BioStation 3

사용자 가이드

버전 1.13

한국어
KO 102.00.BS3

suprema
SECURITY & BIOMETRICS

목차

안전을 위한 주의 사항 4

준수 사항 4

시작하기 8

구성품 8

각 부분의 명칭 및 기능 9

케이블 및 커넥터 11

올바른 얼굴 등록 및 인증 방법 18

QR 코드 및 장치 라이선스에 대한 참고 사항 19

설치하기 20

브래킷 및 제품 고정 20

전원 연결 30

네트워크 연결 31

Input 연결 32

릴레이 연결 33

독립형 연결 35

Secure I/O 2 연결 37

Wiegand 연결 38

사용하기 39

관리자 메뉴 39

사용자 41

인증 45

설정 52

이벤트 로그 69

문제 해결 71

고장 신고 전 확인 사항 71

제품 사양 73

크리덴셜 73

일반 73

저장 용량 74

인터페이스 75

전기 규격 76

크기 및 무게 77

규제 인증 정보 79

규제 인증 및 라이선스 79

FCC 준수 정보 80

IC 정보 81

유럽 연합 적합성 선언 (CE) 81

부록 82

면책 조항 82

저작권 공지 83

오픈 소스 라이선스 83

안전을 위한 주의 사항

사용자의 위험이나 재산상의 손해를 막기 위해 제품을 사용하기 전에 이 설명서를 반드시 읽고 제품을 안전하고 올바르게 사용하세요.

이 설명서에서 말하는 제품이란 본체와 함께 제공되는 모든 구성품을 포함합니다.

준수 사항

경고
제품을 사용할 때 위반할 경우 심각한 상해나 사망에 이를 수 있는 경고 사항을 표기할 때 사용합니다.

주의
제품을 사용할 때 위반할 경우 경미한 상해나 제품 손상이 발생할 수 있는 주의 사항을 표기할 때 사용합니다.

알아두기
제품을 사용할 때 참고 사항이나 추가 정보를 제공할 때 사용합니다.

노트

제품을 사용할 때 참고 사항이나 추가 정보를 제공할 때 사용합니다.

⚠ 경고

설치

고용량의 전원 공급 장치 사용 시 오배선에 각별히 주의하세요.

- 오배선 시 심각한 화재, 감전, 제품 손상이 발생할 수 있습니다.

사용자가 임의로 제품을 설치하거나 수리하지 마세요.

- 화재, 감전, 부상의 원인이 됩니다.
- 사용자의 임의 설치나 수리로 인해 제품이 손상된 경우 무상 수리 서비스가 제공되지 않습니다.

제품을 직사광선에 노출된 장소, 습기, 먼지나 그을음이 많은 장소, 가스가 샐 가능성이 있는 장소에 설치하지 마세요.

- 화재 또는 감전의 원인이 됩니다.

제품을 옥외에 설치할 경우 차양 및 통풍이 원활한 장소에 설치하세요.

제품을 옥외에 설치할 경우 완전히 밀폐된 외함을 사용하지 마세요.

- 직사광선에 의해 외함 내부 온도가 상승하여 과열로 인한 화재, 감전, 제품 손상의 원인이 됩니다.

제품을 전열기 등으로 인해 열이 발생하는 장소에 설치하지 마세요.

- 과열로 인한 화재 또는 감전의 원인이 됩니다.

물기가 있는 곳에 설치하지 마세요.

- 습기로 인한 감전 또는 제품 손상의 원인이 됩니다.

전자파 장해가 있는 곳에 설치하지 마세요.

- 감전 또는 제품 손상의 원인이 됩니다.

사용

제품 내부에 물, 음료수, 약품 등의 액체가 들어가지 않도록 주의하세요.

- 화재, 감전, 제품 손상의 원인이 됩니다.

손상된 전원 어댑터나 플러그, 헐거운 콘센트는 사용하지 마세요.

- 접속이 불안정할 경우 화재 또는 감전의 원인이 됩니다.

전원 코드를 무리하게 구부리거나 망가뜨리지 마세요.

- 화재 또는 감전의 원인이 됩니다.

⚠ 주의

설치

제품을 설치하기 전에 이 설명서를 반드시 읽고 제품을 안전하고 올바르게 설치하세요.

전원 케이블과 케이블을 배선할 때에는 반드시 연결하려는 모든 장치의 전원을 끈 상태에서 배선 및 연결하세요.

- 장치가 오작동할 수 있습니다.

제품에 전원을 연결하기 전에 다시 한번 설명서를 확인하여 배선이 올바르게 되었는지 확인한 후 전원을 연결하세요.

제품을 직사광선이나 자외선에 직접 노출된 장소에 설치하지 마세요.

- 제품 손상, 오작동 및 변색, 변형의 원인이 됩니다.

전원 케이블 등을 통행 장소에 방치하지 마세요.

- 신체 상해 또는 제품 손상의 원인이 됩니다.

자석, TV, (CRT) 모니터, 스피커 등 자성이 강한 물체 주변에 설치하지 마세요.

- 고장의 원인이 됩니다.

여러 대의 장치를 설치할 경우 최소 이격 거리를 확인하세요.

- 다른 장치의 RF 및 BLE 성능에 영향을 주어 장치가 오작동할 수 있습니다.

전원 어댑터는 IEC/EN 62368-1 승인을 받은 제품으로 단말기의 소모 전력 이상의 제품을 사용하세요. 슈프리마에서 판매하는 전원 어댑터를 사용할 것을 권장합니다.

- 적합한 전원을 사용하지 않을 경우 장치가 오작동할 수 있습니다.
- 최대 소모전류 규격은 제품 사양의 전원을 참고하세요.

제품과 Secure I/O 2, 전기정(전기식 잠금 장치)은 반드시 개별 전원을 사용하세요.

- 장치가 오작동할 수 있습니다.

전원 장치와 PoE+ 전원을 함께 연결하지 마세요.

- 장치가 오작동할 수 있습니다.

IP65 등급을 만족하기 위해 제품과 케이블을 연결한 뒤 반드시 케이블 커버를 사용해야 합니다. 완전히 노출된 옥외에 설치할 경우 외함을 사용할 것을 권장합니다.

- 방수·방진 성능이 저하될 경우 고장의 원인이 됩니다.

PoE+ 전원 연결 시에는 반드시 PoE+ 또는 PoE++ 규격으로 연결하세요.

- 표준 PoE를 사용할 경우 장치가 불안정하게 동작하거나 영구적으로 손상될 수 있습니다.

사용

제품을 떨어뜨리거나 충격을 주지 마세요.

- 고장의 원인이 됩니다.

제품의 펌웨어 업그레이드 진행 중 전원 공급이 중단되지 않도록 주의하세요.

- 고장의 원인이 됩니다.

비밀번호를 타인이 알지 못하도록 관리하고, 주기적으로 변경하세요.

- 불법 침입의 원인이 됩니다.

제품의 버튼(터치패드)을 무리하게 누르거나 날카로운 도구를 사용해 누르지 마세요.

- 고장의 원인이 됩니다.

제품을 -20 °C ~ 50 °C 이내에서 사용하고 너무 낮거나 높은 온도에서 보관하지 마세요.

- 고장의 원인이 됩니다.

제품을 청소할 때 주의하세요.

- 제품을 표면을 깨끗한 마른 천으로 부드럽게 닦으세요.
- 제품을 소독해야 할 경우 마른 천에 소독용 알코올을 적당량 묻힌 뒤 제품 표면을 부드럽게 닦으세요. 이소프로필 알코올이 70 ~ 75 % 함유된 소독용 알코올과 깨끗하고 보풀이 없는 부드러운 천을 사용하세요.
- 소독제를 제품에 직접 분사하지 마세요.

제품을 원래 용도 이외 다른 용도로 사용하지 마세요.

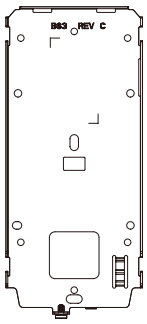
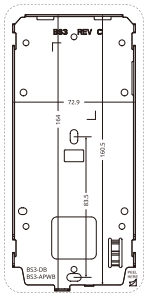
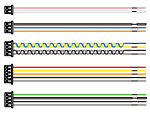
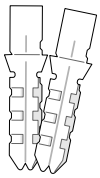
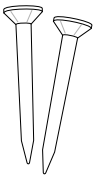
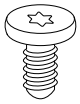
- 고장의 원인이 됩니다.

> **RTC 배터리**
>
> 승인되지 않거나 잘못된 종류의 배터리로 교체하면 폭발의 위험이 있습니다. 배터리는 거주 지역 또는 국제 폐기물 규정에 따라 폐기하세요.

시작하기

장치 사용을 위한 초기 절차를 안내합니다.

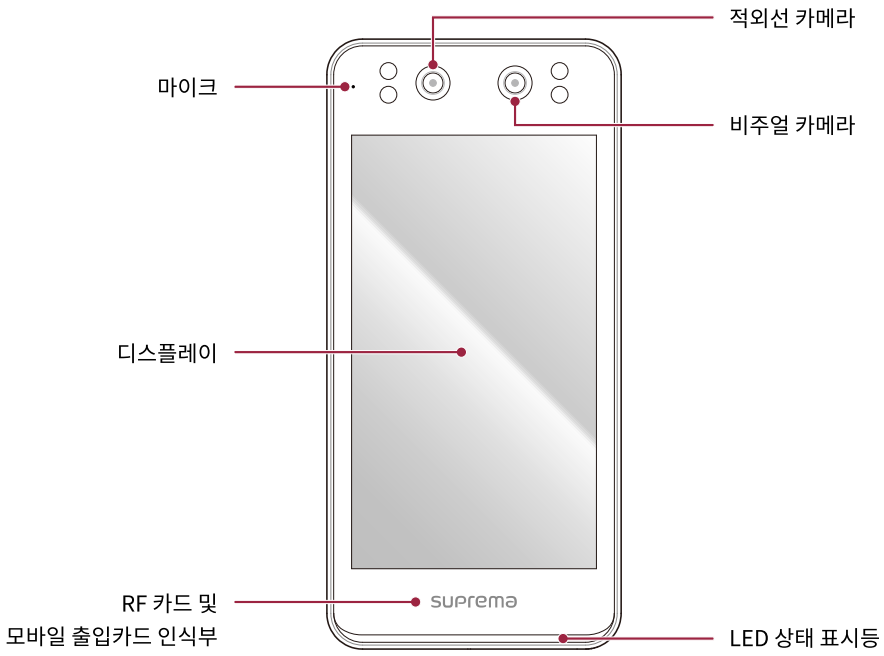
구성품

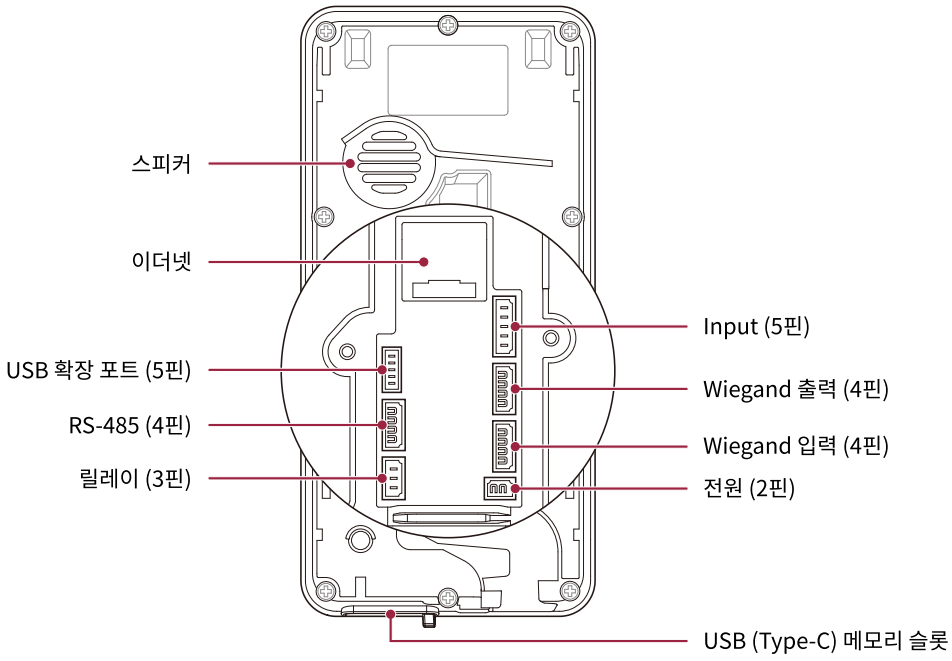
				
BioStation 3	벽걸이용 브래킷	드릴링 템플릿	퀵 가이드	연결 케이블
				
다이오드	120 Ω 저항	PVC 앵커 x2	고정용 나사 x2	브래킷 고정용 나사(별 모양)

알아두기

- 구성품은 설치 환경에 따라 달라질 수 있습니다.
- 브래킷과 제품을 조립할 때 향상된 보안을 위해 제품 고정용 나사 대신 동봉된 브래킷 고정용 나사(별 모양)를 이용할 수 있습니다.

각 부분의 명칭 및 기능





- **마이크**: 인터폰 연결 시 사용자의 음성을 전달합니다.
  - 마이크를 가리거나 막으면 음성 전달이 원활하지 않을 수 있습니다.
- **적외선 카메라**: 적외선 이미지를 촬영합니다.
- **비주얼 카메라**: 실제 이미지를 촬영합니다.
- **디스플레이**: 동작을 위한 UI를 제공합니다.
- **RF 카드 및 모바일 출입카드 인식부**: 출입을 위해 RF 카드 또는 모바일 출입카드를 인식시키는 부분입니다.

- **LED 상태 표시등**: 제품의 작동 상태가 표시됩니다.
  - 초록색: 인증 성공
  - 빨간색: 인증 실패
  - 파란색: 정상 동작 상태
  - 파란색/초록색 점멸:
    - **DHCP**를 사용으로 설정 시 IP 주소를 받아오지 못하는 상태
    - **슬레이브** 모드일 때 마스터 장치와 연결이 끊어진 상태
  - 빨간색/보라색 점멸: 장치 잠금 상태
  - 노란색 점멸: 입력 대기 상태
- **스피커**: 소리를 들을 수 있습니다.
- **이더넷**: 이더넷 케이블을 연결합니다.
- **Input (5핀)**: Input 케이블을 연결합니다.
- **USB 확장 포트 (5핀)**: 기타 액세서리 제품을 연결할 수 있습니다.
- **Wiegand 출력 (4핀)**: Wiegand 출력 케이블을 연결합니다.
- **Wiegand 입력 (4핀)**: Wiegand 입력 케이블을 연결합니다.
- **RS-485 (4핀)**: RS-485 케이블을 연결합니다.
- **릴레이 (3핀)**: 릴레이 케이블을 연결합니다.
- **전원 (2핀)**: 전원 케이블을 연결합니다.
- **USB (Type-C) 메모리 슬롯**: USB 메모리를 연결합니다.

케이블 및 커넥터

전원



핀	명칭	색상
1	PWR +VDC	빨간색(흰띠)
2	PWR GND	검은색(흰띠)

릴레이



핀	명칭	색상
1	RLY NO	흰색
2	RLY COM	파란색
3	RLY NC	주황색

RS-485



핀	명칭	색상
1	485 TRXP	파란색
2	485 TRXN	노란색
3	485 GND	검은색
4	SH GND	회색

Input



핀	명칭	색상
1	INPUT0	빨간색
2	INPUT1	노란색
3	INPUT2	주황색
4	INPUT GND	검은색
5	SH GND	회색

Wiegand 입력



핀	명칭	색상
1	WG D0	초록색
2	WG D1	흰색
3	WG GND	검은색
4	SH GND	회색

Wiegand 출력



핀	명칭	색상
1	WG D0	초록색
2	WG D1	흰색
3	WG GND	검은색
4	SH GND	회색

마스터 관리자 설정하기 CE향 제품

마스터 관리자 기능은 장치의 전체 관리자 권한을 강화하여, 장치의 보안을 향상시키고 무단 접근 및 설정 변경을 방지하기 위한 기능입니다. 이 기능은 EU 지역용 **CE향 제품**에만 적용되며, **CE향 제품**에는 **반드시 마스터 관리자를 등록**해야 합니다. 등록된 마스터 관리자만 관리자 메뉴에 진입하여 장치 설정을 변경할 수 있습니다.

알아두기

- 이 기능은 EU 지역용 **CE향 제품**의 보안성을 강화하기 위해 도입된 필수 정책이며, **글로벌향 (Non-CE)** 장치에서는 지원되지 않습니다.
- 마스터 관리자는 직접 삭제할 수 없으며 **공장 초기화** 시에만 삭제됩니다.

마스터 관리자 지원 정책 CE향 vs 글로벌향 (Non-CE)

마스터 관리자 기능은 **CE 마크가 있는 라벨이 부착된 CE향 제품에서만 활성화**됩니다.

제품 뒷면 라벨 스티커를 통해 **CE향** / **글로벌향 (Non-CE)** 제품을 식별할 수 있으며, 이에 따라 기능이 다음과 같이 구분되어 동작합니다.

- **CE향**: CE 마크 있음
- **글로벌향 (Non-CE)**: CE 마크 없음

구분	CE향 제품	글로벌향 (Non-CE) 제품
마스터 관리자	활성화 (비활성화 불가)	미지원
관리자 2단계 인증	필수	미지원
최소 PIN 길이	최소 8자리 이상	최소 4자리 이상

BioStar X(또는 BioStar 2)와 연결 시, 장치의 지원 여부에 따라 마스터 관리자 설정 표시가 달라지며 관리자 2단계 인증 메뉴의 활성화 여부도 자동으로 동기화됩니다.

펌웨어 업그레이드 시 동작 로직

기존에 사용 중인 제품의 펌웨어를 업그레이드할 경우, **업그레이드 이전 버전**과 **업그레이드 대상 버전**의 조합에 따라 **마스터 관리자** 및 **관리자 2단계 인증** 지원 여부가 달라질 수 있습니다.

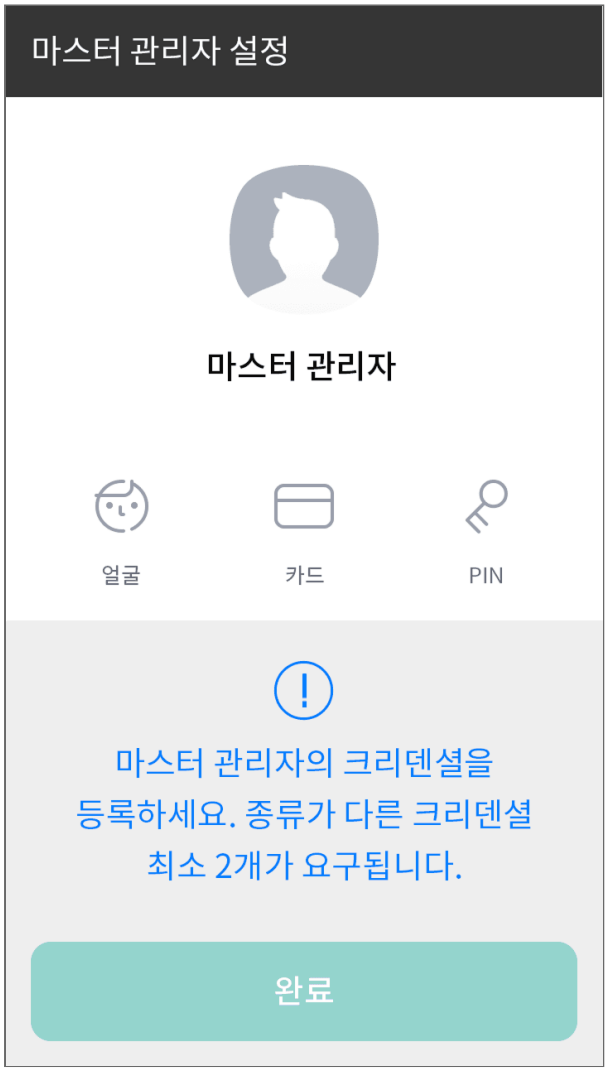
자세한 버전별 지원 여부는 슈프리마 기술 지원팀(CS@suprema.co.kr)에 문의하세요.

새 장치에서 마스터 관리자 등록하기

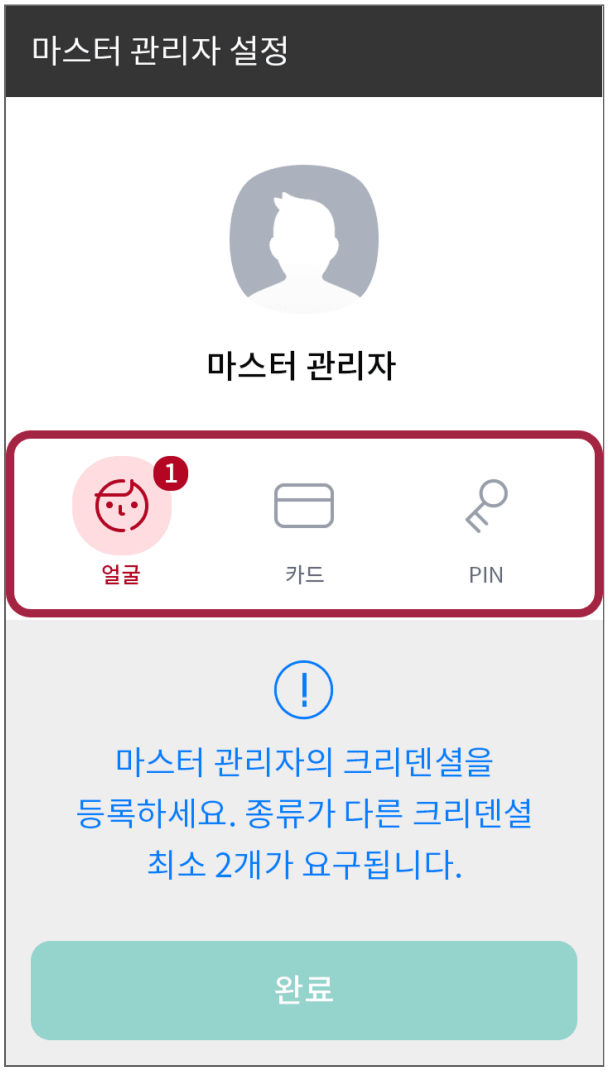
CE향 새 장치에서는 처음부터 **마스터 관리자**를 필수적으로 등록해야 하며, 등록하지 않을 경우 장치 사용이 제한됩니다.

> **알아두기**
>
> - 최초 부팅 시 **마스터 관리자** 등록 화면이 나타나며, 등록을 완료하지 않으면 다음 화면으로 이동할 수 없습니다.
> - BioStar X(또는 BioStar 2)와 연결하여 장치 전체 관리자를 할당하더라도 **마스터 관리자**를 장치에서 직접 등록해야만 모든 기능을 사용할 수 있습니다.
> - 새 장치는 펌웨어 다운그레이드를 할 수 없습니다.

1. 새 장치를 최초 부팅하면 **마스터 관리자** 등록 화면이 나타납니다.



2. EU 지역 보안 정책에 따라 **마스터 관리자**는 **최소 두 종류 이상**의 크리덴셜을 등록해야 합니다. 원하는 크리덴셜 두 종류를 선택하여 등록하세요.

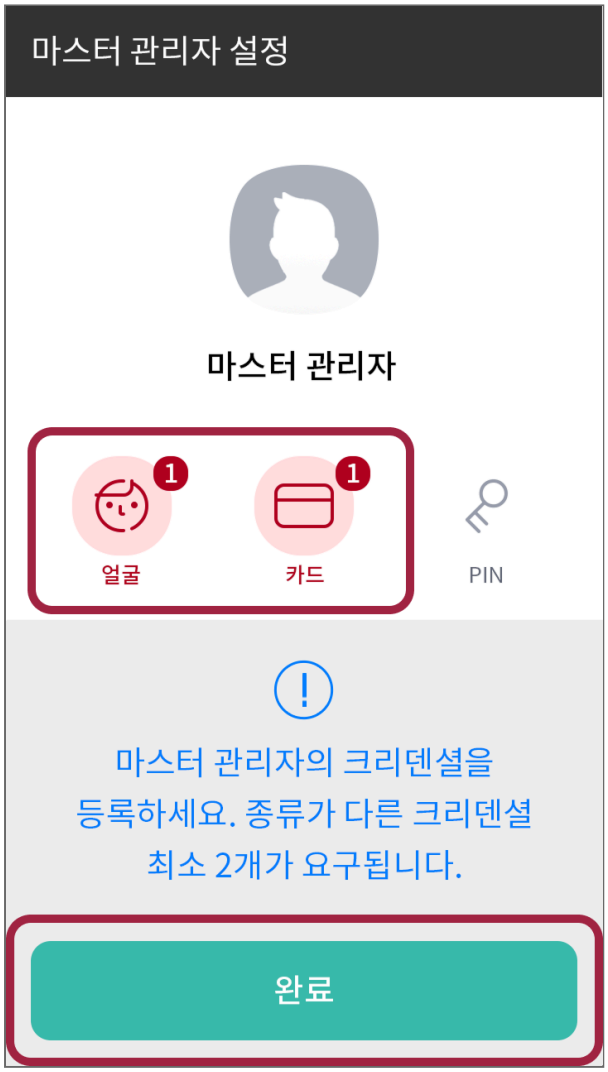


마스터 관리자에 등록할 수 있는 크리덴셜은 다음과 같습니다.

크리덴셜 종류	등록 가능 개수	세부 조건
카드	최대 4개	CSN, Wiegand 타입만 지원 동일 타입 내 중복 등록 불가
얼굴	최대 2개	동종 알고리즘 탑재 장치에서만 등록 가능
지문	최대 2개	-
PIN	1개	최소 8자리 이상 (CE 규제 적용)

등록 조건
- 최소 두 종류 이상의 크리덴셜을 등록해야 합니다.
- 장치가 지원하는 모든 크리덴셜을 인증 수단으로 사용할 수 있습니다.

3. 두 종류 이상의 크리덴셜을 등록한 후, **완료** 버튼을 누르면 **마스터 관리자** 등록이 완료됩니다.



안내 사항

- **BioStar 소프트웨어를 통한 PIN 등록 시**

  마스터 관리자를 지원하지 않는 글로벌향 (Non-CE) 제품은 4자리 이상의 PIN을 장치에서 직접 등록할 수 있습니다. 단, BioStar X(또는 BioStar 2)를 통해 사용자를 등록하는 경우 아래 버전에서는 최소 8자리 PIN이 필요합니다.

  – BioStar 2 v2.9.11 이상

  – BioStar X v1.0.0 ~ v1.0.2

  위 버전에서 4자리 PIN으로 등록된 사용자는 장치 관리자로 지정할 수 없습니다.

- **장치 해시키 수동 변경 시**

  장치 해시키를 수동으로 변경할 경우 마스터 관리자의 PIN이 삭제된다는 경고 메시지가 표시되므로 메시지를 확인한 후 변경하세요.

- **RS-485 통신구간 얼굴 이미지 전송 제한**

  RS-485 통신구간에서는 바이오메트릭 크리덴셜 이미지가 전송되지 않으므로, 슬레이브 장치에서 등록된 마스터 관리자 얼굴 조회 시 대체 이미지를 표시합니다.

올바른 얼굴 등록 및 인증 방법

얼굴 등록 시 주의 사항

- 얼굴을 등록할 때 장치와 얼굴의 거리를 60~100 cm로 유지하세요.
- 표정이 변하지 않도록 주의하세요.
- 마스크, 모자, 안대를 착용하지 마세요.
- 마스크를 착용한 얼굴을 등록하지 마세요. 마스크를 착용한 얼굴과 착용하지 않은 얼굴을 모두 등록할 경우 오인식률이 높아질 수 있습니다.
- 고개를 들거나 숙이지 마세요.
- 진한 화장을 하지 마세요.
- 눈을 감지 마세요.
- 화면에 양쪽 어깨가 모두 나타나도록 하세요.
- 움직이지 말고, 정면으로 서서 얼굴을 등록하세요.
- 두 명의 얼굴이 화면에 동시에 나타나지 않도록 주의하세요. 한 번에 한 사람씩 등록하세요.
- 화면의 지시에 따르지 않을 경우 얼굴 등록이 오래 걸리거나 실패할 수 있습니다.

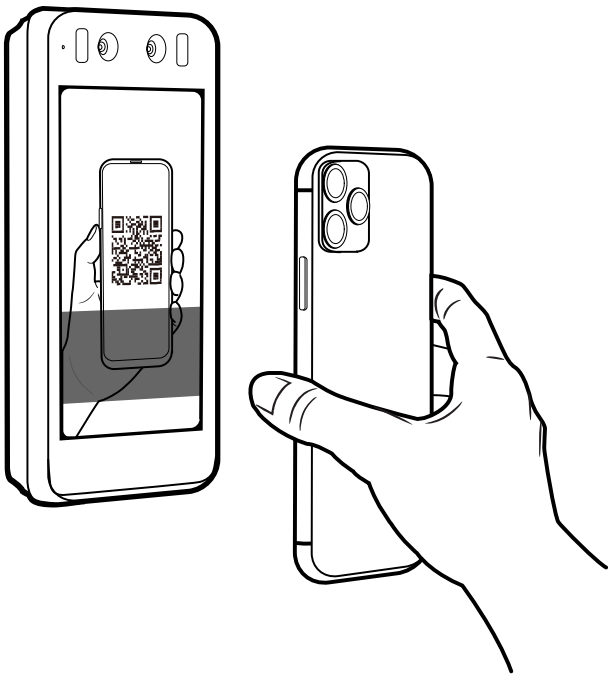
얼굴 인증 시 주의 사항

- 장치의 화면 중앙에 얼굴이 나타나도록 하세요. 위치 가이드가 표시될 경우 화면의 안내에 따라 얼굴을 인증하세요.
- 모자, 마스크, 선글라스, 안대 등으로 얼굴의 일부를 가릴 경우 인증에 실패할 수 있습니다. 눈썹과 얼굴을 모두 장치가 인식할 수 있도록 얼굴을 가리지 마세요.
- 장치와의 거리가 60~100 cm 떨어진 위치에서 인증하세요.
- 장치의 화면에 양쪽 어깨가 모두 나타나도록 하세요. 좌우 어깨의 대칭이 맞지 않을 경우 인증에 실패할 수 있습니다. 움직이지 말고, 정면으로 서서 얼굴을 인증하세요.

QR 코드 및 장치 라이선스에 대한 참고 사항

올바른 QR 코드 인증 방법

사용자에게 QR 코드를 발급하여 인증 수단으로 사용할 수 있습니다. 인식률을 높이기 위해 화면의 안내에 따라 올바르게 QR 코드를 스캔하세요.



- 장치의 카메라와 QR 코드 사이의 거리를 30~40 cm로 유지하세요.
- QR 코드를 장치의 스캔 화면 중앙에 오도록 위치시키세요.
- 모바일 장치에 내려받은 QR 코드로 인증할 경우 화면이 잘 보이도록 모바일 장치의 밝기를 조정하세요.

장치 라이선스 참고 사항

- QR 인증을 사용하려면 별도의 장치 라이선스가 필요합니다. 장치 라이선스를 발급하려면 구입처에 문의하세요.
- 장치 라이선스 파일은 암호화된 파일이므로 임의로 수정할 수 없습니다.
- 장치 라이선스는 장치 ID를 기준으로 발급됩니다. 비정상적인 방법으로 장치 ID를 변경할 경우 라이선스에 대한 보증 서비스가 제공되지 않습니다.

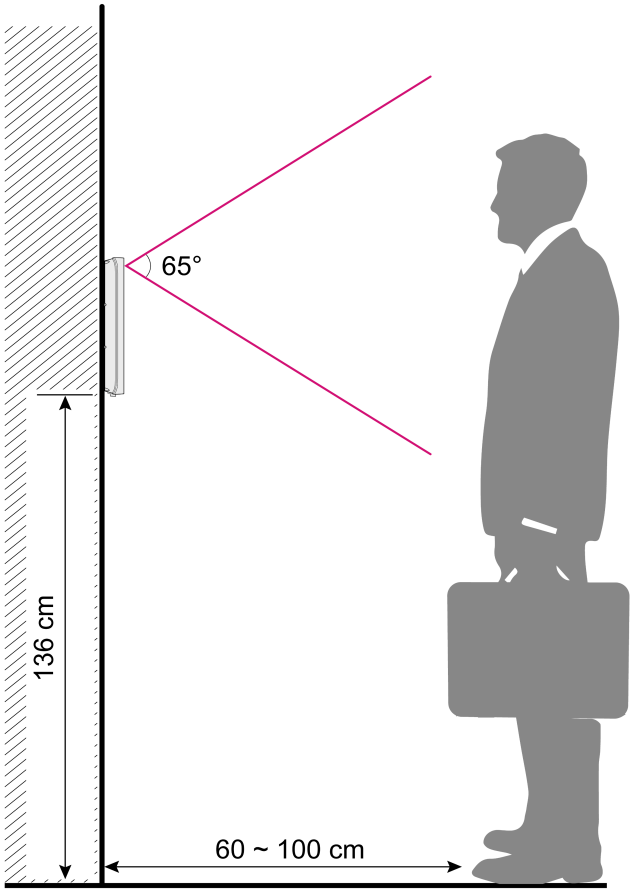
설치하기

설치에 필요한 전체 과정과 연결 예시를 제공합니다.

브래킷 및 제품 고정

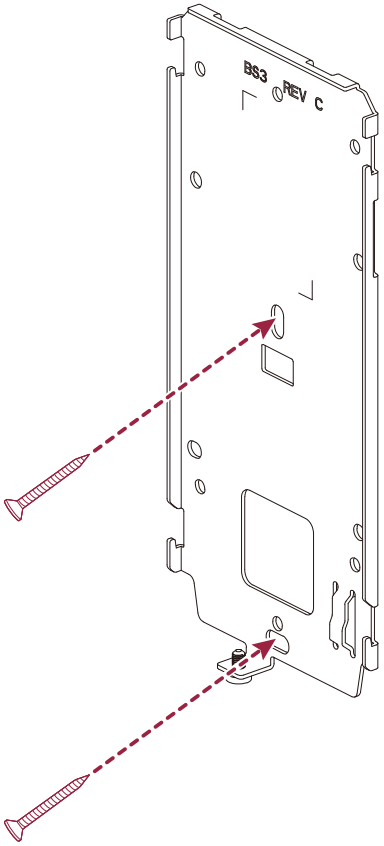
일반 브래킷

1. 제공된 드릴링 템플릿을 이용하여 제품을 장착할 위치를 정하세요.



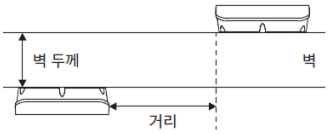
> **알아두기**
>
> - 장치를 설치할 최적의 높이는 136 cm입니다.
> - 장치를 직사 광선이나 자외선에 직접 노출된 장소에 설치하지 마세요.
> - 사용자가 얼굴을 인증할 때 얼굴에 직사광선이 닿지 않도록 설치 위치를 조정하세요.

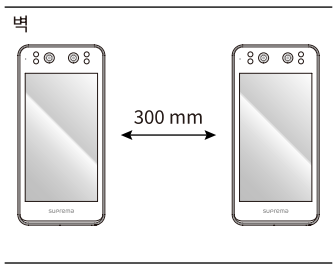
2. 제품을 장착할 위치에 고정용 나사를 이용하여 브래킷을 단단히 고정하세요.



알아두기

- 제품을 콘크리트 벽에 설치할 경우 드릴로 구멍을 뚫어 PVC 앵커를 끼운 뒤 고정용 나사로 고정하세요.
- RF 신호 간섭을 피하기 위해 최소 이격 거리를 확인하여 설치하세요.

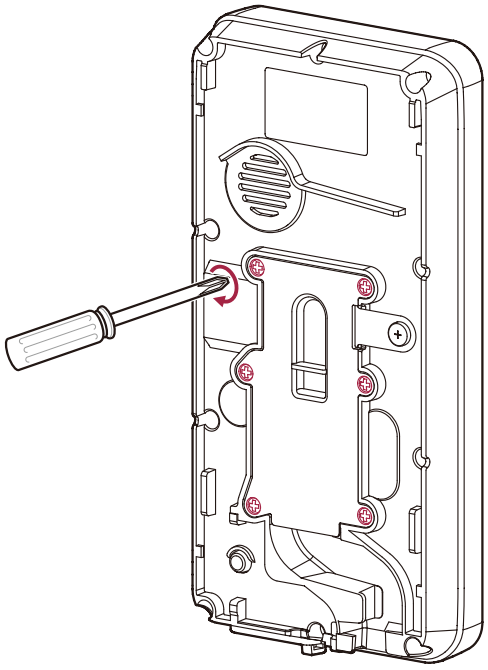




벽 두께	거리
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

- 모바일 출입카드를 사용할 경우 BLE 신호 간섭을 피하기 위해 장치 사이에 최소 1 m 이상의 거리를 두고 설치하세요.

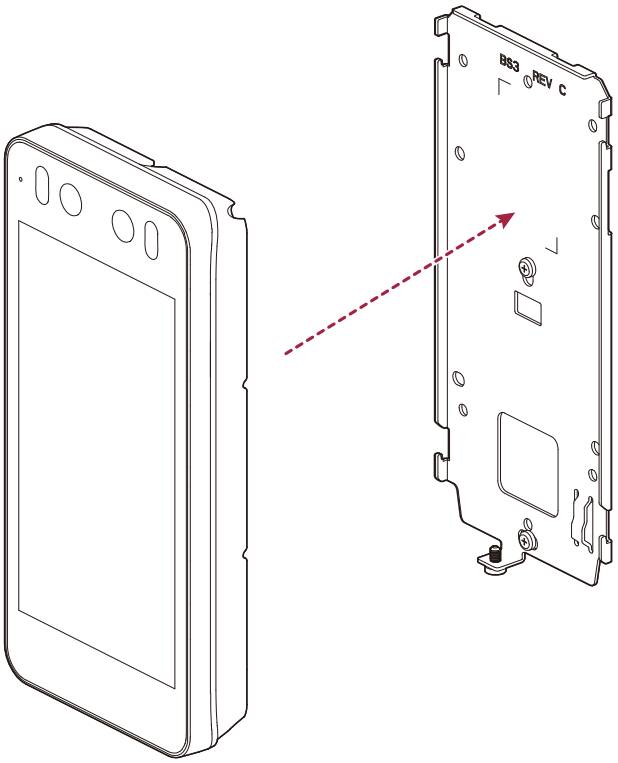
3. 케이블 커버를 장착한 뒤 커버의 나사 6개를 돌려 단단히 고정하세요.



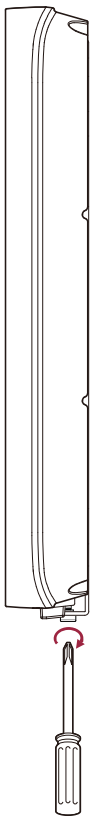
알아두기

IP65 등급을 만족하기 위해 제품과 케이블을 연결한 뒤 반드시 케이블 커버를 사용해야 합니다.

4. 고정된 브래킷 위에 제품을 장착하세요.



5. 제품 고정용 나사를 돌려 제품과 브래킷을 조립하세요.



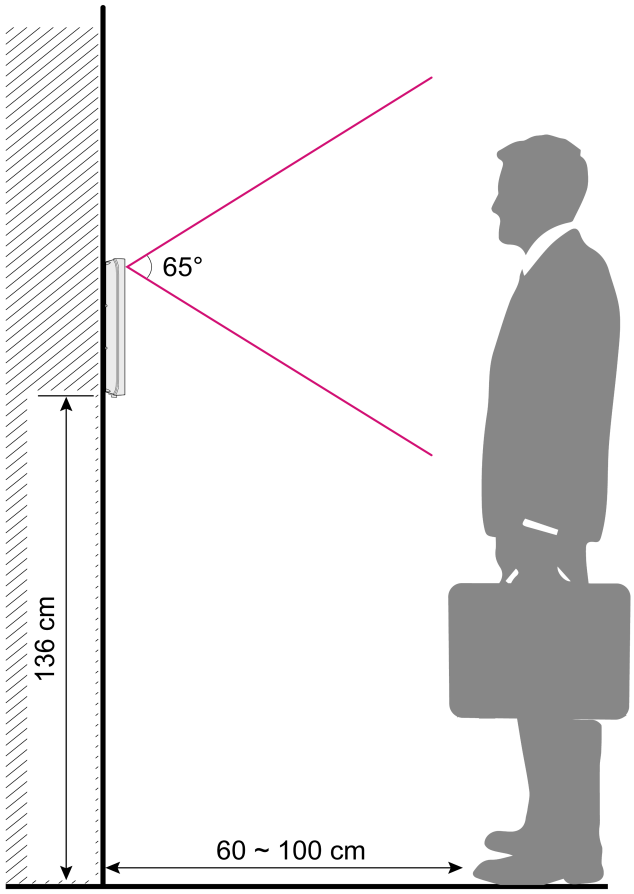
알아두기

브래킷과 제품을 조립할 때 향상된 보안을 위해 제품 고정용 나사 대신 동봉된 브래킷 고정용 나사(별 모양)를 이용할 수 있습니다.

틸팅 브래킷

전용 틸팅 브래킷을 통해 설치 환경에 맞춰 인증 각도를 조절할 수 있습니다. 틸팅 브래킷은 별매품입니다.

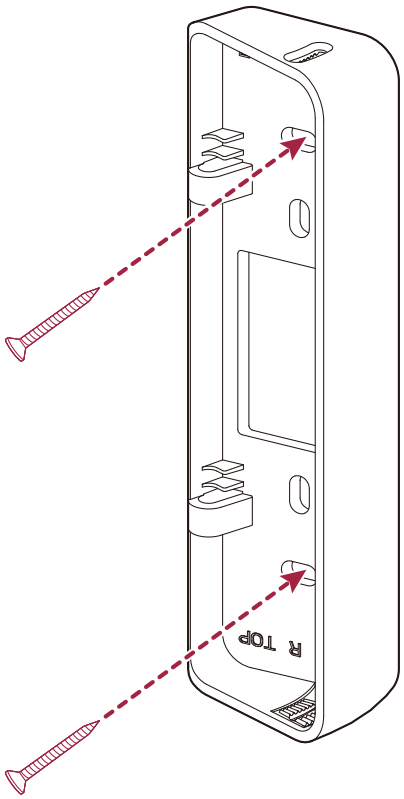
1. 제공된 드릴링 템플릿을 이용하여 제품을 장착할 위치를 정하세요.



알아두기

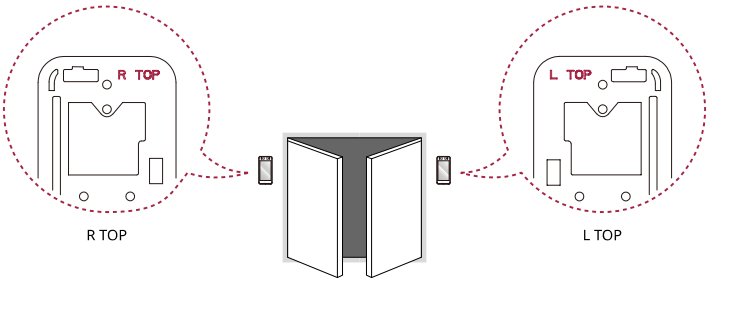
- 장치를 설치할 최적의 높이는 136 cm입니다.
- 장치를 직사 광선이나 자외선에 직접 노출된 장소에 설치하지 마세요.
- 사용자가 얼굴을 인증할 때 얼굴에 직사광선이 닿지 않도록 설치 위치를 조정하세요.

2. 틸팅 브래킷 고정용 나사를 사용하여 장착할 위치(벽면)에 틸팅 브래킷 후면부를 단단히 고정하세요.



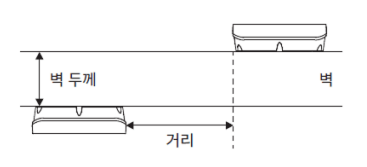
설치 위치에 따라 틸팅 브래킷의 상/하 방향을 다음과 같이 구분하여 설치하세요.

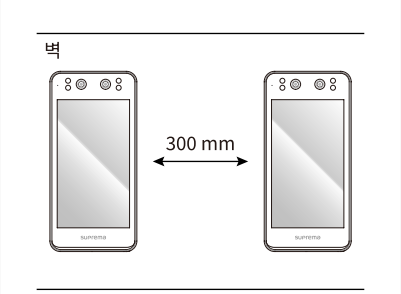
- 출입문 왼쪽에 설치하는 경우: "R TOP" 각인이 상단을 향하도록 설치
- 출입문 오른쪽에 설치하는 경우: "L TOP" 각인이 상단을 향하도록 설치



알아두기

- 제품을 콘크리트 벽에 설치할 경우 드릴로 구멍을 뚫어 PVC 앵커를 끼운 뒤 고정용 나사로 고정하세요.
- RF 신호 간섭을 피하기 위해 최소 이격 거리를 확인하여 설치하세요.

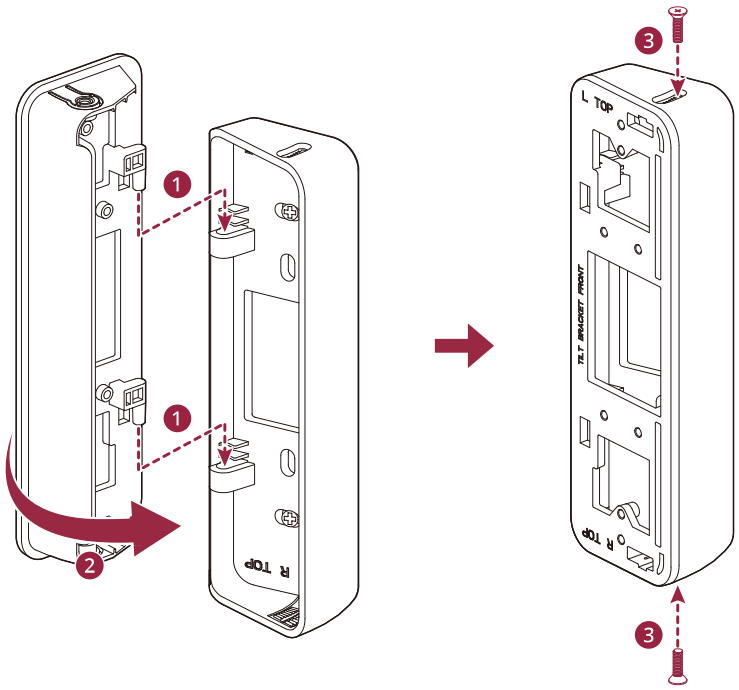




벽 두께	거리
100 mm	200 mm
120 mm	180 mm
150 mm	150 mm

- 모바일 출입카드를 사용할 경우 BLE 신호 간섭을 피하기 위해 장치 사이에 최소 1 m 이상의 거리를 두고 설치하세요.

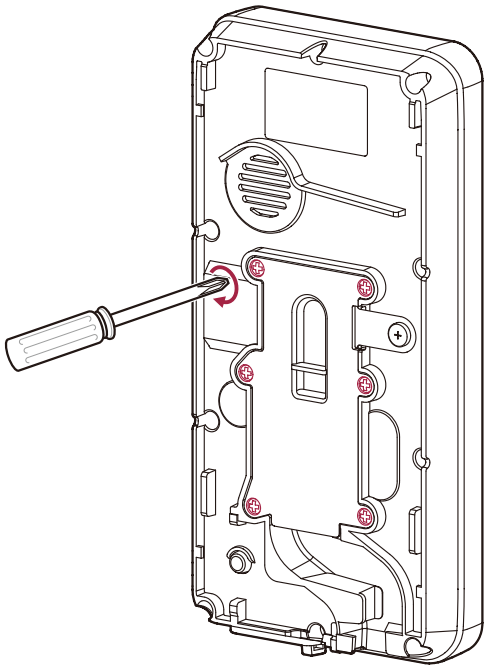
3. 틸팅 브래킷 전면부를 후면부 홈에 결합하여 닫은 후, 상/하단의 나사 홀에 나사 2개를 사용하여 고정하세요.



알아두기

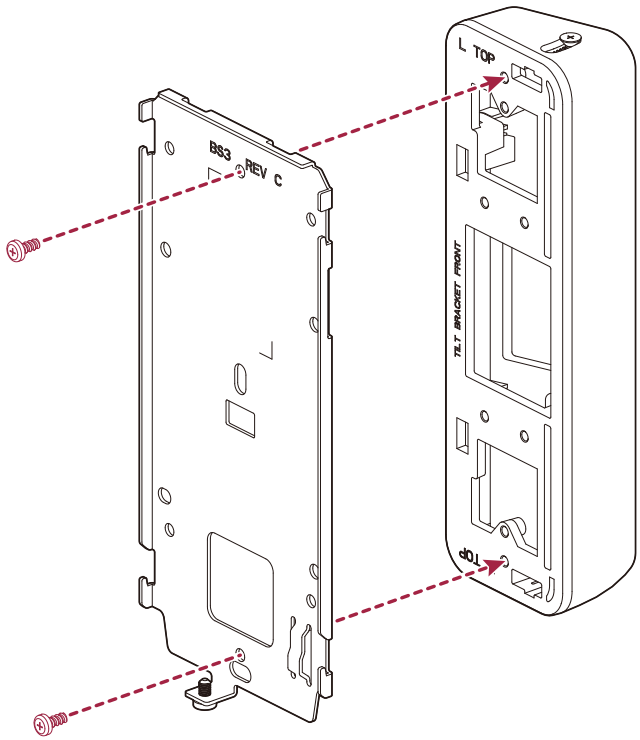
나사를 지나치게 조이면 각도를 조절할 수 없습니다. 적절한 세기로 나사를 조이세요.

4. 케이블 커버를 장착한 뒤 커버의 나사 6개를 돌려 단단히 고정하세요.

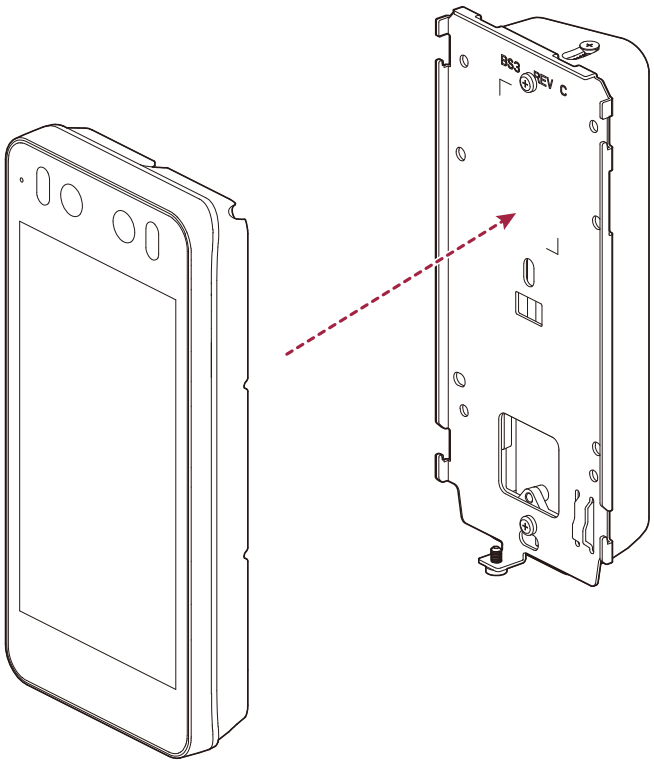


> **알아두기**
> IP65 등급을 만족하기 위해 제품과 케이블을 연결한 뒤 반드시 케이블 커버를 사용해야 합니다.

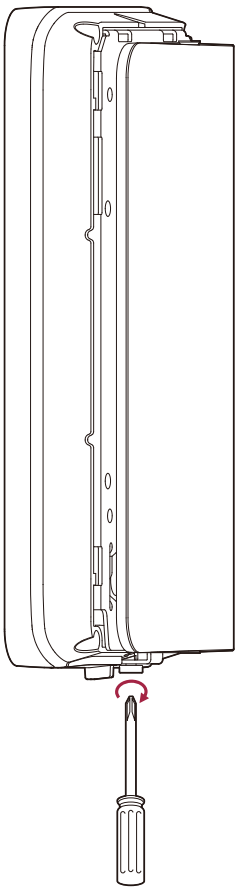
5. 틸팅 브래킷 위에 벽걸이용 브래킷을 단단히 고정하세요.



6. 고정된 벽걸이용 브래킷 위에 제품을 장착하세요.



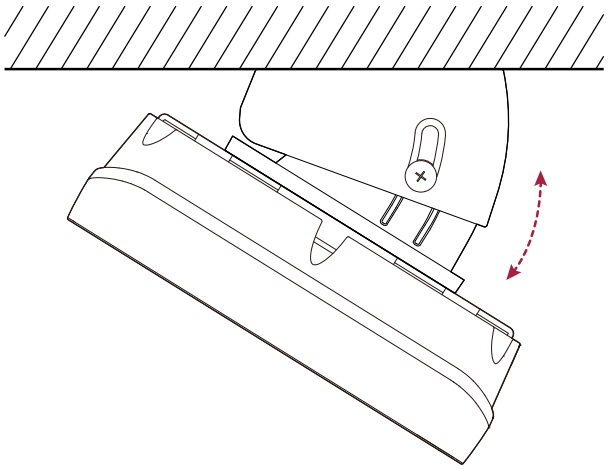
7. 제품 고정용 나사를 돌려 제품과 벽걸이용 브래킷을 조립하세요.



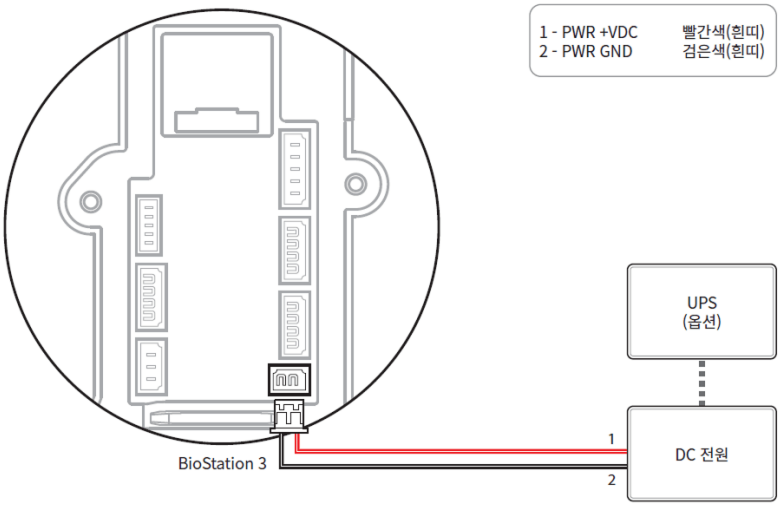
알아두기

브래킷과 제품을 조립할 때 향상된 보안을 위해 제품 고정용 나사 대신 동봉된 브래킷 고정용 나사(별 모양)를 이용할 수 있습니다.

8. 틸팅 브래킷을 원하는 각도로 조정하세요.



전원 연결



주의

- 전원 장치(또는 어댑터)와 PoE 전원 장치를 함께 연결하지 마세요.
- 전원 어댑터는 IEC/EN 62368-1 승인을 받은 제품으로 단말기의 소모 전력 이상의 제품을 사용하세요. 전원 어댑터에 다른 기기를 연결하여 사용하려면 단말기의 소모 전력과 다른 기기에 필요한 소모 전력을 합한 전류 용량 이상의 어댑터를 사용해야 합니다.
  - 최대 소모전류 규격은 제품 사양의 전원을 참고하세요.
- Secure I/O 2, 전기정(전기식 잠금장치), 제품은 반드시 개별 전원을 사용하세요. 전원을 함께 연결하여 사용하면 장치가 오작동할 수 있습니다.
- 전원 연결 시 제품과 전원 장치 간의 거리에 주의하세요. 제품과 전원 장치는 최대한 가깝게 설치해야 합니다. 올바르게 연결하지 않을 경우 제품이 오작동할 수 있으므로 주의하세요. 제품과 전원 장치의 거리가 먼 경우 16 AWG 또는 18 AWG 케이블을 사용할 것을 권장합니다. 사용하는 케이블의 규격과 설치 환경에 따라 연결할 수 있는 거리가 다를 수 있습니다. 이 제품은 DC 24V와 DC 12V 전원을 모두 지원하므로, 각 케이블 규격에 따른 최대 연장 길이를 확인하여 전원을 올바르게 연결하세요.

케이블 규격	최대 연장 길이	
	DC 12V	DC 24V
16 AWG	50 m	150 m
18 AWG	30 m	136 m
20 AWG	20 m	90 m

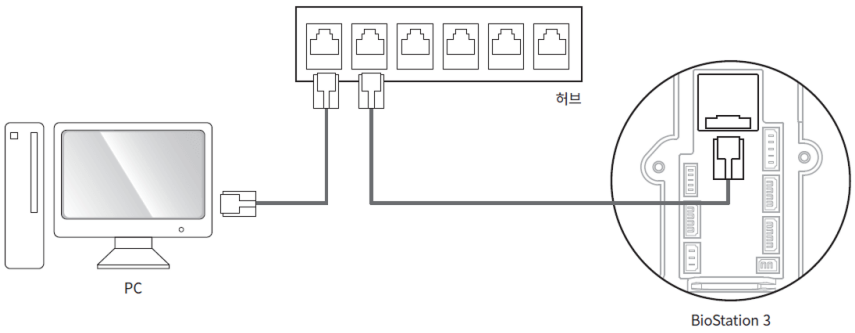
- 전원 어댑터를 사용할 경우 전원 케이블의 길이를 임의로 연장하지 마세요.
- CAT5 UTP 2-Wire 케이블을 전원 공급 용도로 사용하지 마세요.

네트워크 연결

TCP/IP

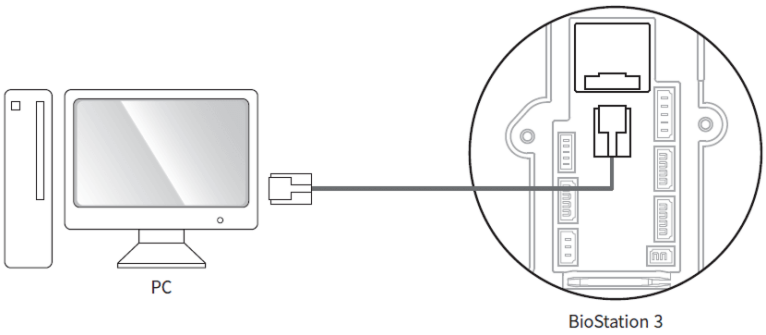
LAN 연결 (허브와 연결)

일반 타입의 CAT-5 이상의 케이블을 사용하여 허브와 연결할 수 있습니다.



LAN 연결 (PC와 직접 연결)

이 제품은 자동 MDI/MDIX 기능을 지원하므로 크로스 케이블이나 일반 스트레이트 타입의 CAT-5 이상의 케이블로 PC에 직접 연결할 수 있습니다.



알아두기

기가 비트 이더넷 스위치를 사용할 때 아래 정보를 확인하세요.

- CAT-5e 비차폐 꼬임선(UTP)을 사용하세요.
- 4 쌍(8 선)을 모두 네트워크 연결로 사용하세요.
- 네트워크 케이블의 일부 쌍이나 선을 다른 용도로 사용하지 마세요.

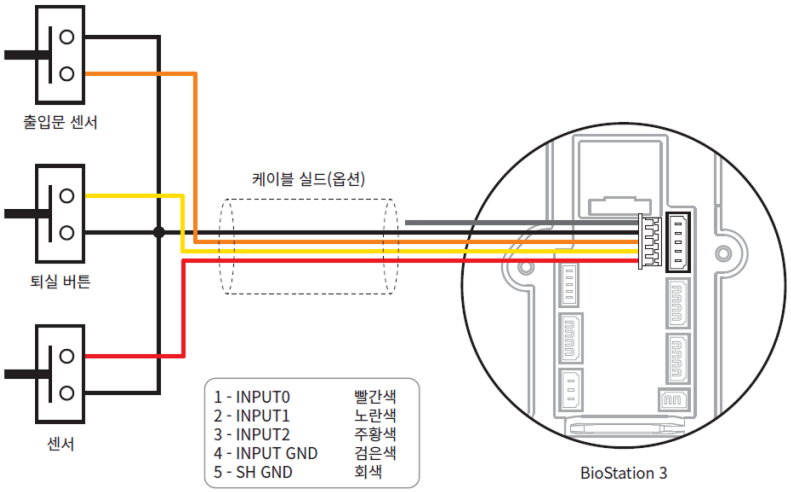
네트워크 포트 및 서비스

이 제품은 네트워크 통신 및 원활한 서비스 운영을 위해 아래와 같은 포트를 사용합니다.

프로토콜	서비스
TCP	서버와 장치 간의 통신 서비스 및 장치 운영 상태 전환 서비스를 위해 사용됩니다.
UDP	네트워크 상에서 장치를 검색하기 위한 장치 검색 서비스에 사용됩니다.

> **알아두기**
> 상기 포트는 제품의 정상적인 네트워크 기능 제공을 위해 사용되며, 방화벽 또는 네트워크 보안 설정 시 해당 포트의 사용이 허용되어야 합니다.

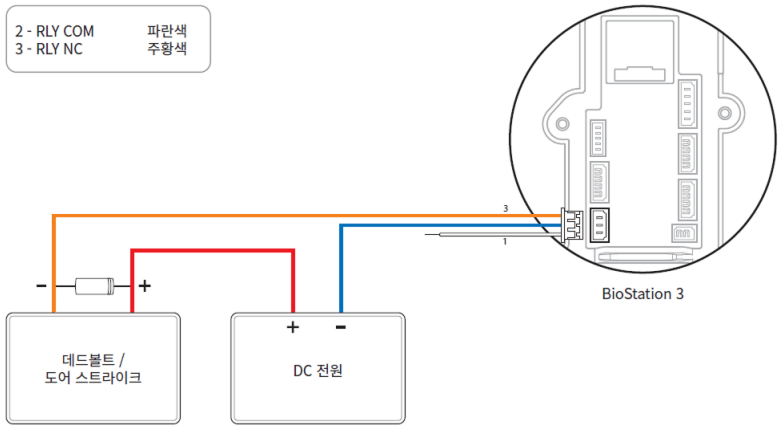
Input 연결



릴레이 연결

Fail Safe Lock

Fail Safe Lock을 사용하려면 아래 그림과 같이 N/C 릴레이를 연결하세요. Fail Safe Lock은 평상 시 릴레이 회로에 전류가 흐르며, 릴레이가 동작하여 전류를 일시적으로 차단하면 출입문이 열립니다. 정전이 되거나 외부 요인으로 장치의 전원이 끊길 경우 출입문이 열립니다.



주의

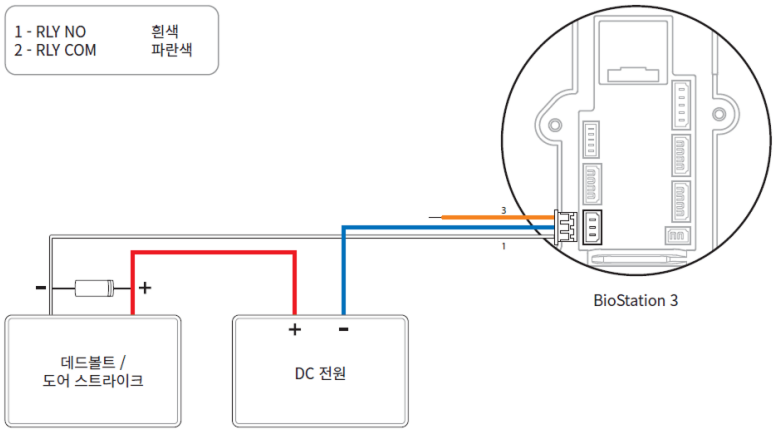
- 출입문 잠금 장치가 작동할 때 발생하는 역전류로부터 릴레이를 보호하기 위해 그림과 같이 출입문 잠금 장치 배선 양쪽에 다이오드를 설치하세요.
- 제품과 출입문 잠금 장치는 별도의 전원을 사용하세요.
- 슈프리마의 지능형 장치에는 편의를 제공하기 위해 별도의 컨트롤러 없이 독립형으로 연결하여 출입문을 직접 열거나 잠글 수 있도록 하는 릴레이가 내장되어 있습니다. 그러나 향상된 보안이 요구되는 출입통제 애플리케이션의 경우 잠재적으로 출입문 잠금 해제를 유발할 수 있는 변조 공격을 방지하기 위해 장치에 내장된 릴레이를 사용하지 않는 것이 좋습니다. 이러한 애플리케이션의 경우 잠금 제어를 위해 출입문 내부의 안전한 위치에 설치된 슈프리마의 Secure I/O 2, DM-20, CoreStation과 같은 별도의 릴레이 장치를 사용할 것을 권장합니다.

알아두기

다이오드의 설치 방향에 주의하세요. 다이오드는 출입문 잠금 장치와 가깝게 설치하세요.

Fail Secure Lock

Fail Secure Lock을 사용하려면 아래 그림과 같이 N/O 릴레이를 연결하세요. Fail Secure Lock은 평상 시 릴레이 회로에 전류가 흐르지 않으며, 릴레이가 동작하여 전류가 흐르면 출입문이 열립니다. 정전이 되거나 외부 요인으로 장치의 전원이 끊길 경우 출입문이 잠깁니다.



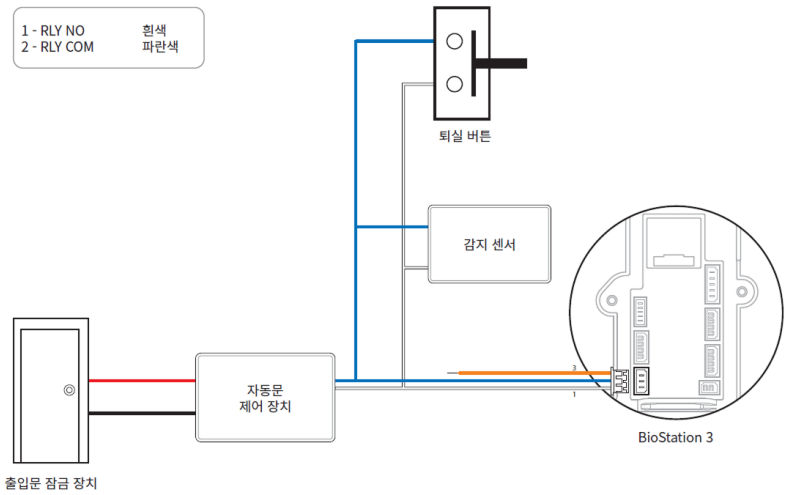
주의

- 출입문 잠금 장치가 작동할 때 발생하는 역전류로부터 릴레이를 보호하기 위해 그림과 같이 출입문 잠금 장치 배선 양쪽에 다이오드를 설치하세요.
- 제품과 출입문 잠금 장치는 별도의 전원을 사용하세요.
- 슈프리마의 지능형 장치에는 편의를 제공하기 위해 별도의 컨트롤러 없이 독립형으로 연결하여 출입문을 직접 열거나 잠글 수 있도록 하는 릴레이가 내장되어 있습니다. 그러나 향상된 보안이 요구되는 출입통제 애플리케이션의 경우 잠재적으로 출입문 잠금 해제를 유발할 수 있는 변조 공격을 방지하기 위해 장치에 내장된 릴레이를 사용하지 않는 것이 좋습니다. 이러한 애플리케이션의 경우 잠금 제어를 위해 출입문 내부의 안전한 위치에 설치된 슈프리마의 Secure I/O 2, DM-20, CoreStation과 같은 별도의 릴레이 장치를 사용할 것을 권장합니다.

알아두기

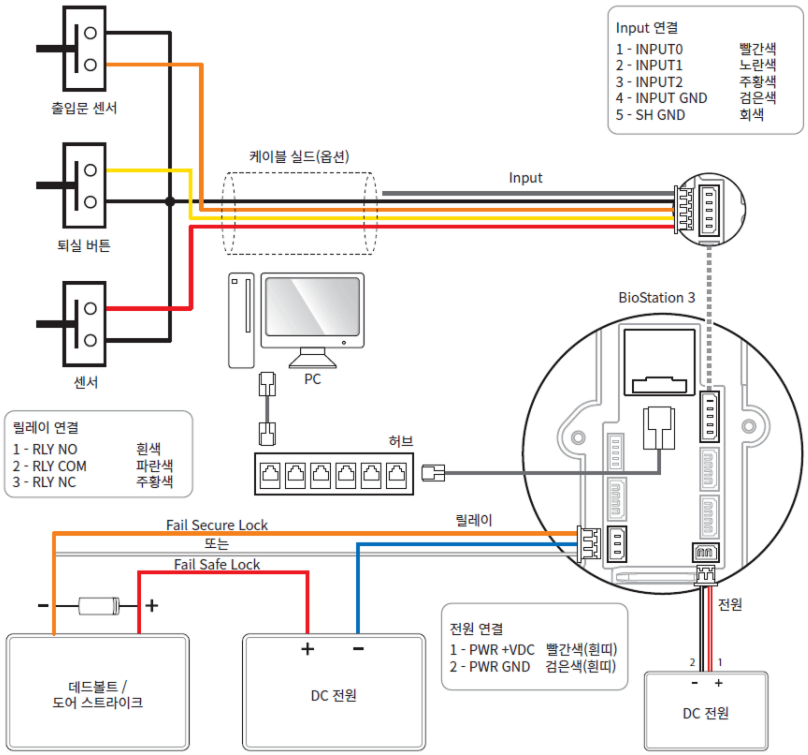
다이오드의 설치 방향에 주의하세요. 다이오드는 출입문 잠금 장치와 가깝게 설치하세요.

자동문 연결



독립형 연결

별도의 I/O 장치를 연결하지 않고 제품을 직접 출입문 잠금 장치, 퇴실 버튼, 출입문 센서 등에 연결할 수 있습니다.



주의

슈프리마의 지능형 장치에는 편의를 제공하기 위해 별도의 컨트롤러 없이 독립형으로 연결하여 출입문을 직접 열거나 잠글 수 있도록 하는 릴레이가 내장되어 있습니다. 그러나 향상된 보안이 요구되는 출입통제 애플리케이션의 경우 잠재적으로 출입문 잠금 해제를 유발할 수 있는 변조 공격을 방지하기 위해 장치에 내장된 릴레이를 사용하지 않는 것이 좋습니다. 이러한 애플리케이션의 경우 잠금 제어를 위해 출입문 내부의 안전한 위치에 설치된 슈프리마의 Secure I/O 2, DM-20, CoreStation과 같은 별도의 릴레이 장치를 사용할 것을 권장합니다.

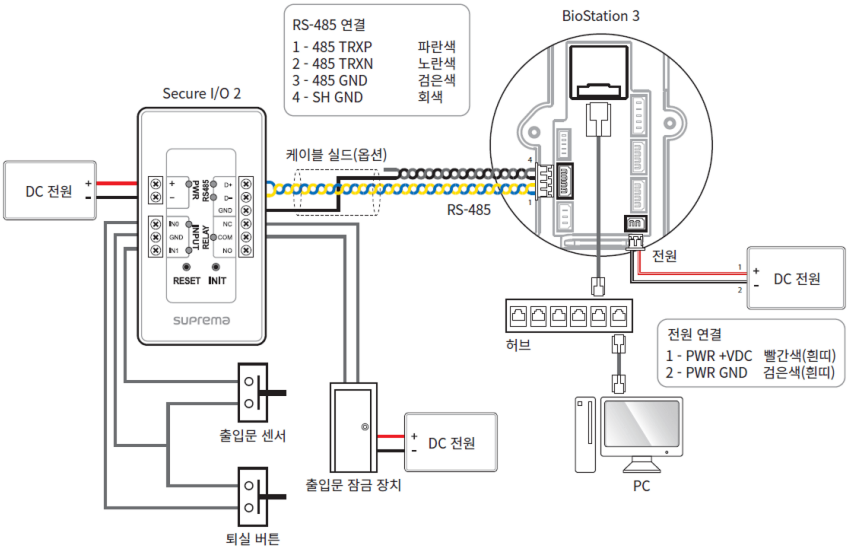
알아두기

- RS-485 케이블로 슬레이브 장치를 연결하여 제품을 다중 출입문 제어 장치로 사용할 수 있습니다. 슬레이브 장치는 더미 리더로 사용되며 인증은 마스터 장치에서 수행합니다.
- FaceStation 2, FaceLite가 마스터 장치일 때 BioStation 3를 슬레이브 장치로 사용할 수 없으며, 반대의 경우로도 사용할 수 없습니다.
- 연결할 수 있는 최대 슬레이브 장치 수는 인증 방법, 사용자 수, 장치 수에 따라 달라지며 슬레이브 장치 수는 인증 속도에 영향을 줍니다.
- 하나의 마스터 장치당 최대 31대의 슬레이브 장치를 연결할 수 있습니다. RS-485 대역폭으로 인해 최대 7대의 지문 인식 장치를 연결할 수 있습니다.
- 더 자세한 내용은 슈프리마 기술 지원팀(CS@suprema.co.kr)에 문의하세요.

Secure I/O 2 연결

제품에 I/O 장치인 Secure I/O 2를 RS-485로 연결할 수 있습니다. 제품과 Secure I/O 2의 연결이 끊기거나 외부 요인에 의해 제품의 전원이 차단되더라도 보안을 유지할 수 있습니다.

- RS-485 케이블은 AWG24, 꼬임선(Twisted Pair), 최대 길이 1.2 km를 사용하세요.
- RS-485 케이블은 특성 임피던스가 120 Ω인 케이블을 사용하는 것을 권장합니다.
- RS-485 데이지 체인으로 연결할 경우 종단 저항(120Ω)을 데이지 체인 연결의 양 끝에 연결하세요. 중간 선로에 연결할 경우 신호 레벨이 작아져 통신 성능이 떨어지므로 반드시 데이지 체인 연결의 양 끝에 연결하세요.

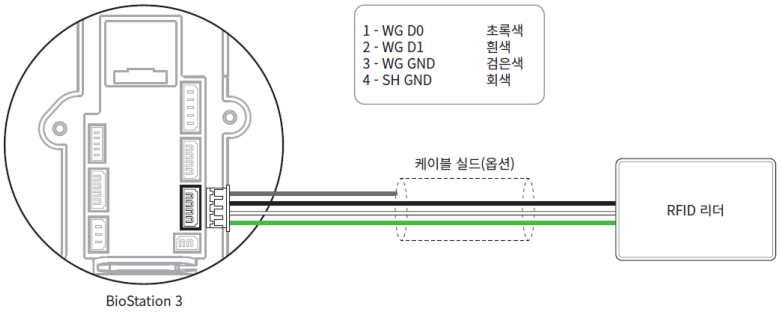


알아두기

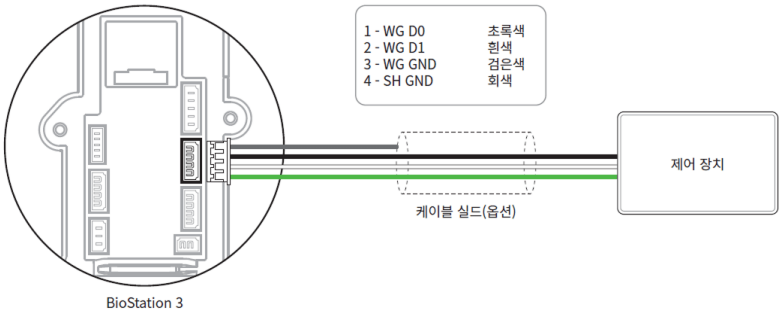
- RS-485 케이블로 슬레이브 장치를 연결하여 제품을 다중 출입문 제어 장치로 사용할 수 있습니다. 슬레이브 장치는 더미 리더로 사용되며 인증은 마스터 장치에서 수행합니다.
- FaceStation 2, FaceLite가 마스터 장치일 때 BioStation 3를 슬레이브 장치로 사용할 수 없으며, 반대의 경우로도 사용할 수 없습니다.
- 연결할 수 있는 최대 슬레이브 장치 수는 인증 방법, 사용자 수, 장치 수에 따라 달라지며 슬레이브 장치 수는 인증 속도에 영향을 줍니다.
- 하나의 마스터 장치당 최대 31대의 슬레이브 장치를 연결할 수 있습니다. RS-485 대역폭으로 인해 최대 7대의 지문 인식 장치를 연결할 수 있습니다.
- 더 자세한 내용은 슈프리마 기술 지원팀(CS@suprema.co.kr)에 문의하세요.

Wiegand 연결

Wiegand 입력 장치로 사용



Wiegand 출력 장치로 사용



사용하기

장치의 주요 기능을 효과적으로 사용하는 방법을 안내합니다.

관리자 메뉴

관리자 권한으로 접근 가능한 주요 메뉴와 기능을 안내합니다.

대시보드

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
   대시보드에서 장치 사용 현황 및 정보를 확인할 수 있습니다. 또는 **사용자 등록 마법사**를 눌러 바로 사용자를 등록할 수도 있습니다.
2. 사용자를 등록하거나 장치를 설정하려면 대시보드 하단에서 원하는 메뉴를 선택하세요.



알아두기

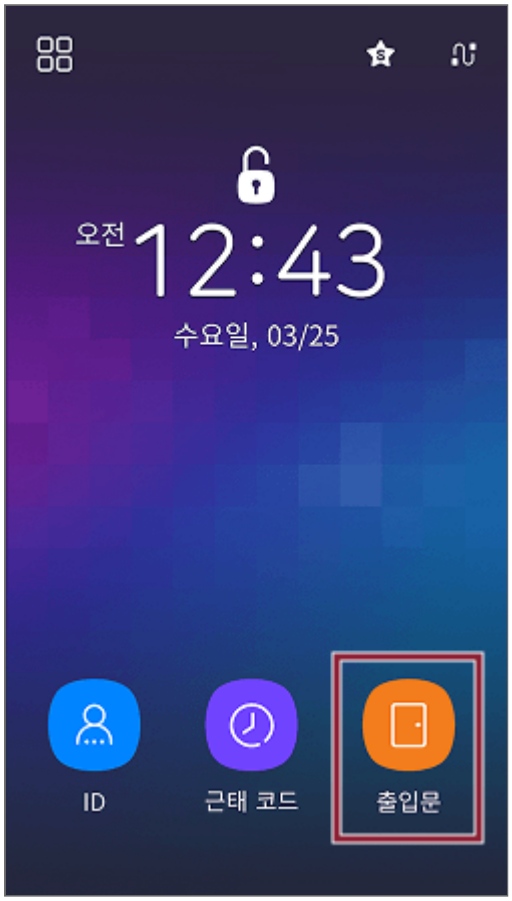
- 관리자가 지정되어 있지 않을 경우 을 누르면 **대시보드** 화면이 나타납니다.
- **무선 MAC** 항목은 BS3-APWB 모델에서만 확인할 수 있습니다.

출입문 제어

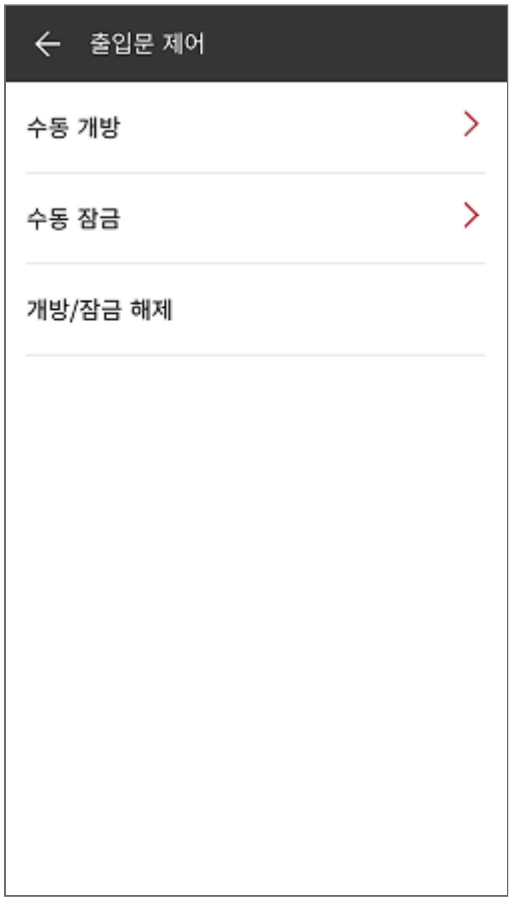
연결된 출입문을 수동으로 개방, 잠금 또는 해제할 수 있습니다.

> **알아두기**
>
> - 장치를 마스터 장치로 구성한 경우에만 출입문을 제어할 수 있습니다.
> - **전체 관리자** 또는 **설정 관리자**가 출입문을 제어할 수 있습니다.

1. 홈 화면에서 **출입문**을 선택하세요.



2. 관리자 권한 인증 수단으로 인증하세요.
3. 원하는 출입문 제어 방식을 선택하세요.



- **수동 개방**: 출입문을 즉시 개방하거나 개방 상태를 유지할 시간을 설정할 수 있습니다.
- **수동 잠금**: 출입문을 즉시 잠그거나 잠금 상태를 유지할 시간을 설정할 수 있습니다.
- **개방/잠금 해제**: 수동 개방 또는 잠금 상태를 해제합니다.

> **알아두기**
> 수동 개방 및 잠금 유지 시간은 1~86,400초로 설정할 수 있습니다.

사용자

사용자 등록, 수정, 삭제 및 관리 방법을 설명합니다.

사용자 정보 등록

생체 인증 정보를 포함한 사용자 정보를 등록할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **사용자** → 을 선택한 뒤 원하는 항목을 설정하세요. 사용자 정보 등록은 2단계로 진행되며, 일부 옵션은 인증 수단을 등록한 뒤에 활성화됩니다.





- : 사용자 사진을 등록할 수 있습니다.
- **이름**: 사용자 이름을 입력할 수 있으며, 특수 기호(`~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`)를 포함하여 최대 48자까지 입력할 수 있습니다. 단, `&` `@` `~`로 시작하는 이름은 입력할 수 없습니다.
- **ID**: 1~4294967295 숫자를 입력해 사용자 ID를 등록할 수 있습니다. **사용자 ID 종류**를 **영숫자**로 설정한 경우 영숫자와 일부 특수 기호(`_` `-` `.`)를 조합하여 최대 32자까지 입력할 수 있습니다. ID는 띄어쓰기를 포함할 수 없으며, 마침표(`.`)는 포함할 수 있으나 마침표 하나(`.`) 또는 마침표 두 개(`..`)만으로는 입력할 수 없습니다.
- **얼굴**: 사용자 인증을 위한 얼굴을 등록할 수 있습니다. **얼굴** → **다음**을 누른 뒤 화면의 지시에 따라 얼굴을 등록하세요. 얼굴을 더 등록하려면 +을 누르세요. 얼굴 등록에 대한 자세한 내용은 사용자 얼굴 등록을 참고하세요.
- **카드 / QR코드**: 사용자 인증을 위한 카드를 등록할 수 있습니다. **카드 / QR코드** → **다음**을 누른 뒤 사용자에게 할당할 카드를 RF 카드 인증부에 스캔하세요. 카드를 더 등록하려면 **카드 / QR코드** → +을 누르세요.
- **PIN**: 사용하려는 PIN을 입력할 수 있습니다. **PIN** → **다음**을 누른 뒤 사용하려는 PIN을 입력하세요. 확인을 위해 한 번 더 PIN을 입력한 뒤 **OK**를 누르세요. PIN은 유출 방지를 위해 최소 4~16자리 숫자를 입력하세요.

> **알아두기**
> **마스터 관리자** 기능을 사용하는 경우 최소 8자리의 숫자를 입력하세요.

- **사용자 권한**: 사용자에게 할당할 권한을 선택할 수 있습니다.

> **알아두기**
>
> 설정된 사용자 권한에 따라 사용할 수 있는 메뉴가 다릅니다.
>
> - **권한 없음**: 일반 사용자 등급이며 메뉴를 사용할 수 없습니다.
> - **전체 관리자**: 모든 메뉴를 사용할 수 있습니다.
> - **설정 관리자**: **인증**, **화면과 소리**, **장치**, **네트워크**, **이벤트 로그** 메뉴를 사용할 수 있습니다.
> - **사용자 관리자**: **사용자**, **이벤트 로그** 메뉴를 사용할 수 있습니다.

- **유효기간**: 사용자 계정을 사용할 기간을 설정할 수 있습니다.
- **확장 개인 인증 모드**: 확장 개인 인증 모드를 설정할 수 있습니다. 확장 개인 인증 모드를 사용하면 사용자에 따른 인증 방식을 얼굴을 포함하여 조합할 수 있습니다. 사용하지 않을 경우 장치의 기본 인증 모드를 사용합니다.

3. 사용자 정보 등록을 완료하려면 **저장**을 누르세요.

사용자 얼굴 등록

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **사용자** → 을 선택하세요.
3. **얼굴** → **다음**을 누르세요.
4. 화면에 얼굴이 나타나도록 거리를 조정하고, 장치의 카메라를 정면으로 바라보세요.
5. 촬영이 완료되면 **확인** → **저장**을 누르세요. 얼굴을 다시 촬영하려면 **재촬영**을 누르세요.

> **알아두기**
>
> - 이 제품의 얼굴 정보는 FaceStation 2, FaceLite의 얼굴 정보와 호환되지 않습니다.
> - 이 제품의 얼굴 정보는 장치에서뿐만 아니라 BioStar X에서 사진을 업로드하거나 CSV 불러오기를 통해 일괄 등록할 수도 있습니다. 사용자에게 얼굴 등록 링크를 전송하여 사용자 개인의 모바일 장치로도 얼굴을 등록할 수 있습니다. 각각의 등록 방법에 대한 자세한 내용은 BioStar X 관리자 설명서를 참고하세요.
> - 얼굴을 등록할 때 다음 사항에 유의하세요.
>   - 얼굴을 등록할 때 장치와 얼굴의 거리를 60~100 cm로 유지하세요.
>   - 표정이 변하지 않도록 주의하세요.
>   - 마스크, 모자, 안대를 착용하지 마세요.
>   - 마스크를 착용한 얼굴을 등록하지 마세요. 마스크를 착용한 얼굴과 착용하지 않은 얼굴을 모두 등록할 경우 오인식률이 높아질 수 있습니다.
>   - 고개를 들거나 숙이지 마세요.
>   - 진한 화장을 하지 마세요.
>   - 눈을 감지 마세요.
>   - 화면에 양쪽 어깨가 모두 나타나도록 하세요.
>   - 움직이지 말고, 정면으로 서서 얼굴을 등록하세요.
>   - 두 명의 얼굴이 화면에 동시에 나타나지 않도록 주의하세요. 한 번에 한 사람씩 등록하세요.
>   - 화면의 지시에 따르지 않을 경우 얼굴 등록이 오래 걸리거나 실패할 수 있습니다.

사용자 정보 편집

사용자 관리자나 전체 관리자가 등록된 사용자 정보를 편집할 수 있습니다. 사용자의 얼굴이나 카드를 추가할 수 있으며, PIN 및 권한을 수정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **사용자** → 을 누르세요.
3. 사용할 검색 조건을 선택하세요. **전체**, **사용자 ID**, **이름**, **얼굴**, **카드**로 사용자를 검색할 수 있습니다.
4. 편집하려는 사용자를 선택하세요.
5. 사용자 정보 등록을 참고하여 정보를 수정한 뒤 **OK**를 누르세요.
   - 사용자를 삭제하려면 을 선택한 뒤 **확인**을 누르세요.

> **알아두기**
> **출입 그룹**은 BioStar X에서 등록할 수 있습니다. 출입 그룹 등록에 대한 자세한 내용은 BioStar X 관리자 설명서를 참고하세요.

사용자 전체 삭제

등록된 모든 사용자를 한 번에 삭제할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **사용자** → 을 선택하세요.
3. **전체 삭제**를 선택해 체크한 뒤 **OK**를 누르세요.
4. 전체 사용자를 삭제하려면 **확인**을 누르세요.

사용자 등록현황 보기

등록된 사용자, 얼굴, 카드 수를 한 눈에 볼 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **사용자** → 을 누르세요. 사용자 등록현황을 확인할 수 있습니다.



인증

지원하는 인증 방식과 인증 절차를 설명합니다.

인증 모드

장치의 인증 모드를 설정할 수 있습니다. **얼굴**, **PIN**, **카드 / QR코드**, **ID**를 조합하여 인증 모드로 사용할 수 있으며, 각 인증 모드마다 사용할 스케줄을 설정할 수도 있습니다.

인증 모드 등록

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증** → **인증 모드**를 누르세요.
3. 을 선택하세요.
4. 을 누르면 추가할 수 있는 크리덴셜이 화면에 나타납니다. 원하는 크리덴셜을 추가하세요. 크리덴셜이 추가된 상태에서 을 누르면 추가한 크리덴셜을 삭제할 수 있습니다.



5. 원하는 인증 모드를 설정한 뒤 **스케줄**을 설정하세요.

구분	설명
얼굴	- : 얼굴만 사용하는 모드입니다. - + : 얼굴로 인증한 뒤 PIN을 입력하는 모드입니다.
카드 / QR코드	- : 카드 / QR코드만 사용하는 모드입니다. - + : 카드 / QR코드로 인증한 뒤 얼굴로 인증하는 모드입니다. - + : 카드 / QR코드로 인증한 뒤 PIN을 입력하는 모드입니다. - + / : 카드 / QR코드로 인증한 뒤 얼굴로 인증하거나 PIN을 입력하는 모드입니다. - + + : 카드 / QR코드로 인증한 뒤 얼굴 인증과 PIN 입력을 모두 사용하는 모드입니다.
ID	- ID + : ID를 입력한 뒤 얼굴로 인증하는 모드입니다. - ID + : ID를 입력한 뒤 PIN을 입력하는 모드입니다. - ID + / : ID를 입력한 뒤 얼굴로 인증하거나 PIN을 입력하는 모드입니다. - ID + + : ID를 입력한 뒤 얼굴 인증과 PIN 입력을 모두 사용하는 모드입니다.

알아두기

- **스케줄**은 BioStar X에서 설정할 수 있습니다. 설정한 스케줄이 없다면 **항상 사용**만 선택할 수 있습니다.
- **스케줄** 설정에 대한 자세한 내용은 BioStar X 관리자 설명서를 참고하세요.
- **QR 코드** 인증을 사용하려면 **인증** → **인증 옵션**에서 **QR 인증**이 활성화 되어있어야 하며, 별도의 장치 라이선스가 필요합니다. 자세한 내용은 라이선스를 참고하세요.

6. 설정을 저장하려면 **OK**를 누르세요.

인증 모드 편집

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증** → **인증 모드**를 누르세요.
3. 수정할 인증 모드를 선택하세요.
4. 인증 모드 등록을 참고하여 인증 모드를 수정한 뒤 **OK**를 누르세요.

인증 모드 삭제

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증** → **인증 모드**를 누르세요.
3. 을 누른 뒤 삭제할 항목을 선택하세요. 여러 개를 선택할 수도 있습니다.
4. 선택한 항목을 삭제하려면 **OK**를 누르세요.

인증 옵션

서버 매칭, **QR 인증** 등 인증 관련 옵션을 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증**을 누른 뒤 **인증 옵션**에서 원하는 옵션을 활성화하세요.



- **서버 매칭 (카드, ID)**: 서버 매칭을 사용하면 장치가 아닌 BioStar X에서 사용자 인증을 수행합니다. 장치에 저장된 사용자 정보가 많거나 크리덴셜 정보가 저장된 장치를 외부에 노출하고 싶지 않은 경우 유용하게 사용할 수 있습니다.

  알아두기

  - **서버 매칭**은 카드, ID만 사용할 수 있습니다.
  - **서버 매칭**을 사용할 경우 장치와 BioStar X에서 서버 매칭을 활성화해야 합니다. BioStar X 서버 매칭 설정에 대한 자세한 내용은 BioStar X 관리자 설명서를 참고하세요.

- **QR 인증**: 장치의 카메라를 통한 QR 코드 인증 사용 여부를 설정할 수 있습니다.

> **알아두기**
> **QR 인증**을 사용하려면 별도의 장치 라이선스가 필요합니다. 자세한 내용은 라이선스를 참고하세요.

- **카드를 QR로 인증하기**: 사용자에게 발급한 CSN 카드 또는 Wiegand 카드와 동일한 데이터의 QR코드로 인증할 수 있도록 설정할 수 있습니다. **QR 인증**이 활성화되어있는 경우에만 설정할 수 있습니다.

PIN

비밀번호 입력 시 스크램블 키패드 사용 여부를 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증**을 누른 뒤 **PIN**에서 **스크램블 키패드** 사용 여부를 설정하세요.



- **스크램블 키패드**: 비밀번호를 입력할 때 숫자 키의 위치가 무작위로 섞여 비밀번호 유출을 방지할 수 있습니다.

인증 결과 표시 옵션

인증 결과 표시 옵션을 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증**을 누른 뒤 **인증 결과 표시 옵션**에서 원하는 항목을 변경하세요.

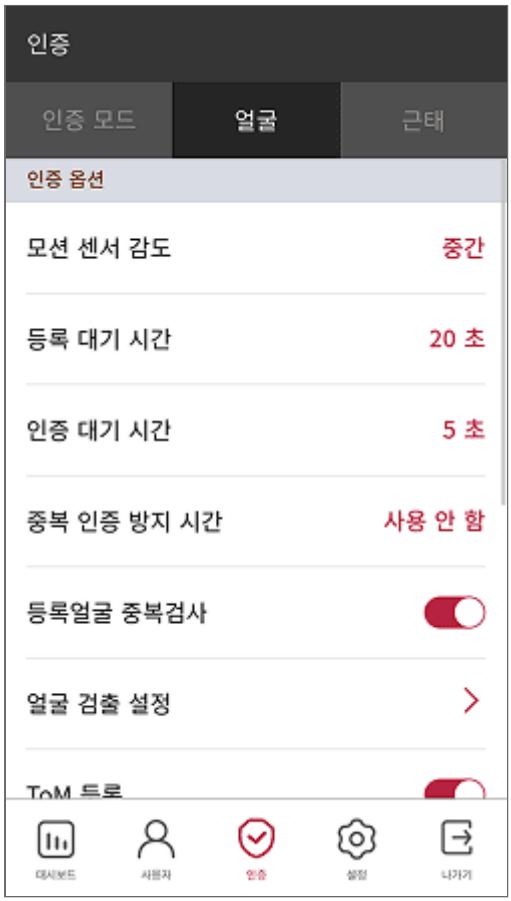


- **사용자 ID 표시**: 장치의 인증 결과 화면에서 사용자 ID가 표시되는 방법을 선택할 수 있습니다.
  - **전체 표시**: 사용자 ID를 모두 표시합니다.
  - **첫 문자만 표시**: 사용자 ID의 첫 문자만 표시합니다.
  - **표시하지 않기**: 사용자 ID를 표시하지 않습니다.
- **사용자 이름 표시**: 장치의 인증 결과 화면에서 사용자 이름이 표시되는 방법을 선택할 수 있습니다.
  - **전체 표시**: 사용자 이름을 모두 표시합니다.
  - **첫 문자만 표시**: 사용자 이름의 첫 문자만 표시합니다.
  - **표시하지 않기**: 사용자 이름을 표시하지 않습니다.

얼굴

얼굴 인증에 대한 설정을 변경할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증** → **얼굴**을 선택하세요.
3. 원하는 항목을 변경하세요.



- **모션 센서 감도**: 장치 주변에 움직임을 감지하는 감도를 설정합니다. **모션 센서 감도**를 **끔**으로 설정한 경우, 얼굴을 인증하려면 화면을 터치한 뒤 인증을 진행하세요.
- **등록 대기 시간**: 설정한 시간 동안 얼굴을 등록하지 못하면 얼굴 등록이 취소됩니다.
- **인증 대기 시간**: 설정한 시간 동안 인증을 완료하지 못하면 인증에 실패합니다.
- **중복 인증 방지 시간**: 동일한 얼굴이 다시 감지되었을 때 설정한 시간 동안 중복으로 인증되지 않도록 설정할 수 있습니다. **사용 안 함** 또는 3~60초로 설정할 수 있습니다.

  > **알아두기**
  > **중복 인증 방지 시간**은 마스터 장치에서만 사용할 수 있습니다.

- **등록얼굴 중복검사**: 얼굴 등록 시 중복 얼굴 여부를 검사할 수 있습니다.
- **얼굴 검출 설정**: 얼굴 인증 시 장치가 얼굴을 검출할 영역의 위치와 크기를 설정할 수 있습니다.

> **알아두기**
>
> 최적의 성능을 위해 **얼굴 검출 설정**의 하위 옵션은 기본 설정 값 사용을 권장합니다. 각 옵션의 기본 값은 다음과 같습니다.
>
> – 최대 얼굴 회전 각도: 15
>
> – 얼굴 인식 거리: 최소 30 cm, 최대 100 cm
>
> – 얼굴 인식 영역 넓히기: 비활성화

- **ToM 등록**: **ToM 등록**을 활성화하면 BioStar X에서 발급받은 **템플릿 온 모바일**을 등록할 수 있습니다. **템플릿 온 모바일**은 사용자의 바이오 메트릭 템플릿을 모바일 기기에 저장하는 모바일 액세스 카드로 BioStar X 서버, Airfob Portal과 장치에 사용자 데이터를 저장하지 않고도 바이오 메트릭으로 인증할 수 있습니다.

> **알아두기**
>
> **템플릿 온 모바일**에 대한 자세한 내용은 BioStar X 관리자 설명서를 참고하세요.

- **비주얼 페이스 이미지 저장하기**: 비주얼 페이스에 실제 이미지와 템플릿을 모두 저장하도록 하거나 실제 이미지는 저장하지 않고 템플릿만 저장하도록 설정할 수 있습니다. 비활성화할 경우 저장된 비주얼 페이스의 이미지가 모두 삭제되며, 앞으로 등록되는 비주얼 페이스도 이미지를 제외한 템플릿만을 저장합니다.

> **알아두기**
>
> 이 설정을 비활성화한 후에는 BioStar 2 v2.9.7 이상 또는 BioStar X에 연결하여 사용하세요.

- **보안 등급**: 1:N 인증을 위한 보안 등급을 설정할 수 있습니다.
- **작동 모드**: 얼굴 인증 시 장치의 작동 모드를 설정할 수 있습니다.
  - **퓨전 매칭**: 비주얼 및 적외선 매칭이 모두 동작하여 얼굴 인증의 정확도를 높일 수 있습니다.
  - **빠른 인증**: 사용자는 장치의 인증 범위 안에서 걸어가면서도 얼굴을 인증하는 등 빠르게 인증을 수행할 수 있습니다.
- **위조 얼굴 검출**: 사진 등의 위조 얼굴을 이용한 사용자 인증을 방지할 수 있습니다. **작동 모드**를 **퓨전 매칭**으로 설정할 때 활성화됩니다.

> **알아두기**
>
> – 위조 얼굴 검출 성능을 개선하여 iBeta Level 1 ISO 30107-3 제시형 공격 탐지 시험에 통과하였습니다.
>
> – 햇빛이 강한 환경에서는 **위조 얼굴 검출** 기능을 **보통**으로 사용하는 것을 권장합니다.

- **고급 설정**: 마스크 검출 등 얼굴 인증에 대한 고급 설정을 변경할 수 있습니다.
  - **마스크 검출**: 마스크 검출 사용 여부를 설정할 수 있습니다.
  - **검출 모드**: 마스크 착용 여부를 확인하는 방식을 설정할 수 있습니다. **마스크 검출**을 **사용**으로 설정할 경우 활성화됩니다.

> **알아두기**
>
> - **마스크 착용 (하드)**: 마스크를 착용하지 않은 사용자는 인증이 거부되며, 마스크 미착용 이벤트가 로그로 기록됩니다.
> - **마스크 착용 (소프트)**: 마스크를 착용하지 않은 사용자도 인증할 수 있으나 마스크 미착용 이벤트가 로그로 기록됩니다.
> - **마스크 미착용**: 마스크를 착용하지 않은 사용자만 인증할 수 있으며, 이 모드를 사용할 경우 마스크 확인 모드가 **확인 후 인증**으로 고정됩니다.

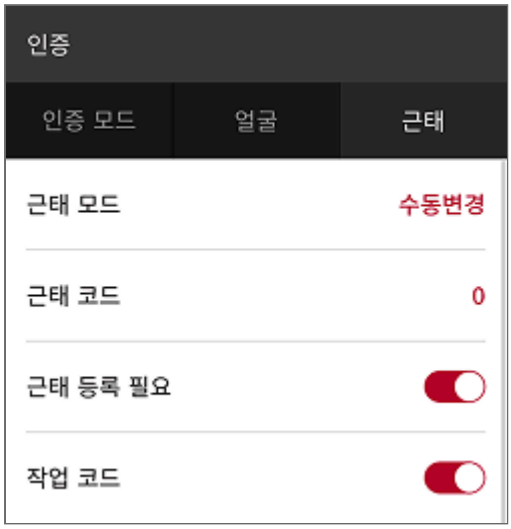
- **마스크 검출 등급**: 마스크 착용을 감지하는 감도를 설정할 수 있습니다. **마스크 검출**을 **사용**으로 설정할 경우 활성화됩니다.
- **확인 모드**: 장치의 용도에 따라 확인 모드를 설정할 수 있습니다.

> **알아두기**
>
> - **인증 후 확인**: 인증을 수행한 뒤 사용자의 마스크 착용 여부를 확인합니다.
> - **확인 후 인증**: 사용자의 마스크 착용 여부를 확인한 뒤 인증을 수행합니다.
> - **확인만**: 장치를 마스크 착용 여부를 확인하는 용도로만 사용할 수 있습니다. 이 모드를 사용할 경우 인증과 관계없이 마스크를 착용한 사용자는 모두 출입할 수 있습니다.

근태

근태 모드 등록 방법을 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **인증** → **근태**를 선택하세요.
3. 원하는 항목을 설정하세요.



- **근태 모드**: 근태 모드를 사용할 방법을 설정할 수 있습니다.
- **근태 코드**: 근태 이벤트를 등록할 수 있습니다. 근태 이벤트를 등록하려면 **근태 코드** → 을 선택한 뒤 화면에 표시할 아이콘, **근태 이벤트 이름**, **스케줄**을 설정하세요.

- **근태 등록 필요**: 사용자가 인증할 때 근태 이벤트를 반드시 선택하도록 설정할 수 있습니다. **근태 모드**를 **수동변경**으로 설정했을 때 사용할 수 있습니다.
- **근태 고정 키**: 관리자가 선택한 근태 이벤트만 사용하도록 설정할 수 있습니다. **근태 모드**를 **고정**으로 설정했을 때 사용할 수 있습니다.
- **작업 코드**: 작업 코드 사용 여부를 선택할 수 있습니다.

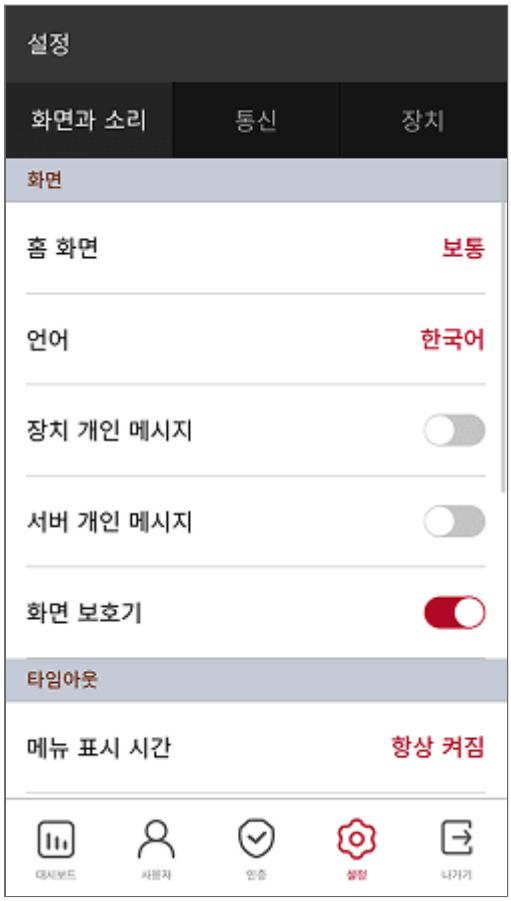
설정

시스템 및 장치 설정 방법을 안내합니다.

화면과 소리

장치의 화면과 소리에 대한 설정을 변경할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **화면과 소리**를 누르세요.
3. 원하는 항목을 변경하세요.



- **홈 화면**: 홈 화면의 배경에 표시할 항목을 선택할 수 있습니다.
- **언어**: 화면에 표시되는 언어를 선택할 수 있습니다.
- **장치 개인 메시지**: 사용자가 인증할 때 화면에 표시할 개인 메시지 사용 여부를 설정할 수 있습니다. **장치 개인 메시지**는 BioStar Device SDK를 이용하여 설정할 수 있습니다. 설정하지 않은 경우, 장치에서 **장치 개인 메시지**를 활성화하더라도 인증 성공 시

메시지가 표시되지 않습니다.

- **서버 개인 메시지**: 사용자가 인증할 때 화면에 표시할 개인 메시지 사용 여부를 설정할 수 있습니다. **서버 개인 메시지**는 BioStar X API를 이용하여 설정할 수 있습니다. 설정하지 않은 경우, 장치에서 **서버 개인 메시지**를 활성화하더라도 인증 성공 시 메시지가 표시되지 않습니다.
- **화면 보호기**: 화면 보호기 사용 여부를 설정할 수 있습니다. 장치를 사용하지 않을 때 화면 밝기를 낮춰 전력 소모를 줄일 수 있습니다.
- **메뉴 표시 시간**: 메뉴 화면이 자동으로 사라지는 시간(초)을 설정할 수 있습니다. 설정한 시간 동안 버튼 입력이 없다면 홈 화면으로 이동합니다.
- **메시지 표시 시간**: 설정 완료 메시지나 알림 메시지 등이 자동으로 사라지는 시간(초)을 설정할 수 있습니다.
- **백라이트 시간**: 화면의 조명이 꺼지는 시간(초)을 설정할 수 있습니다.
- **음성 안내**: 알림음 대신 음성 안내를 사용할 수 있습니다.
- **볼륨**: 소리 크기를 설정할 수 있습니다.
- **IP 인터폰 스피커 음량**: IP 인터폰 사용 시 스피커에서 출력되는 음량을 조절할 수 있습니다.
- **IP 인터폰 마이크 음량**: IP 인터폰 사용 시 마이크에 입력되는 음량을 조절할 수 있습니다.

> **알아두기**
> BioStar Device SDK에 대한 자세한 정보는 슈프리마 지식 베이스의 BioStar Device SDK 페이지를 참고하세요.

통신

이더넷, 서버, OSDP 통신과 같은 장치의 통신 설정을 변경할 수 있습니다.

이더넷

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **통신** → **이더넷**을 선택하세요.
3. 원하는 항목을 설정하세요.



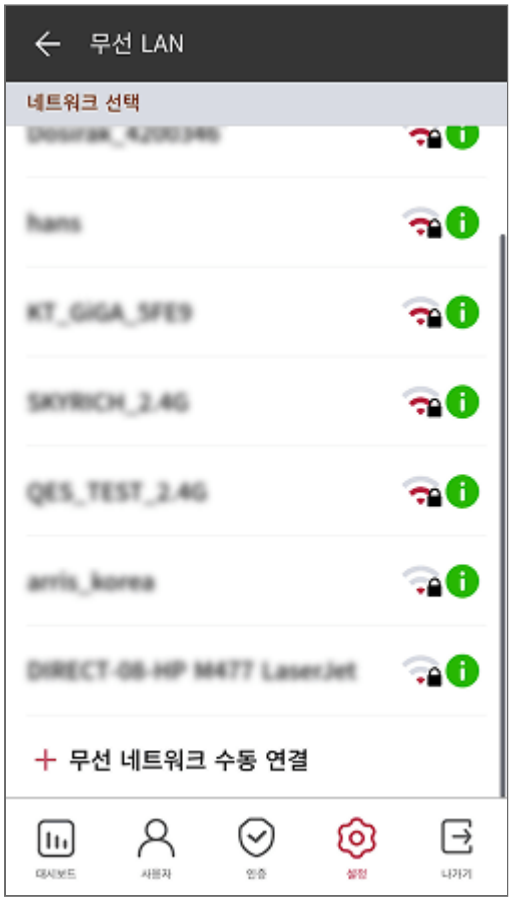
- **DHCP**: DHCP 사용 여부를 설정하세요. DHCP 설정을 끄면 **IP 주소**, **게이트웨이**, **서브넷마스크**를 사용자가 수정할 수 있습니다.
- **장치 포트**: 장치의 포트를 설정할 수 있습니다.
- **IP 주소**: 장치의 IP 주소를 확인할 수 있습니다. 수정하려면 DHCP 설정을 끄세요.
- **게이트웨이**: 장치의 게이트웨이를 확인할 수 있습니다. 수정하려면 DHCP 설정을 끄세요.
- **서브넷마스크**: 장치의 서브넷마스크를 확인할 수 있습니다. 수정하려면 DHCP 설정을 끄세요.
- **도메인네임서버**: 도메인 네임 서버 주소를 설정할 수 있습니다.

4. 설정을 저장하려면 **OK**를 누르세요.

> **알아두기**
> **이더넷**은 **무선 LAN**과 함께 사용할 수 없습니다.

무선 LAN

1. ⊞을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **통신** → **무선 LAN**을 선택하세요.
3. 연결 가능한 네트워크 목록이 나타납니다.



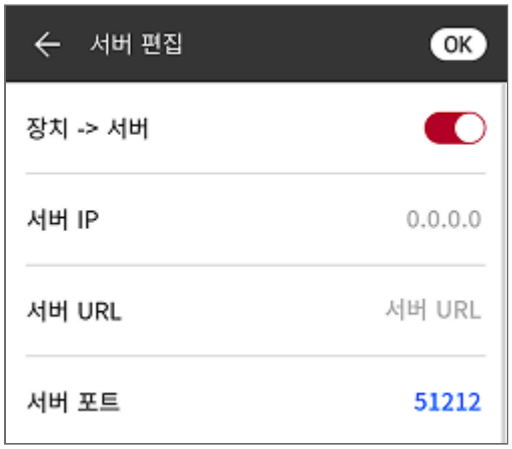
- **무선 네트워크 수동 연결**: 네트워크 정보를 직접 입력하여 무선 네트워크를 추가하고 연결할 수 있습니다.
  - **SSID**: SSID를 입력하세요. SSID는 영문(대소문자 구분), 숫자, 특수 기호를 포함하여 최대 32자까지 입력할 수 있습니다.
  - **비밀번호**: 비밀번호를 입력하세요. 비밀번호는 영문, 숫자, 특수 기호만 입력할 수 있습니다.

4. 연결하려는 네트워크를 선택한 뒤 비밀번호를 입력하세요. **OK**를 누르면 무선 네트워크에 연결됩니다.
5. 사용하려는 무선 네트워크의 ⓘ을 누른 다음 DHCP 설정을 끄면 **IP 주소**, **게이트웨이**, **서브넷마스크**를 사용자가 수정할 수 있습니다.

> **알아두기**
>
> - **무선 LAN**은 BS3-APWB 모델만 사용할 수 있습니다.
> - **무선 LAN**은 **이더넷**과 함께 사용할 수 없습니다.
> - **무선 LAN**으로 연결하려면 무선 공유기가 필요합니다. 무선 공유기에 대한 설치 및 설정에 대한 내용은 무선 공유기의 사용자 설명서를 참고하세요.

서버

1. ⊞을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **통신** → **서버**를 선택하세요.
3. 원하는 항목을 설정하세요.



- **장치 → 서버**: 장치에서 입력한 정보를 가진 서버로 직접 연결 신호를 보낼 수 있습니다. **장치 → 서버** 설정을 켜면 **서버 IP**, **서버 URL**, **서버 포트**를 사용자가 입력할 수 있습니다.
- **서버 IP**: BioStar X가 설치된 PC의 IP를 입력하세요.
- **서버 URL**: **서버 IP** 대신 **서버 URL**을 입력할 수 있습니다.
- **서버 포트**: BioStar X가 설치된 PC의 포트를 입력하세요.

4. 설정을 저장하려면 **OK**를 누르세요.

OSDP 통신 설정

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **통신**을 선택하세요.
3. **OSDP 통신 설정**에서 원하는 항목을 설정하세요.



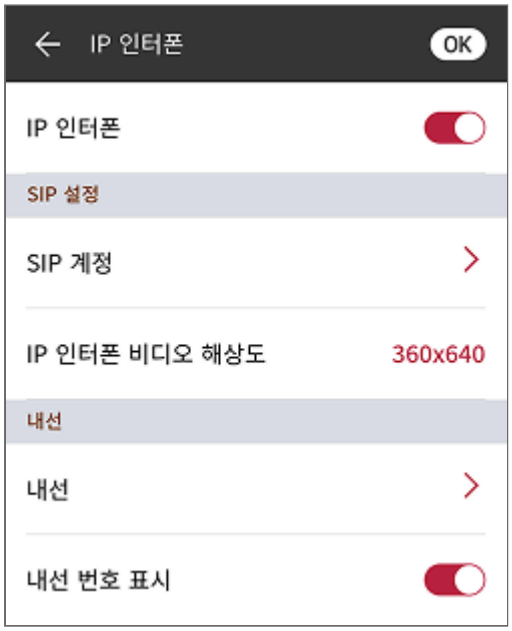
- **RS-485**: RS-485 동작 모드를 선택할 수 있습니다.
- **전송 속도**: 원하는 통신 속도를 선택할 수 있습니다.
- **인증 결과**: **인텔리전트 슬레이브**를 사용할 경우 타사 컨트롤러 또는 장치의 인증 결과를 화면에 표시하도록 선택할 수 있습니다. **RS-485** 모드를 **기본값** 또는 **슬레이브**로 설정했을 때 사용할 수 있습니다.

장치

IP 인터폰

IP 인터폰의 계정과 내선을 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **IP 인터폰**을 누르세요.



- **IP 인터폰**: IP 인터폰 활성화 여부를 설정할 수 있습니다. IP 인터폰 설정을 켜면 **SIP 계정**과 **내선**을 설정할 수 있습니다.
- **SIP 계정**: SIP 서버에 장치가 등록될 수 있도록 각 항목을 알맞게 입력하세요.
- **IP 인터폰 비디오 해상도**: 장치에서 송출되는 IP 인터폰 영상의 해상도를 선택할 수 있습니다.
- **내선**: 내선 번호를 추가 및 삭제할 수 있습니다.
- **내선 번호 표시**: 내선 번호 표시 여부를 설정할 수 있습니다.

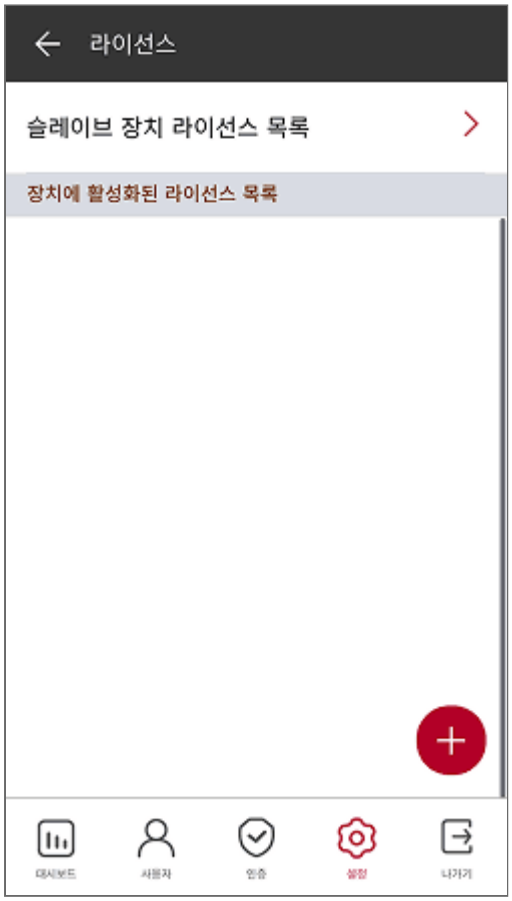
> **알아두기**
>
> - 내선 번호에 **표시 이름**을 설정하지 않은 경우 전화 걸기 화면에서 수신자를 구별할 수 없게 됩니다.
> - 내선 번호는 영문(대문자 또는 소문자), 숫자, 특수 기호 `+` `-` `@` `.`만 입력할수 있습니다.

3. 설정을 저장하려면 **OK**를 누르세요.

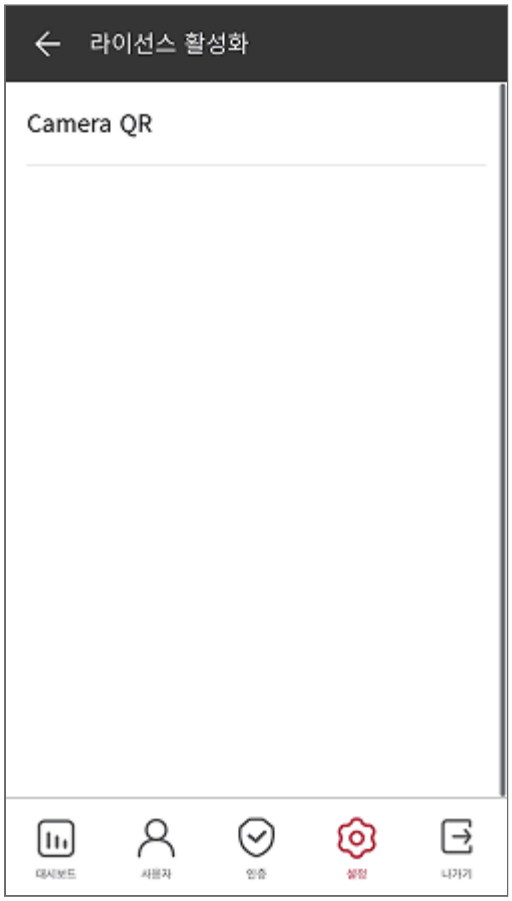
라이선스

장치 라이선스를 활성화하거나 **슬레이브 장치 라이선스 목록**과 **장치에 활성화된 라이선스 목록**을 확인할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **라이선스**를 누르세요.
3. 장치 라이선스를 활성화하려면 라이선스가 저장된 USB를 장치에 연결하고 을 선택하세요.



4. 활성화 할 수 있는 라이선스가 화면에 나타납니다. 원하는 라이선스를 활성화하세요.



알아두기

- 장치 라이선스를 발급하려면 구입처에 문의하세요.
- 장치 라이선스 하나당 한가지의 기능을 사용할 수 있습니다.
- 하나의 장치 라이선스 파일에 다수의 장치 라이선스를 포함시킬 수 있습니다. (최대 100개까지 지원)
- 장치 라이선스 파일은 암호화 된 파일이므로 임의로 수정할 수 없습니다.
- 장치 라이선스는 장치 ID를 기준으로 발급됩니다. 비정상적인 방법으로 장치 ID를 변경할 경우 라이선스에 대한 보증 서비스가 제공되지 않습니다.

릴레이

장치에서 **문열림 시간**과 **퇴실 버튼**의 입력 포트를 설정할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **릴레이**를 누르세요.

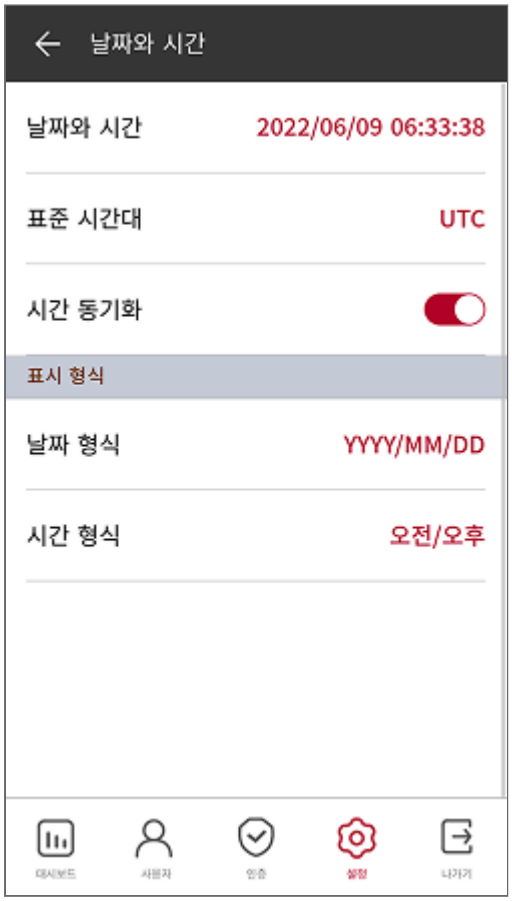


- **릴레이**: 릴레이 활성화 여부를 설정할 수 있습니다. 릴레이 설정을 켜면 **문열림 시간**, **퇴실 버튼**을 설정할 수 있습니다.
- **문열림 시간**: 정상적으로 사용자 인증이 수행되었을 때 출입문이 열려 있는 시간을 설정할 수 있습니다.
- **퇴실 버튼**: 퇴실 버튼이 연결되어 있는 입력 포트를 선택하세요.
- **입력 방식**: 퇴실 버튼 입력 포트의 스위치(**N/O** 또는 **N/C**) 종류를 선택할 수 있습니다.

날짜와 시간

날짜와 시간을 설정할 수 있습니다. 정확한 로그 데이터 수집을 위해 알맞게 설정하세요.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **날짜와 시간**을 누르세요.
3. 원하는 항목을 변경하세요.



- **날짜와 시간**: 현재 날짜와 시간을 확인할 수 있습니다. 직접 수정하려면 **시간 동기화**를 끄세요.
- **표준 시간대**: 현재 지역의 시간 기준을 설정할 수 있습니다.
- **시간 동기화**: 서버와 시간을 동기화할 수 있습니다. 서버와 시간을 동기화하려면 **시간 동기화**를 켜세요.
- **날짜 형식**: 날짜 형식을 설정할 수 있습니다. **YYYY/MM/DD**, **MM/DD/YYYY**, **DD/MM/YYYY**를 선택할 수 있습니다.
- **시간 형식**: 시간 형식을 설정할 수 있습니다. **오전/오후**, **24시간**을 선택할 수 있습니다.

일광절약시간

일광 절약 시간제(DST)를 적용해 장치를 사용할 수 있습니다. 시작 및 종료 일시를 알맞게 설정하세요.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **일광절약시간**을 선택한 뒤 을 눌러 일광 절약 시간을 추가하세요.
3. 원하는 항목을 변경하세요.



- **이름**: 일광 절약 시간의 이름을 입력하세요.
- **시작 월** / **시작 주** / **시작 요일** / **시작 시간**: 일광 절약 시간 적용을 시작할 월, 주, 요일, 시간을 설정하세요.
- **끝 월** / **끝 주** / **끝 요일** / **끝 시간**: 일광 절약 시간 적용을 종료할 월, 주, 요일, 시간을 설정하세요.

4. 설정을 저장하려면 **OK**를 누르세요.

장치 정보

모델명, 장치 ID, 시리얼 번호, 장치 및 펌웨어의 버전, 커널, MAC 주소를 확인할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **장치 정보**를 선택하세요. **모델명**, **장치 ID**, **시리얼 번호**, **HW**, **FW**, **커널**, **MAC**, **무선 MAC** 정보를 확인할 수 있습니다.



알아두기

- **MAC** 항목을 길게 터치하면 위조 얼굴 검출의 알고리즘 버전을 확인할 수 있는 **FAS_IR_SP** 정보가 표시됩니다. **FAS_IR_SP** 항목 터치 시, 전체 해시값을 팝업 메시지로 확인할 수 있습니다.
- **무선 MAC** 항목은 BS3-APWB 모델에서만 확인할 수 있습니다.

메모리 정보

메모리 사용 정보를 확인할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **메모리 정보**를 선택하세요. 장치의 메모리 사용 현황을 확인할 수 있습니다.



USB 메모리

장치에 USB 메모리를 연결하여 장치로 사용자 정보를 가져오거나 장치에서 로그 및 사용자 정보를 내보낼 수 있습니다. 펌웨어를 업그레이드할 수도 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **USB 메모리**를 선택하세요.
3. 원하는 항목을 선택한 뒤 설정을 변경하세요.



- **가져오기**: 연결된 USB 메모리에서 사용자 정보를 가져올 수 있습니다.
- **내보내기**: 연결된 USB 메모리에 내보낼 정보를 선택할 수 있습니다.
- **펌웨어 업그레이드**: 연결된 USB 메모리에 펌웨어 파일이 저장되어 있다면 펌웨어를 업그레이드할 수 있습니다.

주의

펌웨어 업그레이드 진행 중 전원 공급이 중단되지 않도록 주의하세요. 고장의 원인이 됩니다.

알아두기

- USB 메모리는 파일 시스템이 exFAT 형식인 제품을 사용할 것을 권장합니다. FAT32 형식인 USB 메모리를 사용하면 저장된 얼굴 데이터가 50,000개 이상일 경우 장치가 오작동할 수 있습니다.
- USB 메모리의 여유 공간을 확인하세요. 얼굴 데이터 100,000개 기준 15GB 이상의 여유 공간이 필요합니다.

보안 탬퍼

보안 탬퍼 사용 여부를 설정할 수 있습니다. 보안 탬퍼가 발생할 경우 전체 사용자, 전체 로그, 보안 키가 삭제됩니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치**를 선택하세요.
3. 탬퍼 발생 시 전체 사용자, 전체 로그, 보안 키가 삭제되도록 설정하려면 **보안 탬퍼** 설정을 켜세요.

RTSP

타사 비디오 관리 시스템(VMS)과 연결하여 제품의 비주얼 카메라를 통해 촬영된 영상을 모니터링 할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **RTSP**를 선택하세요.
3. 원하는 항목을 선택한 뒤 설정을 변경하세요.



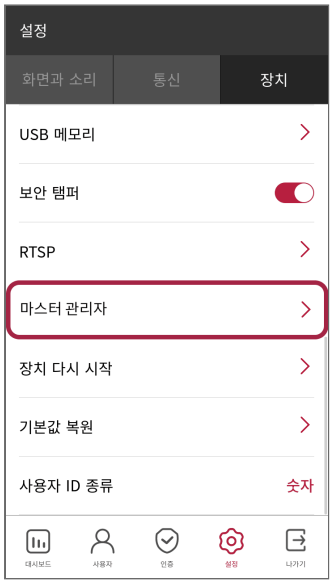
- **RTSP**: RTSP 활성화 여부를 설정할 수 있습니다. RTSP 설정을 켜면 **ID**, **비밀번호**, **RTSP 주소**, **RTSP 포트**, **RTSP 비디오 해상도**를 설정할 수 있습니다.
- **ID**: ID를 입력하세요. ID는 영문(대소문자 구분), 숫자, 일부 기호 `-` `_`를 조합하여 최대 32자까지 입력할 수 있습니다.
- **비밀번호**: 비밀번호를 입력하세요. 비밀번호는 영문(대문자 또는 소문자), 숫자를 조합하여 8~32자를 입력할 수 있습니다.
- **RTSP 주소**: RTSP 주소를 입력하세요.
- **RTSP 포트**: RTSP 포트 번호를 입력하세요.
- **RTSP 비디오 해상도**: 장치에서 송출되는 RTSP 영상의 해상도를 선택할 수 있습니다.

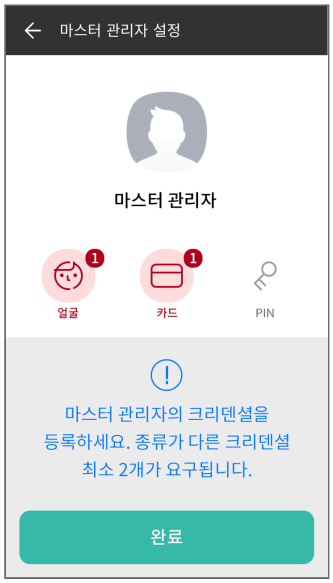
> **알아두기**
> 장치를 슬레이브 장치로 구성한 경우 RTSP 기능을 사용할 수 없습니다.

마스터 관리자 CE향 제품

마스터 관리자의 인증 수단을 변경할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **마스터 관리자**를 선택하세요.
3. 원하는 인증 수단을 설정하세요.





알아두기

- 최소 두 종류 이상의 크리덴셜을 등록해야 합니다.
- 이 기능은 펌웨어 v1.4.0 이상의 새 장치에서만 사용할 수 있습니다.

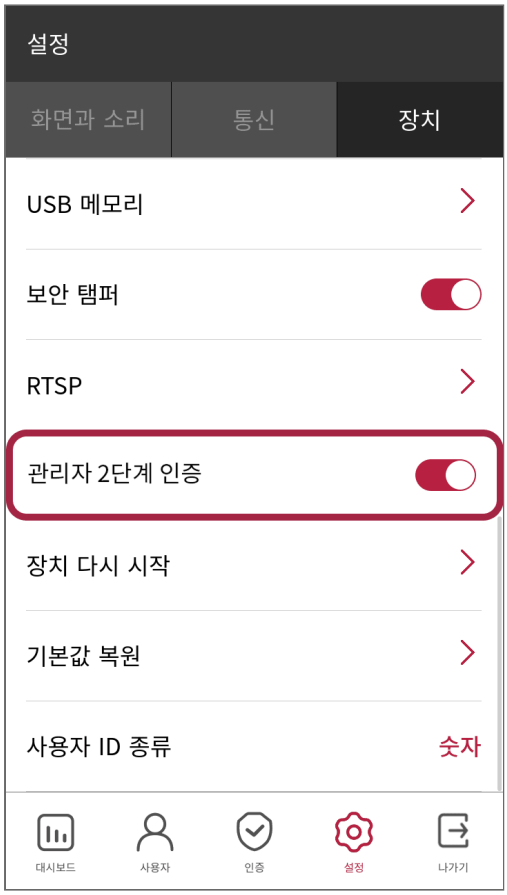
관리자 2단계 인증 CE향 제품

펌웨어를 업그레이드한 CE향 제품은 **마스터 관리자** 설정을 제공하지 않지만, **관리자 2단계 인증** 옵션을 통해 전체 관리자의 권한을 강화하여 장치의 보안을 향상시킬 수 있습니다.

알아두기

- 장치에 등록된 관리자의 크리덴셜이 두 종류 이상인 경우에만 **관리자 2단계 인증**을 활성화할 수 있습니다.
  - PIN은 단독 크리덴셜로 사용할 수 없으므로 ID + PIN 조합은 지원하지 않습니다.
- 업그레이드 장치는 펌웨어 다운그레이드를 할 수 없습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **관리자 2단계 인증**을 활성화하세요.

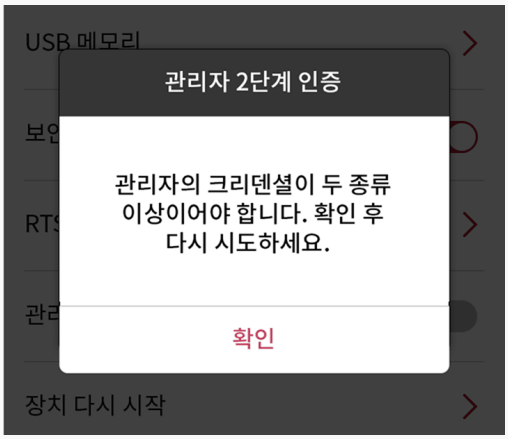


알아두기

모든 관리자에게 두 종류 이상의 크리덴셜이 등록되어 있지 않을 때 활성화 시 설정이 실패하며 에러 메시지가 표시됩니다.

모든 관리자에게 두 종류 이상의 크리덴셜을 등록한 다음 다시 시도하세요.

- PIN은 단독 크리덴셜로 사용할 수 없으므로 ID + PIN 조합은 지원하지 않습니다.



주의

관리자 2단계 인증을 활성화한 후 모든 관리자의 크리덴셜을 2종 미만으로 삭제하면, BioStar X(또는 BioStar 2)에 연결할 수 없는 상황에서 관리자 메뉴에 접근할 수 없게 됩니다. 따라서 관리자 크리덴셜을 삭제할 때는 각별한 주의가 필요합니다.

장치 다시 시작

장치를 다시 시작할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **장치 다시 시작**을 선택하세요.
3. 장치를 다시 시작하려면 **확인**을 누르세요. 이전 화면으로 돌아가려면 **취소**를 누르세요.

기본값 복원

장치 설정, 네트워크 설정, 사용자 권한 등이 초기화됩니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **기본값 복원**을 선택하세요.
   - **전체 설정**: 장치에 저장된 모든 설정을 초기화합니다. 장치 설정을 모두 초기화하려면 **확인**을 누르세요. 이전 화면으로 돌아가려면 **취소**를 누르세요.
   - **네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 네트워크 설정을 제외한 모든 설정을 초기화하려면 **확인**을 누르세요. 이전 화면으로 돌아가려면 **취소**를 누르세요.
   - **공장 초기화**: 장치에 저장된 모든 정보와 루트 인증서를 삭제하고 설정을 초기화합니다.
   - **루트 인증서 삭제**: 장치에 저장된 루트 인증서를 삭제합니다.
3. **기본값 복원**을 실행할 경우 장치가 다시 시작됩니다.

> **알아두기**
>
> - 초기화를 실행할 경우 사용자 권한도 같이 초기화 됩니다. 초기화를 실행한 뒤 반드시 사용자 권한을 다시 설정하세요.
> - 초기화를 실행해도 언어 설정은 변경되지 않습니다.
> - **공장 초기화** 메뉴는 장치에 루트 인증서가 저장되었을 때 사용할 수 있습니다.
> - **루트 인증서 삭제** 메뉴는 장치에 루트 인증서가 저장되어 있고 전체 관리자가 지정되었을 때 사용할 수 있습니다.

사용자 ID 종류

장치에 등록할 사용자 ID의 형태를 선택할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **설정** → **장치** → **사용자 ID 종류**를 선택하세요.
   - **숫자**: 사용자 ID를 숫자로만 입력할 수 있습니다.
   - **영숫자**: 사용자 ID를 영숫자와 일부 특수 기호(`_` `-` `.`)를 조합하여 입력할 수 있습니다.
3. 원하는 항목을 선택하세요.

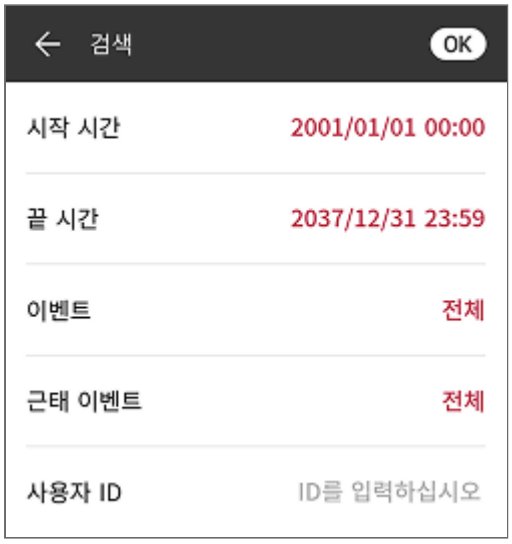
이벤트 로그

장치에서 발생한 이벤트 기록을 확인하는 방법을 설명합니다.

이벤트 로그 검색

조건을 설정하여 로그를 검색할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **대시보드**에서 를 선택하세요. 전체 이벤트 로그 목록이 표시됩니다.
3. 특정 이벤트를 검색하려면 을 누른 뒤 원하는 항목을 변경하세요.



4. 검색 조건을 설정하고 **OK**를 누르면 조건에 맞는 로그가 화면에 나타납니다.

전체 로그 삭제

저장된 로그를 모두 삭제할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **대시보드**에서 를 선택하세요. 전체 이벤트 로그 목록이 표시됩니다.
3. 전체 로그를 삭제하려면 을 선택한 뒤 **확인**을 누르세요. 이전 화면으로 돌아가려면 **취소**를 누르세요.

로그 사용량 보기

로그 사용 현황을 확인할 수 있습니다.

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **대시보드**에서 → 을 누르세요. 장치의 이벤트 로그 및 이미지 로그 사용량을 확인할 수 있습니다.


이벤트 로그 사용량
전체 이벤트 로그
71 / 5,000,000
전체 이미지 로그
777 / 50,000

문제 해결

장치 사용 중 발생할 수 있는 문제에 대한 점검 사항과 기본 해결 방법을 제공합니다.

고장 신고 전 확인 사항

장치를 사용하는 도중 발생할 수 있는 예기치 않은 문제를 해결하는 데 도움이 되는 정보를 제공합니다.

전원

Q. 전원이 공급되고 있으나 작동하지 않습니다.

- 단말기와 브래킷이 떨어져 있으면 탬퍼 스위치에 의해 작동하지 않을 수도 있습니다.
- 어댑터 또는 전원 연결 케이블을 확인하세요.

PIN

Q. PIN을 분실했습니다.

- 일반 사용자의 PIN은 관리자에게 요청한 뒤 다시 입력하세요.
- 관리자 PIN 분실 시 설치 업체에 문의하세요.

Q. PIN을 입력한 뒤 OK 버튼을 눌러도 잠긴 문을 열 수 없습니다.

- 등록한 PIN을 정상적으로 입력하였는지 확인하세요.
- 최근에 PIN을 변경하지 않았는지 확인하세요.
- PIN을 알 수 없는 경우 관리자에게 요청한 뒤 다시 입력하세요.

얼굴

Q. 등록은 되었으나 얼굴 인증이 잘 되지 않고 오류가 많이 납니다.

- 얼굴 등록 시 주의 사항을 확인한 뒤 얼굴을 다시 등록하세요.
- 등록된 얼굴 개수가 많다면 **매칭 대기 시간**을 변경한 뒤 다시 시도하세요.

Q. 갑자기 얼굴 인증이 되지 않습니다.

- 얼굴 인증 시 주의 사항을 확인한 뒤 다시 시도하세요.

Q. 마스크 검출 기능을 사용으로 설정하였으나 마스크 착용 시 얼굴 인증이 잘 되지 않고 오류가 많이 납니다.

- 마스크를 코끝까지 내리고 얼굴을 2회 인증한 뒤 다시 코를 덮고 얼굴 인증을 시도하세요. 문제가 지속될 경우 설치 업체에 문의하세요.

문 잠금

Q. 문을 닫아도 잠금 장치는 잠기지 않습니다.

- 전기 잠금 장치의 이상일 수 있습니다. 설치 업체를 통해 점검을 받으세요.

시간

Q. 갑자기 시간이 맞지 않습니다.

- 장치에는 내장 배터리가 있으나, 오랫동안 전원이 공급되지 않으면 내장 배터리가 방전되어 시간이 달라질 수 있습니다. 날짜와 시간 메뉴를 참고하여 시간을 수정할 수 있습니다.

관리자 접속

Q. 관리자 PIN을 분실하여 관리자 모드에 진입할 수 없습니다.

- 장치는 관리자가 출입 허용 권한을 부여하기 때문에 관리자만 메뉴에 진입할 수 있습니다.
- 관리자 PIN 분실 시 설치 업체에 문의하세요.

마스터 관리자 (CE향 제품)

Q. 기존 장치에서 펌웨어를 업그레이드하면 마스터 관리자 설정이 지원되나요?

- **마스터 관리자** 기능은 **CE 마크가 있는 라벨이 부착된 CE향 제품에서만 지원**됩니다. 제품 뒷면 라벨 스티커를 통해 **CE향 / 글로벌향 (Non-CE)** 제품을 식별할 수 있습니다. 자세한 내용은 마스터 관리자 지원 정책을 참조하세요.

제품 사양

제품에 대한 크기, 기능, 성능 등 주요 사양 정보를 제공합니다.

크리덴셜

바이오 인식	**얼굴** • **인증 거리[1]:0.3 ~ 1.0 m** • **인증 높이:1.4 ~ 1.9 m** • **매칭 속도:0.2초 이내** • **위조 얼굴 검출:지원**	
RF 카드	**BS3-DB**	**125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa**
	BS3-APWB	**125kHz EM, HID Prox & 13.56MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa, iCLASS SE/SR/Seos**
RF 인식 거리[2]	**EM/HID Prox/MIFARE/DESFire/HID iCLASS: 30 mm, FeliCa: 15 mm**	
모바일	**NFC, BLE**	
스크램블 키패드(PIN)	**지원**	
QR/바코드[3]	**지원[4]**	
QR/바코드 인식 권장 거리[5]	**30 ~ 40 cm**	

일반

모델명	**BS3-DB, BS3-APWB**
CPU	**1.5 GHz Quad Core**
메모리	**32 GB Flash + 4 GB RAM**

크립토 칩	**지원**	
디스플레이	**5.5" IPS 컬러 LCD**	
화면 해상도	**720 x 1280 픽셀**	
소리	**16 bit**	
동작 온도	**-20 °C ~ 50 °C**	
보관 온도	**-40 °C ~ 70 °C**	
동작 습도	**0 % ~ 80 %, 비응축**	
보관 습도	**0 % ~ 90 %, 비응축**	
카메라	• **적외선: 2M 픽셀** • **비주얼: 2M 픽셀**	
크기 (W x H x D)	**장치**	**82.5 x 171 x 23.4 (mm)**
	브래킷	**72.9 x 164 (mm)**
무게	**장치**	• **BS3-DB: 370 g** • **BS3-APWB: 380 g**
	브래킷	**90 g (와셔 및 볼트 포함)**
IP 등급	**IP65**	
IK 등급	**IK06**	
인증	**CE, UKCA, KC, FCC, IC, RCM, BIS, SIG, RoHS, REACH, WEEE, MIC, TELEC**	

저장 용량

최대 사용자 수	**100,000**[6)]

최대 크리덴셜 수 (1:N)	**얼굴: 50,000**
최대 크리덴셜 수 (1:1)	• **얼굴: 100,000** • **카드: 100,000** • **PIN: 100,000**
최대 텍스트 로그 수	**5,000,000**
최대 이미지 로그 수	**50,000**

인터페이스

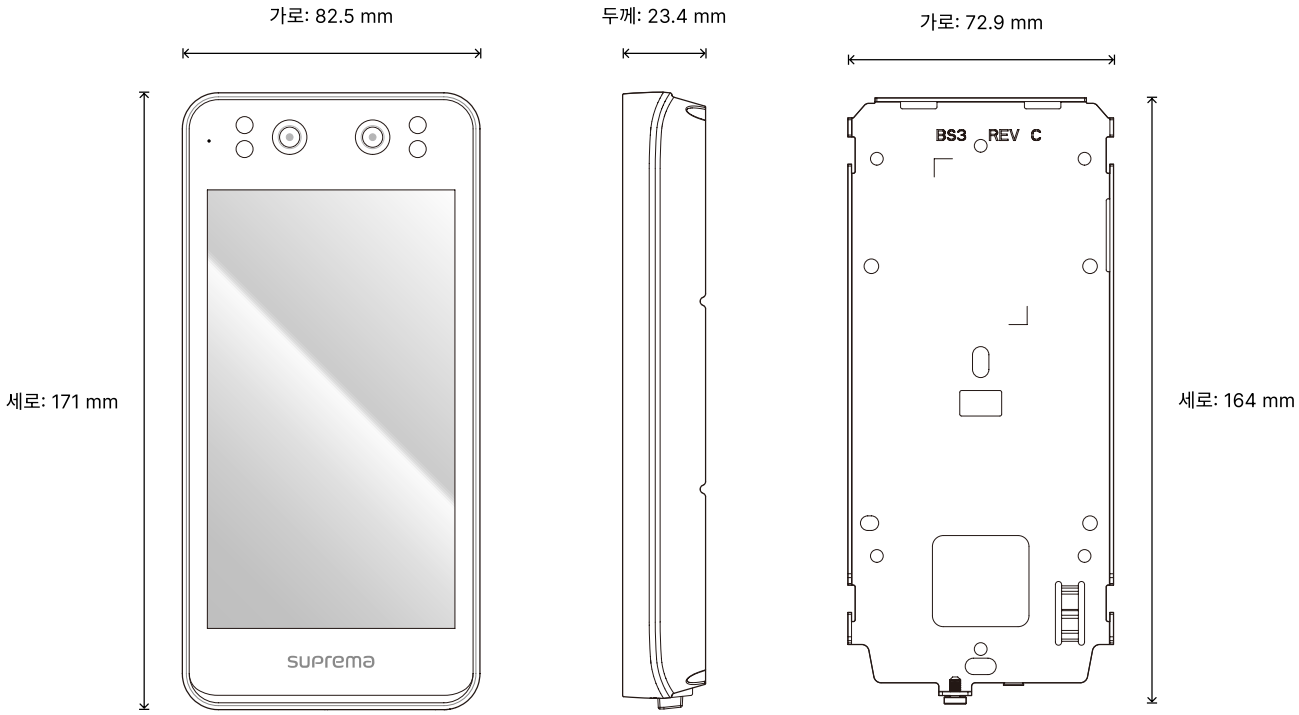
이더넷	**지원 (10/100/1000 Mbps, 자동 MDI/MDI-X)**	
Wi-Fi	**BS3-DB**	**미지원**
	BS3-APWB	**지원 (802.11 b/ g/ n 2.4 GHz)**
네트워크 프로토콜	**TCP, UDP**	
RS-485	**1채널 마스터/슬레이브 (선택 가능)**	
RS-485 통신 프로토콜	**OSDP V2 호환**	
Wiegand	**1채널 입력, 1채널 출력**	
Input	**입력 3채널**	
릴레이	**1개**	
PoE+[7)]	**BS3-DB**	**미지원**
	BS3-APWB	**지원 (IEEE 802.3at 호환)**
인터폰	**지원**	
RTSP	**지원**	

USB	**USB 2.0 (Host)**
USB 확장 포트	**지원**
탬퍼	**지원**

전기 규격

전원	**12 Vdc**	**전류: 최대 1 A**
	24 Vdc	**전류: 최대 0.7 A**
스위치 입력 VIH	• **최소: 3 V** • **최대: 5 V**	
스위치 입력 VIL	**최대: 1 V**	
스위치 풀업 저항	**4.7 kΩ (입력 단자는 4.7 kΩ으로 풀업되어 있습니다.)**	
Wiegand 출력 VOH	**4.8 V 이상**	
Wiegand 출력 VOL	**0.2 V 이하**	
Wiegand 출력 풀업 저항	**1 kΩ으로 내부 풀업**	
릴레이	• **2 A @ 30 VDC Resistive load** • **1 A @ 30 VDC Inductive load**	

크기 및 무게



무게
- BS3-DB: 370 g
- BS3-APWB: 380 g

무게: 90 g (와셔 및 볼트 포함)

---

1) 표기된 최소 얼굴 인증 거리는 제품의 기본 설정이며, 권장하는 얼굴 인증 거리는 0.6~1.0 m입니다.

2) RF 인식 거리는 설치 환경에 따라 다를 수 있습니다.

3) 최대 32개의 ASCII 코드 문자열로 구성된 QR/바코드를 지원합니다.

4) 별도의 장치 라이선스가 필요합니다.

5) 표기된 QR/바코드 인식 거리는 권장 거리이며, 실제 인식 가능 거리는 QR/바코드 크기 및 설치 환경에 따라 달라질 수 있습니다.

6) 크리덴셜 없이 등록된 사용자 기준입니다.

7) PoE+ (IEEE 802.3at, 30 W) 또는 PoE++ (IEEE 802.3bt, 60~100 W) 전원이 필요합니다. 표준 PoE (IEEE 802.3af, 15.4 W)는 지원하지 않습니다. 표준 PoE를 사용할 경우 장치가 불안정하게 동작하거나 영구적으로 손상될 수 있습니다. 장치를 연결하기 전에 네트워크 스위치 또는 PoE 인젝터가 PoE+ 또는 PoE++를 지원하는지 반드시 확인하세요.

알아두기

- 제품 사양은 성능 개선을 위해 예고 없이 변경될 수 있습니다.
- 이 제품이 마스터 장치일 때 지문 센서가 있는 장치를 슬레이브로 연결하면 슬레이브 장치를 사용하여 지문을 인증할 수 있습니다.
  - 최대 지문 크리덴셜 수 (1:N): 100,000
  - 최대 지문 크리덴셜 수 (1:1): 100,000

규제 인증 정보

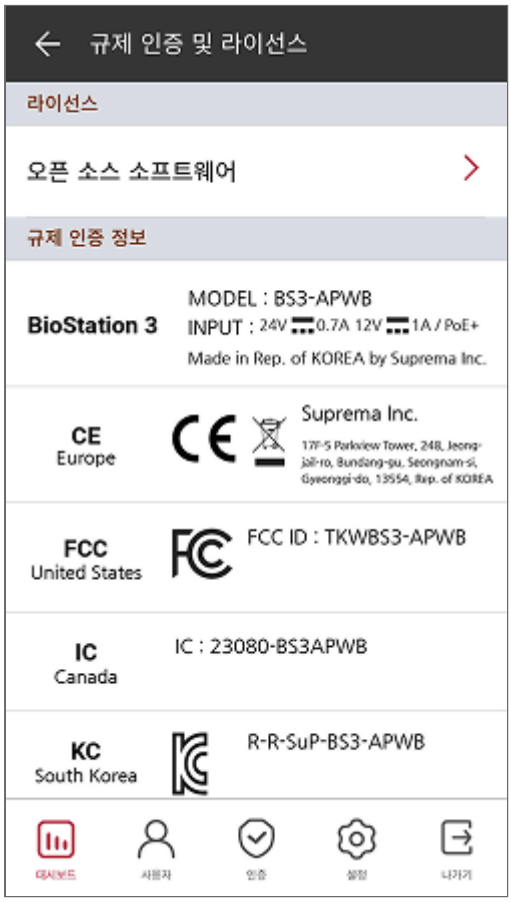
제품이 준수하는 규제 및 인증 관련 정보를 제공합니다.

규제 인증 및 라이선스

라이선스, 규제 인증 및 규정 준수 마크를 제품에서 확인할 수 있습니다.

- CE / FCC / IC / KC / UKCA / RCM / MIC / TELEC

1. 을 누른 뒤 관리자 권한 인증 수단으로 인증하세요.
2. **대시보드** 우측 상단의 를 터치하면 **규제 인증 및 라이선스**를 확인할 수 있습니다.



알아두기

관리자가 지정되어 있지 않을 경우 을 누르면 **대시보드** 화면이 나타납니다.

FCC 준수 정보

이 기기는 FCC 규제의 Part 15를 준수합니다.

작동은 다음의 두 조건을 따릅니다.

1. 이 기기는 유해한 간섭을 발생시키지 않습니다.
2. 이 기기는 원치 않는 작동을 일으키는 간섭을 포함한 어떠한 간섭도 수용합니다.

알아두기

이 기기는 Class A 디지털 기기에 대한 제한 사항을 준수하여 테스트를 거쳤고 FCC규제의 Part 15에 적합하다는 것을 검증받았습니다. 이러한 제한은 장비가 상업적 환경에서 작동될 때 유해한 간섭으로부터 합리적인 보호를 제공하기 위해 설계되었습니다. 이 장비는 무선 주파수 에너지를 생성, 사용 및 방사하므로 지침에 따라 설치하여 사용하지 않을 경우 무선 통신에서 유해한 간섭을 일으킬 수 있습니다. 주거 지역에서 이 장비를 작동하면 유해한 간섭이 발생할 수 있으며 이 경우 사용자는 자신의 비용으로 간섭을 수정해야 합니다.

규정 준수 책임이 있는 당사자가 명시적으로 승인하지 않은 제품 변경 또는 수정은 이 제품을 작동할 수 있는 사용자의 권한을 무효화할 수 있습니다.

이 송신기는 다른 안테나 또는 송신기와 함께 배치하거나 작동해서는 안 됩니다.

이 기기는 통제되지 않은 환경에 대해 규정된 FCC 방사 노출 제한을 준수합니다. 사용자(또는 근처의 다른 사람)와 제품의 안테나간에 최소 20cm의 거리를 유지하세요. 이 기기와 기기의 안테나를 다른 안테나 또는 RF 전송 장치와 함께 설치하거나 작동하지 마세요.

IC 정보

이 기기는 Industry Canada의 라이선스 면제 RSS를 준수합니다.

작동은 다음의 두 조건을 따릅니다.

1. 이 기기는 간섭을 발생시키지 않습니다.
2. 이 기기는 원치 않는 작동을 일으키는 간섭을 포함한 어떠한 간섭도 수용합니다.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence.

L’exploitation est autorisée aux deux conditions suivantes :

1. l’appareil ne doit pas produire de brouillage ;
2. l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

유럽 연합 적합성 선언 (CE)

이 제품은 라디오 및 통신 단말기 장치 지침(RED) 2014/53/EU의 규정에 따라 CE 마크를 제공합니다.

㈜슈프리마는 이 문서에서 설명하는 장치에 유럽 연합 라디오 및 통신 단말기 장치 지침(RED) 2014/53/EU을 준수하는 CE 마크가 있음을 선언합니다. 이 장치는 지침에 따라 클래스 1 라디오 장치입니다.

- Bluetooth 송신 전력: -0.1 dBm
- Bluetooth 주파수: 2402~2480 MHz
- NFC 주파수: 13.56 MHz
- RFID 주파수: 13.56 MHz + 125 kHz

더 자세한 내용은 아래 연락처로 연락하세요.

㈜슈프리마

주소: 경기도 성남시 분당구 정자일로 248 (정자동 6) 파크뷰타워 17층

전화: 1522-4507(영업 문의: 1번, 고객 지원: 2) / 팩스: 031-783-4517

부록

제품에 포함된 법적 고지 사항을 수록합니다.

면책 조항

- 이 웹 사이트는 슈프리마 제품과 관련된 정보를 제공합니다.
- 이 웹 사이트는 슈프리마의 제품 사용 및 판매 계약에 포함된 슈프리마 제품에만 사용될 수 있습니다. 이 웹 사이트는 명시적, 묵시적, 금반언의 원칙 또는 어떠한 방식으로도 지식재산권에 대한 라이선스를 부여하지 않습니다.
- 귀하와 슈프리마 간의 계약에 명시된 경우를 제외하고, 슈프리마는 어떠한 책임도 지지 않으며 슈프리마는 특정 목적에의 적합성, 상품성 또는 비침해와 관련된 모든 명시적, 묵시적 보증을 부인합니다.
- 모든 보증이 무효화되는 경우는 다음과 같습니다: 슈프리마 제품이 1) 잘못 설치된 경우 또는 하드웨어의 일련번호, 보증정보 또는 품질 보증 스티커가 변경 또는 제거된 경우; 2) 슈프리마가 허용한 방법 이외의 방법으로 사용한 경우; 3)슈프리마 또는 슈프리마가 승인한 당사자 이외의 당사자에 의하여 변경, 수정 또는 수리된 경우; 또는 4) 부적절한 환경에서 작동되거나 유지된 경우.
- 슈프리마 제품은 제품의 고장이 부상이나 사망사고로 이어질 수 있는 의료, 인명 구조, 생명 유지와 같은 용도로 사용하도록 만들어진 것은 아닙니다. 만약 귀하께서 이러한 용도로 슈프리마 제품을 구매하거나 사용할 경우, 이로 인한 부상 또는 사망으로 발생하는 모든 청구, 비용, 손실, 지출 및 합리적인 변호사 비용으로부터 슈프리마와 그 구성원, 자회사, 계열사 및 공급사를 면책시켜야 합니다. 제품 디자인이나 제조에 슈프리마의 과실이 있다고 주장되는 경우에도 마찬가지입니다.
- 슈프리마는 신뢰성, 기능 또는 디자인을 개선하기 위하여 언제든지 예고없이 사양과 제품 설명을 변경할 권리를 가지고 있습니다.
- 개인정보는 제품 사용시 인증메시지 및 기타 관련 정보의 형태로 슈프리마 제품에 저장될 수 있습니다. 슈프리마는 슈프리마가 직접 통제할 수 없는 또는 관련 계약에 명시된 슈프리마 제품에 저장되는 개인정보를 비롯한 어떠한 정보에 대해서도 책임지지 않습니다. 개인정보를 포함하여 저장된 정보를 사용하는 경우 제품 사용자는 관련 법률 (예를 들어, GDPR)을 준수하고 적절한 취급과 처리를 해야 할 책임이 있습니다.
- 귀하는 어떠한 기능의 부재 또는 특징, "reserved" 또는 "undefined"로 표시된 설명에 의존해서는 안됩니다. 슈프리마는 이를 추후에 정의할 수 있으며 추후에 가한 변경이 현재와 상충된다고 하더라도 슈프리마는 책임지지 않습니다.
- 이 사이트에 명시적으로 기재되어 있는 경우를 제외하고, 슈프리마는 법률이 허용하는 최대 범위 내에서 "있는 그대로" 판매됩니다.
- 제품을 주문하기 전에 가까운 슈프리마 영업소 또는 대리점에 문의하여 최신 사양을 확인하세요.

저작권 공지

이 웹 사이트의 저작권은 슈프리마에게 있습니다. 다른 제품 이름, 상표, 등록된 상표에 대한 권리는 각각 그것을 소유한 개인이나 단체에게 있습니다.

오픈 소스 라이선스

- 이 제품의 소프트웨어는 Linux 커널 4.x 버전을 수정하여 제작되었으며, Linux 커널의 라이선스는 GPL을 따르고 있습니다. GPL 라이선스에 대한 자세한 내용은 GNU General Public License에서 확인할 수 있습니다.
- 이 제품에 포함된 glibc 라이브러리는 LGPL을 따릅니다. LGPL 라이선스에 대한 자세한 내용은 GNU Lesser General Public License에서 확인할 수 있습니다.
- 이 제품에 포함된 OpenSSL은 OpenSSL 라이선스와 Original SSLeay 라이선스를 따릅니다. OpenSSL 라이선스와 Original SSLeay 라이선스에 대한 자세한 내용은 OpenSSL License와 Original SSLeay License에서 확인할 수 있습니다.
- 이 제품에 포함된 Linux 커널 4.x 기반으로 수정된 소스와 glibc 라이브러리는 슈프리마 기술 지원팀으로 문의하여 다운로드 받을 수 있습니다.

(주) 슈프리마
13554 경기도 성남시 분당구 정자일로 248 파크뷰타워 17층
영업 문의 1522 4507(1번)　korea@suprema.co.kr | 고객지원 1522 4507(2번)　cs@suprema.co.kr

© 2026 Suprema Inc. 이 문서에 표기된 슈프리마, 제품명, 번호는 슈프리마의 등록 상표입니다. 모든 회사명과 제품명은 해당 회사의 상표이거나 등록 상표입니다. 제품 외관, 제조 상태 및 사양은 사전 통지 없이 변경될 수 있습니다.