BioStar X Mobile

관리자 가이드

버전 1.0.5

한국어

KO 102.00.BSX

suprema
SECURITY & BIOMETRICS

목차

시작하기 전에 5

지원 환경 5

라이선스 및 네트워크 요구사항 5

시작하기 7

BioStar X 모바일 앱 다운로드 7

앱 권한 7

앱 시작 및 초기 설정 8

연결 문제 해결 8

앱 사용 9

앱 설정하기 10

앱 버전 정보 확인 10

로그인 설정 11

표준 시간대 설정 13

날짜 및 시간 표시 형식 설정 14

바이오메트릭으로 변경 사항 확인 14

라이선스 정보 및 개인정보 정책 확인 15

사용자 관리하기 16

사용자 등록하기 16

사용자 수정 및 삭제하기 30

사용자 로그 이벤트 조회하기 32

사용자 검색 및 필터링하기 33

출입문 관리하기 35

출입문 원격 제어하기 35

출입문 상세 정보 확인하기 37

장치 관리하기 41

장치 정보 확인 41

장치 상태 확인 41

인증 실패 잠금 해제 42

장치 검색 43

장치 목록 필터링 44

실시간 로그 모니터링 45

실시간 로그 조회 45

특정 로그만 보기 46

로그 상세 정보 확인 47

과거 로그 조회하기 48

과거 로그 조회 49

특정 로그만 보기 49

로그 상세 정보 확인 47

경보 알람 확인 및 해제하기 51

경보 알람 목록 (Alert List) 51

경보 알람 내역 (Alert History) 52

인원 점검(Roll Call) 시작하기 53

모바일 앱에서 인원 점검 사용 53

인원 점검 종료 60

퀵 액션 사용하기 63

퀵 액션 실행 63

퀵 액션 상세보기 63

계정 비밀번호 변경하기 65

부록 66

면책 조항 66

저작권 공지 67

오픈 소스 라이선스 67

시작하기 전에

BioStar X 모바일 앱을 사용하기 전에 다음 항목을 확인한 후 앱을 설치하세요.

지원 환경

다음 조건에서 BioStar X 모바일 앱을 사용할 수 있습니다.

- **지원 시스템**: BioStar X
- **서버 요구사항**: API 액세스가 가능한 BioStar X 서버 필요
- **사용자**: 지원되는 권한은 사전 정의된 모든 계정 레벨이며, 추후 사용자 지정 계정 레벨 지원을 추가할 예정
- **모바일 기기**: iOS 13.0 이상 또는 Android 7.0 이상

> **알아두기**
> BioStar X 모바일 앱은 독립적으로 작동할 수 없으며, 고객사 내부에 운영 중인 BioStar X 서버에 연결해야 합니다.
> - BioStar X 설치를 위한 최소 사양에 대한 자세한 내용은 시스템 최소 요구사항을 참고하세요.
> - BioStar X 설치에 대한 자세한 내용은 간편 설치하기을 참고하세요.

라이선스 및 네트워크 요구사항

BioStar X 모바일 앱을 사용하려면 BioStar X 라이선스가 필요합니다. 라이선스 추가 옵션을 구매해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

접속 환경	필요 라이선스
같은 네트워크	모바일 앱 라이선스
외부 네트워크(공용 IP)	모바일 앱 라이선스
외부 네트워크(공용 IP 없음)	모바일 앱 라이선스 + 리모트 액세스 라이선스

- BioStar X 서버와 모바일 앱을 연동해 사용하려면 **모바일 앱** 라이선스가 필요합니다.
- 기본적으로 같은 네트워크 내에서 BioStar X 서버에 연결하여 모바일 앱을 사용할 수 있습니다.
- 외부 네트워크에서 접속하려면 공용 IP 주소가 필요하며, 그렇지 않은 경우 **리모트 액세스** 라이선스를 추가 구매해야 합니다.

> **알아두기**
> - BioStar X에서 라이선스 적용 방법에 대한 자세한 내용은 BioStar X 라이선스를 참고하세요.
> - BioStar X 서버 설정에 대한 자세한 내용은 서버 상세 설정하기를 참고하세요.
> - BioStar X의 리모트 액세스 기능에 대한 자세한 내용은 리모트 액세스 설정하기를 참고하세요.

다음 단계

사전 준비를 완료했다면 BioStar X 모바일 앱 설치 방법을 확인하세요.

시작하기

BioStar X 모바일 앱은 iOS와 안드로이드에서 사용할 수 있습니다. 안내에 따라 앱을 설치한 후 BioStar X 서버에 연결하세요.

BioStar X 모바일 앱 다운로드

다음 제공하는 링크 또는 QR 코드를 통해 앱을 다운로드하세요.

플랫폼	다운로드 링크	QR 코드
iOS	App Store	
안드로이드	Google Play	

앱 권한

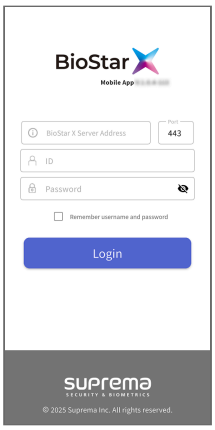
BioStar X 모바일 앱은 특정 기능 사용 시 다음 권한을 요청합니다. 최초 설치 시에는 권한을 요청하지 않습니다.

권한	필수 여부	용도
저장공간	선택 사항	사용자 이미지(예: 갤러리 또는 기기 저장소)를 관리하고 업로드하는 데 필요합니다.
카메라	선택 사항	얼굴 이미지 등록 및 비디오 녹화를 위한 이미지 캡처에 사용합니다.
생체 인식	선택 사항	모바일 기기 지문 또는 얼굴 인식을 사용한 보안 로그인에 필요합니다.

알아두기
모든 권한은 필수가 아니며, 사용자는 앱의 기본 기능에 영향을 미치지 않고 권한을 선택적으로 거부할 수 있습니다.

앱 시작 및 초기 설정

앱을 시작하면 BioStar X 서버 연결을 위한 정보를 입력하는 화면이 표시됩니다.



- **BioStar X Server Address**: BioStar X 서버의 IP 주소 또는 도메인 주소를 입력하세요.
- **Port**: BioStar X 서버의 포트 번호를 입력하세요. 기본값은 `443` 입니다.
- **ID** / **Password**: BioStar X 서버에 로그인하기 위한 아이디와 비밀번호를 입력하세요.

필요한 정보를 모두 입력한 후 로그인하려면 **Login**을 탭하세요.

알아두기
- 계정 아이디와 비밀번호를 입력 필드에 저장하려면 **Remember username and password** 옵션의 체크박스를 선택하세요. 다음 로그인 시 입력한 아이디와 비밀번호가 자동으로 채워집니다.
- BioStar X 서버의 IP 주소, 포트 번호를 확인하려면 서버 상세 설정하기를 참고하세요.

연결 문제 해결

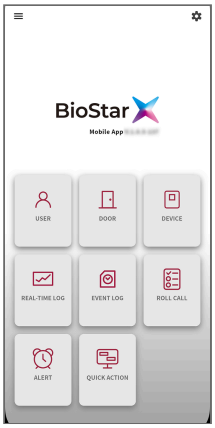
로그인에 실패했다면 아래 사항을 확인하세요.

- BioStar X 서버 주소와 포트 번호가 올바른지 확인하세요.
- 계정 아이디와 비밀번호가 올바른지 확인하세요.
- 모바일 기기와 BioStar X가 네트워크에 연결되어 있는지 확인하세요.

알아두기
외부 네트워크에서 접속하려면 공용 IP 주소가 필요하며, 그렇지 않은 경우 **리모트 액세스** 라이선스를 추가 구매해야 합니다. 자세한 내용은 시작하기 전에를 참고하세요.

앱 사용

로그인에 성공하면 BioStar X 모바일 앱의 홈 화면이 표시됩니다. 홈 화면에서는 등록된 사용자, 출입문, 실시간 로그, 이벤트 로그 및 경보를 확인할 수 있습니다. 또한 사이드 메뉴와 설정 메뉴에 접근할 수 있습니다.

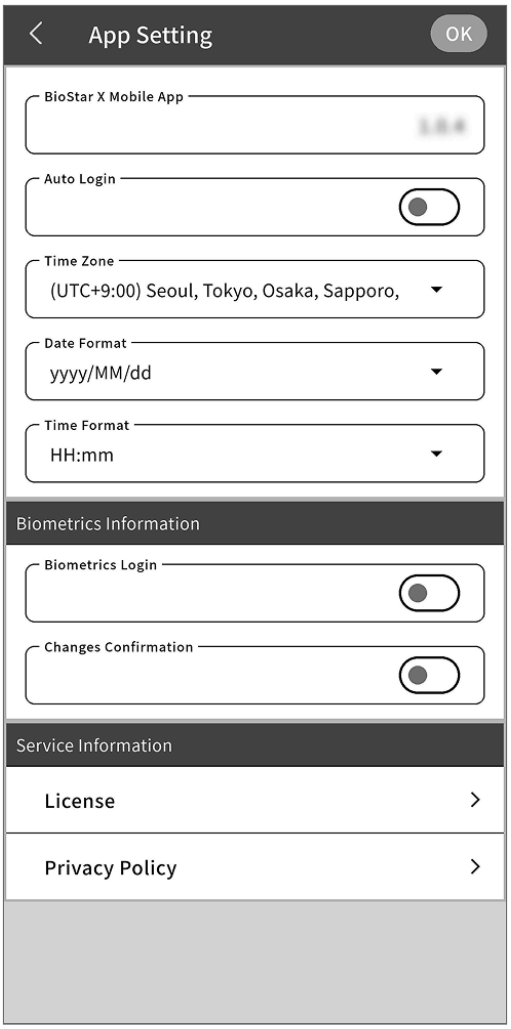


- ☰: 사이드 메뉴를 열 수 있습니다. 사이드 메뉴에서는 비밀번호를 변경하거나 로그아웃할 수 있으며, 주요 메뉴에 접근할 수 있습니다.
- ⚙: 설정 메뉴를 열 수 있습니다. 앱 설정에 대한 자세한 내용은 앱 설정하기를 참고하세요.
- **USER**: 등록된 사용자 목록을 확인하고, 사용자를 관리할 수 있습니다. 사용자 관리에 대한 자세한 내용은 사용자 관리하기를 참고하세요.
- **DOOR**: 등록된 출입문 목록을 확인하고, 원격으로 제어할 수 있습니다. 출입문 관리에 대한 자세한 내용은 출입문 관리하기를 참고하세요.
- **DEVICE**: 등록된 장치 목록에서 장치 상태를 확인하고, 잠금 상태의 장치를 원격으로 해제할 수 있습니다. 장치 관리에 대한 자세한 내용은 장치 관리하기를 참고하세요.
- **REAL-TIME LOG**: 실시간 출입 이벤트 로그를 확인할 수 있습니다. 실시간 로그 모니터링에 대한 자세한 내용은 실시간 로그 모니터링을 참고하세요.
- **EVENT LOG**: BioStar X 서버에 저장된 모든 이벤트 로그를 확인할 수 있습니다. 로그 조회에 대한 자세한 내용은 과거 로그 조회하기를 참고하세요.
- **ROLL CALL**: 위급 상황이 발생할 때, 사용자가 미리 지정된 장소의 입실 또는 퇴실 장치를 통해 인증하고 인원 점검 장소로 도착했는지를 파악할 수 있습니다. 인원 점검(Roll Call) 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 인원 점검 기능에 대한 자세한 내용은 인원 점검(Roll Call) 시작하기를 참고하세요.
- **ALERT**: 출입문 및 장치, 고급 출입 통제 경보 알람을 확인할 수 있습니다. 경보 알람에 대한 자세한 내용은 경보 설정하기를 참고하세요.
- **QUICK ACTION**: 긴급 상황에서 복잡한 제어 절차를 자동화하는 기능입니다. 미리 정의한 여러 기기의 동작을 하나의 버튼으로 즉시 실행하여 신속하게 대응할 수 있습니다. BioStar X 웹 인터페이스에서 퀵 액션을 생성해야 모바일 앱에서 사용할 수 있습니다. **퀵 액션** 기능에 대한 자세한 내용은 퀵 액션 사용하기를 참고하세요.

> **알아두기**
>
> 모든 기능은 사이드 메뉴(☰)를 통해서도 접근할 수 있습니다.

앱 설정하기

BioStar X 모바일 앱의 설정 메뉴에서 로그인, 시간대, 보안 등 앱의 주요 기능을 관리할 수 있습니다. 앱 설정 메뉴에 접근하려면 홈 화면의 오른쪽 상단에서 ⚙를 탭하세요.



앱 버전 정보 확인

BioStar X Mobile App 항목에서 현재 설치된 BioStar X 모바일 앱의 버전 정보를 확인할 수 있습니다. 설치한 앱이 최신 버전인지 확인하려면 **BioStar X Mobile App** 항목을 탭하세요.

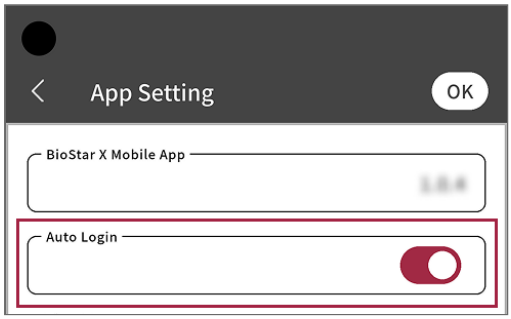
> **알아두기**
> 앱 버전 정보는 문제 해결 시 지원팀에 문의할 때 유용하게 사용할 수 있습니다.

로그인 설정

자동 로그인 설정

사용자가 앱을 열거나 세션 시간이 만료된 후 다시 로그인할 때마다 로그인 정보를 입력하는 대신 자동 로그인 기능을 활성화할 수 있습니다.

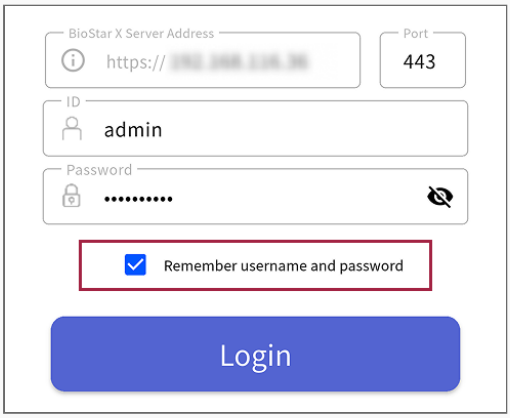
1. 자동 로그인 기능을 활성화하려면 **Auto Login** 옵션을 활성화하세요.



2. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
3. 확인 메시지가 나타나면 **Yes**를 탭하세요.

알아두기

- 자동 로그인 기능은 로그인 화면에서 **Remember username and password** 옵션이 활성화되어야 사용할 수 있습니다. 이 옵션이 활성화되지 않은 경우 자동 로그인 기능을 사용할 수 없습니다.

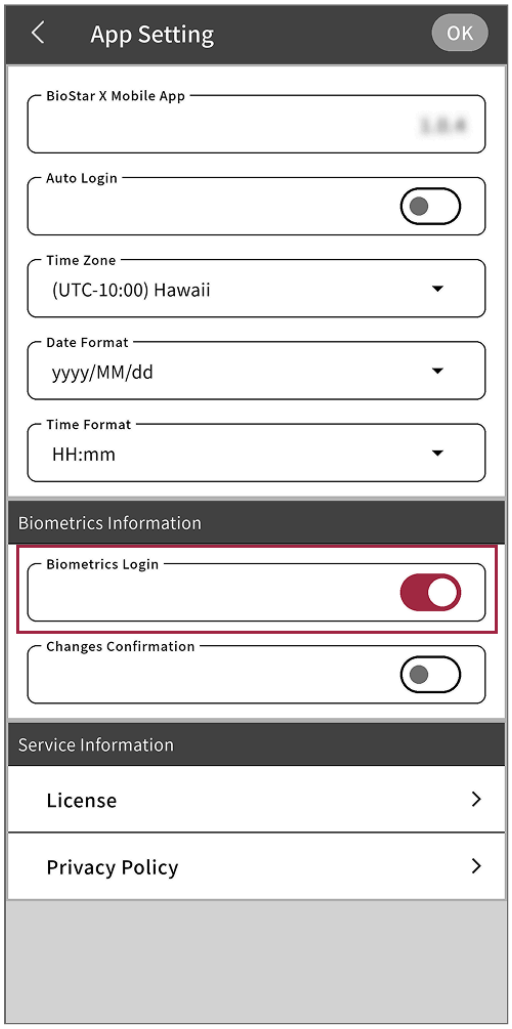


- 자동 로그인 기능이 활성화되어 있으면, 로그아웃할 수 없습니다. 로그아웃하려면 자동 로그인 기능을 비활성화한 후 로그아웃하세요.

바이오메트릭 로그인 설정

바이오메트릭 기능이 있는 모바일 기기에서는 바이오메트릭 로그인 기능을 활성화할 수 있습니다. 이 기능을 활성화하면 사용자는 아이디와 비밀번호 대신 모바일 기기에 등록된 지문인식을 사용해 로그인할 수 있습니다.

1. 바이오메트릭 로그인 기능을 활성화하려면 **Biometrics Information** → **Biometrics Login** 항목을 탭하세요.



2. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
3. 확인 메시지가 나타나면 **Yes**를 탭하세요.

로그인 화면에서 생체인식 기능을 사용할 수 있습니다.

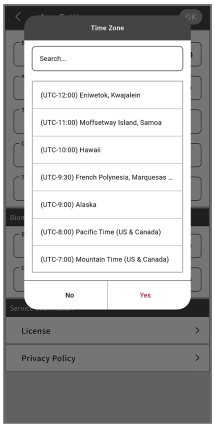


알아두기

이 기능은 모바일 기기에 생체 인식 기능이 있어야 하며, 로그인 화면에서 **Remember username and password** 옵션이 활성화되어야 사용할 수 있습니다.

표준 시간대 설정

BioStar X 서버가 설치된 위치에 해당하는 시간대를 설정할 수 있습니다. 올바른 시간대 설정은 이벤트 로그 및 알림의 정확한 시간 기록에 중요합니다.

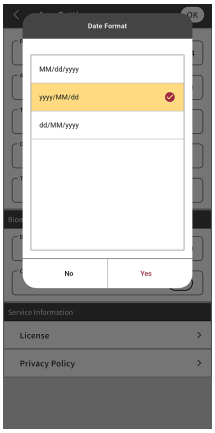


1. **Time Zone**을 탭하세요.
2. 시간대 목록에서 BioStar X 서버가 설치된 위치에 해당하는 시간대를 선택하세요.
3. **Yes**를 탭하세요.
4. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
5. 확인 메시지가 나타나면 **Yes**를 탭하세요.

> **알아두기**
> 변경된 사항은 BioStar X 서버에도 적용되며, 앱에서 표시되는 이벤트 로그 및 알림의 시간 기록이 변경된 시간대를 반영합니다.

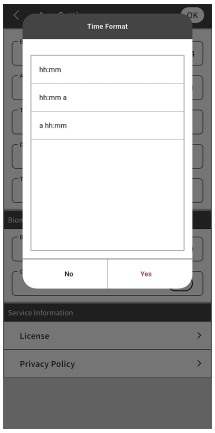
날짜 및 시간 표시 형식 설정

시스템 전체에서 사용할 날짜와 시간 표시 형식을 설정할 수 있습니다.



날짜 표시 형식

1. **Date Format**을 탭하세요.
2. **Date Format** 목록에서 원하는 날짜 표시 형식을 선택하세요.
   - **MM/dd/yyyy**: 01/31/2025
   - **yyyy/MM/dd**: 2025/01/31
   - **dd/MM/yyyy**: 31/01/2025
3. **Yes**를 탭하세요.
4. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
5. 확인 메시지가 나타나면 **Yes**를 탭하세요.

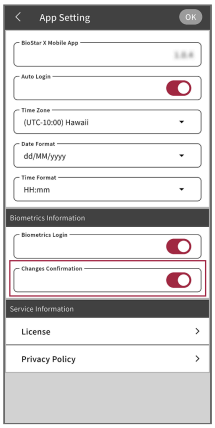


시간 표시 형식

1. **Time Format**을 탭하세요.
2. **Time Format** 목록에서 원하는 시간 표시 형식을 선택하세요.
   - **hh:mm**: 23:59, 24시간 형식
   - **hh:mm a**: 11:59 PM, 12시간 형식
   - **a hh:mm**: PM 11:59, 12시간 형식
3. **Yes**를 탭하세요.
4. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
5. 확인 메시지가 나타나면 **Yes**를 탭하세요.

바이오메트릭으로 변경 사항 확인

중요한 시스템 변경을 수행할 때 바이오메트릭 인증을 추가 요구할 수 있습니다. 이를 통해 다른 사용자에 의한 무단 변경을 방지할 수 있습니다.

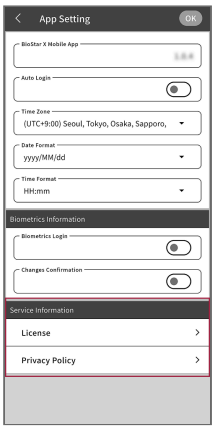


1. **Biometrics Information** → **Changes Confirmation** 항목을 탭하세요.
2. 변경 사항을 저장하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
3. 확인 메시지가 나타나면 **Yes**를 탭하세요.

바이오메트릭 인증이 필요한 변경 사항은 아래와 같습니다.

- 계정 비밀번호 변경
- 앱 설정 변경
- 새 사용자 등록
- 사용자 정보 수정
- 사용자 삭제

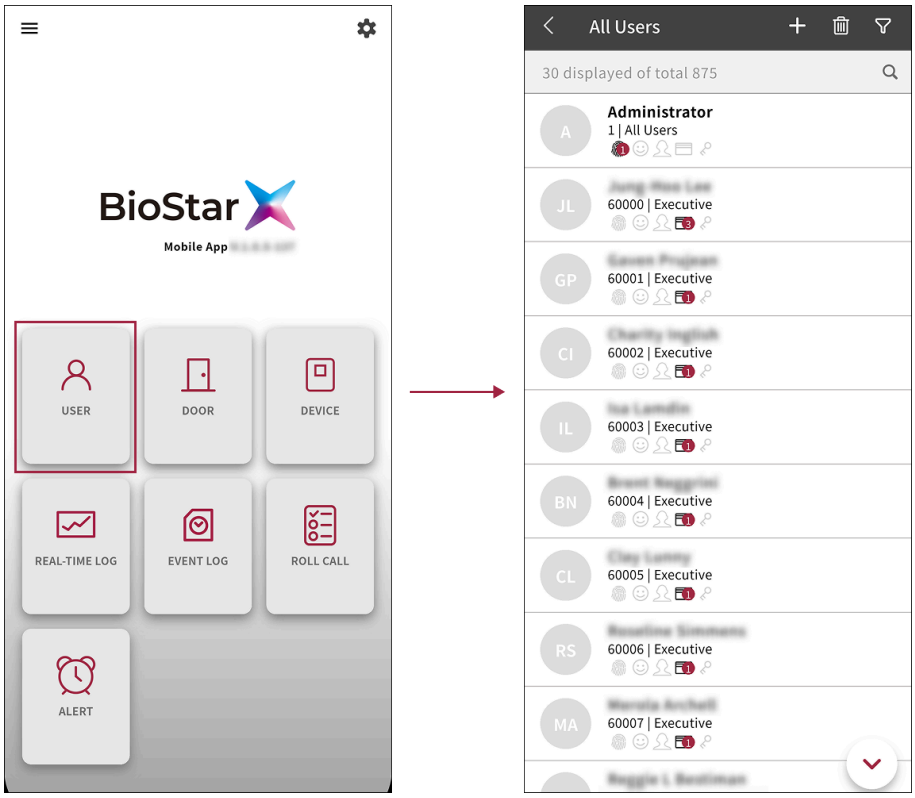
라이선스 정보 및 개인정보 정책 확인



- BioStar X 모바일 앱에 적용된 라이선스 정보를 확인하려면 **Service Information** → **License**를 탭하세요.
- 슈프리마의 개인정보 보호 정책을 확인하려면 **Service Information** → **Privacy Policy**를 탭하세요. 앱에서 제공하는 링크를 통해 슈프리마의 공식 웹사이트에 게시된 개인정보 보호 정책을 확인할 수 있습니다.

사용자 관리하기

새로운 사용자를 등록하거나 퇴사자를 삭제하고, 사용자 정보를 변경해야 할 때는 사용자 목록에서 관리할 수 있습니다. 사용자 검색 및 로그 조회도 함께 지원합니다.

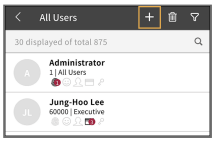


알아두기

BioStar X에서 사용자 관리에 대한 자세한 내용은 사용자를 참고하세요.

사용자 등록하기

새로운 사용자나 임시 방문자를 시스템에 추가해야 할 때, 기본 정보와 권한, 인증 수단을 함께 등록할 수 있습니다.

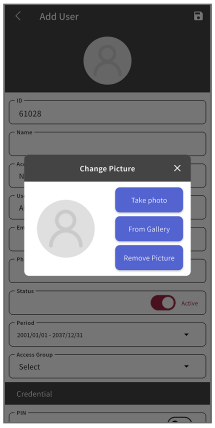


1. 앱 홈 화면에서 **USER**를 탭하세요.

   사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **User**를 탭하세요.

2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. 등록할 사용자의 기본 정보를 입력하고 크리덴셜을 설정하세요.

프로필 이미지 등록

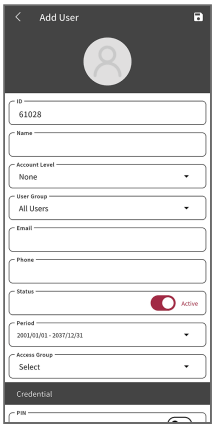


사용자의 프로필 이미지를 등록하려면 화면 상단의 프로필 아이콘을 탭하세요.

- **Take photo**: 모바일 기기의 카메라로 사진을 촬영해 프로필 이미지로 등록할 수 있습니다.
- **From Gallery**: 모바일 기기의 저장된 사진을 선택해 프로필 이미지로 등록할 수 있습니다.

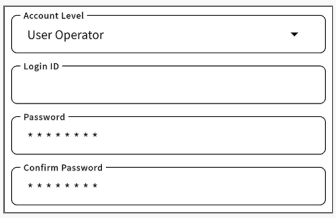
> **알아두기**
> 등록된 프로필 이미지를 삭제하려면 **Remove Picture**를 탭하세요.

사용자 정보 입력 및 권한 설정



- **ID**: 사용자에게 부여되는 고유 아이디입니다. 시스템에 의해 자동 생성된 값이 기본 입력되어 있습니다. 직접 입력할 수도 있습니다.
- **Name**: 사용자의 이름을 입력하세요.
- **Account Level**: 사용자의 관리자 등급을 선택할 수 있습니다.

관리자 등급	메뉴별 권한	
None	-	없음
Administrator	모든 메뉴	모든 권한
User Operator	사용자	읽기, 쓰기
Monitoring Operator	모니터링, 데이터, 대시보드	읽기, 쓰기
T&A Operator	근태 관리	읽기, 쓰기
Visitor Operator	방문자	읽기, 쓰기

> 관리자 등급을 설정하면 로그인 아이디와 비밀번호를 설정해 해당 사용자가 BioStar X 서버에 로그인할 수 있습니다.
>
> 
>

- **User Group**: 사용자가 속한 그룹을 선택하세요.

- **Email**: 사용자의 이메일 주소를 입력하세요.
- **Phone**: 사용자의 전화번호를 입력하세요.
- **Status**: 사용자 계정을 활성화하거나 비활성화할 수 있습니다.
- **Period**: 사용자 계정을 사용할 기간을 설정하세요. 시작 날짜와 종료 날짜를 설정하여 해당 기간 동안만 사용자 계정을 사용할 수 있습니다.
- **Access Group**: 사용자의 출입 그룹을 선택할 수 있습니다.

사용자 ID 및 이름 입력 규칙

- **ID**의 값으로 띄어쓰기를 포함할 수 없습니다.
- **ID**에는 마침표(`.`)를 포함할 수 있으나, 마침표 하나(`.`) 또는 마침표 두 개(`..`)만으로는 입력할 수 없습니다.
- 사용자 이름은 특수 기호를 포함하여 최대 48자까지 입력할 수 있습니다.

  > *특수 기호:* `~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`

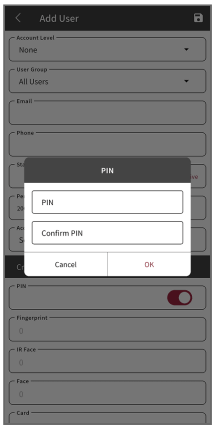
- 사용자 ID 및 이름에는 다음 문자를 사용할 수 없습니다. `₩` `/` `:` `*` `?` `"` `<` `>` `|` `` ` ``
- 사용자 ID에는 홑따옴표(`'`)도 사용할 수 없습니다.
- 사용자 이름의 맨 앞에는 `&@~` 를 연속으로 입력할 수 없습니다. 단, `&`, `@`, `~`를 각각 단독으로 사용자 이름의 첫 글자로 사용할 수 있습니다.

알아두기

- 사용자 아이디는 **설정** → **서버** 메뉴의 **사용자 ID 종류** 옵션에 따라 설정할 수 있는 값이 다를 수 있습니다. 자세한 내용은 서버 상세 설정하기를 참고하세요.
- **T&A Operator** 및 **Visitor Operator** 등급은 별도의 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 출입 그룹 추가 및 설정에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.

크리덴셜 등록

사용자를 등록할 때, 사용자가 출입 통제 시스템에 접근할 수 있도록 크리덴셜을 같이 등록할 수 있습니다. 사용자의 지문 및 얼굴, 카드 정보, 비밀번호 등을 크리덴셜로 등록할 수 있습니다. 크리덴셜은 사용자를 새로 등록하거나 수정할 때 추가 또는 변경할 수 있습니다.

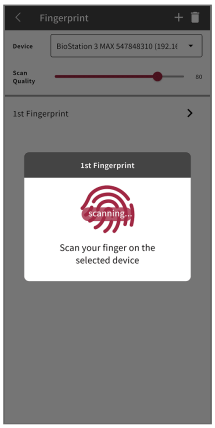


PIN 등록

사용자가 장치에 PIN 번호를 입력하여 출입할 수 있도록 PIN 크리덴셜을 등록할 수 있습니다.

1. **Credential** → **PIN**을 탭하세요.
2. PIN 입력 창이 나타나면 원하는 PIN을 차례로 입력하세요.
3. 입력을 완료하면 **OK**를 탭하세요.

> **알아두기**
>
> - PIN은 최소 4~16자리여야 하며 숫자만 입력할 수 있습니다.
> - 사용자당 최대 1개의 PIN 크리덴셜을 등록할 수 있습니다.

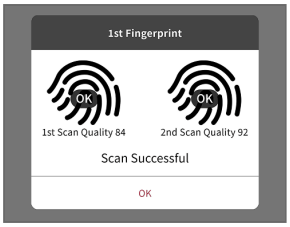


지문 등록

출입을 위한 인증 수단으로 사용자의 지문을 등록해 사용할 수 있습니다. 지문 인증을 지원하는 장치를 통해 사용자의 지문 정보를 등록하세요.

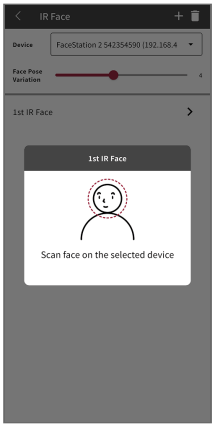
> **지문을 등록하기 전에…**
>
> - 사용자의 지문이 깨끗하고 물기가 없는지 확인하세요.
> - 상처가 있거나 지문이 희미한 손가락은 등록하지 마세요.

1. **Credential** → **Fingerprint**를 탭하세요.
2. 지문을 등록할 장치를 선택하려면 **Device**를 탭하세요.
3. **Add Device** 팝업에서 지문 등록 장치를 선택하고 **Yes**를 탭하세요.
4. **Scan Quality**에서 지문 품질을 조절할 수 있습니다. 기본값은 **80**입니다. 설정한 품질 수준에 미치지 않으면 지문 정보를 등록할 수 없습니다.
5. 화면 오른쪽 상단의 ＋를 탭하세요.
6. 목록에 **1st Fingerprint**가 추가되면 탭하세요.
7. **scanning...** 팝업이 나타나면 선택한 장치에서 지문을 스캔하세요.
8. 지문 확인을 위해 동일한 지문을 다시 스캔하세요.
9. 지문 스캔을 완료하면 **OK**를 탭하세요.



알아두기

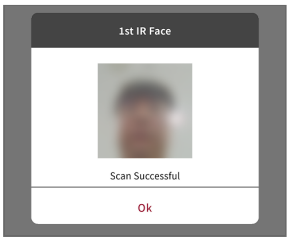
- 장치 목록은 BioStar X 서버에 등록된 지문 인식 장치 중 지문 등록이 가능한 장치만 표시됩니다.
- 지문을 추가 등록하려면 5-9 단계를 반복하세요. 사용자당 최대 10개까지 지문을 등록할 수 있습니다.
- 등록한 지문을 수정하려면 해당 지문 크리덴셜을 탭하고 위 과정을 반복하세요.



IR 페이스 등록

출입을 위한 인증 수단으로 사용자의 얼굴을 등록해 사용할 수 있습니다. IR 페이스 등록은 사용자의 얼굴을 적외선 카메라로 촬영한 인증 수단입니다.

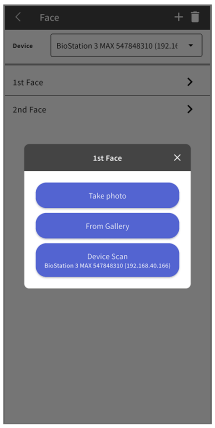
1. **Credential** → **IR Face**를 탭하세요.
2. **Device**를 탭하고 IR 페이스를 등록할 수 있는 장치를 선택하고 **Yes**를 탭하세요.
3. 얼굴의 위치, 각도, 거리에 대한 민감도를 설정하려면 **Face Pose Variation**을 조절하세요. 기본값은 **4**입니다. 정밀한 IR 페이스 템플릿을 얻으려면 높게 설정하세요.
4. 화면 오른쪽 상단의 ＋를 탭하세요.
5. 목록에 **1st IR Face**가 추가되면 탭하세요.
6. 얼굴 등록 팝업이 나타나면 선택한 장치에서 얼굴을 스캔하세요. 얼굴이 인식되면 팝업에 얼굴 이미지가 나타납니다.



7. IR 페이스 등록을 완료하려면 **OK**를 탭하세요.

알아두기

- IR 페이스를 등록할 수 있는 장치는 아래를 참고하세요.
  - FaceStation 2
  - FaceLite
- IR 페이스는 최대 5개까지 등록할 수 있습니다.
- 얼굴 인증률이 낮다면 얼굴 정보를 삭제하고 새로운 얼굴 정보를 등록하세요.
- 등록한 IR 페이스를 수정하려면 해당 IR 페이스 크리덴셜을 탭하고 위 과정을 반복하세요.



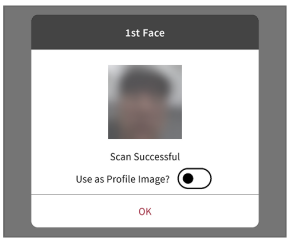
얼굴 등록

출입을 위한 인증 수단으로 사용자의 얼굴을 등록해 사용할 수 있습니다. 얼굴 등록은 사용자의 얼굴을 카메라로 촬영한 인증 수단입니다. BioStar X 모바일 앱에서는 모바일 기기에 저장된 얼굴 이미지를 불러오거나 카메라로 촬영해 얼굴을 등록할 수도 있으며, 얼굴 인식이 가능한 장치에서 얼굴을 스캔해 등록할 수도 있습니다.

1. **Credential** → **Face**를 탭하세요.
2. **Device**를 탭하고 얼굴을 등록할 수 있는 장치를 선택하고 **Yes**를 탭하세요.

   - 장치를 선택하지 않으면 모바일 기기의 사진을 불러오거나 카메라로 촬영해 얼굴을 등록할 수 있습니다.
   - 장치를 선택하면 해당 장치에서 얼굴을 스캔해 등록할 수 있습니다.

3. 화면 오른쪽 상단의 ＋를 탭하세요.
4. 목록에 **1st Face** 항목이 추가되면 탭하세요.
5. 팝업에서 원하는 얼굴 등록 방법을 선택하세요.
   - **Take photo**: 모바일 기기의 카메라로 사진을 촬영해 얼굴을 등록할 수 있습니다.
   - **From Gallery**: 모바일 기기에 저장된 사진을 선택해 얼굴을 등록할 수 있습니다.
   - **Device Scan**: **Device** 항목에서 선택한 장치를 통해 얼굴을 스캔할 수 있습니다.
6. 얼굴이 인식되면 팝업에 얼굴 이미지가 나타납니다.



7. 얼굴 등록을 완료하려면 **OK**를 탭하세요.

알아두기

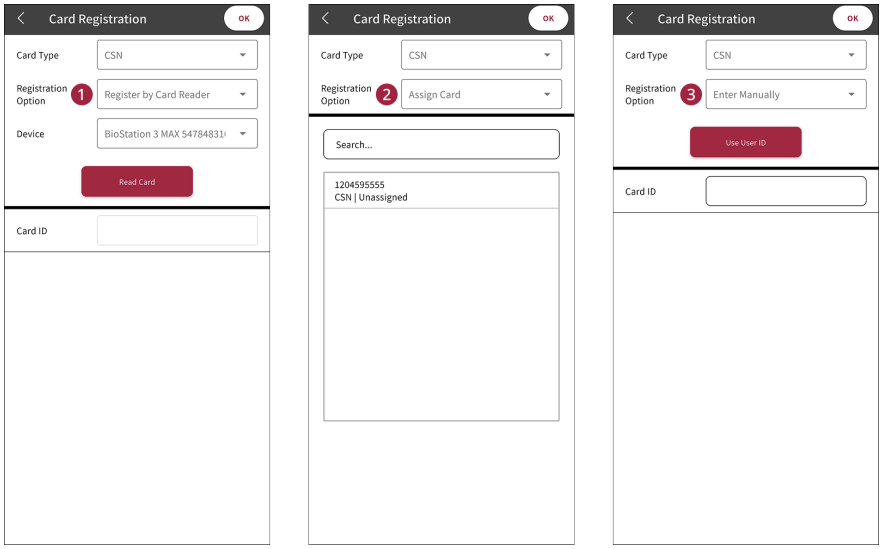
- 등록한 얼굴 이미지를 프로필 이미지로 사용하려면 **Use as Profile Image?** 옵션을 활성화하세요.
- 모바일 기기의 카메라로 얼굴 사진을 촬영하거나 저장된 사진을 불러올 때 접근 권한이 필요합니다. 권한 요청 팝업에서 허용을 선택해야 얼굴 사진을 등록할 수 있습니다.
- 등록한 얼굴을 수정하려면 해당 얼굴 크리덴셜을 탭하고 위 과정을 반복하세요.

출입 카드 등록

출입을 위한 인증 수단으로 새로운 출입 카드를 등록하거나 이미 등록된 출입 카드를 할당할 수 있습니다. 출입 카드 등록은 카드 리더기에 카드를 스캔해 등록하는 방법과 이미 등록된 카드를 할당하는 방법, 카드 번호를 수동으로 입력하는 방법이 있습니다.

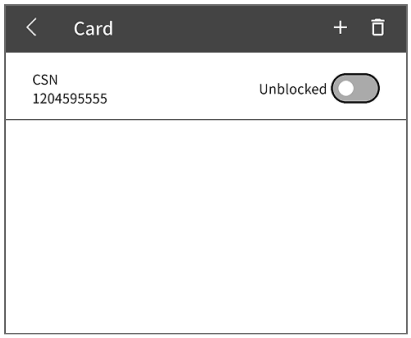
CSN 카드

1. **Credential** → **Card**를 탭하세요.
2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. **Card Type**에서 **CSN**을 선택하고 **Yes**를 탭하세요.
4. **Registration Option**에서 원하는 등록 방식을 선택하세요.



- 1 **Register by Card Reader**: 카드 리더기에 카드를 스캔해 등록할 수 있습니다. **Device**에서 카드를 읽을 장치를 선택하고, **Read Card**를 탭하세요. 카드 리더기에 카드를 가져가 스캔하세요. 카드를 성공적으로 스캔하면 **Card ID**에 카드 번호가 입력됩니다.
- 2 **Assign Card**: 이미 등록된 출입 카드를 사용자에게 할당할 수 있습니다. 목록에서 등록된 카드 번호 중 하나를 선택하세요.
- 3 **Enter Manually**: 카드 번호를 수동으로 입력할 수 있습니다. **Card ID** 입력 필드에 카드 번호를 입력하세요. 사용자의 아이디를 카드 번호로 사용하려면 **Use User ID**를 탭하세요.

5. 카드 등록을 완료하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
6. 카드 목록으로 돌아오면 등록한 카드 번호가 나타납니다.

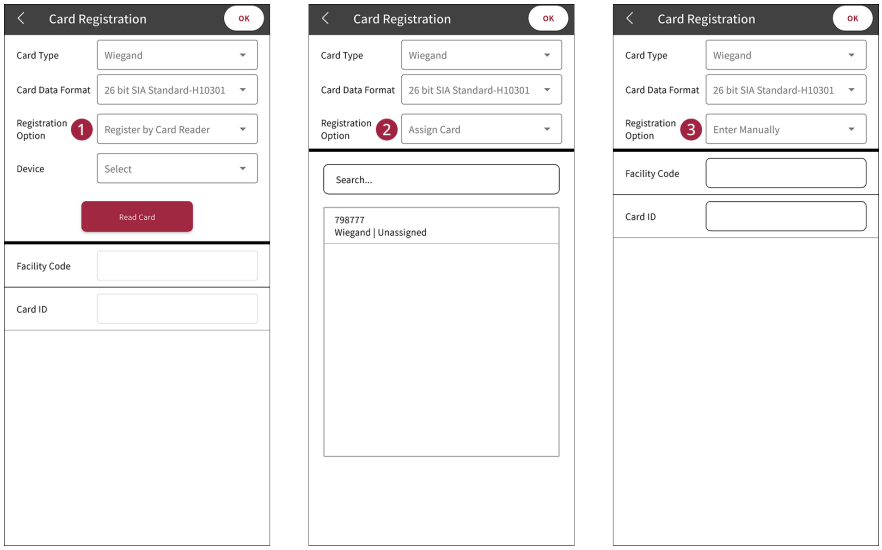


알아두기

등록한 카드의 사용을 중지하려면 카드의 토글 스위치를 탭하여 **Blocked**로 설정하세요.

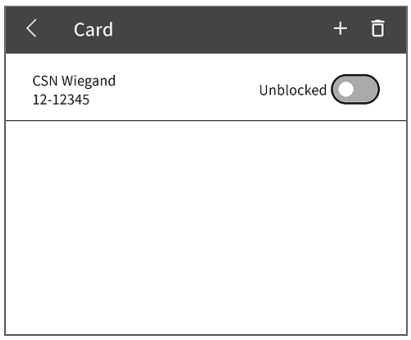
Wiegand 카드

1. **Credential** → **Card**를 탭하세요.
2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. **Card Type**에서 **Wiegand**를 선택하고 **Yes**를 탭하세요.
4. **Card Data Format**에서 원하는 카드 형식을 선택하세요.
5. **Registration Option**에서 원하는 등록 방식을 선택하세요.



- 1 **Register by Card Reader**: 카드 리더기에 카드를 스캔해 등록할 수 있습니다. **Device**에서 카드를 읽을 장치를 선택하고, **Read Card**를 탭하세요. 카드 리더기에 카드를 가져가 스캔하세요. 카드를 성공적으로 스캔하면 **Facility Code**와 **Card ID**에 카드 번호가 입력됩니다.
- 2 **Assign Card**: 이미 등록된 출입 카드를 사용자에게 할당할 수 있습니다. 목록에서 등록된 카드 번호 중 하나를 선택하세요.
- 3 **Enter Manually**: 카드 번호를 수동으로 입력할 수 있습니다. **Facility Code**와 **Card ID** 입력 필드에 카드 번호를 입력하세요.

6. 카드 등록을 완료하려면 화면 오른쪽 상단의 **OK**를 탭하세요.
7. 카드 목록으로 돌아오면 등록한 카드 번호가 나타납니다.



> **알아두기**
> 등록한 카드의 사용을 중지하려면 카드의 토글 스위치를 탭하여 **Blocked**로 설정하세요.

스마트 카드

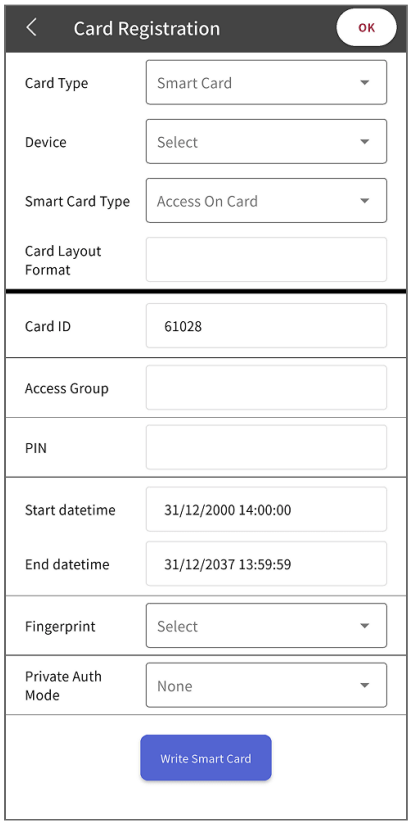
알아두기

- 스마트 카드를 발급하려면 올바른 카드 형식을 설정해야 합니다. 카드 형식에 대한 자세한 내용은 스마트 카드 형식 설정하기를 참고하세요.
- 스마트 카드에 저장하는 사용자 정보는 **BioStar X**에 저장된 정보를 사용합니다. 만약 변경한 사용자 정보를 저장하지 않으면, 스마트 카드에 잘못된 사용자 정보를 저장할 수 있습니다. 또한, 변경한 사용자 정보를 장치와 동기화하지 않으면 장치가 인증을 수행하지 못할 수 있습니다.
- PIN 인증 정보를 추가하려면 먼저 PIN을 등록해야 합니다. PIN 등록에 대한 자세한 내용은 PIN 등록을 참고하세요.
- 지문 크리덴셜 정보를 추가하려면 먼저 지문을 등록해야 합니다. 지문 등록에 대한 자세한 내용은 지문 등록을 참고하세요.

액세스 온 카드(Access On Card)

사용자 정보(카드 ID, PIN, 출입 그룹, 기간, 지문 템플릿, 얼굴 템플릿, 개인 인증 모드)를 카드에 저장할 수 있습니다.

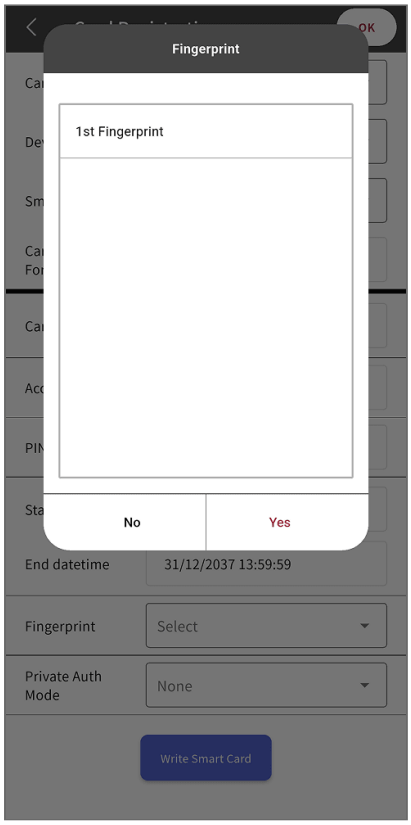
1. **Credential** → **Card**를 탭하세요.
2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. **Card Type**에서 **Smart Card**를 선택하고 **Yes**를 탭하세요.



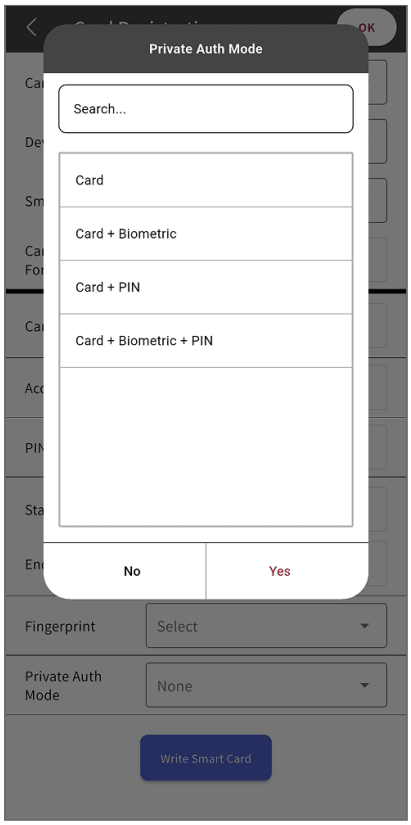
4. **Device**에서 카드를 등록할 장치를 선택하고 **Yes**를 탭하세요.

> **Device**에서 선택한 장치에 설정된 카드 레이아웃이 **Card Layout Format**에 표시됩니다.

5. (선택 사항) 지문 인증을 추가하려면 **Figerprint**를 탭하고 등록한 지문을 선택하세요.



6. (선택 사항) 개인 인증 모드를 추가하려면 **Private Auth Mode**를 탭하고 원하는 인증 방식을 선택하세요.

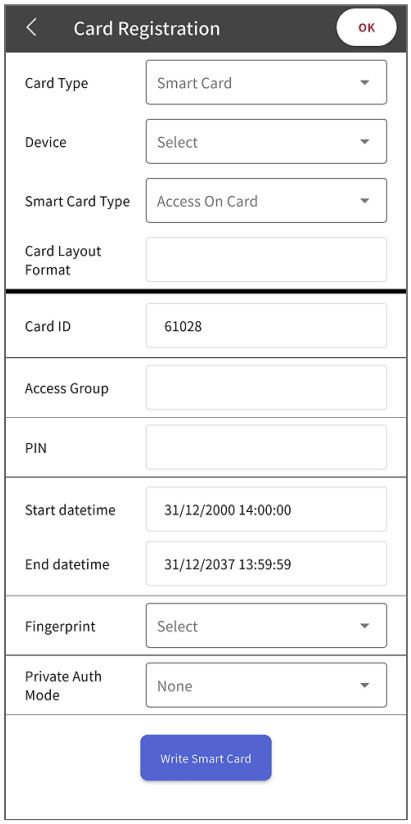


7. 카드를 등록하려면 **Writes Smart Card**를 탭하세요.
8. 선택한 장치에 사용자 정보를 등록할 카드를 대세요.
9. 카드 등록을 완료하면 화면 오른쪽 상단의 **OK**를 탭하세요.

보안 크리덴셜 카드(Secure Credential Card)

사용자 정보(카드 ID, PIN, 지문 템플릿, 얼굴 템플릿)를 카드에 저장할 수 있습니다.

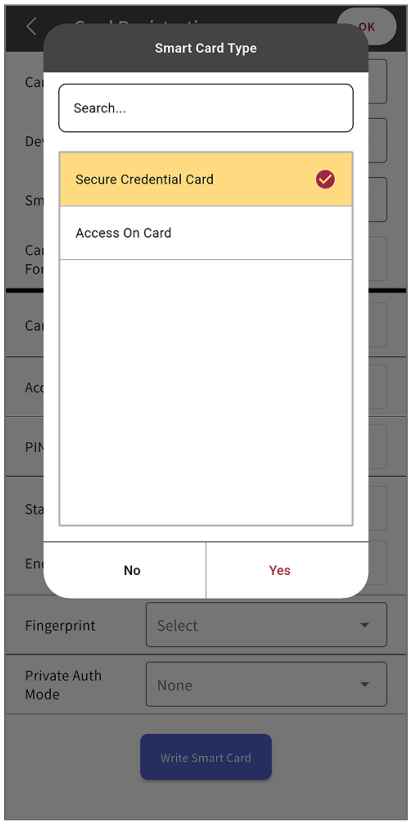
1. **Credential** → **Card**를 탭하세요.
2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. **Card Type**에서 **Smart Card**를 선택하고 **Yes**를 탭하세요.



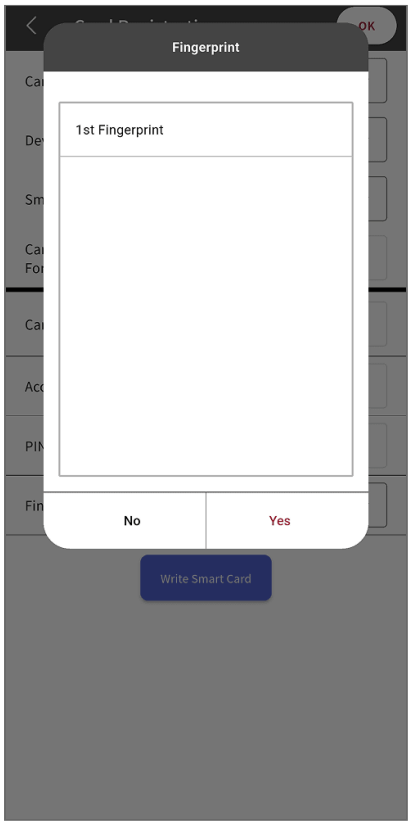
4. **Device**에서 카드를 등록할 장치를 선택하고 **Yes**를 탭하세요.

> **Device**에서 선택한 장치에 설정된 카드 레이아웃이 **Card Layout Format**에 표시됩니다.

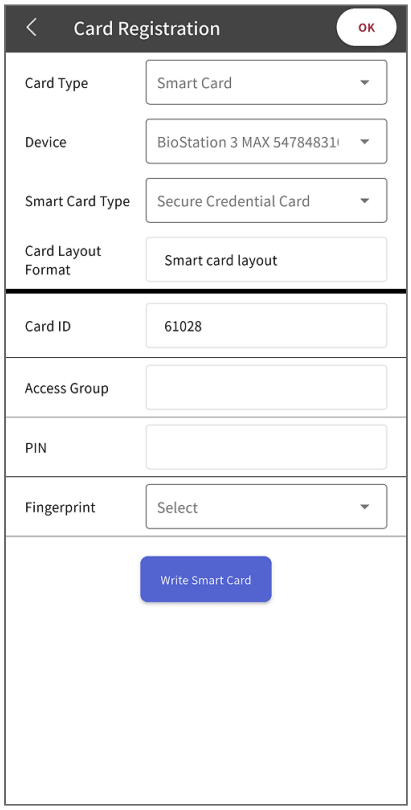
5. **Smart Card Type**을 탭하고, **Secure Credential Card**를 선택한 다음 **Yes**를 탭하세요.



6. (선택 사항) 지문 인증을 추가하려면 **Figerprint**를 탭하고 등록한 지문을 선택하세요.



7. 카드를 등록하려면 **Writes Smart Card**를 탭하세요.

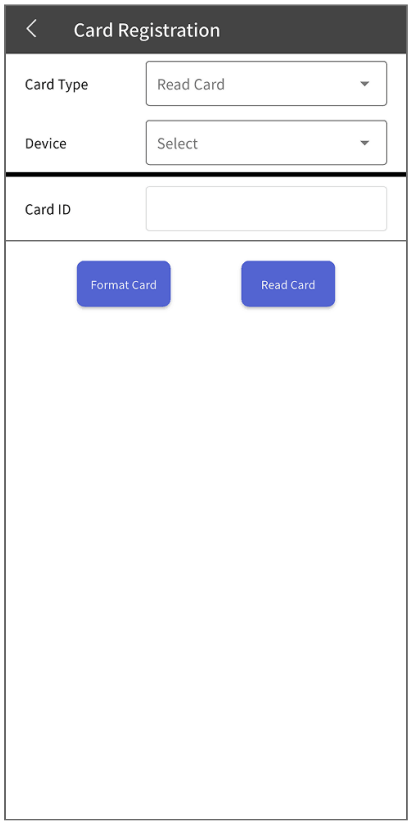


8. 선택한 장치에 사용자 정보를 등록할 카드를 대세요.
9. 카드 등록을 완료하면 화면 오른쪽 상단의 **OK**를 탭하세요.

카드 읽기/포맷

스마트 카드를 포맷하고 정보를 다시 기록할 수 있습니다.

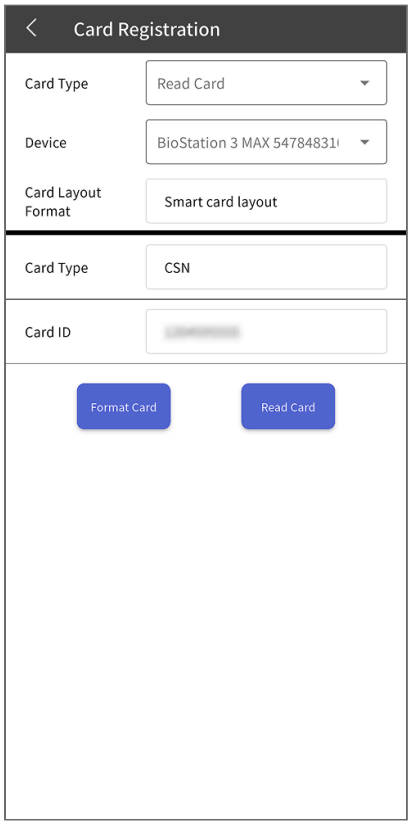
1. **Credential** → **Card**를 탭하세요.
2. 화면 오른쪽 상단의 ＋를 탭하세요.
3. **Card Type**에서 **Read Card**를 선택하고 **Yes**를 탭하세요.



4. **Device**에서 카드를 읽을 장치를 선택하고 **Yes**를 탭하세요.

> **Device**에서 선택한 장치에 설정된 카드 레이아웃이 **Card Layout Format**에 표시됩니다.

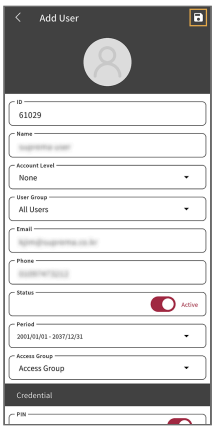
5. **Read Card**를 탭하고 카드를 장치에 가져가 스캔하세요.



6. 카드 정보를 확인한 후 카드를 포맷하려면 **Format Card**를 탭하세요.

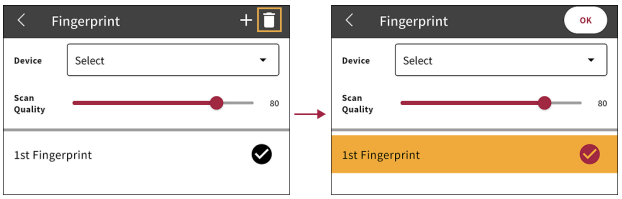
> **알아두기**
> 커스텀 스마트 카드는 포맷할 수 없습니다.

사용자 등록 완료



사용자의 기본 정보와 권한, 크리덴셜을 설정한 후, 사용자 등록을 완료하려면 화면 오른쪽 상단의 를 탭하세요.

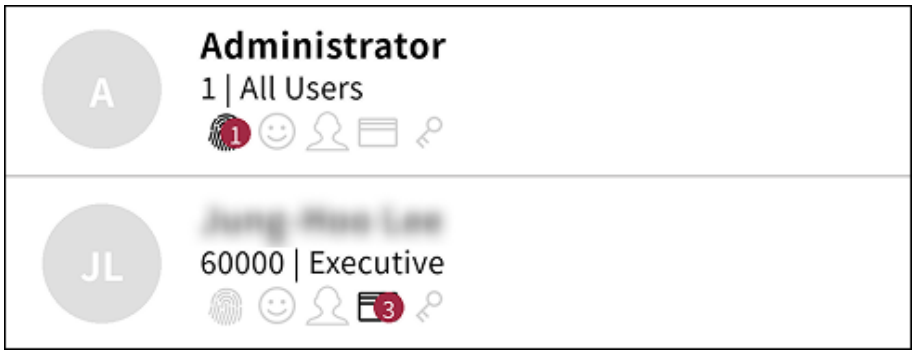
- **Credential** 섹션의 각 크리덴셜마다 등록된 크리덴셜의 수를 확인할 수 있습니다.
- 등록한 크리덴셜을 삭제하려면 삭제할 크리덴셜 항목을 탭하고, 화면 오른쪽 상단의 를 탭하세요. 삭제할 크리덴셜을 선택한 후 **OK**를 탭하세요.



> **알아두기**
> BioStar X에서 사용자 등록 및 관리에 대한 자세한 내용은 사용자를 참고하세요.

사용자 정보 확인

등록한 사용자는 사용자 목록에서 확인할 수 있습니다. 각 사용자는 아래와 같은 정보를 포함하고 있습니다.



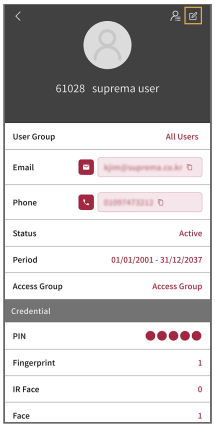
- 사용자 이름
- 사용자 ID | 사용자 그룹
- 등록된 크리덴셜 정보: 지문 / IR 페이스 / 얼굴 / 카드 / PIN

사용자 수정 및 삭제하기

사용자의 소속이 변경되거나 권한을 조정해야 할 때는 정보를 수정할 수 있습니다. 퇴사나 계약 종료 시 사용자를 삭제하여 보안을 강화하는

방법도 알아보세요.

사용자 수정

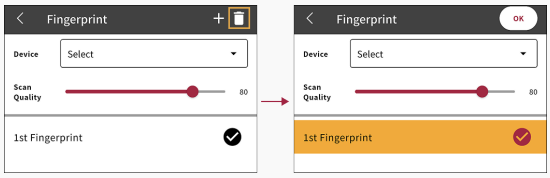


사용자 정보 및 권한, 크리덴셜은 사용자 상세 정보에서 수정할 수 있습니다.

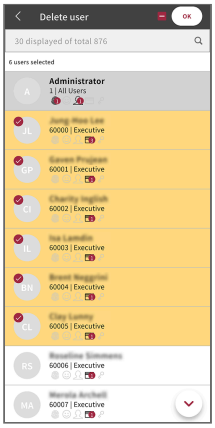
1. 앱 홈 화면에서 **USER**를 탭하세요.

> 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **User**를 탭하세요.

2. 사용자 목록에서 수정하려는 사용자를 탭하세요.
3. 사용자 상세 정보에서 화면 오른쪽 상단의 를 탭하세요.
4. **Edit User**에서 사용자의 기본 정보 수정 및 권한 변경, 크리덴셜을 관리할 수 있습니다.
5. 변경 사항을 저장하려면 화면 오른쪽 상단의 를 탭하세요.

> **알아두기**
>
> - 사용자 정보 및 권한, 크리덴셜 항목에 대한 자세한 내용은 사용자 등록하기를 참고하세요.
> - 사용자를 일시적으로 비활성화하려면 **Status**에서 토글 스위치를 탭하여 **Inactive**로 설정하세요. 비활성화된 사용자는 출입이 차단됩니다.
> - 등록한 크리덴셜을 삭제하려면 삭제할 크리덴셜 항목을 탭하고, 화면 오른쪽 상단의 를 탭하세요. 삭제할 크리덴셜을 선택한 후 **OK**를 탭하세요.
>
> 
>

사용자 삭제



사용자를 삭제해야 한다면, 다음의 안내에 따라 삭제할 수 있습니다.

1. 앱 홈 화면에서 **USER**를 탭하세요.

> 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **User**를 탭하세요.

2. 사용자 목록에서 화면 오른쪽 상단의 를 탭하세요.
3. 삭제하려는 사용자를 선택하세요. 1명 이상의 사용자를 선택할 수 있습니다.
4. 화면 오른쪽 상단의 **OK**를 탭하세요.

5. 확인 메시지가 나타나면 **Yes**를 탭하세요.

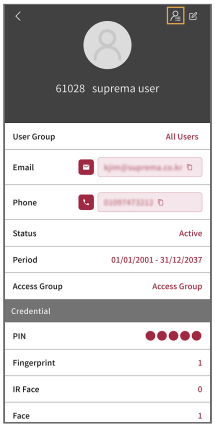
선택한 사용자가 삭제됩니다. 삭제된 사용자는 복구할 수 없습니다.

> **알아두기**
> 아이디가 1인 관리자 계정은 삭제할 수 없습니다.

사용자 로그 이벤트 조회하기

사용자의 출입 이력을 조회해 비정상 접근이나 허가되지 않은 시간대의 출입을 확인할 수 있습니다. 로그 이벤트를 필터링하면 원하는 기간과 장소의 이력을 쉽게 찾을 수 있습니다.

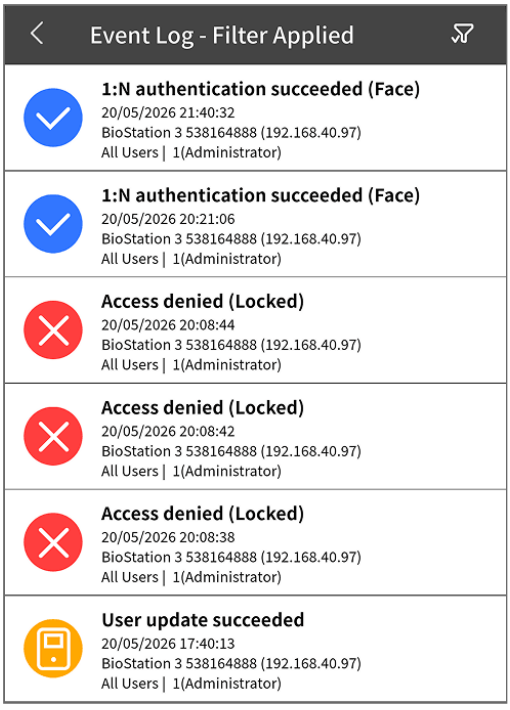
사용자 출입 이력 조회



1. 앱 홈 화면에서 **USER**를 탭하세요.

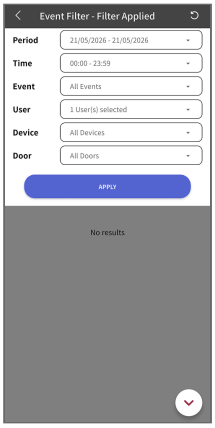
> 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **User**를 탭하세요.

2. 사용자 목록에서 로그 이벤트를 조회하려는 사용자를 탭하세요.
3. 사용자 상세 정보에서 오른쪽 상단의 를 탭하세요.
4. **Event Log**에서 사용자의 출입 이력을 확인할 수 있습니다.



최신 로그 이벤트가 먼저 표시되며, 출입 위치와 이벤트 정보를 확인할 수 있습니다.

로그 이벤트 필터링



사용자의 로그 이벤트를 날짜 및 시간, 이벤트 종류, 출입 위치 등 다양한 조건으로 필터링할 수 있습니다.

1. 이벤트 로그 오른쪽 상단의 를 탭하세요.
2. 필터 조건이 나타나면 원하는 조건을 설정하세요.
   - **Period**: 로그 이벤트가 발생한 기간을 설정하세요.
   - **Time**: 로그 이벤트가 발생한 시간을 설정하세요.
   - **Event**: 로그 이벤트 종류를 선택하세요. 예를 들어, 출입 인증 성공, 출입 인증 실패 등을 선택할 수 있습니다.
   - **User**: 현재 사용자 외 다른 사용자의 로그 이벤트도 조회할 수 있습니다.
   - **Device**: 로그 이벤트가 발생한 장치를 선택할 수 있습니다.
   - **Door**: 로그 이벤트가 발생한 출입문을 선택할 수 있습니다.
3. 설정한 조건으로 로그 이벤트를 필터링하려면 **Apply**를 탭하세요.

> **알아두기**
> 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.

사용자 검색 및 필터링하기

사용자 목록이 많아 원하는 사용자를 찾기 어려울 때, 검색 기능과 필터링 기능을 활용해 빠르게 사용자를 찾을 수 있습니다.

사용자 검색



사용자의 아이디, 이름, 이메일 주소를 기준으로 검색할 수 있습니다.

1. 앱 홈 화면에서 **USER**를 탭하세요.

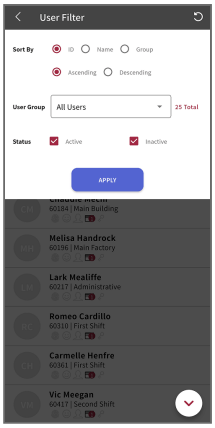
   > 사이드 메뉴를 통해 진입할 수도 있습니다. → **User**를 탭하세요.

2. 사용자 목록 상단의 를 탭하세요.
3. 검색 입력 필드에 검색어를 입력하세요. 아이디, 이름, 이메일 주소를 조합하여 검색할 수 있습니다.
4. 검색어 입력을 완료한 후 를 탭하세요.

검색어와 일치하는 사용자가 검색 결과로 표시됩니다. 검색 결과에서 원하는 사용자를 탭하여 사용자 상세 정보로 이동할 수 있습니다.

> **알아두기**
>
> - 검색 입력 필드 아래에는 최근 검색 기록이 표시됩니다. 최근 검색 기록을 탭하면 해당 검색어로 다시 검색할 수 있습니다.
> - 검색 입력 필드를 닫으려면 ✕를 탭하세요.

사용자 목록 필터링



사용자 목록을 다양한 조건으로 필터링하여 원하는 사용자를 빠르게 찾을 수 있습니다.

1. 앱 홈 화면에서 **USER**를 탭하세요.

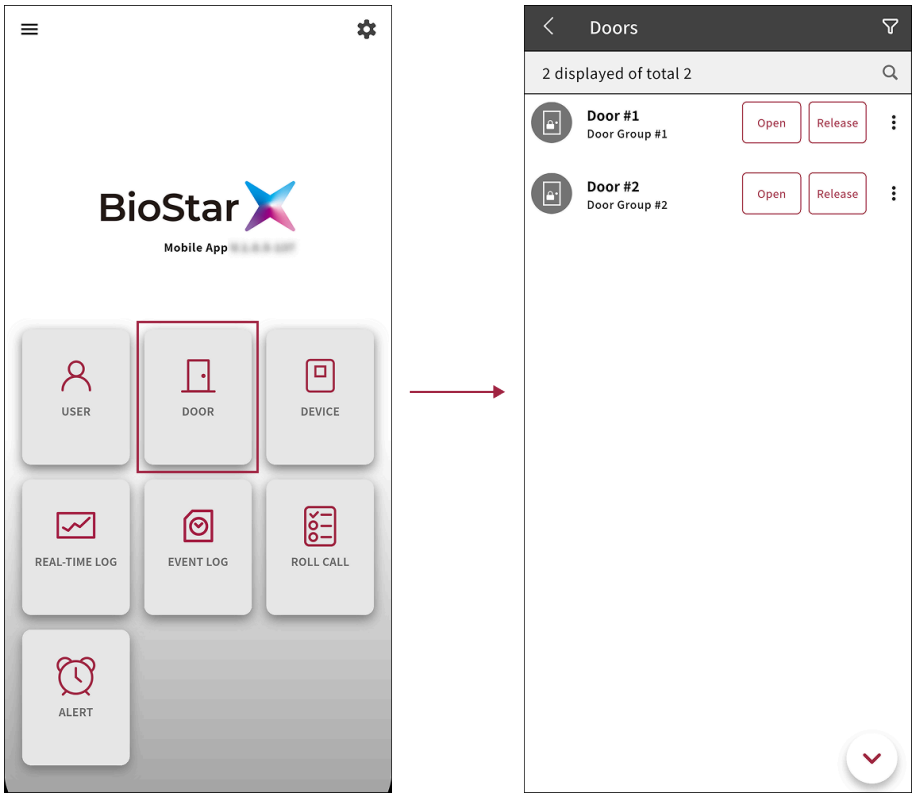
   > 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **User**를 탭하세요.

2. 사용자 목록 상단의 를 탭하세요.
3. **User Filter**에서 원하는 조건을 설정하세요.
   - **Sort By**: 사용자 아이디, 이름, 그룹을 기준으로 오르차순 또는 내림차순 정렬을 선택할 수 있습니다.
   - **User Group**: 특정 사용자 그룹을 선택하여 해당 그룹에 속한 사용자만 표시할 수 있습니다.
   - **Status**: 활성화된 사용자만 표시하려면 **Active**를 선택하세요. 비활성화된 사용자만 표시하려면 **Inactive**를 선택하세요.
4. 설정한 조건으로 사용자 목록을 필터링하려면 **Apply**를 탭하세요.

> **알아두기**
>
> 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.

출입문 관리하기

출입문을 원격으로 제어하여 편리하게 출입을 관리할 수 있습니다. 출입문 상태를 실시간으로 확인하고, 필요에 따라 출입문의 설정을 변경할 수도 있습니다. 출입문과 관련한 로그 이벤트를 조회할 수도 있습니다.



알아두기

BioStar X에서 출입문을 모니터링 및 관리 방법에 대한 자세한 내용은 다음 문서를 참고하세요.

- 출입문 모니터링하기
- 출입문 관리하기

출입문 원격 제어하기

출입문 목록에서 각 출입문의 상태를 실시간으로 확인하고 필요에 따라 제어할 수 있습니다. 정상 운영 중에는 기본 제어 기능으로 관리하고, 보안 강화나 긴급 상황에는 추가 제어 옵션을 활용할 수 있습니다.

앱 홈 화면에서 **DOOR**를 탭하세요. BioStar X에 등록된 출입문 목록이 표시됩니다.

알아두기

사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Door**를 탭하세요.

출입문 상태 확인

출입문 목록에서 출입문의 상태 아이콘을 통해 출입문에 할당된 장치의 이상 상태를 한눈에 확인할 수 있습니다. 출입문 상태 아이콘은 출입문이 열려 있는지, 닫혀 있는지, 알람이 발생했는지 등을 나타냅니다.



상태 아이콘	설명
	출입문에 문제가 발생한 상태입니다. 출입문에 할당된 장치와 연결이 끊어졌거나 멀티 커뮤니케이션 서버 오류, 동기화 오류 등의 이상 상태입니다.
	출입문이 열려 있는 상태입니다.
	출입문이 닫혀 있는 상태입니다.
	출입문에 알람이 발생한 상태입니다.
	출입문에 APB 알람이 발생한 상태입니다.

출입문 열기/잠그기

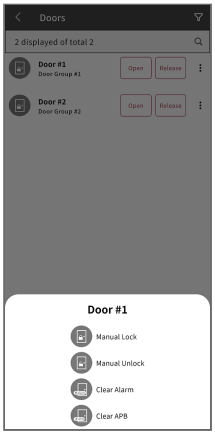


출입문 원격 제어 기능을 통해 출입문을 열거나 잠궈, 출입을 허용하거나 차단할 수 있습니다.

- **Open**: 출입문을 일시적으로 열어 출입을 허용합니다. 출입문은 설정된 시간 후 자동으로 닫힙니다.
- **Release**: 인증된 사용자만 출입할 수 있도록 설정합니다. 출입문에 설정된 스케줄에 따라 출입문 상태가 변경됩니다.

> **알아두기**
> 출입문을 일시적으로 열어 자동으로 닫히는 시간을 설정하는 방법은 출입문 등록하기에서 **출입문 열림** → **열림 시간**을 참고하세요.

추가 제어



보안 강화가 필요하거나 장시간 출입을 통제해야 할 때, 시간 제한 없이 출입문을 수동으로 잠그거나 개방할 수 있습니다. 발생한 알람을 해제할 수도 있습니다.

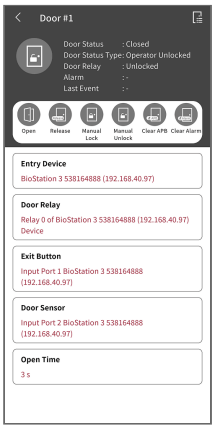
출입문의 가장 오른쪽에 ⋮ 를 탭하면 추가 제어 옵션을 사용할 수 있습니다.

- **Manual Lock**: 출입문을 수동으로 잠가 출입을 차단합니다. 이 기능은 시간 제한 없이 출입문을 잠글 수 있습니다. 이 상태에서는 모든 사용자의 출입을 차단합니다.
- **Manual Unlock**: 출입문을 수동으로 개방하여 출입을 허용합니다. 이 기능은 시간 제한 없이 출입문을 개방합니다. 이 상태에서는 모든 사용자의 출입을 허용합니다.
- **Clear Alarm**: 출입문에서 발생한 알람을 해제할 수 있습니다.
- **Clear APB**: 선택한 출입문의 모든 사용자에 대한 APB 알람을 해제할 수 있습니다.

> **알아두기**
> 출입문을 수동으로 잠그거나 개방한 후에는 출입문 상태가 자동으로 변경되지 않습니다. 보안을 위해 출입문의 상태를 설정된 스케줄에 맞춰 작동하게 하려면 **Release** 기능을 사용하세요.

출입문 상세 정보 확인하기

출입문을 선택하면 현재 상태와 설정된 장치를 확인할 수 있습니다. 문제가 발생하면 바로 제어하거나 최근 활동 기록을 조회할 수 있습니다.



출입문의 상태 정보와, 원격 제어 기능, 출입문에 할당된 장치 정보와 열림 시간을 확인할 수 있습니다.

1. 앱 홈 화면에서 **DOOR**를 탭하세요.

   > 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Door**를 탭하세요.

2. 출입문 목록에서 상세 정보를 확인하려는 출입문을 탭하세요.

출입문 상태 정보

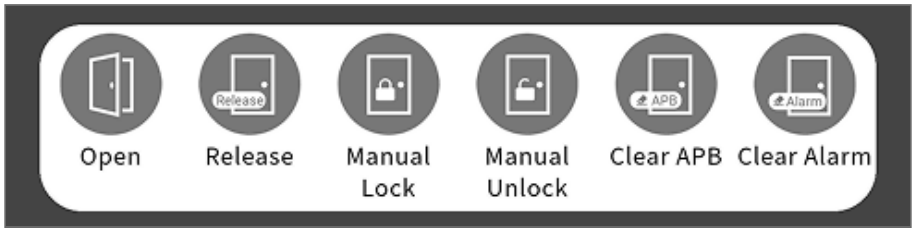
출입문의 현재 상태를 실시간으로 확인할 수 있습니다.



- **Door Status**: 출입문의 열림 또는 닫힘 상태를 표시합니다.
- **Door Status Type**: 출입문의 상태 유형을 표시합니다. 예를 들어, 정상(Normal), 관리자 수동 개방(Operator Unlocked), 관리자 수동 잠금(Operator Locked) 등이 있습니다.
- **Door Relay**: 출입문과 연결된 릴레이의 상태를 표시합니다.
- **Alarm**: 출입문에서 발생한 알람 이벤트를 표시합니다.
- **Last Event**: 출입문에서 발생한 마지막 이벤트의 날짜와 시간, 이벤트 유형을 표시합니다.

원격 제어 기능

출입문을 원격으로 제어하여 출입을 관리할 수 있습니다.

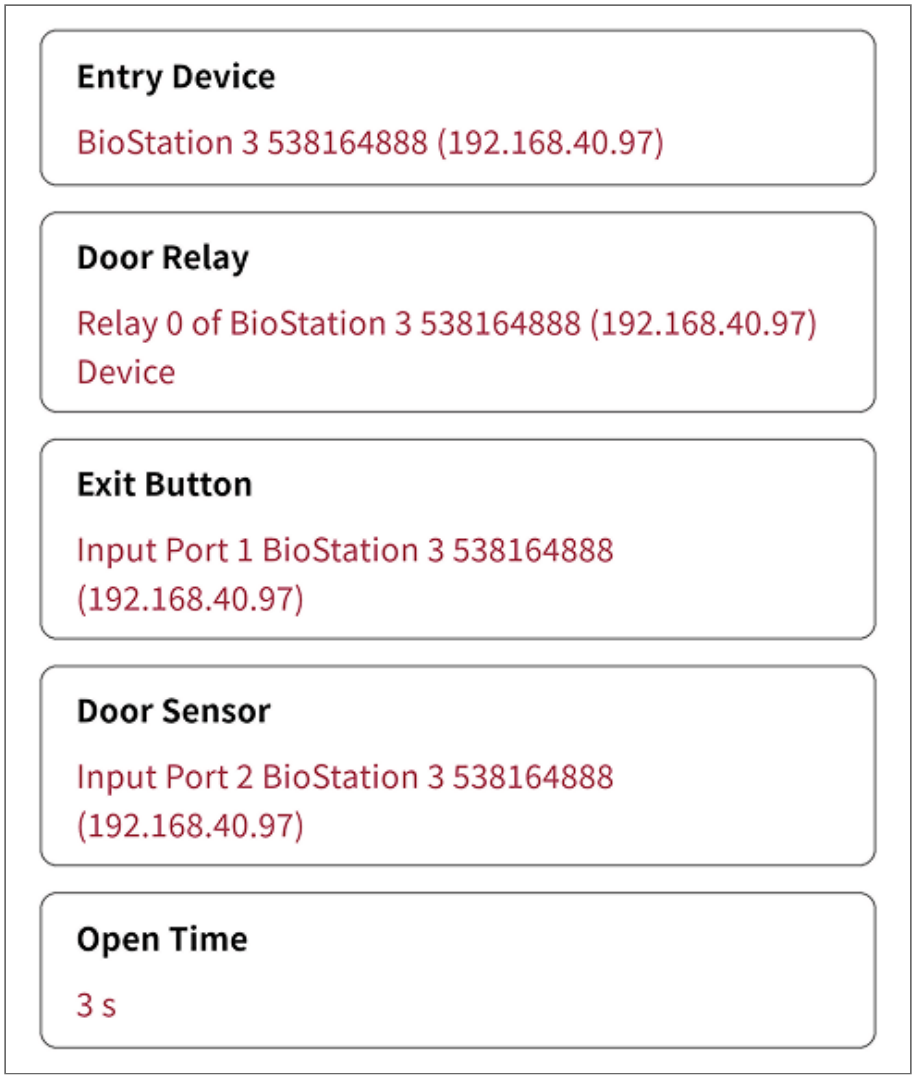


- **Open**: 출입문을 일시적으로 열어 출입을 허용합니다. 출입문은 설정된 시간 후 자동으로 닫힙니다.
- **Release**: 인증된 사용자만 출입할 수 있도록 설정합니다. 출입문에 설정된 스케줄에 따라 출입문 상태가 변경됩니다.
- **Manual Lock**: 출입문을 수동으로 잠가 출입을 차단합니다. 이 기능은 시간 제한 없이 출입문을 잠글 수 있습니다. 이 상태에서는 모든 사용자의 출입을 차단합니다.
- **Manual Unlock**: 출입문을 수동으로 개방하여 출입을 허용합니다. 이 기능은 시간 제한 없이 출입문을 개방합니다. 이 상태에서는 모든 사용자의 출입을 허용합니다.
- **Clear APB**: 선택한 출입문의 모든 사용자에 대한 APB 알람을 해제할 수 있습니다.
- **Clear Alarm**: 출입문에서 발생한 알람을 해제할 수 있습니다.

> **알아두기**
>
> - 출입문을 일시적으로 열어 자동으로 닫히는 시간은 하단의 **Open Time**에서 확인할 수 있습니다.
> - 출입문을 수동으로 잠그거나 개방한 후에는 출입문 상태가 자동으로 변경되지 않습니다. 보안을 위해 출입문의 상태를 설정된 스케줄에 맞춰 작동하게 하려면 **Release** 기능을 사용하세요.

출입문 장치 정보

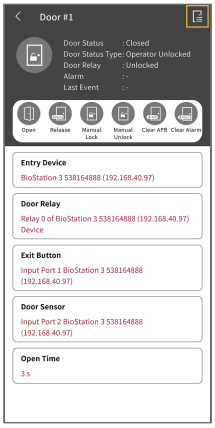
출입문에 할당된 장치 정보를 확인할 수 있습니다.



- **Entry Device**: 입실 장치로 할당된 장치 정보입니다.
- **Door Relay**: 출입문의 잠금 장치로 동작할 릴레이 정보입니다.
- **Exit Button**: 퇴실 버튼으로 사용할 장치의 포트 정보입니다.
- **Door Sensor**: 출입문의 열림과 닫힘을 감지하는 센서로 할당된 장치의 포트 정보입니다.
- **Open Time**: 출입문을 일시적으로 열었을 때, 출입문이 자동으로 닫히기까지 유지되는 시간입니다.

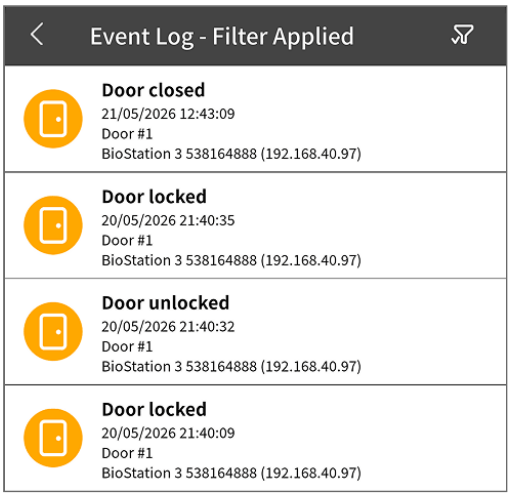
> **알아두기**
> **Open Time** 설정에 대한 자세한 내용은 출입문 등록하기에서 **출입문 열림** → **열림 시간**을 참고하세요.

출입문 로그 이벤트 조회

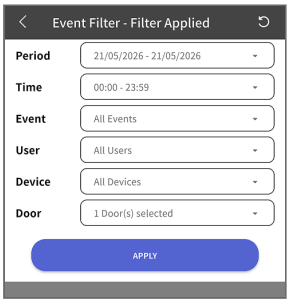


출입문에서 발생한 로그 이벤트를 조회하여 출입문에서 발생한 출입 시도, 알람 등의 이벤트를 확인할 수 있습니다.

1. 출입문 상세 정보 화면에서 오른쪽 상단의 를 탭하세요.



2. 출입문 로그 이벤트를 필터링하려면 화면 오른쪽 상단의 를 탭하세요.

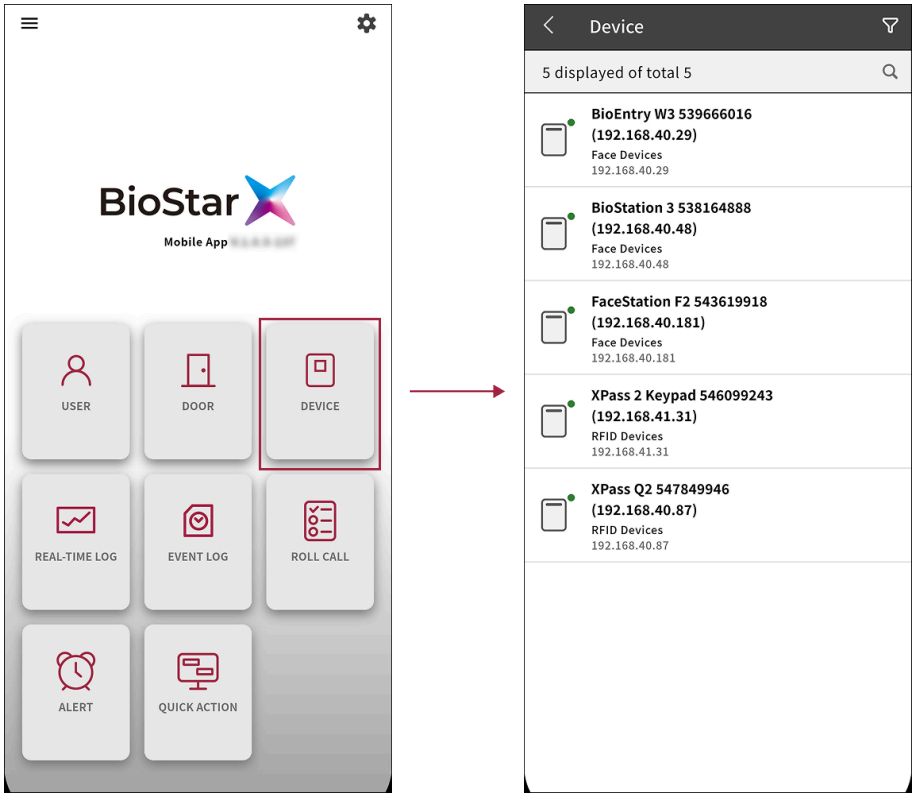


   - **Period**: 로그 이벤트가 발생한 기간을 설정하세요.
   - **Time**: 로그 이벤트가 발생한 시간을 설정하세요.
   - **Event**: 로그 이벤트 종류를 선택하세요. 예를 들어, 출입 인증 성공, 출입 인증 실패 등을 선택할 수 있습니다.
   - **User**: 로그 이벤트를 발생시킨 사용자를 선택할 수 있습니다.
   - **Device**: 로그 이벤트가 발생한 장치를 선택할 수 있습니다.
   - **Door**: 현재 출입문 외 다른 출입문의 로그 이벤트도 조회할 수 있습니다.
3. 필터 조건이 나타나면 원하는 조건을 설정하세요.
4. 설정한 조건으로 로그 이벤트를 필터링하려면 **Apply**를 탭하세요.

> **알아두기**
>
> 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.

장치 관리하기

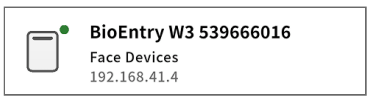
장치 목록에서는 개별 장치의 상태를 확인하고, 잠금 상태의 장치를 원격으로 해제할 수 있습니다. 앱 홈 화면에서 **DEVICE**를 탭하세요.



알아두기

- 모바일 앱에서는 장치를 등록하거나 수정할 수 없습니다.
- 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Device**를 탭하세요.

장치 정보 확인



장치 목록의 각 장치는 다음 정보를 포함하고 있습니다.

- 장치 이름
- 장치 그룹 이름(그룹에 포함되어 있지 않으면, **All Devices**로 표시)
- 장치 IP 주소

장치 상태 확인

장치 목록에서 상태 아이콘을 통해 장치 상태를 확인할 수 있습니다.

상태 아이콘	설명
	장치가 정상 연결된 상태입니다.
	장치가 꺼져 있거나 연결이 해제된 상태입니다.

알아두기
장치 상태를 갱신하려면 장치 목록을 아래로 당겨서 새로고침할 수 있습니다.

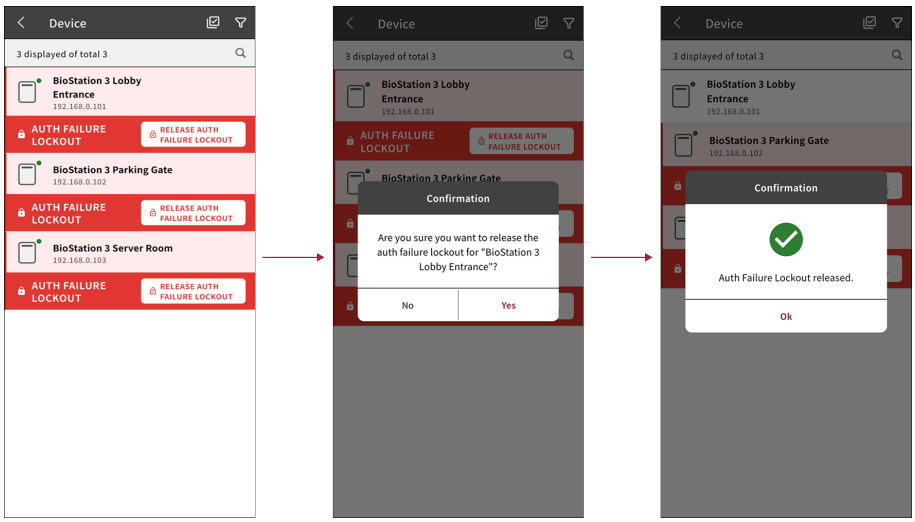
인증 실패 잠금 해제

연속된 인증 실패로 장치가 잠금 상태로 전환되면 모바일 앱을 통해 잠금을 해제할 수 있습니다.

알아두기
BioStar X에서 인증 실패 잠금 설정에 대한 자세한 내용은 인증 설정하기를 참고하세요.

개별 장치의 잠금 해제

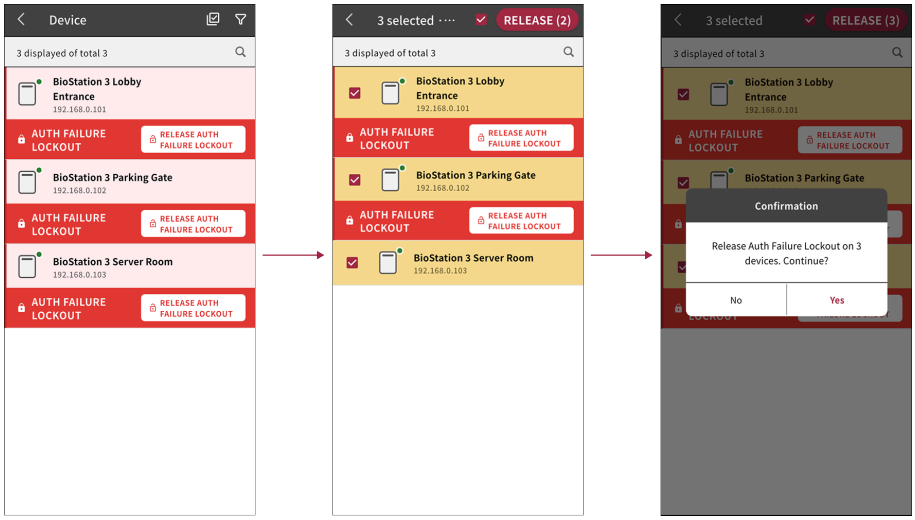
장치 목록에서 인증 실패 잠금 상태의 장치를 해제할 수 있습니다.



1. 장치 목록에서 **AUTH FAILURE LOCKOUT** 라벨이 표시된 장치를 확인하세요.
2. 해당 장치의 잠금을 해제하려면 **RELEASE AUTH FAILURE LOCKOUT** 버튼을 탭하세요.
3. 확인 메시지 창이 나타나면 **Yes** 버튼을 탭하세요.
4. 잠금 해제 성공 메시지가 나타나면 **OK** 버튼을 탭하세요.

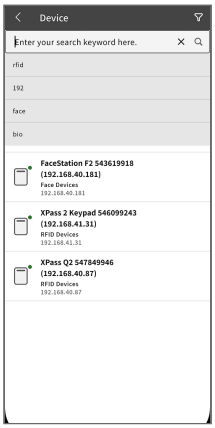
여러 장치의 잠금 해제

AUTH FAILURE LOCKOUT 라벨이 표시된 여러 개의 장치를 동시에 잠금 해제할 수 있습니다.



1. 장치 목록 오른쪽 상단의 를 탭하세요.
2. **AUTH FAILURE LOCKOUT** 라벨이 표시된 장치를 하나 이상 선택하세요.
3. 오른쪽 상단의 **RELEASE** 버튼을 탭하세요.
4. 확인 메시지 창이 나타나면 **Yes** 버튼을 탭하세요.
5. 잠금 해제 성공 메시지가 나타나면 **OK** 버튼을 탭하세요.

장치 검색



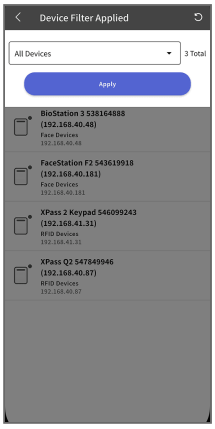
장치의 이름, 그룹, IP 주소를 기준으로 검색할 수 있습니다.

1. 장치 목록 상단의 를 탭하세요.
2. 검색 입력 필드에 검색어를 입력하세요. 장치 이름, 그룹 이름, IP 주소로 검색할 수 있습니다.
3. 검색어 입력을 완료한 후 를 탭하세요.

검색어와 일치하는 장치가 검색 결과로 표시됩니다.

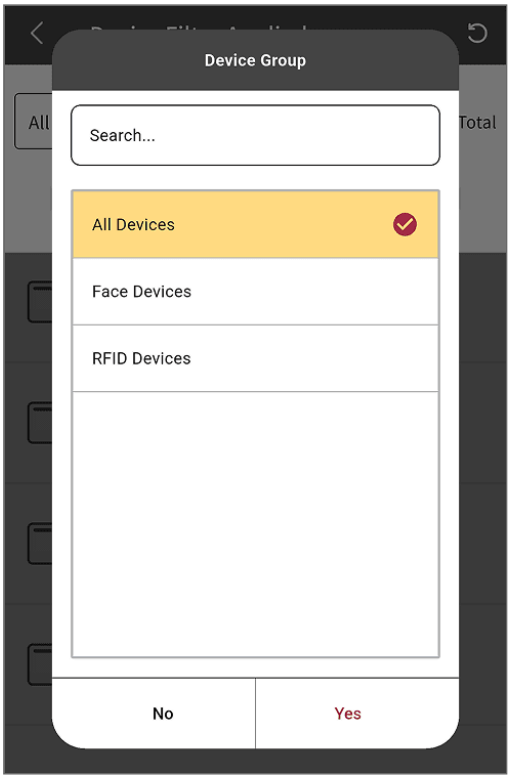
> **알아두기**
>
> - 검색 입력 필드 아래에는 최근 검색 기록이 표시됩니다. 최근 검색 기록을 탭하면 해당 검색어로 다시 검색할 수 있습니다.
> - 검색 입력 필드를 닫으려면 ✕를 탭하세요.

장치 목록 필터링



장치 목록을 장치 그룹 기준으로 필터링할 수 있습니다.

1. 장치 목록 상단의 를 탭하세요.
2. **All Devices**를 탭하세요.
3. 장치 그룹 목록에서 원하는 그룹을 선택하세요.



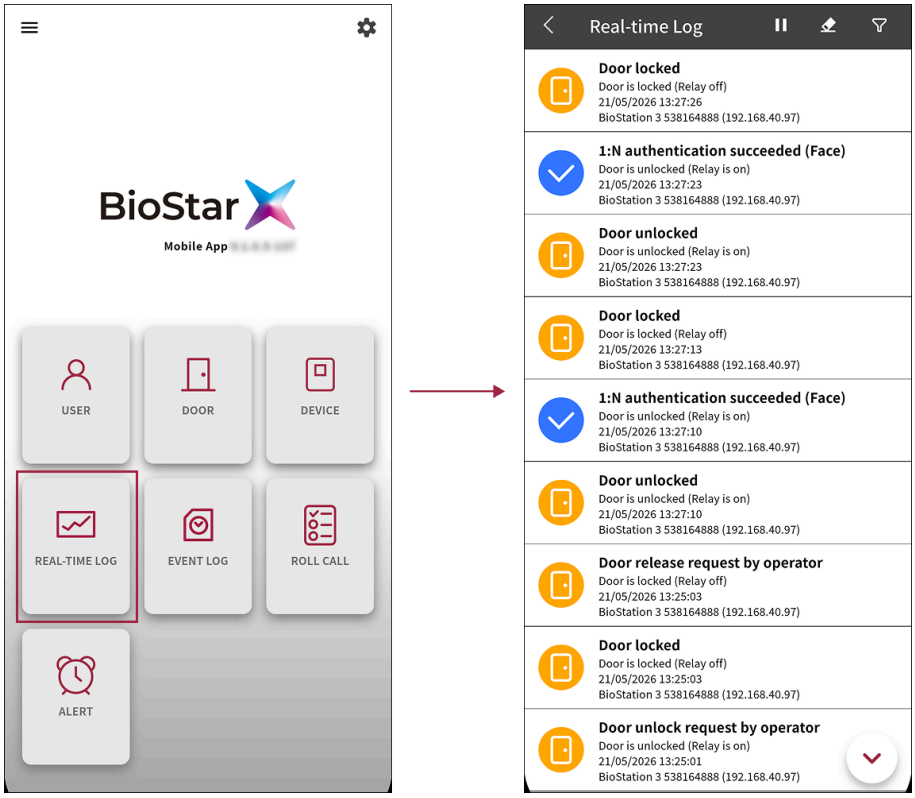
4. 장치 그룹 선택을 완료했다면 **Yes**를 탭하세요.
5. 선택한 조건으로 장치 목록을 필터링하려면 **Apply**를 탭하세요.

선택한 장치 그룹에 속한 장치들이 목록에 표시됩니다.

> **알아두기**
> 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.

실시간 로그 모니터링

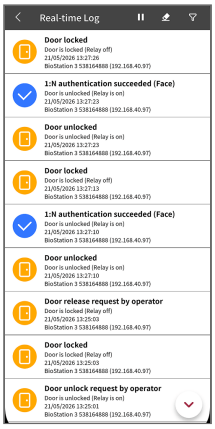
BioStar X 서버에서 발생하는 이벤트를 실시간으로 확인하세요. 앱 홈 화면에서 **REAL-TIME LOG**를 탭하세요.



REAL-TIME LOG 기능은 아래와 같은 상황에서 활용할 수 있습니다.

- 출근 시간대 출입 시도 모니터링
- 현재 수신되는 이벤트를 실시간으로 확인

실시간 로그 조회



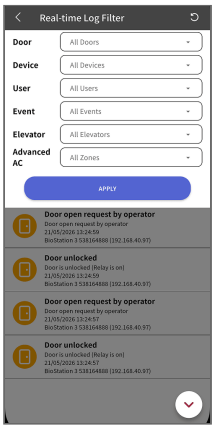
앱 홈 화면에서 **REAL-TIME LOG**를 탭하세요. 처음 실시간 로그(**Real-time Log**) 화면을 열면 목록이 비어 있습니다.

- 새로운 이벤트가 발생하면 자동으로 목록에 실시간으로 추가됩니다. 목록의 행 수는 제한이 없으며, 새로운 이벤트는 맨 위에 추가됩니다.
- 실시간 이벤트 수신을 일시 중지하려면 화면 오른쪽 상단의 ⏸를 탭하세요. 일시 중지된 상태에서는 새로운 이벤트가 목록에 추가되지 않지만 백그라운드에서 대기열에 추가됩니다. 실시간 이벤트 수신을 재개하려면 ▶를 탭하세요. 대기열에 추가된 이벤트가 새로운 이벤트보다 먼저 목록에 추가됩니다.
- 실시간 로그 목록을 비우려면 화면 오른쪽 상단의 을 탭하세요. 로그 목록이 비워지고, 새로운 이벤트가 발생할 때부터 실시간으로 추가됩니다.
- 실시간 로그 목록을 필터링하여 특정 이벤트, 사용자, 출입문 또는 장치 등 관련된 로그만 표시할 수 있습니다. 자세한 내용은 특정 로그만 보기를 참고하세요.

알아두기

- 다른 메뉴로 이동했다가 다시 **Real-time Log**로 돌아오면, 로그 목록은 비어지고, 새로운 로그가 발생할 때부터 실시간으로 추가됩니다.
- 로그에 표시되는 날짜와 시간은 BioStar X 서버의 환경 설정에 따릅니다. BioStar X에서 날짜 및 시간 표시 형식 설정에 대한 자세한 내용은 기본 설정 구성하기를 참고하세요.
- 실시간 로그 화면은 사이드 메뉴(☰) → **Monitoring** → **Real-time Log**를 탭하여 진입할 수도 있습니다.

특정 로그만 보기



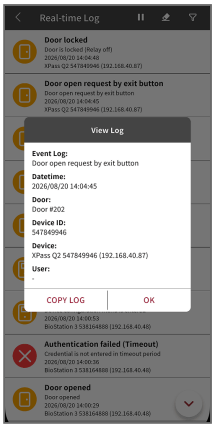
실시간 로그 목록에서 특정 이벤트, 사용자, 출입문 또는 장치 등 관련된 로그만 표시하도록 필터링할 수 있습니다.

1. 화면 오른쪽 상단의 를 탭하세요.
2. 원하는 로그만 표시하려면 아래 필터링 조건을 조합해 설정하세요.
   - **Door**: 특정 출입문 (예: 1층 정문 출입구)
   - **Device**: 특정 장치 (예: 특정 출입 통제 장치에서 발생한 이벤트)
   - **User**: 특정 사용자 (예: VIP 사용자의 출입 기록)
   - **Event**: 특정 이벤트 유형 (예: 얼굴 인증 실패, 침입 경보 알람 등)
   - **Elevator**: 특정 엘리베이터 (예: 특정 층의 엘리베이터)
   - **Advanced AC**: 특정 고급 출입 통제 (예: 안티패스백, 화재 경보, 스케줄 개방/잠금 등)
3. 설정한 조건으로 로그 목록을 필터링하려면 **Apply**를 탭하세요.

알아두기

- 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.
- 엘리베이터, 고급 출입 통제는 **에센셜**(Essential) 이상의 라이선스를 활성화했을 때 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

로그 상세 정보 확인



로그 항목을 탭하여 해당 로그의 상세 정보를 확인하세요.

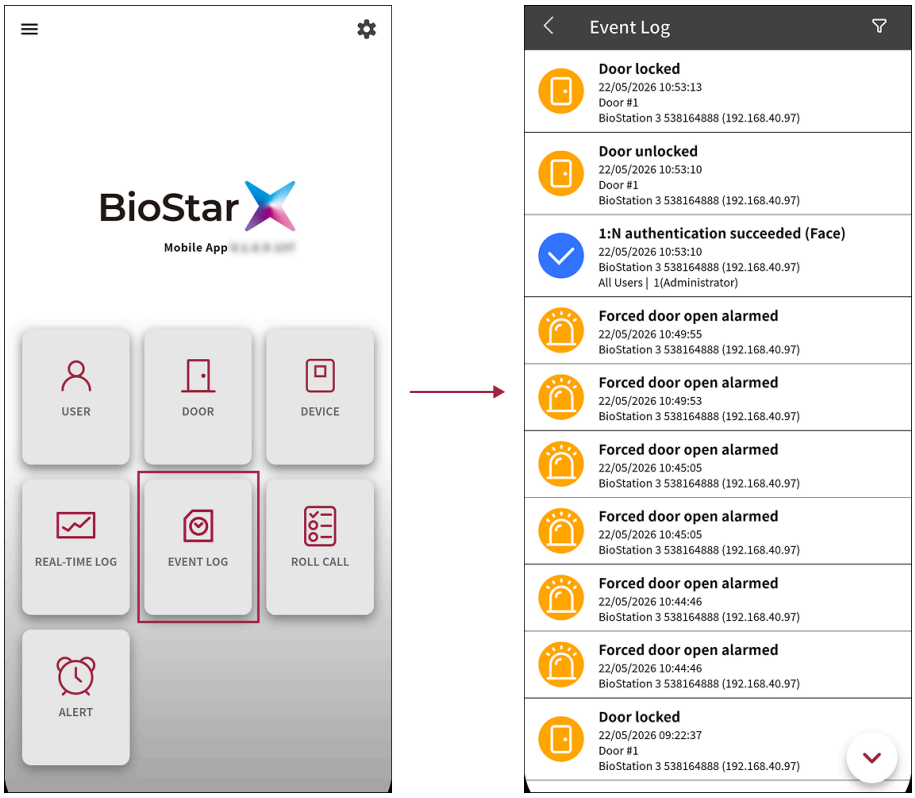
- **Event Log**: 이벤트 유형입니다. 어떤 유형의 이벤트가 발생했는지 표시합니다.
- **Datetime**: 이벤트가 발생한 날짜와 시간입니다.
- **Door**: 이벤트가 발생한 출입문입니다.
- **Device ID**/**Device**: 이벤트가 발생한 장치 ID와 이름입니다.
- **User**: 이벤트를 발생시킨 사용자입니다. 예를 들어, 출입 인증 이벤트의 경우 출입을 시도한 사용자가 표시됩니다.

상세 정보 팝업 하단의 버튼을 탭하여 다음 작업을 수행할 수 있습니다.

- 이벤트 정보를 클립보드에 복사하려면 **COPY LOG**를 탭하세요.
- 상세 정보 팝업을 닫으려면 **OK**를 탭하세요.

과거 로그 조회하기

과거 로그를 조회하여 특정 기간과 장소에서 발생한 출입 이력을 확인할 수 있습니다. 로그를 필터링하면 원하는 조건에 맞는 이벤트를 쉽게 찾을 수 있습니다.



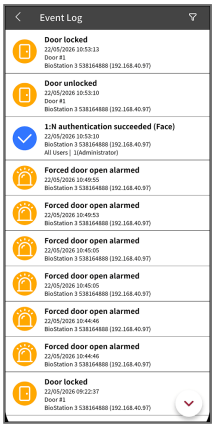
EVENT LOG 기능은 아래와 같은 상황에서 활용할 수 있습니다.

- 특정 사용자의 과거 출입 기록 확인
- 특정 기간 내 보안 이벤트 이력 추적
- 출입 통제 감사 및 보고

실시간 로그와의 차이

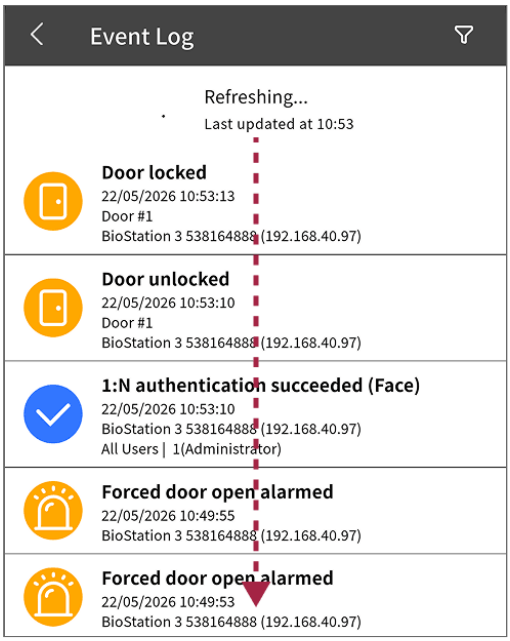
- **실시간 로그**: 현재 발생하는 이벤트를 즉시 모니터링할 수 있습니다. 실시간 로그는 현재 상황을 파악하고 즉각적인 대응이 필요한 경우에 유용합니다.
- **과거 로그**: 특정 기간의 이벤트 이력을 검색 및 조회할 수 있습니다.

과거 로그 조회



앱 홈 화면에서 **EVENT LOG**를 탭하세요.

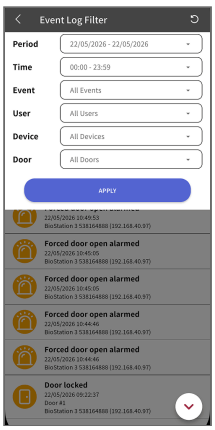
- 각 로그에는 이벤트 유형, 발생 시간, 출입문/장치, 사용자 정보가 표시됩니다.
- 로그 목록을 아래로 당겨서 새로고침하면 로그 목록이 갱신되고 최신 로그가 표시됩니다.



알아두기

- 로그에 표시되는 날짜와 시간은 BioStar X 서버의 환경 설정에 따릅니다. BioStar X에서 날짜 및 시간 표시 형식 설정에 대한 자세한 내용은 기본 설정 구성하기를 참고하세요.
- 이벤트 로그 화면은 사이드 메뉴(☰) → **Monitoring** → **Event Log**를 탭하여 진입할 수도 있습니다.

특정 로그만 보기



로그 목록에서 특정 이벤트, 사용자, 출입문 또는 장치 등 관련된 로그만 표시하도록 필터링할 수 있습니다.

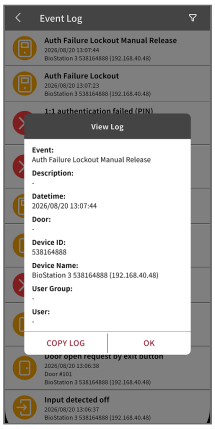
1. 화면 오른쪽 상단의 를 탭하세요.
2. 원하는 로그만 표시하려면 아래 필터링 조건을 조합해 설정하세요.
   - **Period**: 이벤트 발생 기간 설정
   - **Time**: 이벤트 발생 시간 설정
   - **Event**: 특정 이벤트 유형 선택 (예: 얼굴 인증 실패, 침입 경보 알람 등)

- **User**: 특정 사용자 선택 (예: VIP 사용자의 출입 기록)
- **Device**: 특정 장치 선택 (예: 특정 출입 통제 장치에서 발생한 이벤트)
- **Door**: 특정 출입문 선택 (예: 1층 정문 출입구)

3. 설정한 조건으로 로그 목록을 필터링하려면 **Apply**를 탭하세요.

> **알아두기**
> 필터링 조건을 초기화하려면 화면 오른쪽 상단의 → 을 탭하세요.

로그 상세 정보 확인



로그 목록에서 원하는 로그를 탭하면 해당 로그의 상세 정보를 확인할 수 있습니다.

- **Event**: 발생한 이벤트 유형입니다. (예: 출입 인증 성공, 출입 인증 실패, 알람 발생 등)
- **Description**: 이벤트에 대한 설명입니다.
- **Datetime**: 이벤트가 발생한 날짜와 시간입니다.
- **Door**: 이벤트가 발생한 출입문입니다.
- **Device ID**/**Device Name**: 이벤트가 발생한 장치 ID와 이름입니다.
- **User Group**: 이벤트를 발생시킨 사용자의 그룹 이름입니다.
- **User**: 이벤트를 발생시킨 사용자입니다.

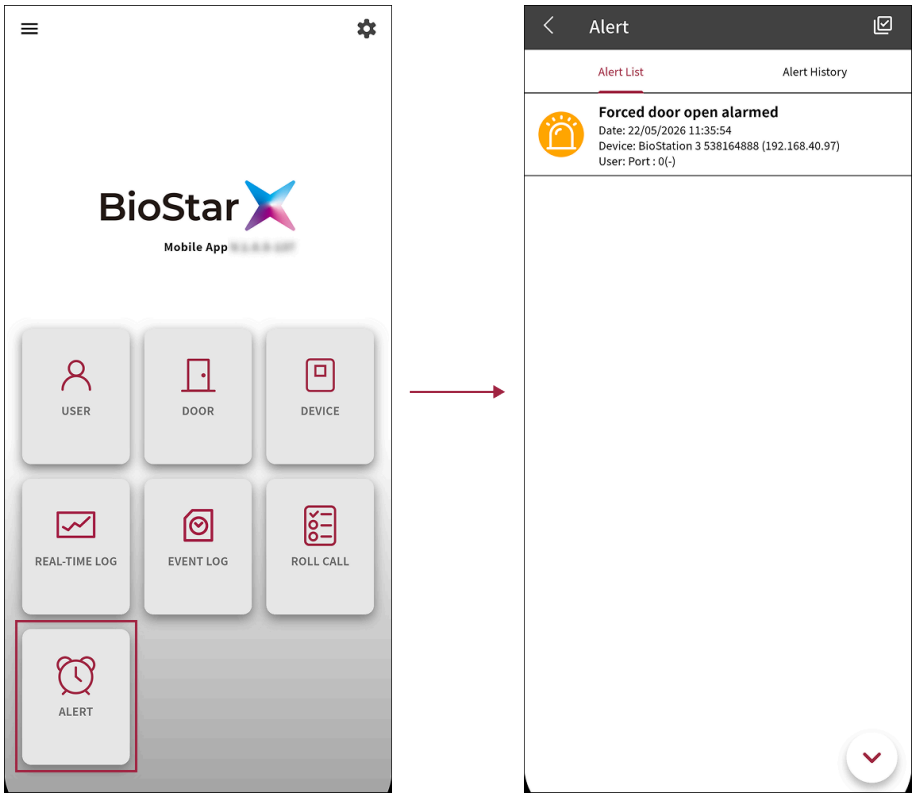
상세 정보 팝업 하단의 버튼을 탭하여 다음 작업을 수행할 수 있습니다.

- 이벤트 정보를 클립보드에 복사하려면 **COPY LOG**를 탭하세요.
- 상세 정보 팝업을 닫으려면 **OK**를 탭하세요.

> **알아두기**
> 이벤트 로그가 출입문 관련 이벤트라면 로그 상세 정보에 출입문 제어 관련 정보가 추가로 표시됩니다.

경보 알람 확인 및 해제하기

BioStar X에서 발생한 경보 알람을 모바일 앱에서 확인하고, 필요에 따라 경보를 해제할 수 있습니다. 출입문 강제 열림과 같은 경보 알람 이벤트가 발생했을 때, 앱에서 경보 알람을 확인하고 조치 사항을 기록할 수 있습니다.



알아두기

- BioStar X에서 경보 알람을 확인하고 해제하는 방법에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.
- 경보 알람 목록에 표시되는 날짜와 시간은 BioStar X 서버의 환경 설정에 따릅니다. BioStar X에서 날짜 및 시간 표시 형식 설정에 대한 자세한 내용은 기본 설정 구성하기를 참고하세요.

경보 알람 목록 (Alert List)

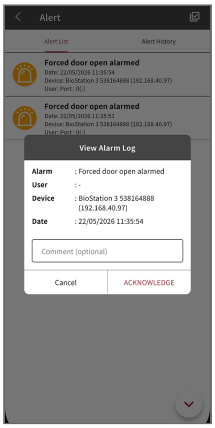


앱 홈 화면에서 **ALERT**를 탭하세요. 경보 알람 목록(**Alert List**)을 확인할 수 있습니다.

경보 알람 목록에서는 출입문 강제 열림과 같은 경보 알람 이벤트를 최신 순으로 확인할 수 있습니다. 새로운 경보 알람 이벤트가 발생하면 자동으로 목록에 실시간으로 추가됩니다.

알아두기

경보 알람 화면은 사이드 메뉴(☰) → **Alert**을 탭하여 진입할 수도 있습니다.

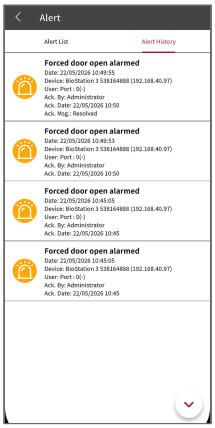


알람 상세 정보 보기

경보 알람 목록에서 특정 알람을 탭하면, 해당 알람의 상세 정보를 확인할 수 있습니다. 알람 상세 정보에는 발생한 알람 이벤트의 유형 및 사용자, 발생 시간, 출입문/장치 등이 표시됩니다.

- 경보 알람을 확인하고 조치 사항 등을 기록하려면 **Comment (optioinal)** 필드에 내용을 입력하세요. 입력한 내용은 BioStar X 서버에 저장되고, 알람 이벤트의 상세 정보에서 확인할 수 있습니다.
- 조치 사항을 입력하고 경보 알람을 해제하려면 **ACKNOWLEDGE**를 탭하세요. 경보 알람이 해제되고, **Alert List**에서 해당 알람 이벤트가 사라집니다.

경보 알람 내역 (Alert History)



경보 알람 내역에서는 확인된 경보 이벤트를 확인할 수 있습니다. 각 알람 이벤트의 유형, 발생 시간, 출입문/장치, 사용자 등의 정보를 확인할 수 있습니다. 확인된 알람 이벤트는 어떤 사용자가 언제 확인했는지 등의 정보도 함께 표시됩니다.

인원 점검(Roll Call) 시작하기

인원 점검(Roll Call)은 특정 시점과 장소 내 출입 기록을 기반으로 인원 목록을 신속하게 생성합니다. 위급 상황이 발생하면, 사용자가 미리 지정된 장소의 입실 또는 퇴실 장치를 통해 인증하여 인원 점검 장소에 도착했는지 파악할 수 있습니다.

비상 대응, 안전 확인, 구조대 정보 제공 등을 위해 사용할 수 있습니다. 이를 통해 출입 기록을 효율적으로 활용하여 인원 현황을 관리할 수 있습니다.

> **알아두기**
>
> - 인원 점검을 시작하기 전에, BioStar X에서 인원 점검 설정을 완료해야 합니다. 인원 점검 설정 방법에 대한 자세한 내용은 인원 점검(Roll Call)을 참고하세요.
> - 인원 점검 설정은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

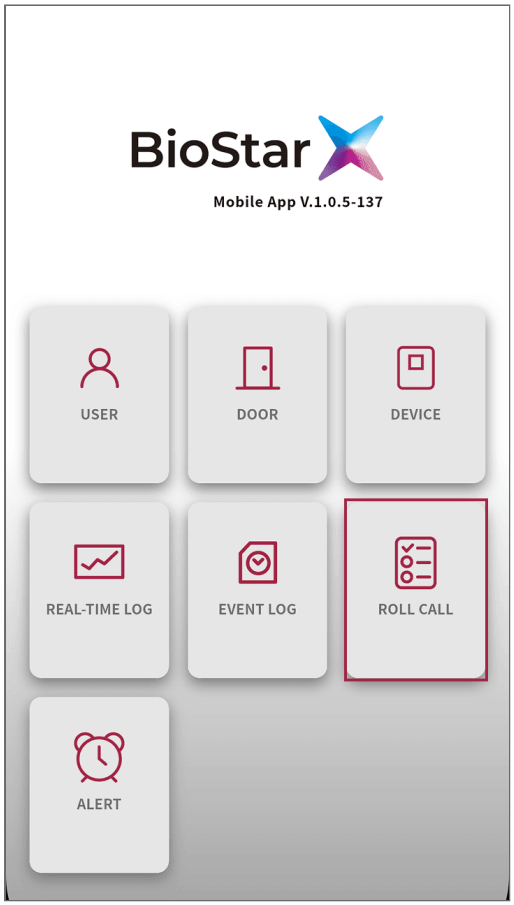
모바일 앱에서 인원 점검 사용

인원 점검 기능은 BioStar X 모바일 앱에서 사용할 수 있습니다.

인원 점검 시작

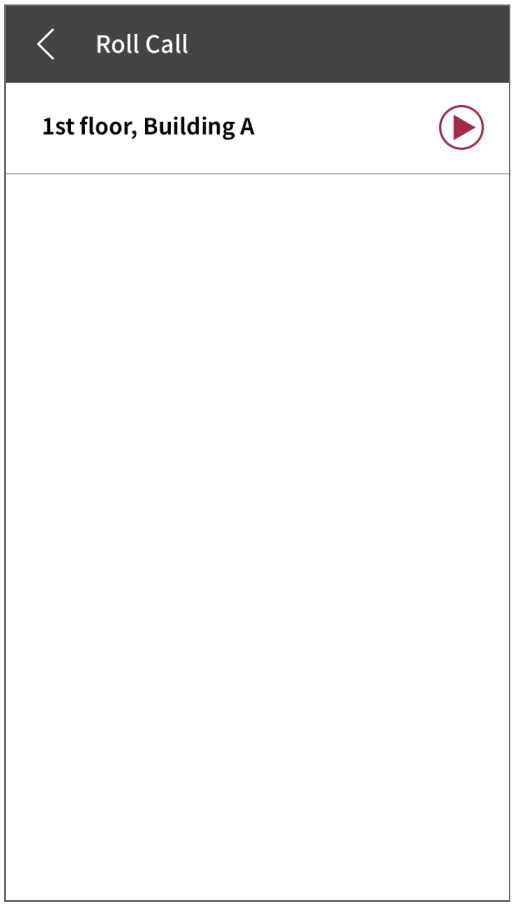
모바일 앱에서 인원 점검 기능을 시작하려면 다음 단계를 따르세요.

1. 모바일 기기에서 BioStar X 모바일 앱을 실행하세요.
2. 앱의 홈 화면에서 **ROLL CALL**을 탭하세요.



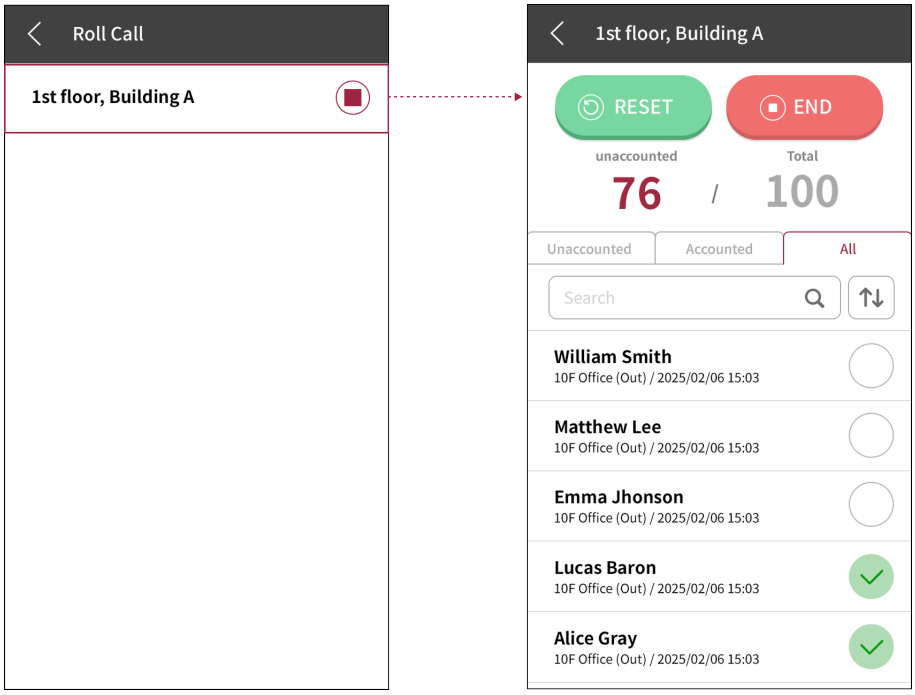
> 사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Monitoring** → **Roll Call**을 탭하세요.

3. Roll Call 목록에서 인원 점검을 실행할 항목의 ▶를 탭하세요.



4. 확인 메시지가 나타나면 **Yes**를 탭하세요.

인원 점검을 시작하며, 진행 중인 인원 점검 항목을 탭하면 인원 점검 현황을 확인할 수 있습니다.



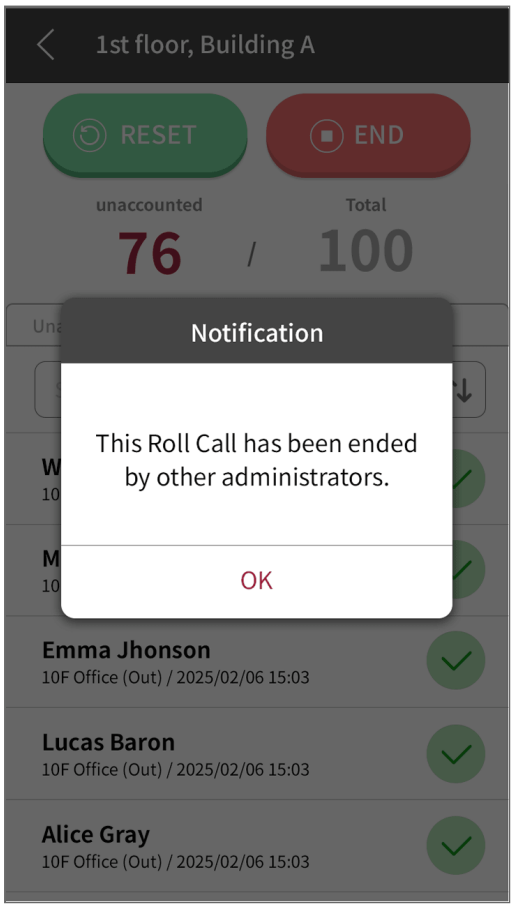
진행 중인 인원 점검 제어

- 입실 사용자는 ✓ 아이콘이 표시됩니다. 모든 사용자가 입실하면 인원 점검이 종료 메시지가 나타납니다. 인원 점검을 종료하려면 **Yes**를 탭하세요.

- 관리자가 수동으로 사용자의 입실 또는 상태를 변경할 수 있습니다. 사용자 목록에서 상태를 변경할 사용자의 가장 오른쪽의 원 버튼을 길게 터치하세요.



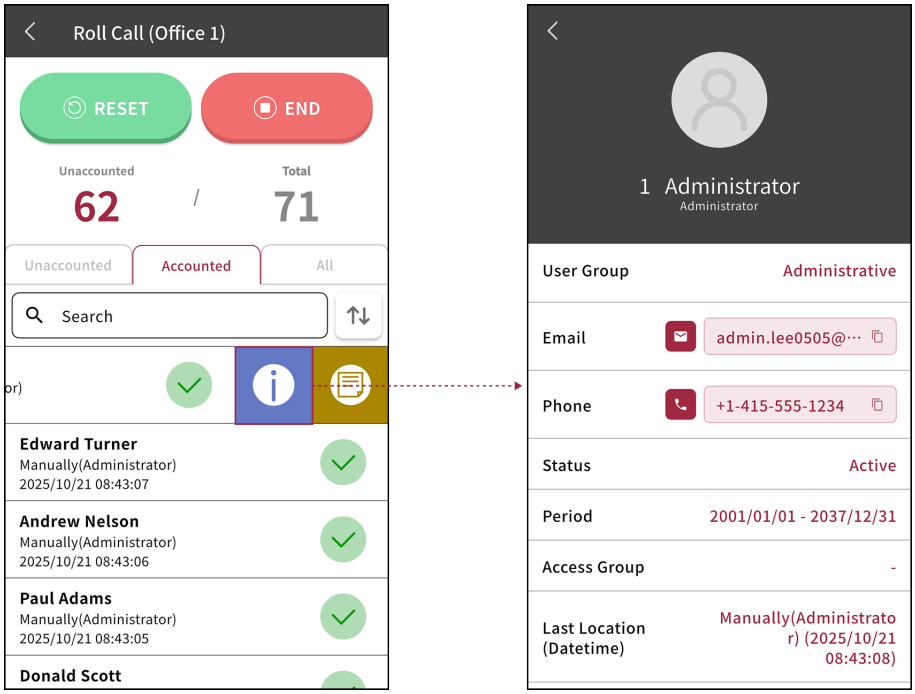
- 인원 점검을 초기화하려면 **Reset**을 탭하세요. 현재까지의 모든 변경 사항이 삭제되고 인원 점검을 처음부터 다시 시작할 수 있습니다.
- 다른 관리자에 의해 인원 점검이 종료되면 알림 메시지가 나타납니다.



인원 점검 진행 중 사용자 정보 확인

모바일 앱에서 인원 점검 진행 중 각 사용자의 정보를 확인할 수 있습니다. 사용자에게 긴급 연락을 취할 수 있는 연락처 정보, 사용자의 마지막 위치 등의 세부 정보를 확인할 수 있습니다.

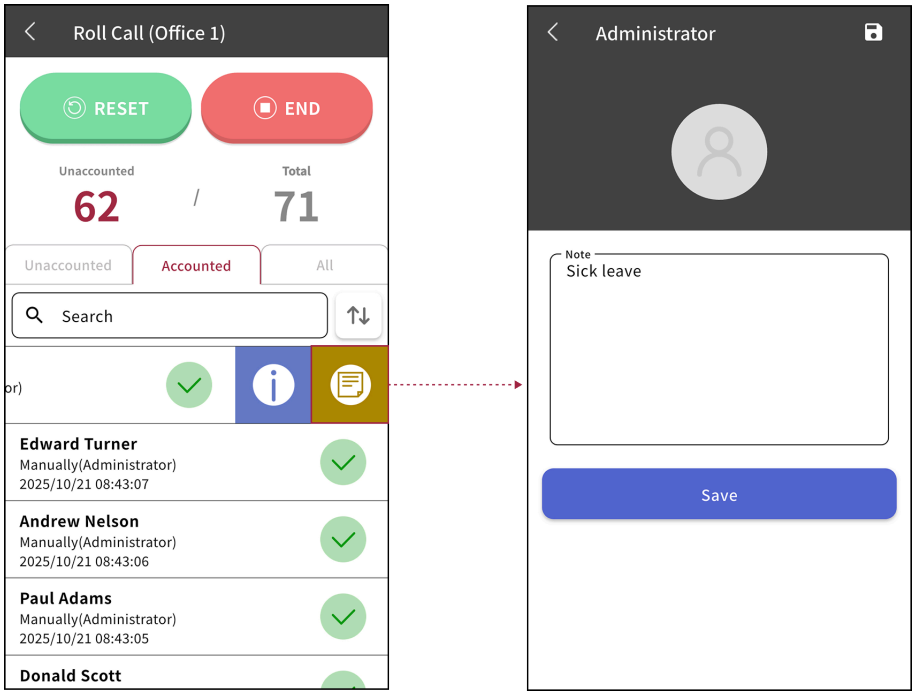
인원 점검 진행 중 세부 정보를 확인할 사용자 항목을 왼쪽으로 스와이프하세요. 이후 ⓘ을 탭하세요.



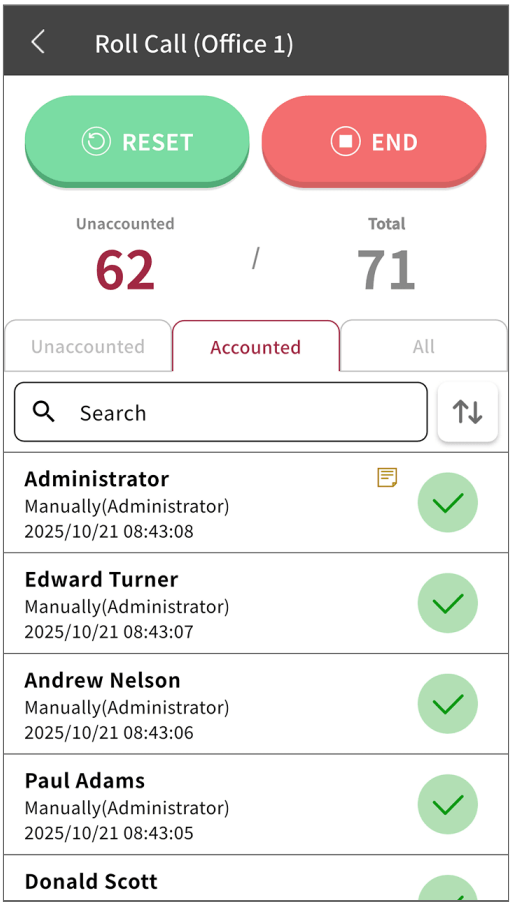
인원 점검 진행 중 사용자에게 메모 남기기

모바일 앱에서 인원 점검 진행 중 특정 사용자가 입실하지 않은 경우, 해당 사용자에게 메모를 남길 수 있습니다.

인원 점검 진행 중 메모를 입력할 사용자 항목을 왼쪽으로 스와이프하세요. 이후 를 탭하세요. 메모 입력 화면에서 내용을 입력한 후 **Save**를 탭하세요.



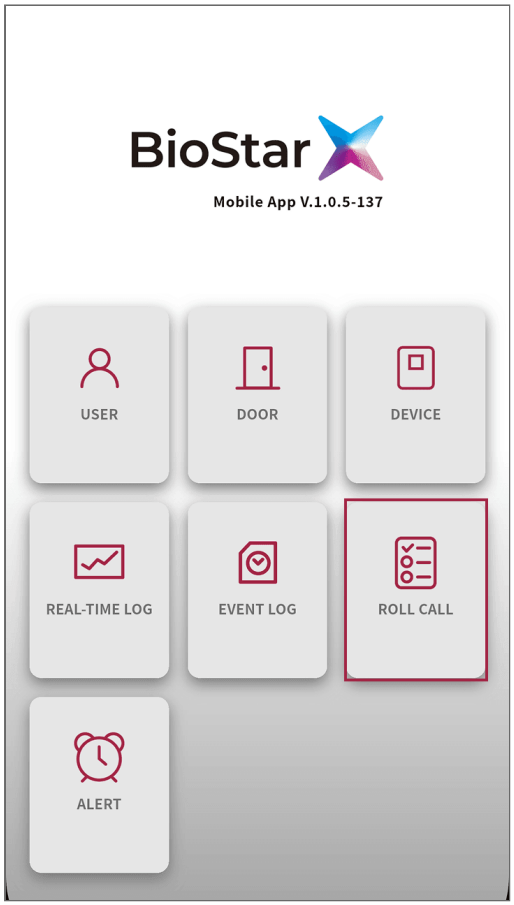
메모를 입력한 사용자는 인원 점검 목록에서 아이콘이 표시됩니다.



인원 점검 세부 정보 확인

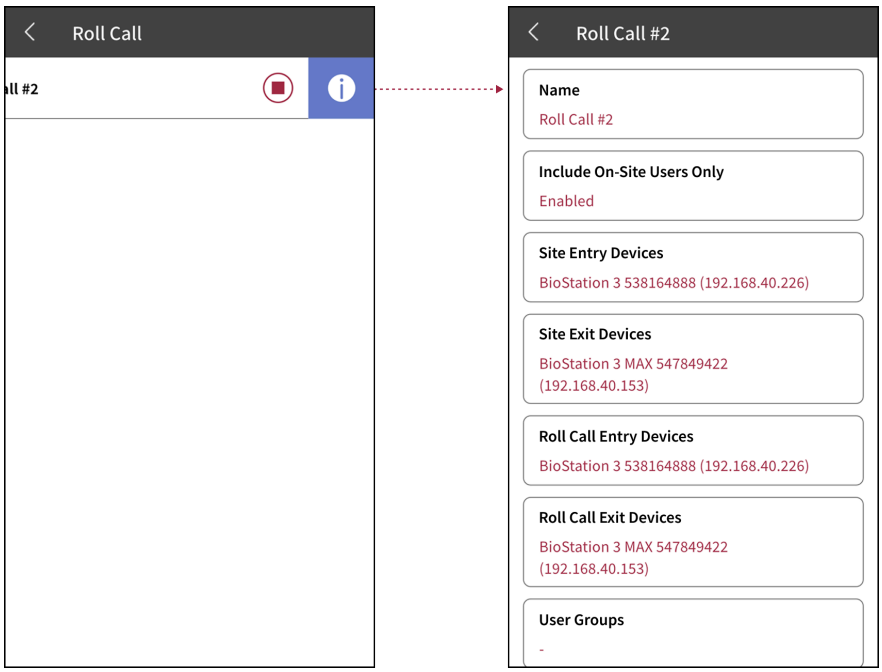
모바일 앱에서 인원 점검 설정의 세부 정보를 확인할 수 있습니다.

1. 모바일 기기에서 BioStar X 모바일 앱을 실행하세요.
2. 앱의 홈 화면에서 **ROLL CALL**을 탭하세요.



사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Monitoring** → **Roll Call**을 탭하세요.

3. 목록에서 세부 정보를 확인할 항목을 왼쪽으로 스와이프한 후 ⓘ을 탭하세요.

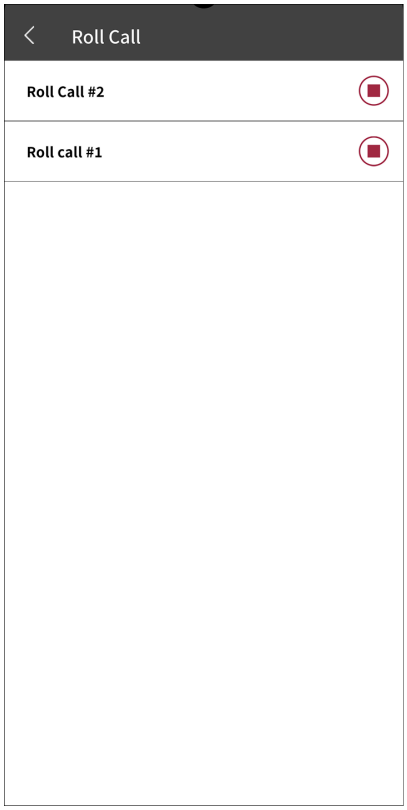


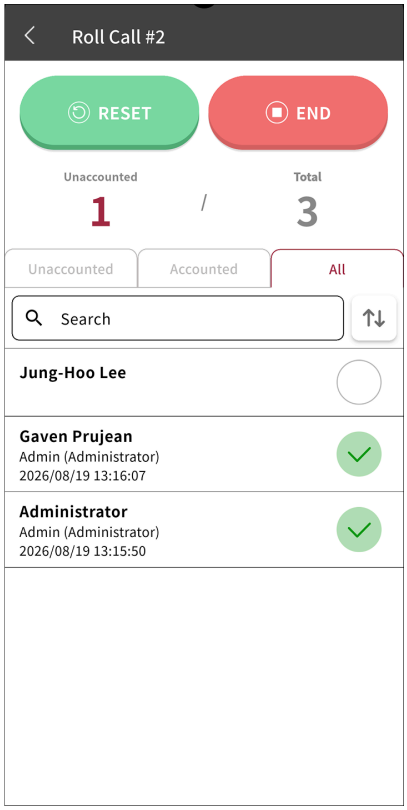
인원 점검 종료

진행 중인 인원 점검은 **BioStar X** 모바일 앱과 웹에서 모두 종료할 수 있습니다.

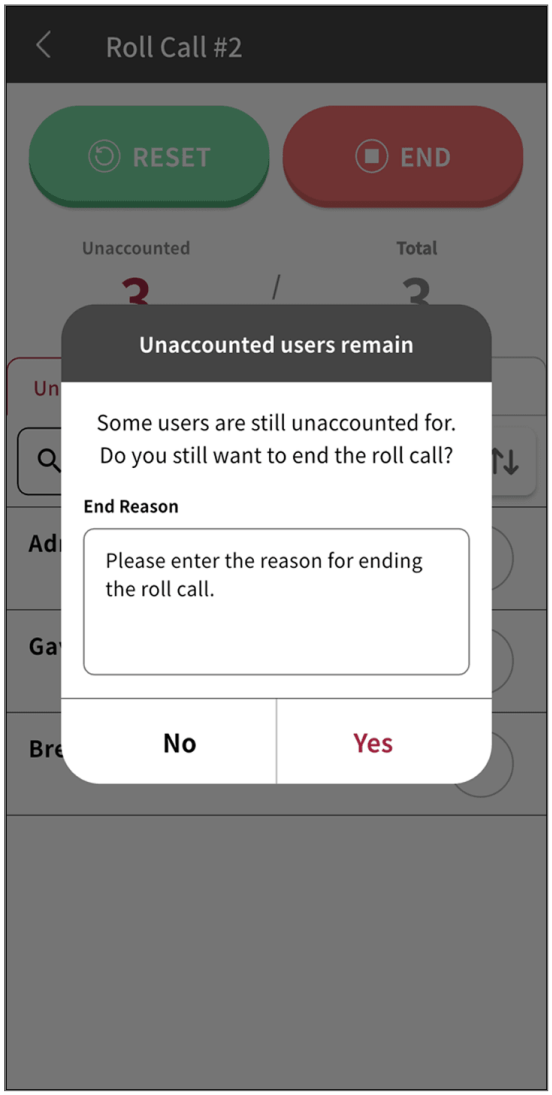
모바일 앱에서 종료

1. 인원 점검을 종료하려면 인원 점검 목록 화면에서 ⏹ 버튼을 탭하거나 인원 점검 현황 화면에서 **END** 버튼을 탭하세요.





2. 미확인 사용자가 남아 있으면 경고 팝업이 나타나며, 인원 점검을 종료하려면 종료 사유를 입력하고 **Yes** 버튼을 탭하세요.



웹에서 종료

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. 목록에서 **인원 점검**을 클릭하세요.
4. 인원 점검 목록 중 종료할 항목의 체크박스를 클릭하세요.



5. 화면 오른쪽 상단의 **종료** 버튼을 클릭하세요.
6. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.

미확인 사용자가 없는 인원 점검은 바로 종료됩니다. 미확인 사용자가 남아 있는 인원 점검은 **미확인 사용자** 목록과 **종료 사유** 입력란이 있는 대화 상자가 나타납니다. 인원 점검을 종료하려면 사유를 입력하고 **인원 점검 종료** 버튼을 클릭하세요.



알아두기

- **종료 사유**는 최대 500자까지 입력할 수 있습니다.
- 여러 인원 점검 항목을 동시에 선택해 종료할 때 그중 하나라도 미확인 사용자가 남아 있으면 종료할 수 없습니다. 인원 점검 항목을 하나씩 선택해 종료하세요.

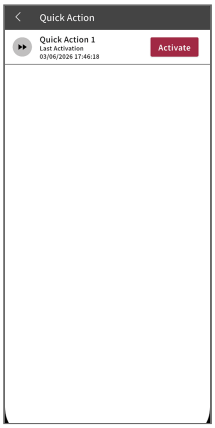
퀵 액션 사용하기

퀵 액션은 긴급 상황에서 복잡한 제어 절차를 자동화하는 기능입니다. 미리 정의한 여러 기기의 동작을 하나의 버튼으로 즉시 실행하여 신속하게 대응할 수 있습니다.

알아두기

- 퀵 액션 기능에 대한 자세한 내용은 퀵 액션 사용하기를 참고하세요.
- 모바일 앱에서는 퀵 액션 기능을 실행하거나 퀵 액션 항목에 대한 자세한 정보를 확인할 수 있습니다. 퀵 액션을 생성하거나 편집하려면 BioStar X 웹 인터페이스에 로그인하여 설정해야 합니다.

퀵 액션 실행



BioStar X 웹 인터페이스에서 퀵 액션을 생성해야 모바일 앱에서 사용할 수 있습니다.

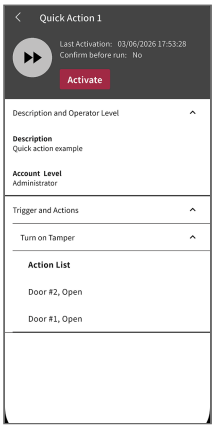
1. 앱 홈 화면에서 **QUICK ACTION**을 탭하세요.
2. 퀵 액션 목록에서 실행할 퀵 액션 항목의 **Activate** 버튼을 탭하세요.

퀵 액션이 성공적으로 실행되면 성공 메시지가 표시됩니다.

알아두기

- 퀵 액션 설정에 따라 실행 여부를 묻는 팝업이 표시될 수 있습니다.
- 각 퀵 액션 항목에는 최근 실행 일시가 표시됩니다.

퀵 액션 상세보기



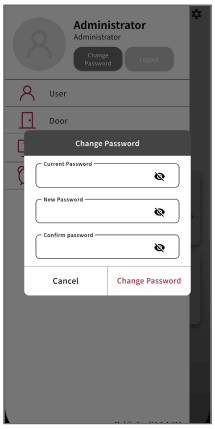
퀵 액션 항목에 설정된 자세한 정보를 확인하려면 퀵 액션 목록에서 항목을 탭하세요.

- **Last Activation**: 퀵 액션이 마지막으로 실행된 일시입니다.
- **Confirm before run**: 퀵 액션 실행 여부를 묻는 팝업이 표시되는지 여부입니다.
- **Activate**: 퀵 액션을 실행하는 버튼입니다.
- **Description and Operator Level**: 퀵 액션에 대한 설명과 실행 권한이 필요한 관리자 등급입니다.
- **Trigger and Actions**: 퀵 액션이 실행될 때 제어되는 출입문과 출입문에 적용되는 동작입니다.

> **알아두기**
> 작업 조건 및 동작에 대한 자세한 내용은 작업 조건 및 동작 설정하기를 참고하세요.

계정 비밀번호 변경하기

BioStar X 모바일 앱에서 계정의 비밀번호를 변경할 수 있습니다. 계정의 비밀번호를 정기적으로 변경하여 계정 보안을 강화할 수 있습니다.



1. 앱 홈 화면에서 화면 왼쪽 상단의 ☰을 탭하세요.
2. 사이드 메뉴에서 **Change Password**를 탭하세요.
3. **Current Password** 입력 필드에 현재 비밀번호를 입력하세요.
4. 새로운 비밀번호를 **New Password**, **Confirm password** 입력 필드에 차례로 입력하세요.
5. 비밀번호 변경을 완료하려면 **Change Password**를 탭하세요.

부록

제품에 포함된 법적 고지 사항을 수록합니다.

면책 조항

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

저작권 공지

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

오픈 소스 라이선스

이 제품에는 오픈 소스 소프트웨어가 포함되어 있습니다. GPL, LGPL, MPL 및 소스 코드 배포가 필요한 기타 오픈 소스 라이선스가 적용되는 소스 코드는 슈프리마 기술 지원팀(CS@suprema.co.kr)으로 요청하여 전달 받을 수 있습니다.

이 제품의 소스 코드는 제품의 최종 배송일로부터 3년 동안 슈프리마 기술 지원팀(CS@suprema.co.kr)으로 요청하여 전달 받을 수 있습니다.

기타 물리적 매체를 통해 소스 코드 전달 받으실 경우 비용이 청구될 수 있습니다. 이 제안은 이 정보를 받은 모든 이에게 유효합니다.

이 제품에 포함된 오픈 소스 소프트웨어에 대한 필수 고지 사항과 라이선스는 ⚙ → **License**에서 확인할 수 있습니다.

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

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