

User Manual | Version eng-1.0



Revision History

Explanation of Term

Admin, Administrator

- A user who can change device settings and modify the operational environment.
- If an administrator is registered, authentication will be required when accessing the Admin menu.
- If there's no administrator, anyone can modify settings. It is recommended to register at least one administrator
- Admins have the privilege to change device system settings, so caution is needed when registering or managing them.

* Admins have the privilege to change device system settings, so caution is needed when registering or managing them.

1 to 1, Verification

- The system verifies the user by checking whether the entered card or password matches the information registered to the user.

Authentication Method

- This refers to various form of authentication methods created by combining RF(Radio Frequency) authentication, mobile card(BLE/NFC) authentication.

* Example: Card or PIN – Authentication using either Card or PIN

Table of Contents

Revision History	1
Explanation of Term	2
Table of Contents	3
Chapter 1 Pre-use Verification	4
01 Cautions	5
Cautions in Installation	6
02 Terminal Specific Names	7
03 Buzzer Sound/LED Guidance	8
Buzzer Sound/LED	8
Status LED	8
Chapter 2 Product Description	10
01 Product Features	11
UBio-X Tag	11
Compliance & Certification	11
Information	11
Providing Various Registration and	11
Authentication Methods	11
02 Product Composition	12
Components	12
Cables	13
03 System Configuration Diagram	14
Standalone Usage (Access)	14
Connection to PC Server	14
(Access/T&A/Meal)	14
04 Specifications	15
Chapter 3 Settings	16
01 UBio-Link Connection Method	17
Firmware Update Method	17
RS485 Settings	17
Chapter 4 Terminal Usage Instructions	18
01 Connection to Server	19
02 Keypad Usage Guide	19
03 Change Authentication Mode	20
T&A (Time&Attendance)	20
Meal Management	20

Chapter 1

Pre-use Verification

01	Cautions	5
	Cautions in Installation	6
02	Terminal Specific Names	7
03	Buzzer Sound/LED Guidance	8
	Buzzer Sound/LED	8
	Status LED	8

Warning



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

→ There is a risk of malfunction and electric shock.



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

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



Prevent children from touching the device recklessly.

→ There is a risk of child safety accidents or malfunctions.



Do not place flammable objects near the device.

→ It may cause a fire.

Caution



Do not install in places exposed to direct sunlight.

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



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

→ There is a risk of malfunction.



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

→ There is a risk of electric shock and fire.



Do not place magnetic objects close to the device.

→ There is a risk of malfunction.



Do not dirty the fingerprint input area.

→ The fingerprint cannot be recognized correctly.



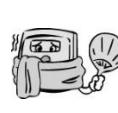
Do not spray insecticides or flammable sprays on the device.

→ There is a concern about deformation and discoloration.



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

→ Product breakage may cause malfunctions.



Do not install in places with extreme temperature changes.

→ There is a risk of malfunction.
→ Be cautious of burns when using the product.

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

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

I Cautions in Installation

- Be extremely careful of incorrect wiring when using a high-capacity power supply, as miswiring may cause fire, electric shock, or device damage.
- Do not install or repair the product on your own, as unauthorized handling may cause fire, electric shock, injury, or void the warranty service.
- Do not install the device in locations exposed to direct sunlight, humidity, dust, soot, or gas leakage risks, as these environments may cause fire or electric shock.
- Do not install the device in areas exposed to direct sunlight or strong heat sources, as excessive heat may cause overheating, fire, electric shock, or device damage.
- Do not install the device in high-temperature environments, as excessive heat increases the risk of fire or electric shock.
- Do not install the device in wet or damp environments, as moisture may cause electric shock or product malfunction.

- If the displayed precautions are not followed, there may be a risk of injury or property damage to the user.
※ We are not responsible for accidents and damages that occur due to the failure to use the product as instructed in the user manual.

02 | Terminal Specific Names

Chapter 1
Pre-use Verification



- For detailed installation instructions for the product, please refer to the UNION biometrics website (<http://unionbiometrics.com>).

I Buzzer Sound/LED

Voice guidance	LED guidance	Operation Status
“Be—Beep”	Blue LED blinking	Authentication success
“Be—”	Red LED blinking	Authentication failure
“Be—Be—Beep”	White LED blinking	During ID/PW input cancellation
“Be—Be—Be—Be—Be—”	Blue LED blinking at 0.2-second intervals(10-second timeout)	When card is presented
“Be—Be—Be—Be—Be—”	Keypad backlight blinking at 0.2-second intervals (10-second timeout)	When waiting for password input (PW mode)
“Be—Be—Beep(5-second interval)”		When cover is opened
“BeepBeBeep BeepBeBeep BeepBeBeep” (5-second interval)		Door Opened Warning Sound

- In Card Standby Mode, only card authentication is allowed. In Password Standby Mode, only password input is allowed.
- If a user attempts authentication using a different method than the one currently active, the system will automatically ignore the attempt.

I Status LED

LAN Connected

LED guidance	Operation Status
Red LED blinking	Server disconnected (normal standby mode)
Blue LED on	Server connected
Blue LED blinking	Server & RS485 both connected
White LED blinking	Server connected, RS485 disconnected
Blue + Red LED blinking	Server disconnected, RS485 connected
Alternating Blue + White LED blinking	Server & RS485 both disconnected

- LED status changes automatically depending on the connection state, and manual control is not available.

LAN Disconnected

LED Guidance	Operation Status
Blue LED On	Normal state
Blue LED Blinking	RS485 connected
Blue + White LED Alternating Blinking	RS485 disconnected

Network Disabled

LED Guidance	Operation Status
White LED On	Normal state
Blue LED Blinking	RS485 connected
White LED Blinking	RS485 disconnected

Others

LED Guidance	Operation Status
White LED On during feature use (Card mode or ID/PW standby mode)	Using T&A/Meal function keys
Red LED + Keypad LED On (temporary blinking if cover switch LED turns on)	During reboot
Pink LED Blinking	Configuration App (UBio-Link) connected
Pink LED On (Displayed when update is in progress after download is complete)	Firmware update in progress (FW Update)

Settings Precautions

- Check the server connection status after establishing an Internet connection.
- RS485 connection can be verified by selecting “LC10/LC15” or “OSDP” in the settings menu.
- Day/Night mode for network time synchronization can be switched ON/OFF in the settings.
- T&A and meal functions operate normally only when each function is assigned in the configuration menu.

※ Authentication is not available while UBio-Link is connected. Please proceed with authentication after the connection is complete.

Chapter 2

Product Description

01	Product Features	11
	UBio-X Tag	11
	Compliance & Certification Information	11
	Providing Various Registration and Authentication Methods	11
02	Product Composition	12
	Components	12
	Cables	13
03	System Configuration Diagram	14
	Standalone Usage (Access)	14
	Connection to PC Server(Access/T&A/Meal)	14
04	Specifications	15

I UBio-X Tag

UBio-X Tag is a slim and compact RFID access device that can be easily installed in narrow spaces and on thin frames. It supports multiple authentication options and ensures enterprise-level security with IP67/IK08 -rated durability, providing reliable performance in both indoor and outdoor environments.

> Multiple Authentication

Supports card, mobile card (NFC, BLE), and PIN (**Keypad model only**)

> Dual Card Reader

Supports both 13.56MHz and 125kHz card authentication on a single device

> TCP/IP Communication Support

Direct connection to a server database for stable network-based operation

➤ **BLE-based setup app (UBio-Link)**

Supports device setup and user management via UBio-Link

I Compliance & Certification Information

	Product : UBio-X Tag
	Model : UBio-X Tag (KP)
	Applicant : UNION biometrics Co., Ltd.
	MFG. Date : See marking
	Manufacturer / Country : UNION biometrics Co., Lt d. / Korea
	Cert. No. : R-R-UCC-UBio-XTag
	Module No. : R-C-ULX-NORA-W401

I Providing Various Registration and Authentication Methods

Card	Card registration / Card authentication
PW	PW registration / PW authentication
Card OR PW	Card, PW registration / Card authentication / PW authentication after entering ID
Card and PW	Card, PW registration / Authenticate your PW after card authentication / Enter your ID and authenticate your PW after authenticating your card
Mobile Key	Mobile key registration

Warning

- Mobile cards can only be registered on the server.

02 | Product Composition

Chapter 2
Product Description

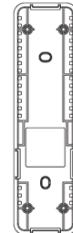
I Components



UBio-X Tag



Wall Bracket (Steel)

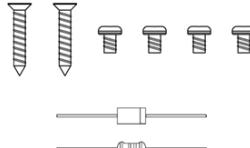


Wall Bracket (Plastic)



Connection Cables (Total 4)

2Pin x 1
4Pin x 1
7Pin x 1
14Pin x 1



4*25 Screws x2
2.6*6 Screws x4
Diode
Resistor



Quick Guide

Warning

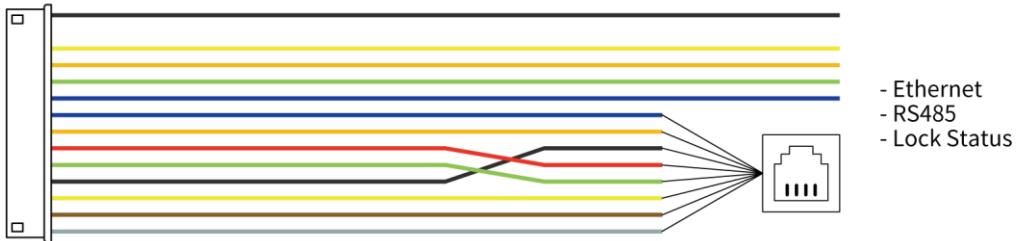
- Components may vary depending on the installation environment.
- For information on product installation, please visit the UNION biometrics website (<https://unionbiometrics.com/>) and check the installation guide.

I Cables

Power Adapter (2P)



Main Cable (14P)



Wiegand Cable (7P)



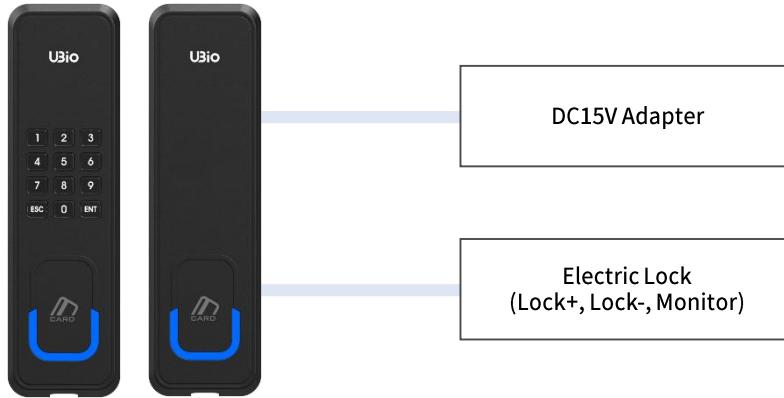
Lock 1 Cable (4P)



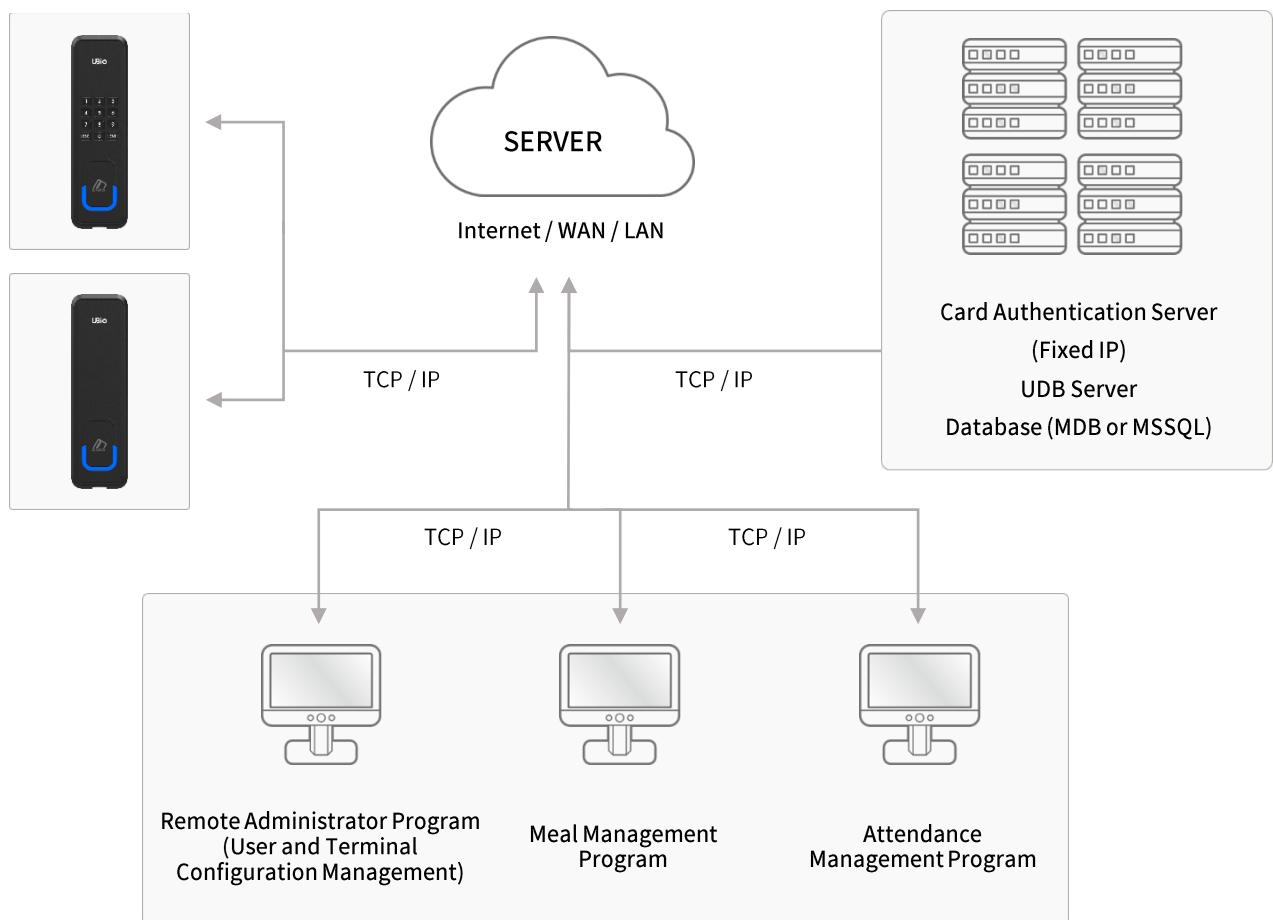
03 | System Configuration Diagram

Chapter 2
Product Description

I Standalone Usage (Access)



I Connection to PC Server (Access/T&A/Meal)



04 | Specifications

Category	SPEC	RMARK
CPU	Cortex A53 Quad Core 1.8GHz)	
MEMORY	eMMC 4GByte	
	256MB RAM	
External Type C USB Supprot	FW Upgrade	
Users	400,000 User / 400,000 Card 10,000,000 Log	
Temperature / Humidity	-20 ~ 60°C / Lower than 90% RH	
AC / DC Adapter	INPUT : Universal AC100 ~ 250V	
	OUTPUT : DC 12V	
POE	INPUT: DC 48V / OUTPUT: DC 12V	Option
Lock Control	EM, Strike, Motor Lock(option), Auto Door	
I/O	2 In (1 Exit, 1 Monitor) 1 Out	
Communication Port	TCP/IP (10/100Mbps)	
	RS-485	
	Wiegand In/Out	
Card Reader	13.56MHz Smart Card Reader, ISO14443A/B, MiFare, Felica, ISO15693 SE iClass(Option), 125KHz RF Card Reader, EM, H iD Prox(Option)	
Keypad	12key	(K), (KP) Model
LED	3 Color (White, Blue, Red)	
Current	Max 1.5A (DC12V) / 0.75A (DC24V)	
SIZE	45 x 157 x 27 (mm)	

Chapter 3

Settings

01	UBio-Link Connection Method	17
	Firmware Update Method	17
	RS485 Settings	17

You can configure the device through the Settings app (UBio-Link).

- > Use Android 10 or higher for installing and running the app.
- > The card format determines how card data is stored. Changing the card format may require re-registering all card users stored in the device. Please choose the format carefully.
※ We recommend using the default card format.
- > When registering users from the server, the card format set on the server must match the card format on the device.

I Firmware Update Method

Firmware updates are supported through UBio-Link BLE and the server.

I RS485 Settings

RS485 settings can be configured through the Settings app (UBio-Link).
After changing the RS485 settings, the device will automatically reboot.

Warning

- It is recommended not to use the monitoring function when using RS485.
- The Lock control function (door lock control) is not supported when RS485 is enabled.

Chapter 4

Terminal Usage Instructions

01	Connection to Server	19
02	Keypad Usage Guide	19
03	Change Authentication Mode	20
	T&A (Time&Attendance)	20
	Meal Management	20

01 | Connection to Server

Chapter 4
Terminal Usage Instructions

Power on the device to begin the booting process. Once the device has fully booted, you can proceed to the next step.

In the Settings app (UBio-Link), configure the network connection. You may select either Wi-Fi or wired Ethernet. For a wired connection, connect the LAN cable to enable communication with the server.

Administrator and user information can be registered through the Settings app (UBio-Link) or from the server.

※ When using DHCP (Automatic IP Assignment), the temporary IP address 255.255.255.255 may be displayed in the Settings app until the device receives a valid IP address from the network.

Warning

- The device automatically performs time synchronization with the server.
- When changing Bluetooth (BT) related settings (BT RSSI, BT Tx Power, etc.) in the Settings app, the Bluetooth connection will be disconnected and must be reconnected.

02 | Keypad Usage Guide

The keypad consists of numeric keys (1–9), the ‘*’ key, and the ‘#’ key.

Type	Description
Basic Input Format	Enter number + ‘#’ (‘#’ is the Enter key).
Cancel Input	Pressing ‘*’ cancels both ID/PW entry, and the process must be restarted from the beginning. This applies equally during administrator authentication.
ID Input Method	ID is confirmed after pressing ‘#’. Example: 2 + ‘#’ → ID “2” is entered.
PW Input Method	PW is confirmed after pressing ‘#’. Example: 1234 + ‘#’ → PW “1234” is entered.

Warning

- If ‘*’ is pressed during ID or PW entry, the entire process is canceled and must be restarted from the ID input step.

Changing the authentication mode is only available on keypad models and works only when Time & Attendance or Meal management mode is enabled in the Settings app(UBio-Link).

I T&A (Time&Attendance)

Function	Input	Operation Description	Beep Sound
Clock-in	Press '*' once	Switches to Attend mode	▲▲▲ (Pitch rising)
Clock-out	Press '#' once	Switches to Leave mode	▼▼▼ (Pitch falling)
Going Out	Press and hold '*' → release after beep	Switches to Out mode	▲▲▼ (Up-down)
Return	Press and hold '#' → release after beep	Switches to In mode	▼▼▲ (Down-up)

> LED Indicator

When the terminal switches to Function Key Mode, the white LED turns on. If no authentication attempt is made for 5 seconds while in Function Key Mode, the terminal automatically returns to the normal mode.

> Cancel

In Function Key Mode (white LED on), you can press the '*' key to cancel the Time & Attendance function and return to the normal mode.

I Meal Management

Function	Input	Operation Description	Beep Sound
Menu 1	Enter '#1#'	Changes to Menu 1	▲▲▲ (Pitch rising)
Menu 2	Enter '#2#'	Changes to Menu 2	▼▼▼ (Pitch falling)
Menu 3	Enter '#3#'	Changes to Menu 3	▲▲▼ (Up-down)
Menu 4	Enter '#4#'	Changes to Menu 4	▼▼▲ (Down-up)

> LED Indication

When the menu selection is completed, the white LED blinks once to indicate that the setting has been applied.

> Cancel

In principle, you must select the desired menu before authentication.

※ If no menu change is made, the previously used menu value will remain and authentication will proceed accordingly.

UBio-X Tag

Have any questions?

- If you have any questions about the content of this product, please contact UNION biometrics.
- Share with us any questions or inconveniences you may have while using the service, then we will discuss this in detail and resolve them quickly.