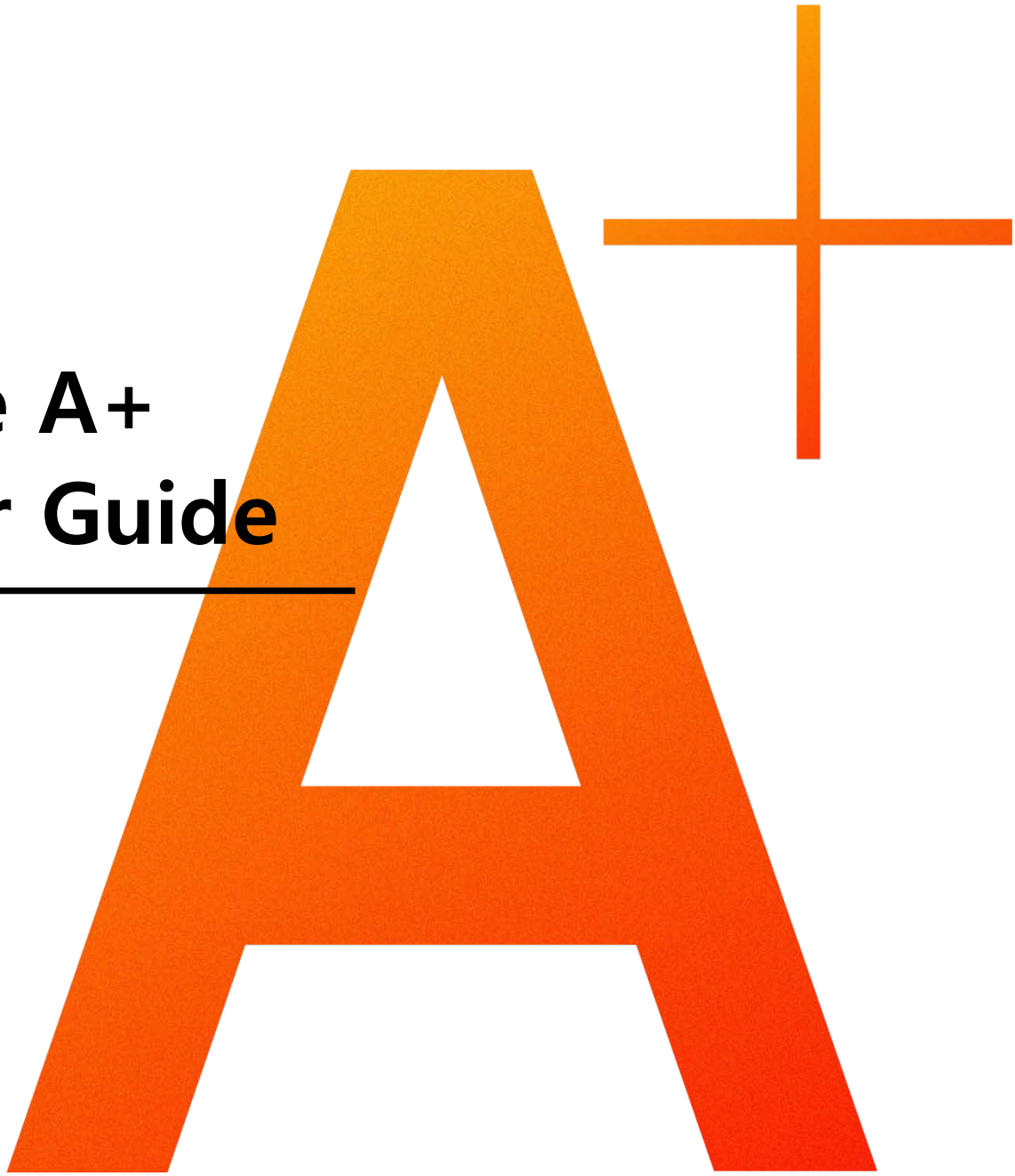
Version 1.01

Face A+
User Guide



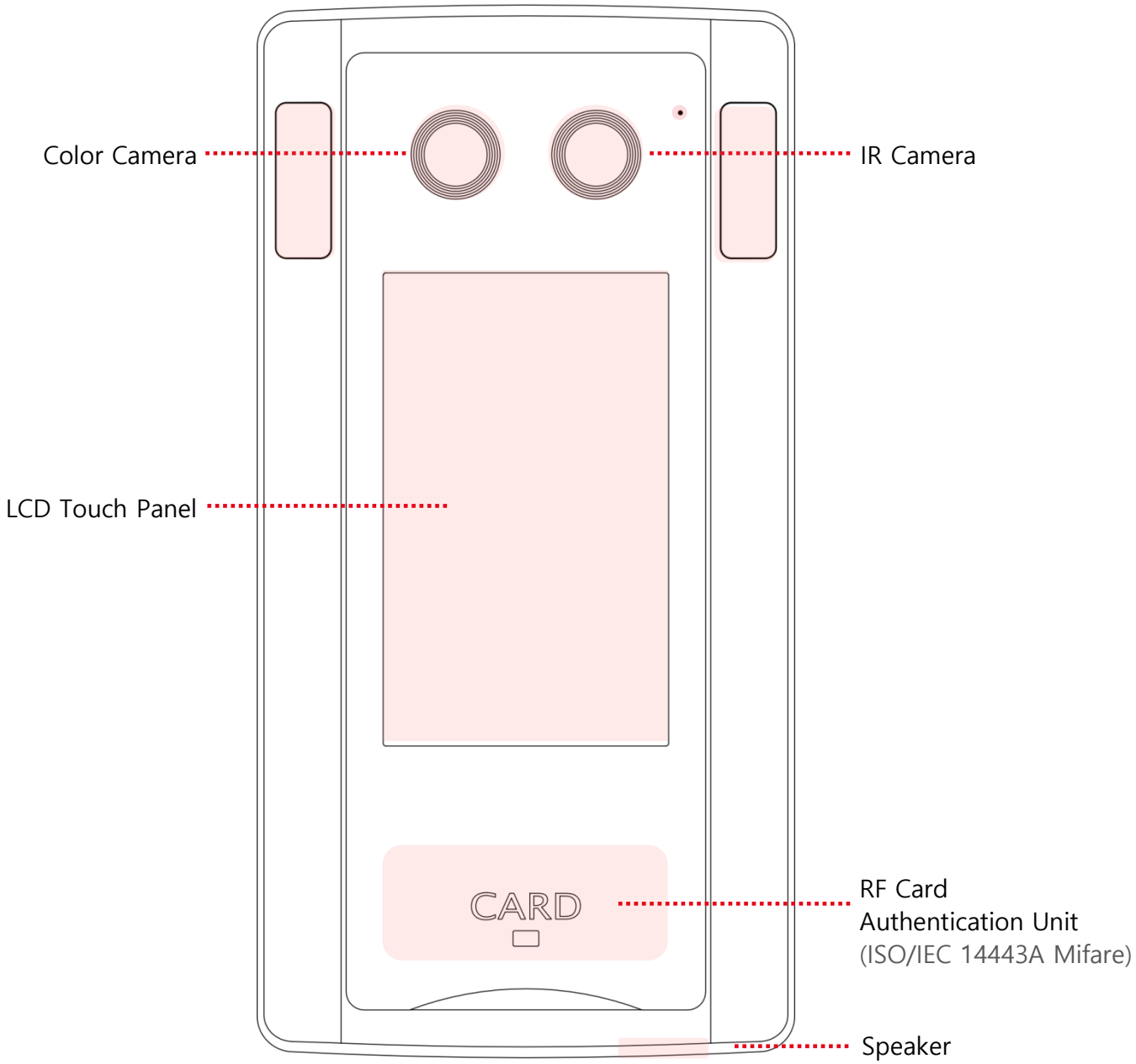
FA-1000/FA-2000

CVT
Creative Value Technology

Contents

1 Device Overview & Installation

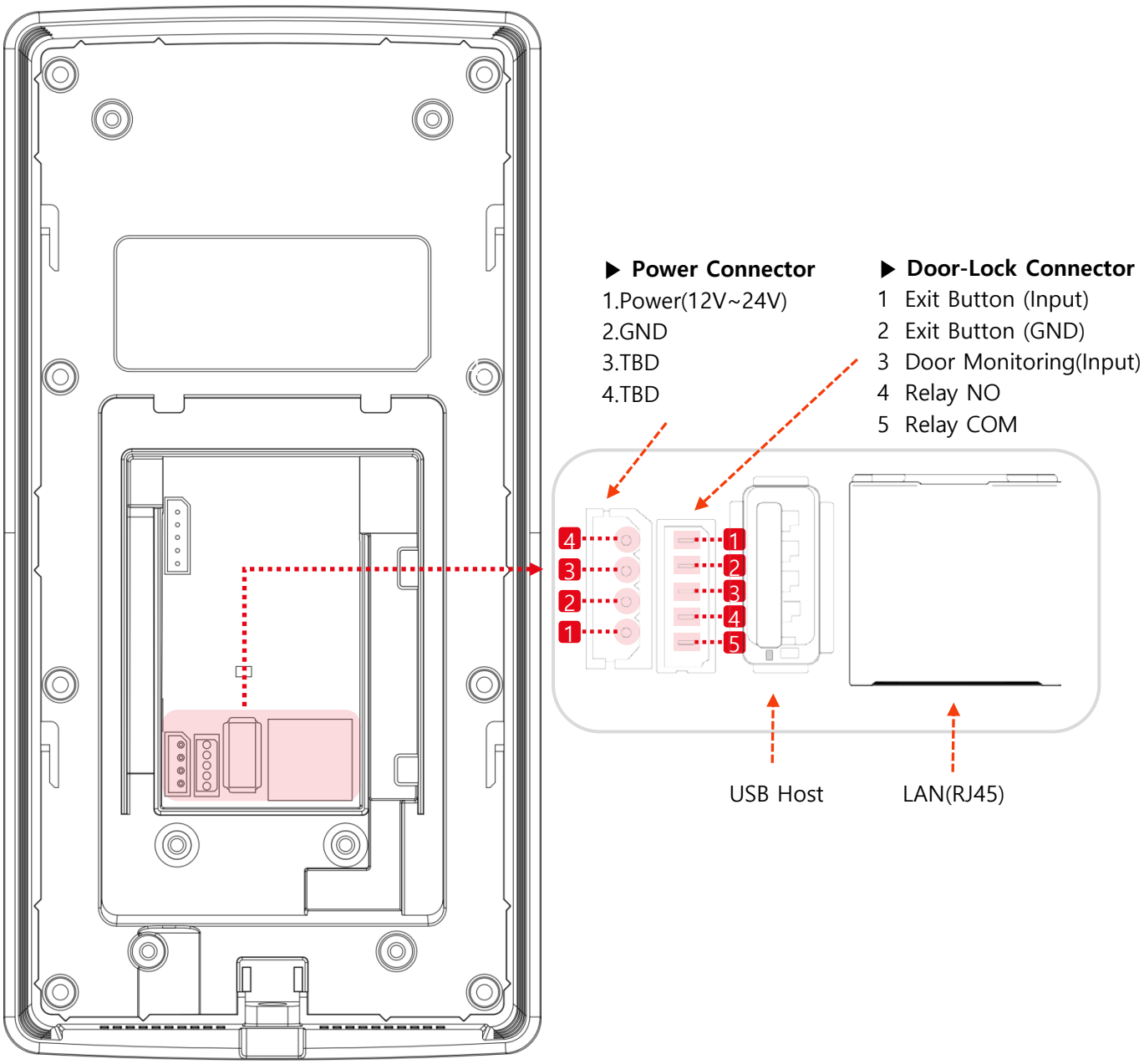
1.1 Device Appearance



Front

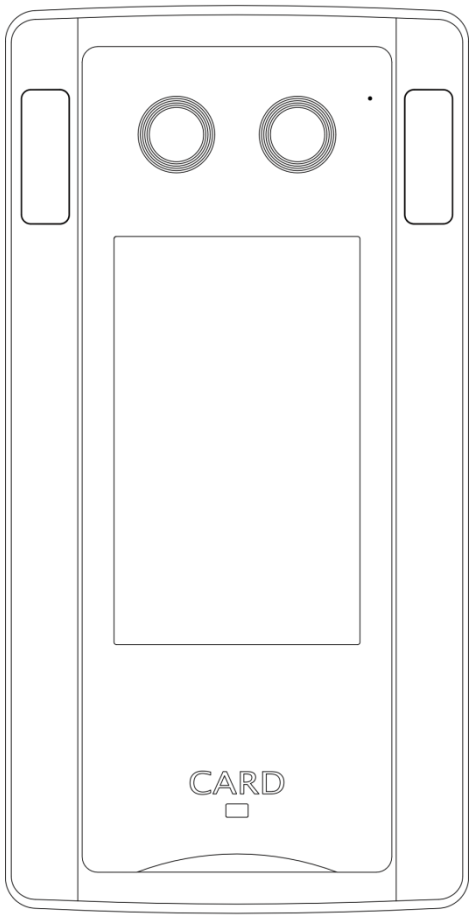
1.1

Device Appearance

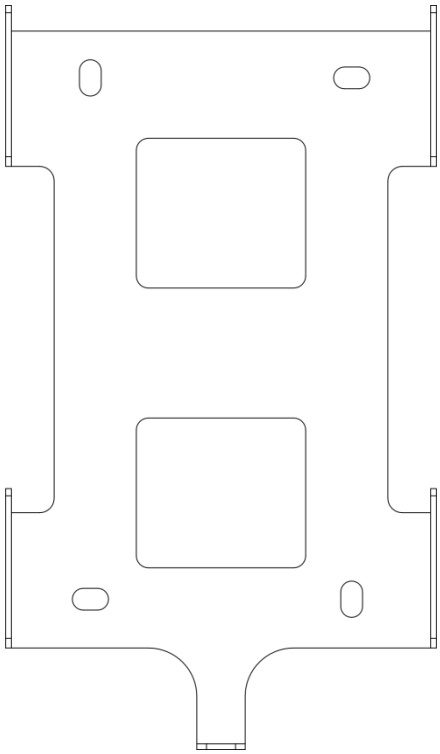


Rear

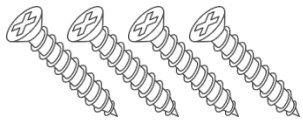
1.2
Components



Face A+



Wall-Mount
Bracket

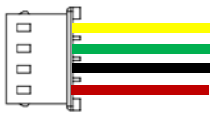


4 screws for fixing
bracket on the wall

1 screw for fixing the
reader onto the bracket

12V Adapter

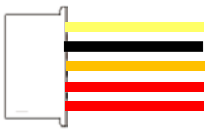
Power Cable



▶ Power Cable Pin-Map

1 Red: 12V
2 Black: GND
3 TBD
4 TBD

Door-Lock Cable

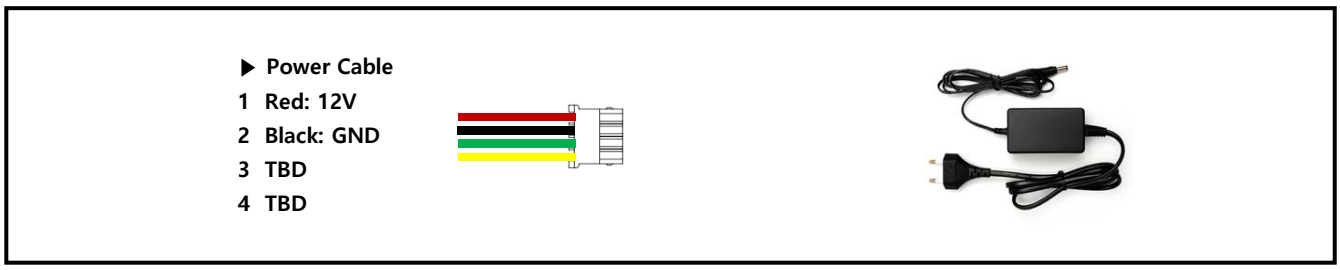


▶ Door-Lock Cable Pin-Map

1 Yellow: EXIT Button (Input)
2 Black: EXIT Button (GND)
3 Orange : Door Monitoring
4 Red: Relay (NO)
5 Red: Relay (COM)

1.3

Cable Connection



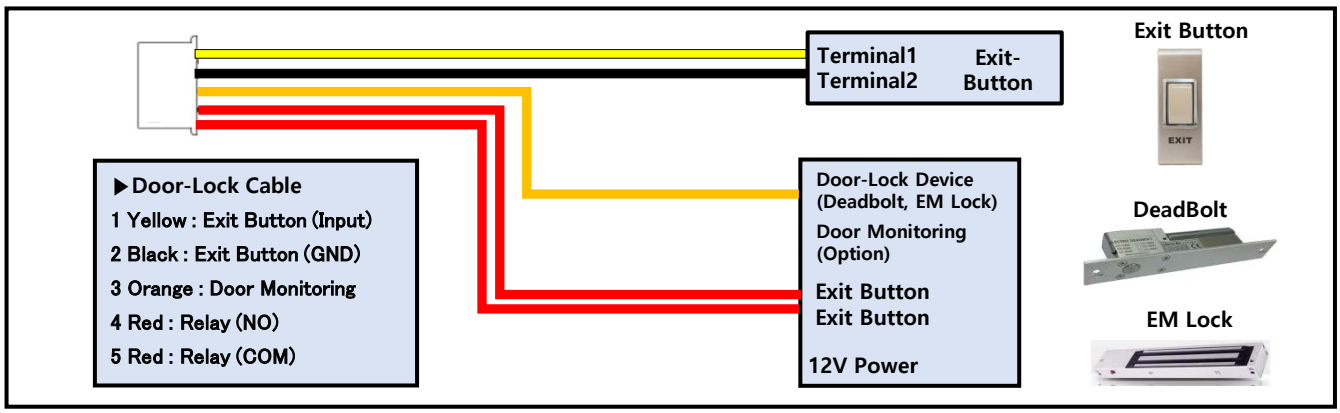
1. Connect the power cable to the adapter. (Maximum consumption power = 0.5A@12V)

2. The door lock cable is for connecting the door lock (deadbolt, EM lock) and EXIT-button.

3. Connect the yellow and black cable to the exit button.

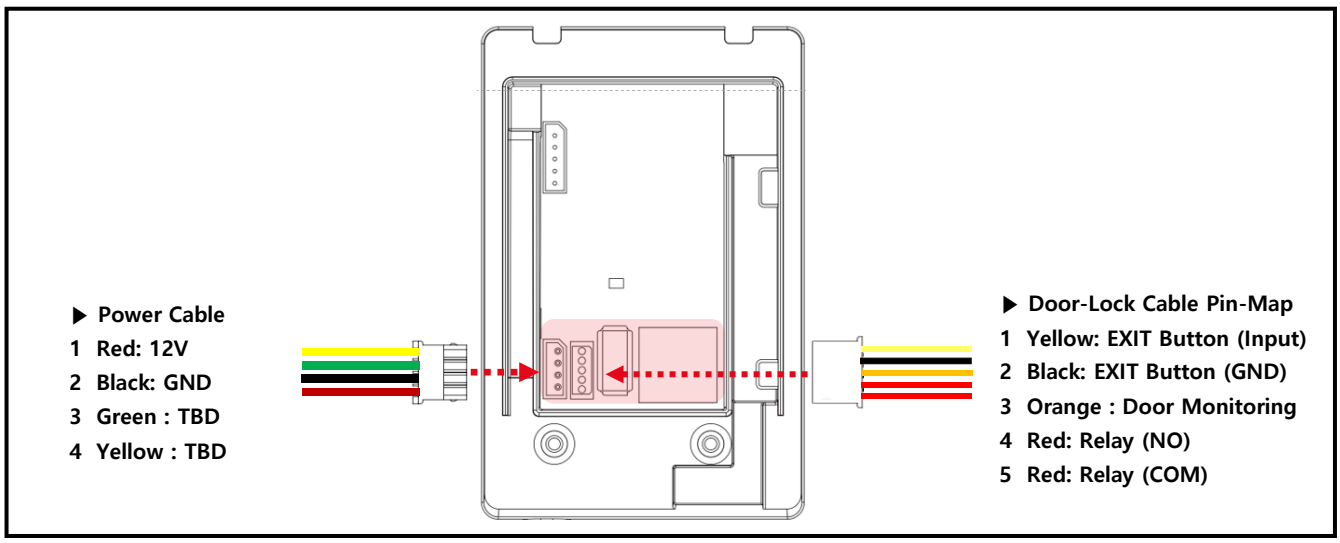
4. Connect the red cable of the door lock cable to the exit button of the door lock. (Relay contact provided)

5. If there is a door open signal output on the deadbolt (EM lock), connect it to the orange color cable (for door monitoring input).



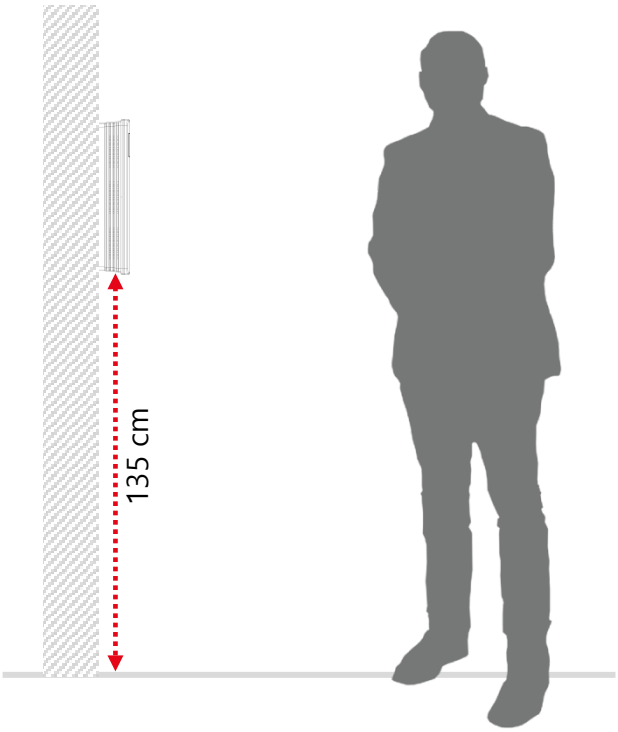
6. Open the cover on the back of the Face A+ and connect the prepared power cable and door lock cable to the corresponding connectors.

7. In addition, when interworking with the manager server, the LAN cable must be connected to the RJ45 port.



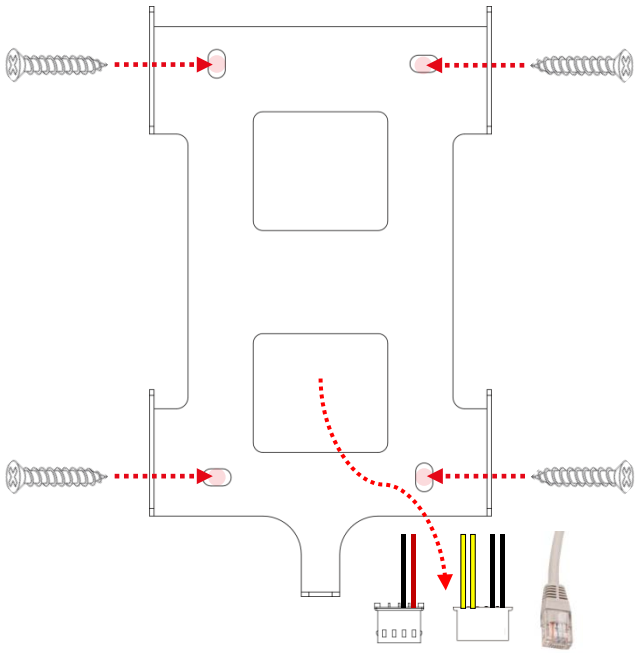
1.4

Device Installation



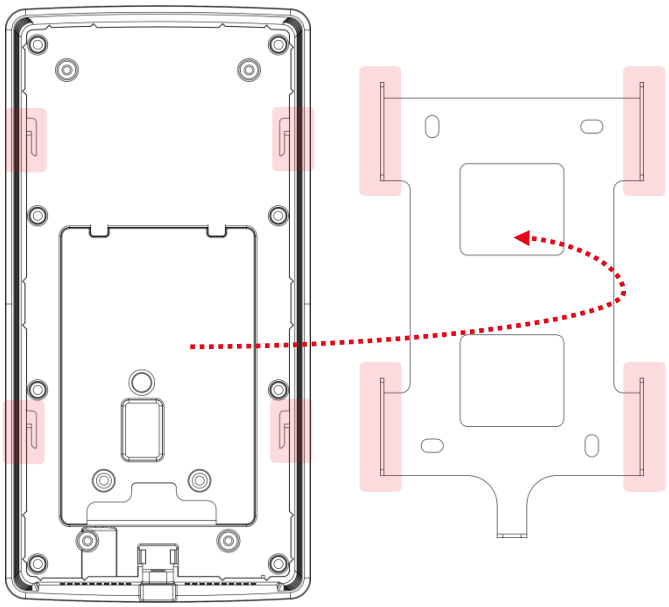
1 Determine the correct position to install the product.

* The optimal height is 135 cm.
* Avoid installing the device in direct sunlight.



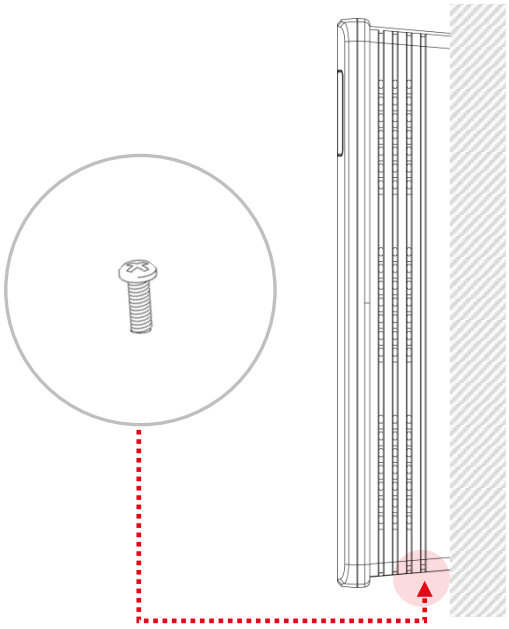
2 Fix the bracket firmly with fixing screws to the position where Face A+ will be installed.

* Power cable, door lock cable and LAN cable must go through the hole in the bottom of the bracket.



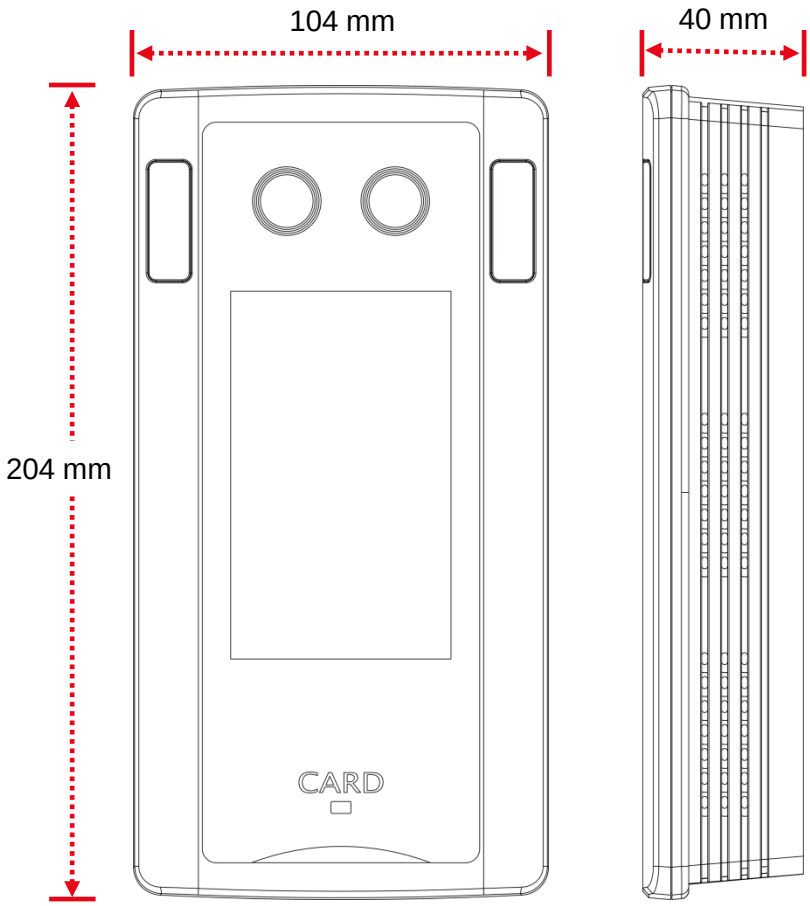
3 Install Face A+ onto the bracket.

* Before installing the product on the bracket, you must open the rear cover and connect the cables to the appropriate port first.

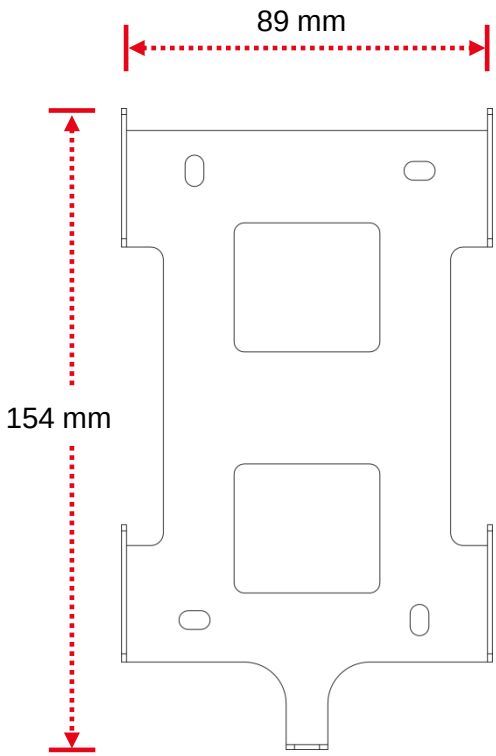


4 Fix Face A+ to the bracket with the bracket fixing screw.

1.5
Dimensions



Face A+

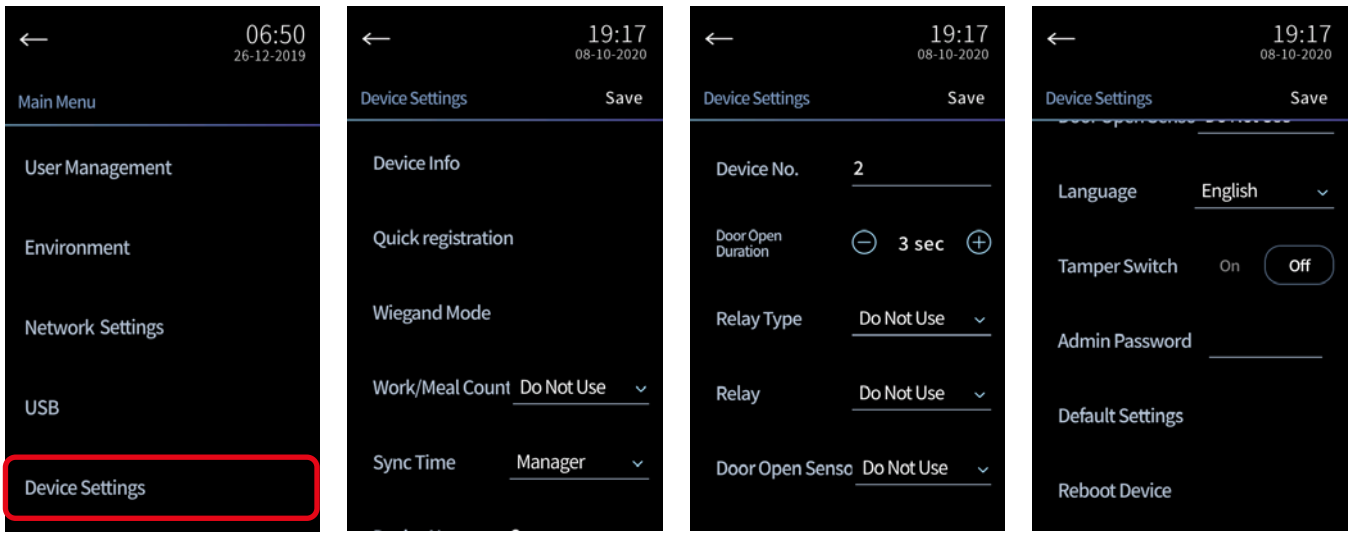


Wall-Mount Bracket

2 Device Initialization

2.1 Set Up the Device

- If you are installing the device for the first time, you must set its purpose of use.
- When turning on the device for the first time, the device setting screen appears as below.
- Refer to the table below for a detailed setup.
- To save the setting values, press Save.
- After saving, user registration for initial administrator registration will begin.
  (To change the settings again after the initial setup, enter the Device Settings menu in the Main Menu.)

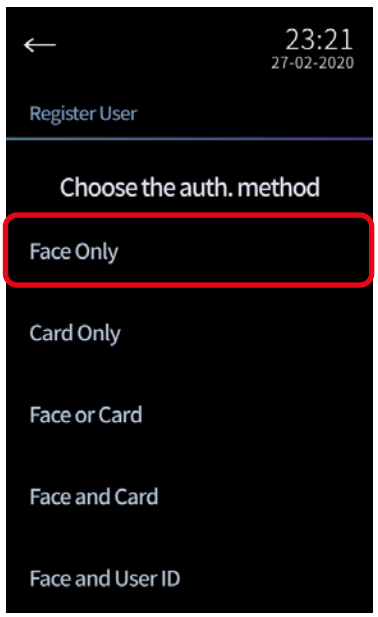


Setting Item	Description
Device Info	Check the device information.
Quick registration	User registration quickly.
T&A/Meal Count	The default mode is access control; you can change it to time and attendance or meal count.
Sync Time	Synchronizes the device time with the Internet NTP server or the Manager server.
Device No.	When working with the Manager server, assign a unique number for individual device control.
Door Open Duration	Set the number of seconds a door remains open.
Relay Type	Select the desired relay connection type (select NC or NO).
Relay	Select Enabled for relay control. In the case of meal count mode, disable the relay.

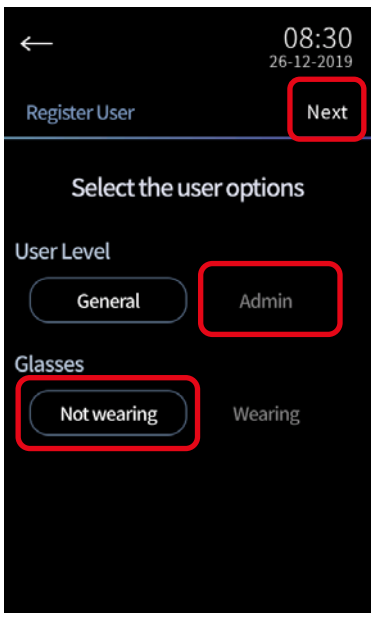
Setting Item	Description
Door Open Sensor	Check status of door open.
Language	Set the language (select between Korean and English).
Tamper Switch	The alarm turns on when the rear cover is opened (for unauthorized use).
Admin Password	Change the administrator password (default is 1234567890).
Default Settings	Set the setting values to default.
Reboot Device	Restart the device.

2.2 Register the Initial Administrator

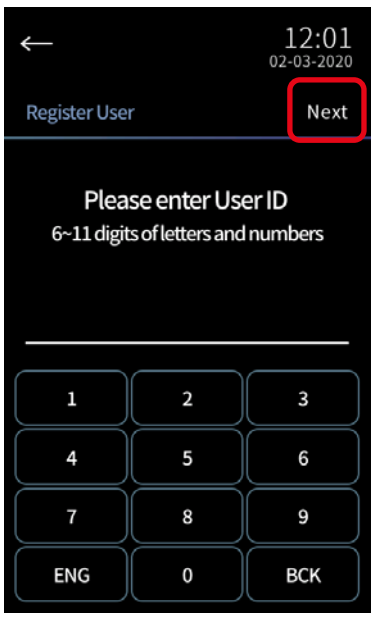
- After device setting, user registration for the initial administrator registration will begin.
- You must register at least one administrator and you may register up to five administrators.
- The administrator password can be changed in Device Settings.
- For security reasons, the administrator password must be changed and memorized when setting up.



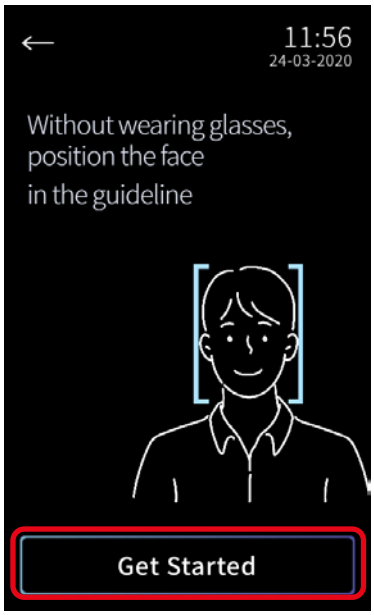
1 To register as an administrator for the first time, on the Register User screen, select Face Only.



2 Select User Level and Glasses option accordingly. For those who do not wear glasses, select Not wearing and press Next.

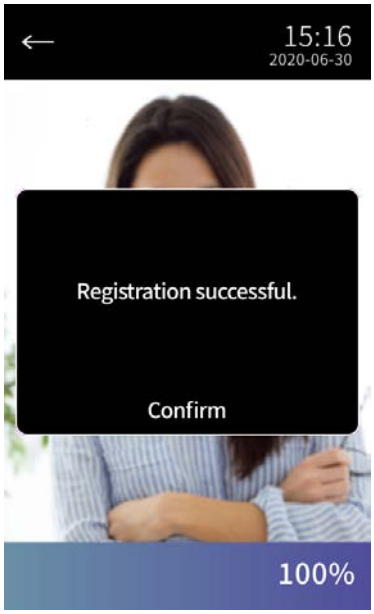


3 Type the administrator ID and press Next. You can enter letters and numbers from a minimum of 6 to a maximum of 11 characters.



4 Press Get Started to register your face.

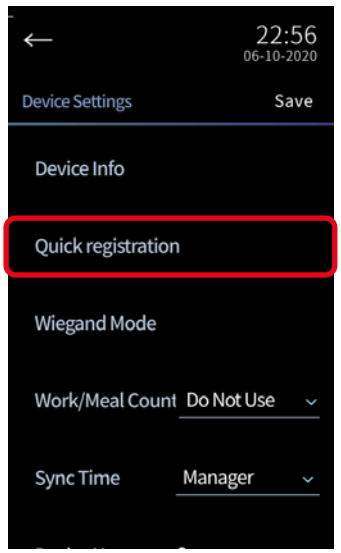
5 Make sure your face stays within the guideline. You may need to adjust your position by moving the face back and forth.

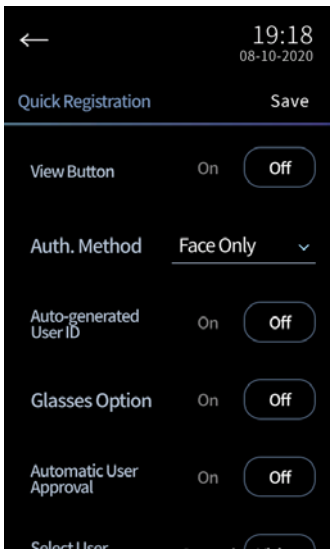


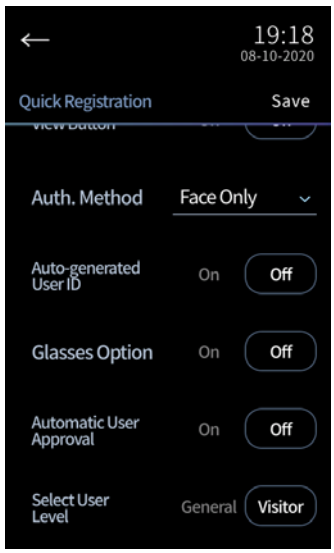
6 Please remain in your position until the status bar reaches 100% and the face registration is complete.

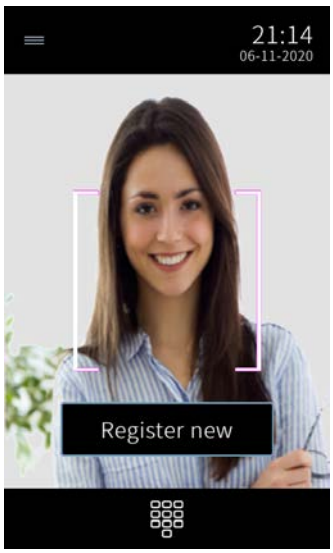
2.3 Quick Registration

- Changing 'Quick registration' setting such as View Button, Auth. Method, Auto-generated User ID. Glasses Option, Automatic User Approval, Select User Level.
- If you select <On> for 'View Button', 'Register new' button appears on the Live View screen.
- When registering using the 'Register new' button, the saved setting is applied automatically.









Setting item	Description
View Button	Select whether to display the 'Register new' button on Live View screen.
Auth. Method	Select either 'Face only' or 'Face or card'.
Auto-generated User ID	Select whether to automatically generate an ID when registering a user.
Glasses Option	Select whether to display glasses option when registering a user.
Automatic User Approval	Select whether to automatically approve after user registration.
Select User Level	The user level is automatically set to the selected level (General/Visitor).

3 User Registration

3.1 User Authentication Methods

- Maximum of 10,000 users (including administrators) can be registered.
- You can register up to 10,000 users, including Face Only users (1:N authentication) and combined authentication users (combined authentication methods: Face + Card authentication or Face authentication + User ID).
- The combined authentication method is called 1:1 authentication.
- In case of Face + User ID, when you try face authentication, press the bell button at the bottom of the LCD screen to enter your User ID and proceed with the face authentication.

Authentication Method	Description	Reference
Card Only	Authentication via Card only, without Face verification.	Refer to 3.2
Face Only	Authentication via Face verification only.	Refer to 3.3
Face or Card	Authentication via either Face verification or Card.	Refer to 3.4
Face and Card	For a high-level identity security service. Authentication via Card, followed by Face verification.	Refer to 3.4
Face and User ID	For a high-level identity security service. Authentication via User ID, followed by Face verification.	Refer to 3.3

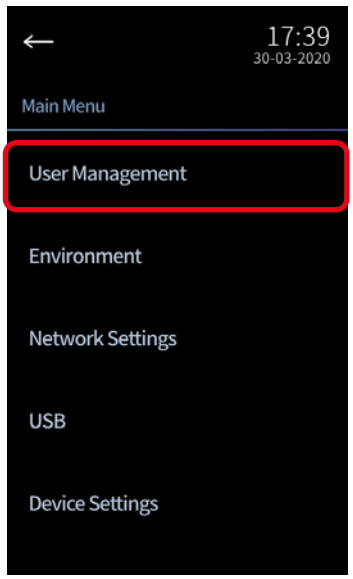
Guidelines for registering a face

- Do not change your facial expression (don't smile, wink, etc.).
- Do not cover your eyes or eyebrows.
- Do not wear hats, sunglasses or any accessory that covers your face.
- Do not display two faces on the screen at the same time. Register one person at a time.
- If wearing glasses, the user should register both with and without glasses. (Choose the "Glasses wearing" option)

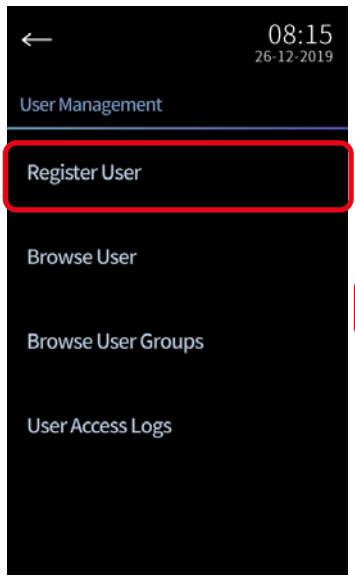
Guidelines for authenticating a face

- It is recommended to position the face inside the guideline displayed on the screen.
- If a user tries to authenticate using different glasses from the ones used for the registration process, the authentication might fail. In this case, the user should authenticate without glasses, if it has been previously registered.
- If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, or any other accessory, authentication may fail. Do not cover any part of the face, including eyebrows.

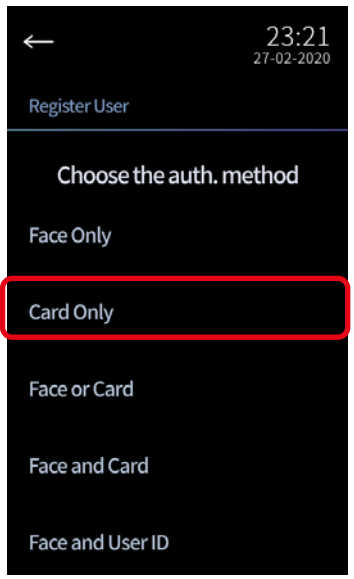
3.2
Card Only User Registration



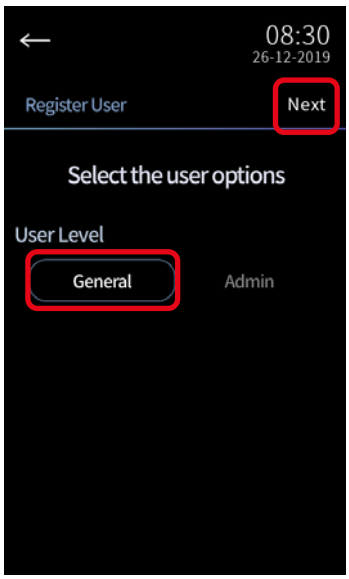
1 Select User Management from the Main Menu.



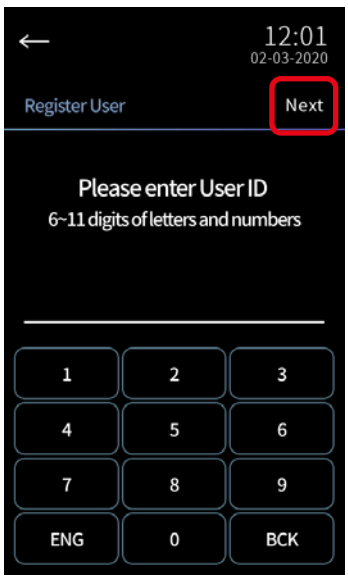
2 Select Register User.



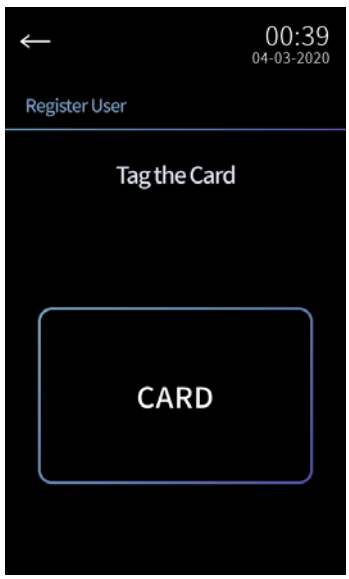
3 Select Card Only.



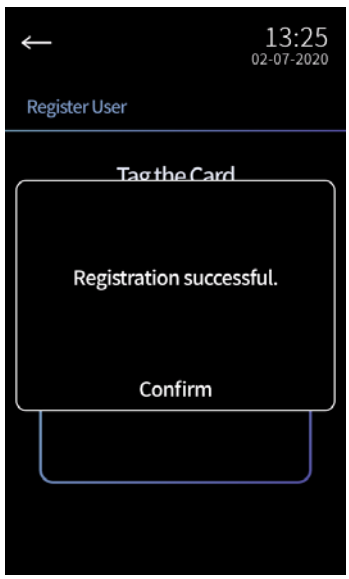
4 Select General for User Level.



5 Type the User ID and press Next. You can enter letters and numbers from a minimum of 6 to a maximum of 11 characters.



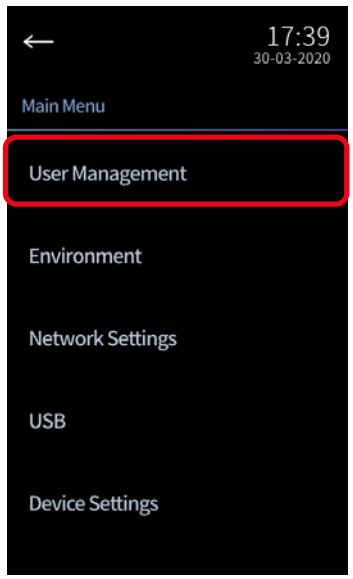
6 Tag the card on the card recognition unit at the bottom of the product.



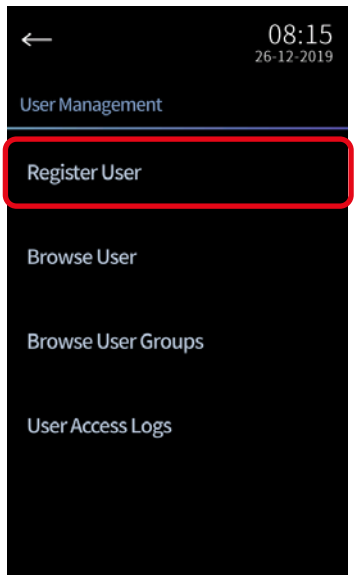
7 When the registration is complete, a pop-up message will appear.

3.3

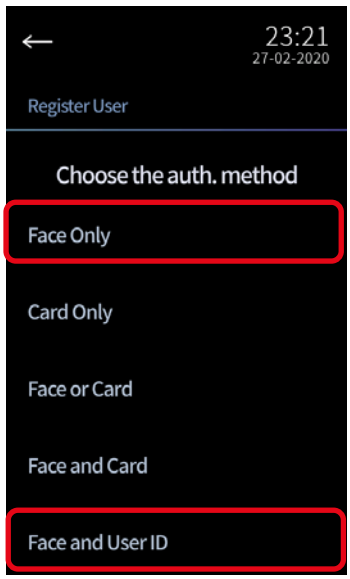
Face Only / Face and User ID User Registration



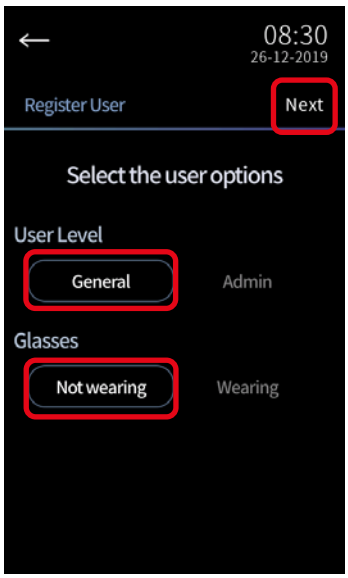
1 Select User Management from the Main Menu.



2 Select Register User.

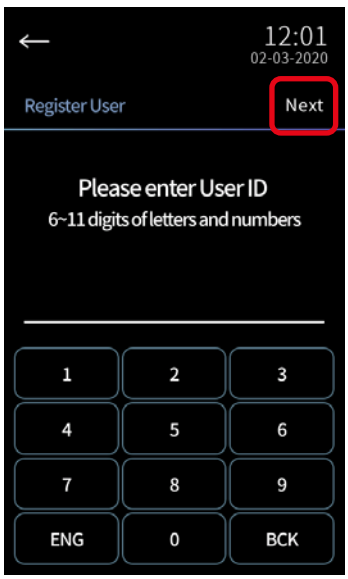


3 Select Face Only or Face and User ID.

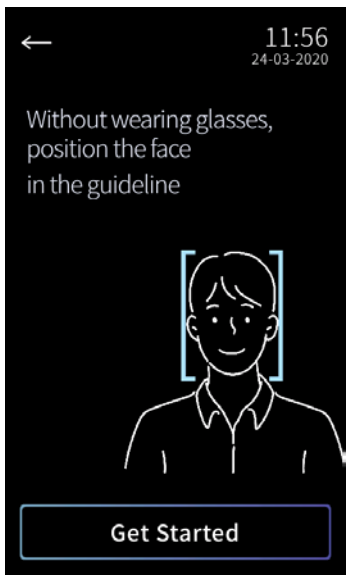


4 Select User Level and Glasses option.

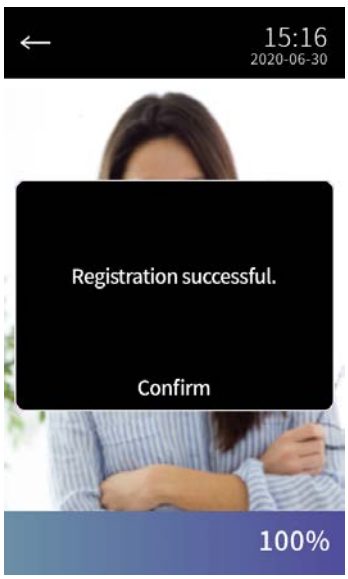
※ Users who wear glasses should select Wearing, follow the steps first without glasses and then again with glasses.



5 Type the User ID and press Next. You can enter letters and numbers from a minimum of 6 to a maximum of 11 characters.



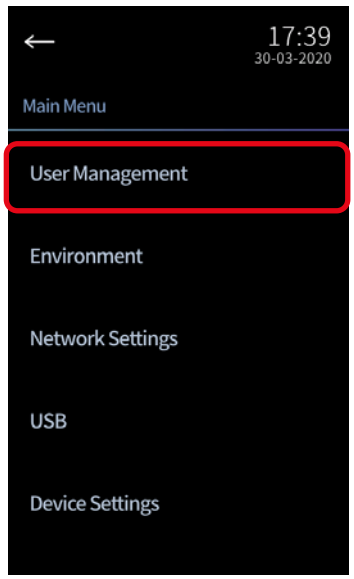
6 Press Get Started to begin the face registration.
Make sure that your face is in the guideline.



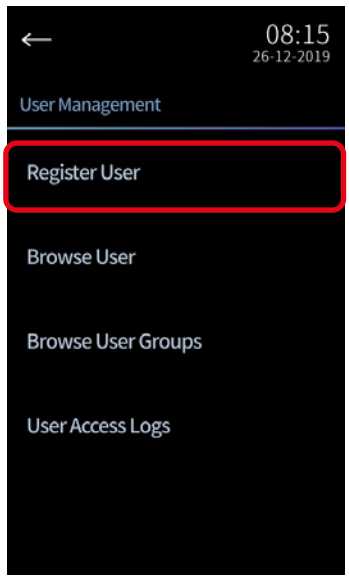
7 When the registration is complete, a pop-up message will appear.

3.4

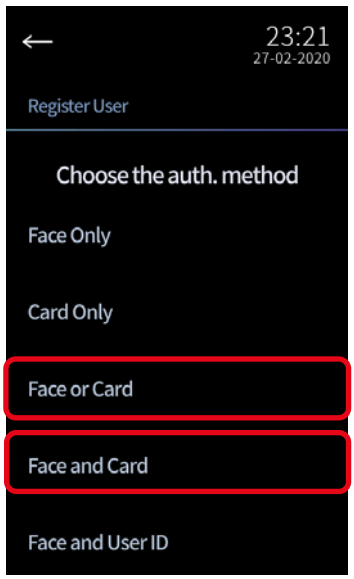
Face or Card / Face and Card User Registration



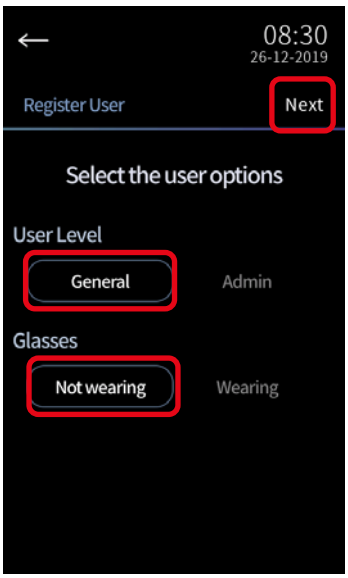
1 Select User Management from the Main Menu.



2 Select Register User.

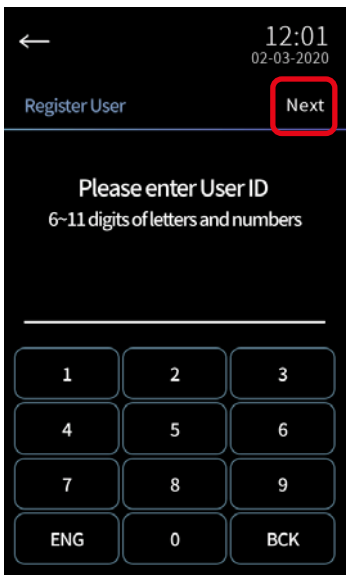


3 Select between Face or Card and Face and Card.

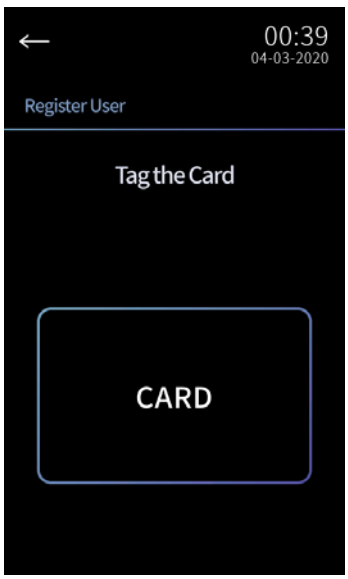


4 Select User Level and Glasses option.

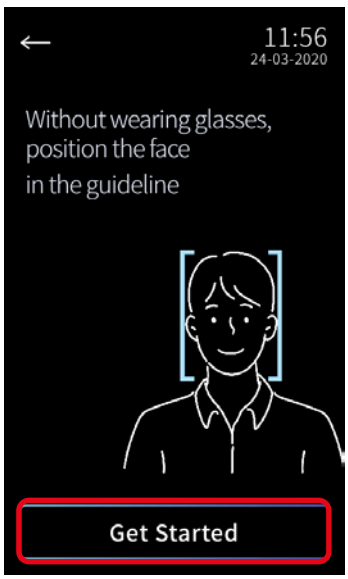
※ Users who wear glasses should select Wearing, follow the steps first without glasses and then again with glasses.



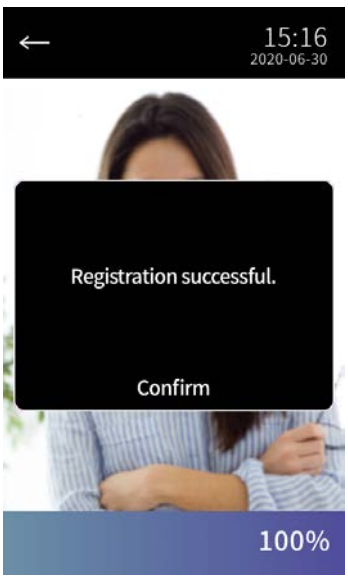
5 Type the User ID and press Next. You can enter letters and numbers from a minimum of 6 to a maximum of 11 characters.



6 Tag the card on the card recognition unit at the bottom of the product.



7 Press Get Started to begin the image capture.
Make sure that your face is in the guideline.



8 When the registration is complete, a pop-up message will appear.

4 User Management

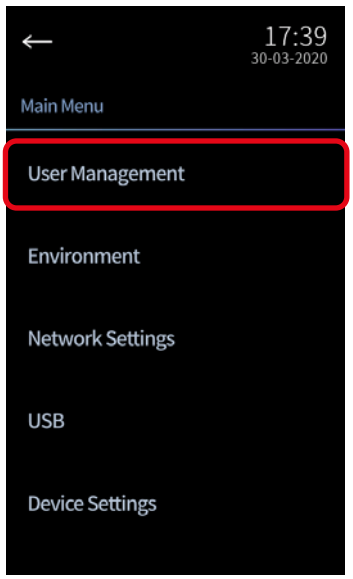
4.1 Methods of Browsing Users

- The administrator can browse or delete users and check their registration method(s) simply by User ID.
- Depending on the authentication method, the administrator can browse and delete the users in several ways.

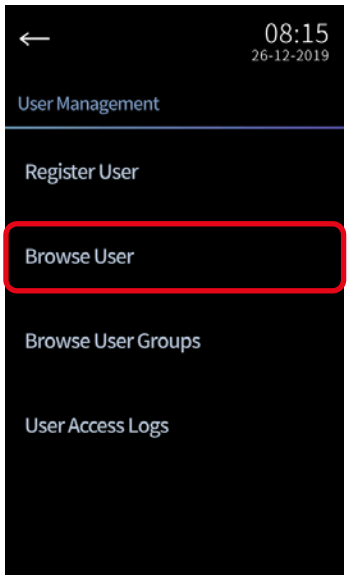
Methods of Browsing User	Description
By Card	Browse and delete users registered using a card.
By Face	Browse and delete users registered with face authentication.
By User ID	Browse and delete users registered using User ID.

4.2

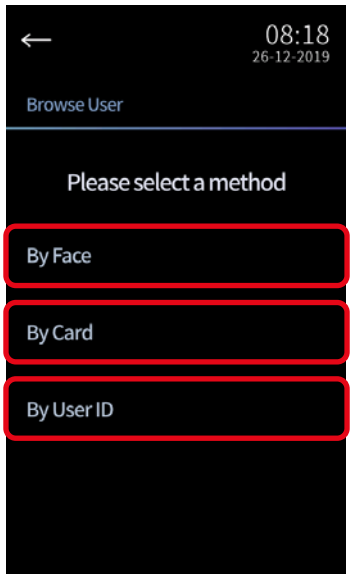
Browse and Delete Individual Users



1 Select User Management from the Main Menu.

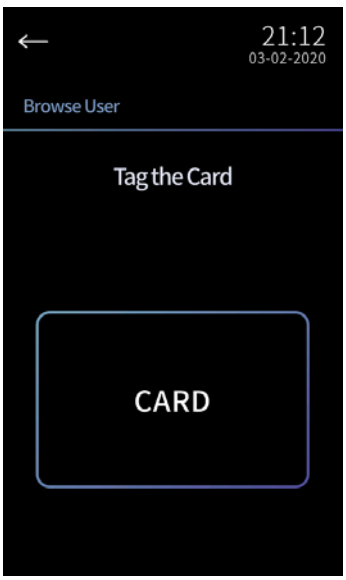


2 Select Browse User.

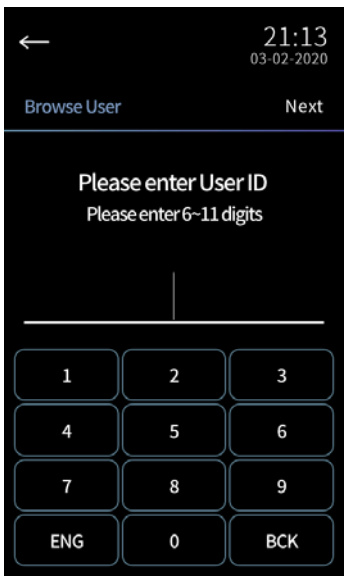


3 Select a search method.

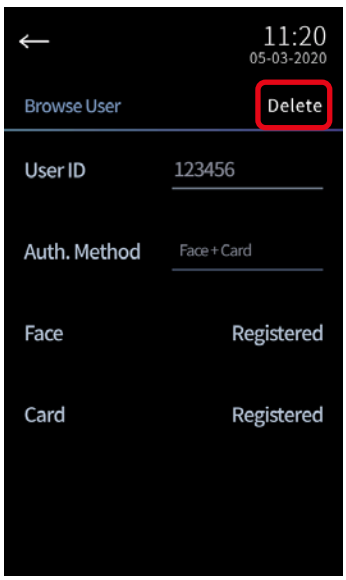
4-1 You can browse and delete users by face recognition.



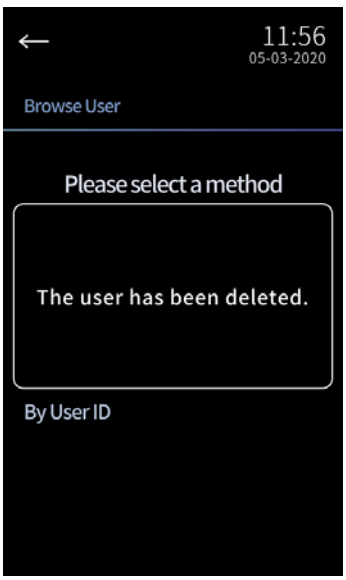
4-2 You can browse and delete users by tagging card.



4-3 You can browse and delete users by entering User ID.



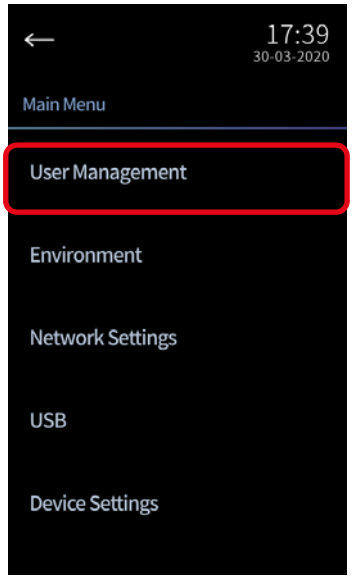
5 On the Browse User screen, press Delete on the right at the top of the screen to delete the user.



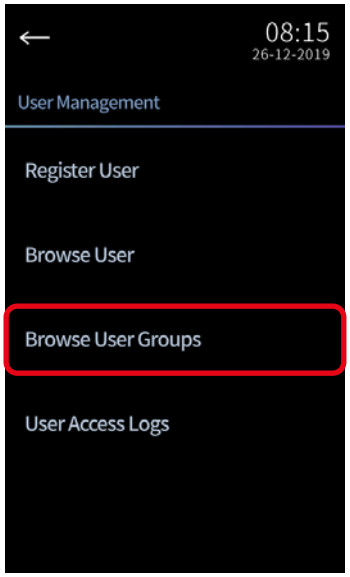
6 Press OK to delete the user.

4.3

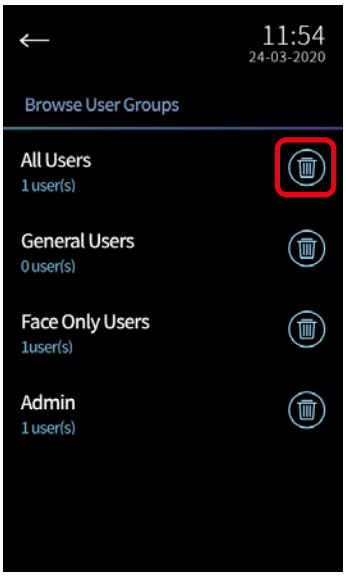
Browse and Delete User Groups



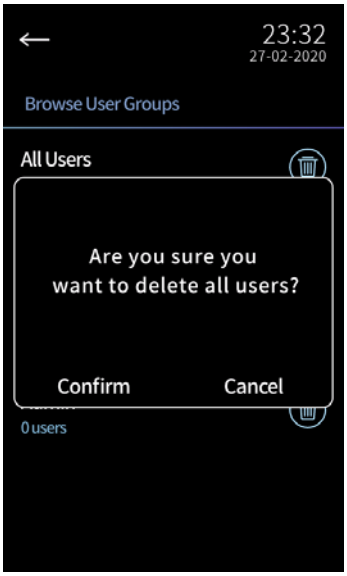
1 Select User Management from the Main Menu.



2 Select Browse User Groups.



3 On the Browse User Groups screen, press the trash can icon to delete a user group.



4 Press Confirm to delete the user group.

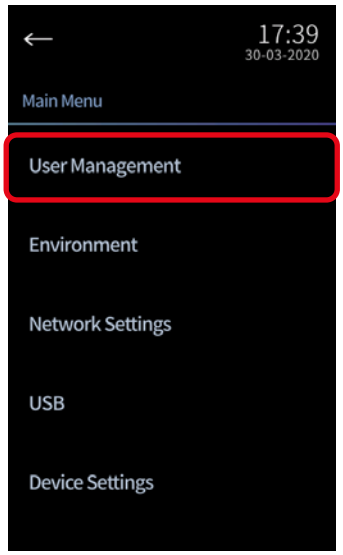
5 Browsing Access Logs

5.1 Methods of Browsing Access Logs

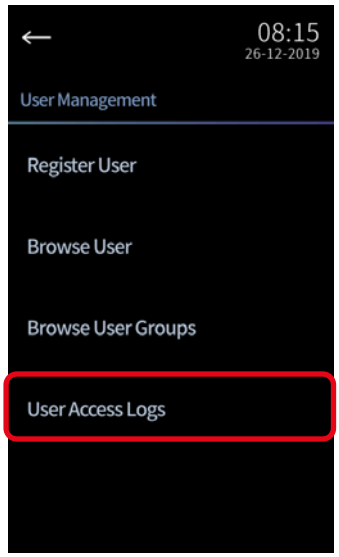
- The administrator can search user's access time, authentication results and authentication method(s).
- The administrator can also search the access record of a specific user by entering the User ID.

Methods of Browsing Access Logs	Description
Period	Access record by period (ex. today, yesterday, last 3 days, last week, last month, or the entire access record)
Auth. Result	Check the user's successful and/or failed authentication records.
Auth. Method	Check the access logs by the authentication method used (Card or Face).
User ID	Search the access record of a specific user by entering the User ID.

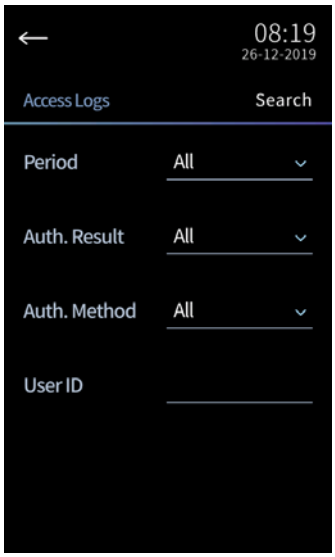
5.2 Browsing Access Logs



1 Select User Management from the Main Menu.



2 Select User Access Logs.

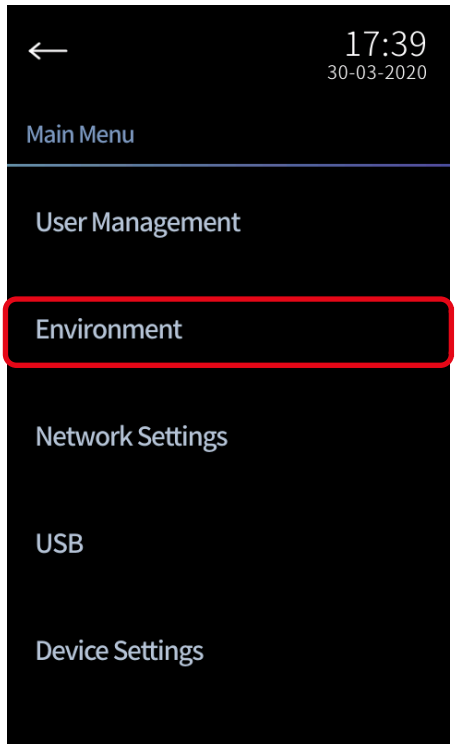


3 After setting the search conditions, press Search.

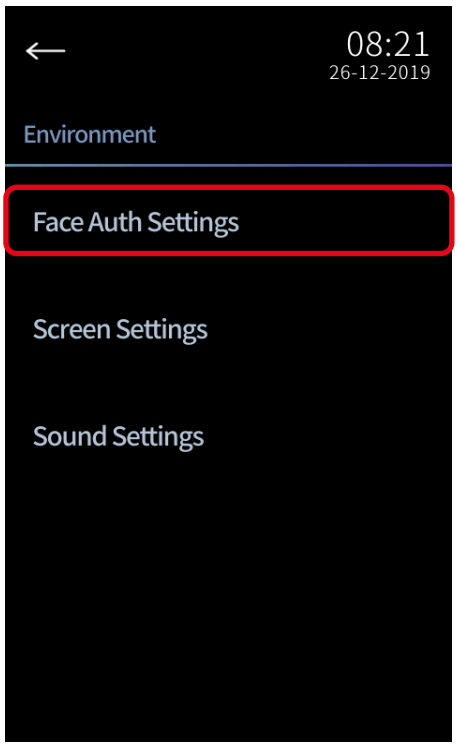
4 Check the status of each user's entry and exit.

6 Environment Settings

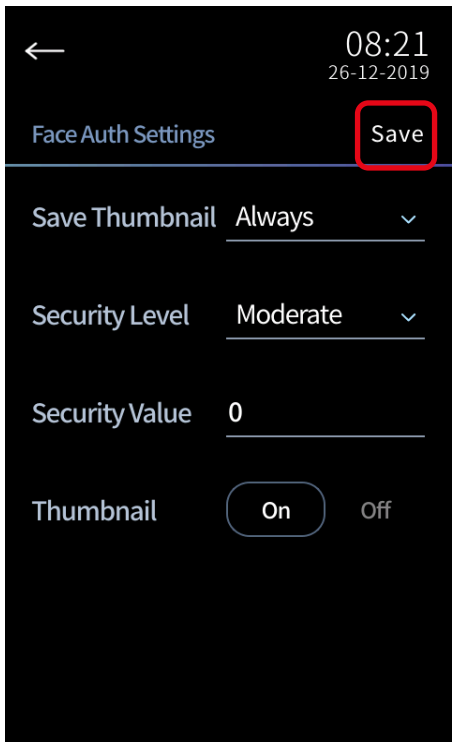
6.1 Face Authentication Setting



1 Select Environment from the Main Menu.



2 Select Face Auth Settings.

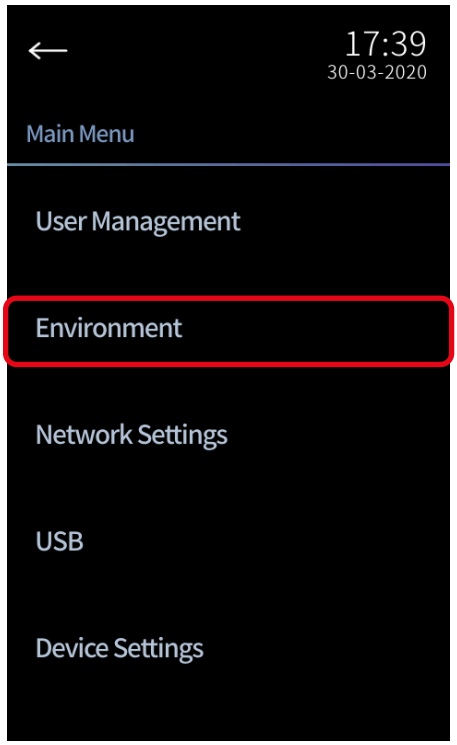


3 The current face authentication settings. In general, it is recommended that you use it without change.

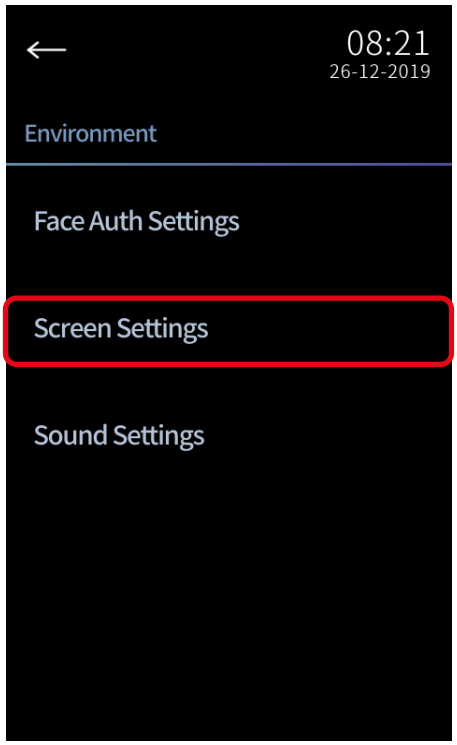
Setting Item	Description
Save Thumbnail	Select the options for saving thumbnail images after the face authentication is successful. A maximum of 300,000 images may be saved.
Security Level	Adjust the accuracy of matching level required to identify users. At a higher seccurity level, the False Rejection Rate (FRR) may also be higher.
Thumbnail	Choose whether to display the thumbnail when authenticated.

6.2

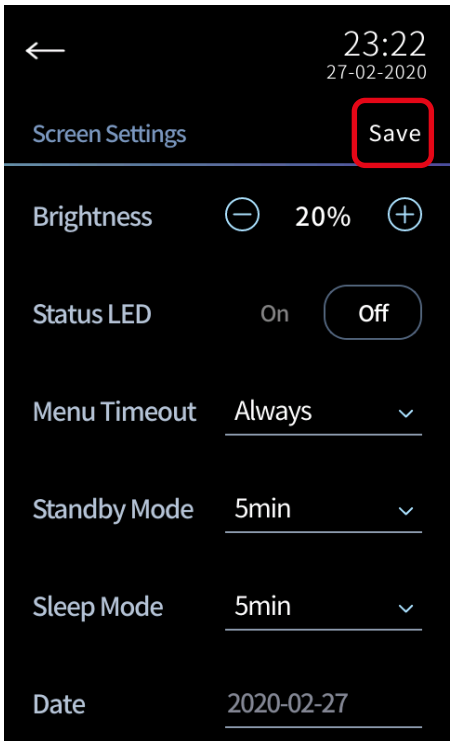
Screen Setting



1 Select Environment from the Main Menu.



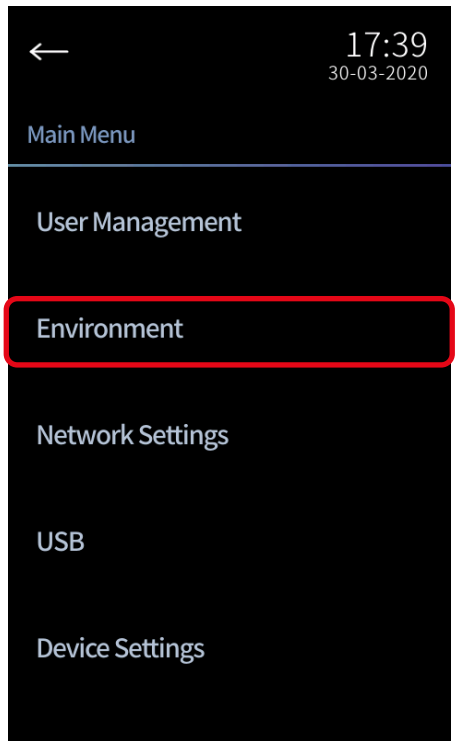
2 Select Screen Settings.



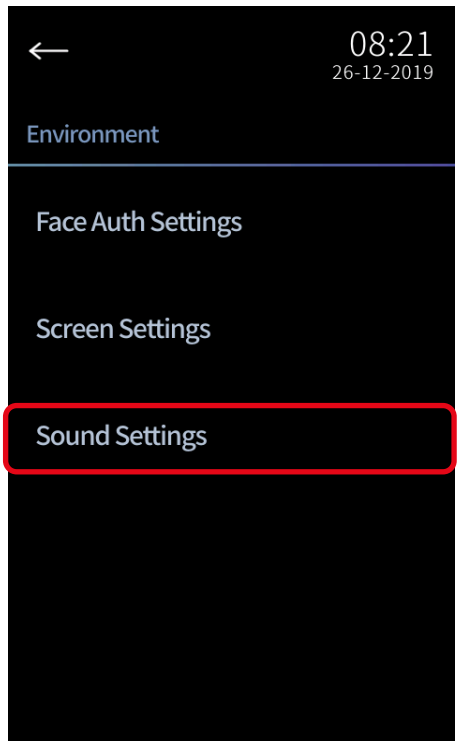
3 The current screen settings.

Setting Item	Description
Brightness	Adjust the display's brightness.
Status LED	Choose options for 'Status LED' located at the bottom of the device.
Menu Timeout	Select the duration of no activity in the menus after which the device would go back to the live view screen.
Standby Mode	Select the duration of no activity on the live view screen after which the timeout screen would turn on.
Sleep Mode	Select the duration of no activity on the timeout screen after which the device would go into sleep mode.
Date	Set the date.
Time	Set the time.

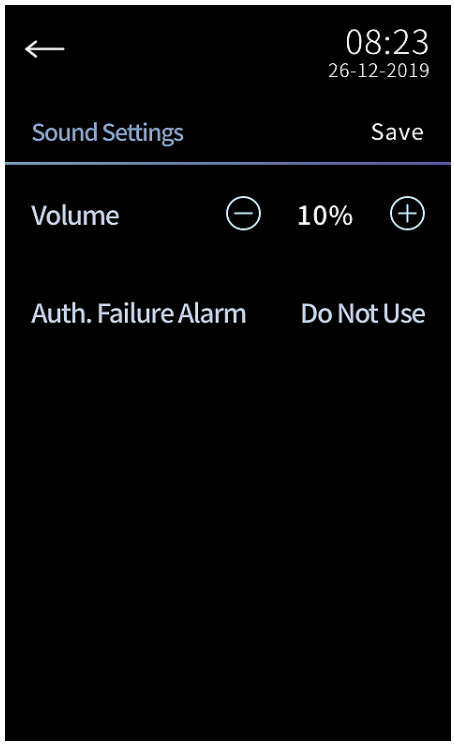
6.3
Sound Setting



1 Select Environment from the Main Menu.



2 Select Sound Settings.

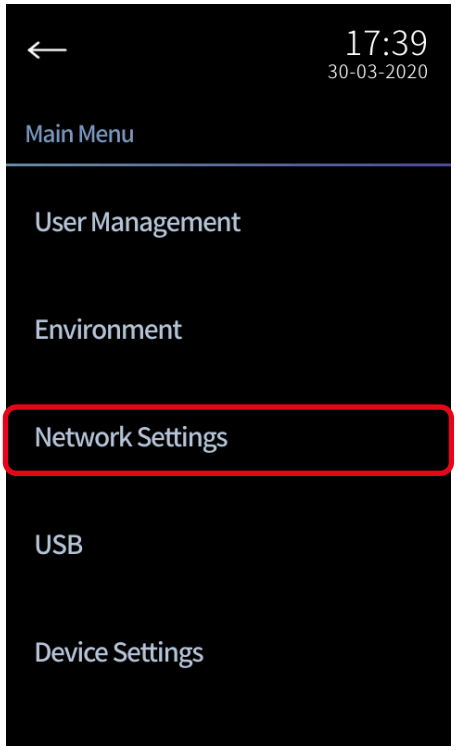


3 The current sound settings.

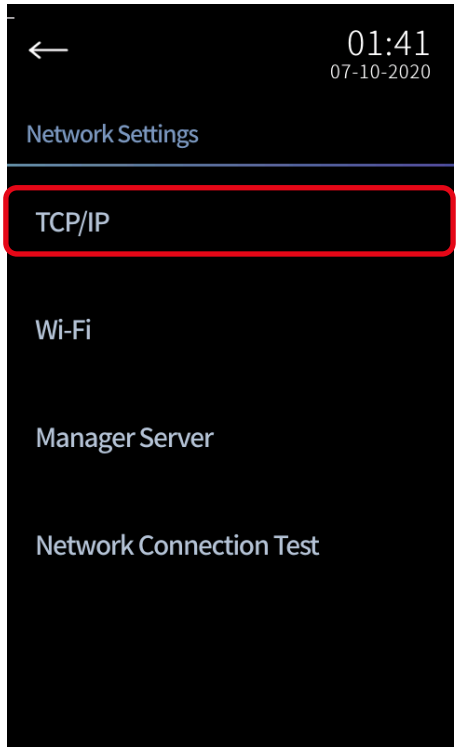
Setting Item	Description
Volume	Adjust the volume of the speaker of the device.
Auth. Failure Alarm	Select whether to sound the alarm and the number of times it sounds when card authentication fails.

7 Network Settings

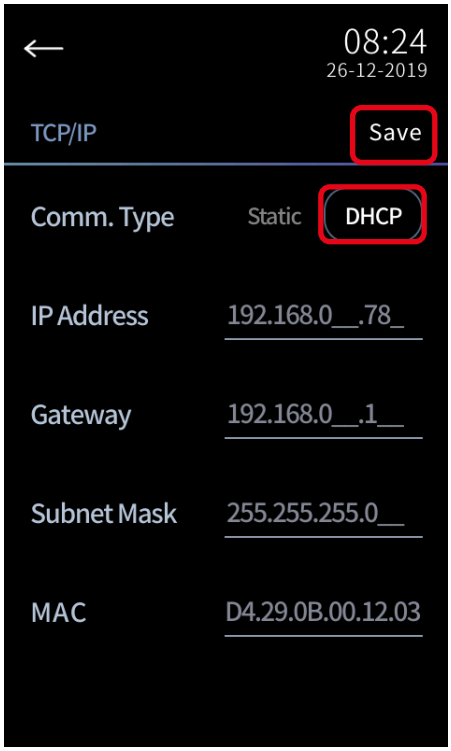
7.1 TCP/IP



1 Select Network from the Main Menu.



2 Select TCP/IP.

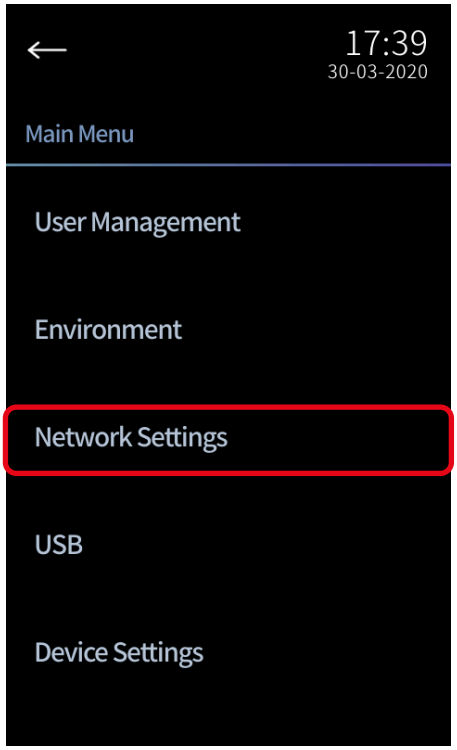


3 If you select Dynamic IP when connected to a router, an IP will be automatically assigned from the router.

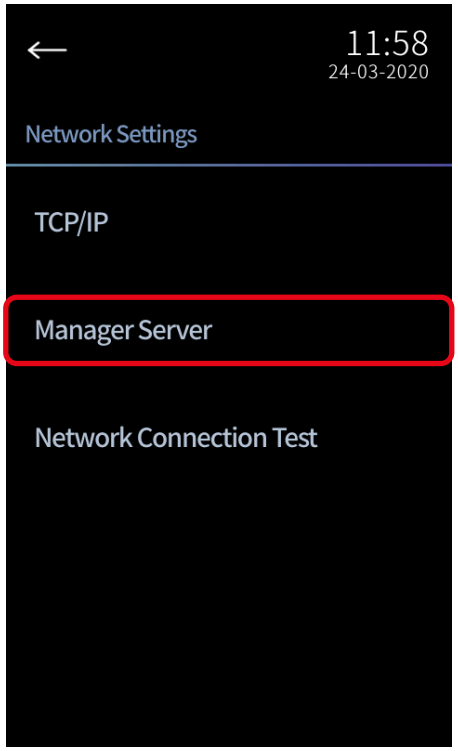
Setting Item	Description
Comm.Type	For static IP, you must personally enter IP address, gateway and subnet mask. If you select Dynamic IP, IP address is automatically assigned when connected to a router.
IP Address	Enter the IP address.
Gateway	Enter the Gateway address.
Subnet Mask	Enter the Subnet mask address.
MAC	Device's MAC address.

7.2

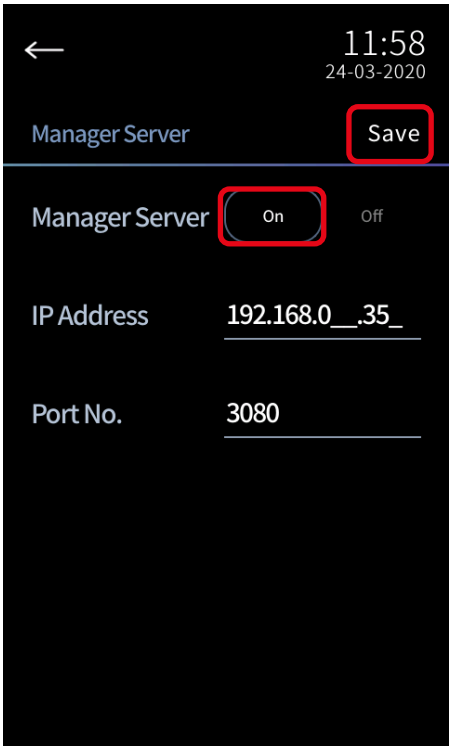
Manager Server Configuration



1 Select Network from the Main Menu.



2 Select Manager.

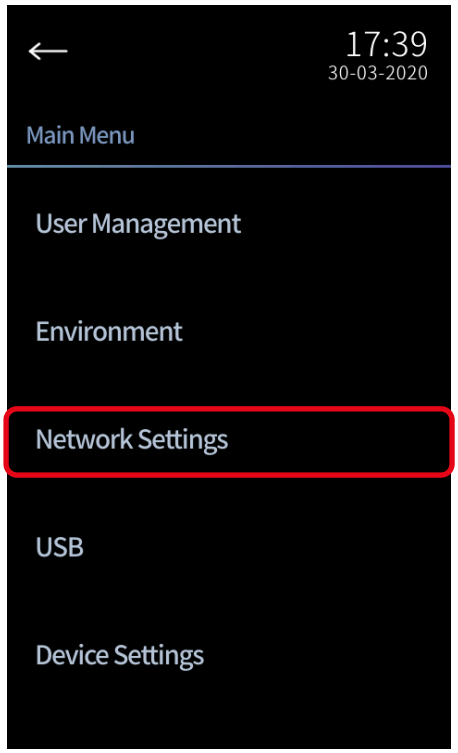


3 When connecting with Access+ Manager, turn on the Manager and enter its IP address.

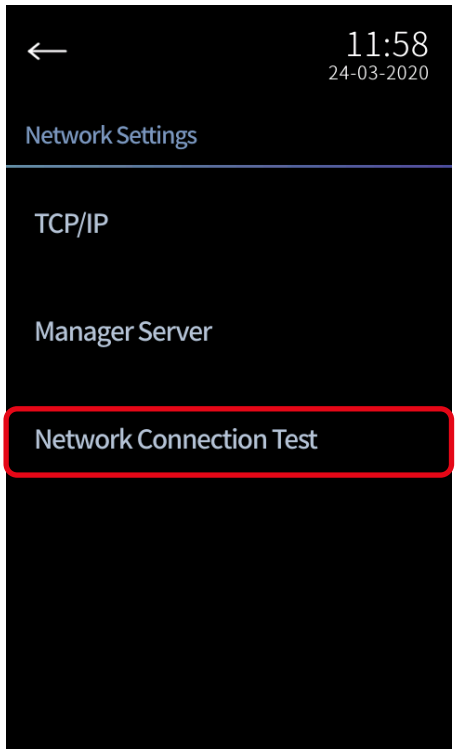
Setting Item	Description
Manager	Select On to connect with Access+ (a server program that facilitates Face A+ management).
IP Address	Enter the IP address of the Access+ server.
Port Number	Enter the port number of the Access+ server.

7.3

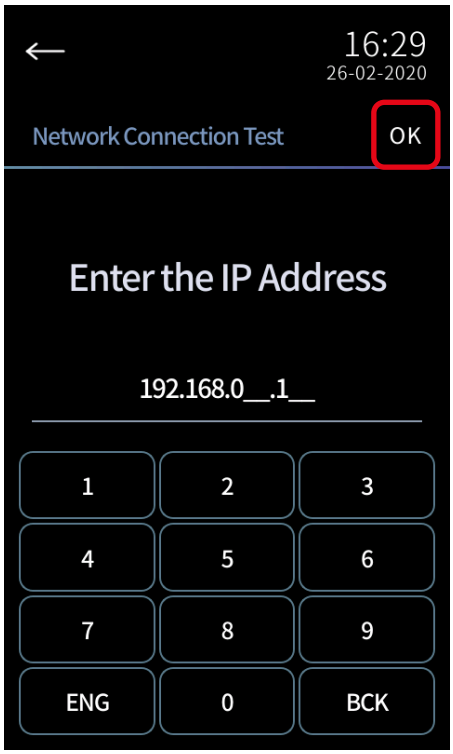
Network Connection Test



1 Select Network from the Main Menu.

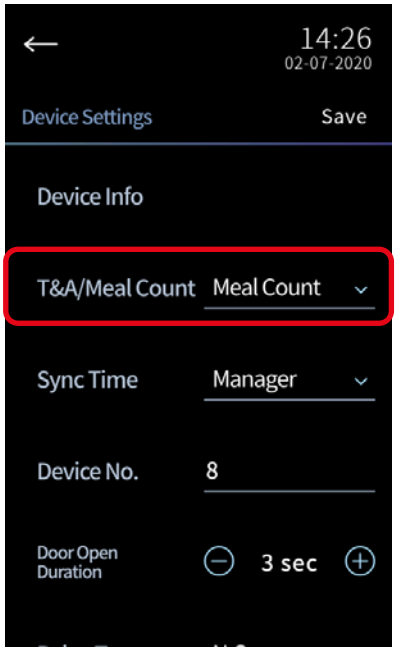


2 Select Network Connection Test.

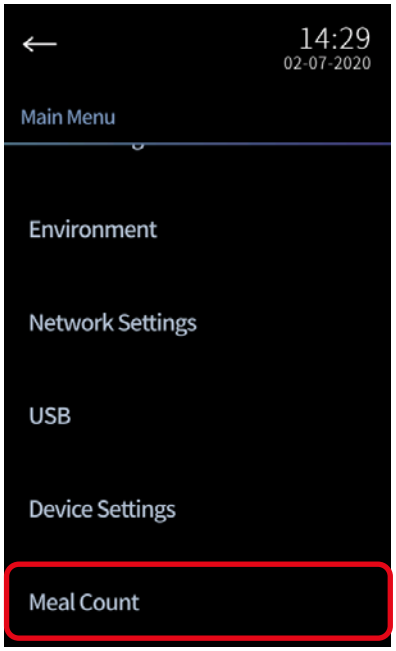


3 Test to check if the device is connected to the network. Enter the address of the gateway and press OK. After four ping tests, it checks whether the network is connected.

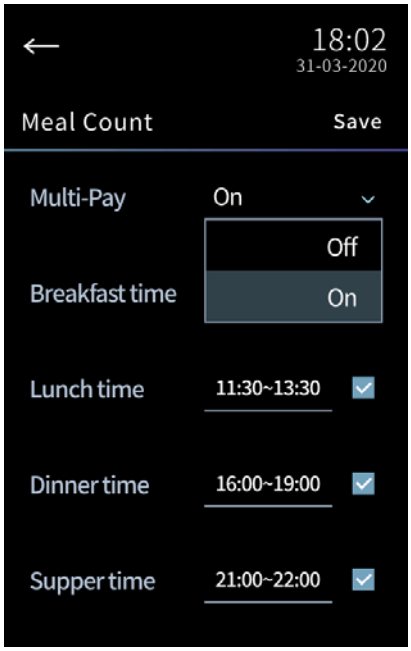
8 Meal Count



1 In Device Settings, select Meal Count.

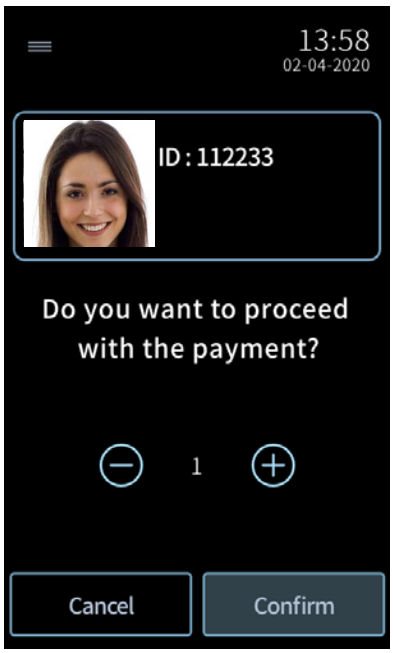


2 When you scroll down at the Main Menu, you can see that Meal Count Settings has been added.



3 Select whether to use Multi-Pay* and set the schedule.

4 When the setting is complete, the meal and time appears on the Live View screen as above.



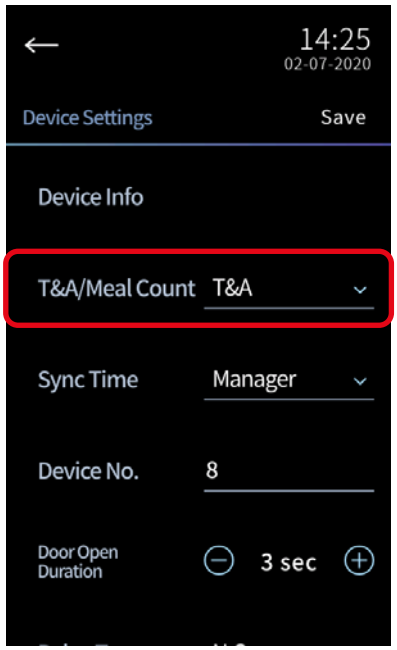
5 In the confirmation window, you can proceed to pay or not. If you do not click OK, payment will be cancelled.

*Set whether to use multiple payment option.

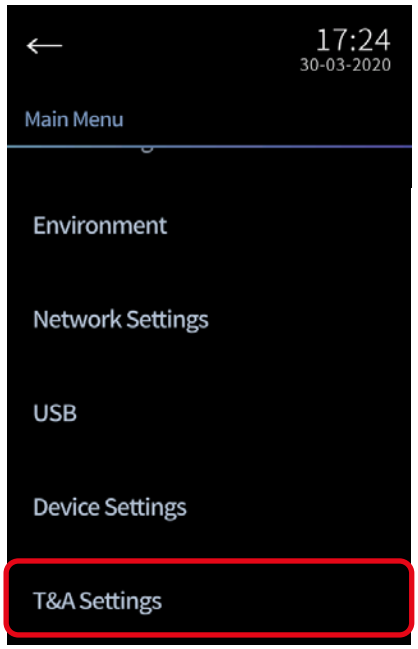
Off : the user will only be able to pay for one time.

On : the user will have the option to choose the number of servings as in 5 .

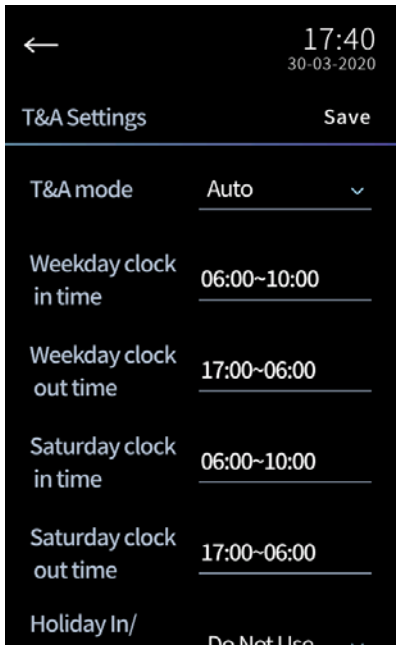
9 Time and Attendance



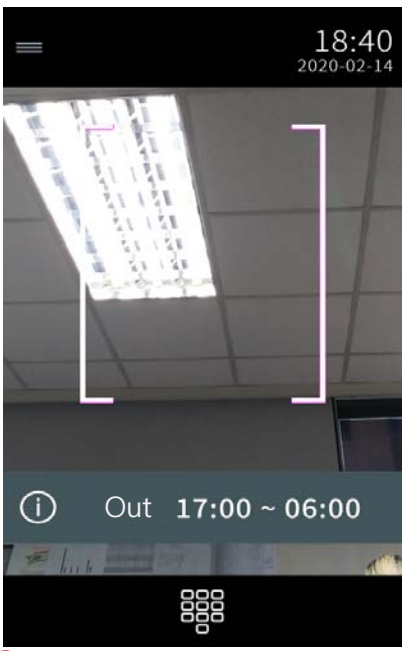
1 In Device Settings, select T&A.



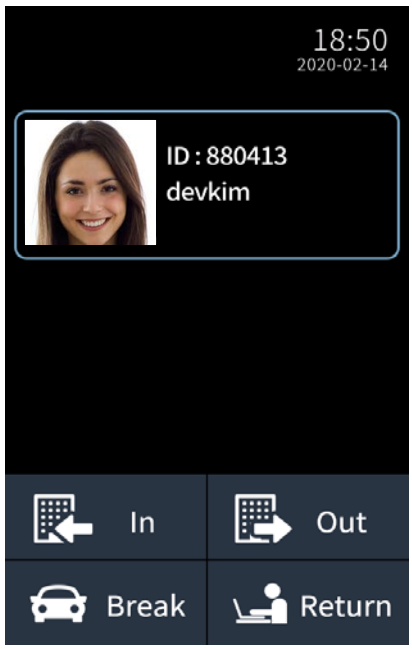
2 When you scroll down at the Main Menu, you can see that T&A Settings has been added.



3 Select in which mode* the device will run and set the schedule.



4 When the setting is complete, the type and time appears on the Live View screen as above.



5 If the mode is set as Manual, after authentication, the users may choose from In, Out, Break, or Return.

*Set whether to record automatically according to the schedule or manually by individual users.

The device can also be set specifically for in, out, break, or return.

10 Trouble Shooting Guide

Trouble	Guide
Touchscreen doesn't work.	- If the LCD touch panel is defective, touch may not work. - Check if there is any foreign substance on the touch panel.
Network connection failure.	- Check if the LED of the Internet port on the back of the device is blinking. - If the LED is not blinking, check if the wire is properly connected. - Go to [Main Menu]-[Network Settings]. - Select [TCP / IP] and check whether the IP address is correct. - If you had selected Dynamic IP, check if an IP address was assigned from the router. - If you had selected Static IP, check if the IP address was entered correctly. - Select [Network Connection Test], press OK and conduct the Ping Test again.
Authentication was successful, but the door does not open.	- Go to [Main Menu]-[Device Settings]. - Check whether the relay is enabled. - Check if the relay type (NO or NC) matches the door lock type. - On the Manager, check if the access time has passed for the user from [User Management]. - If it is not the access time, the user may be authenticated but the door will not open.
LCD screen failure. (No picture on the LCD)	- Check if the device is properly supplied with power. - Check the time set for Standby Mode in [Main Menu]-[Environment]-[Screen Settings]. - After the time you set has expired, the LCD screen will turn off automatically.
Voice message / Sound is not coming out.	- Check Volume is not set at 0 (zero) in [Main Menu]-[Environment]-[Sound Settings].
Card is not recognized.	- Check if the card is registered. - If you're tagging with an unregistered card, you'll see the message, "This card is not registered."

Trouble	Guide
Face is not recognized.	- Face may not be recognized in strong backlight conditions. - In backlight conditions, move your face closer to or away from the device and try the authentication again. - Check if face is covered by mask or hat. - For authentication, eyebrows and mouth must be recognized.
Firmware update failure.	- If updating through the Manager continuously fails, update using a USB. - If the version name on the completion popup starts with %1 after the device is rebooted, update again using USB.

Appendix

Disclaimers

- The information in this manual is provided with regard to CVT products.
- The right to use is acknowledged only for products included in the terms and conditions of the sales agreement guaranteed by CVT.
- The right of license to other intellectual property rights not discussed in this manual is not acknowledged.
- CVT does not guarantee or hold responsibility for the suitability and commerciality of the product for a specific purpose, or the infringement of patent, copyright, or other intellectual property rights with regard to sales or usage of CVT products.
- Do not use a CVT product in situations related to medical, rescue of human lives, or maintenance of life, as a person may be injured or killed due to product malfunction. If an accident occurs while a consumer is using the product under the situations described as examples above, employees, subsidiaries, branches, affiliated companies, and distributors of CVT do not accept responsibility, nor will they be liable for all related direct and indirect expenses or expenditures, including attorney fees, even if the consumer has discovered shortcomings in the product design or manufacturing process and claims this as a significant fault.
- CVT may modify the product size and specifications at any time without proper notice in order to improve the safety, function, and design of the product. Designers must keep in mind that functions or descriptions indicated as "to be implemented" or "undefined" may change at any time. CVT will implement or define such functions or descriptions in the near future, and CVT accepts no responsibility for compatibility issues and any other problems arising from such compatibility issues.
- If you wish to obtain the newest specifications before ordering the product, contact CVT through email: sales@cvtinc.co.kr
- Instructions for use included in this manual are also available on the website(www.cvtinc.co.kr) in multiple languages.

Appendix

Disclaimers

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

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, including interference that may cause undesired operation of the device.

The user manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with minimum distance 10cm between the radiator & your body.

Copyright Notice

Specifications

Main	
CPU	ARM Cortex-A9 Quad Core
EMMC Memory	16GB
DDR3	1GB
LCD	4.2 inch WVGA Touch Screen
Camera	Dual FHD CMOS Camera
RF Card	13.56Mhz Mifare
Mobile Card	NFC, BLE
1:N Verification Time	< 300ms
1:1 Verification Time	< 300ms
# of Max. Users	20,000
Simultaneous Max Persons	No limit
Face Template Size	0.5KB to 20KB (Configurable)
Text Log	3,000,000
Image Log	30,000
Data Encryption	AES-128
Sensor	
Sensor	2M FHD (1920x1080) Biometric IR Sensor 2M FHD (1920x1080) Color Sensor
IR LED	940nm PWM IR
Option	
RF Card	13.56MHz Mifare/DesFire

Interface	
Host Comm.	RS232 UART (Default) USB 2.0 up to 480 Mbps (Option)
External I/O	1x Switch input, 1x Relay out, Ethernet, Speaker, MIC, Door Sensor
Hardware	
Supply Voltage	12 VDC Regulated
Dimensions	104 x 204 X 40mm (L x W x H)

CVT
Creative Value Technology

CVT Co., Ltd.
306, Building D, Yangjae AI Hub, 39 Maeheon-ro 8gil
Seocho-gu, Seoul, Rep. of Korea (Postal Code : 06770)
Tel : +82-70-4490-9388 | Inquiry : info@cvtinc.co.kr | www.cvtinc.co.kr