UBio Tablet5

User Manual

V1.0.0

Table of Contents

Product introduction

1.1 Product overview

Mobile V-Terminal is an App that acts as a virtual access controller.
Fingerprint authentication via fingerprint sensor, card authentication via NFC, and 1:1 ID-password authentication is possible.
You can manage users and logs by connecting to UNIS server and use the app alone without connecting to the server.

1.2 OS Specification & Fingerprint sensor

Below is Android OS specification and fingerprint sensor of UBio Tablet5.

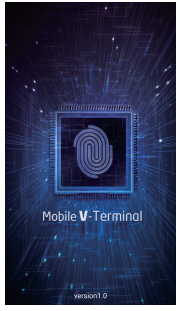
OS Specification	Android 7.0 (OTG-supported)
Fingerprint sensor	NScan-FM

1.3 Notice

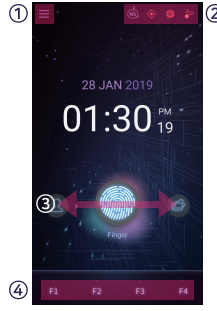
1. What if UBio Tablet 5 is not recognized by your PC?
: From Menu > [Settings] > [Developer options] > Set [USB OTG Mode] as OFF.

Main

2.1 Execute the app.



[App intro screen]



[App main screen]

① Menu button

When clicking the button, the slide menu is displayed.

② Status icon

- Authentication mode : There are NS / SN / NO / SO mode.
  NS : It is the abbreviation for Network StandAlone. If it is connected with the server, it authenticates in server. If not, it authenticates locally. If the server authentication fails, no authentication is attempted locally.
  SN : It is the abbreviation for StandAlone Network. It authenticates locally first and then if fails, it authenticates in server.
  NO : It is the abbreviation for Network Only, which authenticates in server.
  SO : It is the abbreviation for StandAlone Only, which authenticates locally.
- GPS : You can set whether to save the location information or not. (Available to change in [Settings])
  GPS ON GPS ON, No location information GPS OFF
- Fingerprint sensor : You can set whether to connect with fingerprint sensor or not.
  The status that the fingerprint sensor is connected
  The status that the fingerprint sensor is not connected
  When executing the app, it shows the text to check the connection status with the fingerprint sensor.(For reference, when going back to the app, the text to check the connection status with the fingerprint sensor is displayed.)
- Server : You can set whether to connect with server or not. (Available to change in [Settings])
  The status that the server is connected
  The status that the server is not connected

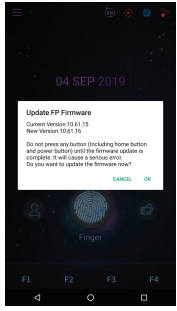
③ Authentication button area

When sliding left and right, it displays FP > Card > ID > FP··· in order.
When clicking the button, the selected authentication is proceeded.

④ Function (Access Mode) setting area

When authenticating, it is reported with the selected function value in log.
Default : Access, F1 : Arriving, F2 : Leaving, F3 : Out, F4 : In

2.2 Main screen Firmware update

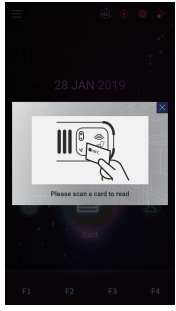


[FP FW update notification pop-up]

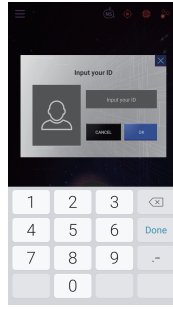
① Update FP Firmware

If the FP firmware version is not the latest one, it shows the pop-up message in main screen at first.
When you cancel, it doesn't display pop-up again. You can update the firmware from [Setting] > [Update FP Firmware].

2.3 Authentication (Fingerprint / Card / ID)



[Card scan notice pop-up screen]



[ID input pop-up screen]

① Fingerprint authentication (1:N authentication)
It scans the fingerprint when connecting with the fingerprint sensor
If not connecting with the fingerprint sensor, the message "The feature you set is not supported." is displayed.

② Card Authentication (1:N authentication)
It displays the pop-up screen to guide you the card scan and scans the card.
If NFC is not supported, the message "The feature you set is not supported" is displayed.

③ ID authentication (1:1 authentication)
It displays the pop-up screen to enter the ID. If the entered ID doesn't exist, it shows the pop-up screen on authentication failure.
If an ID exists, authentication proceeds with the authentication type of the corresponding ID.

④ Authentication type
- Fingerprint
- Password
- Card AND Fingerprint
- Password AND Fingerprint
- Password AND Card
- Card
- Card OR Fingerprint
- Password OR Fingerprint
- Password OR Card

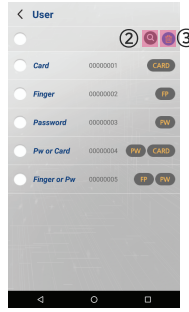
※ In case of the combination OR / AND, the authentication priority is FP > Card > Password.

⑤ Authentication
In NO mode, the ID is displayed in pop-up.
In SO mode, the name is displayed in pop-up.
In case of fingerprint authentication, authentication should be attempted in the registered direction.
In the case of server authentication, the Card AND Fingerprint combination must be authenticated first. (In the opposite case, it fails.)
In case of ID authentication, if it is OR combination, the second authentication is attempted at the first failure.

User Management

3.1 User

[User management screen]



[Edit mode]

① Add

It moves the screen to add the new user. (Max : 1,000 users)

② Search

It displays the search window, which you can search with user's ID or name in. (Available up to 16 digits)

③ Delete

It changes into the edit mode.

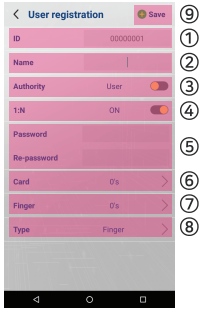
If there is no selected user, the edit mode is cancelled.

If there is the selected user, it deletes the user locally.

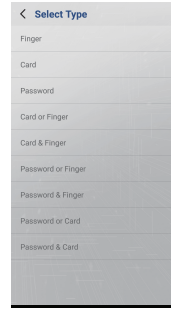
④ User list

- User/Admin icon
- User name
- User ID
- Authentication type

3.2 User registration



[User registration screen]



[Authentication type selection screen]

① ID
It is 8-digit number type. The ID that doesn't exist locally is entered automatically.

② Name
You can enter within 16bytes.

③ Authority
It switches User / Admin.
If there is an admin, it is necessary for admin authentication when moving into every menu.

④ 1:N
It switches ON / OFF.
When setting OFF, the user can only use 1:1 authentication. (ID authentication)

⑤ Password
It enters the password to use in password authentication.

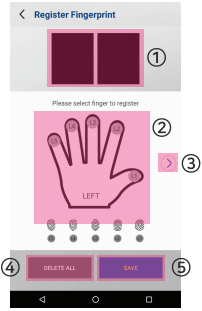
⑥ Card
When clicking, it moves into the card management screen.

⑦ Fingerprint
When clicking, it moves into the fingerprint management screen.

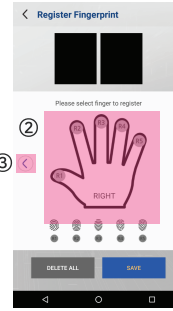
⑧ Type
When clicking, it moves into authentication type selection screen.

⑨ Save
It can add the new user locally with the entered information.

3.3 Register Fingerprint



[FP management - Left]



[FP management - Right]

① Fingerprint scan image

It displays the scanned fingerprint as an image.
The scan is performed twice and the registration fails if fingerprints do not match. The registration fails if the fingerprint is already registered.

② Finger (L5,L4,L3···.R3,R4,R5)

If a fingerprint is stored on that finger, it is deleted.
If a fingerprint is not stored on that finger, it starts to scan the fingerprint.

③ Screen movement

It can move the screen by sliding.
It can move with arrow button.

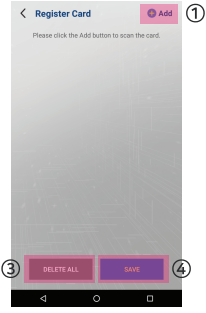
④ DELETE ALL

It deletes all the fingerprint data.

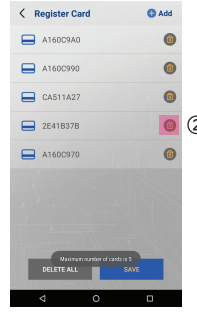
⑤ SAVE

It saves the current fingerprint data and then moves to the previous screen.
It can register up to 10 fingerprints per ID.

3.4 Register Card



[Card management - 0]



[Card management - 5]

① Add

If the number of card data is less than 5, a pop-up to guide the card scan is displayed and the card is scanned.

If the number of card data is 5, the message “Maximum number of card is 5” is displayed.

② Delete

It deletes the card data in the list.

③ DELETE ALL

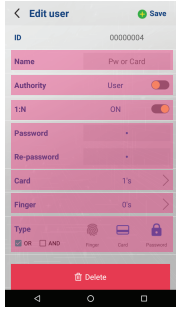
It deletes all the card data.

④ SAVE

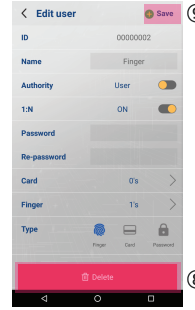
It saves the current card data and moves into the previous screen.

It can register up to 5 cards per ID.

3.5 Edit user



[Edit user – OR Combination]



[Edit user]

① Name
It can enter within 16 bytes range.

② Authority
It switches User / Admin.

③ 1:N
It switches ON / OFF.

④ Password
It displays user's password, which can be modified.

⑤ Card
It displays the number of user's cards and moves into the card management screen when clicking.

⑥ Finger
It displays the number of user's fingerprint and moves into the fingerprint management screen when clicking.

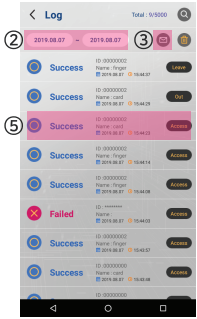
⑦ Type
If you selected an authentication type before, the selection is deleted when you select it again.
If there are two authentication types selected, OR / AND checkbox is displayed.

⑧ Delete
It deletes the user.

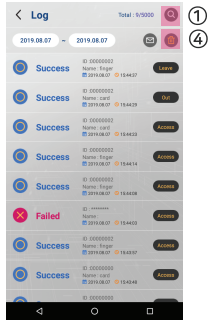
⑨ Save
The user information is updated with the changed information.

Log Management

4.1. Log



[Log management screen]



[Edit mode]

① Search

It displays the search window, which you can search with user's ID or name in. (Available up to 16 digits)

② Select the period

It can search the log for a specific period.
It can display the pop-up of date selection.

③ Share by email

It can share the log data via the email app installed in the device.
Please use after setting the account in UBio Tablet 5's default email app.

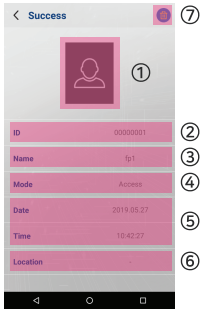
④ Delete

It changes into the edit mode. If there is no selected log, the edit mode is cancelled.
If there is the selected log, it is deleted locally.

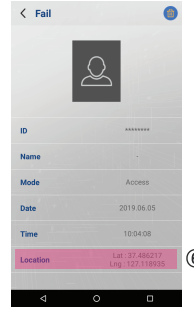
⑤ Log list

- Authentication result
- User ID or Name
- Authentication date / time
- Function (Access mode)

4.2 Log details



[Log details – No location]



[Log details – Location (included)]

① User image
If [Save Image] is ON, the taken photo is displayed when authenticating.
If [Save Image] is OFF, the default image is displayed.

② ID
The user's ID that the authentication is attempted is displayed.

③ Name
The user's name that the authentication is attempted is displayed.

④ Mode
The function that the authentication is attempted (Access Mode) is displayed.
Default : Access, F1 : Arriving, F2 : Leaving, F3 : Out, F4 : In.

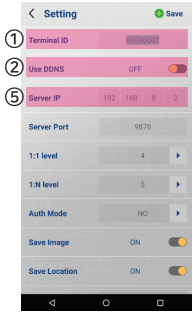
⑤ Date
The date and time attempted authentication is displayed.

⑥ Location
If there isn't any location information, "-" is displayed.
If there is the location, the information is displayed.

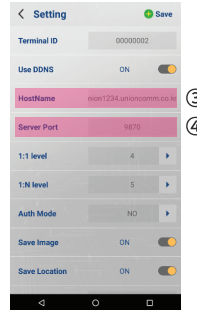
⑦ Delete
The log data is deleted locally.
In case of card authentication, the card number is not saved.
(Server upload is same.)

Setting Management

5.1 Setting



[Server IP setting]



[HostName setting]

① Terminal ID

It specifies the ID of the terminal in 8-digit format.
The default ID is 99999999.

② Use DDNS

It determines whether to use DDNS. (Default OFF)

③ HostName (Available only in DDNS ON)

It sets the hostname of server to connect.
(Available up to 255 digits)
To use DDNS feature of UNIS, you should enter the format as union(contract no.).unioncomm.co.kr.

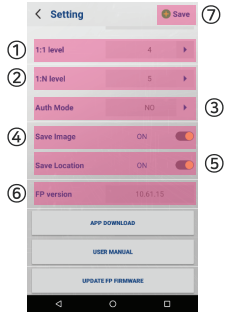
④ Server Port

It specifies the server port to connect.
The default port is 9870.

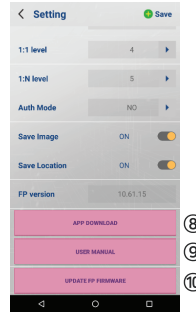
⑤ Server IP (Available only in DDNS OFF)

It sets the server IP to connect.
The default value is 127.0.0.1.

5.2 Additional setting



[Card recognition type – Data]



[Card data - information]

① 1:1 level (Default: 4)

It can be set from 1 to 9, and the higher the number is, the higher the fingerprint matching criteria is.

② 1:N level (Default: 5)

It can be set from 3 to 9, the higher the number is, the higher the fingerprint matching criteria is.

③ Auth Mode (Default: SN)

There are NS / SN / NO / SO mode.

- NS: It is the abbreviation for Network StandAlone. If it is connected with the server, it authenticates in server. If not, it authenticates locally. If the server authentication fails, no authentication is attempted locally.
- SN: It is the abbreviation for StandAlone Network. It authenticates locally first and then if fails, it authenticates in server.
- NO: It is the abbreviation for Network Only, which authenticates in server.
- SO: It is the abbreviation for StandAlone Only, which authenticates locally.

5.2 Additional setting

④ Save Image (Default: OFF)

It switches ON / OFF.

When setting ON, the image is taken and it is saved in log if the user authenticates.

⑤ Save Location (Default: OFF)

It switches ON / OFF.

When setting ON, the location is saved in the log if the user authenticates.

⑥ FP version

It displays FP version.

⑦ Save

It sets the terminal with the entered information.

⑧ APP DOWNLOAD

It moves to URL to download the latest APK file.

⑨ USER MANUAL

It moves to web page to see the user manual.

⑩ UPDATE FP FIRMWARE

If FW version is different, it starts to update.

If it is the latest firmware, it displays the notification pop-up.

6.1 How to use USIM

[Correct direction]

[Wrong direction]

※ How to insert USIM

USIM should be inserted by [Correct direction] referring the picture above.

6.2 USIM type

Correct USIM

Micro SIM

Nano SIM + holder Nano SIM Holder

Wrong USIM

Only Nano SIM

※ USIM type (Micro SIM)

You should use Micro SIM or Nano SIM & Holder referring the picture above.
If you insert Nano SIM, it can damage SI slot of device.

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