suprema

BioStaion T2

고급형 지문인식 출입근태 단말기

사용 설명서



KO 102.00.BST2 V1.21

suprema

www.suprema.co.kr

BioStation T2는 지문, RFID, PIN 인증 방식을 지원하는 출입통제와 근태관리를 위한 IP 네트워크 기반의 고급형 지문인식 단말기입니다.

제품특징

5인치 터치스크린 LCD		제품 전면에 장착된 고내구성의 5인치 터치스크린 LCD를 통해 직관적인 GUI를 제공, 사용자 관리가 용이하며 근태정보, 공지사항 등의 다양한 정보의 표시가 가능합니다.
얼굴 캡처용 카메라		내장된 고성능 카메라를 통해 사용자의 얼굴 영상을 검출, 저장하여 보다 향상된 출입 보안 및 근태 관리 기능을 제공합니다.
Embedded Web Server		BioStar Lite(Embedded Web Server)를 내장하여 중소규모 시스템의 설정 및 관리가 용이합니다.
초고성능 지문인식		1:3,000 인증을 1 초 이내에 수행하며, 1:1 최대 사용자 20만 명, 1:N 최대 사용자 1만 명까지 지원합니다.
다양한 인터페이스 지원		PoE, WiFi, TCP/IP, RS485/232 등의 다양한 인터페이스를 통하여 PC 연결 및 네트워크 구성이 가능합니다. 그리고 Wiegand 및 입출력 포트를 통해서 다양한 출입 통제 시스템을 구성할 수 있습니다.
Video Phone		IP 기반의 AV 인터페이스 및 아날로그 비디오폰 기능을 제공합니다.
다양한 RF 카드 지원		EM, Mifare Classic, Mifare Plus, Mifare DesFire(CSN) 카드 지원

사용자의 안전을 지키고 재산상의 손해를 막기 위한 내용입니다. 잘 읽고 반드시 올바르게 사용해주십시오.

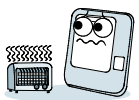
안전 주의 사항



직사광선 또는 습기나 먼지, 그을음이 많은 장소에 설치하지 마십시오.



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



화재의 위험이 있으니 전열 기구를 근처에 두지 마십시오.



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



청소 시 제품에 물을 뿌리지 마시고 부드러운 헝겊이나 수건으로 닦아주십시오.



단말기에 오랫동안 먼지가 쌓이지 않도록 자주 청소하십시오.



제품을 떨어뜨리거나 강한 충격을 가하지 마십시오.



터치스크린에 강한 자극을 주지 마십시오.



임의로 분해, 수리, 개조하지 마십시오. A/S를 받을 수 없습니다.



어린이 안전사고에 유의하여 어린이들이 기기를 함부로 만지지 못하게 하십시오.



다른 용도로 사용하지 마십시오.



기기 고장이나 기타 문제 발생시 고객센터, 가까운 서비스센터 혹은 서비스 협력사에 문의하십시오.

목차

1 사용하기 전에 6
제품 구성품 7
■ 기본 구성품 7
■ 별매품 8
각 부분의 명칭과 기능 9
■ 제품 앞면 9
■ 제품 밑면 10
■ 제품 뒷면 10
제품 크기 11
대기화면 13
인증 방법 14
올바른 지문 입력 방법 15

2 설치하기 17
설치 18
커넥터/케이블 사양 19
■ 232 케이블 (3핀 커넥터) 19
■ SWITCH 케이블 (8핀 커넥터) 19
■ 릴레이 케이블 (3핀 커넥터) 20
■ WIEGAND 케이블 (5핀 커넥터) 20
■ 전원 케이블 (2핀 커넥터) 20
■ 비디오폰 케이블 (7핀 커넥터) 21
■ RS485 케이블 (4핀 커넥터) 21

연결 22
■ 전원 연결(2핀 커넥터) 22
■ USB 케이블 연결 23
■ 이더넷 연결(이더넷 케이블) 24
■ 이더넷 연결 (PC와 직접 연결) 25
■ PoE 허브 연결 26
■ 무선랜 연결 27
■ USB 메모리 연결 28
■ RS485 PC연결(4핀 커넥터) 29
■ RS485 Secure I/O 및 다른 단말기와 연결(4핀 커넥터) 30
■ RS232 연결 31
■ 비디오폰 연결 32
■ 릴레이 연결-Fail safe lock(3핀 커넥터) 33
■ 릴레이 연결-Fail secure lock(3핀 커넥터) 33
■ 릴레이 연결-자동문(3핀 커넥터) 35
■ TTL Switch 입력 연결(8핀 커넥터) 36
■ Wiegand 입력(5핀 커넥터) 37
■ Wiegand 출력(5핀 커넥터) 37
시스템 구성도 38
■ 독립형 38
■ 보안형(Secure I/O 사용) 38
■ 네트워크 구성 39

3 사용자 메뉴 40
출입 인증 41
지문 인증 41
■ 지문만으로 인증하기 41
■ 지문+비밀번호 인증 41
■ 근태키+지문 인증 41
■ 근태키+지문+비밀번호 인증 42
카드 인증 42
■ 카드만으로 인증하기 42
■ 카드+비밀번호 인증 43
■ 카드+지문 인증 43
■ 카드+지문/비밀번호 인증 44
■ 카드+지문+비밀번호 인증 44
ID 인증 45
■ 아이디+비밀번호 인증 45
■ 아이디+지문 인증 45
■ 아이디+지문/비밀번호 인증 46
■ 아이디+지문+비밀번호 인증 46
근태 인증 47
■ 근태 모드 설정 47
■ 근태 인증 방법 48
■ 근태 이벤트 48
■ 개인별 출입/근태 기록 확인 48
인증에 실패하는 경우 49

4 관리자 메뉴 50
관리자 등록 51
■ 관리자 메뉴 진입 52

■ 관리자 메뉴 구성 53
사용자 등록 과정 55
단말기에 사용자 등록 56
■ 신규 등록 57
■ 사용자 편집 및 삭제 60
■ 사용자 검색 61
■ 사용자 등록현황 확인 62
■ 사용자 전체 삭제 62
카드에 사용자 등록 63
■ 템플릿 카드 발급 63
■ 카드 포맷 64
네트워크 설정 65
■ TCP/IP설정 65
■ 서버 설정 66
■ 시리얼통신 66
■ USB 67
■ USB 메모리 67
■ 무선랜 68
동작 모드 69
■ 지문 인증 69
■ 카드 인증 69
■ ID 인증 70
■ 동작 70
■ 근태관리 71
■ 근태 이벤트 72
■ 카메라 이벤트 72
단말기 설정 73
■ 지문 설정 73
■ 출입문 74
■ 인터폰 설정 75
■ 시간 설정 76
■ 단말기 정보 76
■ 메모리 현황 76
■ 화면보정 77
■ 터치 키패드 보정 77
■ 단말기 재시작 77
■ 단말기 초기화 77
화면/음성 78
로그 79
■ 로그 리스트 79
■ 로그 검색 79
■ 전체 삭제 80
■ 로그 현황 80

5 부록 81
제품규격 82
전기규격 83

1 사용하기 전에

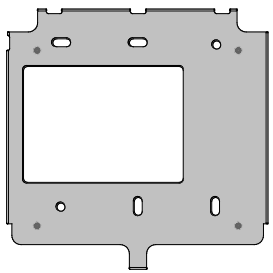
구성품이 모두 들어있는지 확인하십시오.

제품 구성품

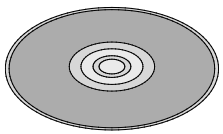
기본 구성품



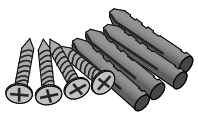
BioStation T2 본체



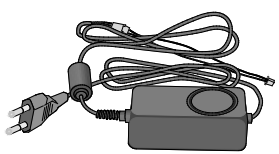
벽면 고정용 브라켓



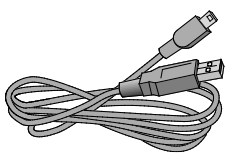
소프트웨어CD(1장)



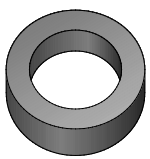
벽면 고정용 스크류와
PVC 앵커(각4개)



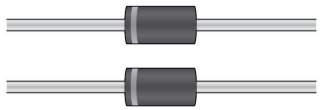
전원 어댑터



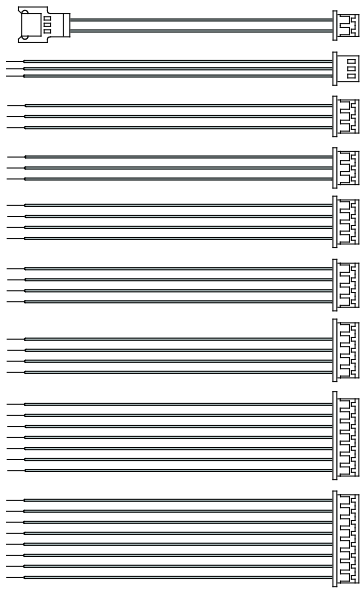
미니 USB 케이블



페라이트코아

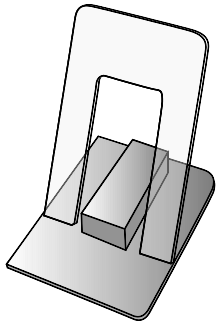


다이오드 (2개)

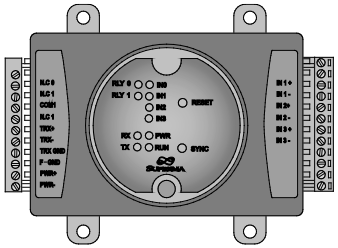


케이블(7종, 9개)

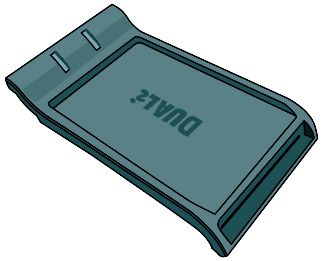
별매품



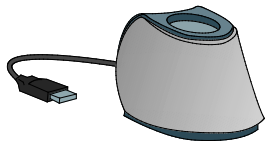
플라스틱 스탠드



Secure I/O



카드 리더기



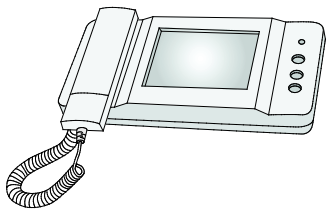
USB 지문 스캐너
(PC용 지문등록기)



Access Point
(무선랜 지원모델에 한함)



RF Cards

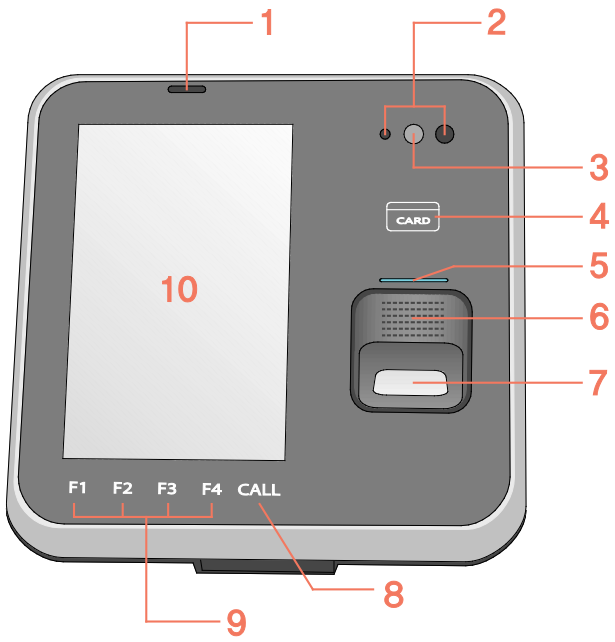


인터폰

참고	*위의 물품은 제품 설명을 위한 이미지 입니다.* *구성품 실물과 다를 수 있으며, 본사의 사정에 따라 일부 품목이 변경될 수 있습니다.*

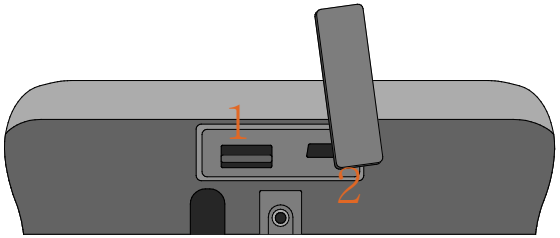
각 부분의 명칭과 기능

■ 제품 앞면



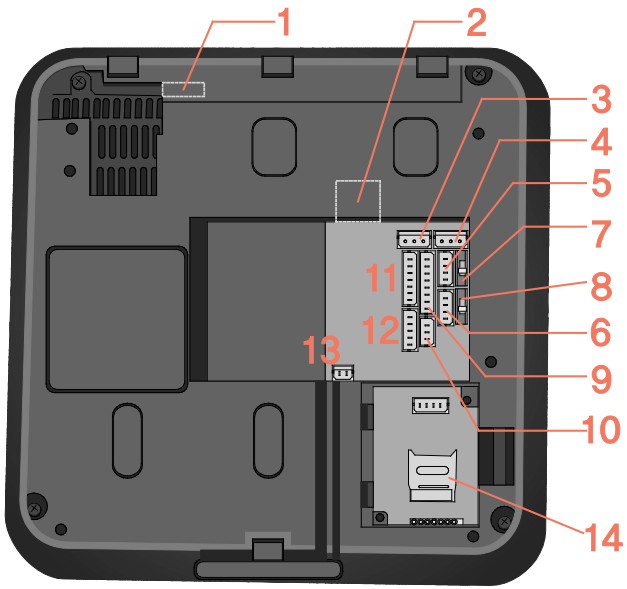
번호	명칭	기능
1	마이크	인터폰 통화시 사용됩니다.
2	근접 센서	물리적 접촉 없이 근처의 물체를 감지하는 센서입니다. BioStation T2는 일정 시간 동안 입력이 없으면 백라이트 밝기를 어둡게 하여 전기 소모를 줄입니다.
3	카메라	정지영상 로그를 남기거나, 인증시 얼굴 검출, 비디오 인터폰 등에 사용됩니다
4	카드 인식부	RF 카드를 인식하는 부분입니다.
5	LED	지문 센서의 상태를 표시합니다. 1)켜짐 – 지문 입력 항시 대기 2)깜박임 – 특정 지문 요청, 등록용 지문 요청
6	스피커	각종 사운드 효과 및 음성을 출력합니다.
7	지문센서	사용자 등록, 인증을 위해 지문 입력시에 사용됩니다.
8	CALL 키	비디오폰에 연결되어 있을 때 이 버튼을 눌러 통화를 요청합니다.
9	근태키(F1~F4)	근태 이벤트 선택 키로 사용합니다.
10	컬러LCD화면	시간 표시 및 상태 표시, 그리고 동작을 위한 UI를 제공합니다.

제품 밑면



번호	명칭	기능
1	USB type A	USB 메모리 장치를 연결하기 위한 슬롯입니다.
2	Mini USB	PC와 USB 연결을 위한 슬롯입니다.

제품 뒷면



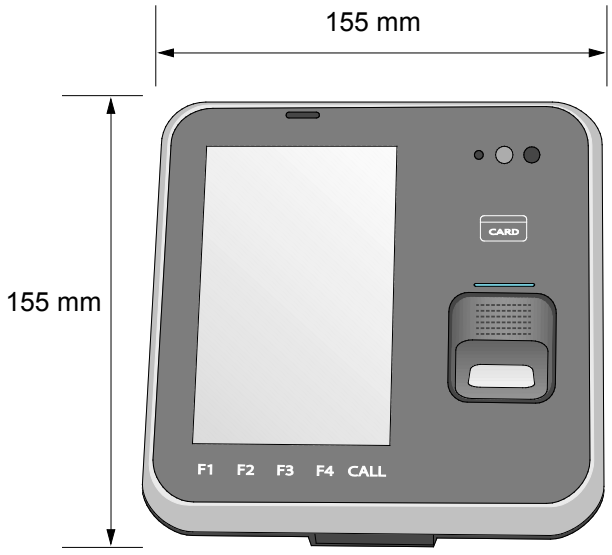
번호	명칭	기능
1	USB 무선랜	USB 무선랜 장치를 연결하기 위한 슬롯입니다. 무선랜 지원 모델의 경우 출고시에 무선랜 장치가 장착됩니다.
2	RJ45 소켓	이더넷 케이블 연결
3, 4	3핀 커넥터	릴레이(0,1) 연결
5, 6	4핀 커넥터	RS485(0,1)* 연결
7, 8	종단저항 스위치	RS485 종단저항 사용 여부 결정
9	8핀 커넥터	SWITCH 입력
10	3핀 커넥터	RS232 포트 연결
11	7핀 커넥터	비디오폰 연결
12	5핀 커넥터	WIEGAND 입출력
13	2핀 커넥터	전원 연결
14	Micro SD 카드 소켓	기능 확장을 위해 Micro SD 타입의 메모리 카드를 삽입할 때 사용합니다.

*RS485-0: PC Connect

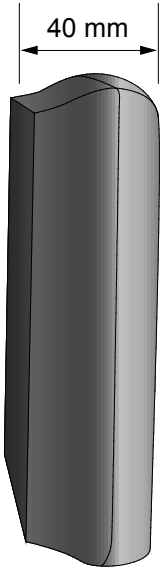
*RS485-1: RS485 Host/Slave

제품 크기

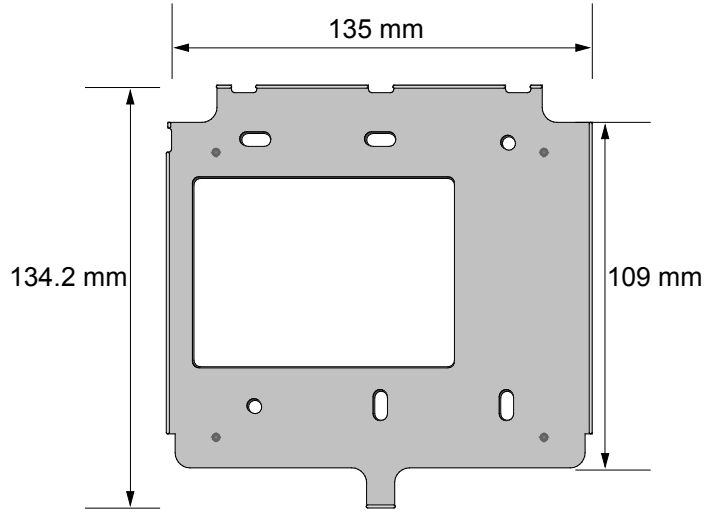
■ 155mm(W) x 155mm(H) x 40mm(D)



제품 앞면

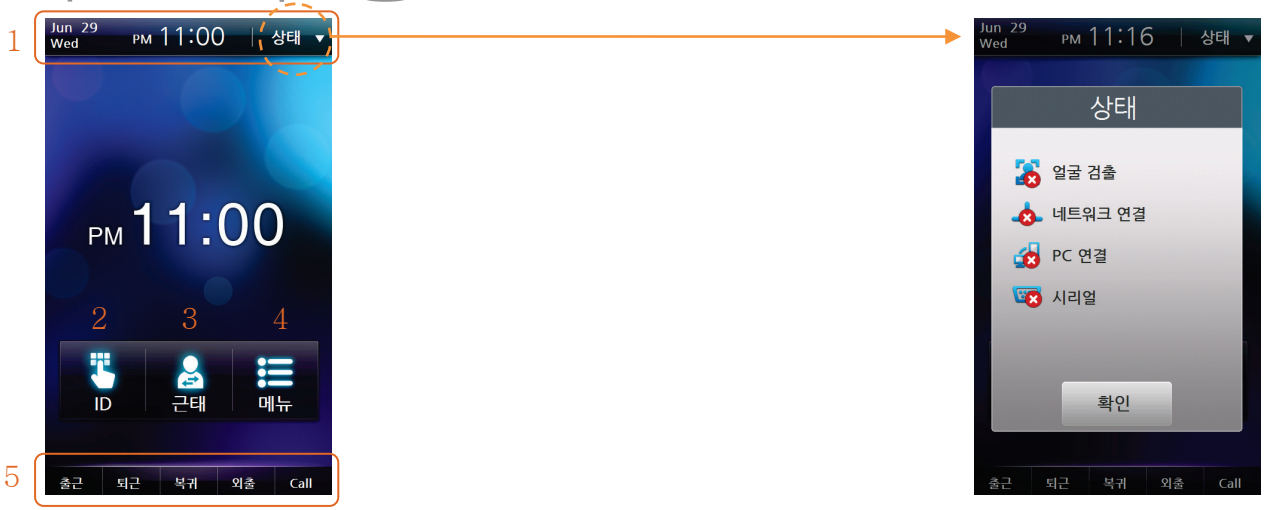


제품 측면



벽면 고정용 브라켓

기본화면 구성



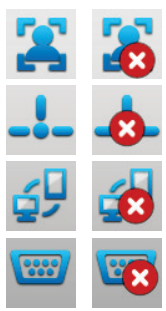
1 상태바 : 현재 날짜와 시간, 상태 아이콘을 표시합니다.

2 ID : 인증을 위해 사용자 ID를 입력합니다.

3 근태 : 추가 근태 이벤트 선택 화면으로 진입합니다.

4 메뉴 : 관리자 메뉴로 진입합니다.

5 근태키 표시부 : F1~F4, CALL에 대한 동작을 설명합니다. 해당 버튼을 터치할 경우 F1~F4, CALL과 동일하게 동작합니다.



인증시 얼굴검출 여부를 표시합니다.

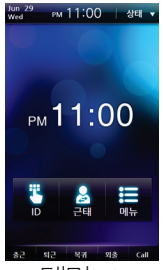
이더넷 및 무선랜 연결 상태를 표시합니다.

이더넷 및 무선랜을 통한 PC 연결 상태를 표시합니다.

RS485 슬레이브 모드일 때, 호스트와의 연결 상태를 표시합니다.

대기화면

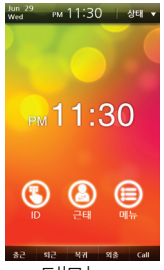
기본 화면



테마 1



테마 2



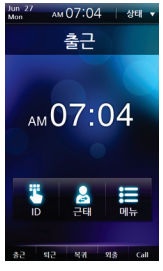
테마 3



테마 4

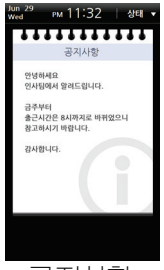
참고 *테마 1과 테마 3은 화면 중앙에 시계를 보이지 않도록 설정할 경우 움직이는 배경화면이 작동됩니다.*

근태 설정시



해당 근태가 상태바 아래에 표시됩니다.

배경 화면 설정시



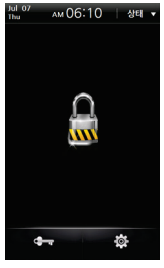
공지사항


슬라이드



PDF

그 밖의 대기화면



잠김 : 탬퍼 스위치나 특정 입력 포트를 이용해서 단말기를 잠글 수 있습니다. 잠김 해제를 위해서는 관리자 인증이 필요합니다.



경비중 : 경비구역이 설정된 경우 단말기를 경비상태로 만들 수 있습니다. 경비해제를 위해서는 해당 경비그룹에 속한 사용자의 인증이 필요합니다.
– 자세한 내용은 BioStar 매뉴얼 참고.

인증 방법

BioStation T2는 지문, RFID 카드, 아이디(PIN) 인증 방식을 지원합니다.

지문 인증 방식

- 지문 : 지문만으로 인증합니다.
- 지문+비밀번호 : 지문 입력 후 비밀번호를 입력하여 인증합니다.

카드 인증 방식

- 카드 : 등록된 카드를 인식하는 것만으로 인증됩니다.
- 카드+지문/비밀번호 : 등록된 카드를 인식 후 지문 또는 비밀번호 중 하나를 입력하여 인증합니다.
- 카드+지문 : 등록된 카드 인식 후 지문을 입력하여 인증합니다.
- 카드+비밀번호 : 등록된 카드 인식 후 비밀번호를 입력하여 인증합니다.
- 카드+지문+비밀번호 : 등록된 카드를 인식 후 지문과 비밀번호를 모두 입력하여 인증합니다.

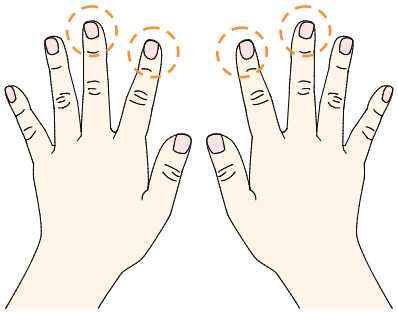
ID 인증 방식

- ID+지문/비밀번호 : 등록된 ID를 입력 후 지문 또는 비밀번호 중 하나를 입력하여 인증합니다.
- ID+지문 : 등록된 ID를 입력 후 지문을 입력하여 인증합니다.
- ID+비밀번호 : 등록된 ID를 입력 후 비밀번호를 입력하여 인증합니다.
- ID+지문+비밀번호 : 등록된 ID를 입력 후 지문과 비밀번호를 모두 입력하여 인증합니다.

참고 *각 인증 방법에 대한 자세한 설명은 [3 장 사용자 메뉴 > 출입인증 (40 페이지)]을 참고하십시오.*

올바른 지문 입력 방법

■ 지문 입력을 위한 손가락 선택



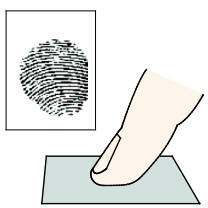
(1) 특별한 사유가 없는 한, 검지와 중지의 등록과 사용을 권장합니다.
(2) 검지와 중지에 비해 엄지, 약지 또는 소지는 정확한 위치에 놓기 어렵기 때문에 사용을 피하는 것이 좋습니다.

■ 지문을 센서에 바르게 입력하는 방법

(1) 지문센서의 불을 확인합니다.
(2) 손가락을 띄운 상태로 지문센서 표면의 정중앙에 손가락을 위치합니다.
(3) 손가락을 위에서 아래로 지장을 찍듯이 누른 상태에서 멈춥니다. 센서를 찍어 누르듯이 손가락을 세워서 입력하면 손끝 부분의 지문만이 인식되므로 왼쪽 그림과 같이 접촉되는 면적이 많도록 입력할 것을 권장합니다.



올바른 방법



잘못된 방법

(4) 신호음이 들리면 손가락을 뗍니다.

■ 손가락 상태에 따른 대처방안

슈프리마의 지문인식 제품은 계절의 변화나 손가락의 상태 변화에 상관없이 지문입력이 잘 되도록 설계되어 있습니다. 하지만 외부 영향에 따라 지문입력이 어려울 경우 다음 사항을 참고하시기 바랍니다.

(1) 손가락에 젖었을 때, 물기를 닦은 후 입력합니다.
(2) 손가락에 먼지 등 이물질이 묻어 있는 경우, 잘 닦거나 털어내고 입력합니다.
(3) 손가락이 너무 건조하여 입력이 안될 경우(동절기), 손끝에 가볍게 입김을 불거나 로션 등 보습제를 바르고 입력합니다.
(4) 손가락에 상처나 났거나 눌린 자국이 있을 때, 등록되어 있는 다른 지문을 사용합니다.

■ 지문 입력시 권고 사항

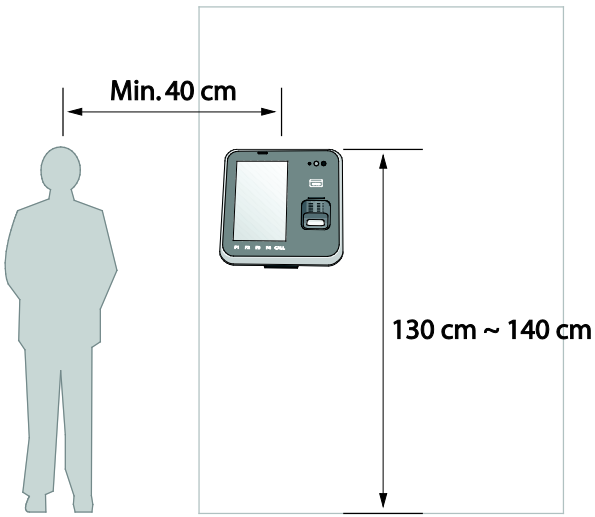
(1) 지문인식에서 등록 과정이 매우 중요합니다. 따라서, 처음에 지문을 등록할 때 신경을 써서 올바르게 지문을 입력해야 합니다.
(2) 인증 성공률이 떨어질 경우 다음과 같은 조치를 권장합니다.
- 등록된 지문을 지우고 다시 등록합니다.
- 같은 지문을 추가로 더 등록합니다.
- 상처 등으로 입력이 어려운 손가락이 있는 경우 등록된 다른 손가락으로 시도합니다.

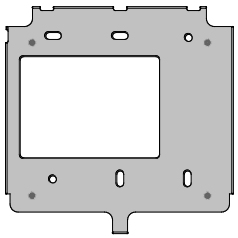
(3) 손에 짐을 들거나 손가락에 상처가 나는 경우 등, 등록된 지문의 사용이 어려운 경우를 대비해 두 개 이상의 손가락 등록을 권장합니다.

2 설치하기

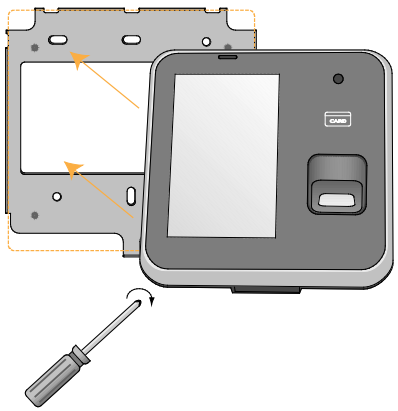
설치

BioStation T2는 얼굴 검출 및 비디오 인터폰용 카메라 장착 제품이므로, 브라켓을 설치하기 전에 설치 높이와 카메라 각도를 고려하여야 합니다. 얼굴 촬영과 지문 인증을 고려하여 제품의 설치 위치를 정합니다. 최적 설치 높이는 상단 기준 130 cm ~140 cm0이고, 제품과 사람 간의 최소 거리는 40 cm 입니다.





1. 브라켓을 설치하려는 위치에 고정시킵니다.

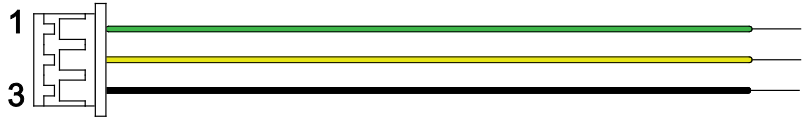


2. 고정된 브라켓에 제품을 설치한 후 하단에 있는 제품 고정용 나사로 고정시킵니다.

커넥터/케이블 사양

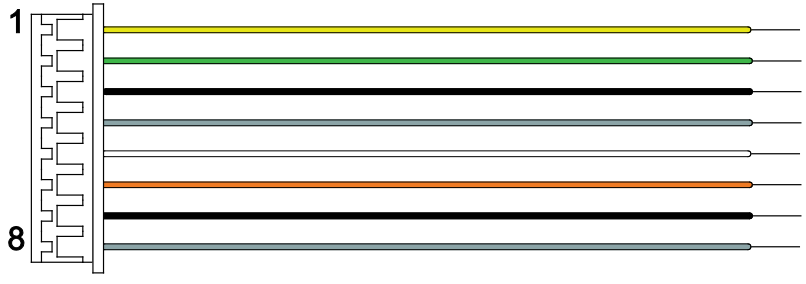
■ 232 케이블 (3 핀 커넥터)

핀	명칭	케이블 타입	색상
1	232 RX	AWG26	GREEN
2	232 TX		YELLOW
3	232 GND		BLACK



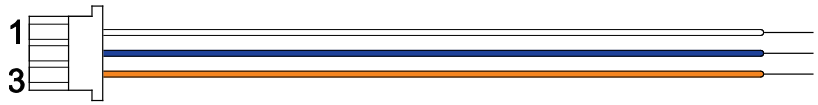
■ SWITCH 케이블 (8 핀 커넥터)

핀	명칭	케이블 타입	색상
1	TTL IN0	AWG26	YELLOW
2	TTL IN1		GREEN
3	TTL GND		BLACK
4	SH GND		GRAY
5	TTL IN2		WHITE
6	TTL IN3		ORANGE
7	TTL GND		BLACK
8	SH GND		GRAY



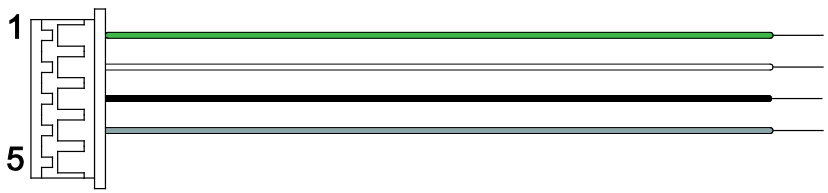
■ 릴레이 케이블 (3 핀 커넥터)

핀	명칭	케이블 타입	색상
1	RLY NO	AWG24	WHITE
2	RLY COM		BLUE
3	RLY NC		ORANGE



■ WIEGAND 케이블 (5 핀 커넥터)

핀	명칭	케이블 타입	색상
1	WG D0	AWG26	GREEN
2	WG D1		WHITE
3	WG GND		BLACK
4	SH GND		GRAY



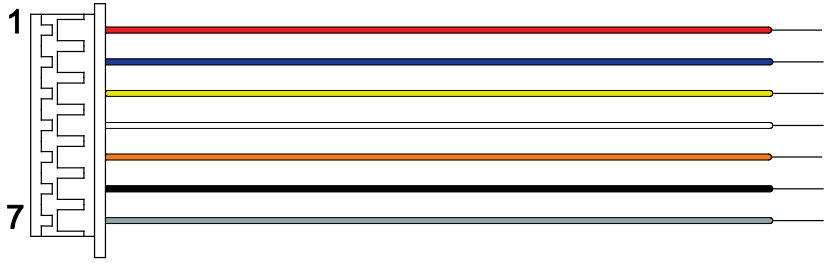
■ 전원 케이블 (2 핀 커넥터)

핀	명칭	케이블 타입	색상
1	PWR +VDC	AWG24	RED
2	PWR GND		BLACK



■ 비디오폰 케이블 (7 핀 커넥터)

핀	명칭	케이블 타입	색상
1	VP VOC	AWG26	RED
2	VP GND		BLUE
3	VP +VDC		YELLOW
4	VP VS		WHITE
5	VP DOS		ORANGE
6	VP GND		BLACK
7	SH GND		GRAY



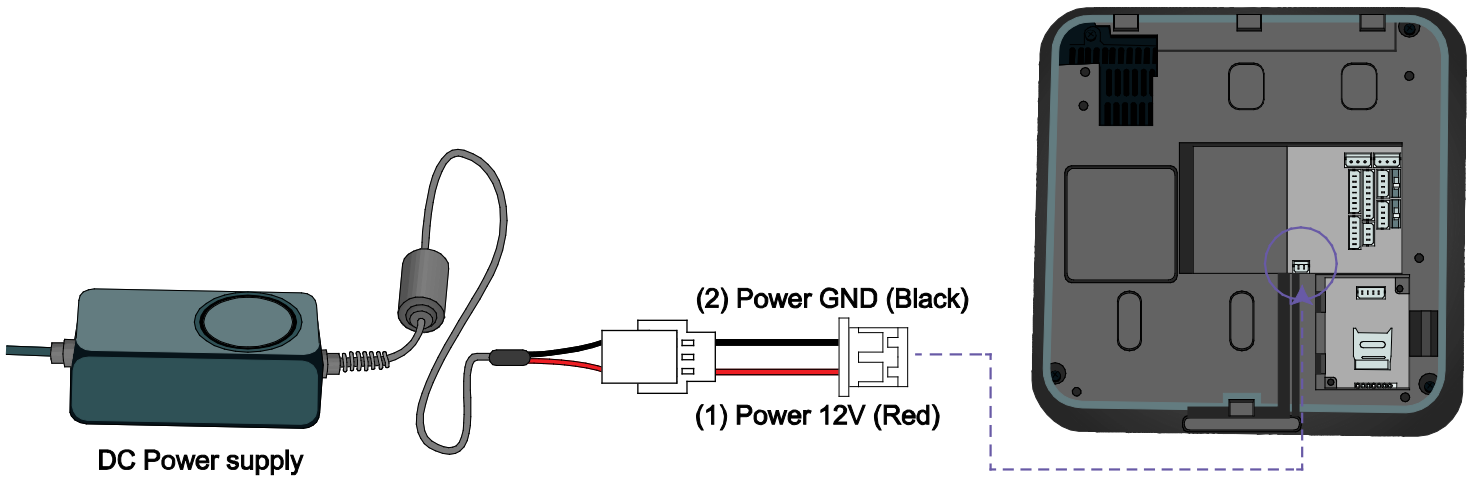
■ RS485 케이블 (4 핀 커넥터)

핀	명칭	케이블 타입	색상
1	485 TRXP	AWG26	BLUE
2	485 TRXN		YELLOW
3	485 GND		BLACK
4	SH GND		GRAY



연결

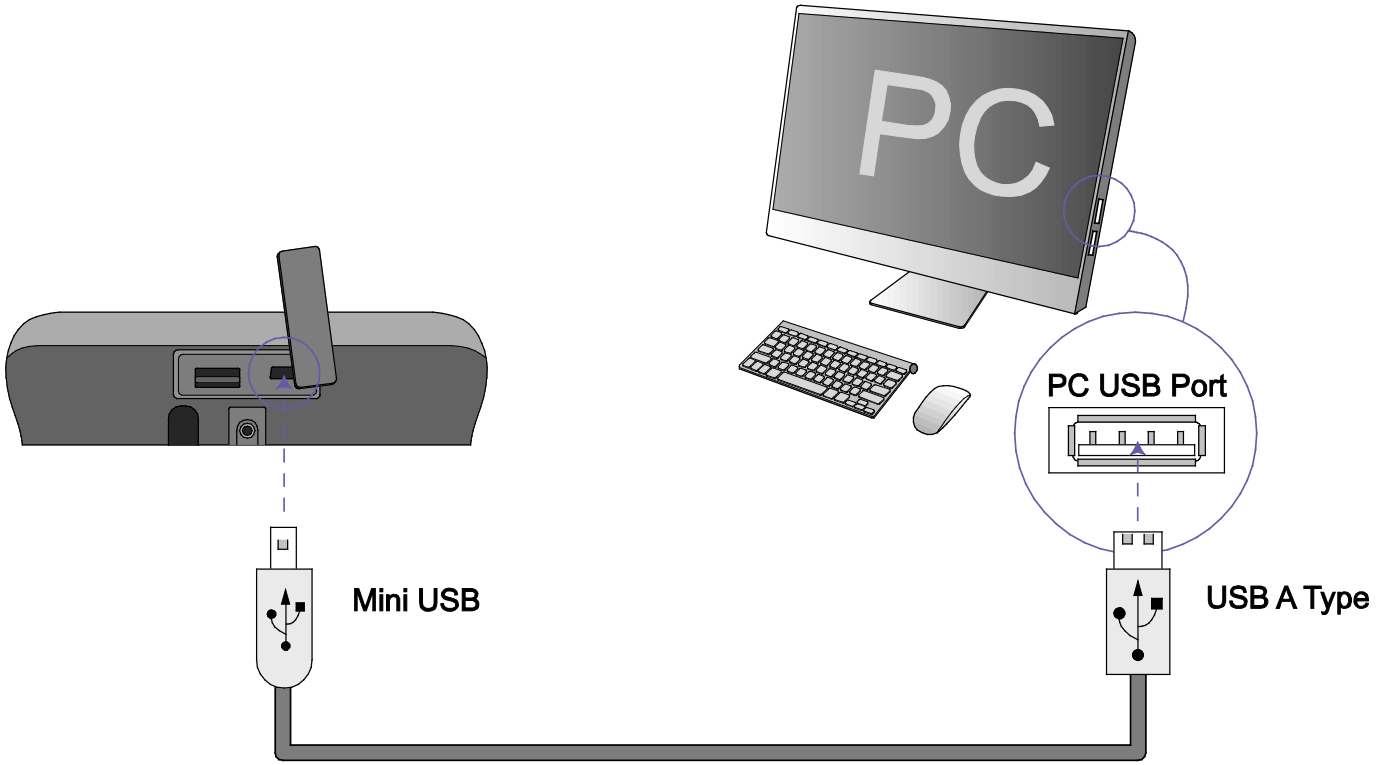
■ 전원 연결(2 핀 커넥터)



참고

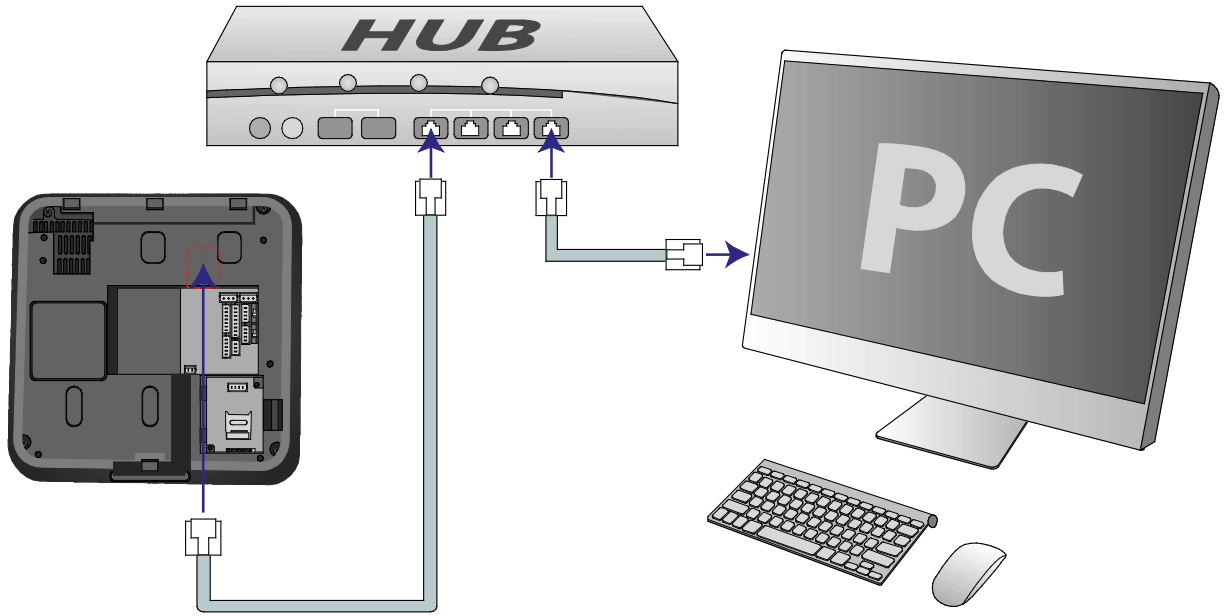
권장전원사양
- 전압 12V ± 10%, 전류 1500mA 이상, IEC/EN 60950-1 으로 승인된 12V 어댑터를 사용해야 합니다.
- BioStation T2 의 전원을 Secure I/O, Lock 등의 다른 장비와 공유해서 사용하지 않을 것을 권장합니다.

■ USB 케이블 연결

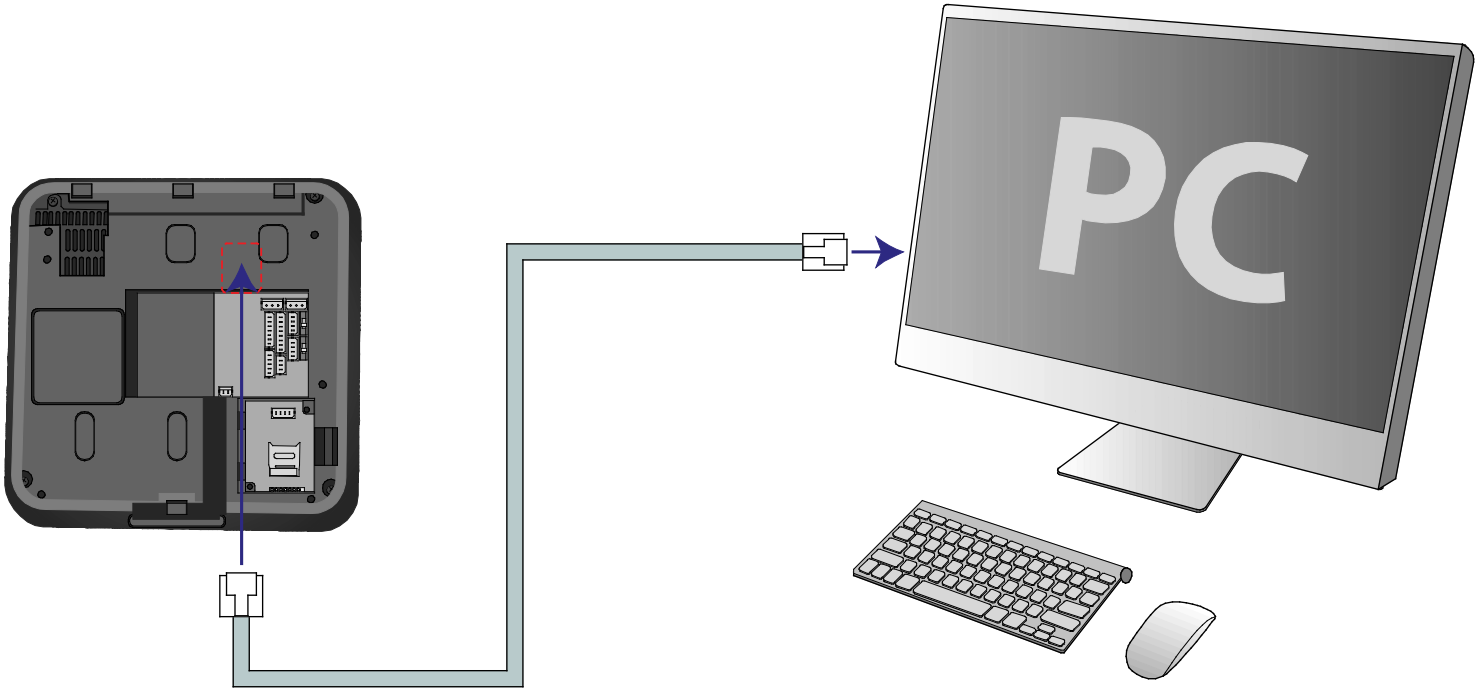


■ 이더넷 연결(이더넷 케이블)

제품 뒷면의 RJ45 소켓에 이더넷 케이블(LAN케이블)로 허브와 연결합니다.

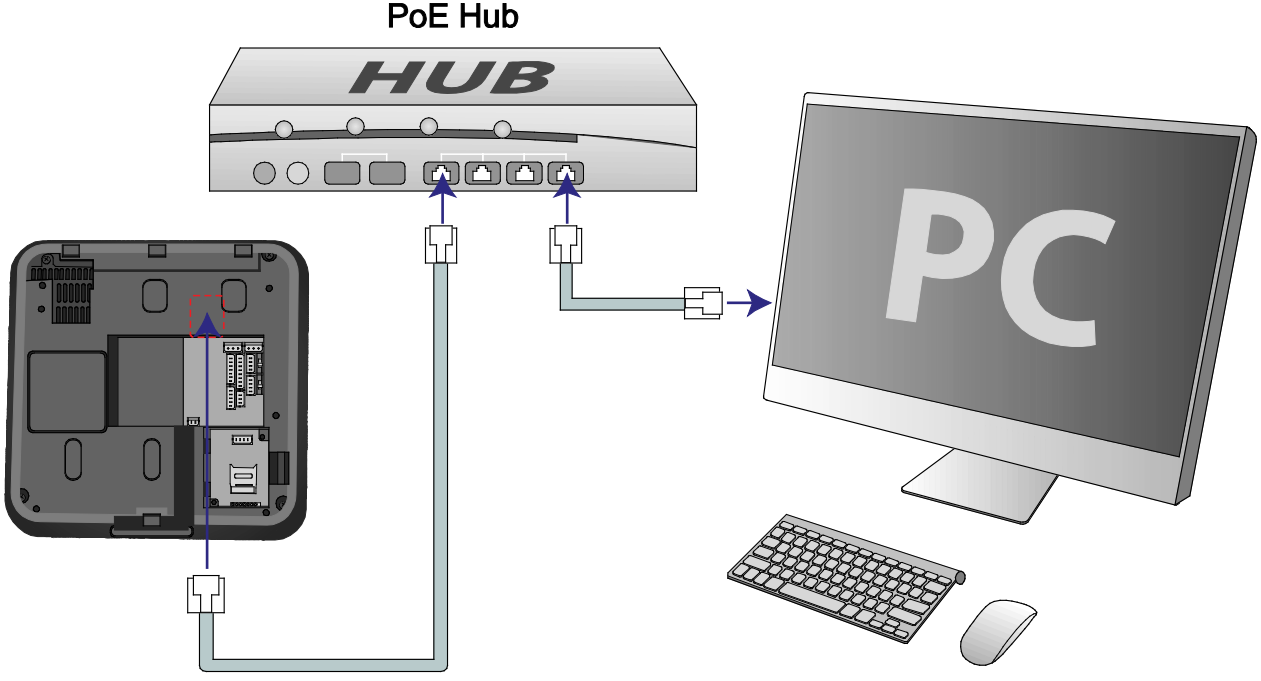


■ 이더넷 연결 (PC 와 직접 연결)



■ PoE 허브 연결

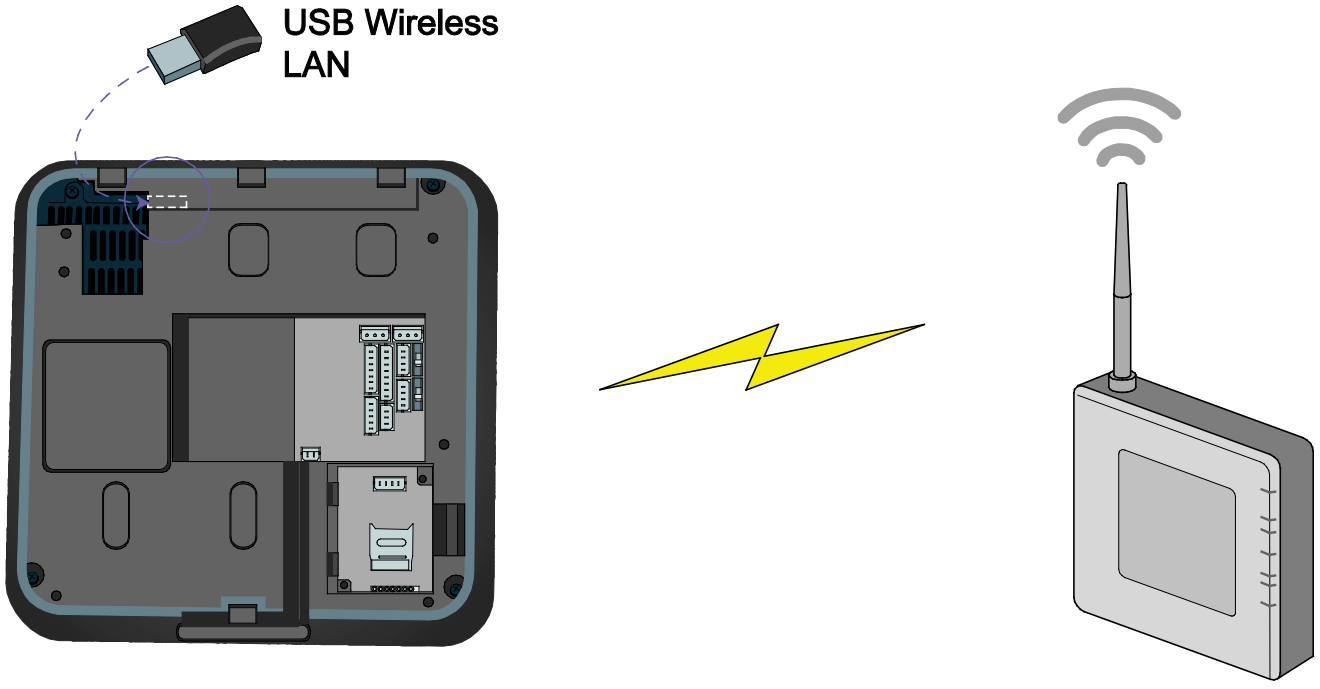
PoE(Power over Ethernet)는 IEEE802.3af 규격을 만족하는 PSE(Power Sourcing Equipment)로부터 전원을 공급받는 이더넷 연결 방식입니다.



참고	*PoE 방식을 사용시 랜케이블의 길이는 100 m 이내로 사용하여 주십시오.*

■ 무선랜 연결

BioStation T2의 무선랜 지원 모델은 출고시에 USB 무선랜 모듈이 장착 됩니다.

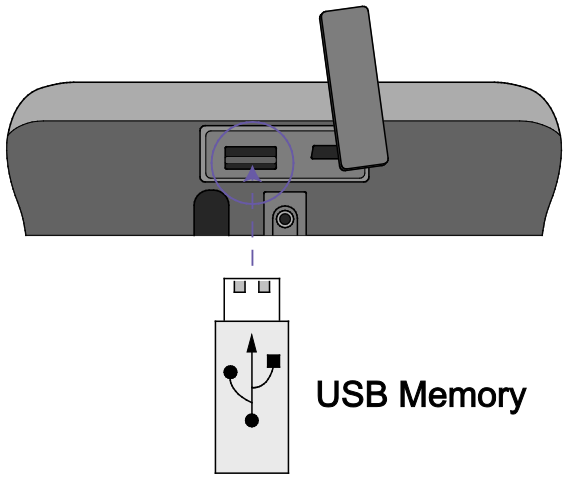


참고

- *무선랜의 성능은 주위 환경과 사용하는 AP(Access Point)의 종류에 따라 많은 영향을 받습니다.*
- *일부 무선 AP는 하드웨어 호환성 문제로 인해 무선랜 연결에 문제가 있을 수 있습니다.*
  아래 목록의 무선 AP들은 BioStation T2와 호환성이 검증된 모델이니 참고하시기 바랍니다.
  - *Buffalo WHR-HP-G54*
  - *IP Time G104*

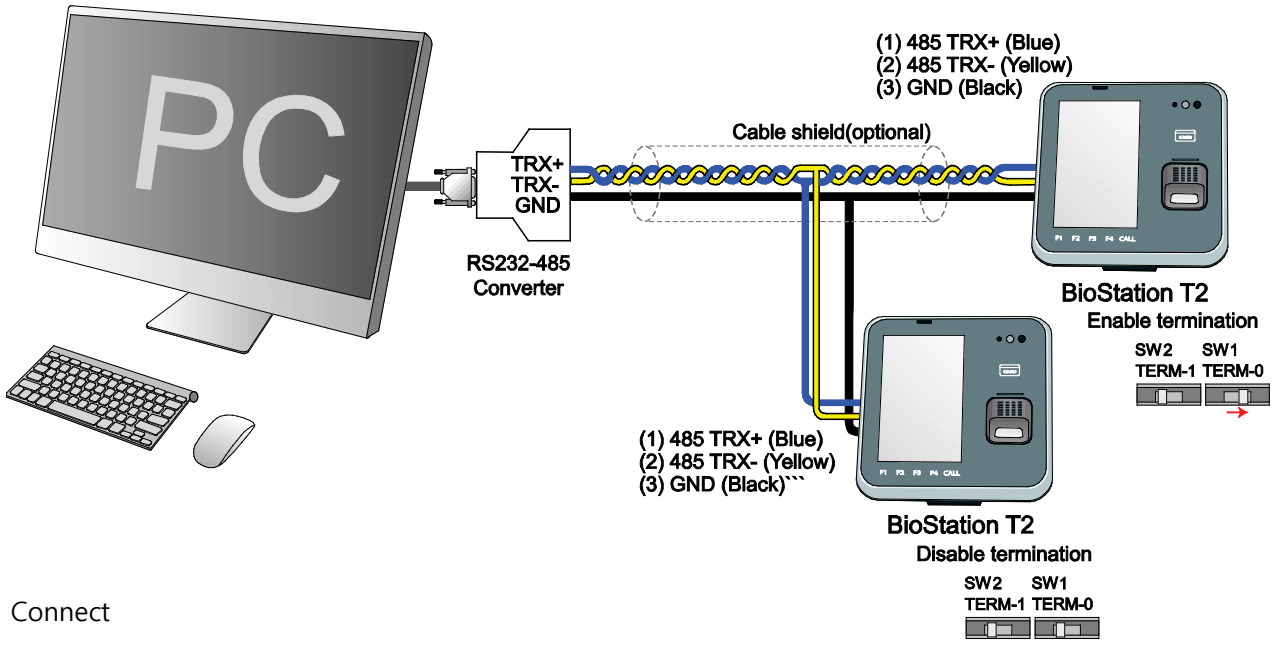
■ USB 메모리 연결

USB 메모리를 이용하여 사용자나 로그 데이터를 다운로드/업로드 할 수 있습니다.



참고	*일부 USB 메모리의 경우 하드웨어 호환성 문제로 인해 연결이 되지 않을 수 있습니다.* *아래 목록의 USB 메모리는 BioStation T2와 호환성이 검증된 모델이니 참고하시기 바랍니다.* ■ *[IMATION] Flash Drive Nano 4GB* ■ *[LG 전자] X TICK M4 4GB* ■ *[LG 전자] X TICK MOBY J1 2GB* ■ *[PQI] Traveling Disk U173 4GB* ■ *[삼성물산] PLEOMAX PUB-S100 4GB* ■ *[IMATION] Flash Drive Nano 4GB* ■ *[LG 전자] X TICK M4 4GB* ■ *[LG 전자] X TICK MOBY J1 2GB* ■ *[PQI] Traveling Disk U173 4GB* ■ *[삼성물산] PLEOMAX PUB-S100 4GB*

■ RS485 PC 연결(4 핀 커넥터)



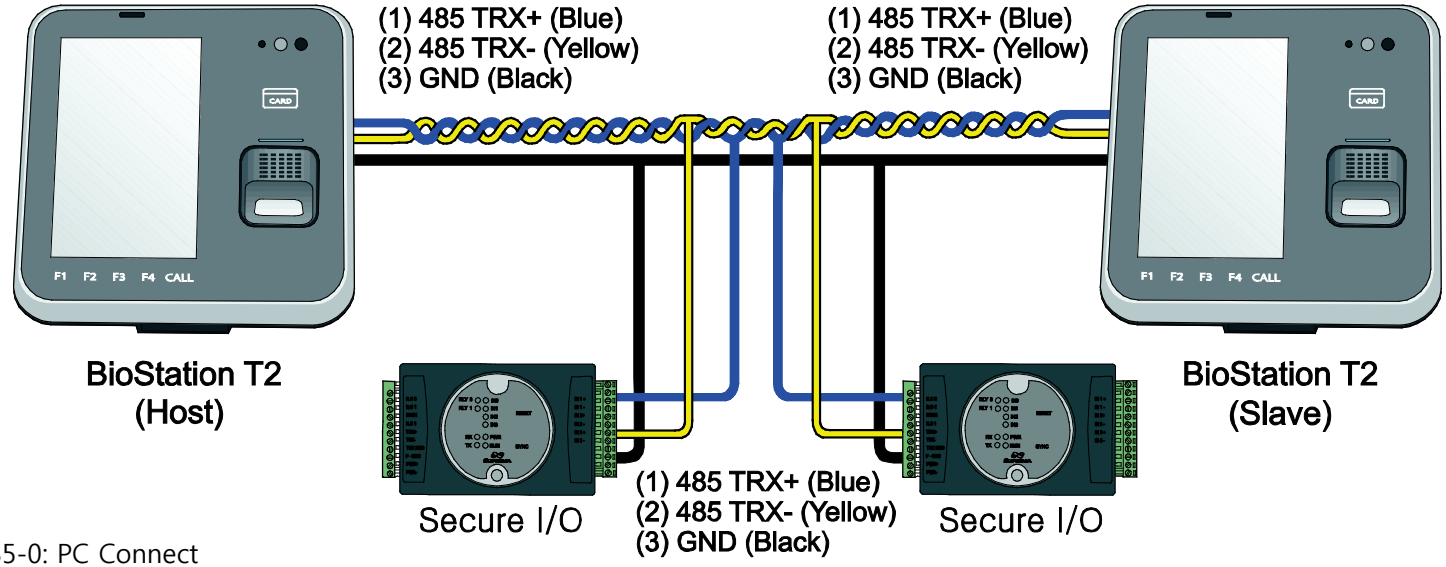
*RS485-0: PC Connect

*RS485-1: RS485 Host/Slave

참고	*RS485 배선이 길어지는 경우, 신호 약화를 방지하기 위해 Dip Switch 를 켜서 종단저항을 걸어주면, 신호가 정상으로 전달됩니다. 배선이 아주 짧은 경우, 저항을 걸어주면 오히려 신호가 제대로 전달되지 않습니다. 따라서, 배선의 길이 및 신호의 상태를 고려하여, 종단 저항 선택 스위치의 On/Off 를 선택합니다.*

주의!	GND 를 연결하지 않을 경우 RS485 칩이 손상되거나 정상적으로 통신이 되지 않을 수 있습니다.

■ RS485 Secure I/O 및 다른 단말기와 연결(4 핀 커넥터)



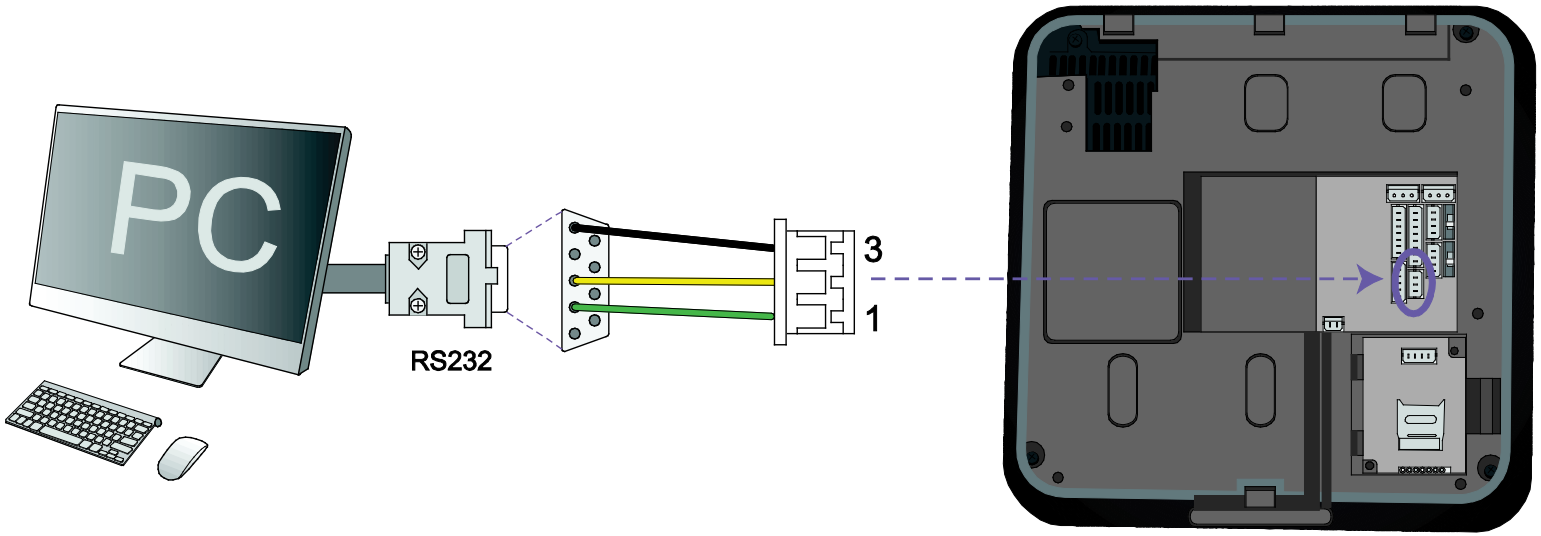
*RS485-0: PC Connect

*RS485-1: RS485 Host/Slave

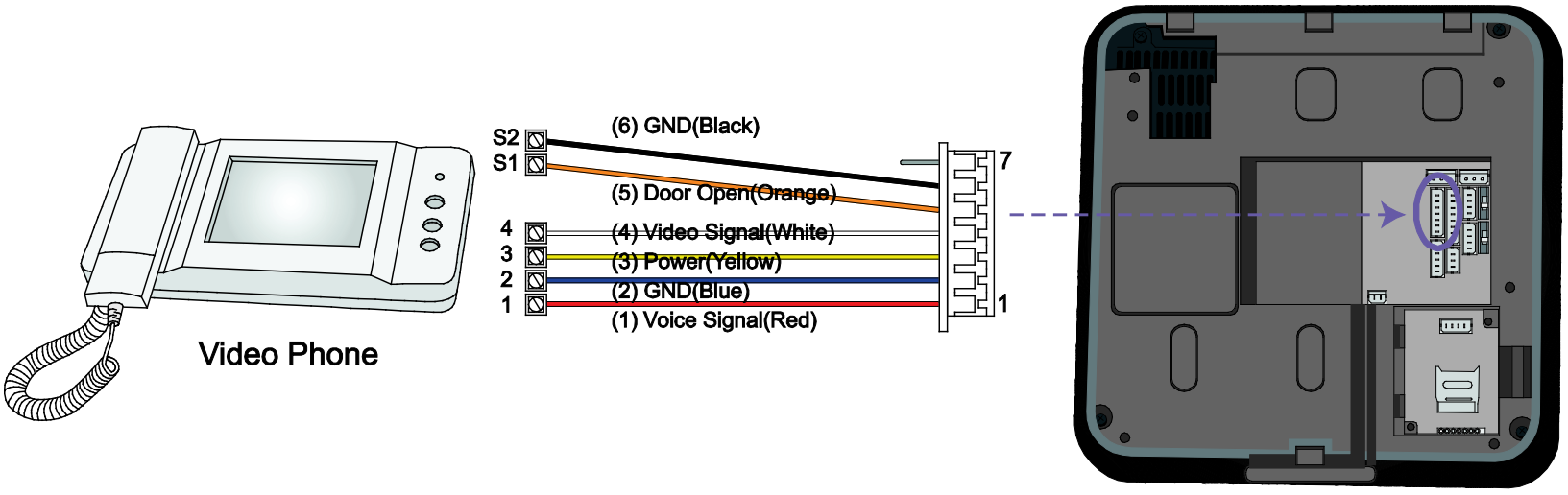
참고 *하나의 RS485 네트워크 당 호스트를 포함하여 최대 8 개까지 연결할 수 있습니다.*

주의! GND 를 연결하지 않을 경우 RS485 칩이 손상되거나 정상적으로 통신이 되지 않을 수 있습니다.

RS232 연결



■ 비디오폰 연결

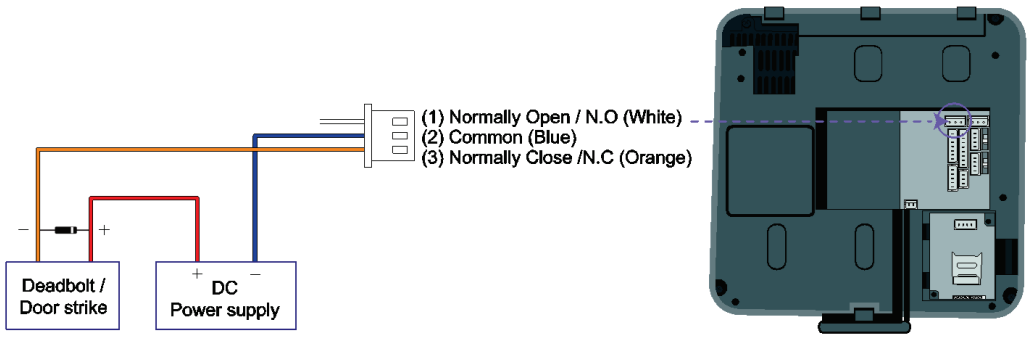


참고

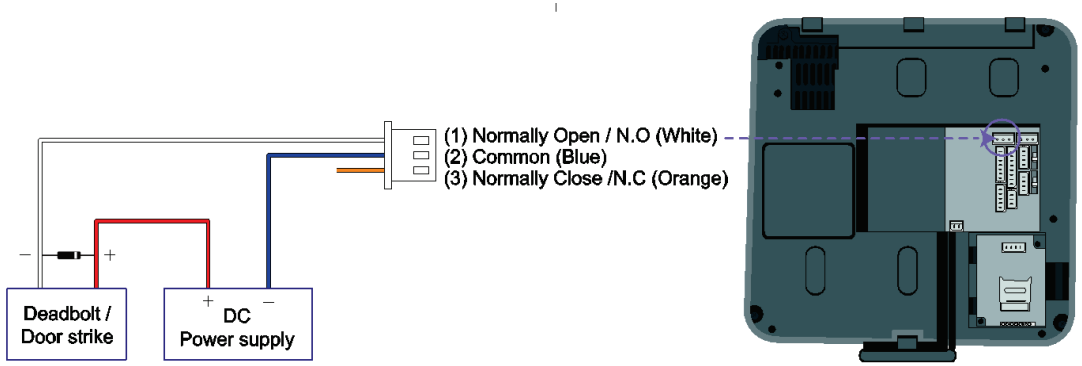
BioStation T2와 연동 가능한 아날로그 비디오폰 목록은 아래와 같습니다.

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

■ 릴레이 연결 - Fail safe lock(3 핀 커넥터)

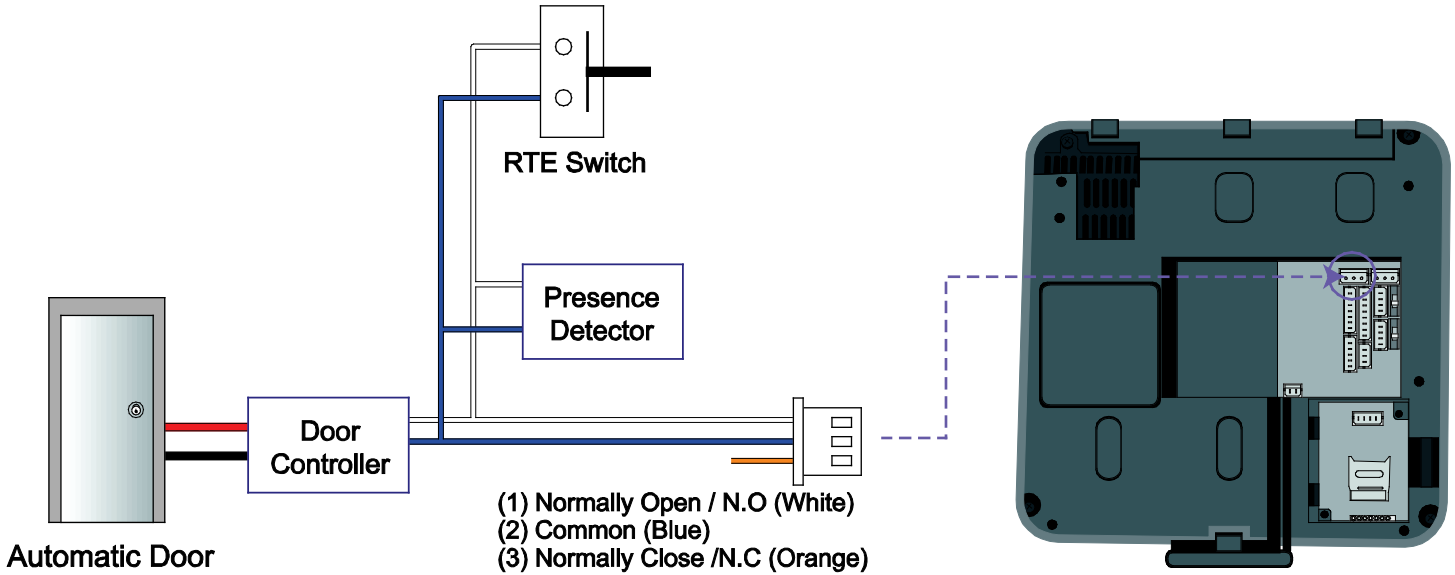


■ 릴레이 연결 - Fail secure lock(3 핀 커넥터)



참고	*-Normally Open/N.O: 제어신호가 없을 때는 전기가 흐르지 않는 상태를 유지하고, 제어신호가 있을 때는 전기가 흐릅니다.* *-Normally Close/N.C: 제어신호가 없을 때는 전기가 흐르는 상태를 유지하고, 제어신호가 있을 때는 전기가 흐르지 않습니다.* *-다이오드의 방향에 주의하세요.* *-다이오드는 도어록에 근접하여 설치해야 합니다.* *-BioStation T2 와 도어록은 별개의 파워서플라이를 사용하십시오.* *-도어록 동작 시 발생하는 역전류로부터 릴레이 접점을 보호하기 위해 상단의 두 그림과 같이 도어록 배선 양단에 다이오드를 설치하십시오.*

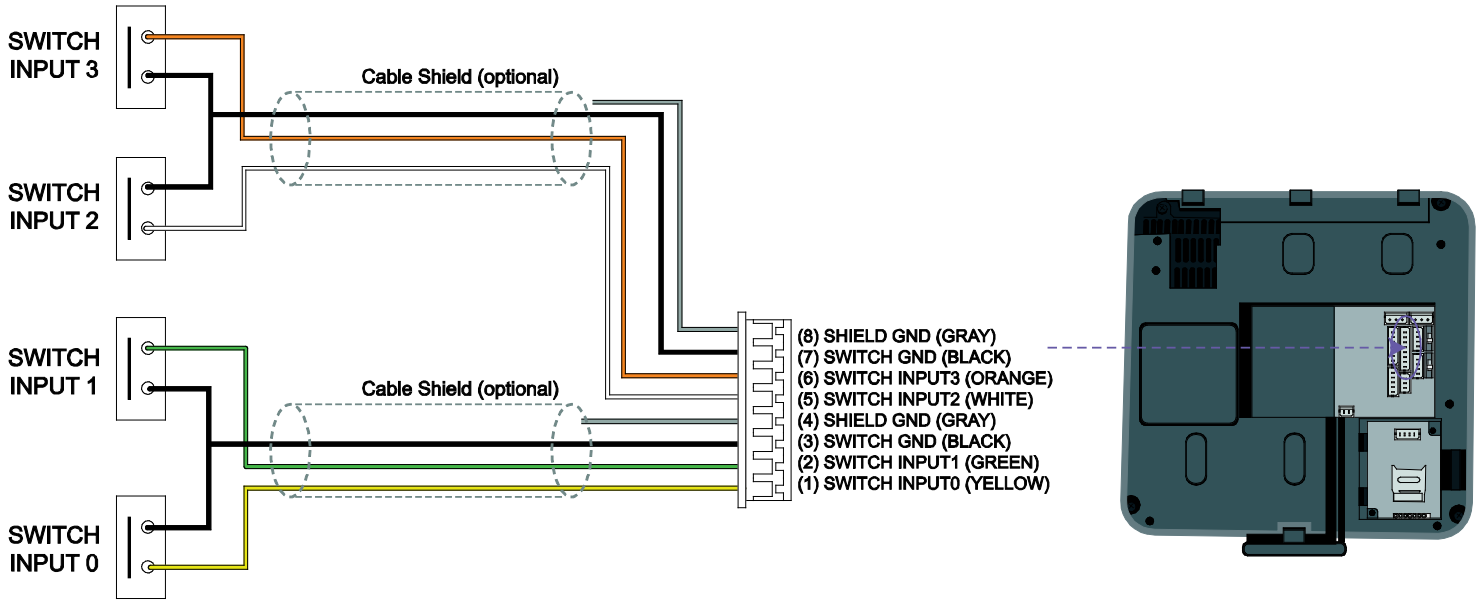
■ 릴레이 연결 - 자동문(3 핀 커넥터)



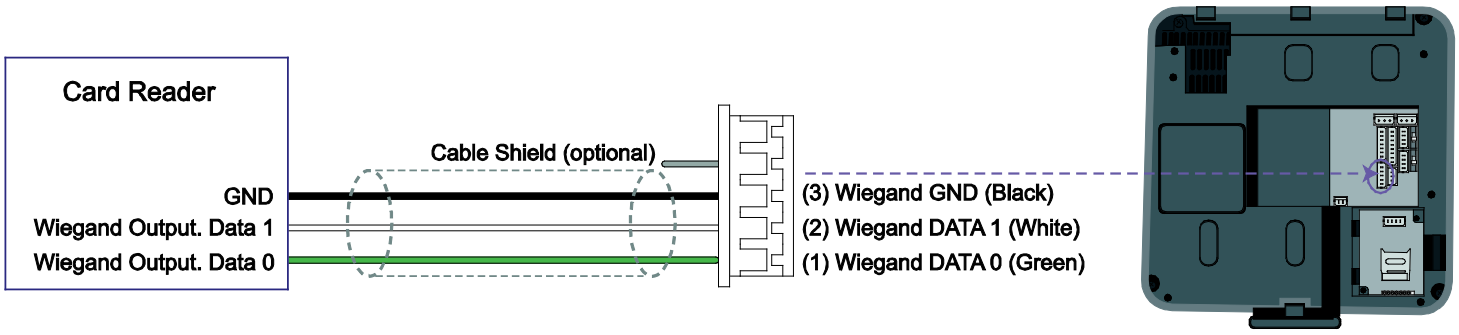
참고

-Normally Open/N.O: 제어신호가 없을 때는 전기가 흐르지 않는 상태를 유지하고, 제어신호가 있을 때는 전기가 흐릅니다.
-Normally Close/N.C: 제어신호가 없을 때는 전기가 흐르는 상태를 유지하고, 제어신호가 있을 때는 전기가 흐르지 않습니다.

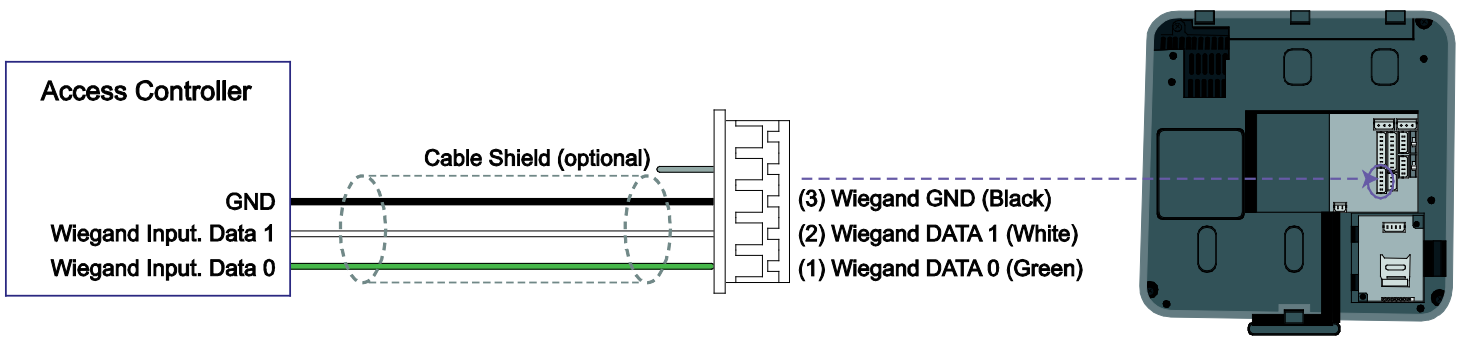
TTL Switch 입력 연결(8 핀 커넥터)



Wiegand 입력(5 핀 커넥터)



Wiegand 출력(5 핀 커넥터)

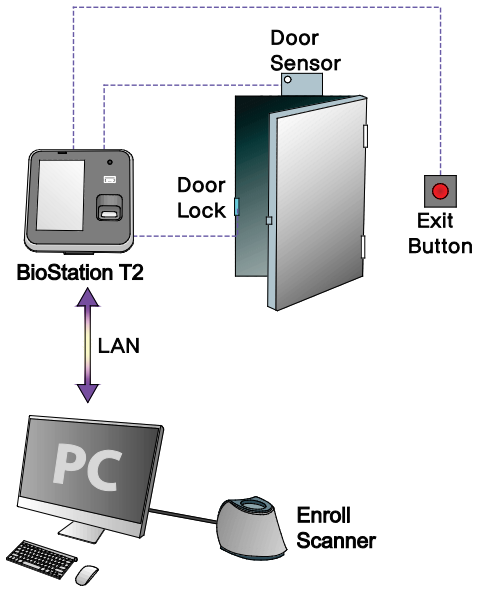


참고 *Wiegand 포트는 하나이며 BioStar 소프트웨어에서 입력 모드 혹은 출력 모드를 설정하여 사용합니다.*

시스템 구성도

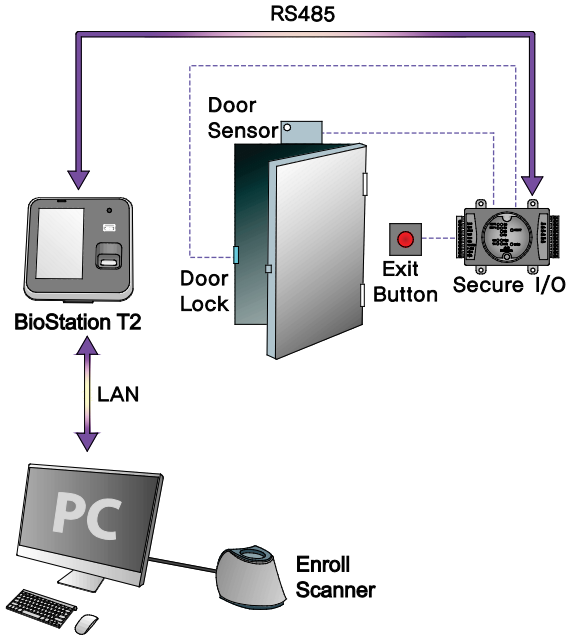
■ 독립형

단말기에서 인증기능과 출입문 제어 역할을 동시에 수행합니다.



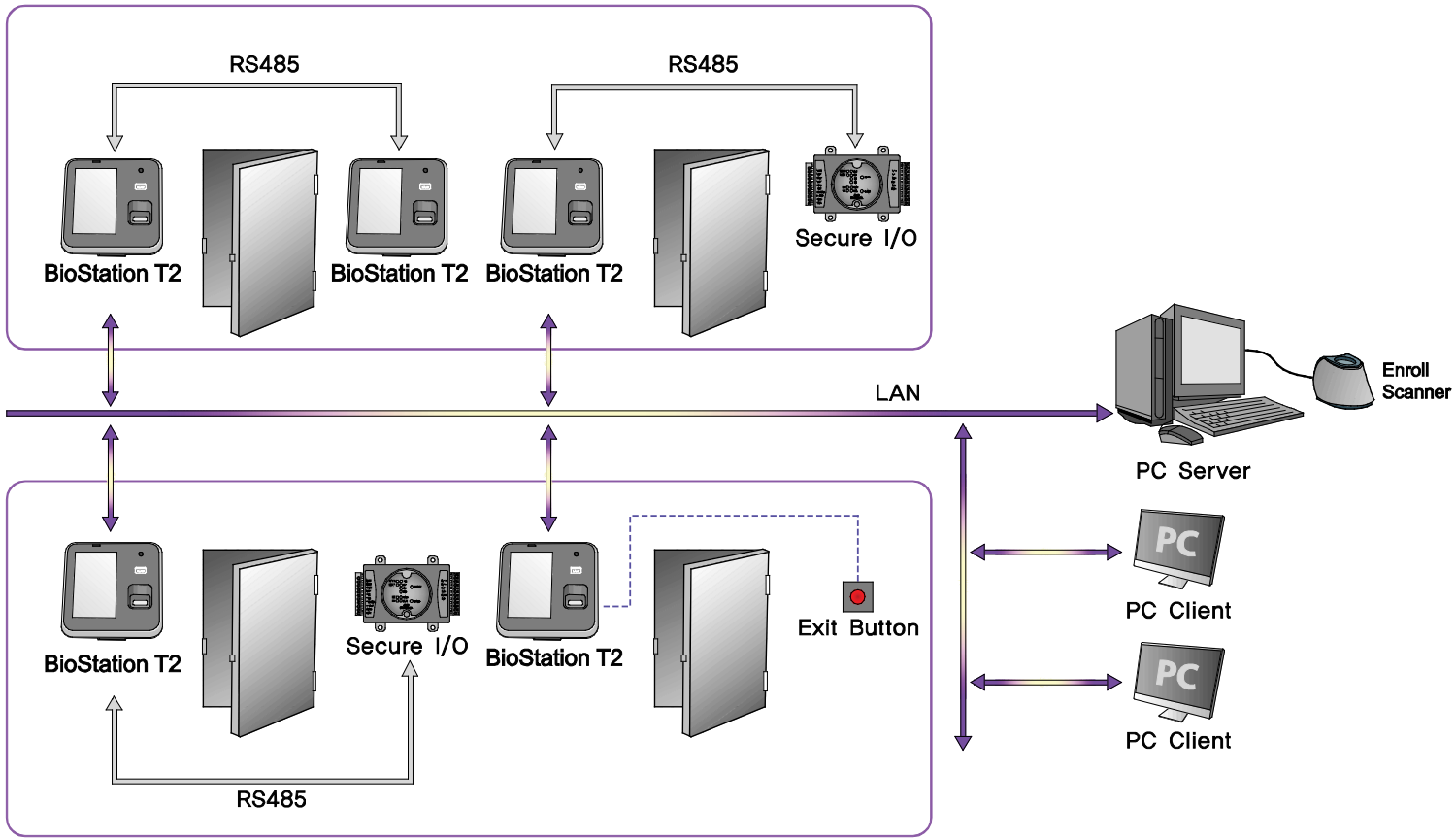
■ 보안형(Secure I/O 사용)

단말기에서 인증기능을 수행하고, Secure I/O에서 출입문 제어 역할을 수행합니다.



■ 네트워크 구성

LAN과 RS485를 이용하여 통합적인 관리가 가능합니다.



3 사용자 메뉴

출입 인증

BioStation T2는 지문, 카드(RFID), 아이디(PIN) 인증 방식을 지원합니다. 인증모드의 경우 설정된 시간대에 따라서 동작하고, 각 인증수단별 시간대는 중복되지 않습니다. 인증모드 설정 시 사용되는 시간대는 BioStar에서 설정하며 최대 128개까지 지원합니다.

■ 지문

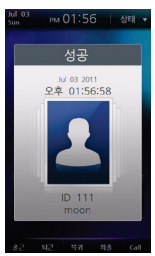
■ 지문만으로 인증하기

<설정 방법>

1. [메뉴] > [동작모드] > [지문 인증] > [지문]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>





1. 센서에 손가락을 올려놓습니다.
2. 인증 성공 화면이 나타납니다.

참고	*인증에 성공하면 인증 성공 화면이 표시됩니다.* *- 이미지가 등록된 경우: 등록된 사용자의 이미지가 인증 성공 창에 표시됩니다.* *- 이미지가 등록되지 않은 경우: 촬영된 이미지가 표시됩니다. 정지영상로그를 촬영하지 않는 경우에는 기본 이미지가 인증 성공 화면에 표시됩니다.*

■ 지문+비밀번호 인증

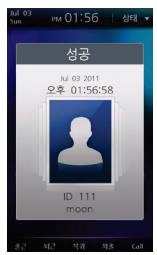
<설정 방법>

1. [메뉴] > [동작모드] > [지문 인증] > [지문+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>







1. 센서에 손가락을 올려놓습니다.
2. 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
3. 인증 성공 화면이 나타납니다.

■ 근태키+지문 인증

<설정 방법>
1. [메뉴] > [동작모드] > [지문 인증] > [근태키+지문]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>

1 원하는 근태키(F1~F4)를 누릅니다.
2 센서에 손가락을 올려놓습니다.
3 인증 성공 화면이 나타납니다.

■ 근태키+지문+비밀번호 인증
<설정 방법>
1. [메뉴] > [동작모드] > [지문 인증] > [근태키+지문+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>

1 원하는 근태키(F1~F4)를 누릅니다.
2 센서에 손가락을 올려놓습니다.
3 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
4 인증 성공 화면이 나타납니다.

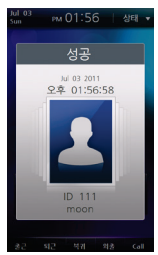
■ 카드

■ 카드만으로 인증하기
단말기의 인증 모드가 ‘카드’로 설정되어 있는 경우와 해당 사용자 카드가 ‘항시통과카드’로 등록된 경우에는 카드만으로 인증이 됩니다.

<설정 방법>
1. [메뉴] > [동작모드] > [카드 인증] > [카드]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>





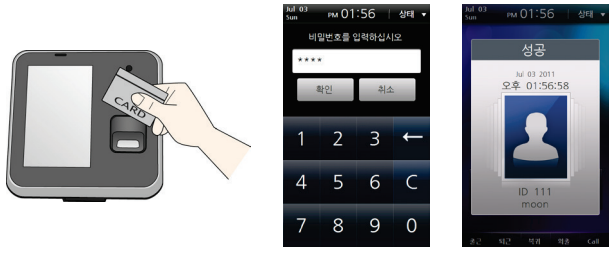
1 단말기 카드 인식부에 카드를 접근합니다.
2 인증 성공 화면이 나타납니다.

■ 카드+비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [카드 인증] > [카드+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 단말기 카드 인식부에 카드를 접근합니다.
2. 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
3. 인증 성공 화면이 나타납니다.

■ 카드+지문 인증

<설정 방법>

1. [메뉴] > [동작모드] > [카드 인증] > [카드+지문]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 단말기 카드 인식부에 카드를 접근합니다.
2. 지문 입력 창이 나타나면 손가락을 센서에 올려놓습니다.
3. 인증 성공 화면이 나타납니다.

■ 카드+지문/비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [카드 인증] > [카드+지문/비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 단말기 카드 인식부에 카드를 접근합니다.
2. 지문 또는 비밀번호를 입력하여 인증합니다.
3. 인증 성공 화면이 나타납니다.

■ 카드+지문+비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [카드 인증] > [카드+지문+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 단말기 카드 인식부에 카드를 접근합니다.
2. 지문 입력 창이 나타나면 손가락을 센서에 올려놓습니다.
3. 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
4. 인증 성공 화면이 나타납니다.

■ ID

■ 아이디+비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [ID 인증] > [아이디+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 대기화면에서 [ID 입력]을 누릅니다.
2. ID 입력 창이 나타나면 ID를 입력합니다.
3. 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
4. 인증 성공 화면이 나타납니다.

■ 아이디+지문 인증

<설정 방법>

1. [메뉴] > [동작모드] > [ID 인증] > [아이디+지문]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 대기화면에서 [ID 입력]을 누릅니다.
2. ID 입력 창이 나타나면 ID를 입력합니다.
3. 지문 입력 창이 나타나면 지문을 센서에 입력합니다.
4. 인증 성공 화면이 나타납니다.

■ 아이디+지문/비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [ID 인증] > [ID+지문/비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



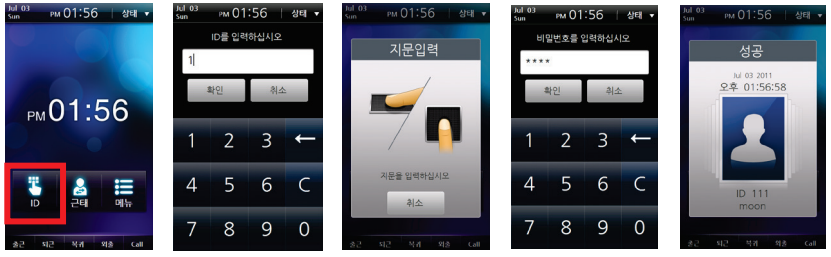
1. 대기화면에서 [ID 입력]을 누릅니다.
2. ID 입력 창이 나타나면 ID를 입력합니다.
3. 인증 창이 나타나면 버튼을 눌러 비밀번호를 입력하거나 지문을 센서에 입력합니다.
4. 인증 성공 화면이 나타납니다.

■ 아이디+지문+비밀번호 인증

<설정 방법>

1. [메뉴] > [동작모드] > [ID 인증] > [ID+지문+비밀번호]
2. “항상적용” 또는 해당 시간대를 선택합니다.

<인증 방법>



1. 대기화면에서 [ID 입력]을 누릅니다.
2. ID 입력 창이 나타나면 ID를 입력합니다.
3. 지문 입력 창이 나타나면 손가락을 센서에 올려놓습니다.
4. 비밀번호 입력 창이 나타나면 비밀번호를 입력하고 [확인]을 누릅니다.
5. 인증 성공 화면이 나타납니다.

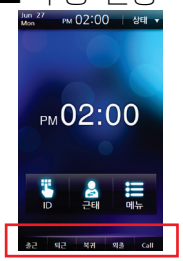
근태 인증

■ 근태 모드 설정

1 [메뉴] > [동작모드] > [근태관리]

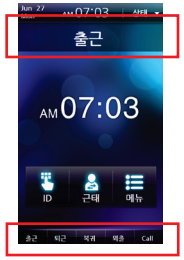
2 원하는 근태 관리 모드를 선택합니다.

■ 수동 변경



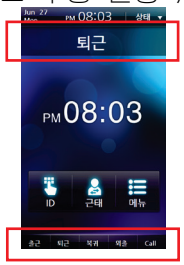
[수동 변경] 모드에서는 매 인증시 F1~F4 또는 추가 근태 이벤트키(근태)를 눌러서 근태 이벤트를 선택합니다. 선택된 근태 이벤트는 인증 후 해제됩니다.

■ 자동 변경



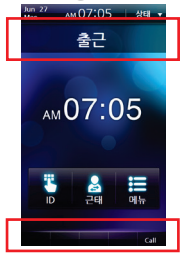
[자동 변경] 모드에서는 인증 시 해당 시간대의 근태 이벤트가 자동으로 적용됩니다. 해당 시간대의 근태 이벤트가 아닌 다른 근태 이벤트로 변경할 경우 근태키(F1~F4)를 눌러 특정 근태 이벤트를 선택할 수 있습니다.

■ 수동 변경 유지



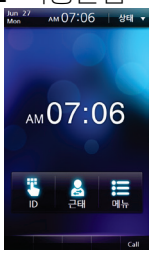
[수동 변경 유지] 모드에서는 [수동 변경]과 마찬가지로 인증시 F1~F4 또는 추가 근태 이벤트키를 눌러서 근태 이벤트를 선택합니다. 한 번 선택된 근태 이벤트가 다른 근태 이벤트를 선택하기 전까지 그대로 유지되는 것이 [수동 변경] 모드와의 차이점입니다.

■ 고정



[고정] 모드에서는 고정된 근태 이벤트로만 인증이 가능합니다. 다른 근태 이벤트는 선택할 수 없습니다.

■ 사용안함



근태 관리 없이 출입 인증만을 사용할 경우 선택합니다.
근태 버튼은 나타나지 않고 Call 버튼만 활성화됩니다.

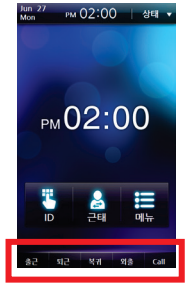
참고 *근태 이벤트 별 자동 변경 시간대 및 고정 근태 이벤트 설정은 BioStar 소프트웨어에서 가능합니다.*

■ 근태 인증 방법

1. F1~F4키 혹은 화면의 해당 근태버튼을 눌러 근태 이벤트를 선택합니다. (자동 변경이나 고정 모드에서는 생략)
2. 인증 절차를 수행합니다. (출입 인증과 동일)
3. 인증 성공 화면이 나타나고, 동시에 해당 근태가 적용됩니다.

■ 근태 이벤트

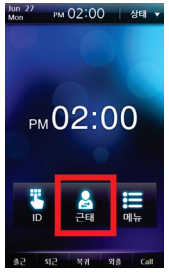
■ 기본 근태 이벤트(F1~F4)



기본 근태 이벤트는 총 4가지이며 화면 하단에 위치한 근태 버튼이나 F1~F4 키를 눌러 선택합니다.

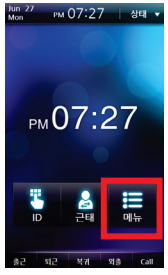
-출근: 출근 시 선택합니다.
-퇴근: 퇴근 시 선택합니다.
-복귀: 복귀 시 선택합니다.
-외출: 외출 시 선택합니다.

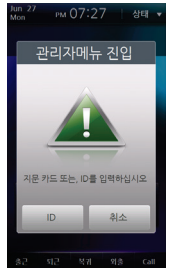
■ 추가 근태 이벤트

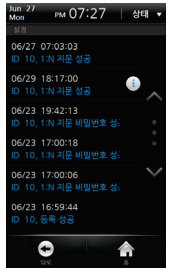


4가지 기본 근태 이벤트 외에 BioStar 소프트웨어에서 사전 정의한 추가 근태 이벤트(최대 12개)를 선택할 수 있습니다.
추가 근태 이벤트를 선택하려면 시작화면에서 [근태] 버튼을 누릅니다.

■ 개인별 출입/근태 기록 확인







사용자는 자신의 출입 및 근태 기록을 확인할 수 있습니다. 개인별 출입/근태 기록 확인을 위해서는 다음의 절차를 수행합니다.

1. 대기화면에서 [메뉴]를 선택합니다.
2. 지문 또는 카드를 입력하거나 [ID]를 눌러 입력합니다.
3. 자신의 출입/근태 기록을 확인할 수 있습니다.

참고

본 페이지의 개인별 출입/근태 기록 확인은 일반 사용자의 경우에만 해당하는 내용입니다. 관리자 등급의 사용자는 위의 방법으로 관리자 메뉴로 진입합니다. (p.51 참조)

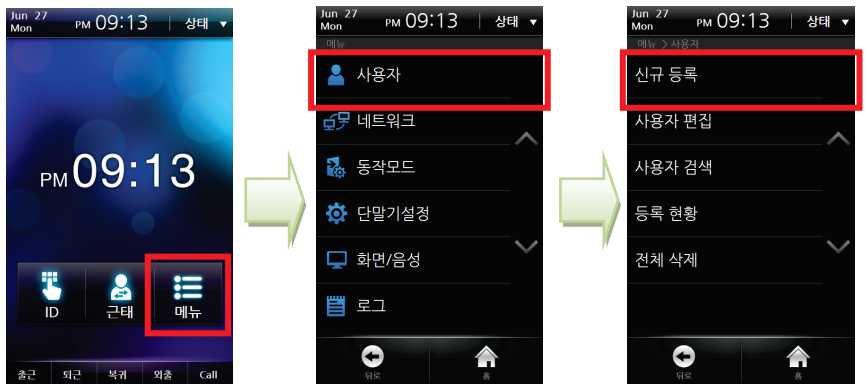
인증에 실패하는 경우

인증이 실패하였습니다	일반적인 인증 실패시 나타나는 화면입니다.
인증 모드 오류	현재 설정된 인증모드에 맞지 않는 경우에 나타나는 화면입니다.
인증 간격 제한	인증 간격제한에 의해서 인증이 제한된 경우에 나타나는 화면입니다.
인증 횟수 제한	인증 횟수 제한에 의해서 인증이 제한된 경우에 나타나는 화면입니다.
접근이 금지된 시간입니다	출입그룹에 의해서 인증이 제한된 경우에 나타나는 화면입니다.
Anti-passback 실패	Anti-passback에 의한 출입제한일 때 나타나는 화면입니다.
등록되지 않은 사용자입니다	등록되지 않은 사용자이거나 데이터 카드에 정보가 저장되지 않은 경우에 나타나는 화면입니다.

4 관리자 메뉴

관리자 등록

제품 출하시 관리자가 등록되어 있지 않습니다. BioStation T2를 설치한 후에는 즉시 관리자를 등록한 후 사용하십시오.
관리자는 사용자의 등록/삭제, 단말기 환경 설정 등의 기능을 사용할 수 있습니다.



1 [메뉴] > [사용자] > [신규 등록]을 선택합니다.

2 카드, 비밀번호, 지문 중 하나와 사용자 ID를 반드시 포함하여 사용자 정보를 입력합니다.

3 관리자 등급에 체크하고 [등록] 버튼을 눌러 관리자 등록을 마칩니다.

사용자 등록 항목

- 얼굴 입력
- 사용자 ID
- 이름
- 지문
- 카드 ID
- 비밀번호
- 관리자 등급
- 협박 손가락
- 항시통과카드
- 개별인증모드
- 출입그룹

참고 *관리자 등록 절차는 [관리자 등급]에 체크하는 것 이외에 사용자 등록과 동일하므로 사용자 등록 페이지(p.55~p.58)를 참고 바랍니다.*

■ 관리자 메뉴 진입

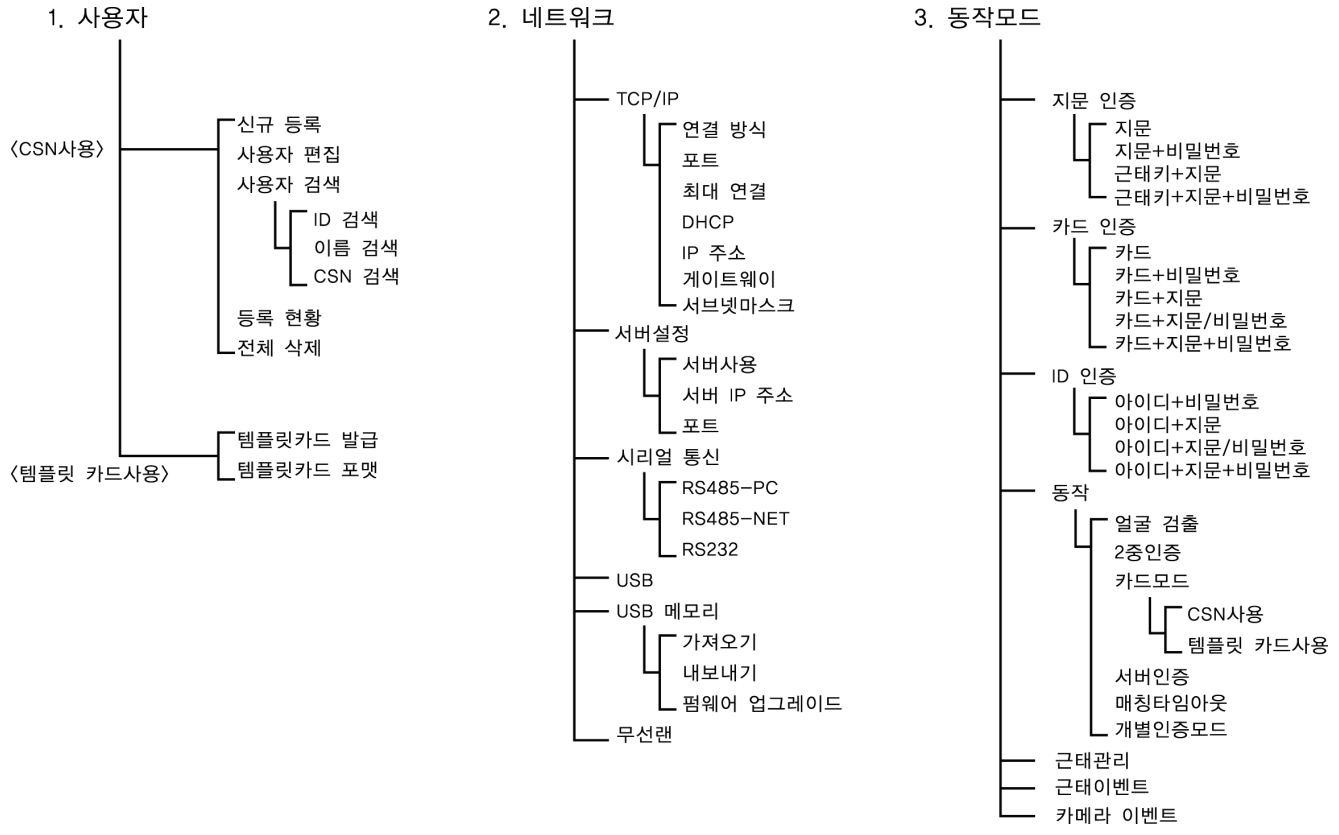


1. 초기 화면에서 [메뉴]를 누릅니다.
2. [관리자 메뉴 진입]화면이 나타납니다.
3. 지문, 카드 또는 ID를 입력합니다.
4. 비밀번호 입력이 필요한 경우 비밀번호를 입력하고 [확인]을 누릅니다.
5. [관리자 메뉴]가 나타납니다.

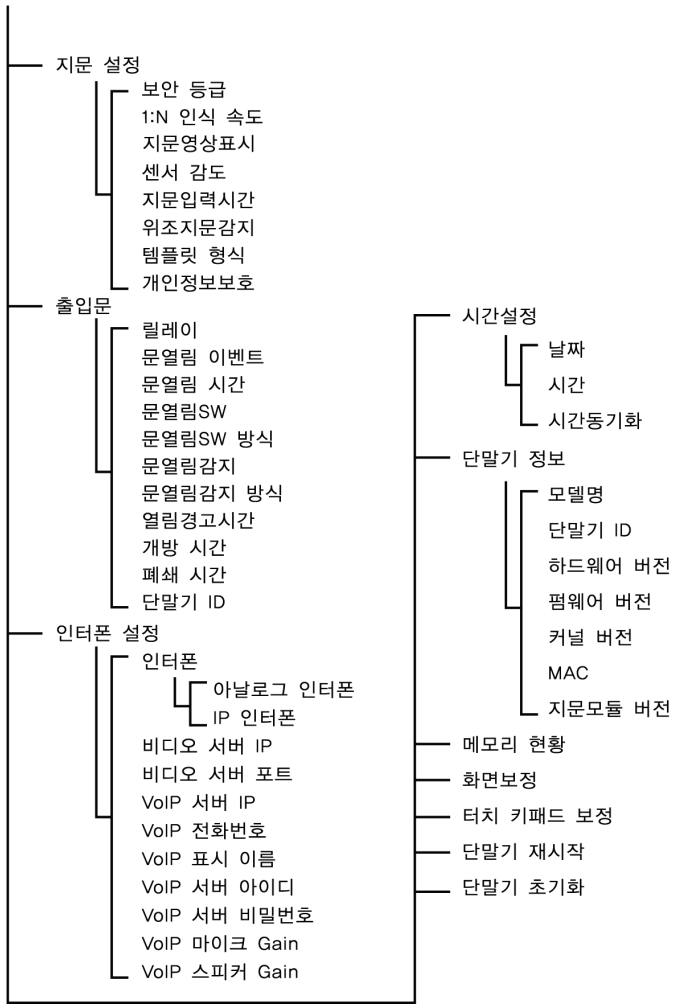
참고

- *사용자 등록이 되어 있지 않은 상태에서 [메뉴] 버튼을 누르면 아무런 인증 절차 없이 관리자 메뉴로 진입하게 됩니다.*
- *관리자가 아닌 일반 사용자의 경우에는 본인의 출입/근태 로그 확인 화면으로 이동합니다. (p.47 참조)*

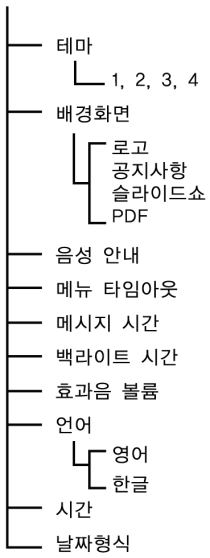
관리자 메뉴 구성


1. 사용자
〈CSN사용〉
신규 등록
사용자 편집
사용자 검색
ID 검색
이름 검색
CSN 검색
등록 현황
전체 삭제
〈템플릿 카드사용〉
템플릿카드 발급
템플릿카드 포맷
2. 네트워크
TCP/IP
연결 방식
포트
최대 연결
DHCP
IP 주소
게이트웨이
서브넷마스크
서버설정
서버사용
서버 IP 주소
포트
시리얼 통신
RS485-PC
RS485-NET
RS232
USB
USB 메모리
가져오기
내보내기
펌웨어 업그레이드
무선랜
3. 동작모드
지문 인증
지문
지문+비밀번호
근태키+지문
근태키+지문+비밀번호
카드 인증
카드
카드+비밀번호
카드+지문
카드+지문/비밀번호
카드+지문+비밀번호
ID 인증
아이디+비밀번호
아이디+지문
아이디+지문/비밀번호
아이디+지문+비밀번호
동작
얼굴 검출
2중인증
카드모드
CSN사용
템플릿 카드사용
서버인증
매칭타임아웃
개별인증모드
근태관리
근태이벤트
카메라 이벤트

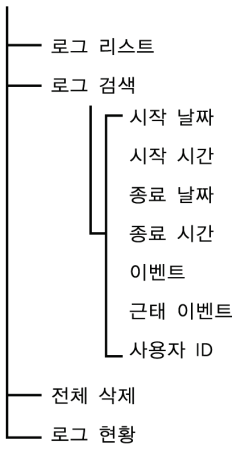
4. 단말기설정



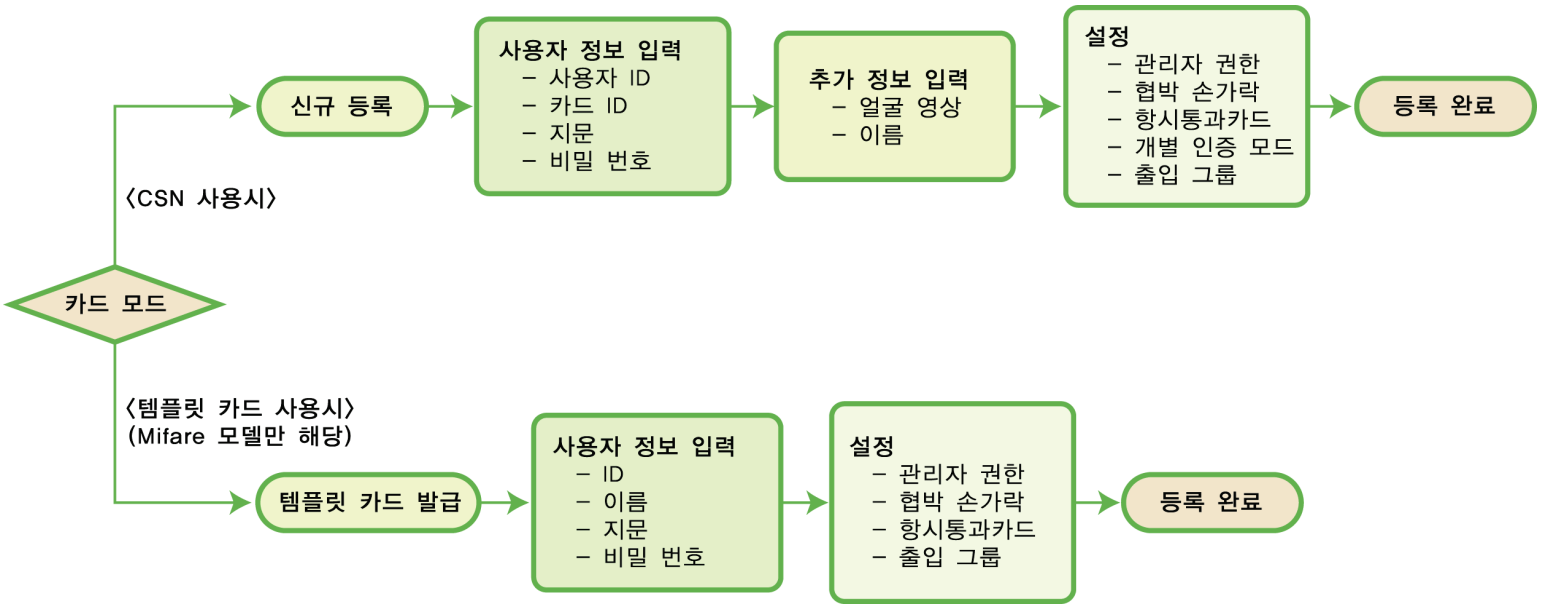
5. 화면/음성



6. 로그



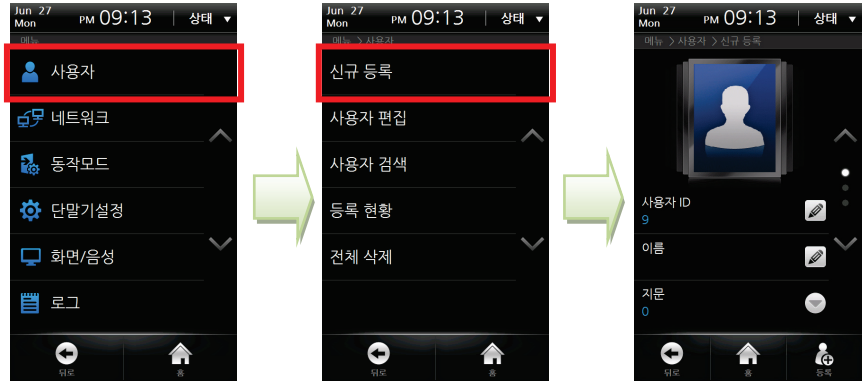
사용자 등록 과정


카드 모드
〈CSN 사용시〉
신규 등록
사용자 정보 입력
– 사용자 ID
– 카드 ID
– 지문
– 비밀 번호
추가 정보 입력
– 얼굴 영상
– 이름
설정
– 관리자 권한
– 협박 손가락
– 항시통과카드
– 개별 인증 모드
– 출입 그룹
등록 완료
〈템플릿 카드 사용시〉
(Mifare 모델만 해당)
템플릿 카드 발급
사용자 정보 입력
– ID
– 이름
– 지문
– 비밀 번호
설정
– 관리자 권한
– 협박 손가락
– 항시통과카드
– 출입 그룹
등록 완료

CSN 카드 사용시

단말기에 사용자 등록

CSN 카드는 카드가 입력되면 카드의 고유번호와 단말기에 등록 저장된 카드 고유번호와 비교해서 인증하는 방식입니다. 카드에 부여된 고유번호는 사용자 등록시 단말기에 저장됩니다.
CSN 카드를 사용할 경우 [동작모드] > [동작] > [카드모드]에서 CSN 카드를 선택합니다.
EM 모델의 경우 CSN 카드 방식만을 지원합니다.



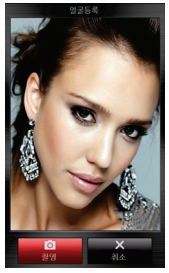
1. 관리자 메뉴에 진입한 후, [사용자] > [신규 등록]을 선택합니다.
2. 카드, 비밀번호, 지문 중 하나와 사용자 ID를 반드시 포함하여 사용자 정보를 입력합니다.
3. [등록] 버튼을 눌러 사용자 등록을 마칩니다.

사용자 등록 정보

- 얼굴 입력
- 사용자 ID
- 이름
- 지문
- 카드 ID
- 비밀번호
- 관리자 등급
- 협박 손가락
- 항시통과카드
- 개별인증모드
- 출입그룹

■ 신규 등록

■ 얼굴 입력



사진이 표시된 부분을 터치하면 내장된 카메라가 작동됩니다. LCD화면에 사용자의 얼굴이 나오면 [촬영]을 눌러 얼굴 정보를 입력합니다. 저장된 얼굴정보는 인증 성공 시에 보여지며 BioStar소프트웨어를 통해서도 사진 저장이 가능합니다.

■ 사용자 ID



사용자 ID를 입력한 후 [확인]을 누릅니다.
사용자 ID는 1~4294967295 범위 내의 숫자에서 선택할 수 있습니다.
신규 등록 메뉴 진입시 사용자 ID는 단말기에 의해서 자동 부여됩니다.

■ 이름



이름을 입력한 후 [확인]을 누릅니다.
이름은 한글, 영어, 숫자, 특수기호 사용이 가능합니다.

■ 지문

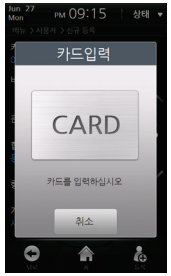


[지문] 메뉴를 선택하면 바로 인증에 사용할 지문을 등록하는 절차가 시작됩니다. 1~10개의 손가락을 등록할 수 있으며 일반적으로 한 사용자마다 두 개 이상의 손가락을 등록할 것을 권장합니다. 지문 등록시 확인을 위해 같은 손가락을 두 번씩 입력합니다. 한 손가락의 지문 입력 후 나타나는 확인창에서 [확인]을 누르면 연이어 다음 손가락 입력을, [취소]를 누르면 입력을 종료합니다. 입력 후 입력된 손가락 개수가 메뉴 아래에 표시됩니다.

주의!	- 상처가 있거나 지문이 희미한 손가락을 등록하지 마십시오. - 지문의 인증 성공률이 낮으면 그 지문정보를 삭제하고 새로운 지문을 등록하십시오.

참고	*바른 입력을 위해 15 페이지의 [올바른 지문 입력 방법]을 참조바랍니다.*

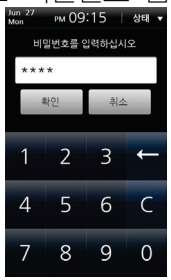
■ 카드 ID입력



카드 ID는 카드에 내장된 정보를 읽어서 등록됩니다.
카드를 입력하라는 화면이 나오면 카드 인식부에 카드를 접근시킵니다.

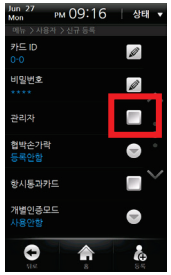
참고 *사용자 ID와 카드/비밀번호/지문 중 하나는 반드시 입력해야 등록할 수 있습니다.*

■ 비밀번호 입력



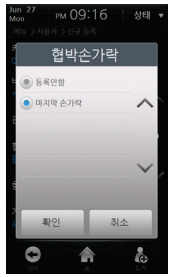
비밀번호를 입력한 후 [확인]을 누릅니다. 비밀번호는 확인을 위해 두 번 입력하게 되며, 4~16자리의 숫자로 구성됩니다. 4자리 미만의 숫자를 입력한 경우 알림 메시지가 표시되고 비밀번호 등록이 되지 않습니다.

■ 관리자 등급 설정



체크하면 사용자가 관리자로 등록되며 체크하지 않으면 일반 사용자로 등록됩니다.

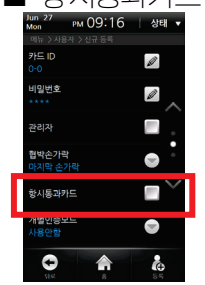
■ 협박 손가락 설정



협박을 당해 강제로 출입문을 열어야 하는 경우를 대비하여 [협박 손가락]을 등록할 수 있습니다. 협박 손가락으로 인증하는 경우 정상적으로 출입문은 열리지만 BioStar에서 설정해 놓은 비상경보장치를 울릴 수 있습니다.
[지문] 메뉴에서 지문을 2개 이상 입력했을 경우에만 설정 가능하며 설정 창에서 [마지막 손가락]을 선택하면 마지막에 입력한 손가락을 협박 손가락으로 사용하게 됩니다.

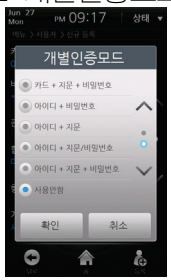
주의!
- 일반적으로 출입할 때는 협박 손가락을 사용하지 마십시오.
- 자연스럽게 사용할 수 있는 손가락을 협박 손가락으로 등록하십시오.
- 협박 손가락으로 인증할 때 자동적으로 문이 닫히거나 무소음 경보가 발동할 수 있으니 이러한 상황을 사용자에게 충분히 설명하십시오.

■ 항시통과카드 설정



필요한 경우 [항시통과카드]를 선택하여 체크합니다. [항시통과카드]로 등록된 사용자의 경우 단말기 카드인증모드에 관계없이 항상 인증됩니다.

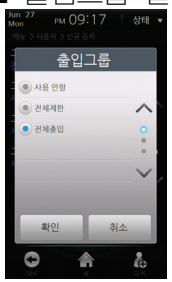
■ 개별인증모드 설정



필요한 경우 개별인증모드를 설정합니다. 개별인증모드가 선택된 사용자는 단말기 인증모드에 우선해서 선택된 개별 인증모드로 인증됩니다.
설정된 개별인증모드는 해당 인증수단에 대해서만 동작합니다.

> 참고 *개별인증모드를 사용하기 위해서는 [메뉴] > [동작모드] > [동작]에서 [개별인증모드]에 체크합니다.*

■ 출입그룹 설정



필요한 경우 출입그룹을 설정합니다. 출입그룹은 해당 사용자의 출입가능여부를 설정합니다. BioStar 소프트웨어에서 해당단말기로 전송한 출입그룹 중에 선택이 가능합니다.

■ 등록



1. 우측 하단의 [등록] 버튼을 누릅니다.
2. 등록 완료 창이 나타납니다. 사용자 등록을 마쳤습니다.

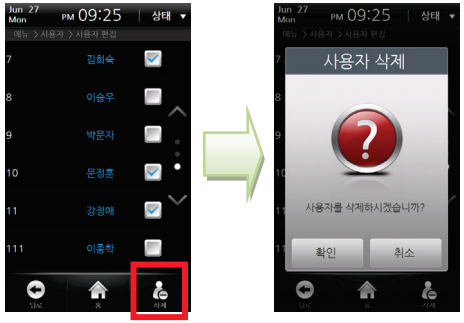
■ 사용자 편집 및 삭제

[메뉴] > [사용자] > [사용자 편집]을 선택합니다.



1. 사용자 목록에서 수정을 원하는 사용자의 이름을 클릭합니다.
2. 사용자 정보를 수정한 후 [등록]을 누릅니다. 신규 사용자를 등록하는 절차와 동일합니다.
3. 등록 성공 창이 나타납니다.

특정 사용자를 삭제하려면 다음의 절차를 수행합니다.



1. 사용자 목록에서 삭제를 원하는 사용자의 우측 체크박스에 체크하여 선택합니다.
2. 화면 오른쪽 아래 [삭제] 아이콘을 클릭합니다.
3. 사용자 삭제 확인창에서 확인을 눌러 삭제합니다.

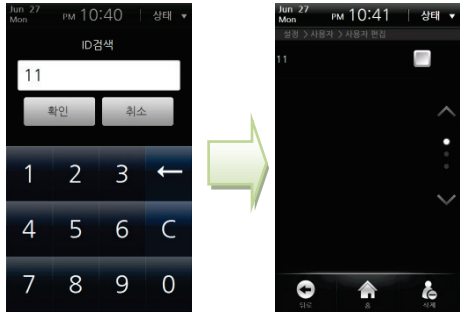
주의!	BioStar 소프트웨어의 데이터베이스에 저장되어 있지 않은 상태에서 사용자를 삭제할 경우, 복구할 수 없습니다.

■ 사용자 검색

[메뉴] > [사용자] > [사용자 검색]을 누른 후 검색 방법을 선택합니다.



ID로 검색



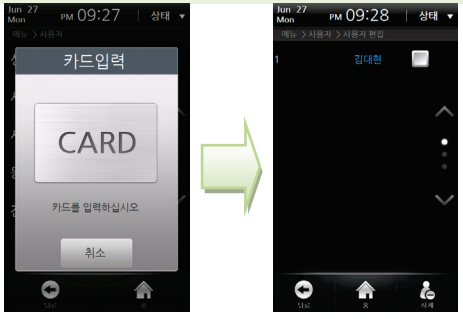
ID검색 창이 나타나면 숫자 ID를 입력하고 [확인]을 누릅니다. 입력한 ID와 일치하는 사용자가 검색됩니다.

이름 검색



이름검색 창이 나타나면 이름을 입력하고 [확인]을 누릅니다. 전체 이름을 모두 입력할 필요는 없으며 앞의 몇 글자만 입력하면 입력한 글자로 시작되는 이름을 가진 사용자가 모두 검색됩니다.

CSN 검색



카드를 입력하라는 창이 나타나면 CSN 카드를 카드 인식부에 접근시킵니다. 해당 카드를 사용하는 사용자가 검색됩니다.

■ 사용자 등록현황 확인



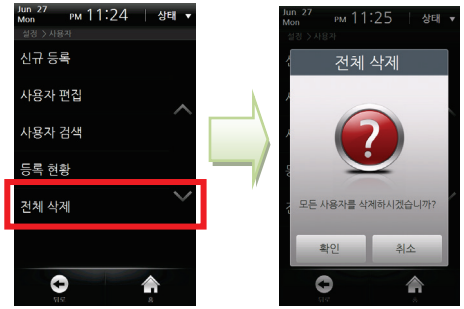
1 [메뉴] > [사용자] > [등록 현황]을 선택합니다.

2 현재 등록된 사용자/사용자 영상/템플릿의 수와 남아 있는 등록가능 용량을 확인할 수 있습니다.

참고 *최대 200,000 명까지 저장할 수 있습니다. 사용자 영상은 최대 5,000 건까지 저장할 수 있습니다. 템플릿은 최대 400,000 건까지 저장할 수 있습니다.*

■ 사용자 전체 삭제

단말기에 등록된 사용자를 모두 삭제합니다.



1 [메뉴] > [사용자] > [전체 삭제]를 누릅니다.

2 전체 삭제 확인창의 [확인]을 누르면 단말기에 등록된 사용자 정보가 모두 삭제됩니다.

주의! BioStar 소프트웨어의 데이터베이스에 저장되어 있지 않은 상태에서 사용자를 삭제할 경우, 복구할 수 없습니다.

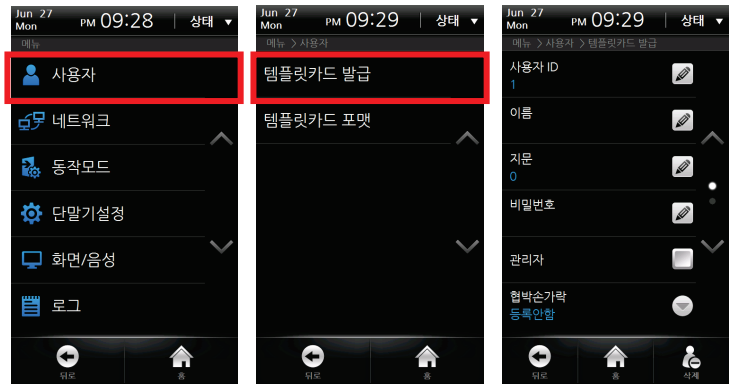
템플릿 카드 사용시 (Mifare 모델만 해당)

카드에 사용자 등록

■ 템플릿 카드 발급

템플릿 카드는 카드가 입력되면 카드에서 사용자 정보를 읽어서 인증하는 방식입니다. 사용자 등록시 카드의 데이터 영역에 사용자 아이디 및 기타 인증 정보를 저장합니다.
템플릿 카드를 사용할 경우 사용자 정보와 지문 정보가 단말기에 저장되지 않고 카드에만 저장되므로 사용자 정보에 대한 별도의 관리가 필요합니다.
템플릿 카드를 사용할 경우 [동작모드] > [동작] > [카드모드]에서 템플릿 카드를 선택합니다.

1. 관리자 메뉴에서 [사용자] > [템플릿카드 발급]을 선택합니다.
2. 등록 화면이 나타나면 사용자 정보를 입력합니다.
3. 사용자 ID, 이름, 지문, 비밀번호를 입력합니다.
4. 관리자 등급, 협박 손가락, 항시통과카드, 출입 그룹 등의 항목을 설정합니다.
5. 우측 아래의 [발급] 버튼을 누르고 설명에 따라 카드를 단말기에 접근하여 등록을 완료합니다.



참고

- [항시통과카드]로 등록된 사용자의 경우 단말기 인증모드에 관계없이 항상 인증됩니다.
- [출입그룹]은 해당 사용자의 출입가능여부를 설정합니다. BioStar 소프트웨어에서 해당단말기로 전송한 출입그룹 중에 선택이 가능합니다.

주의!

CSN 카드와 템플릿 카드는 혼용해서 사용할 수 없으니 주의하십시오.

■ 카드 포맷

템플릿 카드 방식으로 사용할 카드에 저장된 기존 데이터를 모두 지웁니다.



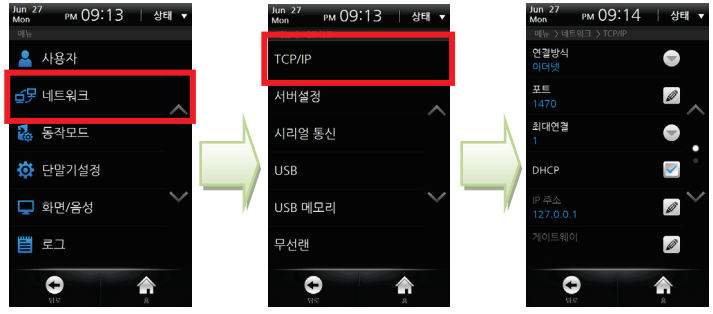
1. [메뉴] > [사용자] > [템플릿카드 포맷]을 선택합니다.
2. 포맷할 템플릿 카드를 카드 인식부에 접근시킵니다.
3. 카드 포맷 확인 창이 표시됩니다.

네트워크 설정

BioStation T2의 네트워크 연결을 설정합니다. 네트워크 연결에는 BioStar 클라이언트에서 단말기로 접속하는 직접 연결과 단말기가 BioStar 서버로 접속하는 서버 연결이 있습니다.

TCP/IP 설정

단말기와 BioStar소프트웨어를 연결할 때의 TCP/IP 방식을 설정합니다.



1 [메뉴] > [네트워크] > [TCP/IP]를 선택합니다.

2 **연결방식:** TCP/IP 연결에 사용할 통신방식을 선택합니다. (설정값: 사용안함/이더넷/무선랜)

3 **포트:** 단말기의 TCP/IP 포트를 지정합니다. 기본값은 '1470'으로 설정되어 있습니다. BioStar 클라이언트가 단말기로 접속할 경우 사용됩니다.

4 **최대연결:** 단말기에 동시 접속할 수 있는 BioStar 클라이언트 수를 설정합니다.(설정값: 1/4/8/16)

5 **DHCP:** DHCP 사용여부를 체크합니다.

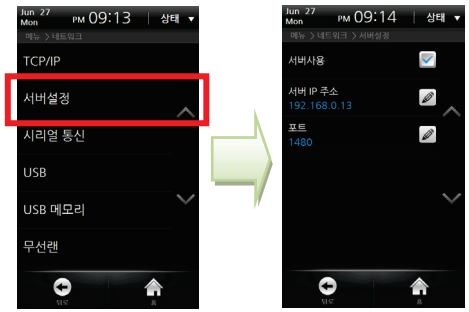
6 **IP주소:** DHCP 방식 대신 고정 IP를 사용할 경우의 IP 주소를 입력합니다. IP 주소를 모를 경우 관리자에게 문의하여 입력하십시오.

7 **게이트웨이:** DHCP 방식대신 고정 IP를 사용할 경우의 게이트웨이 주소를 입력합니다. 관리자에게 문의하여 입력하십시오.

8 **서브넷마스크:** DHCP 방식 대신 고정 IP를 사용할 경우의 서브넷마스크 주소를 입력합니다. 관리자에게 문의하여 주십시오.

서버 설정

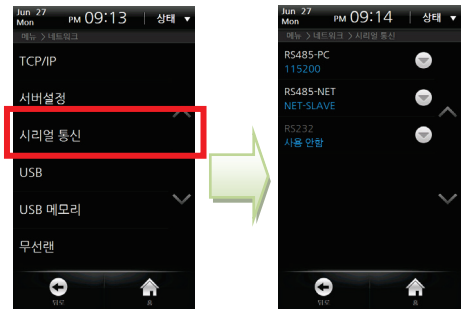
단말기는 BioStar 소프트웨어 서버 또는 SDK를 이용하여 만든 서버 Application으로 접속할 수 있습니다.
[서버설정]에서 연결할 서버의 IP와 포트를 설정해야 서버와 통신이 가능합니다.



1. [메뉴] > [네트워크] > [서버설정]를 선택합니다.
2. **서버사용:** 서버 사용 여부를 체크합니다.
3. **서버 IP 주소:** 서버의 IP를 입력한 후 [확인]을 누릅니다.
4. **포트:** 서버의 포트를 입력한 후 [확인]을 누릅니다.
5. 설정 후 [뒤로]나 [홈] 버튼을 눌러 변경된 사항을 적용합니다.

시리얼통신

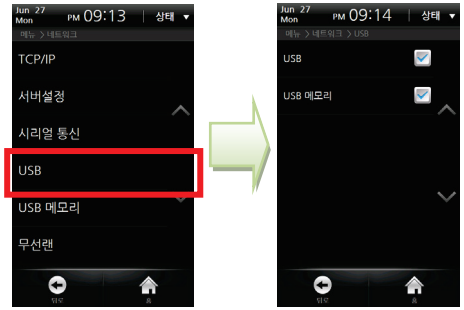
시리얼 통신은 RS485 혹은 RS232를 사용합니다.



1. [메뉴] > [네트워크] > [시리얼 통신]을 선택합니다
2. **RS485-PC:** 단말기와 PC간 통신 사용 여부 및 통신속도를 설정합니다.
   (설정값 : 115200/57600/38400/19200/9600/사용안함)
3. **RS485-NET:** RS485 상에 다른 단말기 또는 Secure I/O와 연결하는 경우 사용합니다.
   - Net-Slave : 해당 단말기를 Slave로 설정합니다.
   - Net-Host : 해당 단말기를 Host로 설정합니다.
4. **RS232 :** 단말기와 PC간 통신 사용 여부 및 통신속도를 설정합니다. RS232는 RS485-PC와 물리적으로 동일한 포트를 이용하기 때문에 RS485가 사용안함으로 설정된 경우에만 사용 가능합니다.
   (설정값 : 사용안함/9600/19200/38400/57600/115200)

참고	*단말기 간 RS485 통신은 1대의 호스트 단말기와 총 7대까지의 슬레이브로 구성이 가능합니다. 이 때 Secure I/O는 최대 4대까지 연결 가능합니다.*

USB

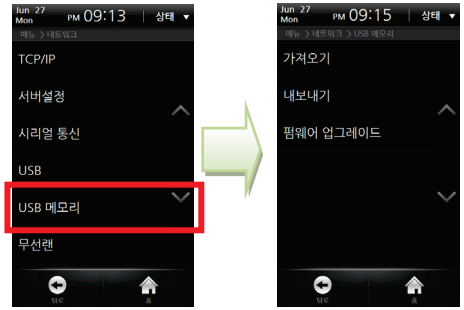


1 [메뉴] > [네트워크] > [USB]를 선택합니다.

2 **USB** : PC와의 USB 연결을 허가할지 여부를 설정합니다. (Mini USB)

3 **USB 메모리** : USB 메모리의 연결을 허가할지 여부를 설정합니다. (USB A Type)

USB 메모리



1 [메뉴] > [네트워크] > [USB 메모리]를 선택합니다.

2 **가져오기:** 선택 창에서 데이터를 가져올 단말기 ID를 선택한 후 [확인]을 누릅니다.

3 **내보내기:** 내보내기 터치 후 동작이 완료할 때까지 기다립니다.

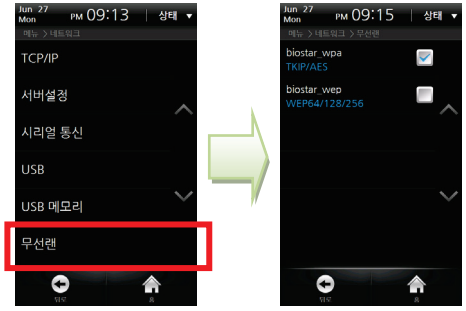
4 **펌웨어 업그레이드:** 업그레이드 할 버전을 선택한 후 [확인]을 누릅니다.

5 가져오기 및 펌웨어 업그레이드 수행 후에 단말기는 재부팅하게 됩니다.

참고	*[메뉴] > [네트워크] > [USB]에서 USB 메모리 항목에 체크하여 사용으로 설정되어야만 [USB 메모리] 메뉴에 진입이 가능합니다.*

무선랜

단말기에서는 BioStar를 통해서 사전에 저장된 4개의 무선랜 설정(Preset) 중 하나를 선택할 수 있습니다.
Preset은 BioStar 소프트웨어에서 SSID와 암호화 방식, 암호화 키 등을 입력하여 설정합니다.



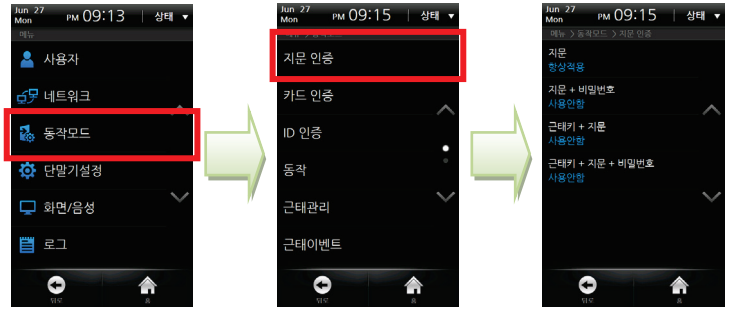
1 [메뉴] > [네트워크] > [무선랜]를 선택합니다.

2 무선랜 연결에 사용할 설정(Preset)을 선택합니다.

동작 모드

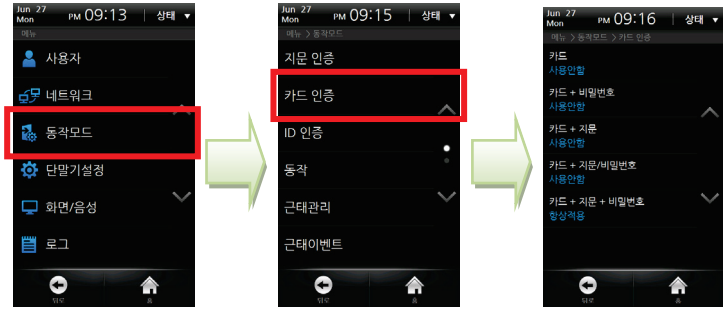
지정한 시간대에 설정한 동작모드로 인증이 가능합니다. 인증모드 설정시 사용되는 적용 시간대는 BioStar를 통해서 설정된 시간대 중에 선택 가능하고 최대 128개까지 선택 항목에 보일 수 있습니다.

지문 인증



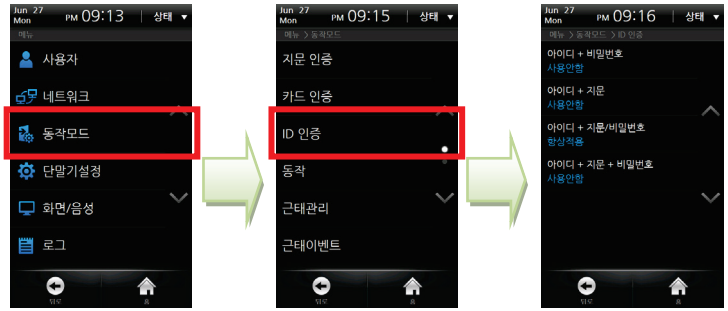
1. [메뉴] > [동작모드] > [지문 인증]을 선택합니다.
2. **지문:** 지문만으로 인증하는 방식입니다.
3. **지문+비밀번호:** 지문 입력 후에 비밀번호를 입력하여 인증하는 방식입니다.
4. **근태키+지문:** 해당 근태 이벤트 키를 누르고 지문을 입력하여 인증하는 방식입니다.
5. **근태키+지문+비밀번호:** 해당 근태 이벤트 키를 누르고 지문 입력 후에 비밀번호를 입력하는 방식입니다.

카드 인증



1. [메뉴] > [동작모드] > [카드 인증]을 선택합니다.
2. **카드:** 카드만으로 인증하는 방식입니다. 인증 방식을 [카드]로 설정해 놓은 경우, [동작] > [카드 모드]에서 인증에 사용할 카드 방식을 반드시 설정해야 합니다.
3. **카드+비밀번호:** 카드 입력 후에 비밀번호를 입력하여 인증하는 방식입니다.
4. **카드+지문:** 카드 입력 후에 지문을 입력하여 인증하는 방식입니다.
5. **카드+지문/비밀번호:** 카드를 입력한 후에 지문이나 비밀번호를 입력하여 인증하는 방식입니다.
6. **카드+지문+비밀번호:** 카드를 입력하고 지문을 입력한 후 비밀번호를 입력하는 방식입니다.

ID 인증



1 [메뉴] > [동작모드] > [ID 인증]을 선택합니다.

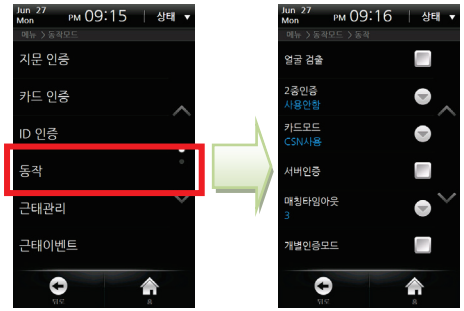
2 **아이디+비밀번호:** 아이디를 입력한 후에 비밀번호를 입력하여 인증하는 방식입니다.

3 **아이디+지문:** 아이디를 입력한 후 지문을 입력하여 인증하는 방식입니다.

4 **아이디+지문/비밀번호:** 아이디를 입력한 후 지문이나 비밀번호를 입력하여 인증하는 방식입니다.

5 **아이디+지문+비밀번호:** 아이디를 입력하고 지문을 입력한 후 비밀번호를 입력하는 방식입니다.

동작



1 [메뉴] > [동작모드] > [동작]을 선택합니다.

2 **얼굴 검출:** 얼굴검출 사용모드를 설정합니다. 체크할 경우, 카드나 비밀번호 인증 후 얼굴이 검출되어야 성공으로 처리됩니다.

3 **2중 인증:** 2중 인증 모드를 설정합니다. 2중 인증을 사용하는 경우, 서로 다른 두 사용자가 15초 이내 인증해야 출입문이 열립니다. 첫 번째 인증 후에 15초가 경과하면 첫 번째 인증은 무효가 되고 다시 두 번의 인증을 기다리는 상태로 돌아갑니다.

4 **카드 모드:** 단말기에 사용할 카드 타입을 설정합니다. EM 모델의 경우는 CSN 카드 방식만 지원합니다.
(설정값: 사용안함/CSN사용/템플릿카드사용)
- CSN카드: 카드에 부여된 고유번호를 읽어서 단말기에 저장한 후, 카드가 입력되면 카드에서 고유번호를 읽고 단말기에 저장된 카드 고유번호와 비교해

서 인증하는 방식입니다.
- 템플릿 카드: 카드에 사용자 아이디 및 기타 인증 정보를 저장하고, 카드가 입력되면 카드에서 사용자 정보를 읽어서 인증하는 방식입니다.

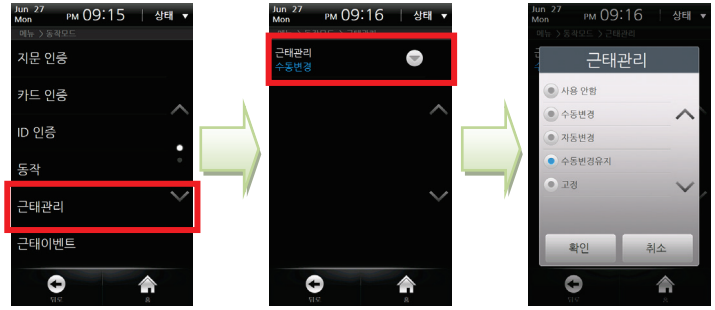
5 **서버 인증:** 서버인증 사용여부를 체크합니다. 서버인증 사용 시에는 단말기에 저장된 사용자 정보가 아닌 서버에 저장된 사용자 정보를 기준으로 인증합니다.
서버와 연결이 끊기는 경우에는 설정변경 없이 단말기에 저장된 사용자 정보를 기준으로 인증합니다. 서버인증은 BioStar SE 로 접속한 경우에만 사용가능합니다.

6 **매칭 타임 아웃:** 인증 시 대기 시간 및 얼굴 검출 시 대기 시간을 설정합니다.(설정값: 5/10/15/20/25/30)
매칭 시간 내에 인증이 되지 않거나 얼굴이 검출되지 않으면 인증 실패로 처리됩니다.

7 **개별인증모드:** 개별인증 모드의 사용여부를 체크합니다.
개별인증모드 사용 설정 시에는 개별 사용자 별로 등록 시에 설정한 인증모드로 동작합니다.

근태관리

단말기에 적용할 근태모드를 설정합니다.



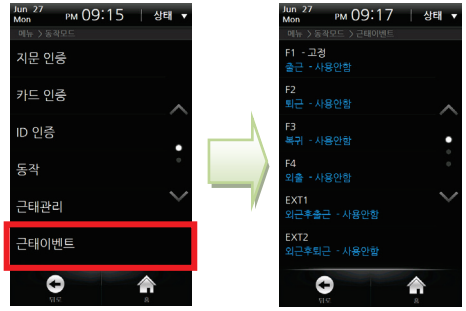
1 [메뉴] > [동작모드] > [근태관리]를 선택합니다.

2 [근태관리]를 눌러서 모드를 설정합니다.
(사용 안함/수동변경/자동변경/수동변경유지/고정)

참고 *자세한 근태모드 설명은 [3 장 사용자 메뉴>근태인증>근태모드설정(p.46)]을 참조하세요.*

근태 이벤트

근태 이벤트는 BioStar 소프트웨어를 이용하여 F1~F4 또는 추가 근태 이벤트(EXT 01~12)에 해당하는 근태이벤트와 자동 시간대 및 고정 여부를 조회할 수 있습니다. 근태 이벤트 설정은 BioStar 소프트웨어에서만 가능하며 단말기에서는 조회만 가능합니다.



1. [메뉴] > [동작모드] > [근태 이벤트]를 선택합니다.
2. BioStar 소프트웨어에서 설정한 내용을 확인할 수 있습니다.

카메라 이벤트

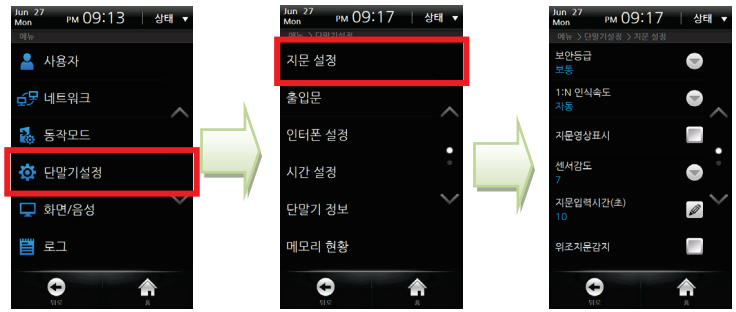
카메라 이벤트로 설정된 이벤트가 발생할 경우에 정지 영상을 촬영하여 정지 영상 로그를 저장합니다. 카메라 이벤트 설정은 BioStar소프트웨어에서만 가능하고, 단말기에서는 조회만 가능합니다.

1. [카메라 이벤트]를 선택합니다.
2. BioStar 소프트웨어에서 설정한 내용을 확인할 수 있습니다.

단말기 설정

■ 지문 설정

[메뉴] > [단말기설정] > [지문 설정]을 선택합니다.



1 보안등급(보통/안전/가장안전): 보안등급은 타인 오인식률(FAR, False Acceptance Ratio)에 의해 결정됩니다. FAR은 등록되지 않은 지문을 받아들일 확률을 의미하는 것으로 이 확률을 낮출수록 보안성이 높아지는 장점이 있는 반면, 본인 거부율(FRR, False Reject Rate)이 높아지게 되어 등록된 사용자의 경우 인식률이 더 낮아지는 단점이 있습니다.
일반적인 근태관리 등의 용도로는 보통 단계를 권장하지만, 고도의 출입통제보안이 요구되는 경우 안전이나 가장안전 단계로 보안 등급을 높일 것을 권장합니다.

2 1:N 인식속도(보통/빠름/가장빠름/자동): 수백 명 이상의 사용자 정보가 저장되어 있고 1:N 인식모드를 사용할 경우 인식시간이 길어질 수 있습니다. 이 경우 1:N 인식속도를 좀 더 빠르게 설정하여 인식 시간을 줄일 수 있습니다. 이 때, FRR이 다소 높아질 수 있습니다. [자동]을 선택하면 장치에 등록된 총 지문 템플릿의 수에 따라 자동으로 판별 속도가 결정됩니다.

3 지문영상표시: 화면에 보일 지문 영상 사용 여부를 체크합니다. 지문 등록시 입력한 지문의 영상을 LCD 화면에서 확인하여 올바른 지문 입력을 유도할 수 있습니다.

4 센서 감도(0[최소]~7[최대]): 지문 센서가 손가락을 받아들이는 감도를 설정합니다. 높은 감도에서는 지문 입력이 쉬워지는 장점이 있습니다. 반면, 낮은 감도에서는 입력된 지문 영상이 항상 높은 품질을 유지할 수 있는 장점이 있습니다. 일반적인 사용 환경에서는 최대값으로 설정할 것을 권장합니다. 직사광선의 영향을 받을 경우 이 값을 낮게 함으로써 영향을 완화시킬 수 있습니다.

5 지문입력시간(1초~20초): 지문을 입력을 마쳐야 하는 시간을 설정하고 [확인]을 누릅니다. 정해진 시간 안에 지문을 입력하지 않으면 인증이 실패하게 됩니다.

6 위조지문감지: 위조지문공격을 방지하기 위한 검사의 사용 여부를 체크합니다.

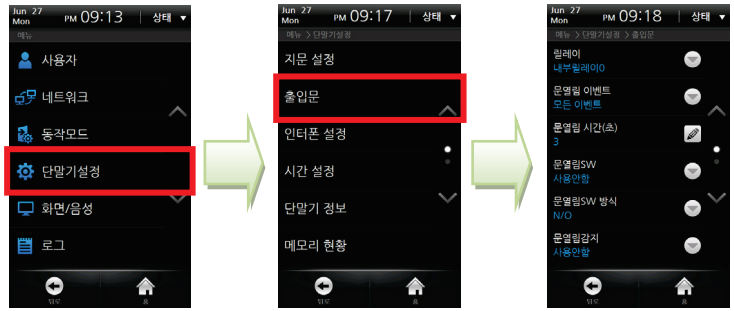
7 템플릿 형식(Suprema/ISO/ANSI): 템플릿 형식을 설정하고 [확인]을 누릅니다.

8 개인정보보호: 개인정보보호 설정여부를 체크합니다.

참고 *일반적인 사용 환경에서는 기본값 사용을 권장합니다.*

출입문

[메뉴] > [단말기설정] > [출입문]을 선택합니다.



1 **릴레이:** 사용자 인증시 출입문에 사용할 릴레이를 선택합니다. (설정값: 사용안함/ 내부릴레이0/ 내부릴레이1/ 외부릴레이0/ 외부릴레이1/ SIO0 릴레이0/ SIO0 릴레이1/ SIO1 릴레이0/ SIO1 릴레이1/ SIO2 릴레이0/ SIO2 릴레이1/ SIO3 릴레이0/ SIO3 릴레이1)

2 **문열림 이벤트:** 출입문을 개방할 이벤트를 설정합니다.
- 모든 이벤트: 일반 인증 및 근태인증에 관계없이 문이 열립니다.
- 인증 이벤트: 근태 인증이 아닌 일반인증에 대해서만 문이 열립니다.
- 근태 이벤트: 근태 인증 중에 릴레이 사용 설정이 된 근태 이벤트에 대해서만 문이 열립니다.
- 인증+근태 이벤트: 일반 인증과 근태 인증 중에 릴레이 사용 설정이 된 근태 이벤트에 대해서만 문이 열립니다.
- 사용안함: 일반 인증 및 모든 근태 이벤트에 대해서 문이 열리지 않습니다.

3 **문열림 시간(초):** 이벤트 발생시 출입문 릴레이의 개방 시간을 설정합니다. 설정한 시간 이후에는 다시 출입문 릴레이가 닫힙니다.

4 **문열림SW:** 문 열림 스위치에 사용할 입력을 선택하고 [확인]을 누릅니다. (설정값: 입력0/ 입력1/ 입력2/ 입력3/ SIO0 입력0/ SIO0 입력1/ SIO0 입력2/ SIO0 입력3/ SIO1 입력0/ SIO1 입력1/ SIO1 입력2/ SIO1 입력3/ SIO2 입력0/ SIO2 입력1/ SIO2 입력2/ SIO2 입력3/ SIO3 입력0/ SIO3 입력1/ SIO3 입력2/ SIO3 입력3)

5 **문열림SW방식:** 문 열림 스위치의 작동 방식을 선택하고 [확인]을 누릅니다. (설정값: N/O, N/C)

6 **문열림 감지:** 출입문이 개방될 경우, 문 열림 감지에 사용할 입력을 선택하고 [확인]을 누릅니다.
(설정값: 입력0/ 입력1/ 입력2/ 입력3/ SIO0 입력0/ SIO0 입력1/ SIO0 입력2/ SIO0 입력3/ SIO1 입력0/ SIO1 입력1/ SIO1 입력2/ SIO1 입력3/ SIO2 입력0/ SIO2 입력1/ SIO2 입력2/ SIO2 입력3/ SIO3 입력0/ SIO3 입력1/ SIO3 입력2/ SIO3 입력3)

7 **문열림감지 방식:** 문 열림 감지 입력의 작동 방식을 선택한 후 [확인]을 누릅니다. (설정값: N/O, N/C)

8 **열림경고시간(초):** 출입문이 개방된 이후 장시간 열림 경고 이벤트가 발생할 때까지의 시간을 설정합니다.

9 **개방 시간:** 출입문을 강제로 열어 놓을 시간대를 설정합니다. 개방 시간 동안에는 출입문이 닫히지 않습니다. 개방 시간에 사용할 시간대는 BioStar 프로그램에서 설정할 수 있습니다.

10 **폐쇄 시간:** 출입문을 강제로 잠그는 시간대를 설정합니다. 폐쇄 시간에 사용할 시간대는 BioStar 프로그램에서 설정할 수 있습니다.

■ 인터폰 설정

[메뉴] > [단말기설정] > [인터폰 설정]을 선택합니다.



인터폰이 설정되면 BioStation T2 단말기의 Call키를 눌러 통화할 수 있습니다. 인터폰의 종류에 따른 통화 화면은 다음과 같습니다.



아날로그 인터폰



IP 인터폰

1 **인터폰:** 사용할 인터폰을 선택한 후 [확인]을 누릅니다. (사용안함/아날로그인터폰/IP인터폰)

2 **비디오 서버 IP:** IP 인터폰을 선택했을 경우 비디오 서버 IP를 입력합니다. 관리자에게 문의하여 주십시오.

3 **비디오 서버 포트:** 비디오 서버의 포트를 입력합니다. 관리자에게 문의하여 주십시오.

4 **VoIP 서버 IP:** IP 인터폰을 선택했을 경우 VoIP 서버 IP를 입력합니다.

5 **VoIP 전화번호:** IP 인터폰을 선택했을 경우 VoIP 전화번호를 입력합니다.

6 **VoIP 표시이름:** IP 인터폰을 선택했을 경우 VoIP 표시이름을 입력합니다.

7 **VoIP 서버 아이디:** VoIP 서버 아이디를 입력합니다. (아이디는 한글, 영어, 숫자, 특수기호가 사용 가능합니다.)

8 **VoIP 서버 비밀번호:** VoIP 서버 비밀번호를 입력한 후 [확인]을 누릅니다.

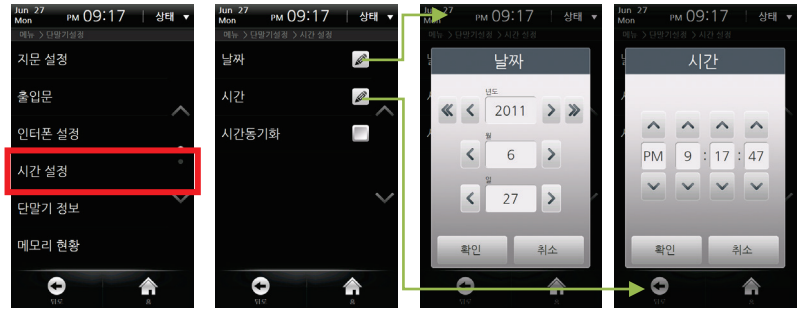
9 **VoIP 마이크 Gain:** VoIP 마이크의 볼륨을 조절합니다. (0~10)

10 **VoIP 스피커 Gain:** VoIP 스피커의 볼륨을 조절합니다. (0~10)

참고	*BioStation T2와 연동 가능한 아날로그 인터폰 목록은 아래와 같습니다.* - *COMMAX / CAV-35N* - *COMMAX / CAV-50H* - *COMMAX / CAV-50P*

시간 설정

단말기에 표시되는 시간을 설정합니다. 단말기 시간을 설정해야 출입 시간과 로그 데이터가 정확하게 저장됩니다.
[메뉴] > [단말기설정] > [시간 설정]을 선택합니다.



1. **날짜(YYYY/MM/DD):** [<], [>]를 이용하여 현재 날짜를 입력한 후 [확인]을 누릅니다.
2. **시간(PM//hh/mm/ss):** [∧], [∨]를 이용하여 현재 시간을 입력한 후 [확인]을 누릅니다.
3. **시간 동기화:** 동기화는 서버에 연결할 경우 사용 가능합니다. 단말기의 시간을 서버에 맞춥니다. 시간 동기화는 1시간에 한 번 수행되며, BioStar 서버와 단말기 간에 5초 이상 시간 차이가 나는 경우에만 동기화됩니다.

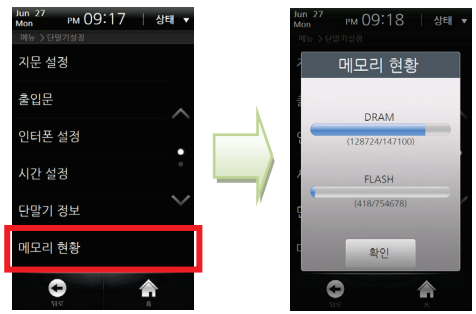
단말기 정보

모델명, 단말기ID, 하드웨어 버전, 펌웨어 버전, 커널 버전, MAC, 지문모듈 버전을 확인할 수 있습니다.
[메뉴] > [단말기설정] > [단말기 정보]를 선택합니다.



메모리 현황

현재 단말기 메모리 사용 현황을 확인할 수 있습니다.
[메뉴] > [단말기설정] > [메모리 현황]을 선택합니다.



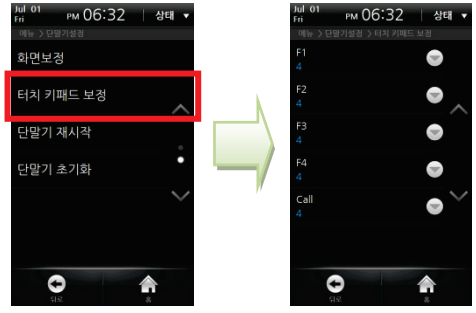
화면보정

[메뉴] > [단말기설정] > [화면보정]을 선택합니다.

1. 화면에 표시되는 십자표시를 누릅니다. 십자표시가 움직이면 따라서 터치합니다
2. 화면보정이 완료되면 십자표시가 사라집니다.

터치 키패드 보정

하단 터치 키의 감도를 조정합니다. 설정값이 작을수록 민감하게 작동하고, 설정값이 클수록 둔감하게 작동합니다.



1. [메뉴] > [단말기설정] > [터치 키패드 보정]을 선택합니다.
2. F1~F4, Call 키의 감도를 각각 설정합니다. (설정값 0~9)

참고 *특별한 문제가 없으면 기본 설정값을 사용할 것을 권장합니다. 공장출하시 기본값은 [4]입니다.*

단말기 재시작

BioStation T2 단말기를 재시동하는 메뉴입니다.

1. [메뉴] > [단말기설정] > [단말기 재시작]을 선택합니다.
2. [확인]을 누르면 단말기를 재시작 할 수 있습니다.

단말기 초기화

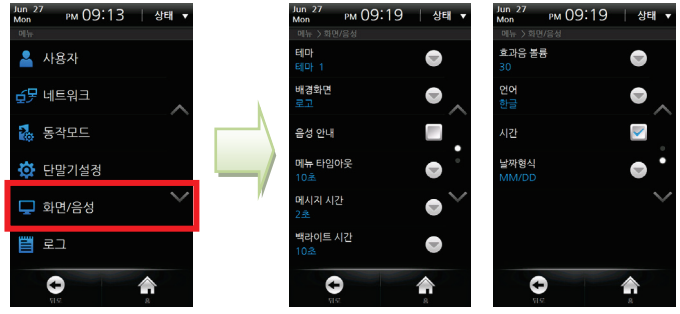
BioStation T2를 공장 출하시의 상태로 초기화 하는 메뉴입니다.

1. [메뉴] > [단말기설정] > [단말기 초기화]를 선택합니다.
2. [확인]을 누르면 단말기의 모든 설정값을 공창출하시의 초기값으로 복원합니다.

주의! 단말기 초기화를 수행하면 단말기의 각종 설정값과 BioStar 소프트웨어를 이용해 새롭게 다운로드한 배경화면, 효과음, 공지사항 등의 모든 정보가 삭제되므로 주의하십시오. 단말기 초기화를 수행하더라도 등록한 사용자 정보와 로그데이터는 삭제되지 않습니다.

화면/음성

[메뉴] > [화면/음성]을 선택합니다.



참고	*[공지사항] 및 [슬라이드쇼]가 설정된 경우, 인증 및 기타 동작 시에 로고화면이 표시되고 메뉴 타임아웃 시간이 경과한 후(무한대인 경우 30 초 후)에 공지사항 또는 슬라이드쇼, PDF 화면이 나타납니다. 공지사항 또는 슬라이드쇼 상태에서 터치시 LCD 백라이트가 꺼진 상태이면 LCD 백라이트가 들어오고, LCD 백라이트가 켜진 상태이면 로고화면으로 전환됩니다.*

1 **테마:** 배경화면에 사용할 테마를 선택한 후 [확인]을 누릅니다.(설정값: 테마1/테마2/테마3/테마4)

2 **배경화면:** 대기화면에 표시할 배경을 선택한 후 [확인]을 누릅니다.(설정값: 로고/공지사항/슬라이드쇼/PDF)

3 **음성 안내:** 음성 안내 사용 여부를 체크합니다.

4 **메뉴 타임아웃:** 설정한 시간 동안 키 입력이 없을 경우, 초기화면으로 이동합니다. (설정값:무한대/10초/20초/30초)

5 **메시지 시간:** 인증시 화면에 나타나는 메시지가 표시되는 시간을 설정합니다. (설정값: 0.5초/1초/2초/3초/4초/5초)

6 **백라이트 시간:** 설정한 시간 동안 키 입력이 없을 경우 LCD 조명이 꺼집니다. (설정값: 무한대/10초/20초/30초/40초/50초/60초)

7 **효과음 볼륨(0~100%):** 효과음의 크기를 설정합니다. 0%로 설정하면 효과음이 출력되지 않습니다.

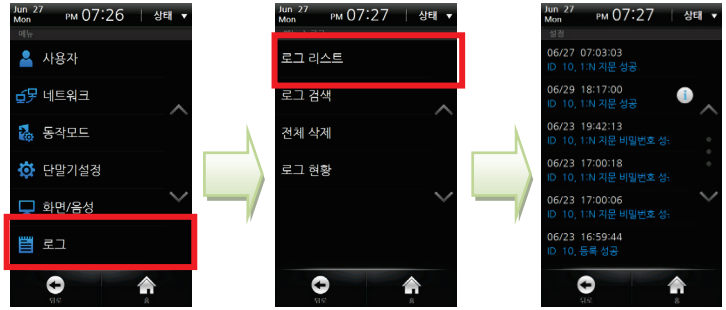
8 **언어:** 단말기에 표시될 언어를 설정합니다. 언어를 변경할 경우 단말기를 재시작해야 합니다.

9 **시간:** 대기 화면 중앙에 시간 표시 여부를 체크합니다.

10 **날짜형식(MM/DD,DD/MM):** 날짜 표시 형식을 설정한 후 [확인]을 누릅니다.

로그

로그 리스트

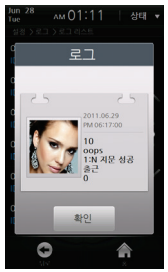


단말기에 저장된 일반 로그와 정지 영상 로그 기록을 확인할 수 있습니다.

1. [메뉴] > [로그] > [로그 리스트]를 선택합니다.
2. 저장된 로그의 목록이 나옵니다. 로그 항목을 누르면 상세 내역을 확인할 수 있습니다.
3. 정지영상로그는 로 표시되어 있습니다.



일반 로그



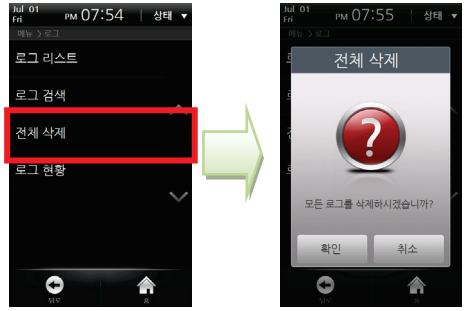
정지 영상 로그

로그 검색



1. [메뉴] > [로그] > [로그 검색]을 선택합니다.
2. 시작 날짜, 시작 시간, 종료 날짜, 종료 시간, 이벤트, 근태 이벤트, 사용자 ID 중 원하는 항목을 설정하여 아래의 [검색] 버튼을 누릅니다.
3. 로그 검색 결과가 나타납니다.

전체 삭제



1 [메뉴] > [로그] > [전체 삭제]를 선택합니다.
2 [확인]을 누르면 저장된 모든 로그가 삭제됩니다.
3 삭제가 완료되면 성공 확인 창이 나타납니다.

로그 현황



1 [메뉴] > [로그] > [로그 현황]을 선택합니다.
2 현재 단말기에 저장된 로그의 수와 남아있는 저장 가능 용량을 확인할 수 있습니다.

참고	*일반 로그는 최대 1,000,000 건까지 저장할 수 있습니다. 정지 영상 로그는 최대 5,000 건까지 저장할 수 있습니다.*

5 부록

제품규격

항목	규격	
카드옵션	125KHz EM, 13.56MHz ISO14443 A/B (MIFARE)	
용량	최대 사용자	200,000
	템플릿 용량	400,000(1:1), 20,000(1:N)
	로그 용량	일반 로그: 1,000,000 / 정지 영상 로그: 5,000
인터페이스	통신 인터페이스	Ethernet, WLAN, RS485 x 1ch, RS232/RS485(changeable) x 1ch, USB
	Wiegand	IN&OUT (Switchable)
	TTL I/O	4 inputs
	내장형 릴레이	2
	PoE	Yes
하드웨어	CPU	667Mhz RISC x 1, 533MHz DSP x 1
	메모리	1GB flash +256MB RAM
	LCD 표시부	5.0인치 WVGA 터치 스크린
	오디오	16 bit Hi-Fi voice & sound indication
	작동 온도	-20℃ ~ 50℃
	습도	90%
	Tamper	Switch
	입력 전압	12V DC
	제품 외형	155 mm(W) x 155 mm(H) x 40 mm(D)

전기규격

	최소값	평균값	최대값	비고
전원				
전압(V)	10.8	12	13.2	제공된 전원어댑터만 사용하여야 합니다.
소비 전류(mA)	-		570	
무선랜 동글을 연결했을 때 소비 전류 (mA)	-	-	1070	
스위치 입력				
VIH(V)	3.5	-	10.0	
VIL(V)	-	-	2.0	
풀업 저항	-	4.7K	-	입력포트는 4.7K 저항으로 Full Up 되어 있습니다.
Wiegand 출력				
VOH(V)	-	5	-	
VOL(V)	-	0.8	-	
풀업저항	-	4.7K	-	
릴레이				
스위칭 용량(A)	-	-	24 VDC	
스위칭 전압(V)	-	0.5 A	1.0 A	

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

Font 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).

"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.

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.



(주) 슈프리마

경기도 성남시 분당구 정자동 파크뷰 오피스타워 16층
TEL : 031-783-4510
FAX :031-783-4517

온라인고객지원 : support@suprema.co.kr
회사홈페이지 : www.suprema.co.kr

BioStation T2의 기능 및 사양은 제품의 품질 향상이나 기능 수정 등으로 인해 예고없이 변경될 수 있습니다.
제품에 대한 자세한 사항은 ㈜슈프리마로 문의 바랍니다.