SNAPCHECK MOAI-O

Product Documentation for Demonstration Kit

MOAI_umandk Rev.1.0 | 2025

ANDOPEN

About document revisions

The following revisions have been made to the documentation

MOAI_umandk Revision History

Date	Version	Change History
Feb. 17, 2025.	Rev.1.0	Initial deployment

About this product documentation

This instruction manual is a guide for the installation, system configuration, setup, and use of the SNAPCHECK MOAI-O, which is a converged biometric access control device for identity verification purposes, including access control, time and attendance, etc.

Be sure to read this manual before installing and using the product. When connecting SNAPCHECK MOAI-O to external devices such as access control panels, access control servers, door locks, etc., please refer to this Product Documentation for Demonstration Kit or contact the product's supplier for proper connection.

The software AOS embedded in SNAPCHECK MOAI-O performs functions such as identification and execution of access control policies, device startup conditions, and device management and is accessible as a web-based service through web browsers such as Chrome, Edge, and Safari on administrators' PCs, laptops, and mobile devices.

Ordinary users (non-administrators) who are not authorized to install, configure, and access the product do not need to familiarize themselves with the AOS content in this product manual and should be aware that AOS only works on SNAPCHECK MOAI-O devices and cannot be applied to other HW.

This product manual describes SNAPCHECK MOAI-O and includes the AOS User Guide as an <Appendix> for reference.

This product documentation is distributed electronically on our website https://www.andopen.co.kr, and only the Installation Guide is included with the product.

The content of the product documentation and specifications of the product are subject to change without prior notice to improve the performance and functionality of the product.

Copyright

Certifications of SNAPCHECK MOAI-O

Notations

To help you understand the content, note the meaning of the following markings.

■ *** Note ***
We've recorded any useful notes or additional information you might want to know when using the product.

■ ***Cautions*, *Warnings***
We've documented the things you need to know or do when using our products.

■ **Figure Description**
Illustrations are used to help you understand the use of the product or to show examples.

■ **>** : Indicates the bottom tree structure of the user interface in AOS. For example, "File > Save" indicates the Save menu under the File menu.

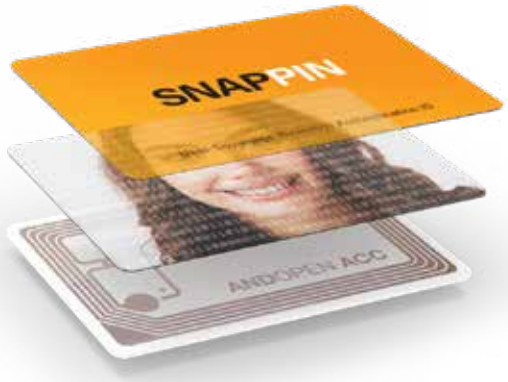
■ **[ ]**: Square brackets indicate the button to press on the AOS page being described.
Example: [Save] is the button labeled "Save".

■ **'Enter '**
This means typing directly on the keyboard.

■ **'Select '**
This means selecting one of the items that appears by pressing a pull-down, radio button, etc. in the GUI.

■ **Cross Reference**
References to other parts of the manual are indicated by double quotes (" ")

Product Features



SNAPCHECK MOAI-O
ID Card and Face Recognition
Converged Access Terminal

SNAPPIN
High secured Bio-ID card
Personalized by using users photo and pre-delivered to personal user

SNAPCHECK MOAI-O is a product that is the core of a 'card, biometric converged authentication solution' that provides flawless facial recognition accuracy and usability by using a 'biometric card' that encrypts and embeds the user's facial image into the card.

Even though it uses the familiar "look-and-tag" behavior like card authentication, it uses facial recognition, and uses RGB/IR dual cameras to work well in different lighting environments, and is built to prevent malicious authentication attempts.

By decentralizing biometric information to the user's biometric card, users have exclusive control over their own biometric information. That is a self-sovereign biometric authentication system. As a result, biometric information is not stored anywhere, including authentication terminals and servers, and there is no networked transmission process. Thus, this is a new concept of biometric authentication system that completely blocks the risk of sensitive information leakage and protects privacy.

This allows SNAPCHECK MOAI-O to integrate with existing card-based access control systems out of the box without any physical changes.

In addition, SNAPCHECK MOAI-O can be easily configured and managed using AOS, a web-based access control management software embedded inside SNAPCHECK MOAI-O without using a separate access control management SW.

For more information on the 'SNAPPASS' solution, biometric cards, and products, and for consulting on building an access control system using them, please contact the product provider or ANDOPEN.

Safety precautions

Please read the following safety precautions before using the product to ensure proper use, your safety, and to prevent property damage.

Failure to do the following can result in serious harm

■ Before using a product, be sure to check the product's usage information and performance.

■ To effectively use the product's features, you must read this documentation and install and use it correctly.

■ Do not throw or impact the product when using or moving it. It can cause electric shock, fire, malfunction, and personal injury. If the product is damaged, contact Customer Support.

■ Do not install the product in direct sunlight, where heat is generated, or near an open flame, as the heat could cause a fire or damage the product.

■ Never use a damaged cable or connect a nonconforming power supply. Doing so may cause electric shock, fire, malfunction, and personal injury.

■ Keep the product's connections (power and cable) free of liquids, dust, and conductive debris such as metal dust. Also, do not poke the connections with pointed objects or apply excessive force.

■ Corrosion or a temporary short circuit in the connecting terminals can cause the product to explode or catch fire.

■ When installing the product, consider the location, position, and angle of the installation to prevent passersby and users from bumping into the installed product.

■ If you have a problem with the product, stop using it and contact support.

■ Be sure to follow the specifications recommended in the manual for DC power input to SNAPCHECK MOAI-O and the lock power, input signals, wiring cables, etc. connected to SNAPCHECK MOAI-O.

Failure to do the following could result in personal injury or property damage.

■ Modification or attachment of parts to this product by anyone other than the manufacturer is strictly prohibited. Any product failure resulting from such actions will void eligibility for free service and warranty coverage.

■ Let a professional install your product.

■ Avoid installing and using the Product in dusty or dirty areas. Dust or debris can cause the product to malfunction or perform poorly.

■ Do not install or use the product in areas exposed to magnetic fields or electromagnetic interference, as this may cause damage to the product or impair its performance.

■ Check the wiring information and connect the appropriate cables. Do not force the cable or apply excessive force. This can cause the product to malfunction or damage cable connections and parts.

■ Do not attach attachments or paint the product. Sensitive optics may not work.

■ Avoid scratching the product and keep it clean at all times. Clean the front of the product regularly to remove dust, dirt, and debris. When cleaning, please wipe with a soft cloth (do not use acids, detergents, etc.).

■ Use the product at room temperature and avoid exposure to high temperatures or direct sunlight. In particular, ensure that the product’s camera is not pointed at strong light sources, such as halogen lights or sunlight, as this can decrease recognition performance.

■ Keep this product away from water, as it is not water-resistant.

■ Do not leave management PCs unattended with access to the product's management software (AOS).

■ Ensure that information that must be secured, such as user accounts, passwords, user DBs, and authentication logs, are not leaked.

■ Do not place or hang objects on the product.

■ AOS is shipped embedded on the device and installed by the vendor (preinstalled), so user installation is unavailable.

■ SNAPCHECK MOAI-O will operate according to the settings you make through AOS, so please read this documentation carefully before setting up and using it to avoid unintended operation.

■ Limit administrators who have access to AOS to those authorized by your organization, and do not leak login IDs and passwords.

■ We recommend that you securely manage administrator and user information stored in AOS so that it is not lost and that you periodically make backups of user information, just in case.

■ Do not attempt to access, delete, or modify AOS for any purpose other than in the prescribed manner outlined in this documentation.

Table of Contents

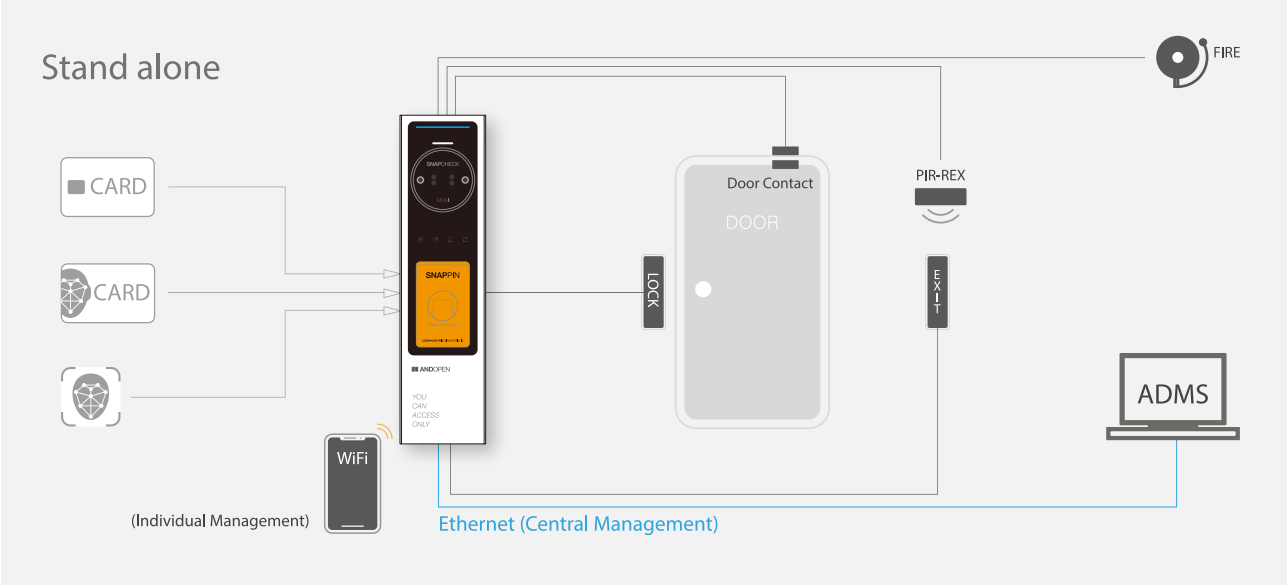
■ SNAPCHECK MOAI-O Product Documentation

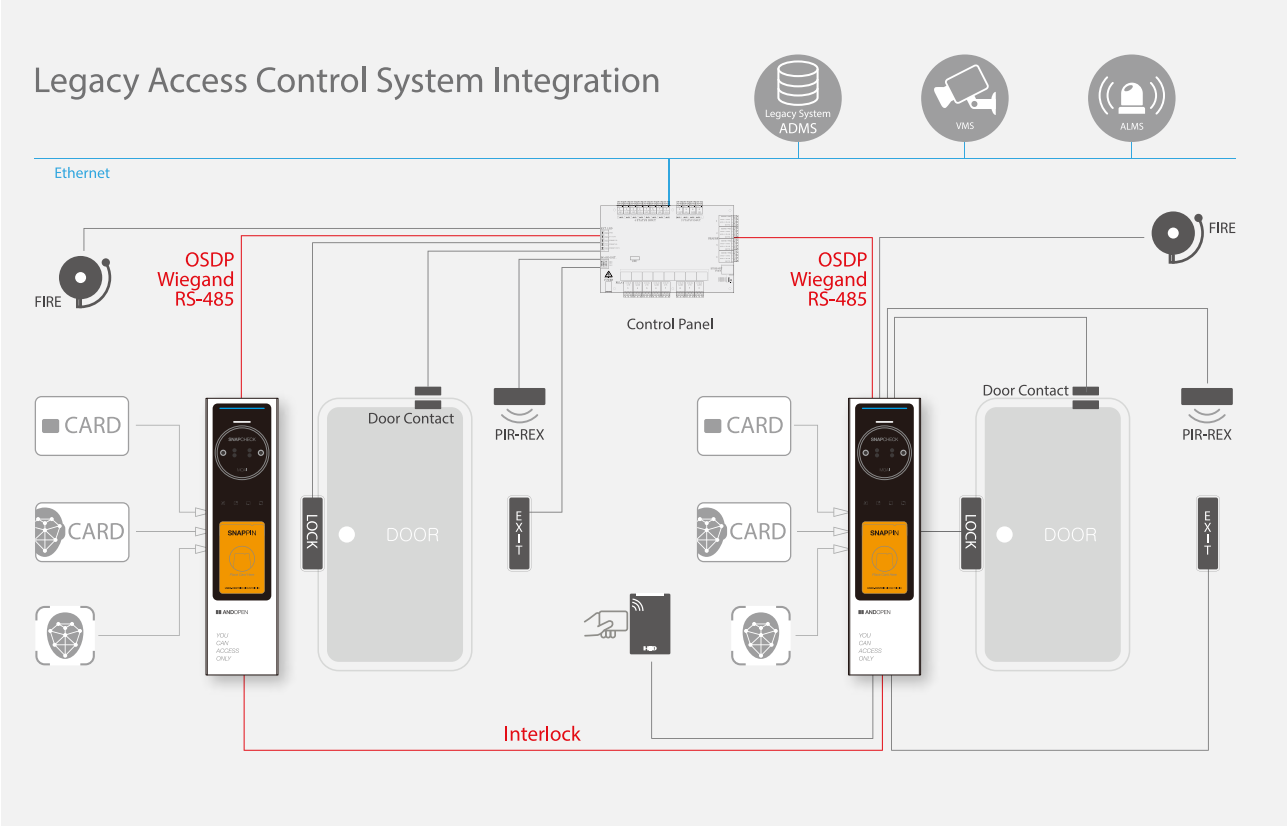
<Appendix>

■ AOS User Guide

■ SNAPCHECK MOAI-O Product Documentation

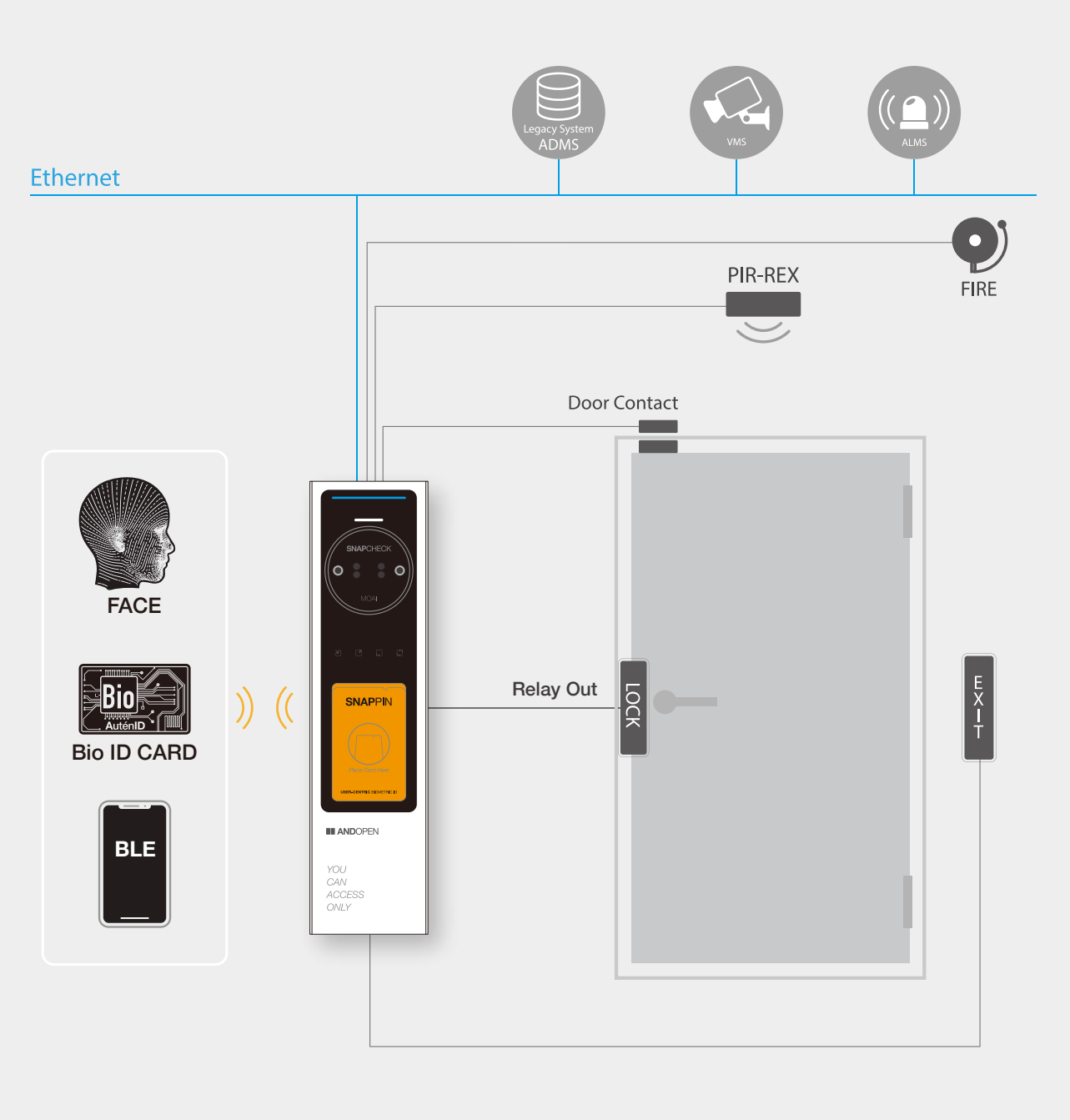
1. System Configuration





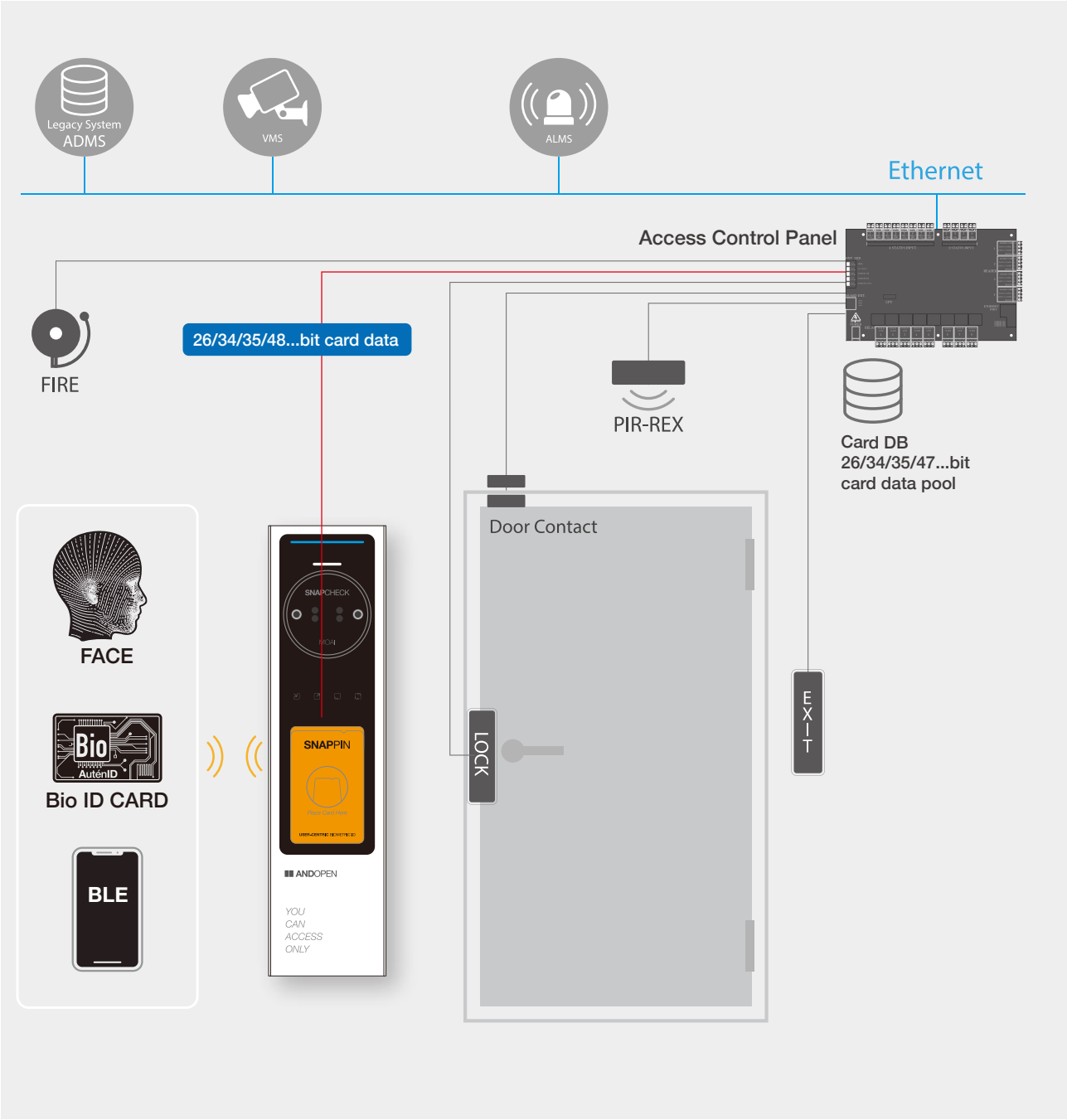
SNAPCHECK MOAI-O can be used to configure various types of access control systems as shown in the figure above,
Instantly upgrade and integrate into a biometric authentication system by simply replacing the RF reader with an SNAPCHECK MOAI-O, while still using all the resources of a traditional card-based system.

1.1 Standalone operating mode



This figure describes a typical configuration where SNAPCHECK MOAI-O directly controls a door by connecting the lock, exit button, door sensor, fire alarm input, etc.
Users perform facial recognition by tagging their biometric card while looking at SNAPCHECK MOAI-O for facial authentication.
SNAPCHECK MOAI-O could be directly connected with diverse access control devices, upon authentication success, SNAPCHECK MOAI-O opens the door.

1.2 Access Control Panel Integration Mode



In this configuration, SNAPCHECK MOAI-O works with the access control panel to control the door. Users perform facial authentication by tagging their biometric card while looking at the SNAPCHECK MOAI-O.

Upon successful authentication, SNAPCHECK MOAI-O sends the biometric card's card number (the card number that is matched to the user in the access controller) to the access control panel via Wiegand communication, and the access control panel unlocks the door if the transmitted card number exists in the access control panel's card number database.

Follow the access controller manufacturer's instructions for the Wiegand communication format, wiring method, etc.

■ SNAPCHECK MOAI-O Product Documentation

2. Product

2.1. Specification

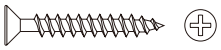
Model Name	SNAPCHECK MOAI-O
Central Processing Unit	Heterogeneous Processor Configuration; Arm Quad core, Arm Dual Core, 1.2 TOPS NPU, and MCU
Display	3-color LED indicator
Touch buttons	4 Button - For Time & Attendance
Supported Authentication modes	Card Authentication Biometric Card & Face Recognition Fusion Authentication TEMPICS (see Appendix)
Camera	RGB/IR dual camera
High-speed image processing	Low-light and backlight compensation, auto exposure, high dynamic range (HDR), Dual Image Fusion.
Fraud Prevention (Liveness)	AI based anti-spoofing technology.
Face Verification Range	0.5m ~ 2.0m
Facial Recognition Speed	< 0.3 sec.
Lens and angle of view	Fixed focus combined lens, around diagonally 70 degrees
Accuracy	100% (over six nine percent, 99.9999%)
Recommended number of facial recognition users	Unlimited
Recommended number of users faces enrollment	Up to 20,000 faces (in TEMPICS authentication)
RF Card Reader	13.56Mhz (ISO-14443A/B, ISO-15693)
Card Technologies	SNAPPIN / Mifare / Desfire / Felica / Java / NFC / iClass (optional)
Communication	Ethernet / WIFI / RS-485
Input	Wiegand / Fire Alarm / Door status / Exit button
Output	Dry contact / Wiegand
Event Logs	1,000,000 events can be stored
Sound Output	Voice / Buzzer
Power Input and Consumption	6~28VDC, 15Watt (Peak)/12 Watt (Operation)
Connectors	RJ45, 17p terminal block
Data encryption	AES 256 encryption
Encrypting communications	ASE 256 encryption
Operating Temperature / Humidity	-10°C ~ 60°C / 0%~80
Dimension	86 × 34 × 330 (WDH, mm)
Authentication	KC, FCC, CE

* **TEMPICS:** ANDOPEN's patented technology that safely protects facial information from hacking and other malicious theft, increasing user convenience while ensuring security.
* **SNAPPIN:** ANDOPEN’s biometric card, other cards cannot embed biometric information.

Caution
Comply with all electrical standards recorded in the specification. Provide sufficient and reliable DC power to SNAPCHECK MOAI-O

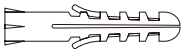
2.2 Components

Upon purchasing the product, verify that all included components are present. If any components are missing, contact your sales representative.



M4 x 25mm (4)

M4 x 15mm (4)



Nylon screw anchor (4)

M3 x 8mm (1)

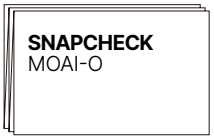
M3 x 8mm (1)

M3 x 6mm (1)

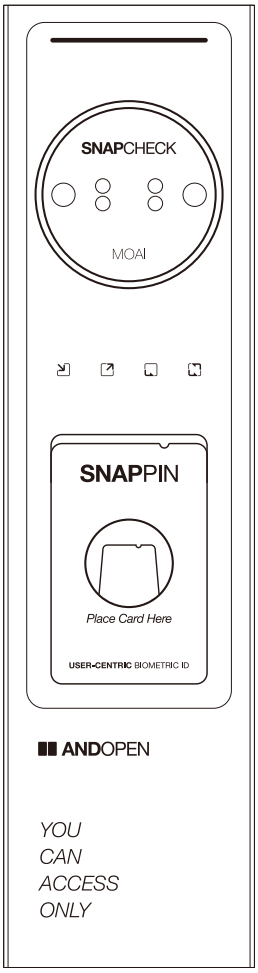
Nylon cable tie (1)

22 ohm resistor (30)

Ferrite (1)



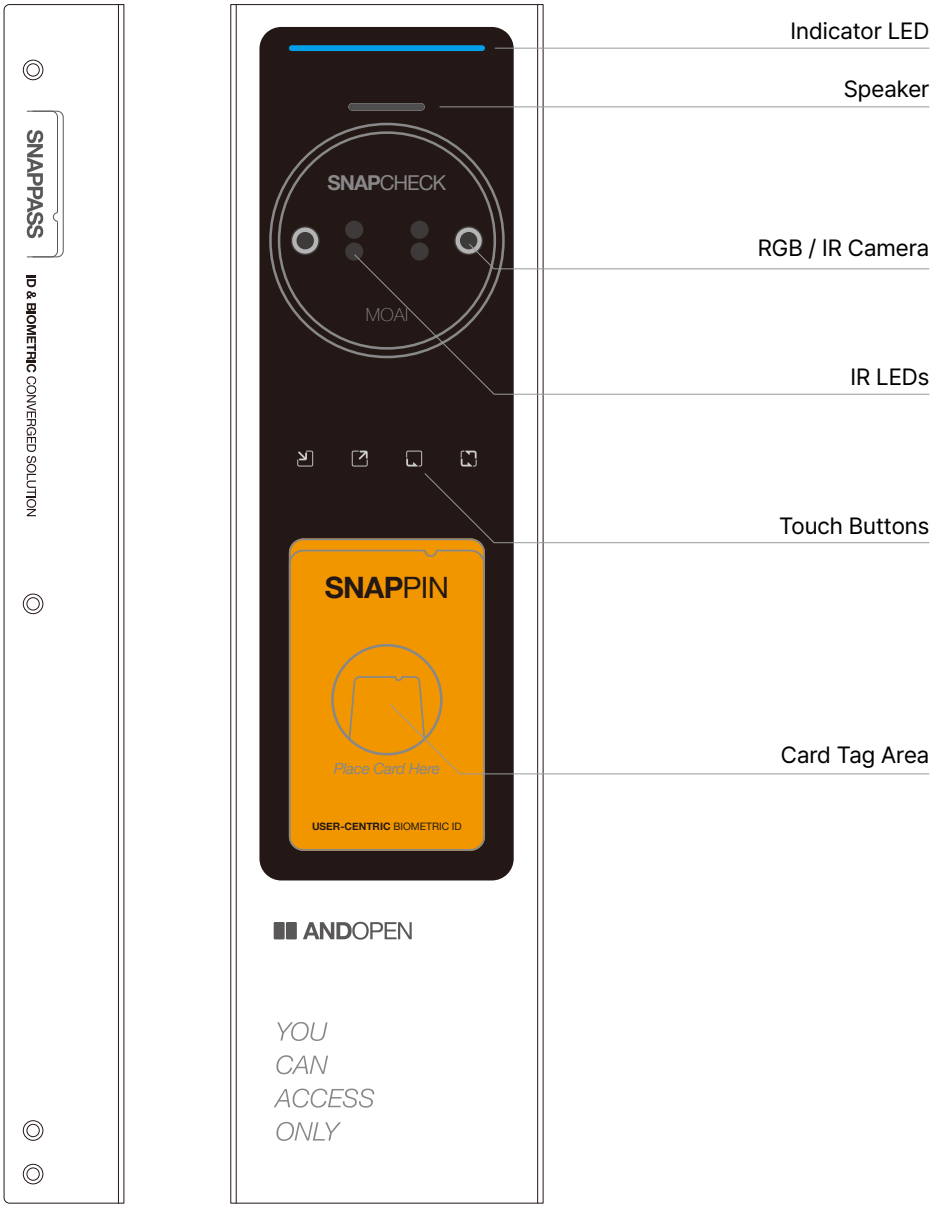
Installation Guide (1)



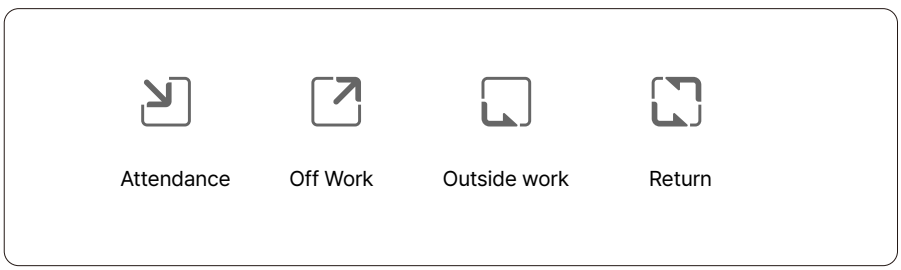
SNAPCHECK MOAI-O

2.3 Part Names and Functions

SNAPCHECK MOAI-O



Touch Buttons



■ SNAPCHECK MOAI-O Product Documentation

3. Installation

- Your product must be installed by a qualified service professional and in compliance with any local laws or rules.
- All wires, cables, etc. required for the installation must be routed through grounded, flame-retardant conduit to protect against breaks, shorts, fire, etc.
- Do not connect the cable when the power is on.
- It is recommended that the provided resistors be connected for reliable communication and circuit protection.
- Refer to the Installation Guide that shipped with your product along with this manual.

3.1 Where to install

- Install on a stable, level surface.
- For optimal performance, ensure that the front face of SNAPCHECK MOAI-O is installed parallel to the user's face.
- For ease of use and optimal performance, install SNAPCHECK MOAI-O at eye level, taking into account the average height of your users.

- Recommended height (height from floor to Camera):
  Northeast Asia: 154 cm/ Southeast Asia: 152 cm/ Americas: 158 cm/ Northern Europe: 163 cm

3.2 Lighting environments

- Set up SNAPCHECK MOAI-O in a location where the lighting evenly illuminates your face.
- Avoid lighting from above, behind, and to the side of your face.
- Avoid direct sunlight or strong lighting on SNAPCHECK MOAI-O.
- Avoid strong downward or upward light and backlighting that creates shadows on the face.

3.3 Wiring

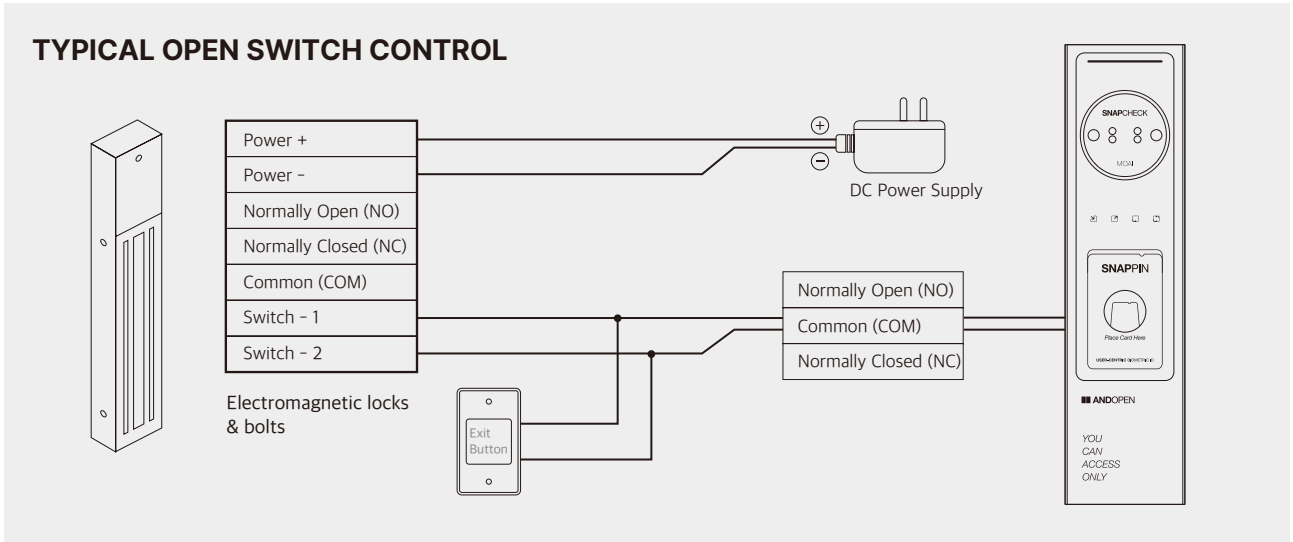
• Familiarize yourself with the wiring manuals of the lock and external device provider, and wire SNAPCHECK MOAI-O concern the operating characteristics of the lock. Also, be sure to fully understand the functionality of AOS later in this manual and proceed with the wiring in line with your purpose.

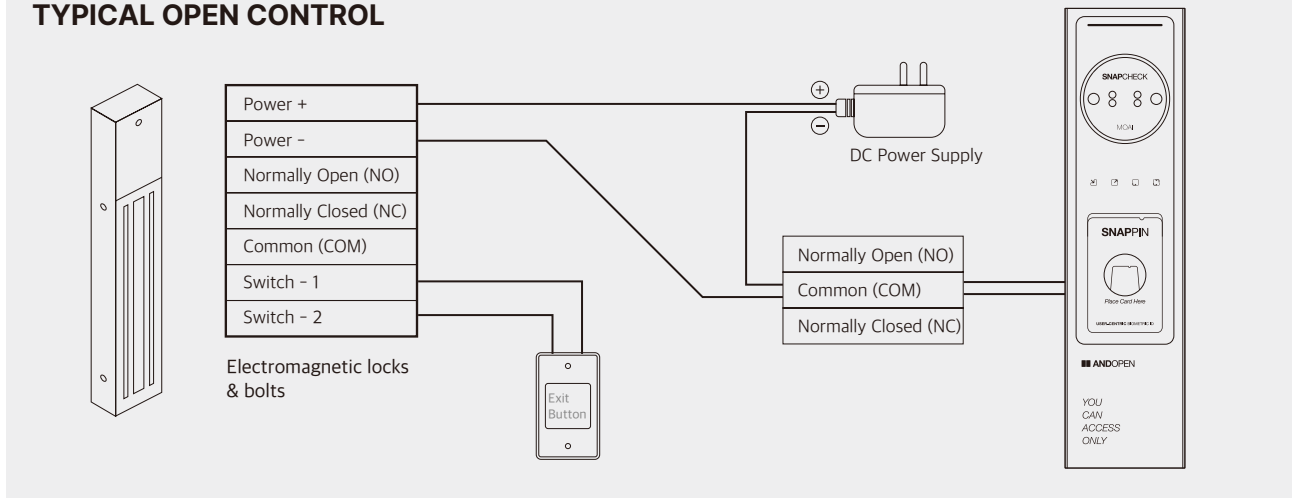
• The maximum current allowed by the Relay circuit in SNAPCHECK MOAI-O that connects to the lock is 2A. Check the compatibility and maximum current of the locks such as EM-LOCK, Dead Bolt, and Striker, and ensure that the current applied to the Relay circuit in SNAPCHECK MOAI-O is 1.8A or less. If more current is applied, permanent circuit damage may occur.

• When interfacing with an access control panel, please refer to the manual provided by the manufacturer for wiring.

* Caution
- All wires used for wiring should be shielded AWG22
- Use Shielded Twisted Pair (STP) Cat5e, 568B for Ethernet connections.

The figure below is just a typical wiring example. Wiring correctly according to users' configuration environment.





■ SNAPCHECK MOAI-O Product Documentation

4. Using the product

■ Boot SNAPCHECK MOAI-O

- When power is applied, the BLUE LED on the top of the device lights up.
- About 25~30 seconds later, the device plays a booting sound.
- When the boot sound plays, SNAPCHECK MOAI-O is ready.

■ Facial Recognition

- When the dual camera of SNAPCHECK MOAI-O detects the face of a person, four infrared LEDs light up.
- Facial recognition is performed by tagging a biometric card while directly looking at the camera. (Keep the card tagged until you hear the card reading sound)
- The upper LED lights up red upon authentication failure, and SNAPCHECK MOAI-O plays the fail sound.
- The upper LED lights up green upon successful authentication, and SNAPCHECK MOAI-O plays the success sound.

5. Troubleshooting

If the device becomes slow or operates abnormally due to unexpected causes such as static electricity or unstable power, restarting the SNAPCHECK MOAI-O may resolve the issue.
You can reboot by accessing AOS (SNAPCHECK MOAI-O built-in Web-based management software) and find the 'System' tab, press the [Reboot] button.

Alternatively, you can reboot by physically disconnecting and reapplying power (disconnecting and reapplying DC power about 5 seconds later).

In some cases, a power reboot may resolve more issues.

<Appendix>

■ AOS User Guide

1. AOS Overview

AOS is a terminal-embedded software for setting SNAPCHECK MOAI-O's operation conditions, setting authentication and access control policies, user management, device management, etc.
By using AOS, you can perform the following functions.

Note
AOS is pre-installed on SNAPCHECK MOAI-O from the vendor and does not support user installation.

Each function is described in detail in **"2. Feature descriptions and usage".**

・Connect to your device
・Login
・Monitoring
・Issuing biometric cards
・User Management
・Setup Device
・Logs Inquiry
・Logout

2. Feature descriptions and usage

2.1 Connect to your device

2.1.1 Set environment for connection

Preparation:
・Equipment with wired and Wi-Fi network connectivity, such as PCs and laptops (hereinafter “PCs”)
・Ethernet Cable (Cat5e, 568B)
・SNAPCHECK MOAI-O which is powered on

To access AOS, you must first connect SNAPCHECK MOAI-O with the administrator's PC with authorized access.
The administrator can connect to SNAPCHECK MOAI-O using two methods: a wired network and a Wi-Fi network.

Connecting over a wired network
First, connect the PC and the RJ45 port on the back of the SNAPCHECK MOAI-O to each other with an Ethernet cable.

Once the PC and SNAPCHECK MOAI-O are physically connected, the PC and SNAPCHECK MOAI-O can attempt to network with each other.
For the PC and SNAPCHECK MOAI-O to communicate, you must make both devices exist on the same network.

The default wired network setting of SNAPCHECK MOAI-O is shown below

IP address	**192.168.30.1**
Netmask	**255.255.255.0**
Gateway	**192.168.30.254**
DNS	**8.8.8.8**

So, for your PC to exist on the same network as SNAPCHECK MOAI-O, **PC must have** the following **network settings**

IP address	192.168.30. **X** (X value is any one of 2 to 254)
Netmask	255.255.255.0
Gateway	192.168.30.254
DNS	8.8.8.8

Connecting via Wi-Fi
SNAPCHECK MOAI-O acts as the Wi-Fi Access Point (Wi-Fi AP) initially. Find SNAPCHECK MOAI-O by searching for Wi-Fi APs on the administrator's PC. The name of the AP appears as a 'MOAIAbc2'
Try connecting to the discovered SNAPCHECK MOAI-O Access point and type the required access password.
The AP access password is '**andopen1234**'. (Case sensitive)
The IP address to access SNAPCHECK MOAI-O through this Wi-Fi connection is '**10.42.0.1**'. The Wi-Fi connection method allows you to access SNAPCHECK MOAI-O directly without having to configure your PC's network settings.

To set up your PC's network, familiarize yourself with how to set up your OS's network, or if you're unfamiliar, seek help from a network administrator or professional.

2.1.2 Accessing AOS

Once the connection environment is ready, you can access AOS. AOS is a web-based service software embedded in SNAPCHECK MOAI-O to set the operation of SNAPCHECK MOAI-O, and it can be accessed through a browser on a PC without installing a separate program on the administrator's PC.

With network connection between SNAPCHECK MOAI-O and administrators PC or devices, launch a web browser on the administrator's PC.
Enter the IP address of SNAPCHECK MOAI-O in the address bar of the web browser to access AOS.

Depending on your network access method, the connection address is as below.

Wired network connection	**http://192.168.30.1**
Wireless network connection (Wi-Fi)	**http://10.42.0.1**

<Supported web browsers>
Microsoft Edge, Google Chrome, Mac Safari
We recommend using the Microsoft Edge web browser.

As shown in the example below, if you type http://192.168.30.1 (wired network connection) or http://10.42.0.1(wireless network connection) into your web browser's address bar and go to the page.

2.2 Login

This product prevents unauthorized access through the login process via ID and Password.
As shown above, once your PC and SNAPCHECK MOAI-O are connected to the network, you will see the login page to access AOS. You can log in to AOS by entering your admin username and password and pressing the login button. To exit, press the 'X' mark in the top right corner.

The maximum number of concurrent connections to the same AOS (same SNAPCHECK MOAI-O) is 5, the factory default username and password are as follows Administrator usernames and passwords are case sensitive.

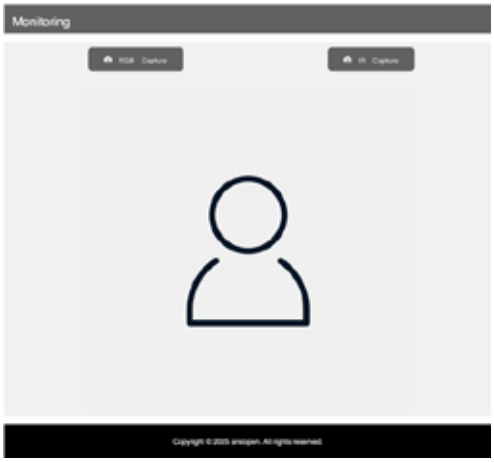
Administrator ID	admin
Administrator Password	admin

Caution
We also strongly recommend that you create a new administrator username and password after the initial login and delete the default administrator username "admin". This process is described in "User > Admin".
Please make your changed password not be leaked or lost.
If you forget your password, you will not be able to access AOS again.

After successfully changing the password, the 'Monitoring' page will be displayed as the default page of AOS as shown below. From then on, when logging into AOS, this monitoring page will always be the default page.

2.3 Monitoring

The Monitoring feature is for observing the status of SNAPCHECK MOAI-O's camera for face recognition and the results of face authentication in real-time. If no authentication attempts have been made since opening the monitoring page, this screen displays nothing.



■ Monitoring Page

When a user attempts to authenticate, the user authentication result is displayed in real-time in a rectangular window at the top center, as shown in the figure above. Along with the image of the user's face taken at the time of the authentication attempt, the user's name is displayed for successful authentication and 'Unknown' for unsuccessful authentication. If you want to clear results on the screen, please refresh your browser.

The bottom row displays the results of each authentication in chronological order.
Successful authentication is indicated by a blue-colored row and failed authentication is indicated by a red-colored row.

From the left of each row, the information displayed is as follows.

o Facial image stored inside the SNAPPIN used during authentication attempt.

o Authentication time: Year-Month-Day Hours, minutes, seconds in order.

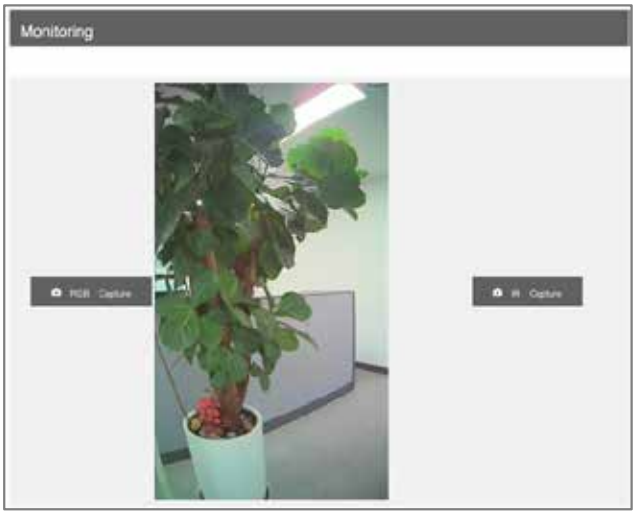
o The user's name stored in the SNAPPIN on successful authentication and 'unknown' on failed authentication.

o Time &Attendance: When the user authenticates by pressing the corresponding T&A button in SNAPCHECK MOAI-O, the corresponding T&A information of 'attendance', 'off work', 'outside work', and 'return' is displayed after 'Function'. If the user authenticates without pressing the T&A button, it is displayed as ' – '.

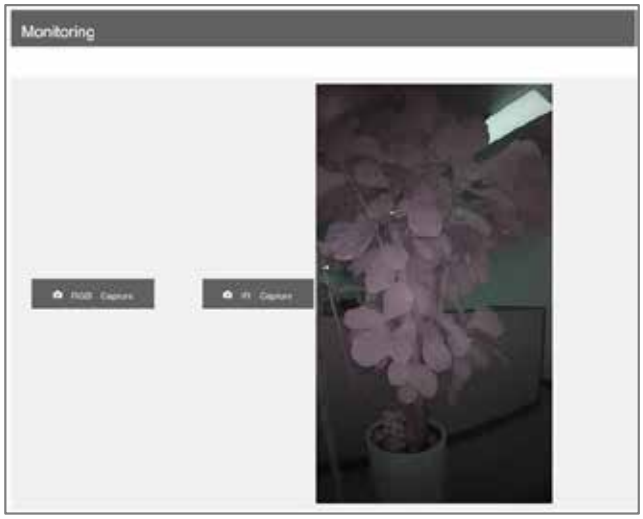
o 'Registered' will be shown at the end of each row when you succeed in authentication by the TEMPICS feature.

* About TEMPICS, please refer to 'Setup > Authentication > TEMPICS'

■ Monitoring > [RGB Camera]:
You can check if the camera is working normally by displaying a single still image of the real-time video from the upper RGB camera.

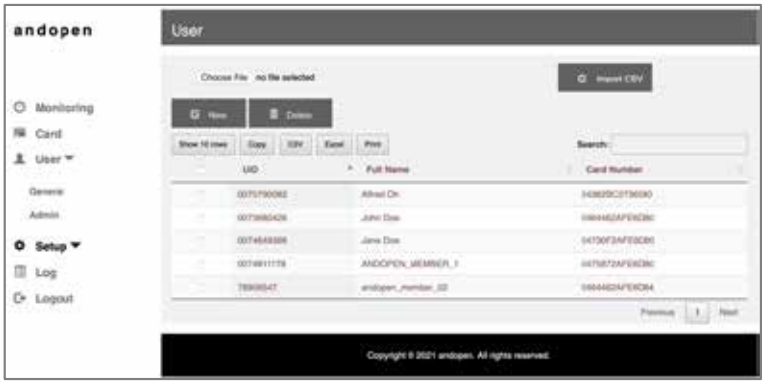


■ Monitoring > [IR Camera]:
You can check if the camera is working normally by displaying a single still image of the real-time video from the lower IR camera.



2.4 User

The User tab is for managing administrators who have access to AOS and regular users who use facial recognition with SNAPCHECK MOAI-O.
You can navigate to the submenu (General, Admin) tab by pressing the triangle on the right side of the User tab.

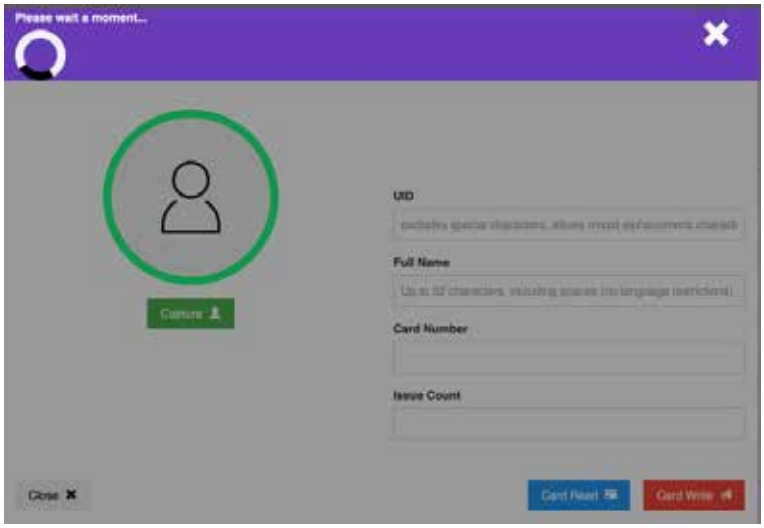


2.4.1 User > General > [Card Issuance]

The Card Issuance button is a feature that allows you to issue biometric cards using SNAPCHECK MOAI-O. You can use the blank SNAPPIN (Andopen Biometric Card Credential) provided by ANDOPEN to record the card user information and the user's face into the card. Cards other than those provided by ANDOPEN do not work with SNAPCHECK MOAI-O.

If you want to issue a large number of cards or write other than information written by this feature into the cards, we recommend using the Card Issuance System (A.CIS) of ANDOPEN. Please contact your product provider or ANDOPEN.

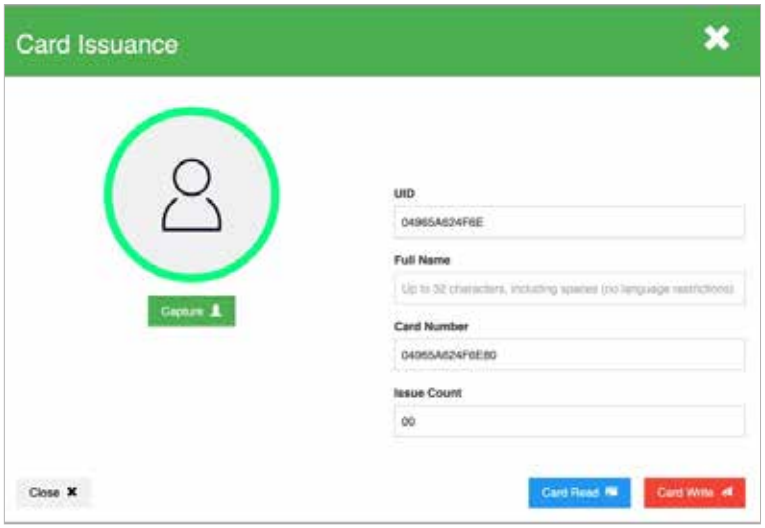
When click [Card Issuance] button, you can see the pop-up windows as below.
The pop-up window will wait for you to tag the card. To do so, tag a new SNAPPIN in the card tagging area of SNAPCHECK MOAI-O.



SNAPCHECK MOAI-O reads information of SNAPPIN and fills the blank UID and Card Number as shown in the figure below. By default, the UID is SANPPIN's unique Card Number. However, we recommend changing it to something unique and recognizable, such as an employee ID or serial number.

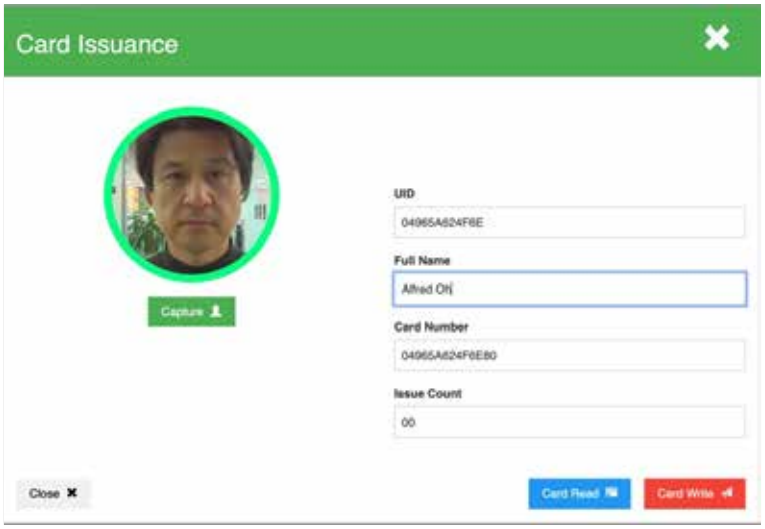
This is because the value of the UID is useful for identifying the user in future authentication results monitoring, logs, etc.

And fill the Full Name field with the user's real name or nickname. This field allows duplicates another users' name.
The card number is SNAPPIN's unique ID and is not allowed to be changed by the user.
The Issue count will be increased whenever the same SNAPPIN is reissued. (default is '00')



■ [Card Issuance] > [Capture]:

Take a picture of the face to be recorded into the SNAPPIN. Face the camera of SNAPCHECK MOAI-O and press the [Capture] button to take a picture of the cardholder's face and confirm it.
If you are not satisfied with the quality of the captured face, you can press [Capture] again and repeat until a good face image is obtained.



- Ask users to remove head coverings or sunglasses that cover part of the face and register their front face
- Avoid facial images with veiled eyebrows or unclear facial contours
- Avoid facial images that are out of focus and blurry, facial images that are too light or dark to distinguish features
- Avoid facial images with uneven exposure.

■ **[Card Issuance] > [Card Write]:**
Record the captured face image and basic information on the biometric card. With the card to be issued tagged to the card recognition area of SNAPCHECK MOAI-O, press the [Card Write] button. When the issuance is completed, you will see the success pop-up and hear a voice prompt saying 'It has been issued'.

***Note*.**
Keep the SNPPIN on the tag area until you hear the guidance voice. Removal while processing can cause an encoding error, and the card may become unusable forever.

When issuing a SNAPPIN by using SNAPCHECK MOAI-O, if you do not fill each field with a custom value, information is automatically generated and recorded on the card using the CSN of SANPPIN as the base information for convenience. The user information that is automatically recorded is as follows.

- UID: CSN (HEX)
- Name: CSN (HEX)
- Card number: CSN (HEX)
- Captured face images

When a card is issued, it is automatically saved to SNAPCHECK MOAI-O's user list using the information above. You can change the name of the user list. User lists and CSNs are described in "2.4.2 General Users"

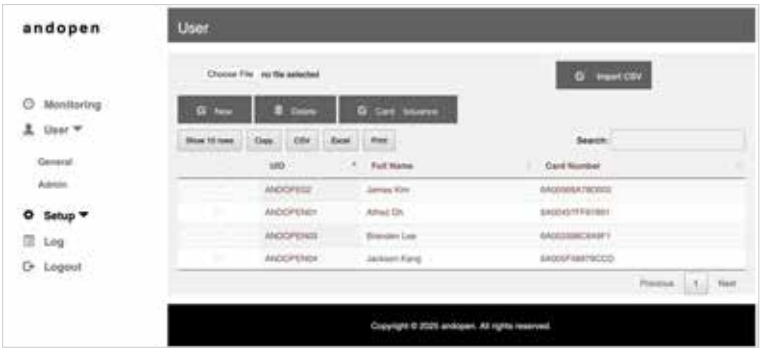
Note
If 60 seconds are passed without any operation, this 'card issuance' window will be closed automatically.

***Caution**
After completing all the issuance, make sure to press [Close X] or [X] to switch SNAPCHECK MOAI-O back to authentication mode.

2.4.2 General Users

You can register or export unique information (UID, name, card number) individually or in batches except for biometric information for general users using face authentication (biometric information, i.e., the user's face image, is only stored on the SNAPPIN). You can also view registered users.

When you open the Users > General Users page, you will see a list of registered users, as shown in the example below. Initially, no information exists.



■ **User > General > [New]:**
Register the face authentication user to the database of AOS through the pop-up page. You can register by pressing the [New] button and typing the user's information (UID, name, card number) in each blank of the pop-up page shown in the figure below. Or, you can tag the user's biometric card to SNAPCHECK MOAI-O while this pop-up page appears to automatically and easily enter the information which is stored in the user's biometric card.
The UID, name, and card number registered are encrypted and stored.

For reference, the rules for user information stored within a SNAPPIN are as follows

o UID: excludes special characters, allows mixed alphanumeric characters (up to 12 characters)

o Name: Up to 32 characters, including spaces (no language restrictions)

o Card number: CSN (hexadecimal, max=FFFFFFFFFFFFF)

* **CSN:** Chip Serial Number, a unique value assigned to the card's semiconductor chip at the factory when the card is manufactured. You must have this number known in advance when typing this information.

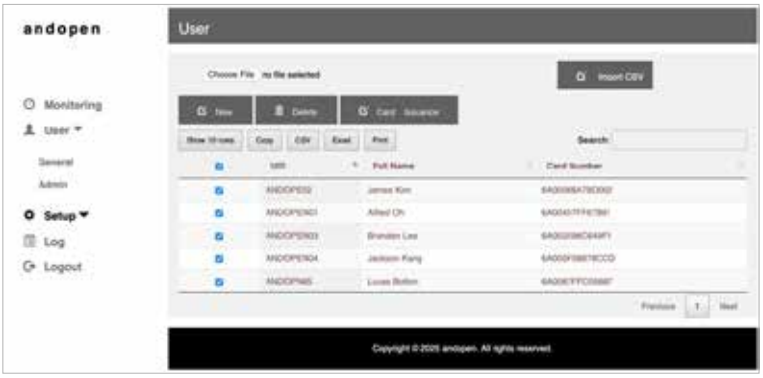
You can find this information on each card using a separate card reader or an NFC-enabled smartphone app.

Once the user information is entered, click the [Save] button to complete the registration. If you do not want to register with the entered information, click [Cancel]. To close the Add User pop-up window, click the 'X' in the upper right corner.

***Caution*.**
When entering user information by typing it in, make sure it is correct and does not differ from the information stored on the user's actual biometric card. In particular, if the card number entered is different from the actual biometric card, authentication will not succeed, even for the correct user. Check with your access security administrator for accurate information on access policies, system configuration, and biometric card information.

■ **Edit existing registered user information**
If you want to edit the information of an already registered user, you can do so by "double-clicking" on one of the user's UID, name, or card number in the user list and change the desired information in the pop-up window that appears. However, you will need to delete the user, reissue a biometric card, and register anew since you can't change the UID which is used as an index code in the database and card number.

■ User > General > [Delete]:
Delete a registered face authentication user.
Click the checkbox to the left of the row of users you want to delete from the list. The selected records (users) will be marked with a blue check. At this point, you can press [Delete] to delete the selected users.
If you want to do a bulk delete, click the checkbox to the left of the top row's 'UID' to select all the records that appear on the page, and then click the [Delete] button to delete them in bulk.
(The deletion process is applied immediately, so please use it with caution).



■ User > General > [Choose File]:
When you want to register users in bulk using a user data file created in CSV file format, use this to select the file. Click the [Select file] button to select the desired data file from the 'Select file to upload' window that appears.
(Please refer to https://www.andopen.co.kr and download the example file for the correct CSV file convention. It must be properly formatted in the format of the example file using an appropriate document writer and saved in UTF- 8).

***Note*.**
We only support .CSV file format for bulk registration. However, when exporting a list of registered users to a file, both CSV and Excel files are supported.

■ User > General > [Import CSV]:
Register users in batch with the contents of the user data file (CSV format file above) selected through [File selection].
The user information that is registered using this feature is the UID, name, and card number, excluding the user's face image.

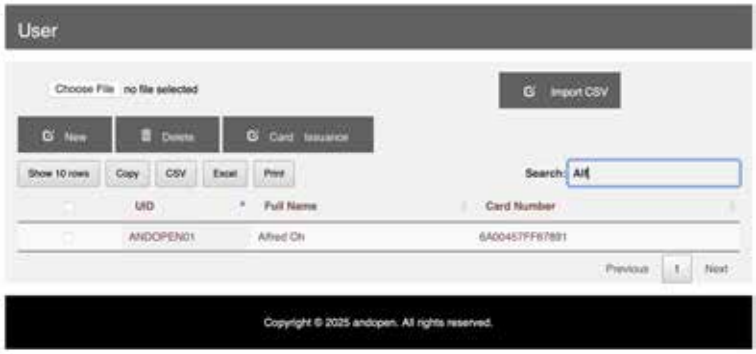
■ Users > General > [CSV]:
Export the entire list of registered users in CSV file format. The exported file will be saved to the automatic download folder assigned by the OS of the PC connecting to AOS. During the export process, please select 'Allow' when asked to 'Allow to downloads?'.
Generated file name: AOS.csv

■ User > General > [Excel]:
Export the entire list of registered users in Excel file format. The exported file will be saved to the automatic download folder assigned by the OS of the PC connecting to AOS.
During the export process, please answer 'Allow' to "Allow to download?"
Generated file name: AOS.xlsx

■ User > General > [Print]:
Print the entire list of registered users to the printer installed on the PC connected to AOS. After that, follow the steps for using the printer.

■ User > General > [Copy]:
Temporarily save the entire list of registered users to the clipboard on the PC connected to AOS. You can paste the user list saved in the clipboard into a document created with a separate document tool program such as 'Notepad', 'Word', etc.

■ User > General User > Search:
Use to look up a specific record in the list of registered users. Enter a part of a UID, name, or card number in the field to the right of 'Search' and it will find and display records containing it in real-time as you type.



■ User > General > [Show 10 rows]:
Set the number of records displayed on one screen. You can set the number of user records (number of rows) displayed at a time by pressing the [Display one screen] button: 10, 25, 50, 100.
The default value is 10.

■ User > General > [1], [2], ...:
The page number containing the currently visible record. You can switch pages by pressing different numbers: 'Previous' and 'Next' to switch to a group of adjacent pages.

2.4.3 Admin

This tab is used to register or delete administrator accounts that have access to AOS.
When you select the 'User > Admin' tab, the Administrator login window appears as shown below.
Enter the password for the currently logged-in administrator account and press [OK] to proceed. To abort, click [Cancel] or the 'X' in the upper right corner of the pop-up window to close the pop-up window.

***Caution ***

o The first time you connect, the factory default is the administrator ID/password, i.e., admin/admin, so enter "admin" for both. For the security of your device, be sure to set your own administrator username and password during the first connection through the "Add Administrator" function described below.

o Be sure to delete the admin account that is registered as factory default.

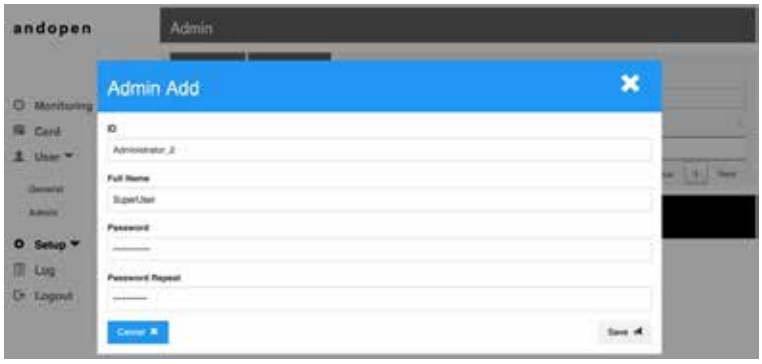
o Do not disclose your registered administrator ID and password to anyone other than those with administrative privileges.

o Administrator account information is not automatically backed up to the device. Please keep a record of your administrator account information in a safe place to prevent loss or leakage. If any damage occurs due to the leakage of the administrator account, ANDOPEN will not be held liable. If you lose your administrator account ID or password so that you cannot access the device, you can return the device to ANDOPEN for a factory reset. This may impose a fee.

o All registered admin accounts have equal permission levels. Therefore, an administrator can create/delete/modify other admin accounts. Please be careful when managing admin accounts.

■ User > Admin > [New]:

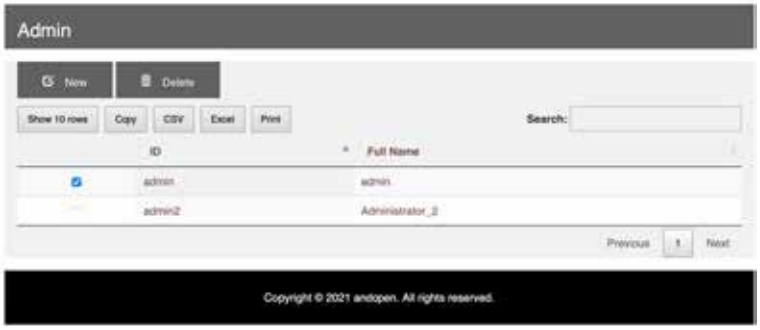
Add an administrator. In the pop-up window that appears after pressing the [New] button, enter a new administrator ID, name, and password, then enter the password again and click [Save] to register. The registered administrator password is encrypted and stored. To quit, click [Cancel] or the 'X' in the upper right corner of the pop-up window to close the window. (Admin usernames and names can be up to 12 characters long, excluding special characters, and contain only alphanumeric characters. Passwords must be 8 to 16 characters long and contain all numbers, uppercase, lowercase, and special characters.)



The maximum number of administrators that can be registered and the maximum number of simultaneous connections is 5.

■ User > Admin > [Delete]:

Delete an administrator account. In the list of registered administrators, click the checkbox to the left of the administrator account you want to delete. The selected account will be marked with a blue check. In this state, you can click [Delete] to delete the selected account.
On the Admin page, at least one admin account must exist; therefore, batched deletion is not available.
(The deletion process takes effect immediately, so please use it with caution).



■ Edit a registered administrator

You can edit the name and password of an already registered admin. You can change the password in the pop-up window that appears by double-clicking the administrator ID or name of the administrator you want to edit. The administrator ID cannot be changed, and if you need to change it, please delete it and make anew

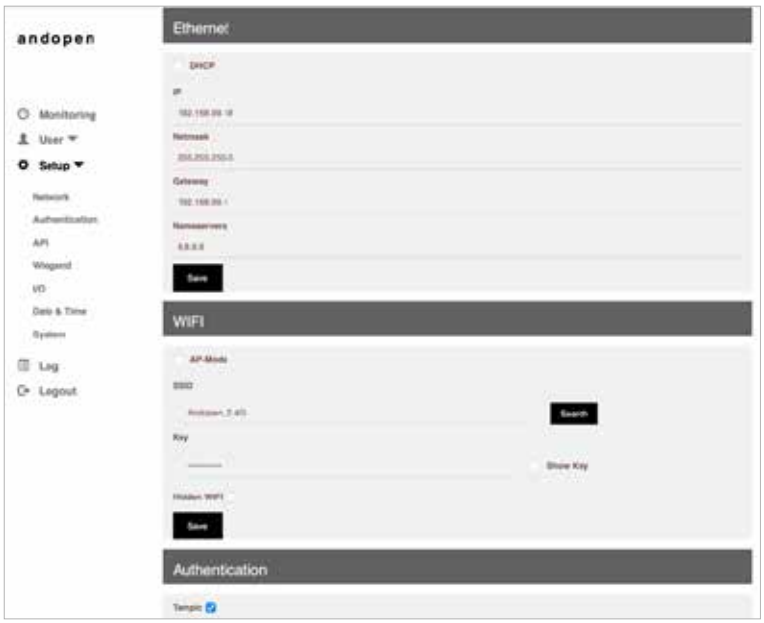
■ User > Admin > [Show One Screen], [Copy], [Export to CSV], [Export to Excel], [Print], Search:

Only the accounts handled by general users and administrators are different, it works the same as each button in "User > General".

2.5 Setup

AOS provides the ability to set the overall initial operation and condition setting for SNAPCHECK MOAI-O. The Settings tab consists of a single page. You can scroll through the web browser to jump to individual settings functions, or you can jump to individual settings functions by pressing the triangle next to the Settings tab and selecting a submenu.

2.5.1 Network



Perform the network settings for SNAPCHECK MOAI-O. SNAPCHECK MOAI-O supports both wired networks and wireless Wi-Fi networks. Due to the nature of the security device, it is recommended to use a safe wired network, and it is not recommended to connect wired and wireless networks at the same time for stable network communication.

If you don't have enough information or familiarity with your network to make this setup, contact your organization's network administrator or expert for help.

Setting up a wired network

You can specify the values of IP address, Netmask, Gateway, and Nameservers for using SNAPCHECK MOAI-O as a static IP environment by entering them directly. If you want to operate in a DHCP environment, click the checkbox on the left of 'DHCP' to enable it.

When DHCP is enabled, the previously registered static IP settings will not disappear, but will be ignored, and will work as a DHCP environment. To apply the changes, click [Save]. The IP address of SNAPCHECK MOAI-O will be changed immediately.

*** Caution ***

o When the network changes are applied, so to reconnect, you need to change again the network settings on the PC appropriately so that SNAPCHECK MOAI-O and the PC are on the same network. Of course, to connect AOS again, you need to type the changed IP address in the address tab of the browser.

o Write down the IP address of each SNAPCHECK MOAI-O so that you do not forget the static IP address you changed. If you forget the IP address, you may be supposed to be unable to connect to AOS again over the network. Therefore, we recommend keeping wireless network status on AP-Mode when you use SNAPCHECK MOAI-O in wired network configuration. Then, even if you forget the IP address of SNAPCHECK MOAI-O, you can access AOS via wireless network.

Set up a wireless network

Set up the wireless network environment for SNAPCHECK MOAI-O. Initially, SNAPCHECK MOAI-O is set to AP-Mode.

When AP-Mode is enabled, SNAPCHECK MOAI-O operates as a Wi-Fi Access Point. Therefore, SNAPCHECK MOAI-O cannot be connected to other wireless APs in this state.
This mode is for connecting to the administrator's terminal (PC, laptop) for the management of SNAPCHECK MOAI-O. It is recommended to keep AP-Mode when using a wired network.

Disabling AP Mode will allow you to set up to connect SNAPCHECK MOAI-O to another wireless AP. Click [Search] to discover and select the AP you want to connect to.
When you want to connect to Hidden WIFI, type the SSID of Hidden AP, which you already know, and make sure to click the check box beside 'Hidden WIFI'.
Be sure to enter the correct passphrase required by the AP you want to connect to.
(check at 'Show Key' to display the password that you have typed.)
Press [Save] to apply the changes.

***Note*.**
The wireless connection does not support static IP settings. The AP which you want to connect to must provide DHCP service.

2.5.2 Authentication

Set the authentication conditions and facial recognition action conditions for SNAPCHECK MOAI-O.

■ Setup > Authentication > TEMPICS:

The TEMPICS feature is ANDOPEN's patented technology designed for convenience. TEMPICS ("Temporary Pictures") enables users to authenticate their face with a biometric card initially and then access without SNAPPIN for a set period of time.

Enable TEMPICS and use the slide below to set the period in hours for TEMPICS to work. Setting it to '0' means that TEMPICS will work forever.

Click [Save] to apply the changes.

To understand this feature, please refer to the TEMPICS operation and usage below.

How it works

① With TEMPICS enabled, when a user presses the ‘Attendance’ button and successfully authenticates with a biometric card, the user's face and time information taken at the time of authentication are temporarily stored in SNAPCHECK MOAI-O's volatile memory.

② After that, when the user is close to SNAPCHECK MOAI-O, the face authentication result is derived by comparing the face information temporarily stored in SNAPCHECK MOAI-O without the need for tagging SNAPPIN.

③ TEMPICS will automatically delete the user's face from the device after the set TEMPICS action time has passed, or when the ‘Off Work’ button is pressed and authentication is successful.

④ When SNAPCHECK MOAI-O is restarted or power is cut off, the volatile memory is initialized and all temporarily stored face images are deleted. The face information stored in volatile memory is safe from hacking, and even if SNAPCHECK MOAI-O is hijacked, it will be volatilized because power is cut off.

*** Note ***
In order not to break access security policy, the face information temporarily stored for TEMPICS function is only stored on the SNAPCHECK MOAI-O device that presses the 'Attendance' button and successfully authenticates. Therefore, the TEMPICS function only works on the first SNAPCHECK MOAI-O device that has been 'Attendance' and does not automatically synchronize with all SNAPCHECK MOAI-Os in the building. In order to synchronize to all SNAPCHECK MOAI-Os installed in the building, ANDOPEN's access control system, ADMS (ANDOPEN Device Managing System), must be installed, and the ADMS and the building's SNAPCHECK MOAI-O terminals must be connected through the TCP/IP network.

■ Setup > Authentication > Rule:
Select Bypass mode (user DB bypass mode) and Local Authentication mode (user DB authentication mode) as authentication conditions.

o Bypass: This method compares the face embedded in the biometric card with the face of the authentication requestor taken by SNAPCHECK MOAI-O and judges the authentication as successful if they match.
This method is recommended when SNAPCHECK MOAI-O is operated in conjunction with an external access control panel.

o Local Authentication: This is an authentication condition that mixes bypass mode and card authentication. If the face stored in the biometric card and the face of the authentication requestor photographed by SNAPCHECK MOAI-O are matched, and if the card number of the used biometric card matches a card number in the user DB stored in SNAPCHECK MOAI-O, then the authentication is judged as successful.

This method is recommended if you operate a method that allows SNAPCHECK MOAI-O to control the opening and closing of the door directly.

If you have difficulty setting up an authorization rule, please contact a physical security expert or visit our website www.andopen.co.kr or www.youtube.com/andopen to help you understand.
The factory default is Bypass.
Please press [Save] to apply the changes.

■ Setup > Authentication > Detect Threshold:
Set the threshold for judging a subject as a human face.

Setting value range: Minimum value 0, Maximum value 1
The factory default value is 0.3.

If the value is too low, there may be cases where subjects that are not faces are judged as faces, and face authentication proceeds. And if the value is close to 1, there may be cases where actual faces are not judged as faces, and face authentication does not proceed. We recommend that you keep the factory default value as much as possible, and use it by fine-tuning it according to the field situation.

■ Setup> Authentication > Matching Threshold:
Set the threshold for face authentication success/failure, which is equivalent to setting the 'similarity' for authentication success. If the face image in the biometric card and the face of the user trying to authenticate are compared and a similarity below this threshold is obtained, the authentication is not judged as identical and the authentication fails.

In the case of TEMPICS feature enabled, if there are multiple temporarily stored facial information with values above this setting, the face that returns the highest similarity is evaluated as the same face, and if all of them return values below this setting, authentication fails.

Setting value range: min 0, max 1

Higher values require higher similarity to pass authentication.
Higher values decrease the false recognition rate, but increase the false rejection rate. Conversely, lower values decrease the false rejection rate but increase the false recognition rate.
We recommend using values between 0.6 and 0.9. The factory default value is 0.6.

* Note *
・False acceptance rate - the rate at which an unauthorized user is recognized as an authorized user.
・False rejection rate - the rate at which an authorized user is recognized as an unauthorized user.

Press [Save] to apply your changes.

*Caution *
Authentication results are very sensitive to small changes in the Matching Threshold value. If you do not have sufficient expertise in facial recognition, we recommend that you use the factory default values, and if you make any adjustments, use a fine-tuning approach.

■ Setup> Authentication > Matching Timeout:
Set the number of seconds to retry facial recognition.

This is the longest amount of time to attempt facial recognition for SNAPCHECK MOAI-O to produce an authentication result.
If authentication is not successful within the set time (in seconds) from the time facial recognition is attempted (when the user's approach is detected and the user's face is detected), authentication is treated as failed and returns to the ready state. If the user is still in the detection range and their face has been detected, face recognition is attempted again and repeated.

Setting maximum: 60 seconds
The factory default value is 2.0 (seconds).

Press [Save] to apply the changes.

■ Setup > Authentication > Liveness Check:
Determine whether to enable the ability to detect fraudulent authentication attempts.

This feature prevents fraudulent face authentication attempts, such as the case that someone steals an authorized user's SNAPPIN, photographs the user's face, and shows it to SNAPCHECK MOAI-O by using smartphones, tablets, or prints.

You can activate or deactivate by click check box. When you activate Liveness check feature, the time required for face recognition is slightly longer than when it is disabled.

The factory default is unchecked.

Click [Save] to apply the changes

2.5.3 Wiegand

If SNAPCHECK MOAI-O interfaces with an external access control panel via Wiegand communication, adjust the Wiegand communication format.

■ Setup > Wiegand > Pulse Time:
physical signal of Wiegand communication.

These values will vary depending on the operational characteristics of the access control panel you're integrating with. Check with your device's manufacturer for recommended values, and input them down accordingly. The factory default values are recommended by many access controllers and are shown below.

Pulse Width: 1~100,000 (unit: microseconds, default: 40)
Pulse Interval: 1~100,000 (unit: microseconds, default: 2,000)

Press [Save] to apply your changes

■ Setup > Wiegand > Card Format:
Determines the card number manipulation method being transmitted by Wiegand communication.

- **34bit:** Adjusts the total length of card number data to 34 bits.
- **24bit:** Adjusts the total length of card number data to 24 bits.
- **Reverse Bits:** If checked, transmits each bit of the card number data in the reverse order.
- **Parity Bits:** If checked, the card data will be transmitted with an Even Parity bit in front of leading bit and Odd Parity bit after trailing bit.

The appropriate card format depends on the access control panel model and your organization's choice. Please consult with your organization's security administrator or expert for accurate settings.

Press [Save] to apply your changes

■ Setup > Wiegand > Wiegand Out:

Determines whether the user's card number data should be sent out over Wiegand communication when authentication is successful.

o If checked, it will be sent out, but if the authentication fails, it will not be sent out, even if checked.
o If unchecked, it will not send outward even if authentication is successful.

The factory default is unchecked.

Press [Save] to apply the changes

2.5.4 I/O

Provides functions for setting interlocking conditions and unlocking doors with external devices (lock devices, fire detection devices, exit buttons, door status detectors, etc.) connected through the I/O port of SNAPCHECK MOAI-O.

■ Setup > I/O > Door Control:

In the configuration that SNAPCHECK MOAI-O directly controls the door's lock, this determines the condition for controlling the lock devices when SNAPCHECK MOAI-O is invalidated by power fail, failure, or vandalism.

o General: The relay on SNAPCHECK MOAI-O will hold the initial COM-NC position and move to COM-NO upon successful authentication. Use this setting when the installer can select the type of lock based on this operational condition.

o Fail-Safe: Select this setting when you want the door to open in the event of a power outage. The lock must be a fail-safe type (Dead bolt, Electro Magnetic), or the lock must be in fail-safe mode by adjusting the physical latch of the lock (Striker, Mortise).

The wiring depends on the following two cases

1. When want to use the power supply control method to manipulate the lock device:
   Connect each end of the open circuit for supplying power to the lock device with the COM-NC of the SNAPCHECK MOAI-O Relay.

2. When the lock device has a separate dry contact for opening door and you want to control the lock using it: Connect the door-open contact with the COM-NO of the SNAPCHECK MOAI-O Relay.

o Fail-Secure: Select this setting when you want to keep the door closed in the event of a power outage. The lock must be a fail-secure type (Dead bolt), or the lock must be in fail-secure mode by adjusting the physical latch of the lock (Striker, Mortise).

The wiring depends on the following two cases

1. When you want to use the power supply control method to manipulate the lock device: Connect each end of the open circuit for supplying power to the lock device with the COM-NO of the SNAPCHECK MOAI-O Relay.

2. When the lock device has a separate dry contact for opening the door and you want to control the lock using it: Connect the door-open contact with the COM-NC of the SNAPCHECK MOAI-O Relay.

The factory default is Fail Secure

*** Note ***

Relay works, please refer to "Glossary > Relay" later in the manual. Select the appropriate option according to your door opening policy and the type and function of the lock you are interfacing with. If you have difficulty with this setting, please provide this manual to your access control installer for assistance.

Click [Save] to apply the changes.

*** Caution ***

Your door control policy should conform to the fire code and legal standards in your region.

■ Setup > I/O > Fire Alarm Input:

This feature is set when a fire signal generator is connected to SNAPCHECK MOAI-O via dry-contact. When SNAPCHECK MOAI-O receives a fire input, it flashes the front LED and sounds an alarm, stops all authentication, and attempts to open the door. If SNAPCHECK MOAI-O is controlling the door, it will open and hold the door open. If the door is controlled by an access control panel, a fire signal generator has to be connected with access control panel.

o uncheck: Do not receive fire signals.
o check: Use this setting when connecting to a fire signal generator that sends fire signals as unpowered contact signals. This is typically used when connecting with fire alarm control panels.

The factory default is unchecked.

Press [Save] to apply the changes.

*** Caution ***

The establishment of access policies in the event of a fire is strictly regulated by your local fire code. You should consult with a fire and access control system expert to configure and set up your system to comply with local fire codes.

■ Setup > I/O > Relay:

Determine whether to enable the relay operation of SNAPCHECK MOAI-O that controls the door.

If checked, the relay will be activated upon successful authentication under the conditions determined by the "Setup > I/O > Door Control" setting.
If unchecked, the relay is disabled and does not work.

If SNAPCHECK MOAI-O does not control the door directly (an external access control panel controls the door), please uncheck to disable the Relay operation to reduce the unnecessary operation of the Relay.

The factory default is checked.

Press [Save] to apply the changes

Note

For more information about Relay, see "Glossary > Relay" later in the documentation.

■ Setup > I/O > Relay > Signal Width(ms):
Specifies the amount of time that the relay operates while it is active. When the relay is activated by checking box, a field appears where you can specify the Signal Width value.

In a configuration where SNAPCHECK MOAI-O directly controls the door, this typically means 'the time the relay is operational is the time to unlock the door'. After successful authentication, the door will remain open for the time you set. If an access control panel controls the door, the open time of the door is determined by the open time setting of the access control panel, and this setting is ignored. In addition, the lock device may also have an unlocking time adjustment, so please adjust the setting value in consideration of the interworking.

The default value is 3,000 ms (milliseconds)

Press [Save] to apply your changes

■ Setup > I/O > Exit Button:
Determines whether to enable receiving an open signal from the Exit Button device in an environment where SNAPCHECK MOAI-O controls the door directly.

In environments where an exit button is not required (e.g., when a striker lock is installed or an automatic door sensor is present, etc.), or if you want to prevent malicious opening attempts, you can use this setting to negate the open signal which is coming into the exit button I/O of SNAPCHECK MOAI-O.
o **Receive a signa**l if there is a **check** (Exit Button works)
o If there is no check, **ignore the signal.**

The factory default is checked.

Press [Save] to apply your changes

■ Setup > I/O > Remote Open:
Temporarily open the door through the AOS.

When the [Open] button is pressed, the Relay in SNAPCHECK MOAI-O will operate one time with the conditions determined by the "Settings > I/O > Door Control" setting.

Can be used to open a door on a one-time basis without authentication in environments where administrators have access to AOS (e.g., to allow visitors to enter in the event of a vacancy).

2.5.5 Date & Time

SNAPCHECK MOAI-O adjusts the time of the built-in clock, which is the basis for all actions and data generation times that require user authentication result logs and time information.

■ Settings > Date & Time > Automatic Date & Time:

If SNAPCHECK MOAI-O is connected to the Internet, click the checkbox to enable this feature to automatically update the time of clock built-in SNAPCHECK MOAI-O to internet time (UTC) on a regular basis.

If you uncheck the box, the built-in clock will be set manually and you can set it by entering the time manually.

Click “Settings > Date & Time > Date & Time” and follow the pop-up calendar to set the year, month, date and type designated hour, minute and AM/PM

Alternatively, for convenient time setting, you can easily set the built-in clock in SNAPCHECK MOAI-O to the current time by getting the browser time of the PC connected to AOS. (Check the 'Browser Time' checkbox and click [Save])

The factory default is checked.

Press [Save] to apply the changes

* Note*

If you set the clock on SNAPCHECK MOAI-O manually, the time may become slightly inaccurate over time. Therefore, we recommend that you enable automatic time renewal to automatically correct the time information if an internet connection is available. Otherwise, we recommend that you periodically reset the time manually using the methods described.

■ Settings > Date & Time > Time Zone:

When Automatic time update is enabled (checked), the time fetched from the internet is UTC+0, i.e. Greenwich Observatory time. Therefore, you need to apply your local time difference to this time to convert it to your local time. That is, if you want to apply local time correctly to SNAPCHECK MOAI-O, you must select right Time Zone of your location.

Click the [Search] button to select the region where SNAPCHECK MOAI-O is used. The correct current time is set by applying the local time difference to the UTC time, which is the reference time of the built-in clock.

The factory default value is ASIA/Seoul.

Click [Save] to apply the changes

2.5.6 System

This tab is primarily for setting operational elements where changes are common to all operations in SNAPCHECK MOAI-O. You can perform software updates, adjust the volume of the voice prompts, and select the language of the voice

■ Setup > System > Software Update
You can update AOS using ANDOPEN's update cloud or from a file. If AOS is connected to the internet, you can click [Online Update] to update AOS version to the latest version.

This process requires an automatic reboot of SNAPCHECK MOAI-O regardless of whether AOS is updated to a higher version, so do not click the [Online Update] in situations where rebooting is restricted.

If you have a specific version of the update file that is downloaded from the ANDOPEN website, you can select its location and update AOS to the designated version by clicking [Offline Update].

The update does not make changes to the previous setup.

***Caution*.**
Do not operate or power off SNAPCHECK MOAI-O while updating the software. The software may become corrupted, and SNAPCHECK MOAI-O may malfunction. You may not be able to access SNAPCHECK MOAI-O again, or SNAPCHECK MOAI-O may not work permanently.

■ Setup > System > Volume:
Adjust the volume of prompts and action sounds (authentication success/failure, alarms, etc.). You can adjust the volume using the slide bar under "Volume".
Press [Save] to test and apply your changes.

■ Setup > System > Voice:
Set the language of the guidance voice.
Choose the desired language of the greeting voice from the pull-down menu that appears.
Currently, AOS supports two languages: Korean and English.

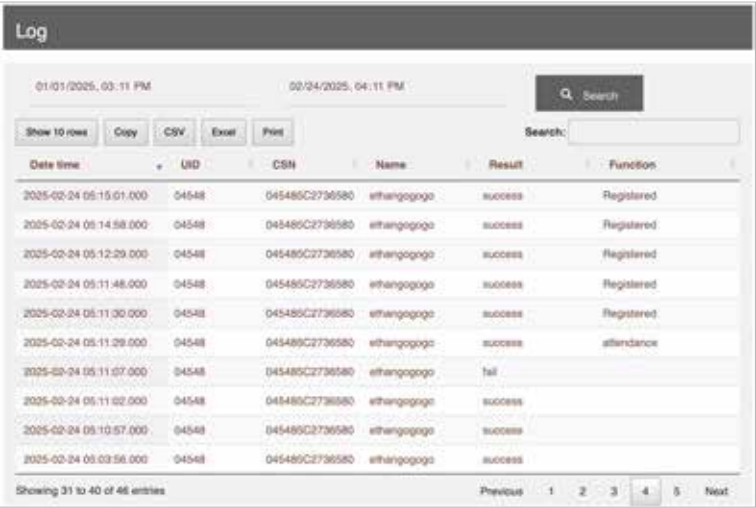
The factory default is English.

Press [Save] to apply your changes

■ Setup > System > Reboot:
You can reboot SNAPCHECK MOAI-O immediately

2.6 Logs

The Logs menu is a page where you can view records that allow you to track and observe user authentication results (up to one million)



This page allows you to view and report on the user's authentication logs.
You can set the desired lookup period by clicking the date and time fields.
Once the lookup period is set, you can click the [Search] button to view user authentication results.

The information displayed as a result of the lookup is shown below.

o Authentication time
o UID: The unique number stored on the biometric card that attempted to authenticate.
o CSN: The card number of the SNAPPIN that attempted to authenticate.
o Name: The username stored on the SNAPPIN that attempted to authenticate.
o Result: Above the value, you set in "Setup > Authentication > Matching Threshold",
facial authentication score will be marked as successful, and below will be marked as failed.
o Function: If the user pressed the T&A buttons and was authenticated, the corresponding time
and attendance information is displayed. If the user did not press those buttons and was authenticated,
it will be displayed as '-', and 'Registered' upon authentication by TEMPICS.

The buttons and user interface of [Show currency], [Copy], [Export to CSV], [Export to Excel], [Print], [1...2], Search, Previous, Next, etc. are the same as the corresponding functions described in "User > General".

2.7 Logout

Log out of AOS. Returns to the login page.

3. Technical support and quality assurance

ANDOPEN provides free and paid services in accordance with the Fair Trade Commission and Consumer Damage Compensation Standards. As the manufacturer of the product, ANDOPEN does not provide warranty services directly to customers, but through authorized dealers.
Please keep your purchase receipt with the contact information of the final supplier of the product and the date of purchase, and request service from the final supplier.

■ Free service

If a malfunction occurs while using the product, you can receive free service for one year from the date of purchase. However, if the malfunction is caused by customer negligence or natural disasters, it will be charged even within the free service period. Our principal maintenance policy is a 1:1 'refurbished' exchange.

■ Paid services

When applying for the service, the following cases will be charged even if it is within the free service period.

- If you can't determine when a purchase was made
- Consumable parts are at the end of their useful life
- Product failure and damage caused by dropping, impacting, or puncturing the product.
- Failure or damage to the product caused by failure to follow the instructions and cautions in the user manual.
- Product damage and breakage caused by the use of unauthorized products or supplies.
- Product failure and damage or degradation caused by the unauthorized installation of the product by anyone other than a surveyor.
- Product damage and breakage due to customer negligence
- Damage and breakage to the product due to unauthorized modification, disassembly, or repair.

■ Technical Support

For questions or technical support on any of our products, please contact our support team at cs@andopen.co.kr.

To ensure a smooth technical support experience, please have the information below ready.

- Company name, name, contact
- Your product's model name and serial number
- Error messages and symptoms

For more information and to provide feedback on the product, please visit the AndOpen website at www.andopen.co.kr.

4. Glossary

The following is a brief description of the standard for any technical terms or specifications used in this documentation.
For more information, please refer to the related resources or documentation. (Order: numeric, English alphabetical, Korean alphabetical)

■ **568B:** One of the specifications for the structure of the arrangement of each wire used when building Ethernet cables. Regarding this specification, please refer to the link below.
(https://en.wikipedia.org/wiki/ANSI/TIA-568)

■ **AWG22:** Abbreviation for American Wire Gauge, which refers to wire sizes in the United States, of which 22 is the largest. The standard is based on the diameter of the wire conductor, and the lower the number after AWG, the larger the diameter. For more information on this standard, please refer to the following link:
(https://en.wikipedia.org/wiki/American_wire_gauge)

■ **Cat5, Cat5e:** A type of wire for network communications that consists of four wires in a single sheath made of two wires twisted together. Cat5 is currently the most commonly used network wire, and Cat5e is an improved version of Cat5 with a stronger twist. You can check the specification when purchasing wire.

■ **CSV (comma-separated values):** Text data and text file with each field of data separated by a comma (,), with the extension .csv.

■ **Dry Contact:** When an electrical circuit is opened or closed by touching or disconnecting the contact surface through which current flows, it is called a dry contact, which means that no current/voltage signal is applied to this contact, i.e., both terminals are mechanically connected or opened. The opposite meaning is 'wet contact'.

■ **DHCP (Dynamic Host Configuration Protocol):** A service command system that automatically assigns an IP address and the address of a gateway or nameserver, so that when you connect to a particular network without network configuration, you are dynamically assigned an IP.

■ **Ethernet:** A technology that allows devices connected to a network to send and receive data to and from each other, standardized as IEEE 802.3. Ethernet cables, Ethernet ports, and Ethernet hubs all refer to the physical devices needed to use this technology.

■ **HEX:** Radix base 16, using 0 through 9 and A through F. Compared to decimal, 1 is 1, 10 is A, and F is 15.

■ **I/O:** Short for Input and Output. In this document, it refers to input signals coming in from external devices and output signals going out from SNAPCHECK MOAI-O to external devices. The format of I/O signals varies depending on their purpose.

■ **IR (or IR camera):** IR stands for Infra-Red, which means infrared light. Cameras that shoot using visible light are often called RGB cameras, while cameras that shoot using infrared light in the non-visible region for specific purposes are called IR cameras. To acquire images with an IR camera, a lighting device that irradiates infrared light is usually used. SNAPCHECK MOAI-O is also illuminated with infrared light.

■ **RJ45:** One of the Registered Jack standards used as a communications network interface, it has connectors and plugs to attach the eight strands of a typical Ethernet cable. Connectors are attached to the ends of Ethernet cables, and plugs are attached to network devices to interconnect them.

■ **Relay:** A Relay in this document is a component that has the purpose of controlling electrical signals, causing a physical switch to operate by applying/rejecting current to the component. In SNAPCHECK MOAI-O, the dry contact and wet contact signals are generated using this component. The basic working principle of a relay is shown in the figure below.

■ **Screw Anchor:** An inserted structure, usually made of plastic, metal, fiber, etc. for the purpose of improving the strength of attachment or fixation. For example, when attaching a wall-mounted product, if a screw anchor is inserted into the drilled hole after drilling and fixed with screws, nails, etc., the attachment strength can be significantly improved compared to fixing without inserting a screw anchor.

■ **STP:** STP stands for Shielded Twisted Pair, a method of construction in which a thin metal foil or metal mesh is inserted into the sheath of twisted pair wires to block electromagnetic noise from the outside and make the cable more durable. The opposite of STP is UTP (Unshielded Twisted Pair), and STP cables offer the benefit of longer transmission distances and more reliable data communication compared to UTP cables.

■ **Wiegand:** It is a communication method that transmits a large amount of data between devices through two wires, the voltage level applied to each wire to generate 1 and 0 binary data values. It is used by setting the pulse width and inter-pulse gab of the device to be the same. For more information, please refer to the link below. (https://en.wikipedia.org/wiki/Wiegand_interface)

■ **UTC time:** Often referred to as "Coordinated Universal Time". UTC is the same as GMT (Greenwich Mean Time), which is what you'll use to calculate your local time by applying the time difference for each region of the world.
For example, KST (Korean Standard Time) = UTC + 09:00, which is calculated

by adding 9 hours, 0 minutes, and 0 seconds to the UTC time. Typically, when you connect to the internet, your device receives UTC and adds the time difference for your region, referencing the region you specified when you initially set up your device, to calculate the final current time.

■ **Refurbish:** It refers to selecting parts that are not abnormal from refunded products or products returned for repair and reassembling (repairing) them to make them as good as new. ANDOPEN provides after-sales service that replaces abnormal products 1:1 with such reassembled products in the event of A/S.

■ **Access control panel:** A device that enables door control and entrant authentication according to the access policy set by the access control system (access control SW or server), and generally exists between the reader (recognition device) and the access control system.
The information transmitted from the reader is compared with the database stored in the access control panel to derive authentication results, and depending on the authentication results, it is decided whether to send an unlock signal to the unlock device installed at the door or not. The database is typically updated periodically or upon event occurrence via Ethernet with the access control system, and this process forwards the information from the reader to the access control system, allowing the access control panel to quickly derive the authentication result without waiting for the authentication result.

This device generally has I/O such as reader input, open button input, door status input, fire signal input, and open signal output.

As access control panels with various shapes and operation methods are being released, when using them in conjunction with SNAPCHECK MOAI-O, please seek professional help to ensure proper use.

■ **Ferrite Core:** A component made from a magnetic ceramic containing iron oxide. It is designed to wrap around cables, and by placing a ferrite core in the cable that connects to the outside of the device, you can block noise signals from entering the cable. High-frequency noise and low-frequency noise have different effects on the device, so it is important to use the correct ferrite core to be effective. The SNAPCHECK MOAI-O component includes a dedicated ferrite core.