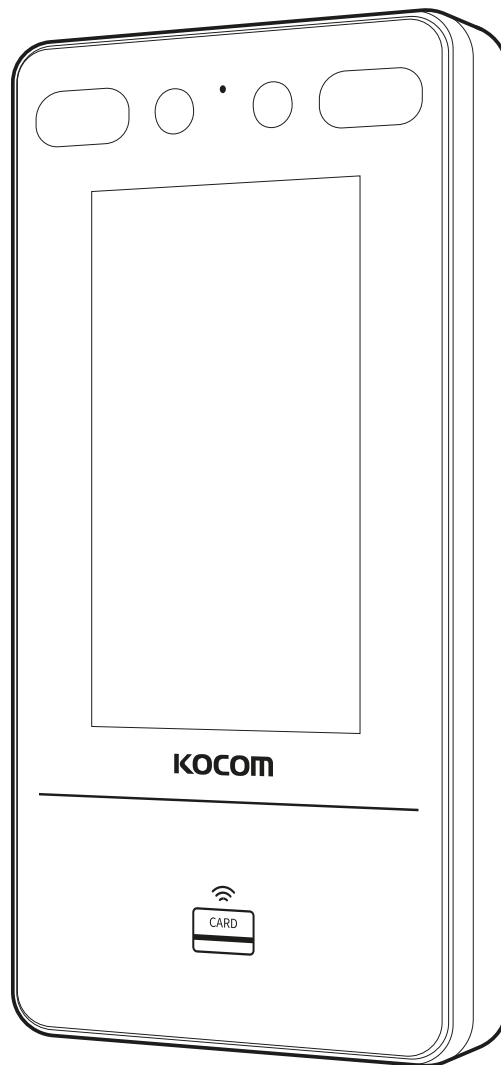


얼굴인식 출입통제기

KAF-W1000 사용자 매뉴얼



※안전한 사용을 위하여 제품 상세매뉴얼의 주의사항을 반드시 읽고 사용해 주시기 바랍니다.
※본 매뉴얼의 세부 조작 사항은 추후 제품의 기능 및 편리성 개선 여부에 따라 변경될 수 있습니다.

목차

0. 안전을 위한 주의사항 01

1. 개요 01

- 1.1 개요 01
- 1.2 특징 01

2. 외형 01

3. 설치 01

- 3.1 설치환경 01
- 3.2 매립 박스와 함께 설치 01
- 3.3 표면 장착 01
- 3.4 브래킷으로 장착 01
 - 3.4.1 브래킷 장착 전 준비사항 01
 - 3.4.2 장착 브래킷 01
- 3.5 실린더 브래킷으로 장착 01
 - 3.5.1 브래킷 장착 전 준비사항 01
 - 3.5.2 실린더 브래킷 마운팅 01

4. 배선 01

- 4.1 단자 설명 01
- 4.2 유선 일반 장치 01
- 4.3 유선 보안 도어 제어 장치 01
- 4.4 화재 시스템 연동 01
 - 4.4.1 전원 차단 시 문 열림 결선도 01
 - 4.4.2 전원 차단 시 도어 잠금 결선도 01

5. 초기 사용 등록(활성화) 01

- 5.1 장비에서의 초기 사용 등록 01
- 5.2 웹 브라우저를 통한 활성화 01
- 5.3 SADP를 통한 활성화 01
- 5.4 Guarding Vision Client 소프트웨어를 통한 장치 활성화 01

6. 사용자 환경 설정 01

- 6.1 언어 선택 01
- 6.2 애플리케이션 모드 설정 01
- 6.3 네트워크 설정 01
- 6.4 플랫폼에 대한 액세스 01
- 6.5 모바일 클라이언트에 연결 01
- 6.6 개인 정보 설정 01
- 6.7 관리자 설정 01

7. 기본 동작 01

- 7.1 로그인 01
 - 7.1.1 관리자 로그인 01
 - 7.1.2 활성화 비밀번호로 로그인 01
- 7.2 통신 설정 01
 - 7.2.1 유선 네트워크 설정 01
 - 7.2.2 Wi-Fi 설정 01
 - 7.2.3 RS-485 설정 01
 - 7.2.4 Wiegand 설정 01
 - 7.2.5 ISUP 설정 01
 - 7.2.6 플랫폼 액세스 01
- 7.3 사용자 관리 01
 - 7.3.1 사용자 추가 01
 - 7.3.2 얼굴 사진 추가 01
 - 7.3.4 카드 추가 01
 - 7.3.5 PIN 코드 보기 01
 - 7.3.6 인증 모드 설정 01
 - 7.3.7 사용자 검색 및 편집 01
- 7.4 데이터 관리 01
 - 7.4.1 데이터 삭제 01
 - 7.4.2 데이터 가져오기 01
 - 7.4.3 데이터 내보내기 01
- 7.5 인증 01
 - 7.5.1 단일 인증 01
 - 7.5.2 멀티 인증 01
- 7.6 기본 설정 01
- 7.7 생체 설정 01
- 7.8 액세스 제어 설정 01
- 7.9 근퇴(체크인/아웃) 설정 01
 - 7.9.1 장치를 통한 출석 모드 비활성화 01
 - 7.9.2 장치를 통한 수동 근태 설정 01
 - 7.9.3 장치를 통한 자동 출결 설정 01
 - 7.9.4 장치를 통한 수동 및 자동 출석 설정 01
- 7.10 단축키 설정 01
- 7.11 시스템 유지보수 01

8. 모바일 브라우저를 통한 장치 구성 01

- 8.1 로그인 01
- 8.2 검색 이벤트 01
- 8.3 사용자 관리 01
- 8.4 설정 01
 - 8.4.1 장치 정보 보기 01
 - 8.4.2 시간 설정 01
 - 8.4.3 오픈 소스 소프트웨어 라이선스 보기 01
 - 8.4.4 네트워크 설정 01
 - 8.4.5 일반 설정 01
 - 8.4.6 얼굴 설정 01
 - 8.4.7 비디오 인터콤 설정 01
 - 8.4.8 액세스 제어 설정 01

9. 웹 브라우저를 통한 작동 01

9.1 로그인	01
9.2 라이브 뷰	01
9.3 사용자 관리	01
9.4 이벤트 로그 검색하기	01
9.5 설정	01
9.5.1 로컬 설정	01
9.5.2 장치 정보 보기	01
9.5.3 시간 설정	01
9.5.4 서머타임 설정	01
9.5.5 오픈 소스 소프트웨어 라이선스 보기	01
9.5.6 업그레이드 및 유지보수	01
9.5.7 로그 쿼리	01
9.5.8 보안 모드 설정	01
9.5.9 인증서 관리	01
9.5.10 관리자 비밀번호 변경	01
9.5.11 감시(방법)/감시(방법) 해제 정보 보기	01
9.5.12 네트워크 설정	01
9.5.13 비디오 및 오디오 설정	01
9.5.14 오디오 콘텐츠 사용자 지정	01
9.5.15 이미지 설정	01
9.5.17 근태 설정	01
9.5.18 일반 설정	01
9.5.19 비디오 인터콤 설정	01
9.5.20 액세스 제어 설정	01
9.5.21 생체(얼굴) 설정	01
9.5.22 공지 게시 설정	01

10. 클라이언트 소프트웨어 구성 01

10.1 클라이언트 소프트웨어의 구성 흐름	01
10.2 장치 관리	01
10.2.1 장치 추가	01
10.2.2 장치 암호 재설정	01
10.2.3 추가된 장치 관리	01
10.3 그룹 관리	01
10.3.1 그룹 추가	01
10.3.2 그룹으로 리소스 가져오기	01
10.4 개인 관리	01
10.4.1 조직 추가	01
10.4.2 개인 식별 정보 가져오기 및 내보내기	01
10.4.3 출입 통제 장치에서 개인 정보 가져오기	01
10.4.4 일괄적으로 사람에게 카드 발급	01
10.4.5 성적표 분실	01
10.4.6 카드 발급 매개변수 설정	01
10.5 일정 및 템플릿 구성	01
10.5.1 휴일 추가	01
10.5.2 템플릿 추가	01
10.6 사람에게 액세스 권한을 할당하도록 액세스 그룹 설정	01
10.7 고급 기능 구성	01
10.7.1 장치 매개변수 구성	01
10.7.2 장치 매개변수 구성	01

10. 클라이언트 소프트웨어 구성 01

10.8 도어 제어	01
10.8.1 컨트롤 도어 상태	01
10.8.2 실시간 접속기록 확인	01

A. 지문 스캔 팁 01

B. 얼굴 사진 수집/비교 시 팁 01

C. 설치 환경에 대한 팁 01

D. 차원 01

안전을 위한 주의사항

- 다 읽으신 후에는 언제든지 볼 수 있는 곳에 보관하여 주십시오. • 바르게 설치하기 위해서는 꼭 읽어 주시고 사양에 맞게 설치하십시오.
- 잘 읽으신 후 올바르게 사용하시고 문의 사항은 A/S 센터로 문의하십시오.

기호



경고: 위반할 경우 사망 또는 심각한 부상을 초래하거나 초래할 수 있는 위험한 상황을 나타냅니다.



주의: 위반할 경우 장비 손상, 데이터 손실, 성능 저하 또는 예기치 않은 결과를 초래할 수 있는 잠재적으로 위험한 상황을 나타냅니다.



안내: 제품을 사용할 때 강조하거나 보완하기 위한 추가 정보를 제공합니다.



경고

- 제품을 사용함에 있어서는 국가 및 지역의 전기안전법규를 엄격히 준수하여야 합니다.
- 하나의 전원 어댑터에 여러 장치를 연결하지 마십시오. 어댑터 과부하로 인해 과열 또는 화재 위험이 있습니다.
- 기기에서 연기, 냄새, 소음이 나면 즉시 전원을 끄고 전원플러그를 뽑은 후 서비스센터로 연락하세요.
- 소켓 콘센트는 장비 근처에 설치하고 쉽게 접근할 수 있어야 합니다.
- 욕실 안이나 세탁기의 가까운 곳 습기, 먼지가 많은 장소에 설치하지 마십시오. 화재, 감전의 원인이 됩니다.
- 조리대, 가습기, 히터 등의 가까운 곳 유열, 열기, 습기가 있는 곳을 피하여 설치하거나 가까이 두지 마십시오. 화재, 감전의 원인이 됩니다.
- 먼지, 금속 분, 유화수소가스 등 유해가스가 있는 장소에는 설치하지 마십시오. 화재, 감전 및 누전의 원인이 됩니다.
- 물이나 약품 등이 있는 장소에는 설치하지 마십시오. 화재, 감전의 원인이 됩니다.
- 무거운 것을 올려놓거나 가열하거나 잡아당기면 파손의 원인이 됩니다.
- 전원코드에 상처를 나거나 파손하거나 가공하지 마십시오. 화재, 감전의 원인이 됩니다.
- 플러그를 뽑 때에는 전원코드를 잡아당기지 마십시오.
- 전원코드를 열기구 가까운 곳에 두지 마십시오. 코드의 피복이 손상되어 화재, 감전의 원인이 됩니다.
- 코드의 손상으로 화재, 감전의 원인이 됩니다. 꼭 플러그를 잡고 빼주세요.
- 젖은 손으로 플러그를 빼지 마십시오. 감전의 원인이 됩니다.
- 본체 전원 단자를 지정된 기기 이외의 다른 기기 전원으로 사용하지 마십시오. 화재, 감전, 누전의 원인이 됩니다.
- 방수성의 성능 표시가 없는 기기는 누수가 있는 장소에 설치하지 마십시오. 전원을 넣은 채 공사를 하지 마십시오. 감전의 원인이 됩니다.
- A/C 개폐기 설치 시 누전, 감전의 요인(철대문 또는 전기가 통하는)을 제거 후 시공하십시오. 전원을 반드시 차단한 후에 A/S 또는 설치를 하십시오.
- 기존 배선을 사용할 경우는 적합한지 확인하시고 설치하여 주십시오. 화재, 감전의 원인이 됩니다.
- 지정된 배선 재질을 사용하여 배선을 실시해 주십시오. 지정된 선재 외에 공사를 행하면 화재의 원인이 됩니다.
- 전원선은 지정된 방법으로 확실하게 접속하시고 반드시 접지하십시오. 화재의 원인이 됩니다.
- 시스템을 구성하는 경우는 지정된 기기 이외의 기기를 접속하지 마십시오. 화재의 원인이 됩니다.
- 전원코드가 파손이 되면(심선의 노출, 단선 등) 반드시 교체하십시오. 화재나 감전의 원인이 됩니다.
- 통화가 되지 않는다, 화상이 나오지 않는다, 호출이 되지 않는다, 이상음이 나온다, 등의 기기상에 이상이 생기면 바로 플러그를 콘센트에서 빼거나 플러그가 없는 경우 전원 차단기를 내리고 판매점 또는 A/S 센터에 수리를 의뢰해 주십시오. 그대로 사용하면 화재, 감전의 원인이 됩니다.
- 만일 이물질이 들어간 경우는 먼저 플러그를 콘센트에서 빼고, 플러그가 없는 경우는 전원 차단기를 내리거나 판매점 또는 A/S 센터에 수리를 의뢰해 주십시오. 그대로 사용하면 화재, 감전의 원인이 됩니다.
- 만일 연기가 나오고 이상한 냄새가 날 경우 그대로 사용하면 화재, 감전의 원인이 됩니다. 바로 플러그를 콘센트에서 빼거나 플러그가 없는 경우는 전원 차단기를 내리거나 판매점 또는 A/S 센터에 수리를 의뢰해 주십시오. 고객께서 직접 수리하는 경우 위험 하오니 절대 직접 수리를 금합니다.
- 직사광선을 피하여 주시고 누수 등이 없는 곳, 가능한 먼지가 적고 고온이 발생하지 않는 장소에 보관해 주십시오. 기기의 열화에 의한 화재, 감전의 원인이 됩니다.



경고

- 비밀번호는 타인이 알지 못하도록 주의하여 관리하십시오. 같은 비밀번호를 장기간 사용하면 주변인 엿보기 등으로 인해 유추될 수 있으니, 주기적으로 비밀번호를 변경하여 사용하시기 바랍니다.
- 비밀번호 설정 시 1234, 0000 등 유추하기 쉬운 암호를 사용하지 마십시오.
- 기기와 모바일기기 연동 시 인증번호와 비밀번호가 노출되지 않도록 주의하십시오.
- 코쿰의 서비스 목적을 제외한 타인에게 기기의 제어권을 양도하지 마십시오.
- 기기를 해킹하려고 하지 마십시오. 법적 책임이 따를 수 있습니다.



주의

- 장치를 떨어뜨리거나 물리적인 충격을 가하지 말고 높은 전자기 방사선에 노출시키지 마십시오. 진동이 있는 표면이나 충격이 가해지는 장소에 장비를 설치하지 마십시오(무시하면 장비가 손상될 수 있음).
- 기기를 극도로 뜨겁거나(자세한 작동 온도는 기기 사양 참조), 차갑거나 먼지가 많거나 습기가 많은 장소에 두지 말고 높은 전자파에 노출하지 마십시오.
- 장비를 직사광선, 낮은 환기 또는 히터 또는 라디에이터와 같은 열원에 노출하는 것은 금지됩니다(무시하면 화재 위험이 발생할 수 있음).
- 실내용 장치 커버는 비와 습기로부터 보호되어야 합니다.
- 장비를 직사광선, 낮은 환기 또는 히터 또는 라디에이터와 같은 열원에 노출하는 것은 금지됩니다(무시하면 화재 위험이 발생할 수 있음).
- 장치 커버의 내부 및 외부 표면을 청소할 때 부드럽고 마른 천을 사용하고 알칼리성 세제를 사용하지 마십시오.
- 생체 인식 제품은 스푸핑 방지 환경에 100% 적용되지 않습니다. 더 높은 보안 수준이 필요한 경우 여러 인증 모드를 사용하십시오.
- 장비의 직렬 포트는 디버깅에만 사용됩니다.
- 이 설명서의 지침에 따라 장비를 설치하십시오. 부상을 방지하려면 이 장비를 설치 지침에 따라 바닥/벽에 단단히 부착해야 합니다.
- 이 브래킷은 장착된 장치에만 사용하도록 되어 있습니다. 다른 장비와 함께 사용하면 불안정해져 부상을 입을 수 있습니다.
- 이 장비는 장착된 브래킷과 함께 사용해야 합니다. 다른 제품(카트, 스탠드 또는 캐리어)과 함께 사용하면 불안정해져 부상을 입을 수 있습니다.

1. 개요

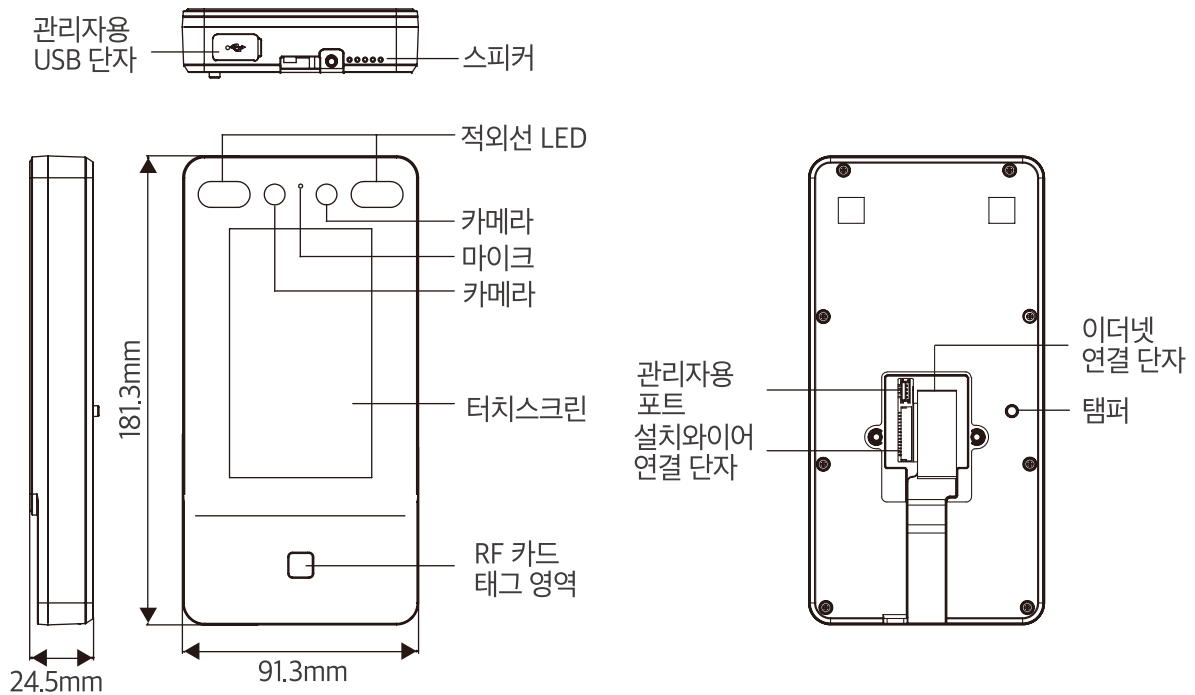
1.1 개요

얼굴인식 출입통제기는 안면인식을 위한 일종의 출입통제장치로 주로 물류센터, 공항, 대학캠퍼스, 경보센터, 주택 등의 보안출입 통제시스템에 적용된다.

1.2 특징

- 4.3인치 LCD 터치 스크린, 272 × 480 화면 해상도, 최대 얼굴 프레임의 실시간 감지 및 표시
- 2MP 광각 듀얼 렌즈
- 얼굴, 지문, 카드, PIN 코드 및 다중 조합 인증과 같은 다중 인증 모드를 지원합니다.
- 출입 통제 기간 통제(계획 템플릿)를 지원하고 필요에 따라 문 열림 권한을 부여합니다.
- 플랫폼을 통한 네트워크 운영 및 출입 정보 발급을 지원합니다.
- 장치 비교 결과 및 연동 캡처 사진을 플랫폼에 실시간으로 업로드할 수 있는 데이터 네트워크 업로드 기능을 지원합니다.
- 장치가 오프라인 상태일 때 장치가 플랫폼에 연결될 때 생성된 이벤트가 다시 업로드됩니다.
- NTP, 수동 및 자동 시간 보정을 지원합니다.
- 관리실기기와 인터폰 통화 및 방문자 확인 후 문열림 기능을 지원합니다.
- RTSP 프로토콜을 통해 원격 비디오 미리보기 및 출력 비디오 코드 스트림을 지원합니다.
- 위치독 가드 메커니즘, 탬퍼 디자인을 지원하여 장치가 제대로 작동하도록 합니다.
- 착용 모드 알림을 포함하여 마스크 감지 모드를 지원하고 마스크 모드를 착용해야 합니다.
- IP65에 준하는 수준의 방수를 지원합니다.

2. 각 부분의 명칭 및 기능



제품명	얼굴인식 출입통제기	사용자 로그	150,000
모델명	KAF-W1000	얼굴 인증 속도	0.2s 이내
전원	DC12V/1A	얼굴 인식 거리	0.3~1.5m
LCD	4.3인치	통신	Wi-Fi(2.4G) , Ethernet(10/100)
카메라	2M(Dual)	온도	-20℃~50℃
사용자 인터페이스	정전식 FULL 터치 방식	보호등급	IP65에 준하는 수준
동작	얼굴 , 카드 , 비밀번호	연동	모바일 App & VMS (PC용)
최대 사용자수	얼굴(3,000), 카드(3,000)	설치방식	노출(벽면부착식)
카드 유형	M1(13.56MHz)	제품 사이즈	91.3mm X 181.3mm X 24.5mm

3. 설치

3.1 설치환경

- 역광, 직사광선 및 간접광선을 피하십시오.
- 더 나은 인식을 위해 설치 환경 또는 주변에 광원이 있어야 합니다.
- 벽이나 기타 장소의 최소 지지 중량은 장치 중량의 3배 이상이어야 합니다.
- 장치 시야 1m 이내에 강한 반사 물체(예: 유리문/벽, 스테인리스 스틸 물체, 아크릴 및 기타 광택 플라스틱, 래커, 세라믹 타일 등)가 없어야 합니다.
- 장치 반사를 피하십시오.
- 얼굴 인식 거리는 30cm 이상이어야 합니다.
- 카메라를 깨끗하게 유지하십시오.



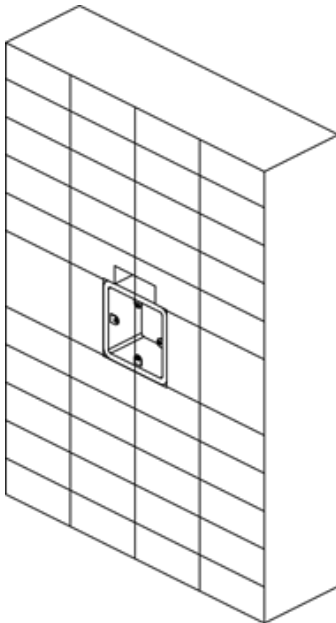
• 설치 환경에 대한 자세한 내용은 설치 환경 팁을 참조하십시오.

3.2 매립 박스와 함께 설치

- ❶ 매립 박스가 벽에 설치되어 있는지 확인하십시오.

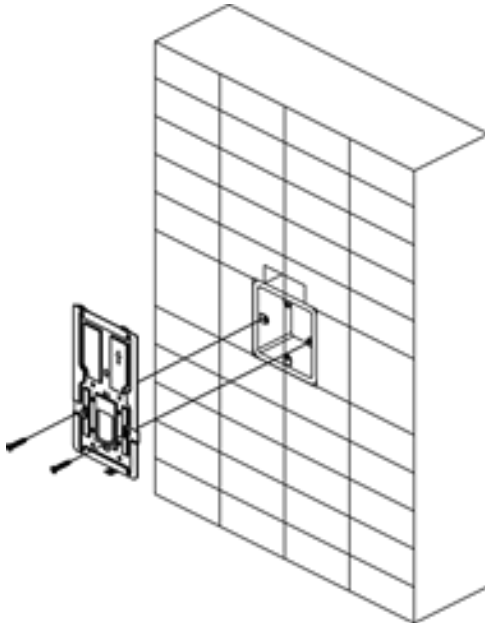


• 매립 박스는 별도로 구매하셔야 합니다.

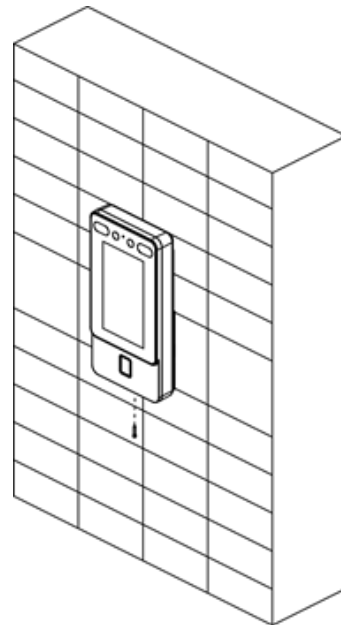
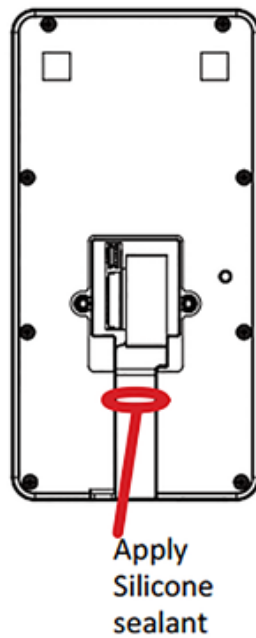


- ❷ 매립 박스 설치: 제공된 나사(SC-KA4X22) 2개를 사용하여 매립 박스에 마운팅 플레이트를 고정합니다.

③ 마운팅 플레이트 설치: 케이블 구멍을 통해 케이블을 배선한 다음 매립 박스에 케이블을 삽입합니다.

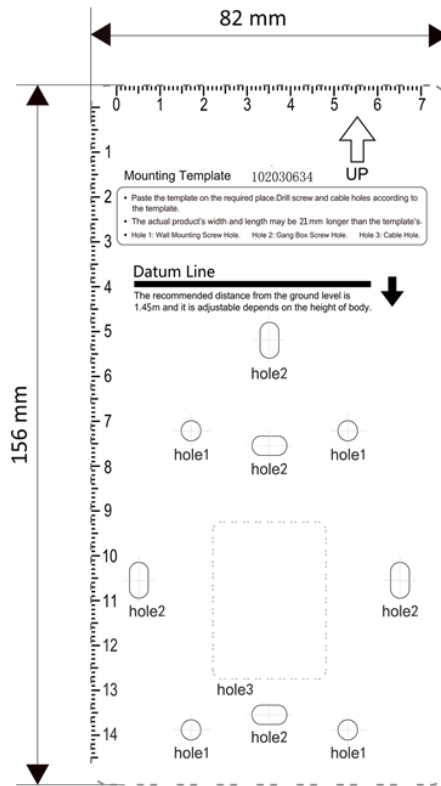


④ 실리콘 실란트 도포: 장치를 장착판과 정렬하고 제공된 나사(SC-KM3X6-T10-SUSS) 1개를 사용하여 장치를 장착판에 고정합니다.



3.3 표면 장착

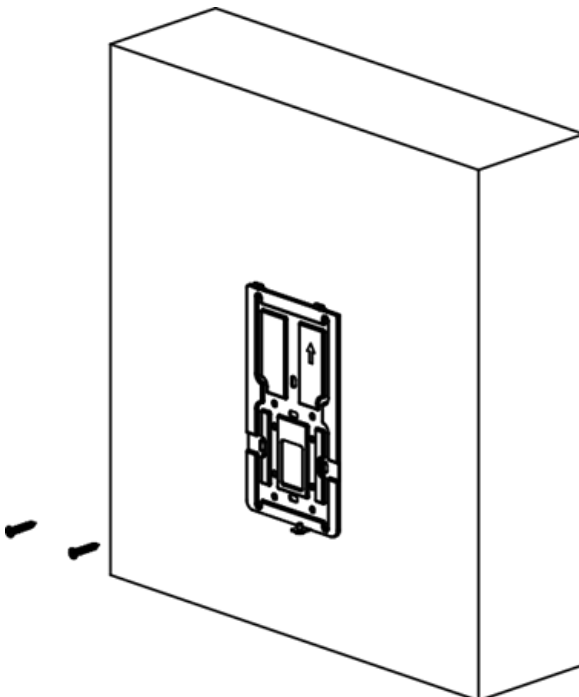
- ❶ 마운팅 템플릿의 기준선에 따라 지면보다 1.45m 높은 벽이나 기타 표면에 마운팅 템플릿을 붙입니다.
- ❷ 장착 템플릿의 구멍 1에 따라 벽이나 다른 표면에 구멍을 뚫습니다.
- ❸ 확장 볼트의 플라스틱 슬리브를 구멍에 삽입합니다.



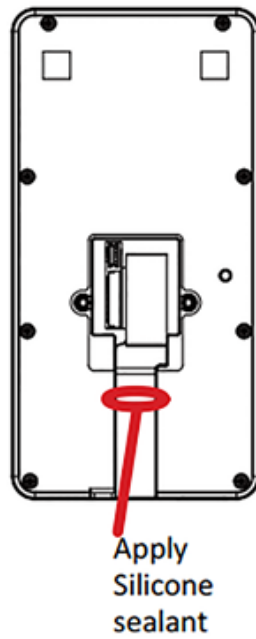
- ❹ 마운팅 플레이트에 구멍을 맞추고 제공된 나사(KA4×22-SUS) 2개로 마운팅 플레이트를 벽에 고정합니다.
- ❺ 마운팅 플레이트 설치: 마운팅 플레이트의 케이블 구멍을 통해 케이블을 배선하고 해당 주변 장치 케이블에 연결합니다.



• 장치를 실외에 설치하는 경우 배선 출구에 실리콘 실런트를 발라 물이 들어가지 않도록 해야 합니다.



⑥ 실리콘 실란트 도포: 장치를 마운팅 플레이트에 정렬하고 장치를 마운팅 플레이트에 겁니다.

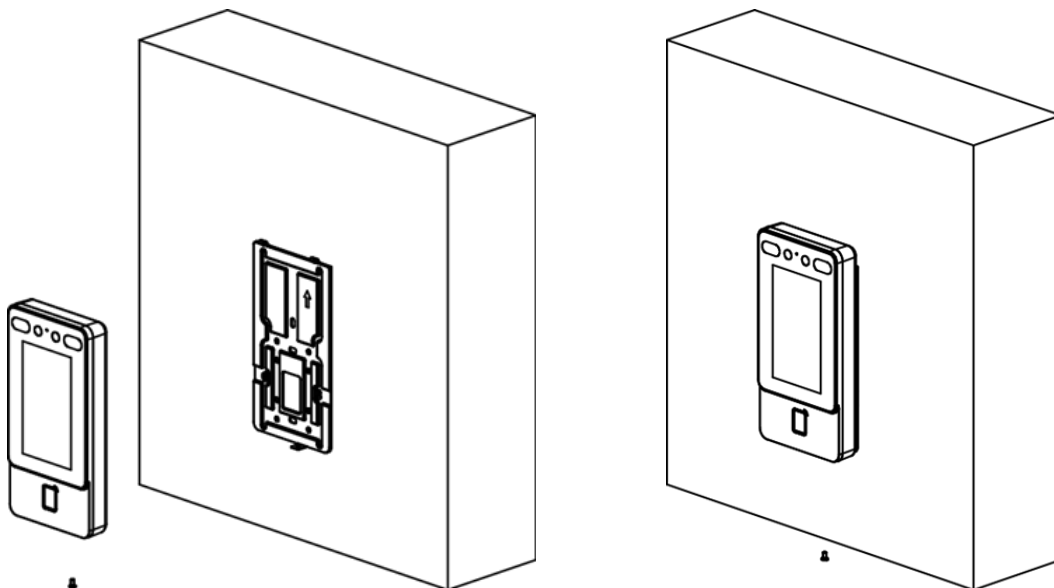


⑦ 장치 걸기: 제공된 나사(KM3×6-SUS) 1개를 사용하여 장치와 마운팅 플레이트를 고정합니다.

⑧ 설치 후 기기의 올바른 사용(실외 사용)을 위해 화면에 보호 필름(제공되는 모델의 일부)을 부착합니다.



- 권장 설치 높이는 1.45m이며 필요에 따라 설치 높이를 설정할 수 있습니다.
- 제공된 마운팅 플레이트를 사용하는 것이 좋습니다.



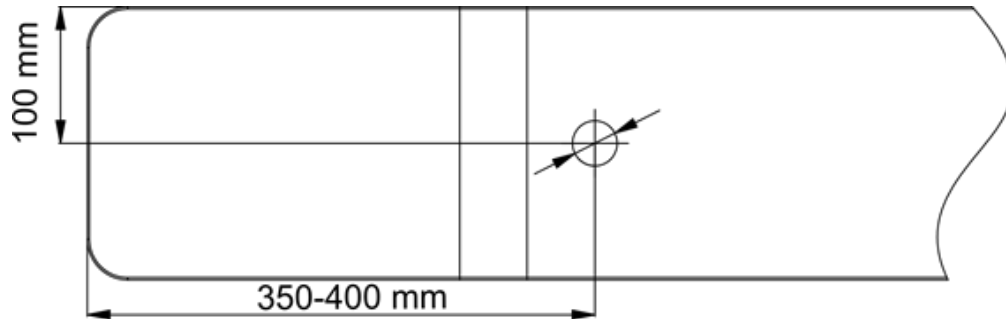
3.4 브래킷으로 장착

3.4.1 브래킷 장착 전 준비사항

❶ 아래 표시된 그림에 따라 개찰구 표면에 구멍을 뚫습니다. 그리고 방수 너트를 설치하십시오.

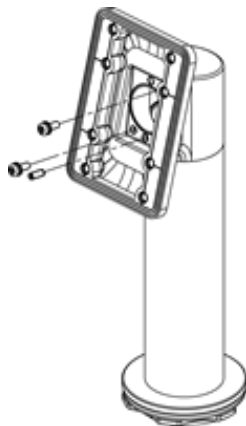


• 물이 들어가지 않도록 리벳을 누른 후 납땜하십시오.

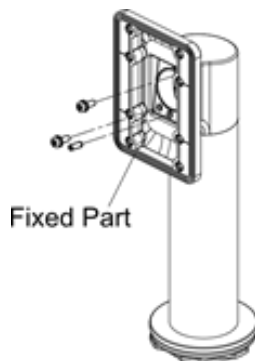


❷ 설치 각도가 개찰구 본체와 수직 180°가 되어야 하는 경우 다음과 같은 작업이 필요합니다.

1) 아래 그림과 같이 3개의 나사를 제거합니다.



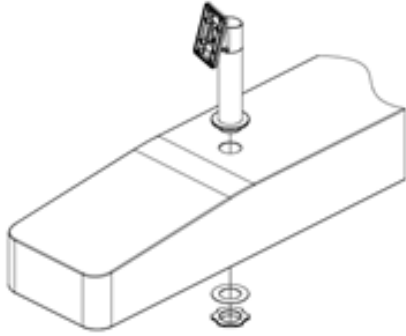
2) 고정부를 180° 회전시키고 나사 3개를 다시 장착합니다.



3.4.2 브래킷 장착

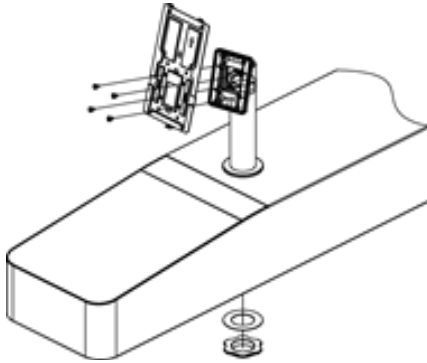
❶ 개찰구에 베이스를 설치합니다.

- 1) 개찰구에 구멍을 맞추고 받침대를 개찰구에 놓습니다.
- 2) 베이스를 획득한 위치로 회전시키고 장치가 올바른 방향을 향하는지 확인합니다.
- 3) 렌치로 베이스를 고정합니다.

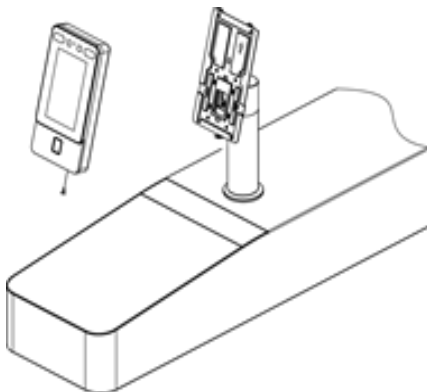


• 개찰구 앞과 뒤에 실리콘 패드를 설치하십시오

❷ 제공된 나사(SC-K1M4×6-SUS) 4개를 사용하여 브래킷에 마운팅 템플릿을 설치합니다.



❸ 개찰구의 케이블 구멍을 통해 케이블을 배선하고 SC-KM3×6-T10-SUS 나사 1개를 사용하여 장치를 장착 플레이트에 고정합니다.



❹ 설치 후 기기의 올바른 사용(실외 사용)을 위해 화면에 보호 필름(제공되는 모델의 일부)을 붙입니다.

3.5 실린더 브래킷으로 장착

3.5.1 브래킷 장착 전 준비사항

❶ 플랜지 너트로 고정된 4개의 나사(M3 또는 M4)를 사용하여 개찰구 내부 표면에 보강판을 설치합니다.

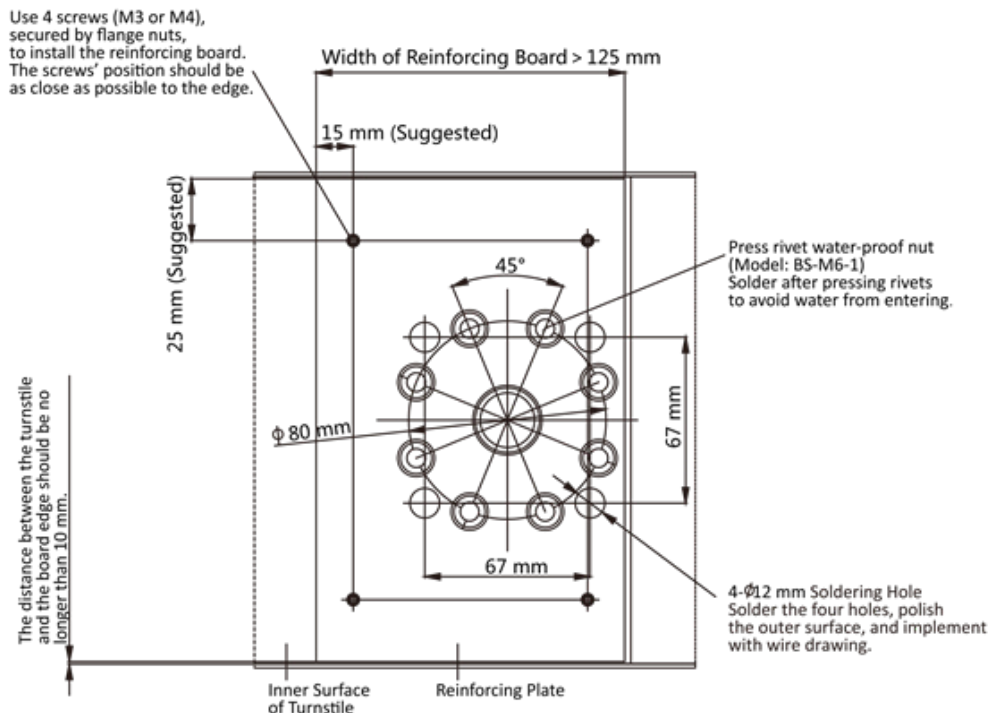


- 개찰구에 구멍을 뚫었는지 확인하십시오. 그렇지 않은 경우 아래 단계에 따라 구멍을 뚫습니다.
- 개찰구와 가장자리 사이의 거리는 10mm를 넘지 않아야 합니다.

❷ 아래 표시된 그림에 따라 개찰구 내부 표면에 구멍을 뚫습니다. 그리고 방수 너트를 설치하십시오.

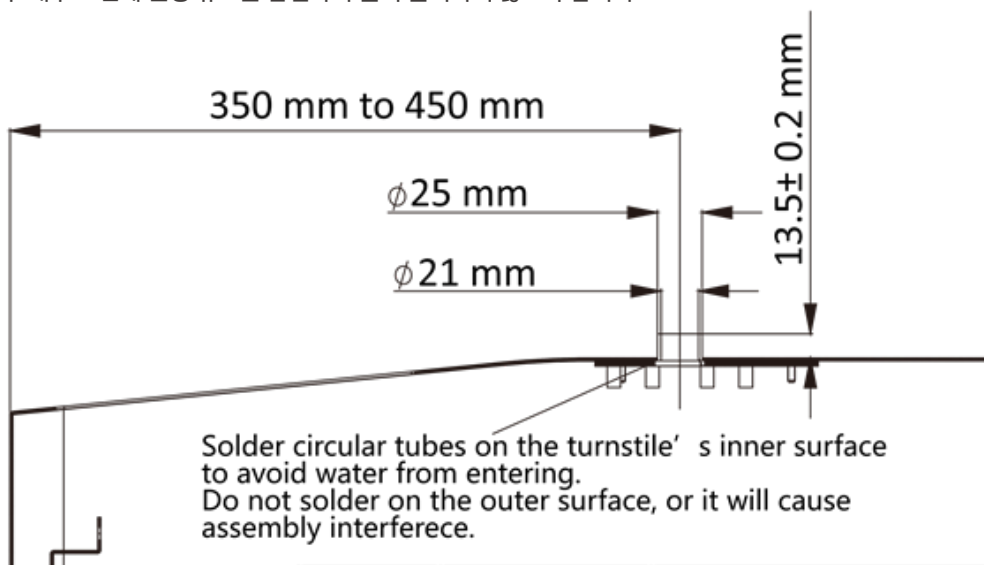


- 물이 들어가지 않도록 리벳을 누른 후 납땜하십시오.



❸ 다른 4개의 구멍을 납땜하고 표면을 연마하고 와이어 드로잉을 구현합니다.

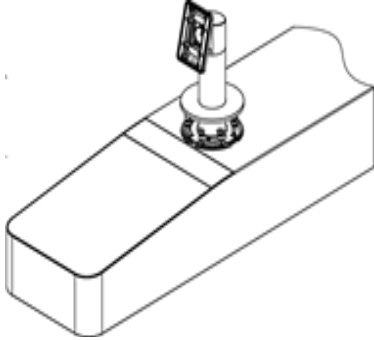
❹ 개찰구 내부 표면에 원형 튜브를 납땜하여 물이 들어가지 않도록 합니다.



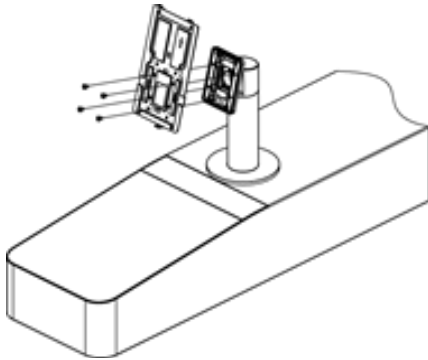
3.5.2 실린더 브라켓 마운팅

❶ 개찰구에 베이스를 설치합니다.

- 1) 개찰구에 구멍을 맞추고 받침대를 개찰구에 놓습니다.
- 2) 베이스를 획득한 위치로 회전시키고 장치가 올바른 방향을 향하는지 확인합니다.
- 3) 4개의 SC-OM6×12-H-SUS 나사로 베이스를 고정합니다.

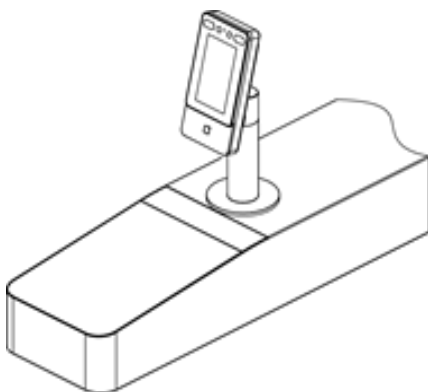


❷ 4개의 SC-K1M4×6-SUS 나사로 마운팅 플레이트를 브라켓에 고정합니다.



❸ 개찰구의 케이블 구멍을 통해 케이블을 배선합니다.

❹ SC-KM3×6-H2-SUS 나사 1개를 사용하여 안면인식 단자를 마운팅 플레이트에 고정합니다.



❺ 설치 후 기기의 올바른 사용(실외 사용)을 위해 화면에 보호 필름(제공되는 모델의 일부)을 붙입니다.

4. 배선

RS-485 카드 리더기에 RS-485 단자를 연결하고, NC/NO 및 COM 단자를 도어락에 연결하고, SEN 및 GND 단자를 도어 컨택트에 연결하고, BTN/GND 단자를 퇴실 버튼에 연결하고, Wiegand 단말기를 Wiegand 카드 리더 또는 액세스 컨트롤러와 연결합니다. Wiegand 단말기와 출입통제기를 연결하면 얼굴인식 단말기가 인증정보를 출입통제기로 전송하고 출입통제자는 출입문의 열림 여부를 판단할 수 있습니다.



- 케이블 크기가 18AWG인 경우 12V 전원 공급 장치를 사용해야 합니다. 그리고 전원 공급 장치와 장치 사이의 거리는 20m를 넘지 않아야 합니다.
- 케이블 크기가 15AWG인 경우 12V 전원 공급 장치를 사용해야 합니다. 그리고 전원 공급 장치와 장치 사이의 거리는 30m를 넘지 않아야 합니다.
- 케이블 크기가 12AWG인 경우 12V 전원 공급 장치를 사용해야 합니다. 그리고 전원 공급 장치와 장치 사이의 거리는 40m를 넘지 않아야 합니다.
- 외부 카드 리더, 도어락, 퇴실 버튼, 도어 마그네틱은 개별 전원 공급이 필요합니다.

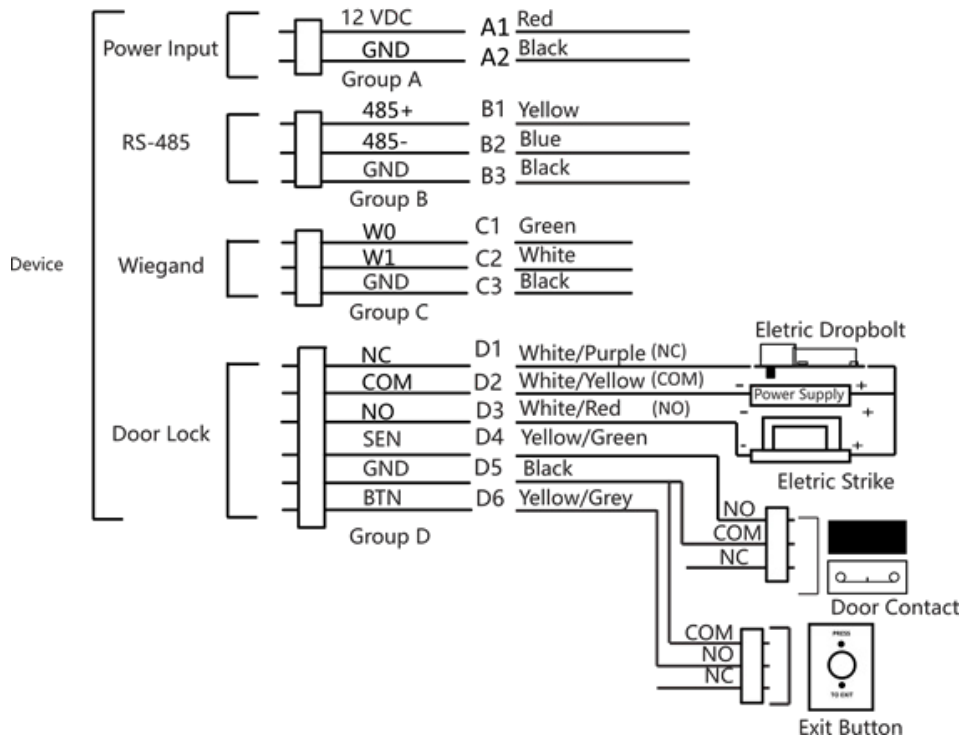
4.1 단자 설명

단자에는 전원 입력, RS-485, Wiegand 출력 및 도어록 연결이 포함되어 있습니다. 단자에 대한 설명은 다음과 같습니다.

그룹	NO	기능	컬러	이름	설명
그룹A	A1	전원 입력	빨강색	+12V	12VDC 전원공급 장치
	A2		검정색	GND	GND
그룹B	B1	RS-485	노랑색	485+	RS-485 배선
	B2		파랑색	485-	
	B3		검정색	GND	GND
그룹C	C1	Wiegand	녹색	W0	Wiegand 배선 0
	C2		흰색	W1	Wiegand 배선 1
	C3		검정색	GND	GND
그룹D	D1	도어락	흰색/보라색	NC	데드볼트/ 도어 스트라이커 연결
	D2		흰색/노랑색	COM	
	D3		흰색/빨강색	NO	
	D4		노랑색/녹색	NO	도어 센서
	D5		검정색	GND	GND
	D6		노랑색/회색	NC	퇴실 버튼

4.2 유선 일반 장치

단자를 자동문의 각 디바이스와 연결할 수 있습니다.

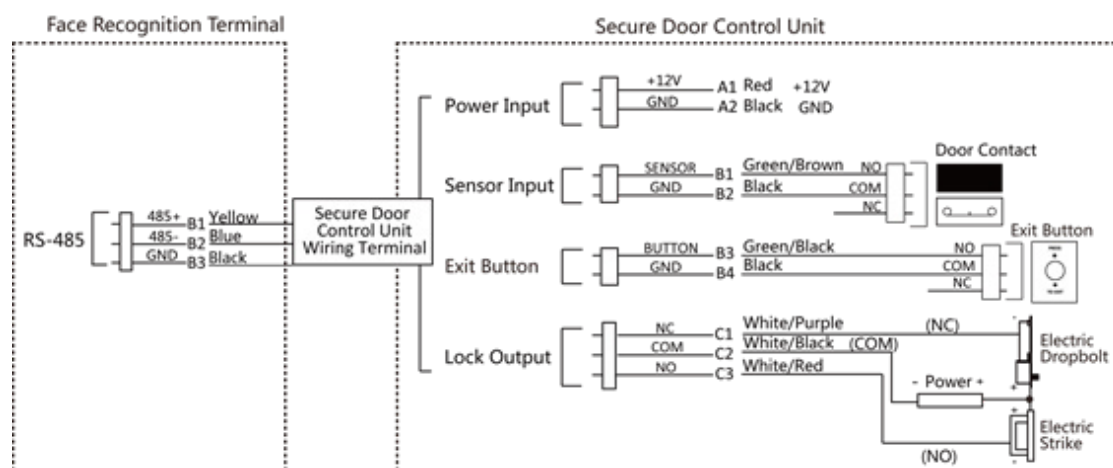


- Wiegand 카드 리더기에 연결하려면 얼굴 인식 단말기의 Wiegand 방향을 입력으로 설정해야 합니다. 출입 통제기에 연결하는 경우 Wiegand 방향을 출력으로 설정해야 출입 통제기에 인증 정보를 전송할 수 있습니다.
- Wiegand 방향 설정에 대한 자세한 내용은 다음을 참조하십시오. [Wiegand 설정]
- 장치를 전기 공급 장치에 직접 연결하지 마십시오.

4.3 유선 보안 도어 제어 장치

보안 도어 제어 장치와 터미널을 연결할 수 있습니다.

배선도는 다음과 같습니다.



- 보안 도어 제어 장치는 외부 전원 공급 장치에 별도로 연결해야 합니다. 권장 외부 전원 공급 장치는 12V, 0.5A입니다.

4.4 화재 시스템 연동

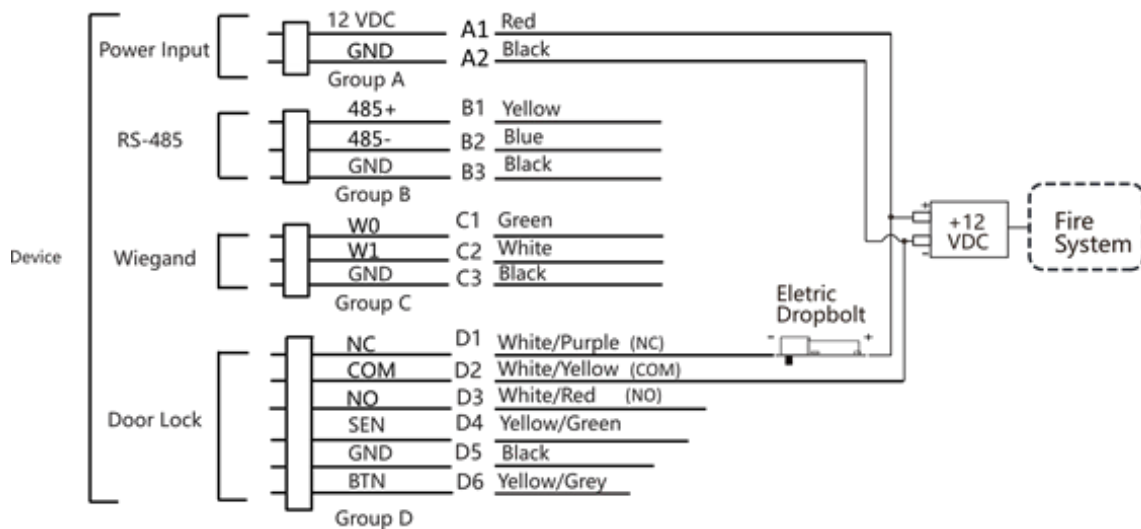
4.4.1 전원 차단 시 문 열림 결선도

- 자물쇠 유형: 양극 자물쇠, 자석 자물쇠 및 전기 놀이쇠(NO)
- 보안 유형: 전원을 끌 때 문 열림
- 시나리오: Fire Engine Access에 설치됨

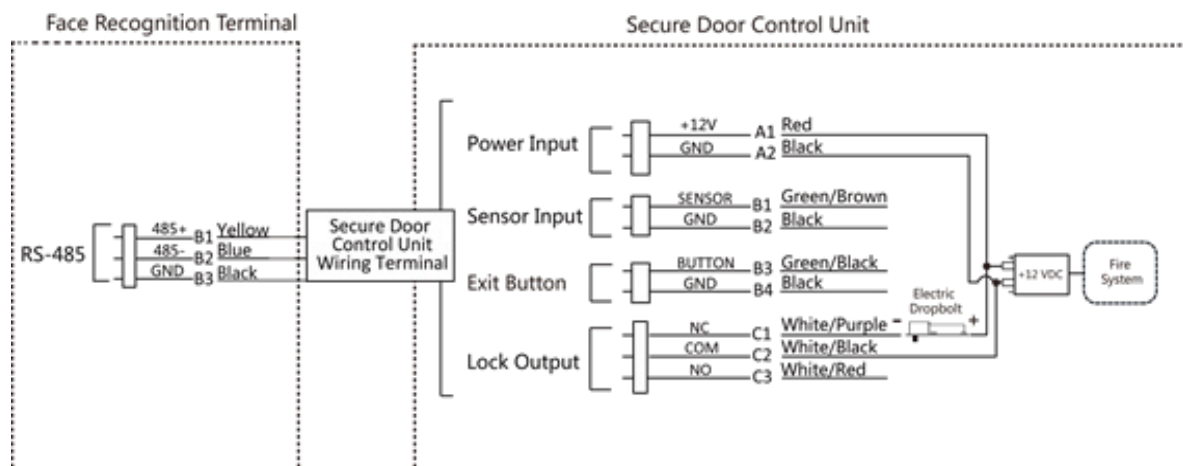
• 유형 1



• 화재 시스템은 액세스 제어 시스템의 전원 공급 장치를 제어합니다.



[와이어 장치]

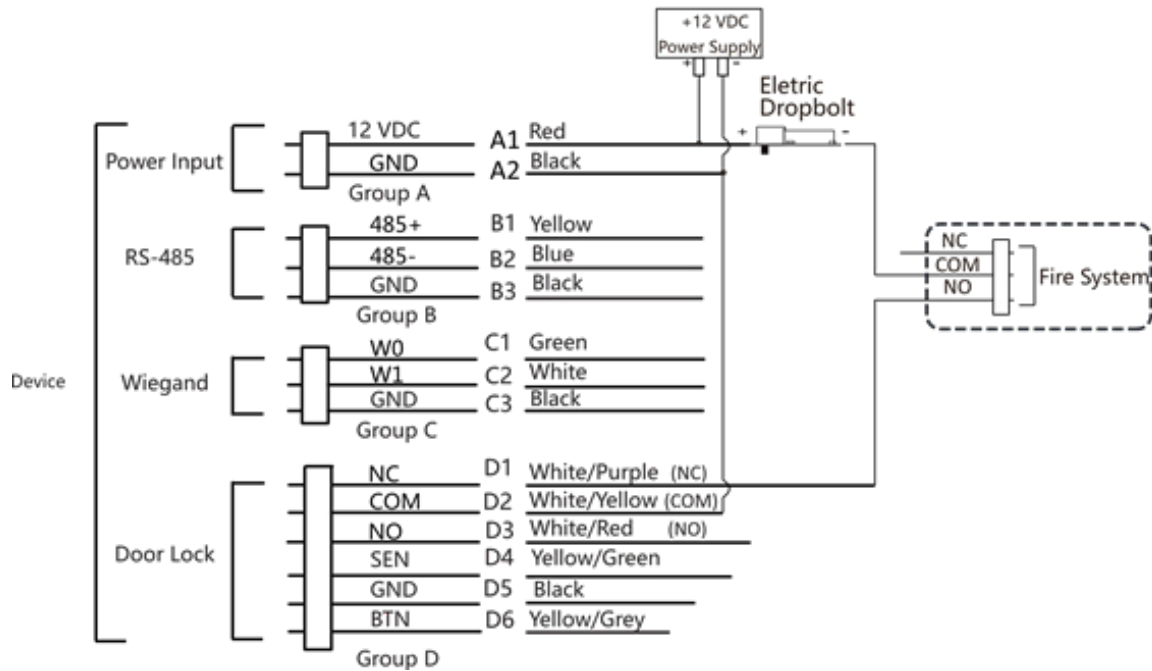


[와이어 보안 도어 제어 장치]

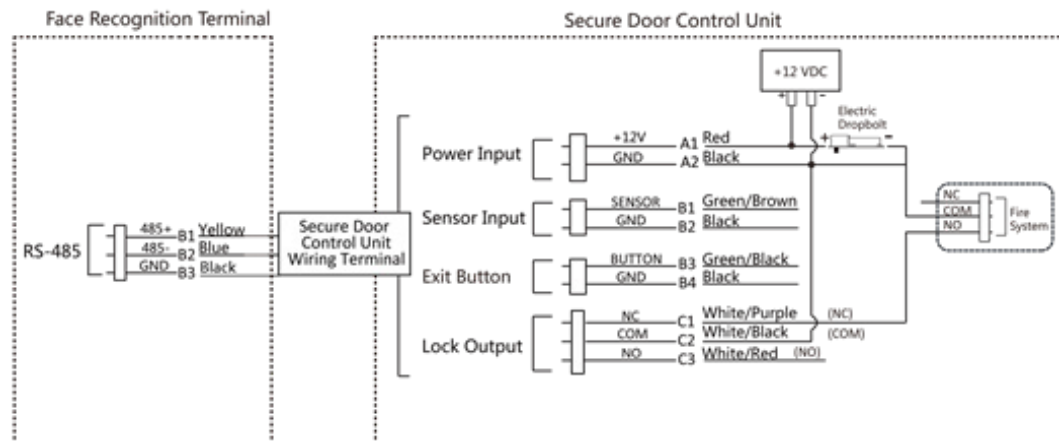
• 유형 2



- 화재 시스템(NO 및 COM, 일반적으로 전원을 끌 때 열림)은 잠금 장치 및 전원 공급 장치와 직렬로 연결됩니다.
- 화재 경보가 울리면 문은 계속 열려 있습니다. 정상 시에는 NO와 COM이 닫혀 있습니다.



[배선 장치]



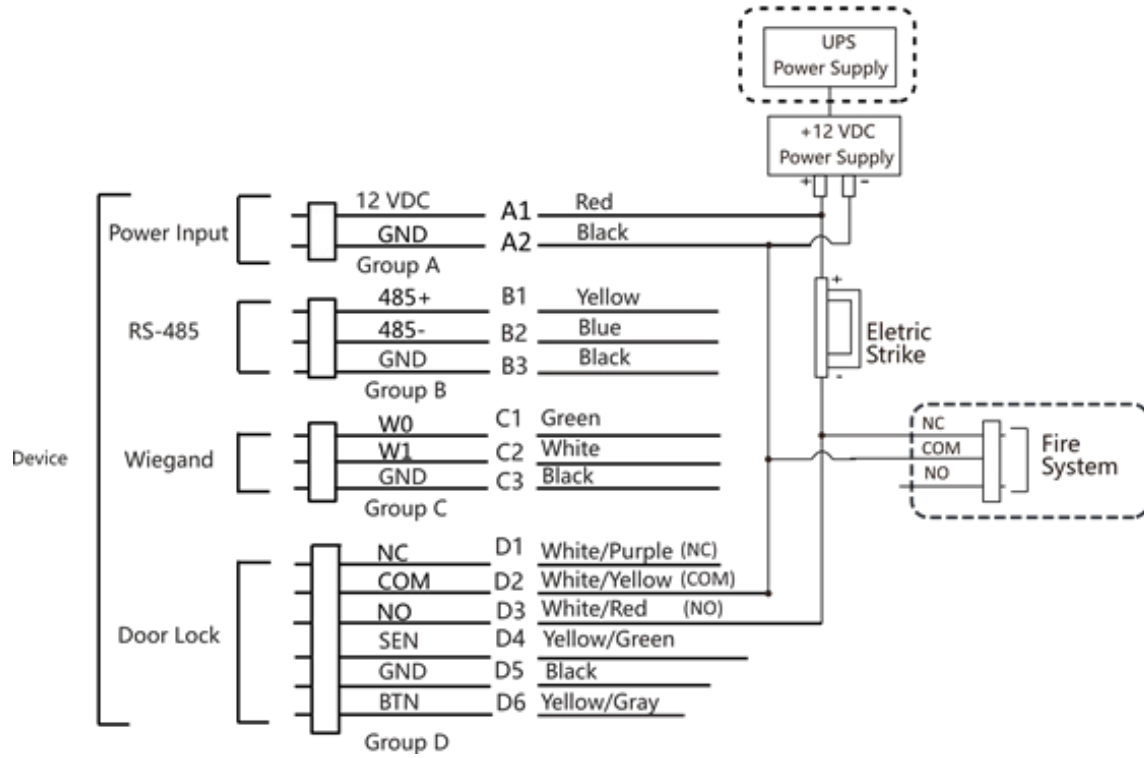
[보안 도어 제어 장치 배선]

4.4.2 전원 차단 시 도어 잠금 결선도

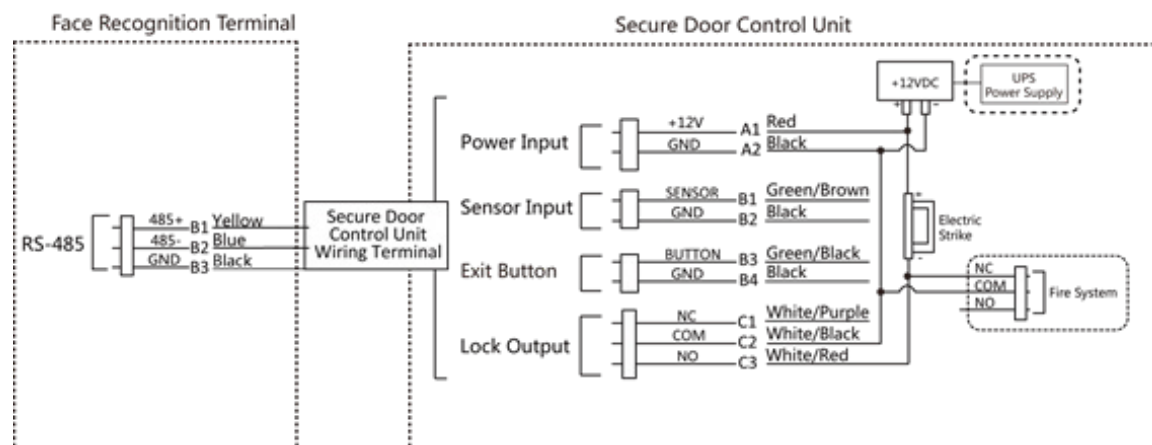
- 자물쇠 유형: 음극 자물쇠, 전기 자물쇠 및 전기 놀이쇠(NC)
- 보안 유형: 전원을 끌 때 잠긴 문
- 시나리오 : Fire Linkage로 출입구에 설치



- UPS(무정전 전원 공급 장치)가 필요합니다.
- 화재 시스템(NC 및 COM, 일반적으로 전원이 꺼지면 닫힘)은 잠금 장치 및 전원 공급 장치와 직렬로 연결됩니다. 화재 경보가 울리면 문은 계속 열려 있습니다.
- 평상시에는 NC와 COM이 열려 있습니다.



[장치 배선]



[배선도]

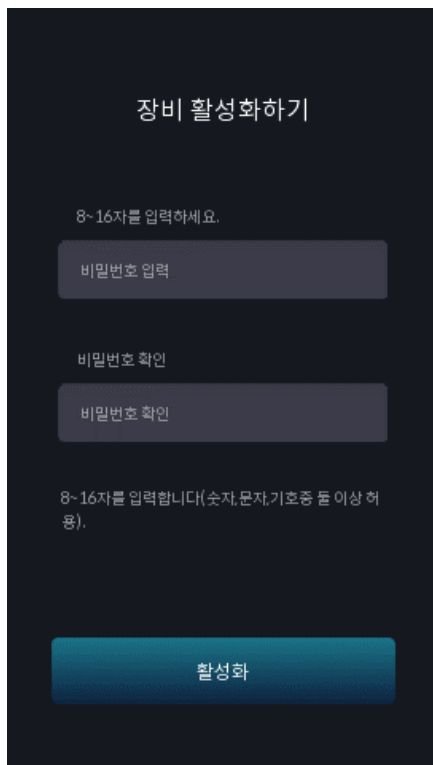
5. 초기 사용 등록(활성화)

처음 사용할 시에는 초기 사용 등록 (활성화)을 해야만 장비를 정상적으로 사용할 수 있습니다.
장비, PC 프로그램 등에서 초기 사용 등록(활성화)을 할 수 있습니다.
장치의 네트워크 기본값은 다음과 같습니다.

- 기본 IP 주소: 192.0.0.64
- 기본 포트 번호: 8000
- 기본 사용자 이름: admin

5.1 장비에서의 초기 사용 등록

장비에서 전원을 켜 후 초기 사용 등록을 할 수 있습니다.
활성화 페이지에서 암호를 등록합니다. 활성화를 탭하면 장치가 활성화됩니다.



장비 활성화하기

8~16자를 입력하세요.

비밀번호 입력

비밀번호 확인

비밀번호 확인

8~16자를 입력합니다(숫자,문자,기호중 둘 이상 허용).

활성화

[활성화 페이지]



- 장치의 암호 레벨을 자동으로 확인할 수 있습니다. 보안을 강화하기 위해 선택한 비밀번호(대문자, 소문자, 숫자, 특수문자 중 최소 3가지 범주를 포함하여 최소 8자 이상 사용)를 변경하는 것이 좋습니다. 제품. 그리고 정기적으로 비밀번호를 변경할 것을 권장하며, 특히 보안이 높은 시스템에서는 매월 또는 매주 비밀번호를 변경을 권장합니다
- 모든 암호 및 기타 보안 설정의 적절한 구성은 설치자 및/또는 최종 사용자의 책임입니다.



- admin 및 nimda를 포함하는 문자는 활성화 암호로 설정할 수 없습니다.

- 활성화 후 실제 필요에 따라 언어를 선택해야 합니다.
- 활성화 후 애플리케이션 모드를 선택해야 합니다. 자세한 내용은 다음을 참조하십시오. [\[애플리케이션 모드 설정\]](#)
- 활성화 후 네트워크를 설정해야 합니다. 자세한 내용은 다음을 참조하십시오. [\[네트워크 설정\]](#)
- 활성화 후 장치를 플랫폼에 추가할 수 있습니다. 자세한 내용은 다음을 참조하십시오. [\[플랫폼에 대한 액세스\]](#)
- 활성화 후 개인정보 설정이 필요한 경우 해당 항목을 체크하셔야 합니다. 자세한 내용은 다음을 참조하십시오. [\[개인 정보 설정\]](#)
- 활성화 후 장치를 관리하기 위해 관리자를 추가해야 하는 경우 관리자를 설정해야 합니다. 자세한 내용은 다음을 참조하십시오. [\[관리자 추가\]](#)

5.2 웹 브라우저를 통한 활성화

웹 브라우저를 통해 장치를 활성화할 수 있습니다.

- 1 웹 브라우저의 주소 표시줄에 장치 기본 IP 주소(192.0.0.64)를 입력하고 Enter 키를 누릅니다.



• 장치 IP 주소와 컴퓨터가 동일한 IP 세그먼트에 있어야 합니다.

- 2 새 비밀번호(관리자 비밀번호)를 만들고 비밀번호를 확인합니다.



• 강력한 비밀번호 권장-제품의 보안을 강화하기 위해 자신이 선택한 강력한 비밀번호(대문자, 소문자, 숫자, 특수 문자를 포함하여 최소 8자 이상 사용)를 생성하는 것이 좋습니다. 그리고 정기적으로 비밀번호 재설정을 권장하며, 특히 보안 수준이 높은 시스템에서는 매월 또는 매주 비밀번호를 재설정하는 것을 권장합니다.



• admin 및 nimda를 포함하는 문자는 활성화 암호로 설정할 수 없습니다.

- 3 활성화를 클릭합니다.

- 4 장치 IP 주소를 편집합니다. SADP 도구, 장치 및 클라이언트 소프트웨어를 통해 IP 주소를 편집할 수 있습니다.

5.3 SADP를 통한 활성화

SADP는 LAN을 통해 장치의 IP 주소를 감지, 활성화 및 수정하는 도구입니다.

시작하기 전에

- 제공된 디스크 또는 공식 웹 사이트에서 SADP 소프트웨어를 다운로드하고 프롬프트에 따라 SADP를 설치합니다.
- SADP 도구를 실행하는 장치와 PC는 동일한 서브넷 내에 있어야 합니다.

다음 단계는 장치를 활성화하고 해당 IP 주소를 수정하는 방법을 보여줍니다. 일괄 활성화 및 IP 주소 수정에 대한 자세한 내용은 SADP 사용 설명서를 참조하십시오.

- 1 SADP 소프트웨어를 실행하고 온라인 장치를 검색합니다.
- 2 온라인 장치 목록에서 장치를 찾아 선택합니다.
- 3 새 비밀번호(admin 비밀번호)를 입력하고 비밀번호를 확인합니다.

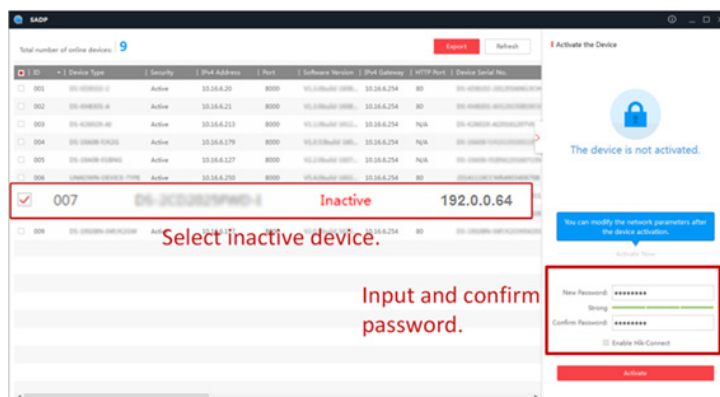


• 강력한 비밀번호 권장-제품의 보안을 강화하기 위해 자신이 선택한 강력한 비밀번호(대문자, 소문자, 숫자, 특수 문자를 포함하여 최소 8자 이상 사용)를 생성하는 것이 좋습니다. 그리고 정기적으로 비밀번호 재설정을 권장하며, 특히 보안 수준이 높은 시스템에서는 매월 또는 매주 비밀번호를 재설정하는 것을 권장합니다.



• admin 및 nimda를 포함하는 문자는 활성화 암호로 설정할 수 없습니다.

- 4 활성화를 클릭하여 활성화를 시작합니다.
성공적으로 활성화되면 장치의 상태가 활성이 됩니다.



- 5 장치의 IP 주소를 수정합니다.

- 1) 장치를 선택합니다.
- 2) IP 주소를 수동으로 수정하거나 DHCP 활성화를 선택하여 장치 IP 주소를 컴퓨터와 동일한 서브넷으로 변경합니다.
- 3) 관리자 암호를 입력하고 수정을 클릭하면 IP 주소 수정이 활성화됩니다.

5.4 Guarding Vision Client 소프트웨어를 통한 장치 활성화

일부 장치의 경우 Guarding Vision 소프트웨어에 추가하고 제대로 작동하려면 암호를 생성하여 활성화해야 합니다



• 이 기능은 장치에서 셋팅해야 합니다.

- ❶ 장치 관리 페이지로 들어갑니다.
- ❷ 장치 관리 오른쪽의 을 클릭하고 장치를 선택합니다.
- ❸ 온라인 장치를 클릭하여 온라인 장치 영역을 표시합니다.
검색된 온라인 장치가 목록에 표시됩니다.
- ❹ 장치 상태(보안 수준 옆에 표시됨)를 확인하고 비활성 장치를 선택합니다.
- ❺ 활성화를 클릭하여 활성화 대화 상자를 엽니다.
- ❻ 암호 필드에 암호를 생성하고 암호를 확인합니다.



• 장치의 암호 강도를 자동으로 확인할 수 있습니다. 귀하의 보안을 강화하기 위해 귀하가 선택한 비밀번호(대문자, 소문자, 숫자, 특수 문자 중 최소 3가지 범주를 포함하여 최소 8자 이상 사용)를 변경하는 것이 좋습니다. 제품. 그리고 정기적으로 비밀번호를 변경할 것을 권장하며, 특히 보안이 높은 시스템에서는 매일 또는 매주 비밀번호를 변경하는 것을 권장합니다.

• 모든 암호 및 기타 보안 설정의 적절한 구성은 설치자 및/또는 최종 사용자의 책임입니다.



• admin 및 nimda를 포함하는 문자는 활성화 암호로 설정할 수 없습니다.

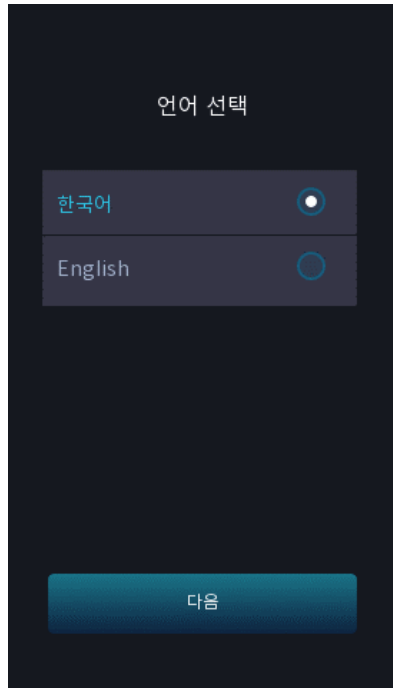
- ❼ 확인을 클릭하여 장치를 활성화합니다.

6. 사용자 환경 설정

6.1 언어 선택

장치 시스템의 언어를 선택할 수 있습니다.

장치 활성화 후 장치 시스템의 언어를 선택할 수 있습니다.



[시스템 언어 선택]

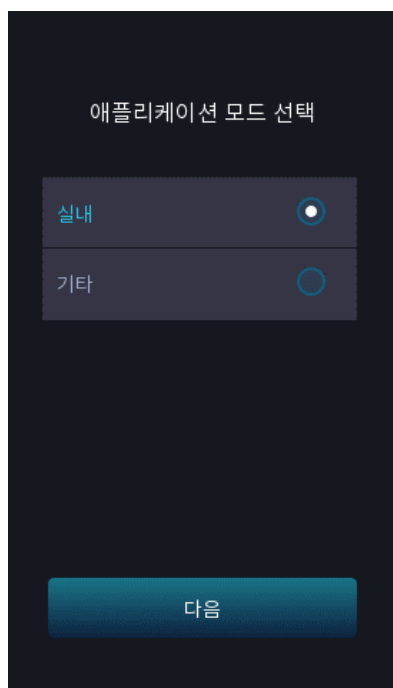


- 기본적으로 시스템 언어는 한국어입니다.
- 시스템 언어를 변경하면 장치가 자동으로 재부팅됩니다.

6.2 애플리케이션 모드 설정

장치를 활성화한 후 더 나은 장치 적응을 위해 응용 프로그램 모드를 선택해야 합니다.

❶ 시작 페이지의 드롭다운 목록에서 실내 또는 기타를 선택합니다. 실외 설치 환경의 경우에는 기타를 선택해 주세요.



[애플리케이션 모드 선택]

❷ 다음을 눌러 저장합니다.

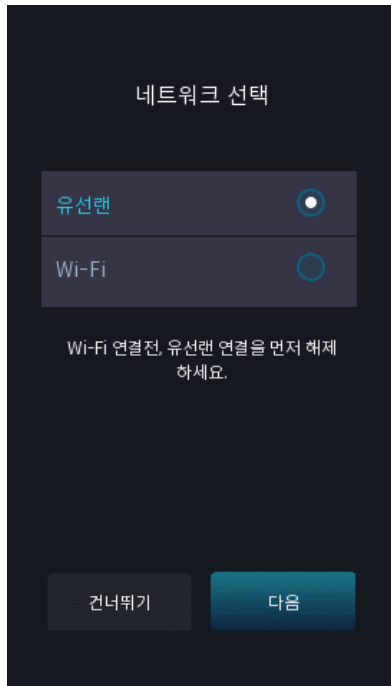


- 시스템 설정에서 설정을 변경할 수도 있습니다.
- 창가에 가까운 실내에 설치하거나 얼굴인식 기능이 잘 작동하지 않는 경우 기타를 선택하세요.
- 애플리케이션 모드를 구성하지 않고 다음을 누르면 시스템은 기본적으로 실내를 선택합니다.
- 다른 도구를 통해 원격으로 장치를 활성화하면 시스템은 기본적으로 실내를 응용 프로그램 모드로 선택합니다.

6.3 네트워크 설정

활성화 및 애플리케이션 모드 선택 후 장치에 대한 네트워크를 설정할 수 있습니다.

- 1 네트워크 선택 페이지에 들어가면 실제 필요에 따라 유선랜 또는 Wi-Fi를 누릅니다.



[네트워크 선택]



- Wi-Fi를 연결하기 전에 유선 네트워크를 분리하십시오.

- 2 다음을 누릅니다.

유선 네트워크



- 장치가 네트워크에 연결되어 있는지 확인하십시오.

DHCP를 활성화하면 시스템이 IP 주소 및 기타 설정을 자동으로 할당합니다.

DHCP를 비활성화하는 경우 IP 주소, 서브넷 마스크 및 게이트웨이를 설정해야 합니다.

와이파이

Wi-Fi를 선택하고 Wi-Fi 비밀번호를 입력하면 연결됩니다.

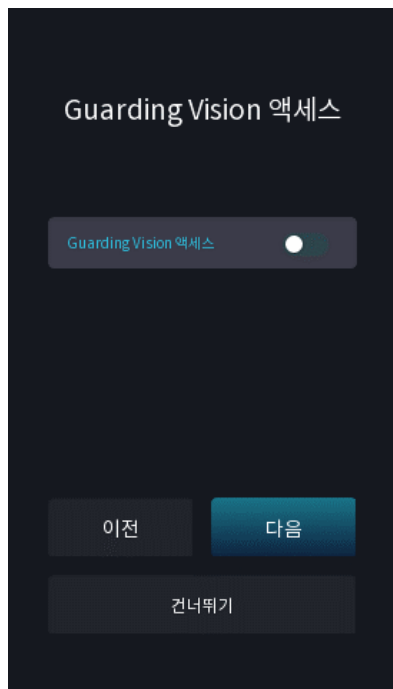
또는 Wi-Fi 추가를 누르고 Wi-Fi 이름과 암호를 입력하여 연결하십시오.

- 3 옵션: 건너뛰기를 탭하여 네트워크 설정을 건너뜁니다.

6.4 플랫폼에 대한 액세스

기능을 활성화하면 장치가 Guarding Vision을 통해 통신할 수 있습니다.
Guarding Vision 모듈 클라이언트 등에 장치를 추가할 수 있습니다.

❶ Guarding Vision에 대한 액세스를 활성화하고 서버 IP 및 인증 코드를 설정합니다.



[Guarding Vision에 대한 액세스]

❷ 다음을 누릅니다.



• 이전을 눌러 Wi-Fi 구성 페이지로 돌아가는 경우 연결된 WiFi를 누르거나 다른 Wi-Fi를 연결해야 플랫폼 페이지에 다시 들어갈 수 있습니다.

6.5 모바일 클라이언트에 연결

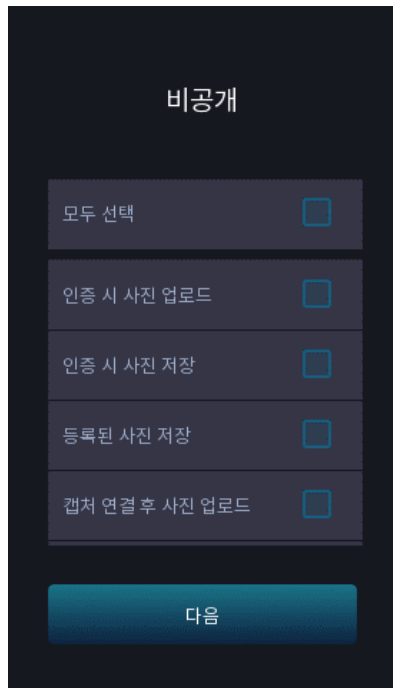
활성화, 애플리케이션 모드 선택, 네트워킹 선택 후 모바일 클라이언트에 장치를 추가할 수 있습니다.

모바일 클라이언트를 다운로드하고 설치합니다. 모바일 클라이언트의 QR 코드 스캔 기능을 사용하고 장치에 표시된 QR 코드를 스캔하여 장치를 모바일 클라이언트에 연결합니다.

지침에 따라 디바이스를 모바일 클라이언트에 연결합니다.

6.6 개인 정보 설정

활성화, 애플리케이션 모드 선택, 네트워크 선택 후 사진 업로드 및 저장을 포함하여 개인정보를 설정해야 합니다. 필요에 따라 항목을 선택하십시오.



[프라이버시]

인증 시 사진 업로드

인증 시 캡처한 사진을 플랫폼에 자동으로 업로드합니다.

인증 시 사진 저장

이 기능을 활성화하면 기기 인증 시 사진을 저장할 수 있습니다.

등록된 사진 저장

기능을 활성화하면 등록된 얼굴 사진이 시스템에 저장됩니다.

캡처 연결 후 사진 업로드

연결된 카메라로 촬영한 사진을 플랫폼에 자동으로 업로드합니다.

캡처 연결 후 사진 저장

이 기능을 활성화하면 연결된 카메라에서 촬영한 사진을 장치에 저장할 수 있습니다.

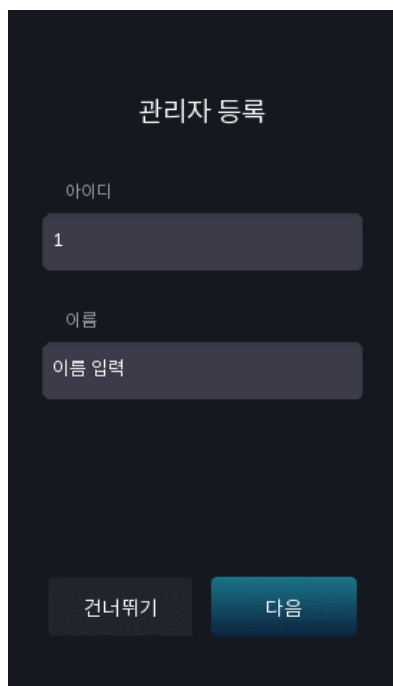
6.7 관리자 설정

장치 활성화 후 관리자를 추가하여 장치를 관리할 수 있습니다.

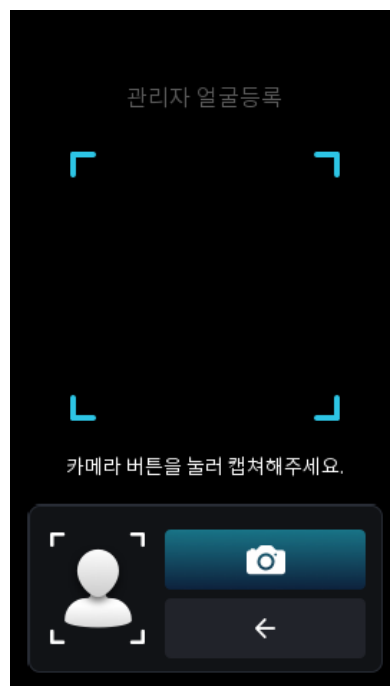
시작하기 전에

• 장치를 활성화하고 애플리케이션 모드를 선택합니다.

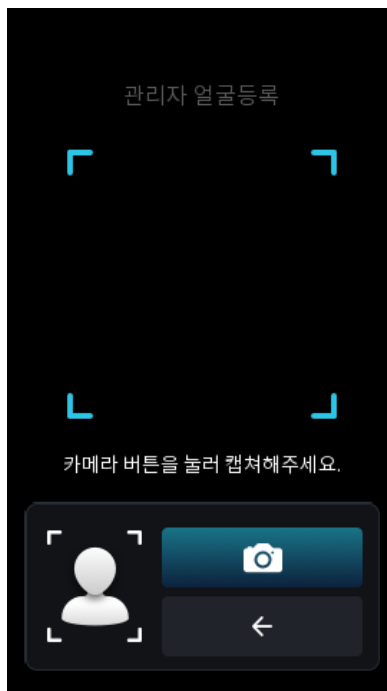
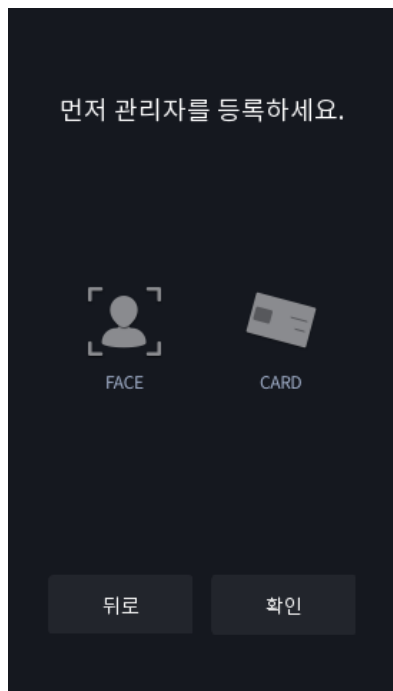
- ① 옵션: 필요한 경우 건너뛰기를 눌러 관리자 추가를 건너뛵니다.
- ② 관리자 이름(선택 사항)을 입력하고 다음을 누릅니다. 관리자 이름은 영문만 지원합니다.



[관리자 등록 페이지]



[관리자 등록 페이지]



③ 추가할 권한 인증 항목을 선택합니다



• 최소한 한 개 이상의 항목을 선택해야 합니다.



카메라를 정면으로 향합니다. 얼굴이 얼굴 인식 영역에 있는지 확인하십시오.



를 클릭하여 캡처하고  을 클릭하여 확인합니다.



카드 제시 영역에 카드 번호 또는 제시 카드를 입력합니다. 확인을 클릭합니다.

④ 확인을 클릭하여 인증 페이지에 들어가게 됩니다.

상태 아이콘 설명



장치가 무장되어 있습니다/무장되어 있지 않습니다.



Guarding Vision이 활성화/비활성화됩니다.



장치 유선 네트워크가 연결됨/연결되지 않음/연결에 실패했습니다.



장치의 Wi-Fi가 활성화되고 연결됨/연결되지 않음/활성화되지만 연결되지 않음.

바로 가기 키 설명



• 화면에 표시되는 바로 가기 키를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오. [기본 설정]
• 장비를 관리 PC 프로그램 또는 관리실기에 추가해야 합니다. 그렇지 않으면 호출 작업이 실패합니다.



장비 번호를 입력하고 확인을 눌러 전화를 겁니다.

관리 PC 프로그램 또는 관리실기에 전화하려면



를 누르십시오.



인증을 위해 PIN 코드를 입력하세요.

7. 기본 동작

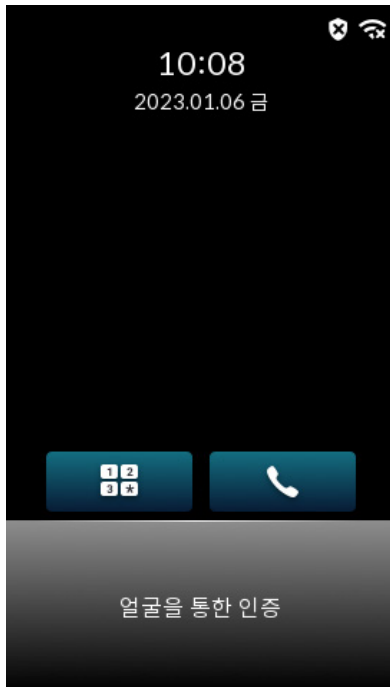
7.1 로그인

장치 기본 매개 변수를 설정하려면 장치에 로그인하십시오.

7.1.1 관리자 로그인

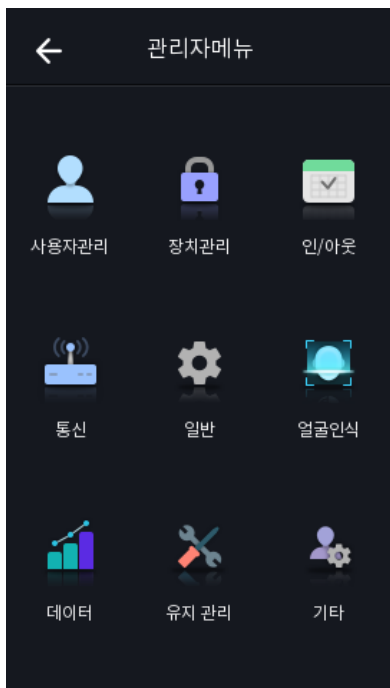
장치에 관리자를 추가한 경우 관리자만 장치에 로그인하여 장치를 작동할 수 있습니다.

- ❶ 초기 페이지를 3초간 길게 누른 후 제스처에 따라 좌/우로 슬라이드하여 관리자 로그인 페이지로 들어갑니다.



[관리자 로그인]

- ❷ 관리자의 얼굴, 지문 또는 카드를 인증하여 관리자 메뉴 페이지로 이동합니다.



[관리자 메뉴 페이지]



• 지문 또는 카드 시도가 5회 실패하면 장치가 30분 동안 잠깁니다.




을 누르고 로그인을 위한 장치 활성화 암호를 입력할 수 있습니다.

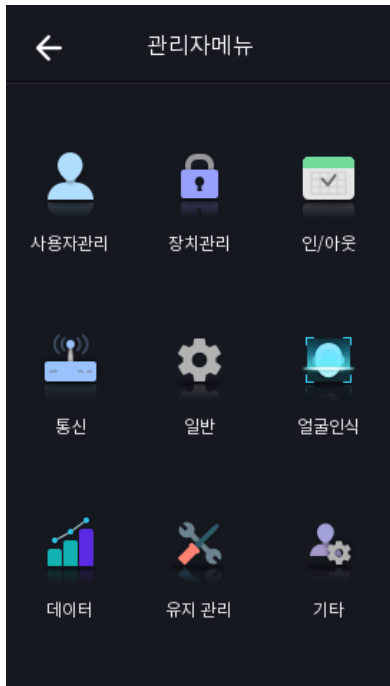


를 탭하면 관리자 메뉴(메인) 페이지를 종료할 수 있습니다.

7.1.2 활성화 비밀번호로 로그인

다른 장치를 조작하기 전에 시스템에 로그인해야 합니다.
관리자를 구성하지 않은 경우 아래 지침에 따라 로그인해야 합니다.

- ❶ 초기 페이지를 3초간 길게 누른 후 제스처에 따라 좌/우로 밀어서 비밀번호 입력 페이지로 진입합니다.
- ❷ 비밀번호를 입력하세요.
 - 장치에 대한 관리자를 추가한 경우  를 누르고 비밀번호를 입력하십시오.
 - 장치에 대한 관리자를 추가하지 않은 경우 암호를 입력합니다.
- ❸ 확인을 눌러 관리자 메뉴(메인) 페이지로 들어갑니다.

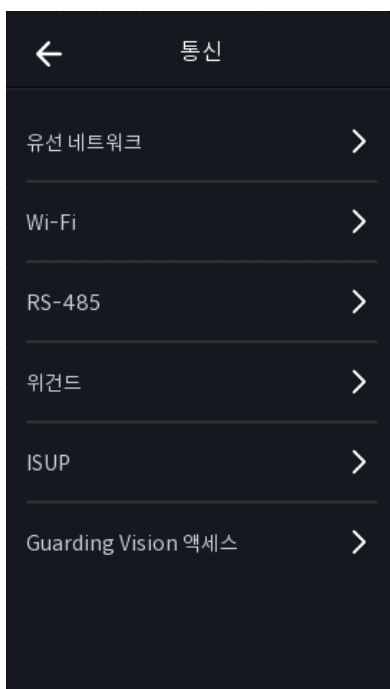


 암호 시도가 5회 실패하면 장치가 30분 동안 잠깁니다.

[관리자 메뉴(메인) 페이지]

7.2 통신 설정

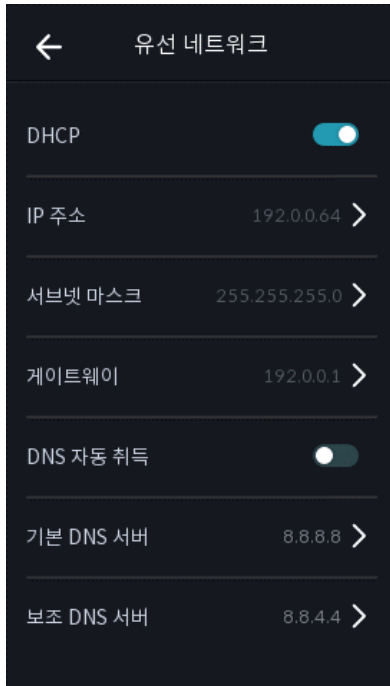
통신 설정 페이지에서 유선 네트워크, Wi-Fi, RS-485, Wiegand, ISUP 및 Guarding Vision에 대한 액세스를 설정할 수 있습니다.



7.2.1 유선 네트워크 설정

IP 주소, 서브넷 마스크, 게이트웨이 및 DNS를 포함하여 장치 유선 네트워크를 설정할 수 있습니다.

- ❶ 통신을 눌러 메인 페이지에서 통신 설정 페이지로 들어갑니다.
- ❷ 통신 설정 페이지에서 유선 네트워크를 탭합니다.



[유선 네트워크 설정]

- ❸ IP 주소, 서브넷 마스크, 게이트웨이를 설정합니다.
 - DHCP를 활성화하면 시스템이 IP 주소, 서브넷 마스크 및 게이트웨이를 자동으로 할당합니다.
 - DHCP를 비활성화하고 IP 주소, 서브넷 마스크 및 게이트웨이를 수동으로 설정해야 합니다.



• 장치의 IP 주소와 컴퓨터 IP 주소는 동일한 IP 세그먼트에 있어야 합니다.

- ❹ DNS를 설정합니다.
Auto Obtain DNS를 활성화하고 선호하는 DNS 서버와 대체 DNS 서버를 설정할 수 있습니다.

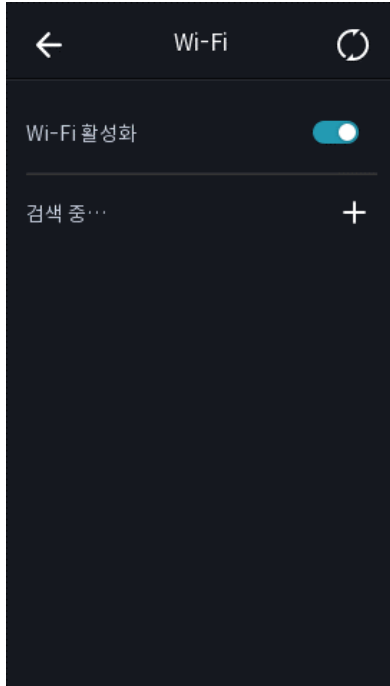
7.2.2 Wi-Fi 설정

Wi-Fi 기능을 활성화하고 Wi-Fi를 설정할 수 있습니다.



• 해당 기능은 장치에서 지원해야 합니다.

- 1 통신을 눌러 메인 페이지에서 통신 설정 페이지로 들어갑니다.
- 2 통신 설정 페이지에서 Wi-Fi를 탭합니다.




[Wi-Fi 설정]

- 3 Wi-Fi 기능을 활성화합니다.
- 4 Wi-Fi를 구성합니다.
 - 목록에서 Wi-Fi를 선택하고 Wi-Fi의 비밀번호를 입력합니다. 확인을 누릅니다.
 - 대상 Wi-Fi가 목록에 없으면 Wi-Fi 추가를 누릅니다. Wi-Fi의 이름과 비밀번호를 입력합니다. 그리고 확인을 누릅니다.



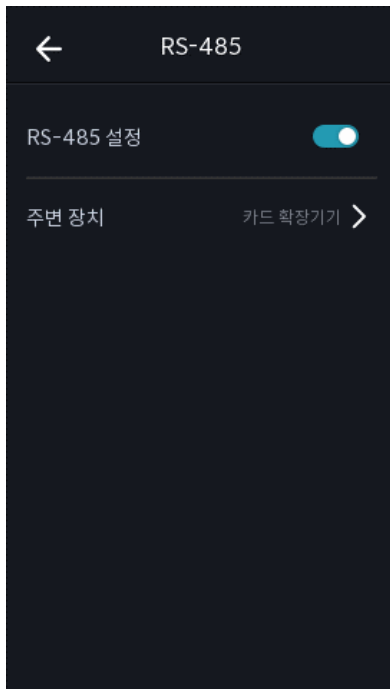
• 비밀번호는 숫자, 영문, 특수문자만 가능합니다.

- 5 Wi-Fi를 설정합니다.
 - 기본적으로 DHCP는 활성화되어 있습니다. 시스템은 IP 주소, 서브넷 마스크 및 게이트웨이를 자동으로 할당합니다.
 - DHCP를 비활성화하는 경우 IP 주소, 서브넷 마스크 및 게이트웨이를 수동으로 입력해야 합니다.
- 6 확인을 눌러 설정을 저장하고 Wi-Fi 탭으로 돌아갑니다.
- 7  을 눌러 네트워크를 저장합니다.

7.2.3 RS-485 설정

얼굴인식단말기는 RS-485단자를 통해 외부출입통제기, 보안도어제어장치, 카드리더기를 연결할 수 있습니다.

- 1 통신을 눌러 메인 페이지에서 통신 설정 페이지로 들어갑니다.
- 2 통신 설정 페이지에서 RS-485를 눌러 RS-485 탭으로 들어갑니다.



[RS-485 설정]

- ❸ 실제 필요에 따라 주변 장치 유형을 선택하십시오.



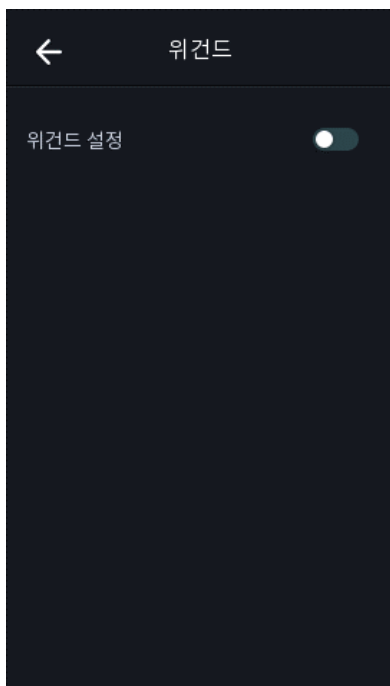
• Access Controller를 선택한 경우: RS-485 인터페이스를 통해 장치를 터미널에 연결하는 경우 RS-485 주소를 2로 설정합니다.
장치를 컨트롤러에 연결하는 경우 출입문 번호에 따라 RS-485 주소를 설정합니다.

- ❹ 왼쪽 상단의 뒤로 아이콘을 탭하고 매개 변수를 변경하는 경우 장치를 재부팅해야 합니다.

7.2.4 Wiegand 설정

Wiegand 전송 방향을 설정할 수 있습니다.

- ❶ 통신을 눌러 메인 페이지에서 통신 설정 페이지로 들어갑니다.
❷ 통신 설정 페이지에서 Wiegand를 눌러 Wiegand 탭으로 들어갑니다.



[Wiegand 설정]

- ❸ Wiegand 기능을 활성화합니다.

- ❹ 전송 방향을 선택합니다.

• 출력: 얼굴 인식 단말기는 외부 액세스 컨트롤러를 연결할 수 있습니다.
그리고 두 장치는 Wiegand 26 또는 Wiegand 34를 통해 카드 번호를 전송합니다.

- ❺  을 눌러 네트워크를 저장합니다.



• 외부 장치를 변경하고 장치 설정을 저장하면 장치가 자동으로 재부팅됩니다.

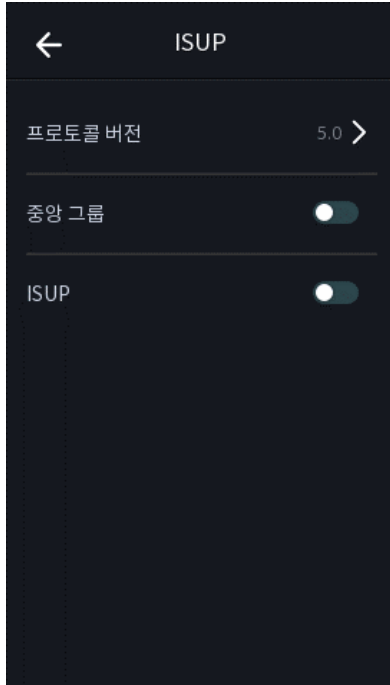
7.2.5 ISUP 설정

ISUP를 설정하면 장치가 ISUP 프로토콜을 통해 데이터를 업로드할 수 있습니다.

시작하기 전에

- 장치가 네트워크에 연결되어 있는지 확인하십시오.

① 통신을 눌러 메인 페이지에서 ISUP 설정 페이지로 들어갑니다.



[ISUP 설정]

② ISUP 기능을 활성화하고 ISUP 서버를 설정합니다.

- **ISUP 버전:** 실제 필요에 따라 ISUP 버전을 설정하십시오.
- **중앙 그룹:** 중앙 그룹을 활성화하면 데이터가 중앙 그룹에 업로드됩니다.
- **메인 채널:** N1 또는 없음을 지원합니다.
- **ISUP:** ISUP 기능을 활성화하면 데이터가 EHome 프로토콜을 통해 업로드됩니다.
- **주소 유형:** 실제 필요에 따라 주소 유형을 선택하십시오.
- **IP 주소:** ISUP 서버의 IP 주소를 설정합니다.
- **포트 번호:** ISUP 서버의 포트 번호를 설정합니다.



- 포트 번호 범위: 0 ~ 65535

- **장치 아이디:** 장치 일련 번호를 설정합니다.
- **비밀번호:** V5.0을 선택한 경우 계정과 ISUP 키를 생성해야 합니다. 다른 버전을 선택하면 ISUP 계정만 생성해야 합니다.



- ISUP 계정과 ISUP 키를 기억하십시오. 장치가 ISUP 프로토콜을 통해 다른 플랫폼과 통신해야 하는 경우 계정 이름 또는 키를 입력해야 합니다.
- ISUP 키 범위: 8~32자

7.2.6 플랫폼 액세스

Guarding Vision 모바일 클라이언트에 장치를 추가하기 전에 장치 확인 코드를 변경하고 서버 주소를 설정할 수 있습니다.

시작하기 전에

- 장치가 네트워크에 연결되어 있는지 확인하십시오.

① 통신을 눌러 메인 페이지에서 통신 설정 페이지로 들어갑니다.

② Communication Settings(통신 설정) 페이지에서 Access to Guarding Vision을 탭합니다.

③ 보호 비전에 대한 액세스 활성화

④ 서버 IP를 입력합니다.

⑤ 인증 코드를 생성하고, Guarding Vision을 통해 기기를 관리할 때 인증 코드를 입력해야 합니다.

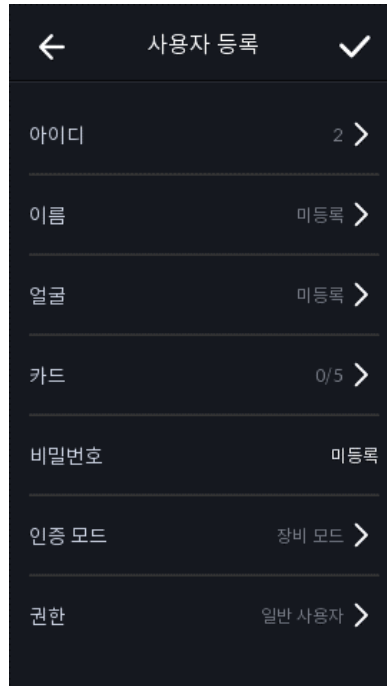
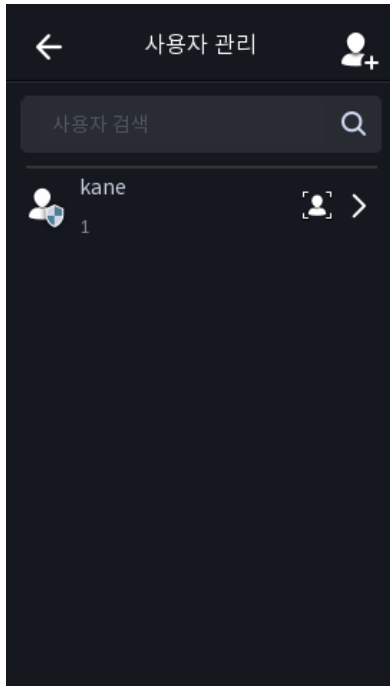
7.3 사용자 관리

사용자 관리 인터페이스에서 사용자를 추가, 수정, 삭제 및 검색할 수 있습니다.

7.3.1 사용자 추가

관리자는 로그인하고 사용자를 추가할 수 있습니다.

- ❶ 초기 페이지를 길게 탭하고 백엔드에 로그인합니다.
- ❷ **사용자** → **+**를 눌러 사용자 추가 페이지로 들어갑니다.



- ❸ **사용자 ID**를 수정합니다.



- 사용자 ID는 32자 미만이어야 합니다. 그리고 소문자, 대문자, 숫자의 조합이 될 수 있습니다.
- 사용자 ID는 중복되어서는 안됩니다.

- ❹ **이름** 필드를 누르고 사용자 이름을 입력합니다.



- 사용자 이름에는 숫자, 영문 대문자, 소문자 및 특수 문자를 사용할 수 있습니다.
- 사용자 이름은 최대 32자까지 허용됩니다.

- ❺ 옵션: **얼굴 사진, 지문, 카드**를 추가합니다.



- 얼굴 사진 추가에 대한 자세한 내용은 다음을 참조하세요. [\[얼굴 사진 추가\]](#)
- 카드 추가에 대한 자세한 내용은 다음을 참조하십시오. [\[카드 추가\]](#)
- 비밀번호 추가에 대한 자세한 내용은 다음을 참조하십시오. [\[PIN 코드 보기\]](#)

- ❻ 옵션: 인증 유형을 설정하십시오.




- 인증 유형 설정에 대한 자세한 내용은 다음을 참조하십시오. [\[인증 모드 설정\]](#)

- ❼ 권한 기능을 활성화합니다.

관리자 권한 활성화

일반 출석 기능을 제외하고 사용자는 권한 인증 후 홈 페이지에 진입하여 동작할 수도 있습니다.

- ❽  을 눌러 설정을 저장합니다.

7.3.2 사용자 얼굴 등록

장치에 사용자의 얼굴 사진을 등록합니다. 그리고 사용자는 얼굴 사진을 사용하여 인증할 수 있습니다.



• 최대 2000개의 얼굴 사진을 추가할 수 있습니다.

❶ 초기 페이지를 3초 동안 길게 탭한 후 제스처를 따라 좌/우로 슬라이드하고 백엔드에 로그인합니다.

❷ 사용자 → +를 눌러 사용자 추가 페이지로 들어갑니다.

❸ 사용자 ID를 수정합니다.



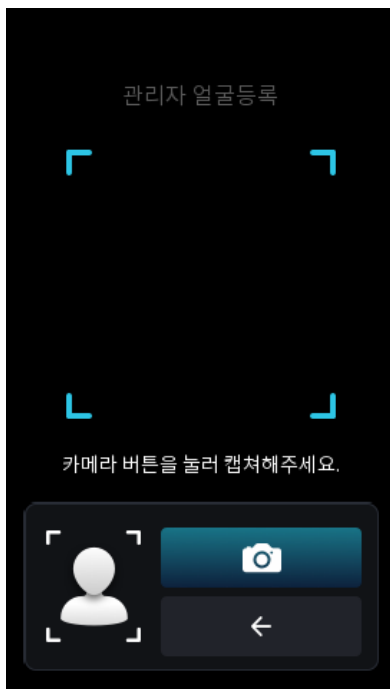
• ID는 32자 미만이어야 합니다. 그리고 소문자, 대문자, 숫자의 조합이 될 수 있습니다.
• ID는 중복되어서는 안됩니다.

❹ 이름 필드를 누르고 소프트 키보드에서 사용자 이름을 입력합니다.



• 사용자 이름에는 숫자, 대문자, 소문자 및 특수 문자를 사용할 수 있습니다.
• 제안된 사용자 이름은 32자 이내여야 합니다.

❺ 얼굴 필드를 눌러 얼굴 사진 추가 페이지로 들어갑니다.



[얼굴 등록 추가]

❻ 카메라를 바라보세요.

얼굴 사진 추가가 완료되면 캡처된 얼굴 사진이 페이지 오른쪽 상단에 표시됩니다.



• 얼굴 사진을 추가할 때 얼굴이 얼굴 사진 윤곽선에 있는지 확인하세요.
• 캡처한 얼굴 사진의 품질이 좋고 정확한지 확인하세요.
• 얼굴 사진 추가 지침에 대한 자세한 내용은 다음을 참조하십시오. [\[얼굴 사진 수집/비교 시 팁\]](#)


❼ 저장을 눌러 얼굴 사진을 저장합니다.

❽ 선택 사항: 다시 시도를 탭하고 얼굴 위치를 조정하여 얼굴 사진을 다시 추가합니다.

❾ 사용자 권한을 설정합니다.

관리자: 일반 출석 기능을 제외하고 사용자는 권한 인증 후 홈 페이지에 진입하여 동작할 수도 있습니다.

일반 사용자: 사용자는 초기 화면에서만 인증 또는 출석을 할 수 있습니다.

❿  을 눌러 설정을 저장합니다.

7.3.4 카드 추가

사용자를 위한 카드를 추가하면 사용자는 추가된 카드를 통해 인증할 수 있습니다.



• 최대 2000개의 카드를 추가할 수 있습니다.

- ❶ 초기 페이지를 3초 동안 길게 탭한 후 제스처를 따라 좌/우로 슬라이드하고 백엔드에 로그인합니다.
- ❷ 사용자 → +를 눌러 **사용자 추가 페이지**로 들어갑니다.
- ❸ 배선도에 따라 외부 카드 리더기를 연결합니다.
- ❹ 직원 ID를 탭합니다. 입력하고 직원 ID를 편집합니다.



• ID는 32자 미만이어야 합니다. 그리고 소문자, 대문자, 숫자의 조합이 될 수 있습니다.
• ID는 중복되어서는 안됩니다.

- ❺ 이름 필드를 누르고 소프트 키보드에서 사용자 이름을 입력합니다.



• 사용자 이름에는 숫자, 대문자, 소문자 및 특수 문자를 사용할 수 있습니다.
• 제안된 사용자 이름은 32자 이내여야 합니다.

- ❻ 카드 필드를 탭하고 +를 탭합니다.
- ❼ 카드번호를 설정합니다.
카드 번호를 수동으로 입력하십시오. 카드 제시 영역에 카드를 제시하면 카드 번호를 얻을 수 있습니다.



• 카드 번호는 비워둘 수 없습니다.
• 카드번호는 최대 20자까지 가능합니다.
• 카드번호는 중복될 수 없습니다.

- ❽ 카드 유형을 구성합니다.
- ❾ 사용자 권한을 설정합니다.
관리자: 일반 출석 기능을 제외하고 사용자는 권한 인증 후 홈 페이지에 진입하여 동작할 수도 있습니다.
일반 사용자: 사용자는 초기 화면에서만 인증 또는 출석을 할 수 있습니다.

- ❿ 을 눌러 설정을 저장합니다.

7.3.5 PIN 코드 보기

사용자를 위한 PIN 코드를 추가하면 사용자는 PIN 코드를 통해 인증할 수 있습니다.

- ❶ 초기 페이지를 3초 동안 길게 탭한 후 제스처를 따라 좌/우로 슬라이드하고 백엔드에 로그인합니다.
- ❷ 사용자 → +를 눌러 **사용자 추가 페이지**로 들어갑니다.
- ❸ ID를 탭합니다. 입력하고 ID를 편집합니다.



• ID는 32자 미만이어야 합니다. 그리고 소문자, 대문자, 숫자의 조합이 될 수 있습니다.
• ID는 중복되어서는 안됩니다.

- ❹ 이름 필드를 누르고 소프트 키보드에서 사용자 이름을 입력합니다.



• 사용자 이름에는 숫자, 대문자, 소문자 및 특수 문자를 사용할 수 있습니다.
• 제안된 사용자 이름은 32자 이내여야 합니다.

- ❺ PIN 코드를 보려면 PIN 코드를 누릅니다.



• PIN 코드는 편집할 수 없습니다. 플랫폼에서만 적용할 수 있습니다.

- ❻ 사용자 권한을 설정합니다.
관리자: 일반 출석 기능을 제외하고 사용자는 권한 인증 후 홈 페이지에 진입하여 동작할 수도 있습니다.
일반 사용자: 사용자는 초기 화면에서만 인증 또는 출석을 할 수 있습니다.
- ❼ 을 눌러 설정을 저장합니다.

7.3.6 인증 모드 설정


사용자의 얼굴 사진, 비밀번호 또는 기타 자격 증명을 추가한 후 인증 모드를 설정해야 하며 사용자는 구성된 인증 모드를 통해 자신의 신원을 인증할 수 있습니다.

- ① 초기 페이지를 3초 동안 길게 탭한 후 제스처를 따라 좌/우로 슬라이드하고 백엔드에 로그인합니다.
- ② 사용자 → 사용자 추가/사용자 편집 → 인증 모드를 누릅니다.
- ③ 인증 모드로 장치 또는 사용자 지정을 선택합니다.

장치: 장치 모드를 선택하려면 먼저 접근 제어 설정 페이지에서 단말기 인증 모드를 설정해야 합니다.

자세한 내용은 액세스 제어 설정을 참조하십시오.


사용자 설정: 실제 필요에 따라 서로 다른 인증 모드를 결합할 수 있습니다.

- ④  을 눌러 설정을 저장합니다.

7.3.7 사용자 검색 및 편집

사용자를 추가한 후 사용자를 검색하고 편집할 수 있습니다.

사용자 검색

사용자 관리 페이지에서 검색 영역을 탭하여 사용자 검색 페이지로 들어갑니다. 페이지 왼쪽의 카드를 누르고 드롭다운 목록에서 검색 유형을 선택합니다. 사원번호, 카드번호 또는 사용자 이름을 입력하여 검색합니다. 검색하려면  을 누르십시오.

사용자 편집

사용자 관리 페이지의 사용자 목록에서 사용자를 선택하여 사용자 편집 페이지로 들어갑니다.

7.3 사용자관리의 단계 따라 편집합니다.  를 눌러 설정을 저장합니다.



• 직원 ID는 수정할 수 없습니다.

7.4 데이터 관리

데이터를 삭제하고, 데이터를 가져오고, 데이터를 내보낼 수 있습니다.

7.4.1 데이터 삭제

사용자 데이터를 삭제합니다.

메인 페이지에서 데이터 → 데이터 삭제 → 사용자 데이터를 선택하세요. 장치에 추가된 모든 사용자 데이터가 삭제됩니다.

7.4.2 데이터 가져오기

- ① 장치에 USB 플래시 드라이브를 연결합니다.
- ② 메인 페이지에서 데이터 → 데이터 가져오기를 누릅니다.
- ③ 사용자 데이터, 얼굴 데이터 또는 액세스 제어를 누릅니다.



• 가져온 액세스 제어는 장치의 구성 파일입니다.

- ④ 데이터를 내보낼 때 생성한 비밀번호를 입력합니다. 데이터를 내보낼 때 암호를 생성하지 않은 경우 입력 상자를 공백으로 두고 즉시 확인을 누릅니다.



- 한 장치(장치 A)에서 다른 장치(장치 B)로 모든 사용자 정보를 전송하려면 장치 A에서 USB 플래시 드라이브로 정보를 내보낸 다음 USB 플래시 드라이브에서 장치 B로 정보를 가져와야 합니다. 이 경우, **프로필 사진을 가져오기 전에 사용자 데이터를 가져와야 합니다.**
- 지원되는 USB 플래시 드라이브 형식은 FAT32입니다.
- 가져온 사진은 루트 디렉토리의 이름이 registered_pic인 폴더에 저장되어야 하며 **사진의 이름은 아래 규칙을 따라야 합니다.**
카드번호.이름.부서.사용자ID.성별.jpg
- registered_pic 폴더가 가져온 모든 사진을 저장할 수 없는 경우 루트 디렉터리 아래에 registered_pic1, registered_pic2, registered_pic3, registered_pic4라는 이름의 다른 폴더를 만들 수 있습니다.
- ID는 32자 미만이어야 합니다. 소문자, 대문자, 숫자의 조합일 수 있습니다. 중복되지 않아야 하며 0으로 시작하지 않아야 합니다.
- 얼굴 사진의 요구 사항은 다음 규칙을 따라야 합니다.
카메라를 정면으로 향하고 정면에서 촬영해야 합니다. 얼굴 사진을 찍을 때 모자나 머리 덮개를 착용하지 마십시오.
형식은 JPEG 또는 JPG여야 합니다. 해상도는 640×480픽셀 이상 또는 640×480픽셀 이상이어야 합니다.
그림 크기는 60KB에서 200KB 사이여야 합니다.

7.4.3 데이터 내보내기

- ❶ 장치에 USB 플래시 드라이브를 연결합니다.
- ❷ 메인 페이지에서 데이터 → 데이터 내보내기를 누릅니다.
- ❸ 얼굴 데이터, 이벤트 데이터, 사용자 데이터 또는 액세스 제어를 누릅니다.



• 내보낸 액세스 제어는 장치의 구성 파일입니다.

- ❹ 옵션: 내보내기를 위한 비밀번호를 생성하십시오. 해당 데이터를 다른 장치로 가져올 때 암호를 입력해야 합니다.



• 지원되는 USB 플래시 드라이브 형식은 DB입니다.
 • 시스템은 1G에서 32G까지의 스토리지가 있는 USB 플래시 드라이브를 지원합니다. USB 플래시 드라이브의 여유 공간이 512M 이상인지 확인하십시오.
 • 내보낸 사용자 데이터는 편집할 수 없는 DB 파일입니다.

7.5 인증

네트워크 구성, 시스템 구성 및 사용자 구성 후 ID 인증을 위한 초기 페이지로 돌아갈 수 있습니다. 시스템은 구성된 인증 모드에 따라 사람을 인증합니다.

7.5.1 단일 인증

인증 전에 사용자 인증 유형을 설정합니다. 자세한 내용은 다음을 참조하십시오. [\[인증 모드 설정\]](#)
 얼굴 또는 카드를 인증합니다.

얼굴: 카메라를 정면으로 바라보고 얼굴 인증을 시작합니다.

카드: 카드 태그 영역에 카드를 태그하고 카드를 통한 인증을 시작합니다.



• 카드는 일반 IC 카드이거나 암호화된 카드일 수 있습니다.

핀코드: PIN 코드를 통해 인증하려면 핀 코드를 입력하십시오.

인증이 완료되면 "인증 완료"에 대한 안내멘트, 인증완료의 화면 표시가 됩니다.

7.5.2 멀티 인증

시작하기 전에

인증 전에 사용자 인증 유형을 설정합니다. 자세한 내용은 다음을 참조하십시오. [\[인증 모드 설정\]](#)

- ❶ 인증 모드가 카드와 얼굴, 비밀번호와 얼굴, 카드와 비밀번호, 카드와 얼굴인 경우 라이브 뷰 페이지의 안내에 따라 크리덴셜을 인증합니다.



• 카드는 일반 IC 카드이거나 암호화된 카드일 수 있습니다.

- ❷ 이전 자격 증명이 인증된 후 다른 자격 증명을 계속 인증합니다.



• 얼굴 인증에 대한 자세한 내용은 얼굴 사진 수집/비교 시 팁을 참조하십시오.

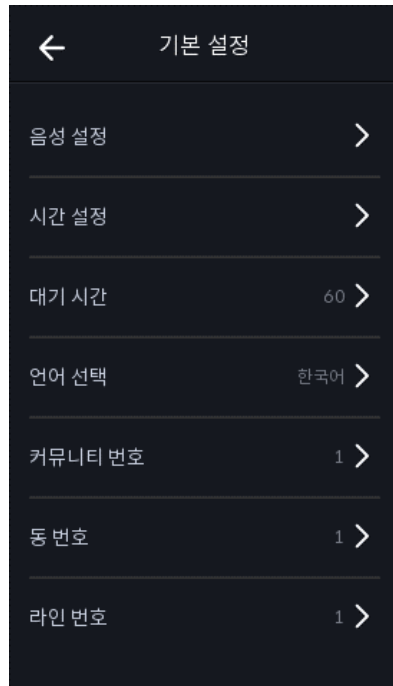
- ❸ 인증이 완료되면 "인증 완료"에 대한 안내멘트, 인증완료의 화면 표시가 됩니다.

7.6 기본 설정

음성설정(소리설정), 시간, 대기, 언어, 커뮤니티 번호, 동 번호, 라인번호를 설정할 수 있습니다.

초기 페이지를 3초 동안 길게 탭하고 제스처를 따라 왼쪽/오른쪽으로 슬라이드한 다음 장치 메인 페이지에 로그인합니다.

기본을 탭합니다.



[기본 설정 페이지]

음성 설정: 음성 안내 기능을 활성화/비활성화하고 음성 볼륨을 조절할 수 있습니다.



• 음성 볼륨은 0~10까지 설정할 수 있습니다.

시간 설정: 시간대, 장치 시간 및 DST를 설정합니다.

대기 시간 설정: 장치 절전 대기 시간을 설정합니다. 예를 들어, 초기 페이지에서 대기 시간을 30초로 설정하면 30초 후 아무런 동작 없이 장치가 절전 모드로 전환됩니다.



• 20초에서 999초까지 구성할 수 있습니다.

언어 선택: 실제 필요에 따라 언어를 선택하십시오.

커뮤니티 번호: 장치가 설치된 커뮤니티 번호를 설정합니다.

동 번호: 장치가 설치된 동 번호를 설정합니다.

라인 번호: 장치 장착 라인 번호를 설정합니다.

7.7 생체 설정

얼굴을 사용자 정의하여 얼굴 인식 성능을 향상시킬 수 있습니다. 구성 가능한 설정에는 선택 적용 모드, 얼굴 활성 수준, 얼굴 인식 거리, 얼굴 인식 간격, 얼굴 1:N 보안 수준, 얼굴 1:1 보안 수준, ECO 설정 및 마스크 감지가 있는 얼굴이 포함됩니다.

초기 페이지를 3초 동안 길게 탭하고 메인 페이지에 로그인합니다.

생체 인식을 탭합니다.

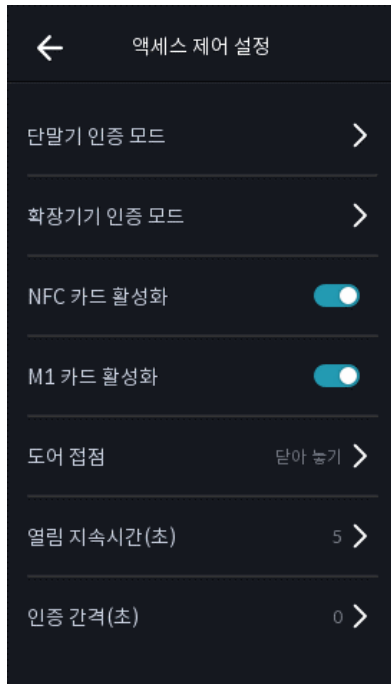


[기본 설정 페이지]

모수	설명
애플리케이션 모드 선택	실제 환경에 따라 기타 또는 실내를 선택하십시오.
얼굴 실시간 레벨	얼굴 위조 방지 기능을 활성화한 후 실시간 얼굴 인증을 수행할 때 일치하는 보안 수준을 설정할 수 있습니다.
얼굴 인식 거리	인증 시 사용자와 카메라 사이의 유효한 거리를 설정합니다.
얼굴 인식 간격	인증 시 두 번의 지속적인 얼굴 인식 사이의 시간 간격입니다. ① 1부터 10까지 숫자를 입력할 수 있습니다.
얼굴 1:N 보안 레벨	1:N 매칭 방식으로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.
얼굴 1:1 보안 레벨	1:1 매칭 방식으로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.
ECO 설정	<p>ECO 모드를 활성화하면 장치는 IR 카메라를 사용하여 어둡거나 어두운 환경에서 얼굴을 인증합니다. 그리고 ECO 모드 임계값, ECO 모드(1:N), ECO 모드(1:1), Face with mask & face(1:1 ECO), Face with mask & face(1:N ECO)를 설정할 수 있습니다.</p> <p>ECO 임계값 ECO 모드를 활성화하면 ECO 모드의 임계값을 설정할 수 있습니다. 값이 클수록 장치가 ECO 모드로 더 쉽게 진입합니다.</p> <p>에코 모드(1:1) ECO 모드 1:1 매칭 모드로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p> <p>에코 모드(1:N) ECO 모드 1:N 매칭 모드로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p> <p>마스크를 쓴 얼굴 & 얼굴 (1:1 ECO) ECO 모드 1:1 매칭 모드를 통해 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p> <p>마스크를 쓴 얼굴 & 얼굴 (1:N ECO) ECO 모드 1:N 매칭 모드를 통해 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p>
마스크 감지 기능이 있는 얼굴	<p>마스크 감지로 얼굴을 활성화하면 시스템이 마스크 사진으로 캡처된 얼굴을 인식합니다. 마스크와 얼굴의 1:N 레벨과 전략을 설정할 수 있습니다.</p> <p>전략 없음, 착용 알림 및 필수 착용 전략을 설정합니다.</p> <p>착용 알림 인증 시 마스크를 착용하지 않은 경우 장치에서 알림 메시지를 표시하고 문이 열립니다.</p> <p>필수 착용 인증 시 마스크를 착용하지 않으면 장치에서 알림을 표시하고 문이 닫힌 상태를 유지합니다.</p> <p>없음 인증할 때 사람이 안면 마스크를 착용하지 않으면 장치에서 알림 메시지를 표시하지 않습니다.</p> <p>마스크를 쓴 얼굴 & 얼굴 (1:1) 1:1 매칭 방식으로 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p> <p>마스크를 쓴 얼굴 & 얼굴 (1:N) 1:N 매칭 방식으로 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.</p>

7.8 액세스 제어 설정

인증 모드, NFC 카드 활성화, M1 카드 활성화, 도어 컨택트, 개방 시간 및 인증 간격 기능을 포함한 액세스 제어 권한을 설정할 수 있습니다. 메인 페이지에서 ACS(액세스 제어 설정)를 눌러 액세스 제어 설정 페이지로 들어갑니다.
이 페이지에서 액세스 제어 설정을 편집합니다.



[액세스 제어 설정]

사용 가능한 설정 설명은 다음과 같습니다

모수	설명
단말기 인증 모드	<p>얼굴인식단말기의 인증모드를 선택합니다. 인증 모드를 사용자 정의할 수도 있습니다.</p> <p>i</p> <ul style="list-style-type: none"> 지문 모듈이 탑재된 기기만 지문 관련 기능을 지원합니다. 생체 인식 제품은 스푸핑 방지 환경에 100% 적용되지 않습니다. 더 높은 보안 수준이 필요한 경우 여러 인증 모드를 사용하십시오. 다중 인증 방식을 채택하는 경우, 얼굴을 인증하기 전에 다른 인증 방식을 먼저 인증해야 합니다.
확장기기 인증 모드 (카드리더 인증모드)	카드 리더의 인증 모드를 선택합니다.
NFC 카드 활성화	기능을 활성화하고 NFC 카드를 제시하여 인증할 수 있습니다.
M1 카드 활성화	기능을 활성화하고 인증을 위해 M1 카드를 제시할 수 있습니다.
도어 접점	실제 필요에 따라 "Open(열림 유지)" 또는 "Close(Remian Closed)"를 선택할 수 있습니다. 기본적으로 Close(Remian Closed)입니다.
열림 지속 시간(초)	문 잠금 해제 시간을 설정합니다. 설정된 시간 동안 문을 열지 않으면 문이 잠깁니다. 사용 가능한 문 잠김 시간 범위: 1 ~ 255초.
인증 간격	장치 인증 간격을 설정합니다. 사용 가능한 인증 간격 범위: 0 ~ 65535.

7.9 근퇴(체크인/아웃) 설정

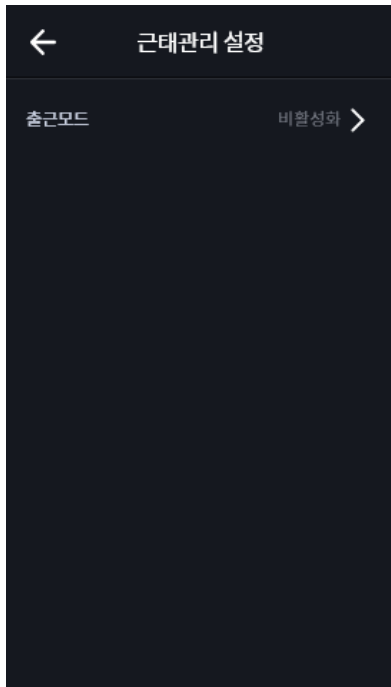
실제 상황에 따라 출석 모드를 체크인, 체크 아웃, 휴식, 휴식, 초과 근무 및 초과 근무로 설정할 수 있습니다.



• 이 기능은 클라이언트 소프트웨어의 근태 기능과 함께 사용해야 합니다.

7.9.1 장치를 통한 출석 모드 비활성화

근태 모드를 비활성화하면 시스템은 초기 화면에 근태 상태를 표시하지 않습니다.
근태 상태를 탭하여 근태 상태 페이지로 들어갑니다.



[출석 모드 비활성화]

출석 모드를 비활성화로 설정하십시오.

초기 페이지에서 출석 상태를 보거나 구성하지 않습니다. 그리고 시스템은 플랫폼에 구성된 출석 규칙을 따릅니다.

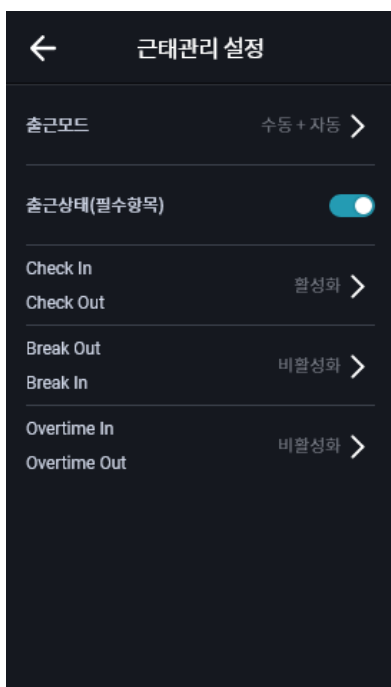
7.9.2 장치를 통한 수동 근태 설정

출석 모드를 수동으로 설정하고 출석을 할 때 수동으로 상태를 선택해야 합니다.

시작하기 전에

하나 이상의 사용자를 추가하고 사용자의 인증 모드를 설정합니다. 자세한 내용은 사용자 관리를 참조하십시오.

- ❶ 근태상태를 눌러 근태상태 화면으로 들어갑니다.
- ❷ 출석 모드를 수동으로 설정합니다.



[수동 출석 모드]

❸ 출석 상태 필수를 활성화합니다.

❹ 출석 상태 그룹을 활성화합니다.



• 출석 속성은 변경되지 않습니다.

❺ 옵션: 상태를 선택하고 필요한 경우 이름을 변경합니다.

근태관리 페이지와 인증결과 페이지에 이름이 표시됩니다.

결과: 인증 후 출석 상태를 수동으로 선택해야 합니다.



• 상태를 선택하지 않으면 인증에 실패하며 유효한 출석으로 표시되지 않습니다.

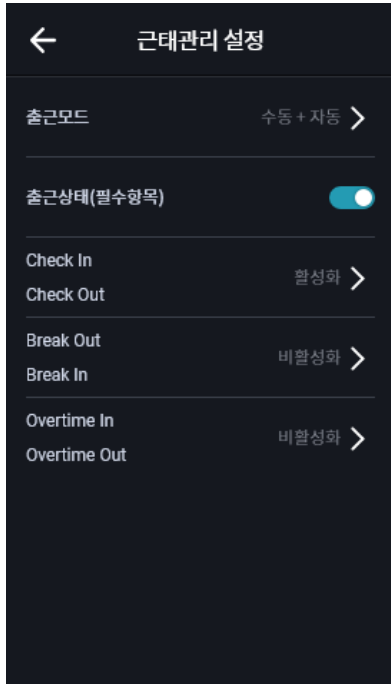
7.9.3 장치를 통한 자동 출결 설정

근태모드를 자동으로 설정하면 근태현황과 출석일정을 설정할 수 있습니다.
시스템은 구성된 일정에 따라 출석 상태를 자동으로 변경합니다.

시작하기 전에

하나 이상의 사용자를 추가하고 사용자의 인증 모드를 설정합니다. 자세한 내용은 사용자 관리를 참조하십시오.

- ① 근태상태를 눌러 근태상태 화면으로 들어갑니다.
- ② 출석 모드를 자동으로 설정합니다.



[자동 출석 모드]

- ③ 출석 상태 기능을 활성화합니다.
- ④ 출석 상태 그룹을 활성화합니다.



• 출석 속성은 변경되지 않습니다.

- ⑤ 옵션: 상태를 선택하고 필요한 경우 이름을 변경합니다.
근태관리 페이지와 인증결과 페이지에 이름이 표시됩니다.
- ⑥ 상태의 일정을 설정합니다.
 - 1) 출석 일정을 탭합니다.
 - 2) 월요일, 화요일, 수요일, 목요일, 금요일, 토요일 또는 일요일을 선택합니다.
 - 3) 선택한 근태현황의 시작시간을 설정합니다.
 - 4) 확인을 누릅니다.
 - 5) 실제 필요에 따라 1~4단계를 반복합니다.



• 출석 상태는 구성된 일정 내에서 유효합니다.

결과: 초기 화면에서 인증을 하면 설정된 일정에 따라 설정된 근태 상태로 인증이 표시됩니다.

예)

Break Out을 월요일 11:00으로 설정하고 Break In을 월요일 12:00으로 설정하면 월요일 11:00부터 12:00까지 유효한 사용자의 인증이 중단으로 표시됩니다.

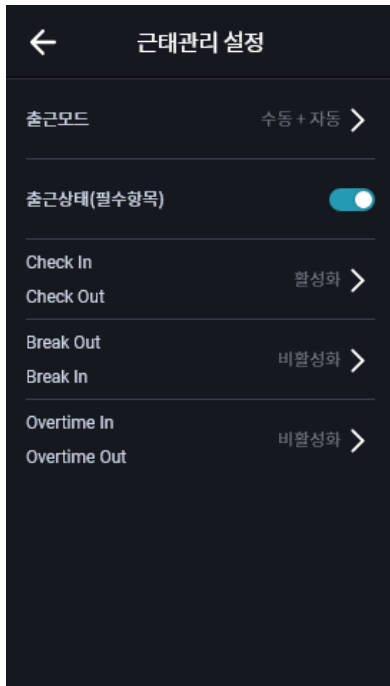
7.9.4 장치를 통한 수동 및 자동 출석 설정

근태 모드를 수동 및 자동으로 설정하면 구성된 일정에 따라 시스템이 자동으로 근태 상태를 변경합니다.
동시에 인증 후 출석 상태를 수동으로 변경할 수 있습니다.

시작하기 전에

하나 이상의 사용자를 추가하고 사용자의 인증 모드를 설정합니다. 자세한 내용은 사용자 관리를 참조하십시오.

- ❶ 근태상태를 눌러 근태상태 화면으로 들어갑니다.
- ❷ 출석 모드를 수동 및 자동으로 설정합니다.



[수동 및 자동 모드]

- ❸ 출석 상태 기능을 활성화합니다.
- ❹ 출석 상태 그룹을 활성화합니다.



• 출석 속성은 변경되지 않습니다.

- ❺ 옵션: 상태를 선택하고 필요한 경우 이름을 변경합니다.
근태관리 페이지와 인증결과 페이지에 이름이 표시됩니다.
- ❻ 상태의 일정을 설정합니다.
 - 1) 출석 일정을 탭합니다.
 - 2) 월요일, 화요일, 수요일, 목요일, 금요일, 토요일 또는 일요일을 선택합니다.
 - 3) 선택한 근태현황의 시작시간을 설정합니다.
 - 4) 확인을 누릅니다.
 - 5) 실제 필요에 따라 1~4단계를 반복합니다.



• 출석 상태는 구성된 일정 내에서 유효합니다.

결과: 초기 페이지에서 인증합니다. 인증은 일정에 따라 구성된 근태 상태로 표시됩니다. 결과 탭에서 편집 아이콘을 탭하면 수동으로 출결 상태를 선택할 수 있으며 인증은 편집된 근태 상태로 표시됩니다.

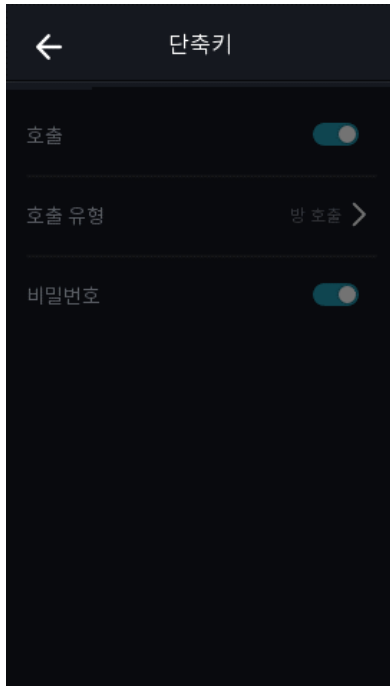
예)

Break Out을 월요일 11:00으로 설정하고 Break In을 월요일 12:00으로 설정하면 월요일 11:00부터 12:00까지 유효한 사용자의 인증이 중단으로 표시됩니다.

7.10 단축키 설정

단축키 설정을 변경할 수 있습니다.

❶ 기타 → 단축키 설정을 눌러 설정 페이지로 들어갑니다.



[기본 설정]

단축키: QR 코드 기능, 통화 기능, 통화 종류, 비밀번호 입력 기능 등 인증 페이지에 표시되는 단축키를 선택합니다.



Call Room, Call Center, Call Specified Room No., Call APP 중에서 호출 방식을 선택할 수 있습니다.

Call Room

인증 화면에서 통화 버튼을 누를 때 방 번호를 눌러야 통화가 됩니다.

Call Center

인증 페이지에서 통화 버튼을 누르면 센터로 바로 전화를 걸 수 있습니다.

지정된 방 번호를 호출합니다.

방 번호를 설정해야 합니다. 인증 페이지에서 통화 버튼을 누르면 전화를 걸지 않고 구성된 방으로 바로 전화를 걸 수 있습니다.

전화 앱

인증 페이지에서 통화 버튼을 누르면 디바이스가 추가된 모바일 클라이언트로 전화를 겁니다.

비밀번호

이 기능을 활성화하면 비밀번호를 입력하여 비밀번호를 통해 인증할 수 있습니다.

QR 코드

인증 인터페이스에서 QR 코드 스캔 기능을 사용할 수 있습니다. 장치는 획득한 QR 코드와 관련된 정보를 플랫폼에 업로드합니다.

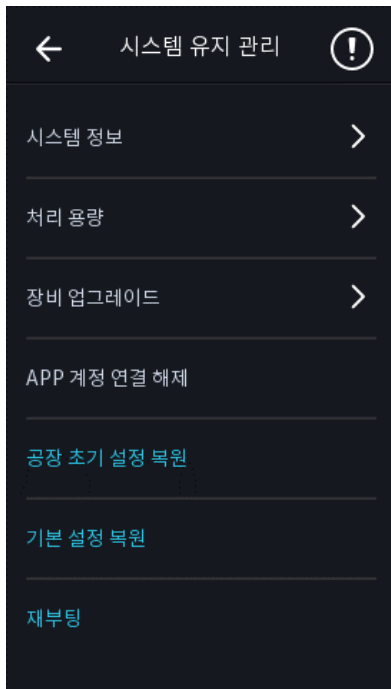
주제: 인증 페이지에서 프롬프트 창의 테마를 설정할 수 있습니다. 테마를 기본/단순으로 선택할 수 있습니다.

단순을 선택하면 인증 페이지의 라이브 뷰가 비활성화되고 그 동안 본인의 이름, 사원 ID, 얼굴 사진이 모두 숨겨집니다.

7.11 시스템 유지보수

장치 시스템 정보 및 용량을 볼 수 있습니다. 시스템을 공장 설정, 기본 설정으로 복원하고 APP 계정 연결을 해제하고 시스템을 재부팅할 수도 있습니다.

초기 페이지를 3초 동안 길게 탭하고 홈 페이지에 로그인합니다. 유지보수를 탭합니다.



[유지보수 페이지]

시스템 정보

일련 번호, 펌웨어 버전, MCU 버전, MAC 주소, 생산 데이터, 장치 QR 코드, 오픈 소스 코드 라이선스를 포함한 장치 정보를 볼 수 있습니다.



• 페이지는 장치 모델에 따라 다를 수 있습니다. 자세한 내용은 실제 페이지를 참조하십시오.

용량

관리자, 사용자, 얼굴 사진, 카드, 이벤트 번호를 볼 수 있습니다.



• 장치 모델의 일부는 지문 번호 표시를 지원합니다. 자세한 내용은 실제 페이지를 참조하십시오.

업그레이드

장치 USB 인터페이스에 USB 플래시 드라이브를 연결합니다. 업그레이드 → 확인을 누르면 장치가 USB 플래시 드라이브의 digicap.dav 파일을 읽어 업그레이드를 시작합니다.

APP 계정 연결 해제

플랫폼에서 Guarding Vision 계정의 연결을 해제합니다.

공장으로 복원

모든 설정은 공장 설정으로 복원됩니다. 적용을 위해 시스템이 재부팅됩니다.

기본값으로 복원

통신 설정, 원격으로 가져온 사용자 정보를 제외한 모든 설정은 기본 설정으로 복원됩니다. 적용을 위해 시스템이 재부팅됩니다.

재부팅

확인 후 장치가 재부팅됩니다.



을 길게 누르고 관리자 암호를 입력하여 장치 버전 정보를 봅니다.

8. 모바일 브라우저를 통한 장치 구성

8.1 로그인

모바일 브라우저를 통해 로그인할 수 있습니다.



- 모델의 일부는 Wi-Fi 설정을 지원하지합니다.
- 장치가 활성화되어 있는지 확인하십시오.

Wi-Fi가 활성화된 후 장치에서 IP 주소를 얻습니다. 장치와 컴퓨터의 IP 세그먼트가 동일한지 확인하십시오.

자세한 내용은 다음을 참조하십시오. [\[Wi-Fi 설정\]](#)

모바일 브라우저의 주소 표시줄에 장치 IP 주소를 입력하고 Enter 키를 눌러 로그인 페이지로 들어갑니다.

장치 사용자 이름과 암호를 입력합니다. 로그인을 클릭합니다.

8.2 검색 이벤트

검색을 클릭하여 검색 페이지로 들어갑니다.

사원번호, 이름, 카드번호, 시작시간, 종료시간 등 검색 조건을 입력하고 검색을 클릭합니다.



- 32자리 이내의 이름 검색을 지원합니다.

결과가 목록에 표시됩니다.

8.3 사용자 관리

모바일 웹 브라우저를 통해 사용자를 추가, 수정, 삭제, 검색할 수 있습니다.

❶ 사용자 관리를 눌러 설정 페이지로 들어갑니다.

❷ 사용자를 추가합니다.

1) +를 누릅니다.

[사용자 추가]

2) 다음을 설정합니다.

직원 ID

직원 아이디를 입력하세요. 직원 ID는 0이거나 32자를 초과할 수 없습니다. 대문자, 소문자 및 숫자의 조합일 수 있습니다.

이름

이름을 입력. 이름은 숫자, 영문 대소문자, 문자를 지원합니다. 이름은 32자 이내로 하는 것이 좋습니다.

성별

성별을 선택합니다.

사용자 직위

사용자 직위를 선택합니다.

층번호/방번호

층번호/방번호를 입력하세요.

얼굴

얼굴 사진을 추가합니다. 얼굴을 누른 다음 가져오기를 누르고 얼굴을 가져올 모드를 선택합니다.

시작일/종료일

사용자 권한의 시작 날짜 및 종료 날짜를 설정합니다.


관리자

사용자를 관리자로 설정해야 하는 경우 관리자를 활성화할 수 있습니다.

인증 유형

인증 유형을 설정합니다.

3) 저장을 탭합니다.

- ③ 사용자 목록에서 수정이 필요한 사용자를 눌러 정보를 수정합니다.
- ④ 사용자 목록에서 삭제할 사용자를 누르고  을 눌러 사용자를 삭제합니다.
- ⑤ 검색창에 직원 ID 또는 이름을 입력하여 사용자를 검색할 수 있습니다.

8.4 설정

8.4.1 장치 정보 보기

장치 이름, 언어, 모델, 일련 번호, QR 코드, 버전 등을 봅니다.

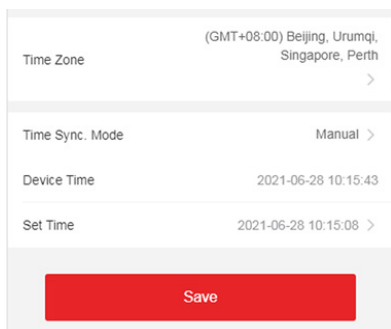
구성 → 시스템 → 시스템 설정 → 기본 정보를 눌러 구성 페이지로 들어갑니다.

장치 이름, 언어, 모델, 일련 번호, QR 코드, 버전 등을 볼 수 있습니다.

8.4.2 시간 설정

시간대, 시간 동기화를 설정합니다. 모드 및 표시된 시간.

구성 → 시스템 → 시스템 설정 → 시간 설정을 눌러 설정 페이지로 들어갑니다.



[시간 설정]

저장을 탭하여 설정을 저장합니다.

시간대

드롭다운 목록에서 장치가 위치한 시간대를 선택합니다.

시간 동기화 방법

수동: 기본적으로 장치 시간은 수동으로 동기화해야 합니다. 장치 시간을 수동으로 설정할 수 있습니다.

NTP: NTP 서버의 IP 주소, 포트 번호 및 간격을 설정합니다.

8.4.3 오픈 소스 소프트웨어 라이선스 보기

구성 → 시스템 → 시스템 설정 → 정보를 누르고 라이선스 보기를 눌러 장치 라이선스를 확인합니다.

8.4.4 네트워크 설정

포트 및 Wi-Fi를 설정할 수 있습니다.

포트 설정

네트워크를 통해 장치에 액세스할 때 실제 필요에 따라 HTTP, RTSP, HTTPS 및 서버를 설정할 수 있습니다.

구성 → 네트워크 → 기본 설정 → 포트를 눌러 설정 페이지로 들어갑니다.

HTTP

브라우저가 장치에 액세스하는 데 사용하는 포트를 나타냅니다. 예를 들어 HTTP 포트를 81로 수정한 경우 브라우저에 http://192.0.0.65:81을 입력해야 로그인 가능합니다.

RTSP

실시간 스트리밍 프로토콜의 포트를 말합니다.

HTTPS

브라우저에 액세스하기 위한 HTTPS를 설정합니다. 접속시 공인인증서가 필요합니다.

SERVER

클라이언트가 장치를 추가하는 데 사용하는 포트를 나타냅니다.

Wi-Fi 설정

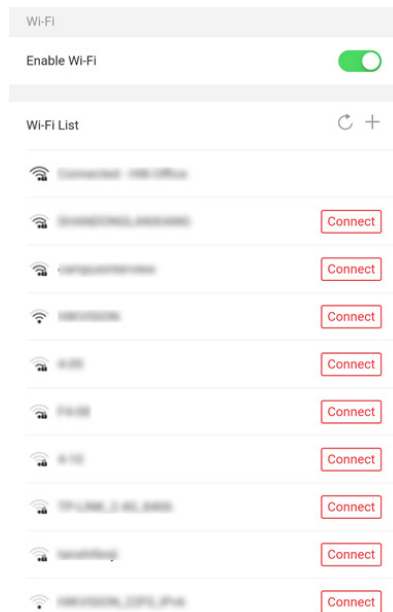
장치 무선 연결을 위한 Wi-Fi를 설정합니다.



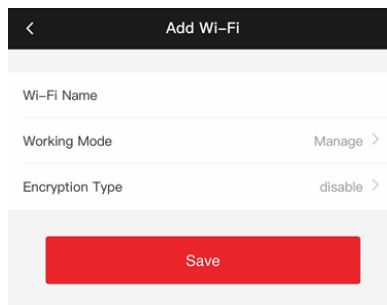
• 해당 기능은 장치에서 지원해야 합니다.

❶ 구성 → 네트워크 → 기본 설정 → Wi-Fi를 눌러 설정 페이지로 들어갑니다.

❷ Wi-Fi 활성화를 선택합니다.



[Wi-Fi]



[Wi-Fi 추가]

❸ Wi-Fi를 추가합니다.

- 1) +를 누릅니다.
- 2) Wi-Fi 이름과 Wi-Fi 비밀번호를 입력하고 작업 모드와 암호화 유형을 선택합니다.
- 3) 저장을 탭합니다.

❹ Wi-Fi 이름을 선택하고 연결을 누릅니다.

❺ 비밀번호를 입력하고 저장을 탭합니다.

❻ WLAN을 설정합니다.

- 1) IP 주소, 서브넷 마스크, 게이트웨이를 설정합니다. 또는 DHCP를 활성화하면 시스템 IP 주소, 서브넷 마스크 및 게이트웨이를 자동으로 할당합니다.
- 2) 저장을 탭합니다.

8.4.5 일반 설정

인증 설정

인증을 설정합니다.

❶ 구성 → 일반 설정 → 인증 설정을 탭합니다.

[인증 설정]

❷ 저장을 탭합니다.

장비 유형

주 카드 판독기(리더기)

장치 카드 판독기의 설정을 구성할 수 있습니다. 기본 카드 리더를 선택하면 다음 설정을 구성해야 합니다.

카드 리더 유형, 카드 리더 설명, 카드 리더 사용, 인증, 인식 간격(s), 최소 카드 스 와이프 간격(s), 최대. 인증 실패 시도 경보/최대 경보. 실패한 시도, 무단 변경 감지 활성화 및 카드 번호 반전 활성화

보조 카드 판독기(리더기)

연결된 주변 카드 판독기의 설정을 구성할 수 있습니다. 서브 카드 리더를 선택하면 다음 설정을 구성해야 합니다.

카드 리더 유형, 카드 리더 설명, 카드 리더 사용, 인증, 인식 간격(s), 최대. 인증 실패 시도 경보/최대 경보. Failed Attempts, Enable Tampering Detection, Communication with Controller Every (s) and Max. 비밀번호를 입력할 때의 간격(들)

카드 리더기 유형: 카드 리더 유형을 가져옵니다.

카드 리더 설명: 카드 판독기 설명을 가져옵니다. 읽기 전용입니다.

카드 리더 활성화: 카드 리더의 기능을 활성화합니다.

인증: 드롭다운 목록에서 실제 필요에 따라 인증 모드를 선택합니다.

인식 간격: 동일한 카드의 카드 태그 간격이 구성된 값보다 작으면 카드 태그가 유효하지 않습니다. 간격 시간 범위는 0 ~ 255초입니다.

인증 간격: 인증 시 동일인의 인증 간격을 설정할 수 있습니다. 동일한 사람은 구성된 간격에서 한 번만 인증할 수 있습니다. 두 번째 인증에 실패합니다.

최대 시도 횟수 실패 알람/ 최대 인증 시도 실패 횟수: 카드 읽기 시도가 설정 값에 도달하면 알람을 보고하도록 활성화합니다.

템퍼링 감지 활성화: 제품 탈착 방지 감지를 활성화합니다.

카드 번호 반향 변경 활성화: 기능을 활성화하면 읽은 카드 번호가 역순으로 됩니다.

비공개(개인 정보 설정)

- ① 이벤트 저장 유형, 사진 업로드 및 저장, 사진 삭제를 설정합니다.
- ② 구성 → 일반 설정 → 비공개(개인 정보)를 누릅니다.

Event Storage Settings

Event Storage Type Overwriting >

Save

Authentication Settings

Display Authentication Result ^

Picture ☒

Name ☒

Employee ID ☒

Name De-identification ☒

ID De-identification ☒

Save

Picture Uploading and Storage

Upload Captured Picture When Authenticating ☐

Save Captured Picture When Authenticating ☐

Save Registered Picture ☐

Upload Picture After Linked Capture ☐

Save Pictures After Linked Capture ☐

Save

Clear All Pictures in Device

Image Type ^

Face Picture ☐

Authentication/Captured Picture ☐

Clear

[프라이버시 설정]

이벤트 저장 유형

이벤트 삭제 방법을 선택하세요. 주기적으로 오래된 이벤트 삭제, 지정된 시간에 오래된 이벤트 삭제 또는 덮어쓰기 중에서 선택할 수 있습니다.

오래된 이벤트를 주기적으로 삭제

이벤트 삭제 기간을 설정할 숫자를 입력하세요. 구성된 기간에 따라 모든 이벤트가 삭제됩니다.

인증 설정

인증 결과 표시

얼굴 사진, 이름 또는 직원 ID를 확인합니다. 인증이 완료되면 선택한 내용이 결과에 표시됩니다.

이름 비식별화

이름 중 일부를 별표처리하여 암호화합니다.

사진 업로드 및 저장

사진을 업로드하고 저장할 수 있습니다.

인증 시 캡처 사진 업로드

인증 시 캡처한 사진을 플랫폼에 자동으로 업로드합니다.

인증 시 캡처 사진 저장

이 기능을 활성화하면 기기 인증 시 사진을 저장할 수 있습니다.

등록된 사진 저장

기능을 활성화하면 등록된 얼굴 사진이 시스템에 저장됩니다.

연결된 캡처 후 사진 업로드

연결된 카메라로 촬영한 사진을 플랫폼에 자동으로 업로드합니다.

연결된 캡처 후 사진 저장

이 기능을 활성화하면 연결된 카메라에서 촬영한 사진을 장치에 저장할 수 있습니다.

장치의 모든 사진 지우기

기기에 등록된 얼굴 사진과 촬영된 사진을 삭제할 수 있습니다.

등록된 얼굴 사진 지우기

얼굴 사진을 선택하고 지우기를 탭합니다. 장치에 등록된 모든 사진이 삭제됩니다.

인증/캡처 사진 지우기

인증/캡처된 사진을 선택하고 지우기를 누릅니다. 기기에 있는 모든 인증/캡처 사진이 삭제됩니다.

카드 보안 설정

❶ 구성 → 일반 설정 → 카드 보안을 눌러 설정 페이지로 들어갑니다.

[카드 보안]

❷ 설정하고 저장을 클릭합니다.

NFC 카드 활성화

휴대폰이 액세스 제어 데이터를 가져오는 것을 방지하기 위해 NFC 카드를 활성화하여 데이터의 보안 수준을 높일 수 있습니다.

M1 카드 활성화

M1 카드를 활성화하고 M1 카드를 제시하여 인증할 수 있습니다.

SECTOR

기능을 활성화하고 암호화 섹터를 설정하십시오. 기본적으로 섹터 13은 암호화됩니다. 섹터 13을 암호화하는 것이 좋습니다.

EM 카드 활성화

EM 카드 활성화 및 EM 카드 제시를 통한 인증이 가능합니다.



• 주변 카드 리더가 EM 카드 표시를 지원하는 경우 EM 카드 기능을 활성화/비활성화하는 기능도 지원됩니다.

CPU 카드 활성화

장치는 CPU 카드 기능을 활성화할 때 CPU 카드에서 데이터를 읽을 수 있습니다.

CPU 카드 읽기 내용

CPU 카드 내용 읽기 기능을 활성화한 후 장치는 CPU 카드 내용을 읽을 수 있습니다.

ID 카드 활성화

ID 카드 활성화 및 ID 카드 제시를 통한 인증이 가능합니다.

카드 인증 설정

❶ 단말기에서 카드로 인증 시 카드 판독 내용을 설정합니다.

❷ 구성 → 일반 설정 → 카드 인증 설정을 누릅니다.

[카드 인증 페이지]

❸ 카드 인증 모드를 선택한 후 저장을 누르세요.

전체 카드 번호: 모든 카드 번호가 읽혀집니다.

Wiegand 26(3바이트): 장치는 Wiegand 26 프로토콜(3바이트 읽기)을 통해 카드를 읽습니다.

Wiegand 34(4바이트): 장치는 Wiegand 34 프로토콜(4바이트 읽기)을 통해 카드를 읽습니다.

8.4.6 얼굴 설정

얼굴을 설정합니다.

얼굴 설정

❶ 구성 → 스마트 → 지능형매개변수를 탭합니다.

Face Anti-spoofing	<input checked="" type="checkbox"/>	Face with Mask Detection	<input checked="" type="checkbox"/>
Live Face Detection Security Level	Normal >	Face without Mask Strategy	None >
Recognition Distance	Auto >	Face with Mask&Face (1:1)	68
Application Mode	Indoor >	Face with Mask 1:N Matching Threshold	80
Face Recognition Mode	Normal Mode >	Face with Mask&Face (1:1 ECO)	78
		Face with Mask 1:N Matching Threshold (ECO Mode)	70
Continuous Face Recognition Interval(s)	3	ECO Mode	<input checked="" type="checkbox"/>
1:1 Matching Threshold	90	ECO Mode Threshold	4
1:N Matching Threshold	90	1:1 Matching Threshold	80
Face Recognition Timeout Value(s)	3	1:N Matching Threshold	80
<div>Save</div>			

[얼굴 설정]

❷ 얼굴인증을 설정합니다.

얼굴 도용(스푸핑) 방지

라이브 얼굴 감지 기능을 활성화 또는 비활성화합니다. 기능을 활성화하면 장치는 사람이 살아있는지 여부를 인식할 수 있습니다.

실시간 얼굴 인식 보안 레벨

얼굴 스푸핑 방지 기능을 활성화한 후 실시간 얼굴 인증을 수행할 때 일치하는 보안 수준을 설정할 수 있습니다.

인식 거리

인증하는 사용자와 장치 카메라 사이의 거리를 선택합니다.

애플리케이션 모드

실제 환경에 따라 실내 또는 기타를 선택합니다. 실외 장면, 창가 근처 실내 장면 또는 실외 환경에서 기타를 선택할 수 있습니다.



• 장치가 다른 도구에 의해 활성화되지 않은 경우 장치는 기본적으로 실내를 환경 모드로 사용합니다.

얼굴 인식 모드

정상 모드

장치는 카메라를 사용하여 얼굴 인식을 수행합니다.

딥 모드

보다 복잡한 환경에 적용할 수 있으며 인식되는 사람의 범위가 더 넓습니다.



- 두 모드는 서로 호환될 수 없습니다. 모드를 선택한 후에는 변경하지 마십시오. 모드를 변경하면 이전 모드의 얼굴 사진은 모두 지워집니다.
- 딥 모드에서는 장치 또는 등록 스테이션의 사용자 추가 기능을 통해서만 얼굴 사진을 추가할 수 있습니다. 사진 가져오기를 통해 얼굴 사진을 추가하는 것은 지원되지 않습니다.

장치는 카메라를 사용하여 얼굴 인식을 수행합니다.

지속적인(연속) 얼굴 인식 간격(들)

인증 시 두 번의 지속적인 얼굴 인식 사이의 시간 간격을 설정합니다.



- 값 범위: 1~10.

1:1 일치(매칭) 임계값

1:1 매칭 방식으로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

1:N 일치(매칭) 임계값

1:N 매칭 방식으로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다. 최대값은 100입니다.

얼굴 인식 시간 초과 값(s)

얼굴 인식에 대한 제한 시간을 구성합니다. 얼굴 인식 시간이 구성된 값을 초과하면 장치에서 얼굴 인식 시간 초과 메시지를 표시합니다.

마스크 착용 감지

마스크 착용을 활성화하면 마스크 착용 얼굴을 인식합니다.

마스크가 있는 1:N 일치 임계값, ECO 모드 및 설정으로 얼굴을 설정할 수 있습니다.

없음: 인증할 때 마스크 미착용에 대한 알림 메시지를 표시하지 않습니다.

착용 알림: 인증 시 마스크 미착용에 대한 알림 메시지를 표시하고 문이 열립니다.

필수 착용: 인증 시 마스크 미착용에 대한 알림을 표시하고 출입을 제한합니다.

마스크 착용 얼굴 & 얼굴 (1:1)

1:1 매칭 방식으로 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

마스크 착용 얼굴 1:N 일치(매칭) 기준값

1:N 매칭 모드를 통해 안면 마스크로 인증할 때 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

마스크 착용 얼굴 & 얼굴 (1:1 ECO)

ECO 모드 1:1 매칭 모드를 통해 안면 마스크 인증 시 매칭 값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

마스크 착용 얼굴 1:N 일치 기준값(ECO 모드)

ECO 모드 1:N 매칭 모드를 통해 안면 마스크로 인증할 때 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

에코 모드

ECO 모드를 활성화하면 장치는 IR 카메라를 사용하여 어둡거나 어두운 환경에서 얼굴을 인증합니다. 그리고 ECO 모드 임계값, ECO 모드(1:1 일치 임계값) 및 ECO 모드(1:N 일치 임계값)를 설정할 수 있습니다.

ECO 모드 임계값

ECO 모드 1:1 매칭 모드와 ECO 모드 1:N 매칭 모드를 통해 인증 시 매칭 임계값을 설정합니다.

1:1 일치(매칭) 임계값

ECO 모드 1:1 매칭 모드로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다.

1:N 일치(매칭) 임계값

ECO 모드 1:N 매칭 모드로 인증 시 매칭 임계값을 설정합니다. 값이 클수록 오인수율은 작아지고 오거부율은 커집니다. 최대값은 100입니다.

인식 영역 설정

구성 → 스마트 → 영역 구성을 눌러 페이지로 들어갑니다.

라이브 영상의 파란색 프레임을 드래그하여 인식 영역을 조정하세요. 해당 영역 내의 얼굴만 시스템에서 인식할 수 있습니다.

슬라이더를 끌어 얼굴 인식 유효 영역을 설정합니다.

저장을 탭하여 설정을 저장합니다.

8.4.7 비디오 인터콤 설정

단말기 ID 설정

이 장치는 도어 스테이션, 외부 도어 스테이션 또는 액세스 제어 장치로 사용할 수 있습니다. 사용하기 전에 장치 ID를 설정해야 합니다.

설정 → 인터콤 구성 → 단말기 ID 설정을 선택하세요.

장치 유형을 도어 스테이션 또는 출입 통제 장치로 설정하면 층 번호와 도어 스테이션 번호를 설정할 수 있습니다.

구성 후 설정을 저장하려면 저장을 누릅니다.

Device Type	Access Control Device >
Floor No.	1 >
Door Station No.	0
<div style="background-color: red; color: white; padding: 5px; display: inline-block;">Save</div>	

[장치 ID 설정(도어 스테이션)]

장비 유형

이 장치는 도어 스테이션, 실외 도어 스테이션 또는 출입 제어 장비(출입통제 단말기)로 사용할 수 있습니다. 드롭다운 목록에서 장치 유형을 선택합니다.



• 장치 유형을 변경하는 경우 장치를 재부팅해야 합니다.

층수

장치가 설치된 층 번호를 설정합니다.

도어 스테이션 번호

장치가 설치된 층 번호를 설정합니다.



• 번호를 변경하면 장치를 재부팅해야 합니다.

장치 유형을 외부 도어 스테이션으로 설정하면 외부 도어 스테이션 번호를 설정할 수 있습니다.

Device Type	Door Station >
Floor No.	3 >
Door Station No.	1
Community No.	0

Save

[장치 ID 설정(외부 도어 스테이션)]

외부 도어 스테이션 번호

외부 도어 스테이션을 장치 유형으로 선택한 경우 1에서 99 사이의 숫자를 입력해야 합니다.



• 번호를 변경하면 장치를 재부팅해야 합니다.

SIP 구성

❶ 장치의 IP 주소와 SIP 서버의 IP 주소를 설정합니다. 값을 설정한 후 액세스 제어 장치, 도어 스테이션, 실내 스테이션, 메인 스테이션 및 플랫폼 간에 통신할 수 있습니다.



• 액세스 제어 장치 및 기타 장치 또는 시스템(예: 도어 스테이션, 실내 스테이션, 메인 스테이션, 플랫폼)만 동일한 IP 세그먼트에 있으면 양방향 오디오를 수행할 수 있습니다.

설정 → 인터콤 구성 → 연결된 네트워크 설정을 선택하세요.

Device Type	Access Control Device >
VideoIntercom Server IP	0.0.0.0

Main Station IP	0.0.0.0
-----------------	---------

Save

[연결된 네트워크 설정]

❷ 비디오 인터콤 서버 IP와 메인 스테이션의 IP를 설정합니다.

❸ 저장을 탭합니다.

호출을 위해 버튼을 누르세요.

❶ 환경 설정 → 인터콤 구성 → 호출을 위해 버튼을 누르세요 설정 페이지로 들어갑니다.

❷ 호출 유형을 설정합니다.

- 콜 관리 센터를 선택하면 관리 PC와 통화를 할 수 있습니다.
- 앱 호출을 선택하면 모바일 APP에서 통화를 할 수 있습니다.

8.4.8 액세스 제어 설정

도어 설정

- 1 구성 → 접근 제어 → 도어 파라미터를 누릅니다.
- 2 구성 후 설정을 저장하려면 저장을 클릭하십시오.

Door No.	Door1 >
Name	
Open Duration(s)	5
Door Open Timeout Alarm(s)	30
Door Contact	Remain Closed >
Exit Button Type	Remain Open >
Door Lock Powering Off	Remain Closed >
Extended Open Duration(s)	15
Door Remain Open Duration with First Person(m)	10
Duress Code
Super Password

Save

[도어 매개변수 설정 페이지]

도어 번호

장치에 해당하는 문 번호를 선택합니다.

이름

문의 이름을 만들 수 있습니다.

열림 지속 시간

문 잠금 해제 시간을 설정합니다. 설정된 시간 동안 문을 열지 않으면 문이 잠깁니다.

도어 열림 시간 초과 알림

설정된 시간 내에 도어가 닫히지 않으면 알람이 울립니다.

도어 접점

실제 필요에 따라 도어 접점을 열린 상태 유지(NO) 또는 닫힌 상태 유지(NC)로 설정할 수 있습니다. 기본적으로 닫힌 상태 유지(NC)로 설정 됩니다.

나가기 버튼 유형

실제 필요에 따라 종료 버튼을 열린 상태 유지(NO) 또는 닫힌 상태 유지(NC)로 설정할 수 있습니다. 기본적으로 열린 상태 유지(NO)로 설정 됩니다.

도어록 전원 끄기

도어록 전원이 꺼진 상태에서 도어록 상태를 설정할 수 있습니다. 기본적으로 닫힌 상태 유지(NC)로 설정 됩니다.

연장 열림 지속 시간

확장 액세스가 필요한 사람이 카드를 테크 후 적절한 지연 시간을 두고 도어 컨택을 활성화할 수 있습니다.

제1 담당자로 도어 열림

첫 번째 사람이 들어올 때 문이 열리는 시간을 설정합니다. 첫 번째 사람이 인증되면 여러 사람이 문에 출입하거나 다른 인증 작업을 할 수 있습니다.

강제 코드 (비상 코드)

비상 상황이 있을 때 강제 코드(비상 코드)를 입력하면 문을 열 수 있습니다. 동시에 클라이언트는 강제코드 이벤트를 보고할 수 있습니다.

마스터 비밀번호

마스터 비밀번호를 입력하면 문을 열 수 있습니다.

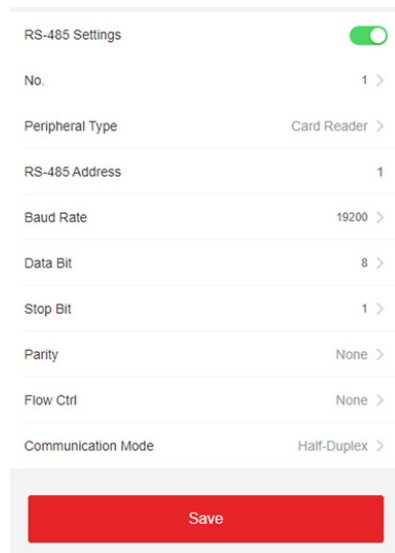


• 강제코드와 마스터 비밀번호는 달라야 합니다. 그리고 숫자의 범위는 4에서 8까지입니다.

RS-485 설정

주변 장치, 주소, 전송 속도 등을 포함한 RS-485를 설정할 수 있습니다.

- 1 설정 → 출입통제 → RS-485를 누르세요.
- 2 구성 후 설정을 저장하려면 저장을 누릅니다.



[RS-485 페이지]

주변장치 유형

실제 상황에 따라 드롭다운 목록에서 주변 장치를 선택합니다. 카드 리더, 확장 모듈 또는 액세스 컨트롤러 중에서 선택할 수 있습니다.



- 주변 장치가 변경되고 저장되면 장치가 자동으로 재부팅됩니다.

RS-485 주소

실제 필요에 따라 RS-485 주소를 설정하십시오.



- Access Controller를 선택한 경우: RS-485 인터페이스를 통해 장치를 터미널에 연결하는 경우 RS-485 주소를 2로 설정합니다. 장치를 컨트롤러에 연결하는 경우 출입문 번호에 따라 RS-485 주소를 설정합니다.

Baud Rate (전송 속도): 실제 필요에 따라 RS-485 주소를 설정하십시오.

데이터 비트: 장치가 RS-485 프로토콜을 통해 통신할 때의 데이터 비트입니다.

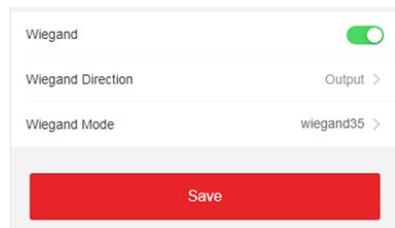
정지 비트: 장치가 RS-485 프로토콜을 통해 통신할 때 정지 비트입니다.

패리티/흐름 제어/통신 모드: 기본적으로 활성화됩니다.

Wiegand 설정

Wiegand 전송 방향을 설정할 수 있습니다.

- 1 설정 → 출입통제 → RS-485를 누르세요.



[Wiegand 페이지]

- 2 Wiegand를 활성화하여 Wiegand 기능을 활성화합니다.
- 3 전송 방향을 설정합니다.

입력

장치는 Wiegand 카드 리더를 연결할 수 있습니다.

산출

외부 액세스 컨트롤러를 연결할 수 있습니다. 그리고 두 장치는 Wiegand 26 또는 34를 통해 카드 번호를 전송합니다.

- 4 저장을 클릭하여 설정을 저장합니다.



- 주변 장치를 변경하고 장치 매개변수를 저장한 후 장치가 자동으로 재부팅됩니다.

9. 웹 브라우저를 통한 작동

9.1 로그인

웹 브라우저 또는 클라이언트 소프트웨어의 원격 구성을 통해 로그인할 수 있습니다.



• 장치가 활성화되어 있는지 확인하십시오. 활성화에 대한 자세한 내용은 다음을 참조하십시오. [\[활성화\]](#)

웹 브라우저를 통한 로그인

웹 브라우저의 주소 표시줄에 장치 IP 주소를 입력하고 Enter 키를 눌러 로그인 페이지로 들어갑니다.



• IP 주소가 "Https:"로 시작하는지 확인하십시오.

장치 사용자 이름과 암호를 입력합니다. 로그인을 클릭합니다.

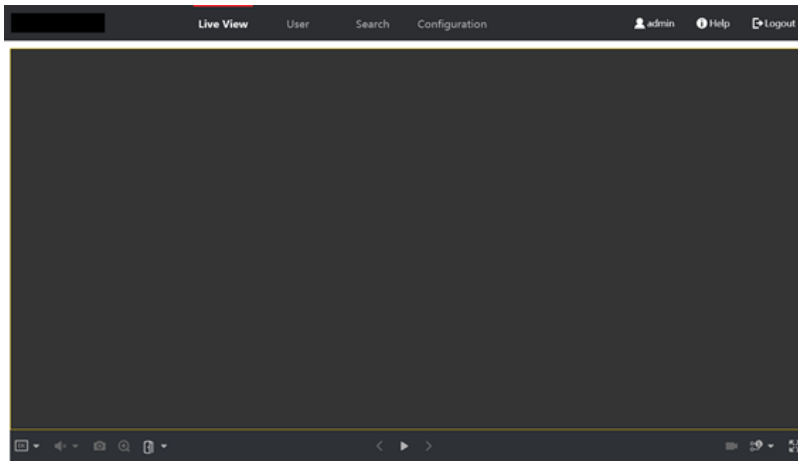
클라이언트 소프트웨어의 원격 구성을 통한 로그인

클라이언트 소프트웨어를 다운로드하고 엽니다. 장치를 추가한 후  을 클릭하여 구성 페이지로 들어갑니다.

9.2 라이브 뷰

장치의 라이브 비디오를 볼 수 있습니다.

로그인 후 라이브 뷰 페이지로 이동합니다. 라이브 뷰, 캡처, 비디오 녹화 및 기타 작업을 수행할 수 있습니다.



[실시간 보기 페이지]



라이브 뷰를 시작할 때 이미지 크기를 선택합니다.



라이브 뷰를 시작할 때 볼륨을 설정합니다.



• 양방향 오디오 시작 시 음량을 조절하면 반복되는 소리가 들릴 수 있습니다.



라이브 뷰를 시작할 때 이미지를 캡처할 수 있습니다.



예약 기능. 라이브 뷰 이미지를 확대할 수 있습니다.



라이브 뷰를 시작하거나 중지합니다.



비디오 녹화를 시작하거나 중지합니다.



라이브 뷰를 시작할 때 스트리밍 유형을 선택합니다. 메인 스트림과 서브 스트림 중에서 선택할 수 있습니다.



전체 화면 보기

9.3 사용자 관리

기본 정보, 인증 모드, 카드 및 지문을 포함한 개인 정보를 클릭하여 추가하십시오. 또한 사용자 목록에서 사용자 정보를 편집하고 사용자 사진을 보고 사용자 정보를 검색할 수 있습니다.

확인을 클릭하여 사람을 저장합니다.

기본 정보 추가

사용자 → + 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

사람 ID, 이름, 성별, 수준(사용자 등급), 층, 방 등 개인의 기본 정보를 추가합니다.

확인을 클릭하여 설정을 저장합니다.

카드 추가

사용자 → 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

카드 추가를 클릭하여 카드번호를 입력하고 속성을 선택한 후 확인을 클릭하면 카드가 추가됩니다.

확인을 클릭하여 설정을 저장합니다.

얼굴 사진 추가

사용자 → 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

오른쪽의 +를 클릭하여 로컬 PC에서 얼굴 사진을 업로드합니다.



• 그림 형식은 JPG 또는 JPEG 또는 PNG여야 하며 크기는 200K 미만이어야 합니다.

확인을 클릭하여 설정을 저장합니다.

권한 시간 설정

사용자 → 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

시작 시간과 종료 시간을 설정합니다.

확인을 클릭하여 설정을 저장합니다.

액세스 제어 설정

사용자 → 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

출입통제에서 관리자 체크 후 추가된 사람은 얼굴인증으로 로그인 가능합니다.

추가를 클릭하여 출입통제 층과 방을 입력하고 를 클릭하여 삭제할 수 있습니다.

확인을 클릭하여 설정을 저장합니다.

인증 유형 추가

사용자 → 추가를 클릭하여 개인 추가 페이지로 들어갑니다.

인증 유형을 설정합니다.

확인을 클릭하여 설정을 저장합니다.

9.4 이벤트 로그 검색하기

검색을 클릭하여 검색 페이지로 들어갑니다.

The form is titled 'Event Types' and contains several input fields and a search button. The fields are: 'Access Control Event' (a dropdown menu), 'Employee ID' (a text input field), 'Name' (a text input field), 'Card No.' (a text input field), 'Start Time' (a date and time picker showing '2021-06-07 00:00:00'), and 'End Time' (a date and time picker showing '2021-06-07 23:59:59'). A search button is located at the bottom right of the form.

사원번호, 이름, 카드번호, 시작시간, 종료시간 등 검색 조건을 입력하고 검색을 클릭합니다. 결과는 오른쪽 패널에 표시됩니다.

[검색 페이지]

9.5 설정

9.5.1 로컬 설정

라이브 뷰, 녹화 파일 저장 경로 및 캡처된 사진 저장 경로를 설정합니다.

라이브 뷰 설정

구성 → 로컬을 클릭하여 로컬 페이지로 들어갑니다. 스트림 유형, 재생 성능, 라이브 보기 자동 시작 및 이미지 형식을 구성하고 저장을 클릭합니다.

녹화 파일 저장 경로 설정

구성 → 로컬을 클릭하여 로컬 페이지로 들어갑니다. 녹화 파일 크기를 선택하고 로컬 컴퓨터에서 저장 경로를 선택한 후 저장을 클릭합니다.

열기를 클릭하여 파일 폴더를 열어 세부 정보를 볼 수도 있습니다.

캡처 사진 저장 경로 설정

구성 → 로컬을 클릭하여 로컬 페이지로 들어갑니다. 로컬 컴퓨터에서 저장 경로를 선택하고 저장을 클릭합니다.

열기를 클릭하여 파일 폴더를 열어 세부 정보를 볼 수도 있습니다.

9.5.2 장치 정보 보기

기기명, 언어, 모델명, 시리얼번호, QR코드, 버전, 채널수, IO 입력, IO 출력, 잠금장치, RS-485 및 알람 출력, 기기 용량 등을 조회합니다.

구성 → 시스템 → 시스템 설정 → 기본 정보를 클릭하여 구성 페이지로 들어갑니다.

기기명, 언어, 모델명, 시리얼 번호, QR코드, 버전, 채널 수, IO 입력, IO 출력, 잠금, RS-485 및 알람 출력, 기기 용량 등을 확인할 수 있습니다.

9.5.3 시간 설정

장치의 시간대, 동기화 모드 및 장치 시간을 설정합니다.

구성 → 시스템 → 시스템 설정 → 시간 설정을 클릭합니다.

[시간 설정]

구성 후 설정을 저장하려면 저장을 클릭하십시오.

시간대

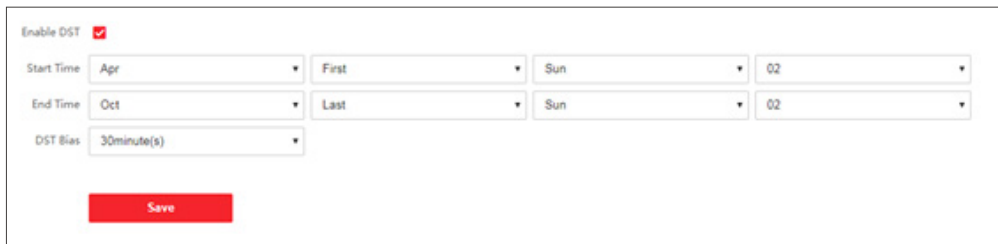
드롭다운 목록에서 장치가 위치한 시간대를 선택합니다.

시간 동기화

- NTP: NTP 서버의 IP 주소, 포트 번호 및 간격을 설정해야 합니다.
- 수동: 기본적으로 장치 시간은 수동으로 동기화해야 합니다. 장치 시간을 수동으로 설정하거나 동기화를 확인할 수 있습니다. 컴퓨터 시간으로 장치 시간을 컴퓨터 시간과 동기화합니다.

9.5.4 서머타임 설정

❶ 구성 → 시스템 → 시스템 설정 → DST를 클릭합니다.

DST 설정 페이지의 스크린샷입니다. 'Enable DST' 체크박스가 선택되어 있습니다. 'Start Time'은 Apr, First, Sun, 02로 설정되어 있으며, 'End Time'은 Oct, Last, Sun, 02로 설정되어 있습니다. 'DST Bias'는 30minute(s)로 설정되어 있습니다. 하단에는 'Save' 버튼이 있습니다.

[DST 페이지]

❷ DST 활성화를 선택합니다.

❸ DST 시작 시간, 종료 시간 및 바이어스 시간을 설정합니다.

❹ 저장을 클릭하여 설정을 저장합니다.

9.5.5 오픈 소스 소프트웨어 라이선스 보기

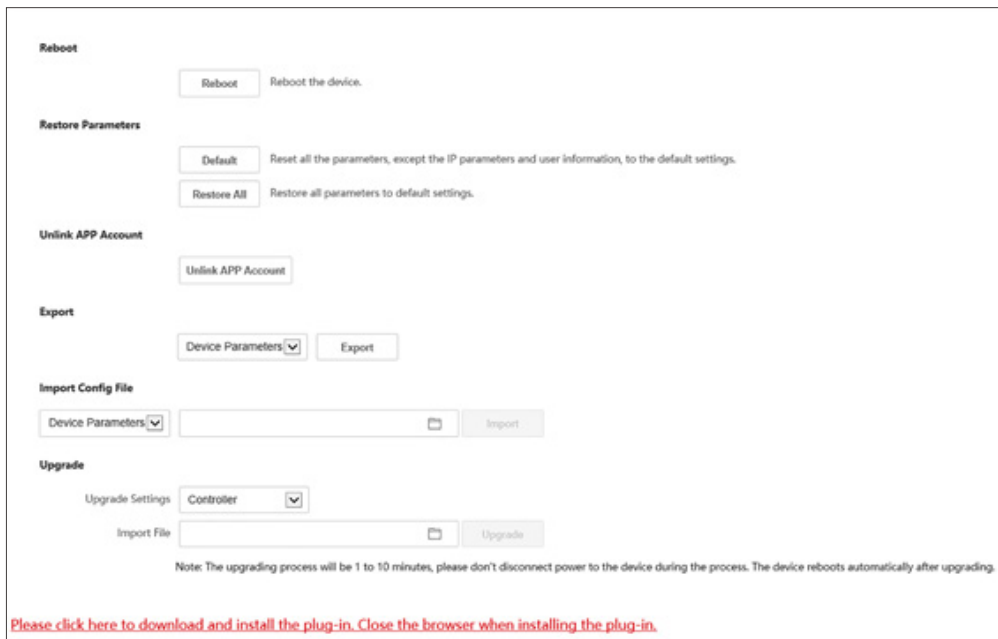
구성 → 시스템 → 시스템 설정 → 관련 정보로 이동하고 라이선스 보기를 클릭하여 장치 라이선스를 봅니다.

9.5.6 업그레이드 및 유지보수

장치를 재부팅하고 설정값을 복원하고 장치 버전을 업그레이드합니다.

기기 재부팅

구성 → 시스템 → 유지 보수 → 업그레이드 & 유지 관리를 클릭합니다.

업그레이드 및 유지 관리 페이지의 스크린샷입니다. 'Reboot' 섹션에는 'Reboot' 버튼이 있습니다. 'Restore Parameters' 섹션에는 'Default'와 'Restore All' 버튼이 있습니다. 'Unlink APP Account' 섹션에는 'Unlink APP Account' 버튼이 있습니다. 'Export' 섹션에는 'Device Parameters' 드롭다운 메뉴와 'Export' 버튼이 있습니다. 'Import Config File' 섹션에는 'Device Parameters' 드롭다운 메뉴, 파일 선택 아이콘, 'Import' 버튼이 있습니다. 'Upgrade' 섹션에는 'Upgrade Settings' 드롭다운 메뉴(현재 Controller로 설정됨), 'Import File' 파일 선택 아이콘, 'Upgrade' 버튼이 있습니다. 하단에는 업그레이드 과정에 대한 주의 사항이 표시되어 있습니다.

[업그레이드 및 유지 관리 페이지]

재부팅을 클릭하여 장치 재부팅을 시작합니다.

매개변수(설정) 복원

구성 → 시스템 → 유지 관리 → 업그레이드 및 유지 관리를 클릭합니다.

모두 복구

모든 설정값은 공장 설정으로 복원됩니다. 사용하기 전에 장치를 활성화해야 합니다.

기본

장치는 장치 IP 주소와 사용자 정보를 제외하고 기본 설정으로 복원됩니다.

APP 계정 연결 해제

플랫폼에서 Guarding Vision 계정의 연결을 해제합니다.

설정값 가져오기 및 내보내기

구성 → 시스템 → 유지 관리 → 업그레이드 및 유지 관리를 클릭합니다.

내보내기

내보내기를 클릭하여 로그 또는 장치 설정값을 내보내기 할 수 있습니다.



• 내보낸 장치 설정값을 다른 장치로 가져올 수 있습니다.

구성파일 가져오기



을 클릭하고 가져올 파일을 선택합니다. 가져오기를 클릭하여 구성 파일 가져오기를 시작합니다.

업그레이드

구성 → 시스템 → 유지 관리 → 업그레이드 및 유지 관리를 클릭합니다.

드롭다운 목록에서 업그레이드 유형을 선택합니다.



을 클릭하고 로컬 PC에서 업그레이드 파일을 선택합니다. 업그레이드를 시작하려면 업그레이드를 클릭하십시오.



• 업그레이드 중에는 전원을 끄지 마십시오.

9.5.7 로그 쿼리

장치 로그를 검색하고 볼 수 있습니다.

구성 → 시스템 → 유지 관리 → 로그 쿼리로 이동합니다.

로그 유형의 주 유형과 부 유형을 설정합니다. 검색 시작 시간과 종료 시간을 설정하고 검색을 클릭합니다.

번호, 시간, 주 유형 마이너 유형, 채널 번호, 로컬/원격 사용자 정보, 원격 호스트 IP 등 결과가 아래에 표시됩니다.

9.5.8 보안 모드 설정

클라이언트 소프트웨어 로그인을 위한 보안 모드를 설정합니다.

구성 → 시스템 → 보안 → 보안 서비스를 클릭합니다.

드롭다운 목록에서 보안 모드를 선택하고 저장을 클릭합니다.

보안 모드

클라이언트 소프트웨어 로그인 시 사용자 정보 확인을 위한 높은 보안 수준.

호환 모드

사용자 정보 확인은 로그인 시 이전 클라이언트 소프트웨어 버전과 호환됩니다.

SSH 활성화

네트워크 보안을 강화하려면 SSH 서비스를 비활성화하십시오. 구성은 전문가를 위해 장치를 디버깅하는 데만 사용됩니다.

호환 모드

웹 사이트 방문 시 네트워크 보안 수준을 높이기 위해 HTTP를 활성화하여 보다 안전하고 암호화된 네트워크 통신 환경을 확보할 수 있습니다. 통신은 HTTP를 활성화한 후 ID 및 암호화 암호로 인증해야 저장됩니다.

9.5.8 보안 모드 설정

서버/클라이언트 인증서 및 CA 인증서 관리에 도움이 됩니다.



• 이 기능은 특정 장치 모델에서만 지원됩니다.