# A.bc1

## Product Documentation

A.bc1_uman Rev.1.0 / 2023

# About document revisions

The following revisions have been made to the documentation

Abc1_uman Revision History

| Date | Version | Change History |
|---|---|---|
| Feb. 29, 2023. | Rev 1.0 | Initial deployment |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# About this product documentation

This instruction manual is a guide for the installation, system configuration, use, and setup of the A.bc1/A.bc-TS1 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 A.bc1 with external devices such as access control panels, access control servers, door locks, etc., please refer to the documentation of the product or contact the product's supplier for proper connection.

The software AOS embedded in A.bc1 performs functions such as identification and access control policies, device startup conditions, and device management, and is accessible as a web-based service through web browsers such as Chrom, Edge, and Safari on users' 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 A.bc1 devices and cannot be applied to other HW.

This product manual describes the A.bc1/A.bc-TS1 and includes both the AOS User's Guide as an <Appendix>, so keep it handy so you can access it whenever you need it.

This product documentation is provided 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 notice to improve the performance of the product

# Copyright

A.bc1, A.bc-TS1, AOS, and all programs, data files, and contents covered in this manual are protected by copyright laws and confidentiality agreements. Any use, copying, disclosure to third parties, or distribution not expressly authorized by ANDOPEN is strictly prohibited.

# Certifications of A.bc1

Type tested
Production monitored
TÜV
SÜD
C
US

# 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.

### ■ > :

Idicates 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 by pressing the keyboard.

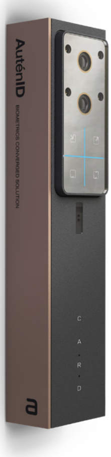
### ■ 'Select '

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



ID Card and Face recognition
Converged Access Terminal

**A.bc1/A.bc-TS1**

+

**High secured Bio-ID card : ACC**

Personalized by using users photo and
pre-delivered to personal users

A.bc1/A.bc-TS1 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 embeds the user's facial image into the card. (A.bc-TS1 is a product that includes a body temperature detector in A.bc1. Hereinafter, we will refer to A.bc1, and the features of A.bc-TS1 are specified separately.)
Even though it uses the familiar "look-and-tag" behavior like card authentication, it is facially recognizable, 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, a user's biometric information is only used under that user's control. As a result, biometric information is not stored anywhere, including authentication terminals and servers, and there is no transmission process, so it is a new concept of biometric authentication system that completely blocks the risk of sensitive information leakage and protects privacy.

This allows A.bc1 to integrate with existing card-based access control systems out of the box without any physical changes.

A.bc1 is a face recognition access control terminal that can be installed in a wide variety of places. The width of the product is about 5cm, and it is designed to be installed not only on the wall but also on the standard door frame. In addition, considering the convenience of construction, DC and PoE power are simultaneously supported and automatically selected. For interconnection with diverse access control devices, it supports various communication environments and connectivity through I/O consisting of 30 lines, allowing you to configure a wide range of access control systems.
In addition, you can easily operate the system by using AOS, a web-based access control management software embedded inside A.bc1 without a separate access control management SW.

For more information on the 'AutenID' 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

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

## 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 use the features of the product effectively, you must read the contents of 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 and do not disconnect power while the Product is in use. This 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 and PoE power input to A.bc1 and the lock power, input signals, wiring cables, etc. provided through A.bc1.

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

- We prohibit anyone other than the manufacturer from modifying or attaching parts to the product. If the product fails due to this, you will not be eligible for free service and warranty service.

- 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 and use the Product in areas that are magnetic or subject to magnetic fields or electromagnetic interference. The product may be damaged by magnetism or its performance may be impaired.

- 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 do not expose it to high temperatures or direct sunlight.
In particular, make sure that the product's camera is not facing a strong light source, such as halogen or sunlight. This can reduce recognition rates.

- This product is IP65 water and dust resistant. Do not expose it to environments above this standard.

- Do not leave management PCs unattended with being accessed to the product's management software (AOS).

- Ensure that information that needs to be secured, such as user accounts, passwords, user DBs, and authentication logs, is not leaked.

- o not place or hang objects on the product

- AOS is shipped embedded on the device and installed by the vendor (preinstalled), so there is no user installation available.

- A.bc1 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 make copies of user information from time to time, 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

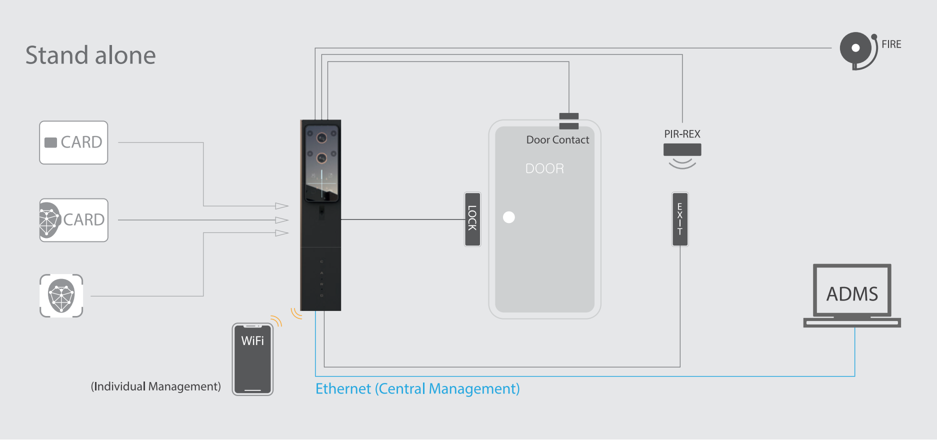
## ■ A.bc1 Product Documentation

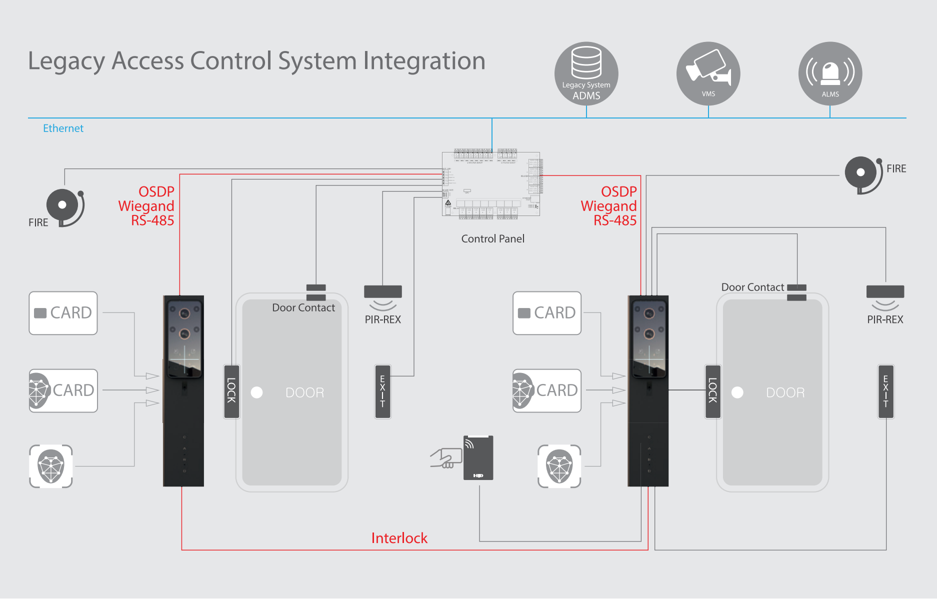
## ■ AOS User Guide <Appendix>

# A.bc1 Product Documentation

## 1. System Configuration

A.bc1 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 A.bc1, while still using all the resources of a traditional card-based system.

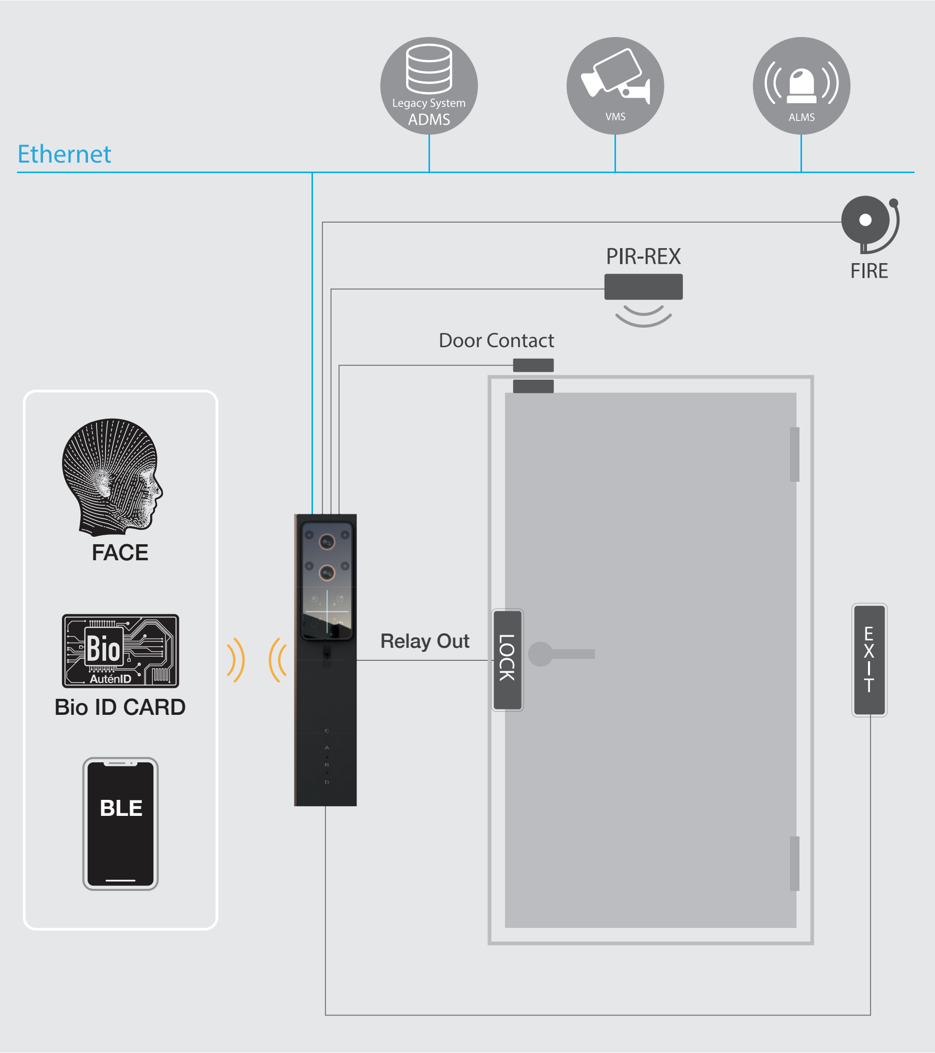




## 1.1 Standalone operating mode

This figure describes the typical configuration that A.bc1 directly controls the door by connecting the lock, exit button, door sensor, RTX, fire input, etc.
Users perform facial recognition by tagging a biometric card while looking at A.bc1 for facial authentication.

A.bc1 could be directly connected with diverse access control devices, upon authentication success, A.bc1 opens the door.

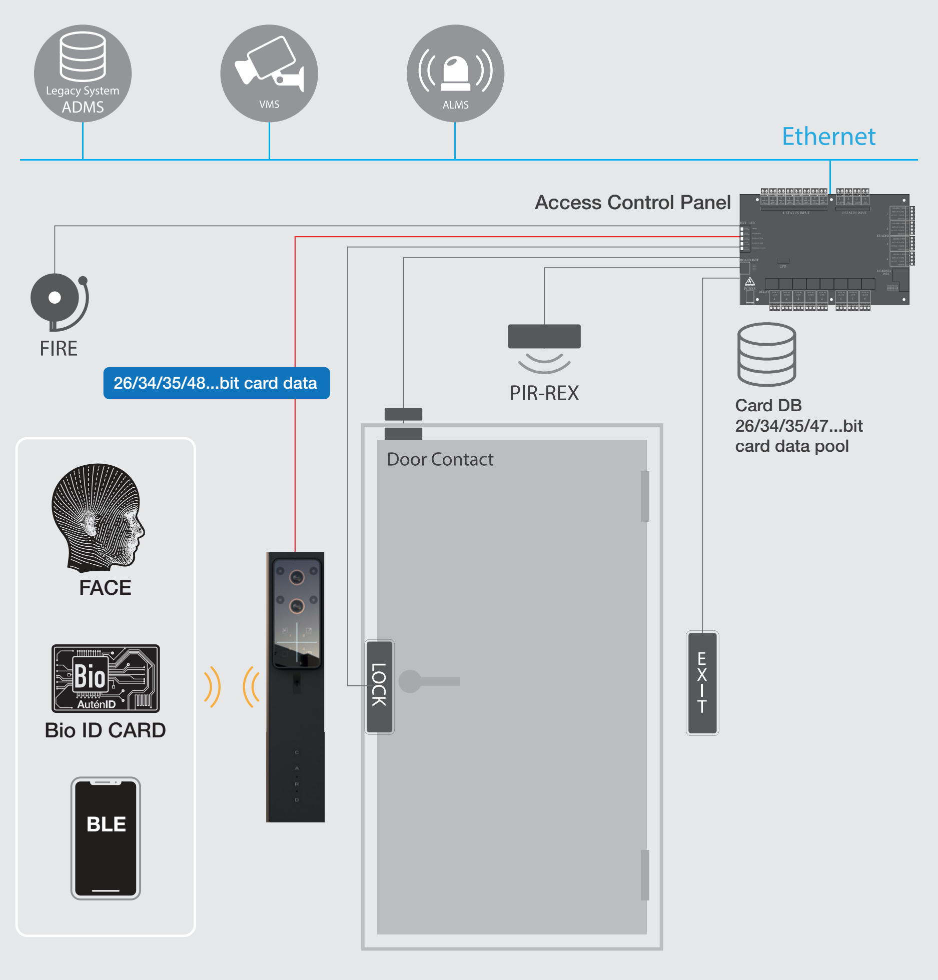


## 1.2 Access Control Panel Integration Mode

A.bc1 works with the access control panel to control the door. The user can perform facial authentication by tagging their biometric card while looking at the A.bc1.

Upon successful authentication, A.bc1 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 door is unlocked by the access control panel 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.



# 2.  Product

## 2.1  Specification

| | |
|---|---|
| Model Name | A.bc1 / A.bc-TS1 |
| Central Processing Unit | ARM Octa Core |
| Display | 3-color LED indicator |
| Touchpad | 4 Button - For Time & Attendance |
| Supported Authentication modes | • Card Authentication<br>• Biometric Card & Face Recognition Fusion Authentication<br>• QR Code Authentication<br>• Bluetooth / NFC Mobile Card Authentication<br>• (Face authentication only mode - optional) |
| Dual camera | Color/infrared dual camera |
| High-speed image processing | Low-light and backlight compensation, auto exposure, high dynamic range (HDR) |
| Fraud Prevention (Liveness) | Triple Fraud Protection |
| Face Verification Distance | Biometric card & facial recognition fusion authentication mode (up to about 1.2 meters)<br>Face authentication only mode (up to about 2 meters) |
| Lens and angle of view | Fixed focus combined lens, 120 degrees |
| Accuracy | 100% (ID card & facial recognition fusion mode) |
| Recommended number of users | Unlimited |
| Recommended number of users enrolled faces | 최대 3,000 Faces (using Face Recognition Only mode) |
| RF Card Reader | 13.56Mhz (ISO-14443A/B, ISO-15693) |
| Card Technologies | ACC / Mifare / Desfire / Felica / Jaca / NFC / iClass (optional) |
| Communication | Ethernet / WIFI / OSDP / RS-485 / Bluetooth |
| Input | Door status detection x2 / Exit button / Motion detection (REX) / Fire Alarm x 2 (dry & wet contact)/ Wiegand / GPI / Hold Open / Alarm release |
| Output | Relay / Wiegand / Alarm / Tamper detection / Operation status / GPO / malfunction (service!request) / 5V DC out |
| Event Logs | 4,000,000 events can be stored |
| Proximity Sensors | Support |
| Sound Output | Voice / Buzzer |
| Power Input and Consumption | PoE and  7~24VDC, 12Watt |
| Connectors | RJ45, 30 pin pig tail |
| Data encryption | AES128 / 256 encryption |
| Encrypting communications | ASE 256 encryption |
| Waterproof / Dustproof | IP 65 |
| Safety standards | 850nm, IEC-62471 |
| Operating Temperature /  Humidity | -10℃ ~ 60℃ / 0%~80% |
| Dimension | 50 x 40 x 230 mm (A.bc1) / 50 x 40 x 275 mm (A.bc-TS1) |
| Authentication | KC, FCC, CE, NRTL |
| Detect detachment | Support |
| Measuring  body temperature | Supported on A.bc-TS1 models |

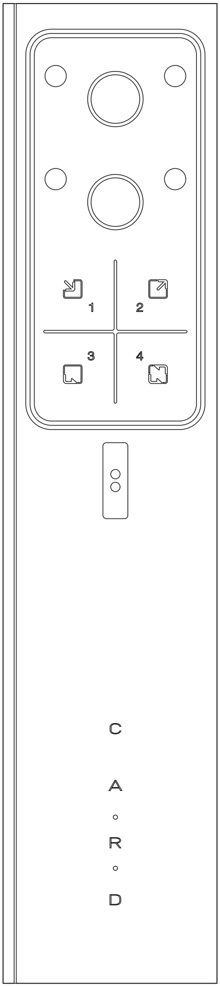
* ACC: ANDOPEN biometric card, other cards cannot embed biometric information.

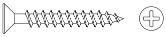
*Caution*   Comply with all electrical standards recorded in the specification.
*Caution*   Provide sufficient and reliable DC power or PoE power to A.bc1

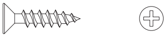
# 2.2 Components

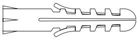
**When you purchase a product, make sure that you have all the components that are included. If the components are missing, contact your sales representative.**

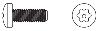
A.bc1 (1)

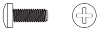


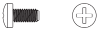

M4 x 25mm (4)

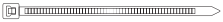

M4 x 15mm (4)


Nylon screw anchor (4)

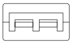

M3 x 8mm (1)

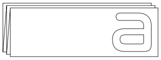

M3 x 8mm (1)


M3 x 6mm (1)


Nylon cable tie (1)

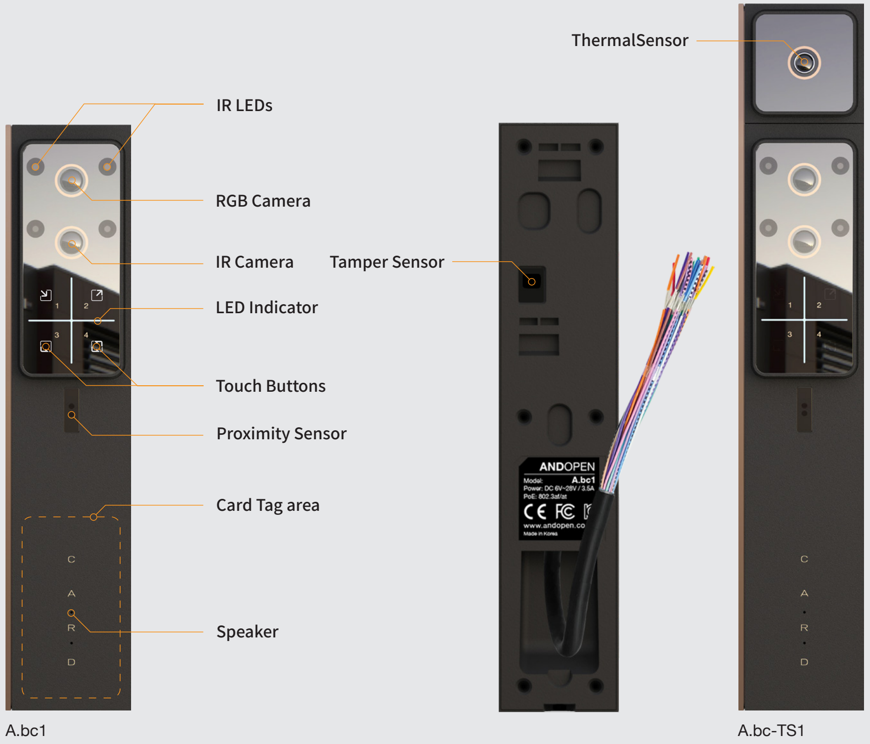
22 ohm resistor (30)

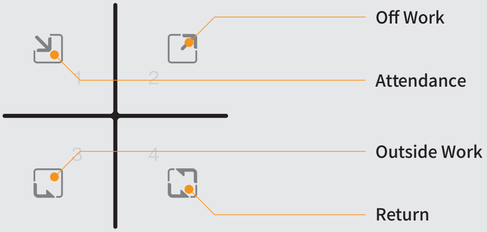

Ferrite (1)


Installation Guide (1)

* The product image above is A.bc1, and the thermal sensor module is shipped with A.bc-TS1.

## 2.3 Part Names and Functions



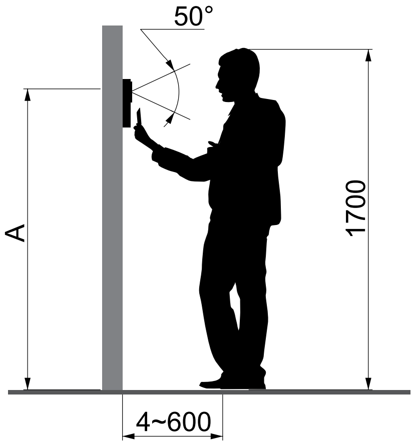


# 3. Installation

- 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 to connect the provided resistors 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, install it so that the mounting surface and the user's face are aligned so that they are parallel.
- For ease of use and optimal performance, install A.bc1 at eye level, taking into account the average height of your users.



**A：Recommended height**
(height from floor to RGB Camera):

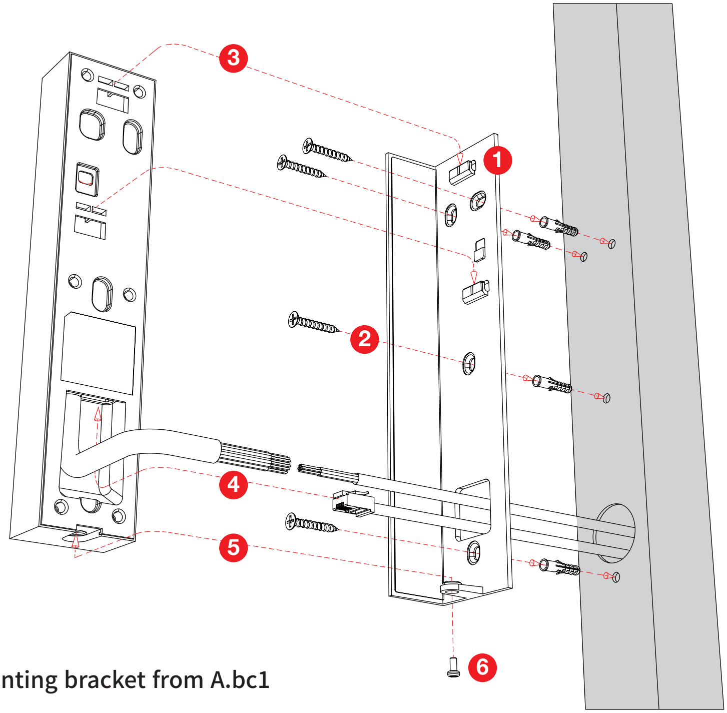
- Northeast Asia: 154 cm
- Southeast Asia: 152 cm
- Americas: 158 cm
- Northern Europe: 163 cm

## 3.2 Lighting environments

- Set up A.bc1 in a place where the light will evenly illuminate your face.
- Avoid lighting from above, behind, and to the side of your face.
- Avoid direct sunlight or strong lighting on A.bc1.
- Avoid strong downward or upward light and backlighting that creates shadows on the face.

## 3.3 Product Installation

Follow these steps to install the product correctly
Pull out the necessary wires, such as power cables, Ethernet cables, and data cables enough from the attachment surface before installing the product.



① Remove the mounting bracket from A.bc1
* Note *
The mounting bracket is assembled on the product (gold color part).
The mounting bracket is assembled and can be removed by pulling the part in a downward direction.

② Pass cables and wires through the rectangle hole of the mounting bracket and securely fasten the fixing bracket to the attachment surface using the screws (M4x25) provided. If necessary, use the included screw anchors.

③ Connect the power, cables, and wires to be used to each other correctly.
* For interface cable details, refer to the Pin map table below.

④ If necessary, connect Ethernet (or PoE) to the Ethernet port on the back of A.bc1.
* Wrap the ferrite core to the 30pin interface cable.

⑤ Combine A.bc1 with the mounting bracket completely.

⑥ Secure A.bc1 to the mounting bracket with the provided M3 screws.

# < Interface Cable PIN MAP >

| | | |
|---|---|---|
| 1 | Blue Dot | OSDP G 1 |
| 2 | White | GND (Signal) |
| 3 | Sky Blue Dot | Wigend IN D1 |
| 4 | Blue | OSDP G 0 |
| 5 | Green Dot | Wigend OUT D1 |
| 6 | Sky Blue | Wigend IN D0 |
| 7 | Black | GND |
| 8 | Green | Wigend OUT D0 |
| 9 | Red | VCC IN |
| 10 | Red Dot | VCC IN |
| 11 | Pink | Fire Alarm OUT |
| 12 | Black Dot | GND |
| 13 | Violet | Fire Alarm IN(DC) |
| 14 | Light Violet Dot | RTE |
| 15 | Brown | Fire Alarm IN |

| | | |
|---|---|---|
| 16 | Light Violet | Exit Button |
| 17 | Light Brown | Door Status2 |
| 18 | Violet Dot | Release Fire alarm |
| 19 | Light Brown Dot | Door Status1 |
| 20 | Gray | Hold Input |
| 21 | Yellow | Relay NC |
| 22 | Brown Dot | Tamper / Power fail |
| 23 | White Dot | Relay COM |
| 24 | Light Green | RS485 RX |
| 25 | Yellow Dot | Relay NO |
| 26 | Light Green Dot | RS485 TX |
| 27 | Orange Dot | Service Required |
| 28 | Gray Dot | GPO |
| 29 | Orange | VCC OUT 5V |
| 30 | Pink Dot | GPIO |

## 3.4 Wiring

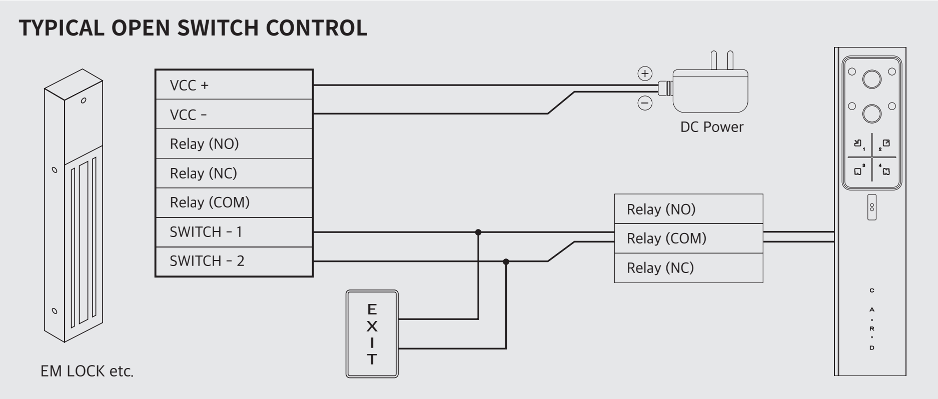
- Familiarize yourself with the wiring manuals of the lock and external device provider, and wire A.bc1 in relation to the operating characteristics of the lock. Also, be sure to fully understand the functionality of AOS later in this manual, and proceed with the wiring in line with your purpose.

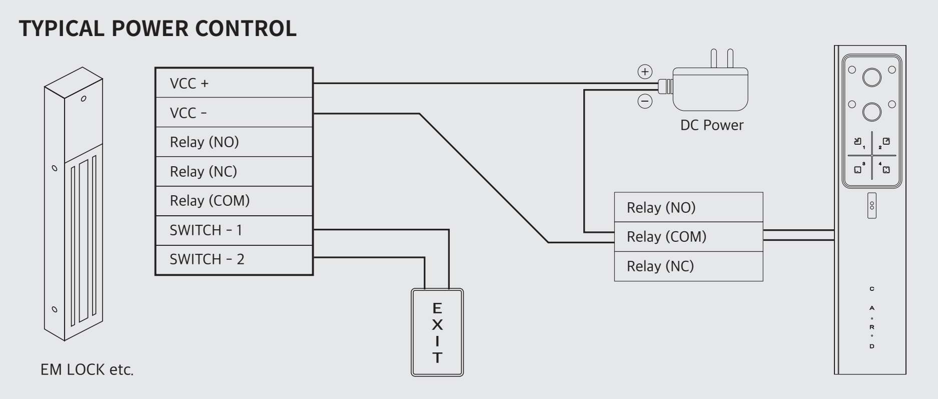
- The maximum current allowed by the Relay circuit in A.bc1 that connects to the lock is 2A. Check the compatibility and maximum current of the locks such as EM-LOCK, Dead Bolt, and Striker, and ensure that the current applied to the Relay circuit in A.bc1 is 1.8A or less. If more current is applied, 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 size
* Caution : Use Shielded Twisted Pair (STP) Cat5e, 568B for Ethernet connections.

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





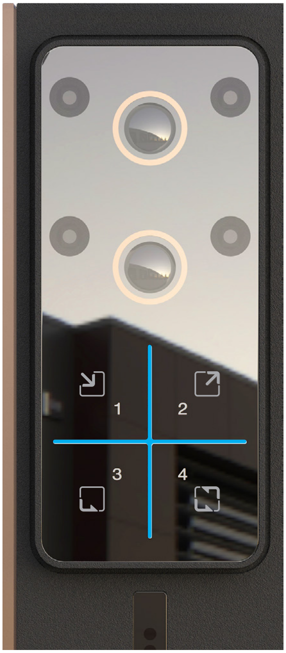
# 4. Using the product

## • Boot A.bc1

- The device's center cross LED lights up and rotates when power is connected.
- It takes about 25 seconds to 1 minute for the device to boot up.

## • A.bc1 is ready

- When booting is complete, you'll hear a boot sound and the cross LED will light up blue, as shown below.



## • Facial Recognition

- When the front proximity sensor detects an object or person, the four Touch LEDs and IR LED light up.
- With the four Touch LEDs and IR LED lit, 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 crosshair LEDs light up red when authentication fails.
- he crossed LEDs light up green upon successful authentication.

# 5. Troubleshooting

## 5.1 Reboot (Restart)

If the device becomes slow or operates abnormally due to unexpected causes such as static electricity or unstable power, restarting the A.bc1 may resolve the issue.
You can reboot by accessing AOS (A.bc1 built-in Web-based management software) and pressing the [Save] button without changing any settings in the network settings.

Alternatively, you can reboot by physically disconnecting and reapplying power (disconnecting and reapplying DC power about 5 seconds later, or removing the PoE cable and inserting it after about 10 seconds).

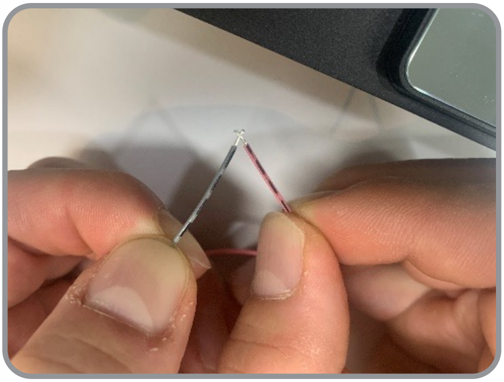
In some cases, a power reboot may resolve more issues.

## 5.2 Factory Reset

If you lose your network information and cannot access AOS permanently, or for any other reason, you want to factory reset the A.bc1, you can do so by touching the GPO (gray dotted line) and GPIO (pink dotted line) wires of the 30-pin interface cable for about 5 seconds, as shown in the figure below.
(See the Pin-map table in "3.3 Product Installation").

This action reverts all settings to factory default values, including the administrator account and password.
However, the user list and various log data will not be initialized.

Please do not use this feature without sufficient knowledge of the product and its usage, and contact an expert before using this feature.



< Appendix >

# AOS User Guide

## 1. AOS Overview

AOS is a terminal-embedded software for setting A.bc1'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 A.bc1 from 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)
- A.bc1 which is powered on

To access AOS, you must first connect A.bc1 with the administrator's PC with authorized access.
The administrator can connect to A.bc1 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 A.bc1 to each other with an Ethernet cable, and make sure the green LED on the A.bc1 RJ45 port is lit to confirm a normal connection. (The green LED above will be lit when the A.bc1 and PC are powered on and connected properly.)

Once the PC and A.bc1 are physically connected, the PC and A.bc1 can attempt to network with each other.
In order for the PC and A.bc1 to communicate, you must make both devices exist on the same network.

**The default wired network setting of Abc1 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 Abc1, **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

A.bc1 acts as the Wi-Fi Access Point (Wi-Fi AP) initially.
Find A.bc1 by searching for Wi-Fi APs on the administrator PC.
The name of the AP appears as a combination of 'Abc1' and 'A.bc1's MAC address'.
**(e.g. A.bc1_c0:84:7d:03:67:b2).**

The AP access password is **'andopen1234'**. (Case sensitive)
The IP address to access A.bc1 through this Wi-Fi connection is **'192.168.20.1'**.
The Wi-Fi connection method allows you to access A.bc1 directly without having to consider 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

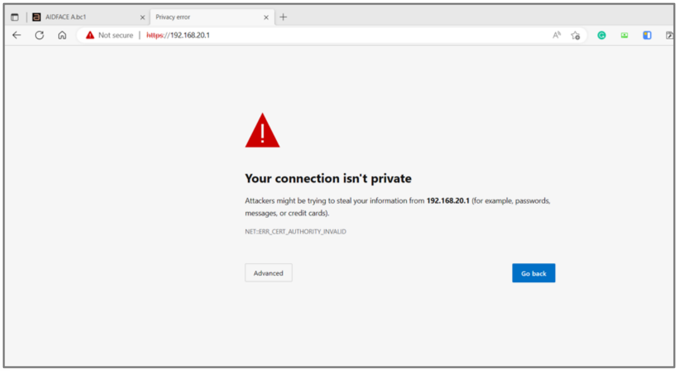
Once the connection environment is ready, you can access AOS. AOS is a web-based service software embedded in A.bc1 to set the operation of A.bc1, and it can be accessed through a browser on a PC like a cloud-based SW, without installing a separate program on the administrator's PC.
With the connection ready, launch a web browser on the administrator's PC.
Enter the address of A.bc1 in the address bar of the web browser to access AOS.

Depending on your network access method, the connection address may look like this

| | |
|---|---|
| 유선 네트워크 연결 | **https://192.168.30.1** |
| 무선 네트워크 연결 (Wifi) | **https://192.168.20.1** |

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

As shown in the example below, if you type https://192.168.30.1 (wired network connection) or https://192.168.20.1 (wireless network connection) into your web browser's address bar and go to the page, you may see a safety warning message, but you can ignore it because your PC and A.bc1 are connected 1:1 and there is no safety risk.

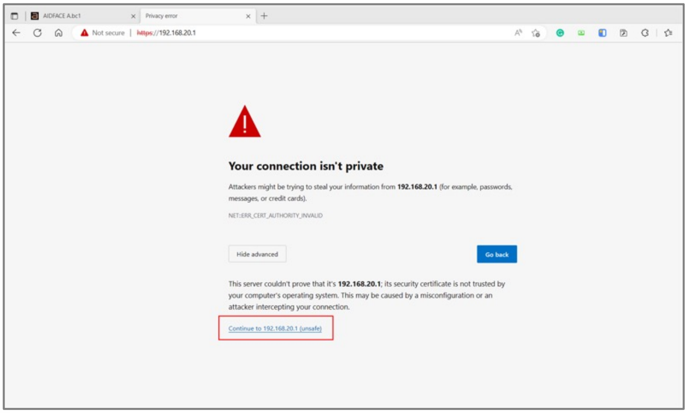


**Your connection isn't private**

Attackers might be trying to steal your information from **192.168.20.1** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

To continue accessing AOS, click [Advanced > 192.168.30 (or 20).1 (unsafe)] and follow the steps to accept the transfer to that page.
(The example screen is based on the Microsoft Edge web browser, other web browsers may have a different format for the safety warning message.
Please follow the steps to accept the navigation to the appropriate page).



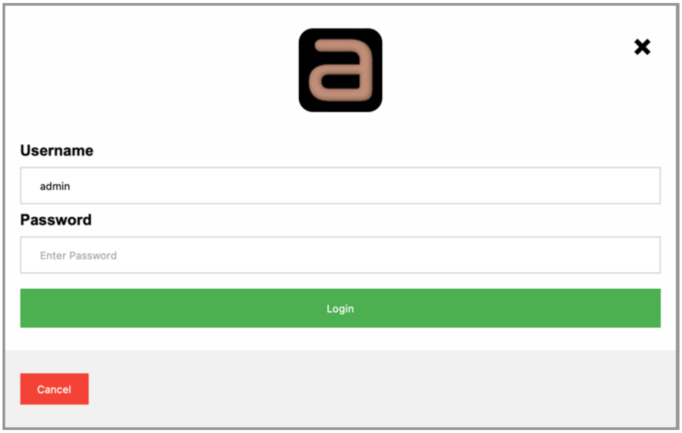
**Your connection isn't private**

Attackers might be trying to steal your information from **192.168.20.1** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.20.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

# 2.2 로그인



This product prevents unauthorized access through the login process via ID and Password.
Once your PC and A.bc1 are connected to the network, you will see the login page to access AOS, as shown above. 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 A.bc1) is 5, the factory default username and password are as follows Administrator usernames and passwords are case sensitive.

| | |
|---|---|
| Administrator ID | admin |
| Administrator Password | admin |

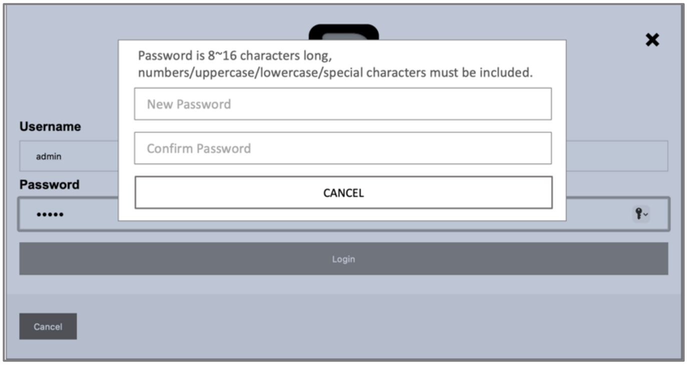
After you successfully log in to your device for the first time with the default username and password above, you will see the password change page below.
**You must change your password before you can proceed to the next step.**

Your password must be 8-16 characters long and contain numbers, uppercase, lowercase, and special characters. Enter the correct password twice in a row to complete the password change process. If you press Cancel, you will be taken back to the initial login screen without changing your password. The changed password is encrypted and stored in AOS.

***Caution***

Please make your changed password not be leaked or lost.

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

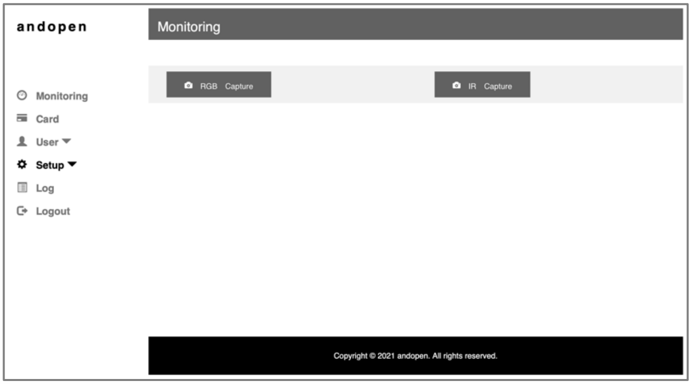


Password is 8~16 characters long, numbers/uppercase/lowercase/special characters must be included.

Username: admin

Password: •••••

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.

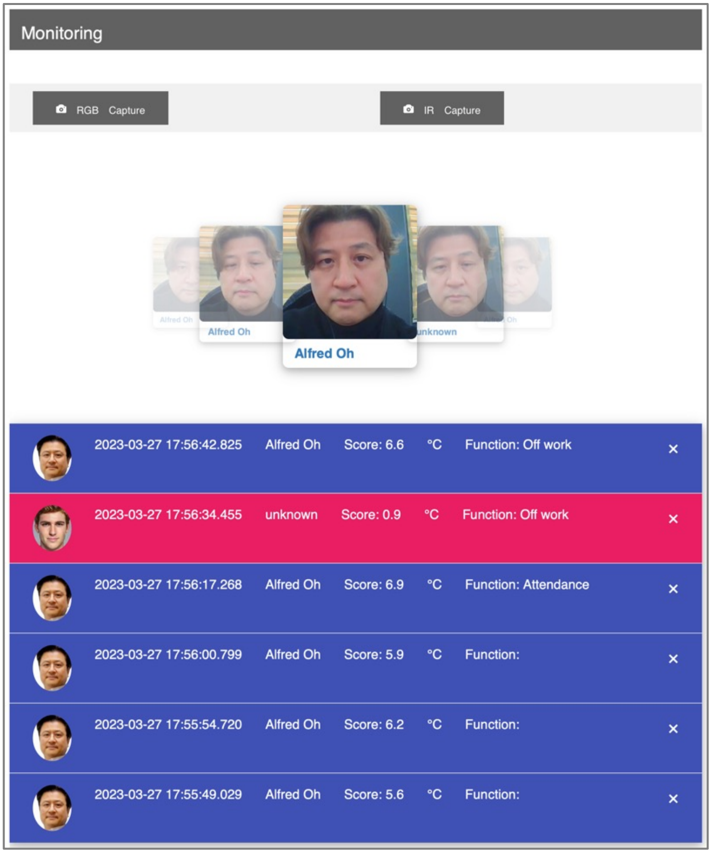


Copyright © 2021 andopen. All rights reserved.

## 2.3 Monitoring

The Monitoring feature is for observing the status of A.bc1'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



| | | | | | | |
|---|---|---|---|---|---|---|
| | 2023-03-27 17:56:42.825 | Alfred Oh | Score: 6.6 | °C | Function: Off work | × |
| | 2023-03-27 17:56:34.455 | unknown | Score: 0.9 | °C | Function: Off work | × |
| | 2023-03-27 17:56:17.268 | Alfred Oh | Score: 6.9 | °C | Function: Attendance | × |
| | 2023-03-27 17:56:00.799 | Alfred Oh | Score: 5.9 | °C | Function: | × |
| | 2023-03-27 17:55:54.720 | Alfred Oh | Score: 6.2 | °C | Function: | × |
| | 2023-03-27 17:55:49.029 | Alfred Oh | Score: 5.6 | °C | Function: | × |

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. The accumulated attempted faces are scrollable, 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.

- Facial image stored inside the biometric card used during authentication attempt, or ‘CARD icon' when users tag a card which is allowed 'card exclusive authentication'.

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

- The user’s name stored in the biometric card on successful authentication and 'unknown' on failed authentication.

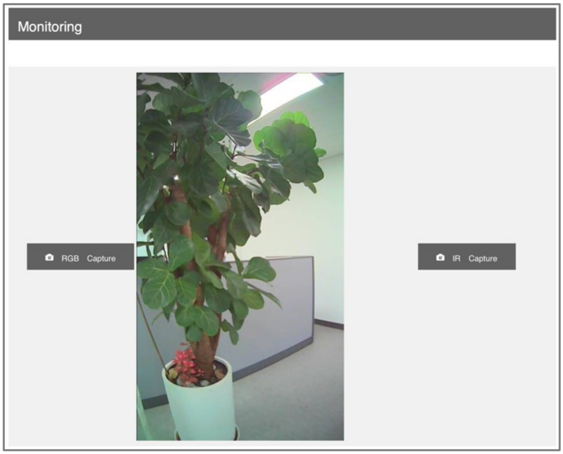
- Facial authentication score: Higher scores mean higher similarity of the face.

- Body temperature: Displayed for A.bc-TS1, otherwise, only the Celsius symbol is displayed.

- Time &Attendance: When the user authenticates by pressing the corresponding T&A button in A.bc1, 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 ‘ – ’.

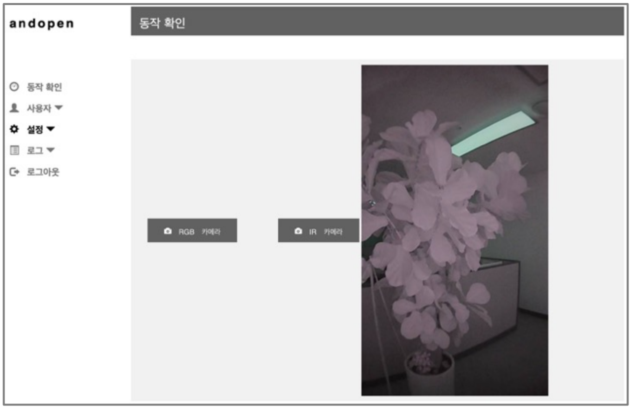
## ▶ Monitoring > [RGB Camera]

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.

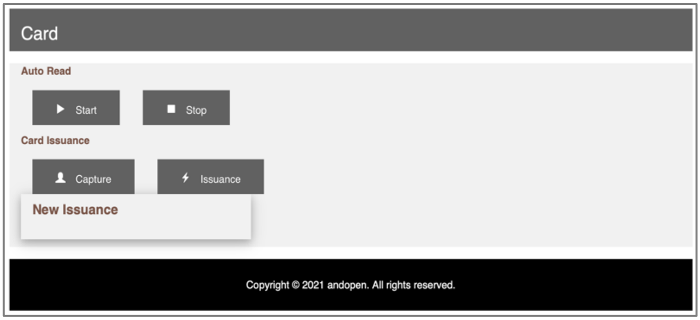


## 2.4 Cards

The Card tab is a feature that allows you to issue biometric cards using A.bc1.
You can use the blank ACC (Andopen 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 A.bc1.

A user's face can be rewritten up to three times on the same card.

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.



### 2.4.1 Card > Auto Read

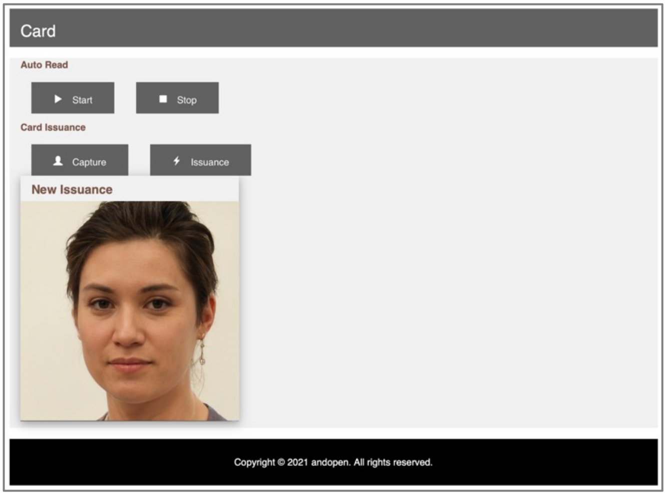
- **Card > [Stop]:**

This button switches A.bc1 from authentication mode to card issuance mode.
If you press [Stop], A.bc1 will not try to authenticate your face even if you tag a card.

- **Card > [Start]:**

Completes card issuance and returns A.bc1 to authentication mode.
After pressing [Start], A.bc1 will perform face authentication when you tag the card.

## 2.4.2 Cards > Card Issuance



### • Card > [Capture]:

Take a picture of the face to be recorded on the card. Face the top camera of A.bc1 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.

*** Note ***

- ake off your hat and register your front face
- Avoid faces with veiled eyebrows or unclear facial contours
- Avoid faces that are out of focus and blurry, faces that are too light or dark to distinguish features
- Avoid faces that are only light on one side.

### • Card > [Issuance]:

Record the captured face image and basic information on the biometric card. The basic information recorded on the card is shown below. With the card to be issued tagged to the card recognition area of A.bc1, press the [Issuance] button. When the issuance is completed, you will hear a voice prompt saying ‘It has been issued’.

*Note*.

Do not take away the card until you hear the guidance voice. An encoding error may occur and the card may be unusable forever.

When issuing a biometric card in A.bc1, user information is automatically generated and recorded on the card using CSN as the base information for convenience. The user information that is automatically recorded is as follows.

- UID: CSN
- Card number: CSN
- Name: CSN
- Captured face images

When a card is issued, it is automatically saved to A.bc1's user list using the information above. You can change the name of the user list.
User lists and CSNs are described in "2.5 Users"

***Caution**
**After completing all the issuance, be sure to press [Start] to switch A.bc1 to authentication mode.**

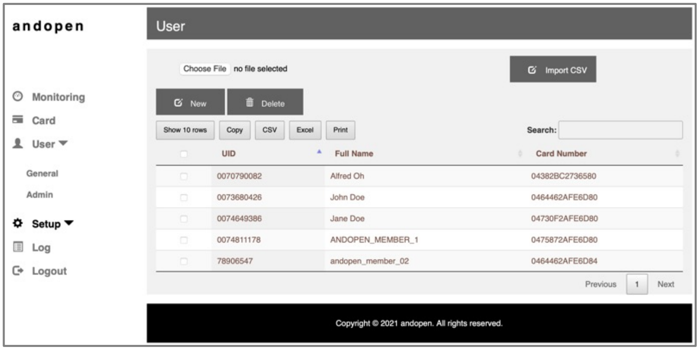
## 2.5 Users

The User tab is for managing administrators who have access to AOS and regular users who use facial recognition with A.bc1.
You can navigate to the submenu (General User, Administrator) tab by pressing the triangle on the right side of the User tab.

### 2.5.1 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 biometric card). 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.

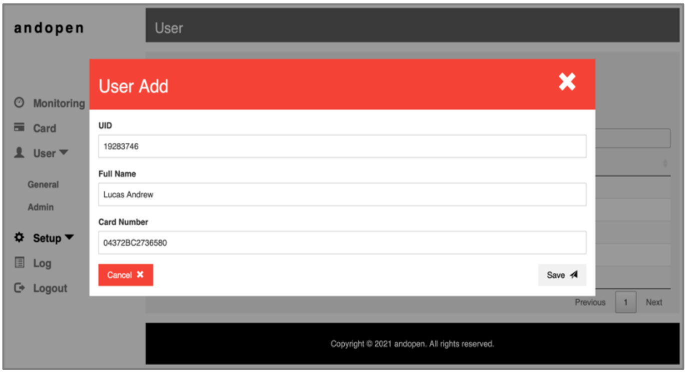


| □ | UID | Full Name | Card Number |
|---|---|---|---|
| □ | 0070790082 | Alfred Oh | 04382BC2736580 |
| □ | 0073680426 | John Doe | 0464462AFE6D80 |
| □ | 0074649386 | Jane Doe | 04730F2AFE6D80 |
| □ | 0074811178 | ANDOPEN_MEMBER_1 | 0475872AFE6D80 |
| □ | 78906547 | andopen_member_02 | 0464462AFE6D84 |

Copyright © 2021 andopen. All rights reserved.

### • 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 A.bc1 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.



User Add

UID: 19283746

Full Name: Lucas Andrew

Card Number: 04372BC2736580

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

- UID: excludes special characters, allows mixed alphanumeric characters (up to 12 characters)
- Name: Up to 32 characters, including spaces (no language restrictions)

- Card number: CSN (hexadecimal, max=FFFFFFF)

- 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.

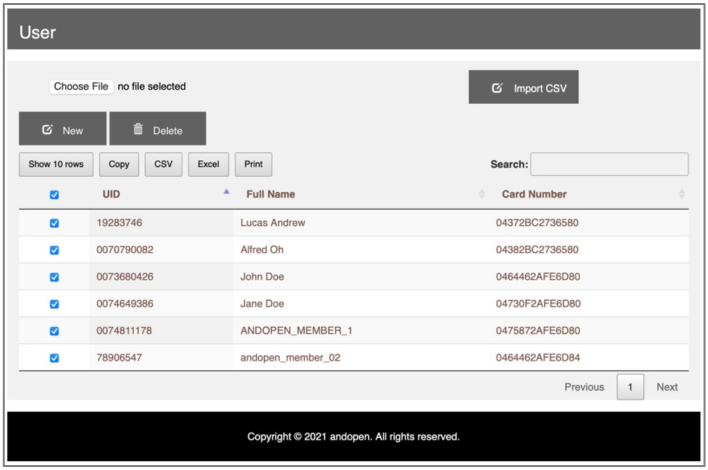
***Caution*.**
When entering user information by typing it in, make sure it is correct and does not differ from the information stored on the user's actual biometric card. In particular, if the card number entered is different from the actual biometric card, authentication may not succeed, even for the 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).



| ☑ | UID | Full Name | Card Number |
|---|---|---|---|
| ☑ | 19283746 | Lucas Andrew | 04372BC2736580 |
| ☑ | 0070790082 | Alfred Oh | 04382BC2736580 |
| ☑ | 0073680426 | John Doe | 0464462AFE6D80 |
| ☑ | 0074649386 | Jane Doe | 04730F2AFE6D80 |
| ☑ | 0074811178 | ANDOPEN_MEMBER_1 | 0475872AFE6D80 |
| ☑ | 78906547 | andopen_member_02 | 0464462AFE6D84 |

Copyright © 2021 andopen. All rights reserved.

## • User > General > [Backup]:

This function manually creates a copy of the current user list on the device. Click [Backup] to update the current user list to the latest one.

*** Note ***
For stable user list management, it is recommended that you create a copy of the user list after making the correct changes in the user list.

## • User > General > [Restore]:

A copy of the user list is automatically created every Monday at 5:00 am, based on the time when A.bc1 was first activated.
If you accidentally delete a user, or for any other reason want to revert the user list to an earlier list, you can press [Revert] to revert the user list to the last created copy.
To apply the recovered user list as the operational user list, press [Save].

### • User > General > [Select 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 > [Batched Registration]:

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 > [Export to CSV]:

[Export to 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 > [Export to 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]:

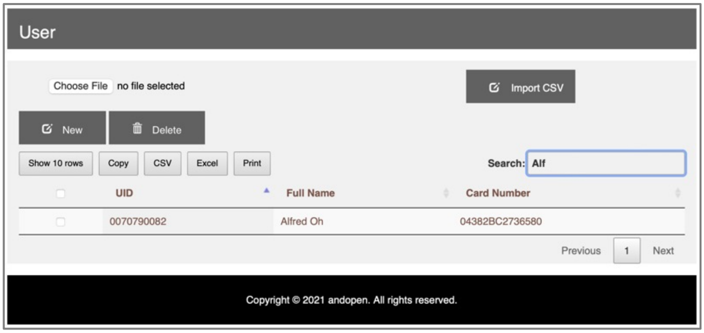
Print the entire list of registered users to the printer installed on the PC connected to AOS. After that follow the steps for using the printer.

### • 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 > [Lookup]:

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 'Lookup' and it will find and display records containing it in real-time as you type.



Search: Alf

| □ | UID | Full Name | Card Number |
|---|---|---|---|
| □ | 0070790082 | Alfred Oh | 04382BC2736580 |

Copyright © 2021 andopen. All rights reserved.

### • User > General > [Show One Screen]:

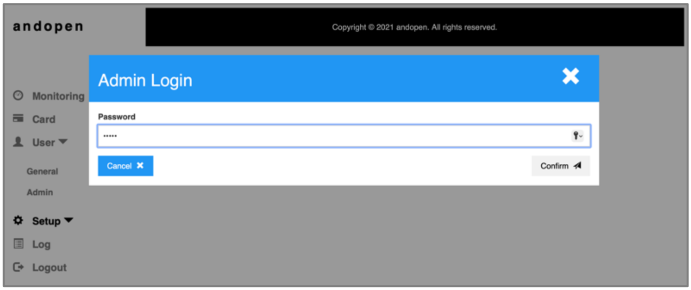
Set the number of records displayed on one screen. You can set the number of user records (number of rows) displayed at a time by pressing the [Display one screen] button: 10, 25, 50, 100. The default value is 10.

### • 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.

## 2.5.2 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 ***

• 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.

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

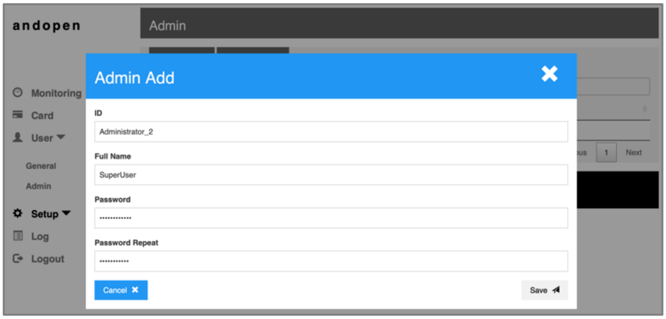
• Do not disclose your registered administrator ID and password to anyone other than those with administrative privileges.

• 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 and cannot access it, you can access it with the initial administrator account by "Factory Reset".

• 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.)



ID: Administrator_2

Full Name: SuperUser

Password: ............

Password Repeat: ...........

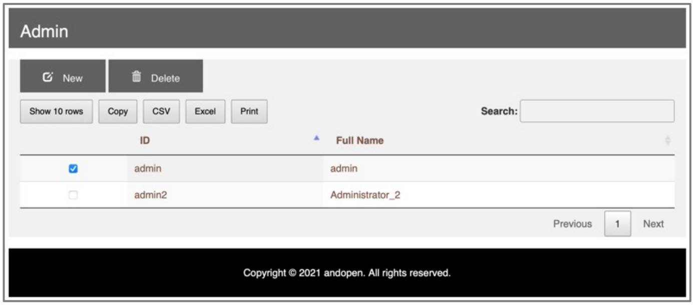
The maximum number of administrators that can be registered and the maximum number of simultaneous connections is 5.

## • 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).



| | ID | Full Name |
|---|---|---|
| ☑ | admin | admin |
| □ | admin2 | Administrator_2 |

Copyright © 2021 andopen. All rights reserved.

### ▶ Edit a registered administrator

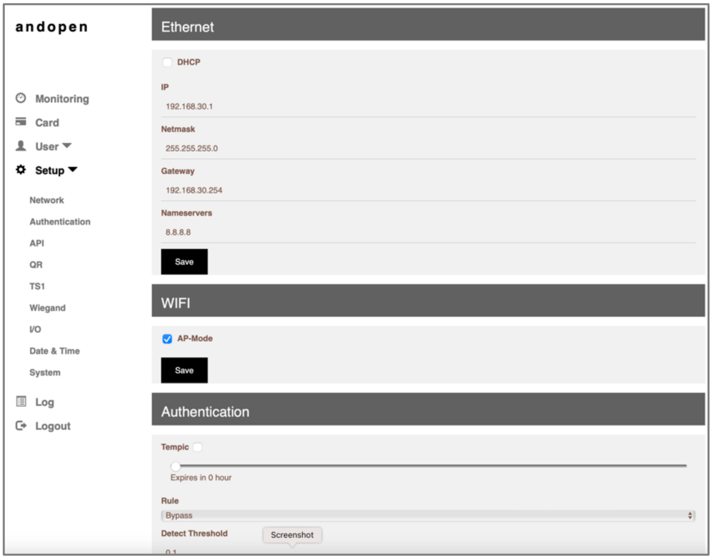
You can edit the name and password of an already registered admin.
You can change the password in the pop-up window that appears by double-clicking the administrator ID or name of the administrator you want to edit.
The administrator ID cannot be changed, and if you need to change it, please delete it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

### • User > Admin > [Show One Screen], [Copy], [Export to CSV], [Export to Excel], [Print], [Lookup]:

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

## 2.6 Setup

AOS provides the ability to set the overall initial operation and condition setting for A.bc1. 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.



□ DHCP

IP
192.168.30.1

Netmask
255.255.255.0

Gateway
192.168.30.254

Nameservers
8.8.8.8

☑ AP-Mode

Tempic □

Expires in 0 hour

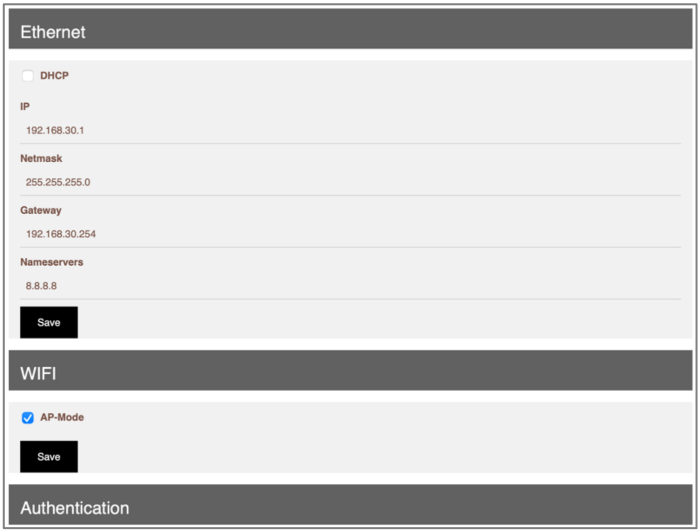
Rule
Bypass

Detect Threshold
0.1

## 2.6.1 Network

Perform the network settings for A.bc1. A.bc1 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.



Ethernet

□ DHCP

IP

192.168.30.1

Netmask

255.255.255.0

Gateway

192.168.30.254

Nameservers

8.8.8.8

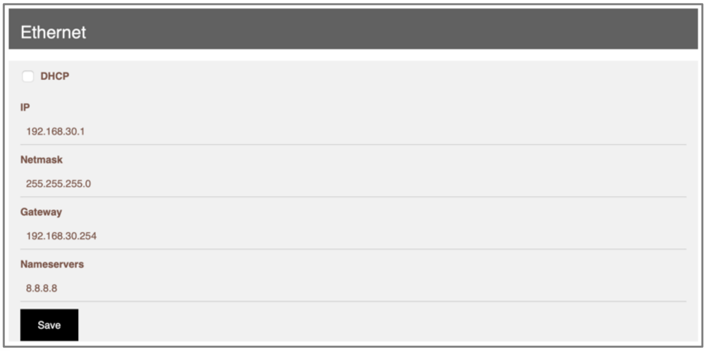
WIFI

☑ AP-Mode

Authentication

### ▶ 유Setting up a wired network

You can specify the values of IP address, Netmask, Gateway, and Nameservers for using A.bc1 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.



Ethernet

□ DHCP

IP

192.168.30.1

Netmask

255.255.255.0

Gateway

192.168.30.254

Nameservers

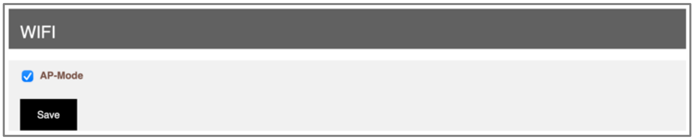
8.8.8.8

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]. **A.bc1 will reboot automatically immediately.**

*** Caution ***

• When A.bc1 reboots, the network changes will be applied, so to reconnect, you need to change again the network settings on the PC appropriately so that A.bc1 and the PC are on the same network.
• Write down the IP address of each A.bc1 so that you do not forget the static IP address you changed. If you forget the IP address or otherwise become unable to connect to the device over the network, you can restore the factory-set IP address by performing a factory reset.
For more information about factory reset, please refer to "Factory Reset" in this user manual.

### ▶ Set up a wireless network

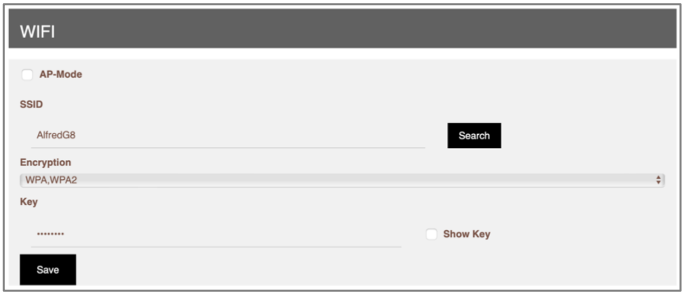


WIFI

☑ AP-Mode

Set up the wireless network environment for A.bc1. Initially, A.bc1 is set to AP-Mode.

When AP-Mode is enabled, A.bc1 operates as a Wi-Fi Access Point. Therefore, A.bc1 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 A.bc1.
It is recommended to keep AP-Mode when using a wired network.



WIFI

□ AP-Mode

SSID: AlfredG8

Encryption: WPA,WPA2

Key: ........

□ Show Key

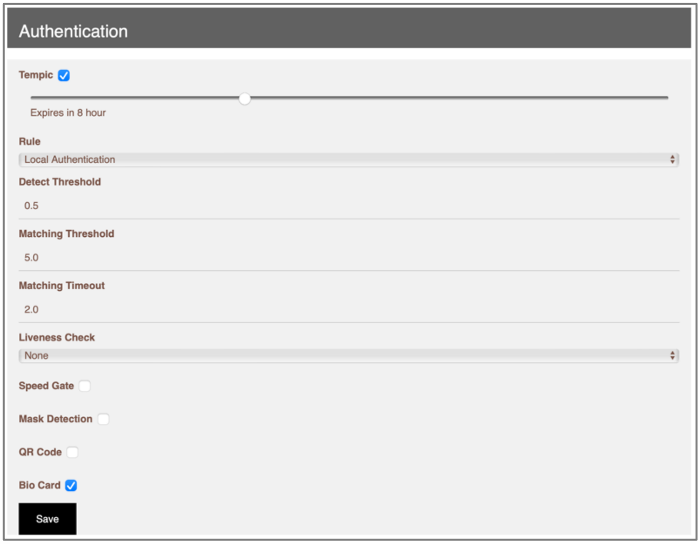
Disabling AP Mode will allow you to set up to connect to another wireless AP. Click [Search] to search and select the AP you want to connect to.
Select a passphrase type, and be sure to enter the correct passphrase required by the AP you want to connect to. Press [Save] to apply the changes. A.bc1 will reboot immediately.

*** Note ***

The wireless connection does not support static IP settings. The AP to which you want to connect must be providing DHCP service.

### 2.6.2 Authentication

Set the authentication conditions and facial recognition action conditions for A.bc1.



Authentication

Tempic ☑

Expires in 8 hour

Rule

Local Authentication

Detect Threshold

0.5

Matching Threshold

5.0

Matching Timeout

2.0

Liveness Check

None

Speed Gate □

Mask Detection □

QR Code □

Bio Card ☑

- **Setup > Authentication > TEMPIC:**

The TEMPIC feature is ANDOPEN's unique patented technology for ease of use. TEMPIC means 'Temporary Picture' and is a feature that allows users to successfully authenticate their face with a biometric card for the first time, and then authenticate without a biometric card for a set period of time.

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

Click [Save] to apply the changes.

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

**▶ How it works**

① With TEMPIC 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 A.bc1's volatile memory.

② After that, when the user is close to A.bc1, the face authentication result is derived by comparing the face information temporarily stored in A.bc1 without the need for a biometric card.
(TEMPIC authentication requires a strict face authentication accuracy of 100 times higher than biometric card authentication to maintain security. Therefore, the authentication time may be slightly longer than biometric card authentication).

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

④ When A.bc1 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 A.bc1 is hijacked, it will be volatilized when power is cut off.

*** Note ***

In order not to break access security policy, the face information temporarily stored for TEMPIC function is only stored on the A.bc1 device that presses the 'Attendance' button and successfully authenticates.
Therefore, the TEMPIC function only works on the first A.bc1 device that has been 'Attendance' and does not automatically synchronize with all A.bc1s in the building.
In order to synchronize to all A.bc1s installed in the building, ANDOPEN's access control system, ADMS (ANDOPEN Device Managing System), must be installed, and the ADMS and the building's A.bc1 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.

• Bypass: This method compares the face embedded in the biometric card with the face of the authentication requestor taken by A.bc1 and judges the authentication as successful if they match.
This method is recommended when A.bc1 is operated in conjunction with an external access control panel.

• 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 A.bc1 are matched, and if the card number of the used biometric card matches a card number in the user DB stored in A.bc1, then the authentication is judged as successful.

This method is recommended if you operate a method that allows A.bc1 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.

Please press [Save] to apply the changes.

### • etup > 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 0.6.**

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 TEMPIC 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 3, max 20**

Higher values require higher similarity to pass authentication. For reference, a value increase of ‘1’ requires about 10 times the similarity.
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 5.0 and 6.0. The factory default value is 5.0.**

*** 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.

- **Settup> Authentication > Matching Timeout:**

Set the number of seconds to retry facial recognition.

This is the longest amount of time to attempt facial recognition for A.bc1 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 stealing an authorized user's biometric card, photographing the user's face, and displaying it on a display such as a phone or tablet.

In the current version of AOS, you can select one of four levels: None, Low, Normal, and High, and the detection sensitivity is applied in the order of High < Normal < Low, meaning that High detects fraudulent authentication with the most stringent criteria.

**The factory default value is None.**

Click [Save] to apply the changes

***Note**

When this feature is enabled, the time required for face authentication is slightly longer than when it is disabled.

- **Setup > Authentication > Speed Gate:**

A.bc1 uses a constant pause between authentication and authorization to reduce unnecessary nested authentication. Enabling this setting minimizes the pause and allows continuous authentication attempts to make A.bc1 suitable for use with Speed Gate. Press [Save] to apply the changes.

- **Setup > Authentication > Mask Detection:**

This feature is designed to encourage people to wear a mask, when activated, it detects whether you are wearing a mask.
If it is determined that you are not wearing a mask, A.bc1 plays ‘Please wear a mask’ voice message.
When this feature is enabled, the authentication time may be relatively long.
Press [Save] to apply the changes.

- **Setup > Authentication > QR Code:**

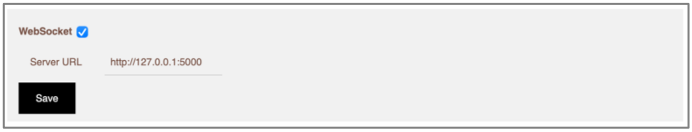
Enable if you are using ANDOPNE's QR authentication cloud service.
If you want to use QR authentication, please contact ANDOPEN.
If you do not use QR authentication, please keep it inactive to prevent unnecessary waste of system resources. Click [Save] to apply the changes.

- **Setup > Authentication > Bio Card:**

This tab is for settings that bypass facial recognition and only attempt card authentication for special purposes, such as frequent conferences, large numbers of visitors, etc.
When disabled, A.bc1 will bypass facial recognition for all authentication attempts and derive authentication success/failure based on card authentication alone.
Press [Save] to apply the changes.

## 2.6.3 Application Programming Interface (API)

If you need to network ANDOPEN's access control system, ADMS, or a third-party access control system with AOS API, please enable this API WebSocket and designate the Server URL. Please contact ANDOPEN for API integration.



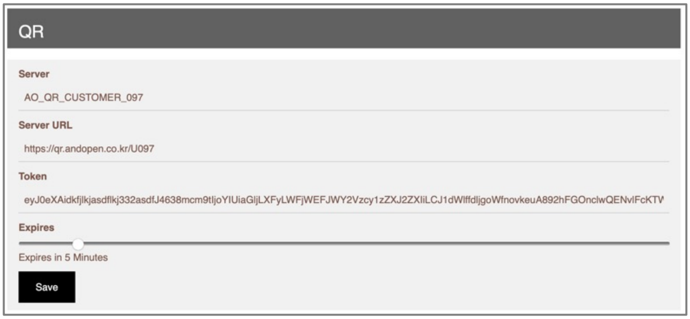
WebSocket ☑

Server URL http://127.0.0.1:5000

## 2.6.4 QR

AA.bc1 supports QR code authentication access.
To use QR code authentication, you need to subscribe to ANDOPEN QR authentication cloud service. This tab is for customers who use QR authentication cloud service only.

ANDOPEN QR Code Authentication can increase the security of the QR Code authentication method by setting the active time of the user's QR Code, such as the one-time password method.
Enter the correct server and certificate information that ANDOPEN provides to each customer, and adjust the Expire time to match your organization's access policy.



Server
AO_QR_CUSTOMER_097

Server URL
https://qr.andopen.co.kr/U097

Token
eyJ0eXAidkfjlkjasdflkj332asdfJ4638mcm9tljoYIUiaGljLXFyLWFjWEFJWY2Vzcy1zZXJ2ZXIiLCJ1dWlffdljgoWfnovkeuA892hFGOnclwQENvIFcKTV

Expires
Expires in 5 Minutes

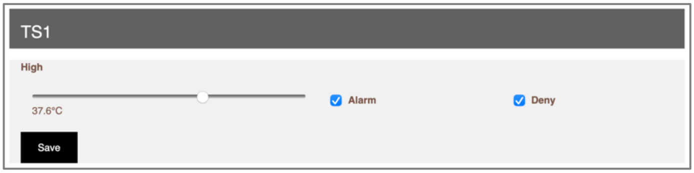
For more information about this QR authentication service, please contact ANDOPEN's sales representative.

## 2.6.5 TS1

This is the section to set when using the temperature detection function of Abc-TS1.
Use the slide bar to set the temperature you want to consider as a high fever.
Check 'Alarm' to sound an alarm when the body temperature is detected above the set value. Check 'Deny' to deny authentication if the temperature is detected above the set value.
If both are checked and a high temperature is detected, an alarm is raised and access is not allowed.

If both are unchecked, the temperature information is ignored, leaving only a log.

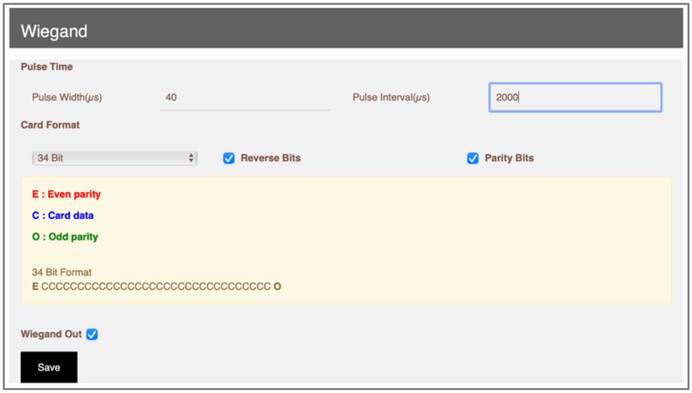
Set these settings to match your organization's access policies.



High
37.6°C
☑ Alarm
☑ Deny

## 2.6.6 Wiegand

If A.bc1 interfaces with an external access control panel via Wiegand communication, adjust the Wiegand communication format.



Wiegand

Pulse Time

Pulse Width(μs) 40

Pulse Interval(μs) 2000

Card Format

34 Bit

☑ Reverse Bits

☑ Parity Bits

E : Even parity

C : Card data

O : Odd parity

34 Bit Format
E CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC O

Wiegand Out ☑

- **Setup > Wiegand > Pulse Time:**

Adjust the length and interval of the 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 note 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 data format of the card number transmitted by Wiegand communication.

- **34bit:** Adjusts the serial number data length to 34 bits.
- **24bit:** Adjusts the total length of the serial number data to 24 bits.
- **Reverse Bits:** If checked, sends each bit of the serial number data in the reverse order of in reverse order.
- **Parity Bits:** If checked, the data will be sent with an Even Parity bit at the beginning and an Odd Parity bit at the end.

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 :**

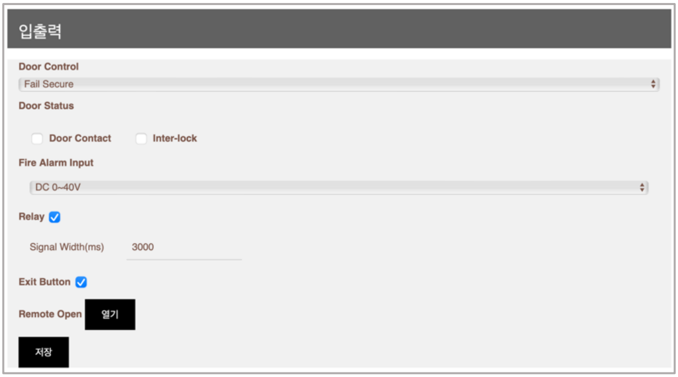
Determines whether the user's card number data should be sent out over Wiegand communication when authentication is successful.

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

Press [Save] to apply the changes.

## 2.6.7 I/O

AProvides 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 A.bc1.



입출력

Door Control: Fail Secure

Door Status

□ Door Contact □ Inter-lock

Fire Alarm Input: DC 0~40V

Relay ☑

Signal Width(ms) 3000

Exit Button ☑

Remote Open

- ## Setup > I/O > Door Control:

If A.bc1 directly controls the door's lock, this determines the condition for controlling the lock (Fail) when A.bc1 is invalidated by failure or vandalism. This function is invalid if the access control panel controls the door's lock device.

- **General:** The relay on A.bc1 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.

- **Fail-Safe:** Keep the door open in A.bc1 Fail condition.
(Connect the open terminal of the Lock device with COM - NC of the A.bc1 Relay).

- **Fail-Secure:** Keeps the door locked in the A.bc1 Fail condition.
(Connect the open terminal of the Lock device with the COM - NO of the A.bc1 Relay).

**The factory default value 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 ***
Door control policy should be based on the legal standards in your region. Make sure that your policy is appropriate for the legal standards in your region.

- ## Setup > I/O > Door Status:

Receives door open/close status information from door contact and decides whether to apply it to the operation of the lock device.

When the **door contact** feature is enabled by check, A.bc1 catches the status of the door and keeps unlocking.

When the **Inter-Lock** feature is enabled by check and each door contact of adjoined two doors is connected with A.bc1, prevents making situation two doors open at the same time.

Press [Save] to apply the changes.

- **Setup > I/O > Fire Alarm Input :**

This feature is set when a fire signal generator is connected to A.bc1. When A.bc1 receives a fire input, it flashes the front LED and sounds an alarm, stops all authentication, and attempts to open the door. If A.bc1 is controlling the door, it will open and hold the door open. If the door is controlled by an access control panel, A.bc1 can send a fire signal to the access control panel. In this case, the opening of the door depends on the settings of the access control panel.

- **None**: Do not receive fire signals.

- **Dry Contact**: 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 servers.

- **DC 0 ~ 40V**: Use this setting when connecting with a fire alarm generator that sends a DC power signal as a fire signal. Mainly used when connecting directly to a fire receiver.

Depending on the selection of Dry Contact and DC0 to 40V, the physical wiring is different. Refer to the A.bc1 product documentation for wiring information.

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 A.bc1 that controls the door.

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

If A.bc1 does not control the door directly (an external access control panel controls the door), please uncheck to disable the Relay operation for reducing the unnecessary operation of the Relay.

Press [Save] to apply the changes

*** Note ***

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

### • Setup > I/O > Release Fire Alarm:

Stop the fire alarm and return to normal status.
When the fire situation is over, check Release Fire Alarm and press [Save] to return A.bc1 to normal operation.

### • Setup > I/O > Relay > Signal Width(ms):

Specifies the amount of time that the relay operates while it is active.

In a configuration where A.bc1 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 the door is controlled by an access control panel, the open time of the door is determined by the open time setting of the access control panel, and this setting is meaningless.
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), or 3 seconds.**

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 A.bc1 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 negate malicious opening attempts, you can use this setting to negate the open signal which is coming from the exit button I/O of A.bc1.

- **Receive a signal** if **there is a** check (Exit Button works)
- If there **is no** check, **ignore the signal.**

Press [Save] to apply your changes

### • Setup > I/O > Remote Open :

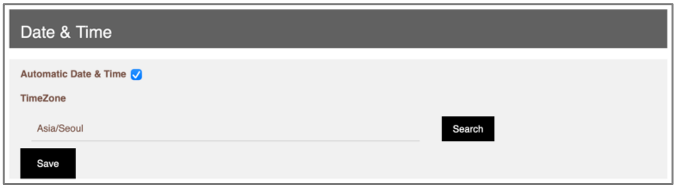
Temporarily open the door through the AOS.

When the [Open] button is pressed, the Relay in A.bc1 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).

## 2.6.8 Date & Time

A.bc1 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.



Date & Time

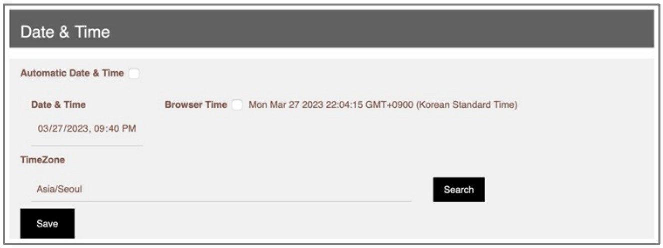
Automatic Date & Time ☑

TimeZone

Asia/Seoul

- **Settings > Date & Time > Automatic Date & Time:**

If A.bc1 is connected to the Internet, click the checkbox to enable this feature to automatically update the Internet Time (UTC) to the reference time of A.bc1's built-in clock on a regular basis.



Date & Time

Automatic Date & Time □

Date & Time

03/27/2023, 09:40 PM

Browser Time □ Mon Mar 27 2023 22:04:15 GMT+0900 (Korean Standard Time)

TimeZone

Asia/Seoul

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 menu to set the calendar and time in the following order, year, month, day, AM/PM, hour, and minute.

Alternatively, for convenient time setting, you can easily set the built-in clock in A.bc1 to the current time by getting the browser time of the PC connected to AOS. (Check the 'Browser time' checkbox and click [Save])

Press [Save] to apply the changes

*** Note***

If you set the clock on A.bc1 manually, the time will become inaccurate over time. Therefore, we recommend that you enable automatic time renewal to automatically revise the time information if an internet connection is available. Otherwise, periodic manual time resets are required using the method described.

### • Settings > Date & Time > Time Zone

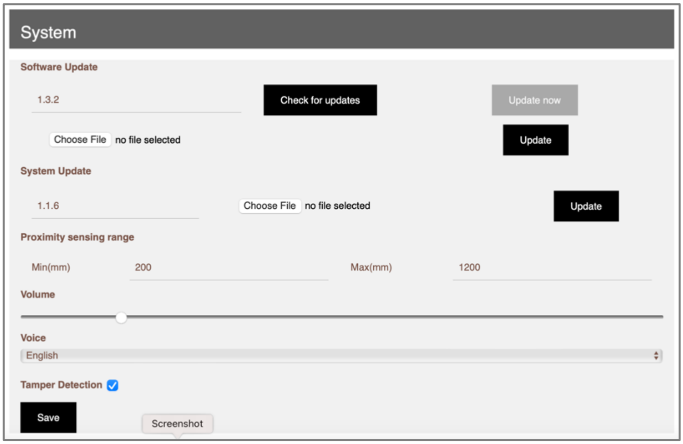
When Automatic time update is enabled (checked), the time fetched from the internet is UTC+0, i.e. Greenwich Observatory time. You need to apply your local time difference to this time to convert it to your local time.

Click the [Lookup] button to select the region where A.bc1 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.

Click [Save] to apply the changes

## 2.6.9 시스템

This tab is primarily for setting operational elements where changes are common to all operations in A.bc1. Set the software update, the range of motion of the user proximity sensor, the volume of the voice prompts, the language of the voice prompts, and the operation of the detachment detection sensor.



System

Software Update

1.3.2

no file selected

System Update

1.1.6

no file selected

Proximity sensing range

Min(mm) 200

Max(mm) 1200

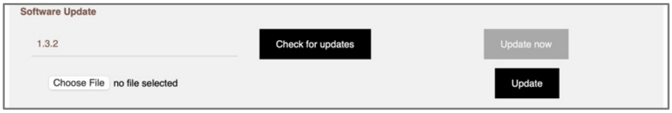
Volume

Voice: English

Tamper Detection ☑

### • Setup > System > Software Update:

You can check and update the currently installed version of AOS.



Software Update

1.3.2

no file selected

AYou can update AOS using ANDOPEN's update cloud or from a file. If AOS is connected to the internet, you can click [Check for updates] to see if a new version is available for update. If you want to update to the new version, you can click [Update Now] to update immediately.

Alternatively, you can download the new version of AOS from ANDOPEN's homepage. After downloading the new version to the PC connected to A.bc1, you can manually update it by pressing [Select File] to select the file and pressing [Update].

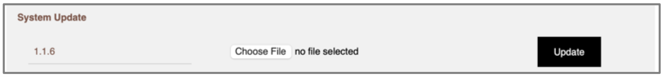
If the update is completed successfully, A.bc1 will reboot automatically.

***Caution***

Do not turn off A.bc1 while updating the software. The software may become corrupted and A.bc1 may be in malfunction as well as you may not be able to access A.bc1 again. Also, be sure to carefully read the Readme file included with the software download and check the compatible System SW version described below to ensure you follow the instructions to perform the update correctly.

- **Setup > System > System Update:**

You can check and update the version of System SW, which manages the main input and output of A.bc1.



System Update

1.1.6

You can download the new version of System SW from the ANDOPEN homepage to the PC connected to A.bc1, select the file by pressing [Choose File] and update it manually by pressing [Update].

***Caution***

Do not turn off A.bc1 while updating the System SW.
It may damage the system and cause A.bc1 to operate abnormally, which may be irreversible.
Also, be sure to carefully read the Readme file included with the System SW download and check the compatible AOS software version to perform the update correctly according to the instructions.

- **Setup > System > Proximity sensing range:**

Set the detection range of the sensor to detect the proximity of a user. When a user is in the range of sensing, A.bc1 start the authentication process. You can set the range by checking Proximity sensing to enable it and entering the setting value.

**Setting range: min 0 to max 1200 (in mm)**

If the user is too close or too far away, face recognition performance decreases, and if A.bc1 is installed in a narrow corridor, it may detect passersby and cause unnecessary maneuvers, so please set the appropriate value according to the installation environment.

**The factory default is 800 mm.**

For reference, the distance between the device and the user with the best facial recognition performance is approx. 60 cm (600 mm).

Press [Save] to apply the changes

- **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 apply your changes

- **Setup > System > Voice:**

Set the language of the guidance voice. Click Language to set the desired language of the greeting voice from the pull-down menu that appears.
Currently, AOS supports silence and three languages: Korean, English, and Chinese.
The default is set differently depending on the country your product is released in.

Press [Save] to apply your changes

- **Setup > System > Tamper Detection:**

Select whether to enable/disable the tamper detection sensor to prevent and monitor unauthorized removal of the installed A.bc1. The A.bc1 is a wall-mounted access control device, so it is an abnormal situation if the A.bc1 is removed from the wall for no particular reason after installation.

If you enable this feature by checking Tamper Detection, if the device is dislodged from the wall during operation (with power applied), an alarm sounds and an emergency indication is displayed on the LED on the front of the device, and the authentication function is invalidated.
If the tamper detection function is disabled, the device cannot detect whether it is detached.

When the device is reattached, it returns to normal operation.

The default value is Enabled.

Press [Save] to apply the changes

*** Caution ***
To prevent malicious device access, we recommend that you keep the tamper protection feature active.

# 2.7 Logs

The Logs menu is a page where you can view records that allow you to track and observe user authentication results, the operation of A.bc1 and AOS, the administrator usage history of AOS, and more (this set of records is called "logs").

The logs that can be viewed are

- Authentication logs: Records of authentication events (up to 2 million)
- System logs: Event records of A.bc1 and AOS (up to 1 million)
- Admin Usage logs: AOS usage records of Administrator (up to 1 million)

and you can navigate to that submenu by pressing the right triangle on the log menu.

## 2.7.1 Authentication logs

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 [Lookup] button to view user authentication results.

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

- Authentication time
- UID: The unique number stored on the biometric card that attempted to authenticate.
- Card number: The card number of the biometric card that attempted to authenticate.
- Name: The username stored on the biometric card that attempted to authenticate.
- 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.
- Score: Shows the score (similarity) derived by the face recognition algorithm
Example.) Score 5.5: The probability that the authentication result is wrong is 1/500,000
- Body temperature: For A.bc-TS1, measured body temperature information.
- Time &Attendance information: If the user pressed the T&A button and authenticated, displays the corresponding time and attendance information. If the user did not press the button and button and authenticated, it will be displayed as ‘-’.

The buttons and user interface of [Show currency], [Copy], [Export to CSV], [Export to Excel], [Print], [1...2], Lookup, Previous, Next, etc. are the same as the corresponding functions described in "2.1.1 User > General".

### 2.7.2 System logs

This is the page where you can view the operation event history of A.bc1 and AOS.

You can set the lookup period the same as the method in "2.6.1 Log > Authentication logs" and click the [Lookup] button to search the operation log for the desired period.

The following information is displayed as a result of the lookup

- Time of occurrence: When the operation (event) happened
- Description: Description of the operation(event)

The types of functions that are looked at are booting of A.bc1, AOS startup, alarms, doors opened, and critical errors.

### 2.7.3 Administrator Usage Logs

This page allows administrators to view a history of significant actions taken in AOS.

You can set the lookup period as the same as the method in "2.6.1 Log > Authentication logs" and click the [Lookup] button to search the actions performed by the administrator for the desired period.

The following information is displayed as a result of the lookup.

- Time it happened: When the action was performed
- Admin ID: The admin account that performed the action.
- Description: A description of the action taken

The kinds of things you'll see include login and logout history, whether you've added or removed administrators, and whether you've made changes that have a major impact on the operation of A.bc1 and AOS.

## 2.8 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 or impacting 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 customer 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 (de-energized 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 (Ethernet):** 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 A.bc1 to external devices. The format of I/O signals varies depending on their purpose.

- **IP65:** A level of International Protection Marking that defines the degree to which a device is protected against water and dust. The first number indicates the degree of dust protection and the second number indicates the degree of water protection. IP65 means 'completely dustproof and protected against water from all directions'.

- **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. A.bc1 is also illuminated with infrared light.

- **PoE:** Short for Power on Ethernet, it refers to a technology that allows you to power network devices over an Ethernet cable. You can use this technology by connecting a PoE-enabled network hub and a PoE-enabled network device with an Ethernet cable.
A.bc1 supports PoE, so when you connect it to a PoE network hub with an Ethernet cable, you can apply power without a separate power supply. The power transmission performance of PoE depends on the performance of the PoE network hub and the length of the Ethernet cable and the quality of the cable. The longer the cable and the poorer the quality of the cable, the more power is lost. We generally recommend a maximum length of less than 50 meters when using Cat5e-compliant cables.

- **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 A.bc1, 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 (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 A.bc1, 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 A.bc1 component includes a dedicated ferrite core.

# ANDOPEN

**ANDOPEN Co., Ltd. :**
BIOMETRICS SOLUTION PROVIDER

46, Dalae-ne-ro, Sujeong-gu, Seongnam-si, Gyeonggi-do, South Korea
Seongnam Global Convergence Center Building A, Room 506

TEL : +82 31 608 0010
FAX : +82 504 374 9019

www.andopen.co.kr
www.youtube.com/andopen

# AuténID

## Authentic Identity

ID CARD & BIOMETRICS CONVERGED SOLUTION

**AND**OPEN