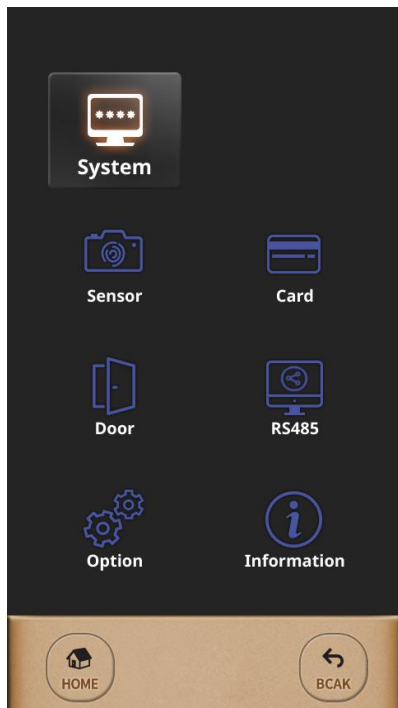


This is the feature to check the authentication logs for the terminal's user.



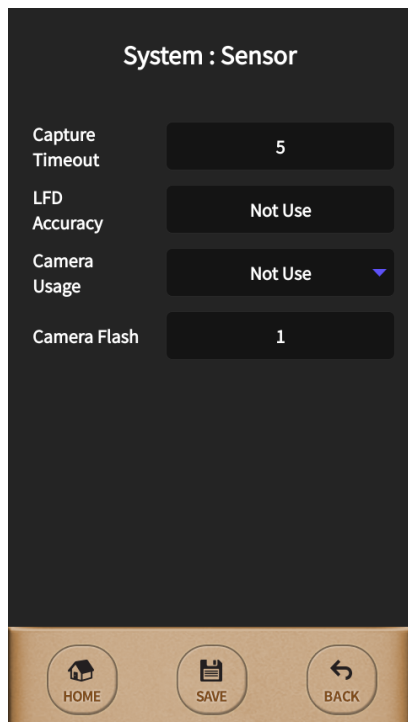
### 3.5. System

Select [Menu] → [System] in order from the terminal, the below picture will be shown.



This menu is to configure Sensor, Card, Door, Option for Door and check the terminal's information.

#### 3.5.1. Sensor



This menu is used to set the Sensor Mode, Capture Timeout, LFD Accuracy, Camera Usage and Camera Flash. And when selecting the terminal basic sensor setting, this setting will be applied to all users who are registered as selecting not individual sensor setting.

##### Capture Timeout

This is the standby time for capturing fingerprint and it is adjustable from 3 to 9 seconds. (Default : 5 seconds)

##### LFD (Live Finger Detection) Accuracy

This menu is used to set the level to inspect the fake finger and to use it. This is graded from 0 to 3 as below. 'Not use' (0), 'Low' (1), 'Middle' (2), 'High' (3)

##### Camera Usage

This menu is set the condition to use the camera. For example, when selecting "Success", the camera will be operated in case the authentication succeeds and when selecting "Fail", the camera will be operated in case that the authentication fails.

And when selecting "All", the camera will be operated regardless of authentication success or failure.

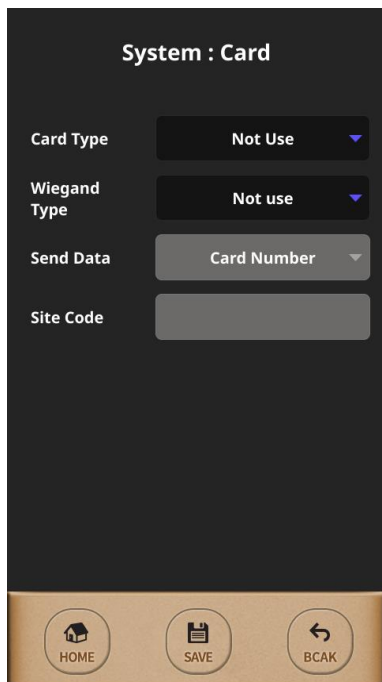
When selecting 'Not Use', the fingerprint image or other suitable image will be displayed.

\* If the authentication type is successful but the authentication type is complex, the image displayed in the result window is the image that matches the last authentication type.

**Camera Flash**

When taking pictures with the camera, if the surroundings are dark, the camera flash turns on and you can adjust the brightness of the camera flash to the camera flash value. '0' does not turn on the camera flash. The flash brightness is bright in the order of 1 <2 <3. The camera flash level value is valid when it is not "Not Use" in the shooting item.

3.5.2. Card



This menu is used to set the card authentication for terminal's user.

**Card Type**

It is selectable among 'Not Use', 'EM', 'MIFARE', 'HID Proxy 26 Bit', 'HID Proxy 35 Bit', 'HID Proxy 37 Bit', 'iClass 26 bit', 'iClass 35 bit', and 'iClass 3 7bit'.

**Wiegand Type**

You can select whether to use Wiegand Out and the bit type. Generally, if the card module is Mifare, it selects 34 bit and if the card module is EM 26 bit, it selects 26 bit.

**Send Data**

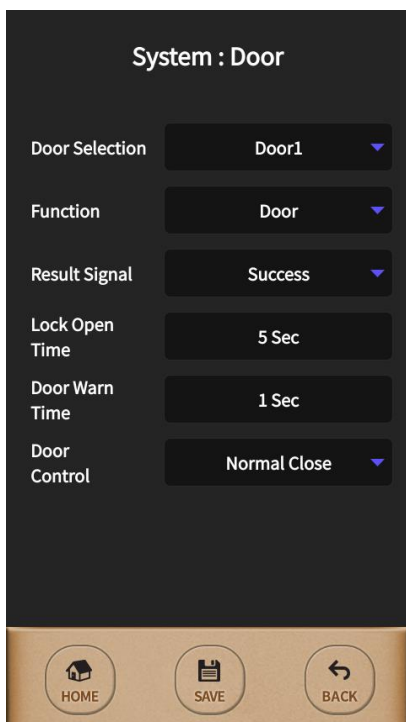
You can select Wiegand Out information between 'Card Number' or 'SiteCode + User ID' option. When selecting 'User ID', 4 digits User ID will be out after authentication success via Wiegand Out but when selecting 'Card Number', the card serial number (CSN) will be out.

**Site Code**

This option is used only on selecting 'User ID' and it can be out differently per each Wiegand bit between 26bit and 34bit as below.

- Site Code for Wiegand 26bit : 0 ~ 255
- Site Code for Wiegand 34bit : 0 ~ 32767

### 3.5.3. Door



There are two functions on this menu. One is able to control two doors and the other is able to support the fire alarm or lighting lamp after connecting to each external device.

**Door Selection**

You can select 'Door1' or 'Door2'.

**Function**

You can set the option among 'Not Use', 'Door', 'Fire Alarm', 'Light Alarm', and 'Motor Lock'.

❖ When Door1 is set to 'Motor Lock', Door2 is also automatically set to 'Motor Lock'. In the opposite case, when Door2 is set to 'Motor Lock', Door1 is also automatically set to 'Motor Lock'.

When 'Motor Lock' is set, the 'Result Signal', 'Lock Open Time', and 'Door Warn Time' of Door2 are ignored.

**Result Signal**

The lock can be set to operate depending on the authentication result setting. When you select 'Success', the door opens in case of authentication success and when you select 'Fail', the door opens in case of authentication fail.

**Lock Open Time**

You can set the lock open time.

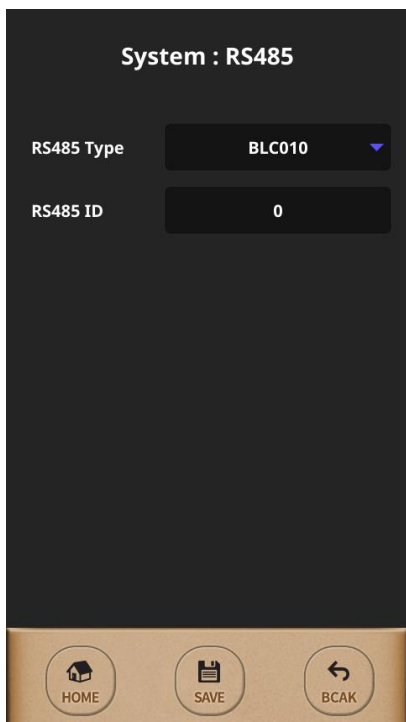
**Door Warn Time**

You can set the time to send the warning if the door opens too long.

**Door Control**

You can set the door control between NC (Normal Close) and NO (Normal Open).

### 3.5.4 RS485



This menu is used to set the external device is communicated to "UBio-X Slim" via RS485.

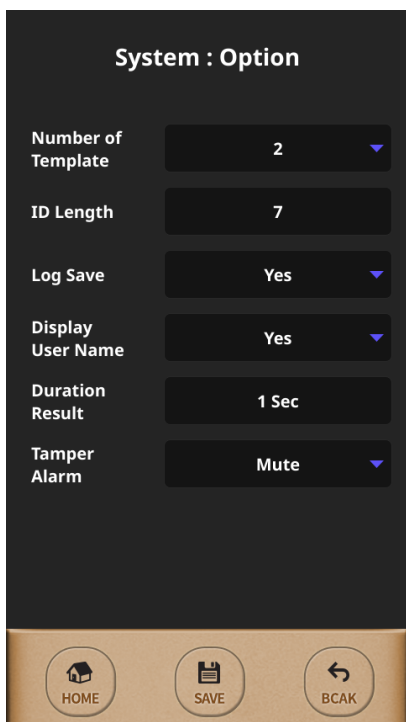
**RS485 Type**

It is selectable between 'Not Use' and 'BLC010'.

**RS485 ID**

When using RS485 communication with the external controller, you can set the RS485 ID 0 to 7.

### 3.5.5 Option



This menu is used to set other terminal options as the left picture. The option 'Number of Template' decides the fingerprint count and the option 'ID Length' on user enrollment. So all registered users on terminal must be deleted before changing these two options.

**Number of Template**

It is selectable between 1 to 2. (Default : 2)

**ID Length**

It is selectable from 4 to 20. (Default : 4)

**Log Save**

It decides to save the log for authentication result.

**Display User Name**

It decides to display the user name in case of authentication success.

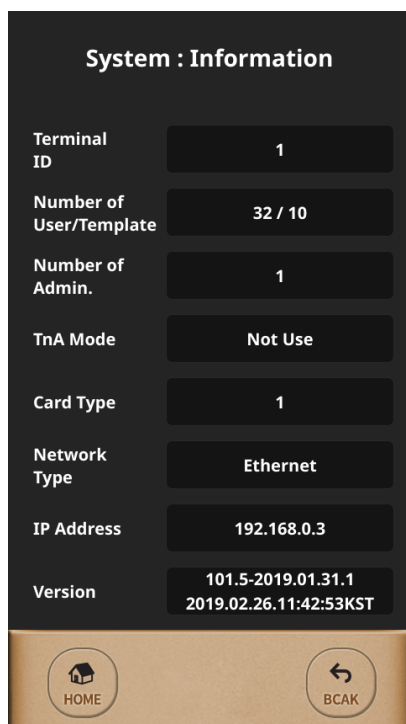
**Duration Result**

It decides the displaying time for the authentication result.

**Tamper Alarm**

It decides to set mute or tamper alarm in case of tamper open. (Mute / Use)

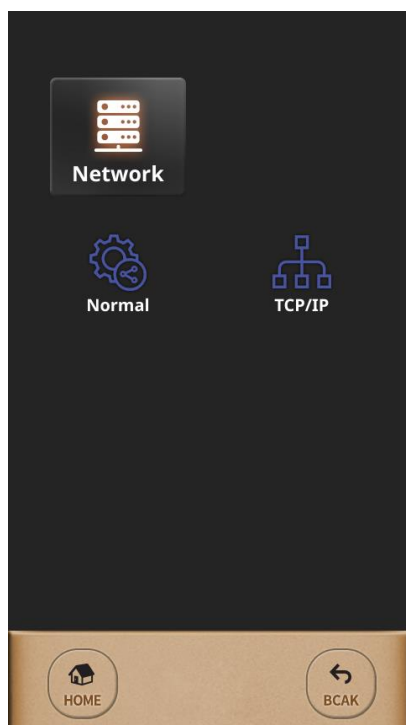
### 3.5.6 Information



You can set the terminal ID, the network mode, the number of users and overall terminal information. In this menu, you can check the information but you cannot change the setting. The version information is shown as 'FW-Kernel version-Root file system version'.

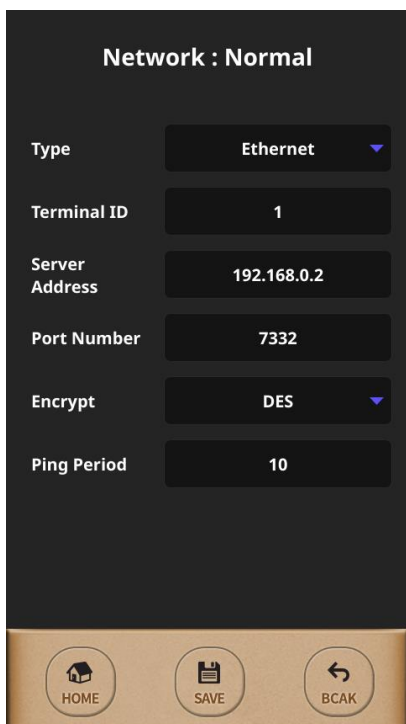
### 3.6. Network

Select [Menu] → [Network] in order from the terminal and the below picture will be shown.



There are two sub menus 'Normal' and 'TCP/IP' under [Network] as the left picture.

### 3.6.1. Normal



There are two modes 'Network mode' and 'Standalone mode' on "UBio-X Slim" model. And the 'Network mode' is divided by 'Wireline' and 'Wireless'.

**Type**

It is selectable among 'Not Use', 'Ethernet', and 'WIFI'. If selecting 'Not Use', terminal is worked as a Standalone mode which is operated independently without connecting network. In this case, authentication is proceeded on the internal database of the terminal only. But if selecting 'Ethernet' or 'WIFI', terminal is worked as a Network mode which is cooperated with the Access Manager Professional program. Meanwhile, the mode 'WIFI' is currently not supported but it will be added on next.

**Terminal ID**

Terminal ID should be given differently from 1 to 2000 because it is the unique ID. It is not duplicable.

**Server Address**

It should be inserted for IP address of the Server PC which is installed the Access Manager Professional.

**Port Number**

It should be inserted for the communication port number between server to terminal.

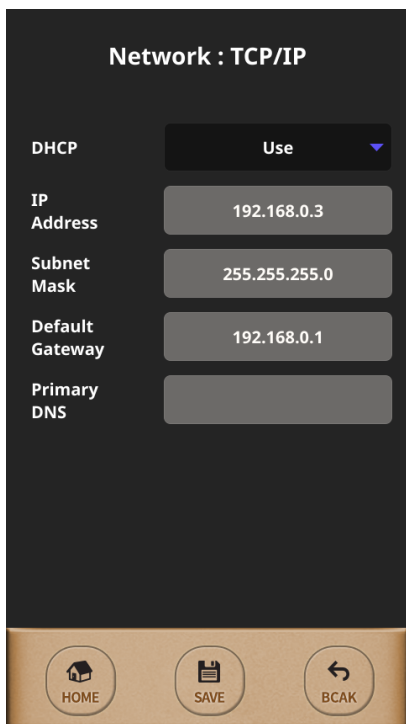
**Encrypt**

You can set the encryption type to send the data between terminal and server. There are 'DES' and 'AES256' in the encryption type.

**Ping Period**

It decides the polling duration to check the communication status between server and terminal. It is given from 2 to 20. (Default : 10 seconds)

### 3.6.2. TCP/IP



The options on [TCP/IP] should be configured properly to connect to the server after selecting 'Network mode'.

#### DHCP

It is decided when selecting 'Use' between 'Use' and 'Not Use'. When using 'DHCP', the terminal IP address cannot be changed. Because it obtains automatically.

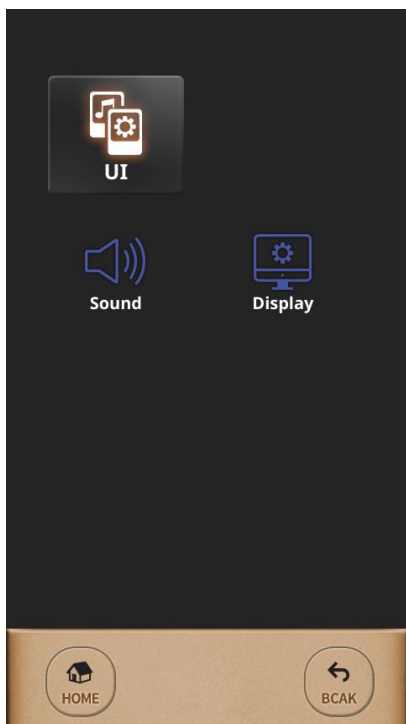
When not using 'DHCP', 'IP Address', 'Subnet Mask' and 'Default Gateway' for terminal should be given manually.

To obtain them, contact the network administrator on the customer site.

**Tip** What is DHCP (Dynamic Host Configuration Protocol)?  
This feature is to assign automatically the IP address of the terminal including Subnet Mask and Gateway by DHCP Server to use TCP/IP communication. So if it is "On", it makes you use more conveniently.

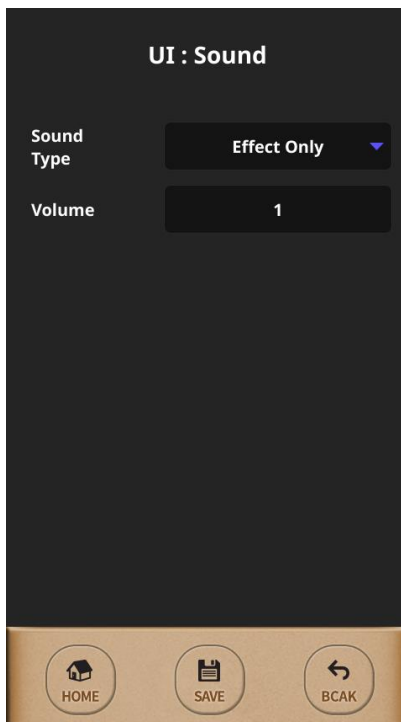
### 3.7. UI

Select [Menu] → [UI] in order from the terminal, the below picture will be shown.



This menu is used to set the terminal display option and sound option as the left picture. And it makes you to change freely as customer wants for the terminal's main display, language, date & time, sound, and etc.

### 3.7.1. Sound



This menu is used to set the sound type about both voice & effect and control its volume.

#### **Sound Type**

If you want the sound as a mute, you can select 'Not Use'. Also, you can select 'All', 'Voice Only' and 'Effect Only' as you want.

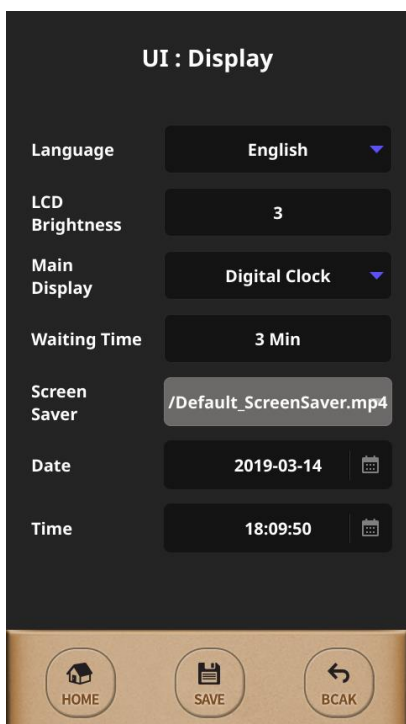
#### **Volume**

You can select the volume from 0 to 5. (Default : 1)

You can control the volume as you want.



### 3.7.2. Display



#### Language

You can select the language as you want.

Below is the supported language.

'English', 'Korean', 'French', 'Spanish', 'Portugues', 'Indonesian', 'Persian', 'Japanese', 'Russian', 'Arabic'

#### LCD Brightness

This is adjustable from 1 to 5 and default is 3.

#### Main Display

It is selectable among 'Analog Clock', 'Digital Clock', and 'Logo Image'.

#### Waiting Time

If there is no any input in the setting time, the screen saver is operated.

#### User Picture

You can set whether to show the user's photo set in server in authentication result window.

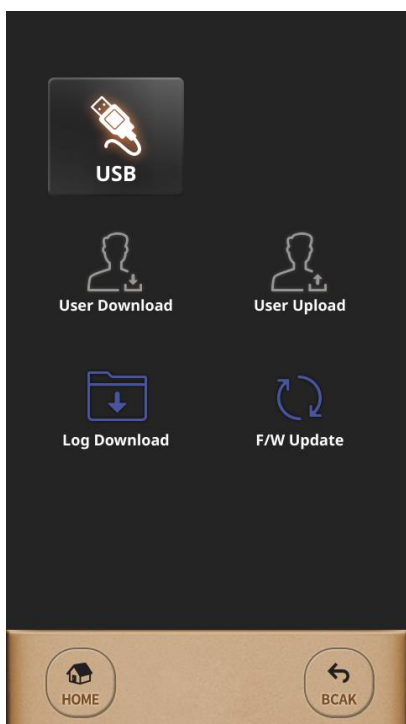
You can set the user's photo only when you use in network mode.

#### Date & Time

Terminal's data & time is adjustable manually on the Standalone mode.

### 3.8. USB

Select [Menu] → [USB] in order from the terminal and the below picture will be shown.



This menu can be used to upload or download the user's information and log information after connecting the terminal with USB memory.

Basically, in the network mode, you can only download the log. Meanwhile, in the standalone mode, you can download the log and upload/download the user's information.

❖ Please use the USB file system format as FAS32. NTFS file system can be fail in case of the user upload/download and the log download.

❖ The time can be different after user download and log download because of the system difference.

Ex) Current time 15:00 User download  
 When checking in Windows, it shows 06:00.  
 When checking in Linux, it shows 15:00.

### 3.8.1. User Download

If the USB memory does not exist or there is a file named Slim\_UserDB.ndb when you select [User Download], an error window is displayed. Otherwise, a pop-up window will appear asking whether to proceed to download the user. If you select [Yes], all user information of the device is saved in the user folder on the USB memory under the file name Slim\_UserDB.ndb (user / Slim\_UserDB.ndb). completing the download, unmount the USB memory. If you download or upload the user again, please remove the USB memory and insert it again.

This file can be read from the Access Manager Professional and stored on the server.

User download feature is only supported in standalone mode.

### 3.8.2. User Upload

When you select [User Upload], if the USB memory does not exist or there is no file named Slim\_UserDB.ndb, an error window appears. If not, a pop-up window will appear asking whether to proceed to download the user. If you select [Yes], the user data is uploaded to the device in a file called Slim\_UserDB.ndb (user / Slim\_UserDB.ndb) in the user folder on the USB memory. If the user ID is duplicated, the user information is not recorded on the device.

The File name should be set as Slim\_UserDB.ndb for normal upload.

The user upload function is only supported in standalone mode.

### 3.8.3. Log Download

If you download the log information of the device to a USB memory, you can download all logs or only the unspent logs.

When all logs are downloaded, all logs in the terminal are saved to USB memory in either network mode or standalone mode.

After selecting [Log Download] button, you can select the range of download date and select which log to download.

The log information is saved as Slim\_Log\_1.nlg in the log folder in the USB memory.

If you download the new log information, it downloads Slim\_Log\_1.nlg, Slim\_Log\_2.nlg in order.

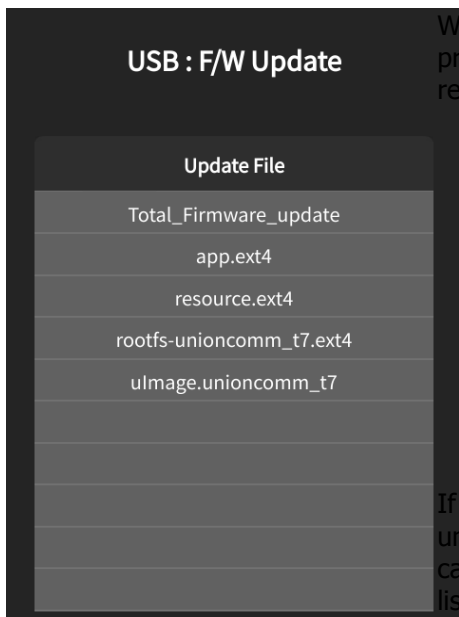
The log information saved in USB can be imported and then saved in server.

After completing the download, unmount USB memory.

If you want to download the log again, take USB out and insert it again.

---

### 3.8.4. F/W Update



When you select the FW file to update in the list, the update proceeds as below. After completing this process, the terminal reboots.

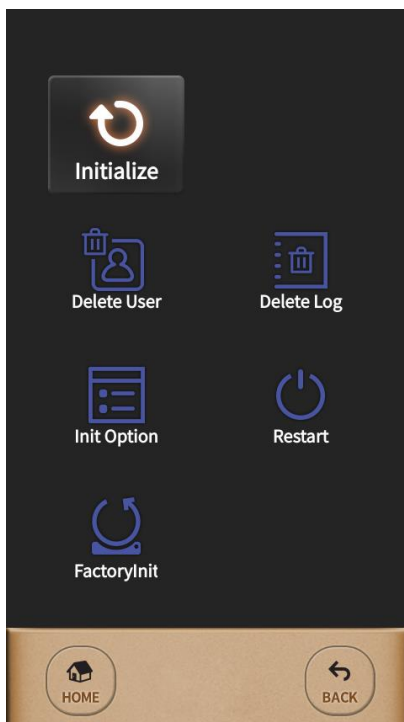


If you want to download app.ext4, resource.ext4, rootfs-unioncomm\_t7.ext4, uImage.unioncomm\_t7 files at a time, you can select 'Total\_Firmware\_update' which is in the first line in the list.

For 'Total\_Firmware\_update', all app.ext4, resource.ext4, rootfs-unioncomm\_t7.ext4, and uImage.unioncomm\_t7 should exist. If any of the four files is missing, Total\_Firmware\_update will not appear.

### 3.9. Initialize

Select [Menu] → [Initialize] in order from the terminal and the below picture will be shown.



This menu is used to set back to the factory format for all terminal's user data, stored log data and configured options. So please be cautious for these initialization because it is not recoverable.

**Delete User**

-It deletes all the users saved in terminal.

**Delete Log**

-It deletes all the logs saved in terminal.

**Init Option**

-The setting value in the terminal is initialized to default value.

**\*If there are users in terminal, it is not available to initialize the option.**

**Restart**

-It reboots the terminal.

**FactoryInit**

-The terminal setting is all initialized as a factory initialization.

-After FactoryInit, the terminal automatically reboots.

## 4. How to use terminal

### 4.1. How to open the door

There are two below methods to open the door with authentication from the terminal basically.

#### 1:1 Verification

This 1:1 Verification can access the door much faster regardless of the number of users on the terminal because it compares only between the inserted fingerprint to the stored fingerprint of the pressed User ID.

As shown in the figure below, press the button [ID] to input the registered User ID first and then input the fingerprint or password after pressing the button [enter].



## 1:N Identification

This method is that the registered fingerprint is placed on the fingerprint sensor in the main screen without inserting User ID. But it can take somewhat long time to authenticate because it compares the inserted fingerprint to all fingerprint data in spite of much more convenient than 1:1 Verification.

### ① Fingerprint Authentication

Insert the fingerprint on the fingerprint sensor without inputting User ID.



### ② Card Authentication

Swipe the Card on the Card Sensing Area without inserting User ID.

If the User ID should be pressed certainly before inserting fingerprint, please check terminal option 'Use Identify' is not selected.

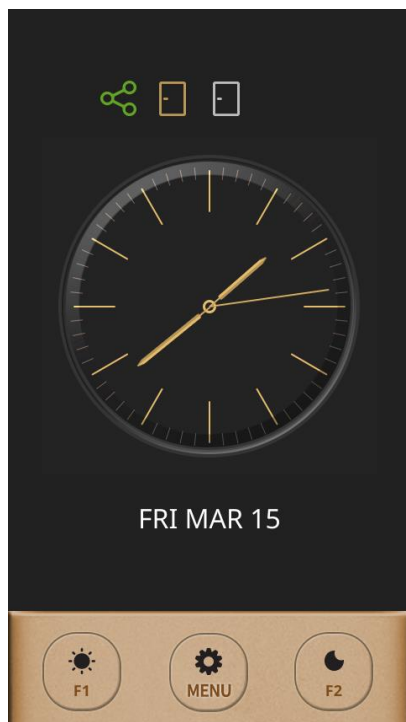


'1:N Identification' for password user is same to '1:1 Verification'.

## 4.2. How to punch for TnA

In TnA mode, a user must click function key before authentication. And the log is transferred to server with information that function key is selected. If the function key is not pressed on authentication, it is possible not to record the TnA type firmly for user's 'Attend', 'Leave', 'Out', 'In'. So it should be pressed for each case before authentication.

"UBio-X Slim" model displays the Function keys on the bottom side as following pictures.



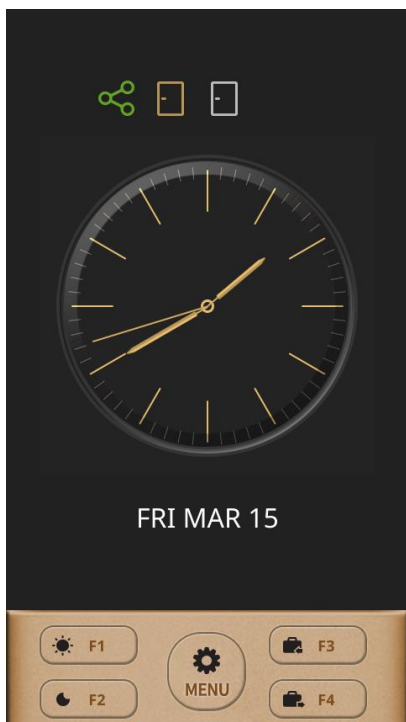
### Simple TnA mode

In this mode, the User ID is pressed after pressing Function key and then try to authenticate.

The function keys in Simple TnA mode are defined as below.

- F1: Attend
- F2: Leave

If the function key is pressed before authentication, the pressed key "F1" or "F2" will be recorded on the authentication logs so that they are used on Time & Attendance software.



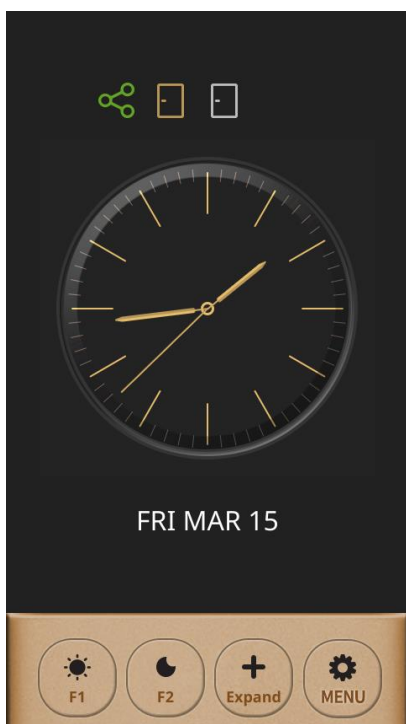
**Normal TnA mode**

In this mode, the User ID is pressed after pressing Function key and then try to authenticate.

The function keys in Normal TnA mode are defined as below.

- F1: Attend
- F2: Leave
- F3: Out
- F4: In

If the function key is pressed before authentication, the pressed key "F1" to "F4" will be recorded on the authentication logs so that they are used on Time & Attendance software.



**Expand TnA mode**

In this mode, the Function keys on the bottom side is displayed as the left picture.

When pressing the function key 'Expand', enter the function key and ID to authenticate.

**TIP** If you want to use 1:N identification on TnA mode, try to authenticate directly after pressing Function key without inserting User ID.

**TIP** When selecting 'TnA Only' to use, the Function key MUST be pressed for authentication.

# FCC Supplier's Declaration of Conformity

## Nitgen / Ubio-X Slim

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, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Distributed by



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

---