동아아이티시스템(주)

주 소 대구광역시 서구 평리1동 1053-2번지 2층
홈페이지 WWW.DONGAIT.CO.KR
고객센터 053-554-1919
팩 스 053-556-1919

D-Station

듀얼지문인식 & 얼굴인식 출입근태단말기

사용설명서

Ver 1.0

목차

목차

목차

1장. 알아두기

1.1 제품 특징

세계 최초로 1,600만 컬러의 5.0인치 대형컬러 LCD와 18비트 고품질 사운드를 적용하여 각종 멀티미디어 정보를 실시간으로 제공합니다.

Tri CPU를 적용하여 10,000개의 지문인식정보를 1초 내에 검색 가능한 세계 최고의 지문인식속도를 갖고 있습니다. 또한, 200,000개의 지문인식정보와 1,000,000개의 로그를 저장할 수 있는 세계 최대의 용량을 가지고있습니다.

Wi-Fi 무선랜을 장착하고 있어, 유선 연결 없이도 PC에서 출입 및 근태기록을 실시간으로 확인할 수 있습니다. (선택사양)

USB 메모리를 이용해 등록된 지문인식정보나 출입 및 근태기록을 다른 D-Station으로 손쉽게 전달할 수 있습니다.

세계적으로 가장 신뢰성있는 솔루션으로 인식률, 인식속도, 메모리 효율에서 성능을 입증받은 핵심 알고리즘 기술을 자랑합니다.

RF 카드 기능이 탑재되어 지문, 카드, 비밀번호, 얼굴 퓨전 네 가지 인증수단을 사용자 별로선택하여 적용할 수 있습니다. (선택사양)

1.2 기본 용어 정리

- 관리자

사용자를 등록하고 삭제하는 등의 사용자정보를 관리하고, 단말기의 각종 설정값을 바꿀 수 있는 권한을 가진 사람입니다. 사용자 중에 관리자의 권한을 가지고 있거나 단말기 비밀번호를 알고 있으면 단말기에 대한 모든 기능을 관리할 수 있습니다.

- 1:1 인증

ID 를 먼저 입력하고 해당ID에 대한 비밀번호나 지문을 입력하여 저장되어 있는 정보와 새로 입력된정보를 1:1로 비교하는 방식입니다.

- 1:N 인식

ID 를 입력하지 않은상태에서 지문만을 입력해 저장되어 있는 모든 지문 중에서 새로 입력된 지문을검색하는 방식입니다.

- 지문등록

지문센서로부터 취득된 지문영상으로부터 각 지문들의 고유한 특징인 지문인식정보를 추출하여 데이터베이스로 저장하는 과정입니다. 지문등록과정에서 저장된 지문인식정보는 계속 사용되므로 이과정에서 올바르게 지문을 입력했는가의 여부가 지문인식성능에 매우 큰 영향을 줍니다.

1장. 알아두기

1.3 안전을 위한 주의사항

사용자의 안전과 재산상의 손해 등을 막기위한 내용입니다. 반드시 읽고 올바르게 사용해주세요.

직사광선 또는 습기나 먼지, 그을음이 많은 장소에 설치하지 마세요.

제품 옆에 자석과 같은 물체를 두지마세요. 자석, CRT, TV, 모니터, 스피커 등 자성이 강한 물체에 의해 손상될 수 있습니다.

전열기구를 근처에 두지 마세요.

단말기 내부에 물, 음료수, 약품 등의 액체가 들어가지 않도록 조심하세요.

단말기에 오랫동안 먼지가 쌓이지 않도록 자주 청소해 주세요.

청소시 제품에 물을 뿌리지 마시고 부드러운 헝겊이나 수건으로 닦아주세요.

- 지문 입력부에 먼지나 이물질이 많은 경우 마른 수건을 이용하여 표면을 깨끗하게 닦아주세요. 세척제, 휘발유, 시너 등으로 지문입력부를 닦으면 표면이 손상되어 지문입력이 잘되지 않을 수 있으

제품을 떨어뜨리거나 강한 충격을 주지마세요.

터치스크린에 강한 자극을 주지 마세요

임의로 분해, 수리, 개조하지 마세요.

어린이들이 함부로 기기를 만지지 못하게 하세요.

다른 용도로 사용하지 마세요.

기기고장이나 기타 문제 발생시 우선 A/S 연락처에 문의하세요.

1장. 알아두기

1.4 지문인식의 기초

지문인식이란

지문은 개인의 고유한 생체정보로서, 일생동안 변하지 않는 특성을 가지고 있습니다. 지문인식은 이러한 지문정보를 이용하여 개인에 대한 인증 및 개인간의 차이를 식별할 수 있는 기술입니다.

비밀번호나 카드 등에서 발생할 수 있는 분실, 도용 등의 위험이 없으며, 신뢰성이 뛰어나고, 편의성 또한 높아, 차세대 보안기술로 다양한 응용분야에서 활용되고 있습니다.

지문인식 과정

1. 지문은 표피면에서 위로 돌출되어 있는 융선(ridge)과 융선 사이의 공간인 골(valley)로 구성되어 있습니다. 개인별로 지문의 융선과 골의 패턴이 각기 다르며, 이러한 패턴의 고유성 및 차별성을 이용하여 지문인식이 이루어집니다.
2. 지문센서는 입력된 손가락으로부터 융선을 감지하여 이를 2차원의 지문영상을 얻는역할을 합니다. 지문센서는 그 원리에 따라서 광학식, 반도체식, 스캔식 등 다양한 종류로 나누어집니다.
3. 지문영상으로부터 지문의 특징을 가려내는 과정을 거쳐 지문인식정보가 생성됩니다. 지문인식정보는 수백 바이트 용량의 데이터로서 이 정보가 단말기의 데이터베이스에 저장되어 추후의 인증과정에 사용됩니다.

참고) 개인 생체정보 보호

슈프리마의 지문인식 제품은 어떠한 경우에도 개인의 고유생체정보인 지문영상을 저장하지 않도록 설계되어, 만일에 일어날 수 있는 유출사고에 대비할 수 있습니다.

올바른 지문인식 방법

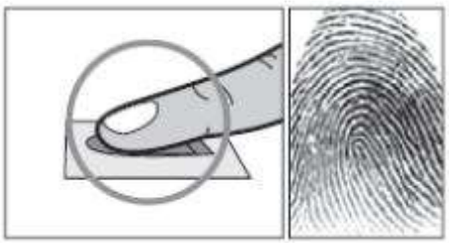
1. 지문 입력을 위한 손가락 선택

- 사용할 손가락은 주로 쓰는 손의 검지 또는 중지의 사용을 권합니다.
- 엄지, 약지, 소지는 센서에 입력하는 자세가 불안정하여 정확히 중앙에 위치하기가 상대적으로 어렵습니다.

1장. 알아두기

2. 지문을 센서에 올바르게 입력하는 방법

- 손가락이 센서를 완전히 덮어 접촉되는 면적이 많도록 깊숙이 위치시킵니다.
- 가급적 특징점이 많은 지문중심점(Core) 부분을 센서의 중앙에 댑니다.
- 지문의 중심점은 지문의 융선이 회전하여 모이는 봉우리 부분으로 대개 손톱의 아래쪽 반달모양의 반대편에 위치합니다.
- 많은 사용자들이 손가락의 위쪽 끝부분만을 대는 경향이 많은데, 손톱의 아래쪽 반달부분이 센서중앙에 위치하도록 손가락을 댑니다.
- 센서를 찍어 누르듯이 손가락을 세워서 대면 손 끝부분의 지문만 입력되므로 정상적인 등록이나 인증이 되지 않습니다.



3. 손가락 상태에 따른 대처방안

- 슈프리마의 지문인식제품은 계절의 변화나 손가락의 상태 변화에 상관없이 지문입력이 잘되도록 설계되어 있습니다. 하지만 외부 영향에 따라 지문입력이 어려울 경우 다음 사항을 참고하시기 바랍니다.
- 손가락에 땀이나 물이 묻어있는 경우, 물기를 닦은 후 입력합니다.
- 손가락에 먼지 등의 물질이 묻어있는 경우, 잘 닦거나 털어내고 입력합니다.
- 손가락이 너무 건조하여 입력이 안 될경우, 손 끝에 입김을 불고 입력합니다.

4. 지문 입력시 권고사항

- 지문인식에서 등록과정이 매우 중요합니다. 따라서, 처음에 지문을 등록할 때는 신중을 기해 올바르게 지문을 입력하도록 합니다.
- 인식률이 떨어질 경우 다음과 같은 조치를 권장합니다.
- 등록된 지문을 지우고 다시 등록합니다.
- 같은 지문을 추가로 등록합니다.
- 상처 등으로 입력이 어려운 손가락이 있을 때에는 다른 손가락을 등록합니다.
- 손에 짐을 들거나 손가락에 상처가 나는 경우 등, 등록된 지문의 사용이 어려운 경우를 대비하여 사용자당 두 개 이상의 손가락을 등록해서 사용할 수 있습니다.

1장. 알아두기

1.5 얼굴 인식

얼굴은 지문 또는 홍채와 더불어 가장 널리 쓰이는 바이오 정보입니다. 얼굴 인식 기술은 얼굴의 특징적인 정보를 추출하여 사람을 자동으로 식별하는 기술입니다. 이러한 얼굴 인식 기술은 지문이나 홍채 인식 기술과 다르며, 간접적인 방법으로 얼굴 정보를 획득할 수 있고, 그 획득 환경이 다른 바이오 정보에 비해 제한적이지 않다는 장점을 가집니다.

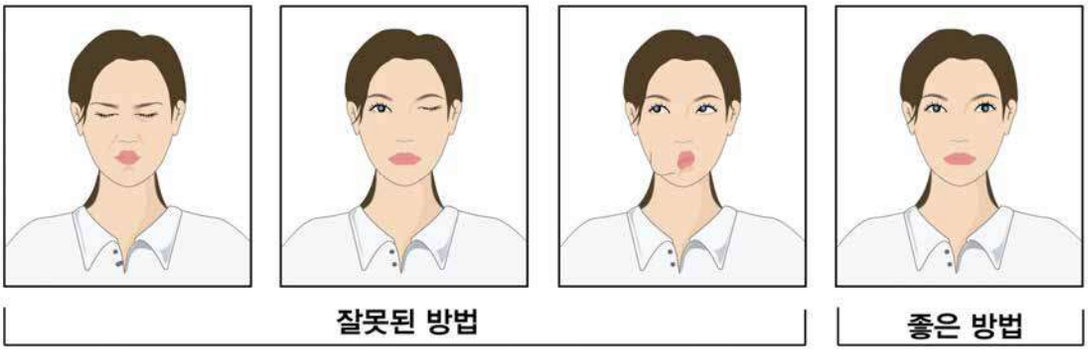
얼굴 인식 절차

1. 얼굴은 다양한 얼굴 특징 요소들로 이루어지며, 이러한 특징 요소들과 선천적인 형태는 다양한 인자들에 대해 영향을 변화가 적기 때문에, 개개인을 구분하기에 좋은 정보가 됩니다. 얼굴 인식은 이러한 개인별 고유의 특징 요소들을 이용해 인물을 식별하게 됩니다.
2. 얼굴 센서는 디지털 영상이나 연속적인 비디오 프레임 형태로 영상을 만들어 냅니다. 얼굴 검출을 위해서 다양한 형태의 광원 (직사광선, 적외선)들이 사용됩니다.
3. 얼굴 검출 과정을 통해, 촬영된 영상 중에 얼굴 영역을 찾아내고, 검출된 얼굴 영역에서 얼굴 특징 정보를 추출합니다. 추출된 정보는 터미널의 데이터베이스에 저장되고, 개인의 식별을 위해 사용됩니다.

얼굴 인식 방법

1. 아래의 설명를 참고하여 정확한 방법으로 얼굴을 입력합니다.

- 얼굴 센서를 응시하고, 화면에 보이는 얼굴이 영상의 중앙에 위치하도록 합니다.
- ID용 사진과 같이 정면 얼굴 모습이 입력되어야 합니다.
- 얼굴 센서와 얼굴 사이의 거리를 조절하여 영상 획득시 전체 얼굴이 포함되도록 합니다.
- 본 제품은 안정적으로 얼굴 정보를 획득하는데 최소의 시간이 필요하며, 얼굴 입력 시에는 급작스럽게 고개를 돌리지 말고 안정적인 상태를 유지하여 줍니다.
- 얼굴 인식을 위한 얼굴의 특징 정보들은 표정의 변화(웃기, 울기, 윙크 등)에 따라 심하게 변형이 될 수 있으니, 얼굴 입력 시에는 평상시 표정으로 일정하게 유지해야 합니다.



1장. 알아두기

2. 권고 사항

- 정확한 얼굴 인식을 위해 얼굴을 올바로 등록하는 것이 매우 중요합니다. 얼굴 등록 과정에서 적절하게 얼굴을 입력하도록 주의를 기울여 주시기 바랍니다.
- 얼굴 정보는 주변 조명 변화에 의해 심하게 영향을 받을 수 있으므로, 제품이 설치되어 실제 사용할 장소에서 얼굴을 등록하는 것을 추천 드립니다.

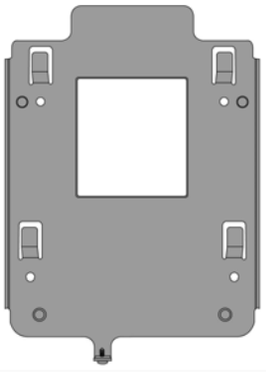
2장. 설치하기

2.1 제품구성품

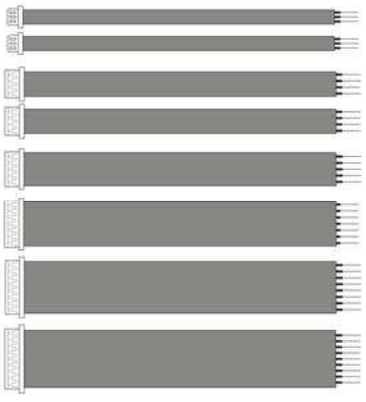
제품 패키지 박스에 다음과 같은 구성 물품이 모두 들어 있는지 확인하시기 바랍니다. 내용물에 이상이 있을 경우, 제품을 구입하신 곳에 문의하시기 바랍니다.

기본 구성품

D-Station 본체



벽면 고정 브라켓



케이블(8종류)

USB 케이블

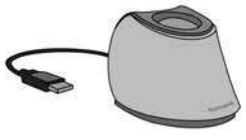
나사와 홀더(각 4개씩)

12V 전원어댑터

소프트웨어 CD

별매품

플라스틱 스탠드



USB 지문스캐너

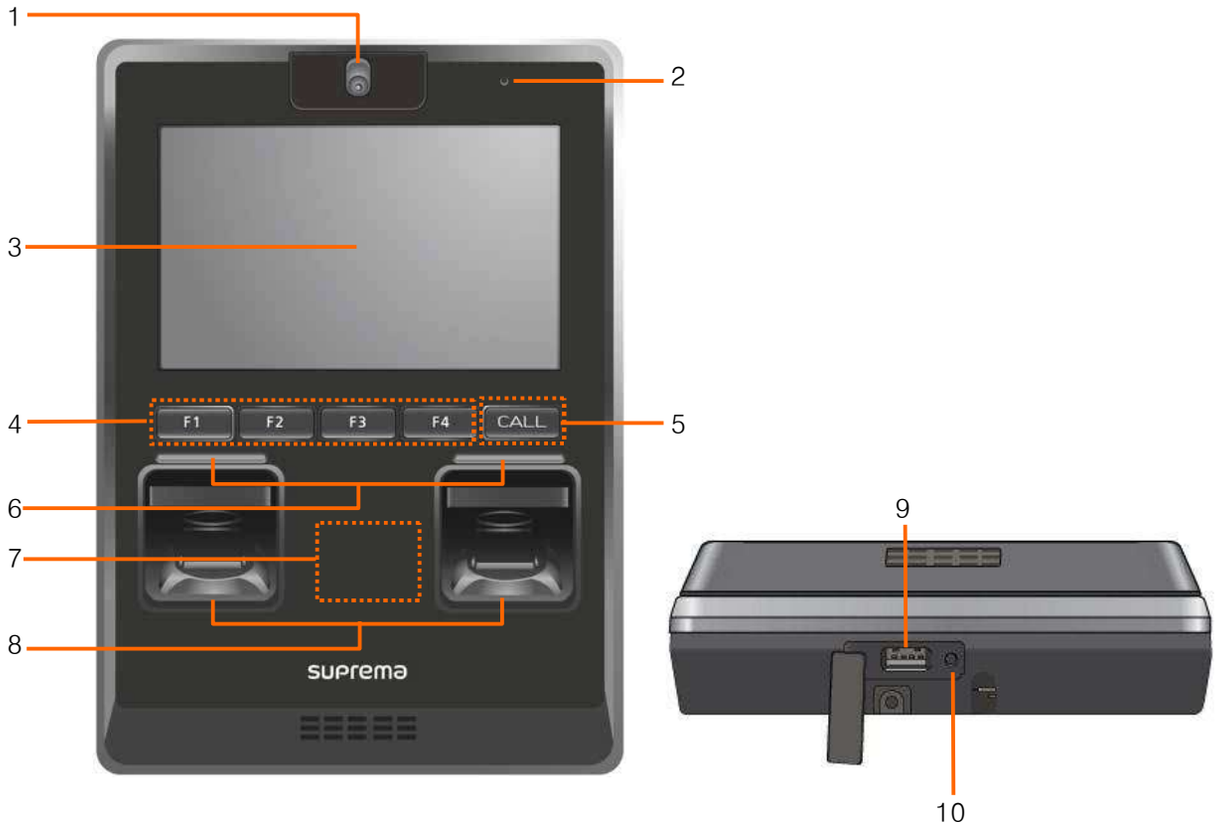
무선랜 Access Point

2장. 설치하기

2.2 각 부분의 명칭과 기능

제품 정면/ 밑면

D-Station 각 부분의 명칭과 기능을 설명합니다.

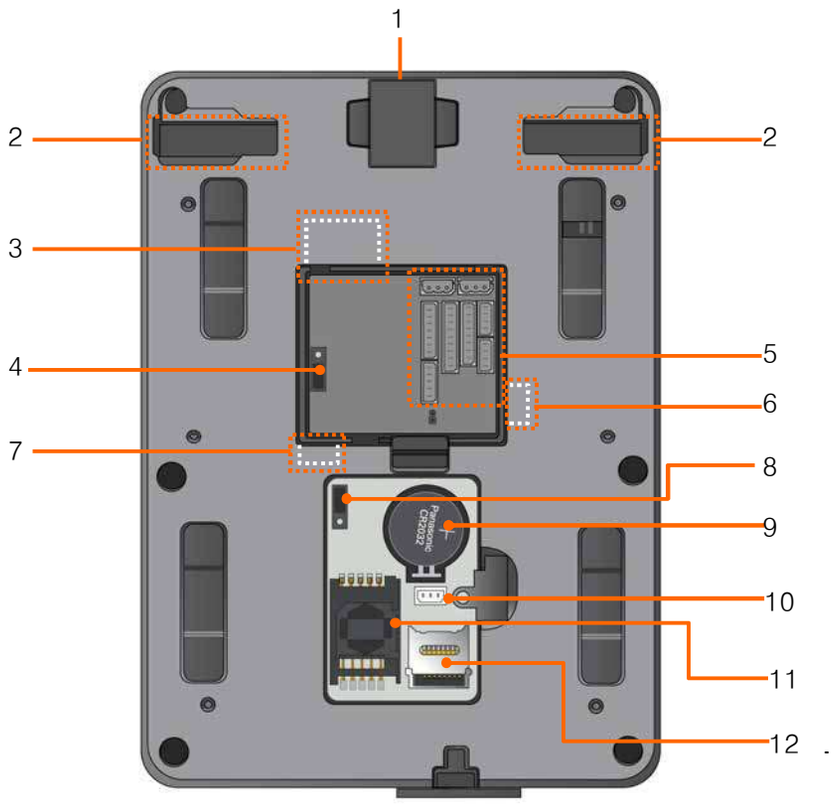


번호	명 칭	기 능
1	카메라	얼굴 인식 또는 비디오폰 통화 시 사용합니다.
2	마이크	비디오폰 통화시 이곳에 대고 말합니다.
3	LCD 화면	현재상태(근태모드, 공지사항 등) 와 시간을 표시해 줍니다.
4	F1~F4	기능키를 근태기능키로 사용합니다.
5	CALL	비디오폰이 연결되어 있을 때 호출버튼으로 사용합니다.

번호	명 칭	기 능
6	상태표시 LED	전원 공급: 파란색 LED 점등 지문 입력 대기: 파란색 LED 점멸
7	카드 인식부	RF 카드를 인식하는 부분입니다.
8	지문 인식부	지문 입력시 이곳에 손가락을 댑니다.
9	PC USB 케이블 단자	USB 케이블로 PC 를 연결하거나 USB 메모리를 연결합니다..
10	리셋버튼	단말기를 재시작합니다.

2장. 설치하기

제품 뒷면



번호	명 칭	기 능
1	카메라 위치 조정 레버	카메라 위치조정을 하기 위한 곳입니다.
2	USB 삽입부	USB WLAN 을 연결합니다..
3	이더넷 케이블 단자 (RJ45)	이더넷 케이블을 연결합니다.
4	전원선택 점퍼	– POE IN: POE(Power Over Ethernet) 방식으로 UTP 케이블을 통해 전원을 공급받음 – DC IN: 전원 어댑터로 공급받음 (디폴트값은 DC IN 입니다.)

번호	명 칭	기 능
7	전원 연결부	12V 전원 어댑터를 연결합니다.
8	동작 모드 선택 점퍼	NORMAL 또는 ADMIN MODE 를 선택 하기 위한 점퍼입니다. ADMIN MODE 는 유지보수를 위한 모드이므로, 정상적인 동작을 위해서는 반드시 NORMAL 모드로 설정이 되어야 합니다.(디폴트 값은 NORMAL 입니다.)
9	RTC Battery	RTC(Real Time Clock) 배터리 (시간 유지용 배터리)
10	Debug	유지보수를 위한 디버그 포트입니다.

2장. 설치하기

5	케이블 커넥터	각종 케이블을 연결합니다. '2.2' 케이블 사양 참조
6	SW3	RS485 종단 방식 선택 스위치

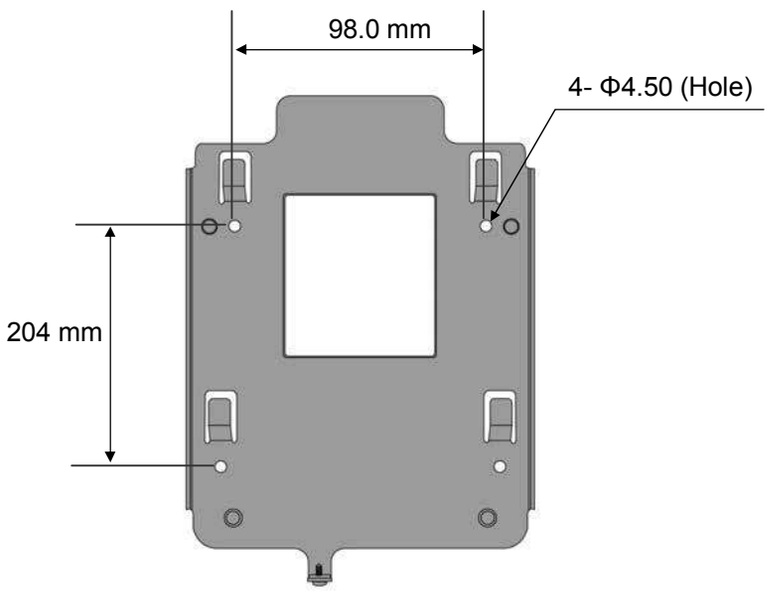
11	SAM	보안 응용 모듈을 삽입하는 곳입니다. (차후 지원)
12	Micro SD	Micro SD 메모리를 삽입하는 곳입니다. (차후 지원)

2장. 설치하기

2.3 제품 크기

- 제품 크기: 148mm(W) x 204mm(H) x 48mm(D)

[제품 전면]



[브라켓]

2장. 설치하기

2.4 브라켓 설치

다음의 절차에 따라 Wall Mount Bracket을 설치합니다.

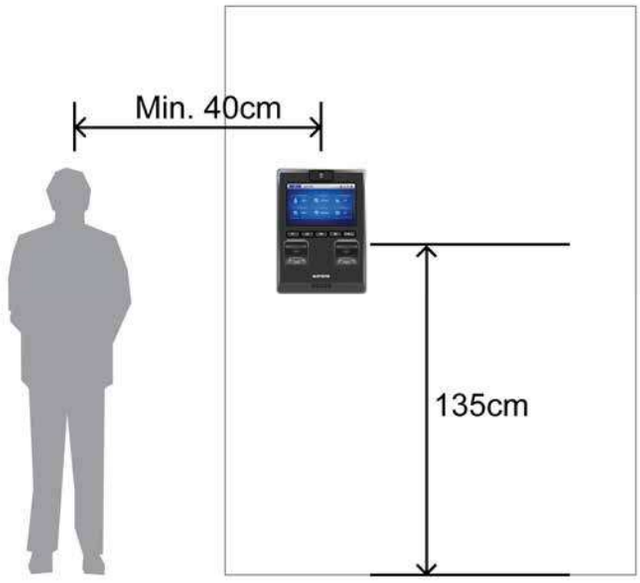
1) D-Station의 설치 위치 정하기
2) Camera 각도 조절하기
3) 브라켓 고정하기

D-Station 의 설치 위치 정하기

D-Station은 얼굴인식을 위한 카메라 장착 제품이므로, 브라켓을 설치하기 전에 설치 높이와 카메라 각도를 고려하여야 합니다."

얼굴인식과 지문 인증을 고려하여 제품의 설치 위치를 정합니다.

최적 설치 높이는 135 cm이고, 제품과 사람 간의 최소 거리는 40 cm 입니다.

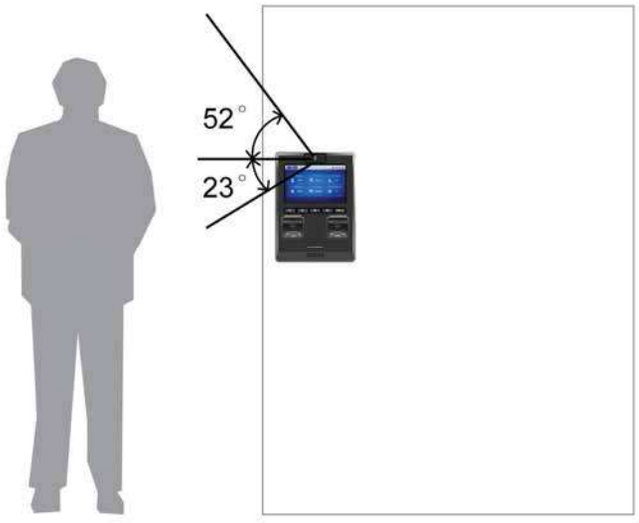


2장. 설치하기

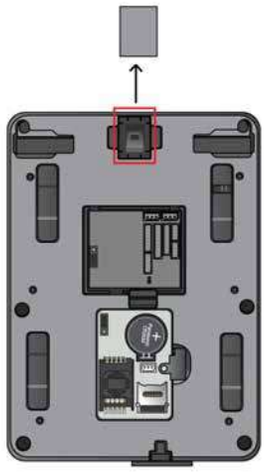
카메라 각도 조절하기

카메라 각도 조절 레버는 제품의 뒷면에 위치하고 있어, 브라켓을 고정하기 전에 카메라의 각도를 조정하여야 합니다.

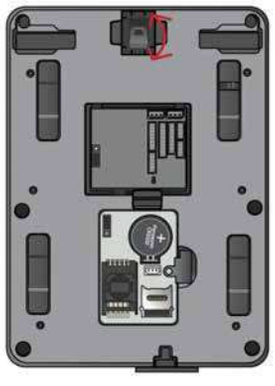
1. 사람의 얼굴인식이 가능하도록 카메라 각도를 고려하여 설치 위치를 정합니다. 카메라는 정면을 기준으로 상하 방향으로만 조절할 수 있으며, 위 방향으로 52도(최대 각도), 아래 방향으로 23도(최소 각도)까지 조절할 수 있습니다.



2. 제품 뒷면에 있는 카메라 각도 조절 레버의 고무캡을 떼어 냅니다.



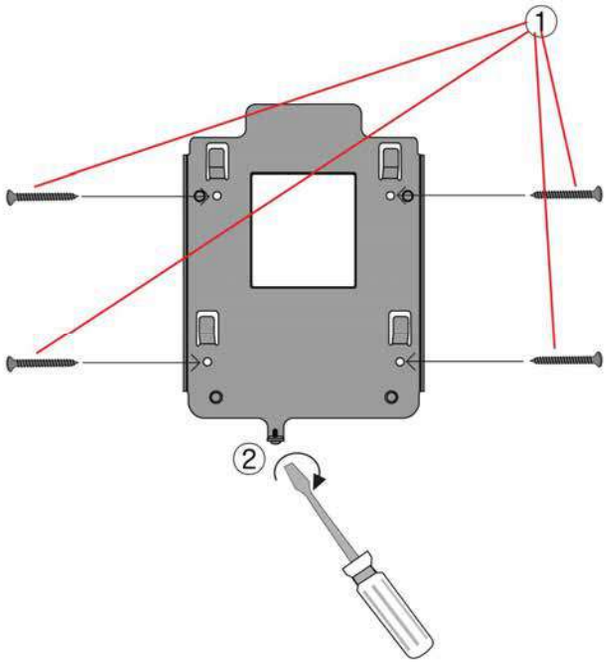
3. 사람 얼굴이 카메라의 중앙에 위치하도록 각도조절레버를 조절합니다.



2장. 설치하기

브라켓 고정하기

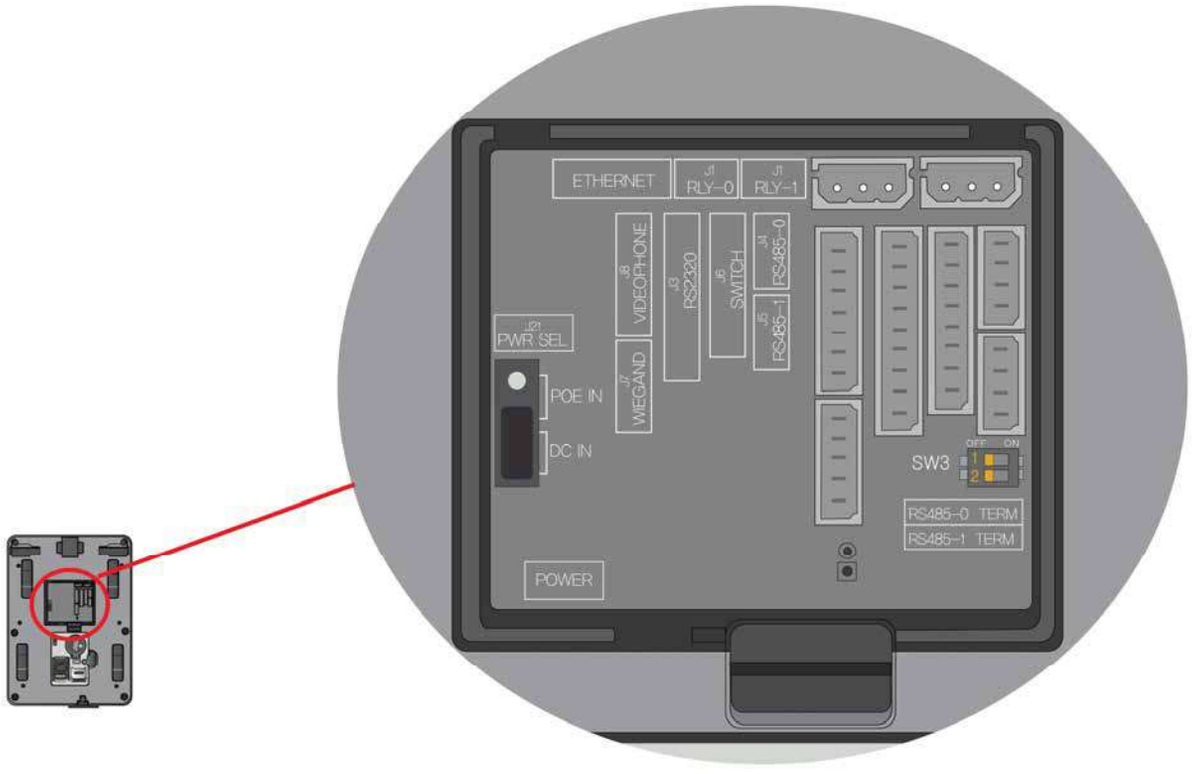
아래 그림과 같이 나사4개로 브라켓을 먼저 고정합니다. 그리고, 제품을 브라켓에 올려놓고 브라켓의 하단에 있는 제품 고정용 나사를 고정합니다.



2.5 커넥터 연결부

아래 그림과 같이 제품 뒷면에 각종 케이블을 연결할 수 있는 커넥터 연결부가 있습니다.

2장. 설치하기



주의

■ RS485-0(J4) : **PC (BioStar Client)**와 RS485 통신으로 연결할 때 사용

■ RS485-1(J5) : **Secure I/O** 혹은 다른 단말기들을 연결할 때 사용

2장. 설치하기

2.6 케이블 사양

RELAY

PIN	PIN DESCRIPTION	WIRE
1	Relay Normal Open	WHITE
2	Relay Common	BLUE
3	Relay Normal Close	ORANGE

RS485

PIN	PIN DESCRIPTION	WIRE
1	485 TRX+	BLUE
2	485 TRX-	YELLOW
3	GND	BLACK
4	SHIELD GND	GRAY

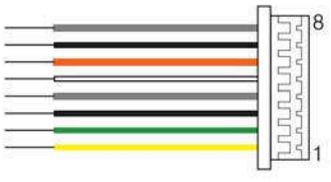
WIEGAND

PIN	PIN DESCRIPTION	WIRE
1	DATA0	GREEN
2	DATA1	WHITE
3	GND	BLACK
4	SHIELD GND	GRAY
5	-	

VIDEOPHONE

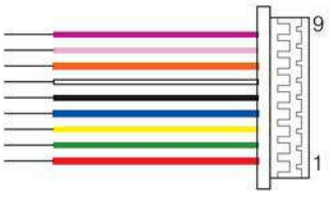
PIN	PIN DESCRIPTION	WIRE
1	VOICE SIGNAL	RED
2	GND	BLUE
3	POWER	YELLOW
4	VIDEO SIGNAL	WHITE
5	DOOR OPEN SIGNAL	ORANGE
6	GND	BLACK
7	SHIELD GND	GRAY

SWITCH



PIN	PIN DESCRIPTION	WIRE
1	SWITCH INPUT0	YELLOW
2	SWITCH INPUT1	GREEN
3	SWITCH GND	BLACK
4	SHIELD GND	GRAY
5	SWITCH INPUT2	WHITE
6	SWITCH INPUT3	ORANGE
7	SWITCH GND	BLACK
8	SHIELD GND	GRAY

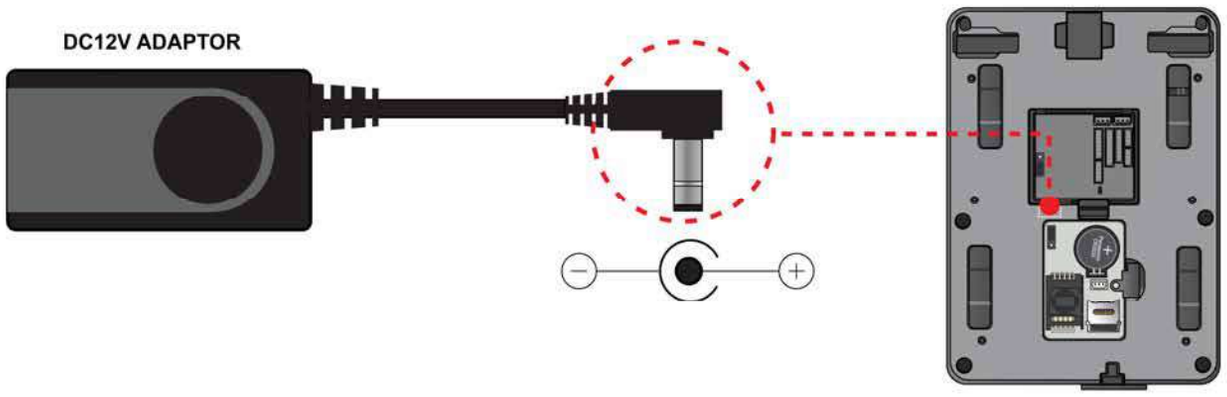
RS232C



PIN	PIN DESCRIPTION	WIRE
1	232 DCD	RED
2	232 RXD	GREEN
3	232 TXD	YELLOW
4	232 DTR	BLUE
5	232 GND	BLACK
6	232 DSR	WHITE
7	232 RTS	ORANGE
8	232 CTS	PINK
9	232 RI	PURPLE

2장. 설치하기

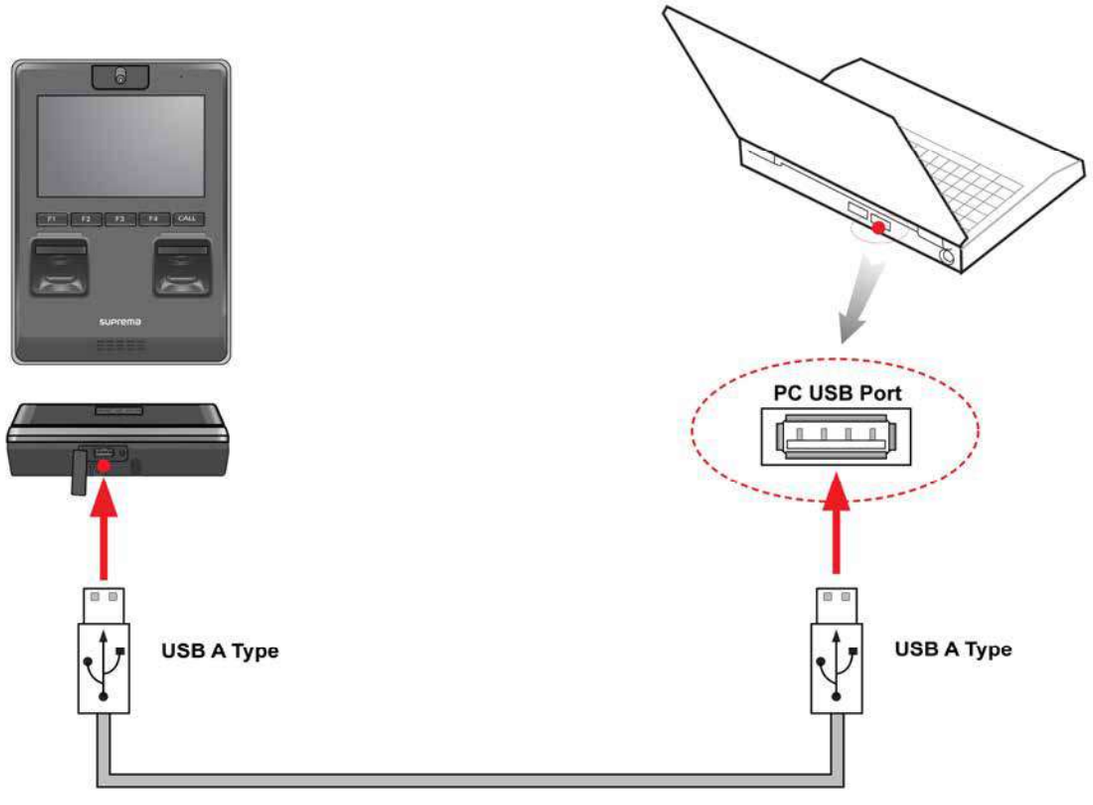
1) 전원 연결



권장 전원 사양

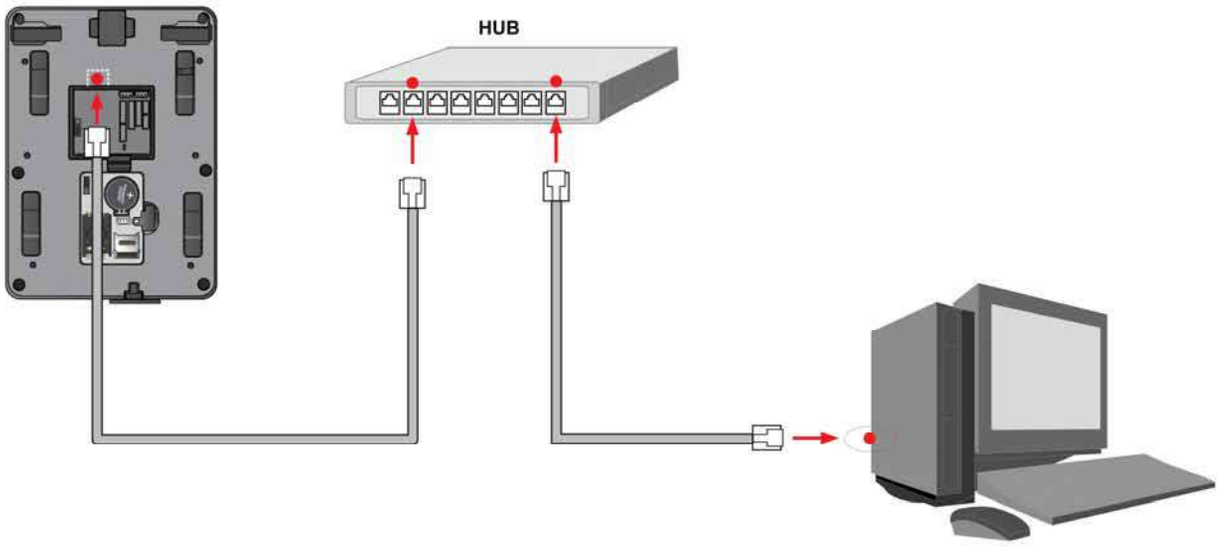
- 전압 12V ± 10%, 전류 1500mA 이상. IEC/EN 60950-1 으로 승인 난 12V adaptor 를 사용해야 합니다.
- 다른 기기의 전원을 D-Station의 전원과 공유하여 사용할 경우에는 1500mA 이상인 어댑터를 사용할 것을 권장합니다.

2) USB 케이블 연결

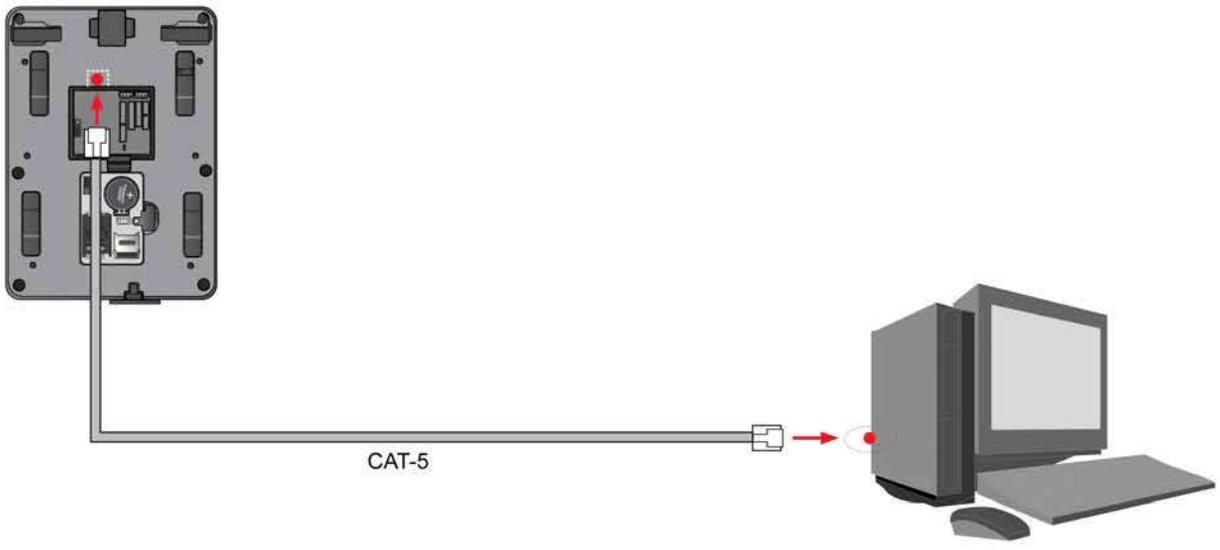


2장. 설치하기

3) LAN 연결



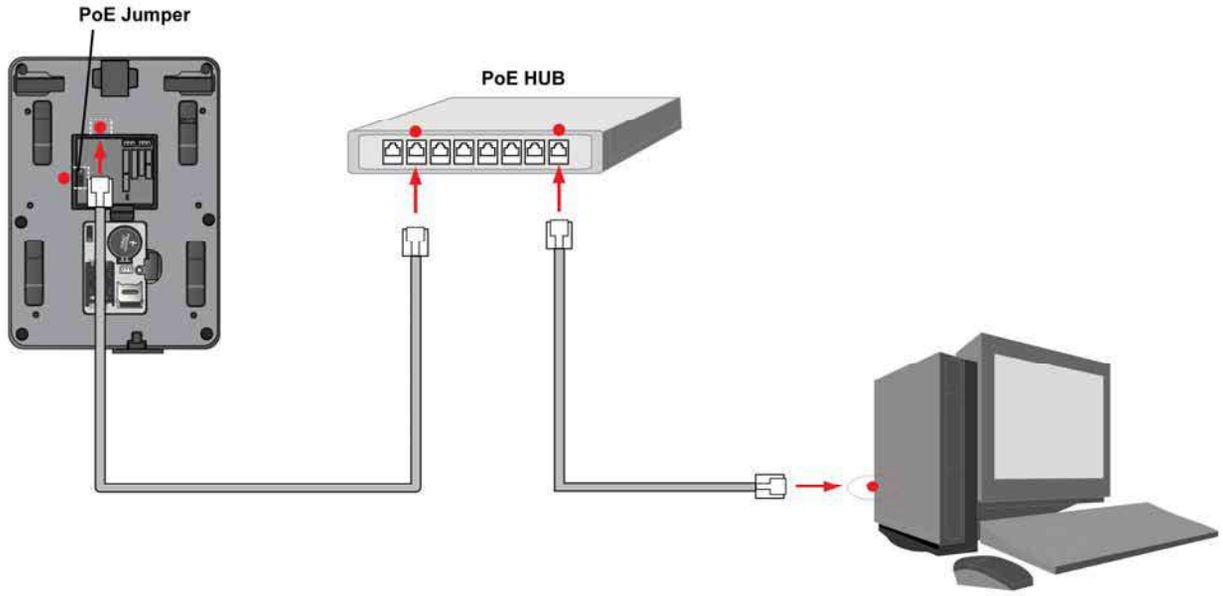
4) LAN 연결(PC 와 직접 연결)



2장. 설치하기

5) PoE Hub 연결

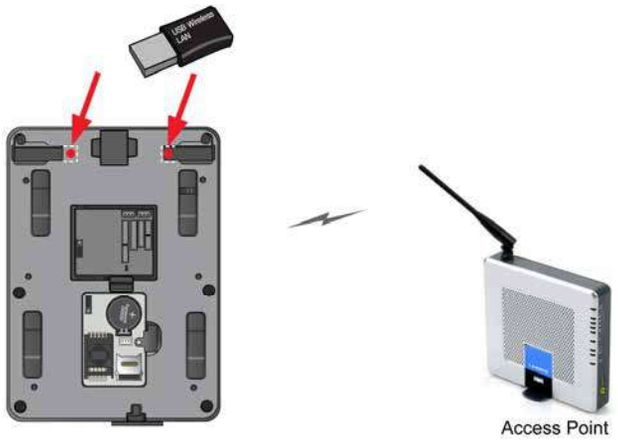
PoE(Power over Ethernet)는 IEEE802.3 규격을 만족하는 PSE(Power sourcing Equipment)로부터 전원을 공급받는 이더넷 연결 방식입니다.



- PoE 방식을 사용시 랜케이블의 길이는 100m 이내로 사용하여 주십시오.
- PoE Jumper : 제품 뒷면의 커넥터 연결부의 PWR SEL 점퍼를 POE IN으로 설정 합니다.

6) Wireless LAN 연결(Wireless Version Only)

무선랜의 성능은 주위 환경과 사용하는 AP(Access Point)의 종류에 따라 많은 영향을 받습니다. 당사에서 제공하는 특정 USB Wireless LAN 모듈을 장착해야 하며, 왼쪽/오른쪽 USB 포트는 모두 Wireless Lan을 꽂을 수 있으며, 설치 위치에 따라 좌우 포트를 선택해서 장



착할 수 있습니다.”

D-Station과의 호환성이 검증된 AP는

다음과 같습니다.

호환성이 검증된 AP 목록
- Buffalo WHR-HP-G54
- IP Time G104

(이 리스트 이외의 AP를 사용할 경우에

는 무선랜이 정상으로 동작하지 않을

수 있습니다.)

7) USB 메모리 연결

일부 USB 메모리의 경우 하드웨어 호환성 문제로

인해 연결이 되지 않을 수 있습니다. 메모리를 이용

하여 사용자나 로그 데이터를 다운로드/업로드 할 수

있습니다.

다음은 D-Station에서 정상 동작하는 것이 검증된

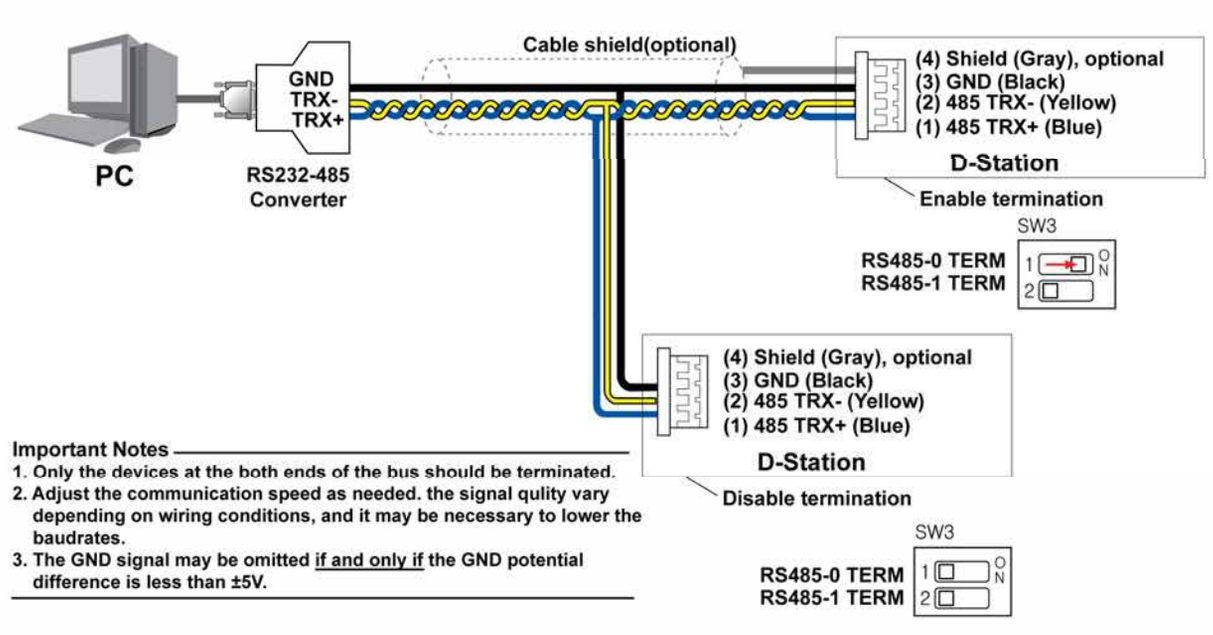
USB 메모리 리스트입니다.

호환성이 검증된 USB 메모리 목록
- [IMATION] Flash Drive Nano 4GB
- [LG전자] X TICK M4 4GB
- [LG전자] X TICK MOBY J1 2GB
- [PQI] Traveling Disk U173 4GB
- [삼성물산] PLEOMAX PUB-S100 4GB

- [삼성전자] SUB-4G MLC 4GB
- [삼성전자] SUM-M2GSD (2GB)
- [SONY] MicroVault Slide USM4GJ 4GB

8) RS485 네트워크 연결

2장. 설치하기

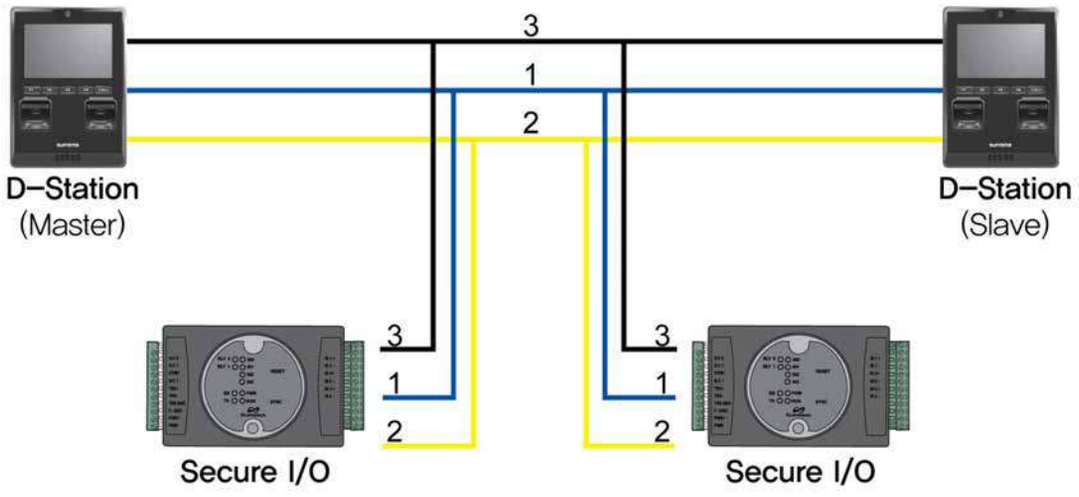


SW3(RS 485 종단 저항 선택 스위치) : RS485 배선이 길어지는 경우, 신호 약화를 방지하기 위해 Dip Switch를 켜서 종단저항을 걸어주면, 신호가 정상으로 전달됩니다. 배선이 아주 짧은 경우, 저항을 걸어주면 오히려 신호가 제대로 전달되지 않습니다. 따라서, 배선의 길이 및 신호의 상태를 고려하여, 종단저항은 켜거나 꺼주어야 합니다.

2장. 설치하기

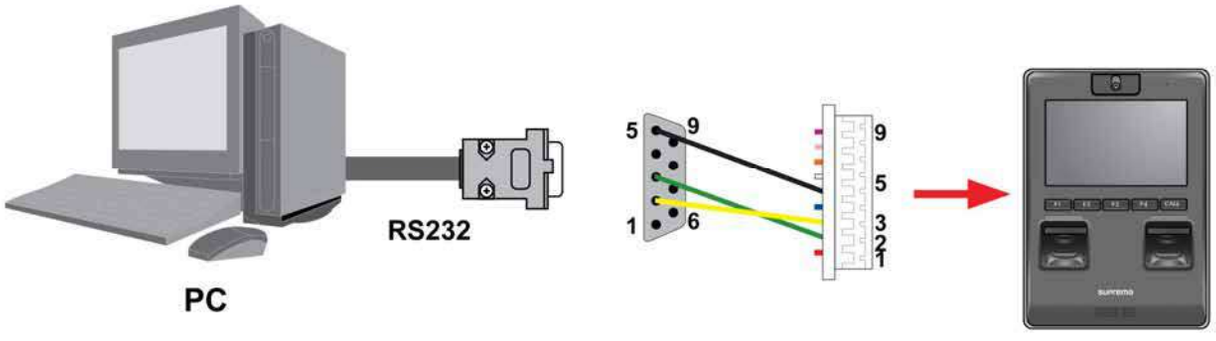
9) Secure I/O 를 사용한 RS485 네트워크 연결

PIN	PIN DESCRIPTION	COLOR
1	485 TRX+	BLUE
2	485 TRX–	YELLOW
3	GND	BLACK



최대 연결: 하나의 RS485 네트워크 당 마스터를 포함하여 최대 8개까지 연결할 수 있습니다.

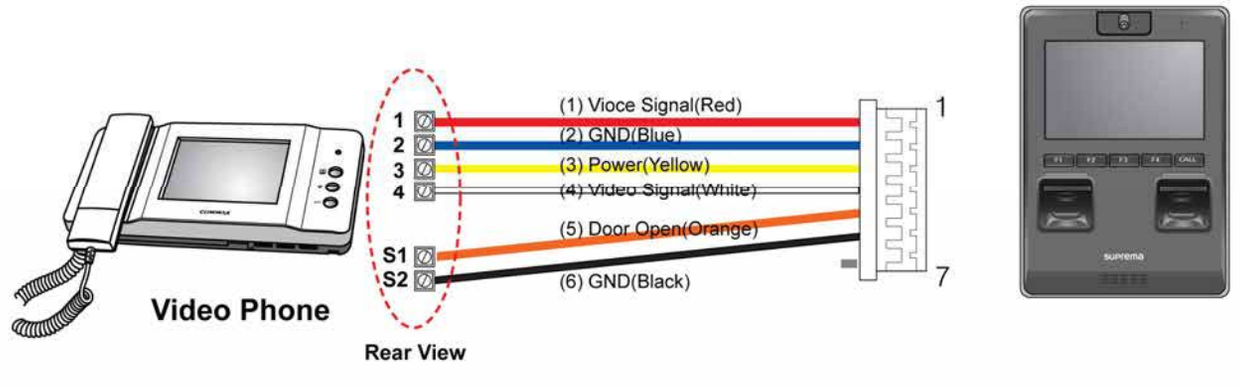
10) RS232 연결



- D-Station은 시리얼 프린터나 무선 모뎀 연결도 지원됨.

2장. 설치하기

11) 비디오폰 연결

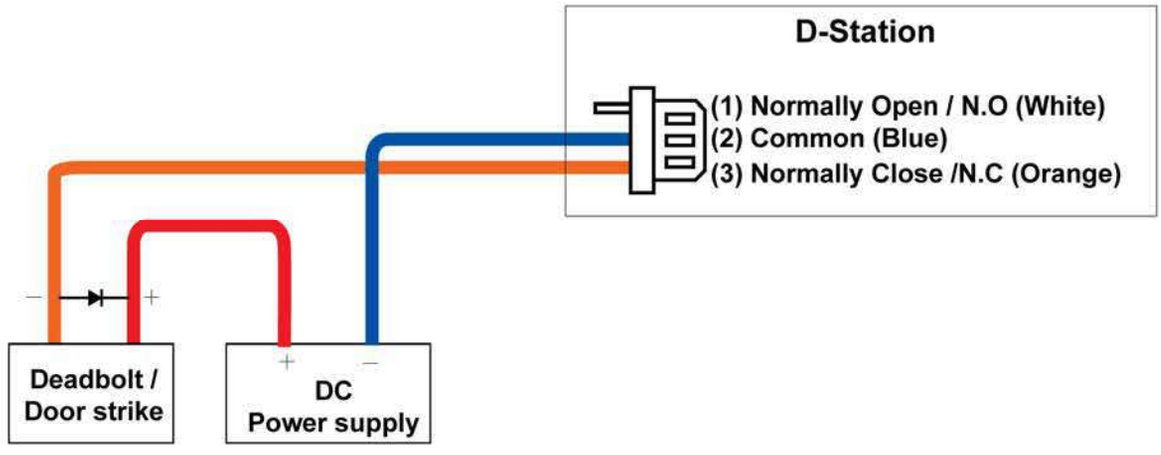


지원 모델

- COMMAX / CAV-35N
- COMMAX / CAV-50H
- COMMAX / CAV-50P

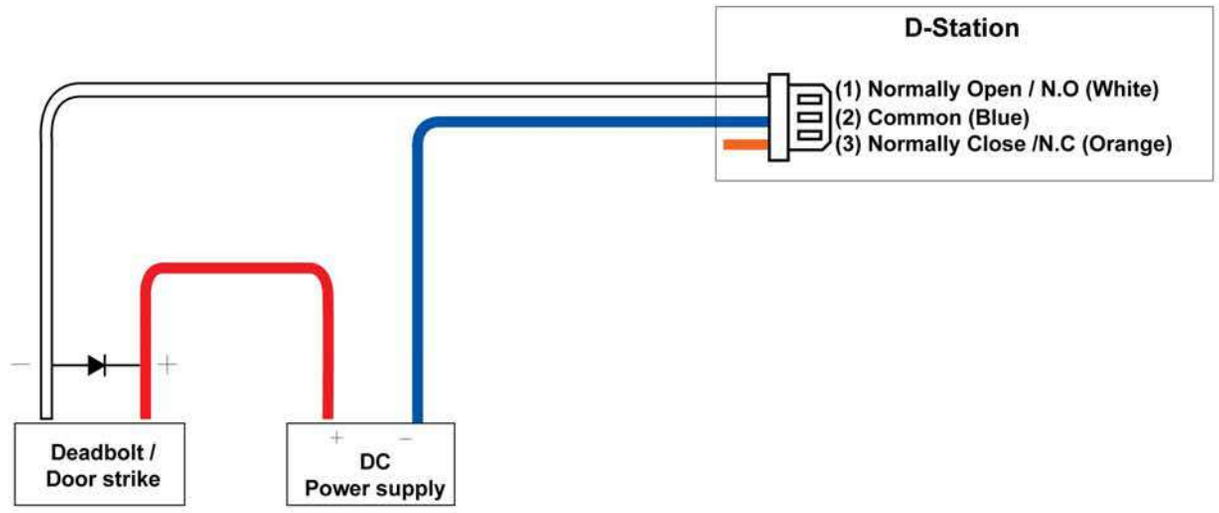
(비디오폰을 구입하려면 슈프리마의 대리점이나 본사에 문의하시기 바랍니다.)

12) 릴레이 연결 – Fail safe lock

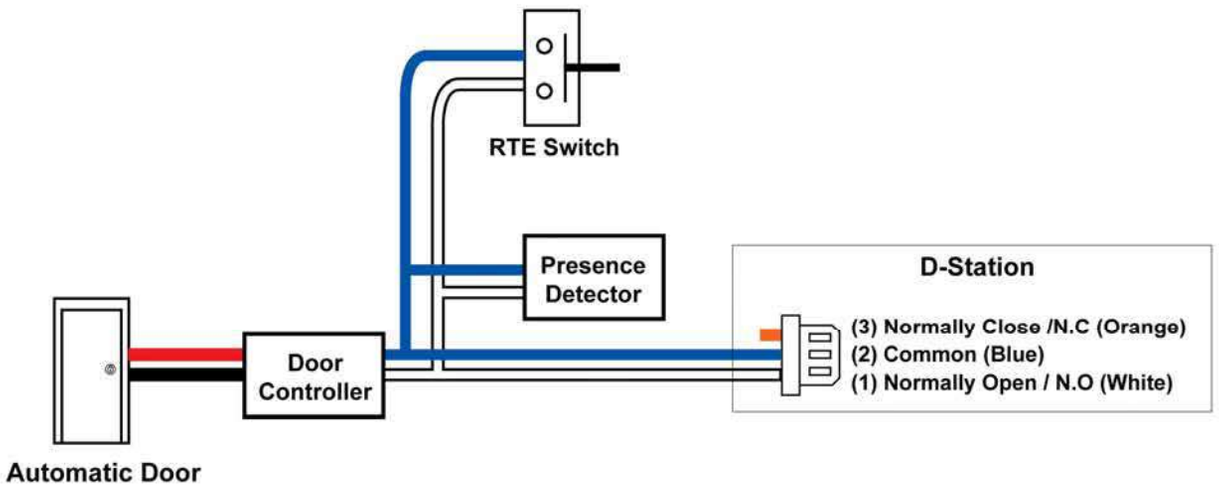


2장. 설치하기

13) 릴레이 연결 – Fail secure lock

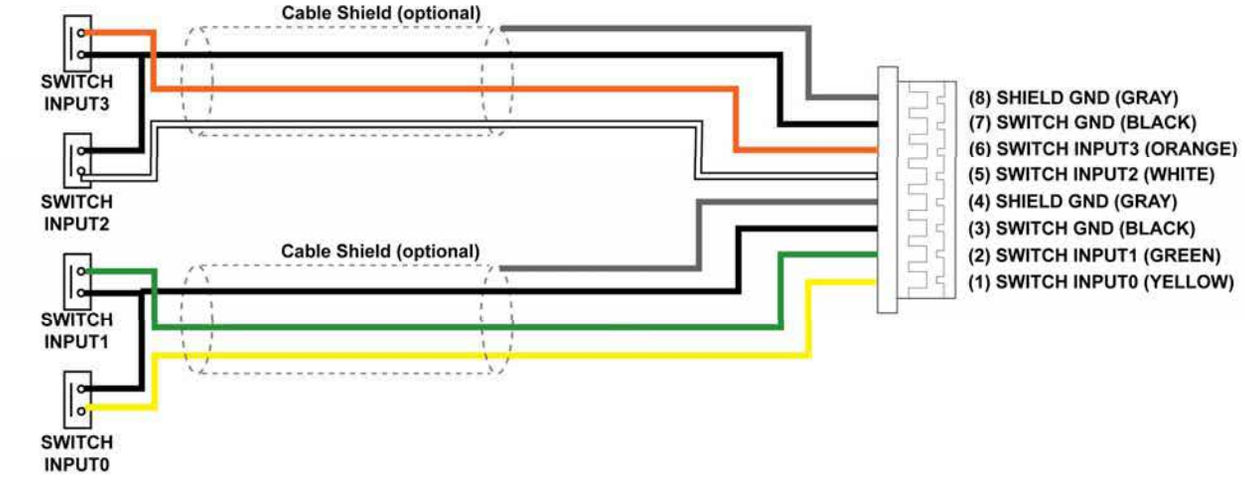


14) 릴레이 연결 – 자동문

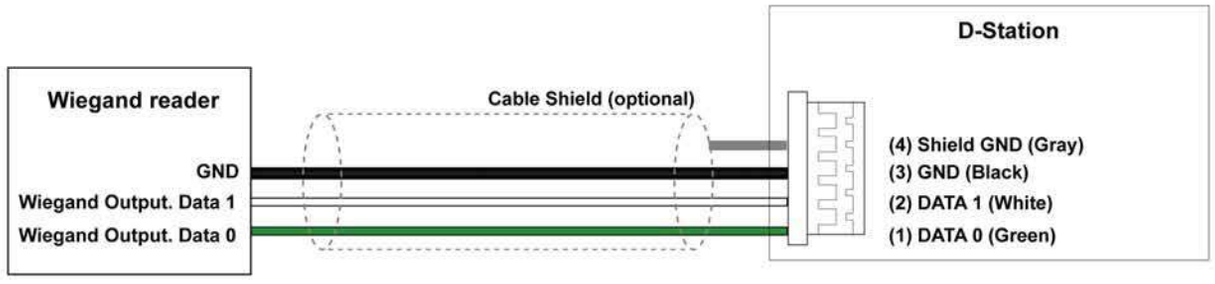


2장. 설치하기

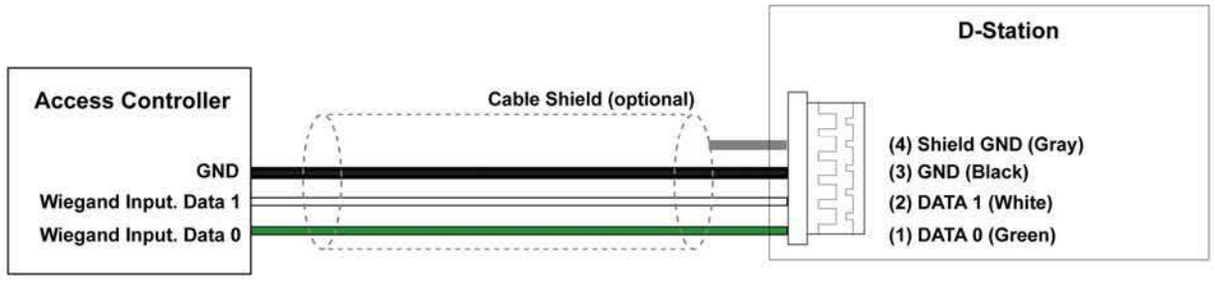
15) SWITCH 입력단자 연결 – RTE, 문 센서, 알람 입력



16) Wiegand 입력 연결 – 별도 Wiegand 리더기 사용시



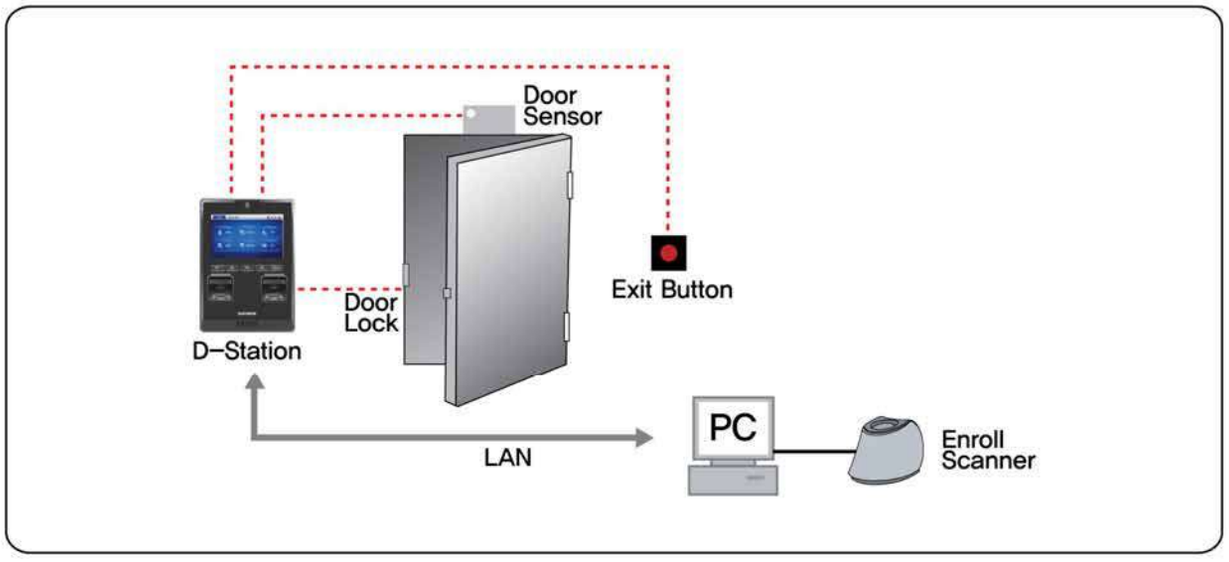
17) Wiegand 출력 연결 – 별도 출입통제기 사용시



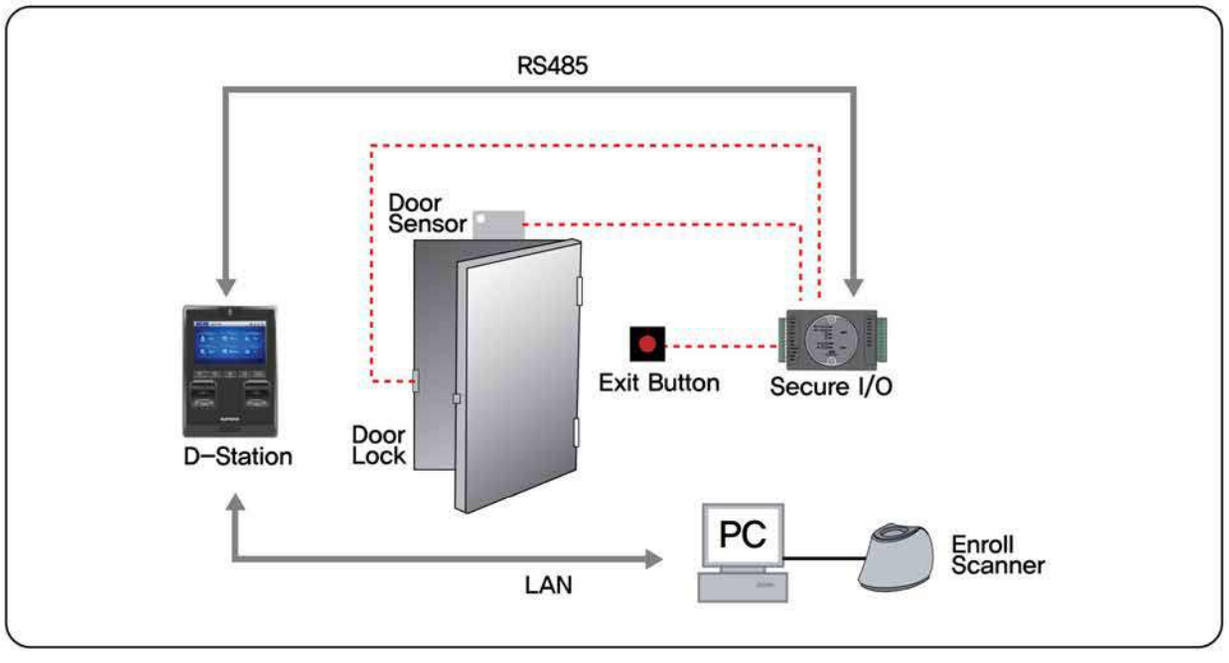
2장. 설치하기

2.7 시스템 구성도

■ 독립형

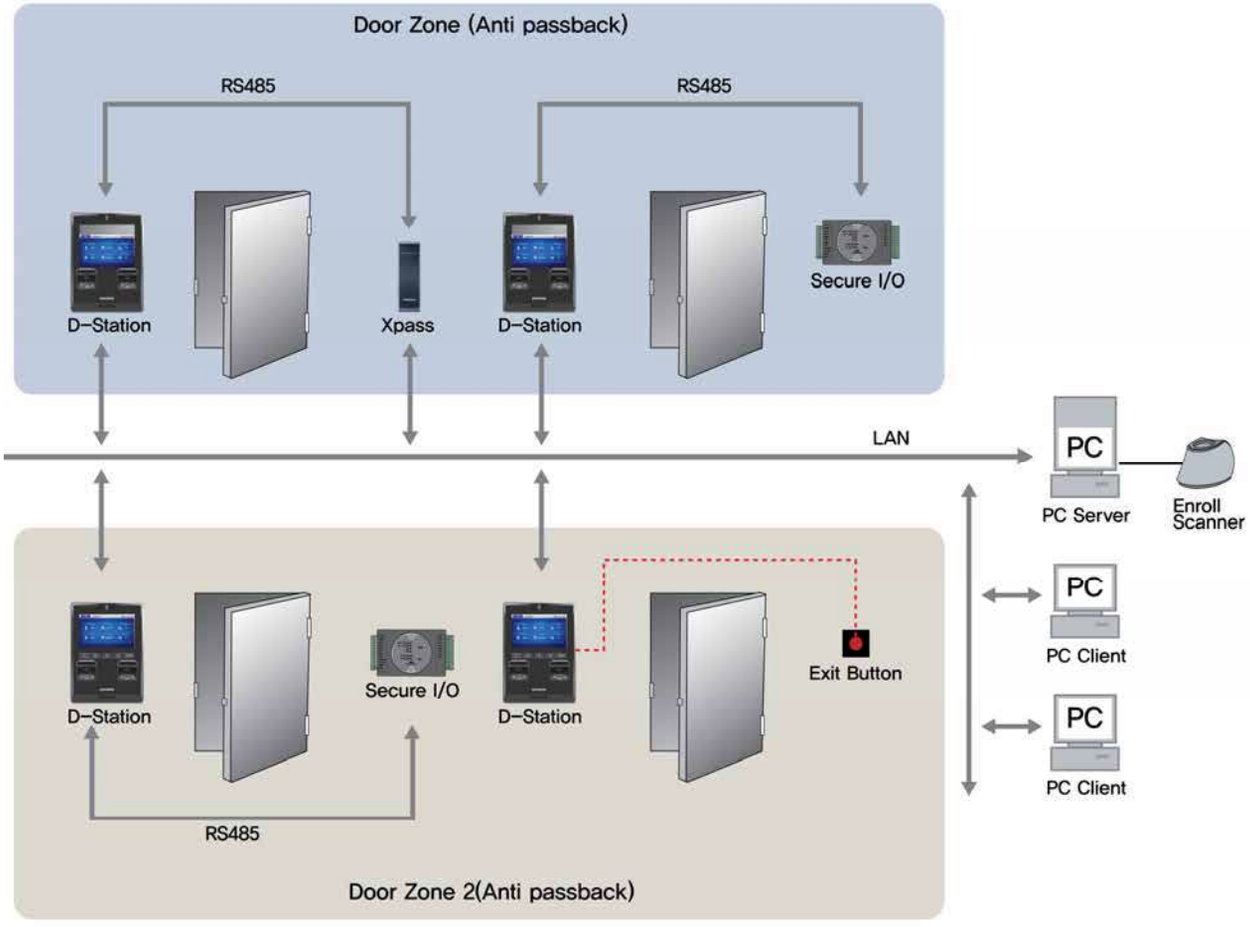


■ 독립형 (Secure)



2장. 설치하기

■ 네트워크 구성 (TCP / IP 또는 RS485)



3장. 관리자 기능

3.1 기본 화면

기본 화면 구성

명 칭	기 능
현재날짜	현재 날짜와 요일을 나타냅니다.
근태상태	현재의 근태 모드를 나타냅니다.
출근	출근 시 누릅니다.
퇴근	퇴근 시 누릅니다.
복귀	외출복귀 시 누릅니다.
외출	외출 시 누릅니다.
인터폰	비디오폰을 사용할 때 누릅니다.
ID 입력	ID 를 입력하고 출입인증을 할 수 있습니다.

명 칭	기 능
	강제 얼굴 검출 기능이 설정되어 있음을 나타냅니다.
	얼굴 인식이 설정되어 있음을 나타냅니다.(퓨전 모드)
	지문 인식이 모드 설정을 나타냅니다.  고속모드  퓨전모드  트윈모드
	문열림을 표시합니다.
	이더넷 연결 상태를 나타냅니다.
	RS485 연결 상태를 나타냅니다.
	PC 와의 연결 상태를 나타냅니다.
	관리자메뉴로 들어갑니다.

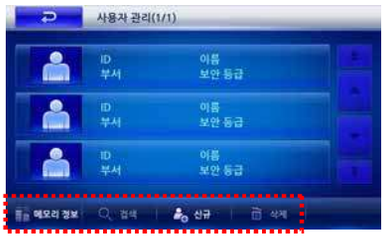
3장. 관리자 기능

관리자 등록하기

제품 구입시 초기에는 어떤 사용자도 등록되어 있지 않습니다. 제품 설치 후 즉시 관리자를 등록한 후 사용하여야 합니다.

처음으로 관리자를 등록하는 방법은 다음과 같습니다.

1. [관리자메뉴] ▸ [사용자] ▸ [사용자 관리]에 들어간 후, 사용자 검색/등록/삭제를 할 수 있습니다.
- 검색: 사용자 검색
- 신규: 사용자 등록
- 삭제: 사용자 삭제

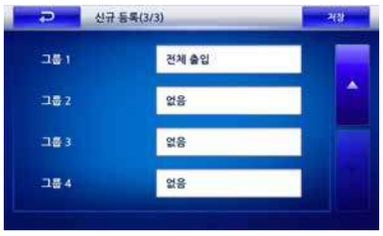


2. 사용자 신규 등록시 [단말기] 또는 [카드]를 선택한 후 사용자를 등록합니다.

3. [이름, 부서, 보안등급, 비밀번호]를 입력하고 [▾]을 누릅니다.
- 보안등급은 관리자를 선택하여야 합니다.
- 비밀번호는 숫자판을 이용하여 2번 입력합니다.

4. 지문, 카드, 얼굴 영상 중 하나를 선택한 후 관리자 정보를 입력합니다. 지문, 카드, 얼굴 영상을 등록하는 순서는 상관없으며, 원하는 관리자 정보만 등록하면 됩니다.

5. [▾]버튼을 누르고 사용자 그룹을 선택합니다. 사용자 그룹은 선택사항으로, 사용자 그룹으로 관리할 경우에만 지정합니다.
- 설정값: 없음/ 전체 제한/ 전체 출입



3장. 관리자 기능

■ 지문 등록

한 개의 ID당 최소한 2개 이상의 지문을 등록하는 것이 좋습니다. 지문인식이 잘 안되는 사용자의 경우 같은 손가락을 여러 번 중복해서 등록하면 인식 성능을 높일 수 있습니다.

지문을 입력할 손과 손가락을 선택합니다.	선택한 손가락의 지문을 입력합니다. (일반/협박 손가락을 선택할 수 있습니다.)
	

- 일반 손가락: 출입이나 기본 인증에 사용할 손가락 지문 정보를 등록합니다.
- 협박 손가락: 협박 손가락은 출입문 앞에서 도둑에게 협박을 당하는 위험한 상황에서 요긴하게 사용될 수 있습니다. 협박 손가락이 입력되면 정상적으로 출입문은 열리지만 출력포트로 설정해 놓은 비상경보장치를 울리거나 비상연락전호로 발신하는 등의 구성이 가능합니다. 협박 손가락은 앞서 등록한 일반 손가락과 반드시 다른 손가락을 등록해야 합니다.

■ 카드 등록

Bypass 사용여부를 선택한 후 카드 ID 를 입력합니다.	카드를 단말기에 접촉한 후 [확인]을 누릅니다.
	

- ID 카드로부터 Custom ID, 카드 ID를 읽어 들여, 해당 ID 필드(위:Custom ID, 아래: 카드 ID)에 자동입력 합니다.

■ 얼굴 영상 등록

얼굴 영상을 등록합니다.	얼굴 영상은 3 번 연속해서 입력합니다.
	

3장. 관리자 기능

관리자 메뉴 들어가기

관리자는 사용자, 네트워크, 동작, 단말기, 화면/음성, 로그 등을 설정할 수 있습니다.

1. [관리자메뉴] 버튼을 선택후, [관리자 인증] 화면이 나타나면 등록된 관리자의 카드 또는 지문을 인식합니다. 인증이 성공하면 관리자 메뉴 화면이 나타납니다.

2. 관리자 인증에 성공하면 오른쪽과 같은 관리자 초기 메뉴가 나타납니다. 이 화면에서 원하는 항목을 선택한 후, 기능을 설정할 수 있습니다.

- 사용자: 사용자를 등록하거나 삭제할 수 있으며 DB를 초기화할 수 있습니다.
- 네트워크: TCP/IP/서버 등을 설정할 수 있으며 USB 사용 여부를 설정할 수 있습니다.
- 동작: 출입 시 인증모드나 근태모드를 설정할 수 있습니다.
- 단말기: 지문 인증 설정/ 출입문 설정이나 단말기 시간 등을 설정할 수 있습니다.
- 화면/음성: 배경화면이나 화면 테마/ LCD조명 등을 설정하며 안내 음량을 조절할 수 있습니다.
- 로그: 단말기에 남겨진 출입/ 동작 로그 정보를 확인할 수 있습니다.

참고

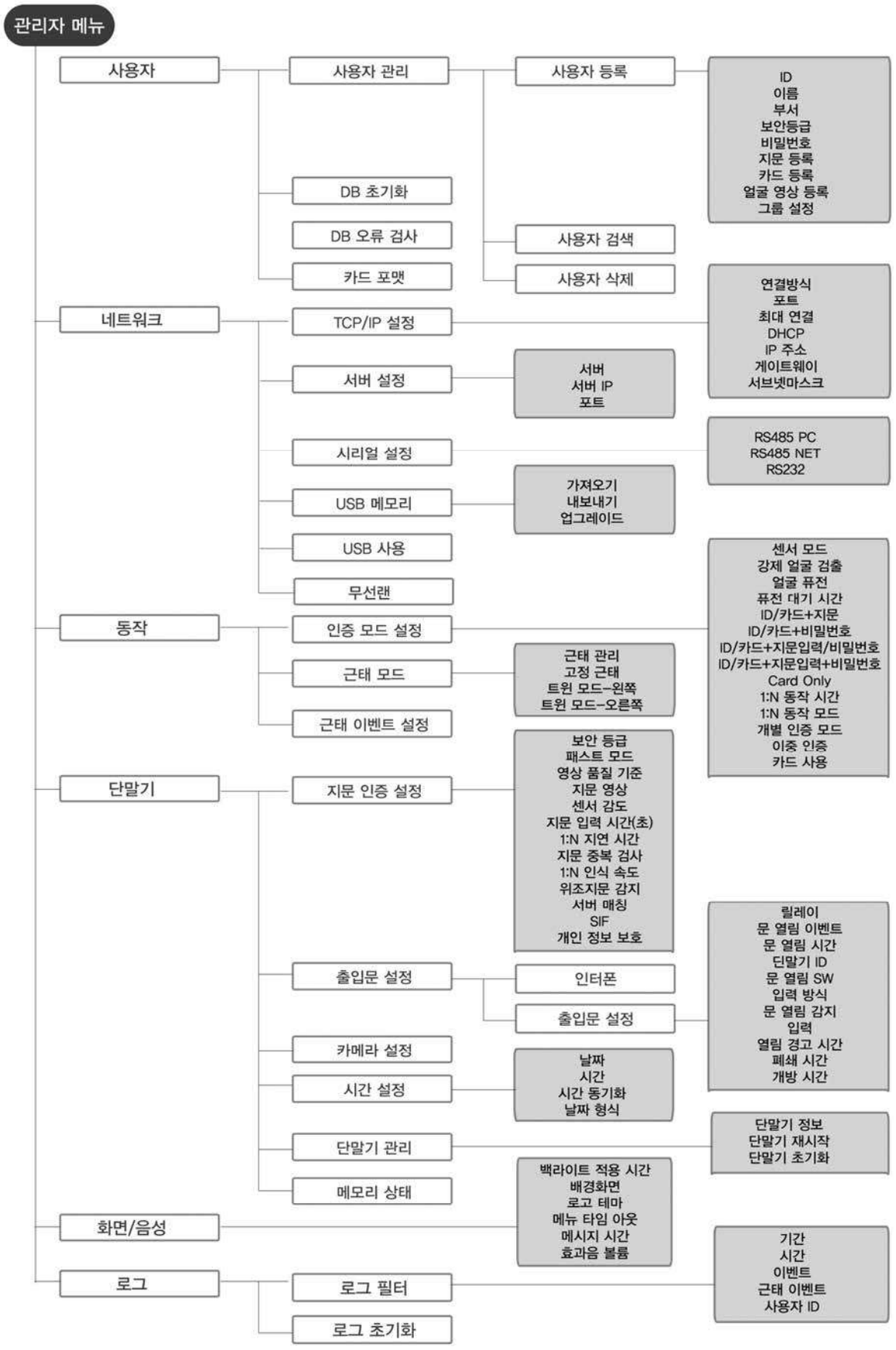
■ 화면의  버튼을 누르면 이전 화면으로 이동합니다.

■ [▼]/[▲] 방향키를 이용하여 세부 메뉴 항목으로 이동할 수 있습니다.

■ 관리자 메뉴에 들어간 후 아무런 키 입력을 하지 않은 상태로 일정시간이 지나면 보안상의 이유로 자동으로 초기 화면으로 빠져 나가도록 설정되어 있습니다. 이 기능을 원하지 않거나 시간을 조정하려면 **'3.7 화면/음성 관리하기'**를 참조하십시오.

3장. 관리자 기능

관리자 메뉴 구성



3장. 관리자 기능

인증 모드 설정

1:1 인증 모드

- ID/카드+지문
- ID/카드+비밀번호,
- ID/카드+지문/비밀번호,
- ID/카드+지문+비밀번호,
- 카드만으로 인증
  - 1:1 인증모드에서 원하는 모드를 선택한 후 지문 사용과 비밀번호 사용여부를 설정합니다. 카드만으로 인증일 경우는 별도의 인증 절차없이 카드를 사용하는 것만으로도 인증가능합니다.

1:1 시간

- 1:1 인증 모드로 선택한 항목의 내용에서 인증모드의 스케줄을 설정합니다.
- 각 인증모드를 사용할 시간을 선택할 수 있으며, 항상 적용/ 비근무시간/출입시간대/퇴근시간대/정규직/생산직/사용 안함 또는 BioStar 프로그램의 출입통제 메뉴에서 미리 설정한 출입시간의 목록이 나타납니다.

1:N 인증 모드

- 설정값: 자동/OK나 근태기능키/사용안함
- 자동: 항상 지문 센서가 입력대기상태여서 손가락만 대면 자동으로 1:N인식을 시작합니다.
- OK나 근태기능키: OK키를 누르거나 근태기능키를 누르고 난 후 지문을 입력받습니다.
- 사용안함: 1:N 인식기능을 사용하지 않습니다. 보안성을 높이기 위해 항상 ID입력을 먼저받는 1:1 인증모드만 사용하게 됩니다.

1:N 시간

- 1:N 시간항목에서는 위 1:N 인증모드의 스케줄을 설정합니다.
- 각 인증모드를 사용할 시간을 선택할 수 있으며, 항상 적용/ 비근무시간/출입시간대/퇴근시간대/정규직/생산직/사용안함 또는 BioStar 프로그램의 출입통제 메뉴에서 미리 설정한 출입시간의 목록이 나타납니다.

개별인증모드

- 설정값: 사용안함/사용
- 개인별로 인증방식을 설정할 것인지 여부를 정합니다.

2중 인증

- 설정값: 사용안함/사용
- 2중 인증을 사용하는 경우, 각각 다른 두사람의 지문이나 카드가 15초 이내 연속입력이 되어야 출입문을 열 수 있도록 동작됩니다.
- 2중 인증 시간항목에서는 위 2중 인증모드의 스케줄을 설정합니다.
- 2중 인증모드를 사용할 시간을 선택할 수 있으며, 항상적용/ 사용안함/ 비근무시

3장. 관리자 기능

간/ 출입시간대/ 퇴근시간대/ 정규직/ 생산직 또는 BioStar 프로그램의 출입통제 메뉴에서 미리 설정한출입시간의 목록이 나타납니다.

Two Sensor Mode

사용자 인증시 2개의 지문센서와 CPU가 작동하는 운용 모드를 선택합니다.

Fast Mode	1개의 지문 입력에 대하여 2개의 내부 CPU가 동시에 인증 처리하는 모드입니다. 인증 속도가 2배 이상 빨리 처리됩니다.
Fusion Mode	2개의 손가락 지문에 대한 퓨전 알고리즘에 하여 인증 처리하는 모드입니다. 1개 혹은 2개의 손가락을 동시에 입력이 가능합니다. 각각의 지문의 인증율이 낮은 사용자의 경우 다른 인증모드를 사용하면 인증 실패되기 쉬우나, 퓨전 인증을 사용하면 특성의 합으로 인증율이 높아집니다.
Twin Mode	2개의 센서가 독립적으로 작동하여 인증 처리하는 모드입니다. 1대의 D-Station으로 동시에 2명을 인증 처리할 수 있습니다.
Demo Mode	얼굴 퓨전 인증을 테스트 하기 위해 지원하는 테스트 모드입니다. 얼굴이 일치하지 않아도 지문만 일치하면 인증 성공이 됩니다. 실제 운영 모드에서는 사용하면 안됩니다.

Detect Face

사용자 인증 시 얼굴의 촬영여부를 선택합니다. 인증이 성공한 경우 얼굴 영상을 강제로 검출하여 출입한 사용자에 대한 얼굴 영상을 로그로 저장합니다.

Face Fusion

현재 설정된 인증 모드에 얼굴 영상까지 포함하여 운용하는 모드입니다. 지문 인식만으로 인증율이 낮은 사용자의 경우는 인증 성공율을 높이는 효과가 있습니다.

- 얼굴 퓨전을 적용할 수 있는 인증 방식은 Fast Mode, Fusion Mode 2가지가 있습니다. ‘Fast Mode + FaceFusion’, ‘Fusion Mode + Face Fusion’과 같이 조합하여 사용할 수 있습니다.

Fusion Time Out

Fusion Mode로 운용 시, 퓨전 인증 수행에 필요한 전체 소요시간에 대한 Time-out을 의미합니다.

3장. 관리자 기능

3.2 사용자 관리하기

사용자 등록하기

사용자 등록은 기본정보, 인증 정보, 그룹정보 입력으로 이루어집니다. 사용자 정보는 단말기 또는 카드에 등록할 수 있습니다.

1) 기본정보는 ID, 이름, 소속, 등급, 비밀번호
2) 인증 정보는 지문, 카드, 얼굴 정보
3) 그룹 정보

1. 단말기에 등록하기

다음은 사용자 정보를 단말기에 등록하는 예제입니다.(예: 지문+카드+얼굴)

1. [관리자메뉴] ▸ [사용자] ▸ [사용자 관리]에 들어간 후, 사용자 검색/등록/삭제를 할 수 있습니다.
- 검색: 사용자 검색
- 신규: 사용자 등록
- 삭제: 사용자 삭제

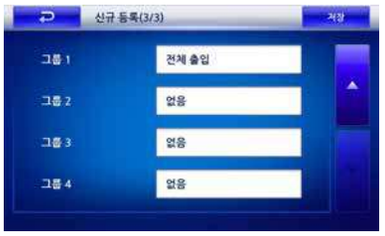
2. 사용자 신규 등록시 [단말기]를 선택한 후 사용자를 등록합니다.
- 단말기: 사용자 정보를 D-Station에 저장할 경우
- 카드: 사용자 정보를 카드에 저장할 경우

3. [이름, 부서, 보안등급, 비밀번호]를 입력하고 [▾]을 누릅니다.
- 얼굴 이미지: 사람 이미지의 하단 카메라 버튼을 클릭한 후 얼굴 이미지를 저장합니다.
- 보안등급은 '일반'을 선택하여야 합니다.
- 비밀번호는 숫자판을 이용하여 2번 입력합니다.
- 사용자 ID는 비어있는 것 중 가장 낮은 ID가 기본값으로 표시됩니다. 원하는 ID를 수동으로 입력할 수도 있습니다. 사용자ID는 1부터 4,294,967,295까지 가능합니다.

4. 지문, 카드, 얼굴 영상 중 하나를 선택한 후 관리자 정보를 입력합니다. 지문, 카드, 얼굴 영상을 등록하는 순서는 상관없으며, 원하는 사용자 정보만 등록하면 됩니다.
- 지문, 카드, 얼굴 영상의 등록은 24페이지를 참조합니다.

3장. 관리자 기능

5. [▾]버튼을 누르고 사용자 그룹을 선택합니다. 사용자 그룹은 선택사항으로, 사용자 그룹으로 관리할 경우에만 지정합니다.
   - 설정값: 전체출입/전체제한 /BioStar에서 생성한 출입그룹
   - 출입그룹의 편집은 BioStar 프로그램을 사용해야 하며, 기본 출입 그룹은 전체출입 / 전체제한 입니다. (동작메뉴에서 설정한 인증시간대와 관계없음)



2. 카드 등록하기

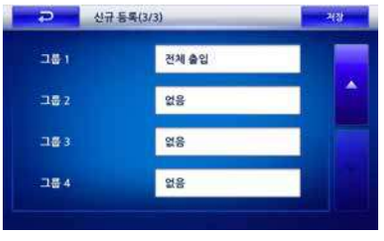
다음은 사용자 정보를 카드에 등록하는 예제입니다.

1. 사용자관리 화면에서 [신규]를 눌러 [카드]를 선택한 후 사용자를 등록합니다.
   - 단말기: 사용자 정보를 D-Station에 저장할 경우
   - 카드: 사용자 정보를 카드에 저장할 경우

2. 이름, Bypass, 보안등급, 비밀번호]를 입력하고 [▾]을 누릅니다.
   - 보안등급은 '일반'을 선택하여야 합니다.
   - 비밀번호는 숫자판을 이용하여 2번 입력합니다.

3. 지문을 선택한 후 관리자 정보를 입력합니다.
   - 지문 등록은 24페이지를 참조합니다.

4. [▾]버튼을 누르고 사용자 그룹을 선택합니다. 사용자 그룹은 선택사항으로, 사용자 그룹으로 관리할 경우에만 지정합니다.
   - 설정값: 전체출입 / 전체제한 / BioStar에서 생성한 출입그룹
   - 출입그룹의 편집은 BioStar 프로그램을 사용해야 하며, 기본 출입 그룹은 전체출입 / 전체제한 입니다. (동작메뉴에서 설정한 인증시간대와 관계없음)



5. 사용자 그룹까지 모두 등록한 후 [확인]을 누르면 카드 등록화면이 나타납니다. 등록할 사용자의 카드를 접촉하여 줍니다.

3장. 관리자 기능

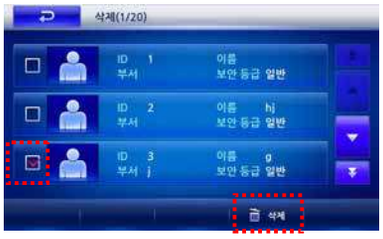
사용자 삭제하기

현재 등록되어 있는 사용자를 검색한 후, 단말기에서 사용자를 삭제합니다.

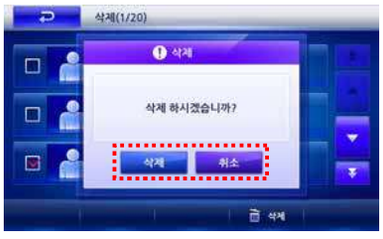
주의
사용자를 삭제하면, BioStar 의 데이터베이스에서 사용자 정보가 저장되어 있지않는 한 복구할 수 없으므로 주의하여야 합니다.

1. 사용자관리 화면에서 [삭제]를 누릅니다.

2. 삭제할 사용자를 체크박스에서 선택한 후 [삭제]를 선택합니다.



3. 팝업창이 나타나면, 사용자를 삭제하려면 [삭제]를 누릅니다. [취소]를 누르면 이전화면으로 돌아갑니다.



3장. 관리자 기능

사용자 수정하기

등록된 사용자를 검색한 후 비밀번호나 지문 등의 사용자 정보를 수정할 수 있습니다.

1. [관리자메뉴] ▸ [사용자] ▸ [사용자 관리]에 들어간 후, 사용자 정보를 수정할 수 있습니다.

[사용자 목록에서 선택할 경우]

2. 사용자 목록에서 선택하거나 [검색]을 누른 후 ID를 입력합니다.

[검색]을 누른 후 ID를 입력할 경우]

3. 수정할 항목을 수정한 후 [▾]을 누릅니다.

4. [지문/카드/얼굴 영상] 중에서 원하는 항목을 선택한 후 수정합니다.
이에 대한 수정방법은 24페이지에 있는 지문/카드/얼굴 영상 등록 내용을 참고합니다.

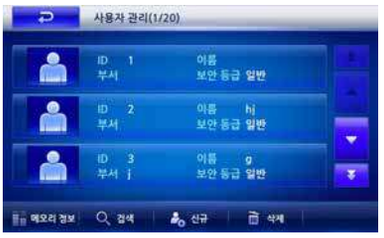
5. 원하는 항목을 모두 수정한 후 [저장]을 누르면 변경된 정보가 저장됩니다.

3장. 관리자 기능

사용자 검색하기

현재 등록되어 있는 사용자를 검색할 수 있습니다.

1. [관리자메뉴] ▸ [사용자] ▸ [사용자 관리]에 들어간 후, 사용자 정보를 검색할 수 있습니다.



2. 사용자 목록에서 [▾/▴] 키를 누르거나 [검색]을 누른 후 ID를 입력합니다.

[검색]을 누른 후 ID를 입력할 경우

3. 사용자를 검색한 결과가 화면에 표시됩니다. 이때, 사용자 정보를 수정하거나 삭제할 수도 있습니다.

3장. 관리자 기능

메모리 정보 확인하기

현재 단말기에서 사용 중인 메모리 현황을 확인할 수 있습니다.

1. [관리자메뉴] ▸ [사용자] ▸ [사용자 관리]에 들어간 후, [메모리 정보]를 선택합니다.

2. 현재 단말기의 메모리 상태를 확인할 수 있습니다.

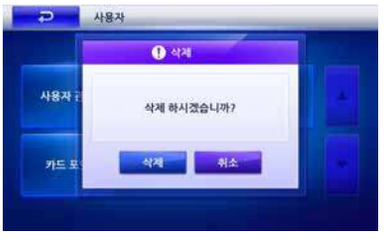
3.3 사용자 메뉴 사용하기

DB 초기화

등록되어 있는 사용자 데이터를 모두 삭제합니다. DB 초기화 후에는 사용자를 포함하여 관리자까지 모두 삭제되므로, 관리자부터 등록하여야 합니다.

1. [관리자메뉴] ▸ [사용자]에 들어간 후, [DB 초기화]를 선택합니다.

2. 초기화 팝업창이 나타나면 [삭제]를 선택합니다.
   - [삭제]를 누르면, 관리자와 모든 사용자가 삭제되고 복원할 수 없습니다.

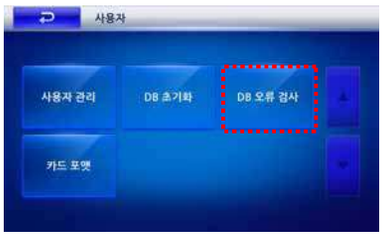


3장. 관리자 기능

DB 오류검사

사용자 DB에 오류로 인하여 사용자가 등록되어 있더라도 인증에 실패할 수 있습니다. DB 오류 검사를 수행하면, 사용자 DB의 레코드를 점검하여 자동으로 복구하여 줍니다.

1. [관리자메뉴] ▸ [사용자]에 들어간 후, [DB 오류 검사]를 선택합니다.



2. 결과가 화면에 표시됩니다.

- 사용자 DB에 오류가 있을 경우 자동으로 복구해주고, 복구에 실패할 때는 오류 안내 메시지가 나옵니다.

카드 포맷

사용자 정보는 단말기에 저장하거나 MIFARE 카드에 저장할 수 있습니다. 카드 포맷을 수행하면 MIFARE 카드에 저장된 사용자 정보를 지웁니다.

1. [관리자메뉴] ▸ [사용자]에 들어간 후, [카드 포맷]을 선택합니다.

2. 오른쪽의 화면이 나타나면 포맷할 카드를 단말기에 접촉합니다. 카드 포맷이 성공하면 확인창이 나타납니다.

3장. 관리자 기능

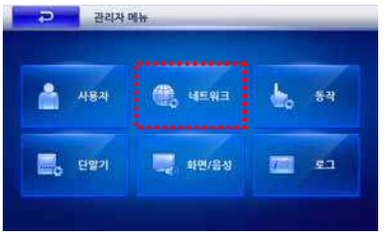
3.4 네트워크 관리하기

제품 설치후 PC와 연결하여 제품을 사용하려면 원하는 연결방식에 따른 네트워크 설정을 해야합니다.

TCP/IP 설정하기

단말기와 BioStar를 연결할 때의 TCP/IP 방식을 설정합니다.

1. [관리자메뉴]에 들어간 후, [네트워크]를 선택합니다.



2. 오른쪽의 화면이 나타나면 [TCP/IP]을 선택합니다.

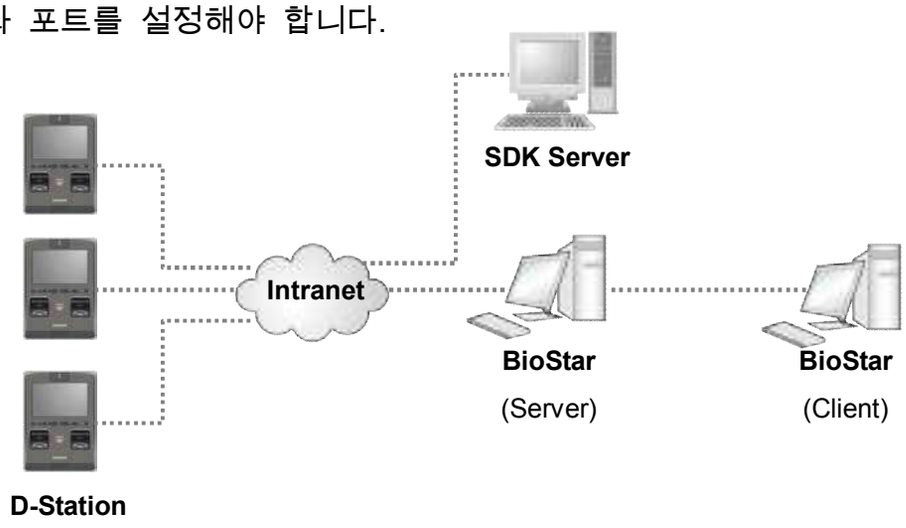
3. 연결 방식, 포트 등을 입력하고, [▾]을 누르고 IP 주소, 게이트웨이 등을 입력합니다. 모두 입력한 후에는 [저장]을 선택합니다.

- 연결 방식: 단말기 뒷면의 RJ45 커넥터를 이용해 이더넷으로 연결하거나 무선랜을 이용해 PC와 연결할 경우 사용합니다. (설정값: 이더넷/ Wireless LAN/ 사용안함)
- 포트: 단말기의 TCP/IP 포트를 지정합니다. 기본값은 '1470'으로 설정되어 있습니다.
- 최대 연결: 단말기에 접속할 수 있는 BioStar의 수를 설정합니다.(설정값: 1/4/6/8/16)
- DHCP: DHCP 프로토콜의 사용여부를 설정합니다. (설정값: 사용함/사용 안 함)
- IP 주소: DHCP 방식대신 고정IP를 사용할 경우의 IP주소를 입력합니다. 관리자에게 문의하여 입력하십시오. 기본값 127.0.0.1으로 설정되어 있습니다.
- 게이트웨이: DHCP 방식대신 고정IP를 사용할 경우의 게이트웨이 주소를 입력합니다. 관리자에게 문의하여 입력하십시오.
- 서브넷마스크: DHCP 방식대신 고정IP를 사용할 경우의 서브넷마스크 주소를 입력합니다. 관리자에게 문의하여 입력하십시오.

3장. 관리자 기능

서버 설정하기

단말기는 BioStar 서버 또는 SDK 서버와 통신할 수 있습니다. 단말기에 연결할 서버의 IP와 포트를 설정해야 합니다.



1. [관리자메뉴]에 들어간 후, [서버설정]을 선택합니다.

2. 서버 정보를 설정한 후 [저장]을 누릅니다.

- 서버: 호스트 서버를 사용할 것인지를 설정합니다. 서버에 접속하지 않고 BioStar Client에서 D-station을 직접 접속하기 위해서는 '서버-사용안함'으로 설정되어야 합니다.
- 서버IP: 호스트 서버의 IP를 입력합니다.
- 포트: 호스트 서버의 포트를 입력합니다.

3. 설정 확인창이 나타납니다.

- 이 과정을 수행하면 서버에 접속된 BioStar Client 프로그램 상에 해당 D-Station이 나타납니다.

3장. 관리자 기능

시리얼 설정하기

단말기에 BioStar 또는 PC 등을 연결하여 통신할 경우, 통신 방식과 속도 등을 설정합니다.

1. [관리자메뉴]에 들어간 후, [시리얼 설정]을 선택합니다.

2. 시리얼 정보를 설정한 후 [저장]을 누릅니다.

- RS485 : 단말기와 PC간 RS485 방식으로 통신시의 속도를 설정합니다. 설정값(사용안함 /9600/19200/38400/57600/ 115200)

- 초기설정값은 '115200'으로 설정되어 있으나, 통신 오류 발생시 낮은 속도로 변경할 수도 있습니다.

- RS485 포트는 단말기의 뒷면에 있습니다.

- RS485 Mode : RS485통신에서 통신환경을 설정합니다. (설정값: 사용안함/ Net-Slave/ Net-Host)
  단말기간 RS485 통신은 1대의 Server 단말기와 총 7대까지의 Slave 단말기로 구성이 가능합니다.

- Net-Slave: 여러 대의 단말기를 연결할 때, 해당 단말기를 Slave로 설정.

- Net-Host: 여러 대의 단말기를 연결할 때, 해당 단말기를 Host로 설정.

- RS232: 단말기와 PC간 RS232 방식으로 통신시의 속도를 설정합니다.

- 단말기 뒷면의 9핀 커넥터를 이용해 RS232로 PC와 연결할 때 사용합니다.

3. 설정 확인창이 나타납니다.

3장. 관리자 기능

USB 사용하기

단말기에 USB 메모리를 연결하여 사용할 경우에만 USB 포트를 '사용함'으로 설정합니다.

주의
단말기의 하단에 있는 USB 포트는 PC 와 연결할 때 사용합니다. 보안으로 인해 공장출하시에는 '사용안함'으로 설정되어 있습니다. 단말기와 PC 간을 USB 로 연결할 경우에는 반드시 '사용함'으로 변경해야 합니다.

1. [관리자메뉴]에 들어간 후, [USB 사용]을 선택합니다.

2. USB 사용여부를 선택한 후 [저장]을 누릅니다.
- 사용함: USB 포트를 이용하여 PC와 연결할 경우
- 사용안함: 평상시 단말기를 작동할 경우

3. 설정 확인창이 나타납니다.

3장. 관리자 기능

USB 메모리 사용하기

단말기에 저장되어 있는 사용자정보, 로그데이터를 USB 메모리에 저장해서 가져오거나 내보낼 수 있습니다. 또한, USB 메모리에 저장되어 있는 각종 정보를 단말기에 가져올 수도 있습니다. 이 기능은 주기적으로 PC의 BioStar 프로그램과 데이터를 교환할 때 유용합니다.

제품 설치후 단말기의 하단에 있는 USB 포트에 PC를 연결하여 사용하려면, 먼저 'USB 사용하기'를 참고하여 USB 포트를 '사용함'으로 설정해야 합니다.

USB 설정을 수행하기 전에 USB 포트에 USB 메모리를 삽입해야 합니다.

주의

가져오기를 수행하면, 기존의 단말기에 있던 사용자 정보와 설정값을 모두 덮어쓰게 됩니다.

1. [관리자메뉴]에 들어간 후, [USB 메모리]를 선택합니다.

2. 가져오기, 내보내기, 업그레이드 중 원하는 항목을 선택합니다. 사용자 정보와 데이터 량에 따라 몇 초에서 수십분의 시간이 소요될 수 있습니다.

- 가져오기: USB 메모리에 저장되어 있는 사용자 정보와 각종 설정값을 단말기에 복사합니다.
- 내보내기: 단말기의 사용자 정보와 각종 설정값을 USB 메모리에 저장합니다.
- 업그레이드: USB 메모리에 저장되어 있는 펌웨어를 이용하여 현재 단말기의 펌웨어를 업그레이드합니다.

■ 가져오기 (예)

- 파일 목록중 가져올 이름을 선택하면, USB 메모리에 저장되어 있는 사용자정보, 로그데이터 등을 단말기로 가져옵니다.

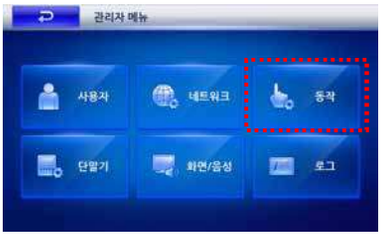
3장. 관리자 기능

3.5 동작 관리하기

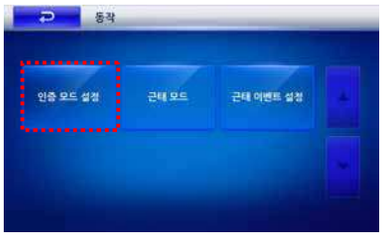
단말기의 동작상태, 근태관리, 출입통제 등을 설정할 수 있습니다.

인증 모드 설정하기

1. [관리자메뉴]에 들어간 후, [동작]을 선택합니다.



2. 오른쪽의 화면이 나타나면 [인증 모드 설정]을 선택합니다.



3. 적용할 인증 모드를 설정하고 [▾]를 선택합니다.

- 센서 모드: 사용자 인증시 2개의 지문센서와 CPU가 작동하는 운용 모드를 선택합니다. (설정값: 패스트 모드/ 퓨전 모드/ 트윈 모드)

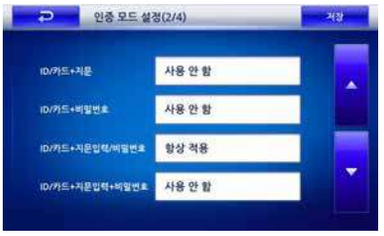
- 패스트 모드: 1개의 지문 입력에 대하여 2개의 내부 CPU가 동시에 인증 처리하는 모드입니다. 인증 속도가 2배 이상 빨리 처리됩니다.
- 퓨전 모드: 2개의 손가락 지문에 대한 퓨전 알고리즘에 의하여 인증 처리하는 모드입니다. 1개 혹은 2개의 손가락을 동시에 입력이 가능합니다. 각각의 지문의 인증율이 낮은 사용자의 경우 다른 인증모드를 사용하면 인증 실패되기 쉬우나, 퓨전 인증을 사용하면 특성의 합으로 인증율이 높아집니다.
- 트윈 모드: 2개의 센서가 독립적으로 작동하여 인증 처리하는 모드입니다. 1대의 D-Station으로 동시에 2명을 인증 처리할 수 있습니다.
- Demo Mode: 얼굴 퓨전 인증을 테스트 하기 위해 지원하는 테스트 모드입니다. 얼굴이 일치하지 않아도 지문만 일치하면 인증 성공이 됩니다. 실제 운영 모드에서는 사용하지 마십시오.

- 강제 얼굴 검출: 사용자 인증시 얼굴의 촬영여부를 선택합니다. 인증이 성공한 경우 얼굴 영상을 강제로 검출하여 출입한 사용자에 대한 얼굴 영상을 로그로 저장합니다.
- 얼굴 퓨전: 현재 설정된 인증 모드에 얼굴 영상까지 포함하여 운용하는 모드입니다. 지문 인식만으로 인증율이 낮은 사용자의 경우는 인증 성공율을 높이는 효과가 있습니다.

- 얼굴 퓨전을 적용할 수 있는 인증 방식은 패스트 모드, 퓨전 모드 2가지가 있습니다. '패스트 모드 + 얼굴 퓨전' , '퓨전 모드 + 얼굴 퓨전'과 같이 조합하여 사용할 수 있습니다.
  - 퓨전 대기 시간: 퓨전 모드로 운용 시, 퓨전 인증 수행에 필요한 전체 소요시간에 대한 Time-out을 의미합니다

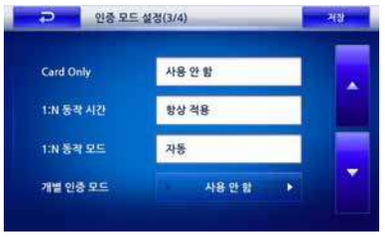
4. 출입 인증 모드를 설정하고 [▾]를 선택합니다. 5가지 인증모드 중 한가지만 '항상 적용'으로 선택하고 나머지 4가지는 '사용 안함'으로 선택해야 합니다.
   - ID/카드+지문: 인증시 ID/카드와 지문을 순차적으로 입력받는 방식입니다.
   - ID/카드+비밀번호: 인증시 ID/카드와 비밀번호를 순차적으로 입력받는 방식입니다.
   - ID/카드+지문입력/비밀번호: 인증시 ID/카드를 입력받고 지문 또는 비밀번호 중 한 가지를 입력받는 방식입니다.
   - ID/카드+지문입력+비밀번호: 인증시 ID/카드, 지문, 비밀번호를 순차적으로 모두 입력받는 방식입니다.
   - Card Only: 인증시 카드만 입력받는 방식입니다. 이 경우, [카드 사용]에서 카드 타입을 설정해야 합니다.
   - 인증 모드 설정값

   - 기본 출입 시간: 항상 적용/ 사용안함



5. 인증 모드를 설정하고 [▾]를 선택합니다.
   - 1:N 동작 시간: 지문만 사용해서 인증할 수 있는 1:N 인증 모드가 작동하는 스케줄을 설정합니다. (설정값: 항상 적용/ 사용안함 / BioStar에서 생성한 출입시간)

   - '항상 적용'으로 설정한 경우, BioStar 프로그램의 출입통제 메뉴에서 미리 출입시간을 설정해 두어야 합니다.
   - 1:N 동작 모드: 지문만 사용해서 인증할 수 있는 1:N 인증 모드 동작을 설정합니다.(설정값: 사용 안 함/ 자동/ 근태기능키)
   - 개별 인증 모드: 개인에게 설정된 인증방식을 사용하는 인증 방식 사용 여부를 선택합니다. (설정값: 사용 안 함/ 사용함)



3장. 관리자 기능

6. 인증 모드를 설정하고 [저장]을 누릅니다.

- 이중 인증: 이중 인증의 사용 여부를 선택합니다. (설정값: 사용안함/사용)

- '사용'으로 설정한 경우, 다른 두사람의 지문이나 카드가 15초 이내 연속해서 입력되어야 인증됩니다. 첫번째 사용자는 정상적으로 인증되지만, 출입문은 열리지 않습니다. 15초 이내 추가 인증이 없으면 첫번째 인증은 무효가 되며 다시 두 사람의 인증이 필요합니다.

- 카드 사용: 인증시 사용되는 카드 타입을 선택합니다.
  (설정값: 사용안함/ 템플릿 사용 / CSN)

- 템플릿 카드: 사용자 정보와 지문정보를 카드에 직접 저장합니다

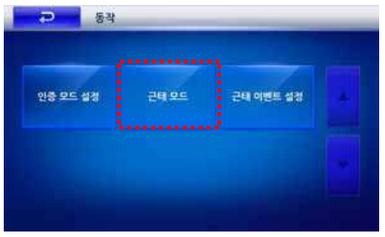
- CSN: 각 사용자에게 할당된 편집할 수 없는 카드 일련번호 (CSN)를 저장합니다. CSN값을 직접 입력할 수 있습니다.

7. 설정 확인창이 나타납니다

근태 모드 설정하기

사용자가 출입문에서 단말기에 입력하는 근태 입력 방식을 설정합니다.

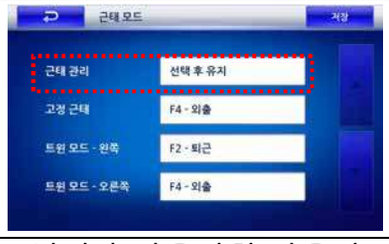
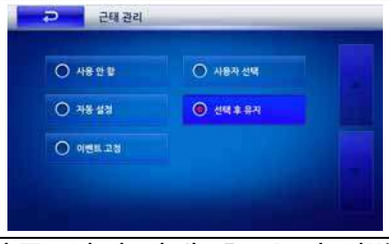
1. [관리자메뉴] ▸ [동작]에 들어간 후, [근태모드]를 선택합니다.



2. [근태모드]의 항목을 선택한 후 기능키 사용방식을 설정합니다.

3장. 관리자 기능

■ 근태 관리

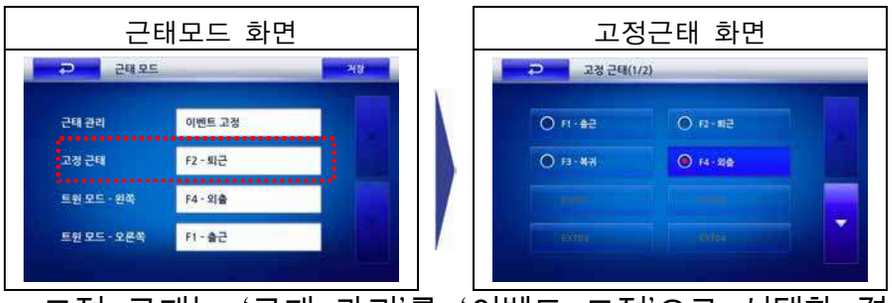
근태모드 화면	근태관리 화면
	

- 설정값(사용안함/사용자 선택/자동 설정/선택 후 유지/이벤트 고정)
  - 사용자 선택: 평상시에는 근태 기능이 비활성화되어 있다가 기능키가 눌리면 근태 상태를 선택할 수 있게 됩니다. 이때 사용자 인증이 성공하면 선택한 근태 상태 로그가 기록됩니다.

3장. 관리자 기능

- 자동 설정: '자동 설정'은 출근시 또는 외근 시와 같이 근태관리의 이벤트 종류와 시간대를 BioStar에서 설정해 둔 상태에서, 출입하는 모든 사용자에게 일괄적으로 적용할 경우에 편리한 방법입니다.
  '자동 설정'의 경우 BioStar에서 근태 이벤트 별로 해당하는 시간대를 설정할 수 있습니다. 미리 지정된 시간대별로 활성화되어 있는 근태 상태가 기록됩니다.
- 선택 후 유지: 화면에 근태 상태가 활성화되어 나타나며, 기능키를 눌러 변경할 수 있습니다. 한 번 변경한 후에는 다른 선택을 하기 전까지 계속 그 상태를 유지하며 인증 성공 시 마다 근태 로그가 기록됩니다.
  '선택 후 유지'는 출근시 또는 외근 시와 같이 근태관리의 이벤트 종류를 변경한 이후에 출입하는 모든 사용자에게 일괄적으로 적용할 경우에 편리한 방법입니다.
- 이벤트 고정: 특정 근태 상태를 유지하며, 사용자 인증이 성공하면 해당 근태 로그가 기록됩니다. 고정으로 설정된 경우에는 다른 기능키 입력은 무시됩니다.
- 근태F1~EXT12 중에서 한가지를 선택합니다. 근태F1~EXT12 의 설정값은 BioStar 프로그램에서 미리 설정해 두어야 합니다.

■ 고정 근태



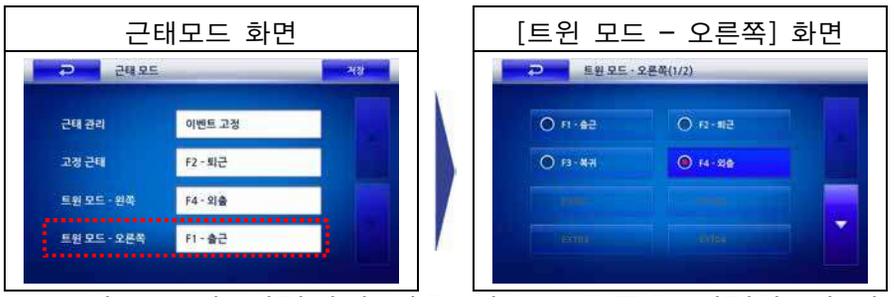
- 고정 근태는 '근태 관리'를 '이벤트 고정'으로 선택한 경우에 인증 시 고정으로 사용할 근태를 선택합니다. F1~EXT12 까지 선택가능합니다.

■ 트윈 모드 – 왼쪽

- 트윈 모드가 설정되어 있을 경우 왼쪽을 선택할 때 사용할 설정키를 설정합니다.
- '근태 관리'를 '이벤트 고정'으로 선택하고, 센서 모드가 트윈 모드인 경우, 사용자가 왼쪽 지문인식부에 인증 시 고정으로 사용할 근태를 선택합니다.
- F1~EXT12 까지 선택가능합니다.

3장. 관리자 기능

■ 트윈 모드 – 오른쪽



- 트윈 모드가 설정되어 있을 경우 오른쪽을 선택할 때 사용할 설정키를 설정합니다.
- '근태 관리'를 '이벤트 고정'으로 선택하고, 센서 모드가 트윈 모드인 경우, 사용자가 오른쪽 지문인식부에 인증 시 고정으로 사용할 근태를 선택합니다.
- F1~EXT12 까지 선택가능합니다.

3. 설정이 끝나면 [저장]을 누릅니다.

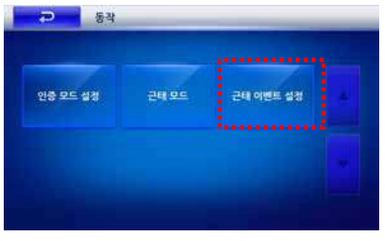
4. 확인창이 나타납니다.

근태 이벤트 확인하기

근태 이벤트는 BioStar를 이용하여 F1~F4 또는 EXT01~12 키에 해당하는 표시 내용과 자동 적용시간을 설정할 수 있습니다.

해당 내용을 근태 이벤트 설정 화면에서 확인할 수 있습니다. 단말기에서는 추가, 변경 및 삭제가 불가능합니다.

1. [관리자메뉴] ▸ [동작]에 들어간 후, [근태 이벤트 설정]을 선택합니다.



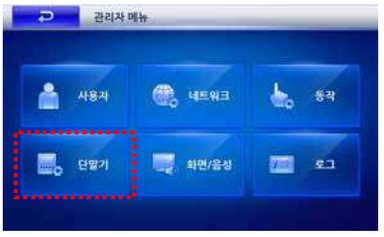
2. [▾]/ [▴]을 이용하여 Biostar에서 설정한 시간을 확인할 수 있습니다. (설정값: F1~F4, EXT01~12)
   - 근태모드가 '자동 설정'이고, 자동 적용 시간이 '사용함'으로 설정되어 있으면, 해당시간에 자동으로 선택한 근태기능키가 적용됩니다.

3.6 단말기 관리하기

단말기의 기본적인 동작상태, 근태관리 및 출입통제 등을 설정합니다.

지문 인증 설정하기

1. [관리자메뉴]에 들어간 후, [단말기]를 선택합니다.

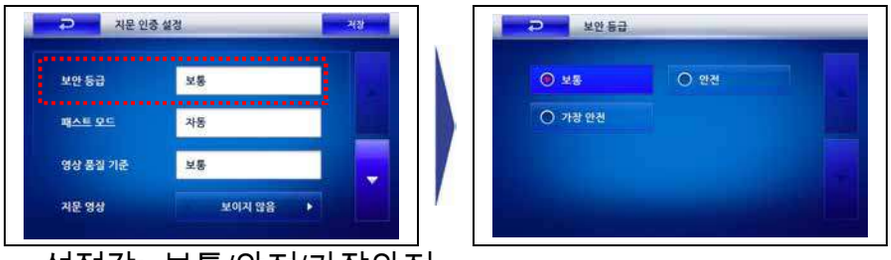


2. 오른쪽의 화면이 나타나면, [지문 인증 설정]을 선택합니다.

3. 지문 인증의 세부 항목을 설정합니다.

■ 보안등급

지문 인증으로 출입할 경우의 지문 인식률에 대한 보안 등급입니다.

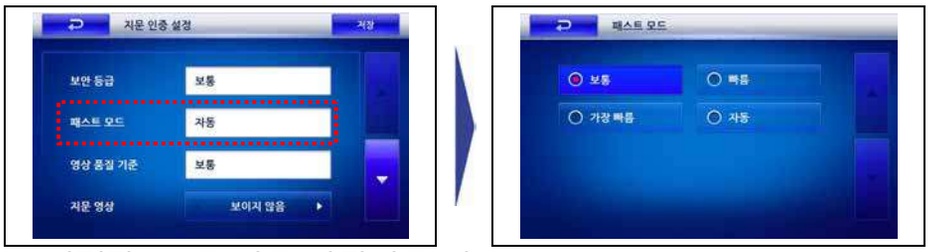


- 설정값: 보통/안전/가장안전
  - 보안등급은 타인오인식률(FAR, False Acceptance Ratio)에 의해 결정됩니다. 보안 등급이 낮으면 사용자 인식은 잘 되고, 보안 등급이 높으면 아주 정확하게 지문을 입력해야 인식됩니다. 따라서, 엄격한 출입통제 보안이 요구되는 경우 '안전'이나 '가장 안전'을 선택하고, 일반적인 경우에는 '보통'을 선택합니다.

3장. 관리자 기능

■ 패스트 모드

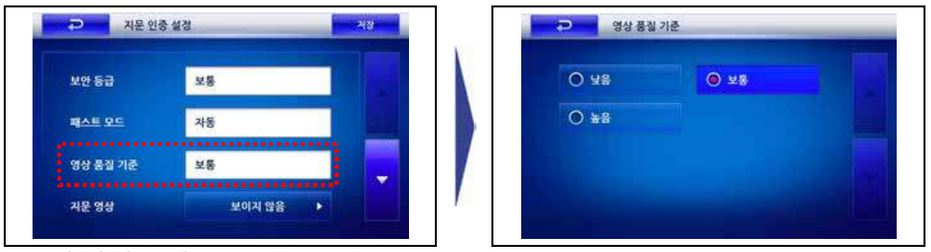
지문 인증으로 출입할 경우의 사용자의 인식속도를 선택합니다.



- 설정값: 보통/빠름/가장빠름/자동
  - 사용자 정보가 수 백명 이상의 경우, 인식속도를 빠르게 설정하면 인식시간이 빠르지만 본인거부율(FRR, False Reject Rate)은 높아질 수 있습니다. '자동'을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.

■ 영상 품질 기준

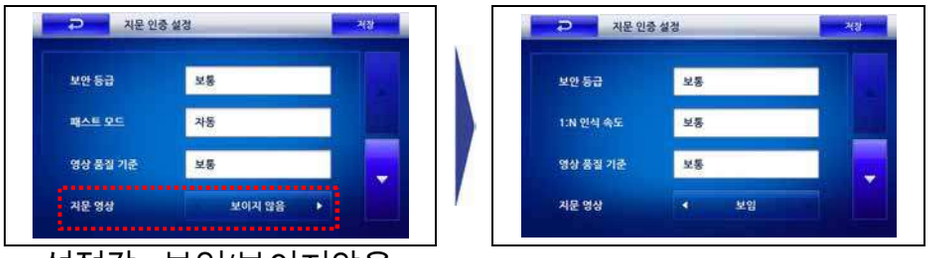
인증시 입력된 지문의 품질에 대한 기준을 선택합니다.



- 설정값: 낮음/보통/높음
  - 만일, '낮음'으로 설정할 경우 지문 인증이 잘 되지 않는 사용자도 쉽게 인증됩니다.

■ 지문 영상

지문 등록시 사용자의 지문을 화면에 표시할 것인지를 선택합니다.



- 설정값: 보임/보이지않음
  - '보임'으로 설정할 경우, 사용자는 LCD화면에서 확인할 수 있어 지문을 올바로 입력할 수 있습니다.

3장. 관리자 기능

4. [▾]을 눌러 세부 항목을 설정합니다.

- 센서 감도: 지문센서가 손가락을 읽어들이는 감도를 설정합니다. 최대 7단계로 설정할 수 있습니다.

- 높은 감도에서는 지문 입력이 쉽고, 낮은 감도에서는 입력된 지문 영상이 항상 높은 품질을 유지할 수 있는 장점이 있습니다. 일반적인 사용 환경에서는 최대값으로 설정할 것을 권장합니다. 광학식 모델의 경우에는 직사광선의 영향을 받을 경우 이 값을 낮게함으로서 영향을 완화시킬 수 있습니다.

- 지문 입력 시간(초): 지문 입력을 위해 대기하는 시간을 초단위로 설정합니다. (설정값: 1/…20)

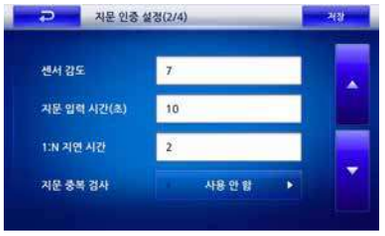
- 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.

- 1:N 지연 시간: 지문을 인증하는 동안 지문 입력을 대기하는 시간(0초-10초)을 설정합니다. (설정값: 1/…10)

- 지연 시간을 설정함으로써 사용자가 지문 스캐너에서 손가락을 떼지 않더라도 같은 지문이 계속해서 인증되는 것을 방지할 수 있습니다.

- 지문 중복 검사: 지문 등록시 등록하는 지문이 이미 등록되어 있는 지문인지 중복검사하여 중복 여부를 표시합니다. (설정값: 사용안함/ 사용함)

- 장치가 입력된 지문을 이미 등록되어 있는 것으로 판단하면 등록과정을 취소합니다.



5. [▾]을 눌러 세부 항목을 설정합니다.

- 1:N 인식 속도: 지문 인증으로 출입할 경우의 사용자의 인식속도를 선택합니다.
  (설정값: 1/2/3/…/19/20)

- 매칭 시간내 일치한 지문을 찾지못하면 인증실패로 처리됩니다.

- 위조지문 감지: 위조지문감지의 사용여부를 선택합니다. (설정값: 사용안함/사용함)

- 서버 매칭: 지문입력시 서버에 등록된 지문과 비교할 것인지를 선택합니다. (설정값: 사용안함/사용함)

6. [▾]을 눌러 세부 항목을 설정합니다.

- SIF: ISO/IEC 호환 데이터 포맷의 사용여부를 선택합니다. (설정값: 사용안함/사용함)

- 개인 정보 보호: 사용자의 정보 보호의 사용여부를 선택합니다. (설정값: 사용안함/사용함)

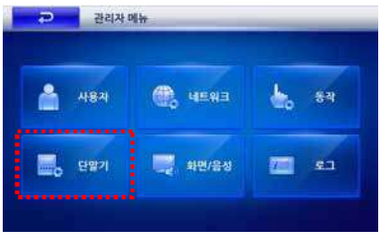
7. [저장]을 누른 후 [ ]버튼을 누릅니다.

3장. 관리자 기능

출입문 설정하기

사용자가 출입문에서 인증을 거치기 이전에 사용하는 인터폰과 릴레이 방식 및 이벤트 발생 등과 관련하여 설정합니다.

1. [관리자메뉴]에 들어간 후, [단말기]를 선택합니다.

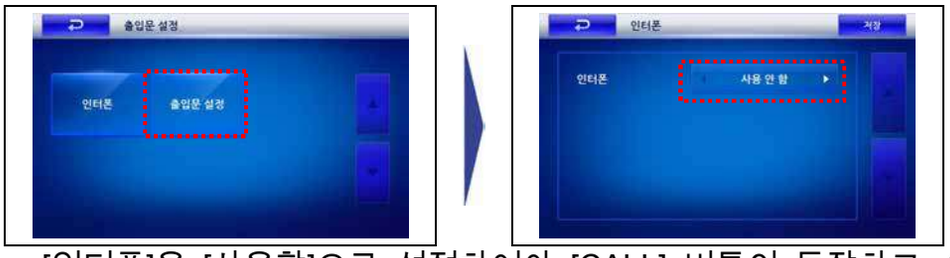


2. 오른쪽의 화면이 나타나면, [출입문 설정]을 선택합니다.

3. 인터폰과 출입문 설정을 각각 설정합니다.

■ 인터폰

[인터폰]의 사용 여부를 선택하고 [저장]을 누릅니다.



- [인터폰]을 [사용함]으로 설정하여야 [CALL] 버튼이 동작하고, 인터폰과 통화가 가능합니다.

■ 출입문 설정

① [출입문]의 세부 항목을 설정하고 [▾]을 누릅니다.

- 릴레이: 사용자 인증시 출입문을 개방할 릴레이를 선택합니다. (설정값: 사용안함/ 내부릴레이 0/ 내부릴레이 1/외부릴레이 0/ 외부릴레이 1/SIO0 릴레이0/SIO0 릴레이1/SIO1 릴레이0/SIO1 릴레이1/SIO2 릴레이0/SIO2 릴레이1/SIO3 릴레이0/SIO3 릴레이1)
  - 초기설정값: 사용안함

3장. 관리자 기능

- 문 열림 이벤트: 출입문을 개방할 이벤트를 선택합니다. (설정값: 모든이벤트/인증+근태이벤트/인증 이벤트/근태 이벤트/사용안함)

3장. 관리자 기능

- 모든이벤트: 모든 인증 성공 이벤트(1:1 비밀번호인증, 1:1 지문인증, 1:1 지문인식)에 대해 출입문을 열립니다.
- 인증+근태이벤트: 근태이벤트 중 출입문 사용이 선택된 이벤트에 대해서만 출입문이 열립니다. 근태이벤트 없이 인증된 경우에도 출입문이 열립니다.
- 근태 이벤트: 근태이벤트 중 출입문사용이 선택된 특정이벤트에 대해서만 출입문이 열립니다.
- 인증 이벤트: 근태이벤트 없이 인증된 경우만 출입문이 열립니다.
- 사용안함: 어떤 인증 및 이벤트에 대해서도 출입문이 열리지 않습니다.

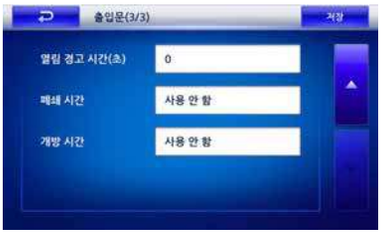
• 문 열림 시간(초): 이벤트가 발생으로 출입문의 개방 시간을 설정합니다. 설정한 시간 이후에는 다시 출입문이 닫힙니다.
• 단말기 ID: 안쪽에서 출입할 때 사용되는 단말기ID를 입력합니다. (설정값: 0/ 단말기ID)

② [▾]을 누른 후 다음 항목을 설정합니다.

• 문 열림 SW: 문 열림 스위치의 사용여부를 선택합니다. (설정값: 사용 안함, 입력0, 입력1, SIO0 입력0~3, SIO1 입력0~3, SIO2 입력0~3, SIO3 입력0~3)
• 입력방식: 문 열림 스위치의 작동 방식을 선택합니다. (설정값: N/O, N/C)
• 문 열림 감지: 출입문의 개방될 경우, 감지하는 방법을 선택합니다. (설정값: 사용 안함, 입력0, 입력1, SIO0 입력0~3, SIO1 입력0~3, SIO2 입력0~3, SIO3 입력0~3)
• 입력: (설정값: N/O, N/C)

③ [▾]을 누른 후 다음 항목을 설정합니다.

• 열림 경고 시간(초): 출입문이 개방된 이후 경고음을 울릴 시간을 설정합니다.
• 폐쇄 시간: 출입문을 강제로 잠궈 놓을 시간을 설정합니다. (설정값: 사용 안 함/항상 적용)
- 폐쇄 시간에는 일반사용자는 출입할 수 없고 관리자만 출입할 수 있습니다. 폐쇄 시간은 BioStar 프로그램에서만 설정할 수 있습니다.
• 개방 시간: 출입문을 강제로 열어 놓을 시간을 설정합니다.
- 설정값: 사용 안 함/항상 적용
(개방 시간 동안에는 어떠한 이벤트가 발생하더라도 출입문이 닫히지 않습니다.)
- 개방 시간은 BioStar 프로그램에서만 설정할 수 있습니다.



④ [저장]을 누른 후 [ ]버튼을 누릅니다.

3장. 관리자 기능

카메라 설정하기

출입문에서 사용자 인증시 카메라의 사용여부를 조회할 수 있습니다. 설정은 BioStar에서만 가능하고, 단말기에서는 조회만 가능합니다.

1. [관리자메뉴]에 들어간 후, [단말기]를 선택합니다.

2. 오른쪽의 화면이 나타나면, [카메라 설정]을 선택합니다.

3. 현재 설정되어 있는 [카메라 이벤트] 화면이 나타납니다.
종료하려면 [ ]버튼을 누릅니다.

시간 설정하기

단말기에 표시되는 시간을 설정합니다. 단말기 시간을 설정해야 출입시간과 로그데이터가 정확하게 저장됩니다.

1. [관리자메뉴] ▸ [단말기]에 들어간 후, [시간 설정]을 선택합니다.

2. 오른쪽의 화면이 나타나면, 세부항목을 설정한 후 [저장]을 선택합니다.

- 날짜: 현재의 날짜를 입력합니다.(YYYYMMDD)
- 시간: 현재의 시간을 입력합니다.(hhmmss)
- 시간 동기화: 단말기의 시간 기준을 선택합니다. (설정값: 사용안함/서버동기화)
  - 사용안함: 단말기에 설정한 시간을 기준합니다.
  - 서버동기화: 서버 시간에 단말기의 시간을 맞춥니다.
- 날짜 형식: 표시할 날짜 형식을 선택합니다. (MM/DD 또는DD/MM)

3장. 관리자 기능

단말기 관리하기

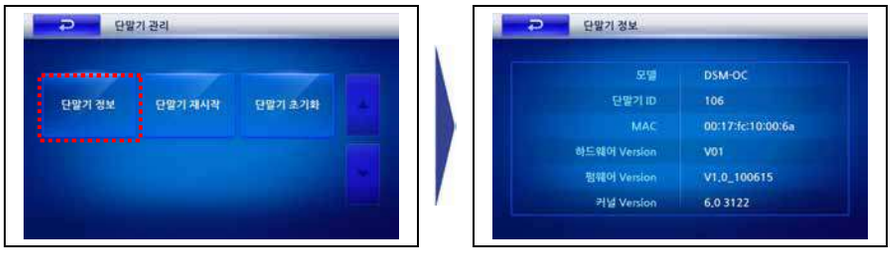
단말기 정보를 확인하거나 단말기 재시작 또는 단말기 초기화를 수행합니다.

1. [관리자메뉴] ▸ [단말기] 에 들어간 후, [단말기 관리]를 선택합니다.

2. 오른쪽의 단말기 관리 화면이 나타나면, 원하는 항목을 선택합니다.

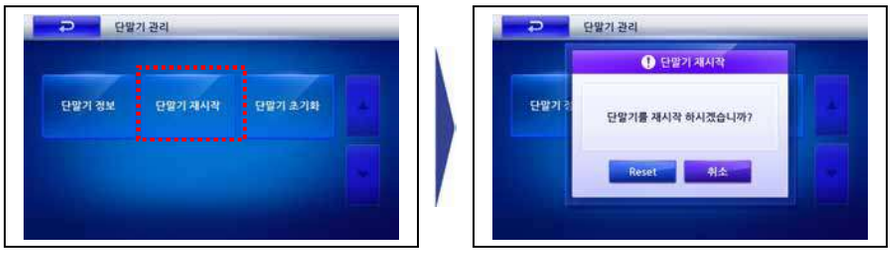
■ 단말기 정보

단말기의 모델명, 하드웨어 버전 등의 기본적인 정보를 보여줍니다.



■ 단말기 재시작

단말기의 불안정한 작동 등이 있을 경우, 단말기를 재시작합니다.

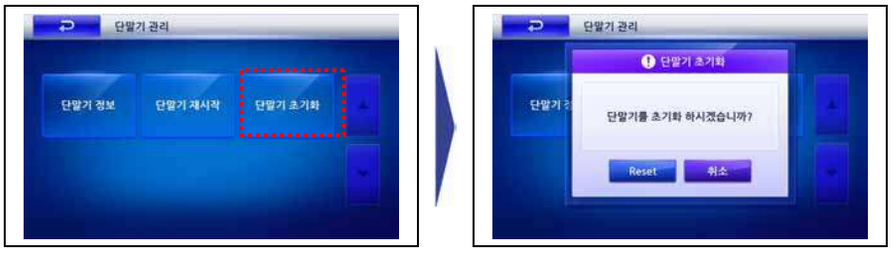


주의

단말기 초기화를 수행하면 단말기의 각종 설정값과 BioStar프로그램을 이용해 새로 다운로드한 배경화면, 효과음, 공지사항 등의 모든 정보가 삭제되므로 주의하십시오.

■ 단말기 초기화

단말기의 모든 설정값을 공장출하상태의 초기값으로 복원합니다.



참고

단말기 초기화를 수행하더라도 등록한 사용자 정보와 로그데이터는 삭제되지 않습니다. 사용자정보를 삭제하려면 29페이지 〈사용자삭제하기〉를, 로그데이터를 삭제하려면 53페이지 〈로그초기화〉를 참조하십시오.

3장. 관리자 기능

메모리 상태 확인하기

단말기의 메모리 사용 현황을 확인합니다.

1. [관리자메뉴] ▸ [단말기] 에 들어간 후, [메모리 상태]를 선택합니다.

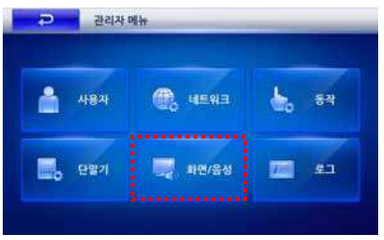
2. 현재 단말기에서 사용중인 메모리 현황을 확인할 수 있습니다.

3.7 화면/음성 관리하기

단말기의 배경화면, 효과음 볼륨 등을 설정합니다.

화면/음성 설정하기

1. [관리자메뉴]에 들어간 후, [화면/음성]을 선택합니다.

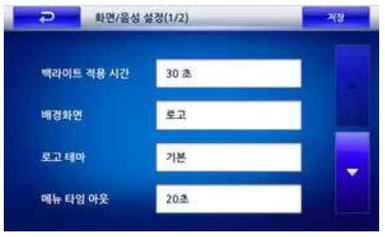


2. [▾]을 눌러 세부 항목을 설정합니다.

- 백라이트 적용 시간: 설정한 시간 동안 키 입력이 없을 경우, 백라이트가 꺼지는 시간입니다.(설정값: 무한대/10초~60초)
- 배경화면: 초기화면에 표시할 배경을 선택합니다. (설정값: 로고/공지사항)

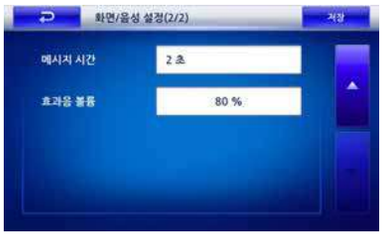
- 배경 이미지는 BioStar 프로그램을 이용하여 업로드 할 수 있습니다.

- 로고테마: 배경화면에 사용할 테마를 선택합니다.(설정값: 테마 1~20/ 기본/ 사용자 정의)
- 메뉴 타임아웃: 설정한 시간 동안 키 입력이 없을 경우, 초기화면으로 이동합니다. (설정값: 무한대/10초/20초/30초)



3. [▾]을 눌러 세부 항목을 설정합니다.

- 메시지 시간: 인증시 화면에 나타나는 메시지가 표시되는 시간입니다.(설정값: 0.5초/1초/2초/3초/4초/5초)
- 효과음 볼륨: 효과음이 발생할 때의 크기입니다. (설정값: 0%/10%/20%/…/100%) 0%로 설정하면 효과음이 출력되지 않습니다.



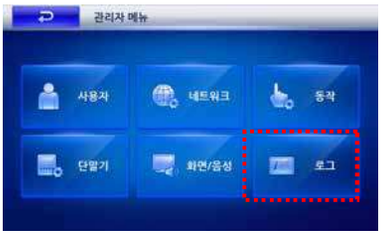
4. [저장]을 누른 후 [ ]버튼을 누릅니다.

3.8 로그 관리하기

단말기에 기록된 출입, 근태 정보를 확인하고 삭제할 수 있습니다.

로그 관리하기

1. [관리자메뉴]에 들어간 후, [로그]를 선택합니다.



2. [▾]을 눌러 로그를 조회하거나 [로그 필터] 또는 [로그 초기화]를 설정합니다.

■ 영상로그 View 기능

로그 목록의 [보기]를 선택하면 촬영된 영상로그를 확인할 수 있습니다.

3장. 관리자 기능

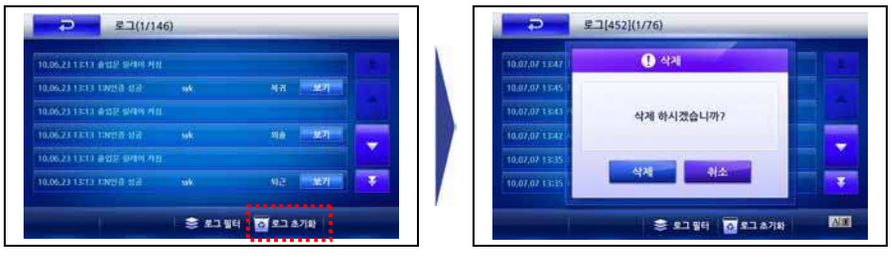
■ 로그필터

[로그 필터]를 선택한 후 이벤트, 근태이벤트, 사용자ID를 지정하여 로그 필터를 편집할 수 있습니다.

- 이벤트: 필터링할 이벤트를 지정합니다.
- 근태 이벤트: 필터링할 근태 이벤트 종류를 지정합니다.
- 사용자ID: 필터링할 사용자ID를 지정합니다. 모든 사용자로 지정하려면 ‘0’을 입력합니다.

■ 로그 초기화

[로그 초기화]를 선택하여 모든 로그를 삭제할 수 있습니다. 팝업창에서 [삭제]를 선택하면 로그 정보가 모두 삭제됩니다.



4장. 사용자 기능

4.1 출입 인증하기

설정된 인증 모드에 따라 지문/카드/ID/비밀번호 입력을 통해 출입할 수 있습니다.

1 : N 지문 인식을 이용해 출입하기

1:N 인식모드가 자동 또는 근태기능키로 설정되어 있을 때, 지문만으로 출입문을 여는 방법입니다.

1. 1:N 인식모드가 자동으로 설정되어 있을 때

- 아무런 키를 누르지 않고도 지문을 입력하면 출입 인증 메시지가 나타나며 출입문이 열립니다.

2. 1:N 인식모드가 근태기능키로 설정되어 있을 때

- 설정된 근태기능키를 누르면 파란색 LED가 깜빡이고 이때 정해진 시간 안에 등록된 지문을 입력하면 출입문이 열립니다.

1 : 1 인증을 이용해 출입하기

ID를 먼저 입력한 후, 지문 또는 비밀번호를 입력해 출입문을 여는 방법입니다.

1:1 인증모드	ID 입력방법	인증방법
지문 또는 비밀번호	ID 또는 카드 제시	지문인증 또는 비밀번호 입력
지문	ID 또는 카드 제시	지문 인증
비밀번호	ID 또는 카드 제시	비밀번호 입력
Card Only	카드 인증	
지문 그리고 비밀번호	ID 또는 카드 제시	지문인증 후 비밀번호 입력

1. 1:1 인증모드가 지문일 경우

- 지문을 입력하면 출입문을 열 수 있습니다.

2. 1:1 인증모드가 비밀번호일 경우

- 등록한 비밀번호를 입력하면 출입문을 열 수 있습니다.

3. 1:1 인증모드가 지문 또는 비밀번호일 경우

- 지문을 입력하거나 비밀번호를 입력하면 출입문을 열 수 있습니다.

4. 1:1 인증시 RF카드를 사용하는 경우

- 1:1인증모드에서 ‘Card Only’인 경우, 카드를 이용해서 별도의 지문이나 비밀번호

4장. 사용자 기능

입력없이 인증하게 됩니다.

- 1:1인증모드에서 'Card Only'가 아닌 경우, 카드는 ID 입력 역할을 하게 되고 지문이나 비밀번호를 통해서 인증하게 됩니다.

지문 인식

1:N 인식 모드가 설정되어 있을 경우 지문을 입력해 문을 여는 방법입니다.

1. 지문 인식부에 지문을 인식합니다.

2. 인증이 성공하면 문이 열리고 인증 팝업창이 나타납니다.

카드 인식하기

카드 인식은 Card only 인증모드로 설정되어 있는 경우에 사용이 가능합니다.

1. 지문 인식부에 카드를 인식합니다.

2. 인증이 성공하면 문이 열리고 인증 팝업창이 나타납니다.

4장. 사용자 기능

ID + 지문 입력하기

1:1 인증이 설정되어 있을 경우, 먼저 ID를 입력한 후 지문을 입력해 문을 여는 방법입니다.

1. 기본화면에서 [ID 입력]을 선택합니다.

2. ID 입력화면이 나타나면 화면의 번호패드를 사용해 숫자로 된 ID를 입력하고 [Enter]를 누릅니다.

3. 지문 인식부에 지문을 인식합니다.

4. 인증이 성공하면 문이 열리고 인증 팝업창이 나타납니다.

4장. 사용자 기능

ID + 비밀번호 입력하기

1:1 인증이 설정되어 있을 경우, 먼저 ID를 입력한 후 비밀번호를 입력해 문을 여는 방법입니다.

1. 기본화면에서 [ID 입력]을 선택합니다.

2. ID 입력화면이 나타나면 화면의 번호패드를 사용해 숫자로 된 ID를 입력하고 [Enter]를 누릅니다.

3. 화면의 번호패드를 사용해 비밀번호를 입력하고 [Enter]를 누릅니다.

4. 인증에 성공하면 문이 열리고 인증 팝업창이 나타납니다.

4장. 사용자 기능

얼굴 퓨전 인식

얼굴 얼굴 퓨전 인식은 1:N 인증 방식에서만 지원하며 1:1 인증 방식에는 지원되지 않습니다.

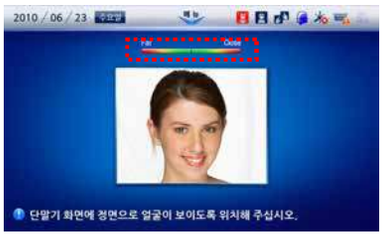
또한, 얼굴 인식만으로 사용자 인증을 지원하지 않습니다. 지문인증을 보완하는 의미의 퓨전방식으로 운용됩니다.

센서모드가 고속모드, 퓨전모드인 경우는 얼굴 퓨전을 함께 사용할 수 있습니다.

그러나 센서모드가 트윈모드인 경우는 얼굴 퓨전을 사용할 수 없습니다. (설정내용은 39p '인증 모드 설정하기'를 참조합니다.)

1. 지문 인식부에 지문을 인식합니다.

2. 지문 인식이 실패할 경우에만 오른쪽과 같이 얼굴 인식 화면이 나타납니다. 이때, 게이지의 중앙에 화살표가 오도록 거리를 조절하여 줍니다.



3. 얼굴 인식이 성공하면 인증 확인창이 표시되고 문이 열립니다.

4장. 사용자 기능

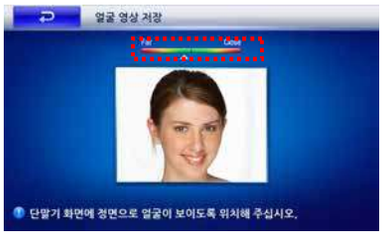
강제 얼굴 검출

강제 얼굴 검출 기능이 설정되었을 때는 인증이 성공한 경우 얼굴 영상을 강제로 검출하여 출입한 사용자에 대한 얼굴 영상을 로그로 저장합니다.
얼굴 영상이 정상적으로 저장되지 않으면, 문이 열리지 않습니다.

1. 지문 인식부에 지문을 인식합니다.

2. 지문 인증이 실패하는 경우, 인증 실패 팝업창이 뜹니다.

3. 인증이 성공한 경우에 얼굴 영상 저장 팝업창이 뜹니다. 이때, 게이지의 중앙에 화살표가 오도록 거리를 조절하여 줍니다.



4. 얼굴 저장이 완료되면, 인증확인 창이 표시되고 문이 열립니다.

4장. 사용자 기능

4.2 근태 관리하기

1:N 지문인식이나 1:1 인증을 이용해 근태관리를 할 수 있습니다.

1:N 지문인식을 이용한 근태관리

ID를 입력하지 않은 상태에서 지문만을 입력해 저장되어 있는 모든 지문 중에서 새로 입력된 지문을 검색하는 방식입니다. F1~F4키를 누른 후 정해진 시간 안에 등록된 지문을 입력하면 해당 사용자에게 설정된 근태이벤트가 적용됩니다.

문열림 이벤트가 설정된 근태이벤트로 설정되어 있고 해당 근태이벤트에 출입문열림으로 설정되어 있는 경우, 근태이벤트가 적용됨과 동시에 출입문도 열리게 됩니다.

1. 기본화면에서 [출근/퇴근/외출/외출복귀] 중에서 선택하거나 단말기의 F1~F4 키중 원하는 항목을 선택합니다.

2. 지문 인식부에 지문을 인식합니다.

3. 인증이 성공하면 출입문이 열리고 인증 팝업창이 나타납니다.

참고

근태이벤트에 출입문 열림기능을 설정하려면 PC 의 BioStar 프로그램을 사용해야 합니다.

4장. 사용자 기능

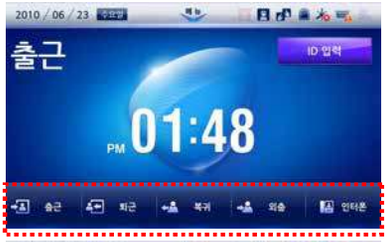
1:1 인증을 이용한 근태관리

ID를 먼저 입력하고 해당 ID에 대한 비밀번호나 지문을 입력하여 저장되어 있는 정보와 새로 입력된 정보를 1:1로 비교하는 방식입니다.

1:1 인증모드에서 “Card Only”인 경우, 카드를 이용해서 별도의 지문이나 비밀번호 입력없이 인증하게 됩니다.

1:1 인증모드에서 “Card Only”가 아닌 경우, 카드는 ID입력 역할을 하게 되고 지문이나 비밀번호를 통해서 인증하게 됩니다.

1. 기본화면에서 [출근/퇴근/외출/외출복귀] 중에서 선택하거나 단말기의 F1~F4 키중 원하는 항목을 선택합니다.



2. 기본 화면에서 [ID 입력]을 누릅니다.

3. ID 입력화면이 나타나면 화면의 번호패드를 사용해 숫자로 된 ID를 입력하고 [Enter]를 누릅니다.

4. 지문 인증이나 비밀번호 인증이 성공하면 근태 팝업창이 나타납니다.

4장. 사용자 기능

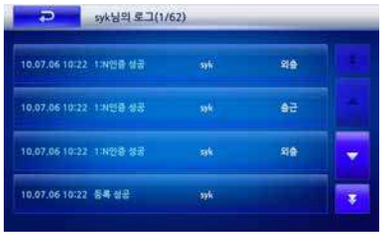
자신의 출입/근태 기록 확인하기

사용자의 지문을 입력하면 아래와 같이 본인의 출입 및 근태 기록을 볼 수 있습니다.

1. 초기화면에서 메뉴버튼()을 누릅니다.

2. 지문 또는 카드를 사용하여 사용자 인증을 합니다.

3. 인증 성공시 본인의 로그 결과가 나타납니다.



4.3 인터폰 사용하기

단말기의 인터폰 기능을 사용하여 관리자와 통화할 수 있습니다.

1. 기본화면에서 [인터폰]을 누르거나 단말기의 [CALL] 버튼을 누릅니다.

또는

2. 단말기의 스피커와 마이크를 이용해 관리자와 통화합니다.

5장. 부록

5.1 문제 해결하기

문제	해결
지문 입력이 잘안되거나 지문입력에 시간이 오래걸려요.	– 손가락이나 지문센서에 땀, 물기, 먼지 등이 묻어있는지 확인하세요. – 마른 수건 등으로 손가락과 지문센서를 닦고 다시 시도하세요. – 지문이 매우 건조할 경우 입김을 불고 다시 시도해보세요.
지문은 입력이 되지만 계속 인증에 실패해요.	– 출입그룹이나 출입시간에 의해 제한된 경우인지 확인해 보세요. – 지문이 등록되어 있는지 관리자에게 확인해 보세요.
카드가 등록되지 않아요.	– 인증 모드 설정에서 [카드 사용]으로 설정되어 있는 지 확인해 보세요. – 장치에 등록가능한 카드인지 확인하신 후 다시 등록해 보세요.
얼굴 인식이 되지 않아요.	– 얼굴 영상을 인증할 때 화면 안에 이마선과 턱선을 정확히 맞춰서 다시 인증해 보세요.
인증은 되지만 출입문이 열리지않아요.	– 폐쇄 시간으로 설정된 시간대가 아닌지 확인해 보세요. – 관리자 메뉴에서 문열림 이벤트를 확인해 보세요. 사용안함이나 선택된 근태이벤트로 설정된 경우 문이 열리지 않을 수 있습니다.
LCD 화면이 터치되지 않아요.	– LCD 화면과 파란색 LED 에 불이 꺼져있다면 전원이 공급되지 않는 상태일 수 있습니다. 정전 등의 전원공급상태를 확인해보세요. – 일시적인 기기이상이라면 단말기 하단의 리셋 버튼을 눌러 재시작합니다. 단말기를 재시작한 후에도 LCD 화면이 터치되지 않으면 제품 구매처에 A/S 를 문의하세요.
일부키가 입력되지 않거나 단말기 상태가 불안해요.	– 어떤 이유에서라도 단말기 상태가 불안해진 경우 단말기 하단의 리셋 버튼을 눌러서 재시작하세요. – 단말기를 재시작 한 후에도 작동이 되지 않을 경우 제품 구매처에 A/S 를 문의하세요.

5장. 부록

5.2 제품 규격

Item	Specification	
Sensor	Optical fingerprint sensor x 2 Face recognition camera	
Matching Speed (1:N)	1:10,000 〈 1 sec)	
Card Options	13.56 MHz ISO 14443 A/B (MIFARE)	
Capacity	Template Capacity	400,000 (1:1) 20,000 (1:N)
	Max. User	200,000
	Log Capacity	1,000,000
Interfaces	Communication Interfaces	Wireless LAN TCP/IP RS485 x 2ch, RS232 USB (Slave)
	Wiegand	IN & OUT
	TTL I/O	4 inputs
	Built-in Relay	2
	Memory Slot	USB host, Micro SD Card
Hardware	CPU	667MHz RISC x 1 400MHz DSP x 2
	Memory	1GB flash + 256MB RAM (with SD card slot)
	LCD Display	5.0" WVGA touch screen
	LED Indicator	Multi-color x 2
	Sound Indication	18-bit Hi-Fi sound
	Voice Instruction	18-bit Hi-Fi sound
	Operating Temperature	-20℃ ~ 50℃
	Humidity	90%
	Tamper	Accelerometer, switch
	Operating Voltage	12V DC
	Dimensions	148mm(W) x 204mm(H) x 48mm(D)

5장. 부록

5.3 전기적인 규격

	최소값	평균값	최대값	비고
Power				
Voltage (V)	10.8	12	13.2	제공된 전원어댑터만 사용하여야 합니다.
Current (mA)	–		1500	
Switch Input				
VIH (V)	–	TBD	–	
VIL (V)	–	TBD		
Pull-up resistance (Ω)	–	4.7K	–	입력포트는 4.7KΩ 저항으로 풀업되어 있습니다.
Wiegand Output				
VOH (V)	–	5	–	
VOL (V)	–	0.8	–	
Pull-up resistance (Ω)	–	4.7K	–	
Relay				
Switching capacity (A)	–	–	2 0.3	30V DC 125V AC
Switching power (resistive)	–	–	30W 37.5VA	DC AC
Switching voltage (V)	–	–	220 250	DC AC

5장. 부록

5.4 FCC Rules

Caution

Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interface, and (2) this device must accept any interface received, including interference that may cause undesired operation.

Information to User

This equipment has been tested and found to comply with the limit of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, user and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.
However, there is no guarantee that interference will not occur in a particular installation; if this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more the following measures:

1. Reorient / Relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help

5장. 부록

5.5 License

Copyright (c) 2010, NHN Corporation (http://www.nhncorp.com),
with Reserved Font Name Nanum, Naver Nanum, NanumGothic, Naver NanumGothic, NanumMyeongjo, Naver NanumMyeongjo

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at:
http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE
Version 1.1 - 26 February 2007

PREAMBLE
The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves.
The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works.
The fonts and derivatives, however, cannot be released under any other type of license.
The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS
"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such.
This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).
"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

5장. 부록

"Modified Version" refers to any derivative made by adding to, deleting, or substituting ? in part or in whole ?
any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS
Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

5장. 부록

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT.
IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE
OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.