BioStar Air

관리자 가이드

버전 2.13.0

한국어

KO 102.00.BSA

suprema

SECURITY & BIOMETRICS

목차

BioStar Air란? 4

100% 클라우드 출입 통제 플랫폼 4

비교할 수 없는 크리덴셜 유연성 4

온프레미스 인프라 불필요 4

손쉬운 다중 사이트 관리 4

엣지 아키텍처를 통한 미래 지향적 확장성 5

클라우드 중심 기업에 최적화 5

BioStar Air 기능 5

지원 장치 6

보안 체계 7

사이트 관리자 10

시작하기 10

사이트 선택(Site Selector) 21

BioStar Air 앱 시작하기 23

사이트 관리하기 25

사이트 설정하기 206

SSO & SCIM 설정하기 226

추가 사이트 구성하기 256

파트너 및 설치 관리자 285

파트너 포털 사용하기 285

페더레이션 사이트 관리하기 287

파트너 관리자 초대하기 289

사이트 관리자 초대하기 294

파트너 기술자 관리하기 299

하드웨어 설치하기 312

인증된 사용자 333

모바일 크리덴셜 사용하기 333

고급 기능 설정하기 335

민감도 설정하기 339

개발자 341

빠른 시작하기 341

API 인증하기 343

사용자 관리 API 사용하기 346

문제 해결 351

일괄 사용자 추가 문제 351

모바일 카드가 작동하지 않아요 354

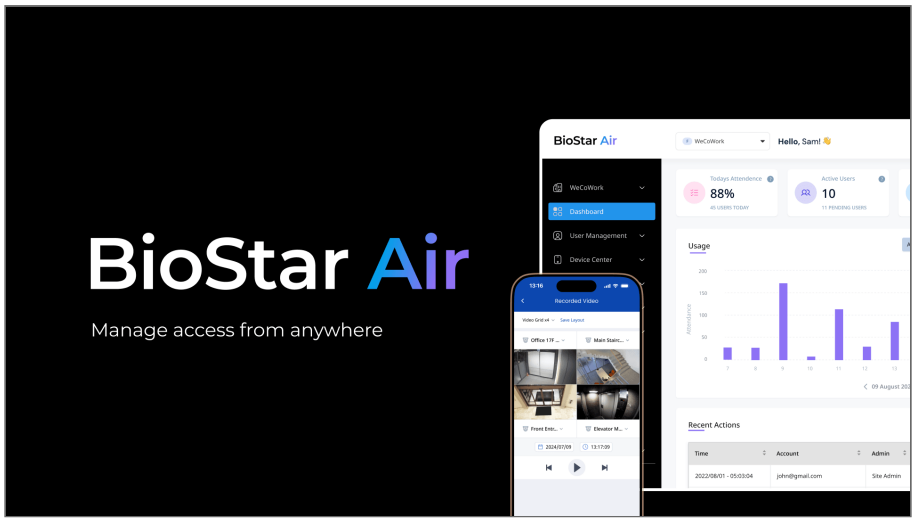
위치 서비스를 활성화해야 하나요? 356

비디오 재생 관련 문제 해결 357

BioStar Air란?

100% 클라우드 출입 통제 플랫폼

BioStar Air는 생체 인식 보안 분야의 세계적인 선도 기업인 슈프리마가 개발한 클라우드 네이티브 출입 통제 솔루션입니다. 온프레미스 인프라의 필요성을 없애도록 설계된 BioStar Air는 어디서나 관리할 수 있는 안전하고 유연하며 확장 가능한 출입 통제를 제공합니다. 클라우드에 직접 연결된 스마트 리더기를 통해 기업은 휴대폰이나 브라우저만으로 여러 위치의 출입을 손쉽게 제어할 수 있습니다.



비교할 수 없는 크리덴셜 유연성

BioStar Air는 가장 완전한 범위의 인증 옵션을 제공하며, 안전하고 편리한 여러가지 방법을 통해 사용자의 시설 출입을 관리할 수 있습니다.

- **얼굴 인증**
- **iOS 및 안드로이드를 위한 맞춤형 모바일 인증**(무료)
- **다양한 형식의 RFID**
- **앱 없이도 사용할 수 있는 Dynamic QR 및 LinkPass**

온프레미스 인프라 불필요

BioStar Air는 온사이트(on-site) 서버, 가상 머신, VPN 또는 출입문 컨트롤러의 필요성을 없앴습니다. IT 유지 보수가 필요하지 않습니다. **스마트 리더기**(Smart reader)를 설치하고 클라우드에 연결하면, 즉시 출입 관리를 시작할 수 있습니다. 리더기(Reader)는 동일한 네트워크나 물리적 위치와 관계 없이 여러 사이트에서 작동합니다.

손쉬운 다중 사이트 관리

사무실, 창고, 소매점 또는 **원격 사이트**의 출입 관리 여부와 관계없이 BioStar Air는 단일 시스템 하에서 모든 위치의 출입을 제어할 수 있는 완벽한 솔루션을 제공합니다.

엣지 아키텍처를 통한 미래 지향적 확장성

BioStar Air의 **엣지 아키텍처**는 출입 통제를 스마트 리더기에 직접 내장하여 별도의 출입문 컨트롤러가 필요하지 않습니다. 이를 통해 기업은 **손쉽게 확장**할 수 있습니다. 현재 필요한 기능만 구매하고 복잡한 업그레이드 없이 간편하게 확장할 수 있습니다.

클라우드 중심 기업에 최적화

BioStar Air는 업계 최고의 생체 인식 기술을 탑재한 완벽한 클라우드 네이티브 출입 통제 솔루션을 원하는 **시스템 통합 업체**와 **고객**을 위해 설계되었습니다. 클라우드 중심 기업의 출입 관리를 위한 현대적이고 유연하며 매우 안전한 방법을 제공합니다.

BioStar Air 기능

기능	설명
완벽한 출입 통제 솔루션	지원
높은 보안성	ISO 27001 / 27701, TLS 1.2, AES-256
생체 인식: 얼굴 및 지문	슈프리마 리더기에 대한 기본 지원하며, 생체 인식 데이터베이스가 내장되어 있습니다.
RFID 카드	MIFARE Classic, DesFire, Felica, EM4100, Custom Wiegand Formats, iClass, Seos. 사용자당 최대 8장의 카드를 지원합니다.
모바일 크리덴셜	무료이며 무제한 제공합니다. 보안 BLE/NFC 크리덴셜(iOS, Android), 앱 없는 LinkPass 및 QR 인증을 포함합니다.
배포	클라우드 네이티브
인터페이스	브라우저, iOS 앱, Android 앱
가격 모델	구독 기반
Integration	광범위한 API, 웹후크 및 SDK
엣지 아키텍처	리더기에는 내장 컨트롤러가 있으며 이더넷을 통해 클라우드에 직접 연결됩니다. 별도의 클라우드 노드나 출입 통제 패널이 필요하지 않습니다.
로그인	어디서나 가능합니다.
서버 위치	한국(글로벌) 및 독일(유럽)
근태	리더기의 근태 키(key)는 이벤트 로그에 기록되며, 근무 시간 보고서가 작성되어 통합 가능합니다.
비디오	Onvif 및 Uniview를 지원하는 기본 VMS입니다. NVR 필요 없으며, 리더기가 게이트웨이 역할을 합니다.

기능	설명
알람	침입 경보 구역에 대한 관리자 알림을 지원합니다.
데이터 파티셔닝	표준
대상	프랜차이즈, 다중 지점, 다중 세대, 원격 지역 등

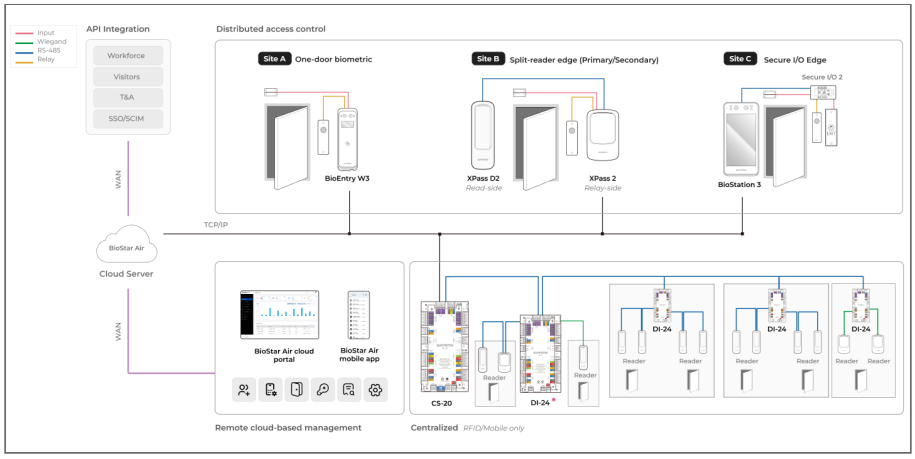
지원 장치

BioStar Air는 분산형 및 중앙 집중식 접근 제어 아키텍처 모두를 지원하는 유연한 기기 관리를 제공합니다. 클라우드를 통해 기기를 등록, 구성, 모니터링, 업데이트, 운영할 수 있으며, 각 사이트(Site)의 출입문, 배선, 보안 요구사항에 맞는 최적의 구성을 선택할 수 있습니다.

사이트(Site)에서는 클라우드에 직접 연결되는 엣지 장치를 사용하거나, RS-485 또는 Wiegand를 통해 리더 장치를 관리하는 제어 패널을 사용할 수 있습니다. 두 아키텍처는 동일한 사이트 내에서 함께 구성할 수 있어, 신규 설치, 바이오메트릭 출입 제어, 중앙 집중식 패널 기반 구성 등 다양한 환경을 지원합니다.

지원 장치

BioStar Air는 다양한 출입 통제 장치와 호환되며, 슈프리마 장치와 원활하게 통합되어 클라우드 기반 출입 통제가 가능합니다.



리더 장치

- **XPass 2** (MDPB, GDPB, GKDPB)
- **X-Station 2** (DPB)
- **BioEntry W3**
- **BioStation 3**
- **XPass D2**

패널

- **CoreStation 20** (CS-20)

패치(Patch) 장치

- **Airfob Patch** (AP-H)
- **Airfob Tag** (AP-B)

기타 호환 장치

- **Output Module** (OM-120)
- **Secure I/O 2** (SIO2)
- **Door Interface** (DI-24, 예정)

보안 체계

BioStar Air는 슈프리마의 안전한 클라우드 기반 모바일 출입 통제 솔루션입니다. 슈프리마의 하드웨어, 소프트웨어 및 펌웨어 엔지니어링 팀은 '설계 시 보안' 원칙에 따라 작업합니다. 시스템 아키텍처의 모든 계층과 모든 통신 접점은 개인 정보 보호 및 데이터 무결성을 유지하도록 설계되었습니다.

주요 조치 사항:

- BioStar Air 관리 포털 및 데이터베이스의 데이터 보호 및 암호화
- BioStar Air API와 클라이언트 간의 데이터 전송 시 암호화 및 보호
- 스마트폰에 저장된 모바일 카드 데이터 암호화
- 스마트폰과 리더 간의 통신 보호(슈프리마 패스)
- 모바일 자격 증명 위조 방지(슈프리마 패스)

ISO 27001 인증

슈프리마는 ISO 27001 인증을 획득하여 데이터 보호 관리, 보안 통제 및 개인 정보 관리에 대한 글로벌 표준을 충족합니다. 2019년 8월에 처음 설립된 ISO 27001 준수는 일반 데이터 보호 규정(GDPR) 및 캘리포니아 소비자 개인 정보 보호법(CCPA)과 같은 유사한 법률과도 일치합니다.

엔드투엔드(End-to-End) 보안을 위한 검증된 기술

보안 포털 액세스 및 데이터 보호

BioStar Air 관리 포털은 AES-256 이상의 암호화를 사용하는 AWS Amazon RDS 암호화 DB 인스턴스에서 실행됩니다. 모든 개인 데이터에는 추가 암호화가 적용됩니다.

BioStar Air API와의 암호화된 통신

BioStar Air REST API와의 모든 통신은 HTTPS를 통해 TLS 1.2를 사용하여 암호화되며 액세스 토큰(기본 1시간 만료)이 필요합니다. AWS API Gateway는 무차별 대입 공격을 방지하기 위해 API 요청을 제한합니다.

암호화 및 해시 처리된 모바일 카드 ID

모바일 카드 ID 번호는 AES-256을 사용하여 암호화되어 타사 서버에서 노출되는 것을 방지합니다. 카드 데이터는 진위 확인을 위해 디지털

서명됩니다.

모바일 기기에 저장된 모바일 카드의 안전한 저장

슈프리마 패스 모바일 자격 증명 및 관련 데이터는 AES-256으로 암호화됩니다. 암호화 키는 모바일 기기의 신뢰 실행 환경(TEE), 예를 들어 Secure Enclave(Apple) 또는 TrustZone(ARM)에 저장됩니다.

모바일 기기와 리더기 간의 보안 통신

Bluetooth Low Energy (BLE)를 통한 '재전송 공격'을 방지하기 위해 BioStar Air는 각 연결에 대해 일회성 암호화 키를 사용하고 전송 직후 연결을 종료하여 중간자 공격(MITM)을 방지합니다.

모바일 카드 위조 방지

각 슈프리마 패스 모바일 크리덴셜은 각 BioStar Air 사이트에 고유한 PKI 기반 디지털 서명으로 보호됩니다. 독점적인 검증 프로세스는 수정 또는 위조 시도를 감지합니다.

취약성 관리

슈프리마의 정보 보안 팀이 취약성 관리를 주도하며, 외부 보안 전문가들이 지원합니다.

- 지속적인 자동화된 위협 스캔
- 전체 시스템 검토가 포함된 연간 ISO 27001 갱신 감사
- 주요 릴리스 전 침투 테스트 및 위험 평가
- 비밀번호 위생, 사회 공학 저항성 및 절차 준수를 위한 점검
- 모든 취약점 및 수정 조치에 대한 포괄적인 문서화 및 보고

위험 평가 접근 방식

자산은 기밀성, 무결성 및 가용성 등급에 따라 분류됩니다. 위협이 식별되고 취약점이 평가되며 위험이 가능성과 영향에 따라 평가됩니다. 완화 조치는 위험 심각도에 따라 우선 순위가 지정됩니다.

멀티팩터 인증 (MFA)

멀티팩터 인증(MFA)은 단계적으로 구현되고 있습니다.

- 관리자 계정에 대한 Email 기반 2FA
- BioStar Air App에 대한 Passcode 기반 2FA
- 90일 후 비활성 관리자 계정 자동 잠금
- 비밀번호 만료 설정 가능(30, 60, 90일)

주요 보안 정책

- 전송 중 데이터 암호화: TLS 1.2
- 저장 중 데이터 암호화: AES-256

- DoS 보호: AWS API Gateway 요청 제한
- 서비스 가용성: 99.9% 가동 시간(SLA 기준)
- API 보안: 토큰 기반 인증, HTTPS 전용, 엄격한 엔드포인트 검증
- 포털 액세스: 글로벌 관리를 위한 클라우드 기반 서비스이며, 개인 클라우드 옵션을 개발 중

사이트 관리자

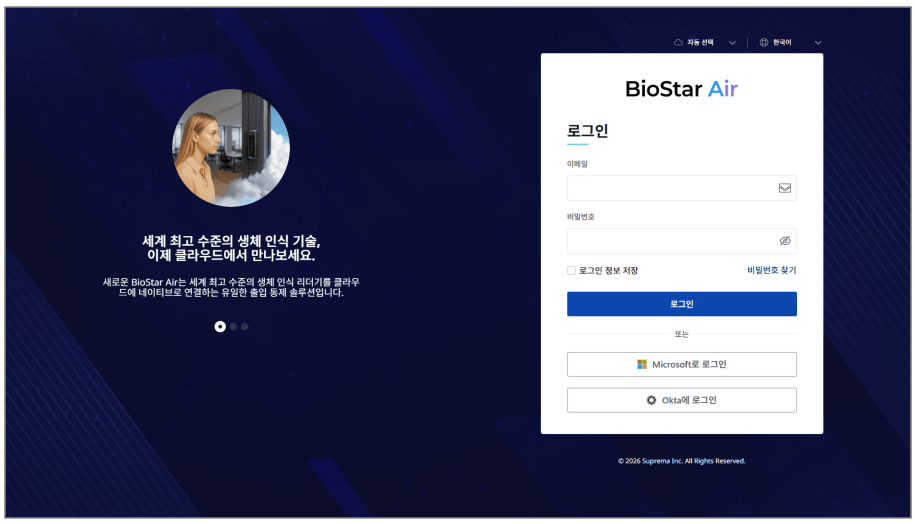
사이트 관리자는 BioStar Air 사이트의 운영 전반을 담당합니다. 사용자 등록과 크리덴셜 관리, 장치, 출입문, 엘리베이터 설정, 출입 권한 및 스케줄 구성, 이벤트 모니터링, 시스템 설정과 서비스 구성까지 필요한 모든 관리 작업을 안내합니다.

시작하기

BioStar Air 포털은 웹과 모바일 앱 전반에 걸쳐 통합된 인터페이스를 제공하여 일관된 사용자 경험을 제공합니다. BioStar Air 포털을 통해 관리자는 출입 통제 설정을 관리하고, 사이트 사용량을 모니터링하고, 사용자와 기기를 원활하게 구성할 수 있습니다.

포털 접속

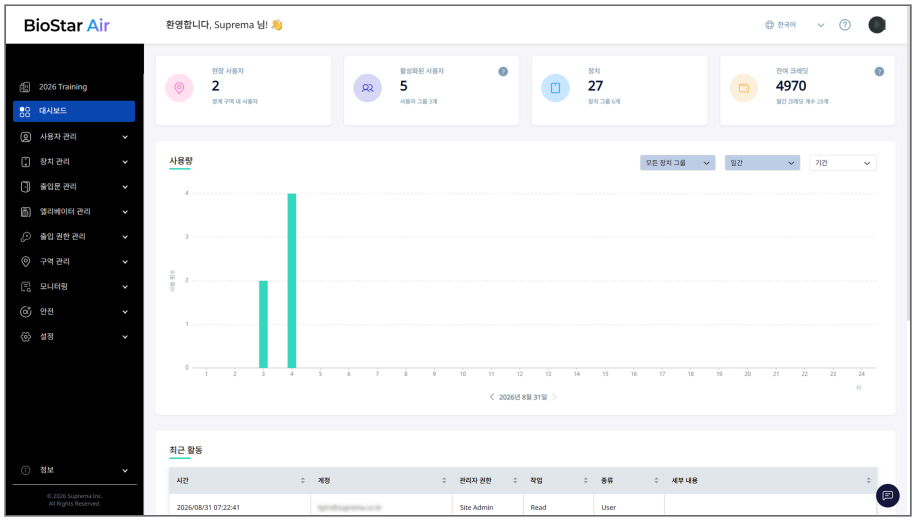
BioStar Air 포털에 접속하려면 웹 브라우저를 열고 admin.biostarair.com으로 이동하세요. 로그인 페이지가 나타나면 사용자의 현재 위치에 따라 **글로벌 서버** 또는 **EU 서버**를 선택하세요.



> **알아두기**
>
> 회원 가입을 통해 계정을 생성할 수 없습니다. 시스템 설치 담당자 또는 기존 관리자가 사이트로 초대해야 합니다. 관리자 계정 관리 및 초대에 대한 자세한 내용은 관리자 계정 및 역할 관리하기를 참고하세요.

대시보드 살펴보기

로그인하면 사이트의 주요 정보를 확인할 수 있는 **대시보드**가 표시됩니다.



- **현장 사용자**: 현재 사이트에 있는 사용자를 실시간으로 확인할 수 있습니다. 재실(Presence) 상태는 **경계 구역**(Perimeter Zone)에 설정한 입실 및 퇴실 장치의 인증 기록을 기준으로 계산됩니다. 자세한 내용은 다음 문서를 참고하세요.
  - 구역 관리하기
  - 재실 확인하기
- **활성화된 사용자**: 등록 및 활성화된 사용자의 총 수를 확인할 수 있습니다. 카드를 클릭하면 **사용자 관리** 메뉴로 이동할 수 있습니다.
- **장치**: 등록된 장치 수를 확인할 수 있습니다. 카드를 클릭하면 **장치 관리** 메뉴로 이동할 수 있습니다.
- **잔여 크레딧**: 계정 크레딧의 잔여 잔액을 확인할 수 있습니다. 카드를 클릭하면 **설정** → **크레딧 센터** 메뉴로 이동할 수 있습니다.
- **사용량**: 장치 그룹, 빈도(일일, 주간, 월간) 또는 원하는 날짜를 지정해 범위별로 정렬할 수 있습니다.
- **최근 활동**: 로그인, 장치 업데이트, 사용자 생성 등 관리자가 수행한 작업에 대한 활동 로그를 표시합니다.

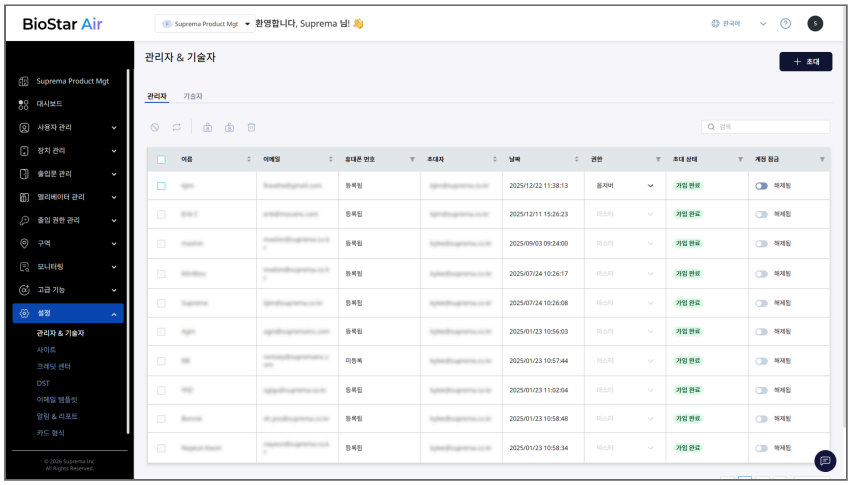
사이트 설정 단계별 안내

다음 안내에 따라 새로운 사이트를 설정하세요.

1 관리자 추가

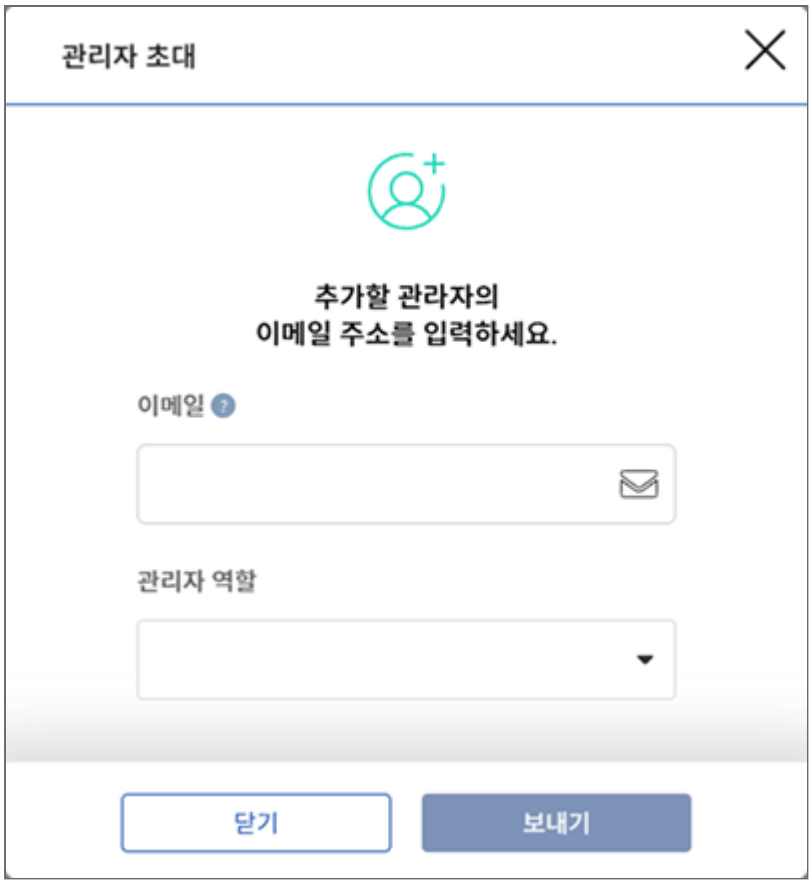
관리자를 초대하세요.

1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.



2. 화면 오른쪽 상단의 **초대** 버튼을 클릭하세요.

3. **관리자 초대** 창이 나타나면 관리자의 이메일 주소를 입력하고 역할을 부여하세요.

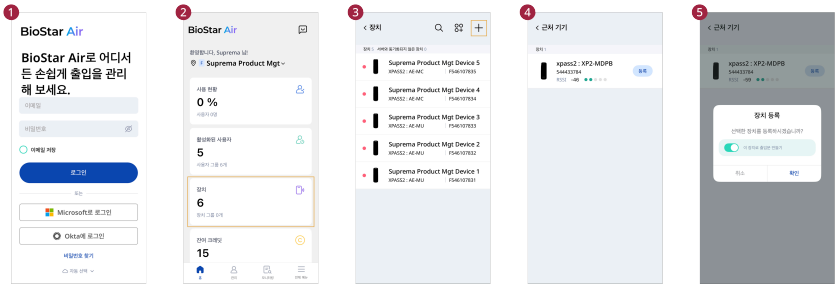


4. **보내기** 버튼을 클릭하세요.

> **알아두기**
> 사이트 관리자는 사이트를 관리할 수 있으며, 인증된 사용자는 **슈프리마 패스** 앱을 통해서만 접근할 수 있습니다.

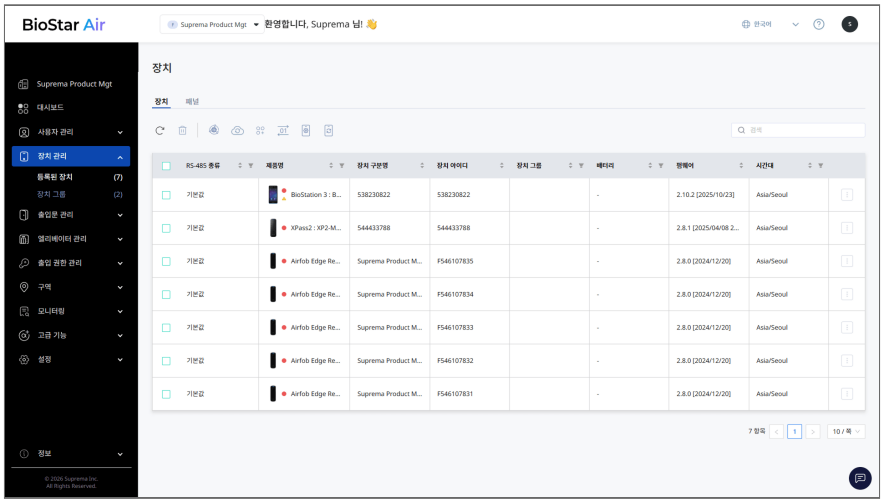
2 장치 등록

BioStar Air 모바일 앱을 사용하여 장치를 등록할 수 있습니다. 장치 등록은 Bluetooth Low Energy(BLE) 방식으로 이루어지며, 등록된 장치는 BioStar Air 포털에서 관리할 수 있습니다.



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. **장치** 카드를 탭하세요.
3. 화면 오른쪽 상단의 ＋ 버튼을 탭하세요.
4. 장치 검색 화면에서 등록하려는 장치의 **등록** 버튼을 탭하세요.
5. 장치 등록 창이 나타나면 **확인** 버튼을 탭하세요.

장치 목록으로 돌아가 추가된 장치를 확인하세요. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.

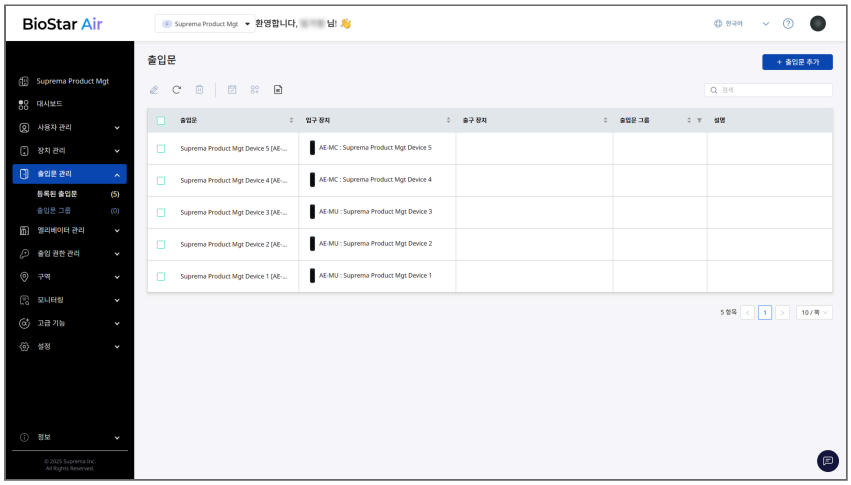


- 장치를 등록하지 않았다면, 다른 관리자가 BioStar Air 모바일 앱을 사용하여 현장에서 등록해야 합니다.
- **등록된 장치**에서는 장치 삭제, 펌웨어 업데이트 및 장치 그룹을 관리할 수 있습니다.

3 출입문 생성 및 관리

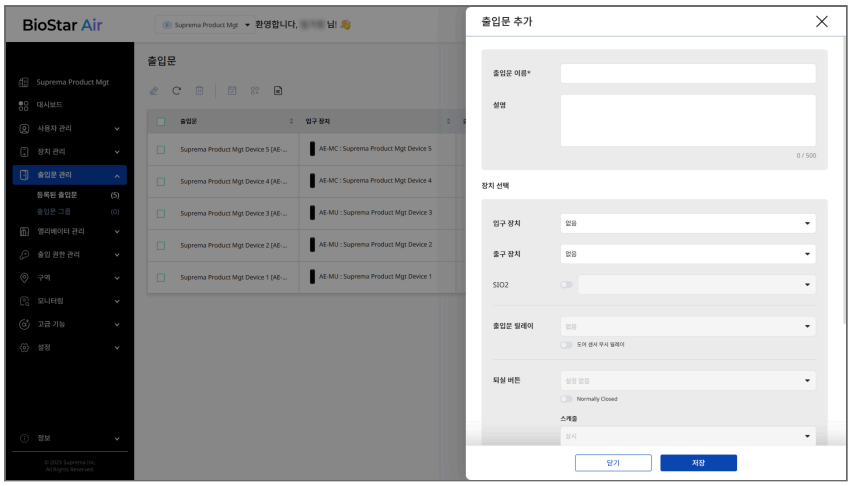
출입문을 추가하고 장치를 할당하세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.



2. 출입문이 없으면 화면 오른쪽 상단의 **출입문 추가** 버튼을 클릭하세요.

3. **출입문 추가** 패널이 나타나면 이름과 설명을 입력하세요.



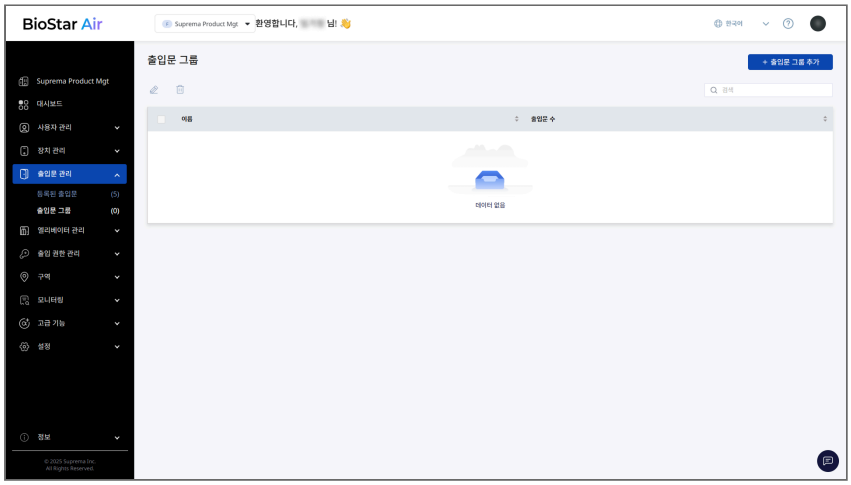
4. 등록된 장치를 **입구 장치** 및 **출구 장치**에 할당하세요.

출입문 관리에서는 출입문 편집 및 삭제, 출입 스케줄을 설정하고, 그룹으로 관리할 수 있습니다.

4 출입문을 그룹으로 분류

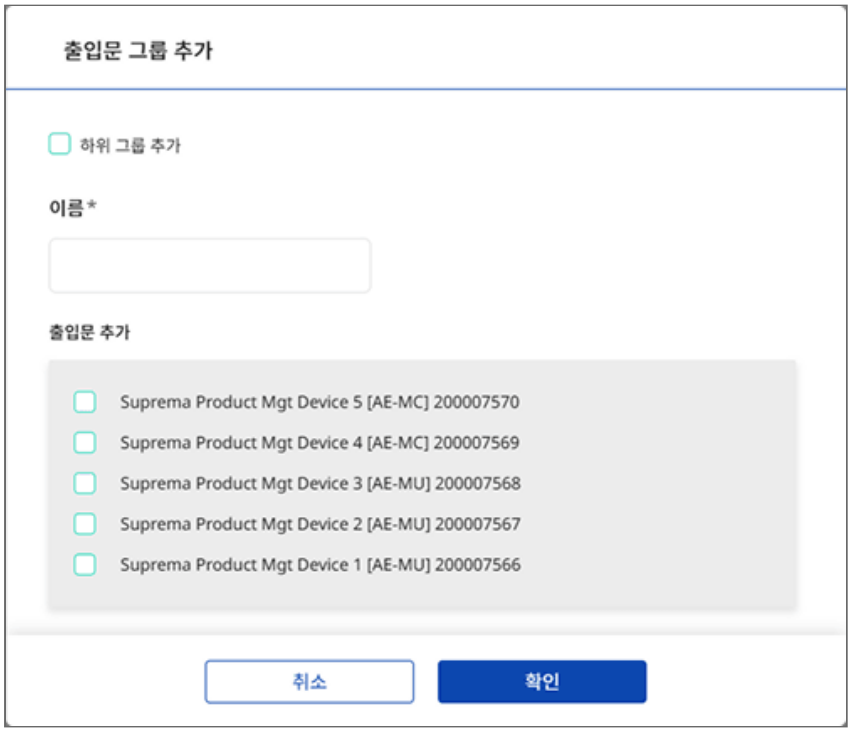
출입문을 그룹으로 분류하세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **출입문 그룹**을 클릭하세요.



2. 화면 오른쪽 상단의 **출입문 그룹 추가** 버튼을 클릭하세요.

3. **출입문 그룹 추가** 창이 나타나면 그룹 이름을 **실내, 실외** 또는 **Trap Doors**와 같은 형식으로 이름을 입력하고 원하는 출입문을 선택하세요.



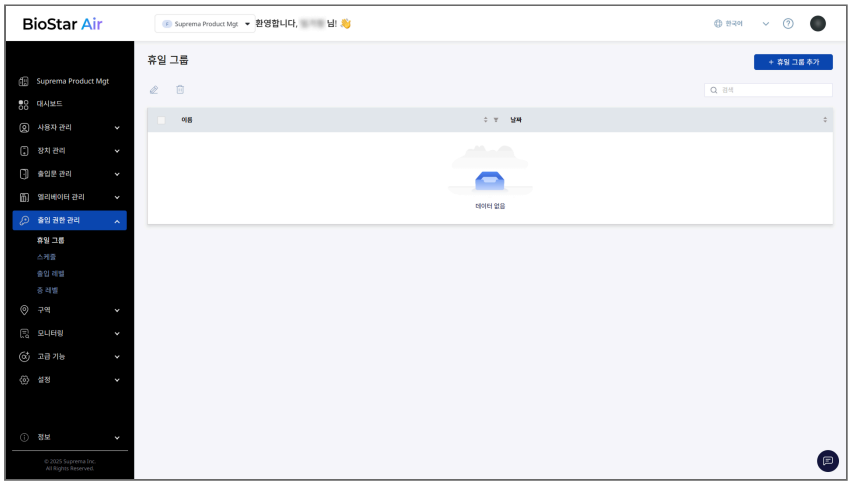
4. 출입문을 모두 선택했으면 **확인** 버튼을 클릭하세요.

5 출입 권한 설정

출입 권한을 관리하려면 다음 단계를 따르세요.

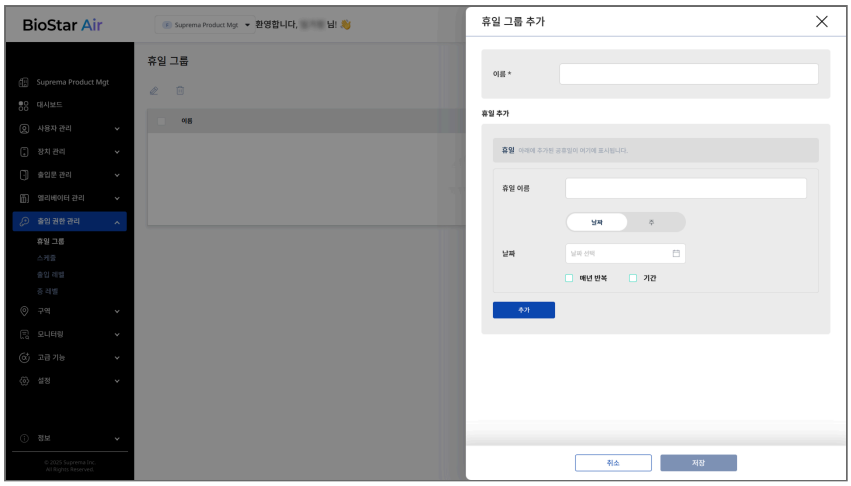
6 휴일 그룹 설정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **휴일 그룹**을 클릭하세요.



2. 화면 오른쪽 상단의 **휴일 그룹 추가** 버튼을 클릭하세요.

3. **휴일 그룹 추가** 패널이 나타나면 이름을 입력하세요 (예: '한국 휴일').

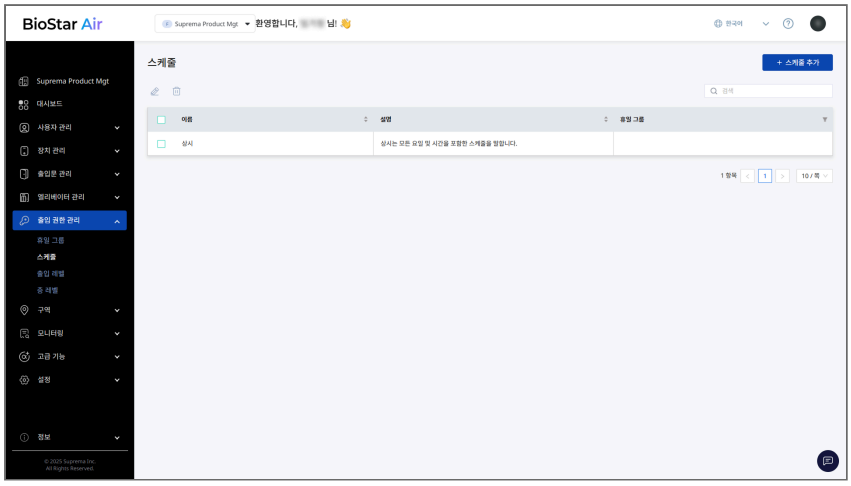


4. **휴일 추가** 섹션에서 출입을 제한할 공휴일을 설정하고, **추가** 버튼을 클릭하세요.

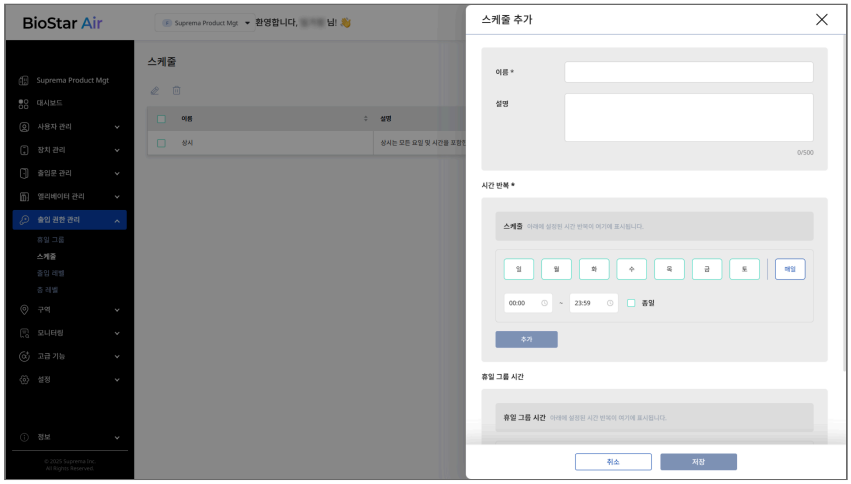
5. 모든 휴일을 추가했으면 **저장** 버튼을 클릭하세요.

7 스케줄 만들기

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **스케줄**을 클릭하세요.



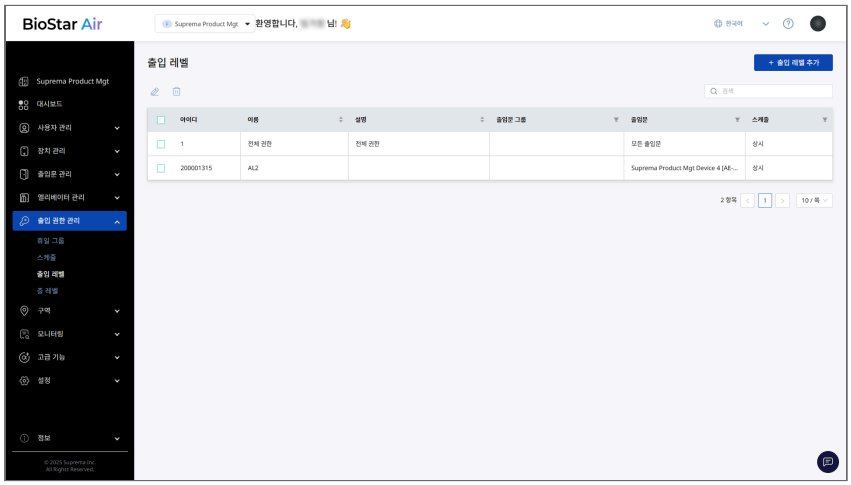
2. 화면 오른쪽 상단의 **스케줄 추가** 버튼을 클릭하세요.
3. **스케줄 추가** 패널이 나타나면 이름을 입력하세요.



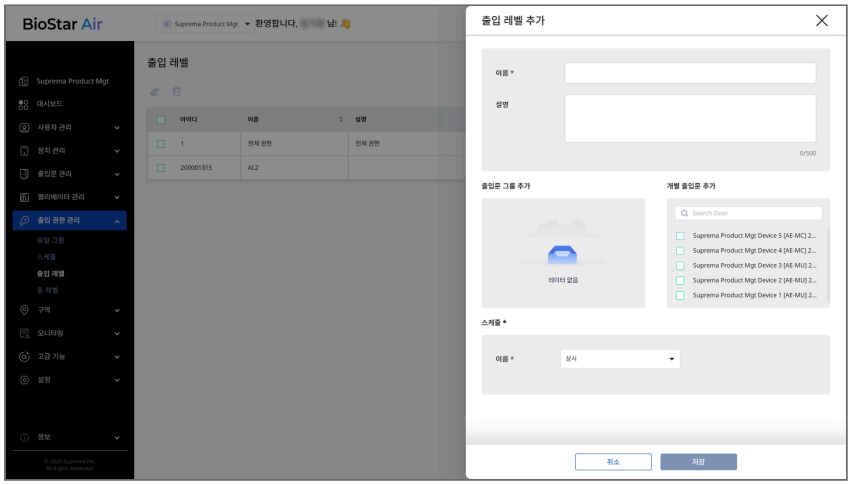
4. 활성화할 요일을 선택하고 휴일 그룹을 연결하세요.
5. 스케줄 설정을 완료하면 **저장** 버튼을 클릭하세요.

8 출입 레벨 설정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **출입 레벨**을 클릭하세요.



2. 화면 오른쪽 상단의 **출입 레벨 추가** 버튼을 클릭하세요.
3. **출입 레벨** 패널이 나타나면 이름을 입력한 후, 출입문 그룹, 개별 출입문 및 스케줄을 할당하세요.

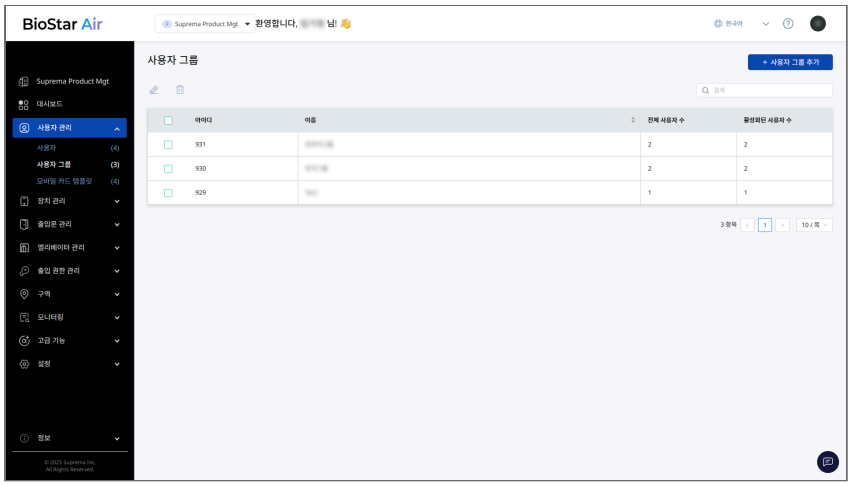


4. 출입 레벨 설정을 완료하면 **저장** 버튼을 클릭하세요.

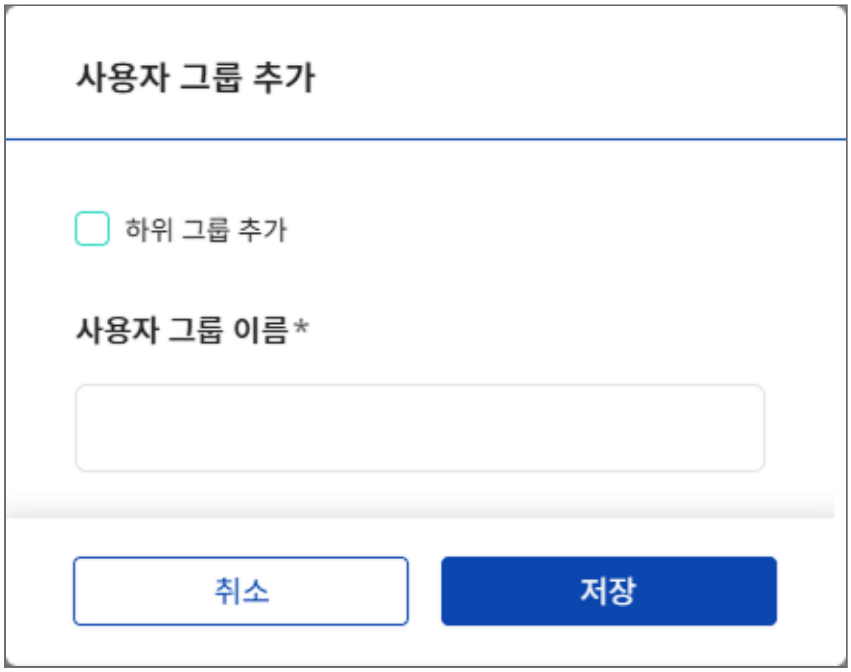
9 사용자 그룹 만들기 및 사용자 추가

사용자 그룹을 만들고, 새로운 사용자 그룹에 사용자를 추가하세요.

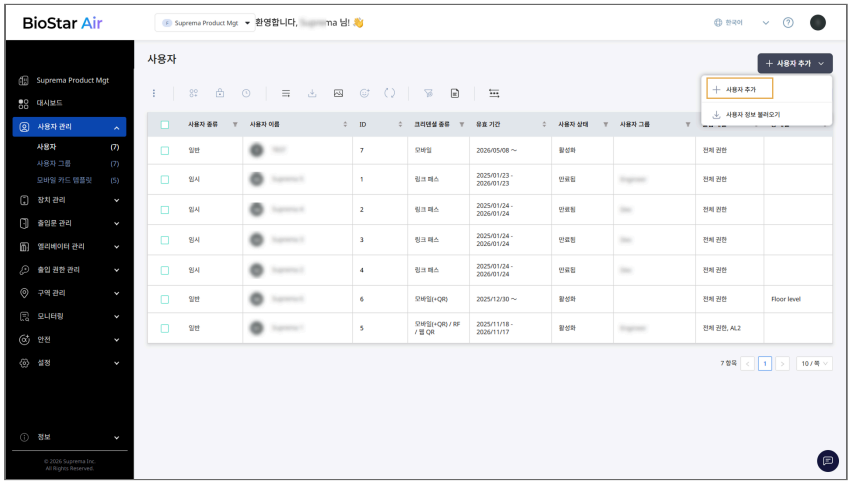
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자 그룹**을 클릭하세요.



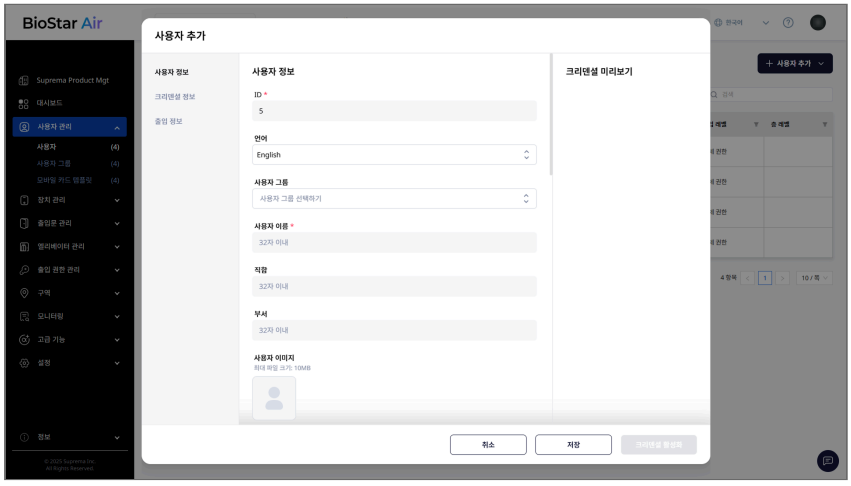
2. 화면 오른쪽 상단의 **사용자 그룹 추가** 버튼을 클릭하세요.
3. **사용자 그룹 추가** 창이 나타나면 사용자 그룹 이름을 입력하세요.



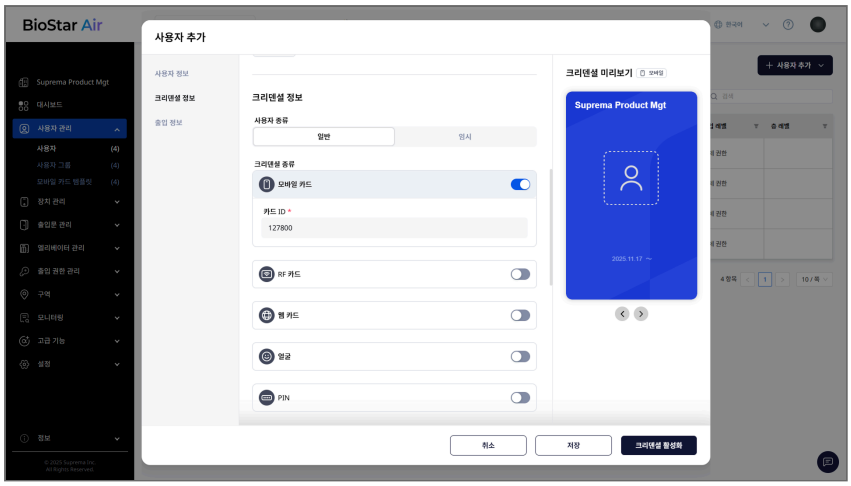
4. 사용자 그룹을 저장하려면 **저장** 버튼을 클릭하세요.
5. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
6. 화면 오른쪽 상단의 **사용자 추가** → **사용자 추가**를 클릭하세요.



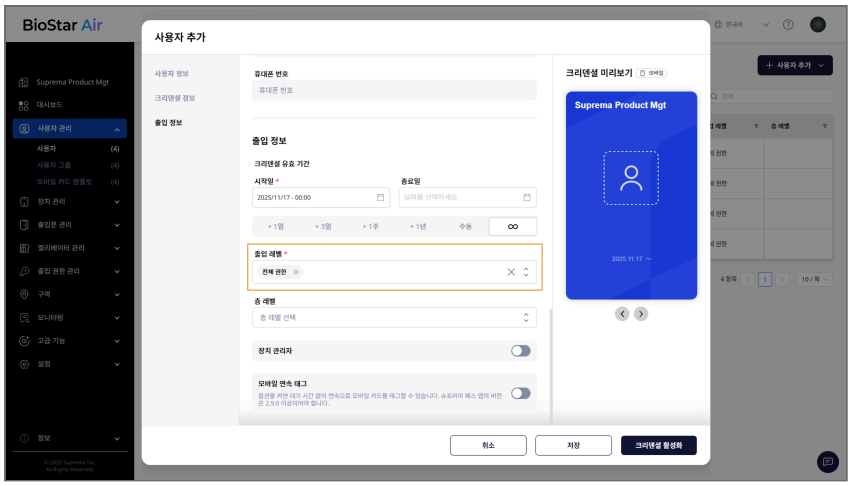
7. **사용자 추가** 창이 나타나면 **사용자 정보** 섹션에서 사용자의 ID, 이름 등을 입력하세요.



8. **크리덴셜 정보** 섹션에서 하나 이상의 인증 수단을 활성화하세요.



9. **출입 정보** 섹션에서 출입 레벨을 선택하세요.



10. 사용자의 접근 설정을 완료하려면 오른쪽 하단의 **크리덴셜 활성화** 버튼을 클릭하세요.

> **알아두기**
>
> **사용자 관리** → **사용자 그룹** 메뉴에서는 사용자를 대량으로 관리하고, 재발급, 정지 또는 삭제할 수 있으며, 데이터를 내보내고 프로필 이미지를 대량으로 업로드할 수도 있습니다.

팁

체크리스트

위 과정을 요약하자면 다음 단계에 따라 진행할 수 있습니다.

1. 관리자를 추가하세요.
2. 장치를 등록하세요.
3. 출입문을 생성하고 장치를 할당하세요.
4. 출입문을 그룹으로 분류하세요.
5. 출입 권한을 설정하세요 (휴일, 일정, 출입 등급).
6. 사용자 그룹을 만들고 사용자를 추가하세요.

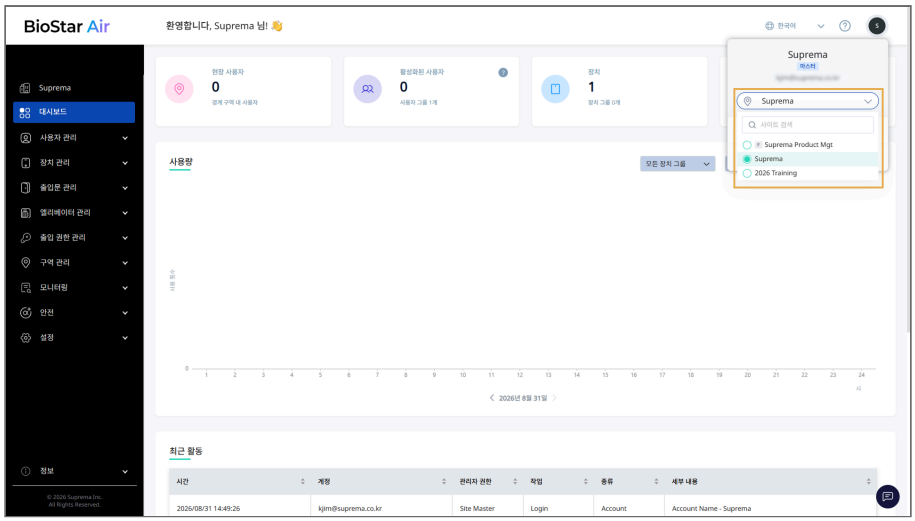
위 단계를 따르면 BioStar Air 사이트를 원활하게 설정할 수 있습니다. 제공하는 사용자 가이드에서 개별 비디오 튜토리얼을 참조하여 더 많은 세부 정보를 확인할 수 있습니다.

사이트 선택(Site Selector)

BioStar Air 포털에서 **사이트 선택**(**Site Selector**) 기능을 사용하면, 하나의 이메일 주소로 여러 사이트를 관리할 수 있어 프로세스가 간소화되고 여러 번 로그인할 필요가 줄어듭니다.

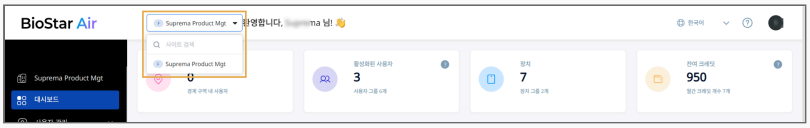
사이트 선택(Site Selector)이란?

사이트 선택 기능을 사용하면 여러 사이트를 관리할 때에도 하나의 통합된 이메일 주소로 BioStar Air 포털에 로그인할 수 있습니다. 각 사이트에 대해 서로 다른 이메일 주소로 로그인하지 않아도 됩니다. 하나의 이메일로 로그인하여 **사이트 선택** 메뉴를 이용하면 관리하는 사이트 간에 쉽게 전환할 수 있습니다.



알아두기

- 통합 이메일을 사용하더라도 각 사이트의 권한 및 설정은 독립적으로 유지됩니다. 관리자 역할과 접근 권한은 사이트마다 고유하게 관리됩니다.
- **사이트 선택** 기능이 보이지 않거나 잘못된 사이트가 표시된다면, 마이그레이션 요청이 완료되었는지 확인하거나 지원팀에 추가 지원을 요청하세요.
- **사이트 선택** 기능은 로그인 과정을 간소화하고 여러 사이트를 하나의 계정으로 통합함으로써 BioStar Air에서 여러 사이트를 관리하는 시간과 노력을 절약할 수 있습니다.
- 사이트 선택 목록에서 F 아이콘이 표시된 사이트는 페더렌이션 사이트(Federation site)입니다. 페더렌이션 사이트는 화면 왼쪽 상단에 표시됩니다. 페더렌이션 사이트에 대한 자세한 내용은 페더레이션 사이트 관리하기을 참고하세요.



새로운 사이트 생성

파트너 포털을 통해 새로운 사이트를 생성할 때, 다른 사이트의 관리자 계정으로 등록한 기존 이메일 주소를 사용할 수 있습니다. 시스템에서 새로운 사이트를 기존 이메일에 자동으로 연결하여 하나의 계정으로 여러 사이트를 관리할 수 있습니다.

- 파트너 포털을 통해 새로운 사이트를 생성하세요.
- 관리자의 이메일을 입력하라는 메시지가 표시되면, 다른 사이트와 이미 연결된 이메일 주소를 사용하세요.
- 새로운 사이트를 기존 계정에 자동 연결됩니다.

알아두기

파트너 포털 가입 및 사용에 대한 자세한 내용은 파트너 포털 사용하기을 참고하세요.

한 개의 이메일로 여러 사이트 관리

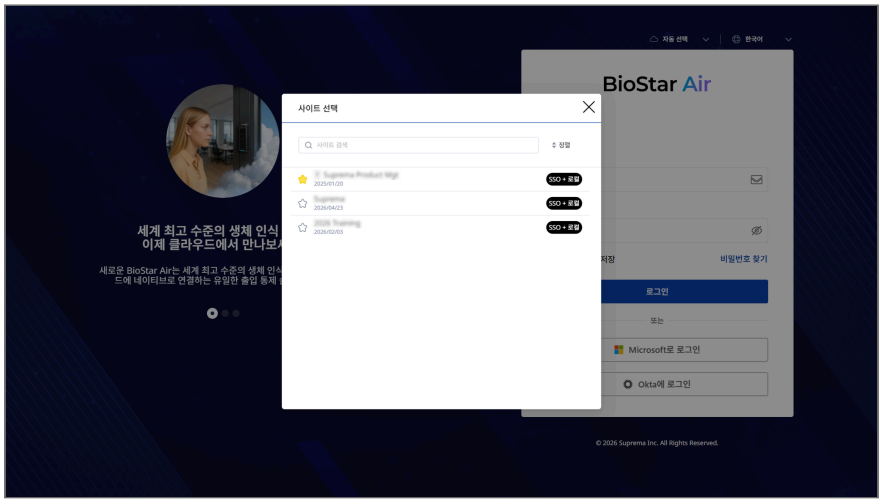
이미 여러 사이트를 관리하고 있지만 각 사이트마다 별도의 로그인 인증을 사용하고 있다면, **슈프리마**에 수동 마이그레이션을 요청해야 합니다. 이 프로세스를 통해 이메일 주소를 통합하여 모든 사이트를 단일 로그인으로 관리할 수 있습니다.

- 지원팀에 연락하여 사이트에 대한 수동 마이그레이션을 요청하세요.
- bob+site1@example.com 및 bob+site2@example.com과 같은 별칭 주소를 사용한다면 루트 이메일 주소(bob@example.com)를 제공하세요.
- 각 사이트에 대해 완전히 고유한 이메일 주소를 사용한다면 전체 이메일 목록을 제공해야 합니다.
- 마이그레이션이 완료되면 **사이트 선택** 기능을 통해 단일 이메일 주소로 모든 사이트에 액세스할 수 있습니다.

사이트 선택(Site Selector) 사용하기

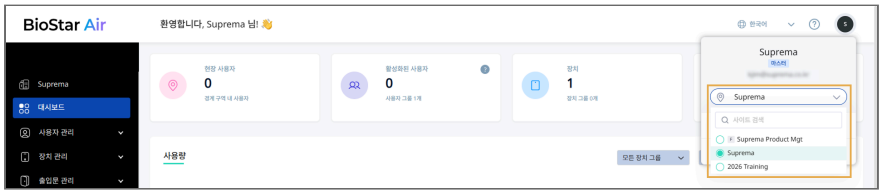
여러 사이트를 관리할 수 있는 이메일 주소가 있다면 로그인하고 사이트 간에 전환하는 것은 간단합니다.

1. 이메일 주소와 비밀번호를 입력하세요.
2. 여러 사이트를 관리한다면 **사이트 선택** 창을 통해 원하는 사이트를 빠르게 찾을 수 있습니다. 사이트를 선택하면 대시보드로 이동합니다.



3. 로그인한 후에는 화면 오른쪽 상단의 프로필 아이콘을 클릭하세요.

4. 팝업 메뉴가 나타나면 이메일 주소 아래의 **사이트 선택** 기능을 클릭하세요.



이메일 주소와 연결된 모든 사이트 목록을 확인할 수 있습니다.

BioStar Air 앱 시작하기

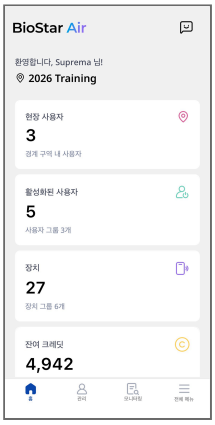
BioStar Air 앱은 BioStar Air 웹 포털과 동일한 모든 기능을 제공합니다. 사용자는 모바일 장치에서 직접 출입 통제를 관리하고, 이벤트 로그를 모니터링하며, 장치를 제어하고, 관리 작업을 수행할 수 있습니다.

모바일 앱 다운로드

모바일 기기에서 BioStar Air 앱을 다운로드하고 로그인하세요.

- 모바일 기기에 BioStar Air 앱을 다운로드하여 설치하세요.
  - iOS
  - Android
- BioStar Air 웹 포털에서 사용하는 아이디와 비밀번호로 로그인하세요.

> **알아두기**
>
> - 웹 버전과 동일한 크리덴셜로 로그인했는지 확인하세요.
> - BLE mode로 업데이트하려면 장치에 가까이 있어야 합니다.
> - 실시간 비디오 모니터링과 같은 일부 기능은 연결된 카메라가 필요합니다.



대시보드

모바일 앱에 로그인하면 초기 화면의 **대시보드**에서 아래와 같은 정보를 제공합니다.

- 일일 사용자 출입 수
- 총 등록된 활성 사용자 수
- 연결된 장치 수
- 크레딧 상태

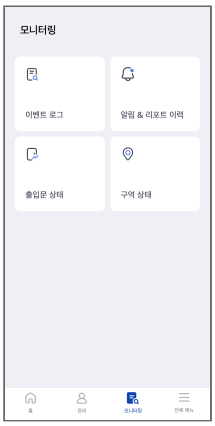


사용자 관리

초기 화면의 **활성화된 사용자** 카드를 탭하거나 **관리** → **사용자**를 차례로 탭하세요.

- 사용자를 선택하고 세부 정보를 확인하세요.
- 사용자 상태를 수정(재발급, 일시 중지, 삭제 또는 활성화)할 수 있습니다.
- 새 사용자를 추가하려면 ＋ 버튼을 탭하고 필요한 세부 정보를 입력하세요.

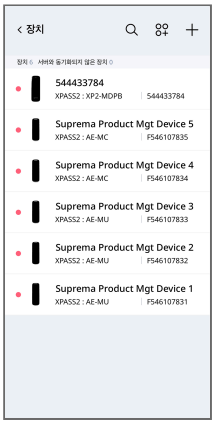
> **알아두기**
>
> - 모바일 앱에서 사용자 추가 방법은 사용자 추가하기를 참고하세요.
> - BioStar Air 포털에서 사용자 추가 방법은 사용자 추가하기를 참고하세요.
> - 사용자 관리에 대한 자세한 내용은 사용자 관리하기를 참고하세요.



모니터링

모니터링에서는 아래와 같은 정보를 제공합니다.

- **이벤트 로그**: 이벤트 로그와 감사 로그를 모니터링하고 분석할 수 있습니다. 자세한 내용은 이벤트 로그 사용하기와 변경 로그 사용하기를 참고하세요.
- **알림 & 리포트 이력**: 웹 포털과 모바일 앱을 통해 이전에 발생한 알림과 생성된 리포트 내역을 조회할 수 있습니다. 자세한 내용은 알림 & 리포트 이력 확인하기를 참고하세요.
- **출입문 상태**: 사이트에 연결된 출입문의 상태를 실시간으로 모니터링할 수 있습니다. 자세한 내용은 출입문 상태 모니터링하기를 참고하세요.
  - 출입문 상태를 확인하고 원격으로 제어할 수 있습니다.
  - 한 번 탭하여 출입문을 편집하거나 길게 눌러 여러 출입문을 선택하고 일괄 작업을 수행할 수 있습니다.
  - 출입문을 **항상 열림** 또는 **폐쇄 모드**로 설정하면 릴레이 설정 또는 일정을 무시합니다.
  - 필요에 따라 사용하지 않는 출입문은 삭제하세요.
- (연결된 카메라가 있는 경우) 실시간 비디오



장치

초기 화면의 **장치** 카드를 탭하거나 **관리** → **장치**를 차례로 탭하세요.

- 모든 등록된 장치를 확인할 수 있습니다.
- 장치를 선택하고 편집, 펌웨어 업데이트 또는 재부팅할 수 있습니다.
- 네트워크에 연결되지 않은 장치는 펌웨어 업데이트를 위해 모바일 기기와 가까운 거리에서 **BLE 모드**를 사용하세요.
- 새 장치를 추가하려면 ＋ 버튼을 탭하세요.

> **알아두기**
> 장치 관리에 대한 자세한 내용은 다음 문서를 참고하세요.
> - BioStar Air App: 엣지 장치 등록 및 삭제하기
> - BioStar Air 포털: 장치

사이트 관리하기

BioStar Air에서 **사이트**는 출입 통제 시스템의 핵심 단위로, 사용자가 출입할 수 있는 물리적 위치를 의미합니다. 각 사이트는 고유한 설정, 사용자, 장치 및 접근 권한을 가질 수 있습니다. 관리자는 여러 사이트를 생성하고 관리하여 다양한 위치에서 출입 통제를 효율적으로 운영할 수 있습니다.

다음 제공하는 문서를 통해 BioStar Air 포털에서 사이트를 효과적으로 관리하는 방법을 알아보세요.

사용자

BioStar Air에서 사용자 계정을 생성하고, 다양한 크리덴셜(Mobile Card, RF Card, Web Card, Face, PIN)을 설정하며, 출입 권한과 유효 기간을 구성하는 방법을 안내합니다. 개별 사용자 관리부터 여러 사용자에 대한 일괄 작업, 사용자 그룹 및 필터링 관리까지 사용자 관리의 전반적인 작업을 다룹니다.

> **팁**
> 사용자 관리 기능은 제공하는 다음 동영상을 통해서 더 쉽게 이해할 수 있습니다.

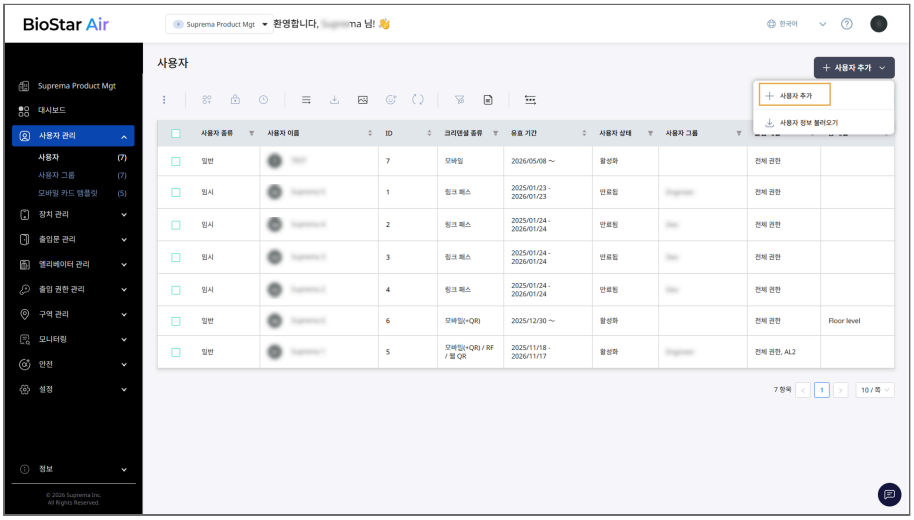
사용자 추가하기
이 문서는 BioStar Air에서 개별 사용자를 추가하고 관리하는 방법을 단계별로 안내합니다. 사용자 유형(일반/임시)을 선택하고, 각 유형에 맞는 크리덴셜을 발급하며, 출입 레벨과 유효 기간을 설정하는 전체 과정을 다룹니다. 추가한 사용자의 정보를 수정하거나 삭제하는 방법도 포함합니다.

> **팁**
> 새로운 사용자 추가에 대한 전체 과정을 단계별로 안내하는 다음 동영상을 참고하세요.

사용자 추가 시작

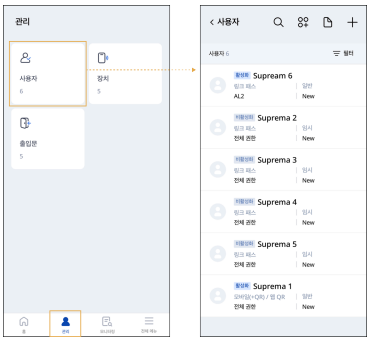
Web

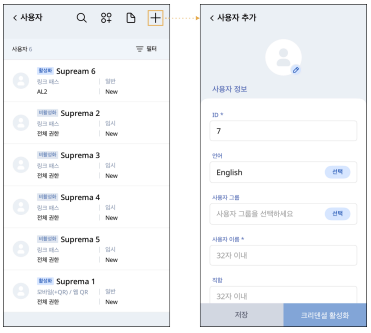
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록이 나타납니다.
3. 화면 오른쪽 상단의 **사용자 추가** → **사용자 추가**를 클릭하세요.



사용자 추가 창이 나타나면 각 섹션마다 필요한 정보를 입력하고 설정하세요. 모든 섹션의 필수 항목을 설정하고 오른쪽 하단의 **크리덴셜 활성화** 버튼을 클릭하세요.

Mobile





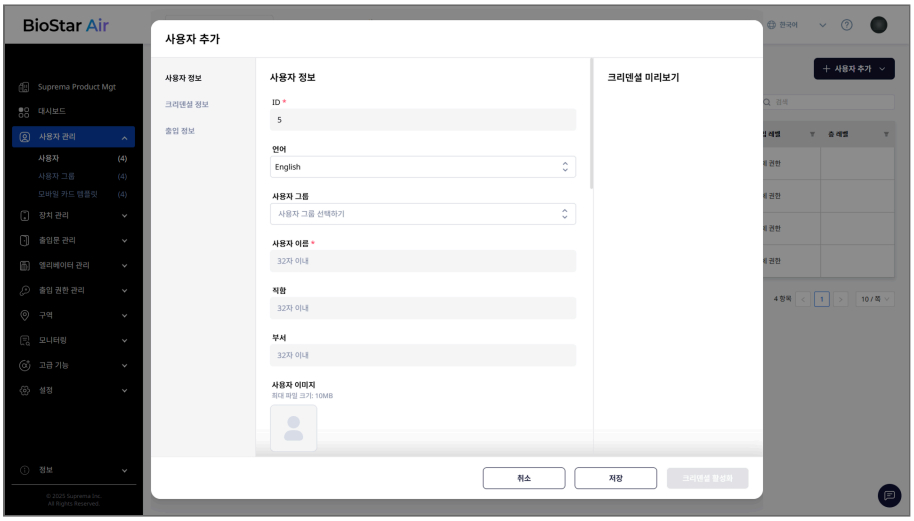
1. 모바일 앱으로 로그인하세요.
2. 화면 하단의 **관리**를 탭하세요.
3. **사용자** 카드를 탭하세요.
4. 사용자 목록 화면 상단의 ＋ 버튼을 탭하세요.

사용자 추가 화면이 나타나면 각 섹션마다 필요한 정보를 입력하고 설정하세요. 모든 섹션의 필수 항목을 설정하고 오른쪽 하단의 **크리덴셜 활성화** 버튼을 클릭하세요.

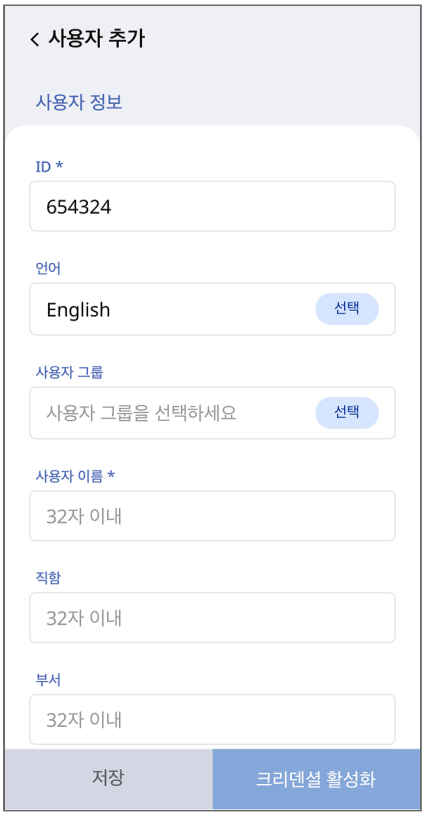
사용자 정보 입력

사용자 정보 섹션에서 새롭게 추가하는 사용자에 대한 기본 정보를 입력하세요.

Web



Mobile



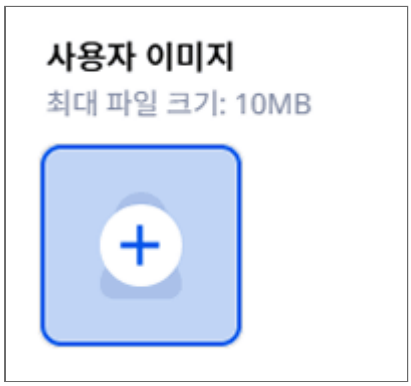
- **ID**: 특정 아이디를 직접 입력하거나 시스템이 순차적으로 생성하도록 허용할 수 있습니다.
- **언어**: 사용자의 기본 언어를 선택하세요.
- **사용자 그룹**: 사용자가 속할 그룹을 선택하세요.
- **사용자 이름**: 사용자의 전체 이름을 입력하세요.
- **직함**: 사용자의 직함을 입력하세요.
- **부서**: 사용자가 속한 부서 이름을 입력하세요.
- **사용자 이미지**: 사용자의 프로필 이미지를 업로드할 수 있습니다. 자세한 내용은 프로필 이미지 업로드를 참고하세요.

> **알아두기**
>
> - * 표시는 필수 입력 항목입니다.
> - 사용자의 이메일과 전화번호는 **크리덴셜 정보** 섹션의 **초대 링크 전송 방법** 항목에서 입력할 수 있습니다.

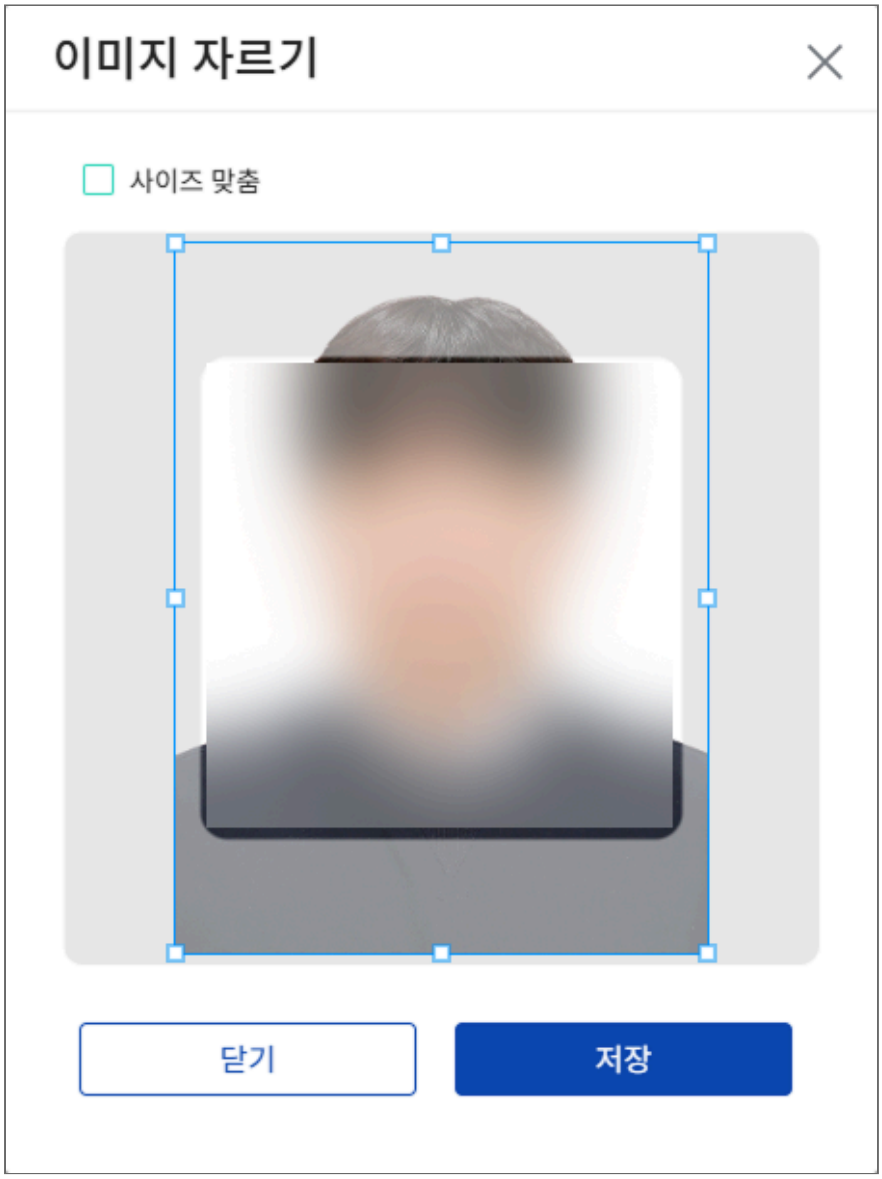
프로필 이미지 업로드

Web

1. 프로필 이미지 영역에 마우스를 오버하고 플러스 버튼을 클릭하세요.

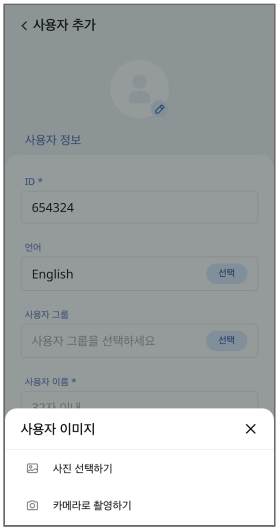


2. 로컬에 저장된 이미지 파일을 선택하세요.
3. **이미지 자르기** 창이 나타나면 원하는 크기로 사진을 조정하세요. 자동으로 이미지 크기를 맞추려면 **사이즈 맞춤** 옵션을 클릭하세요.



4. 업로드한 이미지를 프로필로 저장하려면 **저장** 버튼을 클릭하세요.

Mobile



1. 사용자 프로필 이미지를 탭하세요.
2. 하단에 나타나는 메뉴에서 원하는 방법으로 이미지를 추가하세요.
   - **사진 선택하기**: 모바일 기기에 저장된 이미지 파일을 선택해 업로드할 수 있습니다.
   - **카메라로 촬영하기**: 모바일 기기의 카메라로 사진을 찍어 업로드할 수 있습니다.
3. 업로드한 이미지를 적당한 크기로 조정하고 저장하세요.

사용자 종류 선택

Web

크리덴셜 정보 섹션에서 추가하는 사용자가 일반 사용자인지, 임시로 방문하는 사용자인지 선택하세요. 사용자 종류에 따라 발급할 수 있는 크리덴셜 종류가 달라집니다.

- **일반**: 조직 또는 시설의 정규 구성원으로서 장기적이고 지속적인 출입 권한이 필요한 사용자입니다. 모든 크리덴셜 유형을 발급할 수 있습니다.



- **임시**: 단기적이고 제한적인 출입 권한이 필요한 방문자 또는 비정규 구성원입니다. 게스트, 외부 방문객, 단기 계약자, 배송 기사 등이 해당될 수 있습니다. QR 코드와 링크 패스(LinkPass)를 포함한 **웹 카드** 크리덴셜만 발급할 수 있습니다.



Mobile

사용자 종류에서 추가하는 사용자가 일반 사용자인지, 임시로 방문하는 사용자인지 선택하세요. 사용자 종류에 따라 발급할 수 있는 크리덴셜 종류가 달라집니다.



- **일반**: 조직 또는 시설의 정규 구성원으로서 장기적이고 지속적인 출입 권한이 필요한 사용자입니다. 모든 크리덴셜 유형을 발급할 수 있습니다.
- **임시**: 단기적이고 제한적인 출입 권한이 필요한 방문자 또는 비정규 구성원입니다. 게스트, 외부 방문객, 단기 계약자, 배송 기사 등이 해당될 수 있습니다. QR 코드와 링크 패스(LinkPass)를 포함한 **웹 카드** 크리덴셜만 발급할 수 있습니다.

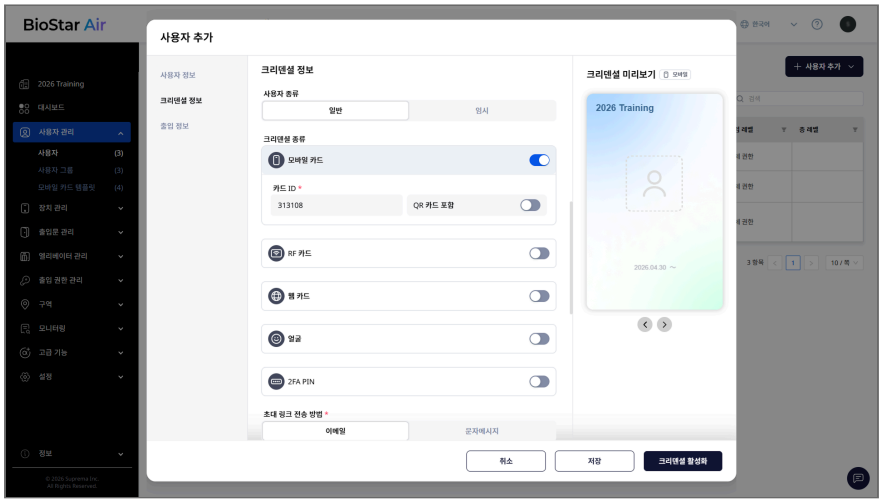
> **알아두기**
>
> - **일반** 유형의 사용자는 자동으로 전체 출입 레벨이 할당될 수 있는 반면, **임시** 유형의 사용자는 수동으로 출입 레벨을 선택해야 합니다.
> - **사용자 종류**는 BioStar Air 2.6 버전 이상에서 지원합니다.

크리덴셜 발급

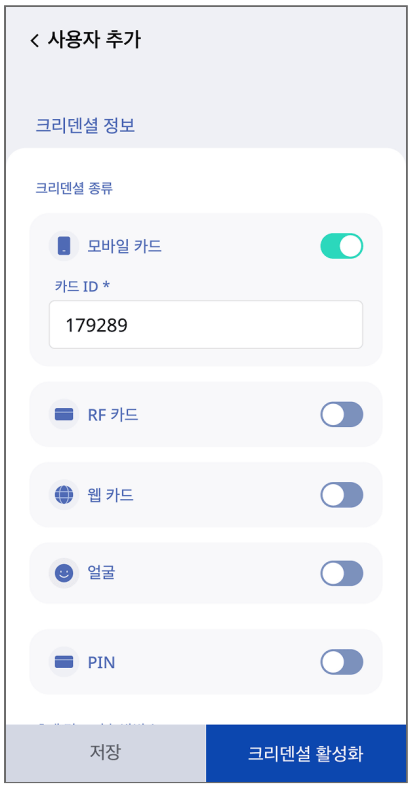
사용자 정보를 입력한 후, **크리덴셜 정보** 섹션에서 출입 인증 수단으로 사용할 크리덴셜을 설정하세요. 각 크리덴셜에는 활성화 또는 비활성화할 수 있는 토글 스위치가 있습니다.

- **모바일 카드**: 슈프리마 패스 모바일 앱을 출입 인증 수단으로 사용할 수 있습니다. 관리자는 카드 ID 번호를 편집할 수 있습니다.

Web

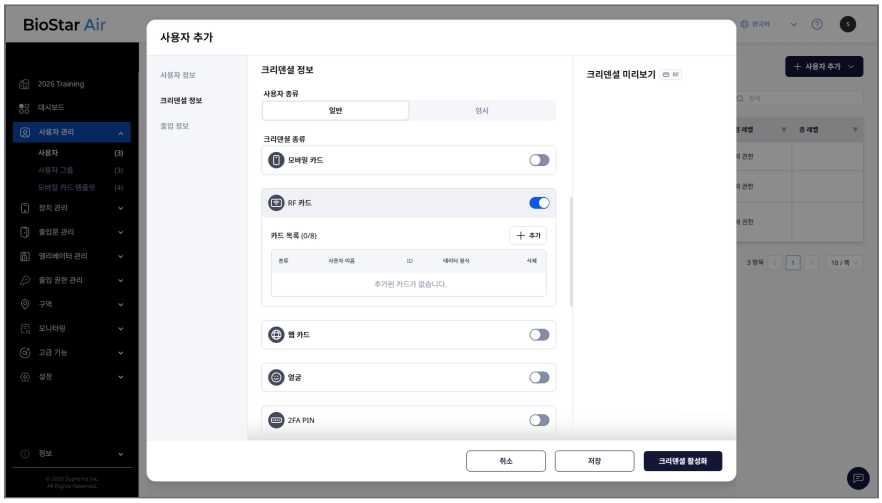


Mobile

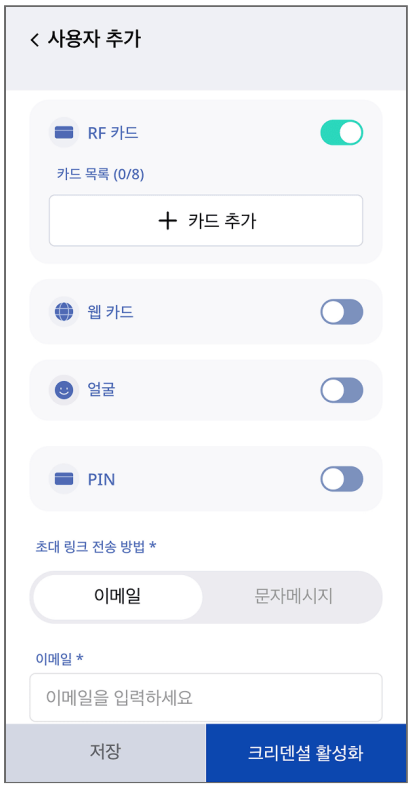


- **RF 카드**: 사용자당 최대 8개의 RFID 카드를 출입 인증 수단으로 추가할 수 있습니다. **추가** 버튼을 클릭하세요.

Web



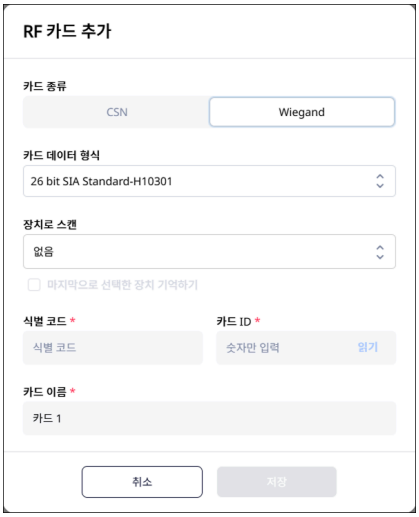
Mobile



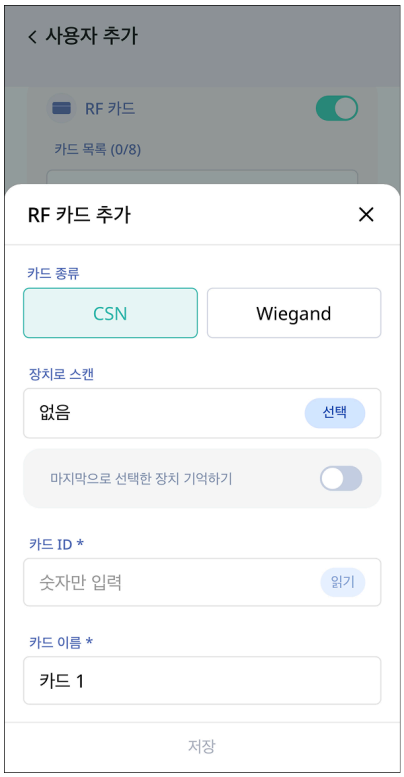
카드 종류(CSN / Wiegand), 카드 ID 및 카드 이름을 구성할 수 있습니다. **장치로 스캔** 항목에서 리더기를 선택하세요. 연결된 리더기를 사용하여 실물 RFID 카드를 스캔할 수도 있습니다.

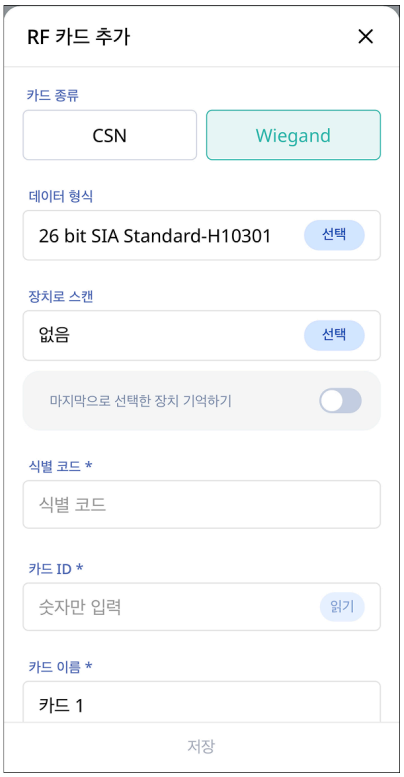
Web





Mobile



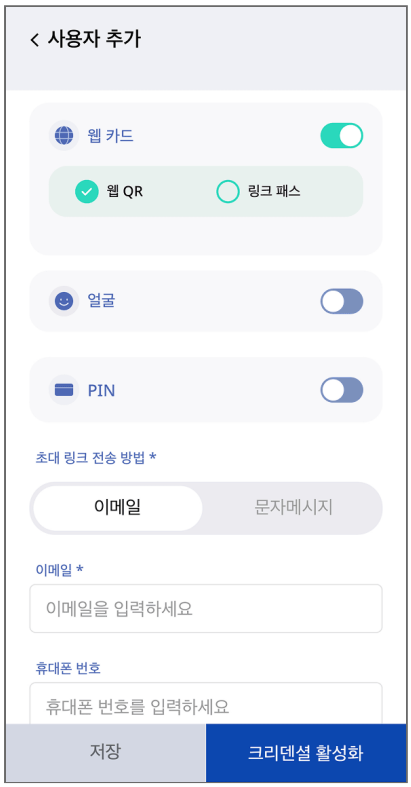


- **웹 카드**: **웹 QR** 또는 **링크 패스**을 출입 인증 수단으로 사용할 수 있습니다.

Web



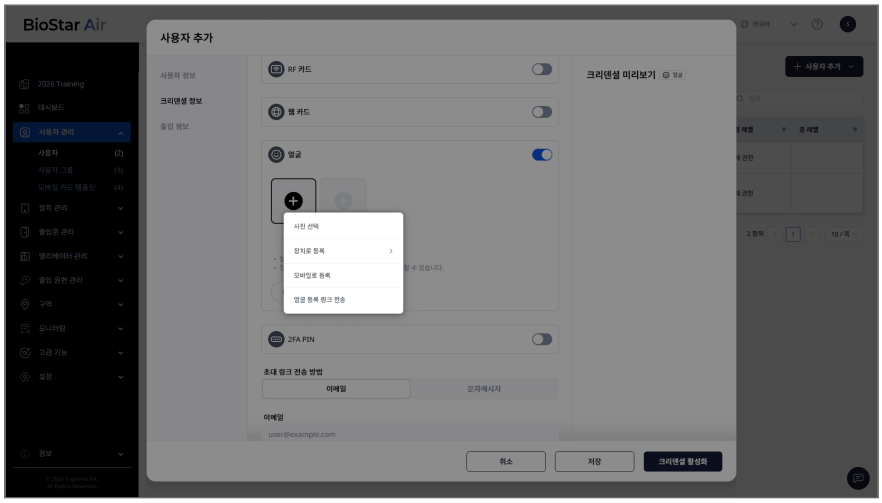
Mobile



> **웹 QR**은 **설정** → **사이트** → **추가 기능**에서 **QR 리더 사용** 옵션을 활성화해야 나타납니다.

- **얼굴**: 출입 인증 수단으로 얼굴 프로필 이미지를 최대 2개까지 추가할 수 있습니다. 기존 이미지를 업로드하거나 장치를 통해 등록할 수 있습니다. 또는 이메일이나 문자 메시지로 링크를 사용자에게 보내서 사용자의 모바일 기기 카메라를 사용해 직접 등록하는 방법도 있습니다.

Web

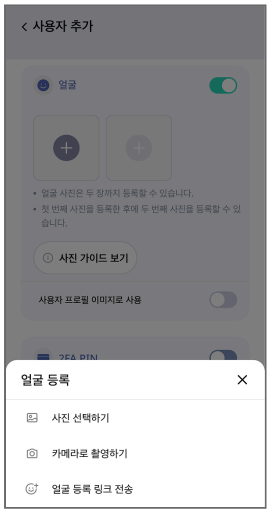


- **사진 선택**: 로컬에 저장된 이미지 파일을 선택하여 업로드할 수 있습니다.
- **장치로 등록**: 등록된 장치를 사용하여 얼굴 이미지를 등록할 수 있습니다.
- **모바일로 등록**: 모바일 기기의 카메라로 QR 코드를 스캔하면 얼굴 이미지를 등록할 수 있는 링크로 이동할 수 있습니다.



- **얼굴 등록 링크 전송**: 사용자의 이메일이나 문자 메시지로 얼굴 등록 링크를 보내 모바일 기기의 카메라로 직접 얼굴을 등록할 수 있습니다.

Mobile



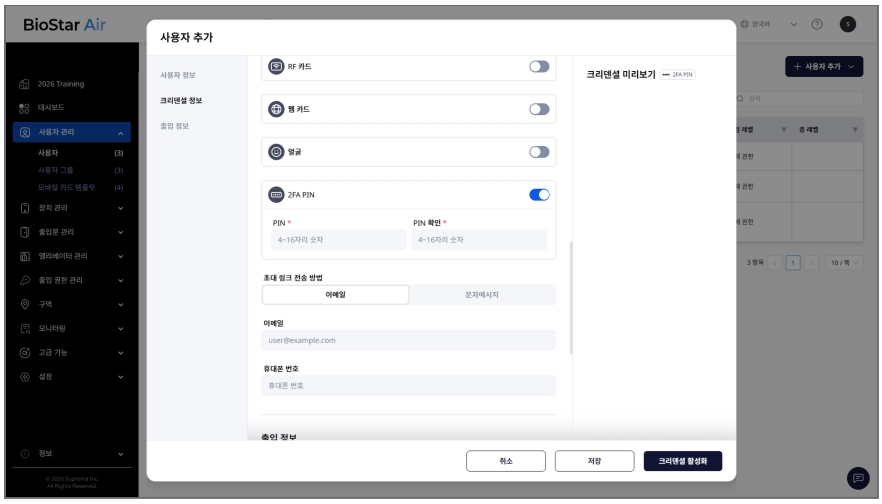
얼굴 사진을 추가하려면 ＋ 버튼을 탭하세요. 하단에 나타나는 메뉴에서 원하는 방법으로 얼굴 사진을 추가할 수 있습니다.

- **사진 선택하기**: 모바일 기기에 저장된 이미지 파일을 선택해 업로드할 수 있습니다.
- **카메라로 촬영하기**: 모바일 기기의 카메라로 사진을 찍어 업로드할 수 있습니다.
- **얼굴 등록 링크 전송**: 사용자의 이메일로 얼굴 등록 링크를 보내 모바일 기기의 카메라로 직접 얼굴을 등록할 수 있습니다.
- **사용자 프로필 이미지로 사용**: 프로필로 사용 중인 이미지를 얼굴 크리덴셜로 사용할 수 있습니다.

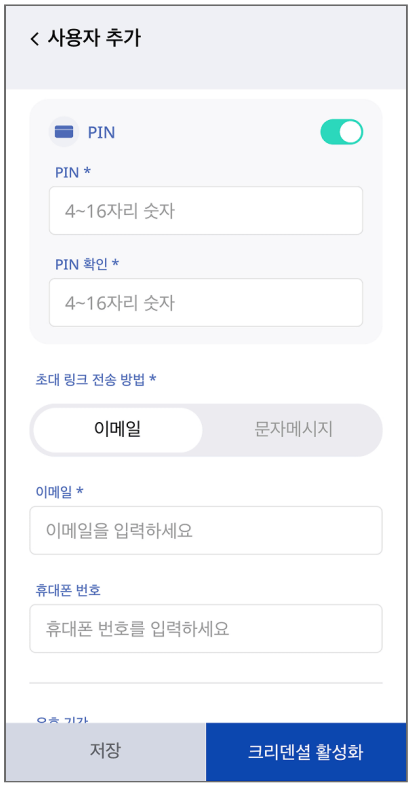
> 얼굴 사진 등록에 대한 자세한 내용을 확인하려면 **사진 가이드 보기** 버튼을 클릭하세요.

- **2FA PIN**: 4~16자리 PIN을 설정하여 2단계 인증(2FA)의 일부로 사용할 수 있습니다.

Web



Mobile



초대 링크 전송

모바일 카드 또는 **웹 카드**를 사용하는 사용자에게 슈프리마 패스 앱 다운로드 링크를 이메일로 전송할 수 있습니다. 이메일 주소(필수)와 휴대폰 번호(선택 사항)를 입력하세요.

Web



Mobile

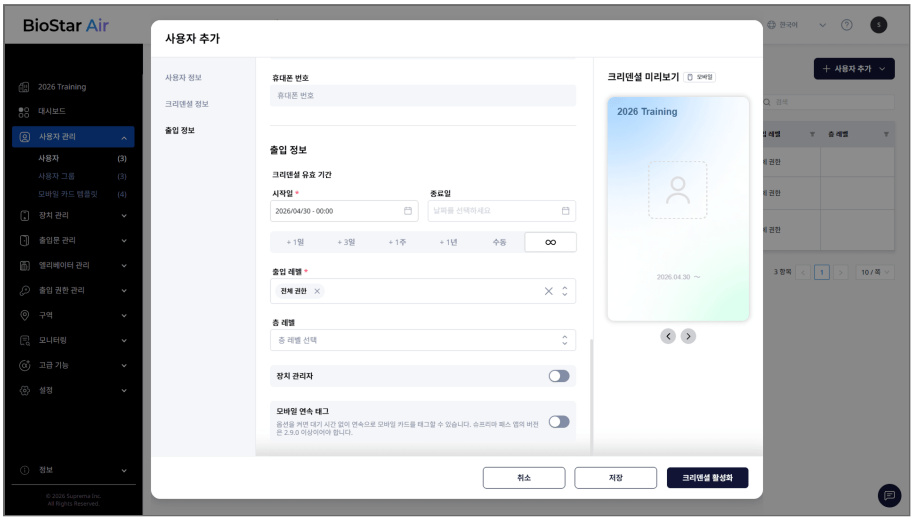


> **알아두기**
> **문자메시지** 옵션은 **설정** → **크레딧 센터**에서 SMS 크레딧 충전을 요청해야 사용할 수 있습니다.

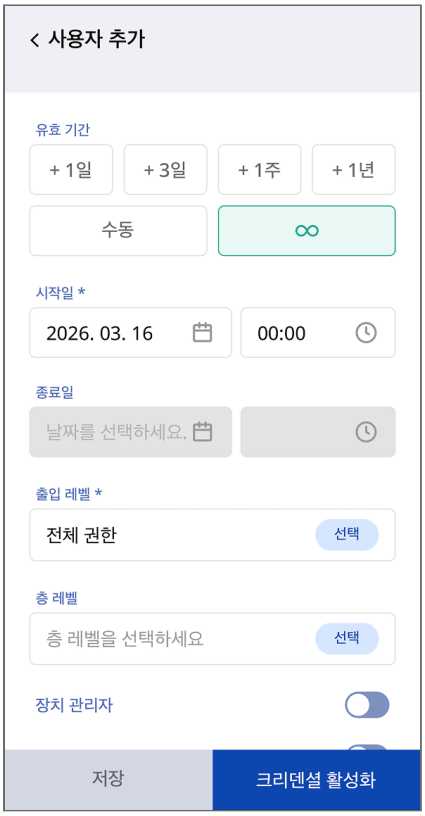
출입 레벨 및 유효성 설정

크리덴셜을 선택한 후 **출입 정보** 섹션에서 사용자의 크리덴셜 유효 기간, 출입 레벨 및 층 레벨 등을 구성하세요.

Web



Mobile



- **크리덴셜 유효 기간**: 사용자에게 발급한 크리덴셜의 유효 기간을 설정하세요. 종료일을 설정하지 않으려면 ∞ 버튼을 클릭하세요.
- **출입 레벨**: 사용자가 출입할 수 있는 권한을 선택하세요. 전체 권한을 부여하거나 사전 정의된 출입 레벨을 선택하세요.
- **층 레벨**: 사용자가 출입할 수 있는 층 레벨을 선택하세요.
- **장치 관리자**: 사용자가 특정 장치에서 출입 권한을 관리할 수 있도록 허용할 수 있습니다.
- **모바일 연속 태그**: 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있도록 허용할 수 있습니다. 이 기능은 슈프리마 패스 앱 2.9.0 버전 이상에서 지원합니다.

> **알아두기**
>
> - 층 레벨 설정에 대한 자세한 내용은 층 레벨 관리하기를 참고하세요.
> - **장치 관리자** 옵션은 BioStation 3, X-Station 2 사용자만 사용할 수 있습니다. 장치 관리자로 설정된 사용자는 BioStation 3, X-Station 2 장치의 관리자 메뉴를 사용할 수 있습니다.

카드 템플릿 선택

Web

카드 템플릿의 디자인을 변경하려면 오른쪽 패널의 카드 템플릿 아래에서 < 또는 > 버튼을 클릭해 선택할 수 있습니다.



Mobile

카드 템플릿의 디자인을 변경하려면 **크리덴셜 미리보기**에서 ‹ 또는 › 버튼을 탭하여 선택할 수 있습니다.



> **알아두기**
> 새로운 카드 템플릿 생성 방법에 대한 자세한 내용은 카드 템플릿 관리하기를 참고하세요.

사용자 저장 또는 활성화

사용자에 대한 모든 설정을 구성하면 아래 옵션 중 하나를 선택할 수 있습니다.

- 사용자를 저장하고 나중에 활성화하려면 **저장** 버튼을 클릭하세요.
- 크리덴셜을 즉시 발급하고 활성화하려면 **크리덴셜 활성화** 버튼을 클릭하세요.

다음 단계

개별 사용자를 추가하는 방법을 확인했다면, 여러 사용자를 한번에 등록하는 방법에 대해 알아보세요.

사용자 관리하기

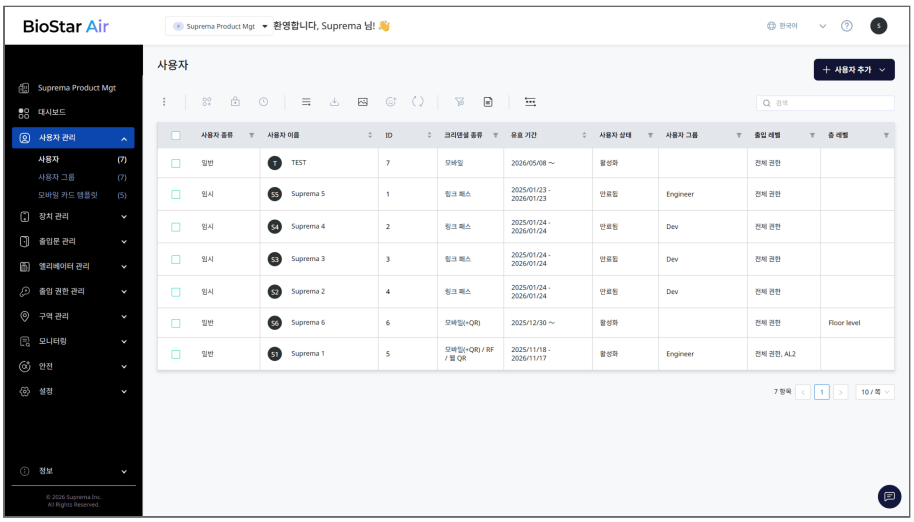
사용자 목록은 조직의 출입 통제를 담당하는 관리자를 위한 필수 관리 도구입니다. 사용자 그룹화를 통한 조직 관리, 실시간 활성화/일시 정지로 신입 또는 퇴사 직원 즉시 대응, 다양한 크리덴셜 통합 관리, 유효 기간 모니터링을 통한 보안 강화, 필터링과 리포트 생성을 통한 보고 및 감사 대비까지 모든 사용자 관리 작업을 수행할 수 있습니다.

사용자 목록 조회

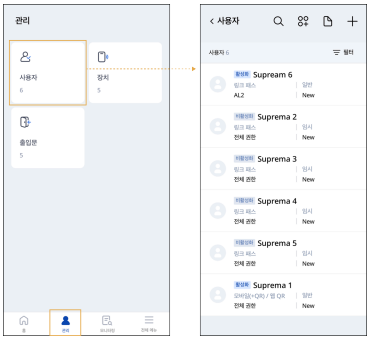
사용자 목록에서는 BioStar Air에 등록된 모든 사용자를 한눈에 확인할 수 있습니다. 각 사용자의 세부 정보를 보고, 필터링 및 정렬 기능을 활용하여 특정 사용자를 쉽게 찾을 수 있습니다. 또한, 사용자 목록에서 직접 사용자 편집, 삭제, 그룹 할당 등의 작업을 수행할 수 있습니다.

Web

화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.



Mobile



BioStar Air 앱에서 사용자 관리 기능을 사용할 수 있습니다.

1. 모바일 기기에서 **BioStar Air** 앱을 실행하세요.
2. 화면 하단의 탐색바에서 **관리**를 탭하세요.
3. **사용자** 버튼을 탭하세요.

사용자 목록이 나타납니다. 새로운 사용자를 추가하거나 기존 사용자의 세부 정보를 편집할 수 있습니다.

사용자 정보

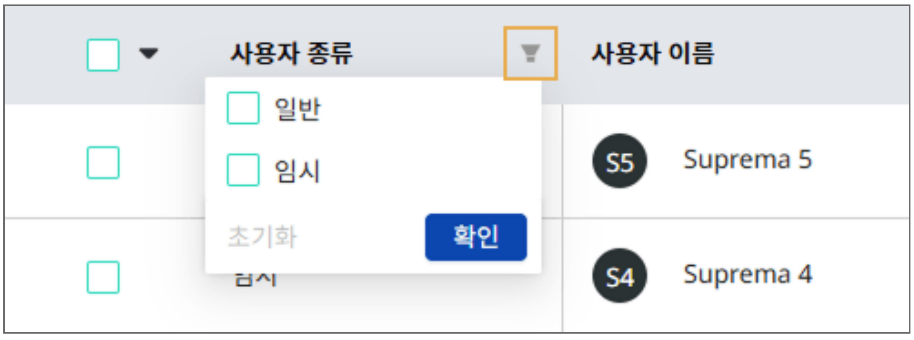
사용자 목록의 테이블에서 제공하는 정보는 아래와 같습니다.

- **사용자 종류**: 사용자가 일반 사용자인지 임시 사용자인지 나타냅니다. 일반 및 임시 사용자에 대한 자세한 내용은 사용자 카드 및 크리덴셜 종류를 참고하세요.
- **사용자 이름**: 사용자의 이름입니다.
- **ID**: 사용자의 고유 아이디입니다.
- **크리덴셜 종류**: 사용자에게 발급한 크리덴셜을 나타냅니다. 크리덴셜의 종류에 대한 자세한 내용은 사용자 카드 및 크리덴셜 종류를 참고하세요.
- **유효 기간**: 사용자에게 발급한 크리덴셜의 유효 기간입니다.
- **사용자 상태**: 해당 사용자의 활성화 또는 비활성화 상태를 나타냅니다.
- **사용자 그룹**: 사용자가 속한 그룹입니다. 사용자 그룹에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.
- **출입 레벨**: 사용자에게 할당한 출입 레벨입니다. 출입 레벨에 대한 자세한 내용은 출입 레벨 관리하기를 참고하세요.
- **층 레벨**: 사용자가 출입할 수 있는 층에 대한 권한입니다. 층 레벨에 대한 자세한 내용은 층 레벨 관리하기를 참고하세요.

필터링

Web

사용자 목록의 상단 헤더 영역에서 필터링 기능을 이용할 수 있습니다. 헤더 영역의 버튼을 클릭하면 원하는 조건을 설정할 수 있습니다.

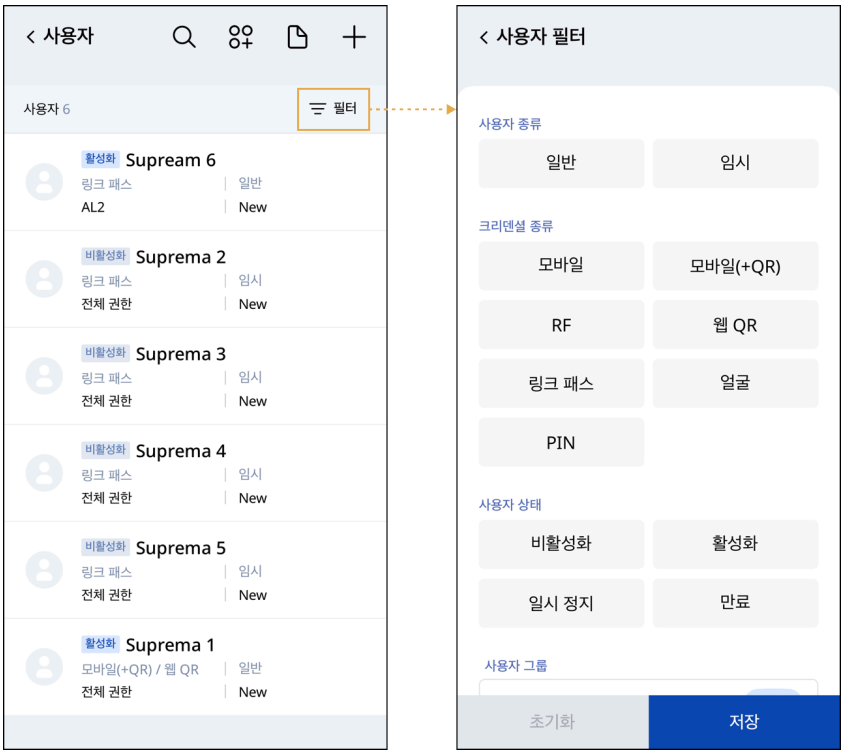


알아두기

적용한 필터 조건을 초기화하려면 사용자 목록 상단의 버튼을 클릭하세요.

Mobile

모바일 앱에서 사용자 목록의 사용자를 원하는 기준으로 필터링하여 볼 수 있습니다. 사용자 목록 오른쪽 상단의 **필터**를 탭하세요. 사용자는 아래 기준으로 필터링할 수 있습니다.

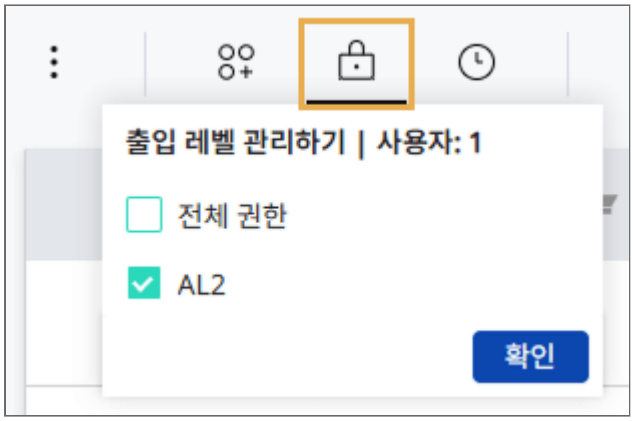


- **사용자 종류**: 일반 또는 임시 사용자로 필터링합니다.
- **크리덴셜 종류**: 크리덴셜 종류에 따라 필터링합니다.
- **사용자 상태**: 활성화 상태에 따라 필터링합니다.
- **사용자 그룹**: 사용자 그룹에 따라 필터링합니다.

추가 기능

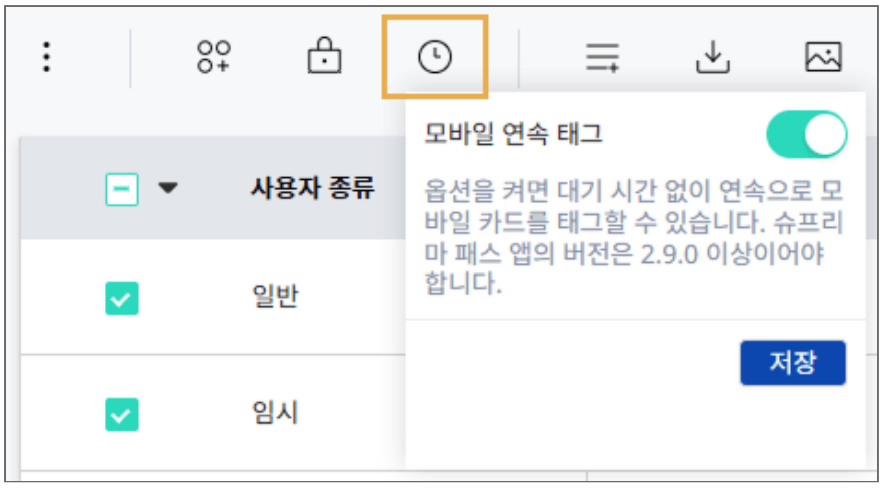
사용자 목록 상단에서 제공하는 기능은 아래와 같습니다.

- : 선택한 사용자에게 그룹을 할당하거나 제외, 이동할 수 있습니다. 자세한 내용은 사용자 그룹 관리를 참고하세요.
- : 선택한 사용자의 출입 레벨을 변경할 수 있습니다. 출입 레벨 관리에 대한 자세한 내용은 출입 레벨 관리하기를 참고하세요.



- : 선택한 사용자에게 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있도록 설정할 수 있습니다. 슈프리마 패스 앱은 2.9.0 버전

이상에서 지원합니다.



- : 선택한 사용자에게 사용자 템플릿을 적용할 수 있습니다. 기본 설정된 사용자 정보 외에 필요한 다른 정보를 추가할 수 있습니다.



- : 선택한 사용자 정보를 PDF 또는 CSV 파일로 내보낼 수 있습니다.
- : 사용자 이미지를 일괄 업로드할 수 있습니다. 업로드하는 이미지 파일의 이름은 사용자 아이디와 일치해야 합니다.

  예, 601.jpg 파일은 사용자 아이디 601에 해당합니다.

  > **파일 형식 요구사항**
  > – 지원되는 형식: *.jpg, .jpeg, .png*
  > – 파일 크기 제한: 이미지당 **1MB**

- : 선택한 사용자에게 얼굴 등록 링크를 이메일 또는 문자 메시지로 전송할 수 있습니다. 사용자가 링크를 클릭해 웹 페이지에서 얼굴을 등록하면, 얼굴 인증을 통해 출입할 수 있는 권한이 부여됩니다.

  > 이메일과 휴대폰 번호가 등록되어 있지 않은 사용자에게는 링크를 전송할 수 없습니다.

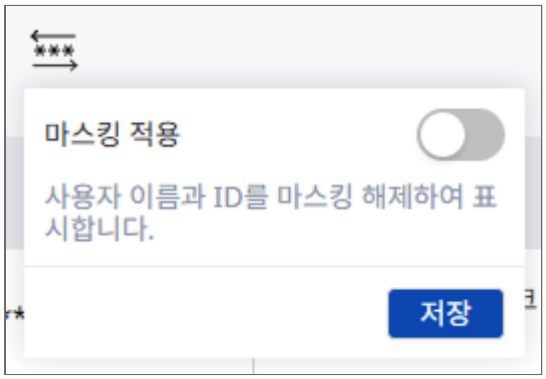
- : SCIM으로 동기화된 사용자의 정보를 로컬에서 수동으로 변경하면 **오버라이드** 상태가 됩니다. 로컬 변경 사항을 취소하고 다시 SCIM 관리 상태로 되돌릴 수 있습니다. 자세한 내용은 SSO & SCIM 설정하기를 참고하세요.



- : 사용자 목록에 적용된 필터를 초기화합니다. 이 기능은 필터링이 적용된 상태에서 사용할 수 있습니다. 필터링 적용 방법에 대한 자세한 내용은 필터링를 참고하세요.

- : 사용자 리포트를 설정할 수 있습니다. 리포트를 생성을 완료하면 관리자의 이메일로 전송됩니다. 리포트 설정에 대한 자세한 내용은 사용자 리포트 생성를 참고하세요.

- : 사용자 목록에서 개인 정보 보호를 위해 이름, 아이디 등의 정보를 마스킹(***)할 수 있습니다. 이 기능은 개인 정보 보호가 필요한 환경에서 유용합니다. 토글 버튼을 선택해 기능을 활성화하고, **저장** 버튼을 클릭하세요.

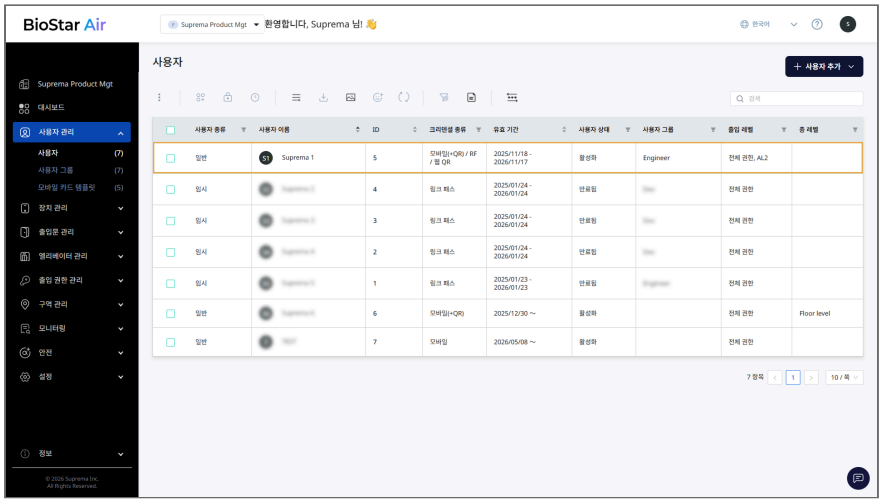


사용자 정보 수정

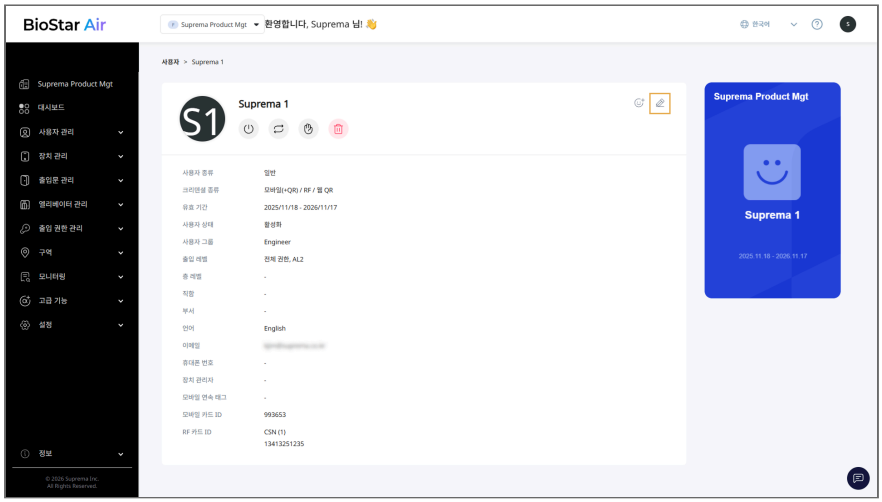
Web

사용자의 세부 정보를 수정하거나 크리덴셜을 변경하려면 다음 단계를 따르세요.

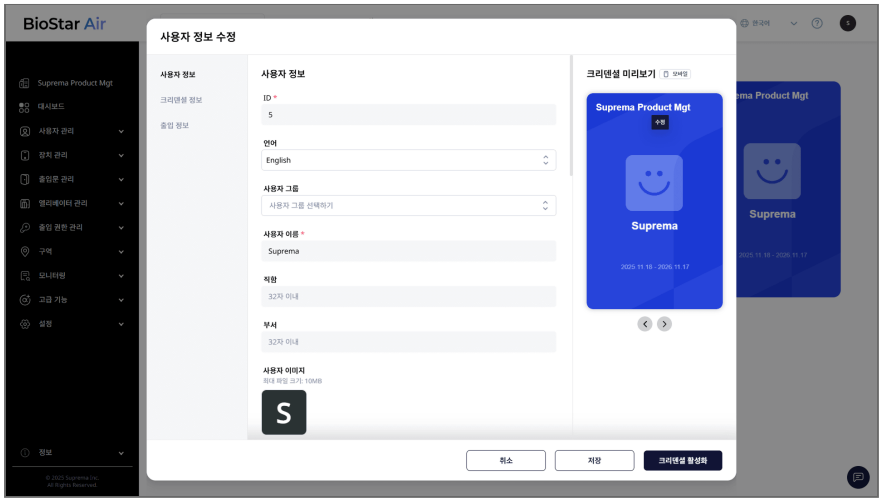
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 목록에서 수정할 사용자를 클릭하세요.



3. 사용자 세부 정보 오른쪽 상단의 버튼을 클릭하세요.

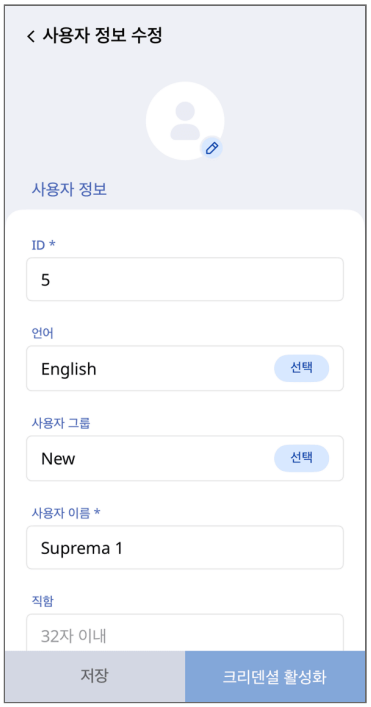


4. **사용자 정보 수정** 창이 나타나면 필요한 세부 정보를 수정하세요.



5. 수정을 완료하면 오른쪽 하단의 **저장** 버튼을 클릭하세요.

Mobile



모바일 앱에서 사용자 세부 정보를 수정하려면 다음 단계를 따르세요.

1. 사용자 목록에서 정보를 수정할 사용자를 탭하세요.
2. 오른쪽 상단의 버튼을 탭하세요.
3. **사용자 정보 수정** 화면에서 필요한 정보를 수정하세요.
4. 수정 사항을 저장하려면 **저장** 버튼을 탭하세요.

   크리덴셜을 발급하려면 **크리덴셜 활성화** 버튼을 사용하세요.

> **알아두기**
> 사용자 정보에 대한 자세한 내용은 사용자 추가하기를 참고하세요.

사용자 그룹 관리

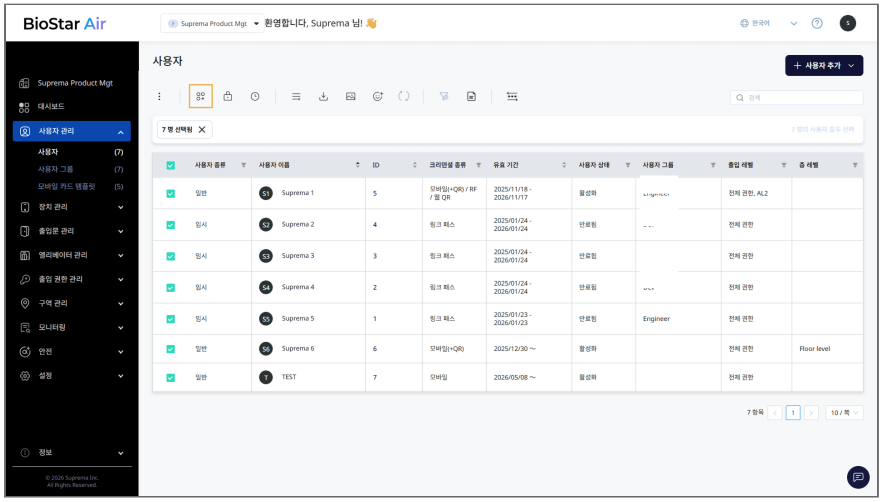
사용자를 사용자 그룹에 할당하거나 이동, 제외하는 방법을 안내합니다. 사용자 그룹 생성 및 관리에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

Web

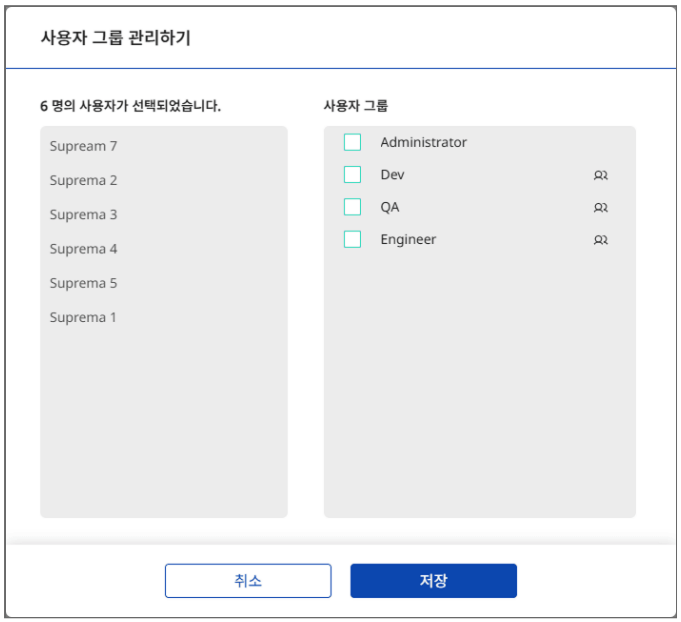
그룹에 사용자 할당하기

사용자 그룹을 생성한 후 사용자 목록에서 사용자를 추가할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 앞서 생성한 그룹에 할당할 사용자의 체크박스를 클릭하세요.
3. 사용자 목록 왼쪽 상단의 버튼을 클릭하세요.

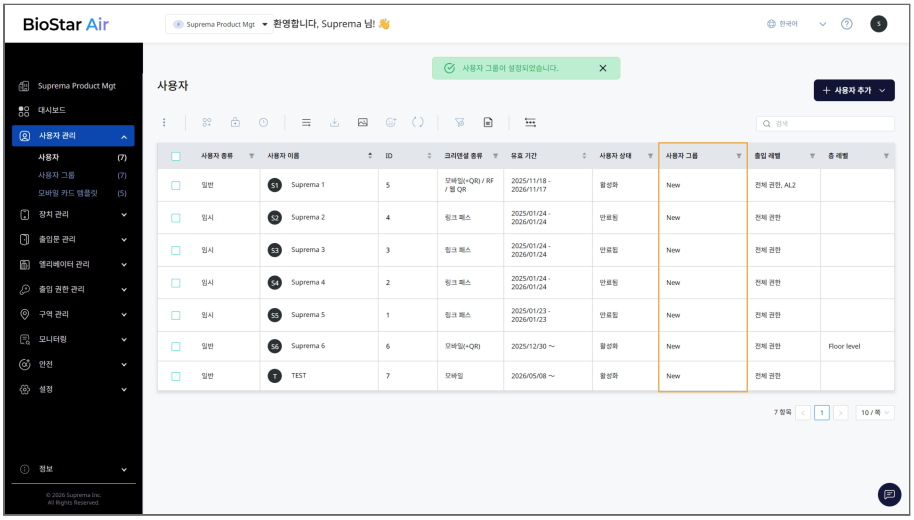


4. **사용자 그룹 관리하기** 창이 나타나면 사용자를 할당할 상위 그룹 또는 하위 그룹을 선택하세요.



5. 선택을 완료하고 그룹 설정을 저장하려면 **저장** 버튼을 클릭하세요.

사용자 목록의 **사용자 그룹** 열에서 사용자가 새 그룹에 할당된 것을 확인할 수 있습니다.



사용자 그룹으로 돌아가면 해당 그룹의 **전체 사용자 수**가 업데이트된 것을 확인할 수 있습니다.

그룹 해제 또는 이동

사용자를 그룹에서 제외하거나 다른 그룹으로 이동할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 그룹에서 해제하거나 이동할 사용자의 체크박스를 클릭하세요.

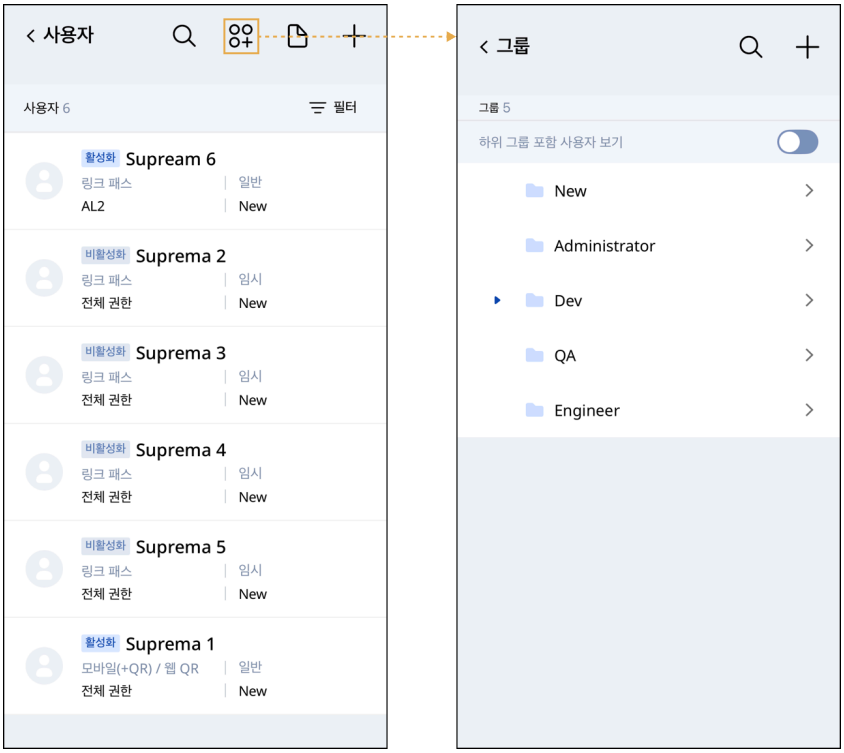
> 그룹 이동 시에는 동일한 그룹의 사용자를 선택한 후 진행하세요.

3. 사용자 목록 왼쪽 상단의 버튼을 클릭하세요.
4. **사용자 그룹 관리하기** 창이 나타나면 다음 중 하나를 수행하세요.
   - 그룹을 해제할 때는 선택된 그룹의 체크박스를 비활성화하세요.
   - 그룹을 이동할 때는 선택된 그룹의 체크박스를 활성화하고, 이동할 그룹을 선택하세요.
5. 그룹 설정을 저장하려면 **저장** 버튼을 클릭하세요.

사용자 목록의 **사용자 그룹** 열에서 사용자의 그룹 변경 사항을 확인할 수 있습니다.

Mobile

모바일 앱에서 사용자 그룹을 관리할 수 있습니다. 사용자 목록 상단의 버튼을 탭하세요. 사용자 그룹 목록을 확인할 수 있습니다.



- 그룹에 속한 사용자를 보려면 원하는 그룹의 오른쪽에 > 버튼을 탭하세요.
- 새로운 그룹을 추가하려면 오른쪽 상단의 + 버튼을 탭하세요.
- 그룹 이름을 수정하려면 원하는 그룹을 길게 터치하고 하단의 버튼을 탭하세요.
- 그룹을 삭제하려면 원하는 그룹을 길게 터치한 후 하단의 버튼을 탭하세요. 하나 이상의 그룹을 선택해 삭제할 수 있습니다.

> **알아두기**
> 사용자 그룹 관리에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

사용자 상태 관리

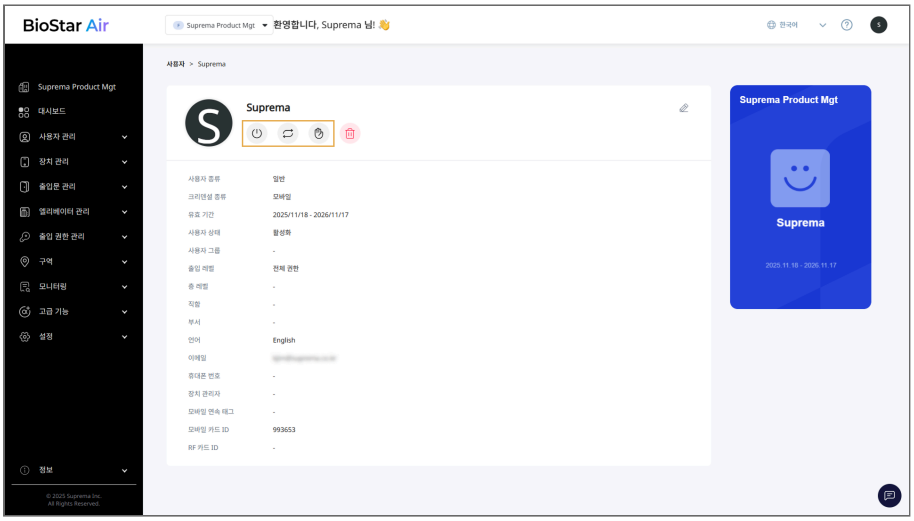
사용자의 출입 권한을 활성화하거나 일시 정지할 수 있습니다. 또한 크리덴셜을 재발급할 수도 있습니다.

> **알아두기**
> 관리자가 BioStar Air에서 사용자의 크리덴셜을 재발급하면 이전에 발급된 모바일 크리덴셜, QR 코드 및 링크패스(LinkPass)는 모두 취소되고 새 크리덴셜로 교체됩니다. 사용자는 사이트 설정에 따라 이메일 또는 SMS로 새 크리덴셜 링크를 받게 됩니다. 사용자는 해당 링크를 통해 슈프리마 패스 앱에 새 모바일 크리덴셜을 다운로드하거나 새 QR 코드 또는 링크패스를 이용해야 합니다. 취소된 모바일 크리덴셜, QR 코드 또는 링크패스로 출입을 시도하면 실패합니다.

개별 사용자

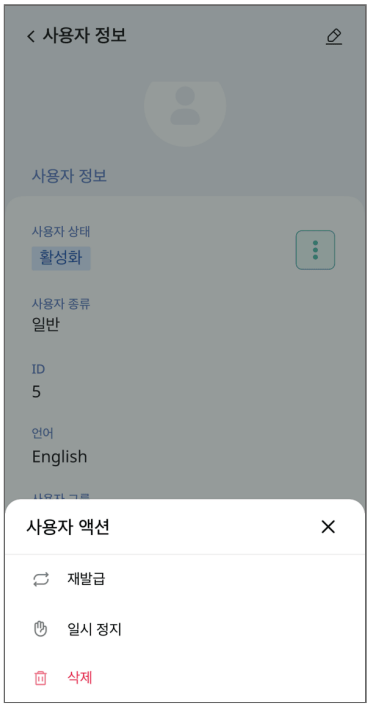
Web

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 상태를 변경할 사용자를 클릭하세요.
3. 사용자 세부 정보 상단에서 원하는 기능을 선택하세요.



- : 사용자의 출입 권한을 활성화합니다. 새 사용자의 초기 활성화 또는 일시 정지된 사용자의 재활성화 시 사용하세요.
- : 크리덴셜을 다시 발급합니다. 이 기능은 사용자의 크리덴셜이 만료되었거나, 크리덴셜을 사용할 수 없어 새로 발급할 때 사용할 수 있습니다.
- : 사용자의 출입을 차단합니다. 이 기능은 사용자가 활성화된 상태일 때 사용할 수 있습니다.

Mobile



모바일 앱에서 사용자 목록에서 사용자를 탭하세요. **사용자 정보** 화면에서 ⋮ 버튼을 탭하세요. **사용자 액션** 메뉴가 나타납니다.

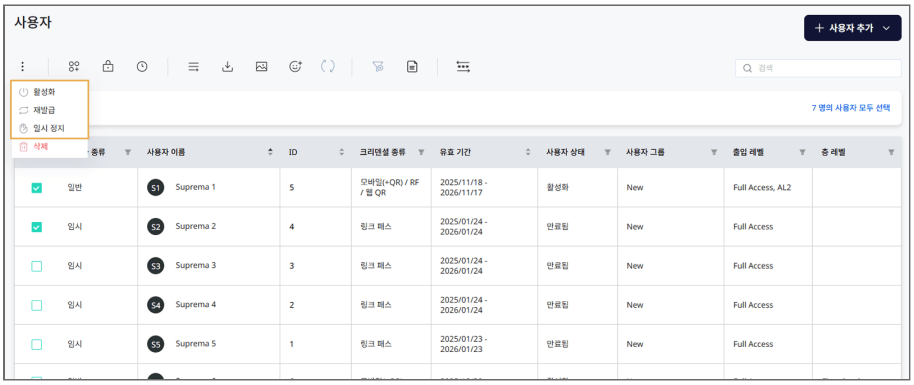
- **활성화** / **재활성화**: 사용자의 출입 권한을 활성화합니다. 새 사용자의 초기 활성화 또는 일시 정지된 사용자의 재활성화 시 사용하세요.
- **재발급**: 사용자의 크리덴셜을 재발급합니다.
- **일시 정지**: 사용자를 일시적으로 비활성화합니다. 일시 중지된 사용자는 출입할 수 없습니다.
- **삭제**: 사용자를 시스템에서 삭제합니다.

> **알아두기**
> **재활성화** 옵션은 일시 중지된 사용자에게만 표시됩니다.

일괄 작업

Web

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 상태를 변경할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 왼쪽 상단의 ⋮ 버튼을 클릭하고 팝업 메뉴에서 원하는 작업을 선택하세요.



- **활성화** / **재활성화**: 사용자의 출입 권한을 활성화합니다. 새 사용자의 초기 활성화 또는 일시 정지된 사용자의 재활성화 시 사용하세요.
- **재발급**: 크리덴셜을 다시 발급합니다. 이 기능은 사용자의 크리덴셜이 만료되었거나, 크리덴셜을 사용할 수 없어 새로 발급할 때 사용할 수 있습니다.
- **일시 정지**: 사용자의 출입을 차단합니다. 이 기능은 사용자가 활성화된 상태일 때 사용할 수 있습니다.

Mobile



모바일 앱에서 사용자 목록에서 상태를 변경할 사용자를 길게 터치하세요. 추가로 상태를 변경할 사용자를 선택하세요. 화면 하단의 **사용자 액션** 메뉴에서 원하는 기능을 탭하세요.

- **활성화** / **재활성화**: 사용자의 출입 권한을 활성화합니다. 새 사용자의 초기 활성화 또는 일시 정지된 사용자의 재활성화 시 사용하세요.
- **재발급**: 사용자의 크리덴셜을 재발급합니다.
- **일시 정지**: 사용자를 일시적으로 비활성화합니다. 일시 중지된 사용자는 출입할 수 없습니다.
- **삭제**: 사용자를 시스템에서 삭제합니다.

> **알아두기**
> **재활성화** 옵션은 일시 중지된 사용자에게만 표시됩니다.

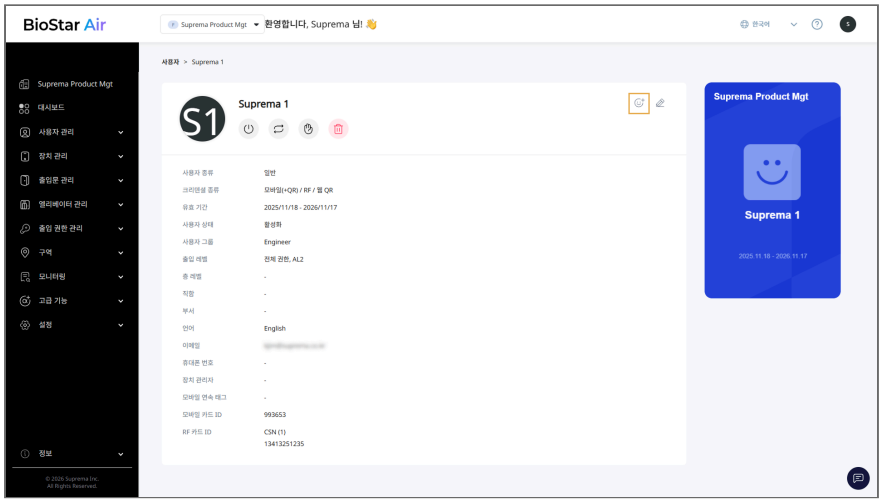
얼굴 등록 링크 전송

이미 등록한 사용자에게 얼굴 등록 링크를 이메일 또는 문자 메시지로 전송하여 얼굴을 등록하도록 안내할 수 있습니다. 사용자가 링크를 클릭해 웹 페이지에서 얼굴을 등록하면, 얼굴 인증을 통해 출입할 수 있습니다.

> **알아두기**
> 이메일과 휴대폰 번호가 등록되어 있지 않은 사용자에게는 링크를 전송할 수 없습니다.

개별 사용자

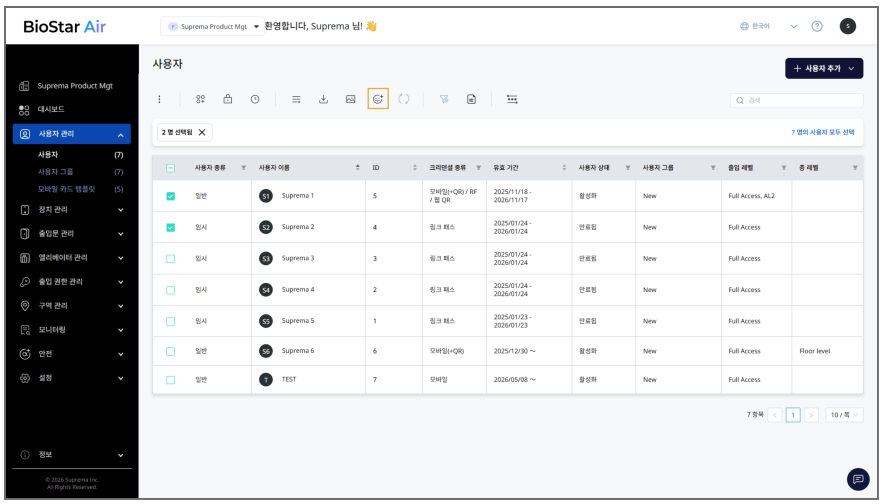
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 링크를 전송할 사용자를 클릭하세요.
3. 사용자 세부 정보 오른쪽 상단의 버튼을 클릭하세요.



4. 팝업 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

일괄 작업

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 사용자 목록에서 링크를 전송할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 왼쪽 상단의 버튼을 클릭하세요.



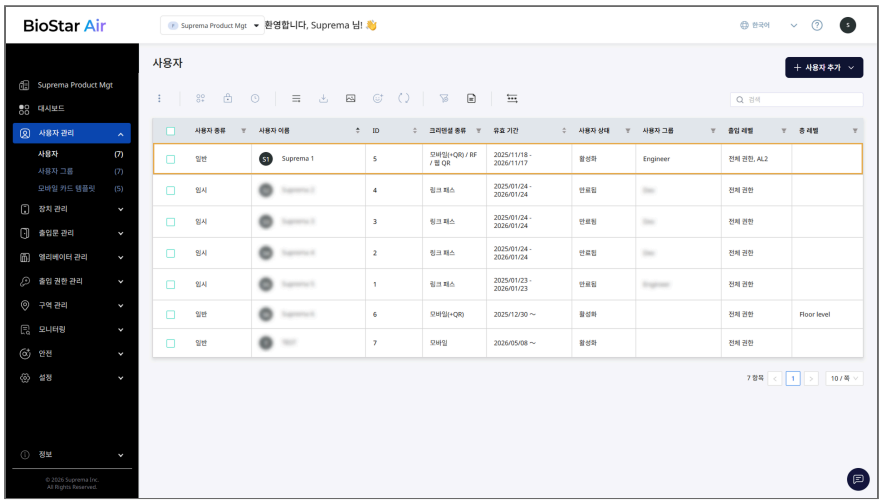
4. 팝업 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

사용자 삭제

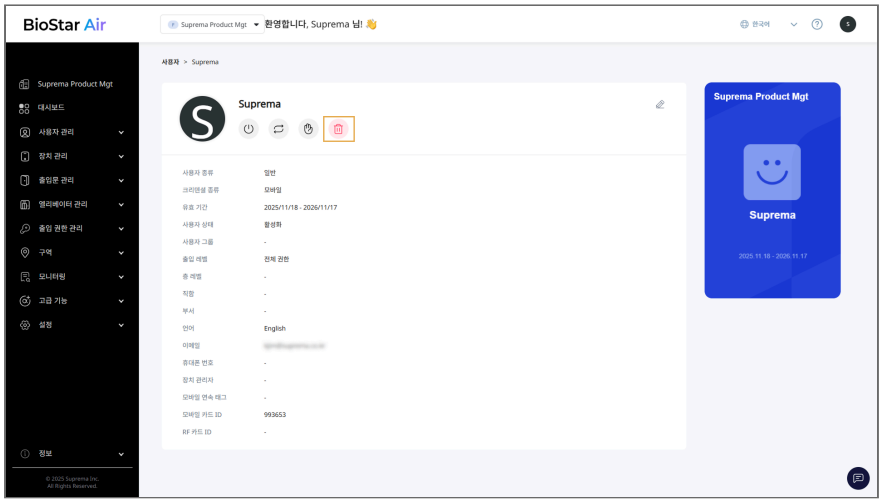
> **주의**
> 삭제한 사용자는 복구할 수 없습니다. 삭제하기 전에 반드시 확인하세요.

개별 사용자

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 목록에서 삭제할 사용자를 클릭하세요.



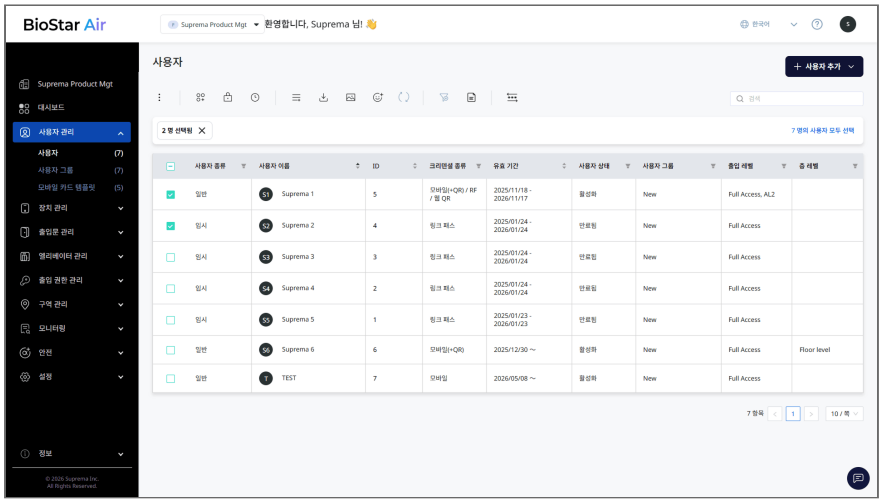
3. 사용자 세부 정보에서 🗑 버튼을 클릭하세요.



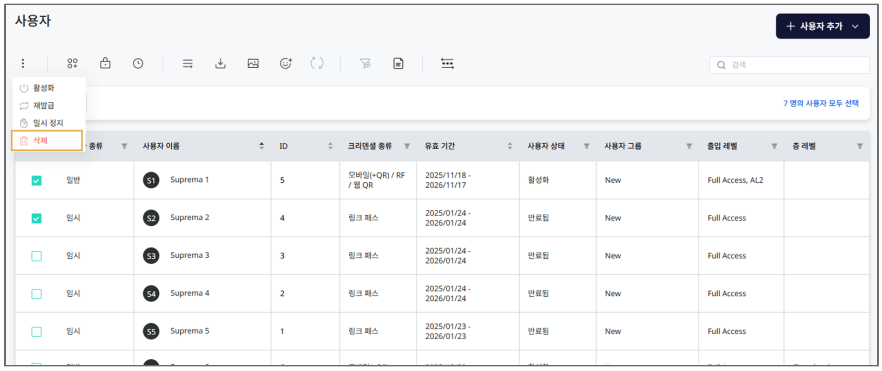
4. 경고 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

일괄 삭제

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 목록에서 삭제할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.



3. 화면 왼쪽 상단의 ⋮ → **삭제**를 클릭하세요.



4. 경고 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

사용자 리포트 생성

사용자 리포트를 생성하여 관리자의 이메일로 전송할 수 있습니다.

1. 사용자 목록 상단의 버튼을 클릭하세요.
2. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



3. 각 필터 옵션에서 리포트에 포함할 항목을 선택하세요.
4. 생성한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
5. **리포트 목록**이 생성되며 관리자의 이메일로 다운로드 링크가 전송됩니다.

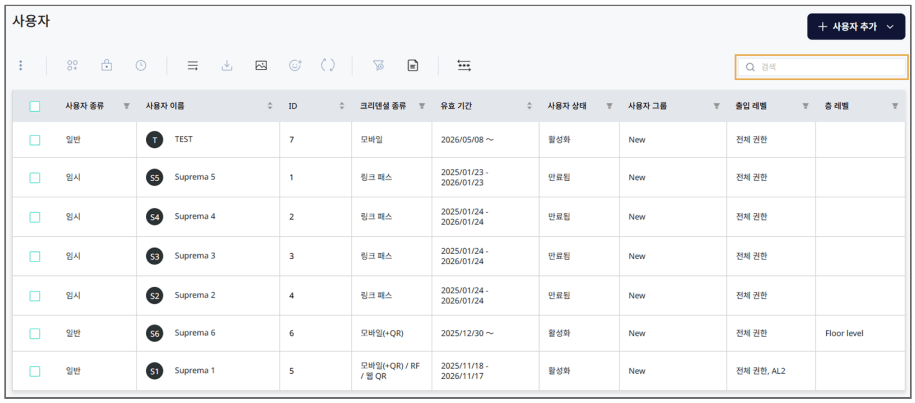


알아두기

리포트 목록에서 생성된 리포트를 검색하거나, 수정, 다운로드, 삭제할 수 있습니다.

사용자 검색

사용자 목록 오른쪽 상단의 검색 입력 필드를 통해 특정 사용자를 빠르게 찾을 수 있습니다. 사용자 이름, 아이디, 전화번호를 기준으로 검색할 수 있습니다.



일괄 작업으로 사용자 추가하기

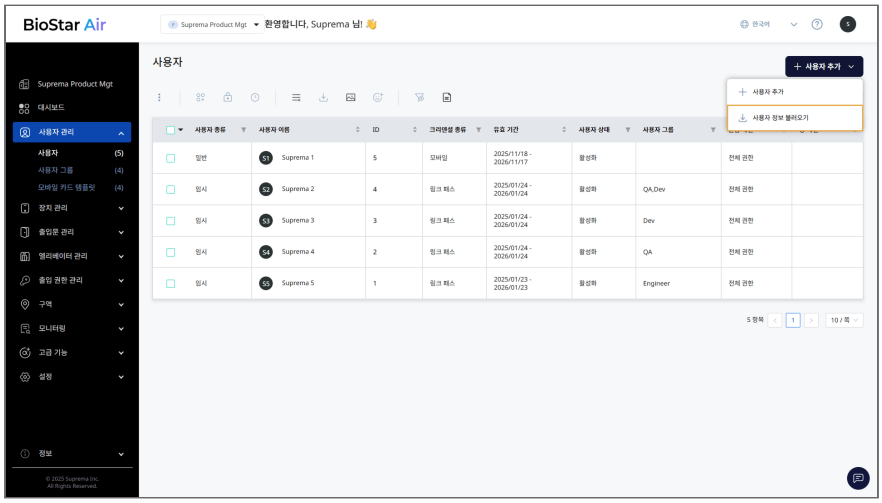
여러 사용자를 한 번에 추가해야 한다면, BioStar Air의 일괄 사용자 추가 기능을 사용하세요. CSV 파일 업로드로 수십, 수백 명의 직원 정보를 몇 분 안에 시스템에 등록할 수 있습니다. 사용자 정보 입력과 동시에 프로필 이미지를 일괄 업로드할 수도 있습니다. 이 문서에서는 CSV 템플릿 다운로드, 파일 준비, 업로드, 프로필 이미지 관리, 그리고 업로드 후 사용자 정보를 검증하는 방법을 단계별로 안내합니다.

> **팁**
> 여러 사용자를 일괄 추가하는 전체 과정을 단계별로 안내하는 다음 동영상을 참고하세요.

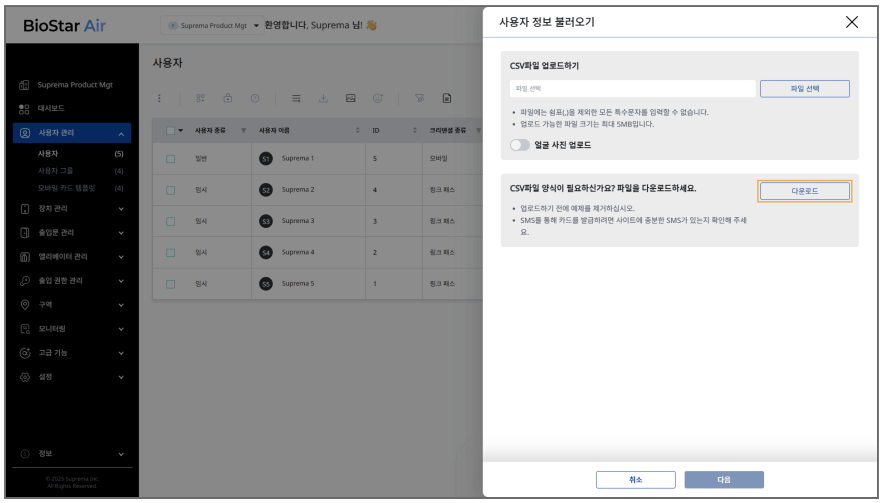
CSV 템플릿 다운로드

다음 안내에 따라 CSV 템플릿 파일을 다운로드하세요.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 **사용자 추가** → **사용자 정보 불러오기**를 클릭하세요.



3. **사용자 정보 불러오기** 패널이 나타나면 **다운로드** 버튼을 클릭하세요.



4. CSV 템플릿 파일(*biostar-import-user-csv-example.csv*)을 로컬에 저장하세요.

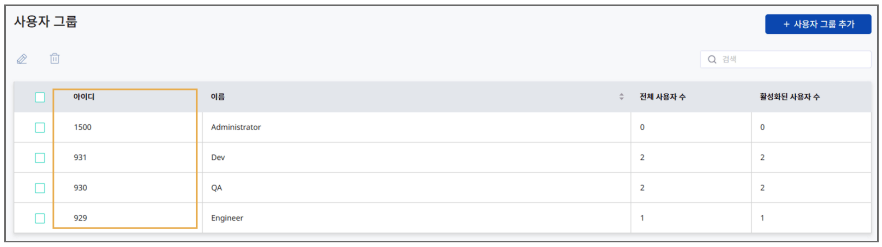
CSV 파일 준비

CSV 템플릿을 다운로드하고 각 사용자에 대한 필수 세부 정보를 입력하세요.

주요 입력 필드

입력할 주요 필드는 아래와 같습니다.

- **사용자 그룹 IDs**: **사용자 관리** → **사용자 그룹**에서 그룹 아이디를 확인할 수 있습니다.



- **출입 레벨 IDs** : **출입 권한 관리** → **출입 레벨**에서 출입 레벨 아이디를 확인할 수 있습니다. **전체 권한**은 항상 **1**로 설정됩니다. 쉼표(`,`)를 구분자로 여러 출입 레벨을 지정할 수 있습니다.



- **이메일**: 이메일을 통해 초대장을 발송한다면 필수로 입력하세요.
- **휴대폰 번호**: 모바일 SMS를 통해 초대장을 발송한다면 필수로 입력하세요.

> **주의**
> **이메일**과 **휴대폰 번호**는 중복되면 안됩니다. 중복된 값을 입력하고 CSV 파일을 업로드하면 오류가 발생할 수 있습니다.

커스텀 Wiegand 형식 지원

시설 코드, 세그먼트, 패리티 비트 등의 정보를 포함한 모든 Wiegand 형식을 자유롭게 구성할 수 있습니다.

- HID Corporate 1000 및 iClass SE, SEOS 형식을 지원합니다.
- **CSV 템플릿**
  - 각 정의된 형식(사용자 정의 또는 기본)은 CSV 파일에서 별도의 열로 표시됩니다.

    > ***26 bit SIA Standard-H10301*, *HID 37 bit-H10302*, *HID 37 bit-H10304*, *HID Corporate 1000*, *HID Corporate 1000 48bit***

  - 여러 항목을 단일 필드에 입력할 때는 슬래시(`/`)로 구분하세요.
  - 카드 이름 주위에는 작은 따옴표(`'`)를 사용할 수 있습니다. 큰 따옴표(`"`)를 사용하면 오류가 발생할 수 있습니다.

    > ✓ *'CardName'* | ✗ *"CardName"*

> **예시**
> - 시설 코드가 있는 경우: *1234567-100-'Main Office Card'* (`CardID` - `FacilityCode` - `'CardName'`)
> - 여러 세그먼트가 있는 경우: *12-3456-78-'Lab Entry Card'*

여러 카드 지원

- 사용자당 최대 8개의 CSN 또는 Wiegand 카드 형식을 할당할 수 있습니다.
- **CSV 템플릿**
  - 단일 카드는 CSN 카드 번호를 입력합니다.

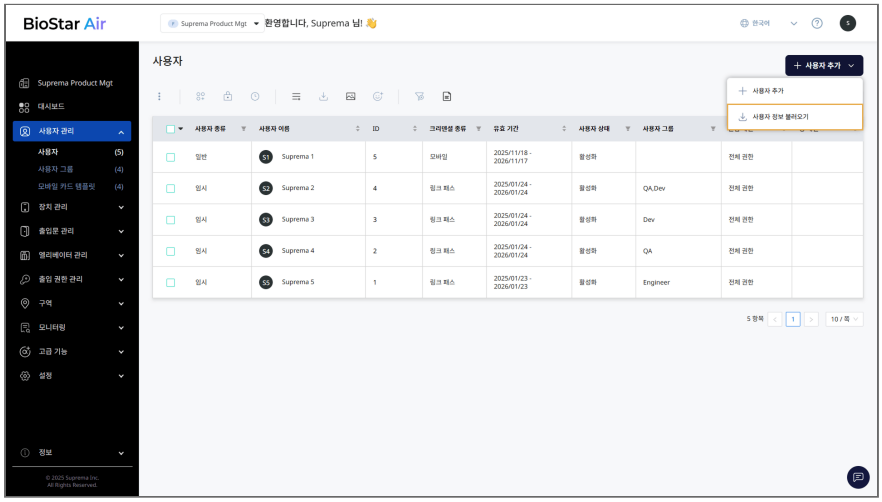
– 여러 카드를 등록할 때는 CSN 카드 번호를 슬래시(`/`)로 구분하세요.

> **카드 이름 지정 형식:** `CSN - 'Card Name'`
>
> 예시: *1234567-'Main Entry' / 7654321-'Back Door'*

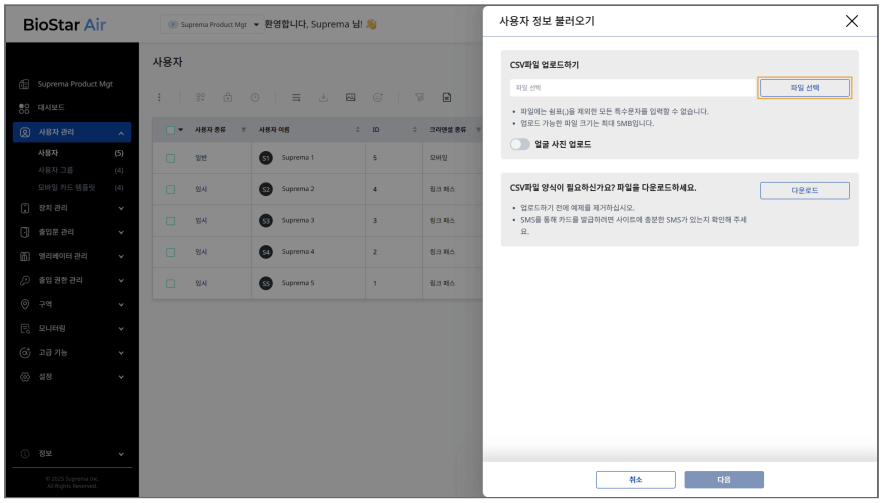
CSV 파일 업로드

CSV 파일 준비를 완료하면 업로드하세요.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 **사용자 추가** → **사용자 정보 불러오기**를 클릭하세요.



3. **사용자 정보 불러오기** 패널이 나타나면 **파일 선택** 버튼을 클릭하세요.

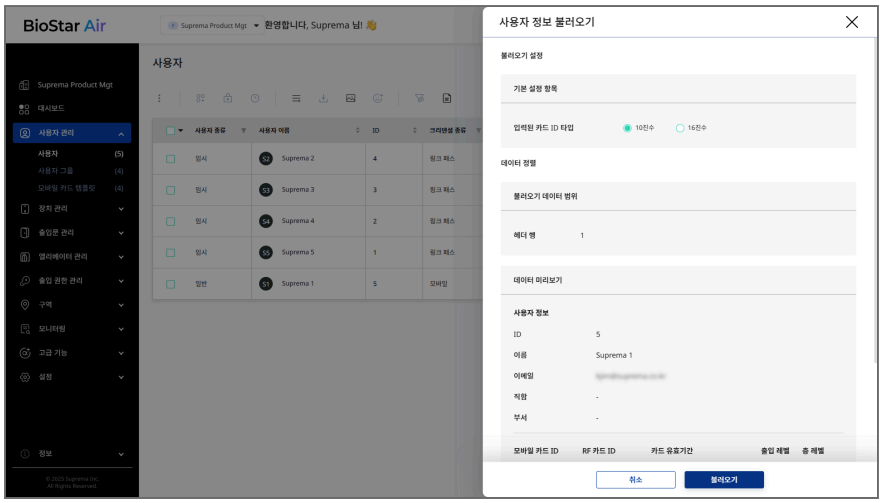


4. 앞서 준비한 CSV 파일을 선택하세요.

> 사용자의 프로필 이미지가 준비되어 있다면 **얼굴 사진 업로드** 옵션을 활성화하세요. 자세한 내용은 사용자 프로필 이미지 업로드를 참고하세요.

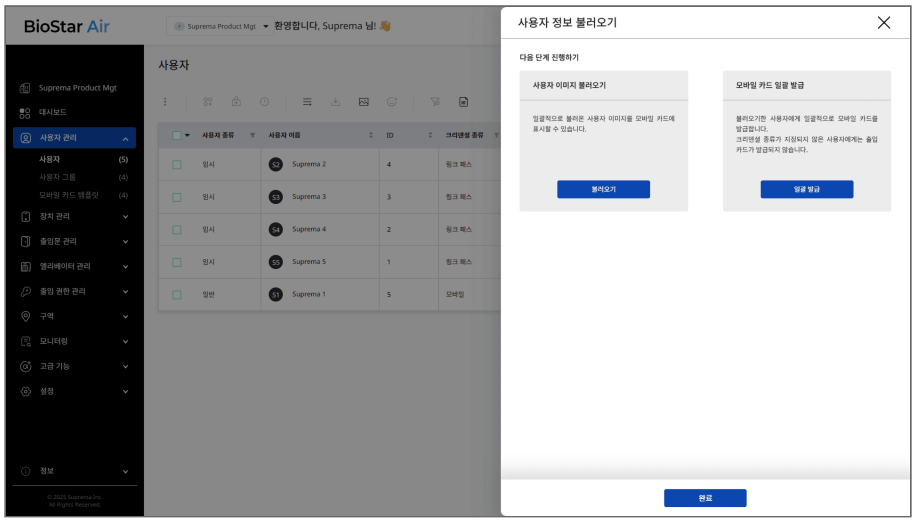
5. 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.

6. **데이터 미리보기** 섹션에서 첫번째 열의 데이터 정확성을 검토하세요.



7. 데이터에 문제가 없다면 오른쪽 하단의 **불러오기** 버튼을 클릭하세요.

업로드를 완료하면 다음 화면에서 사용자의 이미지를 불러오거나 모바일 카드를 일괄로 발급할 수 있습니다. 원하는 작업을 선택하세요.

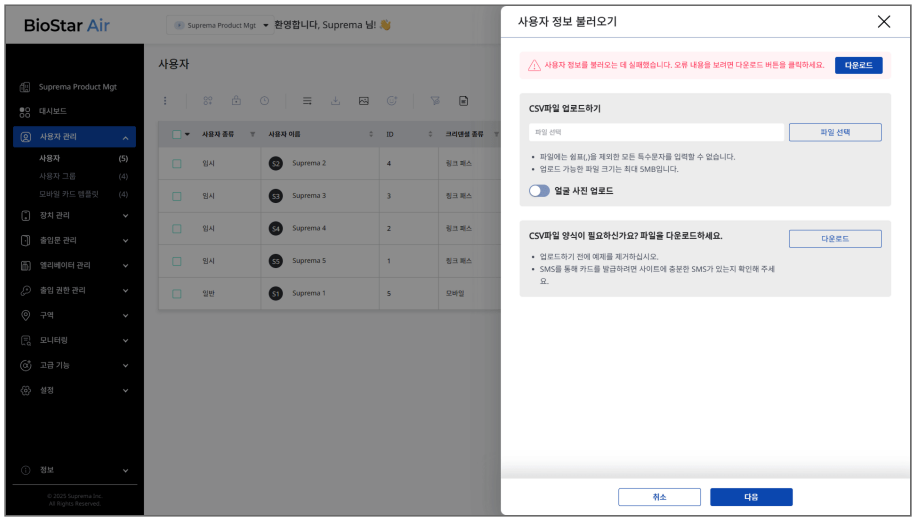


알아두기

- CSV 파일 이름에는 쉼표(,)를 제외한 특수 문자를 사용할 수 없습니다.
- 업로드할 수 있는 CSV 파일의 최대 크기는 **5MB**입니다.
- **사용자 정보 불러오기** 패널의 **CSV파일 업로드하기** 필드에 CSV 파일을 드래그 앤 드롭하여 업로드할 수도 있습니다.

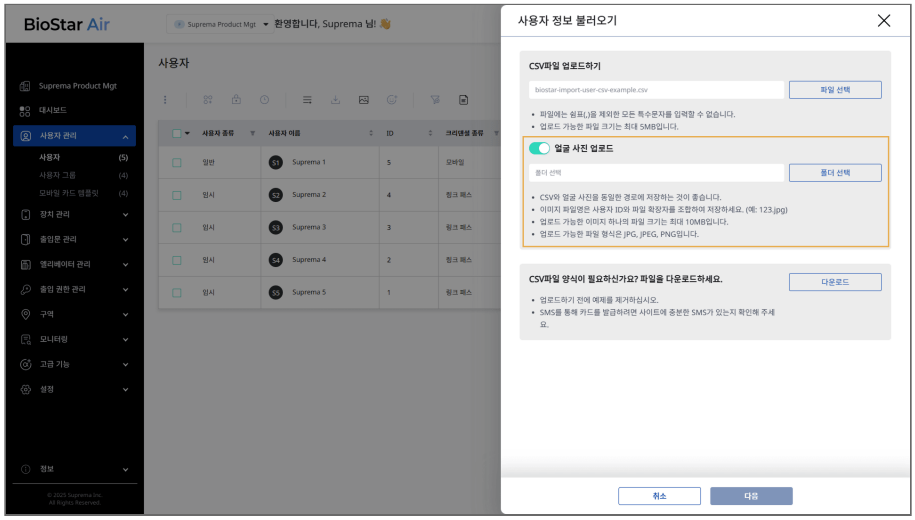
CSV 파일 검증

CSV 업로드 프로세스가 개선되어 **행별 오류 피드백**을 제공하므로 문제 해결이 더 쉬워졌습니다. 업로드 중 오류가 발생하면 오류 내용을 확인할 수 있는 상세 보고서를 제공합니다. 보고서를 다운로드하려면 **다운로드** 버튼을 클릭하세요.



사용자 프로필 이미지 업로드

프로필 이미지는 CSV 파일과 함께 자동으로 업로드하거나 나중에 수동으로 일괄 업로드할 수 있습니다.



1. CSV 파일의 **사용자 키** 열과 일치하는 프로필 이미지 파일을 준비하세요.

   예, *601.jpg* 파일은 사용자 아이디 **601**에 해당합니다.

2. **사용자 정보 불러오기** 패널에서 CSV 파일을 업로드 후 **얼굴 사진 업로드** 옵션을 활성화하세요.

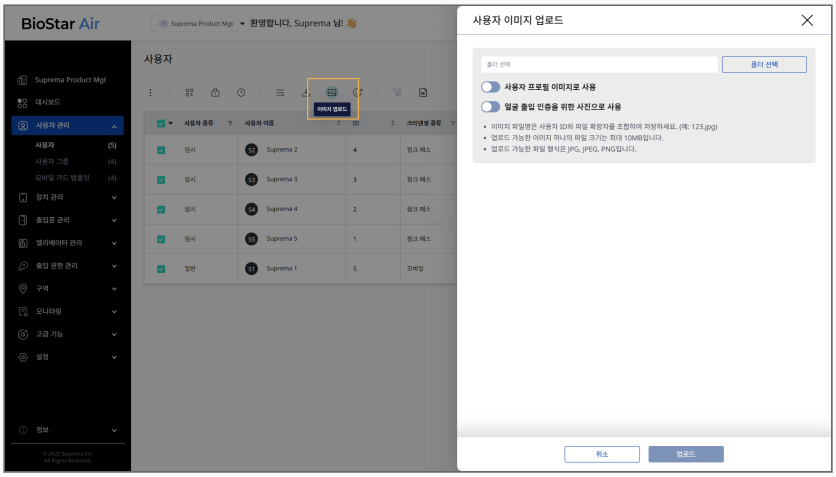
3. **폴더 선택** 버튼을 클릭한 후 프로필 이미지가 저장된 폴더를 선택하세요.

파일 형식 요구사항

- 지원되는 형식: *.jpg, .jpeg, .png*
- 파일 크기 제한: 이미지당 **1MB**

팁

프로필 이미지가 CSV 파일을 업로드할 때 준비되지 않았다면 사용자 목록의 **이미지 업로드**() 기능을 사용하여 나중에 추가할 수 있습니다.



일괄 업로드 마무리

모든 사용자 데이터와 이미지를 업로드하면 시스템이 항목을 처리하고 새 사용자가 할당된 크리덴셜과 함께 사용자 목록에 나타납니다.

문제 해결

CSV 업로드와 관련하여 문제가 발생한다면, 일반적인 문제를 해결하는 데 도움이 되는 일괄 사용자 추가 문제를 확인하세요. 이 문서에는 데이터를 검증하고 중복을 제거하는 데 도움이 되는 엑셀 수식도 포함되어 있습니다.

사용자 그룹 관리하기

사용자 그룹을 통해 조직의 부서, 역할, 위치 등으로 사용자를 분류하고 관리하세요. BioStar Air의 사용자 그룹은 계층적이지 않아 한 사용자가 여러 그룹에 동시에 속할 수 있으므로, 부서 그룹과 역할 그룹, 위치 그룹 등을 자유롭게 조합하여 운영할 수 있습니다. 그룹을 활용하면 출입 레벨을 일괄 관리할 수 있을 뿐만 아니라 이벤트 로그 필터링, 보고서 생성, 소집 구역 장치 할당 등을 효율적으로 처리할 수 있습니다.

팁

사용자 그룹 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

시작하기 전에

사용자 그룹 구성

사용자 그룹은 계층적으로 구성되어 있지 않습니다.

- 하위 그룹의 사용자는 **자동**으로 상위 그룹에 나타나지 않습니다.
- 상위 그룹의 총 사용자 수는 하위 그룹 구성원을 수동으로 추가하지 않는 한 포함되지 않습니다.
- 하위 그룹을 선택하면 해당 하위 그룹에 할당된 사용자만 표시됩니다.

여러 사용자 그룹 구성

BioStar Air의 사용자는 **여러 개의 그룹**의 구성원이 될 수 있습니다.

BioStar 2에서 사용자 그룹은 일반적으로 단일 부서에 연결되어 있었습니다. BioStar Air는 이를 분리하여 보다 동적인 방법으로 사용할 수 있습니다.

- 그룹별로 사용자 목록을 필터링하여 출입 레벨을 빠르게 관리할 수 있습니다.

  > *예, 인사부*

- 여러 부서를 아우르는 상황에 맞는 그룹을 만들 수 있습니다.

  > *예, 남자 탈의실*

- 사용자 그룹은 **이벤트 로그 필터** 및 **보고서 생성**에 사용됩니다.
- 사용자 그룹을 **소집 구역** 장치 또는 장치 그룹에 할당하여 특정 안전 프로토콜을 적용할 수 있습니다.

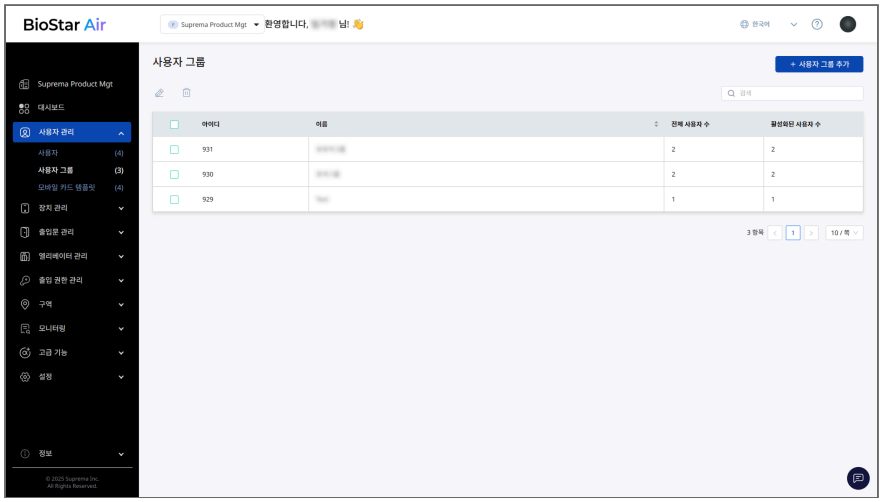
이러한 유연성 덕분에 중복되는 사용자 역할 및 액세스 시나리오를 보다 쉽게 관리할 수 있습니다.

그룹 생성

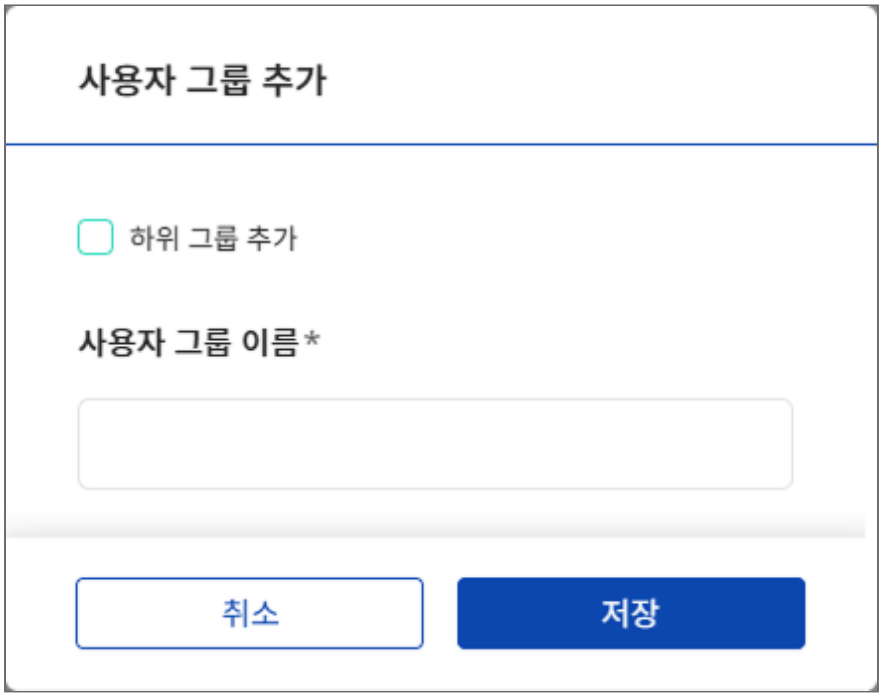
사용자 그룹 생성

새로운 사용자 그룹을 만드세요.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자 그룹**을 클릭하세요.



2. 화면 오른쪽 상단의 **사용자 그룹 추가** 버튼을 클릭하세요.
3. **사용자 그룹 추가** 창이 나타나면 사용자 그룹 이름을 입력하세요.



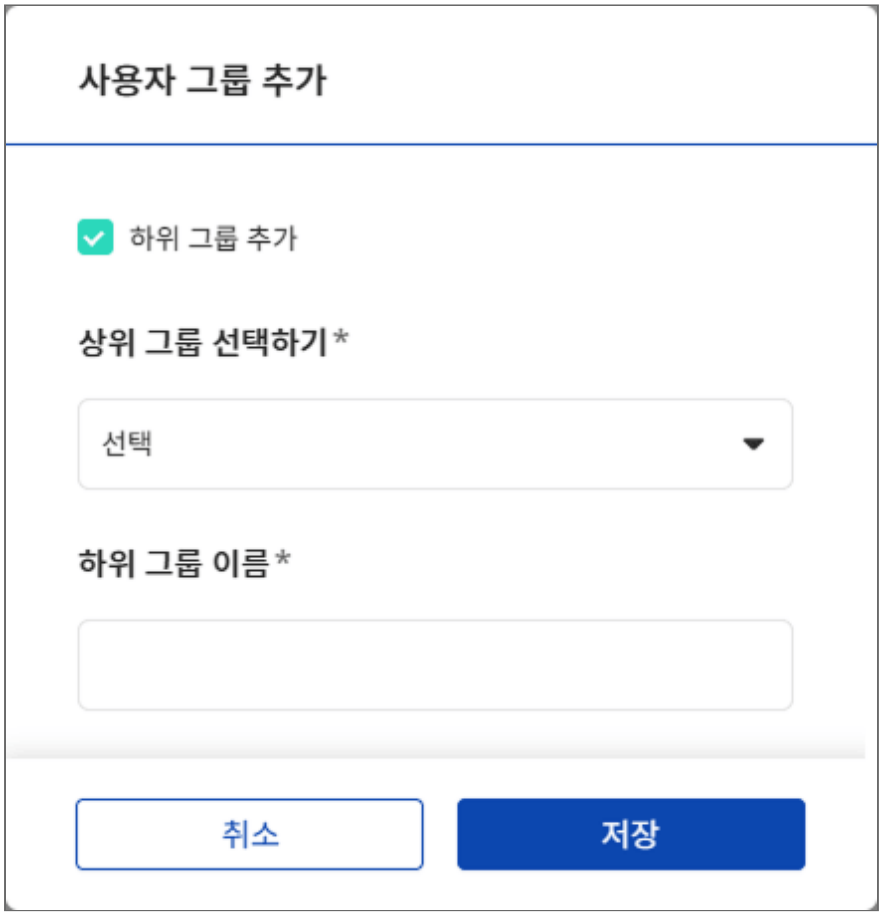
4. 그룹을 생성하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - 그룹을 삭제하더라도 해당 그룹에 속한 사용자는 삭제되지 않습니다. 사용자는 그룹에서 해제될 뿐입니다.
> - 사용자를 그룹에 할당하는 방법에 대한 자세한 내용은 사용자 관리하기를 참고하세요.

하위 그룹 생성

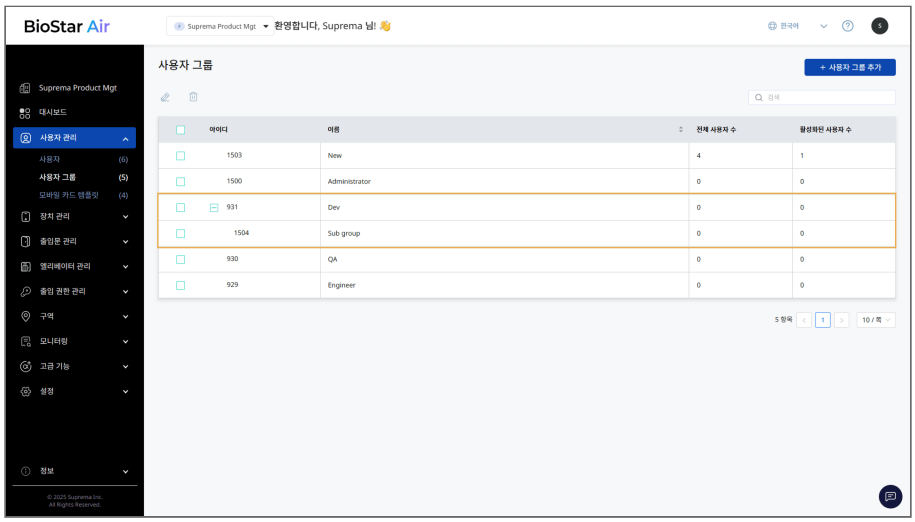
하위 그룹을 사용해 사용자 그룹을 더 세부적으로 분류할 수 있습니다. 하지만 하위 그룹은 **계층적이지 않습니다**. 즉, 하위 그룹의 사용자는 상위 그룹에 자동으로 포함되지 않습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자 그룹**을 클릭하세요.
2. 화면 오른쪽 상단의 **사용자 그룹 추가** 버튼을 클릭하세요.
3. **사용자 그룹 추가** 창이 나타나면 **하위 그룹 추가** 옵션을 클릭하세요.



4. **상위 그룹 선택하기**에서 상위 그룹을 선택하세요.
5. **하위 그룹 이름**에 그룹 이름을 입력하세요.
6. 하위 그룹을 생성하려면 **저장** 버튼을 클릭하세요.

생성된 하위 그룹은 사용자 그룹 목록에서 상위 그룹 아래에 들여쓰기되어 표시됩니다.

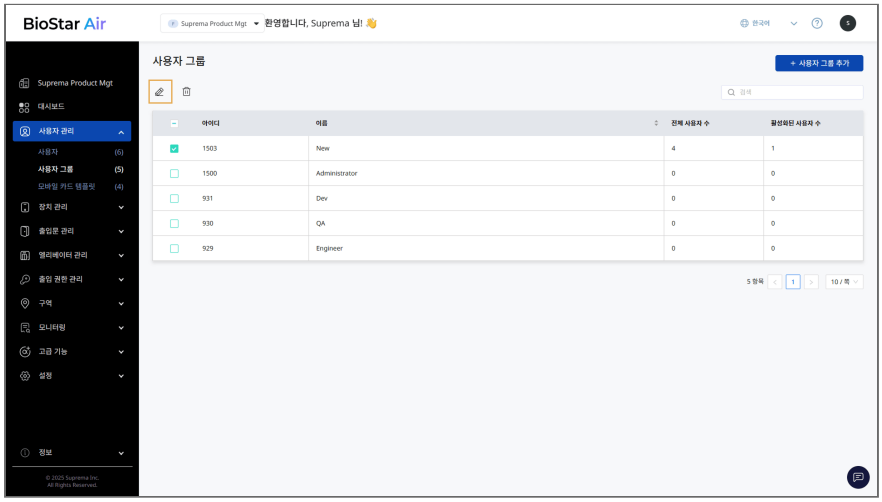


그룹 이름 수정

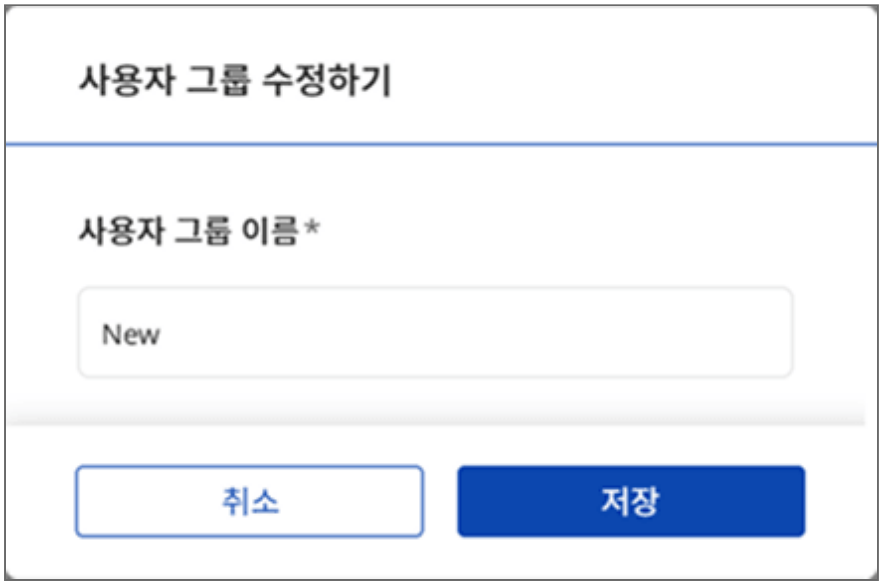
이미 만들어진 사용자 그룹의 이름을 수정할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자 그룹**를 클릭하세요.
2. 목록에서 수정할 사용자 그룹의 체크 박스를 클릭하세요.

3. 사용자 그룹 목록 왼쪽 상단의 버튼을 클릭하세요.



4. **사용자 그룹 수정하기** 창이 나타나면 그룹 이름을 수정하세요.



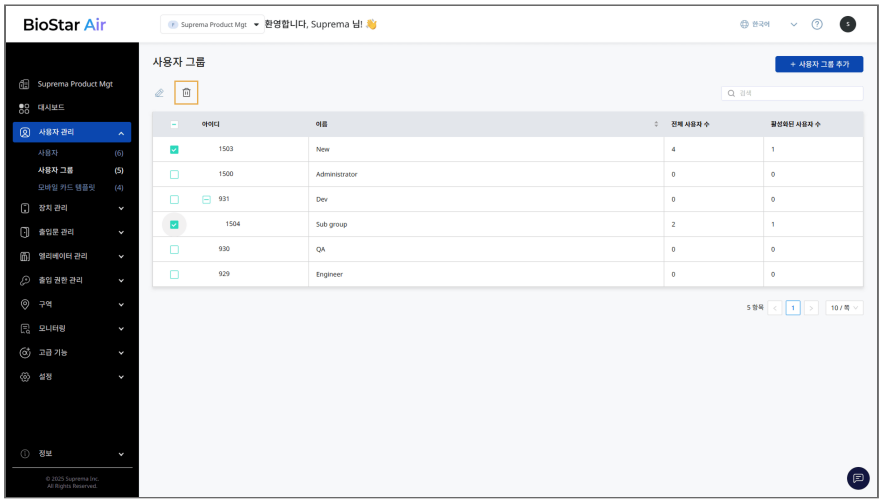
5. 수정한 내용을 저장하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
> 그룹 이름 수정은 한 개의 그룹만 선택했을 때 수정할 수 있습니다.

그룹 삭제

사용하지 않는 사용자 그룹이 있다면 삭제할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자 그룹**을 클릭하세요.
2. 목록에서 삭제할 사용자 그룹의 체크박스를 클릭하세요.
3. 사용자 그룹 목록 왼쪽 상단의 버튼을 클릭하세요.



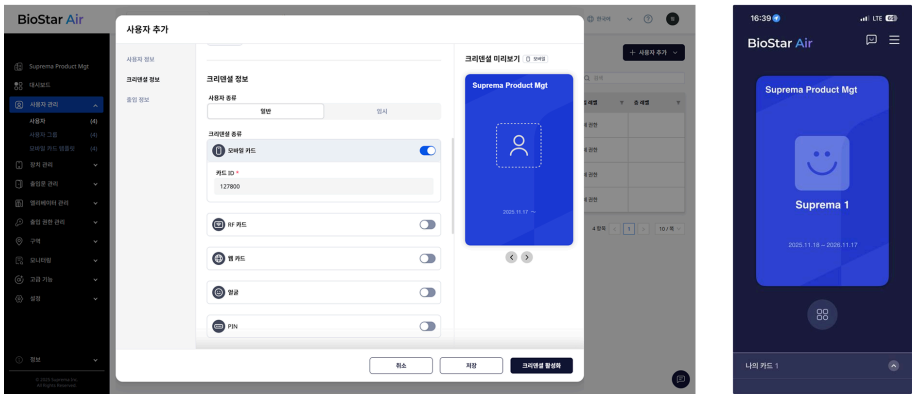
4. 경고 메시지 창이 나타나면 **삭제** 버튼을 클릭하세요.

카드 템플릿 관리하기

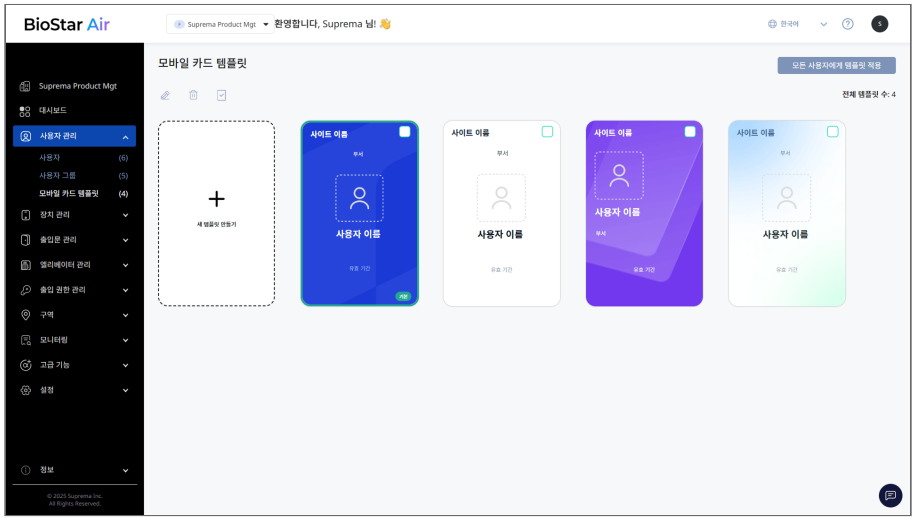
BioStar Air의 카드 템플릿을 사용하면 관리자가 사용자를 위한 모바일 카드를 디자인하고 맞춤 설정할 수 있습니다. 이 템플릿은 회사 색상, 로고 및 개인화된 세부 정보를 포함하여 브랜딩을 강화하는 데 도움이 됩니다. 카드 템플릿은 슈프리마 패스 앱에서 사용되는 모바일 카드에 적용됩니다.

BioStar Air

Mobile device



BioStar Air의 모든 사이트에는 기본 템플릿이 포함되어 있습니다. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.



기본 제공하는 템플릿을 확인할 수 있습니다. 관리자는 다음 세 가지 방법 중 하나를 선택해 모바일 카드 템플릿을 적용할 수 있습니다.

- 기본 제공하는 카드 템플릿을 사용자의 모바일 카드로 적용하기
- 기존 템플릿의 매개 변수를 수정하여 커스텀 설정한 모바일 카드 적용하기

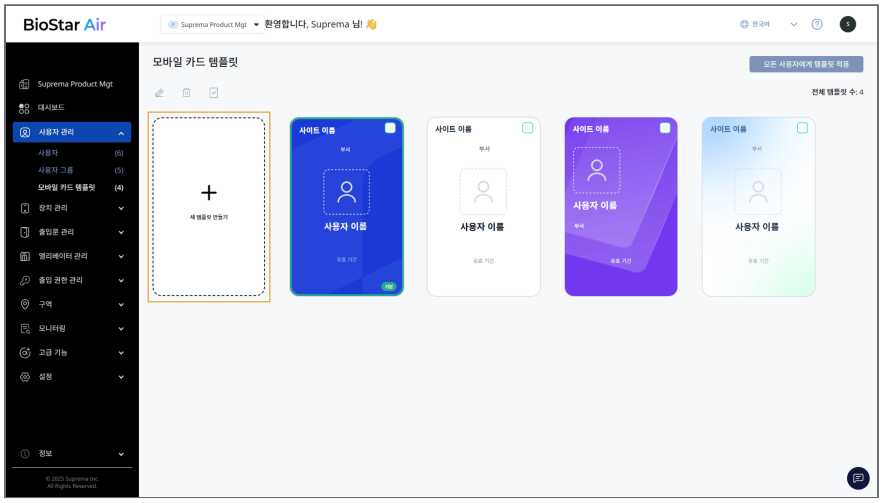
- 새로운 커스텀 템플릿을 만들어 기존 템플릿 대신 적용하기

> **팁**
> 카드 템플릿 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

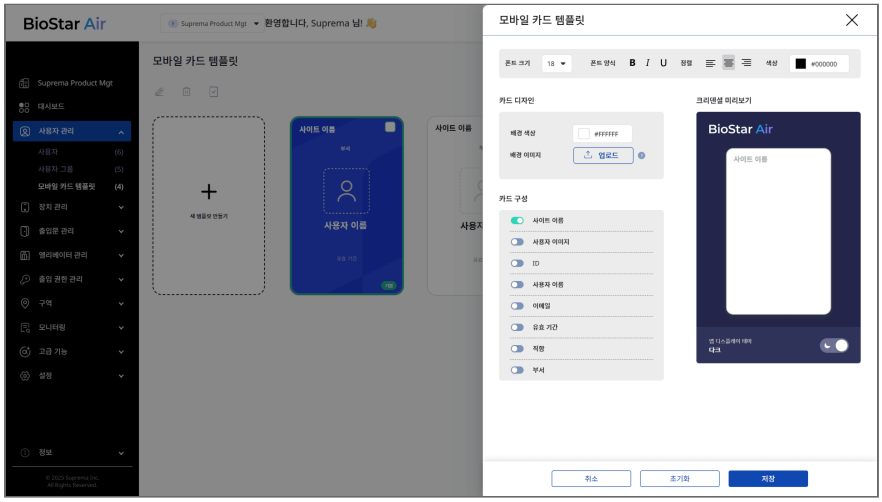
새 카드 템플릿 만들기

새 카드 템플릿을 만들 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.
2. **새 템플릿 만들기**를 클릭하세요.



3. **모바일 카드 템플릿** 패널이 나타나면 카드 디자인 및 구성을 설정하세요.



4. 원하는 설정을 적용한 후 모바일 카드 템플릿을 저장하려면 **저장** 버튼을 클릭하세요.

카드 디자인

카드 디자인 섹션에서는 카드의 배경 색상 또는 배경 이미지를 설정할 수 있습니다.

- **배경 색상**: 모바일 카드의 배경 색상을 설정할 수 있습니다.
- **배경 이미지**: 모바일 카드의 배경 이미지를 업로드할 수 있습니다. **업로드** 버튼을 클릭한 후 로컬에 저장된 배경 이미지 파일을 선택하세요. 이후 **이미지 자르기** 창이 나타나면 **사이즈 맞춤** 옵션을 클릭하거나 수동으로 크기를 조정하세요. 이미지 조정 설정을 완료한

후 **저장** 버튼을 클릭하세요.



카드 구성

카드 구성 섹션에서는 모바일 카드에 포함할 속성을 선택할 수 있습니다. 토글 스위치를 클릭하면 오른쪽 **크리덴셜 미리보기**에 선택한 속성이 표시됩니다.



- 원하는 속성을 배치하고 **크리덴셜 미리보기**에서 해당 요소를 클릭하면 크기, 위치, 각도를 조절할 수 있는 핸들이 표시됩니다.



- 각 속성의 폰트를 커스텀 설정할 수 있습니다. 배치된 속성을 클릭한 후 상단의 폰트 설정 옵션을 사용하세요. 폰트 크기 및 스타일, 정렬, 색상을 조정할 수 있습니다.

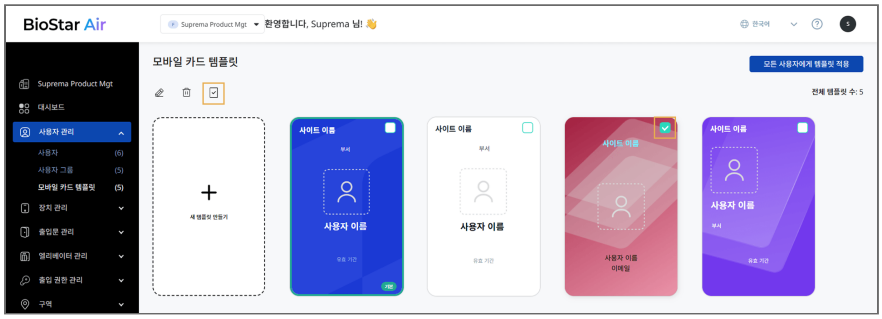


- **앱 디스플레이 테마**에서 다크 모드 또는 라이트 모드를 선택할 수 있습니다.
- 설정한 구성 및 디자인을 초기화하려면 **초기화** 버튼을 클릭하세요.
- 모든 설정을 완료한 후 모바일 카드 템플릿을 저장하려면 **저장** 버튼을 클릭하세요.

기본 카드 템플릿 설정

새로 추가한 모바일 카드 템플릿을 기본 템플릿으로 설정할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.
2. 원하는 템플릿의 오른쪽 상단의 체크박스를 클릭하세요.
3. 템플릿 목록 왼쪽 상단의 ☑ 버튼을 클릭하세요.



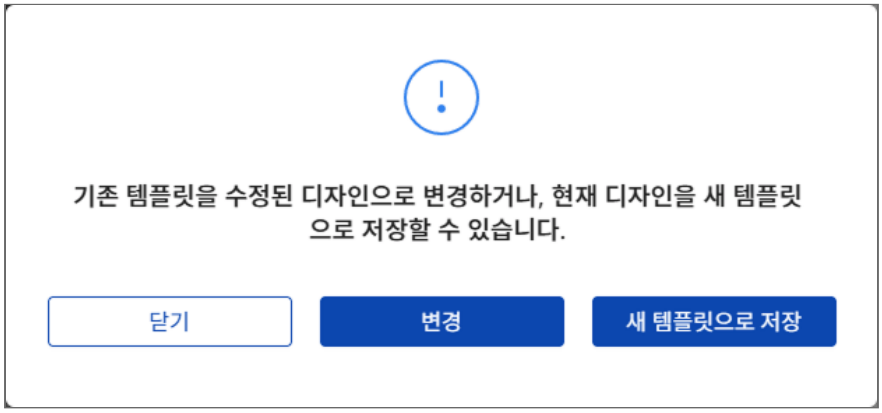
4. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

기본으로 설정된 모바일 카드 템플릿은 사용자를 새로 추가할 때 자동 적용됩니다.

> **알아두기**
> 기본 템플릿 설정 기능은 하나의 템플릿만 적용할 수 있습니다.

카드 템플릿 수정

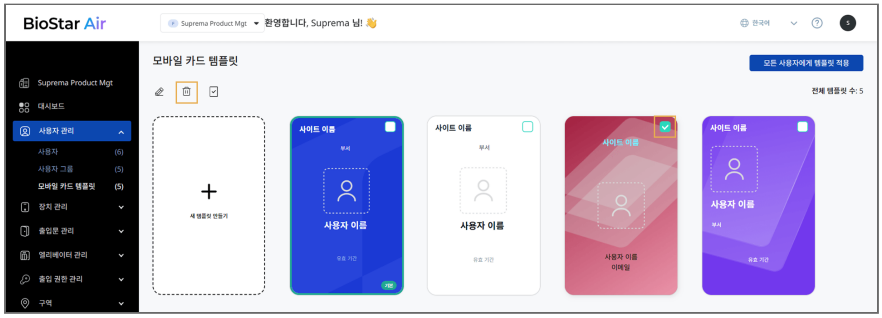
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.
2. 템플릿 목록에서 수정하려는 템플릿을 클릭하세요. 또는 템플릿 오른쪽 상단의 체크박스를 선택한 후 ✎ 버튼을 클릭하세요.
3. **모바일 카드 템플릿** 패널이 나타나면 카드 디자인 및 구성을 변경하세요.
4. 변경 사항을 저장하려면 **저장** 버튼을 클릭하세요.
5. 메시지 창이 나타나면 **변경** 또는 **새 템플릿으로 저장** 버튼을 클릭하세요.



- **변경**: 기존 템플릿을 수정하여 저장합니다.
- **새 템플릿으로 저장**: 수정한 내용을 새 템플릿으로 저장합니다.

카드 템플릿 삭제

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.
2. 템플릿 목록에서 삭제하려는 템플릿 오른쪽 상단의 체크박스를 클릭하세요. 한 개 이상의 템플릿을 선택할 수 있습니다.
3. 템플릿 목록 왼쪽 상단의 버튼을 클릭하세요.

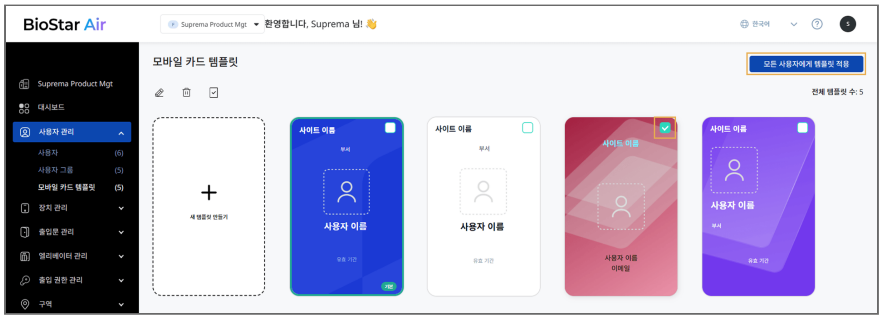


4. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 기본 제공하는 템플릿은 삭제할 수 없습니다.

모든 사용자에게 템플릿 적용

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **모바일 카드 템플릿**를 클릭하세요.
2. 템플릿 목록에서 적용하려는 템플릿 오른쪽 상단의 체크박스를 클릭하세요.
3. 화면 오른쪽 상단의 **모든 사용자에게 템플릿 적용** 버튼을 클릭하세요.



4. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

> **알아두기**
> - 모든 사용자에게 선택한 카드 템플릿을 적용하면 기존에 설정된 템플릿이 대체됩니다.
> - 한 개의 카드 템플릿만 모든 사용자에게 적용할 수 있습니다.

개별 사용자의 카드 템플릿 변경

개별 사용자의 카드 템플릿을 변경하려면 다음 단계를 따르세요.

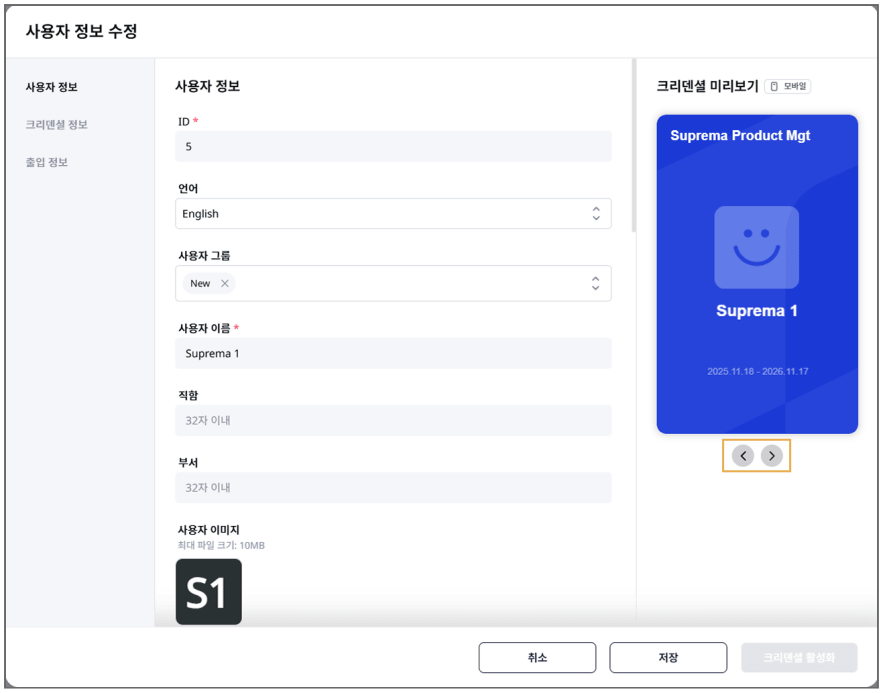
1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.

2. 사용자 목록에서 카드 템플릿을 적용할 사용자를 클릭하세요.

3. 사용자 세부 정보 오른쪽 상단의 버튼을 클릭하세요.



4. **사용자 정보 수정** 창이 나타나면 오른쪽 패널의 카드 템플릿 아래에서 또는 버튼을 클릭해 원하는 카드 템플릿을 선택하세요.



5. 변경 사항을 적용하려면 **저장** 버튼을 클릭하세요.

사용자 카드 및 크리덴셜 종류

BioStar Air 2.6 버전 이상부터 사용자 관리를 개선하기 위해 두 가지 사용자 유형이 도입했습니다.

- **일반**: 조직 또는 시설의 정규 구성원으로서 장기적이고 지속적인 출입 권한이 필요한 사용자입니다. 모든 크리덴셜 유형을 발급할 수 있습니다.
- **임시**: 단기적이고 제한적인 출입 권한이 필요한 방문자 또는 비정규 구성원입니다. 게스트, 외부 방문객, 단기 계약자, 배송 기사 등이 해당될 수 있습니다. QR 코드와 링크 패스(LinkPass)를 포함한 **웹 카드** 크리덴셜만 발급할 수 있습니다.

> **알아두기**
> 사용자 추가 및 수정 시 크리덴셜 발급에 대한 자세한 내용은 사용자 추가하기를 참고하세요.

> **팁**
> 사용자 및 카드 종류에 대한 동영상 가이드를 시청하려면 아래 영상을 참고하세요.

일반 사용자 카드 유형

일반 사용자에게 발급할 수 있는 크리덴셜 종류는 아래와 같습니다.

> **알아두기**
> 슈프리마 패스 앱을 통해 모바일 크리덴셜 사용 방법은 모바일 크리덴셜 사용하기을 참고하세요.

모바일 카드

- 고유한 **카드 아이디**가 자동 할당되지만 수동 설정할 수도 있습니다.
- **Airfob Tag** 또는 **Airfob Patch**를 사용한다면, 모바일 카드 번호를 카드 일련 번호로 사용하여 기존 출입 통제 시스템과 통합할 수 있습니다.
- 이전 시스템과의 호환성을 위해 모바일 카드 아이디는 이전 사이트의 RF 카드 번호와 일치할 수 있습니다.

RF 카드

- 사용자당 최대 8개의 RFID 카드를 추가할 수 있습니다.
- 여러 카드가 할당될 때 관리를 간소화하기 위해 **카드 종류**(CSN 또는 Wiegand), **카드 ID**, 및 **카드 이름**을 구성할 수 있습니다.
- 연결된 슈프리마 장치를 사용하여 기존 RFID 카드를 스캔하려면 **장치로 스캔** 항목에서 리더기를 선택하세요.
- 기존 RF 카드에 **CSN** (카드 일련 번호)이 있다면, CSN을 수동으로 입력할 수 있습니다.

웹 QR

- 일반 사용자는 모바일 카드의 **QR 코드**를 사용할 수 있습니다.
- QR 코드는 모바일 카드 인터페이스의 버튼을 눌러 사용할 수 있습니다.

링크 패스

- 사용자의 이메일 또는 휴대전화 번호로 웹 링크를 전달합니다.
- 사용자는 전달받은 링크를 웹 브라우저에서 열고, **문 열기** 버튼을 클릭해 출입할 수 있습니다.

> **알아두기**
> 링크패스 크리덴셜에 대한 자세한 내용은 링크패스 크리덴셜을 참고하세요.

얼굴 인증

- 사용자당 최대 2개의 얼굴 프로필 이미지를 추가할 수 있습니다.
- 연결된 리더기 또는 이미지 업로드를 통해 등록할 수 있습니다.
- 사용자에게 이메일 링크를 전송한 후 모바일 기기의 카메라로 사진을 찍어 등록할 수 있습니다.

2FA PIN

4~16자리 PIN을 설정하여 2단계 인증(2FA)의 일부로 사용할 수 있습니다.

임시 사용자 카드 유형

임시 사용자는 모바일 또는 RFID 카드를 받지 않습니다. 대신, 앱 다운로드가 필요 없는 **웹 기반 크리덴셜**을 발급할 수 있습니다. 사용할 수 있는 옵션은 아래와 같습니다.

웹 QR

- 이메일 또는 문자 메시지를 통해 전달합니다.
- 웹 브라우저를 통해 접근할 수 있습니다.
- 보안을 강화하기 위해 5분마다 업데이트되는 **동적 QR 코드**(Dynamic QR Code)를 사용합니다.

링크 패스

이메일 또는 문자 메시지를 통해 웹 링크를 사용자에게 전달합니다. 사용자는 웹 브라우저에서 **문 열기** 버튼을 클릭하면 출입할 수 있습니다.

> **알아두기**
> 링크패스 크리덴셜에 대한 자세한 내용은 링크패스 크리덴셜을 참고하세요.

출입 레벨 관리

일반 사용자이든 임시 사용자이든 관계없이 **출입 레벨**을 설정해 크리덴셜이 허용되는 위치를 제어해야 합니다.

> **주의**
> 임시 사용자라면 제한된 출입 레벨을 신중하게 할당하고, 무제한 출입 권한이 부여된 자격 증명을 부여하지 않도록 주의하세요.

링크패스 크리덴셜

링크패스(LinkPass)는 BioStar Air에서 앱 없이 사용할 수 있는 모바일 크리덴셜입니다. 관리자는 앱을 설치하거나 BLE/NFC를 사용하지 않고도 사용자에게 출입 권한을 부여할 수 있습니다. 링크패스는 BioStar Air 클라우드를 통해 작동하며 보안 웹 링크를 통해 활성화되므로, 고객 출입, 배달, 또는 주차장 게이트나 로비와 같은 보안 등급이 낮은 출입구에서 사용하기에 적합합니다.

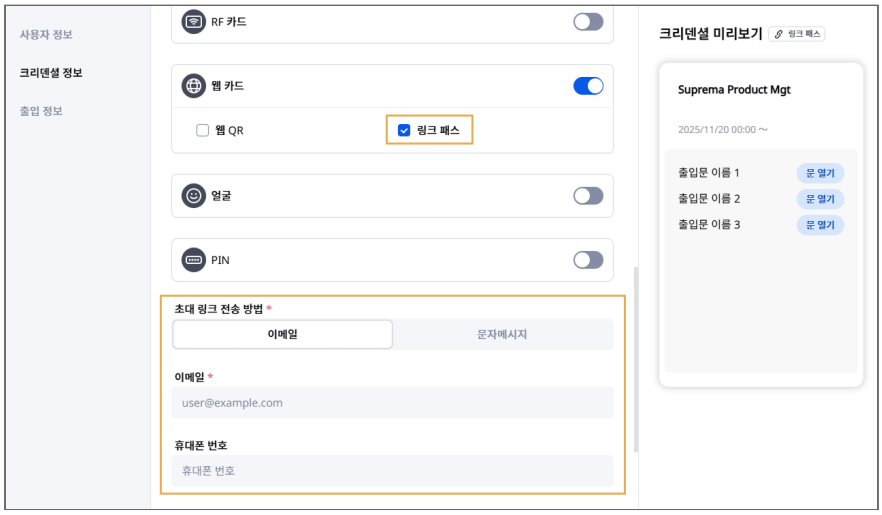
- **크리덴셜 범위**: 링크패스는 사용자에게 할당된 다른 크리덴셜과 동일한 출입문에 대한 접근을 허용합니다. 따라서 보안 등급이 높은 구역에 출입 권한이 없는 사용자에게 링크패스 크리덴셜을 발급하는 것은 권장하지 않습니다.
- **앱 필요 없음**: 링크패스는 웹 브라우저를 통해 작동하므로 모바일 앱, 블루투스 또는 NFC 통신이 필요하지 않습니다.
- **클라우드 기반 액세스**: 링크패스 명령은 BioStar Air 클라우드를 통해 전송되며 인터넷이 연결된 모든 곳에서 활성화할 수 있습니다. 위치 공유 또는 위치 추적 기능은 없습니다.
- **장치 연결성**: 출입문 장치에서 링크패스가 올바르게 작동하려면 온라인 상태여야 하며 BioStar Air에 연결되어 있어야 합니다.
- **사용 사례 권장 사항**: 링크패스는 임시 방문자, 배달 및 로비 또는 주차 게이트와 같은 보안 등급이 낮은 구역에 적합합니다.

링크패스 크리덴셜 활성화

1. BioStar Air 웹 사이트에 로그인하세요.
2. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
3. 다음 중 하나의 방법으로 **사용자 정보 수정** 또는 **사용자 추가** 화면으로 이동하세요.
    - 사용자 목록에서 기존 사용자를 클릭한 후 오른쪽 상단의 버튼을 클릭하세요.
    - 화면 오른쪽 상단의 **사용자 추가** → **사용자 추가**를 클릭하세요.
4. **크리덴셜 정보** 섹션으로 이동하세요.
5. **웹 카드** 옵션을 활성화하세요.



6. **링크 패스**의 체크박스를 클릭하세요.
7. **초대 링크 전송 방법**에서 사용자가 크리덴셜 링크를 받을 수 있는 고유한 **이메일 주소** 또는 **휴대폰 번호**를 입력하세요.



8. 적절한 **출입 레벨**을 선택하고 사용자의 **유효 기간**을 설정하세요.
9. 크리덴셜을 발급하려면 **크리덴셜 활성화** 버튼을 클릭하세요.
10. 사용자에게 고유한 링크패스 URL이 포함된 초대장을 이메일 또는 SMS로 전송합니다.

사용자의 링크패스 사용

1. 이메일 또는 SMS로 전송 받은 사용자는 모바일 기기에서 메시지의 링크패스 URL을 여세요.
2. 웹 페이지에는 사용자에게 할당된 모든 출입문이 표시되며, 각 출입문에는 **문 열기** 버튼이 있습니다.
3. **문 열기** 버튼을 클릭하면 클라우드 기반 잠금 해제 명령이 리더기로 전송되어 출입문을 열 수 있습니다.

> **알아두기**
> 링크패스 사용에는 블루투스 또는 NFC 통신이 필요하지 않습니다.

장치

BioStar Air의 유연한 장치 관리 설정을 통해 모든 사이트(Site)의 요구 사항을 정확하게 구성할 수 있습니다. 이 문서에서 장치 관리는 등록,

구성, 펌웨어 관리, 모니터링, 지속적인 운영을 포함한 장치의 전체 라이프사이클을 의미합니다.

BioStar Air는 두 가지 장치 아키텍처를 지원합니다. 두 아키텍처 모두 동일한 사이트에서 함께 사용할 수 있으므로, 각 출입문나 구역에 가장 적합한 방식을 선택할 수 있습니다.

분산형 아키텍처

분산형 아키텍처에서는 각 엣지 장치가 자체 컨트롤러가 내장되어 있으며 이더넷을 통해 클라우드에 직접 연결됩니다. 네트워크 연결이 끊어지더라도 장치는 독립적으로 작동하며, 연결이 복구되면 자동으로 동기화됩니다.

엣지 장치는 RS-485를 통해 연결된 보조 장치의 컨트롤러 역할도 할 수 있습니다.

이 아키텍처는 다음과 같은 경우에 주로 사용됩니다.

- 신규 설치
- 바이오메트릭 장치
- 인프라 구축을 최소화해야 하는 경우

중앙 집중식 아키텍처

중앙 집중식 아키텍처에서는 장치가 RS-485 또는 Wiegand를 통해 컨트롤 패널에 연결됩니다. 컨트롤 패널은 이더넷을 통해 클라우드에 연결되고 연결된 장치들을 관리하는 컨트롤러로 작동합니다.

컨트롤 패널은 네트워크 연결이 끊기면, 연결된 장치들의 중복성 관리와 출입 제어 결정을 담당합니다.

이 아키텍처는 다음과 같은 경우에 주로 사용됩니다.

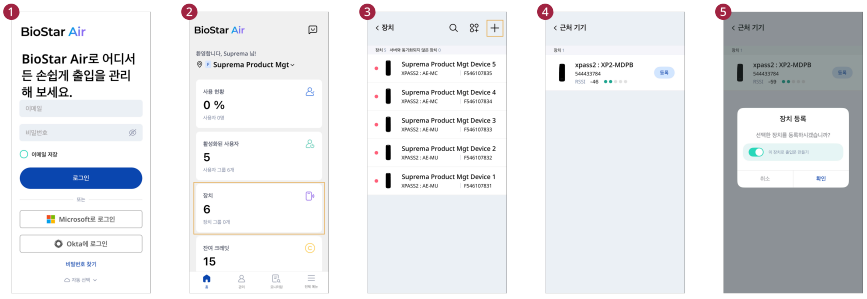
- 기존 저전압 배선이 있는 재구축 프로젝트
- 기존 출입 제어 시스템을 교체하는 사이트
- 중앙 집중식 보안실 또는 제어 패널을 사용하는 구축 환경

엣지 장치 등록 및 삭제하기

장치를 BioStar Air에 추가하려면 BioStar Air 모바일 앱을 사용해야 합니다. 모바일 앱에서는 무선 연결을 통해 새로운 장치를 등록하거나 기존 장치를 제거할 수 있으며, 펌웨어를 업그레이드할 수도 있습니다.

장치 등록

BioStar Air 모바일 앱을 사용하여 장치를 등록할 수 있습니다. 장치 등록은 Bluetooth Low Energy(BLE) 방식으로 이루어지며, 등록된 장치는 BioStar Air 포털에서 관리할 수 있습니다.



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.

2. **장치** 카드를 탭하세요.
3. 화면 오른쪽 상단의 ＋ 버튼을 탭하세요.
4. 장치 검색 화면에서 등록하려는 장치의 **등록** 버튼을 탭하세요.
5. 장치 등록 창이 나타나면 **확인** 버튼을 탭하세요.

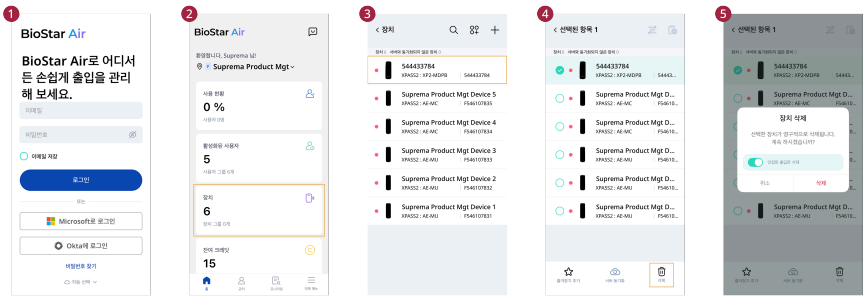
장치 목록으로 돌아가 추가된 장치를 확인하세요.

> **팁**
> 최상의 성능과 신뢰성을 유지하고 최신 기능을 사용하려면 장치를 등록하자마자 펌웨어 업그레이드를 반드시 확인하세요. 장치가 포장된 시점과 설치된 시점 사이에 새 펌웨어가 배포되었을 수 있습니다. 펌웨어 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

> **알아두기**
> - 웹 포털에서는 장치를 등록할 수 없습니다. 장치는 반드시 BioStar Air 모바일 앱을 통해 등록해야 합니다.
> - 장치를 등록할 때는 장치와 모바일 기기가 가까운 거리에 있어야 하며, 모바일 기기의 블루투스 기능이 활성화되어 있어야 합니다.
> - 등록한 장치를 출입문으로 설정하지 않으려면 장치 등록 창에서 **이 장치로 출입문 만들기** 옵션을 해제하세요.

장치 삭제

BioStar Air 포털의 장치 목록에서 장치가 오프라인 상태라면 모바일 앱을 사용하여 장치를 삭제할 수 있습니다.



1. 모바일 기기에서 BioStar Air 앱을 실행하세요.
2. **장치** 카드를 탭하세요.
3. 목록에서 삭제할 장치를 길게 터치하세요. 추가로 삭제할 장치를 선택하세요.
4. 화면 오른쪽 하단의 🗑 버튼을 탭하세요.
5. 팝업 메시지 창에서 연결된 출입문을 삭제할지 선택하세요.
6. **삭제**를 탭하세요.

> **알아두기**
> X-Station 2 제외한 장치는 BioStar Air 포털에서 삭제할 수 있습니다. 단, 장치는 온라인 상태여야 합니다. BioStar Air 모바일 앱을 사용하여 장치를 삭제할 것을 권장합니다.

등록된 엣지 장치 관리하기

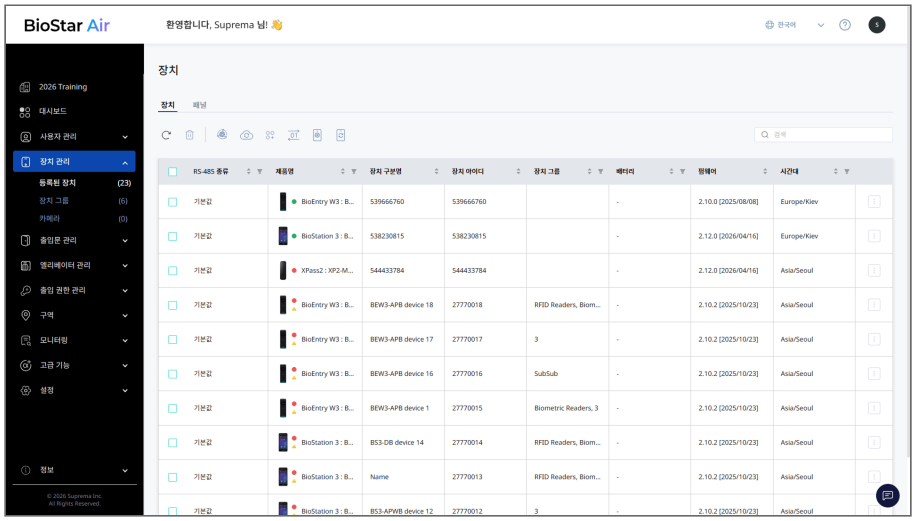
등록된 장치의 연결 상태를 한눈에 확인하고, 생체 인증과 카드 설정을 변경하거나 펌웨어를 업데이트합니다. 소수의 장치는 개별로, 다수의 장치는 일괄로 관리할 수 있어 보안 시스템을 효율적으로 운영할 수 있습니다.

> **알아두기**
>
> - 장치는 iOS 또는 안드로이드의 **BioStar Air 모바일 앱**에서만 등록할 수 있습니다. 웹 포털에서는 등록할 수 없습니다. 모바일 앱에서 장치 등록 방법에 대한 자세한 내용은 엣지 장치 등록 및 삭제하기를 참고하세요.
> - **원격 접속, 생체 인증, QR 코드 출입, 펌웨어 업데이트**와 같은 일부 기능을 사용하려면 장치는 인터넷 연결이 필요합니다.

> **팁**
>
> 장치 등록 및 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

장치 목록 조회

장치 목록에서는 BioStar Air에 등록된 모든 장치를 확인할 수 있습니다. 각 장치의 연결 상태, 모델명, 펌웨어 버전 등 주요 정보를 한눈에 볼 수 있습니다. 또한 개별 장치를 클릭하여 세부 정보를 확인하고 설정을 수정할 수 있습니다.



화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.

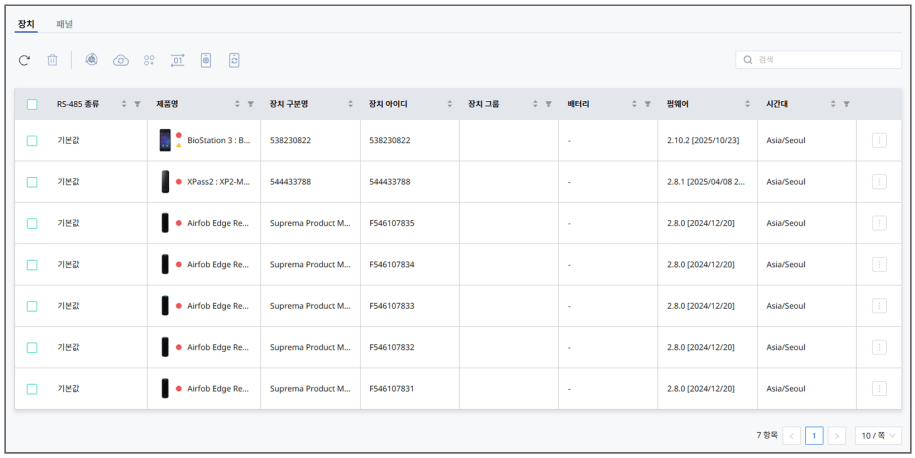
장치 연결 상태

장치 목록에서 상태 아이콘을 통해 각 장치의 연결 상태를 확인할 수 있습니다.

- 🟢 **녹색**: 온라인 상태로, 해당 장치는 원격으로 제어할 수 있으며, QR 인증을 수락하고 업데이트할 수 있습니다.
- 🔴 **빨간색**: 오프라인 상태의 장치입니다.
- 🟠 **주황색**: 펌웨어 업데이트 진행 중인 상태입니다.
- ○ **연결 없음**: 네트워크 연결이 없는 장치입니다. (예, Airfob Patch)
- ⚠️ **주의**: 서버와 장치 간의 동기화가 필요한 상태입니다. 재동기화 방법은 오프라인 장치 재동기화를 참고하세요.

장치 정보

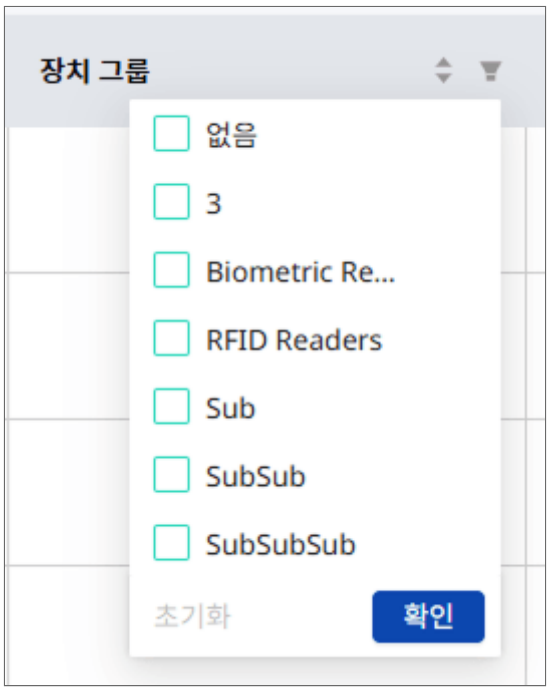
장치 목록의 각 열은 아래 정보를 포함하고 있습니다.



- **RS-485 종류**: RS-485 통신을 지원하는 장치에서 확인할 수 있습니다. 해당 장치가 마스터 장치인지 슬레이브 장치인지 확인할 수 있습니다. 마스터 또는 슬레이브로 설정되지 않은 장치는 **기본값**으로 표시됩니다.
- **제품명**: 슈프리마 데이터베이스로부터 가져온 장치 이름과 모델명입니다.
- **장치 구분명**: 쉽게 식별할 수 있도록 사용자가 수정할 수 있는 항목입니다. 장치 목록에서 장치를 클릭하면 표시되는 **장치 정보 수정** 창에서 변경할 수 있습니다.
- **장치 아이디**: 장치에 할당된 고유 식별자입니다.
- **장치 그룹**: 장치가 속한 그룹입니다.
- **배터리**: 배터리로 작동하는 장치에서 확인할 수 있습니다. 에어팝 태그(AirFob Tag) 장치만 지원합니다.
- **펌웨어**: 현재 설치된 펌웨어 버전입니다.
- **시간대**: 장치에 설정된 시간대입니다.

필터링

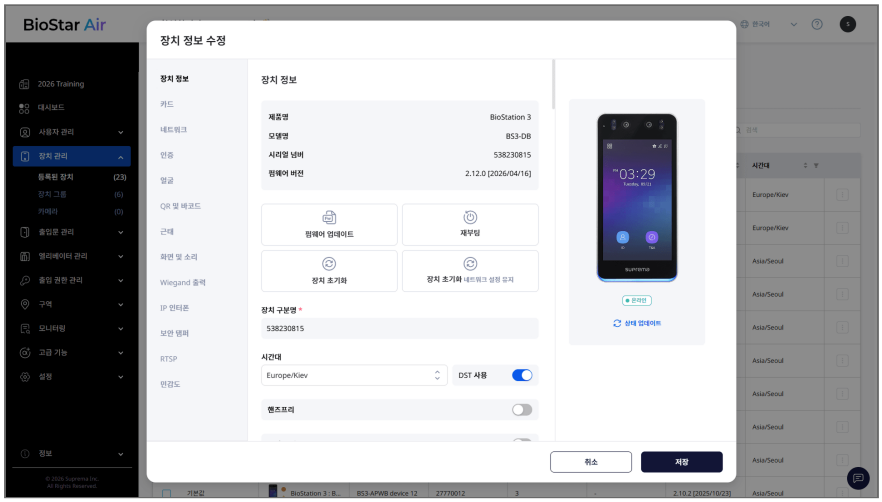
장치 목록의 상단 헤더 영역에서 필터링 기능을 이용할 수 있습니다. 헤더 영역의 버튼을 클릭하면 원하는 조건을 설정할 수 있습니다.



> **알아두기**
>
> 적용한 필터 조건을 초기화하려면 버튼을 클릭하고 **초기화** 버튼을 선택하세요.

개별 장치 정보 및 설정 수정

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 목록에서 수정할 장치를 클릭하세요.
3. **장치 정보 수정** 창이 나타납니다.



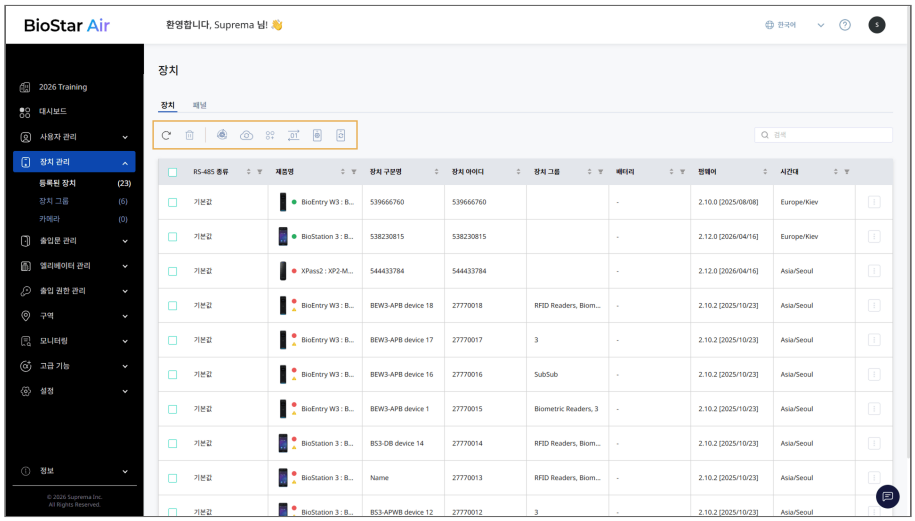
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

4. 장치의 세부 정보 또는 설정을 수정하세요.
5. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

각 섹션별 세부 정보 수정 및 설정 옵션에 대한 자세한 내용은 장치 및 패널 설정 옵션 안내를 참고하세요.

장치 일괄 작업

장치 목록 상단에서 제공하는 기능을 통해 여러 장치를 한 번에 관리할 수 있습니다.



- : 장치 목록을 새로고침할 수 있습니다.

- : 사이트에 등록된 장치를 삭제할 수 있습니다.

  > **경고**
  > 온라인 상태의 장치만 영구적으로 삭제할 수 있입니다. 장치가 오프라인이라면, 다른 사이트에 추가하기 전에 BioStar Air 모바일 앱에서 먼저 삭제하세요. 모바일 앱에서 장치 삭제 방법에 대한 자세한 내용은 엣지 장치 등록 및 삭제하기를 참고하세요.

- : 장치 목록에서 선택한 장치의 펌웨어를 업데이트할 수 있습니다. 펌웨어 업데이트에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.
- : 장치 목록에서 선택한 장치에서 서버로 생체 인증 템플릿을 동기화할 수 있습니다.
- : 장치 목록에서 선택한 장치를 그룹에 할당할 수 있습니다. 장치 그룹 관리에 대한 자세한 내용은 장치 그룹 관리를 참고하세요.
- : 장치 목록에서 선택한 장치의 RF 카드 바이트 순서를 **MSB** 또는 **LSB**로 전환할 수 있습니다.
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- : 독립 실행 모드에서 원래 설정된 장치의 설정을 가져올 수 있습니다.
- : 장치 목록에서 선택한 장치의 상태를 업데이트할 수 있습니다.

오프라인 장치 재동기화

장치가 오랫동안 오프라인 상태였다면 서버와 정보가 어긋나 수동으로 재동기화해야 할 수 있습니다.

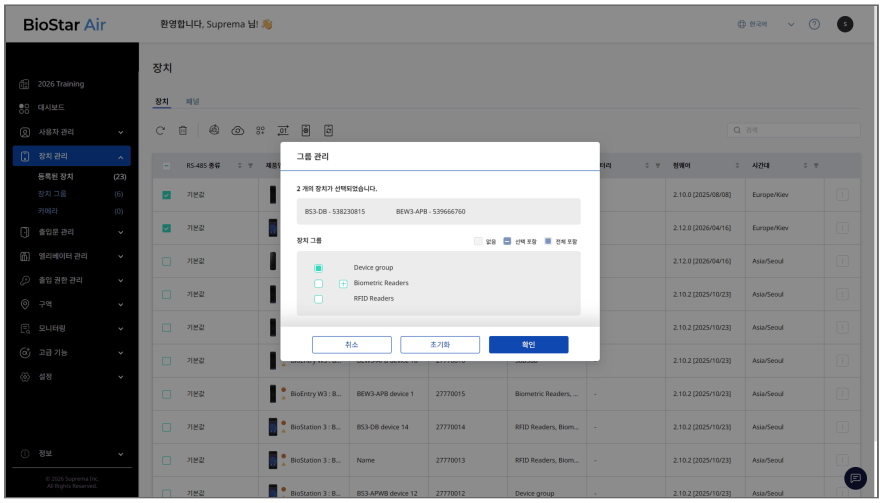
1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록의 **제품명** 열에서 ⚠ 아이콘이 표시된 장치를 확인하세요.
3. 해당 장치의 체크박스를 선택하세요.
4. 목록 상단 도구 모음에서 버튼을 클릭하세요.

> **알아두기**
> 7일 미만 오프라인 상태였던 장치는 재연결 시 자동으로 동기화되므로 별도 조치가 필요하지 않습니다.

장치 그룹 관리

장치 목록에서 개별 장치를 선택하여 장치 그룹에 추가하거나, 기존 그룹에서 제거할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**을 클릭하세요.
2. 장치 목록에서 그룹에 추가하거나 제거하려는 장치의 체크박스를 클릭하세요.
3. 장치 목록 상단의 버튼을 클릭하세요.
4. **그룹 관리** 창이 나타나면 선택한 장치를 그룹에 추가하거나 제거하세요.



장치 그룹의 체크박스 상태는 아래와 같은 의미를 가집니다.

- **없음**: 선택한 장치를 그룹에서 제거합니다.
- **선택 포함**: 선택한 장치 중 일부가 그룹에 포함된 상태입니다.
- **전체 포함**: 선택한 장치를 그룹에 추가합니다.

5. 변경한 내용을 저장하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **그룹 관리** 창에서 다른 그룹을 선택하면 선택한 장치는 해당 그룹으로 이동합니다.
> - 장치는 그룹에 중복으로 속할 수 있습니다. 하나의 장치를 여러 그룹에 할당할 수 있습니다.
> - 변경한 내용을 초기화하려면 **초기화** 버튼을 클릭하세요.

패널 등록 및 삭제하기

BioStar Air 2.12 버전에서는 CoreStation 20(CS-20) 패널을 통해 출입 제어 시스템을 확장할 수 있습니다. 기존의 RS-485 배선을 활용해 추가 장치를 로컬에 연결하므로 인프라 비용을 절감하면서도 복잡한 출입문 구성을 지원할 수 있습니다.

이 문서에서는 CS-20 패널을 등록하고, RS-485, OSDP, Wiegand 통신 방식의 장치를 보조 장치로 구성하는 방법을 단계별로 안내합니다.

> BioStar Air에서는 컨트롤러 역할을 하는 마스터(Primary) 장치, 컨트롤러에 연결되는 보조(Secondary) 장치로 구분됩니다. 일부 시스템에서는 이 개념을 마스터(Master)/슬레이브(Slave)로 표현하지만, BioStar Air 문서에서는 해당 용어를 사용하지 않습니다.

패널 등록

CoreStation 20(이하 CS-20)은 RS-485 통신을 지원하는 장치와 연결하여 출입 제어 시스템을 확장할 수 있는 기능을 제공합니다. CS-20을 등록하려면 다음 단계를 따르세요.

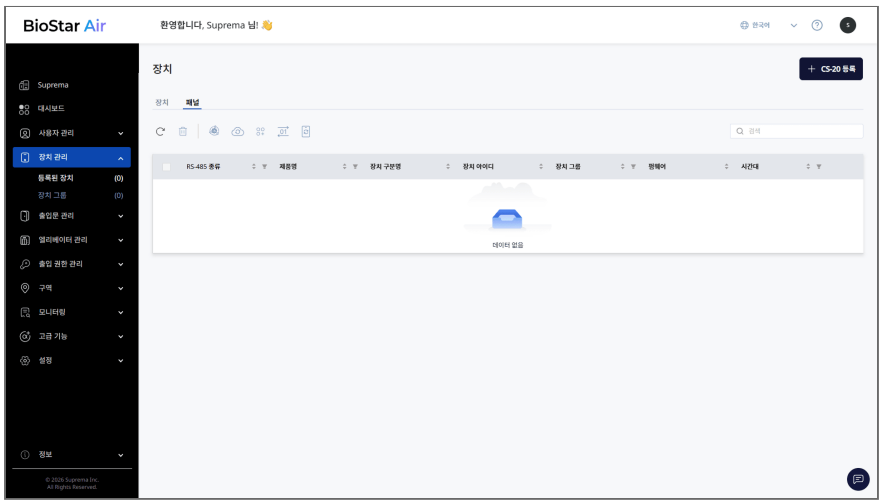
시작하기 전에

- CS-20의 전원이 켜져 있고, **INIT** 버튼을 누르기 위해 물리적으로 접근할 수 있어야 합니다.
- CS-20이 외부 인터넷과 연결되어 있어야 합니다. 네트워크 연결이 불안정한 경우 등록 과정에서 문제가 발생할 수 있습니다.
- 9자리의 시리얼 번호가 필요합니다. 시리얼 번호는 장치 뒷면의 라벨에서 확인할 수 있습니다.

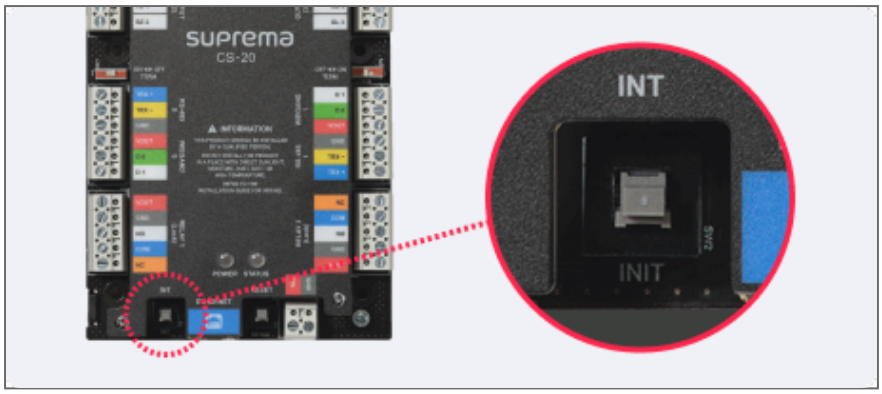
> **알아두기**
> CoreStation 20에 대한 자세한 내용은 CoreStation 20 설치 가이드를 참고하세요.

CS-20 등록

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.

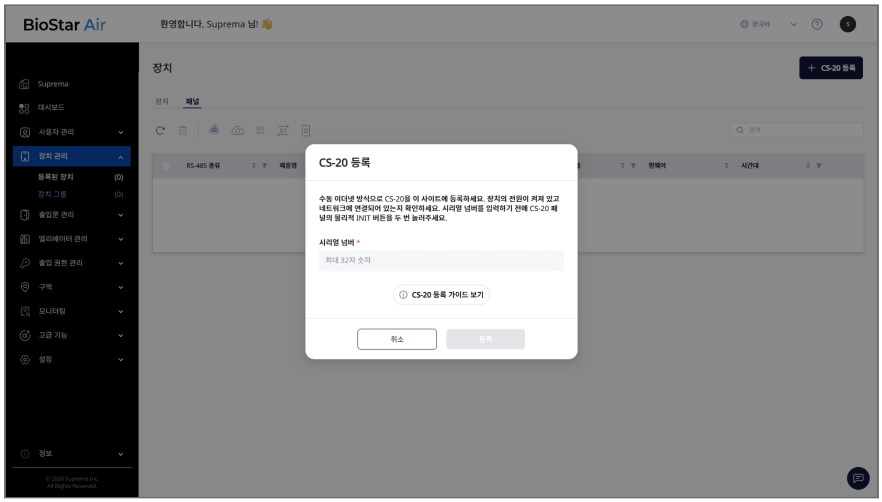


3. 화면 오른쪽 상단의 **CS-20 등록** 버튼을 클릭하세요.
4. **CS-20 등록** 창이 나타나면 CS-20 패널에서 INIT 버튼을 두번 누르세요.



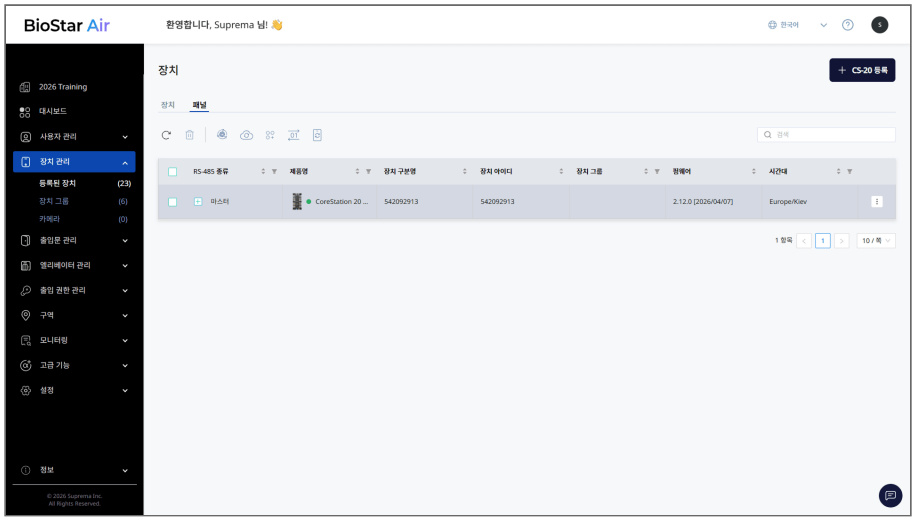
> **주의**
> INIT 버튼을 누른 후 CS-20을 등록 완료할 수 있는 시간은 5분입니다.

5. 시리얼 번호를 입력하세요.



6. 시리얼 번호를 모두 입력한 후 **등록** 버튼을 클릭하세요.

등록을 완료하면 시스템이 보안 연결을 자동 설정하고 패널 목록에 새 CS-20이 표시됩니다. 정상 등록되었다면 장치 이름 옆에 초록색 점이 표시됩니다.



팁

최상의 성능과 신뢰성을 유지하고 최신 기능을 사용하려면 장치를 등록하자마자 펌웨어 업그레이드를 반드시 확인하세요. 장치가 포장된 시점과 설치된 시점 사이에 새 펌웨어가 배포되었을 수 있습니다. 펌웨어 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

알아두기

CS-20 등록 과정에 대한 자세한 내용을 확인하려면 **CS-20 등록 가이드 보기** 버튼을 클릭하세요.

패널 삭제

BioStar Air에 등록된 패널을 삭제하려면 다음 단계를 따르세요. 삭제된 패널은 복구할 수 없습니다. 패널을 삭제하기 전에 해당 패널과 연결된 보조 장치가 더 이상 필요하지 않은지 확인하세요.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.

3. 목록에서 삭제할 패널의 체크박스를 클릭하세요.

4. 화면 왼쪽 상단의 버튼을 클릭하세요.



5. 팝업 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

> **주의**
> 연결된 보조 장치를 다시 사용해야 한다면, SCB 키가 바인딩되어 있을 수 있기 때문에 보조 장치를 먼저 삭제하고 패널을 삭제하는 것을 권장합니다.

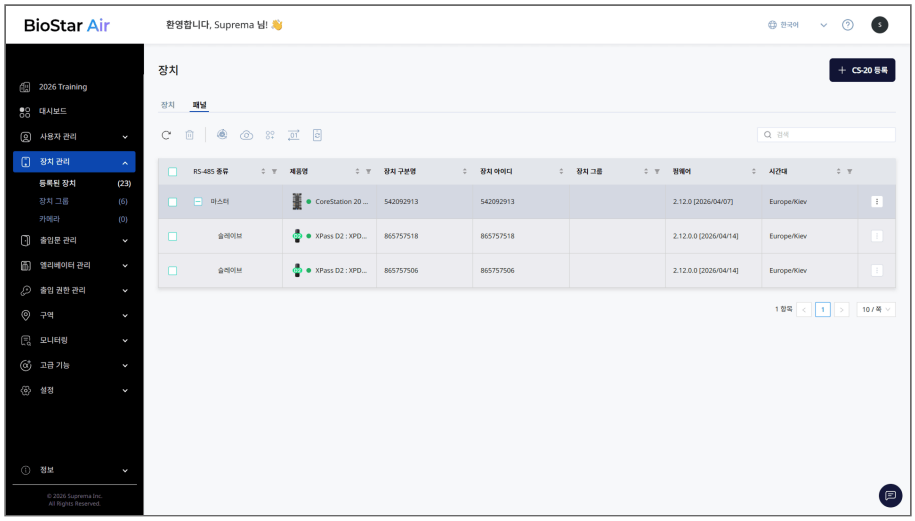
등록된 패널 관리하기

BioStar Air에서 등록된 모든 패널을 한 곳에서 관리할 수 있습니다. 각 패널의 상태를 모니터링하고, 필요에 따라 정보를 수정하며, 그룹으로 구성하고, 펌웨어를 업데이트할 수 있습니다. 이 문서에서는 패널 목록 조회부터 그룹 관리까지 필요한 모든 기능을 확인할 수 있습니다.

> **알아두기**
> BioStar Air에서는 컨트롤러 역할을 하는 마스터(Primary) 장치, 컨트롤러에 연결되는 보조(Secondary) 장치로 구분됩니다. 일부 시스템에서는 이 개념을 마스터(Master)/슬레이브(Slave)로 표현하지만, BioStar Air 문서에서는 해당 용어를 사용하지 않습니다.

패널 목록 조회

등록된 패널은 **패널** 탭에서 관리할 수 있습니다. 패널 목록에서는 각 패널 또는 보조 장치의 종류 및 상태, 이름, 아이디, 그룹, 펌웨어 정보, 시간대와 같은 주요 정보를 한눈에 확인할 수 있습니다.



패널 및 장치 상태

패널 목록의 상태 아이콘을 통해 각 패널 또는 보조 장치의 연결 상태를 확인할 수 있습니다.

- 🟢 **녹색**: 온라인 상태로, 해당 패널 또는 보조 장치는 원격으로 제어할 수 있으며 업데이트할 수 있습니다.
- 🔴 **빨간색**: 오프라인 상태의 패널 또는 보조 장치입니다.
- 🟠 **주황색**: 펌웨어 업데이트 진행 중인 상태입니다.
- ⚠️ **주의**: 서버와 패널 또는 보조 장치 간의 동기화가 필요한 상태입니다. 재동기화 방법은 오프라인 패널 및 보조 장치 재동기화를 참고하세요.

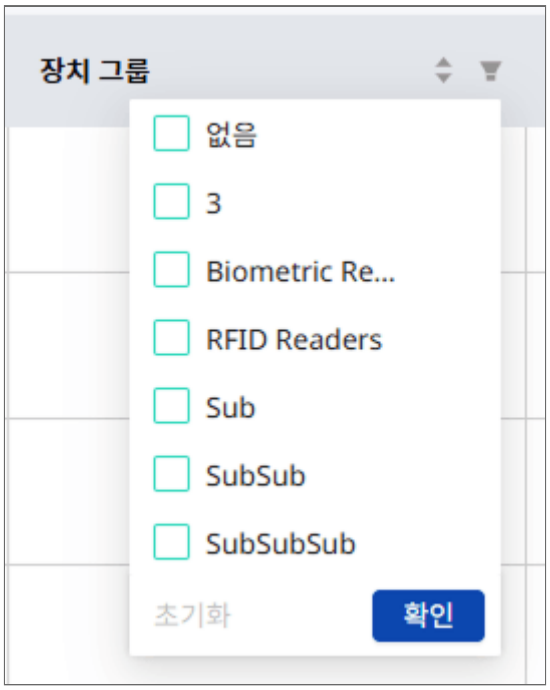
패널 및 장치 정보

패널 목록의 각 열은 아래 정보를 포함하고 있습니다.

- **RS-485 종류**: RS-485 통신을 지원하는 패널 또는 보조 장치에서 확인할 수 있습니다. 해당 장치가 마스터 장치인지 보조 장치인지 확인할 수 있습니다.
- **제품명**: 슈프리마 데이터베이스로부터 가져온 패널 또는 보조 장치 이름과 모델명, 상태를 확인할 수 있습니다.
- **장치 구분명**: 쉽게 식별할 수 있도록 사용자가 수정할 수 있는 항목입니다. 목록에서 패널 또는 보조 장치를 클릭하면 표시되는 정보 수정 창에서 변경할 수 있습니다.
- **장치 아이디**: 패널 또는 보조 장치에 할당된 고유 식별자입니다.
- **장치 그룹**: 패널이 속한 그룹입니다.
- **펌웨어**: 현재 설치된 펌웨어 버전입니다.
- **시간대**: 패널 또는 보조 장치에 설정된 시간대입니다.

필터링

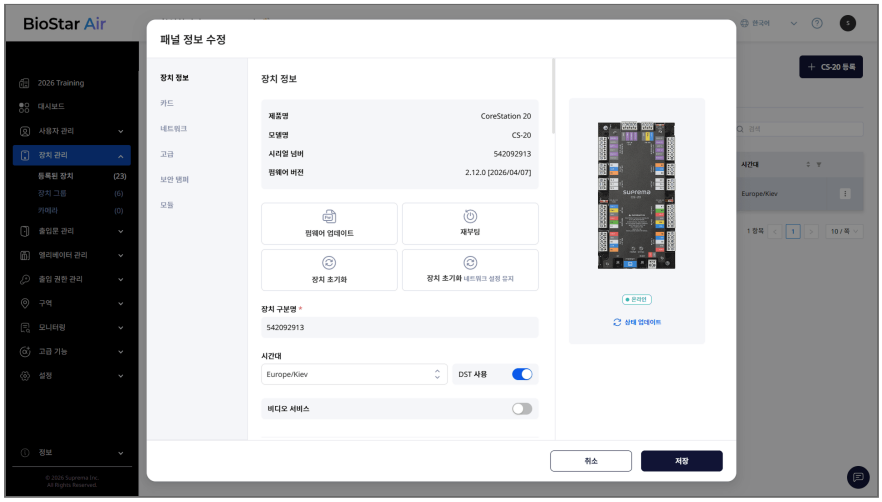
패널 목록의 상단 헤더 영역에서 필터링 기능을 이용할 수 있습니다. 헤더 영역의 ▼ 버튼을 클릭하면 원하는 조건을 설정할 수 있습니다.



> **알아두기**
>
> 적용한 필터 조건을 초기화하려면 ▼ 버튼을 클릭하고 **초기화** 버튼을 선택하세요.

패널 정보 수정

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.
3. 목록에서 정보를 수정할 패널을 클릭하면 **패널 정보 수정** 창이 나타납니다.



4. 패널의 세부 정보 또는 설정을 수정하세요.
5. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

> **알아두기**
> 각 섹션별 세부 정보 수정 및 설정 옵션에 대한 자세한 내용은 장치 및 패널 설정 옵션 안내를 참고하세요.

패널 관리 기능

패널 목록에서 패널을 선택해 목록 상단에서 제공하는 관리 기능을 사용할 수 있습니다.



- : 목록을 새로고침할 수 있습니다.
- : 등록된 패널 또는 보조 장치를 삭제할 수 있습니다.
- : 패널 목록에서 선택한 패널 또는 보조 장치의 펌웨어를 업데이트할 수 있습니다. 펌웨어 업데이트에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

- CS-20에 연결된 보조 장치는 한 번에 한 개의 장치만 업그레이드할 수 있습니다.
- XPass D2 장치 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

- : 목록에서 선택한 패널에서 서버로 생체 인증 템플릿을 동기화할 수 있습니다.
- : 목록에서 선택한 패널을 그룹에 할당할 수 있습니다. 그룹 관리에 대한 자세한 내용은 패널 그룹 관리를 참고하세요.
- : 목록에서 선택한 패널의 RF 카드 바이트 순서를 **MSB** 또는 **LSB**로 전환할 수 있습니다.
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- : 독립 실행 모드에서 원래 설정된 패널의 설정을 가져올 수 있습니다.
- : 목록에서 선택한 패널의 상태를 업데이트할 수 있습니다.

알아두기

CS-20에 연결된 보조 장치는 새로 고침(), 장치 삭제(), 펌웨어 업데이트() 기능만 제공합니다.

오프라인 패널 및 보조 장치 재동기화

패널 또는 보조 장치가 오랫동안 오프라인 상태였다면 서버와 정보가 어긋나 수동으로 재동기화해야 할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.
3. 목록의 **제품명** 열에서 ⚠ 아이콘이 표시된 패널 또는 보조 장치를 확인하세요.
4. 해당 패널 또는 보조 장치의 체크박스를 선택하세요.
5. 목록 상단 도구 모음에서 버튼을 클릭하세요.

알아두기

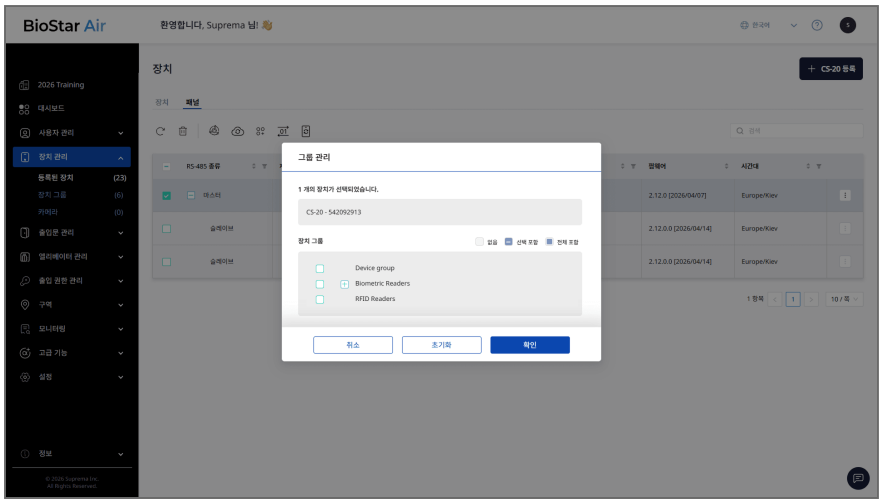
7일 미만 오프라인 상태였던 패널 또는 보조 장치는 재연결 시 자동으로 동기화되므로 별도 조치가 필요하지 않습니다.

패널 그룹 관리

패널 목록에서 개별 패널을 선택하여 그룹에 추가하거나, 기존 그룹에서 제거할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.
3. 패널 목록에서 그룹에 추가하거나 제거하려는 패널의 체크박스를 클릭하세요.
4. 패널 목록 상단의 버튼을 클릭하세요.

5. **그룹 관리** 창이 나타나면 선택한 패널을 그룹에 추가하거나 제거하세요.



장치 그룹의 체크박스 상태는 아래와 같은 의미를 가집니다.

- **없음**: 선택한 패널을 그룹에서 제거합니다.
- **선택 포함**: 선택한 패널 중 일부가 그룹에 포함된 상태입니다.
- **전체 포함**: 선택한 패널을 그룹에 추가합니다.

6. 변경한 내용을 저장하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **그룹 관리** 창에서 다른 그룹을 선택하면 선택한 패널은 해당 그룹으로 이동합니다.
> - 패널은 그룹에 중복으로 속할 수 있습니다. 하나의 패널을 여러 그룹에 할당할 수 있습니다.
> - 패널 목록에서 보조 장치는 펌웨어 업그레이드 기능만 제공합니다.
> - 변경한 내용을 초기화하려면 **초기화** 버튼을 클릭하세요.

패널에 장치 추가 및 관리하기

BioStar Air 시스템은 마스터 장치인 CS-20 패널을 중심으로 여러 종류의 보조 장치를 연결할 수 있습니다. RS-485, OSDP, Wiegand 등 다양한 통신 프로토콜을 지원하여 기존 보안 시스템과의 용이하게 통합할 수 있습니다. 이 문서에서는 보조 장치 구성, 관리, 삭제 방법을 안내합니다.

보조 장치 구성

CS-20을 등록한 후, 다음 중 하나의 방식으로 보조 장치를 구성할 수 있습니다:

보조 장치	설명
슈프리마 RS-485 장치	XPass D2 및 OM-120 장치에 기존 RS-485 배선과 표준 통신 프로토콜 사용
OSDP 장치	보안 강화 통신 프로토콜 사용
Wiegand 장치	카드 리더 등 기존 Wiegand 호환 장치

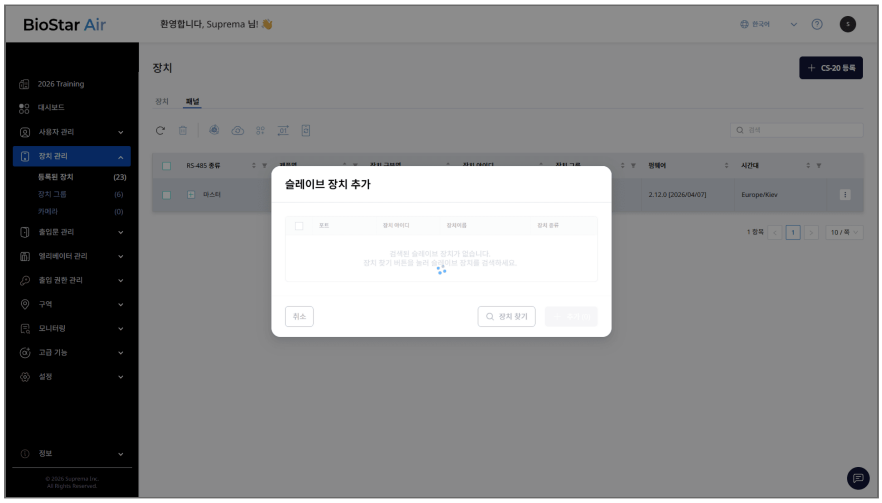
슬레이브 장치 구성

RS-485 통신을 지원하는 장치를 CS-20에 연결하여 슬레이브 장치로 구성할 수 있습니다. 슬레이브 장치는 패널 목록에서 CS-20 아래에 계층적으로 표시됩니다.

1. 패널 목록에서 등록된 CS-20 패널의 가장 오른쪽에 있는 ⋮ 버튼을 클릭하세요.



2. 팝업 메뉴에서 **슬레이브 장치 추가**를 클릭하면 **슬레이브 장치 추가** 창이 나타납니다.



> 검색된 슬레이브 장치가 없으면 **장치 찾기** 버튼을 클릭해 CS-20과 연결된 장치를 다시 검색할 수 있습니다.

3. 연결된 슬레이브 장치가 목록에 표시되면, 각 장치 옆의 체크박스를 클릭해 추가할 장치를 선택하세요.
4. 선택을 완료하면 **추가** 버튼을 클릭하세요.

연결된 슬레이브 장치가 CS-20 아래에 계층적으로 표시됩니다. 이제 패널 목록에서 CS-20과 연결된 모든 장치를 한눈에 확인할 수 있습니다.



> **팁**
> 최상의 성능과 신뢰성을 유지하고 최신 기능을 사용하려면 장치를 등록하자마자 펌웨어 업그레이드를 반드시 확인하세요. 장치가 포장된 시점과 설치된 시점 사이에 새 펌웨어가 배포되었을 수 있습니다. 펌웨어 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

알아두기

- 슬레이브 장치의 정보 수정 및 관리 방법에 대한 자세한 내용은 등록된 엣지 장치 관리하기를 참고하세요.
- 슬레이브 장치 정보 및 설정 옵션에 대한 자세한 내용은 장치 및 패널 설정 옵션 안내를 참고하세요.
- XPass D2 장치 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

OSDP 장치 구성

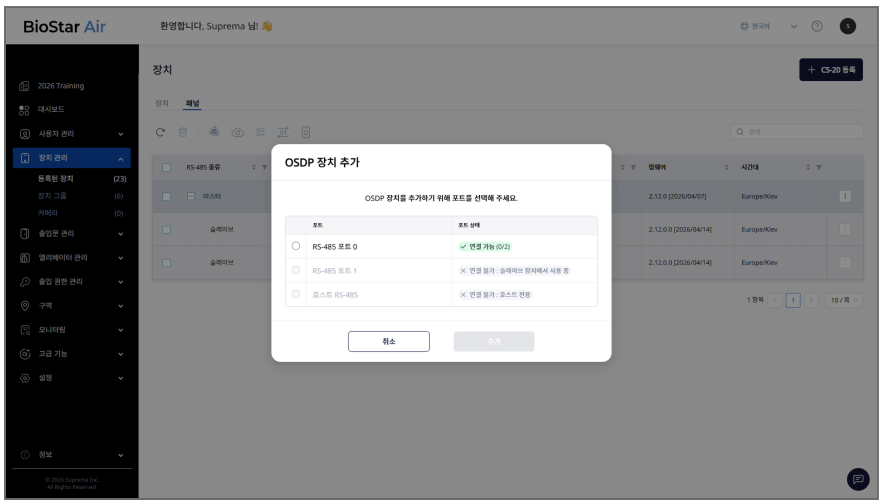
OSDP(Open Supervised Device Protocol)는 보안이 강화된 통신 프로토콜입니다. 높은 보안이 필요한 환경에서 OSDP 호환 장치를 CS-20에 연결하세요.

1. 패널 목록에서 등록된 CS-20 패널의 가장 오른쪽에 있는 ⋮ 버튼을 클릭하세요.



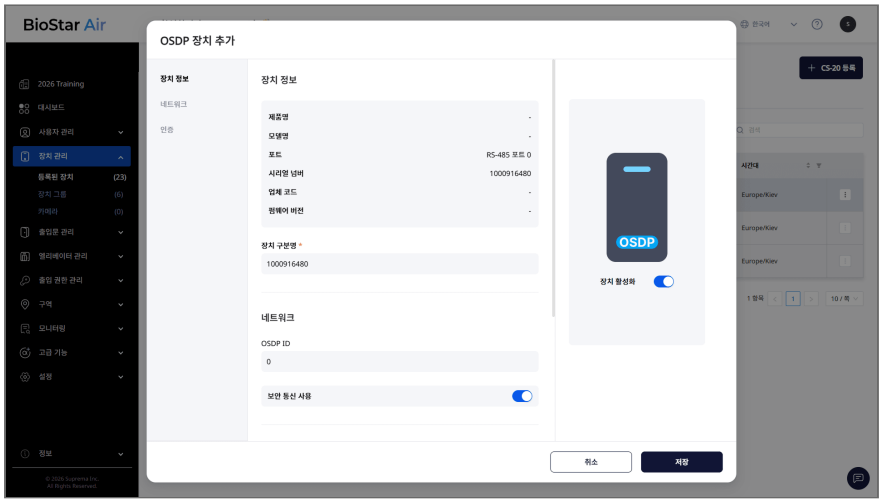
2. 팝업 메뉴에서 **OSDP 장치 추가**를 클릭하세요.

3. **OSDP 장치 추가** 창이 나타나면 장치를 추가하기 위한 포트를 선택하세요.



4. 포트를 선택한 후 **추가** 버튼을 클릭하세요.

5. **OSDP 장치 추가** 창에서 필요한 설정을 완료한 후 **저장** 버튼을 클릭하세요.



Wiegand 장치 구성

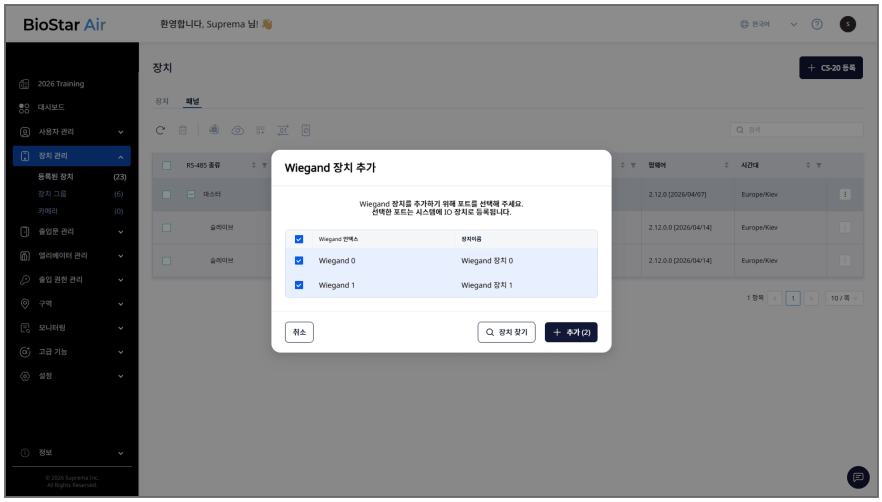
Wiegand는 출입 제어 시스템에서 널리 사용되는 통신 프로토콜입니다. CS-20에 Wiegand 장치를 연결하여 Wiegand 슬레이브 장치로 구성할 수 있습니다.

1. 패널 목록에서 등록된 CS-20 패널의 가장 오른쪽에 있는 ⋮ 버튼을 클릭하세요.



2. 팝업 메뉴에서 **Wiegand 장치 추가**를 클릭하세요.

3. **Wiegand 장치 추가** 창이 나타나면 장치를 추가하기 위한 포트를 선택하세요.



4. 포트를 선택한 후 **추가** 버튼을 클릭하세요.

OSDP/Wiegand 장치 정보 수정

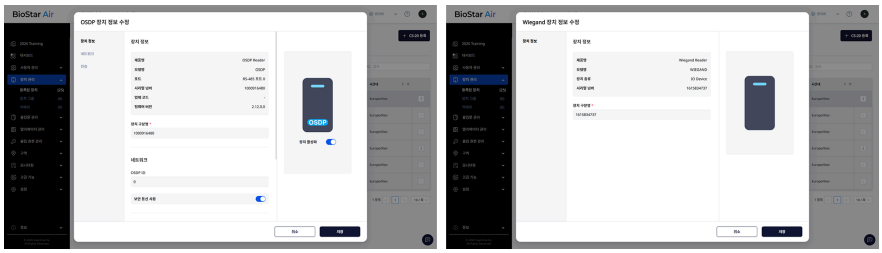
1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.

2. **패널** 탭을 클릭하세요.

3. 목록에서 마스터 장치의 + 아이콘을 클릭해 연결된 보조 장치 목록을 확장하세요.

4. 정보를 수정할 OSDP 또는 Wiegand 보조 장치를 클릭하세요.

5. 장치 정보 수정 창이 나타나면 세부 정보 또는 설정을 수정하세요.



- OSDP 장치: 장치 이름, 네트워크 설정, 인증 설정(RF 카드, RF 카드 + PIN), 인증 대기 시간을 설정할 수 있습니다.
- Wiegand 장치: 장치 이름을 수정할 수 있습니다.

6. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

보조 장치 삭제

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.
3. 목록에서 마스터 장치의 + 아이콘을 클릭해 연결된 보조 장치 목록을 확장하세요.
4. 삭제하려는 보조 장치의 체크박스를 클릭하세요.
5. 목록 상단의 🗑 버튼을 클릭하세요.



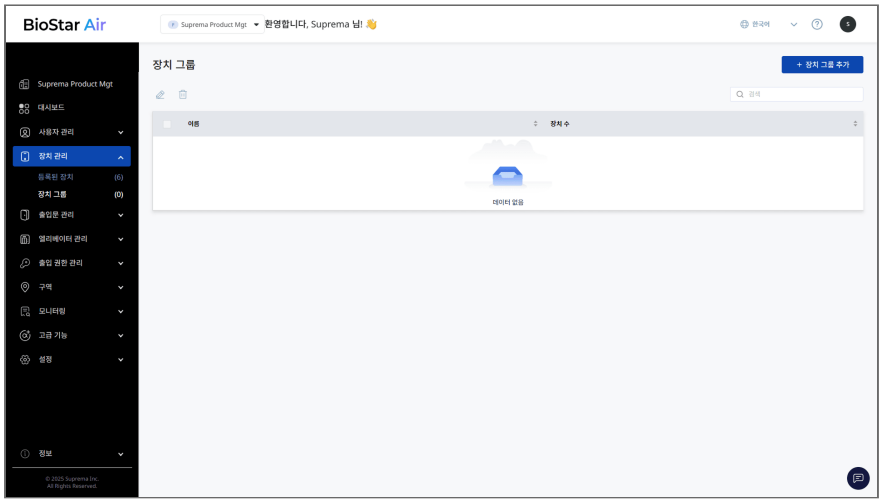
6. 팝업 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

장치 및 패널 그룹 관리하기

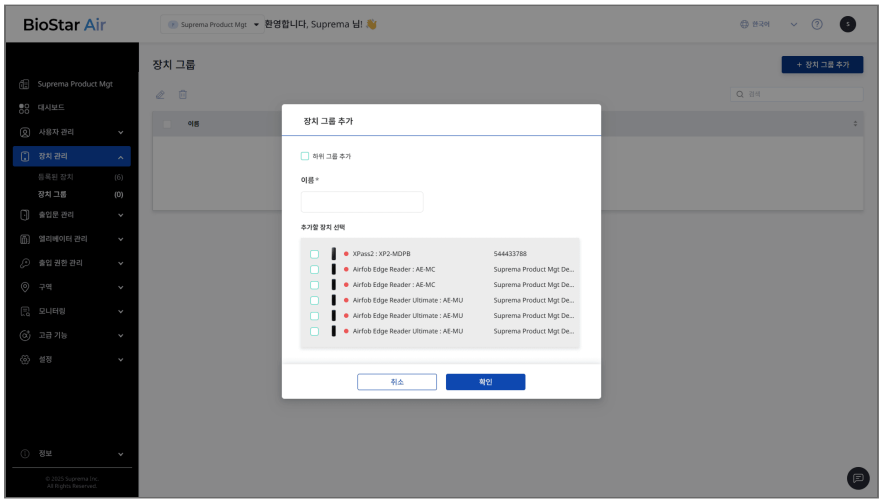
BioStar Air에서는 여러 장치 및 패널을 그룹으로 묶어 효율적으로 관리할 수 있습니다. 장치 그룹을 사용하면 동일한 설정을 여러 장치에 일괄 적용하거나, 특정 그룹의 장치 상태를 쉽게 모니터링할 수 있습니다.

장치 그룹 추가

1. 화면 왼쪽 사이드바에서 **장치 관리** → **장치 그룹**을 클릭하세요.



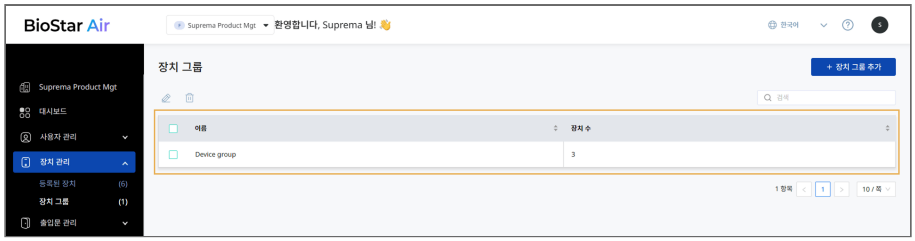
2. 화면 오른쪽 상단의 **장치 그룹 추가** 버튼을 클릭하세요.
3. **장치 그룹 추가** 창이 나타나면 그룹 이름을 입력하세요.



> 특정 그룹의 하위 그룹으로 장치 그룹을 추가하려면 **하위 그룹 추가** 옵션을 클릭하고, 상위 그룹을 선택하세요.

4. **추가할 장치 선택**에서 그룹에 포함할 장치를 선택하세요.
5. 장치를 모두 선택했다면 **확인** 버튼을 클릭하세요.

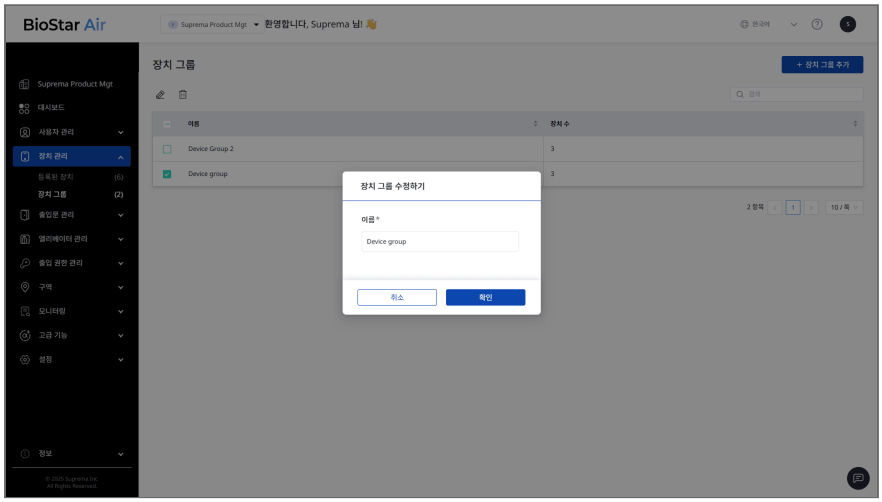
장치 그룹 목록에서 새로 추가된 그룹과 해당 그룹에 속한 장치의 개수를 확인할 수 있습니다. 장치 그룹을 클릭하면 해당 그룹에 속한 장치를 확인할 수 있습니다.



> **알아두기**
>
> 장치를 그룹에 추가하거나, 기존 그룹에서 제거하는 방법에 대한 자세한 내용은 등록된 엣지 장치 관리하기를 참고하세요.

장치 그룹 이름 변경

1. 화면 왼쪽 사이드바에서 **장치 관리** → **장치 그룹**을 클릭하세요.
2. 장치 그룹 목록에서 이름을 변경하려는 장치 그룹의 체크박스를 클릭하세요.
3. 장치 그룹 목록 상단의 버튼을 클릭하세요.
4. **장치 그룹 수정하기** 창이 나타나면 새 그룹 이름을 입력하세요.



5. 변경한 그룹 이름을 저장하려면 **확인** 버튼을 클릭하세요.

장치 그룹 삭제

1. 화면 왼쪽 사이드바에서 **장치 관리** → **장치 그룹**을 클릭하세요.
2. 장치 그룹 목록에서 삭제하려는 장치 그룹의 체크박스를 클릭하세요.
3. 장치 그룹 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

장치 그룹 목록에서 선택한 장치 그룹이 삭제됩니다. 해당 그룹의 하위 그룹까지 모두 삭제됩니다. 그룹을 삭제하더라도 장치는 삭제되지 않습니다.

엣지 장치를 마스터 장치로 사용하기

엣지 장치를 마스터 장치로 설정하여 XPass D2를 보조 장치로 연결할 수 있습니다. 이를 통해 모든 출입 통제 로직은 엣지 장치에서 관리할 수 있습니다. 출입문에 두 개의 네트워크 연결 필요 없이 입구 및 출구 장치가 있는 출입문의 구성이 가능해집니다.

이 문서에서는 XPass 2 장치를 마스터 장치로 설정하고, XPass D2를 보조 장치로 연결하는 방법을 단계별로 안내합니다. 또한, 마스터-보조 장치 구성에서 지원되는 기능과 제한 사항에 대해서도 설명합니다.

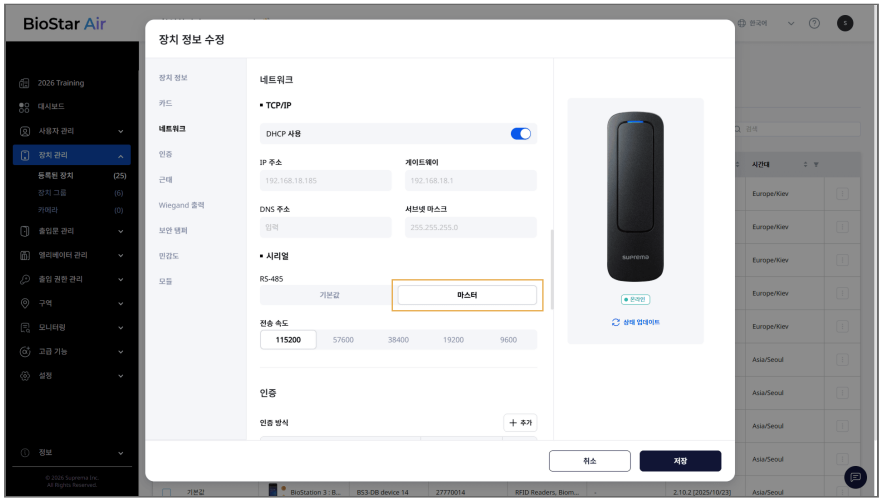
시작하기 전에

XPass 2를 마스터 장치로 설정하기 전에 펌웨어 버전을 **2.12** 이상으로 업데이트해야 합니다. 펌웨어 업데이트에 대한 자세한 내용은 펌웨어 업그레이드를 참고하세요.

XPass 2를 마스터 장치로 변경

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록에서 XPass 2를 클릭하세요.

3. **장치 정보 수정** 창이 나타나면 **네트워크** 섹션으로 이동하세요.
4. **RS-485** 설정을 **마스터**로 변경하세요.



5. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

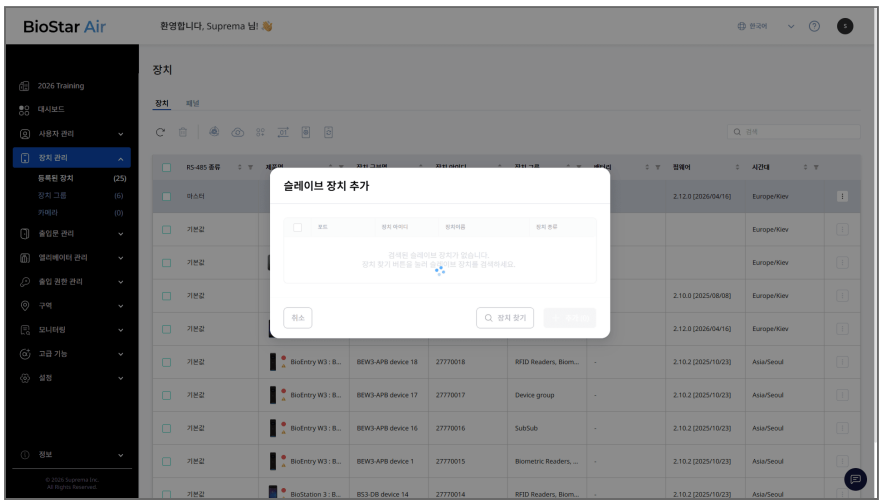
보조 장치 추가

XPass D2 또는 Secure I/O 2(SIO2)과 같은 보조 장치를 추가할 수 있습니다.

1. 장치 목록에서 마스터 장치로 설정한 XPass 2의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



2. 팝업 메뉴에서 **슬레이브 장치 추가**를 클릭하면 **슬레이브 장치 추가** 창이 나타납니다.



> 검색된 슬레이브 장치가 없으면 **장치 찾기** 버튼을 클릭해 XPass 2와 연결된 장치를 다시 검색할 수 있습니다.

3. 연결된 슬레이브 장치가 목록에 표시되면, 장치 옆의 체크박스를 클릭해 추가할 장치를 선택하세요.
4. 선택을 완료하면 **추가** 버튼을 클릭하세요.

연결된 슬레이브 장치가 XPass 2 아래에 계층적으로 표시됩니다. 이제 패널 목록에서 XPass 2와 연결된 모든 장치를 한눈에 확인할 수 있습니다.

> **알아두기**
>
> - XPass D2 장치에 대한 자세한 내용은 XPass D2 설치 가이드를 참고하세요.
> - 마스터 장치로 설정된 XPass 2는 최대 31개의 보조 장치를 할당할 수 있습니다.
> - Secure I/O 2(SIO2) 장치에 대한 자세한 내용은 Secure I/O 2 설치 가이드를 참고하세요.

장치 및 패널 설정 옵션 안내

이 문서는 BioStar Air의 장치 및 패널 설정에 대한 참조 자료입니다. 관리자는 기본 하드웨어 정보 확인, 펌웨어 업데이트, 재부팅 또는 재설정과 같은 작업을 실행할 수 있습니다. 네트워크, 인증, 카드 형식, 근태 관리, Wiegand 출력, 민감도 및 모듈 연결과 같은 동작 설정을 구성할 수 있습니다. 장치 모델 및 패널에 따라 사용 가능한 설정은 다를 수 있습니다.

▼ AirFob Edge

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를

삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **핸즈프리**: BLE 범위를 확장할 수 있습니다.
- **QR 리더**: 장치에 RS-485 QR 리더기가 연결되었음을 확인할 수 있습니다.

  - QR 리더기를 해당 장치와 연결하여 사용할 때, 다른 RS-485 장치를 사용할 수 없습니다.
  - SIO2를 사용할 때, 해당 출입문에 연결된 장치에서 QR 리더기를 사용할 수 없습니다.

- **NFC/RF 카드**: 카드 인증을 활성화하거나 비활성화할 수 있습니다. DESFire, Felica 카드 형식을 지원합니다.
- **Beep 설정**: 출입 인증 성공 알림음을 설정할 수 있습니다.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand 카드**에서 원하는 카드 형식을 선택하세요.

알아두기

- 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
- Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.
- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.
  - **모바일**: 모바일 크리덴셜을 제시할 때 슈프리마 패스 앱에서 근태 이벤트를 선택할 수 있습니다.

> **알아두기**
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

Wiegand 출력

외부 시스템(예, 경보 패널)과의 통합을 위한 기능입니다. 이 기능을 사용하려면 **Wiegand 출력 사용** 옵션을 활성화하세요.

- **출력 모드**: Wiegand 신호 출력 모드를 설정하세요.
  - **일반**: 설정된 Wiegand 형식으로 카드를 스캔합니다.
    - **오류 코드 사용**: 오류 코드를 설정할 수 있으며 Wiegand를 사용하는 카드 인증을 실패했을 때 전송할 값을 선택할 수 있습니다.
  - **항시 통과**: Wiegand 인증과 관계없이 CSN을 전송합니다. 출입문 제어 기능이 없는 장치로 사용할 때 설정하세요.
- **출력 정보**: 인증 시 장치에 출력되는 정보를 선택하세요.
- **펄스 폭**: Wiegand 신호의 펄스 폭을 설정하세요.
- **펄스 간격**: Wiegand 신호의 펄스 간격을 설정하세요.
- **모바일 연속 태그**: 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있습니다.
- **연속 태그 가능 횟수**: 모바일 카드를 연속으로 태그할 수 있는 최대 횟수를 설정할 수 있습니다.

> **알아두기**
> **모바일 연속 태그** 기능은 슈프리마 패스 앱 2.9.0 버전 이상에서 지원합니다.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.

- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

모듈

장치에 연결된 OM-120 모듈을 감지하기 위한 옵션입니다. **추가** 버튼을 클릭해 모듈을 감지할 수 있습니다.

▼ XPass 2

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **사용자 RF 카드 번호**: RF 카드 번호를 키패드로 입력해 사용할 수 있습니다.

> 이 기능은 키패드를 지원하는 **XP2-GKDPB** 모델에서만 지원합니다.

- **핸즈프리**: BLE 범위를 확장할 수 있습니다.
- **QR 리더**: 장치에 RS-485 QR 리더기가 연결되었음을 확인할 수 있습니다.

> – QR 리더기를 해당 장치와 연결하여 사용할 때, 다른 RS-485 장치를 사용할 수 없습니다.
> – SIO2를 사용할 때, 해당 출입문에 연결된 장치에서 QR 리더기를 사용할 수 없습니다.

- **Beep 설정**: 출입 인증 성공 알림음을 설정할 수 있습니다.
- **비디오 서비스**: 장치와 연결된 IP 카메라를 연결해 실시간 영상 및 녹화된 영상을 확인할 수 있습니다. IP 카메라 연결 설정에 대한 자세한 내용은 IP 카메라 지원 및 설정하기를 참고하세요.

카드

카드 섹션에서는 카드 인증과 관련된 설정을 수정할 수 있습니다.

NFC/RF 카드

- **NFC/RF 카드**: 토글 스위치를 클릭해 카드 출입 인증을 켜거나 끌 수 있습니다. 카드 인증을 지원하는 카드 종류를 선택하세요.
  – **EM4100 (125 KHz)**
  – **Mifare Classic/Mifare DESFire/FeliCa**
- **바이트 순서**
  – **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  – **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- **데이터 읽기 방식**: CSN(기본값) 또는 Wiegand 형식을 선택할 수 있습니다.

> Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand 카드**에서 원하는 카드 형식을 선택하세요.

알아두기

- 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
- Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**
- **RS-485**: 장치를 마스터 모드로 설정하여 XPass D2 장치를 보조 장치로 추가할 수 있습니다.
- **전송 속도**: 장치와 보조 장치 간의 직렬 통신 속도를 설정할 수 있습니다.

인증

- **인증 방식**: 인증 방식을 추가할 수 있습니다. **추가** 버튼을 클릭해 인증 방식을 추가하세요.
  - **XP2-MDPB / XP2-GDPB**: 인증 방식으로 RF 카드만 선택할 수 있습니다.
  - **XP2-GKDPB**: 인증 방식으로 RF 카드와 PIN을 조합하여 선택할 수 있습니다.
- **인증 대기 시간**: 설정한 시간 내에 크리덴셜을 인증하지 않으면 인증에 실패합니다.

> 이 기능은 **XP2-GKDPB** 모델에서만 지원합니다.

알아두기

선택한 스케줄에 따라 인증 방식을 다르게 설정할 수 있습니다. 예를 들어, 근무 시간에는 카드 인증만 허용하고 비근무 시간에는 카드와 PIN 조합을 허용할 수 있습니다.

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.

- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.
  - **모바일**: 모바일 크리덴셜을 제시할 때 슈프리마 패스 앱에서 근태 이벤트를 선택할 수 있습니다.

> **알아두기**
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

Wiegand 출력

외부 시스템(예, 경보 패널)과의 통합을 위한 기능입니다. 이 기능을 사용하려면 **Wiegand 출력 사용** 옵션을 활성화하세요.

- **출력 모드**: Wiegand 신호 출력 모드를 설정하세요.
  - **일반**: 설정된 Wiegand 형식으로 카드를 스캔합니다.
    - **오류 코드 사용**: 오류 코드를 설정할 수 있으며 Wiegand를 사용하는 카드 인증을 실패했을 때 전송할 값을 선택할 수 있습니다.
  - **항시 통과**: Wiegand 인증과 관계없이 CSN을 전송합니다. 출입문 제어 기능이 없는 장치로 사용할 때 설정하세요.
- **출력 정보**: 인증 시 장치에 출력되는 정보를 선택하세요.
- **펄스 폭**: Wiegand 신호의 펄스 폭을 설정하세요.
- **펄스 간격**: Wiegand 신호의 펄스 간격을 설정하세요.
- **모바일 연속 태그**: 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있습니다.
- **연속 태그 가능 횟수**: 모바일 카드를 연속으로 태그할 수 있는 최대 횟수를 설정할 수 있습니다.

> **알아두기**
> **모바일 연속 태그** 기능은 슈프리마 패스 앱 2.9.0 버전 이상에서 지원합니다.

보안 탬퍼

장치에서 탬퍼 이벤트가 발생할 경우 장치에 저장된 **전체 사용자 정보**, **전체 로그**, **보안 키**를 삭제하도록 설정할 수 있습니다.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.
- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

모듈

장치에 연결된 OM-120 모듈을 감지하기 위한 옵션입니다. **추가** 버튼을 클릭해 모듈을 감지할 수 있습니다.

▼ XPass D2

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **핸즈프리**: BLE 범위를 확장할 수 있습니다.
- **Beep 설정**: 출입 인증 성공 알림음을 설정할 수 있습니다.

카드

카드 섹션에서는 카드 인증과 관련된 설정을 수정할 수 있습니다.

NFC/RF 카드

- **NFC/RF 카드**: 토글 스위치를 클릭해 카드 출입 인증을 켜거나 끌 수 있습니다. 카드 인증을 지원하는 카드 종류를 선택하세요.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **바이트 순서**
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- **데이터 읽기 방식**: CSN(기본값) 또는 Wiegand 형식을 선택할 수 있습니다.

> Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand 카드**에서 원하는 카드 형식을 선택하세요.

> **알아두기**
>
> - 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
> - Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

인증

- **인증 방식**: 인증 방식을 추가할 수 있습니다. **추가** 버튼을 클릭해 인증 방식을 추가하세요. 인증 방식으로 RF 카드만 선택할 수 있습니다.

> **알아두기**
> 선택한 스케줄에 따라 인증 방식을 다르게 설정할 수 있습니다. 예를 들어, 근무 시간에는 카드 인증만 허용하고 비근무 시간에는 카드와 PIN 조합을 허용할 수 있습니다.

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.
- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.

> **알아두기**
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.
- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

▼ X-Station 2

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **핸즈프리**: BLE 범위를 확장할 수 있습니다.
- **QR 리더**: 장치에 RS-485 QR 리더기가 연결되었음을 확인할 수 있습니다.

> – QR 리더기를 해당 장치와 연결하여 사용할 때, 다른 RS-485 장치를 사용할 수 없습니다.
> – SIO2를 사용할 때, 해당 출입문에 연결된 장치에서 QR 리더기를 사용할 수 없습니다.

- **NFC/RF 카드**: 카드 인증을 활성화하거나 비활성화할 수 있습니다. DESFire, Felica 카드 형식을 지원합니다.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand 카드**에서 원하는 카드 형식을 선택하세요.

> **알아두기**
>
> - 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
> - Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.
- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.
  - **모바일**: 모바일 크리덴셜을 제시할 때 슈프리마 패스 앱에서 근태 이벤트를 선택할 수 있습니다.

> **알아두기**
>
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.
- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

모듈

장치에 연결된 OM-120 모듈을 감지하기 위한 옵션입니다. **추가** 버튼을 클릭해 모듈을 감지할 수 있습니다.

▼ BioEntry W3

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **핸즈프리**: BLE 범위를 확장할 수 있습니다.

카드

카드 섹션에서는 카드 인증과 관련된 설정을 수정할 수 있습니다.

NFC/RF 카드

- **NFC/RF 카드**: 토글 스위치를 클릭해 카드 출입 인증을 켜거나 끌 수 있습니다. 카드 인증을 지원하는 카드 종류를 선택하세요.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **바이트 순서**
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- **데이터 읽기 방식**: CSN(기본값) 또는 Wiegand 형식을 선택할 수 있습니다.

> Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand 카드**에서 원하는 카드 형식을 선택하세요.

> **알아두기**
>
> - 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
> - Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**

인증

- **인증 방식**: 인증 방식을 추가할 수 있습니다. **추가** 버튼을 클릭해 인증 방식을 추가하세요. 인증 방식으로 RF 카드와 얼굴을 조합하여 선택할 수 있습니다.

> **알아두기**
> 선택한 스케줄에 따라 인증 방식을 다르게 설정할 수 있습니다. 예를 들어, 근무 시간에는 카드 인증만 허용하고 비근무 시간에는 카드와 PIN 조합을 허용할 수 있습니다.

얼굴

보안

- **위조 얼굴 검출**: 사진 등의 위조 얼굴을 이용한 사용자 인증을 방지할 수 있습니다.
- **중복 검사**: 얼굴을 등록할 때 중복 등록 여부를 검사할 수 있습니다.

인식

- **모션 센서 감도**: 장치 주변의 움직임을 감지하는 감도를 설정하세요.
- **최대 얼굴 회전 각도**: 허용 가능한 얼굴의 최대 회전 각도를 설정하세요.
- **얼굴 인식 영역 넓히기**: 카메라 영상 전체에서 얼굴을 인식하는 범위를 넓힐 수 있습니다.
- **얼굴 인식 거리 (cm)**: 얼굴을 인식하는 최소, 최대 거리를 설정하세요.
- **등록 대기 시간 (초)**: 사용자 얼굴을 등록할 때 설정한 시간 동안 얼굴을 등록하지 못하면 얼굴 등록이 취소됩니다.

마스크 검출 사용

마스크 검출 기능을 설정하려면 **마스크 검출 사용** 옵션을 활성화하세요.

- **마스크 검출 레벨**: 마스크 검출 민감도를 선택하세요.
- **마스크 검출 실패 시**
  - **인증 거부**: 마스크를 착용하지 않은 사용자는 인증 거부되며 마스크 미착용 이벤트 로그를 기록합니다.
  - **로그 기록 후 인증 허용**: 마스크를 착용하지 않은 사용자도 인증할 수 있으나 마스크 미착용 이벤트 로그를 기록합니다.

- **마스크 확인**
  - **인증 후**: 인증을 수행한 뒤 사용자의 마스크 착용 여부를 확인하거나 온도를 측정합니다.
  - **인증 전**: 사용자의 마스크 착용 여부를 확인하거나 온도를 측정한 뒤 인증을 수행합니다. 이 경우 마스크를 착용하지 않거나 기준 온도를 초과하는 사용자는 인증을 수행할 수 없습니다.
  - **인증 없이**: 장치를 마스크 착용 여부를 확인하거나 온도를 측정하는 용도로만 사용할 수 있습니다. 이 경우 인증과 관계없이 마스크를 착용하거나 기준 온도 이하인 사용자는 모두 출입할 수 있습니다.
- **장치 카메라에 QR 및 바코드 인증하기**: 장치의 카메라를 통한 QR/바코드 인증 사용 여부를 설정할 수 있습니다.
- **QR로 카드 번호 인증하기**: 인증된 사용자에게 발급한 CSN 카드 또는 Wiegand 카드와 동일한 데이터의 QR코드로 인증할 수 있도록 설정할 수 있습니다. 이 기능은 **장치 카메라에 QR 및 바코드 인증하기** 옵션을 활성화해야 사용할 수 있습니다.

> **알아두기**
> 얼굴이 아닌 크리덴셜을 사용할 때는 주로 '이전'과 '이후'가 중요합니다.

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.
- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.

> **알아두기**
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

Wiegand 출력

외부 시스템(예, 경보 패널)과의 통합을 위한 기능입니다. 이 기능을 사용하려면 **Wiegand 출력 사용** 옵션을 활성화하세요.

- **출력 모드**: Wiegand 신호 출력 모드를 설정하세요.
  - **일반**: 설정된 Wiegand 형식으로 카드를 스캔합니다.
    - **오류 코드 사용**: 오류 코드를 설정할 수 있으며 Wiegand를 사용하는 카드 인증을 실패했을 때 전송할 값을 선택할 수 있습니다.
  - **항시 통과**: Wiegand 인증과 관계없이 CSN을 전송합니다. 출입문 제어 기능이 없는 장치로 사용할 때 설정하세요.
- **출력 정보**: 인증 시 장치에 출력되는 정보를 선택하세요.
- **펄스 폭**: Wiegand 신호의 펄스 폭을 설정하세요.
- **펄스 간격**: Wiegand 신호의 펄스 간격을 설정하세요.
- **모바일 연속 태그**: 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있습니다.
- **연속 태그 가능 횟수**: 모바일 카드를 연속으로 태그할 수 있는 최대 횟수를 설정할 수 있습니다.

> **알아두기**
> **모바일 연속 태그** 기능은 슈프리마 패스 앱 2.9.0 버전 이상에서 지원합니다.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.
- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

▼ BioStation 3

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.
- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **핸즈프리**: BLE 범위를 확장할 수 있습니다.
- **비디오 서비스**: 장치와 연결된 IP 카메라를 연결해 실시간 영상 및 녹화된 영상을 확인할 수 있습니다. IP 카메라 연결 설정에 대한 자세한 내용은 IP 카메라 지원 및 설정하기를 참고하세요.

카드

카드 섹션에서는 카드 인증과 관련된 설정을 수정할 수 있습니다.

NFC/RF 카드

- **NFC/RF 카드**: 토글 스위치를 클릭해 카드 출입 인증을 켜거나 끌 수 있습니다. 카드 인증을 지원하는 카드 종류를 선택하세요.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **바이트 순서**
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- **데이터 읽기 방식**: CSN(기본값) 또는 Wiegand 형식을 선택할 수 있습니다.

> Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

Wiegand 카드

Wiegand 카드로 **iClass (SE / SEOS)** 및 **HID Prox** 카드로 선택할 수 있습니다. 토글 버튼을 선택해 기능을 활성화한 후 **Wiegand**

카드에서 원하는 카드 형식을 선택하세요.

> **알아두기**
>
> - 이 기능은 장치에 따라 지원하지 않을 수 있습니다.
> - Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**

인증

- **인증 방식**: 인증 방식을 추가할 수 있습니다. **추가** 버튼을 클릭해 인증 방식을 추가하세요. 인증 방식으로 RF 카드와 얼굴, ID, PIN을 조합하여 선택할 수 있습니다.
- **사용자 이름 표시** / **사용자 ID 표시**: 사용자 이름 또는 아이디를 인증 화면에 표시할지 여부를 선택할 수 있습니다. 화면에 표시하지 않도록 설정하려면 **표시 안함** 옵션을 선택하세요.
- **인증 대기 시간**: 설정한 시간 내에 크리덴셜을 인증하지 않으면 인증에 실패합니다.

> **알아두기**
>
> 선택한 스케줄에 따라 인증 방식을 다르게 설정할 수 있습니다. 예를 들어, 근무 시간에는 카드 인증만 허용하고 비근무 시간에는 카드와 PIN 조합을 허용할 수 있습니다.

얼굴

보안

- **위조 얼굴 검출**: 사진 등의 위조 얼굴을 이용한 사용자 인증을 방지할 수 있습니다.
- **중복 검사**: 얼굴을 등록할 때 중복 등록 여부를 검사할 수 있습니다.

인식

- **모션 센서 감도**: 장치 주변의 움직임을 감지하는 감도를 설정하세요.
- **최대 얼굴 회전 각도**: 허용 가능한 얼굴의 최대 회전 각도를 설정하세요.
- **얼굴 인식 영역 넓히기**: 카메라 영상 전체에서 얼굴을 인식하는 범위를 넓힐 수 있습니다.
- **얼굴 인식 거리 (cm)**: 얼굴을 인식하는 최소, 최대 거리를 설정하세요.
- **등록 대기 시간 (초)**: 사용자 얼굴을 등록할 때 설정한 시간 동안 얼굴을 등록하지 못하면 얼굴 등록이 취소됩니다.

마스크 검출 사용

마스크 검출 기능을 설정하려면 **마스크 검출 사용** 옵션을 활성화하세요.

- **마스크 검출 레벨**: 마스크 검출 민감도를 선택하세요.
- **마스크 검출 실패 시**
  - **인증 거부**: 마스크를 착용하지 않은 사용자는 인증 거부되며 마스크 미착용 이벤트 로그를 기록합니다.
  - **로그 기록 후 인증 허용**: 마스크를 착용하지 않은 사용자도 인증할 수 있으나 마스크 미착용 이벤트 로그를 기록합니다.
- **마스크 확인**
  - **인증 후**: 인증을 수행한 뒤 사용자의 마스크 착용 여부를 확인하거나 온도를 측정합니다.
  - **인증 전**: 사용자의 마스크 착용 여부를 확인하거나 온도를 측정한 뒤 인증을 수행합니다. 이 경우 마스크를 착용하지 않거나 기준 온도를 초과하는 사용자는 인증을 수행할 수 없습니다.
  - **인증 없이**: 장치를 마스크 착용 여부를 확인하거나 온도를 측정하는 용도로만 사용할 수 있습니다. 이 경우 인증과 관계없이 마스크를 착용하거나 기준 온도 이하인 사용자는 모두 출입할 수 있습니다.
- **장치 카메라에 QR 및 바코드 인증하기**: 장치의 카메라를 통한 QR/바코드 인증 사용 여부를 설정할 수 있습니다.
- **QR로 카드 번호 인증하기**: 인증된 사용자에게 발급한 CSN 카드 또는 Wiegand 카드와 동일한 데이터의 QR코드로 인증할 수 있도록 설정할 수 있습니다. 이 기능은 **장치 카메라에 QR 및 바코드 인증하기** 옵션을 활성화해야 사용할 수 있습니다.

> **알아두기**
> 얼굴이 아닌 크리덴셜을 사용할 때는 주로 '이전'과 '이후'가 중요합니다.

근태(Time & Attendance, T&A)

이 기능을 활성화하면 **근태 이벤트**가 **이벤트 로그**에 기록되고 **근태 리포트**에 사용됩니다.

- **근태 사용**: 토글 스위치를 클릭해 근태 관리 기능을 켜거나 끌 수 있습니다.
- **근태 모드**: 원하는 근태 모드를 선택하세요.
  - **수동 변경**: 화면에 근태 키 표시해 인증 시, 사용자가 근태 이벤트를 선택할 수 있습니다.

    > **근태 필수 선택** 옵션을 활성화하면 사용자가 인증할 때 반드시 근태 이벤트를 등록해야 합니다.

  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에서 적용할 스케줄을 선택할 수 있습니다.
  - **수동 고정**: 사용자가 마지막으로 사용한 근태 이벤트를 계속 사용할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다.

> **알아두기**
> 근태 관리 구성에 대한 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.

화면 및 소리

화면

- **화면보호기 사용**: 장치를 사용하지 않을 때 LCD 화면 밝기를 줄여 불필요한 전력 소모를 줄일 수 있습니다.
- **백라이트 항상 켜기**: 화면의 조명을 항상 켜두거나 비활성화 후 어두워지도록 설정할 수 있습니다.
- **백라이트 시간**: 화면 조명이 자동으로 꺼지는 시간을 설정할 수 있습니다.
- **언어**: 장치의 화면에 표시할 언어를 설정할 수 있습니다.
- **홈 화면**: 장치의 홈 화면 배경에 표시할 항목을 설정하세요.
  - **일반**: 기본 이미지를 홈 화면에 표시합니다.
  - **로고**: 사용자가 등록한 이미지를 장치의 홈 화면에 표시할 수 있습니다.
  - **공지사항**: 관리자가 입력한 내용을 홈 화면에 표시할 수 있습니다.

> **업데이트** 버튼을 클릭하고 저장하면 이미지 또는 공지 사항이 편집 화면에 나타나지 않으나 장치에는 계속 표시됩니다.

소리

- **음성 안내**: 알림음 대신 음성 안내를 사용할 수 있습니다.
- **장치 볼륨**: 장치에서 발생하는 소리 크기를 조절할 수 있습니다.
- **IP 인터폰 스피커 볼륨** / **IP 인터폰 마이크 볼륨**: IP 인터폰 기능을 사용할 때 장치에서 출력 또는 입력되는 소리 크기를 조절할 수 있습니다.

Wiegand 출력

외부 시스템(예, 경보 패널)과의 통합을 위한 기능입니다. 이 기능을 사용하려면 **Wiegand 출력 사용** 옵션을 활성화하세요.

- **출력 모드**: Wiegand 신호 출력 모드를 설정하세요.
  - **일반**: 설정된 Wiegand 형식으로 카드를 스캔합니다.
    - **오류 코드 사용**: 오류 코드를 설정할 수 있으며 Wiegand를 사용하는 카드 인증을 실패했을 때 전송할 값을 선택할 수 있습니다.
  - **항시 통과**: Wiegand 인증과 관계없이 CSN을 전송합니다. 출입문 제어 기능이 없는 장치로 사용할 때 설정하세요.
- **출력 정보**: 인증 시 장치에 출력되는 정보를 선택하세요.
- **펄스 폭**: Wiegand 신호의 펄스 폭을 설정하세요.
- **펄스 간격**: Wiegand 신호의 펄스 간격을 설정하세요.
- **모바일 연속 태그**: 대기 시간 없이 연속으로 모바일 카드를 태그할 수 있습니다.
- **연속 태그 가능 횟수**: 모바일 카드를 연속으로 태그할 수 있는 최대 횟수를 설정할 수 있습니다.

> **알아두기**
> **모바일 연속 태그** 기능은 슈프리마 패스 앱 2.9.0 버전 이상에서 지원합니다.

IP 인터폰

- **IP 인터폰 사용**: IP 인터폰 기능을 활성화하거나 비활성화할 수 있습니다.
- **SIP 서버 전송 방식**: IP 인터폰의 SIP 서버 설정 시 SIP 전송 방법을 선택하세요.
- **SIP 서버 주소**: SIP 서버의 주소를 입력하세요.
- **SIP 서버 포트**: SIP 서버의 포트를 입력하세요.
- **등록 유지 시간**: 등록 유지 시간을 입력하세요. 장치는 등록 유지 시간이 끝날 때마다 SIP 서버에 등록을 시도합니다.
- **사용자 이름**: SIP 계정의 사용자 이름을 입력하세요.
- **비밀번호**: SIP 계정의 비밀번호를 입력하세요.
- **인증 ID**: SIP 계정의 인증 아이디를 입력하세요.
- **아웃바운드 프록시 서버**: 별도의 (아웃바운드) 프록시 서버를 통해 SIP 서비스를 사용할 수 있습니다.
- **내선 번호**: 내선 번호를 추가하거나 편집할 수 있습니다.
- **비디오 해상도**: IP 인터폰을 사용할 때 출력되는 영상의 해상도를 선택하세요.
- **문 열기 버튼**: 통화 중 장치의 출입문을 개방할 수 있는 버튼을 지정하세요.

보안 탬퍼

장치에서 탬퍼 이벤트가 발생할 경우 장치에 저장된 **전체 사용자 정보**, **전체 로그**, **보안 키**를 삭제하도록 설정할 수 있습니다.

RTSP

Real Time Streaming Protocol(RTSP) 스트리밍을 위한 세부 항목을 설정할 수 있습니다. 장치의 카메라를 통해 실시간으로 영상을 송출할 수 있습니다.

- **RTSP 사용**: RTSP 스트리밍 기능을 켜거나 끌 수 있습니다.
- **주소**: RTSP 서버 주소입니다.
- **포트**: RTSP 서버 포트를 입력하세요.
- **ID** / **비밀번호**: RTSP 서버의 아이디와 비밀번호를 입력하세요.
- **RTSP 비디오 해상도**: RTSP 사용 시 출력되는 영상의 해상도를 선택하세요.

> **알아두기**
> RTSP 스트리밍 기능은 BioStation 3 장치에서만 지원합니다.

민감도

출입문 잠금을 해제하기 위해 모바일 기기와 장치가 얼마나 가까이 있어야 하는지 RSSI 값을 조정할 수 있습니다.



- 값이 작을수록 의도하지 않은 활성화를 방지합니다.
- 값이 클수록 간섭이 높은 곳에서 감지를 개선합니다.

> **알아두기**
> 설정한 값을 초기화하려면 **초기화** 버튼을 클릭하세요.

▼ CoreStation 20

장치 정보

장치 정보 섹션에서는 장치의 이름, 모델명, 시리얼 번호, 펌웨어 버전과 같은 기본 정보와 기능을 제어하는 액션 메뉴, 기본 설정 옵션을 제공합니다.

기본 정보

장치의 기본 정보를 확인할 수 있습니다. 이 정보는 편집할 수 없습니다.

- **제품명**: 장치의 제품 이름입니다.
- **모델명**: 장치의 모델 이름입니다.
- **시리얼 넘버**: 장치의 시리얼 번호입니다.
- **펌웨어 버전**: 장치에 설치된 펌웨어 버전입니다.

액션 기능

장치의 기능을 제어할 수 있는 **액션**(Action) 기능입니다.



- **펌웨어 업데이트**: 장치의 펌웨어를 최신 버전으로 업데이트할 수 있습니다.
- **재부팅**: 장치에 문제가 있거나 이상이 발생하면 원격으로 재부팅할 수 있습니다.

- **장치 초기화**: 장치에 저장된 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제합니다.
- **장치 초기화 네트워크 설정 유지**: 네트워크 설정을 제외한 모든 설정을 초기화합니다. 이 작업을 수행하면 장치의 모든 설정과 데이터를 삭제하지만, 네트워크 설정은 유지됩니다.

기본 설정

장치의 기본 설정을 수정할 수 있습니다.

- **장치 구분명**: 장치 목록 및 로그에서 표시되는 장치의 별칭입니다. 직접 수정할 수 있습니다.
- **시간대**: 사이트와 장치의 시계가 다를 때 로그를 일관되게 유지할 수 있도록 장치의 시간대를 설정하세요. 일광 절약 시간(Daylight Saving Time, DST)을 적용하려면 **DST 사용** 옵션을 활성화하세요.
- **비디오 서비스**: 패널과 연결된 IP 카메라를 연결해 실시간 영상 및 녹화된 영상을 확인할 수 있습니다. IP 카메라 연결 설정에 대한 자세한 내용은 IP 카메라 지원 및 설정하기를 참고하세요.

카드

카드 섹션에서는 카드 인증과 관련된 설정을 수정할 수 있습니다.

NFC/RF 카드

- **NFC/RF 카드**: 토글 스위치를 클릭해 카드 출입 인증을 켜거나 끌 수 있습니다. 카드 인증을 지원하는 카드 종류를 선택하세요.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **바이트 순서**
  - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
  - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
- **데이터 읽기 방식**: CSN(기본값) 또는 Wiegand 형식을 선택할 수 있습니다.

> Wiegand 형식은 5가지 기본 형식이 포함되어 있습니다. **설정** → **카드 형식**에서 더 많은 형식을 추가할 수 있습니다. 커스텀 카드 형식 설정에 대한 자세한 내용은 커스텀 Wiegand 카드 형식 구성하기를 참고하세요.

네트워크

장치의 네트워크 설정을 수정할 수 있습니다.

- **DHCP 사용**: 장치가 IP 주소를 자동으로 가져오도록 설정할 수 있습니다.

  네트워크 설정을 수동으로 구성하려면 **DHCP 사용** 옵션을 비활성화하고 다음 필드를 입력하세요.
  - **IP 주소**
  - **게이트웨이**
  - **DNS 주소**
  - **서브넷 마스크**
- **SCB 키**: Serial Communication Block(SCB) 보안 키를 입력하세요. 최대 32자까지 입력할 수 있으며, 직렬 통신 보안을 위해 사용합니다.

- **SCB 키 확인**: 보안 키 오류 방지를 위해 동일한 값을 다시 입력하세요.
- **전송 속도**: 패널과 보조 장치 간 직렬 통신 속도를 설정할 수 있습니다.
  - **Host**: 패널의 통신 속도
  - **0** / **1**: 보조 장치가 연결된 각 포트의 통신 속도

> **알아두기**
>
> - OSDP 장치를 추가하기 전에 SCB 키를 설정해야 합니다. 이미 추가된 OSDP 장치가 있다면, SCB 키를 변경할 수 없습니다.
> - 타사 OSDP 장치 제조사가 특정 SCB 키를 사용한다면, CS-20에서 OSDP 장치와 동일한 키를 설정할 수 있습니다.
> - CS-20과 OSDP 장치의 SCB 키가 일치하지 않으면, **Secure Session**을 통해 장치에 연결할 수 없습니다.
> - **전송 속도**는 독립적으로 다른 속도를 설정할 수 있으며, 기본값은 `115200` 입니다.

고급

장치 상태

탬퍼 또는 전원 장애 감지기, 화재 감지기를 AUX IN 단자에 연결했다면 사용 여부를 설정할 수 있습니다.

- **탬퍼**
- **AC Fail**
- **화재**

> **알아두기**
>
> Fail Safe Lock을 사용하려면 **N/C** 릴레이를, Fail Secure Lock을 사용하려면 **N/O** 릴레이를 연결하세요. 릴레이 연결에 대한 자세한 내용은 CoreStation 20 설치 가이드를 참고하세요.

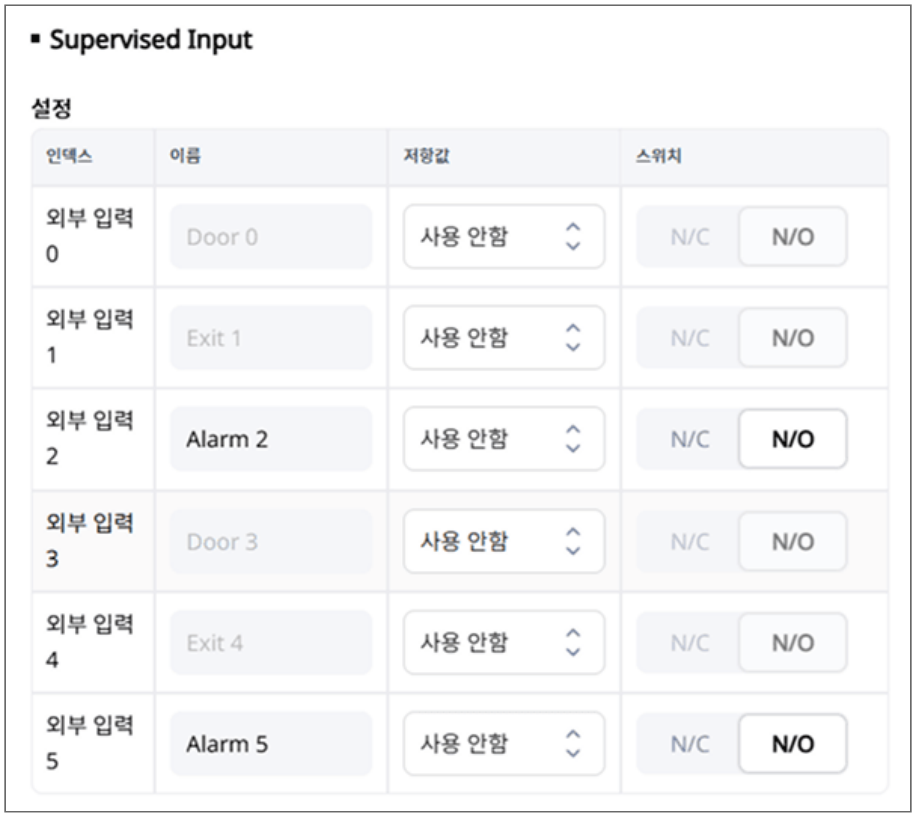
Wiegand 입력

Wiegand 입력 관련 세부 항목을 설정할 수 있습니다.

- **Wiegand 입력 사용**: Wiegand 입력 기능을 활성화하거나 비활성화할 수 있습니다.
- **입력 형식**: Wiegand 입력 형식을 선택하세요.
- **펄스 폭**: Wiegand 신호의 펄스 폭을 설정하세요.
- **펄스 간격**: Wiegand 신호의 펄스 간격을 설정하세요.

Supervised Input

Supervised Input 포트를 Input 포트로 사용하도록 설정할 수 있으며, Supervised Input에 사용할 저항값을 설정할 수 있습니다. 저항값은 1 kΩ, 2.2 kΩ, 4.7 kΩ, 10 kΩ을 설정할 수 있습니다.



보안 탬퍼

패널에서 탬퍼 이벤트가 발생할 경우 패널에 저장된 **전체 사용자 정보, 전체 로그, 보안 키**를 삭제하도록 설정할 수 있습니다.

모듈

패널에 연결된 OM-120 모듈을 감지하기 위한 옵션입니다. **추가** 버튼을 클릭해 모듈을 감지할 수 있습니다.

에어팝 패치와 태그 구성하기

BioStar Air 앱에서 에어팝 패치 등록

시작하기 전에

- 모바일 기기에 BioStar Air 앱이 설치되어 있어야 합니다. 모바일 앱 설치은 다음 링크를 통해 설치할 수 있습니다.
  - iOS
  - Android
- BioStar Air 관리자 포털에서 사용하는 아이디와 비밀번호로 로그인하세요.
- 모바일 기기에서 BLE가 활성화되어 있는지 확인하세요.
- 에어팝 패치를 출입 통제 장치에 영구적으로 또는 임시로 부착하세요. 자세한 내용은 에어팝 패치 설치를 참고하세요.

알아두기

BioStar Air 모바일 앱 사용에 대한 자세한 내용은 BioStar Air 앱 시작하기를 참고하세요.

에어팝 패치 등록

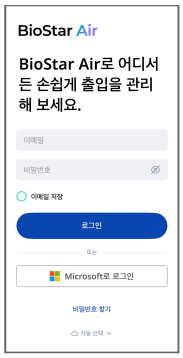
1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. BioStar Air 앱 초기 화면에서 **장치** 카드를 탭하세요.
3. 모바일 기기를 에어팝 패치에 10cm 이내로 가까이 가져가 화면 오른쪽 상단의 ＋ 버튼을 탭하세요.
4. 장치 검색 화면에서 등록하려는 에어팝 패치의 **등록** 버튼을 탭하세요.
5. 장치 등록 창이 나타나면 **확인** 버튼을 탭하세요.

장치 목록으로 돌아가 추가된 에어팝 패치를 확인하세요.

구성 단계

에어팝 패치 또는 태그를 설치하고 BioStar Air 앱에 등록하세요. 다음 단계를 따라 장치를 구성하세요.

1 앱 실행



1. 모바일 기기에서 **BioStar Air** 앱을 실행하세요.
2. 에어팝 패치 또는 태그 장치를 등록한 사이트에 로그인하세요.

2 장치 설정으로 이동



1. **BioStar Air** 앱 초기 화면에서 하단의 **관리**를 탭하세요.
2. 등록된 장치 목록을 확인하려면 **장치**를 탭하세요.
3. 장치 목록에서 에어팝 패치 또는 태그 장치를 선택하세요.

3 BLE 모드 활성화

- 모바일 기기를 장치에 가까이 가져가세요.
- 앱에서 **BLE 모드**를 활성화하세요.

4 카드 ID 출력 방법 설정

- **Card ID Output Method**로 스크롤하여 이동하고 **Edit**를 탭하세요.
- **User Card ID** 옆에 있는 **Select**를 탭하세요.

5 출력 방법 선택

- **None**: 카드 ID를 전송하지 않으려면 이 옵션을 선택하세요. 배터리 수명을 연장하기 위한 근태 관리(T&A) 목적으로 사용할 때 유용합니다.
- **Fixed Device**: 미리 프로그래밍된 고정 카드 ID를 전송합니다. RFID 카드를 개별적으로 프로그래밍해야 하는 도어락이나 인터콤에 유용합니다. 기기 로그에는 이 고정 카드 ID만 표시됩니다.
- **User Card ID**: 각 사용자별로 고유 카드 ID를 전송하며, 출입 통제 시스템의 기존 RFID 카드 번호와 일치합니다. 이를 통해 새로운 실물 카드를 발급하지 않고도 원활하게 통합할 수 있습니다.
- **Direct Input**: 전송할 카드 ID를 수동으로 지정합니다. 여러 장치에서 하나의 ID를 사용해야 하는 사용자 정의 설정에 유용합니다.

6 설정 저장

- 모바일 기기를 장치 근처에 두고 **저장** 버튼을 탭하고 선택 내용을 확인하세요.
- 업데이트 완료 메시지가 나타납니다.

바이오인식 장치와 크리덴셜

BioStar Air는 이제 바이오인식 장치와 바이오메트릭 크리덴셜을 지원하여 안전한 출입 통제를 제공합니다. BioStation 3(이하 BS3) 및 BioEntry W3(이하 W3)와 같은 호환되는 바이오인식 장치를 등록하고 구성하여 얼굴 인식을 통해 사용자를 인증할 수 있습니다. 이 기능은 단일 인증 및 이중 인증을 모두 지원하여 유연성과 보안을 강화합니다.

- **장치 등록**: BioStar Air 모바일 앱을 사용하여 바이오인식 장치를 등록할 수 있습니다.
- **장치 설정**: BioStar Air 포털 → **장치 관리** → **등록된 장치**로 이동해 장치의 얼굴 인증 설정을 구성하세요.
- **사용자 얼굴 크리덴셜 설정**: BioStar Air 포털 → **사용자 관리** → **사용자**로 이동해 사용자를 추가하거나 사용자 정보를 수정하세요. **크리덴셜 정보** 섹션에서 얼굴 크리덴셜을 활성화하세요.

시작하기 전에

- 바이오인식 장치가 정상 작동하려면 BioStar Air 호환 펌웨어가 설치되어 있어야 합니다.
- 얼굴 템플릿은 사용자당 최대 두 개의 템플릿까지 사용할 수 있습니다.
- 고급 구성에 대한 내용은 BioEntry W3 또는 BioStation 3 사용자 가이드를 참고하세요.
- 이중 인증 방식을 사용하려면 크리덴셜을 두 개 이상 등록해야 합니다. 예를 들어, RF 카드와 얼굴 크리덴셜을 모두 등록해야 합니다.

단계별 사용 안내

1 바이오인식 장치 등록

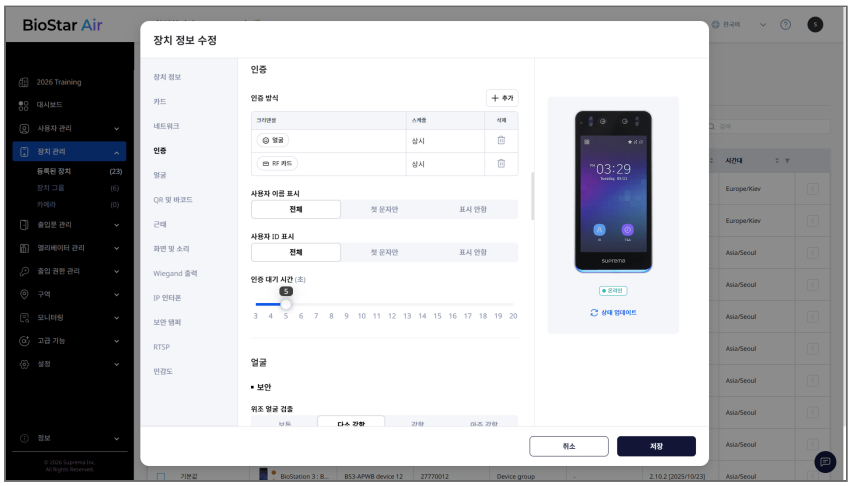
BioEntry W3 또는 BioStation 3 장치에 BioStar Air 호환 펌웨어가 설치되어 있는지 확인하세요. 모델 이름이 `-AIR`로 끝나는 장치는 슈프리마에서 제공하는 기본 펌웨어가 이미 설치되어 있습니다.

모바일 기기에서 BioStar Air 앱을 실행하고 관리자 아이디와 비밀번호로 로그인하세요. 다른 장치를 등록하는 것과 동일한 방식으로 장치를 등록하세요.

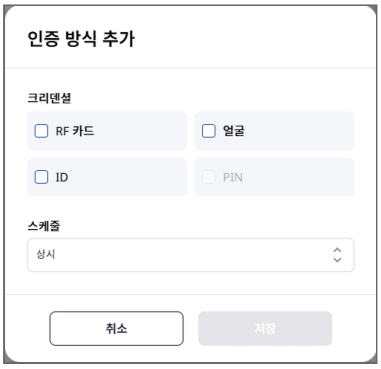
> **알아두기**
> 장치 등록에 대한 자세한 내용은 엣지 장치 등록 및 삭제하기를 참고하세요.

2 장치 설정

1. BioStar Air 포털에 관리자 계정으로 로그인하세요.
2. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
3. 장치 목록에서 바이오인식 장치를 클릭하세요.
4. **장치 정보 수정** 창이 나타나면 **인증** 섹션으로 이동하세요.



5. **인증 방식**를 설정하세요.
   - **Single-factor**: RF 카드 또는 얼굴 중 하나를 사용하여 인증할 수 있습니다.
   - **Two-factor**: RF 카드 또는 얼굴 인증 방식 중 하나를 삭제하고, RF 카드와 얼굴을 모두 사용하여 다시 등록하면 이중 인증할 수 있습니다. **추가** 버튼을 클릭하고 원하는 인증 방식을 조합하세요.

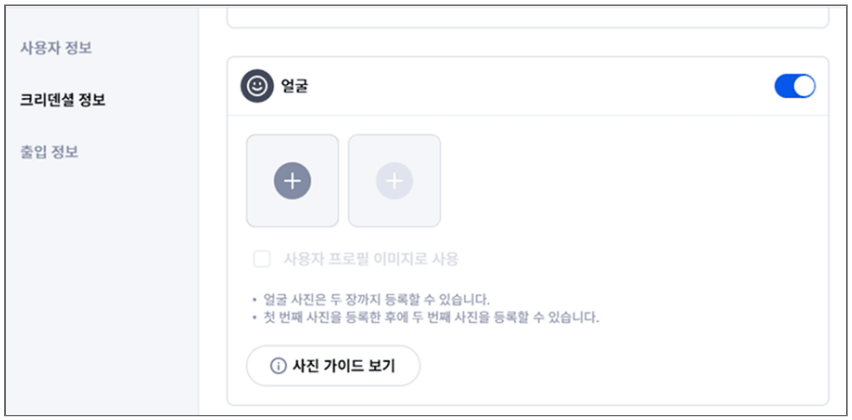


6. **인증 대기 시간**을 설정하세요. 설정한 시간 내에 크리덴셜을 인증하지 않으면 인증에 실패합니다.
7. **얼굴** 섹션에서 다음 옵션을 설정하세요.
   - **위조 얼굴 검출**
   - **모션 센서 감도**
   - **최대 얼굴 회전 각도**
   - **얼굴 인식 거리**
8. 추가 옵션을 구성하세요.
   - **중복 검사**
   - **등록 대기 시간**
   - **마스크 검출 사용**

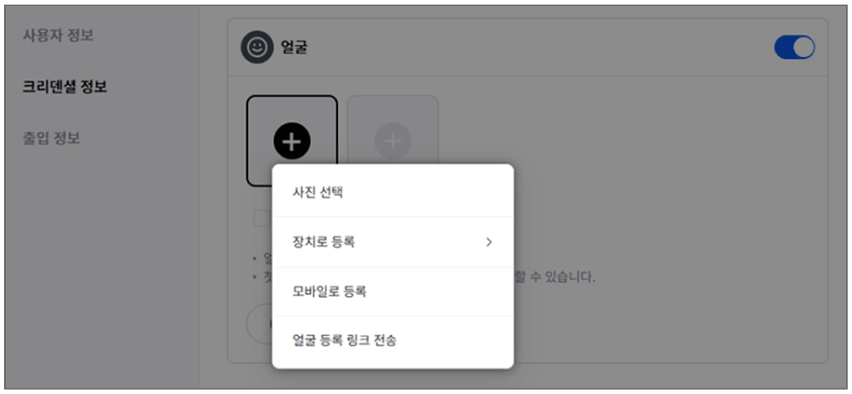
> **알아두기**
> **인증** 섹션의 설정에 대한 자세한 내용은 장치 및 패널 설정 옵션 안내를 참고하세요.

3 사용자 얼굴 등록

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**를 클릭하세요.
2. 새 사용자를 추가하거나 기존 사용자를 수정하기 위한 창을 여세요.
   - **새 사용자 추가**: 사용자 목록 오른쪽 상단의 **사용자 추가** 버튼 클릭
   - **기존 사용자 수정**: 사용자 목록에서 사용자를 클릭 후 ✎ 버튼 클릭
3. 사용자 정보 창에서 **크리덴셜 정보** 섹션으로 이동해 **얼굴** 크리덴셜을 활성화하세요.



4. ＋ 버튼을 클릭하고 얼굴 템플릿을 추가하세요.



- **사진 선택**: 로컬에 저장된 사진 파일 선택
- **장치로 등록**: 연결된 바이오인식 장치(BioEntry W3 또는 BioStation 3) 사용
- **모바일로 등록**: 사용자의 모바일 기기로 전송한 QR 코드를 스캔하고 모바일 기기에서 얼굴 등록
- **얼굴 등록 링크 전송**: 사용자의 이메일 또는 문자 메시지로 얼굴 등록 링크를 보내 모바일 기기의 카메라로 직접 얼굴 등록

> 사용자당 두 개의 얼굴 사진만 업로드할 수 있습니다. 일반적으로 한 장의 사진이면 충분합니다.

5. 얼굴 등록을 완료하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
> 사용자의 얼굴 사진을 일괄로 업로드하는 방법에 대한 자세한 내용은 일괄 작업으로 사용자 추가하기를 참고하세요.

펌웨어 업그레이드

BioStar Air의 펌웨어를 업그레이드하여 장치의 성능을 향상시키고 보안을 강화하며 새로운 기능을 활용할 수 있습니다. 이 과정은 간단하며 BioStar Air 웹 포털이나 BioStar Air 모바일 앱을 통해 실행할 수 있습니다.

시작하기 전에

- 펌웨어 업데이트하려면 **장치는 온라인 상태**여야 합니다. 장치 목록의 **제품명** 열에서 장치 상태를 확인하세요. 장치 이미지 옆에 녹색 점(🟢)이 표시되면 온라인 상태입니다.
- 펌웨어 업데이트 중에는 장치가 **일시적으로 오프라인 상태**가 되지만 **3~5분** 이내에 다시 연결됩니다.

- 펌웨어 업데이트 중에는 장치가 일시적으로 오프라인이 되므로, 업무 시간 외에 실행하기를 권장합니다.
- 새 펌웨어가 업데이트되면 알림을 받을 수 있도록 설정할 수 있습니다. 알림 설정에 대한 자세한 내용은 알림 및 리포트 설정하기를 참고하세요.

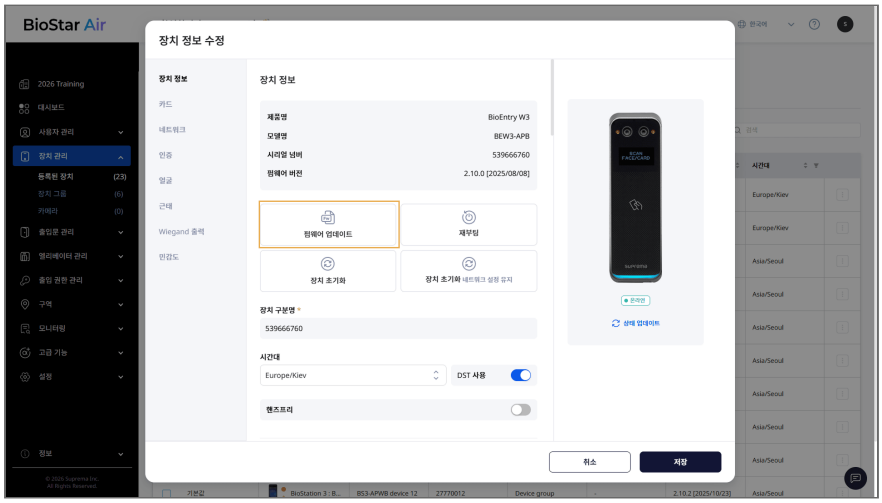
> **알아두기**
> 장치 관리에 대한 자세한 내용은 등록된 엣지 장치 관리하기를 참고하세요.

개별 장치 업그레이드

Web

BioStar Air 포털에 로그인한 후 다음 단계를 따라 펌웨어를 업그레이드하세요.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록에서 펌웨어 업그레이드할 장치를 클릭하세요.
3. **장치 정보 수정** 창이 나타나면 **장치 정보** 섹션으로 이동하세요.
4. **펌웨어 업데이트** 버튼을 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

5. **펌웨어 업데이트** 창이 나타나면 최신 펌웨어 버전을 선택하고 **업데이트** 버튼을 클릭하세요.



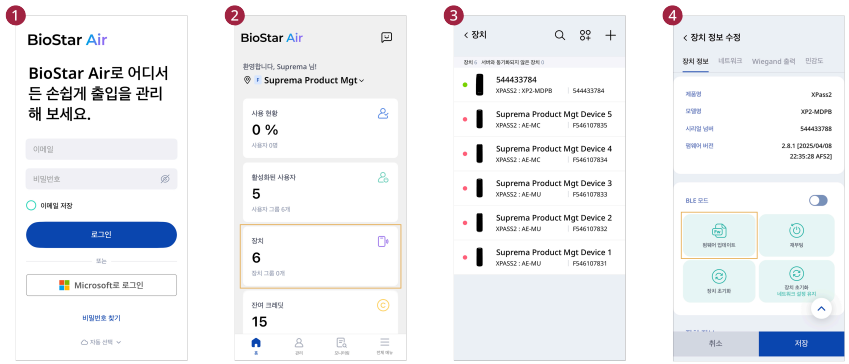
해당 장치가 자동으로 재시작되고 다시 온라인 상태가 될 때까지 기다리세요. 목록의 장치가 녹색 점(🟢)으로 표시되면 온라인 상태입니다.

알아두기

- 해당 펌웨어 버전의 릴리스 노트를 확인하려면 **릴리즈 노트** 버튼을 클릭하세요.
- 모든 장치의 펌웨어 릴리스 노트를 확인하려면 **모든 릴리즈 노트 보기** 버튼을 클릭하세요.

Mobile

모바일 앱에서 펌웨어를 업그레이드하는 과정을 안내합니다.



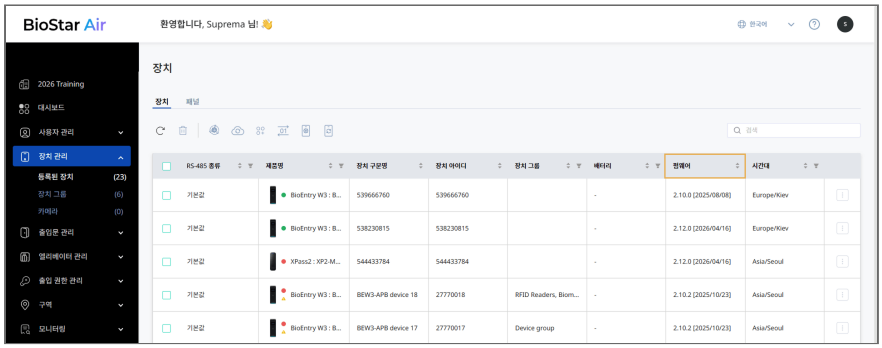
1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. **장치** 카드를 탭하세요.
3. 장치 목록에서 펌웨어 업그레이드할 장치를 탭하세요.
4. **펌웨어 업데이트** 버튼을 탭하세요.
5. 최신 펌웨어 버전을 선택하고 **확인** 버튼을 탭하세요.
6. 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 탭하세요.

알아두기

- 펌웨어 업그레이드는 5~10분 정도 소요될 수 있으며, 장치를 사용할 수 없습니다.
- 장치의 전원을 끄지 마세요.
- 펌웨어 업그레이드를 완료한 후 장치는 자동 재시작합니다.

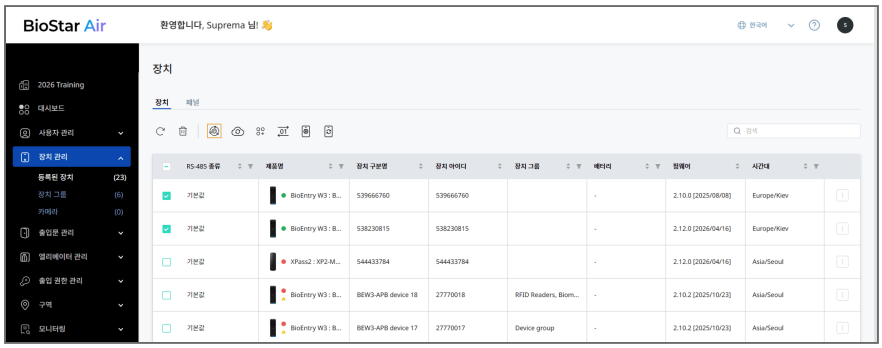
여러 장치 한 번에 업그레이드

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록의 **펌웨어** 열에서 각 장치의 현재 버전을 확인하세요.
3. 장치를 펌웨어 버전별로 정렬하려면 **펌웨어** 열의 오른쪽에 있는 화살표 버튼을 클릭하세요.



4. 업그레이드할 각 장치 왼쪽의 체크박스를 클릭하세요. 같은 종류의 장치를 선택해야 합니다.

5. 장치 목록 상단의 버튼을 클릭하세요.



6. **펌웨어 업데이트** 창이 나타나면 최신 펌웨어 버전을 선택하고 **업데이트** 버튼을 클릭하세요.



선택한 장치가 자동으로 재시작되고 다시 온라인 상태가 될 때까지 기다리세요. 목록의 장치가 녹색 점(🟢)으로 표시되면 온라인 상태입니다.

> **알아두기**
>
> - 펌웨어 업그레이드는 5~10분 정도 소요될 수 있으며, 장치를 사용할 수 없습니다.
> - 장치의 전원을 끄지 마세요.
> - 펌웨어 업그레이드를 완료한 후 장치는 자동 재시작합니다.
> - 해당 펌웨어 버전의 릴리스 노트를 확인하려면 **릴리즈 노트** 버튼을 클릭하세요.
> - 모든 장치의 펌웨어 릴리스 노트를 확인하려면 **모든 릴리즈 노트 보기** 버튼을 클릭하세요.

XPass D2 펌웨어 업그레이드

XPass D2 장치는 두 가지 펌웨어 구성 요소를 사용합니다.

- **MICOM**: 장치 동작, RS-485 통신, 인증 처리, 안정성, 일반적인 버그 수정 등에 대한 업데이트를 포함합니다.
- **BLE**: Bluetooth 통신과 관련된 업데이트를 포함합니다.

XPass D2 장치는 반드시 **MICOM** → **BLE** 순서로 펌웨어를 업그레이드해야 합니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. **패널** 탭을 클릭하세요.
3. XPass D2 장치의 체크박스를 클릭하세요. 1개의 장치만 선택할 수 있습니다.



4. 목록 상단의 버튼을 클릭하세요.
5. **펌웨어 업데이트** 창이 나타나면 **MICOM** 펌웨어 버전을 선택하세요.



6. **업데이트** 버튼을 클릭하세요.
7. 해당 장치가 자동으로 재시작되고 다시 온라인 상태가 될 때까지 기다리세요. 목록의 장치가 녹색 점(🟢)으로 표시되면 온라인 상태입니다.
8. 펌웨어 업그레이드 과정을 반복하여 **BLE** 펌웨어 버전을 선택하고 업데이트하세요.

> **주의**
>
> - 화면에 표시된 펌웨어 버전 정보만으로는 **MICOM**, **BLE** 각 구성 요소의 설치 상태를 개별 확인하기 어렵습니다. BLE 업그레이드를 완료할 때까지 펌웨어 업그레이드를 계속 진행하세요.
> - 장치는 **MICOM** 업데이트 후와 **BLE** 업데이트 후 각각 온라인 상태로 복구됩니다. 녹색 온라인 표시(🟢)만으로 전체 업그레이드 완료를 확인하지 마세요. 두 단계를 모두 완료했는지 다시 한 번 확인하세요.
> - CS-20을 통해 연결된 보조 장치는 한 번에 하나의 장치만 펌웨어를 업그레이드할 수 있습니다.

출입문

BioStar Air의 출입문 관리는 보안과 접근 통제를 효율적으로 운영하는 핵심입니다. 출입문을 등록하고 입구 및 출구 장치를 구성하며, 그룹과 스케줄을 통해 대규모 출입 통제를 관리할 수 있습니다. 또한 자동화된 잠금/해제 정책과 인증 기반 접근 통제로 보안을 강화할 수 있습니다.

등록 출입문 관리하기

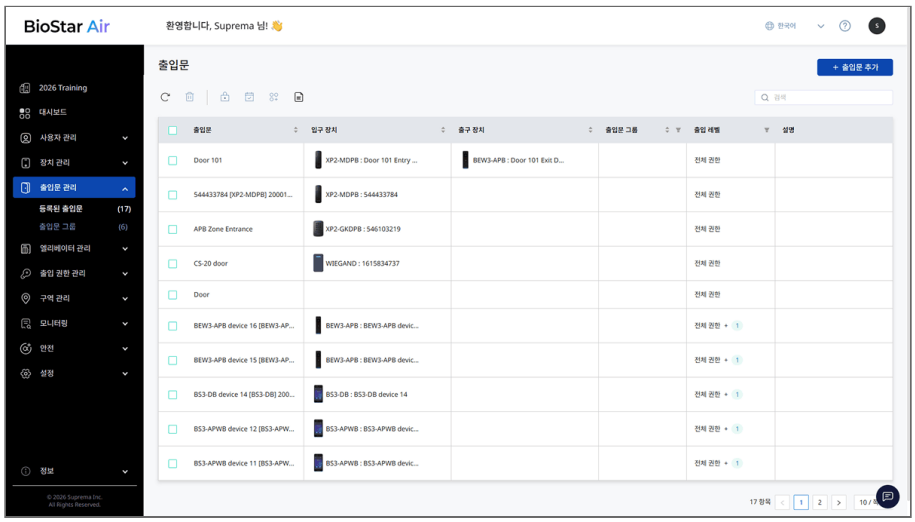
등록된 출입문에 입출입 장치를 할당하고, 릴레이와 출입 레벨을 구성하며, 출입 스케줄을 설정합니다. 보안, 화재 대피, 근태 관리(T&A)를 위해 체계적으로 출입을 통제할 수 있습니다.

> **팁**
> 출입문 등록 및 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

출입문 목록 살펴보기

출입문 목록에서는 BioStar Air에 등록된 모든 출입문을 확인할 수 있습니다. 각 출입문의 이름, 할당된 장치, 그룹, 출입 레벨 등 주요 정보를 확인할 수 있습니다. 또한 개별 출입문을 클릭하여 세부 정보를 확인하고 설정을 수정할 수 있습니다.

등록된 출입문을 확인하려면 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.



출입문 정보

출입문 목록은 다음과 같은 정보를 제공합니다.

- **출입문**: 출입문 이름입니다. 일반적으로 장치 등록 시 자동 지정되며, 관리자는 출입문 이름을 변경할 수 있습니다.
- **입구 장치**: 출입문으로 들어오는 사용자를 인증하는 장치입니다.
- **출구 장치**: 출입문에서 나가는 사용자를 인증하는 장치입니다.
- **출입문 그룹**: 출입문에 할당된 그룹 이름입니다.
- **출입 레벨**: 출입문에 할당된 출입 레벨입니다. 출입 레벨 할당에 대한 자세한 내용은 출입 레벨 일괄 할당을 참고하세요.
- **설명**: 출입문에 대한 설명입니다.
- **카메라**: 출입문과 연결된 카메라 정보가 표시됩니다. **카메라** 열은 **설정** → **사이트** → **추가 기능**에서 **비디오 관리** 기능을 활성화해야 표시됩니다.

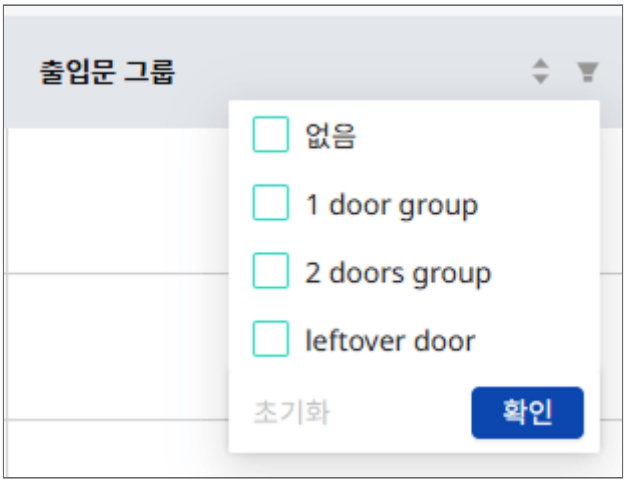
추가 기능

목록에서 하나 또는 여러 개의 출입문을 선택하면 관리자는 제공하는 추가 기능으로 출입문을 관리할 수 있습니다.

- : 출입문 목록을 새로고침할 수 있습니다.
- : 목록에서 선택한 출입문을 제거합니다.
- : 목록에서 선택한 출입문의 출입 레벨을 설정할 수 있습니다. 자세한 내용은 출입 레벨 일괄 할당를 참고하세요.
- : 출입문 열림 및 잠김 상태를 위한 스케줄을 설정합니다. 자세한 내용은 출입문 스케줄 관리하기를 참고하세요.
- : 목록에서 선택한 출입문을 그룹으로 구성할 수 있습니다. 그룹 관리에 대한 자세한 내용은 출입문 그룹 관리하기를 참고하세요.
- : 출입문 리포트를 생성할 수 있습니다. 리포트 생성에 대한 자세한 내용은 출입문 리포트 생성을 참고하세요.

필터링

출입문 목록에서는 출입문 그룹을 기준으로 필터링하여 조회할 수 있습니다. **출입문 그룹** 열의 버튼을 클릭하고 원하는 그룹을 선택하세요. **확인** 버튼을 클릭하면 선택한 그룹에 속한 출입문만 표시됩니다.



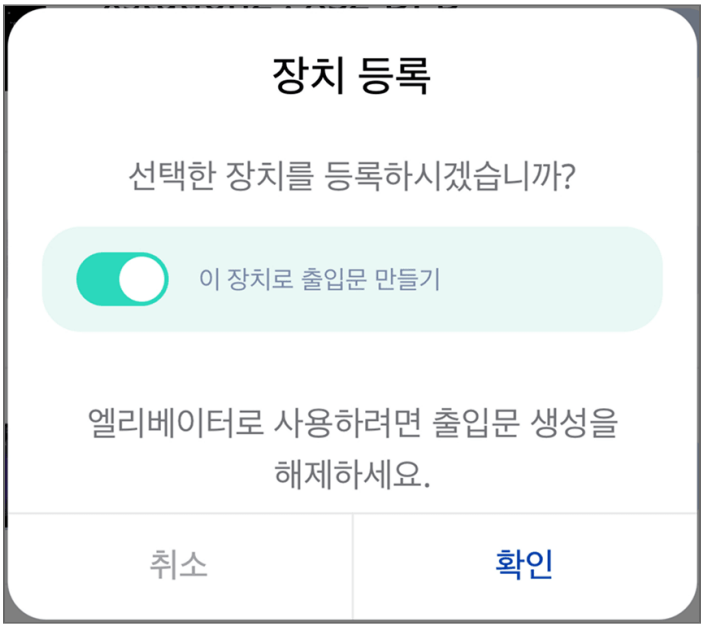
알아두기

적용한 필터 조건을 초기화하려면 버튼을 클릭하고 **초기화** 버튼을 선택하세요.

출입문 추가

장치와 함께 추가

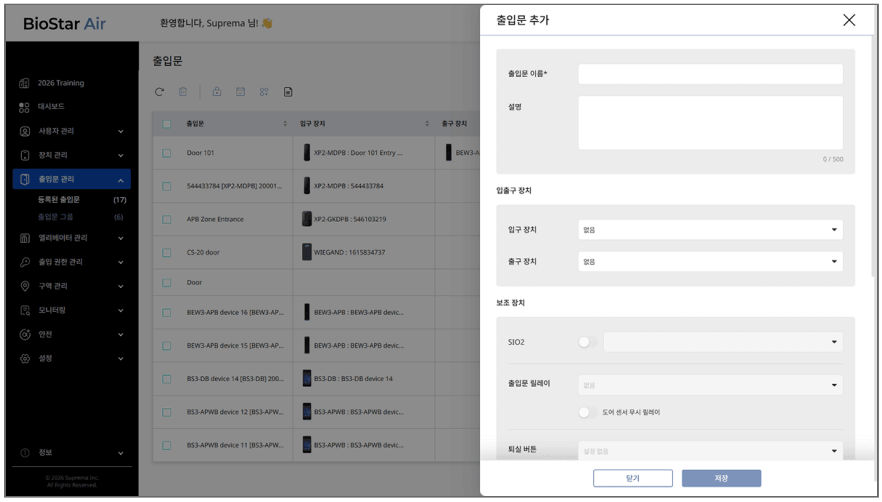
모바일 앱에서 장치 등록 시 마지막 단계에서 **이 장치로 출입문 만들기** 옵션을 선택하면 출입문을 생성할 수 있습니다. 모바일 앱으로 장치를 등록하는 방법에 대한 자세한 내용은 엣지 장치 등록 및 삭제하기를 참고하세요.



웹 포털에서 추가

BioStar Air 포털에서 새 출입문을 추가하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 화면 오른쪽 상단의 **출입문 추가** 버튼을 클릭하세요.
3. **출입문 추가** 패널이 나타나면 **출입문 이름**을 입력하세요.



4. **입구 장치**와 **출구 장치**를 선택하세요.
5. 출입문 설정을 저장하고 추가하려면 **저장** 버튼을 클릭하세요.

출입문의 장치 할당 규칙

- 각 장치는 **하나의 출입문**에만 할당할 수 있습니다.
- 장치가 이미 등록되어 있지만 사용할 수 있는 장치 목록에 나타나지 않는다면, 해당 장치가 다른 출입문에 할당되어 있는지 확인하세요. 다른 장치에 할당되어 있다면 해당 출입문에서 제거한 후 다시 시도하세요.
- **한 개의 장치는 출입문과 엘리베이터에 동시 할당할 수 없습니다.**

마스터/슬레이브 장치를 사용하는 출입문

- 출입문은 마스터 장치(XPass 2, CoreStation 20)가 제어합니다.
- 마스터 장치로 설정된 XPass 2는 할당된 보조 장치, 모듈 수에 관계 없이 한 개의 출입문에만 할당할 수 있습니다.
- 마스터 장치로 설정된 XPass 2는 최대 31개의 보조 장치를 할당할 수 있으며, 보조 Secure I/O 2(SIO2)로 릴레이를 제어하는 새로운 출입문을 추가할 수 있습니다.
- CoreStation 20(CS-20)과 Secure I/O 2(SIO2)을 사용하는 출입문은 생성할 수 없습니다.

출입문 구성 제한 사항

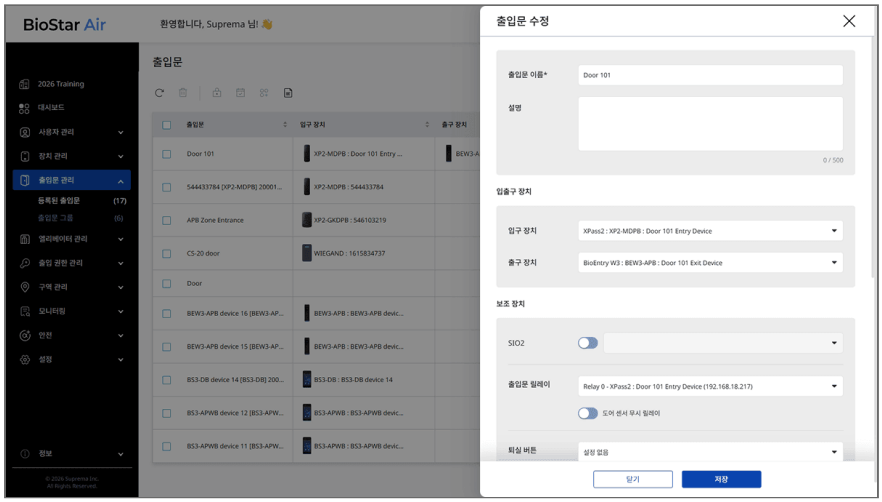
출입문 구성에는 아래와 같은 제한 사항이 있습니다.

- XPass D2 1개 + SIO2 (릴레이는 SIO2 소유)
- XPass 2 1개 + XPass D2 (릴레이는 XPass 2 소유)
- XPass D2 2개 (릴레이는 XPass 2 소유)
- 1개 또는 2개의 OSDP/Wiegand 장치 (릴레이는 CS-20 소유)
- 출입문 당 SIO2는 1개만 허용 (릴레이는 I/O 용): XPass D2와 동일한 XPass 2에 배선 필요

출입문 수정

출입문의 세부 정보 및 설정을 수정하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 목록에서 수정할 출입문을 클릭하세요. 또는 출입문 왼쪽의 체크박스를 클릭한 후 상단의 화면 왼쪽 사이드바에서 버튼을 클릭하세요.
3. **출입문 수정** 패널이 나타나면 **출입문 이름** 및 **설명**을 수정하세요.

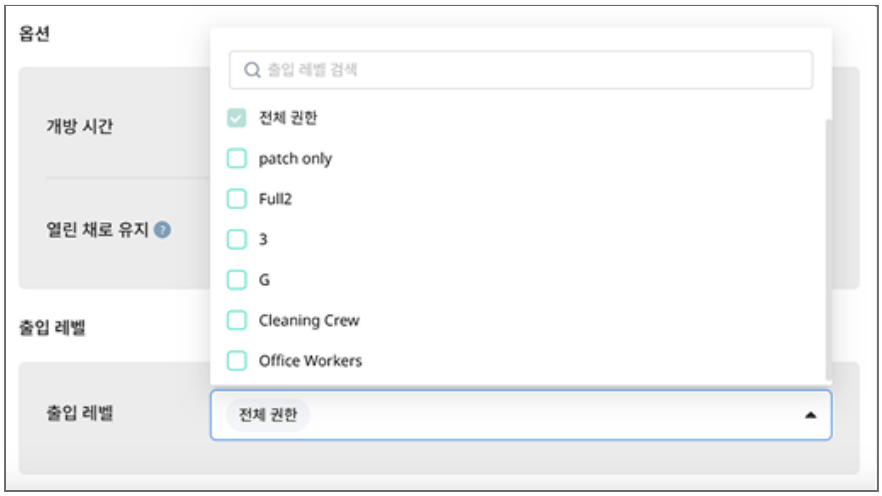


4. **입출구 장치** 섹션에서 출입문의 사용자 인증을 위한 장치를 선택하세요.
   - **입구 장치**: 출입문으로 들어오는 사용자를 인증하는 장치를 선택하세요.
   - **출구 장치**: 출입문에서 나가는 사용자를 인증하는 장치를 선택하세요.
5. **보조 장치** 섹션에서 릴레이 장치를 설정하세요.
   - **카메라**: 이벤트 로그를 위한 CCTV 카메라를 연결할 수 있습니다.

- **출입문 릴레이**: 출입문 잠금을 제어하는 릴레이 장치를 선택하세요.
- **도어 센서 무시 릴레이**: 출입문 센서를 무시하도록 릴레이를 설정할 수 있습니다.

> 카메라는 **설정** → **사이트** → **추가 기능**에서 **비디오 관리** 기능을 활성화해야 사용할 수 있습니다.

6. 추가 설정을 구성하세요.
   - 설치된 경우 **퇴실 버튼**으로 설정할 포트를 선택하세요.
   - **도어 센서**로 설정할 포트를 선택하세요.
   - **개방 시간**에서 출입문이 열린 상태로 유지되는 시간을 설정하세요. (기본값: 3초)
7. **출입 레벨** 섹션에서 해당 출입문에 할당하거나 제거할 출입 레벨의 체크박스를 클릭하세요.



8. 수정 사항을 적용하려면 **저장** 버튼을 클릭하세요.

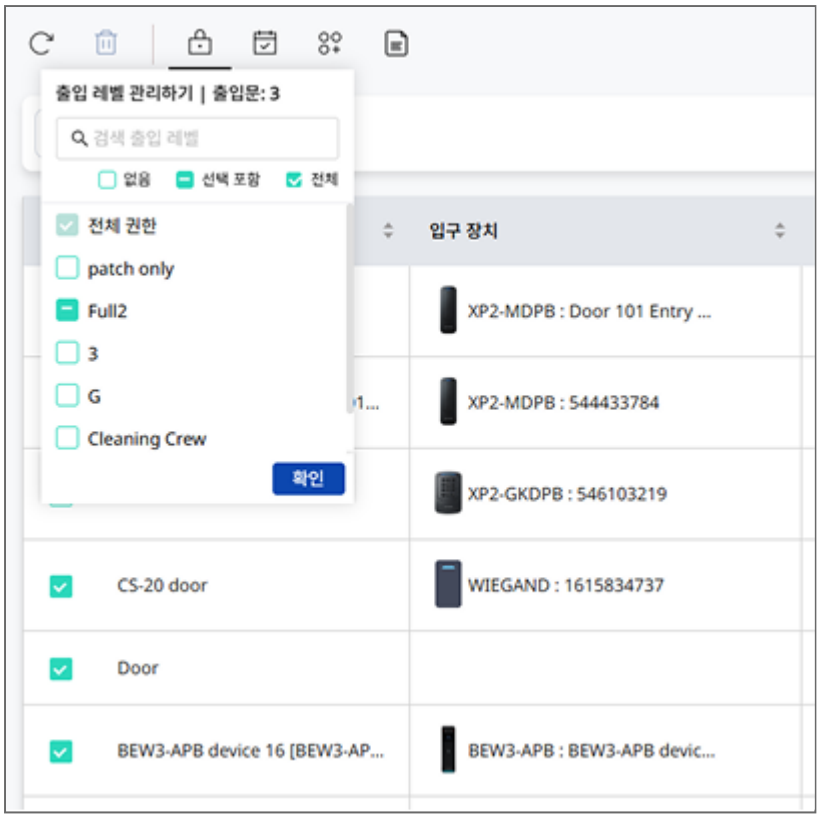
> **알아두기**
>
> - 보안을 위해 릴레이는 항상 출입문의 보안 측에 있는 장치를 연결해야 합니다. 일반적으로 출구 장치의 릴레이를 사용하거나 SIO2 모듈을 사용하는 것을 권장합니다.
> - 클라우드에 직접 연결하여 구성한다면 입구 장치와 출구 장치에 각각 네트워크 케이블 연결이 필요합니다.
> - 마스터-보조 장치 구성에서, 마스터(보통 출구 장치) 장치는 네트워크 연결이 필요하고 보조 장치는 RS-485를 통해 마스터 장치에 연결됩니다.
> - SIO2 보안 모듈 구성에 대한 자세한 내용은 SIO2 보안 모듈 구성하기를 참고하세요.

출입 레벨 일괄 할당

여러 출입문에 같은 출입 레벨을 할당해야 할 때, 출입문을 하나씩 수정하는 대신 목록에서 한 번에 출입 레벨을 할당하거나 해제할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 출입 레벨을 설정할 출입문의 체크박스를 하나 이상 선택하세요.
3. 출입문 목록 상단의 버튼을 클릭하세요.

4. **출입 레벨 관리하기** 팝업 메뉴가 나타나면 선택한 출입문에 적용할 출입 레벨의 체크박스를 클릭하세요.



필요한 경우 검색 필드에서 액세스 레벨을 검색하세요.

- **없음**: 선택한 출입문에서 해당 출입 레벨이 제거됩니다.
- **선택 포함**: 선택한 출입문 중 일부에만 해당 출입 레벨이 할당되어 있는 상태입니다.
- **전체**: 선택한 모든 출입문에 해당 출입 레벨이 할당됩니다.

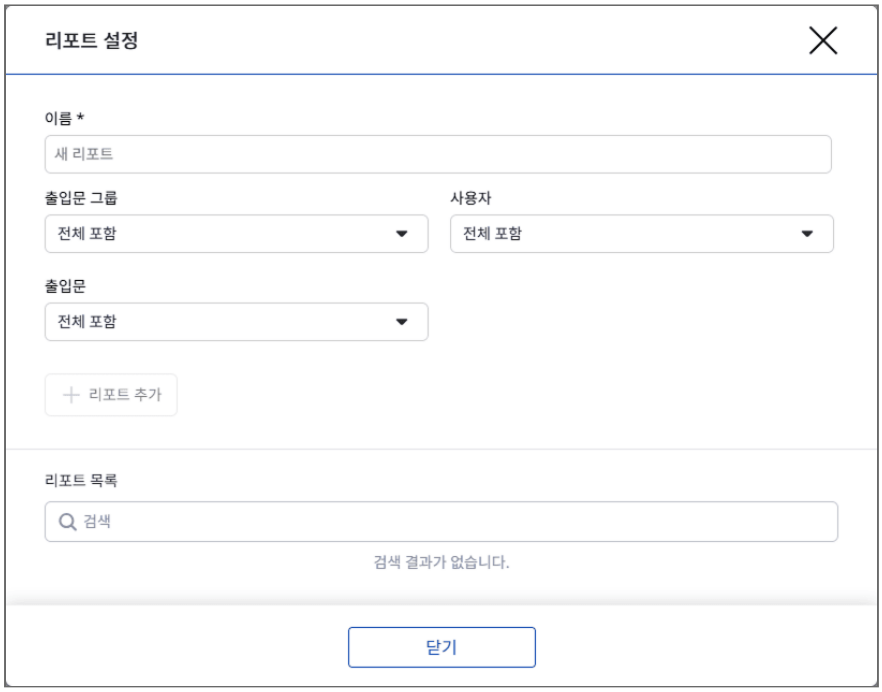
5. 설정을 완료하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 출입문 중 하나 이상이 오프라인 상태이면, 변경한 출입 레벨은 장치가 다시 연결될 때 적용됩니다.
> - **전체 권한** 출입 레벨은 시스템이 자동 관리하므로 변경할 수 없습니다.
> - 설정 변경 중 일부 출입문에서 오류가 발생하여 일부 출입 레벨이 적용되지 않을 수 있습니다. 출입 레벨 변경에 실패한 출입문은 안내 창에 표시됩니다. 다시 시도하려면 **실패 항목 재시도** 버튼을 클릭하세요.

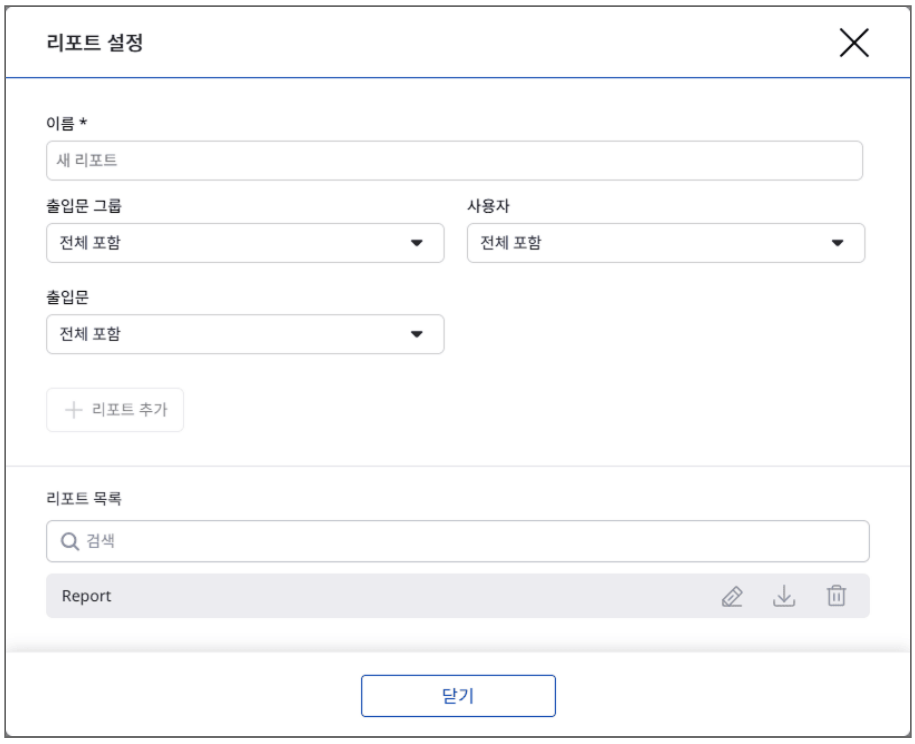
출입문 리포트 생성

출입문 리포트를 생성하여 관리자의 이메일로 전송할 수 있습니다. 출입문 리포트는 출입문을 통해 출입한 사용자에 대한 정보를 제공합니다.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 출입문 목록 상단의 버튼을 클릭하세요.
3. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



4. 리포트에 포함할 항목을 선택하세요.
5. 생성한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
6. **리포트 목록**이 생성되며 관리자의 이메일로 다운로드 링크가 전송됩니다.



알아두기

리포트 목록에서 생성된 리포트를 검색하거나, 수정, 다운로드, 삭제할 수 있습니다.

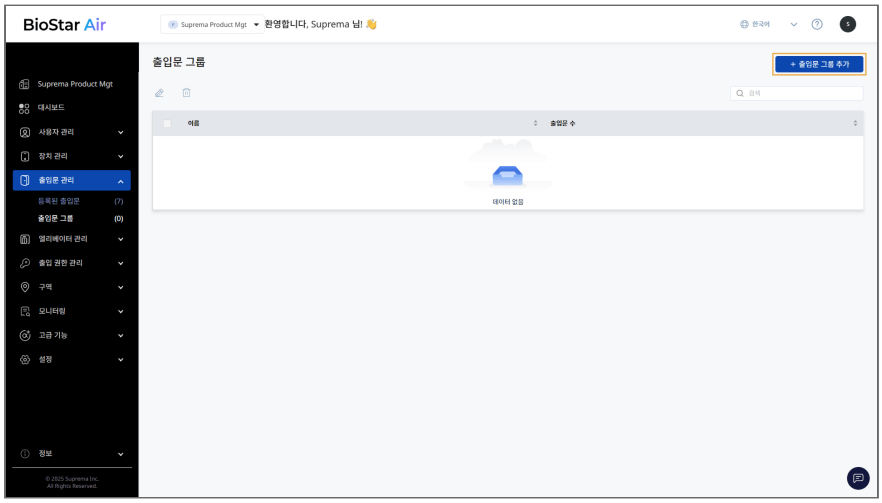
출입문 그룹 관리하기

출입문을 그룹으로 구성하면 출입 통제 정책을 효율적으로 관리할 수 있습니다. 그룹별로 출입 등급 및 권한을 일괄 설정하여 여러 출입문에 일관성 있는 보안 정책을 적용할 수 있습니다.

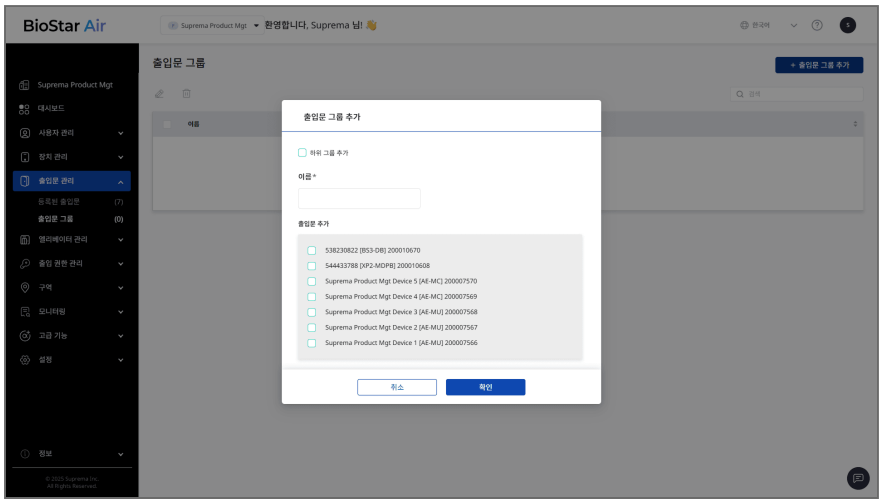
> **알아두기**
>
> - 출입문 관리에 대한 자세한 내용은 등록 출입문 관리하기를 참고하세요.
> - 출입 레벨 관리에 대한 자세한 내용은 출입 레벨 관리하기를 참고하세요.

출입문 그룹 추가

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **출입문 그룹**을 클릭하세요.
2. 화면 오른쪽 상단의 **출입문 그룹 추가** 버튼을 클릭하세요.



3. **출입문 그룹 추가** 창이 나타나면 출입문 그룹 이름을 입력하세요.



> 특정 그룹의 하위 그룹으로 장치 그룹을 추가하려면 **하위 그룹 추가** 옵션을 클릭하고, 상위 그룹을 선택하세요.

4. **출입문 추가**에서 그룹에 포함할 출입문을 선택하세요.
5. 출입문 그룹을 저장하려면 **확인** 버튼을 클릭하세요.

출입문 그룹 목록에서 새로 추가된 그룹과 해당 그룹에 속한 출입문의 수를 확인할 수 있습니다. 출입문 그룹을 클릭하면 해당 그룹에 속하 출입문을 확인할 수 있습니다.

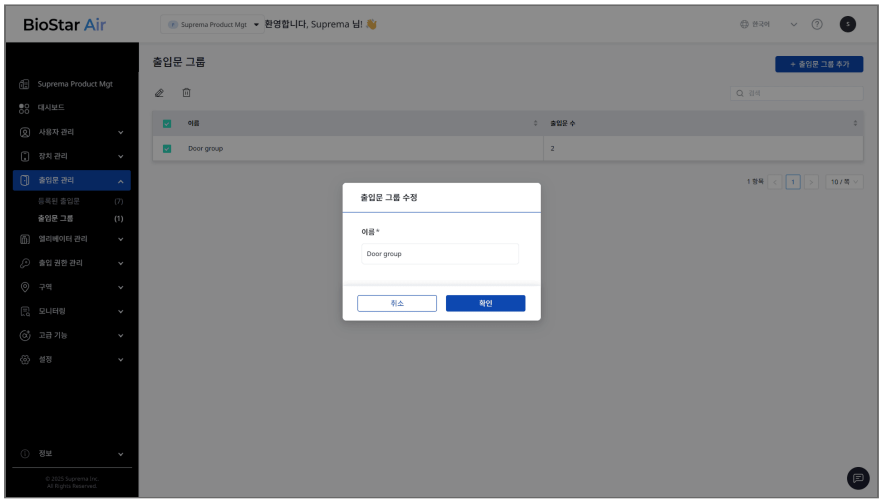


알아두기

- 하위 그룹에 출입문을 추가해도 상위 그룹에 자동 포함되지 않습니다.
- 장치 또는 출입문이 없는 빈 상위 그룹을 추가할 수 있습니다.

출입문 그룹 이름 변경

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **출입문 그룹**을 클릭하세요.
2. 출입문 그룹 목록에서 이름을 변경할 출입문 그룹의 체크박스를 클릭하세요.
3. 출입문 그룹 목록 상단의 버튼을 클릭하세요.
4. **출입문 그룹 수정** 창이 나타나면 새 그룹 이름을 입력하세요.



5. 변경한 그룹 이름을 저장하려면 **확인** 버튼을 클릭하세요.

출입문 그룹 삭제

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **출입문 그룹**을 클릭하세요.
2. 출입문 그룹 목록에서 삭제하려는 출입문 그룹의 체크박스를 클릭하세요.
3. 출입문 그룹 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

출입문 그룹 목록에서 선택한 출입문 그룹이 삭제됩니다. 해당 그룹의 하위 그룹까지 모두 삭제됩니다. 그룹을 삭제하더라도 출입문은 삭제되지 않습니다.

출입문 스케줄 관리하기

출입문 스케줄을 설정하여 시간대별로 출입문을 자동으로 잠그고 열 수 있습니다. 잠김 및 잠김 해제 시간을 구성하고, **최초 인증 후 열림**과

같은 고급 옵션을 활용하여 안전하고 통제된 출입을 설정하세요.

> **알아두기**
>
> - 스케줄은 인터넷이 연결되어 있는 출입문과 장치에만 적용할 수 있습니다.
> - 휴일 그룹은 별도로 구성되지 않는 한 잠김 해제 스케줄을 무시합니다.
> - 비상 상황에 대비해 제한없는 출입 권한을 가진 관리자가 적어도 한 명 이상 있어야 합니다.

스케줄이 필요한 경우

출입문 스케줄은 없어도 괜찮습니다. 대부분의 시설에서는 기본 출입 제어만으로 충분합니다. 인증된 사용자가 크리덴셜을 제시하면 자동으로 출입문이 열리므로, 추가 스케줄 설정 없이도 정상 작동합니다.

아래의 상황에서 스케줄을 설정하세요.

- 특정 시간에 누구든지 자유롭게 출입할 수 있도록 해야 할 때
- 특정 시간에 모든 사용자의 출입을 차단해야 할 때
- 시간대별로 출입 정책을 다르게 적용해야 할 때

열림 스케줄과 **잠김 스케줄**의 혼동을 피하려면 각각의 작동 방식과 사용 시점을 명확히 이해해야 합니다.

열림 스케줄 vs 잠김 스케줄

구분	열림 스케줄	잠김 스케줄
스케줄 시간 중 상태	항상 열림	항상 잠김
인증 필요 여부	불필요, 누구든지 자유롭게 출입	크리덴셜 인증으로 열 수 없음
수동 개방	가능	사이트 관리자만 가능
릴레이 작동	계속 작동함	작동하지 않음

> **알아두기**
>
> 사이트 관리자는 BioStar Air 관리자 포털 또는 모바일 앱에서 지정된 관리자를 의미합니다.

열림 스케줄

스케줄 시간 동안 출입문이 항상 열려있으며, 릴레이가 계속 작동합니다. 인증이 필요하지 않으므로 누구든지 자유롭게 출입할 수 있습니다.

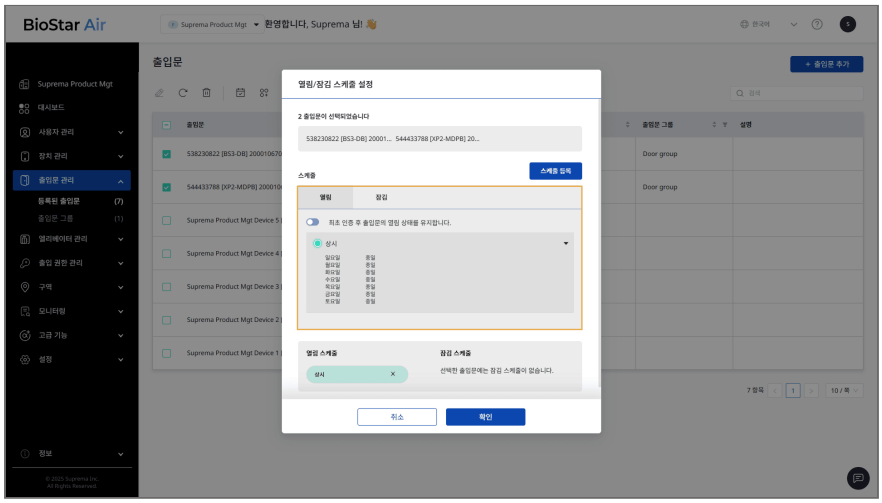
사용 사례

- 공용 공간의 주 출입문
- 주거 단지 내 공용 편의 시설
- 업무 시간 중 사무실 로비 출입문

열림 스케줄 구성

다음 안내에 따라 열림 스케줄을 구성하세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 목록에서 열림 스케줄을 구성할 출입문의 체크박스를 클릭하세요.
3. 출입문 목록 상단의 버튼을 클릭하세요.
4. **열림/잠김 스케줄 설정** 창이 나타나면 **열림** 탭에서 미리 정의된 스케줄을 선택하거나 새 스케줄을 만드세요.



5. 열림 스케줄을 적용하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **최초 인증 후 출입문의 열림 상태를 유지합니다.** 옵션을 활성화하면 사용자가 최초로 인증한 후 선택한 스케줄에 따라 출입문의 열림 상태를 유지할 수 있습니다. 이 옵션은 아래와 같은 사례에서 유용하게 활용할 수 있습니다.
>   - 직원이 도착한 후에 고객 입장을 허용하는 소매점
>   - 첫 직원이 건물을 열면 이후 다른 직원들은 자유롭게 출입할 수 있는 사무실
>   - 시설 담당자가 출입을 개시하면 회원은 자유롭게 이용할 수 있는 멤버십 시설
> - 스케줄 등록에 대한 자세한 내용은 새 스케줄 등록을 참고하세요.

잠김 스케줄

스케줄 시간 동안 출입문이 항상 잠겨있으며, 릴레이가 작동하지 않습니다. 유효한 크리덴셜을 제시해도 인증으로 열 수 없으며, 사이트 관리자만 수동으로 개방할 수 있습니다.

사용 사례

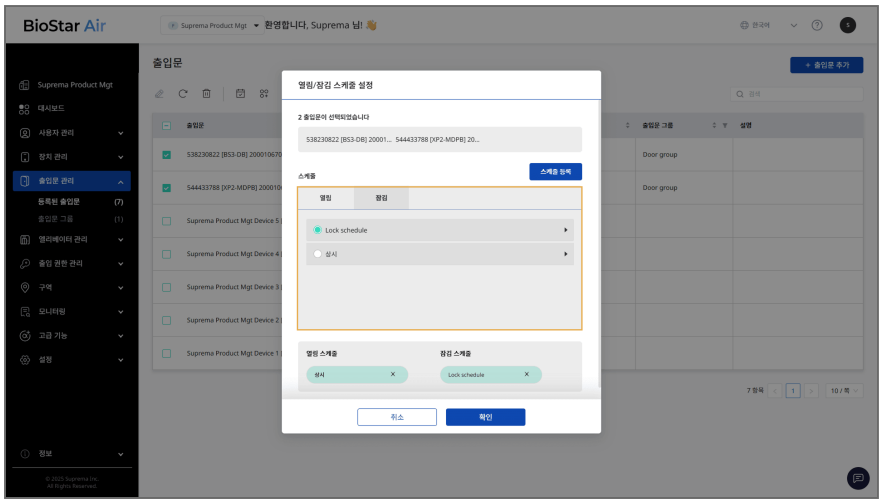
- 특정 시간 이후에 엄격히 폐쇄해야 하는 구역
- 수영장 또는 체육관, 기타 출입 제한 구역과 같은 시설

잠김 스케줄 구성

다음 안내에 따라 잠김 스케줄을 구성하세요.

1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.

2. 목록에서 잠김 스케줄을 구성할 출입문의 체크박스를 클릭하세요.
3. 출입문 목록 상단의 버튼을 클릭하세요.
4. **열림/잠김 스케줄 설정** 창이 나타나면 **잠김** 탭에서 미리 정의된 스케줄을 선택하거나 새 스케줄을 만드세요.



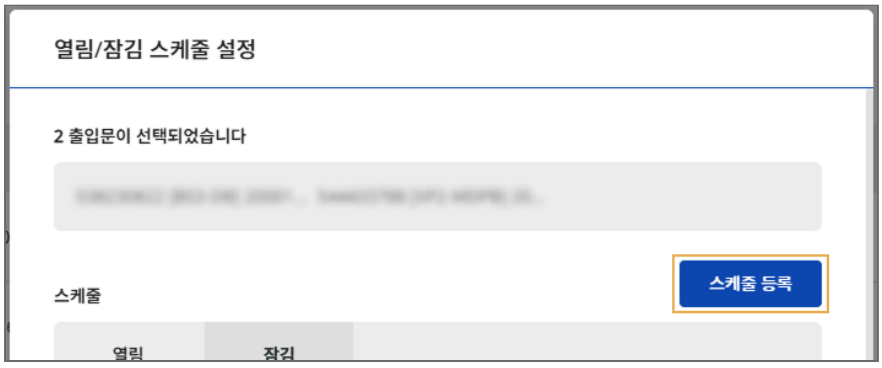
5. 잠김 스케줄을 적용하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 잠김 스케줄은 표준 접근 권한을 무시하므로 사용자는 잠김 시간 동안 출입문을 열림(잠김 해제) 상태로 변경할 수 없습니다.
> - 새 스케줄 등록에 대한 자세한 내용은 새 스케줄 등록을 참고하세요.

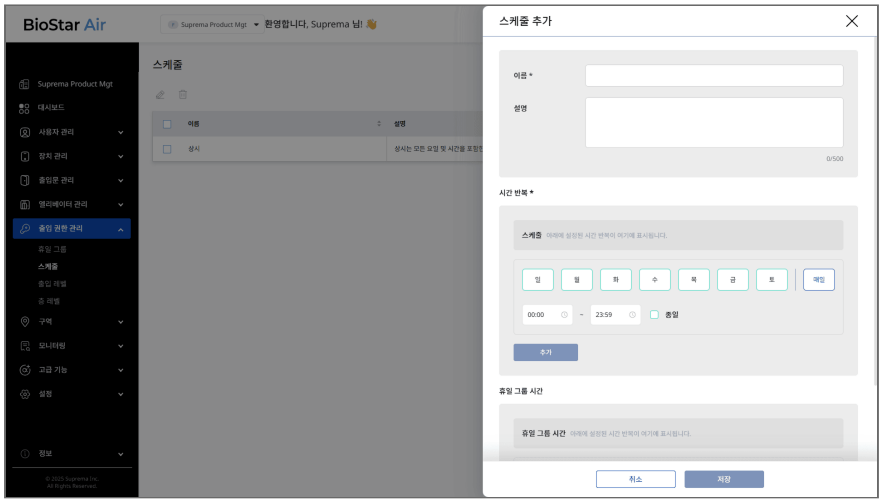
새 스케줄 등록

새 스케줄을 아래의 단계를 따르세요.

1. **열림/잠김 스케줄 설정** 창에서 **스케줄 등록** 버튼을 클릭하세요.



2. 스케줄 추가 화면으로 이동하면 **이름**과 **설명**(선택 사항)을 입력하세요.



3. **시간 반복 *** 섹션에서 인증 없이 출입문이 열려 있어야 하는 요일과 시간을 선택하고 **추가** 버튼을 클릭하세요.
4. 스케줄을 등록하려면 **저장** 버튼을 클릭하세요.

스케줄을 새로 등록한 후 **출입문 관리** → **등록된 출입문**으로 돌아와 출입문 스케줄을 구성하세요.

엘리베이터

슈프리마의 OM-120 모듈을 사용하여 엘리베이터 출입 통제를 지원합니다. OM-120 모듈을 통해 관리자는 BioStar Air와 호환되는 장치와 통합하여 층별 출입을 제어할 수 있습니다. 데이지 체인 방식으로 연결된 OM-120 장치를 통해 최대 144층까지 지원합니다.

> **팁**
> 엘리베이터 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

엘리베이터 관리하기

엘리베이터 출입 통제를 구성하려면 먼저 출입 통제 장치에 OM-120 모듈을 연결합니다. 그 다음 각 층의 이름과 릴레이 번호를 설정하고, 층별로 접근 가능한 시간대를 스케줄로 제한하여 보안을 강화할 수 있습니다.

요구사항

엘리베이터 출입 통제 기능을 활성화하려면 다음 요구사항을 충족해야 합니다.

- 슈프리마 OM-120 모듈: 각 모듈은 최대 12층까지 지원합니다. 최대 12개의 OM-120 모듈을 하나의 출입 통제 장치에 연결하여 최대 144층까지 지원할 수 있습니다.
- OM-120과 연결할 수 있는 BioStar Air와 호환되는 장치가 필요합니다.
- 엘리베이터 제어판에 대한 적절한 배선 작업이 필요합니다. 배선 세부 사항은 엘리베이터 제조업체에 문의하세요.
- 층별 출입 스케줄이 우선 적용되며, 휴일 설정으로 일반 출입 규칙을 재정의할 수 있습니다.

장치와 모듈 연결

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록에서 OM-120 모듈이 연결된 출입 통제 장치를 클릭하세요.

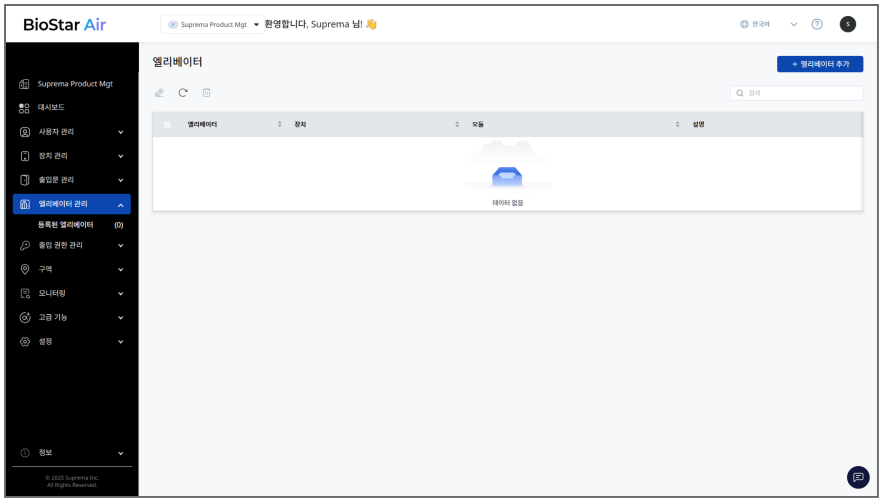
3. **모듈** 섹션에서 **추가** 버튼을 클릭하세요.



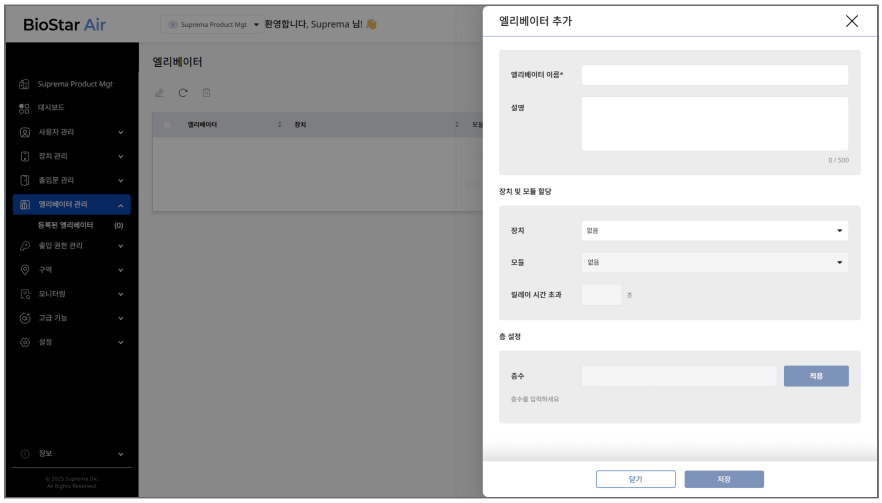
4. 장치와 연결된 OM-120 모듈을 선택하고 **저장** 버튼을 클릭하세요.

엘리베이터 등록

1. 화면 왼쪽 사이드바에서 **엘리베이터 관리** → **등록된 엘리베이터**를 클릭하세요.
2. 화면 오른쪽 상단의 **엘리베이터 추가** 버튼을 클릭하세요.



3. **엘리베이터 추가** 패널이 나타나면 **엘리베이터 이름** 및 **설명**(선택 사항)을 입력하세요.

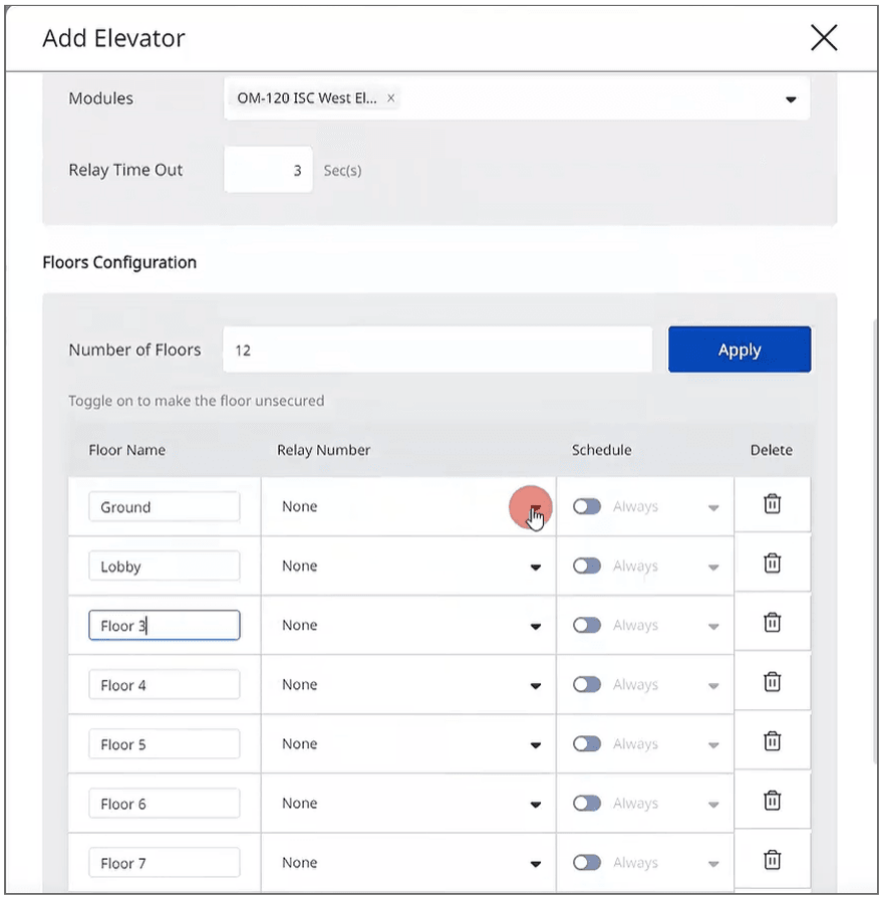


4. **장치 및 모듈 할당** 섹션에서 출입 인증을 위한 장치와 모듈을 선택하세요.
   - **장치**: 출입 인증에 사용할 장치를 선택하세요.

> **주의**
> 장치가 목록에 보이지 않는다면, 해당 장치가 출입문에 할당되어 있는지 확인하세요. 장치는 출입문과 엘리베이터에 동시 할당할 수 없습니다.

- **모듈**: 엘리베이터 버튼 릴레이를 제어할 OM-120 모듈을 선택하세요.
- **릴레이 시간 초과**: 인증 완료 후 층 버튼이 활성화된 상태로 유지되는 시간을 설정하세요. 이 시간이 지나면 릴레이는 층 버튼에 신호를 보내지 않습니다.

5. **층 설정** 섹션에서 제어할 수 있는 층 수를 입력하고 **적용** 버튼을 클릭하세요.
6. 각 층의 이름과 릴레이 번호, 스케줄을 설정하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **층명**: 층 이름을 입력하세요. 1층, 로비, 컨퍼런스 층과 같이 식별하기 쉬운 이름을 사용하는 것이 좋습니다.
- **릴레이 번호**: 엘리베이터 제어판에서 각 층의 버튼에 해당하는 릴레이 출력을 선택하세요.
- **스케줄**: 각 층에 접근할 수 있는 일정을 설정하세요. 예를 들어, 근무 시간 외에는 유지 관리 층에 접근하지 못하도록 제한할 수 있습니다.

7. 엘리베이터 설정을 저장하고 등록하려면 **저장** 버튼을 클릭하세요.

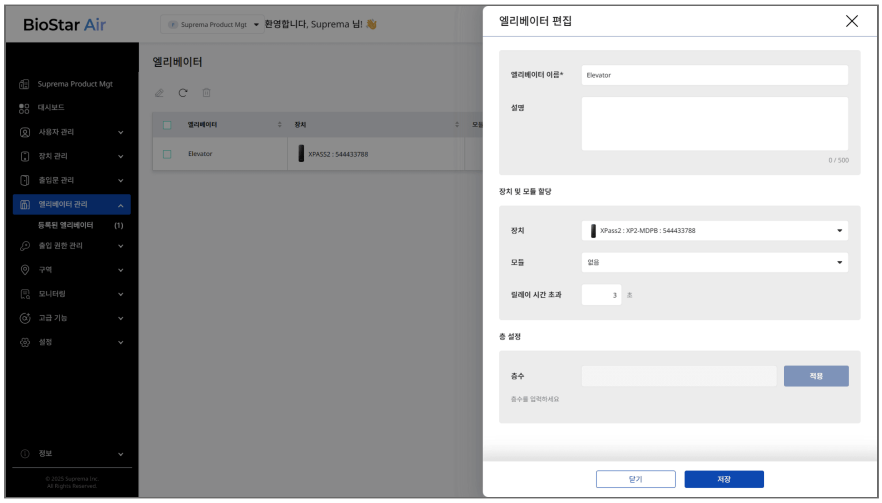
알아두기

- OM-120 모듈당 최대 12층을 지원합니다. 여러 OM-120 모듈을 데이지 체인 방식으로 연결하여 최대 144층까지 확장할 수 있습니다.
- **층 설정** 섹션에서 층을 삭제하려면 버튼을 클릭하세요.
- 스케줄 등록 방법에 대한 자세한 내용은 스케줄 관리하기를 참고하세요.

엘리베이터 수정

등록된 엘리베이터의 세부 정보를 변경하거나 설정을 수정하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **엘리베이터 관리** → **등록된 엘리베이터**를 클릭하세요.
2. 목록에서 수정할 엘리베이터를 클릭하세요. 또는 엘리베이터의 체크박스를 클릭하고 목록 상단의 버튼을 클릭하세요.
3. **엘리베이터 편집** 패널이 나타나면 필요한 정보를 변경하거나 설정을 수정하세요.



4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

엘리베이터 삭제

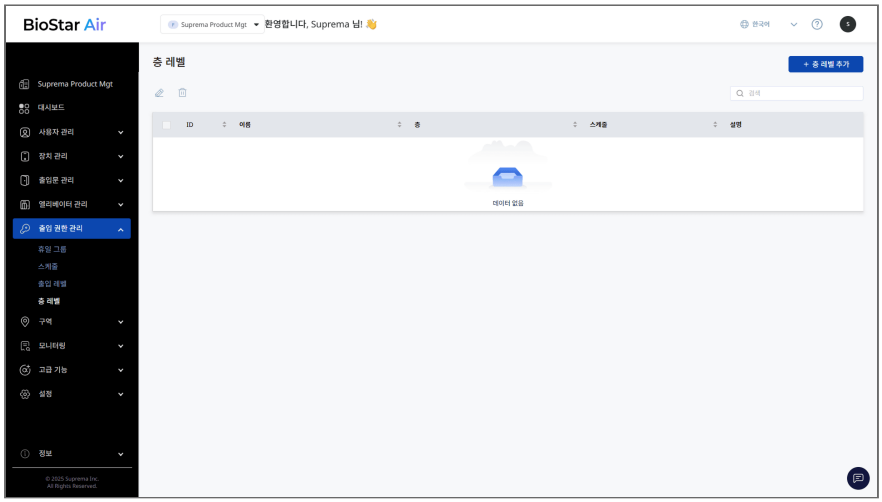
등록된 엘리베이터를 삭제하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **엘리베이터 관리** → **등록된 엘리베이터**를 클릭하세요.
2. 목록에서 삭제할 엘리베이터의 체크박스를 클릭하세요. 1개 이상의 엘리베이터를 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

층별 출입 권한 설정

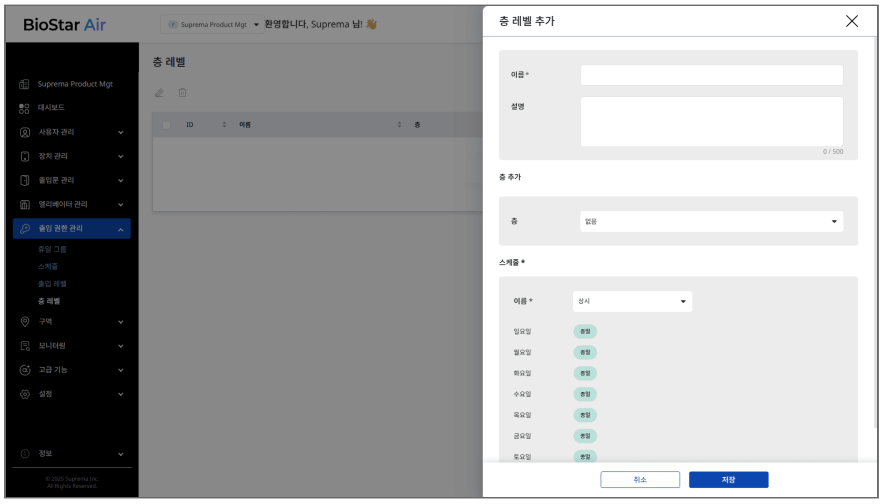
엘리베이터를 등록하고, 층 레벨을 정의하여 사용자와 그룹이 접근할 수 있는 층을 제한합니다. 각 층 레벨별로 출입 스케줄(예: 업무 시간 내)과 휴일 정책을 설정하여 보안과 접근성을 함께 관리할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **층 레벨**을 클릭하세요.
2. 화면 오른쪽 상단의 **층 레벨 추가** 버튼을 클릭하세요.



3. **층 레벨 추가** 패널이 나타나면 **이름** 및 **설명**(선택 사항)을 입력하세요.

   > *예, 보안팀, 청소 인력*



4. **층 추가** 섹션에서 층 레벨을 적용할 층을 선택하세요.
5. **스케줄** 섹션에서 출입 스케줄을 설정하세요.

   > *예, 청소 인력의 경우 업무 시간 외에만 출입을 허용하세요.*

6. 필요하다면 **휴일 그룹**을 추가해 특정 일자의 출입을 제한하세요.
7. 층 레벨을 추가하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
> 층 레벨 추가 및 수정, 삭제에 대한 자세한 내용은 층 레벨 관리하기를 참고하세요.

출입 권한

출입 권한 관리는 보안 시스템의 핵심입니다. 휴일 그룹, 스케줄, 출입 레벨, 층 레벨을 조합하여 사용자가 언제, 어디서 출입할 수 있는지를 세밀하게 제어하세요.

> **팁**
> 출입 권한 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

휴일 그룹 관리하기

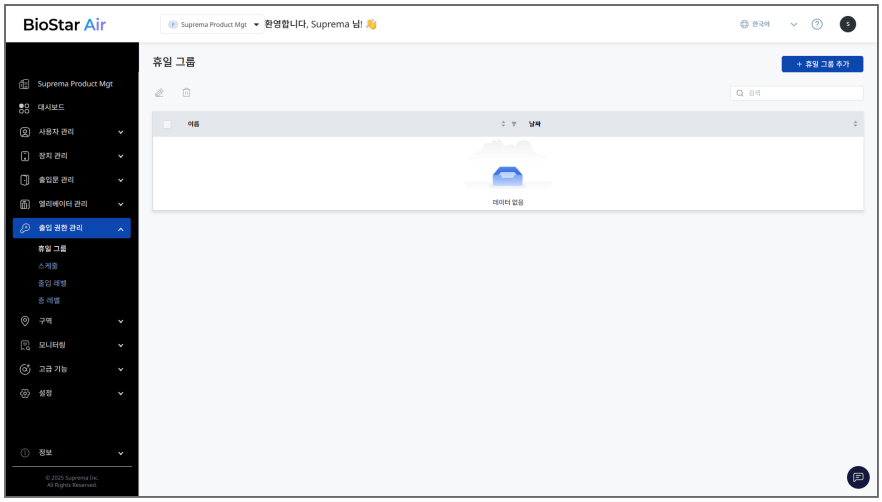
BioStar Air에서 휴일 그룹은 특정 날짜나 기간 동안 출입 규칙을 조정하는 데 사용됩니다. 휴일 그룹을 설정하면 관리자는 공휴일이나 특별한 날에 출입 권한을 제한하거나 변경할 수 있습니다. 이를 통해 보안 수준을 유지하면서도 유연한 출입 통제를 구현할 수 있습니다.

> **팁**
> 출입 통제 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

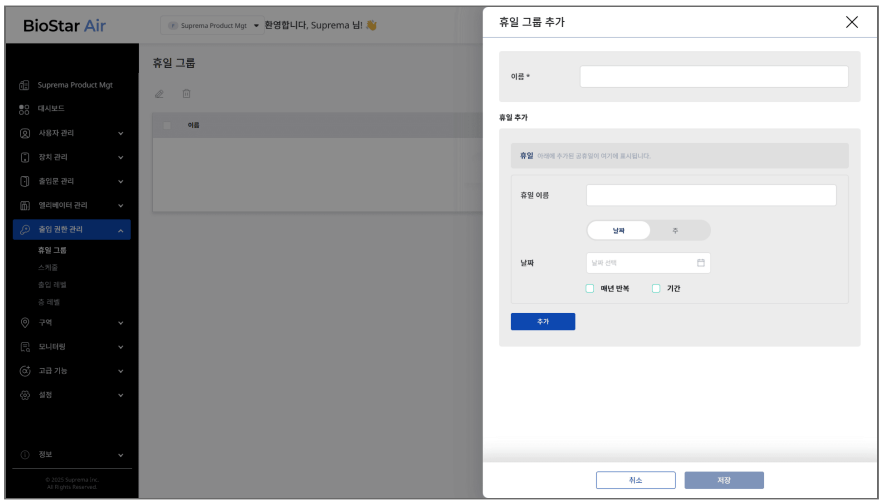
휴일 그룹 추가

휴일 그룹은 매년 반복되는 공휴일과 특정 기간의 휴일을 정의하여 해당 기간 동안 출입 권한을 제한하거나 변경하는 데 사용됩니다.

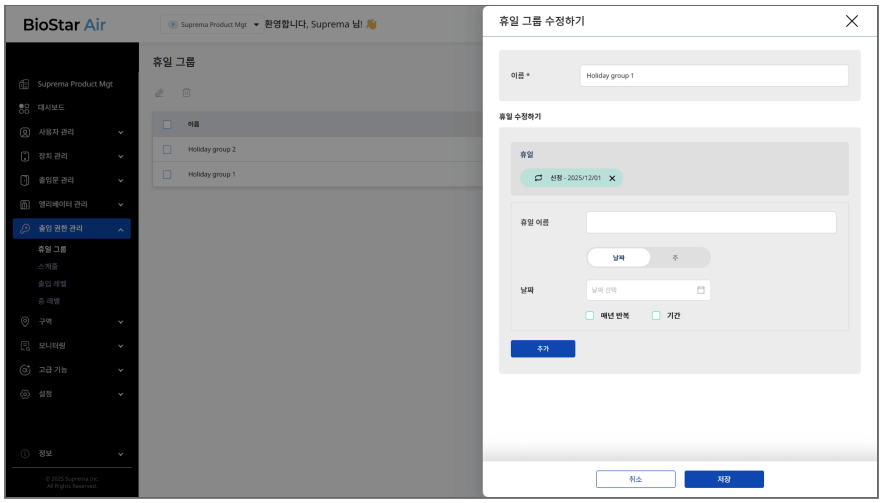
1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **휴일 그룹**를 클릭하세요.
2. 화면 오른쪽 상단의 **휴일 그룹 추가** 버튼을 클릭하세요.



3. **휴일 그룹 추가** 패널이 나타나면 그룹 이름을 입력하세요.



4. **휴일 추가** 섹션에서 휴일 이름과 날짜를 지정하고 **추가** 버튼을 클릭하세요.
    - 날짜가 고정된 공휴일을 추가하려면 이름과 날짜를 설정하고, **매년 반복** 옵션을 선택하세요.
    - 매년 반복되지만 일정한 기간을 갖는 휴일이라면 이름과 날짜를 설정하고, **기간** 옵션을 선택하세요.
5. 같은 방식으로 다른 휴일을 추가하세요.

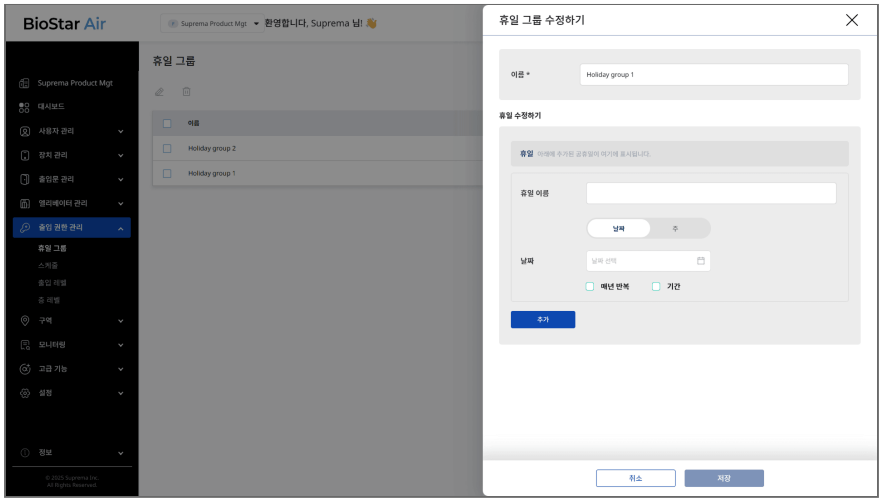


6. 휴일 그룹 설정을 저장하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - 휴일 그룹은 스케줄 보다 우선합니다. 항상 출입이 필요한 사용자에게는 제한 없는 출입 권한을 부여하세요.
> - 한 개의 출입문에는 한 개의 휴일 그룹만 적용할 수 있습니다.

휴일 그룹 수정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **휴일 그룹**를 클릭하세요.
2. 목록에서 수정할 휴일 그룹을 클릭하세요. 또는 휴일 그룹의 체크박스를 클릭해 선택한 후 목록 상단의 버튼을 클릭하세요.
3. **휴일 그룹 수정하기** 패널이 나타나면 원하는 항목을 수정하세요.



4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

휴일 그룹 삭제

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **휴일 그룹**를 클릭하세요.
2. 목록에서 휴일 그룹의 체크박스를 클릭하세요. 1개 이상의 휴일 그룹을 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

스케줄 관리하기

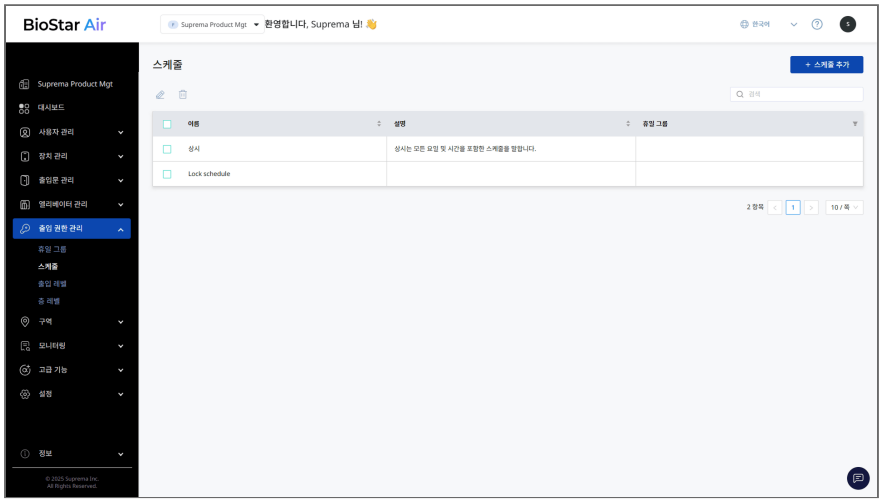
스케줄을 생성하여 특정 요일과 시간대에 출입문이나 엘리베이터의 출입을 허용하거나 제한하세요. 휴일 그룹과 함께 사용하면 출입 규칙을 더욱 세밀하게 조정할 수 있습니다.

알아두기

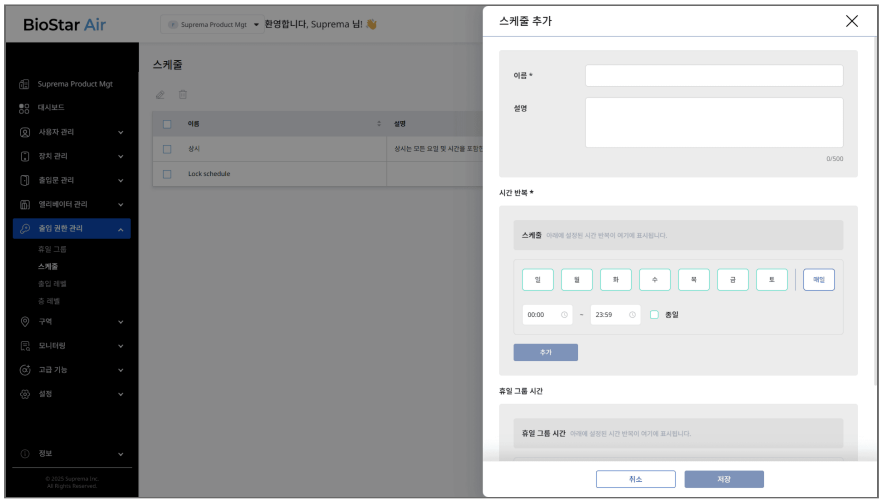
- 휴일 그룹은 스케줄 보다 우선합니다. 항상 출입이 필요한 사용자에게는 제한 없는 출입 권한을 부여하세요.
- 휴일 그룹 설정에 대한 자세한 내용은 휴일 그룹 관리하기를 참고하세요.
- 출입문에 스케줄을 적용하는 방법에 대한 자세한 내용은 출입문 스케줄 관리하기를 참고하세요.
- 엘리베이터의 층마다 출입을 제어하는 스케줄 설정에 대한 자세한 내용은 엘리베이터를 참고하세요.

스케줄 추가

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **스케줄**을 클릭하세요.
2. 화면 오른쪽 상단의 **스케줄 추가** 버튼을 클릭하세요.



3. **스케줄 추가** 패널이 나타나면 **이름**과 **설명**(선택 사항)을 입력하세요.

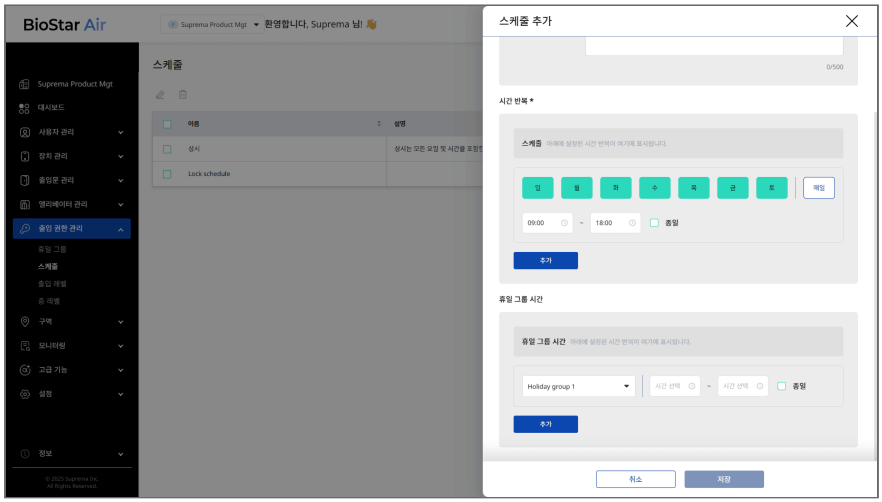


4. **시간 반복 *** 섹션에서 요일과 시간을 선택하세요.

> *예를 들어, 근무 시간을 설정하려면 월요일부터 금요일까지, 오전 9시부터 오후 6시까지 선택하세요. 반대로 근무 시간이 아닌 스케줄을 설정하려면 토요일과 일요일, 또는 매일 오후 6시부터 다음 날 오전 9시까지 선택하세요.*

5. 선택한 일정을 적용하려면 **추가** 버튼을 클릭하세요.

6. **휴일 그룹 시간** 섹션에서 스케줄에 적용할 휴일 그룹을 선택하고 시간을 설정하세요.



7. 휴일 그룹을 적용하려면 **추가** 버튼을 클릭하세요.

8. 스케줄을 추가하려면 **저장** 버튼을 클릭하세요.

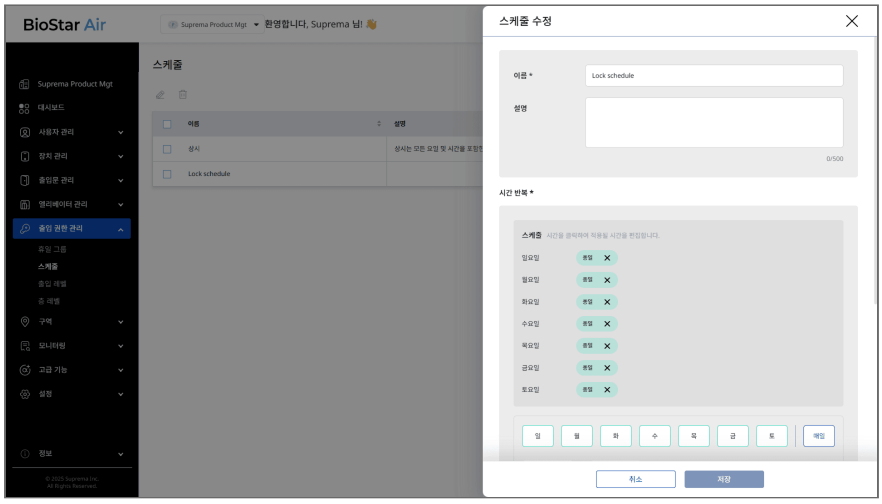
> **알아두기**
>
> - 출입을 허용하는 열림 스케줄과 출입을 제한하는 잠김 스케줄을 추가하여 출입문에 적용할 수 있습니다. 출입문에 스케줄을 적용하는 방법에 대한 자세한 내용은 출입문 스케줄 관리하기를 참고하세요.
> - 하나의 스케줄에는 한 개의 휴일 그룹만 적용할 수 있습니다.
> - 엘리베이터의 층마다 출입을 제어하는 스케줄 설정에 대한 자세한 내용은 엘리베이터를 참고하세요.

스케줄 수정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **스케줄**을 클릭하세요.

2. 목록에서 수정할 스케줄을 클릭하세요. 또는 스케줄의 체크박스를 클릭하고 목록 상단의 버튼을 클릭하세요.

3. **스케줄 수정** 패널이 나타나면 필요한 정보를 변경하거나 일정을 수정하세요.



4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

스케줄 삭제

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **스케줄**을 클릭하세요.

2. 목록에서 삭제할 스케줄의 체크박스를 클릭하세요. 1개 이상의 스케줄을 선택할 수 있습니다.

3. 목록 상단의 버튼을 클릭하세요.

4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

> **알아두기**
> 스케줄을 삭제하면 모든 관련 섹션에서 스케줄이 제거됩니다. 예를 들어, 출입문이나 엘리베이터에 적용된 스케줄이 삭제되면 해당 출입문이나 엘리베이터에서 더 이상 스케줄이 적용되지 않습니다.

출입 레벨 관리하기

출입 레벨을 사용하여 사용자의 출입 권한을 세밀하게 제어하세요. 출입 레벨은 누가, 언제, 어디서 출입할 수 있는지를 정의하는 중요한 요소입니다. 출입 레벨은 아래와 같은 요소로 구성됩니다.

- **출입문 / 출입문 그룹**: 출입을 허용하는 위치
- **스케줄**: 출입을 허용하는 시간
- **휴일 그룹**: 출입을 제한하거나 조정하는 날짜 및 기간

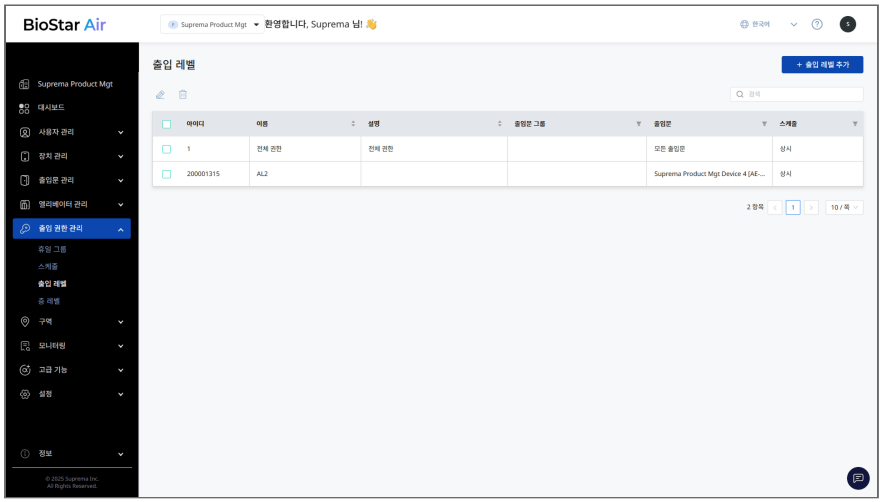
출입 레벨은 사용자를 추가하기 전에 설정해야 사용자 관리 프로세스를 간소화할 수 있습니다.

출입 레벨 추가

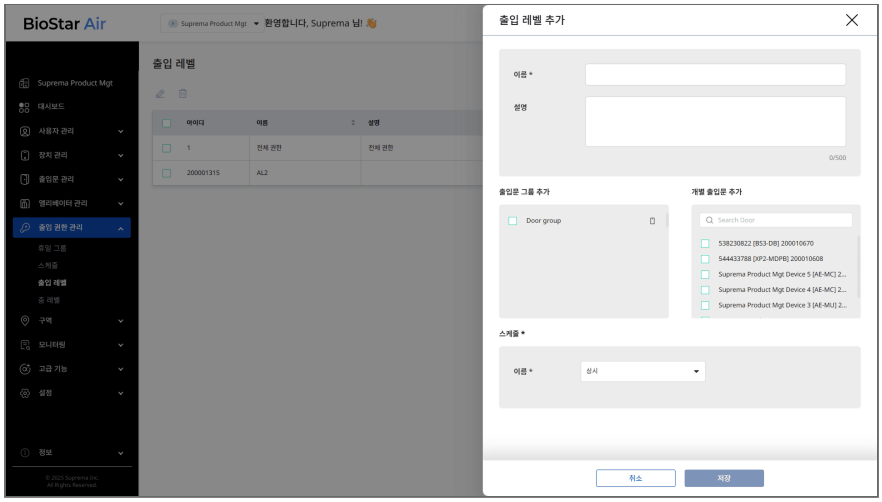
출입 레벨을 통해 출입문, 스케줄 및 휴일에 따라 사용자의 권한을 설정할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **출입 레벨**을 클릭하세요.

2. 화면 오른쪽 상단의 **출입 레벨 추가** 버튼을 클릭하세요.



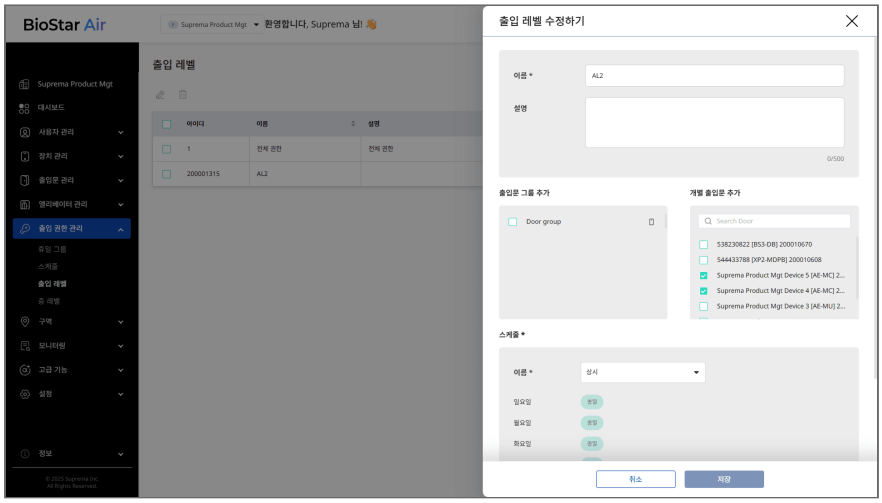
3. **출입 레벨 추가** 패널이 나타나면 **이름** 및 **설명**(선택 사항)을 입력하세요.



4. **출입문 그룹 추가** 또는 **개별 출입문 추가** 섹션에서 출입문 그룹 또는 개별 출입문을 선택하세요.
5. **스케줄** 섹션에서 출입 레벨에 적용할 스케줄을 선택하세요. 제한 없는 출입을 허용하려면 **상시**를 선택하세요.
6. 출입 레벨을 추가하려면 **저장** 버튼을 클릭하세요.

출입 레벨 수정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **출입 레벨**을 클릭하세요.
2. 목록에서 수정할 출입 레벨을 클릭하세요. 또는 수정할 출입 레벨의 체크박스를 클릭하고 목록 상단의 ✎ 버튼을 클릭하세요.



3. **출입 레벨 수정하기** 패널이 나타나면 필요한 정보를 수정하거나 설정을 변경하세요.
4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

출입 레벨 삭제

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **출입 레벨**을 클릭하세요.
2. 목록에서 삭제할 출입 레벨의 체크박스를 클릭하세요. 1개 이상의 출입 레벨을 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

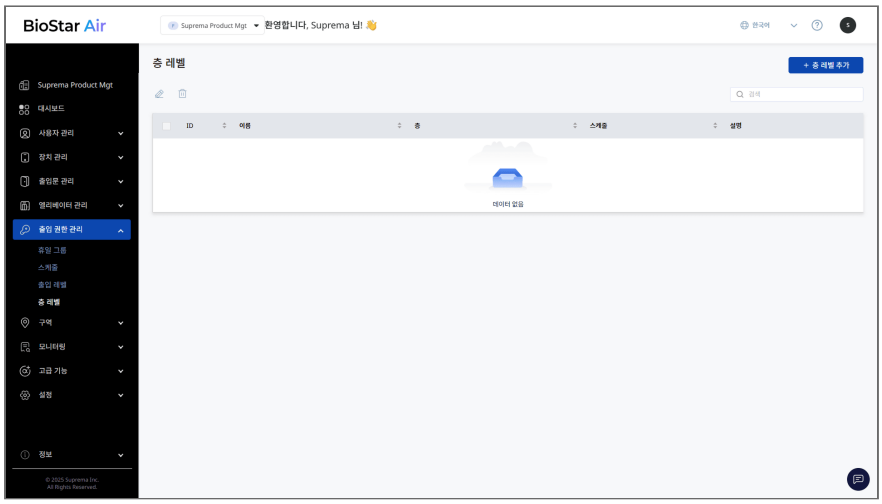
층 레벨 관리하기

층 레벨은 엘리베이터 출입 통제 설정에서 사용됩니다. 층 레벨을 통해 각 층에 대한 출입 권한을 세밀하게 제어할 수 있습니다. 예를 들어, 특정 사용자 그룹이 특정 층에만 출입할 수 있도록 설정할 수 있습니다.

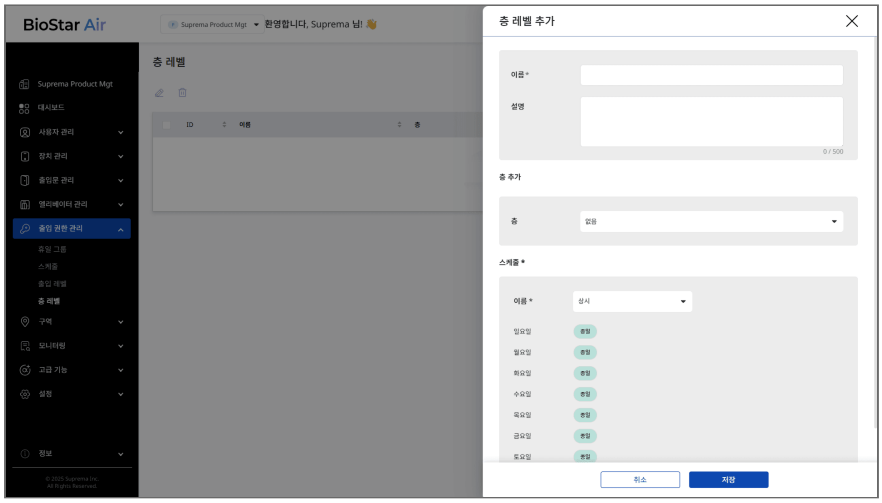
층 레벨 추가

특정 층에 출입할 수 있는 사용자 또는 그룹을 설정하세요.

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **층 레벨**을 클릭하세요.
2. 화면 오른쪽 상단의 **층 레벨 추가** 버튼을 클릭하세요.



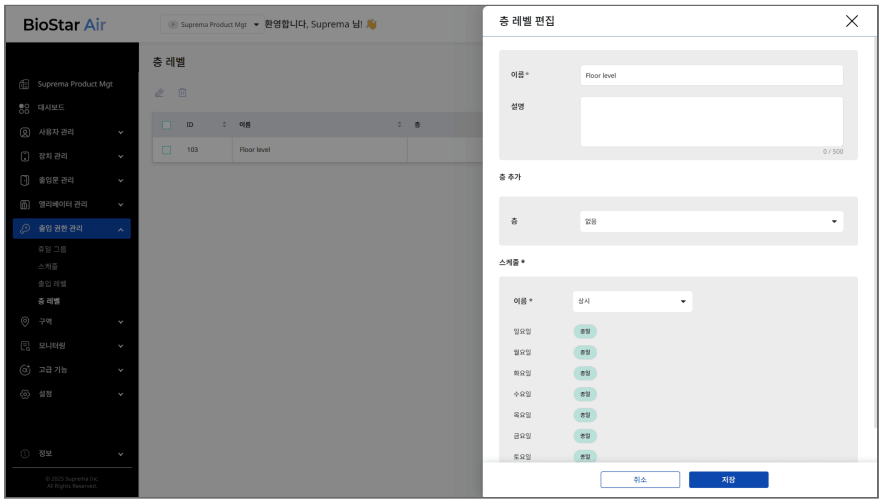
3. **층 레벨 추가** 패널이 나타나면 **이름** 및 **설명**(선택 사항)을 입력하세요.



4. **층 추가** 섹션에서 층 권한을 적용할 층을 선택하세요.
5. **스케줄** 섹션에서 층 레벨에 적용할 스케줄을 선택하세요. 제한 없는 출입을 허용하려면 **상시**를 선택하세요.
6. 층 레벨을 추가하려면 **저장** 버튼을 클릭하세요.

층 레벨 수정

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **층 레벨**을 클릭하세요.
2. 목록에서 수정할 층 레벨을 클릭하세요. 또는 수정할 층 레벨의 체크박스를 클릭하고 목록 상단의 버튼을 클릭하세요.



3. **층 레벨 편집** 패널이 나타나면 필요한 정보를 수정하거나 설정을 변경하세요.
4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

층 레벨 삭제

1. 화면 왼쪽 사이드바에서 **출입 권한 관리** → **층 레벨**을 클릭하세요.
2. 목록에서 삭제할 층 레벨의 체크박스를 클릭하세요. 1개 이상의 층 레벨을 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 경고 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

구역 관리

구역(Zone)은 출입문과 장치를 논리적으로 묶은 단위로, 안티패스백(Anti-passback, APB) 적용, 현장 체류 상태 확인, 인원 집계는 물론 앞으로 추가될 다양한 기능에도 활용할 수 있습니다.

구역과 안티패스백(APB)의 이해

구역에 안티패스백 기능을 적용하려면 먼저 관리자가 해당 구역의 출입 지점(입실 지점과 퇴실 지점)을 설정해야 합니다. 이 설정을 기준으로 사용자가 구역 안에 있는지 밖에 있는지 판단합니다. 구역에서 퇴실하지 않은 사용자는 다른 인증 수단을 사용하더라도 같은 구역에 다시 들어갈 수 없습니다. 또한 안티패스백 기능은 입실과 퇴실 지점을 명확하게 정의하는 데도 활용되며, 사용자가 왔던 길로 되돌아가거나 들어왔던 출입문으로 나가는 것을 막아 줍니다.

경계 구역(Perimeter Zone)

BioStar Air는 안티패스백과 마찬가지로 사용자의 현장 체류 상태를 파악할 수 있도록 **경계 구역**(Perimeter Zone)이라는 개념을 제공합니다. 경계 구역은 **현장 체류 인원 확인**(On-Site Now)과 **비상 호출**(Roll Call) 기능에서 핵심적인 역할을 합니다. 필요하다면 경계 구역에도 안티패스백 기능을 적용할 수 있습니다.

다음 제공하는 문서를 통해 BioStar Air 포털에서 구역과 APB 위반을 관리하는 방법을 알아보세요.

구역 관리하기

BioStar Air의 **구역**(Zone) 기능을 사용하면 출입문을 논리적인 구역으로 구성하고, 필요에 따라 **안티패스백**(Anti-Passback, APB) 규칙을 적용해 사용자가 올바른 순서로 입실 및 퇴실하도록 강제할 수 있습니다. 안티패스백 규칙은 구역마다 선택적으로 적용할 수 있으며, 적용하지 않은 구역도 내부 인원 확인 등 다른 구역 기능은 그대로 사용할 수 있습니다. **구역**은 사이트 전체를 아우르는 경계 구역부터 건물 내부의 특정 구역까지 자유롭게 구성할 수 있습니다.

시작하기 전에

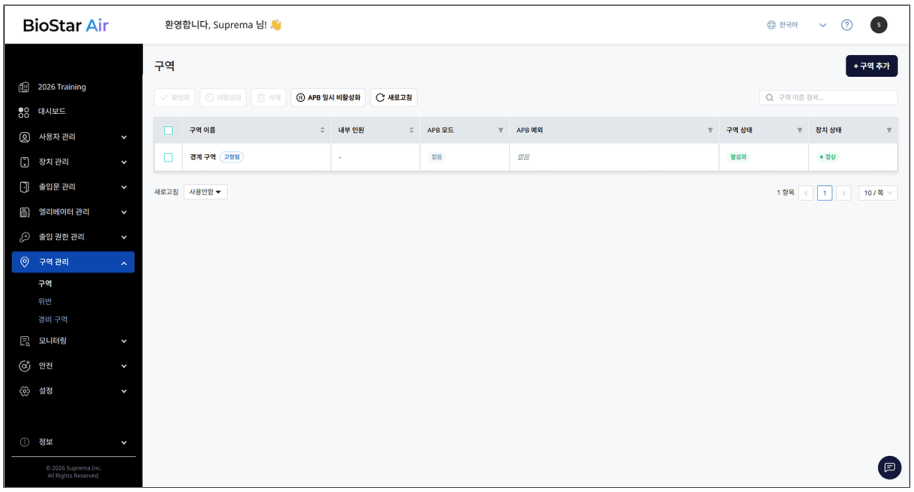
구역을 생성하기 전에 다음 사항을 확인하세요.

- 구역에 할당할 출입문이 먼저 등록되어 있어야 합니다. 출입문 등록 방법은 등록 출입문 관리하기를 참고하세요.
- 한 개의 장치는 한 번에 하나의 구역에서만 사용할 수 있습니다.
- 구역의 입실 및 퇴실 장치를 변경해도 출입문 자체의 설정은 변경되지 않습니다.
- 구역의 입실 및 퇴실 장치가 올바르게 구성되지 않으면 APB 동작과 내부 인원 수가 실제 이동과 다르게 표시될 수 있습니다.
- 오프라인 장치는 온라인 장치보다 변경 사항 적용이 늦어질 수 있습니다. 변경 사항은 온라인 장치에 먼저 적용되고, 오프라인 장치는 다시 온라인으로 연결된 후에 적용됩니다.
- 펌웨어가 **v2.13** 이상인 장치만 구역에 할당할 수 있습니다. 구역에 할당하려는 장치가 최신 펌웨어인지 확인하세요.
- APB 구역에 사용 중인 출입문은 설정 충돌을 막기 위해 보호됩니다. 출입문 설정 중 APB 동작에 영향을 주는 항목을 변경하려면 먼저 해당 출입문을 구역에서 제외하세요.

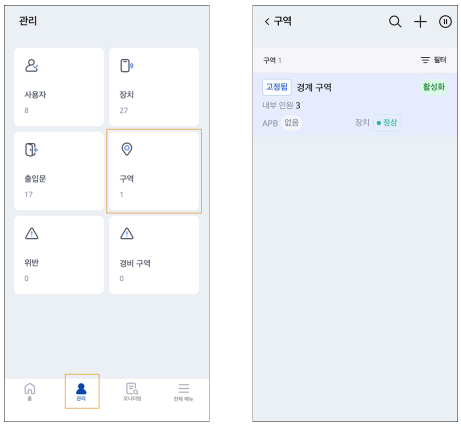
구역 목록 살펴보기

Web

화면 왼쪽 사이드바에서 **구역 관리** → **구역**을 클릭하세요.



Mobile



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 화면 하단의 **관리**를 탭하세요.
3. **구역** 카드를 탭하세요.

구역 목록에서는 사이트에 구성된 모든 구역을 한눈에 확인할 수 있습니다.

- **구역 이름**: 구역 이름입니다. **경계 구역**은 이름 옆에 **고정됨** 배지가 표시됩니다.
- **내부 인원**: 현재 해당 구역 안에 있는 것으로 기록된 사용자 수입니다. 자세한 내용은 내부 인원 확인을 참고하세요.
- **APB 모드**: 구역에 적용된 APB 모드(**Hard**/**Soft**/**없음**)입니다.
- **APB 예외**: 구역에 지정된 APB 예외 그룹입니다.
- **구역 상태**: 구역의 활성화 여부입니다.
- **장치 상태**: 구역에 할당된 장치들의 온라인 상태입니다.

> **경계 구역과 내부 구역**
>
> 사이트를 처음 구성하면 **경계 구역**(Perimeter Zone)이 기본 제공됩니다. **경계 구역**은 사이트의 대문과 같은 구역으로, 이름 변경이나 삭제가 불가능하며 목록에 **고정됨** 배지로 표시됩니다.
>
> - **경계 구역**에서 사용하는 입실 및 퇴실 장치는 **대시보드** 메뉴의 **현장 사용자**와 **안전** → **재실** 메뉴에서 재실 상태를 계산하는 기준이 되기도 합니다.
> - 경계 구역 외에도 내부 통제가 필요한 영역(예: 서버실, 특정 층)마다 별도의 구역을 추가 생성해, 사이트 안에서도 세밀한 이동 통제를 적용할 수 있습니다.

내부 인원 확인

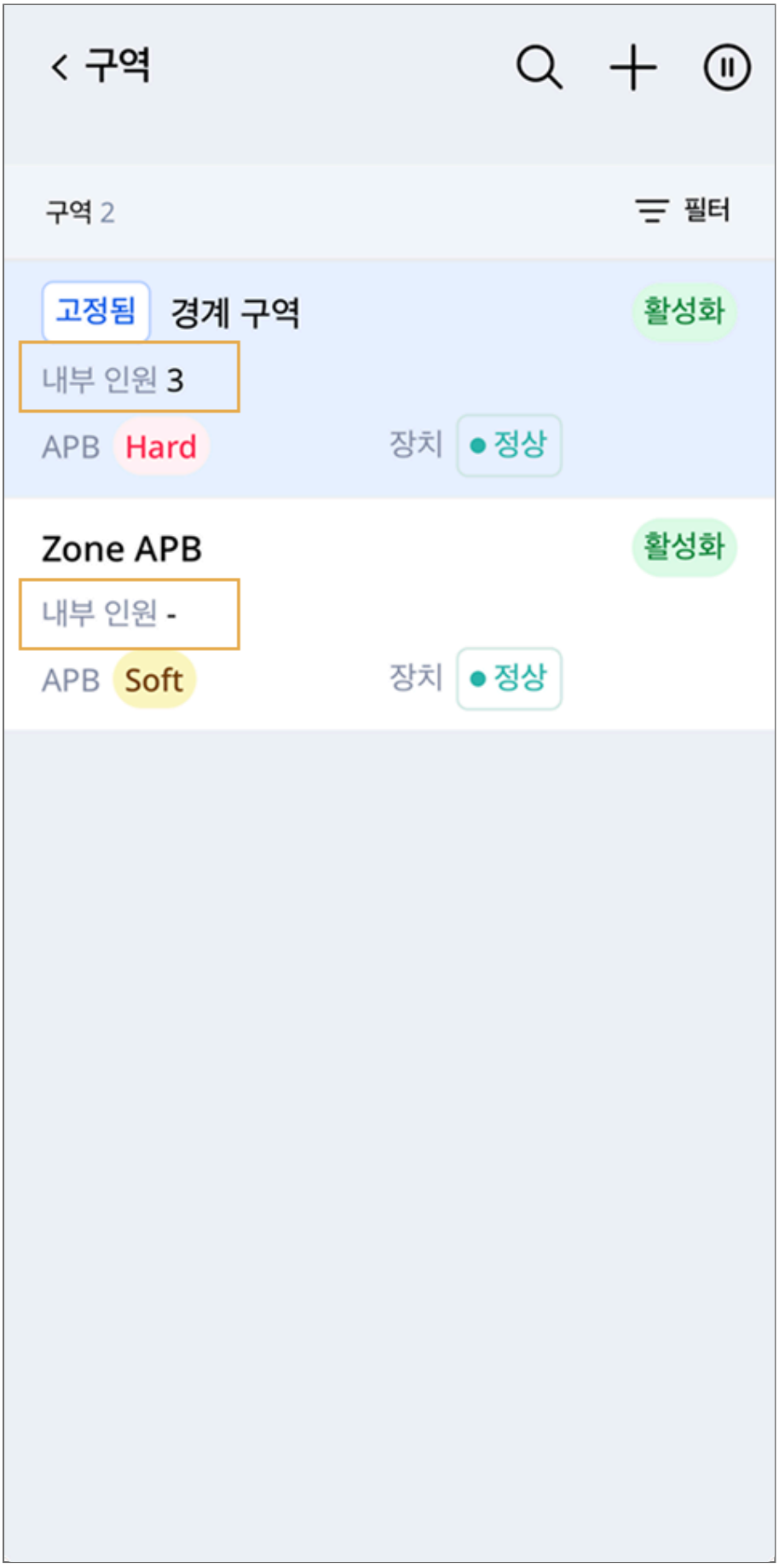
Web

구역 목록의 **내부 인원** 열에서 각 구역에 현재 몇 명이 있는지 확인할 수 있습니다.



Mobile

구역 목록의 **내부 인원** 항목에서 각 구역에 현재 몇 명이 있는지 확인할 수 있습니다.

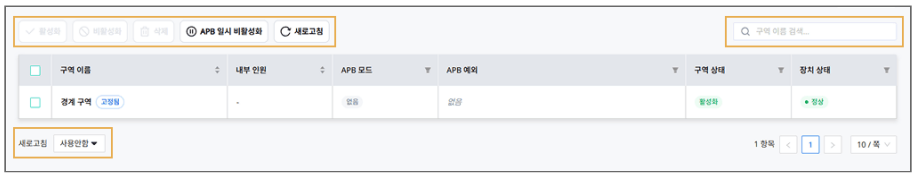


- 이 수치는 구역에 설정한 입실 및 퇴실 장치의 인증 기록을 기준으로 계산됩니다. 입실 장치에서 인증하면 인원 수가 늘고, 퇴실 장치에서 인증하면 인원 수가 줄어듭니다.

- APB 예외 그룹에 속한 사용자는 APB 규칙의 적용을 받지 않지만, 내부 인원 수에는 계속 포함됩니다.
- 구역을 비활성화하면 해당 구역의 내부 인원 수는 0으로 초기화됩니다.
- 최신 값을 유지하려면 목록 상단의 **새로고침** 버튼을 클릭하거나 자동 새로고침 간격을 설정하세요.

구역 관리 기능

구역 목록 상단 및 하단에서 제공하는 관리 기능으로 다음 작업을 수행할 수 있습니다.



- **활성화** / **비활성화**: 선택한 구역을 활성화하거나 비활성화할 수 있습니다.
- **삭제**: 선택한 구역을 삭제할 수 있습니다. **경계 구역**은 삭제할 수 없습니다.
- **APB 일시 비활성화**: 경계 구역을 포함한 사이트의 모든 구역에서 APB 적용을 한 번에 멈출 수 있습니다.
- **새로고침**: 목록을 즉시 새로고침해 최신 상태로 갱신합니다. 목록 하단의 **새로고침**에서 자동 새로고침 간격(**사용안함**/**5초**/**1분**)을 선택하면 설정한 주기마다 목록을 자동 갱신합니다.
- **구역 이름 검색…**: 구역 이름으로 목록을 검색합니다.

구역 목록 필터링

Web

목록 상단 헤더의 **APB 모드**, **APB 예외**, **구역 상태**, **장치 상태** 열에 있는 버튼을 클릭하면 해당 조건으로 목록을 필터링할 수 있습니다.



> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 클릭하세요.

Mobile



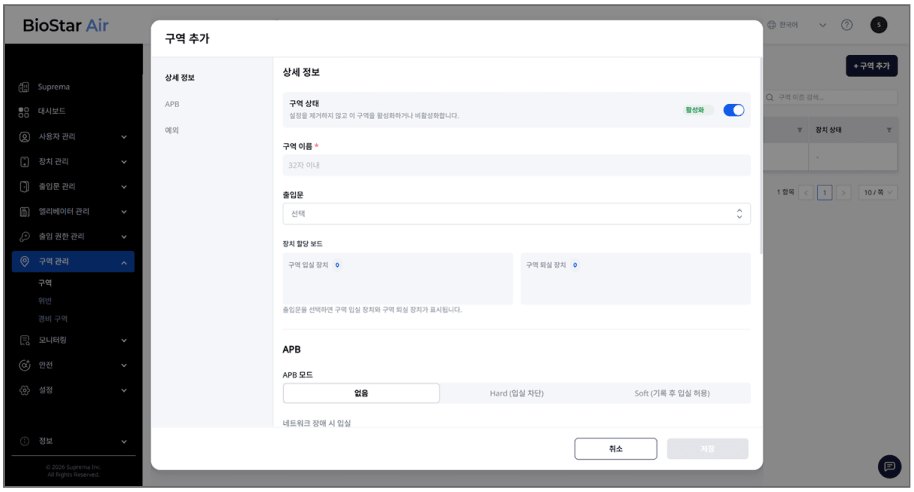
1. 구역 목록 오른쪽 상단의 **필터**를 탭하세요.
2. **APB 모드**, **APB 예외**, **구역 상태**, **장치 상태**에서 원하는 조건을 선택하세요.
3. 선택한 조건으로 목록을 필터링하려면 **저장** 버튼을 탭하세요.

> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 탭하세요.

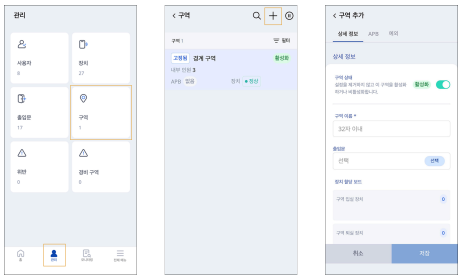
구역 추가

Web

화면 왼쪽 사이드바에서 **구역 관리** → **구역**을 클릭하세요. 화면 오른쪽 상단의 **+ 구역 추가** 버튼을 클릭하세요.



Mobile



1. BioStar Air 앱 화면 하단의 **관리**를 탭하세요.
2. **구역** 카드를 탭하세요.
3. 화면 오른쪽 상단의 ＋ 버튼을 탭하세요.

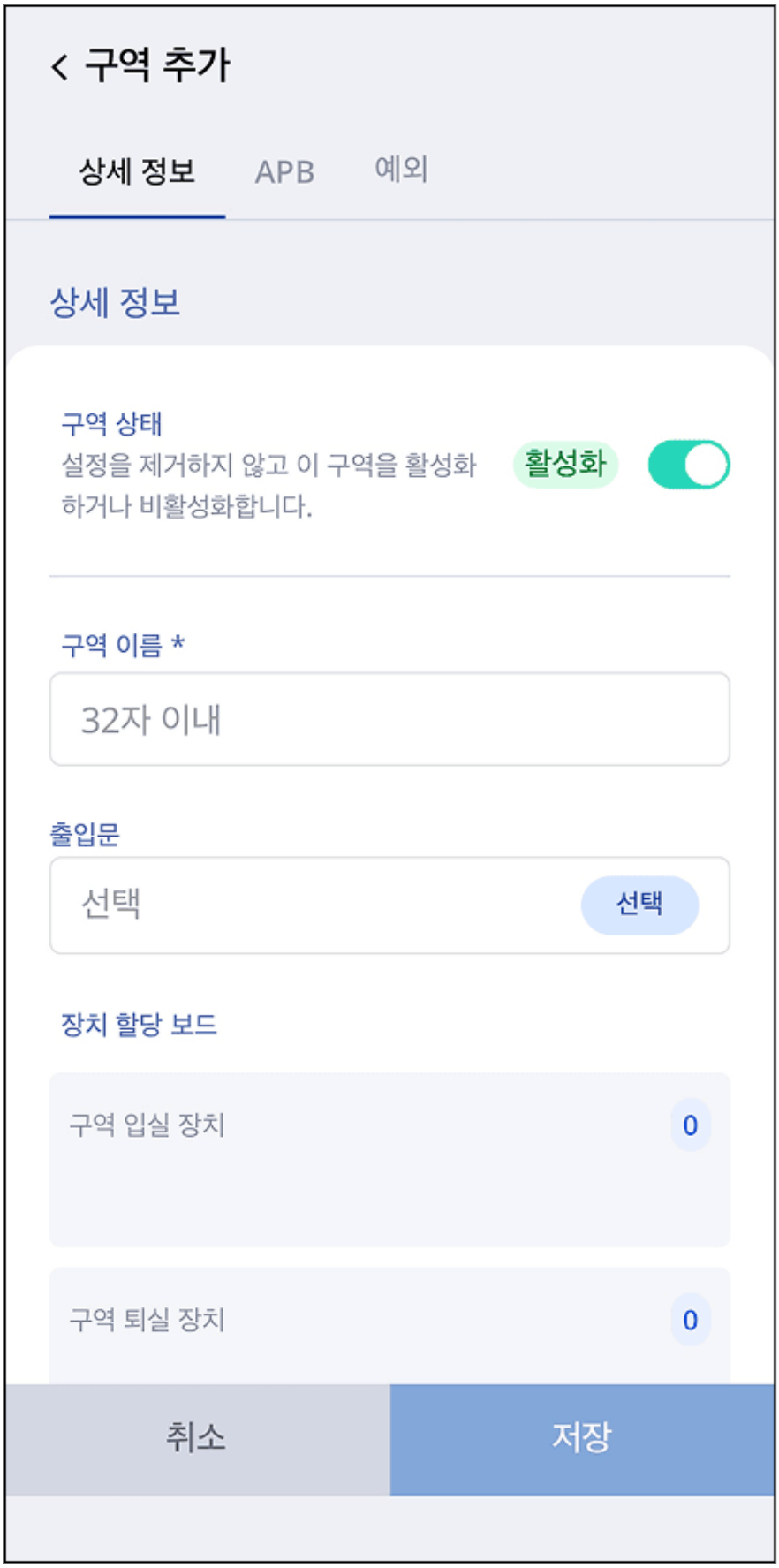
1 기본 정보 입력

상세 정보 섹션에서 구역의 기본 정보를 입력하세요.

Web


상세 정보
구역 상태
설정을 제거하지 않고 이 구역을 활성화하거나 비활성화합니다.
활성화
구역 이름 *
경계 구역
외부 타이머
사용자가 이 시간 동안 활동이 없고 퇴실 리더를 사용하지 않은 경우 자동으로 외부에 있는 것으로 표시합니다.
경계 전용
12
분
시간
일

Mobile



- **구역 상태**: 구역을 바로 활성화할지 선택하세요. 설정을 유지한 채로 나중에 활성하거나 비활성화할 수 있습니다.
- **구역 이름**: 32자 이내로 입력하세요. 여러 건물이 있는 사이트에서는 위치를 바로 알 수 있는 이름을 사용하기를 권장합니다.

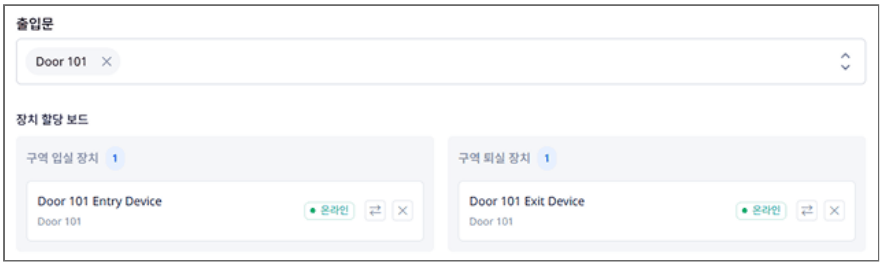
- **외부 타이머**: 설정한 시간 동안 활동이 없고 퇴실 장치도 사용하지 않은 사용자는 **외부** 상태로 자동 전환합니다. 경계 구역에 퇴실 장치를 지정하지 않았다면 반드시 설정해야 합니다.

> **알아두기**
> **외부 타이머** 옵션은 경계 구역 설정 시에만 표시되는 전용 옵션입니다.

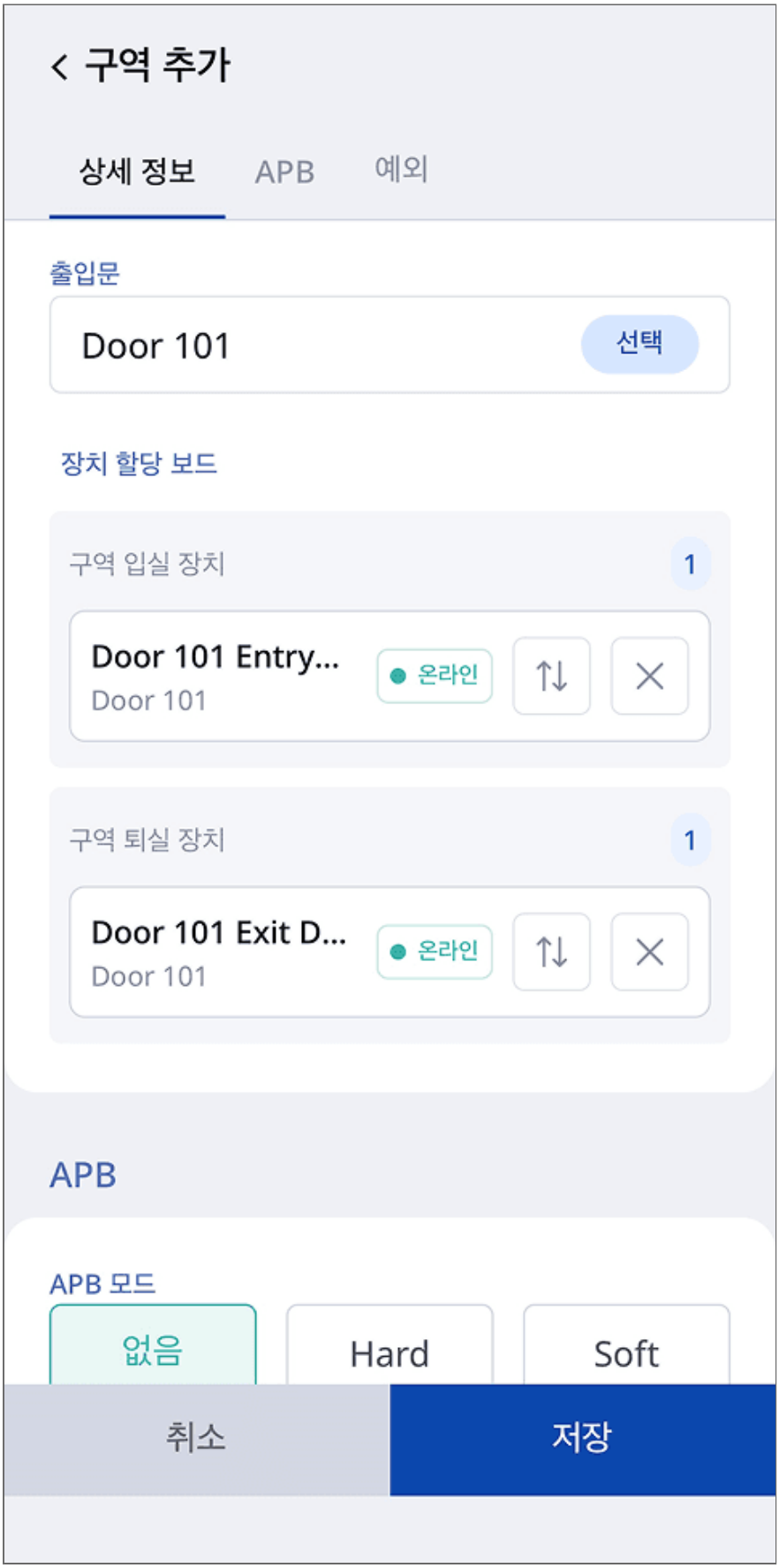
2 출입문 및 장치 할당

구역에 할당할 출입문과 장치를 선택하세요.

Web



Mobile



- **출입문**: 구역에 포함할 출입문을 선택하세요. 1개 이상의 출입문을 선택할 수 있습니다. 출입문을 선택하면 해당 출입문의 장치가 **장치 할당 보드**에 나타납니다.
- **장치 할당 보드**: 각 장치를 **구역 입실 장치** 또는 **구역 퇴실 장치**로 지정하세요. 장치는 **장치 아이디**로 구분되어 표시됩니다. 이동(⇄)

버튼을 클릭해 장치를 입실 또는 퇴실 장치로 옮길 수 있습니다.

> **알아두기**
>
> - 펌웨어가 v2.13 이상인 장치만 **장치 할당 보드**에 나타납니다. 구역에 할당하려는 장치가 최신 펌웨어인지 반드시 확인하세요.
> - 장치 관리에 대한 자세한 내용은 장치 및 패널 그룹 관리하기를 참고하세요.
> - 출입문 관리에 대한 자세한 내용은 등록 출입문 관리하기를 참고하세요.

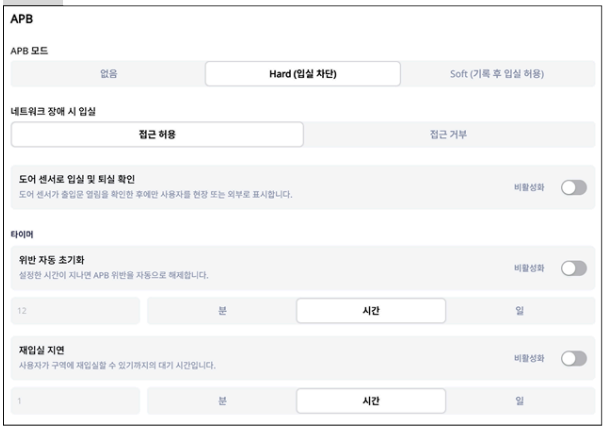
3 APB 모드 설정

APB 섹션에서 안티패스백 규칙을 설정하세요. 안티패스백 규칙 적용은 선택 사항이므로, 구역 내 이동을 엄격하게 통제할 필요가 없다면 **없음** 모드를 선택해 내부 인원 확인 용도로만 구역을 사용할 수 있습니다.

Hard

Hard (입실 차단)

Web



Mobile



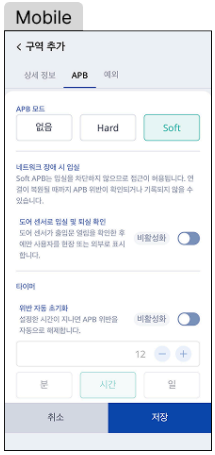
Soft

Soft (기록 후 입실 허용)

Web



Mobile



- **APB 모드**: 원하는 APB 모드를 선택하세요.
  - **Hard (입실 차단)**: 사용자가 APB 규칙을 위반하면 출입을 차단하고 이벤트 로그에 위반으로 기록합니다.

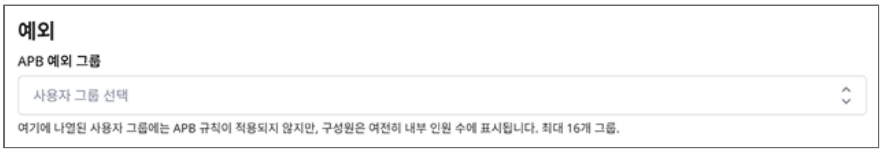
  - **Soft (기록 후 입실 허용)**: 출입은 허용하되 이벤트 로그에 APB 위반으로 기록합니다.
  - **없음**: 구역에 APB를 적용하지 않습니다. APB 모드를 설정하지 않은 구역은 내부 인원을 계산하는 용도로 계속 사용됩니다.

- **네트워크 장애 시 입실**: 네트워크 장애로 BioStar Air 서버와 통신할 수 없을 때 접근을 허용할지 거부할지 선택하세요. **Soft** 모드에서는 출입을 막지 않으므로 접근이 항상 허용되며, 네트워크 연결이 복구될 때까지 위반이 확인되거나 기록되지 않을 수 있습니다.
- **도어 센서로 입실 및 퇴실 확인**: 이 옵션을 활성화하면 도어 센서가 출입문 열림을 확인한 후에만 사용자를 **현장** 또는 **외부** 상태로 표시합니다.
- **타이머**
  - **위반 자동 초기화**: 설정한 시간이 지나면 APB 위반을 자동 해제합니다.
  - **재입실 지연**: 사용자가 같은 구역에 다시 입실할 수 있을 때까지의 대기 시간입니다.

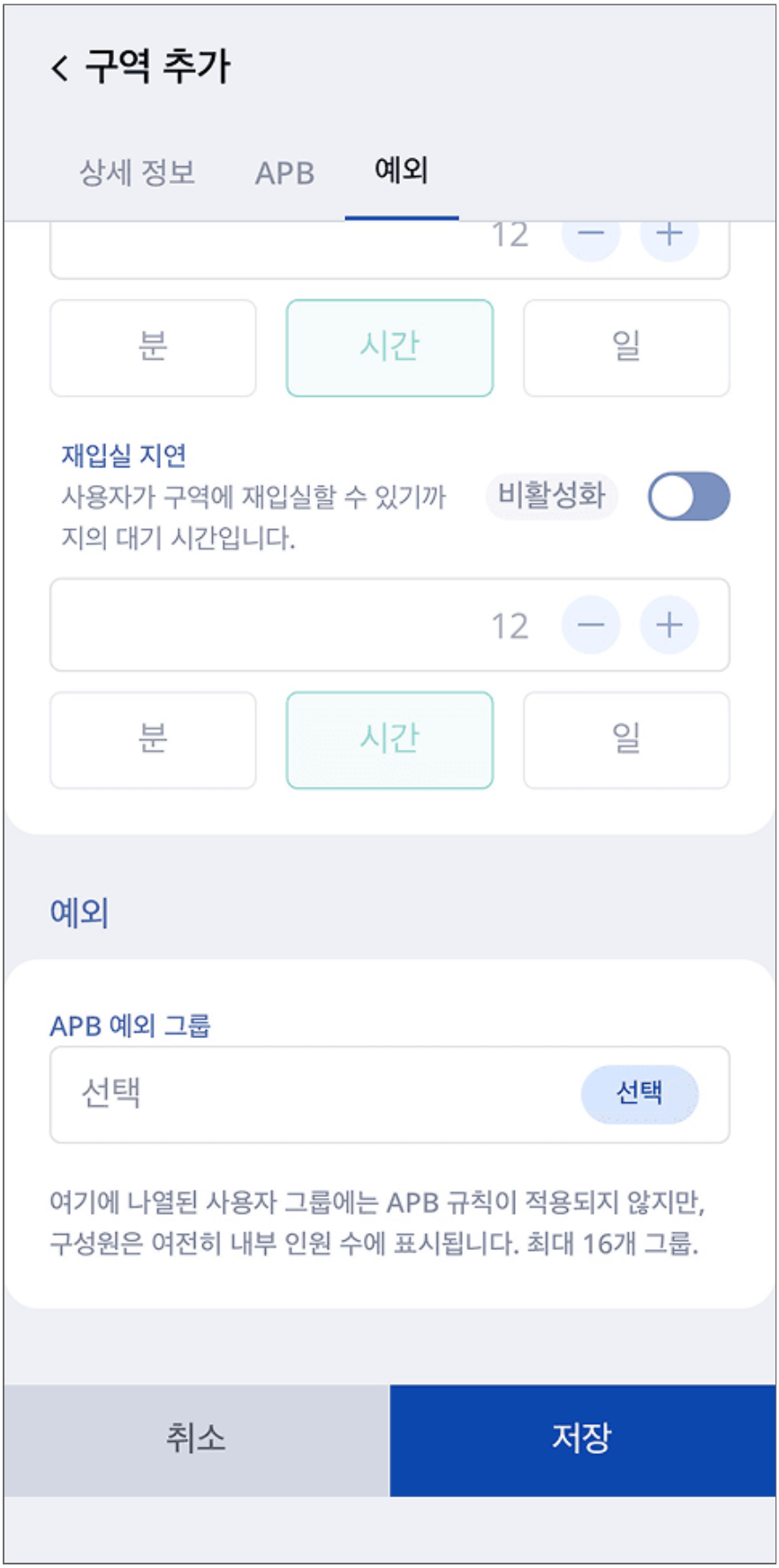
4 예외 설정

예외 섹션에서 APB 규칙을 적용하지 않을 사용자 그룹을 선택할 수 있습니다.

Web



Mobile



- 구역당 최대 16개의 사용자 그룹을 예외로 지정할 수 있습니다.
- 예외 그룹에 속한 사용자는 APB 규칙의 적용을 받지 않지만, 내부 인원 수에는 계속 포함됩니다.

- **APB 모드**가 **없음**이면 **예외** 섹션은 비활성화됩니다.

> **알아두기**
> 사용자 그룹 관리에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

5 구역 저장

구역 설정을 저장하려면 **저장** 버튼을 클릭하세요.

> **구역 추가 시 참고 사항**
> - 이미 다른 APB 구역에 모두 할당된 출입문이거나 장치가 없는 출입문, 에어팝 패치(Airfob Patch) 전용 출입문은 출입문 선택 목록에 나타나지 않습니다.
> - 퇴실 장치를 지정하지 않는 구역은 **위반 자동 초기화**(경계 구역이 아닌 경우) 또는 **외부 타이머**(경계 구역인 경우)를 반드시 활성화해야 저장할 수 있습니다.
> - 동일한 이름의 구역은 만들 수 없습니다.
> - 구역 설정 시 **APB 모드**를 **없음**으로 변경하면 해당 구역에 저장되어 있던 세부 설정(**APB 모드**, **타이머**, **APB 예외 그룹**)이 모두 초기화됩니다. 설정을 유지한 채로 APB 적용만 잠시 멈추려면 구역 비활성화 또는 APB 일시 비활성화 기능을 사용하세요.

구역 활성화/비활성화

구역을 활성화하거나 비활성화할 수 있습니다. 설정 값은 제거되지 않고 그대로 유지됩니다. 구역을 비활성화하면 해당 구역의 내부 인원 수가 0으로 초기화됩니다. 다만 이미 발생한 APB 위반은 그대로 남아 있으며, APB 위반 확인하기 메뉴에서 해제할 수 있습니다.

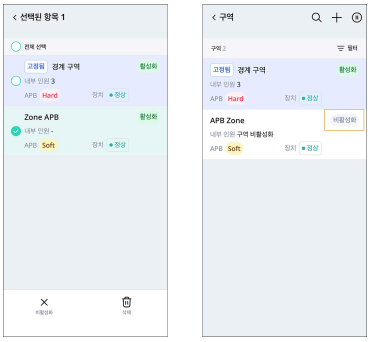
Web

1. 목록에서 활성화 또는 비활성화할 구역의 체크박스를 클릭하세요. 한 개 이상의 구역을 선택할 수 있습니다.
2. 목록 상단의 **활성화** 또는 **비활성화** 버튼을 클릭하세요.
3. 확인 메시지가 나타나면 **활성화** 또는 **비활성화** 버튼을 클릭하세요.

각 구역 활성화 상태는 목록의 **구역 상태** 열에서 확인할 수 있습니다.



Mobile



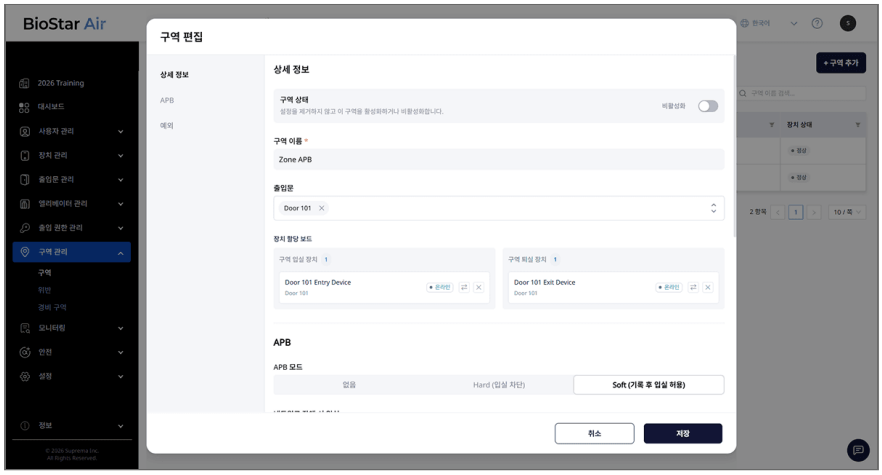
1. 목록에서 활성화 또는 비활성화할 구역을 길게 누르세요.
2. 활성화하거나 비활성화할 구역을 선택하세요. 한 개 이상의 구역을 선택할 수 있습니다.
3. 화면 하단의 **활성화** 또는 **비활성화** 버튼을 탭하세요.
4. 확인 메시지가 나타나면 **활성화** 또는 **비활성화** 버튼을 클릭하세요.

구역 수정

이미 설정된 구역의 상세 정보/APB/예외 설정 등을 수정할 수 있습니다.

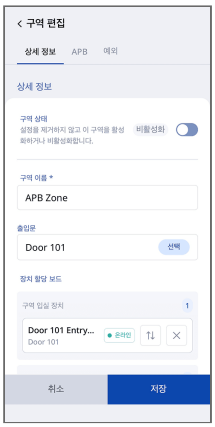
Web

1. 목록에서 수정할 구역을 클릭하세요.
2. **구역 편집** 창이 나타납니다.



3. **상세 정보**/**APB**/**예외** 섹션에서 필요한 항목을 수정하세요.
4. 수정 사항을 저장하려면 **저장** 버튼을 클릭하세요.

Mobile



1. 목록에서 수정할 구역을 탭하세요.
2. **구역 편집** 화면이 나타납니다.
3. **상세 정보**/**APB**/**예외** 섹션에서 필요한 항목을 수정하세요.
4. 수정 사항을 저장하려면 **저장** 버튼을 탭하세요.

> **알아두기**
> **상세 정보**/**APB**/**예외** 섹션의 세부 설정에 대한 자세한 내용은 구역 추가를 참고하세요.

APB 일시 비활성화

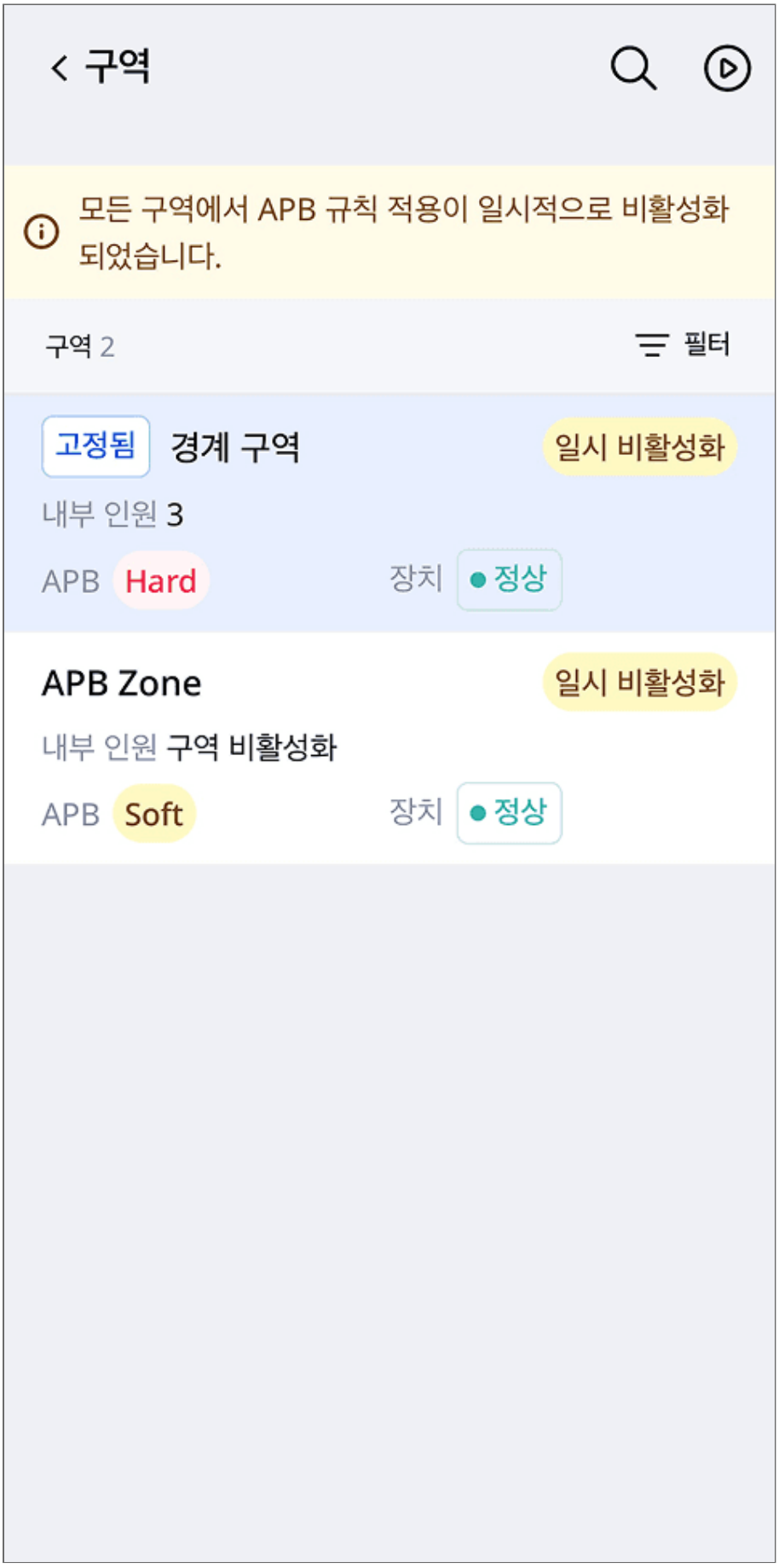
사이트 전체의 APB 적용을 잠시 멈춰야 할 때(예: 특별 행사, 대규모 이동이 예상되는 시간대) 목록 상단의 **APB 일시 비활성화**(⏸) 버튼을 사용하세요. 경계 구역을 포함한 모든 구역의 APB 적용이 중지되며, 재개하면 각 구역은 일시 비활성화 전의 활성화/비활성화 상태로 복원됩니다. 일시 비활성화 중에는 구역 목록이 잠겨 다른 변경을 할 수 없습니다.

구역에 설정된 APB 모드를 다시 시작하려면 **APB 재개**(▶) 버튼을 클릭하세요.

Web



Mobile

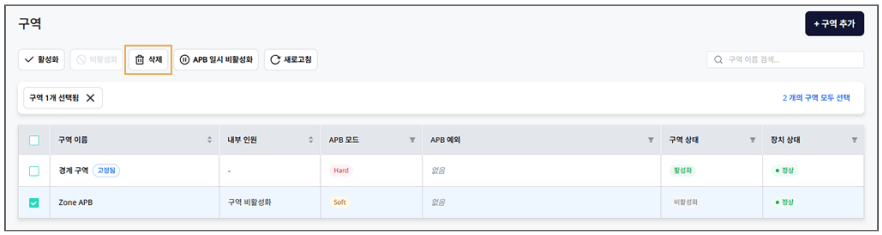

구역
모든 구역에서 APB 규칙 적용이 일시적으로 비활성화 되었습니다.
구역 2
필터
고정됨
경계 구역
일시 비활성화
내부 인원 3
APB
Hard
장치
정상
APB Zone
일시 비활성화
내부 인원 구역 비활성화
APB
Soft
장치
정상

비상 호출(Roll Call)이 진행되는 동안에는 안티패스백 구역을 활성화할 수 없습니다. 비상 호출이 끝난 후 다시 시도하세요. 비상 호출에 대한 자세한 내용은 비상 호출을 참고하세요.

구역 삭제하기

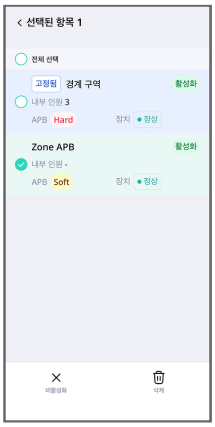
Web

1. 목록에서 삭제할 구역의 체크박스를 클릭하세요. 한 개 이상의 구역을 선택할 수 있습니다.
2. 목록 상단의 **삭제** 버튼을 클릭하세요.



3. 확인 메시지 창이 나타나면 **삭제** 버튼을 클릭하세요.

Mobile



1. 목록에서 삭제할 구역을 길게 누르세요.
2. 삭제할 구역을 선택하세요. 한 개 이상의 구역을 선택할 수 있습니다.
3. 화면 하단의 **삭제** 버튼을 탭하세요.
4. 확인 메시지가 나타나면 **삭제** 버튼을 클릭하세요.

알아두기

- **경계 구역**은 삭제할 수 없습니다.
- 선택한 구역만 삭제되며, 구역에 할당된 출입문과 장치는 삭제되지 않습니다. 삭제 작업은 취소할 수 없습니다.
- 구역에 할당된 장치가 오프라인이거나, 동기화 중, 펌웨어 업그레이드 중이면 구역을 삭제할 수 없습니다. 장치가 다시 연결될 때까지 기다리거나, 구역에서 해당 장치를 먼저 제거한 후 다시 시도하세요.

APB 위반 확인하기

구역 관리 → **위반** 메뉴에서는 구역에 설정한 안티패스백(APB) 규칙을 어긴 사용자를 확인하고, 필요할 때 위반 상태를 해제할 수 있습니다. 구역과 APB 모드를 아직 설정하지 않았다면 먼저 구역 관리하기를 참고하세요.

위반이 발생하는 경우

APB 위반은 사용자가 구역에 설정된 APB 모드에 따라 순서에 어긋난 출입을 시도할 때 기록됩니다.

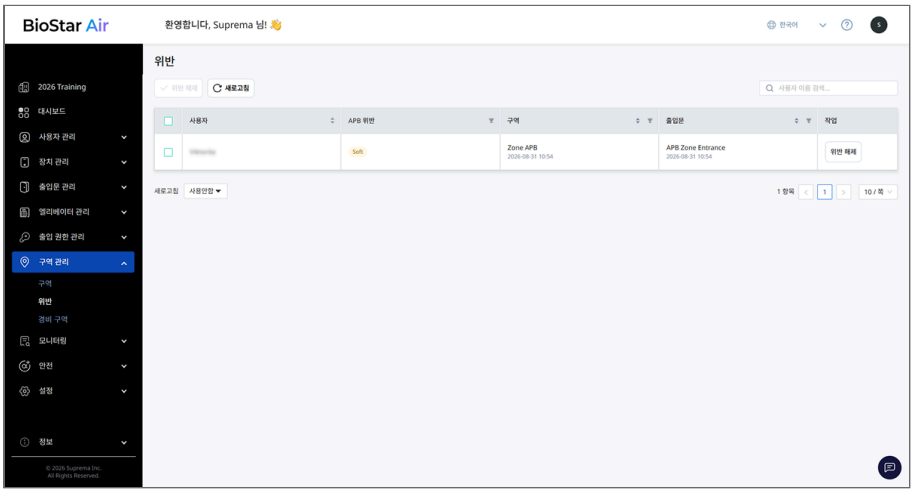
- **Hard 모드**로 설정된 구역에서는 APB 위반 시 출입이 차단되고, APB 위반으로 기록됩니다.

- **Soft 모드**로 설정된 구역에서는 APB 위반 시 출입은 허용되지만, APB 위반으로 기록됩니다.
- APB 예외 그룹에 속한 사용자는 APB 규칙이 적용되지 않으므로 위반 목록에 나타나지 않습니다.

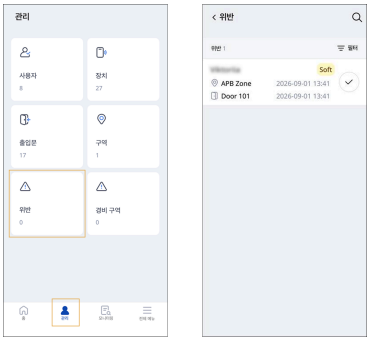
위반 목록 살펴보기

Web

화면 왼쪽 사이드바에서 **구역 관리** → **위반**를 클릭하세요.



Mobile



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 화면 하단의 **관리**를 탭하세요.
3. **위반** 카드를 탭하세요.

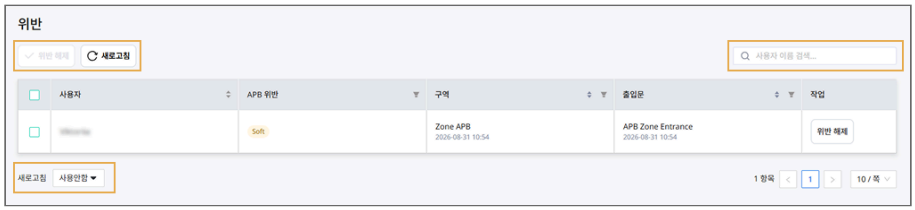
목록에서는 현재 활성 상태인 APB 위반 사용자를 확인할 수 있습니다. 활성 APB 위반이 없으면 목록 대신 빈 상태 화면이 표시됩니다.

- **사용자**: APB 위반이 기록된 사용자입니다.
- **APB 위반**: APB 위반이 발생한 모드(Hard/Soft)입니다.
- **구역**: APB 위반이 발생한 구역입니다.
- **출입문**: APB 위반이 발생한 출입문입니다.
- **작업**: 개별 APB 위반을 해제할 수 있습니다.

> **알아두기**
> 해제된 APB 위반과 과거 APB 위반 이력은 **모니터링** → **이벤트 로그**에서 계속 확인할 수 있습니다.

위반 목록 관리 기능

목록 상단 및 하단에서 제공하는 관리 기능으로 다음 작업을 수행할 수 있습니다.

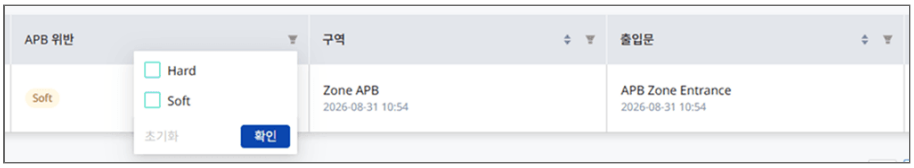


- **위반 해제**: 목록에서 선택한 사용자의 APB 위반을 해제할 수 있습니다. 자세한 내용은 위반 해제를 참고하세요.
- **새로고침**: 목록을 즉시 새로고침해 최신 상태로 갱신합니다. 목록 하단의 **새로고침**에서 자동 새로고침 간격(**사용안함**/**5초**/**1분**)을 선택하면 설정한 주기마다 목록을 자동 갱신합니다.
- **사용자 이름 검색…**: 사용자 이름으로 검색할 수 있습니다.

위반 목록 필터링

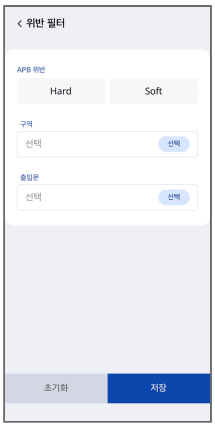
Web

목록 상단 헤더의 **APB 위반**, **구역**, **출입문** 열에 있는 버튼을 클릭하면 해당 조건으로 목록을 필터링할 수 있습니다.



> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 클릭하세요.

Mobile



1. 위반 목록 오른쪽 상단의 **필터**를 탭하세요.
2. **APB 위반**, **구역**, **출입문**에서 원하는 조건을 선택하세요.
3. 선택한 조건으로 목록을 필터링하려면 **저장** 버튼을 탭하세요.

> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 탭하세요.

위반 해제

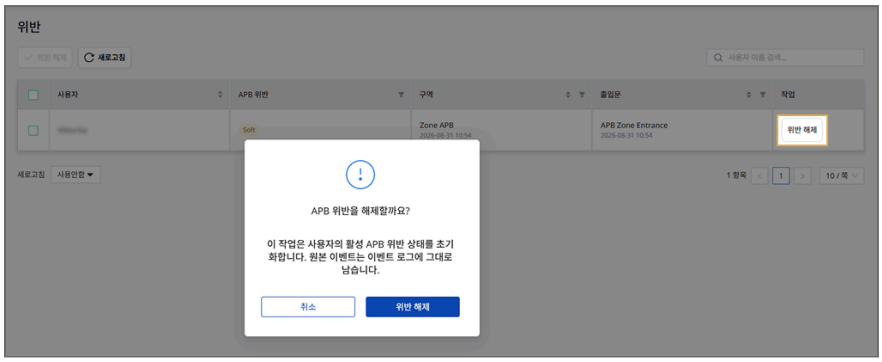
APB 위반을 해제하면 사용자의 활성 APB 위반 상태가 초기화되어, 다시 구역에 정상 출입할 수 있습니다.

> **알아두기**
>
> - **위반 해제**는 사용자의 활성 APB 위반 상태만 초기화합니다. APB 위반이 발생한 원본 이벤트는 삭제되지 않으며 이벤트 로그에 그대로 남습니다.
> - 구역이 비활성화되어도 이미 발생한 APB 위반은 그대로 유지되며, 위반 목록에서 해제할 수 있습니다.
> - APB 예외 그룹에 속한 사용자는 이 목록에 표시되지 않지만, 구역의 내부 인원 수에는 계속 포함됩니다.

개별 사용자의 위반 해제

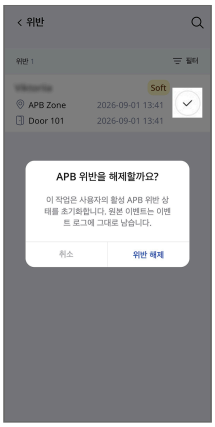
Web

1. 목록에서 APB 위반을 해제할 사용자의 **작업** 열에서 **위반 해제** 버튼을 클릭하세요.



2. 확인 메시지가 나타나면 **위반 해제** 버튼을 클릭하세요.

Mobile

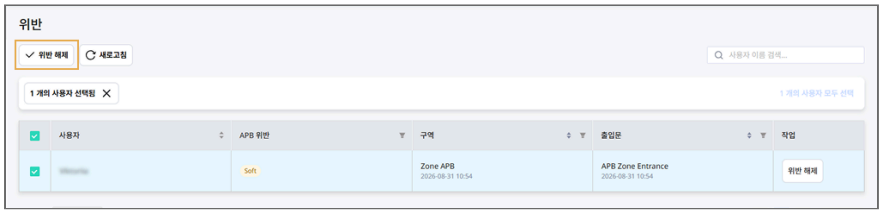


1. 목록에서 APB 위반을 해제할 사용자의 ⌄ 버튼을 탭하세요.
2. 확인 메시지가 나타나면 **위반 해제** 버튼을 탭하세요.

여러 사용자의 위반 해제

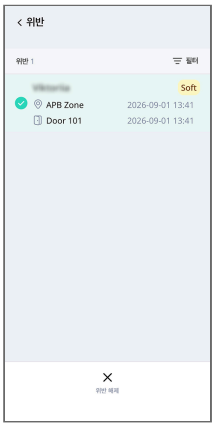
Web

1. 목록에서 APB 위반을 해제할 사용자의 체크박스를 클릭하세요. 한 명 이상의 사용자를 선택할 수 있습니다.
2. 목록 상단의 **위반 해제** 버튼을 클릭하세요.



3. 확인 메시지가 나타나면 **위반 해제** 버튼을 클릭하세요.

Mobile



1. 목록에서 APB 위반을 해제할 사용자를 길게 누르세요.
2. 위반을 해제할 사용자를 선택하세요. 한 명 이상의 사용자를 선택할 수 있습니다.
3. 화면 하단의 **위반 해제** 버튼을 탭하세요.
4. 확인 메시지가 나타나면 **위반 해제** 버튼을 탭하세요.

모니터링

BioStar Air의 모니터링 기능을 통해 시스템의 주요 활동을 실시간으로 추적하고 관리할 수 있습니다. 이벤트 및 변경 로그를 모니터링하여 시스템 활동을 분석하고, 출입문의 상태를 실시간으로 확인한 후 원격으로 제어하며, 생성된 알림과 리포트를 통해 보안 활동을 종합적으로 관리합니다.

이벤트 로그 사용하기

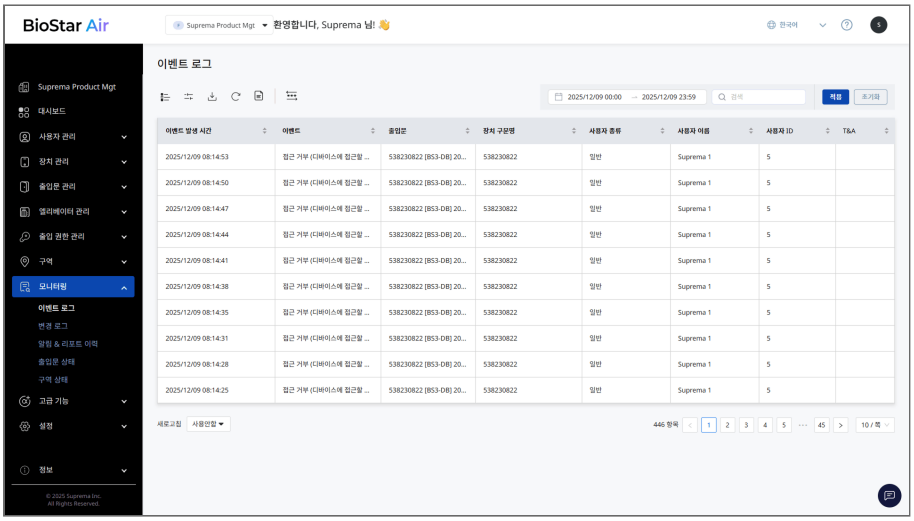
클라우드 출입 통제 플랫폼의 주요 장점 중 하나는 언제 어디서나 사이트 활동을 모니터링할 수 있는 기능입니다. 이 문서는 BioStar Air에서 이벤트 로그를 모니터링하고 분석하는 방법을 안내합니다.

> **팁**
> 이벤트 로그에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

이베트 로그 확인

Web

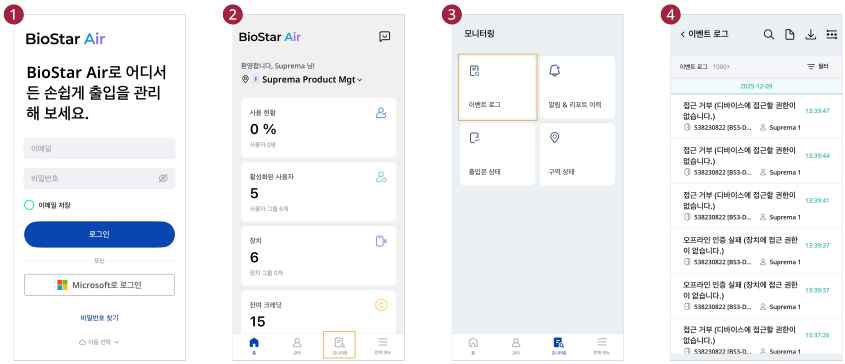
이벤트 로그를 확인하려면 **이벤트 로그**로 이동하세요. 화면 왼쪽 사이드바에서 **모니터링** → **이벤트 로그**를 클릭하세요.



이벤트 로그 화면에는 이벤트 발생 시간 및 이벤트 이름, 출입문 이름, 장치 구분명, 사용자 유형, 사용자 이름 등과 같은 세부 정보가 포함된 테이블 목록을 확인할 수 있습니다.

Mobile

모바일 앱에서 이벤트 로그를 확인하는 방법을 안내합니다.



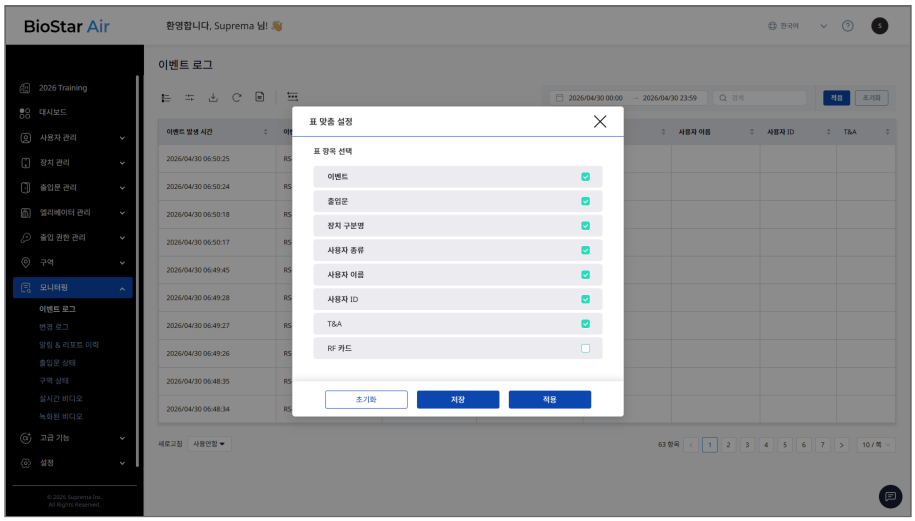
1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 초기 화면 하단의 **모니터링**을 탭하세요.
3. **이벤트 로그** 카드를 탭하세요.
4. 이벤트 로그 목록을 스크롤하여 내용을 확인할 수 있습니다.

알아두기

- **필터**: 이벤트 로그를 필터링할 수 있습니다.
- : 특정 키워드를 검색할 수 있습니다. RF 카드 아이디, 사용자 아이디 및 이메일, 이름 중 하나를 입력하세요.
- : 리포트를 생성할 수 있습니다. 리포트 생성에 대한 자세한 내용은 리포트 설정을 참고하세요.
- : 리포트를 CSV 또는 PDF 파일 형식으로 다운로드할 수 있습니다.
- : 개인정보 마스킹 처리를 적용할 수 있습니다.

표 맞춤 설정

테이블의 열을 사용자 지정하여 원하는 정보를 표시하거나 숨길 수 있습니다. 순서를 변경해 자주 사용하는 열을 앞쪽에 배치할 수도 있습니다.
이벤트 로그 목록 상단의 ⚙ 버튼을 클릭하세요. **표 맞춤 설정** 창이 나타납니다.



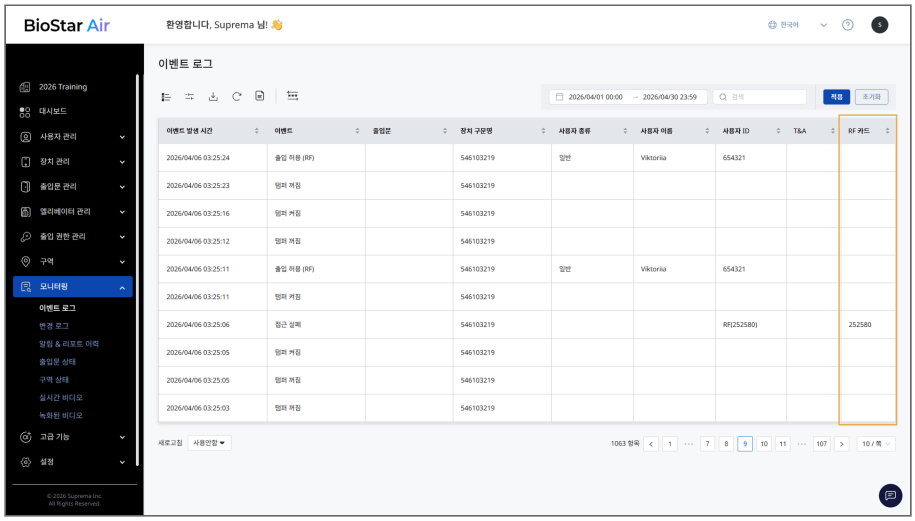
- 표시하거나 숨기려는 열의 체크박스를 선택하거나 선택 해제하세요.
- 열의 순서를 변경하려면 해당 열을 클릭한 상태에서 원하는 위치로 드래그하세요.
- **표 맞춤 설정**을 저장하려면 **저장** 버튼을 클릭하세요.
- **표 맞춤 설정**을 저장하지 않고 로그 목록에 적용하려면 **적용** 버튼을 클릭하세요.
- **표 맞춤 설정**의 변경 사항을 취소하고 처음 상태로 되돌리려면 **초기화** 버튼을 클릭하세요.

> **알아두기**
>
> - **저장** 버튼을 클릭하면 설정이 저장되어 다른 메뉴로 이동한 후에도 유지됩니다. **적용** 버튼을 클릭하면 변경 사항이 현재 목록에만 적용되며, 다른 메뉴로 이동하면 이전 설정으로 되돌아갑니다.
> - **변경 로그**에서는 **표 맞춤 설정** 기능을 지원하지 않습니다.

RF 카드 번호 열 표시

이벤트 로그에서 사용자가 RF 카드로 인증했다면, **RF 카드** 열을 추가하여 RF 카드 번호를 확인할 수 있습니다.

1. 이벤트 로그 목록 상단의 ⚙ 버튼을 클릭하세요.
2. **표 맞춤 설정** 창이 나타나면 **RF 카드**의 체크박스를 클릭하고 원하는 위치로 드래그하세요.
3. **저장** 또는 **적용** 버튼을 클릭하세요.
4. 이벤트 로그 목록에 **RF 카드** 열이 표시됩니다.

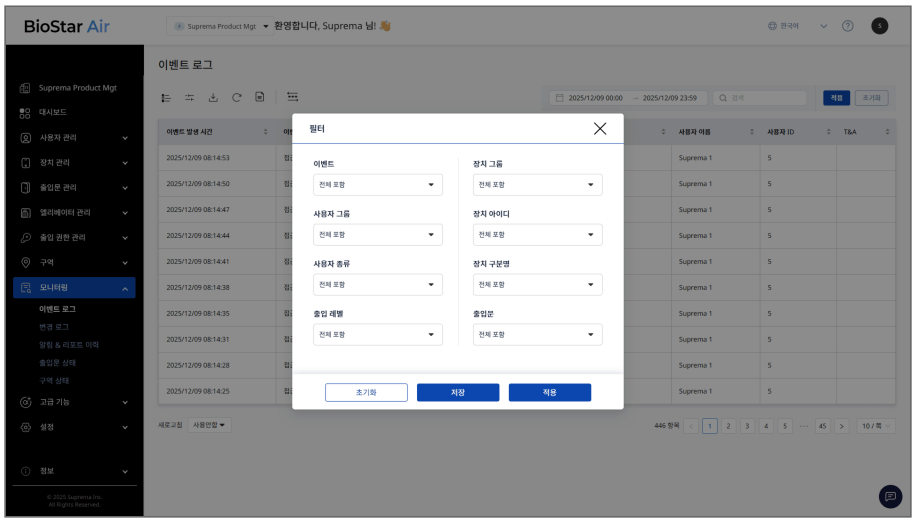


알아두기

이벤트 로그에 표시되는 RF 카드 번호는 사용자에게 할당된 카드가 하나일 때만 나타납니다. 사용자가 여러 개의 RF 카드를 가지고 있다면 카드 번호가 표시되지 않습니다.

로그 필터링

로그를 필터링해 원하는 정보를 빠르게 찾을 수 있습니다. 로그 목록 상단의 버튼을 클릭하세요. **필터** 창이 나타나면 각 항목에서 원하는 값을 선택하세요.



알아두기

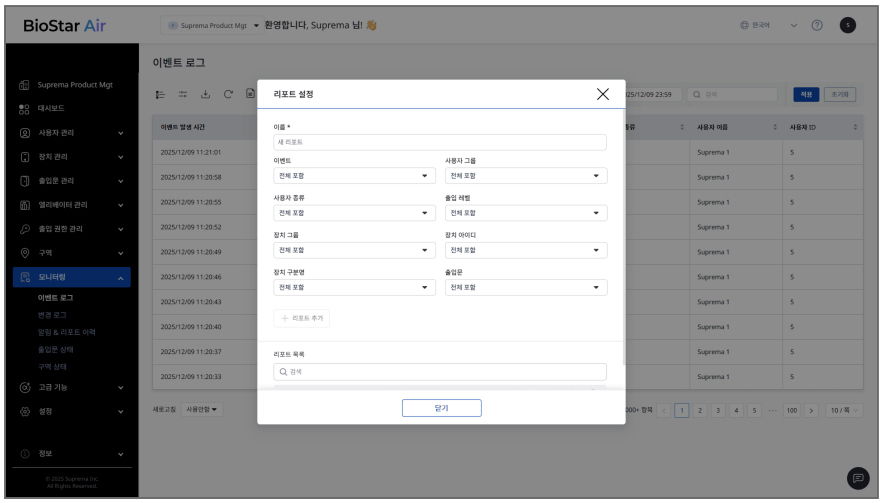
- **저장** 또는 **필터 저장** 버튼을 클릭하면 설정이 저장되어 다른 메뉴로 이동한 후에도 유지됩니다. **적용** 또는 **필터 적용** 버튼을 클릭하면 변경 사항이 현재 목록에만 적용되며, 다른 메뉴로 이동하면 이전 설정으로 되돌아갑니다.
- 변경 사항을 취소하고 처음 상태로 되돌리려면 **초기화** 또는 **필터 초기화** 버튼을 클릭하세요.

리포트 설정

로그 데이터를 필터링하여 특정 기간 동안 발생한 이벤트에 대한 리포트를 생성할 수 있습니다.

1. 로그 목록 상단의 버튼을 클릭하세요.

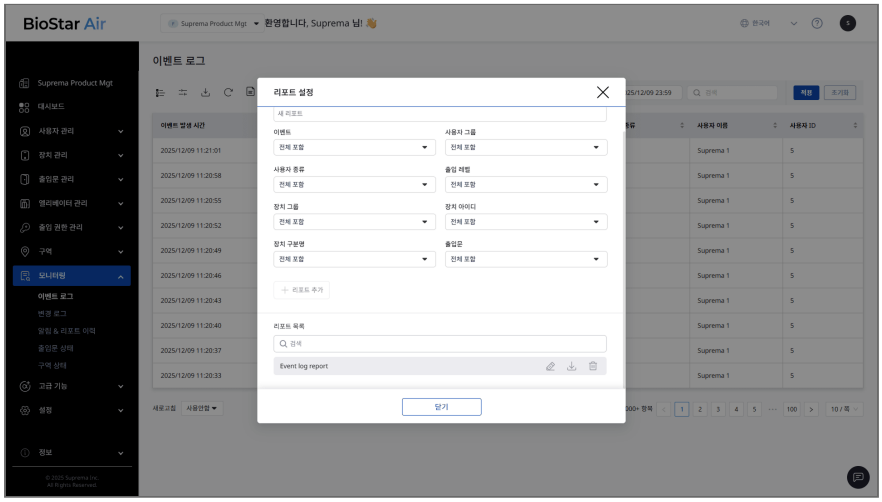
2. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



3. 리포트에 포함할 항목을 선택하세요.

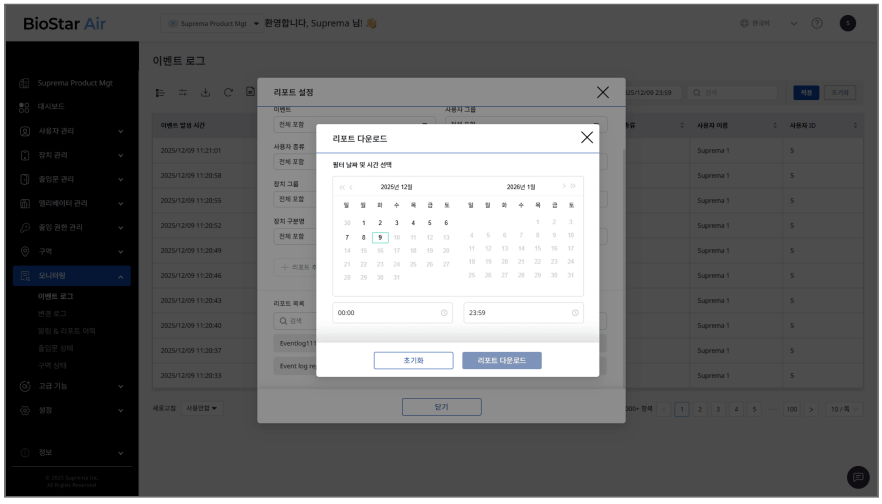
4. 설정한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.

5. **리포트 목록**에 설정한 이름으로 리포트가 생성됩니다.



6. 생성된 리포트를 다운로드하려면 리포트 이름 옆의 ⭳ 버튼을 클릭하세요.

7. **리포트 다운로드** 창이 나타나면 이벤트를 조회할 기간을 선택하고 **리포트 다운로드** 버튼을 클릭하세요.



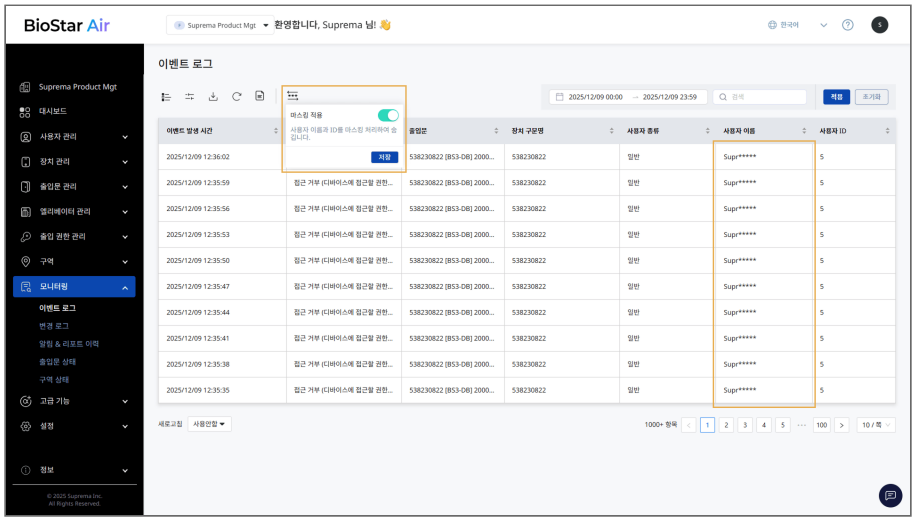
관리자의 이메일로 다운로드 링크가 전송됩니다.

> **알아두기**
> **리포트 목록**에서 생성한 리포트를 검색하거나 수정, 다운로드, 삭제할 수 있습니다.

개인정보 마스킹 처리

로그에서 개인정보를 마스킹 처리하여 민감한 정보를 보호할 수 있습니다. 개인정보 마스킹 처리를 활성화하면 사용자 이름, 이메일 주소 및 전화번호와 같은 정보가 부분적으로 숨겨집니다.

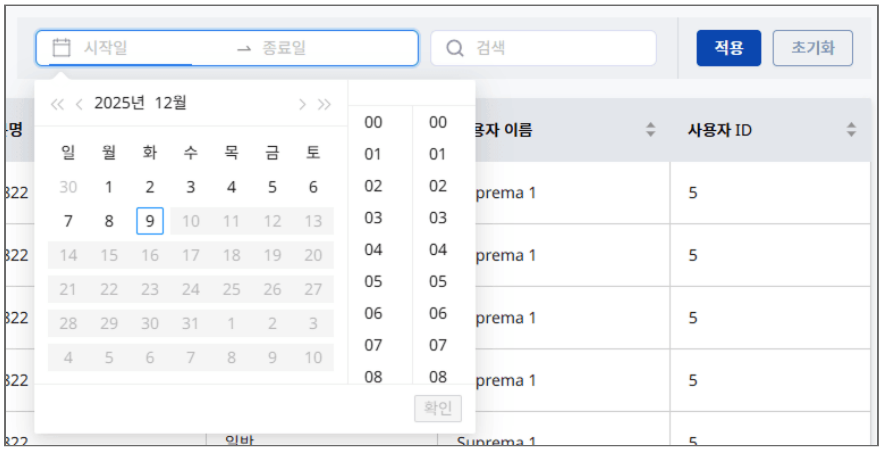
개인정보 마스킹 처리를 활성화하려면 로그 목록 상단의 버튼을 클릭하세요. 팝업 메뉴에서 **마스킹 적용** 옵션을 활성화하고 **저장** 버튼을 클릭하세요.



기타 기능

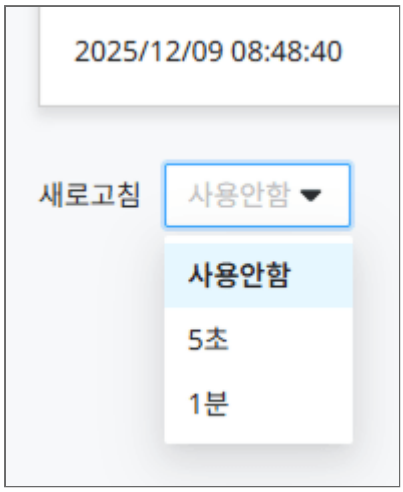
로그 목록 상단의 도구 모음을 사용하여 로그를 보다 효율적으로 관리할 수 있습니다.

- 로그를 날짜별로 정렬하려면 날짜 및 시간 범위를 선택한 후 **적용** 버튼을 클릭하세요. 날짜를 재설정하려면 **초기화** 버튼을 클릭하세요.



- **검색** 입력 필드에서 특정 키워드를 입력하여 로그를 검색할 수 있습니다. RF 카드 아이디, 사용자 아이디 및 이메일, 이름 중 하나를 입력하세요.
- 로그를 CSV 또는 PDF 파일로 저장하려면 버튼을 클릭하세요.
- 로그를 새로 고침하려면 목록 상단의 버튼을 클릭하세요.

- 특정 시간 간격으로 새로 고침하려면 목록 왼쪽 하단의 **새로고침**에서 5초 또는 1분을 선택하세요.



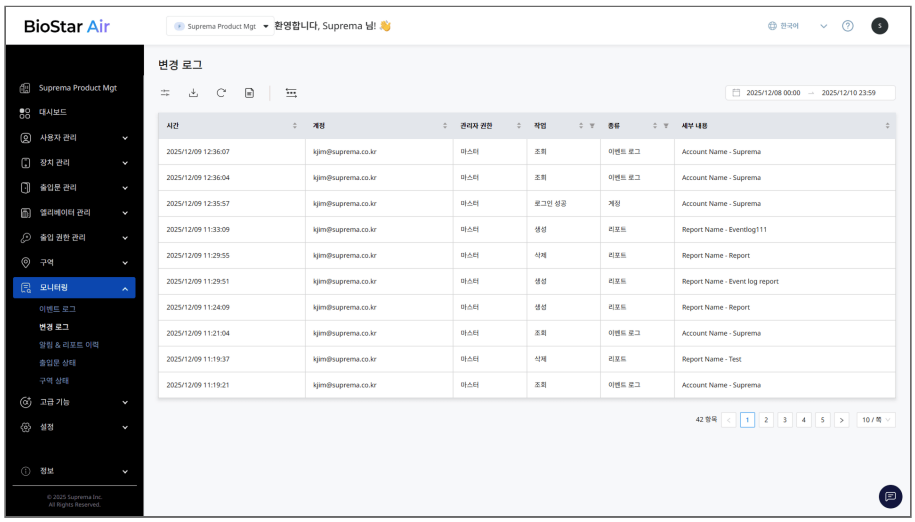
변경 로그 사용하기

클라우드 출입 통제 플랫폼의 주요 장점 중 하나는 언제 어디서나 사이트 활동을 모니터링할 수 있는 기능입니다. 이 문서는 BioStar Air에서 변경 로그를 모니터링하고 분석하는 방법을 안내합니다.

> **팁**
> 변경 로그에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

변경 로그 확인

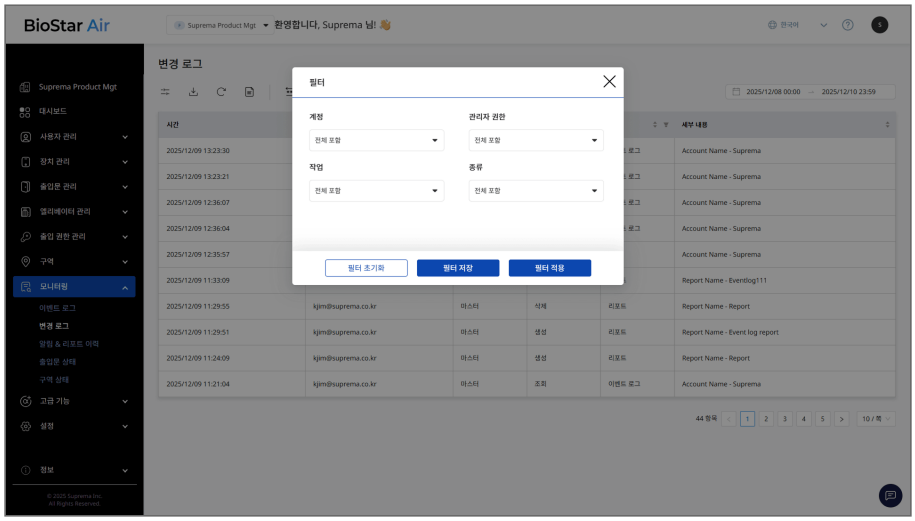
변경 로그를 확인하려면 **변경 로그**로 이동하세요. 화면 왼쪽 사이드바에서 **모니터링** → **변경 로그**를 클릭하세요.



변경 로그에서는 관리자가 수행한 작업을 추적할 수 있습니다. 목록의 각 로그에는 작업 시간 및 이메일 주소, 관리자 권한, 작업 유형, 메뉴 경로, 작업 세부 정보와 같은 정보가 포함된 테이블 목록을 확인할 수 있습니다.

로그 필터링

로그를 필터링해 원하는 정보를 빠르게 찾을 수 있습니다. 로그 목록 상단의 버튼을 클릭하세요. **필터** 창이 나타나면 각 항목에서 원하는 값을 선택하세요.



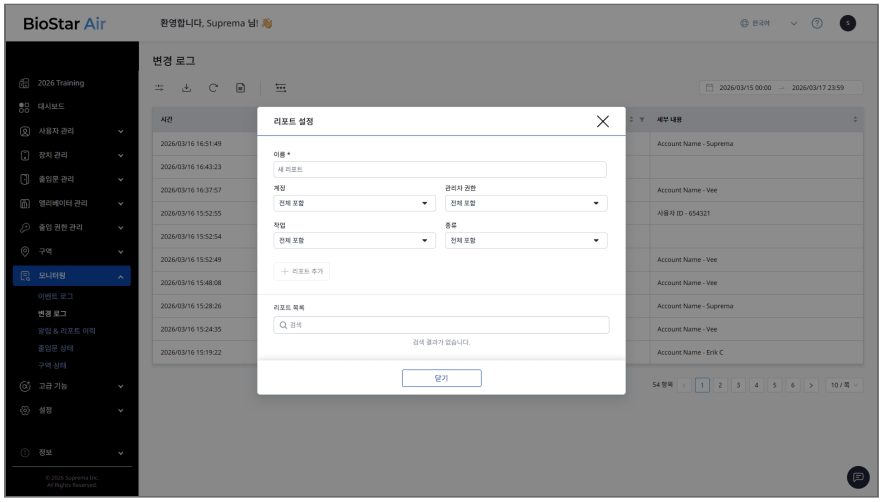
알아두기

- **저장** 또는 **필터 저장** 버튼을 클릭하면 설정이 저장되어 다른 메뉴로 이동한 후에도 유지됩니다. **적용** 또는 **필터 적용** 버튼을 클릭하면 변경 사항이 현재 목록에만 적용되며, 다른 메뉴로 이동하면 이전 설정으로 되돌아갑니다.
- 변경 사항을 취소하고 처음 상태로 되돌리려면 **초기화** 또는 **필터 초기화** 버튼을 클릭하세요.

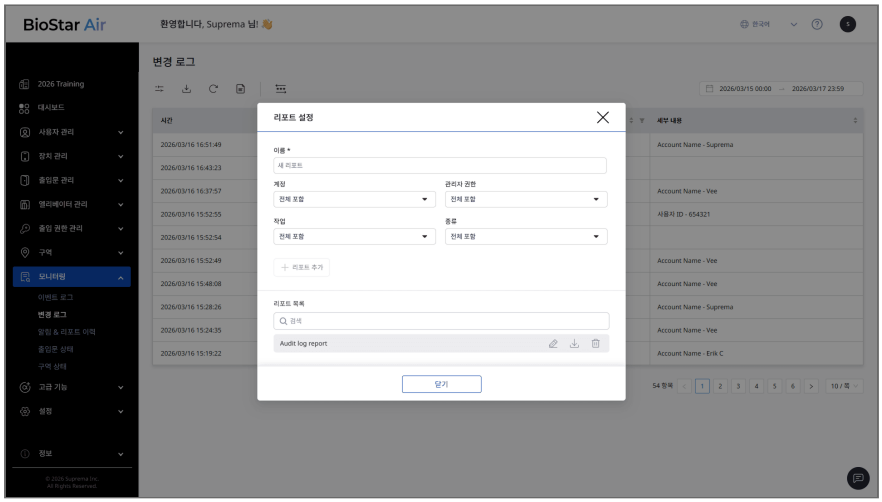
리포트 설정

로그 데이터를 필터링하여 특정 기간 동안 발생한 이벤트에 대한 리포트를 생성할 수 있습니다.

1. 로그 목록 상단의 버튼을 클릭하세요.
2. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.

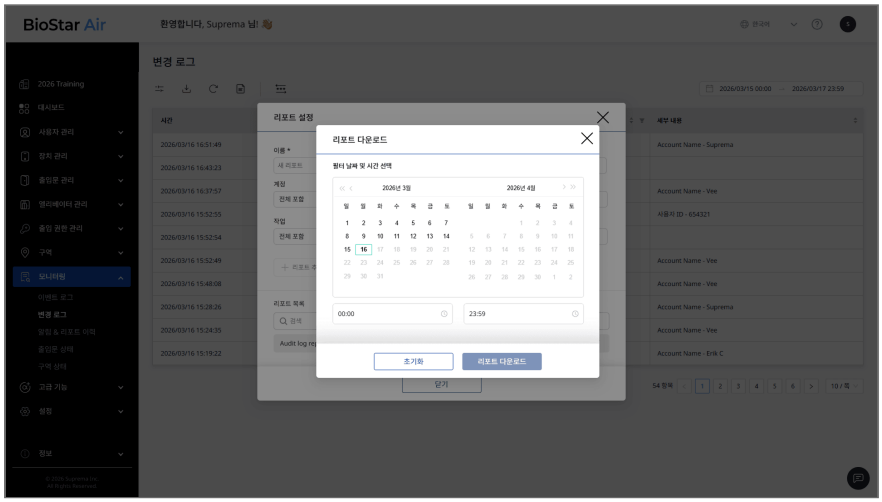


3. 리포트에 포함할 항목을 선택하세요.
4. 설정한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
5. **리포트 목록**에 설정한 이름으로 리포트가 생성됩니다.



6. 생성된 리포트를 다운로드하려면 리포트 이름 옆의 ⭳ 버튼을 클릭하세요.

7. **리포트 다운로드** 창이 나타나면 이벤트를 조회할 기간을 선택하고 **리포트 다운로드** 버튼을 클릭하세요.



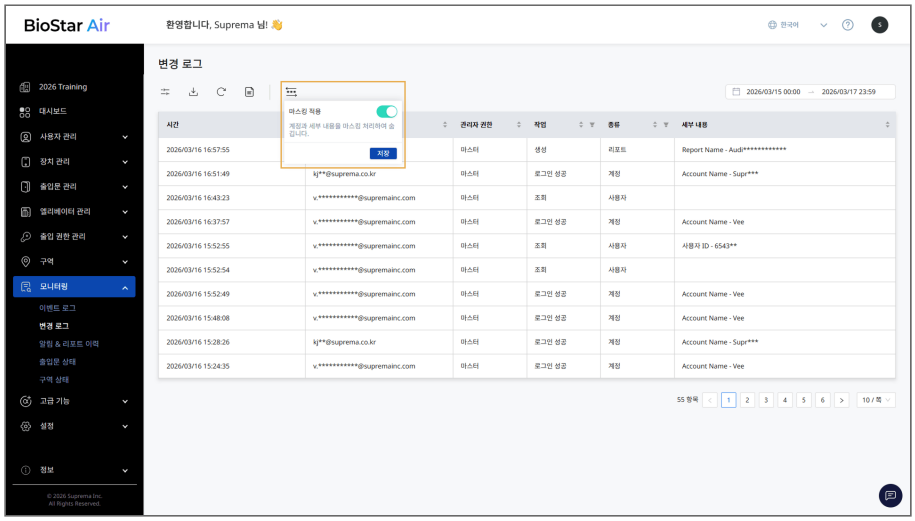
관리자의 이메일로 다운로드 링크가 전송됩니다.

> **알아두기**
> **리포트 목록**에서 생성한 리포트를 검색하거나 수정, 다운로드, 삭제할 수 있습니다.

개인정보 마스킹 처리

로그에서 개인정보를 마스킹 처리하여 민감한 정보를 보호할 수 있습니다. 개인정보 마스킹 처리를 활성화하면 사용자 이름, 이메일 주소 및 전화번호와 같은 정보가 부분적으로 숨겨집니다.

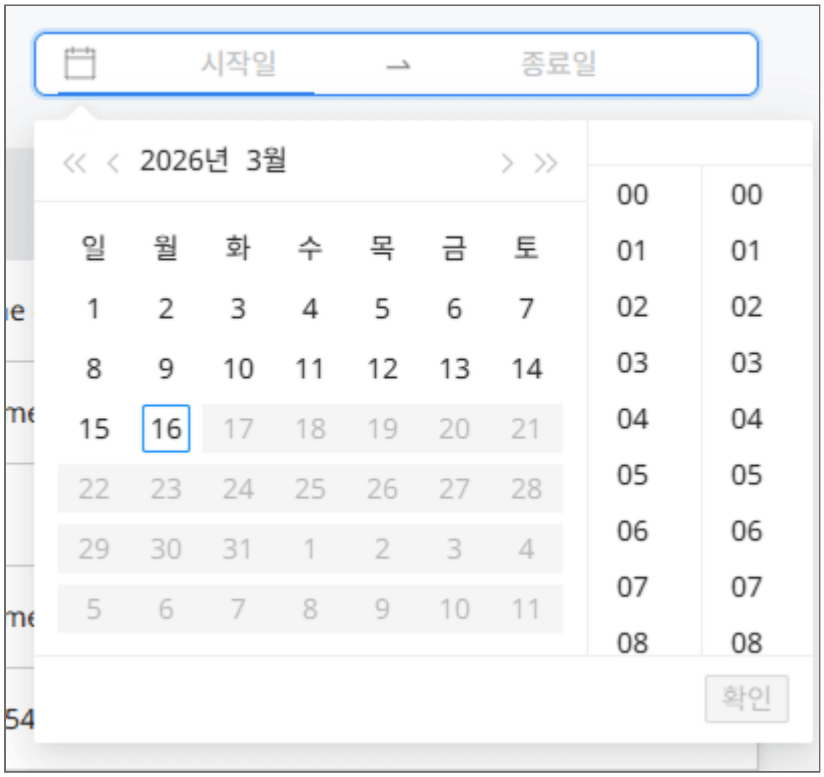
개인정보 마스킹 처리를 활성화하려면 로그 목록 상단의 ⟷ 버튼을 클릭하세요. 팝업 메뉴에서 **마스킹 적용** 옵션을 활성화하고 **저장** 버튼을 클릭하세요.



기타 기능

로그 목록 상단의 도구 모음을 사용하여 로그를 보다 효율적으로 관리할 수 있습니다.

- 로그를 날짜별로 정렬하려면 날짜 및 시간 범위를 선택하고, **확인** 버튼을 클릭하세요.



- 로그를 CSV 또는 PDF 파일로 저장하려면 ⭳ 버튼을 클릭하세요.
- 로그 목록을 새로 고침하려면 목록 상단의 ↻ 버튼을 클릭하세요.

알림 & 리포트 이력 확인하기

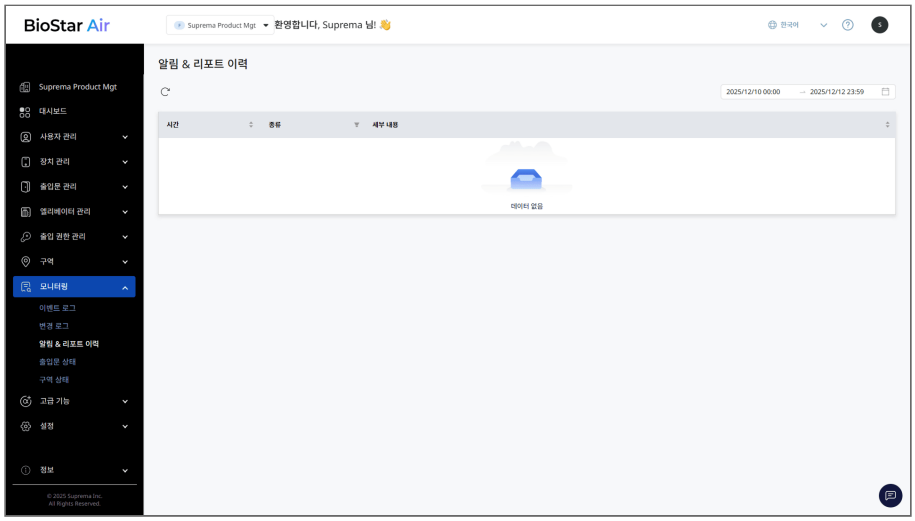
BioStar Air에서 생성된 알림 및 리포트의 이력을 확인하는 방법을 안내합니다. 관리자는 웹 포털과 모바일 앱을 통해 이전에 발생한 알림과 생성된 리포트 내역을 조회할 수 있습니다.

시작하기 전에

알림 및 리포트 이력은 **설정** → **알림 & 리포트 이력**에서 설정한 알림 및 리포트 생성 규칙에 의해 생성된 내역만 확인할 수 있습니다. 알림 및 리포트 생성 규칙 설정에 대한 자세한 내용은 알림 및 리포트 설정하기를 참고하세요.

알림 및 리포트 이력 확인

화면 왼쪽 사이드바에서 **모니터링** → **알림 & 리포트 이력**을 클릭하세요. 알림 및 리포트 이력을 확인할 수 있습니다.



- 알림이나 리포트를 생성한 시간 및 종류, 세부 내용을 목록에서 확인할 수 있습니다.
- 화면 오른쪽 상단의 날짜 조회 영역을 클릭해 원하는 기간을 설정하고, 해당 기간 내의 알림 및 리포트 이력을 필터링할 수 있습니다.
- 목록을 새로고침하려면 목록 상단의 ↻ 버튼을 클릭하세요.

출입문 상태 모니터링하기

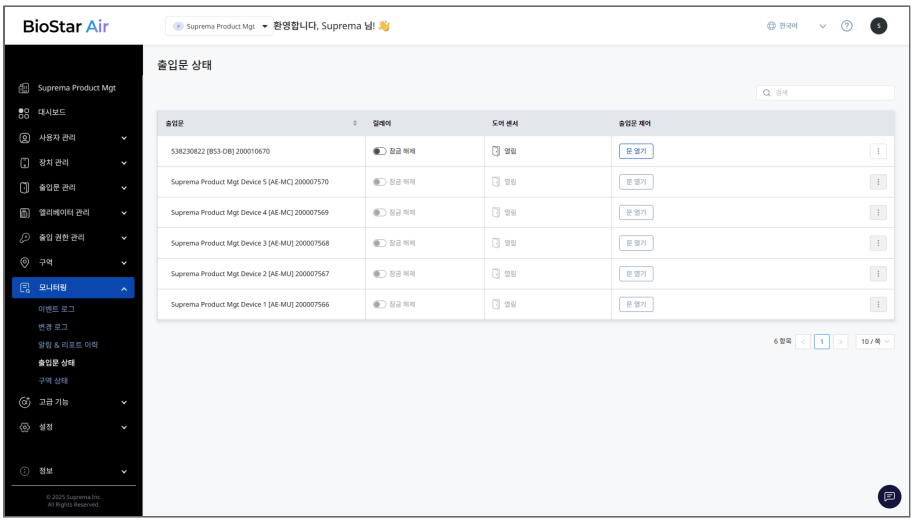
BioStar Air 시스템에 연결된 출입문의 상태를 실시간으로 모니터링할 수 있습니다. 관리자는 출입문의 잠금 또는 잠금 해제 여부 및 릴레이 센서 상태를 확인하고, 문을 잠그거나 잠금 해제하여 원격으로 출입을 제어할 수 있습니다.

> **팁**
> 출입문 상태 모니터링에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

출입문 상태 모니터링

Web

BioStar Air 웹 포털에서 출입문 상태를 모니터링할 수 있습니다. 화면 왼쪽 사이드바에서 **모니터링** → **출입문 상태**를 클릭하세요. BioStar Air에 등록된 출입문의 목록을 확인할 수 있습니다.

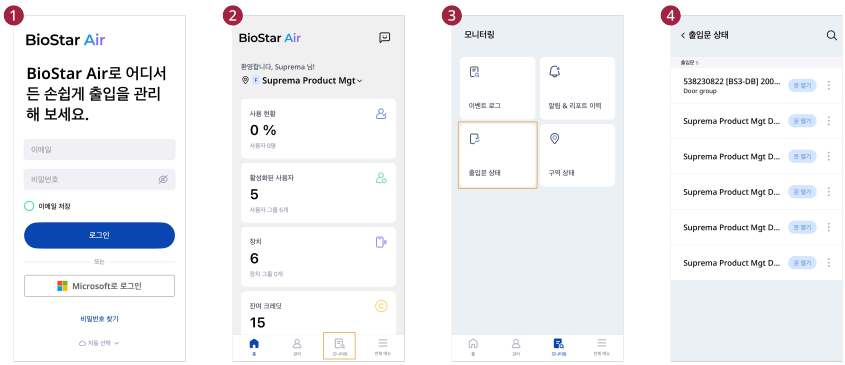


각 출입문에서는 아래 항목을 확인할 수 있습니다.

- **릴레이**: 출입문의 잠금 또는 잠금 해제 상태를 표시합니다.
- **도어 센서**: 출입문이 물리적으로 열려 있는지 또는 닫혀 있는지 표시합니다.

Mobile

모바일 기기에서 BioStar Air 앱을 사용하여 출입문 상태를 확인할 수 있습니다.



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 초기 화면 하단의 **모니터링**을 탭하세요.
3. **출입문 상태** 카드를 탭하세요.
4. BioStar Air에 등록된 출입문의 목록을 확인할 수 있습니다.

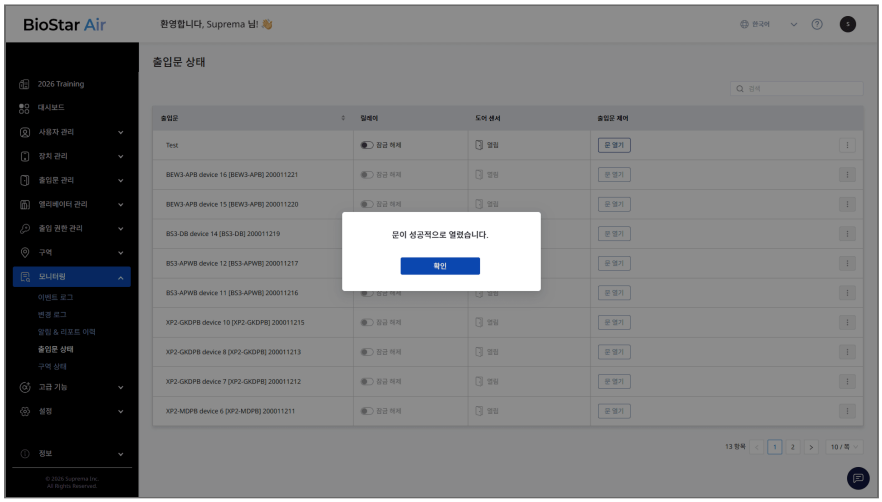
> **알아두기**
> 출입문 등록 및 관리에 대한 자세한 내용은 등록 출입문 관리하기를 참고하세요.

출입문 잠금 해제

출입문이 온라인 상태이고 BioStar Air에 연결되어 있다면 원격으로 잠금 해제할 수 있습니다.

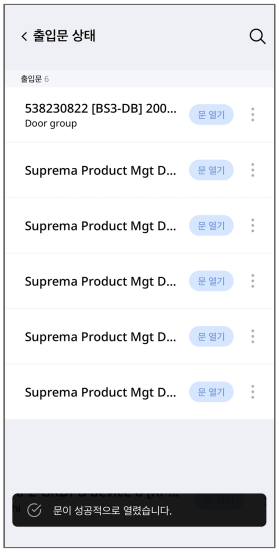
Web

1. **출입문 제어** 열에서 **문 열기** 버튼을 클릭하세요.
2. **릴레이** 열의 상태가 잠금 해제로 변경되고, 성공 메시지가 나타납니다.



3. 설정된 시간이 지나면 출입문은 다시 잠금 상태로 돌아갑니다.

Mobile



1. 출입문을 원격으로 잠금 해제하려면 **문 열기** 버튼을 탭하세요.
2. 화면 하단에 성공 메시지가 나타납니다.
3. 설정된 시간이 지나면 출입문은 다시 잠금 상태로 돌아갑니다.

> **알아두기**
> 출입문이 열린 상태로 유지되는 시간을 설정하는 방법은 등록 출입문 관리하기를 참고하세요.

항상 열림 모드 설정

출입문을 무기한 열림 상태로 유지할 수 있습니다. 방문객 또는 임시 출입이 필요한 경우에 유용하게 사용할 수 있습니다.

Web

1. 출입문 목록에서 열림 상태로 유지할 출입문의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



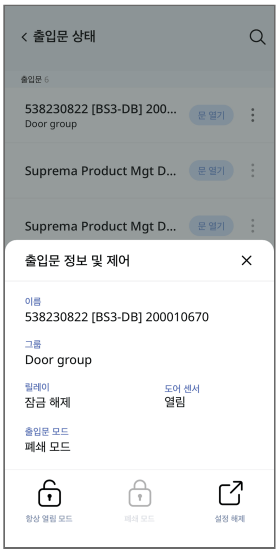
2. 팝업 메뉴에서 **항상 열림**을 클릭하세요.

3. **출입문 제어** 열에 **열린 상태 유지**로 상태가 변경됩니다.



정상 동작 상태로 되돌리려면 ⋮ → **설정 해제**를 클릭하세요.

Mobile



1. 출입문의 가장 오른쪽에 ⋮ 버튼을 탭하세요.
2. **출입문 정보 및 제어** 옵션이 나타나면 **항상 열림 모드**를 탭하세요.
3. 화면 하단에 성공 메시지가 나타납니다.

정상 동작 상태로 되돌리려면 ⋮ → **설정 해제**를 탭하세요.

폐쇄 모드 설정

현재 스케줄에 관계없이 출입문을 잠금 상태로 유지할 수 있습니다. 보안 강화가 필요한 경우에 유용하게 사용할 수 있습니다.

Web

1. 출입문 목록에서 잠금 상태로 유지할 출입문의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.

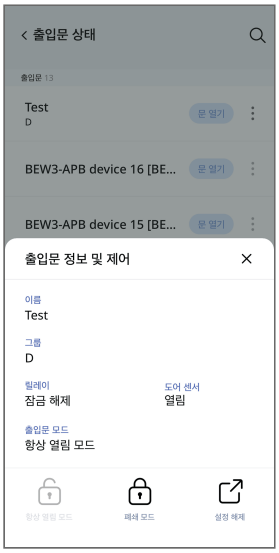


2. 팝업 메뉴에서 **폐쇄 모드**를 클릭하세요.
3. **출입문 제어** 열에 **닫힌 상태 유지**로 상태가 변경됩니다.



정상 동작 상태로 되돌리려면 ⋮ → **설정 해제**를 클릭하세요.

Mobile



1. 출입문의 가장 오른쪽에 ⋮ 버튼을 탭하세요.
2. **출입문 정보 및 제어** 옵션이 나타나면 **폐쇄 모드**를 탭하세요.
3. 화면 하단에 성공 메시지가 나타납니다.

정상 동작 상태로 되돌리려면 ⋮ → **설정 해제**를 탭하세요.

안전

BioStar Air의 **안전 관리** 기능은 정상 운영 중에는 현장 내 인원을 파악하고, 비상시에는 대피 과정을 관리할 수 있도록 지원합니다. **현장 체류 인원 확인**(On-Site Now) 및 **구역** 기능을 포함한 재실(Presence) 기능을 통해 관리자는 출입 권한 소유자가 현재 현장에 있는지, 그리고 현장 내 어느 위치에 있는지 실시간으로 확인할 수 있습니다. 또한 관리자가 개별 인원의 현황 상태를 수동으로 변경할 수도 있습니다.

인원 점검(Roll Call) 기능은 지정된 관리자가 특정 집결지를 책임지고 해당 구역에 배정된 인원의 안전을 감독하게 함으로써 질서 있는 대피를 지원합니다. 이 기능은 **On-Site Now** 기능과 동일한 현장 인원 파악 엔진을 기반으로 작동합니다.

다음 제공하는 문서를 통해 BioStar Air 포털에서 재실과 비상 호출을 관리하는 방법을 알아보세요.

재실 확인하기

안전 → **재실** 메뉴에서는 현재 사이트에 있는 사용자를 실시간으로 확인할 수 있습니다. 재실(Presence) 상태는 **경계 구역**(Perimeter Zone)에 설정한 입실 및 퇴실 장치의 인증 기록을 기준으로 계산되며, 경계 구역을 아직 설정하지 않았다면 먼저 구역 관리하기를 참고하세요.

재실 상태가 결정되는 방식

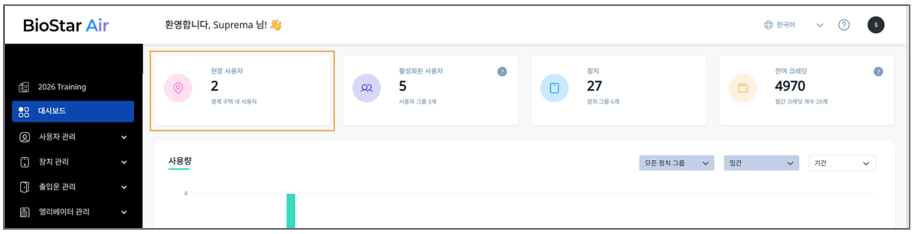
사용자는 경계 구역의 입실 장치에서 인증하면 **현장** 상태로, 퇴실 장치에서 인증하면 **외부** 상태로 전환됩니다.

- 경계 구역에 퇴실 장치를 지정하지 않은 사이트는 **외부 타이머**를 반드시 설정해야 합니다. 설정한 시간 동안 활동이 없으면 사용자가 **외부** 상태로 자동 전환됩니다.
- 경계 구역의 입실 및 퇴실 장치, **외부 타이머** 설정 방법은 구역 관리하기를 참고하세요.
- 관리자는 여러 메뉴를 통해 현장에 있는 사람들의 목록과 인원을 확인할 수 있습니다.
  - **대시보드** 위젯
  - **안전** → **재실**
  - **구역 관리** → **구역** → **내부 인원** (경계 구역)

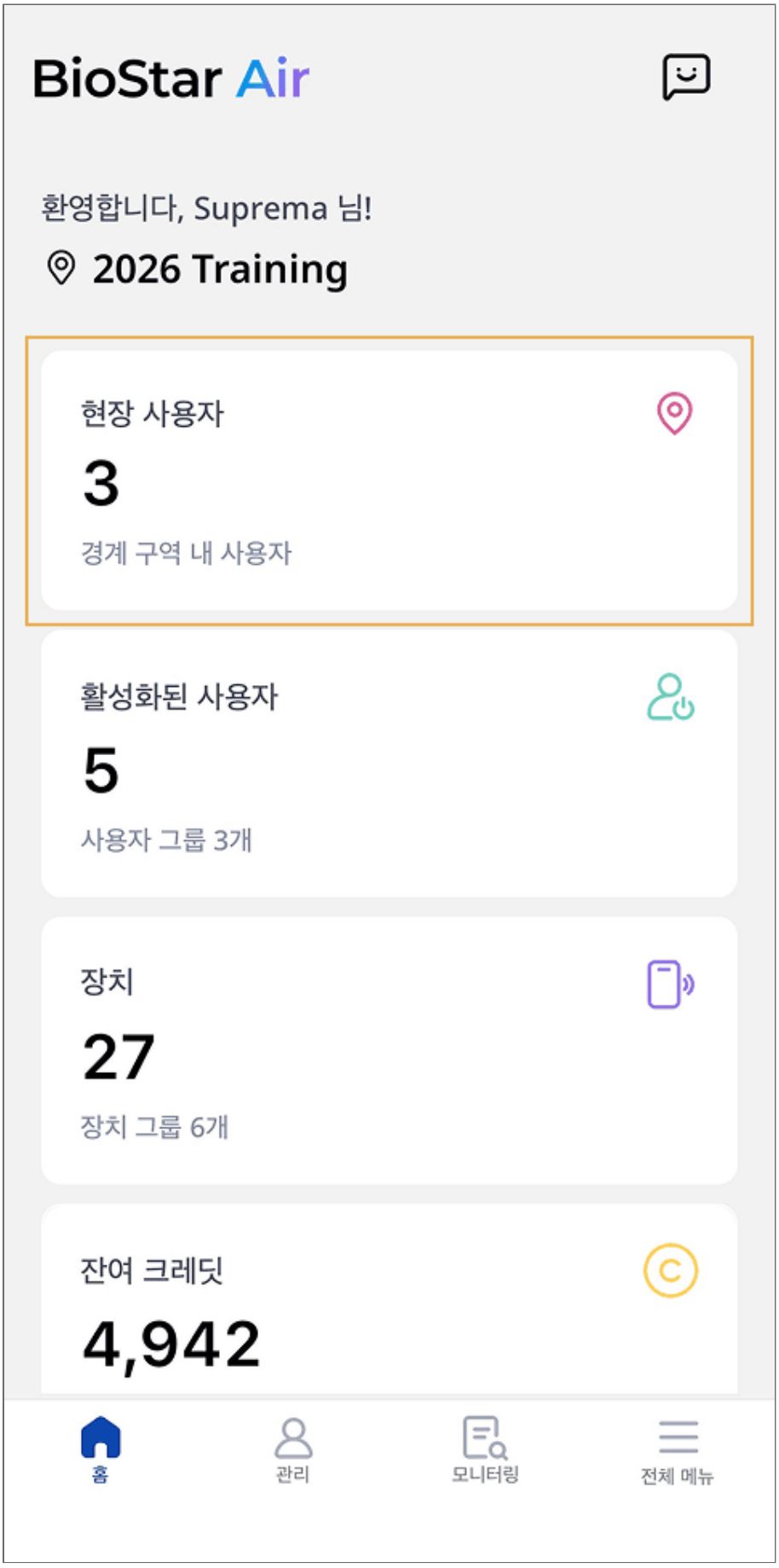
대시보드에서 확인

대시보드 메뉴에서도 **현장 사용자** 카드로 현재 사이트에 있는 사용자 수를 빠르게 확인할 수 있습니다.

Web


BioStar Air
환영합니다, Suprema 님!
2026 Training
대시보드
사용자 관리
장치 관리
출입문 관리
엘리베이터 관리
현장 사용자
2
활성화된 사용자
5
장치
27
잔여 크레딧
4970
사용량
모든 장치 그룹
일간
기간

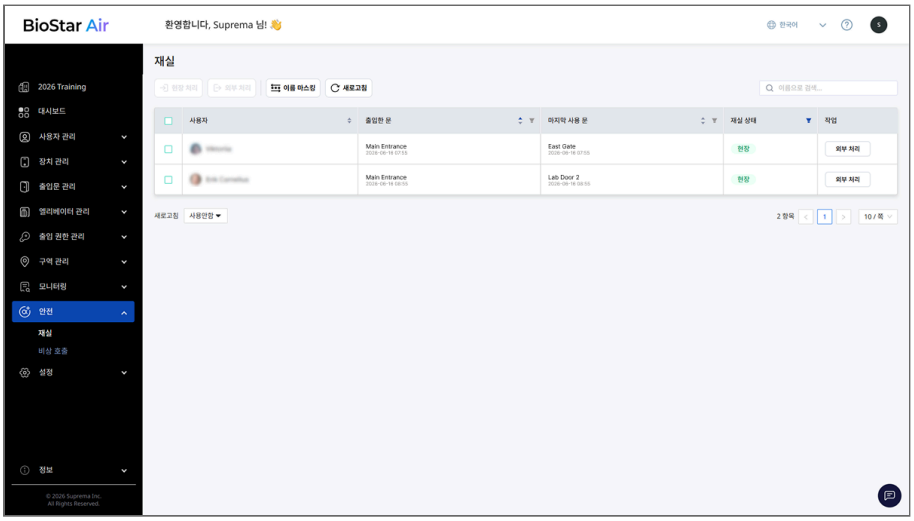
Mobile


BioStar Air
환영합니다, Suprema 님!
2026 Training
현장 사용자
3
경계 구역 내 사용자
활성화된 사용자
5
사용자 그룹 3개
장치
27
장치 그룹 6개
잔여 크레딧
4,942
홈
관리
모니터링
전체 메뉴

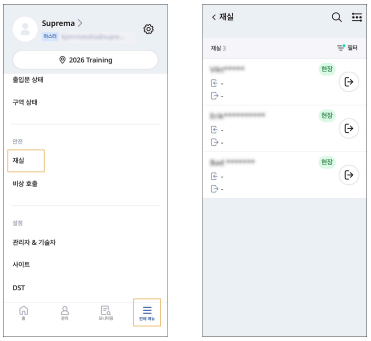
재실 목록 살펴보기

Web

화면 왼쪽 사이드바에서 **안전** → **재실**을 클릭하세요.



Mobile



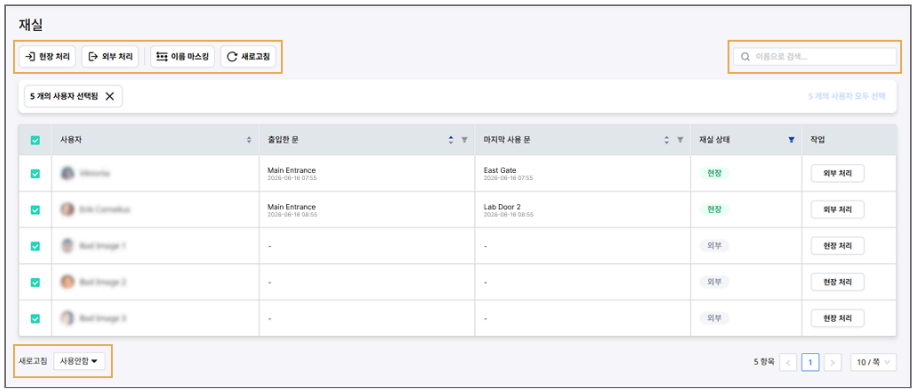
1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 화면 하단의 **전체 메뉴** → **재실**을 탭하세요.

재실 목록은 기본적으로 **현장** 상태인 사용자만 표시합니다.

- **사용자**: 사용자의 프로필 사진과 이름입니다.
- **출입한 문**: 사용자가 사이트에 들어올 때 인증한 입실 장치와 시각입니다.
- **마지막 사용 문**: 사용자가 가장 최근에 사용한 출입문과 시각입니다.
- **재실 상태**: 사용자의 현재 재실 상태(**현장**/**외부**)입니다.
- **작업**: 개별 사용자의 재실 상태를 변경할 수 있습니다.

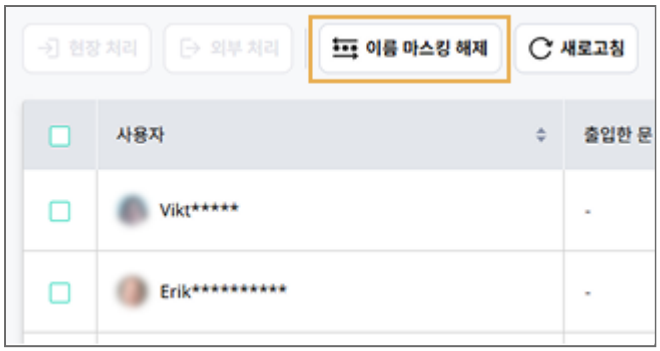
재실 목록 관리 기능

목록 상단 및 하단에서 제공하는 관리 기능으로 다음 작업을 수행할 수 있습니다.

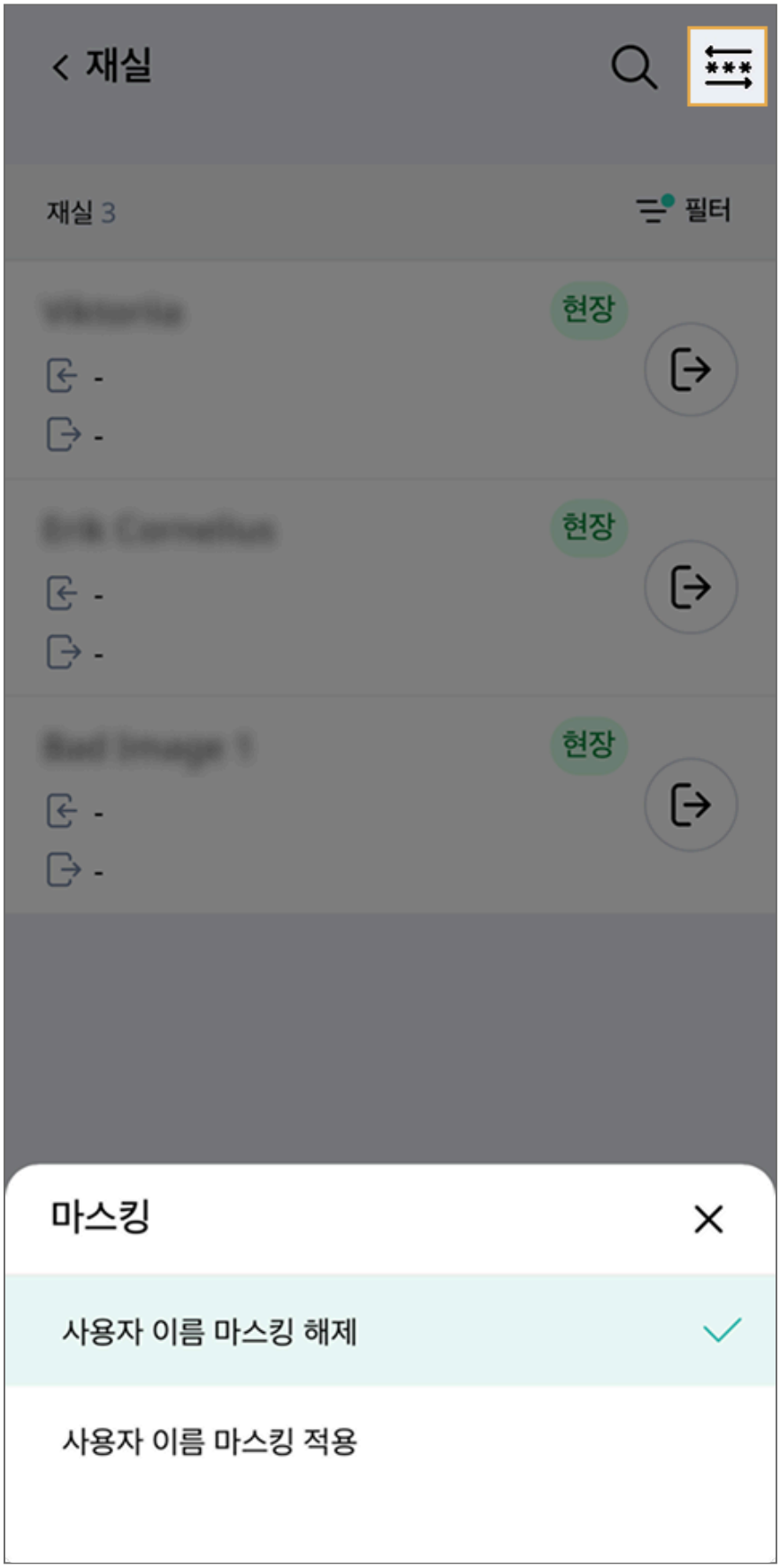


- **현장 처리** / **외부 처리**: 사용자의 재실 상태를 현장 또는 외부로 변경할 수 있습니다. 자세한 내용은 재실 상태 수동 변경을 참고하세요.
- **이름 마스킹** / **이름 마스킹 해제** (***): 사용자 이름을 가리거나 다시 표시합니다. 정보가 민감한 환경에서 화면을 공유할 때 유용합니다.

Web



Mobile



- **새로고침**: 목록을 즉시 새로고침해 최신 상태로 갱신합니다. 목록 하단의 **새로고침**에서 자동 새로고침 간격(**사용안함**/**5초**/**1분**)을 선택하면 설정한 주기마다 목록을 자동 갱신합니다.
- **이름으로 검색...**: 사용자 이름으로 목록을 검색합니다.

재실 목록 필터링

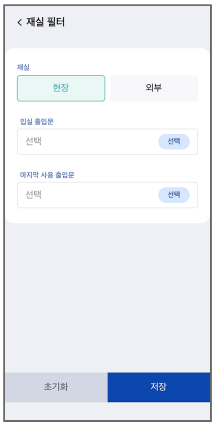
Web

재실 상태 열에 있는 버튼을 클릭하면 **현장**, **외부**, 전체 사용자 중에서 원하는 조건으로 목록을 필터링할 수 있습니다. 그 외에도 **출입한 문**, **마지막 사용 문** 열에서 원하는 조건으로 필터링할 수 있습니다.



> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 클릭하세요.

Mobile



1. 재실 목록 오른쪽 상단의 **필터**를 탭하세요.
2. **현장** 또는 **외부** 상태를 선택하거나 모두 선택하세요.
3. **입실 출입문**, **마지막 사용 출입문**에서 원하는 조건을 선택하세요.
4. 선택한 조건으로 목록을 필터링하려면 **저장** 버튼을 탭하세요.

> **알아두기**
> 필터링을 해제하려면 **초기화** 버튼을 탭하세요.

> **알아두기**
> - 전체 사용자를 확인하려면 **재실 상태** 열에서 **현장**, **외부**를 모두 선택하세요.
> - 재실 목록은 **현장** 상태의 사용자를 기본 표시합니다.

재실 상태 수동 변경

실제 상황과 시스템에 기록된 재실 상태가 다를 때 관리자가 직접 상태를 변경할 수 있습니다.

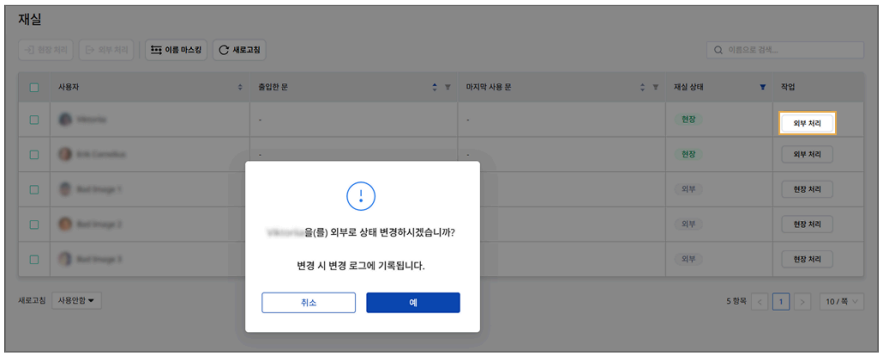
- 재실 정확도는 사이트의 입실 및 퇴실 장치 구성에 따라 달라집니다. 입실 및 퇴실 장치가 명확하게 구성된 사이트일수록 더 신뢰도 높은 재실 정보를 제공합니다.
- 장치가 오프라인이었거나 이벤트 전달이 지연되면, 재실 상태는 동기화가 끝난 뒤에 갱신될 수 있습니다.
- 재실 상태는 출입 권한과 다릅니다. **현장** 상태로 표시된 사용자라도 모든 출입문에 접근할 수 있는 것은 아닙니다.
- 만료, 비활성, 정지 상태인 사용자는 계정이 활성화되기 전까지 재실 상태를 변경할 수 없습니다.

> **알아두기**
>
> 수동 변경은 시스템에 기록된 상태를 바꿀 뿐, 사용자의 실제 위치를 물리적으로 확인하는 기능이 아닙니다. 변경 이력은 **모니터링** → **변경 로그**에서 확인할 수 있습니다.

개별 사용자의 재실 상태 변경

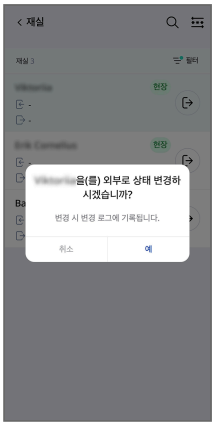
Web

1. 목록에서 상태를 변경할 사용자의 **작업** 열에서 **현장 처리** 또는 **외부 처리** 버튼을 클릭하세요.



2. 확인 메시지가 나타나면 **예** 버튼을 클릭하세요.

Mobile

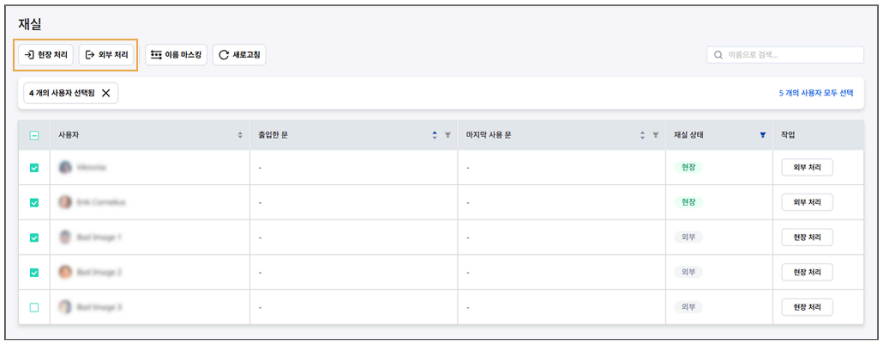


1. 목록에서 상태를 변경할 사용자의 ⎋ 또는 ⎋ 버튼을 탭하세요.
2. 확인 메시지가 나타나면 **예** 버튼을 탭하세요.

여러 사용자의 재실 상태 변경

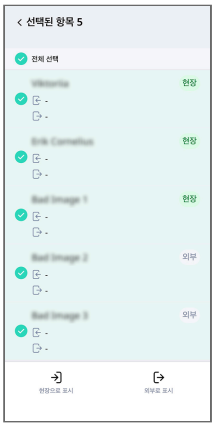
Web

1. 목록에서 상태를 변경할 사용자의 체크박스를 클릭하세요. 한 명 이상의 사용자를 선택할 수 있습니다.
2. 목록 상단의 **현장 처리** 또는 **외부 처리** 버튼을 클릭하세요.



3. 확인 메시지가 나타나면 **예** 버튼을 클릭하세요.

Mobile



1. 목록에서 상태를 변경할 사용자를 길게 누르세요.
2. 상태를 변경할 사용자를 선택하세요. 한 명 이상의 사용자를 선택할 수 있습니다.
3. 화면 하단의 **현장으로 표시**( ) 또는 **외부로 표시**( ) 버튼을 탭하세요.
4. 확인 메시지가 나타나면 **예** 버튼을 클릭하세요.

비상 호출

BioStar Air의 비상 호출(Roll Call) 기능을 통해 조직은 비상 상황 발생 시 어떤 사용자가 안전하게 대피했는지 추적할 수 있습니다. 소집 구역을 설정하고 BioStar Air 모바일 앱으로 비상 호출을 진행하면, 관리자는 재실 정보를 기반으로 실제 현장에 있던 사용자를 신속하게 파악하고 안전 여부를 확인할 수 있습니다.

재실(Presence) 기반의 정확한 소집 명단

- 비상 호출은 모든 사용자가 현장에 있다고 가정하지 않습니다. 재실(Presence) 로직을 함께 사용해, 비상 상황이 발생한 시점에 실제로 현장에 있는 것으로 확인된 사용자만 소집 대상으로 표시합니다.
- 사용자 그룹을 특정 소집 구역에 배정하고 전담 관리자를 지정할 수 있어, 안전 담당자는 자신이 맡은 사용자만 집중해서 관리할 수 있습니다.
- Suprema Pass 앱은 현장에 있는 모바일 크리덴셜 사용자에게 올바른 소집 구역을 안내하고, 외부에 있는 사용자에게는 비상 상황이 진행되는 동안 시설에 들어오지 말라고 경고합니다.

알아두기

- 사용자 그룹에 소집 구역이 올바르게 할당되었는지 확인하여 혼란을 방지하세요.
- 실제 비상 상황 발생 시 원활한 진행을 위해 비상 호출 기능을 정기적으로 테스트하세요.
- 출입 기록을 통해 안전 규정 준수를 위한 출석을 확인할 수 있습니다.

> **팁**
> 비상 호출 및 소집 구역에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

시작하기 전에

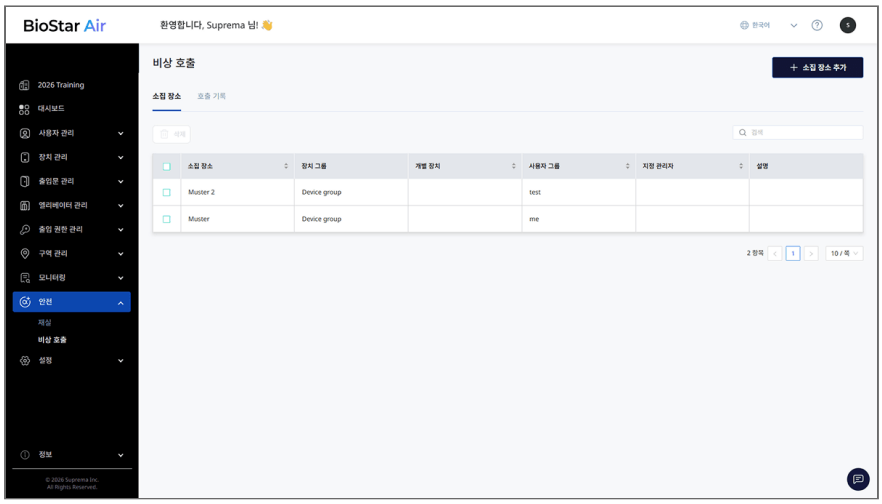
- 비상 호출의 정확도는 재실 감지에 따라 달라집니다. **경계 구역**이 올바르게 구성되지 않으면 비상 호출 목록이 실제 현장 인원과 다를 수 있습니다.
- 모바일 알림에는 Suprema Pass 앱이 필요합니다. RF 카드나 바이오메트릭 크리덴셜만 사용하는 사용자는 모바일 비상 호출 알림을 받을 수 없습니다.
- 소집 구역에 배정되지 않은 현장 사용자는 소집 장소 안내를 받지 못할 수 있습니다.
- **지정 관리자** 설정이 올바르지 않으면 담당자가 예상한 비상 호출 화면이 나타나지 않을 수 있습니다.
- 장치가 오프라인이었거나 이벤트 전달이 지연되면 재실 정보와 비상 호출 정확도에 영향을 줄 수 있습니다.
- 비활성 상태인 사용자는 비상 호출 알림을 받지 못합니다.

> **알아두기**
> 이전 버전의 Suprema Pass 또는 BioStar Air 앱을 사용하는 사용자와 관리자는 기존 비상 호출 방식을 계속 사용할 수 있지만, 새로운 기능을 사용하려면 최신 버전으로 업데이트해야 합니다.

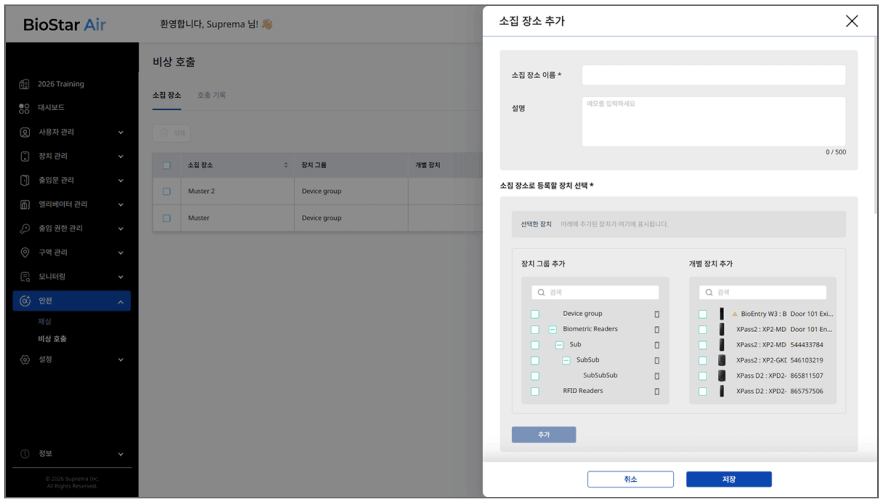
소집 구역 설정

소집 구역은 사용자가 비상 상황에서 자신이 안전하다는 것을 표시하기 위해 크리덴셜을 인증할 수 있는 지정된 장소입니다.

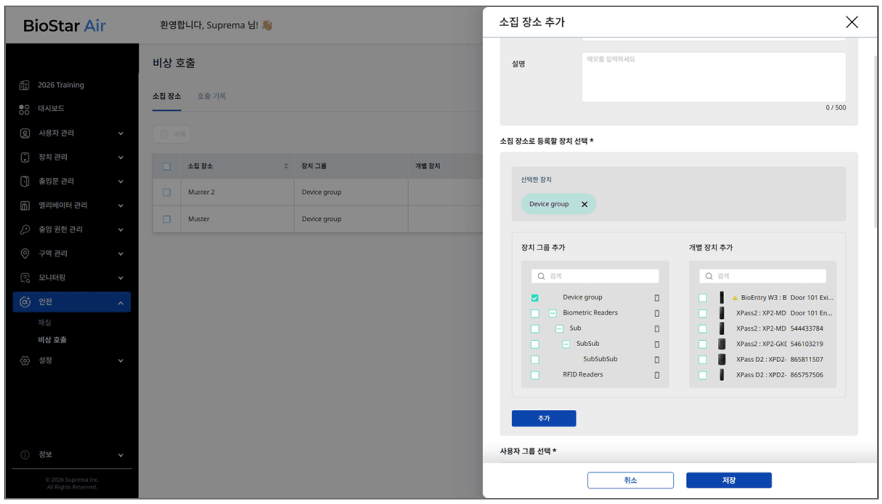
1. 화면 왼쪽 사이드바에서 **안전** → **비상 호출**을 클릭하세요.
2. 화면 오른쪽 상단의 **소집 장소 추가** 버튼을 클릭하세요.



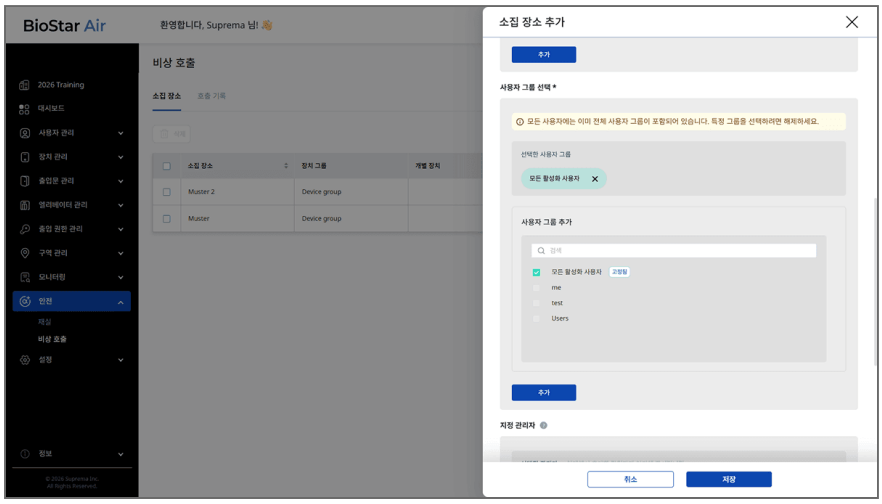
3. **소집 장소 추가** 패널이 나타나면 소집 장소 이름과 설명(선택 사항)을 입력하세요.



4. **소집 장소로 등록할 장치 선택 *** 섹션에서 소집 구역에 할당할 장치 그룹 또는 장치를 추가하세요. 장치 그룹 또는 장치의 체크박스를 클릭하고 **추가** 버튼을 클릭하세요.

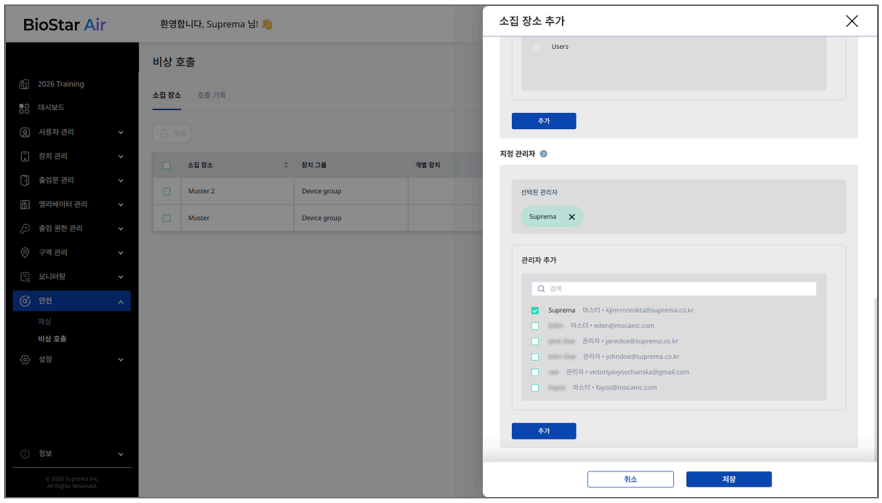


5. **사용자 그룹 선택 *** 섹션에서 소집 구역에 도착했을 때 보고해야할 사용자 그룹을 선택하세요.



- 특정 사용자 그룹을 선택하려면 원하는 그룹의 체크박스를 선택하고 **추가** 버튼을 클릭하세요.
- **모든 활성화 사용자**: BioStar Air 사이트에 현재 활성 상태인 모든 사용자를 선택한 소집 구역으로 지정합니다. 실제 비상 호출을 실행하면 모든 활성 사용자를 현장에 있다고 가정하지 않고, 재실 감지를 기반으로 사이트에 있는 것으로 확인된 사용자만 소집 대상으로 합니다. 이 옵션을 켜면 개별 사용자 그룹 선택 기능은 비활성화되며, 특정 그룹만 선택하려면 이 옵션을 먼저 꺼야 합니다.

6. **지정 관리자** 섹션에서 해당 소집 장소에서 비상 호출을 진행할 관리자의 체크박스를 선택하고 **추가** 버튼을 클릭하세요.



> - **지정 관리자**를 선택했다면, 선택된 관리자만 해당 비상호출을 시작할 수 있으며, 진행 중인 비상 호출에서도 자신이 담당하는 소집 구역의 사용자만 확인하고 관리할 수 있습니다.
> - **지정 관리자**를 지정하지 않으면 **마스터**, **관리자** 또는 **오퍼레이터** 등급의 사용자가 비상 호출을 시작할 수 있습니다.
> - 한 명의 관리자는 동시에 여러 소집 구역에 지정 관리자로 배정될 수 없습니다.

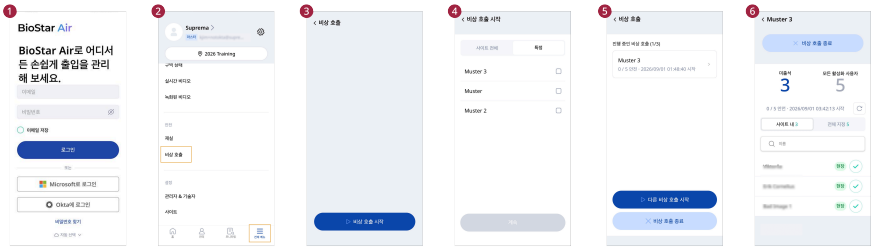
7. 소집 구역 설정을 저장하려면 **저장** 버튼을 클릭하세요.

> **소집 구역에 대한 모범 사례**
> - 소집 구역 이름과 설명은 명확하고 이해하기 쉽게 지정하세요. 예를 들어, '동쪽 주차장' 또는 '본관 로비'와 같이 지정할 수 있습니다.
> - 소집 구역에 여러 개의 장치를 추가할 경우 개별 장치를 선택하는 것보다 장치 그룹을 선택하기를 권장합니다. 장치 그룹을 사용하면 여러 장치를 한 번에 관리할 수 있습니다. 장치 그룹 관리에 대한 자세한 내용은 장치 및 패널 그룹 관리하기를 참고하세요.
> - 여러 건물이 있는 대규모 캠퍼스에서는 **관련 사용자만** 특정 소집 구역에 배정하도록 하세요.
> - 유선 출입 통제 장치는 모바일과 카드 인증을 모두 지원하는 반면, 에어팝 태그(Airfob Tag)와 에어팝 패치(Airfob Patch)는 모바일 크리덴셜만 지원합니다.

비상 호출 시작

모바일에서 시작

BioStar Air 모바일 앱에서 비상 호출을 시작하고 출석을 확인하세요.



1. 모바일 기기에서 BioStar Air 앱을 실행하고 로그인하세요.
2. 화면 하단의 **전체 메뉴** → **비상 호출**을 차례로 탭하세요.

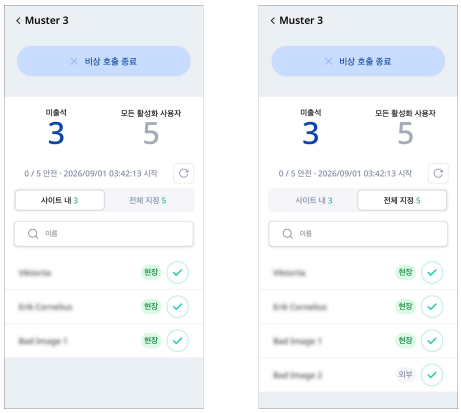
3. **비상 호출 시작** 버튼을 탭하세요.
4. 비상 호출을 시작할 소집 구역을 선택하고, **계속** 버튼을 클릭하세요.

   모든 소집 구역에서 비상 호출을 진행하려면 **사이트 전체**를 선택하고, **계속** 버튼을 클릭하세요.
5. 진행 중인 비상 호출 목록에서 소집 구역을 선택하세요.
6. 소집 장소에 모여야할 모든 사용자 목록이 표시됩니다.

> **관리자 역할에 따른 차이**
> - 소집 구역의 **지정 관리자**로 지정되지 않은 **마스터**, **관리자**, **오퍼레이터**는 위 순서대로 비상 호출 목록을 직접 확인하고 새 비상 호출을 시작합니다.
> - **지정 관리자**는 자신이 담당하는 소집 구역에서 비상 호출이 시작되면 알림을 받습니다. 알림을 탭하면 목록을 거치지 않고 담당 소집 구역의 진행 화면으로 바로 이동합니다.

진행 중인 비상 호출 화면 살펴보기

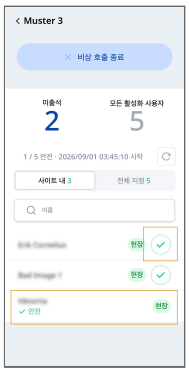
비상 호출이 시작되면 소집 구역 이름과 함께 진행 현황이 표시됩니다.



- 화면 상단에 **미출석**과 **모든 활성화 사용자** 인원 수를 확인할 수 있습니다.

  인원 수 아래에 **안전하다고 표시된 인원/전체 인원**과 **비상 호출 시작 시각**이 표시됩니다. 새로고침(↻) 버튼으로 최신 상태를 확인할 수 있습니다.
- 목록에 표시할 사용자 범위를 전환할 수 있습니다.
  - **사이트 내**: 현재 재실 상태가 현장(On Site)인 사용자만 표시합니다.
  - **전체 지정**: 재실 상태와 관계없이 이 소집 구역에 배정된 사용자 전체를 표시합니다. 안전하다고 표시된 사용자는 목록의 맨 아래로 이동합니다.
- 검색 기능으로 특정 사용자를 찾을 수 있습니다.
- 목록의 각 사용자 오른쪽에서 재실 상태(**현장**/**외부**)를 확인할 수 있습니다.

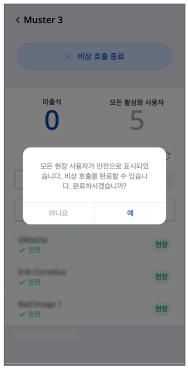
사용자가 안전하다고 표시하기



관리자 또는 사용자는 아래 방법으로 자신이 안전하다고 표시할 수 있습니다.

- 관리자는 모바일 앱에서 사용자 이름 옆에 있는 **체크 표시** 버튼을 길게 눌러서 사용자가 안전하다고 체크할 수 있습니다.
- 사용자는 지정된 소집 구역에서 장치에 자신의 크리덴셜을 태깅하세요.

비상 호출 완료



아래의 사항이 충족되면 비상 호출을 완료합니다.

- 소집 범위에 포함된 현장 사용자, 즉 **미출석** 인원이 0이 되어 나타나는 완료 메시지 창에서 **예** 버튼을 탭할 때
- 관리자가 모든 사용자를 수동으로 안전하다고 표시하고, **비상 호출 종료** 버튼을 탭할 때
- 24시간이 경과했을 때

역할별 종료 범위

- 사이트 마스터는 비상 호출을 하나씩 개별적으로 종료하거나, 여러 건을 선택해 한 번에 종료하거나, 사이트에서 진행 중인 모든 비상 호출을 한 번에 종료할 수 있습니다.
- **지정 관리자**로 선택된 관리자 또는 오퍼레이터는 자신이 담당하는 소집 구역의 비상 호출만 종료할 수 있습니다.

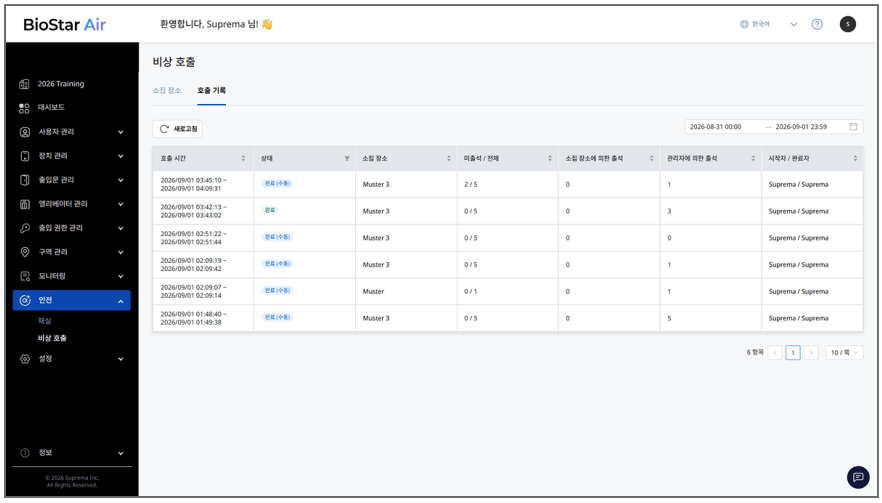
알아두기

외부 상태인 사용자도 수동으로 안전하다고 표시할 수 있습니다. 예를 들어 당일 재택근무 중인 사용자를 안전하다고 미리 확인해 둘 수 있습니다.

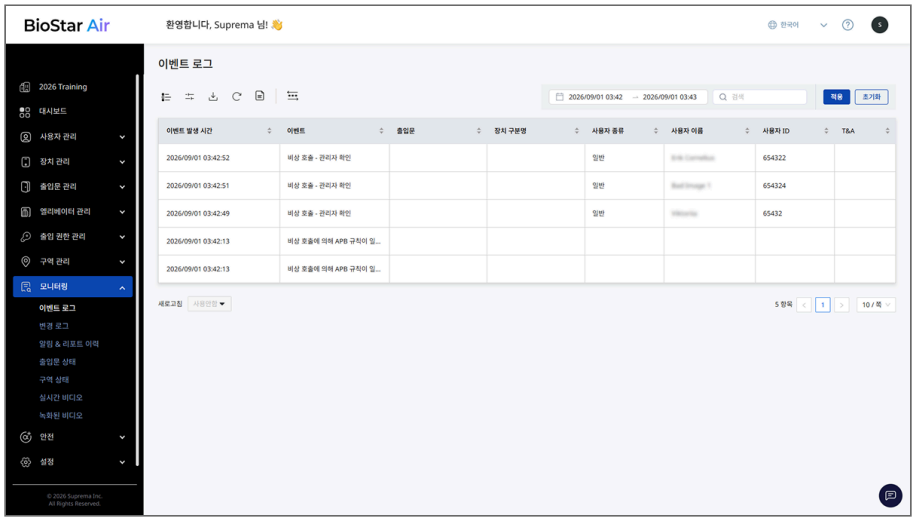
비상 호출 내역 보기

이전에 실시한 비상 호출 내역을 확인할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **안전** → **비상 호출**을 클릭하세요.
2. **호출 기록** 탭을 클릭하세요.



3. 세부 사항을 확인하려면 완료된 비상 호출 항목을 클릭하세요.



- 비상 호출 중 기록된 모든 출입 이벤트 목록을 확인할 수 있습니다.
- 사용자가 안전하다고 표시되었는지 또는 확인되지 않았는지에 대한 세부 정보를 확인할 수 있습니다.
- 비상 호출 시작 및 완료 시간을 확인할 수 있습니다.

사이트 설정하기

BioStar Air 시스템을 원활하게 운영하기 위한 기본 설정들을 관리합니다. 운영 권한을 가진 관리자 계정 관리, 조직의 기본 정보 설정, 시간대 및 알림 구성, 이메일 템플릿 사용자정의, 카드 형식 설정 등을 통해 시스템을 조직의 요구사항에 맞게 구성할 수 있습니다.

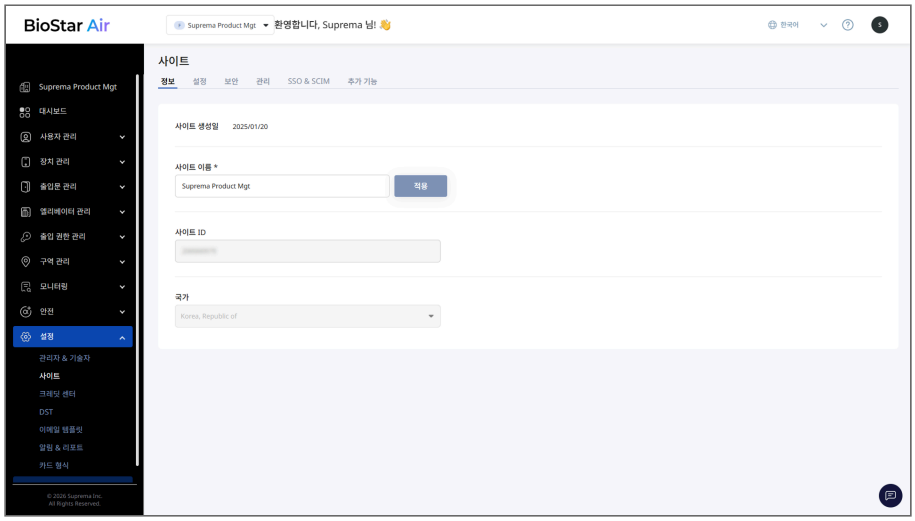
> **팁**
> 사이트 설정에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

기본 정보 설정하기

사이트 정보는 BioStar Air에서 가장 기본적인 설정입니다. 이 문서에서는 사이트명, 식별자 등의 기본 정보를 관리하거나 필요시 사이트 삭제하는 방법을 안내합니다.

사이트 정보 설정

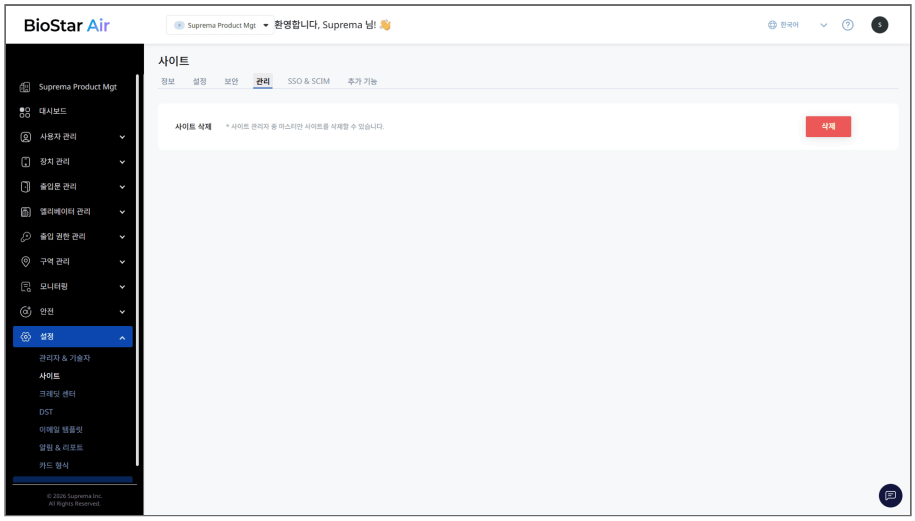
화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **정보** 탭에서 사이트의 기본 정보를 수정할 수 있습니다.



- **사이트 이름**: 사이트의 이름입니다. 새 이름을 입력하고 **적용** 버튼을 클릭하세요. 언제든지 변경할 수 있습니다.
- **사이트 ID**: 지원 요청 시 필요한 고유 식별자입니다. 모카(MOCA) 팀과 소통할 때 사이트 ID를 복사하여 제공할 수 있습니다.
- **국가**: 사이트 생성 시 설정되며 나중에 변경할 수 없습니다. 변경이 필요하면 BioStar Air 파트너 포털을 통해 진행해야 합니다.

사이트 삭제

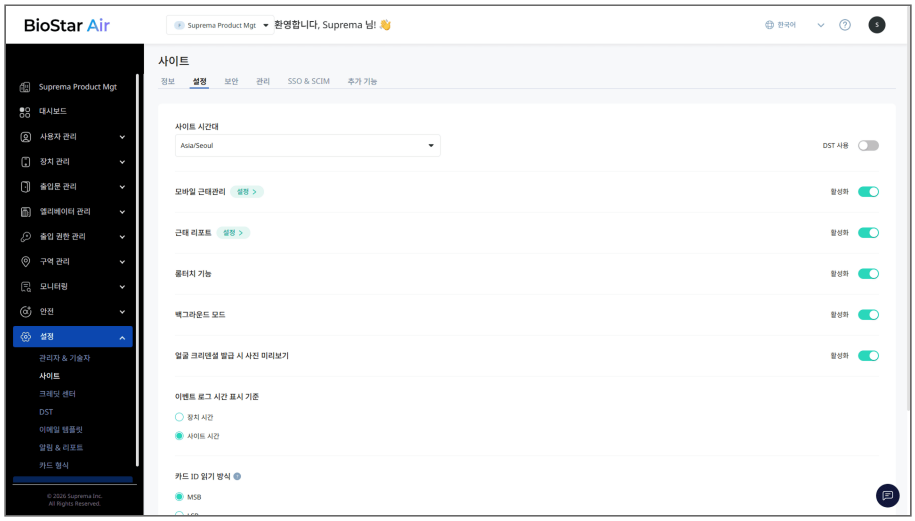
화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **관리** 탭에서 사용할 수 있는 유일한 옵션은 **사이트 삭제** 기능입니다. 이 작업은 되돌릴 수 없으며 **마스터 관리자**만 사이트를 삭제할 수 있습니다.



고급 설정하기

고급 옵션을 구성하여 BioStar Air를 조직의 업무 환경에 맞게 최적화하세요. 시간대와 일광 절약 시간을 설정하고, 근태 관리를 활성화하며, 모바일 인증 방식과 이벤트 로그 표시 방법을 조정할 수 있습니다.

화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **설정** 탭에서 사이트의 설정을 구성할 수 있습니다.



- **사이트 시간대**: 시간대는 언제든지 변경할 수 있습니다. 설정한 시간대에 따라 로그 및 이벤트를 기록합니다. 자세한 내용은 일광 절약 시간(DST) 구성하기를 참고하세요.
  - **DST 사용**: 특정 지역에서 적용되는 일광 절약 시간을 활성화하거나 비활성화하세요.
- **모바일 근태관리**: 근태 관리(T&A) 기능을 활성화할 수 있습니다. 근태 관리 기능을 활성화한 후 **설정** 버튼을 클릭해 세부 설정을 구성하세요. 자세한 내용은 근태 관리(T&A) 구성하기를 참고하세요.
- **근태 리포트**: 근태 보고서(T&A Report)를 생성할 수 있습니다. 근태 보고서 기능을 활성화한 후 **설정** 버튼을 클릭해 보고서 생성 조건을 구성하세요. 자세한 내용은 근태 보고서 구성하기를 참고하세요.
- **롱터치 기능**: 일정 거리 떨어진 출입문을 원격으로 열 수 있는 롱터치(Long Touch) 기능을 활성화할 수 있습니다.
- **백그라운드 모드**: 슈프리마 패스 앱이 백그라운드 모드일 때 모바일 카드를 사용할 수 있도록 허용합니다. 이 설정을 활성화하면 사용자가 앱을 열지 않고도 출입문을 열 수 있습니다.
- **얼굴 크리덴셜 발급 시 사진 미리보기**: 얼굴 크리덴셜을 발급할 때 얼굴 사진 미리보기를 표시할 수 있습니다.
- **이벤트 로그 시간 표시 기준**: 이벤트 로그의 시간 표시 방법을 설정합니다.
  - **장치 시간**: 각 장치의 설정에서 구성한 시간대를 기준으로 이벤트 로그를 표시합니다.
  - **사이트 시간**: 사이트의 시간대에 따라 로그를 표시합니다. 모든 장치가 한 위치에 있는 사이트에 유용합니다. **사이트 시간대** 옵션을 참고하세요.
- **카드 ID 읽기 방식**: 에어팝 패치(Airfob Patch)를 타사 리더기와 함께 사용할 때 카드 데이터를 전송하는 방법을 설정합니다.

> 패치 장치 전용 설정으로, 패치를 부착하는 타사 장치의 타입에 맞게 설정할 수 있습니다.

- **모바일 출입카드 활성화/재발급 링크 유효기간**: 모바일 크리덴셜의 기본 유효 기간을 설정합니다.

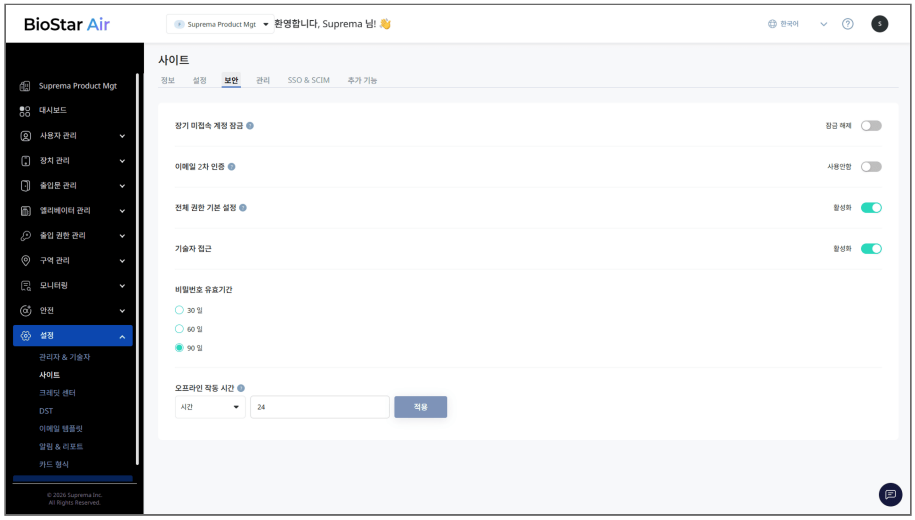
> 관리자는 개별 사용자의 크리덴셜에 대해 별도의 만료 날짜를 설정할 수 있습니다. 자세한 내용은 사용자 추가하기를 참고하세요.

보안 설정하기

무단 접근을 방지하고 사이트를 안전하게 운영하려면 보안 정책을 적절히 구성해야 합니다. 비활성 관리자 계정 잠금, 이메일 2차 인증,

비밀번호 변경 주기 설정 등을 통해 사이트 보안 수준을 강화할 수 있습니다.

화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **보안** 탭에서 사이트 보안과 관련한 설정을 구성할 수 있습니다.



- **장기 미접속 계정 잠금**: 90일 이상 접속하지 않은 관리자 계정을 잠금 상태로 변경할 수 있습니다.
- **이메일 2차 인증**: 관리자 계정으로 로그인할 때마다 이메일 2차 인증을 요구할 수 있습니다.
- **전체 권한 기본 설정**: 다른 출입 권한이 선택되지 않은 경우, 신규 사용자에게 '전체 출입 권한'을 기본 부여합니다. 이 설정을 비활성화하면 수동으로 출입 레벨을 할당해야 합니다. 임시 사용자는 위 설정이 활성화되어 있어도 자동으로 전체 출입 권한을 허용하지 않습니다.

> 출입 레벨 관리에 대한 자세한 내용은 출입 레벨 관리하기를 참고하세요.

- **기술자 접근**: 기술자 계정이 사이트에 접근할 수 있도록 허용합니다. 이 설정이 비활성화된 경우, 기술자 계정은 사이트에 접근할 수 없습니다.

> 기술자 계정의 사이트 접근 권한 관리 방법에 대한 자세한 내용은 사이트에 기술자 배정하기를 참고하세요.

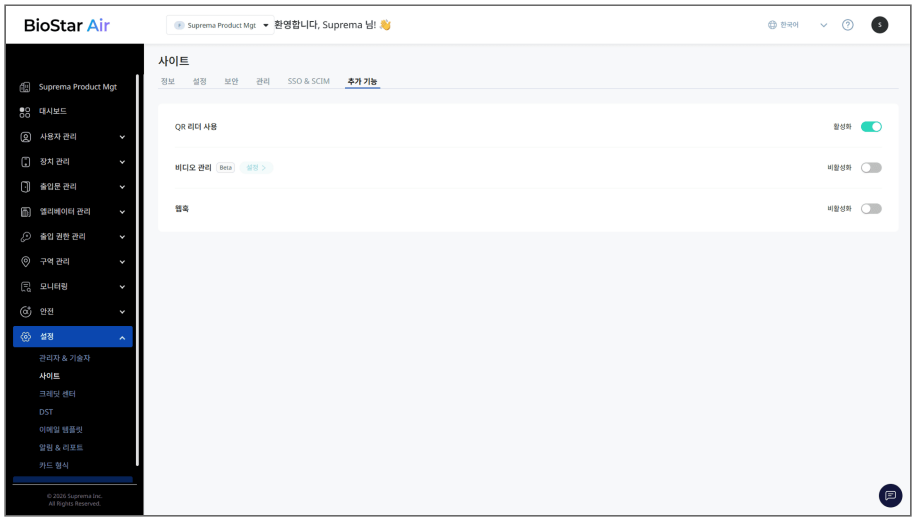
- **비밀번호 유효기간**: 30일 또는 60일, 90일마다 비밀번호를 재설정하도록 설정할 수 있습니다.
- **오프라인 작동 시간**: 모바일 기기에 네트워크 연결이 없더라도 모바일 크리덴셜이 유효한 시간을 설정할 수 있습니다.

> – 기본값은 5분이며, 1분에서 8일 사이로 설정할 수 있습니다.
> – 보안과 편의성의 균형을 맞추는 데 유용하며, 특히 네트워크 연결이 제한된 원격 사이트에서 유용합니다.

추가 기능 설정하기

QR 코드 리더기 사용 여부, ONVIF 카메라 연동, 외부 시스템으로의 이벤트 전송(웹훅) 등 사이트 운영에 필요한 확장 기능을 활성화하거나 비활성화할 수 있습니다.

화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **추가 기능** 탭에서 추가 기능을 활성화하거나 비활성화할 수 있습니다.



- **QR 리더 사용**: QR 코드 리더기를 지원합니다. QR 리더기를 사용하지 않는다면 해당 옵션을 비활성화하세요.
- **비디오 관리**: ONVIF 호환 IP 카메라를 지원합니다. BioStar Air와 비디오 감시를 통합하려면 이 기능을 활성화하세요. 기능을 활성화한 후 **설정** 버튼을 클릭하면 이벤트 로그 재생 시간을 설정할 수 있습니다.

> 비디오 관리에 대한 자세한 내용은 IP 카메라 지원 및 설정하기을 참고하세요.

- **웹훅**: 웹훅을 활성화하여 BioStar Air의 이벤트를 외부 시스템으로 전송할 수 있습니다. 이 기능을 활성화한 후 아래 필드를 구성하세요.



  - **웹훅 URL**: 이벤트를 수신할 외부 서버의 엔드포인트 주소를 입력하세요. 예: `https://example.com/webhook-endpoint`
  - **보안 키**: 웹훅 요청이 신뢰할 수 있는 발신 서버에서 전송되었는지 검증하는 보안 토큰입니다. 발신 서버는 보안 키를 이용해 데이터 본문(Payload)을 SHA256으로 암호화하고, 헤더에 `X-Signature`로 전송합니다.
  - **테스트 전송**: 웹훅이 올바르게 작동하는지 확인할 수 있습니다. 테스트 메시지를 전송하여 외부 서버가 요청을 수신하고 응답하는지 검증하세요.

> **알아두기**
>
> - 필요한 정보를 모두 입력했다면 **저장** 버튼을 클릭하세요.
> - 입력한 정보를 초기화하려면 **초기화** 버튼을 클릭하세요.

관리자 계정 및 역할 관리하기

BioStar Air의 관리자 계정 및 역할 관리를 통해 사이트 접근 권한을 효과적으로 제어할 수 있습니다. 옵저버(Observer), 오퍼레이터(Operator), 관리자(Administrator), 마스터(Master) 4가지 역할을 할당하여 각 담당자에게 필요한 권한만 부여함으로써 보안과 운영 효율성을 동시에 확보하세요.

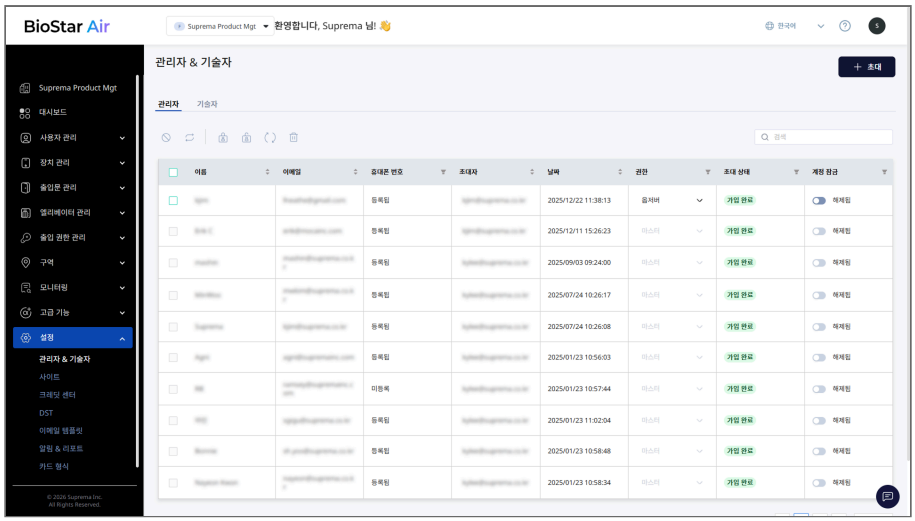
이 문서에서는 관리자 초대부터 역할 할당, 권한 관리, 계정 잠금까지 관리자 계정 수명 주기 전 과정을 안내합니다.

팁

관리자 관리에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

관리자 보기

화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.



알아두기

기술자 접근 옵션을 활성화하면 **설정** → **관리자** 메뉴가 **관리자 & 기술자** 메뉴로 변경됩니다. **관리자**와 **기술자** 탭으로 나뉘어져 관리자 계정과 기술자 계정을 각각 관리할 수 있습니다.

기술자 접근 옵션을 활성화하는 방법에 대한 자세한 내용은 기술자 계정 관리하기를 참고하세요.

관리자 목록

관리자 & 기술자 메뉴에서는 모든 관리자 목록을 확인할 수 있습니다. 관리자 목록에는 다음 정보를 포함합니다.

- **이름**: 관리자의 이름입니다.
- **이메일**: 관리자의 이메일 주소입니다.
- **모바일**: 관리자의 전화 번호입니다.
- **초대자**: 관리자를 초대한 사람의 이메일입니다.
- **날짜**: 관리자가 초대된 날짜입니다.
- **권한**: 관리자의 권한 레벨입니다. 자세한 내용은 관리자 레벨을 참고하세요.
- **초대 상태**: 관리자 계정의 초대 상태입니다. 자세한 내용은 초대 상태를 참고하세요.
- **계정 잠금**: 관리자 계정의 잠금 상태입니다. 계정을 잠김 처리하거나 잠금 해제할 수 있습니다. 자세한 내용은 관리자 잠금/해제를 참고하세요.

초대 상태

관리자 목록에서는 각 관리자의 초대 상태를 확인할 수 있습니다.

가입 대기 상태

초대된 관리자가 이메일 초대를 수락하여 가입을 완료하기 전까지, 초대 상태는 **가입 대기** 상태로 표시됩니다. 초대된 관리자는 이메일 내의 링크를 클릭하여 계정을 등록하거나 로그인하여 사이트에 진입할 수 있습니다.

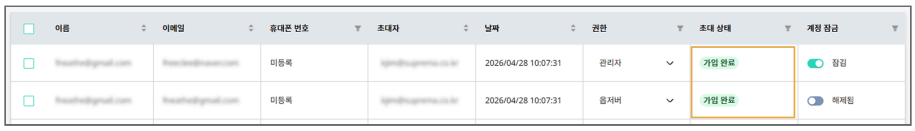


알아두기

초대된 관리자는 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 **만료됨** 상태로 변경됩니다. 초대장이 만료되면 해당 계정이 다시 가입할 수 있도록 초대 링크를 재전송할 수 있습니다. 초대 링크 재전송에 대한 자세한 내용은 초대 링크 재전송을 참고하세요.

가입 완료 상태

초대된 관리자가 이메일 초대를 수락하여 가입을 완료하면, 초대 상태는 **가입 완료** 상태로 변경됩니다. 가입이 완료된 관리자는 사이트에 로그인하여 부여받은 역할에 따라 메뉴와 기능에 접근할 수 있습니다.



초대 취소 상태

초대된 관리자의 이메일 주소를 잘못 입력했거나 더 이상 관리자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다. 초대를 취소하면 초대 상태가 **취소됨** 상태로 변경됩니다. 관리자 초대 취소에 대한 자세한 내용은 초대 취소를 참고하세요.



관리자 레벨

BioStar Air의 각 관리자 레벨은 특정 권한을 가지며, 높은 레벨은 낮은 레벨의 권한을 상속받습니다.

알아두기

각 관리자 역할은 BioStar Air 전반에 걸쳐 서로 다른 권한을 가지고 있습니다. **옵저버**는 가장 제한된 접근을 가지며, 화면에 나타나지 않는 제한된 메뉴가 있습니다.

권한 비교

기능	옵저버	오퍼레이터	관리자	마스터
대시보드/로그 조회	✔	✔	✔	✔
로그 내보내기 및 보고서 생성	✔	✔	✔	✔

기능	옵저버	오퍼레이터	관리자	마스터
사용자 관리	✕	✔	✔	✔
사용자 그룹 관리	✕	✔	✔	✔
출입 레벨 관리	✕	✔	✔	✔
스케줄 관리	✕	✔	✔	✔
휴일 그룹 관리	✕	✔	✔	✔
장치 제어 및 설정	✕	✕	✔	✔
관리자 초대	✕	✕	✔	✔
마스터 역할 할당	✕	✕	✕	✔
마스터 관리자 수정/삭제	✕	✕	✕	✔
하위 사이트 생성	✕	✕	✕	✔
사이트 설정 구성	✕	✕	✕	✔

옵저버 (Lowest Level)

- **대시보드**와 로그를 **볼 수 있습니다**.
- 로그를 **내보내고** 보고서를 생성할 수 있습니다.
- 설정, 사용자 또는 장치를 수정할 수 **없습니다**.
- 메뉴 진입에 제한됩니다. 대부분의 메뉴가 화면에 나타나지 않습니다.

오퍼레이터

- **사용자** 및 **사용자 그룹 출입 레벨**, **스케줄**, **휴일 그룹**을 관리할 수 있습니다.
- 장치 제어 또는 관리 설정에 대한 접근 권한이 **없습니다**.
- 일상적인 사용자 및 출입 구성을 관리하는 데 적합합니다.

관리자

- 새로운 관리자를 **초대할 수 있습니다**. 하지만 **마스터** 역할을 할당할 수는 없습니다.
- **전체 장치 제어** 권한이 있어 설정을 수정하고 연결된 장치를 관리할 수 있습니다.
- **마스터** 역할의 관리자를 삭제하거나 수정할 수 없습니다.
- 일반적으로 시스템 관리를 담당하는 IT 담당자에게 역할을 할당할 것을 권장합니다.

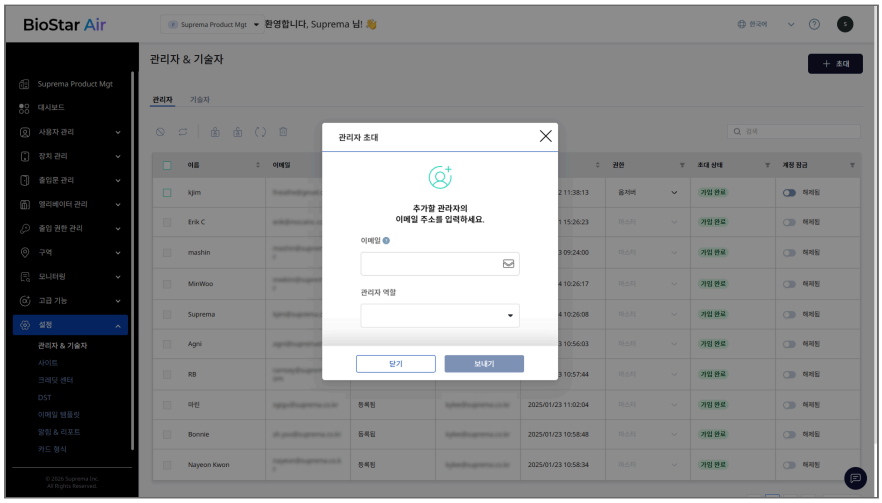
마스터 (Highest Level)

- 모든 설정 및 기능에 **전체 접근** 권한이 있습니다.
- **Administrators**에 의해 삭제되거나 수정될 수 **없습니다**.
- **하위 사이트**를 생성하여 다양한 위치 또는 조직을 관리할 수 있습니다.
- **사이트 설정**을 구성할 수 있으며, 여기에는 중요한 시스템 전체 구성도 포함됩니다.
- 다른 관리자가 로그인하기 전에 **약관**에 동의할 책임이 있습니다.
- 일반적으로 회사 소유자 또는 높은 신뢰를 받는 임원에게 할당할 수 있습니다.

새로운 관리자 초대

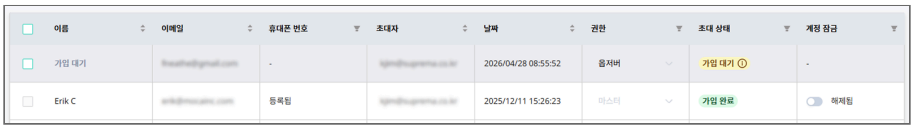
새로운 관리자를 추가할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.
2. 화면 오른쪽 상단의 **초대** 버튼을 클릭하세요.
3. **관리자 초대** 창이 나타나면 이메일 주소를 입력하세요.



4. **관리자 역할**에서 새로운 관리자에게 할당할 역할을 선택하세요.
5. 초대장을 보내려면 **보내기** 버튼을 클릭하세요.

초대된 계정은 관리자 목록에서 **초대 상태**가 **가입 대기** 상태로 표시됩니다. 초대된 계정이 이메일을 통해 초대를 수락하면 **초대 상태**가 **가입 완료** 상태로 변경됩니다.

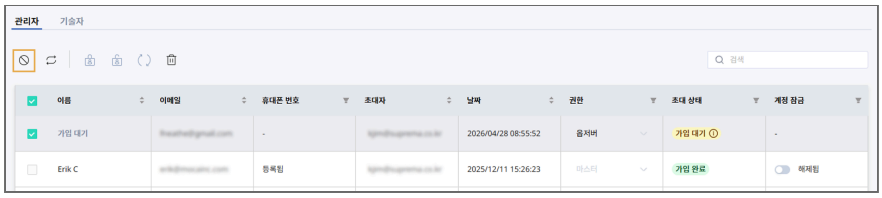


- 초대 받은 계정은 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 **만료됨** 상태로 변경됩니다.
- 각 관리자는 고유한 이메일 주소를 가져야 합니다. 필요하다면 별칭 주소(예: erik+training@example.com)를 사용할 수 있습니다.
- 초대 메일을 받은 관리자는 이메일 내의 링크를 클릭하세요. 계정을 등록하지 않은 관리자는 회원 가입을 진행하세요. 이미 계정이 있는 관리자는 로그인 후 바로 **사이트**에 진입할 수 있습니다.

초대 취소

초대된 계정이 아직 초대를 수락하지 않았다면, 초대를 취소할 수 있습니다. 초대를 취소하면 가입 대기 상태인 계정은 이메일의 초대 링크로 가입할 수 없습니다.

1. 관리자 목록에서 초대 상태가 **가입 대기** 상태인 계정의 체크박스를 클릭하세요. 1명 이상의 계정을 선택할 수 있습니다.
2. 관리자 목록 왼쪽 상단의 ⃠ 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

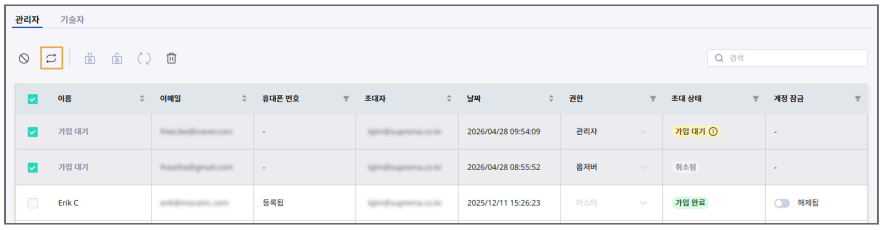
관리자 목록에서 초대를 취소한 계정은 초대 상태가 **취소됨** 상태로 변경됩니다.



초대 링크 재전송

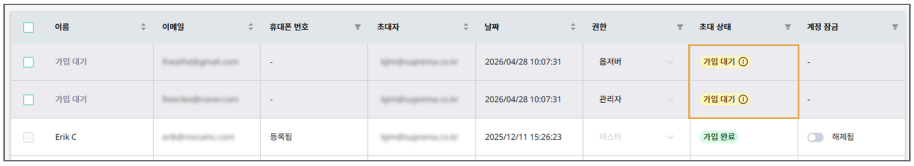
초대된 계정이 초대 이메일을 받지 못했거나 초대 이메일을 분실했을 때, 또는 초대 링크가 만료되었을 때 초대 링크를 재전송할 수 있습니다. 초대 링크를 재전송하면 해당 사용자는 새로운 초대 링크를 통해 가입할 수 있습니다.

1. 관리자 목록에서 초대 상태가 **가입 대기** 또는 **만료됨**, **취소됨** 상태인 계정의 체크박스를 클릭하세요. 1명 이상의 계정을 선택할 수 있습니다.
2. 관리자 목록 왼쪽 상단의 ⟲ 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

초대 링크를 재전송한 계정은 초대 상태가 **가입 대기** 상태로 변경됩니다.



관리자 잠금/해제

이메일 초대를 수락하여 가입 완료한 관리자는 **계정 잠금** 옵션을 통해 계정을 잠그거나 해제할 수 있습니다. 계정을 잠그면 해당 관리자는 사이트에 로그인할 수 없으며, 계정 정보는 유지되어 나중에 필요할 때 계정을 다시 활성화할 수 있습니다.

잠김 상태의 관리자는 **계정 잠금** 열이 **잠김** 상태로 표시되고, 해제된 관리자는 **해제됨** 상태로 표시됩니다.

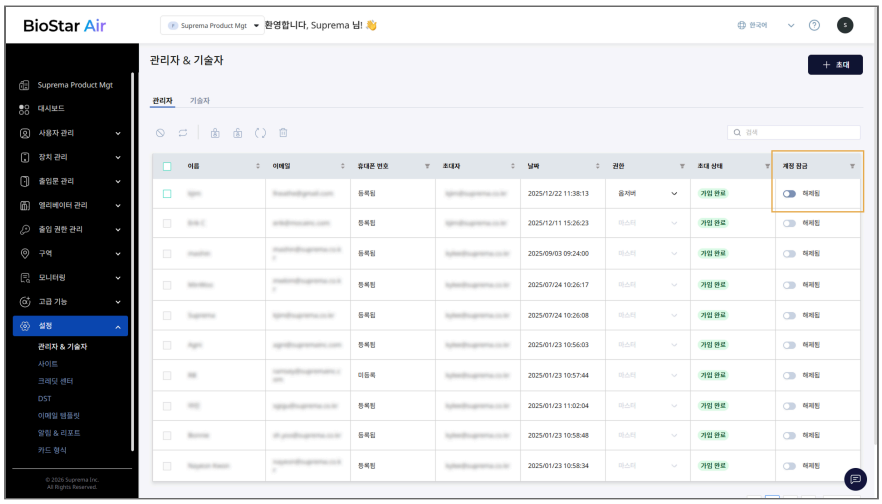


알아두기

- 가입 완료한 관리자 계정만 잠그거나 해제할 수 있습니다.
- 관리자 **계정 잠금** 기능은 관리자의 권한에 따라 제한될 수 있습니다. **마스터** 권한을 가진 관리자는 다른 **마스터** 관리자를 잠김 처리할 수 없습니다.

개별 관리자 잠금/해제

1. 관리자 목록에서 잠그거나 해제할 관리자를 찾으세요.
2. **계정 잠금** 열에서 토글 스위치를 클릭하세요.



3. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

여러 관리자 잠금/해제

1. 관리자 목록에서 잠그거나 해제할 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.
2. 화면 왼쪽 상단의 🔒 또는 🔓 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

관리자 역할 변경

관리자는 자신보다 낮은 레벨의 관리자 역할을 변경할 수 있습니다. 직원의 업무 변경, 책임 범위 확대 또는 축소, 조직 개편 등의 상황에서 역할을 조정합니다. 역할을 축소하면 해당 관리자는 기존에 접근 가능했던 기능에 더 이상 접근할 수 없습니다.

1. 관리자 목록에서 역할을 변경할 관리자를 찾으세요.

2. **권한** 열에서 새 관리자 레벨을 선택하세요.



3. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

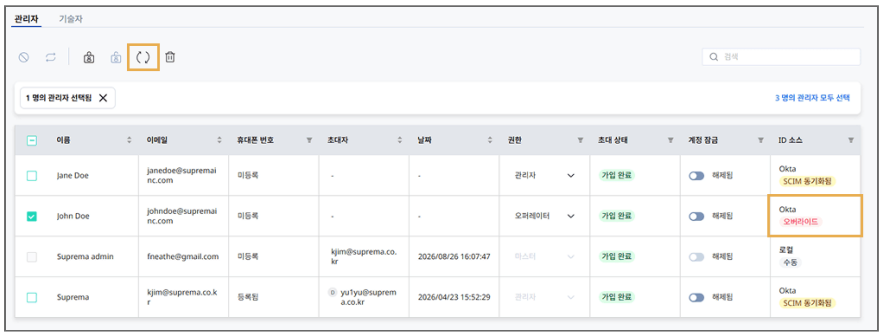
> **마스터** 관리자만이 다른 관리자에게 **마스터** 권한을 할당하거나 수정할 수 있습니다.

오버라이드 상태 해제

SCIM으로 동기화된 관리자의 권한이나 잠금 상태를 로컬에서 수동으로 변경하면 **오버라이드** 상태가 됩니다. 로컬 변경 사항을 취소하고 다시 SCIM 관리 상태로 복구할 수 있습니다.

1. 관리자 목록에서 **오버라이드** 상태인 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.

2. 화면 왼쪽 상단의 ↻ 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

선택한 관리자 계정의 **오버라이드** 상태가 해제되고, **SCIM 동기화됨** 상태로 변경됩니다.

> **알아두기**
> SSO & SCIM 설정에 대한 자세한 내용은 SSO & SCIM 설정하기를 참고하세요.

관리자 계정 삭제

관리자 계정을 삭제하면 해당 관리자는 사이트에 로그인할 수 없으며, 삭제된 계정 정보는 복구할 수 없습니다.

1. 관리자 목록에서 삭제할 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.

2. 화면 왼쪽 상단의 🗑 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

삭제한 관리자 계정은 관리자 목록에서 더 이상 표시되지 않습니다.

기술자 계정 관리하기

기술자는 고객 사이트에 대한 접근 권한을 부여받은 전문가입니다. 기술자 계정을 관리하려면 파트너 포털에서 기술자 계정을 초대하고, 각 사이트에 배정하여 권한 수준을 설정해야 합니다.

BioStar Air 포털에서는 사이트에 초대된 기술자의 접근 권한을 수정하거나 사이트에 대한 접근을 잠그거나 해제할 수 있습니다. 또한, 기술자 계정을 완전히 삭제하여 사이트 접근 권한을 제거할 수도 있습니다.

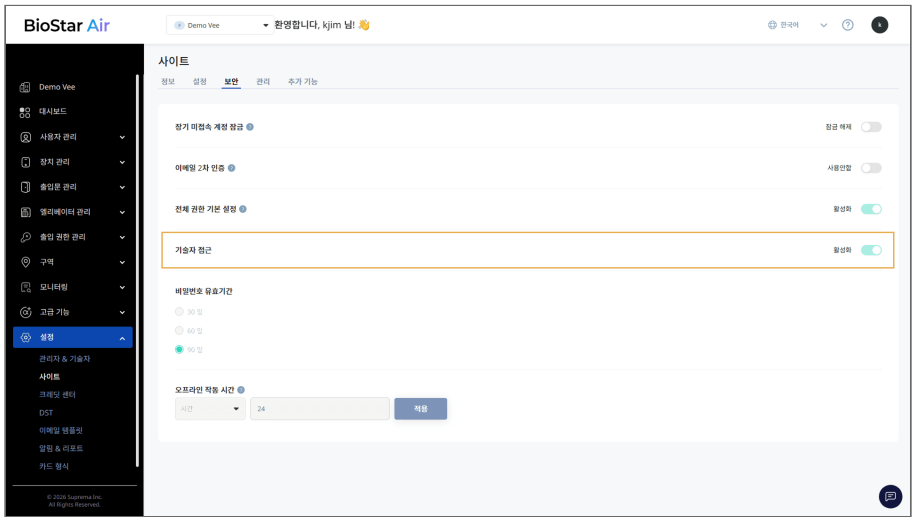
알아두기

- 파트너 포털에서 기술자를 초대하고 사이트에 배정하는 방법에 대한 자세한 내용은 파트너 기술자 관리하기를 참고하세요.
- 기술자로 초대된 사용자의 활동은 **모니터링** → **이벤트 로그**/**변경 로그**에서 개별 계정으로 기록되어 추적할 수 있습니다.

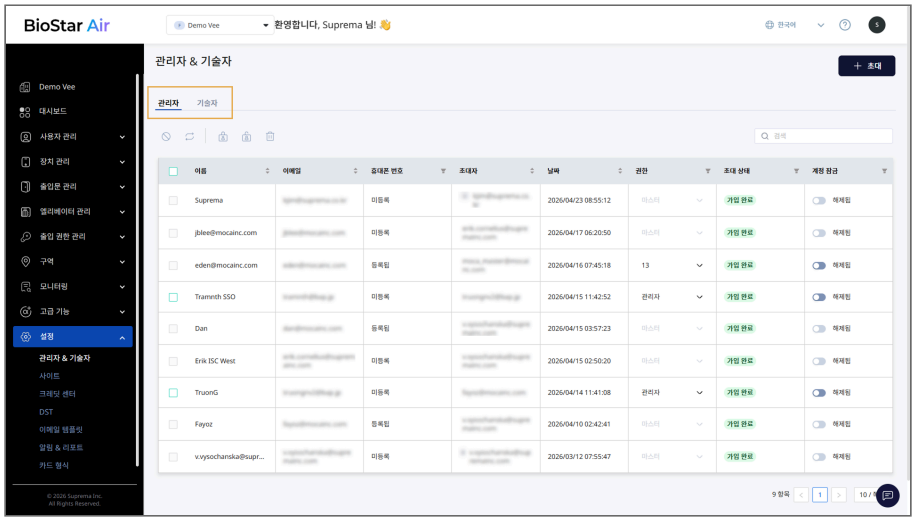
시작하기 전에

기술자 계정을 관리하기 전에, 사이트 보안 설정에서 기술자 계정이 사이트에 접근할 수 있도록 허용되어 있는지 확인하세요. 사이트 보안 설정에서 기술자 계정이 사이트에 접근할 수 있도록 허용되어 있지 않으면, 기술자 계정을 관리할 수 없습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요.
2. **보안** 탭을 클릭하세요.
3. **기술자 접근** 옵션을 활성화하세요.



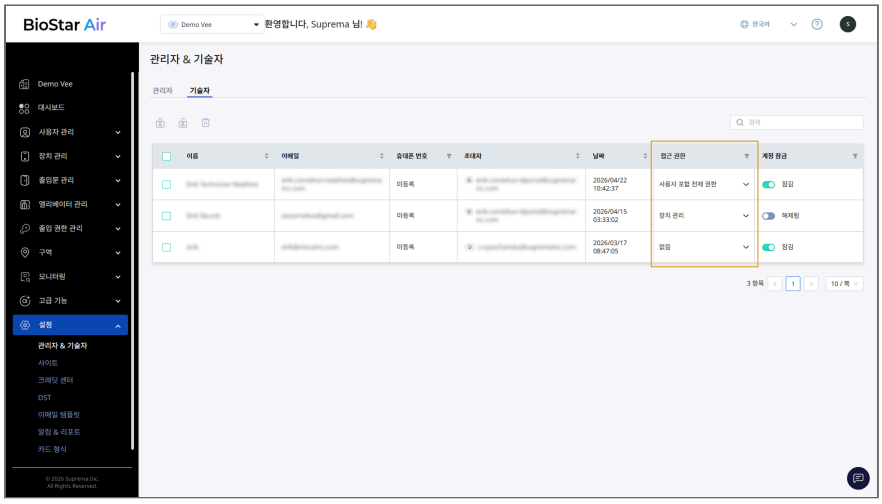
기술자 접근 옵션을 활성화하면 **설정** → **관리자** 메뉴가 **관리자 & 기술자** 메뉴로 변경됩니다. **관리자**와 **기술자** 탭으로 나뉘어져 관리자 계정과 기술자 계정을 각각 관리할 수 있습니다.



기술자 권한 변경

사이트에 초대된 기술자의 접근 권한을 변경하려면 다음 안내를 따르세요.

1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.
2. **기술자** 탭을 클릭하세요.
3. 기술자 목록에서 접근 권한을 변경할 기술자의 **접근 권한** 열을 클릭하세요.



4. 접근 권한 선택 목록에서 원하는 권한 수준을 선택하세요.



- : 사이트에 로그인할 수 없습니다.
- **장치 관리**: **대시보드** 및 **장치 관리** 메뉴에만 접근할 수 있습니다.
- **사용자 제외 전체 권한**: **사용자 관리** 메뉴를 제외한 모든 메뉴에 접근할 수 있지만, 일부 설정 기능에 대한 접근은 제한됩니다.
- **사용자 포함 전체 권한**: **사용자 관리** 메뉴를 포함한 모든 메뉴에 접근할 수 있지만, 일부 설정 기능에 대한 접근은 제한됩니다.

5. 변경 확인을 위한 팝업 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

화면 상단의 성공 메시지와 함께 해당 기술자의 접근 권한이 변경됩니다.

> **알아두기**
> **사용자 제외 전체 권한** 및 **사용자 포함 전체 권한**은 다음 메뉴 경로에 대해 보기 권한은 있지만 수정 권한은 없습니다.
> - **설정** → **관리자 & 기술자**
> - **설정** → **사이트**

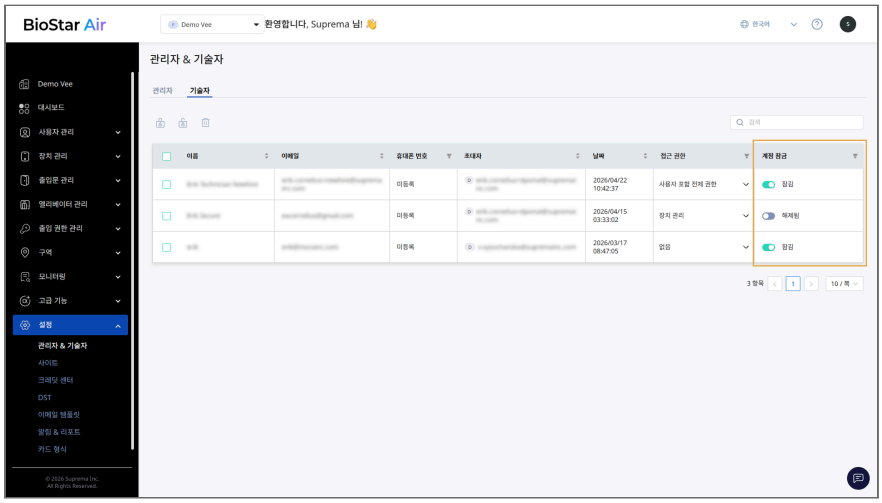
기술자 계정 잠금/해제

기술자의 지원이 더 이상 필요없거나 보안상의 이유로 사이트 접근을 제한해야 한다면, 기술자의 계정을 잠김 처리하여 사이트 접근을 차단할 수 있습니다. 반대로, 기술자의 지원이 다시 필요해진다면, 계정 잠금을 해제하여 사이트 접근을 허용할 수 있습니다.

사이트에 초대된 기술자의 계정을 잠김 처리하면 해당 기술자는 사이트에 로그인할 수 없습니다.

개별 기술자 잠금/해제

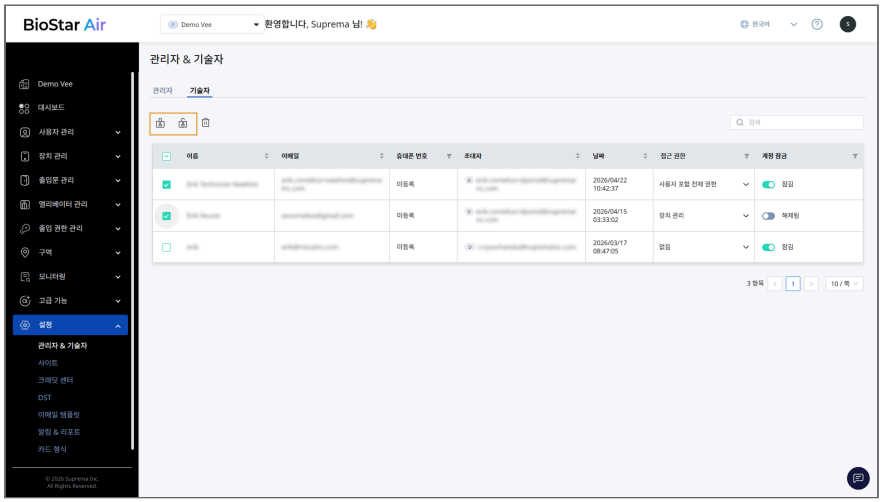
1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.
2. **기술자** 탭을 클릭하세요.
3. 기술자 목록에서 계정을 잠그거나 해제할 기술자의 **계정 잠금** 열의 토글 버튼을 클릭하세요.



4. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

여러 기술자 잠금/해제

1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.
2. **기술자** 탭을 클릭하세요.
3. 기술자 목록에서 계정을 잠그거나 해제할 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
4. 기술자 목록 상단에서 🔒 또는 🔓 버튼을 클릭하세요.



5. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

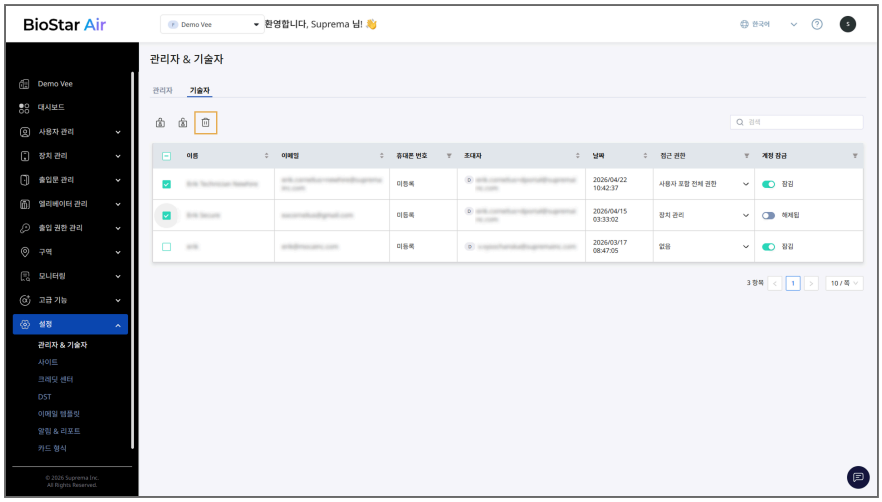
화면 상단의 성공 메시지와 함께 선택한 기술자들의 계정이 잠김 처리되거나 해제됩니다.

> **알아두기**
> 선택한 여러 기술자 중 서로 다른 계정 잠금 상태의 기술자가 있더라도, 일괄 작업을 수행하면 모두 잠김 처리되거나 모두 해제됩니다.

기술자 계정 삭제

사이트에 초대된 기술자의 계정을 삭제하면 해당 기술자의 사이트 접근 권한이 완전히 제거됩니다.

1. 화면 왼쪽 사이드바에서 **설정** → **관리자 & 기술자**를 클릭하세요.
2. **기술자** 탭을 클릭하세요.
3. 기술자 목록에서 계정을 삭제할 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
4. 기술자 목록 상단의 버튼을 클릭하세요.



5. 팝업 메시지 창이 나타나면 내용을 확인하고 **예** 버튼을 클릭하세요.

화면 상단의 성공 메시지와 함께 선택한 기술자들의 계정이 삭제되고, 기술자 목록에서 더 이상 표시되지 않습니다.

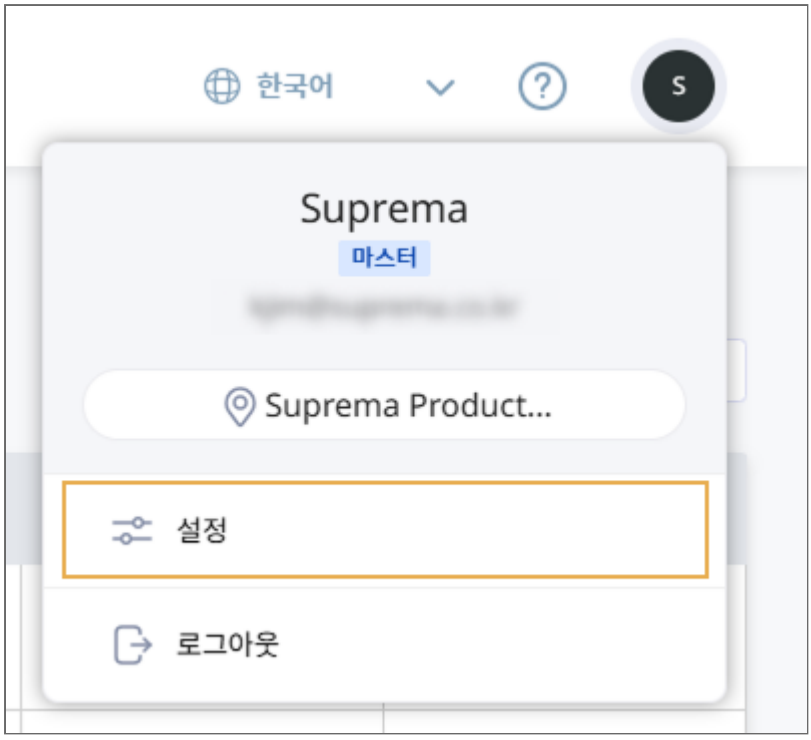
> **알아두기**
> 기술자 계정이 삭제되면 복구할 수 없습니다. 사이트에서 삭제한 기술자는 파트너 포털에서 사이트에 다시 배정할 수 있습니다. 파트너 포털에서 기술자를 사이트에 배정하는 방법은 사이트에 기술자 배정하기를 참고하세요.

개인 계정 설정하기

비밀번호 변경, 알림 수신 방식 조정, IP 인터폰 설정 등 계정과 관련된 개인 설정을 직접 관리할 수 있습니다. 사이트를 탈퇴하거나 계정을 영구적으로 삭제할 수도 있습니다.

계정 설정 접근

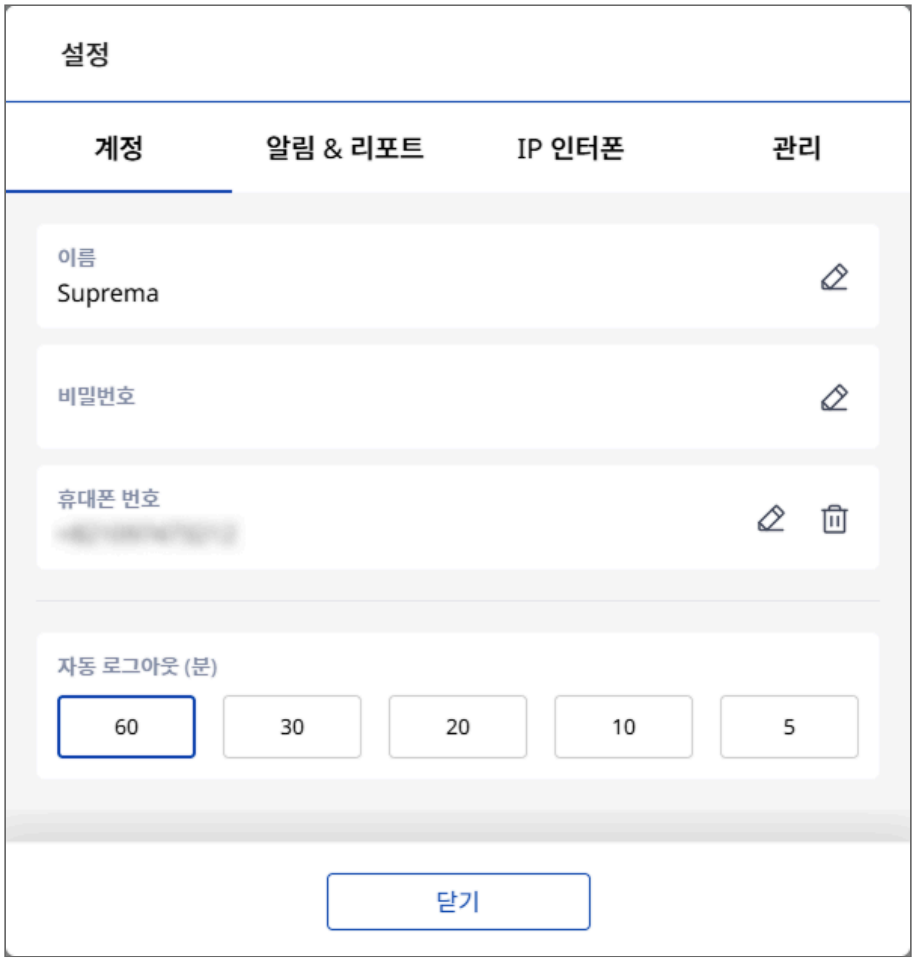
1. BioStar Air 포털에 로그인하세요.
2. 화면 오른쪽 상단의 사용자 프로필 아이콘을 클릭하세요.
3. 드롭다운 메뉴에서 **설정**를 클릭하세요.



4. **설정** 창이 나타나면 원하는 옵션을 설정하세요.
   - **계정**: 사용자 이름, 비밀번호, 전화번호 등을 수정할 수 있습니다. 자세한 내용은 계정 정보 변경을 참고하세요.
   - **알림 & 리포트**: 알림 수신 방식을 설정할 수 있습니다. 자세한 내용은 알림 설정을 참고하세요.
   - **IP 인터폰**: SIP 인터폰 설정 정보를 관리할 수 있습니다. 자세한 내용은 IP 인터폰 설정을 참고하세요.
   - **관리**: 사이트를 탈퇴하거나 계정을 삭제할 수 있습니다. 자세한 내용은 탈퇴 또는 계정 삭제를 참고하세요.

계정 정보 변경

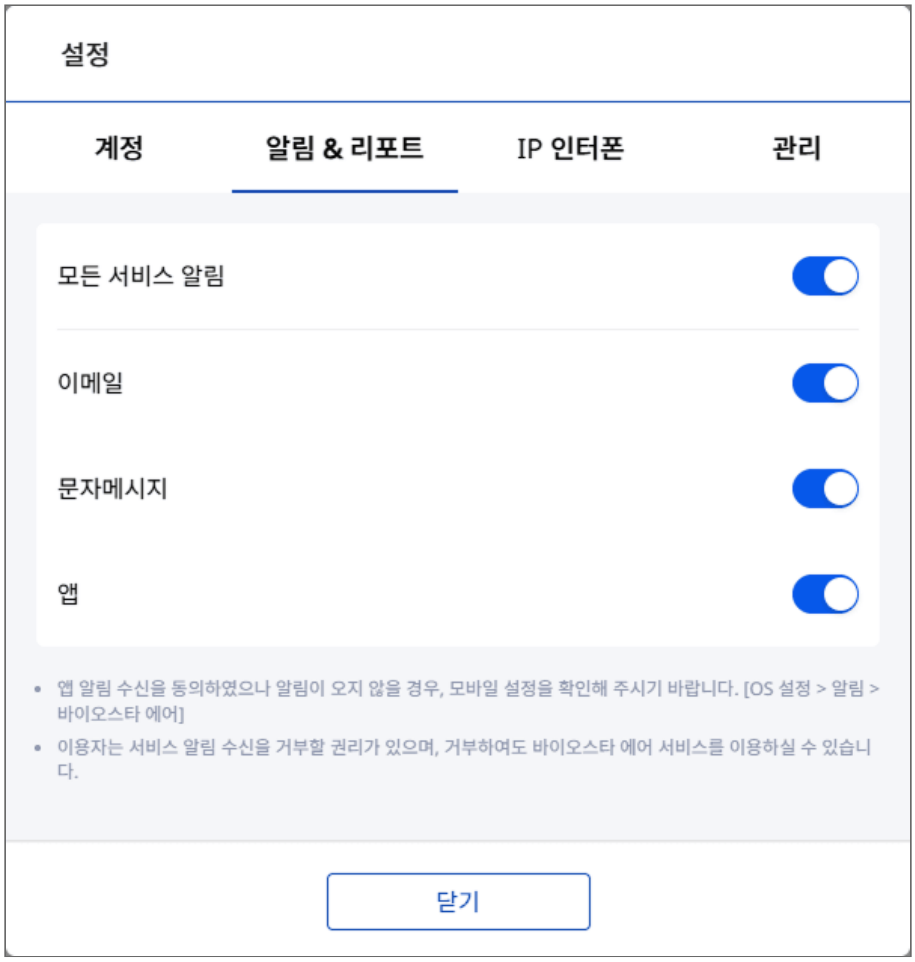
계정 탭에서는 현재 접속한 사용자의 정보를 변경할 수 있습니다.



- 사용자의 이름, 비밀번호, 전화번호를 변경할 수 있습니다. 각 항목의 버튼을 클릭하세요.
- **자동 로그아웃 (분)**: 선택한 시간이 지나면 자동으로 로그아웃됩니다. 원하는 시간을 선택하세요.

알림 설정

알림 & 리포트 탭에서는 알림 수신 방식을 설정할 수 있습니다. 모든 알림을 수신하려면 **모든 서비스 알림** 옵션을 활성화하세요. 원치 않는 알림은 개별적으로 비활성화할 수 있습니다.

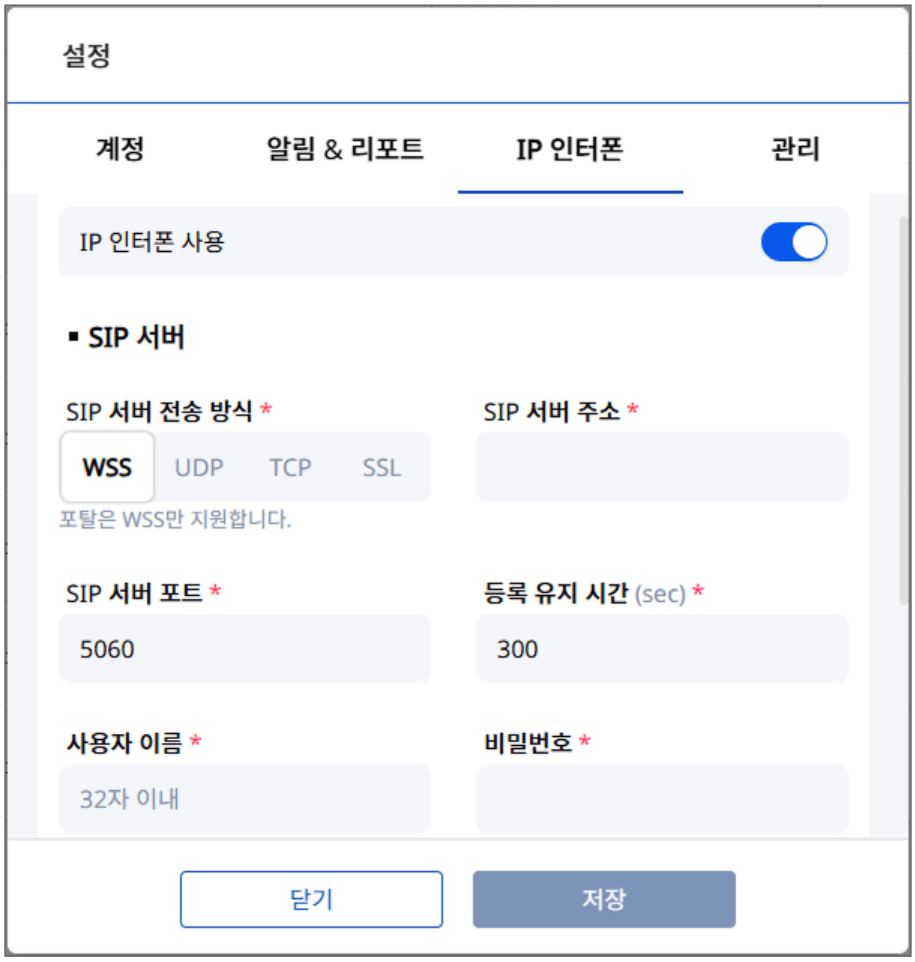


알아두기

- 앱 알림 수신을 동의했으나 알림이 오지 않는다면 모바일 설정을 확인하세요. iOS 또는 안드로이드 기기에서 앱 알림을 허용해야 합니다.
- 사용자는 서비스 알림 수신을 거부할 수 있으며, 거부하여도 서비스 이용에 제한이 없습니다.

IP 인터폰 설정

IP 인터폰 탭에서는 SIP 인터폰 설정 정보를 관리할 수 있습니다.

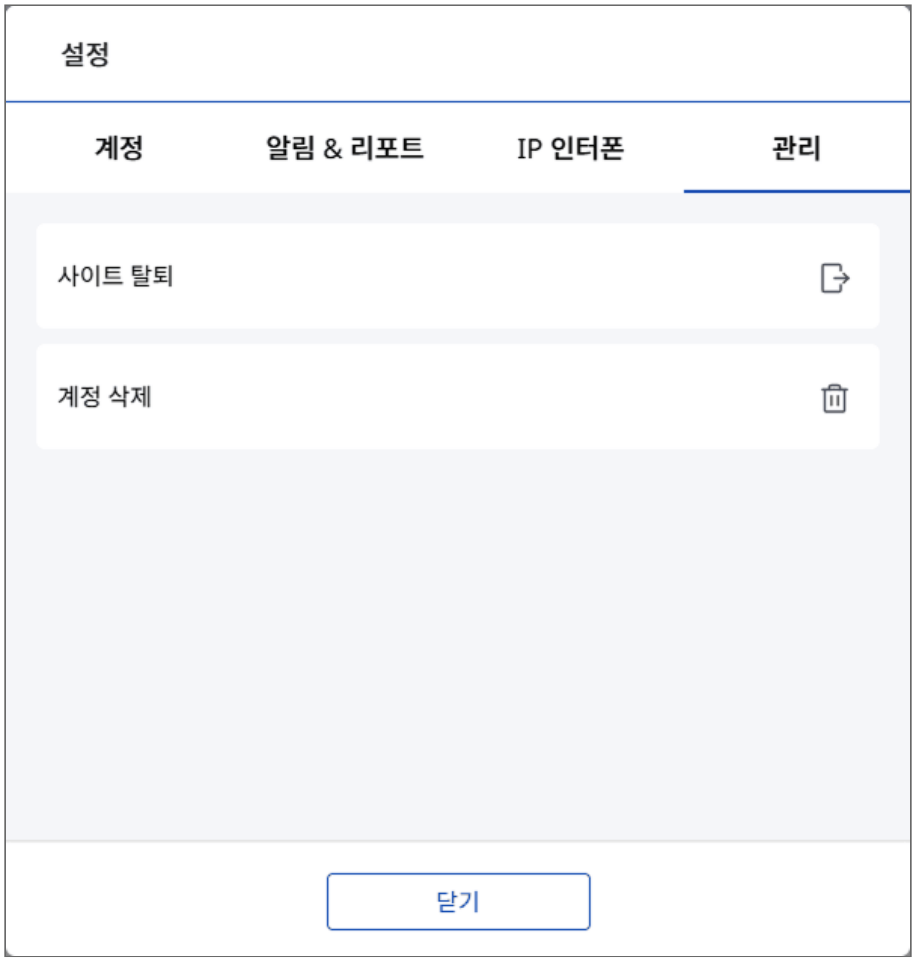


알아두기

SIP 인터폰 설정에 대한 자세한 내용은 BioStation 3 SIP 인터폰 설정하기를 참고하세요.

탈퇴 또는 계정 삭제

관리 탭에서는 사이트를 탈퇴하거나 계정을 삭제할 수 있습니다.



- **사이트 탈퇴**: 사이트를 탈퇴할 수 있습니다. 사이트를 탈퇴한 후 다시 사이트에 가입하려면 해당 사이트 관리자에게 초대를 받아야 합니다.
- **계정 삭제**: 계정을 영구적으로 삭제할 수 있습니다. 계정을 삭제하면 모든 개인 정보와 설정이 영구적으로 삭제되며 복구할 수 없습니다.

SSO & SCIM 설정하기

기업 규모와 관계없이 많은 조직이 이미 Microsoft Entra ID나 Okta로 사내 시스템의 접근 권한을 관리하고 있습니다. BioStar Air는 이러한 기존 ID 공급자와 연동하여 관리자 계정과 크리덴셜 사용자를 하나의 소스에서 통합 관리할 수 있도록 지원합니다.

SSO(Single Sign-On)를 적용하면 조직에서 이미 사용 중인 ID 정책을 BioStar Air 관리자 로그인에도 그대로 적용해 보안을 강화할 수 있습니다. SCIM(System for Cross-domain Identity Management)을 통해 사용자 계정을 자동으로 만들고 삭제하면, 권한이 없어진 사용자의 계정을 미처 정지하지 못해 발생하는 보안 사고를 줄일 수 있습니다. 이를 통해 관리자는 사용자, 사용자 그룹, 관리자 계정을 일일이 생성하고 수정하고 삭제하는 반복 작업의 부담을 줄일 수 있습니다.

화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하면 **SSO & SCIM** 탭에서 로그인 정책과 ID 공급자를 선택하고 설정할 수 있습니다. 기본 설정 방법은 SSO & SCIM 활성화하기를 참고하세요.

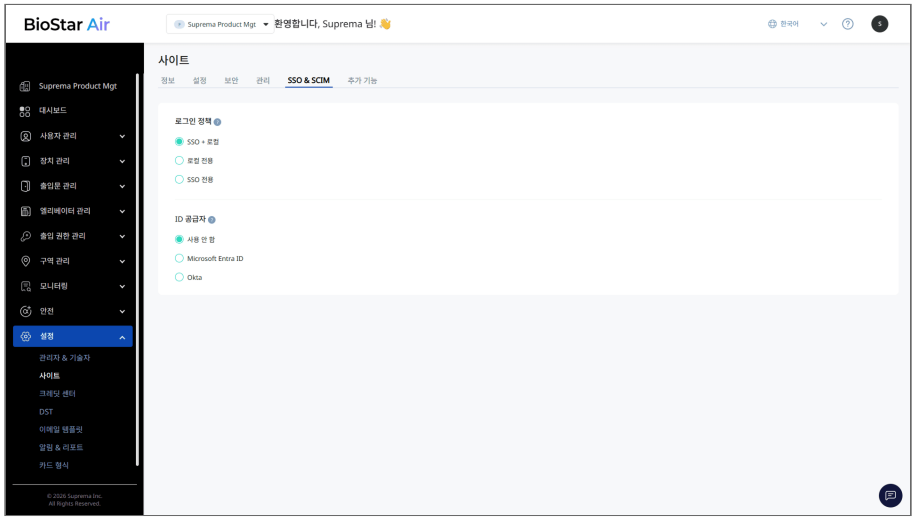
BioStar Air는 **Microsoft Entra ID** 또는 **Okta**를 통한 사이트 관리자 및 크리덴셜 사용자 프로비저닝을 지원합니다. 해당 ID 공급자를 사용한다면, 아래 문서를 참조하여 BioStar Air 사이트의 SSO 및 SCIM을 설정하세요.

최소 요구 사항

- BioStar Air SSO & SCIM 라이선스
- Microsoft Entra ID 또는 Okta 유효 구독
- ID 공급자에서 새 애플리케이션을 생성할 수 있는 권한
- ID 공급자에서 그룹을 생성 및 푸시, 할당할 수 있는 권한
- BioStar Air 마스터 권한

SSO & SCIM 활성화하기

화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요. **SSO & SCIM** 탭에서 로그인 정책과 ID 공급자를 선택해 설정하거나 해제할 수 있습니다.



주의

ID 공급자 설정을 변경하기 전에는 반드시 로컬 로그인이 가능한 마스터 관리자 계정을 최소 한 개 이상 유지하세요. 그렇지 않으면 ID 공급자 연동에 문제가 생겼을 때 사이트에 접근할 수 없는 잠금 상태에 빠질 수 있습니다.

알아두기

- SSO 및 SCIM 설정은 사이트 마스터 관리자만 관리할 수 있습니다.
- 크리덴셜 사용자는 BioStar Air에 로그인하지 않으므로 SSO 및 SCIM 설정의 영향을 받지 않습니다.
- 파트너 포털은 SSO 및 SCIM 설정 적용 범위에 포함되지 않습니다.

로그인 정책

로그인 정책에서는 BioStar Air 관리자의 로그인 방식을 설정할 수 있습니다.

- **SSO**: 관리자가 ID 공급자를 통해 인증합니다.
- **로컬**: 관리자가 BioStar Air에 설정된 이메일 주소와 비밀번호로 인증합니다.

다음 세 가지 옵션 중 하나를 선택하세요.

- **SSO + 로컬**: SSO 로그인과 로컬 로그인을 모두 사용할 수 있습니다.
- **로컬 전용**: 로컬 로그인만 사용할 수 있습니다.
- **SSO 전용**: SSO 로그인만 사용할 수 있습니다.

ID 공급자 연동 설정

ID 공급자에서는 BioStar Air 관리자 계정을 연동할 외부 ID 공급자를 선택할 수 있습니다. 사이트에는 한 번에 하나의 ID 공급자만 활성화할 수 있습니다.

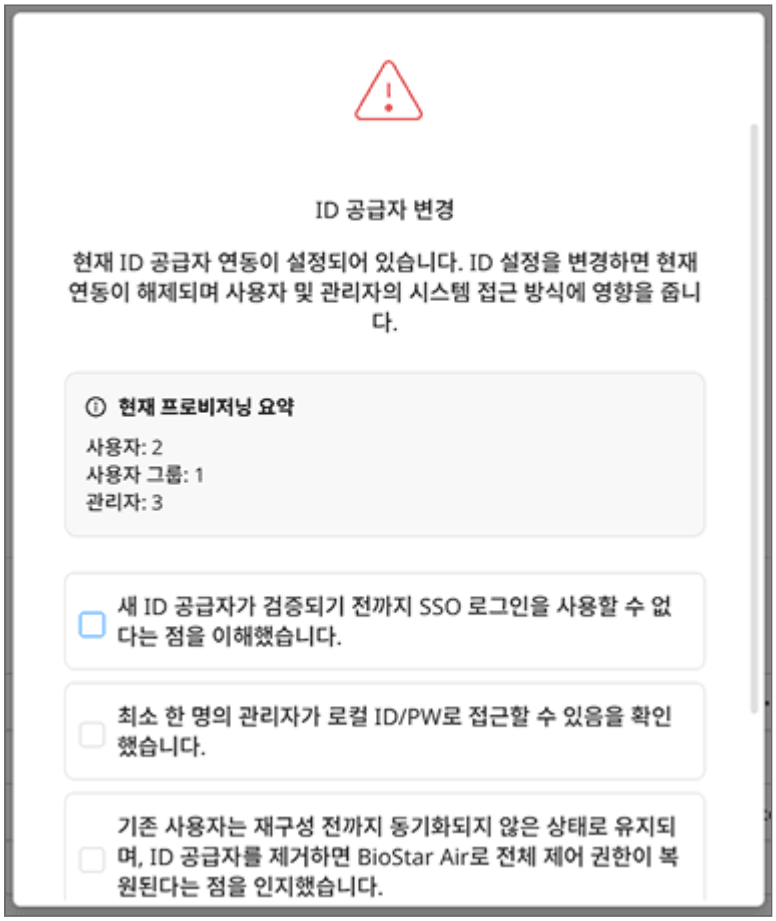
- **사용 안 함**
- **Microsoft Entra ID**: Microsoft Entra ID 연동 설정하기
- **Okta**: Okta 연동 설정하기

> **알아두기**
> 이미 연결된 ID 공급자를 다른 공급자로 변경할 때는 먼저 **사용 안 함**으로 설정해 기존 연결을 해제한 후 새 ID 공급자를 선택하세요. 연결을 해제하지 않으면 다른 ID 공급자로 바로 전환할 수 없습니다.

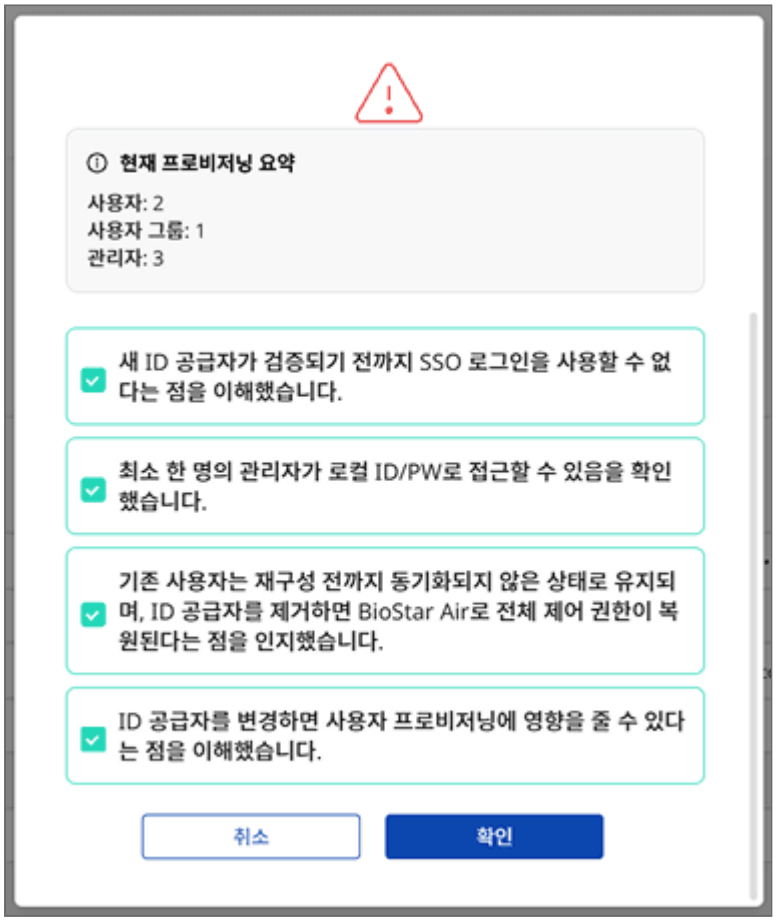
SSO & SCIM 설정 해제

ID 공급자 연동 설정을 해제할 수 있습니다.

1. **ID 공급자** 섹션에서 **사용 안 함**을 선택하세요.
2. 경고 팝업창의 메시지를 확인하세요.



3. 설정 변경으로 인한 영향 범위를 확인하고 체크박스를 클릭하세요.



4. **확인** 버튼을 클릭하세요.

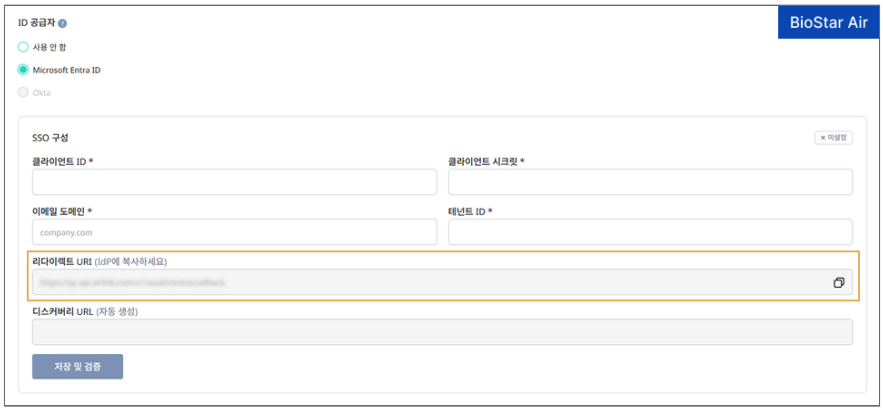
Microsoft Entra ID 연동 설정하기

BioStar Air에 Microsoft Entra ID로 로그인하려면, 조직의 ID 관리자가 Entra ID에 앱을 등록하고 BioStar Air의 SSO 설정과 연결해야 합니다.

Entra ID SSO 연결

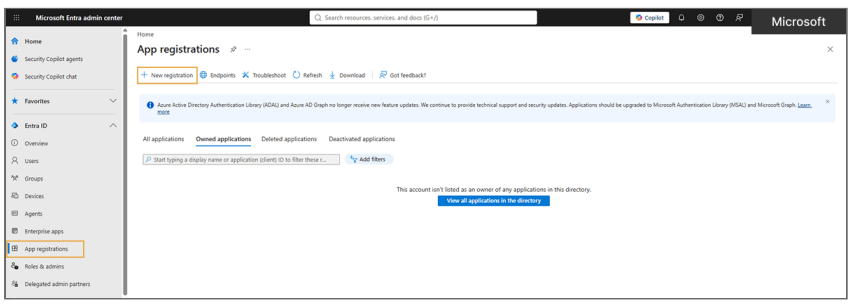
1 BioStar Air: 리다이렉트 URI 준비

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **ID 공급자**에서 **Microsoft Entra ID**를 선택하세요.
4. **리다이렉트 URI** 항목에 표시되는 URI 값을 복사하세요.



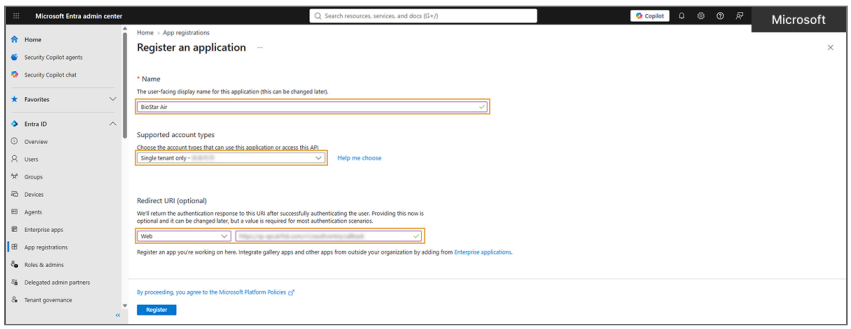
2 Microsoft Entra 관리 센터: 앱 등록

1. Microsoft Entra 관리 센터로 로그인하세요.
2. **Entra ID** → **App registrations**으로 이동하세요.
3. **New registration** 버튼을 클릭하세요.



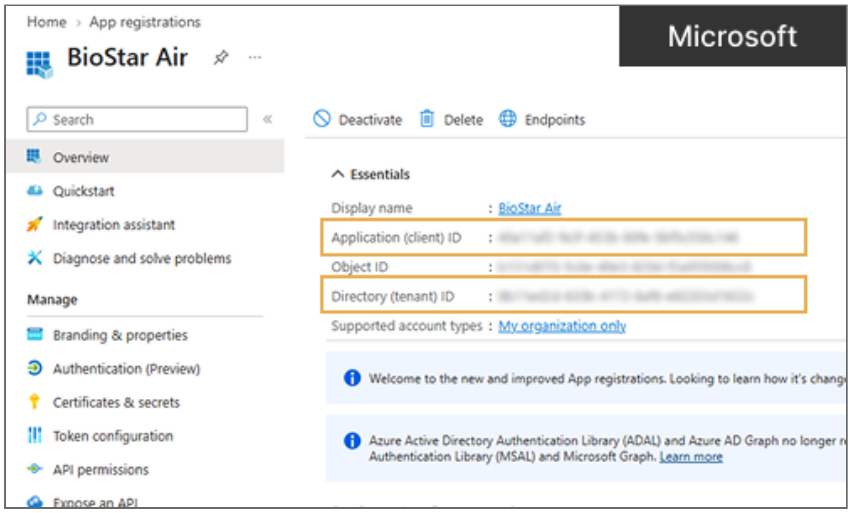
4. 앱 이름을 'BioStar Air'로 입력하세요.
5. **Supported account types**에서 **Single tenant only**를 선택하세요.

6. **Redirect URI** 섹션에서 **Web**을 선택하고, BioStar Air: 리다이렉트 URI 준비 단계에서 복사한 URI 값을 입력 필드에 붙여넣으세요.



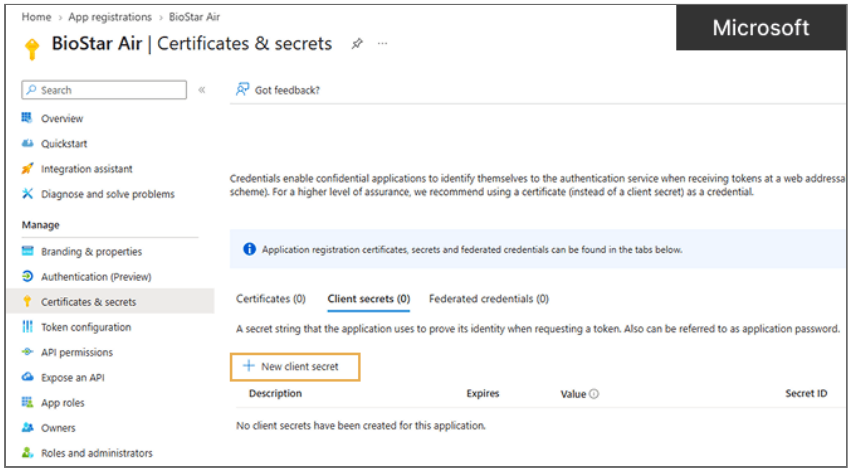
7. **Register** 버튼을 클릭하세요.

8. 등록한 BioStar Air 앱의 **Overview**에서 다음 값을 복사하세요.

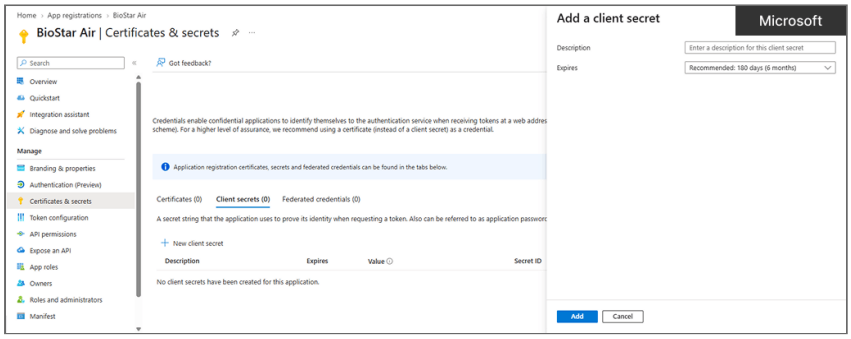


- **Application (client) ID**
- **Directory (tenant) ID**

9. **Certificates & secrets** → **Client secrets**에서 **New client secret**을 클릭하세요.

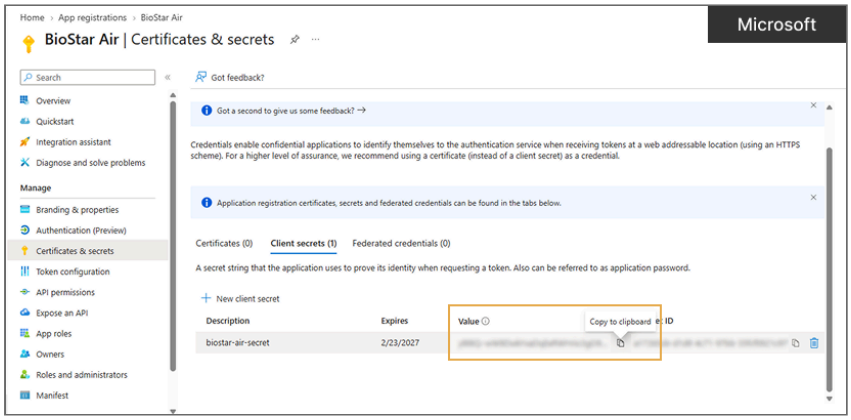


10. 설명을 입력하고 만료 기간을 선택하세요.



11. **Add** 버튼을 클릭하세요.

12. 생성된 클라이언트 시크릿의 **Value**를 복사하세요.



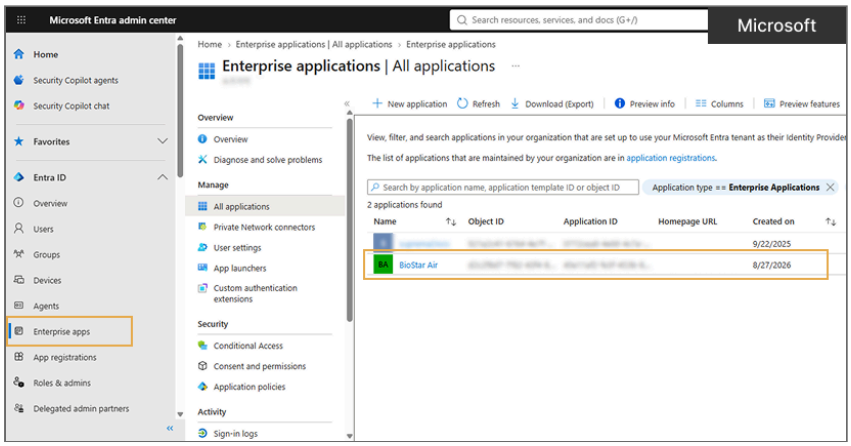
복사한 **Application (client) ID**와 **Directory (tenant) ID**, **Value** 값을 다음 단계에서 입력합니다.

> **주의**
> **Secret ID**가 아니라 **Value**를 사용해야 합니다. **Value**는 이 시점 이후에는 다시 표시되지 않으므로 반드시 복사해 두세요.

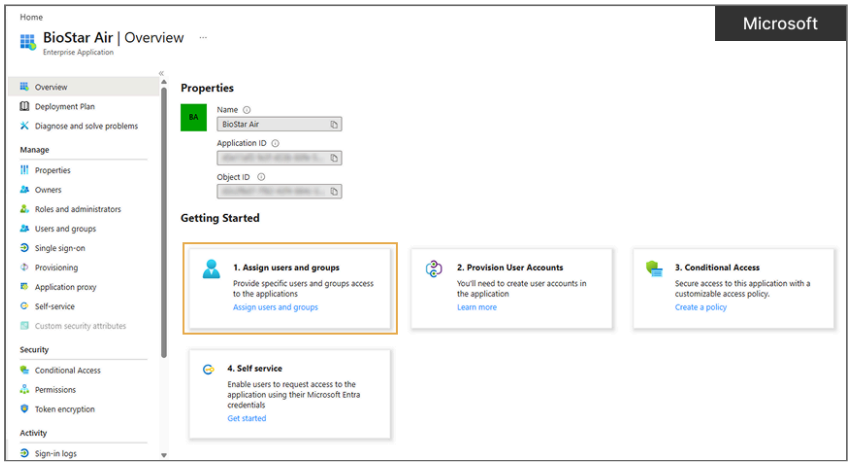
3 Microsoft Entra 관리 센터: 사용자 및 그룹 할당

사용자 및 그룹을 할당하기 전에 사용자와 그룹을 먼저 생성해야 합니다.

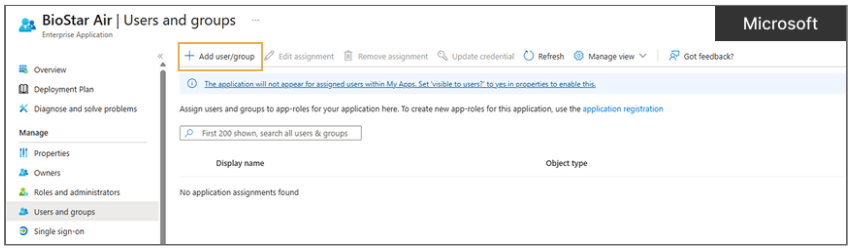
1. **Enterprise apps**에서 앞서 생성한 앱(BioStar Air)을 클릭하세요.



2. **Assign users and groups**를 클릭하세요.



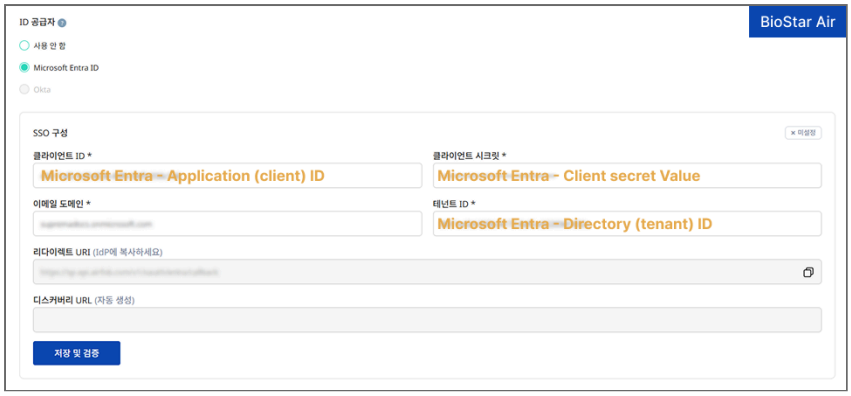
3. 사용자 및 그룹을 할당하려면 **Add user/group**을 클릭하세요.



4. 사용자 및 그룹 할당을 완료하면 **Assign** 버튼을 클릭하세요.

4 BioStar Air: SSO 구성

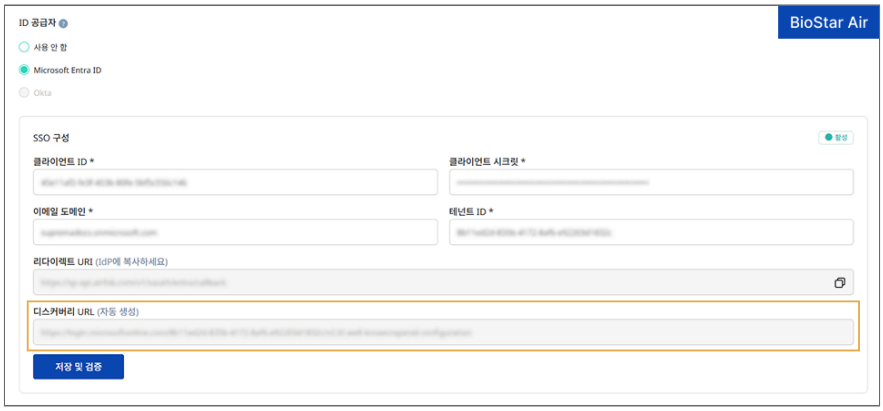
1. BioStar Air 설정 화면으로 돌아와 Microsoft Entra 관리 센터: 앱 등록 단계에서 복사한 값을 각 필드에 입력하세요.



- **클라이언트 ID**: Application (client) ID
- **클라이언트 시크릿**: Value
- **테넌트 ID**: Directory (tenant) ID

2. **이메일 도메인** 필드에 조직의 이메일 도메인을 입력하세요.
3. **저장 및 검증** 버튼을 클릭하세요.

저장 및 검증에 성공하면 **디스커버리 URL** 항목의 값이 자동 생성됩니다.



Entra ID SCIM 프로비저닝 연결

1 BioStar Air: SCIM 토큰 복사

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **SCIM 프로비저닝** 섹션에서 **SCIM 엔드포인트 URL** 값을 복사하세요.

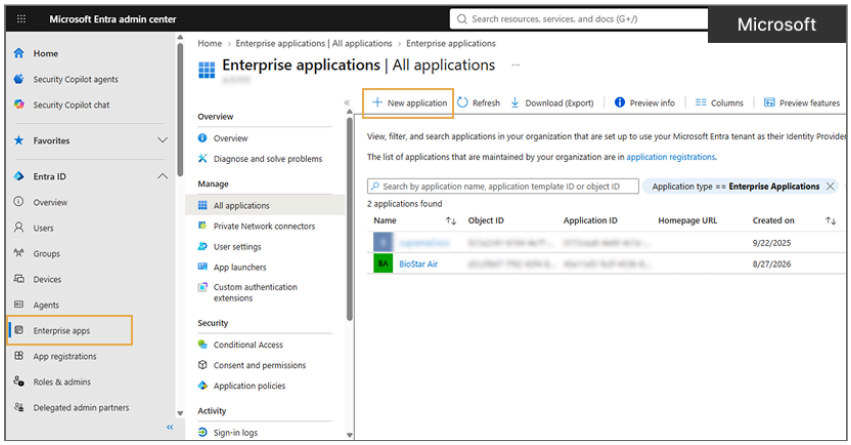


4. **토큰 생성** 버튼을 클릭하세요.
5. 토큰 생성 완료 대화 상자에서 토큰을 복사하세요.

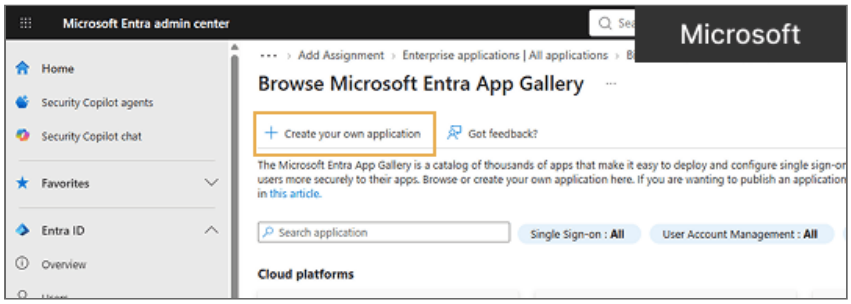
> **알아두기**
>
> - 생성된 토큰을 즉시 복사하세요. 토큰을 생성한 시점에만 복사할 수 있습니다. 대화 상자를 닫으면 토큰을 다시 복사할 수 없습니다.
> - 토큰을 분실했다면 새 토큰을 생성을 위해 **토큰 갱신** 버튼을 클릭하세요. 새 토큰을 ID 공급자에 다시 입력해야 합니다.
> - 이 단계에서 복사한 SCIM 엔드포인트 URL, 토큰을 다음 단계에서 입력해야 합니다.

2 Microsoft Entra 관리 센터: SCIM 프로비저닝 앱 생성

1. **Enterprise apps**에서 **New application**을 클릭하세요.

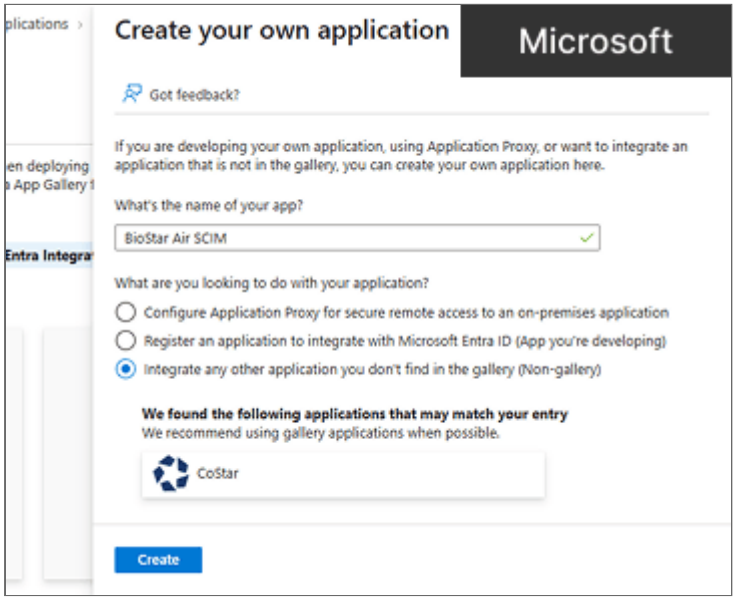


2. **Create your own application**을 클릭하세요.



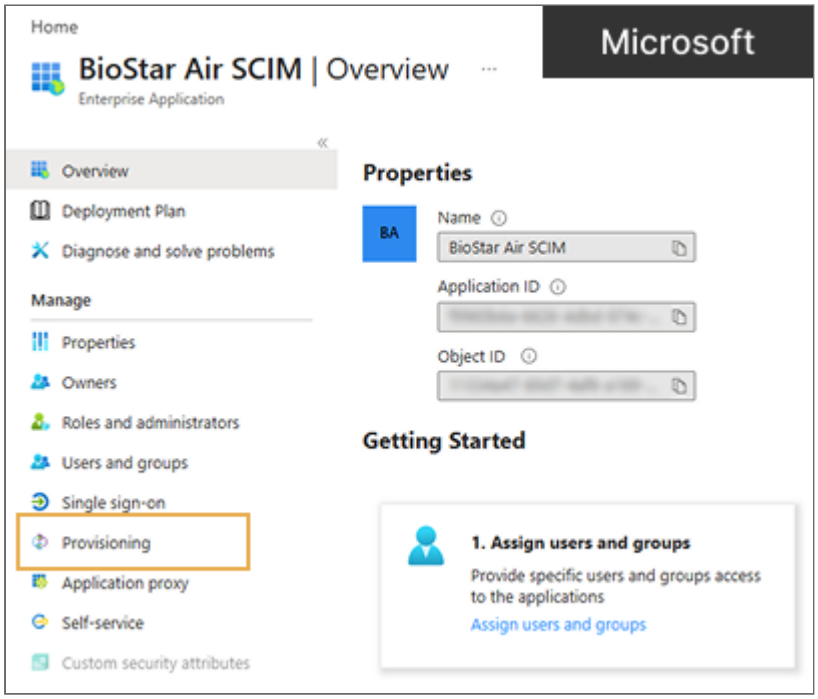
3. 앱 이름을 'BioStar Air SCIM'으로 입력하세요.

4. **Integrate any other application you don't find in the gallery (Non-gallery)** 옵션을 선택하세요.



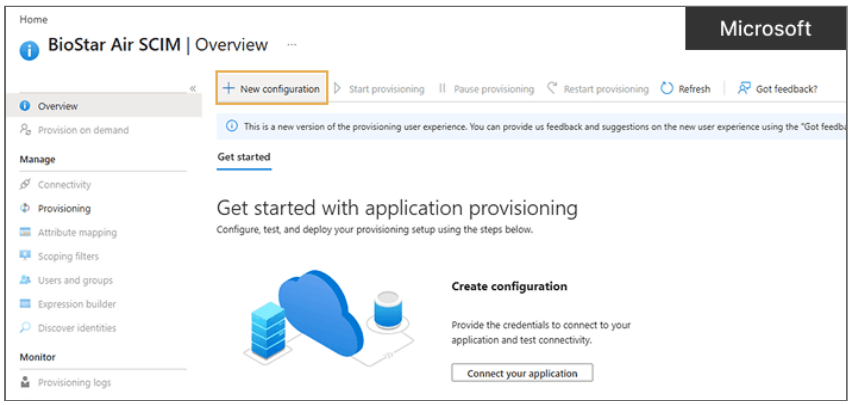
5. **Create** 버튼을 클릭하세요.

6. 생성한 BioStar Air SCIM 앱에서 **Manage** → **Provisioning**을 클릭하세요.

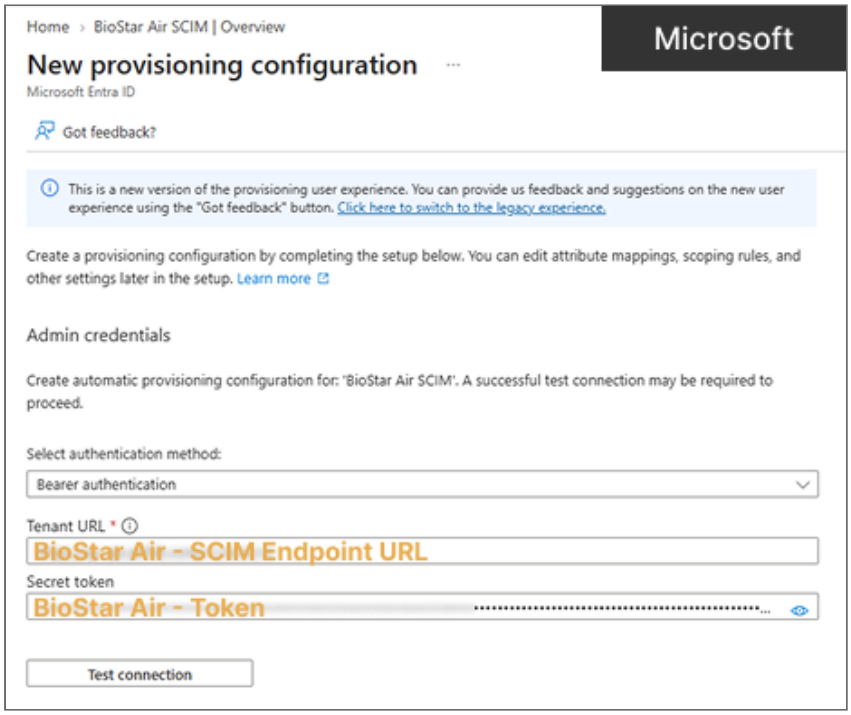


❸ Microsoft Entra 관리 센터: Admin Credentials 설정 및 프로비저닝 시작

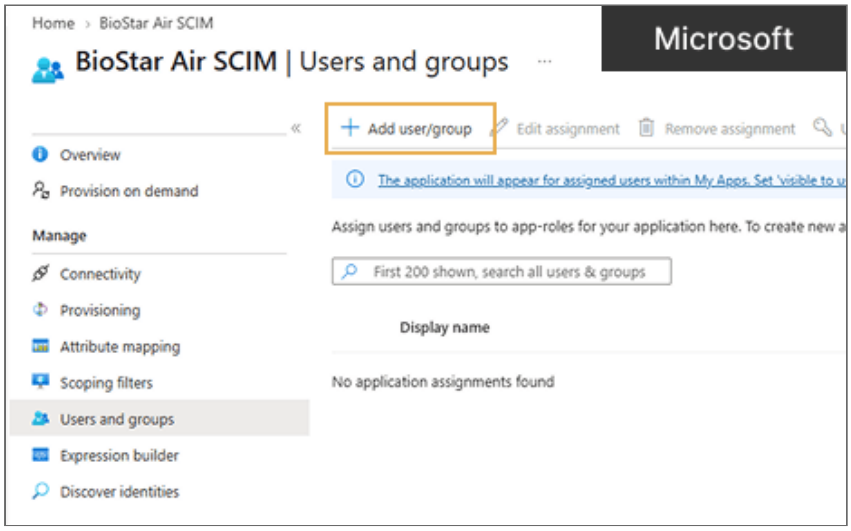
1. **New Configuration**을 클릭하세요.



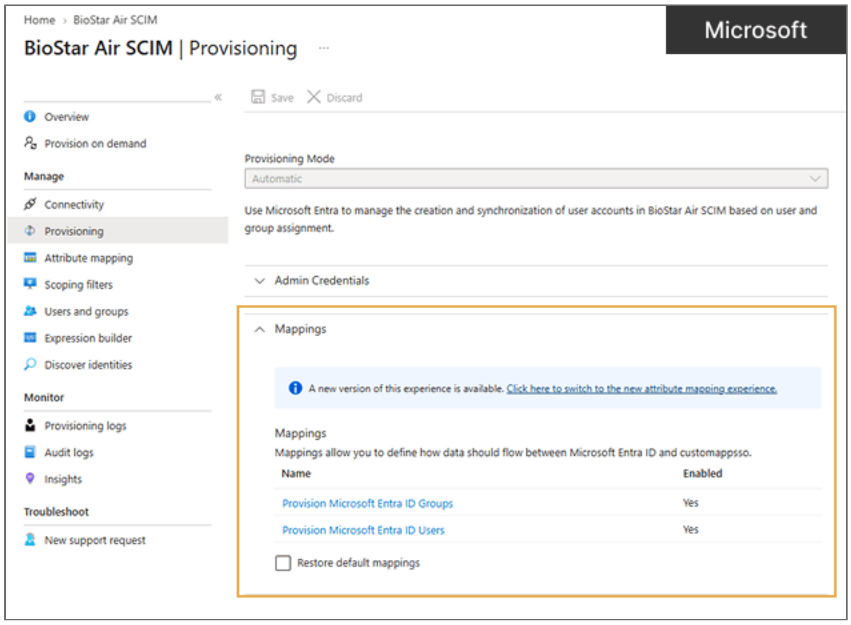
2. BioStar Air: SCIM 토큰 복사 단계에서 복사한 SCIM 엔드포인트 URL, 토큰 값을 **Admin credentials**의 **Tenant URL**, **Secret token** 필드에 입력하세요.



3. 동기화가 정상 동작하는지 테스트하려면 **Test Connection** 버튼을 클릭하세요.
4. **Create** 버튼을 클릭하세요.
5. **Users and groups**에서 **Add user/group**을 클릭하세요.

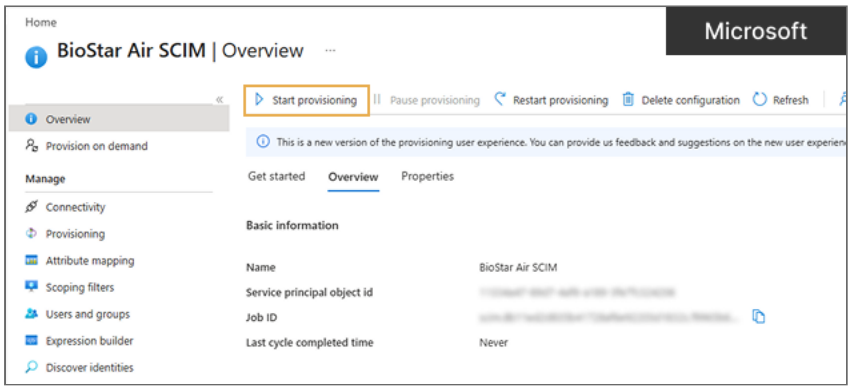


6. 프로비저닝할 사용자와 보안 그룹을 할당하세요.
7. **Assign** 버튼을 클릭하세요.
8. **Provisioning** → **Mappings**로 이동해 사용자와 그룹 동기화가 모두 활성화되어 있는지 확인하세요.



9. 속성 매핑을 변경하기 전에 먼저 매핑 내용을 검토하세요.

10. SCIM 앱 **Overview**에서 **Start provisioning**을 클릭하세요.



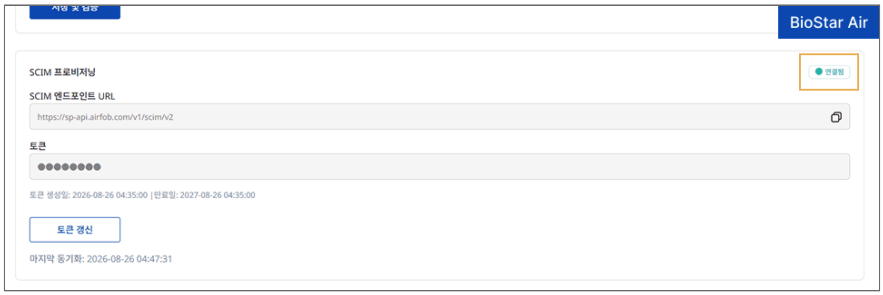
> **알아두기**
> 소규모 테스트 그룹으로 먼저 시작하는 것을 권장합니다. 그룹 멤버십 변경 사항이 BioStar Air에 반영되기까지 최대 약 40분이 걸릴 수 있습니다.

4 BioStar Air: 연결 확인

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.

2. **SSO & SCIM** 탭을 클릭하세요.

3. **SCIM 프로비저닝** 섹션에서 **연결됨** 표시를 확인하세요.



그룹 매핑

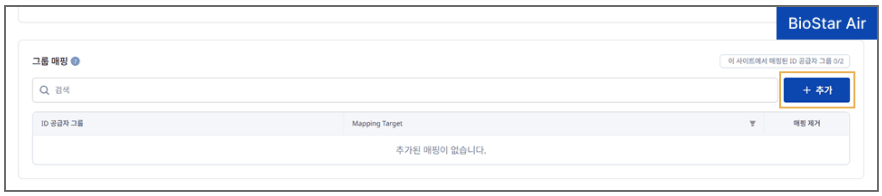
SSO와 SCIM 연결을 완료하고 ID 공급자 그룹을 BioStar Air로 푸시했다면, 사이트 관리자는 푸시된 그룹을 BioStar Air 그룹에 매핑해야 합니다.

매핑 규칙

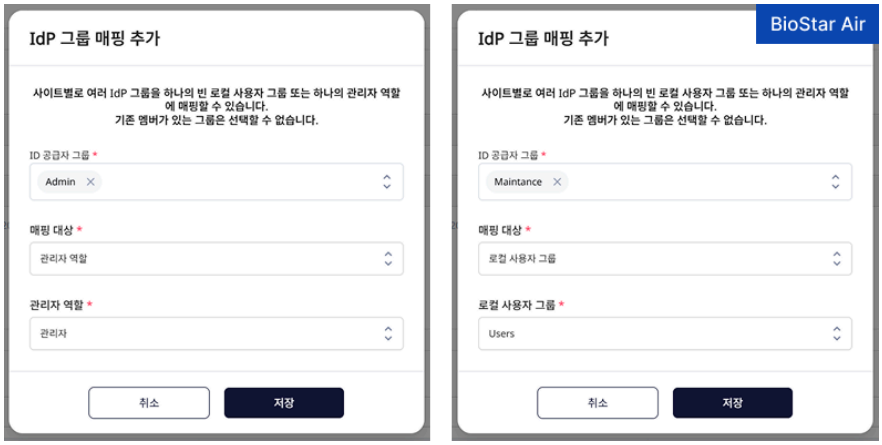
- 하나의 BioStar Air 사용자 그룹에 둘 이상의 ID 공급자 그룹을 매핑할 수 있습니다.
- BioStar Air 사용자 그룹은 매핑하기 전에 비어 있어야 합니다.
- 이미 구성원이 있는 BioStar Air 그룹은 매핑 대상으로 선택할 수 없습니다.
- ID 공급자 그룹 매핑은 사이트 마스터 관리자만 관리할 수 있습니다.
- ID 공급자 그룹을 마스터 역할에 매핑하면 이후에는 역할을 변경할 수 없습니다.

관리자/사용자 그룹 매핑하기

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **그룹 매핑** 섹션으로 이동해 **추가** 버튼을 클릭하세요.



4. **ID 공급자 그룹**에서 ID 공급자 그룹을 선택하세요.
5. **매핑 대상**에서 선택한 IdP 그룹에 따라 **관리자 역할** 또는 **로컬 사용자 그룹**을 선택하세요.
6. 매핑 대상에 따라 관리자 역할을 지정하거나 사용자 그룹을 선택할 수 있습니다.



7. 매핑을 저장하려면 **저장** 버튼을 클릭하세요.

그룹 매핑 섹션에서 ID 공급자 그룹과 매핑된 BioStar Air 그룹을 확인할 수 있습니다.

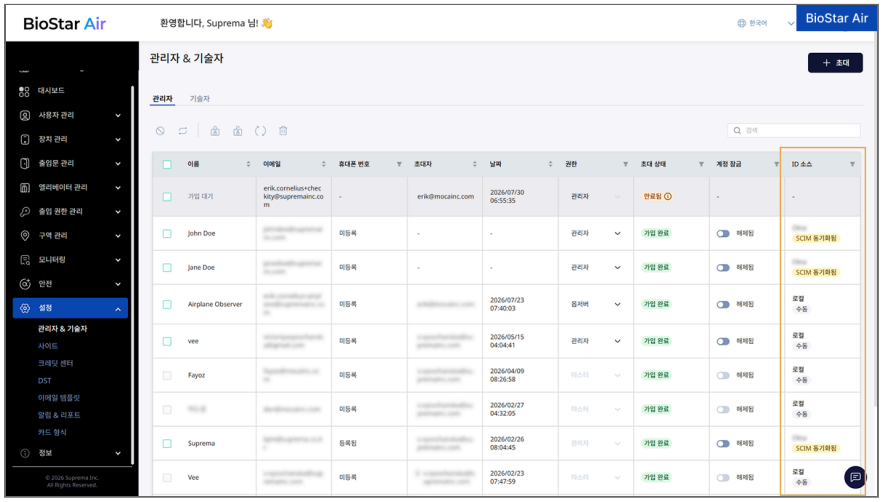


> **알아두기**
>
> - 관리자 역할에 대한 자세한 내용은 관리자 계정 및 역할 관리하기를 참고하세요.
> - 사용자 그룹에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

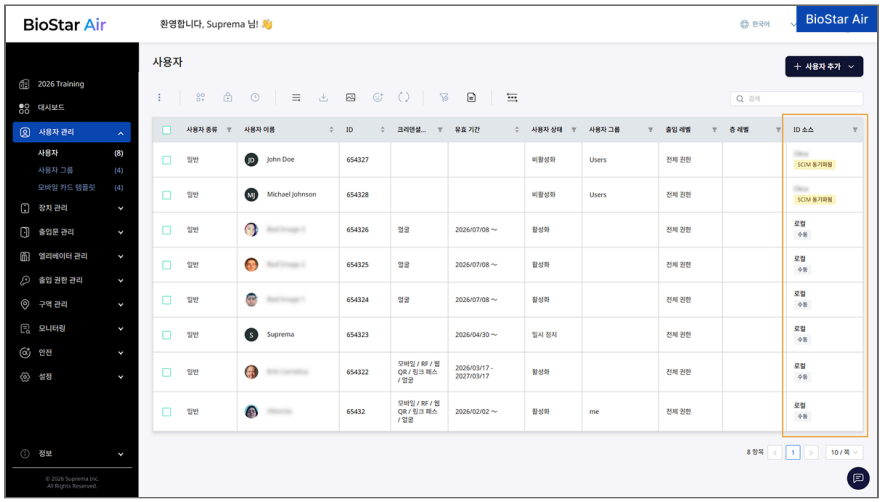
동기화된 관리자/사용자/그룹 관리

프로비저닝이 활성화되면 BioStar Air는 각 관리자, 사용자, 사용자 그룹이 로컬에서 직접 관리되는지, ID 공급자에서 동기화된 것인지 화면에 표시합니다.

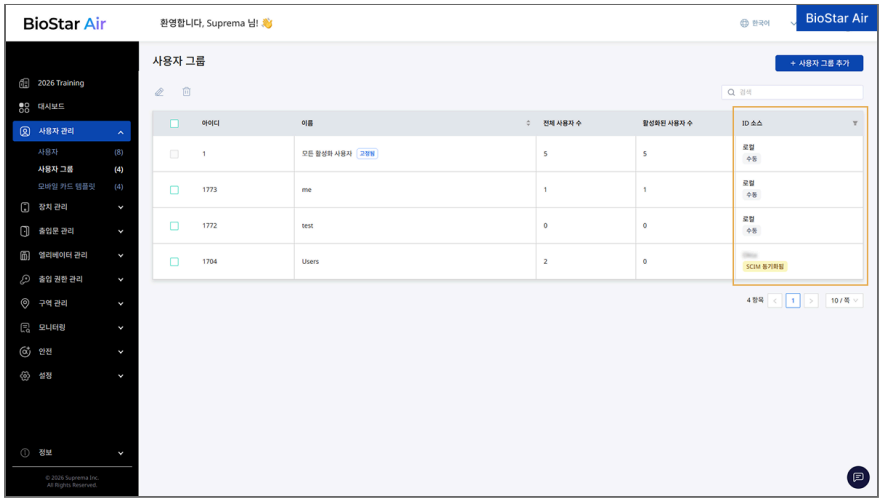
- **설정** → **관리자 & 기술자** 메뉴의 관리자 목록에서 **ID 소스** 열을 확인하세요.



- **사용자 관리** → **사용자** 메뉴의 사용자 목록에서 **ID 소스** 열을 확인하세요.

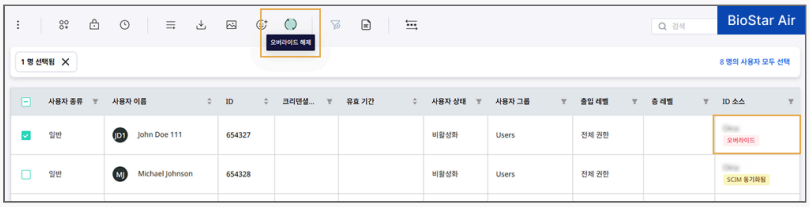


- **사용자 관리** → **사용자 그룹** 메뉴의 사용자 그룹 목록에서 **ID 소스** 열을 확인하세요.



SCIM 동기화 항목의 동작 방식

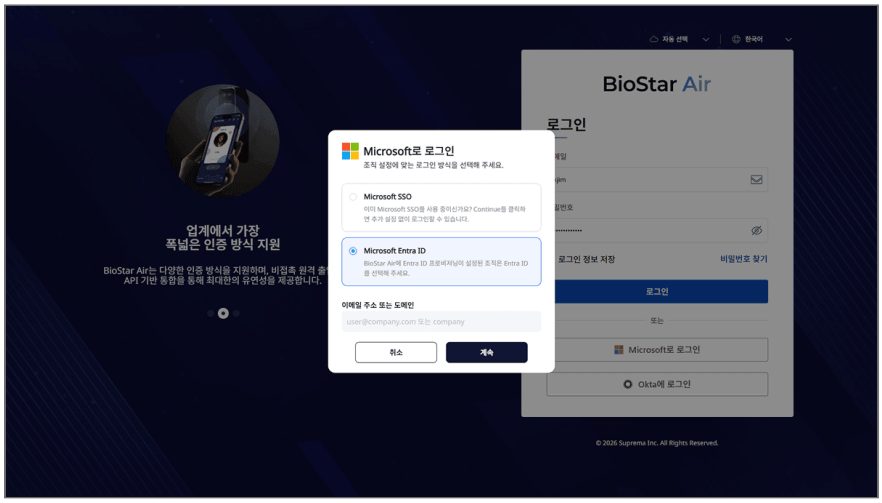
- 기존에 수동으로 생성한 사용자와 관리자는 계속 수동 관리 상태로 유지됩니다.
- SCIM으로 동기화된 항목은 BioStar Air에서 수동으로 삭제할 수 없습니다.
- SCIM으로 동기화된 그룹은 사용자를 수동으로 추가하거나 제거할 수 없습니다.
- 동기화된 항목을 로컬에서 수동으로 변경하면 **오버라이드** 상태가 됩니다. **오버라이드 해제**를 실행하면 로컬 변경 사항이 취소되고 항목이 다시 SCIM 관리 상태로 돌아갑니다.



Entra ID로 로그인

Entra ID SSO 연결을 완료하면 사용자는 BioStar Air 로그인 화면에서 Microsoft 계정으로 로그인할 수 있습니다.

1. BioStar Air 로그인 화면에서 **Microsoft로 로그인** 버튼을 클릭하세요.
2. **Microsoft Entra ID**를 선택하세요.



> 이미 Microsoft SSO를 사용 중인 조직은 **Microsoft SSO**를 선택하면 추가 설정 없이 로그인할 수 있습니다.

3. **이메일 주소 또는 도메인** 필드에 조직의 이메일 주소 또는 도메인을 입력하세요. (예: `user@company.com` 또는 `company`)
4. **계속** 버튼을 클릭하세요.
5. Microsoft Entra ID 로그인 화면으로 이동하면 조직 계정의 이메일 주소와 비밀번호를 입력하세요.
6. 인증을 완료하면 BioStar Air로 자동 리디렉션되어 로그인이 완료됩니다.

> **알아두기**
> 입력한 이메일 도메인에 대해 Entra ID SSO가 설정되어 있지 않으면 오류 메시지가 표시됩니다. 이때는 사이트 관리자에게 문의하세요.

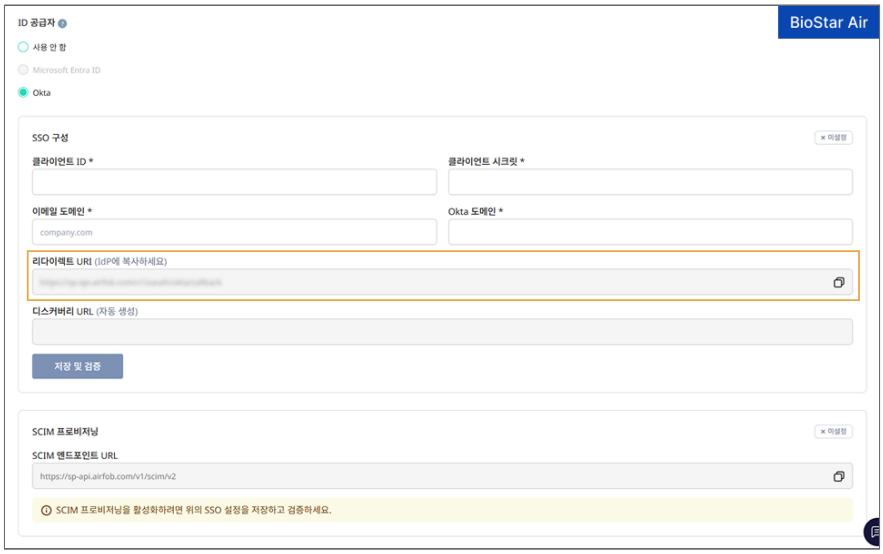
Okta 연동 설정하기

BioStar Air에 Okta로 로그인하려면, 조직의 ID 관리자가 Okta에 OIDC 애플리케이션을 생성하고 BioStar Air의 SSO 설정과 연결해야 합니다.

Okta SSO 연결

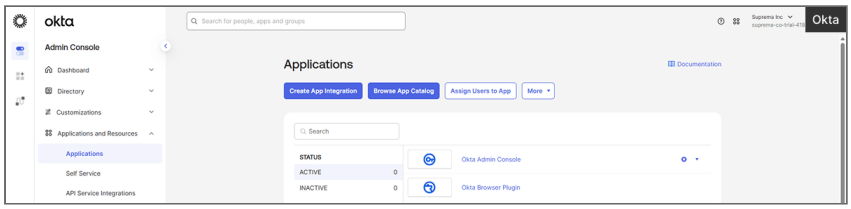
1 BioStar Air: 리다이렉트 URI 준비

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **ID 공급자**에서 **Okta**를 선택하세요.
4. **리다이렉트 URI** 항목에 표시되는 URI 값을 복사하세요.

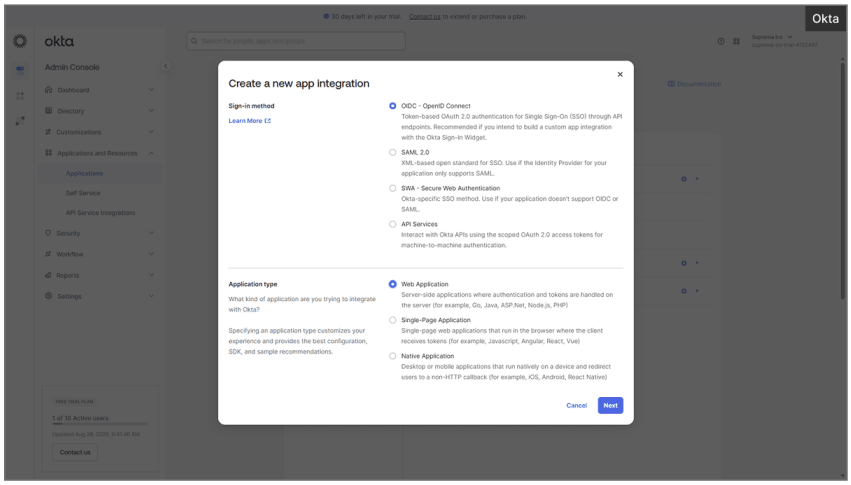


2 Okta: 앱 생성

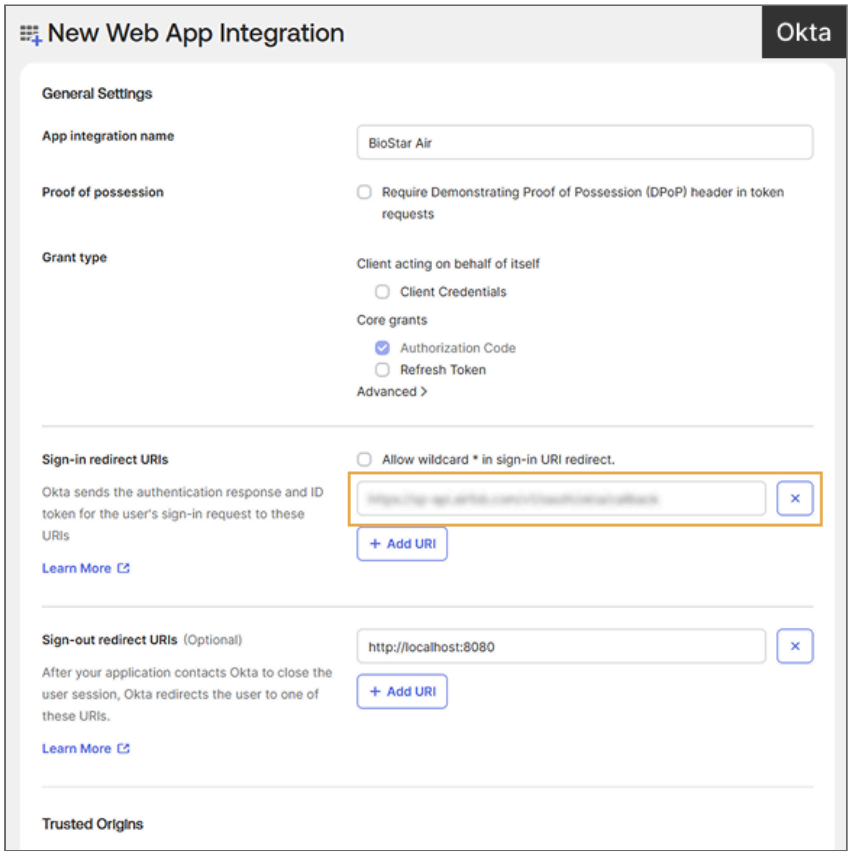
1. **Okta 관리자 콘솔**에 로그인하세요.
2. **Applications and Resources** → **Applications** 메뉴로 이동하세요.



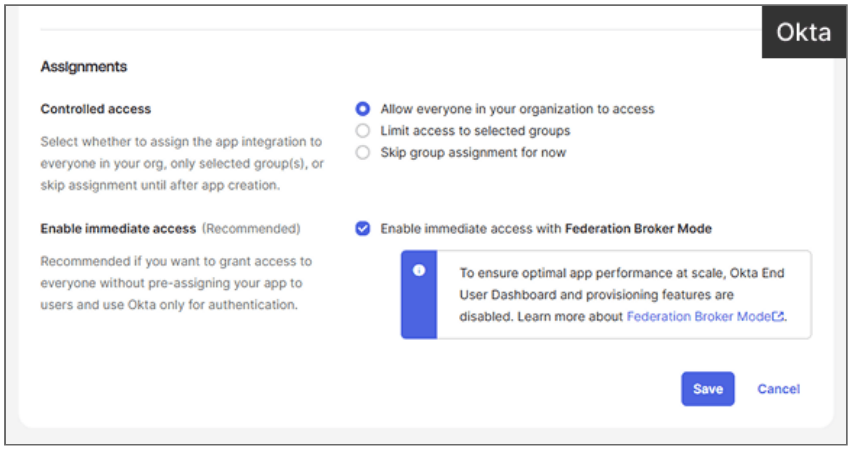
3. **Create App Integration** 버튼을 클릭하세요.
4. **Sign-in method**에서 **OIDC - OpenID Connet**를 선택하세요.
5. **Application type**에서 클라이언트 시크릿(Client secret)을 발급받을 수 있도록 **Web Application**을 선택하세요.



6. **Next** 버튼을 클릭하세요.
7. **App Integration name** 항목에서 'BioStar Air'를 입력하세요.
8. BioStar Air: 리다이렉트 URI 준비 단계에서 복사한 URI 값을 **Sign-in redirect URIs** 섹션의 입력 필드에 붙여넣으세요.



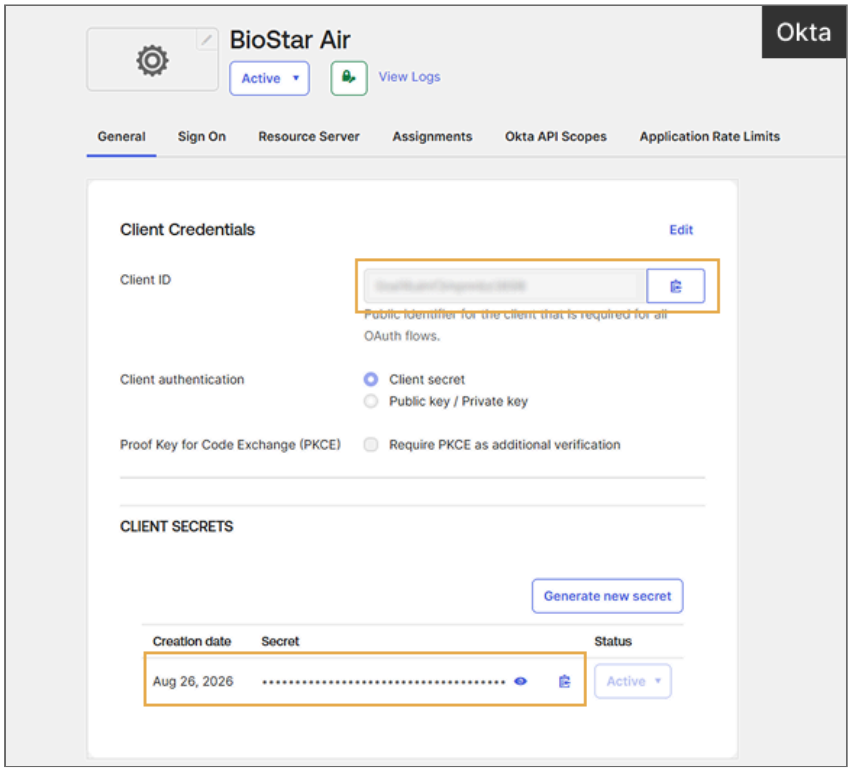
9. **Assignments** 섹션으로 이동해 조직 내 사용자가 애플리케이션에 접근할 수 있도록 **Allow everyone in your organization to access**를 선택하세요.



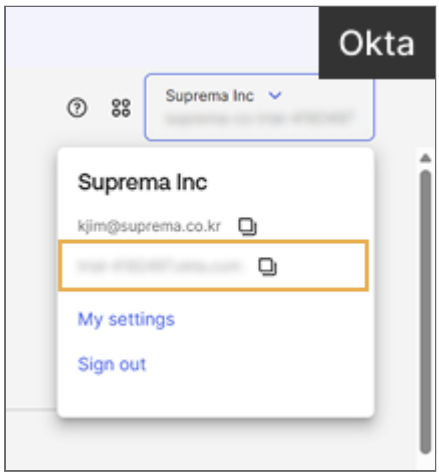
10. **Save**를 클릭하세요.

3 Okta: 앱 클라이언트 정보 복사

1. 애플리케이션을 생성하면 **General** 탭에서 **Client ID**와 **Client Secret**을 복사하세요.



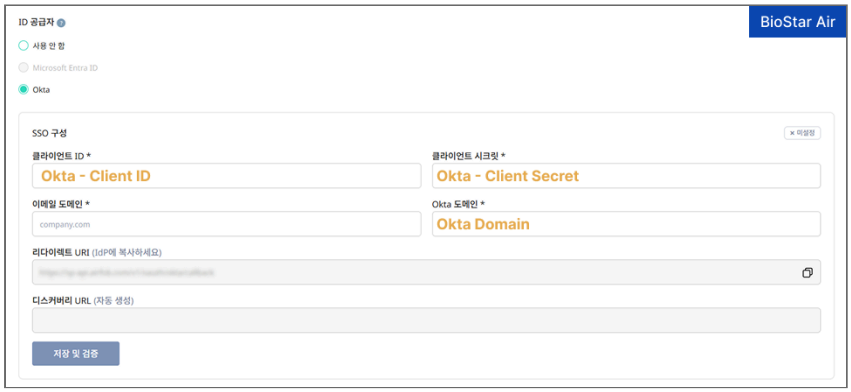
2. 화면 오른쪽 상단의 프로필을 클릭하고 **Okta Domain**을 복사하세요.



복사한 **Client ID**와 **Client Secret, Okta Domain** 값을 다음 단계에서 입력합니다.

4 BioStar Air: SSO 구성

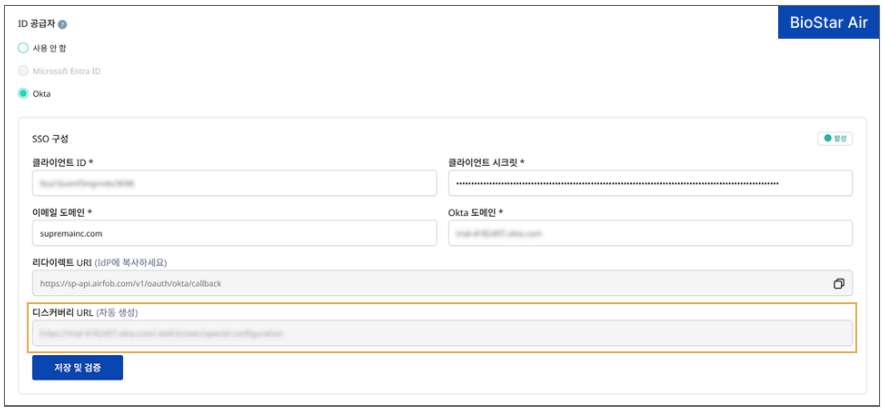
1. BioStar Air 설정 화면으로 돌아와 Okta: 앱 클라이언트 정보 복사 단계에서 복사한 값을 각 필드에 입력하세요.



- **클라이언트 ID**: Client ID
- **클라이언트 시크릿**: Client Secret
- **Okta 도메인**: Okta Domain

2. **이메일 도메인** 필드에 조직의 이메일 도메인을 입력하세요.
3. **저장 및 검증** 버튼을 클릭하세요.

저장 및 검증에 성공하면 **디스커버리 URL** 항목의 값이 자동 생성됩니다.



Okta SCIM 프로비저닝 연결

1 BioStar Air: SCIM 토큰 복사

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **SCIM 프로비저닝** 섹션에서 **SCIM 엔드포인트 URL** 값을 복사하세요.



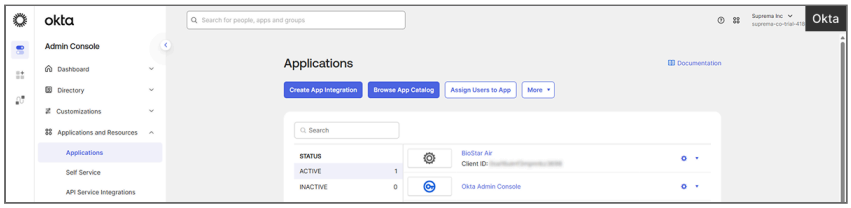
4. **토큰 생성** 버튼을 클릭하세요.

5. 토큰 생성 완료 대화 상자에서 토큰을 복사하세요.

> **알아두기**
>
> - 생성된 토큰을 즉시 복사하세요. 토큰을 생성한 시점에만 복사할 수 있습니다. 대화 상자를 닫으면 토큰을 다시 복사할 수 없습니다.
> - 토큰을 분실했다면 새 토큰을 생성을 위해 **토큰 갱신** 버튼을 클릭하세요. 새 토큰을 ID 공급자에 다시 입력해야 합니다.
> - 이 단계에서 복사한 SCIM 엔드포인트 URL, 토큰을 다음 단계에서 입력해야 합니다.

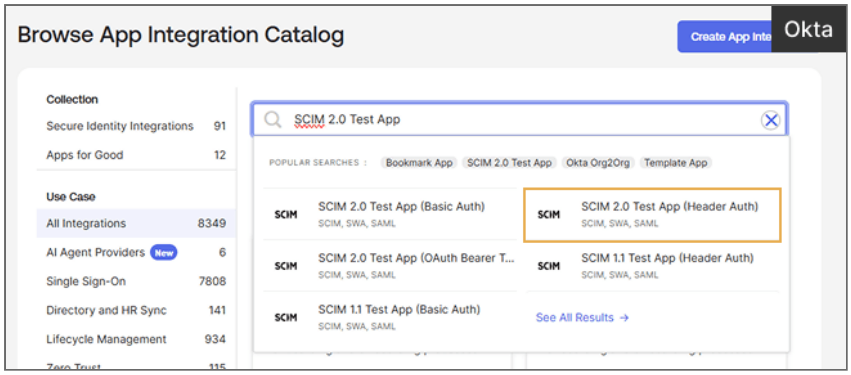
2 Okta: SCIM 프로비저닝 앱 생성

1. Okta 관리자 콘솔에서 **Applications and Resources** → **Applications** 메뉴로 이동하세요.



2. **Browse App Catalog** 버튼을 클릭하세요.

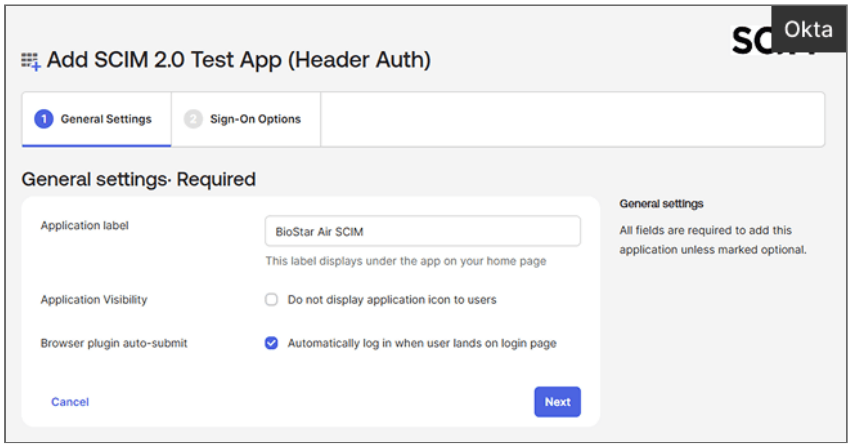
3. 'SCIM 2.0 Test App'을 검색하세요.



4. 검색 결과에서 **SCIM 2.0 Test App (Header Auth)**을 선택하세요.

5. **Add Integration** 버튼을 클릭하세요.

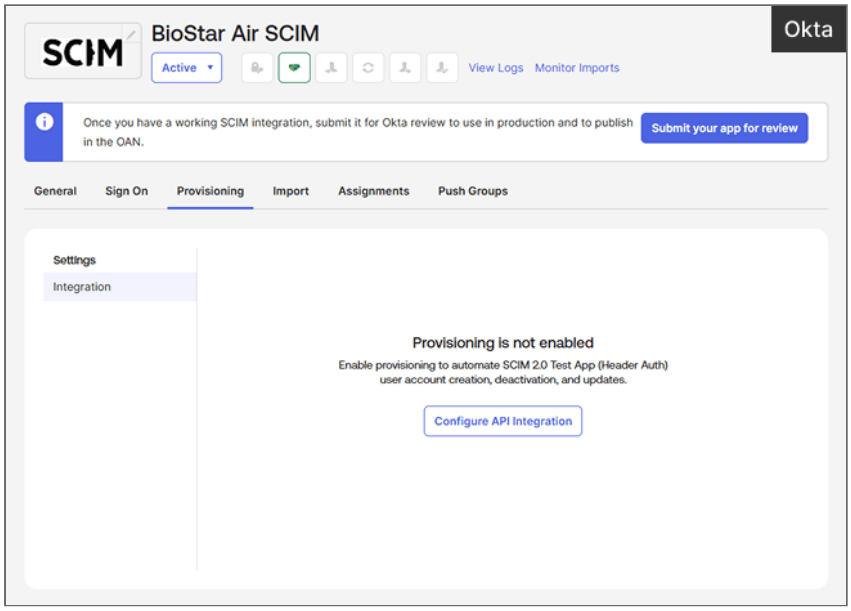
6. **Application label** 입력 필드에 'BioStar Air SCIM'을 입력하세요.



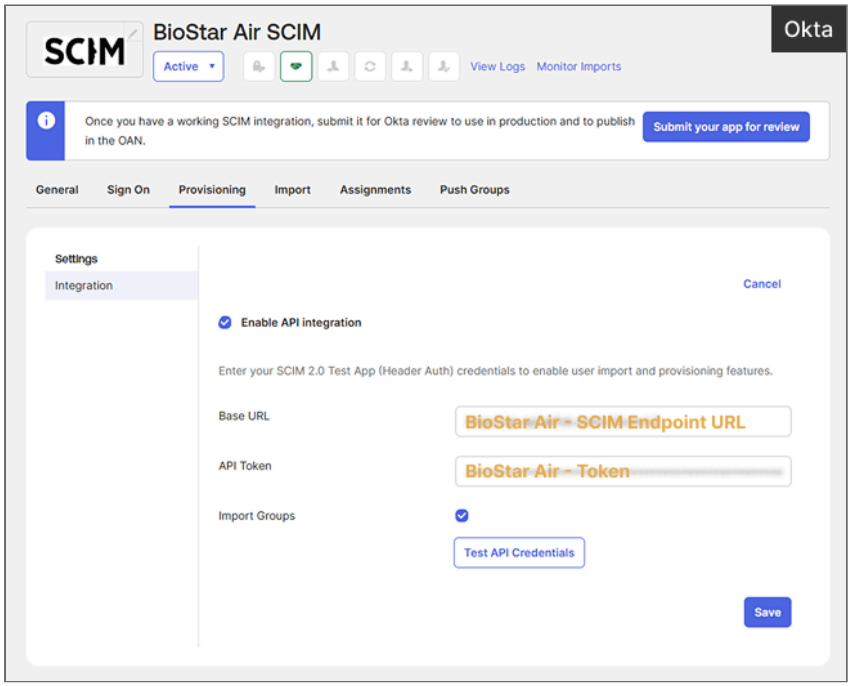
7. **Next** 버튼을 클릭하세요.
8. **Sign-on options** 단계에서는 별도 설정 없이 아래로 스크롤한 후 **Done** 버튼을 클릭하세요.

3 Okta: API 통합 설정

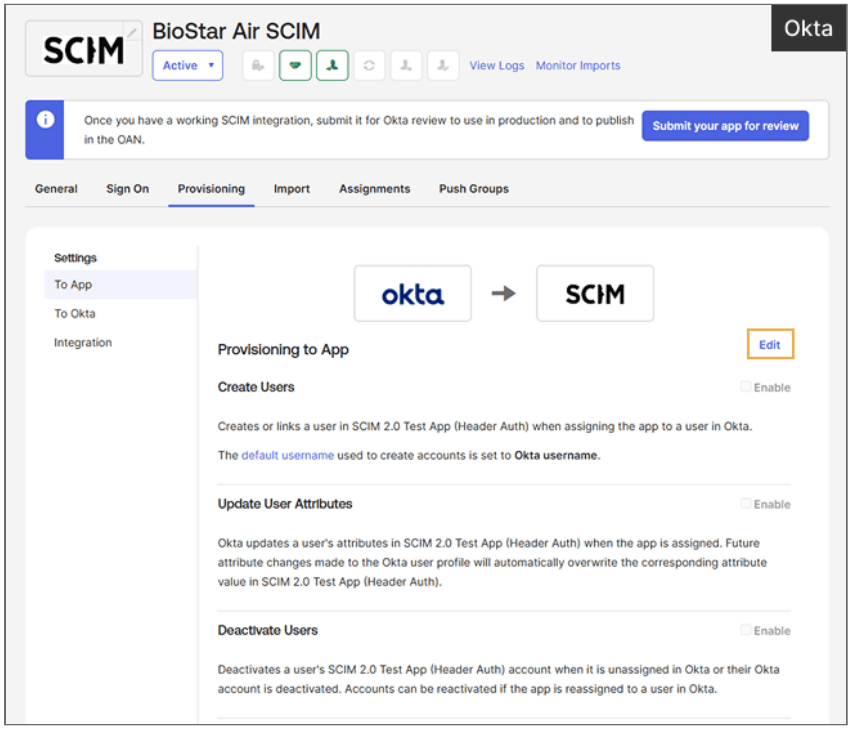
1. 프로비저닝 앱 생성을 완료하면 **Provisioning** 탭을 클릭하세요.



2. **Configure API Integration** 버튼을 클릭하세요.
3. **Enable API integration**을 클릭하세요.
4. BioStar Air: SCIM 토큰 복사 단계에서 복사한 SCIM 엔드포인트 URL, SCIM 베어러 토큰 값을 **Base URL**, **API Token** 필드에 입력하세요.

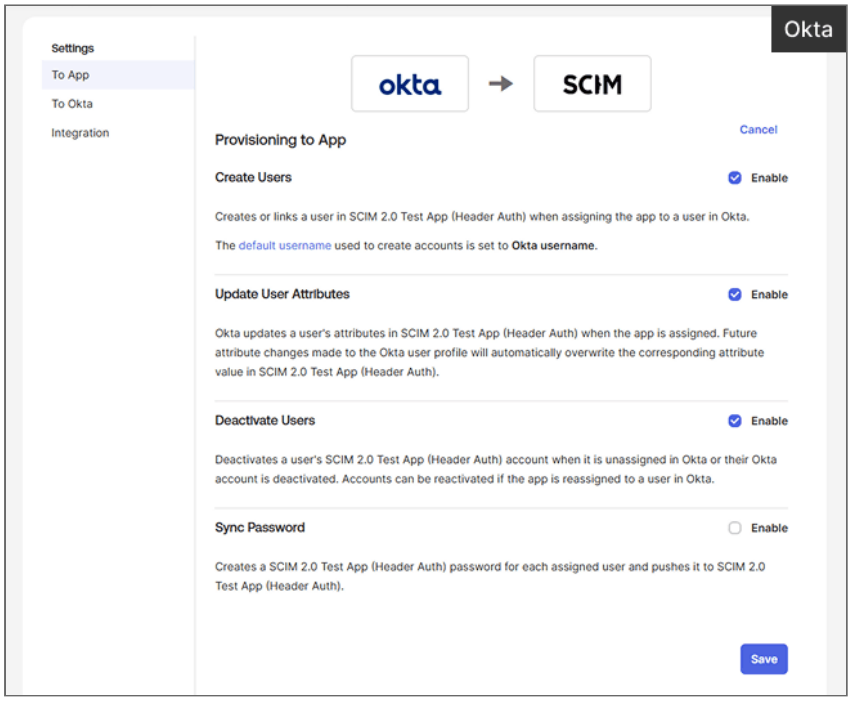


5. 동기화가 정상 동작하는지 테스트하려면 **Test API Credentials** 버튼을 클릭하세요.
6. **Save** 버튼을 클릭하세요.
7. 그룹 푸시 동작 설정을 위해 **Provision** 탭을 클릭하세요.
8. **Edit**를 클릭한 다음 아래 속성을 활성화하세요.



- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

9. 변경한 설정을 저장하려면 **Save** 버튼을 클릭하세요.

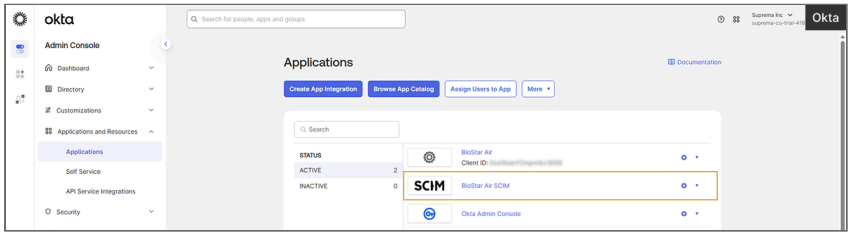


IdP 그룹을 BioStar Air로 푸시

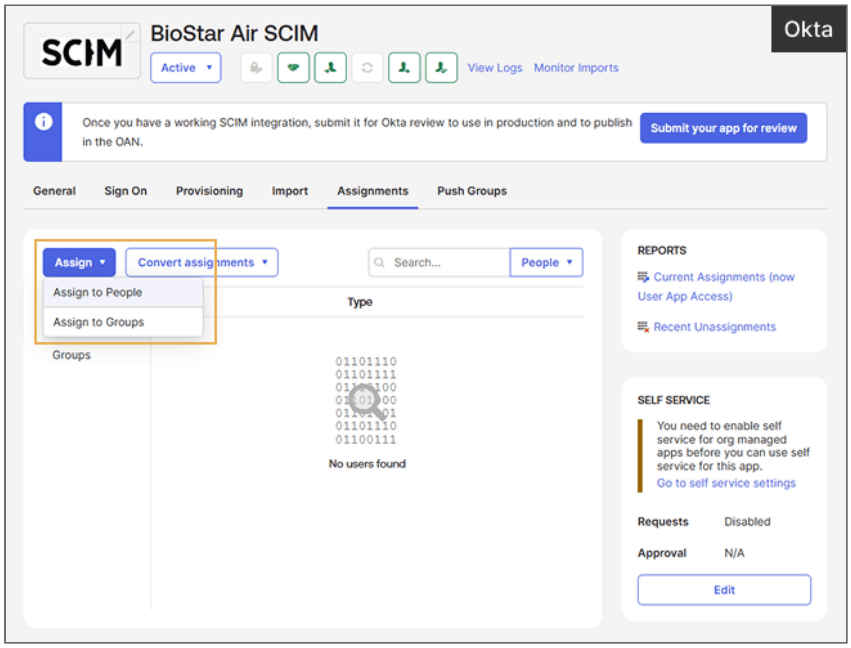
IdP 그룹을 BioStar Air로 푸시하려면 먼저 사용자 그룹과 사용자가 Okta에 준비되어 있어야 합니다. 사용자 그룹과 사용자가 준비되었다면 SCIM을 통해 BioStar Air로 푸시할 수 있습니다.

1 Okta: 사용자 그룹 할당

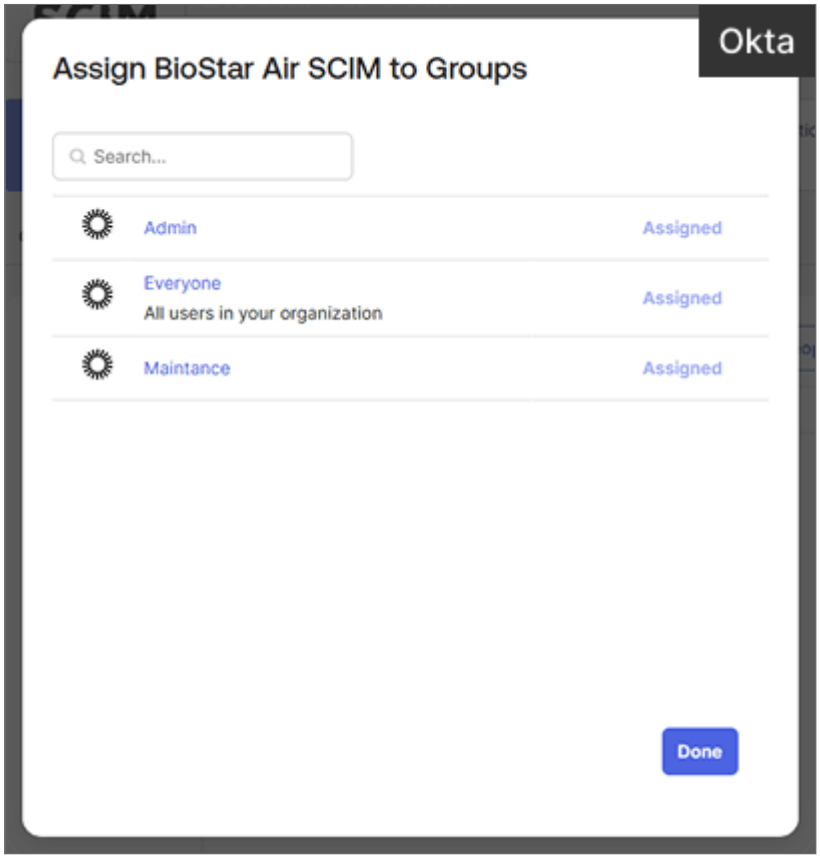
1. **Okta 관리자 콘솔**에 로그인하세요.
2. **Applications and Resources** → **Applications** 메뉴로 이동하세요.
3. SCIM 애플리케이션을 선택하세요.



4. **Assignments** 탭을 클릭하세요.
5. **Assign** → **Assign to Groups**를 클릭하세요.

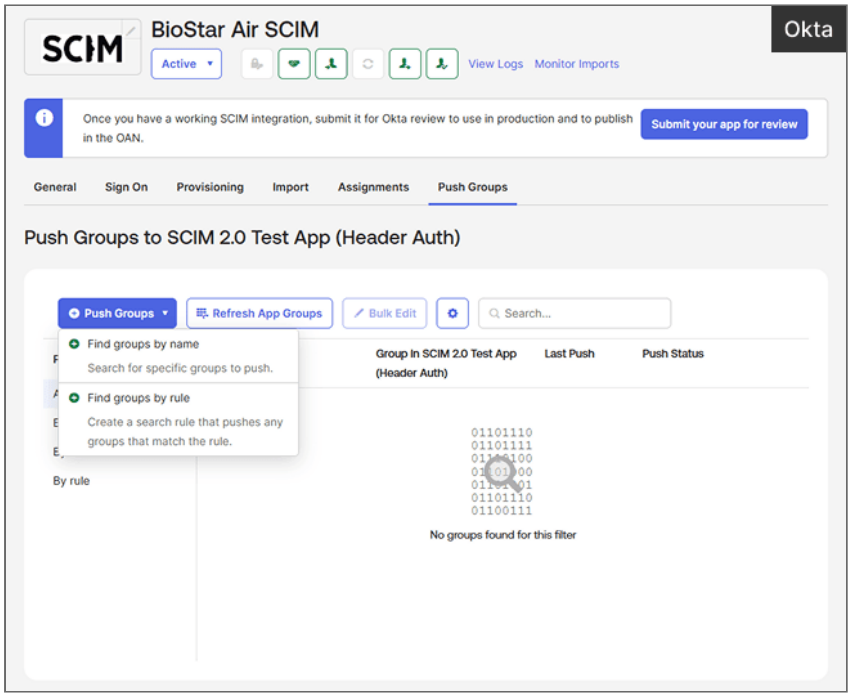


6. SCIM 애플리케이션에 할당할 사용자 그룹에서 **Assign**을 클릭하세요.
7. 그룹 할당을 완료하면 **Done** 버튼을 클릭하세요.

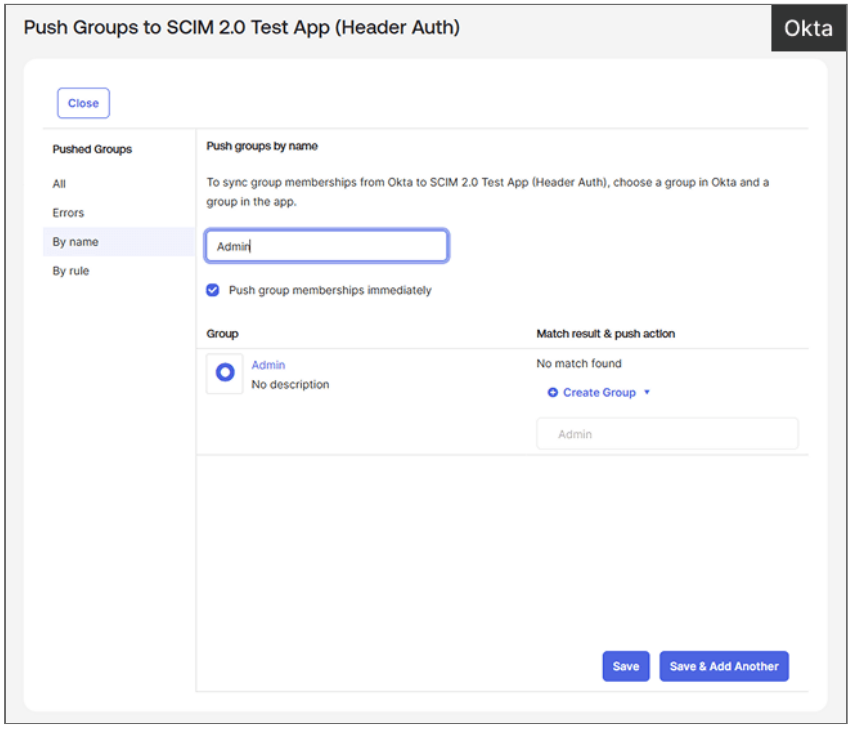


❷ Okta: 사용자 그룹 푸시

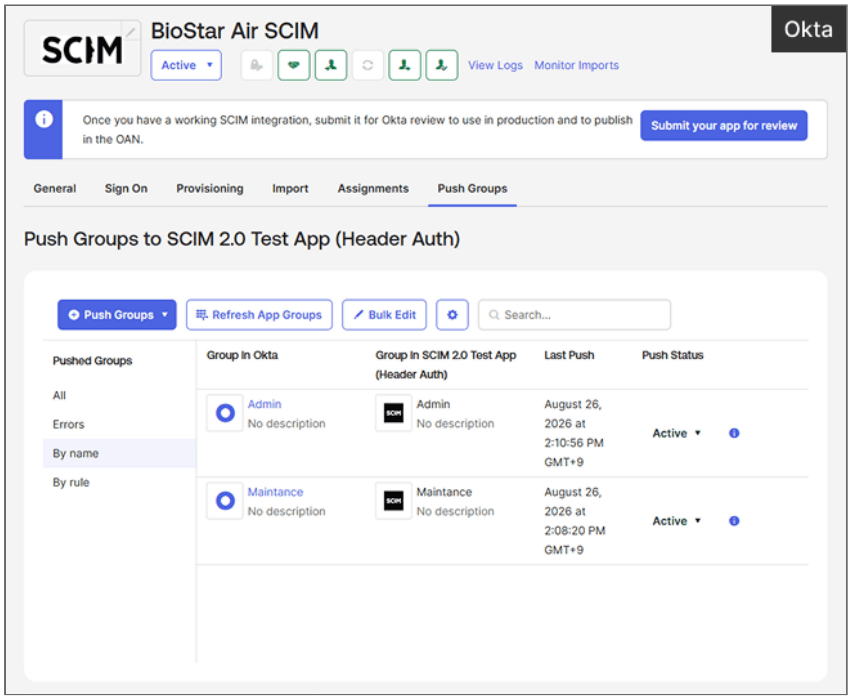
1. **Push Groups** 탭을 클릭하세요.
2. **Push Groups** → **Find groups by name**을 클릭하세요.



3. 입력 필드에 푸시할 그룹 이름을 입력하세요.
4. 일치하는 사용자 그룹이 나타나면 선택하세요.

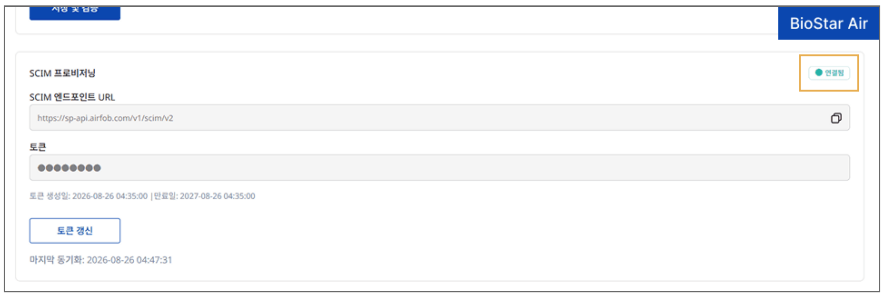


5. 사용자 그룹 선택을 완료하면 **Save** 버튼을 클릭하거나 **Save & Another** 버튼을 클릭해 사용자 그룹을 추가할 수 있습니다.
6. **Push Groups** 탭에서 푸시된 사용자 그룹을 확인할 수 있습니다.



❸ BioStar Air: 연결 확인

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **SCIM 프로비저닝** 섹션에서 **연결됨** 표시를 확인하세요.



그룹 매핑

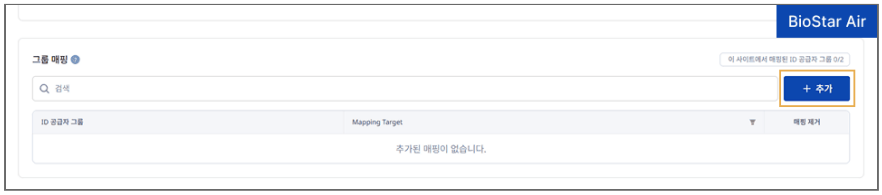
SSO와 SCIM 연결을 완료하고 ID 공급자 그룹을 BioStar Air로 푸시했다면, 사이트 관리자는 푸시된 그룹을 BioStar Air 그룹에 매핑해야 합니다.

매핑 규칙

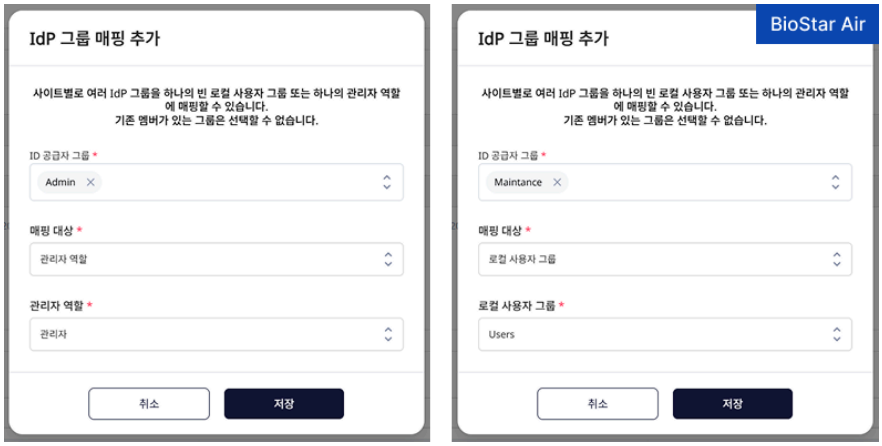
- 하나의 BioStar Air 사용자 그룹에 둘 이상의 ID 공급자 그룹을 매핑할 수 있습니다.
- BioStar Air 사용자 그룹은 매핑하기 전에 비어 있어야 합니다.
- 이미 구성원이 있는 BioStar Air 그룹은 매핑 대상으로 선택할 수 없습니다.
- ID 공급자 그룹 매핑은 사이트 마스터 관리자만 관리할 수 있습니다.
- ID 공급자 그룹을 마스터 역할에 매핑하면 이후에는 역할을 변경할 수 없습니다.

관리자/사용자 그룹 매핑하기

1. BioStar Air 화면 왼쪽 사이드에서 **설정** → **사이트**를 클릭하세요.
2. **SSO & SCIM** 탭을 클릭하세요.
3. **그룹 매핑** 섹션으로 이동해 **추가** 버튼을 클릭하세요.



4. **ID 공급자 그룹**에서 ID 공급자 그룹을 선택하세요.
5. **매핑 대상**에서 선택한 IdP 그룹에 따라 **관리자 역할** 또는 **로컬 사용자 그룹**을 선택하세요.
6. 매핑 대상에 따라 관리자 역할을 지정하거나 사용자 그룹을 선택할 수 있습니다.



7. 매핑을 저장하려면 **저장** 버튼을 클릭하세요.

그룹 매핑 섹션에서 ID 공급자 그룹과 매핑된 BioStar Air 그룹을 확인할 수 있습니다.

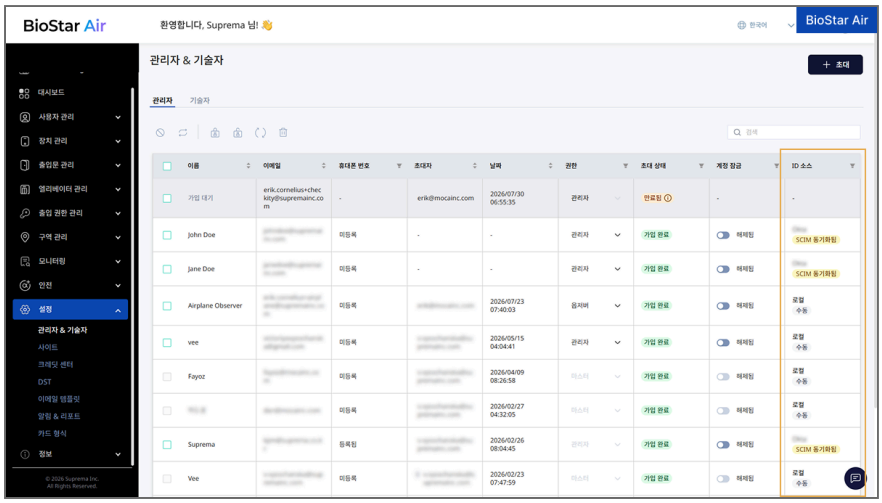


> **알아두기**
>
> - 관리자 역할에 대한 자세한 내용은 관리자 계정 및 역할 관리하기를 참고하세요.
> - 사용자 그룹에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

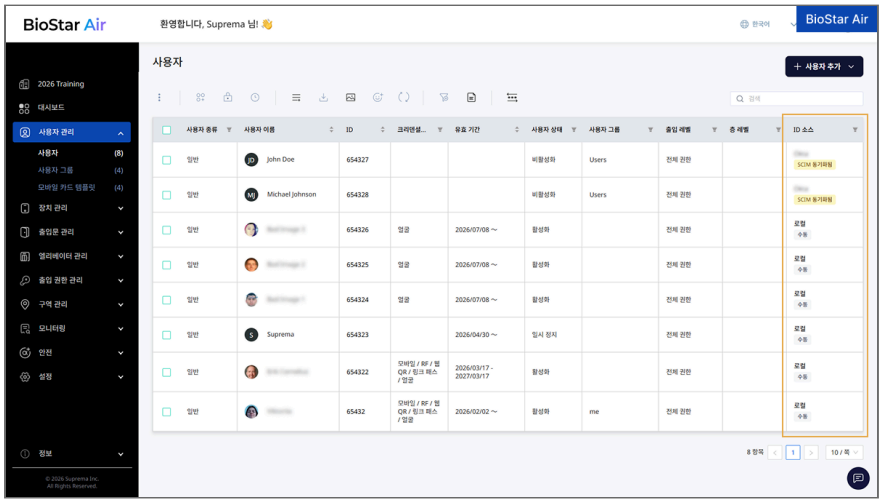
동기화된 관리자/사용자/그룹 관리

프로비저닝이 활성화되면 BioStar Air는 각 관리자, 사용자, 사용자 그룹이 로컬에서 직접 관리되는지, ID 공급자에서 동기화된 것인지 화면에 표시합니다.

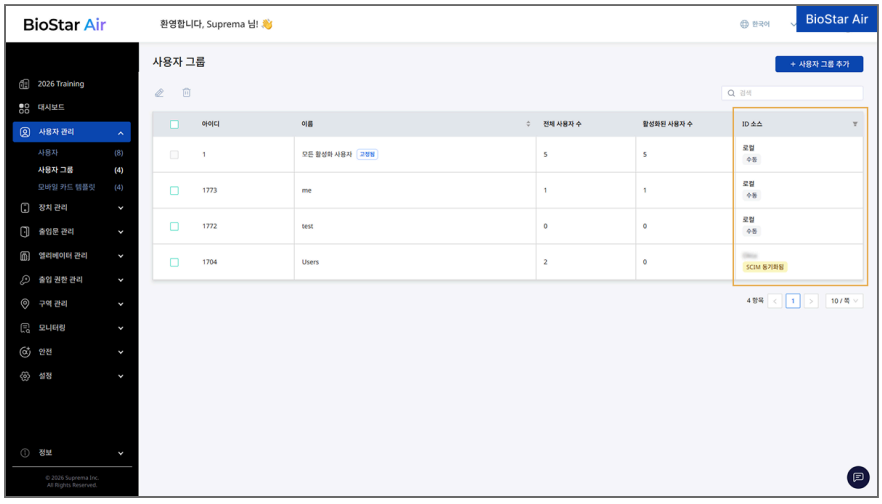
- **설정** → **관리자 & 기술자** 메뉴의 관리자 목록에서 **ID 소스** 열을 확인하세요.



- **사용자 관리** → **사용자** 메뉴의 사용자 목록에서 **ID 소스** 열을 확인하세요.



- **사용자 관리** → **사용자 그룹** 메뉴의 사용자 그룹 목록에서 **ID 소스** 열을 확인하세요.



SCIM 동기화 항목의 동작 방식

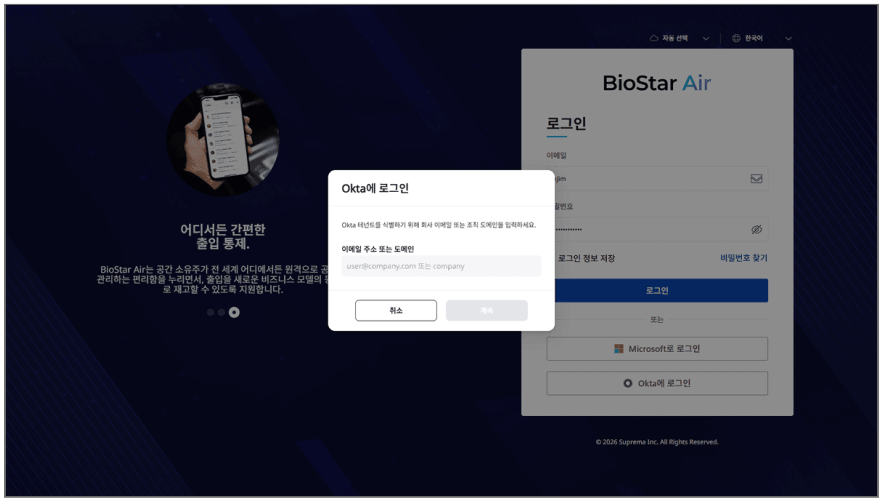
- 기존에 수동으로 생성한 사용자와 관리자는 계속 수동 관리 상태로 유지됩니다.
- SCIM으로 동기화된 항목은 BioStar Air에서 수동으로 삭제할 수 없습니다.
- SCIM으로 동기화된 그룹은 사용자를 수동으로 추가하거나 제거할 수 없습니다.
- 동기화된 항목을 로컬에서 수동으로 변경하면 **오버라이드** 상태가 됩니다. **오버라이드 해제**를 실행하면 로컬 변경 사항이 취소되고 항목이 다시 SCIM 관리 상태로 돌아갑니다.



Okta에 로그인

Okta SSO 연결을 완료하면 사용자는 BioStar Air 로그인 화면에서 Okta 계정으로 로그인할 수 있습니다.

1. BioStar Air 로그인 화면에서 **Okta에 로그인** 버튼을 클릭하세요.



2. **이메일 주소 또는 도메인** 필드에 조직의 이메일 주소 또는 도메인을 입력하세요. (예: `user@company.com` 또는 `company`)
3. **계속** 버튼을 클릭하세요.
4. Okta 로그인 화면으로 이동하면 조직 계정의 이메일 주소와 비밀번호를 입력하세요.
5. 인증을 완료하면 BioStar Air로 자동 리디렉션되어 로그인이 완료됩니다.

알아두기

입력한 이메일 도메인에 대해 Okta SSO가 설정되어 있지 않으면 오류 메시지가 표시됩니다. 이때는 사이트 관리자에게 문의하세요.

추가 사이트 구성하기

사이트 기본 설정 외에도 시간 정책, 이메일 발송 양식, 알림 수신 방식, 근태 기록 등 BioStar Air 서비스 전반에 영향을 주는 세부 기능을

구성할 수 있습니다. 커스텀 Wiegand 카드 형식을 추가하거나, T&A 운영 방식과 리포트 생성 기준을 직접 설정할 수도 있습니다.

일광 절약 시간(DST) 구성하기

일광 절약 시간(Daylight Saving Time, DST) 설정을 통해 사이트의 시간 조정 방식을 구성할 수 있습니다. 이는 특히 여러 시간대에 걸쳐 장치와 기록이 있는 사이트를 관리할 때 일관되고 정확한 시간 추적을 보장하는 데 중요합니다.

BioStar Air에서 정확한 시간 관리를 위해서는 **세 곳에서 DST 설정**이 필요합니다:

- **DST 프로필**: 각 시간대별로 DST의 시작 및 종료 일시를 정의합니다.
- **사이트 시간**: 사이트와 이벤트 로그에 적용될 시간대를 설정합니다.
- **장치 시간**: 각 개별 장치가 올바르게 시간을 조정하도록 설정합니다.

일광 절약 시간을 준수하는 시간대에 있는 경우 이 세 가지 설정이 모두 올바르게 구성되어야 합니다.

> **팁**
> 일광 절약 시간(Daylight Saving Time, DST) 설정에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

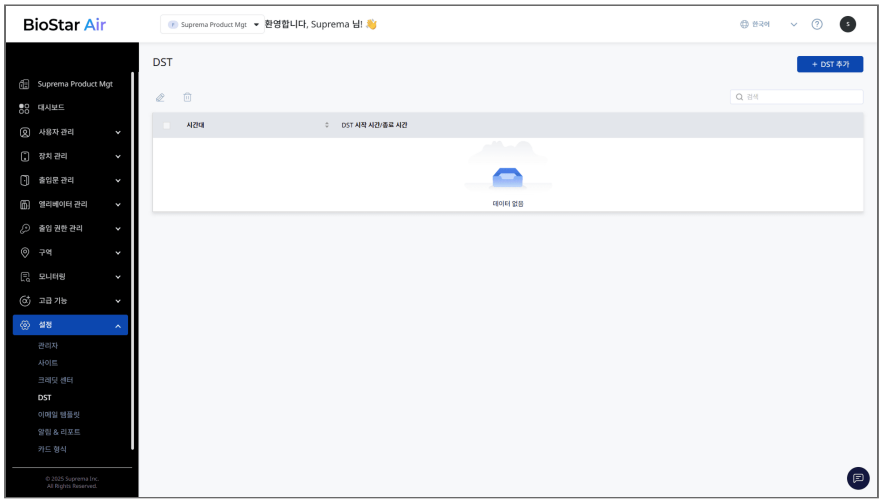
> **알아두기**
> 이벤트 로그를 확인할 때 아래 사항을 참고하세요.
> - 장치 시간이 설정되어 있다면 이벤트 로그 타임스탬프는 각 개별 장치의 DST 시간에 맞춰 조정됩니다.
> - 사이트 시간이 설정되어 있다면 타임스탬프는 장치별이 아닌 사이트의 DST 구성에 따라 조정됩니다.

1단계: DST 프로필 만들기

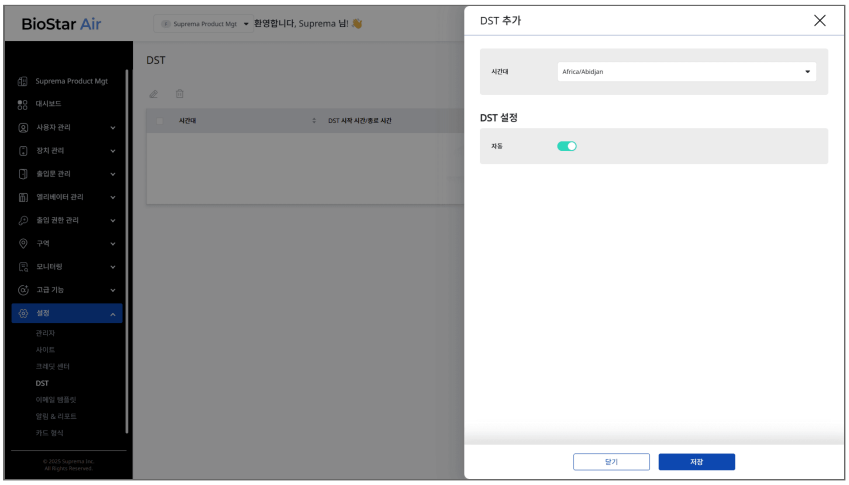
DST 프로필은 특정 시간대에 대해 DST가 시작되고 종료되는 일시를 정의합니다. 사이트와 장치가 위치한 시간대마다 DST 프로필을 만들어야 합니다.

새로운 프로필 추가

1. 화면 왼쪽 사이드바에서 **설정** → **DST**를 클릭하세요.
2. 화면 오른쪽 상단의 **DST 추가** 버튼을 클릭하세요.



3. **DST 추가** 패널이 나타나면 **시간대**에서 원하는 항목을 선택하세요.
4. **DST 설정**에서 자동 또는 수동 구성을 선택하세요.
   - **자동 구성**: 선택한 시간대에 대한 DST 구성이 자동으로 추가됩니다. DST가 시작되고 종료되는 날짜는 해당 시간대의 표준 규칙에 따라 설정됩니다.



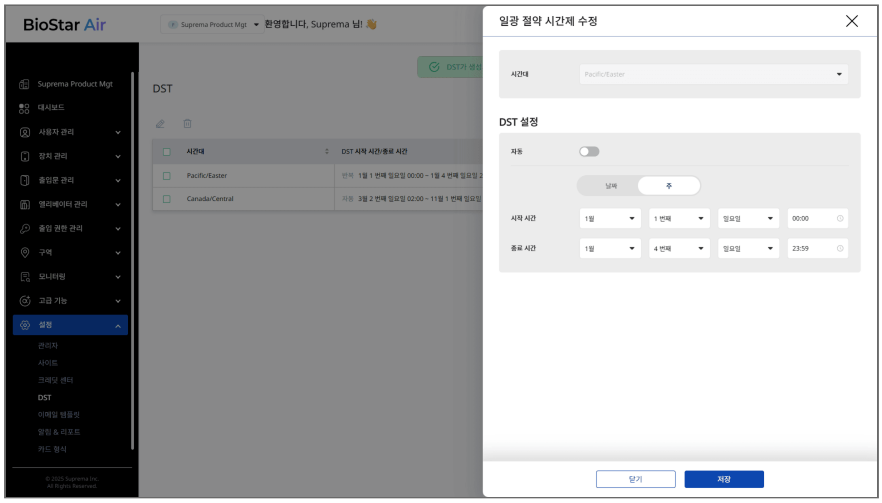
   - **수동 구성**: 수동으로 구성하려면 해당 시간대에 대한 적절한 시작 시간과 종료 시간을 설정하세요.



     - **날짜**: DST가 시작되고 종료되는 날짜를 선택할 수 있습니다.
     - **주**: DST가 시작되고 종료되는 주를 선택할 수 있습니다.
5. DST 프로필을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

기존 프로필 수정

1. 화면 왼쪽 사이드바에서 **설정** → **DST**를 클릭하세요.
2. 목록에서 수정하려는 DST 프로필을 클릭하세요. 또는 체크박스를 클릭하고 상단의 버튼을 클릭하세요.
3. **일광 절약 시간제 수정** 패널이 나타나면 시작 시간과 종료 시간을 수정하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

4. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

프로필 삭제

1. 화면 왼쪽 사이드바에서 **설정** → **DST**를 클릭하세요.
2. 목록에서 삭제하려는 DST 프로필의 체크박스를 클릭하세요. 1개 이상의 프로필을 선택할 수 있습니다.
3. 화면 상단의 버튼을 클릭하세요.
4. 메시지 창이 나타나면 **삭제** 버튼을 클릭하세요.

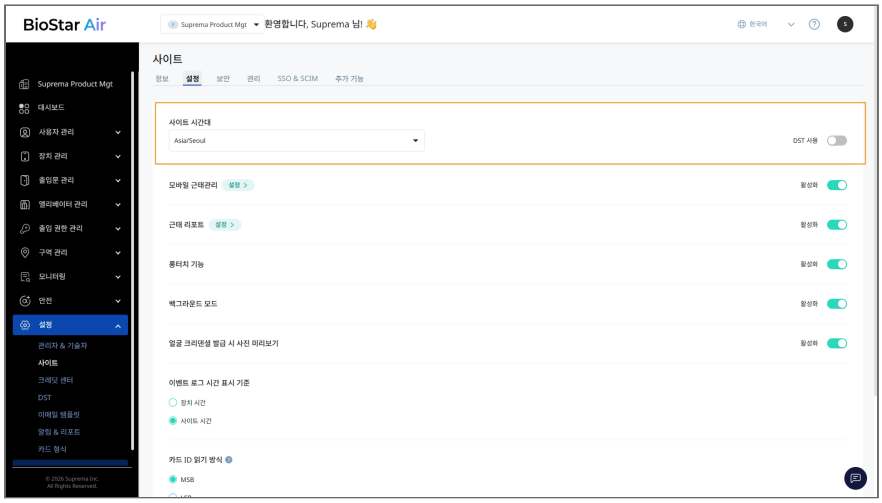
2단계: 사이트 시간 설정

사이트 시간은 전체 시스템이 사용할 기본 시간대를 결정합니다. 이 설정에 영향받는 항목은 아래와 같습니다.

- 이벤트 로그 및 기록의 타임스탬프
- 보고서 및 모니터링 데이터
- 새로운 장치를 등록할 때 적용되는 기본 시간대

다음 안내에 따라 사이트 시간대를 설정하고 DST를 활성화하세요.

1. 화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요.
2. **설정** 탭을 클릭하세요.
3. **사이트 시간대**에서 원하는 시간대를 선택하세요.



4. 선택한 시간대가 일광 절약 시간을 적용하려면, **DST 사용** 옵션을 활성화하세요.

> **주의**
>
> DST가 적용되는 시간대인데 **DST 사용** 옵션을 활성화하지 않으면, 시스템이 자동으로 시간을 조정하지 않아 이벤트 로그가 잘못 표시될 수 있습니다.

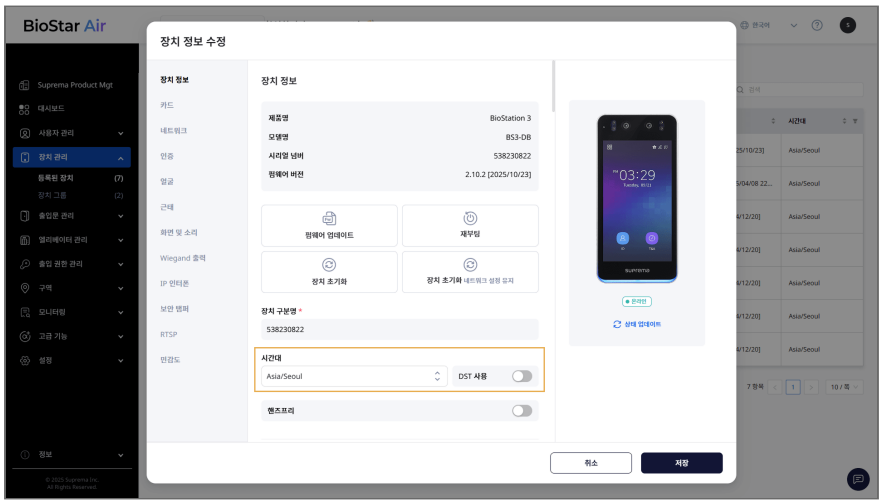
3단계: 장치의 DST 활성화

BioStar Air에 연결된 각 장치는 자체 시계를 유지하며, 이를 출입 제어와 근태 기록에 사용합니다. 일광 절약 시간이 적용되는 시간대에 위치한 장치라면 반드시 DST 설정을 해야 합니다.

BioStation 3와 같이 화면이 있는 장치는 사용자에게 시간을 표시합니다. XPass 2와 같이 화면이 없는 장치도 내부적으로 시계를 유지하며, 출입 제어와 근태 기록에 사용합니다.

화면 유무와 관계없이 모든 장치에서 DST를 설정해야 이벤트 로그, 출입 기록, 근태 데이터가 정확하게 기록할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 목록에서 DST 설정을 적용하려는 장치를 클릭하세요.
3. **시간대** 섹션에서 원하는 시간대를 선택하고 **DST 사용** 옵션을 활성화하세요.



> DST를 적용하는 시간대에서 이 설정은 기본 활성화됩니다.

4. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

> **알아두기**
> 장치 시간이 올바르게 설정되지 않으면 아래와 같은 문제가 발생할 수 있습니다:
> - **출입 거부 오류**: 출입 시간이 오전 07:00부터 설정되어 있는데, 장치가 오전 06:00이라고 생각하면 사용자 출입이 거부됩니다.
> - **일정 오류**: 예약된 시간의 잠금/해제가 정확하지 않을 수 있습니다.
> - **기록 오류**: 이벤트 로그와 근태 기록의 시간이 실제 시간과 맞지 않습니다.

체크리스트

일광 절약 시간이 적용되는 지역에서 정확한 시간 관리를 보장하려면 다음 세 단계를 모두 완료했는지 확인하세요.

- **DST 프로필 생성**: 시간대별로 필요한 DST 프로필을 만들었나요?
- **사이트 시간 설정**: 사이트의 시간대를 설정하고 **DST 사용** 옵션을 활성화했나요?
- **장치 DST 적용**: 각 장치의 시간대를 설정하고 **DST 사용** 옵션을 활성화했나요?

이 세 가지가 모두 올바르게 구성하면 이벤트 로그, 접근 시간, 근태 기록이 모두 정확한 시간으로 표기됩니다.

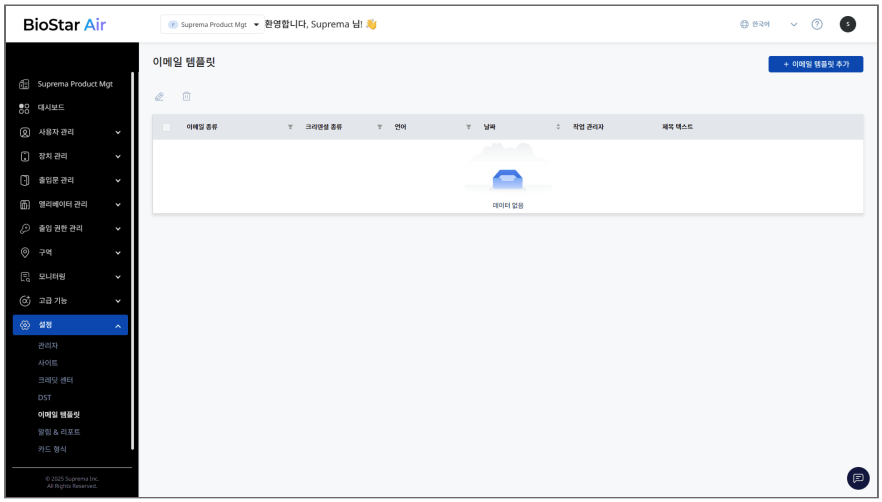
이메일 템플릿 사용자 정의하기

이메일 템플릿 기능을 사용하여 사이트 사용자에게 전송되는 이메일을 사용자 정의하여 회사의 브랜드와 메시지를 반영할 수 있습니다. 이메일 템플릿에는 초대장, 활성화 이메일 및 기타 알림 등이 포함됩니다.

> **팁**
> 이메일 템플릿 설정에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

이메일 템플릿 추가

1. 화면 왼쪽 사이드바에서 **설정** → **이메일 템플릿**을 클릭하세요.
2. 화면 오른쪽 상단의 **이메일 템플릿 추가** 버튼을 클릭하세요.

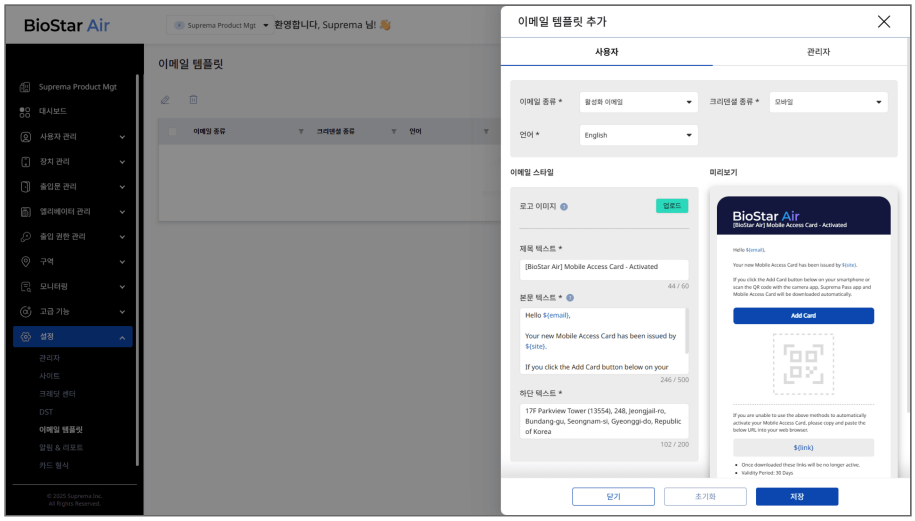


3. **이메일 템플릿 추가** 패널이 나타나면 각 항목의 설정을 구성하세요. **사용자** 또는 **관리자** 탭을 선택하여 사용자 또는 관리자 이메일 템플릿을 설정할 수 있습니다.

> **알아두기**
>
> 언어에 따라 이메일 템플릿을 별도로 생성할 수 있습니다. **언어** 옵션에서 언어를 선택할 수 있습니다. 지원하는 언어는 아래와 같습니다.
>
> > *English, 한국어, 日本語, Nederlands, Español, Português*
>
> 더 많은 언어를 지원할 예정입니다.

사용자

사용자에게 전송되는 이메일 템플릿을 사용자 정의할 수 있습니다.



- **이메일 종류**: 만들고자 하는 이메일 템플릿 유형을 선택하세요. 사용 가능한 옵션은 아래와 같습니다.
  - **활성화 이메일**: 일반적으로 모바일 카드를 다운로드하기 위한 초대장으로 사용합니다.
  - **재활성화 이메일**: 모바일 카드를 재활성화되었음을 알림을 사용자에게 전송합니다.
  - **재발급 이메일**: 새 모바일 카드를 발급할 때 사용합니다.
  - **삭제 이메일**: 카드 삭제에 대한 알림을 사용자에게 전송합니다.
  - **일시 정지 이메일**: 카드가 일시 중지되었음을 사용자에게 알립니다.

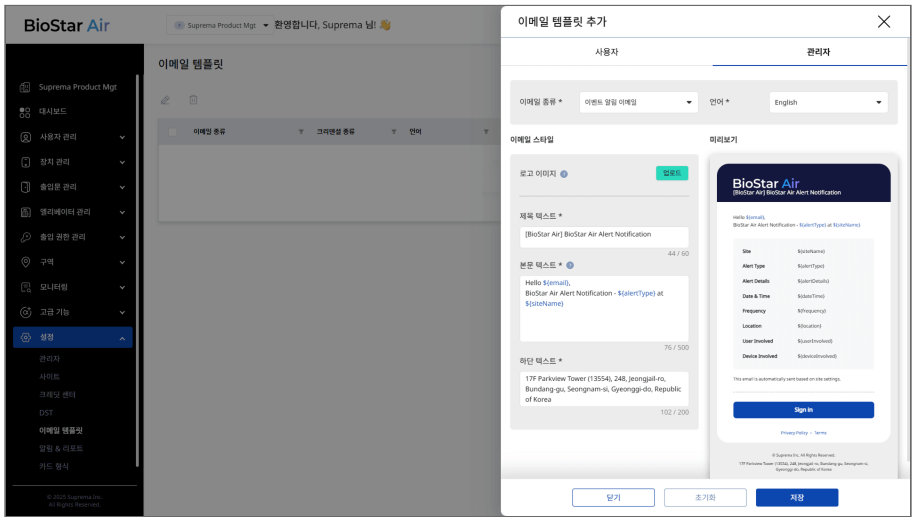
  - **얼굴 등록 요청**: 사용자에게 얼굴 사진 등록을 요청할 때 사용합니다.

- **크리덴셜 종류**: **활성화 이메일** 및 **재발급 이메일**과 같이 모바일 카드 다운로드를 허용하는 이메일 종류에서 선택할 수 있습니다.
  - **모바일**
  - **웹 QR**
  - **링크 패스**

> 크리덴셜 유형에 대한 자세한 내용은 사용자 카드 및 크리덴셜 종류를 참고하세요.

관리자

관리자에게 전송되는 이메일 템플릿을 사용자 정의할 수 있습니다.

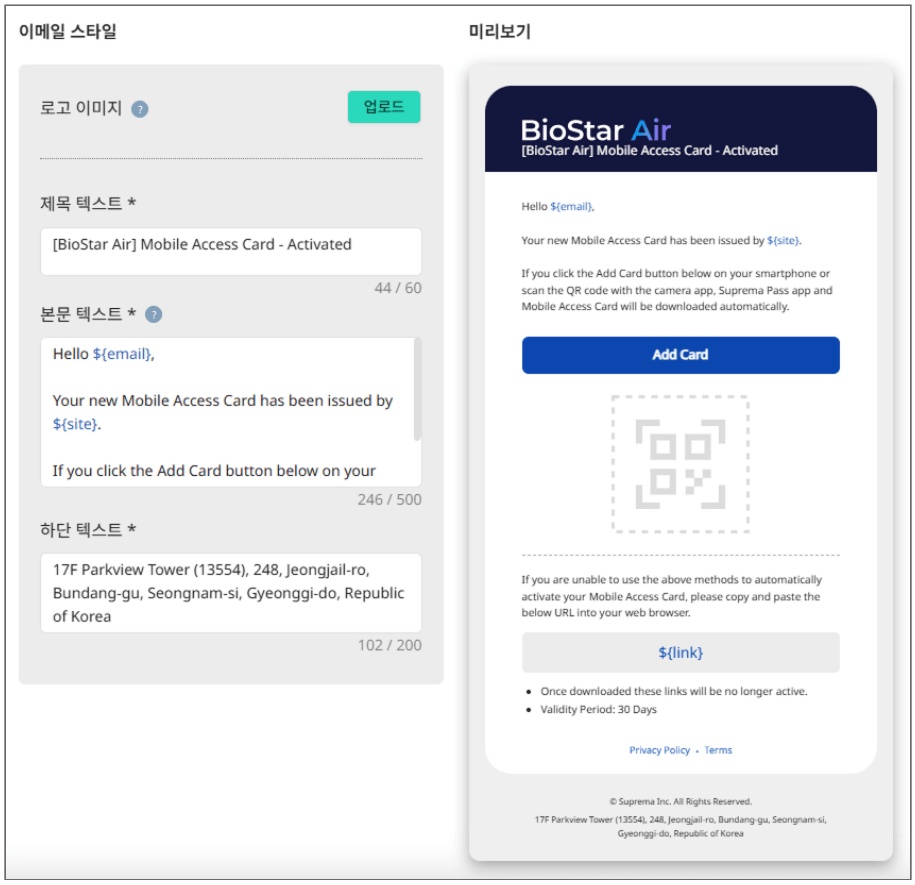


이메일 종류: 만들고자 하는 이메일 템플릿 유형을 선택하세요. 사용 가능한 옵션은 아래와 같습니다.

- **이벤트 알림 이메일**: 사이트에서 발생한 이벤트에 대한 알림을 관리자에게 전송합니다.
- **시스템 알림 이메일**: 시스템 경고를 관리자에게 전송합니다.
- **리포트 알림 이메일**: 리포트를 생성한 후 다운로드 링크를 관리자에게 전송합니다.

이메일 스타일

이메일의 로고와 내용을 사용자 정의할 수 있습니다. **미리보기**에서 실시간으로 변경 사항을 확인할 수 있습니다.



- **로고 이미지**: 이메일에 표시할 로고 이미지를 업로드하세요.

  - 파일 형식: JPG, JPEG, PNG
  - 최소 해상도: 200 x 60
  - 파일 크기: 1 MB 이하

- **제목 텍스트**: 이메일 제목을 입력하세요.
- **본문 텍스트**: 이메일 본문에 표시할 메시지를 입력하세요.

이메일 본문에는 HTML 키(key)가 포함되어야 합니다. 키(key)는 각각 수신자의 이메일 주소와 사이트 이름 등으로 대체됩니다. **이메일 종류**에서 선택한 값에 따라 사용할 수 있는 키(key)는 다를 수 있습니다.

- **사용자** 탭
  - `${email}`: 이메일 주소
  - `${siteName}`: 사이트 이름
- **관리자** 탭
  - `${email}`: 이메일 주소
  - `${siteName}`: 사이트 이름
  - `${alertType}`: 알림 유형
  - `${alertDetails}`: 알림 세부 정보
  - `${frequency}`: 알림 발생 빈도
  - `${location}`: 알림 발생 위치
  - `${userInvolved}`: 알림과 관련된 사용자
  - `${deviceInvolved}`: 알림과 관련된 장치
  - `${dateTime}`: 알림 발생 일시

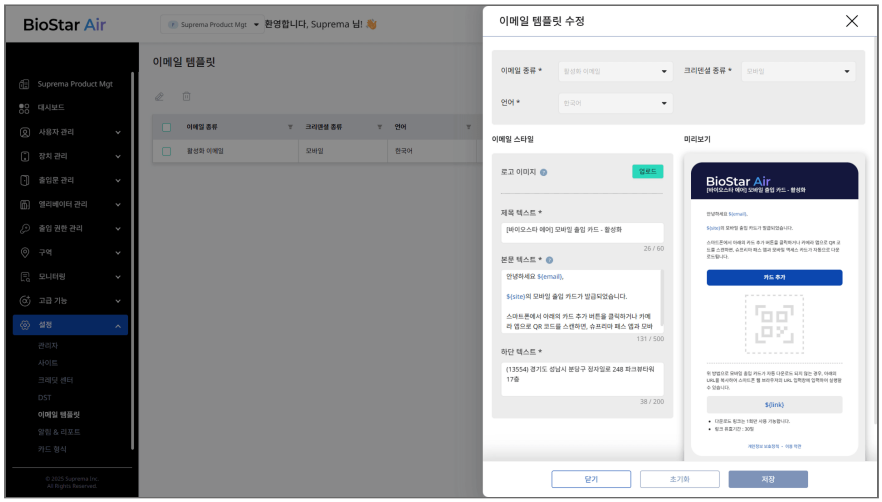
- **하단 텍스트**: 이메일 하단에 표시할 추가 정보를 입력하세요. 규정 준수를 위해 또는 사용자에게 위치 세부 정보를 제공하기 위해 회사 주소나 연락처 정보를 추가하세요.

알아두기

- 로고 이미지가 이메일에 적절하게 표시될 수 있도록 적절한 형식과 크기인지 확인하세요.
- 현재 사용하는 언어가 지원되지 않는다면 향후 업데이트를 확인하세요. 더 많은 언어를 추가할 예정입니다.
- 주소 필드는 규제 준수 및 명확성을 위해 중요하므로 정확하게 입력하세요.
- 이메일 템플릿을 저장하려면 하단의 **저장** 버튼을 클릭하세요.
- 기존에 주어진 내용을 변경한 후 복원하려면 하단의 **초기화** 버튼을 클릭하세요.

이메일 템플릿 수정

1. 화면 왼쪽 사이드바에서 **설정** → **이메일 템플릿**을 클릭하세요.
2. 목록에서 수정하려는 이메일 템플릿을 클릭하세요. 또는 체크박스를 클릭하고 상단의  버튼을 클릭하세요.
3. **이메일 템플릿 수정** 패널이 나타나면 필요한 항목을 수정하세요.



4. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

이메일 템플릿 삭제

1. 화면 왼쪽 사이드바에서 **설정** → **이메일 템플릿**을 클릭하세요.
2. 목록에서 삭제하려는 이메일 템플릿의 체크박스를 클릭하세요. 1개 이상의 템플릿을 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 메시지 창이 나타나면 **삭제** 버튼을 클릭하세요.

알림 및 리포트 설정하기

알림과 리포트를 설정하면 시스템 이벤트와 보안 상황을 자동으로 감지하고 추적할 수 있습니다. 이 문서에서는 BioStar Air에서 알림 및 리포트 설정을 구성하는 방법을 안내합니다.

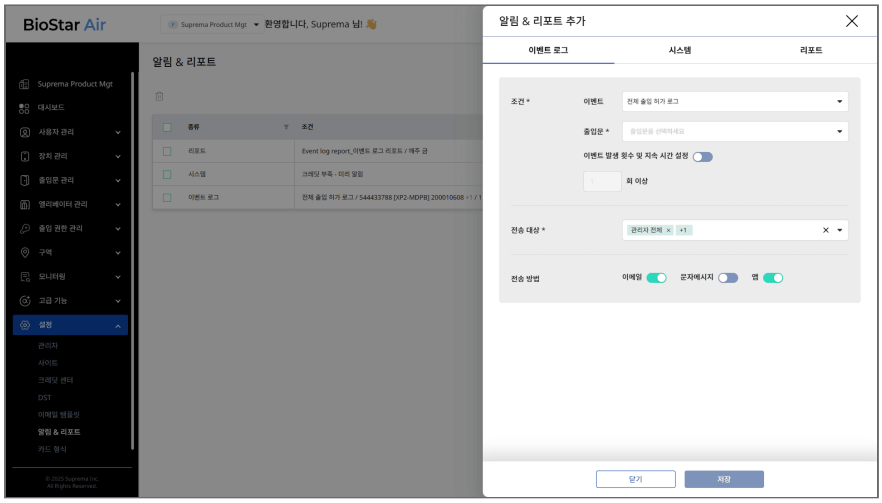
알림 및 리포트 설정을 통해 다음과 같은 효과를 얻을 수 있습니다.

- 보안 위협이나 시스템 문제를 즉시 감지하고 관리자에게 실시간 알림을 보냅니다.
- 시스템 상태 및 사용자 활동에 대한 리포트를 자동 생성하여 관리 효율성을 높일 수 있습니다.

알림 추가

사이트에서 발생하는 특정 이벤트 로그, 시스템에 대한 알림을 설정할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **알림 & 리포트**를 클릭하세요.
2. 화면 오른쪽 상단의 **알림 & 리포트 추가** 버튼을 클릭하세요.
3. **알림 & 리포트 추가** 패널이 나타나면 **이벤트 로그**, **시스템** 탭 중 하나를 선택하세요.



4. 각 항목의 설정을 구성한 후 저장하려면 **저장** 버튼을 클릭하세요.

조건 설정

이벤트 로그

이벤트 로그 탭에서 이벤트 종류에 따라 알림 발생 조건을 설정할 수 있습니다.



- **이벤트**: 알림을 설정할 이벤트 종류를 선택하세요. 사전 정의된 **자주 사용하는 이벤트**을 선택할 수도 있습니다.
- **출입문**: 출입문을 선택하세요. 선택한 출입문에서 이벤트가 발생할 경우 알림을 전송합니다. 1개 이상의 출입문을 선택할 수 있습니다.
- **이벤트 발생 횟수 및 지속 시간 설정**: 설정한 시간 동안 특정 빈도로 이벤트가 발생할 경우 알림을 전송합니다. 예를 들어, 5분 동안 3회 이상 이벤트가 발생할 경우 알림을 전송하도록 설정할 수 있습니다.

> **팁**
> BioStar Air 2.12 버전 이상에서는 장치의 네트워크 연결 해제 이벤트를 실시간 알림으로 설정할 수 있습니다.

시스템



시스템 탭에서 시스템 상태에 따라 알림 발생 조건을 설정할 수 있습니다.선택할 수 있는 옵션은 다음과 같습니다.

- **크레딧 부족 - 미리 알림**
- **크레딧 부족 - 사이트 정지**
- **크레딧 부족 - SMS (10개 미만)**
- **APB 배터리 부족**
- **새 펌웨어 업데이트**
- **네트워크 연결 없음 (장치 감지)**

알림 대상 설정

전송 대상에서 알림을 받을 대상을 설정할 수 있습니다. 관리자 권한별 사용자를 선택할 수 있고, 개별 사용자를 선택할 수 있습니다.

전송 방법 설정

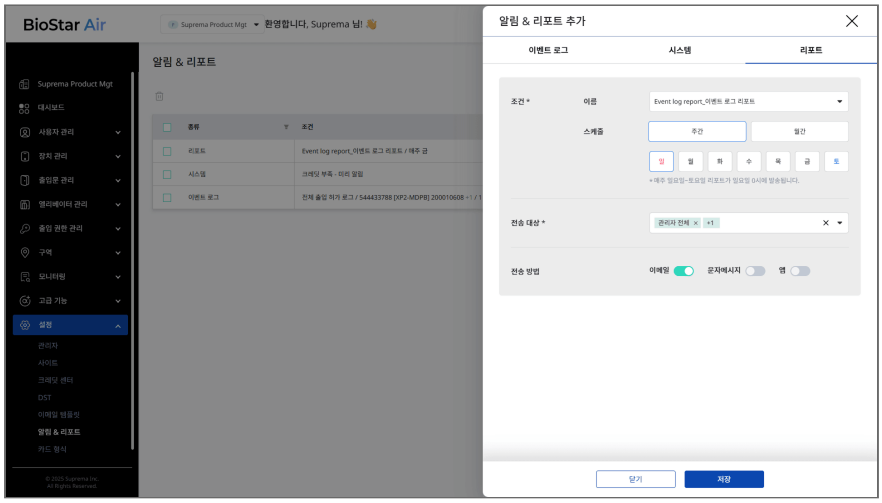
전송 방법에서 알림을 전송할 수단을 선택하세요. 이메일, 문자 메시지, 앱 푸시 알림의 방법으로 알림을 전송할 수 있습니다.

> **알아두기**
> 문자 메시지 전송은 SMS 크레딧을 충전해야 사용할 수 있습니다. 잔여 SMS 크레딧은 **설정** → **크레딧 센터**에서 확인할 수 있습니다.

리포트 생성

특정 시간 간격으로 리포트를 자동 생성하고 관리자에게 전송할 수 있습니다. 이벤트 로그 발생 현황 및 사용자 현황에 대한 리포트를 생성할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **알림 & 리포트**를 클릭하세요.
2. 화면 오른쪽 상단의 **알림 & 리포트 추가** 버튼을 클릭하세요.
3. **알림 & 리포트 추가** 패널이 나타나면 **리포트** 탭을 선택하세요.



4. 각 항목의 설정을 구성한 후 저장하려면 **저장** 버튼을 클릭하세요.

조건 설정

리포트 종류와 생성 주기를 설정하세요.

- **이름**: 생성할 리포트 종류를 선택하세요.
  - **근태 리포트**: 선택한 기간 동안의 사용자 근태 현황에 대한 리포트를 생성합니다.
  - **변경 로그 리포트**: 선택한 기간 동안의 변경 로그 현황에 대한 리포트를 생성합니다.
  - **이벤트 로그 리포트**: 선택한 기간 동안의 이벤트 로그 발생 현황에 대한 리포트를 생성합니다.
  - **사용자 리포트**: 선택한 기간 동안의 사용자 현황에 대한 리포트를 생성합니다.
- **스케줄**: 리포트 생성 주기를 선택하세요. **주간**, **월간** 중에서 선택할 수 있습니다.

알림 대상 설정

전송 대상에서 알림을 받을 대상을 설정할 수 있습니다. 관리자 권한별 사용자를 선택할 수 있고, 개별 사용자를 선택할 수 있습니다.

전송 방법 설정

전송 방법에서 알림을 전송할 수단을 선택하세요.

> **알아두기**
> 리포트는 **이메일로만 전송**할 수 있습니다. 문자 메시지 또는 앱 푸시 알림을 통해 전송할 수 없습니다.

알림 및 리포트 수정

1. 화면 왼쪽 사이드바에서 **설정** → **알림 & 리포트**를 클릭하세요.
2. 목록에서 수정하려는 알림 또는 리포트를 클릭하세요.
3. **알림 수정** 또는 **리포트 수정** 패널이 나타나면 필요한 항목을 수정하세요.
4. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

알림 및 리포트 삭제

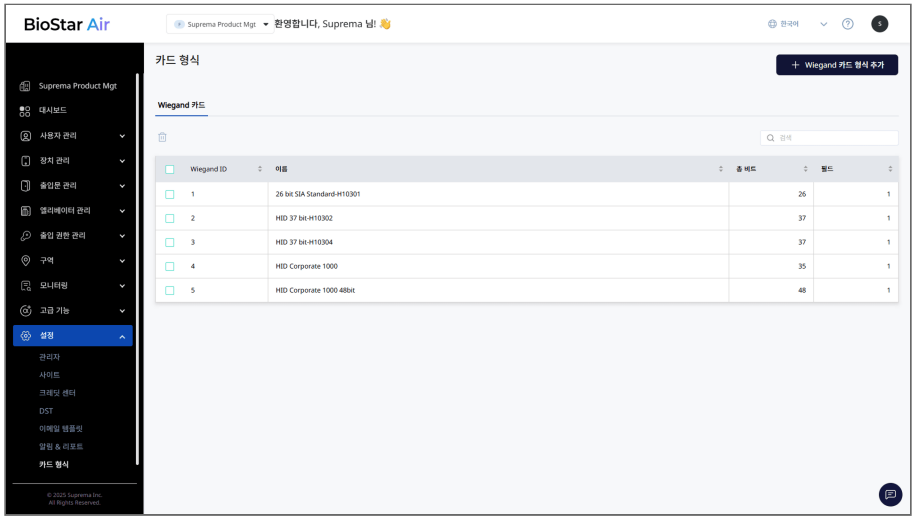
1. 화면 왼쪽 사이드바에서 **설정** → **알림 & 리포트**를 클릭하세요.
2. 목록에서 수정하려는 알림 또는 리포트의 체크박스를 클릭하세요. 한 개 이상의 항목을 선택할 수 있습니다.
3. 목록 왼쪽 상단의 버튼을 클릭하세요.
4. 메시지 창이 나타나면 **삭제** 버튼을 클릭하세요.

커스텀 Wiegand 카드 형식 구성하기

기존 출입 통제 시스템에서 원활하게 마이그레이션하기 위한 시설 코드, ID 세그먼트, 패리티 비트, 비트 할당을 비롯하여 BioStar Air v2.10에서 사용자 정의 Wiegand 카드 형식을 만들고 구성하는 방법을 안내합니다.

Wiegand 카드 형식 목록

화면 왼쪽 사이드바에서 **설정** → **카드 형식**을 클릭하세요. **Wiegand 형식** 및 **SIA, HID 형식**을 포함한, 특별한 카드 형식을 생성 및 관리, 조회할 수 있습니다. 이미 카드가 제공된 기존 출입 통제 솔루션에서 마이그레이션하는 사이트에서 유용하게 사용할 수 있습니다.

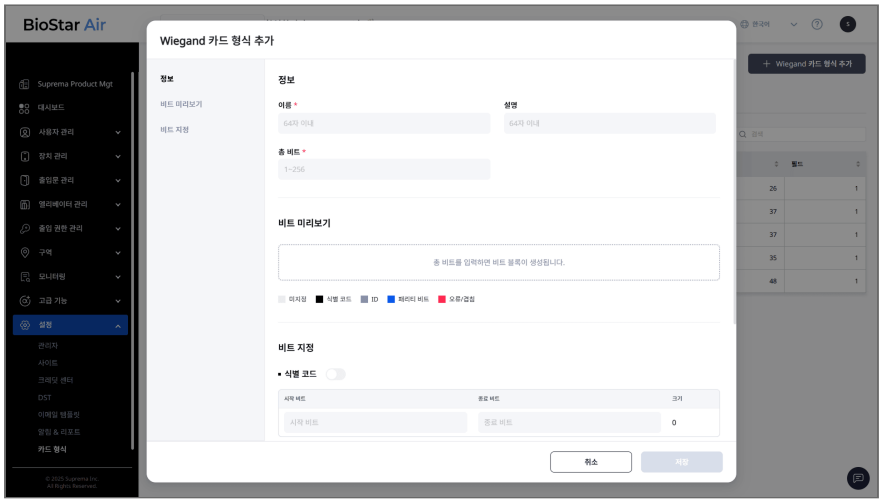


- BioStar Air에 포함된 기본 형식을 포함해 등록된 모든 Wiegand 카드 형식을 조회할 수 있습니다.
- 카드 형식의 이름, 설명, 총 비트 수, 비트 미리보기 및 세부 비트 할당을 확인할 수 있습니다.
- 이름, 설명, 총 비트 수 및 세부 비트 할당을 포함하여 새로운 사용자 정의 카드 형식을 구성할 수 있습니다. 시스템은 시각적 확인을 위한 비트 미리보기를 제공합니다.

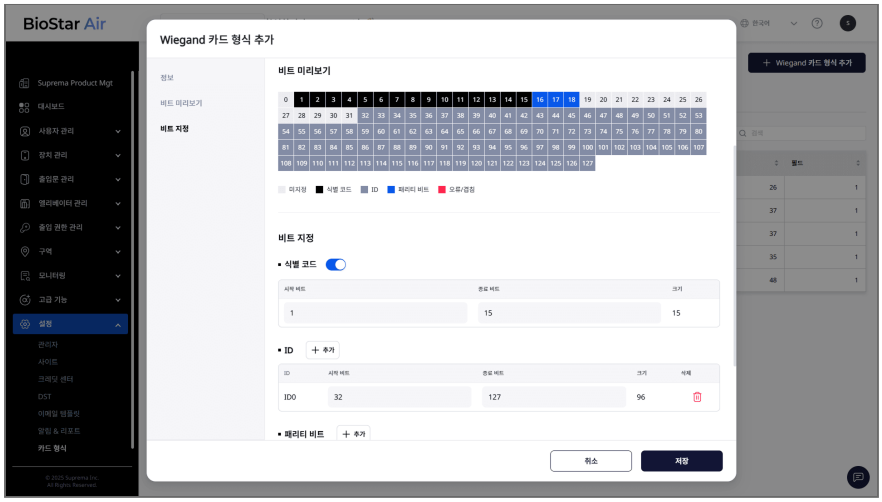
카드 형식 추가

기본 제공하는 Wiegand 카드 형식 외에 새로운 사용자 정의 Wiegand 카드 형식을 추가할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **카드 형식**을 클릭하세요.
2. 화면 오른쪽 상단의 **Wiegand 카드 형식 추가** 버튼을 클릭하세요.
3. **Wiegand 카드 형식 추가** 창이 나타나면 **정보** 섹션에서 이름 및 설명(선택 사항), 총 비트를 입력하세요.



4. 총 비트를 입력하면 **비트 미리보기**가 활성화되며, **비트 지정** 섹션에서 비트 할당을 구성하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

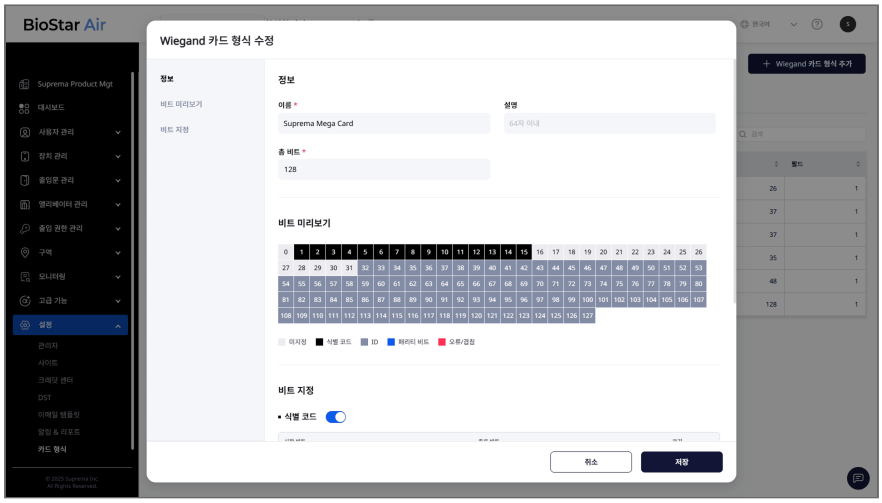
- **식별 코드**: 식별 코드 사용하려면 토글 스위치를 클릭해 활성화하세요. **시작 비트**와 **종료 비트**를 입력하세요.
- **ID**: 시작 및 종료 비트를 지정하여 하나 이상의 ID 세그먼트를 추가하세요.
- **패리티 비트**: 시작 및 종료 비트를 지정하여 홀수/짝수 패리티 비트를 추가하세요.

5. 새로운 카드 형식을 추가하려면 **저장** 버튼을 클릭하세요.

카드 형식 수정

기존 Wiegand 카드 형식을 수정하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **설정** → **카드 형식**을 클릭하세요.
2. 수정하려는 카드 형식을 클릭하세요.
3. **Wiegand 카드 형식 수정** 창이 나타나면 필요한 항목을 수정하세요.



4. 수정한 카드 형식을 저장하려면 **저장** 버튼을 클릭하세요.

카드 형식 삭제

1. 화면 왼쪽 사이드바에서 **설정** → **카드 형식**을 클릭하세요.
2. 삭제하려는 카드 형식의 체크박스를 클릭하세요. 1개 이상의 카드 형식을 선택할 수 있습니다.
3. 목록 상단의 버튼을 클릭하세요.
4. 메시지 창이 나타나면 **예** 버튼을 클릭하세요.

> **알아두기**
> 기본 제공되는 5개의 Wiegand 카드 형식은 삭제할 수 없습니다.

근태 관리(T&A) 구성하기

BioStar Air는 교대 근무 및 휴식 시간을 기록하여 기본적인 **근태 관리**(T&A) 추적 기능을 제공하며, 외부 근태 관리 시스템과 연동하거나 내보낼 수 있습니다. BioStar Air는 완전한 근태 관리 시스템을 제공하지는 않지만, 이벤트 로깅 및 급여, 근태 관리 시스템과의 API 연동을 지원합니다. 또한 기본적인 **근무 시간** 보고서도 생성할 수 있습니다.

> **팁**
> 근태 관리 구성에 대한 동영상 가이드를 시청하려면 다음 영상을 참고하세요.

근태 이벤트

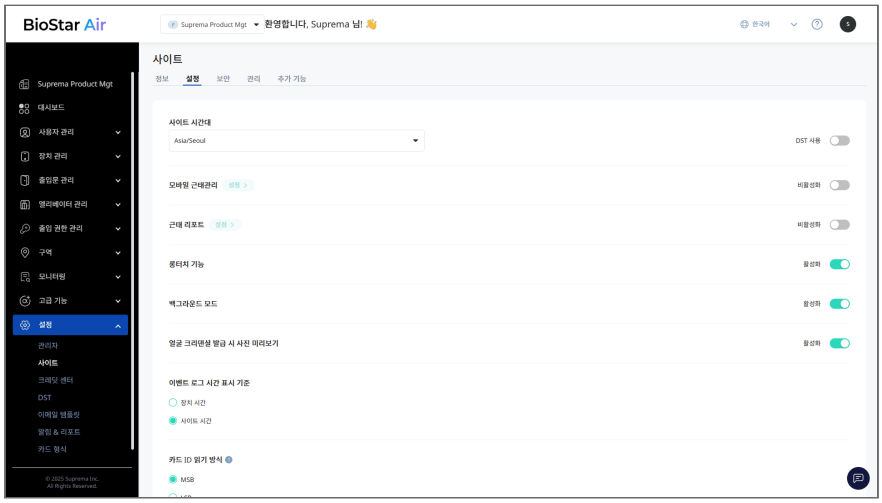
사용자는 아래와 같은 근태 이벤트를 기록할 수 있습니다. 근태 이벤트는 이벤트 로그에 기록되며 CSV 파일로 내보내거나 API를 통해 검색할 수 있습니다.

- **교대 시작**
- **교대 종료**
- **휴식 시작**
- **휴식 종료**

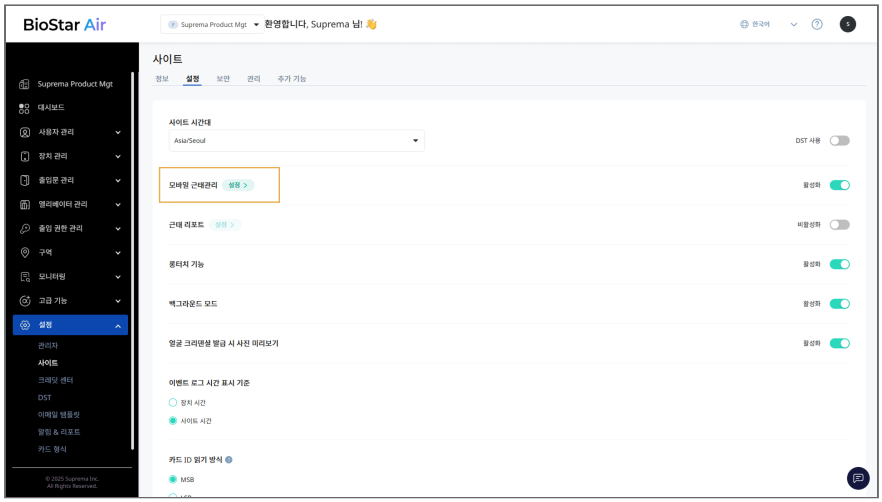
근태 관리 설정

근태 관리를 위한 설정을 활성화하고 세부 설정을 구성하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요.
2. 화면 상단의 **설정** 탭을 클릭하세요.

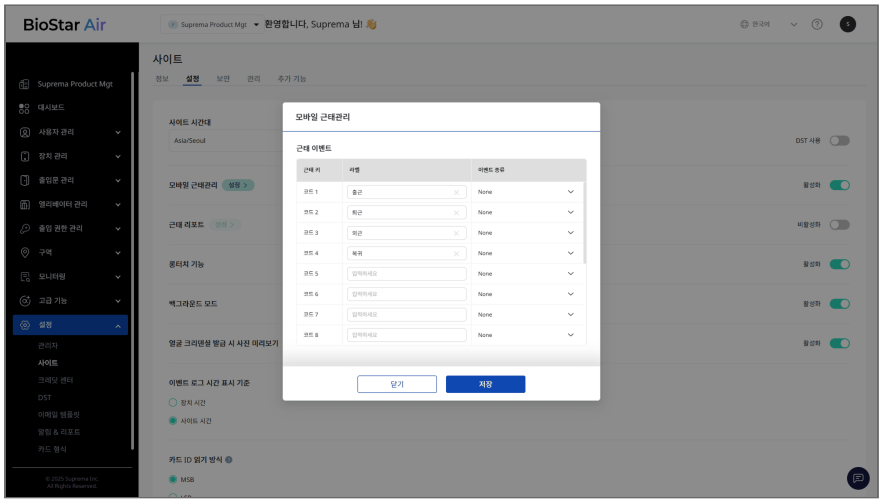


3. **모바일 근태관리** 기능을 활성화하세요.
4. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.
5. **모바일 근태관리** 기능에서 **설정** 버튼을 클릭하세요.



6. **모바일 근태관리** 창이 나타나면 **근태 키**에 대한 라벨을 설정하세요.

> *예, 교대 시작, 교대 종료, 휴식 시작, 휴식 종료*

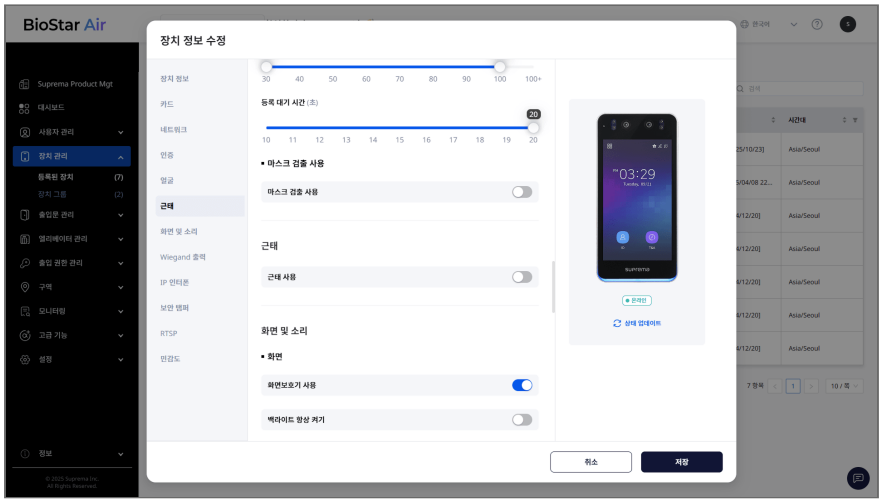


7. **근태 키**에 대한 이벤트 종류가 **Clock-In** 또는 **Clock-Out**인지 선택하세요.
8. 설정을 저장하려면 **저장** 버튼을 클릭하세요.

장치에서 근태 기능 설정

모바일 근태관리 기능을 활성화하면 이를 사용할 장치를 지정할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
2. 장치 목록에서 근태 관리 기능을 설정할 장치를 클릭하세요.
3. **장치 정보 수정** 창이 나타나면 **근태** 섹션으로 이동하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

4. **근태 사용** 옵션의 토글 버튼을 클릭해 근태 관리 기능을 활성화하세요.
5. 설정을 저장하려면 **저장** 버튼을 클릭하세요.

> - **근태 모드**를 **모바일**로 설정하면, 출입 인증 시 근태를 필수로 선택할 수 있는 **근태 필수 선택** 옵션을 사용할 수 있습니다.
> - 근태 이벤트 라벨은 **사이트** 등급에서 관리되며 장치별로 변경할 수 없습니다.

근태 모드

장치는 다양한 방법으로 근태 이벤트를 기록할 수 있습니다. **근태 모드**에서 원하는 근태 관리 모드를 선택하세요.

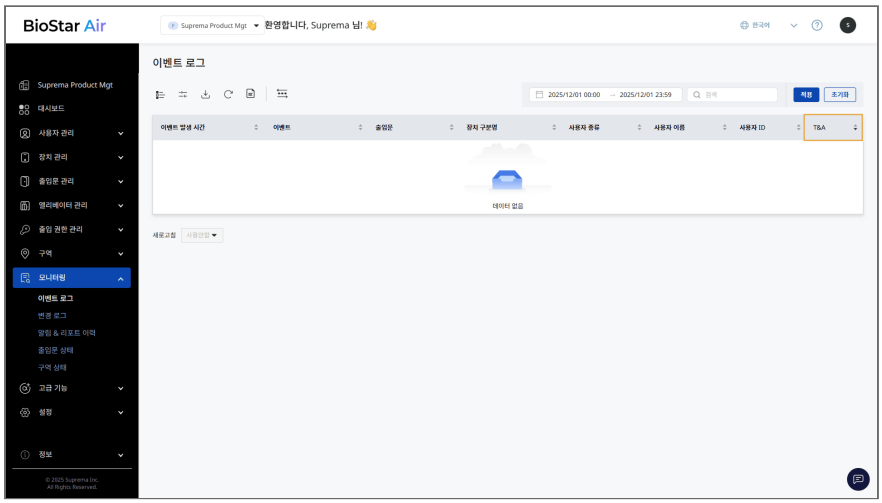
- **수동 변경**: 화면에 근태 키 표시해 인증 시, 사용자가 근태 이벤트를 선택할 수 있습니다.
- **자동 변경**: 설정된 일정에 따라 출근 및 퇴근 시간을 기록합니다. 예를 들어, 8:00 AM - 12:00 PM 사이에 기록된 이벤트는 **Clock-In**으로, 1:00 PM - 5:00 PM 사이에 기록된 이벤트는 **Clock-Out**으로 기록됩니다.
- **수동 고정**: 사용자가 마지막으로 사용한 근태 이벤트를 계속 사용할 수 있습니다.
- **고정**: 고정된 근태 코드를 장치에 할당합니다. 해당 장치에서 인증할 때마다 동일한 근태 이벤트가 기록됩니다. 이 옵션을 통해 해당 장치를 출근용 또는 퇴근용 장치로 사용할 수 있습니다.
- **모바일**: 사용자가 인증하기 전에 근태 코드를 선택해야 합니다. 선택한 근태 이벤트는 출입 로그와 함께 기록됩니다.

> **알아두기**
> 장치 모델에 따라 지원되는 근태 관리 모드가 다를 수 있습니다. 자세한 내용은 장치 및 패널 설정 옵션 안내에서 장치별 근태 모드를 참고하세요.

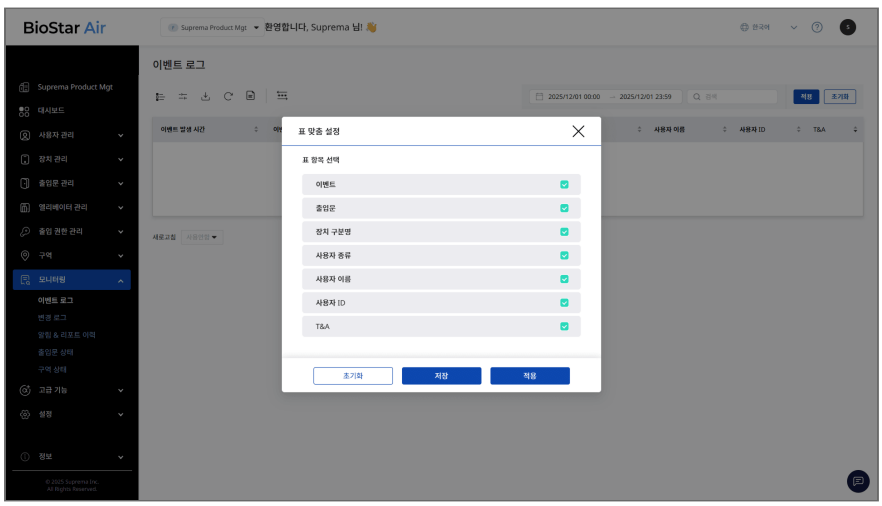
근태 로그 보기 및 내보내기

근태 이벤트는 이벤트 로그에 기록되며, 이를 검토하거나 CSV 파일로 내보낼 수 있습니다.

1. 화면 왼쪽 사이드바에서 **모니터링** → **이벤트 로그**를 클릭하세요.
2. 로그 테이블에서 **T&A** 열(column)을 찾으세요.



3. 로그 테이블 상단의 버튼을 클릭해 사용자 정의하여 **T&A** 열을 더 잘 보이도록 이동하세요.



4. 데이터를 CSV 파일로 다운로드하려면 ⬇ 버튼을 클릭하고, **CSV 다운로드**를 선택하세요.

근태 보고서 구성하기

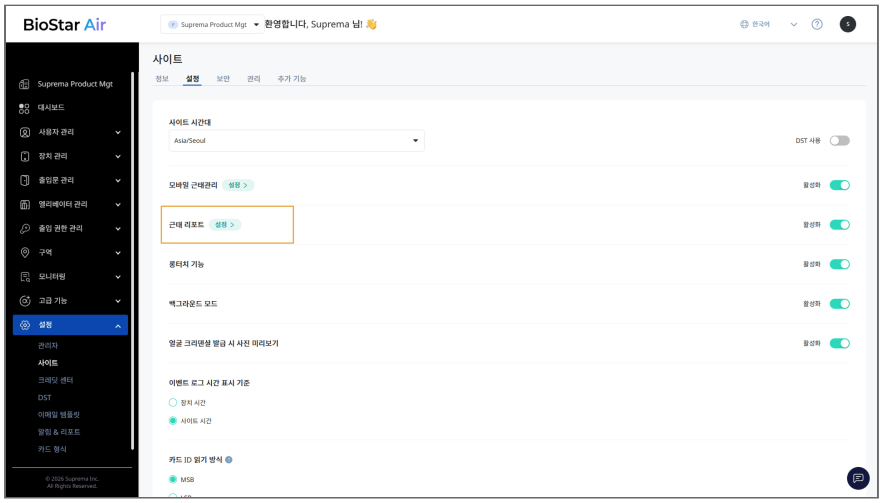
BioStar Air의 근태 보고서(T&A Report)는 간단한 **현장 근무 시간** 보고서입니다. 이벤트 로그를 기반으로 직원의 시작 및 종료 시간을 표시합니다.

이 기능은 복잡한 구성 옵션 없이 기본 보고를 위해 설계되었습니다. 근태 시스템은 지역 규정에 따라 다양한 요구 사항이 있을 수 있습니다. 기본 제공되는 근태 보고서가 조직의 요구를 충족하지 못하는 경우, 타사 T&A 솔루션을 사용하는 것을 권장합니다. 이벤트 로그는 **CSV로 내보내기**하거나 BioStar Air API를 사용하여 타사 근태 소프트웨어와 직접 통합할 수 있습니다.

> **알아두기**
>
> - 기본 제공되는 근태 보고서는 의도적으로 간단하게 설계되었으며 모든 준수 요구 사항을 충족하지 못할 수 있습니다.
> - 복잡한 근태 규칙(예, 지역 노동법, 근무 교대 패턴)이 있는 경우 타사 근태 솔루션을 사용하세요.
> - 이벤트 로그를 CSV로 내보내어 수동으로 처리하거나 API를 사용하여 다른 시스템과 자동으로 통합할 수 있습니다.

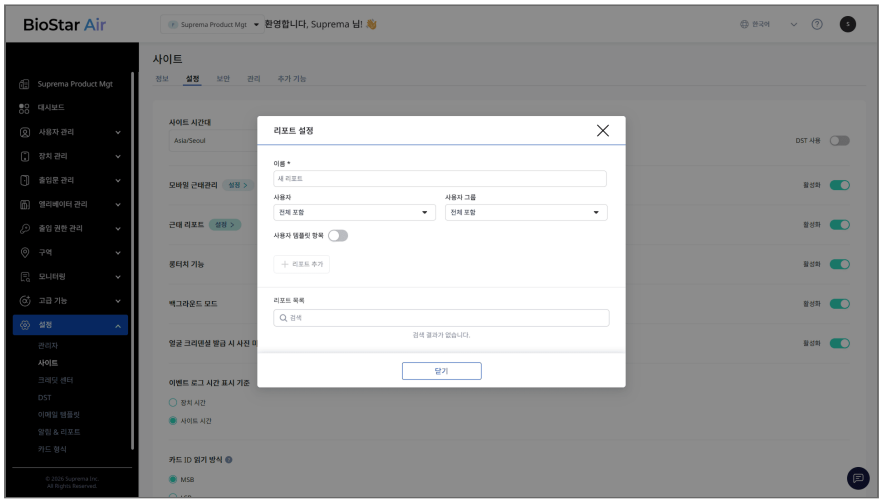
근태 보고서(T&A Report)를 생성하려면 다음 단계를 따르세요.

1. 화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요.
2. **설정** 탭에서 **근태 리포트** → **설정** 버튼을 클릭하세요.

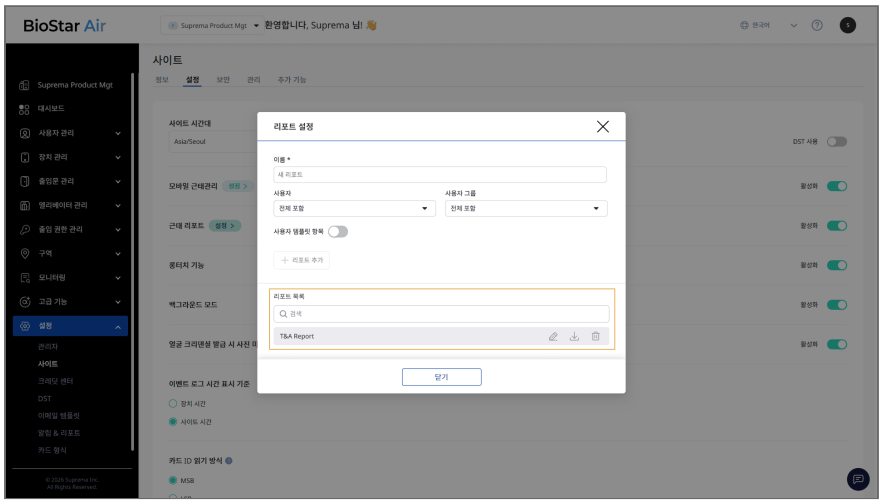


> **근태 리포트** 기능을 활성화하려면 오른쪽에 토글 스위치를 클릭하세요.

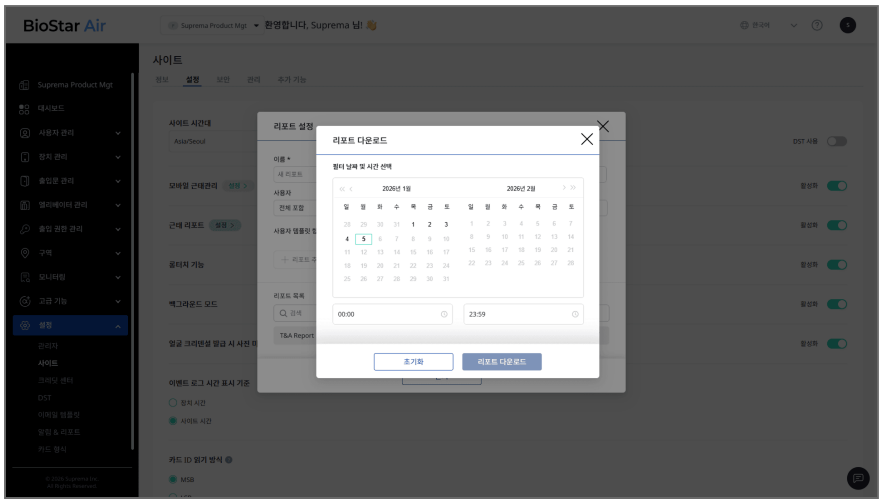
3. **리포트 설정** 창이 나타나면 보고서의 이름을 입력하세요.



4. 보고서에 포함할 사용자 또는 사용자 그룹을 선택하세요.
5. **리포트 추가** 버튼을 클릭하세요.
6. **리포트 목록**에 다운로드할 수 있는 보고서가 생성됩니다.



7. 보고서를 다운로드하려면 ⭳ 버튼을 클릭하세요.
8. **리포트 다운로드** 창이 나타나면 날짜 및 시간 범위를 선택하세요.



9. **리포트 다운로드** 버튼을 클릭하세요.

리포트 생성을 완료하며 관리자의 이메일로 다운로드 링크를 전송합니다. 이메일에서 PDF 또는 CSV 파일 형식으로 리포트를 다운로드할 수 있습니다.

알아두기

- 보고서에 사용자 템플릿을 포함하려면 **사용자 템플릿 항목**을 활성화하고, 원하는 템플릿 항목을 선택하세요.
- 리포트 다운로드 메일을 수신 후 24시간 동안 리포트를 다운로드할 수 있습니다. 기간이 만료되면 더 이상 다운로드할 수 없습니다.
- **알림 & 리포트**에서 자동화된 일정을 구성할 수도 있습니다. 자세한 내용은 알림 및 리포트 설정하기를 참고하세요.

리포트 생성 및 예약하기

BioStar Air의 리포트는 리포트 유형에 따라 다양한 화면에서 구성할 수 있습니다. 이 문서에서는 사용자, 이벤트 로그 및 변경 로그에 대한 리포트를 생성하고 예약하는 방법을 안내합니다.

리포트 구성으로 이동

리포트 유형에 따라 진입 경로가 다릅니다.

- 사용자 리포트: **사용자 관리** → **사용자**
- 이벤트 로그 리포트: **모니터링** → **이벤트 로그**
- 변경 로그 리포트: **모니터링** → **변경 로그**

위 메뉴에서 목록 상단의 도구 모음에서  버튼을 클릭하세요. 리포트 설정 화면으로 이동합니다.

사용자 리포트 구성

사이트에 등록된 사용자 현황을 파악할 수 있는 사용자 리포트를 구성할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**로 이동하세요.
2. 사용자 목록 상단의 도구 모음에서  버튼을 클릭하세요.
3. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



4. 각 필터 옵션에서 리포트에 포함할 항목을 선택하세요.
5. 생성한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
6. 하단에 **리포트 목록**이 생성되며, 관리자의 이메일로 다운로드 링크가 전송됩니다.



알아두기

- 생성한 리포트를 편집하려면 버튼을 클릭하세요.
- 리포트를 PDF 또는 CSV 파일로 내보내려면 버튼을 클릭하세요.
- 리포트를 삭제하려면 버튼을 클릭하세요.
- 사용자 관리에 대한 자세한 내용은 사용자를 참고하세요.

이벤트 로그 리포트 구성

사이트에서 발생한 이벤트 로그에 대한 리포트를 구성할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **모니터링** → **이벤트 로그**로 이동하세요.
2. 로그 목록 상단의 도구 모음에서 버튼을 클릭하세요.
3. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



4. 각 필터 옵션에서 리포트에 포함할 항목을 선택하세요.
5. 생성한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
6. 하단에 **리포트 목록**이 생성되며, 관리자의 이메일로 다운로드 링크가 전송됩니다.



알아두기

- 생성한 리포트를 편집하려면 버튼을 클릭하세요.
- 리포트를 PDF 또는 CSV 파일로 내보내려면 버튼을 클릭하세요.
- 리포트를 삭제하려면 버튼을 클릭하세요.
- 이벤트 로그에 대한 자세한 내용은 이벤트 로그 사용하기를 참고하세요.

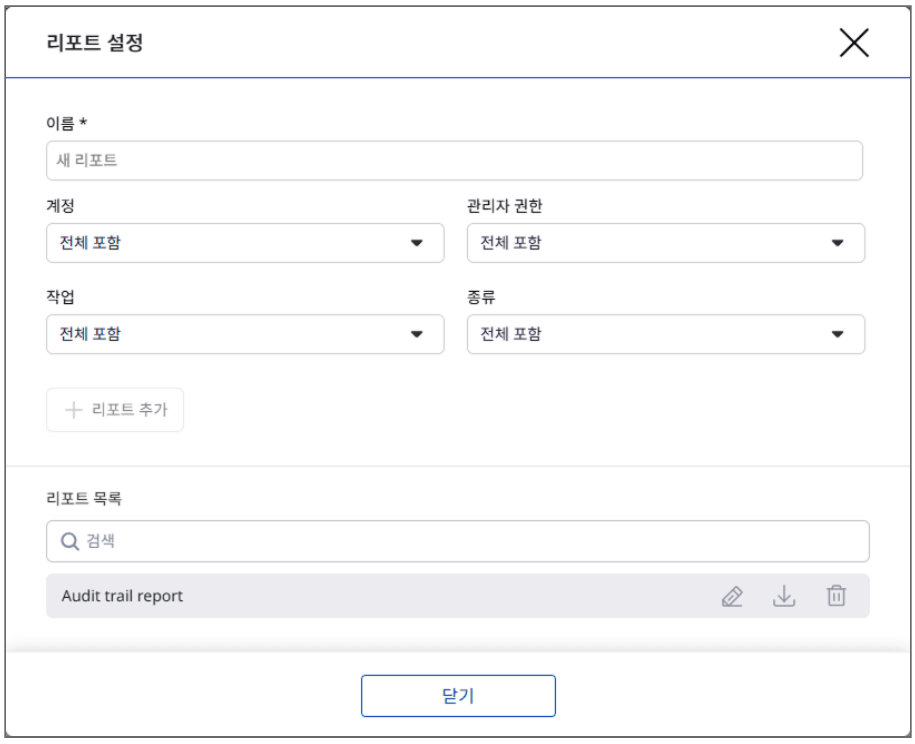
변경 로그 리포트 구성

관리자가 수행한 변경 사항에 대한 변경 로그 리포트를 구성할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **모니터링** → **변경 로그**로 이동하세요.
2. 로그 목록 상단의 도구 모음에서 버튼을 클릭하세요.
3. **리포트 설정** 창이 나타나면 리포트 이름을 입력하세요.



4. 각 필터 옵션에서 리포트에 포함할 항목을 선택하세요.
5. 생성한 리포트를 저장하려면 **리포트 추가** 버튼을 클릭하세요.
6. 하단에 **리포트 목록**이 생성되며, 관리자의 이메일로 다운로드 링크가 전송됩니다.



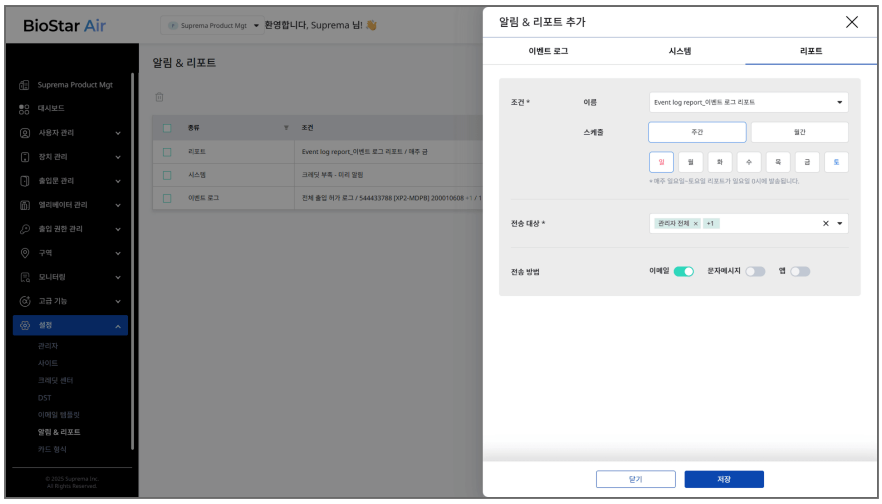
알아두기

- 생성한 리포트를 편집하려면 버튼을 클릭하세요.
- 리포트를 PDF 또는 CSV 파일로 내보내려면 버튼을 클릭하세요.
- 리포트를 삭제하려면 버튼을 클릭하세요.
- 변경 로그에 대한 자세한 내용은 변경 로그 사용하기를 참고하세요.

리포트 생성 예약

특정 시간 간격으로 리포트를 자동 생성하고 관리자에게 전송할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **설정** → **알림 & 리포트**로 이동하세요.
2. 화면 오른쪽 상단의 **알림 & 리포트 추가** 버튼을 클릭하세요.
3. **알림 & 리포트 추가** 패널이 나타나면 **리포트** 탭을 선택하세요.



4. **조건** 섹션의 **이름**에서 생성할 리포트 종류를 선택하세요.
5. **스케줄**에서 리포트 생성 주기를 선택하세요.
   - **주간** 또는 **월간** 중에서 선택하세요.
   - 리포트를 전송할 구체적인 날짜를 선택하세요.
   - 모든 리포트는 선택한 날 자정에 전송됩니다.
6. **전송 대상**에서 알림을 받을 대상을 선택하세요.
   - 특정 관리자 레벨의 모든 관리자
   - 개별 관리자
7. **전송 방법**에서 알림을 전송할 수단을 선택하세요.
   - 리포트는 이메일로만 전송할 수 있습니다.
   - 문자 메시지 또는 앱 푸시 알림을 통해 전송할 수 없습니다.
8. 각 항목의 설정을 구성한 후 저장하려면 **저장** 버튼을 클릭하세요.

알아두기

리포트 생성 예약에 대한 자세한 내용은 알림 및 리포트 설정하기를 참고하세요.

파트너 및 설치 관리자

BioStar Air 파트너 포털은 유통 계약을 체결한 부가 가치 리셀러(VAR)를 위한 전용 플랫폼입니다. 파트너 포털에서 고객 사이트를 생성하고 크레딧을 배포하거나, 페더레이션 사이트를 구성해 여러 사이트를 통합 관리할 수 있습니다.

SIP 인터폰, IP 카메라, QR 스캐너 등 현장 하드웨어 설치와 네트워크 구성 방법도 함께 안내합니다.

파트너 포털 사용하기

BioStar Air 파트너 포털은 부가 가치 리셀러(VAR)를 위한 독점 도구로, 고객 사이트를 관리하고, 크레딧을 분배하며, 관리 기능을 효율적으로 감독할 수 있습니다.

파트너 포털에 로그인하면 다음 작업을 수행할 수 있습니다.

- 고객을 위한 새로운 사이트를 생성합니다.
- 해당 사이트에 크레딧을 할당하고 분배합니다.

> **알아두기**
>
> - 파트너 포털은 부가가치 리셀러(VAR) 전용이며 사이트 관리자 또는 최종 고객용이 아닙니다.
> - 초대 이메일을 받지 못하면 스팸 폴더를 확인하거나 파트너 포털 관리자에게 문의하세요.
> - 등록에 사용된 이메일이 올바른지 확인하세요. 나중에 변경할 수 없습니다.

> **팁**
> BioStar Air 파트너 포털 사용 방법에 대한 동영상 가이드를 시청하려면 아래 영상을 참고하세요.

파트너 포털 접속

파트너 포털은 웹 포털로만 제공됩니다. 다음 링크를 통해 방문할 수 있습니다. https://partner.biostarair.com/

파트너 포털 회원 가입

1. 유통 계약을 체결하면 파트너 포털 회원 가입 초대 이메일을 받게 됩니다.
2. 이메일에서 **가입하기** 링크를 클릭하세요.
3. 개인정보 보호정책 및 이용 약관을 검토하고 동의하세요.
4. 이메일이 미리 채워진 가입 화면이 나타나면 필수 정보를 입력하세요.
5. 회원 가입 프로세스를 완료하고 포털에 로그인하세요.

알아두기

- 파트너 포털은 승인된 리셀러 전용이며 사이트 관리자 또는 최종 사용자는 액세스할 수 없습니다.
- 이메일 초대장을 받지 못한 경우 스팸 폴더를 확인하거나 파트너 포털 관리자에게 문의하세요.
- 등록에 사용된 이메일이 올바른지 확인하세요. 회원 가입 후에는 변경할 수 없습니다.

사이트 관리

파트너 포털에 로그인하면 계정과 연결된 사이트 목록을 확인할 수 있습니다.

- 사이트 이름, 국가 및 할당된 크레딧을 포함한 사이트 세부 정보를 확인하세요.
- 각 사이트의 월별 비용을 모니터링하여 추가 크레딧이 필요한 시점을 결정하세요.
- 사용자 수 및 등록된 장치 수를 추적할 수 있습니다.
- 내부 추적을 위한 메모를 추가하세요.

사이트 세부 정보 편집

사이트 목록에서 세부 정보를 편집할 사이트를 클릭하세요. 사이트 편집 화면에서 다음 작업을 수행할 수 있습니다.

- 사이트의 시간대 및 국가 정보를 포함한 세부 정보를 업데이트할 수 있습니다.
- 사이트와 관련된 메모를 추가하거나 수정할 수 있습니다.
- 할당된 크레딧 수를 조정할 수 있습니다.
- 사이트에 추가 관리자를 초대할 수 있습니다.
- 필요한 경우 사이트를 삭제할 수 있습니다.

크레딧 내역 추적

크레딧 내역 섹션에서는 모든 크레딧 변동 사항을 볼 수 있습니다.

- 특정 기간 동안의 크레딧 변동을 검토할 수 있는 시간 범위를 설정할 수 있습니다.
- 고객 사이트에 대한 최근 크레딧 추가를 모니터링할 수 있습니다.

관리자 관리

관리자 섹션에서는 다른 사용자를 파트너 포털로 초대할 수 있습니다.

1. 관리자 레벨을 선택하세요.
2. 초대할 사용자의 이메일 주소를 입력하세요.
3. 초대장을 보내려면 **확인**을 클릭하세요.

> **알아두기**
> 최종 고객은 파트너 포털에 추가되어서는 안 됩니다. 오직 부가가치 리셀러(Value-Added Reseller, VAR)만 사이트 생성 및 크레딧 분배를 관리해야 합니다.

역할 및 권한 이해

파트너 포털에는 네 가지 권한 레벨이 있습니다.

- **옵저버**: 사이트 정보를 볼 수 있지만 변경할 수 없습니다.
- **오퍼레이터**: 새 사이트를 설정하고 크레딧을 할당할 수 있지만 관리자 권한을 수정하거나 새 관리자를 초대할 수 없습니다.
- **관리자**: 다른 관리자를 초대하고 관리할 수 있지만 마스터 레벨 사용자를 제거할 수 없습니다.
- **마스터**: 포털에 대한 전체 제어 권한이 있으며, 사용자 관리, 사이트 생성 및 크레딧 분배를 포함합니다. 마스터 레벨만 파트너 포털 계정을 처음 활성화할 수 있습니다.

> **알아두기**
> 마스터 관리자가 아닌 다른 권한의 사용자가 포털에 진입하려면 먼저 마스터 계정을 설정하고 활성화해야 합니다.

페더레이션 사이트 관리하기

BioStar Air는 **페더레이션 사이트**를 생성하여 주 사이트에서 여러 하위 사이트를 원활하게 관리할 수 있는 기능을 제공합니다. 이 기능은 다중 테넌트 건물이나 여러 지점을 운영하는 조직에 적합하며, 분산형 출입 관리를 통해 중앙 집중식 제어 기능을 제공합니다.

BioStar Air의 페더레이션 사이트 기능을 활용함으로써 관리자는 복잡한 환경에 대한 출입을 효과적으로 관리하고 모든 이해 관계자에게 안전하고 확장 가능한, 간소화된 경험을 제공합니다.

페더레이션 사이트란?

페더레이션 사이트는 **기본 사이트**가 하나 이상의 **하위 사이트**를 관리하는 계층적 구조를 지원합니다. **페더레이션 관리자**라고 하는 기본 사이트의 관리자는 BioStar Air 화면을 통해 하위 사이트에 직접 액세스하고 관리할 수 있습니다.

페더레이션 사이트는 다음과 같은 상황에서 유용합니다.

멀티 테넌트 빌딩

예를 들어, 각 층에 서로 다른 회사가 입주해 있는 상업용 건물에서는 아래와 같은 구성을 할 수 있습니다.

- 건물에 대한 **마스터 계정**
- 각 임차인 회사에 대한 **하위 계정**

이 구성을 통해 특정 층에 대한 접근을 허가받은 직원만 가능하게 하여 건물 관리자의 관리를 단순화할 수 있습니다.

멀티 브랜치 조직

여러 위치에 사무실이 있는 회사는 아래와 같이 구성할 수 있습니다.

- **마스터 계정**을 통해 전역(Global) 설정 관리

- 각 지점에 대한 **하위 계정** 생성

예를 들어, 전 세계에 10개의 사무실이 있는 기업은 연합 구조를 사용하여 관리를 간소화할 수 있습니다.

페더레이션 사이트 설정

1 파트너 포털 접속

접속 URL: https://partner.biostarair.com

- BioStar Air 파트너 포털은 오직 파트너와 설치 업체만 사용할 수 있습니다.
- 최종 고객이 이 기능을 구성하려면 설치 업체에 문의하세요.

2 기본 사이트 생성

1. 파트너 포털에 로그인하세요.
2. 을 클릭하고 에서 를 선택하세요.
   - 이 단계는 사이트를 처음 설정할 때 **반드시** 수행해야 합니다.
   - 일반 사이트는 나중에 페더레이션 사이트로 변경할 수 없습니다.
3. 동일한 화면에서 페더레이션 사이트 관리자를 추가하세요.
   - 파트너 포털에서 추가한 **페더레이션 사이트 관리자**는 기본 사이트와 모든 하위 사이트에 진입할 수 있습니다.
   - BioStar Air에서 추가한 **일반 관리자**는 개별 사이트만 관리할 수 있습니다.

3 하위 사이트 추가

1. 기본 사이트가 페더레이션 사이트로 설정되면 에 하위 사이트를 생성할 수 있는 옵션이 표시됩니다.
2. 버튼을 클릭하고 다른 사이트와 마찬가지로 구성하세요.

중요 고려사항

사용자 및 장치 관리

- 사용자 및 장치는 각 하위 사이트에 별도로 추가해야 합니다.
- 장치는 한 번에 하나의 사이트에만 등록할 수 있습니다. 기본 사이트 또는 하위 사이트 중 하나를 선택하세요.

기본 사이트 사용

- 일부 고객은 기본 사이트를 하위 사이트 관리를 위한 액세스 포인트로만 사용하며, 기본 사이트에 사용자나 장치를 등록하지 않습니다.
- **예시 1**: 세 개의 지사 사무실이 있는 회사는 장치가 없는 기본 사이트를 설정하고 각 지사에 대한 하위 사이트를 생성합니다.
- **예시 2**: 본사와 세 개의 지사가 있는 회사는 본사(기본 사이트)에서 사용자와 장치를 등록하고 지사에 대한 하위 사이트를 설정합니다.

청구

- 청구는 사이트당 등록된 장치(리더기)의 수를 기준으로 계산됩니다.
- 등록된 장치가 없는 기본 사이트를 생성하는 데 추가 비용은 없습니다.

파트너 관리자 초대하기

파트너 포털에서 파트너 관리자 계정 초대 및 역할 할당, 권한 관리 방법을 안내합니다. 파트너 관리자는 고객 사이트에 대한 접근 권한을 제어하여 보안과 운영 효율성을 확보할 수 있습니다.

파트너 관리자는 옵저버(Observer), 오퍼레이터(Operator), 관리자(Administrator), 마스터(Master)의 4가지 역할 중 하나로 할당되며, 각 역할에 따라 접근 권한이 다릅니다. 이 문서에서는 각 역할의 권한 차이를 비교하고, 관리자 계정 초대부터 권한 관리, 계정 잠금/해제, 계정 삭제까지의 전체 과정을 단계별로 안내합니다.

관리자 역할 및 권한 이해

파트너 포털에서 관리자는 다음 4가지 역할 중 하나를 할당할 수 있습니다.

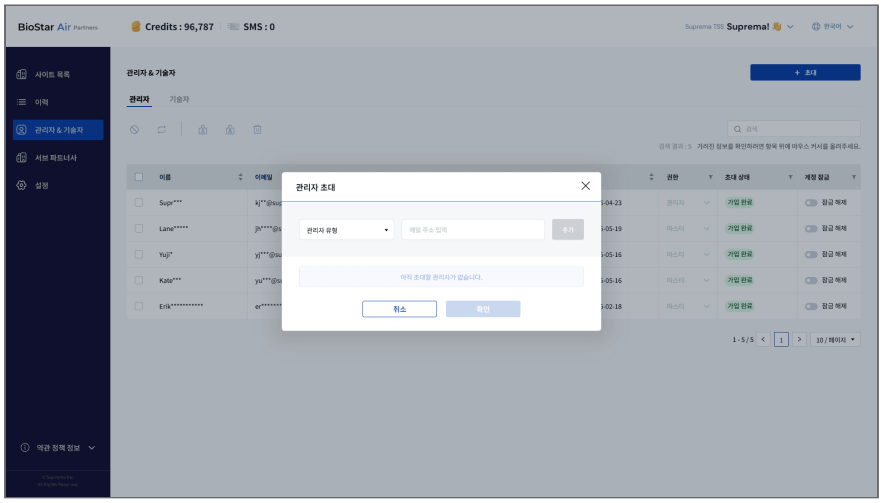
- **옵저버**: 사이트 정보를 볼 수 있지만 변경할 수 없습니다.
- **오퍼레이터**: 새 사이트를 설정하고 크레딧을 할당할 수 있지만 관리자 권한을 수정하거나 새 관리자를 초대할 수 없습니다.
- **관리자**: 다른 관리자를 초대하고 관리할 수 있지만 마스터 레벨 사용자를 제거할 수 없습니다.
- **마스터**: 포털에 대한 전체 제어 권한이 있으며, 사용자 관리, 사이트 생성 및 크레딧 분배를 포함합니다. 마스터 레벨만 파트너 포털 계정을 처음 활성화할 수 있습니다.

> **알아두기**
> 마스터 관리자가 아닌 다른 권한의 사용자가 포털에 진입하려면 먼저 마스터 계정을 설정하고 활성화해야 합니다.

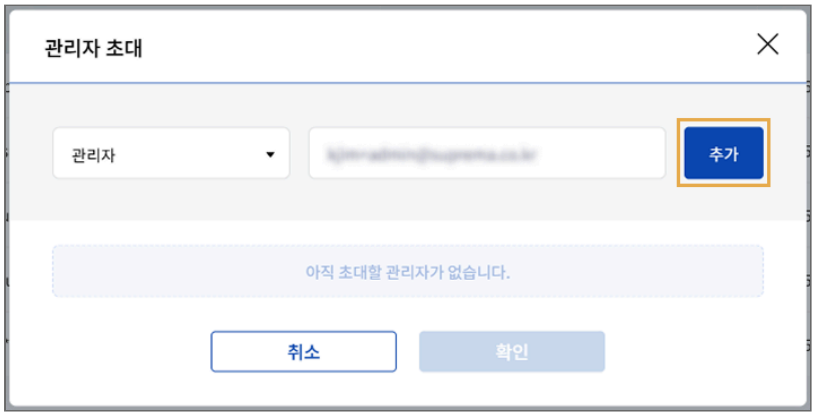
관리자 초대

관리자를 초대하려면 다음 단계를 따르세요.

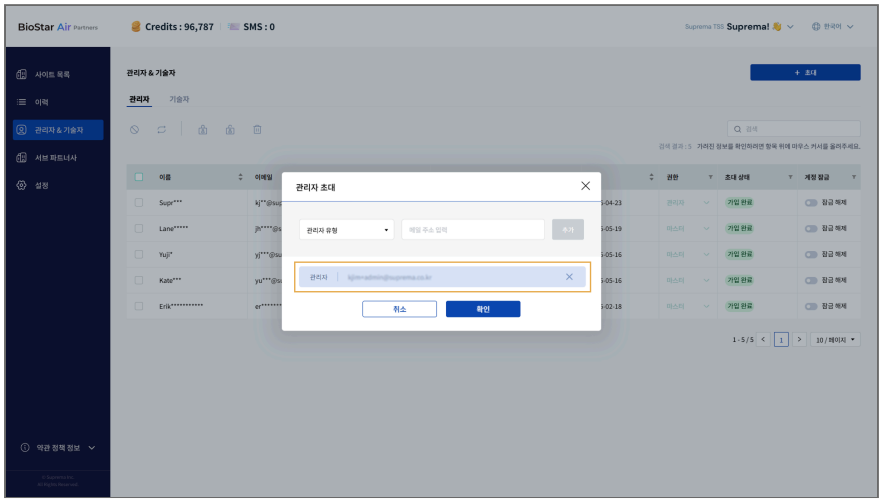
1. 파트너 포털에 **관리자** 권한 이상의 계정으로 로그인하세요.
2. 화면 왼쪽 사이드바에서 를 클릭하세요.
3. 화면 오른쪽 상단의 버튼을 클릭하세요.
4. 창이 나타나면 에서 초대할 관리자의 역할을 선택하세요.



5. 초대할 관리자의 이메일 주소를 입력하세요.
6. 버튼이 활성화되면 클릭하세요.



7. 추가된 관리자는 이메일 주소 입력란 하단에 표시됩니다. 추가로 관리자를 초대하려면 4~6단계를 반복하세요.



8. 관리자를 모두 추가했다면 **확인** 버튼을 클릭하세요.
9. 전송 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 파트너 포털에 관리자 계정을 초대했더라도 각 사이트에 대한 초대는 별도로 진행해야 합니다.

초대 상태

관리자를 초대한 후 관리자 목록에서 초대한 계정의 초대 상태를 확인할 수 있습니다.

가입 대기 상태

초대된 관리자가 이메일을 통해 초대를 수락하여 계정을 활성화하기 전까지는 상태입니다. 초대 받은 관리자는 이메일 내의 링크를 클릭하여 계정을 등록하거나 로그인하여 파트너 포털에 진입할 수 있습니다.



> **알아두기**
> 초대 받은 관리자는 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 상태로 변경됩니다. 초대장이 만료되면 해당 계정이 다시 가입할 수 있도록 초대 링크를 재전송할 수 있습니다. 초대 링크 재전송에 대한 자세한 내용은 초대 링크 재전송을 참고하세요.

가입 완료 상태

초대된 관리자가 이메일 초대를 수락하고 가입을 완료하면 초대 상태가 로 변경됩니다.



초대 취소 상태

초대된 관리자의 이메일 주소를 잘못 입력했거나 더 이상 관리자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다. 초대를 취소하면 초대 상태가 상태로 변경됩니다. 관리자 초대 취소에 대한 자세한 내용은 초대 취소를 참고하세요.

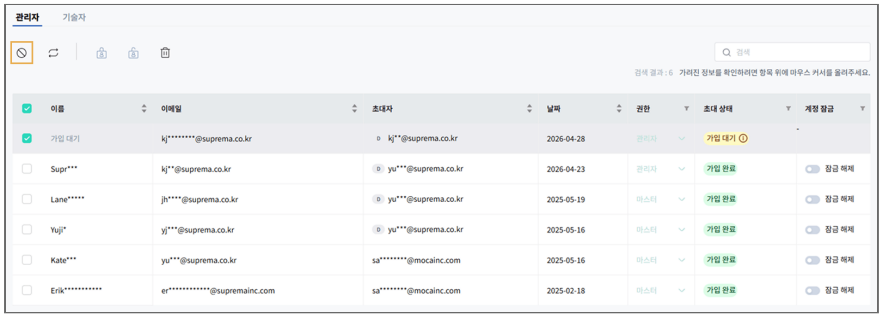


초대 취소

파트너가 초대한 관리자의 이메일 주소를 잘못 입력했거나 더 이상 관리자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다. 초대를 취소하면 해당 사용자는 초대 받은 링크로 가입할 수 없게 됩니다.

1. 관리자 목록에서 초대 상태가 상태인 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.

2. 관리자 목록 왼쪽 상단의 ⃠ 버튼을 클릭하세요.



> 상태인 관리자만 초대 취소할 수 있습니다.

3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 초대 취소 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

관리자 목록에서 초대 취소한 관리자의 초대 상태가 상태로 변경됩니다.



초대 링크 재전송

초대된 관리자가 초대 이메일을 받지 못했거나 초대 이메일을 분실했을 때, 또는 초대 링크가 만료되었을 때 초대 링크를 재전송할 수 있습니다.

1. 관리자 목록에서 초대 상태가 또는 , 상태인 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.
2. 관리자 목록 왼쪽 상단의 ↻ 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 초대 링크 재전송 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

관리자 목록에서 초대 링크를 재전송한 관리자의 초대 상태가 상태로 변경됩니다.



관리자 관리

초대된 관리자가 이메일 초대를 수락하여 가입을 완료하면, 관리자 목록에서 해당 관리자를 관리할 수 있습니다. 관리자의 계정을 잠금 또는 해제하거나 권한을 변경할 수 있습니다. 관리자가 더 이상 필요하지 않을 때는 관리자 계정을 삭제할 수도 있습니다.

관리자 계정 잠금/해제

이메일 초대를 수락하여 가입 완료한 관리자는 옵션을 통해 계정을 잠그거나 해제할 수 있습니다. 계정을 잠그면 관리자는 파트너 포털에 로그인할 수 없으며, 계정 정보는 유지되어 나중에 필요할 때 계정을 다시 활성화할 수 있습니다.

잠금 상태의 관리자는 열이 으로 표시되고, 해제된 관리자는 로 표시됩니다.



> **알아두기**
>
> - 가입 완료한 관리자의 계정은 기본적으로 잠금 해제된 상태입니다.
> - **관리자** 권한 이상의 계정은 잠그거나 해제할 수 없습니다.

개별 관리자 잠금/해제

관리자 목록에서 열의 토글 버튼을 클릭해 개별 관리자 계정을 잠그거나 해제할 수 있습니다.

1. 관리자 목록에서 열의 토글 버튼을 클릭하세요.

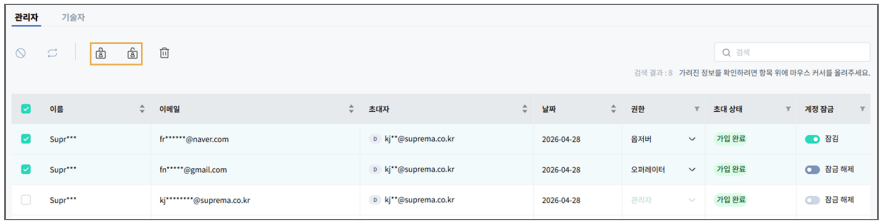


2. 팝업 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.

여러 관리자 잠금/해제

관리자 목록에서 여러 관리자 계정을 선택해 일괄적으로 잠그거나 해제할 수 있습니다.

1. 관리자 목록에서 잠그거나 해제할 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.
2. 화면 왼쪽 상단의 🔒 또는 🔓 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 계정 잠금 또는 해제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

관리자 권한 변경

관리자의 권한을 변경할 수 있습니다. 관리자 권한에 대한 자세한 내용은 관리자 역할 및 권한 이해를 참고하세요.

1. 관리자 목록에서 권한을 변경할 관리자의 열을 클릭하세요.



2. 목록에서 변경할 권한을 선택하세요.
3. 팝업 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

관리자 목록에서 해당 사용자의 권한이 변경됩니다.

관리자 계정 삭제

더 이상 관리자가 필요하지 않을 때, 관리자 계정을 삭제할 수 있습니다. 관리자 계정을 삭제하면 해당 관리자는 파트너 포털에 로그인할 수 없으며, 계정 정보가 완전히 제거되어 복구할 수 없습니다.

1. 관리자 목록에서 삭제할 관리자의 체크박스를 클릭하세요. 1명 이상의 관리자를 선택할 수 있습니다.
2. 화면 왼쪽 상단의 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.
4. 계정 삭제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

삭제한 관리자 계정은 관리자 목록에서 더 이상 표시되지 않습니다.

사이트 관리자 초대하기

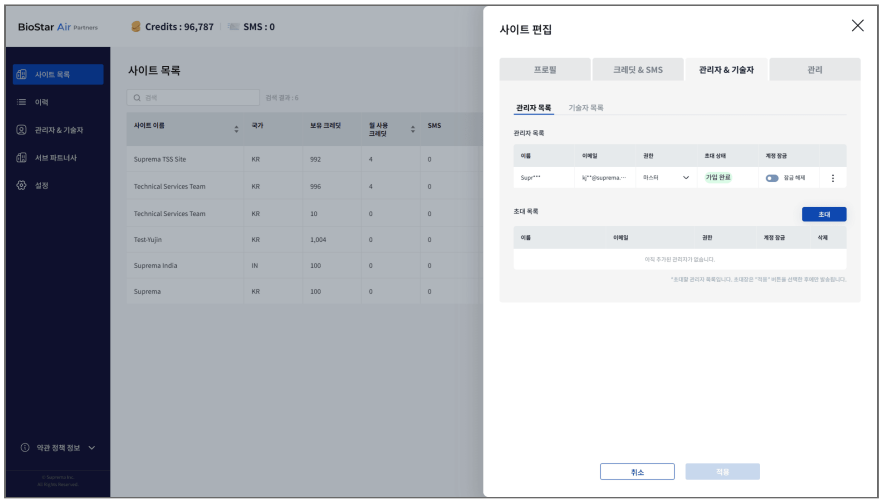
파트너는 고객 사이트에 관리자를 초대하고 권한을 설정할 수 있습니다. 각 관리자별로 필요한 접근 권한 수준을 세분화하여 관리하고, 고객 사이트의 보안과 운영 효율성을 확보할 수 있습니다.

> **알아두기**
>
> - 사이트의 관리자 권한 및 역할에 대한 자세한 내용은 관리자 계정 및 역할 관리하기를 참고하세요.
> - BioStar Air 포털에서 관리자 초대 및 역할 설정에 대한 자세한 내용은 관리자 계정 및 역할 관리하기를 참고하세요.

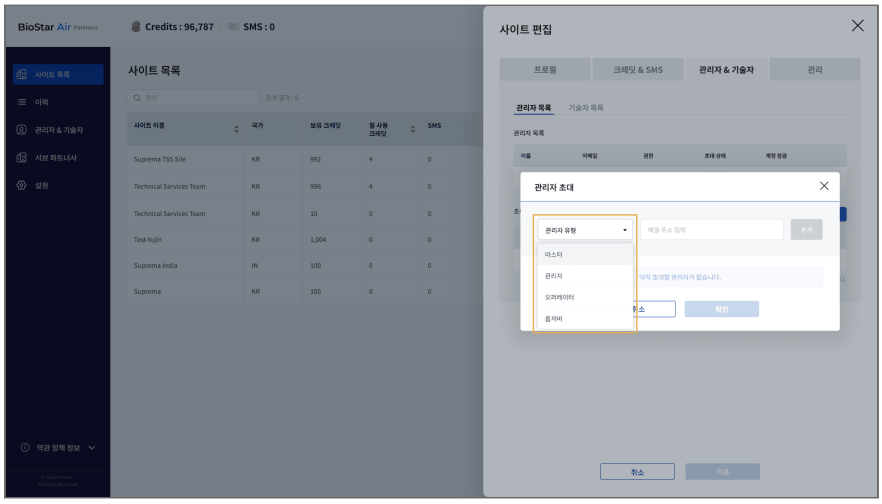
사이트에 관리자 초대

파트너 포털에서 고객 사이트에 관리자를 초대하고 권한을 설정하는 방법을 안내합니다.

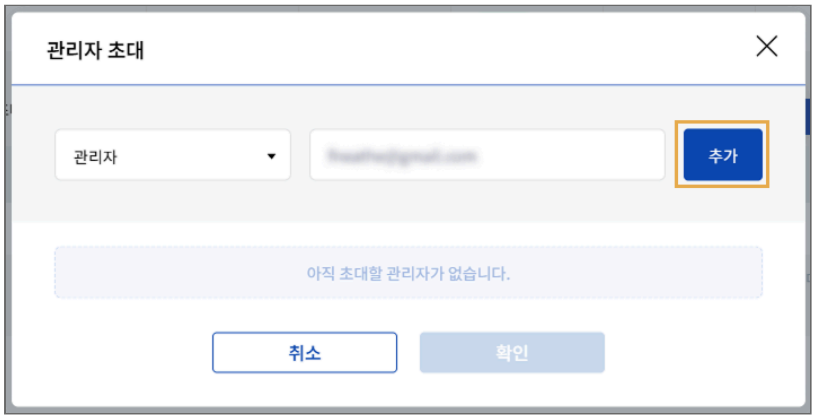
1. 파트너 포털에 **관리자** 권한 이상의 계정으로 로그인하세요.
2. 화면 왼쪽 사이드바에서 을 클릭하세요.
3. 사이트 목록에서 관리자를 배정할 사이트를 클릭하세요.
4. 패널이 나타나면 → 탭을 차례로 클릭하세요.



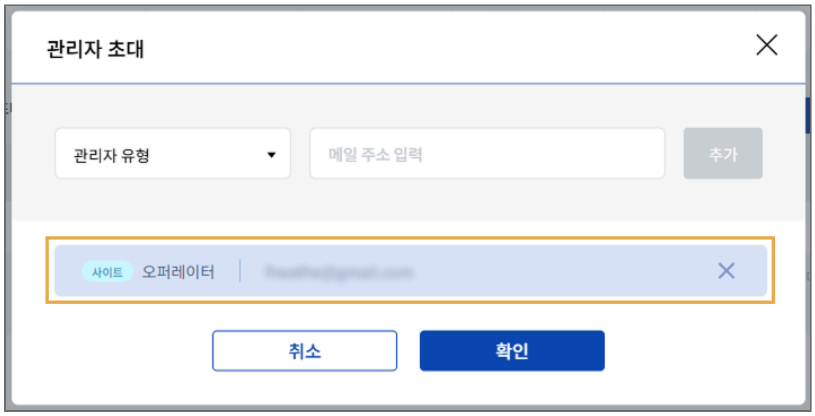
5. 버튼을 클릭하세요.
6. 창이 나타나면 에서 초대할 관리자의 역할을 선택하세요.



7. 초대할 관리자의 이메일 주소를 입력하세요.
8. 버튼이 활성화되면 클릭하세요.



9. 추가된 관리자는 이메일 주소 입력란 하단에 표시됩니다. 추가로 관리자를 초대하려면 6~8단계를 반복하세요.



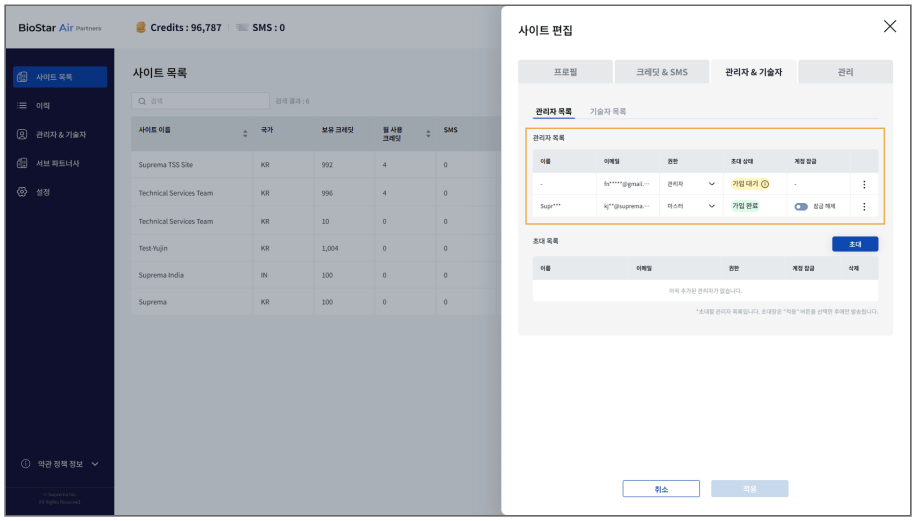
10. 관리자를 모두 추가했다면 **확인** 버튼을 클릭하세요.
11. 에서 추가한 관리자를 확인한 후 초대 메일을 전송하려면 버튼을 클릭하세요.
12. 성공 메시지가 나타나면 **확인** 버튼을 클릭하세요.

초대 상태 확인

사이트에 초대된 관리자의 초대 상태를 확인할 수 있습니다. 초대 받은 관리자가 이메일을 수락하기 전까지는 초대 상태가 로 표시됩니다. 초대 받은 관리자는 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 상태로 변경됩니다.

1. 사이트 목록에서 관리자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 초대 상태를 확인할 수 있습니다.

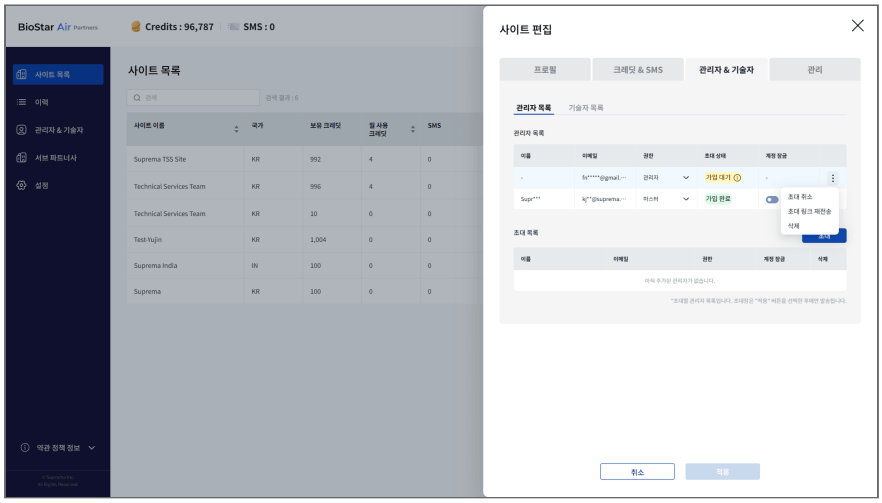
관리자가 사이트에 가입을 완료하면 상태에서 상태로 변경됩니다.



초대 취소

사이트에 초대된 관리자의 이메일 주소를 잘못 입력했거나 더 이상 관리자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다.

1. 사이트 목록에서 관리자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 상태인 관리자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



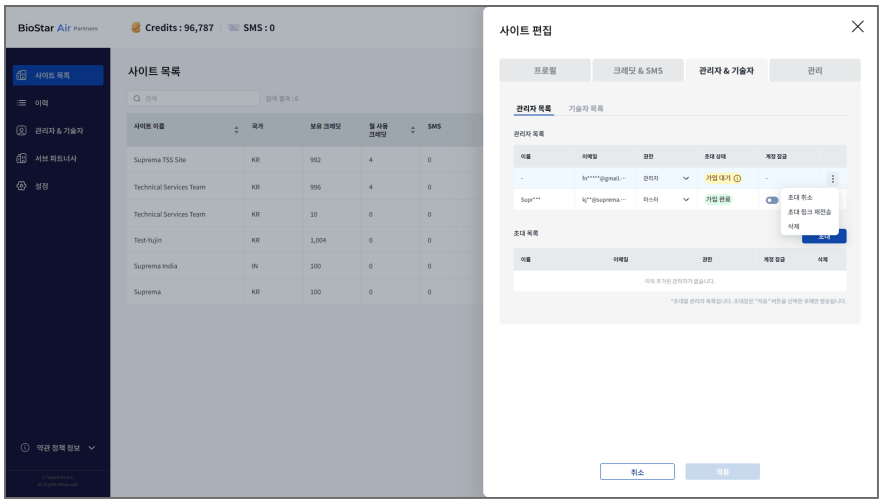
4. 팝업 메뉴에서 를 클릭하세요.
5. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
6. 초대 취소 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

초대 취소된 관리자는 초대 상태가 상태에서 상태로 변경됩니다.

초대 링크 재전송

사이트에 초대된 관리자가 초대 이메일을 받지 못했거나 분실한 경우, 초대 링크를 재전송할 수 있습니다.

1. 사이트 목록에서 관리자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 또는 , 상태인 관리자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.

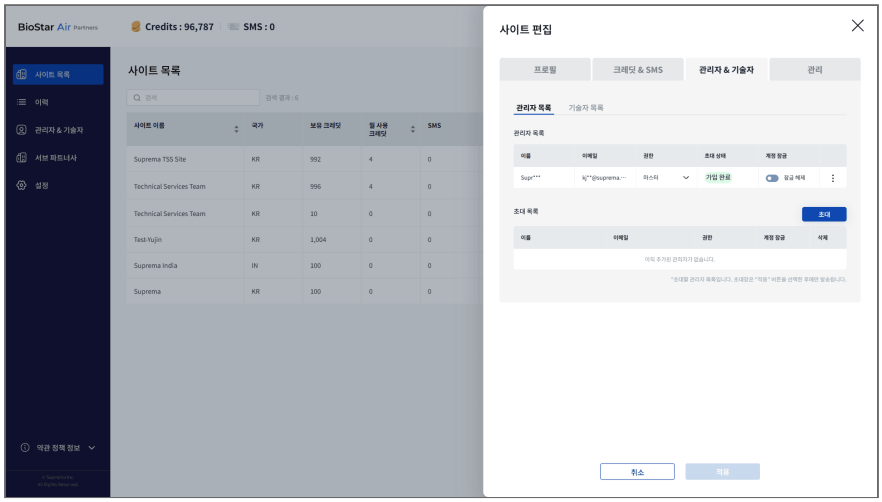


4. 팝업 메뉴에서 을 클릭하세요.
5. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
6. 초대 링크 재전송 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

관리자 계정 잠금/해제

사이트에 배정된 관리자의 계정을 잠그거나 해제할 수 있습니다.

1. 화면 왼쪽 사이드바에서 을 클릭하세요.
2. 사이트 목록에서 관리자의 접근을 관리할 사이트를 클릭하세요.
3. 패널이 나타나면 → 탭을 차례로 클릭하세요.

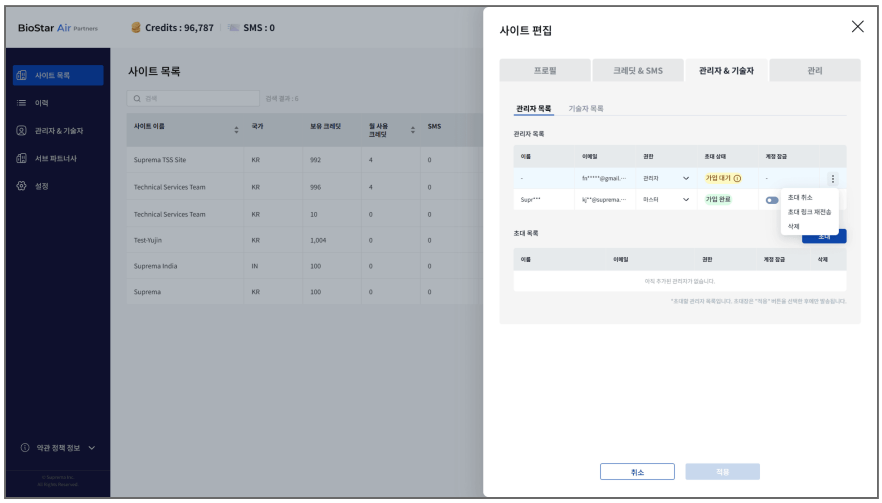


4. 에서 관리자 계정을 잠그거나 해제하려면 열에서 토글 버튼을 클릭하세요.
5. 수정한 내용을 적용하려면 하단의 버튼을 클릭하세요.

관리자 삭제

사이트에 초대된 관리자의 계정을 삭제할 수 있습니다. 관리자의 계정이 삭제되면 해당 관리자는 사이트에 로그인할 수 없으며, 사이트 접근 권한이 완전히 제거됩니다. 관리자 계정이 삭제되면 복구할 수 없습니다.

1. 사이트 목록에서 관리자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 삭제할 관리자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



4. 팝업 메뉴에서 **삭제**를 클릭하세요.

5. 팝업 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.
6. 관리자 삭제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

파트너 기술자 관리하기

기술자 계정을 사용하면 파트너와 설치 담당자가 관리자 계정을 공유하지 않고도 고객 사이트를 지원할 수 있습니다. 파트너는 파트너 포털에서 기술자를 초대하고 특정 사이트에 배정합니다. 배정 후 고객 및 사이트 관리자는 BioStar Air 관리자 포털에서 기술자의 사이트 권한을 활성화하거나 업데이트할 수 있습니다. 이를 통해 파트너의 지원 접근을 통제하고, 감사 추적을 구현하며, 필요한 사이트로만 제한할 수 있습니다.

기술자 관리의 장점

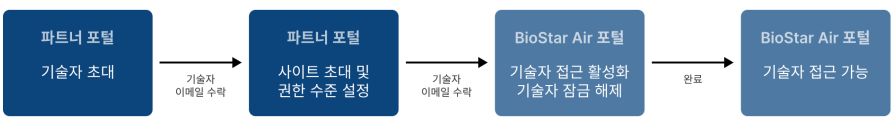
기술자 계정은 여러 고객 사이트에 걸쳐 시스템 설치, 유지보수, 기술 지원을 제공하는 전문가들을 위해 설계되었습니다. 파트너는 각 기술자의 역할과 권한 수준을 정의하여 다음을 구현할 수 있습니다.

- **보안 강화**: 공유 관리자 계정 제거로 부정 접근 위험 감소
- **규정 준수**: 개인정보 보호 규정 준수, 사용자 데이터 접근 제외 옵션
- **효율적인 관리**: 여러 사이트에서 개별 기술자 활동 추적 및 감사
- **유연한 권한 제어**: 기술자별, 사이트별 세분화된 권한 설정

제한 사항

- **파트너 포털과 BioStar Air 포털의 별도 계정 필요**: 각 포털마다 별도의 가입 절차가 필요합니다. 비밀번호는 각 포털 간 동기화되지 않습니다.
- **만료 또는 시간 기반 접근 제어 없음**: 기술자 접근은 자동으로 만료되지 않습니다. 사이트 관리자가 수동으로 잠김 처리하거나 제거해야 합니다.
- **접근 권한 고정**: 4가지 사전 정의된 권한 수준만 제공합니다. 사용자 정의 역할이나 세분화된 권한을 생성할 수 없습니다.
  - **없음** / **장치 관리** / **사용자 제외 전체 권한** / **사용자 포함 전체 권한**
- **기술자 배정 시 고객 활성화 필요**: 파트너가 배정한 기술자는 사이트 관리자가 잠금 해제해야 접근할 수 있습니다. 명확하게 전달되지 않으면 지원 또는 설치가 지연될 수 있습니다.
- **일괄 배정 없음**: 기술자는 사이트별로 개별 배정해야 합니다.
- **기술자와 관리자 역할은 동일 이메일 공유 불가**: 파트너 포털에서 이미 기술자로 등록된 이메일은 관리자로 초대할 수 없습니다. 역할 변경 시 기존 계정을 삭제한 후 새 역할로 다시 초대해야 합니다.

전체 프로세스



파트너 포털에 기술자 초대하기

기술자 계정을 통해 공유 관리자 계정 없이 파트너와 설치 업체에 제한된 사이트 접근 권한을 부여할 수 있습니다. 기술자는 파트너 포털에서 중앙 집중식으로 관리되며, 각 사이트별로 개별 할당할 수 있습니다.

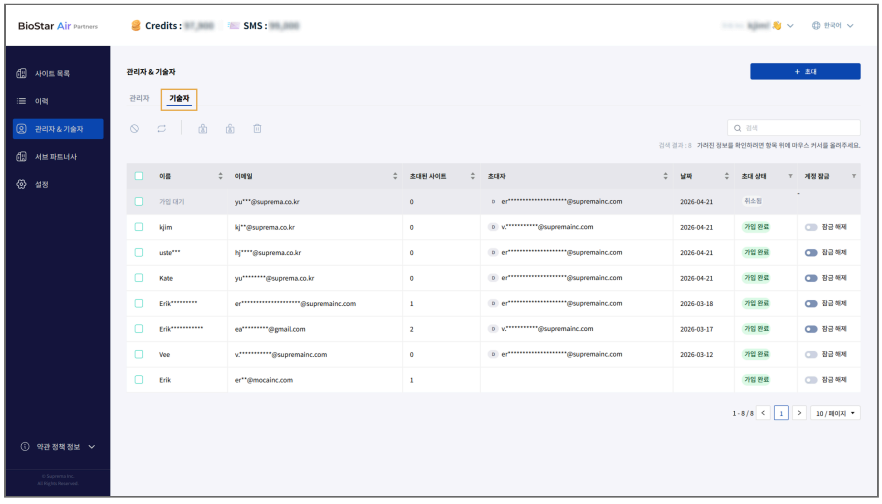
기술자 계정 사용의 주요 이점

- **보안 강화**: 공유 관리자 계정 제거로 부정 접근 위험 감소
- **규정 준수**: 개인정보 보호 규정(GDPR 등) 준수 가능, 사용자 데이터 접근 제외 옵션 제공
- **접근 제어**: 기기 접근부터 완전한 관리자 권한까지 세분화된 권한 설정 가능
- **감사 추적성**: 감사 로그에 개별 기술자 활동 기록으로 책임 추적 가능
- **효율성 증대**: 로그인 충돌 없이 여러 사이트에서 기술자 배정 및 관리 가능
- **빠른 해제**: 기술자 접근 권한을 언제든 즉시 취소 가능

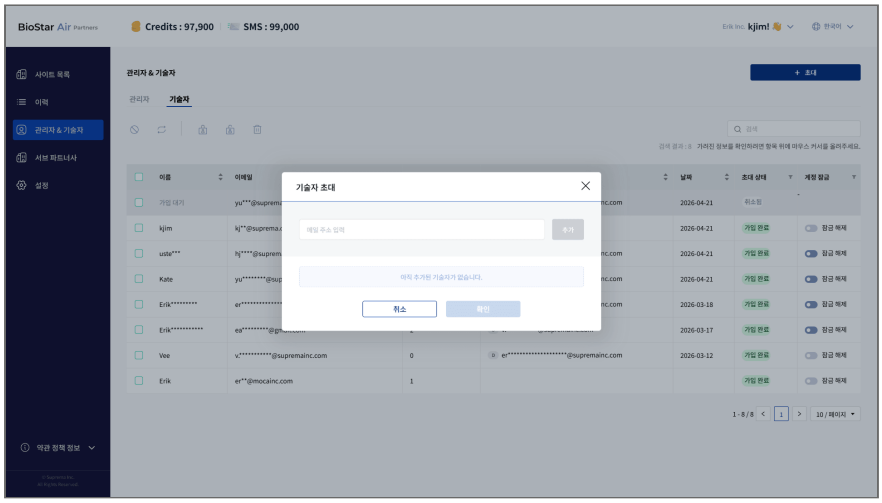
기술자 초대

사이트에 대한 접근 권한을 부여하기 전에 파트너는 기술자를 초대하여 기술자 계정을 생성해야 합니다. 기술자 계정은 이메일 주소를 기반으로 생성되며, 초대된 기술자는 이메일을 통해 초대를 수락하여 계정을 활성화할 수 있습니다.

1. 파트너 포털에 로그인하세요.
2. 화면 왼쪽 사이드바에서 를 클릭하세요.
3. 탭을 클릭하세요.

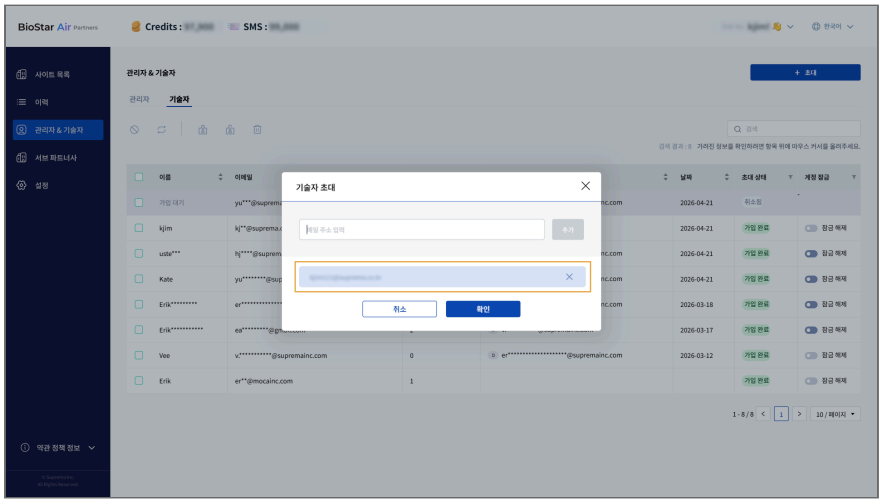


4. 화면 오른쪽 상단의 버튼을 클릭하세요.
5. 창이 나타나면 초대할 기술자의 이메일 주소를 입력하세요.



6. 버튼이 활성화되면 클릭하세요.

7. 추가된 기술자는 메일 주소 입력란 하단에 표시됩니다. 기술자를 추가로 초대하려면 5~6단계를 반복하세요.



8. 기술자를 모두 추가했다면 **확인** 버튼을 클릭하세요.

9. 전송 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 파트너 포털에 기술자 계정을 초대했더라도 각 사이트에 대한 초대는 별도로 진행해야 합니다. 사이트에 기술자를 초대하는 방법에 대한 자세한 내용은 사이트에 기술자 배정하기를 참고하세요.
> - 초대 이메일을 통해 가입한 기술자는 파트너 포털에 로그인할 수 있지만, 모든 메뉴에 대한 접근을 제한합니다. 기술자 본인 계정의 비밀번호 변경 및 계정 삭제, 언어 설정만 사용할 수 있습니다.

초대 상태

파트너는 기술자를 초대한 후 기술자 목록에서 기술자의 초대 상태를 확인할 수 있습니다.

가입 대기 상태

초대 받은 기술자가 이메일을 수락하기 전까지는 초대 상태가 로 표시됩니다. 초대 받은 기술자는 이메일 내의 링크를 클릭하여 계정을 등록하거나 로그인하여 파트너 포털에 진입할 수 있습니다.



> **알아두기**
>
> 초대 받은 기술자는 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 상태로 변경됩니다. 초대장이 만료되면 기술자가 다시 가입할 수 있도록 초대 링크를 재전송할 수 있습니다. 초대 링크 재전송에 대한 자세한 내용은 초대 링크 재전송을 참고하세요.

가입 완료 상태

기술자가 이메일 초대를 수락하고 가입을 완료하면 초대 상태가 로 변경됩니다.



초대 취소 상태

초대된 기술자의 이메일 주소를 잘못 입력했거나 문제가 해결되어 더 이상 기술자 초대가 필요하지 않을 때, 파트너는 기술자 초대를 취소할 수 있습니다. 초대 상태가 상태로 변경됩니다. 기술자 초대 취소에 대한 자세한 내용은 초대 취소를 참고하세요.



초대 취소

파트너가 초대한 기술자의 이메일 주소를 잘못 입력했거나 문제가 해결되어 더 이상 기술자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다. 초대를 취소하면 해당 사용자는 초대 받은 링크로 가입할 수 없게 됩니다.

1. 기술자 목록에서 초대 상태가 상태인 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
2. 기술자 목록 왼쪽 상단의 ⃠ 버튼을 클릭하세요.



> 상태인 기술자만 초대 취소할 수 있습니다.

3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 초대 취소 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

기술자 목록에서 초대 취소한 기술자의 초대 상태가 상태로 변경됩니다.



초대 링크 재전송

초대된 기술자가 초대 이메일을 받지 못했거나 초대 이메일을 분실했을 때, 또는 초대 링크가 만료되었을 때 초대 링크를 재전송할 수 있습니다.

1. 기술자 목록에서 초대 상태가 또는 , 상태인 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
2. 기술자 목록 왼쪽 상단의 ↻ 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 초대 링크 재전송 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

기술자 목록에서 초대 링크를 재전송한 기술자의 초대 상태가 상태로 변경됩니다.



기술자 관리

초대된 기술자가 이메일 초대를 수락하여 가입을 완료한 후, 파트너는 기술자 목록에서 다음 항목을 관리할 수 있습니다.

- 기술자 계정 잠금 또는 해제
- 사이트에 대한 접근 권한 수정
- 필요하지 않은 기술자 계정 삭제

기술자 계정 잠금/해제

파트너는 옵션을 통해 기술자 계정을 잠그거나 해제할 수 있습니다. 계정을 잠그면 기술자는 파트너 포털 및 배정받은 사이트에 로그인할 수 없습니다. 계정 정보는 유지되므로 필요할 때 계정을 다시 활성화할 수 있습니다.

잠금 상태의 기술자는 열이 으로 표시되고, 해제된 기술자는 로 표시됩니다.



> **알아두기**
>
> - 가입 완료한 기술자의 계정은 기본적으로 잠금 해제된 상태입니다.
> - 파트너 포털 관리자 계정이 일부 사이트에서 기술자 접근 권한을 가지고 있더라도 기술자 목록 표시될 수 있지만, 해당 관리자 계정은 기술자 목록에서 잠그거나 해제할 수 없습니다.

개별 기술자 잠금/해제

기술자 목록에서 열의 토글 버튼을 클릭해 개별 기술자 계정을 잠그거나 해제할 수 있습니다.

1. 기술자 목록에서 열의 토글 버튼을 클릭하세요.



2. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
3. 계정 잠금 또는 해제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

여러 기술자 잠금/해제

기술자 목록에서 여러 기술자 계정을 선택해 일괄적으로 잠그거나 해제할 수 있습니다.

1. 기술자 목록에서 잠그거나 해제할 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
2. 화면 왼쪽 상단의 🔒 또는 🔓 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
4. 계정 잠금 또는 해제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

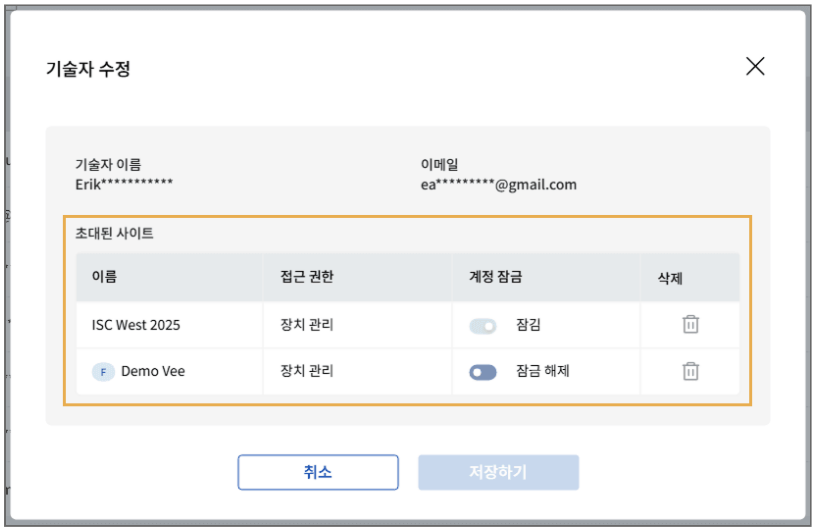
사이트 접근 권한 수정

기술자의 사이트 접근 권한을 수정할 수 있습니다.

1. 기술자 목록의 열에서 1개 이상인 기술자를 클릭하세요.



2. 창이 나타나면 에서 기술자가 초대된 사이트 목록을 확인하세요.



3. 열의 토글 버튼을 클릭해 사이트 접근을 허용하거나 차단하세요.
4. 수정 사항을 저장하려면 버튼을 클릭하세요.
5. 사이트 접근 권한 수정 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

> **알아두기**
>
> - 파트너 포털에서 기술자를 사이트에 배정하면서 접근 권한을 설정한 후에는 BioStar Air 관리자 포털의 관리자 계정으로만 접근 권한을 변경할 수 있습니다.
> - BioStar Air 관리자 포털에서 사이트 관리자가 기술자의 사이트 접근을 잠근 경우, 파트너 포털에서 잠금 해제할 수 없습니다. 사이트에 대한 기술자 접근 권한을 수정하려면 BioStar Air 관리자 포털에서 해당 사이트의 관리자 권한을 가진 계정으로 수정할 수 있습니다.
> - 기술자에게 사이트 접근 권한을 부여하는 방법에 대한 자세한 내용은 사이트에 기술자 배정하기를 참고하세요.

기술자 계정 삭제

더 이상 기술자의 지원이 필요하지 않을 때, 기술자 계정을 삭제할 수 있습니다. 기술자 계정을 삭제하면 해당 기술자는 파트너 포털에 로그인할 수 없으며, 기술자 계정과 관련된 모든 정보가 시스템에서 완전히 제거됩니다.

1. 기술자 목록에서 삭제할 기술자의 체크박스를 클릭하세요. 1명 이상의 기술자를 선택할 수 있습니다.
2. 화면 왼쪽 상단의 버튼을 클릭하세요.



3. 팝업 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.
4. 계정 삭제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

삭제한 기술자 계정은 기술자 목록에서 더 이상 표시되지 않습니다.

사이트에 기술자 배정하기

파트너는 고객 사이트에 기술자를 배정하고 권한을 설정할 수 있습니다. 각 기술자별로 필요한 접근 권한 수준을 세분화하여 관리하고, 민감한 개인 정보를 보호할 수 있습니다.

사이트별 기술자 배정의 주요 기능

- **세분화된 권한 설정**: 기기 접근부터 완전한 관리자 권한까지 유연하게 설정 가능
- **사용자 데이터 보호**: 사용자 데이터 접근 제외 옵션으로 개인정보 규정 준수
- **효율적인 관리**: 파트너가 정의한 권한 수준에 따라 사이트별 기술자 관리

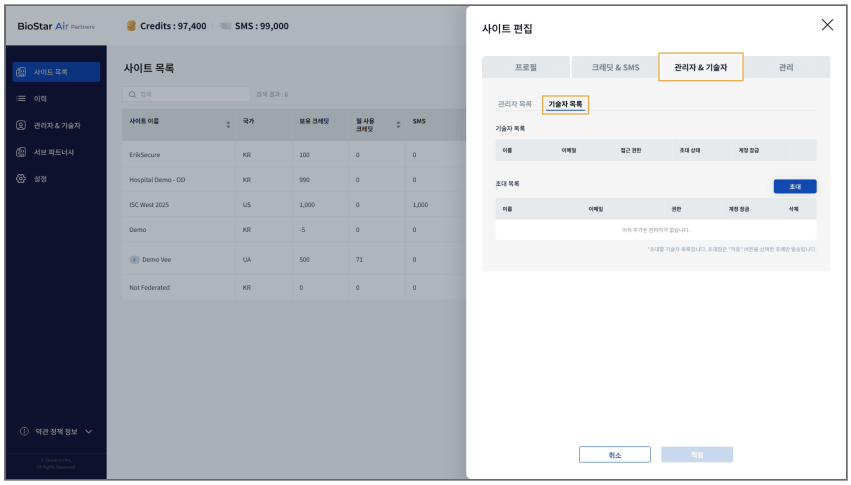
> **알아두기**
>
> - 사이트에 기술자를 초대하기 전에 파트너 포털에서 먼저 기술자 계정을 초대해야 합니다. 자세한 내용은 파트너 포털에 기술자 초대하기를 참고하세요.
> - BioStar Air 관리자 포털에서 기술자를 사이트에 배정하는 방법에 대한 자세한 내용은 기술자 계정 관리하기를 참고하세요.

사이트에 기술자 배정

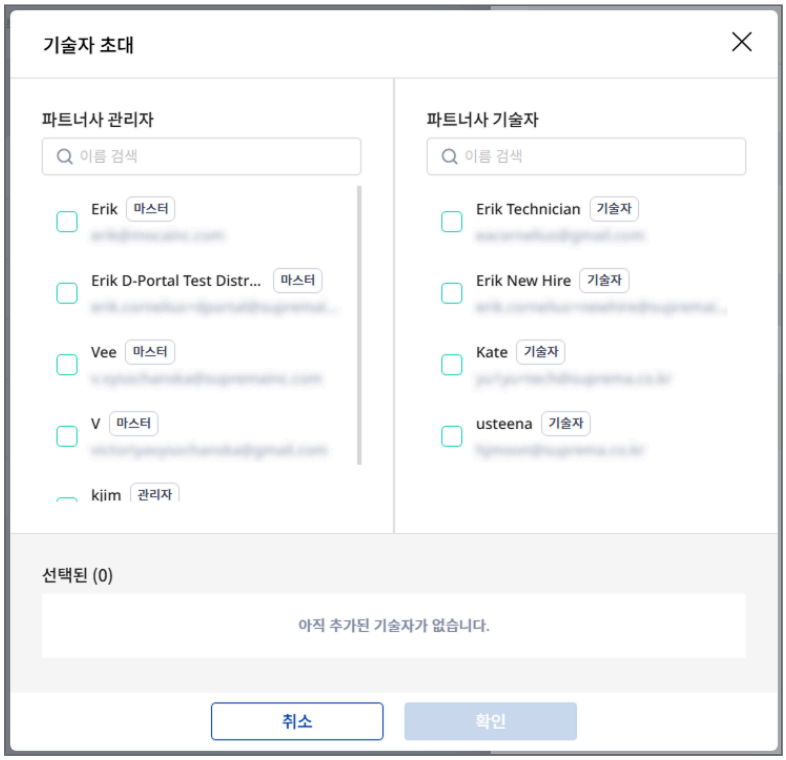
파트너 포털에서 기술자를 초대했다면, 다음 단계로 개별 사이트에 기술자를 배정해야 기술자가 해당 사이트에 접근할 수 있습니다. 사이트에 기술자를 배정하려면 다음 안내를 따르세요.

1 사이트 목록으로 이동

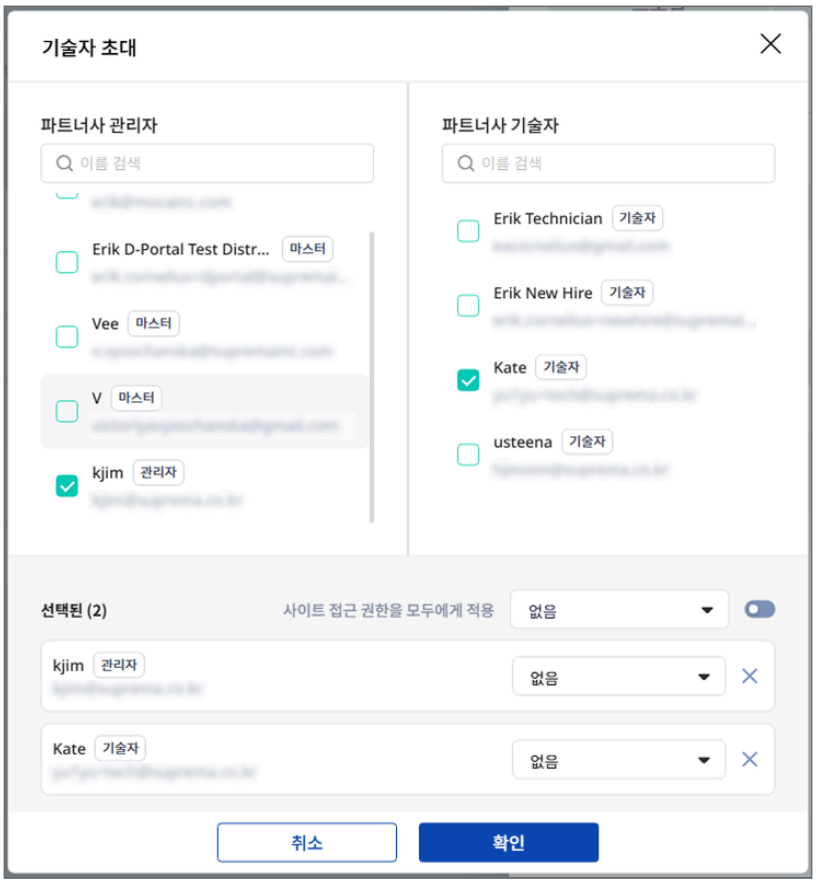
1. 파트너 포털에 로그인하세요.
2. 화면 왼쪽 사이드바에서 을 클릭하세요.
3. 사이트 목록에서 기술자를 배정할 사이트를 클릭하세요.
4. 패널이 나타나면 → 탭을 차례로 클릭하세요.



5. 버튼을 클릭하세요.
6. 창이 나타나면 또는 목록에서 원하는 계정을 선택하세요.



선택한 계정이 하단의 목록에 표시됩니다.



알아두기

- 이름 검색 입력란에 관리자 또는 기술자 이름을 입력해 검색할 수 있습니다.
- 선택한 계정을 취소하려면 목록에서 해당 계정의 오른쪽에 있는 ✕ 버튼을 클릭하세요.
- 사이트에 관리자로 등록된 계정이나 이미 등록된 기술자 계정은 목록에 표시되지 않습니다.

2 사이트 접근 권한 설정

초대할 기술자를 모두 선택했다면 사이트 접근 권한을 적용하세요. 적용할 수 있는 권한은 아래와 같습니다.

- : 사이트에 가입할 수는 있지만 로그인할 수 없습니다.
- : **대시보드** 및 **장치 관리** 메뉴에만 접근할 수 있습니다.
- : **사용자 관리** 메뉴를 제외한 모든 메뉴에 접근할 수 있지만, 일부 설정 기능에 대한 접근은 제한됩니다.
- : **사용자 관리** 메뉴를 포함한 모든 메뉴에 접근할 수 있지만, 일부 설정 기능에 대한 접근은 제한됩니다.

알아두기

- 및 은 다음 메뉴 경로에 대해 보기 권한은 있지만 수정 권한은 없습니다.
  - **설정** → **관리자 & 기술자**
  - **설정** → **사이트**
- 파트너 포털에서 기술자를 사이트에 배정하면서 접근 권한을 설정한 후에는 BioStar Air 관리자 포털의 관리자 계정으로만 접근 권한을 변경할 수 있습니다.

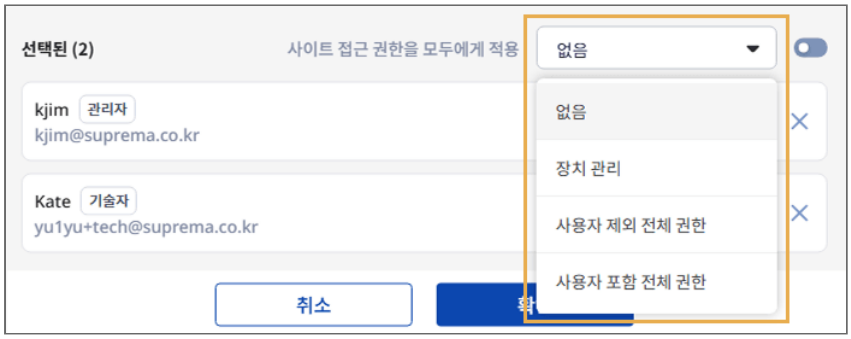
3 개별 기술자 권한 설정

개별 기술자에게 서로 다른 권한을 적용할 수 있습니다. 각 계정의 오른쪽에서 원하는 권한 수준을 선택하세요.

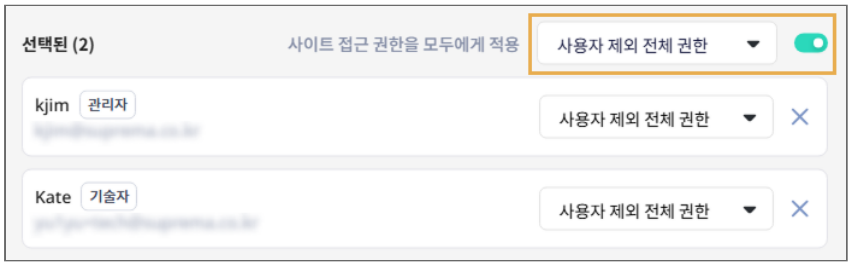


4 모든 기술자에게 동일한 권한 적용

1. 선택한 모든 계정에 동일한 권한을 적용하려면 옵션에서 원하는 권한 수준을 선택하고 오른쪽의 토글 버튼을 클릭하세요.

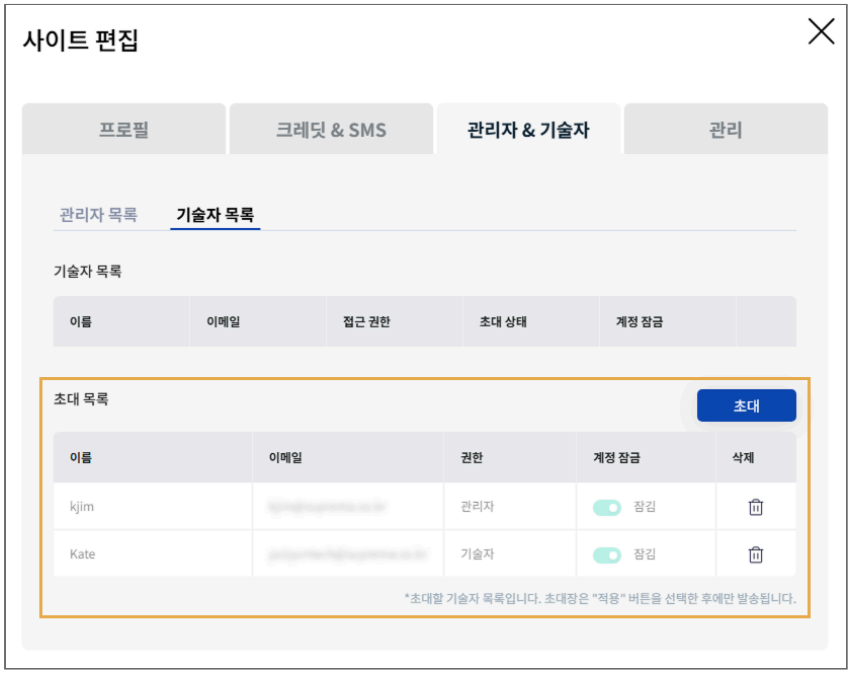


2. 팝업 메시지가 나타나면 버튼을 클릭하세요.
3. 목록의 모든 계정에 선택한 권한이 적용됩니다.



5 기술자 초대 완료

1. 기술자 초대 및 권한 설정을 완료하면 창에서 **확인** 버튼을 클릭하세요.
2. 창이 닫히고, 패널의 에 초대한 기술자들이 표시됩니다.



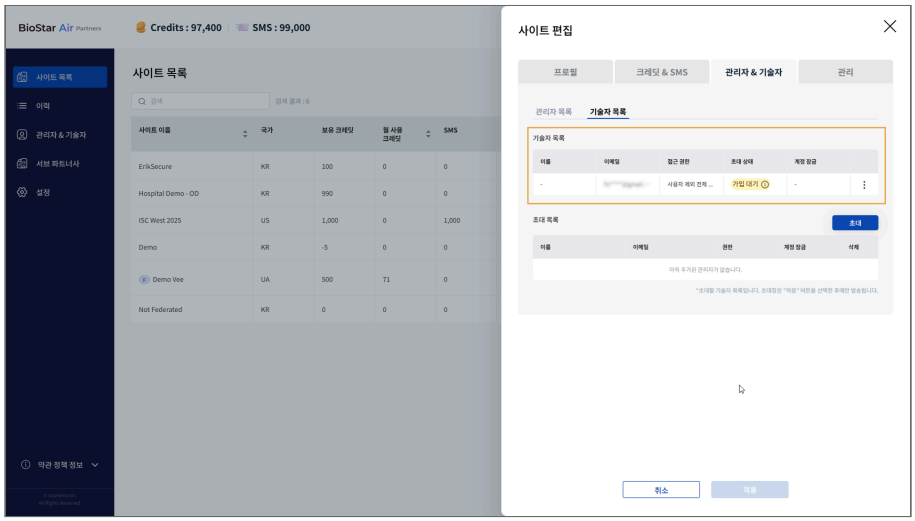
3. 초대 이메일을 발송해 기술자가 사이트에 접근하도록 하려면 패널 하단의 버튼을 클릭하세요.

초대 상태 확인

사이트에 초대된 기술자의 초대 상태를 확인할 수 있습니다. 초대 받은 기술자가 이메일을 수락하기 전까지는 초대 상태가 로 표시됩니다. 초대 받은 기술자는 최대 7일까지 초대를 수락할 수 있으며, 7일이 지나면 초대가 만료되어 상태로 변경됩니다.

1. 사이트 목록에서 기술자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 초대 상태를 확인할 수 있습니다.

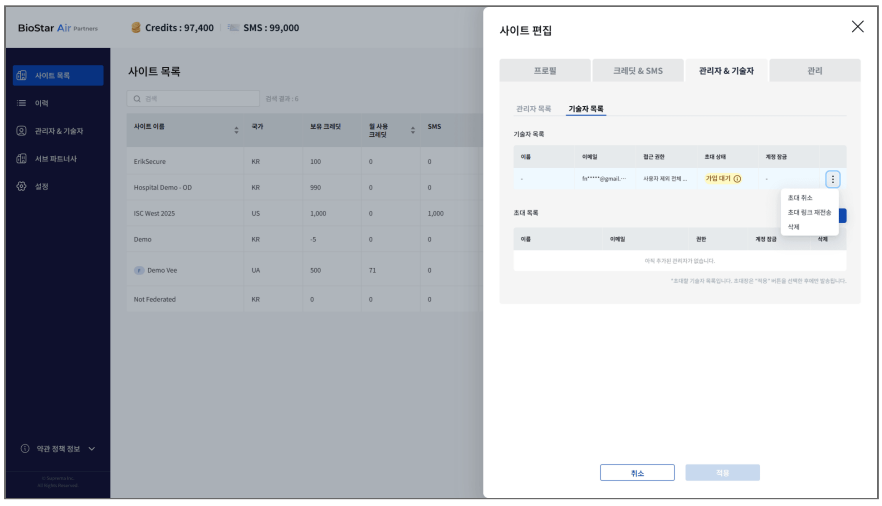
기술자가 사이트에 가입을 완료하면 상태에서 상태로 변경됩니다.



초대 취소

사이트에 초대된 기술자의 이메일 주소를 잘못 입력했거나 문제가 해결되어 더 이상 기술자 초대가 필요하지 않을 때, 초대를 취소할 수 있습니다.

1. 사이트 목록에서 기술자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 상태인 기술자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



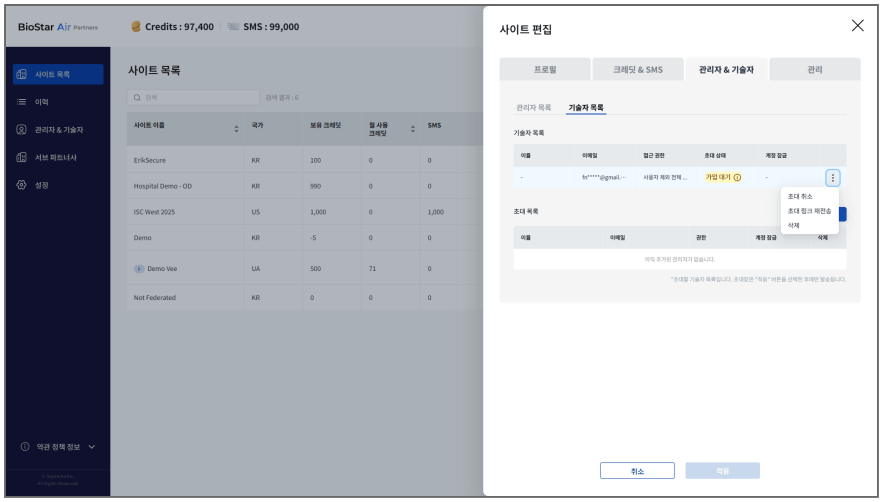
4. 팝업 메뉴에서 를 클릭하세요.
5. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
6. 초대 취소 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

초대 취소된 기술자는 초대 상태가 상태에서 상태로 변경됩니다.

초대 링크 재전송

사이트에 초대된 기술자가 초대 이메일을 받지 못했거나 분실한 경우, 초대 링크를 재전송할 수 있습니다.

1. 사이트 목록에서 기술자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 또는 , 상태인 기술자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.

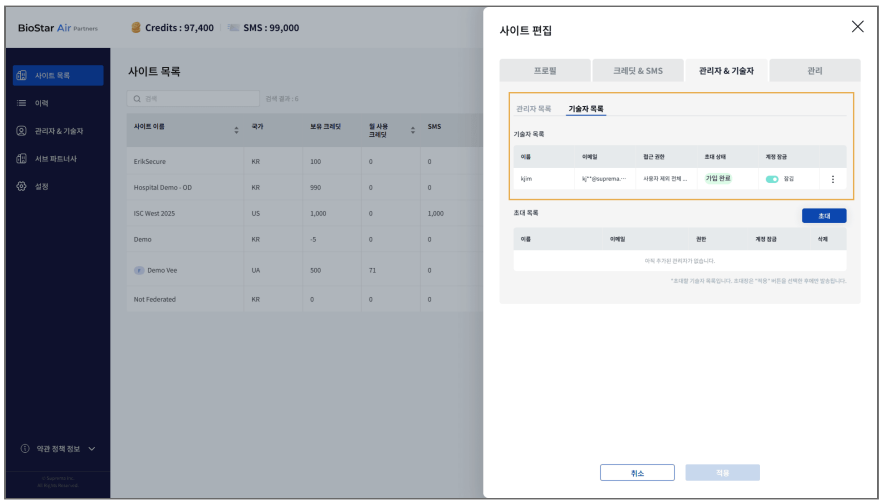


4. 팝업 메뉴에서 을 클릭하세요.
5. 팝업 메시지 창이 나타나면 내용을 확인하고 버튼을 클릭하세요.
6. 초대 링크 재전송 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

기술자 계정 잠금/해제

사이트에 배정된 기술자의 계정을 잠그거나 해제할 수 있습니다.

1. 화면 왼쪽 사이드바에서 을 클릭하세요.
2. 사이트 목록에서 기술자의 접근을 관리할 사이트를 클릭하세요.
3. 패널이 나타나면 → 탭을 차례로 클릭하세요.



4. 에서 기술자 계정을 잠그거나 해제하려면 열에서 토글 버튼을 클릭하세요.

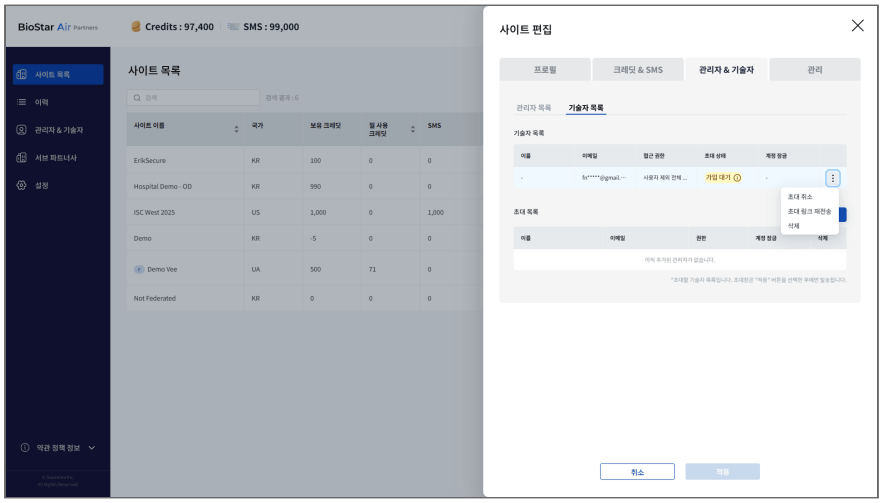
5. 수정한 내용을 적용하려면 하단의 버튼을 클릭하세요.

> **알아두기**
> 최초 등록된 기술자 계정은 사이트에 대한 접근 권한이 상태입니다. 상태를 해제하려면 BioStar Air 포털에서 해당 사이트의 관리자 권한을 가진 계정으로 해제할 수 있습니다.

기술자 삭제

사이트에 초대된 기술자의 계정을 삭제할 수 있습니다. 기술자의 계정이 삭제되면 해당 기술자는 사이트에 로그인할 수 없으며, 사이트 접근 권한이 제거됩니다.

1. 사이트 목록에서 기술자를 초대한 사이트를 클릭하세요.
2. 패널이 나타나면 → 탭을 차례로 클릭하세요.
3. 에서 삭제할 기술자의 가장 오른쪽에 ⋮ 버튼을 클릭하세요.



4. 팝업 메뉴에서 **삭제**을 클릭하세요.
5. 팝업 메시지 창이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.
6. 기술자 삭제 성공 메시지가 나타나면 **닫기** 버튼을 클릭하세요.

> **알아두기**
> 삭제된 기술자 계정은 완전히 삭제되는 것이 아니라 해당 사이트에 대한 접근 권한만 제거됩니다. 삭제된 기술자 계정은 사이트에 다시 초대하여 접근 권한을 부여할 수 있습니다.

하드웨어 설치하기

BioStar Air 시스템을 올바르게 구성하기 위한 하드웨어 설치 및 설정 가이드입니다. SIP 인터폰, IP 카메라, QR 스캐너, 에어팝 패치 등 각 장치의 연결과 설정 방법, 네트워크 포트 구성, 보안 모듈 설정을 안내합니다.

BioStation 3 SIP 인터폰 설정하기

BioStar Air v2.10부터는 **BioStation 3**(BS3)에서 SIP 인터폰 기능을 지원합니다. 이를 통해 리더기와 관리자 간의 양방향 음성 통화는 물론 원격으로 출입문을 잠금 해제할 수 있습니다.

> **알아두기**
> 이 기능을 사용하려면 SIP 서버가 필요하며, 별도로 구매 및 구성해야 합니다. 슈프리마는 SIP 서비스를 제공하지 않습니다.

SIP

세션 시작 프로토콜(**Session Initiation Protocol, SIP**)은 IP 네트워크를 통해 실시간 음성 및 비디오 통화를 시작, 유지 및 종료하는 데 널리 사용되는 통신 프로토콜입니다. 이 경우 SIP는 BioStation 3가 인터폰 엔드포인트로 작동하여 호환되는 SIP 서비스를 통해 전화를 걸고 받을 수 있도록 합니다.

전화 받기

BioStation 3에서 수신된 전화는 아래의 방식으로 받을 수 있습니다.

- **BioStar Air Web**: 웹 브라우저에서 직접 통화 수신
- **BioStar Air Mobile App** (iOS / Android): 이동 중에도 통화 수신

원격 출입문 제어

SIP 전화를 받을 때, **DTMF 명령**을 사용하여 출입문을 열 수 있습니다:

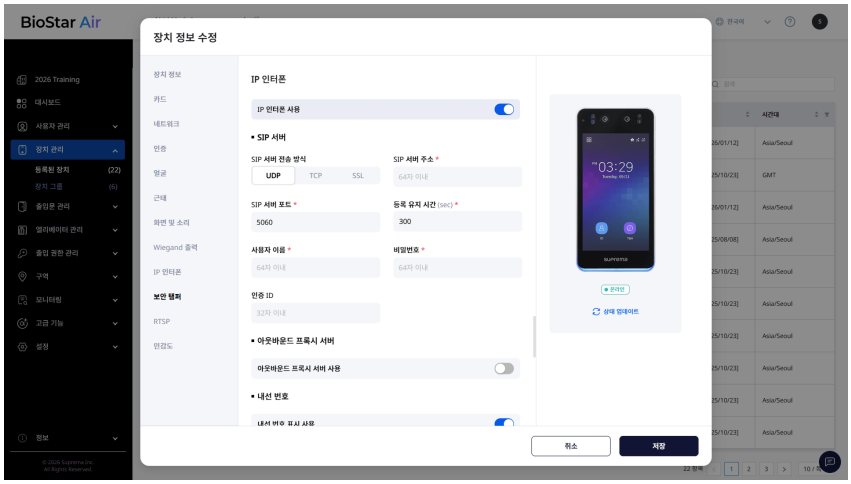
- 물리적 SIP 전화
- BioStar Air 모바일 앱
- BioStar Air Web 인터페이스

구성 단계

장치 설정 및 관리자 계정 설정에서 구성할 수 있습니다.

1 장치 설정

1. BioStar Air 포털에 로그인하세요.
2. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
3. 장치 목록에서 **BioStation 3**를 클릭하세요.
4. **IP 인터폰** 섹션으로 이동해 **IP 인터폰 사용** 옵션을 활성화하세요.
5. SIP 서버 정보를 입력하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **SIP 서버 주소**
- **SIP 서버 포트**
- **사용자 이름** / **비밀번호**

6. 변경 사항을 저장하려면 **저장** 버튼을 클릭하세요.

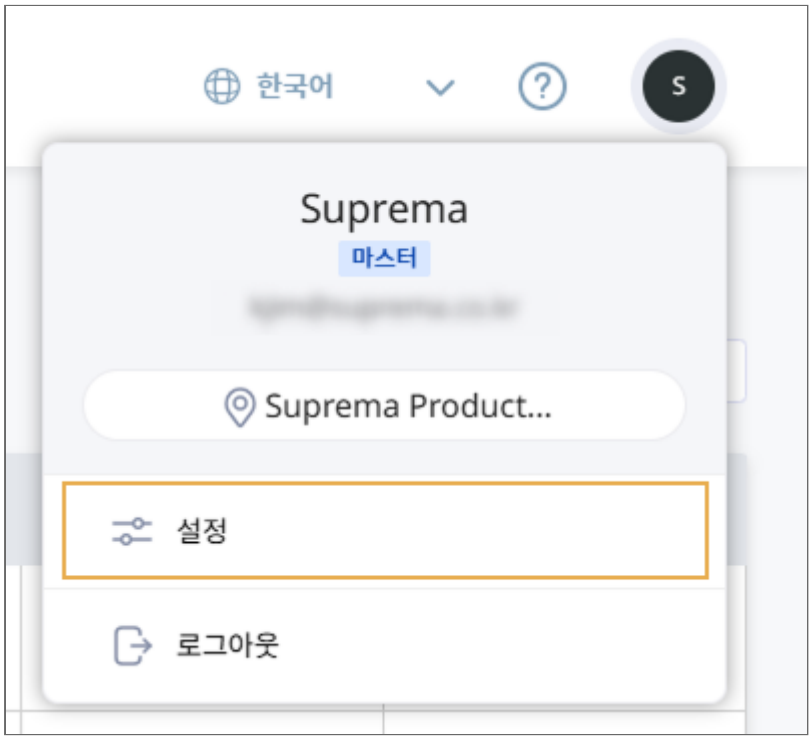
2 계정 설정

BioStation 3의 통화를 브라우저나 앱으로 라우팅할 수 있습니다.

1. 통화를 수신해야 하는 각 관리자는 BioStar Air 포털 또는 모바일 앱에 로그인하세요.
2. **계정 설정**으로 이동하세요.

Web

화면 오른쪽 상단의 사용자 프로필 아이콘을 클릭한 후 **설정**을 선택하세요.



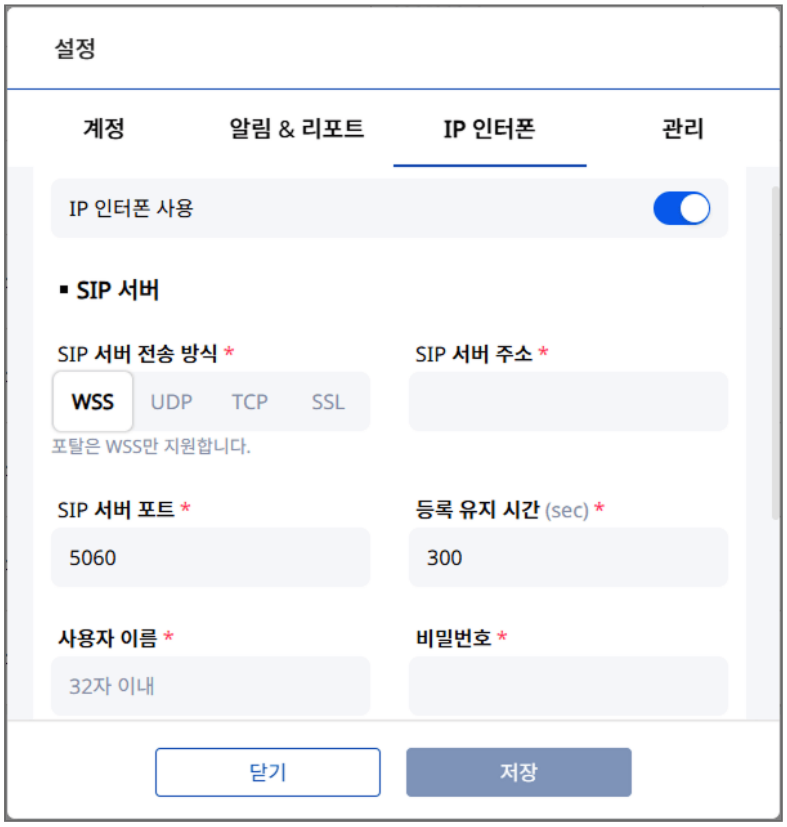
Mobile

초기 화면에서 하단의 **전체 메뉴**를 탭한 후 사용자 프로필 영역을 탭하세요.

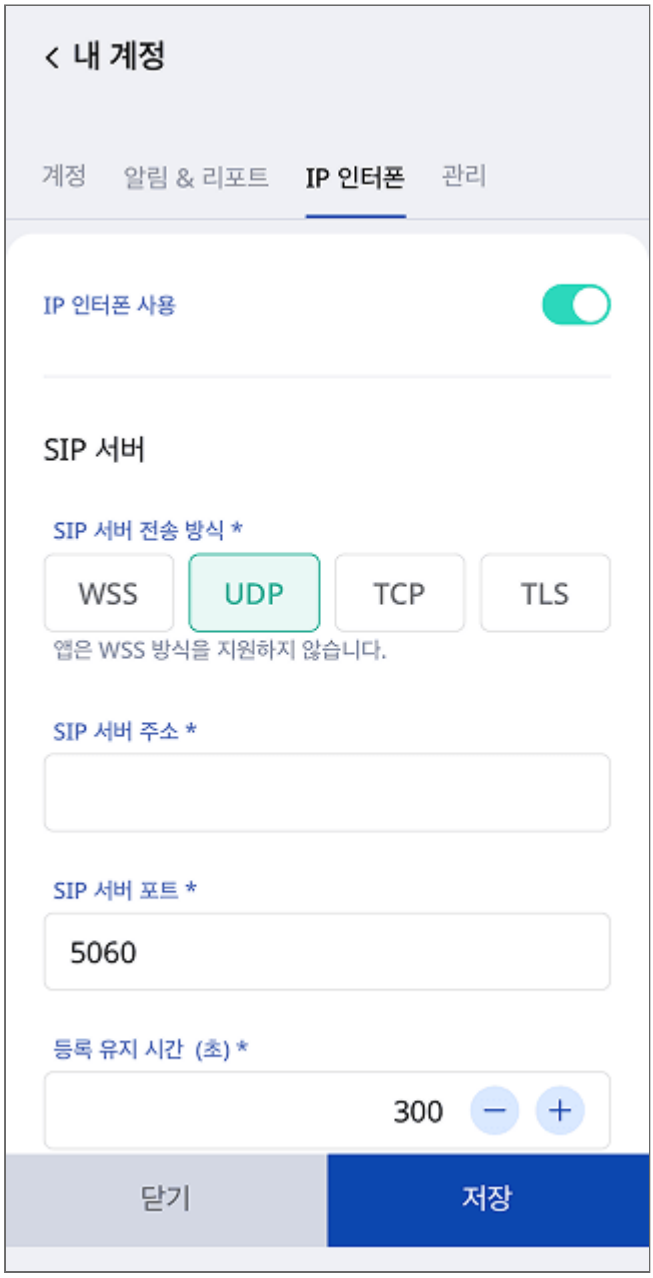


3. **설정** 창이 나타나면 **IP 인터폰** 탭을 클릭한 후 SIP 서버 로그인 정보를 추가하세요.

Web


설정
계정
알림 & 리포트
IP 인터폰
관리
IP 인터폰 사용
▪ SIP 서버
SIP 서버 전송 방식 *
WSS
UDP
TCP
SSL
포탈은 WSS만 지원합니다.
SIP 서버 주소 *
SIP 서버 포트 *
5060
등록 유지 시간 (sec) *
300
사용자 이름 *
32자 이내
비밀번호 *
닫기
저장

Mobile



4. 설정을 저장하려면 **저장** 버튼을 클릭하세요.

검증된 SIP 공급자

BioStation 3는 아래 공급자와 함께 정상 작동함을 테스트 및 확인하였습니다.

- RingCentral
- FreePBX
- Linphone
- Linhome

IP 카메라 지원 및 설정하기

BioStar Air와 호환되는 장치와 동일한 네트워크에 연결된 IP 카메라를 BioStar Air에서 자동 감지합니다. 카메라는 장치를 게이트웨이로 사용하므로 네트워크 비디오 레코더(Network Video Recorder, NVR)가 필요하지 않습니다. 대신 카메라는 내장 SD 카드 저장 장치를

사용합니다.

BioStar Air와 호환되는 장치를 설치했다면 BioStar Air는 아래와 같은 동시 라이브 뷰 스트림을 표시할 수 있습니다.

- 최대 2대의 카메라에서 Full HD 해상도(1080p)
- 최대 4대의 카메라에서 HD 해상도(720p)

이 사양은 X-Station 2를 사용할 때 두 배로 증가합니다.

> **알아두기**
> BioStar Air에 카메라를 등록한 후 녹화된 비디오가 재생되지 않으면 비디오 재생 관련 문제 해결를 참고하세요.

호환성

- **Onvif Profiles**: IP 카메라는 Onvif 프로필 S 또는 G와 호환되어야 합니다.
  - **Onvif Profile S**: 라이브 비디오 스트리밍
  - **Onvif Profile G**: 녹화된 비디오를 SD 카드에 저장
- **SD 카드**: IP 카메라는 나중에 녹화한 영상을 재생할 수 있도록 내장 SD 카드가 있어야 합니다.

  > SanDisk microSDXC Class10 Max Endurance 256GB 또는 512GB를 권장합니다.

- **인코딩**: 카메라는 H.264(AVC)를 지원해야 하며 활성 코덱으로 설정되어 있어야 합니다. BioStar Air는 현재 H.265를 지원하지 않습니다.
- **추천 브랜드**: 한화(Hanwhavision) 및 하이크비전(Hikvision), 다후아(Dahua) 카메라와의 호환성이 뛰어납니다. 다른 브랜드와의 호환성은 Onvif 프로필 준수 여부에 따라 달라질 수 있습니다. 테스트 및 검증된 장치 목록에 대한 자세한 내용은 테스트 및 검증된 장치 목록을 참고하세요.
- 테스트하고 싶은 다른 카메라 브랜드가 있다면 서비스 팀에 문의하세요.

기능 소개

BioStar Air 포털 또는 모바일 앱에서 아래와 같은 작업을 수행할 수 있습니다.

- 실시간 카메라 피드를 볼 수 있습니다.
- 녹화된 카메라 영상을 볼 수 있습니다.
- 출근 이벤트와 관련된 카메라 영상에 접근할 수 있습니다.

사용 안내

1 IP 카메라 연결

- **네트워크 연결**: IP 카메라가 BioStar Air와 호환되는 장치와 동일한 네트워크에 연결되어 있는지 확인하세요.
- **Onvif 활성화**: 카메라에서 Onvif가 활성화되어 있는지 확인하세요.

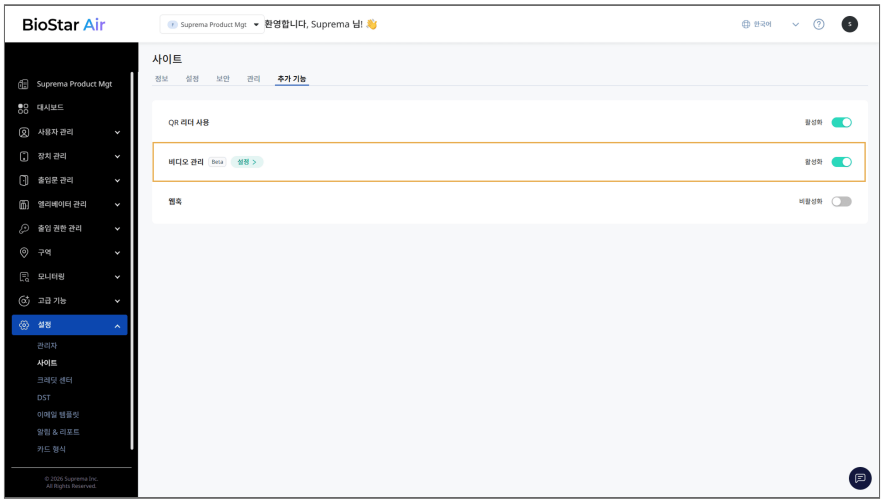
- **장치 등록**: 장치가 BioStar Air 포털에 등록되어 있는지 확인하세요.

2 BioStar Air 로그인

마스터 관리자만 비디오 관리 활성화와 같은 사이트 설정을 변경할 수 있습니다. BioStar Air 포털에 **마스터** 권한으로 로그인하세요.

3 비디오 관리 활성화

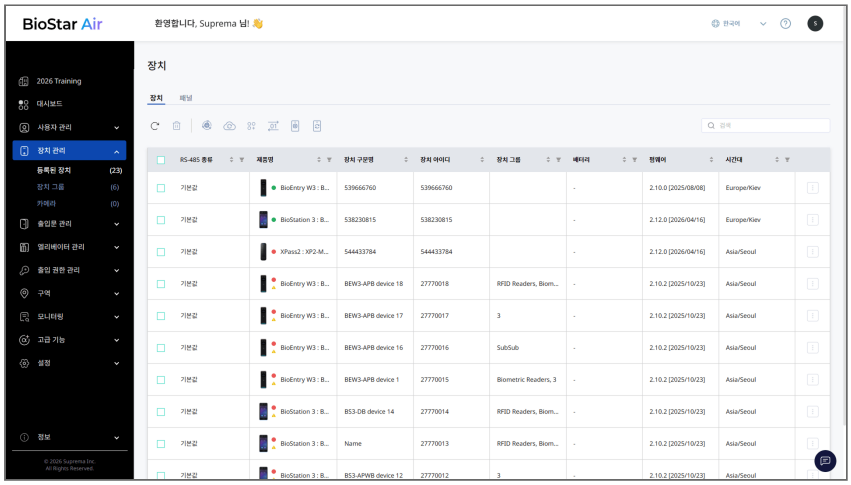
1. 화면 왼쪽 사이드바에서 **설정** → **사이트**를 클릭하세요.
2. **추가 기능** 탭을 클릭하세요.
3. **비디오 관리** 옵션을 활성화하세요.



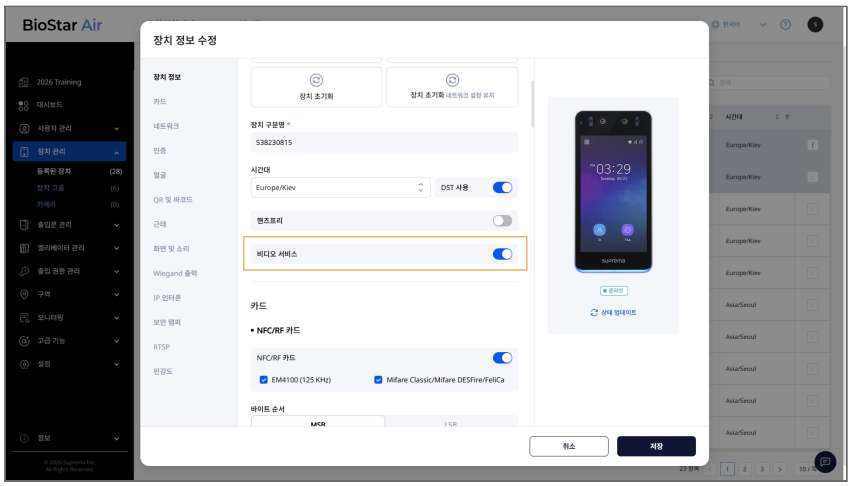
> **알아두기**
> 이 기능은 **마스터** 레벨의 관리자만 활성화할 수 있습니다.

4 비디오 서비스 활성화

1. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.



2. 목록에서 BioStar Air와 호환되는 장치(예: BioStation 3)를 클릭하세요.
3. **장치 정보 수정** 창이 나타납니다.
4. **장치 정보** 섹션의 **비디오 서비스** 옵션을 활성화하세요.

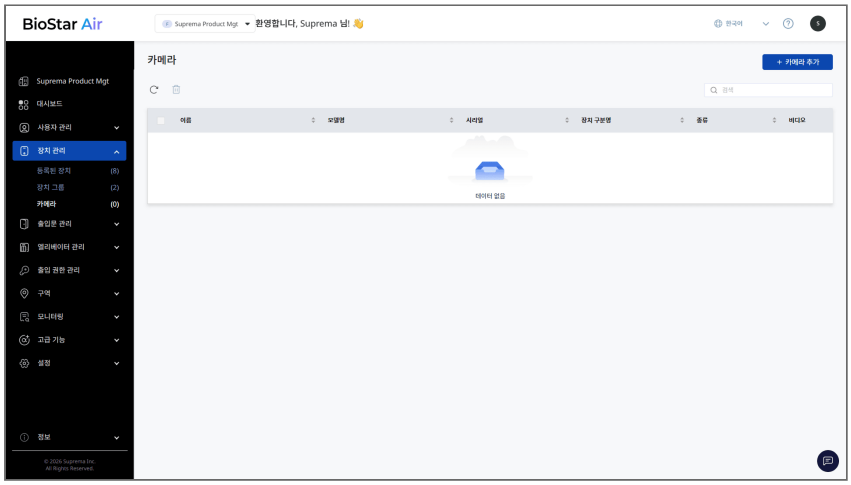


5. 변경 사항을 저장하려면 하단의 **저장** 버튼을 클릭하세요.

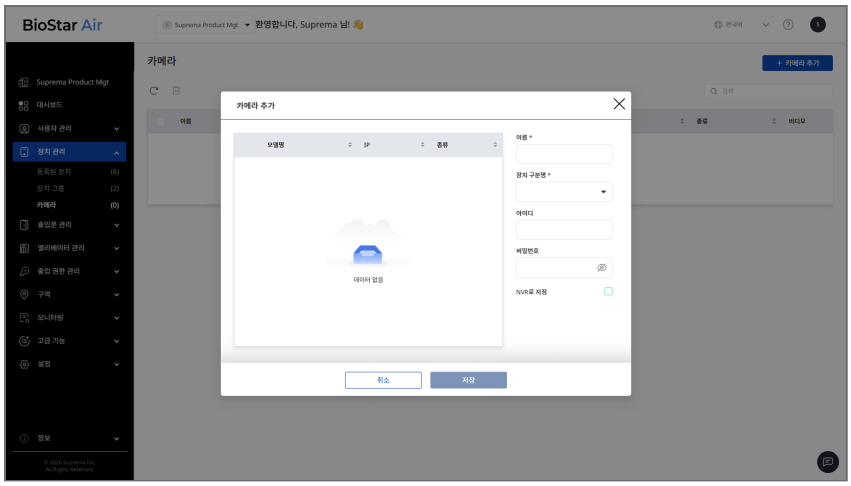
> **알아두기**
> 장치는 펌웨어 2.5.1 버전 이상이 설치되어 있어야 하며, 카메라와 동일한 네트워크에 있어야 합니다.

5 카메라 추가

1. 화면 왼쪽 사이드바에서 **장치 관리** → **카메라**를 클릭하세요.



2. 화면 오른쪽 상단의 **카메라 추가** 버튼을 클릭하세요.
3. **카메라 추가** 창이 나타나면 게이트웨이 역할을 할 장치를 선택하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

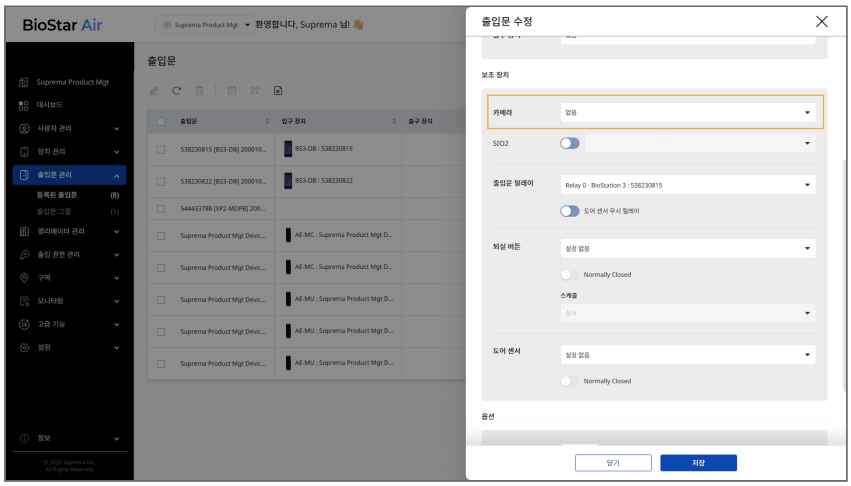
4. 카메라를 추가하려면 아래 정보를 설정하세요.
   - **이름**: 카메라 이름을 입력하세요.
   - **장치 구분명**: 카메라를 구분할 이름을 선택하세요.
   - **아이디**: 카메라에 접속할 아이디를 입력하세요.
   - **비밀번호**: 카메라에 접속할 비밀번호를 입력하세요.
5. 선택한 카메라를 추가하려면 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - 장치는 펌웨어 2.5.1 버전 이상이 설치되어 있어야 하며, 카메라와 동일한 네트워크에 있어야 합니다.
> - BioStar Air는 자동으로 네트워크에서 카메라를 검색합니다.

6 출입문과 연결

추가한 카메라를 출입문과 연결하여 출입 이벤트와 관련 영상을 연동할 수 있습니다.

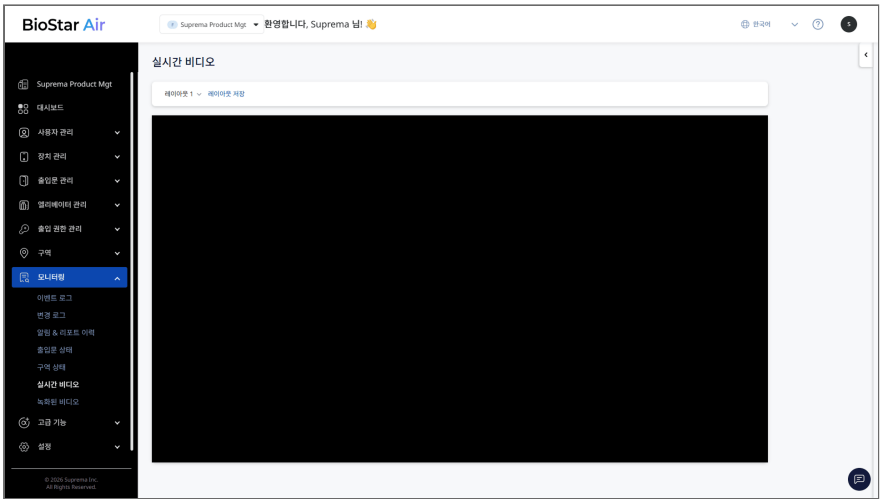
1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 목록에서 카메라를 할당할 출입문을 클릭하세요.
3. **출입문 수정** 패널이 나타나면 **보조 장치** 섹션으로 스크롤하세요.
4. **카메라** 옵션에서 추가한 카메라를 선택하세요.



5. 변경 사항을 저장하려면 **저장** 버튼을 클릭하세요.

7 실시간 카메라 영상 보기

추가한 카메라의 영상을 실시간으로 볼 수 있습니다. 화면 왼쪽 사이드바에서 **모니터링** → **실시간 비디오**를 클릭하세요.



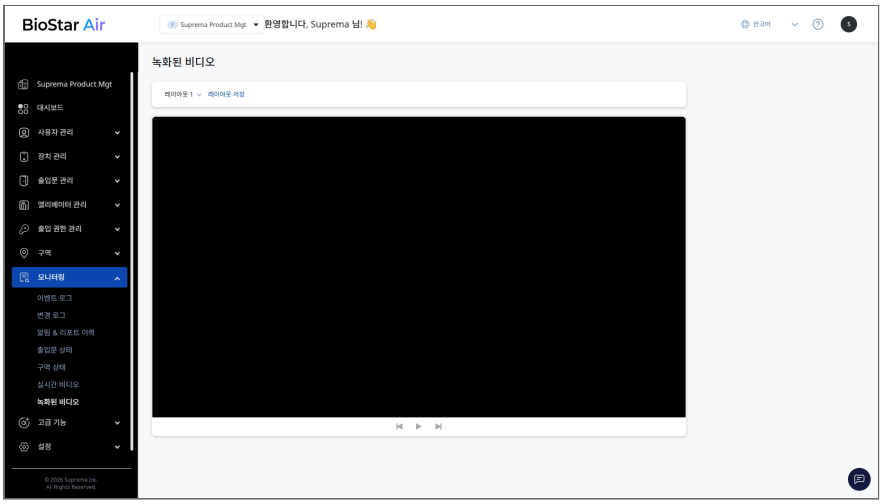
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- BioStar Air와 호환되는 장치에 대해 최대 2개의 Full HD (1080p) 실시간 스트림을 볼 수 있습니다.
- 더 많은 실시간 스트림을 보려면 더 많은 장치를 추가하거나 카메라 해상도를 줄이세요.

> ***장치 관리*** → ***카메라*** → *목록에서 카메라 클릭* → ***비디오 프로파일***

8 녹화된 카메라 영상 보기

녹화된 비디오 스트림을 볼 수 있습니다. 화면 왼쪽 사이드바에서 **모니터링** → **녹화된 비디오**를 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

9 이벤트 영상 보기

화면 왼쪽 사이드바에서 **모니터링** → **이벤트 로그**를 클릭하세요. 관련 비디오 클립이 있는 이벤트 로그를 찾아 재생 버튼을 클릭하면 영상을 시청할 수 있습니다.

테스트 및 검증된 장치 목록

No	제조사	모델 번호	장치 유형	Onvif 프로필	해상도
1	Hanwha Techwin	QNV-C8011R	Camera	S, G, T, M	2592x1944
2	Hanwha Techwin	QND-6022R	Camera	S, G, T	1920x1080
3	Hanwha Techwin	MMI-600R	Camera	S, T	1920x1080
4	HIKVISION	DS-2CD2025FWD-I	Camera	S, G, T	1920x1080
5	HIKVISION	DS-2CD2166G2-I	Camera	S, G, T	3200×1800
6	HIKVISION	DS-2CD1121-I	Camera	S	1920x1080
7	Dahua	DHI-NVR2104HS-P-S3	NVR	S, G, T	12MP
8	Dahua	IPC-HDBW3249E-AS-NI	Camera	S, G, T	1920×1080
9	Dahua	SD22204UEN-GN	Camera	S, G, T	1920×1080
10	Dahua	DH-IPC-HFW1230DT-STW-VN	Camera	S, T	1920×1080
11	Marruy	IPC-A32E-L	Camera	S, T	2304×1296

No	제조사	모델 번호	장치 유형	Onvif 프로필	해상도
12	TP-Link	Tapo C210	Camera	S	2304×1296

IP 카메라의 ONVIF 활성화 방법

1. 웹 브라우저를 열고, 카메라의 IP 주소를 입력하세요.
2. 관리자 크리덴셜로 인증 후 로그인하세요.
3. **Network** 또는 **Configuration** 섹션으로 이동하세요.
4. ONVIF 또는 개방형 네트워크 비디오 인터페이스를 활성화하세요.
5. 필요에 따라 ONVIF 전용 사용자 프로필을 생성하세요.
6. 설정을 저장하고 BioStar Air에서 ONVIF 연결을 테스트하세요.

팁

- **펌웨어 업데이트**: 카메라와 장치를 최신 펌웨어로 업데이트하세요.
- **포트 포워딩**: 필요에 따라 ONVIF에 대한 포트 포워딩을 구성하세요.
- **Third-Party 도구**: ONVIF Device Manager를 사용하여 카메라 설정 및 기능을 확인하세요.

에어팝 패치 설치

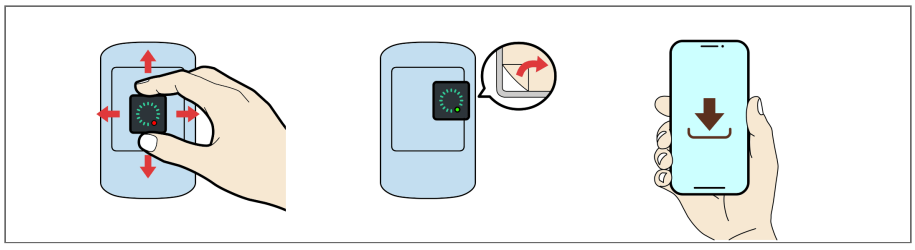
에어팝 패치(Airfob Patch)를 설치 방법을 안내합니다. 에어팝 패치는 기존 출입 통제 시스템을 BioStar Air 모바일 크리덴셜과 호환될 수 있도록 업그레이드하는 장치입니다.

알아두기

- 에어팝 패치는 MIFARE 1K 기술과 호환되지만 125 KHz **저주파** 리더기와는 호환되지 않습니다.
- 에어팝 패치는 모바일 기기에서 암호화된 BioStar Air 크리덴셜을 블루투스로 인증하고 리더에 MIFARE RFID 신호를 에뮬레이션하여 작동합니다. 테이프를 사용하여 출입 통제 장치에 부착하며 배선이 필요하지 않습니다.
- 에어팝 패치를 BioStar Air 앱에 등록하는 방법에 대한 자세한 내용은 에어팝 패치와 태그 구성하기를 참고하세요.

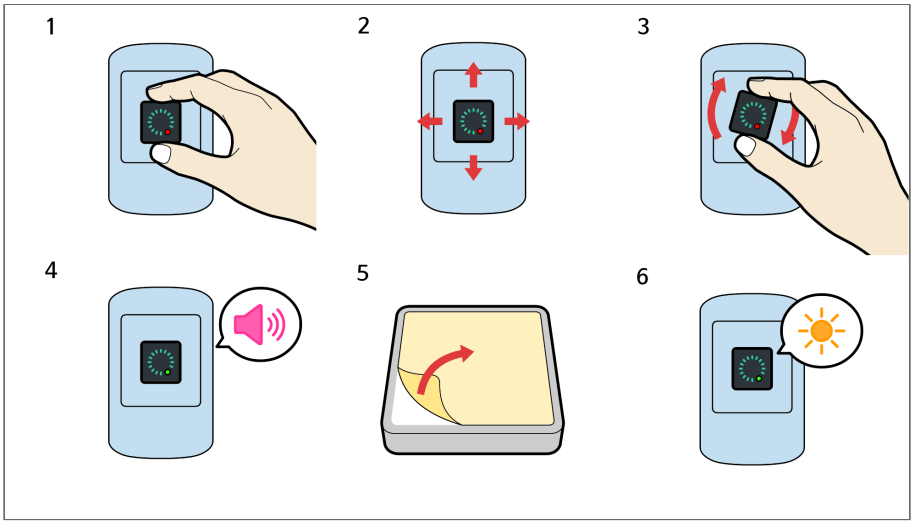
설치 개요

에어팝 패치가 장치의 RF 필드를 통해 전원을 공급받을 수 있는 위치를 찾으세요.



에어팝 패치 설치 위치 확인

함께 제공된 접착 테이프로 에어팝 패치를 출입 통제 장치에 부착하기 전에, 아래의 그림과 지침에 따라 장치에서 가장 적합한 위치를 찾으세요.



1. 에어팝 패치를 출입 통제 장치에 서로 닿도록 위치시키세요.
2. 에어팝 패치의 LED가 1초에 한 번 이상 녹색으로 깜박이는지 위치를 찾으세요.
3. 에어팝 패치를 장치에 대거나, 탈착식 테이프를 사용해 임시로 부착하세요. BioStar Air 앱을 사용해 에어팝 패치를 등록하세요. 자세한 내용은 에어팝 패치와 태그 구성하기를 참고하세요.
4. 에어팝 또는 BioStar Air 모바일 크리덴셜을 사용해 최소 5회 이상 테스트 인증을 수행하세요.
5. 에어팝 패치의 뒷면에 부착된 양면 접착 테이프의 보호 필름을 제거하세요.
6. 출입 통제 장치에 에어팝 패치를 부착하세요.

알아두기

- 에어팝 패치는 별도의 전원 공급 장치가 필요하지 않습니다. 출입 통제 장치에 부착하면 자동으로 전원이 켜집니다.
- 함께 제공된 양면 테이프로 Airfob Patch를 장치에 부착하면 영구적으로 고정됩니다. 에어팝 패치를 제거하면 에어팝 패치가 손상되어 재사용이 불가능할 수 있습니다.

문제 해결

▼ Q. 출입 통제 장치에서 연속 5회의 작동음이 발생하지 않아요.

출입 통제 장치에서 연속 5회의 작동음이 발생하지 않는다면 에어팝 패치를 재부팅하세요.

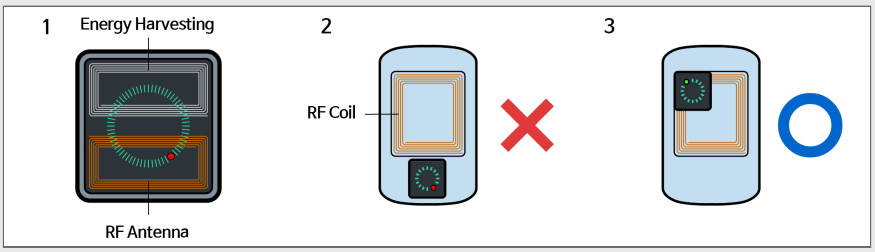
1. 출입 통제 장치에서 에어팝 패치를 분리하세요.
2. 전원이 꺼지면 에어팝 패치 LED가 약 6초 동안 빨간색으로 깜박인 후 꺼집니다.
3. 에어팝 패치의 전원이 꺼져 있는지 확인하고 처음부터 다시 시작하세요.

▼ Q. 에어팝 패치의 LED가 빨간색으로 깜박여요.

에어팝 패치의 빨간색 LED가 깜박인다면 에어팝 패치의 위치를 조정하세요.

1. 에어팝 패치를 출입 통제 장치의 다른 위치로 이동시켜 LED가 녹색으로 깜박이는지 확인하세요.
2. 전력 강도가 강하면 LED가 0.5초 또는 1초 간격으로 깜박입니다.
3. 에어팝 패치의 위치를 변경했다면 에어팝 패치를 재부팅하고 처음부터 다시 시작하세요.

▼ Q. 출입 통제 장치가 에어팝 패치를 인식하지 못해요.



- 출입 통제 장치의 RF 코일 위치와 에어팝 패치의 RF 안테나 위치가 일치할 때 두 장치가 정상 작동합니다.
- 모바일 기기로 출입 제어 장치를 터치했을 때 유효한 접근 권한이 부여되지 않으면, 에어팝 패치의 위치를 조정하거나 회전시켜 정상 작동하는 위치를 찾으세요.
- 에어팝 패치의 위치와 방향은 출입 통제 장치에 따라 다를 수 있습니다.
- 에어팝 패치의 작동 범위는 출입 통제 장치의 RF 신호 강도와 RF 코일의 위치 및 크기에 따라 작거나 클 수 있습니다.

SIO2 보안 모듈 구성하기

SIO2 보안 모듈은 BioStar Air와 호환되는 장치와 릴레이 사이의 중개 역할을 하여 출입 통제 시스템의 보안을 강화합니다. **RS485 케이블**을 통해 리더기와 통신하며, 암호화된 통신을 통해 보안 위반을 방지합니다.

> **주의**
> **SIO2 보안 모듈**의 정확한 설치 지침은 제품 패키지에 포함된 배선 다이어그램을 참고하세요. 환경에 따라 설치 방식이 다를 수 있으므로 슈프리마 대리점의 전문적인 지원을 요청하세요.

BioStar Air 포털에서 SIO2 활성화

SIO2 보안 모듈을 정상 통합시키고 출입 통제 시스템의 보안을 강화하려면 다음 단계를 따라 **SIO2** 옵션을 활성화하세요.

> **알아두기**
> SIO2를 설치하고 BioStar Air 포털에서 설정을 변경하지 않으면 작동하지 않을 수 있습니다.

1 리더기 등록

- 리더기, SIO2 및 도어 릴레이가 성공적으로 연결되었는지 확인하세요.
- **BioStar Air 앱**을 통해 사이트에 리더기를 등록하세요.

2 장치 연결 확인

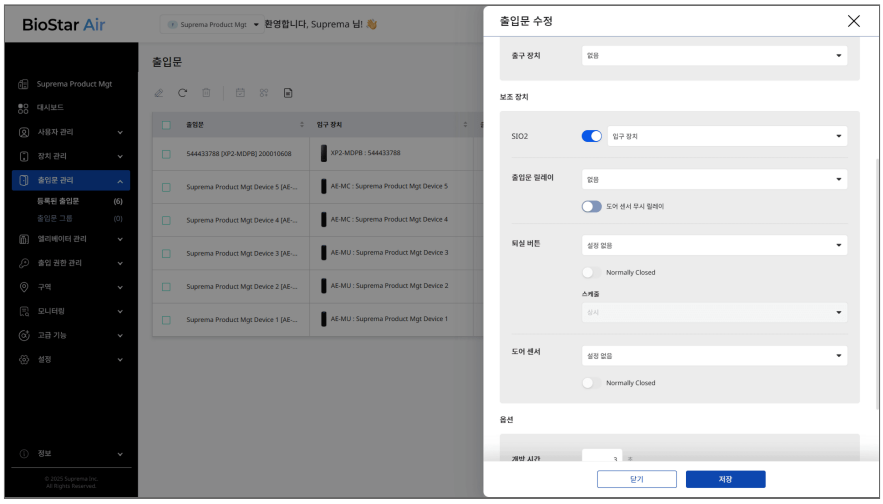
1. BioStar Air 포털에 접속하세요.
2. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
3. 장치 목록에서 해당 장치가 **녹색**(🟢)으로 표시되어 연결이 완료되었는지 확인하세요.

3 SIO2를 출입문에 할당

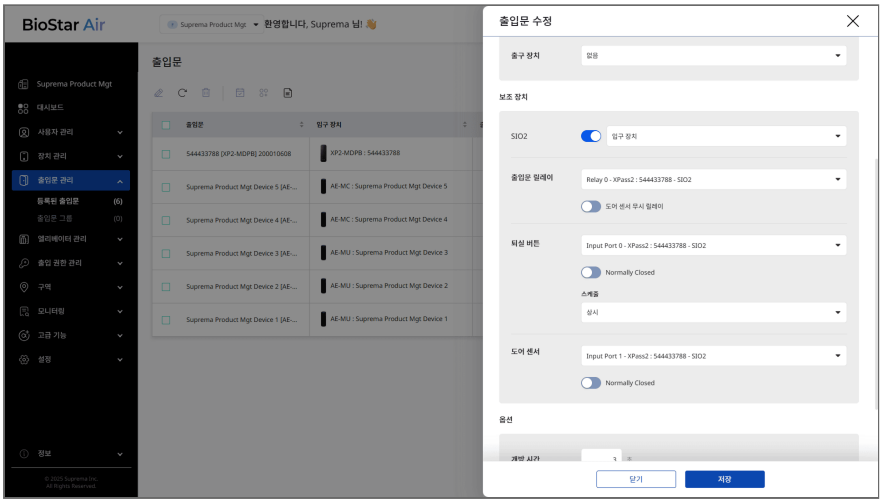
1. 화면 왼쪽 사이드바에서 **출입문 관리** → **등록된 출입문**을 클릭하세요.
2. 목록에서 장치가 연결된 출입문을 클릭하세요. 장치가 등록하면 출입문을 자동 생성합니다.

4 SIO2 활성화

1. **출입문 수정** 패널이 나타나면 **보조 장치** 섹션으로 이동하세요.
2. **SIO2** 옵션을 활성화하세요.



5 릴레이 및 센서 구성



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **출입문 릴레이**는 **Relay 0**을 선택하세요.

> SIO2 모듈에는 하나의 출입문 릴레이 포트만 있습니다.

- **도어 센서**는 연결된 SIO2의 입력 포트 번호를 선택하세요.
- **퇴실 버튼**이 연결되어 있다면 SIO2의 해당 입력 포트를 선택하세요.
- 다른 유형의 출구 장치를 사용한다면 **출구 장치**를 선택하세요.

6 설정 저장

- 설정을 적용하려면 **저장** 버튼을 클릭하세요.
- 이제 SIO2 보안 모듈이 정상 작동합니다.

E200 QR Scanner 배선 및 구성하기

Step 1: 배선

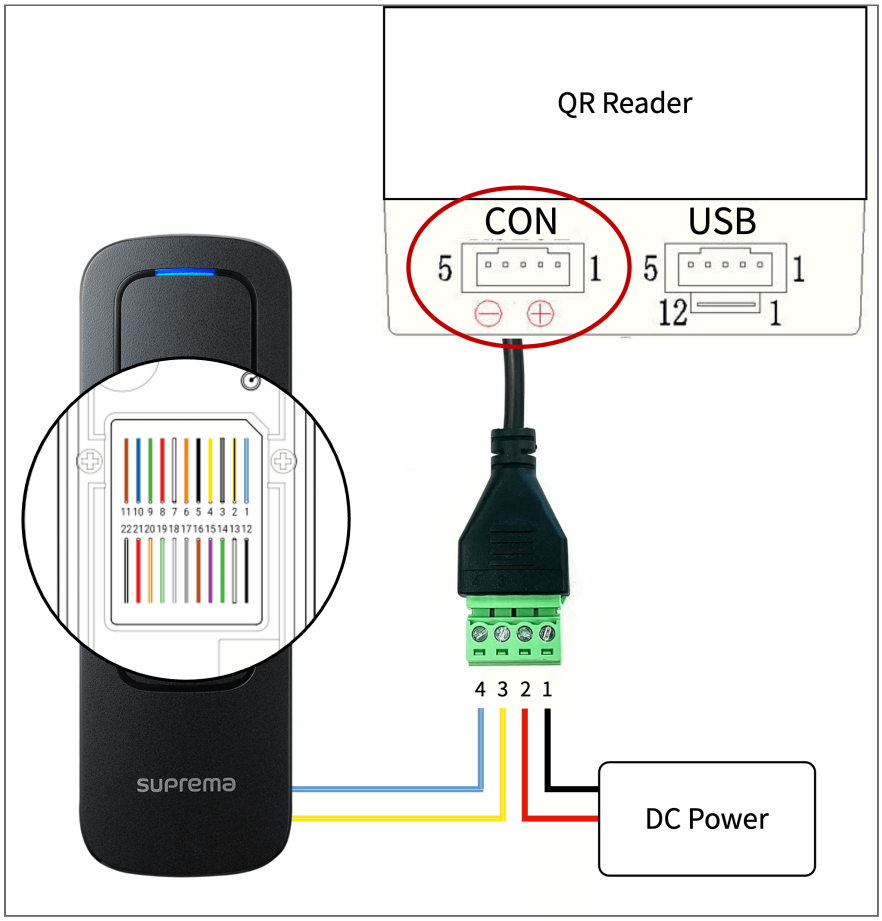
아래와 같이 동봉된 어댑터 케이블을 사용하여 E200 시리즈 QR 스캐너를 연결하세요.

- 녹색 단자 블록에는 **1에서 4**까지 라벨이 붙은 핀이 있으며, 커넥터의 앞면을 바라볼 때 **오른쪽에서 왼쪽**으로 배치됩니다.

Pin	배선색	기능
1	Black	Negative / Ground
2	Red	Positive (V+)
3	Yellow (white stripe)	RS-485 TRXN
4	Blue (white stripe)	RS-485 TRXP

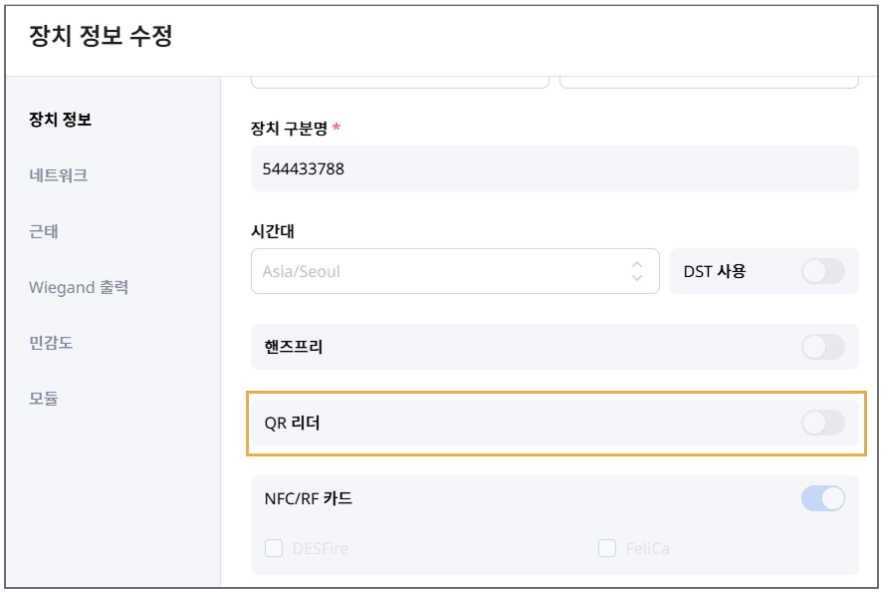
> **알아두기**
> 다른 많은 커넥터와는 배선 방향이 정반대입니다. 배선하기 전에 방향을 다시 한 번 확인하세요.

- QR 스캐너 하단의 CON 포트에 4핀 커넥터를 연결하세요. 이 커넥터는 **편극성**(홈이 있음)이므로 한 방향으로만 맞습니다.



Step 2: QR 리더기 활성화

1. BioStar Air 포털(웹 또는 앱)에 로그인하세요.
2. 화면 왼쪽 사이드바에서 **장치 관리** → **등록된 장치**를 클릭하세요.
3. 목록에서 E200 QR 스캐너를 연결한 장치를 클릭하세요.
4. **장치 정보** 섹션에서 **QR 리더** 옵션을 활성화하세요.



5. 변경 사항을 저장하려면 **저장** 버튼을 클릭하세요.

알아두기

QR 리더기를 활성화하면 동일한 리더기에서 다른 RS-485 연결 장치(예, SIO2)를 사용할 수 없습니다.

Step 3: QR 스캐너 구성

기본적으로 **E200 QR 스캐너**는 **115,200**의 전송 속도로 설정되어 있습니다. 슈프리마 장치와 함께 사용하려면 전송 속도를 **9,600**으로 변경해야 합니다.

QR 스캐너를 장치에 연결하고 **아래 바코드를 스캔**하여 새로운 전송 속도를 적용하세요.



배선이 올바르고 슈프리마 장치가 네트워크에 연결되어 있다면, BioStar Air를 통해 제공된 **다이나믹 QR 크리덴셜**을 사용할 수 있습니다.

네트워크 포트 및 장치 식별하기

BioStar Air와 호환 장치가 원활하게 연결되려면 특정 네트워크 포트에 접근할 수 있어야 합니다. 네트워크 포트를 통해 호환 장치, 클라우드 서비스 및 사용자 애플리케이션 간에 안전하게 통신할 수 있습니다. 관리자는 네트워크 구성 작업을 위해 BioStar Air 호환 장치의 일련 번호를 통해 MAC 주소를 확인해야 할 수도 있습니다.

필수 네트워크 포트

다음 포트가 네트워크 방화벽에서 열려 있는지 확인하십시오.

- **6379, 6381**: Redis Ports

  사용자 정보를 동기화하고, 빠른 이벤트 로깅을 처리하고, 세션을 관리하며, 장치와 클라우드 간의 신호 처리를 위한 메시지 브로커로 사용됩니다.

- **5671**: AMQP over TLS (RabbitMQ)

  서비스 간의 실시간 통신을 위한 안전한 메시징 프로토콜을 제공합니다.

- **443**: HTTPS (TLS)

  표준 보안 웹 트래픽으로 사용되며, 아래와 같은 다양한 서비스에 필요합니다:

  - 웹 브라우저를 통해 관리 포털 웹 앱 접속
  - BioStar Air 모바일 앱 (iOS/Android)
  - API 호출
  - 클라우드를 통한 장치 펌웨어 업데이트
  - 장치 로그인 및 인증 서비스
- BioStar Air의 내장 비디오 관리 기능을 사용하는 경우:
  - 웹 소켓 도메인: eu-wss-api.airfob.com
  - 웹 소켓 포트: 3500
  - TURN/STUN 포트: 80, 443, 3478, 5349

> **알아두기**
> 장치 로그인 및 인증을 위한 다음 엔드포인트 액세스를 확인하세요.
> - https://e-afs-api.airfob.com/v1/device/login (Europe)
> - https://afs-api.airfob.com/v1/device/login (Rest of world)

일련번호를 통해 MAC 주소 확인하기

경우에 따라 BioStar Air 호환 리더기의 MAC 주소를 일련 번호만 사용하여 확인해야 할 수도 있습니다. 이는 장치를 네트워크에 추가하기 전에 화이트 리스트에 추가하는 등의 작업에 유용합니다.

단계

1. **일련 번호 찾기**:

   장치의 뒷면에서 9자리 일련 번호를 찾으세요.

2. **일련 번호를 16진수로 변환**:

   계산기나 온라인 도구를 사용하여 일련 번호를 10진수에서 16진수 형식으로 변환하세요.

3. **마지막 3바이트 추출**:

   16진수 값에서 마지막 6자리를 가져오세요. 마지막 6자리는 마지막 3바이트를 나타냅니다.

4. **MAC 주소 구성**:

   MAC 주소는 항상 `00:17:FC:` 로 시작합니다. 마지막 3바이트(6자리)를 16진수 값에서 가져와 각 쌍을 콜론으로 구분하여 추가하세요.

예시

1. **일련 번호**: 546089489
2. **16진수로 변환**: 208CAA11
3. **마지막 3바이트 추출**: 8CAA11
4. **MAC 주소 구성**: 00:17:FC:8C:AA:11

이 단계를 따르면 일련 번호를 사용하여 네트워크에서 BioStar Air 호환 리더기를 정확하게 식별할 수 있습니다.

MAC 주소 변환기

아래에 장치의 일련 번호를 입력하면 MAC 주소를 바로 확인할 수 있습니다.

인증된 사용자

슈프리마 패스 앱을 사용하면 스마트폰 하나로 출입문을 열 수 있습니다. Bluetooth·NFC·QR 코드 인증 방식 선택부터 2단계 인증 설정, 블루투스 인식 감도 조정까지 앱 사용에 필요한 주요 기능을 안내합니다.

모바일 크리덴셜 사용하기

슈프리마 패스 앱을 사용하면 플라스틱 RFID 카드 대신 모바일 크리덴셜로 출입문을 열 수 있습니다. Bluetooth 또는 NFC를 통해 모바일 기기를 태그하거나 카드를 길게 누를 수 있으며, QR 코드 스캔으로도 출입문을 열 수 있습니다.

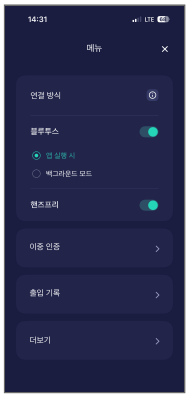
> **알아두기**
> 슈프리마 패스 앱은 BioStar Air 시스템의 사용자 인터페이스 역할을 하며, 주로 모바일 자격 증명을 위한 디지털 지갑 역할을 합니다. 사용자는 앱 내에서 모바일 출입 카드를 발급받고 저장하여 모바일 기기를 통해 안전한 장소에 출입할 수 있습니다.

필수 요구사항 및 준비

모바일 크리덴셜로 출입문을 열기 위해 다음 요구사항을 충족해야 합니다.

- 슈프리마 패스 모바일 크리덴셜과 호환되는 출입 통제 장치가 설치되어 있어야 합니다.
- 사용자의 모바일 기기에 슈프리마 패스 앱이 설치되어 있어야 합니다.
  - iOS
  - 안드로이드
- 모바일 기기에서 블루투스 또는 NFC 통신이 활성화되어 있어야 합니다.
- 2단계 인증을 활성화하면 **백그라운드 모드**는 비활성화됩니다.
- QR 인증은 관리자가 BioStar Air 포털을 통해 활성화해야 합니다.
- Hands-free 출입 기능을 사용하려면 해당 출입 방법을 사이트에서 지원하는지 확인하세요.

> **알아두기**
> - 모바일 기기의 슈프리마 패스 앱에서 모바일 출입 카드로 인증하려면 위치 서비스가 필요합니다. 위치 서비스를 활성화해야 하나요?에서 관련한 FAQ를 확인하세요.
> - 모바일 카드가 장치와 인증되었지만 출입문이 열리지 않는다면 제공하는 안내에 따라 문제를 해결하세요. 모바일 카드가 작동하지 않아요에서 관련한 FAQ를 확인하세요.



연결 방식 설정

슈프리마 패스 앱에서 사용자는 두 가지 작동 모드 중에서 선택할 수 있습니다. 슈프리마 패스 앱 초기 화면에서 오른쪽 상단의 ☰ 아이콘을 탭한 후 **연결 방식**에서 원하는 모드를 선택하세요.

- **앱 실행 시**: 앱이 화면에 표시되고 모바일 카드가 보이는 경우에만 출입문을 열 수 있습니다.
- **백그라운드 모드**: 앱이 백그라운드에서 실행 중이라면 휴대폰이 잠겨 있어도 출입문을 열 수 있습니다.

> **알아두기**
> 모드에 관계없이 사용자는 항상 모바일 기기를 장치에 태그하여 인증할 수 있습니다.

출입문 열기

슈프리마 패스 앱을 사용해 사용자는 다양한 방법으로 출입문을 열 수 있습니다.

모바일 기기를 장치에 태그

모바일 기기를 BioStar Air와 호환되는 장치에 가까이 가져가 블루투스 또는 NFC를 통해 인증하여 출입문을 열 수 있습니다.

1. 슈프리마 패스 앱이 실행 중인지 확인하세요.
2. 모바일 기기의 블루투스 또는 NFC 안테나 부분을 장치에 가까이 가져가세요.
3. 모바일 크리덴셜이 인증되면 출입문이 열립니다.

> **알아두기**
>
> - 사용자는 두 가지 통신 모드 중에서 선택할 수 있습니다. 자세한 내용은 고급 기능 설정하기을 참고하세요.
> - **블루투스 모드**: 모바일 기기가 장치와 무선으로 통신합니다.
> - **NFC 모드**: 안드로이드 기기에서만 사용할 수 있으며, 모바일 기기를 장치에 태그하여 인증할 수 있습니다.
> - 모바일 기기의 블루투스 또는 NFC 안테나 위치는 모델에 따라 다를 수 있습니다. 최적의 접촉 지점은 모바일 기기의 사양을 참고하세요.

모바일 카드 길게 누르기

슈프리마 패스 앱에서 모바일 카드를 길게 누르는 방법으로 출입문을 열 수 있습니다.

1. 슈프리마 패스 앱의 초기 화면을 표시하세요.
2. BioStar Air와 호환되는 장치 근처에서 모바일 카드를 2-3초 길게 누르세요.
3. 모바일 크리덴셜이 인증되면 출입문이 열립니다.

알아두기

- 이 기능을 사용하려면 **연결 방식** 설정에서 반드시 **백그라운드 모드**를 선택해야 합니다. 자세한 내용은 연결 방식 설정을 참고하세요.
- 보안상의 이유로 **사이트 관리자가 이 기능을 비활성화할 수 있습니다.**
- **유효 범위는** 모바일 기기 블루투스 강도에 따라 다릅니다.
- 인근 출입 통제 리더기가 의도하지 않은 인증을 유발할 수 있습니다.

QR 코드 인증

관리자가 BioStar Air 포털에서 **QR 리더 사용** 옵션을 활성화했다면, 슈프리마 패스 앱에서 QR 코드를 QR 리더기로 스캔하여 출입문을 열 수 있습니다. 슈프리마 패스 앱의 초기 화면에서 모바일 카드 하단의 아이콘을 탭하세요.





알아두기

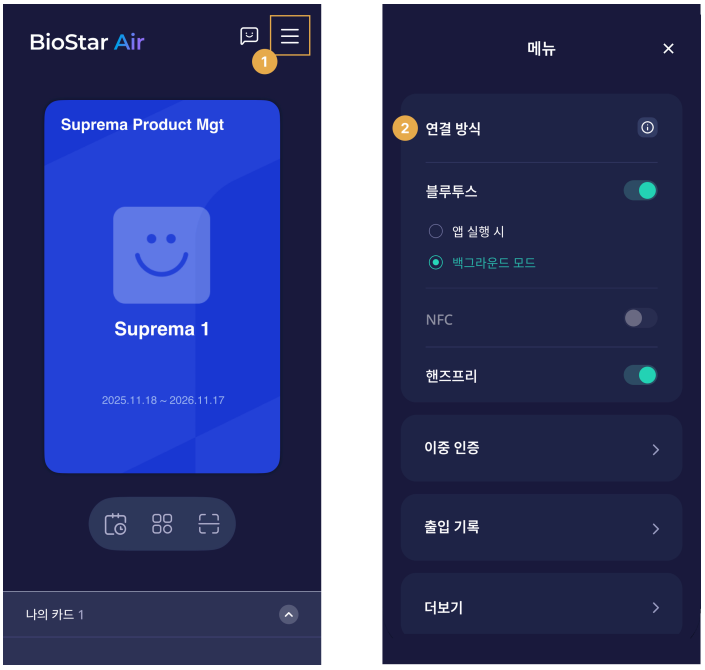
- **QR 리더 사용** 옵션에 대한 자세한 내용은 추가 기능 설정하기를 참고하세요.
- QR 코드 인증은 QR 리더기가 설치된 출입문에서만 사용할 수 있습니다.

고급 기능 설정하기

슈프리마 패스 앱은 사용자 경험과 출입 통제 기능을 향상시키기 위한 고급 설정 및 보안 옵션을 포함합니다. 사용자는 인증 방법 구성, 2단계 인증 활성화, 액세스 로그 검토, 문제 보고 및 지원 기능을 사용할 수 있습니다.

연결 방식 설정

사용자가 출입 통제 장치와 통신하는 데 선호하는 연결 방식을 선택할 수 있습니다. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 아이콘을 탭한 후 **연결 방식**에서 원하는 모드를 선택하세요.



블루투스

사용자는 두 가지 블루투스 인증 모드 중에서 선택할 수 있습니다.

- **앱 실행 시**: 모바일 기기에서 앱이 열려 있을 때만 모바일 카드로 인증할 수 있습니다. 이 모드는 배터리를 절약하지만 출입문에 접근하기 전에 수동으로 앱을 실행해야 합니다.
- **백그라운드 모드**: 앱이 백그라운드에서 실행 중인 경우 모바일 기기의 화면이 꺼져 있어도 모바일 카드로 인증할 수 있습니다. 이 모드는 더 편리하지만 배터리를 더 소모합니다. 앱이 종료되면 백그라운드 기능을 재개하기 위해 앱을 다시 실행해야 합니다.

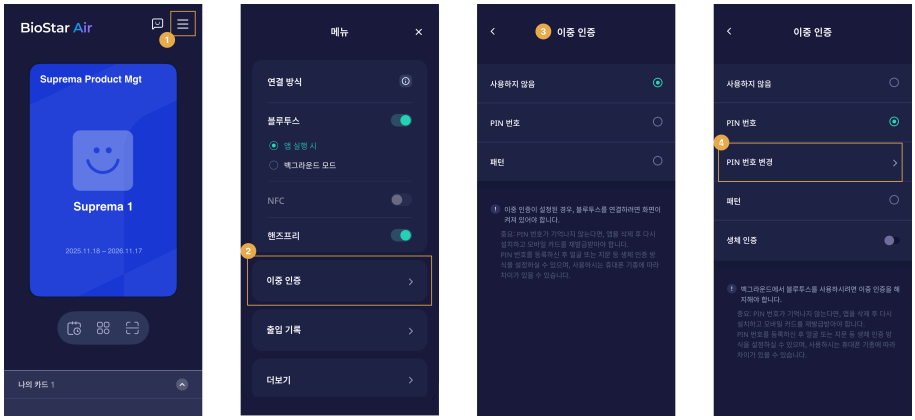
NFC

NFC 인증은 안드로이드 기기에서만 사용할 수 있습니다. 사용자는 더 빠른 출입을 위해 NFC를 단독으로 사용하거나 블루투스와 함께 사용할 수 있습니다.

> **알아두기**
> NFC 호환 장치를 사용하는 안드로이드 사용자는 블루투스와 함께 NFC를 사용할 수 있습니다.

이중 인증(2FA)

추가 보안을 위해 사용자는 **PIN, 패턴 또는 생체 인식 인증**(얼굴 또는 지문)을 사용하여 이중 인증을 활성화할 수 있습니다.



알아두기

- 이 기능은 출입 인증 중에 앱 화면이 열려 있어야 하므로 **백그라운드 모드** 연결 방식에서는 지원하지 않습니다.
- PIN 또는 패턴을 잊어버렸다면 앱을 재설치하고 모바일 카드를 다시 활성화해야 합니다.
- 모바일 기기에 따라 지원하는 기능은 다를 수 있습니다.

iOS 사용자

1. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
2. 연결 방식을 **앱 실행 시**로 설정하세요.
3. **이중 인증**을 탭하세요.
4. **PIN 번호 등록**을 탭하세요.
5. 6자리 PIN 번호를 입력하세요.
6. 성공 알림 메시지가 나타나면 **OK**를 탭하세요.

알아두기

- PIN 번호를 변경하려면 **PIN 번호 변경**을 탭한 후 새 PIN 번호를 입력하세요.
- 생체 인식 기능을 사용하려면 **생체 인증**을 활성화하고 설정 안내를 따르세요.

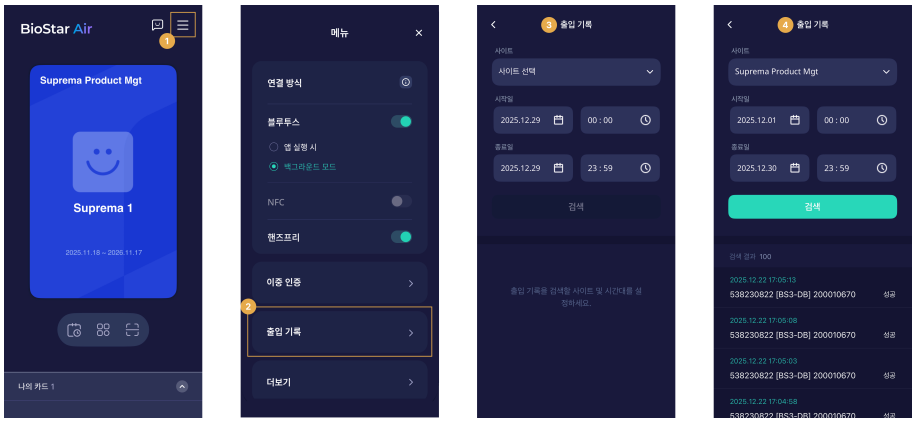
안드로이드 사용자

1. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
2. 연결 방식을 **앱 실행 시** 또는 **NFC**로 설정하세요.
3. **이중 인증**을 탭하세요.
4. **PIN 번호** → **PIN 번호 등록** 또는 **패턴** → **패턴 등록**을 탭하세요.
5. 선택한 PIN 번호 또는 패턴을 입력하세요.
6. 성공 알림 메시지가 나타나면 **OK**를 탭하세요.

> **알아두기**
>
> - PIN 번호를 변경하려면 **PIN 번호 변경**을 탭한 후 새 PIN 번호를 입력하세요.
> - 패턴을 변경하려면 **패턴 변경**을 탭한 후 새 패턴을 입력하세요.
> - 생체 인식 기능을 사용하려면 **생체 인증**를 활성화하고 설정 안내를 따르세요.

출입 로그

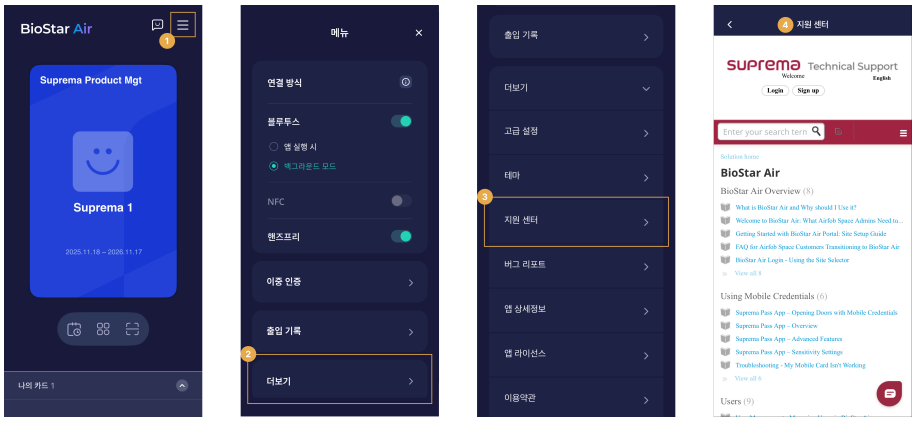
출입 기록을 통해서 사용자의 출입 시도를 추적하고 출입 관련 문제를 해결할 수 있습니다.



1. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
2. **출입 기록**을 탭하세요.
3. 사이트를 선택하고, 시작일과 종료일을 설정하세요.
4. **검색** 버튼을 탭하세요.

지원 센터

추가 지원이 필요한 사용자는 **지원 센터**로 진입하여 도움을 받을 수 있습니다.



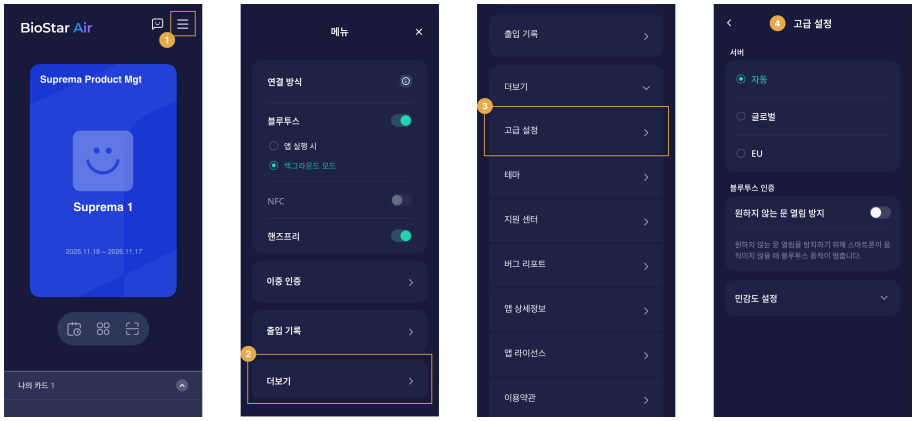
1. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
2. **더보기**를 탭하세요.
3. **지원 센터**를 탭하세요.

4. **슈프리마 Technical Support** 페이지로 이동합니다.

- 궁금한 사항을 검색하거나 자주 묻는 질문을 확인하세요.
- 지원이 필요하다면 오른쪽 하단의 채팅 아이콘을 탭하여 모카(MOCA) 시스템 팀에 지원 티켓을 제출할 수 있습니다.

고급 설정

슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭한 후 **더보기** → **고급 설정**에서 다음 추가 기능을 사용할 수 있습니다.



- **위치 설정**: 사용자의 위치에 따라 **글로벌** 또는 **EU** 서버 중 하나를 선택하세요. **자동**을 선택하면 앱이 위치를 감지하여 적절한 서버를 선택합니다.
- **블루투스 인증**: 모바일 기가가 움직이지 않을 때 블루투스 인증이 작동하지 않도록 하려면 **원하지 않는 문 열림 방지** 옵션을 활성화하세요.
- **민감도 설정**: 모바일 기기와 BioStar Air와 호환되는 장치 간의 블루투스 인식 감도를 조정할 수 있습니다. 자세한 내용은 민감도 설정하기를 참고하세요.

추가 기능

슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭한 후 **더보기**에서 다음 추가 기능을 사용할 수 있습니다.

- **테마**: 앱의 색상 모드를 설정할 수 있습니다. **라이트** 또는 **다크**, **시스템** 모드를 선택할 수 있습니다.
- **버그 리포트**: 오류 발생 상황과 재현 방법 등의 세부 내용을 작성하여 개발자에게 버그 보고서를 제출할 수 있습니다.
- **앱 상세정보**: 모바일 기기의 모델 이름, OS 버전, BLE 지원 및 상태 등의 관련 정보를 확인할 수 있습니다.
- **앱 라이선스**: 슈프리마 패스 앱에 적용되는 오픈 소스 라이선스 정보를 확인할 수 있습니다.
- **이용 약관**: BioStar Air 플랫폼의 이용 약관을 확인할 수 있습니다.

민감도 설정하기

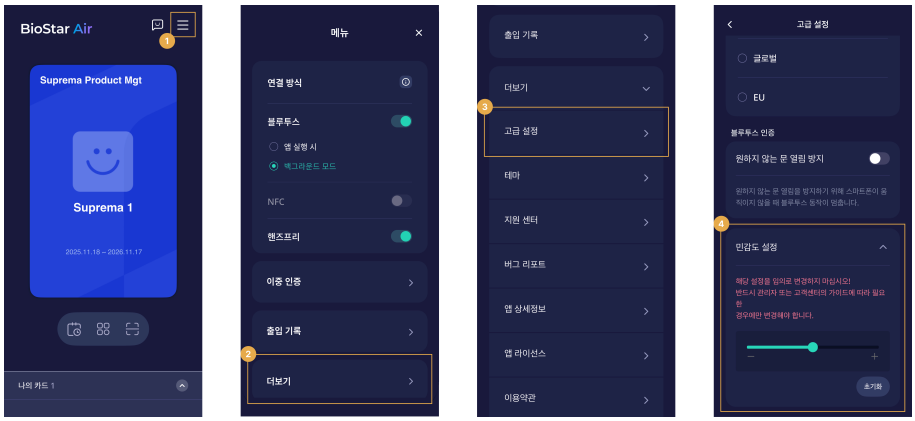
민감도 설정 기능을 사용하면 사용자는 모바일 기기와 BioStar Air와 호환되는 장치 간의 블루투스 인식 감도를 조정할 수 있습니다. 이 기능은 원활한 인증을 보장하고 원치 않는 접근 시도나 인증 실패를 줄이는 데 유용합니다.

알아두기

모바일 기기 모델마다 블루투스 신호 강도가 다르기 때문에 사용자는 서로 다른 인식 거리를 경험할 수 있습니다. 또한 벽, 간섭 또는 BioStar Air와 호환되는 장치의 배치와 같은 환경적 요인이 블루투스 인식에 영향을 줄 수 있습니다.

감도 설정 조정 방법

사용자는 모바일 기기의 블루투스 강도와 개인적 선호도에 따라 블루투스 인증 민감도를 미세하게 조정할 수 있습니다.



1. 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
2. **더보기**를 탭하세요.
3. **고급 설정**을 탭하세요.
4. **민감도 설정**을 탭한 후 슬라이더를 이동하여 감도를 조정하세요.

알아두기

- 의도하지 않은 인증을 방지하려면 － 방향으로 슬라이더를 이동해 감도를 낮추세요.

  > *예, 모바일 기기가 책상에 있을 때*

- 인증을 실패하면 ＋ 방향으로 슬라이더를 이동해 감도를 높이세요. 단, 모바일 기기가 BioStar Air와 호환되는 장치에 매우 가까이 있어야 합니다.

팁

iOS 사용자 팁

Apple Pay를 사용하는 아이폰을 BioStar Air와 호환되는 장치에 가까이 가져가면 Apple Pay가 실행됩니다. 이는 모바일 기기의 NFC 영역이 모바일 카드 인증과 함께 감지되기 때문입니다.

해결 방법: 감도 설정을 ＋ 방향으로 조정하면 BioStar Air와 호환되는 장치가 모바일 기기의 블루투스 신호를 더 일찍 인식하여 장치에 물리적으로 접촉할 필요가 없습니다. 이를 통해 Apple Pay가 트리거되는 것을 방지하면서 원활하게 출입할 수 있습니다.

개발자

BioStar Air는 클라우드 기반 RESTful API를 제공합니다. 외부 시스템과의 연동, 사용자 라이프사이클 자동화, 크리덴셜 관리를 API로 처리할 수 있습니다. 데모 환경을 구성하고 인증 흐름을 이해한 뒤, 사용자 관리 API로 실제 통합을 구현하세요.

빠른 시작하기

BioStar Air 데모 사이트를 설정하고 호환 장치를 연결·등록하여 클라우드 API 통합을 테스트하는 방법을 안내합니다. BioStar 2에서 작업한 경험이 있다면 많은 개념이 친숙하게 느껴질 것입니다. BioStar Air는 완전한 클라우드 기반 시스템입니다.

사전 요구 사항

시작하기 전에 다음 사항을 확인하세요.

- 공장 초기화된 펌웨어를 설치한 **BioStar Air 호환 장치**를 준비하세요.
  - XP2-AIR, XS2-AIR, BEW3-AIR, BS3-AIR, BLN2-AIR
  - 장치는 공인 슈프리마 대리점을 통해 구매할 수 있습니다.
- 장치는 이더넷을 통해 인터넷에 연결되어 있어야 합니다.
- 네트워크에서 아웃바운드 액세스를 허용하세요.
  - Port 443 (HTTPS)
  - Port 5671 (MQTT over TLS)

데모 환경과 API 키 설정

1 회원 가입 및 로그인

1. BioStar Air Developer로 이동하세요.
2. **회원 가입**을 클릭하고 양식을 작성한 후 승인을 기다리세요.
3. 승인이 완료되면 사용자 이메일 주소와 비밀번호를 사용해 개발자 포털에 로그인하세요.

> **알아두기**
> 개발자 포털의 이메일 주소와 비밀번호는 데모 포털에서 사용할 수 없습니다.

2 데모 애플리케이션 생성

1. **API → Management**로 이동하세요.

2. **+ Register** 버튼을 클릭하세요.
3. 애플리케이션 유형을 **Demo**로 선택하세요.
4. 애플리케이션 이름을 입력하고 **Register** 버튼을 클릭하세요.
5. 데모 애플리케이션 등록을 완료하면 *site_info.csv* 파일을 다운로드할 수 있습니다.

> **알아두기**
>
> - *site_info.csv* 파일에는 별칭 이메일 주소와 비밀번호가 포함되어 있습니다.
> - 데모 포털에 로그인할 때는 반드시 이 별칭 이메일과 비밀번호를 사용해야 합니다.
> - **개발자 포털에서 로그인하는 이메일 주소와 비밀번호를 데모 포털에서 사용하지 마세요.**

3 API 키 발급

1. **API** → **Management**로 이동하세요.
2. 등록된 애플리케이션을 클릭하세요.
3. **API Management**로 스크롤하세요.
4. **Add** 버튼을 클릭하세요.
5. 이름을 입력하고 확인하세요.
6. 생성된 API 키를 복사하고 안전하게 저장하세요.

이 API 키를 사용하여 데모 환경에 대한 API 요청을 인증할 수 있습니다.

4 데모 포털 로그인

1. 개발자 포털의 메뉴에서 **Demo Portal**을 클릭하거나 https://demo.airfobspace.com/login 주소로 직접 이동하세요.
2. *site_info.csv* 파일에 있는 별칭 이메일과 비밀번호로 로그인하세요.

> **알아두기**
> **개발자 포털에서 로그인하는 이메일 주소와 비밀번호를 데모 포털에서 사용하지 마세요.**

장치 등록

모바일 기기에 BioStar Air Demo App(안드로이드 전용)을 사용하세요.

1. BioStar Air Developers 링크로 이동해 데모 앱을 다운로드하세요.
2. 데모 앱을 실행하고, *site_info.csv* 파일에 있는 별칭 이메일과 비밀번호로 로그인하세요.
3. 안드로이드 환경의 모바일 기기를 리더기 근처(BLE 범위)로 가져가세요.

- **All Menu** → **Devices**에서 오른쪽 상단의 ＋ 버튼을 탭하세요.
- 장치를 검색하고 **Register** 버튼을 탭하세요.

4. 장치에서 소리가 나고 재부팅되며 등록된 장치 목록에 나타납니다.

> **알아두기**
> 장치는 모바일 앱을 통해서만 등록할 수 있습니다. 웹 포털에서는 등록할 수 없습니다. API 기반 등록에는 파트너에게 제공되지 않는 암호화 인증서가 필요합니다.

장치 관리

데모 앱 또는 데모 웹 포털에서 장치를 관리할 수 있습니다.

- **BioStar Air Demo App**
- **Demo Web Portal**: https://demo.airfobspace.com/login

Demo vs Production

- 테스트를 위한 **Demo** 사이트는 개발자 포털을 통해 생성됩니다.
- **Production** 사이트는 파트너 포털을 통해 생성되며 사이트 ID, 사용자 이메일 및 비밀번호가 필요합니다. Production 사이트는 승인된 판매자 또는 슈프리마 지사만 생성할 수 있습니다.

> **알아두기**
> - 사용자 ID와 계정 ID는 다릅니다. 혼동하지 마세요.
> - 여러 사이트를 관리한다면 비밀번호를 안전하게 저장하세요.
> - 항상 최신 Bearer 토큰을 사용하세요.
> - 브라우저에서 복사한 Bearer 토큰은 Postman에서 재사용할 수 있습니다.

도움이 필요하세요?

슈프리마 기술 지원 포털에서 티켓을 여세요. https://support.supremainc.com

API 인증하기

BioStar Air Cloud API는 Bearer 토큰(JWT) 기반 인증을 사용합니다. API를 호출하기 전에 로그인 절차를 통해 토큰을 발급받아야 하며, 모든 요청의 Authorization 헤더에 토큰을 포함해야 합니다.

API Base URLs

환경	Base URL	설명
Demo(TEST)	https://sp-demo-api.airfob.com/v1	애플리케이션 유형을 'Demo'로 등록하면 데모 환경 사이트와 사이트 마스터 계정 정보를 csv 파일로 다운로드할 수 있습니다.
Production (LIVE)	https://sp-api.airfob.com/v1	(**자동 라우팅**) 클라이언트 지역에 따라 글로벌 또는 EU 서버를 자동 선택합니다.
	https://sp-a-api.airfob.com/v1	(**글로벌 전용**) 글로벌 서버 환경으로 연결됩니다.
	https://sp-e-api.airfob.com/v1	(**EU 전용**) EU 서버 환경으로 연결됩니다.

> **자동 라우팅** 환경은 지역 감지에 따라 예상치 못한 라우팅(routing)이 발생할 수 있습니다.

API 로그인 절차

Postman 또는 프로그래밍 방식으로 API 호출을 수행할 수 있습니다.

로그인

- **Endpoint**: `login`
- **Payload**:

```
{
  "username": "your_email",
  "password": "your_password"
}
```

Bearer 토큰(JWT)을 반환합니다.

계정 정보 조회

- **Endpoint**: `getSelfAccounts`
- **Authorization**: Bearer Token

접근 가능한 사이트 및 계정 목록을 반환합니다.

계정에 로그인

- **Endpoint**: `loginAccount`
- **Authorization**: Bearer Token

특정 사이트 토큰을 반환합니다.

웹 브라우저에서 Bearer 토큰 얻는 방법

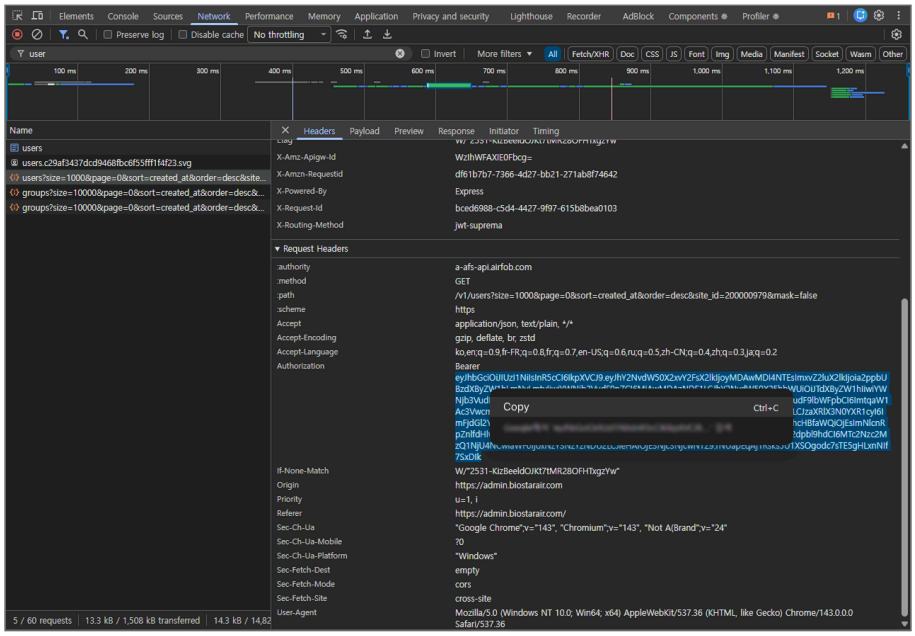
Postman 없이 브라우저 개발자 도구를 사용해 Bearer 토큰을 직접 얻을 수 있습니다.

Chrome/Edge (Windows 또는 Mac)

1. 웹 브라우저에서 `F12` 또는 `Ctrl/Cmd + Shift + I`를 누르세요.
2. **Network** 탭으로 이동하세요.
3. 페이지를 새로 고침하세요.
4. API 호출을 검색하세요.

   > 예, *groups*, *login*

5. 목록에서 요청을 클릭하세요.
6. **Headers** 탭으로 이동하세요.
7. 요청 헤더에서 `Authorization: Bearer ...`를 찾으세요.
8. 오른쪽 마우스를 클릭하여 토큰을 복사하세요.



Safari (Mac)

1. **개발자** 메뉴를 활성화하세요. Safari → Preferences → Advanced → **Show Develop menu**를 체크하세요.
2. **Develop** → **Show Web Inspector**으로 이동하세요.
3. **Network** 탭으로 이동하세요.
4. 페이지를 새로 고침하세요.
5. API 호출을 필터링하고 검사하세요.

6. 요청 헤더에서 `Authorization: Bearer` 토큰을 복사하세요.

> **알아두기**
> 브라우저에서 복사한 Bearer 토큰은 Postman에서 재사용할 수 있습니다. 항상 최신 토큰을 사용하세요.

사용자 관리 API 사용하기

인증 토큰을 발급받은 후에는 API를 통해 사용자 라이프사이클을 관리할 수 있습니다. 사용자 조회, 생성, 수정, 중단 등의 엔드포인트를 사용하여 BioStar Air 사이트의 사용자를 자동화된 방식으로 관리하세요.

권장 API 통합 범위

API 통합은 가능한 한 아래의 범위로 제한하세요.

- 사용자 라이프사이클(lifecycle) 관리(생성/업데이트/삭제)
- 자격 증명 관리(모바일, RF 카드, 생체 인식)

관리자가 기존 BioStar Air 웹 및 모바일 관리 앱을 사용할 수 있도록 허용하세요.

- 출입 등급
- 일정
- 출입문 및 장치 설정
- 사이트 설정

사용자 관리 API 호출

로그인 후 다음 엔드포인트를 사용하여 사용자를 관리하세요.

- `getUsers`
- `createUser`
- `updateUser`
- `suspendUsers`

항상 Authorization 헤더에 Bearer 토큰을 포함하세요.

> 사용자를 활성화하려면 최소한 하나의 크리덴셜 유형을 할당해야 합니다.
>
> > *예, RF 카드, 모바일, LinkPass*

애플리케이션 예제

다음은 API를 통해 CSV 파일을 업로드하고 사용자를 일괄 중단할 수 있는 Python 앱의 샘플 코드입니다.

Python

```
import requests
import csv
import getpass
from pathlib import Path

def select_server():
    servers = {
        "1": ("Demo", "https://demo-afs-api.airfob.com/v1"),
        "2": ("Global", "https://a-afs-api.airfob.com/v1"),
        "3": ("EU", "https://e-afs-api.airfob.com/v1")
    }

    print("Please select a server:")
    for key, (name, _) in servers.items():
        print(f"{key}: {name}")

    choice = input("Enter server number: ").strip()
    return servers.get(choice, (None, None))[1]

def login(base_url, username, password):
    url = f"{base_url}/login"
    payload = {"username": username, "password": password}
    response = requests.post(url, json=payload)
    response.raise_for_status()
    data = response.json()
    token = data.get("access_token")
    if not token:
        raise ValueError("Login succeeded but no access_token returned.")
    print("✅ Login successful.")
    return token

def login_to_account(base_url, token, account_id):
    url = f"{base_url}/login/{account_id}"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.post(url, headers=headers)
    response.raise_for_status()
    new_token = response.json().get("access_token")
    if new_token:
        print(f"✅ Switched to account ID: {account_id}")
        return new_token
    return token

def get_accounts(base_url, token):
    url = f"{base_url}/accounts/self"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.get(url, headers=headers)
    response.raise_for_status()
    accounts = response.json().get("accounts", [])
    return [{"id": acc["id"], "name": acc["site"]["name"]} for acc in accounts]

def suspend_users_from_csv(base_url, csv_path, token):
    if not Path(csv_path).exists():
        print(f"❌ File not found: {csv_path}")
        return

    headers = {"Authorization": f"Bearer {token}"}
```

```
    with open(csv_path, newline='', encoding='utf-8-sig') as f:
        reader = csv.DictReader(f)

        # Normalize headers
        reader.fieldnames = [field.strip().lower() for field in reader.fieldnames]
        if 'email' not in reader.fieldnames:
            print("❌ Missing required 'email' column in CSV.")
            return

        for row in reader:
            email = row.get("email")
            if not email:
                print("⚠️ Skipping row with missing email.")
                continue

            # Search user
            search_url = f"{base_url}/users/search"
            payload = {"filters": [{"field": "email", "equals": email}]}
            search_resp = requests.post(search_url, headers=headers, json=payload)
            if search_resp.status_code != 200:
                print(f"❌ Failed to search user {email}: {search_resp.text}")
                continue

            users = search_resp.json().get("users", [])
            if not users:
                print(f"❌ No user found with email: {email}")
                continue

            user_id = users[0]["id"]

            # Suspend user
            suspend_url = f"{base_url}/users/suspend"
            suspend_payload = {
                "ids": [user_id],
                "certify_by": "none",
                "use_site_template": True
            }
            suspend_resp = requests.post(suspend_url, headers=headers, json=suspend_payload)
            if suspend_resp.status_code == 200:
                print(f"✅ Suspended user: {email}")
            else:
                print(f"❌ Failed to suspend user {email}: {suspend_resp.text}")

def main():
    base_url = select_server()
    if not base_url:
        print("❌ Invalid selection. Exiting.")
        return

    print("\n🔑 BioStar Air Login")
    username = input("Email: ")
    password = getpass.getpass("Password: ")

    token = login(base_url, username, password)
    accounts = get_accounts(base_url, token)

    print("\n🌐 Available Sites:")
```

```
    for i, acc in enumerate(accounts):
        print(f"{i}: {acc['name']} (ID: {acc['id']})")

    selected = int(input("\nSelect site number to log into: "))
    account_id = accounts[selected]["id"]
    token = login_to_account(base_url, token, account_id)

    csv_path = input("Enter path to CSV file with user emails: ").strip()
    suspend_users_from_csv(base_url, csv_path, token)

if __name__ == "__main__":
    main()
```

문제 해결

BioStar Air를 사용하다가 예상치 못한 문제가 발생했나요? 이 문서에서는 BioStar Air 사용 중 자주 발생하는 문제들의 원인을 파악하고 해결하는 방법을 제공합니다.

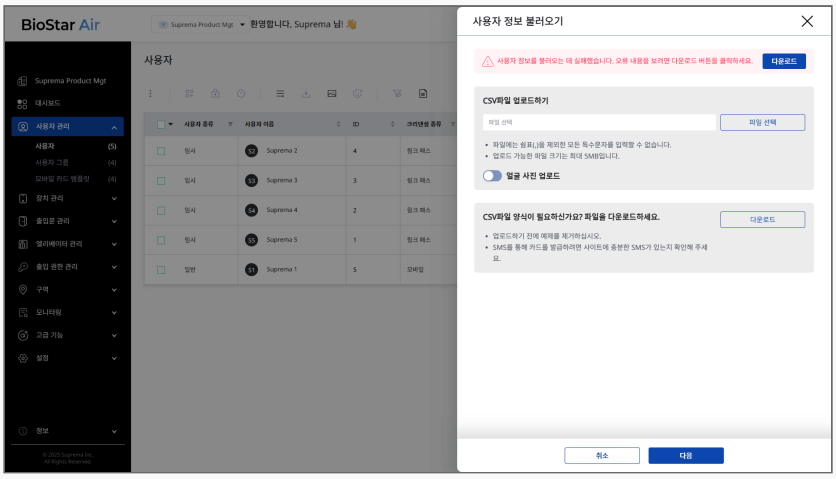
아래에 나열된 문제를 선택하고, 단계별 해결 방법을 확인하세요.

일괄 사용자 추가 문제

여러 고객과 파트너가 사용자 목록을 일괄 방식으로 추가할 때 문제를 보고했습니다. 대부분의 문제는 잘못된 형식의 CSV 파일에서 발생합니다. 일괄 추가 기능이 예상대로 작동하도록 아래 지침을 정확히 따르세요.

알아두기

v2.10부터 BioStar Air는 잘못된 항목이 포함된 CSV 파일을 업로드할 경우 검증 보고서를 반환합니다. 오류를 수정한 후 파일을 다시 업로드하세요.



CSV 파일 준비

CSV 템플릿 다운로드

1. 화면 왼쪽 사이드바에서 **사용자 관리** → **사용자**로 이동하세요.
2. 화면 오른쪽 상단의 **사용자 추가** → **사용자 정보 불러오기**를 클릭하세요.
3. **사용자 정보 불러오기** 패널이 나타나면 **다운로드** 버튼을 클릭하세요.
4. CSV 템플릿 파일(*biostar-import-user-csv-example.csv*)을 로컬에 저장하세요.

CSV 템플릿의 정확한 형식 사용

- **열(column)을 수동으로 추가하거나 삭제하지 마세요.** 예기치 않은 열(column)이 있다면 오류가 발생할 수 있습니다.
- 추가 필드(예: 직원 ID 또는 부서)를 포함해야 한다면, 사용자 목록 상단의 **사용자 템플릿**() 기능을 이용해 해당 필드를 추가하세요.

필드를 추가하면 다운로드한 CSV 파일에 해당 열이 자동으로 포함됩니다.

각 열의 요구 사항을 참고하여 데이터를 올바르게 입력하세요.

사용자 키

- 각 사용자의 고유한 숫자 ID입니다.
- **사용자 키** 열은 **비워둘 수 있으며** 시스템에서 자동으로 값을 할당합니다.
- 사용자 아이디를 직접 작성하는 경우
  - **숫자만** 사용하세요.
  - **고유한 값**을 사용하세요.
  - 문자, 공백, 하이픈 또는 특수 문자를 포함하지 마세요.

> **주의**
> 문자를 포함한 회사별 직원 ID를 사용하려 한다면 **사용자 키** 필드를 사용하지 마세요. 대신 **사용자 템플릿** 기능을 사용해 별도의 커스텀 사용자 필드를 만드세요.

이메일

- 유효한 이메일 형식을 사용하세요. 유효성 검사 수식을 참고하여 이메일 형식을 검증할 수 있습니다.
  - 공백은 포함할 수 없습니다.
  - 골뱅이 문자(`@`, at sign)를 포함해야 합니다.
  - 도메인에는 마침표(`.`) 및 최상위 도메인을 포함해야 합니다.

    > *예시: example.com, gmail.com, suprema.co.kr*

  - 주소 뒤에 추가 마침표가 없어야 합니다.
  - 특수 문자 또는 숨겨진 문자가 없어야 합니다.
  - 이메일 주소여야 합니다. '제공하지 않음' 또는 '제공되지 않음'과 같은 오류가 발생할 수 있습니다.
- 이메일 주소는 **고유해야 합니다**. 파일 내 또는 기존 사용자 간에 중복을 허용하지 않습니다.
- 아래 크리덴셜을 발급받는다면 이메일 주소는 필수로 입력해야 합니다.
  - **모바일 카드**
  - **웹 QR**
  - **링크 패스**
- RFID 카드만 가지고 있는 사용자는 이메일 주소를 입력할 필요가 없습니다.

휴대폰 번호

- 모바일 SMS를 통해 크리덴셜을 전달하지 않는다면 선택 사항입니다.
- 이메일 주소와 마찬가지로 **고유해야** 하며, 파일 내 또는 기존 사용자 간에 중복을 허용하지 않습니다.

- 크리덴셜 전달을 전달할 때는 이메일을 권장합니다. SMS 메시지는 추가 요금이 발생합니다.

날짜 (시작일 / 종료일)

모든 날짜 필드는 아래와 같은 정확한 형식을 따라야 합니다.

```
YYYY-MM-DDTHH:MM:SS.sssZ

Example:
1995-05-09T00:00:00.000Z
```

'Z'를 누락하거나, 대시(`—`) 대신 슬래시(`/`)를 사용하거나, 시간을 생략하는 등 사소한 차이도 업로드를 실패할 수 있습니다.

크리덴셜 요구 사항

크리덴셜 형식	이메일 또는 전화번호
RF 카드 Only	아니요.
모바일 카드 / **웹 QR** / **링크 패스**	예, 하나가 필요합니다.

- 크리덴셜은 이메일 주소 또는 전화번호로 전달되어야 합니다.
- 둘 다 제공할 수 있지만 **모바일 형식의 크리덴셜**에는 **최소 하나가 필요**합니다.
- 이메일은 무료입니다. SMS는 요금이 부과됩니다.

사전 검증을 위한 엑셀 수식

데이터를 업로드하기 전에 **helper columns**에서 다음 수식을 사용하여 데이터를 확인할 것을 권장합니다.

이메일 또는 전화번호 중복 검증

Detect Duplicate Emails or Phone Numbers

```
=IF(E2="", "", IF(COUNTIF(E$2:E2, E2)>1, "Duplicate", "First Occurrence"))
```

날짜 형식 검증

Validate ISO 8601 Date Format (Column Q)

```
=IF(Q2="", "", IF(AND(LEN(Q2)=24,
  ISNUMBER(VALUE(MID(Q2,1,4))), MID(Q2,5,1)="-",
  ISNUMBER(VALUE(MID(Q2,6,2))), MID(Q2,8,1)="-",
  ISNUMBER(VALUE(MID(Q2,9,2))), MID(Q2,11,1)="T",
  ISNUMBER(VALUE(MID(Q2,12,2))), MID(Q2,14,1)=":",
  ISNUMBER(VALUE(MID(Q2,15,2))), MID(Q2,17,1)=":",
  ISNUMBER(VALUE(MID(Q2,18,2))), MID(Q2,20,1)=".",
  ISNUMBER(VALUE(MID(Q2,21,3))), RIGHT(Q2,1)="Z"),
  "Valid", "Invalid"))
```

이메일 형식 검증

Validate Email Format (Column E)

```
=IF(TRIM(E2)="", "", IF(AND(
  ISNUMBER(FIND("@", E2)),
  ISNUMBER(FIND(".", E2)),
  FIND("@", E2) > 1,
  FIND(".", E2, FIND("@", E2)) > FIND("@", E2) + 1,
  LEN(E2) - LEN(SUBSTITUTE(E2, "@", "")) = 1,
  ISERROR(FIND(" ", E2))
), "Valid", "Invalid"))
```

에러가 발생하나요?

- 올바른 템플릿을 다운로드하고 추가 열을 추가하지 않았습니까?
- 모바일 크리덴셜을 받는 사용자에 대한 모든 필수 필드가 작성되었습니까?
- 이메일 주소와 전화번호가 파일 및 기존 사용자 간에 고유합니까?
- 날짜 및 이메일 형식이 위에 지정된 대로 정확합니까?

알아두기

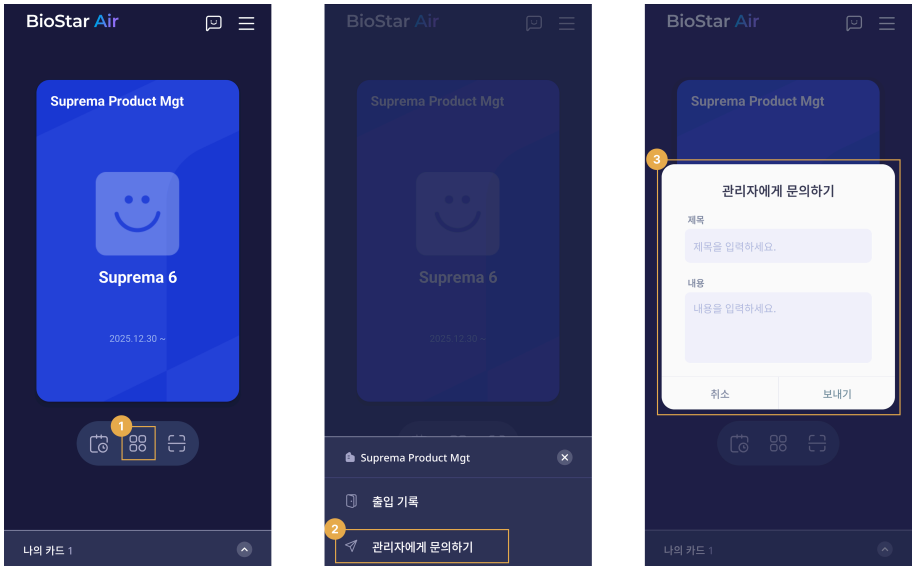
- 서비스팀은 파일 수정 서비스를 제공하지 않습니다. 파일이 업로드되지 않으면 위의 검증 도구를 사용하여 문제를 파악하고 해결하세요.
- 이 문서는 서비스 팀의 수동 문제 해결 없이도 업로드를 성공적으로 완료할 수 있도록 돕기 위해 작성되었습니다.

모바일 카드가 작동하지 않아요

모바일 카드가 장치와 인증되었지만 출입문이 열리지 않는다면 다음 안내를 따라 문제를 해결하세요.

BioStar Air 관리자에게 문의

사이트 관리자는 모바일 카드 재발급, 일시적인 모바일 기기 문제 및 설정 문제를 도와줄 수 있습니다.



1. 모바일 기기의 슈프리마 패스 앱에서 모바일 카드 아래에 위치한 아이콘을 탭하세요.
2. 하단의 패널이 나타나면 **관리자에게 문의하기**를 탭하세요.
3. 팝업창이 나타나면 제목과 내용을 작성하세요.
4. 메시지를 관리자에게 전송하려면 **보내기**를 탭하세요.

모바일 카드가 삭제되었나요?

모바일 기기를 변경하거나 슈프리마 패스 앱을 재설치했다면 보안상의 이유로 모든 모바일 카드가 삭제됩니다. 다음은 모바일 카드 재발급 문의처입니다.

- **Company Spaces**: HR, IT, 보안 또는 운영팀
- **Shared Spaces**: 지역 관리자 또는 고객 서비스 팀

> **알아두기**
> 관리자가 BioStar Air에서 사용자의 크리덴셜을 재발급하면 이전에 발급된 모바일 크리덴셜, QR 코드 및 링크패스(LinkPass)는 모두 취소되고 새 크리덴셜로 교체됩니다. 사용자는 사이트 설정에 따라 이메일 또는 SMS로 새 크리덴셜 링크를 받게 됩니다. 사용자는 해당 링크를 통해 슈프리마 패스 앱에 새 모바일 크리덴셜을 다운로드하거나 새 QR 코드 또는 링크패스를 이용해야 합니다. 취소된 모바일 크리덴셜, QR 코드 또는 링크패스로 출입을 시도하면 실패합니다.

단계별 문제 해결 안내

1 슈프리마 패스 앱에서 오류 메시지가 나타났나요?

- 출입문이 열리지 않는다면 슈프리마 패스 앱에서 다시 인증을 시도하세요.
- 에러 메시지가 나타나면 스크린샷을 캡쳐해 사이트 관리자에게 공유하세요.

2 모바일 기기의 블루투스가 켜져 있나요?

모바일 카드는 모바일 기기와 출입 통제 장치 간의 블루투스 통신에 의존합니다.

- 블루투스가 켜져 있는지 확인하세요.
- 블루투스를 껐다가 다시 켜보세요.
- 필요하다면 모바일 기기를 재시작하세요.

3 슈프리마 패스 앱의 위치 권한을 허용하세요

블루투스 및 NFC 인증에는 위치 권한이 필요합니다.

1. 모바일 기기의 **설정** → **앱**으로 이동하세요.
2. **슈프리마 패스** 앱을 선택하세요.
3. **권한** → **위치**에서 위치 액세스 권한을을 **항상 허용** 또는 **앱 사용 중에만 허용**으로 설정하세요.

4 무선 네트워크와 Wi-Fi 연결을 확인하세요

모바일 카드 인증을 위해서는 안정적인 무선 네트워크 또는 Wi-Fi 연결이 필요합니다.

5 선택한 연결 방법을 사용했나요?

슈프리마 패스 앱에서 연결 방식을 확인하세요.

- 슈프리마 패스 앱 초기화면에서 오른쪽 상단의 ☰ 아이콘을 탭하세요.
- **연결 방식**에서 인증 모드를 확인하세요.
- **백그라운드 모드**를 사용한다면 앱이 백그라운드에서 열려 있어야 합니다.

6 인증 시 모바일 기기에 진동이 발생했나요?

- 모바일 기기가 진동했지만 출입문이 열리지 않았다면 슈프리마 패스 앱을 열고 다시 인증을 시도하세요.
- 에러 메시지가 나타나면 스크린샷을 캡쳐해 사이트 관리자에게 공유하세요.

위치 서비스를 활성화해야 하나요?

모바일 기기의 슈프리마 패스 앱에서 모바일 출입 카드로 인증하려면 위치 서비스가 필요합니다. 이를 통해 모바일 기기와 출입 통제 장치 간의 안전한 블루투스 통신을 보장합니다.

Q. Airfob Space에서 BioStar Air로 전환해야 하나요?

아니요. 기존 Airfob Space 고객은 플랫폼을 그대로 사용할 수 있습니다. 현재 강제 마이그레이션은 없습니다.

Q. 내 장치나 데이터에 영향을 미치나요?

아니요. 두 플랫폼은 동일한 백엔드를 공유합니다. 장치, 사용자 데이터 및 구성은 두 서비스 간에 완전히 호환됩니다.

Q. 슈프리마 패스를 Airfob Space 앱 대신 사용해야 하나요?

기존 모바일 인증 사용자를 BioStar Air로 마이그레이션할 필요는 없습니다. app.airfobspace.com URL 또는 Airfob Pro 앱을 사용하여 사용자를 관리하고 모바일 인증을 발급하는 경우 해당 사용자는 Airfob Space 앱을 사용하기 위한 초대장을 받게 됩니다. admin.biostarair.com 또는 BioStar Air 앱을 사용하여 사용자를 관리하고 모바일 인증을 발급하는 경우 해당 사용자는 슈프리마 패스 앱을 사용하기 위한 초대장을 받게 됩니다.

Q. 고객 지원 또는 요금이 변경되나요?

고객 지원이나 요금 프로세스에 즉각적인 변경은 발생하지 않습니다. 그러나 시간이 지남에 따라 BioStar Air는 문서화, 고객 지원 및 기능 발표를 위한 주요 브랜드가 될 것입니다.

Q. 원한다면 BioStar Air로 전환할 수 있나요?

예. 백엔드가 공유되므로 전환은 간단하지만 일부 브랜딩 및 기능 제공 여부에 차이가 있을 수 있습니다. admin.biostarair.com 및 BioStar Air 앱을 사용하여 사이트 관리를 시작하세요. app.airfobspace.com의 기존 관리자 로그인 정보를 그대로 사용할 수 있습니다.

Q. BioStar Air의 이점은 무엇인가요?

BioStar Air는 미래 지향적인 브랜드입니다. 향후 개선 사항, 통합 향상, UI/UX 업데이트 그리고 Airfob Space로 다시 전환하지 않을 수 있는 새로운 기능을 지속적으로 개선시켜 나갈 것입니다.

Q. 향후 기능은 Airfob Space와 호환되나요?

일부는 호환되지만 모두는 아닙니다. 새로운 기능은 앞으로 BioStar Air에만 독점적일 수 있습니다. 최상의 경험과 지원을 위해 새로운 배포는 BioStar Air를 사용해야 합니다.

비디오 재생 관련 문제 해결

BioStar Air에 카메라를 등록한 후 녹화된 비디오가 재생되지 않으면 다음 단계에 따라 문제를 진단하고 해결하세요. 이 단계를 따르면 비디오 재생 문제를 해결하고 BioStar Air에서 제대로 작동하는지 확인할 수 있습니다.

> **알아두기**
> 카메라 등록에 대한 자세한 내용은 IP 카메라 지원 및 설정하기을 참고하세요.

Q. Airfob Space에서 BioStar Air로 전환해야 하나요?

아니요. 기존 Airfob Space 고객은 플랫폼을 그대로 사용할 수 있습니다. 현재 강제 마이그레이션은 없습니다.

Q. 내 장치나 데이터에 영향을 미치나요?

아니요. 두 플랫폼은 동일한 백엔드를 공유합니다. 장치, 사용자 데이터 및 구성은 두 서비스 간에 완전히 호환됩니다.

Q. 슈프리마 패스를 Airfob Space 앱 대신 사용해야 하나요?

기존 모바일 인증 사용자를 BioStar Air로 마이그레이션할 필요는 없습니다. app.airfobspace.com URL 또는 Airfob Pro 앱을 사용하여 사용자를 관리하고 모바일 인증을 발급하는 경우 해당 사용자는 Airfob Space 앱을 사용하기 위한 초대장을 받게 됩니다. admin.biostarair.com 또는 BioStar Air 앱을 사용하여 사용자를 관리하고 모바일 인증을 발급하는 경우 해당 사용자는 슈프리마 패스 앱을 사용하기 위한 초대장을 받게 됩니다.

Q. 고객 지원 또는 요금이 변경되나요?

고객 지원이나 요금 프로세스에 즉각적인 변경은 발생하지 않습니다. 그러나 시간이 지남에 따라 BioStar Air는 문서화, 고객 지원 및 기능 발표를 위한 주요 브랜드가 될 것입니다.

Q. 원한다면 BioStar Air로 전환할 수 있나요?

예. 백엔드가 공유되므로 전환은 간단하지만 일부 브랜딩 및 기능 제공 여부에 차이가 있을 수 있습니다. admin.biostarair.com 및 BioStar Air 앱을 사용하여 사이트 관리를 시작하세요. app.airfobspace.com의 기존 관리자 로그인 정보를 그대로 사용할 수 있습니다.

Q. BioStar Air의 이점은 무엇인가요?

BioStar Air는 미래 지향적인 브랜드입니다. 향후 개선 사항, 통합 향상, UI/UX 업데이트 그리고 Airfob Space로 다시 전환하지 않을 수 있는 새로운 기능을 지속적으로 개선시켜 나갈 것입니다.

Q. 향후 기능은 Airfob Space와 호환되나요?

일부는 호환되지만 모두는 아닙니다. 새로운 기능은 앞으로 BioStar Air에만 독점적일 수 있습니다. 최상의 경험과 지원을 위해 새로운 배포는 BioStar Air를 사용해야 합니다.

(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.