BioStar X

관리자 가이드

버전 1.0.3

한국어

KO 102.00.BSX

suprema

SECURITY & BIOMETRICS

목차

개요 6

한층 강화된 운영 효율성과 보안성 6

강력한 확장성과 안정성 제공 6

시작하기 전에 7

지원 장치 11

시스템 최소 요구사항 13

시작하기 17

네트워크 우선순위 확인하기 17

간편 설치하기 24

사용자 정의 설치하기 31

업그레이드하기 39

멀티 커뮤니케이션 서버 설치하기 46

로그인하기 53

라이선스 키 등록하기 55

초기 설정 가이드 58

서버 관리 60

서버 시작 및 종료 60

서비스 설정 61

메인 서버의 IP 주소 변경하기 64

포트 변경하기 67

데이터베이스 변경하기 68

보조 데이터베이스 추가하기 69

BioStar X 서버 제거 및 보안 인증서 복구하기 78

런처 84

사용자 85

사용자 그룹 관리하기 85

사용자 등록하기 89

사용자 기본 정보 입력하기 91

사용자 크리덴셜 등록하기 93

사용자 권한 설정하기 116

사용자 고급 설정하기 119

신분증 스캔으로 사용자 등록 및 수정하기 120

사용자 탐색하기 124

사용자 관리하기 129

출입 그룹 관리하기 139

다중 인증으로 로그인하기 140

얼굴 일괄 등록하기 143

얼굴 마이그레이션 147

비상 개방 권한 설정하기 149

모니터링 152

출입문 모니터링하기 152

맵 모니터링하기 178

장치 모니터링하기 187

비디오 모니터링하기 195

이벤트 모니터링하기 202

데이터 210

리포트 생성하기 210

자동 생성 스케줄 설정하기 224

리포트 저장 경로 설정하기 226

대시보드 227

위젯 추가하기 227

위젯 수정하기 233

위젯 삭제하기 234

설정 235

장치 관리하기 235

장치 설정하기 257

이미지 로그 설정하기 293

USB 에이전트 설정하기 297

장치 연결 관리 설정하기 298

출입문 관리하기 301

운영 권한 관리하기 313

장기 미출입자 조치하기 319

신분증 스캔 설정하기 323

출입 통제 설정하기 324

스케줄 설정하기 334

작업 조건 및 동작 설정하기 337

퀵 액션 사용하기 339

이벤트 로그 가져오기 342

경보 설정하기 343

크리덴셜 관리하기 345

라이선스 활성화하기 367

감사 추적 관리하기 373

시스템 설정하기 381

고급 설정 412

엘리베이터 관리하기 412

고급 출입 통제 설정하기 419

비디오 설정하기 449

맵 관리하기 470

방문자 설정하기 485

디렉토리 연동 설정하기 489

리모트 액세스 설정하기 501

가상 장치 이벤트 로그 연동하기 503

플러그인 508

플러그인(Plugins)이란? 508

BioStar X 제공 플러그인 508

주요 활용 사례 508

플러그인 등록 508

플러그인 관리 510

근태 관리 사용하기 511

방문자 신청 및 관리하기 556

UI 알아보기 571

공통 UI 이해하기 571

사용자 571

모니터링 573

대시보드 573

설정 574

라이선스 정책 576

기본 라이선스 576

라이선스 업그레이드 577

기능 추가 옵션 (Feature Add-ons) 577

고급 출입 통제(Advanced Access Control) 578

장치 라이선스 579

부록 580

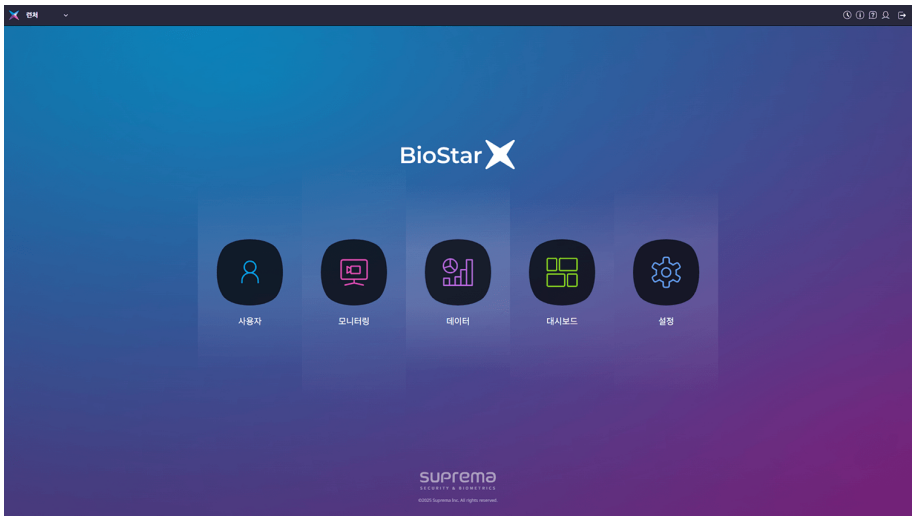
면책 조항 580

저작권 공지 581

오픈 소스 라이선스 581

개요

BioStar X는 AI 기반 출입통제와 지능형 영상 분석을 결합한 슈프리마의 차세대 통합 보안 플랫폼입니다. 단순한 출입 관리를 넘어 보안 운영 전반을 효과적으로 통합 관리할 수 있는 혁신적인 플랫폼입니다.



AI 기반 출입통제와 지능형 영상 분석 결합의 완성인 **BioStar X**는 AI 기술을 활용해 실시간 출입 관리와 영상 모니터링, 이상 행동 감지를 하나의 플랫폼에서 수행할 수 있도록 설계되었습니다. 출입통제뿐만 아니라 침입 탐지, 배회 감지, 쓰러짐 감지 등 다양한 AI 기반 영상 분석 기능을 갖추고 있어 사전 대응이 가능합니다.

또한, 피플카운팅, 테일게이팅 감지, 블랙리스트 검출, 실종자 수색 기능을 통해 대형 시설에서도 더욱 정교한 보안 관제를 지원합니다. 이러한 기능은 학교, 쇼핑몰, 공항, 병원과 같은 다중 이용 시설뿐만 아니라 스마트 빌딩에서도 유용하게 활용할 수 있습니다.

한층 강화된 운영 효율성과 보안성

BioStar X는 하나의 플랫폼에서 모든 보안 요소를 실시간으로 통합 관리할 수 있도록 지원합니다. 이를 통해 보안 담당자는 개별 시스템을 따로 관리할 필요 없이 단일 인터페이스에서 효율적으로 모니터링하고 제어할 수 있습니다.

또한, 통합된 운영 방식은 보안 관제 인력을 최적화하고 유지보수에 드는 비용과 시간을 절감하는 효과를 가져옵니다. 별도의 개별 보안 시스템을 추가할 필요 없이, **BioStar X**의 유연한 확장성을 활용하면 필요한 기능을 손쉽게 추가할 수 있어 더욱 안전하고 효율적인 보안 환경을 구축할 수 있습니다.

강력한 확장성과 안정성 제공

대기업이나 공공기관 등의 엔터프라이즈 환경에서는 보안 시스템의 확장성과 안정성이 필수적입니다. **BioStar X**는 수만 명 이상의 사용자 등록을 지원하며, 다양한 장치를 연결해도 안정적인 운영이 가능합니다.

또한, 사용자 맞춤형 UI·UX를 제공해 복잡한 보안 운영을 더욱 직관적으로 관리할 수 있도록 지원합니다. 모니터링 화면의 인터페이스 레이아웃을 직접 구성할 수 있어, 원하는 정보를 빠르고 효과적으로 확인할 수 있습니다.

필수 보안 솔루션 BioStar X

보안 위협이 다양해지고 보안 운영의 복잡성이 증가하는 지금, AI와 통합 보안 기술을 결합한 **BioStar X**는 필수적인 보안 솔루션으로 자리 잡고 있습니다. 강력한 보안성과 효율적인 운영을 동시에 원하는 기업이라면, **BioStar X**가 최고의 선택이 될 것이라고 확신할 수 있습니다.

시작하기 전에

> **팁**
> **BioStar X**를 시작하기 전에 알아야 할 내용을 안내합니다. **BioStar X**는 64비트 운영 체제를 지원합니다. **BioStar X**를 설치하려는 PC의 시스템 사양을 확인한 후 설치하세요.

설치 전 참고 사항

BioStar X를 설치하기 전에 다음 사항을 확인하고 설치를 진행하세요.

- **BioStar X**는 64bit 운영체제에서만 설치할 수 있습니다.
- MS SQL 2012 Express를 사용한다면 서비스 팩 3를 설치하세요.
- MS SQL 2014 Express를 사용한다면 서비스 팩 2를 설치하세요.
- MS SQL Server를 사용할 경우 서버 및 각 테이블의 `Collation` 옵션을 CI(Case-insensitive)로 설정하세요.
- 이전 버전의 **BioStar X**에서 데이터베이스를 백업할 때 모든 서비스를 사용 중지한 후 진행하세요. 또한, AC 데이터베이스와 TA 데이터베이스를 함께 백업하고, 복원하지 않으면 TA 데이터베이스를 사용할 수 없습니다.
- **BioStar X** 데이터베이스를 백업하려면 *\Program Files\BioStar X\util* 폴더의 *enckey* 파일과 *\Program Files\BioStar X* 폴더의 *system.conf*, *setting.conf* 파일도 반드시 함께 백업하세요. 그렇지 않으면, 데이터베이스를 사용할 수 없게 됩니다.
- **BioStar X**가 사용하는 포트의 기본값은 서비스 설정을 참고하세요. 다른 프로그램에서 동일한 포트를 점유한다면, **BioStar X**가 정상 구동되지 않을 수 있습니다.

데이터베이스 확인

BioStar X를 설치하기 전에 사용자가 직접 구성한 데이터베이스를 사용한다면 아래 사항을 확인하세요.

MariaDB

1. *my.cnf* 파일에서 `[mysql]` 항목 하단의 옵션을 아래와 같이 변경하세요.

   my.cnf

   ```
   character-set-server=utf8
   collation-server=utf8_unicode_ci
   max_connections = 600
   ```

2. *my.cnf* 파일에서 `[mysql]` 항목 하단에 아래 옵션을 추가하세요.

   my.cnf

   ```
   log_bin_trust_function_creators = 1
   group_concat_max_len = 102400
   ```

3. 루트(root) 권한으로 MariaDB에 접속해 아래 명령어를 실행하세요.

   SQL

```
GRANT SUPER ON . TO user_id@'localhost' IDENTIFIED BY "password";
GRANT SUPER ON . TO user_id@'%' IDENTIFIED BY "password";
```

MS SQL Server

> **알아두기**
>
> - 모든 데이터베이스 및 테이블의 `Collation` 옵션을 대소문자로 구분하지 않는 CI(Case-insensitive)로 설정하세요.
> - 데이터베이스 이름에는 숫자, 영문(대소문자 구분), 특수 기호 `-` `_`만 사용할 수 있습니다.

포트 설정

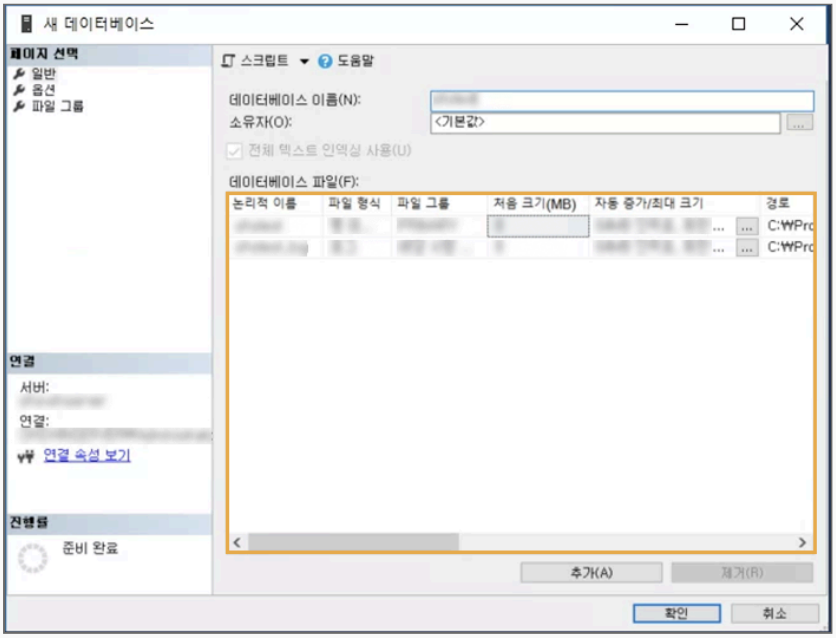
- **SQL Server 구성 관리자**를 실행한 후 **SQL EXPRESS에 대한 프로토콜**의 **TCP/IP 프로토콜**을 사용하려는 포트 번호로 설정하세요.
- 설정을 적용하려면 SQL Server 서비스를 재시작하세요.

사용자 및 데이터베이스 생성

1. **SQL Server Management Studio**에 **SQL Server 인증**을 이용하여 **sa** 계정으로 로그인하세요.
2. **보안**에서 마우스 오른쪽 버튼을 클릭한 뒤 **새 로그인**을 클릭하세요.
3. **로그인 이름** 필드에 원하는 이름을 입력한 뒤 **SQL Server 인증**을 선택하세요.
4. **암호**와 **암호 확인** 필드에 사용하려는 암호를 입력한 뒤 **암호 정책 강제 적용**을 해제하세요.
5. **확인**을 클릭하세요.
6. **데이터베이스**에서 마우스 오른쪽 버튼을 클릭한 뒤 **새 데이터베이스**를 클릭하세요.
7. **데이터베이스 이름** 필드에 원하는 이름을 입력하세요.
8. **소유자** 필드에 3단계에서 설정한 로그인 이름을 입력하세요.

팁

데이터베이스 파일 섹션에서 아래 권장값으로 설정하세요. **자동 증가**는 퍼센트 대신 고정 크기(MB/GB)로 설정하되, 지나치게 작은 단위로 잦은 증가가 일어나지 않도록 주의하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

소규모 조직 (10 GB 이하)

- 데이터: **처음 크기** 1 ~ 5 GB, **자동 증가** 100 ~ 512 MB
- 로그: **처음 크기** 512 MB ~ 2 GB, **자동 증가** 100 ~ 512 MB
- TempDB: **처음 크기** 512 MB ~ 1 GB

> *예: 데이터 2 GB (**자동 증가** 256 MB) / 로그 1 GB (**자동 증가** 128 MB) / TempDB 512 MB*

중규모 조직 (10 ~ 500 GB)

- 데이터: **처음 크기** 10 ~ 50 GB, **자동 증가** 512 MB ~ 1 GB
- 로그: **처음 크기** 5 ~ 10 GB, **자동 증가** 512 MB ~ 1 GB
- TempDB: **처음 크기** 2 ~ 8 GB

> *예: 데이터 20 GB (**자동 증가** 1 GB) / 로그 5 GB (**자동 증가** 512 MB) / TempDB 4 GB*

대규모 조직 (500 GB 이상)

- 데이터: **처음 크기** 100 GB 이상, **자동 증가** 1 ~ 4 GB
- 로그: **처음 크기** 20 ~ 100 GB, **자동 증가** 1 ~ 4 GB
- TempDB: **처음 크기** 8 ~ 32 GB

> *예: 데이터 100 GB (**자동 증가** 2 GB) / 로그 50 GB (**자동 증가** 2 GB) / TempDB 16 GB*

> **주의**
>
> - **자동 증가**를 매우 작은 단위로 설정하거나 **최대 크기**를 **무제한**으로 설정하지 말고, 예상 증가량에 따라 적절히 설정하거나 모니터링하세요.
> - 트랜잭션이 많은 환경에서는 로그를 주기적으로 백업하여 로그 파일의 크기가 증가하지 않도록 주의하세요.

Windows Authentication 데이터베이스 설정

1 사전 설정

Microsoft Windows Active Directory를 사용한다면 Windows Authentication 데이터베이스를 설정하기 전에 아래와 같이 사전 설정을 완료하세요.

1. **SQL Server Management Studio**에 관리자 계정으로 로그인하세요.
2. **보안**에서 마우스 오른쪽 버튼을 클릭한 뒤 **새 로그인**을 클릭하세요.
3. **Windows 인증**을 선택한 뒤 **검색**을 클릭하세요.
4. **사용자 또는 그룹 선택** 창에서 위치를 클릭한 뒤 Active Directory 경로를 선택하고 **확인**을 클릭하세요.
5. **선택할 개체 이름 입력** 필드에 사용자 이름을 입력한 뒤 **이름 확인** > **확인**을 클릭하세요.
6. **페이지 선택** 항목에서 **서버 역할**을 클릭하세요.
7. **sysadmin**을 선택한 뒤 **확인**을 클릭하세요.
8. **페이지 선택** 항목에서 **사용자 매핑**을 클릭하세요.
9. **ac, master, ta, ve**를 선택한 뒤 **기본 스키마**를 **dbo**로 설정하세요.
10. **확인**을 클릭하여 저장하세요.

2 Active Directory 계정으로 MS SQL Windows Authentication을 사용하기 위한 설정

1. *services.msc*를 실행하세요.
2. SQL Server 데이터베이스의 **속성** > **로그온** 창에서 **계정 지정**을 선택한 뒤 도메인 사용자로 로그인하세요.
3. Windows 방화벽에 1433 포트를 예외로 추가하세요.
4. SQL Server에 비어 있는 **ac, ta, ve** 데이터베이스를 **sysadmin** 인증으로 생성하세요.
5. SQL Server에 도메인 사용자가 Windows Authentication을 사용하도록 설정하고 **ac, ta, ve** 데이터베이스에 **sysadmin**을 제외한 나머지 모든 권한을 할당하세요.
6. 로컬 컴퓨터를 제외한 모든 서비스를 *services.msc*에서 연결하세요.
7. 도메인 사용자를 로컬 서비스 컴퓨터에서 관리자로 설정하세요.
8. MS SQL ODBC를 연결하세요.

3 데이터베이스 설정

1. **SQL Server 구성 관리자**를 실행한 뒤 **SQL Native Client** 하위의 **클라이언트 프로토콜**을 클릭하세요.
2. **TCP/IP**를 선택한 뒤 기본 포트를 확인하세요.
3. **SQL Server 네트워크 구성** 하위의 **SQL EXPRESS에 대한 프로토콜**을 클릭하세요.
4. **TCP/IP**에서 ODBC 포트가 기본 포트와 동일하게 설정되었는지 확인하세요.
5. **SQL Server Management Studio**에 관리자 계정으로 접속하세요.
6. **보안 > 로그인**을 클릭한 뒤 **NT AUTHORITY\SYSTEM**을 더블 클릭하세요.
7. **페이지 선택** 항목에서 **서버 역할**을 클릭하세요.
8. **public, sysadmin**을 선택해 체크한 뒤 **확인**을 클릭하세요.
9. **페이지 선택** 항목에서 **사용자 매핑**을 클릭하세요.
10. **ac, ta, ve** 데이터베이스를 선택한 뒤 **확인**을 클릭하여 저장하세요.

다음 단계

BioStar X를 설치하기 위한 시스템의 최소 사양을 알아보세요.
처음 설치하는 사용자를 위한 간편 설치 방법을 안내합니다.
사용자가 이미 설치한 데이터베이스와 연동하기 위한 사용자 정의 설치 방식을 안내합니다.

지원 장치

BioStar X 플랫폼에서 지원하는 장치 목록입니다.



BioStation 3 Max



XPass Q2



BioEntry W3



BioStation 2a



BioStation 3



X-Station 2



FaceStation F2



XPass 2



FaceLite



BioLite N2



XPass D2



BioEntry R2



BioEntry P2



FaceStation 2



BioEntry W2



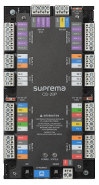
BioStation L2



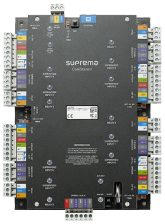
BioStation A2



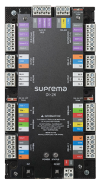
BioStation 2



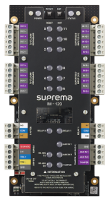
CoreStation 20



CoreStation



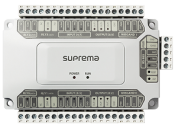
Door Interface



Input Module



Output Module



Door Module



Secure I/O 2

시스템 최소 요구사항

BioStar X는 대규모 엔터프라이즈 환경에서 안정적이고 확장 가능한 통합 보안 관리 솔루션을 제공합니다. 시스템은 메인 서버와 멀티 커뮤니케이션 서버로 구성되는 분산 아키텍처를 통해 최대 천대 이상의 장치를 효율적으로 관리할 수 있습니다.

메인 서버는 시스템의 핵심 관리 기능을, 멀티 커뮤니케이션 서버는 장치 통신을 전담하여 부하를 분산시키고 성능을 최적화합니다. 또한 관리자는 클라이언트 PC에서 웹 브라우저를 통해 시스템에 접속하여 모든 관리 업무를 수행할 수 있습니다. 아래의 시스템 요구사항을 확인하여 조직 규모에 맞는 최적의 환경을 구성하세요.

> **알아두기**
> 라이선스 구성 및 최적화에 대한 자세한 내용은 슈프리마 기술 지원팀(CS@suprema.co.kr)으로 문의하세요.

메인 서버

메인 서버는 **BioStar X**의 중앙 관리 시스템이 설치되는 서버입니다. 사용자가 웹 브라우저로 접속하여 시스템을 관리하고, 사용자 정보나 출입 권한 설정 등의 모든 업무를 처리합니다. 또한 시스템 전체의 상태를 모니터링하고, 이벤트 로그나 알람을 관리하는 역할을 담당합니다.

항목		소규모 조직	중규모 조직	대규모 조직
사용 환경	장치 수	1 - 50 대	51 - 100 대	101 - 1,000 대
시스템 환경	운영체제	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025		

항목	소규모 조직	중규모 조직	대규모 조직
데이터베이스	MariaDB 11.4.4, MS SQL Server 2012 SP3, MS SQL Server 2014 SP2, MS SQL Server 2016 SP1, MS SQL Server 2017, MS SQL Server 2019, MS SQL Server 2022		
CPU	2.3GHz 6코어	2.3GHz 8코어	최소 2.3GHz 권장 4.0GHz 16코어
RAM	16GB	32GB	최소 64GB 권장 128GB
SSD	512GB	512GB	1TB
HDD	**이미지 로그** 기능을 사용 시, 1,000만 개의 이미지 로그 기준 200GB 필요		

알아두기

- **BioStar X**는 64비트 운영체제에서만 설치할 수 있습니다.
- MS SQL Server 보안 통신은 TLS 1.2를 지원합니다.
- MS SQL Server와 **BioStar X**가 서로 다른 PC에 설치되어 있으면 **BioStar X**가 설치된 PC에 Microsoft OLE DB Driver for SQL Server를 설치해야 합니다.
- 대규모 조직에서는 MS SQL Server 데이터베이스를 설치하는 것을 권장합니다.
- 데이터베이스를 MS SQL Server를 사용하고, **BioStar X T&A**를 사용한다면 Microsoft ODBC Driver 17 for SQL Server가 필요하므로 사용자의 환경에 적합한 드라이버를 설치하세요.
- Mac 운영체제에서 제공하는 부트 캠프의 Windows 가상 환경은 지원하지 않습니다.
- 이더넷(TCP/IP)으로 연결할 수 있는 장치는 최대 1,000대입니다. 더 많은 장치를 연결하려면 멀티 커뮤니케이션 서버를 추가하세요.

SQL Server 라이선스 요구사항

데이터베이스로 SQL Server를 사용하는 경우, **BioStar X**의 안정적인 운영을 위해서는 연결된 장치 수에 따라 적절한 SQL Server 라이선스가 필요합니다. 각 환경별 권장 라이선스 구성을 참고하여 조직의 규모와 필요에 맞는 라이선스를 선택하세요.

알아두기

SQL Server 라이선스에 대한 자세한 내용은 Microsoft SQL Server 라이선스를 참고하세요.

일반 사용

조직	장치 수	코어 수
소규모 조직	1 - 50 대	4 - 6
중규모 조직	50 - 300 대	8 - 12

조직	장치 수	코어 수
대규모 조직	300 - 1,000 대	16 - 24

BioStar X API 사용

조직	장치 수	코어 수
소규모 조직	1 - 50 대	4 - 6
중규모 조직	50 - 300 대	8 - 12
대규모 조직	300 - 1,000 대	16 - 24

멀티 커뮤니케이션 서버

멀티 커뮤니케이션 서버는 출입통제 장치들과의 통신을 전담하는 서버입니다. 메인 서버와 별도로 설치하여 많은 수의 장치를 안정적으로 관리할 수 있도록 도와줍니다. 한 대의 멀티 커뮤니케이션 서버로 최대 1,000대의 장치를 연결할 수 있으며, 필요에 따라 여러 대의 멀티 커뮤니케이션 서버를 추가할 수 있습니다.

항목		사양
시스템 환경	운영체제	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025
	CPU	최소 2.3GHz, 권장 4.0GHz 16코어
	RAM	최소 64GB, 권장 128GB
	SSD	1TB

알아두기
이더넷(TCP/IP)으로 연결할 수 있는 장치는 최대 1,000대입니다.

클라이언트

클라이언트는 관리자가 웹 브라우저를 통해 **BioStar X**에 접속하여 시스템을 운영하는 PC입니다.

항목		소규모 조직	중규모 조직	대규모 조직
시스템 환경	CPU	2.5GHz	2.5GHz	최소 2.5GHz
	RAM	16GB	32GB	최소 32GB

항목		소규모 조직	중규모 조직	대규모 조직
	GPU	VMS 사용 시, 최소 NVIDIA GeForce RTX 4060		
	웹 브라우저	Google 크롬 100 버전 이상		

알아두기

- **BioStar X**는 Google 크롬에 최적화되어 있습니다.
- **BioStar X**의 웹 인터페이스는 모바일 브라우저에 대한 지원을 제공하지 않습니다.

시작하기

BioStar X를 처음 사용하는 사용자를 위한 필수 설정 가이드입니다. 설치 방법 선택부터 라이선스 등록까지 **BioStar X**를 성공적으로 구축하고 운영하는 데 필요한 핵심 절차를 단계별로 안내합니다.

네트워크 우선순위 확인하기

BioStar X를 설치하기 전에 서버의 네트워크 우선순위를 확인하고 설정하는 방법을 안내합니다.

언제 필요한가요?

아래와 같은 상황에서 네트워크 우선순위 확인 및 설정이 필요합니다.

- 서버에 2개 이상의 네트워크 어댑터(랜카드)가 설치되어 있을 때
- 특정 네트워크 어댑터를 **BioStar X** 서비스에서 사용해야 할 때
- **BioStar X** 설치 후 네트워크 연결 문제가 발생하는 것을 미리 방지할 때

> **알아두기**
> 위와 같은 상황에 해당하지 않는다면 네트워크 우선순위를 변경할 필요가 없습니다. 이 단계를 건너뛰고 **BioStar X** 설치를 진행하세요. **BioStar X** 설치에 대한 자세한 내용은 간편 설치하기를 참고하세요.

> **경고**
> **BioStar X** 설치 시 네트워크 메트릭 값이 낮은(우선순위가 높은) 네트워크 어댑터가 자동 선택됩니다. 설치 후에는 이 설정을 변경하기 어려우므로, **설치 전에 반드시 네트워크 우선순위를 확인하고 조정**해야 합니다.

네트워크 우선순위 확인하기

명령 프롬프트에서 확인

1. **시작** 메뉴에서 `cmd`를 검색하여 **명령 프롬프트**를 실행하세요.
2. 다음 명령어를 입력하세요.

```
route print
```

3. 출력 결과에서 **IPv4 Route Table** 섹션의 **Network Destination**이 `0.0.0.0`인 항목들을 찾아보세요.
4. **Metric** 열의 값을 확인하세요. **값이 낮을수록 우선순위가 높습니다.**

예시 출력:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.120.1  192.168.120.141     306
          0.0.0.0          0.0.0.0     192.168.40.1  192.168.40.123      20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     331
     192.168.40.0    255.255.252.0         On-link    192.168.40.123     266
   192.168.40.123  255.255.255.255         On-link    192.168.40.123     266
   192.168.43.255  255.255.255.255         On-link    192.168.40.123     266
    192.168.56.0    255.255.255.0         On-link     192.168.56.1     281
```

위 예시에서는 `192.168.40.123` 인터페이스가 메트릭 값 **20**으로 더 높은 우선순위를 가집니다.

네트워크 어댑터 정보 확인

각 인터페이스가 어떤 네트워크 어댑터에 해당하는지 확인하세요.

1. **명령 프롬프트** 창에서 아래 명령어를 입력하세요.

   ```
   ipconfig /all
   ```

2. 각 네트워크 어댑터의 **IPv4 주소**와 앞서 확인한 **Gateway** 주소를 매칭하여 어떤 어댑터인지 식별하세요.

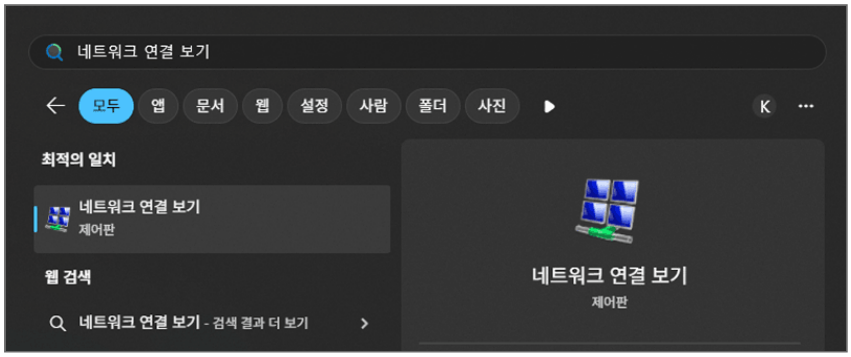
네트워크 우선순위 변경하기

원하는 네트워크 어댑터의 우선순위를 높이려면 다음 단계를 따르세요.

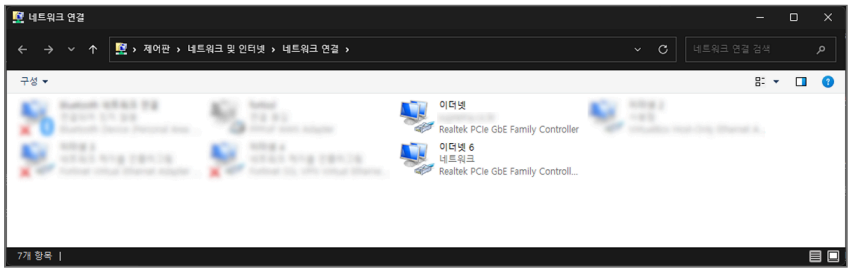
> **알아두기**
> 다음 단계는 Windows 11 기준입니다. 사용 중인 Windows 버전에 따라 메뉴 위치가 다를 수 있습니다.

1 네트워크 설정 열기

1. **시작** 메뉴에서 **네트워크 연결 보기**를 입력하세요.

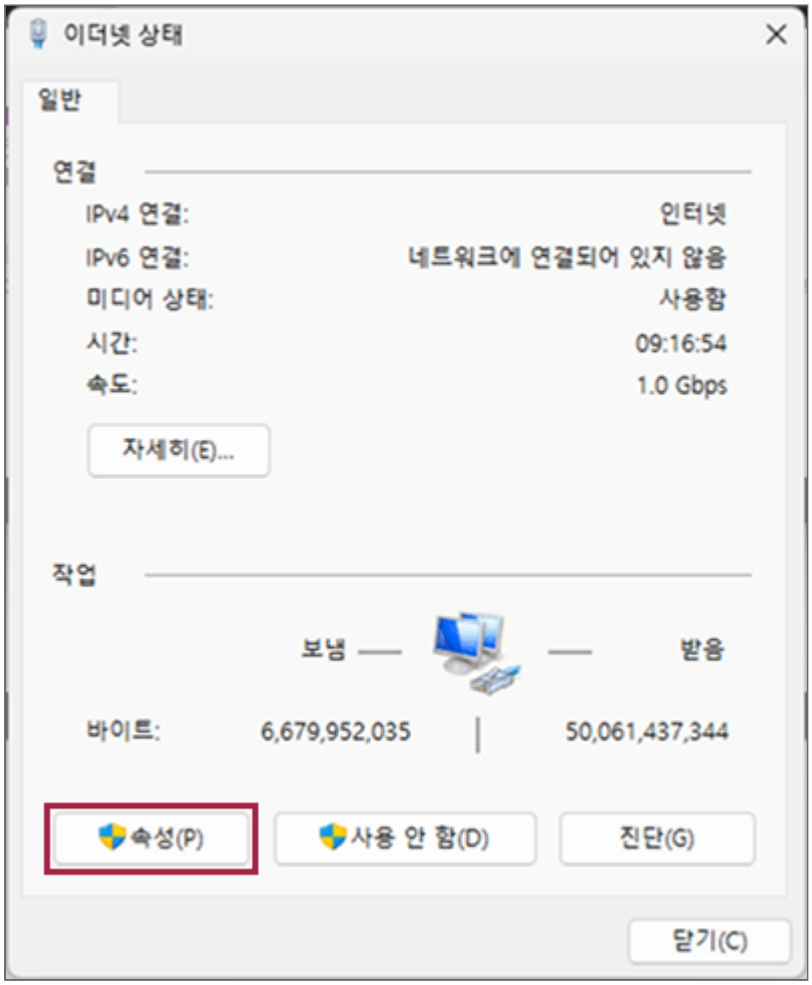


2. 검색 결과에서 **네트워크 연결 보기**를 클릭하세요.
3. 목록에서 인터넷에 연결된 어댑터를 더블 클릭하세요.

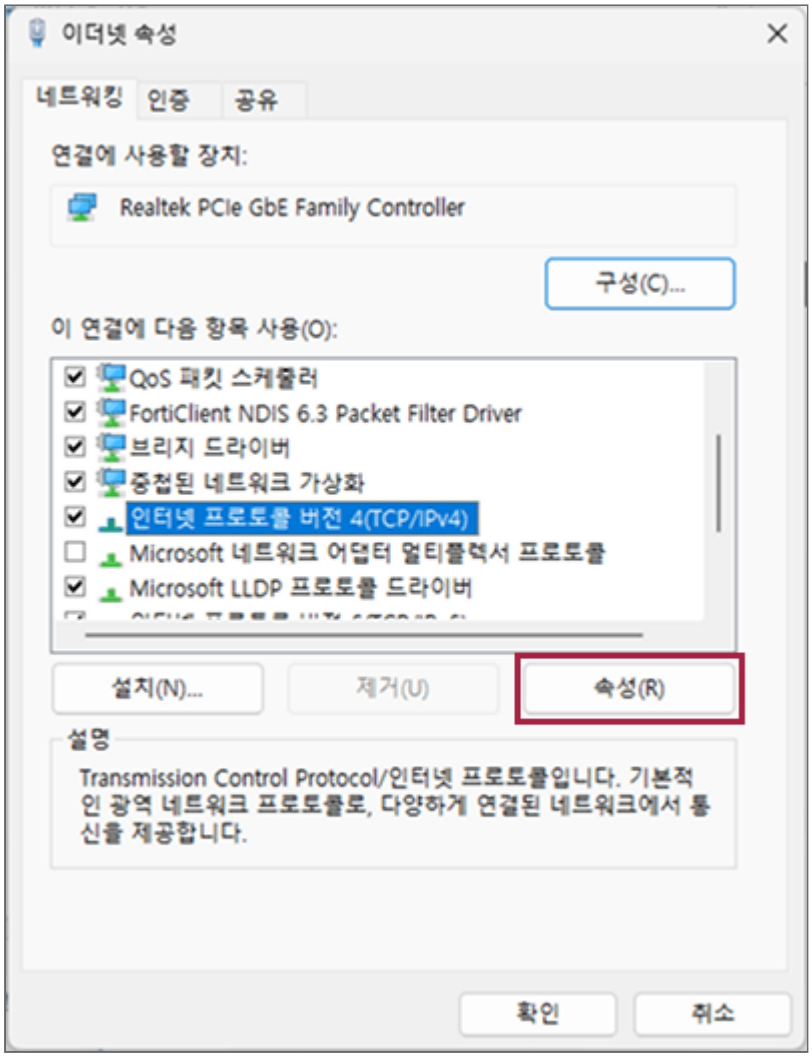


2 어댑터 옵션 열기

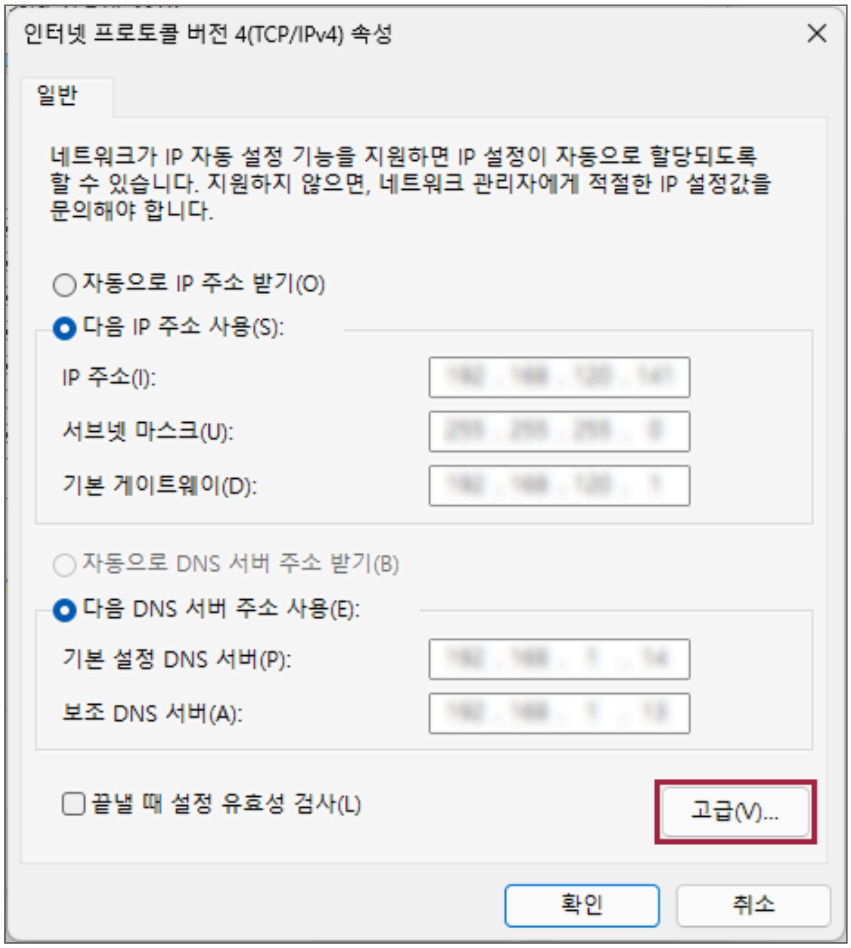
1. **이더넷 상태** 창이 나타나면 **속성** 버튼을 클릭하세요.



2. 이더넷 속성 창이 나타나면 목록에서 **인터넷 프로토콜 버전 4(TCP/IPv4)**를 선택하세요.

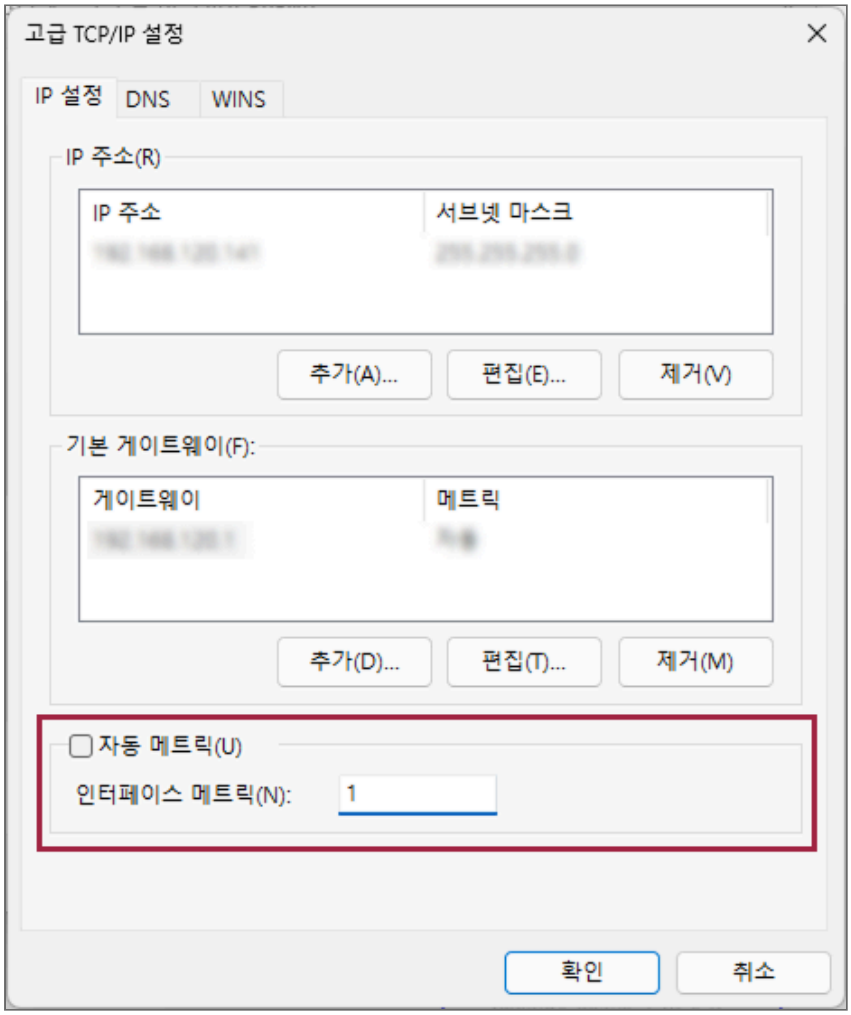


3. **속성** 버튼을 클릭하세요.
4. **인터넷 프로토콜 버전 4(TCP/IPv4) 속성** 창이 나타나면 **고급** 버튼을 클릭하세요.



3 메트릭 설정

1. **자동 메트릭** 체크박스를 **해제**하세요.



2. **인터페이스 메트릭** 필드에 원하는 값을 입력하세요.
   - 가장 높은 우선순위를 원한다면, `1` 을 입력하세요.
   - 다른 어댑터보다 높은 우선순위를 원한다면, 다른 어댑터의 메트릭 값보다 작은 수를 입력하세요.
3. 설정을 저장하고 모든 창을 닫으려면 **확인** 버튼을 클릭하세요.

> **알아두기**
> **인터페이스 메트릭**로 입력할 수 있는 값은 `1` 부터 `9999` 까지입니다. 값이 낮을수록 우선순위가 높습니다.

4 설정 확인

1. **명령 프롬프트**를 다시 열고 `route print` 명령어를 실행하세요.
2. 메트릭 값이 변경되었는지 확인하세요.

문제 해결

- 설정이 적용되지 않는다면 컴퓨터를 재시작하거나 네트워크 어댑터를 비활성화한 후 다시 활성화하세요.
- 네트워크 연결이 끊어진다면 원래 설정으로 되돌리고 **자동 메트릭** 옵션을 다시 활성화하세요. 네트워크 관리자에게 문의하여 올바른 설정값을 확인하세요.

> **알아두기**
> BioStar X 설치 후 네트워크 설정을 변경해야 한다면, 프로그램을 완전히 제거한 후 재설치하는 것을 권장합니다.

다음 단계

처음 설치하는 사용자를 위한 간편 설치 방법을 안내합니다.
사용자가 이미 설치한 데이터베이스와 연동하기 위한 사용자 정의 설치 방식을 안내합니다.

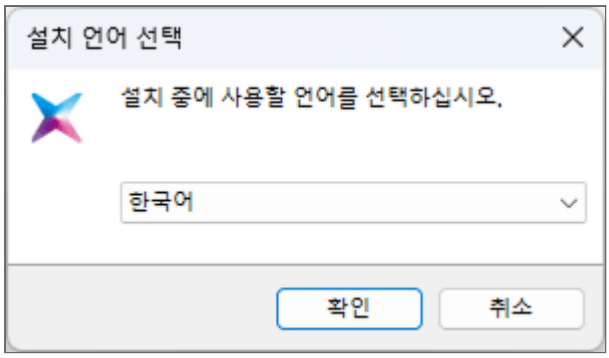
간편 설치하기

간편 설치 방식으로 BioStar X를 설치하는 절차를 단계별로 안내합니다. **간편 설치**는 내장된 MariaDB 서버를 자동으로 설치하고 데이터베이스를 생성하여 별도의 데이터베이스 설정 없이 빠르게 설치를 완료할 수 있습니다.

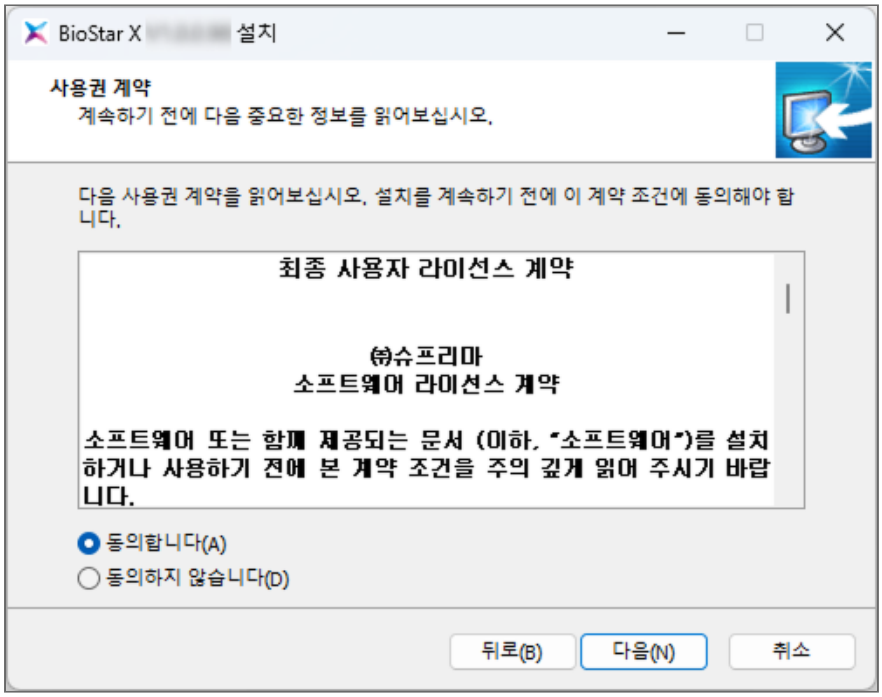
> **알아두기**
> 이미 설치한 데이터베이스와 연동하기 위해 **사용자 정의 설치**로 진행하려면 사용자 정의 설치하기를 참고하세요.

설치 안내

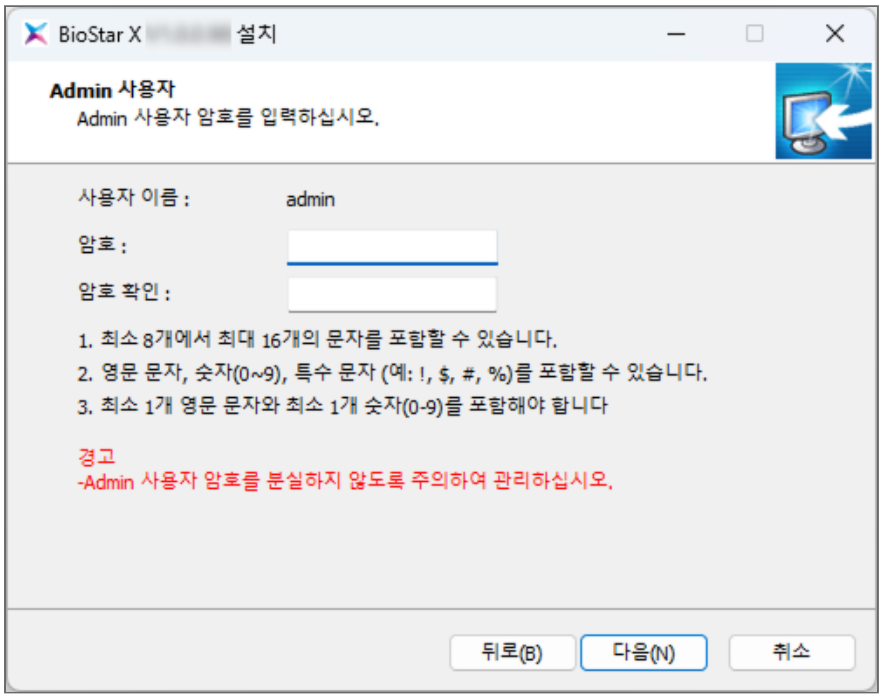
1. 슈프리마 다운로드 센터로 접속해 로그인한 후 설치 패키지(*BioStar X Setup.X.Y.Z.BB.exe*)를 다운로드하세요.
2. 다운로드한 설치 파일을 실행하세요.
3. 사용할 언어를 선택하고 **확인** 버튼을 선택하세요.



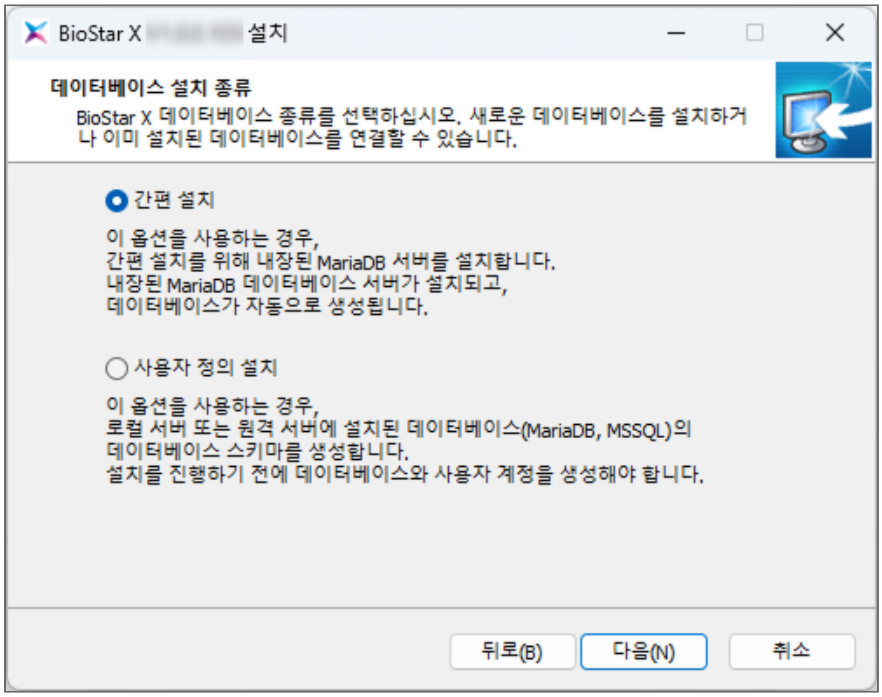
4. 설치를 계속하려면 **동의합니다**를 선택하고 **다음** 버튼을 클릭하세요.



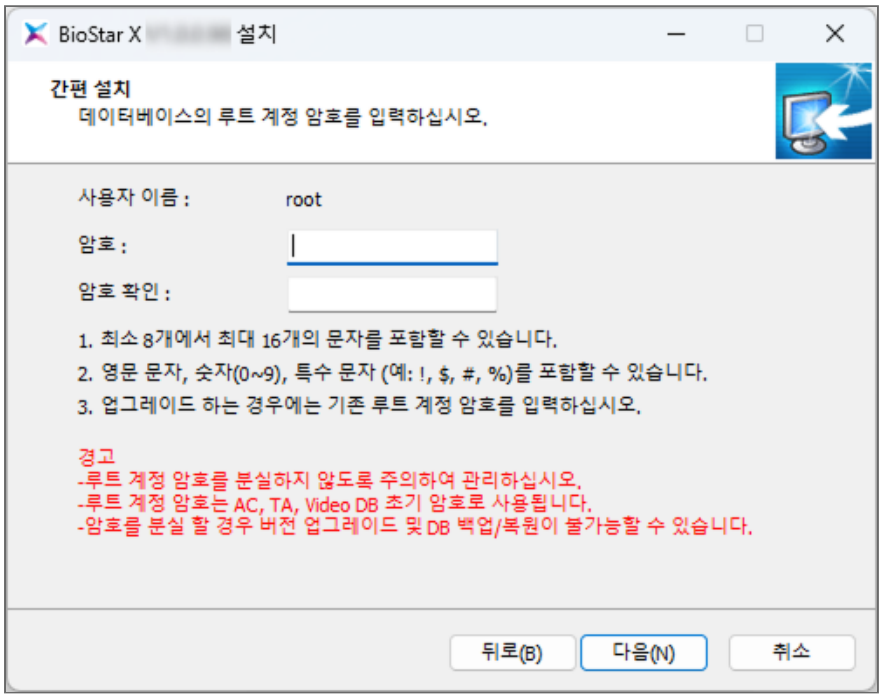
5. 관리자 계정 암호를 입력하고 **다음** 버튼을 클릭하세요.



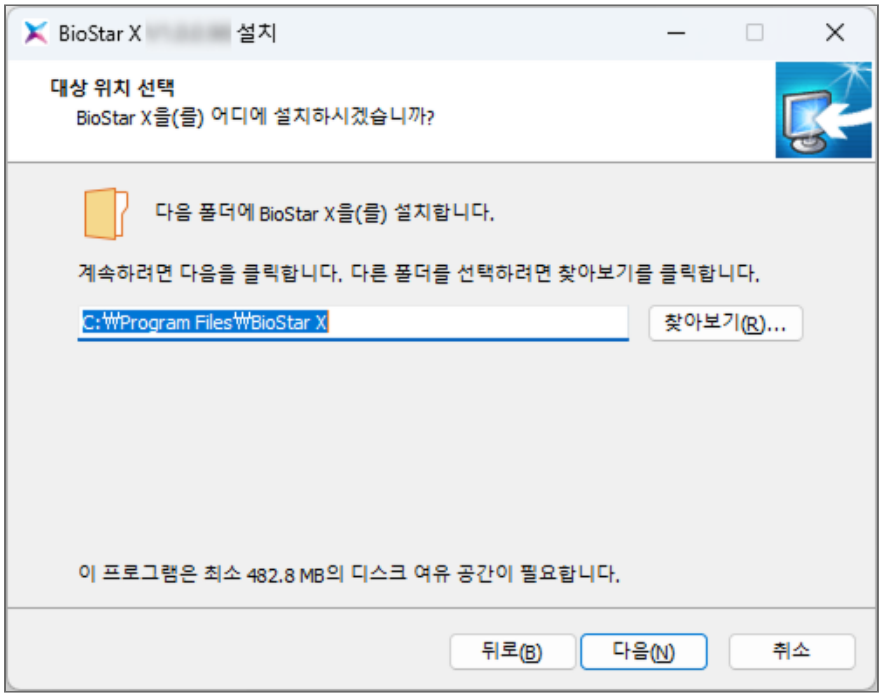
6. **간편 설치**를 선택하고 **다음** 버튼을 클릭하세요.



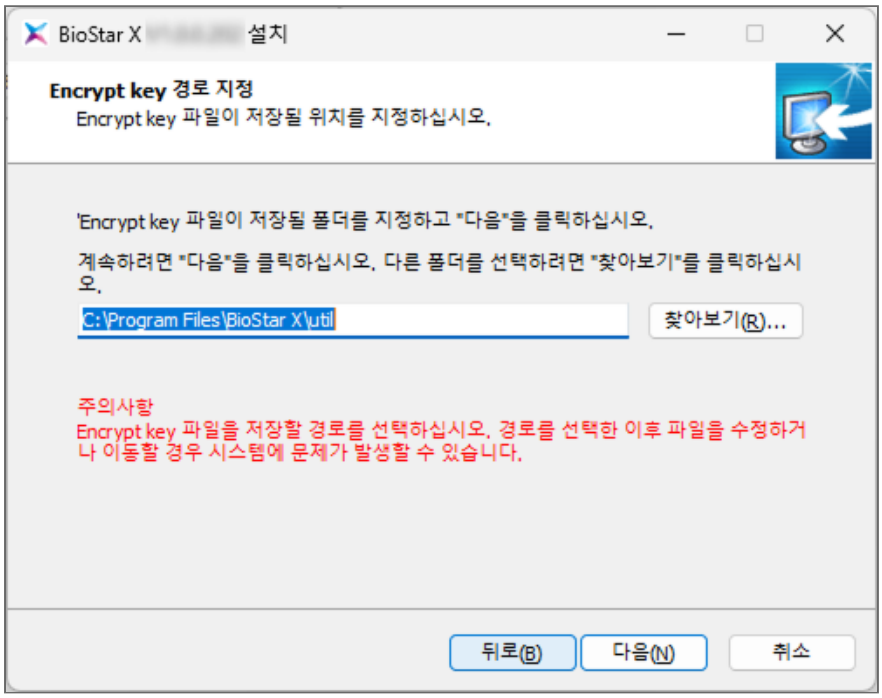
7. 데이터베이스의 루트(root) 계정 암호를 입력하고 **다음** 버튼을 클릭하세요.



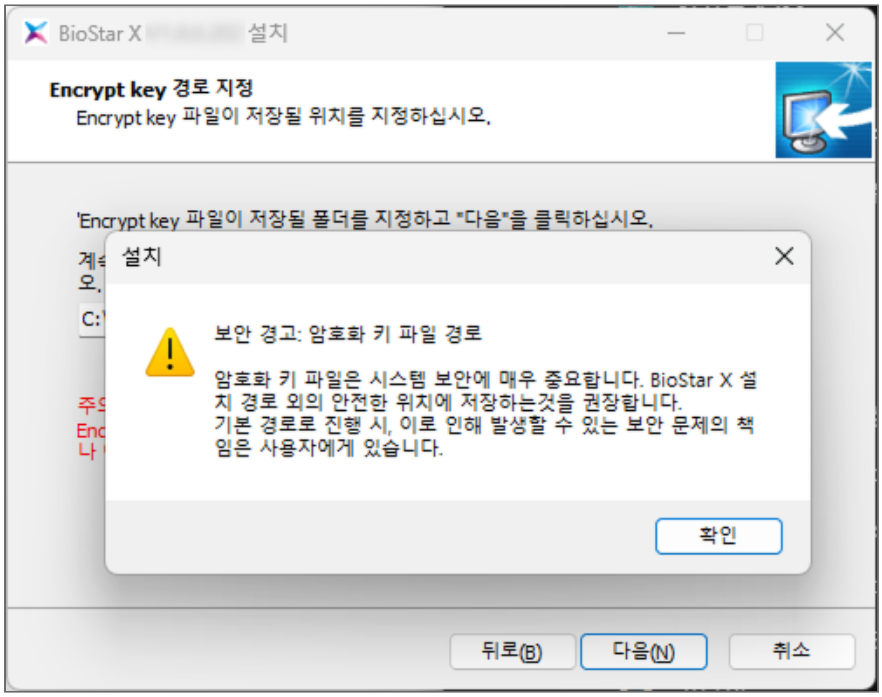
8. **BioStar X**를 설치할 경로를 설정하고 **다음** 버튼을 클릭하세요.



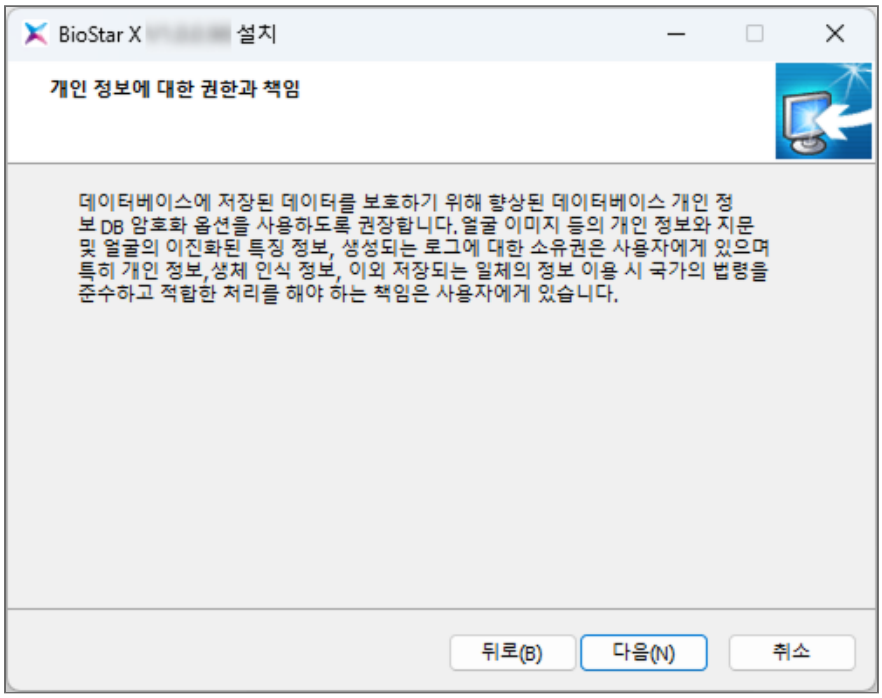
9. 암호화 키를 저장할 경로를 설정하고 **다음** 버튼을 클릭하세요.



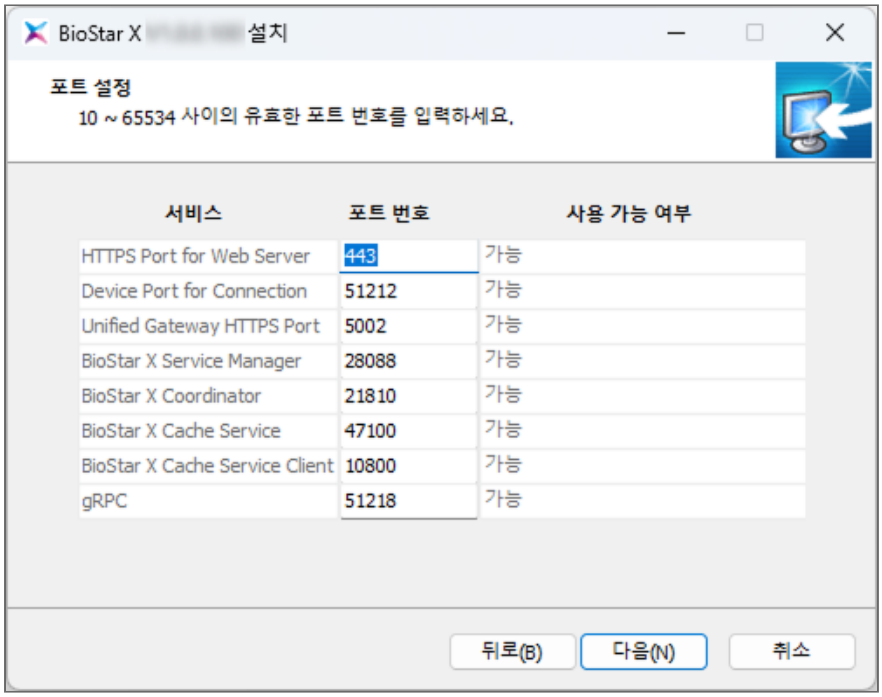
10. 보안 경고 메시지의 내용을 확인하고 **확인**을 클릭하세요.



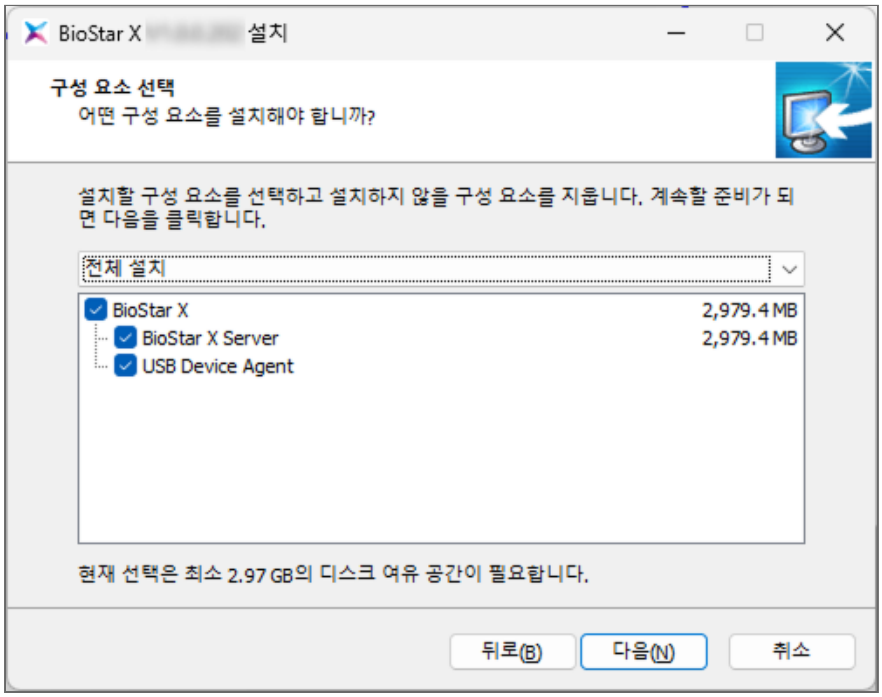
11. 데이터베이스에 저장되는 개인 정보 관리 권한 및 책임에 대한 안내를 읽고 설치를 계속하려면 **다음** 버튼을 클릭하세요.



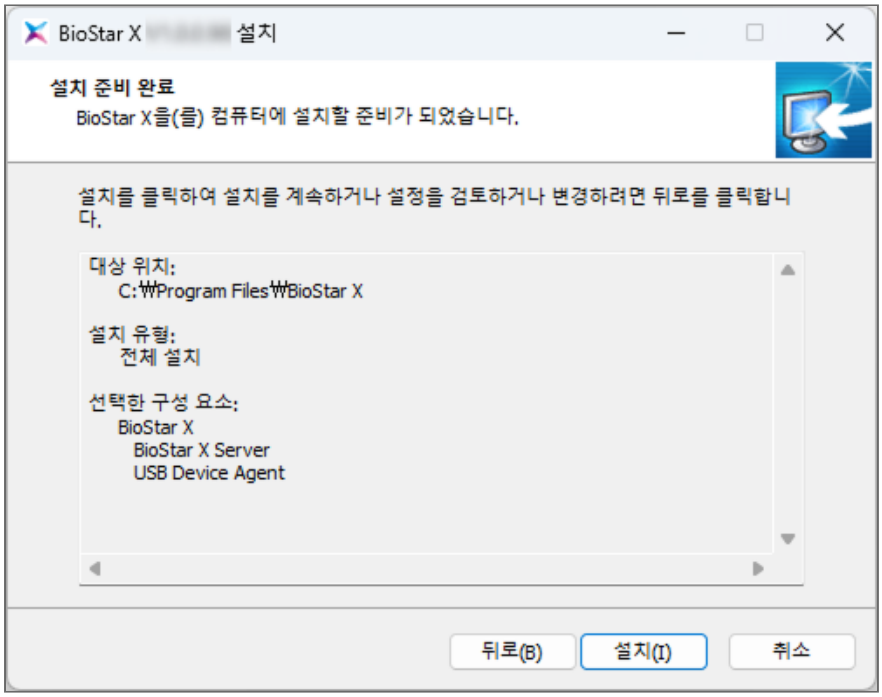
12. **BioStar X**의 통신을 위한 포트를 설정하고 **다음** 버튼을 클릭하세요.



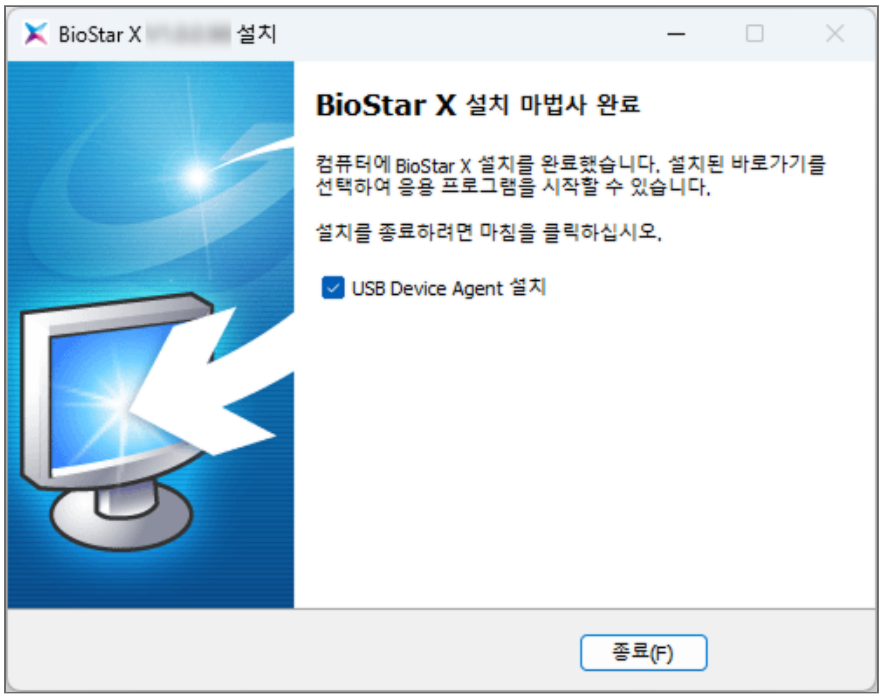
13. **BioStar X**의 구성 요소를 선택한 뒤 **다음** 버튼을 클릭하세요. **USB Device Agent**를 선택하면 BioMini, BioMini Plus 2, BioMini Slim 2, DUALi DE-620을 사용하기 위한 USB Agent와 드라이버를 함께 설치합니다.



14. 모든 설치 준비를 완료했다면 **설치** 버튼을 클릭하세요.



15. 부가 프로그램 설치 여부를 선택하고 **종료** 버튼을 클릭하세요.



16. 설치 화면의 안내에 따라 **USB Device Agent** 설치를 완료하세요.

알아두기

- 다운로드한 파일명에서 `X.Y.Z`는 버전 정보이며, `BB`는 빌드 번호입니다.
- 관리자 계정 암호는 **BioStar X**를 설치한 다음 처음 로그인할 때 사용합니다.
- 데이터베이스의 루트(root) 계정 암호는 AC, TA, Video DB 초기 암호로 사용합니다.
- 암호화 키의 저장 경로를 변경할 수 있습니다. 경로를 변경한 이후에 암호화 키 파일을 수정하거나 다른 경로로 이동시키면 시스템 오류가 발생할 수 있습니다.
- **BioStar X**를 삭제하면 암호화 키 파일도 함께 삭제합니다.
- 제공된 USB Device Agent 인증서는 로컬 네트워크에만 적용할 수 있습니다.
- 다른 프로그램에서 443 포트를 사용하고 있다면 BioStar X Setting 프로그램이 자동으로 실행되어 포트 번호를 변경할 수 있습니다. 포트 번호 변경에 대한 내용은 포트 변경하기를 참고하세요.
- 데이터베이스 설정 변경에 대한 자세한 내용은 데이터베이스 변경하기를 참고하세요.

경고

- 관리자 또는 데이터베이스의 루트(root) 계정 암호를 분실하지 않도록 주의하세요.
- 암호를 분실하면 버전 업그레이드 및 DB 백업/복원이 불가능할 수 있습니다.

다음 단계

웹 브라우저를 실행해 **BioStar X**로 로그인하는 방법을 확인하세요.
BioStar X의 서버 상태를 확인하고 종료 또는 다시 시작하는 방법을 확인하세요.

사용자 정의 설치하기

이 문서에서는 **사용자 정의 설치** 방식으로 **BioStar X**를 설치하는 절차를 단계별로 안내합니다. **사용자 정의 설치**는 로컬 서버 또는 원격 서버에 기존에 설치된 데이터베이스(MariaDB, MS SQL Server)와 연동하여 데이터베이스 스키마를 생성합니다. 설치를 시작하기 전에 연동할 데이터베이스와 사용자 계정을 미리 준비하세요.

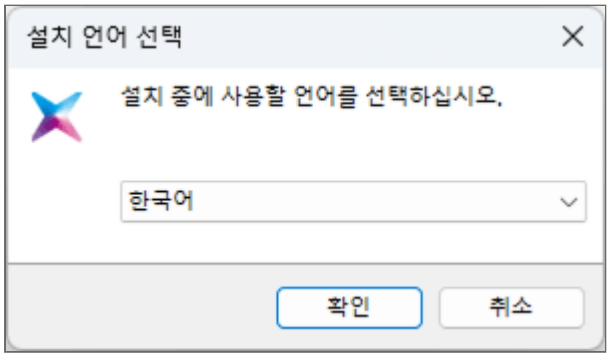
시작하기 전에

- **BioStar X**와 연동하여 사용할 수 있는 데이터베이스는 아래와 같습니다.
  - MariaDB 11.4.4
  - MS SQL Server 2012 SP3
  - MS SQL Server 2014 SP2
  - MS SQL Server 2016 SP1
  - MS SQL Server 2017

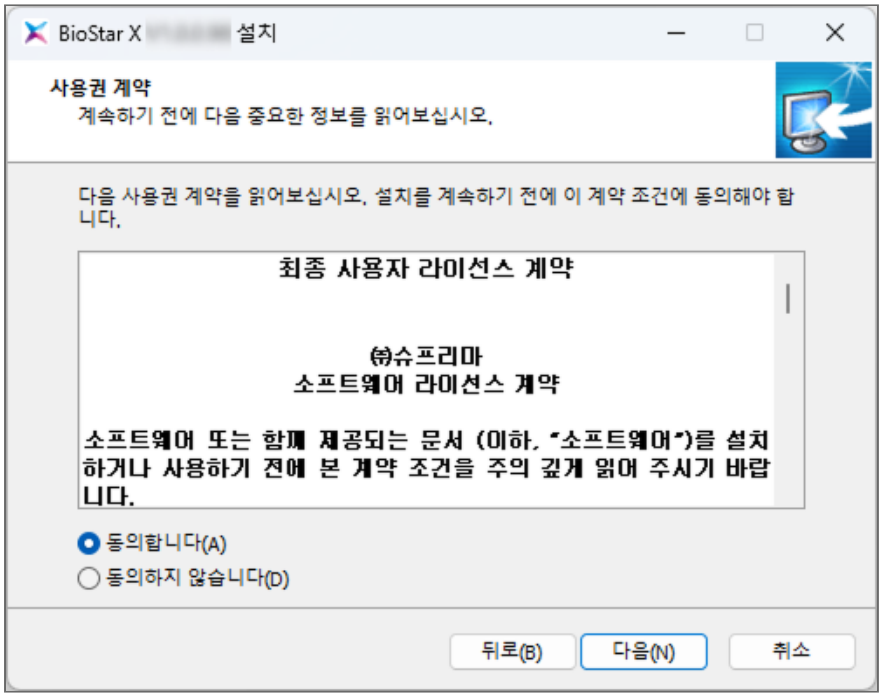
  - MS SQL Server 2019
  - MS SQL Server 2022
- MS SQL Server의 보안 통신은 TLS 1.2를 지원합니다.
- MS SQL Server를 데이터베이스로 설정하고, 데이터베이스 테이블 생성에 실패했다면 *C:\Program Files\BioStar X\dbscript\mssql* 경로의 스크립트를 실행하여 테이블을 생성할 수 있습니다.
- 설치 옵션으로 **사용자 정의 설치**를 선택할 때 **AC DB name, TA DB name, VE DB name**은 동일하게 설정할 수 없습니다.
- Windows 인증을 사용하려면 Microsoft ODBC Driver 17 for SQL Server가 필요합니다. 먼저 해당 드라이버를 설치하세요.

설치 안내

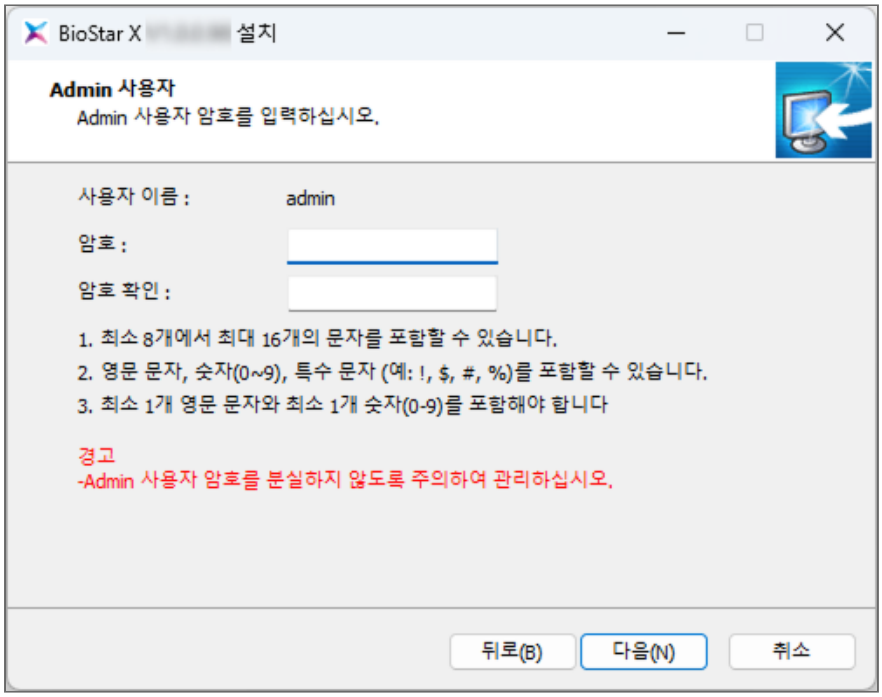
1. 슈프리마 다운로드 센터로 접속해 로그인한 후 설치 패키지(*BioStar X Setup.X.Y.Z.BB.exe*)를 다운로드하세요.
2. 다운로드한 설치 파일을 실행하세요.
3. 사용할 언어를 선택하고 **확인** 버튼을 선택하세요.



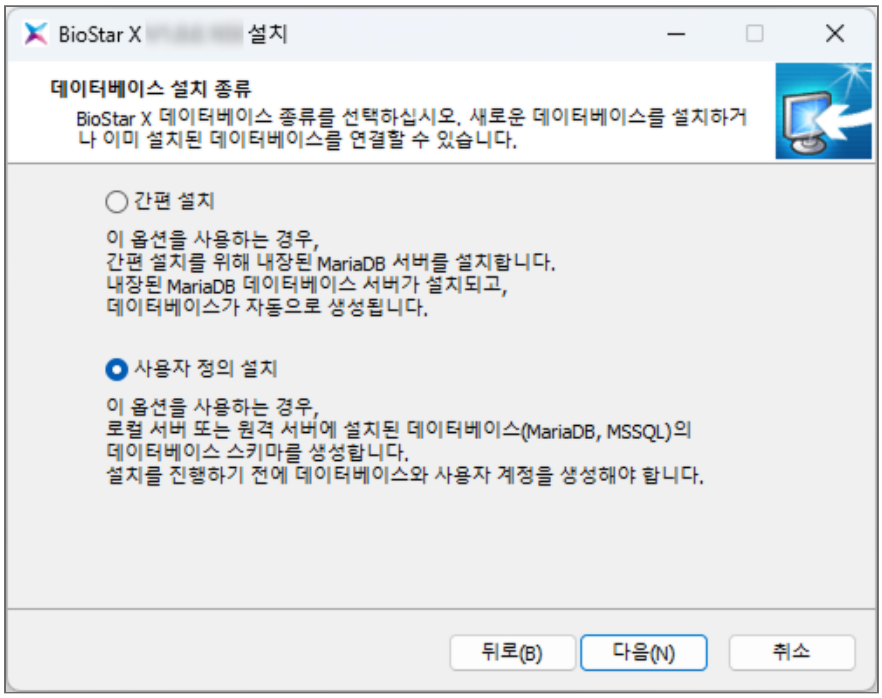
4. 설치를 계속하려면 **동의합니다**를 선택하고 **다음** 버튼을 클릭하세요.



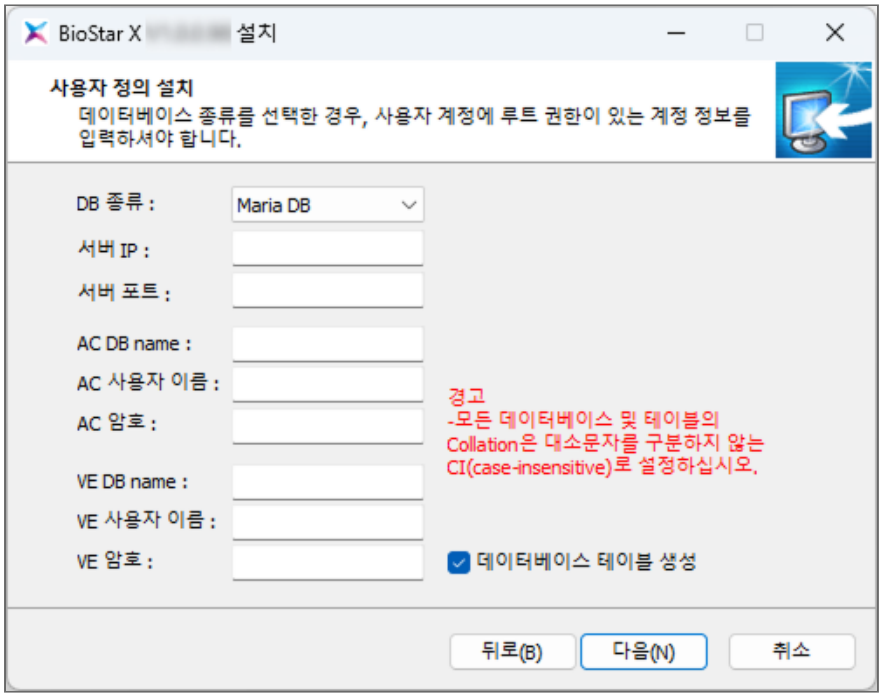
5. 관리자 계정 암호를 입력하고 **다음** 버튼을 클릭하세요.



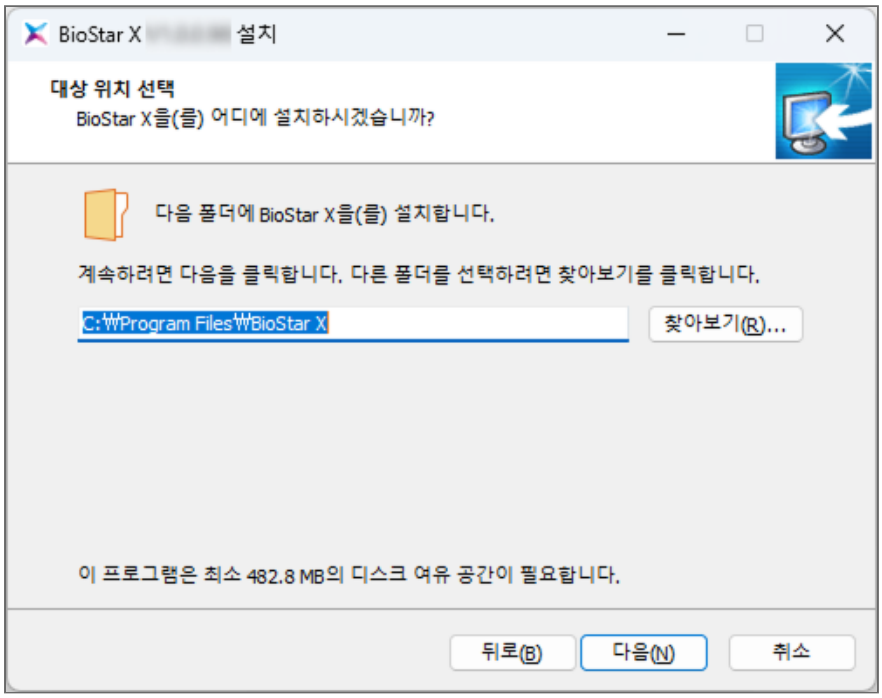
6. **사용자 정의 설치**를 선택하고 **다음** 버튼을 클릭하세요.



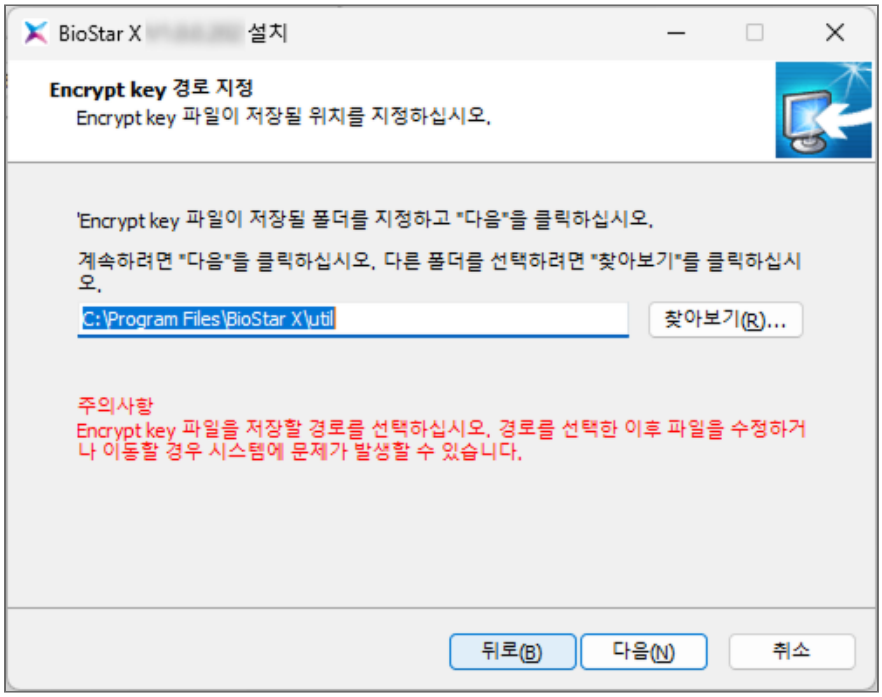
7. 이미 구성된 데이터베이스의 세부 정보를 입력하고 **다음** 버튼을 클릭하세요.



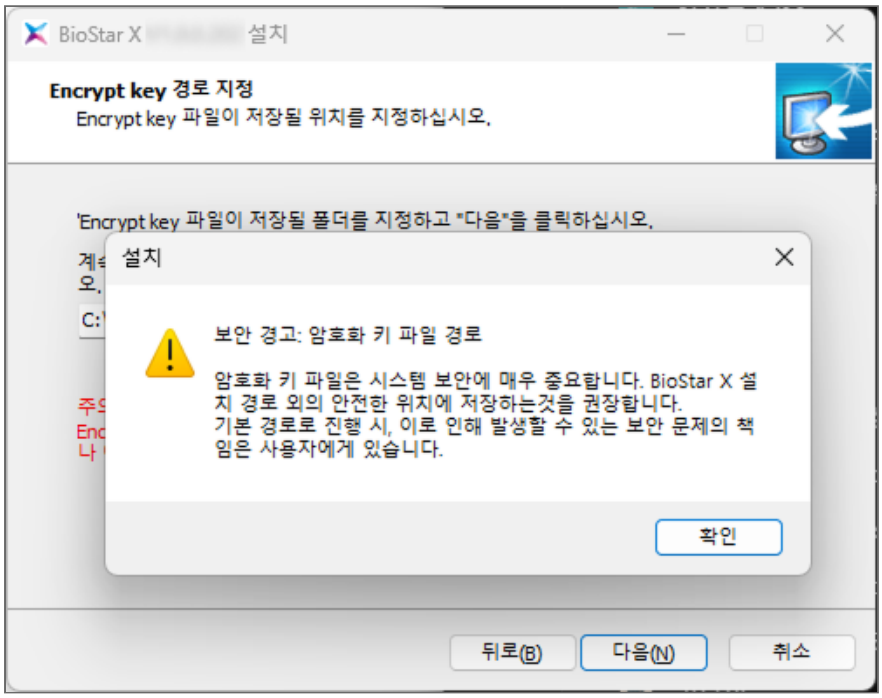
8. **BioStar X**를 설치할 경로를 설정하고 **다음** 버튼을 클릭하세요.



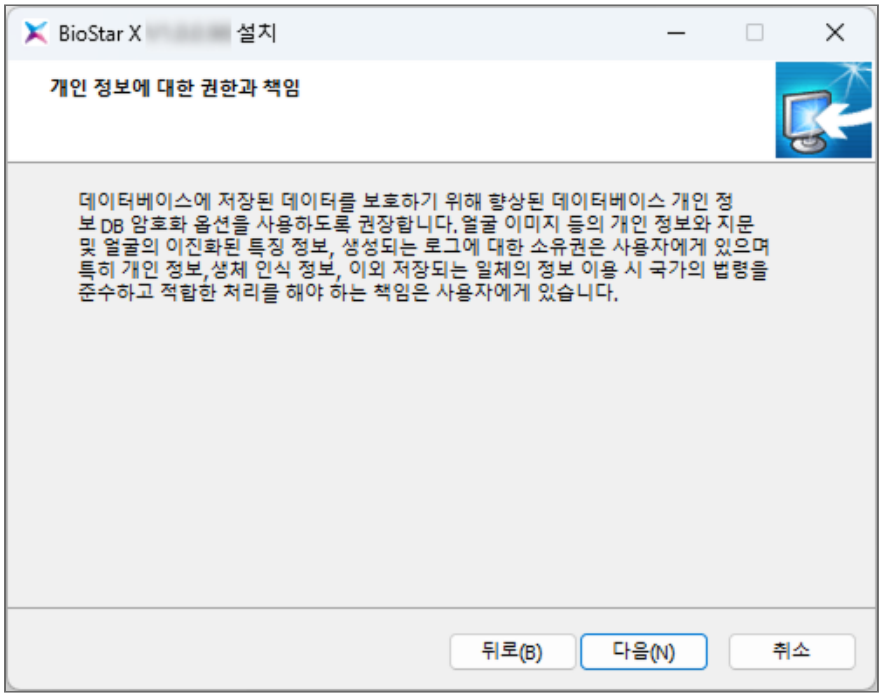
9. 암호화 키를 저장할 경로를 설정하고 **다음** 버튼을 클릭하세요.



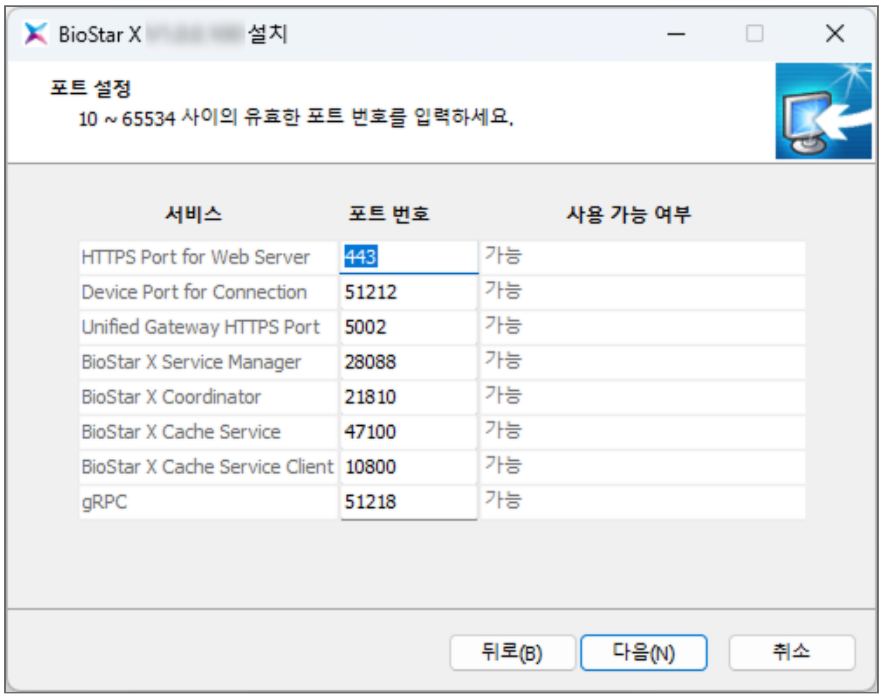
10. 보안 경고 메시지의 내용을 확인하고 **확인**을 클릭하세요.



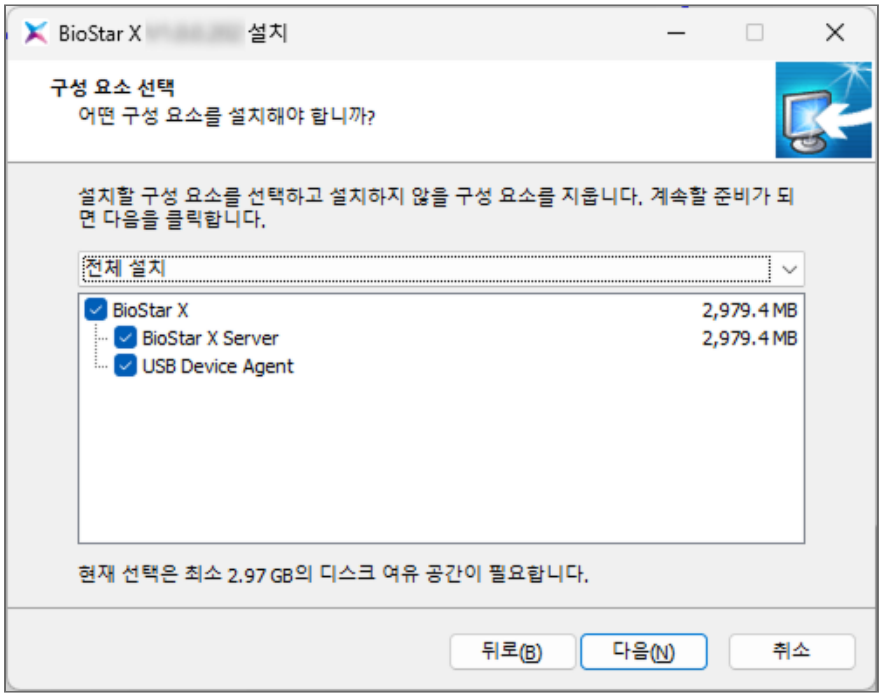
11. 데이터베이스에 저장되는 개인 정보 관리 권한 및 책임에 대한 안내를 읽고 설치를 계속하려면 **다음** 버튼을 클릭하세요.



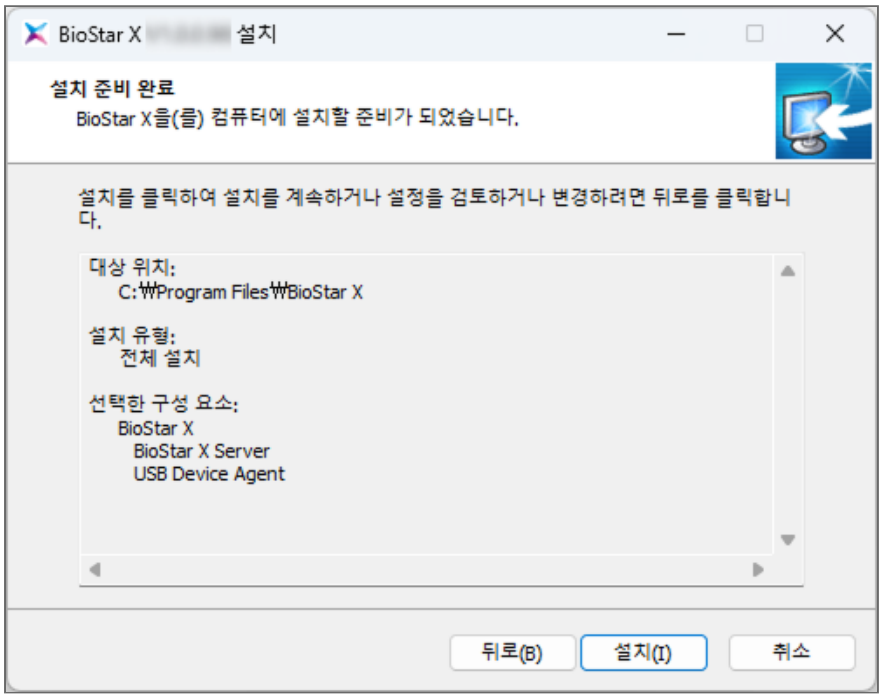
12. **BioStar X**의 통신을 위한 포트를 설정하고 **다음** 버튼을 클릭하세요.



13. **BioStar X**의 구성 요소를 선택한 뒤 **다음** 버튼을 클릭하세요. **USB Device Agent**를 선택하면 BioMini, BioMini Plus 2, BioMini Slim 2, DUALi DE-620을 사용하기 위한 USB Agent와 드라이버를 함께 설치합니다.



14. 모든 설치 준비를 완료했다면 **설치** 버튼을 클릭하세요.



15. 부가 프로그램 설치 여부를 선택하고 **종료** 버튼을 클릭하세요.



16. 설치 화면의 안내에 따라 **USB Device Agent** 설치를 완료하세요.

알아두기

- 다운로드한 파일명에서 X.Y.Z는 버전 정보이며, BB는 빌드 번호입니다.
- 관리자 계정 암호는 **BioStar X**를 설치한 다음 처음 로그인할 때 사용합니다.
- 데이터베이스의 루트(root) 계정 암호는 AC, TA, Video DB 초기 암호로 사용합니다.
- 암호화 키의 저장 경로를 변경할 수 있습니다. 경로를 변경한 이후에 암호화 키 파일을 수정하거나 다른 경로로 이동시키면 시스템 오류가 발생할 수 있습니다.
- **BioStar X**를 삭제하면 암호화 키 파일도 함께 삭제합니다.
- 제공된 USB Device Agent 인증서는 로컬 네트워크에만 적용할 수 있습니다.
- 다른 프로그램에서 443 포트를 사용하고 있다면 BioStar X Setting 프로그램이 자동으로 실행되어 포트 번호를 변경할 수 있습니다. 포트 번호 변경에 대한 내용은 포트 변경하기를 참고하세요.
- 데이터베이스 설정 변경에 대한 자세한 내용은 데이터베이스 변경하기를 참고하세요.

경고

- 관리자 또는 데이터베이스의 루트(root) 계정 암호를 분실하지 않도록 주의하세요.
- 암호를 분실하면 버전 업그레이드 및 DB 백업/복원이 불가능할 수 있습니다.

다음 단계

웹 브라우저를 실행해 **BioStar X**로 로그인하는 방법을 확인하세요.
BioStar X의 서버 상태를 확인하고 종료 또는 다시 시작하는 방법을 확인하세요.

업그레이드하기

이 문서는 BioStar 2를 **BioStar X**로 업그레이드하는 절차를 단계별로 안내합니다. 업그레이드를 시작하기 전에 시스템 요구 사항과 주의 사항을 먼저 확인하세요.

시작하기 전에

BioStar 2에서 **BioStar X**로 업그레이드하기 전에 다음 사항을 확인하세요.

알아두기

Important

최소 요구 사항

- 업그레이드를 진행하기 전에 시스템 최소 요구사항을 참고하여 서버 사양이 충족되는지 확인하세요.
- BioStar 2 v2.9.11 이상의 환경이라면 **BioStar X**로 업그레이드할 수 있습니다.
  - BioStar 2 v2.6.4 이하 버전을 사용하고 있다면 v2.9.11까지 순차 업그레이드를 진행한 후 업그레이드할 수 있습니다. BioStar 2를 단계별로 업그레이드하는 방법은 **BioStar 2 관리자 가이드**를 참고하세요.
  - BioStar 2 v2.9.10 이하 버전에서는 업그레이드할 수 없습니다.
- BioStar 2에 아래 장치가 연결되어 있다면 **BioStar X** 업그레이드를 지원하지 않습니다.
  - XPass S2, XPass, BioEntry W, BioEntry Plus, BioLite Net

라이선스

- **BioStar X**로 업그레이드하기 전에 대리점에 문의하여 최소 하나의 BioStar X 라이선스를 준비해야 합니다.
- **BioStar X**로 업그레이드할 때 BioStar 2와는 다른 라이선스 정책이 적용됩니다.
- BioStar 2 AC 라이선스 중 어드밴스(Advanced) 등급 이상의 라이선스가 활성화되어 있는 상태에서 업그레이드한다면 아래 서비스 기능 및 설정은 삭제됩니다.
  - 그래픽 맵(Graphic Map)
  - 클라우드(Cloud)
- BioStar 2 T&A 서비스를 **BioStar X**에서도 사용하려면 **BioStar X T&A** 라이선스를 별도 구매해야 합니다.

경고

인증서 확인

BioStar 2에서 BioStar X로 업그레이드했을 때, `nginx\conf` 경로와 `nginx\cert` 경로에 있는 `biostar_cert.crt` 파일이 서로 다를 수 있습니다. 이 상태로 업그레이드하면 다음과 같은 문제가 발생합니다.

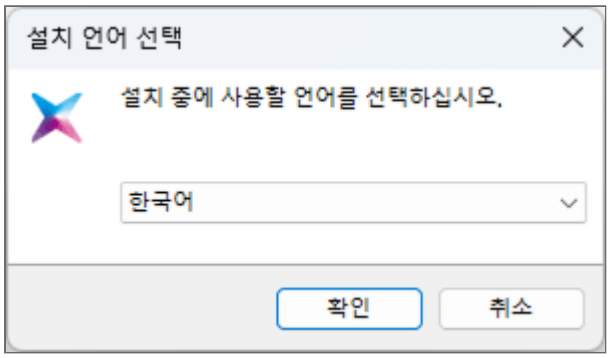
- 감사 로그가 일부 기록되지 않습니다.
- 사용자 그룹 생성, Wiegand 추가, 트리 갱신에 실패합니다.

BioStar X로 업그레이드하기 전에 인증서 파일을 일치시키려면 다음 단계를 따르세요.

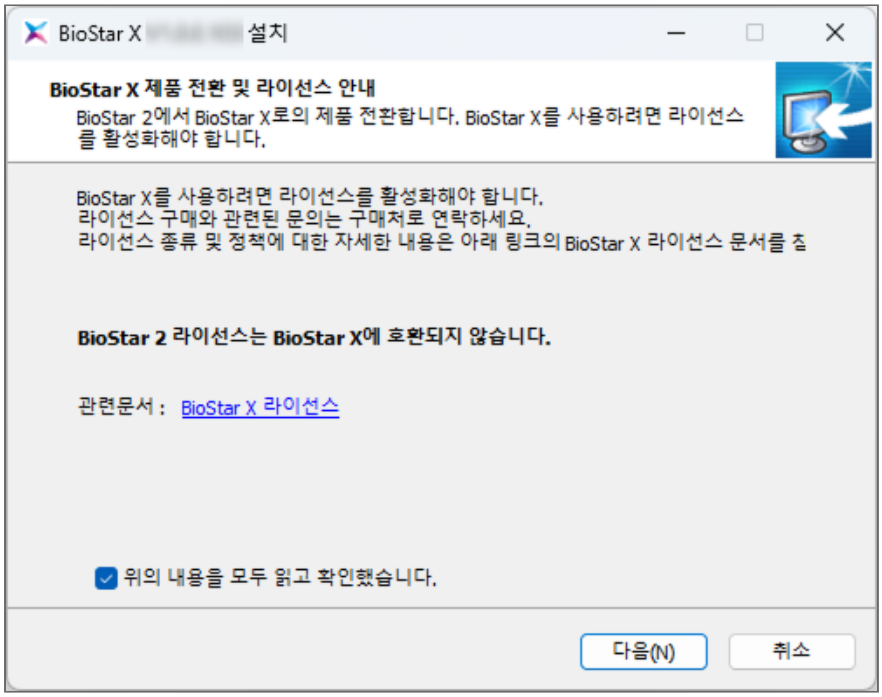
1. BioStar 2 서비스를 중지하세요.
2. `nginx\conf` 경로의 `biostar_cert.crt`, `biostar_cert.key` 파일을 `nginx\cert` 경로에 덮어쓰세요.
3. BioStar 2 서비스를 다시 시작하세요.

업그레이드 설치 안내

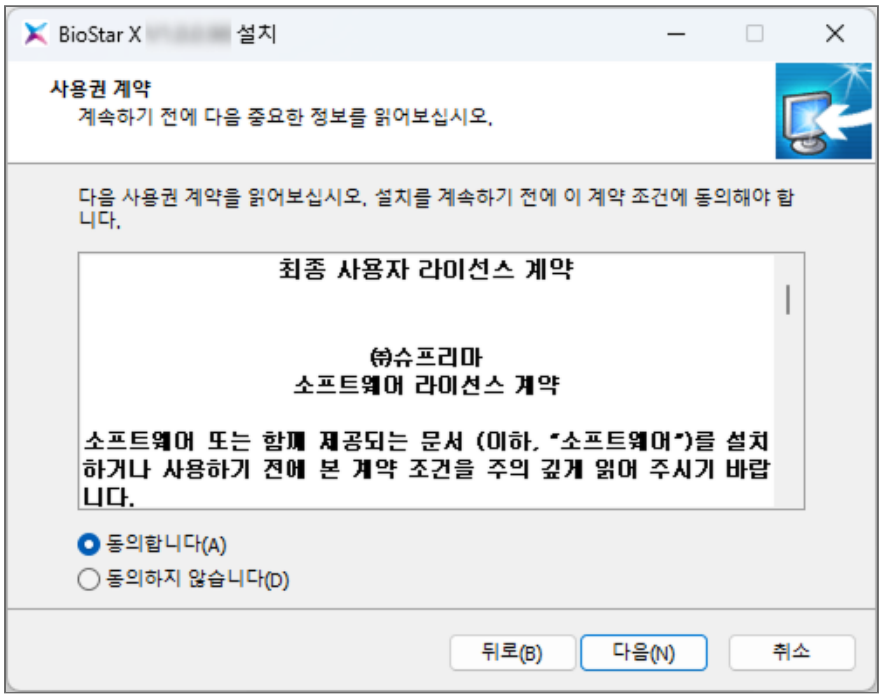
1. 슈프리마 다운로드 센터로 접속해 로그인한 후 설치 패키지(*BioStar X Setup.X.Y.Z.BB.exe*)를 다운로드하세요.
2. 다운로드한 설치 파일을 실행하세요.
3. 사용할 언어를 선택하고 **확인** 버튼을 선택하세요.



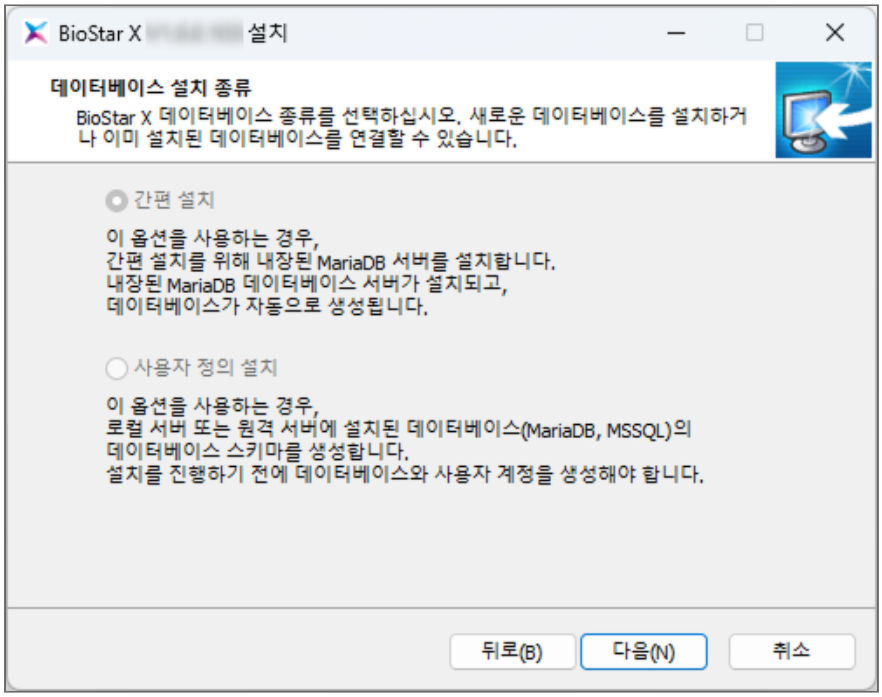
4. BioStar 2에서 **BioStar X**로 전환한다는 라이선스 정책에 동의하세요. 체크박스를 클릭하고 **다음** 버튼을 선택하세요.



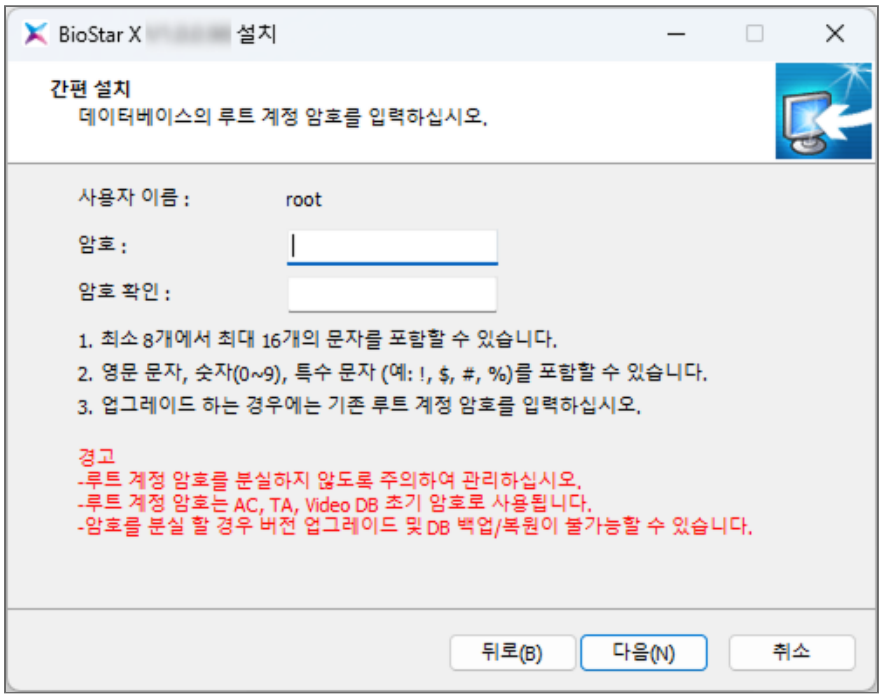
5. 설치를 계속하려면 **동의합니다**를 선택하고 **다음** 버튼을 클릭하세요.



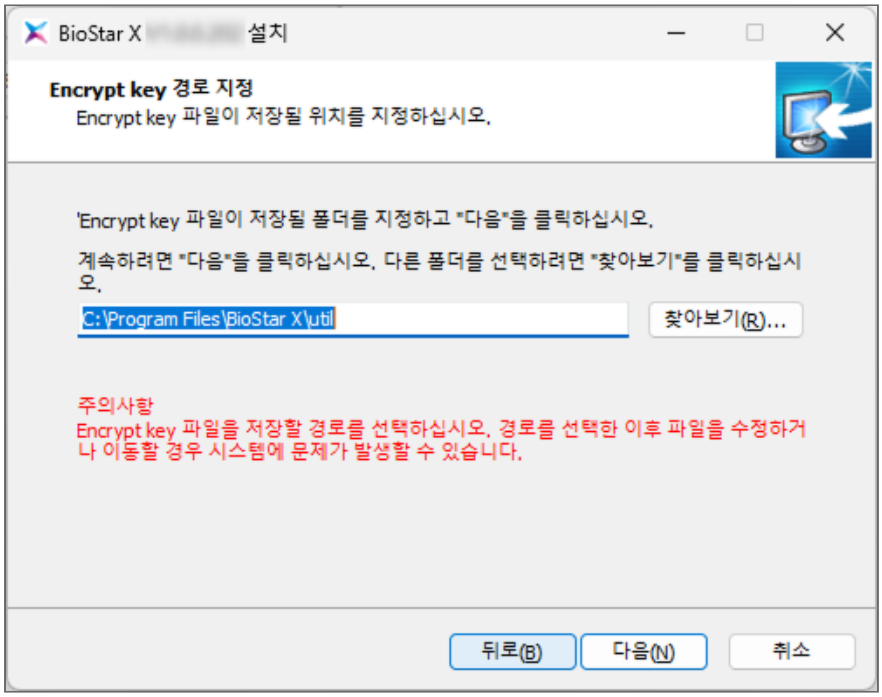
6. BioStar 2에서 업그레이드하는 경우, 기존에 사용하던 데이터베이스를 연결하여 설치를 진행합니다. **다음** 버튼을 클릭하세요.



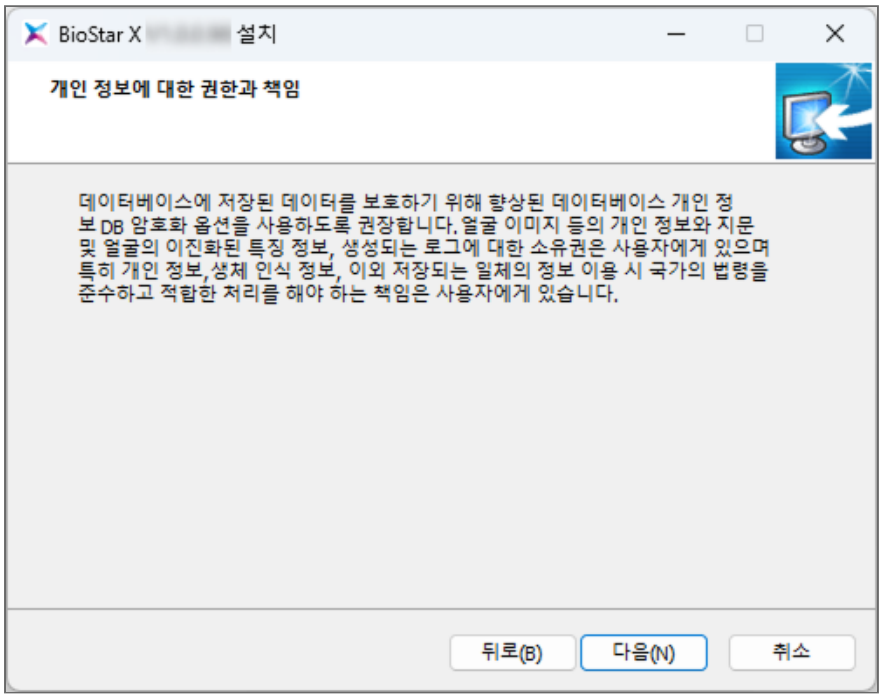
7. 기존에 사용하던 데이터베이스의 루트(root) 계정 암호를 입력하고 **다음** 버튼을 클릭하세요.



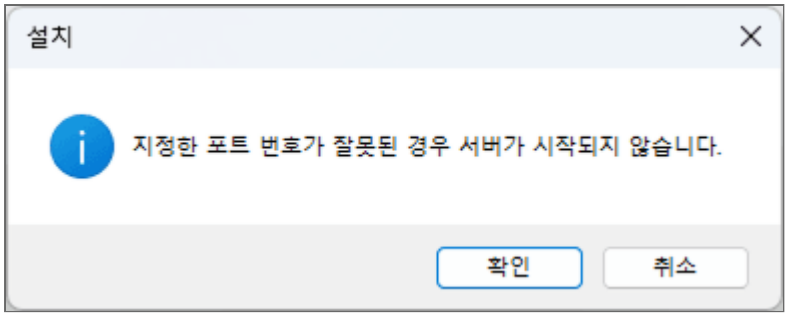
8. 암호화 키를 저장할 경로를 설정하고 **다음** 버튼을 클릭하세요.



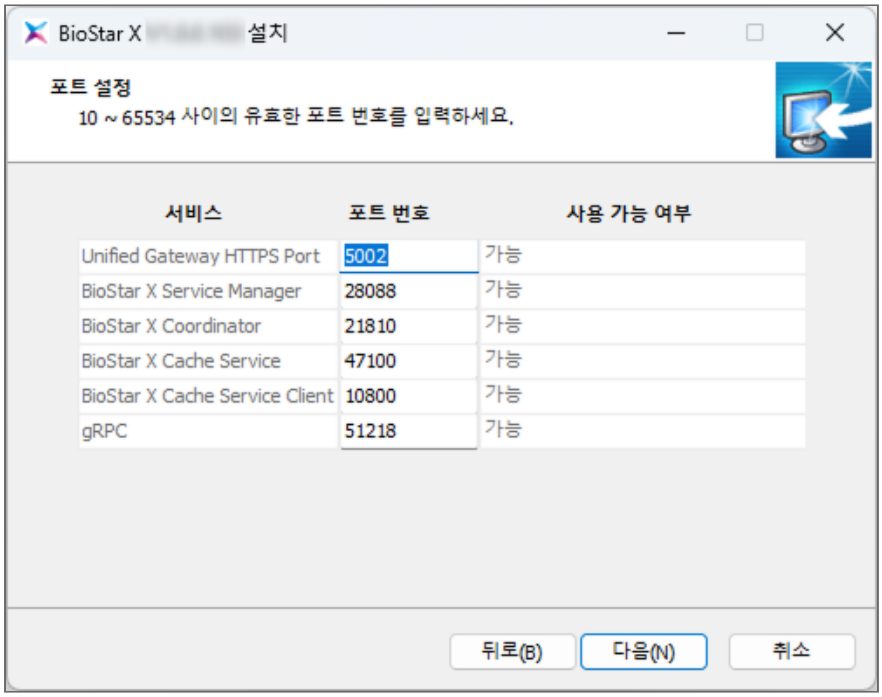
9. 데이터베이스에 저장되는 개인 정보 관리 권한 및 책임에 대한 안내를 읽고 설치를 계속하려면 **다음** 버튼을 클릭하세요.



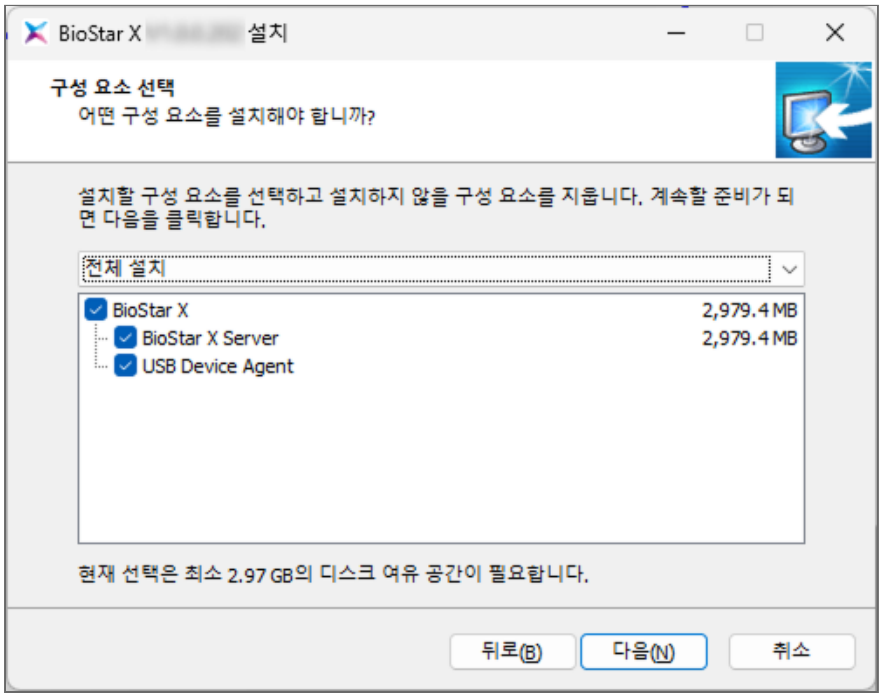
10. 포트 번호 관련 메시지가 표시되면 **확인**을 클릭하세요.



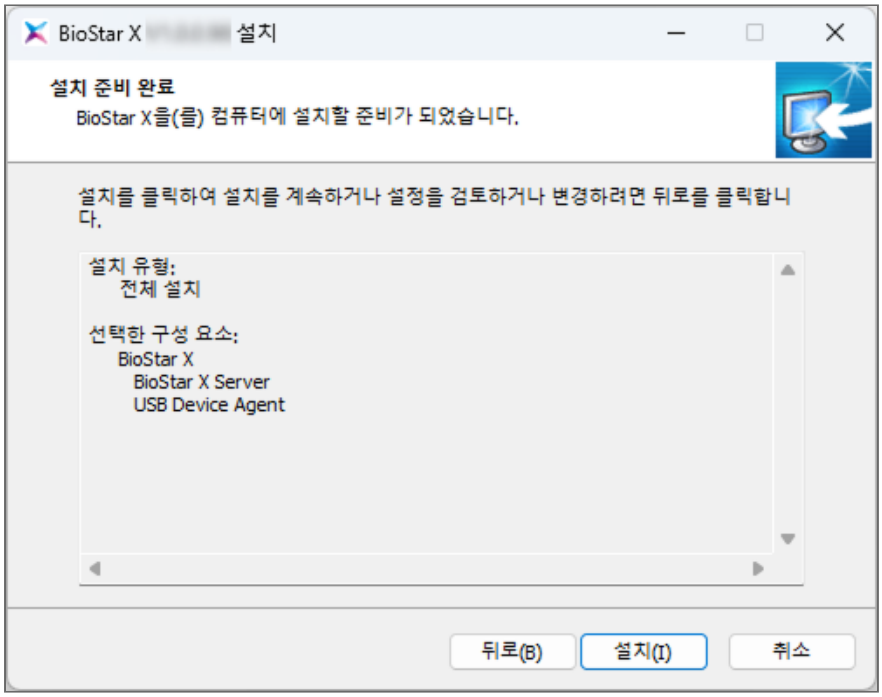
11. **BioStar X**의 통신을 위한 포트를 설정하고 **다음** 버튼을 클릭하세요.



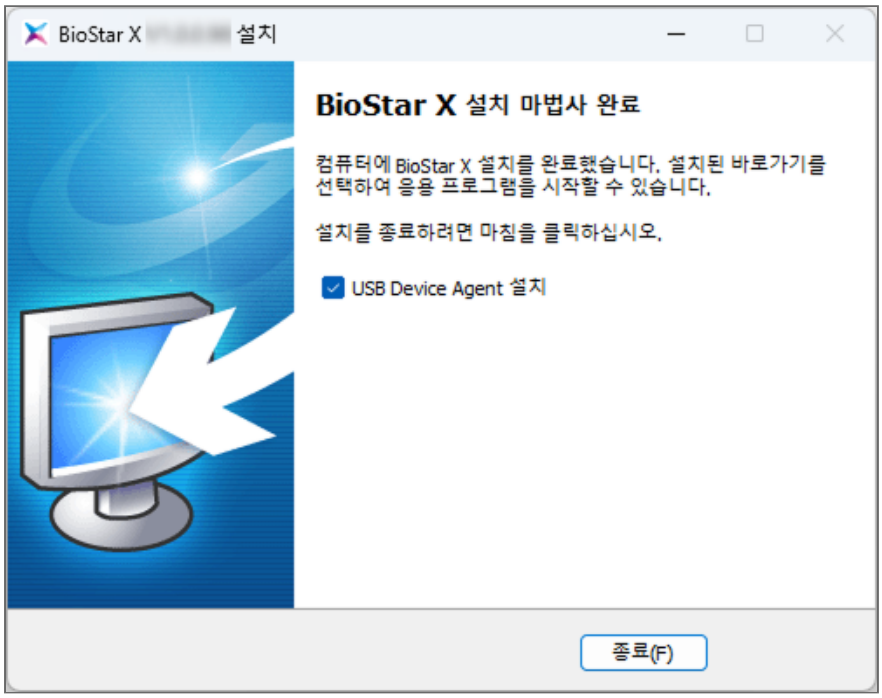
12. **BioStar X**의 구성 요소를 선택한 뒤 **다음** 버튼을 클릭하세요. **USB Device Agent**를 선택하면 BioMini, BioMini Plus 2, BioMini Slim 2, DUALi DE-620을 사용하기 위한 USB Agent와 드라이버를 함께 설치합니다.



13. 모든 설치 준비를 완료했다면 **설치** 버튼을 클릭하세요.



14. 부가 프로그램 설치 여부를 선택하고 **종료** 버튼을 클릭하세요.



15. 설치 화면의 안내에 따라 **USB Device Agent** 설치를 완료하세요.

알아두기

- 다운로드한 파일명에서 `X.Y.Z`는 버전 정보이며, `BB`는 빌드 번호입니다.
- 관리자 계정 암호는 **BioStar X**를 설치한 다음 처음 로그인할 때 사용합니다.
- 데이터베이스의 루트(root) 계정 암호는 AC, TA, Video DB 초기 암호로 사용합니다.
- 암호화 키의 저장 경로를 변경할 수 있습니다. 경로를 변경한 이후에 암호화 키 파일을 수정하거나 다른 경로로 이동시키면 시스템 오류가 발생할 수 있습니다.
- **BioStar X**를 삭제하면 암호화 키 파일도 함께 삭제합니다.
- 제공된 USB Device Agent 인증서는 로컬 네트워크에만 적용할 수 있습니다.
- 다른 프로그램에서 443 포트를 사용하고 있다면 BioStar X Setting 프로그램이 자동으로 실행되어 포트 번호를 변경할 수 있습니다. 포트 번호 변경에 대한 내용은 포트 변경하기를 참고하세요.
- 데이터베이스 설정 변경에 대한 자세한 내용은 데이터베이스 변경하기를 참고하세요.

경고

- 관리자 또는 데이터베이스의 루트(root) 계정 암호를 분실하지 않도록 주의하세요.
- 암호를 분실하면 버전 업그레이드 및 DB 백업/복원이 불가능할 수 있습니다.

다음 단계

웹 브라우저를 실행해 **BioStar X**로 로그인하는 방법을 확인하세요.
BioStar X의 서버 상태를 확인하고 종료 또는 다시 시작하는 방법을 확인하세요.

멀티 커뮤니케이션 서버 설치하기

이 문서에서는 **BioStar X**의 **멀티 커뮤니케이션(Multi Communications) 서버** 설치 방법을 안내합니다.

멀티 커뮤니케이션 서버는 출입통제 장치들과의 통신을 전담하는 서버입니다. 메인 서버와 별도로 설치하여 많은 수의 장치를 안정적으로 관리할 수 있도록 도와줍니다. 한 대의 멀티 커뮤니케이션 서버로 최대 1,000대의 장치를 연결할 수 있으며, 필요에 따라 여러 대의 멀티 커뮤니케이션 서버를 추가할 수 있습니다.

알아두기

이더넷(TCP/IP)으로 연결할 수 있는 장치는 최대 1,000대입니다.

시작하기 전에

멀티 커뮤니케이션 서버를 설치하기 전에 다음 사항을 확인하세요.

- 멀티 커뮤니케이션 서버는 **BioStar X** 서버와 같은 서버에 설치할 수 없습니다.

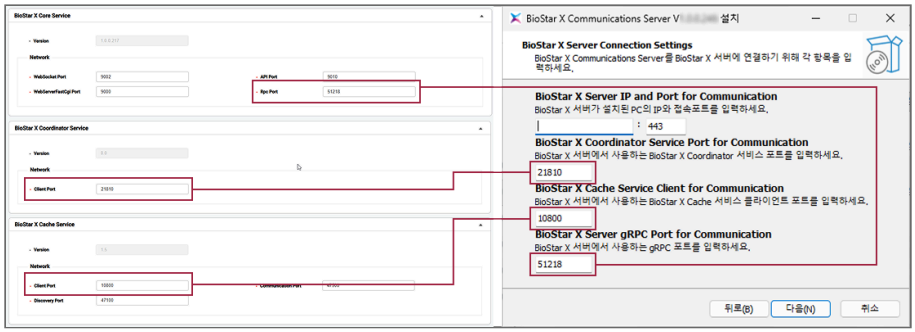
- 멀티 커뮤니케이션 서버는 64비트 운영 체제에서만 설치할 수 있습니다. 시스템 최소 요구 사항에 대한 자세한 내용은 시스템 최소 요구사항을 참고하세요.
- 멀티 커뮤니케이션 서버를 설치하고 연결하려면 멀티 커뮤니케이션 서버 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

설치 전 확인 사항

멀티 커뮤니케이션 서버를 설치하기 전에 **BioStar X Service Manager**를 실행해 설치 중 입력해야 하는 정보를 확인하세요.

1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
2. **BioStar X Service Manager** 창이 나타납니다.
3. **SERVICE SETTINGS**를 클릭하세요.

아래에 멀티 커뮤니케이션 서버 설치 시 입력해야 하는 정보가 나와 있습니다. 각 항목을 확인하고 준비하세요.



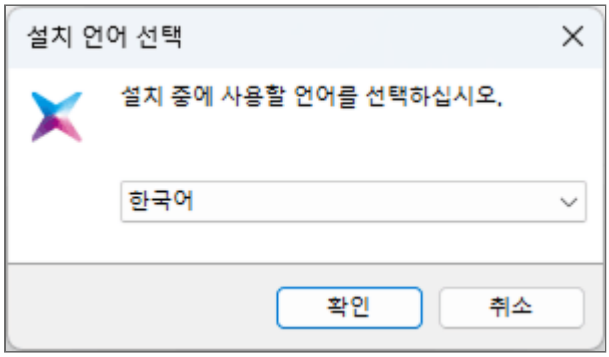
BioStar X Service Manager	멀티 커뮤니케이션 서버 설치 시 입력 정보
BioStar X Core Service → **RPC Port**	BioStar X Server gRPC Port for Communication
BioStar X Coordinator Service → **Client Port**	BioStar X Coordinator Service Port for Communication
BioStar X Cache Service → **Client Port**	BioStar X Cache Service Client for Communication

> **알아두기**
> **SERVICE SETTINGS**에 대한 자세한 내용은 서비스 설정을 참고하세요.

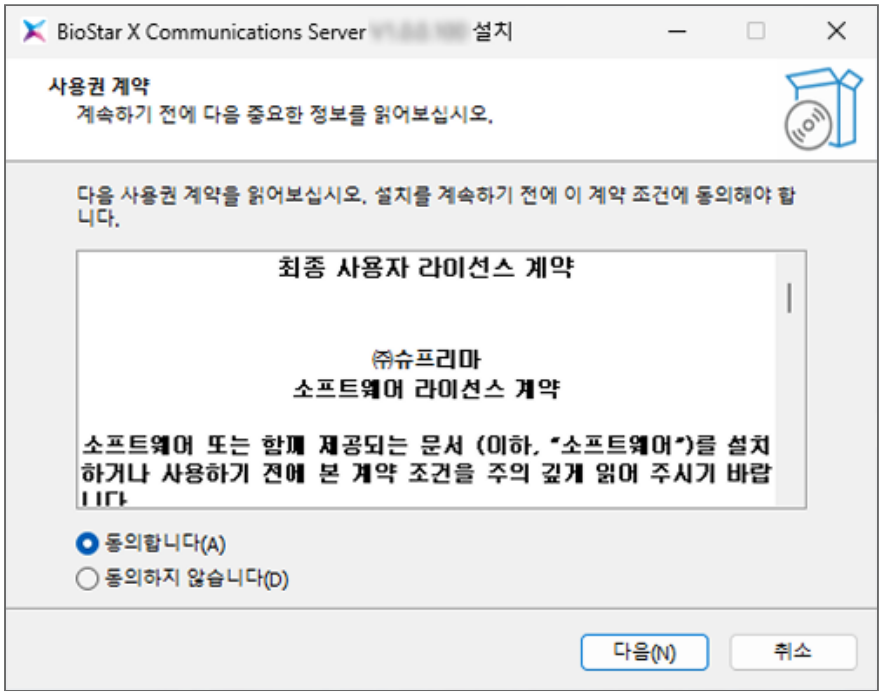
설치 안내

멀티 커뮤니케이션 서버를 설치하려면 다음 단계를 따르세요.

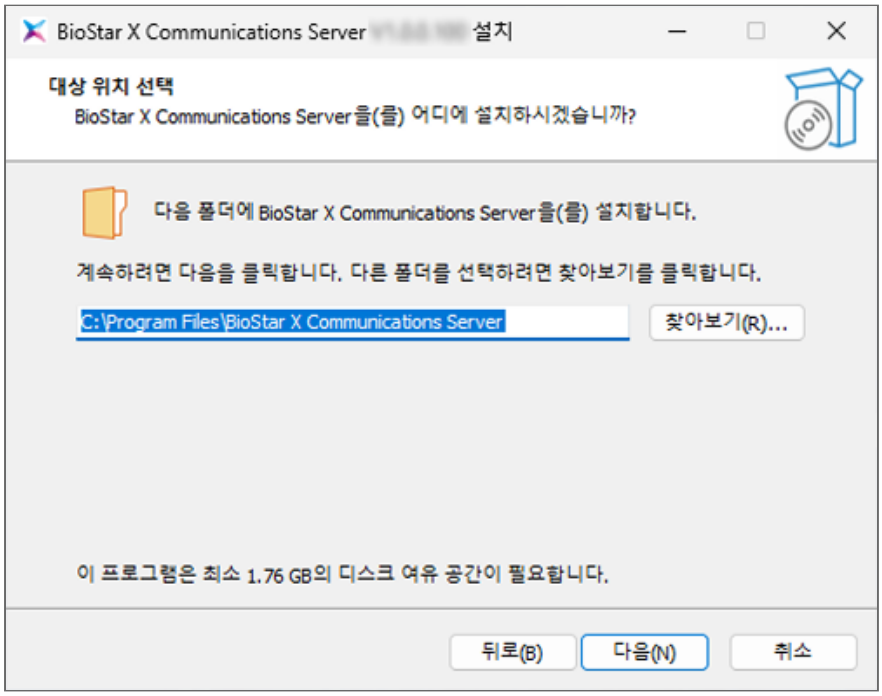
1. 슈프리마 다운로드 센터로 접속해 로그인한 후 설치 패키지(*BioStar X Communications Server.X.Y.X.BB.exe*)를 다운로드하세요.
2. 다운로드한 설치 파일을 실행하세요.
3. 사용할 언어를 선택하고 **확인** 버튼을 선택하세요.



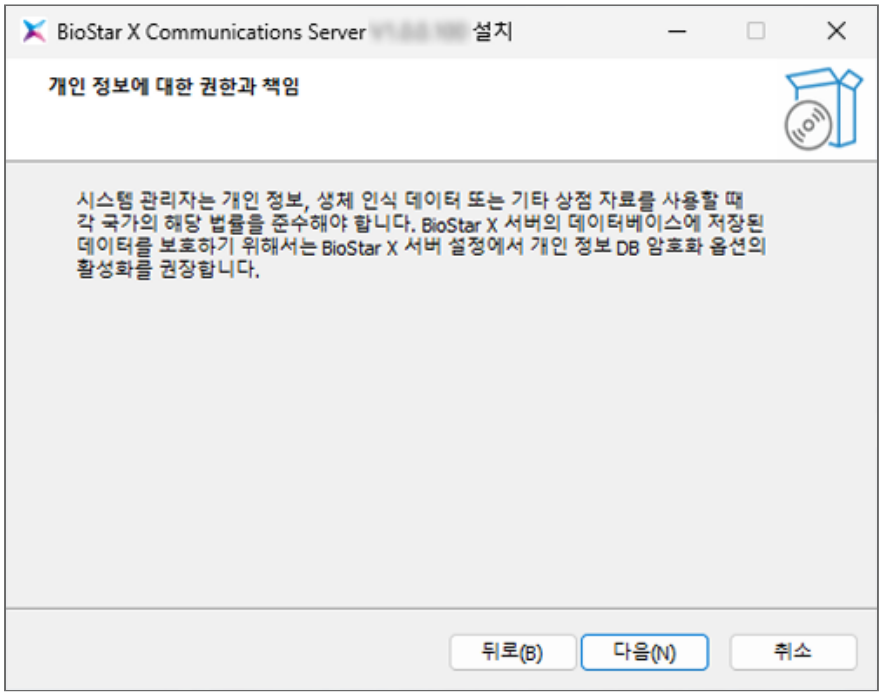
4. 설치를 계속하려면 **동의합니다**를 선택하고 **다음** 버튼을 클릭하세요.



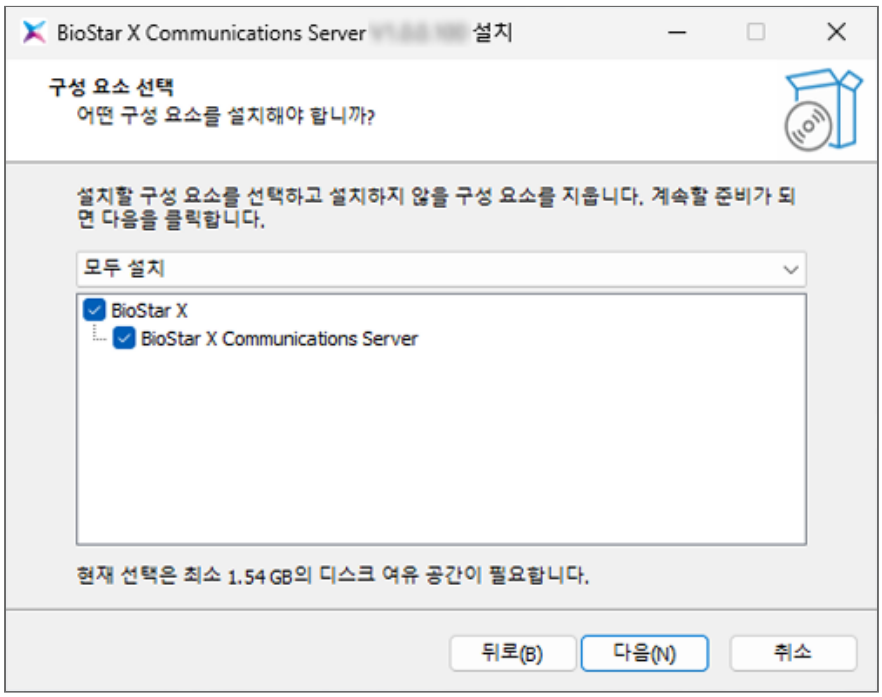
5. 멀티 커뮤니케이션 서버를 설치할 경로를 설정하고 **다음** 버튼을 클릭하세요.



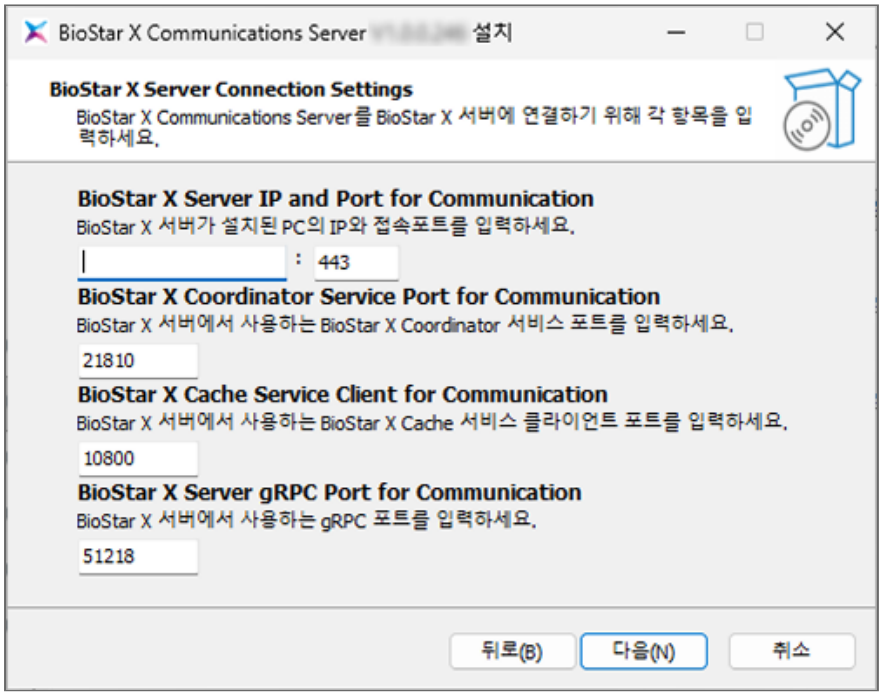
6. 개인 정보에 대한 권한과 책임 내용을 확인하고 설치를 계속하려면 **다음** 버튼을 클릭하세요.



7. 멀티 커뮤니케이션 서버의 구성 요소를 선택하고 **다음** 버튼을 클릭하세요.

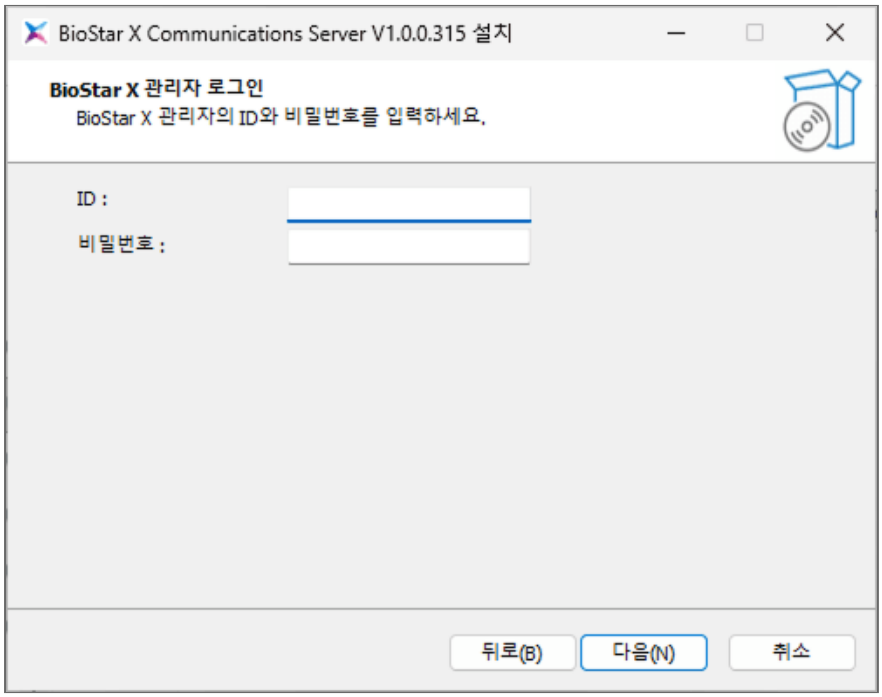


8. **BioStar X** 서버의 IP 주소와 포트 번호를 입력하고, **BioStar X** 서버와 연결하기 위해 각 항목을 입력하세요. 설정을 완료하고 **다음** 버튼을 클릭하세요.

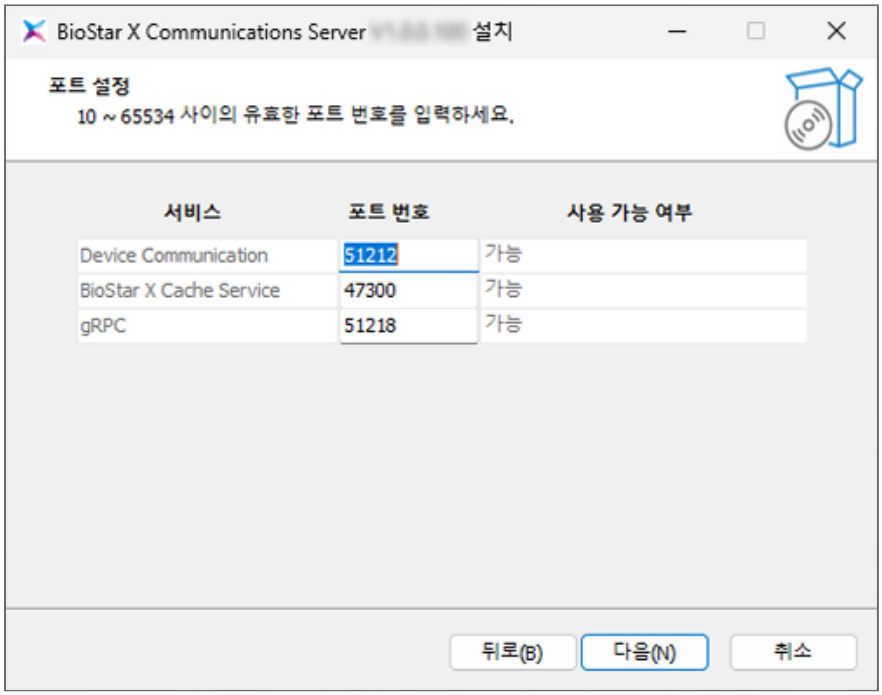


> 각 입력 항목에 대한 자세한 내용은 설치 전 확인 사항을 참고하세요.

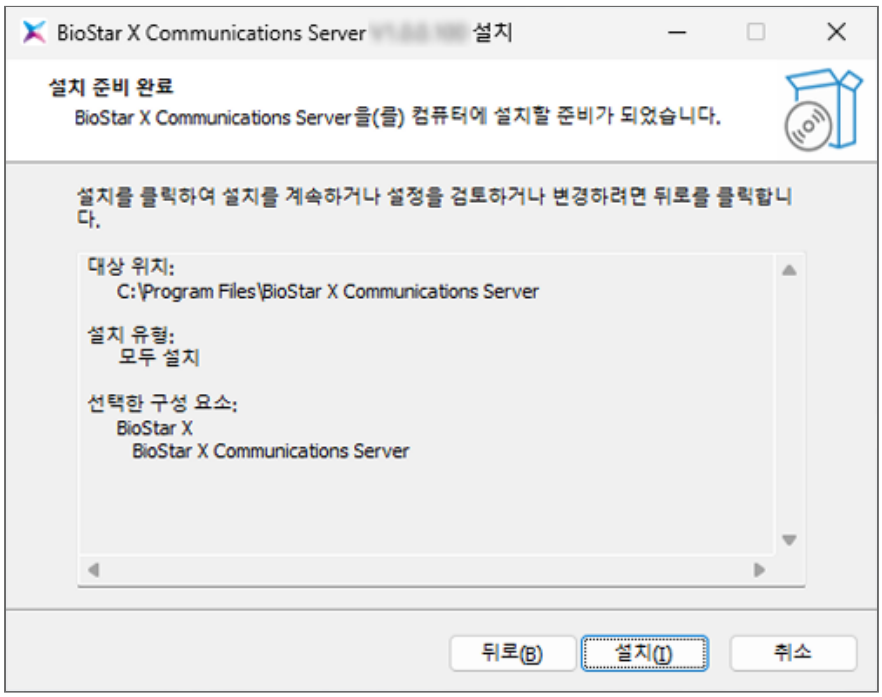
9. **BioStar X**의 관리자 아이디와 비밀번호를 입력하고 **다음** 버튼을 클릭하세요.



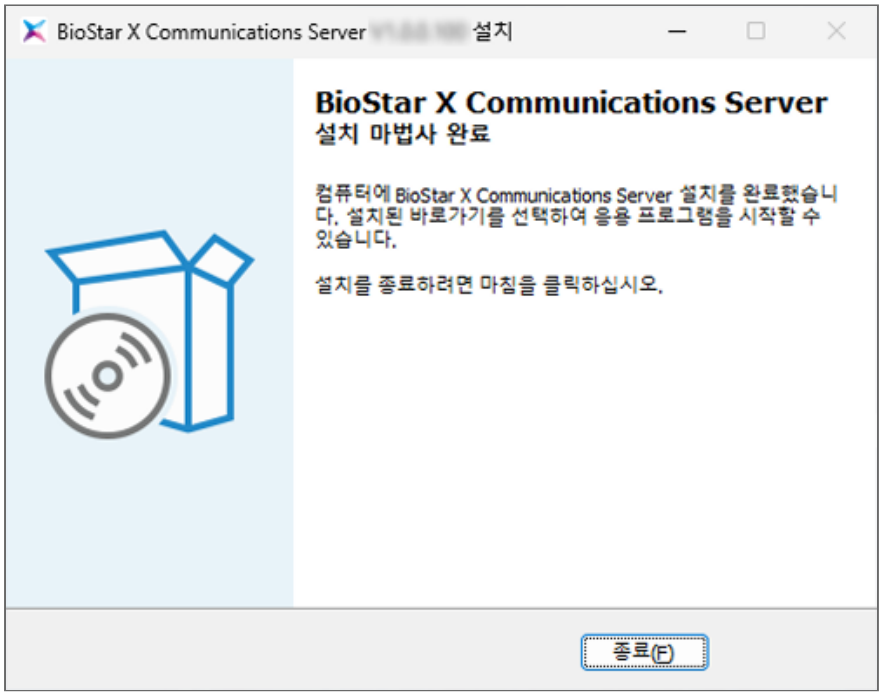
10. 통신을 위한 포트를 설정하고 **다음** 버튼을 클릭하세요.



11. 모든 설치 준비를 완료했다면 **설치** 버튼을 클릭하세요. 설치를 진행합니다.



12. 설치 완료 메시지를 확인하고 **완료** 버튼을 클릭하세요.

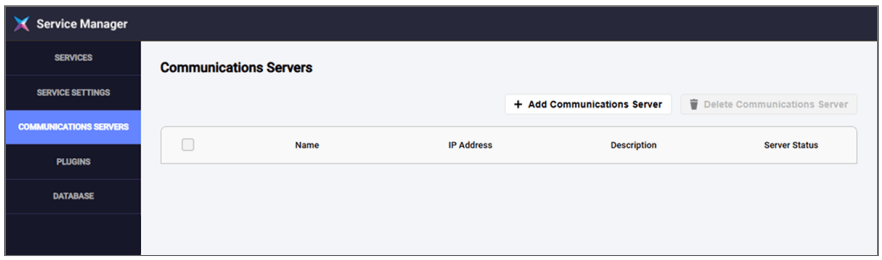


멀티 커뮤니케이션 서버 설치를 완료합니다. 설치를 완료하면 **BioStar X** 메인 서버에서 멀티 커뮤니케이션 서버와 연결되었는지 확인하세요.

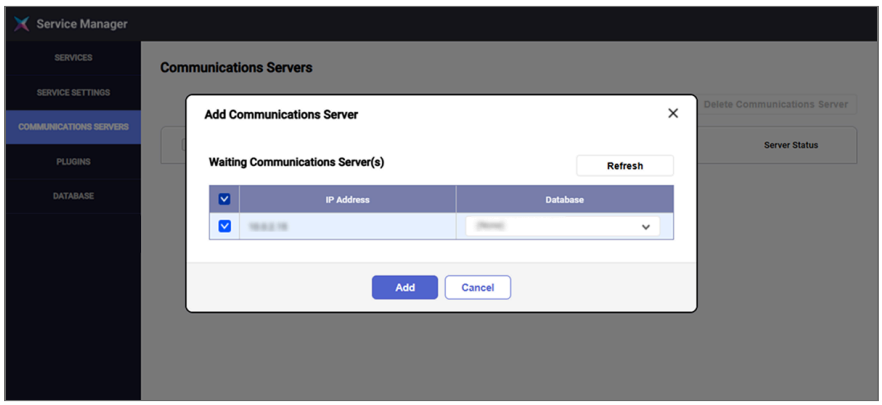
설치 후 확인 사항

멀티 커뮤니케이션 서버 설치를 완료하면 **BioStar X Service Manager**를 통해 메인 서버와 멀티 커뮤니케이션 서버를 연결해야 합니다.

1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
2. **BioStar X Service Manager** 창이 나타납니다.
3. 화면 왼쪽 사이드바에서 **COMMUNICATIONS** 메뉴를 클릭하세요.

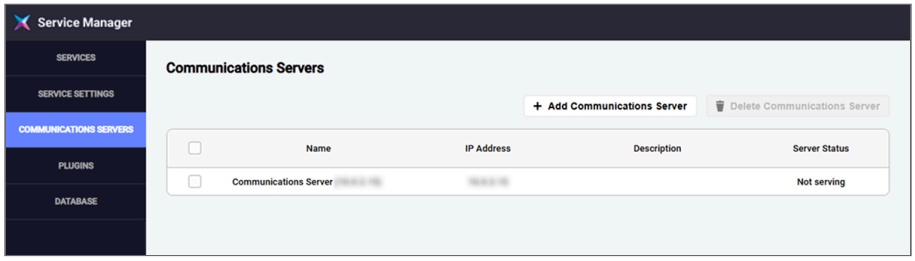


4. 화면 오른쪽 상단의 **Add Communication Server** 버튼을 클릭하세요.
5. **Add Communication Server** 창이 나타나면 설치한 멀티 커뮤니케이션 서버의 IP 주소와 일치하는 항목의 체크박스를 클릭하고, **Database** 열에서 사용할 데이터베이스를 선택하세요.



6. **Add** 버튼을 클릭하세요.

멀티 커뮤니케이션 서버 목록에서 추가한 멀티 커뮤니케이션 서버의 **Server Status** 열이 **Connected** 상태인지 확인하세요.



알아두기

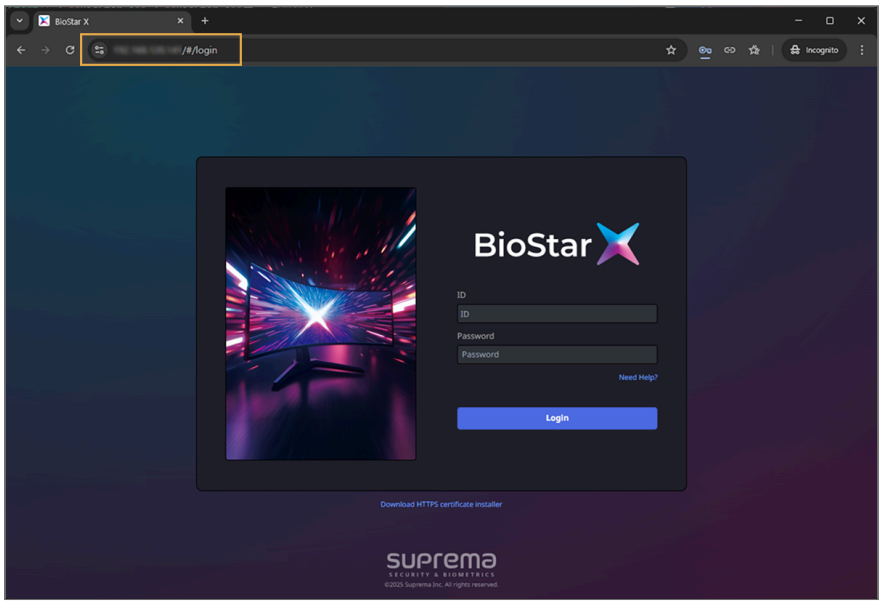
- **COMMUNICATIONS** 메뉴는 멀티 커뮤니케이션 서버 라이선스를 활성화했을 때 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 멀티 커뮤니케이션 서버를 삭제하려면 목록에서 삭제할 서버의 체크박스를 클릭하고 화면 오른쪽 상단의 **Delete Commnunication Server** 버튼을 클릭하세요.
- 멀티 커뮤니케이션 서버를 추가했을 때 메인 서버의 부하를 줄이기 위해 멀티 커뮤니케이션 서버와 연동할 보조 데이터베이스를 추가할 수 있습니다. 보조 데이터베이스 추가에 대한 자세한 내용은 보조 데이터베이스 추가하기를 참고하세요.

로그인하기

설치 패키지를 통해 **BioStar X** 설치를 모두 완료했다면 웹 브라우저로 접속해 정상 동작하는지 확인하세요. **BioStar X**는 웹 기반 서비스를 제공하여 언제 어디서든 접속할 수 있습니다.

웹 브라우저에서 로그인하기

1. Windows에서 시작 → **BioStar X** → **BioStar X**를 클릭하세요.
2. 웹 브라우저를 통해 **BioStar X**로 연결됩니다.



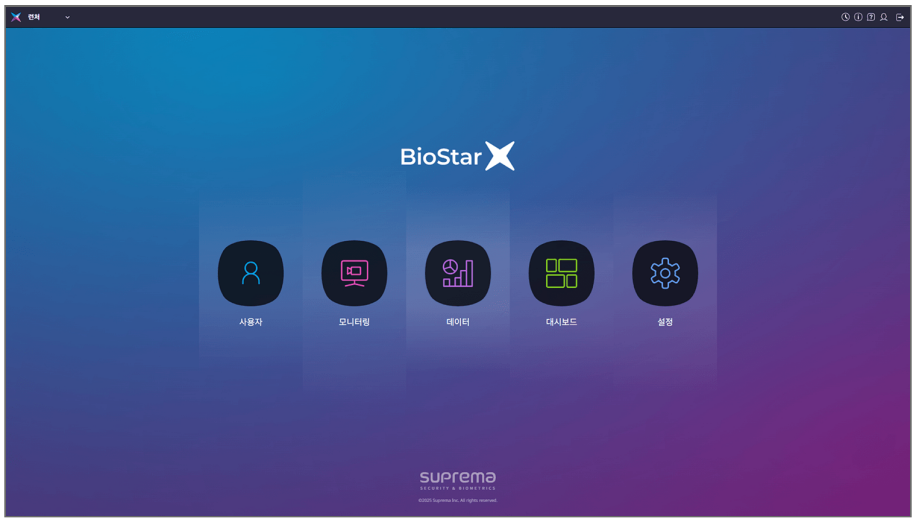
- 웹 브라우저의 주소 표시줄에서 **BioStar X**의 접속 주소를 확인하세요.
- **BioStar X**를 다른 PC에 설치했다면 해당 PC의 IP 주소를 입력하세요. 예, https://192.168.0.1
- 'localhost'를 **BioStar X** 접속 주소로 사용하지 마세요.
- **BioStar X**는 통합 게이트웨이(Unified Gateway)를 통해 모든 요청을 통합 처리합니다. 따라서 웹 접속 및 API 호출은 통합 게이트웨이 포트(기본 443)를 통해 이루어집니다.

3. 로그인 화면이 나타나면 관리자 계정으로 로그인하세요.



- 관리자 아이디는 **admin**입니다.
- 만약 웹 브라우저의 주소 표시줄에 **안전하지 않음** 경고가 표시된다면 HTTPS 인증서를 설치해야 합니다. 인증서 설치에 대한 자세한 내용은 HTTPS 인증서 설치하기를 참고하세요.

로그인하면 **런처** 화면을 확인할 수 있습니다.



알아두기

- Chrome 100 버전 이상의 브라우저를 사용하기를 권장합니다.
- **BioStar X**를 설치한 PC의 외부 IP 주소는 다음 링크로 접속해 확인할 수 있습니다.
- **BioStar X**는 **443** 포트를 기본으로 사용합니다. **443** 포트를 사용하는 프로그램이 있다면 종료하고, 다시 접속을 시도하세요. 해당 프로그램을 종료할 수 없다면 **BioStar X Service Manager**를 실행하여 포트 번호를 변경하세요. 자세한 내용은 포트 변경하기를 참고하세요.

라이선스 키 등록하기

BioStar X 라이선스를 구매했다면 라이선스 키를 등록하고 더 많은 기능을 사용할 수 있습니다.

설정 → **라이선스** → **BioStar X 라이선스** 메뉴로 진입하세요.

사용자의 네트워크 환경에 따라 **BioStar X 라이선스**를 활성화할 수 있는 방법이 다릅니다. 제공하는 안내에 따라 네트워크 상태를 확인하고 라이선스를 활성화하세요.

알아두기

- 라이선스를 등록하지 않은 상태에서는 사용자 추가 및 출입문, 장치 추가와 같은 일부 기능이 제한됩니다.
- **라이선스** 메뉴에 대한 자세한 내용은 라이선스 활성화하기를 참고하세요.
- 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 라이선스 에러코드를 확인하려면 다음 링크를 참고하세요.

온라인 상태에서 등록

알아두기

라이선스 키는 숫자와 하이픈(`-`)만 입력할 수 있습니다. `1111-1111-1111-1111` 형식으로 최대 16자의 숫자를 입력해야 합니다.

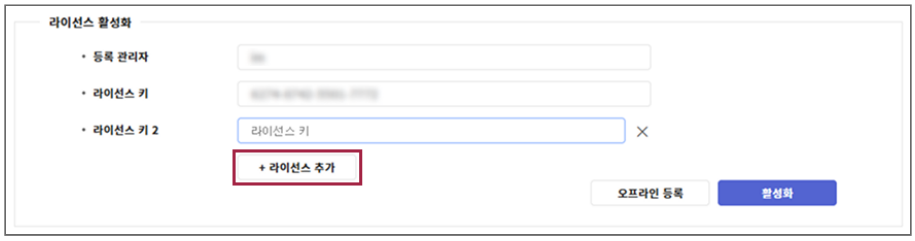
단일 라이선스 등록

인터넷이 연결된 온라인 상태에서 **BioStar X** 라이선스를 활성화하려면, 이름과 전달받은 라이선스 키를 입력하고, **활성화** 버튼을 클릭하세요.



여러 개의 라이선스 등록

최대 30개까지의 라이선스를 한 번에 추가할 수 있습니다. ＋ **라이선스 추가** 버튼을 클릭하세요. 라이선스를 모두 입력한 후 **활성화** 버튼을 클릭하세요.



- 입력 칸이 30개에 도달하면 ＋ **라이선스 추가** 버튼이 비활성화되어 더 이상 추가할 수 없습니다.
- 여러 개의 라이선스 키를 한 번에 복사해 입력 칸에 붙여넣으면, `1111-1111-1111-1111` 형식에 맞는 키만 자동으로 인식해 각 입력 칸에 나눠 추가합니다.
- 붙여넣은 키가 30개를 초과하면 30개까지만 자동으로 입력되고, 초과한 키는 무시됩니다.

활성화 진행 상태

활성화 버튼을 클릭하면 진행 상태 팝업이 표시됩니다. 활성화가 완료될 때까지 페이지나 팝업을 닫지 마세요.

오프라인 상태에서 등록

폐쇄된 네트워크 환경이나 인터넷 연결이 제한된 오프라인 상태에서 **BioStar X** 라이선스를 활성화하려면 다음의 안내에 따르세요.

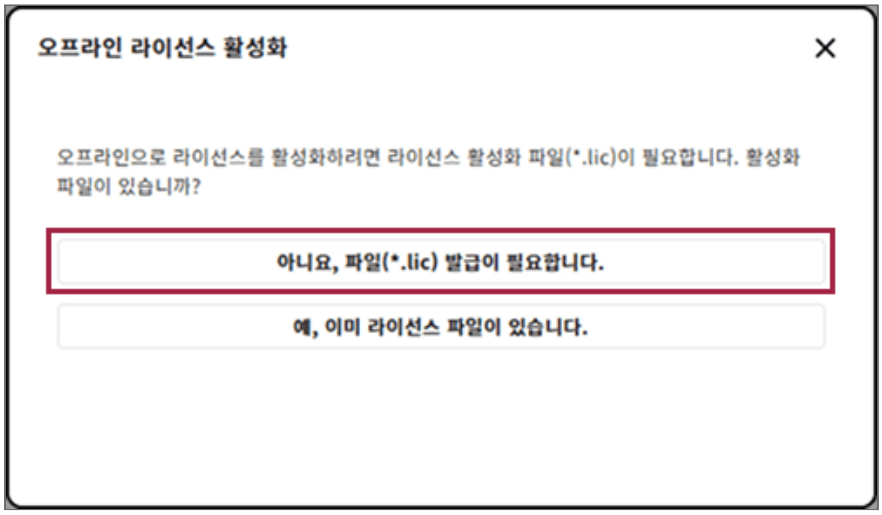
1. **라이선스 활성화** 섹션에서 임의의 등록 관리자 이름과 라이선스 키를 입력하세요.

   - 라이선스 키는 숫자와 하이픈(`-`)만 입력할 수 있습니다. `1111-1111-1111-1111` 형식으로 최대 16자의 숫자를 입력해야 합니다.
   - 등록 관리자 이름과 라이선스 키를 기억하거나 메모해두세요.
   - 여러 개의 라이선스가 필요하다면 ＋ **라이선스 추가** 버튼을 클릭해 추가하세요.

2. **오프라인 등록** 버튼을 클릭하세요.

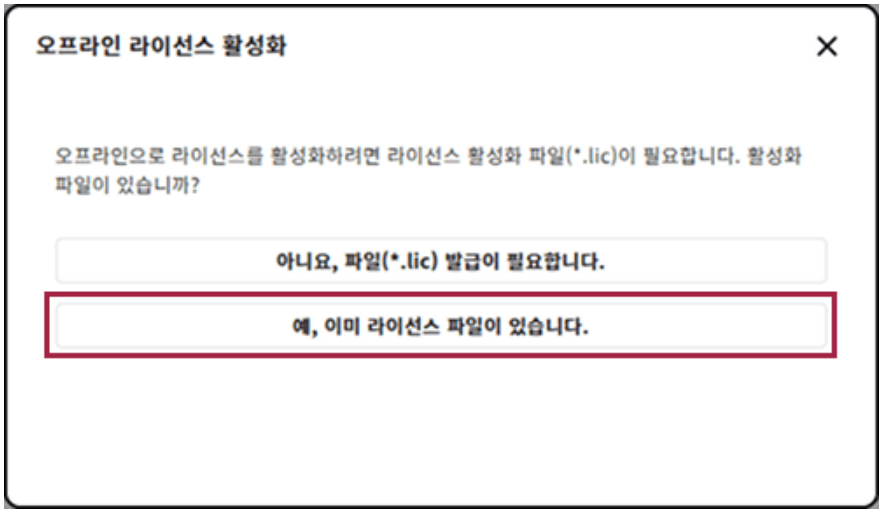


3. **오프라인 라이선스 활성** 창이 나타나면 **아니요, 파일(*.lic) 발급이 필요합니다.** 버튼을 클릭하세요.



> 이미 발급받은 라이선스 파일이 있다면, 이 화면에서 **예, 이미 라이선스 파일이 있습니다.** 버튼을 클릭한 후 9단계로 이동하세요.

4. 발급 요청 파일(*.req)이 생성되면 사용자의 로컬 디스크에 다운로드하세요.
5. 다운로드한 발급 요청 파일을 구매처에 보내 오프라인 활성화 파일(*.lic)을 요청하세요.
6. 오프라인 활성화 파일을 전달 받은 후 1단계에서 입력한 관리자 이름과 라이선스 키를 **라이선스 활성화** 섹션에 입력하세요.
7. **오프라인 등록** 버튼을 클릭하세요.
8. **오프라인 라이선스 활성** 창이 나타나면 **예, 이미 라이선스 파일이 있습니다.** 버튼을 클릭하세요.



9. 파일 열기 창이 나타나면 로컬에 저장된 오프라인 활성화 파일(*.lic) 또는 압축 파일(*.zip)을 선택하세요.

> 여러 개의 라이선스를 요청했을 때는 압축 파일을 전달받을 수 있습니다.

10. 진행 상태 팝업이 표시됩니다. 활성화가 완료될 때까지 페이지나 팝업을 닫지 마세요.

초기 설정 가이드

BioStar X를 처음 설치한 후 정상적으로 운영하기 위해 필요한 설정을 단계별로 안내합니다. 각 단계를 순서대로 진행하여 효율적인 출입 통제 환경을 구축하세요.

1 장치 등록

BioStar X에 연결할 장치를 등록하세요. 장치에 따른 인증 모드를 따로 구성하거나 각각의 장치에 관리자를 설정할 수 있습니다.

또한, 장치에서 발생하는 각종 이벤트(인증 실패, 협박 지문 인증, 안티패스백 위반 등)에 따른 동작을 설정할 수 있습니다.

- 장치 그룹 관리하기
- 장치 등록하기
- Wiegand 장치 등록하기
- 슬레이브 장치 등록하기
- 장치 설정하기

> **알아두기**
> 장치를 등록하려면 **디바이스 매니저** 이상의 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

2 출입문 등록 및 설정

장치가 설치된 출입문 정보를 등록하세요. 릴레이, 안티패스백, 이중 인증, 알람 등을 설정할 수 있습니다.

- 출입문 그룹 관리하기
- 출입문 등록하기

3 출입 등급 설정

출입 등급은 출입문과 스케줄 정보를 조합하여 생성하며, 하나의 출입 등급에 여러 개의 출입문과 스케줄을 등록할 수 있습니다.

출입 등급 관리하기

4 출입 그룹 설정

출입 그룹은 출입 등급(출입문, 스케줄)과 사용자 정보를 조합하여 생성하며, 하나의 출입 그룹에 여러 출입 등급, 사용자를 등록할 수 있습니다.

출입 그룹 관리하기

5 사용자 등록

사용자 정보와 크리덴셜 등 출입 통제에 사용될 정보를 등록하세요. 사용자 정보는 장치에서 직접 등록하거나 BioStar X에서 등록할 수

있습니다. 또한, 장치에서 등록된 사용자 정보를 **BioStar X**로 가져오거나, **BioStar X**에서 등록된 사용자 정보를 장치로 전송할 수 있습니다.

- 사용자 그룹 관리하기
- 사용자 관리하기
- 사용자 등록하기
- 사용자 크리덴셜 등록하기

6 고급 출입 통제 설정

안티패스백, 화재 경보 등을 설정할 수 있으며, 화재 경보는 로컬과 글로벌을 설정할 수 있습니다.

- 고급 출입 통제 설정하기
- 맵 모니터링하기

> **알아두기**
> **에센셜**(Essential) 이상의 라이선스에서만 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

7 모니터링

출입문, 장치, 이벤트 등 다양한 모니터링 기능을 통해 실시간으로 출입 통제 시스템을 관리할 수 있습니다.

- 출입문 모니터링하기
- 장치 모니터링하기
- 이벤트 모니터링하기

서버 관리

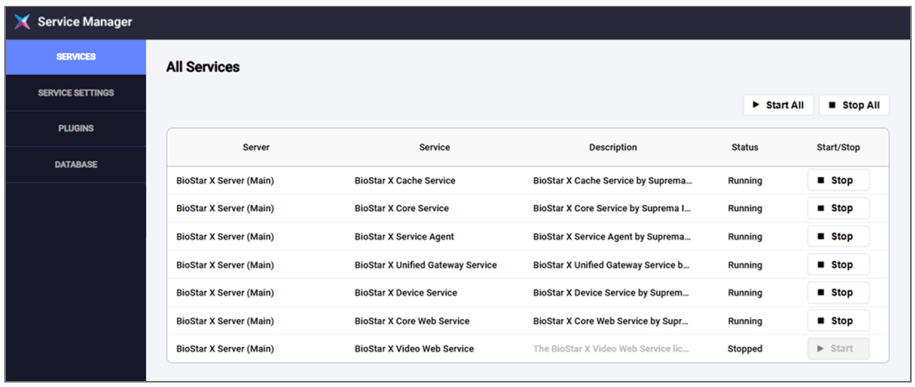
BioStar X를 설치한 후 사용자는 다양한 서버 관리 기능을 통해 시스템을 효율적으로 운영할 수 있습니다. 이 문서에서는 BioStar X의 서버 관리 기능에 대해 안내합니다.

서버 시작 및 종료

BioStar X Service Manager를 사용하여 BioStar X 서버의 서비스를 관리하는 방법을 확인하세요. 개별 서비스를 시작하거나 종료할 수 있습니다.

BioStar X Service Manager

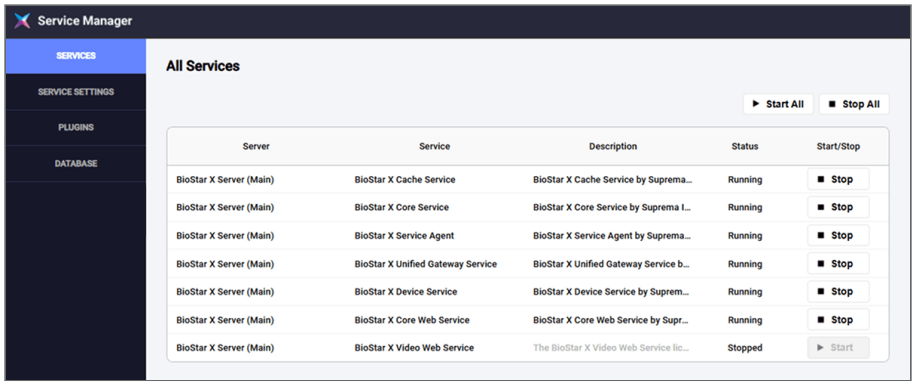
BioStar X 서버의 상태를 관리할 수 있는 도구를 제공합니다. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요. **BioStar X Service Manager** 창이 나타납니다.



> **알아두기**
>
> **BioStar X** 서버의 시간 설정을 변경했다면 **BioStar X Core Service**를 종료하고 다시 시작하세요. 다시 시작하지 않으면 **BioStar X**가 동작하지 않을 수 있습니다.

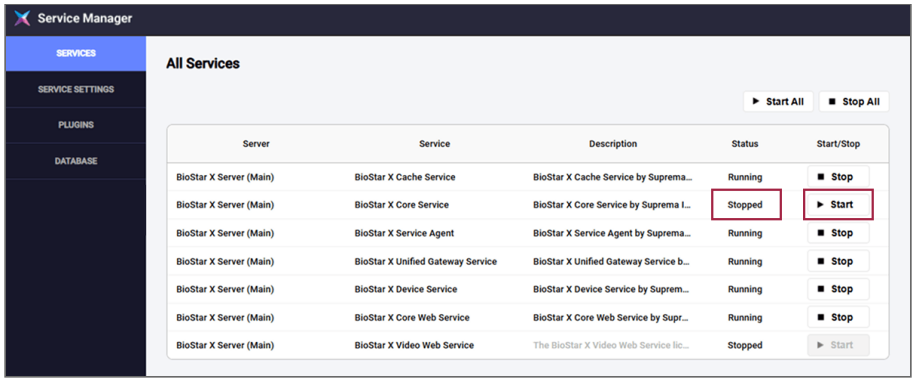
서비스 종료하기

BioStar X를 종료하려면, **SERVICES** 메뉴에서 개별 서비스의 **Stop** 버튼을 클릭하세요. 모든 서비스를 종료하려면 화면 오른쪽 상단의 **Stop All** 버튼을 클릭하세요.



서버 시작하기

BioStar X를 다시 시작하려면, **SERVICES** 메뉴의 **Status** 열에서 **Stopped** 상태인 서비스의 **Start** 버튼을 클릭하세요. 모든 서비스를 다시 시작하려면 화면 오른쪽 상단의 **Start All** 버튼을 클릭하세요.



서비스 설정

BioStar X Service Manager의 **Service Settings** 메뉴에서는 시스템의 핵심 서비스들을 구성하고 관리할 수 있습니다. 각 서비스는 독립적으로 설정되며, 네트워크 포트와 버전 정보를 확인할 수 있습니다.

Service Settings는 아래의 주요 서비스로 구성됩니다.

- **BioStar X Core Web Service**: 웹 인터페이스 서비스
- **BioStar X Core Service**: 시스템 핵심 기능 및 API 통신 서비스
- **Unified Gateway Service**: 역방향 프록시 기반 통합 게이트웨이 서비스
- **BioStar X Coordinator Service**: 분산 시스템 구성 정보 관리 및 서비스 간 동기화
- **BioStar X Server (Main)**: 메인 서버 서비스
- **BioStar X Cache Service**: 데이터 캐싱 및 시스템 성능 향상

설정 변경이 필요한 상황

다음과 같은 상황에서 서비스 설정을 변경해야 할 수 있습니다.

- **포트 충돌 해결**: 다른 애플리케이션이 동일한 포트를 사용하여 충돌이 발생할 때
- **보안 정책 준수**: 조직의 네트워크 보안 정책에 따라 특정 포트 범위만 허용될 때
- **방화벽 설정**: 기업 방화벽에서 허용하는 포트로 변경해야 할 때
- **서버 환경 변경**: 서버 IP 주소 변경이나 네트워크 구성 변경 시
- **성능 최적화**: 트래픽 분산이나 로드 밸런싱을 위한 포트 분리가 필요할 때

설정 변경 방법

1. **BioStar X Service Manager**에서 **SERVICE SETTINGS** 메뉴를 클릭하세요.
2. 변경하려는 서비스 섹션으로 이동하세요.

3. 필요한 포트 번호나 주소를 수정하세요.
4. 변경사항을 적용하려면 화면 오른쪽 상단의 **Apply** 버튼을 클릭하세요.

- 서비스 설정을 변경한 후 변경 사항을 적용하려면 관련 서비스를 재시작하세요.
- 일부 서비스에 따라 포트 변경을 지원하지 않을 수 있습니다.

주의
포트 번호 변경 시 다른 서비스나 애플리케이션과 충돌이 발생하지 않도록 주의하세요.

서비스 구성

BioStar X Core Web Service

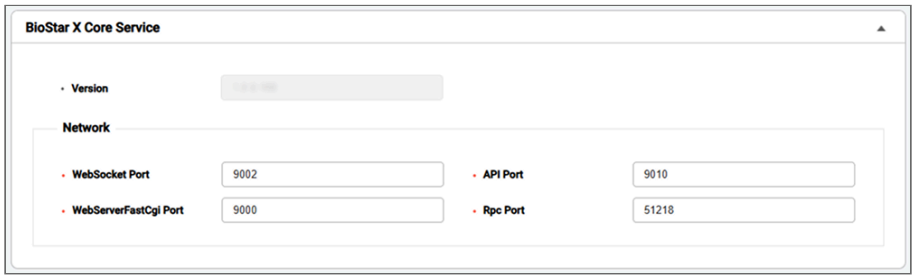
웹 기반 사용자 인터페이스를 담당하는 서비스입니다.



- **HTTPS Port**: 웹 인터페이스 접속 포트 (기본값: 5002)
- **WebServerThrift Port**: Thrift 프로토콜 기반 웹서버 통신 포트 (기본값: 9310)

BioStar X Core Service

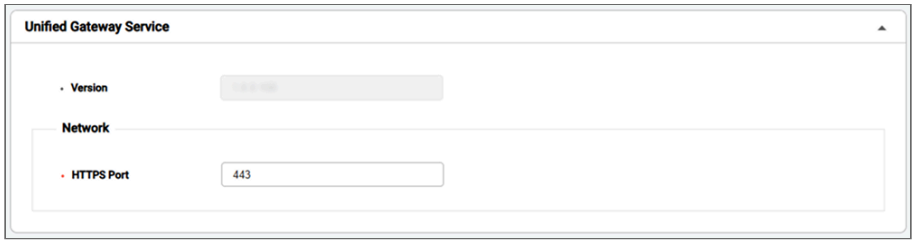
시스템의 핵심 기능과 외부 API 통신을 처리하는 메인 서비스입니다.



- **WebSocket Port**: 실시간 양방향 통신을 위한 웹소켓 포트 (기본값: 9002)
- **API Port**: REST API 통신 포트 (기본값: 9010)
- **WebServerFastCgi Port**: FastCGI 프로토콜 기반 웹서버 통신 포트 (기본값: 9000)
- **Rpc Port**: 원격 프로시저 호출(RPC) 통신 포트 (기본값: 51218)

Unified Gateway Service

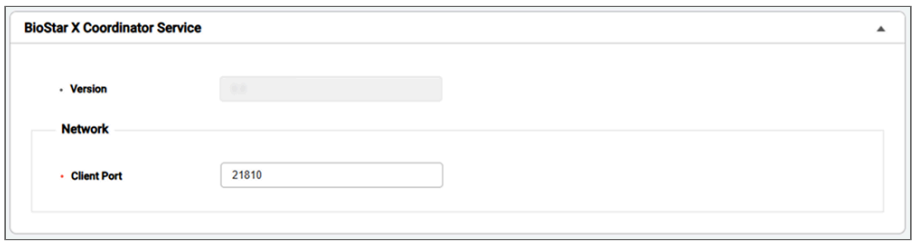
역방향 프록시(Reverse Proxy) 방식을 통해 **BioStar X** 서버에 대한 요청을 효율적으로 처리하고, iframe의 보안 취약점을 개선하며, SSL 인증서 오류를 최소화합니다.



- **HTTPS Port**: 통합 게이트웨이 HTTPS 통신 포트 (기본값: 443)

BioStar X Coordinator Service

분산 시스템의 구성 정보 관리, 서비스 상태 모니터링 및 서비스 간 동기화를 담당하는 서비스입니다.

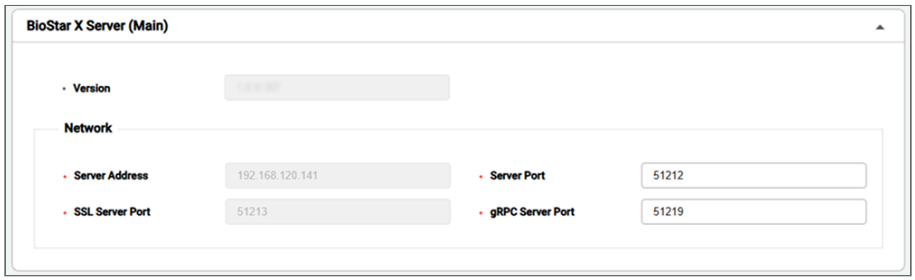


- **Client Port**: 클라이언트 연결을 위한 통신 포트 (기본값: 21810)

> **알아두기**
>
> - **Client Port** 값을 변경하면, **Windows Services**(*services.msc*)에서 **BioStar X Coordinator Service** 서비스를 찾아 수동으로 재시작하세요.
> - **BioStar X Coordinator Service** 서비스를 재시작한 후 **BioStar X Service Manager** → **SERVICES** 메뉴에서 모든 서비스를 재시작하세요.
>
> 화면 오른쪽 상단의 **Stop All** 버튼을 클릭하세요. 모든 서비스가 중지된 후 **Start All** 버튼이 활성화되면 버튼을 클릭하세요.

BioStar X Server (Main)

시스템의 메인 서버 역할을 수행하는 핵심 서비스입니다.

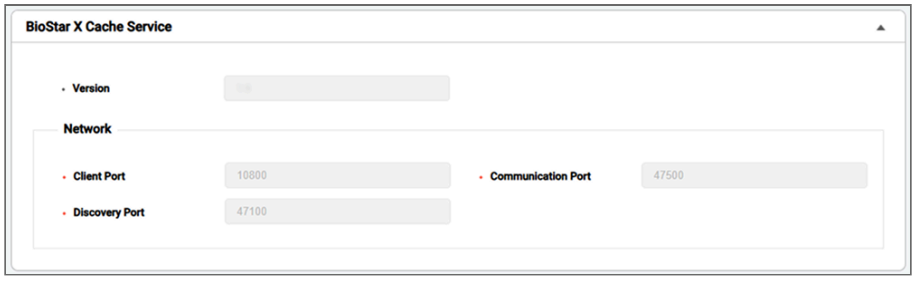


- **Server Address**: 메인 서버의 IP 주소
- **Server Port**: 일반 서버 통신 포트 (기본값: 51212)
- **SSL Server Port**: SSL 보안 암호화 통신 포트 (기본값: 51213)

- **gRPC Server Port**: gRPC 프로토콜 기반 고성능 통신 포트 (기본값: 51219)

BioStar X Cache Service

자주 사용되는 데이터를 메모리에 저장하여 시스템의 데이터 처리 속도와 성능을 향상시키는 서비스입니다.



- **Client Port**: 캐시 서비스 클라이언트 연결 포트 (기본값: 10800)
- **Communication Port**: 캐시 노드 간 내부 통신 포트 (기본값: 47500)
- **Discovery Port**: 분산 캐시 노드 자동 발견을 위한 포트 (기본값: 47100)

다음 단계

BioStar X의 기본 포트(443)를 변경하는 방법을 단계별로 알아보세요.

메인 서버의 IP 주소 변경하기

서버의 네트워크 환경이 변경되었거나 초기 설정 후 IP 주소를 변경해야 할 때 이 문서를 참고하세요. BioStar X 메인 서버의 IP을 안전하게 변경하고 연결된 멀티 커뮤니케이션 서버를 재구성하는 방법을 안내합니다.

> **알아두기**
> 메인 서버의 IP 주소 변경 기능은 **BioStar X v1.0.2** 이상에서 지원합니다.

IP 주소 변경

BioStar X를 설치한 서버에서 먼저 IP 주소를 변경하세요. 외부 네트워크와 연결된 랜 카드의 IP 주소를 변경해야 합니다.

> **알아두기**
> Windows에서 IP 주소 변경에 대한 자세한 내용은 Microsoft 고객 지원에서 확인할 수 있습니다.

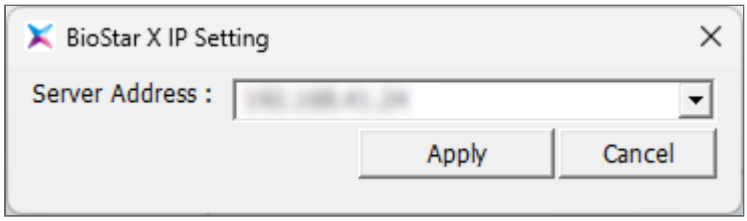
변경한 IP 주소 적용

다음 안내에 따라 **BioStar X**를 설치한 서버의 IP 주소를 변경하세요.

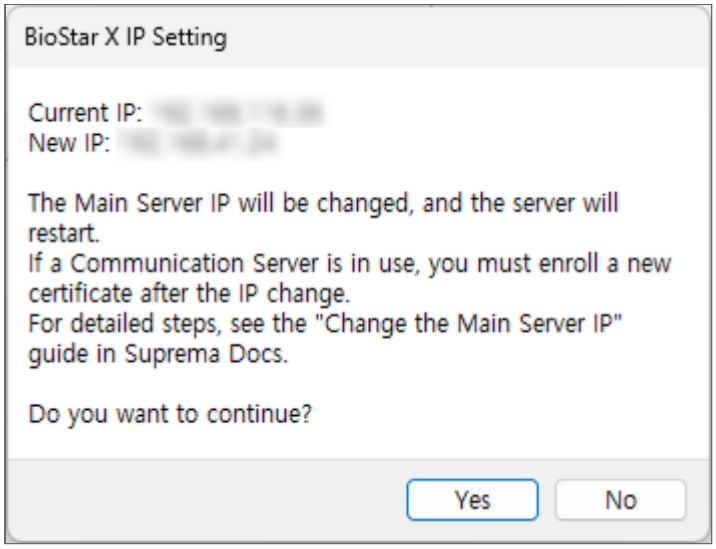
BioStar X IP Setting

BioStar X IP Setting 툴을 사용해 IP 주소를 변경할 수 있습니다.

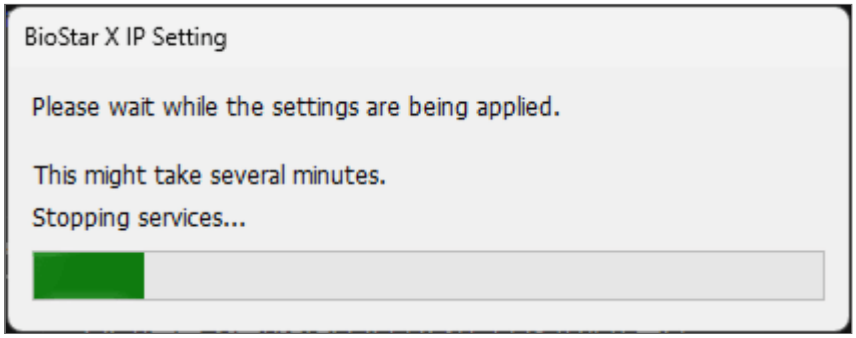
1. Windows에서 시작 → **BioStar X** → **BioStar X IP Setting**을 클릭하세요.
2. **BioStar X IP Setting** 창이 나타나면 **Server Address**에서 변경할 IP 주소를 선택하세요.



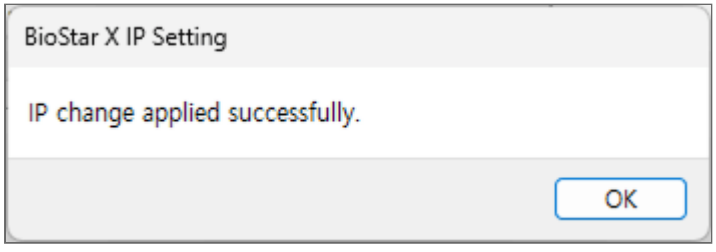
3. **Apply** 버튼을 클릭하세요.
4. IP 주소 변경에 대한 메시지 창이 나타나면 내용을 확인하고 **Yes** 버튼을 클릭하세요.



5. IP 주소 변경 프로세스가 완료될 때까지 기다리세요. 완료되면 성공 메시지 창이 나타납니다.



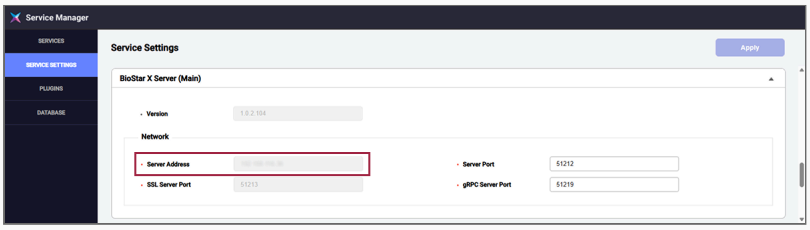
6. **IP change applied successfully** 메시지 창이 나타나면 **OK** 버튼을 클릭하세요.



IP 주소 변경이 완료되면 모든 서비스를 재시작합니다.

알아두기

- 변경할 IP 주소는 수동으로 입력할 수 없으며, **Server Address** 항목에 표시된 IP 주소 중에서 선택할 수 있습니다.
- 변경한 IP 주소는 **BioStar X Service Manager** → **SERVICE SETTINGS** → **BioStar X Server (Main)** 섹션의 **Server Address** 항목에서 확인할 수 있습니다.



- 장치가 **장치에서 서버 연결** 옵션으로 BioStar X에 등록되었다면, 해당 장치에서 서버 IP 주소를 변경한 IP 주소로 관리자가 직접 업데이트해야 합니다.

데이터베이스 서버 설정 수정

데이터베이스를 **BioStar X**와 같은 서버에 설정해 운영 중이라면, 모든 서비스를 중지한 후 **BioStar X**의 *system.conf* 파일을 수정해야 합니다. 외부 데이터베이스 서버를 사용 중이라면 이 단계를 건너뛰세요.

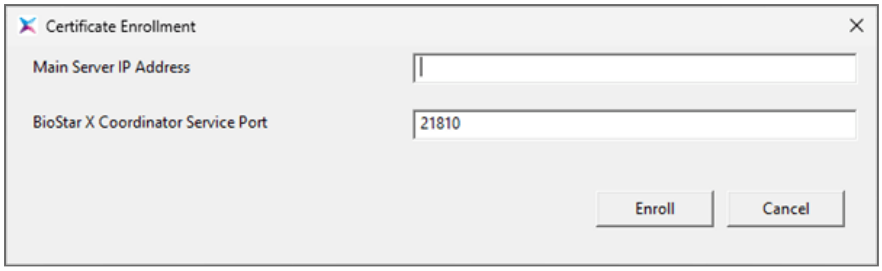
1. Windows 서비스(service.msc)에서 **BioStar X** 관련 모든 서비스를 중지하세요.
2. *C:\Program Files\BioStar X Server* 경로로 이동하세요.
3. *system.conf* 파일을 메모장과 같은 텍스트 편집기로 열어주세요.
4. `database` 관련 항목의 `server_ip` 값에서 변경된 IP 주소로 수정하세요.
5. *system.conf* 파일을 저장하고 닫으세요.
6. Windows 서비스(service.msc)에서 **BioStar X** 관련 모든 서비스를 재시작하세요.

웹 브라우저를 열어 변경된 IP 주소로 정상 접속되는지 확인하세요.

멀티 커뮤니케이션 서버 업데이트

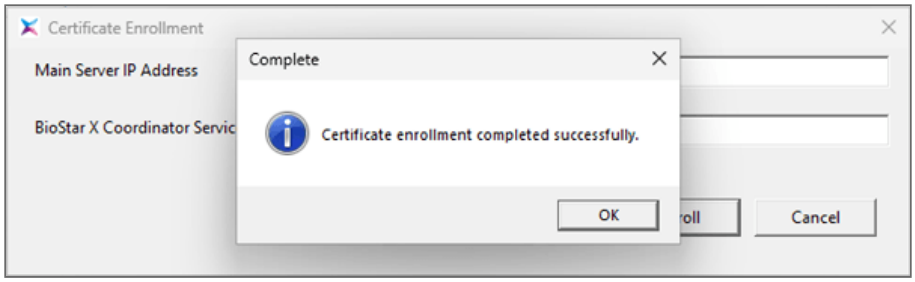
멀티 커뮤니케이션 서버를 추가로 설치했다면 메인 서버의 변경한 IP 주소로 멀티 커뮤니케이션 서버 설정을 변경해야 합니다. 멀티 커뮤니케이션 서버를 설치한 서버에서 진행하세요.

1. *C:\Program Files\BioStar X Communications Server* 경로로 이동하세요.
2. *biostar-device-cert-enroll.exe* 파일을 실행하세요.
3. **Certificate Enrollment** 창이 나타나면 **Main Server IP Address** 입력 필드에 변경한 메인 서버의 IP 주소를 입력하세요.



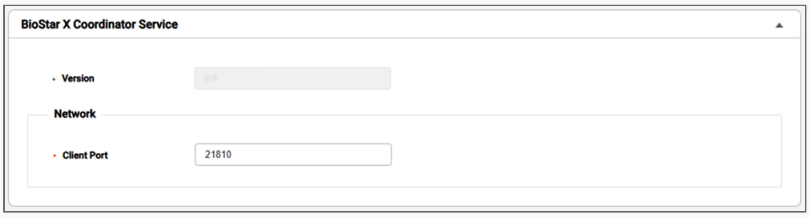
4. 메인 서버의 포트 번호가 기본값(21810)과 다르다면 **BioStar X Coordinator Service Port** 필드에 변경한 포트 번호를 입력하세요.
5. **Enroll** 버튼을 클릭하세요.

메인 서버에 대한 IP 주소 변경을 완료하면 성공 메시지가 나타납니다.



알아두기

- 멀티 커뮤니케이션 서버를 설치하지 않았다면 이 단계를 건너뛰세요.
- BioStar X를 설치한 메인 서버의 포트 번호를 변경했다면, 메인 서버에서 **BioStar X Service Manager**를 실행하고 **SERVICE SETTINGS** → **BioStar X Coordinator Service** 섹션의 **Client Port** 값을 확인하세요.

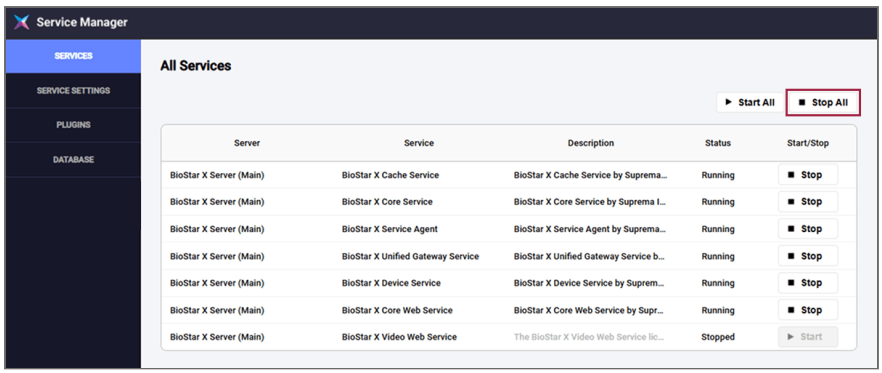


- 멀티 커뮤니케이션 서버 설치에 대한 자세한 내용은 멀티 커뮤니케이션 서버 설치하기를 참고하세요.

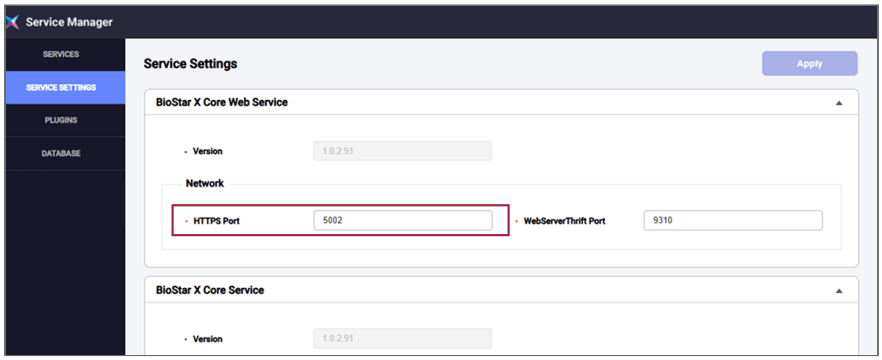
포트 변경하기

BioStar X의 기본 포트(443)를 사용할 수 없을 때 포트를 변경하는 방법을 안내합니다.

1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
2. 웹브라우저를 통해 **BioStar X Service Manager** 창이 나타나면 **SERVICES** 메뉴를 클릭하세요.
3. 모든 서비스를 종료하려면 화면 오른쪽 상단의 **Stop All** 버튼을 클릭하세요.



4. 화면 왼쪽 사이드바에서 **SERVICE SETTINGS** 메뉴를 클릭하세요.
5. **Unified Gateway Service** 섹션의 **HTTPS Port** 입력 필드에서 변경할 포트 번호를 입력하세요.



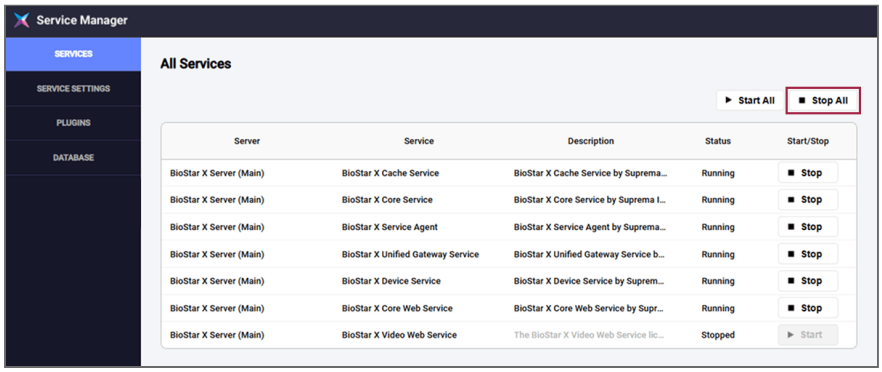
6. 화면 오른쪽 상단의 **Apply** 버튼을 클릭하세요.
7. 확인 메시지가 나타나면 **OK** 버튼을 클릭하세요.
8. **SERVICES** 메뉴로 이동하여 모든 서비스의 **Start** 버튼을 클릭하세요.
9. 웹 브라우저를 통해 **BioStar X**로 접속하세요.

> **알아두기**
>
> - 포트 번호를 450으로 변경했다면 주소 표시줄에 `https://{ip_address}:450`을 입력하세요.
> - 일부 서비스에 따라 포트 변경을 지원하지 않을 수 있습니다.

데이터베이스 변경하기

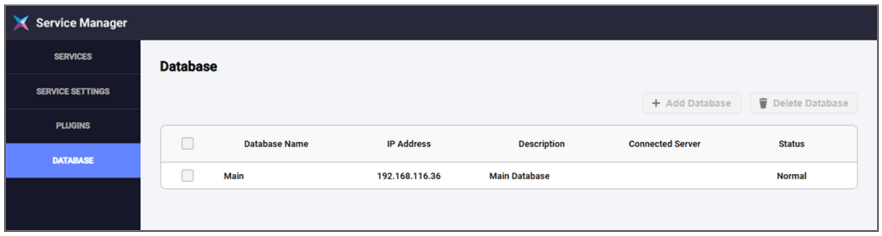
데이터베이스의 설정을 변경할 수 있습니다.

1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
2. 웹브라우저를 통해 **BioStar X Service Manager** 창이 나타나면 **SERVICES** 메뉴를 클릭하세요.
3. 모든 서비스의 **Stop** 버튼을 클릭하세요.

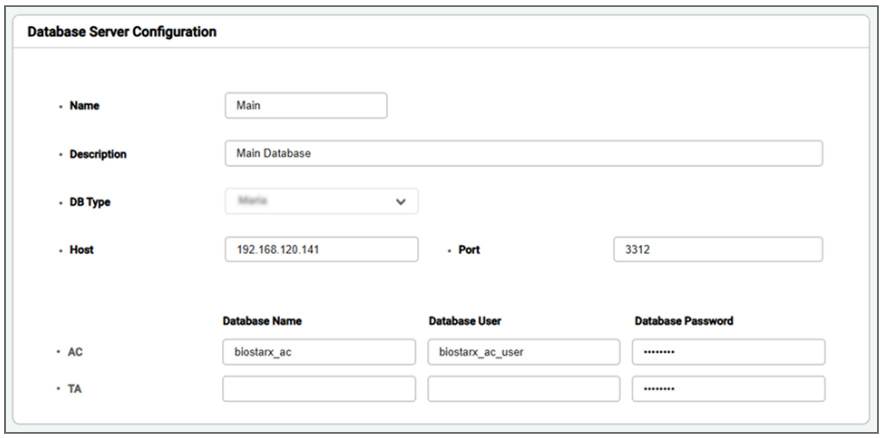


> 모든 서비스를 한번에 중지하려면 **Stop All** 버튼을 클릭하세요.

4. 화면 왼쪽 사이드바에서 **DATABASE** 메뉴를 클릭하세요.



5. 데이터베이스 목록에서 설정을 변경할 데이터베이스를 선택하세요.
6. **Database Server Configuration** 섹션에서 다음 설정을 변경할 수 있습니다.



- **Name**: 데이터베이스 이름을 입력하세요.
- **Description**: 데이터베이스 설명을 입력하세요.
- **DB Type**: 데이터베이스 유형을 선택하세요. (MariaDB, MS SQL)
- **Host**: 데이터베이스 서버의 호스트 이름 또는 IP 주소를 입력하세요.
- **Port**: 데이터베이스 서버의 포트 번호를 입력하세요.
- **AC** / **TA** / **Video**: AC, TA, Video 데이터베이스의 이름, 사용자, 비밀번호를 입력하세요.

7. 데이터베이스가 정상 연결되었는지 확인하려면 화면 오른쪽 상단의 **Test Connection** 버튼을 클릭하세요.
8. 설정을 저장하려면 화면 오른쪽 상단의 **Save** 버튼을 클릭하세요.

보조 데이터베이스 추가하기

멀티 커뮤니케이션 서버를 추가했을 때 메인 서버의 부하를 줄이기 위해 멀티 커뮤니케이션 서버와 연동할 보조 데이터베이스를 추가하고 연결하는 방법을 안내합니다.

알아두기

- 보조 데이터베이스를 추가하려면 **멀티 커뮤니케이션 서버** 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 멀티 커뮤니케이션 서버 설치에 대한 자세한 내용은 멀티 커뮤니케이션 서버 설치하기를 참고하세요.

시작하기 전에

MariaDB를 사용하는 환경에서 데이터베이스 간 통신할 때 IP 주소가 아닌 도메인 또는 호스트 이름을 사용한다면 다음 안내 사항을 반드시 확인하세요.

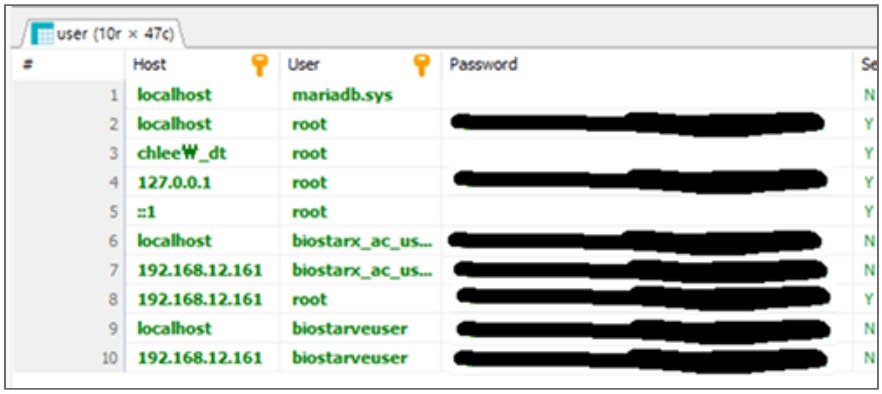
- IP 주소를 사용하지 않는다면 `Create user` 또는 `Grant` 등록이 불가능할 수 있습니다.
- 도메인 또는 호스트 이름을 사용하여 통신한다면 반드시 localhost에 대해 user 및 권한 등록이 되어 있는지 확인하세요.
- BioStar X를 간편 설치 방식으로 설치했다면 루트(root) 계정이 localhost로만 user 및 권한이 등록되어 있기 때문에 해당 서버의 IP 주소나 *127.0.0.1*로 추가 등록해야 합니다.

등록 방법

호스트가 *127.0.0.1*이고, User가 root인 계정에 대해서 비밀번호가 설정되어 있는지 확인하고, 설정되어 있지 않다면 반드시 비밀번호를 설정하고 권한을 부여하세요.

1. 호스트가 *127.0.0.1*이고, User가 root인 계정에 대해서 비밀번호가 설정되어 있는지 확인하세요.

```
SELECT * FROM mysql.user;
```



빈칸이면 비밀번호가 설정되어 있지 않기 때문에 다음 항목에 있는 쿼리를 실행해서 비밀번호 추가 및 권한 부여를 반드시 진행하세요.

2. 호스트가 *127.0.0.1*이고, User가 root인 계정에 대해서 비밀번호를 설정하고 권한을 부여하세요.

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';

CREATE USER '<Main DB AC User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'127.0.0.1';
CREATE USER '<Main DB AC User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'::1';

CREATE USER '<Main DB TA User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'127.0.0.1';
CREATE USER '<Main DB TA User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'::1';

CREATE USER '<Main DB VE User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'127.0.0.1';
CREATE USER '<Main DB VE User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'::1';

FLUSH PRIVILEGES;
```

Example

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY 'admin1234!';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';
FLUSH PRIVILEGES;
```

IP 주소로 통신 설정

아래 설정을 통해 강제로 IP 주소로 통신하도록 설정할 수 있습니다.

1. **BioStar X**를 설치한 다음 경로로 이동하세요.

   > *C:\Program Files\BioStar X\ta\mariadb-11.4.4-winx64*

2. *my.cnf* 파일을 권리자 권한으로 열고 [mysqld] 섹션에 `skip-name-resolve` 옵션을 추가하세요.

```
[mysqld]
port = 3312
character-set-server=utf8
collation-server=utf8_unicode_ci
socket = /tmp/mysql.sock
skip-external-locking
key_buffer_size = 32M
max_allowed_packet = 64M
...
skip-name-resolve
```

3. MariaDB 서비스를 재시작하세요.

보조 데이터베이스 추가

보조 데이터베이스를 추가하는 방법을 안내합니다. 사용하는 데이터베이스 종류에 따라 MariaDB와 SQL Server, 두 가지 방법이 있습니다.

MariaDB

1 메인 데이터베이스

신규 보조 데이터베이스에서 메인 데이터베이스로 접근할 수 있도록 계정 및 권한을 부여하세요.

```
CREATE USER '<Main DB AC Schema User>'@'<Sub DB IP>' IDENTIFIED BY '<Main DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Main DB AC Schema>.* TO '<Main DB AC Schema User>'@'<Sub DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.42' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.42';
FLUSH PRIVILEGES;
```

2 보조 데이터베이스

메인 데이터베이스에서 신규 보조 데이터베이스로 접근할 수 있도록 계정 및 권한을 부여하세요.

```
CREATE USER '<Sub DB AC Schema User>'@'<Main DB IP>' IDENTIFIED BY '<Sub DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Sub DB AC Schema>.* TO '<Sub DB AC Schema User>'@'<Main DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.161' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.161';
FLUSH PRIVILEGES;
```

3 FederatedX 사용 여부 확인

메인 및 보조 데이터베이스에서 아래 명령어를 실행해 FederatedX 스토리지 엔진이 활성화되어 있는지 확인하세요.

```
SHOW ENGINES;
```

쿼리 결과에 `Engine : FEDERATED, Support : YES` 라고 표시되면 이미 설치되어 있습니다. FederatedX 스토리지 엔진이 설치되어 있지 않다면 아래 쿼리를 실행하세요.

```
INSTALL PLUGIN federated SONAME 'ha_federatedx';
```

> **알아두기**
> MariaDB를 설치한 경로 하위에서 *lib/plugin* 폴더에 *ha_federatedx.dll* 파일이 있는지 확인하세요. 일반적으로 *C:\Program Files\MariaDB {version}\lib\plugin* 경로에 dll 파일이 존재합니다.

4 서버 별칭 등록

보조 데이터베이스에 생성될 federatedX 테이블이 메인 데이터베이스의 원본 테이블에 접근할 수 있도록 서버 별칭(alias)을 등록하세요.

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');

-- 정상 등록 확인
SELECT * FROM mysql.servers;
```

기존 등록한 서버 이름에 Host, Port, DB, User, Password에 대한 정보를 변경해야 한다면 `Alter` 문으로 수정할 수 있습니다. 일부 정보만 변경할 수도 있습니다.

```
ALTER SERVER 'default' OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');
```

Example

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_user', PASSWORD 'password');

ALTER SERVER 'default' OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER 'biostarx_ac_usermt__fttid__', PASSWORD 'password');
```

5 테이블 link 설정

보조 데이터베이스에 필요한 테이블은 아래 순서대로 진행해서 메인 데이터베이스의 테이블을 보조 데이터베이스에 link 설정하세요.

- 아래는 메인 데이터베이스에서 `CREATE TABLE` 문 쿼리 생성 쿼리입니다.

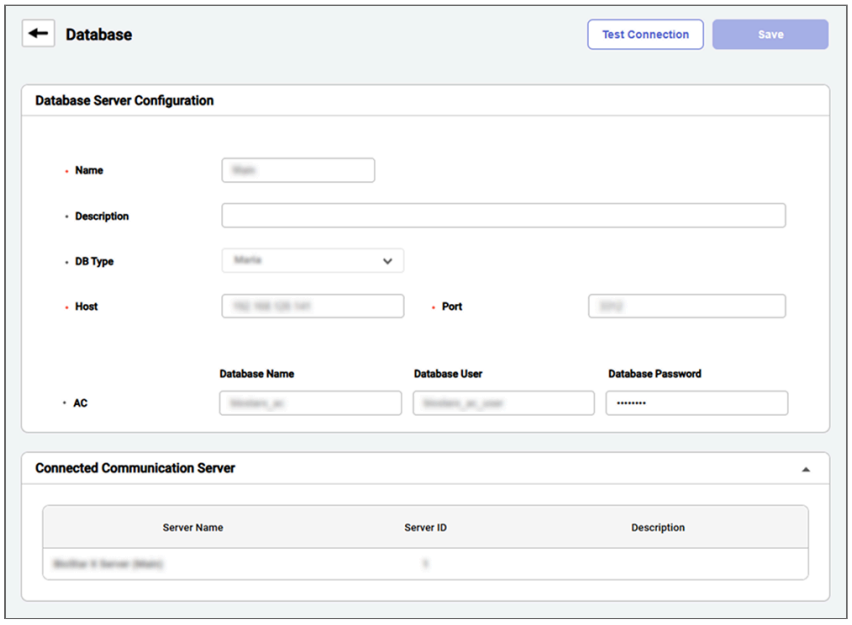
```
select
  concat(
     'CREATE TABLE IF NOT EXISTS <SubDB_AC_Database_Schema>.', table_name,
     ' ENGINE=FEDERATED ',
     'CONNECTION="default/', table_name, '";'
  ) as create_table_sql
from information_schema.TABLES
where TABLE_SCHEMA = '<MainDB_AC_Database_Schema>'
   AND TABLE_TYPE = 'BASE TABLE'
   AND NOT TABLE_NAME REGEXP '^t_lg[0-9]{6}$'
   AND NOT TABLE_NAME REGEXP '^t_almevt[0-9]{6}$'
   AND NOT TABLE_NAME REGEXP '^t_lgalmtrstrc[0-9]{6}$'
ORDER BY TABLE_NAME;
```

알아두기

FederatedX 특성 상 `Table_type`이 'BASE TABLE'으로 설정하는 것을 권장합니다. `VIEW type`도 가능하지만 권장하지는 않습니다.

6 Service Manager 설정

1. **BioStar X Service Manager**를 실행하세요. (시작 → **BioStar X** → **BioStar X Service Manager**)
2. 화면 왼쪽 사이드바에서 **DATABASE** 메뉴를 클릭하세요.
3. 화면 오른쪽 상단의 **+ Add Database** 버튼을 클릭하세요.
4. 데이터베이스 추가 화면에서 각 항목을 입력하세요.



- **Name**: 데이터베이스 이름을 입력하세요.
- **Description**: 데이터베이스 설명을 입력하세요.
- **DB Type**: 데이터베이스 유형을 선택하세요. (Maria, MS SQL)

- **Host**: 데이터베이스 서버의 호스트 이름 또는 IP 주소를 입력하세요.
- **Port**: 데이터베이스 서버의 포트 번호를 입력하세요.
- **AC** / **TA**: AC, TA 데이터베이스의 이름, 사용자, 비밀번호를 입력하세요.

5. 데이터베이스가 정상 연결되었는지 확인하려면 화면 오른쪽 상단의 **Test Connection** 버튼을 클릭하세요.
6. 설정을 저장하려면 화면 오른쪽 상단의 **Save** 버튼을 클릭하세요.

SQL Server

1 메인 데이터베이스 권한 부여

sysadmin 권한을 가진 계정으로 메인 데이터베이스에 아래 권한을 부여하세요.

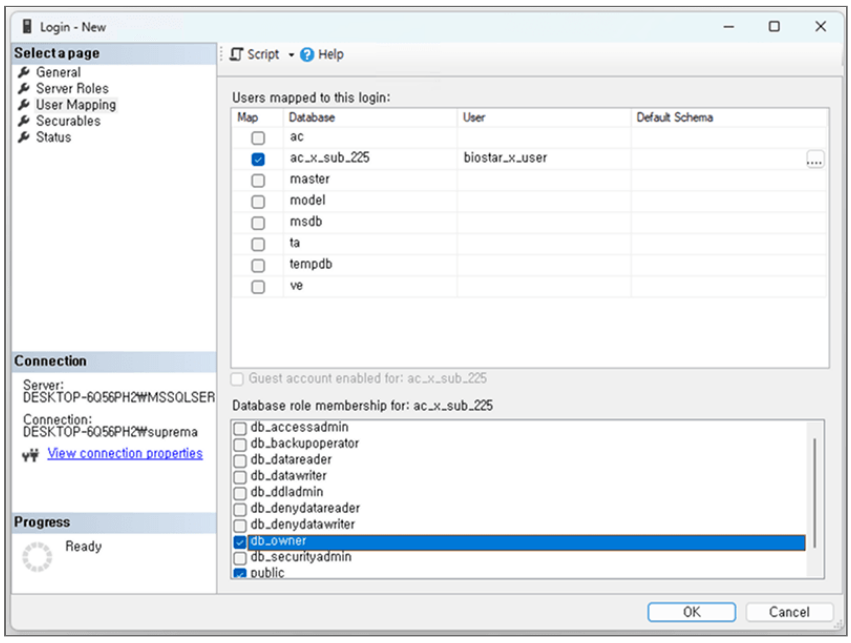
```
GRANT ALTER ANY LINKED SERVER TO [<MAIN DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<MAIN DATABASE AC USER>];
```

Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user];
GRANT ALTER ANY LOGIN TO [biostar_x_user];
```

2 보조 데이터베이스 권한 부여

1. sysadmin 권한을 가진 계정으로 보조 데이터베이스에 테이블 및 사용자에 대한 User Mapping 연결이 필요합니다. 이 때 `db_owner` 역할 추가가 필요합니다.



2. 추가할 데이터베이스에 아래 권한을 부여하세요.

```
GRANT ALTER ANY LINKED SERVER TO [<SUB DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<SUB DATABASE AC USER>];
```

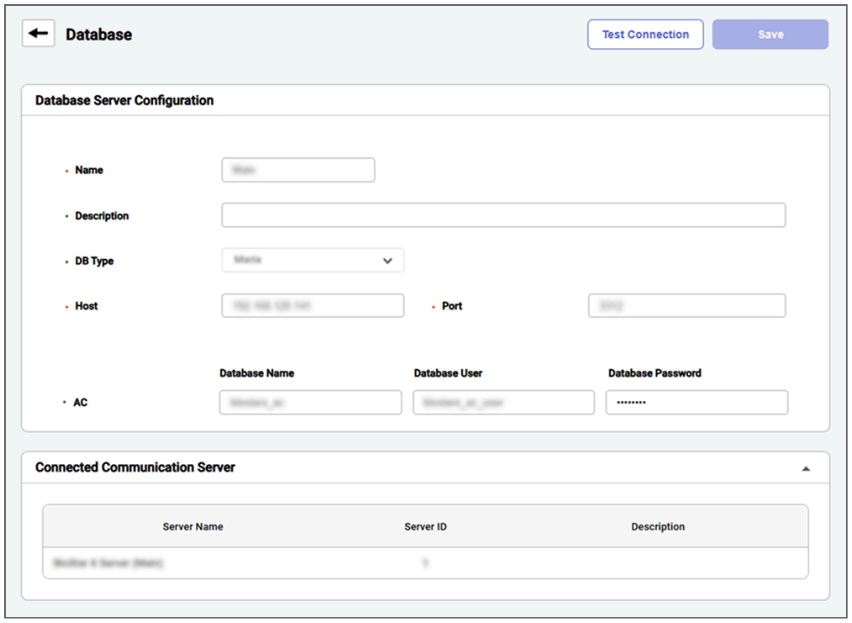
Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user_sub];
GRANT ALTER ANY LOGIN TO [biostar_x_user_sub];
```

3 Service Manager 설정

BioStar X Service Manager를 통해서 보조 데이터베이스를 추가하세요.

1. **BioStar X Service Manager**를 실행하세요. (시작 → **BioStar X** → **BioStar X Service Manager**)
2. 화면 왼쪽 사이드바에서 **DATABASE** 메뉴를 클릭하세요.
3. 화면 오른쪽 상단의 **+ Add Database** 버튼을 클릭하세요.
4. 데이터베이스 추가 화면에서 각 항목을 입력하세요.



- **Name**: 데이터베이스 이름을 입력하세요.
- **Description**: 데이터베이스 설명을 입력하세요.
- **DB Type**: 데이터베이스 유형을 선택하세요. (Maria, MS SQL)
- **Host**: 데이터베이스 서버의 호스트 이름 또는 IP 주소를 입력하세요.
- **Port**: 데이터베이스 서버의 포트 번호를 입력하세요.
- **AC** / **TA**: AC, TA 데이터베이스의 이름, 사용자, 비밀번호를 입력하세요.

5. 데이터베이스가 정상 연결되었는지 확인하려면 화면 오른쪽 상단의 **Test Connection** 버튼을 클릭하세요.
6. 설정을 저장하려면 화면 오른쪽 상단의 **Save** 버튼을 클릭하세요.

알아두기

- 설정을 완료하고, 메인 데이터베이스와 보조 데이터베이스에 각각 Linked Server 설정이 자동 진행됩니다.
- 데이터베이스 정보를 수정할 때에도 Linked Server 설정은 자동 변경됩니다. 메인 데이터베이스를 수정할 때에는 등록되어 있는 모든 보조 데이터베이스에 Linked Server 설정이 변경된 정보로 반영됩니다. 보조 데이터베이스를 수정할 때에는 메인 데이터베이스와 해당 보조 데이터베이스만 변경된 정보로 반영됩니다.

4 Linked Temp Table 쿼리문 생성

메인 데이터베이스에서 아래 쿼리 실행해서 보조 데이터베이스에 생성할 Linked Temp Table 쿼리문을 생성하세요.

```
USE [<AC Schema>];
GO
DECLARE @LinkedServer  sysname = N'default';
DECLARE @SourceSchema  sysname = N'dbo';
DECLARE @TargetSchema  sysname = N'dbo';

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

Example

```
-- 예시
USE [main_ac_x_215];
GO
DECLARE @LinkedServer  sysname = N'default';  -- Linked Server name set in the sub DB
DECLARE @SourceSchema  sysname = N'dbo';      -- Schema to target in the main DB
DECLARE @TargetSchema  sysname = N'dbo';      -- Schema to create synonyms in the sub DB (reflected in the output string)

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'') + '.' + QUOTENAME(t.name,'') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' + QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

5 보조 데이터베이스에 쿼리문 실행

앞서 생성된 `CREATE SYNONYM` 쿼리를 전체 복사하세요. 추가할 보조 데이터베이스 서버로 접속해서 아래와 같이 쿼리를 작성하고 실행하세요. 보조 데이터베이스의 AC 스키마 안에 Synonyms(동의어)에 저장됩니다.

```
use [<Sub DB AC Database>];

IF OBJECT_ID(N'[dbo].[T_ACSGR]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGR];CREATE SYNONYM [dbo].[T_ACSGR] FOR
[default].[main_ac_x_215].[dbo].[T_ACSGR];
IF OBJECT_ID(N'[dbo].[T_ACSGRLVLS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRLVLS];CREATE SYNONYM [dbo].[T_ACSGRLVLS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRLVLS];
IF OBJECT_ID(N'[dbo].[T_ACSGRSENT]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRSENT];CREATE SYNONYM
[dbo].[T_ACSGRSENT] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRSENT];
IF OBJECT_ID(N'[dbo].[T_ACSGRUSS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRUSS];CREATE SYNONYM [dbo].[T_ACSGRUSS]
FOR [default].[main_ac_x_215].[dbo].[T_ACSGRUSS];
...
```

BioStar X 서버 제거 및 보안 인증서 복구하기

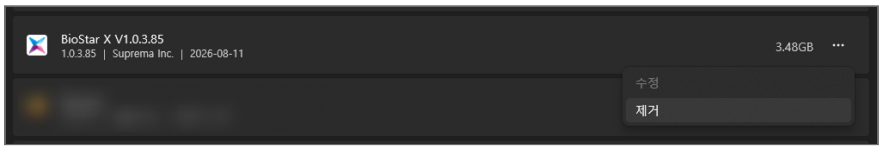
BioStar X 서버를 컴퓨터에서 제거하는 절차를 안내합니다. **장치와 보안 통신** 옵션을 사용 중이 아니라면 인증서 백업 및 복구 절차 없이 제거를 진행할 수 있습니다.

장치와 보안 통신 옵션을 사용 중이라면, **BioStar X**를 제거하기 전에 서버의 보안 인증서 세트(루트 CA/서버 인증서/키)를 반드시 백업해야 합니다. 이 백업은 같은 서버를 다시 설치한 뒤 기존 장치를 재연결할 수 있는 유일한 복구 수단입니다. 시스템에서 제공하는 복원 기능과 달리, 데이터베이스나 설정은 그대로 두고 보안 통신 인증서만 재사용하려고 한다면 백업한 보안 인증서 복구를 참고하세요.

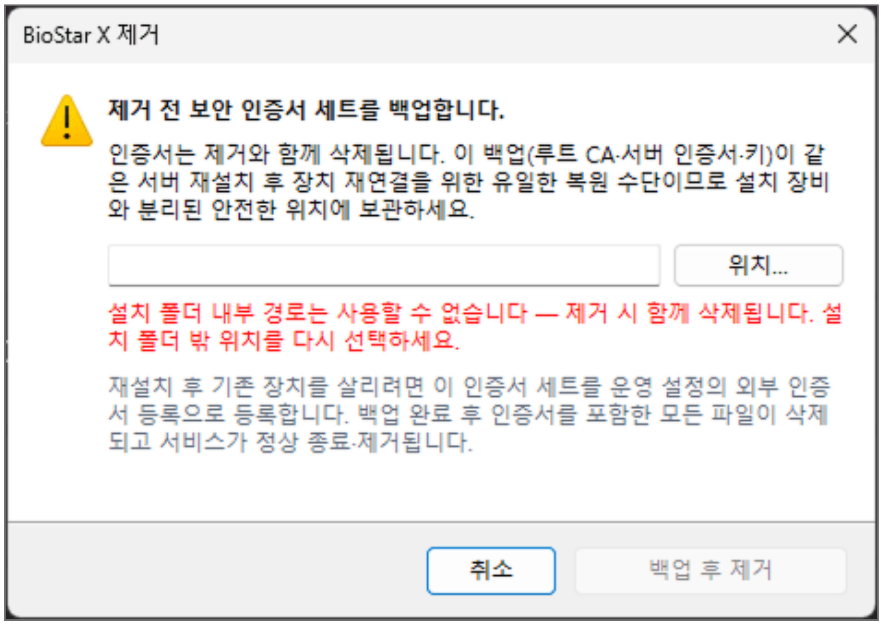
BioStar X 서버 제거

> **주의**
> **BioStar X**를 제거하면 인증서를 포함한 설치 파일이 모두 삭제되며, 컨텐츠(사용자 정보)까지 함께 삭제할 수도 있습니다. 데이터베이스, 설정, 키 등을 보존하려면 제거하기 전에 시스템 백업하기를 참고해 시스템을 먼저 백업하세요.

1. Windows에서 **설정** → **앱** → **설치된 앱**으로 이동하세요.
2. 목록에서 **BioStar X**를 찾아 ••• 버튼을 클릭하고 **제거**를 선택하세요.

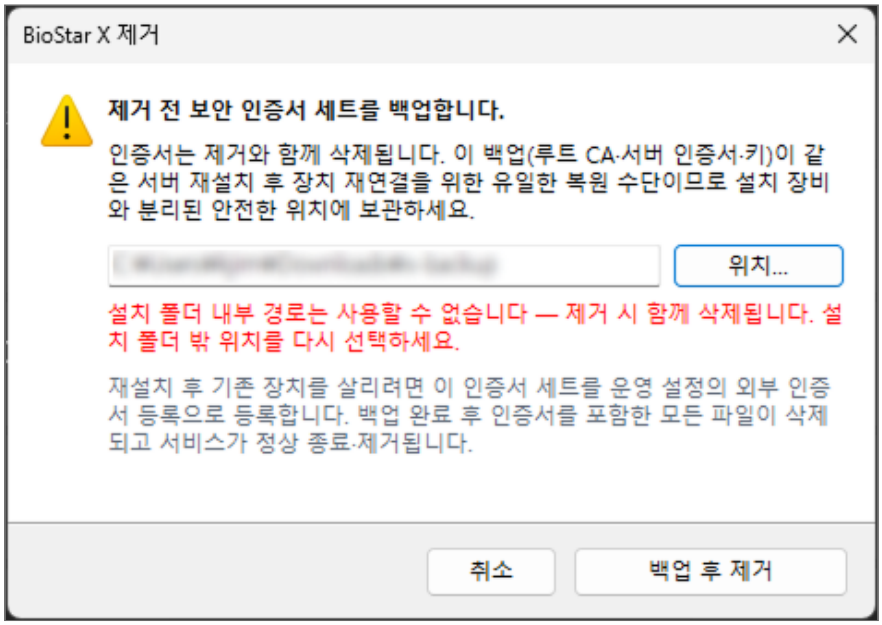


3. **장치와 보안 통신** 옵션을 사용 중이면 인증서 백업 안내 창이 나타납니다. **위치...** 버튼을 클릭하고 백업 경로를 지정하세요. 이 옵션을 사용하지 않는다면 인증서 백업 절차 없이 7단계로 이어집니다.

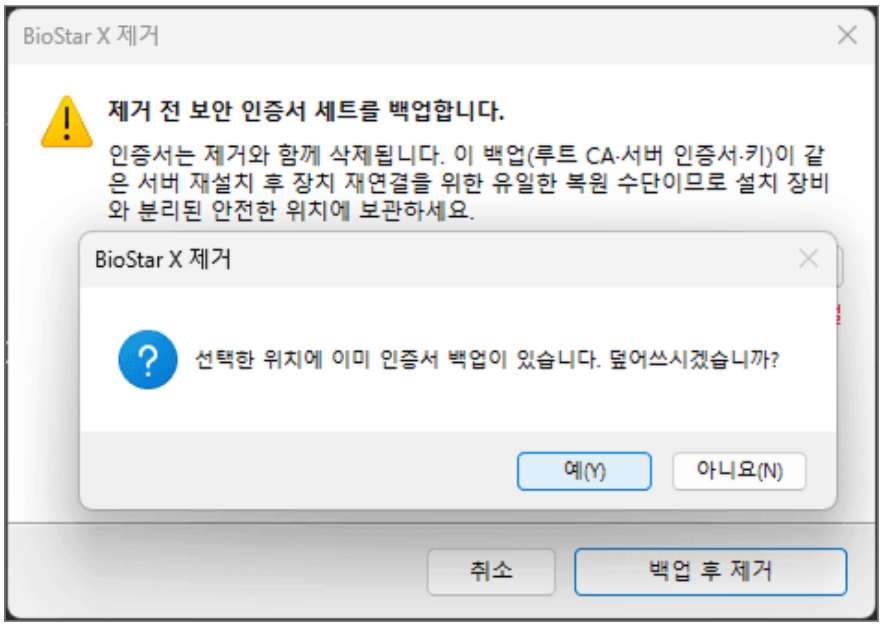


> **주의**
> **BioStar X**가 설치된 경로는 백업 위치로 사용할 수 없습니다. 제거할 때 **BioStar X** 설치 폴더와 함께 삭제되기 때문입니다. 반드시 **BioStar X** 설치 경로가 아닌 경로를 지정하세요.

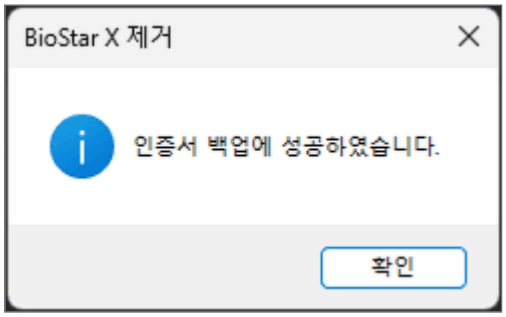
4. 경로를 지정하고 **백업 후 제거** 버튼이 활성화되면 클릭하세요.



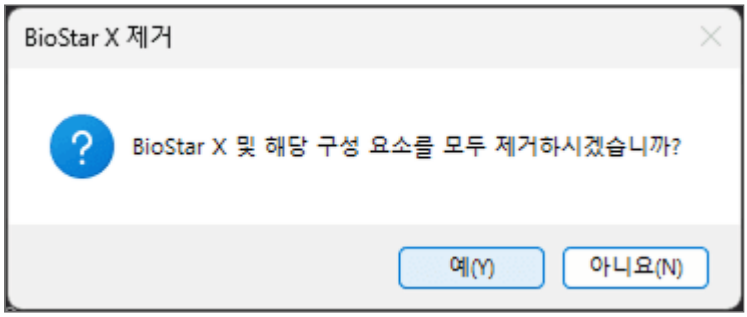
5. 지정한 위치에 이미 인증서 백업 파일이 있으면 덮어쓸지 확인하는 창이 나타납니다. 기존 백업을 덮어쓰려면 **예**를, 다른 경로를 다시 지정하려면 **아니요**를 클릭하세요.



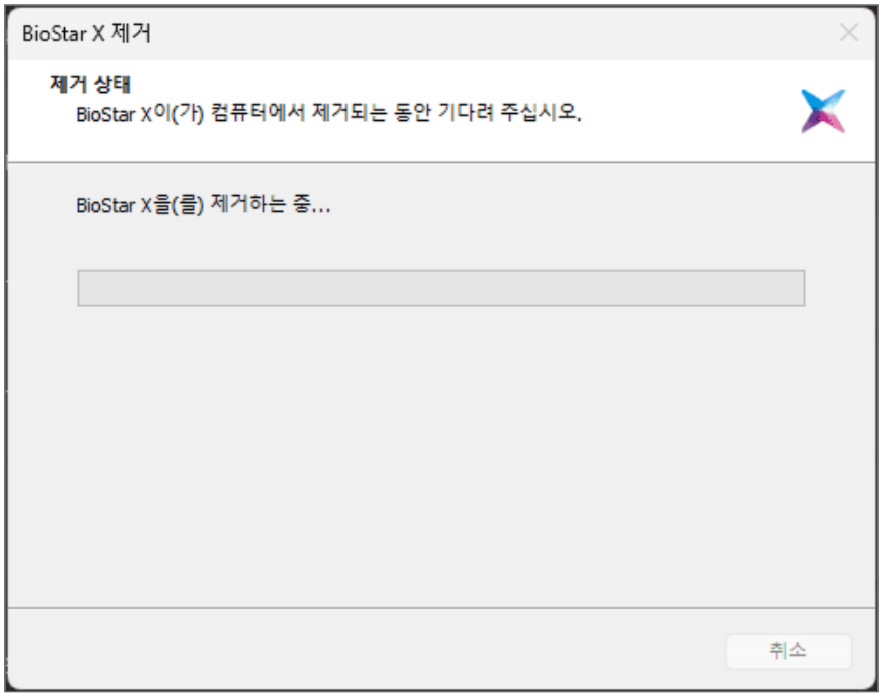
6. 인증서 백업이 완료되면 안내 창이 나타납니다. **확인**을 클릭하세요.



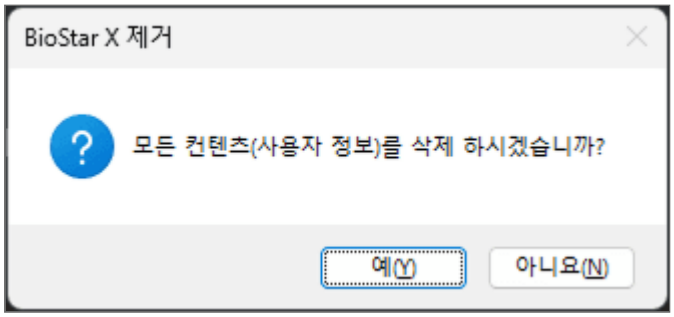
7. **BioStar X** 및 관련 구성 요소를 모두 제거할지 확인하는 창이 나타나면 **예**를 클릭하세요.



8. 제거가 진행되는 동안 기다리세요.

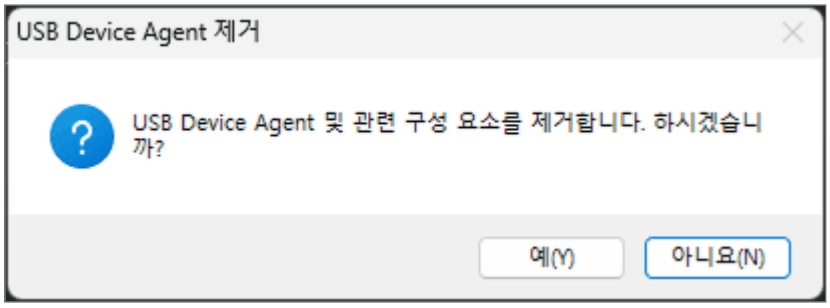


9. 모든 컨텐츠(사용자 정보)를 삭제할지 확인하는 창이 나타납니다. 데이터베이스에 저장된 사용자 정보까지 모두 삭제하려면 **예**를, 남겨두려면 **아니요**를 클릭하세요.



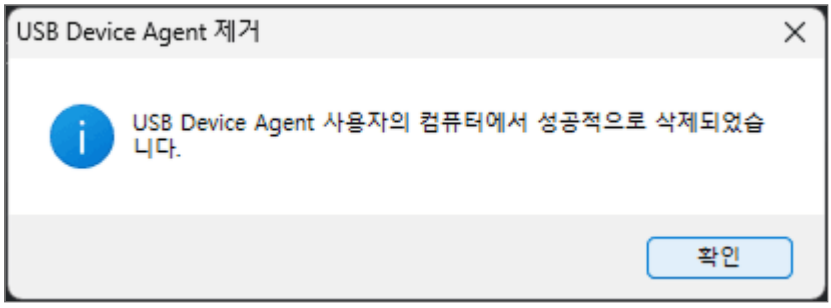
> **주의**
> **예**를 클릭하면 데이터베이스에 저장된 사용자 정보를 포함한 모든 데이터가 삭제되며 복구할 수 없습니다. 데이터를 보존해야 한다면 **아니요**를 클릭하거나, 제거하기 전에 시스템 백업하기를 참고해 시스템을 먼저 백업하세요.

10. **USB Device Agent**가 설치되어 있다면 함께 제거할지 확인하는 창이 나타납니다. **예**를 클릭하세요.

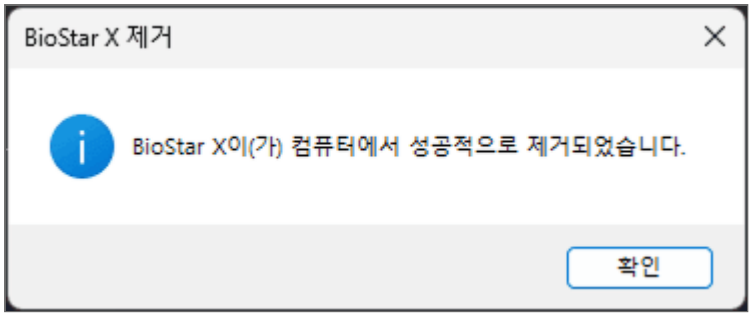


> 사용 중인 구성 요소에 따라 관련 드라이버의 제거 창이 추가로 나타날 수 있습니다. 화면의 안내에 따라 제거를 완료하세요.

11. 구성 요소 제거가 완료되면 안내 창이 나타납니다. **확인**을 클릭하세요.



12. **BioStar X** 제거가 완료되면 안내 창이 나타납니다. **확인**을 클릭하세요.

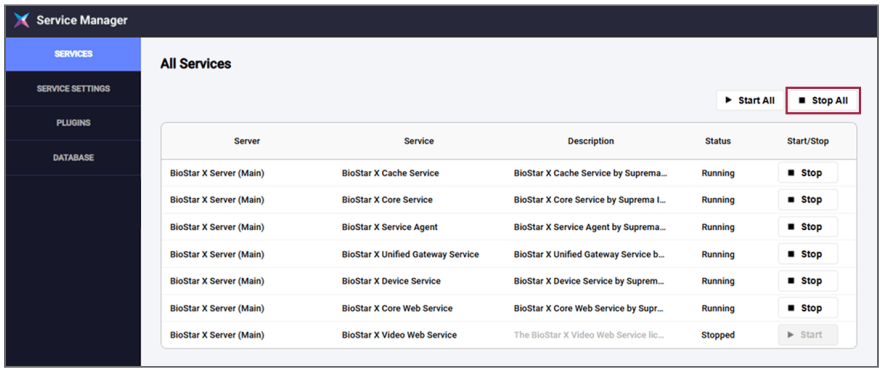


백업한 보안 인증서 복구

장치와 보안 통신 옵션을 사용하던 서버를 재설치한 뒤, 기존 장치를 다시 연결하려면 보안 통신 인증서를 복구해야 합니다. 시스템 복원 도구가 데이터베이스와 설정을 포함한 시스템 전체를 이전 상태로 되돌리는 기능이라면, 이 과정은 시스템 복원 없이 보안 통신 인증서만 재사용할 때 사용하는 방식입니다. 전용 도구 없이 백업해 둔 인증서 파일을 설치 경로에 직접 복구해야 합니다.

> **알아두기**
> 메인 서버와 멀티 커뮤니케이션 서버로 구성된 환경이면 각 서버가 개별적인 보안 통신 인증서를 사용합니다. 인증서 복구 후 멀티 커뮤니케이션 서버 설치 및 추가하면 멀티 커뮤니케이션 서버의 인증서는 자동 복사되므로 별도로 복구하지 않아도 됩니다.

1. **BioStar X**를 새로 설치하세요. 설치 방법은 간편 설치하기 또는 사용자 정의 설치하기를 참고하세요.
2. **BioStar X** 설치를 완료한 후, Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
3. 웹브라우저를 통해 **BioStar X Service Manager** 창이 나타나면 **SERVICES** 메뉴를 클릭하세요.
4. 모든 서비스를 종료하려면 화면 오른쪽 상단의 **Stop All** 버튼을 클릭하세요.



5. 백업해 둔 인증서 파일(루트 CA, 서버 인증서, 키)을 모두 **BioStar X** 설치 경로 하위의 *cert* 폴더에 복사하세요.

   > *예: C:\Program Files\BioStar X\cert*

   > 새로 설치하며 자동 생성된 인증서 파일과 이름이 같으므로, 덮어쓸지 확인하는 창이 나타나면 **예**를 클릭해 기존 파일을 덮어쓰세요.

6. **SERVICES** 메뉴에서 모든 서비스를 다시 시작하려면 **Start All** 버튼을 클릭하세요.

7. 멀티 커뮤니케이션 서버를 사용한다면, 별도 환경에 멀티 커뮤니케이션 서버를 설치하세요. 설치 방법은 멀티 커뮤니케이션 서버 설치하기를 참고하세요.

8. 메인 서버의 **BioStar X Service Manager**에서 멀티 커뮤니케이션 서버를 추가하세요. 추가하는 방법은 멀티 커뮤니케이션 서버 설치하기를 참고하세요.

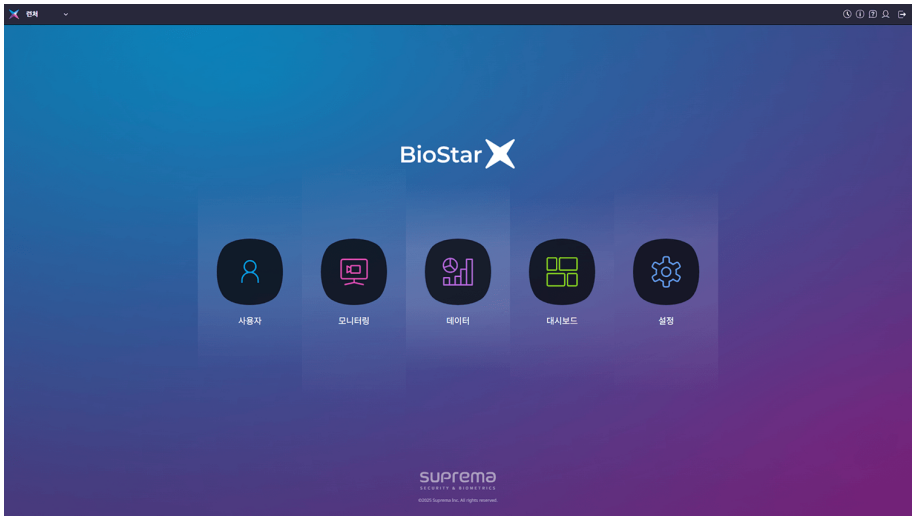
멀티 커뮤니케이션 서버를 추가하면 메인 서버의 *cert* 폴더에 있는 보안 인증서 파일이 멀티 커뮤니케이션 서버로 자동 복사됩니다.

> **주의**
> 인증서를 복구하기 전(4~6단계 이전)에 멀티 커뮤니케이션 서버를 먼저 설치하고 추가했다면, 멀티 커뮤니케이션 서버에는 복구 전의 인증서가 이미 복사된 상태입니다. 이때는 아래 절차에 따라 멀티 커뮤니케이션 서버의 인증서도 별도로 교체하세요.
>
> 1. 멀티 커뮤니케이션 서버를 설치한 환경에서 **BioStar X Service Manager**를 실행하고 모든 서비스를 종료하세요.
> 2. 백업해 둔 인증서 파일을 멀티 커뮤니케이션 서버 설치 경로 하위의 *cert* 폴더에 동일하게 복사하세요.
>
>   > *예: C:\Program Files\BioStar X Communications Server\cert*
>
> 3. 메인 서버와 멀티 커뮤니케이션 서버 양쪽에서 **BioStar X Service Manager**를 통해 모든 서비스를 다시 시작하세요.

> **알아두기**
>
> - **BioStar X Service Manager** 사용 방법에 대한 자세한 내용은 서버 시작 및 종료를 참고하세요.
> - **장치와 보안 통신** 옵션에 대한 자세한 내용은 시스템 보안 강화하기를 참고하세요.
> - 멀티 커뮤니케이션 서버를 설치하고 연결하려면 멀티 커뮤니케이션 서버 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

런처

런처 페이지는 로그인 후 처음 접할 수 있는 **BioStar X**의 시작 페이지로, 사용자가 **BioStar X**의 주요 기능에 접근할 수 있는 중심 허브 역할을 합니다. 이 페이지는 사용자가 **BioStar X**의 모든 기능을 쉽게 탐색하고 사용할 수 있도록 설계되었습니다. 런처 페이지의 UI 구성 요소를 살펴보면 다음과 같습니다.



런처 페이지에서는 **사용자**, **모니터링**, **데이터**, **대시보드**, **설정** 페이지로 이동할 수 있는 링크를 제공합니다.

- **사용자**: 사용자 그룹 관리, 사용자 관리, 사용자 템플릿 관리, 출입 권한별 사용자 확인 등 다양한 기능을 통해 사용자를 효율적으로 관리하고, 권한을 통해 보안을 강화할 수 있습니다. 자세한 내용은 사용자를 참고하세요.
- **모니터링**: 출입문, 장치, 비디오, 이벤트를 다양한 방식으로 모니터링합니다. 관련한 기능들을 제어하고 실시간 영상을 통해 모니터링할 수 있습니다. 자세한 내용은 모니터링을 참고하세요.
- **데이터**: 사용자 정보나 원하는 조건의 이벤트를 조회할 수 있고, 보고서를 일정 주기에 맞춰 생성할 수 있습니다. 자세한 내용은 데이터를 참고하세요.
- **대시보드**: **BioStar X**에서 제공하는 다양한 데이터를 통해 사용자가 선택한 데이터 기반의 위젯을 추가하고, 배치하여 원하는 대시보드를 구성할 수 있습니다. 자세한 내용은 대시보드를 참고하세요.
- **설정**: 장치 및 출입 통제, 사용자에 따른 권한, 언어, 시간 등 다양한 설정을 통해 사용자의 환경에 최적화된 **BioStar X**를 구성할 수 있습니다. 자세한 내용은 설정을 참고하세요.

알아두기

- 화면 상단 헤더 영역에 대한 자세한 내용은 공통 UI 이해하기를 참고하세요.
- 화면 하단에는 플러그인 추가를 통해 설치된 기능을 이용할 수 있습니다. 플러그인 기능을 사용하려면 플러그인 라이선스가 필요합니다.
  - 플러그인 사용에 대한 자세한 내용은 플러그인을 참고하세요.
  - 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

사용자

BioStar X의 핵심 기능 중 하나인 **사용자** 페이지에서 활용할 수 있는 다양한 기능에 대해 안내합니다. 이 페이지에서는 사용자 그룹 관리, 사용자 관리, 사용자 템플릿 관리, 출입 권한별 사용자 확인 등 다양한 기능을 통해 사용자를 효율적으로 관리하고, 권한을 통해 보안을 강화하는 방법을 소개합니다. 각 기능을 통해 **BioStar X**를 더욱 효과적으로 활용해 보세요.

런처 페이지에서 **사용자**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **사용자**를 선택하세요.

사용자 그룹 관리하기

사용자 그룹은 공통 속성과 권한을 공유할 수 있습니다. 사용자가 그룹의 멤버가 되면 해당 그룹의 모든 속성을 자동으로 상속받을 수 있습니다. 사용자는 하나의 사용자 그룹에만 속할 수 있습니다.

- 개별 사용자마다 출입 권한을 설정하는 대신, 부서별 또는 역할별 사용자 그룹을 만들어 동일한 권한을 한 번에 적용할 수 있습니다.
- 그룹의 출입 권한을 수정하면 해당 그룹에 속한 모든 사용자에게 자동 적용되므로 관리자의 업무 부담을 줄일 수 있습니다. 조직 변경이나 신규 프로젝트 발생 시 빠르게 권한을 조정할 수 있습니다.
- 그룹별 권한 설정을 통해 불필요한 출입을 방지하고 보안성을 높일 수 있습니다.
- 특정 그룹의 출입 기록을 별도로 분석할 수 있어 보안 감사 및 로그 관리가 쉬워집니다.
- 사용자 그룹은 출입 등급과 연동하여 출입 제한 시간, 출입 제한 구역 등 세부 정책을 적용할 수 있습니다.

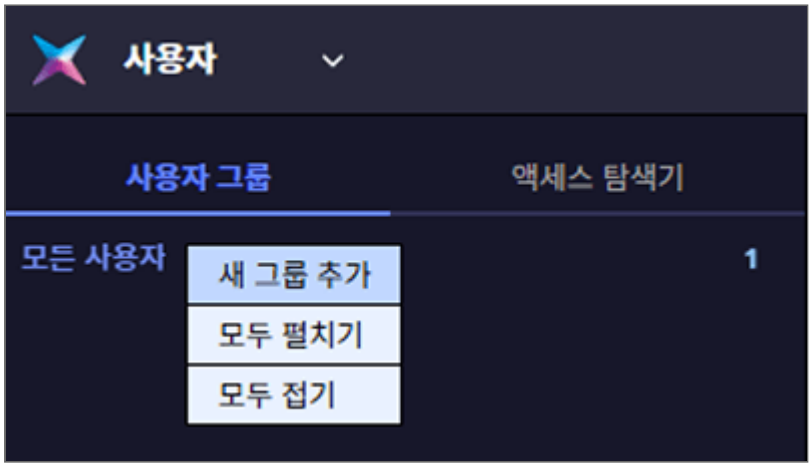
그룹 추가

여러 명의 사용자를 효율적으로 관리하기 위해 그룹을 생성하세요. 사용자가 속한 조직 등으로 이름을 등록하면 편리하게 관리할 수 있습니다.

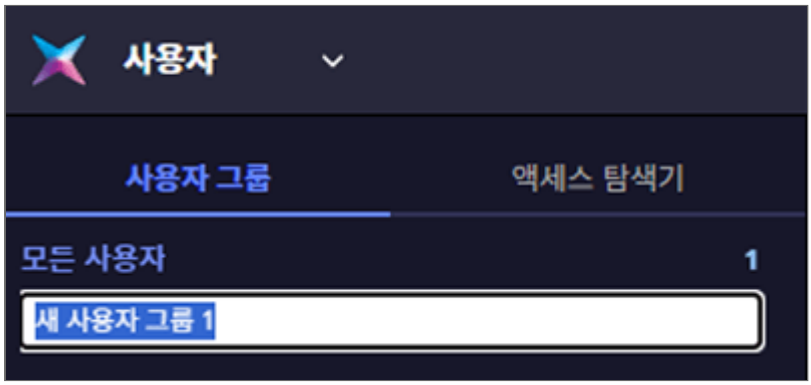
> **알아두기**
>
> - 그룹 이름은 사용자가 속한 조직 또는 부서 이름으로 등록하면 관리가 편리합니다.
> - 그룹의 하위 그룹을 최대 8단계까지 순차적으로 생성할 수 있습니다.
> - 사용자 그룹 이름은 최대 48자까지 입력할 수 있습니다.
> - 사용자 그룹 목록에서 그룹을 선택하면 해당 그룹에 속한 사용자만 사용자 목록에 표시할 수 있습니다.

최상위 그룹 생성

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 왼쪽 사이드바의 **사용자 그룹** 탭에서 **모든 사용자**을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



3. 팝업 메뉴에서 **새 그룹 추가**를 클릭하세요.
4. 그룹이 생성되면 원하는 그룹 이름을 입력하세요.



하위 그룹 생성

1. 화면 왼쪽 사이드바의 **사용자 그룹** 탭에서 상위 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



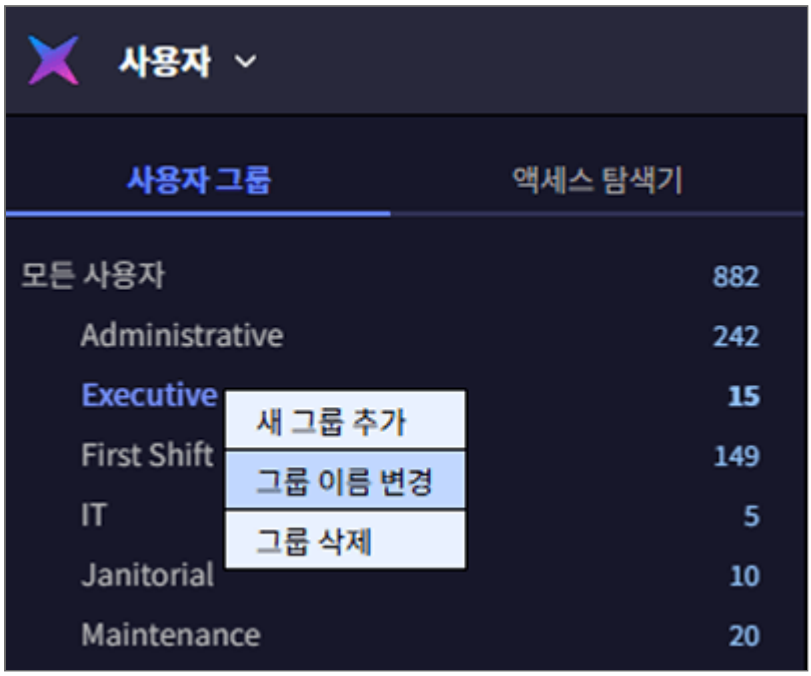
2. 팝업 메뉴에서 **새 그룹 추가**를 클릭하세요.
3. 그룹이 생성되면 원하는 그룹 이름을 입력하세요.

> **알아두기**
>
> - 하위 그룹을 생성할 때는 상위 그룹을 선택해야 하며, 최대 8단계까지 생성할 수 있습니다.
> - 그룹을 다른 그룹으로 드래그하여 이동시키면 대상 그룹의 하위 그룹으로 설정할 수 있습니다. **모든 사용자**로 그룹을 이동시키면 최상위 그룹으로 설정할 수 있습니다.

그룹 이름 변경

사용자가 속한 그룹의 이름을 변경할 수 있습니다. 조직 또는 부서의 이름이 변경되었을 때 그룹 이름도 같이 변경하는 것을 권장합니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 왼쪽 사이드바의 **사용자 그룹** 목록에서 이름을 변경할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



3. 팝업 메뉴에서 **그룹 이름 변경**을 클릭하세요.
4. 원하는 그룹 이름으로 변경하세요.

사용자 그룹 목록에서 변경 사항을 확인하세요.

> **알아두기**
>
> 사용자 그룹 이름은 최대 48자까지 입력할 수 있습니다.

그룹 삭제

사용자가 속한 그룹을 삭제할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 왼쪽 사이드바의 **사용자 그룹** 목록에서 삭제할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.

3. 팝업 메뉴에서 **그룹 삭제**를 클릭하세요.

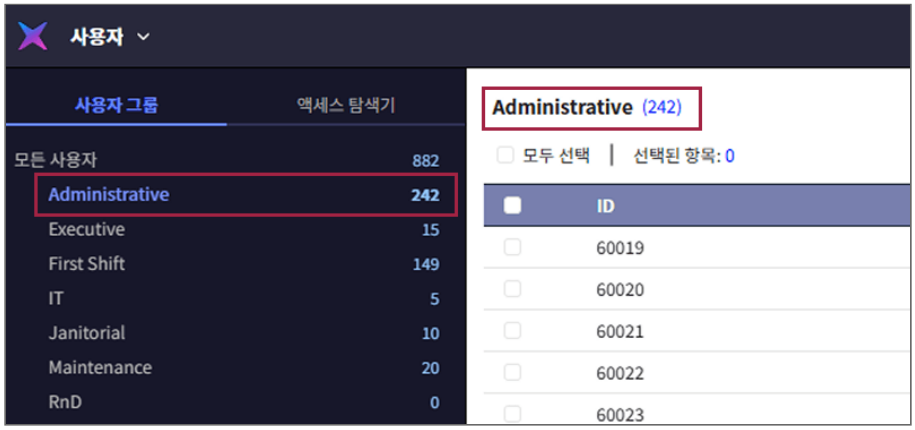


4. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.

사용자 그룹 목록에서 선택한 그룹이 삭제된 것을 확인하세요.

그룹별 사용자 확인하기

사용자 그룹에 속한 사용자를 확인할 수 있습니다. **사용자** 페이지에서 화면 왼쪽 사이드바에서 원하는 사용자 그룹을 선택하세요. 선택한 사용자 그룹의 사용자가 목록에 표시됩니다.

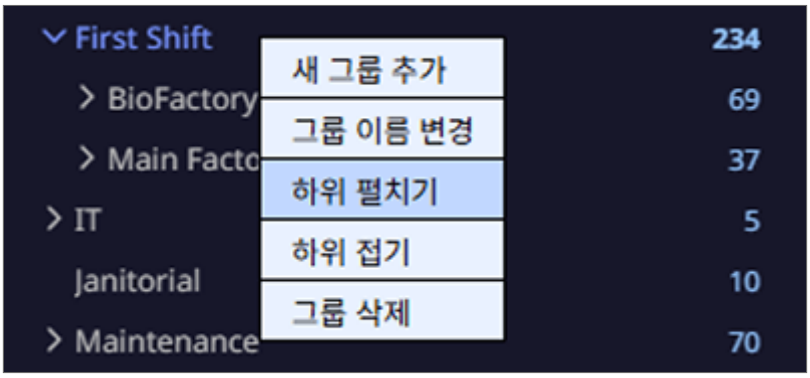


그룹 목록 확장/축소

사용자 그룹 목록을 확장하거나 축소할 수 있습니다. **사용자 그룹** 탭에서 **모든 사용자**를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **모두 펼치기** 또는 **모두 접기**를 클릭하세요.



그룹 내 하위 그룹이 있다면 하위 그룹을 확장하거나 축소할 수 있습니다. 상위 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **하위 펼치기** 또는 **하위 접기**를 클릭하세요.



사용자 등록하기

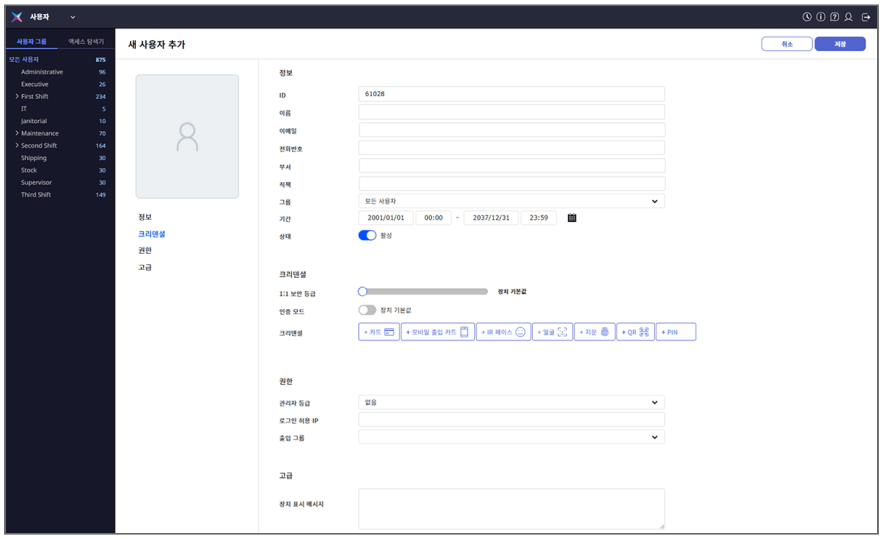
새로운 사용자를 등록하는 방법을 안내합니다. 사용자의 사진 및 이름, 이메일, 전화번호 등과 같은 정보를 입력하고 사용자의 출입 권한 및 생체 정보를 설정할 수 있습니다.

사용자 정보 입력 및 출입 권한 설정, 크리덴셜 등록순으로 진행합니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. **사용자** 페이지의 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요.



3. **새 사용자 추가** 화면에서 사용자 정보를 입력하세요.



4. **정보** 섹션에서 사용자의 기본 정보를 입력하세요.
5. **크리덴셜** 섹션에서 사용자의 생체 인식 정보를 등록하세요.
6. **권한** 섹션에서 사용자의 **BioStar X** 운영 권한과 출입 권한을 설정하세요.
7. **고급** 섹션에서 사용자가 출입 시 장치에 표시할 메시지를 입력할 수 있습니다.
8. 모든 정보를 입력하고 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

사용자 목록에서 등록한 사용자를 확인할 수 있습니다. 섹션별 입력 및 설정에 대한 자세한 내용은 아래를 참고하세요.

정보 섹션에서 사용자의 기본 정보를 입력하세요. 각 항목에 대한 자세한 내용을 확인할 수 있습니다.
크리덴셜 섹션에서 사용자 크리덴셜을 등록하고 출입 인증 방식을 설정하세요.
권한 섹션에서 사용자의 출입 권한 설정 방법을 확인하세요.
고급 섹션에서 사용자 출입 시 장치에 표시할 메시지를 설정하거나 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다.
여권 스캔으로 사용자를 등록하거나 수정하는 방법을 확인하세요.

알아두기

- 출입 권한 및 생체 인식 정보는 선택 사항입니다. 기본 정보를 입력하고 저장한 후에 수정하거나 추가할 수 있습니다.
- 사용자 정보를 카드 템플릿을 통해 카드로 인쇄하려면 화면 오른쪽 상단의 **카드 인쇄** 버튼을 클릭하세요. 자세한 내용은 카드 인쇄하기를 참고하세요.
- 사용자 등록을 취소하려면 화면 오른쪽 상단의 **취소** 버튼을 클릭하세요.

사용자 기본 정보 입력하기

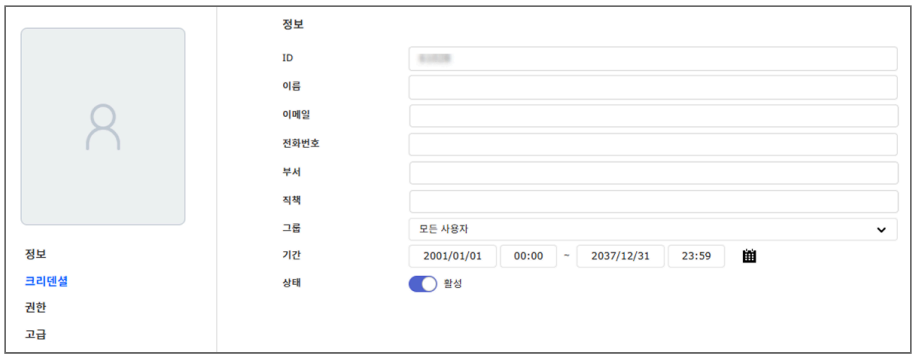
사용자의 기본 정보 입력에 대한 자세한 내용을 안내합니다. 입력한 사용자 정보는 검색 및 관리에 사용됩니다. 사용자 정보를 명확히 관리하면 조직의 보안 정책이나 개인정보 보호 정책을 준수하는데 도움이 됩니다.

- 이름, 부서, 직책, 그룹 등 기본 정보를 체계적으로 입력하면 사용자를 쉽게 검색 또는 분류, 관리할 수 있습니다.
- 사용자의 소속, 직책, 그룹 정보에 따라 출입 권한을 세분화하여 설정할 수 있습니다.
- 사용자별로 활동 이력, 출입 기록 등을 정확하게 추적할 수 있어 보안 및 감사에 유리합니다.

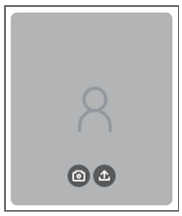
런처 → **사용자** 페이지로 이동해, 아래 두 가지 방식으로 사용자 정보를 입력할 수 있습니다.

- **새로운 사용자**: 화면 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요. **새 사용자** 창이 나타납니다.
- **기존 사용자**: 사용자 목록에서 사용자를 더블 클릭하세요. 또는, 사용자를 클릭하면 화면 오른쪽에 표시되는 프리뷰 화면에서 **자세히 보기** 버튼을 클릭하세요. 사용자 정보를 수정할 수 있는 창이 나타납니다.

정보 섹션에서 설정할 수 있는 항목은 아래와 같습니다. 각 항목에 대한 설명을 참고하여 사용자 정보를 입력하세요.



- **사진**: 사용자의 사진을 등록하세요. 웹캠으로 사진을 촬영하거나 PC에서 사진을 업로드할 수 있습니다. 프로필에 마우스를 오버하면 사용할 수 있는 도구가 표시됩니다.



  - : PC에 웹캠이 연결되어 있다면 버튼을 클릭해 사진을 촬영하고 등록할 수 있습니다.
  - : PC에 저장된 이미지 파일을 업로드할 수 있습니다.

  자세한 내용은 얼굴 등록하기를 참고하세요.

- **ID**: 사용자에게 부여할 고유 ID를 입력하세요.
- **이름**: 사용자의 이름을 입력하세요.
- **이메일**: 이메일을 입력하세요.
- **전화번호**: 전화번호를 입력하세요.
- **부서**: 사용자가 소속된 부서를 입력하세요.
- **직책**: 사용자의 직책을 입력하세요.
- **그룹**: 사용자의 그룹을 선택하세요. 사용자 그룹 추가 및 관리에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.
- **기간**: 사용자 계정을 사용할 기간을 설정하세요. 날짜 및 시간 영역을 클릭해 직접 입력하거나 버튼을 클릭해 원하는 날짜와 시간을 선택할 수 있습니다.

- **상태**: 사용자 계정을 사용하지 않도록 임시로 설정할 수 있습니다.

입력한 기본 정보를 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

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

- **ID**는 **설정** → **시스템** → **서버** 메뉴의 **사용자 ID 종류** 옵션에 따라 설정할 수 있는 값이 다를 수 있습니다. 자세한 내용은 서버 상세 설정하기를 참고하세요.
  - **숫자**: 1 ~ 4294967294 숫자로 입력할 수 있습니다.
  - **영숫자**: 영문자와 숫자를 조합하여 입력할 수 있습니다.
- 모바일 출입 카드에 사용자의 사진, 부서, 직책을 표시하려면, 반드시 사진을 추가하고 부서와 직책을 입력하세요.
- 직책 및 부서명은 특수 기호 `공백` `_`를 포함해 최대 64자까지 입력할 수 있습니다.
- 모바일 출입 카드를 사용한다면, 발송 방법에 따라 이메일 전송 시 사용자의 이메일을 반드시 입력하세요.
- 얼굴 모바일 등록, BioStar X QR을 사용하려면 반드시 사용자의 이메일 주소를 입력하세요.

팁

BioStar X에서 제공하는 기본 입력 필드 외에 추가 사용자 정보를 입력하려면 **사용자 정의 필드** 기능을 사용해 맞춤형 필드를 추가할 수 있습니다. **사용자 정의 필드**는 조직의 요구 사항에 맞게 사용자 정보를 확장할 수 있는 유용한 기능입니다.

사용자 정의 필드 추가 방법에 대한 자세한 내용은 서버 상세 설정하기를 참고하세요.

다음 단계

크리덴셜 섹션에서 사용자 크리덴셜을 등록하고 출입 인증 방식을 설정하세요.
권한 섹션에서 사용자의 출입 권한 설정 방법을 확인하세요.
고급 섹션에서 사용자 출입 시 장치에 표시할 메시지를 설정하거나 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다.
사용자 정보를 수정하는 방법을 확인하세요.

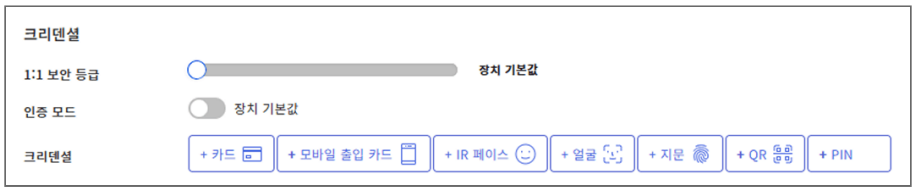
사용자 크리덴셜 등록하기

사용자의 크리덴셜을 등록하는 방법을 안내합니다. 사용자의 지문 및 얼굴, 카드 정보, 비밀번호 등을 크리덴셜로 등록할 수 있습니다. 크리덴셜은 사용자를 새로 등록하거나 수정할 때 추가 또는 변경할 수 있습니다.

런처 → **사용자** 페이지로 이동해, 아래 두 가지 방식으로 크리덴셜을 등록하거나 추가, 변경할 수 있습니다.

- **새로운 사용자**: 화면 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요. **새 사용자** 창이 나타납니다.
- **기존 사용자**: 사용자 목록에서 사용자를 더블 클릭하세요. 또는, 사용자를 클릭하면 화면 오른쪽에 표시되는 프리뷰 화면에서 **자세히 보기** 버튼을 클릭하세요. 사용자 정보를 수정할 수 있는 창이 나타납니다.

크리덴셜 섹션에서 설정할 수 있는 항목은 아래와 같습니다. 각 항목에 대한 설명을 참고하여 적절한 사용자 권한을 설정하세요.



크리덴셜을 등록하고 **1:1 보안 등급** 항목에서 적절한 보안 등급을 설정하세요. 보안 등급이 높을수록 인증률이 낮거나 본인 거부율(FRR)이 높을 수 있습니다.

> **크리덴셜(Credential)**: 사용자의 신원을 확인하기 위한 데이터입니다. 일반적으로 디지털 서명, 스마트카드, 바이오 정보, 사용자 이름과 비밀번호 등이 있습니다.

> **알아두기**
>
> - 모바일 출입 카드는 에어팝 포털과 연동해야 사용할 수 있습니다. 에어팝 포털 연동 및 모바일 출입 카드 사용에 대한 자세한 내용은 모바일 출입 카드 관리하기를 참고하세요.

크리덴셜 등록하기

사용자의 크리덴셜을 등록하는 방법은 아래와 같습니다. 크리덴셜은 지문, 얼굴, 카드, 비밀번호 등 다양한 형태로 등록할 수 있습니다.

다음 단계

권한 섹션에서 사용자의 출입 권한 설정 방법을 확인하세요.
고급 섹션에서 사용자 출입 시 장치에 표시할 메시지를 설정하거나 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다.
사용자 정보를 수정하는 방법을 확인하세요.

보안 등급 설정하기

장치에서 설정한 바이오메트릭 1:N 보안 등급과 상관없이 사용자에게 별도의 보안 등급을 부여할 수 있습니다. 장치의 1:N 보안 등급을 높게

설정해 자주 인증에 실패하는 사용자가 있다면, **1:1 보안 등급**을 낮게 설정하여 인증 실패를 완화할 수 있습니다.



1:1 보안 등급 항목에서 원하는 수준을 설정하세요. 설정할 수 있는 값은 아래를 참고하세요.

- **장치 기본값**
- **가장 낮음**
- **낮음**
- **보통**
- **높음**
- **가장 높음**

설정을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - **크리덴셜** 섹션의 **개인 인증 모드** 항목을 **바이오메트릭**으로 설정했다면, 입력된 사용자를 알 수 없기 때문에 1:1 보안 등급을 적용할 수 없으며, 사용자 특정이 가능한 카드 또는 ID를 포함한 인증 모드를 설정했을 때만 1:1 보안 등급을 적용할 수 있습니다. **개인 인증 모드**에 대한 자세한 내용은 인증 모드 설정하기를 참고하세요.
> - 적절한 보안 등급을 설정하세요. 보안 등급이 높을수록 지문 인증률이 낮거나 본인 거부율(FRR)이 높을 수 있습니다.

인증 모드 설정하기

사용자별로 인증 방식을 유연하게 설정할 수 있습니다. 장치에서 설정한 기본 인증 방식을 사용하거나, 각 사용자에게 맞는 개별 인증 모드를 지정할 수 있습니다. 또한 얼굴과 지문을 모두 포함한 확장 인증 모드를 통해 보안 수준을 높일 수 있습니다.

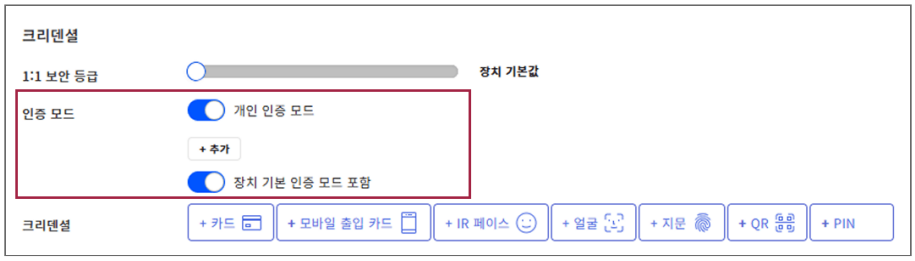
장치 기본값

인증 모드 옵션을 **장치 기본값**으로 설정하면 장치에서 설정한 방식에 따라 인증할 수 있습니다.



개인 인증 모드

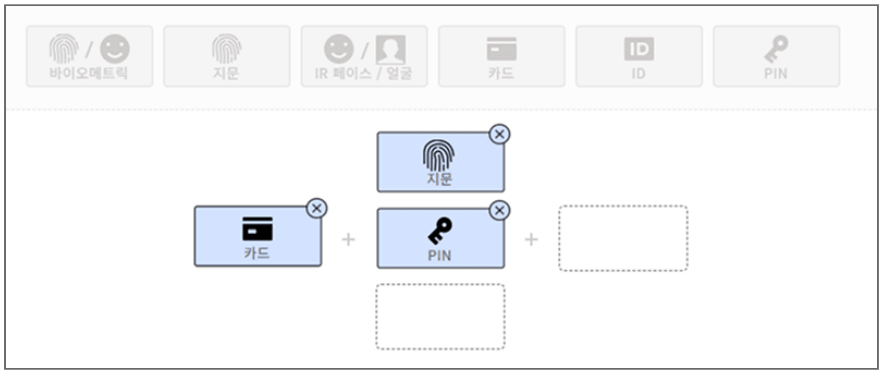
인증 모드 옵션을 **개인 인증 모드**로 설정하면 사용자마다 인증 방식을 다르게 설정할 수 있습니다.



+ 추가 버튼을 클릭하면 **인증모드 추가** 창이 나타납니다. 원하는 인증 방식을 설정하세요.



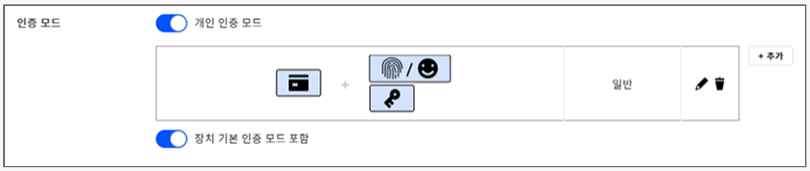
- **확장 인증 모드**: 확장 인증 모드 사용 여부를 설정하세요. 확장 인증 모드를 사용하면 얼굴과 지문을 모두 포함하여 인증 모드를 조합할 수 있습니다.
- **인증 모드**: 사용할 인증 모드를 드래그 앤 드랍으로 설정하세요.



설정한 인증 모드를 등록하려면 **확인** 버튼을 클릭하세요.

알아두기

- **확장 인증 모드** 옵션은 BioStation 3 Max, BioEntry W3, BioStation 3, FaceStation F2 모델에서 지원합니다.
- **장치 기본 인증 모드 포함**으로 설정하면 장치에서 설정된 인증 모드와 **BioStar X**에서 설정한 개인 인증 모드를 모두 사용할 수 있습니다.



- **장치 기본 인증 모드 미포함**으로 설정하면 **BioStar X**에서 설정한 개인 인증 모드만 사용할 수 있습니다.

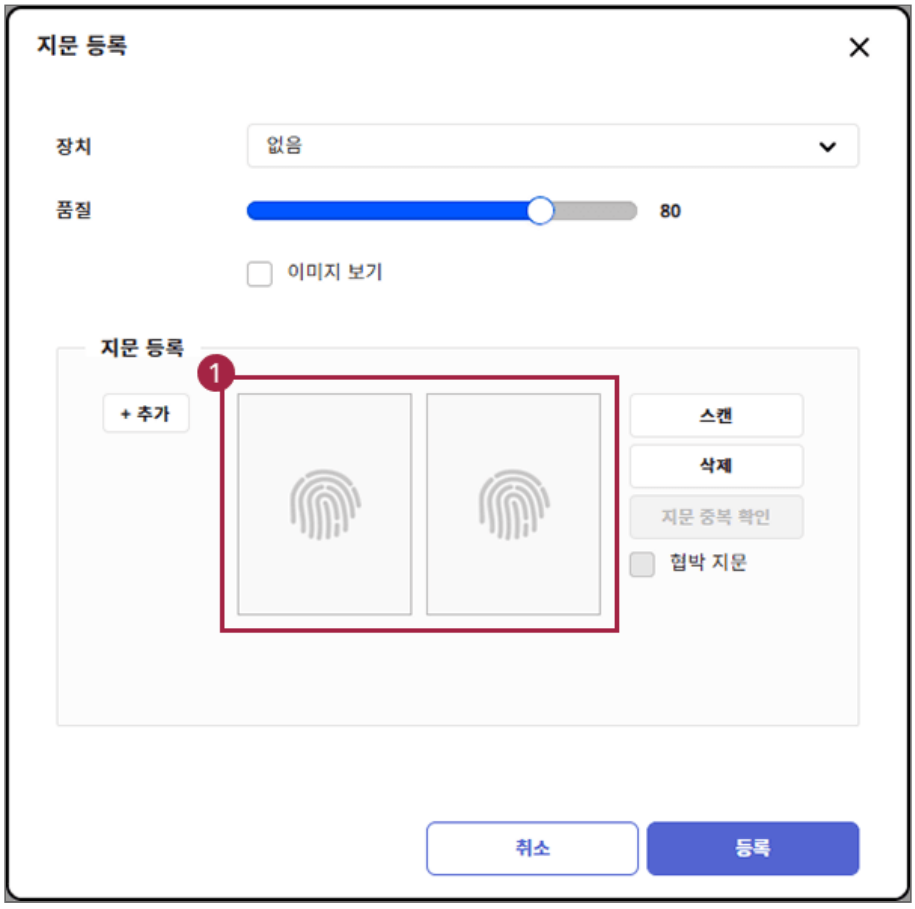
지문 등록하기

출입을 위한 인증 수단으로 사용자의 지문을 등록해 사용할 수 있습니다. 지문 인증을 지원하는 장치를 통해 사용자의 지문 정보를 등록하세요. 지문은 지문 스캐너가 설치된 장치에서 스캔할 수 있습니다.

지문을 등록하기 전에…

- 사용자의 지문이 깨끗하고 물기가 없는지 확인하세요.
- 상처가 있거나 지문이 희미한 손가락은 등록하지 마세요.

크리덴셜 섹션에서 **+ 지문** 버튼을 클릭하세요. **지문 등록** 창이 나타나면 각 항목을 설정하고 **등록** 버튼을 클릭하세요.



- **장치**: 지문을 등록할 장치를 선택하세요.

- **품질**: 지문 등록 품질을 조절할 수 있습니다. 설정한 품질 수준에 미치지 않으면 지문 정보를 등록할 수 없습니다.
- **이미지 보기**: 지문을 스캔했을 때 원본 이미지를 1 영역에서 확인할 수 있습니다.
- **+ 추가**: 지문을 추가하려면 버튼을 클릭하세요. 지문은 최대 10개까지 등록할 수 있습니다.
- **스캔**: 추가한 지문 번호를 선택하고 버튼을 클릭하세요. 지문 스캐너나 장치 센서에 손가락을 대고 지문을 스캔하세요.



- **삭제**: 등록한 지문을 삭제할 수 있습니다. 삭제할 지문 번호를 선택하고 버튼을 클릭하세요.
- **지문 중복 확인**: 이미 등록한 지문인지 확인할 수 있습니다.
- **협박 지문**: 협박 지문으로 등록하려면 이 옵션을 선택하고 지문을 스캔하세요. 누군가에게 협박을 당하거나 강제로 출입문을 열어야 할 때, 해당 지문을 사용해 알림을 보낼 수 있습니다.

알아두기

- 일상 출입을 위해 사용하는 지문을 협박 지문으로 사용하지 마세요.
- **이미지 보기** 옵션을 활성화할 때, 지문 이미지를 확인할 수 있지만 **BioStar X** 서버에 저장하지 않습니다.
- 지문 인증률이 낮다면 지문 정보를 삭제하고 새로운 지문 정보를 등록하세요.
- 좋은 품질의 지문 정보를 얻으려면 지문 인식 센서 표면을 모두 덮을 수 있도록 손가락을 대세요. 검지나 중지의 지문을 등록하세요.



IR 페이스 등록하기

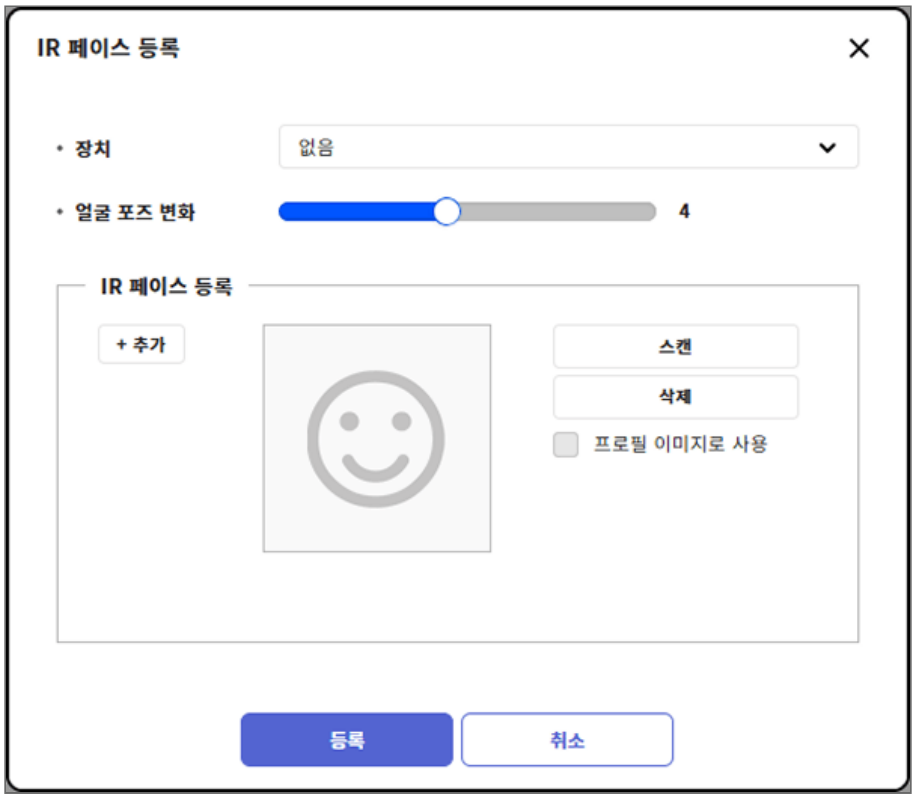
출입을 위한 인증 수단으로 사용자의 얼굴을 등록해 사용할 수 있습니다. IR 페이스 등록은 사용자의 얼굴을 적외선 카메라로 촬영한 인증 수단입니다.

IR 페이스 등록 시 주의 사항

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

장치로 등록

크리덴셜 섹션에서 **+ IR 페이스** 버튼을 클릭하세요. **IR 페이스 등록** 창이 나타나면 각 항목을 설정하고 **등록** 버튼을 클릭하세요.



- **장치**: IR 페이스를 등록할 장치를 선택하세요.
- **얼굴 포즈 변화**: IR 페이스를 등록할 때 얼굴의 위치, 각도, 거리에 대한 민감도를 설정할 수 있습니다. 정밀한 IR 페이스 템플릿을 얻으려면 높게 설정하세요.
- **+ 추가**: IR 페이스를 등록하려면 버튼을 클릭하세요. IR 페이스는 최대 5개까지 추가할 수 있습니다.
- **스캔**: IR 페이스를 스캔하려면 추가한 **N번째** 버튼을 클릭하세요. 장치 화면의 지시에 따라 얼굴을 스캔하세요.



- **프로필 이미지로 사용**: 등록한 IR 페이스 이미지를 프로필 이미지로 사용하려면 해당 옵션의 체크박스를 클릭하세요.
- **삭제**: IR 페이스 크리덴셜을 삭제할 수 있습니다. 삭제할 번호를 선택하고 버튼을 클릭하세요.

알아두기

- IR 페이스를 등록할 수 있는 장치는 아래를 참고하세요.
  - FaceStation 2
  - FaceLite
- 얼굴 인증률이 낮다면 얼굴 정보를 삭제하고 새로운 얼굴 정보를 등록하세요.

얼굴 등록하기

출입을 위한 인증 수단으로 사용자의 얼굴을 등록해 사용할 수 있습니다. 얼굴 등록은 사용자의 얼굴을 카메라로 촬영한 인증 수단입니다. 카메라로 촬영한 사용자의 얼굴 정보는 모바일 기기에서 비대면으로 등록할 수도 있습니다.

얼굴 등록 시 주의 사항

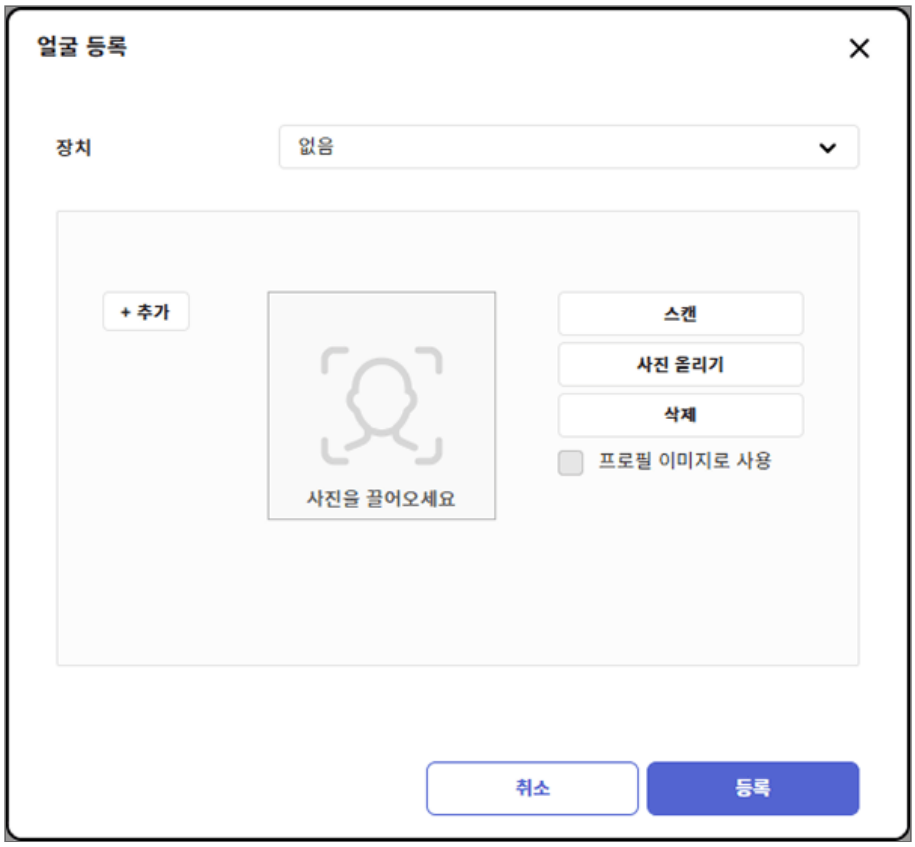
- 얼굴을 등록할 때 장치와 얼굴의 거리를 60~100 cm로 유지하세요.
- 표정이 변하지 않도록 주의하세요.
- 마스크, 모자, 안대를 착용하지 마세요.
- 마스크를 착용한 얼굴을 등록하지 마세요. 마스크를 착용한 얼굴과 착용하지 않은 얼굴을 모두 등록할 경우 오인식률이 높아질 수 있습니다.
- 고개를 들거나 숙이지 마세요.
- 진한 화장을 하지 마세요.
- 눈을 감지 마세요.
- 화면에 양쪽 어깨가 모두 나타나도록 하세요.
- 움직이지 말고, 정면으로 서서 얼굴을 등록하세요.
- 두 명의 얼굴이 화면에 동시에 나타나지 않도록 주의하세요.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

알아두기

CSV 파일로 가져오기 기능을 사용하거나 여러 명의 사용자 얼굴을 한 번에 등록하는 기능, 또는 여러 명의 사용자에게 이메일로 얼굴 등록 링크를 전송해 모바일 장치에서 직접 얼굴을 등록할 수도 있습니다. 자세한 내용은 얼굴 일괄 등록하기를 참고하세요.

장치로 등록

크리덴셜 섹션에서 **+ 얼굴** 버튼을 클릭하세요. **얼굴 등록** 창이 나타나면 각 항목을 설정하고 **등록** 버튼을 클릭하세요.



- **장치**: 얼굴을 등록할 장치를 선택하세요.
- **+ 추가**: 얼굴을 등록하려면 버튼을 클릭하세요. 최대 2개의 얼굴을 추가할 수 있습니다.
- **스캔**: 얼굴을 스캔하려면 추가한 **N번째** 버튼을 클릭하세요. 장치 화면의 지시에 따라 얼굴을 스캔하세요.



- **사진 올리기**: 얼굴을 스캔하지 않고 얼굴 이미지를 업로드해 사용할 수 있습니다.

  – 지원하는 이미지 파일의 크기는 최대 10MB입니다.
  – 지원하는 이미지 파일은 JPG, JPEG, PNG 형식입니다.

- **프로필 이미지로 사용**: 등록한 얼굴 이미지를 프로필 이미지로 사용하려면 해당 옵션의 체크박스를 클릭하세요.
- **삭제**: 얼굴 크리덴셜을 삭제할 수 있습니다. 삭제할 번호를 선택하고 버튼을 클릭하세요.

알아두기

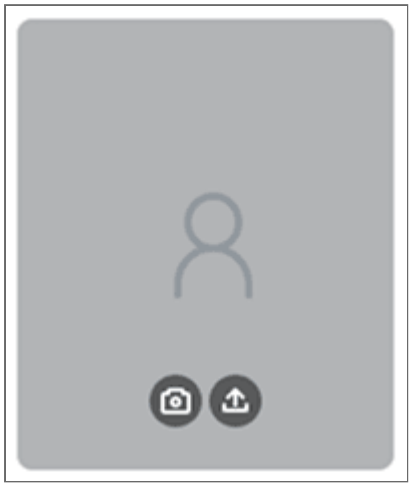
- 얼굴을 등록할 수 있는 장치는 아래를 참고하세요.
  - BioStation 3 Max
  - BioEntry W3
  - BioStation 3
  - FaceStation F2
- 얼굴 인증률이 낮다면 얼굴 정보를 삭제하고 새로운 얼굴 정보를 등록하세요.

웹캠 또는 사진 이미지로 등록

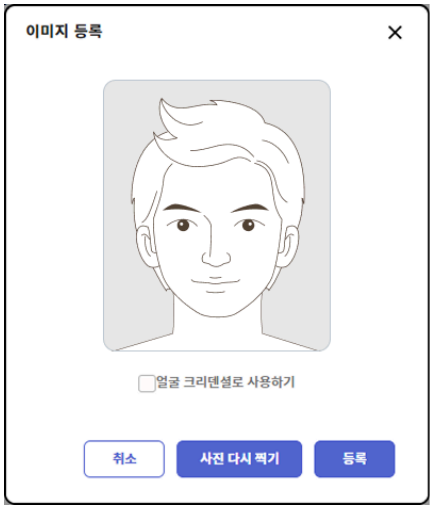
PC에 연결된 웹캠으로 사진을 촬영하고, 촬영된 사진으로 사용자 프로필 사진을 설정하고 얼굴을 크리덴셜로 등록할 수 있습니다. 또는 업로드한 사진을 얼굴 크리덴셜로 등록할 수 있습니다.

1. PC에 웹캡을 연결하세요.
2. 화면 오른쪽 상단의 프로필 이미지 영역에 마우스를 오버하면 나타나는 버튼을 클릭하세요.

   PC에 저장한 이미지를 업로드하려면 버튼을 클릭하세요.



3. **이미지 등록** 창이 나타나면 **사진 찍기** 또는 **사진 업로드** 버튼을 클릭하세요.
4. 웹캠으로 사진을 촬영하면 사진이 표시되고, PC에서 사진을 업로드하면 업로드한 사진을 표시합니다.





5. 웹캠으로 촬영한 사진이나 업로드한 사진을 얼굴 크리덴셜로 등록하려면 **얼굴 크리덴셜로 사용하기** 옵션의 체크박스를 클릭하세요.
6. 얼굴 등록을 완료하려면 **등록** 버튼을 클릭하세요.

알아두기

- 웹캠을 처음 사용한다면 브라우저의 카메라 사용 권한을 묻는 팝업이 나타납니다. 웹캠을 사용하기 위해서는 브라우저의 카메라 사용 권한을 허용해야합니다.
- 브라우저에 따라 카메라 사용 권한을 허용하는 과정이 다를 수 있습니다.
- **사진 찍기** 버튼을 클릭하고 사진을 촬영하기까지 몇 초 정도 소요될 수 있습니다.
- Google 크롬 100 버전 이상을 사용하는 것을 권장합니다.
- 사진을 업로드하기 위한 이미지 파일의 크기는 최대 10MB입니다.
- 지원하는 이미지 파일의 형식은 JPG, JPEG, PNG입니다.
- 웹캠으로 얼굴을 촬영할 때 다음 사항에 유의하세요.
  - 웹캠과 너무 가깝거나 너무 멀지 않게 거리를 유지하세요.
  - 움직이지 말고 정면으로 얼굴을 등록하세요.
  - 표정이 변하지 않도록 주의하세요.
  - 마스크, 모자, 안대를 착용하지 마세요.
  - 고개를 들거나 숙이지 마세요.
  - 진한 화장을 하지 마세요.
  - 눈을 감지 마세요.
  - 양쪽 어깨가 모두 나타나도록 하세요.
  - 두 명의 얼굴이 동시에 나타나지 않도록 주의하세요. 한 번에 한 사람씩 촬영하세요.

출입 카드 등록하기

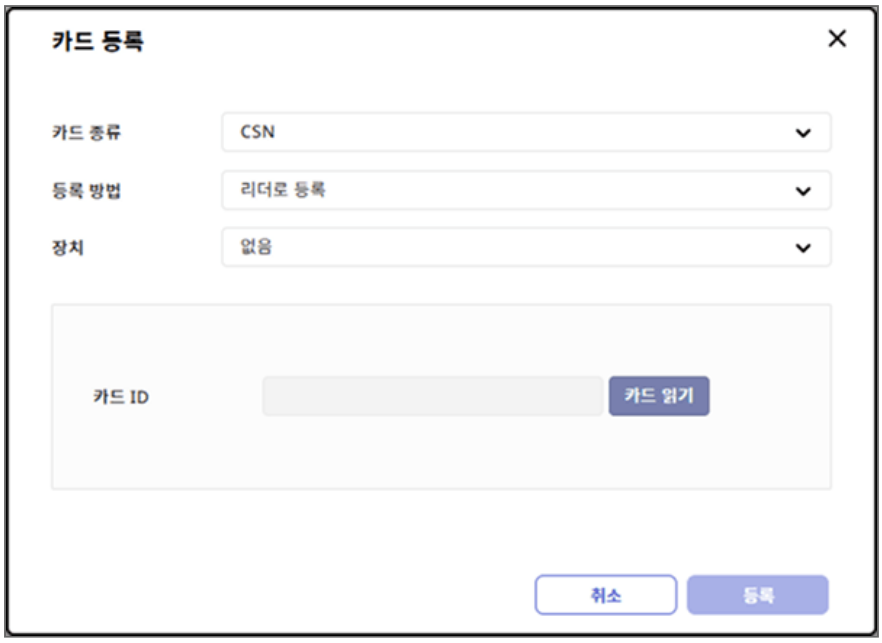
사용자에게 출입 카드를 등록하는 방법을 안내합니다. CSN 카드, Wiegand 카드, 스마트 카드 등록 방법과 카드 읽기/포맷 기능을 설명합니다. 장치가 지원하는 카드 종류는 해당 장치의 매뉴얼을 참고하세요.

USB 에이전트를 이용한 카드 등록

카드 종류	CSN	Wiegand	스마트 카드
EM	✕	✕	✕
MIFARE	✓	✕	✓
DESFire	✓	✕	✓
FeliCa	✓	✕	✕
HID Prox	✕	✕	✕
HID iCLASS	✕	✕	✕

CSN 카드

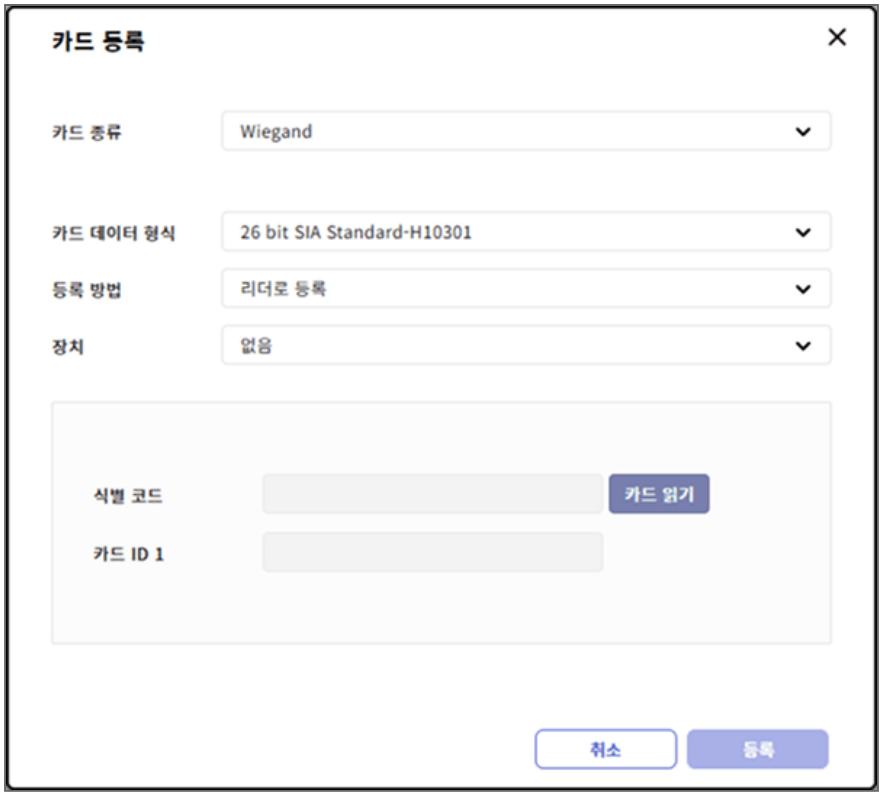
1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **CSN**을 선택하세요.



3. **등록 방법** 옵션에서 원하는 카드 등록 방식을 선택하세요.
   - **리더로 등록**: **장치** 목록에서 카드를 스캔할 장치를 선택하고 **카드 읽기** 버튼을 클릭하세요.
   - **카드 할당**: 목록에서 사용자에게 할당하려는 카드를 선택하세요. 입력 필드를 통해 검색할 수도 있습니다.
   - **직접 입력**: 카드 번호를 직접 입력하거나 **사용자 ID 사용** 버튼을 클릭하세요.
4. **등록** 버튼을 클릭하세요.

Wiegand 카드

1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **Wiegand**을 선택하세요.



3. **카드 데이터 형식** 옵션에서 원하는 형식을 선택하세요.
4. **등록 방법** 옵션에서 원하는 카드 등록 방식을 선택하세요.
   - **리더로 등록**: **장치** 목록에서 카드를 스캔할 장치를 선택하고 **카드 읽기** 버튼을 클릭하세요.
   - **카드 할당**: 목록에서 사용자에게 할당하려는 카드를 선택하세요. 입력 필드를 통해 검색할 수도 있습니다.
   - **직접 입력**: 시설 코드(Facility Code)와 카드 ID를 직접 입력하세요.
5. **등록** 버튼을 클릭하세요.

> **알아두기**
> **카드 데이터 형식** 옵션에 원하는 카드 데이터 형식이 없다면 Wiegand 카드 형식 설정하기를 참고하세요.

스마트 카드

액세스 온 카드 또는 보안 크리덴셜 카드, 커스텀 스마트 카드를 등록할 수 있습니다.

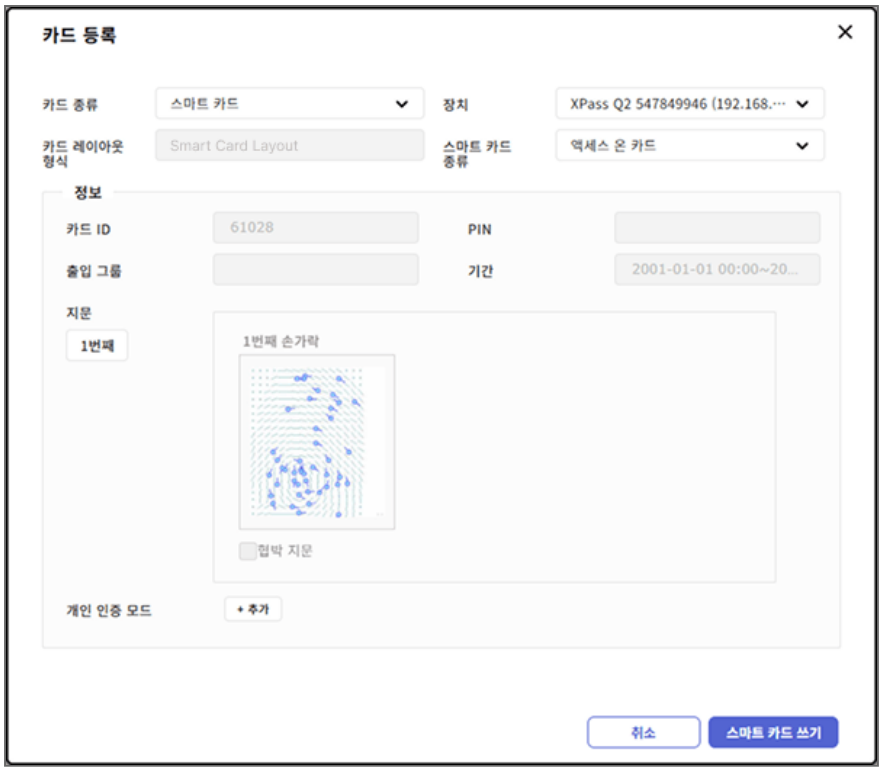
알아두기

- 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.
- 얼굴 템플릿을 사용하려면 **설정** → **크리덴셜** → **카드 형식** 메뉴에서 새 스마트 카드를 추가할 때 **레이아웃** 섹션에서 **얼굴 템플릿 사용**을 선택하세요. 자세한 내용은 스마트 카드 형식 설정하기를 참고하세요.
- 장치에 스마트 카드 레이아웃을 설정하려면 인증 설정하기를 참고하세요.
- 스마트 카드를 포맷하여 정보를 다시 기록하려면 카드 읽기/포맷을 참고하세요.

액세스 온 카드

카드 ID, PIN, 출입 그룹, 기간, 지문 템플릿, 얼굴 템플릿, 개인 인증 모드를 포함한 사용자 정보를 카드에 저장하려면 **액세스 온 카드**를 선택하세요.

1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **스마트 카드**를 선택하세요.
3. **장치** 옵션에서 카드를 등록할 장치를 선택하세요.
4. 장치를 선택하면 **카드 레이아웃 형식** 옵션에 설정된 카드 레이아웃 형식이 표시됩니다.
5. **스마트 카드 종류** 옵션에서 **액세스 온 카드**를 선택하세요.



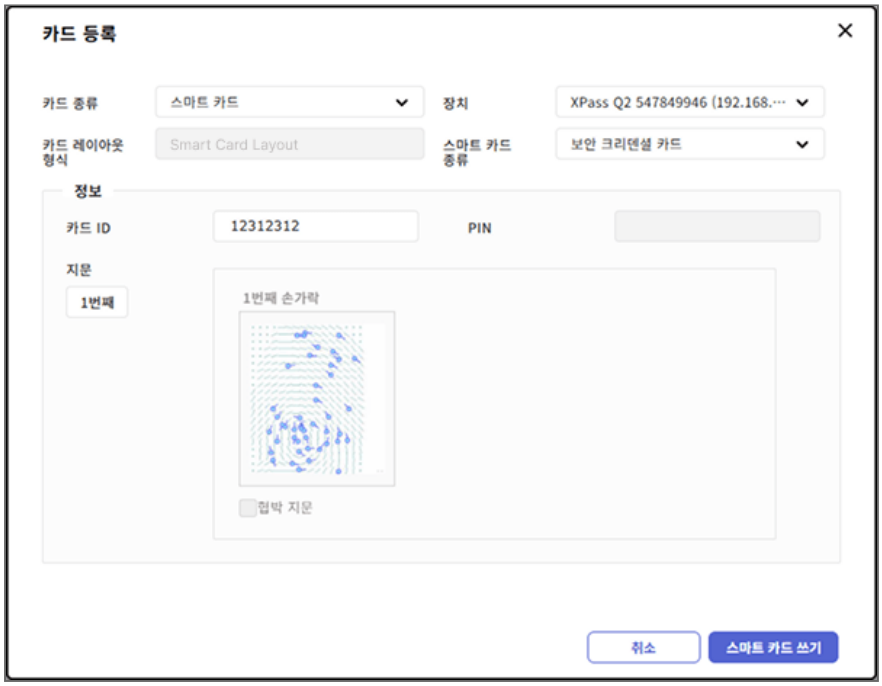
6. 지문 또는 템플릿이 있다면 선택하고, 없는 경우 이 단계를 건너뛰세요.
7. **스마트 카드 쓰기** 버튼을 클릭하세요.

> **알아두기**
> 액세스 온 카드는 카드 ID를 직접 설정할 수 없습니다.

보안 크리덴셜 카드

카드 ID, PIN, 지문 템플릿, 얼굴 템플릿을 포함한 사용자 정보를 카드에 저장하려면 **보안 크리덴셜 카드**를 선택하세요.

1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **스마트 카드**를 선택하세요.
3. **장치** 옵션에서 카드를 등록할 장치를 선택하세요.
4. 장치를 선택하면 **카드 레이아웃 형식** 옵션에 설정된 카드 레이아웃 형식이 표시됩니다.
5. **스마트 카드 종류** 옵션에서 **보안 크리덴셜 카드**를 선택하세요.

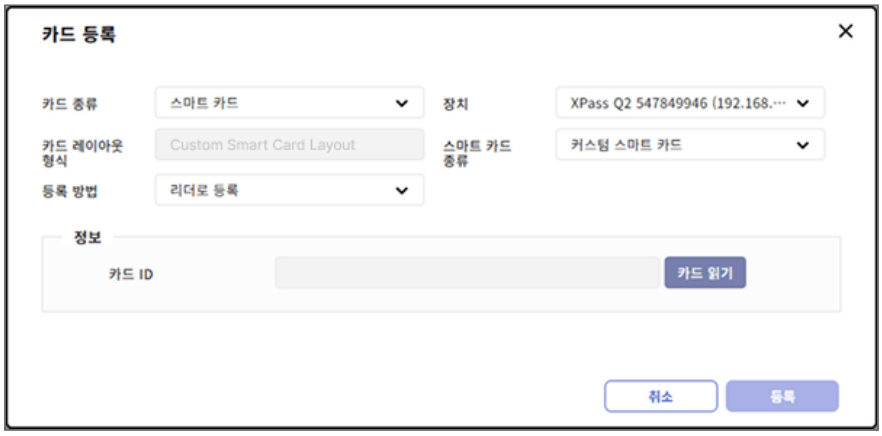


6. **카드 ID**를 직접 입력하세요.
7. 지문 또는 얼굴 템플릿이 있다면 선택하고, 없는 경우 이 단계를 건너뛰세요.
8. **스마트 카드 쓰기** 버튼을 클릭하세요.

커스텀 스마트 카드

타사에서 발급한 스마트 카드를 등록하려면 **커스텀 스마트 카드**를 선택하세요.

1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **스마트 카드**를 선택하세요.
3. **장치** 옵션에서 카드를 등록할 장치를 선택하세요.
4. 장치를 선택하면 **카드 레이아웃 형식** 옵션에 설정된 카드 레이아웃 형식이 표시됩니다.
5. **스마트 카드 종류** 옵션에서 **커스텀 스마트 카드**를 선택하세요.



6. **등록 방법** 옵션에서 원하는 카드 등록 방식을 선택하세요.
   - **리더로 등록**: **장치** 목록에서 카드를 스캔할 장치를 선택하고 **카드 읽기** 버튼을 클릭하세요.
   - **카드 할당**: 목록에서 사용자에게 할당하려는 카드를 선택하세요. 입력 필드를 통해 검색할 수도 있습니다.
   - **직접 입력**: 카드 번호를 10진수 형태로 직접 입력하세요.
7. **등록** 버튼을 클릭하세요.

> **알아두기**
> 커스텀 스마트 카드를 사용할 수 있는 장치와 펌웨어 버전은 아래 목록을 참고하세요.
>
> **▼ 커스텀 스마트 카드 지원 장치와 펌웨어 버전 보기**
> - BioStation 3 Max 펌웨어 1.0.0 이상
> - XPass Q2 펌웨어 1.0.0 이상
> - BioEntry W3 펌웨어 1.0.0 이상
> - BioStation 2a 펌웨어 1.1.0 이상
> - BioStation 3 펌웨어 1.3.0 이상
> - X-Station 2 펌웨어 1.3.0 이상
> - BioLite N2 펌웨어 1.6.2 이상
> - XPass D2 펌웨어 1.7.1 이상
> - BioEntry P2 펌웨어 1.5.1 이상
> - BioEntry W2 펌웨어 1.8.0 이상

카드 읽기/포맷

스마트 카드를 포맷하고 정보를 다시 기록할 수 있습니다.

1. **크리덴셜** 섹션에서 **+ 카드** 버튼을 클릭하세요.
2. **카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **카드 읽기**를 선택하세요.

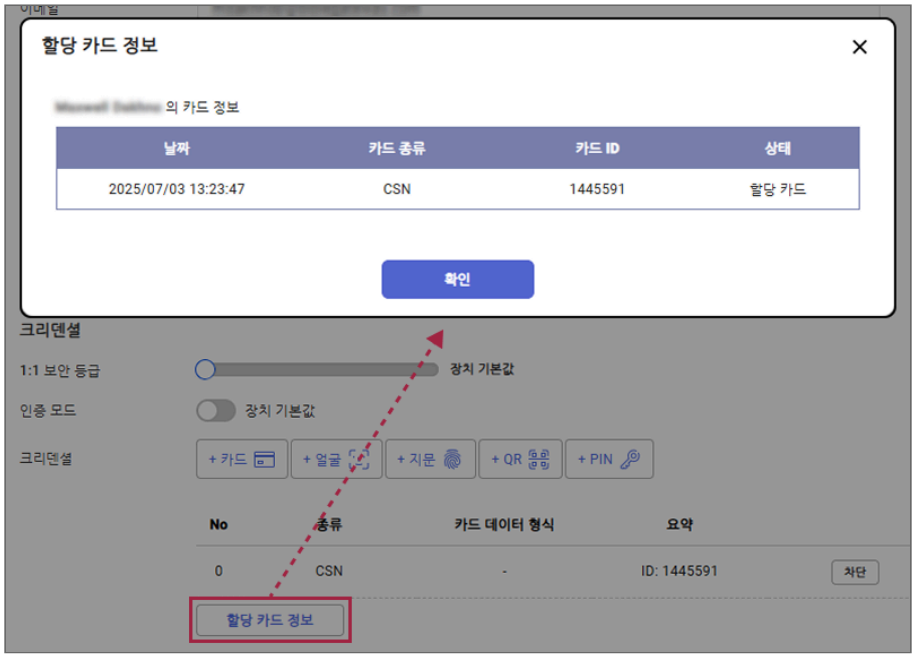


3. **장치** 옵션에서 스마트 카드를 읽을 수 있는 장치를 선택하세요.
4. **스마트 카드 유형**를 선택하세요.
5. **카드 읽기** 버튼을 클릭하세요.
6. 카드 정보를 확인하고 **카드 포맷** 버튼을 클릭하세요.

> **알아두기**
>
> - **장치** 항목의 장치 목록은 스마트 카드 레이아웃이 설정되어야 표시되며, 설정에 대한 자세한 내용은 인증 설정하기를 참고하세요.
> - 커스텀 스마트 카드는 포맷할 수 없습니다.

할당 카드 정보 확인

사용자에게 할당된 카드 정보를 확인하려면 **크리덴셜** 섹션의 **할당 카드 정보** 버튼을 클릭하세요. 카드를 할당한 날짜 및 카드 종류, 카드 아이디, 상태를 확인할 수 있습니다.



모바일 출입 카드 등록하기

슈프리마의 에어팝 포털(Airfob Portal)과 연동하여 모바일 출입 카드를 사용하면, 사용자에게 모바일 출입 카드를 발급할 수 있습니다. 모바일 출입 카드는 각 사용자가 개별 등록하거나 CSV 불러오기 기능을 이용해 다수의 사용자를 한 번에 등록할 수도 있습니다.

에어팝 포털에서 설정한 모바일 출입 카드 발송 방법에 따라 사용자의 이메일을 입력해야 합니다.

> **알아두기**
>
> - 모바일 출입 카드는 **CSN 모바일 카드**와 **템플릿 온 모바일** 중 하나만 사용할 수 있습니다.
> - 이 기능은 에어팝 포털과 연동해야 사용할 수 있습니다. 에어팝 포털 연동 및 모바일 출입 카드 사용에 대한 자세한 내용은 모바일 출입 카드 관리하기를 참고하세요.

CSN 모바일

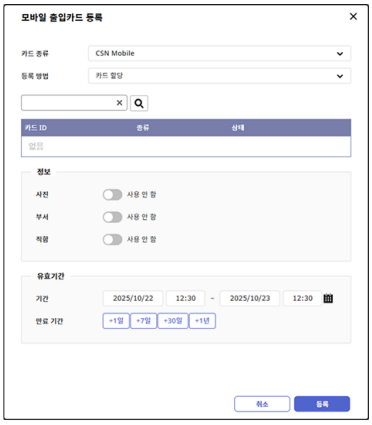
사용자에게 CSN 모바일 출입 카드를 발급할 수 있습니다.

카드 할당

1. **크리덴셜** 섹션에서 **모바일 출입 카드** 버튼을 클릭하세요.
2. **모바일 출입카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **CSN Mobile**을 선택하세요.
3. **등록 방법** 옵션에서 **카드 할당**을 선택하세요.



Airfob portal site: Regular



Airfob portal site: Dynamic

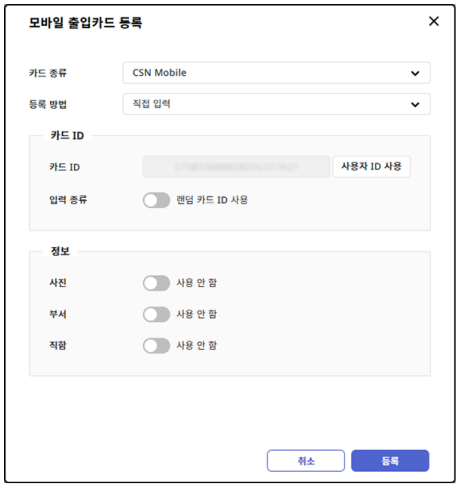
> **유효기간** 항목은 에어팝 포털에서 사이트 생성 시 **다이내믹(Dynamic)** 사이트로 설정할 때 활성화됩니다. 사용자의 모바일 출입 카드의 만료 기간 및 사용 기간을 설정할 수 있습니다. 에어팝 포털 사용에 대한 자세한 내용은 다음 링크를 참고하세요.

4. 카드 목록에서 할당하려는 카드를 선택하거나 검색하세요.
5. **정보**와 **유효기간**을 설정하세요.
6. **등록** 버튼을 클릭하세요.

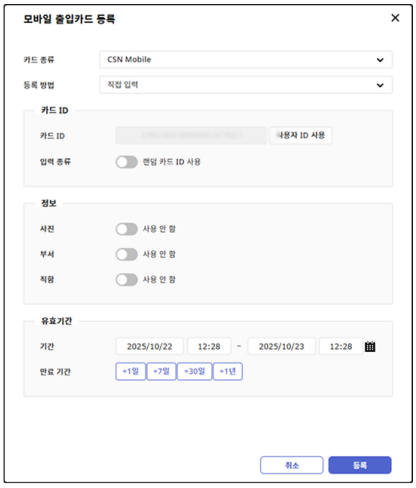
> **알아두기**
>
> - **정보** 섹션의 **사진**, **부서**, **직책** 옵션을 활성화했다면, 해당 정보를 사용자의 모바일 출입 카드에 표시할 수 있습니다. 이때 표시하는 항목은 사용자 정보에 입력된 내용을 기준으로 합니다. 사용자 기본 정보 입력에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.
> - 사용자 이름에 모바일 액세스 카드와 호환되지 않는 특수 문자가 포함된 경우 발급이 제한됩니다. `@` `-` `_` `+` `[` `]` `,` `.` 만 사용할 수 있습니다.
> - 사용자 이름에 홑따옴표(`'`)가 포함되어 있다면, 사용자 저장 시 홑따옴표가 제거된 값이 모바일 출입 카드 발급 시스템으로 전송된다는 안내가 표시됩니다. 이 안내가 표시되는 시점에는 카드 레코드가 이미 생성된 상태이므로, 안내를 취소하면 에어팝 포털로의 전송만 중단되어 해당 카드는 사용할 수 없는 상태로 남습니다. 이 경우 시스템은 사용할 수 없는 카드를 사용자와 연결하지 않고, 나머지 사용자 정보만 저장합니다.

직접 입력

1. **크리덴셜** 섹션에서 **모바일 출입 카드** 버튼을 클릭하세요.
2. **모바일 출입카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **CSN Mobile**을 선택하세요.
3. **등록 방법** 옵션에서 **직접 입력**을 선택하세요.



Airfob portal site: Regular



Airfob portal site: Dynamic

> **유효기간** 항목은 에어팝 포털에서 사이트 생성 시 **다이내믹(Dynamic)** 사이트로 설정할 때 활성화됩니다. 사용자의 모바일 출입 카드의 만료 기간 및 사용 기간을 설정할 수 있습니다. 에어팝 포털 사용에 대한 자세한 내용은 다음 링크를 참고하세요.

4. **입력 종류** 옵션을 선택하세요.
   - **랜덤 카드 ID 사용**: 자동으로 카드 아이디를 생성합니다.
   - **사용자 ID 사용**: 사용자 아이디를 카드 아이디로 사용합니다. 사용자 아이디가 숫자로만 구성된 경우에만 사용할 수 있습니다.
   - **수동 입력**: 카드 아이디를 직접 입력할 수 있습니다.
5. **정보**와 **유효기간**을 설정하세요.
6. **등록** 버튼을 클릭하세요.

> **알아두기**
>
> - **정보** 섹션의 **사진**, **부서**, **직책** 옵션을 활성화했다면, 해당 정보를 사용자의 모바일 출입 카드에 표시할 수 있습니다. 이때 표시하는 항목은 사용자 정보에 입력된 내용을 기준으로 합니다. 사용자 기본 정보 입력에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.
> - 사용자 이름에 모바일 액세스 카드와 호환되지 않는 특수 문자가 포함된 경우 발급이 제한됩니다. `@` `-` `_` `+` `[` `]` `,` `.` 만 사용할 수 있습니다.
> - 사용자 이름에 홑따옴표(`'`)가 포함되어 있다면, 사용자 저장 시 홑따옴표가 제거된 값이 모바일 출입 카드 발급 시스템으로 전송된다는 안내가 표시됩니다. 이 안내가 표시되는 시점에는 카드 레코드가 이미 생성된 상태이므로, 안내를 취소하면 에어팝 포털로의 전송만 중단되어 해당 카드는 사용할 수 없는 상태로 남습니다. 이 경우 시스템은 사용할 수 없는 카드를 사용자와 연결하지 않고, 나머지 사용자 정보만 저장합니다.
> - 이메일을 통해 전송한 활성화 코드를 사용자가 분실하거나 삭제하여 활성화 링크를 다시 발급하려면 **재전송** 버튼을 클릭하세요.
> - CSN 모바일 애플리케이션에 대한 자세한 내용은 다음 링크를 참고하세요.

템플릿 온 모바일

템플릿 온 모바일은 사용자의 바이오메트릭 템플릿을 모바일 기기에 저장하는 모바일 출입 카드입니다. **BioStar X** 서버, 에어팝 포털(Airfob Portal)과 장치에 사용자 데이터를 저장하지 않고도 바이오메트릭으로 인증할 수 있습니다.

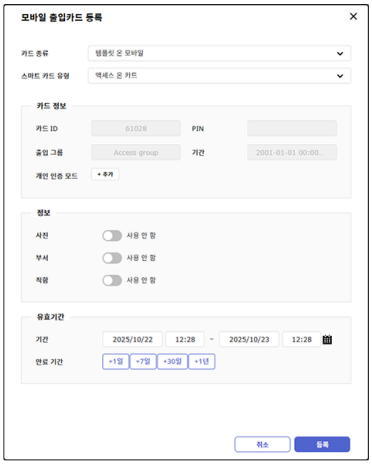
이 기능은 바이오메트릭을 크리덴셜로 사용하고 싶으나 개인정보 보호로 인해 서버 및 장치에 생체 정보를 저장할 수 없는 환경에서 유용하게

사용할 수 있습니다. **템플릿 온 모바일**의 발급과 바이오메트릭 템플릿 등록 과정이 따로 진행되기 때문에, 사용자는 관리자와 대면하지 않고도 **템플릿 온 모바일** 지원 장치에서 직접 얼굴을 등록할 수 있습니다.

1. **크리덴셜** 섹션에서 **모바일 출입 카드** 버튼을 클릭하세요.
2. **모바일 출입카드 등록** 창이 나타나면 **카드 종류** 옵션에서 **템플릿 온 모바일**을 선택하세요.



Airfob portal site: Regular



Airfob portal site: Dynamic

> **유효기간** 항목은 에어팝 포털에서 사이트 생성 시 **다이내믹(Dynamic)** 사이트로 설정할 때 활성화됩니다. 사용자의 모바일 출입 카드의 만료 기간 및 사용 기간을 설정할 수 있습니다. 에어팝 포털 사용에 대한 자세한 내용은 다음 링크를 참고하세요.

3. **스마트 카드 유형** 옵션에서 원하는 카드 종류를 선택하세요.
   - **액세스 온 카드**: 사용자의 정보(카드 ID, PIN, 출입 그룹, 기간, 개인 인증 모드)를 카드에 저장할 수 있습니다.
   - **보안 크리덴셜 카드**: 보안 크리덴셜 카드입니다. 사용자의 카드 ID, PIN 데이터를 카드에 저장할 수 있습니다.
4. **정보**와 **유효기간**을 설정하세요.
5. **등록** 버튼을 클릭하세요.

등록한 사용자의 메일 주소로 발급 메일을 발송합니다. 메일의 링크를 통해 에어팝 패스(Airfob Pass) 애플리케이션을 설치하고, 모바일 기기에 **템플릿 온 모바일** 발급을 완료해야 사용할 수 있습니다.

> **팁**
> **템플릿 온 모바일 인증 방법**
>
> 사용자는 템플릿 온 모바일을 발급받은 모바일 기기를 장치에 태그하고, 화면의 안내에 따라 얼굴을 인증하세요.

알아두기

- **정보** 섹션의 **사진**, **부서**, **직책** 옵션을 활성화했다면, 해당 정보를 사용자의 모바일 출입 카드에 표시할 수 있습니다. 이때 표시하는 항목은 사용자 정보에 입력된 내용을 기준으로 합니다. 사용자 기본 정보 입력에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.
- 사용자 이름에 모바일 액세스 카드와 호환되지 않는 특수 문자가 포함된 경우 발급이 제한됩니다. `@` `-` `_` `+` `[` `]` `,` `.` 만 사용할 수 있습니다.
- 사용자 이름에 홑따옴표(`'`)가 포함되어 있다면, 사용자 저장 시 홑따옴표가 제거된 값이 모바일 출입 카드 발급 시스템으로 전송된다는 안내가 표시됩니다. 이 안내가 표시되는 시점에는 카드 레코드가 이미 생성된 상태이므로, 안내를 취소하면 에어팝 포털로의 전송만 중단되어 해당 카드는 사용할 수 없는 상태로 남습니다. 이 경우 시스템은 사용할 수 없는 카드를 사용자와 연결하지 않고, 나머지 사용자 정보만 저장합니다.
- **템플릿 온 모바일**을 사용할 수 있는 장치와 펌웨어 버전은 아래 목록을 참고하세요.
  - BioStation 3 Max 펌웨어 1.0.0 이상
  - BioEntry W3 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.2.0 이상
  - FaceStation F2 펌웨어 2.2.0 이상
- 모바일 출입 카드는 **CSN 모바일 카드**와 **템플릿 온 모바일** 중 하나만 발급할 수 있습니다.

QR/Barcode 등록하기

사용자 인증 수단으로 QR 코드 또는 바코드를 등록하는 방법을 안내합니다. **BioStar X**에서 직접 생성하는 QR 코드와 외부에서 발급된 QR/바코드를 등록할 수 있습니다.

알아두기

- 스캐너로 QR/Barcode 인증을 사용할 수 있는 장치는 아래를 참고하세요.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- 카메라로 QR/Barcode 인증을 사용할 수 있는 장치는 아래 목록을 참고하세요.
  - BioStation 3 Max 펌웨어 1.0.0 이상
  - XPass Q2 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.1.0 이상
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) 펌웨어 1.2.0 이상
  - X-Station 2 (XS2-QDPB, XS2-QAPB) 펌웨어 1.4.1 이상
- 카메라로 QR/Barcode 인증을 사용하려면 별도의 장치 라이선스가 필요합니다. 자세한 내용은 장치 라이선스를 참고하세요.

BioStar X QR

암호화된 PIN을 포함한 QR 코드를 사용자에게 발급해 출입을 허용할 수 있습니다.

시작하기 전에

- **BioStar QR**을 사용하기 전에 SMTP 설정을 포함한 이메일 정보 설정을 완료하세요. 자세한 내용은 이메일 설정하기를 참고하세요.
- **BioStar QR**을 발급하려면 반드시 사용자 정보에 이메일 주소를 등록해야 합니다. 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.

1. **크리덴셜** 섹션에서 **+ QR/바코드** 버튼을 클릭하세요.
2. **QR/바코드 등록** 창이 나타나면 **QR/바코드 종류** 옵션에서 **BioStar QR**을 선택하세요.



3. **입력 종류** 옵션을 선택하세요.
   - **랜덤 카드 ID 사용**: 자동으로 카드 아이디를 생성합니다.
   - **수동 입력**: 카드 아이디를 직접 입력하세요.
4. **등록** 버튼을 클릭하세요.

이후 사용자가 출입 인증할 때 QR 코드를 발급하여 사용자 정보에 등록된 이메일 주소로 전송합니다. 사용자는 이메일에 포함된 QR 코드를 장치에 스캔하여 출입할 수 있습니다.

알아두기

중복된 카드 아이디 생성을 방지하기 위해 **입력 종류** 옵션에서 **랜덤 카드 ID 사용**을 설정하길 권장합니다.

QR/바코드

외부의 기타 발급처에서 발급된 QR/바코드를 사용자에게 등록할 수 있습니다.

1. **크리덴셜** 섹션에서 **+ QR/바코드** 버튼을 클릭하세요.
2. **QR/바코드 등록** 창이 나타나면 **QR/바코드 종류** 옵션에서 **QR/바코드**을 선택하세요.



3. **등록 방법** 옵션에서 **직접 입력**을 선택하세요.
4. **카드 ID** 옵션에 기존에 발급된 QR/바코드 아이디를 직접 입력하세요.
5. **등록** 버튼을 클릭하세요.

> **알아두기**
> **카드 ID** 옵션에는 영문, 숫자, 특수 기호를 포함하여 최대 32자까지 입력할 수 있습니다.

PIN 등록하기

사용자가 장치에 PIN을 입력하여 출입할 수 있도록 PIN을 등록하는 방법을 안내합니다. 개별 사용자에게 PIN을 등록하거나 CSV 가져오기를 통해 다수의 사용자에게 PIN을 일괄 등록할 수 있습니다.

PIN 등록

1. **크리덴셜** 섹션에서 **PIN** 버튼을 클릭하세요.



2. 입력 필드가 활성화되면 비밀번호를 입력하세요.
3. **PIN 확인**에 동일한 비밀번호를 입력하세요.
4. **등록** 버튼을 클릭하세요.

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

CSV 가져오기로 PIN 등록

CSV 가져오기 기능을 사용해 다수의 사용자를 한 번에 등록할 수 있습니다.

1. 가져올 CSV 파일에 `pin` 열을 추가하세요.
2. `pin` 열에 사용자의 PIN을 입력하고 CSV 파일을 저장하세요.
3. **사용자** 페이지로 이동하세요.
4. 화면 오른쪽 상단의 [•••] 버튼을 클릭하고 **가져오기** → **CSV**를 선택하세요.
5. 화면의 안내에 따라 CSV 파일을 선택하고 가져오기 옵션을 설정하세요.

> **알아두기**
>
> - 사용자당 최대 1개의 PIN 크리덴셜을 등록할 수 있습니다.
> - CSV 가져오기 기능에 대한 자세한 내용은 사용자 정보 내보내기/가져오기를 참고하세요.

사용자 권한 설정하기

조직의 보안 정책에 따라 사용자별로 **BioStar X** 운영 권한과 출입 권한을 차별화하여 설정할 수 있습니다. 관리자 등급을 통해 주요 메뉴 접근을 제한하고, 출입 그룹을 통해 물리적 공간 접근을 제어할 수 있습니다. 또한 IP 주소 제한과 다중 인증을 통해 보안을 강화할 수 있습니다.

런처 → **사용자** 페이지로 이동해, 아래 두 가지 방식으로 출입 권한을 설정할 수 있습니다.

- **새로운 사용자**: 화면 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요. **새 사용자** 창이 나타납니다.
- **기존 사용자**: 사용자 목록에서 사용자를 더블 클릭하세요. 또는, 사용자를 클릭하면 화면 오른쪽에 표시되는 프리뷰 화면에서 **자세히 보기** 버튼을 클릭하세요. 사용자 정보를 수정할 수 있는 창이 나타납니다.

권한 섹션에서 설정할 수 있는 항목은 아래와 같습니다. 각 항목에 대한 설명을 참고하여 적절한 사용자 권한을 설정하세요.



관리자 등급 선택

관리자 등급에 따라 접근할 수 있는 메뉴가 제한됩니다. **권한** 섹션의 **관리자 등급** 항목에서 사용자의 관리자 등급을 선택하세요. 사용자에게 할당할 수 있는 관리자 등급은 아래 목록을 참고하세요.

- **전체 관리자**: 모든 메뉴를 사용할 수 있는 관리자 등급입니다.
- **사용자 관리자**: **사용자** 메뉴에 대한 **읽기, 수정** 권한을 가집니다. **사용자** 메뉴 외 다른 설정 그룹에 대한 권한은 없습니다.
- **모니터링 관리자**: **모니터링**과 **데이터** 메뉴에 대한 **읽기, 수정** 권한을 가지며, **대시보드** 메뉴에 대한 **읽기** 권한을 가집니다.
- **근태 관리자**: **근태 관리** 메뉴에 대한 **읽기, 수정** 권한을 가지며, **사용자** 메뉴에 대한 **읽기** 권한을 가집니다.
- **방문자 관리자**: **방문자** 메뉴에서 **읽기, 수정** 권한을 가집니다.

알아두기

- 관리자 등급을 설정하지 않으려면 **없음**을 선택하세요. 이 경우 해당 사용자는 **BioStar X**에 로그인할 수 없습니다.
- **모니터링** 메뉴의 **수정** 권한은 탭을 추가하거나 상태 트리 항목을 제어할 수 있습니다.
- **데이터** 메뉴의 **수정** 권한은 보고서 저장 및 자동 보고서 일정 추가, 설정에 접근할 수 있습니다.
- 사전 정의된 사용자 권한 외 새로운 사용자 권한을 추가하려면 커스텀 권한 추가하기를 참고하세요.
- 기본 제공하는 계정의 권한은 수정하거나 삭제할 수 없습니다.
- **근태 관리자** 및 **방문자 관리자** 등급은 별도의 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

로그인 아이디 및 비밀번호 설정

관리자 등급을 선택했다면 해당 사용자가 **BioStar X**에 로그인할 때 사용할 아이디와 비밀번호를 설정해야 합니다.



알아두기

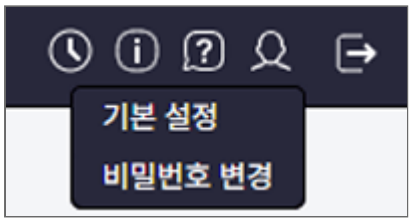
아이디 및 비밀번호 설정 시 주의사항

- 아이디는 영문, 숫자, 마침표(.)를 조합하여 8~32자 이내로 설정하세요. 단, 홑따옴표(')는 사용할 수 없습니다.
- 비밀번호 정책 설정에 대한 자세한 내용은 시스템 보안 강화하기를 참고하세요.
- 보안상 취약한 비밀번호는 사용을 피하세요.
  - 연속된 문자나 숫자(예, abcd, 1234)
  - 일반적인 단어나 패턴(예, qwerty, password)

로그인 사용자 비밀번호 변경

사용자는 **BioStar X**에 로그인한 후 본인의 비밀번호를 변경할 수 있습니다.

1. **BioStar X**에 로그인하세요.
2. 화면 오른쪽 상단의 버튼을 클릭하세요.



3. 드롭다운 메뉴에서 **비밀번호 변경**을 클릭하세요.
4. **비밀번호 변경** 창이 나타나면 현재 비밀번호와 새 비밀번호를 입력하세요.



5. 모든 항목을 입력했으면 **변경** 버튼을 클릭하세요.

다중 인증 설정

다중 인증 로그인을 활성화하면 사용자가 **BioStar X**에 로그인할 때 지문 인증을 추가해 로그인할 수 있습니다.

> **알아두기**
> 다중 인증 설정에 대한 자세한 내용은 다중 인증으로 로그인하기를 참고하세요.

사용자 IP 주소로 로그인 설정

사용자 IP 주소를 등록하면, 계정에 등록한 IP 정보와 일치할 경우에만 PC에 로그인할 수 있습니다. 이를 통해 보안을 강화할 수 있습니다.
권한 섹션의 **로그인 허용 IP** 항목에 사용자의 IP 주소를 입력하세요.

> **알아두기**
>
> - IP 주소는 xxx.xxx.xxx.xxx 형식으로 입력할 수 있으며 각 옥텟은 0~255 범위의 숫자로만 입력할 수 있습니다.
> - IP 주소를 등록하지 않으면 IP 정보와 관계없이 PC에 로그인할 수 있습니다.

출입 그룹 선택

사용자의 출입 그룹을 설정해 조직별, 부서별로 출입을 제한할 수 있습니다. **권한** 섹션의 **출입 그룹** 항목에서 출입 그룹을 선택하세요.

> **알아두기**
>
> 출입 그룹 추가 및 설정에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.

다음 단계

고급 섹션에서 사용자 출입 시 장치에 표시할 메시지를 설정하거나 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다.
사용자 정보를 수정하는 방법을 확인하세요.

사용자 고급 설정하기

사용자 출입 시 장치에 표시할 메시지를 설정하거나 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다. 이 기능은 사용자를 새로 추가하거나 수정할 때 설정할 수 있습니다.

런처 → **사용자** 페이지로 이동해, 아래 두 가지 방식으로 출입 권한을 설정할 수 있습니다.

- **새로운 사용자**: 화면 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요. **새 사용자** 창이 나타납니다.
- **기존 사용자**: 사용자 목록에서 사용자를 더블 클릭하세요. 또는, 사용자를 클릭하면 화면 오른쪽에 표시되는 프리뷰 화면에서 **자세히 보기** 버튼을 클릭하세요. 사용자 정보를 수정할 수 있는 창이 나타납니다.

고급 섹션에서 설정할 수 있는 항목은 아래와 같습니다.



- **장치 표시 메시지**: 사용자 출입 시 장치에 표시할 메시지를 입력할 수 있습니다. 메시지는 최대 128자까지 입력할 수 있습니다.
- **디렉토리 연동 제외**: 디렉토리 서비스 연동 시 해당 사용자를 동기화에서 제외할 수 있습니다.

알아두기

- **디렉토리 연동 제외** 옵션은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 디렉토리 연동 설정에 대한 자세한 내용은 디렉토리 연동 설정하기를 참고하세요.

다음 단계

사용자 정보를 수정하는 방법을 확인하세요.

신분증 스캔으로 사용자 등록 및 수정하기

사용자 정보를 하나하나 입력하는 대신, 신분증을 스캔해 이름 및 사진 등의 정보를 자동으로 가져와 사용자를 등록하거나 기존 사용자 정보를 수정할 수 있습니다.

시작하기 전에

- 신분증 스캔을 위해 DESKO 스캐너를 클라이언트 PC에 연결해야 합니다.
- 신분증을 스캔해 사용자를 등록하기 전에 신분증에서 가져올 데이터를 설정했는지 확인하세요. 신분증 스캔 설정에 대한 자세한 내용은 신분증 스캔 설정하기를 참고하세요.

알아두기

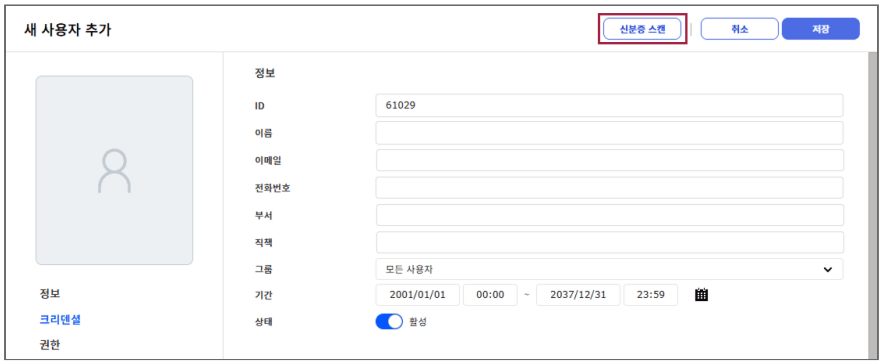
신분증 스캔 기능은 현재 여권 스캔만 지원합니다.

신분증 스캔으로 사용자 등록

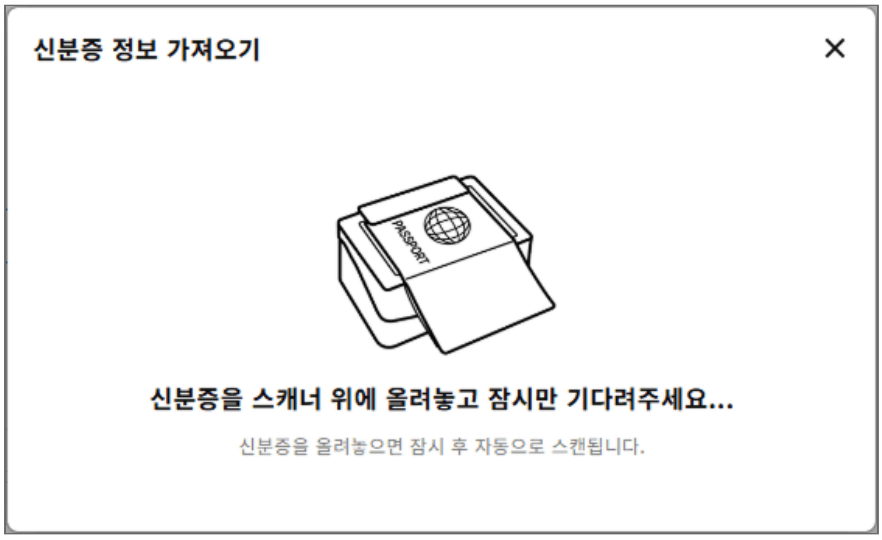
1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. **사용자** 페이지의 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요.



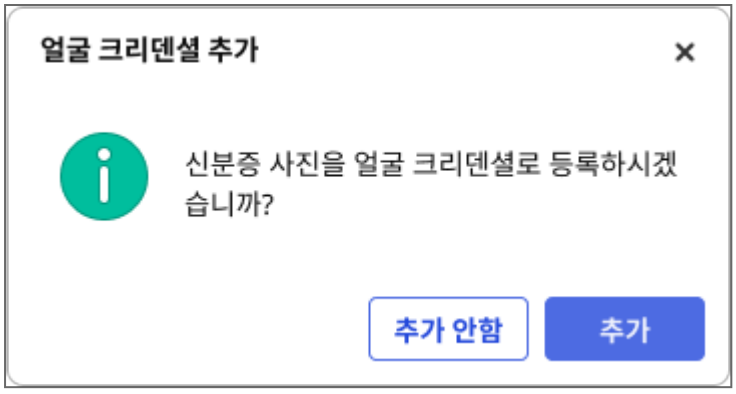
3. **새 사용자 추가** 화면에서 오른쪽 상단의 **신분증 스캔** 버튼을 클릭하세요.



4. **신분증 정보 가져오기** 창이 나타나면 스캐너에 신분증을 올려놓으세요.



5. 신분증 스캔 성공 메시지가 나타난 후 신분증 사진을 얼굴 크리덴셜로 등록할 지 여부를 선택하세요.



> 이 메시지는 **설정** → **계정** → **신분증 스캔**에서 **얼굴 크리덴셜** 옵션을 **확인 요청**으로 설정했을 때 나타납니다. **묻지 않음** 옵션으로 설정하면 이 메시지가 나타나지 않고 바로 얼굴 크리덴셜로 등록됩니다.

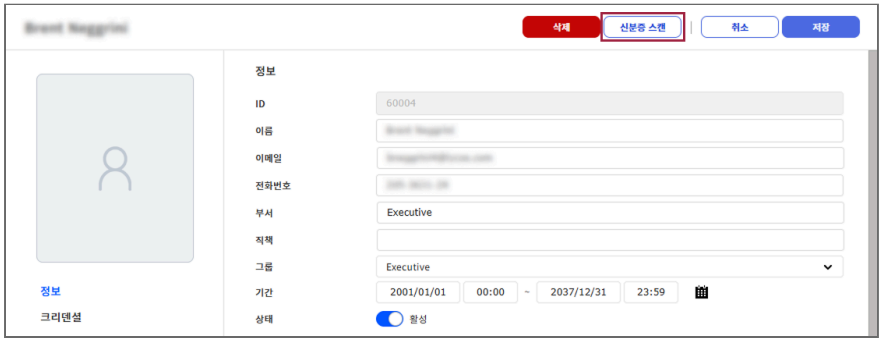
6. 신분증 스캔으로 가져온 정보를 확인하고 필요한 경우 수정하세요.
7. 사용자를 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

신분증 스캔으로 사용자 수정

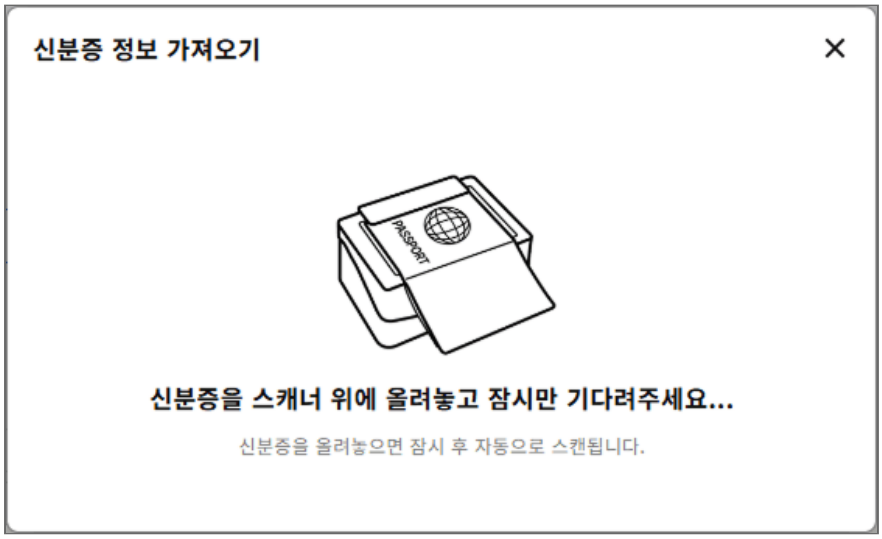
1. **런처** 페이지에서 **사용자**를 클릭하세요.

2. 사용자 목록에서 신분증 스캔으로 수정할 사용자를 더블 클릭하세요.

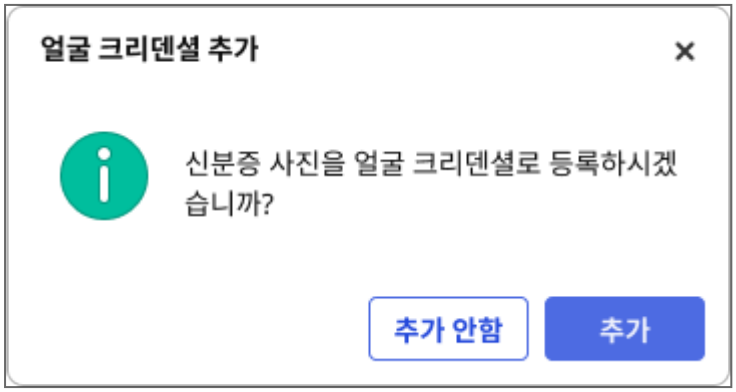
3. 사용자 정보 수정 화면의 오른쪽 상단의 **신분증 스캔** 버튼을 클릭하세요.



4. **신분증 정보 가져오기** 창이 나타나면 스캐너에 신분증을 올려놓으세요.



5. 신분증 스캔 성공 메시지가 나타난 후 신분증 사진을 얼굴 크리덴셜로 등록할 지 여부를 선택하세요.



> 이 메시지는 **설정** → **계정** → **신분증 스캔**에서 **얼굴 크리덴셜** 옵션을 **확인 요청**으로 설정했을 때 나타납니다. **묻지 않음** 옵션으로 설정하면 이 메시지가 나타나지 않고 바로 얼굴 크리덴셜로 등록됩니다.

6. 신분증 스캔으로 가져온 정보를 확인하고 필요한 경우 수정하세요.

7. 스캔한 정보로 사용자 정보를 수정하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

> **알아두기**
> 신분증 스캔으로 수정하려는 사용자의 얼굴 크리덴셜이 2개 이상 등록되어 있다면 첫번째 등록된 얼굴 크리덴셜을 덮어쓰기합니다.

오류 안내

신분증을 스캔하는 중에 문제가 발생하면 화면에 원인과 해결 방법을 안내하는 메시지가 표시됩니다. 아래 내용을 참고하여 오류를 해결하세요.

스캔 실패

신분증을 스캐너에 올려놓고 자동으로 인식하는 과정에서 문제가 발생하면 아래 메시지 중 하나가 나타납니다.

원인	오류 메시지
신분증의 보안 요소(UV 무늬 등) 검증 실패	**유효하지 않은 신분증입니다. 신분증 확인 후 다시 시도하세요.**
지정된 시간 안에 신분증이 인식되지 않음	**시간 내에 신분증이 스캔되지 않았습니다. 다시 시도하세요.**
스캔 도중 신분증 이탈, 페이지 인식 실패 등 그 외 스캔 오류	**신분증을 스캔할 수 없습니다. 신분증 및 스캐너 확인 후 다시 시도하세요.**

위 메시지가 나타나면 화면에 표시된 **재시도** 버튼을 클릭해 다시 스캔하세요. 신분증을 스캐너에 올바르게 올려놓았는지 확인한 후 재시도하면 정상 인식됩니다.

> **알아두기**
> **재시도** 버튼을 클릭하면 **신분증을 스캐너 위에 올려놓고 잠시만 기다려주세요...** 안내부터 자동 인식을 다시 시작합니다.

스캐너 연결 오류

스캐너 연결에 문제가 있으면 아래 메시지가 나타납니다. 이 오류에는 재시도 버튼이 제공되지 않으므로, 안내에 따라 문제를 해결한 후 **신분증 스캔** 버튼을 다시 클릭해 스캔을 처음부터 진행하세요.

상황	오류 메시지	해결 방법
스캐너가 클라이언트 PC에 연결되어 있지 않음	**스캐너가 연결되지 않았습니다. 장치 연결 확인 후 다시 시도하세요.**	신분증 스캐너와 클라이언트 PC의 연결 상태를 확인하세요.

USB Agent 확인 필요

신분증 스캐너를 사용하려면 최신 버전의 USB Agent가 설치되어 있어야 합니다. USB Agent가 설치되어 있지 않거나 버전이 낮으면 **신분증 스캔** 버튼을 클릭했을 때 다음과 같은 오류 창이 나타납니다.



- **취소**: 오류 창을 닫고 스캔을 진행하지 않습니다.
- **USB Agent 설정으로 이동**: **설정** → **장치** → **USB Agent** 화면으로 이동합니다. 이동한 화면에서 USB Agent를 최신 버전으로 업그레이드한 후 다시 스캔을 시도하세요.

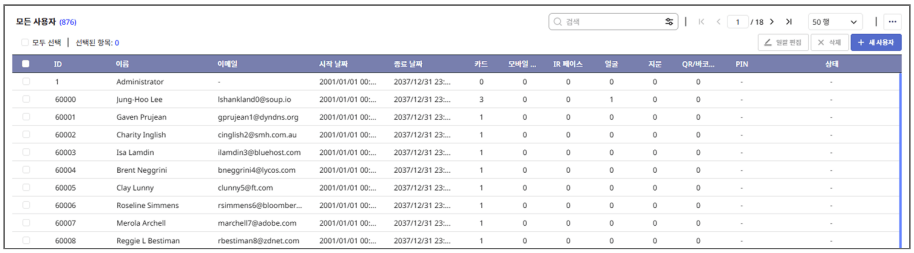
사용자 탐색하기

사용자 목록 페이지에서 등록된 사용자를 조회하고 관리하는 방법을 안내합니다. 일반 검색과 고급 검색을 통해 원하는 사용자를 빠르게 찾을 수 있으며, 목록 정렬, 열 설정, 인쇄 등의 기능을 사용할 수 있습니다.

사용자 페이지에 접근하려면 **런처** 페이지에서 **사용자**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **사용자**를 선택하세요.

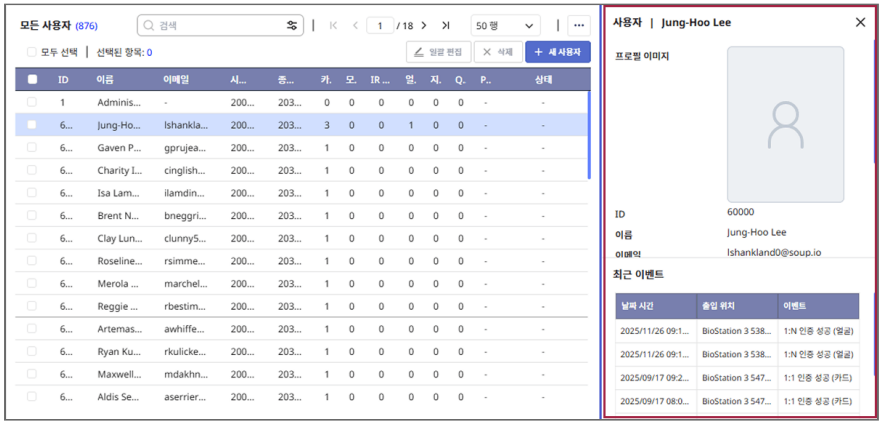
사용자 목록 보기

사용자 목록 페이지에서는 사용자의 기본 정보와 상태를 확인할 수 있으며, 각 사용자의 상세 정보를 열람하거나 수정할 수 있습니다.



사용자 목록은 등록된 사용자를 모두 표시하며, 각 사용자의 아이디, 이름, 이메일 주소, 사용 기간, 등록한 크리덴셜 현황, 상태를 기본으로 확인할 수 있습니다. 사용자는 아이디 순으로 목록에 표시됩니다.

- 개별 사용자의 상세 정보를 확인하려면 사용자 목록에서 원하는 사용자를 클릭하세요. 사용자의 프로필 정보가 화면 오른쪽에 표시됩니다. 사용자 프로필 정보에서 **자세히 보기** 버튼을 클릭하면 사용자의 상세 정보를 수정할 수 있는 페이지로 이동합니다.



- 사용자 상세 정보를 수정하려면 사용자 목록에서 원하는 사용자를 더블 클릭하세요. 사용자의 상세 정보를 수정할 수 있는 페이지로 이동합니다.

> **알아두기**
>
> - 사용자 정보 수정에 대한 자세한 내용은 사용자 정보 수정하기를 참고하세요.
> - 사용자 목록에서 열(Column) 레이아웃을 변경할 수 있습니다. 열 레이아웃 변경에 대한 자세한 내용은 사용자 탐색하기를 참고하세요.

보기 옵션 선택

화면 오른쪽 상단의 도구 버튼을 이용해 사용자 목록의 보기 옵션을 변경할 수 있습니다.

사용자 목록 페이지 이동

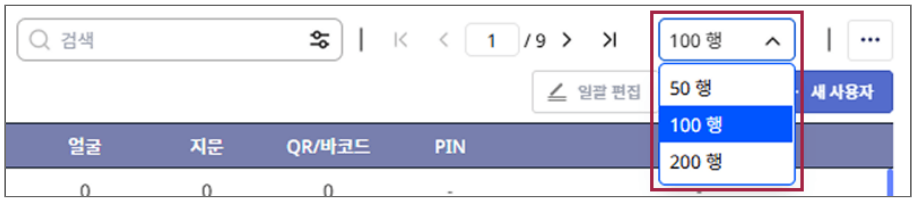
사용자 목록에는 기본 10명의 사용자를 표시합니다. 화면 상단의 버튼을 클릭해 다른 페이지로 이동할 수 있습니다.



- |< : 사용자 목록의 첫 페이지로 이동합니다.
- < : 사용자 목록의 이전 페이지로 이동합니다.
- > : 사용자 목록의 다음 페이지로 이동합니다.
- >| : 사용자 목록의 마지막 페이지로 이동합니다.
- 원하는 페이지로 이동하려면 숫자 입력 필드에 페이지 번호를 입력하고 Enter 키를 누르세요.

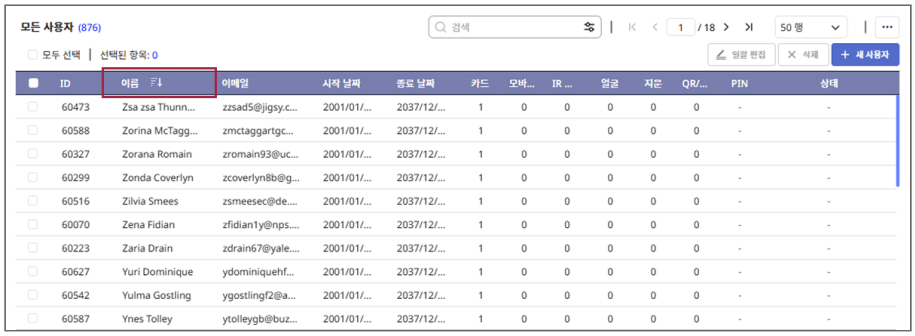
사용자 목록 표시 개수 변경

사용자 목록에 표시되는 사용자 수를 변경할 수 있습니다. 화면 오른쪽 상단의 목록 선택 상자에서 원하는 사용자 수를 선택하세요. 선택할 수 있는 옵션은 50명, 100명, 200명입니다.



사용자 목록 정렬

사용자 목록의 정렬 기준을 변경할 수 있습니다. 목록 상단의 열 제목을 클릭하면 오름차순 또는 내림차순으로 정렬할 수 있습니다. 예를 들어, **이름** 열 제목을 클릭하면 사용자의 이름을 기준으로 오름차순 또는 내림차순으로 정렬됩니다. 이때 클릭한 항목에는 오름차순(↑) 또는 내림차순(↓) 아이콘이 표시됩니다.



> **알아두기**
>
> 열의 종류에 따라 정렬할 수 없는 항목이 있을 수 있습니다.

사용자 검색

특정 사용자를 검색하는 방법을 안내합니다. 사용자 목록 페이지에서 검색 기능을 사용하여 원하는 사용자를 빠르게 찾을 수 있습니다.

> **알아두기**
>
> - 검색 시 사용하는 키워드는 대소문자를 구분하지 않습니다.
> - 사용자의 기본 정보가 입력되어 있어야 검색할 수 있습니다. 사용자의 기본 정보 입력에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.

일반 검색

사용자의 아이디, 이름, 이메일을 기준으로 검색할 수 있습니다. 화면 상단의 검색 입력 필드에 원하는 키워드를 입력하고 `Enter` 키를 누르세요. 해당 키워드와 일치하는 사용자가 목록에 표시됩니다. 목록 최상단에서 검색 결과 개수를 확인할 수 있습니다.



고급 검색

사용자의 아이디, 이름, 이메일 주소, 전화번호 등을 특정해 검색할 수 있습니다.

1. 화면 상단의 검색 입력 필드 옆에 있는 ⚙ 버튼을 클릭하세요.
2. 고급 검색 창이 열리면, 원하는 검색 조건을 입력하고 **검색** 버튼을 클릭하세요.



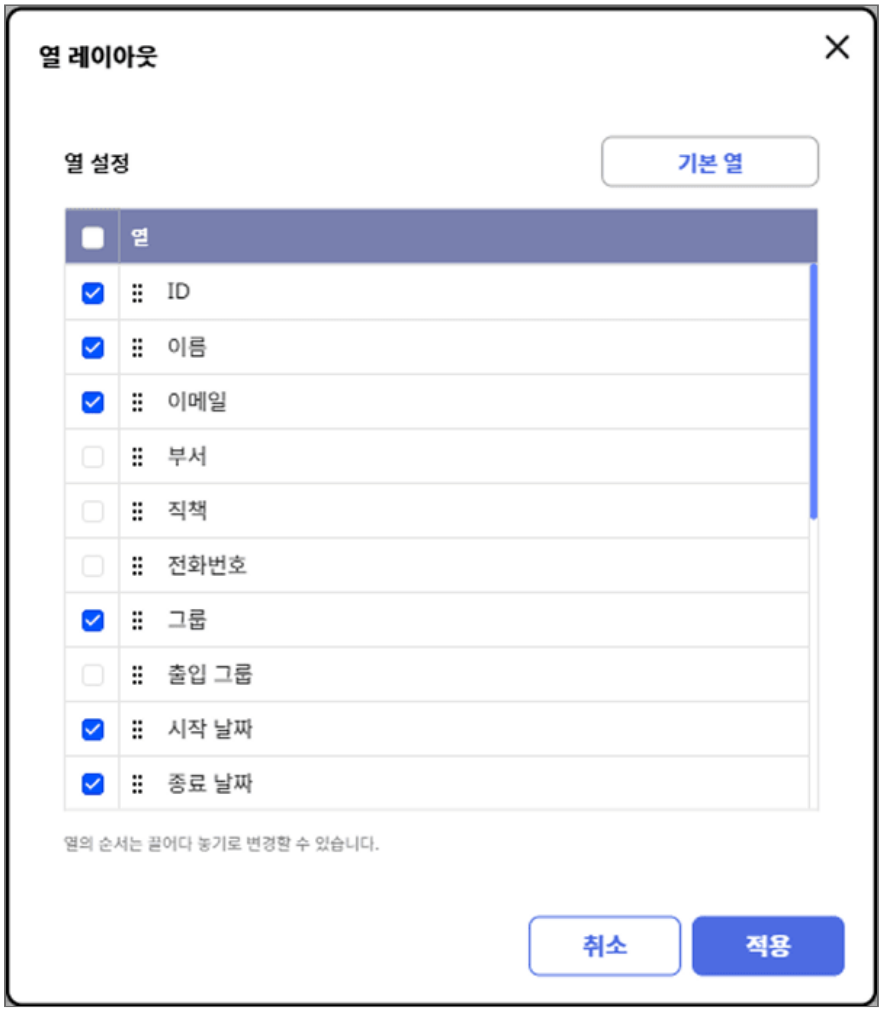
알아두기

- 입력 필드 중 ! 아이콘이 표시된 항목은 개인 정보 DB 암호화로 인해 전문만 검색할 수 있습니다.
- 고급 검색 창에서 입력한 조건을 초기화하려면 **초기화** 버튼을 클릭하세요.
- 고급 검색은 **커스텀 사용자 필드**에 대한 검색을 지원합니다. **커스텀 사용자 필드**에 대한 자세한 내용은 서버 상세 설정하기를 참고하세요.

사용자 목록 열(Column) 설정

사용자 목록에서 표시되는 열(Column) 설정을 변경할 수 있습니다. 열 설정을 통해 표시할 열을 선택하거나 열의 순서를 변경할 수 있습니다.

1. 사용자 목록 화면 오른쪽 상단의 ••• 버튼을 클릭하세요.
2. **열 레이아웃**을 클릭하세요.
3. **열 레이아웃** 창이 나타나면 원하는 열을 선택하거나 선택 해제하세요.



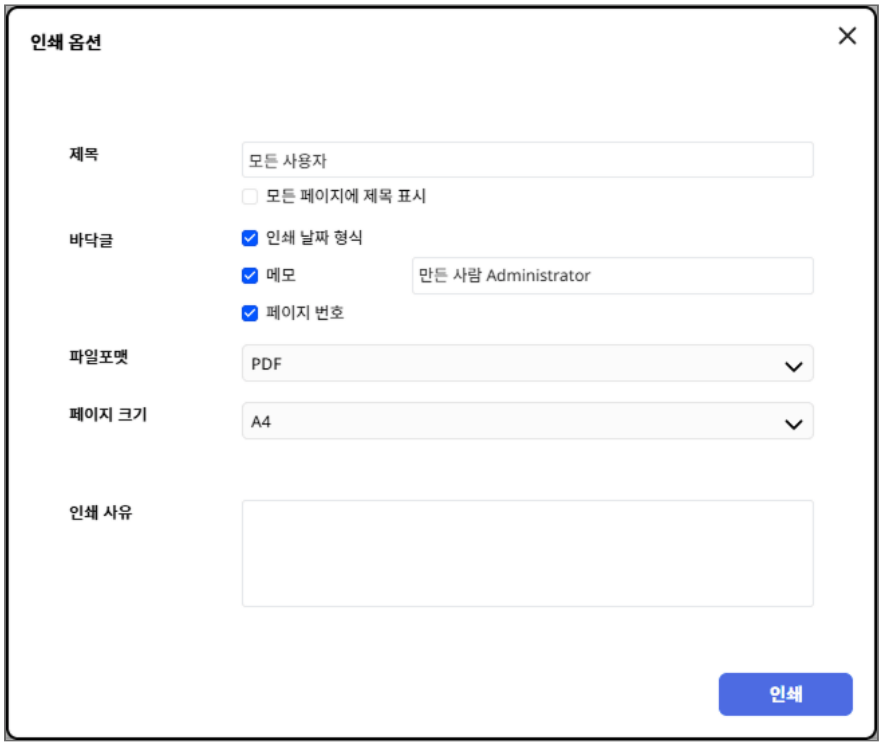
4. 열의 순서를 변경하려면 원하는 열을 클릭한 채로 드래그하여 위치를 변경하세요.
5. 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 열 설정은 각 사용자 계정별로 저장됩니다.
> - 열 레이아웃 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

사용자 목록 인쇄

현재 보고 있는 사용자 목록을 PDF 또는 SVG 파일로 저장할 수 있습니다.

1. 사용자 목록 화면 오른쪽 상단의 ••• 버튼을 클릭하세요.
2. **인쇄**를 클릭하세요.
3. **인쇄 옵션** 창이 나타나면 **파일포맷** 옵션에서 원하는 포맷을 선택하고 나머지 옵션을 설정하세요.



4. **인쇄 사유**(선택 사항)를 입력하고 **인쇄** 버튼을 클릭하세요.

브라우저를 통해 열리는 PDF 또는 SVG 파일을 인쇄할 수 있습니다.

> **알아두기**
> **인쇄 사유**는 필수 입력 항목이 아닙니다. **인쇄 사유**는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

사용자 관리하기

등록된 사용자를 효과적으로 관리하는 방법을 안내합니다. 사용자 정보 수정 및 삭제, 장치와의 데이터 동기화, 출입 이력 추적, 사용자 데이터 내보내기/가져오기 등 사용자 관리에 필요한 핵심 기능들을 단계별로 설명합니다.

사용자 정보 수정하기

등록된 사용자의 정보를 수정하는 방법을 안내합니다. 개별 사용자의 기본 정보, 출입 권한, 크리덴셜을 수정하거나 여러 사용자의 정보를 일괄로 수정할 수 있습니다.

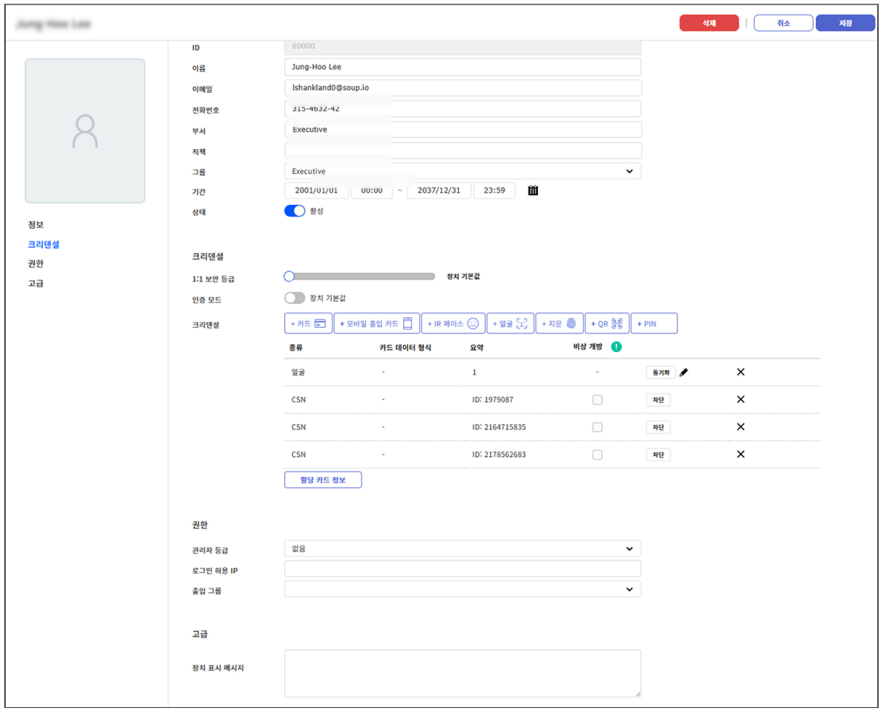
> **알아두기**
> 최초 만들어진 아이디가 `1`인 사용자는 다른 관리자가 수정할 수 없습니다. 해당 계정으로 로그인한 본인만 자신의 정보를 수정할 수 있습니다.

사용자 정보 수정

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 수정할 사용자를 선택하세요.

3. 사용자를 더블 클릭하거나 화면 오른쪽에 사용자의 프로필 정보가 표시되면 **자세히 보기** 버튼을 클릭하세요.

4. 사용자 정보를 수정할 수 있는 창이 나타납니다.



5. 원하는 항목을 수정하세요.

6. 크리덴셜 항목을 수정하려면 ✎ 버튼을 클릭하고, 삭제하려면 ✕ 버튼을 클릭하세요.



7. 수정 사항을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - **정보** 섹션의 각 항목에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.
> - **크리덴셜** 섹션의 각 항목에 대한 자세한 내용은 사용자 크리덴셜 등록하기를 참고하세요.
> - **권한** 섹션의 각 항목에 대한 자세한 내용은 사용자 권한 설정하기를 참고하세요.
> - **고급** 섹션에서 사용자와 관련한 개인 메시지를 입력할 수 있습니다.

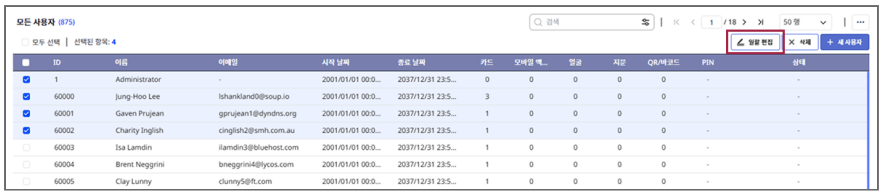
사용자 정보 일괄 수정

한 번에 여러 사용자의 정보나 출입 권한을 수정할 수 있습니다. 이 기능은 다수의 사용자에게 동일한 출입 권한이나 그룹을 설정할 때 유용합니다.

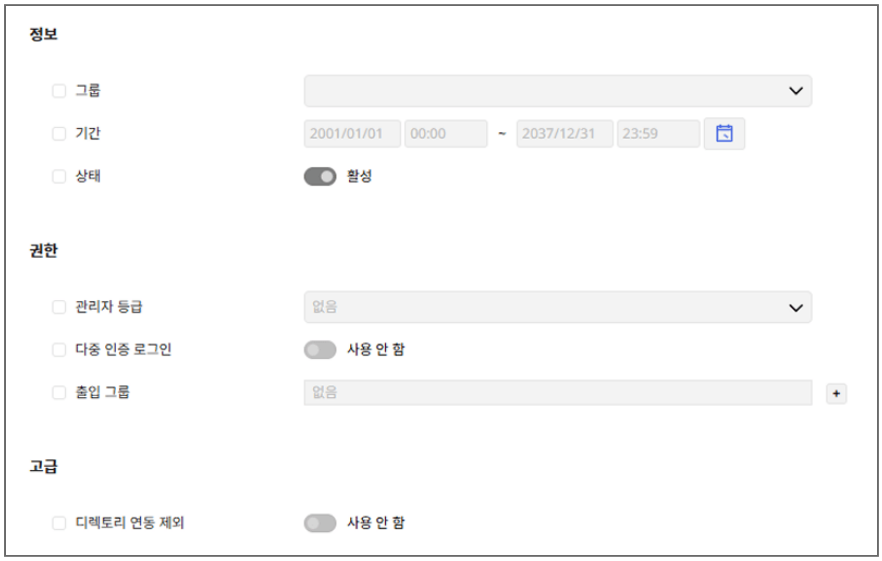
1. **런처** 페이지에서 **사용자**를 클릭하세요.

2. 사용자 목록에서 수정할 사용자의 가장 왼쪽에 체크박스를 클릭하세요. 2명 이상의 사용자를 선택하세요.

3. 화면 오른쪽 상단의 **일괄 편집** 버튼을 클릭하세요.



4. **일괄 편집** 화면이 나타나면 원하는 항목의 체크박스를 클릭하고 수정하세요.



5. 수정한 정보를 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

> **알아두기**
>
> - 사용자의 ID 및 이름, 이메일, 전화번호, 크리덴셜과 같은 개인정보는 일괄 수정할 수 없습니다.
> - 수정한 정보를 취소하려면 화면 오른쪽 상단의 **취소** 버튼을 클릭하세요.

다음 단계

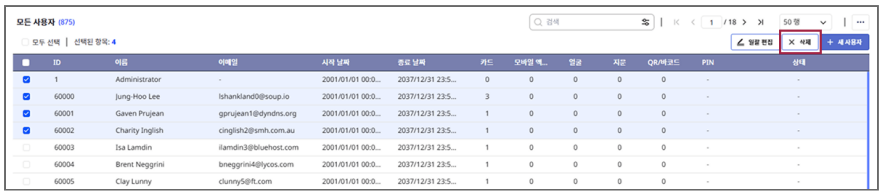
사용자 크리덴셜을 등록하고 출입 인증 방식을 설정하세요.
사용자의 출입 권한 설정 방법을 확인하세요.
사용자 정보를 변경했다면 장치로 전송해야 합니다. 사용자 정보를 장치로 전송하는 방법을 확인하세요.

사용자 삭제하기

BioStar X에 등록한 사용자를 퇴사, 계약 종료, 보안 위반 등의 사유로 삭제해야 하는 경우, 다음의 안내에 따라 삭제할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 삭제할 사용자의 가장 왼쪽에 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.

3. 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.



4. 확인 메시지가 나타나면 **삭제** 버튼을 클릭하세요.

사용자 목록에서 선택한 사용자가 삭제된 것을 확인하세요.

> **알아두기**
>
> - 아이디가 `1`인 사용자는 삭제할 수 없습니다.
> - 장치에서 사용자 정보를 삭제하는 방법에 대한 자세한 내용은 장치에 등록한 사용자 관리하기를 참고하세요.

장치로 사용자 정보 전송하기

출입 통제를 위해 **BioStar X** 서버에 등록한 사용자 정보를 장치로 전송하는 기능을 제공합니다. 장치로 사용자 정보를 전송하면, 장치는 사용자 데이터를 활용하여 출입 권한을 판단하고, 오프라인 환경에서도 인증을 수행할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 사용자 정보를 전송하려는 사용자의 가장 왼쪽에 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 오른쪽 상단의 [•••] 버튼을 선택하고 **장치로 전송**을 클릭하세요.



4. **장치로 전송** 창이 나타나면 장치 목록에서 사용자 정보를 전송할 장치를 선택하세요.



5. 같은 아이디이지만 정보가 다를 경우 **BioStar X** 서버의 내용으로 덮어쓰기하려면 **정보가 다른 사용자 덮어쓰기** 옵션의 체크박스를 클릭하세요.

6. 전송할 장치를 모두 선택했다면 **적용** 버튼을 클릭하세요.

선택한 장치로 사용자 정보를 전송합니다.

알아두기

- 검색 입력 필드에 키워드를 입력해 장치를 검색할 수도 있습니다.
- 사용자 정보를 전송하려면 장치가 **BioStar X** 서버에 연결되어 있어야 합니다.
- 장치에 이미 등록된 사용자의 정보를 변경한 경우, 변경 사항을 장치에 반영하려면 사용자 정보를 다시 전송해야 합니다. 사용자 정보를 장치와 동기화하는 **사용자 자동 동기화** 옵션을 이용하려면 서버 상세 설정하기를 참고하세요.
- 장치마다 등록할 수 있는 사용자 수에 제한이 있습니다. 장치에 등록할 수 있는 사용자 수를 확인하세요.

사용자 출입 이력 추적하기

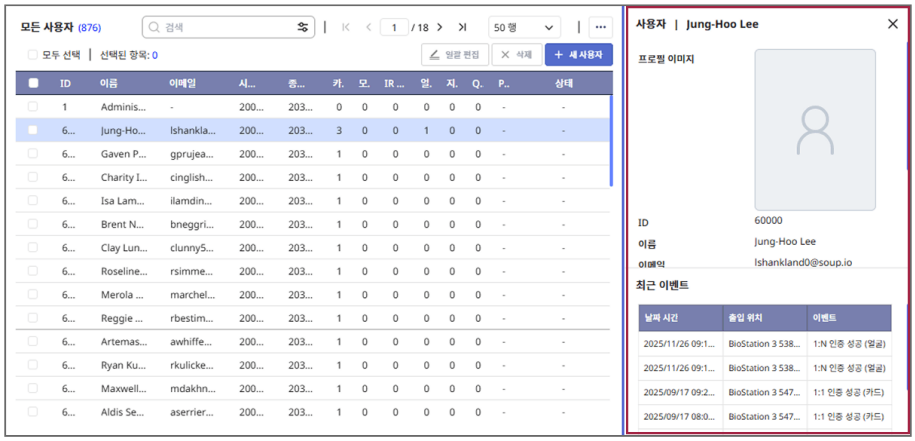
사용자의 출입 이력을 추적하고 확인하는 것은 보안을 강화하고 운영 효율성을 높이는 데 매우 중요합니다. 출입 이력을 통해 보안 위협을 예방하고, 운영을 최적화할 수 있습니다. 출입 권한이 없는 장소나 허가되지 않은 시간에 출입을 시도한 사용자를 파악할 수 있습니다. 이를 통해 보안 위협에 신속하게 대응할 수 있습니다. 반복적인 인증 실패나 비정상 시간대의 출입과 같은 이상 징후를 파악하여 보안 위협을 조기에 발견할 수 있습니다.

다음 단계에 따라 사용자의 출입 이력을 확인할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.

2. 사용자 목록에서 출입 이력을 확인하려는 사용자를 클릭하세요.

3. 화면 오른쪽에 선택한 사용자의 프로필 정보가 표시됩니다.



프리뷰 화면 아래에 **최근 이벤트** 섹션에서 해당 사용자의 출입 이력을 확인할 수 있습니다.

> **알아두기**
>
> - 실시간 출입 이벤트는 **모니터링** 페이지에서 확인할 수 있습니다. 자세한 내용은 이벤트 모니터링하기를 참고하세요.
> - 과거의 출입 이벤트는 **데이터** 페이지에서 확인할 수 있습니다. 자세한 내용은 데이터를 참고하세요.

사용자 정보 내보내기/가져오기

사용자 정보를 내보내거나 가져오기를 통해 이전 버전 또는 다른 서버의 사용자 정보를 활용할 수 있습니다.

CSV 내보내기/가져오기

선택한 사용자 정보를 CSV 파일로 저장하거나, 저장된 CSV 파일을 불러올 수 있습니다. CSV 파일을 이용하여 간편하게 사용자 정보를 옮길 수 있습니다.

> **알아두기**
>
> - **BioStar X**에 추가하지 않은 커스텀 사용자 필드 정보가 있다면 CSV 파일을 올바르게 가져올 수 없습니다. 커스텀 사용자 필드를 추가하는 방법은 서버 상세 설정하기를 참고하세요.
> - 영어와 한국어를 제외한 다른 언어로 사용자 정보가 입력된 경우 CSV 파일을 UTF-8로 저장하세요.

CSV 내보내기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 CSV 파일로 저장할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **내보내기** → **CSV**를 선택하세요.



4. **CSV 내보내기** 창이 나타나면, **내보내기 사유**(선택 사항)를 입력하고 **다운로드** 버튼을 클릭하세요.



5. 로컬의 원하는 경로에 CSV 파일을 저장하세요.

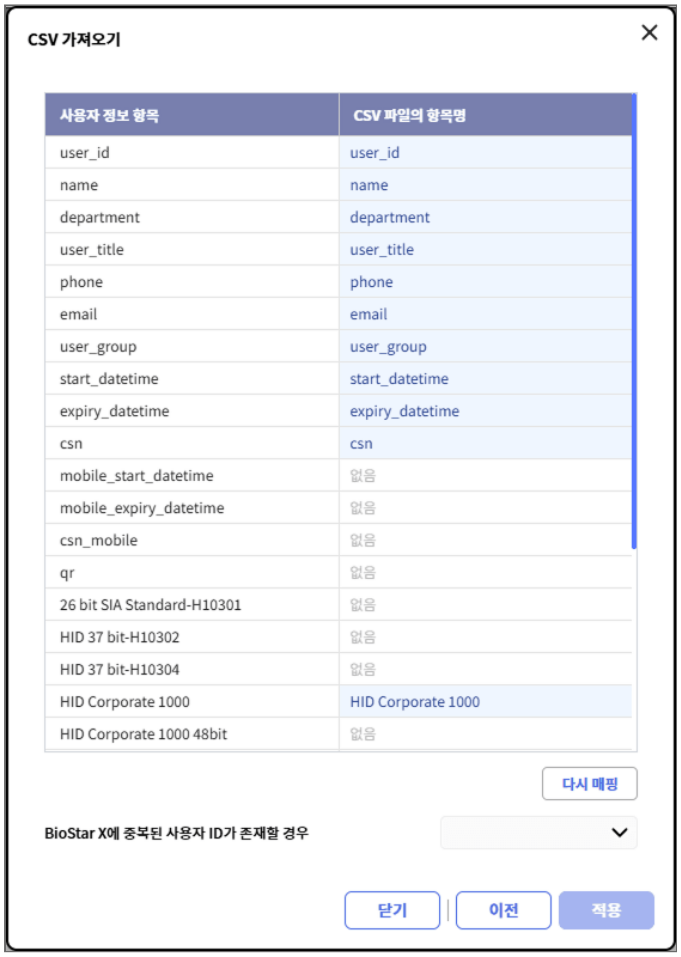
> **알아두기**
> **내보내기 사유**는 필수 입력 항목이 아닙니다. 내보내기 사유는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

CSV 가져오기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **가져오기** → **CSV**를 선택하세요.
3. 로컬에 저장된 CSV 파일을 선택하세요.
4. **CSV 가져오기** 창에서 **가져오기 시작 행**을 설정하고 **다음** 버튼을 클릭하세요.



5. CSV 파일의 사용자 데이터 필드와 **BioStar X**의 사용자 데이터 필드가 자동으로 매핑되어 나타납니다. **다시 매핑**을 클릭하면 이름이 동일한 필드끼리 재매핑됩니다.



6. **BioStar X**에 이미 사용자 ID가 등록된 사용자 데이터를 유지할 지 CSV 파일의 정보로 덮어쓰기할 지 선택하고 **적용**을 클릭하세요.



CSV 파일의 정보를 가져오는 중 오류가 발생했다면 오류가 발생한 CSV 데이터만 다시 확인하여 업로드할 수 있습니다.

알아두기

- CSV 가져오기를 통해 모바일 출입 카드를 발급할 수 있습니다. 레귤러 사이트를 사용할 경우 가져오기가 완료되면 에어팝 포털(Airfob Portal)에서 모바일 출입 카드당 1개의 크레딧이 차감됩니다. 모바일 출입 카드를 발급하지 않으려면 매핑을 해제하세요.
- CSV 파일에 **BioStar X**에 이미 등록된 사용자에게 발급한 모바일 출입 카드와 **동일한** 데이터가 존재할 경우 데이터 유지 또는 덮어쓰기할 수 있으며, 이 경우 기존 모바일 출입 카드가 유지됩니다.
- CSV 파일에 **BioStar X**에 이미 등록된 사용자에게 발급한 모바일 출입 카드와 **다른** 데이터가 존재할 경우 데이터를 유지하면 기존 모바일 출입 카드가 유지되며, 덮어쓰기할 경우 해당 사용자에게 새 모바일 출입 카드가 발급됩니다.
- CSV 가져오기를 통해 모바일 출입 카드를 발급할 때 다이나믹 사이트를 사용할 경우 `mobile_start_datetime`과 `mobile_expiry_datetime` 필드의 값을 반드시 입력해야 합니다.
- **BioStar X** QR은 CSV 가져오기를 통해 발급할 수 없습니다.
- CSV 가져오기를 통해 사용자의 얼굴을 등록할 수 있습니다. 자세한 내용은 얼굴 일괄 등록하기를 참고하세요.
- CSV 가져오기를 통해 사용자의 PIN을 등록할 수 있습니다. 자세한 내용은 PIN 등록하기를 참고하세요.
- 저장된 CSV 파일에 매칭되지 않는 열을 추가하면 **BioStar X**에서 파일을 가져올 수 없습니다.
- 사용자 이름의 맨 앞에 `&@~` 연속으로 시작하는 경우 해당 사용자는 CSV 항목 가져오기에 실패합니다.
- 유효 기간(만료 일시)은 2037-12-31 23:59:59까지 설정할 수 있습니다. 이 날짜를 초과하는 값이 있는 항목은 가져오기에 실패합니다.
- 내보낸 CSV 파일은 Excel 등 표 계산 프로그램에서 직접 열지 않는 것을 권장합니다. 사용자 이름이 `=` 문자로 시작하는 경우, 프로그램이 이를 수식으로 인식해 실제 값과 다르게 표시될 수 있습니다.

데이터 파일 내보내기/가져오기

외부 저장매체(USB)에 사용자 정보를 저장하여 **BioStar X**나 장치에서 가져올 수 있습니다. 최대 500,000명의 사용자 정보를 서버에서 장치로 옮기거나 장치에서 장치로 옮길 수 있습니다.

알아두기

- 오래된 펌웨어 버전을 사용하는 장치에서 내보내기한 데이터는 **BioStar X**로 불러올 수 없습니다. 항상 최신 버전의 펌웨어를 사용하세요.
- 서로 다른 지문 템플릿 형식을 사용할 경우 데이터를 가져올 수 없습니다. 예를 들어, 슈프리마 지문 템플릿 형식을 사용하는 장치에서 내보내기한 데이터를 ISO 지문 템플릿 형식을 사용하는 장치에서 가져올 수 없습니다.
- 사용자 데이터를 가져올 때 **BioStar X** 서버에 등록한 지문과 얼굴 크리덴셜이 이미 존재할 경우 기존 데이터에 덮어씌워집니다.
- 오래된 펌웨어 버전을 사용하는 장치의 데이터를 불러올 수 없습니다. 장치의 펌웨어를 호환하는 버전으로 업그레이드하세요.

  ▼ 호환하는 장치와 펌웨어 버전 보기

  – BioStation 2 펌웨어 1.9.0 이상
  – BioStation A2 펌웨어 1.8.0 이상
  – FaceStation 2 펌웨어 1.4.0 이상
  – FaceStation F2 펌웨어 2.2.0 이상
  – X-Station 2 펌웨어 1.0.0 이상
  – BioStation 3 펌웨어 1.3.1 이상
  – BioStation 2a 펌웨어 1.0.0 이상

데이터 내보내기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 내보낼 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **내보내기** → **데이터 파일**을 선택하세요.



4. **데이터 파일로 내보내기** 창에서 데이터 파일을 적용할 장치를 선택하세요.



5. **내보내기 사유**(선택 사항)를 입력하고 **적용** 버튼을 클릭하세요.
6. 로컬의 원하는 경로에 데이터 파일을 저장하세요.

> **알아두기**
>
> - 데이터 파일 내보내기는 사용자 정보 중 프로필 사진, ID, 이름, 유효 기간, 출입 그룹, PIN, 개인인증모드, 크리덴셜(얼굴, 지문, 카드, 모바일 카드, 얼굴, QR/Barcode), 1:1 보안 등급 정보를 파일 형태로 저장합니다.
> - 데이터 파일을 적용할 장치를 정확하게 선택하지 않으면 해당 장치에서 데이터 파일을 인식할 수 없습니다.
> - **내보내기 사유**는 필수 입력 항목이 아닙니다. 내보내기 사유는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

> **주의**
>
> BioStar X에서 내보낸 파일을 장치로 가져오려면, 현재 장치에서 인식할 수 있도록 파일 이름을 아래와 같이 변경해야 합니다. 파일명 형식은 향후 장치 펌웨어 업데이트를 통해 자동 인식하도록 조정될 예정입니다.
>
> ***BioStarX**_YYYYMMDD_HHMMSS.tgz* → ***BioStar2**_YYYYMMDD_HHMMSS.tgz*
>
> - **내보내기 사유**는 필수 입력 항목이 아닙니다. **내보내기 사유**는 **설정** → **시스템** → **감사 추적**에서 기록을 확인할 수 있습니다.

데이터 가져오기

1. **런처** 페이지에서 **사용자**를 클릭하세요.

2. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **가져오기** → **데이터 파일**을 선택하세요.



3. 로컬에 저장된 데이터 파일(*.tgz*)을 선택하세요.

데이터 파일을 가져오는데 성공하면 화면에 메시지가 나타납니다.

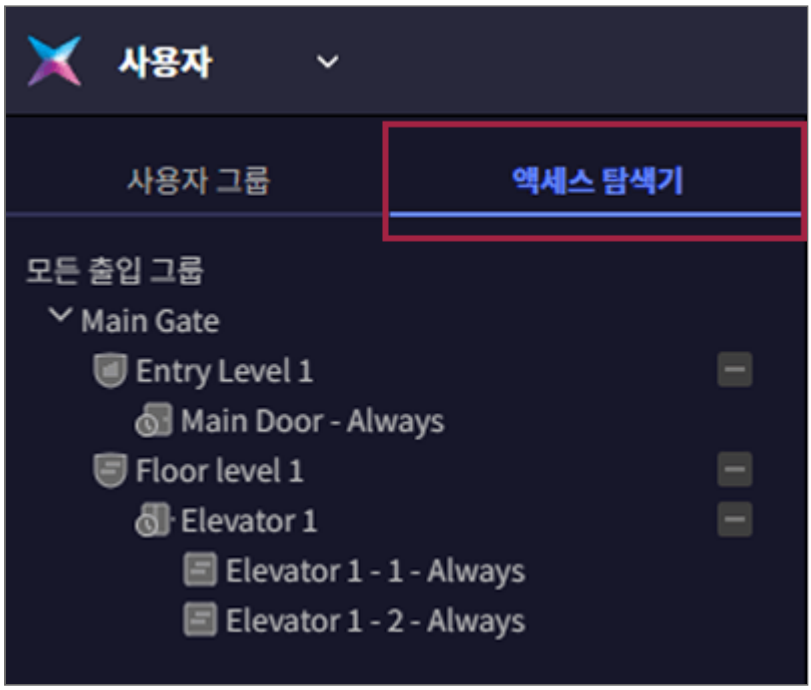
출입 그룹 관리하기

출입 그룹을 기준으로 사용자를 조회 및 관리 방법을 안내합니다. **액세스 탐색기**를 사용하여 출입 그룹별로 등록된 사용자를 확인하고, 트리 구조를 통해 출입 권한 계층을 탐색할 수 있습니다.

> **알아두기**
> **액세스 탐색기**에서 출입 그룹에 속한 출입문이나 층을 확인하려면 출입 통제 기능을 미리 설정해야 합니다. 자세한 내용은 출입 통제 설정하기를 참고하세요.

출입 그룹별 사용자 확인하기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 트리 구조 메뉴에서 **액세스 탐색기** 탭을 클릭하세요.



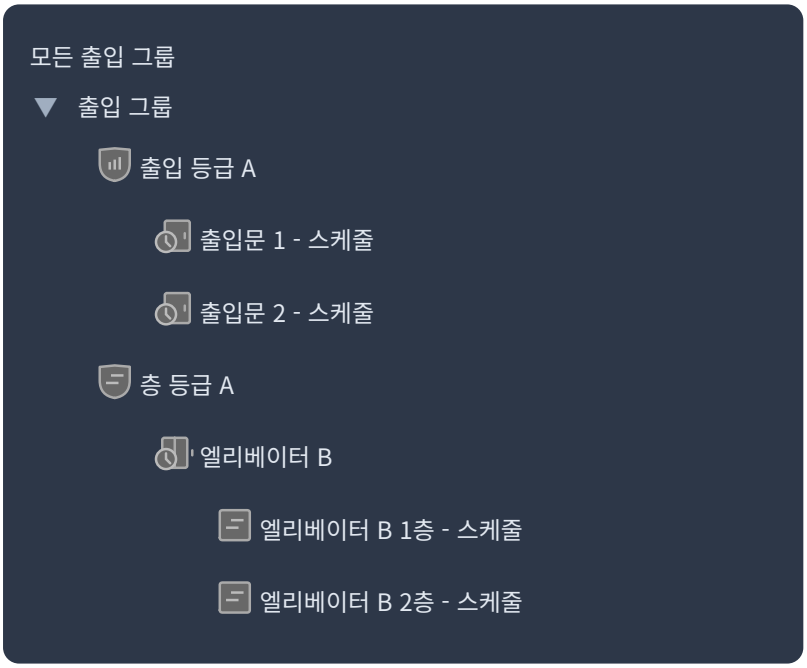
3. **모든 출입 그룹**에서 원하는 출입 권한 그룹을 클릭하세요.

선택한 출입 권한 그룹에 속한 사용자를 사용자 목록에서 확인할 수 있습니다.

> **알아두기**
>
> 출입 그룹 하위의 출입 등급 또는 층 등급을 확장하거나 축소하려면 ＋ 또는 － 버튼을 클릭하세요.

트리 구조 알아보기

트리 구조 메뉴는 아래와 같은 구조로 구성되어 있습니다.



- **출입 그룹**은 출입 등급, 층 등급, 사용자 그룹, 사용자를 포함하는 상위 계층입니다. **출입 그룹**을 통해 출입 권한을 관리할 수 있습니다. 출입 그룹 생성에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.
- **출입 등급**은 사용자가 출입할 수 있는 시간을 설정하고, 이 시간 동안 출입문에 출입할 수 있는 권한을 부여합니다. 출입 등급 생성에 대한 자세한 내용은 출입 등급 관리하기를 참고하세요.
- **층 등급**을 통해 사용자가 엘리베이터를 이용해 출입할 수 있는 층을 관리할 수 있습니다. 층 등급 생성에 대한 자세한 내용은 층 등급 관리하기를 참고하세요.
- **스케줄**은 출입 및 휴일 스케줄을 설정하여 출입 통제와 근태 관리를 효율적으로 운영하는 기능입니다. 스케줄 등록에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
- **엘리베이터**를 등록하고 엘리베이터를 통해 출입할 수 있는 층을 관리할 수 있습니다. 엘리베이터 등록에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.

> **알아두기**
>
> 엘리베이터 등록 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

다중 인증으로 로그인하기

BioStar X에 로그인 시 보안 강화를 위해 **다중 인증** 기능을 사용할 수 있습니다. **다중 인증 로그인** 기능을 활성화하면 사용자 아이디와 비밀번호 조합에 지문 스캐너를 통한 지문 인증 단계를 추가합니다.

알아두기

- **다중 인증 로그인** 기능을 사용하려는 사용자는 지문 정보를 등록하고, 아이디 및 비밀번호, 권한 등급을 모두 설정해야 합니다.
- **다중 인증 로그인** 기능을 사용하려면 **BioStar X** 클라이언트 PC에 다중 인증 로그인을 지원하는 지문 스캐너를 연결해야 합니다. 지문 스캐너로 지원하는 장치는 아래 목록을 참고하세요.
  - BioMini
  - BioMini Plus 2
  - BioMini Slim 2
- 디렉토리 서비스 계정으로 **BioStar X 로그인에 사용** 옵션을 사용한다면 **다중 인증 로그인** 기능을 사용할 수 없습니다.
- **다중 인증 로그인**을 설정한 관리자는 출입 통제 이외의 **BioStar X** 서비스(근태 관리 및 비디오)에 최초 인증할 수 없습니다. 해당 서비스를 사용하려면 **다중 인증 로그인** 설정을 해제한 후 로그인하세요. 이후 다시 **다중 인증 로그인** 설정을 활성화할 수 있습니다.

주의

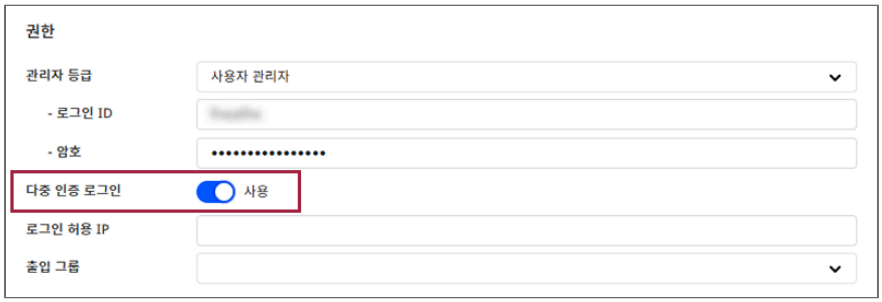
- 전체 관리자(ID 1번) 계정에 다중 인증 기능을 설정한 후, 지문 인증 기능을 사용할 수 없게 되면 해당 계정으로 더 이상 로그인할 수 없으므로 주의하세요.
- 지문 인증을 사용해 로그인할 수 없다면 슈프리마 기술 지원팀(CS@suprema.co.kr)으로 문의하세요.

다중 인증 설정

다중 인증 로그인을 설정하려면 다음 단계를 따르세요.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 **다중 인증 로그인**을 설정하려는 사용자를 더블 클릭하세요.

   또는 사용자를 선택하고 오른쪽 화면에 표시되는 프로필에서 **자세히 보기** 버튼을 클릭하세요.
3. 사용자 프리뷰 화면이 나타나면 **권한** 섹션에서 **다중 인증 로그인** 항목을 **사용**으로 설정하세요.



4. 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

다중 인증 설정을 완료합니다.

다중 인증 일괄 설정

> **시작하기 전에**
>
> 다중 인증 로그인 기능을 사용하려면 다음 조건을 만족해야 합니다.
> - 해당 사용자의 지문 인증 수단이 등록되어 있어야 합니다.
> - **권한 등급**, **로그인 ID**, **암호**가 설정되어 있어야 합니다. 자세한 내용은 사용자 권한 설정하기를 참고하세요.

일괄 편집 기능을 사용해 여러 명의 사용자에게 **다중 인증 로그인** 기능을 적용할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 다중 인증을 설정하려는 사용자의 가장 왼쪽에 체크박스를 클릭하세요.
3. 화면 오른쪽 상단의 **일괄 편집** 버튼을 클릭하세요.
4. 일괄 편집 창이 나타나면 **권한** 섹션에서 **다중 인증 로그인** 옵션의 체크박스를 클릭하고 **사용**으로 설정하세요.



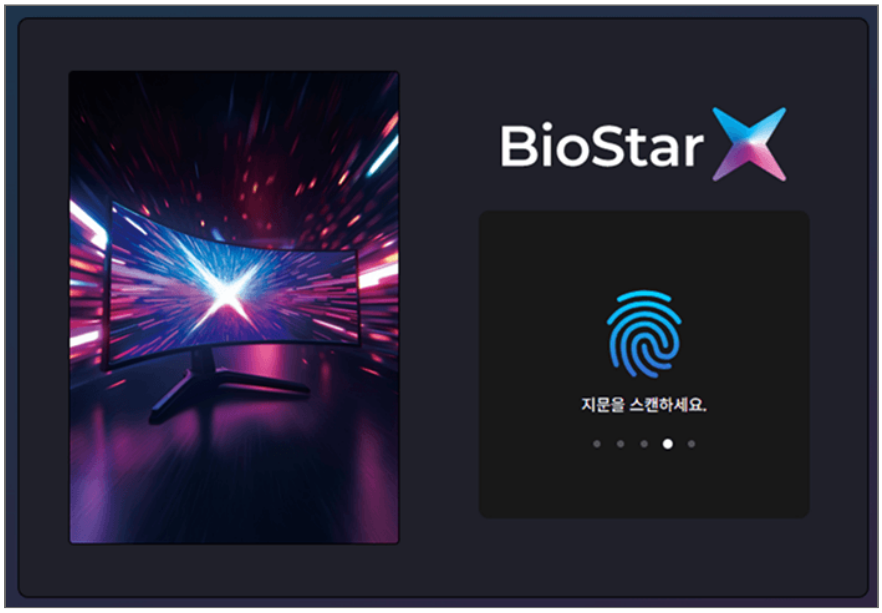
5. 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

선택한 다수의 사용자에 대한 다중 인증 설정을 완료합니다.

> **알아두기**
>
> 선택한 사용자 중 **다중 인증 로그인** 기능을 활성화하는 데 필요한 조건을 만족하지 않는 사용자는 팝업 메시지에 **적용할 수 없는 사용자** 목록을 통해 확인할 수 있습니다. 설정에 필요한 조건을 확인하고 다시 시도하세요.

다중 인증으로 로그인

1. 웹 브라우저를 통해 **BioStar X** 로그인 화면으로 접속하세요.
2. 사용자 아이디와 비밀번호를 입력한 후 **로그인** 버튼을 클릭하세요.
3. 지문 입력 화면이 나타나면 지문 스캐너를 통해 지문을 스캔하세요.



로그인을 완료합니다.

알아두기

- 지문 스캔 제한 시간은 18초로 고정되어 있으며, 변경할 수 없습니다.
- 최대 3회까지 연속으로 지문을 스캔할 수 있으며, 3회 동안 지문이 정확히 스캔 되지 않으면 인증 실패 처리됩니다.
- 인증에 실패했다면 **재시도** 버튼을 클릭해 지문 인증을 재시도하세요. 최대 2회까지 재시도할 수 있습니다. 재시도 횟수 동안 인증에 실패한다면 로그인 초기 화면으로 전환됩니다.

얼굴 일괄 등록하기

사용자의 얼굴을 일괄 등록할 수 있는 방법을 안내합니다. CSV 파일로 가져오기 기능을 사용하거나 사용자 아이디와 일치하는 파일 이름을 가진 얼굴 사진을 불러와 등록해 여러 명의 사용자 얼굴을 한 번에 등록할 수 있습니다. 또는 여러 명의 사용자에게 이메일로 얼굴 등록 링크를 전송해 모바일 장치에서 직접 얼굴을 등록할 수도 있습니다.

시작하기 전에

얼굴 일괄 등록을 시작하기 전에 사용자의 얼굴 이미지를 준비하세요.

- 얼굴 이미지 파일은 한 폴더에 모두 저장되어 있어야 합니다. 얼굴 이미지 파일의 이름은 사용자 아이디와 동일해야 합니다.
- 지원하는 이미지 파일의 크기는 최대 10MB입니다.
- 지원하는 이미지 파일의 형식은 JPG, JPEG, PNG입니다.

CSV 파일 가져오기로 등록

CSV 가져오기 기능으로 사용자의 얼굴을 일괄 등록할 수 있습니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 얼굴을 등록할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.

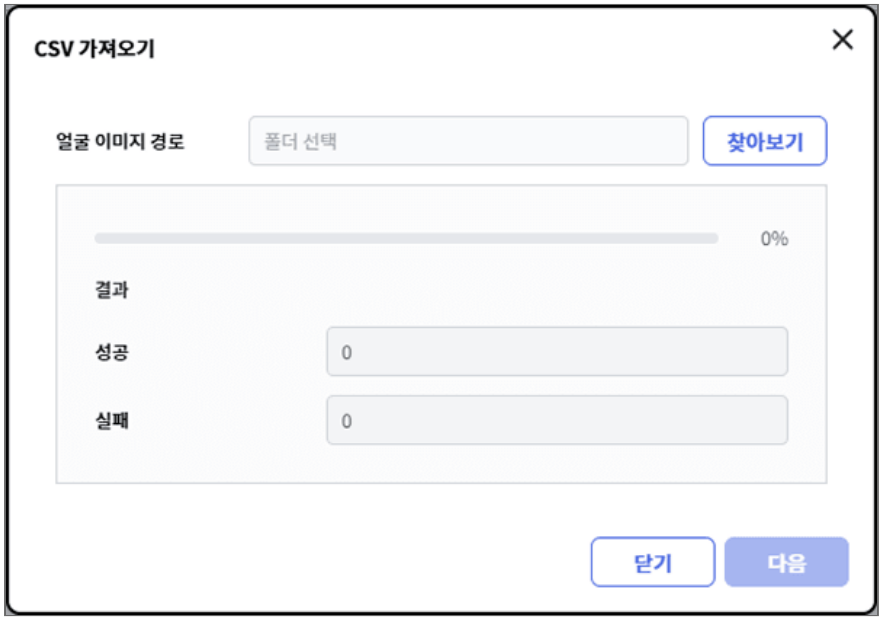
3. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **내보내기** → **CSV**를 선택하세요.
4. CSV 내보내기 창이 나타나면 **다운로드** 버튼을 클릭하세요.
5. 로컬의 원하는 경로에 CSV 파일을 저장하세요.
6. CSV 파일을 열어 `face_image_file1`, `face_image_file2` 열을 추가하세요.
7. 추가한 열에 얼굴 이미지의 파일명을 확장자를 포함해 입력하고 저장하세요.
8. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **가져오기** → **CSV**를 선택하세요.
9. 수정한 CSV 파일을 선택하세요.
10. CSV 가져오기 창이 나타나면 **가져오기 시작 행**을 설정하고 **다음** 버튼을 클릭하세요.



11. **BioStar X**에 이미 등록된 사용자 데이터를 유지할 지 CSV 파일의 정보로 덮어쓰기할 지 선택하고 **적용** 버튼을 클릭하세요.



12. **얼굴 이미지 경로** 항목에서 **찾아보기** 버튼을 클릭하세요.



13. 얼굴 이미지가 저장된 경로를 선택하고 **업로드** 버튼을 클릭하세요.

14. CSV 가져오기를 완료하려면 **다음** 버튼을 클릭하세요.

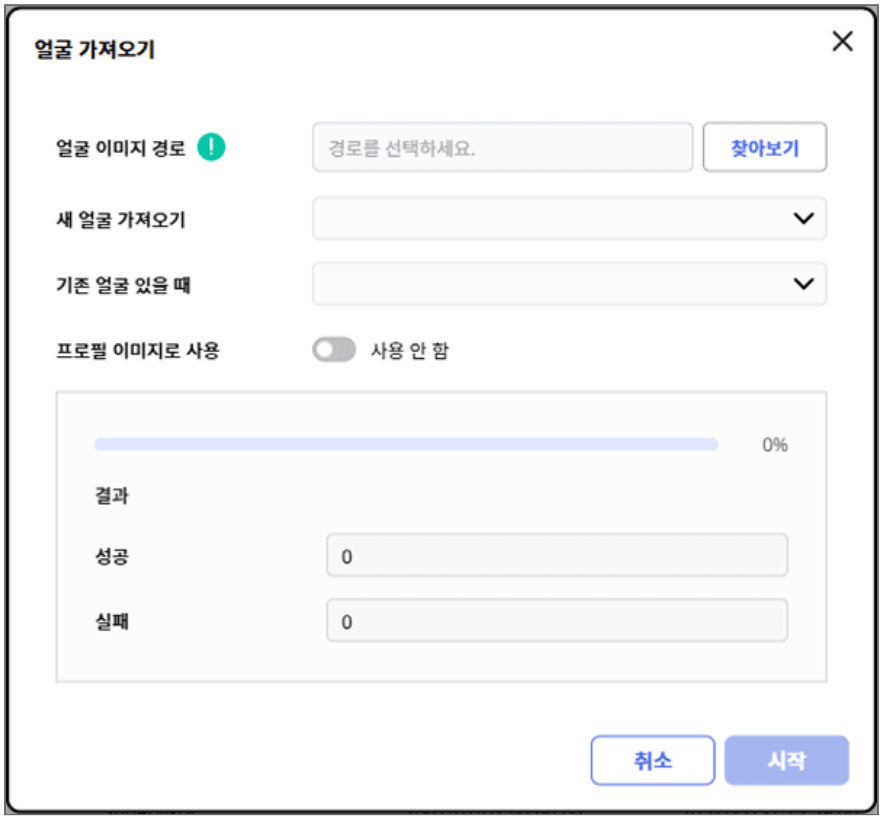
CSV 파일의 정보를 가져오는 중 오류가 발생했다면 오류가 발생한 CSV 데이터만 다시 확인하여 업로드할 수 있습니다.

> **알아두기**
> 가져올 CSV 파일과 얼굴 이미지 파일은 동일한 경로를 사용할 것을 권장합니다.

얼굴 가져오기

사용자 아이디와 일치하는 파일 이름을 가진 얼굴 사진을 불러와 얼굴 인증으로 등록할 수 있습니다. 시작하기 전에 사용자 얼굴 이미지 파일을 준비하세요. 얼굴 이미지 파일의 이름은 사용자 아이디와 동일해야 합니다.

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **가져오기** → **얼굴**을 선택하세요.
3. **얼굴 가져오기** 창이 나타나면 **찾아보기** 버튼을 클릭하세요.



4. 얼굴 이미지가 저장된 경로를 선택하세요.
5. **새 얼굴 가져오기** 옵션에서 얼굴 이미지를 불러올 방식을 선택하세요.
   - **파일 이름이 사용자 ID와 일치하는 이미지 불러오기**: 얼굴 이미지 파일명과 사용자 아이디가 일치하는 이미지를 가져옵니다.
   - **파일 이름이 사용자 ID와 일치하는 이미지 불러오기+ 이미지 파일 이름을 사용자 ID로 사용하여 신규 사용자 추가하기**: 등록된 사용자 아이디와 얼굴 이미지 파일명이 일치하면 이미지를 불러오고, 일치하지 않으면 해당 파일 이름을 사용자 아이디로 사용해 신규 사용자를 생성하고 얼굴 인증 수단으로 등록합니다.
6. **기존 얼굴 있을 때** 옵션에서 **데이터 유지** 또는 **덮어쓰기**를 선택하세요.
   - **데이터 유지**: 등록된 사용자의 얼굴 이미지를 유지합니다.

- **덮어쓰기**: 등록된 사용자의 얼굴 이미지를 새로 가져오는 얼굴 이미지로 덮어씁니다.

7. 가져오는 얼굴 이미지를 프로필 이미지로 사용하려면 **프로필 이미지로 사용** 옵션을 클릭해 활성화하세요.
8. **시작** 버튼을 클릭하세요.

얼굴 사진 파일을 가져오는 중 오류가 발생하면 오류가 발생한 사진의 목록이 나타납니다. 목록을 확인하고 다시 시도하세요.

> **알아두기**
> 얼굴 이미지는 한 명의 사용자 아이디당 1개까지 가져올 수 있습니다.

모바일 장치로 얼굴 등록

사용자에게 이메일로 얼굴 등록 링크를 전송할 수 있습니다. 사용자는 모바일 장치에서 해당 링크로 접속하여 얼굴을 직접 등록할 수 있습니다.

시작하기 전에

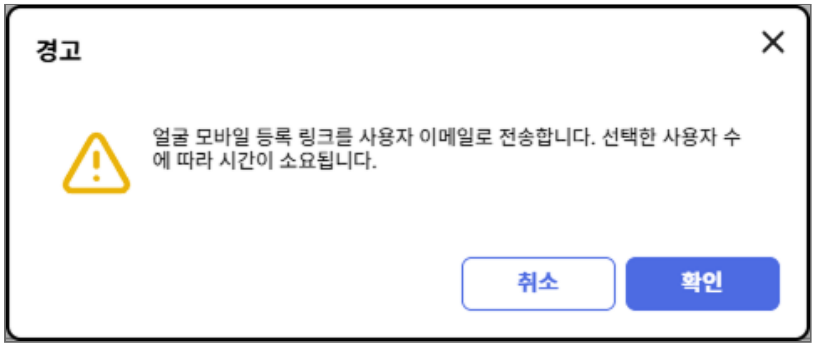
- 모바일 얼굴 등록 기능을 사용하기 전에 SMTP 설정을 포함한 이메일 정보 설정을 완료하세요. 자세한 내용은 이메일 설정하기를 참고하세요.
- 모바일 얼굴 등록 기능은 **리모트 액세스** 기능을 활성화해야 사용할 수 있습니다. **리모트 액세스**에 대한 자세한 내용은 리모트 액세스 설정하기를 참고하세요.

얼굴 등록 링크 전송

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 얼굴을 등록할 사용자의 체크박스를 클릭하세요. 1명 이상의 사용자를 선택할 수 있습니다.
3. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **얼굴 등록 모바일 링크 전송**를 선택하세요.



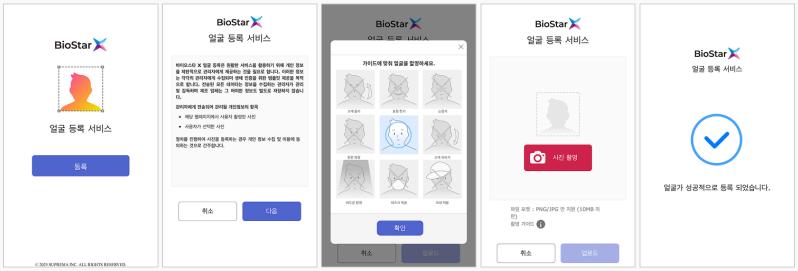
4. 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.



선택한 사용자의 이메일로 얼굴 등록 링크를 전송합니다. 사용자가 업로드 완료하면 사용자 정보에 얼굴 정보가 추가됩니다.

알아두기

- **감사 추적**에서 이메일 전송 성공 여부를 확인할 수 있습니다. 자세한 내용은 감사 추적 관리하기를 참고하세요.
- 얼굴 등록 모바일 링크를 통해 접속하는 페이지에 표시되는 언어는 모바일 기기에서 사용하는 브라우저의 언어 설정을 따릅니다.
- 사용자가 전송 받은 얼굴 등록 모바일 링크로 접속하면 아래와 같이 얼굴 등록 서비스가 실행됩니다. 화면의 안내에 따라 진행하세요.



- 지원하는 이미지 파일의 크기는 최대 10MB입니다.
- 지원하는 이미지 파일의 형식은 JPG, JPEG, PNG입니다.
- 전송된 얼굴 등록 모바일 링크는 24시간 뒤 만료됩니다.
- 얼굴 사진을 업로드하여 얼굴 모바일 등록에 성공하면 등록 성공 메시지가 화면에 나타납니다. 등록에 실패한 경우 등록 실패 메시지와 실패 사유가 표시되며, 사용자는 다른 사진을 이용하여 얼굴 등록을 다시 시도할 수 있습니다.

얼굴 마이그레이션

BioStar X 이전 버전에서 등록한 얼굴을 최신 알고리즘으로 업그레이드하여 인식 성능을 향상할 수 있습니다. 사용자를 동기화할 때 얼굴에서 이미지를 제외한 템플릿만 전송하도록 프로토콜을 개선하여 동기화 소요 시간을 대폭 단축하고 개인 정보 관련 문제 발생을 방지할 수 있습니다.

시작하기 전에

얼굴 마이그레이션 기능을 실행하기 전에 다음 사항을 확인하세요.

얼굴 마이그레이션이란?

BioStar X 서버에 이미 저장되어 있던 사용자의 이미지로 두 가지 유형의 얼굴 템플릿을 생성하는 기능입니다. 사용자 동기화 시 얼굴을 템플릿으로만 동기화하려면 **얼굴 마이그레이션**을 진행해야 합니다.

지원 장치 및 펌웨어 버전

얼굴을 템플릿으로 동기화할 수 있는 장치 목록은 아래 목록을 참고하세요.

- BioStation 3 Max 펌웨어 v1.0.0 이상
- BioEntry W3 펌웨어 v1.0.0 이상
- BioStation 3 펌웨어 v1.3.1 이상
- FaceStation F2 펌웨어 v2.2.0 이상

▼ **FaceStation F2 v1.x.x 펌웨어 지원 중단 안내**

BioStar X는 사용자의 얼굴을 장치에 동기화할 때 템플릿만 전송하도록 변경하여 동기화 성능을 최적화했습니다. 따라서 장치에서만 템플릿을 추출할 수 있는 FaceStation F2 v1.x.x 펌웨어의 지원이 중단됩니다. 현재 FaceStation F2의 1.x.x 버전 펌웨어를 사용 중인 경우 **BioStar X**를 사용하기 위해서는 FaceStation F2를 최신 펌웨어로 업그레이드하여 사용하세요.

최신 펌웨어는 슈프리마 다운로드 센터에서 다운로드할 수 있습니다.

얼굴 템플릿 타입 관련 유의 사항

BioStation 3 Max 와 BioEntry W3, BioStation 3, FaceStation F2는 서로 얼굴 템플릿 타입이 다릅니다.

- **NPU 타입**: BioStation 3 Max, BioEntry W3, BioStation 3
- **GPU 타입**: FaceStation F2

- **얼굴 템플릿 타입이 다른 장치 간 동기화 소요 시간**

  얼굴 마이그레이션을 하기 전, FaceStation F2만 연결하여 사용하던 환경에 BioStation 3 Max나 BioEntry W3, BioStation 3를 추가하여 동기화하면 템플릿 타입이 달라 이미지에서 NPU 타입 템플릿을 추출하므로, 서버에 등록된 얼굴의 개수에 따라 상당한 시간이 소요될 수 있습니다.

- **BioStar X에서 얼굴 등록 권장**

  장치의 **얼굴 이미지 저장하기** 옵션을 사용하지 않는 상태에서 얼굴을 등록한 경우, **BioStar X**에는 템플릿만 동기화되기 때문에 얼굴 템플릿 타입이 다른 장치에 동기화할 수 없게 되므로 얼굴은 **BioStar X**에서 등록하는 것을 권장합니다.

장치 관련 유의 사항

BioStar X에서 내보낸 사용자 데이터 파일은 이미지 없이 템플릿만 가지고 있으므로 기존 펌웨어를 사용 중인 FaceStation F2 및 BioStation 3에 사용자 데이터 파일을 가져올 수 없습니다.

따라서 FaceStation F2 및 BioStation 3에서 데이터 파일 내보내기 시에는 아래의 버전 이상에서만 데이터 파일을 내보낼 수 있습니다.

- FaceStation F2 펌웨어 v2.2.0 이상
- BioStation 3 펌웨어 v1.3.1 이상

주의

FaceStation F2, BioStation 3를 사용한다면 최신 버전의 펌웨어로 업그레이드할 것을 권장합니다. 최신 펌웨어는 슈프리마 다운로드 센터에서 다운로드할 수 있습니다.

마이그레이션하기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 ••• 버튼을 선택하고 **얼굴 마이그레이션** 버튼을 클릭하세요.



3. 경고 팝업창의 내용을 확인하고 **계속**을 클릭하세요.



얼굴 마이그레이션을 진행합니다. 얼굴 마이그레이션을 완료하면 총 얼굴 수, 성공 및 실패 건수를 확인할 수 있는 팝업창이 나타납니다.

- 마이그레이션 성공 후, 장치에 사용자 정보를 동기화하여 변경 사항을 적용하세요. 장치에 사용자 정보를 전송하는 방법에 대한 자세한 내용은 장치로 사용자 정보 전송하기를 참고하세요.
- 얼굴 마이그레이션에 실패하면, 실패한 사용자 목록을 CSV 파일로 다운로드할 수 있습니다. 마이그레이션에 실패한 얼굴을 일괄 삭제하려면 **삭제** 버튼을 클릭하세요.

알아두기

- 이 기능은 사용자 아이디가 1인 관리자 계정만 사용할 수 있습니다.
- 마이그레이션을 진행하는 동안 현재 페이지를 벗어나지 마세요.
- 사용자에 따라 등록된 얼굴 이미지의 크기가 클수록 템플릿 생성 시 시간이 다소 오래 소요될 수 있습니다.
- 얼굴 1,000개 기준 소요 시간은 약 18분이며 서버의 성능에 따라 달라질 수 있습니다.
- 사용자의 얼굴 이미지를 서버에 저장하지 않고 템플릿만 저장하는 방법에 대한 자세한 내용은 서버 상세 설정하기를 참고하세요.

비상 개방 권한 설정하기

비상 상황에서 특정 사용자가 모든 출입문에 접근할 수 있도록 비상 개방 권한을 설정할 수 있습니다. 비상 개방 권한이 설정된 카드로 출입문을 개방하면, 해당 출입문은 열린 상태를 유지하여 누구나 출입할 수 있습니다.

시작하기 전에

비상 개방 권한을 설정하기 전에 카드 크리덴셜을 우선 추가해야 합니다. 카드 크리덴셜을 추가 방법에 대한 자세한 내용은 출입 카드 등록하기를 참고하세요.

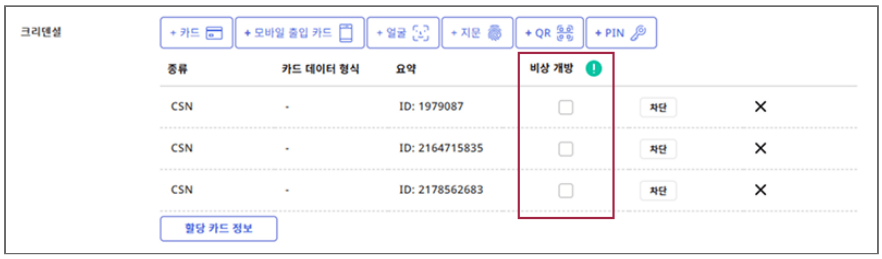
알아두기

- 카드 크리덴셜을 제외한 다른 크리덴셜은 지원하지 않습니다.
- 스마트 카드(AoC), ToM 모바일 액세스 카드(ToM AoC)를 제외한 모든 카드 크리덴셜을 지원합니다.
- 장치에 따라 비상 개방 기능을 지원하지 않을 수 있습니다. 지원하는 장치와 펌웨어 버전은 아래를 참고하세요.
  - BioStation 3 Max 펌웨어 v1.0.0 이상
  - XPass Q2 펌웨어 v1.0.0 이상
  - BioStation 3 펌웨어 v1.4.0 이상

비상 개방 권한 설정하기

1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 사용자 목록에서 비상 개방 권한을 설정할 사용자를 더블 클릭하세요.

   또는 사용자를 선택하고 오른쪽 화면에 표시되는 프로필에서 **자세히 보기** 버튼을 클릭하세요.
3. 사용자 상세 화면이 나타나면 **크리덴셜** 섹션으로 이동하세요.
4. 비상 개방을 허용할 카드 크리덴셜의 **비상 개방** 항목의 체크박스를 클릭하세요.



5. 경고 메시지가 표시되면 내용을 확인하고 **계속** 버튼을 클릭하세요.



6. 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

비상 개방 권한 설정을 완료합니다.

주의

사용자는 비상 개방 권한이 설정된 출입 카드로 모든 출입문을 개방할 수 있습니다.

알아두기

- 비상 개방 권한을 부여할 카드 크리덴셜은 하나 이상 선택할 수 있습니다.
- 비상 개방 권한을 해제하려면 선택한 카드 크리덴셜의 **비상 개방** 항목의 체크박스를 다시 클릭하세요.

모니터링

BioStar X의 핵심 기능 중 하나인 **모니터링** 페이지에서 활용할 수 있는 기능에 대해 안내합니다.

런처 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요.

출입문 모니터링하기

출입문 모니터링은 보안 시스템의 핵심 기능 중 하나로, 출입문 상태를 실시간으로 확인하고 제어할 수 있습니다. 이 문서에서는 출입문과 엘리베이터, 고급 출입 통제를 모니터링하고 제어하는 방법을 안내합니다. 이를 통해 효율적인 보안 관리와 신속한 대응이 가능합니다.

상태 확인하기

출입문, 엘리베이터, 고급 출입 통제의 상태를 실시간으로 모니터링하여 보안 시스템을 안정적으로 운영할 수 있습니다. **모니터링**에서 제공하는 상태 아이콘을 통해 알람과 이상 상태를 한눈에 확인하고, 조치가 필요한 항목만 모아 즉시 대응하세요.

런처 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요. 화면 왼쪽 사이드바의 **출입문** 탭에서 각 항목의 상태를 확인할 수 있습니다.

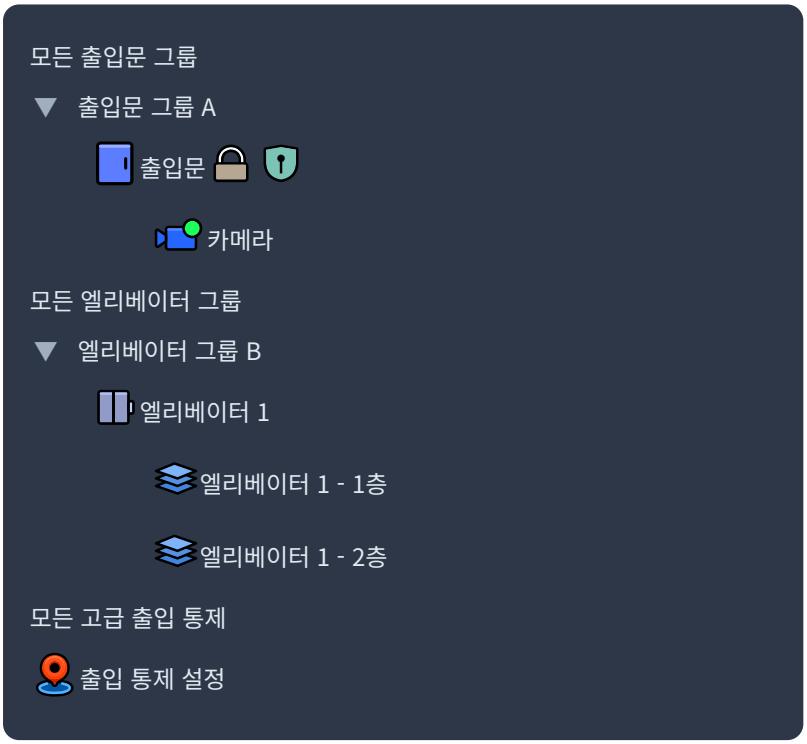
시작하기 전에

출입문과 연결된 장치를 올바르게 구성했는지 확인하세요. 장치가 네트워크에 연결되어 있고, 최신 펌웨어로 업데이트되어 있는지 점검하는 것이 중요합니다. 문제가 발생할 경우, 장치의 전원 상태와 네트워크 연결 상태를 먼저 확인하는 것이 좋습니다.

> **알아두기**
>
> - 장치 추가 및 구성에 대한 자세한 내용은 장치 관리하기를 참고하세요.
> - 출입문 추가 및 구성에 대한 자세한 내용은 출입문 관리하기를 참고하세요.
> - 출입문의 상태를 모니터링하거나 제어하려면 **로그 업로드** 기능이 활성화되어 있어야 합니다. 이 기능은 **설정** → **시스템** → **서버** 메뉴 경로의 **일반** 섹션에서 활성화할 수 있습니다.
> - VMS 서버와 연동해 카메라를 출입문과 연결하는 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

트리 구조 알아보기

화면 왼쪽 사이드바의 **출입문** 탭에서 트리 구조는 아래와 같은 구조로 구성되어 있습니다.



알아두기

- 장치 추가 및 구성에 대한 자세한 내용은 장치 관리하기를 참고하세요.
- 출입문 추가 및 구성에 대한 자세한 내용은 출입문 관리하기를 참고하세요.
- 엘리베이터 추가 및 구성에 대한 자세한 내용은 엘리베이터 관리하기를 참고하세요.
- 고급 출입 통제 설정에 대한 자세한 내용은 고급 출입 통제 설정하기를 참고하세요.
- 출입문과 카메라를 연동하려면 비디오 규칙 설정하기를 참고하세요.

상태 확인하기

연결 오류 및 알람 확인

출입문 또는 엘리베이터 상태를 확인하여 정상 작동 여부를 확인할 수 있습니다. 각 아이콘별 상태는 아래를 참고하세요.

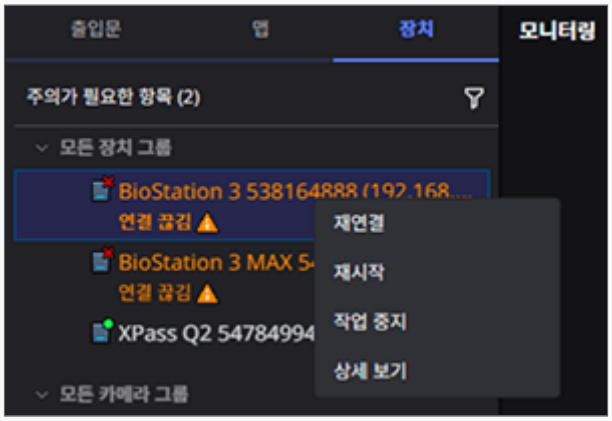
상태 아이콘	설명
⚠	장치 연결 끊김, 멀티 커뮤니케이션 서버 오류, 동기화 오류 등 장치 이상 상태를 표시합니다.
🚨	출입문, 엘리베이터, 고급 출입 통제, AI 영상 분석 알람이 발생한 상태를 표시합니다.

팁

상태 아이콘을 클릭하면 툴팁을 통해서 상세 정보를 확인할 수 있습니다. 툴팁에 표시된 오류 메시지의 링크를 클릭하면 출입문 또는 엘리베이터와 연결된 장치 목록으로 이동할 수 있습니다.



해당 장치에서 마우스 오른쪽 버튼을 클릭하고, **재연결** 또는 **재시작** 옵션을 선택하세요.

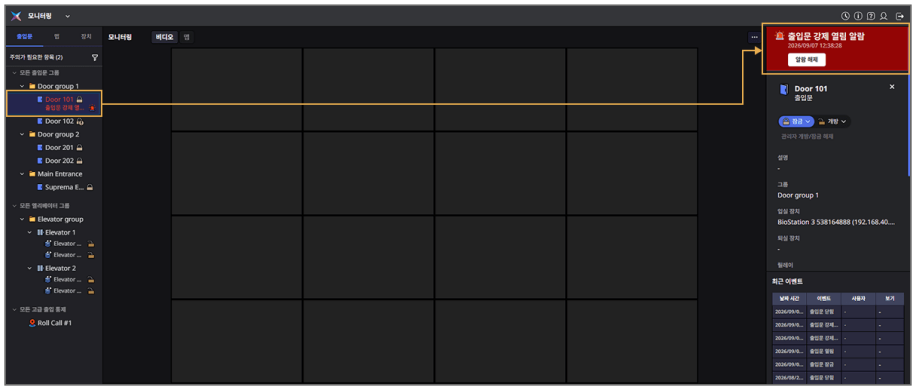


알아두기

- 출입문 또는 엘리베이터에서 발생하는 알람은 다음 설정을 통해 구성할 수 있습니다.
  - 출입문 알람 설정
  - 엘리베이터 알람 설정
  - 고급 출입 통제 설정
- 비디오 규칙에서 출입문과 카메라를 연결하여 알람을 설정할 수 있습니다. 비디오 규칙 설정에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.
- VMS 서버와 연동 시 영상에 대한 AI 이벤트 알람을 설정하면 **BioStar X**로 알람을 전송할 수도 있습니다. 자세한 내용은 VMS 서버의 매뉴얼을 참고하세요.
- 알람 해제에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

미리보기 패널에서 알람 확인

출입문 탭에서 알람( ) 아이콘이 표시된 출입문, 엘리베이터 또는 고급 출입 통제를 선택하면 화면 오른쪽 미리보기 패널 상단에서 알람을 자세히 확인할 수 있습니다. 출입문과 엘리베이터는 이상( ) 상태가 있을 때도 패널 상단에서 함께 확인할 수 있습니다.

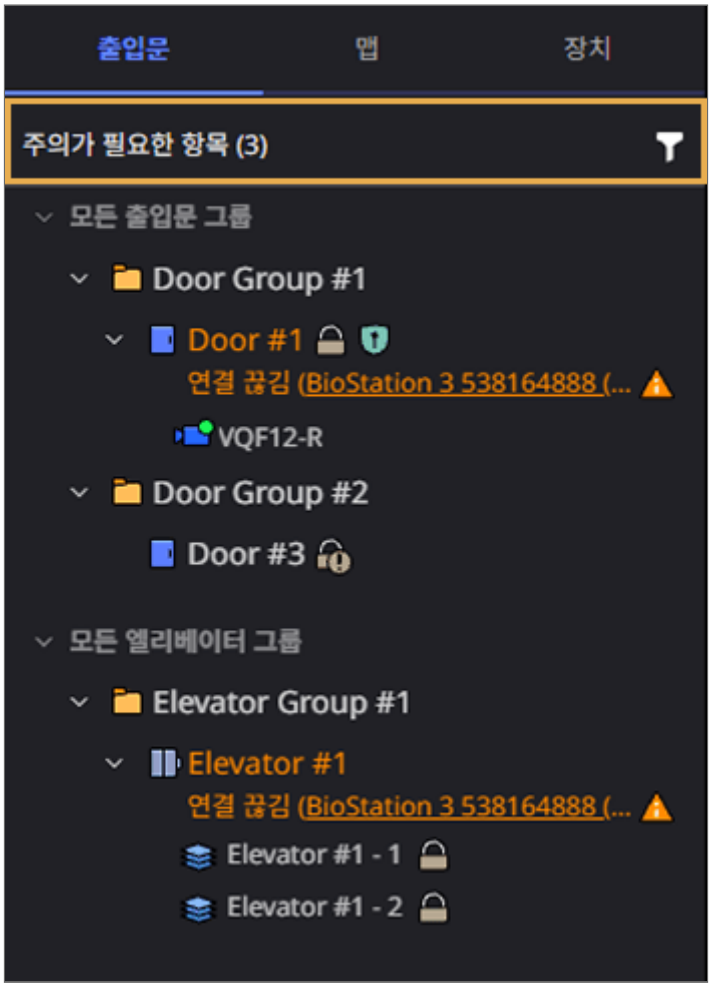


패널 상단에는 알람 이름, 발생 시각 등 현재 상태 정보가 배너로 표시되며, 상황에 맞는 조치를 바로 실행할 수 있는 버튼도 함께 제공됩니다.

> **알아두기**
>
> - 알람이 여러 건 동시에 발생해도 배너에는 가장 최근에 발생한 알람 1건만 표시됩니다.
> - 출입문 또는 엘리베이터의 경우, 장치 연결이 끊긴 상태에서 발생한 알람은 발생 시각 없이 알람 종류만 표시됩니다.
> - 배너에서 제공하는 버튼은 알람 종류에 따라 다르며, 버튼을 클릭하면 알람에 맞는 조치를 진행할 수 있습니다.
> - 알람이 표시된 상태에서도 출입문 잠금, 개방 등 제어 기능은 그대로 사용할 수 있습니다. 출입문 제어에 대한 자세한 내용은 출입문 제어하기를 참고하세요.

주의가 필요한 항목 모아보기

관리자는 조치가 필요한 출입문과 엘리베이터만 한 번에 모아 볼 수 있습니다. 화면 왼쪽 사이드바의 **주의가 필요한 항목**을 클릭하세요. 출입문과 엘리베이터의 상태를 확인하고, 문제가 발생한 장치에 대해 즉시 조치를 취할 수 있습니다.



알아두기
어떤 상태일 때 출입문과 엘리베이터가 조치 대상으로 표시되는지 조치 대상 판정 기준을 참고하세요.

조치 대상 판정 기준

출입문

출입문은 아래 조건 중 하나라도 해당하면 조치가 필요한 항목으로 표시됩니다.

출입문 모드 변경

관리자, 스케줄, 비상 상황에 의해 출입문이 잠기거나 개방된 상태를 포함합니다.

사유	상태 표시
관리자 수동 조작	**관리자에 의한 잠김** / **관리자에 의한 개방**
스케줄	**스케줄에 의한 잠김** / **스케줄에 의한 개방**
비상 상황	**비상상태에 의한 잠김** / **비상상태에 의한 개방**

알람

해제되지 않은 알람이 하나라도 있으면 조치 대상으로 표시됩니다. 강제 열림, 장시간 열림, 안티패스백 관련 알람은 이상 상태가 아닌 알람으로 분류됩니다.

알람 종류	설명
출입문 강제 열림	잠금을 해제하지 않고 강제로 연 상태
출입문 장시간 열림	설정한 시간을 초과해 열려 있는 상태
안티패스백(APB) 알람	재입출입 규칙을 위반한 상태
시간 제한 안티패스백 알람	시간 기준 재입출입 규칙을 위반한 상태
비상 개방(Lock Override) 알람	잠금 상태(관리자에 의해 잠김 또는 스케줄 잠금 상태)에서 비상 개방(Lock Override) 카드 인증으로 개방된 상태
AI 영상 분석 알람	테일게이팅, 배회, 침입, 쓰러짐, 방치 등 영상 분석 기반 알람

이상 상태

출입문에 연결된 장치의 연결 상태를 기준으로 판정합니다.

이상 상태 종류	설명
연결 끊김	장치와의 네트워크 연결이 끊긴 상태
동기화 오류	연결은 되어 있으나 데이터 동기화가 어긋난 상태
멀티 커뮤니케이션 서버 오류	장치가 속한 멀티 커뮤니케이션 서버에서 오류가 발생한 상태

알아두기

- **주의가 필요한 항목** 필터에는 위 이상 상태 외에도 장치 잠금, 인증 연속 실패로 인한 잠금(Auth Fail Lockout) 상태가 포함됩니다.
- 알람과 이상 상태가 동시에 발생하면 두 상태 아이콘이 함께 표시되며, 하나가 다른 하나를 가리지 않고 한 행에서 모두 확인할 수 있습니다.
- 하위 장치에서 발생한 이상 상태는 상위 출입문 노드로 집계되어 표시되므로, 필터가 켜진 상태에서도 문제가 발생한 위치를 계층 구조를 따라 확인할 수 있습니다.

엘리베이터

엘리베이터도 출입문과 같은 조건으로 판정합니다. 다만 이상 상태와 알람 조건에는 아래와 같은 차이가 있습니다.

- **모드 변경**: 출입문과 동일합니다. 관리자, 스케줄, 비상 상황에 의해 잠기거나 개방되면 조치 대상으로 표시됩니다.
- **이상 상태**: 출입문과 같은 기준을 적용합니다. 다만 강제 열림과 장시간 열림은 엘리베이터에 없는 상태이므로 판정 대상에서 제외됩니다.

- **알람**: 엘리베이터에는 출입문과 다른 전용 알람이 있습니다. 아래를 참고하세요.

알람 종류	설명
엘리베이터 경보 발생	엘리베이터에서 알람이 발생한 상태
엘리베이터 입력 경보	외부 입력 신호로 발생한 알람
엘리베이터 전 층 개방 경보	모든 층이 강제로 개방된 상태

알아두기

- 층은 엘리베이터 노드 하위의 독립된 노드로 표시되며, 각 층은 잠금()/개방() 상태만 가집니다.
- 알람과 이상 상태는 층이 아닌 상위 엘리베이터 노드에 표시됩니다. 엘리베이터를 펼치면 조치가 필요한 층만 표시되고, 정상 층은 숨겨집니다.

고급 출입 통제

고급 출입 통제 그룹의 항목(안티패스백, 화재 경보, 침입, 소집, 재실 인원 제한, 인터락)도 조치 대상 판정에 포함됩니다. 다만 출입문이나 엘리베이터와 달리 모드 변경이나 이상 상태 조건은 적용되지 않으며, 해제되지 않은 알람이 하나라도 있으면 조치 대상으로 표시됩니다.

알람 종류	설명
안티패스백(APB) 알람	재입출입 규칙을 위반한 상태
화재 경보	화재를 감지해 발생한 알람
스케줄 잠금 알람	스케줄 잠금을 설정한 상태에서 발생한 알람
침입 알람	침입을 감지해 발생한 알람
인터락 알람	인터락 규칙을 위반한 상태
소집 알람	소집 상황에서 발생한 알람

알아두기

- 경비(Arm) 상태와 비활성화된 항목은 조치 대상으로 표시되지 않습니다. 경비는 정상적으로 운영 중인 상태이고, 비활성화는 의도적으로 꺼둔 상태이기 때문입니다.
- 각 항목은 고급 출입 통제 그룹의 직계 하위로 표시되며, 하위에 출입문이 펼쳐지지 않습니다. 조치가 필요한 항목만 트리에 남고, 조치 대상이 없으면 고급 출입 통제 그룹 자체가 트리에서 제외됩니다.

출입문 상태 확인

출입문의 닫힘 또는 열림, 이상 상태를 확인할 수 있습니다. 출입문 상태는 아래를 참고하세요.

상태 아이콘	설명
	출입문이 닫힌 상태입니다.
	출입문이 열린 상태입니다.
	출입문 센서가 설정되지 않은 상태 입니다.

출입문 잠금 확인

출입문 릴레이 상태를 통해 출입문의 잠금 상태를 확인할 수 있습니다. 출입문 릴레이의 상태는 아래를 참고하세요.

상태 아이콘	설명
	출입문이 잠긴 상태입니다.
	출입문을 **시간 설정** 또는 **고정** 옵션으로 잠근 상태입니다.
	출입문이 개방된 상태입니다.
	출입문을 **시간 설정** 또는 **고정** 옵션으로 개방한 상태입니다.

알아두기

출입문 제어 옵션에 대한 자세한 내용은 출입문 제어하기를 참고하세요.

카메라 상태 확인

카메라의 상태를 확인하여 카메라가 정상적으로 작동하는지 확인할 수 있습니다. 카메라의 상태는 아래를 참고하세요.

상태 아이콘	설명
	카메라가 연결된 상태입니다.
	카메라가 꺼져 있거나 연결이 해제된 상태입니다.

알아두기

- 출입문과 연동된 카메라가 보이지 않는다면 카메라 그룹 권한을 확인하세요. 커스텀 권한의 관리자가 카메라 그룹 권한을 설정하지 않았다면 카메라가 보이지 않을 수 있습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.
- 출입문과 카메라를 연동하려면 비디오 규칙을 추가해야 합니다. 자세한 내용은 비디오 규칙 설정하기를 참고하세요.

경비 상태 확인

출입문 또는 고급 출입 통제 설정의 경비 상태를 확인할 수 있습니다.

상태 아이콘	설명
	경비 상태입니다.
	경비가 해제된 상태입니다.

> **알아두기**
> 경비 상태는 출입문을 **경비**으로 설정했을 때만 표시됩니다. 경비 설정에 대한 자세한 내용은 경비를 참고하세요.

엘리베이터 상태 확인

엘리베이터를 통한 층 접근 제어 상태를 확인할 수 있습니다.

상태 아이콘	설명
	엘리베이터를 통해 해당 층이 잠긴 상태입니다.
	엘리베이터를 통해 해당 층이 개방된 상태입니다.

그룹 목록 확장/축소

최상위 그룹 또는 하위 그룹을 통해서 목록을 확장하거나 축소할 수 있습니다.



최상위 그룹

1. **출입문** 탭에서 **모든 출입문 그룹** 또는 **모든 엘리베이터 그룹**, **모든 고급 출입 통제**를 선택하고 마우스 오른쪽 버튼을 클릭하세요.

2. 팝업 메뉴에서 **모두 펼치기** 또는 **모두 접기** 옵션을 선택하세요.

선택한 최상위 그룹을 기준으로 모든 하위 목록을 확장하거나 축소할 수 있습니다.

하위 그룹

1. 각 최상의 그룹의 하위 그룹 목록을 확장하거나 축소하려면 하위 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.
2. 팝업 메뉴에서 **하위 펼치기** 또는 **하위 접기** 옵션을 선택하세요.

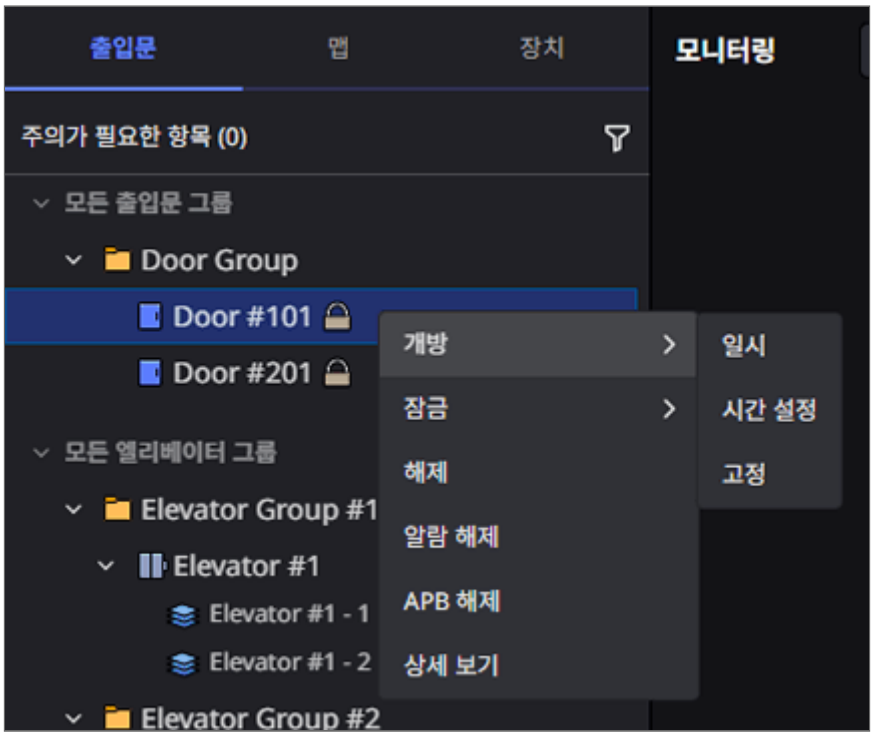
선택한 하위 그룹의 목록을 확장하거나 축소할 수 있습니다.

출입문 제어하기

출입문을 제어하는 방법을 안내합니다. 출입문을 일정 시간 동안 잠금 하거나 출입문과 연결된 카메라를 확인하고, 발생한 알람을 해제할 수 있습니다.

- 출입문을 원격으로 제어하여 출입을 관리하세요. 특정 시간 동안 출입문을 개방하거나 잠금 상태로 설정할 수 있습니다.
- 출입문과 연결된 카메라를 통해 실시간으로 출입 상황을 모니터링할 수 있습니다.
- 안티패스백 기능을 통해 무단출입을 방지하고, 출입 기록을 정확하게 관리할 수 있습니다.

런처 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요. 제어하길 원하는 출입문을 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택할 수 있습니다.

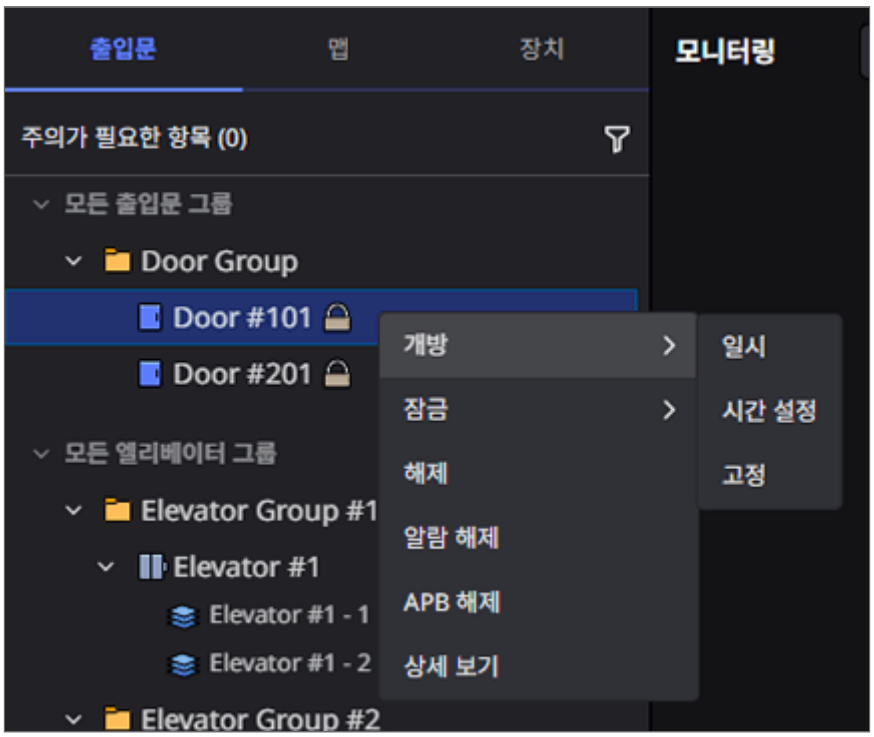


알아두기

- 출입문의 상태를 모니터링하거나 제어하려면 **로그 업로드** 기능이 활성화되어 있어야 합니다. 이 기능은 **설정** → **시스템** → **서버** 메뉴 경로의 **일반** 섹션에서 활성화할 수 있습니다.
- **비디오 열기** 옵션은 VMS와 연동되어 있고, 출입문과 카메라가 연계되어 있어야 사용할 수 있습니다. 또한 이 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 여러 출입문을 한 번에 선택해서 제어하려면 일괄 제어하기를 참고하세요.

출입문 개방

개방 상태의 출입문은 누구든지 출입할 수 있습니다. 팝업 메뉴에서 **개방**을 클릭하고 원하는 옵션을 선택하세요.



- **일시**: 한 번만 출입문을 개방합니다.
- **시간 설정**: 일정 시간 동안 출입문을 개방합니다. 원하는 시간을 초(second) 단위로 입력하세요.
- **고정**: 시간에 상관없이 출입문을 개방합니다.

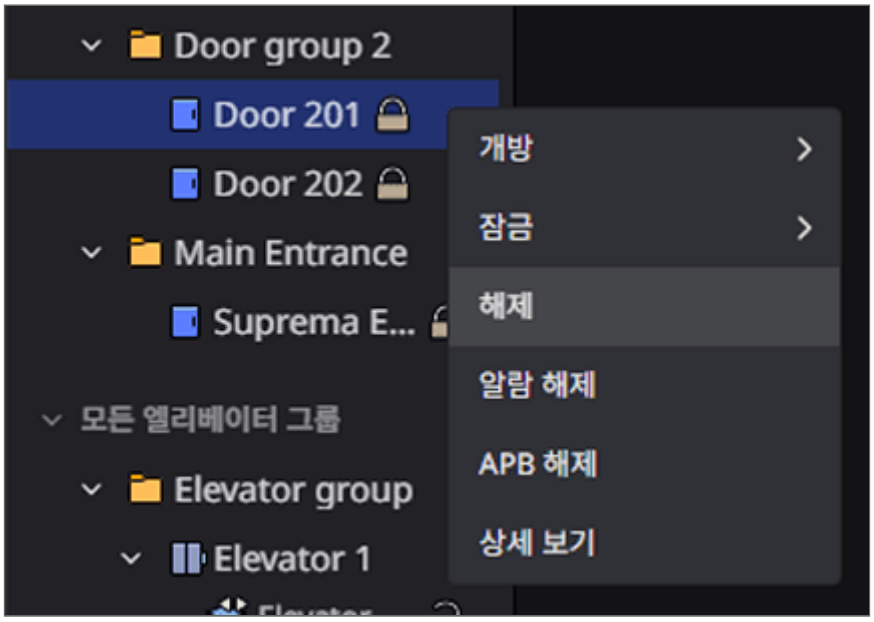
출입문을 일시적으로 개방하면 출입문 릴레이 아이콘이 상태에서 상태로 변경됩니다. **시간 설정** 또는 **고정** 옵션으로 개방하면 상태로 아이콘이 변경됩니다.

팁

외부 손님이 방문할 때 출입문을 일시적으로 개방하여 편리하게 출입할 수 있습니다. 출입문을 개방한 후에는 반드시 **해제** 상태로 변경하세요.

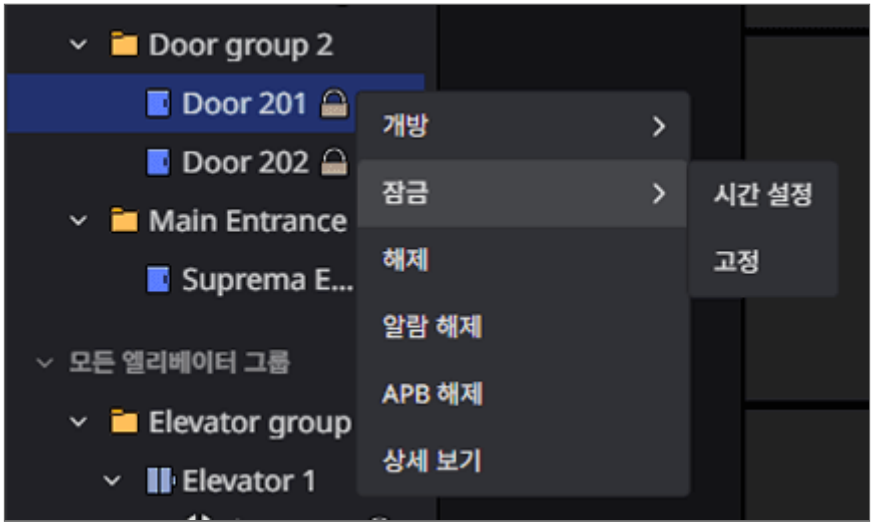
출입문 해제

출입문을 **해제** 상태로 변경하면 허가된 사용자만 출입할 수 있습니다. 팝업 메뉴에서 **해제**를 클릭하세요.



출입문 잠금

출입문을 **잠금** 상태로 변경하면 아무도 출입할 수 없습니다. 팝업 메뉴에서 **잠금**을 클릭하고 원하는 옵션을 선택하세요.

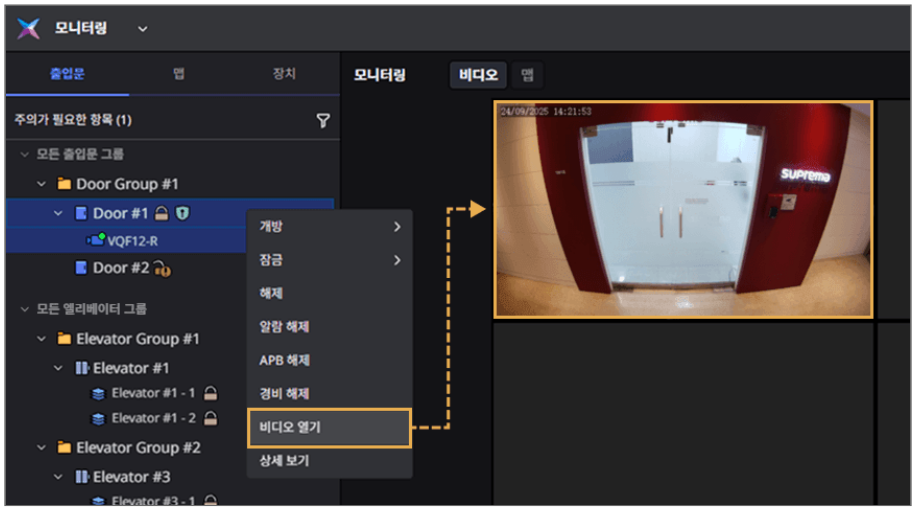


- **시간 설정**: 일정 시간 동안 출입문을 잠금 상태로 변경합니다. 원하는 시간을 초(second) 단위로 입력하세요.
- **고정**: 시간에 상관없이 출입문을 잠금 상태로 변경합니다.

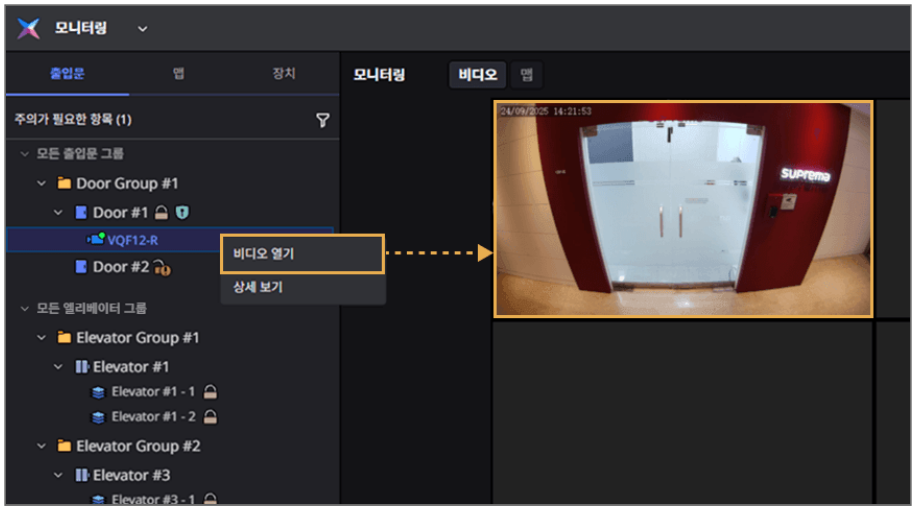
출입문을 잠금 상태로 변경하면 출입문 릴레이 아이콘이 상태로 변경됩니다.

출입문 카메라 확인

출입문과 연결된 카메라를 확인할 수 있습니다. 팝업 메뉴에서 **비디오 열기**를 클릭하세요. **모니터링** 섹션의 비디오 타일에 선택한 카메라의 영상을 추가하고, 재생할 수 있습니다.



또는 원하는 카메라를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **비디오 열기**를 클릭하면 선택한 카메라의 영상을 추가하고, 재생할 수 있습니다.



알아두기

- 출입문에 연결된 카메라가 한 대 이상이라면 첫번째로 연결된 카메라가 비디오 타일에 표시됩니다.
- 비디오 타일에는 화면 왼쪽 상단부터 차례로 추가되며, 현재 화면에 추가할 공간이 없으면 에러 메시지가 표시됩니다.
- 비디오 모니터링에 대한 자세한 내용은 비디오 모니터링하기를 참고하세요.
- 출입문과 연동된 카메라가 보이지 않는다면 카메라 그룹 권한을 확인하세요. 커스텀 권한의 관리자가 카메라 그룹 권한을 설정하지 않았다면 카메라가 보이지 않을 수 있습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.
- 이 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

알람 해제

출입문에서 발생한 알람을 해제할 수 있습니다. 팝업 메뉴에서 **알람 해제**를 클릭하세요. 화면 오른쪽 상단에 알람 메시지가 표시됩니다.



APB 해제

안티패스백 위반이 발생했을 때, APB 알람을 해제할 수 있습니다.

1. 팝업 메뉴에서 **APB 해제**를 클릭하세요.



2. **APB 해제** 창이 나타나면 모든 사용자 목록을 확인할 수 있습니다.



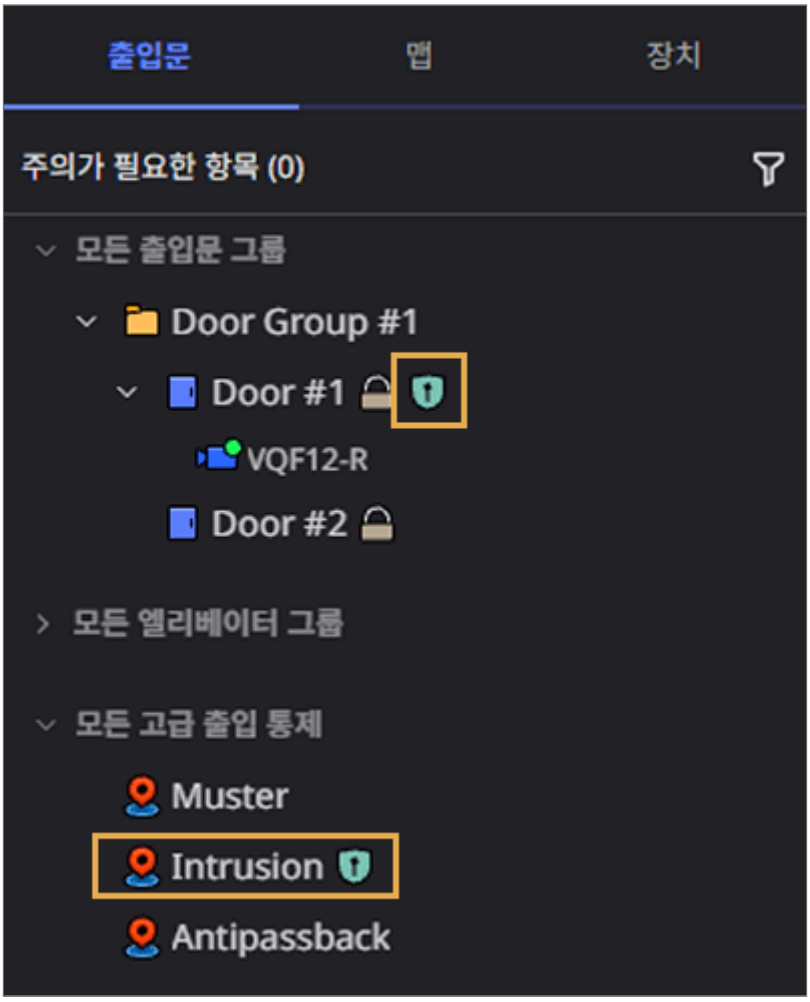
3. 안티패스백을 위반한 사용자를 선택하고 **적용** 버튼을 클릭하세요.

화면 오른쪽 상단에 완료 메시지가 표시됩니다.

> **알아두기**
>
> - **안티패스백(Anti-Passback)**: 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다.
> **안티패스백**은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.
> - 출입문에 **안티패스백**을 설정하는 방법에 대한 자세한 내용은 출입문 등록하기를 참고하세요.

경비 설정 및 해제

출입문이 경비로 설정되어 있다면 경비를 설정하거나 해제할 수 있습니다. 팝업 메뉴에서 **경비** 또는 **경비 해제**을 클릭하세요.

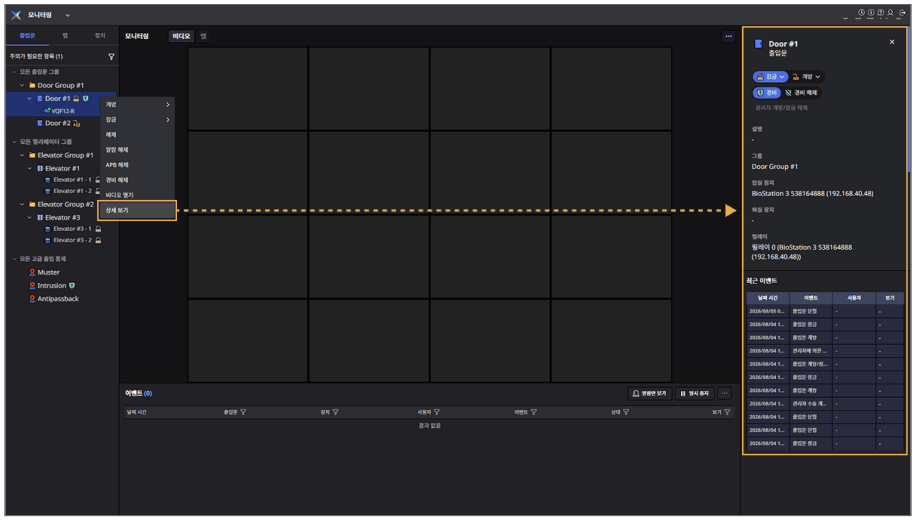


경비 상태의 출입문은 경비 상태 아이콘이 상태에서 상태로 변경됩니다. 이때 해당 출입 통제 설정에도 아이콘이 적용됩니다.

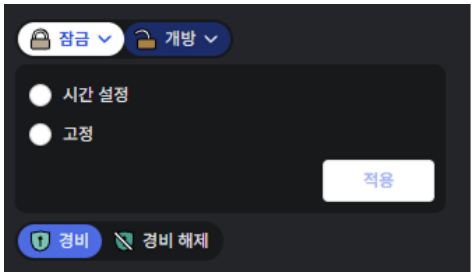
> **알아두기**
>
> 이 기능은 **에센셜**(Essential) 라이선스에서 추가 옵션을 구매하거나 **엔터프라이즈**(Enterprise) 라이선스 이상에서 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

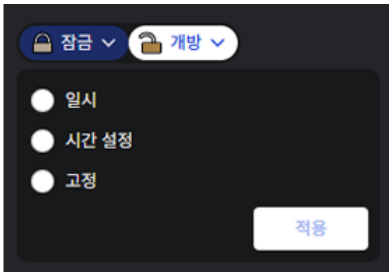
상세 정보 확인

출입문에 대한 상세 정보와 이벤트 발생 이력을 확인할 수 있습니다. 팝업 메뉴에서 **상세 보기**를 클릭하세요. 화면 오른쪽에 출입문 제어 및 출입문 상세 정보, 이벤트 발생 이력을 확인할 수 있는 패널이 나타납니다.



- **출입문 제어**: 출입문을 잠금, 개방, 경비 또는 경비 해제 상태로 변경할 수 있습니다.





- **관리자 개방/잠금 해제**: 관리자가 직접 출입문을 개방하거나 잠금 상태로 변경했을 때 사용할 수 있습니다.
- **출입문 상세 정보**: 출입문의 이름, 위치, 상태, 연결된 서브 장치 정보 등을 확인할 수 있습니다.
- **최근 이벤트**: 선택한 출입문에서 발생한 최근 이벤트 목록을 확인할 수 있습니다.

> **알아두기**
> 출입문 상세 정보 섹션의 각 항목에 대한 자세한 내용은 출입문 등록하기를 참고하세요.

엘리베이터 제어하기

엘리베이터를 제어하는 방법을 안내합니다. 제공하는 기능을 통해 엘리베이터를 제어하거나 상세 정보를 확인할 수 있습니다.

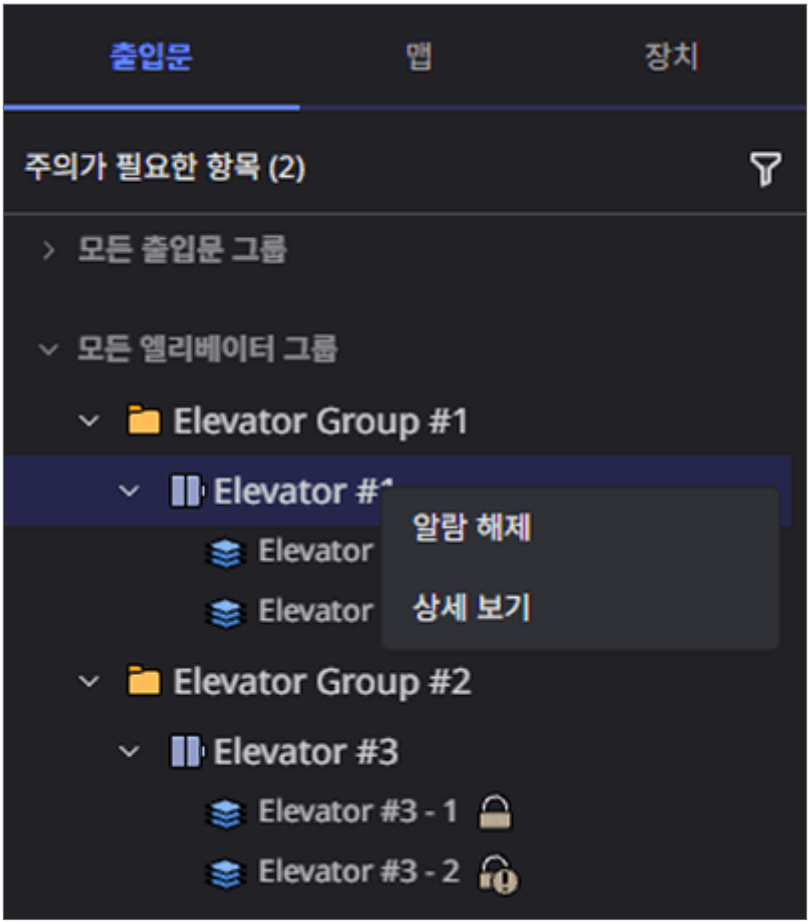
1. **런처** 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요.
2. 화면 왼쪽 사이드바의 **출입문** 탭에서 **모든 엘리베이터 그룹**으로 이동하세요.
3. 원하는 그룹의 엘리베이터를 선택하고 오른쪽 마우스 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택할 수 있습니다.

알아두기

- 엘리베이터 설정 및 그룹 구성 방법에 대한 자세한 내용은 엘리베이터 관리하기를 참고하세요.
- 여러 엘리베이터와 층을 한 번에 선택해서 제어하려면 일괄 제어하기를 참고하세요.

엘리베이터 제어하기

엘리베이터에서 발생한 알람을 해제하거나 상세 정보를 확인할 수 있습니다.

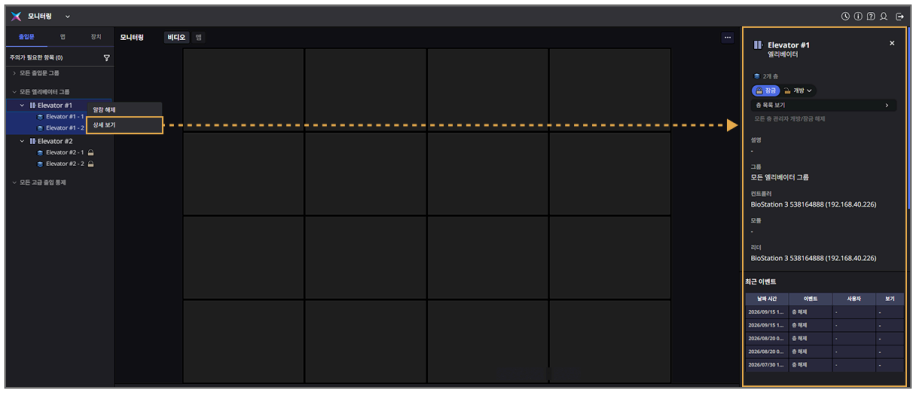


알람 해제

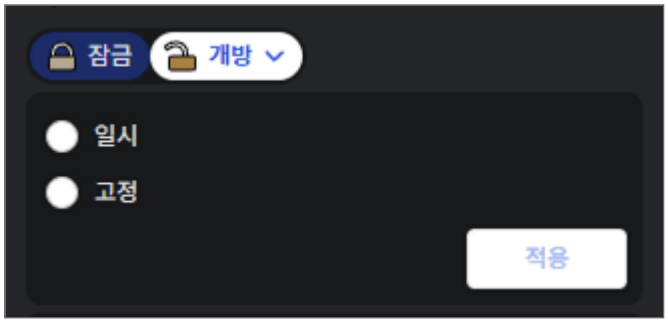
해당 엘리베이터에서 발생한 알람을 해제할 수 있습니다. 팝업 메뉴에서 **알람 해제**를 클릭하세요. 화면 오른쪽 상단에 완료 메시지가 표시됩니다.

상세 정보 확인

엘리베이터에 대한 상세 정보와 이벤트 발생 이력을 확인할 수 있습니다. 팝업 메뉴에서 **상세 보기**를 클릭하세요. 화면 오른쪽에 엘리베이터 상세 정보와 이벤트 발생 이력이 표시됩니다.



- **엘리베이터 제어**: 엘리베이터를 잠금 또는 개방 상태로 변경할 수 있습니다.



- **층 목록 보기**: 엘리베이터에 설정된 층 목록을 확인할 수 있습니다.

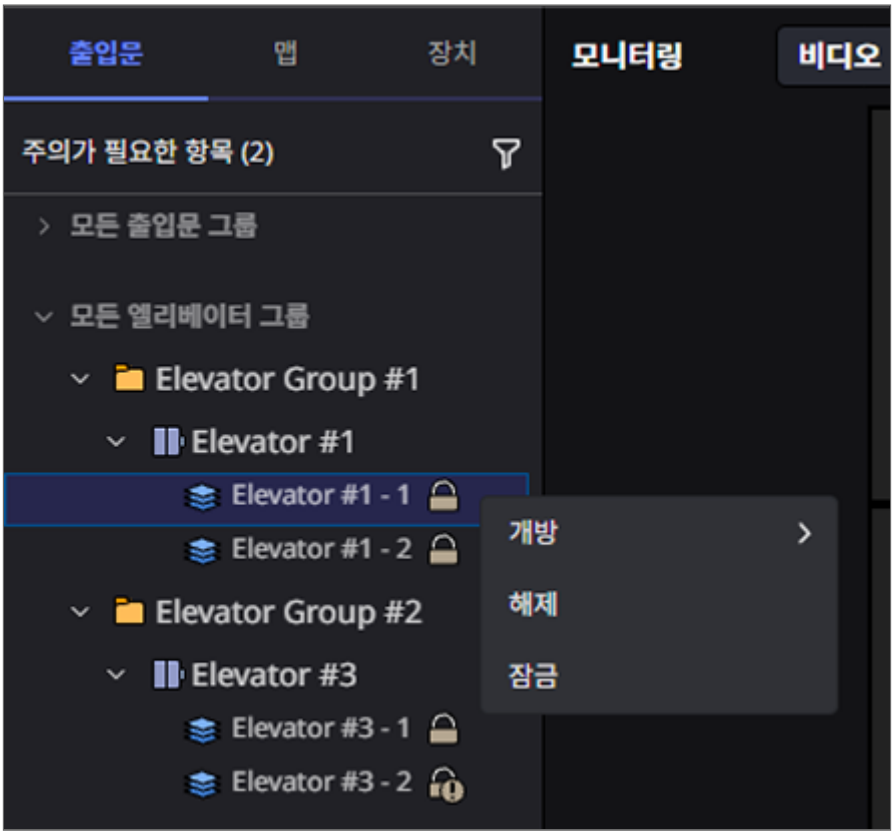


- **모든 층 관리자 개방/잠금 해제**: 관리자가 직접 모든 층을 개방하거나 잠금 상태로 변경했을 때 사용할 수 있습니다.
- **엘리베이터 상세 정보**: 엘리베이터의 이름, 위치, 상태 정보 등을 확인할 수 있습니다.
- **최근 이벤트**: 선택한 엘리베이터에서 발생한 최근 이벤트 목록을 확인할 수 있습니다.

> **알아두기**
> 엘리베이터 상세 정보 섹션의 각 항목에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.

층 출입 제어

엘리베이터로 이동할 수 있는 층을 제어할 수 있습니다. 엘리베이터에 설정된 층의 릴레이를 클릭하고 오른쪽 마우스 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택하세요.



층 개방

개방 상태의 층은 누구든지 출입할 수 있습니다. 팝업 메뉴에서 **개방**을 클릭하고 원하는 옵션을 선택하세요.

- **일시**: 한 번만 층을 개방합니다.
- **고정**: 시간에 상관없이 층을 개방합니다.

> **팁**
> 외부 손님이 방문할 때 선택한 층을 일시적으로 개방하여 편리하게 출입할 수 있습니다. 층을 개방한 후에는 반드시 **해제** 상태로 변경하세요.

층 해제

선택한 층을 **해제** 상태로 변경하면 허가된 사용자만 출입할 수 있습니다. 팝업 메뉴에서 **해제**를 클릭하세요.

층 잠금

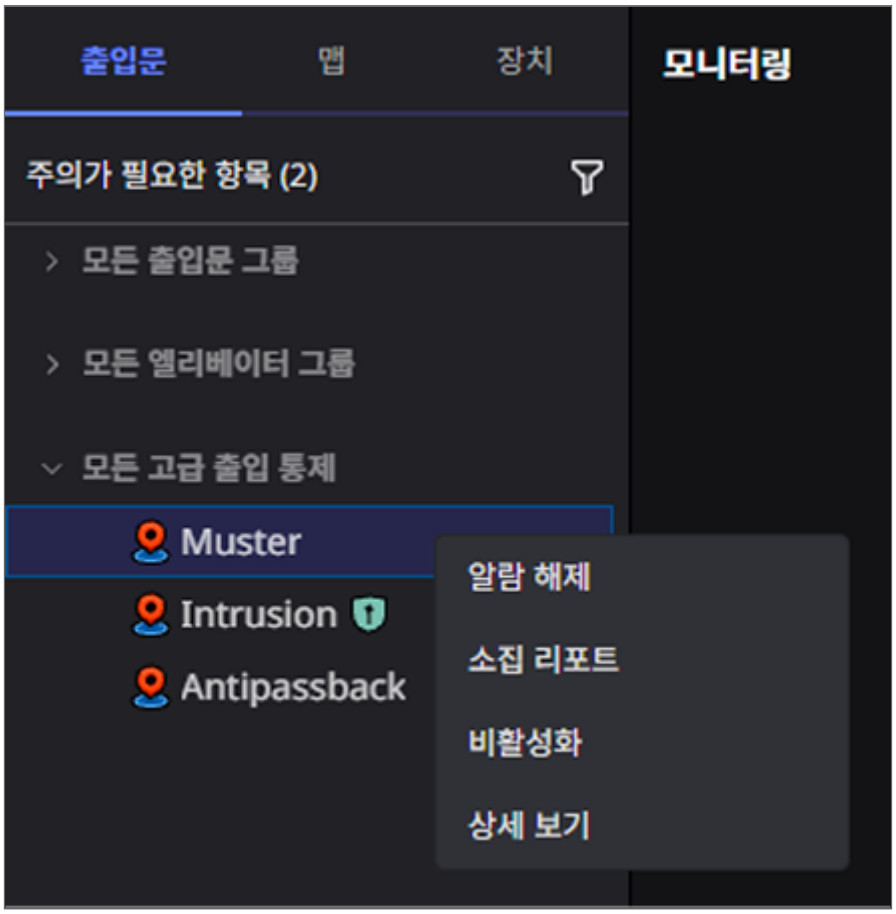
선택한 층을 **잠금** 상태로 변경하면 아무도 출입할 수 없습니다. 팝업 메뉴에서 **잠금**을 클릭하세요.

고급 출입 통제 제어하기

고급 출입 통제로 설정된 출입문 또는 장치 제어 방법을 안내합니다. 제공하는 기능을 통해 문제 발생 시 빠른 대처 및 효율적으로 관리할 수 있습니다.

1. **런처** 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요.
2. 화면 왼쪽 사이드바의 **출입문** 탭에서 **모든 고급 출입 통제**로 이동하세요.

3. 설정된 고급 출입 통제를 선택하고 오른쪽 마우스 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택할 수 있습니다.



알아두기

- 고급 출입 통제의 종류에 따라 제공하는 기능이 다릅니다. 고급 출입 통제의 종류는 다음과 같습니다.
  - **안티패스백**
  - 화재 경보
  - 스케줄 잠금/개방
  - 경비
  - 인터락
  - 소집
  - 재실 인원 제한
  - 인원 점검(Roll Call)
- 각 고급 출입 통제에 대한 자세한 내용은 고급 출입 통제 설정하기를 참고하세요.
- 여러 고급 출입 통제 설정을 한 번에 선택해 제어하려면 일괄 제어하기를 참고하세요.

APB 해제

안티패스백으로 설정된 출입문 또는 장치의 APB 알람을 해제할 수 있습니다. 팝업 메뉴에서 **APB 해제**를 클릭하세요. 화면 상단에 완료 메시지가 표시됩니다.

알아두기

- **APB 해제** 기능은 **안티패스백**에서만 사용할 수 있습니다.
- **안티패스백** 설정에 대한 자세한 내용은 안티패스백을 참고하세요.
- **안티패스백**에 대한 자세한 내용은 용어집을 참고하세요.

알람 해제

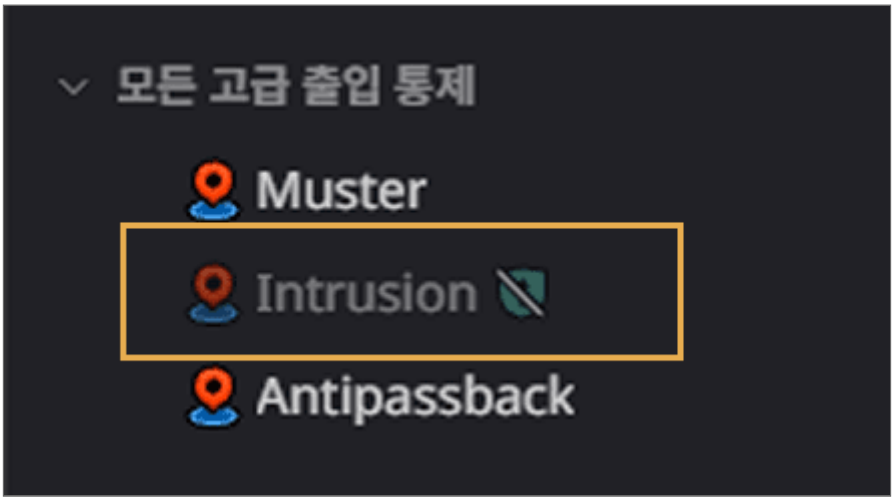
출입문 또는 장치에서 발생한 알람을 해제할 수 있습니다. 팝업 메뉴에서 **알람 해제**를 클릭하세요. 화면 상단에 완료 메시지가 표시됩니다.

알아두기

알람 해제는 재실 인원 제한 기능에서 사용할 수 없습니다.

활성화/비활성화

고급 출입 통제 기능을 활성화하거나 사용하지 않는 기능은 비활성화할 수 있습니다. 비활성화된 고급 출입 통제는 불투명 상태로 변경됩니다. 팝업 메뉴에서 **활성화** 또는 **비활성화**를 클릭하세요.



경비/경비 해제

출입문 또는 장치의 경비를 설정하거나 해제할 수 있습니다. 팝업 메뉴에서 **경비** 또는 **경비 해제**를 클릭하세요.

알아두기

- **경비** 또는 **경비 해제**는 경비로 설정된 고급 출입 통제에서만 사용할 수 있습니다.
- 경비 설정에 대한 자세한 내용은 경비를 참고하세요.

소집 리포트 확인

소집에 대한 보고서를 확인하려면 **소집 리포트**를 클릭하세요. 새 창이 열리면 사용자 목록과 소집 기능으로 설정된 장치를 통해 사용자의 입실 및 퇴실 시간, 체류 시간 초과 여부를 확인할 수 있습니다.

> **알아두기**
>
> - **소집 리포트** 기능은 소집에서만 사용할 수 있습니다.
> - 소집 기능에 대한 자세한 내용은 소집을 참고하세요.

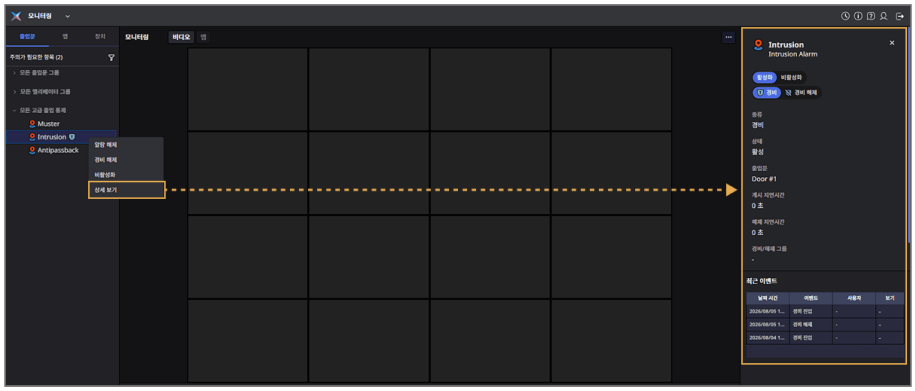
재실 인원 제한 모니터링

재실 인원 제한 기능으로 설정된 장치에 대한 상태를 확인할 수 있습니다. 팝업 메뉴에서 **재실 인원 제한 모니터링**을 클릭하세요. 새 창이 열리면 **설정** → **출입 관리** → **고급 출입 통제** 메뉴로 이동합니다. **재실 인원 제한** 목록에서 상태를 확인할 수 있습니다.

> **알아두기**
>
> - **재실 인원 제한 모니터링** 기능은 재실 인원 제한 기능으로 설정된 항목에서만 사용할 수 있습니다.
> - 재실 인원 제한 설정에 대한 자세한 내용은 재실 인원 제한을 참고하세요.

상세 정보 확인

고급 출입 통제에 대한 상세 정보와 이벤트 발생 이력을 확인할 수 있습니다. 팝업 메뉴에서 **상세 보기**를 클릭하세요. 화면 오른쪽 패널에 상세 정보와 이벤트 발생 이력이 표시됩니다.



- **고급 출입 통제 제어**: 선택한 고급 출입 통제에 해당하는 제어 기능을 사용할 수 있습니다.
- **상세 정보**: 고급 출입 통제 기능의 이름 및 상태, 장치 정보 등을 확인할 수 있습니다.
- **최근 이벤트**: 선택한 고급 출입 통제에서 발생한 최근 이벤트 목록을 확인할 수 있습니다.

> **알아두기**
>
> 고급 출입 통제 상세 정보 섹션의 각 항목에 대한 자세한 내용은 고급 출입 통제 설정하기를 참고하세요.

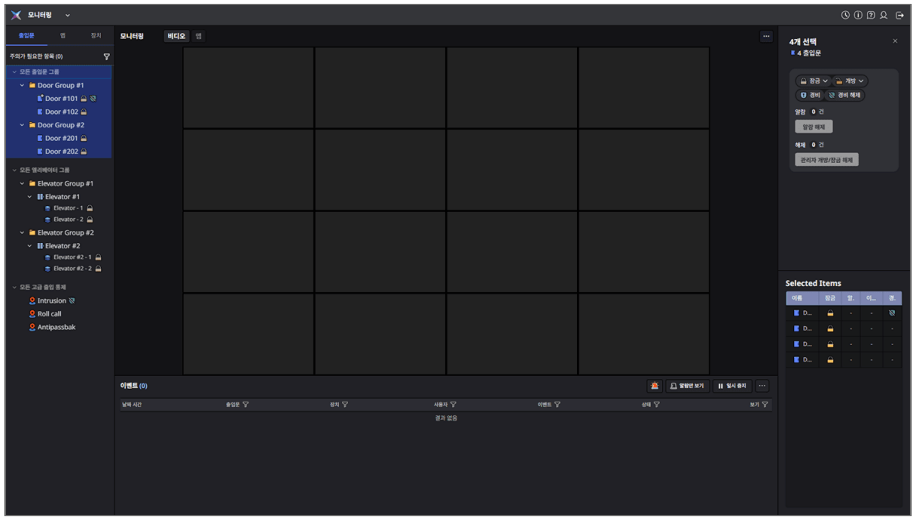
일괄 제어하기

여러 출입문, 엘리베이터, 고급 출입 통제 설정을 한 번에 선택해서 개방, 잠금, 알람 해제 등의 명령을 한 번에 실행하는 방법을 안내합니다.

- 상태 트리에서 항목을 두 개 이상 선택하면 화면 오른쪽에 일괄 제어 패널이 나타납니다. 항목을 하나씩 제어할 필요 없이 한 번에 명령을 실행할 수 있습니다.
- 비상 상황이나 여러 출입구를 동시에 통제해야 할 때 신속하게 대응할 수 있습니다.

- 출입문, 엘리베이터(층), 고급 출입 통제 설정을 각각 일괄 선택하여 제어할 수 있습니다. 서로 다른 종류를 함께 선택하면 제어할 수 없습니다.

런처 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하세요. 화면 왼쪽 사이드바의 상태 트리에서 제어할 항목을 두 개 이상 선택하면 화면 오른쪽에 일괄 제어 패널이 나타납니다.



알아두기

- 카메라는 일괄 제어 대상이 아닙니다. 다른 항목과 함께 선택해도 선택 목록에서 제외됩니다.
- 이 문서는 여러 항목을 한 번에 제어하는 방법을 다룹니다. 출입문, 엘리베이터, 고급 출입 통제 중 하나를 선택해서 제어하는 방법은 다음 문서를 참고하세요.
  - 출입문 제어하기
  - 엘리베이터 제어하기
  - 고급 출입 통제 제어하기

여러 항목 선택

화면 왼쪽 사이드바의 상태 트리에서 출입문, 엘리베이터, 층, 고급 출입 통제를 선택하는 방법은 다음과 같습니다. Windows 탐색기에서 여러 파일을 선택하는 방식과 같습니다.

- **클릭**: 항목 하나만 선택합니다. 기존 선택은 해제됩니다.
- `Ctrl` + **클릭**: 클릭한 항목을 선택 목록에 추가하거나 제외합니다. 나머지 선택은 그대로 유지됩니다.
- `Shift` + **클릭**: 마지막으로 클릭한 항목부터 지금 클릭한 항목까지 화면에 보이는 범위를 모두 선택합니다. 기존 선택은 이 범위로 대체됩니다.
- `Ctrl` + `Shift` + **클릭**: 기존 선택을 유지한 채로 범위를 추가로 선택합니다. 서로 떨어진 여러 항목을 모아서 선택할 때 사용하세요.
- **그룹 클릭**: 그룹(🗀) 이름을 클릭하면 그 아래에 있는 모든 출입문, 엘리베이터, 층, 고급 출입 통제 설정이 한 번에 선택됩니다. 그룹을 펼치거나 접으려면 그룹 이름 앞의 화살표(›)를 클릭하세요.

알아두기

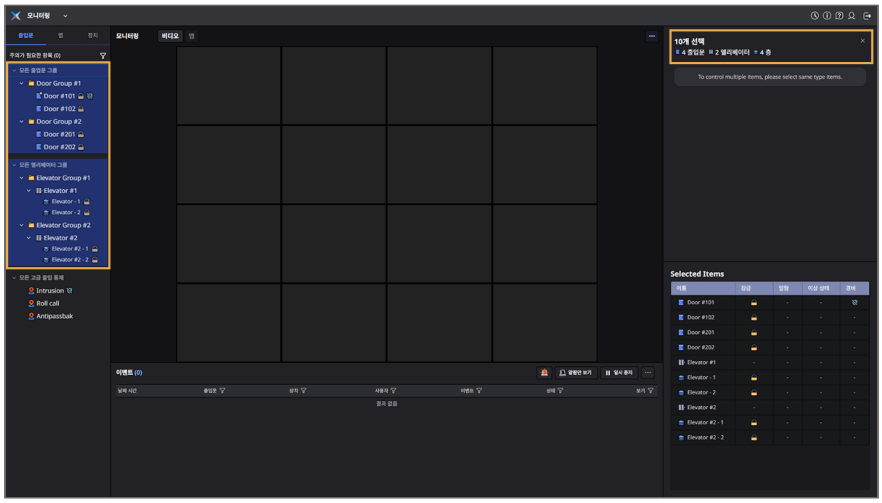
선택한 항목이 없거나 한 개뿐이면 일괄 제어 패널이 열리지 않습니다. 항목을 한 개만 남기면 해당 항목의 상세 보기가 표시되고, 모두 선택 해제하면 오른쪽에 위치한 패널이 사라집니다.

일괄 제어 패널 구성

화면 왼쪽 사이드바의 상태 트리에서 여러 항목을 선택하면 화면 오른쪽에 나타나는 일괄 제어 패널은 다음과 같이 구성됩니다.

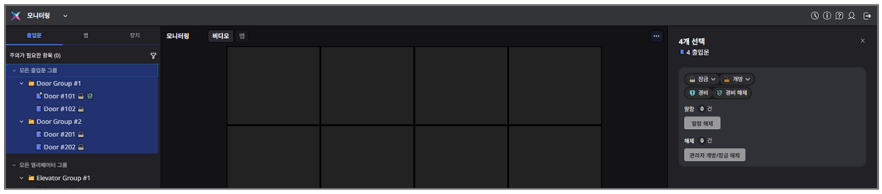
- **선택 개수와 종류**: 예를 들어 출입문 4개와 엘리베이터 2개, 4개 층을 선택하면 다음과 같이 표시됩니다.

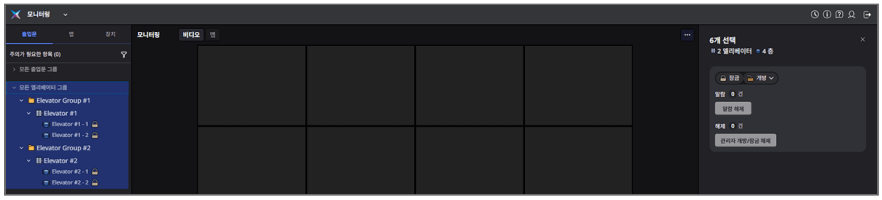
  > *10개 선택 / 4 출입문 2 엘리베이터 4 층*



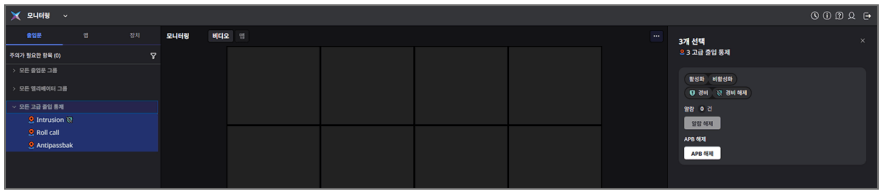
> 서로 다른 종류를 함께 선택하면 제어 기능은 사용할 수 없습니다.

- **출입문/엘리베이터 제어**: 출입문, 엘리베이터에서 사용할 수 있는 제어 기능이 표시됩니다.

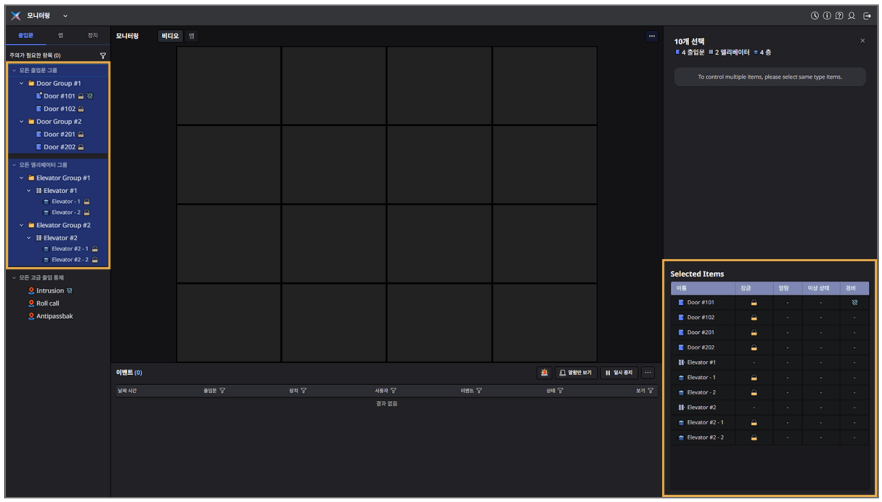




- **고급 출입 통제 제어**: 고급 출입 통제에서 사용할 수 있는 제어 기능이 표시됩니다.



- **선택된 항목 요약 표**: 화면 오른쪽 패널 하단에는 선택한 각 항목의 이름과 상태를 확인할 수 있습니다. 제어 영역과 요약 표 사이의 구분선을 위아래로 드래그하면 두 영역의 높이를 조절할 수 있습니다. 선택한 항목이 많으면 구분선을 드래그해서 요약 표 영역을 넓게 확인하세요.



출입문 일괄 제어

출입문만 두 개 이상 선택하면 단일 출입문 제어와 같은 기본 제어와 고급 제어를 사용할 수 있습니다.





기본 제어

- **일시**: 개방 상태로 한번만 적용합니다.
- **시간 설정**: 입력한 시간 동안 잠금 또는 개방 상태로 유지하도록 적용합니다.
- **고정**: 시간에 상관없이 잠금 또는 개방 상태로 적용합니다.

원하는 명령을 선택하고 적용하려면 **적용** 버튼을 클릭하세요.

고급 제어

다음 버튼은 아래 조건에 해당하는 항목이 하나라도 있을 때 사용할 수 있습니다.

- **알람 해제**: 선택한 출입문 중 알람이 발생한 항목이 있을 때 사용할 수 있습니다.
- **APB 해제**: 선택한 출입문 중 안티패스백을 설정한 항목이 있을 때 사용할 수 있습니다. 자세한 내용은 출입문 제어하기를 참고하세요.
- **관리자 개방/잠금 해제**: 관리자가 수동으로 개방하거나 잠근 출입문이 있을 때 사용할 수 있습니다. 스케줄이나 비상 상황으로 변경된 상태는 포함하지 않습니다.
- **경비/경비 해제**: 고급 출입 통제 설정 중 하나인 경비로 설정된 출입문이 있을 때만 표시됩니다.

> **알아두기**
>
> - **알람 해제**, **관리자 개방/잠금 해제** 버튼을 클릭하면 팝업창이 나타납니다. 팝업창에서 **알람 해제** 또는 **관리자 개방/잠금 해제** 버튼을 클릭해야 해제할 수 있습니다. 반면 **경비**/**경비 해제** 버튼은 별도 확인 창 없이 상태를 전환할 수 있습니다.
> - 고급 출입 통제 설정은 **에센셜**(Essential) 라이선스에서 추가 옵션을 구매하거나 **엔터프라이즈**(Enterprise) 라이선스 이상에서 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

엘리베이터 및 층 일괄 제어

엘리베이터를 선택하면 설정된 모든 층을 함께 제어할 수 있습니다. 특정 층만 제어하려면 층을 직접 선택하세요.

출입문과 다른 점은 다음과 같습니다.

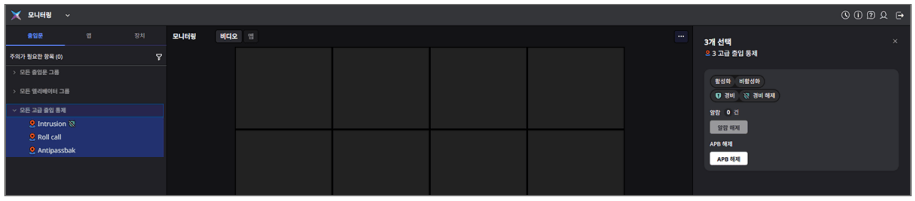
제어 기능	출입문	엘리베이터, 층
개방	**일시**, **시간 설정**, **고정**	**일시**, **고정**
잠금	**시간 설정**, **고정**	**고정**
관리자 개방/잠금 해제	지원	지원
알람 해제	지원	선택 항목에 엘리베이터가 포함되어 있다면 표시, 층만 선택하면 표시되지 않음
APB 해제	지원	미지원

> **알아두기**
> 엘리베이터와 그 하위 층을 함께 선택해서 개방하거나 잠그면, 층마다 각각 명령이 전송되지 않고 엘리베이터 단위로 한 번만 전송됩니다.

고급 출입 통제 일괄 제어

고급 출입 통제 설정도 여러 개를 선택해서 한 번에 제어할 수 있습니다. 두 개 이상 선택하면 오른쪽 영역이 일괄 제어 패널로 전환됩니다. 선택, 범위, 필터 동작은 출입문, 엘리베이터와 같습니다.

고급 출입 통제 설정은 잠금 릴레이나 관리자 개방/잠금 개념이 없어 출입문, 엘리베이터와 제어 항목이 다릅니다. 선택한 설정의 종류에 따라 다음 제어 버튼이 표시됩니다.

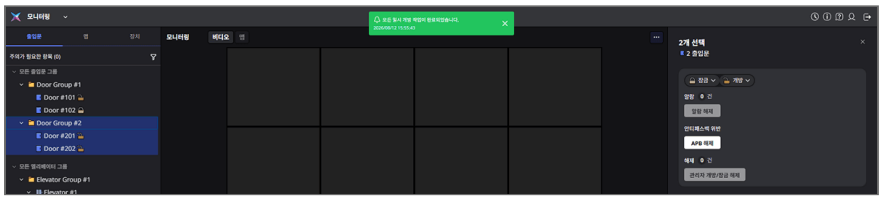


- **활성화**/**비활성화**: 모든 고급 출입 통제 설정에 공통 표시됩니다.
- **경비**/**경비 해제**: 선택한 항목에 경비 설정이 있을 때만 표시됩니다.
- **알람 해제**: 선택한 항목에 알람이 발생하는 설정(안티패스백, 화재 경보, 스케줄 잠금, 경비, 인터락, 소집)이 있을 때만 표시됩니다. 재실 인원 제한, 인원 점검처럼 알람이 발생하지 않는 설정만 선택하면 표시되지 않습니다.
- **APB 해제**: 선택한 항목에 안티패스백 설정이 있을 때만 표시됩니다. 이 버튼을 클릭하면 사용자를 선택하는 창을 통해 안티패스백을 위반한 사용자의 APB 알람을 해제할 수 있습니다. 자세한 내용은 고급 출입 통제 제어하기를 참고하세요.

> **알아두기**
>
> - **잠금**, **개방**, **관리자 개방/잠금 해제** 기능은 일괄 제어에 포함되지 않습니다. 소집 리포트 확인, 재실 인원 제한 모니터링처럼 다른 화면으로 이동하는 기능도 일괄 제어 패널에서는 제공하지 않습니다. 이 기능들은 해당 설정을 하나만 선택했을 때, 상세 정보 화면에서 사용할 수 있습니다.
> - 고급 출입 통제 제어에 대한 자세한 내용은 고급 출입 통제 제어하기를 참고하세요.

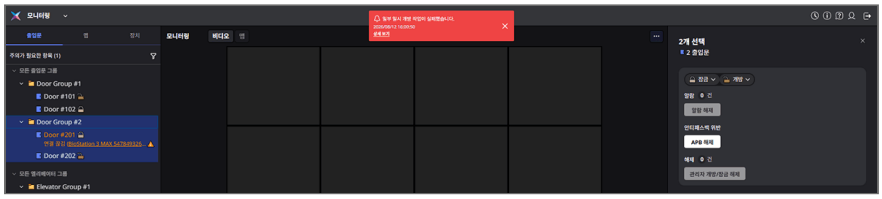
실행 결과 확인

- 선택한 모든 항목이 성공하면 화면 상단에 성공 메시지가 표시됩니다.



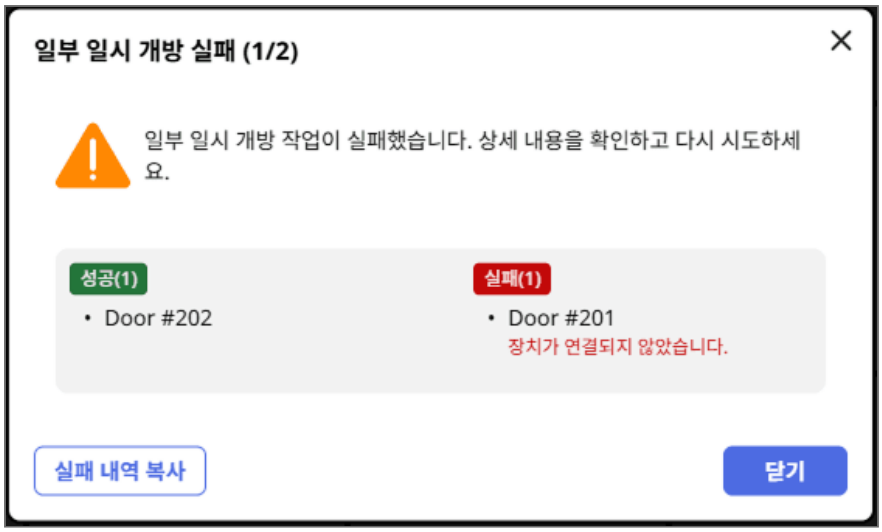
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- 한 항목이라도 실패하면 실패 메시지와 함께 **상세 보기** 버튼이 표시됩니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

상세 보기를 클릭하면 **성공**, **실패**, **대상 아님** 세 그룹으로 구분된 결과를 확인할 수 있습니다. 실패한 항목의 이름과 사유를 클립보드에 복사하려면 **실패 내역 복사** 버튼을 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

맵 모니터링하기

맵 모니터링 기능을 통해 구역과 구역 내 층별 출입문, 카메라 현황을 실시간으로 확인하고, 제어하는 방법을 안내합니다. 맵 모니터링은 구글 지도와 연동된 시각적 인터페이스를 통해 구역(Area)과 층(Floor)을 손쉽게 탐색하며, 출입문 제어, 카메라 영상 재생 등 다양한 기능을 활용할 수 있습니다.

모니터링 페이지는 **런처** 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하여 진입할 수 있습니다.

BioStar X에서는 한 개의 구역(Area)에 여러 개의 시설(Facility)을 구성할 수 있습니다. 각 시설에는 여러 개의 층을 구성할 수 있습니다. 한 개의 층(Floor)에는 도면을 기준으로 출입문(Door), 카메라(Camera)를 설정해 모니터링할 수 있습니다. 아래 그림을 참고하세요.



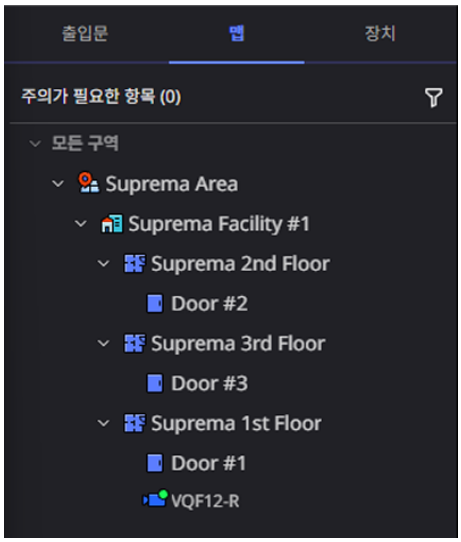
그림과 같이 구성한 지역을 GIS 지도와 연동하여 지도 위의 구역(Area) → 시설(Facility) → 층(Floor) 순으로 접근하여 출입문과 카메라를 모니터링하고 제어할 수 있습니다. 이러한 구조는 **모니터링** 페이지의 사이드바에서도 같은 구조로 확인할 수 있습니다.

> **알아두기**
>
> - 맵을 구성하는 방법에 대한 자세한 내용은 맵 관리하기를 참고하세요.
> - **모니터링** 영역은 시스템에 등록된 장치 카메라가 없거나 맵 구성 요소(구역, 시설, 층)가 등록되어 있지 않으면 활성화되지 않습니다.
> - GIS와 연동한 맵 모니터링 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

구성 요소 및 옵션 기능

맵 트리 구성 요소

화면 왼쪽 사이드바에는 맵 트리 구성 요소가 표시됩니다. 맵 트리에 표시되는 각 구성 요소의 아이콘에 따라 구역, 시설, 층, 출입문, 카메라를 구분할 수 있습니다.

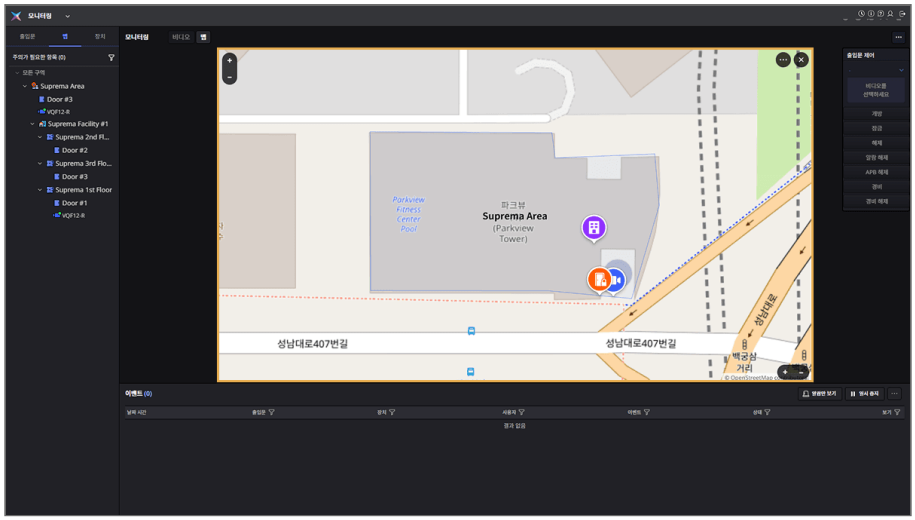


아이콘	이름
	구역(Area)
	시설(Facility)
	층(Floor)
	출입문

아이콘	이름
	카메라

맵 영역 구성 요소

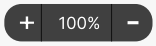
맵에 표시되는 구성 요소는 구역(Area)과 시설(Facility), 시설에 연결된 카메라를 확인할 수 있습니다. 시설을 통해서 층(Floor)으로 접근할 수 있습니다. 층에는 출입문과 카메라를 확인할 수 있습니다.



구성 요소	설명
	**시설(Facility)**: 맵에 배치된 시설을 클릭하면 해당 시설에 설정된 층(Floor)으로 진입할 수 있습니다.
	**출입문**: 맵에 배치된 출입문을 클릭하면 해당 출입문을 제어할 수 있는 팝업 메뉴가 표시됩니다. 제공하는 기능에 대한 자세한 내용은 출입문 제어하기를 참고하세요.
	**카메라**: 카메라를 클릭하면 해당 시설 또는 층의 영상을 재생할 수 있습니다.
	**카메라 오류**: 카메라가 연결되지 않았거나, 전원이 꺼져 있는 경우에 표시됩니다.
	**열린 출입문**: 층(Floor)에 배치된 출입문이 열린 상태입니다.
	**잠긴 출입문**: 층(Floor)에 배치된 출입문이 잠긴 상태입니다.

옵션 기능

맵 또는 층에서 제공하는 옵션 기능은 아래와 같습니다.

기능	설명
	맵의 왼쪽 상단, 오른쪽 하단에 위치한 버튼을 클릭해 확대/축소할 수 있습니다. 또는 마우스 휠을 사용하여 맵을 확대하거나 축소할 수 있습니다.
	층의 오른쪽 하단에 위치한 버튼을 클릭해 확대/축소할 수 있습니다.
	버튼을 클릭하면 추가 기능을 이용할 수 있습니다.
×	비디오 타일에 위치한 맵 또는 층을 닫으려면 오른쪽 위에 버튼을 클릭하세요.
	아이콘을 클릭한 상태에서 드래그하면 맵을 다른 위치로 이동할 수 있습니다.

알아두기

- 맵 위에서 마우스를 클릭한 상태로 드래그하면 위치를 이동할 수 있습니다. 마우스 휠을 사용해 확대하거나 축소할 수 있습니다.
- 맵을 더블 클릭하면 전체 화면으로 확대됩니다. 다시 더블 클릭하거나 `ESC` 키를 누르면 원래 크기로 돌아갑니다.

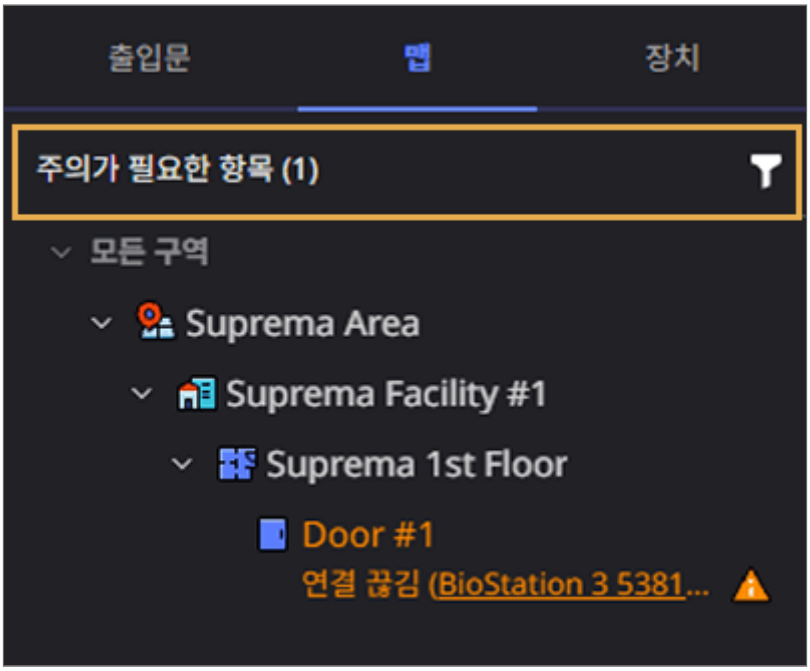
상태 점검하기

화면 왼쪽 사이드바에서 각 시설 또는 층의 출입문과 카메라 상태를 점검할 수 있습니다. 각 아이콘별 상태는 아래를 참고하세요.

상태 아이콘	설명
	멀티 커뮤니케이션 서버 오류이거나 연결이 끊긴 상태입니다.
	출입문에서 알람이 발생한 상태입니다. 배회 감지, 침입 감지 등이 발생하면 해당 아이콘이 표시됩니다.
	카메라가 연결된 상태입니다.
	카메라가 꺼져 있거나 연결이 해제된 상태입니다.

주의가 필요한 항목 모아보기

관리자는 조치가 필요한 항목만 한 번에 모아 볼 수 있습니다. 화면 왼쪽 사이드바의 **주의가 필요한 항목**을 클릭하세요. 구역, 시설, 층 계층에 배치된 출입문의 상태를 확인하고, 문제가 발생한 대상에 조치를 취할 수 있습니다.



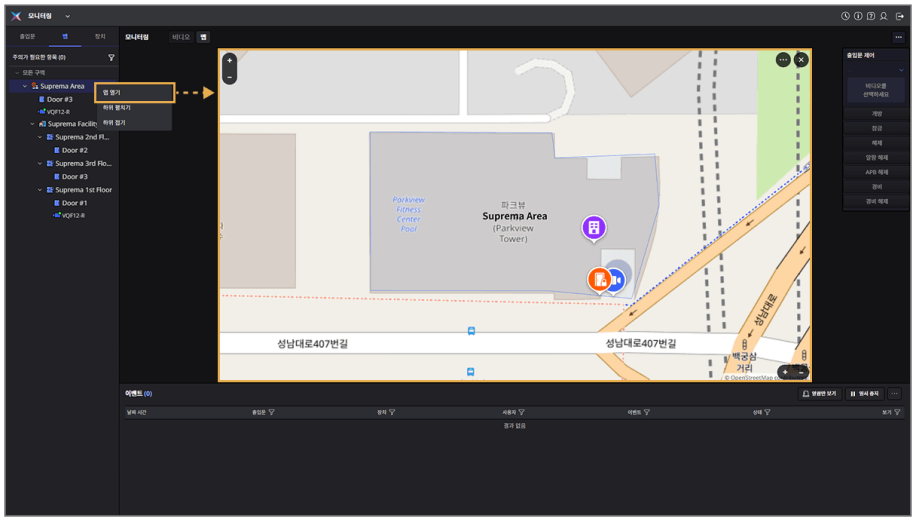
> **알아두기**
> 출입문 대상 조치 판정 기준은 상태 확인하기를 참고하세요.

맵 열기

구역이 GIS 지도와 연동되어 있다면, **모니터링** 섹션에 맵을 표시할 수 있습니다.

1. 화면 왼쪽 사이드바에서 맵으로 확인할 시설을 선택하세요.
2. 마우스 오른쪽 버튼을 클릭하세요.
3. 팝업 메뉴에서 **맵 열기**를 클릭하세요.

모니터링 섹션의 비디오 타일에 선택한 구역의 맵이 표시됩니다.

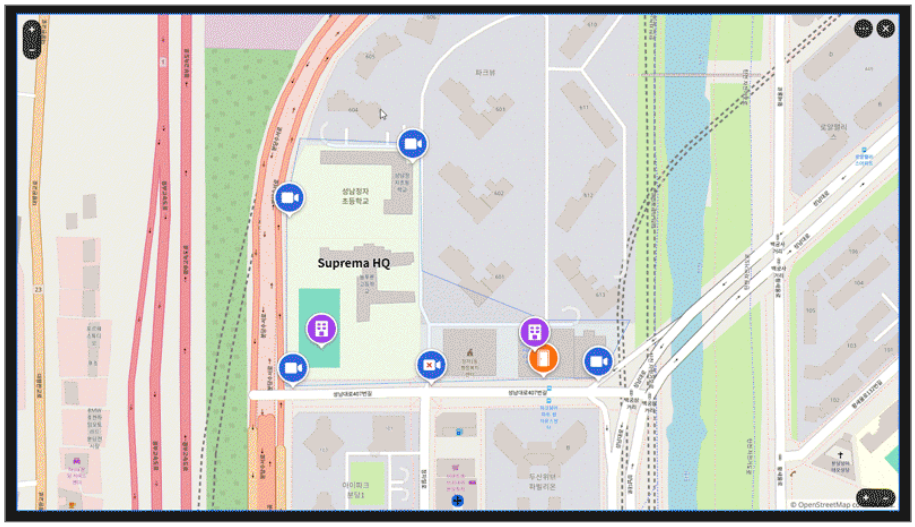


알아두기

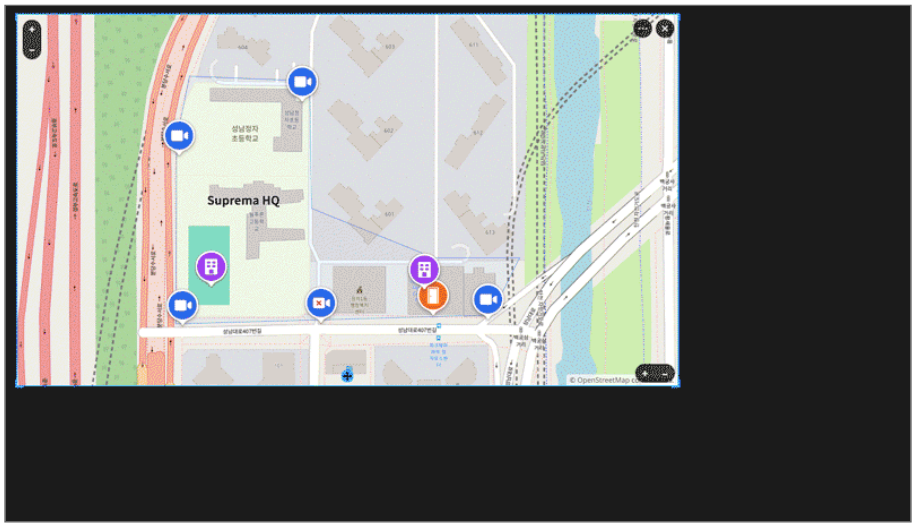
- 화면 왼쪽 사이드바에서 해당 시설을 더블 클릭하면 시설이 위치한 맵을 열 수 있습니다.
- 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.
- GIS 지도와 연동하여 구역을 구성하는 방법에 대한 자세한 내용은 구역 구성하기를 참고하세요.

맵 크기 조절 및 위치 이동

맵의 크기를 조절하려면 지도 상에서 빈 영역을 클릭하세요. 각 모서리에 크기를 조절할 수 있는 핸들이 표시됩니다. 핸들을 클릭한 상태에서 드래그하여 원하는 크기로 조절하세요.



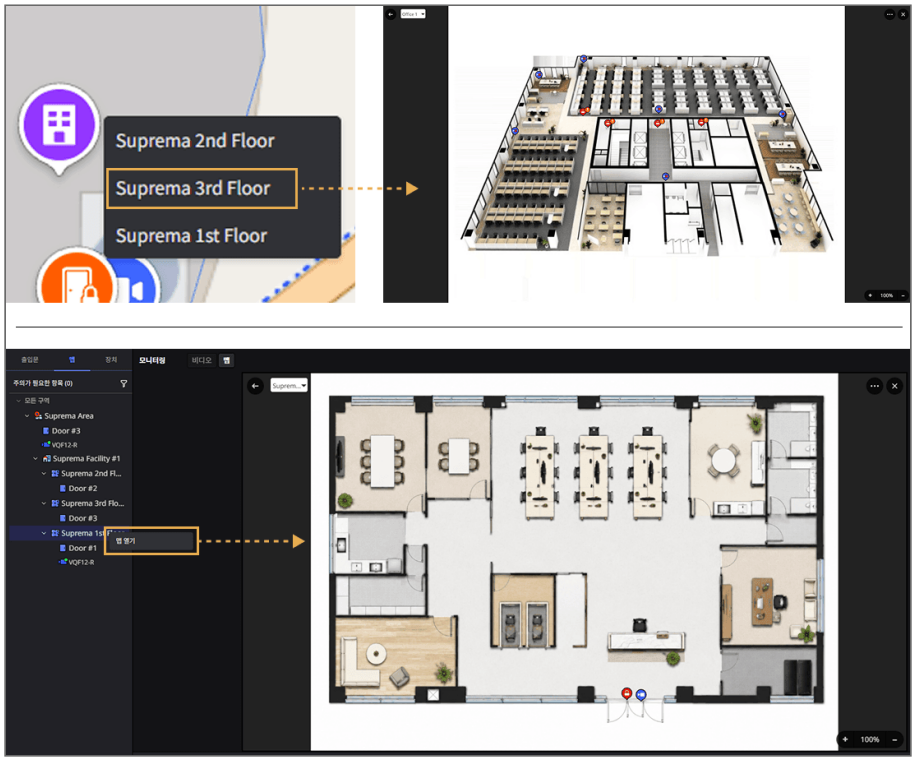
크기를 조절한 상태에서 맵을 다른 위치로 이동하려면 맵 위에 아이콘을 클릭한 상태에서 원하는 위치로 드래그하세요.



층으로 진입하기

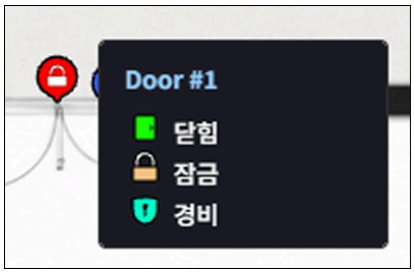
맵에서 층으로 진입하려면 시설(Facility)을 클릭하세요. 팝업 메뉴에 진입할 수 있는 층 목록이 표시되면 원하는 층을 선택하세요. 선택한 층의 도면과 출입문, 카메라를 확인할 수 있습니다.

또는 화면 왼쪽 사이드바에서 층을 더블 클릭하거나 마우스 오른쪽 버튼을 클릭하고 팝업 메뉴에서 **맵 열기**를 클릭하세요.



구성 요소	설명
	**열린 출입문**: 층(Floor)에 배치된 출입문이 열린 상태입니다.
	**잠긴 출입문**: 층(Floor)에 배치된 출입문이 잠긴 상태입니다.
	**카메라**: 카메라를 클릭하면 해당 시설 또는 층의 영상을 재생할 수 있습니다.

- 출입문 또는 카메라에 마우스를 오버하면 현재 상태를 확인할 수 있습니다.

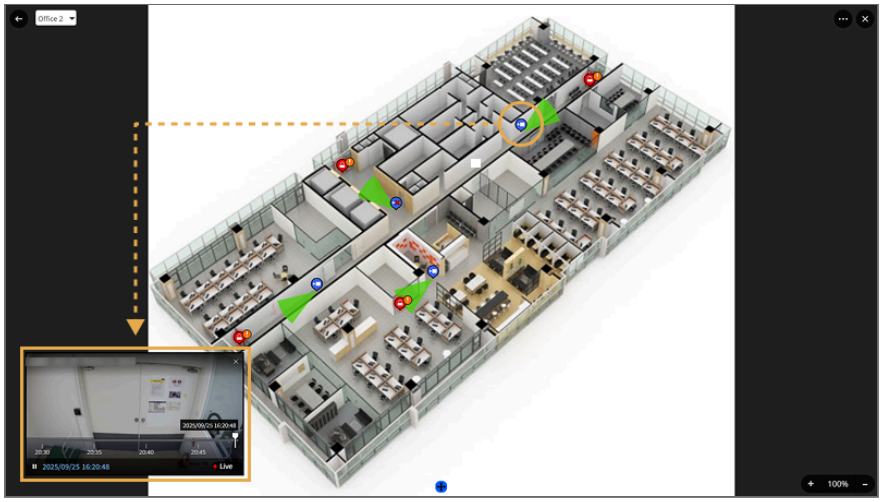




- 출입문을 클릭하면 해당 출입문을 제어할 수 있는 팝업 메뉴가 표시됩니다. 제공하는 기능에 대한 자세한 내용은 출입문 제어하기를 참고하세요.



- 카메라를 더블 클릭하면 실시간 영상을 재생할 수 있습니다.



알아두기

- 시설이 표시되는 맵으로 이동하려면 왼쪽 상단의 ← 버튼을 클릭하세요.
- 층(Floor)에 출입문과 카메라를 설정하는 방법에 대한 자세한 내용은 층 구성하기를 참고하세요.
- 영상 제어 방법 및 영상에 표시되는 도구에 대한 자세한 내용은 비디오 모니터링하기를 참고하세요.
- 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

다른 층으로 이동하기

다른 층으로 이동하려면 맵 왼쪽 상단의 선택 옵션을 클릭하고, 목록에서 이동하길 원하는 층을 선택하세요.



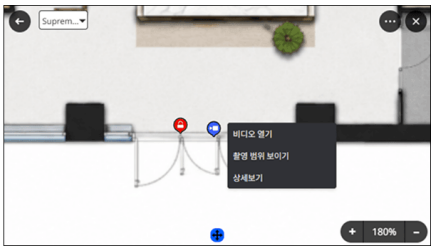
알아두기

- 시설이 표시되는 맵으로 이동하려면 왼쪽 상단의 ← 버튼을 클릭하세요.
- 맵 왼쪽 상단의 층 선택 옵션은 시설(Facility)에 설정되어 있는 층(Floor)만 표시합니다. 해당 층이 시설에 설정되어 있지 않으면 목록에 표시되지 않습니다. 시설에 층을 설정하는 방법에 대한 자세한 내용은 시설 구성하기를 참고하세요.

카메라 제어하기

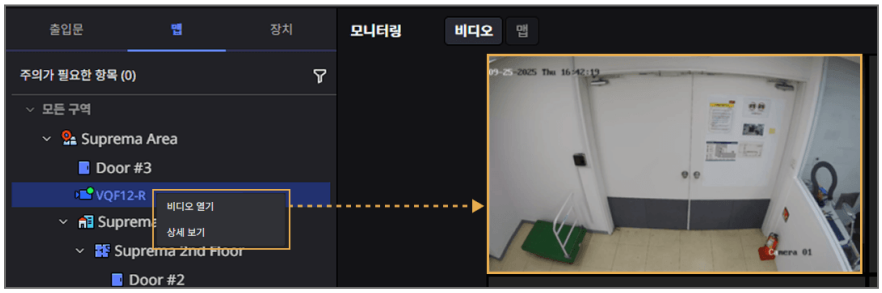
- 맵 또는 층에서 카메라를 제어하려면 카메라 아이콘을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택하세요.





  - **비디오 열기**: 카메라 영상을 실시간으로 확인할 수 있습니다.
  - **촬영 범위 보이기** / **촬영 범위 숨기기**: 카메라의 촬영 범위를 표시하거나 숨길 수 있습니다.
  - **상세보기**: 카메라의 상세 정보를 확인할 수 있습니다. 화면 오른쪽 패널에 카메라의 이름, 그룹, 아이디, IP 주소 등을 표시합니다.

- 비디오 타일에 카메라 영상을 배치하고 재생하려면, 화면 왼쪽 사이드바의 **맵** 목록에서 카메라를 더블 클릭하세요. 또는 마우스 오른쪽 버튼을 클릭하고 팝업 메뉴에서 **비디오 열기**를 클릭하세요.



카메라의 이름, 그룹 등과 같은 상세 정보를 확인하려면 팝업 메뉴에서 **상세 보기**를 클릭하세요.

알아두기

- 비디오 타일에는 화면 왼쪽 상단부터 차례로 추가되며, 현재 화면에 추가할 공간이 없으면 에러 메시지가 표시됩니다.
- 영상 제어 방법 및 영상에 표시되는 도구에 대한 자세한 내용은 비디오 모니터링하기를 참고하세요.
- 맵에서 카메라가 보이지 않는다면 카메라 그룹 권한을 확인하세요. 커스텀 권한의 관리자가 카메라 그룹 권한을 설정하지 않았다면 카메라가 보이지 않을 수 있습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.

장치 모니터링하기

장치 및 카메라 모니터링 기능을 사용하는 방법을 안내합니다. 장치와 카메라의 상태를 점검하고, 상세 정보를 확인하며, 카메라 영상을 실시간으로 재생하는 등 다양한 기능을 활용할 수 있습니다. 또한, 최근 발생한 이벤트를 확인하여 장치와 카메라의 상태를 효율적으로 관리하는 방법을 확인하세요.

모니터링 페이지는 **런처** 페이지에서 **모니터링**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **모니터링**을 선택하여 진입할 수 있습니다.

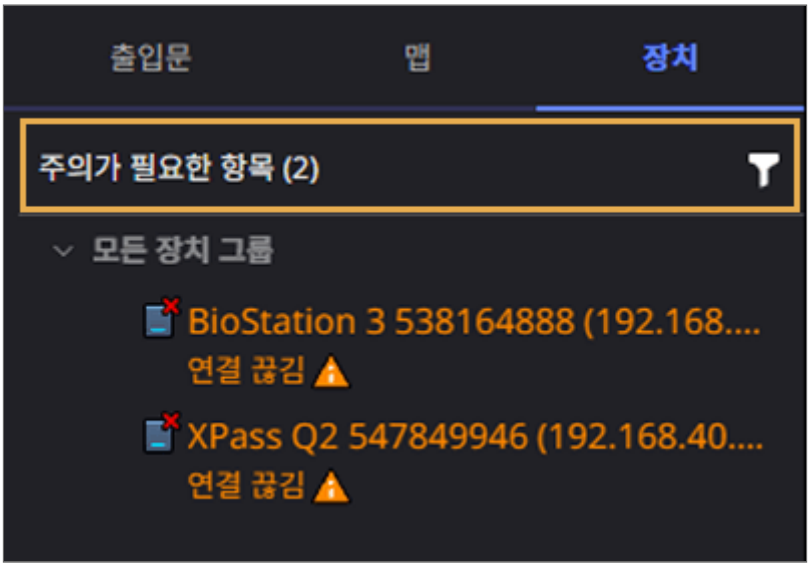
장치 및 카메라 상태 점검

화면 왼쪽 사이드바에서 **장치** 탭을 클릭하세요. 모든 장치와 카메라의 상태를 점검할 수 있습니다. 장치와 카메라의 상태는 아래를 참고하세요.

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

주의가 필요한 장치 모아보기

관리자는 조치가 필요한 장치만 한 번에 모아 볼 수 있습니다. 화면 왼쪽 사이드바의 **주의가 필요한 항목**을 클릭하세요. 장치의 상태를 확인하고, 문제가 발생한 대상에 조치를 취할 수 있습니다.



조치 대상 판정 기준

장치 트리에서 정상이 아닌 장치를 조치 대상으로 판정합니다.

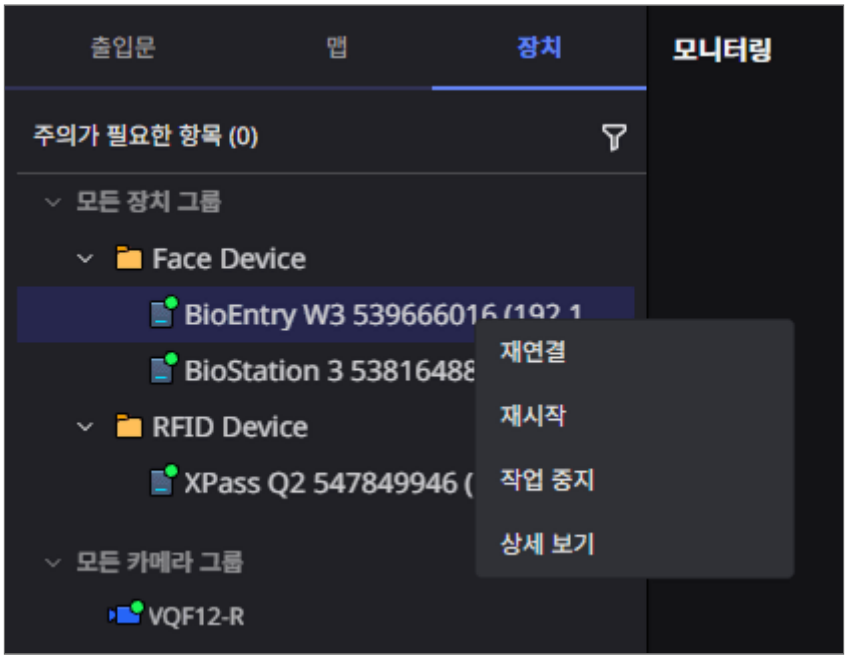
이상 상태 종류	상태 표시	설명
연결 끊김	**연결 끊김**	장치와의 네트워크 연결이 끊긴 상태
동기화 오류	**동기화 오류**	연결은 되어 있으나 데이터 동기화가 어긋난 상태
멀티 커뮤니케이션 서버 오류	**커뮤니케이션 서버 오류**	장치가 속한 멀티 커뮤니케이션 서버에서 오류가 발생한 상태
장치 잠금	**장치 잠금**	작업 조건 및 동작에 의해 장치가 잠긴 상태
인증 실패 잠금	**인증 실패 잠금**	지정한 횟수 이상 인증에 실패하여 장치가 잠긴 상태

알아두기

- **장치 잠금** 조건은 작업 조건 및 동작 설정하기에서 설정한 작업 조건 및 동작에 따라 결정됩니다. 이 상태를 확인하고 해제하는 방법은 장치 잠금 해제를 참고하세요.
- **인증 실패 잠금** 조건은 장치 설정에서 구성할 수 있습니다. 자세한 내용은 인증 설정하기를 참고하세요. 이 상태를 확인하고 해제하는 방법은 인증 실패 잠금 해제를 참고하세요.

장치 제어

화면 왼쪽 사이드바의 장치 목록에서 원하는 장치를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택할 수 있습니다.



장치 유형에 따라 표시되는 제어 기능은 다를 수 있습니다.

장치 유형	제어 기능
마스터 장치, 슬레이브 없이 서버에 직접 연결되는 기본 장치	**작업 중지**, **재시작**, **장치 잠금 해제**, **인증 실패 잠금 해제**, **재연결**(서버에서 장치로 연결하는 방식일 때만)
슬레이브 장치	**작업 중지**, **재시작**, **장치 잠금 해제**, **인증 실패 잠금 해제**
OSDP 통신 장치	**장치 잠금 해제**, **재연결**(연결 방식에 따라 다름)
Wiegand 장치	**장치 잠금 해제**
확장 모듈(Secure I/O 2, DM-20, OM-120, IM-120)	**작업 중지**
장치에서 서버로 연결하는 방식의 장치	**작업 중지**, **재시작**, **장치 잠금 해제**, **인증 실패 잠금 해제**
무선 안테나 모듈	없음

장치 재연결

장치의 연결 상태와 관계없이 팝업 메뉴에서 **재연결**을 클릭하세요. 연결이 끊긴 장치는 다시 연결을 시도하고, 정상 연결된 장치는 설정을 다시 전송하거나 이상 상태를 해소하는 용도로 사용할 수 있습니다. 장치가 다시 연결되면 상태 아이콘이 정상 상태( )로 변경됩니다.

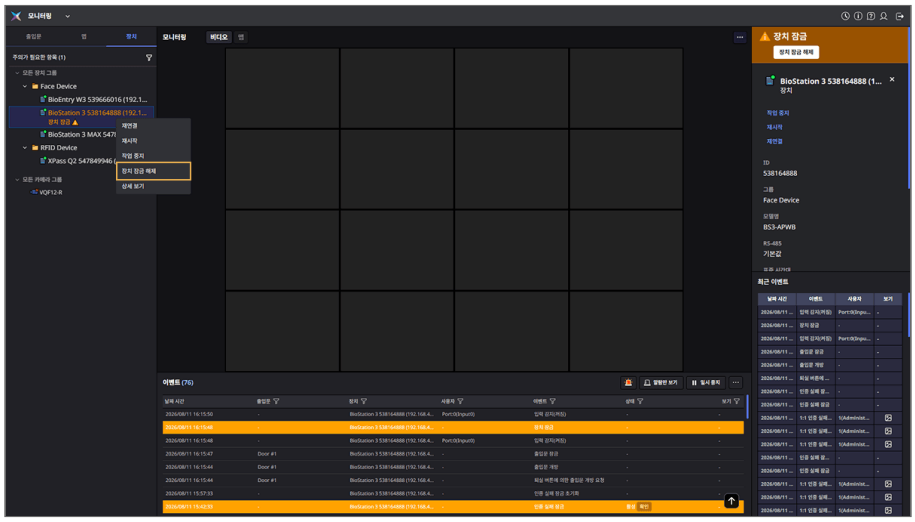
> **알아두기**
> **재연결** 기능은 **장치에서 서버 연결** 옵션으로 설정된 장치는 지원하지 않습니다. 장치 등록에 대한 자세한 내용은 장치 등록하기를 참고하세요.

장치 재시작

장치를 재시작하려면, 팝업 메뉴에서 **재시작**을 클릭하세요. 경고 메시지 창이 나타나면 **확인** 버튼을 클릭하세요.

장치 잠금 해제

관리자가 설정한 작업 조건 및 동작에 의해 장치가 잠기면, 화면 왼쪽 사이드바의 장치 이름 아래에 **장치 잠금** 상태가 표시됩니다. 장치를 선택하면 화면 오른쪽 미리보기 패널 상단에도 같은 배너가 나타납니다.



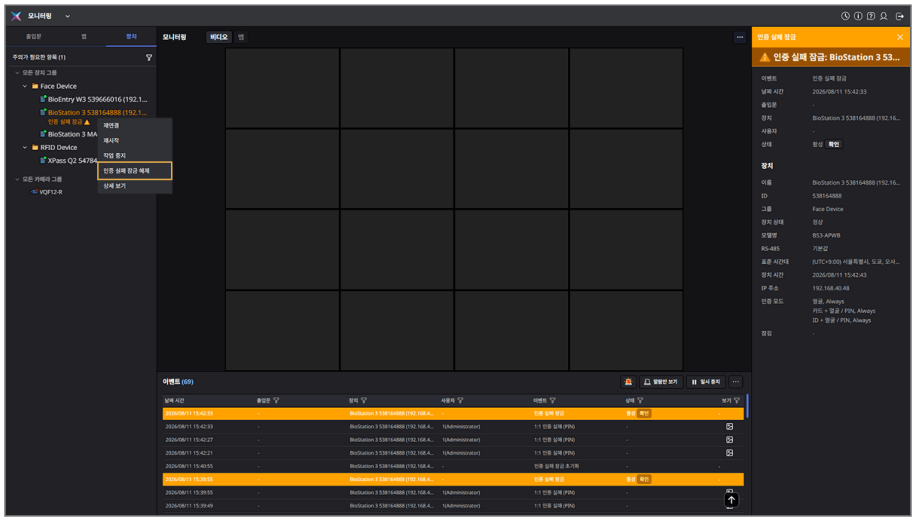
- 장치가 잠금 상태일 때만 팝업 메뉴에 **장치 잠금 해제**가 표시됩니다. 잠금 상태를 해제하려면 잠긴 장치를 선택하고 팝업 메뉴에서 **장치 잠금 해제**를 클릭하세요.
- 잠긴 장치를 선택하면 화면 오른쪽 미리보기 패널 상단에 나타나는 배너에서 **장치 잠금 해제** 버튼을 클릭하세요.

> **알아두기**
> **장치 잠금 해제** 기능은 **전체 관리자** 또는 **모니터링 관리자** 권한이 있는 사용자에게만 표시됩니다.

인증 실패 잠금 해제

인증 실패 잠금 옵션에서 설정한 횟수 이상 인증에 실패하면 장치가 잠금 상태로 전환됩니다. 장치가 잠금 상태이면 화면 왼쪽 사이드바의 장치 이름 아래에 **인증 실패 잠금** 상태가 표시되고, 장치를 선택하면 화면 오른쪽 미리보기 패널 상단에도 같은 배너가 나타나며 이벤트 발생 시각과 장치 정보를 확인할 수 있습니다.

장치가 인증 실패 잠금 상태일 때만 팝업 메뉴에 **인증 실패 잠금 해제**가 표시됩니다. 잠긴 장치를 선택하고 팝업 메뉴에서 **인증 실패 잠금 해제**를 클릭하세요.



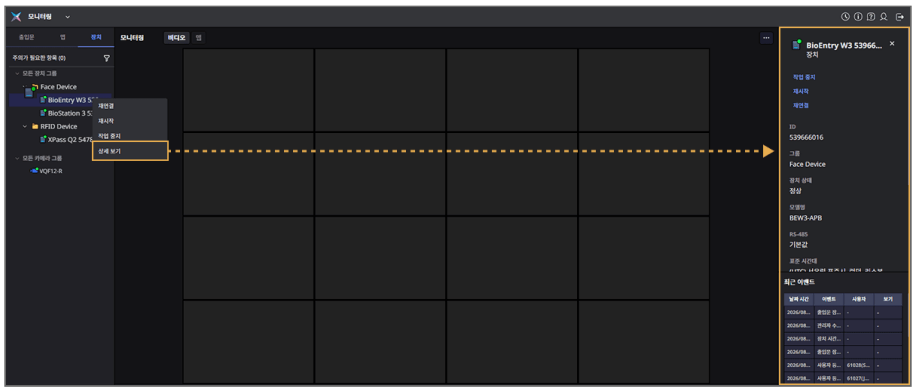
> **알아두기**
>
> - **인증 실패 잠금 해제** 메뉴는 **전체 관리자** 또는 **모니터링 관리자** 권한이 있는 사용자에게만 표시됩니다.
> - 설정한 잠금 시간(**1차 잠금 시간**/**2차 잠금 시간**)이 지나면 장치가 자동으로 잠금을 해제합니다. 이때는 별도 조치 없이도 잠금 상태가 해소됩니다. 잠금 조건 및 잠금 시간 설정에 대한 자세한 내용은 인증 설정하기를 참고하세요.

작업 중지

장치에서 실행 중인 알람 기반, 트리거 기반 동작을 모두 중지하려면 팝업 메뉴에서 **작업 중지**를 클릭하세요. 화면 상단에 작업 중지 성공 메시지가 나타납니다.

장치 상세 보기

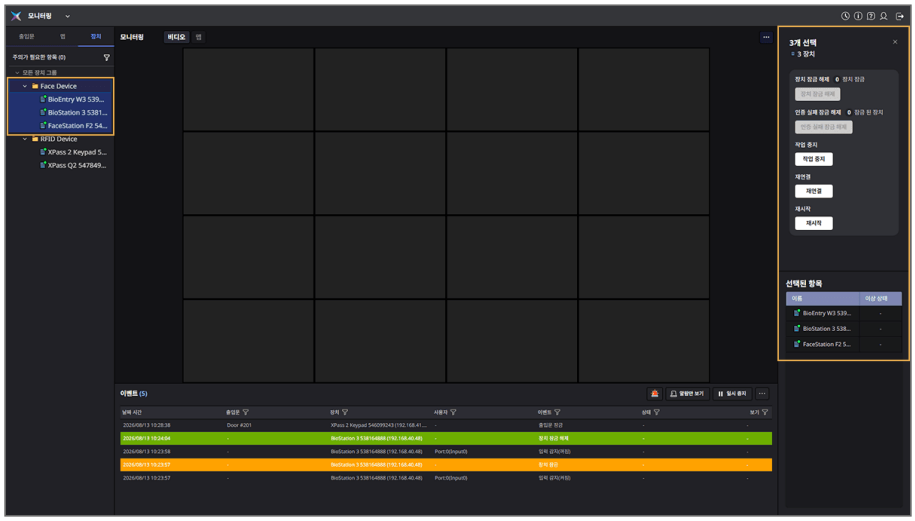
장치의 상세 정보를 확인하려면, 팝업 메뉴에서 **상세 보기**를 클릭하세요. 또는 장치를 더블 클릭하세요. 화면 오른쪽에 장치의 상세 정보가 나타납니다.



- **장치 제어**: 장치 작업 중지 또는 재시작, 재연결 등의 제어 기능을 실행할 수 있습니다.
- **장치 상세 정보**: 장치의 ID 및 그룹, 모델명, 기동 시간, IP 주소 등의 정보를 확인할 수 있습니다.
- **최근 이벤트**: 선택한 장치에서 발생한 최근 이벤트 목록을 확인할 수 있습니다.

여러 장치 한 번에 제어하기

여러 장치를 한 번에 선택해서 재연결, 재시작, 잠금 해제 등의 명령을 한 번에 실행하는 방법을 안내합니다. 화면 왼쪽 사이드바의 **장치** 탭에서 장치를 두 개 이상 선택하면 화면 오른쪽에 일괄 제어 패널이 나타납니다.



> **알아두기**
> 카메라는 일괄 제어 대상이 아닙니다. 카메라 제어 방법은 카메라 제어를 참고하세요.

여러 장치 선택하기

화면 왼쪽 사이드바의 **장치** 탭에서 장치를 선택하는 방법은 다음과 같습니다.

- `Ctrl` + **클릭**: 클릭한 장치를 선택 목록에 추가하거나 제외합니다. 나머지 선택은 그대로 유지됩니다.
- `Shift` + **클릭**: 마지막으로 클릭한 장치부터 지금 클릭한 장치까지 범위를 선택합니다. 장치 그룹은 범위 선택 대상이 아닙니다.
- **그룹(📁) 클릭**: 그룹 이름을 클릭하면 그 아래에 있는 모든 장치가 선택 목록에 추가됩니다. 이미 선택한 장치는 그대로 유지됩니다.

> **알아두기**
> - 하위에 장치가 없는 빈 그룹만 선택하면 화면 오른쪽 패널이 닫힙니다.
> - 장치를 한 개만 선택하면 장치 상세 정보 패널이 나타나고, 두 개 이상 선택하면 일괄 제어 패널로 전환됩니다.



일괄 제어 패널 구성

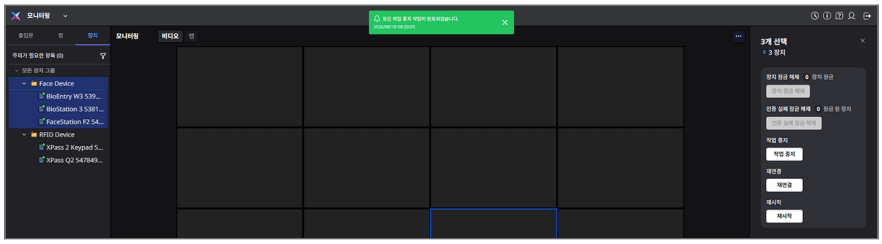
- **장치 잠금 해제**, **인증 실패 잠금 해제**: 선택한 장치 중 각각 잠금·인증 실패 잠금 상태인 장치가 있을 때 활성화되며, 버튼 옆에 대상 장치 수가 함께 표시됩니다.
- **작업 중지**, **재연결**, **재시작**: 대상 장치 수를 표시하지 않고, 선택한 장치 중 해당 제어를 지원하는 장치가 있으면 활성화됩니다.
- **장치 제어**: **장치 잠금 해제**, **인증 실패 잠금 해제**, **작업 중지**, **재연결**, **재시작** 기능 실행 버튼을 사용할 수 있습니다.
- **구분 경계선**: 장치 제어 영역과 **선택된 항목** 사이의 경계선을 위아래로 드래그하면 두 영역의 높이 배분을 조절할 수 있습니다.
- **선택된 항목**: 선택한 장치의 연결 상태 및 이름, 이상 상태를 확인할 수 있습니다. 이상 상태 종류는 조치 대상 판정 기준을 참고하세요.

각 버튼을 클릭하면 확인 창이 나타납니다. 확인 창에서 **취소**를 클릭하면 선택한 기능을 실행하지 않고, 선택한 기능이 표시된 버튼을 클릭하면 선택한 장치 전체로 해당 기능을 실행합니다.

> **알아두기**
>
> 선택한 장치 유형이 섞여 있으면 각 장치가 지원하는 제어를 합쳐서 표시합니다. 선택한 장치 중 어느 장치도 지원하지 않는 제어는 버튼이 나타나지 않으며, 지원하는 제어가 하나도 없으면 안내 문구와 선택 장치 목록 표만 표시됩니다.

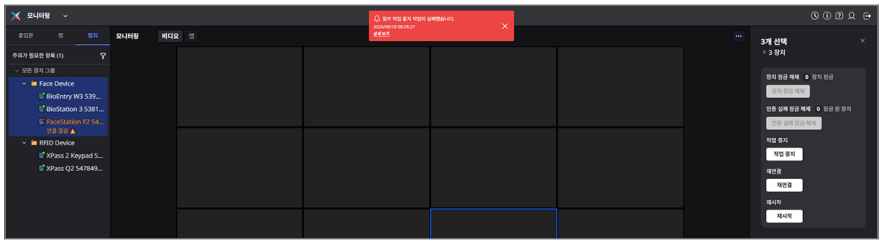
실행 결과 확인하기

- 선택한 모든 장치가 성공하면 성공 메시지만 표시됩니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- 한 개의 장치라도 실패하면 실패 메시지와 함께 **상세 보기** 버튼이 표시됩니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

상세 보기를 클릭하면 **성공**, **실패**, **대상 아님** 세 그룹으로 구분된 결과를 확인할 수 있습니다. 실패한 항목의 이름과 사유를 클립보드에 복사하려면 **실패 내역 복사** 버튼을 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

알아두기

- **재연결** 버튼은 예외입니다. 요청이 접수되면 항상 성공 메시지만 표시되며, 실패 여부나 상세 결과 창은 제공되지 않습니다. 실제 연결 성공 여부는 상태 트리에서 확인하세요.
- **장치 잠금 해제**와 **인증 실패 잠금 해제**는 각각 별도로 처리되어 결과 창도 따로 표시됩니다.

카메라 제어

화면 왼쪽 사이드바의 카메라 목록에서 원하는 카메라를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 원하는 기능을 선택할 수 있습니다.



카메라 영상 재생

비디오 타일에 카메라 영상을 배치하고 실시간으로 모니터링하려면, 팝업 메뉴에서 **비디오 열기**를 클릭하세요.

비디오 타일에 카메라 영상을 추가하는 방법은 아래와 같은 방식도 지원합니다.

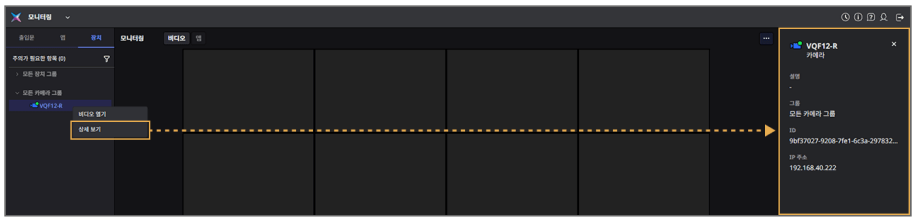
- 화면 왼쪽 사이드바의 카메라 목록에서 영상을 재생할 카메라를 더블 클릭하세요.
- 카메라를 비디오 타일 영역으로 드래그 앤 드롭 방식으로 영상을 추가할 수도 있습니다.

알아두기

- 비디오 타일에는 화면 왼쪽 상단부터 차례로 추가되며, 현재 화면에 추가할 공간이 없으면 에러 메시지가 표시됩니다.
- 영상 제어 방법 및 영상에 표시되는 도구에 대한 자세한 내용은 비디오 모니터링하기를 참고하세요.
- **모든 카메라 그룹** 목록에서 카메라가 보이지 않는다면 카메라 그룹 권한을 확인하세요. 커스텀 권한의 관리자가 카메라 그룹 권한을 설정하지 않았다면 카메라가 보이지 않을 수 있습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.

카메라 상세 보기

카메라의 상세 정보를 확인하려면, 팝업 메뉴에서 **상세 보기**를 클릭하세요. 카메라의 그룹, 설명, 아이디와 IP 주소를 확인할 수 있습니다.

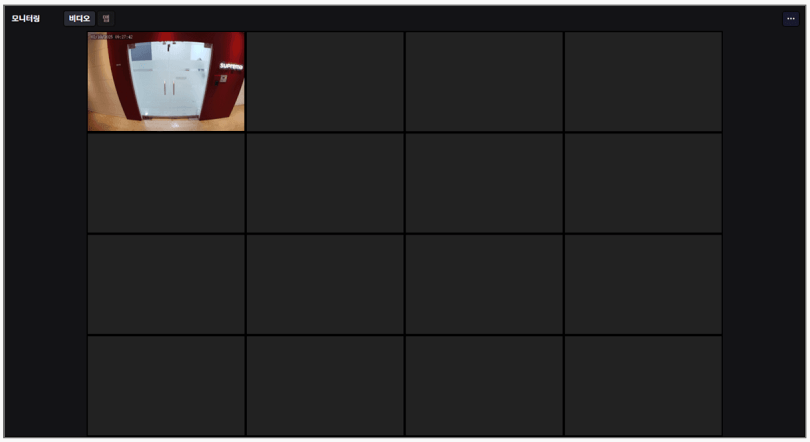


비디오 모니터링하기

비디오 모니터링 기능을 통해 출입문, 구역, 장치와 연계된 카메라 영상을 실시간으로 확인하고 제어할 수 있습니다. 이 문서에서는 비디오 타일을 활용하여 카메라 영상을 추가하고, 크기 조정, 위치 변경, 전체 화면 보기 등 다양한 작업을 수행하는 방법을 안내합니다. 또한, 알람 상태 확인 및 해제와 같은 관리 기능을 통해 보안 상황에 신속히 대응할 수 있도록 지원합니다.

알아두기

- **비디오 타일**은 화면 중앙에 위치한 카메라 영상 표시 영역입니다. 여러 개의 카메라 영상을 동시에 배치하고 모니터링할 수 있는 인터페이스 구성 요소입니다. 사용자는 비디오 타일에서 영상의 크기를 조정하거나 위치를 변경하고, 필요에 따라 영상을 닫거나 전체 화면으로 전환할 수 있습니다.



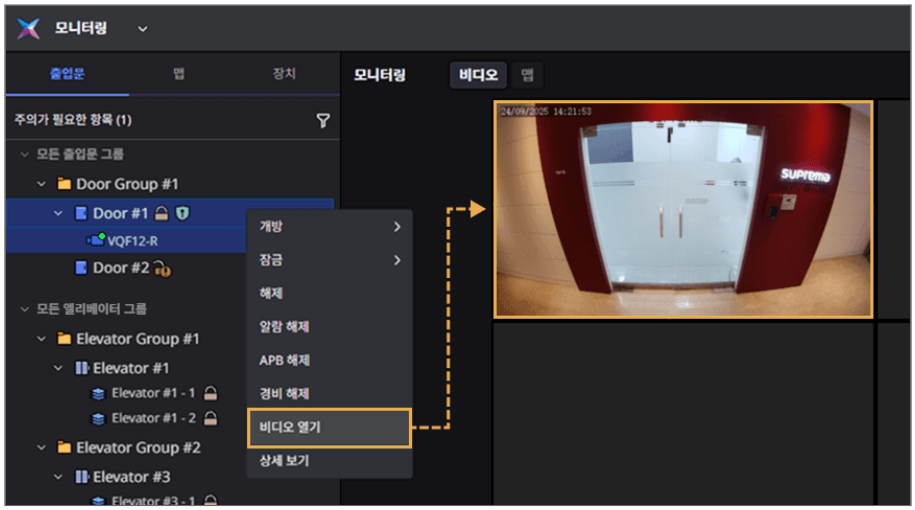
- **모니터링** 영역은 시스템에 등록된 장치 카메라가 없거나 맵 구성 요소(구역, 시설, 층)가 등록되어 있지 않으면 활성화되지 않습니다.
- VMS와 연동하고 카메라를 추가 및 관리하는 방법은 비디오 설정하기를 참고하세요.
- VMS의 녹화 영상을 재생할 때 로드 에러가 발생한다면, VMS 서버에 인증서를 설치하고, 클라이언트 PC에서 VMS 서버의 인증서를 설치해야 합니다. 자세한 내용은 다음 문서를 참고하세요.
  - VMS 서버에서 인증서 설치
  - 클라이언트 PC에서 VMS 서버 인증서 설치
- 구역과 연동된 카메라가 보이지 않는다면 카메라 그룹 권한을 확인하세요. 커스텀 권한의 관리자가 카메라 그룹 권한을 설정하지 않았다면 카메라가 보이지 않을 수 있습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.
- 비디오 모니터링은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

영상 재생하기

비디오 타일에 카메라 영상을 추가하여 모니터링할 수 있습니다. 비디오 타일은 화면 가운데 위치하며, 여러 개의 카메라 영상을 동시에 모니터링할 수 있습니다.

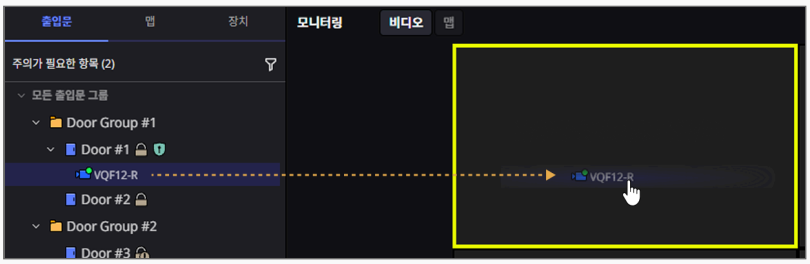
1. 화면 왼쪽 사이드바에서 **출입문** 또는 **맵**, **장치** 탭에서 영상을 확인할 카메라 장치를 선택하세요.
2. 마우스 오른쪽 버튼을 클릭하세요.
3. 팝업 메뉴에서 **비디오 열기**를 클릭하세요.

선택한 카메라의 영상을 화면 가운데 비디오 타일에 배치할 수 있습니다.



알아두기

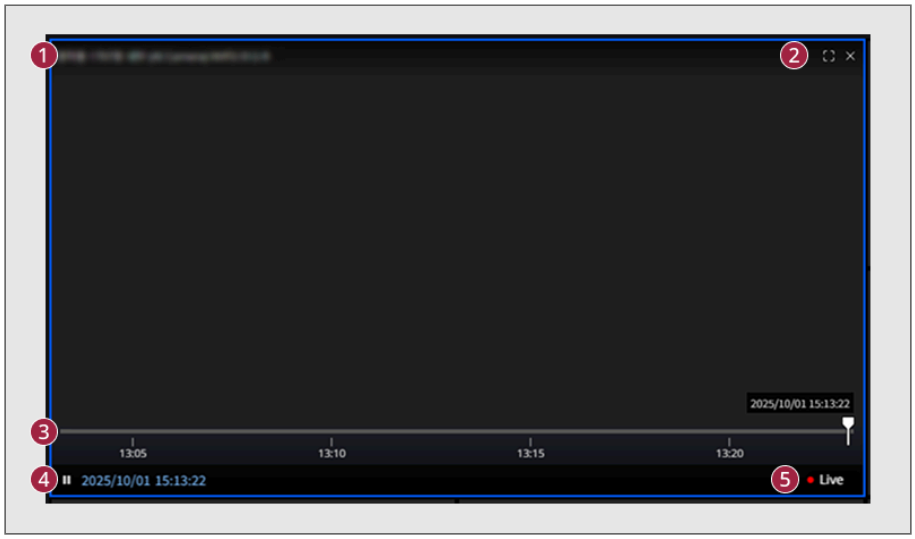
- 사이드바의 목록에서 카메라를 선택하고 비디오 타일 영역으로 드래그 앤 드롭 방식으로 영상을 추가할 수도 있습니다.



- 비디오 타일에는 화면 왼쪽 상단부터 차례로 추가되며, 현재 화면에 추가할 공간이 없으면 에러 메시지가 표시됩니다.

영상 제어하기

비디오 타일에 배치한 영상은 기본적으로 실시간 재생됩니다. 영상의 재생 도구를 통해 영상을 멈추거나 과거 시간의 녹화된 영상을 조회할 수 있습니다.



1. 카메라 장치의 이름입니다.
2. 영상을 전체 화면(⛶)으로 재생하거나 비디오 타일에서 제외(✕)할 수 있는 버튼입니다.
3. 영상의 재생 위치를 조정할 수 있는 슬라이더입니다. 슬라이더를 드래그하여 과거 시간의 영상을 조회할 수 있습니다.
4. 영상을 재생하거나 일시 정지하려면 ▶ 또는 ⏸ 버튼을 클릭하세요.
5. 현재 영상을 실시간 재생하고 있음을 나타내는 아이콘입니다. 과거 시간의 영상을 재생할 때 다시 실시간 영상으로 전환하려면 이 아이콘을 클릭하세요.

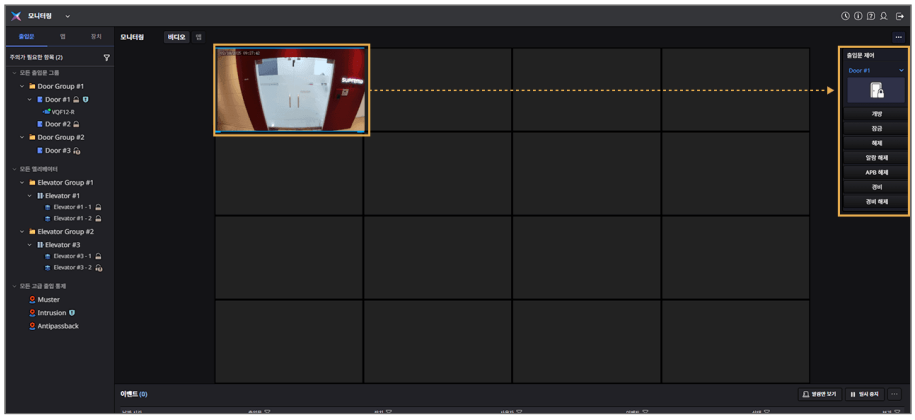
녹화 영상 재생 유지 및 실패 안내

비디오 탭에서 다른 화면으로 이동한 뒤(예: 다른 페이지로 이동, **맵** 탭으로 전환, 새로고침) 다시 **비디오** 탭으로 돌아오면 이전에 재생하던 녹화 영상 상태를 그대로 유지합니다. 이때 각 비디오 타일은 배치된 순서대로 영상을 다시 불러옵니다.

> **알아두기**
> 영상마다 응답 속도가 달라 재생 실패가 표시되는 시점은 타일마다 다를 수 있습니다. 다만 재생에 실패하는 타일은 대체로 타일 순서상 뒤쪽부터 나타나는 경향이 있습니다.

출입문 제어 도구

영상을 추가한 후 **출입문 제어** 도구를 활용해 추가 작업을 수행할 수 있습니다. 비디오 타일에서 출입문과 연계된 카메라를 선택하면 출입문을 제어할 수 있는 **출입문 제어** 도구가 활성화됩니다. 출입문을 개방하거나 잠금, 해제, 알람 해제 등의 기능을 사용할 수 있습니다.

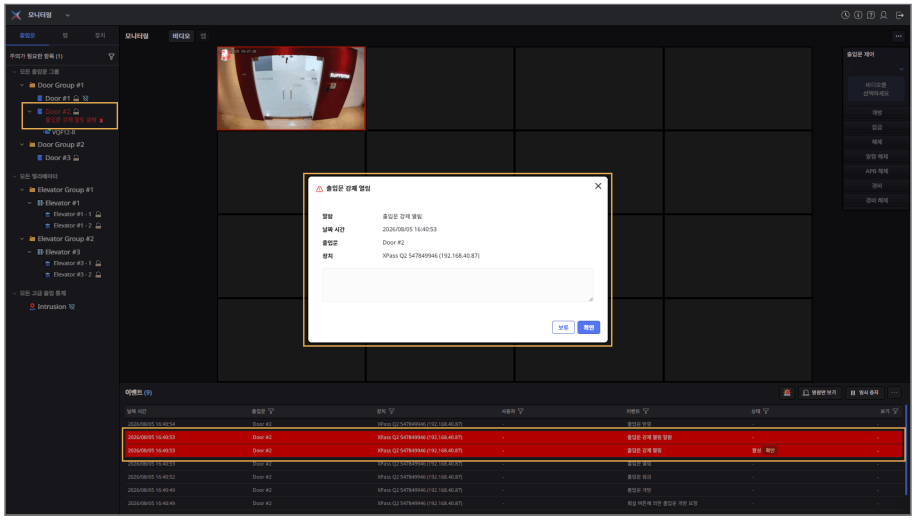


알아두기

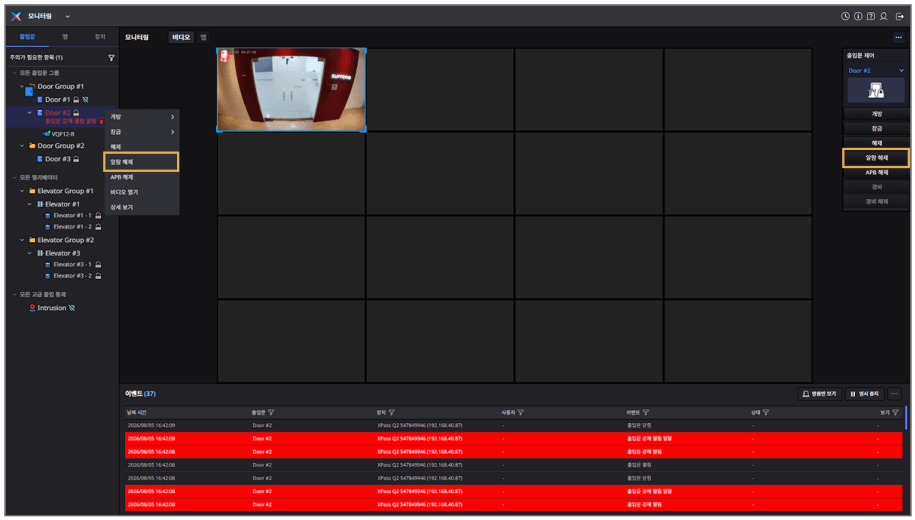
- **출입문 제어** 도구는 오른쪽 패널에 아무것도 열려있지 않을 때 사용할 수 있습니다. 오른쪽 패널에 상세 정보가 열려있다면 닫은 채로 사용하세요.
- 이 기능은 출입문에 카메라가 연계되어 있어야 사용할 수 있습니다. 출입문과 카메라 연동에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.
- **출입문 제어** 도구에서 사용할 수 있는 기능에 대한 자세한 내용은 출입문 제어하기를 참고하세요.

영상 알람 확인하기

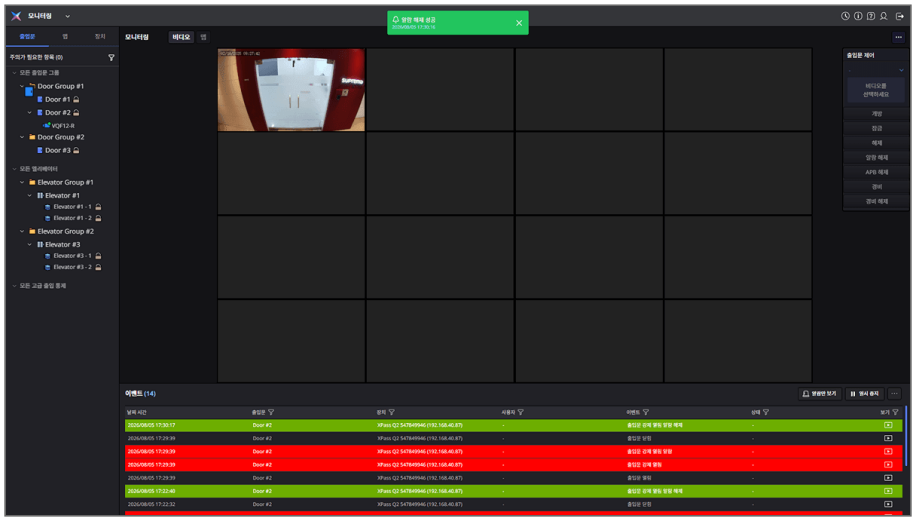
카메라와 연계된 출입문 중 하나가 알람 상태가 되면 영상에 알람 아이콘이 표시됩니다. 연계된 출입문의 알람을 모두 해제해야 알람 아이콘이 사라집니다.



출입문의 알람을 해제하려면 출입문 목록에서 오른쪽 마우스 버튼을 클릭하고, 팝업 메뉴에서 **알람 해제**를 클릭하세요. 또는 **출입문 제어** 도구에서 **알람 해제**를 클릭하세요.



화면 상단에 성공 또는 실패 메시지가 표시됩니다.

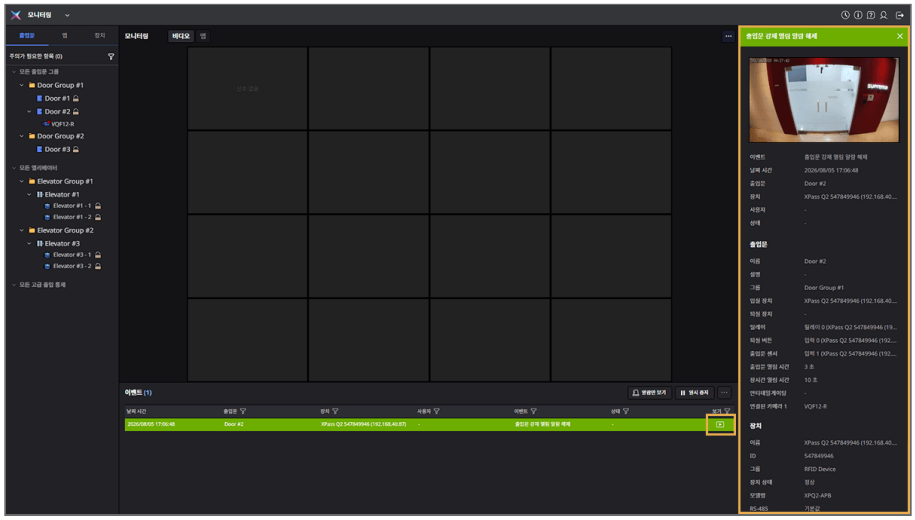


알아두기

화면 아래의 **이벤트** 섹션에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

비디오 로그 확인하기

규칙으로 설정된 출입문에 특정 이벤트가 발생하면 **이벤트** 섹션 목록의 해당 이벤트 항목에는 비디오 로그(▶) 아이콘이 표시됩니다. 비디오 로그 아이콘이 표시된 이벤트 항목을 클릭하면 화면 오른쪽에 상세 정보가 나타납니다. 특정 이벤트가 발생한 시간의 영상을 확인할 수 있습니다.



알아두기

- 비디오 로그 아이콘은 출입문에 카메라가 연계되어 있어야 표시됩니다. 카메라와 출입문 연동에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.
- 이벤트 설정 규칙 기준 가장 첫 번째로 연결한 카메라를 우선 재생합니다. 영상을 보다 큰 화면으로 재생하려면 화면을 더블 클릭하세요.
- 출입문에는 최대 4개의 카메라를 연결할 수 있으며, 영상 하단의 카메라 버튼을 클릭해 원하는 카메라의 영상을 재생할 수 있습니다. 연결된 카메라가 한 개라면 카메라 버튼은 표시되지 않습니다.
- 화면 아래의 **이벤트** 섹션에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

비디오 타일 레이아웃 설정

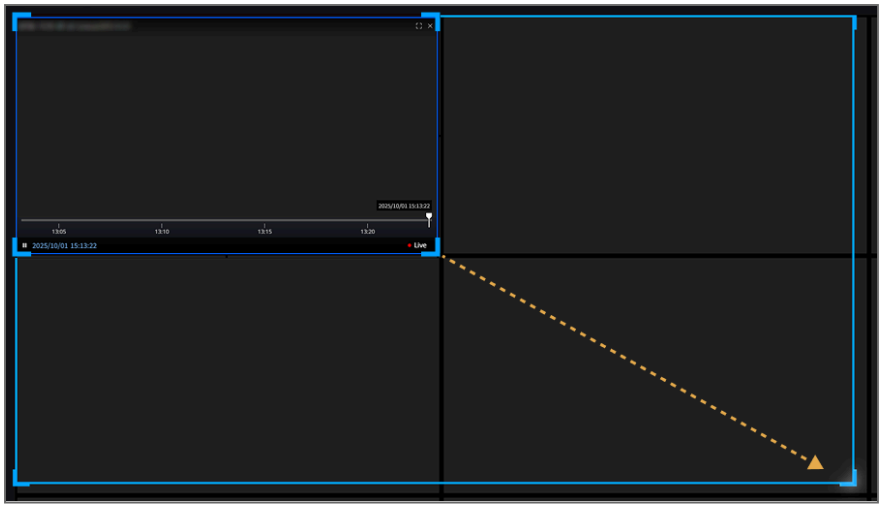
비디오 타일에 배치한 영상은 크기를 변경하거나 원하는 위치로 변경할 수 있습니다. 중요도에 따라 영상의 크기를 조정하고 위치를 변경하여 모니터링하세요.

영상 크기 변경

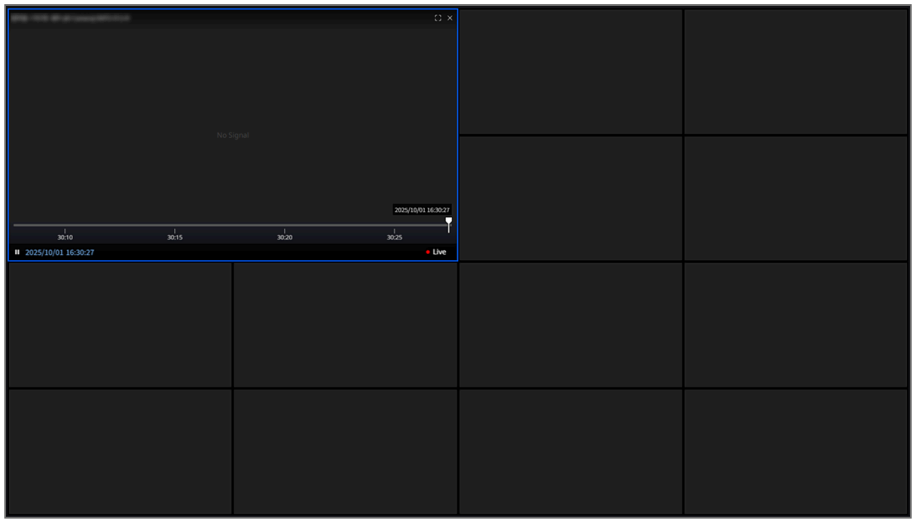
1. 영상의 크기를 변경할 비디오를 클릭하면 선택한 영상의 프레임이 활성화됩니다.



2. 프레임의 경계 위로 마우스 커서를 가져가면, 크기를 조절할 수 있는 커서 모양으로 변경됩니다.
3. 모서리를 클릭하고 원하는 크기로 드래그하세요.

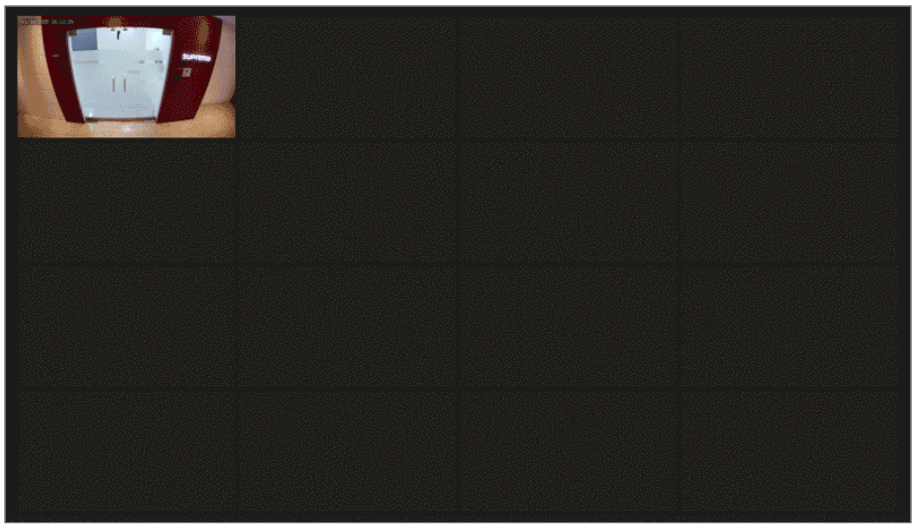


배치된 타일의 크기에 비례하여 영상의 크기를 조절할 수 있습니다. 반대로 영상의 크기를 줄일 수도 있습니다.



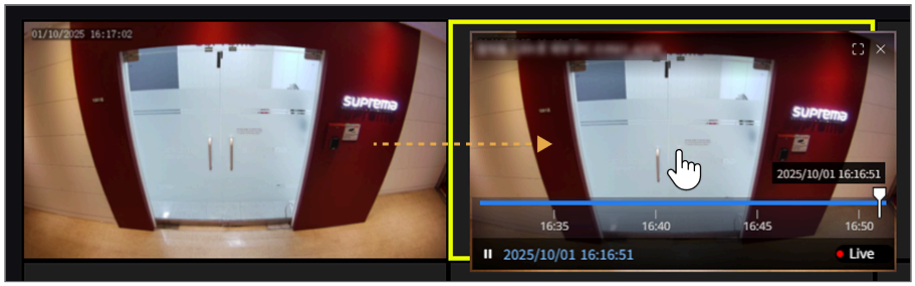
영상 크기 확대

영상을 비디오 타일 전체 크기로 확대하려면 영상을 더블 클릭하세요. 영상이 비디오 타일의 크기로 확대됩니다.

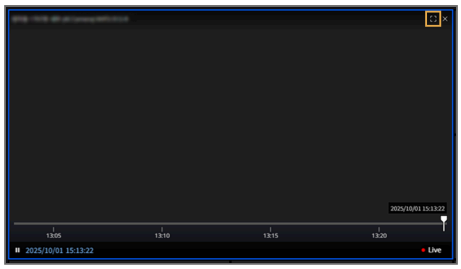


영상 위치 변경하기

위치를 변경할 영상을 클릭하고 원하는 위치로 드래그하세요. 선택한 영상의 위치를 변경할 수 있습니다.



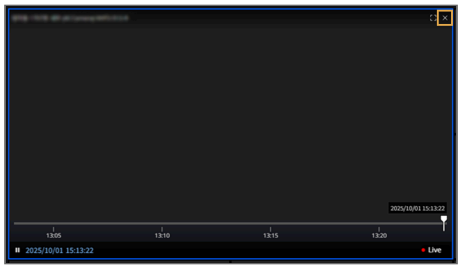
전체 화면 보기



비디오 타일에 배치된 영상을 전체 화면으로 보려면 영상의 오른쪽 상단에 있는 ⛶ 버튼을 클릭하세요.

전체 화면을 종료하려면 화면 오른쪽 상단에 ⛶ 버튼을 클릭하세요. 또는 키보드의 키를 누르세요.

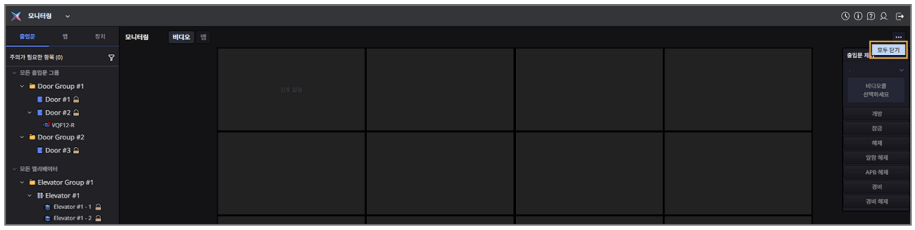
영상 닫기



비디오 타일에 배치된 영상을 닫으려면 영상의 오른쪽 상단에 있는 ✕ 버튼을 클릭하세요.

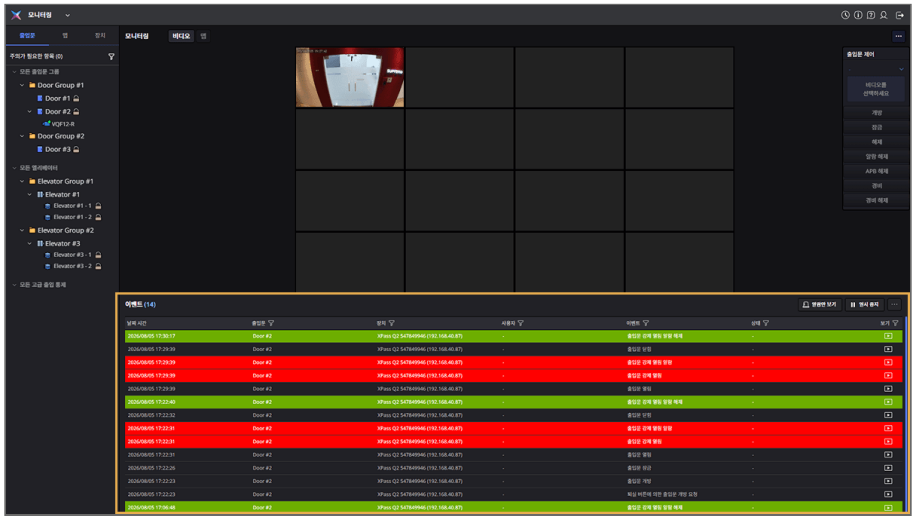
모든 영상 닫기

비디오 타일에 배치한 모든 영상을 닫으려면 화면 오른쪽 상단에 ••• 버튼을 클릭하세요. 팝업 메뉴에서 **모두 닫기**를 클릭하세요.



이벤트 모니터링하기

모니터링 페이지에서 화면 하단의 **이벤트** 섹션에서는 실시간으로 발생하는 이벤트를 확인하고 관리할 수 있습니다. 이벤트의 상태, 알람 이벤트 처리, 필터링, 색상 구분 등 다양한 기능을 통해 효율적으로 이벤트를 관리할 수 있습니다. 특히, 출입문, 장치, 사용자와 연관된 이벤트를 실시간으로 모니터링하고 필요한 조치를 빠르게 수행할 수 있습니다.



이벤트 목록 확인하기

이벤트 섹션에서는 발생한 이벤트를 실시간으로 확인할 수 있습니다. 이벤트는 아래 정보를 포함합니다.



- **날짜 시간**: 이벤트가 발생한 날짜와 시각입니다.
- **출입문**: 이벤트가 발생한 출입문입니다.
- **장치**: 이벤트가 발생한 장치입니다.
- **사용자**: 이벤트를 발생시킨 사용자입니다.
- **이벤트**: 이벤트 상세 내용입니다.
- **상태**: 이벤트 상태입니다. 활성화된 이벤트의 경우 **활성** 상태로 표시됩니다. 알람 이벤트에는 **확인** 버튼이 표시됩니다. **확인** 버튼을

클릭하면 해당 이벤트는 해소됩니다.

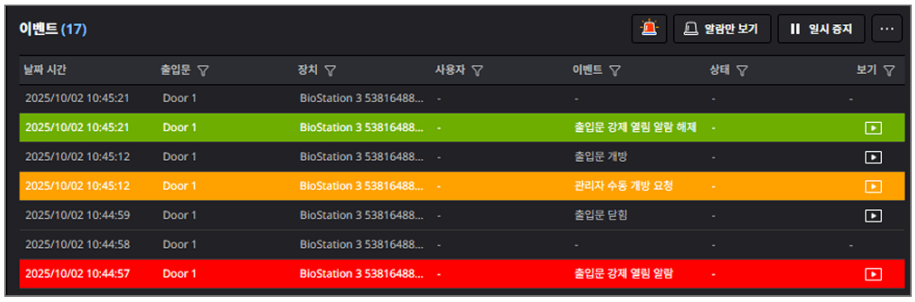


- **보기**: 이벤트에 출입문과 연결된 카메라의 영상 정보를 포함하고 있다면 비디오 아이콘(▶)이 표시됩니다. 아이콘을 클릭하면 영상을 확인할 수 있습니다.

> **알아두기**
>
> - 개별 이벤트를 클릭하면 화면 오른쪽에 상세 정보가 나타납니다. 상세 정보에는 이벤트 발생 시각과 구역, 출입문, 장치, 사용자 그룹, 사용자, 포트, 이벤트 상세 내용이 포함됩니다.
> - 이벤트에 출입문과 연결된 카메라의 영상 또는 이미지 정보를 포함하고 있다면 비디오 및 이미지 로그를 같이 확인할 수 있습니다.

색상에 따른 이벤트 구분

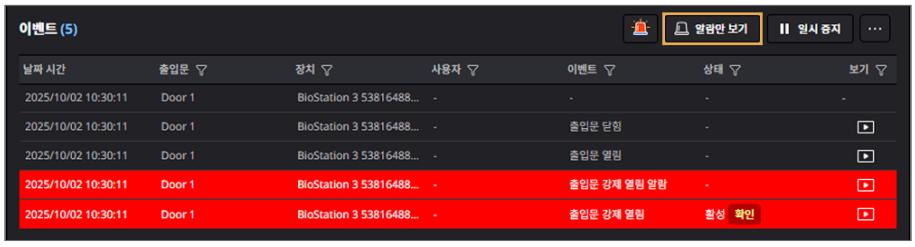
이벤트 목록에서 발생한 이벤트는 색상으로 구분할 수 있습니다.



- **색상 없음**: 일반 이벤트입니다.
- 주황색: 주의 이벤트입니다. 출입이 허용되지 않은 구역에 사용자가 출입을 시도했거나, 출입문이 열려 있는 경우와 같이 주의가 필요한 이벤트입니다.
- 빨간색: 알람 이벤트입니다. 시스템에서 발생한 이벤트 중 조치가 필요한 경고 이벤트입니다.
- 녹색: 해소된 알람 이벤트입니다.

알람 이벤트 확인

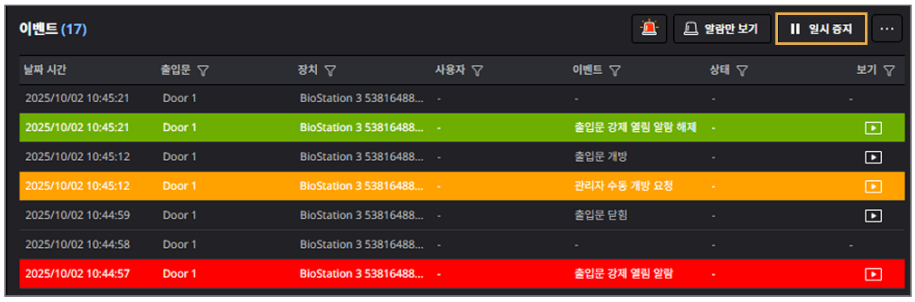
이벤트 섹션 목록에서 알람 이벤트만 확인할 수 있습니다. **이벤트** 섹션 상단 오른쪽에 **알람만 보기** 버튼을 클릭하세요. 이벤트 목록에 알람 이벤트만 표시됩니다. 알람 이벤트는 빨간색으로 표시됩니다.



> **알아두기**
>
> 알람 이벤트를 포함한 모든 이벤트를 확인하려면 **이벤트** 섹션 상단 오른쪽에 **모든 이벤트** 버튼을 클릭하세요.

실시간 이벤트

이벤트 섹션의 이벤트 목록에서는 실시간으로 발생하는 이벤트를 확인할 수 있습니다. 실시간 이벤트를 중지하고 싶다면 **이벤트** 섹션 상단 오른쪽에 ⏸ **일시 중지** 버튼을 클릭하세요. ▶ **시작** 버튼을 클릭하면 실시간 이벤트를 재개합니다.

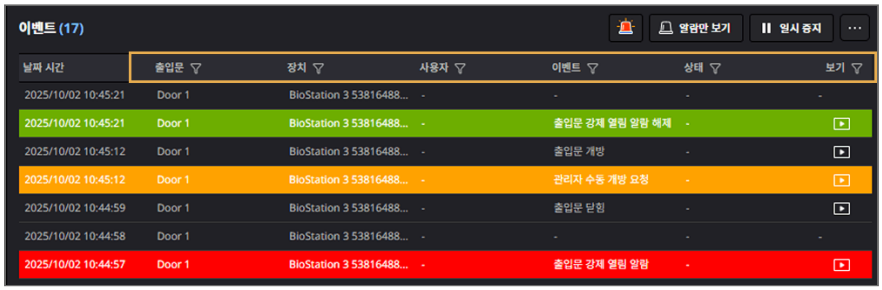


이벤트 필터링

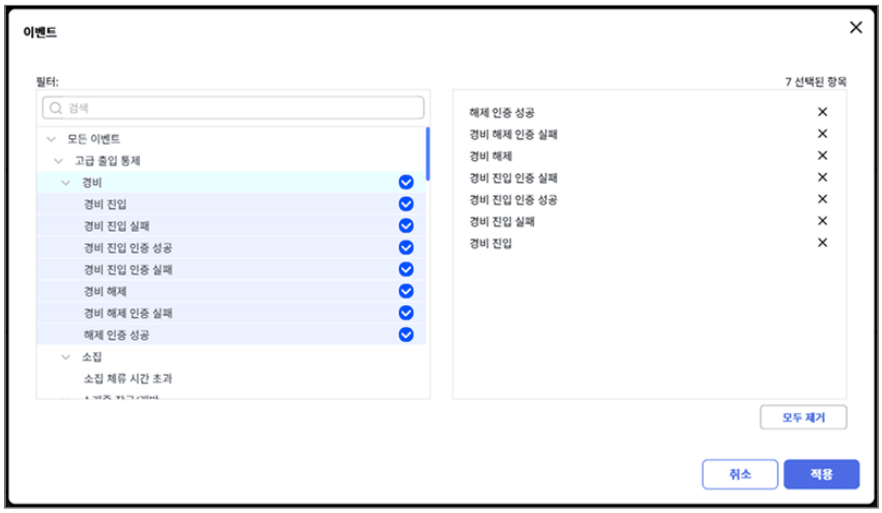
필터 적용

사용자가 원하는 조건으로 이벤트 목록을 필터링할 수 있습니다. 이를 통해 원하는 조건의 이벤트를 빠르게 확인할 수 있습니다.

1. **이벤트** 섹션 목록의 각 헤더 컬럼에 ▽ 아이콘을 클릭하세요.



2. 필터 창이 나타나면 왼쪽 목록에서 원하는 항목을 클릭하세요.



   - 상위 항목을 선택하면 하위 항목 모두를 선택할 수 있습니다.
   - 선택한 항목을 해제하려면 ✕ 버튼을 클릭하세요. 모든 항목을 해제하려면 **모두 제거** 버튼을 클릭하세요.

3. 모든 설정을 완료했다면 **적용** 버튼을 클릭하세요.

이벤트 목록에 설정한 조건의 이벤트만 표시됩니다.

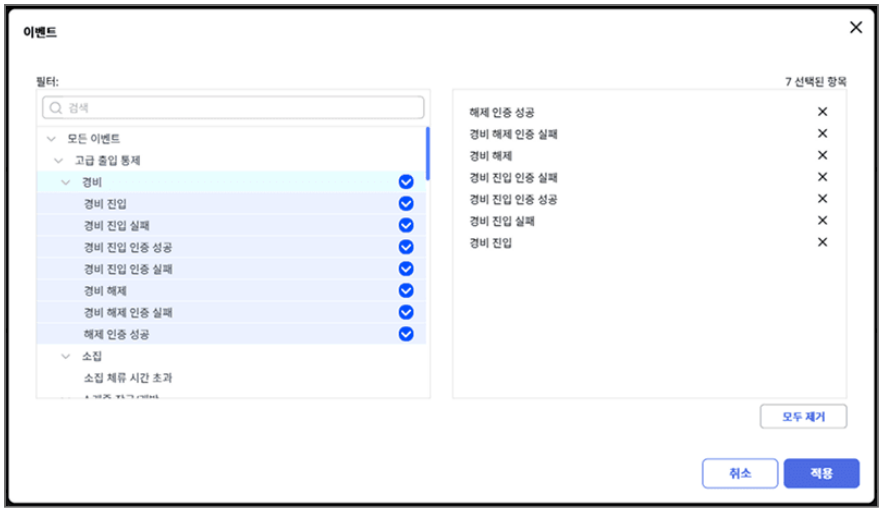
알아두기

- 필터 창의 검색 입력 필드를 통해서 원하는 항목을 빠르게 검색할 수도 있습니다.
- 각 헤더 컬럼별로 원하는 조건을 여러 개 설정할 수 있습니다. 한 개 이상의 조건을 설정하면 AND 조건을 적용합니다.
- 각 헤더 컬럼별로 필터링할 수 있는 항목은 다를 수 있습니다.
- 필터링 조건을 설정하면 헤더 컬럼의 ▼ 아이콘 색상이 변경됩니다.

필터링 해제

적용한 필터 조건을 해제할 수 있습니다.

1. **이벤트** 섹션 목록의 필터를 적용한 헤더 컬럼에 ▼ 아이콘을 클릭하세요.
2. 필터 창이 나타나면 오른쪽 목록에서 해제할 항목의 오른쪽에 ✕ 버튼을 클릭하세요. 모든 필터를 해제하려면 **모두 제거** 버튼을 클릭하세요.



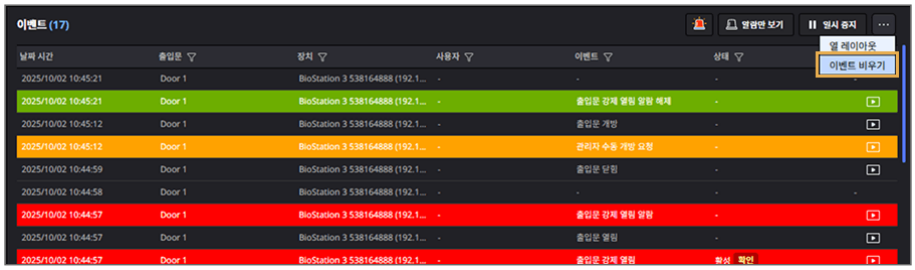
3. 해제할 조건을 모두 설정했다면 **적용** 버튼을 클릭하세요.

알아두기

- 필터 창의 검색 입력 필드를 통해서 원하는 항목을 빠르게 검색할 수도 있습니다.
- 필터링 조건이 해제되면 헤더 컬럼의 아이콘 색상이 원래대로 전환됩니다.

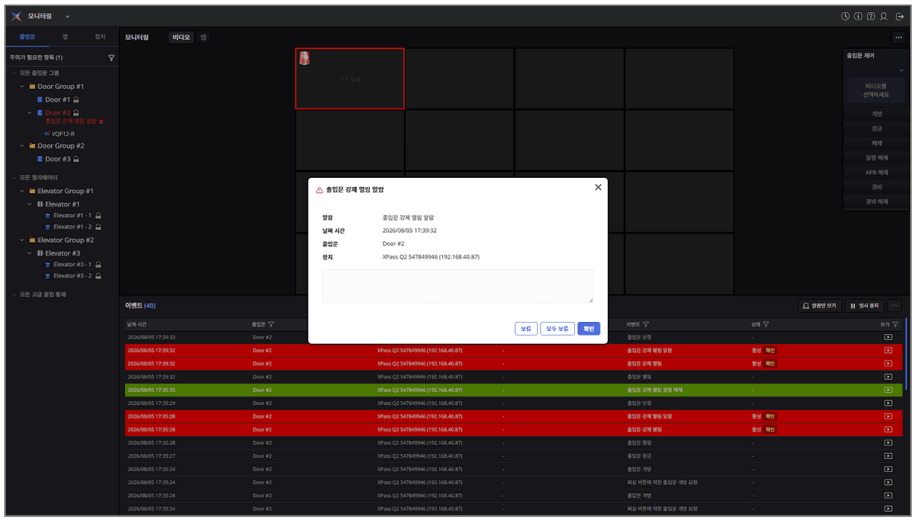
이벤트 목록 비우기

이벤트 섹션 목록에서 이벤트를 지울 수 있습니다. **이벤트** 섹션 오른쪽 상단에 ••• 버튼을 클릭하고 팝업 메뉴에서 **이벤트 비우기**를 선택하세요. 이벤트 목록에 불필요한 이벤트가 많이 쌓여 있다면 **이벤트 비우기** 기능을 사용해 정리할 수 있습니다.



알람 확인 및 조치 사항 기록

출입문 강제 열림과 같은 알람 이벤트가 발생하면 알람 메시지 창이 표시됩니다. 알람 메시지 창에는 발생한 알람 이벤트의 상세 내용이 포함됩니다. 이때 관리자는 발생한 알람 이벤트에 대한 인지 여부와 조치 내용을 기록할 수 있습니다.



알아두기

모두 보류 버튼은 알람 이벤트가 2개 이상 발생했을 때만 표시됩니다.

알람 이벤트에 대한 조치 사항 기록

메시지 입력 필드에 알람 이벤트에 대한 조치 사항을 입력하세요. 최대 500자까지 입력할 수 있습니다. 조치 사항을 입력하고 **확인** 버튼을 클릭하세요. 알람 이벤트에 대한 인지 여부와 조치 사항이 기록됩니다. 알람 메시지 창은 닫힙니다.



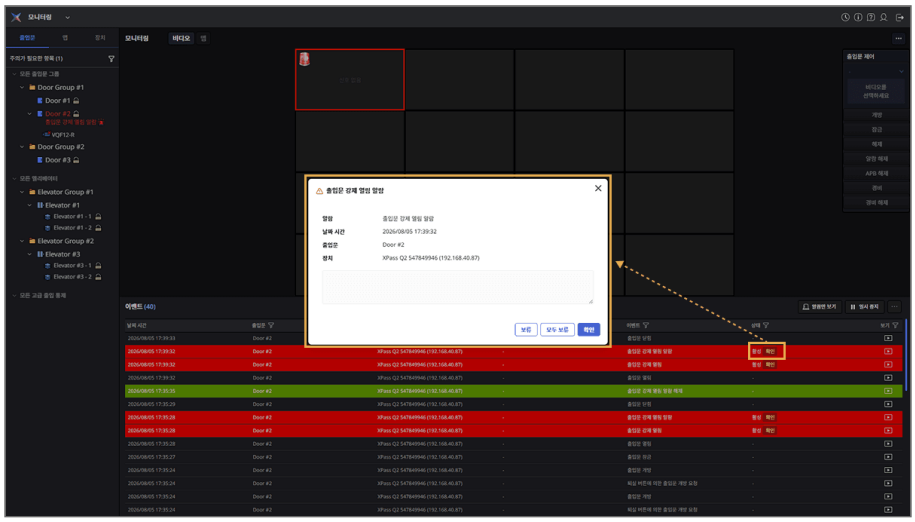
알람 이벤트 인지 여부 보류

보류 버튼을 클릭해 알람 이벤트에 대한 인지 여부를 보류할 수도 있습니다. 조치 사항은 기록할 수 있습니다. 알람 메시지 창은 닫힙니다. 보류한 알람 이벤트는 이벤트 목록에서 **활성** 상태로 표시되고, **확인** 버튼을 사용할 수 있습니다.



이벤트 목록에서 알람 이벤트 확인

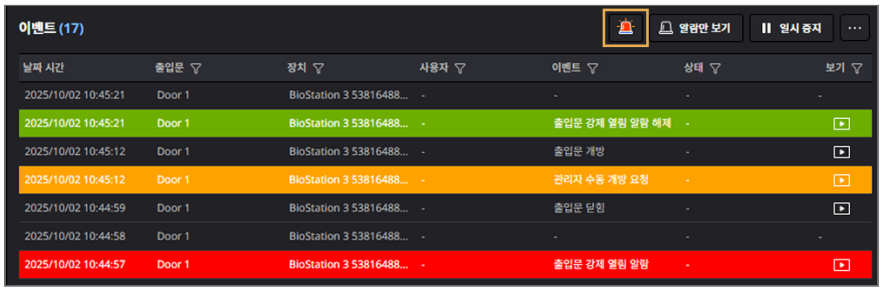
이벤트 목록의 **상태** 컬럼에 표시된 **확인** 버튼을 클릭하면 발생한 알람 이벤트에 대한 인지 여부와 조치 내용을 기록할 수 있습니다. 입력을 완료하고 **확인** 버튼을 클릭하세요.



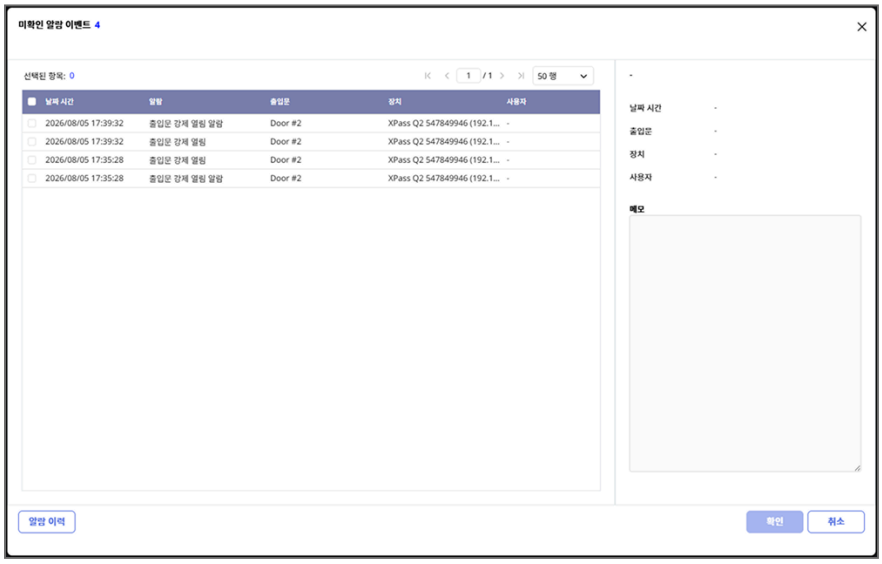
확인하지 않은 알람 이벤트 보기

아직 확인하지 않은 알람 이벤트를 한 번에 확인하고 조치 사항을 기록할 수 있는 기능을 제공합니다. 동일한 알람 이벤트가 여러 개 발생했을 때 유용하게 이용할 수 있습니다.

1. **이벤트** 섹션 오른쪽 상단의  버튼을 클릭하세요.



2. **미확인 알람 이벤트** 창이 나타나면 왼쪽 목록에서 조치 사항을 기록할 알람 이벤트를 선택하세요. 모든 이벤트를 선택하려면 헤더 컬럼 가장 왼쪽의 체크박스를 클릭하세요.



3. **메모** 입력 필드에 알람 이벤트에 대한 조치 사항을 입력하세요.
4. **확인** 버튼을 클릭하세요.

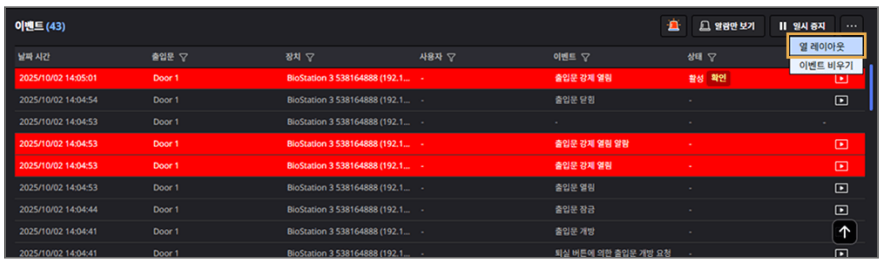
선택한 이벤트에 대한 조치 사항을 기록합니다. 알람 이벤트 팝업 창은 닫힙니다.

> **알아두기**
> 알람 이벤트 목록에서 한 개 이상의 이벤트를 선택해야 **확인** 버튼이 활성화됩니다.

이벤트 목록 열 설정

이벤트 목록에서 표시할 열을 추가하거나 순서 변경, 숨김 설정을 할 수 있습니다.

1. **이벤트** 섹션의 오른쪽 상단에서 ••• → **열 레이아웃**을 클릭하세요.



2. **열 레이아웃** 창이 나타나면 표시할 열의 체크박스를 클릭해 추가하거나 숨김 설정을 할 수 있습니다. 드래그 앤 드롭으로 열의 순서를 변경할 수도 있습니다.



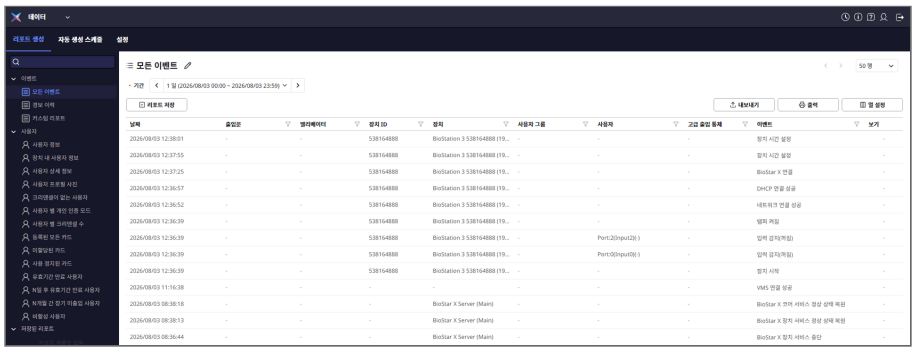
3. 열 설정을 모두 변경했으면 **적용** 버튼을 클릭하세요.

> **알아두기**
> 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

데이터

데이터 메뉴를 사용하면 **BioStar X**에 등록된 사용자 정보나 원하는 조건의 이벤트를 조회할 수 있고, 보고서를 일정 주기에 맞춰 생성할 수 있습니다. 필요시 원하는 리포트를 일정 주기로 자동 생성할 수 있으며 생성된 리포트는 CSV, PDF 파일로 내보내거나 인쇄할 수 있습니다.

런처 페이지에서 **데이터**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **데이터**를 선택하세요.



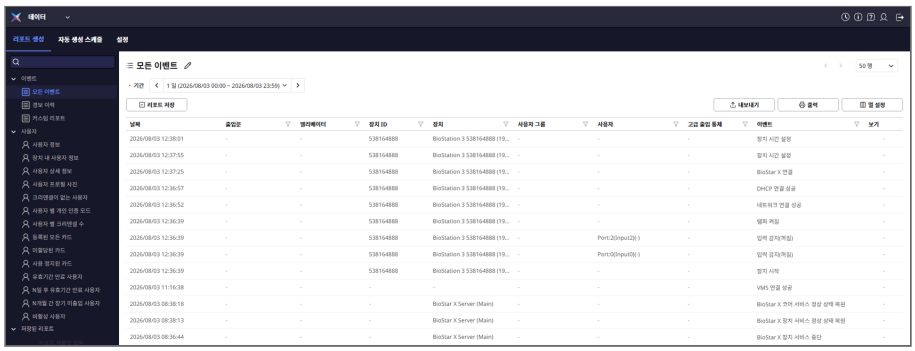
리포트 생성하기

BioStar X에서 발생한 모든 이벤트를 조회하거나 경보 이력만 조회할 수 있습니다. 사용자가 원하는 조건에 맞게 필터링하여 커스텀 리포트를 생성할 수도 있습니다.

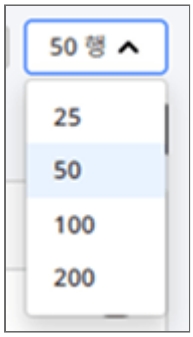
런처 페이지에서 **데이터**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **데이터**를 선택하세요.

모든 이벤트 조회

BioStar X에서 발생한 모든 이벤트를 조회할 수 있습니다. 화면 왼쪽 사이드바에서 **이벤트** → **모든 이벤트**를 클릭하세요.

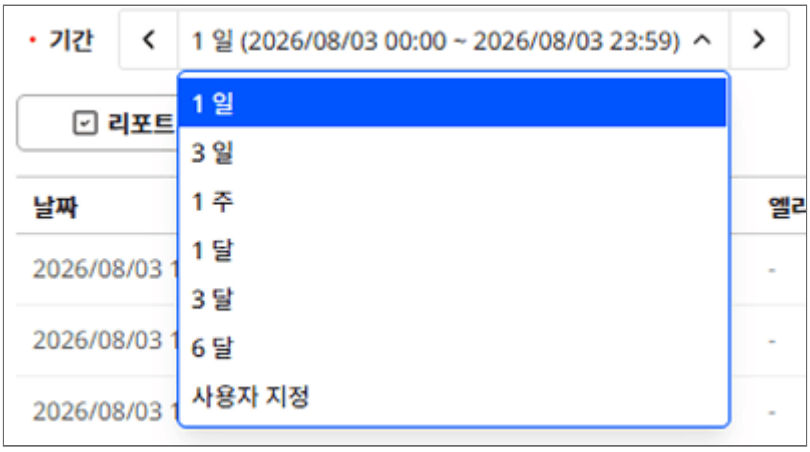


- 조회된 목록에서 이전 또는 다음 페이지를 확인하려면 화면 오른쪽 상단의 ‹ 또는 › 버튼을 클릭하세요.
- 목록에 표시할 행의 수를 변경하려면 화면 오른쪽 상단의 드랍다운 메뉴를 클릭하고 원하는 값을 선택하세요. 최소 25행부터 최대 200행까지 선택할 수 있습니다.

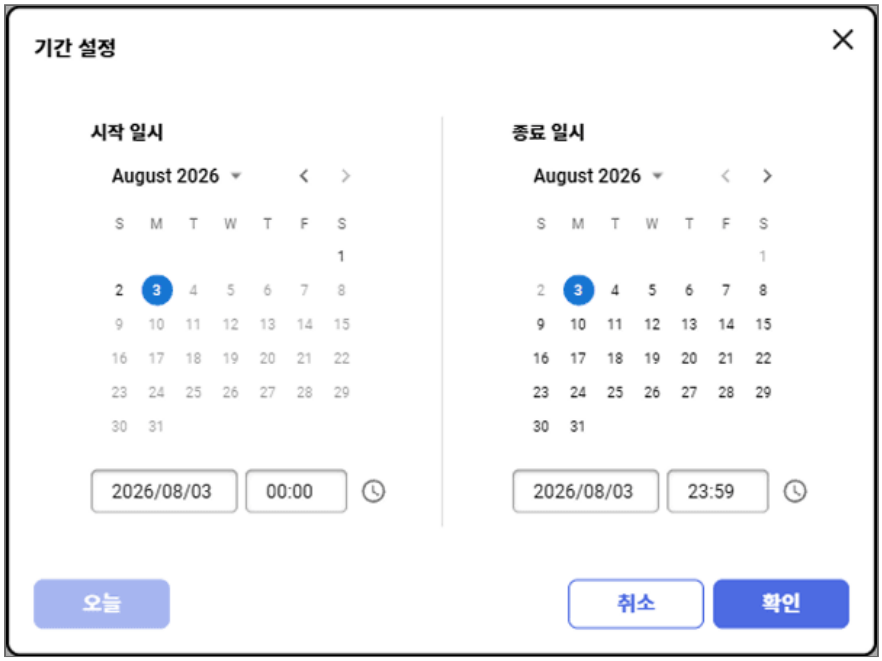


기간 설정

화면 왼쪽 상단의 **기간** 항목에서 원하는 기간을 설정할 수 있습니다. 날짜 영역을 클릭하세요.



- 오늘 날짜를 기준으로 1일부터 6달까지 사전 정의된 기간을 선택할 수 있습니다. 원하는 기간을 선택하면 해당 기간에 발생한 이벤트가 목록에 자동 표시됩니다.
- **사용자 정의**을 선택하면 원하는 기간을 직접 설정할 수도 있습니다. 기간 선택 창이 나타나면 시작 날짜와 종료 날짜, 시간을 설정하고 **확인** 버튼을 클릭하세요. 설정한 기간에 발생한 이벤트가 목록에 자동 표시됩니다.



> **알아두기**
> 오늘 날짜를 선택하려면 **오늘** 버튼을 클릭하세요.

조회 조건 설정

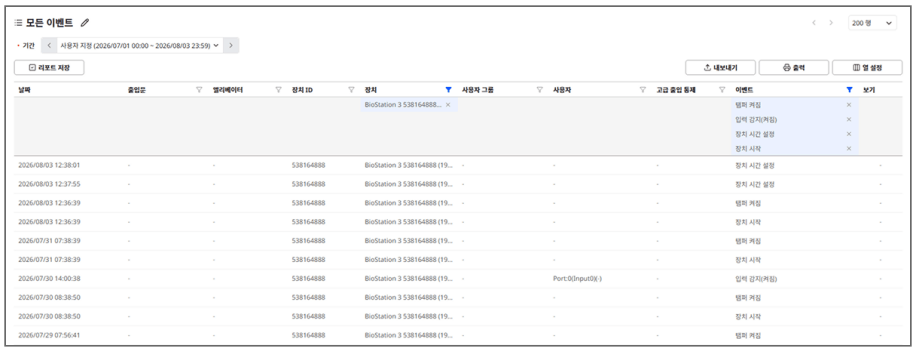
조회 목록의 헤더 부분에서 원하는 조건을 설정하여 목록을 필터링할 수 있습니다. 날짜를 제외한 모든 항목에 조건을 설정할 수 있습니다.

1. 이벤트 목록의 헤더 부분에서 원하는 컬럼의 ▽ 버튼을 클릭하세요.
2. 필터 조건 창이 나타나면 원하는 항목을 선택하세요.



3. 선택을 완료했으면 **필터 조건 추가** 버튼을 클릭하세요.

선택한 조건에 맞는 이벤트만 목록에 표시됩니다.



조회 조건 해제

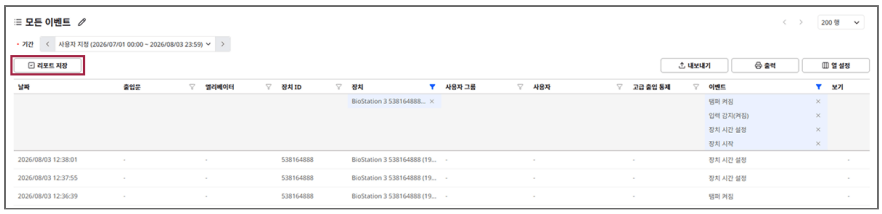
설정한 조회 조건을 해제하려면 헤더 부분 아래에 설정된 조건에서 ✕ 버튼을 클릭하세요. 설정한 조건이 해제되고 모든 이벤트가 목록에 다시 표시됩니다.



리포트 저장

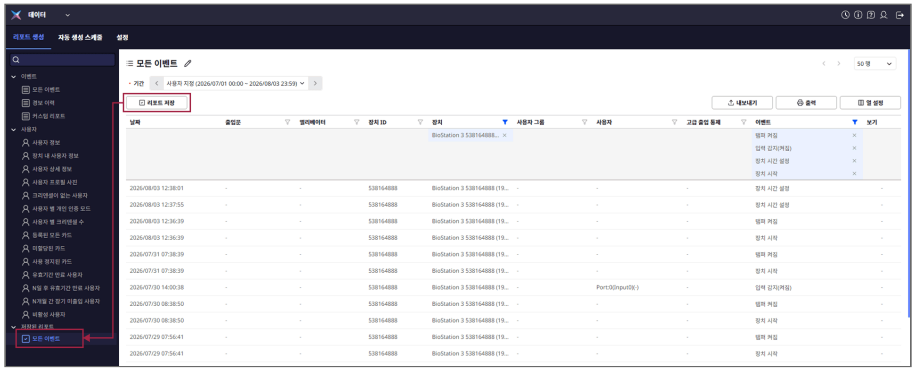
사용자가 설정한 조회 기간 및 조건으로 이벤트를 리포트로 저장할 수 있습니다.

1. 이벤트 목록 왼쪽 상단의 **리포트 저장** 버튼을 클릭하세요.



2. 리포트 템플릿 저장 성공 메시지가 나타나면 **확인** 버튼을 클릭하세요.

3. 화면 왼쪽 사이드바의 **저장된 리포트** 하위에 저장한 리포트가 표시됩니다.



저장한 리포트는 템플릿으로 저장되며, 추후 동일한 조건으로 리포트를 생성할 때 유용하게 사용할 수 있습니다.

알아두기

- 저장한 리포트의 제목, 이벤트 항목, 기간, 필터 조건을 수정하려면, 리포트 상단 영역에서 ✎ 버튼을 클릭하세요.
- 리포트 제목은 화면 왼쪽 사이드바의 **저장된 리포트** 하위에서도 변경할 수 있습니다. 제목을 변경할 커스텀 리포트를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **리포트 템플릿 이름 변경**을 선택하세요.



- 리포트 관리에 대한 자세한 내용은 리포트 관리를 참고하세요.

이벤트 영상 확인하기

이벤트 목록에서 특정 이벤트가 발생한 장치에 카메라가 연결되어 있다면 해당 이벤트의 **보기** 컬럼에 ▶ 아이콘이 표시됩니다. 아이콘을 클릭하면 팝업창을 통해 해당 이벤트가 발생한 시점의 영상을 확인할 수 있습니다.



알아두기

- 카메라 규칙 설정에서 한 개 이상의 카메라를 연결했다면 첫 번째 카메라의 영상을 재생합니다. 카메라 규칙 설정에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.
- 출입문과 카메라 연동에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.
- 이 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

CSV 내보내기

조회된 이벤트 목록을 CSV 파일로 내보낼 수 있습니다.

1. 화면 오른쪽 상단의 **내보내기** 버튼을 클릭하세요.
2. **리포트 내보내기** 창이 나타나면 **파일 포맷**에서 **CSV**를 선택하세요.



3. **파일 이름**에서 저장할 파일 이름을 수정할 수 있습니다.
4. **내보내기 사유**(선택 사항)를 입력하고 **내보내기** 버튼을 클릭하세요.
5. 로컬의 원하는 경로에 CSV 파일을 저장하세요.

알아두기

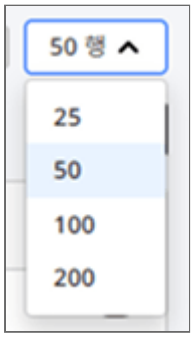
내보내기 사유는 필수 입력 항목이 아닙니다. 내보내기 사유는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

경보 이력 조회

경보(알람) 이력만 조회할 수 있습니다. 화면 왼쪽 사이드바에서 **이벤트** → **경보 이력**을 클릭하세요.



- 조회된 목록에서 이전 또는 다음 페이지를 확인하려면 화면 오른쪽 상단의 < 또는 > 버튼을 클릭하세요.
- 조회된 목록에서 첫 페이지 또는 마지막 페이지로 이동하려면 화면 오른쪽 상단의 |< 또는 >| 버튼을 클릭하세요.
- 목록에 표시할 행의 수를 변경하려면 화면 오른쪽 상단의 드랍다운 메뉴를 클릭하고 원하는 값을 선택하세요. 최소 25행부터 최대 200행까지 선택할 수 있습니다.

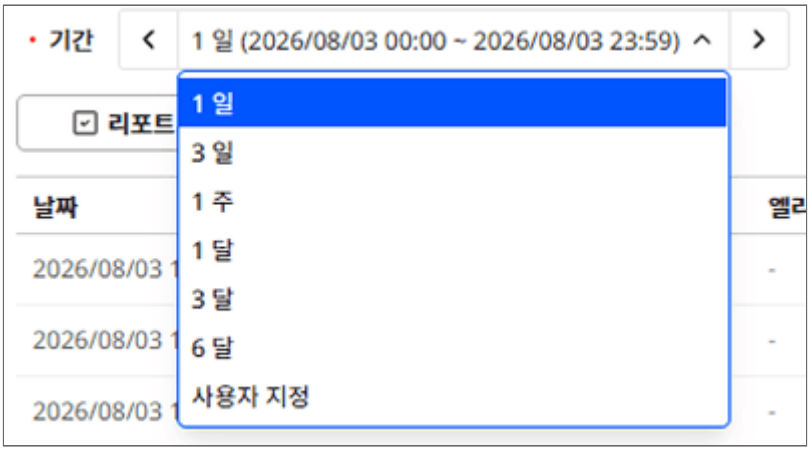


알아두기

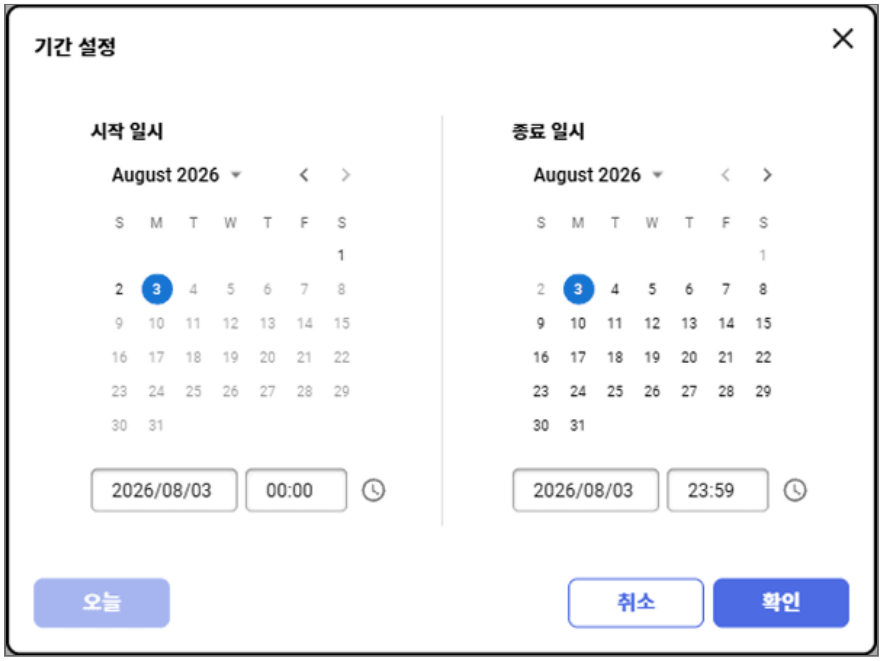
이벤트 모니터링에서 경보(알람) 이벤트 확인에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

기간 설정

화면 왼쪽 상단의 **기간** 항목에서 원하는 기간을 설정할 수 있습니다. 날짜 영역을 클릭하세요.



- 오늘 날짜를 기준으로 1일부터 6달까지 사전 정의된 기간을 선택할 수 있습니다. 원하는 기간을 선택하면 해당 기간에 발생한 이벤트가 목록에 자동 표시됩니다.
- **사용자 정의**을 선택하면 원하는 기간을 직접 설정할 수도 있습니다. 기간 선택 창이 나타나면 시작 날짜와 종료 날짜, 시간을 설정하고 **확인** 버튼을 클릭하세요. 설정한 기간에 발생한 이벤트가 목록에 자동 표시됩니다.



> **알아두기**
> 오늘 날짜를 선택하려면 **오늘** 버튼을 클릭하세요.

조회 조건 설정

조회 목록의 헤더 부분에서 원하는 조건을 설정하여 목록을 필터링할 수 있습니다. 날짜를 제외한 모든 항목에 조건을 설정할 수 있습니다.

1. 이벤트 목록의 헤더 부분에서 원하는 컬럼의 ▽ 버튼을 클릭하세요.
2. 필터 조건 창이 나타나면 원하는 항목을 선택하세요.



3. 선택을 완료했으면 **필터 조건 추가** 버튼을 클릭하세요.

선택한 조건에 맞는 이벤트만 목록에 표시됩니다.



조회 조건 해제

설정한 조회 조건을 해제하려면 헤더 부분 아래에 설정된 조건에서 ✕ 버튼을 클릭하세요. 설정한 조건이 해제되고 모든 이벤트가 목록에 다시 표시됩니다.



리포트 저장

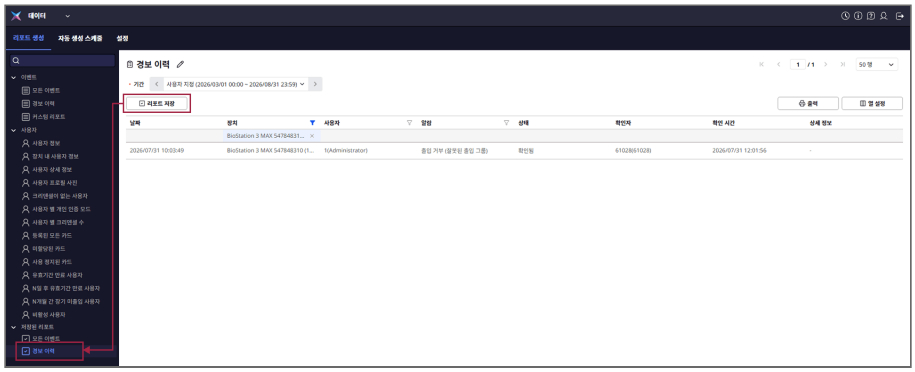
사용자가 설정한 조회 기간 및 조건으로 경보 이력을 리포트로 저장할 수 있습니다.

1. 경보 이력 목록 왼쪽 상단의 **리포트 저장** 버튼을 클릭하세요.



2. 리포트 템플릿 저장 성공 메시지가 나타나면 **확인** 버튼을 클릭하세요.

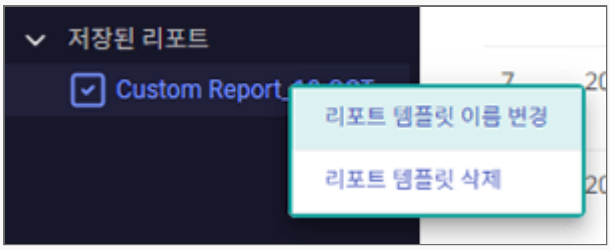
3. 화면 왼쪽 사이드바의 **저장된 리포트** 하위에 저장한 리포트가 표시됩니다.



저장한 리포트는 템플릿으로 저장되며, 추후 동일한 조건으로 리포트를 생성할 때 유용하게 사용할 수 있습니다.

알아두기

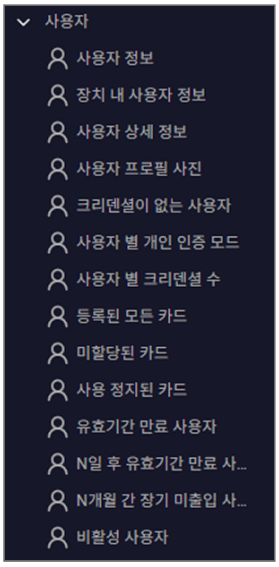
- 저장한 리포트의 제목, 이벤트 항목, 기간, 필터 조건을 수정하려면, 리포트 상단 영역에서 ✎ 버튼을 클릭하세요.
- 리포트 제목은 화면 왼쪽 사이드바의 **저장된 리포트** 하위에서도 변경할 수 있습니다. 제목을 변경할 커스텀 리포트를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **리포트 템플릿 이름 변경**을 선택하세요.



- 리포트 관리에 대한 자세한 내용은 리포트 관리를 참고하세요.

사용자 리포트 조회

사용자 관련 템플릿을 선택하여 리포트를 생성할 수 있습니다. 화면 왼쪽 사이드바에서 **사용자** 하위에서 원하는 템플릿을 클릭하세요.



- **사용자 정보**: 사용자 상세 정보를 목록 형식으로 조회할 수 있습니다.
- **장치 내 사용자 정보**: 장치에 등록된 사용자의 정보를 조회할 수 있습니다.
- **사용자 상세 정보**: 사용자 상세 정보를 카드 형식으로 조회할 수 있습니다.
- **사용자 프로필 사진**: 사용자 프로필 사진을 갤러리 형식으로 조회할 수 있습니다.
- **크리덴셜이 없는 사용자**: 크리덴셜을 설정하지 않은 사용자를 조회할 수 있습니다.
- **사용자 별 개인 인증 모드**: 사용자의 개인 인증 모드 설정 정보를 조회할 수 있습니다.
- **사용자 별 크리덴셜 수**: 사용자에게 설정된 크리덴셜 개수를 조회할 수 있습니다.
- **등록된 모든 카드**: 등록된 카드를 기준으로 사용자를 조회할 수 있습니다.
- **미할당된 카드**: 사용자에게 할당되지 않은 카드를 조회할 수 있습니다.
- **사용 정지된 카드**: 사용 정지된 카드를 조회할 수 있습니다.
- **유효기간 만료 사용자**: 유효 기간이 만료된 사용자를 조회할 수 있습니다.
- **N일 후 유효기간 만료 사용자**: N일 이내에 유효 기간이 만료되는 사용자를 조회할 수 있습니다. 일 수는 리포트를 생성하기 전에 직접 입력할 수 있습니다.
- **N개월 간 장기 미출입 사용자**: 최근 N개월 동안 출입 기록이 없는 사용자를 조회할 수 있습니다. 개월 수는 리포트를 생성하기 전에 직접 입력할 수 있습니다.
- **비활성 사용자**: 비활성화된 사용자를 조회할 수 있습니다.

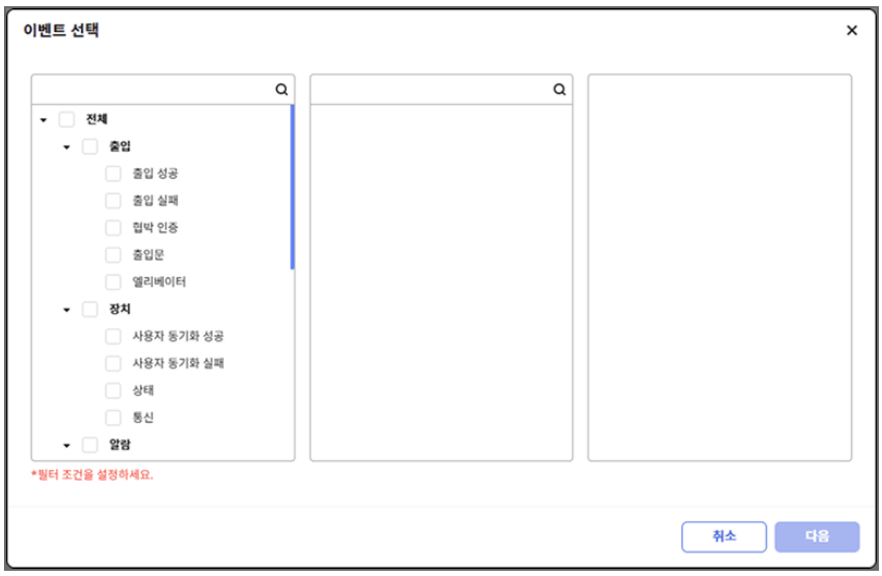
알아두기

- 생성한 리포트는 **저장된 리포트** 하위에 저장할 수 있습니다. 리포트 왼쪽 상단의 **리포트 저장** 버튼을 클릭하세요.
- 리포트 관리에 대한 자세한 내용은 리포트 관리를 참고하세요.

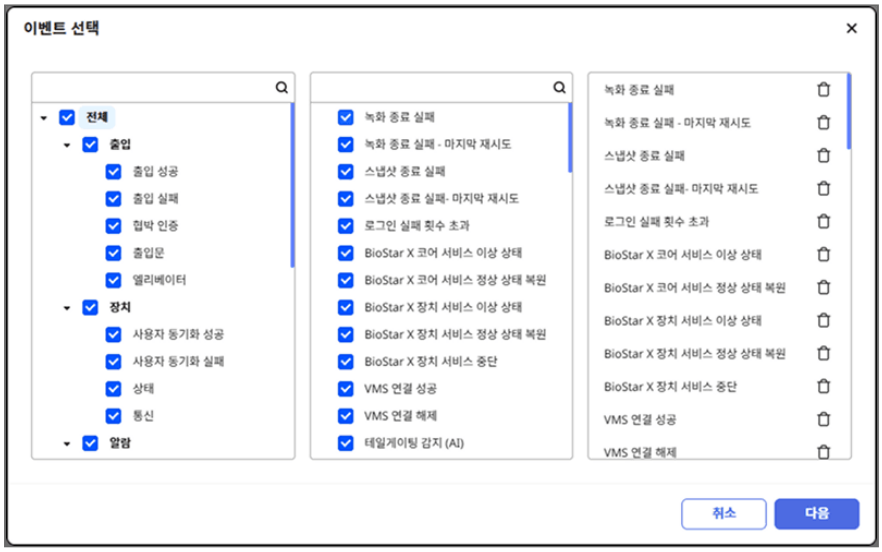
커스텀 리포트 생성

원하는 조건에 맞게 필터링하여 커스텀 리포트를 생성할 수 있습니다. 생성한 리포트는 템플릿으로 저장하여 추후 동일한 조건으로 리포트를 생성할 때 유용하게 사용할 수 있습니다.

1. 화면 왼쪽 사이드바에서 **이벤트** → **커스텀 리포트**를 클릭하세요.
2. **이벤트 선택** 창에서 원하는 이벤트를 선택하세요.

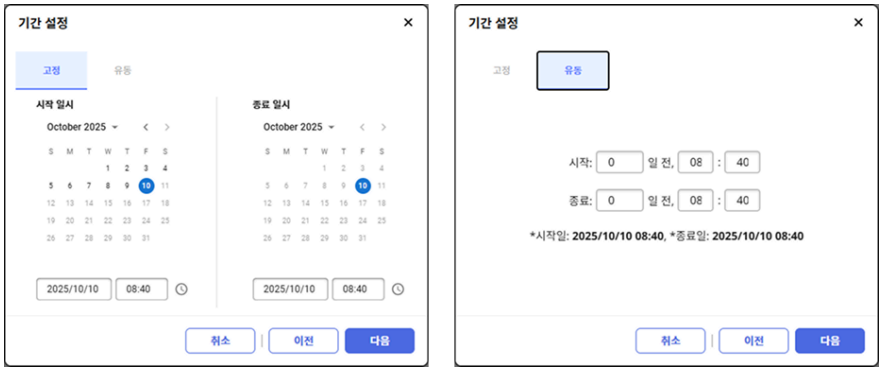


3. 원하는 이벤트 선택을 완료하면 **다음** 버튼을 클릭하세요.



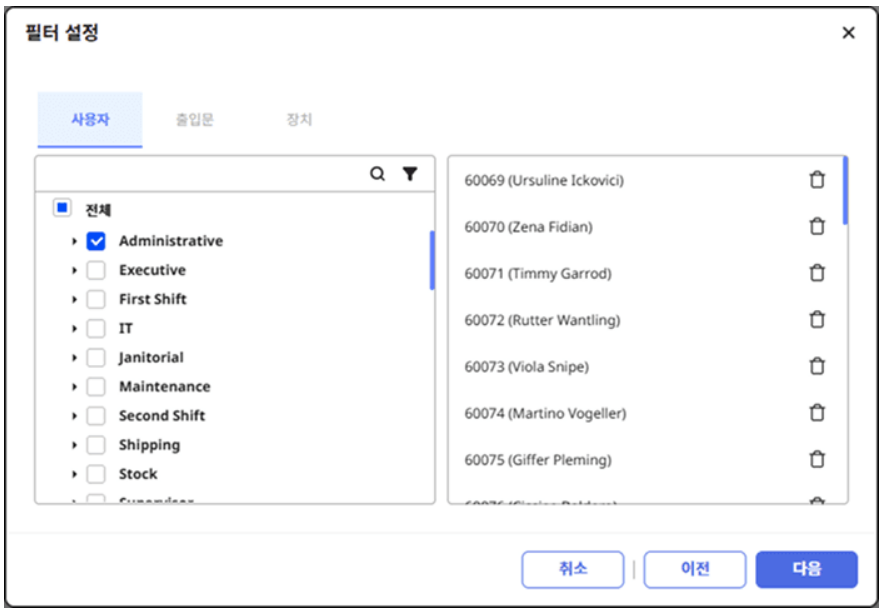
- 검색(Q) 입력 필드에서 원하는 항목을 검색할 수 있습니다.
- 가장 오른쪽 목록에서 🗑 버튼을 클릭하면 선택한 항목을 제외할 수 있습니다.

4. 조회 기간을 설정하고 **다음** 버튼을 클릭하세요.



- **고정**: 특정 날짜와 시간을 설정해 조회 기간을 설정할 수 있습니다.
- **유동**: 오늘 날짜를 기준으로 시작일, 종료일, 시간을 설정할 수 있습니다. 반복적으로 일정 기간의 리포트를 생성할 때 유용합니다.

5. 사용자, 출입문, 장치를 기준으로 그룹별, 개별적으로 조건을 설정할 수 있습니다.



- 오른쪽 목록에서 🗑 버튼을 클릭하면 선택한 항목을 제외할 수 있습니다.

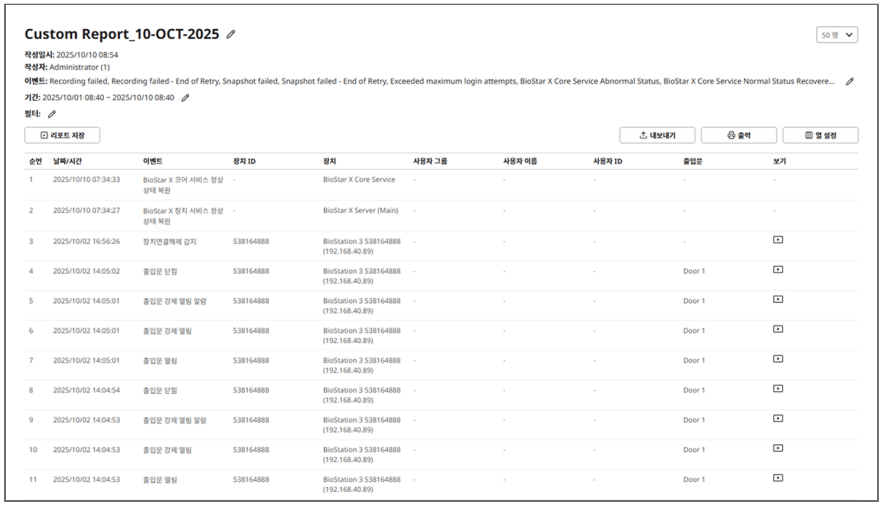
6. 원하는 조건을 선택하고 **다음** 버튼을 클릭하세요.

7. 열 설정 창에서 리포트에 표시할 컬럼을 선택하세요.

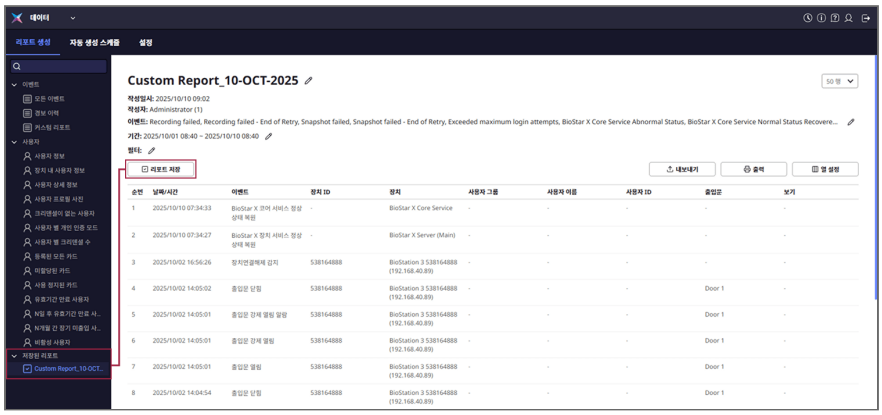


8. 원하는 컬럼 선택을 완료하면 **생성** 버튼을 클릭하세요.

9. 설정한 조건으로 리포트를 생성합니다.



10. 생성한 리포트를 템플릿으로 저장하려면 목록 왼쪽 상단의 **리포트 저장** 버튼을 클릭하세요. 저장한 리포트는 화면 왼쪽 사이드바의 **저장된 리포트** 하위에서 확인할 수 있습니다.



저장한 리포트는 템플릿으로 저장되며, 추후 동일한 조건으로 리포트를 생성할 때 유용하게 사용할 수 있습니다.

알아두기

- 저장한 리포트의 제목, 이벤트 항목, 기간, 필터 조건을 수정하려면, 리포트 상단 영역에서 ✎ 버튼을 클릭하세요.
- 리포트 제목은 화면 왼쪽 사이드바의 **저장된 리포트** 하위에서도 변경할 수 있습니다. 제목을 변경할 커스텀 리포트를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **리포트 템플릿 이름 변경**을 선택하세요.

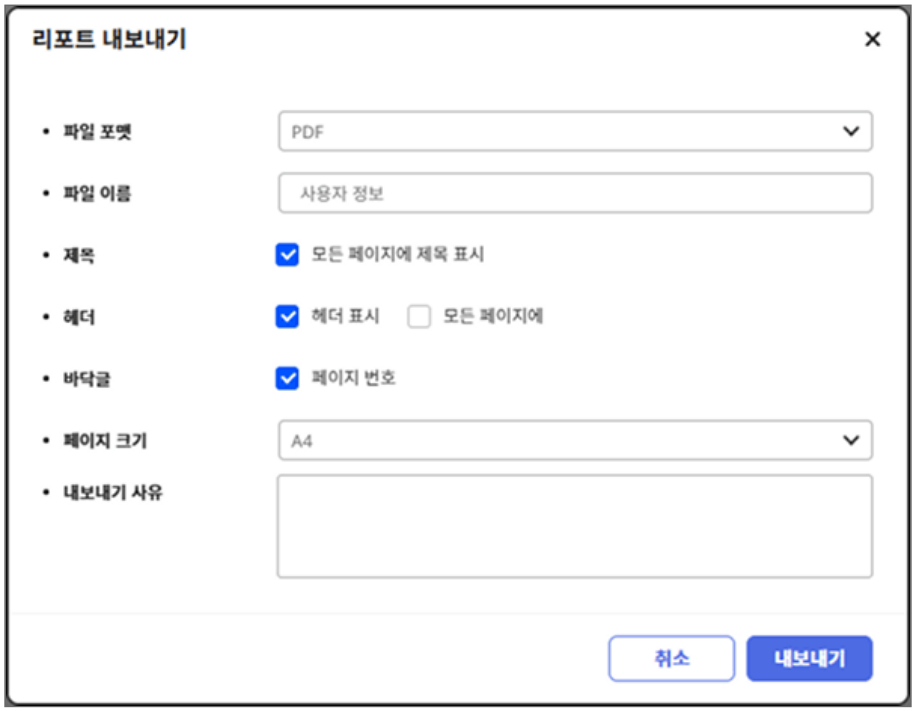


- 리포트 관리에 대한 자세한 내용은 리포트 관리를 참고하세요.

리포트 관리

리포트 파일 저장

리포트를 PDF 또는 CSV 파일로 내보내려면 **내보내기** 버튼을 클릭하세요. **리포트 내보내기** 창이 나타나면 각 항목을 설정하고 **내보내기** 버튼을 클릭하세요.

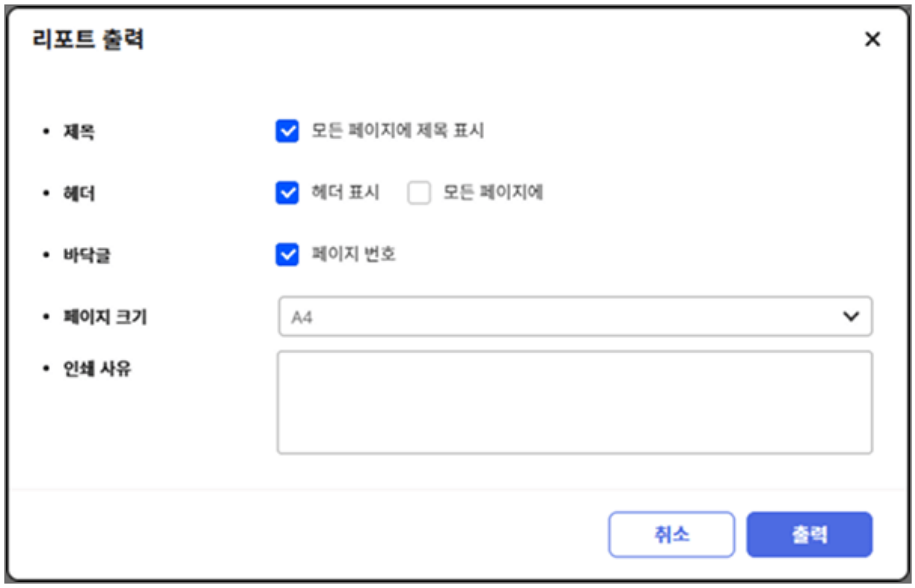


알아두기

내보내기 사유는 필수 입력 항목이 아닙니다. 내보내기 사유는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

리포트 인쇄

PC와 연결된 프린터로 리포트를 인쇄하려면 **출력** 버튼을 클릭하세요. **리포트 출력** 창이 나타나면 각 항목을 설정하고 **출력** 버튼을 클릭하세요.



웹 브라우저의 새 탭을 통해 인쇄 미리보기 화면이 나타납니다. 화면 오른쪽 상단의 인쇄 버튼을 클릭하면 인쇄를 시작할 수 있습니다.

> **알아두기**
> **인쇄 사유**는 필수 입력 항목이 아닙니다. 인쇄 사유는 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 기록을 확인할 수 있습니다.

리포트 삭제

저장한 리포트를 삭제하려면 화면 왼쪽 사이드바의 **저장된 리포트** 하위에서 삭제할 리포트를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **리포트 템플릿 삭제**를 선택하세요.



열 설정

리포트에 표시되는 열(Column) 설정을 변경할 수 있습니다. 열 설정을 통해 표시할 열을 선택하거나 열의 순서를 변경할 수 있습니다.

1. 리포트 오른쪽 상단의 **열 설정** 버튼을 클릭하세요.
2. **열 레이아웃** 창이 나타나면 원하는 열을 선택하거나 선택 해제하세요.



3. 열의 순서를 변경하려면 원하는 열을 클릭한 채로 드래그하여 위치를 변경하세요.

4. 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 열 레이아웃 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.
> - 생성한 리포트에 따라 선택 또는 선택 해제할 수 있는 열이 다를 수 있습니다.

자동 생성 스케줄 설정하기

유동 기간으로 설정하여 생성한 **커스텀 리포트**를 자동으로 생성하도록 스케줄을 설정할 수 있습니다.

자동 생성 스케줄 추가

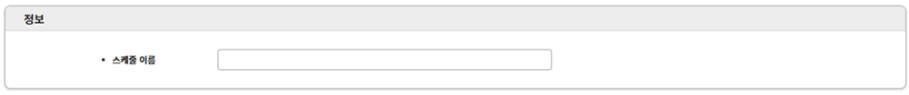
1. **런처** 페이지에서 **데이터**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **데이터**를 선택하세요.
2. **자동 생성 스케줄** 탭을 클릭하세요.
3. 화면 오른쪽 상단의 **스케줄 추가**를 클릭하세요.



4. **자동 생성 스케줄 추가** 화면이 나타나면 각 항목을 설정하세요.

정보 설정

자동 생성 스케줄의 기본 정보를 설정할 수 있습니다.



- **스케줄 이름**: 스케줄의 이름을 입력하세요.

리포트 및 스케줄 설정

리포트별 자동 생성 스케줄을 설정할 수 있습니다.



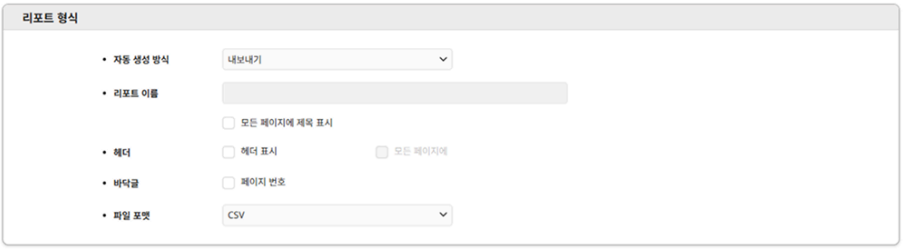
- **리포트**: 자동 생성할 커스텀 리포트를 선택할 수 있습니다. 유동 기간으로 설정된 커스텀 리포트만 나타납니다.
- **생성 주기**: 리포트를 자동 생성할 주기를 설정할 수 있습니다.

- **생성 시간**: 리포트를 자동 생성할 시간을 설정할 수 있습니다.

> **알아두기**
> 커스텀 리포트 생성에 대한 자세한 내용은 리포트 생성하기를 참고하세요.

리포트 형식 설정

리포트별 형식을 설정할 수 있습니다.



- **자동 생성 방식**: 리포트의 자동 생성 방식을 설정할 수 있습니다.
- **리포트 이름**: 리포트 이름을 모든 페이지에 제목으로 표시하려면 **모든 페이지에 제목 표시**를 선택하세요.
- **헤더**: **헤더 표시**를 선택하면 리포트 생성 시 헤더를 표시할 수 있습니다. 헤더를 모든 페이지에 표시하려면 **모든 페이지에**를 선택하세요.

> **알아두기**
> 리포트별로 생성되는 헤더는 다를 수 있습니다.

- **바닥글**: 페이지 번호 표시 여부를 설정할 수 있습니다.
- **파일 포맷**: 리포트를 내보낼 파일 형식을 설정할 수 있습니다.

3. 설정을 저장하려면 **적용**을 클릭하세요.

> **알아두기**
> 모든 설정을 완료했다면 리포트를 저장할 경로를 설정하세요. 자세한 내용은 리포트 저장 경로 설정하기를 참고하세요.

자동 생성 스케줄 삭제

1. **런처** 페이지에서 **데이터**를 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **데이터**를 선택하세요.
2. **자동 생성 스케줄** 탭을 클릭하세요.
3. 자동 스케줄 목록에서 삭제할 스케줄의 체크박스를 클릭하세요.

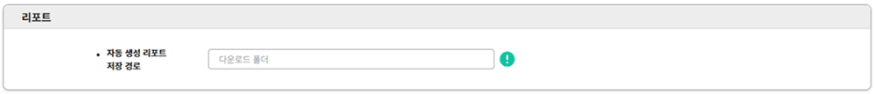


4. 화면 오른쪽 상단의 **삭제**를 클릭하세요.

리포트 저장 경로 설정하기

자동 생성 스케줄을 설정했다면 리포트를 저장할 경로를 설정하세요.

1. **설정**을 클릭하세요.
2. 리포트를 저장할 경로를 입력하세요.



   - **자동 생성 리포트 저장 경로**: 지정한 경로로 리포트가 저장되며, 경로를 입력하지 않으면 사용자 PC의 *Documents\BioStarX* 폴더에 자동 저장됩니다.

3. 설정을 저장하려면 **적용**을 클릭하세요.

대시보드

대시보드는 사용자 개인별로 원하는 정보를 선택하여 위젯을 추가하고, 자유롭게 위젯을 설정하고 배치하여 입맛에 맞게 구성할 수 있습니다.

> **알아두기**
>
> - 각 사용자마다 개인별로 **대시보드**를 구성할 수 있습니다.
> - **대시보드**에서 확인할 수 있는 정보는 **관리자 등급**에 따라 다를 수 있습니다.

위젯 추가하기

BioStar X 대시보드는 사용자가 원하는 정보를 자유롭게 배치할 수 있는 사용자 정의형 모니터링 화면입니다. 다양한 위젯을 추가하여 출입 통제 시스템의 주요 정보를 업무 환경에 맞게 구성할 수 있습니다.

추가할 수 있는 위젯 종류는 아래와 같습니다.

- **차트**: 출입 이벤트 데이터를 막대/선/원형 차트로 시각화
- **카운터**: 일간/주간 이벤트 발생 수를 숫자로 표시
- **실시간 이벤트**: **BioStar X**에서 발생하는 모든 이벤트를 실시간 모니터링
- **실시간 출입 모니터링**: 특정 장치의 인증 성공 사용자 정보를 실시간 표시
- **시스템 사용 현황**: 사용자, 장치, 출입문 등의 등록 현황을 숫자로 표시
- **출입문 제어**: 선택한 출입문의 상태 확인 및 원격 제어
- **텍스트**: 공지사항이나 위젯 타이틀 등 사용자 정의 텍스트 배치

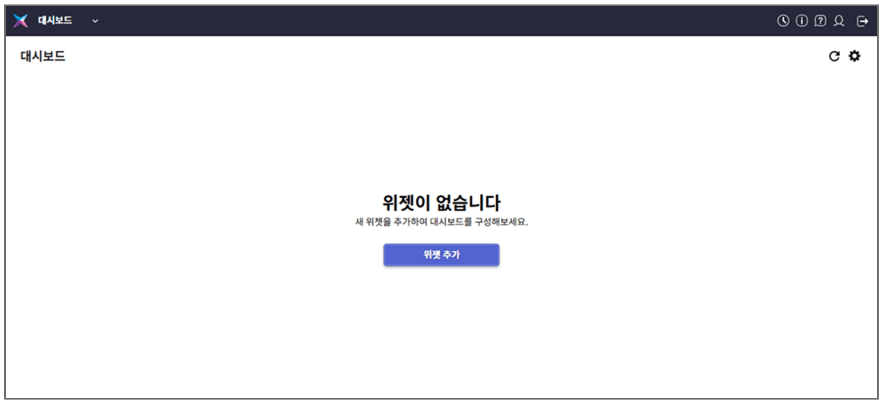
대시보드에 배치한 위젯을 통해서 아래와 같은 이점을 얻을 수 있습니다.

- **맞춤형 구성**: 업무에 필요한 정보만 선별하여 한 화면에 배치
- **실시간 모니터링**: 출입 이벤트와 시스템 상태를 즉시 확인
- **직관적인 시각화**: 차트와 카운터를 통한 데이터의 시각적 표현
- **효율적인 관리**: 모니터링과 제어 기능을 통합하여 업무 효율성 향상

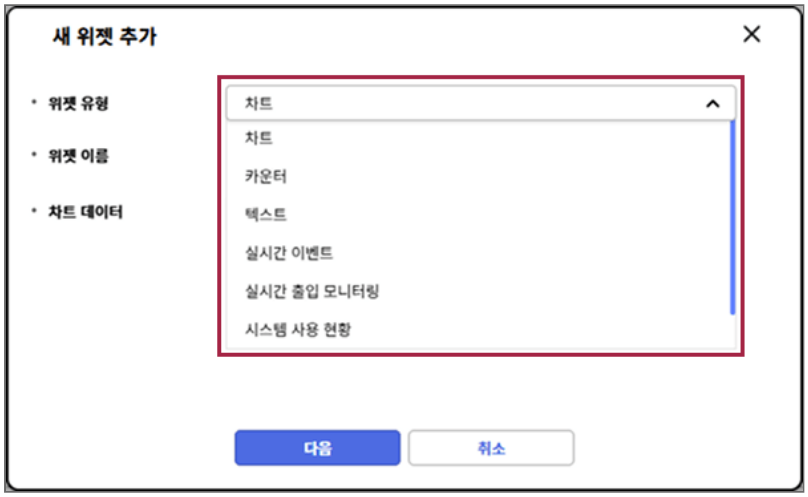
위젯 추가

대시보드에 위젯을 추가하여 원하는 정보를 확인할 수 있습니다.

1. **런처** 페이지에서 **대시보드**를 클릭하세요.
2. **위젯 추가** 버튼을 클릭하세요.



3. **새 위젯 추가** 창이 나타나면 **위젯 유형**에서 원하는 항목을 선택하고 필수 항목을 입력 또는 설정하세요.



4. 위젯 설정을 완료하고 **적용** 버튼을 클릭하세요.
5. 위젯 표시 영역에 위젯이 생성되면 크기를 조절하거나 원하는 위치에 배치하세요.
6. 모든 설정을 완료하면 화면 오른쪽 상단의 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> 이미 위젯이 추가 되어있다면 화면 오른쪽 상단의 ⚙ 아이콘을 클릭하세요. **대시보드 설정** 모드로 진입하면 **위젯 추가** 버튼을 클릭하세요.

위젯 종류

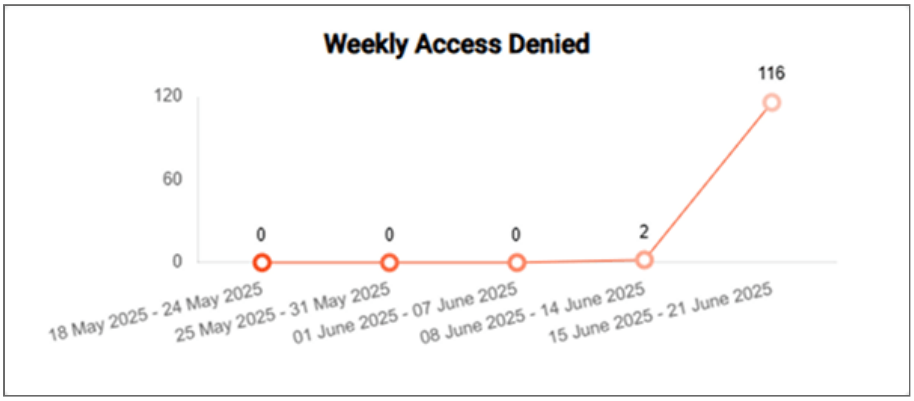
- 각 위젯 별로 위젯 크기 기본값이 다르게 설정되어 있으며 기본값에서 가장 보기 좋게 최적화되어 있습니다.
- 모든 위젯은 우측 하단부를 드래그하여 크기를 조절할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

차트

원하는 차트 데이터를 선택하여 발생한 이벤트 수를 차트로 나타낼 수 있습니다.



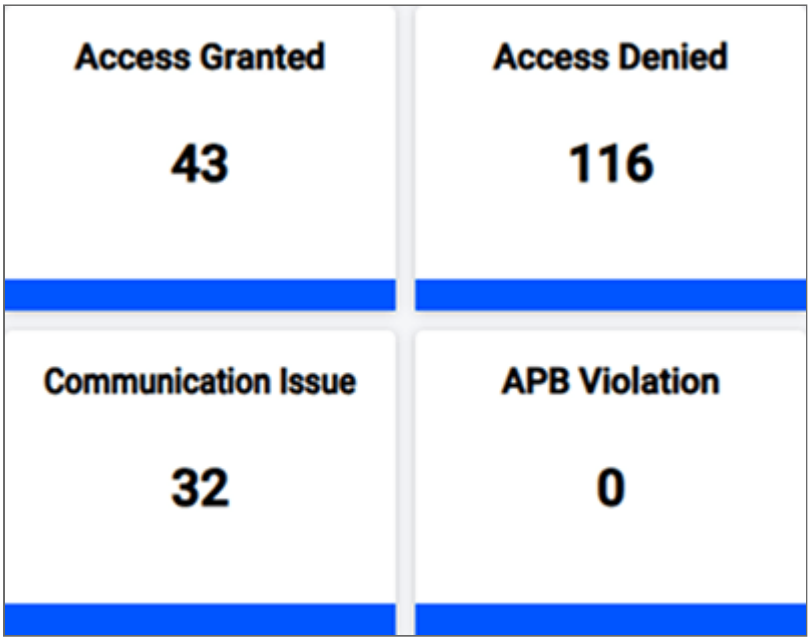
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **차트 데이터**: 일간, 주간 이벤트 목록 중에서 원하는 차트 데이터를 선택하세요.
  - **일간 출입 성공**, **일간 출입 실패**, **일간 통신 이슈**, **일간 APB 위반**, **주간 출입 성공**, **주간 출입 실패**, **주간 통신 이슈**, **주간 APB 위반**
- **차트 유형**: **세로 막대 차트**, **가로 막대 차트**, **선형 차트**, **파이 차트** 중에 원하는 타입을 선택하세요.
- **색상 조합**: 다섯 가지의 색상 조합 중에 원하는 색상을 선택하세요.

> **알아두기**
> **색상 조합**을 선택할 때 보여지는 차트의 값은 실제 값이 아닌 미리보기를 위한 임의의 값입니다.

카운터

원하는 카운터 데이터를 선택하여 발생한 이벤트 수를 숫자로 나타낼 수 있습니다.

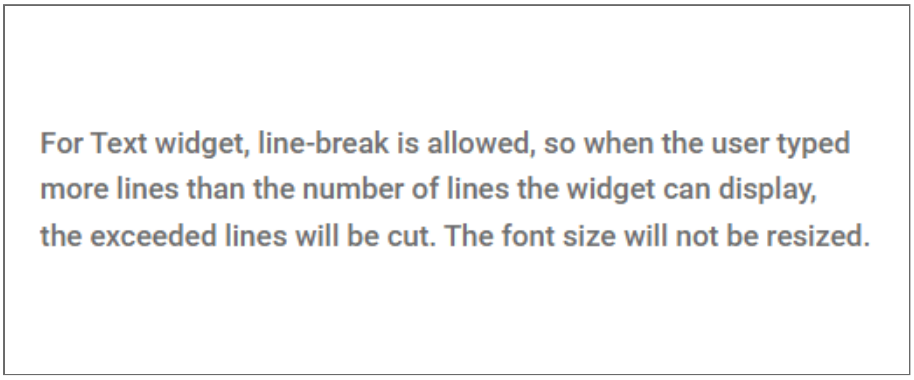


위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **카운터 데이터**: 일간, 주간 이벤트 목록 중에서 원하는 카운터 데이터를 선택하세요.
  - **일간 출입 성공**, **일간 출입 실패**, **일간 통신 이슈**, **일간 APB 위반**, **주간 출입 성공**, **주간 출입 실패**, **주간 통신 이슈**, **주간 APB 위반**

텍스트

대시보드의 위젯 영역에 사용자가 원하는 텍스트를 입력하여 배치할 수 있습니다. 생성 후 필요한 위치에 배치하여 위젯의 타이틀로 사용하거나 공지사항 등으로 사용할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

> **알아두기**
> **텍스트** 위젯 생성 시 **배경 제거** 옵션을 체크하면 배경에 투명도가 적용됩니다.

실시간 이벤트

BioStar X에서 발생하는 이벤트를 실시간으로 보여줍니다. 특정 이벤트, 사용자, 출입문, 장치를 필터링해서 이벤트를 확인할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **일시 중지**: 실시간 이벤트를 정지할 수 있습니다.
- **시작**: 중지한 실시간 이벤트를 다시 시작할 수 있습니다.
- **지우기**: 인증 기록을 전체 삭제할 수 있습니다.

> **알아두기**
> 다른 페이지로 이동했다가 다시 **대시보드**로 돌아올 경우 목록이 비워지고 다시 이벤트가 기록됩니다.

실시간 출입 모니터링

하나의 장치를 선택하여 선택한 장치에 인증을 성공한 사용자의 프로필 사진 및 정보(**사용자**, **날짜**, **장치**)를 실시간으로 보여줍니다.



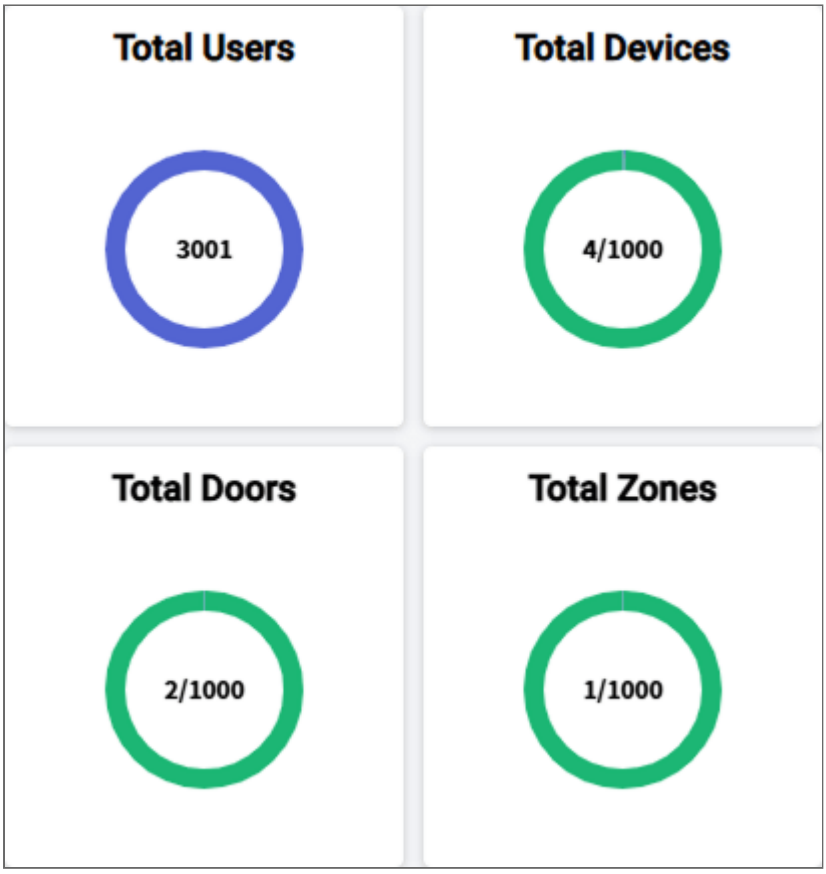
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

- **일시 중지**: 실시간 출입 모니터링을 정지할 수 있습니다.
- **시작**: 중지한 실시간 출입 모니터링을 다시 시작할 수 있습니다.
- **지우기**: 인증 기록을 전체 삭제할 수 있습니다.

> **알아두기**
> **실시간 출입 모니터링**은 최대 5명까지 기록됩니다.

시스템 사용 현황

BioStar X의 다양한 사용 현황을 숫자로 나타냅니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

나타낼 수 있는 **시스템 사용 현황**은 다음과 같습니다.

- **사용자**, **카드**, **지문**, **얼굴**, **페이스**, **QR/바코드**, **모바일 액세스**, **장치**, **출입문**, **고급 출입 통제**, **출입 그룹**, **사용자 그룹**, **장치 그룹**, **IR 페이스**

출입문 제어

하나의 출입문을 선택하여 선택한 출입문의 상태를 확인하고 제어할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

제어 버튼으로 제어할 수 있는 항목은 다음과 같습니다.

- **열림**, **해제**, **수동 잠금**, **수동 개방**, **알람 해제**, **APB 초기화**

> **알아두기**
> **출입문 제어** 위젯의 이름은 출입문의 이름으로 자동 지정되며 수정할 수 없습니다.

위젯 데이터 새로고침 간격 설정

대시보드에 추가된 위젯의 데이터 새로고침 간격을 설정할 수 있습니다.

1. **런처** 페이지에서 **대시보드**를 클릭하세요.
2. 화면 오른쪽 상단의 ⚙ 아이콘을 클릭하세요.
3. **대시보드 설정** 모드로 진입하면 화면 하단에 일반 설정에서 **자동 새로고침 주기**를 설정하세요.

위젯 수정하기

대시보드에 추가한 위젯을 수정하는 방법을 안내합니다.

1. **런처** 페이지에서 **대시보드**를 클릭하세요.
2. 화면 오른쪽 상단의 ⚙ 아이콘을 클릭하세요.
3. **대시보드 설정** 모드로 진입하면 수정하려는 **위젯**의 오른쪽 상단에 ✎ 아이콘을 클릭하세요.
4. **위젯 수정** 창이 나타나면 원하는 항목을 수정하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

5. 수정을 완료하면 **적용** 버튼을 클릭하세요.
6. **대시보드 설정** 화면 오른쪽 상단의 **적용** 버튼을 클릭하세요.

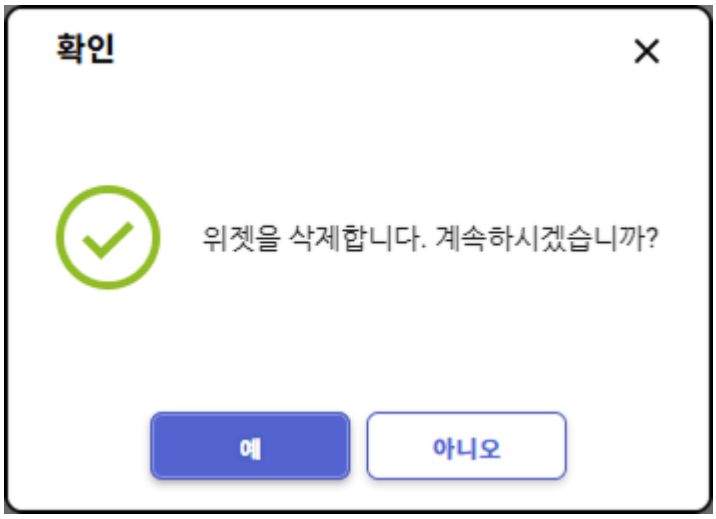
대시보드 화면에서 수정한 사항이 반영된 것을 확인하세요.

> **알아두기**
> - **위젯 수정**에서 **위젯 유형**은 변경할 수 없습니다.
> - 정해진 항목을 사용하는 **텍스트**, **시스템 사용 현황**, **출입문 제어**는 **위젯 이름**을 수정할 수 없습니다.

위젯 삭제하기

대시보드에 추가된 위젯을 삭제하는 방법을 안내합니다.

1. **런처** 페이지에서 **대시보드**를 클릭하세요.
2. 화면 오른쪽 상단의 ⚙ 아이콘을 클릭하세요.
3. **대시보드 설정** 모드로 진입하면 삭제하려는 **위젯**의 오른쪽 상단에 🗑 버튼을 클릭하세요.
4. 삭제 확인 팝업창을 확인하고 **네** 버튼을 클릭하세요.



5. **대시보드 설정** 화면 오른쪽 상단의 **적용**을 클릭하세요.

대시보드 화면에서 수정한 사항이 반영된 것을 확인하세요.

설정

BioStar X의 **설정** 페이지에서 설정할 수 있는 다양한 기능을 안내합니다. 장치를 추가하고, 권한, 언어, 날짜 및 시간, 출입 카드 관리 등 사용자 환경에 맞춤 설정을 위한 다양한 옵션을 살펴볼 수 있습니다.

런처 페이지에서 **설정**을 클릭하거나 화면 왼쪽 상단의 바로 가기 목록에서 **설정**을 선택하세요.

> **알아두기**
> 사용자의 권한에 따라 설정할 수 있는 기능이 다를 수 있습니다. 일부 기능은 관리자 권한이 있는 사용자만 사용할 수 있습니다. 사용자 권한별 접근할 수 있는 메뉴에 대한 자세한 내용은 사용자 권한 설정하기를 참고하세요.

장치 관리하기

장치를 추가하거나 삭제, 수정에 대한 관리 방법을 안내합니다. 장치에 등록된 사용자 정보를 **BioStar X** 서버로 가져오거나 원격으로 펌웨어를 업그레이드할 수 있습니다.

장치 그룹 관리하기

여러 개의 장치를 효율적으로 관리할 수 있는 장치 그룹 기능을 안내합니다. 장치 그룹을 사용하면 여러 장치를 하나의 그룹으로 묶어 관리할 수 있어, 대규모 시스템에서 장치 설정을 일괄적으로 적용하거나 모니터링할 때 유용합니다.

> **팁**
> 장치 그룹 이름은 장치가 위치한 장소나 용도로 지정하면 관리가 편리합니다. 예를 들어, '1층 출입구', '2층 사무실', '회의실' 등으로 그룹을 지정할 수 있습니다.

장치 그룹 생성

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록의 **모든 장치**에서 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **그룹 추가**를 클릭하세요.
5. 원하는 그룹 이름을 입력하세요.

> **알아두기**
>
> - 장치 그룹은 8단계의 하위 그룹까지 생성할 수 있습니다.
> - 장치 그룹 이름은 최대 48자까지 입력할 수 있습니다.
> - 장치 목록에서 장치 그룹을 선택하면 해당 그룹에 속한 장치만 목록에 표시됩니다.

장치 그룹 이름 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록의 **모든 장치** 하위에서 이름을 변경할 장치 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **이름 변경**을 클릭하세요.
5. 수정하려는 그룹 이름을 입력하세요.

> **알아두기**
> 장치 그룹 이름은 최대 48자까지 입력할 수 있습니다.

장치 그룹 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록의 **모든 장치** 하위에서 삭제할 장치 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **그룹 삭제**를 클릭하세요.

> **주의**
> 장치 그룹을 삭제하면 해당 그룹에 속한 모든 장치가 삭제됩니다.

장치 등록하기

BioStar X에 장치를 등록하는 방법을 안내합니다. 장치를 등록하면 **BioStar X**에서 해당 장치의 상태를 모니터링하고 관리할 수 있습니다. 장치를 검색하기 전에 장치가 올바르게 연결되어 있는지 확인하세요. 여러 개의 장치를 한번에 추가할 때 각 장치의 위치, ID, IP 주소 등을 미리 알아두면 편리합니다.

알아두기

- 장치를 새로 등록할 때 장치의 키 값을 서버의 데이터 암호화 키 값으로 변경합니다. 키 변환 시 장치의 모든 사용자 데이터가 삭제됩니다.
- 장치에 저장된 모든 설정 정보 및 사용자 정보를 삭제한 뒤 다시 전송하려면 **데이터 삭제 후 장치 동기화**를 클릭하세요. **데이터 삭제 후 장치 동기화** 옵션은 장치 목록에서 장치를 선택하고 ••• 버튼을 클릭하면 확인할 수 있습니다.
- **대기 장치** 그룹의 모든 장치를 등록하려면 그룹 이름에서 마우스 오른쪽 버튼을 클릭하고 **모든 등록 대기 장치 등록**를 클릭하세요. 장치를 각각 등록하려면 장치 이름에서 마우스 오른쪽 버튼을 클릭하고 **등록 대기 장치 추가**를 클릭하세요.
- **BioStar X**와 장치에 사용자 ID 종류가 다르게 설정되어 있다면 **BioStar X**의 사용자 ID 설정에 따라 장치 설정을 변경하세요.
- **BioStar X**의 사용자 ID 종류가 영숫자로 설정된 경우 일부 장치를 사용할 수 없거나 제약 사항이 발생할 수 있습니다. 자세한 내용은 서버 상세 설정하기를 참고하세요.
- 장치를 등록하고 세부 정보를 설정하려면 장치 설정하기를 참고하세요.
- 이더넷(TCP/IP)으로 연결할 수 있는 장치는 최대 1,000대입니다.
- 장치를 등록하려면 **디바이스 매니저** 이상의 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

시작하기 전에

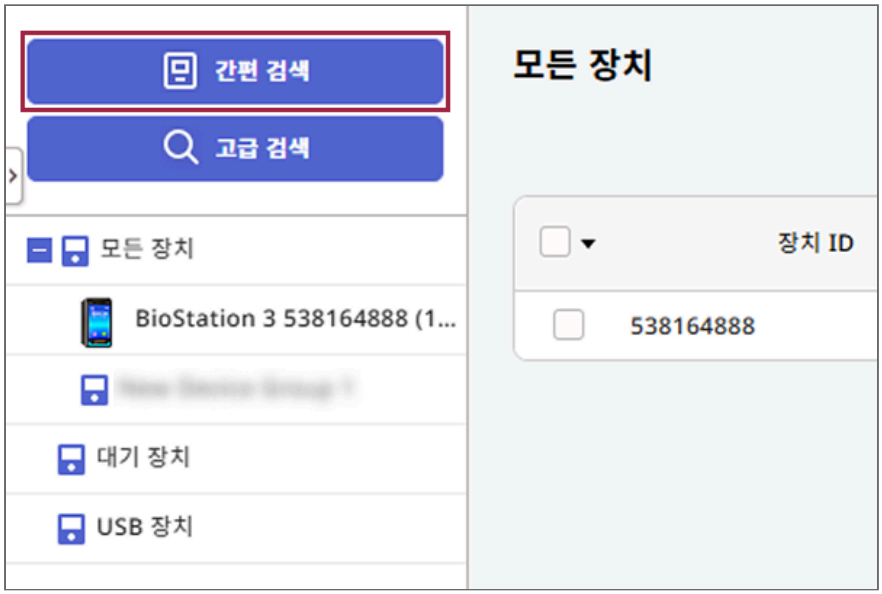
장치를 등록하기 전에 다음 사항을 확인하세요.

- 출입 통제를 위한 출입 등급, 출입 그룹, 층 등급을 설정하세요. 자세한 내용은 출입 통제 설정하기를 참고하세요.
- 장치를 효율적으로 관리하기 위한 그룹을 생성하세요. 자세한 내용은 장치 그룹 관리하기를 참고하세요.

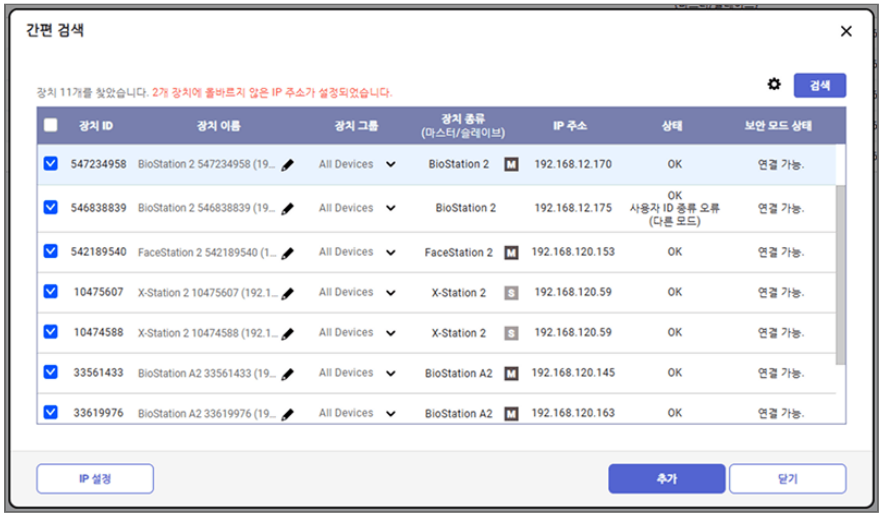
간편 등록하기

BioStar X와 같은 네트워크에 있는 장치를 자동으로 검색하고 등록할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 **간편 검색** 버튼을 클릭하세요.

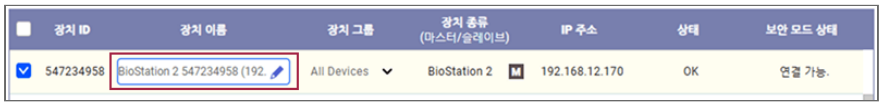


4. **간편 검색** 창이 나타나면 등록할 수 있는 모든 장치 목록이 표시됩니다. 원하는 장치가 목록에 없다면 오른쪽 상단의 **검색** 버튼을 클릭하세요.

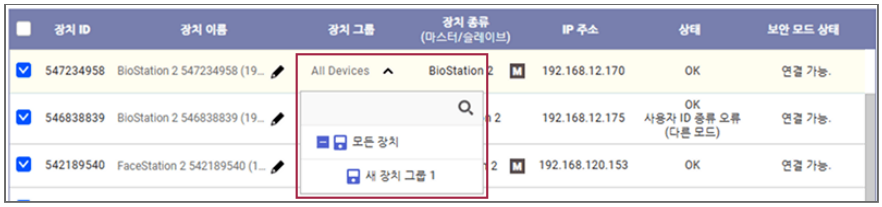


5. 장치 목록에서 등록할 장치를 선택하거나 등록하지 않을 장치는 선택을 해제하세요.

6. 등록할 장치의 이름을 변경하려면 **장치 이름** 열에서 ✎ 버튼을 클릭한 뒤 변경하세요.



7. 등록할 장치의 그룹을 설명하려면 **장치 그룹** 열에서 선택하세요.



8. 선택한 장치에 대한 설정을 모두 완료했다면 **추가** 버튼을 클릭하세요.

장치 목록에 추가한 장치가 나타납니다. 추가한 장치를 선택하고 **장치 동기화** 버튼을 클릭하세요.



> **알아두기**
> IP 주소를 사용할 수 없거나 변경이 필요한 장치는 **IP 설정** 버튼을 클릭해 변경할 수 있습니다. 자세한 내용은 IP 주소 설정을 참고하세요.

IP 주소 설정

새로 등록하려는 장치의 IP 주소를 변경할 수 있습니다. **간편 검색** 창의 왼쪽 하단에 **IP 설정** 버튼을 클릭하세요. **IP 설정** 창이 나타나면 장치 목록에서 IP 주소를 변경할 장치를 선택하세요.



- **DHCP 사용**: 장치가 DHCP를 통해 IP 주소를 자동으로 할당받도록 설정합니다. 이 옵션을 선택하면 장치가 네트워크에 연결될 때마다 IP 주소가 변경될 수 있습니다.

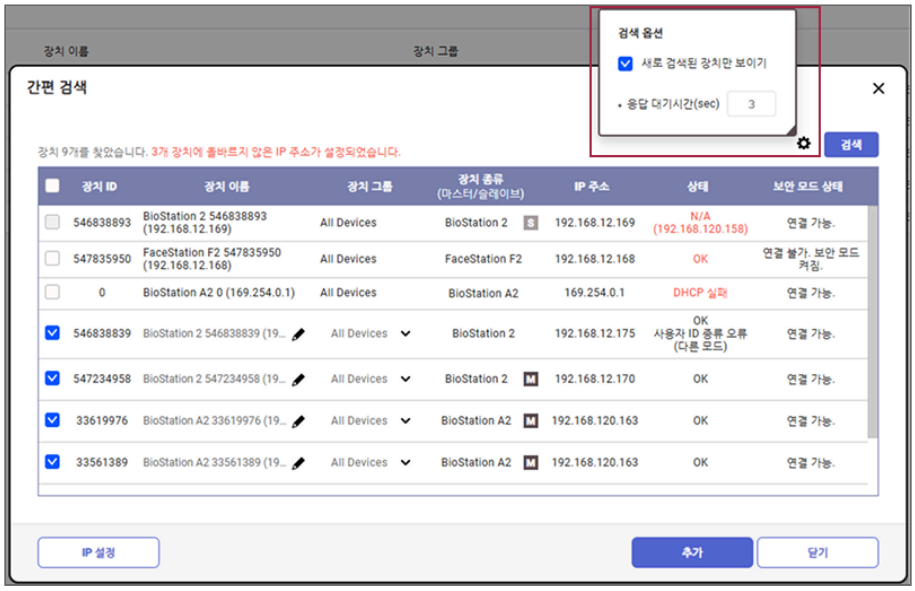
  > IP 주소와 서브넷 마스크, 게이트웨이 등을 수동으로 입력하려면 옵션을 선택 해제하세요.

- **장치에서 서버 연결**: 장치에서 **BioStar X** 서버로 연결하도록 설정하려면 이 옵션을 선택하세요. **BioStar X**를 설치한 서버의 IP 주소와 포트 번호를 입력해야 합니다.

> **알아두기**
> IP 설정을 모두 완료하고 변경 사항을 저장하려면 **확인** 버튼을 클릭하세요. 변경 사항을 취소하려면 **취소** 버튼을 클릭하세요.

장치 검색 옵션

간편 검색 창 오른쪽 상단의 ⚙ 버튼을 클릭하면 장치 검색 옵션을 설정할 수 있습니다.

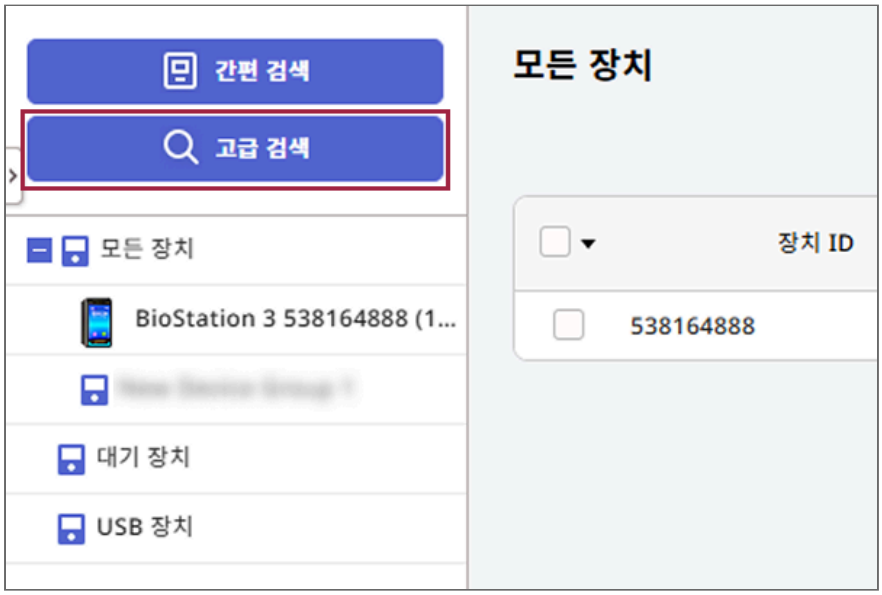


- **새로 검색된 장치만 보이기**: 새로 검색된 장치만 검색 목록에 표시하려면 이 옵션을 선택하세요.
- **응답 대기시간(sec)**: 일정 시간 동안 응답하지 않는 장치를 검색 목록에서 제외하려면 원하는 시간을 설정하세요. 초 단위로 설정할 수 있으며, 기본값은 3초입니다.

고급 검색

특정 장치의 IP 주소와 포트 번호를 지정하여 등록할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 **고급 검색** 버튼을 클릭하세요.



4. **고급 검색** 창이 나타나면 등록할 장치의 IP 주소와 포트 번호를 입력하세요.



5. **검색** 버튼을 클릭하면 입력한 조건과 일치하는 장치가 목록에 표시됩니다.



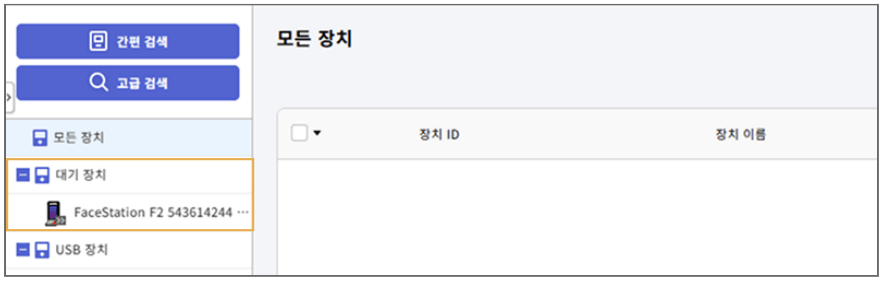
6. 장치를 등록하려면 **추가** 버튼을 클릭하세요.

장치 목록에 추가한 장치가 나타납니다. 추가한 장치를 선택하고 **장치 동기화** 버튼을 클릭하세요.

대기 중인 장치 등록

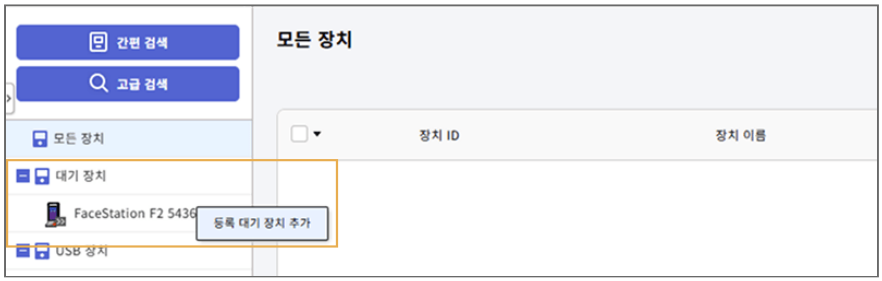
장치 → 서버 옵션으로 구성된 장치는 서버의 IP 주소와 포트 번호를 사용해 **BioStar X** 서버로 연결을 시도합니다. 이와 같은 방식으로 연결된 장치는 활성 장치 목록에 자동 추가되지 않습니다. 해당 장치는 **대기 장치** 그룹에 표시되며, 권한이 있는 관리자가 직접 등록해야 합니다.

1. 장치의 **장치 → 서버** 옵션에서 **BioStar X**의 IP 주소와 포트 번호를 설정하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
4. **대기 장치** 그룹에 표시된 장치를 확인하세요.



5. 개별 장치를 등록하려면 **대기 장치** 그룹의 장치 이름에서 마우스 오른쪽 버튼을 클릭하세요.

   대기 장치 그룹의 모든 장치를 등록하려면 **대기 장치** 그룹에서 마우스 오른쪽 버튼을 클릭하세요.



6. 팝업 메뉴에서 **등록 대기 장치 추가**(개별 장치) 또는 **모든 등록 대기 장치 등록**(모든 장치)을 클릭하세요.

대기 장치 그룹의 장치가 등록되면 **모든 장치** 목록으로 이동합니다.

> **알아두기**
>
> - 장치의 **장치 → 서버** 옵션은 **설정** → **통신** → **서버**에서 설정할 수 있습니다. 메뉴 경로는 장치에 따라 다를 수 있습니다.
> - BioStar X에서 **IP 설정** → **장치에서 서버 연결** 옵션(IP 주소 설정)으로 설정할 수도 있습니다.
> - **대기 장치** 그룹의 장치는 동기화되지 않습니다. 장치를 등록하고 장치 동기화가 실행되기 전까지 사용자 데이터, 출입 등급, 출입 그룹 및 장치 설정 등은 해당 장치로 전송되지 않습니다.

Wiegand 장치 등록하기

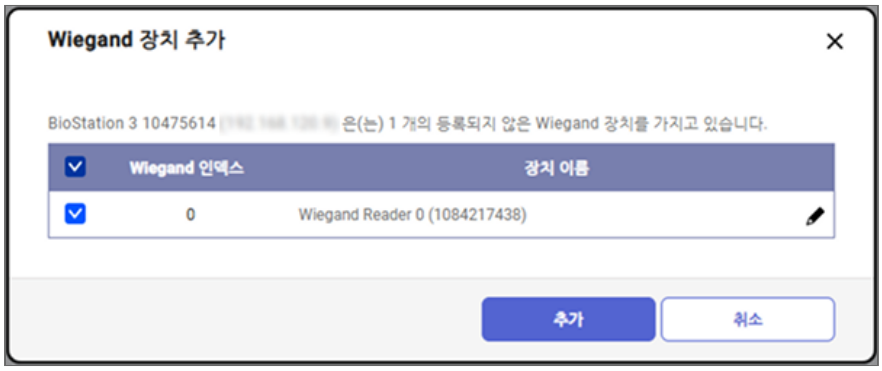
등록한 마스터 장치나 슬레이브 장치에 Wiegand 장치를 추가하는 방법을 안내합니다.

> **알아두기**
>
> - **마스터(Master) 장치**: RS-485로 연결한 장치 중 컨트롤러 역할을 수행하는 장치입니다. 슬레이브 장치를 주기적으로 모니터링하여 데이터를 처리합니다. 호스트(Host) 장치라고도 부릅니다.
> - **슬레이브(Slave) 장치**: RS-485로 연결한 장치 중 리더 또는 입출력 기능만 수행하는 장치입니다. 사용자 정보를 갖고 있지 않으며 마스터 장치에 의해 제어됩니다.
> - **Wiegand**: Wiegand는 두 개의 신호선(DATA0, DATA1)을 사용하여 데이터를 전송하는 통신 방식입니다. 주로 출입 통제 시스템에서 리더(Reader)와 컨트롤러 간의 통신에 사용되며, 간단한 구조와 낮은 비용으로 구현할 수 있습니다. 다만, 전송 거리가 짧고 데이터 전송 속도가 느린 한계가 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. **모든 장치** 목록의 마스터 또는 슬레이브 장치에서 마우스 오른쪽 버튼을 클릭하세요.

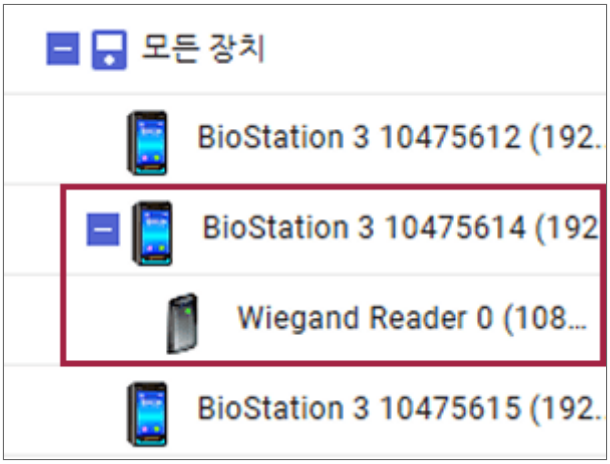


4. 팝업 메뉴에서 **Wiegand 장치 추가**를 클릭하세요.
5. 해당 마스터 장치에 연결된 Wiegand 장치 목록이 나타나면 등록할 장치를 선택하세요.



6. **추가** 버튼을 클릭하세요.
7. 장치 등록 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

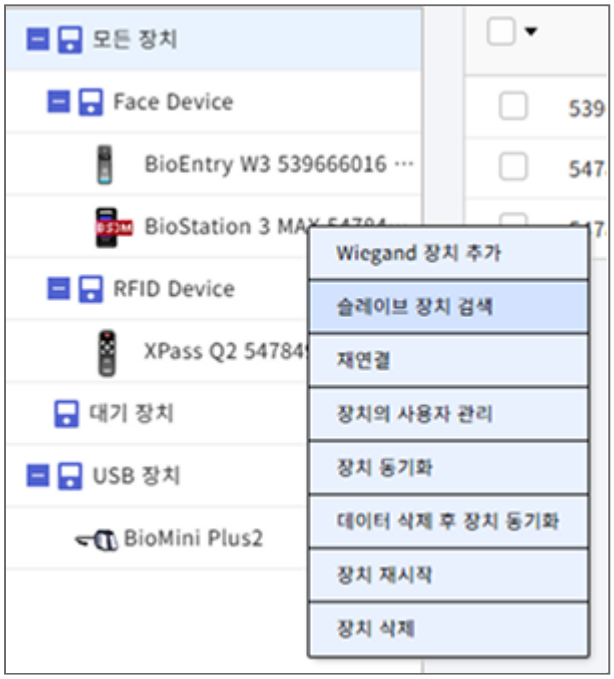
선택한 장치의 하위로 등록한 Wiegand 장치가 나타납니다.



슬레이브 장치 등록하기

등록한 마스터 장치에 슬레이브 장치를 추가해 손쉽게 출입 통제 시스템의 네트워크를 확장할 수 있습니다. 마스터 장치와 슬레이브 장치는 RS-485 통신으로 연결할 수 있습니다. 장치뿐만 아니라 Secure I/O 2와 같은 부가 장치도 연결해 사용할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. **모든 장치** 목록의 마스터 또는 슬레이브 장치에서 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **슬레이브 장치 검색**를 클릭하세요.
5. 해당 마스터 장치에 연결된 슬레이브 장치 목록이 나타나면 등록할 장치를 선택하세요. 원하는 장치가 없다면 오른쪽 상단의 **검색** 버튼을 클릭하세요.



6. **추가** 버튼을 클릭하세요.
7. 장치 등록 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

선택한 장치의 하위로 등록한 슬레이브 장치가 나타납니다. 장치 목록에서 마스터 장치는 아이콘이, 슬레이브 장치는 아이콘이 표시됩니다.



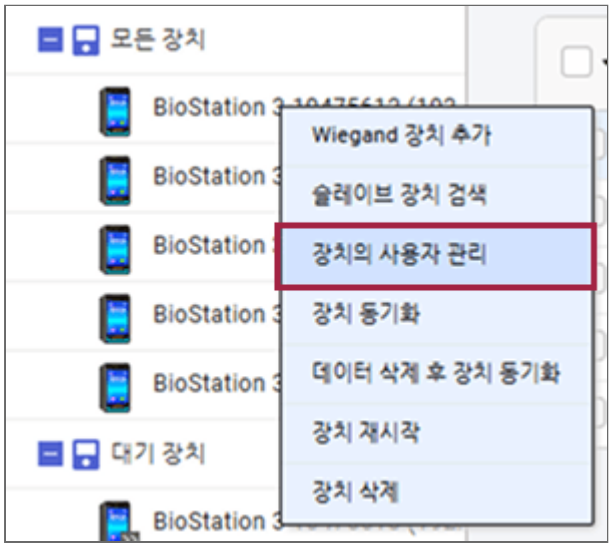
알아두기

- 지문 인식 장치가 마스터 장치일 때 얼굴 인증 장치를 슬레이브 장치로 추가할 수 없습니다.
- 얼굴 인증 장치가 마스터 장치이고 다른 슬레이브 장치가 이미 추가되어 있다면 얼굴 인증 장치를 슬레이브 장치로 추가할 수 없습니다.
- 얼굴 인증 장치가 마스터 장치이고 얼굴 인증 장치를 슬레이브 장치로 연결할 때 1대의 얼굴 인증 장치만 슬레이브 장치로 추가할 수 있습니다.
- 얼굴 인증 장치가 마스터 장치이고 얼굴 인증 장치를 슬레이브 장치로 연결할 때 Secure I/O 2와 DM-20을 각각 1대씩 추가로 연결할 수 있습니다.
- 연결할 수 있는 최대 슬레이브 장치 수는 인증 방법, 사용자 수, 장치 수에 따라 달라지며 슬레이브 장치 수는 인증 속도에 영향을 줍니다.

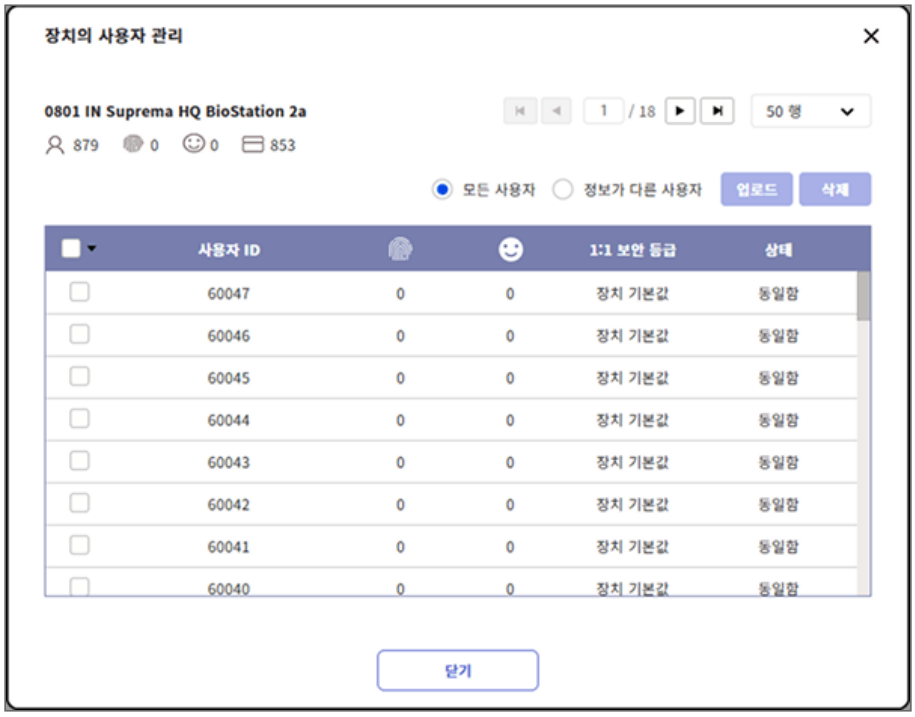
장치에 등록한 사용자 관리하기

장치에 등록한 사용자 수, 지문 수, 얼굴 수, 카드 수를 확인할 수 있습니다. **BioStar X**에 등록하지 않았거나 이미 등록한 사용자 정보와 비교해 **BioStar X** 서버로 전송하거나 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. **모든 장치** 목록에서 장치를 선택하고 마우스 오른쪽 버튼을 클릭하세요.
4. 팝업 메뉴에서 **장치의 사용자 관리**를 클릭하세요.



장치의 사용자 관리 창이 나타나면 장치에 등록한 사용자 정보와 **BioStar X**에 등록한 사용자 정보를 비교할 수 있습니다.



상태 열에서 표시된 값을 참고하여 사용자 정보를 장치에서 삭제할지, **BioStar X** 서버로 전송할지 선택할 수 있습니다. **상태** 열의 값은 다음과 같습니다.

- **동일함**: **BioStar X** 서버에 등록한 정보와 동일한 사용자
- **정보가 다름**: **BioStar X** 서버에 등록한 정보와 다른 사용자를
- **새 사용자**: **BioStar X** 서버에 등록되어 있지 않은 사용자

특정 사용자 정보를 장치에서 삭제하려면 삭제할 사용자를 선택하고 **삭제** 버튼을 클릭하세요. 사용자 정보를 **BioStar X** 서버로 전송하려면 **업로드** 버튼을 클릭하세요.

> **알아두기**
>
> - **장치의 사용자 관리** 기능은 하나의 장치만 선택해 사용할 수 있습니다.
> - **업로드** 버튼을 클릭할 때 **BioStar X** 서버에 동일한 ID를 가진 사용자가 있다면 장치의 정보로 업데이트할 수 있습니다.
> - 삭제한 사용자 정보는 장치에서만 삭제되며 **BioStar X** 서버에서는 유지됩니다.
> - 장치의 세부 설정에 대한 자세한 내용은 장치 설정하기를 참고하세요.

펌웨어 업그레이드하기

BioStar X와 연결된 장치는 별도의 연결이나 동작없이 손쉽게 펌웨어를 업그레이드할 수 있습니다. 장치의 펌웨어를 최신 버전으로 유지하면 보안 취약점을 해결하고 새로운 기능을 사용할 수 있습니다.

시작하기 전에

장치의 펌웨어를 업그레이드하기 전에 새로운 버전의 펌웨어 파일을 먼저 준비하세요. 다운로드한 펌웨어 파일을 아래 경로에 저장하고 압축을 해제하세요. *firmware* 폴더가 없다면 새로 생성하세요.

> *C:\Program Files\BioStar X\firmware*

> **알아두기**
> 새로운 버전의 펌웨어 파일은 슈프리마 다운로드 센터에서 장치 모델명을 검색하고 최신 버전의 펌웨어 파일을 다운로드하세요.

펌웨어 업그레이드

> **주의**
> - 펌웨어 업그레이드 전 장치의 전원 공급 혹은 네트워크 상태를 반드시 확인하세요. 특히 업그레이드 중 전원 공급이 차단되지 않도록 주의하세요.
> - 장치 종류와 모드에 따라 최대 1시간 이상이 걸릴 수 있습니다. 또한 업그레이드 중에는 장치를 사용할 수 없습니다.
> - 펌웨어 업그레이드가 진행되는 동안 장치의 전원을 끄지 마세요. 업그레이드를 완료하면 장치가 자동으로 재시작합니다.

한 개 장치의 펌웨어 업그레이드

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 펌웨어를 업그레이드할 장치를 클릭하세요.
4. 장치 세부 정보 화면의 **정보** 섹션에서 **펌웨어 업그레이드** 버튼을 클릭하세요.



5. **펌웨어 업그레이드** 창이 나타나면 펌웨어 버전을 클릭하세요.



6. 경고 메시지 창이 나타나면 **계속** 버튼을 클릭하세요.

장치에 대한 펌웨어 업그레이드를 진행합니다.

여러 장치의 펌웨어 업그레이드

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 펌웨어를 업그레이드할 장치의 가장 왼쪽에 체크박스를 선택하세요. 여러 개의 장치를 선택할 수 있습니다.
4. 장치 목록 오른쪽 상단의 **펌웨어 업그레이드** 버튼을 클릭하세요.



5. **펌웨어 업그레이드** 창이 나타나면 펌웨어 버전을 클릭하세요.



6. 경고 메시지 창이 나타나면 **계속** 버튼을 클릭하세요.

선택한 장치에 대한 펌웨어 업그레이드를 진행합니다.

> **알아두기**
>
> - **펌웨어 업그레이드** 버튼은 장치 목록에서 장치를 선택한 후에만 활성화됩니다.
> - 동일한 RS-485 모드를 가진 장치는 한 번에 여러 개를 동시에 업그레이드할 수 있습니다. 예를 들면, 마스터 장치는 마스터 장치끼리 한 번에 여러 개를 동시에 업그레이드할 수 있으며, 슬레이브 장치는 슬레이브 장치끼리 한 번에 여러 개를 동시에 업그레이드할 수 있습니다.
> - 마스터 장치나 마스터가 없는 슬레이브 장치는 한 번에 여러 개를 동시에 업그레이드할 수 있습니다.
> - 동일한 마스터 장치에 연결된 슬레이브 장치는 여러 개를 동시에 업그레이드할 수 없습니다.

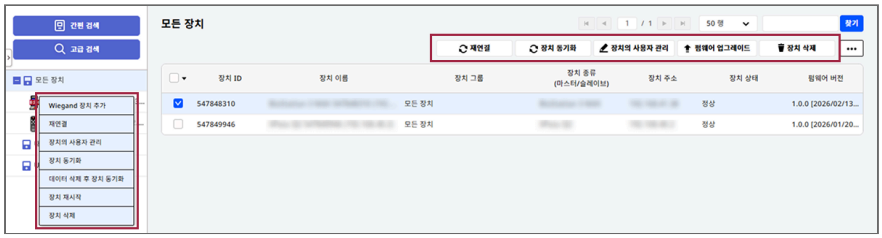
장치 관리 기능 사용하기

BioStar X에서 장치의 기타 기능을 사용하는 방법을 안내합니다. 장치를 재연결하거나 동기화, 정보 일괄 편집, 삭제, 설정 내보내기/가져오기 기능을 제공하며, 장치 삭제 시 보안 통신 인증서를 함께 삭제하는 옵션도 함께 안내합니다.

개별 장치의 관리 기능

한 개의 장치에 대한 관리 기능을 사용하는 방법은 아래와 같습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. **모든 장치** 목록에서 장치를 선택하고 마우스 오른쪽 버튼을 클릭하세요. 또는 장치 목록에서 원하는 장치의 체크박스를 클릭하세요.



4. 팝업 메뉴 또는 장치 목록 상단에서 원하는 기능을 선택하세요.

제공하는 기능은 아래를 참고하세요. 장치에 따라 제공하는 기능은 다를 수 있습니다.

- **재연결**: 선택한 장치를 재연결할 수 있습니다. 한 개의 장치를 선택했을 때 사용할 수 있습니다. 일반적으로 장치는 네트워크 연결이 복구되면 별도의 조작 없이 자동으로 온라인 상태로 돌아갑니다. 이 기능은 네트워크가 복구된 후에도 장치가 자동으로 재연결되지 않을 때 사용할 수 있습니다.

  > **알아두기**
  > 이 기능은 **장치에서 서버 연결** 옵션으로 연결된 장치는 지원하지 않습니다. 장치 등록에 대한 자세한 내용은 장치 등록하기를 참고하세요.

- **장치 동기화**: 등록한 장치와 **BioStar X**의 모든 사용자 정보를 동기화할 수 있습니다. **BioStar X** 데이터베이스 정보를 기준으로 사용자 정보를 동기화하며, 장치에만 등록한 사용자 정보는 삭제합니다. 사용자 정보를 **BioStar X**에 업로드하려면 **장치의 사용자 관리** 기능을 사용하세요.
- **데이터 삭제 후 장치 동기화**: 장치에 저장된 모든 설정 정보 및 사용자 정보를 삭제하고 다시 전송할 수 있습니다. 이 기능은 장치 목록에서 장치를 선택하고 ••• 버튼을 클릭하여 사용할 수도 있습니다.
- **장치의 사용자 관리**: 장치에 등록된 사용자 정보를 **BioStar X**에 업로드하거나 장치에서 삭제할 수 있습니다. 자세한 내용은 장치에 등록한 사용자 관리하기를 참고하세요.
- **펌웨어 업그레이드**: 장치의 펌웨어를 간편하게 업그레이드할 수 있습니다. 자세한 내용은 펌웨어 업그레이드하기를 참고하세요.
- **장치 재시작**: 선택한 장치를 재시작할 수 있습니다. 이 기능은 장치가 정상 동작하지 않을 때 사용할 수 있습니다.
- **장치 삭제**: 선택한 장치를 목록에서 삭제할 수 있습니다. 출입문 또는 구역으로 설정한 장치는 삭제할 수 없습니다. 자세한 내용은 장치 삭제를 참고하세요.

> **알아두기**
> - **Wiegand 장치 추가** 기능에 대한 자세한 내용은 Wiegand 장치 등록하기를 참고하세요.
> - **슬레이브 장치 검색** 기능에 대한 자세한 내용은 슬레이브 장치 등록하기를 참고하세요.

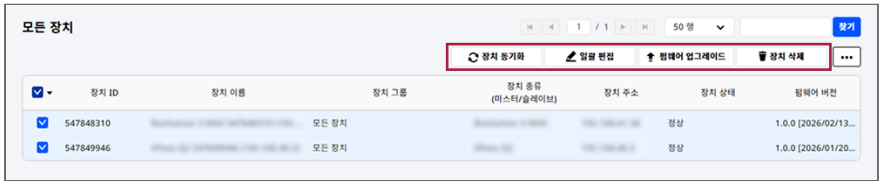
여러 장치의 관리 기능

한 개 이상의 장치에 대한 관리 기능을 사용하는 방법은 아래와 같습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.

3. 장치 목록에서 원하는 장치의 체크박스를 클릭하세요. 1개 이상의 장치를 선택할 수 있습니다.



4. 장치 목록 상단에서 원하는 기능을 선택하세요.

제공하는 기능은 아래를 참고하세요. 장치에 따라 제공하는 기능은 다를 수 있습니다.

- **장치 동기화**: 등록한 장치와 **BioStar X**의 모든 사용자 정보를 동기화할 수 있습니다. **BioStar X** 데이터베이스 정보를 기준으로 사용자 정보를 동기화하며, 장치에만 등록한 사용자 정보는 삭제합니다.

- **일괄 편집**: 선택한 장치의 정보를 일괄 편집할 수 있습니다. 버튼을 클릭하면 **일괄 편집** 창이 나타납니다.



> **알아두기**
>
> – 선택한 장치 종류에 따라 **일괄 편집** 창에 표시되는 세부 항목이 다를 수 있습니다.
>
> – 마스터 장치와 슬레이브 장치를 동시에 선택하고 일괄 편집을 클릭하면 **인증**과 **화면/소리** 항목의 일부만 변경할 수 있습니다.
>
> – **인증 모드**는 모델명이 동일한 장치를 선택했을 때만 일괄 편집할 수 있습니다.

- **펌웨어 업그레이드**: 장치의 펌웨어를 간편하게 업그레이드할 수 있습니다. 자세한 내용은 펌웨어 업그레이드하기를 참고하세요.

- **장치 삭제**: 선택한 장치를 목록에서 삭제할 수 있습니다. 출입문 또는 구역으로 설정한 장치는 삭제할 수 없습니다. 자세한 내용은 장치 삭제를 참고하세요.

장치 삭제

장치 삭제 기능으로 장치를 목록에서 삭제할 수 있습니다. 삭제할 때 나타나는 옵션은 **장치와 보안 통신** 옵션의 활성화 여부에 따라 다릅니다.

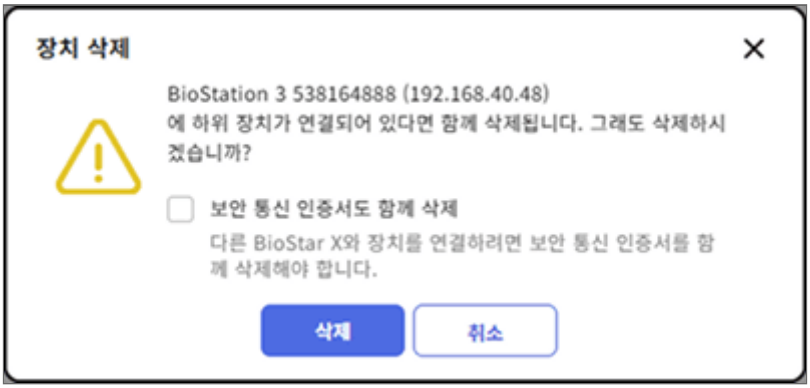
장치와 보안 통신을 사용하지 않을 때

장치와 보안 통신 옵션이 **사용 안 함** 상태이면 별도의 옵션 없이 선택한 장치를 삭제할 수 있습니다.



장치와 보안 통신을 사용할 때

장치와 보안 통신 옵션이 **사용** 상태이면 **장치 삭제** 창에 **보안 통신 인증서도 함께 삭제** 옵션이 나타납니다.



- **보안 통신 인증서도 함께 삭제** 옵션을 선택하지 않으면(기본값) 인증서는 삭제하지 않고 장치만 삭제합니다.
- **보안 통신 인증서도 함께 삭제** 옵션을 선택하면 장치에 저장된 보안 통신 인증서도 함께 삭제합니다. 삭제한 장치를 다른 **BioStar X** 서버에 연결하려면 이 옵션을 사용하세요.

> **주의**
> **BioStar X**와 연결이 끊긴 장치는 인증서를 삭제할 수 없으므로, **보안 통신 인증서도 함께 삭제** 옵션을 선택한 상태에서는 장치를 삭제할 수 없습니다. 장치를 삭제하려면 옵션을 선택 해제하거나, 장치를 먼저 재연결한 후 다시 시도하세요.

알아두기

- **장치와 보안 통신** 옵션을 사용 중인 상태에서 **보안 통신 인증서도 함께 삭제** 옵션을 선택하지 않고 장치를 삭제하면 장치에 인증서가 남습니다. 이후 **장치와 보안 통신** 옵션을 **사용 안 함**으로 변경하고, 해당 장치를 다시 **BioStar X**에 등록하면 장치에 남은 인증서 때문에 연결되지 않습니다. 기본 인증서를 사용하고 있다면 **장치와 보안 통신** 옵션을 다시 **사용**으로 변경하세요.
- 선택한 장치가 모두 슬레이브 장치이거나 보안 통신을 지원하지 않는 장치라면 **보안 통신 인증서도 함께 삭제** 옵션 없이 장치를 삭제할 수 있습니다.
- **보안 통신 인증서도 함께 삭제** 옵션은 **장치와 보안 통신** 옵션을 활성화했을 때만 표시됩니다. 자세한 내용은 시스템 보안 강화하기를 참고하세요.

장치 설정 내보내기/가져오기

한 장치의 설정을 파일로 내보낸 후 같은 모델의 다른 장치에 그대로 가져와 적용할 수 있습니다. 여러 대의 장치에 같은 설정을 반복해서 입력하는 대신, 설정을 마친 장치 한 대의 설정 파일을 만들어 나머지 장치에 적용하세요.

알아두기

- 같은 모델이란 장치의 세부 모델명과 파트 넘버(예: XPD2-XXX에서 XXX 부분)까지 모두 일치하는 장치를 의미합니다.
- 장치 설정 내보내기/가져오기 기능은 장치 설정에 대한 전체 권한이 있는 관리자가 사용할 수 있습니다. 관리자 권한 설정에 대한 자세한 내용은 운영 권한 관리하기를 참고하세요.

장치 설정 내보내기

장치 한 대의 설정을 파일로 내려받는 방법은 아래와 같습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 설정을 내보낼 장치의 체크박스를 클릭하세요. 한 개의 장치만 선택할 수 있습니다.
4. 장치 목록 상단에서 ••• → **장치 설정 내보내기**를 클릭하세요.



5. 다운로드 창이 나타나면 설정 파일을 로컬에 저장하세요.

주의

다음에 해당하는 장치는 설정을 내보낼 수 없습니다.

- **BioStar X**와 연결이 끊겼거나 응답 시간이 초과된 장치
- 가상 장치(Virtual Device)
- RS-485 통신 모드가 없는 장치(예: Wiegand 장치, IO 모듈, Door Interface, Door 모듈, Secure 모듈, OSDP Antenna/Reader)

알아두기

- 장치를 한 개도 선택하지 않거나 두 개 이상 선택한 상태에서는 이 기능을 실행할 수 없습니다.
- 파일 이름은 모델명, 장치 ID, RS-485 통신 모드(Master/Default/Slave), 내보낸 날짜 순서로 자동 지정됩니다. 날짜는 **설정** → **시스템** → **기본 설정**에서 지정한 날짜 형식을 따릅니다.

  예를 들어 모델명이 BS3-DB, 장치 ID가 538001234, 시리얼 통신 모드가 **마스터**, 내보낸 날짜가 2026년 6월 23일인 장치는 `BS3-DB_538001234_Master_20260623.json` 형태의 파일로 저장됩니다.

내보내기에 제외되는 설정

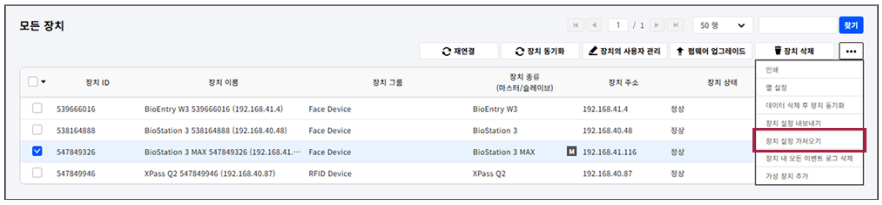
아래 설정은 장치마다 고유해야 하거나, 장치에만 저장되어 있거나, 인증 정보와 같은 민감한 정보이므로 내보내기 파일에 포함되지 않습니다.

- 장치 고유 설정: 장치 이름, 장치 그룹, 유/무선 네트워크 설정, 서버 연결 설정, OSDP 식별자, 작업 조건 및 동작
- 장치에만 저장되어 있어 다른 장치로 옮길 수 없는 설정: 화면/소리의 언어 리소스, 홈 화면, 소리, 시리얼 통신의 SCB 키, BioStation 3 Max에 추가한 영상 설정
- 인증 정보 및 민감 정보: IP 인터폰과 RTSP의 사용자 이름 및 비밀번호, 마스터 관리자 설정, 2단계 인증 옵션

장치 설정 가져오기

내보낸 설정 파일을 같은 모델의 장치 한 대 이상에 적용하는 방법은 아래와 같습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 설정을 적용할 장치의 체크박스를 클릭하세요. 한 개 이상의 장치를 선택할 수 있습니다.
4. 장치 목록 상단에서 ••• → **장치 설정 가져오기**를 클릭하세요.



5. 웹 브라우저의 열기 창이 나타나면 로컬에 저장한 설정 파일을 선택하세요.
6. 장치 설정 가져오기 결과 메시지가 나타나면 내용을 확인하고, **확인** 버튼을 클릭하세요.

주의

시스템은 다른 사이트나 서버에서 만든 설정 파일도 출처를 확인하거나 경고 없이 정상 파일로 받아들입니다. 가져올 파일이 신뢰할 수 있는 출처에서 만들어졌는지 확인하세요.

알아두기

장치를 한 개도 선택하지 않은 상태에서는 이 기능을 실행할 수 없습니다.

가져오기를 실행하면 설정을 적용하기 전에 시스템이 다음 항목을 차례로 검사합니다. 검사 중 하나라도 조건에 맞지 않으면 설정을 적용하지

않고 사유를 안내합니다.

- 선택한 장치들의 모델명(파트 넘버 포함)이 모두 같은지
- 선택한 장치들과 파일의 RS-485 통신 모드가 모두 같은지
- 파일에 저장된 모델명(파트 넘버 포함)이 선택한 장치들의 모델명(파트 넘버 포함)과 같은지
- 선택한 장치 중에 가상 장치(Virtual Device)가 있는지

검사를 통과하면 시스템은 내보내기에 제외되는 설정을 제외한 나머지 설정을 선택한 모든 장치에 적용합니다.

알아두기

- 특정 기능을 지원하지 않는 장치에서 내보낸 파일을 지원하는 장치로 가져오면, 해당 기능은 꺼진 상태로 적용되어 대상 장치에서 미리 켜둔 옵션이 꺼집니다. 반대로 기능을 지원하는 장치에서 내보낸 파일을 지원하지 않는 장치로 가져오면, 해당 기능은 적용되지 않고 나머지 설정만 적용됩니다. 두 경우 모두 가져오기 실패로 처리되지 않으며, 실패 목록에도 포함되지 않습니다.
- 장치 라이선스가 있어야 동작하는 설정은 해당 라이선스가 적용되지 않은 장치에는 적용되지 않습니다. 반대로 라이선스가 적용되지 않은 장치에서 내보낸 파일을 라이선스가 적용된 장치로 가져오면, 해당 설정은 꺼진 상태로 적용되어 대상 장치에서 미리 켜둔 옵션이 꺼집니다. 두 경우 모두 가져오기 실패로 처리되지 않으며, 실패 목록에도 포함되지 않습니다.
- 모든 장치에 성공적으로 적용되면 성공 메시지가 나타납니다. 일부 또는 전체 장치에 적용하지 못하면 실패한 장치 수와 함께 실패 목록을 CSV 파일로 내려받을 수 있는 안내 메시지가 나타납니다. 이 파일에는 실패한 장치의 ID, 이름, 실패 사유(장치와의 연결 끊김, 또는 출입 그룹이 설정되어 있어 전체 출입 권한을 줄 수 없는 경우)가 담겨 있습니다.

  > *예를 들어, 2026년 6월 23일 15시 45분 30초에 실행한 가져오기가 실패했다면 파일 이름은 `Device_Template_Import_Error_20260623T154530.csv` 형태가 됩니다.*

- CoreStation 장치도 적용 대상에 포함됩니다.
- 장치 설정 내보내기와 가져오기 작업 내역은 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 확인할 수 있습니다.

장치 내 이벤트 로그 삭제

장치에 저장된 이벤트 로그를 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 원하는 장치의 체크박스를 클릭하세요. 1개 이상의 장치를 선택할 수 있습니다.
4. 장치 목록 상단에서 ••• → **장치 내 모든 이벤트 로그 삭제** 버튼을 클릭하세요.



5. 경고 메시지 창이 나타나면 내용을 확인하고 **계속** 버튼을 클릭하세요.

장치 이벤트 로그 삭제 작업이 완료되면 팝업 메시지가 나타납니다. 대상 장치 수, 성공 장치 수, 실패 장치 수를 확인할 수 있습니다.

주의

장치에서 삭제된 이벤트 로그는 복구할 수 없으며, 서버에서 다시 장치로 전송할 수 없습니다. 삭제를 진행하기 전에 장치 이벤트 로그가 서버에 저장되었는지 확인하세요. 또한 선택한 장치에 슬레이브 또는 가상 장치, Wiegand 장치가 포함되어 있다면, 해당 장치는 로그를 저장하지 않아 로그 삭제 대상에서 제외됩니다.

알아두기

- 이 기능은 **전체 관리자** 권한을 가진 사용자만 사용할 수 있습니다.
- 장치의 이벤트 로그 삭제 이력은 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 확인할 수 있습니다.

추가 기능

장치 목록을 인쇄하거나 열 설정을 변경하는 등의 추가 기능을 사용할 수 있습니다.

장치 목록 인쇄하기

장치 목록을 PDF 또는 SVG 파일 형식으로 저장해 인쇄할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록 상단의 ••• 버튼을 클릭하세요.
4. 팝업 메뉴에서 **인쇄**를 클릭하세요.
5. **인쇄 옵션** 창이 나타나면 **파일포맷** 옵션에서 원하는 포맷을 선택하고 나머지 옵션을 설정하세요.



6. **인쇄** 버튼을 클릭하세요.

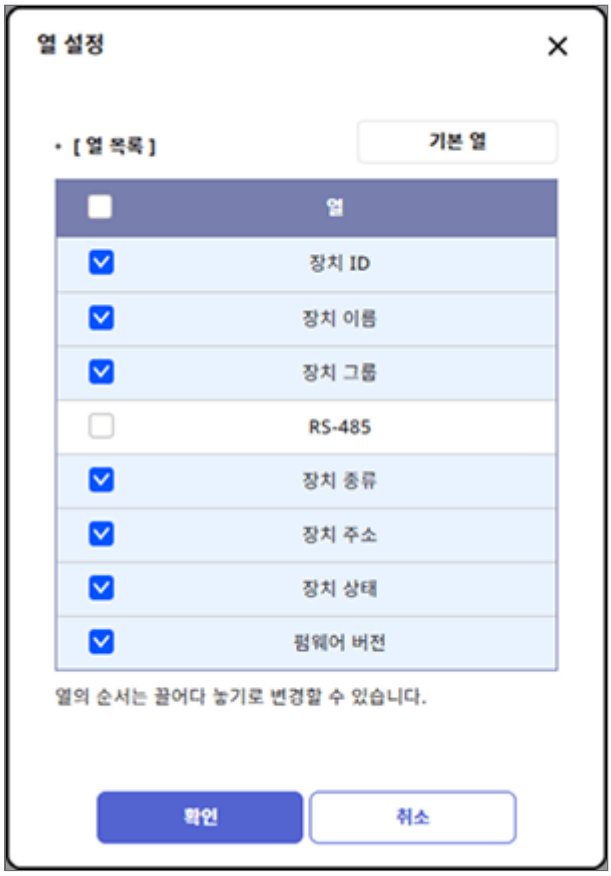
브라우저를 통해 열리는 PDF 또는 SVG 파일을 인쇄할 수 있습니다.

장치 목록 열(Column) 설정

장치 목록에서 표시되는 열(Column) 설정을 변경할 수 있습니다. 열 설정을 통해 표시할 열을 선택하거나 열의 순서를 변경할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록 상단의 ••• 버튼을 클릭하세요.
4. 팝업 메뉴에서 **열 설정**을 클릭하세요.
5. **열 설정** 창이 나타나면 원하는 열을 선택하거나 선택 해제하세요.



6. 열의 순서를 변경하려면 원하는 열을 클릭한 채로 드래그하여 위치를 변경하세요.
7. 설정을 저장하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

장치 설정하기

등록한 장치의 세부 기능을 설정하고 관리하는 방법을 안내합니다. 장치의 정보, 네트워크, 인증, 고급 설정 등의 세부 정보를 설정할 수 있습니다. 세부 정보는 RS-485 연결 방식이나 장치 종류에 따라 달라질 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 세부 정보를 설정하려는 장치를 클릭하세요.
4. 각 섹션의 세부 항목을 참고하여 장치 정보를 설정하세요.

- **정보**: 장치의 이름과 그룹, 표준 시간대, 하드웨어 및 펌웨어 버전을 확인하고 변경할 수 있습니다. 자세한 내용은 기본 정보 설정하기를 참고하세요.
- **네트워크**: 장치의 TCP/IP, RS-485, 서버 통신 등의 네트워크를 설정할 수 있습니다. 자세한 내용은 네트워크 설정하기를 참고하세요.
- **인증**: 장치의 사용자 인증과 관련한 옵션을 설정할 수 있습니다. 자세한 내용은 인증 설정하기를 참고하세요.
- **고급**: 마스터 관리자, 장치 관리자, 화면/소리, 작업 조건 및 동작 등을 설정할 수 있습니다. 자세한 내용은 고급 설정하기를 참고하세요.
- **열화상 및 마스크** / **마스크**: 열화상 카메라 및 마스크 사용에 대한 세부 항목을 설정할 수 있습니다. 자세한 내용은 열화상 및 마스크 설정하기를 참고하세요.
- **IP 인터폰**: IP 인터폰 사용에 대한 세부 항목을 설정할 수 있습니다. 자세한 내용은 IP 인터폰 설정하기를 참고하세요.
- **RTSP**: **Real Time Streaming Protocol**(RTSP) 스트리밍을 위한 세부 항목을 설정할 수 있습니다. 자세한 내용은 RTSP 설정하기를 참고하세요.

5. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

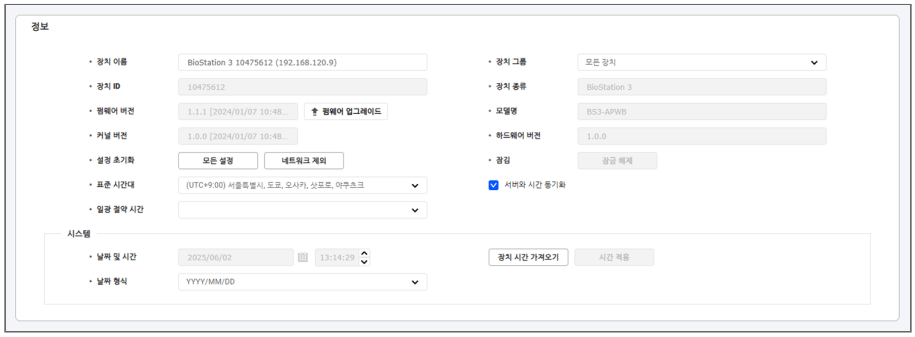
- 여러 개의 장치 정보를 한 번에 수정할 수도 있습니다. 두 개 이상의 장치를 선택하고 화면 오른쪽 상단의 **일괄 편집**을 클릭하세요.



- 선택한 장치 종류에 따라 **일괄 편집** 창에 표시되는 세부 항목이 다를 수 있습니다.
- 마스터 장치와 슬레이브 장치를 동시에 선택하고 일괄 편집을 클릭하면 **인증**과 **화면/소리** 항목의 일부만 변경할 수 있습니다.
- **인증 모드**는 모델명이 동일한 장치를 선택했을 때만 일괄 편집할 수 있습니다.

기본 정보 설정하기

정보 섹션에서는 장치의 기본 정보를 설정할 수 있습니다. 장치의 이름과 그룹, 표준 시간대, 하드웨어 및 펌웨어 버전 등을 확인할 수 있습니다. 장치의 이름과 그룹을 변경하거나 장치의 펌웨어를 업그레이드할 수 있습니다.



아래는 장치에 설정된 기본 정보로 사용자가 변경할 수 없는 항목입니다.

- **장치 ID**: 장치의 아이디를 확인할 수 있습니다.
- **장치 종류**: 장치의 종류를 확인할 수 있습니다.
- **모델명**: 장치의 모델 이름을 확인할 수 있습니다.
- **커널 버전**: 장치의 커널 버전을 확인할 수 있습니다.
- **하드웨어 버전**: 장치의 하드웨어 버전을 확인할 수 있습니다.

> **알아두기**
> 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

장치 이름 변경

기본 설정된 장치의 이름을 변경할 수 있습니다. **장치 이름** 항목에서 원하는 장치 이름을 입력하세요. 장치 이름은 최대 48자까지 입력할 수 있습니다. 장치 이름은 장치 목록에서 장치를 식별하는 데 사용합니다.

장치 그룹 변경

장치가 속한 그룹을 변경할 수 있습니다. **장치 그룹** 항목에서 원하는 장치 그룹을 선택하세요.

> **알아두기**
> 새로운 장치 그룹을 생성하거나 그룹 이름 변경 및 삭제에 대한 자세한 내용은 장치 그룹 관리하기를 참고하세요.

펌웨어 업그레이드

장치의 펌웨어 버전을 확인하려면 **펌웨어 버전** 항목에서 확인할 수 있습니다. 펌웨어를 업그레이드하려면 **펌웨어 업그레이드** 버튼을 클릭하세요.

> **알아두기**
> 장치의 펌웨어 업그레이드에 대한 자세한 내용은 펌웨어 업그레이드하기를 참고하세요.

장치의 날짜 및 시간 설정

아래의 옵션을 통해 장치의 날짜와 시간을 설정할 수 있습니다.

- **표준 시간대**: 장치가 위치한 표준 시간대를 선택할 수 있습니다.
- **서버와 시간 동기화**: 장치의 시간 정보를 BioStar X 서버의 시간과 동기화할 수 있습니다.
- **일광 절약 시간**: 사용자가 설정한 일광 절약 시간을 장치에 적용할 수 있습니다. 새 일광 절약 시간을 추가하려면 일광 절약 시간 설정하기를 참고하세요.
- **날짜 및 시간**: 장치의 날짜와 시간을 수동으로 설정할 수 있습니다. 날짜와 시간을 모두 설정했다면 **시간 적용** 버튼을 클릭하세요.

  > 이 기능은 **서버와 시간 동기화** 옵션을 선택하지 않았을 때 사용할 수 있습니다.

- **날짜 형식**: 장치에 표시되는 날짜 형식을 선택할 수 있습니다.
- **장치 시간 가져오기**: 장치에 설정된 시간을 불러올 수 있습니다.

> **주의**
> 설정한 날짜와 시간은 이벤트 로그와 실시간에 로그에 기록됩니다. 장치의 날짜와 시간이 정확하지 않으면 로그 기록이 잘못될 수 있습니다.

잠금 장치 해제

작업 조건 및 동작에 의해 장치가 잠겼을 때 **잠김** 항목의 **잠금 해제** 버튼을 클릭하세요. 장치의 잠금을 해제할 수 있습니다.

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

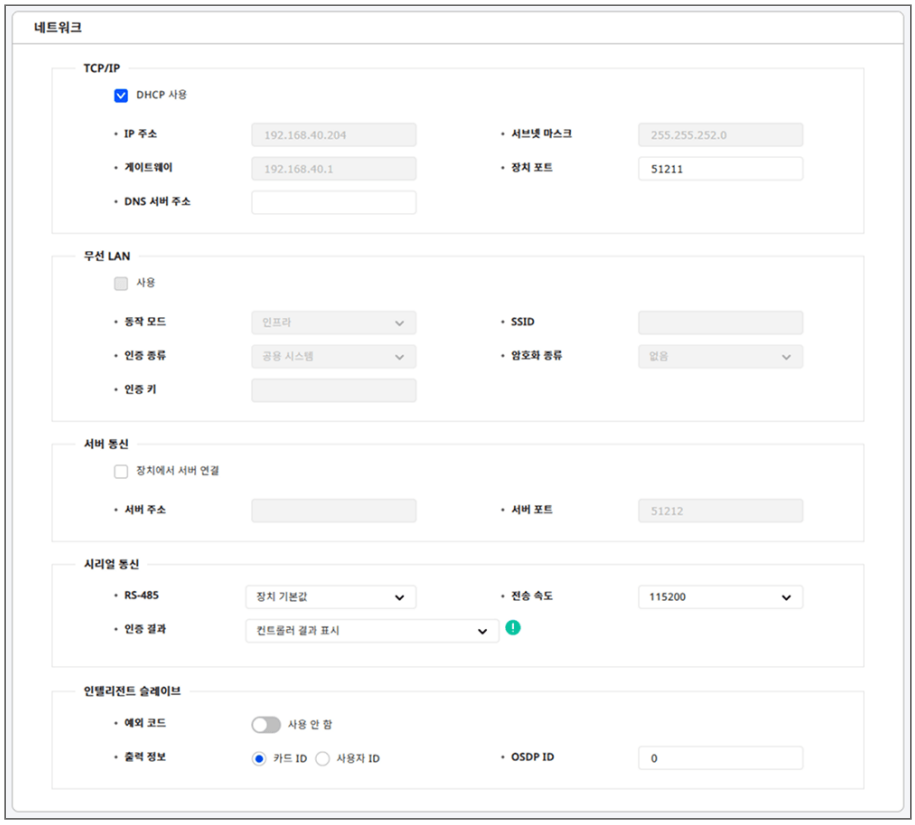
장치 초기화

장치의 설정을 초기화하려면 **설정 초기화** 항목에서 아래 기능 중 하나를 선택하세요.

- **모든 설정**: 장치의 모든 설정을 초기화합니다.
- **네트워크 제외**: 네트워크 설정은 유지하고 나머지 설정을 초기화합니다.

네트워크 설정하기

등록한 장치의 네트워크 설정을 안내합니다. **네트워크** 섹션에서는 장치의 TCP/IP, RS-485, 서버 통신 등의 네트워크를 설정할 수 있습니다.



알아두기

- 장치 종류에 따라 설정할 수 있는 네트워크 옵션은 다를 수 있습니다.
- 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

TCP/IP 설정

TCP/IP 그룹에서는 장치의 IP 주소를 설정할 수 있습니다.

알아두기

장치를 등록할 때 IP 주소 설정에 대한 자세한 내용은 장치 등록하기를 참고하세요.

유동 IP 설정

장치가 유동 IP를 사용하도록 설정하려면 **DHCP 사용** 옵션의 체크박스를 클릭하세요. 장치가 DHCP 서버로부터 IP 주소를 자동으로 할당받습니다. 이 경우 장치의 IP 주소는 변경될 수 있습니다.

고정 IP 설정

장치의 IP 주소를 고정으로 설정하려면 **DHCP 사용** 옵션의 체크박스 선택을 해제하세요. 아래의 세부 항목에 장치의 네트워크 정보를 입력할 수 있습니다.

- **IP 주소**: 장치의 IP 주소를 입력하세요. IP 주소는 `xxx.xxx.xxx.xxx` 형식으로 입력할 수 있으며 각 옥텟은 0~255 범위의 숫자로만 입력할 수 있습니다.
- **서브넷 마스크**: 장치의 서브넷 마스크를 입력하세요.

- **게이트웨이**: 장치의 게이트웨이 주소를 입력하세요.
- **장치 포트**: 장치의 포트 번호를 입력하세요.
- **DNS 서버 주소**: 장치의 DNS 서버 주소를 입력하세요.

▼ DNS 서버 주소를 입력할 수 있는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.0.0 이상
- FaceStation F2 펌웨어 1.0.0 이상
- XPass 2 펌웨어 1.0.0 이상
- FaceLite 펌웨어 1.0.0 이상
- BioLite N2 펌웨어 1.0.0 이상
- FaceStation 2 펌웨어 1.0.0 이상
- BioStation L2 펌웨어 1.0.0 이상
- BioStation A2 펌웨어 1.0.0 이상
- BioStation 2 펌웨어 1.2.0 이상

무선 랜 설정

무선 LAN 그룹에서는 장치의 무선 랜 설정을 켜거나 끌 수 있습니다. 세부 항목은 장치에서 설정할 수 있으며, 자세한 내용은 장치의 사용자 가이드를 참고하세요.

알아두기

무선 랜 설정을 지원하는 장치는 아래를 참고하세요.

- BioStation 2
- BioStation A2
- FaceStation 2
- BioStation 3

서버 통신 설정

서버 통신 그룹에서는 **BioStar X** 서버와 통신하는 방식을 설정할 수 있습니다.

- **장치에서 서버 연결**: 이 옵션을 선택하면 장치에서 연결할 **BioStar X** 서버의 IP 주소와 포트 번호를 입력할 수 있습니다.
- **서버 주소**: **BioStar X** 서버의 IP 주소 또는 도메인 주소를 입력하세요.
- **서버 포트**: **BioStar X** 서버의 포트 번호를 입력하세요.

팁

이 기능은 **BioStar X** 서버의 IP 주소가 변경될 때 유용하게 사용할 수 있습니다. **BioStar X** 서버의 IP 주소를 변경하기 전에 여러 개의 장치에서 이 옵션을 미리 설정하면 장치가 자동으로 변경된 IP 주소로 연결합니다.

▼ 서버 주소에 도메인을 입력할 수 있는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.0.0 이상
- FaceStation F2 펌웨어 1.0.0 이상
- XPass 2 펌웨어 1.0.0 이상
- FaceLite 펌웨어 1.0.0 이상
- BioLite N2 펌웨어 1.0.0 이상
- BioEntry P2 펌웨어 1.0.0 이상
- FaceStation 2 펌웨어 1.0.0 이상
- BioEntry W2 펌웨어 1.0.0 이상
- BioStation L2 펌웨어 1.0.0 이상
- BioStation A2 펌웨어 1.0.0 이상
- BioStation 2 펌웨어 1.2.0 이상

시리얼 통신 설정

시리얼 통신 그룹에서는 RS-485 통신 방식으로 연결된 장치의 모드와 전송 속도, 표시할 인증 결과를 설정할 수 있습니다.

- **RS-485**: RS-485 모드를 설정하세요.
- **전송 속도**: RS-485 통신 속도를 설정하세요.
- **인증 결과**: 타사 컨트롤러와 연동해 장치를 사용할 때 장치 화면에 표시할 인증 결과를 선택하세요.
  - **컨트롤러 결과 표시**: 타사 컨트롤러의 인증 결과를 장치에 표시할 수 있습니다.
  - **장치 인증 결과 표시**: 장치의 인증 결과를 표시할 수 있습니다.

알아두기

인증 결과 옵션은 **RS-485** 옵션을 **슬레이브** 또는 **장치 기본값**을 선택했을 때 활성화됩니다.

인텔리전트 슬레이브 설정

인텔리전트 슬레이브 그룹에서는 슈프리마 장치와 타사 컨트롤러를 연결한 환경에서 사용자가 지문으로 인증했을 때, 인증 결과를 Open Supervised Device Protocol(OSDP) 카드 데이터로 전송하여 다수의 1:1 또는 1:N 매칭을 지원합니다.

- **예외 코드**: 인텔리전트 슬레이브를 사용할 때 인증 실패 등 예외 상황이 발생하면, 예외 코드를 10진수(0~18446744073709551615)

또는 16진수(0~FFFFFFFFFFFFFFFF) 형식으로 입력해 정확한 로그를 남길 수 있습니다. 16진수는 숫자 또는 영문자로 입력할 수 있습니다.



- **출력 정보**: 인증을 성공할 때 카드 아이디 또는 사용자 아이디를 출력할 수 있습니다.
- **OSDP ID**: 장치의 OSDP 주소를 입력하세요. 0~126 사이의 숫자로 입력할 수 있습니다.

알아두기

- **예외 코드**의 데이터 크기는 최대 8바이트까지 입력할 수 있습니다.
- **인텔리전트 슬레이브** 옵션은 **RS-485** 옵션을 **장치 기본값**을 선택했을 때 활성화됩니다.

▼ 인텔리전트 슬레이브 옵션을 지원하는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.1.0 이상
- FaceStation F2 펌웨어 1.1.2 이상
- XPass 2 펌웨어 1.2.3 이상
- BioLite N2 펌웨어 1.4.1 이상
- BioEntry P2 펌웨어 1.4.1 이상
- BioEntry W2 펌웨어 1.6.3 이상
- BioStation L2 펌웨어 1.6.1 이상

인증 설정하기

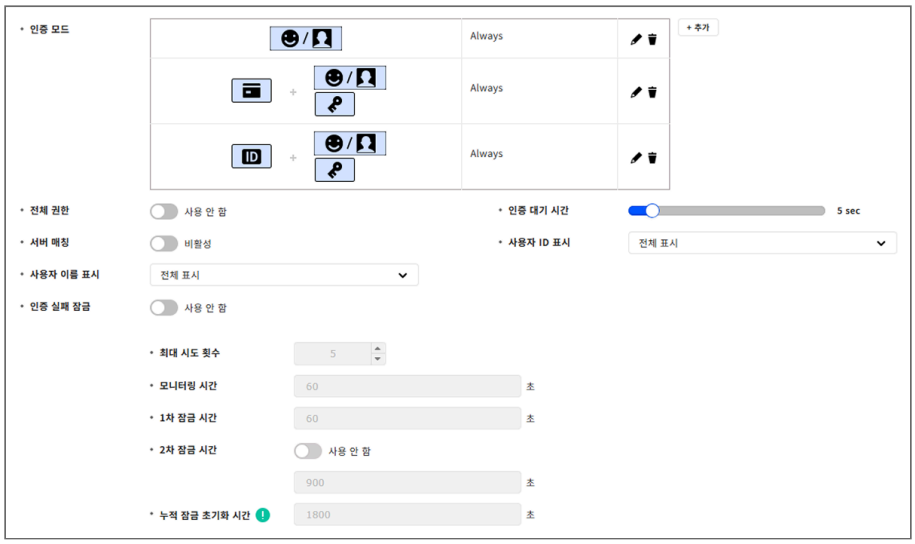
장치의 사용자 인증과 관련된 다양한 설정 방법을 안내합니다. **인증** 섹션에서는 인증 방식과 장치에서 지원하는 주요 인증 옵션을 단계별로 확인할 수 있습니다. 설정을 변경하면 실제 장치에 적용되는 점을 유의하고, 각 옵션의 기능과 주의 사항을 참고하여 환경에 맞는 인증 정책을 구성하세요.

알아두기

- 장치 종류에 따라 설정할 수 있는 네트워크 옵션은 다를 수 있습니다.
- 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

인증 방법 설정

장치의 인증 모드 및 권한, 서버 매칭, 인증 대기 시간을 설정할 수 있습니다.



- **인증 모드**: 한 개 이상의 크리덴셜을 조합해 장치의 인증 모드를 설정하세요. 자세한 내용은 인증 모드 추가를 참고하세요.
  - 추가한 인증 모드를 수정하려면 ✎ 버튼을 클릭하세요.
  - 추가한 인증 모드를 삭제하려면 🗑 버튼을 클릭하세요.
- **전체 권한**: 장치에 등록된 사용자에게 출입 그룹 설정 없이 모든 출입 권한을 부여할 수 있습니다.

> **알아두기**
> 이 옵션을 **사용**으로 설정하면 **출입 등급** 및 **층 등급**에 장치를 등록할 수 없습니다.

- **인증 대기 시간**: **인증 모드** 옵션에서 여러가지 크리덴셜을 조합해 사용할 때 두 번째 크리덴셜을 인증하는 대기 시간입니다. 지정한 시간 내에 크리덴셜을 인증하지 않으면 인증에 실패합니다.
- **서버 매칭**
  - **활성**: 서버 매칭 기능을 활성화합니다. **BioStar X**를 설치한 서버에 저장된 사용자 정보를 이용하여 인증을 수행하는 서버 매칭 기능을 설정하세요.
  - **비활성**: 서버 매칭 기능을 비활성화합니다. 이 경우 장치에 등록된 사용자 정보로 인증을 수행합니다.

▼ 서버 매칭 기능 지원 장치 및 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.0.0 이상
- FaceStation F2 펌웨어 1.0.0 이상
- XPass 2 펌웨어 1.0.0 이상
- BioLite N2 펌웨어 1.0.0 이상

  - XPass D2 펌웨어 1.0.0 이상
  - BioEntry P2 펌웨어 1.0.0 이상
  - FaceStation 2 펌웨어 1.4.0 이상
  - BioEntry W2 펌웨어 1.0.0 이상
  - BioStation L2 펌웨어 1.0.0 이상
  - BioStation A2 펌웨어 1.0.0 이상
  - BioStation 2 펌웨어 1.2.0 이상
  - CoreStation 펌웨어 1.0.0 이상
  - FaceLite는 서버 매칭 기능을 지원하지 않습니다.
  - BioStation 3, BioEntry W3, FaceStation F2 장치는 얼굴 인증을 위한 서버 매칭을 사용할 수 없습니다.

- **얼굴 인식 레벨**: 사용자가 인증할 때 장치에 내장된 카메라로 얼굴을 인식하는 알고리즘 단계를 설정하세요.
  - **보통**: 사람 팔 길이 정도의 거리에서 얼굴을 검출할 수 있습니다.
  - **높음**: 사람 팔 길이보다 더 가까이 다가가야 얼굴을 검출할 수 있습니다.
  - **사용 안 함**: 얼굴 인식 기능을 사용하지 않습니다.

> **알아두기**
> 이 옵션은 BioStation A2 모델에서 지원합니다.

- **사용자 ID 표시**: 인증을 성공할 때 장치에 표시되는 사용자 아이디를 표시하거나 숨길 수 있습니다.
  - **전체 표시** / **첫 문자만 표시** / **표시하지 않기**
- **사용자 이름 표시**: 인증을 성공할 때 장치에 표시되는 사용자 이름을 표시하거나 숨길 수 있습니다.
  - **전체 표시** / **첫 문자만 표시** / **표시하지 않기**
- **인증 실패 잠금**: 짧은 시간 안에 인증을 반복해서 실패하면 장치를 일정 시간 동안 잠가 무차별 대입 공격을 차단합니다. 이 옵션을 **사용**으로 설정하면 아래 항목을 설정할 수 있습니다. 기본값은 **사용 안 함**입니다.
  - **최대 시도 횟수**: 장치를 잠그기까지 허용하는 인증 실패 횟수를 3~15회 사이로 설정하세요. 기본값은 5회입니다.
  - **모니터링 시간**: 인증 실패 횟수를 누적해서 계산하는 시간을 30~300초 사이로 설정하세요. 기본값은 60초입니다.
  - **1차 잠금 시간**: 인증 실패 횟수가 **최대 시도 횟수**에 도달했을 때 장치를 잠그는 시간을 30~900초 사이로 설정하세요. 기본값은 60초이며 반드시 값을 입력해야 합니다.
  - **2차 잠금 시간**: 1차 잠금이 해제된 뒤에도 인증 실패가 반복될 때 적용하는 2차 잠금 시간입니다. 이 옵션을 **사용**으로 설정하면 900~3,600초 사이의 값을 입력할 수 있습니다. 기본값은 900초입니다.

    > 이 옵션을 **사용 안 함**으로 설정하면 2차 잠금 없이 1차 잠금만 반복해서 적용합니다.

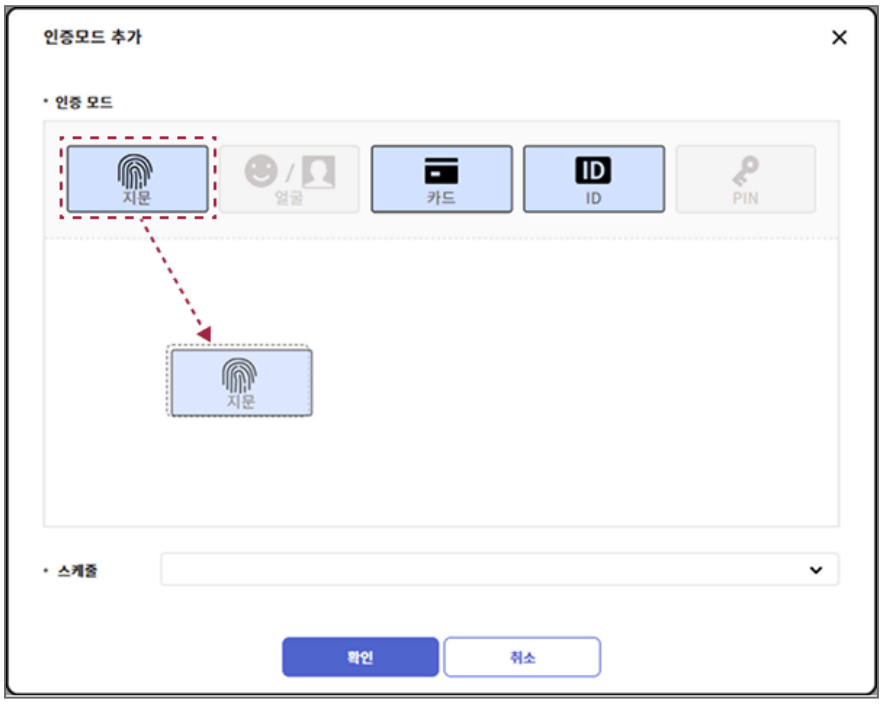
  - **누적 잠금 초기화 시간**: 마지막 인증 실패 후 이 시간 안에 추가 실패가 없으면 누적 실패 횟수를 초기화합니다. 600~3,600초 사이로 설정하세요. 기본값은 1,800초입니다.

> **알아두기**
>
> – 장치가 현재 잠금 상태일 때 **인증 실패 잠금**을 **사용 안 함**으로 변경하고 저장하면 잠금이 즉시 해제됩니다. 단, **2차 잠금 시간**을 **사용 안 함**로 변경하고 저장하면 잠금이 해제되지 않습니다.
>
> – **인증 실패 잠금** 옵션은 BioStation 3 펌웨어 1.5.0 이상에서 지원합니다.

인증 모드 추가

인증 모드 옵션에서 장치의 인증 모드를 설정하세요. 지문, 아이디, 카드, PIN, 얼굴과 같은 크리덴셜을 조합해 인증 모드를 설정할 수 있습니다.

1. **인증 모드** 옵션에서 ＋ **추가** 버튼을 클릭하세요.
2. **인증모드 추가** 창이 나타나면 원하는 인증 모드를 가운데 영역으로 드래그하세요.



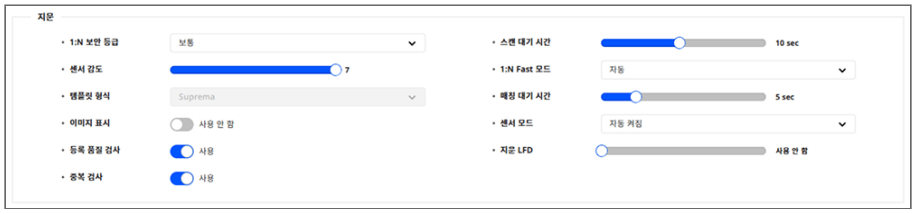
원하는 인증 모드는 최대 5개까지 추가할 수 있습니다.

3. **스케줄** 옵션에서 원하는 항목을 선택하세요.
4. 모든 설정을 완료했다면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> **스케줄** 옵션에서 원하는 스케줄이 없다면 ＋ **새 스케줄 추가**를 클릭하세요. 새 스케줄을 추가할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

지문 인증 설정

지문 그룹에서는 장치의 지문 인증에 대한 세부 사항을 설정할 수 있습니다.

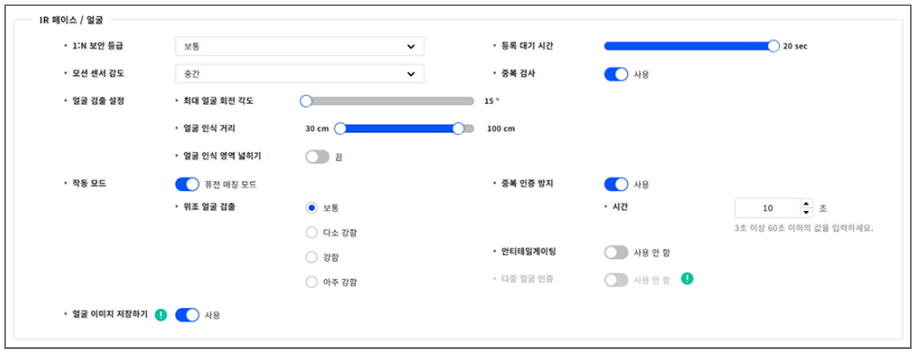


- **1:N 보안 등급**: 지문을 인증할 때 사용할 보안 등급을 설정하세요. 보안 등급이 높을수록 본인 거부율(FRR)이 높아지지만 타인 수락율(FAR)이 낮아집니다.
- **스캔 대기 시간**: 지문 스캔 대기 시간을 설정하세요. 설정한 시간 동안 지문을 스캔하지 못하면 인증을 실패합니다.
- **센서 감도**: 지문 인식 센서의 민감도를 설정하세요. 센서 감도를 높여 정밀한 지문 정보를 얻으려면 센서 감도를 높게 설정하세요.
- **1:N Fast 모드**: 지문 인증 속도를 설정하세요. **자동**을 선택하면 장치에 등록된 총 지문 템플릿에 따라 인증 속도를 설정합니다.
- **템플릿 형식**: 설정된 지문 템플릿 형식을 확인할 수 있습니다.
- **매칭 대기 시간**: 지문 매칭 대기 시간을 설정하세요. 설정한 시간 동안 인증을 완료하지 못하면 인증을 실패합니다.
- **이미지 표시**: 지문을 인증할 때 화면에 지문 이미지를 표시할 수 있습니다.
- **센서 모드**: 지문 센서의 작동 모드를 설정하세요.
  - **자동 켜짐**: 지문 센서가 사용자의 손가락을 인식하여 센서가 켜집니다.
  - **항상 켜짐**: 지문 센서가 항상 켜져 있습니다.
- **등록 품질 검사**: 높은 품질의 지문 정보를 저장하기 위해 스캔한 지문의 품질을 검사할 수 있습니다. **사용**으로 설정하면 지문 품질이 낮을 경우 사용자에게 알려주어 지문을 올바르게 스캔하도록 도와줍니다.
- **지문 LFD**: 위조 지문 검사 등급을 설정하세요. 위조 지문 검사 등급이 높을수록 실제 사람 지문에 대한 거부율도 높아질 수 있습니다.
- **중복 검사**: 지문을 등록할 때 중복 등록 여부를 검사할 수 있습니다.

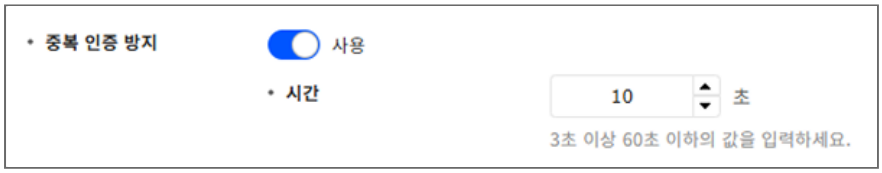
> **알아두기**
>
> - 장치 종류에 따라 설정할 수 있는 옵션은 다를 수 있습니다.
> - 지문 인증 설정에서 **템플릿 형식** 옵션을 변경하면 이전에 저장된 모든 지문은 사용할 수 없습니다. 사용자의 지문을 등록하기 전에 반드시 **템플릿 형식** 옵션에서 템플릿을 선택하세요.
> - **이미지 표시** 옵션은 BioStation 3 Max(BS3M-ODB, BS3M-OAPB), X-Station 2(XS2-ODPB, XS2-OAPB), FaceStation F2(FSF2-ODB), BioLite N2, BioStation L2, BioStation A2, BioStation 2 모델에서 지원합니다.
> - **지문 LFD** 옵션은 BioStation 3 Max(BS3M-ODB, BS3M-OAPB), X-Station 2(XS2-ODPB, XS2-OAPB), FaceStation F2(FSF2-ODB), BioLite N2, BioStation L2, BioStation A2, BioEntry W2 모델에서 지원합니다.

얼굴 인증 설정

IR 페이스 / 얼굴 또는 **얼굴** 그룹에서는 장치의 얼굴 인증에 대한 세부 사항을 설정할 수 있습니다.



- **1:N 보안 등급**: 얼굴을 인증할 때 사용할 보안 등급을 설정하세요. 보안 등급이 높을수록 본인 거부율(FRR)이 높아지지만 타인 수락율(FAR)이 낮아집니다.
- **등록 대기 시간**: 사용자 얼굴을 등록할 때 설정한 시간 동안 얼굴을 등록하지 못하면 얼굴 등록이 취소됩니다.
- **모션 센서 감도**: 장치 주변의 움직임을 감지하는 감도를 설정하세요.
- **주변 밝기**: 장치 주변의 밝기를 감지하여 IR LED 세기를 조절할 수 있습니다.
- **위조 얼굴 등록 검사 강화**: 위조 얼굴 검사 등급을 설정하세요. 위조 얼굴 등록 검사 강화 등급이 높을수록 실제 얼굴에 대한 거부율도 높아질 수 있습니다.
- **조명 밝기**: 장치 조명의 밝기를 수동으로 조절할 수 있습니다. **보통** 또는 **높음**으로 밝기를 설정하거나 **사용 안함**을 선택해 조명을 끌 수 있습니다.
- **빠른 등록**: 빠른 얼굴 등록 사용 여부를 설정하세요.
  - **사용**: 얼굴 등록 절차를 1단계로 설정합니다.
  - **사용 안 함**: 얼굴 등록 절차를 3단계로 설정합니다. 고품질의 얼굴 템플릿을 등록하려면 **사용 안 함**으로 설정하세요.
- **중복 검사**: 얼굴을 등록할 때 중복 등록 여부를 검사할 수 있습니다.
- **얼굴 검출 설정**: 얼굴을 인증할 때 사용자의 얼굴을 인식하는 환경을 설정하세요.
  - **최대 얼굴 회전 각도**: 허용 가능한 얼굴의 최대 회전 각도를 설정하세요.
  - **얼굴 인식 거리**: 얼굴을 인식하는 최소, 최대 거리를 설정하세요.
  - **얼굴 인식 영역 넓히기**: 카메라 영상 전체에서 얼굴을 인식하게 하려면 **켬**으로 설정하세요.
- **작동 모드**: 얼굴을 인증할 때 장치의 작동 모드를 설정하세요.
  - **퓨전 매칭 모드**: 비주얼 및 적외선 매칭을 모두 수행하여 얼굴 인증의 정확도를 높일 수 있습니다.
  - **빠른 인증 모드**: 장치의 인증 범위 안에서 사용자가 걸어가면서도 얼굴을 인증할 수 있도록 빠르게 인증을 수행할 수 있습니다.
- **위조 얼굴 검출**: 사진 등의 위조 얼굴을 이용한 사용자 인증을 방지할 수 있습니다. **작동 모드** 옵션을 **퓨전 매칭 모드**로 설정하면 활성화됩니다.
- **얼굴 이미지 저장하기**: 얼굴의 실제 이미지와 특징 정보만 추출한 템플릿을 저장합니다. 실제 이미지를 저장하지 않으려면 이 설정을 비활성화하세요.
- **중복 인증 방지**: 같은 사용자의 얼굴이 짧은 시간 안에 다시 감지될 때 중복으로 인증되지 않도록 설정하세요. **사용**으로 설정하면 **시간**을 3~60초 사이로 설정할 수 있습니다.



> 이 설정은 **안티테일게이팅**과 **다중 얼굴 인증** 중 어느 옵션을 사용하더라도 공통 적용됩니다.

- **안티테일게이팅**: 장치 카메라 촬영 범위 안에서 2명 이상의 얼굴이 동시에 감지되면 동반 출입으로 판단하여 인증을 중단합니다.
- **다중 얼굴 인증**: 장치 카메라 촬영 범위 안에 있는 여러 사용자의 얼굴을 순서대로 인증합니다.

> – 이 옵션을 사용하려면 별도의 장치 라이선스가 필요합니다. 라이선스가 없는 장치에서는 옵션을 사용으로 설정할 수 없습니다. 자세한 내용은 장치 라이선스를 참고하세요.
> – 이 옵션을 **사용**으로 설정하면 장치에 설정된 **인증 모드**와 관계없이 얼굴 인증 전용으로 동작합니다.
> – 이 옵션을 사용하는 장치에서는 **근태 관리**와 **서버 개인 메시지** 기능을 사용할 수 없습니다.

알아두기

- 장치 종류에 따라 설정할 수 있는 옵션은 다를 수 있습니다.
- **주변 밝기**, **위조 얼굴 등록 검사 강화**, **빠른 등록** 옵션은 FaceStation 2, FaceLite 모델에서 지원합니다.
- **조명 밝기** 옵션은 FaceStation F2 펌웨어 1.1.0 이상 모델에서 지원합니다.
- **얼굴 검출 설정**, **작동 모드** 옵션은 BioStation 3 Max, BioStation 3, FaceStation F2 모델에서 지원합니다.
- **안티테일게이팅**과 **다중 얼굴 인증**은 동시에 **사용**으로 설정할 수 없습니다. 한 옵션을 **사용**으로 설정하면 다른 옵션은 자동으로 **사용 안 함**으로 전환됩니다.
- **중복 인증 방지**와 **다중 얼굴 인증** 옵션은 마스터 장치에서만 설정할 수 있습니다. **안티테일게이팅** 옵션은 마스터, 슬레이브 장치에서 각각 설정할 수 있습니다.
- **중복 인증 방지**, **안티테일게이팅**, **다중 얼굴 인증** 옵션은 장치 종류 및 펌웨어 버전에 따라 지원 여부가 다를 수 있습니다.
  – BioStation 3 펌웨어 1.5.0 이상

QR/바코드 설정

QR/바코드 그룹에서는 장치의 QR/바코드 인증에 대한 세부 사항을 설정할 수 있습니다.



- **카메라로 QR/Barcode 인증** / **QR/바코드 사용**: 장치의 카메라를 통한 QR/바코드 인증 사용 여부를 설정하세요.
- **카메라 대기 시간** / **스캔 대기 시간**: 카메라의 스캔 대기 시간을 설정하세요. 설정한 시간 동안 QR/바코드를 스캔하지 못하면 인증이 실패됩니다.
- **카드를 QR로 인증하기**: 사용자에게 발급한 CSN 카드 또는 Wiegand 카드와 동일한 데이터의 QR코드로 인증할 수 있도록 설정하세요.
- **모션 센서 감도**: 움직임을 감지하여 카메라가 스캔을 시작하는 감도를 설정하세요.
- **스캐너로 QR/Barcode 인증**: 장치의 스캐너를 통한 QR/바코드 인증 사용 여부를 설정하세요.

- **스캐너 대기 시간**: 스캔 대기 시간을 설정하세요. 설정한 시간 동안 QR/바코드를 스캔하지 못하면 인증이 실패됩니다.
- **LED 조명**: QR 코드를 인증할 때 장치의 LED 조명 사용 여부를 설정하세요.

> **알아두기**
>
> - **카메라로 QR/Barcode 인증** 옵션을 사용하려면 별도의 장치 라이선스가 필요합니다. 자세한 내용은 장치 라이선스를 참고하세요.
> - **카메라로 QR/Barcode 인증**, **카메라 대기 시간**, **카드를 QR로 인증하기**, **모션 센서 감도** 옵션을 지원하는 장치는 아래를 참고하세요.
>   - BioStation 3 Max 펌웨어 1.0.0 이상
>   - BioStation 3 펌웨어 1.1.0 이상
>   - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) 펌웨어 1.2.0 이상
>   - X-Station 2 (XS2-QDPB, XS2-QAPB) 펌웨어 1.4.1 이상
> - **스캐너로 QR/Barcode 인증** 및 **스캐너 대기 시간** 옵션을 지원하는 장치는 아래를 참고하세요.
>   - X-Station 2 (XS2-QDPB, XS2-QAPB)
> - **QR/바코드 사용** 및 **스캔 대기 시간**, **LED 조명** 옵션을 지원하는 장치는 아래를 참고하세요.
>   - XPass Q2 펌웨어 1.0.0 이상

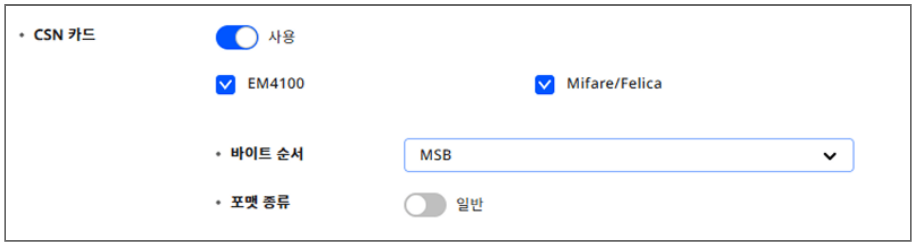
카드 인증 설정

카드 종류 그룹에서는 장치에서 사용할 카드 종류를 설정할 수 있습니다.

> **알아두기**
>
> 장치에서 지원하는 카드 종류만 **카드 종류** 그룹에 표시됩니다.

CSN 카드

CSN 카드 및 포맷 종류를 선택하고 바이트 순서를 설정할 수 있습니다.



- **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.
- **포맷 종류**
  - **일반**: 카드의 일련 번호(CSN)를 별도의 변환 없이 모두 읽어서 표현합니다.
  - **Wiegand**: 사용자가 정의한 Wiegand 형식에 따라 카드 일련 번호(CSN)를 변환하여 표현합니다. 새로운 Wiegand 형식을 설정하려면 Wiegand 카드 형식 설정하기를 참고하세요.

Wiegand 카드

Wiegand 카드 종류를 선택하고 Wiegand 형식을 설정할 수 있습니다. **Wiegand 형식** 옵션에서 사용할 Wiegand 형식을 선택하세요.



> **알아두기**
> 새로운 Wiegand 형식을 설정하려면 Wiegand 카드 형식 설정하기를 참고하세요.

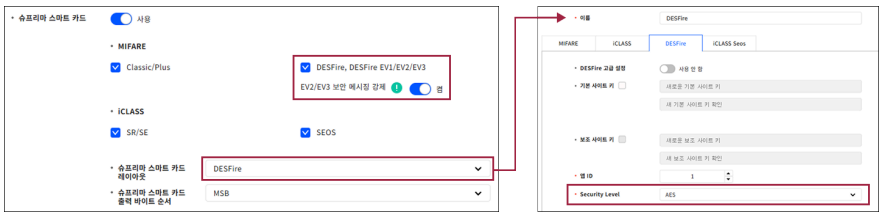
슈프리마 스마트 카드

슈프리마 스마트 카드 종류를 선택하고 카드 레이아웃과 바이트 순서를 설정할 수 있습니다.



- **EV2/EV3 보안 메시징 강제**: 이 옵션을 **켬**으로 설정하면 EV2 보안 메시징을 지원하는 카드(DESFire EV2/EV3)로만 인증할 수 있습니다. EV2 보안 메시징을 지원하지 않는 DESFire EV1 카드의 인증은 거부됩니다.

  이 옵션은 **DESFire, DESFire EV1/EV2/EV3** 항목을 선택하고, 선택한 **슈프리마 스마트 카드**의 **암호화 종류**가 **AES**일 때 활성화됩니다. **슈프리마 스마트 카드**를 사용하지 않으면 이 옵션은 **끔** 상태로 표시됩니다.



> – **슈프리마 스마트 카드**와 **커스텀 스마트 카드**는 설정값을 공유하고 있습니다. 둘 중 하나라도 사용 중이라면 어느 한쪽의 값을 변경할 때 확인 메시지 창이 나타납니다. 메시지 창에서 **확인** 버튼을 클릭하면 두 옵션이 함께 변경됩니다. 한쪽에서 스마트 카드를 사용하지 않으면 확인 메시지 없이 값을 변경할 수 있습니다.
> – 보안 메시징은 DESFire EV2 및 EV3 카드에서만 사용할 수 있습니다. 사용하려면 DESFire를 활성화하고 카드 레이아웃의 암호화 종류를 AES로 설정하세요.
> – 장치가 EV2 보안 메시징 기능을 지원하지 않으면 **EV2/EV3 보안 메시징 강제** 옵션은 표시되지 않습니다.
> – 여러 장치를 선택해 **일괄 편집**으로 이 옵션을 설정할 수도 있습니다. EV2 보안 메시징을 지원하지 않는 장치는 일괄 편집 시 자동 제외됩니다.

- **슈프리마 스마트 카드 레이아웃**: 슈프리마 스마트 카드 레이아웃을 선택하세요. 새로운 스마트 카드 레이아웃을 설정하려면 스마트 카드 형식 설정하기를 참고하세요.
- **슈프리마 스마트 카드 출력 바이트 순서**
  - **MSB**: 카드 데이터를 큰 바이트 단위에서 작은 바이트 단위 순서로 처리합니다.
  - **LSB**: 카드 데이터를 작은 바이트 단위에서 큰 바이트 단위 순서로 처리합니다.

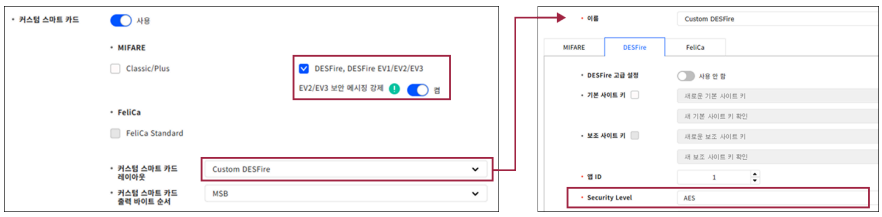
커스텀 스마트 카드

타사에서 발급한 커스텀 스마트 카드의 종류를 선택하고 카드 레이아웃과 바이트 순서를 설정할 수 있습니다.



- **EV2/EV3 보안 메시징 강제**: 이 옵션을 **켬**으로 설정하면 EV2 보안 메시징을 지원하는 카드(DESFire EV2/EV3)로만 인증할 수 있습니다. EV2 보안 메시징을 지원하지 않는 DESFire EV1 카드의 인증은 거부됩니다.

  이 옵션은 **DESFire, DESFire EV1/EV2/EV3** 항목을 선택하고, 선택한 **커스텀 스마트 카드**의 **암호화 종류**가 **AES**일 때 활성화됩니다. **커스텀 스마트 카드**를 사용하지 않으면 이 옵션은 **끔** 상태로 표시됩니다.



> – **슈프리마 스마트 카드**와 **커스텀 스마트 카드**는 설정값을 공유하고 있습니다. 둘 중 하나라도 사용 중이라면 어느 한쪽의 값을 변경할 때 확인 메시지 창이 나타납니다. 메시지 창에서 **확인** 버튼을 클릭하면 두 옵션이 함께 변경됩니다. 한쪽에서 스마트 카드를 사용하지 않으면 확인 메시지 없이 값을 변경할 수 있습니다.
> – 보안 메시징은 DESFire EV2 및 EV3 카드에서만 사용할 수 있습니다. 사용하려면 DESFire를 활성화하고 카드 레이아웃의 암호화 종류를 AES로 설정하세요.
> – 장치가 EV2 보안 메시징 기능을 지원하지 않으면 **EV2/EV3 보안 메시징 강제** 옵션은 표시되지 않습니다.
> – 여러 장치를 선택해 **일괄 편집**으로 이 옵션을 설정할 수도 있습니다. EV2 보안 메시징을 지원하지 않는 장치는 일괄 편집 시 자동 제외됩니다.

- **커스텀 스마트 카드 레이아웃**: 커스텀 스마트 카드 레이아웃을 선택하세요. 새로운 스마트 카드 레이아웃을 설정하려면 스마트 카드 형식 설정하기를 참고하세요.
- **커스텀 스마트 카드 출력 바이트 순서**
  - **MSB**: 카드 데이터를 큰 바이트 단위에서 작은 바이트 단위 순서로 처리합니다.
  - **LSB**: 카드 데이터를 작은 바이트 단위에서 큰 바이트 단위 순서로 처리합니다.

▼ 커스텀 스마트 카드를 지원하는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.3.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 2a 펌웨어 1.1.0 이상
- BioStation 3 펌웨어 1.3.0 이상
- X-Station 2 펌웨어 1.3.0 이상
- BioLite N2 펌웨어 1.6.2 이상
- XPass D2 펌웨어 1.7.1 이상
- BioEntry P2 펌웨어 1.5.1 이상
- BioEntry W2 펌웨어 1.8.0 이상

CSN 모바일

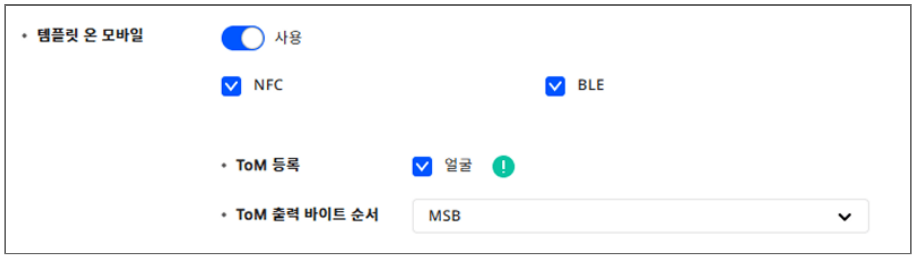
모바일 카드의 인식 방법을 설정할 수 있습니다.



- **NFC**: 모바일 기기에서 NFC 통신을 통해 모바일 카드를 인식합니다.
- **BLE**: 저전력 블루투스(Bluetooth Low Energy, BLE) 통신를 통해 모바일 카드를 인식합니다.

템플릿 온 모바일

템플릿 온 모바일의 인식 방법과 사용자가 장치에서 직접 등록할 바이오메트릭을 지정하고 바이트 순서를 설정할 수 있습니다.



- **ToM 출력 바이트 순서**
  - **MSB**: 카드 데이터를 큰 바이트 단위에서 작은 바이트 단위 순서로 처리합니다.
  - **LSB**: 카드 데이터를 작은 바이트 단위에서 큰 바이트 단위 순서로 처리합니다.

▼ 템플릿 온 모바일을 지원하는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- BioEntry W3 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.2.0 이상

PIN 인증 설정

PIN 그룹에서는 장치의 PIN 인증을 위해 **스크램블 키패드** 옵션을 켜거나 끌 수 있습니다.



> **알아두기**
> **스크램블 키패드** 옵션은 LCD 화면을 통한 사용자 인터페이스가 지원되는 슈프리마 제품에서만 사용할 수 있습니다.

고급 설정하기

고급 섹션에서 설정할 수 있는 항목에 대해 안내합니다. 마스터 관리자, 관리자 권한 관리, 근태 이벤트, 화면 및 소리, 작업 조건 및 동작, 이미지 로그, Wiegand, 보안 탬퍼 등 다양한 고급 기능의 설정 방법과 각 옵션의 의미를 확인할 수 있습니다. 환경에 맞는 설정을 적용해 효율적으로 장치를 관리하세요.

> **알아두기**
> - 장치 종류에 따라 설정할 수 있는 네트워크 옵션은 다를 수 있습니다.
> - 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

마스터 관리자 추가 CE향 제품

마스터 관리자 기능은 장치의 전체 관리자 권한을 강화하여, 장치의 보안을 향상시키고 무단 접근 및 설정 변경을 방지하기 위한 기능입니다. 새 장치는 이 기능을 통해 반드시 마스터 관리자를 등록해야 하며, 등록된 마스터 관리자만 관리자 메뉴에 진입하여 설정을 변경할 수 있습니다.

고급 → **관리자**의 **마스터 관리자** 메뉴에서 원하는 크리덴셜 2종류를 선택하여 등록하세요.



마스터 관리자에 등록할 수 있는 크리덴셜은 다음과 같습니다.

크리덴셜 종류	등록 가능 개수	세부 조건
카드	최대 4개	CSN, Wiegand 타입만 지원하며, 동일 타입 내 중복 등록할 수 없습니다.
얼굴	최대 2개	동종 알고리즘 탑재 장치에서만 등록할 수 있습니다.
지문	최대 2개	-

크리덴셜 종류	등록 가능 개수	세부 조건
PIN	1개	최소 8자리 이상의 숫자를 입력할 수 있습니다.

- 등록한 크리덴셜을 변경하려면 해당 크리덴셜 오른쪽에 ✎ 버튼을 클릭하세요.
- 등록한 크리덴셜을 삭제하려면 해당 크리덴셜 오른쪽에 🗑 버튼을 클릭하세요.

주의

이 기능은 **LCD 화면을 통한 사용자 인터페이스가 지원되는 슈프리마 제품** 중 **CE향 제품**에서만 사용할 수 있습니다. 지원하는 장치 및 펌웨어 버전에 대한 자세한 내용은 마스터 관리자 설정 방법 안내를 참고하세요.

등록 조건

- 최소 두 종류 이상의 크리덴셜을 등록해야 합니다.
- 마스터 관리자를 지원하는 펌웨어 업그레이드 장치 모두 동일한 조건이 적용됩니다.
- 장치가 지원하는 모든 크리덴셜을 인증 수단으로 사용할 수 있습니다.

알아두기

- 이 기능은 LCD 화면을 통한 사용자 인터페이스가 지원되는 슈프리마 제품에서만 사용할 수 있습니다.
- 펌웨어를 업그레이드한 기존 장치는 **BioStar X**의 장치 설정에 **마스터 관리자** 메뉴가 나타나지 않습니다.
- **마스터 관리자** 설정을 제공하지 않는 장치 중 일부는(예: 펌웨어 업그레이드로 해당 기능이 추가된 장치) **2단계 인증** 옵션을 통해 전체 관리자의 권한을 강화할 수 있습니다. 장치 종류에 따라 **2단계 인증** 옵션 자체가 표시되지 않을 수 있습니다.
- 마스터 관리자의 크리덴셜은 장치 내 별도로 저장되어, 일반 사용자의 PIN과는 독립적으로 관리됩니다. 따라서 사용자 PIN을 변경하거나 삭제해도 마스터 관리자 크리덴셜에는 영향을 미치지 않습니다.

2단계 인증 설정

마스터 관리자를 지원하지 않는 글로벌 장치에서 펌웨어를 업그레이드한 경우, **2단계 인증** 옵션을 통해 전체 관리자의 권한을 강화하여 장치의 보안을 향상시킬 수 있습니다.



2단계 인증 옵션을 **사용**으로 설정하면, 장치의 전체 관리자 인증 시 두 종류 이상의 크리덴셜을 사용해야 합니다. 예를 들어, 카드와 PIN을 모두 등록한 경우, 전체 관리자 인증 시 카드 스캔과 PIN 입력을 모두 해야만 인증을 성공할 수 있습니다.

알아두기

- 모든 관리자에게 2종류 이상의 크리덴셜이 등록되어 있지 않을 때 활성화 시 설정이 실패하며 에러 메시지가 표시됩니다. 모든 관리자에게 2종류 이상의 크리덴셜을 등록한 다음 다시 시도하세요.



- 장치에 따라 **2단계 인증** 옵션이 화면에 표시되지 않으면서도 이전에 활성화한 설정이 유지되는 경우가 있습니다. 이때는 **BioStar X**에서 비활성화할 수 없으므로 슈프리마 기술 지원팀(CS@suprema.co.kr)에 문의하세요.

주의

장치에 전체 관리자가 설정되어 있지 않은 경우 다음과 같은 팝업 메시지가 나타납니다. **고급** → **관리자**에서 모든 권한에 관리자를 추가하세요.

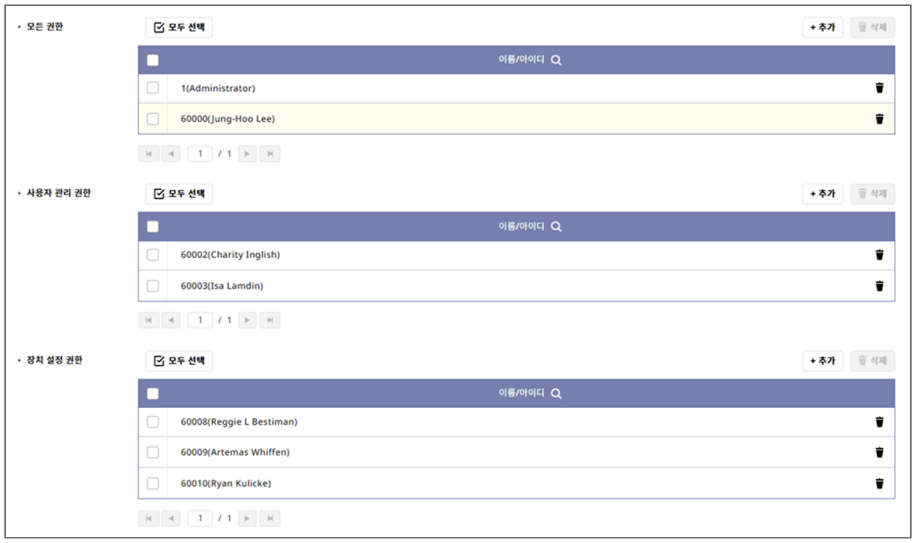


경고

2단계 인증을 활성화한 후 모든 관리자의 크리덴셜을 2종 미만으로 삭제하면, **BioStar X**에 연결할 수 없는 상황일 때 장치에서 관리자 메뉴에 접근할 수 없게 됩니다. 따라서 관리자 크리덴셜을 삭제할 때는 각별한 주의가 필요합니다.

관리자 추가

관리자 그룹에서는 장치의 관리자를 등급별로 관리할 수 있습니다.



등급별 관리자를 추가하려면 **+ 추가** 버튼을 클릭하세요. 사용자 목록이 나타나면 원하는 사용자를 선택하세요. 사용자 목록에서 🔍 버튼을 클릭하면 원하는 사용자를 검색할 수도 있습니다.

각 등급별 사용 권한은 아래를 참고하세요.

등급	사용자 정보 관리	장치 설정
모든 권한	✔	✔
사용자 관리 권한	✔	✕
장치 설정 권한	✕	✔

알아두기

- 관리자는 최대 1,000명까지 추가해 관리할 수 있습니다. 추가할 수 있는 관리자 수는 장치 펌웨어 버전에 따라 달라질 수 있습니다.
- 등록한 사용자를 검색하려면 **이름/아이디**에서 🔍 버튼을 클릭하세요.
- **장치 설정**은 장치의 화면 및 소리, 네트워크, RS-485 등의 설정을 변경할 수 있습니다.
- 관리자를 삭제하려면 해당 관리자의 오른쪽에 🗑 버튼을 클릭하세요.
- 각 장치에 설정된 관리자는 **BioStar X** 권한에 영향을 미치지 않습니다.
- 마스터 관리자를 지원하는 장치(**CE향 제품**)에 장치 관리자로 등록한 사용자의 PIN이 8자리 미만이면, 해당 사용자의 PIN을 8자리 이상으로 다시 등록해야 합니다. PIN 등록에 대한 자세한 내용은 PIN 등록하기를 참고하세요.
- **장치 설정 권한** 권한이 부여된 사용자의 PIN을 4자리로 변경하려면 먼저 모든 장치의 관리자 권한에서 제외해야 합니다.

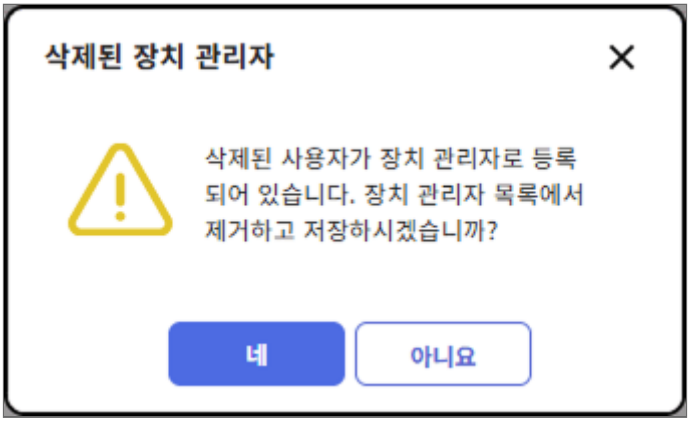
주의

장치 관리자로 설정하려는 사용자에게 등록된 크리덴셜이 2종류 미만이면 에러 메시지가 표시됩니다. 모든 장치 관리자에게 2종류 이상의 크리덴셜을 등록한 후 다시 시도하세요.



삭제된 사용자의 관리자 등록 처리

장치에 등록된 관리자 중 **BioStar X**에서 이미 삭제된 사용자가 있는 경우, 장치 설정을 저장하기 위해 화면 가장 아래의 **확인** 버튼을 클릭하면 다음과 같은 팝업이 나타납니다.



- **네**: 삭제된 사용자를 관리자 목록에서 제거하고 저장합니다.
- **아니요**: 저장을 취소합니다.

근태 관리

근태 관리 그룹에서는 장치의 근태 이벤트 이름을 변경하거나 근태 모드를 설정할 수 있습니다.



- **근태 모드**: 근태 이벤트 등록 방법을 설정하세요.
  - **사용 안 함**: 근태 이벤트를 기록할 수 없습니다.
  - **수동 변경**: 사용자가 인증할 때 원하는 근태 이벤트를 선택할 수 있습니다.

  - **자동 변경**: 설정한 스케줄에 따라 근태 이벤트가 자동으로 변경됩니다. 근태 이벤트에 적용할 스케줄을 선택할 수 있습니다.
  - **수동 고정**: 사용자가 마지막으로 사용한 근태 이벤트를 계속 사용할 수 있습니다.
  - **고정**: 선택한 근태 이벤트만 사용할 수 있습니다. 고정으로 사용할 근태 이벤트를 선택하세요.
- **근태 등록 필요**: 사용자가 인증할 때 반드시 근태 이벤트를 등록하도록 설정하세요.

> 이 옵션은 **근태 모드** 옵션이 **수동 변경**으로 설정되었을 때 사용할 수 있습니다.

- **근태 이벤트**: 근태 이벤트의 이름을 수정하거나 **근태 모드** 옵션을 **자동 변경**으로 설정했을 때 사용되는 스케줄을 추가할 수 있습니다.
  - **근태 키**: 근태 등록에 사용할 수 있는 키 목록입니다.
  - **라벨**: **근태 키**에 따른 근태 이벤트 이름을 변경할 수 있습니다.
  - **스케줄**: **근태 모드** 옵션을 **자동 변경**으로 설정하면 자동으로 변경할 스케줄을 설정할 수 있습니다.



> **알아두기**
>
> - LCD 화면이 없는 장치는 근태 모드를 **고정**과 **자동 변경**으로 설정할 수 있으며, 고정된 근태 이벤트를 등록하거나 미리 설정된 스케줄에 따라 변경되는 근태 이벤트를 등록할 수 있습니다. 지원하는 장치 종류는 XPass Q2, XPass 2, XPass D2, BioEntry P2, BioEntry W2입니다.
> - 새 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
> - 장치에서 **다중 얼굴 인증** 옵션을 **사용**으로 설정하면 이 장치는 근태 관리에 사용할 수 없습니다. **다중 얼굴 인증**에 대한 자세한 내용은 인증 설정하기를 참고하세요.

화면 및 소리 설정

장치의 화면이나 소리에 대한 설정을 변경할 수 있습니다. 장치에 따라 설정할 수 있는 옵션은 다를 수 있습니다.

▼ XPass 2, XPass D2, BioEntry P2, BioEntry W2

- **소리**: 소리를 켜거나 끌 수 있습니다.
- **LED 및 버저**: LED나 버저를 작동할 이벤트 항목을 선택하고 설정하세요.
- **키패드 백라이트**: 키패드 백라이트를 켜거나 끌 수 있습니다. 이 옵션을 활성화하면 키패드 후면의 조명이 켜집니다. 어두운 환경에서도 키를 쉽게 식별할 수 있습니다.

> **키패드 백라이트** 옵션은 XPass D2 하드웨어 V02M, 펌웨어 1.7.1 버전 이상에서 사용할 수 있습니다.

▼ **FaceLite, BioLite N2, BioStation L2, BioStation 2**

- **언어**: 장치의 화면에 표시할 언어를 설정하세요. 장치에 언어 리소스 파일을 전송하려면 **리소스 업데이트** 버튼을 클릭하세요.
- **장치 음량**: 장치에서 발생하는 기본 소리 크기를 설정하세요.
- **메뉴 표시 시간**: 메뉴 화면에서 대기 화면으로 변경되는 시간을 설정하세요.
- **테마**: 장치의 홈 화면 스타일을 변경하세요.
- **백라이트 시간**: 화면 조명이 자동으로 꺼지는 시간을 설정하세요.
- **메시지 표시 시간**: 메시지가 자동으로 사라지는 시간을 설정하세요.
- **음성 안내**: 알림음 대신 음성 안내를 사용할 수 있습니다.
- **배경화면**: 장치의 홈 화면 배경에 표시할 항목을 설정하세요.
  - **로고**: 사용자가 등록한 이미지를 장치의 홈 화면에 표시할 수 있습니다. 원하는 이미지를 등록하려면 **추가** 버튼을 클릭하세요.
  - **공지사항**: 관리자가 입력한 내용을 홈 화면에 표시할 수 있습니다.
  - **슬라이드쇼**: 사용자가 등록한 최대 10장의 이미지를 슬라이드쇼로 홈 화면에 표시할 수 있습니다. 원하는 이미지를 등록하려면 **추가** 버튼을 클릭하세요.

> ⓘ
> - 변경 사항을 장치에 실시간으로 반영하려면 **업데이트** 버튼을 클릭하세요.
> - 배경화면 종류를 변경할 경우 **업데이트** 버튼을 클릭해도 장치에 적용되지 않습니다. 화면 가장 아래에 **확인** 버튼을 클릭하세요.
> - **공지사항**, **슬라이드쇼** 옵션은 BioStation 2 모델에서 지원합니다.

- **소리**: 장치에서 시작, 인증 성공, 인증 실패 이벤트가 발생할 때 재생할 효과음을 설정하세요. 파일 크기가 500Kb 이하인 **.wav* 파일을 선택하세요. **찾아보기** 버튼을 클릭하세요.

> ⓘ 변경 사항을 장치에 실시간으로 반영하려면 **업데이트** 버튼을 클릭하세요.

▼ **BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, BioStation A2**

- **언어**: 장치의 화면에 표시할 언어를 설정하세요. 장치에 언어 리소스 파일을 전송하려면 **리소스 업데이트** 버튼을 클릭하세요.
- **장치 음량**: 장치에서 발생하는 기본 소리 크기를 설정하세요.
- **IP 인터폰 스피커 음량**: IP 인터폰 기능을 사용할 때 장치에서 출력되는 소리 크기를 설정하세요.
- **IP 인터폰 마이크 음량**: IP 인터폰 기능을 사용할 때 장치로 입력되는 소리 크기를 설정하세요.
- **메뉴 표시 시간**: 메뉴 화면에서 대기 화면으로 변경되는 시간을 설정하세요.
- **백라이트 시간**: 화면 조명이 자동으로 꺼지는 시간을 설정하세요.
- **메시지 표시 시간**: 메시지가 자동으로 사라지는 시간을 설정하세요.
- **서버 개인 메시지**: 사용자가 인증할 때 화면에 표시할 개인 메시지 사용 여부를 설정할 수 있습니다.

> ⓘ 장치에서 **다중 얼굴 인증** 옵션을 **사용**으로 설정하면 이 옵션을 사용할 수 없습니다. **다중 얼굴 인증**에 대한 자세한 내용은 인증 설정하기를 참고하세요.

- **음성 안내**: 알림음 대신 음성 안내를 사용할 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. 원하는 이미지를 등록하려면 **추가** 버튼을 클릭하세요.
- **공지사항**: 관리자가 입력한 내용을 홈 화면에 표시할 수 있습니다.

> - 변경 사항을 장치에 실시간으로 반영하려면 **업데이트** 버튼을 클릭하세요.
> - 배경화면 종류를 변경할 경우 **업데이트** 버튼을 클릭해도 장치에 적용되지 않습니다. 화면 가장 아래에 **확인** 버튼을 클릭하세요.
> - 홈 화면을 **로고**로 설정하고 **슬라이드쇼**로 설정하면 최대 10장의 이미지를 슬라이드쇼로 홈 화면에 표시할 수 있습니다. 원하는 이미지를 등록하려면 **추가** 버튼을 클릭하세요.

- **소리**: 장치에서 시작, 인증 성공, 인증 실패 이벤트가 발생할 때 재생할 효과음을 설정하세요. 파일 크기가 500Kb 이하인 **.wav* 파일을 선택하세요. **찾아보기** 버튼을 클릭하세요.

> 변경 사항을 장치에 실시간으로 반영하려면 **업데이트** 버튼을 클릭하세요.

- **기본 대기 화면**: 장치를 사용하지 않는 시간에 화면에 표시할 대기 화면을 선택할 수 있습니다.
  - **화면보호기**: 화면 보호기를 대기 화면으로 표시합니다.
  - **홈 화면**: **홈 화면** 옵션에서 선택한 항목을 표시합니다.

> - 이 옵션은 BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2 모델에서 지원합니다.
> - **동영상 재생** 옵션에 대한 자세한 내용은 대기 화면에 동영상 재생을 참고하세요.

▼ XPass Q2

LED 및 버저: LED나 버저를 작동할 이벤트 항목을 선택하고 설정하세요.

대기 화면에 동영상 재생

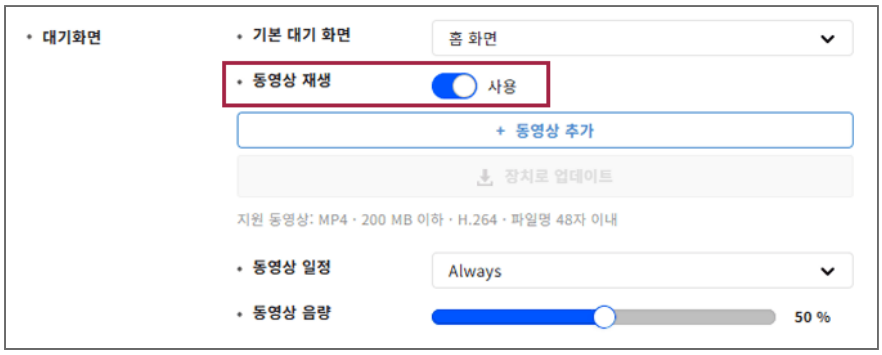
> 대기 화면에 동영상을 재생하는 기능은 **BioStation 3 Max** 펌웨어 1.1.0 이상에서 지원합니다. 동영상을 장치에 전송하기 전에 미리 준비하세요.

동영상 추가 및 장치 전송

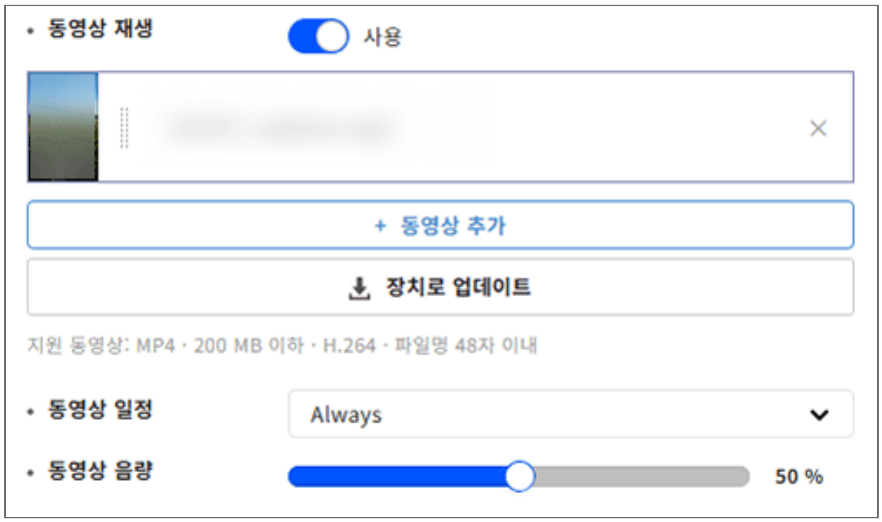
장치의 대기 화면에 원하는 콘텐츠를 재생할 수 있도록 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 BioStation 3 Max를 클릭하세요.
4. **고급** → **화면/소리** 섹션으로 이동하세요.

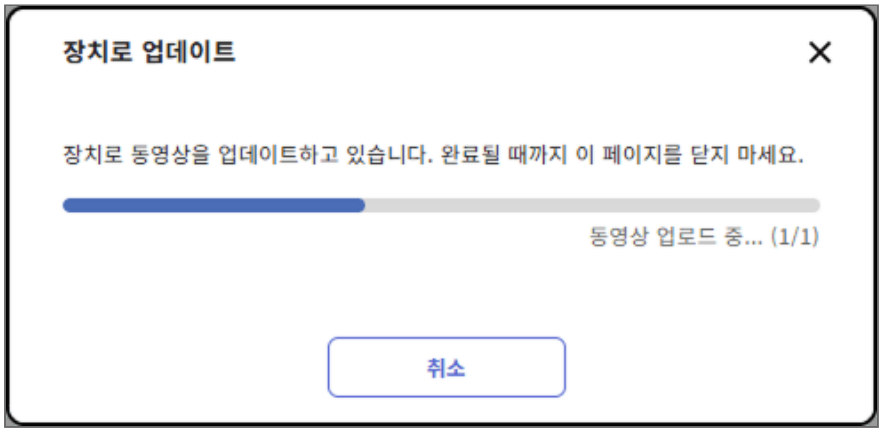
5. **대기화면** → **동영상 재생** 옵션을 **사용**으로 설정하세요.



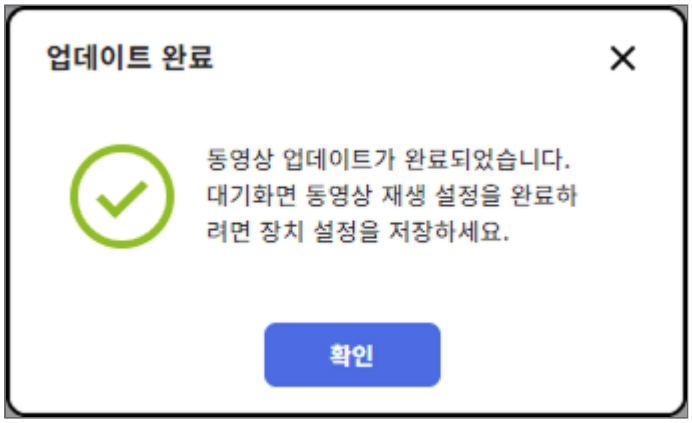
6. **동영상 추가** 버튼을 클릭하세요.
7. 로컬에 저장된 동영상을 선택하세요.
8. 동영상이 업로드되면 **동영상 일정**과 **동영상 음량**을 설정하세요.



9. 업로드한 동영상을 장치로 전송하려면 **장치로 업데이트** 버튼을 클릭하세요.
10. 업데이트 진행 팝업이 나타납니다. 업로드를 완료할 때까지 페이지를 닫지 마세요.



11. 업로드 완료 메시지가 나타나면 **확인** 버튼을 클릭하세요.



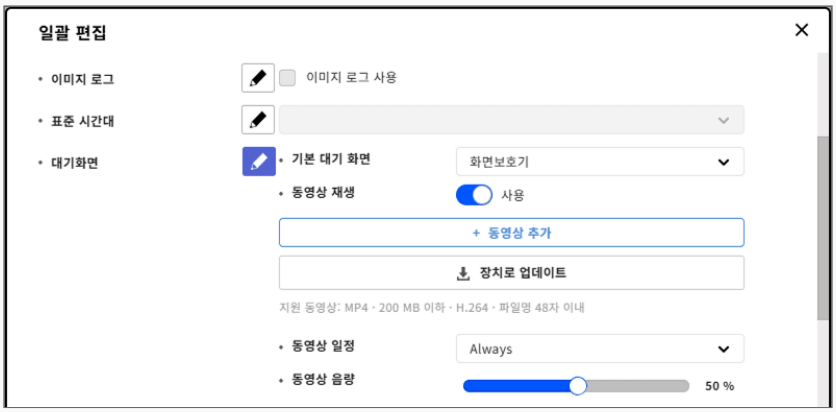
12. 변경 사항을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 동영상은 **동영상 일정** 옵션에서 지정한 스케줄에 따라 **동영상 재생**이 **사용**으로 설정되어 있고 동영상이 1개 이상 등록되어 있을 때만 재생됩니다. 이 조건을 만족하지 않는 스케줄에는 **기본 대기 화면**에서 선택한 화면이 표시됩니다.
- 지원하는 동영상 파일의 크기는 최대 200MB이며, 파일 포맷은 MP4(H.264)입니다.
- 동영상 파일명 길이는 최대 48자입니다. 파일명에는 마침표(`.`), 홑따옴표(`'`), 백틱(`` ` ``)과 같은 문자가 포함되면 추가할 수 없습니다.
- 동영상은 최대 3개까지 추가할 수 있습니다. 동영상이 3개까지 추가되었다면 **동영상 추가** 버튼은 비활성화됩니다.
- 장치가 슬레이브로 연결된 경우(RS-485로 연결된 경우)에는 동영상을 추가 또는 삭제, 전송할 수 없습니다.
  - 마스터 장치가 동영상 재생 기능을 지원하면 슬레이브 화면에는 마스터 장치에 등록된 동영상 목록이 조회 전용으로 표시됩니다. 목록은 확인만 가능하며 추가 및 삭제, 전송, 순서 변경은 마스터 장치에서만 할 수 있습니다.
  - 마스터 장치가 동영상 재생 기능을 지원하지 않으면 슬레이브 화면에는 동영상 목록이 표시되지 않고 **기본 대기 화면** 옵션만 표시됩니다.

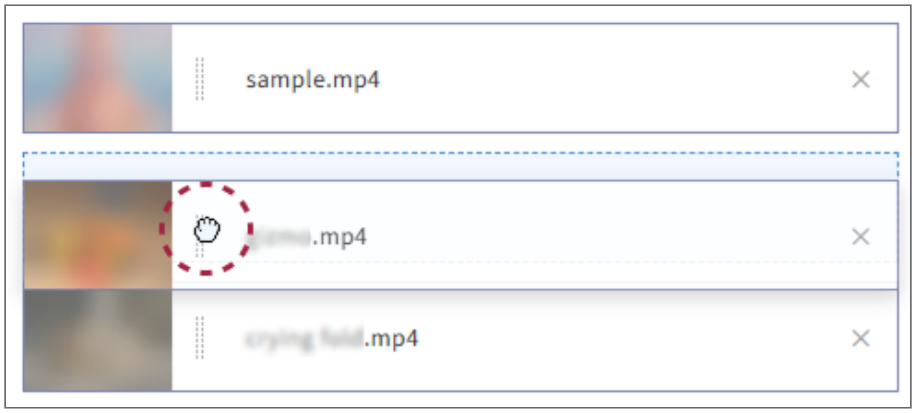
팁

일괄 편집 기능으로 여러 대의 장치에 동영상을 한번에 추가하고 전송할 수 있습니다. **일괄 편집** 기능에 대한 자세한 내용은 장치 관리 기능 사용하기를 참고하세요.



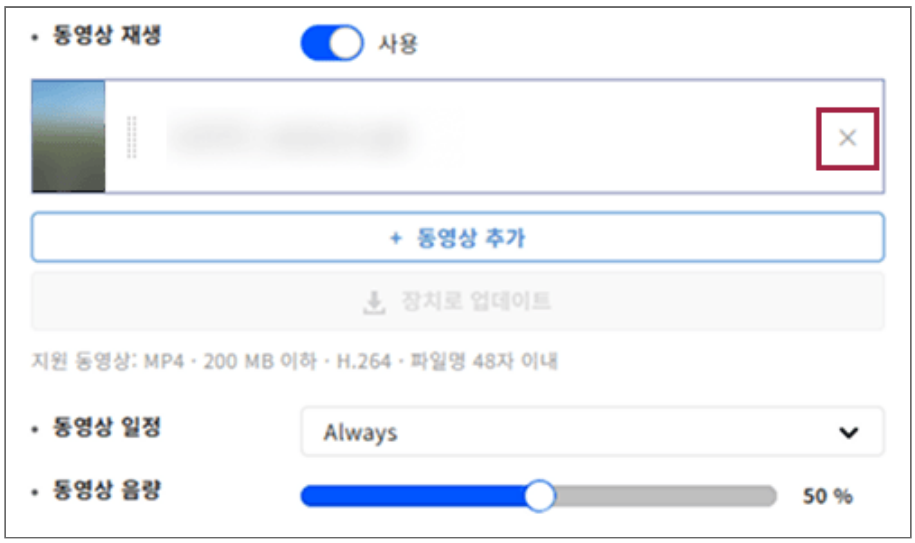
동영상 재생 순서 변경

동영상 썸네일 오른쪽 영역을 클릭한 상태로 드래그하여 재생 순서를 변경할 수 있습니다. 순서를 변경한 후 변경 사항을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.



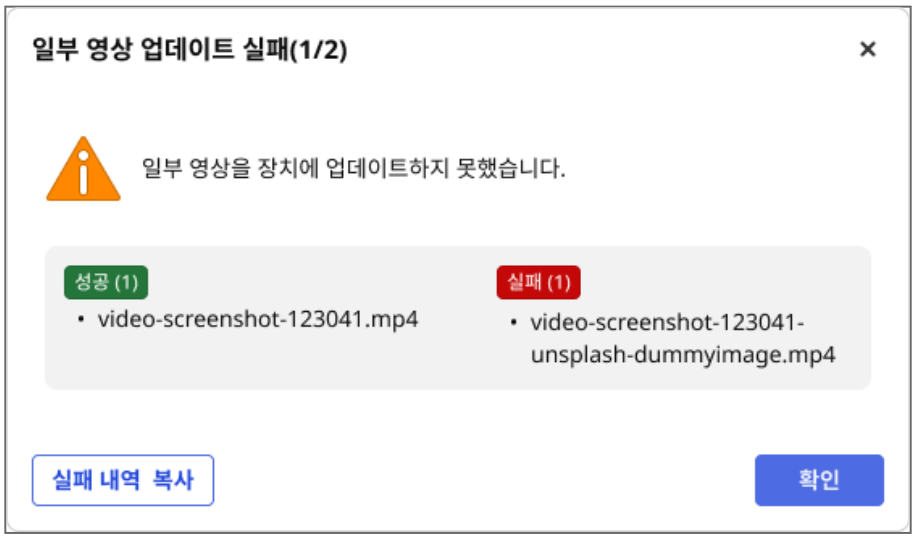
동영상 삭제

업로드한 동영상을 삭제하려면 **대기화면** → **동영상 재생**에서 삭제하려는 동영상의 ✕ 버튼을 클릭하세요. 이후 **장치로 업데이트** 버튼을 클릭하세요. 변경 사항을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.



동영상 전송 실패

동영상을 장치로 전송하는 데 실패하면 팝업을 통해서 실패한 영상 이름을 확인할 수 있습니다.



대표적인 전송 실패 사유는 다음과 같습니다.

- 장치의 응답을 처리하는 중 오류가 발생했을 때

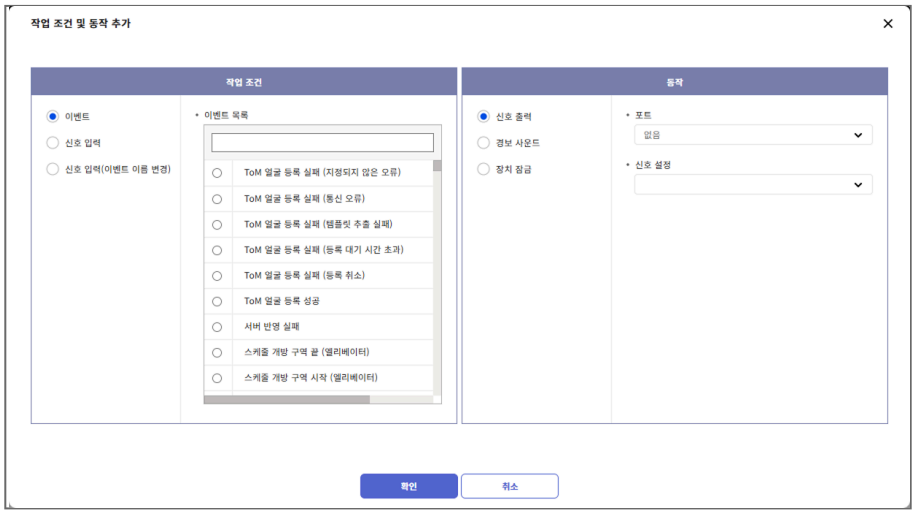
- 위 사유에 해당하지 않는 그 외 오류가 발생했을 때

> **팁**
>
> **일괄 편집** 기능로 여러 대의 장치에 동영상을 일괄 전송했을 때 일부 장치만 실패했다면, 결과 팝업에서 **실패 내역 복사** 버튼을 클릭해 실패한 장치 목록과 사유를 클립보드에 복사할 수 있습니다.

작업 조건 및 동작 설정

작업 조건 및 동작 그룹에서는 각 상황에 따른 작업 조건과 동작을 설정할 수 있습니다. 예를 들어, 인증에 실패하면 모든 알람을 울리거나, RS-485 연결이 끊어지면 장치를 사용하지 못하도록 설정할 수 있습니다.

작업 조건과 동작은 이벤트를 선택하여 등록할 수도 있고, 사용자가 원하는 작업 조건이나 동작을 설정할 수도 있습니다. **작업 조건 및 동작** 그룹에서 오른쪽에 ＋ **추가** 버튼을 클릭하세요.



작업 조건

미리 설정한 이벤트를 선택하거나 사용자 정의 조건을 추가할 수 있습니다.

- **이벤트**: 미리 설정한 이벤트를 선택하세요.
- **신호 입력**: 옵션 내 각 항목을 선택해 사용자 정의 조건을 설정하세요.
- **신호 입력(이벤트 이름 변경)**: 옵션 내 각 항목을 선택해 사용자 정의 조건을 설정하세요. 입력에 대한 별도의 동작 없이 입력만 감지하도록 설정할 수 있습니다.

> **알아두기**
>
> - **작업 조건**을 **이벤트**로 설정한 경우 이벤트 목록에서 하나의 이벤트만 선택할 수 있습니다.
> - **신호 입력** 또는 **신호 입력(이벤트 이름 변경)** 옵션을 선택하여 사용자 정의 조건을 설정할 때 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭하세요. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
> - **신호 입력(이벤트 이름 변경)** 옵션을 선택하여 사용자 정의 조건을 설정할 때 원하는 이벤트 이름이 없다면 **이벤트 이름 추가**를 클릭하세요. 해당 이벤트가 발생하면 이벤트 로그 및 실시간 로그에 설정한 이벤트 이름이 표시됩니다.
> - 이벤트 이름은 최대 64자까지 입력할 수 있습니다.

동작

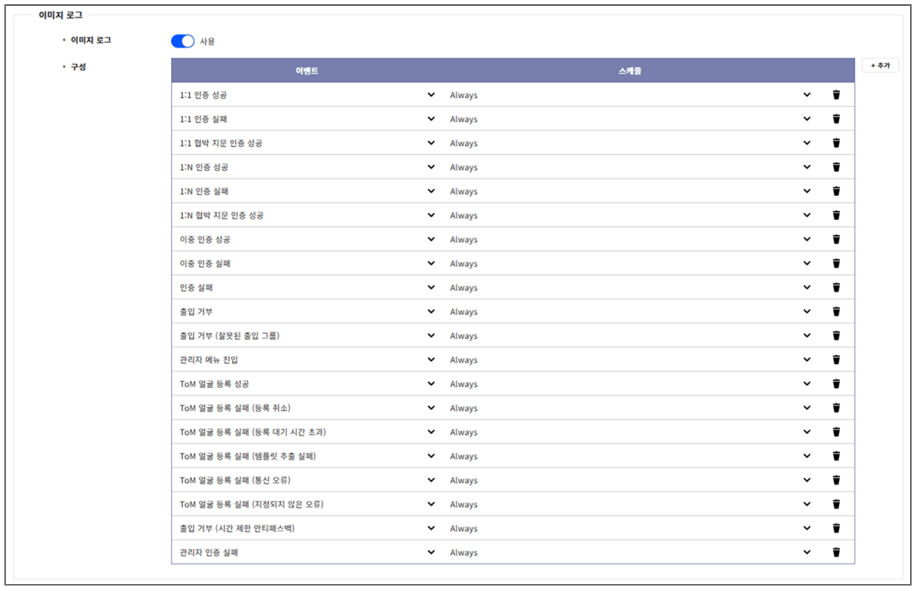
미리 설정된 동작을 선택하거나 사용자 정의 동작을 추가할 수 있습니다.

> **알아두기**
>
> - **신호 출력** 옵션을 선택해 사용자 정의 동작을 설정할 때 원하는 신호 설정이 없다면 **+ 신호 추가**를 클릭하여 설정하세요.
> - **작업 조건**을 **신호 입력(이벤트 이름 변경)**으로 선택했다면, **동작**을 **없음**으로 설정할 수 있습니다.

이미지 로그 설정

이미지 로그 그룹에서는 장치에서 사용할 이미지 로그 이벤트와 스케줄을 설정할 수 있습니다.

1. **이미지 로그** 옵션을 **사용**으로 설정하세요.
2. **구성**에서 **+ 추가**를 클릭해 원하는 이벤트와 스케줄을 설정하세요.



> **알아두기**
>
> - 이 기능은 BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, BioStation A2 모델에서 지원합니다.
> - 이미지 로그의 기본 설정에 대한 자세한 내용은 이미지 로그 설정하기를 참고하세요.

Wiegand 설정

Wiegand 그룹에서는 Wiegand 장치의 입출력 관련 세부 항목을 설정할 수 있습니다.



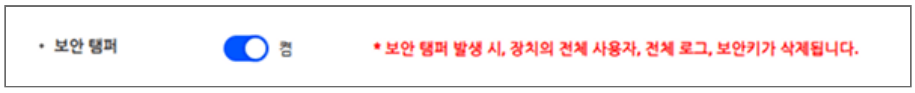
- **입출력**: 입출력 모드를 선택하세요.
- **펄스 폭(µs)**: Wiegand 신호의 펄스 폭을 설정하세요.

- **입력 형식**: 장치에 지정할 Wiegand 형식을 변경하세요.
- **펄스 간격(µs)**: Wiegand 신호의 펄스 간격을 설정하세요.
- **출력 모드**: Wiegand 신호 출력 모드를 설정하세요.
  - **일반**: 설정된 Wiegand 형식으로 카드를 스캔합니다. 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.

> **알아두기**
> Wiegand 형식 설정에 대한 자세한 내용은 Wiegand 카드 형식 설정하기를 참고하세요.

보안 탬퍼 설정

장치에서 탬퍼 이벤트가 발생할 경우 장치에 저장된 전체 사용자 정보, 전체 로그, 보안 키를 삭제하도록 설정할 수 있습니다. **보안 탬퍼** 기능을 활성화하려면 **켬**으로 설정하세요.



아날로그 인터폰 설정

아날로그 인터폰 사용 여부를 설정할 수 있습니다. 장치에 연결된 인터폰을 사용하려면 **인터폰** 그룹에서 **사용**을 클릭하세요.

> **알아두기**
> 이 기능은 BioStation 2 모델만 지원합니다.

카메라 설정

카메라 주파수를 설정할 수 있습니다. 형광등을 사용하는 환경에서 주파수를 잘못 설정하면 이미지에 깜빡임이 발생할 수 있습니다. **카메라** 그룹에서 해당 지역의 주파수를 설정하세요.

> **알아두기**
> - 이 기능은 펌웨어 2.1.4 버전 이상의 FaceStation F2 모델과 BioStation A2 모델에서 지원합니다.
> - 카메라 주파수는 지리적인 위치마다 다르게 사용합니다. 미국은 60Hz를 일반적으로 사용하며 대부분의 다른 지역은 50Hz를 사용합니다. 해당 지역의 카메라 주파수는 대리점에 문의하세요.

열화상 및 마스크 설정하기

열화상 및 마스크 또는 **마스크** 섹션에서는 열화상 카메라 및 마스크 사용에 대한 세부 항목을 설정할 수 있습니다.

- 열화상 카메라를 슈프리마의 얼굴 인증 장치와 연동해 출입문을 오가는 사용자의 온도를 측정하고, 기준 온도를 초과하는 사용자의 접근을 제한할 수 있습니다.

- 마스크를 검출하여 마스크를 착용하지 않은 사용자의 접근을 제한할 수 있습니다.

> **알아두기**
>
> - **열화상 카메라** 설정 기능은 FaceStation 2, FaceStation F2 모델에서 지원합니다. 지원하는 열화상 카메라는 아래를 참고하세요.
>   - TCM10-FS2
>   - TCM10-FSF2
> - **마스크 검출** 설정 기능은 FaceStation F2, BioStation 3, BioEntry W3, BioStation 3 Max 모델에서 지원합니다.
> - 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

마스크 설정

마스크 설정 그룹에서는 마스크 검출 사용 여부를 설정할 수 있습니다.

- **마스크 검출**: 마스크 검출 사용 여부를 선택하세요.
  - **사용 (검출 실패 시 인증 거부)**: 마스크를 착용하지 않은 사용자는 인증 거부되며 마스크 미착용 이벤트 로그를 기록합니다.
  - **사용 (검출 실패 시 로그 기록 후 인증 허용)**: 마스크를 착용하지 않은 사용자도 인증할 수 있으나 마스크 미착용 이벤트 로그를 기록합니다.
  - **사용 안함**: 마스크 검출 기능을 사용하지 않습니다.
- **마스크 검출 레벨**: 마스크 검출 민감도를 선택하세요.

> **알아두기**
>
> **마스크 확인 방식** 옵션에 대한 자세한 내용은 열화상 및 마스크 확인 방식을 참고하세요.

열화상 카메라 설정

열화상 카메라 그룹에서는 열화상 카메라 사용 여부 및 세부 항목을 설정할 수 있습니다.

- **열화상 카메라 사용**: 열화상 카메라 사용 여부를 설정하세요.
  - **사용 (기준 온도 초과 시 인증 거부)**: 기준 온도를 초과한 사용자는 인증 거부되며 기준 온도 초과 이벤트 로그를 기록합니다.
  - **사용 (기준 온도 초과 시 로그 기록 후 인증 허용)** 기준 온도를 초과한 사용자도 인증할 수 있으나 온도 초과 이벤트 로그를 기록합니다.
- **섭씨/화씨**: 온도 표시 단위를 설정하세요.
- **기준 온도 (°C)** / **기준 온도 (°F)**: 출입을 제한할 기준 온도의 최저 값과 최고 값을 설정하세요.

  표면 온도가 **Low** 값보다 낮거나 **High** 값보다 높은 사용자는 **열화상 카메라 사용** 옵션에 따라 출입을 제한합니다. 1°C~45°C의 범위에서 설정할 수 있으며, **Low** 값은 **High** 값보다 높게 설정할 수 없습니다.
- **온도 로그 저장**: 사용자의 온도 로그 저장 여부를 설정하세요.
  - **사용**: 인증 성공 여부 및 사용자의 온도 값을 로그로 저장합니다.
  - **사용 안 함**: 인증 성공 여부 로그만 저장합니다.

- **인증 실패 알림**: 기준 온도 초과로 인한 인증 실패 시 알림 여부를 설정하세요.
- **적외선 영상 표시**: 장치 화면에 적외선 영상 표시 여부를 설정하세요.
- **카메라 설정**: 열화상 카메라의 세부 옵션을 설정하세요.
  - **온도 보정값 (°C)**: 제품 사용 환경에 따라 온도를 일정한 값만큼 높거나 낮게 측정하도록 보정할 수 있습니다. 예를 들어, 온도 값이 항상 0.1°C씩 높게 측정되는 환경에서는 온도 보정값을 -0.1°C로 설정하세요.
  - **온도 측정 거리(cm)**: 사용자와 열화상 카메라 사이의 거리를 설정하세요.
  - **적외선 방사율**: 적외선 방사율을 설정하세요.
  - **다이내믹 ROI**: 주변에 기타 조명이 설치되어 있다면 열화상 카메라가 자동으로 해당 조명이 아닌 사용자의 온도를 측정하도록 설정할 수 있습니다.
  - **ROI X(%)** / **ROI Y(%)** / **ROI Width(%)** / **ROI Height(%)**: **다이내믹 ROI** 옵션을 **사용 안 함**으로 설정할 경우 수동으로 ROI(관심 영역)를 설정할 수 있습니다. ROI 위치와 크기를 조절하여 열화상 카메라가 온도를 측정할 영역을 수동으로 설정하세요.

알아두기

- **기준 온도** 옵션의 **Low** 값과 **High** 값 설정은 아래 펌웨어 버전부터 지원합니다.
  - FaceStation 2 펌웨어 1.4.2 이상
  - FaceStation F2 펌웨어 1.0.2 이상
- 최적의 성능을 위해 **카메라 설정**의 하위 옵션은 기본 설정 값 사용을 권장합니다. 장치별 각 옵션의 기본 값은 아래를 참고하세요.

항목	FaceStation 2	FaceStation F2
온도 측정 거리(cm)	100	100
적외선 방사율	0.98	0.98
ROI X(%)	47	30
ROI Y(%)	45	25
ROI Width(%)	15	50
ROI Height(%)	10	55

열화상 및 마스크 확인 방식

열화상 및 마스크 확인 방식 또는 **마스크 확인 방식** 그룹에서는 **마스크 검출** 또는 **열화상 카메라 사용** 옵션을 **사용**으로 설정하면 장치의 용도에 따라 확인 방식을 설정할 수 있습니다.

- **인증 후 확인**: 인증을 수행한 뒤 사용자의 마스크 착용 여부를 확인하거나 온도를 측정합니다.
- **인증 전 확인**: 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 확인**: 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.

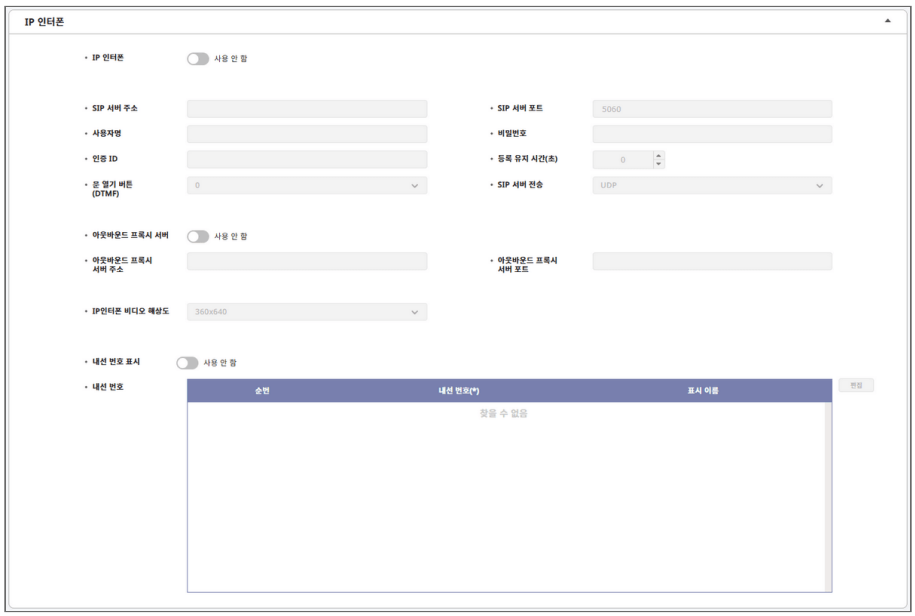
IP 인터폰 설정하기

IP 인터폰 섹션에서는 IP 인터폰 사용에 대한 세부 항목을 설정할 수 있습니다.

> **알아두기**
>
> - 이 기능은 BioStation 3 Max, BioStation 3, FaceStation 2, BioStation A2 모델에서 지원합니다.
> - 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

IP 인터폰 설정

Session Initiation Protocol(SIP) 서버에 장치를 등록하도록 각 옵션을 설정하세요.



- **IP 인터폰**: 장치를 IP 인터폰으로 사용하려면 **사용**으로 설정하세요.
- **SIP 서버 주소**: SIP 서버의 주소를 입력하세요.
- **SIP 서버 포트**: SIP 서버의 포트를 입력하세요. 기본값은 5060입니다.
- **사용자명**: SIP 계정의 사용자 이름을 입력하세요.
- **비밀번호**: SIP 계정의 비밀번호를 입력하세요.
- **인증 ID**: SIP 계정의 인증 아이디를 입력하세요.
- **등록 유지 시간(초)**: 초 단위로 등록 유지 시간을 입력하세요. 장치는 등록 유지 시간이 끝날 때마다 SIP 서버에 등록을 시도합니다.
- **문 열기 버튼 (DTMF)**: 통화 중 장치의 출입문을 개방할 수 있는 버튼을 지정하세요.
- **SIP 서버 전송**: IP 인터폰의 SIP 서버 설정 시 SIP 전송 방법을 선택하세요.
- **아웃바운드 프록시 서버**: 별도의 (아웃바운드) 프록시 서버를 통해 SIP 서비스를 사용하려면 **사용**으로 설정하세요.
  - **아웃바운드 프록시 서버 주소**: 아웃바운드 프록시 서버의 주소를 입력하세요.

  - **아웃바운드 프록시 서버 포트**: 아웃바운드 프록시 서버의 포트를 입력하세요.

- **IP인터폰 비디오 해상도**: IP 인터폰을 사용할 때 출력되는 영상의 해상도를 선택하세요. 기본값은 **360 x 640**입니다.
- **내선 번호 표시**: 장치에서 내선 번호를 표시하지 않도록 하려면 **사용 안 함**으로 설정하세요. 내선 번호를 표시하지 않으면 전화 걸기 화면에서 수신자를 구별할 수 없습니다.
- **내선 번호**: 최대 128개의 내선 번호를 등록할 수 있습니다. 내선 번호를 추가하거나 편집하려면 **편집** 버튼을 클릭하세요. 자세한 내용은 내선 번호 편집을 참고하세요.

> **알아두기**
>
> - **사용자명**과 **인증 ID** 옵션은 숫자, 영문(대소문자 구분), 특수 기호만 입력할 수 있습니다.
> - **등록 유지 시간(초)** 옵션은 60초에서 600초 사이로 설정할 수 있습니다.
> - **SIP 서버 전송**과 **IP인터폰 비디오 해상도** 옵션은 BioStation 3 펌웨어 1.3.0 버전 이상에서 지원합니다.
> - **Session Initiation Protocol**(SIP)은 인터넷 전화, 화상 회의 등 다양한 멀티미디어 통신을 위한 인터넷 프로토콜 기반의 통신 프로토콜입니다. SIP 서버는 이러한 통신을 관리하고 연결을 설정하는 역할을 합니다.

내선 번호 편집

내선 번호 편집 창에서 제공하는 기능에 대해 안내합니다.



- **맨 위로 보내기**: 선택한 내선 번호를 목록의 최상단으로 이동시킬 수 있습니다.
- **CSV 불러오기**: 내선 번호를 저장한 CSV 파일을 불러올 수 있습니다.
- **CSV 내보내기**: 저장된 내선 번호를 CSV 파일로 내보낼 수 있습니다.
- **추가**: 내선 번호를 추가합니다.
- **삭제**: 내선 번호를 삭제합니다.
- **순서 변경**: 내선 번호를 마우스로 끌어서 순서를 변경합니다.

> **알아두기**
>
> - FaceStation 2와 BioStation A2 모델은 내선 번호를 최대 16개까지 저장할 수 있습니다.
> - 지원하는 최대 내선 번호보다 많은 내선 번호를 포함한 CSV 파일을 불러올 수 없습니다.
> - 내선 번호는 숫자, 영문(대소문자 구분), 특수 기호만 입력할 수 있습니다.

RTSP 설정하기

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

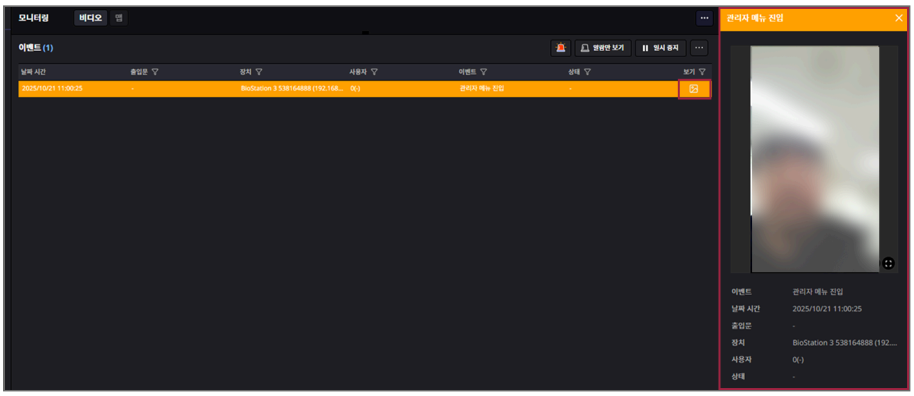


- **RTSP**: RTSP 스트리밍을 사용하려면 **사용**으로 설정하세요.
- **주소**: RTSP 서버 주소는 고정되어 있습니다. RTSP 주소를 복사하려면 **복사** 버튼을 클릭하세요.
- **포트**: RTSP 포트를 설정하세요.
- **ID**: RTSP 서버의 아이디를 입력하세요.
- **암호**: RTSP 서버의 비밀번호를 입력하세요.
- **RTSP 비디오 해상도**: RTSP 사용 시 출력되는 영상의 해상도를 선택하세요. 기본값은 **180 x 320**입니다.

> **알아두기**
>
> - 이 기능은 BioStation 3 Max, BioStation 3, BioEntry W3 모델에서 지원합니다.
> - **RTSP 비디오 해상도** 옵션은 BioStation 3 펌웨어 1.3.0 버전 이상에서 지원합니다.
> - 사용자가 임의로 변경한 사항이 있다면 **확인** 버튼을 클릭하세요. 변경 사항을 저장하지 않으면 장치에 적용되지 않습니다.

이미지 로그 설정하기

이미지 로그는 카메라가 있는 장치에서 발생한 이벤트를 이미지로 확인할 수 있는 기능입니다. 출입문을 통과하는 사용자의 얼굴 이미지나 이벤트 발생 시의 상황을 장치의 카메라로 기록할 수 있습니다. 기록된 이미지는 **모니터링** 페이지에서 실시간 이벤트를 통해 확인할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

이미지 로그를 설정하면 **이벤트** 목록에서 해당 이벤트에 대한 이미지 로그가 생성됩니다. 이벤트 항목의 가장 오른쪽에 버튼을 클릭하세요. 오른쪽 패널에서 해당 이벤트가 발생했을 때 촬영된 이미지를 확인할 수 있습니다.

알아두기

- 이 기능은 BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, BioStation A2 모델에서 지원합니다.
- **모니터링** 페이지에서 이벤트 로그를 확인하는 방법에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

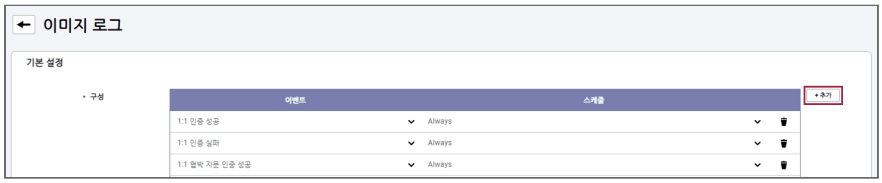
주의

설정 → **장치** → **이미지 로그** 메뉴에서 설정한 내용은 장치에 반영되지 않습니다. 개별 장치에서 **이미지 로그** 옵션을 활성화해야 합니다. 자세한 내용은 고급 설정하기를 참고하세요.

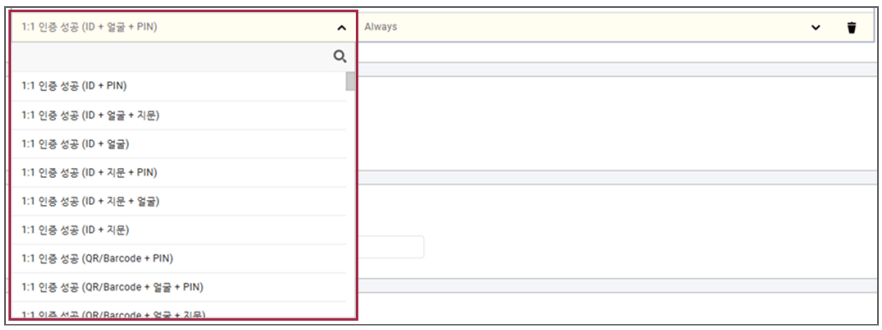
기본 설정 추가

장치의 **이미지 로그** 옵션을 활성화했을 때 적용되는 기본 설정을 구성할 수 있습니다. 이미지 로그 생성을 위한 이벤트 및 스케줄을 구성하세요. 이벤트와 스케줄 조건에 부합하면 이미지 로그를 생성합니다.

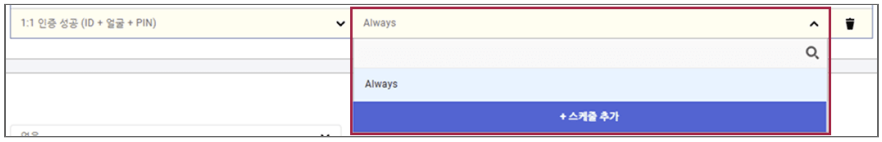
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **기본 설정** 섹션의 오른쪽에 **+ 추가** 버튼을 클릭하세요.



4. 목록 하단에 이벤트가 추가되면 원하는 이벤트의 ⌄ 버튼을 클릭하고 원하는 항목을 선택하세요.



5. 해당 이벤트의 스케줄에서 ⌄ 버튼을 클릭하고 원하는 항목을 선택하세요.



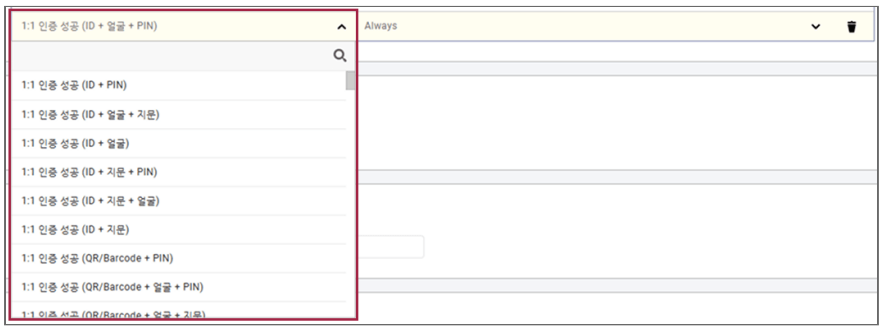
6. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

기본 설정 변경

기존에 설정한 이미지 로그의 이벤트와 스케줄을 변경할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **기본 설정** 섹션의 목록에서 변경할 이벤트의 ⌄ 버튼을 클릭하고 원하는 항목을 선택하세요.



4. 해당 이벤트의 스케줄에서 ⌄ 버튼을 클릭하고 원하는 항목을 선택하세요.



5. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
> - 변경된 기본 설정은 새로 추가된 장치에만 적용됩니다. 이미 **이미지 로그** 옵션을 활성화한 장치에는 반영되지 않으므로 해당 장치 설정에서 추가해야 합니다.

기본 설정 삭제

기존에 설정한 이미지 로그의 이벤트와 스케줄을 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **기본 설정** 섹션의 목록에서 삭제할 이벤트의 🗑 버튼을 클릭하세요.



4. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

삭제 옵션

이미지 로그 파일이 계속 저장되어 **BioStar X** 서버의 저장 공간을 차지하지 않도록 삭제 옵션을 설정할 수 있습니다. 설정한 파일 크기 또는 기간이 지난 이미지 로그는 자동으로 삭제됩니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **삭제 옵션** 섹션에서 이미지 로그 삭제 조건을 설정하세요.



- **삭제 옵션**: 파일 크기 단위(**MB**/**GB**) 또는 기간 단위(**일**/**주**/**월**)를 선택하세요.
- **이미지 로그의 양**: **삭제 옵션**에서 설정한 조건의 단위를 설정하세요.
- **삭제 주기**: 이미지 로그를 삭제할 주기를 선택하세요.

4. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

저장 경로 설정

이미지 로그를 저장하는 경로를 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **저장 경로 설정** 섹션의 **이미지 파일 경로** 입력 필드에 이미지 로그를 저장할 경로를 입력하세요.



4. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 저장 경로는 자동 생성되지 않으므로 이미지 로그를 저장할 경로를 미리 생성해 두어야 합니다.
> - 예를 들어, `.\imagelog\` 와 같이 입력하면 BioStar X를 설치한 경로 하위에 이미지 로그를 저장합니다.
>
> *C:\Program Files\BioStar X\imagelog*

사용자 프로필 이미지 옵션

이미지 로그를 촬영할 수 없는 장치에서 이벤트 로그, 실시간 로그를 모니터링할 때 사용자 프로필 사진을 보여주도록 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **이미지 로그**를 클릭하세요.
3. **사용자 프로필 이미지 옵션** 섹션의 **이미지 로그 없는 경우 사용자 프로필 이미지 표시** 항목의 체크박스를 클릭하세요.



4. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 이 옵션이 활성화되어 있을 때 이미지 로그가 발생하면 사용자 프로필 사진을 보여주지 않고 촬영된 이미지 로그를 보여줍니다.
> - **모니터링** 페이지에서 이벤트 로그를 확인하는 방법에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.

USB 에이전트 설정하기

클라이언트 PC에서 **BioStar X**에 접속했을 때 USB 지문 등록 장치 및 카드 등록 장치를 사용할 수 있도록 지원합니다. 이를 위해 USB Device Agent를 설치해야 합니다. 이 문서에는 USB Device Agent를 설치하고 설정하는 방법을 안내합니다.

USB Device Agent 설치하기

클라이언트 PC에서 **BioStar X**에 접속해 USB 지문 등록 장치 및 카드 등록 장치를 사용하려면 USB Device Agent를 설치해야 합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **USB Agent**를 클릭하세요.
3. **USB Device Agent** 섹션에서 **다운로드** 버튼을 클릭하세요.



4. 다운로드한 파일을 실행해 화면의 안내에 따라 설치를 완료하세요.

> **알아두기**
>
> Windows에서 **사용자 계정 컨트롤**이 활성화된 경우 USB Agent를 자동 실행할 수 없습니다. 사용자 계정 컨트롤을 끄거나 관리자 권한으로 직접 실행하세요.

USB 카드 장치 바이트 순서 설정

USB 카드 장치의 바이트 순서를 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **USB Agent**를 클릭하세요.
3. **USB 카드 장치 바이트 순서** 섹션에서 **바이트 순서** 옵션을 설정하세요.



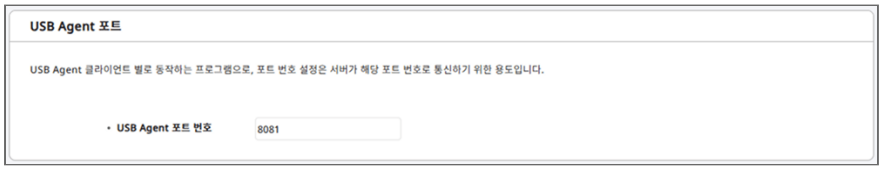
   - **MSB**: 카드 데이터를 처리할 때 큰 바이트 단위에서 작은 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 왼쪽에서 오른쪽으로 순차 저장합니다.
   - **LSB**: 카드 데이터를 처리할 때 작은 바이트 단위에서 큰 바이트 단위 순서로 처리하여 카드 일련 번호(CSN)를 저장합니다.
4. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **바이트 순서** 옵션은 CSN 카드에 한해서만 적용할 수 있습니다.

USB Agent 포트 설정

USB Agent가 사용하는 포트를 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **USB Agent**를 클릭하세요.
3. **USB Agent 포트** 섹션의 **USB Agent 포트 번호** 입력 필드에서 포트 번호를 입력하세요.



4. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> USB Agent 클라이언트별 동작하는 프로그램으로, 포트 번호 설정은 서버가 해당 포트 번호를 통신하기 위한 용도입니다.

장치 연결 관리 설정하기

BioStar X의 **장치 연결 관리**는 회사나 대형 건물에서 많은 수의 장치를 효율적으로 관리하기 위해 만들어진 기능입니다. 기존에는 하나의 서버에서 최대 1,000대의 장치만 연결할 수 있었지만, 이제 **커뮤니케이션**(Communication) 서버를 여러 대의 컴퓨터에 설치하여 최대 3,000대의 네트워크 장치를 관리할 수 있습니다.

알아두기

- 이 기능은 **디바이스 매니저** 라이선스를 활성화했을 때 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 멀티 커뮤니케이션 서버의 사양과 설치에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 시스템 최소 요구사항
  - 멀티 커뮤니케이션 서버 설치하기

주요 기능

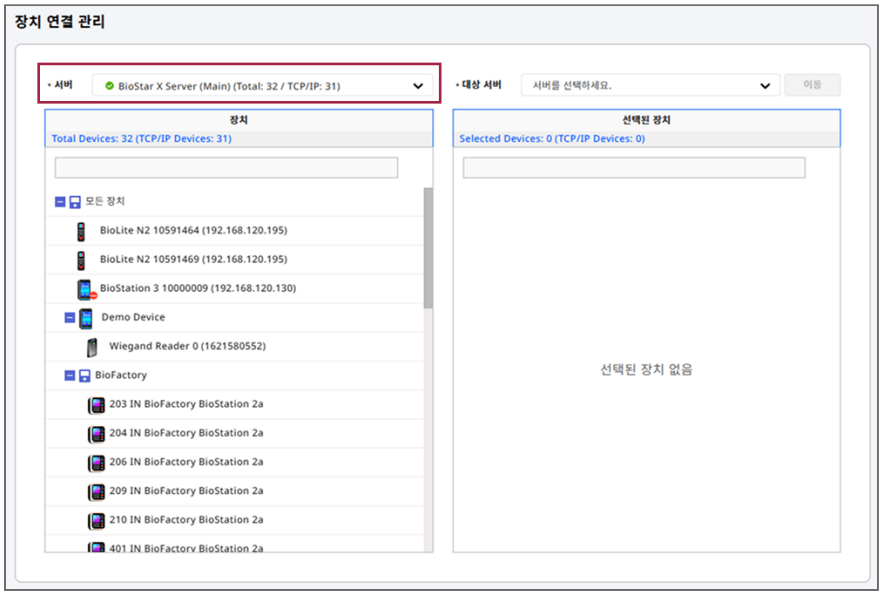
- **서버 확장**: 메인 컴퓨터 외에 추가 컴퓨터에 통신 서버를 설치하여 더 많은 장치 연결할 수 있습니다.
- **여러 서버 운영**: 최대 3개의 서버를 함께 사용하여 총 3,000대 장치 지원합니다.
- **편리한 장치 관리**: 새 장치를 추가할 때 어느 서버에 연결할지 선택할 수 있으며, 기존 장치를 다른 서버로 옮길 수도 있습니다.
- **대용량 환경 지원**: 큰 규모의 사업장이나 건물에서 요구하는 많은 장치를 안정적으로 운영할 수 있습니다.

멀티 커뮤니케이션 서버는 BioStar X의 통합 서버에서 장치와의 연결 기능만을 분리한 전용 서비스입니다. 장치와의 안정적인 통신에만 집중하여 전체 시스템의 성능을 향상시킵니다.

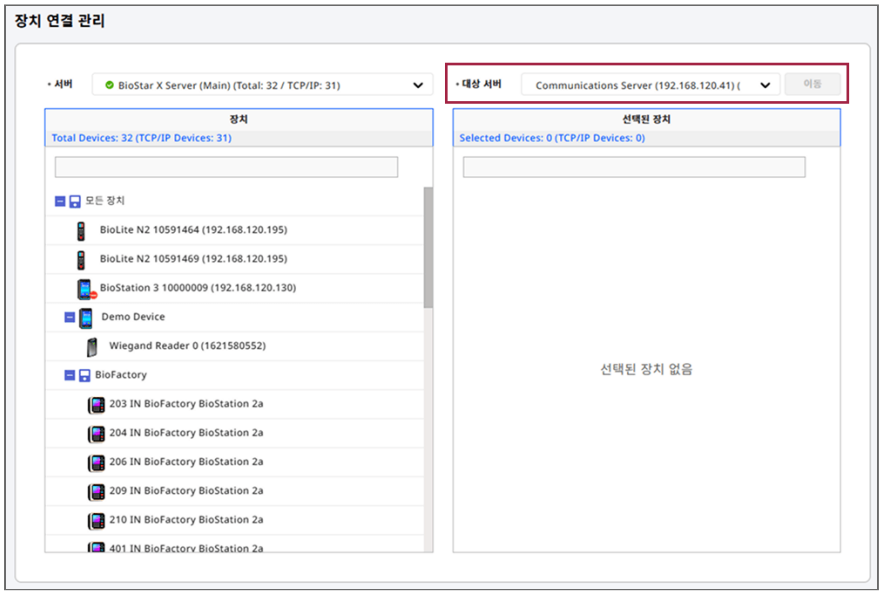
다른 서버로 장치 이동하기

메인 서버 또는 다른 멀티 커뮤니케이션 서버에 등록된 장치를 다른 멀티 커뮤니케이션 서버로 이동할 수 있습니다. 이 기능은 장치의 연결 상태를 유지하면서 서버 간에 장치를 이동할 수 있도록 도와줍니다.

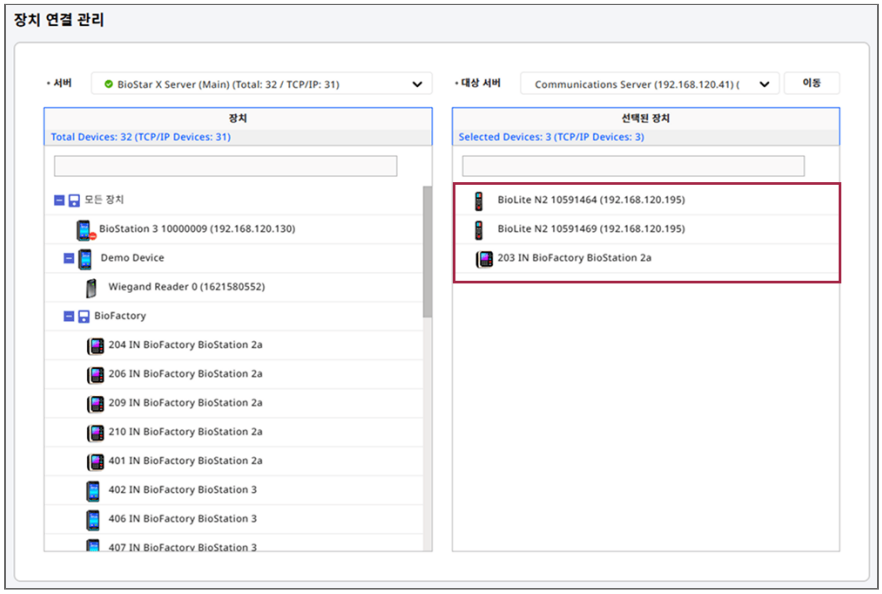
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치 연결 관리**를 클릭하세요.
3. 왼쪽에 **서버** 항목에서 이동시키려는 장치가 등록된 서버를 선택하세요.



4. 오른쪽에 **대상 서버** 항목에서 장치를 이동시킬 대상 서버를 선택하세요.

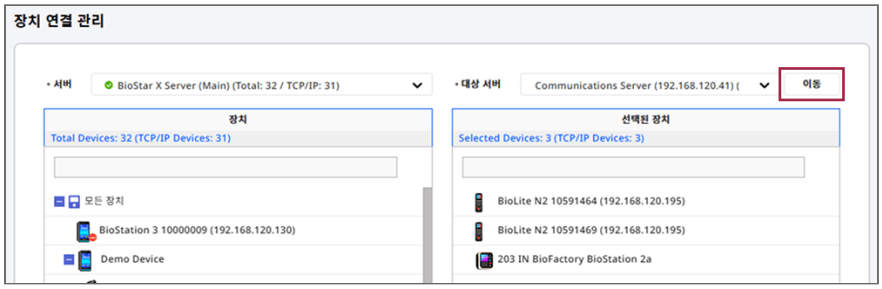


5. 장치 목록에서 이동시키려는 장치를 선택하세요. 여러 개의 장치를 선택할 수 있습니다.



> 특정 장치를 검색하려면 상단의 입력 필드에 키워드를 입력하세요. 장치 이름, 시리얼 번호로 검색할 수 있습니다.

6. 장치를 대상 서버로 이동하려면 **이동** 버튼을 클릭하세요.



7. 메시지 창에서 이동할 총 장치 수, TCP/IP 연결 장치 수, 이동할 서버 이름 및 IP 주소를 확인하세요.
8. **네** 버튼을 클릭하세요.

이동을 완료하면 메시지 창을 통해 이동된 총 장치 수, TCP/IP 연결 장치 수, 이동된 서버 이름 및 IP 주소를 확인할 수 있습니다.

이동을 실패한 장치가 있다면 메시지 창에 이동 실패한 장치 수와 TCP/IP 연결 장치 수를 확인할 수 있습니다. 이동 실패한 장치 목록 및 실패 사유를 CSV 파일로 확인하려면 **다운로드** 버튼을 클릭하세요.

> **알아두기**
>
> - 연결된 확장 서버가 없다면 화면 오른쪽의 **대상 서버**는 표시되지 않습니다.
> - 서버를 선택하면 해당 서버에 Wiegand, RS-485 연결 장치를 포함한 등록된 모든 장치를 확인할 수 있습니다.
> - 장치 또는 장치 그룹을 선택하면 장치에 연결된 하위 장치와 그룹에 포함된 장치들도 함께 이동합니다.
> - TCP/IP 통신으로 연결하지 않은 장치들은 이동할 수 없습니다.

출입문 관리하기

등록한 장치가 설치된 출입문 정보를 설정하고 관리하는 방법을 안내합니다. 장치의 릴레이, 이중 인증, 안티패스백, 강제 문 열림, 장시간 문 열림에 대한 알람 등의 정보를 설정할 수 있으며, 설정한 출입문 정보는 출입 등급의 구성 요소로 사용됩니다.

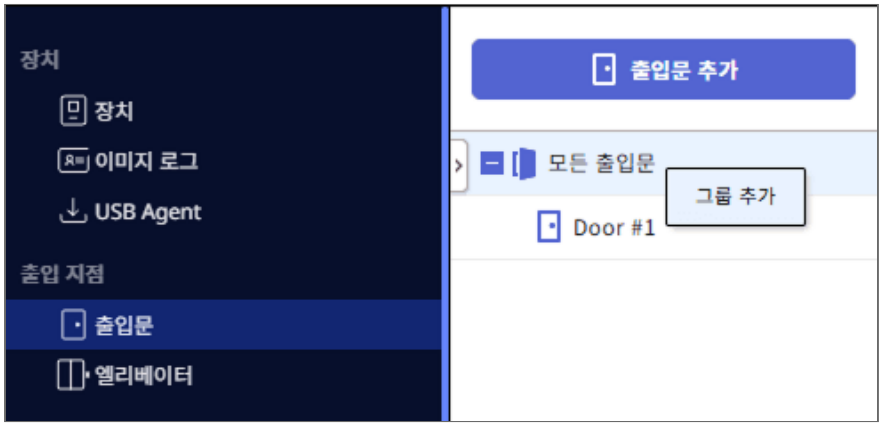
출입문 그룹 관리하기

여러 개의 출입문을 쉽게 관리할 수 있도록 그룹 설정 방법을 안내합니다. 출입문 그룹은 여러 개의 출입문을 하나의 그룹으로 묶어 관리할 수 있는 기능입니다. 그룹을 설정하면 출입문을 일괄 설정할 수 있습니다.

> **팁**
>
> 출입문 위치나 사무실 이름 등으로 그룹 이름을 등록하면 관리가 편리합니다.

출입문 그룹 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**을 클릭하세요.
3. 출입문 목록에서 **모든 출입문**을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **그룹 추가**를 클릭하세요.



5. 원하는 그룹 이름을 입력하세요.

> **알아두기**
>
> - 출입문 그룹은 최대 8단계까지 생성할 수 있습니다.
> - 출입문 그룹 이름은 최대 48자까지 입력할 수 있습니다.

출입문 그룹 이름 변경

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 이름을 변경할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **이름 변경**을 클릭하세요.
5. 변경할 그룹 이름을 입력하세요.

알아두기
출입문 그룹 이름은 최대 48자까지 입력할 수 있습니다.

출입문 그룹 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 삭제할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **그룹 삭제**을 클릭하세요.

주의
출입문 그룹을 삭제하면 그룹에 포함된 모든 출입문이 삭제됩니다. 그룹에 포함된 출입문을 삭제하지 않으려면 먼저 출입문을 다른 그룹으로 이동한 후 그룹을 삭제하세요.

그룹에 출입문 추가

출입문 목록에서 그룹에 추가하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 그룹에 추가할 출입문을 선택하고 원하는 그룹으로 드래그하세요.



선택한 출입문이 그룹으로 이동합니다.

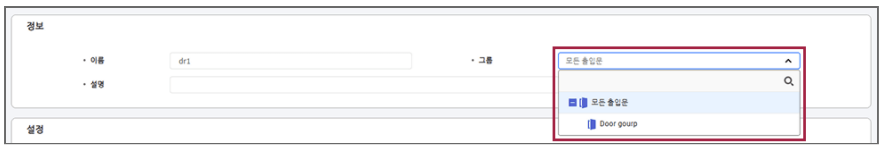


출입문 정보에서 그룹에 추가하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 화면 오른쪽의 출입문 목록에서 그룹에 추가할 출입문을 클릭하세요.



4. 출입문 정보 수정 화면이 나타나면 **정보** 섹션의 **그룹** 옵션을 클릭하세요.



5. 원하는 그룹을 선택하세요.
6. 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

출입문 등록하기

출입문을 등록하고 설정하는 방법을 안내합니다. 출입문별로 입실·퇴실 장치를 연결하고, 안티패스백과 이중 인증 등 보안 기능을 설정하여 체계적인 출입 관리 환경을 구축할 수 있습니다. 또한 출입문 상태에 따른 알람 설정으로 보안 사고를 사전에 예방할 수 있습니다.

시작하기 전에

- 출입문을 등록하기 전에 출입 통제를 위한 출입 등급, 출입 그룹, 층 등급을 설정하세요. 자세한 내용은 출입 통제 설정하기를 참고하세요.
- 출입문을 등록하기 전에 장치를 등록하세요. 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 장치 등록하기
  - Wiegand 장치 등록하기
  - 슬레이브 장치 등록하기

출입문 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. **출입문 추가** 버튼을 클릭하세요.



4. **새 출입문 추가** 화면이 나타나면 각 섹션 항목을 차례로 설정하세요.
   - **정보**: 출입문의 기본 정보를 설정하세요. 자세한 내용은 기본 정보 설정을 참고하세요.
   - **설정**: 출입문과 연결된 장치와 입실 및 퇴실 버튼, 출입문 센서를 설정하세요. 자세한 내용은 출입문 설정을 참고하세요.
   - **옵션**: 부가 옵션을 설정하세요. 자세한 내용은 부가 옵션 설정을 참고하세요.
   - **안티패스백**: 출입 이력을 관리하고 보안을 강화하기 위한 안티패스백 기능을 설정하세요. 자세한 내용은 안티패스백 설정을 참고하세요.
   - **시간 제한 안티패스백**: 안티패스백 기능의 초기화 시간을 설정할 수 있습니다. 자세한 내용은 시간 제한 안티패스백 설정을 참고하세요.

- **알람**: 안티패스백 위반이 발생했을 때 경보를 울리거나 장치를 사용하지 못하도록 설정할 수 있습니다. 자세한 내용은 알람 설정을 참고하세요.

5. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

기본 정보 설정

정보 섹션에서는 출입문의 이름 및 그룹, 설명을 입력하거나 변경할 수 있습니다.



- **이름**: 출입문의 이름을 입력하세요. 편리한 관리를 위해 특정할 수 있는 이름을 입력하세요.
- **그룹**: 출입문 그룹을 선택하세요.
- **설명**: 출입문에 대한 간단한 설명을 입력하세요.

> **알아두기**
>
> - 출입문 이름은 최대 48자까지 입력할 수 있습니다.
> - 출입문 그룹 등록에 대한 자세한 내용은 출입문 그룹 관리하기를 참고하세요.

출입문 설정

설정 섹션에서는 출입문과 연결된 장치와 퇴실 버튼, 출입문 세선 등을 설정할 수 있습니다.



- **입실 장치**: 입실할 때 사용할 장치를 선택하세요. 장치가 목록에 없다면 먼저 장치를 등록하세요.
- **출입문 릴레이**: 출입문 잠금 장치로 동작할 릴레이를 선택하세요.
- **퇴실 버튼**: 퇴실 버튼으로 사용할 포트를 선택하세요.
  - **스위치**: **N/C**(Normally Closed) 또는 **N/O**(Normally Open)으로 설정할 수 있습니다.
  - **릴레이 비활성**: 퇴실 버튼 입력 시 출입문 열림 요청 로그는 발생하지만 릴레이는 동작하지 않도록 설정할 수 있습니다.
- **출입문 센서**: 출입문 상태를 확인할 때 사용할 포트를 선택하세요. **없음**으로 설정하면 **알람** 섹션을 사용할 수 없습니다.
  - **스위치**: **N/C**(Normally Closed) 또는 **N/O**(Normally Open)으로 설정할 수 있습니다.
  - **출입 기반 APB 사용 시 센서 사용**: **출입 기반 APB** 옵션을 사용할 때 출입문 센서 사용 여부를 설정할 수 있습니다.

> **시간 제한 안티패스백**이 활성화되어 있다면 **출입 기반 APB 사용 시 센서 사용** 옵션은 사용할 수 없습니다.

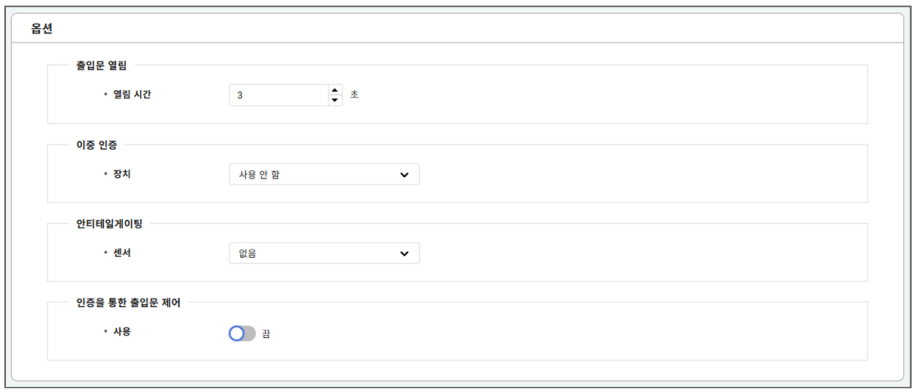
- **퇴실 장치**: 퇴실할 때 사용할 장치를 선택하세요.

알아두기

- **입실 장치**로 무선 도어락을 선택했다면 **퇴실 장치**에도 무선 도어락을 선택해야 합니다.
- **입실 장치**로 무선 도어락을 선택했다면 **출입문 릴레이** 옵션은 사용할 수 없습니다.
- CoreStation 모델은 입실 장치나 퇴실 장치로 사용할 수 없습니다.

부가 옵션 설정

옵션 섹션에서는 출입문에 대한 부가 옵션을 설정할 수 있습니다.



- **출입문 열림**: 출입문 열림에 대한 옵션을 설정하세요.
  - **열림 시간**: 인증 완료 후 출입문이 열린 상태로 유지되는 시간을 설정하세요. 이 시간이 지나면 출입문이 자동으로 잠깁니다.
  - **닫힘 시 잠금**: 출입문이 닫힌 것을 출입문 센서가 감지하면 출입문이 잠깁니다. **자동문 사용**을 **켬**으로 설정하면 사용할 수 없습니다.
  - **자동문 사용**: 자동문을 출입문으로 사용하면 출입문 센서의 상태와 상관없이 릴레이를 동작할 수 있습니다. **닫힘 시 잠금**을 **켬**으로 설정하면 사용할 수 없습니다.

  열림 시간은 사용하는 출입문 잠금 장치의 종류에 따라 다를 수 있습니다.

- **이중 인증**: 두 사람(일반 사용자와 관리자)이 크리덴셜을 인증하여 출입문을 열도록 설정할 수 있습니다.
  - **장치**: 이중 인증을 사용할 장치를 선택하세요. 이중 인증을 사용하지 않으려면 **사용 안 함**을 선택하세요.
  - **스케줄**: 이중 인증을 사용할 스케줄을 선택하세요. 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다.
  - **관리자 인증 순서**: 관리자 인증 순서를 설정하세요.
    - **사용 안 함**: 인증 그룹과 관계 없이 두 명의 인증이 필요합니다.
    - **마지막**: 일반 사용자가 인증하고 설정된 인증 그룹에 포함된 사용자가 인증해야 합니다.
  - **인증 그룹**: 관리자가 속한 그룹을 설정하세요. 이 옵션은 **관리자 인증 순서**을 **마지막**으로 선택했을 때 사용할 수 있습니다.
  - **인증 대기 시간**: 첫 번째 인증 후 두 번째 인증까지의 대기 시간을 설정하세요. 설정된 시간 내에 두 번째 인증이 완료되지 않으면 출입문이 열리지 않습니다.

- 재실 인원 제한 설정에 구성된 장치의 이중 인증을 변경하려면 다음 메뉴에서 설정을 수정하세요. **설정** → **출입 관리** → **고급 출입 통제** → **재실 인원 제한**

  재실 인원 제한 설정에 대한 자세한 내용은 고급 출입 통제 설정하기를 참고하세요.

- 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

- **안티테일게이팅**: 인증하지 않은 사람이 인증한 사람을 따라 출입하는 테일게이팅을 감지하도록 설정할 수 있습니다.
  - **센서**: 테일게이팅을 감지할 센서를 선택하세요.
- **인증을 통한 출입문 제어**: 권한이 있는 사용자가 더블 배지(Double Badge)하면 출입문을 상시 개방 상태로 전환하도록 설정할 수 있습니다. 자세한 내용은 인증을 통한 출입문 제어 설정하기를 참고하세요.

새 출입문을 추가하는 화면에서는 출입문이 아직 출입 그룹에 포함되어 있지 않아 이 설정을 사용할 수 없습니다. 출입문을 저장하고 출입 그룹에 포함한 뒤 출입문 정보 수정 화면에서 설정하세요.

안티패스백 설정

안티패스백은 출입 이력을 관리하고 보안을 강화하기 위해 사용합니다. 사용자가 출입 카드로 입실 후 다른 사용자에게 카드를 넘겨주는 악용 사례를 막을 수 있으며, 외부인이 출입 권한을 가진 사용자를 뒤따라 들어올 때 나가지 못하도록 막을 수 있습니다.

아래를 참고하여 **안티패스백** 섹션에서 설정을 완료하세요.

- **종류**: 안티패스백 종류를 선택하세요.
  - **사용 안 함**: 안티패스백 기능을 사용하지 않습니다.
  - **소프트 안티패스백**: 안티패스백을 위반하면 출입은 가능하지만 경보를 울리거나 **BioStar X**에 로그를 생성합니다.
  - **하드 안티패스백**: 안티패스백을 위반하면 출입할 수 없으며 경보를 울리거나 **BioStar X**에 로그를 생성합니다.
- **초기화 시간**: 안티패스백 기능이 초기화될 때까지의 시간을 설정하세요. 최대 7일(10080분)까지 설정할 수 있으며, 0으로 설정하면 초기화되지 않습니다.

알아두기

- 입실 장치와 퇴실 장치가 모두 설치된 경우 사용할 수 있으며, **설정** 섹션에서 **퇴실 장치** 옵션을 **없음**으로 설정하면 사용할 수 없습니다. 퇴실 장치 설정 방법은 출입문 설정을 참고하세요.
- **안티패스백** 섹션을 활성화하려면 RS-485로 구성된 마스터 장치와 슬레이브 장치가 필요합니다.
- **시간 제한 안티패스백** 섹션이 활성화되어 있으면 **안티패스백**을 사용할 수 없습니다.

시간 제한 안티패스백 설정

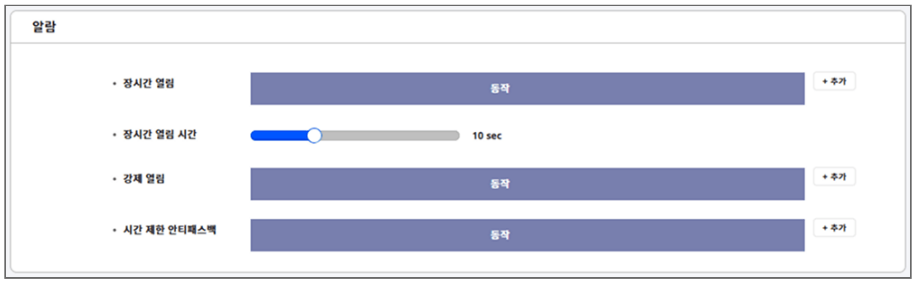
사용자가 출입 인증 후 동일한 장치에서 다시 인증을 시도할 때, 안티패스백 기능이 작동하여 즉시 재인증할 수 없습니다. **시간 제한 안티패스백** 섹션에서는 안티패스백 기능의 초기화 시간을 설정하여 사용자의 빈번한 입실을 효과적으로 제한할 수 있습니다.



- **시간 제한 안티패스백**: 시간 제한 안티패스백 기능을 사용할 장치를 선택하세요.
- **초기화 시간**: 안티패스백 기능이 초기화될 때까지의 시간을 설정하세요. 입력 단위는 분(min)이며 기본값은 10분입니다. 최대 60분까지 설정할 수 있습니다.
- **항시 통과 그룹**: 시간 제한 안티패스백 기능을 제한받지 않고 항상 통과할 수 있는 출입 그룹을 선택할 수 있습니다.

알람 설정

알람 섹션에서는 출입문이 강제로 열리거나, 열린 채로 방치되었거나 안티패스백 위반이 발생했을 때 경보를 울리거나 장치를 사용하지 못하도록 막을 수 있습니다. 알람을 추가할 항목에서 **+ 추가** 버튼을 클릭하세요.



- **장시간 열림**: 출입문이 열린 채로 방치되었을 때 알람 동작을 설정하세요.
- **장시간 열림 시간**: 장시간 출입문이 열렸을 경우 경보를 울리는 시간을 설정하세요. 출입문이 열려 있을 수 있는 최대 시간을 설정하세요.
- **강제 열림**: 강제로 출입문이 열렸을 때 알람 동작을 설정하세요.
- **안티패스백** / **시간 제한 안티패스백**: 안티패스백 또는 시간 제한 안티패스백 위반이 발생했을 때 알람 동작을 설정하세요.

> **알아두기**
> **안티패스백** 옵션은 퇴실 장치가 등록되어 있어야 설정할 수 있습니다.

출입문 정보 수정하기

등록된 출입문의 설정 정보를 수정하는 방법을 안내합니다. 개별 출입문의 상세 설정을 변경하거나, 여러 출입문을 선택하여 공통 항목을 일괄 수정할 수 있습니다.

한 개의 출입문 정보 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 정보를 수정하려는 출입문을 클릭하세요.
4. 각 섹션의 세부 항목을 수정하세요.
5. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 출입문 정보 수정 화면의 각 섹션에 대한 자세한 내용은 출입문 등록하기를 참고하세요.
- 출입문이 출입 그룹에 포함된 이후에는 **인증을 통한 출입문 제어** 기능을 설정할 수 있습니다. 자세한 내용은 인증을 통한 출입문 제어 설정하기를 참고하세요.

여러 개의 출입문 일괄 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 정보를 수정하려는 출입문의 체크박스를 클릭하세요. 두 개 이상의 출입문을 선택하세요.
4. 화면 오른쪽 상단에 **일괄 편집** 버튼을 클릭하세요.
5. **일괄 편집** 창이 나타나면 원하는 옵션을 설정하세요.



- **열림 시간**: 인증 완료 후 출입문이 열린 상태로 유지되는 시간을 설정하세요. 이 시간이 지나면 출입문이 자동으로 잠깁니다.

6. 설정을 모두 완료했다면 **확인** 버튼을 클릭하세요.

알아두기

일괄 편집 버튼은 출입문 목록에서 두 개 이상의 출입문을 선택해야 활성화됩니다.

인증을 통한 출입문 제어 설정하기

인증을 통한 출입문 제어는 지정된 사용자가 지원 장치에 동일한 카드로 연속 두 번 인증(더블 배지, Double Badge)하면 해당 출입문을 상시 개방 상태로 전환하는 기능입니다. 상시 개방 상태에서 다시 더블 배지하거나 허용된 스케줄이 종료되면 출입문은 원래의 모드로 자동 복귀합니다.

시작하기 전에

- 출입문이 출입 그룹에 포함되어 있어야 합니다. 새 출입문을 추가하는 화면에서는 아직 출입 그룹에 포함되어 있지 않아 이 기능을 사용할 수 없습니다. 출입문을 저장한 뒤 출입 그룹에 포함하고, 출입문 정보 수정 화면에서 이 기능을 설정하세요. 출입 그룹 설정에 대한 자세한 내용은 출입 통제 설정하기를 참고하세요.
- 출입문 등록 및 정보 수정에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 출입문 등록하기

- 출입문 정보 수정하기

> **알아두기**
>
> - 인증을 통한 출입문 제어는 다음 장치와 펌웨어 버전부터 지원합니다. 이 기능은 지원하는 장치로 구성된 출입문에서 사용할 수 있습니다.
>   - XPass 2 펌웨어 1.5.3 이상
>   - FaceStation F2 펌웨어 2.3.0 이상
> - 카드 계열 크리덴셜(CSN, Wiegand, 스마트 카드, 모바일 카드의 CSN/ToM)에서만 동작합니다. 템플릿 크리덴셜이나 지문, 얼굴 등 생체 인증은 대상이 아니며 일반 출입 인증으로 처리됩니다.
> - 인증을 통한 출입문 제어는 장치의 인증 모드가 카드 인증 모드일 때만 동작합니다. **BioStar X**는 장치의 인증 모드를 확인하지 않으므로 기능을 사용하기 전에 장치의 인증 모드를 직접 확인하세요.
> - 장치는 첫 번째 인증과 두 번째 인증의 간격이 3초 이내일 때만 더블 배지로 인식됩니다. 간격이 3초를 초과하면 장치는 두 인증을 각각 개별 출입 인증으로 처리합니다.

인증을 통한 출입문 제어 설정

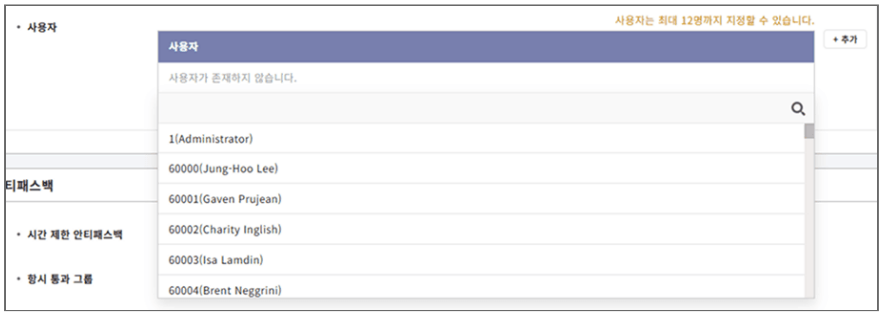
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 설정하려는 출입문을 클릭하세요.
4. **옵션** 섹션에서 **인증을 통한 출입문 제어** 항목으로 이동하세요.



5. **사용** 옵션을 **켬**으로 설정하세요.



6. **스케줄**에서 이 기능을 사용할 스케줄을 선택하세요. 기본값은 **Always**입니다. 원하는 스케줄이 없다면 스케줄을 먼저 추가하세요.
7. 더블 배지로 출입문을 제어할 수 있는 사용자를 추가하려면 **+ 추가** 버튼을 클릭하고, **사용자** 목록에서 선택하세요.



- **사용자** 목록에는 해당 출입문에 대한 출입 권한이 있는 사용자만 표시됩니다. **설정** → **출입 관리** → **출입 통제**에서 출입 그룹과 출입 등급을 확인하세요.
- 사용자는 최대 12명까지 지정할 수 있습니다.
- 원하는 사용자를 검색하려면 Q 버튼을 클릭하세요.
- 사용자 그룹 단위로는 지정할 수 없으며 개별 사용자만 선택할 수 있습니다.

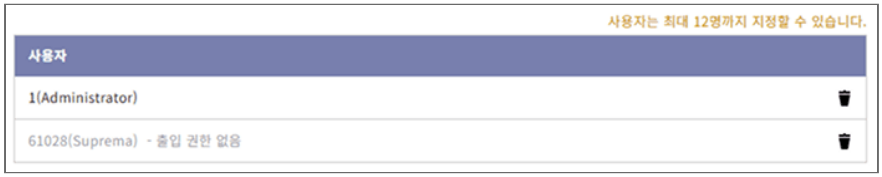
8. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 스케줄 추가에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
- 출입 그룹과 출입 등급 설정에 대한 자세한 내용은 출입 통제 설정하기를 참고하세요.

유의 사항

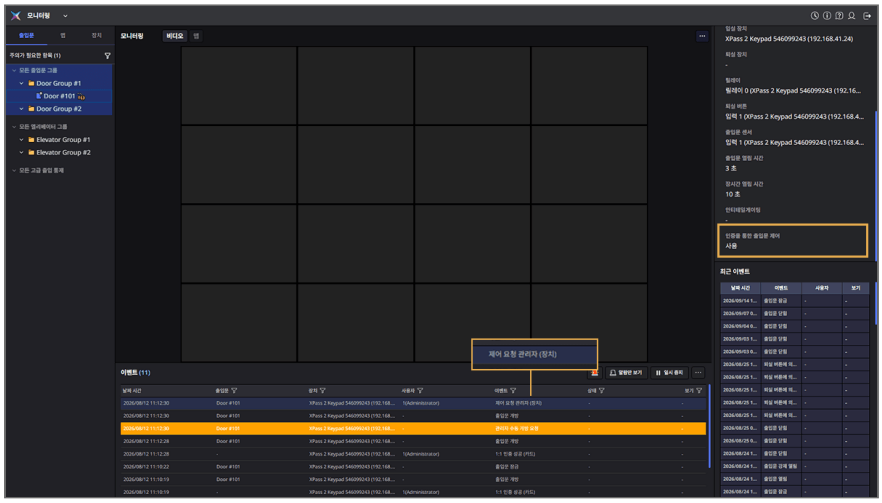
- 인증을 통한 출입문 제어를 사용 중인 출입문은 입실 장치 또는 퇴실 장치를 미지원 모델로 변경할 수 없습니다. 장치를 변경하려면 먼저 **인증을 통한 출입문 제어** 옵션을 **끔**으로 설정하세요.
- 제어 권한 사용자로 지정된 사용자가 출입 그룹 변경 등으로 해당 출입문의 출입 권한을 잃으면 목록에 **출입 권한 없음** 상태로 구분되어 표시됩니다. 이 상태에서는 저장할 수 없으므로 출입 권한을 다시 부여하거나 목록에서 제거하세요.



- 제어 권한 사용자를 한 명도 지정하지 않은 상태에서는 저장할 수 없습니다.
- 지정한 스케줄이 삭제되면 **스케줄** 항목에 **삭제된 스케줄**로 표시됩니다. 이 상태에서는 저장할 수 없으므로 다른 스케줄을 선택하세요.
- 안티패스백 위반이 발생하면 출입이 거부되는 하드(Hard) 모드에서는 인증을 통한 출입문 제어가 동작하지 않고, 출입이 허용되는 소프트(Soft) 모드에서는 동작합니다.
- 화재 경보, 스케줄 잠금, 스케줄 개방 등 다른 고급 출입 통제 기능이 함께 적용된 상태에서는 적용된 고급 출입 통제 기능이 우선합니다.

참고 사항

- 인증을 통한 출입문 제어 상태는 **모니터링** 화면의 출입문 미리보기 패널에서 확인할 수 있으며, 인증을 통한 출입문 제어로 발생한 기록은 **이벤트** 목록에서 **제어 요청 관리자**로 표시됩니다. 출입문 모니터링에 대한 자세한 내용은 출입문 모니터링하기를 참고하세요.

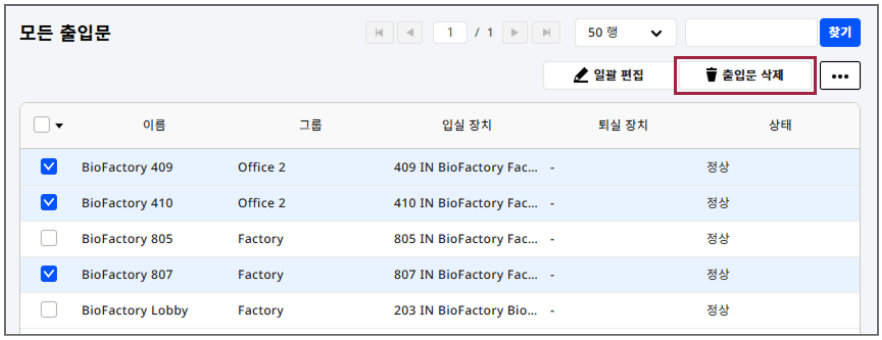


- 설정 변경 이력은 감사 추적에 기록됩니다. 자세한 내용은 출입 통제 감사 로그 조회하기를 참고하세요.

출입문 삭제하기

등록된 출입문을 삭제하는 방법을 안내합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **출입문**를 클릭하세요.
3. 출입문 목록에서 삭제하려는 출입문의 체크박스를 클릭하세요.
4. 화면 오른쪽 상단의 **출입문 삭제** 버튼을 클릭하세요.



5. 확인 메시지 창이 나타나면 **네** 버튼을 클릭하세요.

선택한 출입문이 삭제됩니다. 삭제된 출입문은 복구할 수 없습니다.

> **알아두기**
> **출입문 삭제** 버튼은 출입문 목록에서 한 개 이상의 출입문을 선택해야 활성화됩니다.

운영 권한 관리하기

등록한 사용자에게 운영 권한을 부여하고 커스텀 권한을 추가 및 설정하는 방법을 안내합니다. 운영 권한은 사용자가 **Biostar X**에서 수행할 수 있는 작업을 제어하는 기능입니다. **커스텀 권한**은 기본 운영 권한 외에 추가적인 권한을 설정할 수 있는 기능입니다.

권한 종류 확인하기

런처 페이지에서 **설정**을 클릭하세요. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요. 권한 등급에 따라 기본 제공하는 계정을 참고하세요.

- **전체 관리자**: 모든 메뉴를 사용할 수 있는 관리자 등급입니다.
- **사용자 관리자**: **사용자** 메뉴에 대한 **읽기, 수정** 권한을 가집니다. **사용자** 메뉴 외 다른 설정 그룹에 대한 권한은 없습니다.
- **모니터링 관리자**: **모니터링**과 **데이터** 메뉴에 대한 **읽기, 수정** 권한을 가지며, **대시보드** 메뉴에 대한 **읽기** 권한을 가집니다.
- **근태 관리자**: **근태 관리** 메뉴에 대한 **읽기, 수정** 권한을 가지며, **사용자** 메뉴에 대한 **읽기** 권한을 가집니다.
- **방문자 관리자**: **방문자** 메뉴에서 **읽기, 수정** 권한을 가집니다.

> **알아두기**
>
> - **모니터링** 메뉴의 **수정** 권한은 탭을 추가하거나 상태 트리 항목을 제어할 수 있습니다.
> - **데이터** 메뉴의 **수정** 권한은 보고서 저장 및 자동 보고서 일정 추가, 설정에 접근할 수 있습니다.
> - 사전 정의된 사용자 권한 외 새로운 사용자 권한을 추가하려면 커스텀 권한 추가하기를 참고하세요.
> - 기본 제공하는 계정의 권한은 수정하거나 삭제할 수 없습니다.
> - **근태 관리자** 및 **방문자 관리자** 등급은 별도의 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

사용자에게 운영 권한 부여하기

일반 사용자에게 운영 권한을 부여하는 방법을 안내합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요.
3. 계정 목록에서 원하는 항목을 클릭하세요.
4. **권한 부여** 옵션에서 **+ 추가** 버튼을 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

5. 사용자 목록에서 운영 권한을 부여할 사용자를 선택하세요.
6. 원하는 사용자를 모두 선택했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 사용자가 많아 찾기 어려울 때 🔍 버튼을 클릭해 원하는 사용자를 검색하고 선택할 수 있습니다.
- 운영 권한은 사용자 정보를 추가 또는 수정할 때 부여할 수도 있습니다. 자세한 내용은 사용자 권한 설정하기를 참고하세요.
- 사용자 정보를 추가 또는 수정할 때 권한을 이미 설정했다면 **권한 부여** 옵션에는 추가되어 있습니다.

운영 권한 제외하기

사용자에게 부여한 운영 권한을 제외하는 방법을 안내합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요.
3. 계정 목록에서 원하는 계정 종류를 클릭하세요.
4. **권한 부여** 옵션에서 운영을 제외할 사용자의 🗑 버튼을 클릭하세요.

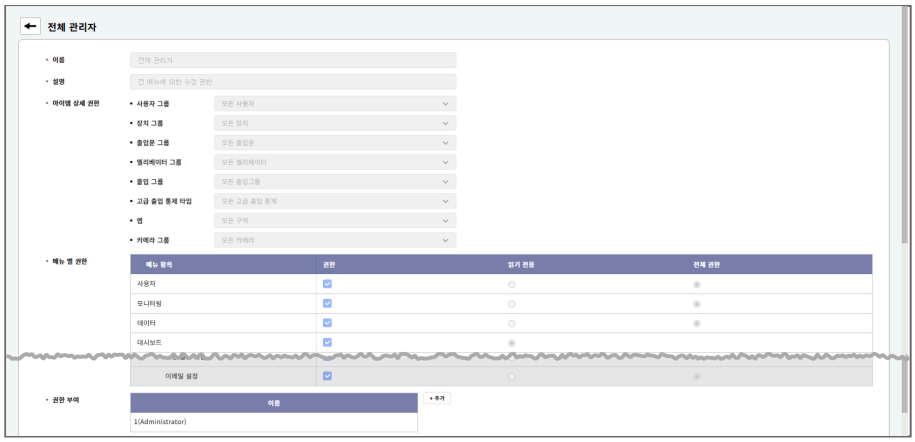


위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

5. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

운영 권한 상세 정보 확인하기

계정 메뉴의 계정 목록에서 계정을 클릭하면 해당 계정의 운영 권한 상세 정보를 확인할 수 있습니다.



- **이름**: 선택한 운영 권한의 이름입니다.
- **설명**: 권한에 대한 간략한 설명을 확인할 수 있습니다.
- **아이템 상세 권한**: 아이템별 권한이 부여된 그룹을 확인할 수 있습니다.
- **메뉴 별 권한**: 메뉴에 접근할 수 있는 권한을 확인할 수 있습니다.

  - **읽기 전용**: 해당 메뉴의 항목을 추가, 편집, 삭제할 수 있는 권한을 부여합니다.
  - **전체 권한**: 해당 메뉴를 진입하여 설정 내용을 확인만 할 수 있는 권한을 부여합니다.

- **권한 부여**: 권한이 부여된 사용자를 확인할 수 있습니다.

> **알아두기**
> 특정 사용자에게 권한을 부여하는 방법은 사용자에게 운영 권한 부여하기를 참고하세요.

커스텀 권한 추가하기

사용자가 원하는 권한 등급을 추가하는 방법을 안내합니다. 커스텀 권한은 기본 제공하는 운영 권한 외에 추가적인 권한을 설정할 수 있는 사용자 맞춤형 기능입니다.

커스텀 권한 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요.
3. **커스텀 권한 추가** 버튼을 클릭하세요.



4. 새로 생성하는 권한에 대한 이름과 설명을 입력하세요.



5. 나머지 각 항목을 입력하거나 선택하세요.
6. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 활성화된 라이선스 종류에 따라 설정할 수 있는 **메뉴 별 권한**은 다를 수 있습니다.
- **아이템 상세 권한**에 대한 자세한 내용은 detailSetting을 참고하세요.
- **메뉴 별 권한**에 대한 자세한 내용은 menuSetting을 참고하세요.
- **권한 부여**에 대한 자세한 내용은 addUser를 참고하세요.

아이템 상세 권한

아이템에 대한 상세 권한을 설정하세요. 각 메뉴에 대한 수정 및 보기 권한을 부여할 그룹을 선택할 수 있습니다. 아이템 상세 권한은 **사용자 그룹**, **장치 그룹**, **출입문 그룹**, **출입 그룹**에 대해 설정할 수 있으며, 각 메뉴에서 이미 생성되어 있는 그룹 정보를 기준으로 설정할 수 있습니다.

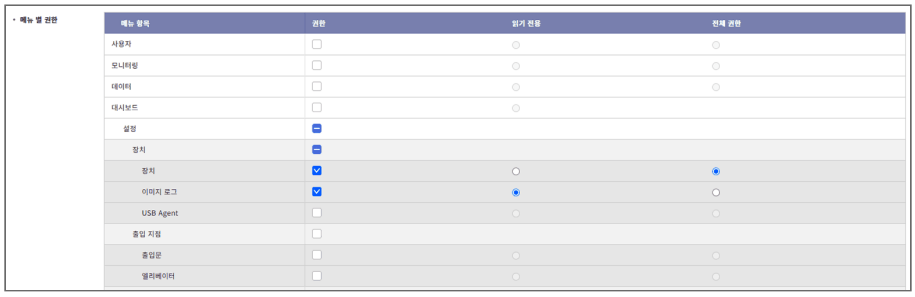


알아두기

- 원하는 그룹이 없을 경우 해당 메뉴로 이동하여 새 그룹을 추가하세요. 그룹 추가에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 사용자 그룹 관리하기
  - 장치 그룹 관리하기
  - 출입문 그룹 관리하기
  - 엘리베이터 그룹 관리하기
  - 출입 그룹 관리하기
- **맵** 권한은 **에센셜**(Essential) 라이선스 이상에서 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- **엘리베이터 그룹**, **고급 출입 통제 타입**, **카메라 그룹** 권한은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

메뉴 별 권한

개별 메뉴에 대한 **읽기 전용** 또는 **전체 권한**을 선택할 수 있습니다. 메뉴마다 다른 권한을 부여할 수 있습니다. 권한을 부여할 메뉴의 **권한** 체크박스를 클릭하고 **읽기 전용** 또는 **전체 권한**을 선택하세요.



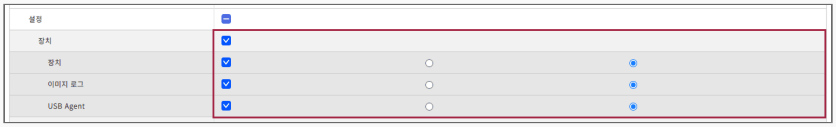
- **읽기 전용**: 해당 메뉴를 진입하여 설정 내용을 확인만 할 수 있는 권한을 부여합니다.
- **전체 권한**: 해당 메뉴의 항목을 추가, 편집, 삭제할 수 있는 권한을 부여합니다.

알아두기

- **모니터링** 메뉴의 **전체 권한**은 탭을 추가하거나 상태 트리 항목을 제어할 수 있습니다.
- **데이터** 메뉴의 **전체 권한**은 보고서 저장 및 자동 보고서 일정 추가, 설정에 접근할 수 있습니다.
- **대시보드** 메뉴의 **읽기 전용** 권한만으로도 새 대시보드와 위젯을 생성할 수 있습니다.
- **메뉴 항목** 목록에 없는 메뉴는 권한과 무관하게 진입할 수 있습니다.

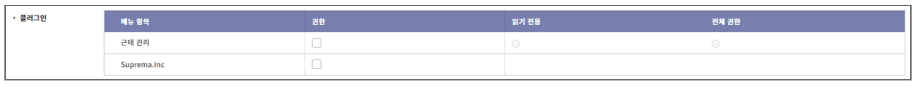
팁

상위 메뉴의 권한을 클릭하면 하위 모든 메뉴에 대한 권한이 활성화됩니다.



플러그인

플러그인을 추가했다면 플러그인 권한을 설정할 수 있습니다. 플러그인 권한이 없는 사용자는 해당 플러그인에 대한 접근할 수 없으며, 초기 화면이나 런처에 표시되지 않습니다.



알아두기

- 플러그인 기능을 사용하려면 플러그인 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- **근태 관리** 플러그인에만 **읽기 전용** 또는 **전체 권한**을 적용할 수 있습니다.

권한 부여

권한을 부여할 사용자 정보를 추가하거나 확인할 수 있습니다. 사용자를 추가하려면 **+ 추가** 버튼을 클릭하세요. 사용자 목록에서 권한을 부여할 사용자를 선택하세요.



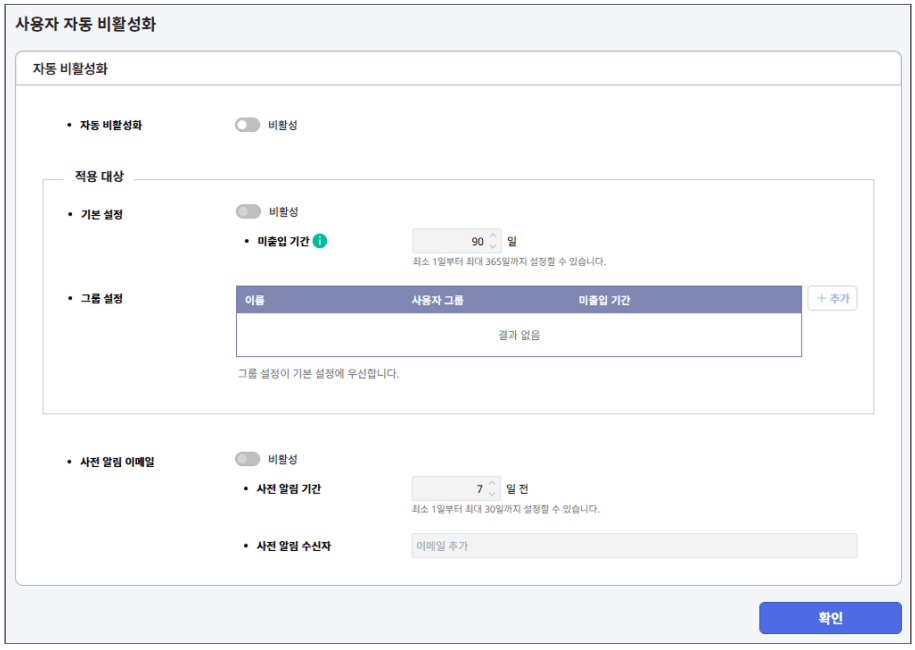
알아두기

사용자 목록에서 사용자의 버튼을 클릭하면 해당 사용자는 권한에서 제외됩니다.

장기 미출입자 조치하기

퇴사, 휴직 등으로 오랫동안 출입하지 않는 사용자의 크리덴셜을 그대로 두면 도용이나 무단 출입과 같은 보안 위협으로 이어질 수 있습니다. 자동 비활성화 기능을 사용하면 마지막 출입 이후 일정 기간이 지난 사용자를 자동으로 비활성화하여 관리자가 매번 수동으로 정리하지 않아도 사용자 계정을 안전하게 관리할 수 있습니다. 자동으로 비활성화되기 전에는 지정한 수신자에게 사전 알림 이메일을 보내 미리 검토하거나 예외 처리할 시간을 확보할 수 있습니다.

런처 페이지에서 **설정**을 클릭하세요. 화면 왼쪽 사이드바에서 **계정** → **사용자 자동 비활성화**를 클릭하세요.



알아두기

계정 → **사용자 자동 비활성화** 메뉴는 해당 메뉴 권한이 있는 관리자만 접근할 수 있습니다. 특정 메뉴에 대한 권한을 관리자에게 적용하려면 운영 권한 관리하기를 참고하세요.

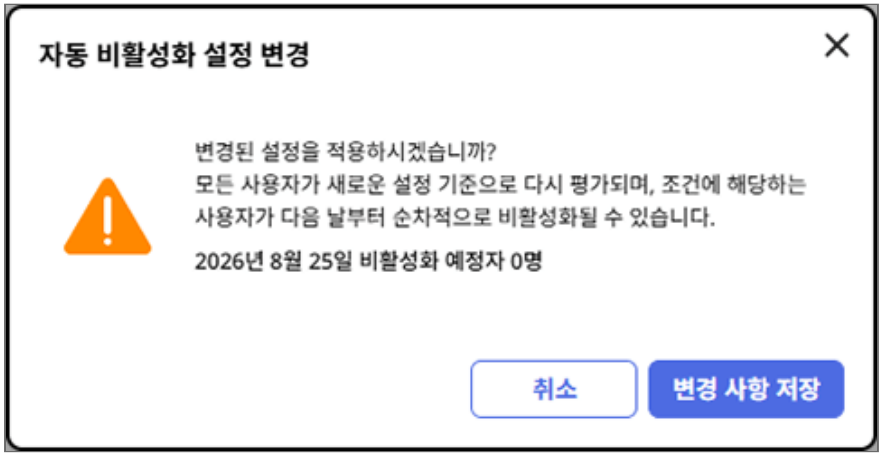
자동 비활성화 설정

1. **자동 비활성화** 옵션에서 토글 버튼을 클릭해 활성화하세요.
2. **적용 대상** 섹션에서 자동 비활성화 적용 대상을 설정하세요.



- 모든 사용자에게 동일한 기준을 적용하려면 **기본 설정** 옵션에서 토글 버튼을 클릭해 활성화하고 **미출입 기간**을 입력하세요. 최소 1일부터 최대 365일까지 설정할 수 있습니다.
- 특정 사용자 그룹에 다른 기준을 적용하려면 **그룹 설정**을 추가하세요. 추가 방법은 그룹별 다른 기준 적용를 참고하세요.

3. 설정을 완료했다면 화면 가장 아래의 **확인** 버튼을 클릭하세요.
4. 확인 창이 나타나면 다음 자동 처리 예정일과 비활성화 예정 사용자 수를 확인하고 **변경 사항 저장** 버튼을 클릭하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

알아두기

- 사용자가 자동으로 비활성화되기 전에 지정한 수신자에게 이메일로 미리 알리려면 **사전 알림 이메일**에서 설정할 수 있습니다. 자세한 내용은 사전 알림 이메일 설정을 참고하세요.
- **자동 비활성화** 옵션을 활성화해도 **기본 설정** 옵션은 자동으로 활성화되지 않습니다. **그룹 설정**만으로 정책을 구성하려면 **기본 설정** 옵션은 비활성 상태로 두세요.
- 자동 비활성화는 마지막 출입 인증 시각을 기준으로 판정합니다. 출입 기록이 없거나 사용자 등록 이전의 출입 이력만 있는 사용자는 비활성화 대상에서 제외됩니다.
- 한 사용자가 **기본 설정**과 **그룹 설정**에 모두 해당하면 **그룹 설정**의 **미출입 기간**이 우선 적용됩니다. 2개 이상의 **그룹 설정**에 속한다면 그중 가장 짧은 **미출입 기간**이 적용됩니다.
- 자동 비활성화는 하루 1회(자정) 실행됩니다. 설정을 변경해도 즉시 반영되지 않고 다음 처리 시점부터 적용되며, 이미 발송된 사전 알림 일정에는 영향을 주지 않습니다.
- **자동 비활성화** 옵션을 비활성 상태로 변경할 때는 확인 창 없이 바로 저장됩니다.

그룹별 다른 기준 적용

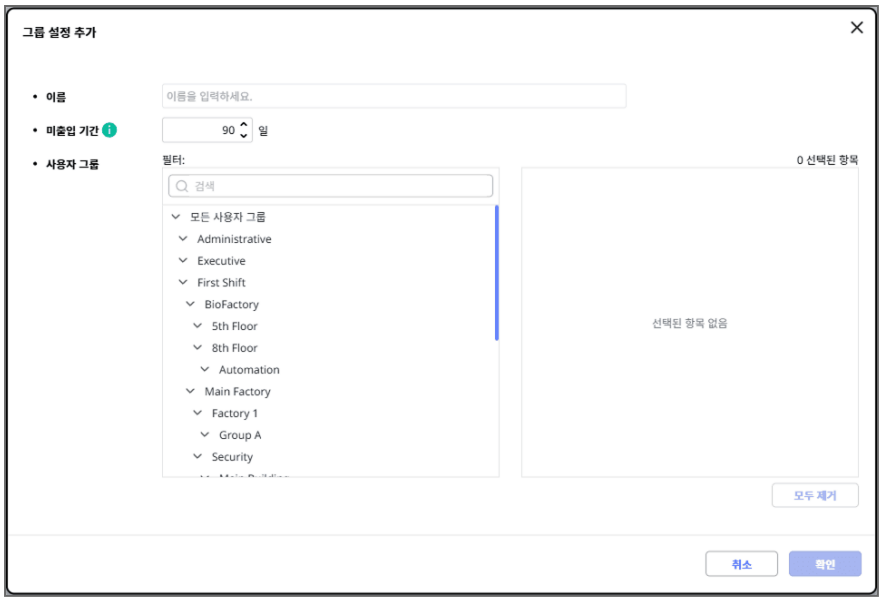
특정 사용자 그룹에는 **기본 설정**과 다른 **미출입 기간**을 적용할 수 있습니다.

그룹 설정 추가

1. **그룹 설정** 목록 오른쪽의 **+ 추가** 버튼을 클릭하세요.



2. **그룹 설정 추가** 창이 나타나면 각 항목을 설정하세요.



   - **이름**: 다른 그룹 설정과 중복되지 않는 이름을 입력하세요. 대소문자와 앞뒤 공백은 구분하지 않습니다.
   - **미출입 기간**: 최소 1일부터 최대 365일까지 설정할 수 있습니다.
   - **사용자 그룹**: 적용할 사용자 그룹을 선택하세요. 그룹을 선택하면 하위 사용자 그룹도 함께 선택됩니다.
3. 사용자 그룹 선택을 완료하면 **확인** 버튼을 클릭하세요.
4. 변경 사항을 저장하려면 화면 가장 아래의 **확인** 버튼을 클릭하세요.
5. 확인 창이 나타나면 다음 자동 처리 예정일과 비활성화 예정 사용자 수를 확인하고 **변경 사항 저장** 버튼을 클릭하세요.

> **알아두기**
>
> - **사용자 그룹**에서 관리자의 권한 범위를 벗어난 사용자 그룹은 선택할 수 없도록 비활성화되어 표시되며, 목록에서 숨겨지지는 않습니다. 이 그룹은 펼쳐볼 수 있으며, 하위 그룹 중 권한 범위 안에 있는 그룹은 선택할 수 있습니다.
> - 관리자 권한이 **모든 사용자**로 설정된 관리자 또는 전체 관리자는 사용자 그룹 선택에 제한이 없습니다. 관리자 권한에 대한 자세한 내용은 운영 권한 관리하기를 참고하세요.

그룹 설정 수정 및 삭제



- 수정하려면 **그룹 설정** 목록에서 원하는 행의 버튼을 클릭하고 값을 변경한 뒤 **확인** 버튼을 클릭하세요.
- 삭제하려면 원하는 행의 버튼을 클릭하세요. 확인 메시지가 나타나면 **삭제** 버튼을 클릭하세요.

수정 또는 삭제한 내용을 저장하려면 화면 가장 아래의 **확인** 버튼을 클릭하세요. 확인 창이 나타나면 다음 자동 처리 예정일과 비활성화 예정 사용자 수를 확인하고 **변경 사항 저장** 버튼을 클릭하세요.

> **알아두기**
>
> - **그룹 설정**에 관리자의 권한 범위를 벗어난 사용자 그룹이 포함되어 있다면, 목록에는 계속 표시되지만 수정 및 삭제할 수 없습니다.
> - **그룹 설정**이 **기본 설정** 보다 우선합니다.
> - **그룹 설정**을 삭제해도 이미 비활성화된 사용자는 복구되지 않습니다. 삭제 후에는 해당 사용자에게 적용 가능한 다른 설정(**기본 설정** 등)이 있으면 그 설정으로 전환됩니다.

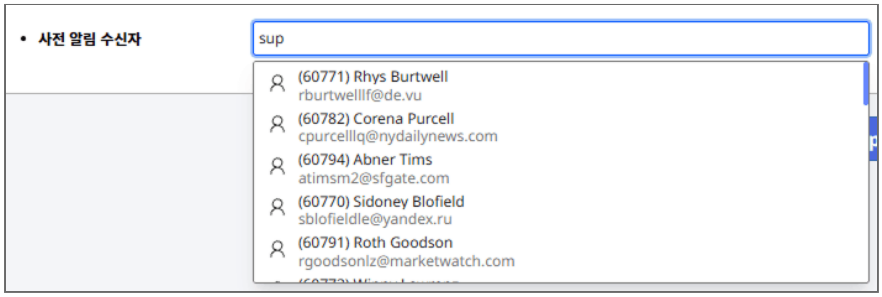
사전 알림 이메일 설정

사용자가 자동으로 비활성화되기 전에 지정한 수신자에게 이메일로 미리 알릴 수 있습니다.

1. **사전 알림 이메일** 옵션에서 토글 버튼을 클릭해 활성화하세요.



2. **사전 알림 기간**을 입력하세요. 입력한 기간만큼 자동 비활성화 알림 메일이 발송됩니다. 최소 1일부터 최대 30일까지 설정할 수 있습니다.
3. **사전 알림 수신자** 입력 필드에 이름, ID, 이메일로 사용자를 검색해 선택하거나 이메일 주소를 직접 입력하고 Enter 키를 누르세요.



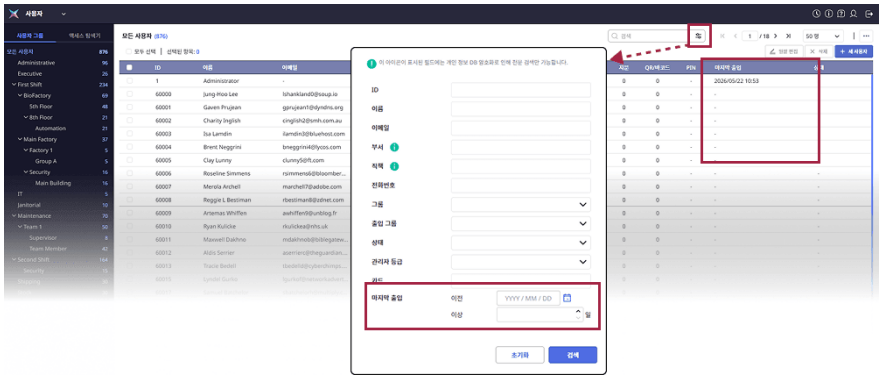
4. 설정을 완료했다면 화면 가장 아래의 **확인** 버튼을 클릭하세요.
5. 확인 창이 나타나면 다음 자동 처리 예정일과 비활성화 예정 사용자 수를 확인하고 **변경 사항 저장** 버튼을 클릭하세요.

알아두기

- 사전 알림 이메일을 사용하려면 SMTP 설정이 완료되어 있어야 합니다. 자세한 내용은 이메일 설정하기를 참고하세요.
- **사전 알림 기간**은 **기본 설정**과 모든 **그룹 설정**의 미출입 기간보다 짧게 설정해야 합니다.
- **BioStar X**에 등록되지 않은 이메일 주소도 수신자로 추가할 수 있습니다.
- 비활성화 예정 사용자는 사용자별 개별 메일이 아닌 하루 1회 통합 메일로 발송됩니다.
- **기본 설정**이 비활성 상태이고 **그룹 설정**도 없는 상태에서 **사전 알림 이메일**만 활성화하면, 적용 대상이 없어 실제로 메일이 발송되지 않습니다.

관련 정보

- 장기 미출입 사용자는 사용자 목록의 **마지막 출입** 열이나 고급 검색으로 조회할 수 있습니다. 자세한 내용은 사용자 탐색하기를 참고하세요.

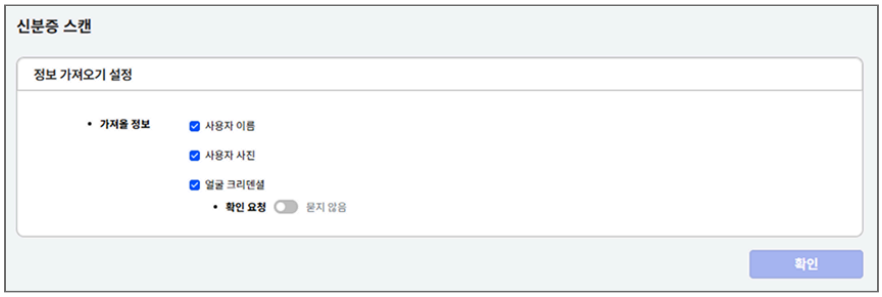


- 자동 및 수동으로 비활성화된 사용자 이력은 **비활성 사용자** 리포트에서 확인할 수 있습니다. 자세한 내용은 리포트 생성하기를 참고하세요.

신분증 스캔 설정하기

신분증 스캔으로 사용자를 등록하기 전에, 스캔 시 가져올 사용자 이름, 프로필 이미지와 얼굴 크리덴셜 등록 방식을 미리 설정해야 합니다. 이 문서에서는 신분증 스캔 설정 방법을 안내합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **신분증 스캔**을 클릭하세요.



3. 신분증을 스캔할 때 가져올 데이터를 선택하세요.
   - **사용자 이름**: 신분증에 기재된 이름을 가져옵니다.
   - **사용자 사진**: 신분증에 기재된 프로필 이미지를 가져옵니다.

- **얼굴 크리덴셜**: 신분증에 기재된 얼굴 이미지를 얼굴 크리덴셜로 등록합니다.
  - **확인 요청**: 신분증에 기재된 얼굴 이미지를 얼굴 크리덴셜로 등록할 때 항상 확인합니다.
  - **묻지 않음**: 신분증에 기재된 얼굴 이미지를 얼굴 크리덴셜로 등록할 때 확인하지 않고 등록할 수 있습니다.

4. 설정을 저장하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **사용자 사진** 옵션이 선택되어 있지 않으면 **얼굴 크리덴셜** 옵션을 선택할 수 없습니다.
> - 신분증을 스캔해 사용자를 등록하거나 수정하는 방법에 대한 자세한 내용은 신분증 스캔으로 사용자 등록 및 수정하기를 참고하세요.

출입 통제 설정하기

출입 통제 시스템을 설정하는 방법을 안내합니다. 출입문과 출입 시간을 설정하여 출입 등급을 생성하고, 출입 등급과 사용자 그룹 정보로 출입 그룹을 설정할 수 있습니다. 설정한 출입 그룹은 출입 통제 구성에 사용합니다.

출입 등급 관리하기

출입 등급은 사용자가 출입할 수 있는 시간을 설정하고, 이 시간 동안 출입문에 출입할 수 있는 권리입니다. 출입 등급은 출입 그룹을 설정하기 위한 주요 요소입니다.

시작하기 전에

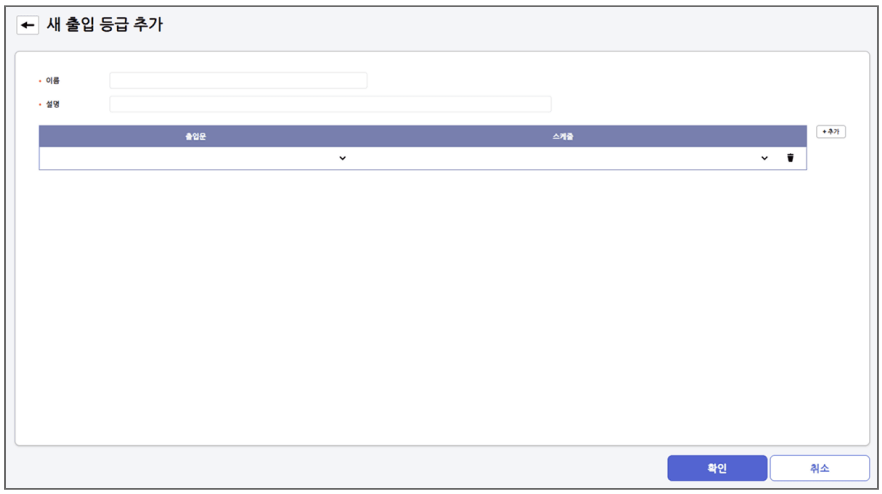
- 출입 등급을 등록하기 전에 출입문을 설정해야 합니다. 출입문 등록에 대한 자세한 내용은 출입문 등록하기를 참고하세요.
- 스케줄 설정을 통해 출입 등급에 적용할 시간을 미리 정의할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

출입 등급 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**를 클릭하세요.
3. **출입 등급 추가** 버튼을 클릭하세요.



4. **새 출입 등급 추가** 화면에서 **이름**과 **설명**을 입력하세요.



5. **출입문** 항목에서 출입 등급에 적용할 출입문을 선택하세요.
6. **스케줄** 항목에서 출입 등급에 적용할 스케줄을 선택하세요.
7. 출입 등급을 등록하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 출입 등급은 출입 그룹당 최대 128개까지 등록할 수 있습니다.
- **출입문**과 **스케줄** 항목에서 🔍 버튼을 클릭하면 원하는 출입문과 스케줄을 검색할 수 있습니다.
- **출입문**과 **스케줄** 항목에서 추가한 항목을 삭제하려면 🗑 버튼을 클릭하세요.
- 원하는 출입문이 없다면 새로운 출입문을 등록해야 합니다. 출입문 등록에 대한 자세한 내용은 출입문 등록하기를 참고하세요.
- 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

출입 등급 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **출입 등급** 탭을 클릭하세요.



4. 출입 등급 목록에서 수정할 출입 등급을 클릭하세요.
5. 원하는 항목을 수정하세요.
6. 수정을 완료하면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

출입 등급 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **출입 등급** 탭을 클릭하세요.
4. 출입 등급 목록에서 삭제할 출입 등급의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단에 있는 **출입 등급 삭제** 버튼을 클릭하세요.



출입 그룹 관리하기

출입 등급과 사용자 그룹 정보를 사용해 출입 그룹을 설정하는 방법을 안내합니다. 출입 그룹은 출입문에 출입할 수 있는 권한을 설정하는 중요한 요소입니다. 출입 그룹을 설정하면 사용자가 출입문에 출입할 수 있는 권한을 관리할 수 있습니다.

시작하기 전에

출입 그룹을 등록하기 전에 다음 사항을 확인 후 진행하세요.

- 출입 등급을 설정하세요. 출입 등급 등록에 대한 자세한 내용은 출입 등급 관리하기를 참고하세요.
- 층 등급을 설정하세요. 층 등급 등록에 대한 자세한 내용은 층 등급 관리하기를 참고하세요.

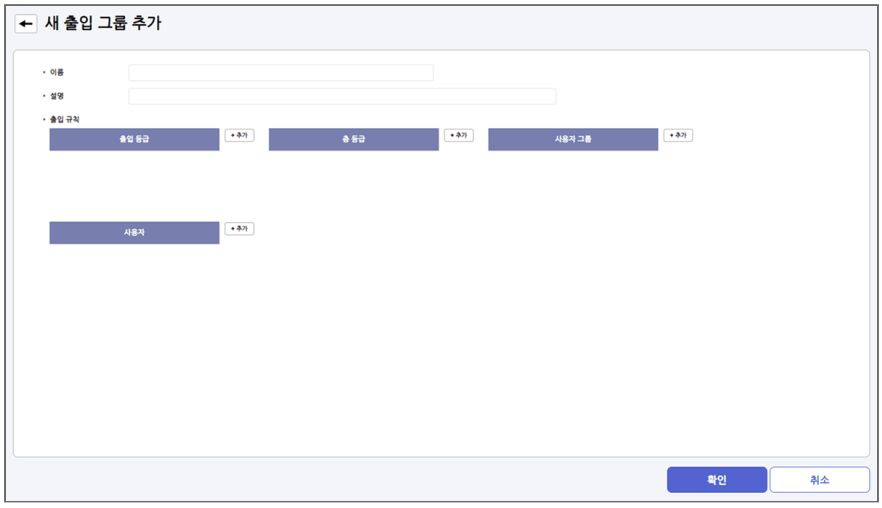
- 사용자 그룹을 설정하세요. 사용자 그룹 등록에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

출입 그룹 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **출입 그룹 추가** 버튼을 클릭하세요.



4. **새 출입 그룹 추가** 화면에서 **이름**과 **설명**을 입력하세요.



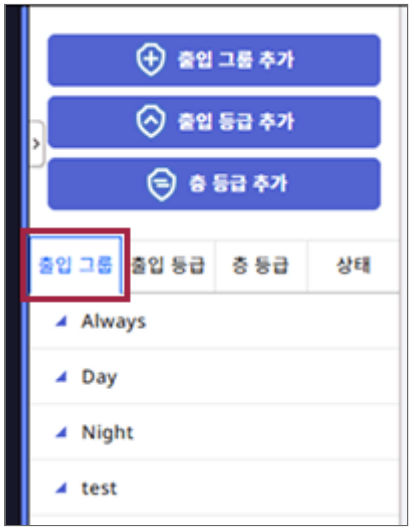
5. **출입 등급** 항목에서 **+ 추가** 버튼을 클릭해 출입 그룹에 적용할 출입 등급을 선택하세요.
6. **층 등급** 항목에서 **+ 추가** 버튼을 클릭해 출입 그룹에 적용할 층 등급을 선택하세요.
7. **사용자 그룹** 항목에서 **+ 추가** 버튼을 클릭해 출입 그룹에 적용할 사용자 그룹을 선택하세요.
8. **사용자** 항목에서 **+ 추가** 버튼을 클릭해 출입 그룹에 사용자를 선택하세요.
9. 출입 그룹을 등록하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

알아두기

- 원하는 출입 등급이 없다면 새로운 출입 등급을 등록해야 합니다. 출입 등급 등록에 대한 자세한 내용은 출입 등급 관리하기를 참고하세요.
- 원하는 층 등급이 없다면 새로운 층 등급을 등록해야 합니다. 층 등급 등록에 대한 자세한 내용은 층 등급 관리하기를 참고하세요.
- 추가한 항목을 삭제하려면 버튼을 클릭하세요.
- 원하는 항목을 검색하려면 버튼을 클릭하세요.

출입 그룹 수정

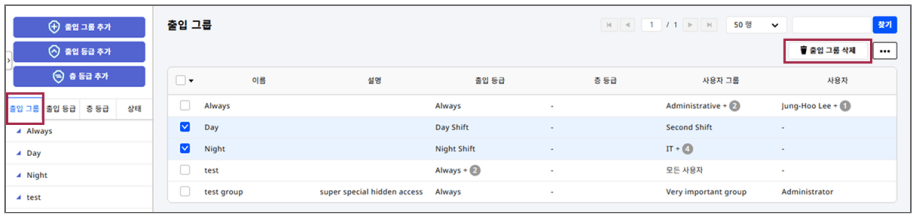
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **출입 그룹** 탭을 클릭하세요.



4. 출입 그룹 목록에서 수정할 출입 그룹을 클릭하세요.
5. 원하는 항목을 수정하세요.
6. 수정을 완료하면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

출입 그룹 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **출입 그룹** 탭을 클릭하세요.
4. 출입 그룹 목록에서 삭제할 출입 그룹의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단에 있는 **출입 그룹 삭제** 버튼을 클릭하세요.



층 등급 관리하기

설정한 엘리베이터와 층 정보를 이용해 층 등급을 설정하는 방법을 안내합니다. 층 등급은 출입 그룹에 적용할 수 있는 중요한 요소입니다. 층 등급을 설정하면 사용자가 엘리베이터를 이용해 출입할 수 있는 층을 관리할 수 있습니다.

> **알아두기**
> 층 등급과 관련한 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

시작하기 전에

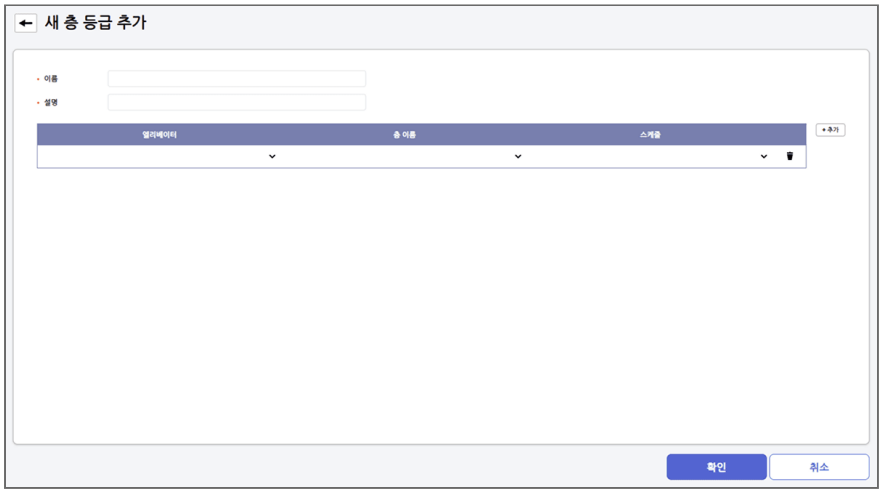
- 층 등급을 등록하기 전에 엘리베이터를 설정해야 합니다. 엘리베이터 등록에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.
- 스케줄 설정을 통해 층 등급에 적용할 시간을 미리 정의할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

층 등급 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**를 클릭하세요.
3. **층 등급 추가** 버튼을 클릭하세요.



4. **새 층 등급 추가** 화면에서 **이름**과 **설명**을 입력하세요.



5. **엘리베이터** 항목에서 층 등급에 적용할 엘리베이터를 선택하세요.
6. **층 이름** 항목에서 층 등급에 적용할 층을 선택하세요.
7. **스케줄** 항목에서 층 등급에 적용할 스케줄을 선택하세요.
8. 층 등급을 등록하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 원하는 출입 등급이 없다면 새로운 출입 등급을 등록해야 합니다. 출입 등급 등록에 대한 자세한 내용은 출입 등급 관리하기를 참고하세요.
> - 원하는 엘리베이터가 없다면 새로운 엘리베이터를 등록해야 합니다. 엘리베이터 등록에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.
> - 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.
> - 추가한 항목을 삭제하려면 버튼을 클릭하세요.
> - 원하는 항목을 검색하려면 버튼을 클릭하세요.

층 등급 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **층 등급** 탭을 클릭하세요.



4. 층 등급 목록에서 수정할 층 등급을 클릭하세요.
5. 원하는 항목을 수정하세요.
6. 수정을 완료하면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

층 등급 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**을 클릭하세요.
3. **층 등급** 탭을 클릭하세요.
4. 층 등급 목록에서 삭제할 층 등급의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단에 있는 **층 등급 삭제** 버튼을 클릭하세요.



출입 권한 상태 확인하기

사용자가 출입할 수 있는 출입문 목록을 확인하는 방법을 안내합니다. 출입 권한 상태를 확인하면 사용자가 출입할 수 있는 출입문과 해당 출입문에 대한 권한을 관리할 수 있습니다. 필터 기능을 사용해 원하는 결과를 정렬해 볼 수 있으며, CSV 파일로 목록을 저장할 수 있습니다.

출입 권한 상태 확인

출입 권한은 출입문 또는 층, 사용자를 기준으로 볼 수 있습니다.



1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **출입 통제**를 클릭하세요.

3. **상태** 탭을 클릭하세요.
4. **상태** 탭 아래의 상태 목록에서 원하는 항목을 클릭하세요.
   - **출입문 권한 상태 - 출입문별**
   - **출입문 권한 상태 - 사용자별**
   - **엘리베이터 권한 상태 - 층별**
   - **엘리베이터 권한 상태 - 사용자별**

선택한 항목에 대한 출입 권한 상태를 확인할 수 있습니다.

필터 저장

원하는 결과를 정렬하려면 출입 권한 목록 테이블의 헤더에서 ▼ 버튼을 클릭하세요. 필터 조건을 추가할 수 있습니다.

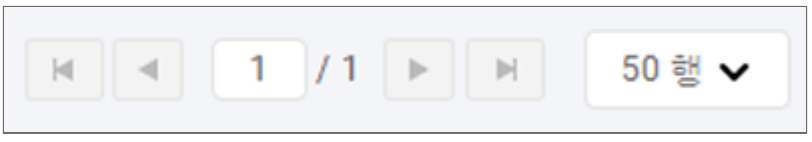
필터를 설정한 후에는 필터를 저장할 수 있습니다. **필터 저장** 버튼을 클릭하세요. 저장된 필터는 **상태** 탭 아래의 상태 목록에서 확인할 수 있습니다.



- 필터 이름을 변경하려면 ✎ 아이콘을 클릭하세요.
- 필터를 삭제하려면 🗑 아이콘을 클릭하세요.

목록 페이지 탐색

페이지를 이동하거나 한 페이지에 표시할 목록 개수를 설정할 수 있습니다. 화면 오른쪽 상단의 페이지 이동 도구를 사용하세요.



- ⏮: 첫 페이지로 이동합니다.
- ◀: 이전 페이지로 이동합니다.
- ▶: 다음 페이지로 이동합니다.
- ⏭: 마지막 페이지로 이동합니다.
- 원하는 페이지로 이동하려면 숫자 입력 필드에 페이지 번호를 입력하세요.

- 한 페이지에 표시할 목록 개수를 설정하려면 행 선택 상자를 클릭하세요.

CSV 내보내기

현재 보고 있는 출입 권한 상태 목록을 CSV 파일로 내보낼 수 있습니다. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **CSV 내보내기**를 선택하세요.

열 설정

현재 보고 있는 출입 권한 상태 목록 테이블에서 원하는 열을 숨기거나 표시할 수 있습니다. 화면 오른쪽 상단의 ••• 버튼을 클릭하고 **열 설정**을 선택하세요.



- **열 목록**에서 표시할 열을 선택하세요. 선택한 열은 목록 테이블에 표시됩니다. 선택하지 않은 열은 목록 테이블에서 숨겨집니다.
- 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

모든 설정을 완료하면 **확인** 버튼을 클릭하세요.

스케줄 설정하기

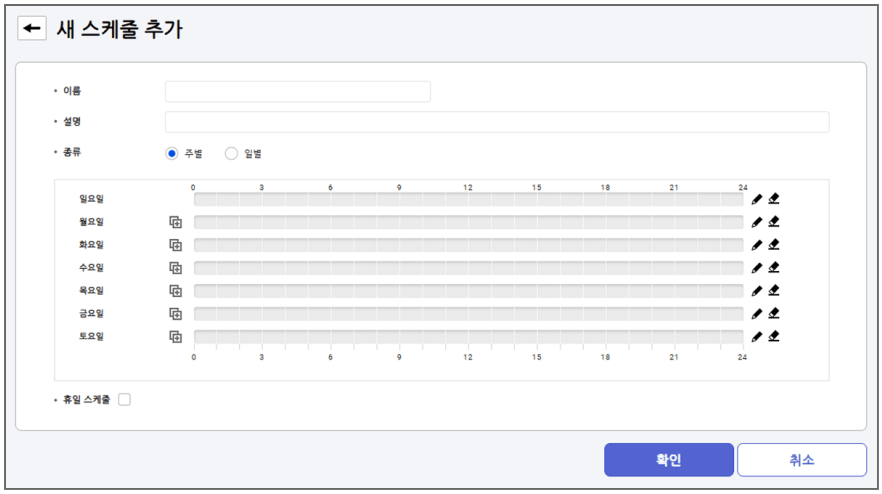
출입 및 휴일 스케줄을 설정하여 출입 통제와 근태 관리를 효율적으로 운영하는 방법을 안내합니다. 스케줄은 출입 통제에 적용할 수 있는 중요한 요소로, 사용자의 출입 시간과 휴일을 관리할 수 있습니다.

스케줄 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **스케줄**을 클릭하세요.
3. 화면 왼쪽 상단의 **스케줄 추가** 버튼을 클릭하세요.



4. **새 스케줄 추가** 화면에서 각 항목을 입력 또는 설정하세요.

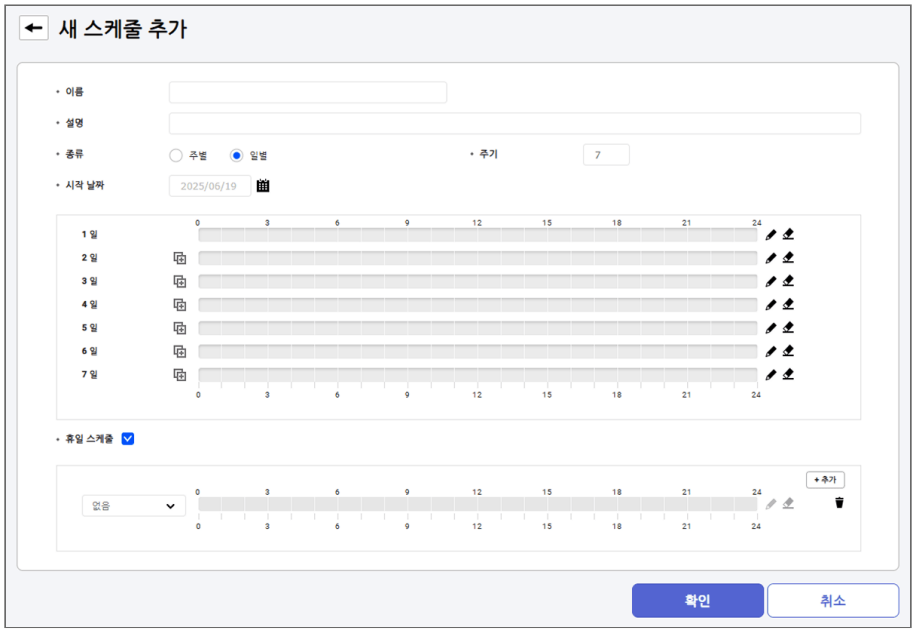


5. 모든 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **새 스케줄 추가** 화면의 개별 항목에 대한 자세한 내용은 새 스케줄 추가 옵션 안내를 참고하세요.

새 스케줄 추가 옵션 안내

새 스케줄 추가 화면에서 설정할 수 있는 개별 항목에 대해 안내합니다.



- **이름**: 스케줄 이름을 입력하세요.
- **설명**: 스케줄에 대한 간략한 설명을 입력하세요.
- **종류**: 주 단위 또는 일 단위의 스케줄을 선택하세요. **일별**을 선택하면 **주기**와 **시작 날짜**를 선택할 수 있습니다.



- 가운데 영역의 **시간 슬롯**을 클릭하여 원하는 시간을 설정하세요. 설정을 완료했다면 **확인** 버튼을 클릭하세요.



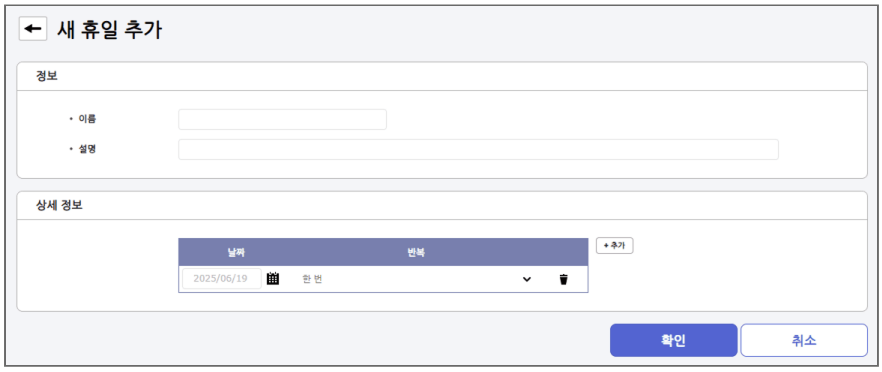
  - 요일별, 일별에 따라 시간 슬롯은 최대 5개까지 설정할 수 있습니다.

  - 스케줄을 설정하고 버튼을 클릭하면 바로 위에 설정된 시간 슬롯을 복사할 수 있습니다.
  - 시간 슬롯을 수정하려면 버튼을 클릭하세요. 설정된 시간 슬롯을 삭제하려면 버튼을 클릭하세요.
- **휴일 스케줄**: 휴일 스케줄 적용 여부를 선택하세요. 항목을 선택하면 세부 설정을 적용할 수 있습니다.
  - **없음** 선택 상자를 선택해 미리 설정한 휴일을 선택할 수 있습니다. 휴일을 더 추가하려면 **+ 추가** 버튼을 클릭하고 휴일을 설정하세요.
  - **휴일 시간 슬롯**: 시간 슬롯을 클릭하여 휴일에 적용할 시간 슬롯을 설정하세요.

> **알아두기**
>
> - 시간 슬롯을 수정하려면 버튼을 클릭하세요. 설정된 시간 슬롯을 삭제하려면 버튼을 클릭하세요.
> - 추가한 휴일을 삭제하려면 버튼을 클릭하세요.
> - 휴일 일정 추가에 대한 자세한 내용은 휴일 일정 추가를 참고하세요.

휴일 일정 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **스케줄**을 클릭하세요.
3. 화면 왼쪽 상단의 **휴일 추가** 버튼을 클릭하세요.
4. **새 휴일 추가** 화면에서 **이름**과 **설명**을 입력하세요.



5. **상세 정보** 섹션에서 **+ 추가** 버튼을 클릭하세요.
6. 버튼을 클릭하여 날짜를 선택하고 반복 횟수와 기간을 설정하세요.
7. 설정한 휴일 일정을 등록하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> 휴일 일정을 삭제하려면 버튼을 클릭하세요.

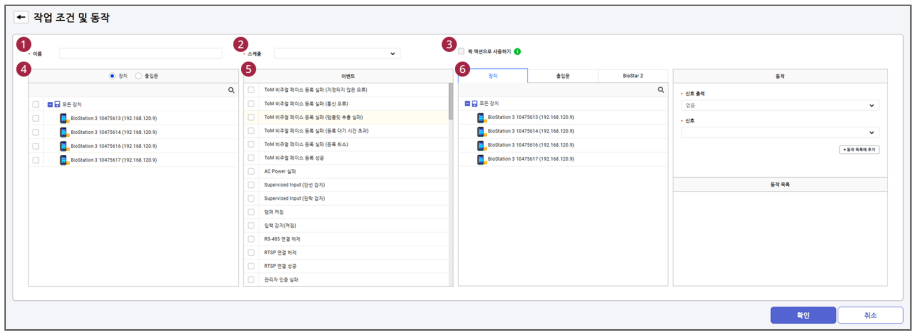
작업 조건 및 동작 설정하기

장치, 출입문, 구역에서 특정 이벤트가 발생했을 때 사용자가 원하는 동작을 장치나 BioStar X가 수행하도록 설정할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **작업 조건 및 동작**을 클릭하세요.
3. 화면 왼쪽 상단의 **출입 관리** → **작업 조건 및 동작 추가** 버튼을 클릭하세요.



화면의 안내에 따라 세부 항목을 설정하세요.



1 이름 입력

이름: 작업 조건 및 동작 이름을 입력하세요.

2 스케줄 설정

스케줄: 작업 조건 및 동작이 적용될 스케줄을 설정하세요.

> **알아두기**
>
> - **신호 입력**을 선택해 사용자 정의 조건을 설정할 때 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭하여 설정하세요.
> - 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

3 퀵 액션으로 사용하기

퀵 액션을 설정하면 BioStar X 메인 화면에서 **퀵 액션** 버튼으로 한번에 다수의 출입문을 제어할 수 있습니다. **퀵 액션으로 사용하기** 체크박스를 클릭하세요.

> **알아두기**
>
> - 이 기능은 **스케줄** 옵션이 **Always**일 때만 사용할 수 있습니다.
> - **퀵 액션**은 **설정** → **출입 관리** → **퀵 액션**에서 설정할 수 있습니다. **퀵 액션**에 대한 자세한 내용은 퀵 액션 사용하기를 참고하세요.

4 장치, 출입문, 고급 출입 통제 선택

이벤트 신호를 보낼 항목을 선택하세요. 각 장치는 여러 개를 선택할 수 있으며, **BioStar X**와의 연결이 끊어져도 독립적으로 동작합니다.

> **알아두기**
>
> **고급 출입 통제** 항목은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

5 작업 조건 이벤트 설정

조건 이벤트를 설정하세요. 하나 이상의 이벤트를 선택해야 합니다.

> **알아두기**
>
> 이전 단계에서 선택한 옵션에 따라 각각 다른 이벤트 목록이 활성화됩니다.

6 동작 설정

동작을 수행할 장치를 선택하세요. 동작을 수행할 장치, 출입문, **BioStar X**의 동작을 선택할 수 있습니다.

동작 섹션에서는 선택한 조건 이벤트가 발생했을 때 전송할 신호를 설정할 수 있습니다. 이메일로 로그를 전달 받으려면 **BioStar X**에서 설정할 수 있습니다.

> **알아두기**
>
> - **장치**, **출입문**, **BioStar X** 탭을 클릭하면 동작 섹션의 내용이 변경됩니다.
> - 이메일 서버 정보를 설정하려면 **BioStar X** 탭에서 ⚙ 아이콘을 클릭하세요. **SMTP 정보** 창이 나타나면 이메일 서버 정보를 입력하고 **확인** 버튼을 클릭하세요. 자세한 내용은 이메일 설정하기를 참고하세요.
> - 이메일 서버 정보에 대한 자세한 내용은 시스템 관리자에게 문의하세요.

모든 설정을 완료했다면 **확인** 버튼을 클릭하세요.

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.

퀵 액션 메뉴에서 퀵 액션 버튼을 추가하면 **BioStar X** 메인 화면에서 간편하게 퀵 액션 버튼을 클릭하여 다수의 출입문을 한 번에 제어할 수 있습니다.

> **알아두기**
> 퀵 액션으로 사용할 **퀵 액션**을 추가하려면 작업 조건 및 동작 설정하기를 참고하세요.

퀵 액션 버튼 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **퀵 액션**을 클릭하세요.



3. **퀵 액션 레이아웃** 섹션에서 **+ 추가** 버튼을 클릭하세요.
4. **새 퀵 액션 추가** 창이 나타나면 각 항목을 입력하고 설정하세요.



- **관리자 등급**: 추가하려는 퀵 액션을 실행할 수 있는 **관리자 등급**을 선택하세요. 복수로 선택할 수 있습니다.
- **작업 조건 및 동작**: 실행할 **작업 조건 및 동작**을 선택하세요. 복수로 선택할 수 있습니다.
- **실행 전 확인하기**: 이 옵션을 활성화하면 **퀵 액션** 버튼을 눌렀을 때 실행 여부를 묻는 확인 팝업창이 나타납니다.

5. 설정을 저장하려면 **확인** 버튼을 클릭하세요.

6. 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

BioStar X 화면의 오른쪽 상단 헤더 영역에 추가한 **퀵 액션** 버튼이 생성됩니다. 생성한 **퀵 액션** 버튼을 클릭해 **퀵 액션**에서 설정한대로 동작하는지 확인하세요.

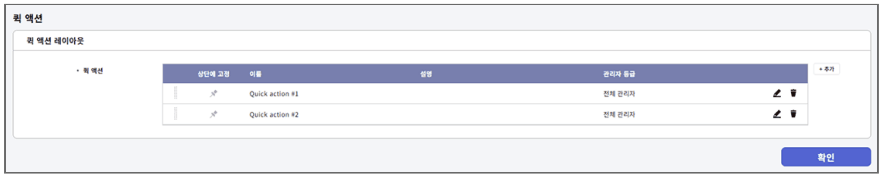


알아두기

- **퀵 액션** 버튼은 화면 상단 헤더 영역에 최대 4개까지 추가할 수 있습니다. 어느 페이지에서든 사용할 수 있도록 고정되어 있습니다.
- 사용자에게 설정된 **관리자 등급**에 따라 사용할 수 있는 **퀵 액션** 버튼이 다를 수 있습니다.

퀵 액션 버튼 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **퀵 액션**을 클릭하세요.
3. 수정하려는 퀵 액션 버튼의 오른쪽에 ✎ 버튼을 클릭하세요.



4. 수정을 위한 팝업창이 나타나면 원하는 항목을 수정하고 **확인** 버튼을 클릭하세요.
5. 수정 사항을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

퀵 액션 순서 변경

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **퀵 액션**을 클릭하세요.
3. 퀵 액션 목록에서 순서를 이동할 항목의 가장 왼쪽 열을 클릭한 상태에서 원하는 위치로 드래그하세요.



4. 변경한 순서를 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

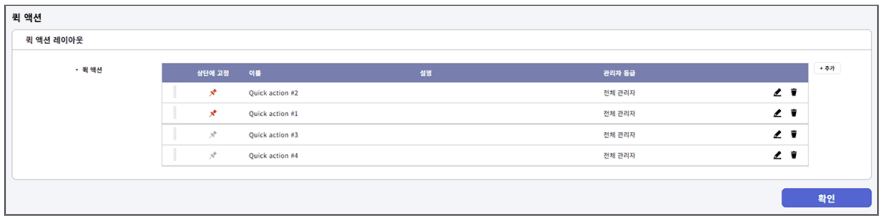
화면 오른쪽 상단의 퀵 액션 목록에서 변경된 순서를 확인할 수 있습니다.



헤더 영역에 버튼 고정

빠르게 실행할 필요가 있는 퀵 액션 항목을 화면 헤더 영역에 배치할 수 있습니다.

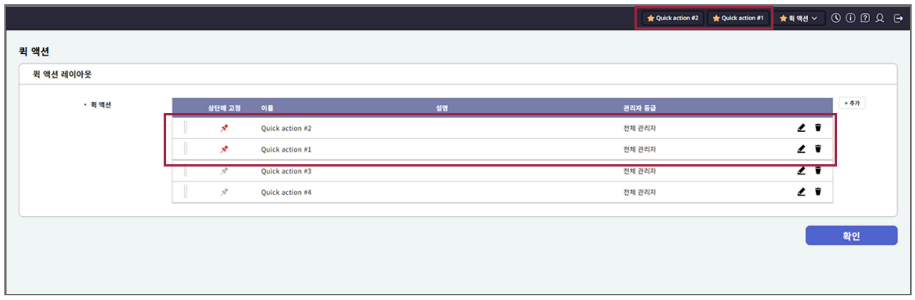
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **퀵 액션**을 클릭하세요.
3. 헤더 영역에 배치하려면 **상단에 고정**( )을 클릭하세요.



> 가장 왼쪽 열을 클릭한 상태에서 원하는 위치로 드래그하여 순서를 변경하거나 **상단에 고정** 상태를 해제할 수 있습니다.

4. 헤더 영역에 고정할 항목을 모두 선택했다면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

화면 오른쪽 상단의 **퀵 액션** 버튼 왼쪽에 고정된 퀵 액션을 확인할 수 있습니다.

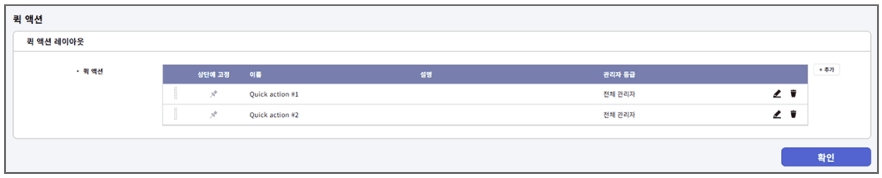


알아두기

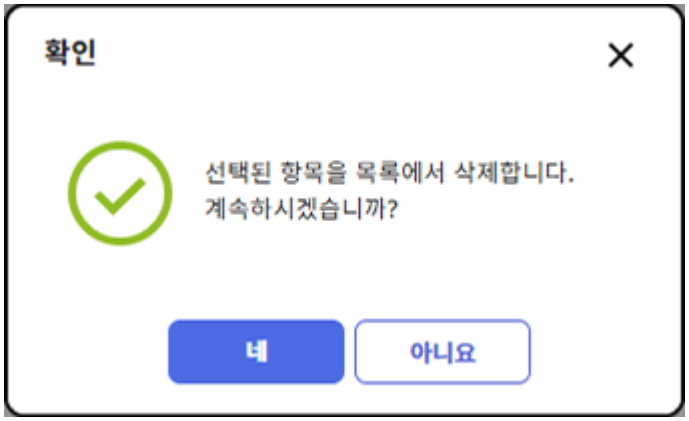
- 최대 4개의 퀵 액션을 헤더 영역에 고정할 수 있습니다. 이미 4개가 고정된 상태에서는 퀵 액션을 추가로 고정할 수 없습니다. 다른 항목을 해제한 후 다시 시도하세요.
- 웹 브라우저의 창 폭이 좁아지면 헤더에 있던 개별 버튼은 모두 사라지고, 고정했던 퀵 액션 항목은 핀( ) 아이콘과 함께 **퀵 액션** 버튼의 드롭다운 목록에서 확인할 수 있습니다.
- 등록된 모든 퀵 액션을 헤더에 고정하면 **퀵 액션** 버튼이 나타나지 않습니다. 일부 항목의 고정을 해제하면 버튼이 다시 나타납니다.

퀵 액션 버튼 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **퀵 액션**을 클릭하세요.
3. 삭제하려는 퀵 액션 버튼의 오른쪽에 버튼을 클릭하세요.



4. 삭제 확인 팝업창을 확인하고 **네**를 클릭하세요.



5. 삭제한 사항이 반영하려면 화면 오른쪽 하단의 **확인**을 클릭하세요.

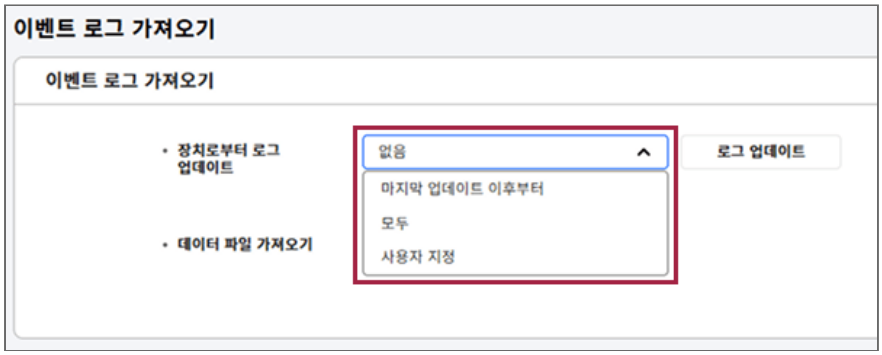
이벤트 로그 가져오기

장치의 로그를 BioStar X의 서버로 가져와 이벤트를 확인할 수 있습니다. 이 기능은 **서버** 설정에서 **로그 업로드** 옵션을 **수동**으로 설정한 경우에 사용할 수 있습니다.

> **알아두기**
> **로그 업로드** 옵션에 대한 자세한 내용은 서버 상세 설정하기를 참고하세요.

수동으로 가져오기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **이벤트** → **이벤트 로그 가져오기**를 클릭하세요.
3. **장치로부터 로그 업데이트** 항목에서 로그를 가져올 기간을 선택하세요.



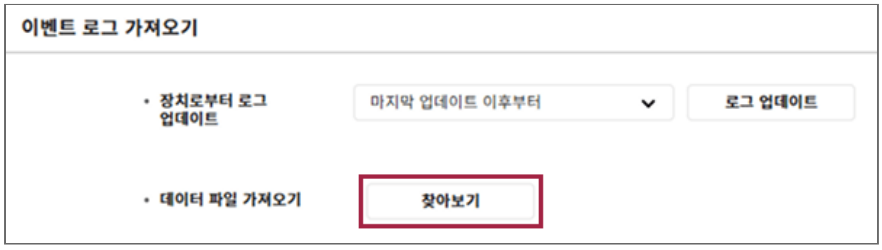
- **마지막 업데이트 이후부터**: 마지막으로 **BioStar X** 서버로 저장된 로그의 날짜 이후의 로그를 가져옵니다.
- **모두**: 장치의 모든 로그를 가져옵니다.
- **사용자 지정**: 로그를 가져올 시작일과 종료일을 선택할 수 있습니다.

4. 로그를 가져오려면 **로그 업데이트** 버튼을 클릭하세요.

외부 저장매체로 가져오기

외부 저장매체(USB)에 저장된 이벤트 로그를 **BioStar X**에 불러올 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **이벤트** → **이벤트 로그 가져오기**를 클릭하세요.
3. **데이터 파일 가져오기** 항목의 **찾아보기** 버튼을 클릭하세요.



4. 로컬에 저장된 데이터 파일(*.tgz*)을 선택하세요.

데이터 파일을 가져오는데 성공하면 화면에 메시지가 나타납니다.

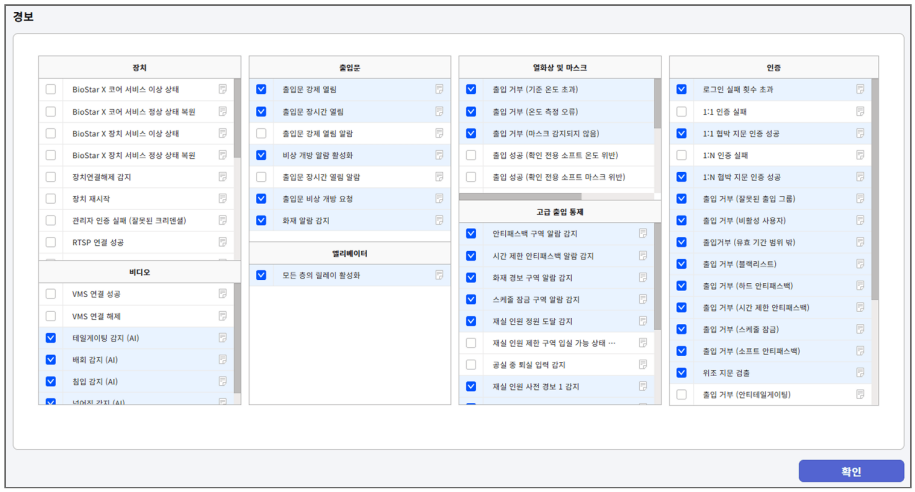
> **알아두기**
>
> - 오래된 펌웨어 버전을 사용하는 장치에서 내보내기한 데이터는 **BioStar X**로 가져올 수 없습니다. 항상 최신 버전의 펌웨어를 사용하세요.
> - BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceLite, FaceStation 2, BioStation A2, BioStation 2 모델에서 내보낸 데이터 파일만 가져올 수 있습니다.
> - **BioStar X** 시스템에서 설정한 출입문, 엘리베이터, 구역 이벤트 로그가 아닌 경우 일부 정보가 빈 칸으로 나타날 수 있습니다.

경보 설정하기

장치, 출입문, 구역에 이벤트가 발생했을 경우 화면에 표시할 경보 종류와 메시지를 설정할 수 있습니다. 또한, 경보가 발생했을 경우 사용자가 업로드한 사운드 파일을 재생하도록 설정할 수 있습니다.

경보 설정하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **이벤트** → **경보**을 클릭하세요.
3. 각 카테고리의 이벤트 목록에서 화면에 표시할 이벤트를 선택하세요.
4. 모든 설정을 완료했다면 **확인** 버튼을 클릭하세요.



경보 메시지 수정하기

경보 메시지를 수정하려면 이벤트 목록에서 버튼을 클릭하세요. **경보 메시지** 창이 나타나면 각 항목을 설정하고 **확인** 버튼을 클릭하세요.



- **이름**: 경보 메시지 이름을 변경할 수 있습니다.
- **메시지**: 화면에 표시할 메시지를 입력하세요.
- **사운드 이름**: 해당 이벤트가 발생할 때 재생할 사운드 파일을 업로드 했다면 목록에서 선택할 수 있습니다.
- **재생 옵션**: 사운드 파일을 선택했다면 재생할 횟수를 선택하세요.

> **알아두기**
> 재생할 사운드 파일이 없다면 기본 설정 구성하기를 참고하여 업로드하세요.

크리덴셜 관리하기

출입 인증에 사용하는 크리덴셜의 관리 방법을 안내합니다. 카드 발급 상태와 소지 사용자, 블랙리스트를 확인하고 Wiegand 및 스마트 카드 형식을 설정할 수 있습니다. 이 외에도 cardPresso와 연동한 카드 인쇄, 에어팝 포털(Airfob Portal)과 연동한 모바일 출입 카드 관리, IR 페이스 그룹 매칭 설정 방법도 확인할 수 있습니다.

카드 관리하기

카드의 발급 상태를 확인하고, Wiegand 카드 데이터 형식을 변경하며, CSN 모바일 카드 삭제 이력을 관리할 수 있습니다.

카드 관리

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드**를 클릭하세요.
3. 카드 목록 화면에서 등록된 카드를 확인할 수 있습니다.



화면 왼쪽 발급 상태를 클릭하면 카드 발급 상태별로 필터링할 수 있습니다. 카드 발급 상태는 아래와 같습니다.

- **미할당된 카드**: 사용자에게 할당하지 않은 카드입니다.
- **할당된 카드**: 특정 사용자에게 할당한 카드입니다. 카드 목록에서 할당된 사용자의 아이디와 이름을 확인할 수 있습니다.
- **사용 정지된 카드**: 블랙리스트로 등록된 카드입니다. 해당 카드 소지자는 출입 인증할 수 없습니다.
- **삭제된 CSN 모바일 카드**: 삭제된 모바일 출입 카드입니다.

> **알아두기**
> 사용자의 카드를 차단했다면 **사용 정지된 카드** 목록에서 카드 정보를 확인할 수 있습니다. 차단을 해제하려면 원하는 카드를 선택하고 **차단 해제**를 클릭하세요.

Wiegand 카드 데이터 형식 변경

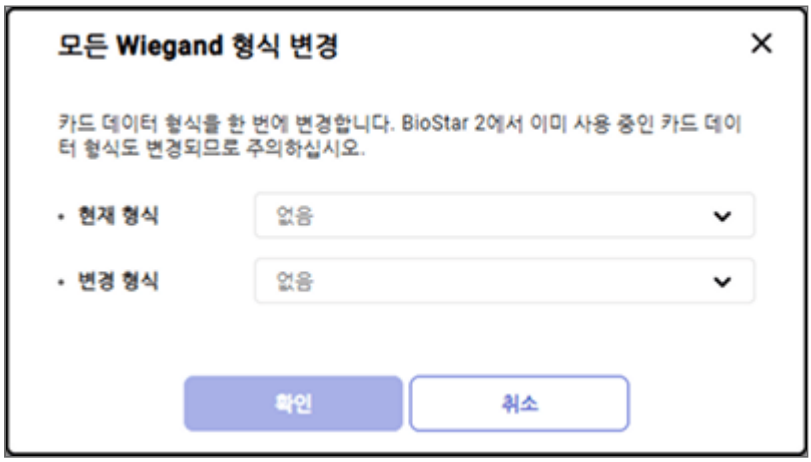
사용 중인 Wiegand 카드 데이터 형식을 한 번에 변경할 수 있습니다.

> **주의**
> 이미 사용자에게 할당된 카드의 데이터 형식도 변경되므로 주의하세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드**를 클릭하세요.
3. 카드 목록의 오른쪽 상단에 ••• 버튼을 클릭하고 **모든 Wiegand 형식 변경**을 선택하세요.



4. **모든 Wiegand 형식 변경** 창이 나타나면 변경하려는 카드 데이터 형식을 **현재 형식** 목록에서 선택하세요.



5. 변경하길 원하는 카드 데이터 형식을 **변경 형식** 목록에서 선택하세요.
6. 카드 데이터 형식을 변경하려면 **확인** 버튼을 클릭하세요.

CSN 모바일 카드 삭제 시 관리 지침

BioStar X에 에어팝 포털 레귤러 사이트를 연동하여 CSN 모바일 카드를 사용 중일 때, 카드를 소지한 사용자가 카드를 삭제하더라도 동일한 카드 ID를 다른 사용자에게 발급할 수 있게 되어 있었습니다. 그러나 동일한 카드 ID를 다른 사용자에게 발급할 경우 기존의 카드 소지자도 계속 출입이 가능한 문제가 발생합니다.

이 문제를 해결하기 위해 CSN 모바일 카드를 삭제한 후 삭제 이력을 관리할 수 있는 기능을 제공합니다.

삭제된 CSN 모바일 카드 별도 관리

삭제된 CSN 모바일 카드는 **설정** → **크리덴셜** → **카드**의 **삭제된 CSN 모바일 카드** 목록에 기록됩니다. 목록에서 **카드 종류**, **카드 데이터 형식**, **카드 ID**, **마지막 카드 소지자**를 확인할 수 있습니다.



삭제된 카드 ID로 재발급 방지

삭제 이력이 있는 CSN 모바일 카드를 다른 사용자에게 발급하려고 하는 경우 실패 처리합니다.

삭제된 카드 ID로 카드를 발급하고자 하는 경우 **삭제된 CSN 모바일 카드** 목록에서 해당 CSN 모바일 카드를 제외한 후에만 발급할 수 있습니다.



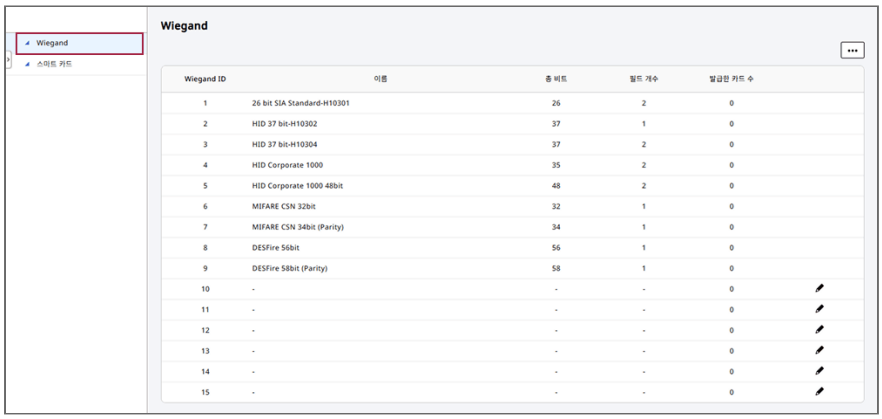
> **알아두기**
>
> **삭제된 CSN 모바일 카드** 목록에 포함되어 있는 CSN 모바일 카드는 **미할당된 카드** 목록에서 삭제할 수 없습니다.
>
> **미할당된 카드** 목록에서 카드를 삭제하려면 **삭제된 CSN 모바일 카드** 목록에서 카드를 먼저 제외한 다음 다시 시도하세요.

Wiegand 카드 형식 설정하기

카드 데이터를 읽는 형식을 설정할 수 있습니다. 설정된 Wiegand 형식으로 카드 데이터가 처리됩니다.

Wiegand 카드 형식 설정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드 형식**을 클릭하세요.
3. 화면 왼쪽 카드 형식 목록에서 **Wiegand**를 클릭하세요.



4. Wiegand 형식 목록에서 이름이 지정되지 않은 항목의 ✎ 버튼을 클릭하세요.
5. **새 Wiegand 추가** 화면이 나타나면 각 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
6. 설정한 Wiegand 형식을 추가하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - Wiegand 형식은 최대 15개까지 사용할 수 있습니다.
> - 미리 정의된 형식은 수정하거나 삭제할 수 없습니다.

설정 옵션 안내

Wiegand 카드 형식을 추가하거나 수정할 때 아래 항목을 참고하여 비트 구성을 설정하세요.



- **이름**: Wiegand 형식 이름을 입력하세요.
- **설명**: Wiegand 형식에 대한 간단한 설명을 입력하세요.
- **총 비트**: 총 비트 수를 입력하세요.
- **식별 코드 필드**: 식별 코드 사용 여부를 설정할 수 있습니다. 식별 코드를 사용하려면 체크 박스를 클릭하고 **시작 비트**와 **종료 비트**를 입력하세요.
- **ID 필드**: 사용하려는 아이디의 **시작 비트**와 **종료 비트**를 입력하세요. **+ 추가** 버튼을 클릭하면 ID 필드를 추가할 수 있습니다.
- **패리티 비트**: **+ 추가** 버튼을 클릭하면 패리티 비트 수를 입력하세요. 사용하려는 패리티 비트의 위치와 시작 및 종료 비트를 입력하세요.

> **알아두기**
> 패리티 비트를 추가하려면 **총 비트** 옵션을 입력해야 합니다.

스마트 카드 형식 설정하기

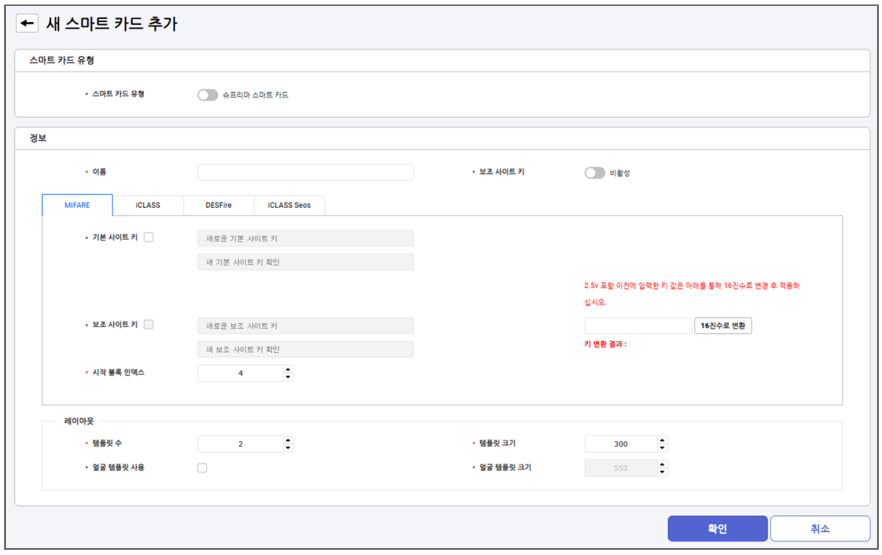
MIFARE, iCLASS, DESFire, iCLASS Seos와 같은 스마트 카드의 레이아웃을 설정할 수 있습니다.

스마트 카드 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드 형식**을 클릭하세요.
3. 화면 왼쪽 카드 형식 목록에서 **스마트 카드**를 클릭하세요.



4. 화면 왼쪽 상단의 **스마트 카드 추가** 버튼을 클릭하세요.
5. **새 스마트 카드 추가** 화면이 나타나면 각 항목을 설정하세요. 자세한 내용은 스마트 카드 유형을 참고하세요.

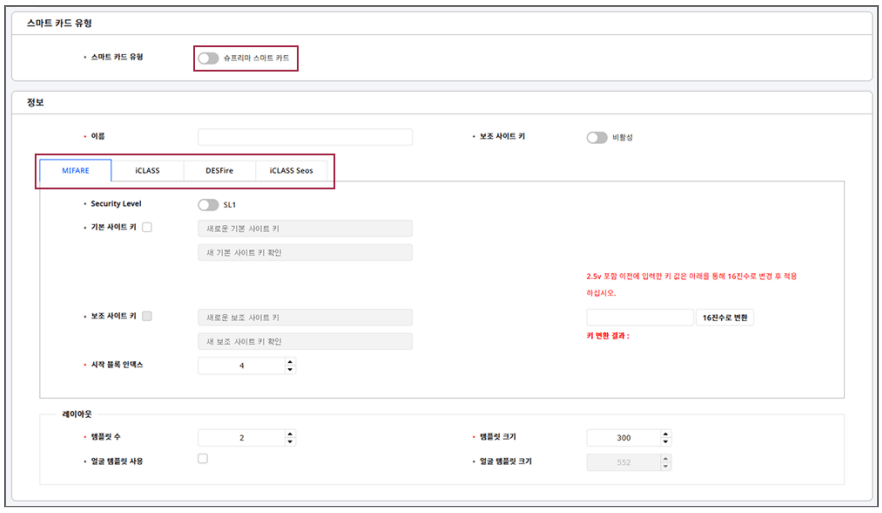


6. 모든 설정을 마쳤다면 **확인** 버튼을 클릭하세요.

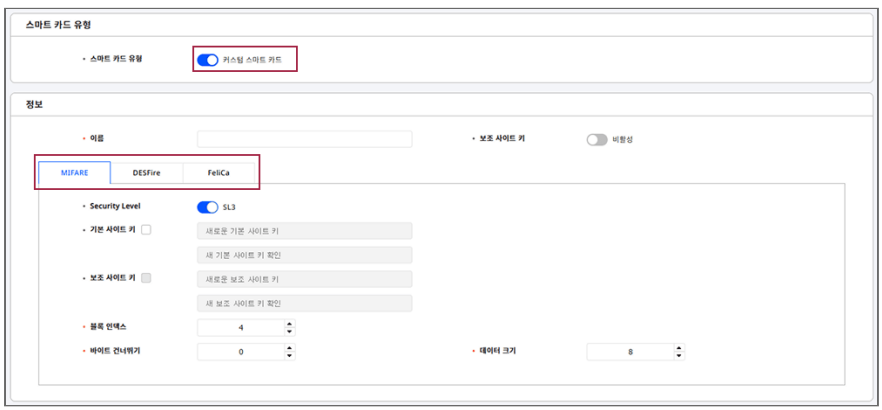
스마트 카드 유형

스마트 카드 유형 옵션에서 원하는 스마트 카드 유형을 설정할 수 있습니다.

- **슈프리마 스마트 카드**



- **커스텀 스마트 카드**

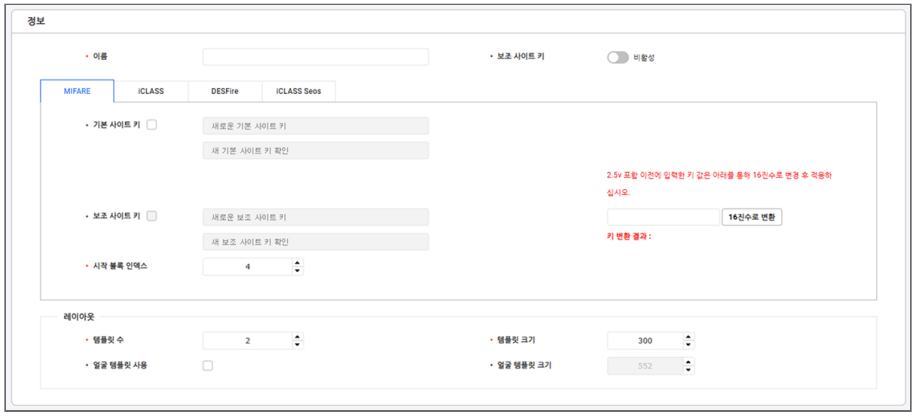


알아두기

- 커스텀 스마트 카드는 MIFARE, DESFire, FeliCa만 지원합니다.
- FeliCa는 BioStation 3 펌웨어 1.3.0 이상에서만 지원합니다.

설정 옵션 안내

정보 섹션에서 카드 레이아웃을 설정하세요.

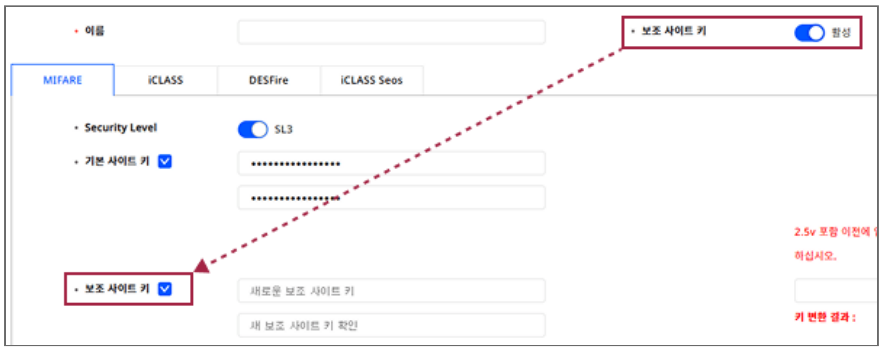


알아두기

- **기본 사이트 키**와 **보조 사이트 키**는 16진수만 지원합니다. 화면 오른쪽 필드에 사용할 키 값을 입력하고 **16진수로 변환** 버튼을 클릭하세요. 변환된 값을 사이트 키로 사용하세요.
- **16진수로 변환** 버튼은 **스마트 카드 유형** 옵션이 **슈프리마 스마트 카드**일때만 사용할 수 있습니다.

기본 정보 설정

- **이름**: 스마트 카드 이름을 입력하세요.
- **보조 사이트 키**: 보조 사이트 키 사용 여부를 설정할 수 있습니다. **활성**으로 설정하면 보조 사이트 키를 설정할 수 있습니다. 보조 사이트 키를 설정하면 카드의 기본 사이트 키가 일치하지 않을 때 보조 사이트 키를 사용하여 인증을 수행합니다.



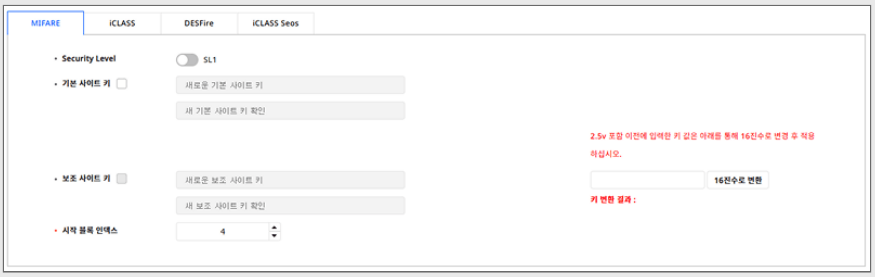
스마트 카드 설정

스마트 카드의 구조를 설정할 수 있습니다.

슈프리마 스마트 카드

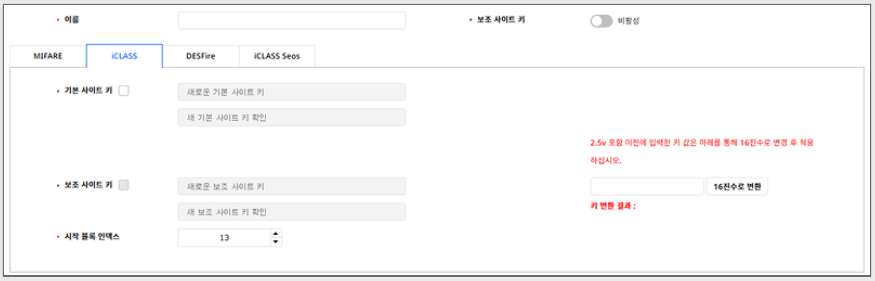
기본 사이트 키와 **보조 사이트 키**는 16진수만 지원합니다. 각 입력 필드에 사용할 키 값을 입력한 후 **16진수로 변환** 버튼을 클릭하세요. 변환된 값을 사이트 키로 사용하세요.

▼ MIFARE



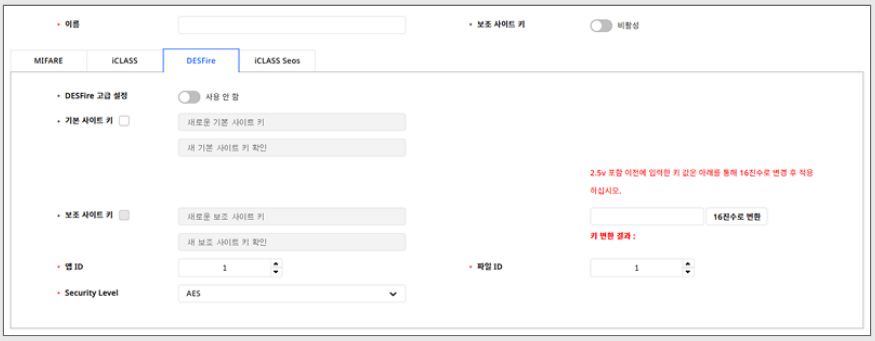
- **암호화 종류**: 암호화 종류를 **SL1** 또는 **SL3**로 설정할 수 있습니다.
- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **시작 블록 인덱스**: 각 템플릿이 저장될 시작 블록을 선택하세요. 이 블록은 사용자 정보가 저장될 블록의 인덱스이며, 사용자가 이미 스마트 카드를 사용하고 있다면 저장 가능한 블록을 설정하세요.

▼ iCLASS



- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **시작 블록 인덱스**: 각 템플릿이 저장될 시작 블록을 선택하세요. 이 블록은 사용자 정보가 저장될 블록의 인덱스이며, 사용자가 이미 스마트 카드를 사용하고 있다면 저장 가능한 블록을 설정하세요.

▼ DESFire

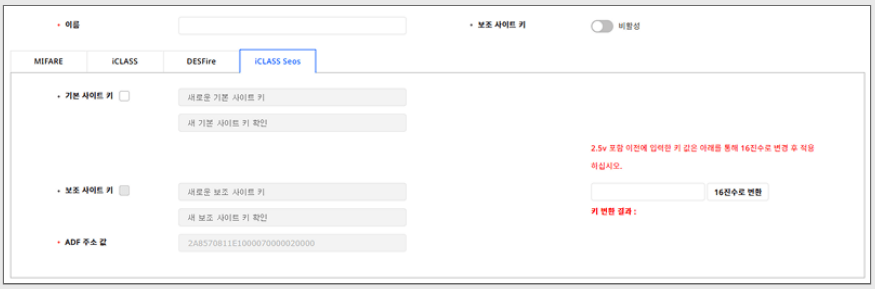


- **DESFire 고급 설정**: 타사에서 발급한 DESFire 카드를 사용할 수 있습니다. DESFire만 설정할 수 있습니다.

- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **앱 ID**: 애플리케이션 아이디를 설정하세요. **파일 ID**를 포함하는 일종의 디렉토리 역할을 합니다.
- **파일 ID**: 파일 아이디를 설정하세요.
- **암호화 종류**: 암호화 종류를 **DES/3DES** 또는 **AES**로 설정할 수 있습니다.

> **알아두기**
> 암호화 종류가 **AES**로 저장되어 있는 카드 레이아웃을 **DES/3DES**로 변경하면 다음 경고 팝업이 나타납니다.
>
> > ***암호화 종류를 DES/3DES로 변경하면 이 카드 레이아웃을 사용하는 장치에서 EV2/EV3 보안 메시징 강제를 설정할 수 없습니다.***
>
> **확인** 버튼을 클릭하면 변경한 내용이 저장되며, 이 카드 레이아웃을 사용하는 장치의 **EV2/EV3 보안 메시징 강제** 옵션은 자동으로 꺼집니다. **EV2/EV3 보안 메시징 강제** 옵션에 대한 자세한 내용은 인증 설정하기를 참고하세요.

▼ iClass Seos



- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **ADF 주소 값**: 디지털 자격 증명이 저장되는 ADF 주소입니다.

레이아웃

사용자 정보와 얼굴 및 지문 정보가 기록되는 레이아웃을 수정할 수 있습니다.

- **템플릿 수**: 레이아웃에 포함할 지문 템플릿 수를 설정하세요.
- **템플릿 크기**: 지문 템플릿이 사용하는 바이트 수를 설정하세요.
- **얼굴 템플릿 사용**: 얼굴 템플릿 사용 여부를 선택할 수 있습니다.
- **얼굴 템플릿 크기**: 얼굴 템플릿이 사용하는 바이트 수를 설정하세요.

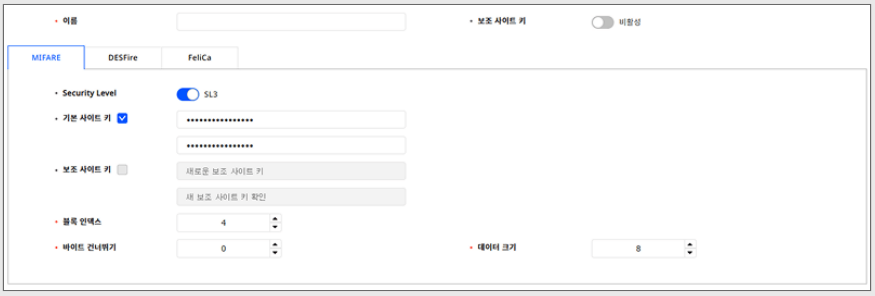
> **알아두기**
> **얼굴 템플릿 사용**은 BioStation 3 Max, BioEntry W3, BioStation 3, FaceStation F2 모델에서 사용할 수 있습니다.

커스텀 스마트 카드

커스텀 스마트 카드는 MIFARE, DESFire, FeliCa만 지원합니다.

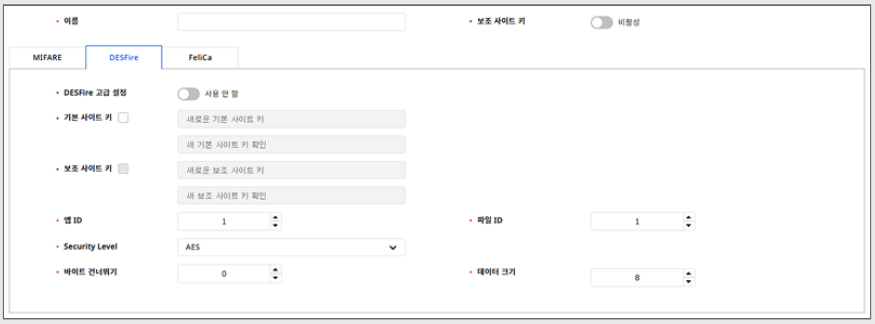
> **알아두기**
> FeliCa는 BioStation 3 펌웨어 1.3.0 이상에서만 지원합니다.

▼ MIFARE



- **암호화 종류**: 암호화 종류를 **SL1** 또는 **SL3**로 설정할 수 있습니다.
- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **블록 인덱스**: 각 템플릿이 저장될 시작 블록을 선택하세요. 이 블록은 사용자 정보가 저장될 블록의 인덱스이며, 사용자가 이미 스마트 카드를 사용하고 있다면 저장 가능한 블록을 설정하세요.
- **바이트 건너뛰기**: 카드 번호를 읽어들일 시작점을 설정할 수 있습니다.
- **데이터 크기**: (설정한 **기본 사이트 키**와 **보조 사이트 키**가 카드의 설정값과 동일한 경우) 읽어들일 카드의 데이터 크기를 설정할 수 있습니다.

▼ DesFire



- **DESFire 고급 설정**: 타사에서 발급한 DESFire 카드를 사용할 수 있습니다. DESFire만 설정할 수 있습니다.
- **기본 사이트 키**: 스마트 카드와 카드 리더 사이의 통신을 암호화하는 키입니다.
- **보조 사이트 키**: 카드의 기본 사이트 키가 일치하지 않을 때 사용하여 인증을 수행할 수 있습니다. 보조 사이트 키는 섹션 상단의 **보조 사이트 키** 옵션을 활성화해야만 입력할 수 있습니다.
- **앱 ID**: 애플리케이션 아이디를 설정하세요. **파일 ID**를 포함하는 일종의 디렉토리 역할을 합니다.
- **파일 ID**: 파일 아이디를 설정하세요.
- **암호화 종류**: 암호화 종류를 **DES/3DES** 또는 **AES**로 설정할 수 있습니다.

알아두기

암호화 종류가 **AES**로 저장되어 있는 카드 레이아웃을 **DES/3DES**로 변경하면 다음 경고 팝업이 나타납니다.

> ***암호화 종류를 DES/3DES로 변경하면 이 카드 레이아웃을 사용하는 장치에서 EV2/EV3 보안 메시징 강제를 설정할 수 없습니다.***

확인 버튼을 클릭하면 변경한 내용이 저장되며, 이 카드 레이아웃을 사용하는 장치의 **EV2/EV3 보안 메시징 강제** 옵션은 자동으로 꺼집니다. **EV2/EV3 보안 메시징 강제** 옵션에 대한 자세한 내용은 인증 설정하기를 참고하세요.

- **바이트 건너뛰기**: 카드 번호를 읽어들일 시작점을 설정할 수 있습니다.
- **데이터 크기**: (설정한 **기본 사이트 키**와 **보조 사이트 키**가 카드의 설정값과 동일한 경우) 읽어들일 카드의 데이터 크기를 설정할 수 있습니다.

▼ Felica



- **시스템 코드**: FeliCa 카드를 읽기 위한 시스템 코드를 16진수로 최대 4자리까지 입력하세요.
- **서비스 코드**: FeliCa 카드를 읽기 위한 서비스 코드를 16진수로 최대 4자리까지 입력하세요.
- **ID 필드**: 카드에서 특정 영역을 읽을 수 있도록 설정합니다. **+ 추가** 버튼을 클릭해 읽고자 하는 최대 8개 블록에 대해 설정할 수 있습니다.

  블록 번호: 카드를 읽어들일 블록을 설정합니다. (0 ~ 150)

카드 인쇄하기

BioStar X와 cardPresso를 연동하여 사용자가 원하는 디자인의 카드를 인쇄할 수 있습니다. cardPresso는 카드 디자인 및 인쇄를 위한 전문 소프트웨어입니다. cardPresso를 사용하면 다양한 카드 템플릿을 생성하고 사용자 정보를 카드에 맞게 배치할 수 있습니다.

시작하기 전에

BioStar X의 카드 프린터 기능을 사용하려면 cardPresso 프로그램을 설치하고 **BioStar X**와 연결해야 합니다. cardPresso 프로그램의 웹 인쇄 서버 기능을 사용하려면 cardPresso XXL edition 라이선스가 필요합니다.

알아두기

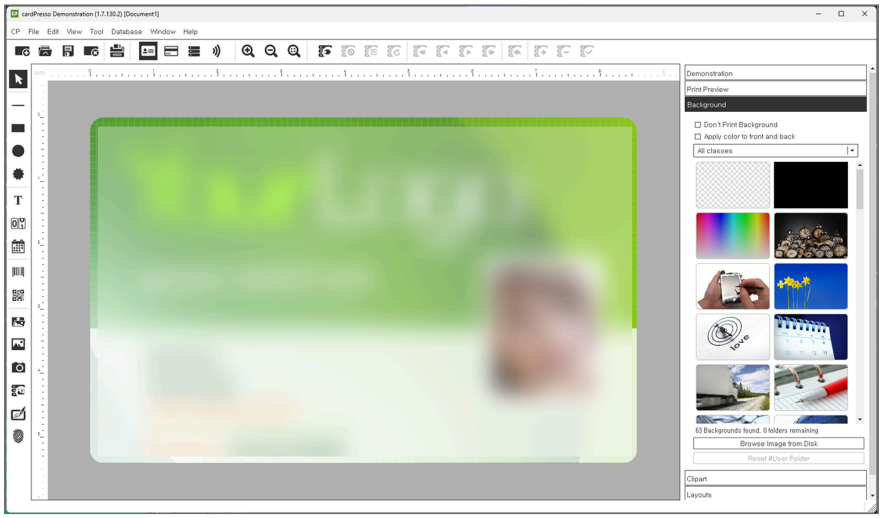
- cardPresso 프로그램의 라이선스 유형에 대한 자세한 내용은 cardPresso Editions 페이지를 참고하세요.
- 웹 인쇄 서버 기능은 Windows 운영체제에서만 지원됩니다.

cardPresso 설치 및 설정하기

cardPresso 프로그램을 설치하고 웹 인쇄 서버를 설정하려면 아래 단계를 따르세요.

> 설치 버전에 따라 메뉴 경로나 화면이 다를 수 있습니다.

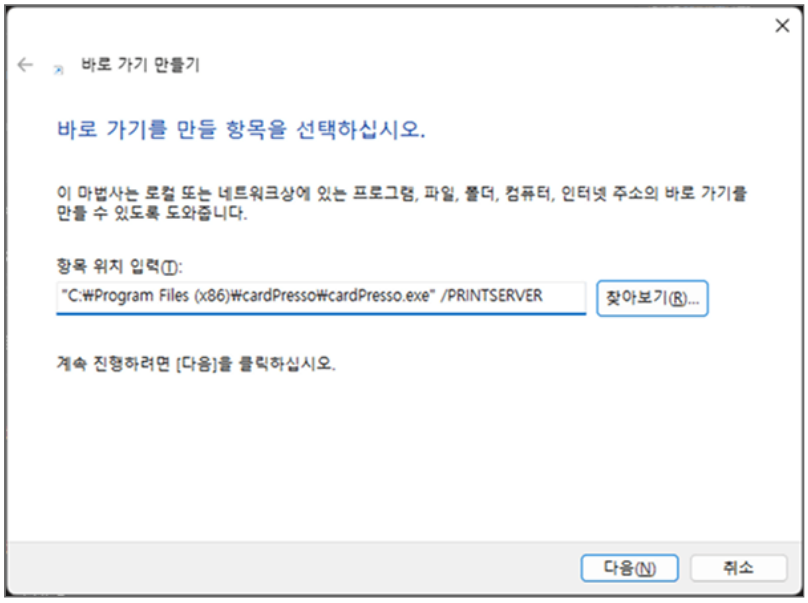
1. 웹 인쇄 서버로 운영할 PC의 운영체제에 맞는 최신 버전의 cardPresso를 cardPresso Download에서 다운로드하세요.
2. 프로그램을 설치하고 cardPresso에서 발급한 라이선스를 활성화하세요.
3. cardPresso를 실행한 후 카드 템플릿을 제작하세요.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

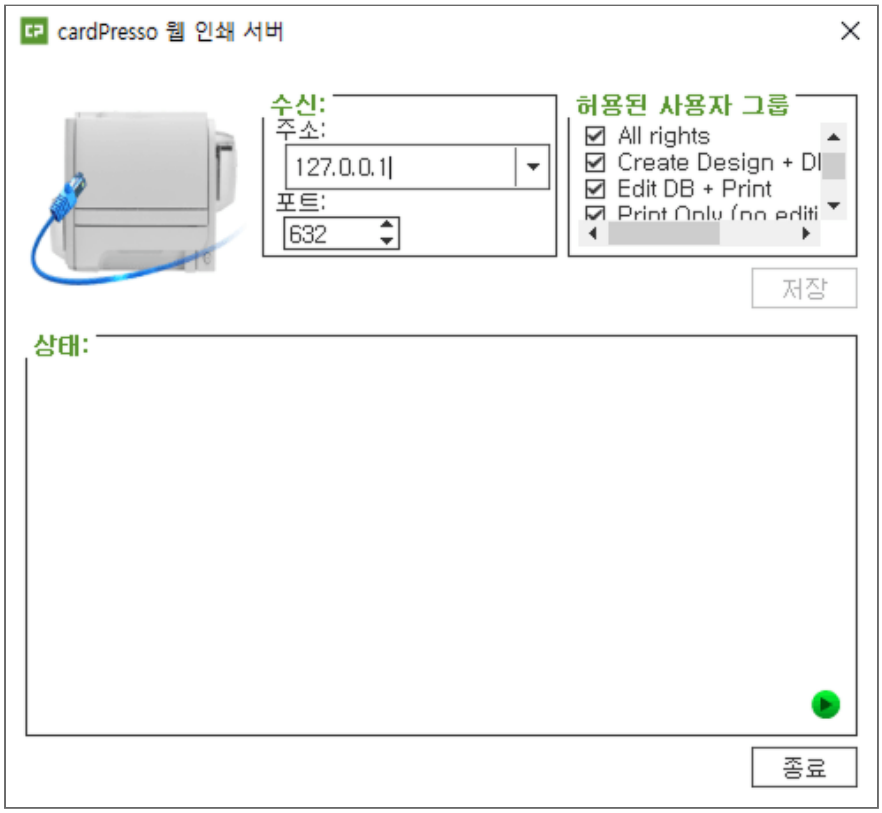
4. 제작한 카드 템플릿을 **BioStar X**를 설치한 서버의 원하는 경로에 저장하세요. (예, *C:\template\example.card*)
5. cardPresso를 설치한 PC의 바탕 화면에서 마우스 오른쪽 버튼을 클릭한 후 팝업 메뉴에서 **새로 만들기** → **바로 가기**를 클릭하세요.
6. **항목 위치 입력** 필드에 아래와 같이 입력한 후 **다음** 버튼을 클릭하세요.

```
"C:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER
```



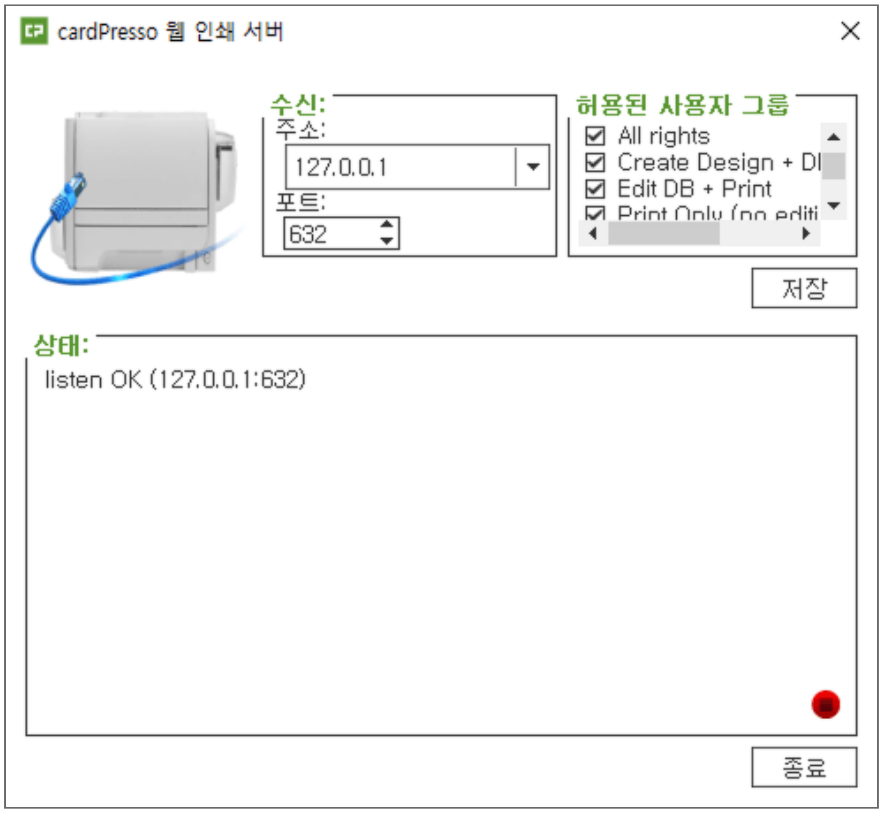
> 설치 환경에 따라 cardPresso가 설치된 경로가 다를 수 있습니다. cardPresso가 설치된 경로를 확인한 후, 위 경로를 알맞게 수정하세요.

7. 바로 가기 이름을 입력한 후 **마침** 버튼을 클릭하세요.
8. 바탕화면에 생성한 cardPresso 웹 인쇄 서버 바로가기 아이콘을 더블 클릭하여 실행하세요.
9. cardPresso 웹 인쇄 서버 창이 나타나면, **설정** 아이콘을 클릭하세요.



- **주소**: 웹 인쇄 서버로 동작하는 PC의 IP 주소를 입력하세요.
- **포트**: cardPresso에서 인쇄 동작을 수신하는데 사용하는 포트 번호입니다.
- **허용된 사용자 그룹**: 웹 인쇄 서버에 접근할 권한이 있는 사용자 그룹을 선택하세요.

10. 설정이 완료되면 **저장**을 클릭하세요.
11. 오른쪽 하단에 있는 을 클릭하여 서비스를 시작하세요. 알맞게 설정된 경우 아이콘이 로 변경되고 **listen OK** 메시지가 나타납니다.



> 카드 인쇄가 완료되기 전까지 창을 닫지 마세요.

cardPresso를 BioStar X에 연결하기

cardPresso를 **BioStar X**에 연결하려면 아래와 같이 설정하세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드 프린터**를 클릭하세요.
3. **cardPresso 설정**을 **사용**으로 설정한 뒤 각 항목을 입력하세요.



- **ID**: cardPresso 로그인 ID를 입력하세요. (기본값: ADMIN)
- **암호**: cardPresso 로그인 암호를 입력하세요. (기본값: admin)
- **IP 주소**: 웹 인쇄 서버로 동작하는 PC의 IP 주소를 입력하세요.
- **Port**: cardPresso에서 인쇄 동작을 수신하는데 사용하는 포트 번호입니다.
- **프린터 이름**: 카드 프린터로 사용할 프린터 이름을 입력하세요. Windows의 **제어판** → **장치 및 프린터**에서 확인할 수 있습니다.

- **카드 템플릿**: **+ 추가**를 클릭해 **카드 템플릿**을 추가할 수 있습니다. **이름** 항목에 카드 템플릿의 파일명과 확장자가 포함된 전체 경로를 입력하세요.
  - 카드 템플릿의 파일명은 영문, 숫자, 특수 기호로 설정할 수 있습니다.
  - 최대 20개의 카드 템플릿을 지원합니다.
  - 경로 예시: C:\template\example.card
- **카드 템플릿 테스트 인쇄**: 카드 템플릿을 테스트 인쇄할 수 있습니다.

4. 설정을 완료하면 **확인**을 클릭하세요.

카드 템플릿 테스트 인쇄하기

Administrator 정보를 가진 카드 템플릿을 테스트 인쇄할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **카드 프린터**를 클릭하세요.
3. 인쇄하려는 카드 템플릿을 선택한 후, **테스트 인쇄** 버튼을 클릭하세요.

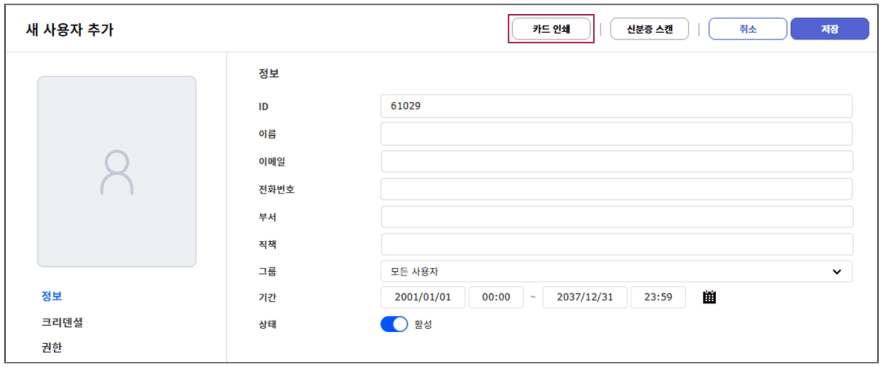


4. Administrator 정보를 가진 카드 템플릿이 인쇄됩니다.

사용자별 카드 템플릿 인쇄하기

사용자별 정보를 가진 카드 템플릿으로 카드를 인쇄할 수 있습니다.

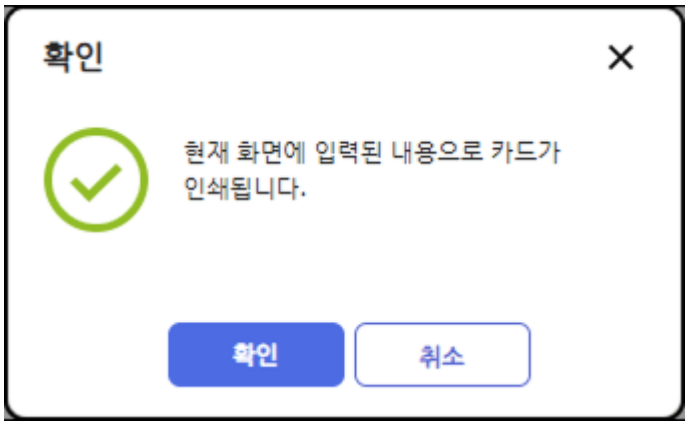
1. **런처** 페이지에서 **사용자**를 클릭하세요.
2. 화면 오른쪽 상단의 **새 사용자** 버튼을 클릭하세요. **새 사용자** 창이 나타납니다.
3. 양식을 입력하고 **카드 인쇄** 버튼을 클릭하세요.
   - 사용자 정보는 영문, 숫자, 특수 기호로 입력할 수 있습니다.



4. 인쇄하려는 카드 템플릿을 선택하고 **인쇄** 버튼을 클릭하세요.



5. 카드 인쇄 여부를 묻는 팝업창이 나타나면 **확인** 버튼을 클릭하세요.



새 사용자가 생성되고 사용자 정보를 가진 카드 템플릿으로 카드가 인쇄됩니다.

커스텀 사용자 필드 추가하기

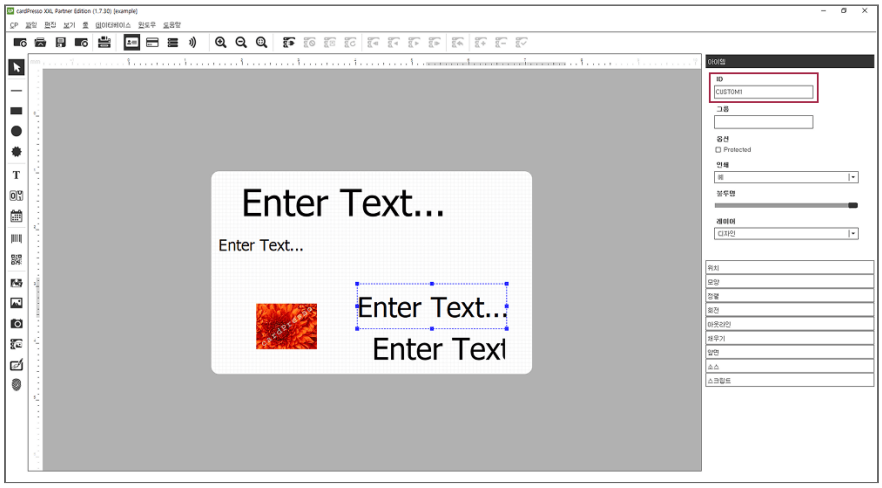
커스텀 사용자 필드를 추가한 카드 템플릿으로 카드를 인쇄할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **서버**를 클릭하세요.
3. **사용자 및 장치 관리** 섹션의 **커스텀 사용자 필드** 항목에서 **+ 추가** 버튼을 클릭해 **이름**을 입력하고 **유형**을 선택하세요. 추가한 **커스텀 사용자 필드**의 순서대로 카드 템플릿의 속성 **ID**가 결정됩니다.



BioStar X 속성 ID 기준으로 **순서 1**은 **CUSTOM1**과 같습니다. BioStar X 속성 ID에 대한 자세한 내용은 카드 템플릿 속성 ID를 참고하세요.

4. 설정을 완료하면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.
5. cardPresso 프로그램에서 **파일** → **템플릿 열기**를 클릭해 카드 템플릿 파일을 여세요. 새로운 속성을 추가하고 BioStar X 속성 ID 순서에 알맞은 **XML 항목 ID 이름**으로 **ID**를 입력하세요.



6. 설정이 완료되면 **파일** → **저장**을 클릭하세요.

7. **BioStar X**로 돌아와 **사용자** 페이지에서 카드 템플릿을 적용할 사용자를 선택하세요.

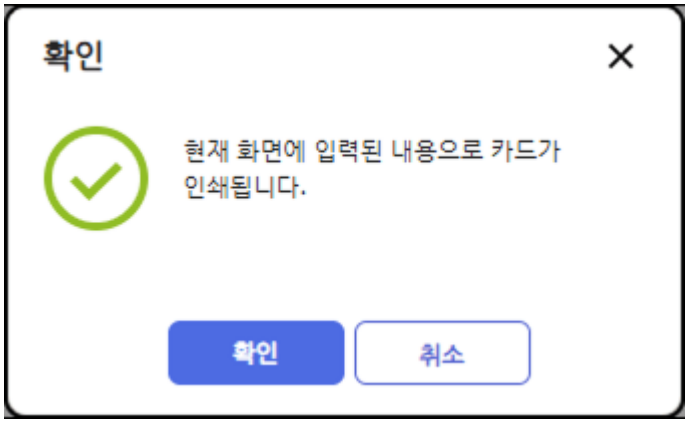
8. 추가한 커스텀 사용자 필드 항목을 확인할 수 있습니다. 해당 양식에 맞게 입력하고 **카드 인쇄** 버튼을 클릭하세요.



9. 인쇄하려는 카드 템플릿을 선택하고 **인쇄** 버튼을 클릭하세요.



10. 카드 인쇄 여부를 묻는 팝업창이 나타나면 **확인** 버튼을 클릭하세요.



사용자 정보가 저장되고 커스텀 사용자 필드를 추가한 카드 템플릿으로 카드가 인쇄됩니다.

카드 템플릿 속성 ID

BioStar X에서 지원하는 속성 ID는 아래와 같습니다. 카드 템플릿 생성 시, 속성 ID를 알맞은 **XML 항목 ID 이름**으로 입력하세요.

목록	BioStar X 사용자 데이터	XML 항목 ID 이름
1	User ID	ID
2	User Name	NAME
3	Email	EMAIL
4	Department	DEPARTMENT
5	Telephone	TELEPHONE
6	User Group	GROUP
7	Profile Photo	PHOTO
8	Custom Field 1	CUSTOM1
9	Custom Field 2	CUSTOM2
10	Custom Field 3	CUSTOM3
11	Custom Field 4	CUSTOM4
12	Custom Field 5	CUSTOM5
13	Custom Field 6	CUSTOM6
14	Custom Field 7	CUSTOM7
15	Custom Field 8	CUSTOM8

목록	BioStar X 사용자 데이터	XML 항목 ID 이름
16	Custom Field 9	CUSTOM9
17	Custom Field 10	CUSTOM10

모바일 출입 카드 관리하기

에어팝 포털(Airfob Portal)을 연동하여 **BioStar X**에서 사용자에게 모바일 출입 카드를 발급하거나 삭제할 수 있습니다.

사용자는 에어팝 포털에 가입하거나 별도로 모바일 출입 카드를 등록하지 않아도 이메일로 수신된 링크를 통해 모바일 출입 카드를 발급 받을 수 있습니다.

알아두기

- 모바일 출입 카드는 **CSN Mobile** 카드와 **템플릿 온 모바일** 중 한 가지만 사용할 수 있습니다.
- **CSN Mobile** 카드를 사용할 수 있는 장치와 펌웨어 버전은 아래를 참고하세요.

  ▼ CSN Mobile 카드 지원 장치 및 펌웨어 버전 보기

  - BioStation 3 Max 펌웨어 1.0.0 이상
  - XPass Q2 펌웨어 1.0.0 이상
  - BioEntry W3 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.0.0 이상
  - X-Station 2 펌웨어 1.0.0 이상
  - FaceStation F2 펌웨어 1.0.0 이상
  - XPass 2 펌웨어 1.1.0 이상
  - FaceLite 펌웨어 1.2.0 이상
  - BioLite N2 펌웨어 1.3.0 이상
  - XPass D2(Rev 2) 펌웨어 1.4.0 이상
  - FaceStation 2 펌웨어 1.4.0 이상
  - BioEntry W2(Rev 2) 펌웨어 1.6.0 이상
  - BioStation A2 펌웨어 1.8.0 이상 (NFC 지원 모델)
  - BioStation 2 펌웨어 1.9.0 이상 (NFC 지원 모델)

- **템플릿 온 모바일**을 사용할 수 있는 장치와 펌웨어 버전은 아래를 참고하세요.
  - BioStation 3 Max 펌웨어 1.0.0 이상
  - BioEntry W3 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.2.0 이상

슈프리마 모바일 출입 카드를 사용하기 위해 에어팝 포털에 가입하고 사이트를 개설해야 합니다. 에어팝 포털에 가입한 후, **BioStar X**에서 모바일 출입 카드를 관리할 수 있습니다.

1 에어팝 포털 가입 및 사이트 개설

에어팝 포털(Airfob Portal)에서 모바일 출입 카드 및 등록 장치를 설정하고, 사이트 및 크레딧을 관리할 수 있습니다.

1. 에어팝 포털(Airfob Portal)에 접속하세요.
2. **시작하기**를 클릭해 회원가입 및 사이트 개설을 진행하세요.
3. 이메일 입력 필드에 에어팝 포털 관리자의 이메일 주소를 입력한 뒤 **시작하기**를 클릭하세요. 입력한 이메일 주소로 인증 코드가 전송됩니다.
4. 인증 코드 입력란에 이메일로 수신한 인증 코드를 입력한 뒤 **확인**을 클릭하세요.

> 인증 코드는 6자리 숫자입니다.

5. 개인 정보 정책 및 약관을 확인한 뒤 **동의**를 클릭하세요.
6. 에어팝 포털에서 사용할 비밀번호 및 닉네임을 설정한 뒤 **계정 생성**을 클릭하세요. 계정 생성이 완료됩니다.
7. 계정 생성이 완료되면 **로그인**을 클릭하세요.
8. 이메일과 비밀번호를 입력한 뒤 **로그인**을 클릭하세요.
9. **사이트 생성**을 클릭해 사이트 개설을 진행하세요.

> **사이트**는 모바일 출입 카드를 사용하는 조직 또는 회사를 의미합니다.

10. 사이트의 이름 및 국가를 설정하고 **다음**을 클릭하세요.
11. 사이트 종류를 선택하세요.

> 사이트 종류에 따라 카드의 유형을 **다이나믹** 또는 **레귤러**로 선택할 수 있습니다.
> - **다이나믹**: 장치 및 사용 기간에 따라 크레딧을 차감하는 유형으로, 카드를 발급한 뒤에도 회수, 중지, 재발급, 만료 날짜 지정과 같은 관리가 가능합니다. 따라서 피트니스 클럽이나 독서실과 같은 회원제 시설 또는 공유 사무실에서 사용할 수 있습니다.
> - **레귤러**: 발급한 카드 개수에 따라 크레딧을 차감하는 유형으로, 관리자가 **BioStar X**에서 카드를 삭제하기 전까지 영구적으로 사용할 수 있습니다. 따라서 일반 회사나 집단에서 사원증 및 출입증으로 사용할 수 있습니다.

12. **생성**을 클릭하세요. 사이트 생성이 완료됩니다.
13. 사이트 이름을 클릭해 해당 사이트의 에어팝 포털에 접속하세요.

> **알아두기**
> 에어팝 포털 사용에 대한 자세한 내용은 다음 링크를 참고하세요.

2 BioStar X에서 모바일 출입 카드 구성

모바일 출입 카드 사용 여부를 설정하고, 에어팝 포털 연동과 관련된 설정을 관리할 수 있습니다. 또한 모바일 출입 카드를 사용할 장치를 등록할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **모바일 출입 카드**을 클릭하세요.
3. 각 항목을 설정하세요.



- **모바일 출입 카드 설정**: 모바일 출입 카드 사용 여부를 설정할 수 있습니다. **사용**으로 설정하면 사용자에게 모바일 출입 카드를 발급할 수 있습니다.
- **사이트 ID**: 에어팝 포털에서 개설한 사이트 ID를 입력하세요. 사이트 ID는 에어팝 포털의 **설정**(Settings) → **사이트**(Site) 메뉴 경로에서 확인할 수 있습니다.
- **이메일**: 모바일 출입 카드 관리자 계정의 이메일 주소를 입력하세요.
- **암호**: 모바일 출입 카드 관리자 계정의 암호를 입력하세요.

4. 모든 설정을 마쳤다면 **연결** 버튼을 클릭하세요.

> **알아두기**
>
> BioStar X에서 모바일 출입 카드를 사용하려면 에어팝 포털 가입 및 초기 설정을 먼저 완료하세요. 자세한 내용은 에어팝 포털 가입 및 사이트 개설을 참고하세요.

3 장치 등록

에어팝 패스(Airfob Pass) 애플리케이션 또는 **BioStar X**에서 직접 모바일 출입 카드를 사용할 장치를 등록할 수 있습니다.

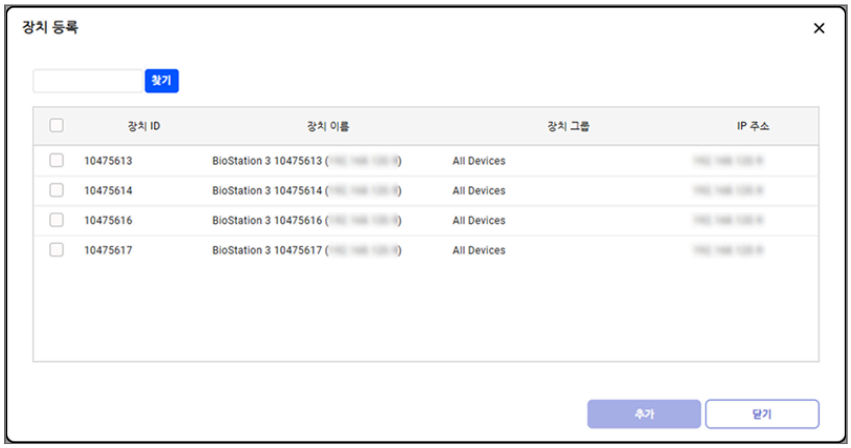


에어팝 포털(Airfob Portal)과 연동을 위한 설정을 완료하면 **연결** 버튼을 클릭하세요. **장치 등록** 옵션을 사용할 수 있습니다.

1. 모바일 출입 카드를 사용할 장치를 추가하려면 **+ 추가** 버튼을 클릭하세요.



2. **장치 등록** 창의 장치 목록에서 모바일 출입 카드를 사용할 장치의 체크박스를 클릭하세요.



3. 장치를 모두 선택했다면 **추가** 버튼을 클릭하세요.

장치 목록에서 추가된 장치를 확인할 수 있습니다.

- 모바일 출입 카드 인증서를 재전송하려면 ↻ 버튼을 클릭하세요.
- 등록된 장치를 삭제하려면 🗑 버튼을 클릭하세요.

알아두기

- 모바일 출입 카드를 사용할 수 있는 장치와 펌웨어 버전은 아래를 참고하세요.

  ▼ 모바일 출입 카드를 사용할 수 있는 장치 및 펌웨어 버전 보기

  - BioStation 3 Max 펌웨어 1.0.0 이상
  - XPass Q2 펌웨어 1.0.0 이상
  - BioEntry W3 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.0.0 이상
  - X-Station 2 펌웨어 1.0.0 이상
  - FaceStation F2 펌웨어 1.0.0 이상
  - XPass 2 펌웨어 1.1.0 이상
  - FaceLite 펌웨어 1.2.0 이상
  - BioLite N2 펌웨어 1.3.0 이상
  - XPass D2(Rev 2) 펌웨어 1.4.0 이상
  - FaceStation 2 펌웨어 1.4.0 이상
  - BioEntry W2(Rev 2) 펌웨어 1.6.0 이상
  - BioStation A2 펌웨어 1.8.0 이상 (NFC 지원 모델)
  - BioStation 2 펌웨어 1.9.0 이상 (NFC 지원 모델)

- 에어팝 패스(Airfob Pass) 애플리케이션을 이용해 장치를 등록할 수도 있습니다.
- 등록된 장치를 삭제할 경우 장치에 전송된 모바일 출입 카드 인증서가 삭제됩니다.

4 모바일 출입 카드 발급

BioStar X에 등록된 사용자에게 모바일 출입 카드를 발급할 수 있습니다. 사용자에게 모바일 출입 카드를 발급하려면 모바일 출입 카드 발송 방법에 따른 사용자 정보를 필수적으로 입력해야 합니다. 자세한 내용은 다음 문서를 참고하세요.

- 사용자 등록하기
- 모바일 출입 카드 등록하기

IR 페이스 그룹 매칭 설정하기

IR 페이스 그룹 매칭은 사용자 그룹을 기반으로 매칭 그룹을 설정하여 사용자를 인증하는 기능입니다. 이 기능을 사용하면 특정 사용자 그룹에 속한 사용자만 IR 페이스 인증을 통해 출입을 허용할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **크리덴셜** → **IR 페이스 그룹 매칭**를 클릭하세요.
3. **그룹 매칭 사용 여부** 옵션을 **사용**으로 변경하세요.



4. **그룹 매칭 용 장치 설정**에서 **+ 추가** 버튼을 클릭하세요.
5. **그룹 매칭 용 장치 설정** 창이 나타나면 원하는 장치를 선택하고 **추가** 버튼을 클릭하세요.

> FaceStation 2 모델만 선택할 수 있습니다.

6. **매칭 그룹 설정**에서 **+ 추가** 버튼을 클릭하세요.
7. **그룹 이름** 및 **사용자 그룹** 항목을 설정하세요.
8. 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

알아두기

- 최대 10개의 매칭 그룹을 생성할 수 있습니다.
- 그룹당 최대 3,000개의 IR 페이스 템플릿을 포함할 수 있습니다.
- 하나의 매칭 그룹에 여러 개의 사용자 그룹을 설정할 수 있습니다.
- 매칭 그룹의 전체 IR 페이스 템플릿 수는 5,000개를 초과할 수 없습니다.
- 사용자 그룹에 포함된 IR 페이스 템플릿이 3,000 개를 초과하면 매칭 그룹으로 설정할 수 없습니다.
- 이 기능은 FaceStation 2 모델만 지원합니다.
- 그룹 매칭 기능을 비활성화하려면 이미 설정된 장치와 그룹 설정을 모두 삭제해야 합니다.

라이선스 활성화하기

BioStar X 라이선스 및 장치 라이선스를 활성화 방법을 안내합니다.

BioStar X 라이선스

구매한 BioStar X 라이선스를 등록할 수 있습니다.

사용자의 네트워크 환경에 따라 **BioStar X 라이선스**를 등록할 수 있는 방법이 다릅니다. 제공하는 안내에 따라 네트워크 상태를 확인하고 라이선스를 활성화하세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **라이선스** → **BioStar X 라이선스**를 클릭하세요.

> **알아두기**
>
> - 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
> - 라이선스 에러코드를 확인하려면 다음 링크를 참고하세요.

온라인 상태에서 등록

> **알아두기**
>
> 라이선스 키는 숫자와 하이픈(`-`)만 입력할 수 있습니다. `1111-1111-1111-1111` 형식으로 최대 16자의 숫자를 입력해야 합니다.

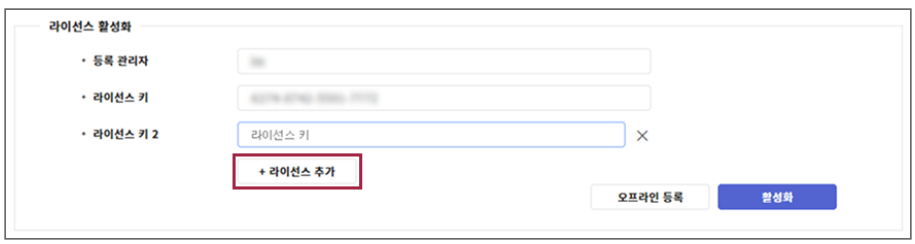
단일 라이선스 등록

인터넷이 연결된 온라인 상태에서 BioStar X 라이선스를 활성화하려면, 이름과 전달받은 라이선스 키를 입력하고, **활성화** 버튼을 클릭하세요.



여러 개의 라이선스 등록

최대 30개까지의 라이선스를 한 번에 추가할 수 있습니다. ＋ **라이선스 추가** 버튼을 클릭하세요. 라이선스를 모두 입력한 후 **활성화** 버튼을 클릭하세요.



- 입력 칸이 30개에 도달하면 ＋ **라이선스 추가** 버튼이 비활성화되어 더 이상 추가할 수 없습니다.
- 여러 개의 라이선스 키를 한 번에 복사해 입력 칸에 붙여넣으면, `1111-1111-1111-1111` 형식에 맞는 키만 자동으로 인식해 각 입력 칸에 나눠 추가합니다.
- 붙여넣은 키가 30개를 초과하면 30개까지만 자동으로 입력되고, 초과한 키는 무시됩니다.

활성화 진행 상태

활성화 버튼을 클릭하면 진행 상태 팝업이 표시됩니다. 활성화가 완료될 때까지 페이지나 팝업을 닫지 마세요.

오프라인 상태에서 등록

폐쇄된 네트워크 환경이나 인터넷 연결이 제한된 오프라인 상태에서 **BioStar X** 라이선스를 활성화하려면 다음의 안내에 따르세요.

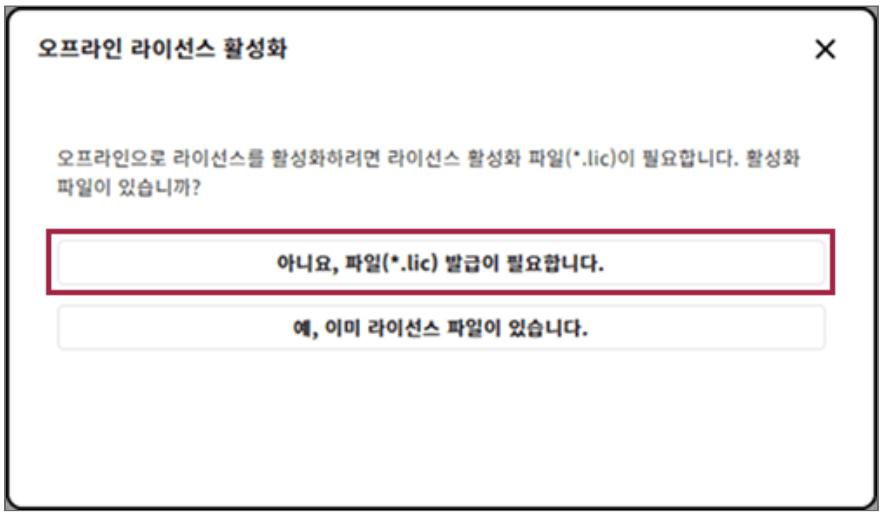
1. **라이선스 활성화** 섹션에서 임의의 등록 관리자 이름과 라이선스 키를 입력하세요.

   - 라이선스 키는 숫자와 하이픈(`-`)만 입력할 수 있습니다. `1111-1111-1111-1111` 형식으로 최대 16자의 숫자를 입력해야 합니다.
   - 등록 관리자 이름과 라이선스 키를 기억하거나 메모해두세요.
   - 여러 개의 라이선스가 필요하다면 ＋ **라이선스 추가** 버튼을 클릭해 추가하세요.

2. **오프라인 등록** 버튼을 클릭하세요.

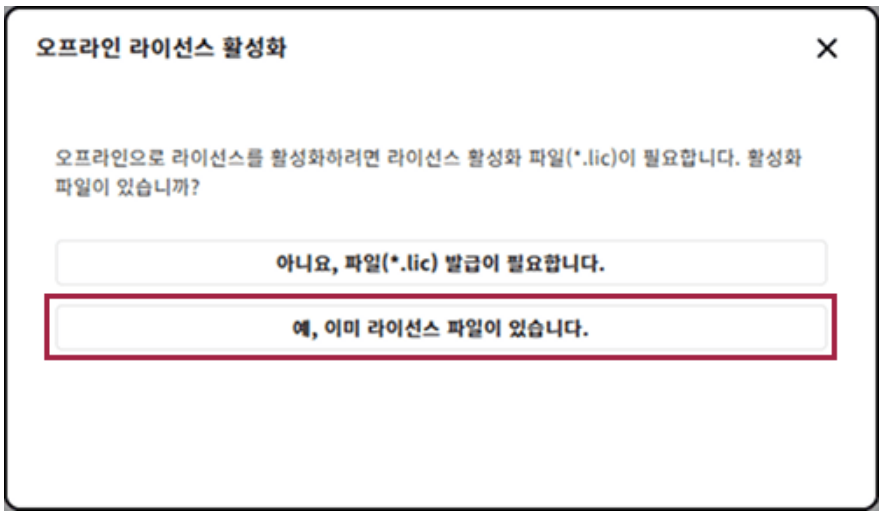


3. **오프라인 라이선스 활성** 창이 나타나면 **아니요, 파일(*.lic) 발급이 필요합니다.** 버튼을 클릭하세요.



이미 발급받은 라이선스 파일이 있다면, 이 화면에서 **예, 이미 라이선스 파일이 있습니다.** 버튼을 클릭한 후 9단계로 이동하세요.

4. 발급 요청 파일(*.req)이 생성되면 사용자의 로컬 디스크에 다운로드하세요.
5. 다운로드한 발급 요청 파일을 구매처에 보내 오프라인 활성화 파일(*.lic)을 요청하세요.
6. 오프라인 활성화 파일을 전달 받은 후 1단계에서 입력한 관리자 이름과 라이선스 키를 **라이선스 활성화** 섹션에 입력하세요.
7. **오프라인 등록** 버튼을 클릭하세요.
8. **오프라인 라이선스 활성** 창이 나타나면 **예, 이미 라이선스 파일이 있습니다.** 버튼을 클릭하세요.



9. 파일 열기 창이 나타나면 로컬에 저장된 오프라인 활성화 파일(*.lic) 또는 압축 파일(*.zip)을 선택하세요.

> 여러 개의 라이선스를 요청했을 때는 압축 파일을 전달받을 수 있습니다.

10. 진행 상태 팝업이 표시됩니다. 활성화가 완료될 때까지 페이지나 팝업을 닫지 마세요.

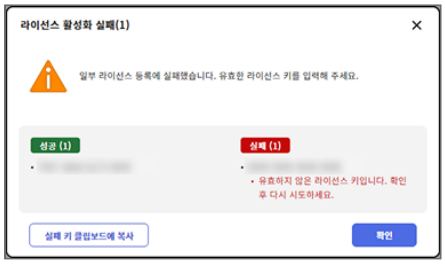
라이선스 활성화 결과 확인

입력한 라이선스 키의 활성화 결과에 따라 다음과 같이 안내가 표시됩니다.

- 입력한 모든 라이선스 키가 유효하면 성공 메시지가 표시됩니다.



- 일부 키만 활성화에 성공했거나 모든 키가 실패하면, 키별 성공·실패 여부와 실패 사유를 확인할 수 있습니다. 성공한 키의 입력란은 초기화되고, 실패한 키는 재입력할 수 있도록 입력란에 그대로 남습니다.





- 인터넷 연결이 되지 않아 모든 키가 실패하면, 인터넷 연결을 확인한 후 다시 시도하라는 안내와 함께 **오프라인 등록** 버튼이 표시됩니다. 폐쇄된 네트워크 환경이라면 이 버튼을 클릭해 오프라인 상태에서 등록하세요.

> **알아두기**
> 실패한 키를 복사하려면 **실패 키 클립보드에 복사** 버튼을 클릭하세요.

활성화된 라이선스 확인

등록한 **BioStar X** 라이선스 정보는 **활성화된 라이선스**에서 확인할 수 있습니다.



장치 라이선스

슈프리마에서 발급한 **장치 라이선스**를 활성화하여 라이선스에 해당하는 특정 기능을 사용하세요.

장치 라이선스는 **BioStar X** 및 USB 메모리를 이용하여 장치의 라이선스를 활성화할 수 있습니다.

알아두기

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

시작하기 전에

장치 라이선스를 활성화하기 전에 다음 사항을 확인하세요.

- 유효한 장치 라이선스 파일을 준비하세요. 장치 라이선스 파일은 구입처에 문의하세요.
- 대상 장치가 **BioStar X**에 등록되어 있는지 확인하세요. 장치 등록에 대한 자세한 내용은 장치 등록하기를 참고하세요.

장치 라이선스 적용

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **라이선스** → **장치 라이선스**를 클릭하세요.
3. **찾아보기** 버튼을 클릭하세요.



4. 장치 라이선스가 저장된 경로에서 장치 라이선스 파일을 불러오세요.
5. 불러온 라이선스에 해당하는 정보가 **라이선스 종류**, **대상 장치 수**, **장치 목록** 항목에 표시됩니다.



6. **장치 목록**을 확인하고, 장치 라이선스를 활성화하려면 **활성화** 버튼을 클릭하세요.

알아두기

라이선스 활성화를 실패하면 오류 메시지가 표시됩니다. 라이선스 활성화를 다시 시도하세요.

장치 라이선스 정보

장치 라이선스 파일을 불러오면 다음 정보가 표시됩니다.

- **라이선스 종류**: 장치 라이선스 파일에 포함된 라이선스의 종류를 확인할 수 있습니다.
  - Camera QR

    > **Camera QR**을 사용할 수 있는 장치는 아래와 같습니다.
    > - BioStation 3 Max 펌웨어 1.0.0 이상
    > - XPass Q2 펌웨어 1.0.0 이상
    > - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) 펌웨어 1.2.0 이상
    > - X-Station 2 (XS2-QDPB, XS2-QAPB) 펌웨어 1.4.1 이상
    > - BioStation 3 펌웨어 1.1.0 이상

  - **다중 얼굴 인증**

    > **다중 얼굴 인증** 라이선스를 사용할 수 있는 장치는 아래와 같습니다.
    >
    > - BioStation 3 펌웨어 1.5.0 이상
    >
    > 이 라이선스를 활성화한 장치에서 **다중 얼굴 인증** 옵션 설정 방법은 인증 설정하기를 참고하세요.

  - 무선 도어락

    > - 지원되는 OSDP 안테나와 무선 도어락은 다음과 같습니다.
    >   - U&Z OSDP 안테나: CX8936
    >   - U&Z 무선 도어락: CX217x(Handle), CX212x(Knob)
    > - 연결하려는 무선 도어락 대수만큼 최대 12대까지 장치 라이선스를 발급받을 수 있습니다.
    > - 장치 라이선스로 연결할 수 있는 무선 도어락의 최대 장치 수는 12대입니다. 장치 라이선스 여러개를 활성화하여도 12대를 초과할 수 없습니다.

- **대상 장치 수**: 장치 라이선스 파일에 포함된 장치의 수를 확인할 수 있습니다.
- **라이선스 수**: 장치 라이선스로 활성화할 수 있는 무선 도어락의 대수를 확인할 수 있습니다.
- **장치 목록**: 장치 라이선스 파일에 포함된 장치의 상세 정보를 확인할 수 있습니다.
  - **장치 ID**: 장치를 식별하는 고유 아이디입니다.
  - **장치 이름**: 장치의 이름입니다.
  - **모델명**: 장치의 모델명입니다.
  - **장치 상태**: 장치의 현재 상태입니다. **정상** 상태의 장치만 라이선스를 활성화할 수 있습니다.
    - **정상**, **연결 끊김**, **미지원**, **미등록**

    > 장치가 라이선스의 기능을 지원하지 않는 모델이거나 펌웨어 버전이 낮으면 **장치 상태**가 **미지원**으로 표시됩니다. 해당 기능의 지원 모델과 펌웨어 버전을 확인하세요.

- **라이선스 상태**: 라이선스 활성화 여부입니다. **비활성** 상태의 장치만 라이선스를 활성화할 수 있습니다.
  - **비활성**, **활성**, **해당 없음**
- **활성화된 수**: 무선 도어락의 연결 현황입니다.

> **알아두기**
>
> - **라이선스 수**, **활성화된 수** 항목은 무선 도어락 장치 라이선스를 불러들였을 때만 값이 표시됩니다.

감사 추적 관리하기

감사 추적 기능은 시스템에서 발생하는 모든 활동을 기록하고 추적하는 기능입니다. 사용자의 로그인/로그아웃, 설정 변경, 시스템 관리 작업 등 모든 활동이 기록되어 보안 감사와 시스템 모니터링에 활용할 수 있습니다.

화면 왼쪽 사이드바의 **감사 추적** 그룹에는 다음 메뉴가 있습니다.

- **출입 통제 감사 로그**: 사용자, 장치, 출입문 등 출입 통제와 관련된 모든 생성·수정·삭제·조회·내보내기·가져오기·운영 활동을 기록합니다.
- **감사 설정**: 감사 로그의 보관 기간과 조회 기록 여부를 설정합니다.

> **알아두기**
>
> **T&A 감사 로그**에 대한 자세한 내용은 근태 감사 로그 조회하기를 참고하세요. **T&A 감사 로그** 메뉴는 근태 관리(T&A) 라이선스가 활성화되어 있어야 사용할 수 있습니다.

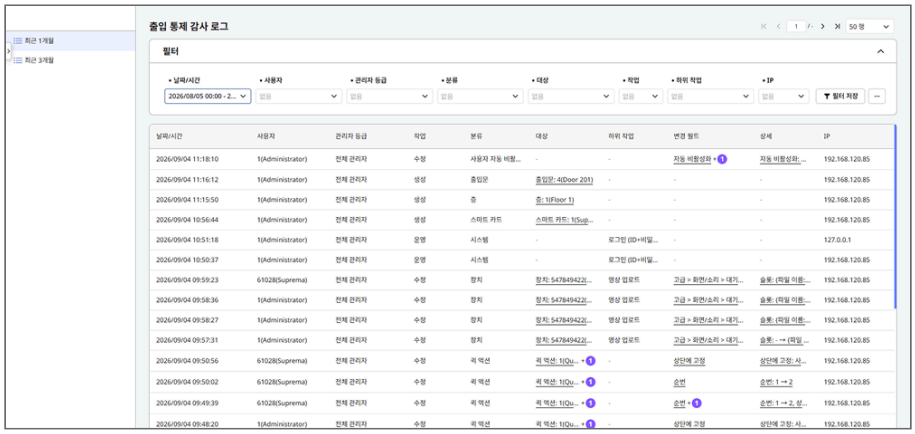
출입 통제 감사 로그 조회하기

출입 통제 감사 로그 기능은 사용자, 장치, 출입문 등 출입 통제와 관련된 모든 생성 및 수정, 삭제, 조회, 내보내기, 가져오기, 운영 활동을 기록합니다. 각 기록은 언제, 누가, 무엇을, 어떻게 변경했는지 함께 보여주므로 보안 감사와 문제 해결에 활용할 수 있습니다.

- **보안 감사**: 비인가 접속 시도나 권한 남용을 탐지하세요.
- **문제 해결**: 시스템 오류 발생 시점과 설정 변경 이력을 추적하세요.
- **규정 준수**: 개인정보 조회 이력을 포함한 접근 기록을 보관하고 감사 보고서를 작성하세요.

출입 통제 감사 로그 확인

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **감사 추적** → **출입 통제 감사 로그**를 클릭하세요.
3. 감사 로그 목록이 화면에 표시됩니다.



> **알아두기**
>
> - 보관 기간 등 감사 로그 정책을 변경하려면 감사 설정 관리하기를 참고하세요.
> - 1.0.3 버전으로 업그레이드한 이후 새로 생성되는 감사 로그는 **설정** → **시스템** → **시스템 보안** 메뉴의 **개인 정보 DB 암호화** 옵션과 무관하게 암호화된 상태로 저장됩니다.
> - BioStar 2에서 **BioStar X**로 업그레이드한 후 감사 로그가 일부 기록되지 않으면 업그레이드하기를 참고하세요.

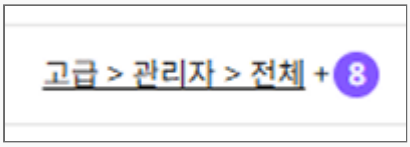
테이블 구성

감사 로그 목록 테이블은 10개 컬럼으로 구성되며, 현재 검색 조건에 해당하는 기록을 **날짜/시간** 기준 최신순으로 표시합니다.

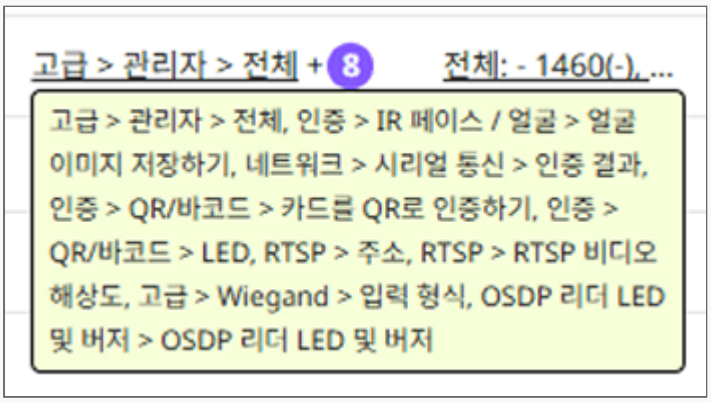
컬럼	설명
날짜/시간	이벤트가 발생한 날짜와 시간입니다.
사용자	이벤트를 수행한 사용자입니다. **id(이름)** 형식으로 표시됩니다.
관리자 등급	이벤트를 수행한 사용자의 관리자 등급입니다.
작업	수행된 동작 종류입니다. **생성**, **수정**, **삭제**, **조회**, **내보내기**, **가져오기**, **운영** 중 하나로 분류됩니다.
분류	이벤트 대상의 도메인 분류입니다(예: 사용자, 장치, 출입문).
대상	동작이 적용된 대상입니다. **타입: id(이름)** 형식으로 표시됩니다.
하위 작업	로그인 방식, 알람 해제처럼 세부 동작 이름이 있는 경우에만 표시됩니다.
변경 필드	변경되거나 조회된 필드 이름입니다.
상세	동작별 상세 정보입니다. (예: 변경 값, 사유, 조회 조건 등)
IP	사용자가 접속한 IP 주소입니다. 시스템이 자동으로 발급한 기록은 **127.0.0.1**로 표시됩니다.

알아두기

- **대상**과 **변경 필드** 값이 2건 이상이면 첫 항목만 표시되고, 나머지는 오른쪽에 잔여 건수 배지(예: +208)로 압축됩니다. 잔여 건수가 1,000건 이상이면 +999로 표기하며, 정확한 총 건수는 상세 팝업 제목에서 확인할 수 있습니다. 배지를 클릭하면 해당 셀의 상세 팝업이 열립니다.

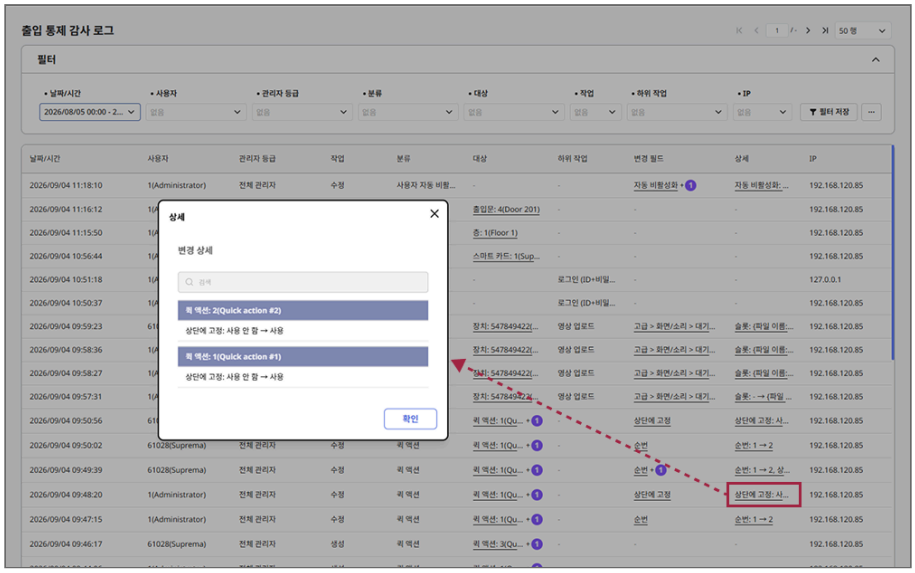


- 셀 값이 길면 한 줄로 말줄임 처리됩니다. 마우스를 오버하면 전체 값이 툴팁으로 표시되며, 툴팁을 벗어나는 길이는 ... 으로 줄여 표기됩니다.



상세 정보 확인

값이 있는 **대상**, **변경 필드**, **상세** 열은 밑줄로 표시되며 클릭할 수 있습니다. 해당 열의 값을 클릭하면 동작에 맞는 상세 팝업이 열리고, 팝업을 닫으려면 **확인** 버튼 또는 ✕ 버튼을 클릭하세요.



팝업 상단의 **검색** 입력 필드에 검색어를 입력하면 일치하는 항목만 강조되거나 필터링됩니다. 대상 팝업은 검색 시 그룹과 그룹별 건수도 함께 갱신되지만, 제목의 전체 건수는 검색과 관계없이 그대로 유지됩니다.

필터로 원하는 기록 찾기

필터 섹션에서 제공하는 필터를 조합해 원하는 기록을 좁혀서 찾으세요. 한 필터 안에서 여러 값을 선택하면 OR 로, 서로 다른 필터를 함께 적용하면 AND 로 결합됩니다.

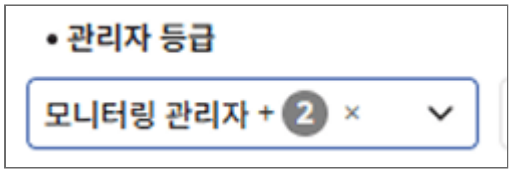


필터	동작 방식
날짜/시간	시작·종료 날짜와 시각을 지정합니다. 조회 기간에는 길이 제한이 없습니다.
사용자	검색어를 입력하고 Enter 키를 눌러 일치하는 사용자를 찾으세요. 처음 열면 목록이 비어 있습니다.
관리자 등급	검색어를 입력하고 Enter 키를 눌러 일치하는 관리자 등급을 찾으세요.
분류	검색 가능한 체크박스 목록에서 하나 이상의 분류를 선택하세요.
대상	검색어를 입력하고 Enter 키를 눌러 일치하는 대상을 찾으세요.
작업	체크박스 목록에서 하나 이상의 동작을 선택하세요.
하위 작업	검색 가능한 목록에서 세부 작업을 선택하세요.
IP	검색어를 입력하고 Enter 키를 눌러 일치하는 IP를 찾으세요.

- 적용된 필터가 없으면 현재 날짜로부터 30일 전까지의 기록을 기본 표시합니다.
- 각 필터 팝업에서 원하는 값을 선택한 뒤 **조건 추가** 버튼을 클릭하면 즉시 검색에 반영됩니다. **취소**을 클릭하면 선택을 취소하고 팝업을 닫습니다.



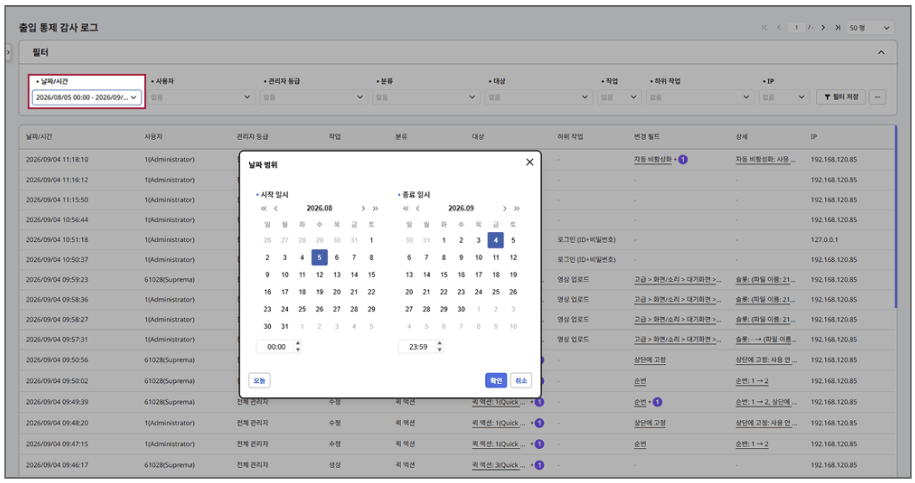
- 적용된 필터는 첫 항목과 추가 건수로 요약되어 표시됩니다. ✕ 버튼을 클릭하면 해당 필터만 해제됩니다. 값을 선택하지 않은 필터는 **없음**으로 표시됩니다.



> **알아두기**
>
> **사용자**, **관리자 등급**, **대상**, **IP** 필터는 검색어를 입력해야 결과가 나타납니다. 부분 일치를 지원하므로 이름이나 아이디의 일부만 입력해도 됩니다. 삭제된 대상은 **삭제됨** 표기로 함께 검색됩니다.

조회 기간 지정

날짜/시간를 클릭하면 **날짜 범위** 팝업이 열립니다.

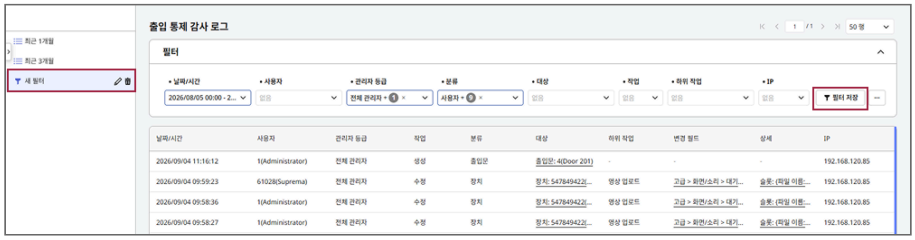


1. **시작 일시**과 **종료 일시**의 날짜와 시각을 각각 지정하세요. **오늘**를 클릭하면 오늘 날짜로 바로 이동합니다.
2. 조회 기간을 적용하려면 **확인** 버튼을 클릭하세요.

필터 저장

자주 사용하는 검색 조건은 **저장된 필터**에 저장해 두고 다시 불러올 수 있습니다.

1. 원하는 조건으로 필터를 설정하세요.
2. **필터** 섹션의 **필터 저장** 버튼을 클릭하세요.
3. 화면 왼쪽 필터 목록에 **새 필터** 항목이 추가됩니다.



- 필터 이름을 바꾸려면 ✎ 버튼을 클릭하고 새 이름을 입력한 뒤 `Enter` 키를 누르세요.
- 필터를 삭제하려면 🗑 버튼을 클릭하세요.

> **알아두기**
> 저장할 수 있는 필터는 최대 20개입니다. 저장한 필터는 브라우저에 보관되므로 다른 PC나 브라우저에서는 표시되지 않습니다.

페이지 탐색

페이지를 이동하거나 한 페이지에 표시할 목록 개수를 설정할 수 있습니다.

- |< : 처음 페이지로 이동합니다.
- < : 이전 페이지로 이동합니다.
- > : 다음 페이지로 이동합니다.
- >| : 마지막 페이지로 이동합니다.
- 50 행 : 한 페이지에 표시할 목록 개수를 선택합니다.

열 설정



감사 로그 테이블의 컬럼 위치를 바꾸거나 숨길 수 있습니다. **필터** 섹션 오른쪽의 ••• → **열 설정**을 클릭하세요.

- **[열 목록]**에서 숨기려는 항목의 체크박스 선택을 해제하세요.
- 열 순서를 바꾸려면 원하는 항목을 드래그하세요.
- 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

설정을 저장하려면 **적용** 버튼을 클릭하세요.

CSV로 내보내기

감사 로그를 CSV 파일로 내보내 외부 분석 도구에서 활용하세요.

1. **필터** 섹션에서 필요한 경우 필터를 설정하세요.
2. 섹션 오른쪽의 ••• → **CSV 내보내기**를 클릭하세요.
3. **CSV 내보내기** 창이 나타나면 **내보내기 사유**(선택 사항)를 입력하고 **적용** 버튼을 클릭하세요.



내보낸 CSV 파일은 레코드당 한 줄로 10개 컬럼을 모두 포함하며, 모든 값은 인용 부호로 감싸 표기됩니다. 대상이 여러 개인 값은 버티컬 바(|)로 구분되고(예: **User: 7(Kim)|User: 8(Lee)**), **상세** 값은 말줄임 없이 전체 대상과 전체 필드를 포함합니다.

> **주의**
> CSV 파일에는 스프레드시트 프로그램이 수식으로 해석할 수 있는 값이 원본 그대로 담깁니다. 내려받은 CSV 파일을 스프레드시트 프로그램에서 곧바로 열지 말고, 필요하면 텍스트 가져오기 기능으로 여세요.

> **팁**
> 필터를 설정했다면 필터링된 결과만 CSV 파일로 내보내집니다.

BioStar 2 기록 확인

이전 버전(BioStar 2)에서 남긴 기록도 같은 테이블에서 함께 조회할 수 있습니다. BioStar 2 기록은 다음과 같이 표시됩니다.

- **사용자**와 **대상**은 **이름(id)** 형식(공백 변형 포함)으로 원형 그대로 보존됩니다.
- **변경 필드**는 항상 하이픈(-)로 표시됩니다.
- 제공되는 필터로 BioStar 2 기록도 동일하게 검색할 수 있으며, **사용자**와 **대상**은 이름과 아이디 양쪽으로 매칭됩니다.

> **알아두기**
> 레거시 기록에는 지원하지 않는 검색 조건이 포함될 수 있습니다. 저장된 필터를 불러올 때 일부 조건이 제외되면 안내 메시지가 표시됩니다.

감사 설정 관리하기

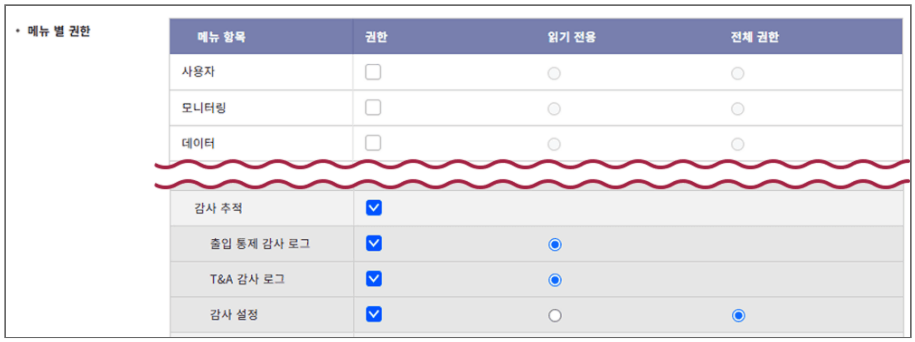
감사 로그는 시간이 지날수록 계속 쌓이므로 저장 공간과 개인정보 보호 관점에서 보관 기간을 관리해야 합니다. **감사 설정**에서 **출입 통제 감사 로그** 기록의 보관 기간과 조회 기록 여부를 설정하세요.

> **알아두기**
> 근태 관리(T&A) 감사 로그의 보관 정책은 별도 문서에서 다룹니다.

권한 안내

전체 관리자는 **감사 설정** 메뉴에서 항상 조회하고 변경할 수 있습니다. 커스텀 권한 관리자는 **메뉴 별 권한**에서 **감사 설정** 메뉴 항목을 **읽기 전용**으로 적용하면 조회만, **전체 권한**으로 적용하면 조회와 변경 모두 할 수 있습니다.

설정 → 계정 → 계정 → 커스텀 권한 추가



감사 설정 열기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **감사 추적** → **감사 설정**을 클릭하세요.



보관 정책 설정

출입 통제 섹션은 다음 두 그룹으로 구성됩니다.

- **변경(생성, 수정, 삭제)**: 생성, 수정, 삭제 기록입니다. 항상 기록되며 끄거나 켤 수 없습니다.
- **조회**: 조회 기록입니다. 기록 여부를 직접 설정할 수 있습니다.

> **알아두기**
>
> - **보존 기간**은 최소 1일, 최대 2,147,483,647까지 정수로 입력할 수 있습니다.
> - **출입 통제** 섹션의 설정 변경 사항은 **출입 통제 감사 로그**에 감사 기록으로 확인할 수 있습니다.

변경 기록

변경(생성, 수정, 삭제) 그룹은 항상 기록되므로, 원하는 **보존**을 선택하세요.

- **영구**: 자동 삭제 없이 기록을 영구 보관합니다.
- **사용자 정의**: 규정이나 내부 정책에 따라 보관 기간을 제한해야 한다면 이 옵션을 선택하세요. **보존 기간** 입력칸이 활성화되면, 보관 기간을 일 단위로 입력하세요.

조회 기록

조회 그룹에서 조회 기록을 남길지 여부를 직접 정할 수 있습니다.

- **기록**: 조회 기록을 남기려면 **사용**으로 설정하세요. 필요하지 않으면 **사용 안 함** 상태로 설정하세요.
- **보존**: 원하는 보관 방식을 선택하세요.
  - **영구**: 조회 기록을 자동 삭제 없이 영구 보관합니다.
  - **사용자 정의**: **보존 기간** 입력칸이 활성화됩니다. 원하는 보관 기간을 일 단위로 입력하세요.

> **알아두기**
>
> **기록**이 **사용 안 함**으로 설정되어 있다면, 조회 이벤트 자체를 기록하지 않습니다. 이후 **사용**으로 설정해도 이전 기간의 기록은 조회할 수 없습니다.

설정 저장

변경(생성, 수정, 삭제)과 **조회** 설정을 완료했다면, **출입 통제** 섹션 하단의 **적용** 버튼을 클릭하세요. 두 그룹의 설정값을 함께 저장합니다.

자동 삭제 동작 방식

사용자 정의에서 설정한 보관 기간을 초과한 기록은 사용자 조작과 관계없이 서버가 매일 오전 1시에 실행하는 작업에서 자동 삭제합니다. 판정과 삭제는 같은 작업에서 한 번에 일어나며, 이 판정은 하루에 한 번만 이뤄집니다.

> *예를 들어, **조회** 기록을 **사용자 정의** 방식으로 30일 적용했다면, 오전 1시 작업 실행 시점을 기준으로 30일을 초과한 기록이 그 작업에서 바로 삭제됩니다. 보관 기간을 막 넘긴 기록이라도 작업이 하루에 한 번만 실행되므로, 그 시점이 지나야 다음 날 오전 1시 작업에서 삭제됩니다.*

보존을 **영구**로 설정하면 자동 삭제 작업이 동작하지 않아 기록이 영구 보존됩니다.

시스템 설정하기

BioStar X 시스템을 안정적으로 운영하기 위한 설정 방법을 안내합니다. 서버 기본 정보와 HTTPS 인증서를 구성하고, 시스템 백업과 복원으로 데이터를 보호하며, 비밀번호 정책과 암호화로 보안을 강화할 수 있습니다. 이 외에도 일광 절약 시간, 이메일 알림, 언어 및 시간대 같은 기본 환경을 설정할 수 있습니다.

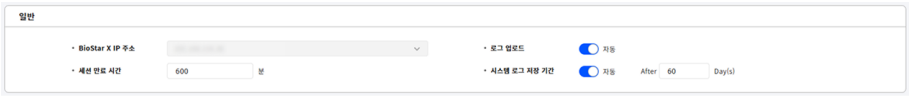
서버 상세 설정하기

BioStar X 서버의 기본 정보, 사용자 및 장치 관리, 서버 매칭, 시스템 로그 단계, 얼굴 이미지 저장에 대한 설정을 변경할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **서버**를 클릭하세요.
3. 각 섹션에서 원하는 항목을 설정하세요.
    - **일반**: IP 주소, 포트 번호, 세션 만료 시간, 이벤트 로그 업로드 방법, 로그 저장 기간을 설정할 수 있습니다.
    - **사용자 및 장치 관리**: 사용자 및 장치 관리 설정을 변경할 수 있습니다.
    - **시스템 로그 단계 설정**: 시스템 로그 단계 설정을 변경할 수 있습니다.
    - **전문가 설정**: 얼굴의 실제 이미지와 템플릿을 모두 저장하도록 하거나 실제 이미지는 저장하지 않고 템플릿만 저장하도록 설정할 수 있습니다.
4. 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

기본 정보 설정

일반 섹션에서는 **BioStar X**의 기본 정보를 확인하거나 설정할 수 있습니다.

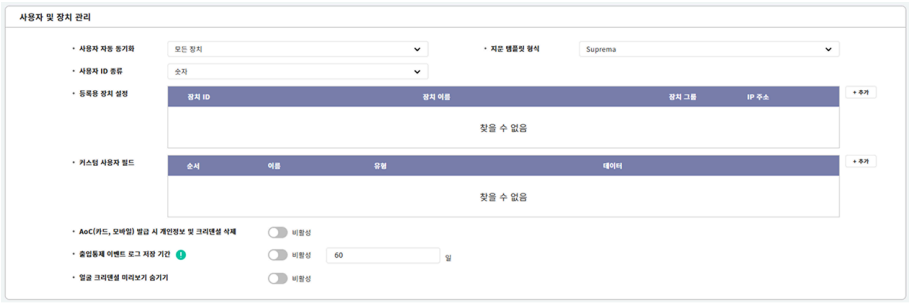


- **BioStar X IP 주소**: 서버 IP 주소를 확인할 수 있습니다.
- **로그 업로드**: 이벤트 로그의 업로드 방법을 선택할 수 있습니다. 서버와 실시간 통신이 어려운 경우 **수동**으로 설정하세요.
- **시스템 로그 저장 기간**: 로그 저장 기간은 1~120까지 설정할 수 있습니다.
- **세션 만료 시간**: 세션 만료 시간을 설정할 수 있습니다. **BioStar X**에 로그인한 뒤 설정한 시간 동안 조작이 없다면 자동으로 로그아웃됩니다.

> **알아두기**
> **로그 업로드** 옵션을 **자동**으로 설정하면 서버와 장치 간에 연결이 끊어지고 다시 연결될 때 장치에 저장된 이벤트 로그가 서버로 자동 업로드됩니다.

사용자 및 장치 관리

사용자 및 장치 관리 섹션에서는 사용자와 장치간 동기화 및 인증 방법을 설정할 수 있습니다.



사용자 자동 동기화

사용자 자동 동기화 옵션에서는 서버와 장치 간에 사용자 정보를 동기화하는 방법을 선택할 수 있습니다. 동기화에는 사용자에게 할당된 출입 등급 및 출입 그룹도 포함되므로, **BioStar X** 서버에서 출입 등급이나 출입 그룹을 변경하면 해당 변경 사항이 관련 장치에 자동으로 적용됩니다.

- **모든 장치**: 사용자 정보가 서버와 장치 간에 자동으로 동기화됩니다.
- **모든 장치(장치 사용자 변경 포함)**: 서버의 사용자 정보가 서버에 등록된 모든 장치와 동기화됩니다. 단, 장치에서 수정한 사용자 정보는 서버에 동기화되지 않으며 장치에서 추가한 사용자 정보만 서버에 동기화됩니다.
- **특정 장치(해당하는 출입 그룹에 속한 장치만 동기화)**: 변경 사항이 있는 출입 그룹에 속한 장치만 서버와 자동 동기화됩니다.

> **알아두기**
>
> - **특정 장치(해당하는 출입 그룹에 속한 장치만 동기화)** 옵션을 선택하면 장치에 저장된 사용자 중 출입 그룹에 속하지 않은 사용자는 서버에서 관리할 수 없습니다. 이 옵션을 사용하려면 **설정** → **장치** → **장치** 메뉴에서 각 장치를 선택하고 **데이터 삭제 후 장치 동기화**를 클릭해 동기화를 진행하세요. **데이터 삭제 후 장치 동기화** 기능에 대한 자세한 내용은 장치 관리 기능 사용하기를 참고하세요.
> - **특정 장치(해당하는 출입 그룹에 속한 장치만 동기화)** 옵션을 선택하더라도 아래와 같이 특수한 목적을 위해 지정된 출입 그룹의 경우 장치의 출입 그룹에 상관없이 동기화됩니다.
>   - 장치 및 엘리베이터에 설정된 이중 인증 출입 그룹
>   - 안티패스백 설정의 항시 통과 그룹
>   - 스케줄 잠금 설정의 항시 통과 그룹
>   - 스케줄 개방 설정의 개방 인증 출입 그룹
>   - 경비 설정의 경비/해제 그룹
> - **특정 장치(해당하는 출입 그룹에 속한 장치만 동기화)** 옵션을 선택하더라도 장치 관리자로 지정된 사용자는 출입 그룹에 상관없이 동기화됩니다.

지문 템플릿 형식

지문 템플릿 형식 옵션에서는 지문 템플릿 형식을 선택할 수 있습니다. 다음 항목에서 선택하세요.

- **SUPREMA**: 슈프라마 지문 템플릿 형식입니다. 슈프라마 장치에서 지문을 등록할 때 사용합니다.
- **ISO**: ISO 국제 지문 템플릿 형식입니다.
- **ANSI378**: 미국 규격 협회(American National Standards Institute, ANSI)에서 정의한 지문 템플릿 형식입니다.

> **알아두기**
>
> 장치에 사용자 지문 템플릿이 남아 있다면 다른 형식으로 변경할 수 없습니다.

사용자 ID 종류

사용자 ID 종류 옵션에서는 사용자 아이디 종류를 **숫자** 또는 **영숫자**로 선택할 수 있습니다. **BioStar X** 서버에 등록된 장치 목록을 확인하고 호환되는 설정값을 선택하세요.

▼ 사용자 ID 종류를 변경할 수 있는 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.0.0 이상
- XPass 2 펌웨어 1.0.0 이상
- FaceLite 펌웨어 1.0.0 이상
- BioLite N2 펌웨어 1.0.0 이상
- XPass D2 펌웨어 1.0.0 이상
- BioEntry R2 펌웨어 1.0.0 이상
- BioEntry P2 펌웨어 1.0.0 이상
- FaceStation 2 펌웨어 1.0.0 이상
- BioEntry W2 펌웨어 1.1.0 이상
- BioStation L2 펌웨어 1.2.0 이상
- BioStation A2 펌웨어 1.3.0 이상
- BioStation 2 펌웨어 1.4.0 이상
- CoreStation 펌웨어 1.0.0 이상

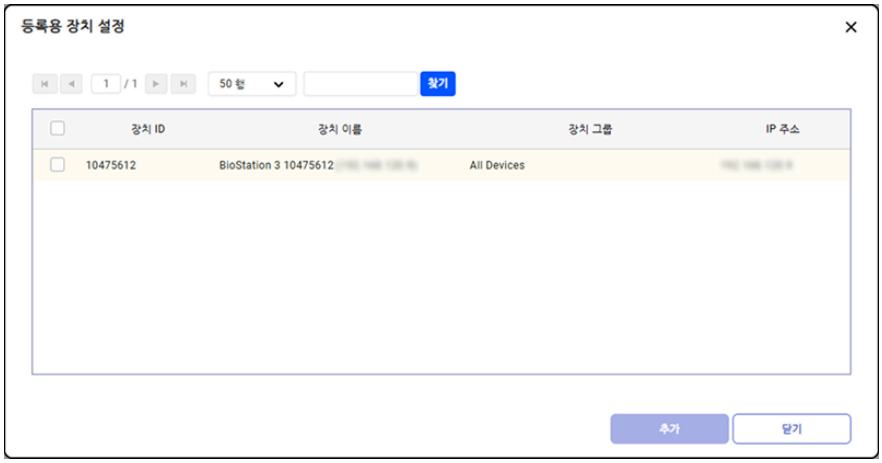
알아두기

영숫자에서 **숫자**로 변경하면 **BioStar X**에 등록한 모든 사용자 정보를 삭제해야 합니다.

등록용 장치 설정

지문이나 얼굴, 카드를 등록할 때 자주 사용하는 장치를 **등록용 장치 설정** 옵션에 추가해 편리하게 사용할 수 있습니다.

1. 장치를 추가하려면 **+ 추가** 버튼을 클릭하세요.
2. **등록용 장치 설정** 창이 나타나면 목록에서 원하는 장치의 체크박스를 클릭하세요.



3. 선택한 장치를 추가하려면 **추가** 버튼을 클릭하세요.
4. 추가한 장치 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 등록한 장치가 너무 많아 목록에서 찾기 어렵다면 검색 입력 필드에 키워드를 입력해 장치를 검색하세요. 장치 아이디, 장치 이름, 장치 그룹, IP 주소를 입력할 수 있습니다.
> - 사용자 정보를 등록할 때 지문 또는 얼굴, 카드 크리덴셜 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
>   - 지문 등록하기
>   - 얼굴 등록하기
>   - 출입 카드 등록하기
>   - 모바일 출입 카드 등록하기

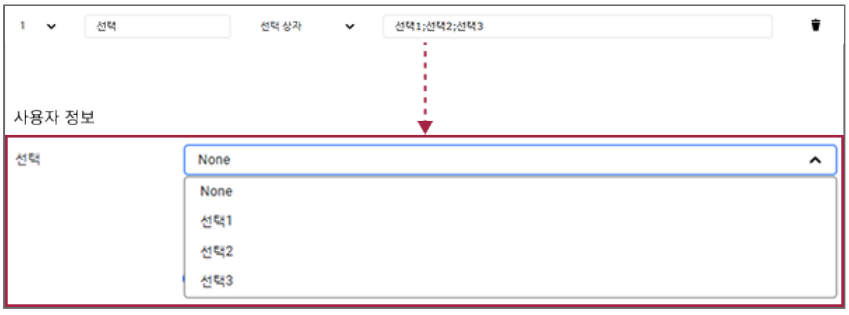
커스텀 사용자 필드

커스텀 사용자 필드 옵션에서는 사용자의 부가 정보를 입력할 필드를 추가할 수 있습니다. 추가된 필드는 사용자 정보 화면에 표시됩니다.

1. 커스텀 사용자 필드를 추가하려면 **+ 추가** 버튼을 클릭하세요.
2. 커스텀 사용자 필드의 이름을 입력하고 유형에서 원하는 항목을 선택하세요.



- **숫자 입력 상자**: 0부터 4294962795까지 입력할 수 있으며, 문자를 입력할 수 없습니다.
- **문자 입력 상자**: 최대 32자의 숫자 및 문자를 입력할 수 있습니다.
- **선택 상자**: 최대 20개 세부 항목을 32자로 추가할 수 있으며, 각 항목은 세미 콜론(;) 기호로 구분합니다. (예, 선택1;선택2;선택3)



- **파일 업로드**: 파일 업로드를 위한 필드를 추가할 수 있습니다.

  - 최대 파일 크기는 1MB입니다.
  - 파일명은 최소 1자에서 최대 120자까지 가능합니다.
  - 파일명 제약사항: 파일명은 영숫자, 밑줄(`_`), 하이픈(`-`)을 사용하고, 확장자를 구분할 때는 점(`.`)을 사용합니다.
  - 허용되는 파일 확장자는 제약이 없으며, 업로드된 파일은 암호화되어 데이터베이스에 저장됩니다.

3. 추가한 커스텀 사용자 필드를 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

알아두기

- 커스텀 사용자 필드의 순서를 변경하려면 **순서** 열의 숫자를 변경하세요. 해당 필드의 위치가 변경됩니다.
- 커스텀 사용자 필드를 수정한 후에는 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.
- 커스텀 사용자 필드를 삭제하려면 버튼을 클릭하세요. 삭제된 필드는 복구할 수 없습니다.
- 사용자 정보 등록 및 수정에 대한 자세한 내용은 사용자를 참고하세요.
- 커스텀 사용자 필드를 추가한 사용자 정보를 카드로 인쇄할 수 있습니다. 자세한 내용은 카드 인쇄하기를 참고하세요.

AoC 카드 설정

사용자의 크리덴셜을 카드에 저장하는 AoC(Access on Card)를 발급할 때 **BioStar X** 서버에서 개인 정보와 크리덴셜 정보를 삭제하려면 **AoC(카드, 모바일) 발급 시 개인정보 및 크리덴셜 삭제** 옵션을 활성화하세요.

알아두기

▼ **NFC 모바일 카드를 지원하는 장치 보기**

- 모바일 장치 OS: 안드로이드 7.0 이상
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite
- BioLite N2
- XPass D2
- BioEntry R2
- BioEntry P2
- FaceStation 2
- BioEntry W2
- BioStation L2: BSL2-OM
- BioStation A2: BSA2-OMPW, BSA2-OIPW
- BioStation 2: BS2-OMPW, BS2-OIPW

▼ **BLE 모바일 카드를 지원하는 장치 보기**

- 모바일 장치 OS: 안드로이드 7.0 이상 / iOS 13.0 이상
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite: FL-DB
- BioLite N2
- XPass D2
- FaceStation 2: FS2-AWB

- **모바일 카드**와 **모바일 출입 카드**는 동시에 사용할 수 없습니다.

기타

- **출입통제 이벤트 로그 저장 기간**: 출입통제 이벤트 로그를 저장할 기간을 설정하세요.

알아두기

출입통제 이벤트 로그 저장 기간 설정은 서버 로그에만 적용됩니다. 장치 이벤트 로그에는 해당 설정이 적용되지 않습니다. 장치 이벤트 로그를 삭제해야 한다면, **설정** → **장치** → **장치** 메뉴에서 장치 이벤트 로그를 개별적으로 삭제하세요.

- **얼굴 크리덴셜 미리보기 숨기기**: 사용자의 개인 정보 보호를 위해 얼굴 크리덴셜을 등록할 때 미리 보기 이미지를 숨길 수 있습니다. 이 옵션을 활성화하면 사용자의 얼굴 크리덴셜을 등록할 때 미리 보기 화면이 제공되지 않습니다.

서버 매칭 설정하기

서버 매칭 섹션에서는 사용자 정보를 장치에서 인증하지 않고 **BioStar X**에서 인증할 수 있는 서버 매칭 기능을 설정할 수 있습니다.



- **서버 매칭 사용**: 서버 매칭 사용 여부를 설정할 수 있습니다.
- **최대 동시 서버 매칭 수**: 한 번에 매칭할 수 있는 최대 서버 매칭 수를 설정할 수 있습니다.

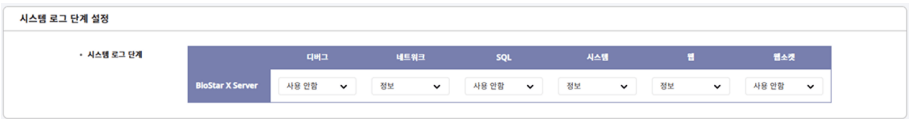
> 이 옵션은 **BioStar X**를 설치한 서버 PC의 CPU 성능에 따라 달라질 수 있습니다.

- **지문**
  - **Fast 모드**: 지문 매칭 속도를 조절할 수 있습니다.
  - **보안 레벨**: 지문에 대한 서버 매칭 보안 레벨을 설정할 수 있습니다. 보안 등급이 높을 수록 본인 거부율(FRR)이 증가합니다.
- **IR 페이스**
  - **보안 레벨**: IR 페이스에 대한 서버 매칭 보안 레벨을 설정할 수 있습니다. 보안 등급이 높을 수록 본인 거부율(FRR)이 증가합니다.

> **알아두기**
> **서버 매칭** 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

시스템 로그 단계 설정

시스템 로그 단계 설정 섹션에서는 데이터베이스에 저장되는 시스템 로그의 레벨을 설정할 수 있습니다.



시스템 로그는 미리 지정된 카테고리에 따라 관리하며 로그의 레벨은 **추적**, **디버그**, **정보**, **경고**, **에러**로 구분합니다. 상위 레벨은 하위 레벨의 로그를 모두 포함합니다. 예를 들어, 시스템 로그 단계를 **추적**으로 선택하면, 하위 레벨인 **디버그**, **정보**, **경고**, **에러** 로그를 모두 포함하여 저장합니다.

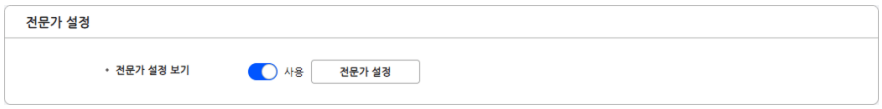
얼굴 이미지 저장하기

얼굴을 크리덴셜로 등록할 때 실제 이미지와 템플릿을 모두 저장하도록 하거나, 실제 이미지는 저장하지 않고 템플릿만 저장하도록 설정할 수 있습니다.

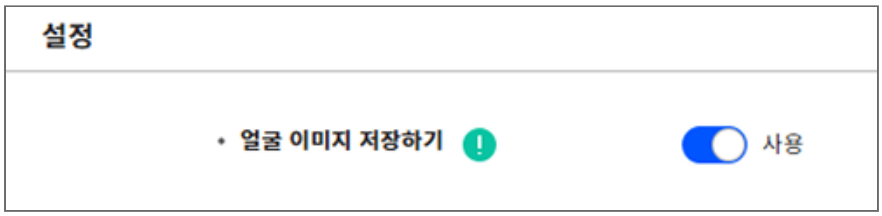
사용하기 전에

전문가 설정 보기 옵션을 활성화하기 전에 **서버** 메뉴 내에서 변경한 사항이 있다면 먼저 변경 내용을 저장해야 합니다. 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

1. **전문가 설정** 섹션에서 **전문가 설정 보기** 옵션을 **사용**으로 설정하세요.



2. **전문가 설정** 버튼을 클릭하세요.
3. **전문가 설정** 화면으로 진입하면 **얼굴 이미지 저장하기** 옵션을 설정하세요.



- **사용**: 기본값입니다. 얼굴 크리덴셜의 실제 이미지와 템플릿을 모두 저장합니다.
- **사용 안 함**: 얼굴 크리덴셜의 실제 이미지는 저장하지 않고 템플릿만 저장합니다. 이 옵션을 선택하면 나타나는 경고 팝업을 주의 깊게 읽어본 다음 설정하세요.

4. 설정을 저장하려면 **확인**을 클릭하세요.

주의

얼굴 이미지 저장하기 옵션 비활성화 시 주의 사항

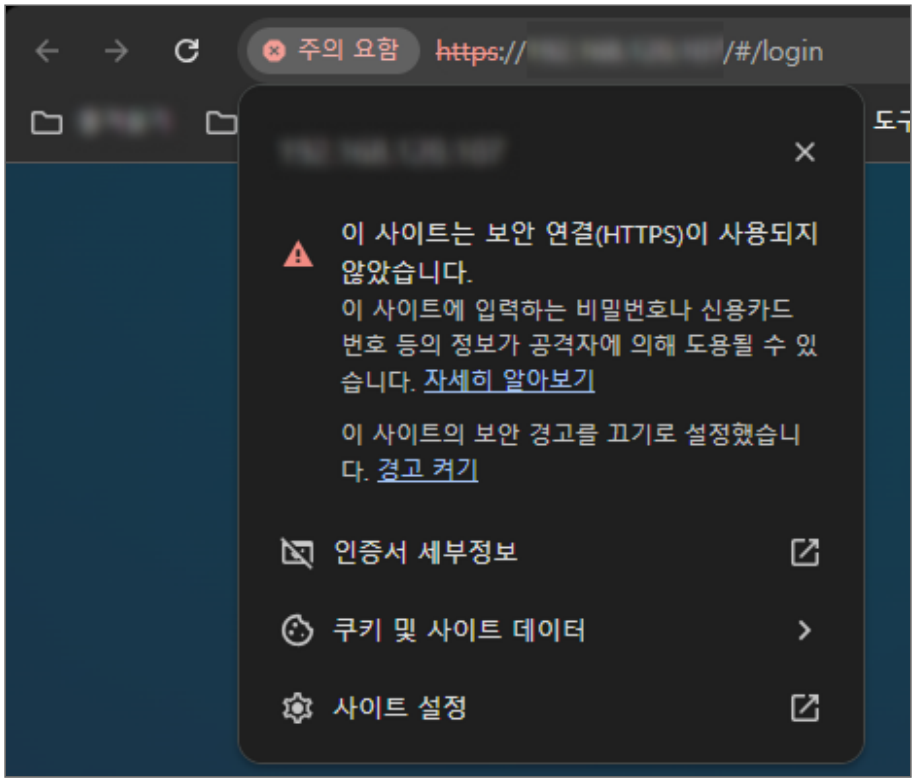
- 이 기능을 비활성화할 경우 저장된 얼굴 이미지가 모두 삭제되며, 앞으로 등록되는 얼굴 이미지도 이미지를 제외한 템플릿만을 저장합니다.
- 등록된 얼굴 이미지가 두 가지 타입의 템플릿을 가지고 있지 않은 경우 이 기능을 비활성화할 수 없습니다. **얼굴 마이그레이션** 기능에 대한 자세한 내용은 얼굴 마이그레이션을 참고하세요.
- 이 기능을 비활성화한 후 **데이터 파일 가져오기** 시 유효하지 않은 얼굴 이미지 템플릿이 포함되어 있는 경우 데이터 파일을 가져올 수 없습니다. 문제를 해결하려면 이 기능을 일시적으로 활성화한 후 데이터 파일을 가져오세요.

HTTPS 인증서 설치하기

BioStar X를 HTTPS로 연결하려면 **BioStar X**를 설치한 서버의 IP 주소를 등록하여 인증서를 설치해야 합니다.

인증서 설치가 필요한 경우

HTTPS 인증서가 설치되지 않은 상태에서 **BioStar X**에 접속하면 웹 브라우저에서 다음과 같은 보안 경고가 표시됩니다.

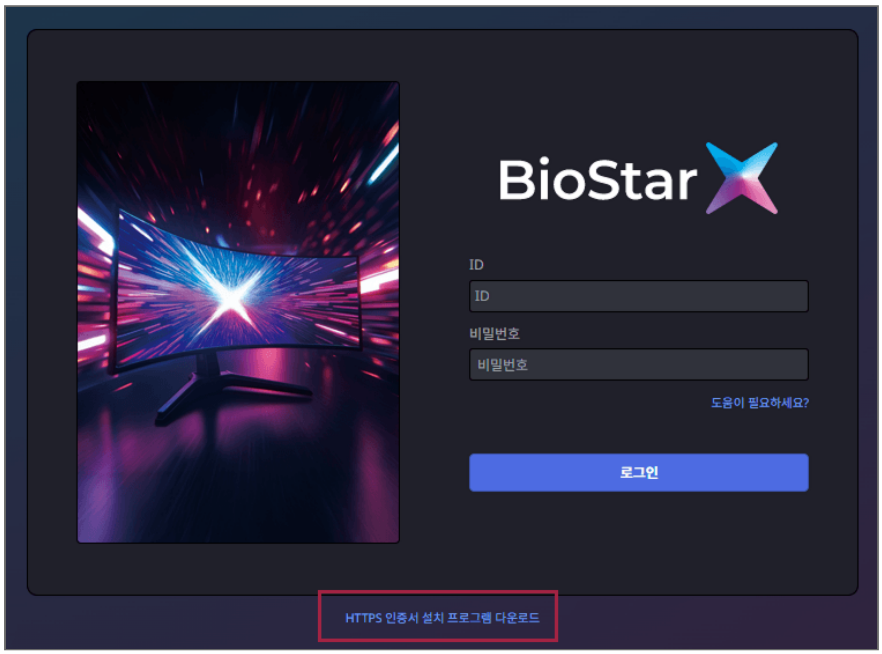


이러한 경고는 브라우저가 서버의 신원을 확인할 수 없기 때문에 나타납니다. 인증서를 설치하면 브라우저가 **BioStar X** 서버를 신뢰하게 되어 보안 경고 없이 안전한 HTTPS 연결을 사용할 수 있습니다.

인증서 설치

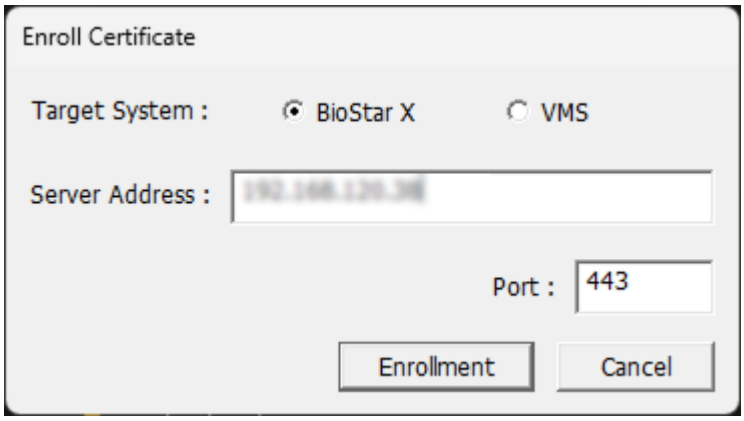
올바른 네트워크 연결을 위해 **BioStar X**를 사용하기 전에 인증서를 설치하세요.

1. **BioStar X** 로그인 페이지로 접속하세요.
2. 화면 하단의 **HTTPS 인증서 설치 프로그램 다운로드** 링크를 클릭하세요.



3. *cert-register.zip* 파일을 로컬에 저장하세요.
4. 다운로드한 파일의 압축을 해제하고, *cert-register.exe* 파일을 실행하세요. **Enroll Certificate** 프로그램이 실행됩니다.

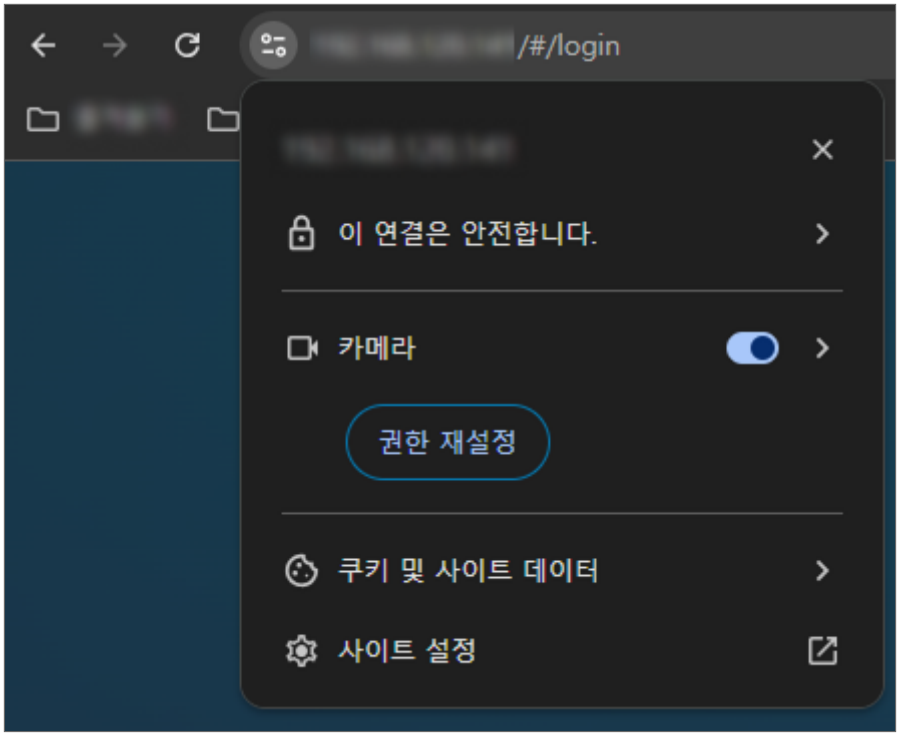
5. **Target System**을 **BioStar X**로 선택하고, **BioStar X**가 설치된 PC의 IP 주소를 **Server Address**에 입력한 뒤 **Enrollment** 버튼을 클릭하세요.



> **BioStar X**의 기본 포트 번호는 443입니다. 포트 번호를 변경했다면 **Port**에 변경한 포트 번호를 입력하세요.

6. 보안 경고 메시지를 확인한 뒤 **예**를 클릭하세요.

웹 브라우저를 다시 시작한 뒤 등록한 IP 주소를 입력해 **BioStar X** 페이지로 이동하세요. 주소 표시줄 왼쪽의 아이콘을 클릭했을 때 **이 연결은 안전합니다** 메시지가 표시됩니다.

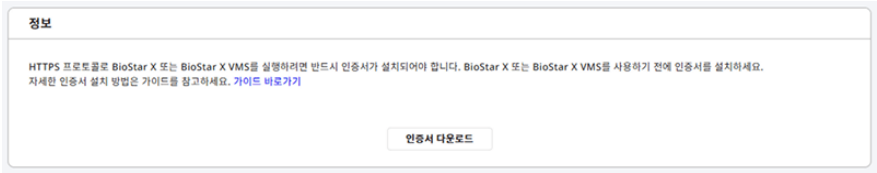


> **알아두기**
> **Enroll Certificate**에서 입력하는 IP 주소는 **BioStar X**에 설정된 IP 주소와 동일해야 합니다. **설정** → **시스템** → **서버** 메뉴 경로의 **BioStar X IP 주소** 항목에서 확인할 수 있습니다.

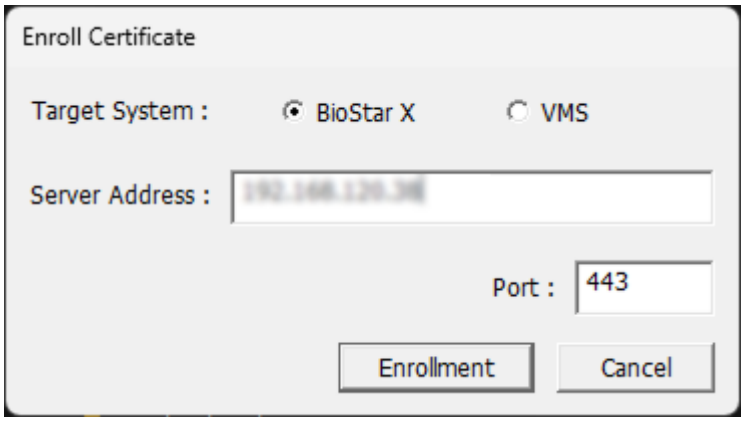
서버 설정에서 인증서 설치

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **시스템** → **HTTPS**를 클릭하세요.
3. **인증서 다운로드**를 클릭하세요.



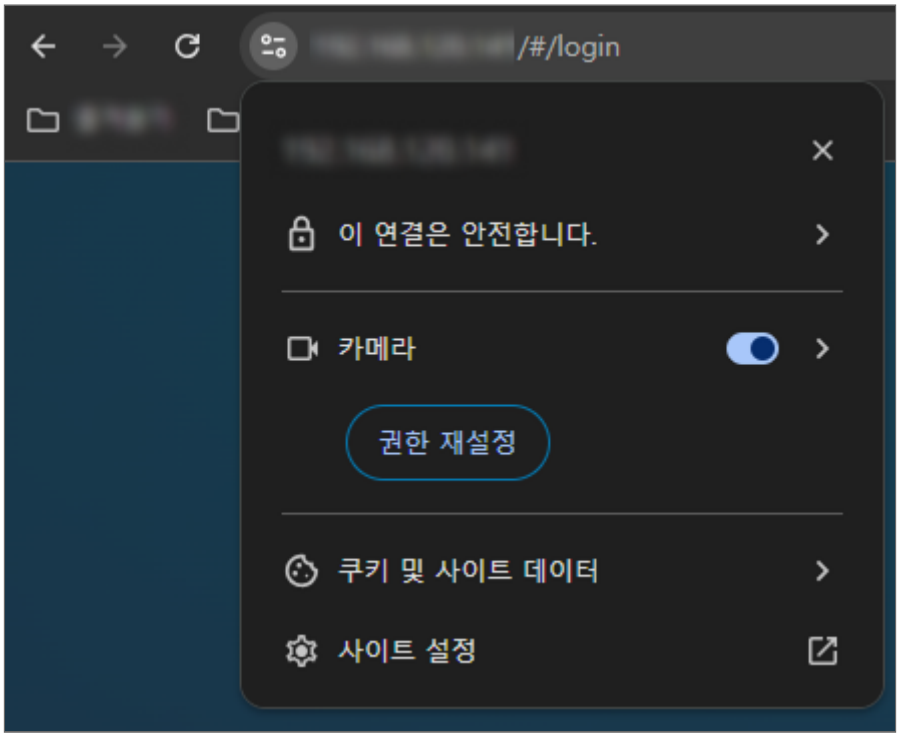
4. *cert-register.zip* 파일을 로컬에 저장하세요.
5. 다운로드한 파일의 압축을 해제한 뒤 **cert-register.exe** 파일을 실행하세요. **Enroll Certificate** 프로그램이 실행됩니다.
6. **Target System**을 **BioStar X**로 선택하고, **BioStar X**가 설치된 PC의 IP 주소를 **Server Address**에 입력한 뒤 **Enrollment** 버튼을 클릭하세요.



> **BioStar X**의 기본 포트 번호는 443입니다. 포트 번호를 변경했다면 **Port**에 변경한 포트 번호를 입력하세요.

7. 보안 경고 메시지를 확인한 뒤 **예**를 클릭하세요.

웹 브라우저를 다시 시작한 뒤 등록한 IP 주소를 입력해 **BioStar X** 페이지로 이동하세요. 주소 표시줄 왼쪽의 아이콘을 클릭했을 때 **이 연결은 안전합니다** 메시지가 표시됩니다.



VMS 서버의 인증서 설치

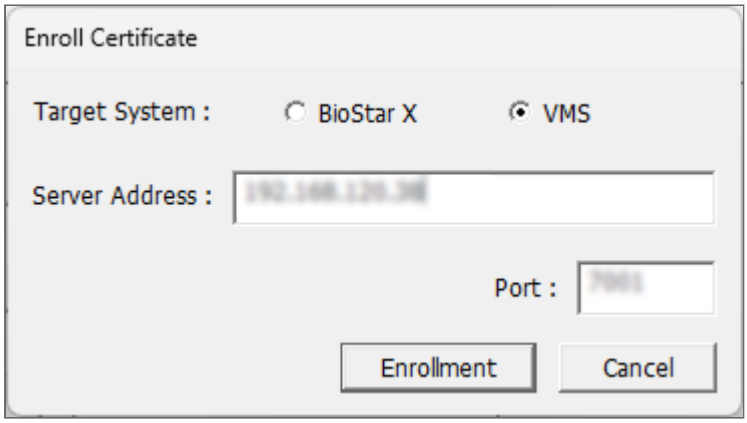
아래와 같은 상황이 발생한다면 VMS 서버에 설치된 인증서를 클라이언트 PC에 설치해 문제를 해결할 수 있습니다.

- **Video Management System**(VMS)을 브라우저를 통해서 접속했을 때 '안전하지 않음' 경고가 표시될 때
- **모니터링** 페이지에서 실시간 영상은 재생되나 녹화 영상이 재생되지 않을 때
- VMS 서버와 **BioStar X**를 같은 서버에 설치할 때

> **알아두기**
>
> - VMS 서버에 인증서를 설치하는 방법은 VMS 연동하기를 참고하세요.
> - VMS 서버와 연동하는 기능은 기능 추가 옵션을 별도로 구매해야 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

클라이언트 PC에서 인증서 설치

1. **BioStar X**를 설치한 클라이언트 PC에서 로그인 화면 또는 **설정** → **시스템** → **HTTPS**에서 HTTPS 인증서 설치 프로그램(*cert-register.zip*)을 다운로드하세요.
2. 다운로드한 파일의 압축을 해제한 뒤 **cert-register.exe** 파일을 실행하세요. **Enroll Certificate** 프로그램이 실행됩니다.
3. **Target System**을 **VMS**로 선택하고 다음 정보를 입력하세요.



- **Server Address**: VMS 서버의 IP 주소
- **Port**: VMS 서버의 포트 번호

4. **Enrollment** 버튼을 클릭하세요.
5. 보안 경고 메시지를 확인한 뒤 **예**를 클릭하세요.

웹 브라우저를 다시 시작한 뒤 **모니터링** 페이지에서 VMS 서버의 녹화 영상이 정상 재생되는지 확인하세요.

시스템 백업하기

BioStar X의 데이터베이스, 각종 설정, 키 등 주요 정보를 백업할 수 있습니다. 백업 파일에는 암호화 키(enc key), 이미지 로그 경로 등 사용자가 설정한 값도 포함됩니다. **시스템 백업** 기능을 사용하면 서버의 데이터 손실을 방지하거나 새로운 PC로 이전할 때 사용하세요.

지원하는 백업 방식은 아래와 같습니다.

- **수동 백업**: 사용자가 수동으로 백업 파일을 생성합니다.
- **자동 백업**: 시스템에서 정해진 주기마다 백업 파일을 자동 생성합니다.

> **알아두기**
>
> - 이전 PC에서 백업한 **BioStar X** 백업 파일로 새 PC에서 **BioStar X** 복원을 진행하면 라이선스를 재발급 받아야 합니다.
> - SQL Server 데이터베이스와 **BioStar X**가 서로 다른 서버에 설치되어 있다면 **BioStar X** 시스템 백업 및 복원을 사용할 수 없습니다.
> - 시스템 복원에 대한 자세한 내용은 시스템 복원하기를 참고하세요.

수동 백업

사용자가 직접 백업 파일을 생성할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **시스템 백업**을 클릭하세요.
3. **일반** 섹션에서 백업 파일을 저장할 경로와 최대 백업 파일 수를 설정하세요.



- **백업 파일 저장 경로**: 백업 파일을 저장할 경로를 입력하세요. 저장 경로는 이미 생성되어 있는 디렉토리 경로를 입력하세요.
- **최대 백업파일 수**: 최대 백업 파일 수를 설정하세요.

4. 백업 파일을 생성하려면 **백업하기** 버튼을 클릭하세요.
5. 경고 메시지가 나타나면 내용을 확인하고 **계속** 버튼을 클릭하세요.

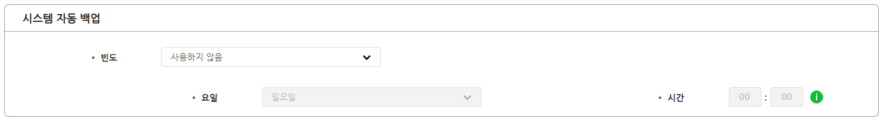
백업 파일은 **백업 파일 저장 경로** 옵션에 지정된 경로에 *zip* 파일 형식으로 저장됩니다. 파일 이름은 `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip` 형식으로 생성됩니다. 여기서 `YYYYMMDD`는 백업 날짜, `HHMMSS`는 백업 시간입니다.

> **알아두기**
>
> - 최대 백업 수를 초과할 경우 가장 오래된 백업 파일부터 자동으로 삭제됩니다.
> - **최대 백업파일 수**는 1 ~ 100 사이의 숫자만 입력할 수 있습니다.

자동 백업 설정

자동 백업을 설정하면 시스템에서 정해진 주기마다 백업 파일을 생성합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **시스템 백업**을 클릭하세요.
3. **시스템 자동 백업** 섹션에서 **빈도** 옵션을 선택하세요.



- **일간**: 매일 자동으로 백업합니다. **시간** 옵션에서 백업 시간을 설정하세요.
- **주간**: 매주 자동으로 백업합니다. **요일** 옵션에서 자동으로 백업할 요일을 설정하고, **시간** 옵션에서 백업 시간을 설정하세요.
- **월간**: 매월 자동으로 백업합니다. **날짜** 옵션에서 자동으로 백업할 날짜를 설정하고, **시간** 옵션에서 백업 시간을 설정하세요.

4. 설정을 저장하려면 **확인**을 클릭하세요.

자동 백업 설정 후 정해진 주기마다 백업이 진행됩니다. 자동 백업 실행 중 실패가 발생하면 이벤트 로그 및 감사 추적에 실패 이력이 기록되며, 실패 원인에 대한 상세 정보는 로그 파일에서 확인할 수 있습니다.

백업 파일은 **일반** 섹션의 **백업 파일 저장 경로** 옵션에 지정된 경로에 *zip* 파일 형식으로 저장됩니다. 파일 이름은 `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip` 형식으로 생성됩니다. 여기서 `YYYYMMDD`는 백업 날짜, `HHMMSS`는 백업 시간입니다.

알아두기

- 자동 백업 빈도를 **월간**으로 선택하고, 날짜를 29, 30, 31일로 설정하면 해당 날짜가 없는 달에는 자동 백업을 실행하지 않습니다.
- 시간은 **기본 설정**에서 설정한 표준 시간대를 기준으로 합니다. 표준 시간대 설정에 대한 자세한 내용은 기본 설정 구성하기를 참고하세요.

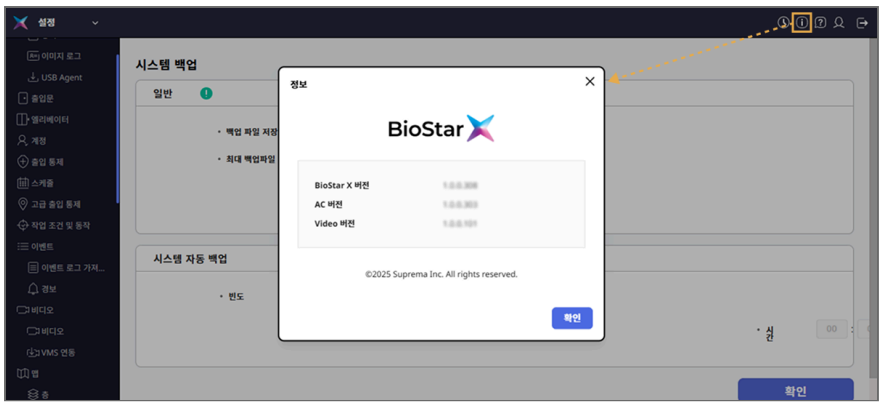
시스템 복원하기

BioStar X에서 문제가 발생했거나 이전 상태로 되돌려야 할 때 시스템 백업 파일을 사용하여 복원할 수 있습니다. 복원 기능을 사용하면 데이터베이스, 각종 설정, 라이선스 정보 등을 백업 시점의 상태로 복원할 수 있습니다.

시작하기 전에

시스템 복원을 시작하기 전에 다음 사항을 확인하세요.

- 백업 시점의 **BioStar X** 버전과 현재 버전이 다를 경우 복원을 진행할 수 없습니다. **BioStar X**의 버전을 확인하려면 화면 오른쪽 최상단의 ⓘ 버튼을 클릭하세요.



- 백업 시점의 **BioStar X** 버전을 확인하려면 백업 파일의 압축을 해제하고, *sysbackup.conf* 파일의 `biostarVersion` 값을 확인하세요.
- SQL Server 데이터베이스와 **BioStar X**가 서로 다른 서버에 설치되어 있다면 **BioStar X** 시스템 백업 및 복원을 사용할 수 없습니다.
- 복원 대상 서버의 IP 주소가 백업 서버와 다른 경우:
  - **BioStar X v1.0.2 이상**: 복원 시 복원 대상의 IP 주소를 감지하고, 기존 인증서 대신 새로운 IP 주소 기반으로 인증서를 자동으로 재발급합니다. 인증서 재발급 후 인증서를 사용하는 관련 서비스들이 자동으로 재연결되므로 별도 작업이 필요하지 않습니다.
  - **BioStar X v1.0.1 이하**: 복원을 실패할 수 있습니다. 복원을 진행하기 전에 서버 IP 주소를 확인하세요.
- 암호화 키와 이미지 로그 경로가 변경되었어도 복원 시에는 복원 대상 **BioStar X**의 현재 설정 경로를 따릅니다. 별도의 경로 설정을 지정하지 않았다면 복원 대상 **BioStar X**의 기본 경로를 사용합니다.
- 복원 수행 시 현재 시점의 데이터는 자동으로 백업되므로, 복원이 실패하더라도 복원 수행 이전 시점의 상태로 복원될 수 있습니다.

알아두기

시스템 백업 생성에 대한 자세한 내용은 시스템 백업하기를 참고하세요.

시스템 복원

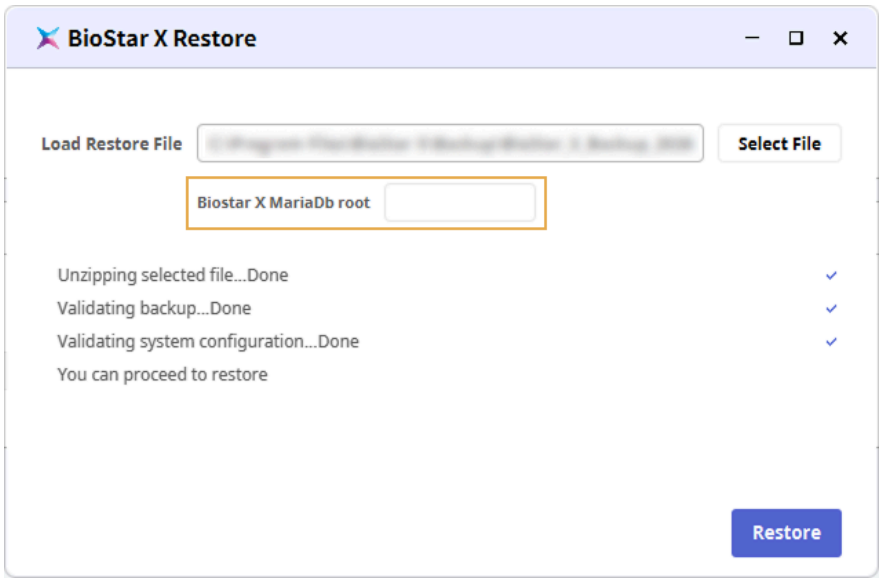
1. Windows에서 시작 → **BioStar X** → **BioStar X Restore**를 실행하세요.

   > *프로그램 경로: C:\Program Files\BioStar X\biostar-restore.exe*

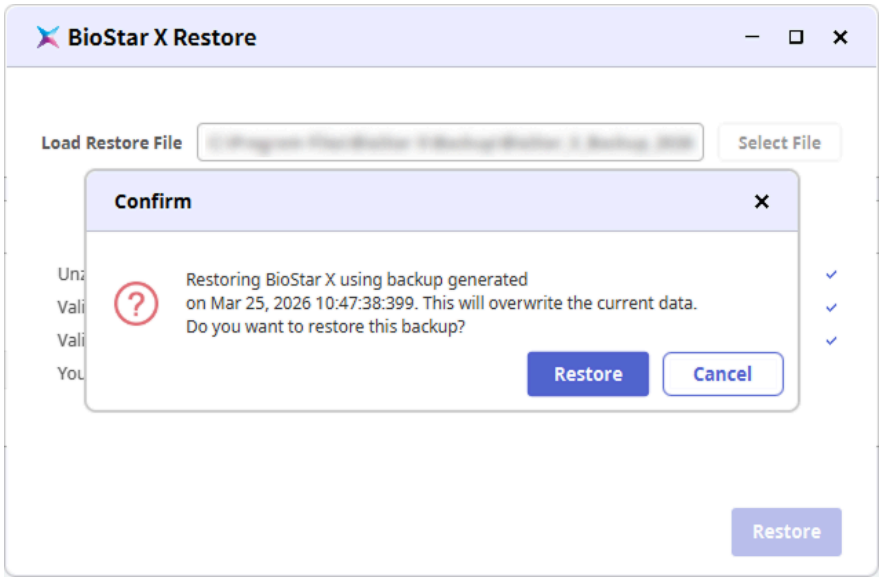
2. **Select File** 버튼을 클릭하고 복원할 백업 파일을 선택하세요.



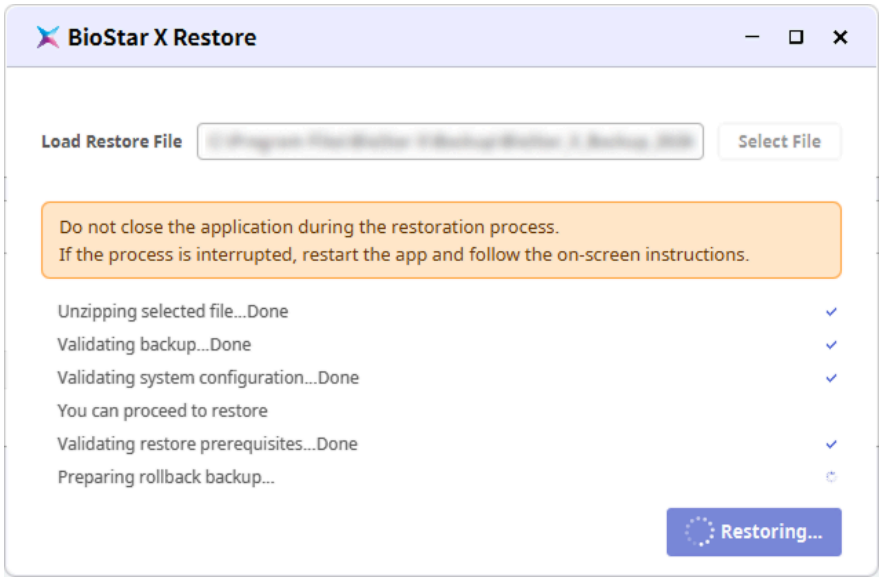
3. 복원을 시작하려면 **Restore** 버튼을 클릭하세요.
4. 백업 파일에 대한 유효성 검증을 진행합니다.
5. **You can proceed to restore** 메시지가 나타나면 데이터베이스 암호를 입력하고 **Restore** 버튼을 클릭하세요.



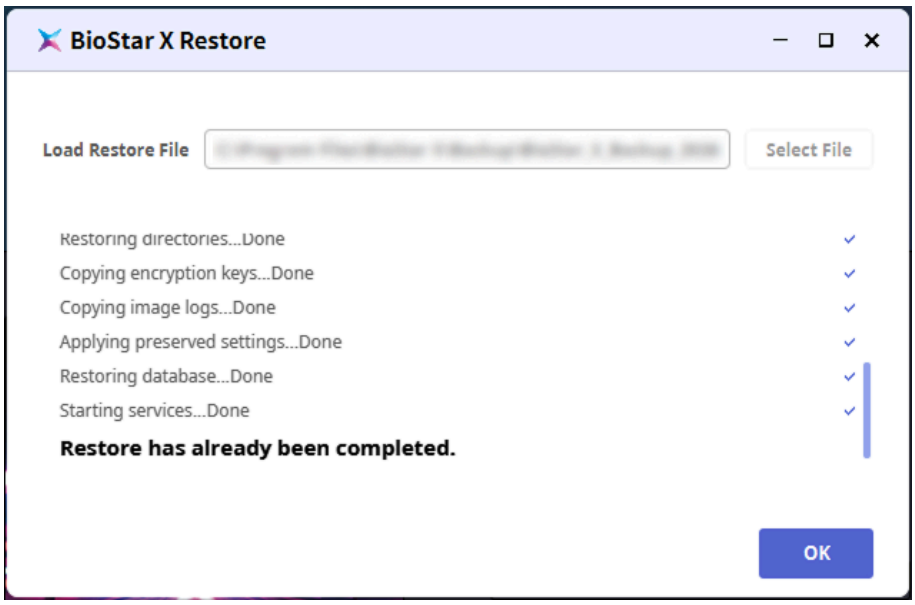
6. 확인 메시지를 확인하고 복원을 계속 진행하려면 **Restore** 버튼을 클릭하세요.



7. 복원 진행 상황을 확인할 수 있는 메시지가 나타납니다. 복원 작업이 완료될 때까지 기다리세요.



Restore has already been completed 메시지가 나타나면 복원이 완료된 상태입니다. **BioStar X**에 접속해 복원된 데이터를 확인하세요.



알아두기

- 복원 과정에서 PC가 비정상 종료되면 **BioStar X Restore**를 다시 실행하여 복원을 재시도하세요.
- 복원 대상 서버의 IP 주소가 백업 서버와 다르고, 멀티 커뮤니케이션 서버가 연결되어 있다면 인증서를 새로 발급해야 합니다. 멀티 커뮤니케이션 서버에서 인증서를 새로 발급하는 방법은 메인 서버의 IP 주소 변경하기를 참고하세요.

시스템 보안 강화하기

조직의 보안 정책에 맞춰 **BioStar X**의 보안 설정을 구성하세요. 비밀번호 정책, 개인정보 암호화, 장치 간 통신 보안, 동시 접속 제어 등을 선택적으로 설정할 수 있습니다.

알아두기

시스템 보안을 강화하기 전에 조직의 보안 정책 및 규정을 확인하세요.

시스템 보안 사용하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **시스템 보안**을 클릭하세요.
3. 보안과 관련한 각 항목을 설정하세요.
   - **로그인 비밀 번호**: 로그인 비밀번호와 관련된 보안 수준을 설정합니다. 자세한 내용은 비밀번호 정책 설정을 참고하세요.
   - **고급 보안 설정**:개인 정보와 장치 간 통신 보안을 강화할 수 있습니다. 자세한 내용은 고급 보안 설정을 참고하세요.
   - **세션 보안**: 세션 보안을 강화할 수 있습니다. 자세한 내용은 동시 접속 제어를 참고하세요.
4. 설정을 저장하려면 화면 오른쪽 하단의 **확인**을 클릭하세요.

알아두기

고급 보안 설정 메뉴는 아이디가 1인 최초 관리자 계정만 사용할 수 있습니다.

비밀번호 정책 설정

로그인 비밀 번호 섹션에서는 로그인 비밀번호와 관련된 보안 수준을 설정합니다. 조직의 보안 요구 사항에 맞춰 비밀번호 정책을 설정하세요.



비밀번호 복잡성 설정

사용자 비밀번호의 복잡성을 설정할 수 있습니다. **비밀번호 레벨** 옵션의 슬라이더를 조정해 보안 수준을 설정하세요.

- **낮음**: 최대 32자까지 입력할 수 있습니다.
- **보통**: 비밀번호를 설정할 때 8~32 영문 문자(대문자 또는 소문자)와 숫자를 조합해야 합니다.

- **강함**: 비밀번호를 설정할 때 10~32 영문 문자(대문자와 소문자, 최소 한 글자 이상의 대문자 포함)와 숫자, 특수 기호를 조합해야 합니다.

비밀번호 변경 주기 설정

비밀번호 사용 기간을 제한하려면 **비밀번호 변경 주기** 옵션에서 토글 버튼을 클릭해 **활성** 상태로 변경하세요. 사용자는 설정한 기간마다 비밀번호를 변경해야 합니다. 비밀번호 변경 주기를 초과하면 로그인 시 비밀번호 변경 요청 메시지가 표시됩니다.

> **알아두기**
> 1일부터 180일까지 설정할 수 있습니다.

로그인 실패 제한 설정

비밀번호 입력 실패 허용 횟수와 로그인 제한 시간을 설정할 수 있습니다. **비밀번호 최대 실패 허용 횟수** 옵션에서 설정한 횟수를 초과하여 비밀번호를 잘못 입력하면 제한 시간 동안 로그인할 수 없습니다.

> **알아두기**
> 이 옵션은 기본적으로 활성화 상태이며, 100회 실패 시 10분간 로그인이 제한됩니다. 필요에 따라 값을 조정하거나 비활성화할 수 있습니다.

비밀번호 변경 횟수 제한 설정

사용자가 하루에 비밀번호를 변경할 수 있는 횟수를 제한하려면 **비밀번호 일일 변경 허용 횟수** 옵션에서 토글 버튼을 클릭해 **활성** 상태로 변경하세요. 사용자는 설정한 횟수만큼 비밀번호를 변경할 수 있습니다.

> **알아두기**
> 최대 10회까지 설정할 수 있습니다.

고급 보안 설정

고급 보안 설정 섹션에서는 개인 정보와 장치 간 통신 보안을 강화할 수 있습니다.



> **알아두기**
> **고급 보안 설정** 섹션은 최초 관리자 계정으로 접속한 경우에만 활성화됩니다.

개인 정보 보호 강화

민감한 개인 정보를 암호화하여 데이터 유출 위험을 최소화하려면 아래 옵션을 설정하세요.

- **개인 정보 DB 암호화**
  - **사용**: 크리덴셜 데이터를 포함한 사용자의 개인 정보를 암호화하여 저장합니다.

  - **사용 안 함**: 사용자의 개인 정보를 암호화하지 않은 상태로 저장합니다. 기존에 암호화된 데이터는 복호화하여 저장하며, 새로운 데이터는 암호화하지 않습니다.

- **개인 정보 DB 암호화 키**: 사용자의 개인 정보를 안전하게 보호하기 위해 데이터베이스에 저장된 정보를 암호화하거나 복호화할 때 사용합니다. **변경** 버튼을 클릭하고 새 암호화 키 값을 설정하세요. 암호화 키를 변경하면 기존에 암호화된 데이터를 재암호화합니다.

알아두기

- 개인 정보 DB 암호화 또는 복호화 기능을 진행하는 동안 서버를 강제로 시작하지 마세요. 로그인 실패, 데이터 손상과 같은 오류가 발생할 수 있습니다. 데이터베이스의 크기 및 서버의 성능에 따라 일정 시간이 소요될 수 있습니다.

  ▼ 개인 정보 암호화 항목 보기

  - 프로필 이미지
  - 사용자 ID
  - 이름
  - 전화번호
  - 사용자 IP
  - 보낸 사람 및 받는 사람의 이메일 정보
  - 로그인 ID
  - 로그인 암호
  - 얼굴 템플릿
  - 지문 템플릿
  - 카드 ID
  - 스마트 카드 레이아웃 키
  - 사용자 및 방문자에 대한 커스텀 정보
  - 이미지 로그 파일

- **개인 정보 DB 암호화 키**는 문자와 숫자, 기호를 사용하여 32자로 입력할 수 있습니다.
- 1.0.3 버전으로 업그레이드한 이후 새로 생성되는 감사 로그는 **개인 정보 DB 암호화** 옵션의 설정과 무관하게 암호화된 상태로 저장됩니다.

장치 간 통신 보안 설정

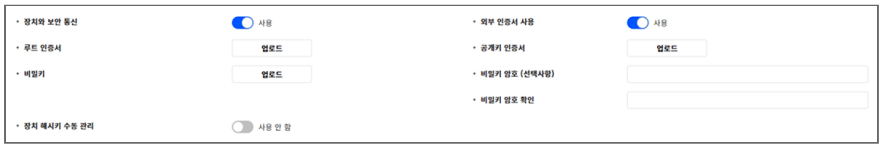
BioStar X 서버와 출입통제 장치 간 통신을 인증서로 보호해 보안을 강화하세요. 신규로 설치한 BioStar X 시스템은 **장치와 보안 통신** 옵션이 기본적으로 **사용** 상태로 제공되며, 별도의 활성화 조작이 필요하지 않습니다. 기존 시스템을 업그레이드하면 이전 설정을 그대로 유지하며, 기존 보안 인증서도 그대로 재사용되어 이미 등록된 장치를 추가 조치 없이 재연결합니다.

- **장치와 보안 통신**: BioStar X 서버와 출입통제 장치 간의 통신을 인증서로 보호합니다. 이 옵션이 **사용** 상태이면 서버가 자동으로 인증서를 생성하여 장치에 전송하고, 이후 모든 통신이 암호화됩니다. 장치는 이 인증서를 이용하여 BioStar X 서버와 데이터를 주고받을 때 보안 채널을 사용합니다.

  외부 인증서를 사용하려면 **외부 인증서 사용** 옵션을 **사용**으로 설정하고 아래 항목을 등록하세요.

  - **루트 인증서**, **공개키 인증서**, **비밀키** 파일을 각각 업로드하세요.
  - 비밀키에 암호가 설정되어 있으면 **비밀키 암호 (선택사항)**와 **비밀키 암호 확인**에 동일한 값을 입력하세요. (선택 사항)

외부 인증서가 아닌, 서버를 제거하면서 백업해 둔 보안 인증서를 그대로 복구하려면 **BioStar X** 설치 경로에 직접 복사해야 합니다. 보안 인증서 백업 및 복구 방법은 BioStar X 서버 제거 및 보안 인증서 복구하기를 참고하세요.



- **장치 해시키 수동 관리**: 장치에 적용하는 해시 키를 사용자가 직접 관리합니다. 이 옵션을 **사용**으로 설정하면 **장치 해시키** 값을 확인하고 변경할 수 있습니다. **변경** 버튼을 클릭하고 새 해시 키 값을 설정하세요.

주의

장치 해시키 수동 관리 옵션을 활성화하기 전에 아래 내용을 반드시 확인하세요.

- 활성화하면 보안을 강화하기 위해 장치에서 템퍼(Tamper) 이벤트가 발생할 때 사용자, 로그, 암호화 키 값이 함께 삭제되도록 설정되므로 주의하세요.
- 전체 관리자 계정을 제외한 사용자에게 로그인 비밀번호 또는 PIN이 설정되어 있으면 해시 키 값을 적용할 수 없습니다. 로그인 비밀번호 또는 PIN을 삭제한 후 다시 시도하세요. 비밀번호와 PIN은 보안 요구 사항을 충족하기 위해 복호화할 수 없는 방식으로 암호화되기 때문입니다.
- 장치 해시 키를 변경하면 장치에 설정된 마스터 관리자 PIN 정보가 삭제됩니다. 크리덴셜 삭제로 인해 장치 관리자 메뉴에 접근하지 못할 수 있으므로 각별히 주의하세요.
- **개인 정보 DB 암호화**와 **장치 해시키 수동 관리**는 동시에 사용할 수 없습니다. 두 옵션 중 하나를 사용 안 함으로 전환한 후 나머지 옵션을 설정하세요.

알아두기

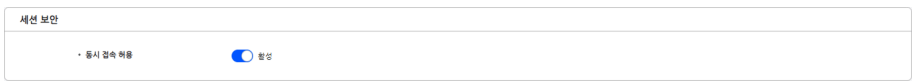
- **BioStar X**는 **장치와 보안 통신** 옵션을 **사용 안 함**으로 변경해도 서버가 생성한 기본 인증서를 삭제하지 않습니다. 옵션을 다시 **사용**으로 변경하면 기존 인증서를 그대로 재사용하며, 인증서가 없는 경우에만 새로 생성합니다. 따라서 **사용** → **사용 안 함** → **사용** 순서로 변경해도 같은 인증서가 유지되어, 이전에 등록된 장치를 추가 조치 없이 다시 연결할 수 있습니다. 단, 외부 인증서를 사용하는 상태에서 **사용 안 함**으로 변경하면 등록했던 외부 인증서(루트 인증서, 공개키 인증서, 비밀키)와 비밀키 암호는 서버에서 삭제됩니다.
- 등록된 모든 장치와 멀티 커뮤니케이션 서버가 서버에 연결된 상태에서만 **장치와 보안 통신** 옵션과 **외부 인증서 사용** 옵션을 변경할 수 있습니다. 연결이 끊긴 장치가 있거나 멀티 커뮤니케이션 서버가 연결되어 있지 않으면 변경이 거부되고 오류 메시지가 표시됩니다. 장치 또는 멀티 커뮤니케이션 서버를 다시 연결한 후 시도하고, 더 이상 사용하지 않는 장치라면 장치 목록에서 삭제한 후 다시 시도하세요.
- 이전에 정상적으로 연결되던 장치가 인증서 불일치로 연결에 실패하면 **BioStar X**는 이를 시스템 로그에 기록합니다. 장치가 갑자기 연결되지 않는다면 시스템 로그에서 원인을 확인한 후, 장치를 공장 초기화하거나 이전에 내보내 둔 인증서 세트를 **외부 인증서 사용** 옵션으로 다시 등록하여 복구하세요. 단, 서버를 제거한 뒤 재설치했다면 BioStar X 서버 제거 및 보안 인증서 복구하기를 참고하세요.
- 서버를 제거할 때 인증서를 백업하는 방법은 BioStar X 서버 제거 및 보안 인증서 복구하기를 참고하세요.

▼ 장치와 보안 통신 기능 지원 장치와 펌웨어 버전 보기

- BioStation 3 Max 펌웨어 1.0.0 이상
- XPass Q2 펌웨어 1.0.0 이상
- BioStation 3 펌웨어 1.0.0 이상
- BioStation 2a 펌웨어 1.0.0 이상
- X-Station 2 펌웨어 1.0.0 이상
- XPass 2 펌웨어 1.0.0 이상
- FaceLite 펌웨어 1.0.0 이상
- BioLite N2 펌웨어 1.0.0 이상
- BioEntry P2 펌웨어 1.1.0 이상
- FaceStation 2 펌웨어 1.1.0 이상
- BioEntry W2 펌웨어 1.2.0 이상
- BioStation L2 펌웨어 1.3.0 이상
- BioStation A2 펌웨어 1.5.0 이상
- BioStation 2 펌웨어 1.6.0 이상
- CoreStation 펌웨어 1.1.0 이상

동시 접속 제어

세션 보안 섹션에서는 보안 강화를 위해 동일 계정의 중복 로그인을 제한할 수 있습니다. **동시 접속 허용** 옵션을 **비활성**으로 설정하세요. 동일한 계정에 대한 동시 접속 시도 시 기존에 접속해 있던 사용자는 로그아웃됩니다.



일광 절약 시간 설정하기

일광 절약 시간(Daylight Saving Time, DST)을 설정하여 현지 법정 시간에 맞춰 시스템 시간을 자동으로 조정할 수 있습니다. 이를 통해

출입 기록의 정확성을 보장하고 다른 시스템과의 시간 동기화 문제를 방지할 수 있습니다.

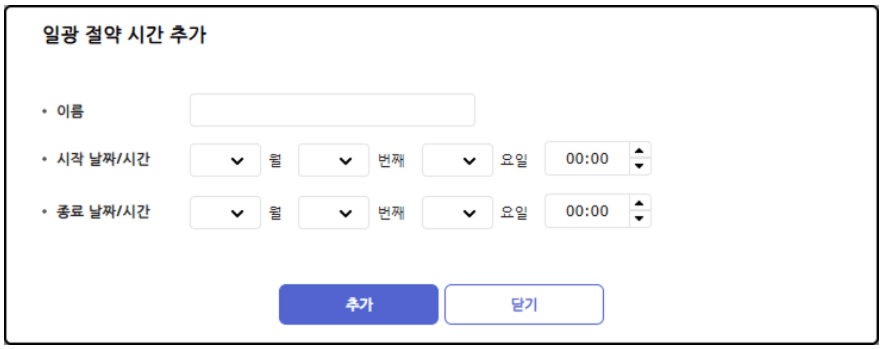
> **알아두기**
> 아래와 같은 경우에 일광 절약 시간을 설정하세요.
> - 일광 절약 시간을 채택한 국가나 지역에서 시스템을 운영하는 경우
> - 근태 관리 시스템과 연동하여 정확한 출입 시간을 기록해야 하는 경우
> - 여러 시간대에 걸쳐 운영되는 통합 보안 시스템을 관리하는 경우

일광 절약 시간 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **일광 절약 시간**을 클릭하세요.
3. **+ 추가** 버튼을 클릭하세요.



4. 각 항목을 설정하고 **추가** 버튼을 클릭하세요.



5. 추가한 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
> - 사용 중인 일광 절약 시간 설정은 수정하거나 삭제할 수 없습니다. 사용 중인 일광 절약 시간 설정은 **설정** → **시스템** → **기본 설정** 메뉴에서 확인할 수 있습니다.
> - 추가한 일광 절약 시간 설정을 시스템에 적용하는 자세한 내용은 기본 설정 구성하기를 참고하세요.

일광 절약 시간 수정

> **알아두기**
> 현재 사용 중인 설정은 수정할 수 없습니다. 수정하려면 먼저 **설정** → **시스템** → **기본 설정** 메뉴의 **언어/표준 시간대** 섹션에서 선택을 해제하세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **일광 절약 시간**을 클릭하세요.
3. 일광 절약 시간 목록 중 수정할 항목의 ✎ 버튼을 클릭하세요.
4. **일괄 절약 시간 편집** 창이 나타나면 원하는 항목을 수정하세요.



5. 수정을 완료하면 **편집** 버튼을 클릭하세요.
6. 수정한 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
> 일광 절약 시간 설정을 시스템에 적용하는 자세한 내용은 기본 설정 구성하기를 참고하세요.

일광 절약 시간 삭제

사용하지 않는 일광 절약 시간 설정을 삭제하세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **일광 절약 시간**을 클릭하세요.
3. 일광 절약 시간 목록 중 삭제할 항목의 🗑 버튼을 클릭하세요.
4. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.
5. 삭제한 설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

이메일 설정하기

사용자에게 얼굴 등록 모바일 링크를 전송하거나 QR/바코드를 발급할 이메일의 제목, 회사 이름, 회사 로고, 연락처와 같은 정보를 설정할 수 있습니다.

알아두기

- 사용자에게 얼굴 등록 모바일 링크를 전송하거나 QR/바코드를 발급하려면 반드시 사용자 정보에 이메일 주소가 등록되어 있어야 합니다. 사용자 정보에 대한 자세한 내용은 사용자 기본 정보 입력하기를 참고하세요.
- **얼굴 인증**할 수 있는 장치는 아래와 같습니다.
  - FaceStation F2, BioStation 3, BioEntry W3, BioStation 3 Max
- **스캐너로 QR/Barcode 인증**을 사용할 수 있는 장치는 아래와 같습니다.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- **카메라로 QR/Barcode 인증**을 사용할 수 있는 장치는 아래와 같습니다.
  - BioStation 3 Max 펌웨어 1.0.0 이상
  - BioStation 3 펌웨어 1.1.0 이상
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) 펌웨어 1.2.0 이상
  - X-Station 2 (XS2-QDPB, XS2-QAPB) 펌웨어 1.4.1 이상
- **카메라로 QR/Barcode 인증**을 사용하려면 별도의 장치 라이선스가 필요합니다. 장치 라이선스에 대한 자세한 내용은 장치 라이선스를 참고하세요.

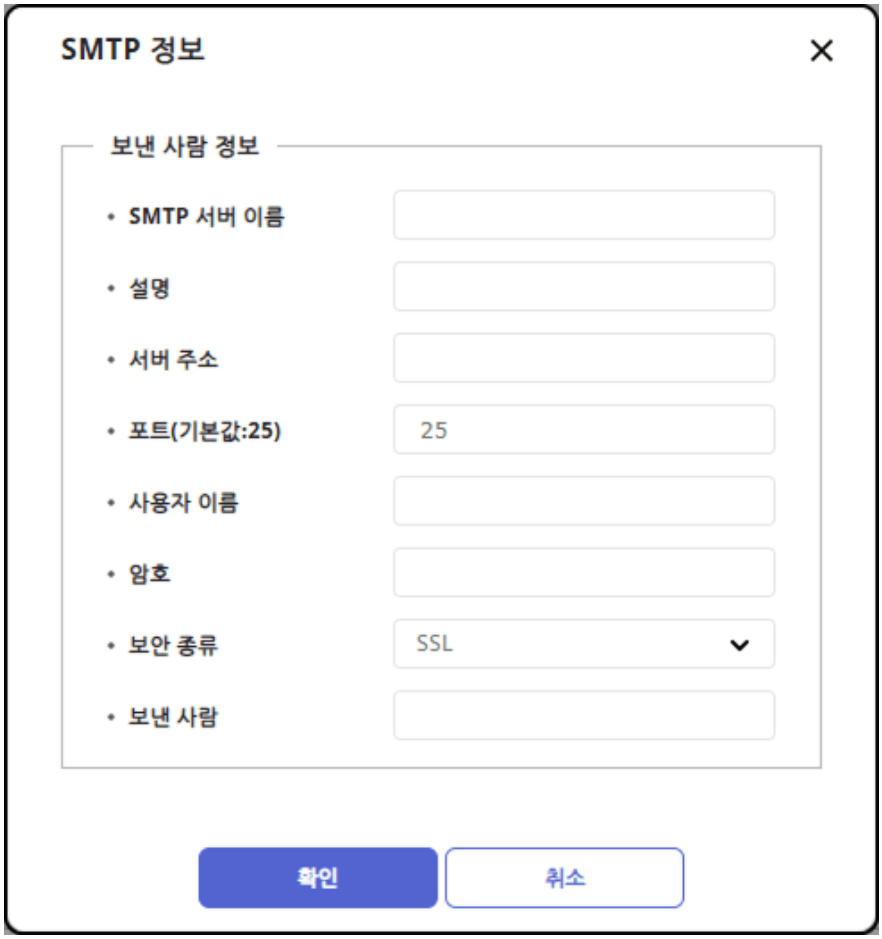
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **이메일 설정**을 클릭하세요.
3. 각 항목을 설정하세요.
4. 설정을 저장하려면 **확인**을 클릭하세요.

이메일 콘텐츠 설정하기

이메일 발송을 위한 SMTP 서버 정보를 입력하세요.



- **SMTP 설정**: 이메일 발송을 위해 간이 우편 전송 프로토콜(Simple Mail Transfer Protocol, SMTP)을 설정하세요. **SMTP 세팅** 버튼을 클릭하면 **SMTP 설정** 설정 창이 나타납니다.



- **SMTP 서버 이름**: SMTP 서버 이름을 입력하세요.
- **설명**: SMTP에 대한 설명을 입력하세요.
- **서버 주소**: SMTP 서버 주소를 입력하세요. SMTP 서버 주소는 `smtp.{email-service-provider}.com`과 같은 형태이며, SMTP 서버로 사용할 이메일의 설정 화면에서 확인할 수 있습니다.
- **포트(기본값:25)**: SMTP 서버의 포트 번호를 입력하세요. SMTP 서비스 공급자의 이메일 설정 화면에서 확인할 수 있습니다.
- **사용자 이름**: SMTP 서비스의 계정을 입력하세요.
- **암호**: SMTP 서비스의 계정 암호를 입력하세요.
- **보안 종류**: 보안 종류를 선택하세요.
- **보낸 사람**: 보낸 사람의 이메일 주소를 입력하세요.

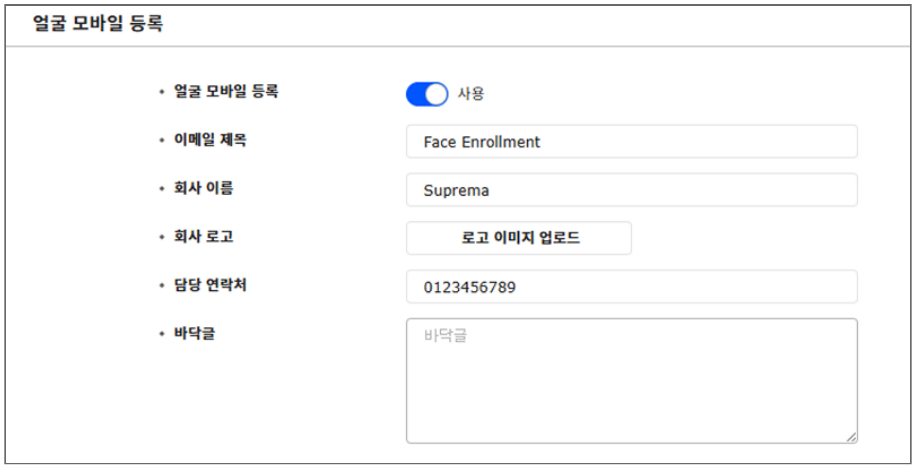
알아두기

- SMTP에 대한 자세한 내용은 시스템 관리자에게 문의하세요.
- SMTP 서버를 2단계 인증이 설정된 이메일 계정으로 사용할 경우 해당 계정의 비밀번호 변경 시 다음 사항에 유의하세요.
  - 2단계 인증을 설정하면 SMTP 암호는 해당 이메일 계정의 비밀번호가 아닌 2단계 인증으로 생성된 앱 비밀번호를 사용합니다.
  - 이때 해당 이메일 계정의 비밀번호가 변경되면 앱 비밀번호는 자동으로 삭제되며, SMTP 암호는 사용할 수 없게 됩니다.
  - 해당 이메일 계정의 비밀번호 변경 시 앱 비밀번호를 다시 생성한 뒤 SMTP 암호를 다시 설정하세요.

- **확인 메일 수신 주소**: SMTP 설정에 문제가 없는지 확인하려면 수신할 이메일 주소를 입력한 후 **이메일 보내기** 버튼을 클릭하세요.

얼굴 등록 모바일 링크 설정하기

이메일을 통해 사용자에게 얼굴 등록 모바일 링크를 전송하려면 **사용**으로 설정하세요.



- **이메일 제목**: 얼굴 등록 모바일 링크를 전송할 이메일의 제목을 입력하세요.
- **회사 이름**: 회사 이름을 입력하세요.
- **회사 로고**: 회사 로고 이미지를 업로드하세요.

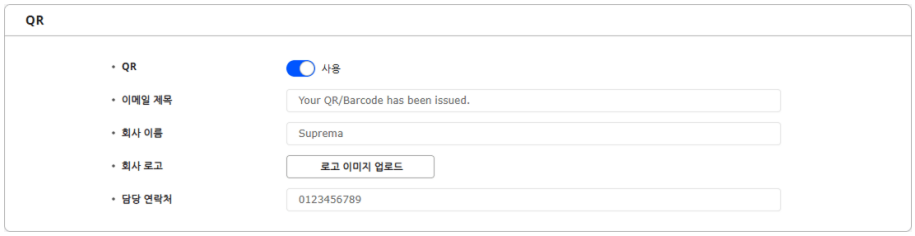
> **알아두기**
>
> – 지원되는 이미지 파일 형식은 GIF, JPG, JPEG, JPE, JFIF, PNG입니다.
>
> – 지원되는 이미지 파일의 크기는 최대 5MB입니다.

- **담당 연락처**: 담당자의 연락처를 입력하세요.
- **바닥글**: 법적 고지문 등 얼굴을 등록할 사용자에게 고지할 내용을 입력하세요. 얼굴 등록 모바일 링크 전송 메일의 하단에 표시됩니다.

> **알아두기**
>
> 바닥글은 최대 5,000자까지 입력할 수 있습니다.

QR/바코드 발급 설정하기

이메일을 통해 사용자에게 QR/바코드를 발급하려면 **사용**으로 설정하세요.



- **이메일 제목**: QR/바코드를 전송할 이메일의 제목을 입력하세요.
- **회사 이름**: 회사 이름을 입력하세요.

- **회사 로고**: 회사 로고 이미지를 업로드하세요.

> **알아두기**
>
> – 지원되는 이미지 파일 형식은 GIF, JPG, JPEG, JPE, JFIF, PNG입니다.
>
> – 지원되는 이미지 파일의 크기는 최대 5MB입니다.

- **담당 연락처**: 담당자의 연락처를 입력하세요.

기본 설정 구성하기

BioStar X를 효율적으로 사용하기 위해서는 사용 환경에 맞는 기본 설정이 필요합니다. 아래와 같은 상황에서 필요한 설정 방법을 안내합니다.

- 새로 설치한 **BioStar X**의 초기 설정
- 사용자가 선호하는 언어로 변경
- 현지 시간대에 맞는 시간 설정
- 이벤트 알림음 사용자화

기본 설정 진입

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템** → **기본 설정**을 클릭하세요.
3. 각 섹션에서 원하는 옵션을 설정하세요.
   - **언어/표준 시간대**: 인터페이스 언어 및 시간대, 일광 절약 시간
   - **날짜/시간**: 날짜 및 시간 형식
   - **소리**: 이벤트 알림음
4. 모든 설정을 완료하고 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

언어 및 표준 시간대 설정

BioStar X의 인터페이스 언어와 시간대, 일광 절약 시간 규칙을 설정할 수 있습니다.



- **언어**: 사용하려는 인터페이스 언어를 선택하세요.
- **표준 시간대**: 현재 위치에 해당하는 시간대를 선택하세요.
- **일광 절약 시간**: **BioStar X** 서버에 적용할 일광 절약 시간 규칙을 선택하세요. 원하는 항목이 없다면 일광 절약 시간 설정하기를 참고하여 추가할 수 있습니다.

설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

날짜 및 시간 표시 형식 설정

시스템 전체에서 사용할 날짜와 시간 표시 형식을 설정할 수 있습니다.



- **날짜 형식**: 날짜 형식을 변경할 수 있습니다.
  - **mm/dd/yyyy**: 01/31/2025
  - **yyyy/mm/dd**: 2025/01/31
  - **dd/mm/yyyy**: 31/01/2025
- **시간 형식**: 시간 형식을 변경할 수 있습니다.
  - **hh:mm**: 23:59, 24시간 형식
  - **hh:mm a**: 11:59 PM, 12시간 형식
  - **a hh:mm**: PM 11:59, 12시간 형식

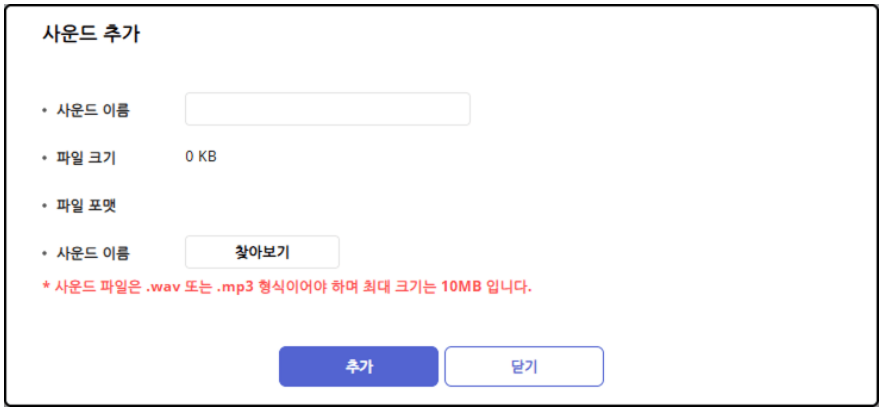
설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

이벤트 알림 소리 설정

이벤트가 발생할 때 사용할 사운드 파일을 업로드할 수 있습니다.



1. **+ 추가**를 클릭하세요.
2. **사운드 추가** 창이 나타나면 **찾아보기**를 클릭하세요.



3. 업로드하려는 *.wav* 또는 *.mp3* 파일을 선택하고 **열기**를 클릭하세요.
4. 사운드 파일을 업로드하려면 **추가** 버튼을 클릭하세요.

설정을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

알아두기

- 사운드 파일은 *.wav* 또는 *.mp3* 파일 형식만 업로드할 수 있습니다.
- 업로드할 수 있는 최대 파일 크기는 10MB입니다.
- 이벤트가 발생할 때 업로드한 사운드 파일을 적용하는 방법은 경보 설정하기를 참고하세요.

고급 설정

에센셜(Essential) 라이선스에서 추가 옵션을 구매하거나 **엔터프라이즈**(Enterprise) 라이선스 이상에서 사용할 수 있는 고급 설정 기능을 안내합니다.

엘리베이터 관리하기

엘리베이터를 그룹 등록 및 관리하는 방법을 안내합니다. 엘리베이터와 관련한 출입 통제 설정을 통해 특정 층에 대한 출입 권한을 제어할 수 있습니다. 이를 통해 보안과 편의성을 강화할 수 있습니다.

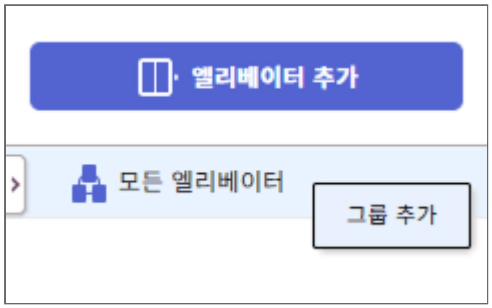
엘리베이터 그룹 관리하기

여러 개의 엘리베이터를 쉽게 관리할 수 있도록 그룹 설정 방법을 안내합니다. 엘리베이터 그룹은 여러 개의 엘리베이터를 하나의 그룹으로 묶어 관리할 수 있는 기능입니다. 그룹을 설정하면 엘리베이터를 일괄 설정할 수 있습니다.

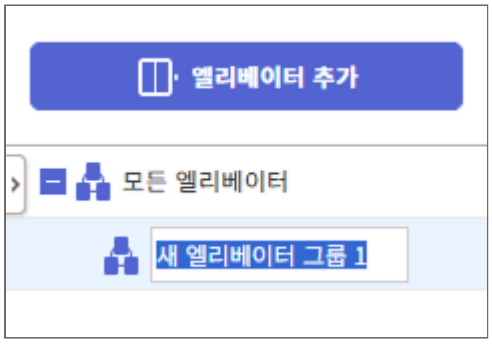
> **팁**
> 엘리베이터 위치로 그룹 이름을 등록하면 관리가 편리합니다.

엘리베이터 그룹 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 **모든 엘리베이터**를 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **그룹 추가** 버튼을 클릭하세요.
5. 원하는 그룹 이름을 입력하세요.



알아두기

- 엘리베이터 그룹은 최대 8단계까지 생성할 수 있습니다.
- 엘리베이터 그룹 이름은 최대 48자까지 입력할 수 있습니다.

엘리베이터 그룹 이름 변경

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 이름을 변경할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



4. 팝업 메뉴에서 **이름 변경**을 클릭하세요.
5. 변경할 그룹 이름을 입력하세요.

알아두기
엘리베이터 그룹 이름은 최대 48자까지 입력할 수 있습니다.

엘리베이터 그룹 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.

3. 엘리베이터 목록에서 삭제할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



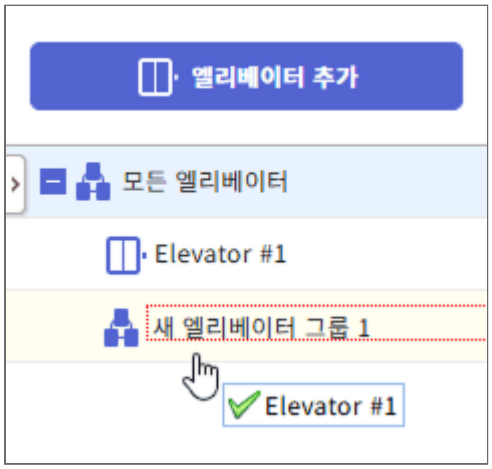
4. 팝업 메뉴에서 **그룹 삭제**을 클릭하세요.

> **주의**
> 엘리베이터 그룹을 삭제하면 그룹에 포함된 모든 엘리베이터가 삭제됩니다. 그룹에 포함된 엘리베이터를 삭제하지 않으려면 먼저 엘리베이터를 다른 그룹으로 이동한 후 그룹을 삭제하세요.

그룹에 엘리베이터 추가

엘리베이터 목록에서 그룹에 추가하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 그룹에 추가할 엘리베이터를 선택하고 원하는 그룹으로 드래그하세요.



선택한 엘리베이터가 그룹으로 이동합니다.

엘리베이터 정보에서 그룹에 추가하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.

3. 화면 오른쪽의 엘리베이터 목록에서 그룹에 추가할 엘리베이터를 클릭하세요.
4. 엘리베이터 정보 수정 화면이 나타나면 **정보** 섹션의 **그룹** 옵션을 클릭하세요.



5. 원하는 그룹을 선택하세요.
6. 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

엘리베이터 등록하기

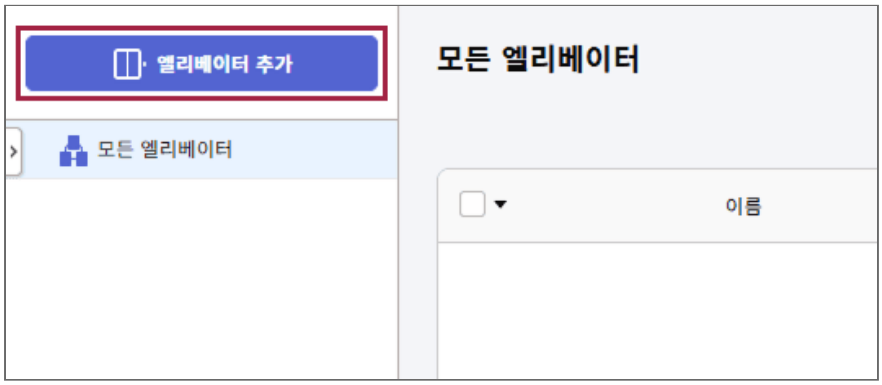
엘리베이터를 등록하고 설정하는 방법을 안내합니다. 엘리베이터는 층 제어에 사용되며, 출입문과 함께 출입 통제 시스템을 구성합니다. 엘리베이터를 등록하면 특정 층에 대한 출입 권한을 제어할 수 있습니다.

시작하기 전에

- 엘리베이터를 등록하기 전에 출입 통제를 위한 출입 등급, 출입 그룹, 층 등급을 설정하세요. 자세한 내용은 출입 통제 설정하기를 참고하세요.
- 엘리베이터를 등록하기 전에 장치를 등록하세요. 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 장치 등록하기
  - Wiegand 장치 등록하기
  - 슬레이브 장치 등록하기

엘리베이터 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 화면 왼쪽 상단의 **엘리베이터 추가** 버튼을 클릭하세요.



4. **새 엘리베이터 추가** 화면이 나타나면 각 섹션 항목을 차례로 설정하세요.
   - **정보**: 엘리베이터의 기본 정보를 설정하세요. 자세한 내용은 기본 정보 설정을 참고하세요.
   - **상세 정보**: 엘리베이터의 세부 정보를 설정하세요. 자세한 내용은 상세 정보 설정을 참고하세요.
   - **옵션**: 부가 옵션을 설정하세요. 자세한 내용은 부가 옵션 설정을 참고하세요.

- **알람**: 안티패스백 위반이 발생했을 때 경보를 울리거나 장치를 사용하지 못하도록 설정할 수 있습니다. 자세한 내용은 알람 설정을 참고하세요.

5. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

기본 정보 설정

정보 섹션에서는 엘리베이터의 이름 및 그룹, 설명을 입력하거나 변경할 수 있습니다.

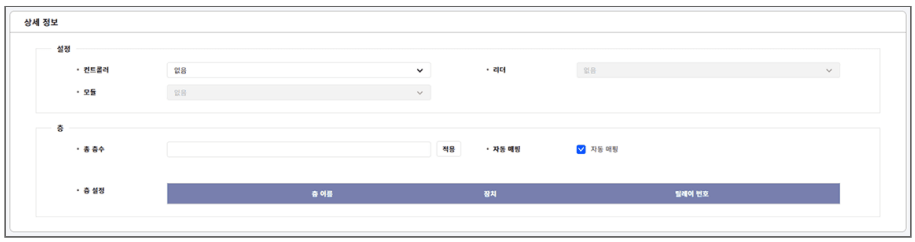


- **이름**: 엘리베이터의 이름을 입력하세요. 엘리베이터의 위치를 특정할 수 있는 이름을 입력하면 편리하게 관리할 수 있습니다.
- **그룹**: 엘리베이터 그룹을 선택하세요.
- **설명**: 엘리베이터에 대한 간단한 설명을 입력하세요.

> **알아두기**
>
> - 엘리베이터 이름은 최대 48자까지 입력할 수 있습니다.
> - 엘리베이터 그룹 등록에 대한 자세한 내용은 엘리베이터 그룹 관리하기를 참고하세요.

상세 정보 설정

상세 정보 섹션에서는 엘리베이터의 세부 정보를 설정할 수 있습니다. 엘리베이터에 연결할 장치와 층 정보를 설정하세요.



- **컨트롤러**: 엘리베이터 접근 권한을 제어할 장치를 선택하세요.
- **리더**: 인증할 때 사용할 장치를 선택하세요.
- **모듈**: 엘리베이터 버튼 릴레이를 제어할 장치를 선택하세요.
- **총 층수**: 엘리베이터로 이동할 수 있는 총 층수를 입력하세요. 최대 192층까지 입력할 수 있습니다.
- **자동 매핑**: 자동 매핑 사용 여부를 선택하세요. 자동 매핑을 사용하면 릴레이 번호를 순차적으로 부여합니다.
- **층 설정**: 층 이름과 층을 제어할 릴레이 번호를 설정하세요.

> **알아두기**
>
> - **컨트롤러** 옵션에서는 마스터 장치만 선택할 수 있습니다.
> - **리더** 옵션에서는 마스터 장치, 슬레이브 장치, Wiegand 장치만 선택할 수 있으며, 최대 4개까지 선택할 수 있습니다.
>
> OM-120 모델은 리더로 설정할 수 없습니다.
> - **모듈** 옵션에서는 OM-120, DM-20, IM-120, SIO2 모델만 선택할 수 있습니다.

부가 옵션 설정

옵션 섹션에서는 엘리베이터의 부가 옵션을 설정할 수 있습니다.



- **릴레이 제어**: 층 버튼 릴에이에 대한 옵션을 설정하세요.
  - **열림 시간**: 인증 완료 후 층 버튼이 활성화된 상태로 유지되는 시간을 설정하세요. 이 시간이 지나면 릴레이는 층 버튼에 신호를 보내지 않습니다.
- **이중 인증**: 두 사람(일반 사용자와 관리자)이 크리덴셜을 인증하여 층 버튼이 활성화되도록 설정할 수 있습니다.
  - **장치**: 이중 인증을 사용할 장치를 선택하세요. 이중 인증을 사용하지 않으려면 **없음**을 선택하세요.
  - **스케줄**: 이중 인증을 사용할 스케줄을 선택하세요. 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다.
  - **관리자 인증 순서**: 관리자 인증 순서를 설정하세요.
  - **사용 안 함**: 인증 그룹과 관계 없이 두 명의 인증이 필요합니다.
  - **마지막**: 일반 사용자가 인증하고 설정된 인증 그룹에 포함된 사용자가 인증해야 합니다.
  - **인증 그룹**: 관리자가 속한 그룹을 설정하세요. 이 옵션은 **관리자 인증 순서**을 **마지막**으로 선택했을 때 사용할 수 있습니다.
  - **인증 대기 시간**: 첫 번째 인증 후 두 번째 인증까지의 대기 시간을 설정하세요. 설정된 시간 내에 두 번째 인증이 완료되지 않으면 층 버튼이 활성화되지 않습니다.

> **알아두기**
>
> - 재실 인원 제한 설정에 구성된 장치의 이중 인증을 변경하려면 다음 메뉴에서 설정을 수정하세요. **설정** → **출입 관리** → **고급 출입 통제** → **재실 인원 제한**
>
> **재실 인원 제한** 설정에 대한 자세한 내용은 고급 출입 통제 설정하기를 참고하세요.
> - 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

- **탬퍼**: 탬포 신호를 출력할 포트를 설정하세요.

알람 설정

알람 섹션에서는 탬퍼 입력을 감지하거나 별도의 입력 신호를 감지했을 때 수행할 동작을 설정할 수 있습니다. 작업 조건 및 동작을 추가하려면

+ 추가 버튼을 클릭하세요.



- **작업 조건**: 탬퍼 입력 감지 또는 별도의 입력 신호 감지를 설정하세요.
- **동작**: 설정한 작업 조건에 따라 수행할 동작을 설정하세요. 엘리베이터의 모든 층 버튼을 활성화하거나 특정 신호를 출력할 수 있습니다.

엘리베이터 정보 수정하기

등록된 엘리베이터의 설정 정보를 수정하는 방법을 안내합니다. 개별 엘리베이터의 상세 설정을 변경하거나, 여러 엘리베이터를 선택하여 공통 항목을 일괄 수정할 수 있습니다.

한 개의 엘리베이터 정보 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 정보를 수정하려는 엘리베이터를 클릭하세요.
4. 각 섹션의 세부 항목을 수정하세요.
5. 설정을 모두 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> 엘리베이터 정보 수정 화면의 각 섹션에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.

여러 개의 엘리베이터 일괄 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 정보를 수정하려는 엘리베이터의 체크박스를 클릭하세요. 두 개 이상의 엘리베이터를 선택하세요.
4. 화면 오른쪽 상단에 **일괄 편집** 버튼을 클릭하세요.
5. **일괄 편집** 창이 나타나면 원하는 옵션을 설정하세요.



6. 설정을 모두 완료했다면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **일괄 편집** 버튼은 엘리베이터 목록에서 두 개 이상의 엘리베이터를 선택해야 활성화됩니다.
> - 일괄 편집 시 **열림 시간** 옵션만 수정할 수 있습니다.

엘리베이터 삭제하기

등록된 엘리베이터를 삭제하는 방법을 안내합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 지점** → **엘리베이터**를 클릭하세요.
3. 엘리베이터 목록에서 삭제하려는 엘리베이터의 체크박스를 클릭하세요.
4. 화면 오른쪽 상단에 **엘리베이터 삭제** 버튼을 클릭하세요.

선택한 엘리베이터가 삭제됩니다. 삭제된 엘리베이터는 복구할 수 없습니다.

> **알아두기**
>
> **엘리베이터 삭제** 버튼은 엘리베이터 목록에서 한 개 이상의 엘리베이터를 선택해야 활성화됩니다.

고급 출입 통제 설정하기

고급 출입 통제 설정을 통해 출입을 통제할 수 있습니다. 보안 요구사항과 운영 환경에 따라 다양한 고급 출입 통제 기능을 설정할 수 있습니다. 안티패스백으로 무단 재출입을 방지하고, 화재나 침입 같은 긴급 상황에 대응하며, 스케줄 기반으로 출입문을 자동 제어하거나, 특정 장소의 인원을 제한하고 모니터링할 수 있습니다.

안티패스백

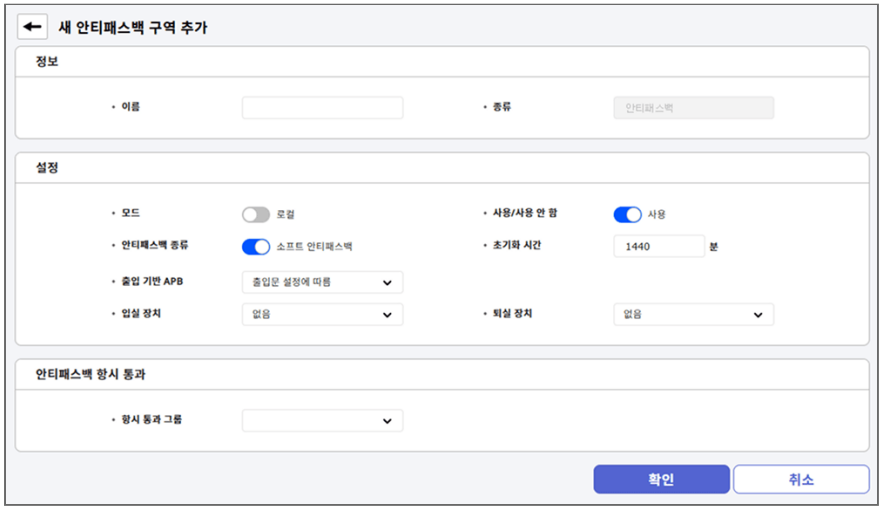
안티패스백은 출입문 또는 장치를 기준으로 생성된 안티패스백보다 향상된 기능을 제공합니다. 안티패스백을 설정하여 사용자가 입실 및 퇴실할 때 지정된 출입문과 장치를 사용하도록 강제할 수 있습니다. 이를 통해 무단 재출입을 방지하고, 보안을 강화할 수 있습니다.

> **알아두기**
>
> **안티패스백(Anti-Passback)**: 출입 통제를 위해 구조적인 방법으로서, 출입문 안쪽/바깥쪽에 출입 통제 장치를 설치하여 구역에 출입할 때 반드시 인증을 통해 출입해야 하는 기능입니다. 카드를 사용해 출입할 때 리더기에 카드를 인식하지 않고 앞 사람을 따라 입실했다면, 퇴실할 때 출입문이 열리지 않으며 **안티패스백** 이벤트가 발생합니다.
> **안티패스백**은 Hard APB와 Soft APB로 구분합니다. **안티패스백** 위반 시 Hard APB는 **안티패스백** 이벤트를 생성하고 출입할 수 없으며, Soft APB는 **안티패스백** 이벤트를 생성하고 출입은 가능합니다.

안티패스백 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.

4. **안티패스백**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 안티패스백 기능의 이름을 입력하세요.



6. **설정** 섹션에서 안티패스백 기능의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **알람** 섹션에서 안티패스백 위반이 발생했을 때 수행할 동작을 설정하세요.
8. **안티패스백 항시 통과** 섹션에서 안티패스백을 우회하여 통과할 수 있는 출입 그룹을 선택하세요. 이 그룹에 속한 사용자는 안티패스백을 우회할 수 있습니다.
9. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **알람** 섹션은 **입실 장치**와 **퇴실 장치**를 모두 설정해야 사용할 수 있습니다.

설정 옵션 안내

안티패스백 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 설정하세요.
  - **로컬**: 입실 장치와 RS-485로 연결된 장치들로 설정할 수 있습니다.
  - **글로벌**: BioStar X에 등록된 모든 장치로 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **안티패스백 종류**: 안티패스백 종류를 선택하세요.
  - **하드 안티패스백**: 안티패스백 이벤트를 생성하고 출입할 수 없습니다.
  - **소프트 안티패스백**: 안티패스백 이벤트를 생성하고 출입할 수 있습니다.
- **초기화 시간**: 안티패스백 규칙을 위반한 사용자에게 출입을 다시 허용할 때까지의 대기 시간을 설정하세요. 알람 발생 후 설정된 시간이 지나면 해당 사용자의 출입을 자동으로 허용합니다.
  - 1분에서 10080분(7일) 범위에서 설정할 수 있습니다.
  - 0분으로 설정하면 알람은 자동으로 해제되지 않아 관리자가 수동으로 해제할 때까지 출입할 수 없습니다.

- **출입 기반 APB**: 안티패스백 규칙을 적용할 범위를 설정하세요.
  - **켬**: 입실 장치와 퇴실 장치가 구성된 출입문의 실제 동작에 따라 안티패스백 규칙이 적용됩니다.
  - **끔**: 출입문의 동작과 관계없이 사용자의 인증에 따라 규칙이 적용됩니다.
  - **출입문 설정에 따름**: 해당 출입문의 출입 기반 APB 사용 시 센서 사용 옵션 설정에 따라 안티패스백 규칙이 적용됩니다.
- **입실 장치**: 입실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **퇴실 장치**: 퇴실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **네트워크 오류 동작**: BioStar X와 안티패스백이 설정된 장치의 통신이 끊어졌을 때 출입문 동작을 설정하세요. 이 기능은 **모드** 옵션을 **글로벌**로 설정했을 때 사용할 수 있습니다.
  - **인증 시 문 열림**: 사용자를 정상적으로 인증할 때 출입문이 열립니다.
  - **인증 시 문 열림 및 APB 로그 기록**: 안티패스백 위반 알람이 발생하며 출입문이 열립니다.
  - **문 잠금 및 APB 로그 기록**: 안티패스백 위반 알람이 발생하며 출입문이 열리지 않습니다.

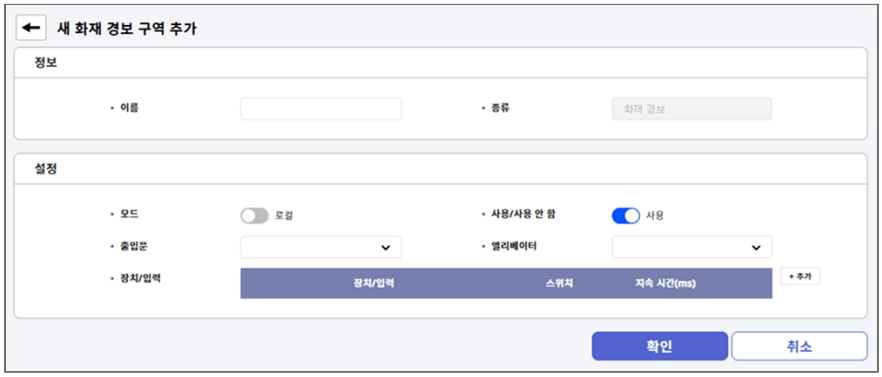
> **알아두기**
> 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
> - 장치 등록하기
> - Wiegand 장치 등록하기
> - 슬레이브 장치 등록하기

화재 경보

화재 경보 설정 방법을 안내합니다. 화재 경보는 화재가 발생할 때 모든 출입문 또는 엘리베이터가 개방되거나 잠기도록 설정하는 기능입니다.

화재 경보 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **화재 경보**를 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 화재 경보의 이름을 입력하세요.



6. **설정** 섹션에서 화재 경보의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **알람** 섹션에서 화재 경보가 발생했을 때 수행할 동작을 설정하세요.
8. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **알람** 섹션은 **출입문**을 설정해야 사용할 수 있습니다.

설정 옵션 안내

화재 경보 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 설정하세요.
  - **로컬**: 입실 장치와 RS-485로 연결된 장치들로만 설정할 수 있습니다.
  - **글로벌**: BioStar X에 등록된 모든 장치로 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **출입문**: 화재 경보 규칙을 지정할 출입문을 선택하세요.
- **엘리베이터**: 화재 경보 규칙을 지정할 엘리베이터를 선택하세요.
- **장치/입력**: **+ 추가** 버튼을 클릭하고 화재 경보 신호를 발생할 장치를 설정하세요.

> **알아두기**
> - **모드** 옵션을 **로컬**로 설정하면 출입문이나 엘리베이터 중 하나만 화재 경보 기능을 설정할 수 있습니다.
> - **모드** 옵션을 **글로벌**로 설정하면 출입문과 엘레베이터를 동시에 화재 경보 기능을 설정할 수 있습니다.
> - 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
>   - 장치 등록하기
>   - Wiegand 장치 등록하기
>   - 슬레이브 장치 등록하기

스케줄 잠금

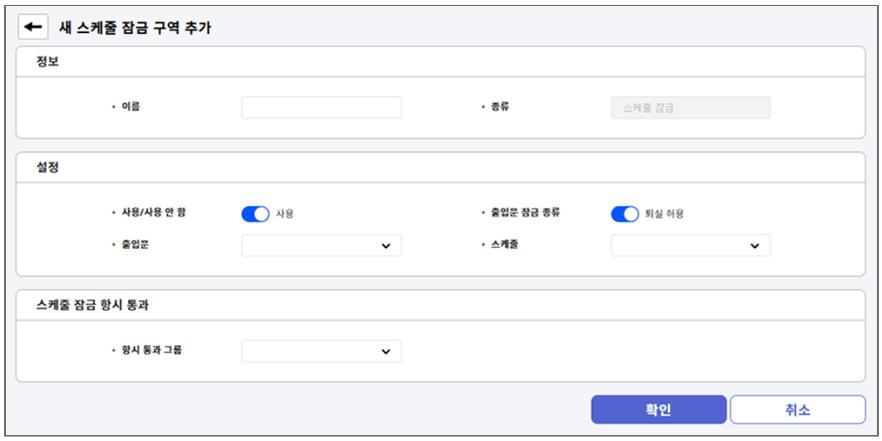
스케줄 잠금 설정 방법을 안내합니다. 스케줄 잠금은 특정 시간에 출입문을 잠그는 기능을 제공합니다. 이 기능은 출입 통제를 강화하고, 특정 시간대에 출입을 제한하는 데 유용합니다.

> **알아두기**
> 스케줄 잠금 설정은 **로컬** 모드만 지원합니다.

스케줄 잠금 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **스케줄 잠금**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 스케줄 잠금 기능의 이름을 입력하세요.



6. **설정** 섹션에서 스케줄 잠금 기능의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **알람** 섹션에서 스케줄 잠금 기능 위반이 발생했을 때 수행할 동작을 설정하세요.
8. **스케줄 잠금 항시 통과** 섹션에서 스케줄 잠금을 우회하여 통과할 수 있는 출입 그룹을 선택하세요. 이 그룹에 속한 사용자는 스케줄 잠금을 우회할 수 있습니다.
9. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **알람** 섹션은 **출입문**을 설정해야 사용할 수 있습니다.

설정 옵션 안내

스케줄 잠금 설정을 위한 세부 항목은 아래와 같습니다.

- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **출입문 잠금 종류**: 입실 장치만 잠그도록 설정하거나 입실 장치와 퇴실 장치를 모두 잠그도록 설정할 수 있습니다.
- **출입문**: 스케줄 잠금 규칙을 지정할 출입문을 선택하세요.
- **스케줄**: 스케줄을 선택하세요. 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다.

> **알아두기**
> - **로컬** 모드에서 다수의 출입문을 선택하여 스케줄 잠금 기능을 구성할 수 있습니다.
> - 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

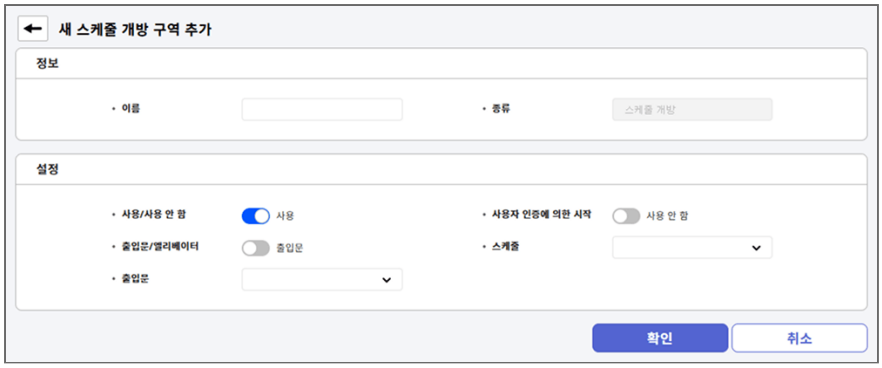
스케줄 개방

스케줄 개방 설정 방법을 안내합니다. 스케줄 개방은 특정 시간에 출입문을 개방하는 기능을 제공합니다. 이 기능은 출입 통제를 강화하고, 특정 시간대에 출입을 허용하는 데 유용합니다.

> **알아두기**
> 스케줄 개방은 **로컬** 모드만 지원합니다.

스케줄 개방 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **스케줄 개방**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 스케줄 개방 기능의 이름을 입력하세요.



6. **설정** 섹션에서 스케줄 개방 기능의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **스케줄 개방 인증** 섹션에서 스케줄 개방을 시작할 수 있는 사용자를 포함한 출입 그룹을 선택할 수 있습니다.
8. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

설정 옵션 안내

스케줄 개방 설정을 위한 세부 항목은 아래와 같습니다.

- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **사용자 인증에 의한 시작**: **사용**으로 설정하면 **스케줄 개방 인증** 섹션이 나타납니다. **출입 그룹**에서 선택한 사용자 그룹의 사용자가 지정한 스케줄에 맞춰 인증해야 스케줄 개방을 시작합니다.
- **출입문/엘리베이터**: 스케줄 개방 기능을 적용할 출입문 또는 엘리베이터를 선택하세요.
  - **출입문**을 선택하면 출입문 목록이 활성화됩니다. 스케줄 개방 기능을 적용할 출입문을 선택하세요. 여러 개의 출입문을 선택할 수 있습니다.
  - **엘리베이터**를 선택하면 엘리베이터 목록이 활성화됩니다. 스케줄 개방 기능을 적용할 엘리베이터를 선택하세요. 여러 개의 엘리베이터를 선택할 수 있습니다.

> **출입문/엘리베이터** 옵션은 엘리베이터가 등록되어 있을 때 표시됩니다. 엘리베이터를 등록하지 않았다면 **출입문** 옵션만 표시됩니다. 엘리베이터 등록에 대한 자세한 내용은 엘리베이터 등록하기를 참고하세요.

- **스케줄**: 스케줄을 선택하세요. 원하는 스케줄이 없다면 **+ 스케줄 추가**를 클릭해 추가할 수 있습니다.
- **층**: 선택한 엘리베이터의 층을 선택할 수 있습니다.

> **알아두기**
>
> - **로컬** 모드에서 다수의 출입문을 선택하여 스케줄 개방 기능을 구성할 수 있습니다.
> - 이미 다른 스케줄 개방 설정에 속한 엘리베이터를 선택할 경우 동일한 층을 중복하여 설정할 수 없습니다.
> - 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

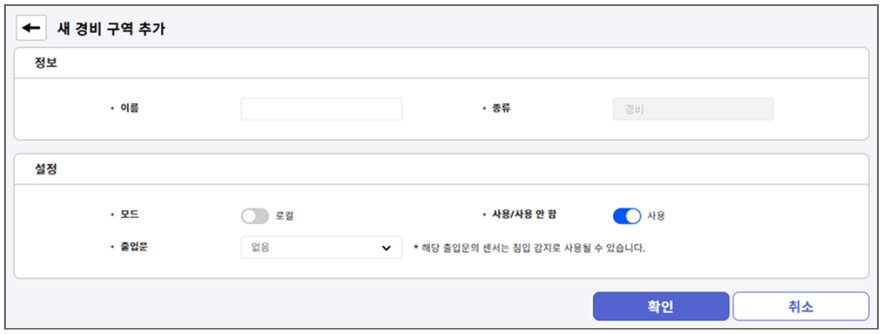
경비

경비 설정 방법을 안내합니다. 경비 설정은 침입 감지 시 출입문을 잠그거나 알람을 발생시키는 기능을 제공합니다.

> **알아두기**
>
> **경비 구역**: 경비 개시 후 허가받지 않은 사람이 침입을 시도하면 경고음을 출력하거나 릴레이 신호를 출력하도록 설정한 구역입니다. 주로 업무 종료 이후 경비를 개시하며, 경비 개시 이후 출입을 시도하면 설정된 알람이나 신호를 출력합니다.

경비 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **경비**를 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 경비 설정의 이름을 입력하세요.



6. **설정** 섹션에서 경비 설정의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **경비 / 해제 설정** 섹션에서 경비 개시와 해제에 대한 인증 설정을 추가하세요. 자세한 내용은 경비 개시 또는 해제 설정을 참고하세요.



> **경비 / 해제 설정** 섹션은 **정보** 섹션에서 출입문을 선택했을 때 표시됩니다.

8. **침입감지 설정** 섹션에서 침입 감지 신호를 설정하세요. 자세한 내용은 침입감지 설정을 참고하세요.



9. **알람** 섹션에서 특정 이벤트가 발생했을 때 수행할 동작을 설정하세요.
10. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **경비 / 해제 설정** 및 **침입감지 설정**, **알람** 섹션은 **설정** 섹션에서 **출입문** 옵션을 설정해야 사용할 수 있습니다.

설정 옵션 안내

경비 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 설정하세요. 경비 설정은 **로컬** 모드만 지원하며, 입실 장치와 RS-485로 연결된 장치들로만 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **출입문**: 경비 기능을 적용할 출입문을 선택하세요.

경비 개시 또는 해제 설정

경비 개시와 해제에 대한 인증 설정을 추가할 수 있습니다.



- **지연시간**: 경비 시작이나 경비 해제까지의 지연 시간을 설정할 수 있습니다. 즉, 개시는 인증 후 경비 시작까지의 지연 시간이며, 해제는 침입 감지 후 경보가 발생하기 전까지의 지연 시간입니다.
- **경비/해제 카드**: 경비 시작이나 해제 권한을 부여한 카드를 추가할 수 있습니다. 경비/해제 카드는 최대 128개까지 등록할 수 있습니다.
- **경비/해제 그룹**: 경비 시작이나 해제 권한을 부여한 그룹을 선택할 수 있습니다. 경비/해제 그룹은 최대 128개까지 등록할 수 있습니다.

- **경비/해제의 개시**: 장치에 의한 경비 시작/해제 또는 입력 신호에 의한 경비 시작/해제를 설정할 수 있습니다. **+ 추가** 버튼을 클릭하고 각 항목을 설정하세요.

장치에 의한 경비 시작/해제 추가

경비/해제의 개시 (**장치**) 옵션에서 **+ 추가** 버튼을 클릭하세요. 경비 기능을 제어할 장치를 선택하고 **경비 종류**를 선택하세요.

입력 종류는 **카드**, **키**, **카드 또는 키**를 선택할 수 있습니다. LCD 화면이 없는 장치는 입력 종류를 **카드**만 사용할 수 있습니다.



입력 신호에 의한 경비 시작/해제 추가

경비/해제의 개시 (**입력**) 옵션에서 **+ 추가** 버튼을 클릭하세요. 경비 기능을 제어할 장치를 선택하세요. **포트**를 클릭하여 선택된 장치의 입력 포트를 선택하세요.

경비 종류를 선택한 뒤 스위치 종류와 신호의 지속 시간을 설정하세요.



침입감지 설정

침입 감지 신호를 설정할 수 있습니다. **+ 추가** 버튼을 클릭하고 아래와 같이 설정하면 BioStation 3 장치의 0번 입력 포트에 연결된 N/O 센서가 100(ms) 동안 신호를 보낸 경우 침입을 감지한 것으로 인식합니다.



인터락

인터락은 보안이 중요한 영역에서 사용하는 출입 통제 방식입니다. 두 개 이상의 출입문이 구성되어 있는 장소에서 인터락을 설정하면 다음과 같이 작동합니다.

- 출입문 센서와 릴레이를 통해 각 출입문의 상태를 실시간으로 모니터링합니다.
- 한 출입문이 열려 있거나 잠금이 해제되어 있으면, 다른 모든 출입문은 자동으로 잠금 상태가 됩니다.
- 해당 장소에 사용자가 머물러 있는 동안에는 추가 출입을 차단하도록 설정할 수 있습니다.

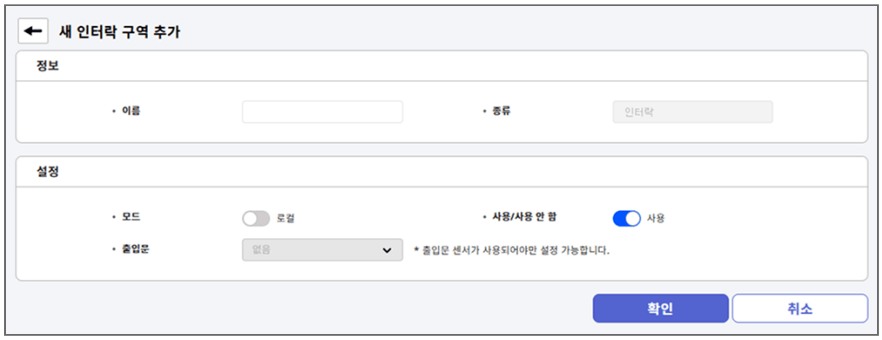
이러한 방식으로 동시에 여러 출입문이 열리는 것을 방지하여 보안을 강화합니다.

> **알아두기**
>
> - 하나의 인터락 설정은 최대 4개의 출입문으로 구성할 수 있습니다.
> - CoreStation에 연결된 장치로 구성된 출입문만 인터락을 설정할 수 있습니다.
> - 인터락으로 설정된 장치는 다른 인터락 설정에서 사용할 수 없습니다.
> - 인터락으로 설정된 출입문은 화재 경보 설정 외에 다른 설정에서 사용할 수 없습니다.

인터락 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.

3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **인터락**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 인터락 설정의 이름을 입력하세요.



6. **설정** 섹션에서 인터락 설정의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **옵션** 섹션에서 사용자가 체류할 경우 출입할 수 없도록 설정할 수 있습니다.
8. **알람** 섹션에서 인터락 설정에 특정 이벤트가 발생했을 때 수행할 동작을 설정하세요.

> **알아두기**
> **옵션** 및 **알람** 섹션은 **설정** 섹션에서 **출입문**을 설정해야 사용할 수 있습니다.

설정 옵션 안내

인터락 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 설정하세요. 인터락 설정은 **로컬** 모드만 지원하며, CoreStation에 RS-485로 연결된 장치들로만 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **출입문**: 인터락으로 지정할 출입문을 선택하세요. 최소 2개 이상의 출입문을 선택해야 하며, 출입문 센서가 연결된 출입문만 추가할 수 있습니다.

소집

소집은 비상 상황 발생 시 효과적인 인원 관리와 안전 확보를 위한 필수 설정입니다. 이 기능을 통해 관리자는 특정 장소를 소집 지점으로 지정하여 긴급 상황에서 사용자들이 모이는 장소를 미리 정의할 수 있습니다.

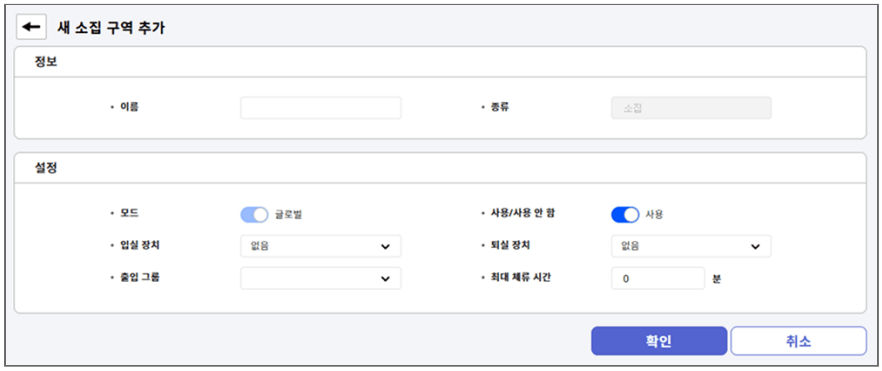
소집 설정은 다음과 같은 목적으로 활용합니다.

- **비상 대응**: 화재, 지진 등 긴급 상황 발생 시 사용자들이 안전하게 모일 수 있는 장소 지정
- **인원 모니터링**: 특정 장소 내 현재 인원 수와 출입자 명단을 실시간으로 확인
- **장시간 체류 감지**: 설정된 시간 이상 특정 장소에 머무는 사용자를 감지하여 관리자에게 알림 발송
- **보안 강화**: 민감한 장소의 출입을 지속적으로 모니터링하여 보안 수준 향상

이러한 기능을 통해 관리자는 보다 체계적이고 효율적인 보안 관리 체계를 구축할 수 있습니다.

소집 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **소집**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 소집 설정의 이름을 입력하세요.



6. **설정** 섹션에서 소집 설정의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **알람** 섹션에서 소집 설정에 특정 이벤트가 발생했을 때 수행할 동작을 설정하세요.
8. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **알람** 섹션은 **입실 장치**와 **퇴실 장치**를 모두 설정해야 사용할 수 있습니다.

설정 옵션 안내

소집 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 확인할 수 있습니다. 소집 설정은 **글로벌** 모드만 지원하며 **BioStar X**에 등록된 모든 장치로 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **입실 장치**: 입실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **퇴실 장치**: 퇴실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **출입 그룹**: 소집 장소에 체류할 사용자가 속한 출입 그룹을 설정하세요. 최대 16개의 출입 그룹을 설정할 수 있습니다.
- **최대 체류 시간**: 소집 장소에 머무를 수 있는 최대 시간을 설정할 수 있습니다. 최대 4320분으로 설정할 수 있으며, 지정된 시간을 초과하여 사용자가 소집 장소에 체류할 경우 알람이 발생합니다.

알아두기

장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.

- 장치 등록하기
- Wiegand 장치 등록하기
- 슬레이브 장치 등록하기

재실 인원 제한

재실 인원 제한은 공간의 안전성과 효율성을 보장하기 위한 핵심적인 출입 통제 기능입니다. 이 기능을 통해 관리자는 각 장소별로 동시에 입실할 수 있는 최대 인원 수를 미리 설정하여 과밀 상황을 예방하고, 보다 체계적인 공간 관리를 실현할 수 있습니다.

재실 인원 제한 설정의 주요 활용 분야는 다음과 같습니다.

- **안전 관리**: 화재 안전 규정이나 건물 수용 한계에 따른 최대 인원 제한으로 안전사고 예방
- **공간 효율성**: 회의실, 실험실, 작업장 등의 적정 인원 유지로 업무 환경 최적화
- **감염병 대응**: 사회적 거리두기나 밀집도 제한이 필요한 상황에서의 인원 관리
- **실시간 모니터링**: 각 장소별 현재 재실 인원과 입출입 현황을 실시간으로 확인
- **자동 경보**: 설정된 인원 수 도달하면 관리자에게 즉시 알림 발송으로 신속한 대응 가능

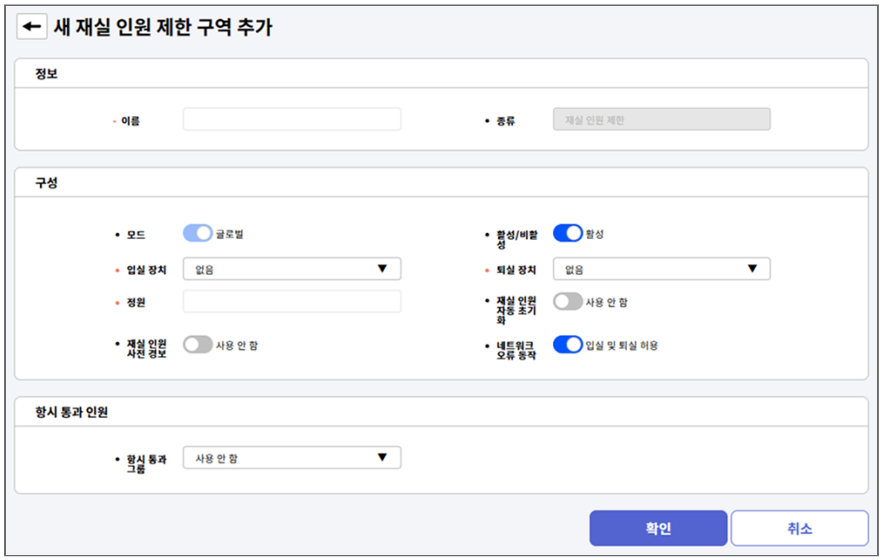
이러한 기능을 활용하여 관리자는 각 공간의 특성에 맞는 맞춤형 인원 관리 정책을 수립하고, 안전하고 효율적인 시설 운영을 보장할 수 있습니다.

알아두기

- 재실 인원 제한 설정은 최대 100개까지 추가할 수 있습니다.
- 재실 인원 제한 설정에 구성할 수 있는 장치와 펌웨어 버전은 아래와 같습니다.
  - FaceStation F2 펌웨어 1.1.0 이상
  - FaceStation 2 펌웨어 1.5.0 이상

재실 인원 제한 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **재실 인원 제한**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 재실 인원 제한 설정의 이름을 입력하세요.



6. **구성** 섹션에서 재실 인원 제한 설정의 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. **항시 통과 인원** 섹션에서 재실 인원 제한 설정을 항상 우회할 수 있는 출입 그룹을 선택할 수 있습니다. 자세한 내용은 항시 통과 인원 설정을 참고하세요.
8. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **이름**은 최대 48자까지 입력할 수 있으며, 다른 설정과 동일한 이름으로 설정할 수 없습니다.

설정 옵션 안내

재실 인원 제한 설정을 위한 세부 항목은 아래와 같습니다.

- **모드**: 적용 범위를 확인할 수 있습니다. 재실 인원 제한 설정은 **글로벌** 모드만 지원하며 **BioStar X**에 등록된 모든 장치로 설정할 수 있습니다.
- **활성/비활성**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **입실 장치**: 입실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **퇴실 장치**: 퇴실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **정원**: 입실을 제한할 인원을 입력할 수 있습니다. 입실한 인원이 설정한 제한 인원 수에 도달할 경우 입실이 제한됩니다. 0부터 10,000까지의 숫자로 입력할 수 있으며, 0으로 설정하면 인원 제한 없이 출입할 수 있습니다.
- **재실 인원 자동 초기화**: 저장된 재실 인원을 자동으로 초기화할 시간을 설정할 수 있습니다. 매일 설정한 시간에 재실 인원 및 항시 통과 인원 수가 초기화됩니다.
- **재실 인원 사전 경보**: 입실한 인원이 설정한 제한 인원 수에 도달하기 전에 미리 관리자에게 경보를 보내거나 이벤트 로그로 기록할 수 있습니다. 재실 인원 사전 경보를 사용으로 설정하면 **경보 1** 입력 필드가 활성화됩니다. **경보 2**를 설정하려면 ＋ 버튼을 클릭하세요.
- **네트워크 오류 동작**: 설정된 장치에 네트워크 오류가 발생하였을 때 사용자의 입실 및 퇴실 허용 여부를 설정할 수 있습니다. 입실 및 퇴실 허용으로 설정하면 장치의 네트워크 연결이 끊겼을 때 입실 제한이 중지되며, 실제 입실한 인원이 제한 인원을 초과하더라도 사용자가 입실할 수 있습니다.

알아두기

- 동일한 장치를 **입실 장치**와 **퇴실 장치**로 동시에 설정할 수 없습니다.
- **입실 장치**와 **퇴실 장치**는 최대 128개까지 선택할 수 있습니다.
- 출입문에서 **이중 인증**을 설정한 장치는 **입실 장치**와 **퇴실 장치**로 설정할 수 없습니다.
- **재실 인원 자동 초기화** 옵션의 시간은 실제 해당 장소가 위치한 지역의 표준 시간대를 고려하여 설정하세요. 예를 들어, UTC+1:00인 지역에 위치한 **BioStar X** 서버에서 재실 인원 자동 초기화 시간을 00:00으로 설정하면 UTC+2:00인 지역의 **BioStar X** 클라이언트에서는 01:00에 재실 인원이 자동으로 초기화됩니다.
- **재실 인원 사전 경보**는 최대 2개까지 설정할 수 있으며, 제한 설정 값보다 작은 숫자만 입력할 수 있습니다. **경보 1**과 **경보 2**는 동일하게 설정할 수 없습니다.
- 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 장치 등록하기
  - Wiegand 장치 등록하기
  - 슬레이브 장치 등록하기

항시 통과 인원 설정

재실 인원 제한 설정을 항상 통과할 수 있는 출입 그룹을 선택할 수 있습니다. 항시 통과 그룹에 속한 사용자는 재실 인원에 관계없이 출입할 수 있으며, 재실 인원 수로 세어지지 않습니다. 실제로 재실 중인 항시 통과 인원은 재실 인원 제한 설정 목록의 항시 통과 인원 열에서 확인할 수 있습니다.

알아두기

- 장치를 열화상 카메라와 연결하여 사용할 때 **열화상 및 마스크 확인 방식**을 **인증 없이 확인**으로 설정할 경우 항시 통과 인원을 설정하더라도 동작하지 않습니다.
- **항시 통과 그룹**은 최대 16개까지 설정할 수 있습니다.

목록 현황 확인

재실 인원 제한 설정 목록을 확인할 수 있습니다. 각 설정의 상태 및 재실 인원 수를 확인하고, 필요에 따라 설정을 변경할 수 있습니다.

- **이름**: 이름을 확인할 수 있습니다.
- **상태**: 상태를 확인할 수 있습니다.
  - **정상**: 사용자가 **제한**, **재실 인원 사전 경보**(**경보 1**, **경보 2**)에 설정한 인원 수보다 적게 재실 중인 상태입니다. 사용자는 해당 장소에 입실할 수 있습니다.
  - **재실 인원 사전 경보**: 재실한 사용자의 수가 **경보 1** 또는 **경보 2**에 설정한 인원에 도달한 상태입니다.
  - **정원 도달**: 재실한 사용자의 수가 제한에 설정한 인원에 도달한 상태입니다. 더 이상의 입실이 제한됩니다.
- **재실 인원/정원**: 정원 대비 현재 입실한 인원의 수를 확인할 수 있습니다. 또한 네트워크 오류 등 특수한 상황에서 재실 인원과 실제로 재실한 사용자의 수가 일치하지 않을 경우 관리자가 ＋ 또는 － 버튼을 클릭하거나 재실 인원을 클릭해 재실 인원을 직접 수정할 수도 있습니다.
- **항시 통과 인원**: 현재 입실 중인 항시 통과 인원에 속한 사용자의 수를 확인할 수 있습니다.
- **장치 상태**: 설정된 장치의 상태를 확인할 수 있습니다.

  - **정상**: 설정된 모든 장치의 네트워크가 정상적으로 동작하는 상태입니다.
  - **네트워크 오류**: 1대 이상의 장치에 네트워크 오류가 발생한 상태입니다.
- **전체 화면**: 재실 인원 제한 설정의 현황을 전체 화면으로 확인할 수 있습니다.

> **알아두기**
> **정원**을 설정한 경우 재실 인원은 최대 50,000까지의 숫자로 입력할 수 있습니다. **정원**을 설정하지 않은 경우 최대 999,999까지의 숫자로 입력할 수 있습니다. 최대 입력 값 이상의 숫자는 입력할 수 없으며, 실제 재실 인원 수가 최대 입력 값보다 많은 경우 초과한 값에 대해서는 데이터베이스에 저장되지 않습니다.

재실 인원 초기화하기

재실 인원 및 항시 통과 인원 수를 초기화할 수 있습니다. 재실 인원 초기화를 진행하면 사용자의 입실 및 퇴실 정보는 모두 삭제되며, 네트워크 연결 상태에 따라 재실 인원이 부정확해질 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. 목록에서 **재실 인원 제한**을 클릭하세요.
4. 재실 인원 제한 설정 목록 중 초기화할 설정의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단의 **재실 인원 초기화** 버튼을 클릭하세요.
6. 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

활성/비활성화

비활성화된 재실 인원 제한 설정을 활성화하거나 활성화된 설정을 비활성화할 수 있습니다. 설정을 비활성화하면 **재실 인원** 및 **항시 통과 인원**이 초기화됩니다.

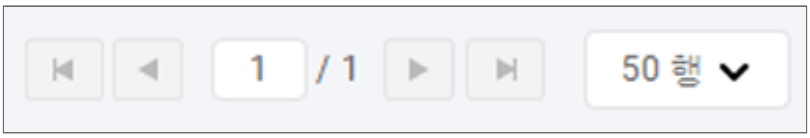
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. 목록에서 **재실 인원 제한**을 클릭하세요.
4. 재실 인원 제한 설정 목록 중 활성 또는 비활성화할 항목의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단의 **활성화** 또는 **비활성화** 버튼을 클릭하세요.

삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. 목록에서 **재실 인원 제한**을 클릭하세요.
4. 재실 인원 제한 설정 목록 중 삭제할 항목의 체크박스를 클릭하세요.
5. 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.
6. 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

목록 페이지 탐색

페이지를 이동하거나 한 페이지에 표시할 목록 개수를 설정할 수 있습니다. 화면 오른쪽 상단의 페이지 이동 도구를 사용하세요.



- ⏮: 첫 페이지로 이동합니다.
- ◀: 이전 페이지로 이동합니다.
- ▶: 다음 페이지로 이동합니다.
- ⏭: 마지막 페이지로 이동합니다.
- 원하는 페이지로 이동하려면 숫자 입력 필드에 페이지 번호를 입력하세요.
- 한 페이지에 표시할 목록 개수를 설정하려면 행 선택 상자를 클릭하세요.

인원 점검(Roll Call)

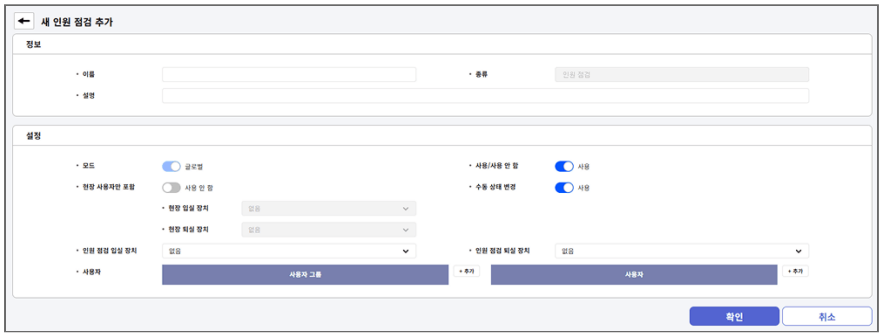
인원 점검(Roll Call)은 특정 시점과 장소 내 출입 기록을 기반으로 인원 목록을 신속하게 생성합니다. 위급 상황이 발생하면, 사용자가 미리 지정된 장소의 입실 또는 퇴실 장치를 통해 인증하여 인원 점검 장소에 도착했는지 파악할 수 있습니다.

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 점검 설정은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

인원 점검 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 관리** → **고급 출입 통제**를 클릭하세요.
3. **고급 출입 통제 추가** 버튼을 클릭하세요.
4. **인원 점검**을 선택하고 **확인** 버튼을 클릭하세요.
5. **정보** 섹션에서 추가할 인원 점검 설정의 이름과 설명을 입력하세요.



6. **설정** 섹션에서 세부 항목을 설정하세요. 자세한 내용은 설정 옵션 안내를 참고하세요.
7. 모든 설정을 완료했다면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> **이름**은 최대 48자까지 입력할 수 있으며, 다른 설정과 동일한 이름으로 설정할 수 없습니다.

설정 옵션 안내

인원 점검 설정을 위한 세부 항목은 아래와 같습니다.



- **모드**: 적용 범위를 확인할 수 있습니다. 인원 점검 설정은 **글로벌** 모드만 지원하며 **BioStar X**에 등록된 모든 장치로 설정할 수 있습니다.
- **사용/사용 안 함**: 설정을 활성화하거나 일시적으로 비활성화할 수 있습니다.
- **현장 사용자만 포함**: **사용**으로 설정하면 인원 점검을 시작하는 시점에 **현장 입실 장치에서 마지막으로 인증한 사용자**만 점검 대상자로 고정합니다. 기본값은 **사용 안 함**이며, 이 경우 설정된 전체 사용자(사용자 그룹 + 개별 사용자)가 점검 대상입니다.

  > 시스템은 각 사용자의 최근 7일 이내 현장 입실 또는 퇴실 장치 인증 기록으로 사용자가 현장에 있는지 판단합니다. 인원 점검 시작 시점 기준으로 가장 최근 인증이 현장 입실 장치에서 발생했다면 현장에 있는 것으로, 현장 퇴실 장치에서 발생했다면 현장을 벗어난 것으로 판단합니다. 최근 7일 이내에 인증 기록이 없는 사용자는 현장에 없는 것으로 간주되어 대상에서 제외됩니다.
  >
  > 대상자 목록은 인원 점검을 시작하는 시점에 한 번만 확정되며, 점검이 진행되는 동안 사용자가 현장에 입실하거나 퇴실해도 목록은 변경되지 않습니다.

  현장 사용자만 포함을 **사용**으로 설정했을 때 다음 옵션을 사용할 수 있습니다.

  - **현장 입실 장치**: 현장 입실 인증에 사용할 장치를 선택하세요.
  - **현장 퇴실 장치**: 현장 퇴실 인증에 사용할 장치를 선택하세요.
- **수동 상태 변경**: 수동으로 상태를 변경할 수 있도록 설정할 수 있습니다.
- **인원 점검 입실 장치**: 입실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **인원 점검 퇴실 장치**: 퇴실할 때 사용할 장치를 선택하세요. 등록된 장치 목록에서 선택할 수 있습니다.
- **사용자**: 입실할 수 있는 사용자 그룹 또는 개별 사용자를 선택할 수 있습니다.

> **알아두기**
>
> - 동일한 장치를 **인원 점검 입실 장치**와 **인원 점검 퇴실 장치**로 동시에 설정할 수 없습니다.
> - **인원 점검 입실 장치**와 **인원 점검 퇴실 장치**는 최대 10개까지 선택할 수 있습니다.
> - 장치 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
>   - 장치 등록하기
>   - Wiegand 장치 등록하기
>   - 슬레이브 장치 등록하기

목록 현황 확인

인원 점검 목록에서 각 설정의 세부 정보와 상태를 확인할 수 있습니다.

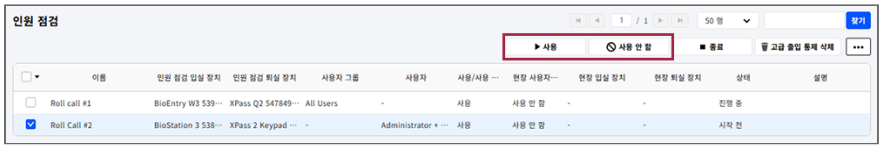


- **이름**: 이름을 확인할 수 있습니다.
- **인원 점검 입실 장치** / **인원 점검 퇴실 장치**: 설정된 장치를 확인할 수 있습니다.
- **사용자 그룹** / **사용자**: 설정된 대상자를 확인할 수 있습니다.
- **사용/사용 안 함**: 활성화 상태를 확인할 수 있습니다.
- **현장 사용자만 포함**: 사용 여부를 확인할 수 있습니다.
- **현장 입실 장치** / **현장 퇴실 장치**: 설정된 현장 입실 또는 퇴실 장치를 확인할 수 있습니다.
- **상태**: 인원 점검의 진행 상태(**시작 전**, **진행 중** 등)를 확인할 수 있습니다.
- **설명**: 등록된 설명을 확인할 수 있습니다.

활성/비활성화

비활성화된 인원 점검 설정을 활성화하거나 활성화된 설정을 비활성화할 수 있습니다.

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 설정 목록 중 활성 또는 비활성화할 항목의 체크박스를 클릭하세요.

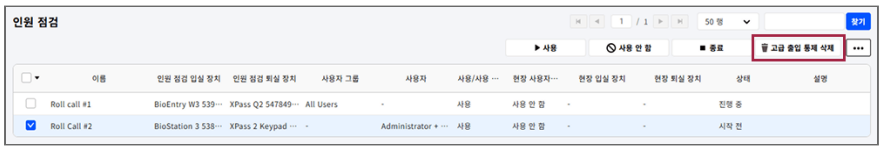


5. 화면 오른쪽 상단의 **사용** 또는 **사용 안 함** 버튼을 클릭하세요.

> **알아두기**
>
> - **사용 안 함**을 선택하면 확인 메시지가 나타납니다. **네** 또는 **아니요**를 선택하세요.
> - 진행 중인 인원 점검은 비활성화할 수 없습니다. 확인 후 다시 시도하세요.

삭제

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 설정 목록 중 삭제할 항목의 체크박스를 클릭하세요.

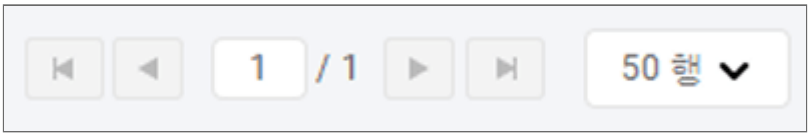


5. 화면 오른쪽 상단의 **고급 출입 통제 삭제** 버튼을 클릭하세요.
6. 경고 메시지가 나타나면 **계속** 버튼을 클릭하세요.

> **알아두기**
>
> 진행 중인 인원 점검은 삭제할 수 없습니다. 인원 점검을 종료 후 다시 시도하세요.

목록 페이지 탐색

페이지를 이동하거나 한 페이지에 표시할 목록 개수를 설정할 수 있습니다. 화면 오른쪽 상단의 페이지 이동 도구를 사용하세요.



- ⏮: 첫 페이지로 이동합니다.
- ◀: 이전 페이지로 이동합니다.
- ▶: 다음 페이지로 이동합니다.
- ⏭: 마지막 페이지로 이동합니다.
- 원하는 페이지로 이동하려면 숫자 입력 필드에 페이지 번호를 입력하세요.
- 한 페이지에 표시할 목록 개수를 설정하려면 행 선택 상자를 클릭하세요.

모바일 앱에서 인원 점검 사용

인원 점검 기능은 BioStar X 모바일 앱에서 사용할 수 있습니다.

알아두기

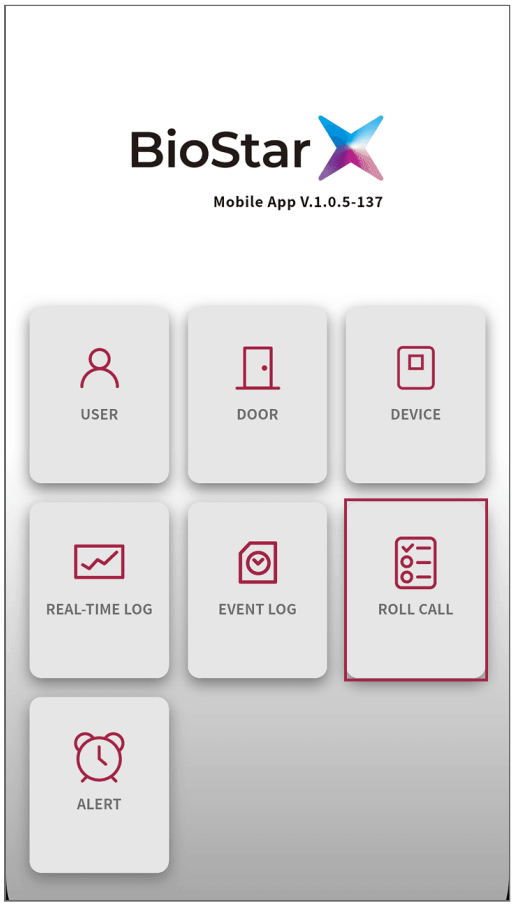
BioStar X 모바일 앱은 다음 링크를 통해 설치할 수 있습니다.

- iOS: Apple App Store
- 안드로이드: Google Play'

인원 점검 시작

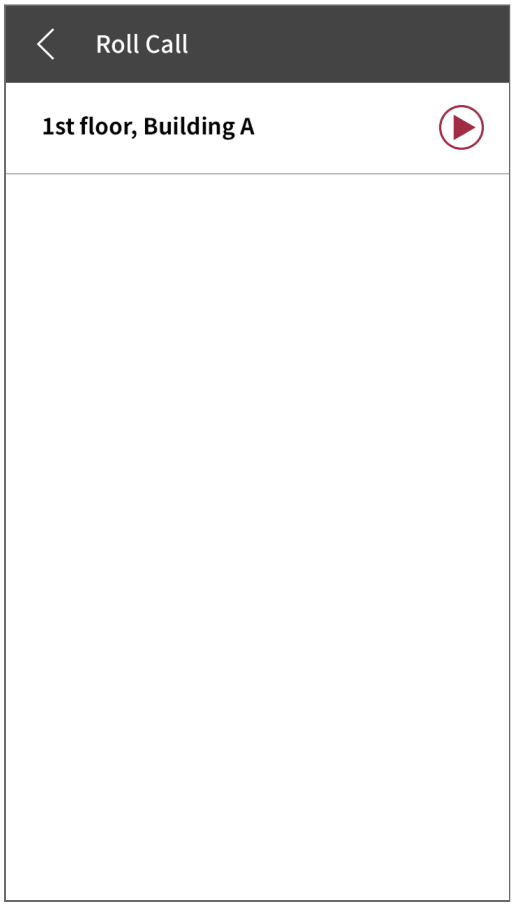
모바일 앱에서 인원 점검 기능을 시작하려면 다음 단계를 따르세요.

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



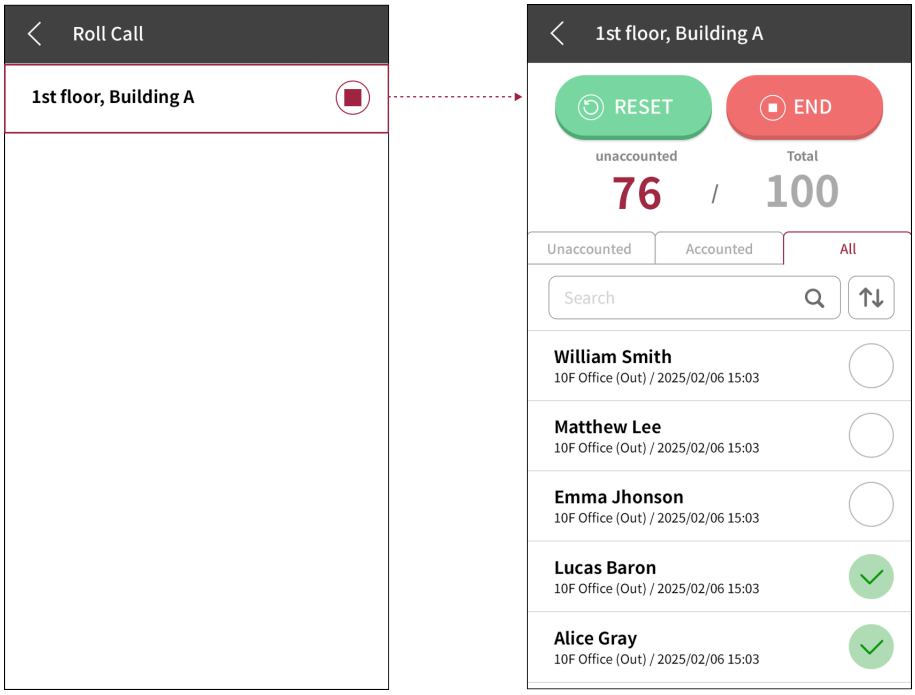
사이드 메뉴를 통해 진입할 수도 있습니다. ☰ → **Monitoring** → **Roll Call**을 탭하세요.

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.



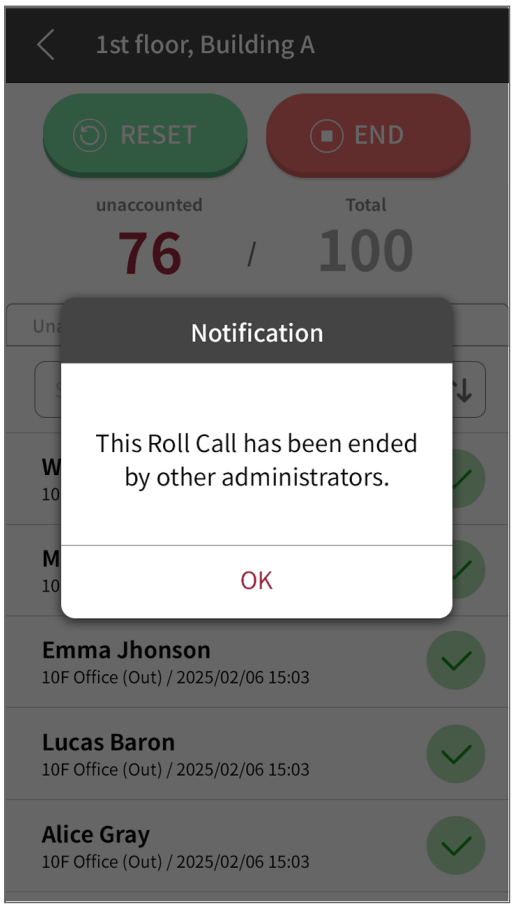
진행 중인 인원 점검 제어

- 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.

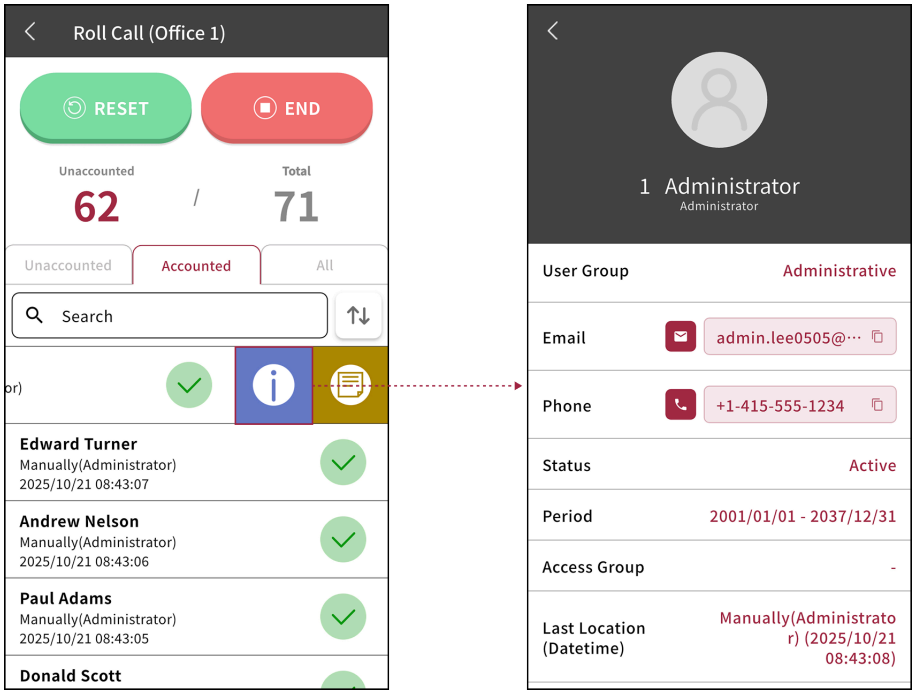


- 인원 점검을 완료한 후 **데이터** → **리포트 생성** → **인원 점검**에서 관련 보고서를 확인할 수 있습니다. 자세한 내용은 인원 점검 보고서 확인을 참고하세요.

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.

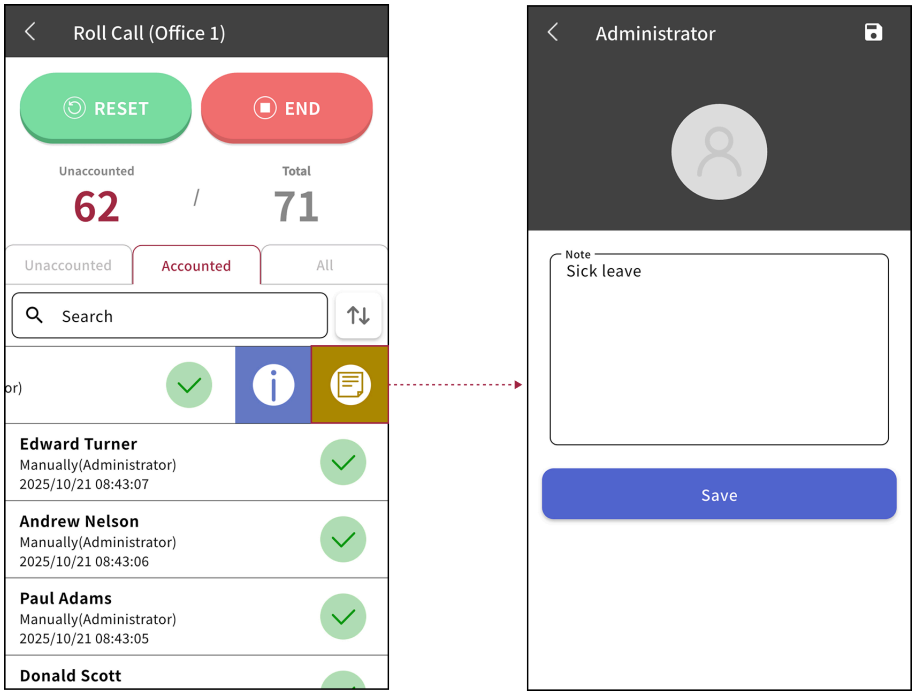
인원 점검 진행 중 세부 정보를 확인할 사용자 항목을 왼쪽으로 스와이프하세요. 이후 ⓘ을 탭하세요.



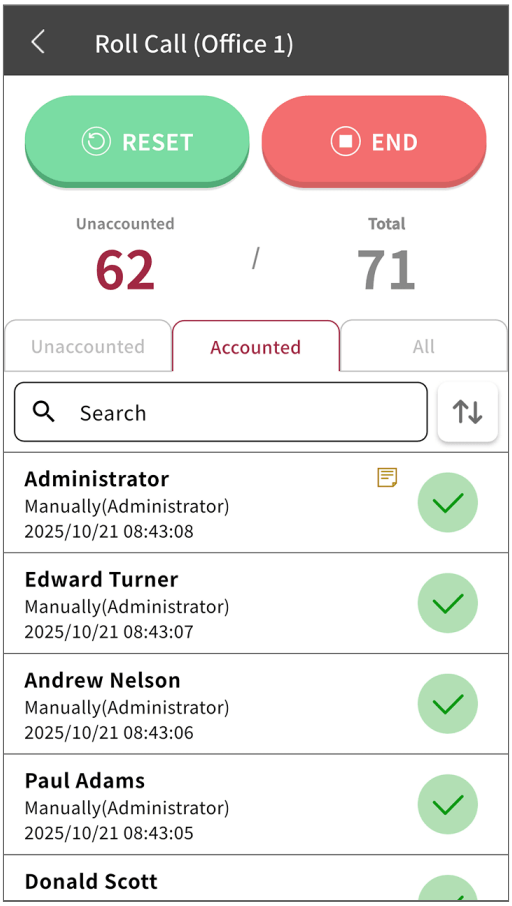
인원 점검 진행 중 사용자에게 메모 남기기

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.



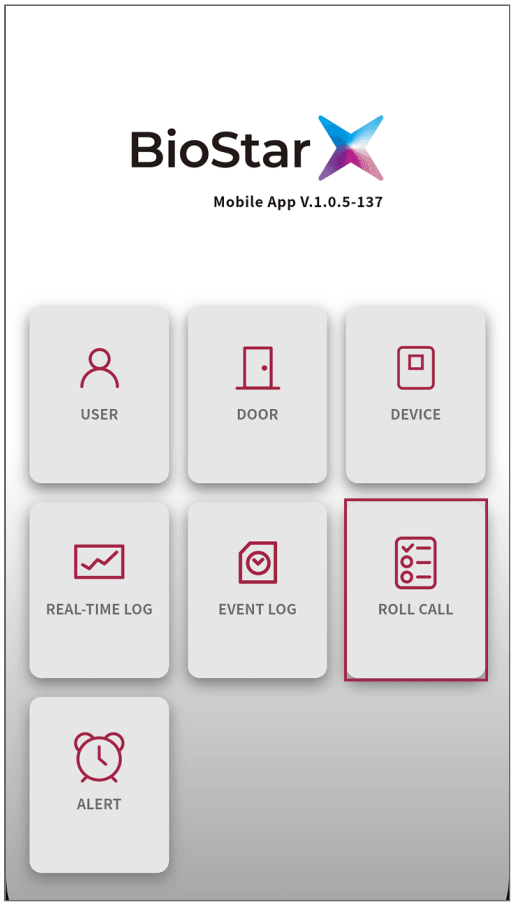
메모를 입력한 사용자는 인원 점검 목록에서 아이콘이 표시됩니다.



인원 점검 세부 정보 확인

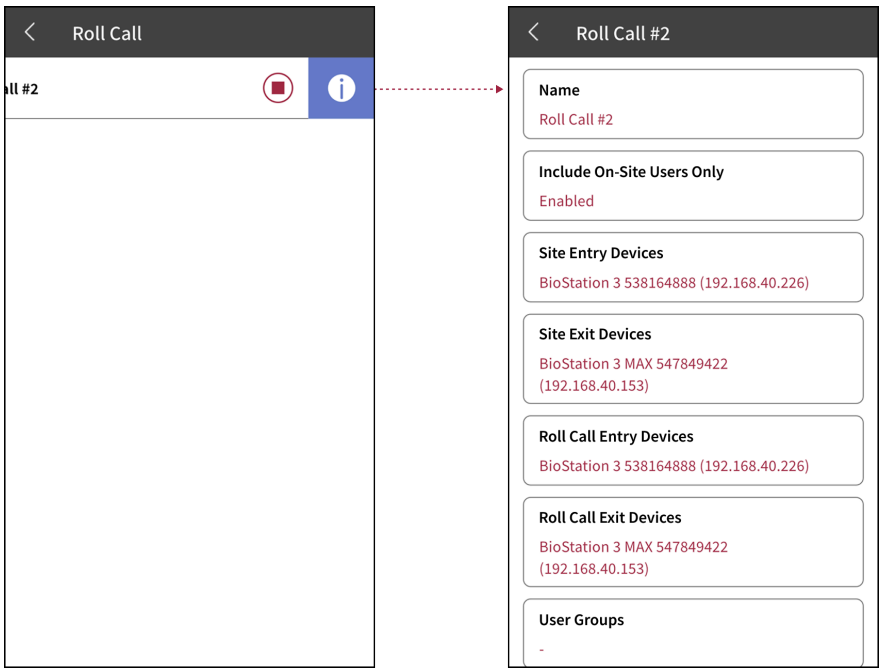
모바일 앱에서 인원 점검 설정의 세부 정보를 확인할 수 있습니다.

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.

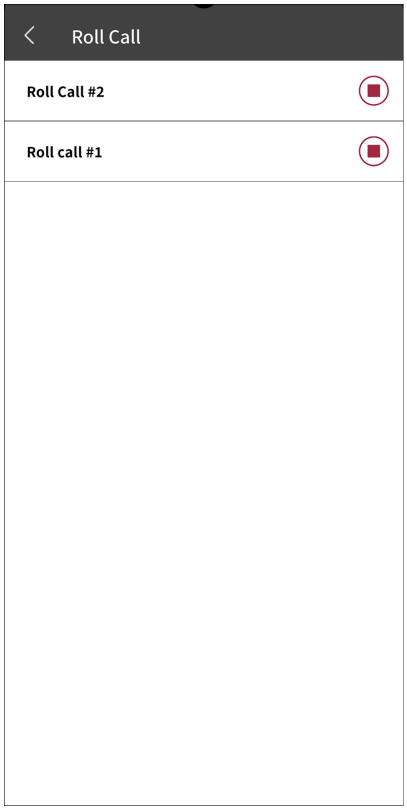


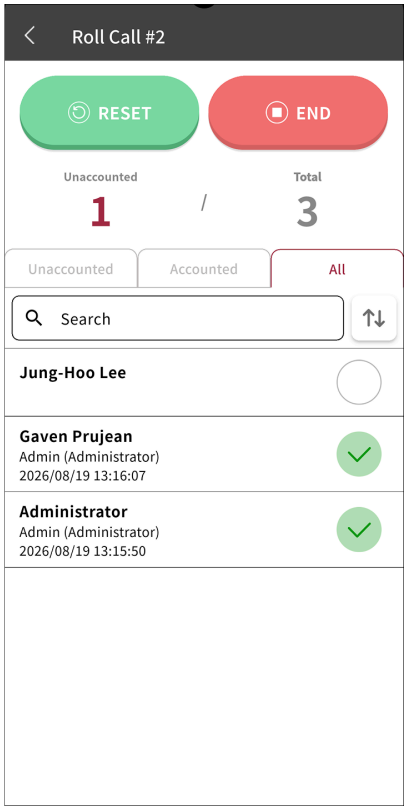
인원 점검 종료

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

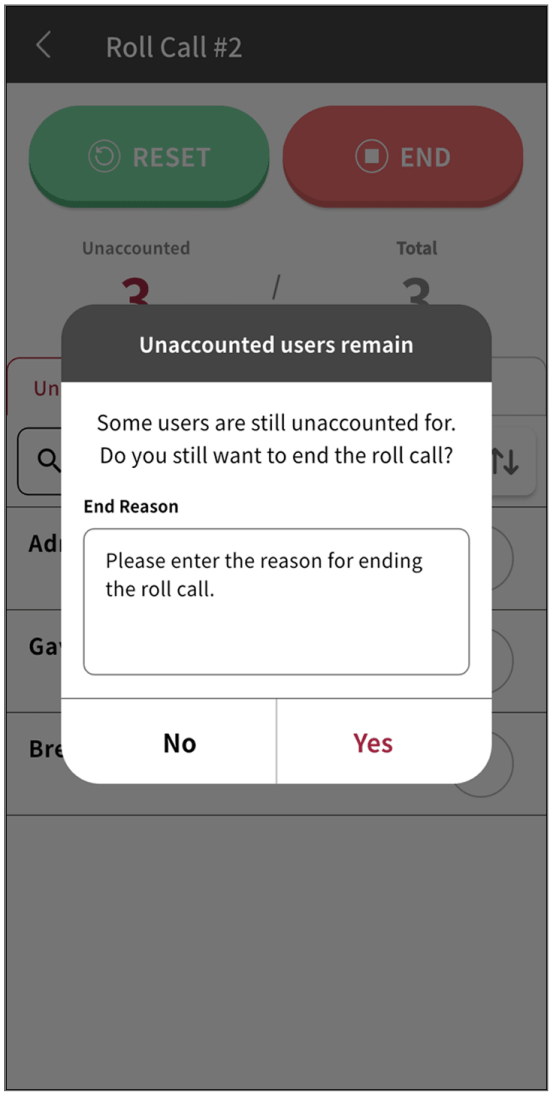
모바일 앱에서 종료

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.

인원 점검 보고서 확인

인원 점검 보고서를 확인하려면 다음 단계를 따르세요.

1. **런처** 페이지에서 **데이터**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **이벤트** → **인원 점검**을 클릭하세요.
3. **인원 점검 선택** 창이 나타나면 보고서로 확인할 인원 점검 항목을 선택한 후 **다음** 버튼을 클릭하세요.



> 원하는 인원 점검 항목이 보이지 않는다면 화면 상단의 기간을 조정해보세요.

4. 옵션 설정 창에서 보고서에 포함할 데이터를 선택한 후 **생성** 버튼을 클릭하세요.

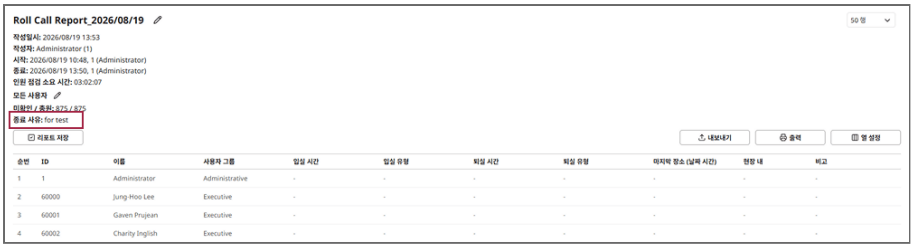


보고서를 생성합니다. 보고서에서는 각 사용자의 정보 및 입실 시간, 퇴실 시간, 마지막 장소, 메모 내용 등을 확인할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

미확인 사용자가 남아 있는 인원 점검 보고서는 **종료 사유**를 확인할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

비디오 설정하기

BioStar X의 비디오 설정 기능을 통해 출입 통제와 영상 보안을 통합 관리할 수 있습니다. **Video Management System**(VMS)과 연동하여 실시간 영상 모니터링, 이벤트 연계 녹화, 자동 북마크 생성 등 강력한 보안 관리 기능을 활용하세요.

> **알아두기**
> 비디오 설정 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

비디오 설정 개요

비디오 설정은 다음 3단계로 구성됩니다.

1 VMS 서버 연동하기

VMS 서버와 **BioStar X** 간의 연결을 설정하고 인증서를 구성합니다. 통합 영상 보안 관리 시스템을 구축하는 필수 단계입니다. 자세한 내용은 VMS 연동하기를 참고하세요.

2 카메라 설정하기

VMS에 연결된 카메라 중 필요한 카메라를 선택하고, 효율적인 관리를 위한 그룹을 구성하세요. 자세한 내용은 카메라 설정하기를 참고하세요.

3 규칙 설정하기

출입 이벤트와 영상을 연계하는 규칙을 생성하여 자동 북마크, 이벤트 기록 등의 고급 기능을 활용합니다. 자세한 내용은 비디오 규칙 설정하기를 참고하세요.

주요 기능

- **통합 모니터링**: 출입 통제와 영상 보안을 하나의 인터페이스에서 관리할 수 있습니다.
- **자동 이벤트 기록**: 출입 이벤트 발생 시 관련 영상을 자동으로 기록하고 태그를 생성합니다.
- **효율적인 검색**: 북마크와 이벤트 태그를 통한 빠른 영상 검색 및 증거 수집이 가능합니다.
- **실시간 대응**: 보안 상황 발생 시 즉시 관련 카메라 영상 확인할 수 있습니다.

VMS 연동하기

Video Management System(VMS)는 여러 카메라의 영상을 통합 관리하고 녹화, 재생할 수 있는 영상 관리 시스템입니다. BioStar X와 VMS를 연동하면 출입 통제와 영상 보안을 하나의 플랫폼에서 통합 관리할 수 있습니다.

VMS 연동 시 다음과 같은 기능을 사용할 수 있습니다.

- **실시간 모니터링**: 출입문과 연결된 카메라의 실시간 영상을 확인할 수 있습니다.
- **통합 이벤트 관리**: 출입 이벤트와 영상을 연계하여 보안 상황을 파악할 수 있습니다.
- **효율적인 증거 수집**: 특정 시점의 녹화 영상을 빠르게 검색하고 재생할 수 있습니다.
- **북마크 기능**: 중요한 이벤트 시점에 영상 태그를 추가하여 쉽게 찾고 검토할 수 있습니다.

시작하기 전에

Video Management System(VMS)과 연동하려면 다음 사항을 확인하세요.

- VMS 연동 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- VMS 서버가 올바르게 설치되고 구성되었는지 확인하세요. VMS 서버는 **BioStar X**와 온라인으로 연결 가능한 상태여야 합니다.

- **BioStar X**와 호환되는 VMS를 사용하세요. BioStar X VMS 또는 **Nx Witness v5.1.5, v6.x.x** 계열의 VMS를 사용할 수 있습니다.
- VMS 서버의 IP 주소, 포트 번호, 관리자 계정 정보를 준비하세요. 이 정보는 **BioStar X**에서 VMS 서버에 연결하는 데 필요합니다.

VMS 서버 연동 설정

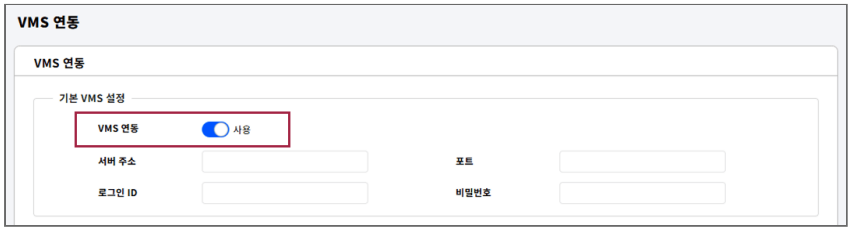
VMS 서버와 **BioStar X**를 연동하려면 다음 단계를 따르세요.

1 VMS 연동 활성화

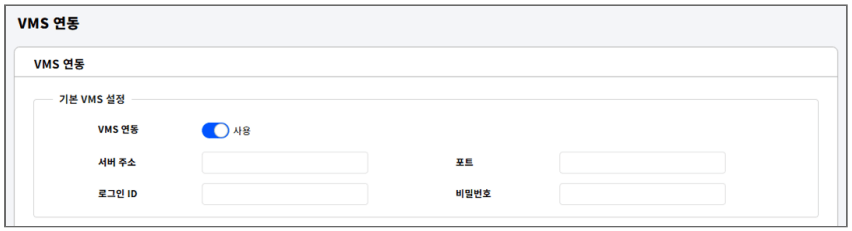
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **VMS 연동**을 클릭하세요.
3. 처음 접속한다면 **BioStar X** 관리자 계정으로 로그인해야 합니다.



4. **VMS 연동** 옵션을 **사용**으로 설정하세요.



5. VMS 서버 정보를 입력하세요.



- **서버 주소**: VMS 서버의 IP 주소를 입력하세요.
- **포트**: VMS 서버의 포트 번호를 입력하세요.
- **로그인 ID**: VMS 서버의 관리자 계정 아이디를 입력하세요.
- **비밀번호**: VMS 서버의 관리자 계정 비밀번호를 입력하세요.

6. VMS 서버 정보를 모두 입력했으면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - VMS 서버와 연동에 실패해 오류 메시지가 나타나면 서버 주소 및 관리자 계정 정보 등을 다시 확인하세요. VMS 서버가 온라인 상태인지, 방화벽 설정으로 인해 네트워크 연결이 차단되지 않았는지 점검하는 것도 필요합니다.
> - **VMS 이벤트/북마크** 섹션의 설정에 대한 자세한 내용은 VMS 이벤트 및 북마크 설정을 참고하세요.

2 VMS 서버에 인증서 설치

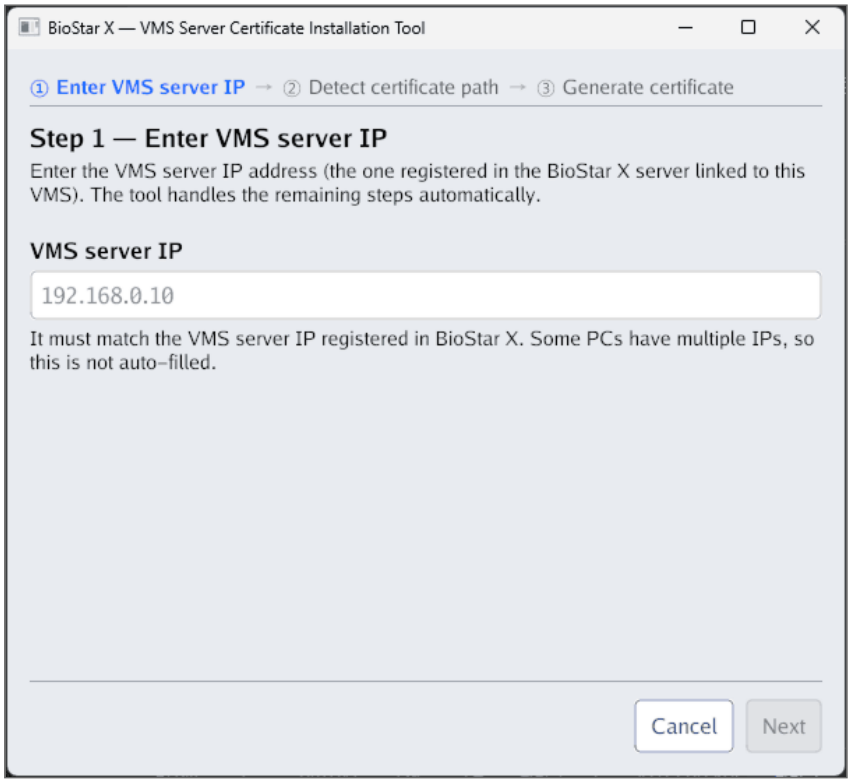
VMS 서버의 녹화된 영상을 재생하려면 HTTPS 프로토콜을 사용해야 합니다. 일반적인 SSL 인증서는 도메인 이름 기반으로 발급되므로, IP 주소로 VMS 서버에 접근하는 환경에서는 유효하지 않습니다. 따라서 VMS 서버의 IP 주소를 포함한 인증서를 별도로 생성해야 합니다.

> **알아두기**
>
> VMS 서버와 **BioStar X**를 같은 서버에 설치하거나 서로 다른 서버에 설치하는 경우 모두 인증서를 설치해야 합니다.

VMS 연동 옵션을 **사용**으로 설정하면 **NX Witness 인증서 설정** 섹션이 활성화됩니다.

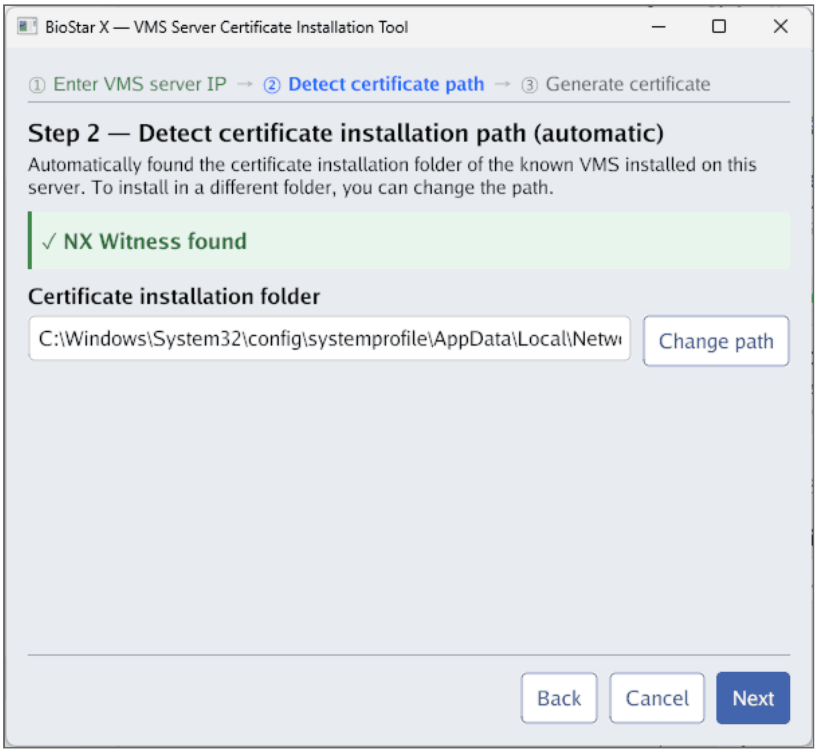


1. 인증서 설치 프로그램을 다운로드하려면 VMS가 설치된 서버에서 **인증서 설치 프로그램 다운로드** 버튼을 클릭하세요.
2. 다운로드한 *vmsCertMaker.exe* 파일을 실행하세요.
3. **VMS server IP** 입력 필드에 IP 주소를 입력하세요.

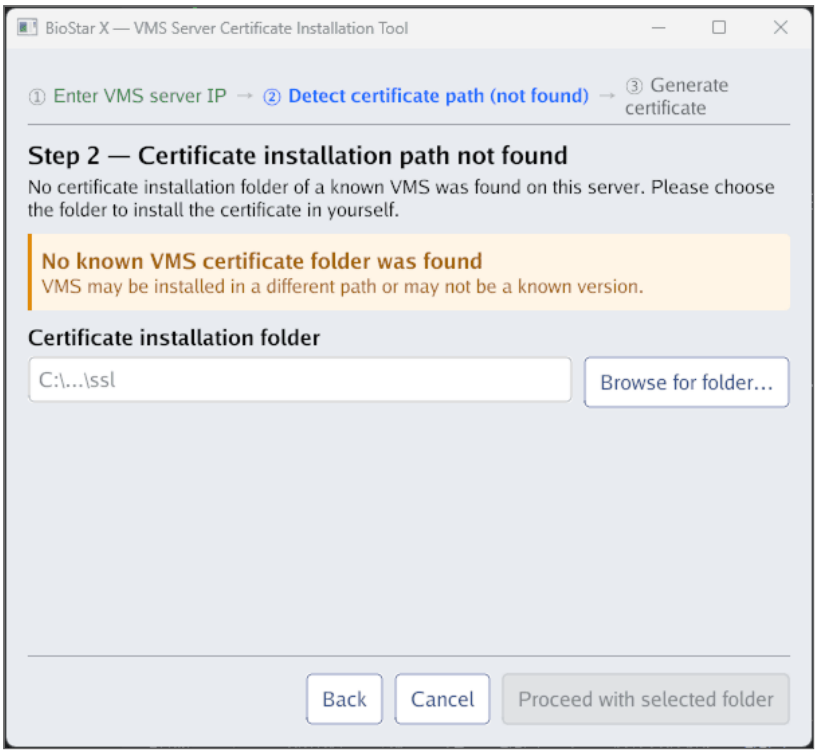


> IPv4 주소 형식으로 입력해야 합니다. 예: 192.168.0.10

4. 올바른 형식의 IP 주소를 입력하면 **Next** 버튼이 활성화됩니다. **Next** 버튼을 클릭하세요.
5. VMS의 인증서 설치 경로를 선택하세요.
   - 호환되는 VMS의 경우 자동으로 설치 경로를 인식합니다.

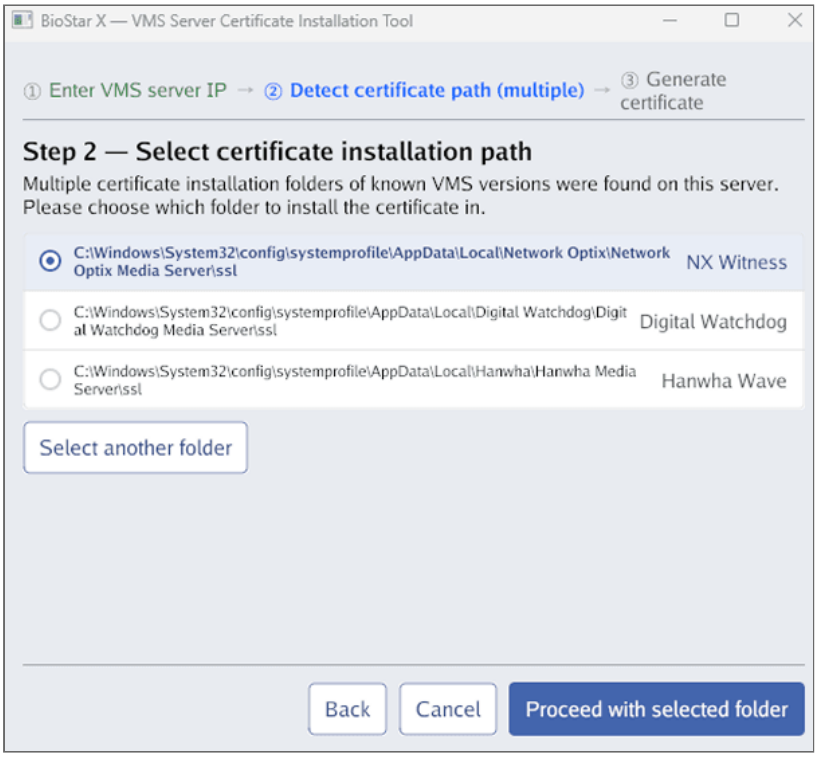


- 설치 경로가 자동 인식되지 않는다면 **Browse for folder** 버튼을 클릭하고, 인증서 설치 경로를 직접 선택하세요.

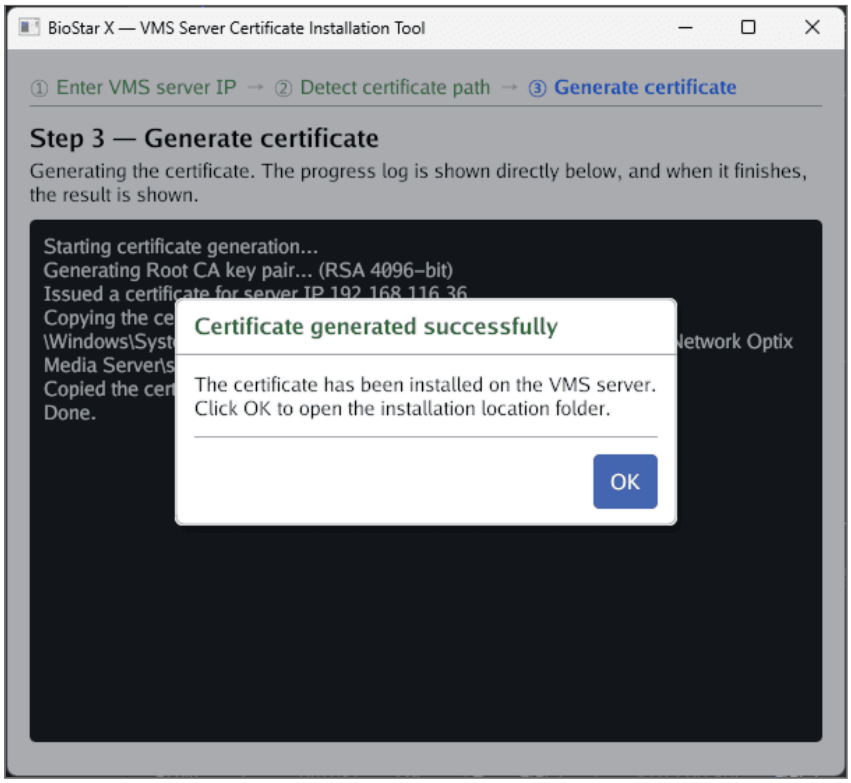


> VMS에 따라 인증서 설치 경로가 다를 수 있습니다. 아래 예시를 참고하세요.
> - **BioStar 2 VMS**: *C:\Windows\System32\config\systemprofile\AppData\Local\Suprema Inc\Suprema Inc. Media Server\ssl*
> - **Digital Watchdog**: *C:\Windows\System32\config\systemprofile\AppData\Local\Digital Watchdog\Digital Watchdog Media Server\ssl*
> - **Hanwha Wave**: *C:\Windows\System32\config\systemprofile\AppData\Local\Hanwha\Hanwha Media Server\ssl*
> - **NX**: *C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\ssl*

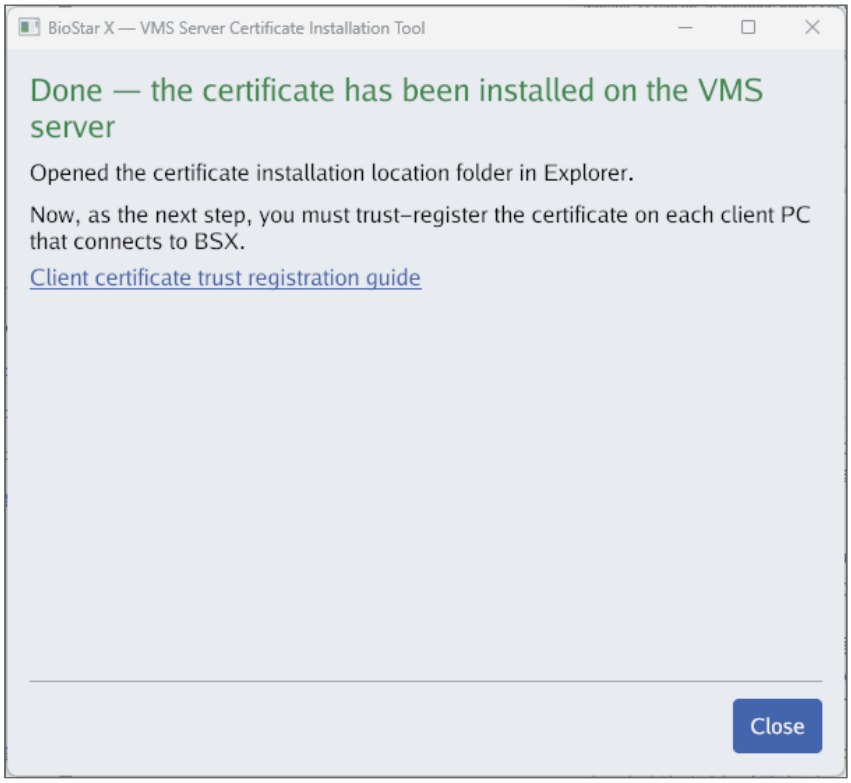
- 여러 개의 VMS 인증서 경로가 있다면 모든 경로가 표시됩니다. **Select another folder** 버튼을 클릭하고 원하는 경로를 선택하세요.



6. **Next** 또는 **Proceed with selected folder** 버튼을 클릭하세요.
7. 인증서 생성을 완료하면 **Certificate generated successfully** 메시지 창이 나타납니다.



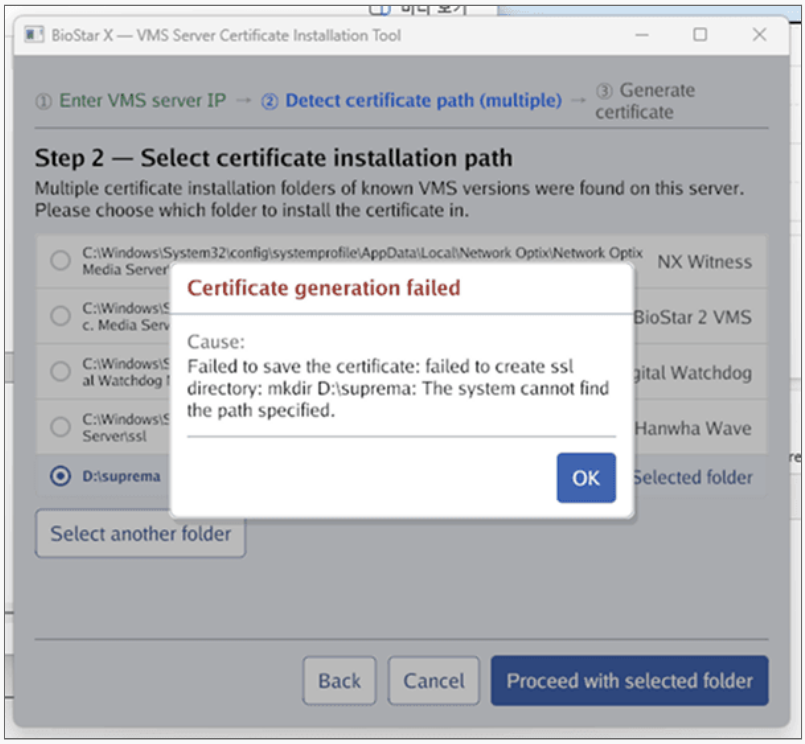
8. **OK** 버튼을 클릭하면 인증서를 설치한 경로가 나타납니다. 인증서 파일(*cert.pem*)이 생성되었는지 확인하세요.
9. 인증서 설치를 완료하면 **Close** 버튼을 클릭하세요.



10. VMS 서버를 재부팅하세요.

알아두기

인증서 설치에 실패하면 실패 사유가 메시지에 출력됩니다. 메시지 내용을 확인한 후 필요한 조치를 취하세요.



3 클라이언트 PC에서 인증서 설치

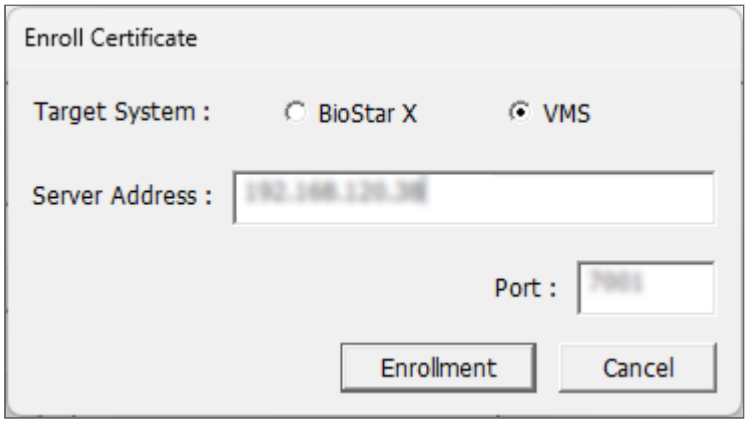
아래와 같은 상황이 발생한다면 VMS 서버에 설치된 인증서를 클라이언트 PC에 설치해 문제를 해결할 수 있습니다.

- **Video Management System**(VMS)을 브라우저를 통해서 접속했을 때 '안전하지 않음' 경고가 표시될 때
- **모니터링** 페이지에서 실시간 영상은 재생되나 녹화 영상이 재생되지 않을 때

> **주의**
> VMS 서버에 인증서를 설치하지 않고 클라이언트 PC에만 등록하면 정상 작동하지 않습니다.

---

1. 웹 브라우저를 통해 **BioStar X**로 접속하세요.
2. 로그인 화면 또는 **설정** → **시스템** → **HTTPS**에서 HTTPS 인증서 설치 프로그램(*cert-register.zip*)을 다운로드하세요.
3. 다운로드한 파일의 압축을 해제한 뒤 **cert-register.exe** 파일을 실행하세요. **Enroll Certificate** 창이 나타납니다.
4. **Target System**을 **VMS**로 선택하고 다음 정보를 입력하세요.



   - **Server Address**: VMS 서버의 IP 주소
   - **Port**: VMS 서버의 포트 번호(기본값: 7001)
5. **Enrollment** 버튼을 클릭하세요.
6. 보안 경고 메시지를 확인한 뒤 **예**를 클릭하세요.

웹 브라우저를 다시 시작한 뒤 **모니터링** 페이지에서 VMS 서버의 녹화 영상이 정상 재생되는지 확인하세요.

4 카메라 확인 및 설정

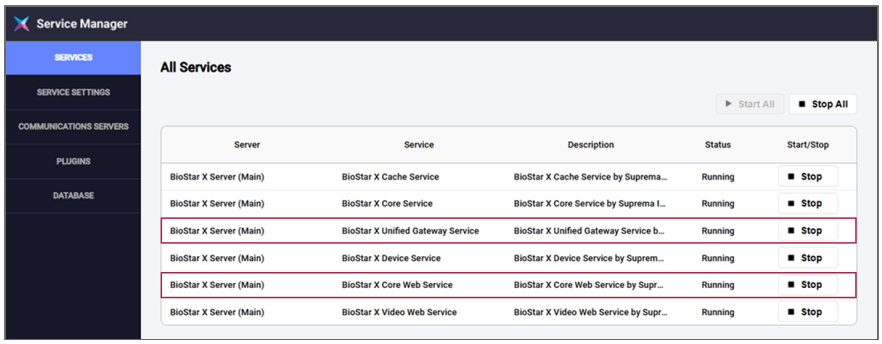
VMS 서버와 정상 연동되었다면 **비디오** → **비디오** 메뉴에서 연결된 카메라를 확인할 수 있습니다. 자세한 내용은 카메라 설정하기를 참고하세요.

문제 해결

VMS 서버와 처음 연동 후 정상 작동하지 않는다면, 다음 안내에 따라 수동으로 서비스를 재시작하세요.

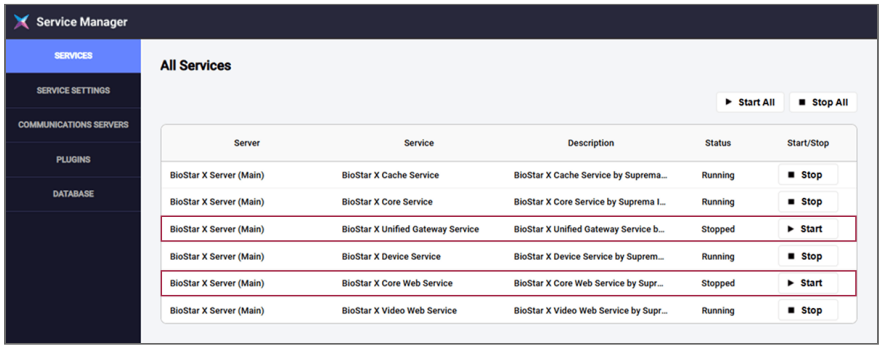
1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.

2. **All Services** 목록에서 아래 서비스의 **Stop** 버튼을 클릭해 서비스를 중지하세요.



- **BioStar X Unified Gateway Service**
- **BioStar X Core Web Service**

3. 중지 요청한 서비스의 상태가 **Pending**에서 **Stopped**로 변경되면 **Start** 버튼을 클릭해 서비스를 재시작하세요.



VMS 이벤트 및 북마크 설정

연동한 VMS 서버에 북마크 태그, 이벤트 태그 정보를 전달할 수 있습니다. 이때, 이벤트 로그, 출입문 이름, 장치 이름, 사용자 아이디를 함께 전달할 수 있도록 선택할 수 있습니다. 원하는 옵션을 선택하고 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.



- **언어**: VMS 서버에 전달하는 이벤트 및 북마크 태그의 언어를 선택하세요. 한국어 또는 영어를 선택할 수 있습니다.
- **북마크 태그**: 북마크 태그는 VMS 서버에 보관된 영상에 표시와 이름이 지정되어 쉽게 찾고 검토할 수 있는 기능입니다. 북마크 태그로 전송할 정보를 선택하세요.
- **이벤트 태그**: 특정 시점에 발생한 이벤트를 VMS 서버로 전송해 기록할 수 있습니다. 이벤트 태그로 전송할 정보를 선택하세요.

알아두기

- VMS에서 북마크 기능에 자세한 내용은 다음 링크를 참고하세요.
- VMS에서 이벤트 기능에 대한 자세한 내용은 다음 링크를 참고하세요.
- 북마크 태그와 이벤트 태그에 다음 문자가 포함되어 있으면 VMS 서버로 전달할 때 자동 제거됩니다.
  - 이벤트 태그: `\` `'` `,` `#` `%` `=` `&` `<` `>`
  - 북마크 태그: `<` `'`

VMS 서버 연동 해제

연동한 VMS 서버의 연결을 해제하려면 다음 단계를 따르세요. VMS 연동을 해제하면 비디오 설정, 등록한 카메라, 규칙이 모두 삭제됩니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **VMS 연동**을 클릭하세요.
3. **VMS 연동** 옵션을 **사용 안 함**으로 설정하세요.
4. 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.
5. 메시지 창의 내용을 확인하고 **네** 버튼을 클릭하세요.

카메라 설정하기

VMS 연동을 완료한 후에는 BioStar X에서 사용할 카메라를 선택하고 설정해야 합니다. 적절한 카메라 설정을 통해 다음과 같은 보안 관리 기능을 활용할 수 있습니다.

- **선택적 모니터링**: VMS의 모든 카메라 중 필요한 카메라만 **BioStar X**에 추가할 수 있습니다.
- **효율적인 관리**: 카메라를 그룹별로 구성하여 위치나 용도에 따른 체계적으로 관리할 수 있습니다.

알아두기

- VMS 서버와 연동하는 방법은 VMS 연동하기를 참고하세요.
- 카메라를 추가하거나 그룹을 구성하려면 카메라 그룹 권한이 필요합니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 그룹 권한 설정을 참고하세요.

카메라 설정 및 관리

VMS 연동 후 **설정** → **비디오** → **비디오** 메뉴에서 카메라를 설정하고 관리할 수 있습니다.

카메라 추가

VMS와 연동되어 있다면 VMS 서버에 연결된 카메라를 **BioStar X**에 추가하고 **모니터링** 페이지에서 실시간 영상 및 녹화 영상을 재생할 수 있습니다.

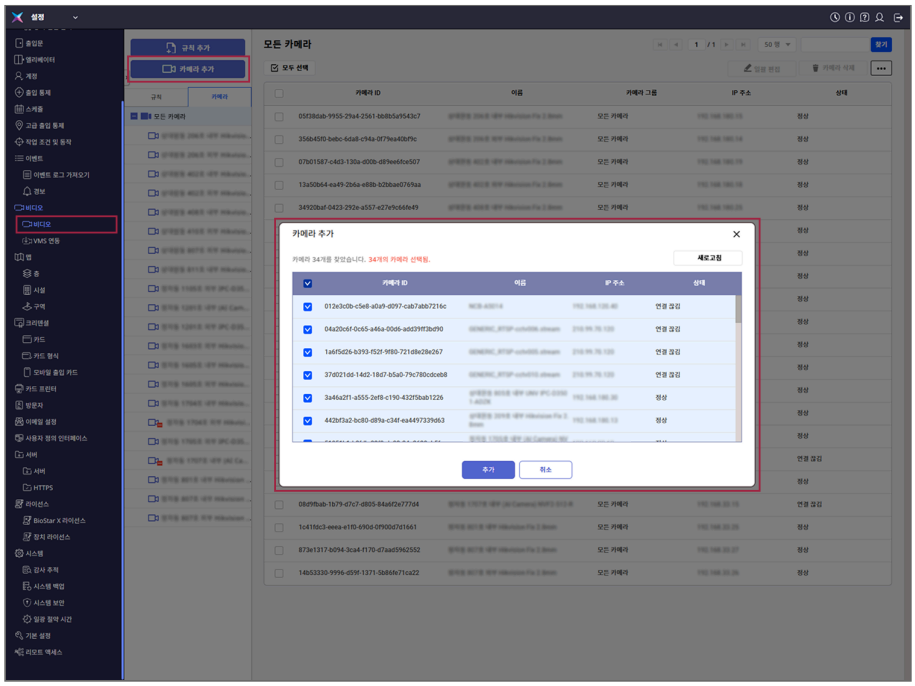
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **카메라 추가** 버튼을 클릭하세요.

4. **카메라 추가** 창이 나타나면 카메라 목록에서 제외할 카메라를 선택하세요.

   원하는 카메라가 표시되지 않는다면 **새로고침** 버튼을 클릭해 카메라 목록을 새로고침하세요.

5. 카메라를 모두 선택했으면 화면 오른쪽 하단의 **추가** 버튼을 클릭하세요.

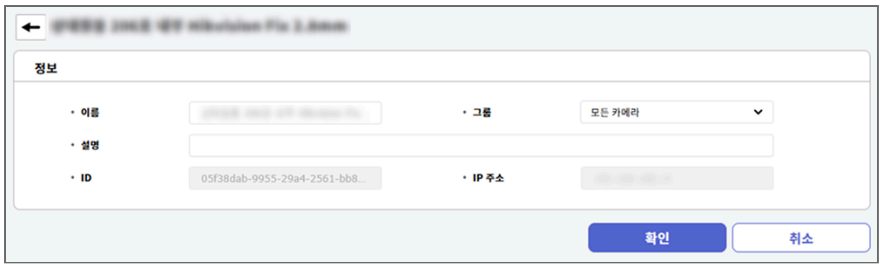
카메라 목록에서 추가한 카메라를 확인할 수 있습니다.



카메라 정보 수정

추가한 카메라의 정보를 수정할 수 있습니다. 카메라 이름 및 그룹, 설명 등을 변경할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. 화면 왼쪽 상단의 **카메라** 탭을 클릭하세요.
4. 카메라 목록에서 정보를 수정할 카메라를 클릭하세요.
5. 카메라 정보가 표시된 화면이 나타나면 원하는 항목을 수정하세요.



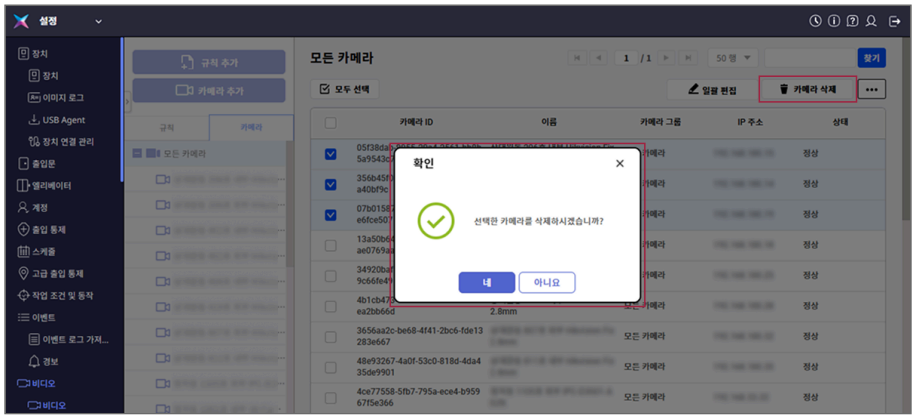
6. 카메라 정보를 모두 수정했으면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
> 카메라 아이디와 IP 주소는 수정할 수 없습니다.

카메라 삭제

추가한 카메라를 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. 카메라 목록에서 삭제할 카메라의 가장 왼쪽에 체크박스를 클릭하세요. 1대 이상의 카메라를 선택할 수 있습니다.
4. 화면 오른쪽 상단의 **카메라 삭제** 버튼을 클릭하세요.
5. 메시지를 확인하고 **네** 버튼을 클릭하세요.



> **알아두기**
>
> 삭제하려는 카메라가 하나의 규칙에 포함되어 있다면 카메라를 삭제할 수 없습니다. 해당 카메라를 규칙에서 제거한 후 다시 시도하세요. 규칙 생성 및 관리에 대한 자세한 내용은 비디오 규칙 설정하기를 참고하세요.

카메라 그룹 설정 및 관리

여러 대의 카메라를 그룹으로 묶어 위치나 용도에 따라 체계적으로 관리할 수 있습니다. 카메라 그룹을 생성하고 관리하기 위한 절차는 아래와 같습니다.

카메라 그룹 권한 설정

관리자가 카메라를 추가하거나 그룹을 구성하려면 카메라 그룹 권한이 필요합니다. 전체 관리자 및 사용자 관리자, 모니터링 관리자는 모든 카메라 그룹에 대한 권한을 가지고 있습니다. 별도의 권한 설정이 필요한 경우 커스텀 권한을 추가하여 카메라 그룹 권한을 설정할 수 있습니다.

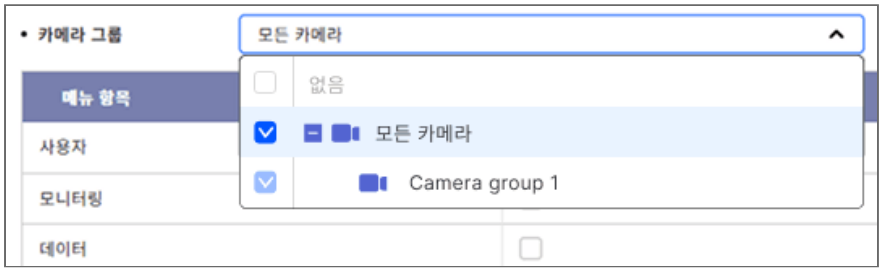
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요.
3. **커스텀 권한 추가** 버튼을 클릭하세요.



4. 새로 생성하는 권한에 대한 이름과 설명을 입력하세요.



5. **아이템 상세 권한**의 **카메라 그룹** 항목에서 권한을 할당할 카메라 그룹을 선택하세요.



- 모든 카메라 그룹에 대한 권한을 부여하려면 **모든 카메라**를 선택하세요.
- 개별 카메라 그룹에 대한 권한을 부여하려면 카메라 그룹 목록에 표시된 그룹 중 원하는 그룹을 선택하세요. 한 개 이상의 그룹을 선택할 수 있습니다.

6. **권한 부여**에서 **+ 추가** 버튼을 클릭하고 권한을 부여할 사용자를 선택하세요.
7. 설정을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

> **알아두기**
> 특정 카메라 그룹에 대한 권한이 없다면 해당 그룹에 속한 카메라를 볼 수 없습니다.

카메라 그룹 추가

카메라 그룹을 추가해 여러 대의 카메라를 그룹으로 묶어 관리할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. 화면 왼쪽 상단의 **카메라** 탭을 클릭하세요.
4. **모든 카메라** 항목을 선택하고 마우스 오른쪽 버튼을 클릭하세요.



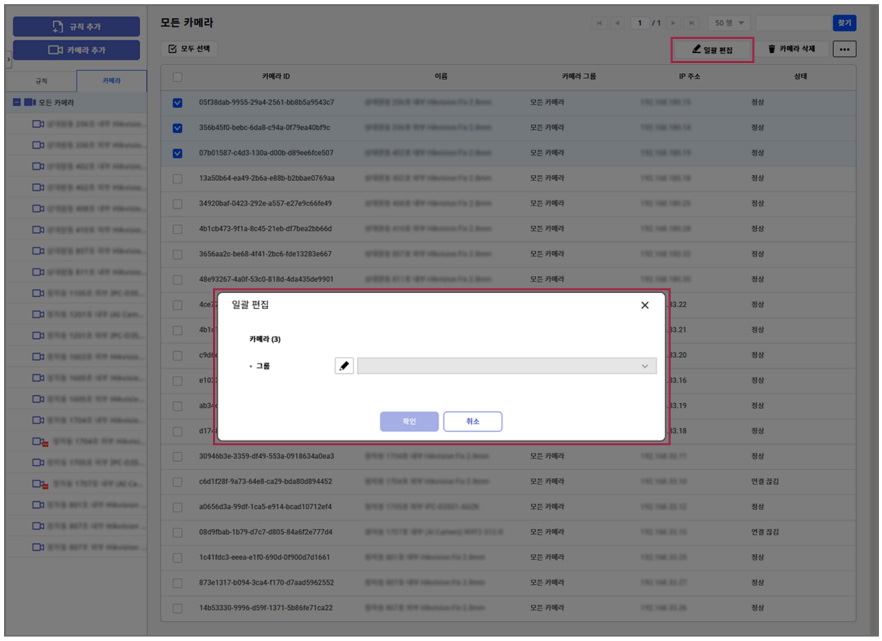
5. 팝업 메뉴에서 **카메라 그룹 추가**를 클릭하세요.
6. 원하는 그룹 이름을 입력하고 `Enter` 키를 누르세요.

> **알아두기**
>
> - 카메라 그룹은 8단계의 하위 그룹까지 생성할 수 있습니다.
> - 카메라 그룹 이름은 최대 48자까지 입력할 수 있습니다.
> - 카메라 목록에서 카메라 그룹을 선택하면 해당 그룹에 속한 카메라만 목록에 표시됩니다.

그룹에 여러 대의 카메라 추가

추가한 그룹에 1대 이상의 카메라를 추가할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. 카메라 목록에서 그룹에 추가할 카메라의 가장 왼쪽에 체크박스를 클릭하세요. 1대 이상의 카메라를 선택할 수 있습니다.
4. 1대 이상의 카메라를 선택하면 화면 오른쪽 상단의 **일괄 편집** 버튼이 활성화됩니다. **일괄 편집** 버튼을 클릭하세요.



5. **일괄 편집** 창이 나타나면 **그룹** 항목의 ✎ 버튼을 클릭하세요.
6. 그룹 목록에서 원하는 그룹을 선택하세요.
7. **확인** 버튼을 클릭하세요.

> **알아두기**
> **카메라** 탭의 카메라 목록에서 원하는 항목을 선택하고 드래그 앤 드롭으로도 카메라를 그룹에 추가할 수 있습니다.



카메라 그룹 이름 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **카메라** 탭을 클릭하세요.
4. 이름을 변경할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.
5. 팝업 메뉴에서 **카메라 그룹 이름 변경**을 클릭하세요.



6. 원하는 그룹 이름을 입력하고 `Enter` 키를 누르세요.

카메라 그룹 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **카메라** 탭을 클릭하세요.

4. 이름을 변경할 그룹을 선택하고 마우스 오른쪽 버튼을 클릭하세요.
5. 팝업 메뉴에서 **카메라 그룹 삭제**를 클릭하세요.
6. 경고 메시지를 확인하고 **네** 버튼을 클릭하세요.

> **알아두기**
> 카메라 그룹에 카메라가 포함되어 있다면 그룹을 삭제할 수 없습니다. 그룹에 속한 카메라를 다른 그룹으로 이동하거나 그룹에서 제거한 후 다시 시도하세요.

목록 열 설정

목록에서 표시할 열을 추가하거나 순서 변경, 숨김 설정을 할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **모든 카메라** 목록의 오른쪽 상단에서 ••• → **열 설정**을 클릭하세요.
4. **열 설정** 창이 나타나면 표시할 열의 체크박스를 클릭해 추가하거나 숨김 설정을 할 수 있습니다. 드래그 앤 드롭으로 열의 순서를 변경할 수도 있습니다.



5. 열 설정을 모두 변경했으면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

비디오 규칙 설정하기

규칙은 카메라와 출입문에서 발생하는 이벤트를 조합해 VMS 서버에 이벤트와 북마크 형식으로 전송하기 위한 설정입니다. 적절한 비디오 규칙 설정을 통해 다음과 같은 보안 관리 기능을 활용할 수 있습니다.

- **자동 북마크 생성**: 특정 출입 이벤트 발생 시 자동으로 북마크를 생성하여 중요한 영상을 쉽게 찾을 수 있습니다.
- **효율적인 모니터링**: 출입문과 연결된 카메라의 영상을 실시간으로 모니터링하고, 이벤트 발생 시 즉시 확인할 수 있습니다.
- **통합 이벤트 관리**: 출입 이벤트와 영상을 연계하여 보안 상황을 종합적으로 파악할 수 있습니다.

> **알아두기**
>
> - 비디오 규칙 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
> - 출입문과 카메라를 연동할 때 해당 카메라가 속한 그룹 권한이 필요합니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.

규칙 추가

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. 화면 왼쪽 상단의 **규칙 추가** 버튼을 클릭하세요.

새 규칙 추가 화면이 나타나면 다음 안내에 따라 규칙을 설정하세요. 모든 설정을 완료하고 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.

규칙 정보 입력

정보 섹션에서 새로운 규칙의 이름과 설명을 입력하세요.



> **알아두기**
>
> **설명** 항목은 선택 사항입니다. 규칙의 용도나 특징을 쉽게 파악할 수 있도록 간단한 설명을 입력하는 용도로 사용하세요.

비디오 로그 설정

비디오 로그는 특정 이벤트 발생 시점 전후의 영상을 자동 기록하는 기능입니다. 이벤트 발생 전후 맥락을 파악할 수 있도록 지정된 시간 동안의 영상을 보존합니다.

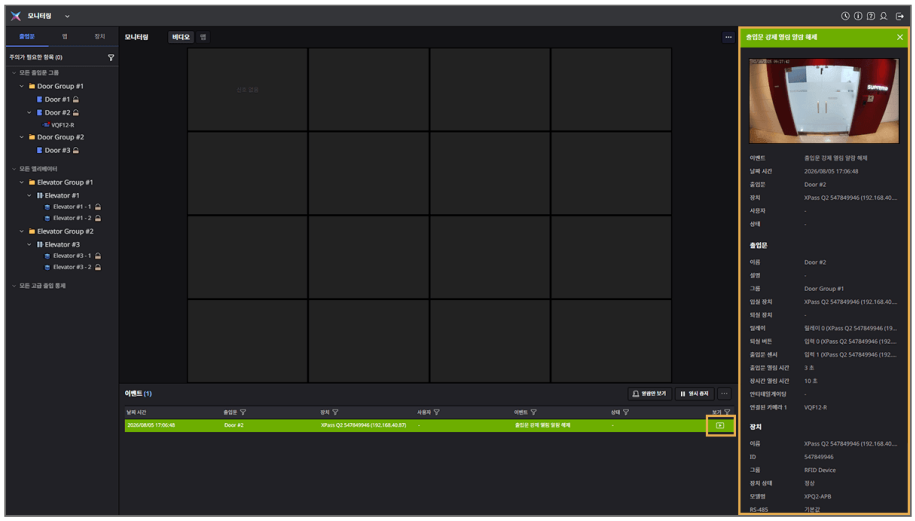


- **비디오 로그**: 현재 규칙에서 비디오 로그 기능 사용 여부를 설정하세요.
  - **사용**: 이벤트 발생 시 자동으로 전후 시간의 영상을 기록합니다.

  - **사용 안 함**: 비디오 로그 기능을 비활성화합니다.

- **비디오 로그 길이**: 이벤트 발생 시점을 기준으로 10초 전후의 영상을 기록할 범위를 설정하세요. 최대 60초까지 설정할 수 있습니다.

비디오 로그 옵션을 활성화하면 모니터링 화면의 이벤트 패널의 이벤트 항목에 비디오 로그(▶) 아이콘이 표시됩니다. 비디오 로그 아이콘이 표시된 이벤트 항목을 클릭하면 화면 오른쪽에 상세 정보가 나타납니다. 특정 이벤트가 발생한 시간의 영상을 확인할 수 있습니다.

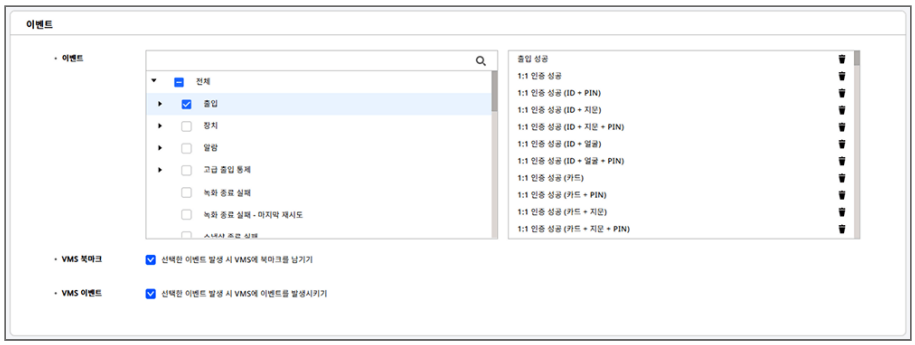


알아두기

비디오 로그 길이의 설정한 범위가 길수록 더 많은 저장 공간이 필요할 수 있습니다. 시스템 성능과 저장 용량을 고려하여 적절한 길이를 설정하세요.

VMS에 기록할 이벤트 설정

이벤트 섹션에서는 VMS 서버에 기록할 이벤트를 선택하고 북마크 또는 이벤트 전송 여부를 설정할 수 있습니다.



- **이벤트**: VMS 서버에 전송할 이벤트 유형을 선택하세요. 왼쪽 이벤트 목록에서 원하는 이벤트를 선택하면 오른쪽 목록에 추가됩니다.
- **VMS 북마크**: 이벤트 목록에서 선택한 이벤트가 발생할 때 VMS 서버에 북마크를 생성할지 설정할 수 있습니다.
- **VMS 이벤트**: 이벤트 목록에서 선택한 이벤트가 발생할 때 VMS 서버에 이벤트 기록을 생성할지 설정할 수 있습니다.

알아두기

- 이벤트 선택은 필수가 아닙니다.
- 왼쪽 이벤트 목록 상단의 검색 필드를 사용해 원하는 이벤트를 빠르게 찾을 수 있습니다.
- 오른쪽 목록에서 이벤트를 제거하려면 버튼을 클릭하세요.
- 북마크 및 이벤트를 VMS 서버에 전송할 때 메시지의 언어를 설정할 수 있습니다. 자세한 내용은 VMS 연동하기를 참고하세요.

출입문과 카메라 연동

출입문-카메라 연동 섹션에서는 출입문과 카메라를 연동하여 출입문에서 이벤트가 발생할 때 연결된 카메라의 영상과 함께 VMS 서버에 전송할 수 있습니다. 이를 통해 출입 이벤트와 관련된 영상을 쉽게 확인할 수 있습니다.



1. 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
2. **연동 추가** 창이 나타나면 출입문을 선택하고 해당 출입문과 연관된 카메라를 선택하세요.



3. 출입문과 카메라를 모두 선택했다면 **추가** 버튼을 클릭하세요.

목록에서 출입문과 연결된 카메라를 확인할 수 있습니다.



알아두기

- 카메라 그룹 권한이 없는 관리자는 특정 카메라 그룹에 속한 카메라를 조회하거나 선택할 수 없습니다. 카메라 그룹 권한 설정에 대한 자세한 내용은 카메라 설정하기를 참고하세요.
- 한 개의 출입문에는 최대 4대의 카메라를 추가할 수 있습니다.
- 한 규칙에 포함된 출입문은 다른 규칙에서 사용할 수 없습니다.
- 카메라를 여러 출입문과 제한 없이 연동할 수 있으며, 이미 다른 출입문과 연동된 카메라도 재사용할 수 있습니다.
- 출입문과 카메라 연동 규칙을 삭제하려면 목록에서 삭제하려는 항목의 체크박스를 클릭하고 오른쪽 상단의 **삭제** 버튼을 클릭하세요.
- 출입문과 연동된 카메라는 **모니터링** 페이지의 출입문 목록에서 출입문의 하위 구조로 확인할 수 있습니다. 자세한 내용은 상태 확인하기를 참고하세요.
- 모든 설정을 완료하고 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.

규칙 수정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **모든 규칙** 목록에서 수정하려는 규칙을 클릭하세요.
4. 규칙 수정 화면이 나타나면 원하는 항목을 수정하세요.
5. 수정한 규칙을 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

알아두기

규칙 수정 화면의 각 섹션에 대한 자세한 내용은 규칙 추가를 참고하세요.

규칙 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **모든 규칙** 목록에서 삭제하려는 규칙의 체크박스를 클릭하세요. 1개 이상의 규칙을 선택할 수 있습니다.
4. 화면 오른쪽 상단의 **규칙 삭제** 버튼을 클릭하세요.
5. 메시지를 확인하고 **네** 버튼을 클릭하세요.

목록 열 설정

목록에서 표시할 열을 추가하거나 순서 변경, 숨김 설정을 할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **비디오** → **비디오**를 클릭하세요.
3. **모든 규칙** 목록의 오른쪽 상단에서 ••• → **열 설정**을 클릭하세요.

4. **열 설정** 창이 나타나면 표시할 열의 체크박스를 클릭해 추가하거나 숨김 설정을 할 수 있습니다. 드래그 앤 드롭으로 열의 순서를 변경할 수도 있습니다.



5. 열 설정을 모두 변경했으면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

맵 관리하기

맵 설정 기능은 지도와 연동하여 층, 시설, 구역을 설정하고 관리하는 기능입니다. 이 기능을 사용하면 **모니터링** 페이지에서 구역과 시설, 층으로 구분된 지도를 확인할 수 있습니다.

> **알아두기**
> 맵 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.

층 구성하기

구역과 시설을 구성하기 전에 층을 구성하세요. 해당 층의 배치도를 이미지로 업로드하고, 출입문과 카메라를 배치하여 시각적으로 관리할 수 있습니다. 층을 구성하면 **모니터링** 페이지에서 해당 층의 출입문과 카메라를 확인할 수 있습니다.



위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

> **알아두기**
>
> - 층을 구성하기 전에 출입문을 먼저 등록하세요. 출입문 등록에 대한 자세한 내용은 출입문 등록하기를 참고하세요.
> - 맵 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.
> - 층 추가 및 설정 기능은 **에센셜**(Essential) 라이선스 이상에서 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

층 추가

층의 배치도 또는 3D 조감도 이미지를 업로드하여 층을 추가하고 출입문과 카메라를 배치할 수 있습니다.

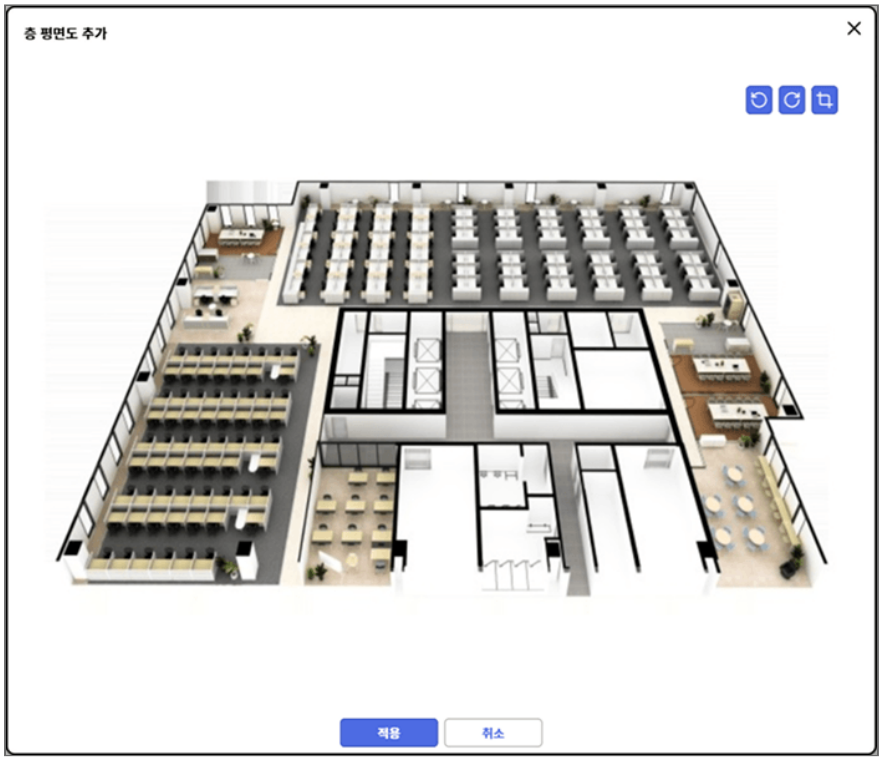
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **층**을 클릭하세요.
3. 층 목록 화면의 오른쪽 상단에 **새 층** 버튼을 클릭하세요.



4. **새 층** 화면의 **정보** 섹션에서 추가하려는 층의 이름과 설명을 입력하세요.
5. **층 설정** 섹션의 **층 평면도** 버튼을 클릭하거나 업로드할 이미지를 드래그하여 업로드하세요.

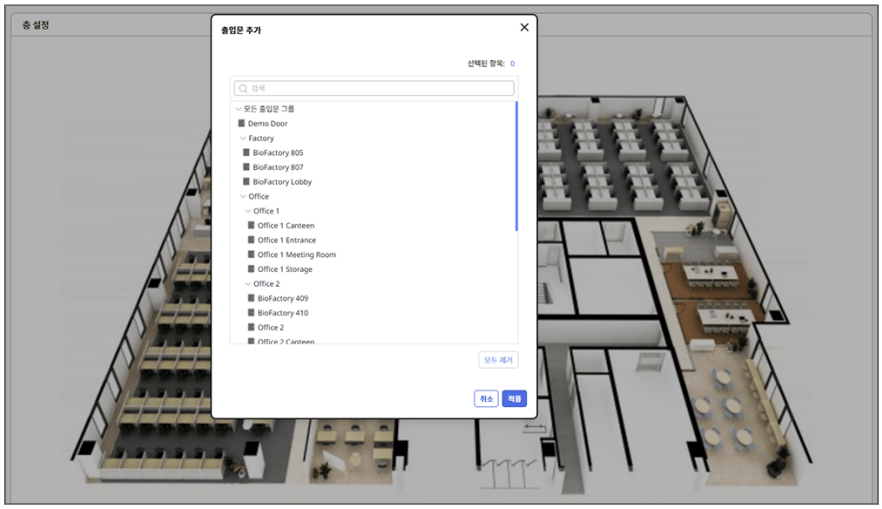
> 지원하는 이미지 파일은 PNG, JPEG, JPG 형식입니다.

6. **층 평면도 추가** 창에서 업로드한 이미지를 확인하고 설정을 진행하세요.

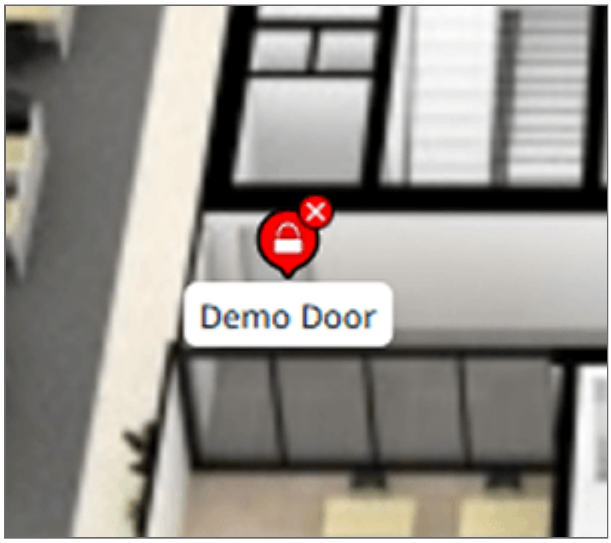


- 이미지를 회전하려면 ↺ 또는 ↻ 버튼을 클릭하세요.
- 이미지를 자르려면 ⌗ 버튼을 클릭하세요.

7. 이미지 설정을 완료하면 **적용** 버튼을 클릭하세요.
8. **층 설정** 섹션에 업로드한 이미지에 출입문을 추가하려면 이미지의 원하는 위치에서 오른쪽 마우스 버튼을 클릭하고 **출입문 추가**를 선택하세요.
9. **출입문 추가** 창이 나타나면 등록된 출입문 중 하나를 선택하세요.

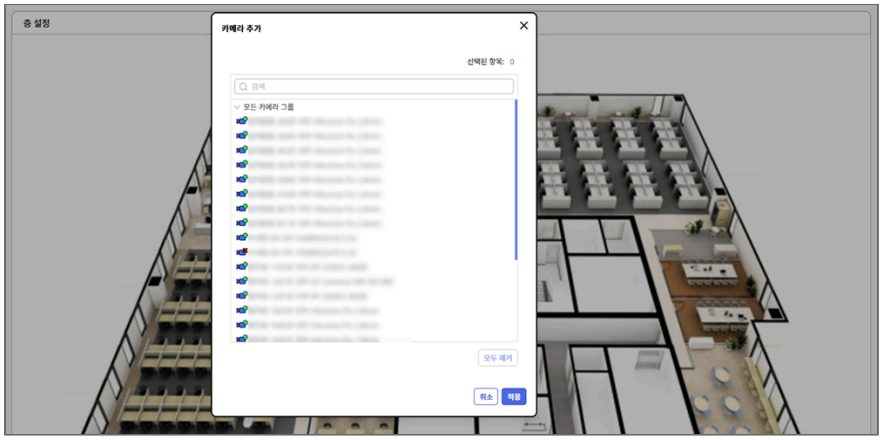


10. 출입문을 이미지에 배치하려면 **적용** 버튼을 클릭하세요.



11. 업로드한 이미지에 카메라를 추가하려면 이미지의 원하는 위치에서 오른쪽 마우스 버튼을 클릭하고 **카메라 추가**를 선택하세요.

12. **카메라 추가** 창이 나타나면 등록된 카메라 중 하나를 선택하세요.



13. 카메라를 이미지에 배치하려면 **적용** 버튼을 클릭하세요.



14. 실제 층에 배치된 출입문과 카메라를 추가로 배치하세요.

15. 모든 설정을 완료하고 설정한 층을 저장하려면 **확인** 버튼을 클릭하세요.

알아두기

- 층에 배치된 출입문과 카메라의 위치를 변경하려면 해당 출입문 또는 카메라를 클릭한 상태에서 원하는 위치로 드래그하세요.
- 층에 배치된 출입문과 카메라의 아이콘 및 상태에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.

층 구성 수정

출입문과 카메라를 추가한 층의 배치도를 수정할 수 있습니다. 층의 배치도를 수정하면 출입문과 카메라의 위치를 변경하거나 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **층**을 클릭하세요.
3. 층 목록에서 수정하려는 층을 클릭하세요.

모든 설정을 완료하고 설정한 층을 저장하려면 **적용** 버튼을 클릭하세요.

출입문/카메라 삭제

층의 이미지에서 삭제하려는 출입문 또는 카메라의 ⊗ 아이콘을 클릭하세요. 해당 출입문 또는 카메라를 삭제할 수 있습니다.

카메라 촬영 범위 설정

층의 이미지에서 촬영 범위를 설정할 카메라에서 마우스 오른쪽 버튼을 클릭하세요. 팝업 메뉴에서 **촬영 범위 추가**를 클릭하세요.



- 촬영 범위를 변경하려면 녹색 영역으로 마우스 포인터를 이동하세요. 마우스 포인터가 십자 모양으로 변경되면 마우스를 클릭한 상태에서 원하는 위치로 드래그하세요.



- 촬영 범위를 조정하려면 범위의 끝 모서리 부분을 클릭한 상태에서 원하는 크기로 드래그하세요.

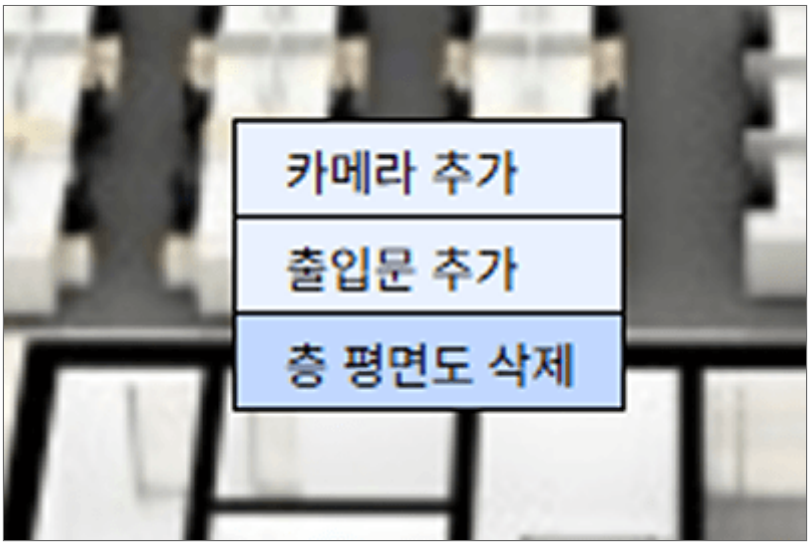


- 촬영 범위를 삭제하려면 ⊗ 아이콘을 클릭하세요.

> **주의**
> 사용자가 설정한 사항은 보안 관리의 편의성을 위해 제공하는 기능일 뿐, 실제 카메라의 촬영 범위를 반영하지 않습니다.

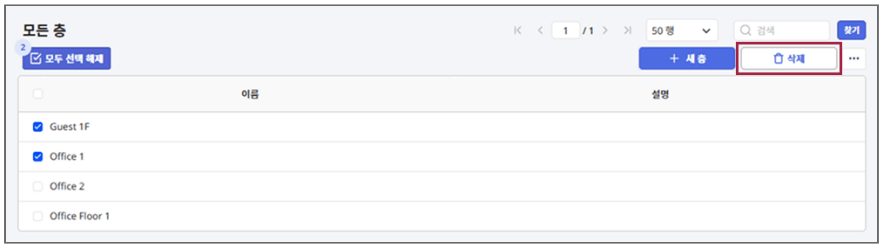
층 이미지 삭제

층의 이미지를 삭제하려면 층 이미지에서 마우스 오른쪽 버튼을 클릭하고 팝업 메뉴에서 **층 평면도 삭제**를 선택하세요.



층 삭제하기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **층**을 클릭하세요.
3. 층 목록에서 삭제하려는 층의 체크박스를 클릭하세요. 1개 이상의 층을 선택할 수 있습니다.

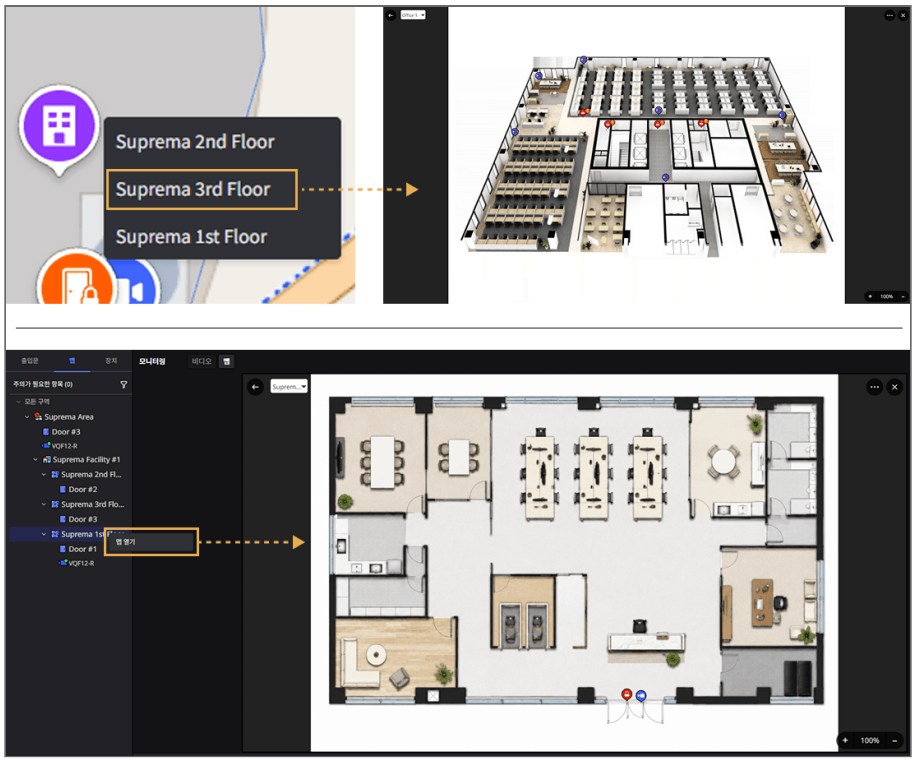


4. 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.

층 목록에서 선택한 층이 삭제됩니다. 선택한 층은 복구할 수 없습니다.

시설 구성하기

시설(Facility)을 구성하고 층을 배치하세요. 층을 순차적으로 배치하여 실제 시설의 구조를 표현할 수 있습니다. 시설을 구성하면 **모니터링** 페이지에서 지도에 배치된 시설을 선택하고 각 층으로 진입하여 모니터링할 수 있는 기능을 제공합니다.



알아두기

- 시설을 구성하기 전에 층을 먼저 등록하세요. 층 등록에 대한 자세한 내용은 층 구성하기를 참고하세요.
- 맵 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.
- 시설 추가 및 설정 기능은 **에센셜**(Essential) 라이선스 이상에서 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

시설 추가

시설에 층을 추가하여 구조를 설계하려면 다음 단계를 따르세요.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **시설**을 클릭하세요.

3. 시설 목록 화면 오른쪽 상단의 **새 시설** 버튼을 클릭하세요.

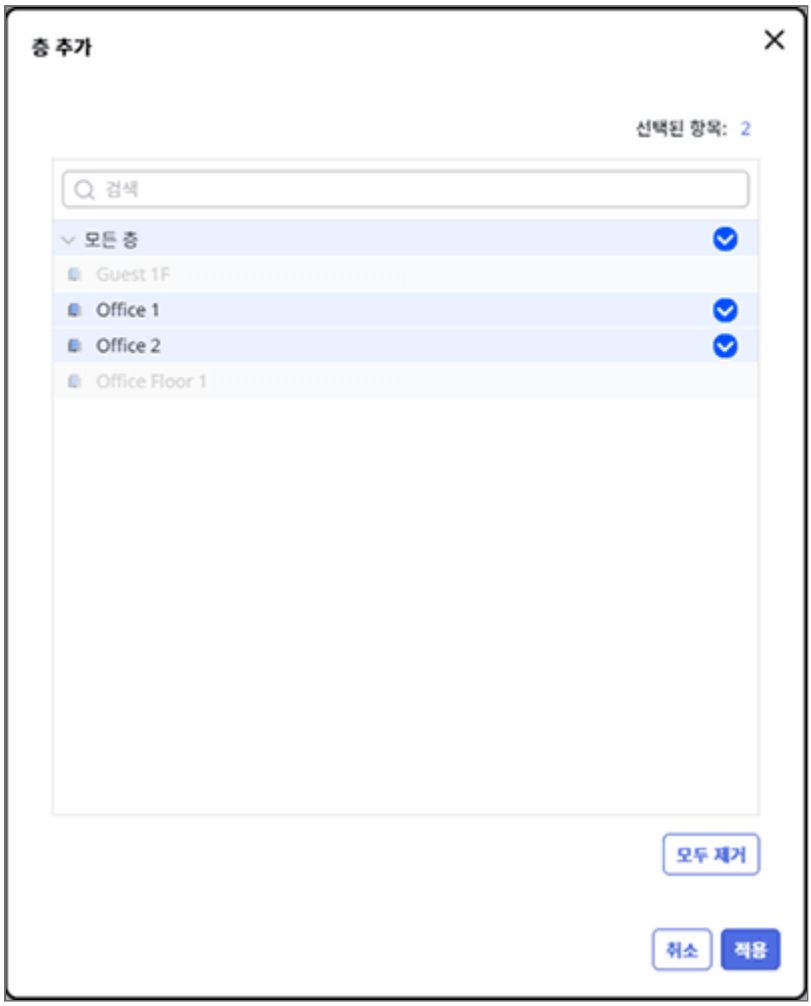


4. **새 시설 추가** 화면의 **정보** 섹션에서 추가하려는 시설의 이름과 설명을 입력하세요.

5. **시설 설정**에서 **추가** 버튼을 클릭하세요.



6. **층 추가** 창이 나타나면 층 목록에서 추가할 층을 선택하세요.



- 입력 필드에 키워드를 입력해 층을 검색할 수도 있습니다.
- 모든 층을 선택하려면 **모든 층**을 선택하세요.

7. 층을 모두 선택했다면 **적용** 버튼을 클릭하세요.

8. 출입문 목록에 추가한 층을 확인하고 순서를 변경하려면 **순서** 열의 ⠿ 아이콘을 드래그하여 순서를 변경하세요.

9. 시설 구성을 완료하고 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

시설 수정

기존 시설에 층 추가

이미 만들어진 시설에 층을 추가할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **시설**을 클릭하세요.
3. 시설 목록에서 층을 추가할 시설을 선택하세요.
4. **시설 설정**에서 **추가** 버튼을 클릭하세요.



5. **층 추가** 창이 나타나면 추가할 층의 체크박스를 클릭해 층을 선택하세요.
6. 층을 모두 선택했다면 **적용** 버튼을 클릭하세요.
7. 출입문 목록에 추가한 층을 확인하고 순서를 변경하려면 **순서** 열의 ⠿ 아이콘을 드래그하여 순서를 변경하세요.
8. 시설 구성을 완료하고 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

시설의 층 삭제

이미 만들어진 시설에 층을 삭제할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **시설**을 클릭하세요.
3. 시설 목록에서 층을 삭제할 시설을 선택하세요.
4. **시설 설정**에서 삭제할 층의 ✕ 버튼을 클릭하세요.
5. 층 삭제를 완료하고 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

시설 삭제

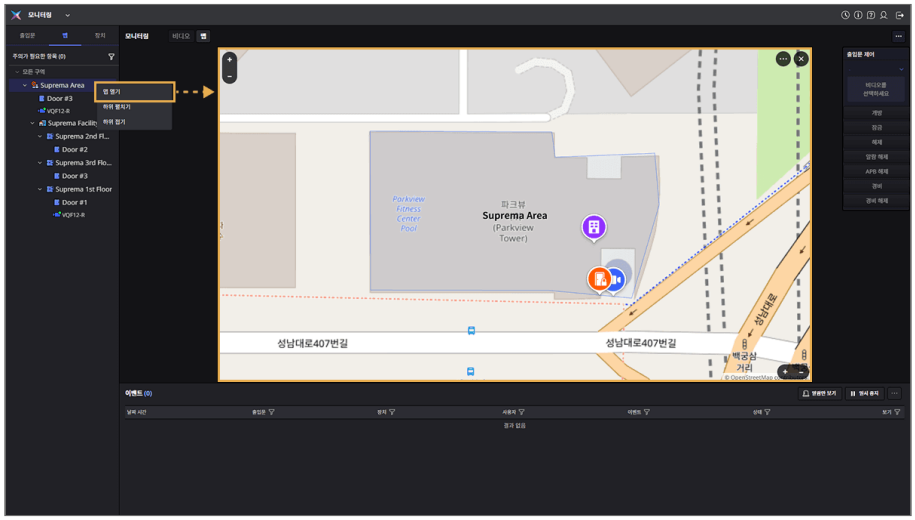
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **시설**을 클릭하세요.
3. 시설 목록에서 삭제할 시설의 체크박스를 클릭하세요.



4. 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.
5. 확인 메시지 창이 나타나면 **네** 버튼을 클릭하세요.

구역 구성하기

층과 시설 구성을 완료하고 구역을 구성할 수 있습니다. 보안 관리하고 있는 구역을 지도를 통해 관리하고 확인할 수 있습니다. 구역을 구성하면 **모니터링** 페이지에서 해당 구역의 시설과 층으로 진입하여 모니터링할 수 있는 기능을 제공합니다.



알아두기

- 구역을 구성하기 전에 층과 시설을 먼저 등록하세요. 층과 시설 등록에 대한 자세한 내용은 다음 문서를 참고하세요.
  - 층 구성하기
  - 시설 구성하기
- 맵 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.
- 구역 추가 및 설정 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

구역 추가

현재 관리하고 있는 보안 지역의 구역을 지도를 통해 설정하고 관리할 수 있습니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **구역**을 클릭하세요.
3. 구역 목록 화면 오른쪽 상단의 **새 구역** 버튼을 클릭하세요.



4. **새 구역 추가** 화면의 **정보** 섹션에서 추가하려는 구역의 이름과 설명을 입력하세요.
5. **구역 설정** 섹션의 지도에서 추가할 구역의 위치를 설정하세요.
6. 지도에서 마우스 오른쪽 버튼을 클릭하고 **구역 설정**을 선택하세요.

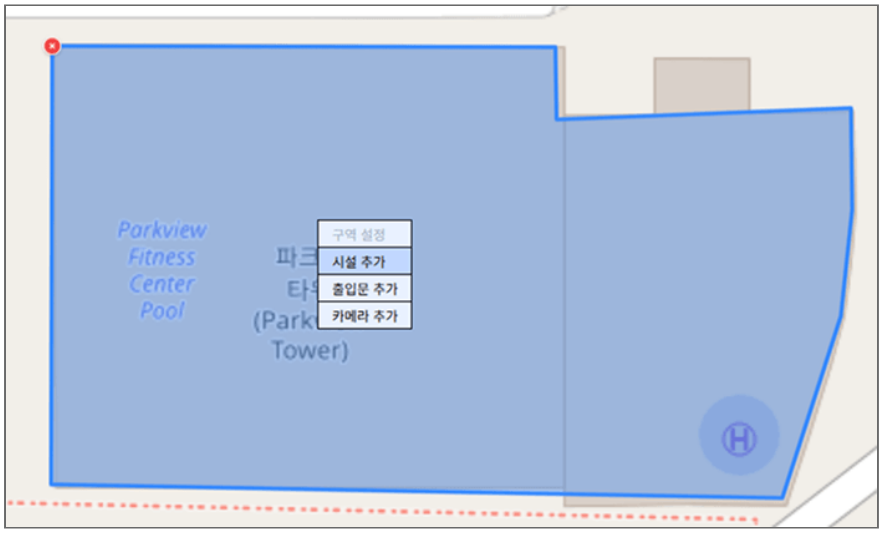


7. 원하는 형태로 구역을 설정하세요. 마우스를 클릭해 시작하고 드래그하여 구역을 설정할 수 있습니다.



> 구역을 다시 설정하려면 설정된 구역을 삭제해야 합니다. 해당 구역을 삭제하려면 ⊗ 버튼을 클릭하세요.

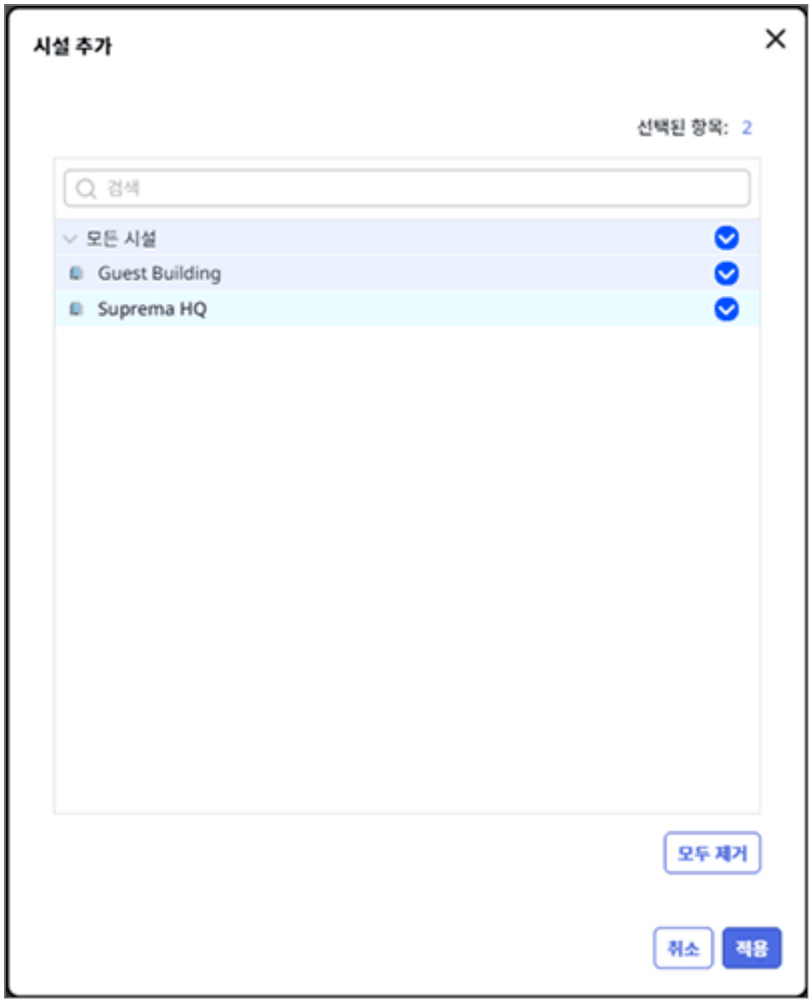
8. 설정한 구역에 시설을 추가하려면 마우스 오른쪽 버튼을 클릭하고 **시설 추가**를 선택하세요.



구역을 추가할 때는 적어도 하나의 시설 또는 출입문, 카메라를 설정해야 합니다.

- 출입문을 추가하려면 마우스 오른쪽 버튼을 클릭하고 **출입문 추가**를 선택하세요.
- 카메라를 추가하려면 마우스 오른쪽 버튼을 클릭하고 **카메라 추가**를 선택하세요.

9. **시설 추가** 창이 나타나면 추가할 시설을 선택하고 **적용** 버튼을 클릭하세요.



> 출입문 또는 카메라를 추가할 때, 마찬가지로 **출입문 추가** 또는 **카메라 추가** 창이 나타납니다. 추가할 항목을 선택하고 **적용** 버튼을 클릭하세요.

10. 구역 설정을 완료하면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 지도에서 왼쪽 상단의 입력 필드를 통해 원하는 위치를 검색할 수 있습니다. 현재 위치로 돌아가려면 버튼을 클릭하세요.
>
> 
>
>
> - 구역을 추가할 때 지도에서는 하나의 다각형을 통해서 구역을 설정할 수 있습니다. 구역을 설정할 때는 반드시 시작점과 끝점을 동일하게 설정해야 합니다. 구역을 설정한 후에는 구역의 모양을 변경할 수 없습니다. 구역을 수정하려면 구역을 삭제하고 다시 추가해야 합니다.
> - 추가한 시설 및 출입문, 카메라의 위치는 지도 상에서 드래그앤드랍 방식으로 위치를 변경할 수 있습니다.

구역 수정

이미 만들어진 구역을 삭제하고 다시 설정하거나, 시설 또는 출입문, 카메라를 추가 또는 삭제할 수 있습니다.

구역 재설정

지도에서 하나의 구역을 재설정하려면 이미 만들어지 구역을 삭제하고 다시 추가해야 합니다.

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **맵** → **구역**을 클릭하세요.
3. 구역 목록에서 재설정할 구역을 선택하세요.
4. **구역 설정** 섹션의 지도에서 이미 만들어진 구역의 왼쪽 상단에 버튼을 클릭하세요.



5. 지도에서 마우스 오른쪽 버튼을 클릭하고 팝업 메뉴에서 **구역 설정**을 선택하세요.
6. 원하는 형태로 구역을 설정하고 저장하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

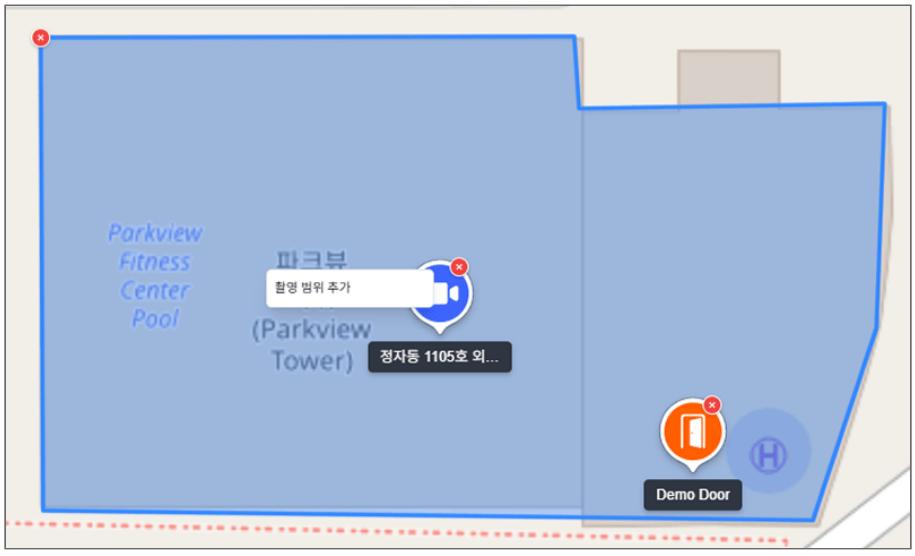
시설/출입문/카메라 삭제

지도에서 삭제하려는 시설 또는 출입문, 카메라를 클릭하세요. ⊗ 아이콘이 나타납니다. 아이콘을 클릭하면 선택한 시설을 삭제할 수 있습니다.

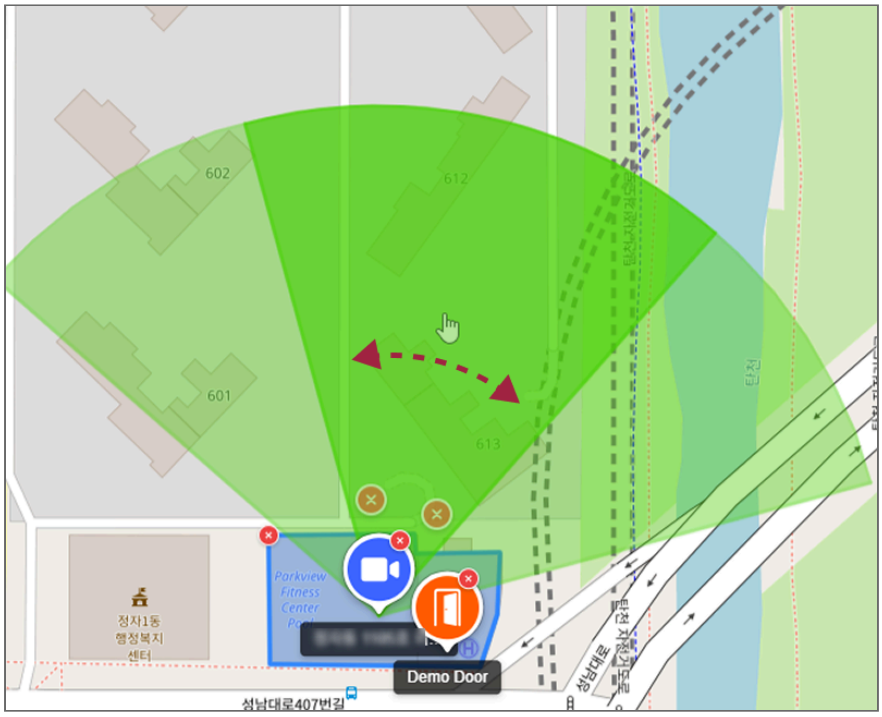


카메라 촬영 범위 설정

지도에서 카메라 촬영 범위를 설정할 수 있습니다. 카메라가 배치된 아이콘에서 마우스 오른쪽 버튼을 클릭하고 **촬영 범위 추가**를 선택하세요.



- 촬영 범위를 변경하려면 녹색 영역의 촬영 범위를 클릭한 상태에서 원하는 방향으로 드래그하세요.



- 촬영 범위를 조정하려면 범위의 끝 모서리 부분을 클릭한 상태에서 원하는 크기로 드래그하세요.



- 촬영 범위를 삭제하려면 ⓧ 아이콘을 클릭하세요.

> **주의**
> 사용자가 설정한 사항은 보안 관리의 편의성을 위해 제공하는 기능일 뿐, 실제 카메라의 촬영 범위를 반영하지 않습니다.

구역 삭제

1. **런처** 페이지에서 **설정**을 클릭하세요.

2. 화면 왼쪽 사이드바에서 **맵** → **구역**을 클릭하세요.
3. 구역 목록에서 삭제할 구역의 체크박스를 클릭하세요.



4. 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.
5. 확인 메시지 창이 나타나면 **네** 버튼을 클릭하세요.

방문자 설정하기

방문자 관리를 위해 방문처와 방문 PC를 구성할 수 있으며, 방문자를 위한 출입 약관 및 안내 문구를 설정할 수 있습니다. 또한 커스텀 방문자 필드를 이용해 방문자에게 요구할 정보를 직접 추가할 수도 있습니다.

> **알아두기**
>
> - **방문자** 설정은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
> - **방문자** 메뉴를 사용하려면 **사용자 자동 동기화** 또는 **서버 매칭 사용** 옵션을 활성화해야 합니다. 자세한 내용은 서버 상세 설정하기를 참고하세요.

방문 설정

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **방문자** → **방문자**를 클릭하세요.
3. 다음 안내에 따라 방문자 설정을 구성하세요.

1 방문처 설정

각 방문처의 방문 신청용 또는 방문자 관리용 PC에서 사용할 출입 그룹과 카드 사용 여부를 설정할 수 있습니다. 카드를 사용할 경우 카드 종류 및 데이터 형식도 설정할 수 있습니다.



- **이름**: 방문처의 이름을 입력할 수 있습니다.

> **알아두기**
>
> – 방문처 이름은 최대 48자까지 입력할 수 있습니다.

- **출입 그룹**: 방문자에게 할당할 출입 그룹을 선택할 수 있습니다.

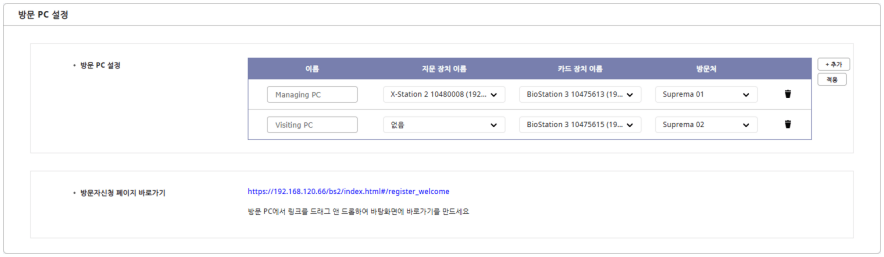
> **알아두기**
> 방문자를 위한 출입 그룹을 미리 설정해 놓으면 관리가 용이합니다. 출입 그룹 설정에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.

- **카드 사용**: 카드 사용 여부를 선택할 수 있습니다.
- **카드 종류**: 방문처에서 사용할 카드 종류를 선택할 수 있습니다. 카드 종류는 **카드 사용**을 설정할 경우에만 활성화됩니다.
- **카드 데이터 형식**: 카드 데이터를 읽는 형식을 설정할 수 있습니다. **카드 데이터 형식**은 **카드 종류**를 **Wiegand**로 설정할 경우에만 활성화됩니다.

방문처 설정을 저장하려면 **적용** 버튼을 클릭하세요.

2 방문 PC 설정

방문 신청용 또는 방문자 관리용 PC를 설정할 수 있습니다.



- **이름**: 방문 신청용 또는 방문자 관리용 PC의 이름을 설정할 수 있습니다.
- **지문 장치 이름**: 방문자가 지문 인증을 통해 출입할 경우 방문자의 지문을 등록할 장치를 선택하세요.
- **카드 장치 이름**: 방문자가 카드 인증을 통해 출입할 경우 카드를 발급할 장치를 선택하세요. 카드 장치 이름은 카드 사용을 선택한 방문처를 설정한 경우에만 활성화됩니다.
- **방문처**: 해당 방문 PC에서 방문을 관리할 방문처를 선택하세요.

방문 PC 설정을 저장하려면 **적용**을 클릭하세요.

> **알아두기**
> - 방문 PC 이름은 최대 48자까지 입력할 수 있습니다.
> - 지문 및 카드 장치를 동시에 사용할 수 있으며 각각 1대씩 선택할 수 있습니다.
> - 방문처는 PC당 1개만 선택할 수 있습니다.

3 방문 PC 선택

방문 PC 설정에서 설정한 PC를 선택하여 사용 중인 PC에 할당할 수 있습니다.



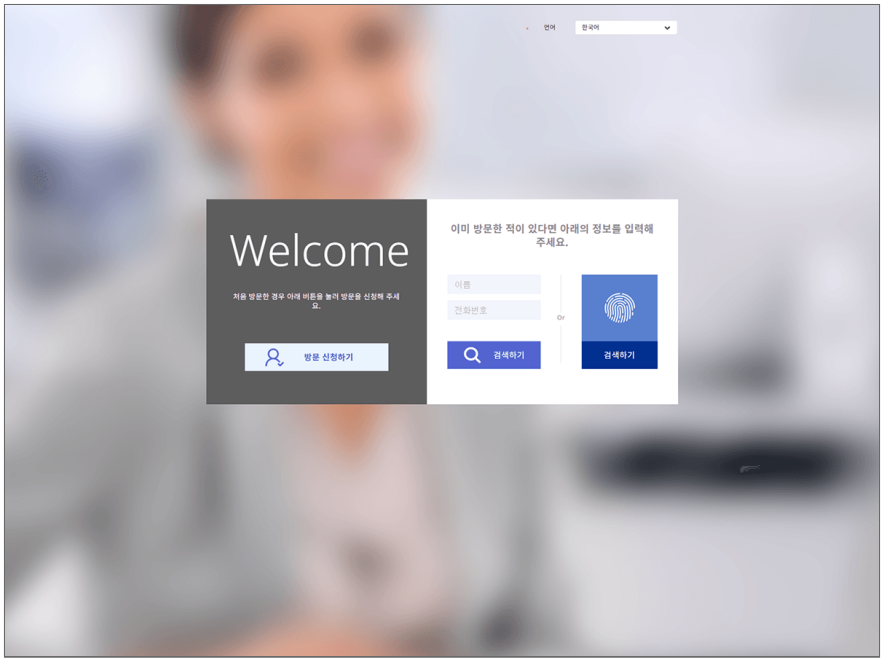
설정을 저장하려면 **적용**을 클릭하세요.

4 방문자 신청 페이지 바로가기

방문 신청용 PC의 바탕 화면에 방문 신청 페이지 바로가기 아이콘을 생성할 수 있습니다. **방문자신청 페이지 바로가기** 항목의 URL 주소를 바탕 화면에 끌어다 놓으세요.

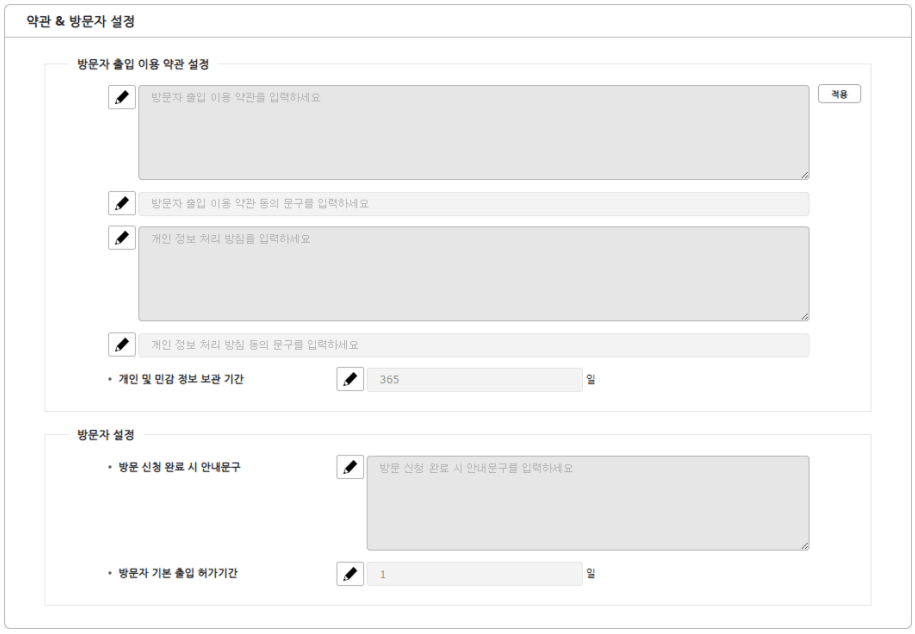


웹 브라우저에서 URL 주소로 접속하면 방문 신청 페이지를 확인할 수 있습니다.



약관 & 방문자 설정하기

방문자 출입 약관, 개인정보 처리 방침, 안내 문구 등 방문자 관련 주요 설정을 관리할 수 있습니다.



- **출입 이용 약관**: 출입에 대한 이용 약관 및 약관 동의 문구를 입력할 수 있습니다. ✎을 클릭해 입력 필드를 활성화한 뒤 이용 약관 및 약관 동의 문구를 입력하세요.

  > **알아두기**
  >
  > – 출입 약관은 최대 65,535자까지 입력할 수 있습니다.
  >
  > – 약관 동의 문구는 최대 64자까지 입력할 수 있습니다.

- **개인 정보 처리 방침**: 방문자가 방문 시 제공한 개인 정보에 대한 처리 방침 및 해당 방침에 대한 동의 문구를 입력할 수 있습니다. ✎을 클릭해 입력 필드를 활성화한 뒤 개인 정보 처리 방침 및 해당 방침에 대한 동의 문구를 입력하세요.

  > **알아두기**
  >
  > – 개인 정보 처리 방침은 최대 65,535자까지 입력할 수 있습니다.
  >
  > – 개인 정보 처리 방침에 대한 동의 문구는 최대 64자까지 입력할 수 있습니다.

- **개인 및 민감 정보 보관 기간**: 방문자가 방문 시 제공한 개인 정보에 대한 보관 기간을 설정할 수 있습니다. ✎을 클릭해 입력 필드를 활성화한 뒤 개인 정보 보관 기간을 일 단위로 입력하세요.

  > **알아두기**
  >
  > – 개인 및 민감 정보 보관 기간이 만료된 방문자 목록은 **방문자** 메뉴에서 삭제할 수 있습니다.

- **방문 신청 완료 시 안내문구**: 방문 신청 완료 시 팝업 화면으로 표시할 안내 문구를 입력할 수 있습니다. ✎을 클릭해 입력 필드를 활성화한 뒤 안내 문구를 입력하세요.

> **알아두기**
>
> – 방문 신청 완료 시 안내 문구는 최대 65,535자까지 입력할 수 있습니다.
>
> – 안내 문구를 입력하지 않을 경우 방문 신청 완료 시 안내 문구 팝업 화면이 출력되지 않습니다.

- **방문자 기본 출입 허가기간**: 방문자의 출입에 대한 허가 기간을 설정할 수 있습니다. ✎을 클릭해 입력 필드를 활성화한 뒤 방문자 기본 출입 허가 기간을 일 단위로 입력하세요.

커스텀 방문자 필드 설정하기

방문자의 부가 정보를 입력할 필드를 추가할 수 있으며, 추가된 필드는 방문 신청 화면에 나타납니다.



- **순서**: 사용자 정의로 추가한 입력 필드의 순서를 설정할 수 있습니다.
- **이름**: 사용자 정의로 추가한 입력 필드의 이름을 설정할 수 있습니다.
- **유형**: 문자 입력 상자, 숫자 입력 상자, 선택 상자를 선택할 수 있습니다.
- **데이터**:선택 상자 목록에 표시할 선택지를 입력하세요. 각 항목은 세미 콜론(;) 기호로 구분합니다. 데이터는 **유형**을 **선택 상자**로 설정한 경우에만 활성화됩니다.

설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - **문자 입력 상자**로 추가된 커스텀 방문자 필드에는 숫자와 문자를 입력할 수 있습니다.
> - **숫자 입력 상자**로 추가된 커스텀 방문자 필드에는 숫자만 입력할 수 있으며, 문자는 입력할 수 없습니다.
> - **선택 상자**로 추가된 커스텀 방문자 필드는 방문자가 항목을 선택할 수 있습니다. 커스텀 방문자 필드를 설정할 때 데이터에 **Option 1; Option 2; Option 3; Option 4**를 입력하세요.

디렉토리 연동 설정하기

Microsoft Entra ID(이하 **Entra ID**) 또는 **액티브 디렉토리**(Active Directory)와 **BioStar X**를 연동하여 사용자를 동기화하고 관리하는 방법을 안내합니다.

Entra ID 또는 **Active Directory**와 연동하면 아래의 편의 기능을 사용할 수 있습니다. 이를 통해 보안과 편의성을 높일 수 있습니다.

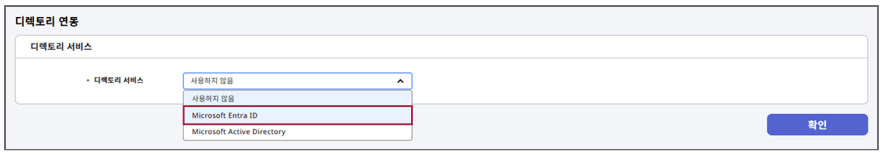
- **Entra ID**에서 제공하는 Single Sign-On(SSO) 기능을 통해 **Entra ID** 계정으로 **BioStar X**에 로그인할 수 있습니다.
- **Active Directory**에서 제공하는 Lightweight Directory Access Protocol(LDAP) 인증을 통해 **BioStar X**에 로그인할 수 있습니다.
- **Entra ID** 또는 **Active Directory**에서 구성한 사용자 및 그룹을 **BioStar X**와 동기화할 수 있습니다.
- **Entra ID** 또는 **Active Directory**에서 사용되는 직책과 부서, 그룹 등의 사용자 정보를 **BioStar X**의 사용자 정의 필드와 맵핑할 수 있습니다.

> **알아두기**
>
> **Entra ID** 또는 **Active Directory** 설정 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

디렉토리 연동 설정

Entra ID

1. **BioStar X**에 관리자 아이디로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **시스템** → **디렉토리 연동**을 클릭하세요.
4. **디렉토리 서비스** 항목에서 **Microsoft Entra ID**를 선택하세요.



5. 다음 안내에 따라 각 항목을 설정하세요.

> **알아두기**
>
> Entra ID와 연동하려면 **시스템** → **서버** 메뉴에서 **사용자 ID 종류** 항목을 **영숫자**로 설정해야 합니다.

1 디렉토리 서버

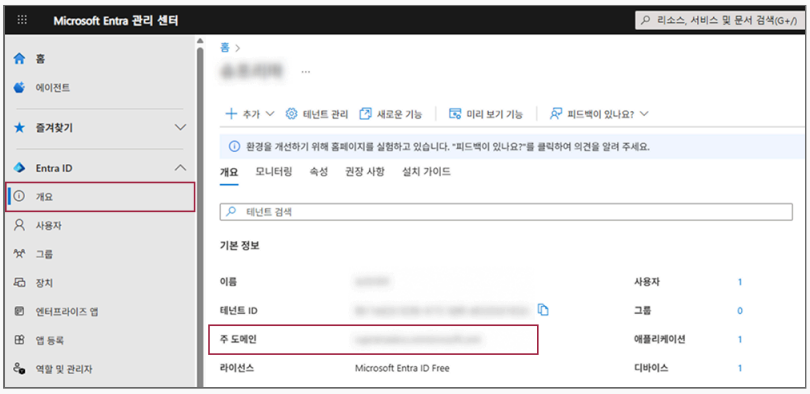
디렉토리 서버 섹션에서 **Entra ID**의 서버 정보를 입력하고 **연결** 버튼을 클릭하세요.



- **클라이언트 ID**: **Entra ID**에서 등록한 애플리케이션의 **클라이언트 아이디**(**Client ID**)를 입력하세요.
- **클라이언트 시크릿**: **Entra ID**에서 등록한 애플리케이션의 **인증서 및 암호**(**Certificates & secrets**)에 추가한 **클라이언트 암호**(**Client secrets**)를 입력하세요.
- **주 도메인**: **Entra ID**에서 조직을 만들 때 입력한 기본 도메인 이름을 입력하세요.

알아두기

- Entra ID에서 애플리케이션을 등록하는 방법은 다음 링크를 참고하세요.
- Entra ID에서 **인증서 및 암호** 설정 방법은 다음 링크를 참고하세요.
- 테넌트 ID는 Entra ID에서 등록한 애플리케이션의 **개요(Overview)**에서 확인할 수 있습니다.
- **주 도메인** 정보는 Entra ID의 **개요(Overview)**에서 확인할 수 있습니다.



1 사용자 그룹 필터

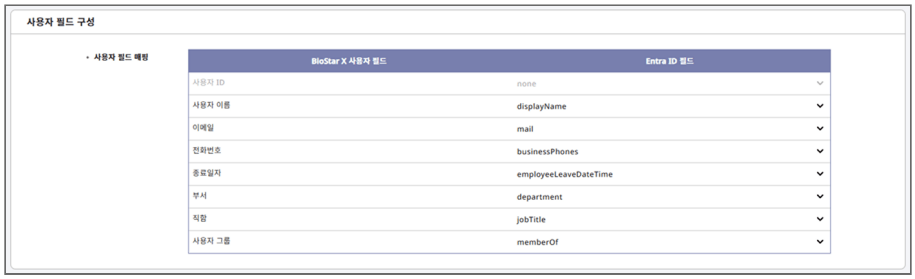
디렉토리 서버 섹션에서 설정을 완료하고 **연결** 버튼을 클릭하면, **사용자 그룹 필터** 섹션에 로부터 사용자 그룹 정보를 가져옵니다. BioStar X에 동기화하지 않을 사용자 그룹을 선택 해제하세요.



- **업데이트**: 사용자 그룹 정보를 새로 불러오려면 클릭하세요.
- 🔍 버튼을 클릭해 원하는 사용자 그룹을 검색할 수 있습니다.

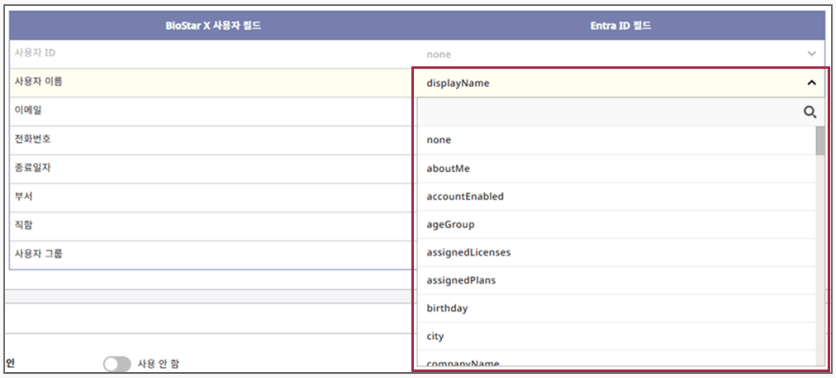
1 사용자 필드 구성

BioStar X의 사용자 필드와 맵핑할 필드를 설정할 수 있습니다. **사용자 필드 구성** 섹션에서 BioStar X의 사용자 필드로 사용할 의 필드를 선택하세요.



알아두기

BioStar X의 각 사용자 필드는 의 사용자 정보와 일치하는 항목을 맵핑할 수 있도록 기본 설정되어 있습니다. 기본 설정된 필드값이 아닌 다른 필드값을 선택하려면 **Entra ID 필드** 열의 항목을 클릭하고 원하는 필드값을 선택하세요.

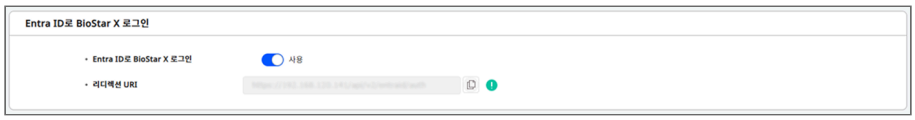


주의

Entra ID와 연동할 때 **사용자 ID** 필드는 맵핑할 수 없습니다. **사용자 ID**는 BioStar X에서 자동 생성하여 적용합니다.

1 Entra ID로 BioStar X 로그인

Entra ID SSO로 BioStar X를 로그인하도록 설정하려면, **Entra ID로 BioStar X 로그인** 항목을 **사용**으로 변경하세요.



리디렉션 URI 항목의 리디렉션 주소를 복사(⧉)하고, Entra ID 포털의 SSO 리디렉션 설정에 붙여넣으세요. 사용자가 Entra ID로 로그인에 성공하면 이 주소로 리디렉션됩니다.

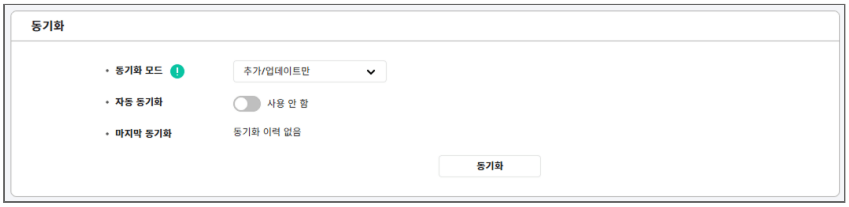
알아두기

- Entra ID에 애플리케이션을 등록하고, 리디렉션 URI를 추가하는 방법은 다음 링크를 참고하세요.
  - Microsoft Entra ID에 애플리케이션 등록
  - 앱에 리디렉션 URI 추가
- 리디렉션 주소는 Entra ID에서 등록한 애플리케이션의 개요(Overview)에서 확인할 수 있습니다.

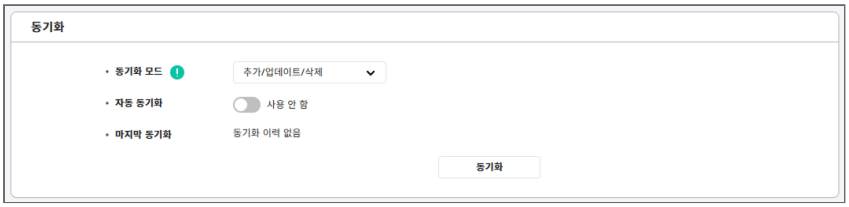
❶ 동기화

에서 변경된 사용자 정보를 동기화할 수 있는 기능입니다.

- **동기화 모드**: 원하는 동기화 방식을 선택하세요.
  - **추가/업데이트만**: 연동된 디렉토리 서비스에서 사용자를 동기화할 때, **BioStar X**에 없는 사용자를 추가하고, 정보가 변경된 사용자를 업데이트합니다. 단, 다음 사용자는 삭제하지 않고 유지합니다.
    - **BioStar X**에만 등록된 사용자
    - 에서 삭제된 사용자



  - **추가/업데이트/삭제**: **BioStar X**의 사용자 정보를 연동된 디렉토리 서비스와 완전히 동일하게 동기화합니다. **BioStar X**에만 등록된 사용자 및 에서 삭제된 사용자를 모두 포함하여 동기화하므로, 양측의 데이터가 동일하게 관리됩니다.



- **자동 동기화**: 자동 동기화 간격을 설정할 수 있습니다. **동기화 주기**에 설정한 간격에 따라 자동 동기화됩니다. 분 단위로 입력할 수 있습니다. 최소 설정값은 **30**분, 최대 설정값은 **10,080**분(7일)입니다.



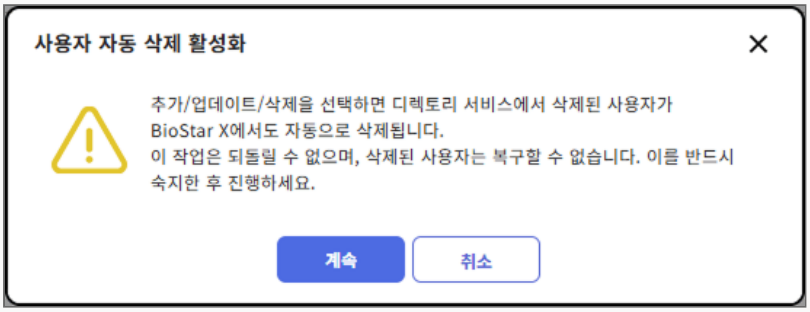
- **마지막 동기화**: 가장 최근에 동기화한 날짜와 시간을 확인할 수 있습니다.

주의

- **추가/업데이트만** 모드 사용 시 같은 이름의 사용자 그룹이 있다면 삭제하지 않고 유지합니다.
- **추가/업데이트/삭제** 모드에서는:
  - **같은 이름의 그룹이 이미 있는 경우**: 그룹이 새로 생성되지 않고 기존 그룹의 정보를 유지합니다. 다만 해당 그룹에 속한 사용자는 디렉토리 서비스의 최신 정보로 반영하기 위해 모두 제거한 후 다시 추가합니다. 단, 해당 그룹의 같은 이름 사용자는 유지합니다.
  - **BioStar X에서 생성된 사용자**: BioStar X에서 직접 생성한 사용자는 디렉토리 서비스와 연결되지 않은 상태입니다. 동기화 시 이들 사용자의 정보가 디렉토리 서비스와 연결되도록 업데이트합니다.
  - **제한사항**: 동기화 후 동일 이름의 그룹이 이미 있다면, 해당 그룹의 정보와 소속 사용자가 정상적으로 동기화되지 않을 수 있습니다.
- 디렉토리 연동을 설정한 상태에서 BioStar X v1.0.2로 업그레이드한 경우 동기화 모드는 **추가/업데이트/삭제**로 기본 설정됩니다.

알아두기

- **동기화** 버튼을 클릭할 때마다 선택한 동기화 모드로 디렉토리 서비스와 사용자 정보를 동기화합니다.
- **추가/업데이트/삭제** 모드를 선택하면 경고 메시지가 나타납니다. 메시지를 확인하고 계속하려면 **계속** 버튼을, 취소하려면 **취소** 버튼을 클릭하세요.



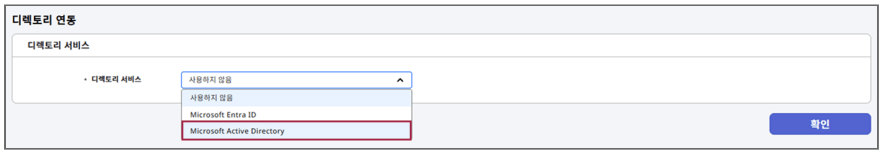
- 동기화 기능을 통해 연동할 때 특정 사용자를 동기화에서 제외하려면 디렉토리 연동 제외를 참고하세요.
- 동기화되는 사용자 아이디 또는 사용자 이름에 BioStar X에서 허용하지 않는 문자가 포함되어 있다면, 해당 문자만 제외한 값으로 등록합니다. 단, 사용자 아이디의 마침표(`.`), 사용자 이름의 마침표(`.`) 및 홑따옴표(`'`)는 제외 대상에서 빠지므로 원본 그대로 유지됩니다. 허용하지 않는 문자에 대한 자세한 내용은 사용자 ID 및 이름 입력 규칙을 참고하세요.

1 설정 저장

디렉토리 연동 설정을 모두 완료한 후 저장하려면 화면 가장 아래에 **확인** 버튼을 클릭하세요. 설정 결과를 확인하려면 설정 결과 확인을 참고하세요.

Active Directory

1. BioStar X에 관리자 아이디로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **시스템** → **디렉토리 연동**을 클릭하세요.
4. **디렉토리 서비스** 항목에서 **Microsoft Active Directory**를 선택하세요.



5. 다음 안내에 따라 각 항목을 설정하세요.

> **알아두기**
>
> - Active Directory는 Widows Server 2008 R2 이상의 시스템 환경에서 사용할 수 있습니다.
> - Active Directory와 연동하려면 **시스템** → **서버** 메뉴에서 **사용자 ID 종류** 항목을 **영숫자**로 설정해야 합니다.

1 디렉토리 서버

디렉토리 서버 섹션에서 **Active Directory**의 서버 정보를 입력하고 **연결** 버튼을 클릭하세요.



- **서버 주소**: Windows Active Directory 서버 주소를 입력하세요.
- **사용자명**: Windows Active Directory 로그인 아이디를 입력하세요.
- **비밀번호**: Windows Active Directory 로그인 비밀번호를 입력하세요.
- **기본 Domain 명**: Windows Active Directory 기본 도메인 이름을 입력하세요. 기본 도메인 이름은 아래 과정을 통해 확인할 수 있습니다.
  1. **Active Directory 관리 센터**를 실행하세요.
  2. 사용자 데이터가 저장된 노드(Node)에서 마우스 오른쪽 버튼을 클릭하고 **속성**을 선택하세요.
  3. **속성** 창에서 **확장**을 선택하고, **특성 편집기**를 클릭하세요.
  4. **distinguishedName** 값을 확인하세요.
- **암호화 사용**: Windows Active Directory 서버와 통신할 때 암호화를 사용할 수 있습니다. Active Directory 인증서 서비스를 설치하고 **키 저장소 비밀번호**를 설정하려면 액티브 디렉토리 암호화 설정를 참고하세요.
  - **키 저장소 비밀번호**: Windows Active Directory 서버 암호화 키 저장소 비밀번호를 입력하세요. **암호화 사용** 항목을 **사용**으로 설정하면 입력할 수 있습니다.

1 사용자 그룹 필터

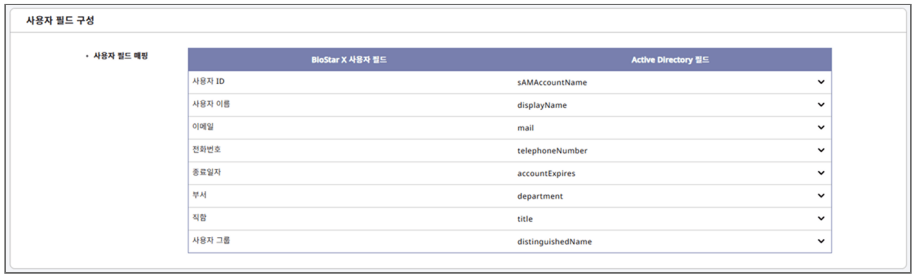
디렉토리 서버 섹션에서 설정을 완료하고 **연결** 버튼을 클릭하면, **사용자 그룹 필터** 섹션에 로부터 사용자 그룹 정보를 가져옵니다. **BioStar X**에 동기화하지 않을 사용자 그룹을 선택 해제하세요.

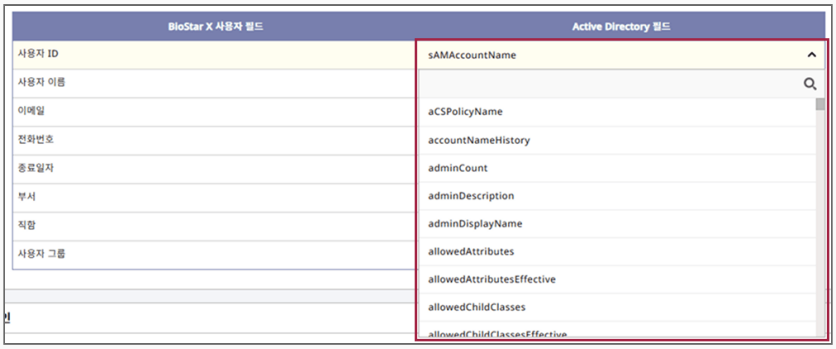


- **업데이트**: 사용자 그룹 정보를 새로 불러오려면 클릭하세요.
- 🔍 버튼을 클릭해 원하는 사용자 그룹을 검색할 수 있습니다.

1 사용자 필드 구성

BioStar X의 사용자 필드와 맵핑할 필드를 설정할 수 있습니다. **사용자 필드 구성** 섹션에서 **BioStar X**의 사용자 필드로 사용할 의 필드를 선택하세요.



> **알아두기**
>
> **BioStar X**의 각 사용자 필드는 의 사용자 정보와 일치하는 항목을 맵핑할 수 있도록 기본 설정되어 있습니다. 기본 설정된 필드값이 아닌 다른 필드값을 선택하려면 **Active Directory 필드** 열의 항목을 클릭하고 원하는 필드값을 선택하세요.
>
> 
>

1 Active Directory로 BioStar X 로그인

Active Directory 서버의 사용자 아이디로 로그인하도록 설정하려면 **Active Directory로 BioStar X 로그인** 항목을 **사용**으로 변경하세요. Active Directory 서버의 `sAMAccountName` 필드의 값이 **BioStar X** 로그인 아이디로 맵핑됩니다.

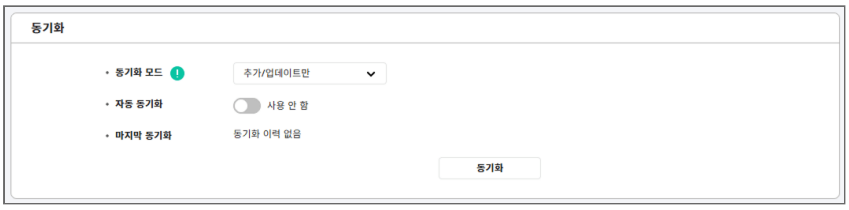
> **주의**
>
> sAMAccountName 필드에는 특수 문자가 포함될 수 없습니다. **BioStar X**의 로그인 아이디 정책에 맞지 않는 경우, 로그인에 실패할 수 있습니다.



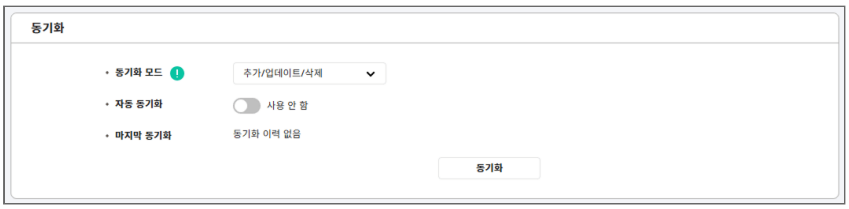
1 동기화

에서 변경된 사용자 정보를 동기화할 수 있는 기능입니다.

- **동기화 모드**: 원하는 동기화 방식을 선택하세요.
  - **추가/업데이트만**: 연동된 디렉토리 서비스에서 사용자를 동기화할 때, **BioStar X**에 없는 사용자를 추가하고, 정보가 변경된 사용자를 업데이트합니다. 단, 다음 사용자는 삭제하지 않고 유지합니다.
    - **BioStar X**에만 등록된 사용자
    - 에서 삭제된 사용자



  - **추가/업데이트/삭제**: **BioStar X**의 사용자 정보를 연동된 디렉토리 서비스와 완전히 동일하게 동기화합니다. **BioStar X**에만 등록된 사용자 및 에서 삭제된 사용자를 모두 포함하여 동기화하므로, 양측의 데이터가 동일하게 관리됩니다.



- **자동 동기화**: 자동 동기화 간격을 설정할 수 있습니다. **동기화 주기**에 설정한 간격에 따라 자동 동기화됩니다. 분 단위로 입력할 수 있습니다. 최소 설정값은 **30**분, 최대 설정값은 **10,080**분(7일)입니다.



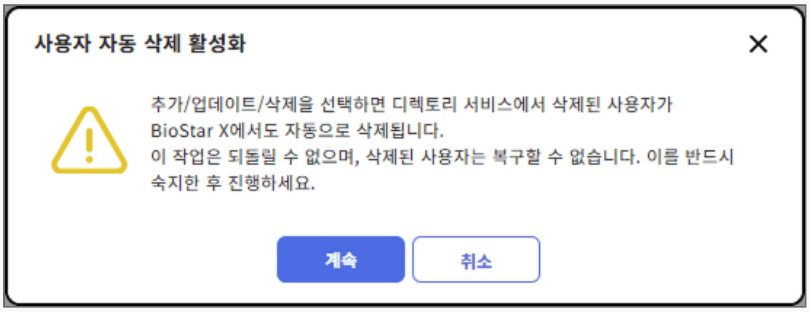
- **마지막 동기화**: 가장 최근에 동기화한 날짜와 시간을 확인할 수 있습니다.

주의

- **추가/업데이트만** 모드에서는 같은 이름의 사용자 그룹과 동일한 사용자 아이디(User ID)를 삭제하지 않고 유지합니다.
- **추가/업데이트/삭제** 모드에서는:
  - **같은 이름의 그룹이 이미 있는 경우**: 그룹이 새로 생성되지 않고 기존 그룹의 정보를 유지합니다. 다만 해당 그룹에 속한 사용자는 디렉토리 서비스의 최신 정보로 반영하기 위해 모두 제거한 후 다시 추가합니다. 단, 해당 그룹의 같은 이름 사용자는 유지합니다.
  - **BioStar X에서 생성된 사용자**: BioStar X에서 직접 생성한 사용자는 디렉토리 서비스와 연결되지 않은 상태입니다. 동기화 시 이들 사용자의 정보가 디렉토리 서비스와 연결되도록 업데이트합니다.
  - **제한사항**: 동기화 후 동일 이름의 그룹이 이미 있다면, 해당 그룹의 정보와 소속 사용자가 정상적으로 동기화되지 않을 수 있습니다.
- 디렉토리 연동을 설정한 상태에서 BioStar X v1.0.2로 업그레이드한 경우 동기화 모드는 **추가/업데이트/삭제**로 기본 설정됩니다.

알아두기

- **동기화** 버튼을 클릭할 때마다 선택한 동기화 모드로 디렉토리 서비스와 사용자 정보를 동기화합니다.
- **추가/업데이트/삭제** 모드를 선택하면 경고 메시지가 나타납니다. 메시지를 확인하고 계속하려면 **계속** 버튼을, 취소하려면 **취소** 버튼을 클릭하세요.



- 동기화 기능을 통해 연동할 때 특정 사용자를 동기화에서 제외하려면 디렉토리 연동 제외를 참고하세요.
- 동기화되는 사용자 아이디 또는 사용자 이름에 BioStar X에서 허용하지 않는 문자가 포함되어 있다면, 해당 문자만 제외한 값으로 등록합니다. 단, 사용자 아이디의 마침표(`.`), 사용자 이름의 마침표(`.`) 및 홑따옴표(`'`)는 제외 대상에서 빠지므로 원본 그대로 유지됩니다. 허용하지 않는 문자에 대한 자세한 내용은 사용자 ID 및 이름 입력 규칙을 참고하세요.

1 설정 저장

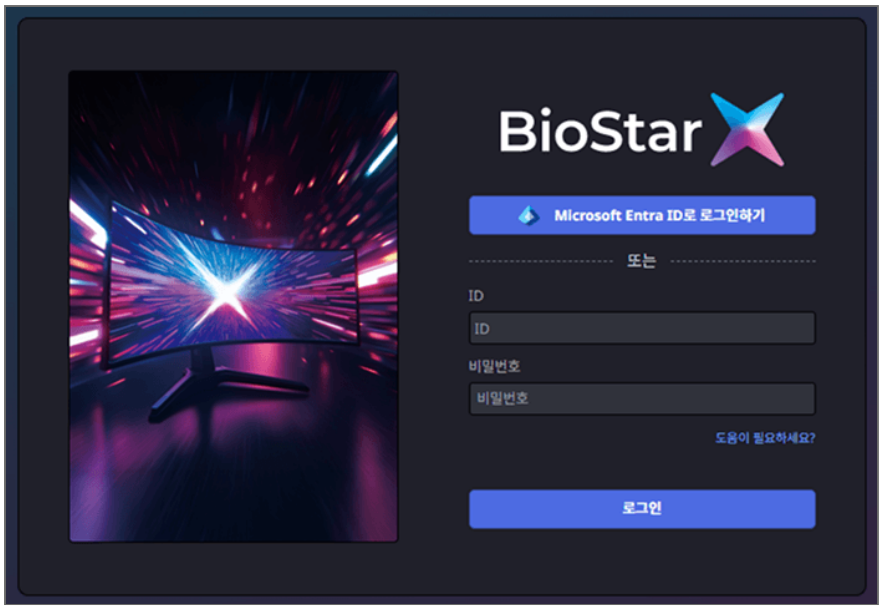
디렉토리 연동 설정을 모두 완료한 후 저장하려면 화면 가장 아래에 **확인** 버튼을 클릭하세요. 설정 결과를 확인하려면 설정 결과 확인을 참고하세요.

설정 결과 확인

Entra ID 또는 Active Directory와 연동 설정을 완료하고, 화면 아래에 **확인** 버튼을 클릭하세요. 다음 항목을 참고해 동기화된 설정을 확인할 수 있습니다.

- **사용자** 메뉴에서 동기화된 사용자 목록을 확인할 수 있습니다.
- Entra ID 또는 Active Directory로 로그인 설정을 완료한 후, BioStar X에 로그인할 때 **Microsoft Entra ID로 로그인하기** 버튼을

확인할 수 있습니다.



지원하지 않는 문자 처리

Entra ID 또는 **Active Directory**의 사용자 아이디 또는 사용자 이름에 **BioStar X**에서 지원하지 않는 문자가 포함되어 있다면, 시스템은 지원하지 않는 문자만 제거한 값으로 사용자를 동기화합니다.

> *예를 들어 디렉토리 서비스의 사용자 아이디가 `john/doe`이고 사용자 이름이 `John<Doe>`라면, **BioStar X**에는 각각 `johndoe`, `JohnDoe`로 등록합니다.*

알아두기

- 사용자 이름의 마침표(`.`)와 홑따옴표(`'`)는 지원하지 않는 문자에서 제외되어 디렉토리 서비스 값 그대로 등록합니다.

  > *예: `O'Brien`, `John.Doe` → 디렉토리 서비스 값 그대로 등록*

- 사용자 아이디의 마침표(`.`)는 지원하지 않는 문자에서 제외되어 디렉토리 서비스 값 그대로 등록되지만, 홑따옴표(`'`)는 사용자 아이디에서 사용할 수 없는 문자이므로 제거된 값으로 등록됩니다.

  > *디렉토리 서비스 사용자 아이디 예:*
  >
  > – `O'Brien` → `OBrien`로 등록
  >
  > – `john.doe` → `john.doe` 그대로 등록

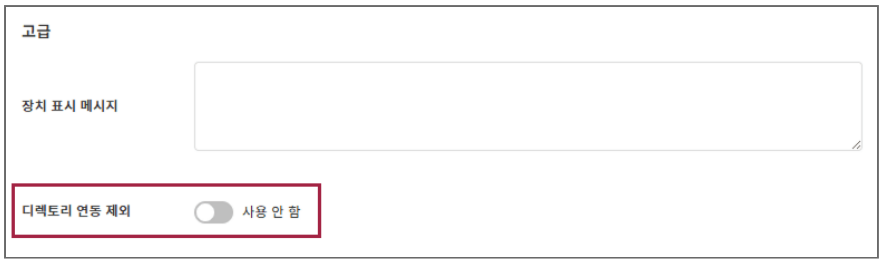
- 사용자 ID 및 이름 입력 규칙에 대한 자세한 내용은 사용자 기본 정보 입력하기을 참고하세요.

디렉토리 연동 제외

디렉토리 연동 기능을 통해 **Entra ID** 또는 **Active Directory**와 연동할 경우, 디렉토리 서비스에 존재하지 않는 사용자는 **BioStar X**에서 삭제될 수 있습니다. 삭제되지 않길 원하는 사용자가 있다면 아래 방법을 통해 연동에서 제외할 수 있습니다.

1. **BioStar X**에 관리자 아이디로 로그인하세요.
2. **사용자** 메뉴로 이동하세요.
3. **모든 사용자** 목록에서 연동에서 제외할 사용자를 클릭하세요.

4. 선택한 사용자의 상세 정보 화면이 나타나면 **고급** 섹션에서 **디렉토리 연동 제외** 옵션을 활성화하세요.



5. **확인** 버튼을 클릭하세요.

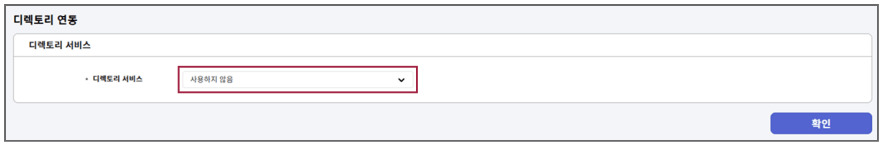
선택한 사용자는 **디렉토리 연동** 기능을 사용할 때 연동에서 제외됩니다.

> **알아두기**
> 다음에 해당하는 사용자는 자동으로 연동에서 제외됩니다.
> - 사용자 이름의 맨 앞에는 `&@~`를 연속으로 시작하는 경우
> - 사용자 아이디 또는 사용자 이름 값이 비어 있는 경우
> - 사용자 아이디(최대 32자) 또는 사용자 이름(최대 48자)의 길이 한도를 초과하는 경우
> - 사용자 아이디가 `admin`처럼 시스템에서 예약한 값과 같은 경우
> - 사용자 아이디가 마침표 하나(`.`) 또는 마침표 두 개(`..`)인 경우

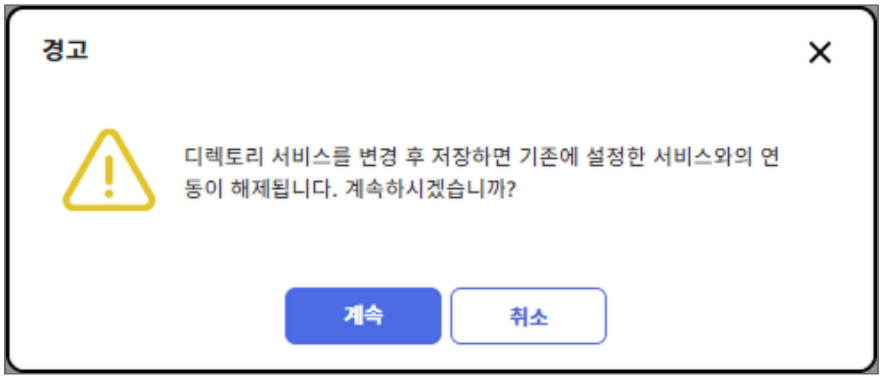
디렉토리 연동 해제

디렉토리 서비스 기능을 해제하려면 다음 안내에 따라 진행하세요.

1. **BioStar X**에 관리자 아이디로 로그인하세요.
2. **시스템** → **디렉토리 연동**을 클릭하세요.
3. **디렉토리 서비스** 항목에서 **사용하지 않음**을 선택하세요.



4. **경고** 메시지가 나타나면 **계속** 버튼을 클릭하세요.



5. 화면 하단의 **확인** 버튼을 클릭하세요.

주의

디렉토리 서비스 기능을 **사용하지 않음**으로 설정하면, **BioStar X**에서 **Entra ID** 또는 **Active Directory**와 연동된 모든 설정이 해제됩니다. 연동된 사용자 및 그룹 정보는 삭제되지 않지만, 이후에는 동기화되지 않습니다. 연동을 해제하기 전에 반드시 확인하세요.

리모트 액세스 설정하기

리모트 액세스(Remote Access)는 ngrok 서비스를 통해 외부 네트워크에서 내부 네트워크로 안전하게 접속할 수 있는 기능입니다. 이 기능을 사용하면 방화벽 설정이나 포트 포워딩 없이도 원격지에서 **BioStar X** 서버에 접속할 수 있습니다.

알아두기

- 리모트 액세스(Remote Access) 기능은 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요. 리모트 액세스 라이선스는 연간 구독 라이선스입니다.
- 리모트 액세스 라이선스를 구매하면 슈프리마에서는 리모트 액세스 라이선스 발급 및 리모트 액세스 사용을 위한 ngrok 슈프리마 사이트의 bot 계정, 엔드포인트를 생성하고 라이선스 문서를 사용자에게 제공합니다.

주의

- 리모트 액세스(Remote Access) 기능은 제3자 서비스인 ngrok의 터널링 서비스를 통해 제공됩니다. 기능 사용 전 반드시 Remote Access 기능 사용 동의 약관을 확인하세요.
- BioStar X는 단순히 ngrok API를 호출하여 연결을 지원할 뿐, 인터넷 연결의 보안성, 안전성, 연속성은 ngrok 서비스에 전적으로 의존합니다. 따라서 본 기능 사용 중 발생할 수 있는 보안 사고, 데이터 손실, 시스템 침해 등에 대하여 슈프리마는 어떠한 책임도 지지 않습니다.

언제 사용하나요?

다음과 같은 상황에서 리모트 액세스 기능을 사용하세요.

- 외부 네트워크에서 사내 **BioStar X** 서버에 접속해야 할 때
- 방화벽이나 NAT 환경으로 인해 직접 접속이 어려운 경우
- 복잡한 네트워크 설정 없이 간편하게 원격 접속을 구성하고 싶을 때
- 임시로 외부 접속 권한을 제공해야 하는 경우

리모트 액세스 설정

1 리모트 액세스 라이선스 활성화

1. **BioStar X** 관리자 아이디로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.

3. 화면 왼쪽 사이드바에서 **라이선스** → **BioStar X 라이선스**를 클릭하세요.
4. 슈프리마에서 전달한 리모트 액세스 라이선스 키와 관리자 이름을 입력하고 **활성화** 버튼을 클릭하세요.

> **알아두기**
> 라이선스 등록에 대한 자세한 내용은 BioStar X 라이선스를 참고하세요.

2 리모트 액세스 활성화

1. BioStar X 관리자 아이디로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **시스템** → **리모트 액세스**를 클릭하세요.
4. **ngrok 리모트 액세스** 섹션에서 **리모트 액세스** 옵션을 **사용**으로 변경하세요.



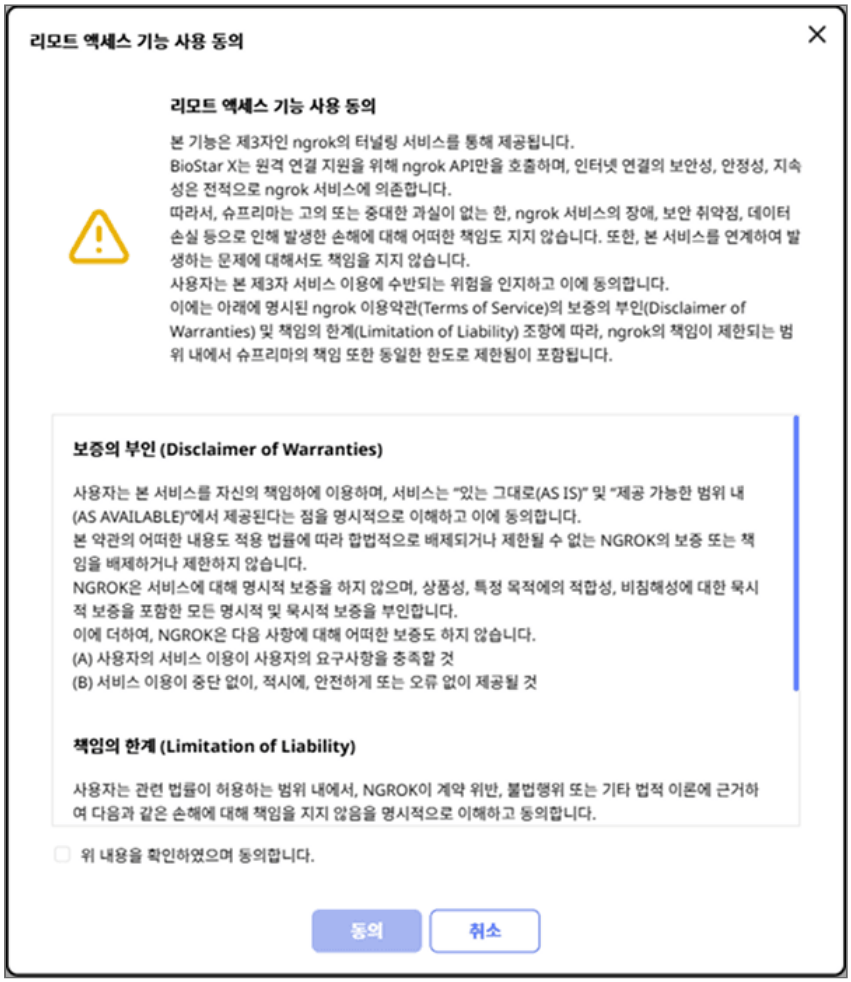
3 ngrok 설정 정보 입력

슈프리마에서 전달받은 ngrok 설정 정보를 입력하세요.

- **인증 토큰**: Authtoken을 입력하세요.
- **URL**: 엔드포인트 URL을 입력하세요. URL은 `https://subdomain.bsx.ngrok.app` 형식입니다.

> **알아두기**
> 서브 도메인(`subdomain`)은 아래와 같은 규칙을 따릅니다. 규칙을 준수하지 않은 서브 도메인은 사용할 수 없습니다.
> - 영문 알파벳(A-Z, a-z), 숫자(0-9), 하이픈(`-`)만 사용할 수 있습니다.
> - 특수 문자, 공백은 사용할 수 없습니다.

1. 모든 정보를 입력한 후 **확인** 버튼을 클릭하세요.
2. **리모트 액세스 기능 사용 동의** 창이 나타나면 내용을 확인하세요.



3. 약관 동의를 위한 체크박스를 선택하고 **동의** 버튼을 클릭하세요.

엔드포인트 URL 접속

설정을 완료하고 **URL** 항목에 입력한 엔드포인트 URL을 통해 외부 네트워크에서 **BioStar X** 서버에 접속할 수 있는지 확인하세요.

> **알아두기**
>
> - 엔드포인트 URL 주소로 접속하면 **설정** → **감사 추적** → **출입 통제 감사 로그**에서 접속 기록을 확인할 수 있습니다.
>
> *예: [Remote Access] 192.168.1.100*
>
> - 외부 네트워크에서 엔드포인트 URL을 통해 접속할 수 없다면 라이선스를 발급받은 영업점 또는 대리점에 문의하세요.

가상 장치 이벤트 로그 연동하기

가상 장치 기능을 사용하면, 근태 관리 기능을 연동할 때 모바일 앱이나 타사 서비스에서 발생한 출근, 퇴근 등의 이벤트를 **BioStar X**에 직접 기록할 수 있습니다. 실제 물리적 장치 없이도 이벤트 로그를 체계적으로 관리할 수 있어 외부 시스템과의 연동에 유용합니다.

언제 사용하나요?

다음과 같은 상황에서 가상 장치 이벤트 로그 연동 기능을 사용하세요.

- 외부 근태 관리 시스템의 이벤트를 **BioStar X**에서 통합 관리해야 할 때
- 모바일 앱이나 외부 시스템에서 발생한 출입 기록(Punch Log)을 **BioStar X**에 직접 저장해야 할 때(데이터베이스 연동 없이 출근/퇴근 이벤트 기록)
- 타사 애플리케이션이나 서비스에서 **BioStar X** API를 통해 직접 이벤트를 전송해야 할 때

시작하기 전에

이벤트 로그 API 라이선스가 활성화되어 있어야 합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

> **알아두기**
> 라이선스 적용에 대한 자세한 내용은 BioStar X 라이선스를 참고하세요.

가상 장치 등록

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **장치** → **장치**를 클릭하세요.
3. 장치 목록에서 화면 오른쪽 상단의 ••• 버튼을 클릭한 후 **가상 장치 추가**를 선택하세요.



4. **가상 장치 추가** 화면이 나타나면 설정 정보를 입력하세요.



   - **장치 이름**: 가상 장치의 이름을 입력하세요.
   - **장치 그룹**: 가상 장치를 할당할 그룹을 선택하세요.
   - **장치 ID**: 가상 장치의 고유 ID를 입력하세요. 기존 장치 ID와 중복되지 않는 범위 내에서 지정해야 합니다.
   - **설명**: 가상 장치에 대한 설명을 입력하세요.
5. 가상 장치를 등록하려면 화면 오른쪽 하단의 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - **장치 ID**는 100000~999999 범위 내에서 지정할 수 있습니다. 기존 슈프리마 장치 ID와 중복되지 않는 범위 내에서 지정해야 합니다.
> - 이미 생성한 **장치 ID**의 값은 수정할 수 없습니다.

장치 그룹 관리

가상 장치도 일반 장치와 동일하게 장치 그룹 기능을 사용할 수 있습니다.

- 기존 장치들과 동일한 그룹에 배치할 수 있습니다.
- 그룹 권한이 있으면 해당 그룹 내 가상 장치에도 권한을 부여할 수 있습니다.

> **알아두기**
> 장치 그룹에 대한 자세한 내용은 장치 그룹 관리하기를 참고하세요.

가상 장치 제약 사항

- 가상 장치는 다음 메뉴에서만 표시됩니다.
  - **설정** → **장치** → **장치**
  - **모니터링** 메뉴의 모든 이벤트 로그 조회 및 이벤트 로그 미리보기
  - **데이터** 메뉴의 이벤트 로그 조회
- 가상 장치는 출입문 및 **고급 출입 통제**에서 출입 제어 기능을 사용할 수 없습니다.
- **근태 관리** 설정을 위한 장치로 지정할 수 없습니다.
- **모니터링** 메뉴의 사이드바에서 장치 목록으로 표시되지 않습니다.
- 장치 제어 기능을 사용할 수 없습니다.
- **멀티 커뮤니케이션 서버** 라이선스의 장치 수에 포함되지 않습니다.

API를 통한 이벤트 로그 기록

지원 이벤트 유형

다음 이벤트 유형만 기록할 수 있습니다.

- **출입 허용** (Access granted: `4088`)
- **출입 거부** (Access denied: `6400`)

API Parameters

이벤트 로그 기록 시 다음 파라미터를 제공해야 합니다.

파라미터	설명	필수 여부
dev_id	등록된 가상 장치 ID만 허용	필수
evt	Access Granted 또는 Access Denied	필수
datetime	이벤트 발생 시간	필수
user_id	사용자 ID	필수
tna_key	지정된 값으로만 입력 가능	선택

Request example

```
{
  "packet_device_id" : 100003, // required
  "is_virtual_device" : "true", // required
  "events":[ //4088 access granted, 6400 access denied
    {
      "dev_id": 100003, // required
      "evt": 6400, // required
      "datetime": "2025-08-21T14:12:00Z", // required
      "user_id": "2", // required
      "tna_key": "1"
    },
    {
      "dev_id": 100003,
      "evt": 6400,
      "datetime": "2025-08-21T14:13:01Z",
      "user_id": "2",
      "tna_key": "1"
    }
  ]
}
```

Response example

```
{
  "Response": {
    "code": "0",
    "link": "https://support.supremainc.com/en/support/home",
    "message": "Success"
  }
}
```

알아두기

- 단일 API 호출로 하나의 가상 장치에 대한 여러 이벤트 로그를 한번에 기록할 수 있습니다.
- API 사용에 대한 자세한 내용은 BioStar X API를 참고하세요.

이벤트 로그 조회

가상 장치를 통해 기록된 이벤트 로그는 메뉴에서 조회할 수 있습니다.

- **모니터링**: 모든 이벤트 조회 및 필터, 이벤트 프리뷰
- **데이터**: 모든 이벤트 조회 및 필터

> **알아두기**
>
> - **모니터링** 메뉴에서 이벤트 조회에 대한 자세한 내용은 이벤트 모니터링하기를 참고하세요.
> - **데이터** 메뉴에 대한 자세한 내용은 리포트 생성하기를 참고하세요.

감사 추적

이벤트 로그 기록 시 아래 예시와 같이 감사 추적이 기록됩니다.

```
Access Granted, 2025/08/05 03:37:49, 12층 출입문 외부, Administrator(1)
```

> **알아두기**
>
> - 이벤트를 일괄로 기록하더라도 각 이벤트마다 개별 감사 추적 항목이 생성됩니다.
> - **감사 추적**에 대한 자세한 내용은 감사 추적 관리하기를 참고하세요.

문제 해결

가상 장치 추가 버튼이 보이지 않는 경우

이벤트 로그 API 라이선스를 활성화했는지 확인하세요.

API 호출이 실패하는 경우

- **이벤트 로그 API** 라이선스를 활성화했는지 확인하세요.
- 장치 ID가 등록된 가상 장치인지 확인하세요.
- API 파라미터 형식이 올바른지 확인하세요.

이벤트가 조회되지 않는 경우

- 기록한 장치가 올바른 가상 장치 ID인지 확인하세요.
- 이벤트 필터에서 해당 가상 장치가 선택되어 있는지 확인하세요.
- 이벤트 기록 시 오류가 발생하지 않았는지 감사 추적을 확인하세요.

플러그인

플러그인(Plugins)이란?

BioStar X 플러그인(Plugins)은 **BioStar X** 플랫폼의 확장 기능으로, 고객의 특별한 요구사항이나 기존 시스템과의 연동을 위해 추가 기능을 제공합니다.

> **알아두기**
>
> - 플러그인 기능을 사용하려면 플러그인 라이선스가 필요합니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
> - 플러그인 개발에 대한 자세한 내용은 BioStar X 플러그인 개발자 가이드를 참고하세요.

BioStar X 제공 플러그인

라이선스 추가 옵션을 통해 사용할 수 있는 플러그인 목록입니다.

- 근태 관리 사용하기
- 방문자 신청 및 관리하기

> **알아두기**
> 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

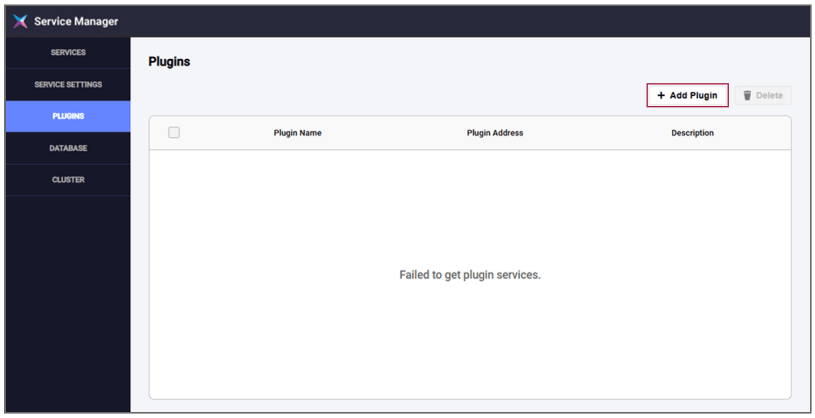
주요 활용 사례

BioStar X 플러그인(Plugins) 시스템을 통해 다양한 외부 시스템과 연동할 수 있습니다. 대표적인 활용 사례는 다음과 같습니다.

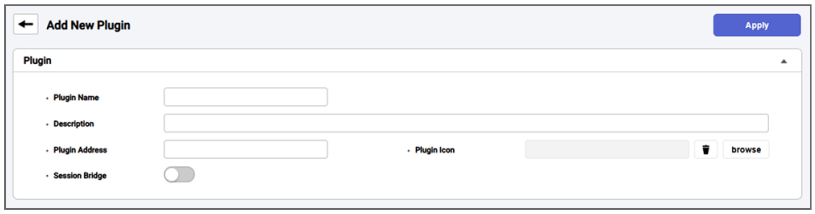
- **근태 관리 시스템**: 외부 T&A(Time & Attendance) 솔루션과 연동
- **방문자 관리 시스템**: 별도의 방문자 등록 및 관리 시스템과 연동
- **보고서 솔루션**: 사용자 정의 보고서 생성 및 분석 도구 연동
- **타사 시스템 연동**: ERP, HRM 등 기존 업무 시스템과의 데이터 연동

플러그인 등록

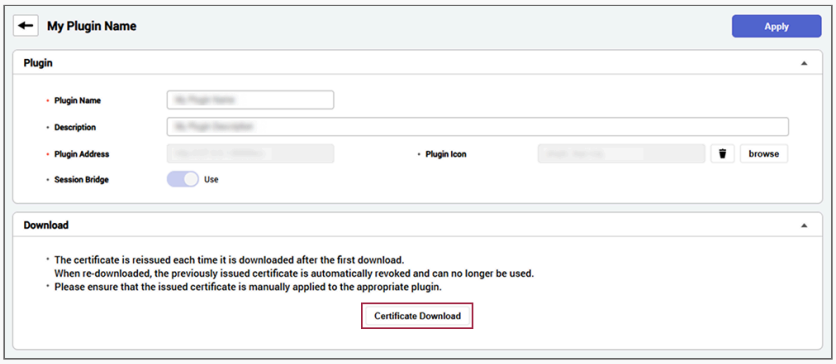
1. Windows에서 시작 → **BioStar X** → **BioStar X Service Manager**를 클릭하세요.
2. 화면 왼쪽 사이드 메뉴에서 **PLUGINS**를 클릭하세요.
3. 화면 오른쪽 상단의 **Add Plugin** 버튼을 클릭하세요.



4. **Add New Plugin** 화면에서 플러그인 정보를 입력하세요.



5. 플러그인 정보를 입력하고 등록을 완료하려면 **Apply** 버튼을 클릭하세요.

> **알아두기**
>
> **Session Bridge**를 활성화했다면 화면 하단에서 인증서를 다운로드할 수 있습니다. 인증서는 **BioStar X**와 플러그인 간의 보안 통신을 위해 필요합니다. 인증서를 분실했다면 새로 다운로드할 수 있습니다. 이때 기존 인증서는 무효화됩니다.
>
> 
>

플러그인 정보 입력

- **Plugin Name**: 플러그인의 이름을 입력하세요. 최대 48자까지 입력할 수 있습니다. 기존 등록한 플러그인과 같은 이름을 사용할 수 없습니다.
- **Description**: 플러그인의 설명을 입력하세요. 최대 500자까지 입력할 수 있습니다.
- **Plugin Address**: 플러그인의 주소를 입력하세요. `http://` 또는 `https://`로 시작하는 유효한 URL이어야 하며, 기존 등록한 플러그인과 같은 주소를 사용할 수 없습니다.
- **Plugin Icon**: 플러그인의 아이콘을 업로드하세요.
  - 지원되는 형식은 JPEG, PNG, SVG, GIF입니다.
  - 파일의 최대 크기는 1MB이며, 0KB 빈 파일은 업로드할 수 없습니다.

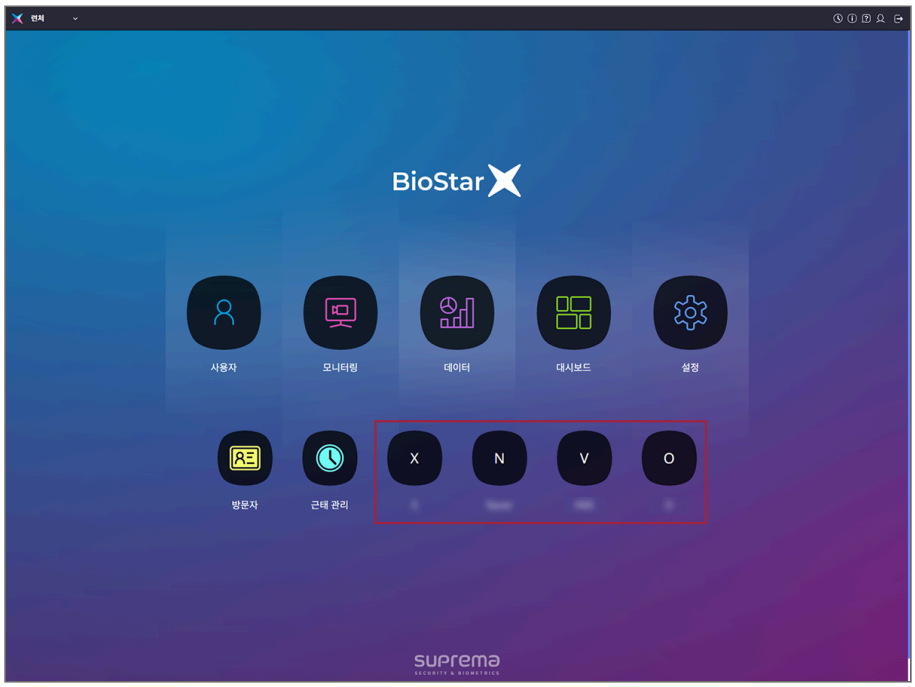
  - 업로드된 이미지는 104×104 픽셀로 자동 리사이징됩니다.

- **Session Bridge**: 세션 브리지를 사용하려면 활성화하세요. 이 기능을 사용하면 BioStar X 사용자의 권한을 자동 상속하여 플러그인 접근 시 별도 로그인이 필요 없습니다.

> **알아두기**
>
> - 아이콘을 업로드하지 않으면 플러그인 이름의 첫 글자로 아이콘이 자동 생성됩니다. 업로드한 아이콘은 버튼을 클릭해 삭제할 수 있으며, 삭제 시 자동 생성 아이콘으로 변경됩니다.
> - **Session Bridge**를 활성화하면 비활성화할 수 없으며, 보안상의 이유로 플러그인 주소를 변경할 수 없습니다.

런처 화면에서 확인

BioStar X의 **런처** 화면에서 추가한 플러그인을 확인할 수 있습니다.



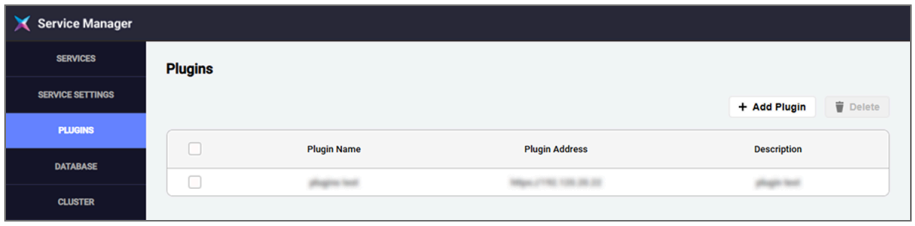
플러그인 관리

BioStar X Service Manager를 통해서 설치한 플러그인을 관리할 수 있습니다.

Windows에서 시작 → BioStar X → BioStar X Service Manager를 클릭하세요. BioStar X Service Manager 화면의 사이트 메뉴에서 **PLUGINS**를 클릭하세요.

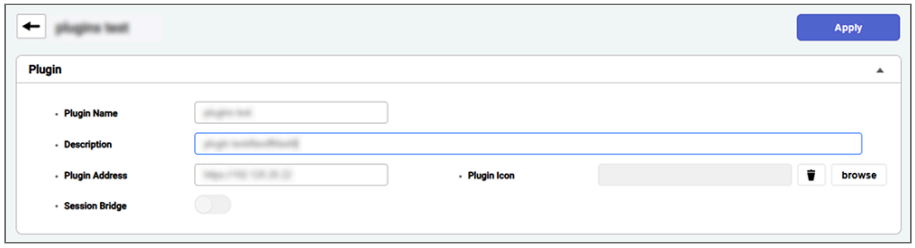
플러그인 목록 확인

사용자가 등록한 모든 플러그인을 확인할 수 있습니다.



플러그인 수정

플러그인 목록에서 수정할 플러그인을 클릭하세요. 플러그인 정보 수정 화면이 나타납니다. 플러그인 이름(**Plugin Name**), 설명(**Description**), 아이콘(**Plugin Icon**) 항목을 수정할 수 있습니다.



> **알아두기**
> **Plugin Address**는 **Session Bridge**를 활성화한 상태에서는 수정할 수 없습니다.

플러그인 삭제

1. 플러그인 목록에서 삭제할 플러그인의 가장 왼쪽에 체크 박스를 클릭해 선택하세요.
2. 화면 오른쪽 상단의 **Delete** 버튼을 클릭하세요.
3. 확인 메시지가 나타나면 **OK** 버튼을 클릭하세요.

> **알아두기**
> - 근태 관리 라이선스를 적용해 추가된 근태 관리(T&A) 플러그인은 삭제할 수 없습니다.
> - 근태 관리 플러그인은 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

근태 관리 사용하기

근태 관리 규칙을 설정하고, 장치를 통해 기록된 근무 기록을 확인하거나 보고서로 출력할 수 있습니다. 근태 관리 기능은 플러그인 형태로 제공되며 별도의 라이선스가 필요합니다.

> **알아두기**
> 근태 관리 기능은 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.

시작하기 전에

근태 관리 기능을 사용하려면 라이선스를 적용하고 별도의 설치 파일을 다운 받아 설치해야 합니다.

라이선스 적용

근태 관리 라이선스 적용 방법을 안내합니다. **BioStar X** 구입처로부터 근태 관리 라이선스를 구입한 후 다음 안내에 따라 라이선스를 적용하세요.

1. **BioStar X** 관리자 계정으로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **라이선스** → **BioStar X 라이선스**를 클릭하세요.
4. **라이선스 활성화**에서 **등록 관리자**와 **라이선스 키** 항목을 차례로 입력하세요.



5. **활성화** 버튼을 클릭하세요.

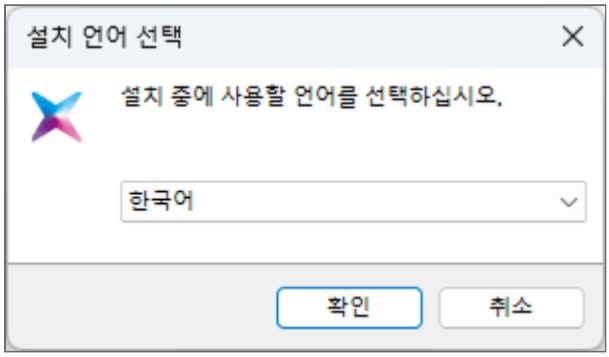
등록한 라이선스는 **활성화된 라이선스**에서 확인할 수 있습니다.

> **알아두기**
> 폐쇄된 네트워크 환경이나 인터넷 연결이 제한된 오프라인 상태에서 라이선스를 활성화하려면 BioStar X 라이선스를 참고하세요.

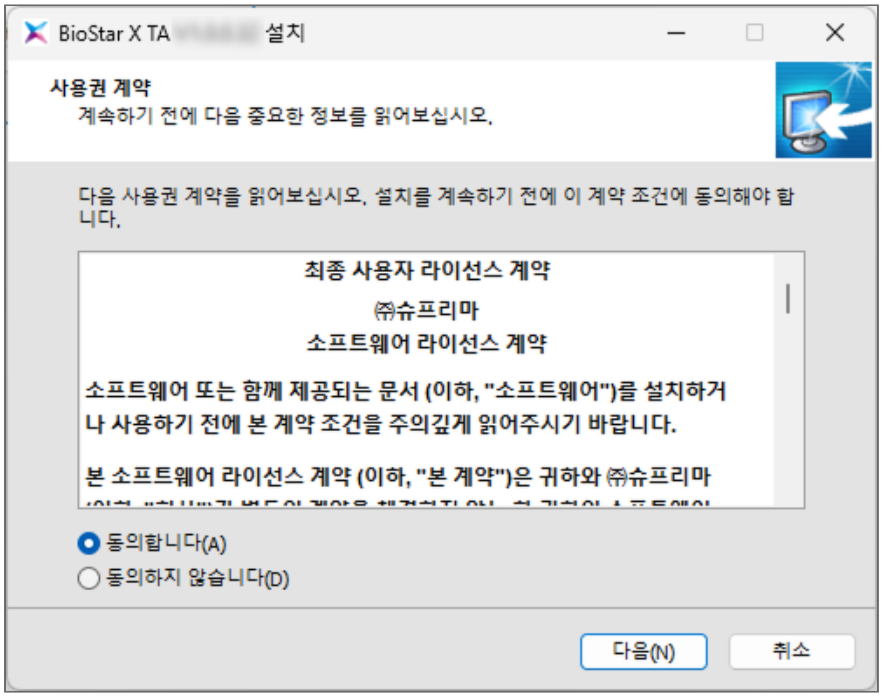
플러그인 설치

근태 관리 기능을 사용하려면 별도의 설치 파일을 다운 받아 설치해야 합니다. 다음 안내에 따라 플러그인을 설치하세요.

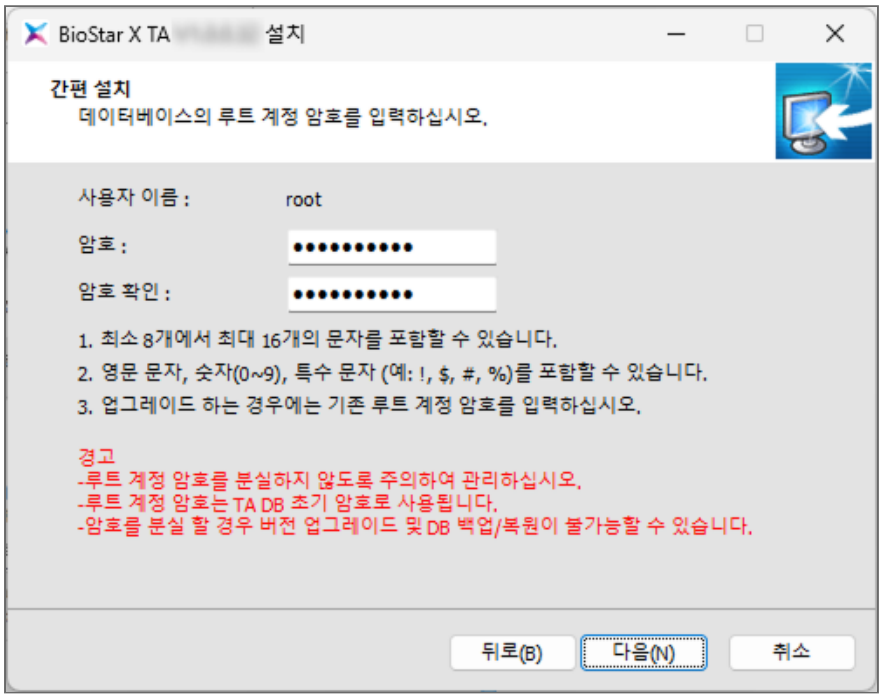
1. 슈프리마 다운로드 센터로 접속해 근태 관리 플러그인 설치 파일(*BioStar X TA.X.Y.Z.BB.exe*)을 다운로드하세요.
2. 설치 파일을 실행하고 안내에 따라 설치를 완료하세요.
3. 다운로드한 설치 파일을 실행하세요.
4. 사용할 언어를 선택하고 **확인** 버튼을 선택하세요.



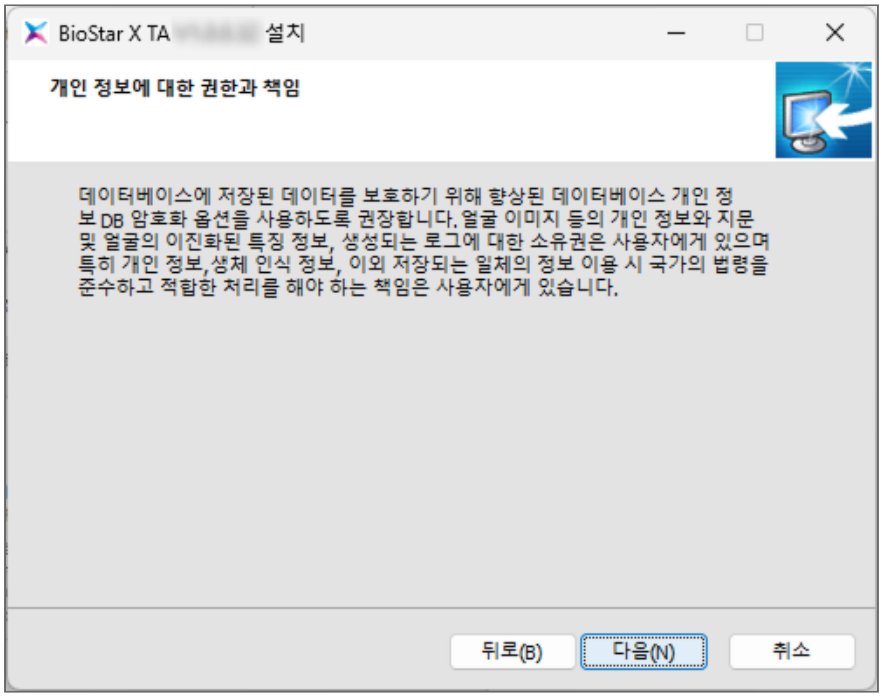
5. 설치를 계속하려면 **동의합니다**를 선택하고 **다음** 버튼을 클릭하세요.



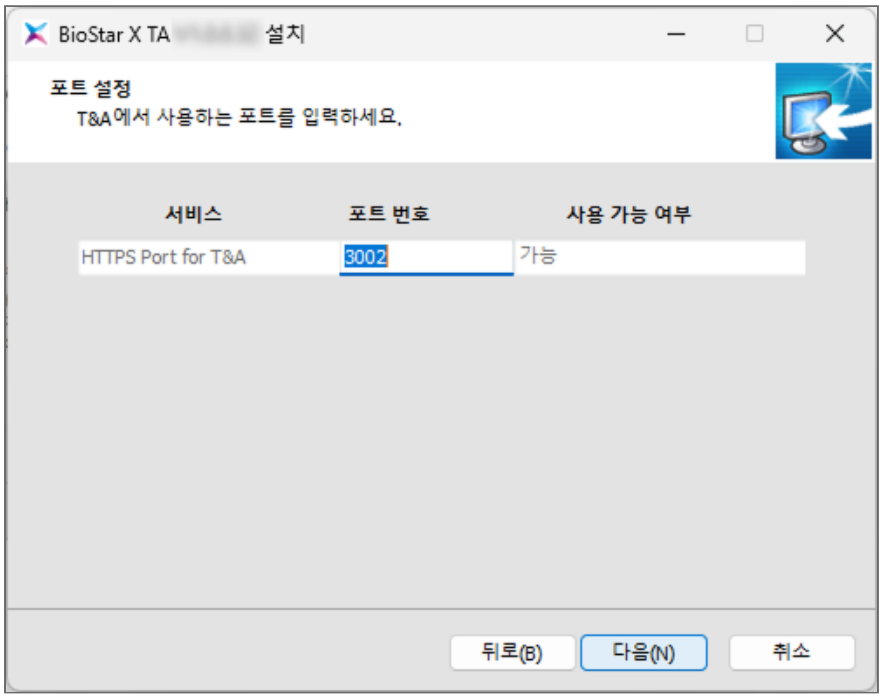
6. 데이터베이스의 루트(root) 계정 암호를 입력하고 **다음** 버튼을 클릭하세요.



7. 데이터베이스에 저장되는 개인 정보 관리 권한 및 책임에 대한 안내를 읽고 설치를 계속하려면 **다음** 버튼을 클릭하세요.

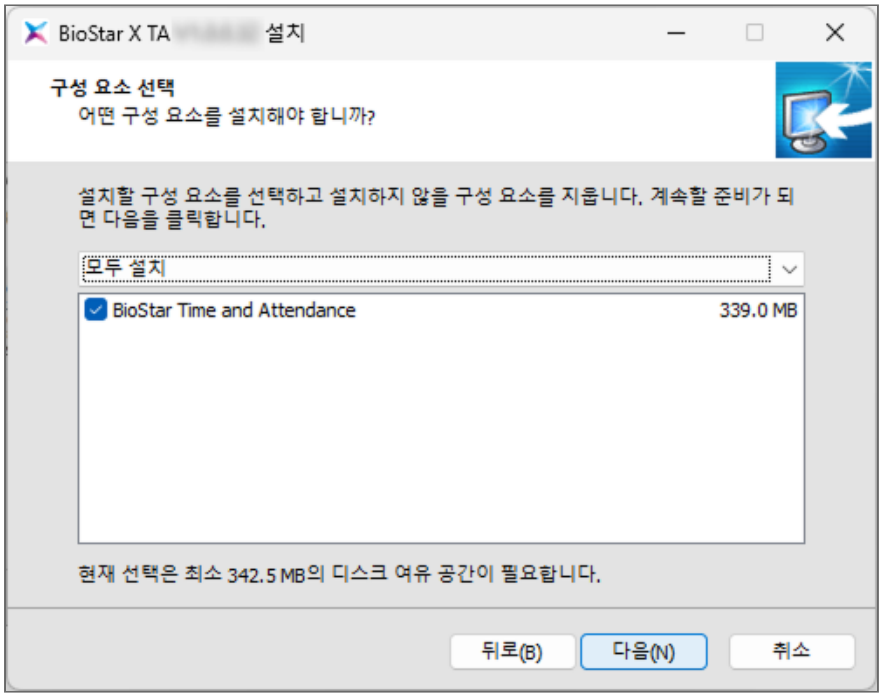


8. **BioStar X**와 통신하기 위한 포트를 설정하고 **다음** 버튼을 클릭하세요.

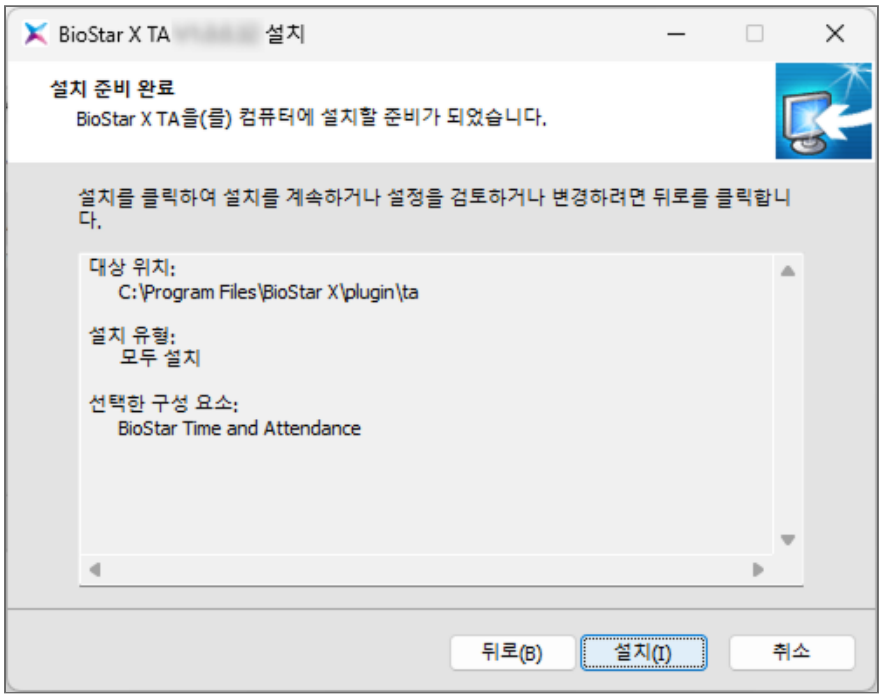


> 포트 번호는 기본값(3002)을 사용하거나 다른 포트 번호로 변경할 수 있습니다. 포트 번호를 변경한 경우 방화벽에서 해당 포트가 열려 있는지 확인하세요.

9. 설치 구성 요소를 선택한 후 **다음** 버튼을 클릭하세요.



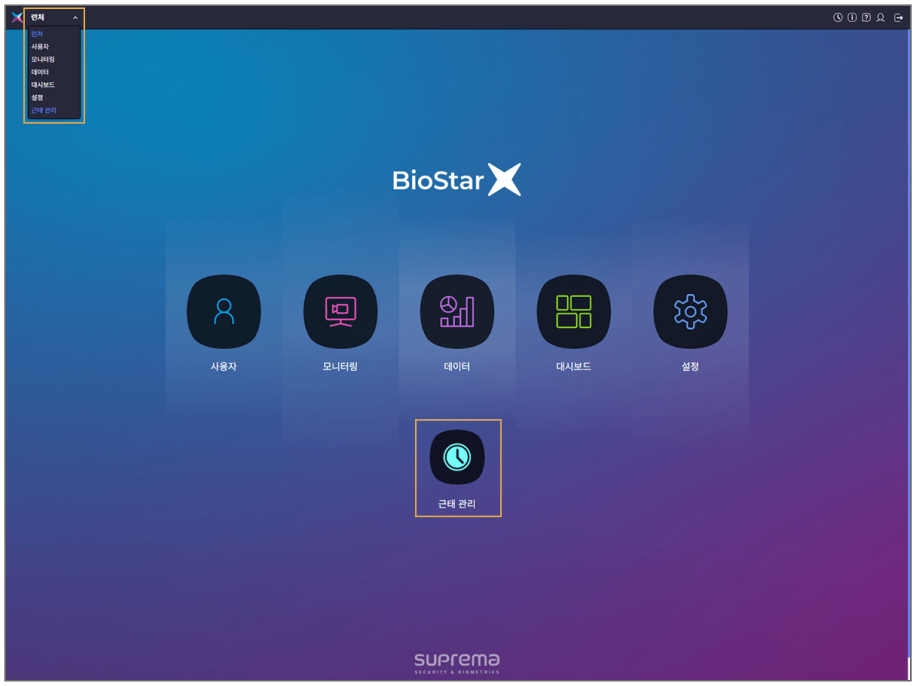
10. 모든 설치 준비를 완료했다면 **설치** 버튼을 클릭하세요.



> **알아두기**
>
> - 다운로드한 파일명에서 X.Y.Z 는 버전 정보이며, BB 는 빌드 번호입니다.
> - 데이터베이스의 루트(root) 계정 암호는 **BioStar X**를 설치할 때 사용한 암호를 사용하세요.

근태 관리 메뉴

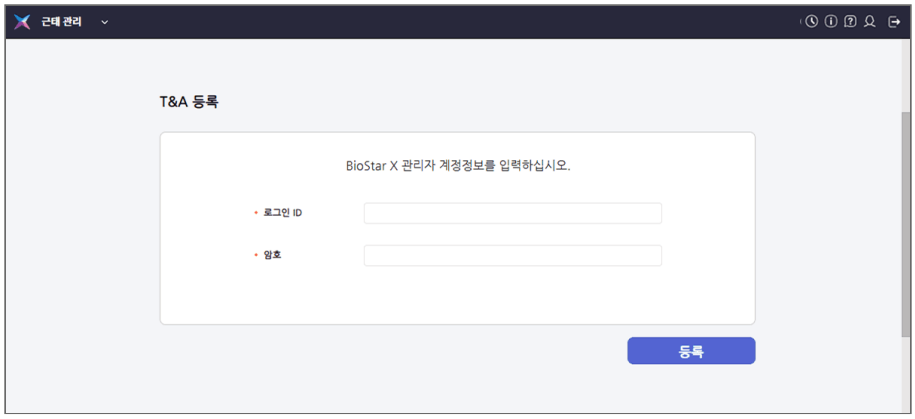
근태 관리 라이선스와 플러그인 설치를 완료하면 **런처** 페이지에서 **근태 관리** 메뉴가 추가됩니다.



런처 페이지에서 **근태 관리** 아이콘을 클릭하거나, 화면 왼쪽 상단의 바로 가기 목록에서 **근태 관리**를 선택하세요.

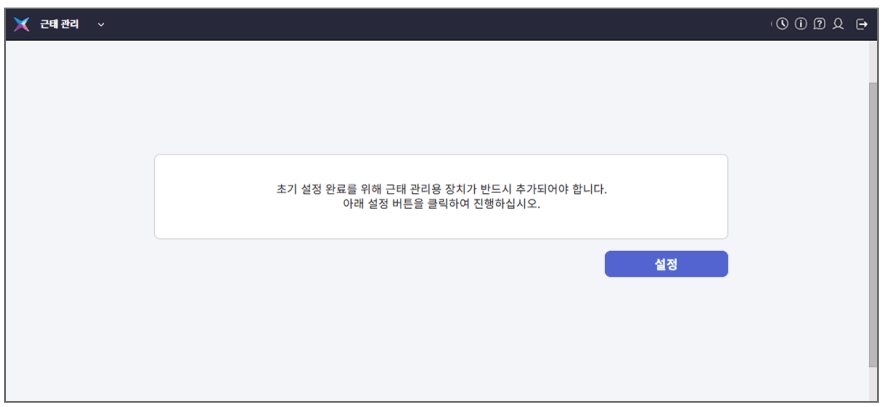
근태 관리 로그인

근태 관리 기능에 최초 진입 시 별도의 로그인 화면이 나타납니다. **BioStar X** 관리자 계정으로 로그인하세요. 근태 관리 기능에 관리자 계정으로 로그인하면 이후로 별도의 로그인 과정 없이 근태 관리 기능을 사용할 수 있습니다.

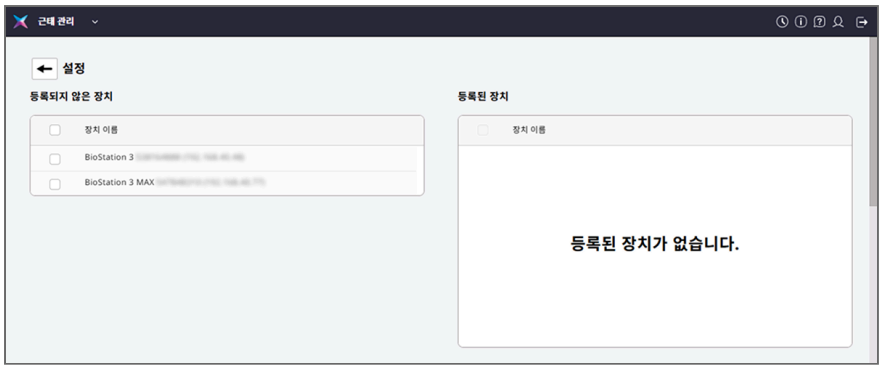


초기 설정

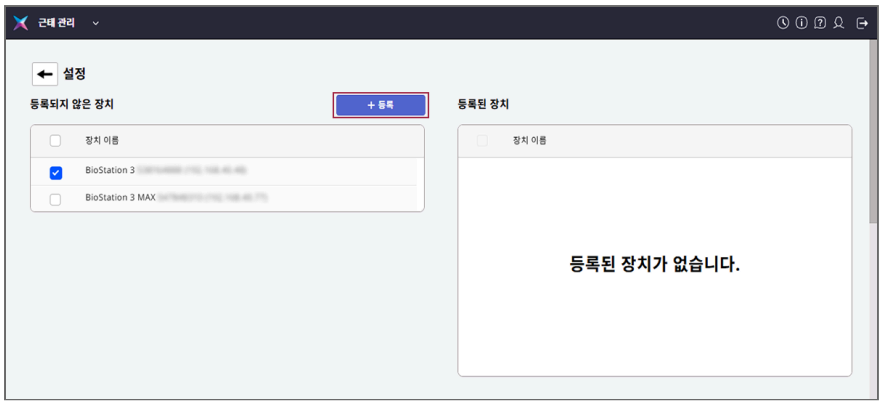
1. 근태 관리 기능에 최초 로그인하면 초기 설정을 위해 근태 관리자용 장치를 추가해야 합니다. 화면에서 **설정** 버튼을 클릭하세요.



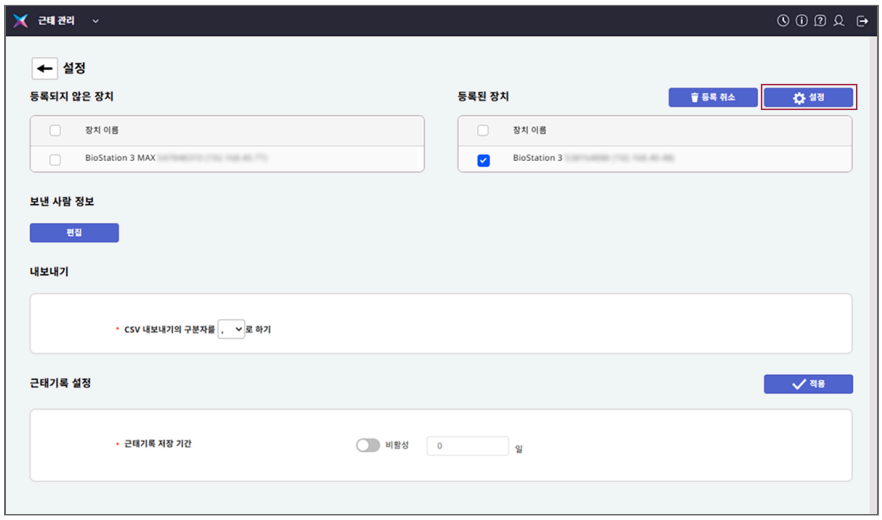
2. 장치 목록에서 근태 관리를 위한 장치를 선택하세요.



3. 활성화된 ＋ **등록** 버튼을 클릭하세요.



4. 선택한 장치가 **등록된 장치** 목록에 표시되면 **설정** 버튼을 클릭하세요.



5. **설정** 창이 나타나면 근태 관리를 위한 기본 설정을 완료하세요.

근태 모드 설정

근태 모드 및 근태 이벤트 설정을 진행하세요.



- **근태 모드**: 근태 이벤트 등록 방법을 선택하세요.
  - **수동 변경**: 인증할 때 사용자가 근태 이벤트를 선택할 수 있습니다.
  - **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.
  - **사용 안 함**: 근태 이벤트를 기록하지 않습니다.
- **근태 등록 필요**: 인증할 때 반드시 근태 이벤트를 등록하도록 설정할 수 있습니다. **근태 모드**를 **수동 변경**으로 설정했을 때 사용할 수 있습니다.
- **근태 이벤트**: 근태 이벤트의 이름을 수정하거나 **근태 모드**를 **자동 변경**으로 설정했을 때 사용되는 스케줄을 추가할 수 있습니다.
  - **근태 키**: 근태 등록에 사용할 수 있는 키 목록입니다.
  - **라벨**: 근태 키에 따른 근태 이벤트 이름을 변경할 수 있습니다.
  - **스케줄**: **근태 모드**를 **자동 변경** 설정하면 자동으로 변경할 스케줄을 설정할 수 있습니다. 스케줄 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

> **알아두기**
>
> - LCD 화면을 지원하지 않는 장치는 **근태 모드**를 **자동 변경**과 **고정**으로 설정할 수 있습니다. 고정된 근태 이벤트를 등록하거나 미리 설정된 스케줄에 따라 변경되는 근태 이벤트를 등록할 수 있습니다.
> - **자동 변경**과 **고정** 모드를 지원하는 장치 모델은 XPass Q2, XPass 2, XPass D2, BioEntry W3, BioEntry P2, BioEntry W2입니다.
> - **설정** 메뉴에 대한 자세한 내용은 근태 관리 설정하기를 참고하세요.

근무 규칙 설정하기

근무 스케줄을 시간, 일, 주간 단위로 설정하여 근태 관리 규칙을 구성하는 방법을 안내합니다.

근무 규칙을 처음 등록하다면 아래 순서에 따라 설정하세요.

1 시간 규칙

근태 기록 관리, 초과 근무, 부재에 대한 시간 규칙을 설정할 수 있습니다. 시간당 가중치를 설정할 수 있으며, 한 눈에 알아보기 쉽도록 색상을 지정하여 표시할 수 있습니다.

시간 규칙 설정에 대한 자세한 내용은 시간 규칙 설정하기를 참고하세요.

2 일일 근무 규칙

하루(24시간) 단위의 근무 규칙을 설정할 수 있습니다. 근무 규칙은 시간에 따른 시간 규칙 설정, 하루 시작 시간 설정, 시간 반올림 규칙 등을 포함합니다.

일일 근무 규칙 설정에 대한 자세한 내용은 일일 근무 규칙 설정하기를 참고하세요.

3 주간 근무 규칙

설정된 하루 단위의 근무 규칙으로 주간 근무 규칙을 설정할 수 있습니다. 주별, 일별 주간 근무 규칙을 설정할 수 있습니다.

주간 근무 규칙 설정에 대한 자세한 내용은 주간 근무 규칙 설정하기를 참고하세요.

4 기타 근무 규칙

일일 근무 규칙에 초과 근무 시간 규칙을 추가하지 않았을 때 유용하게 사용할 수 있습니다. 일일 근무 규칙에서 설정하는 초과 근무는 시작 시간과 종료 시간을 갖고 있으나 **기타 근무 규칙**은 정규 근무 시간 범위를 넘어선 총 시간을 계산합니다. **기타 근무 규칙**은 일별/주별/월별 총 초과 근무 시간으로 관리할 때 편리하게 사용할 수 있으며 **기타 근무 규칙**을 설정하면 근무 규칙에 추가된 초과 근무 시간 규칙 대신 적용됩니다.

기타 근무 규칙 설정에 대한 자세한 내용은 기타 근무 규칙 설정하기를 참고하세요.

5 근무 스케줄

이전 단계에서 설정한 근무 스케줄을 적용할 기간, 사용자, 기타 근무 규칙, 휴가 일정을 설정할 수 있습니다.

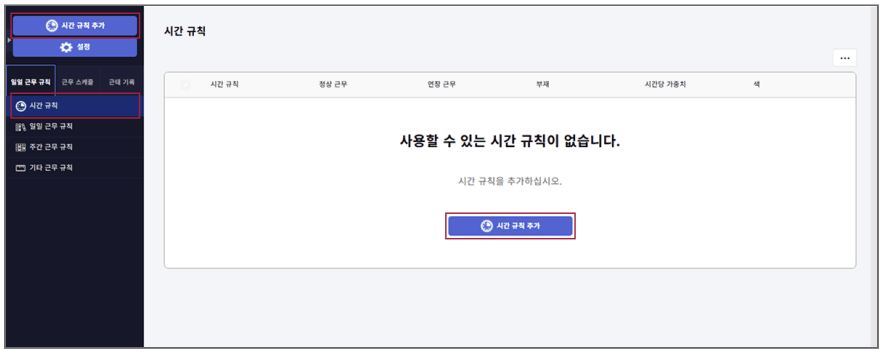
근무 스케줄 설정에 대한 자세한 내용은 근무 스케줄 설정하기를 참고하세요.

시간 규칙 설정하기

근무 시간 계산에 사용될 시간 규칙 설정을 안내합니다. 정상 근무용 시간 규칙, 연장 근무용 시간 규칙, 부재용 시간 규칙을 설정할 수 있습니다. 각 시간 규칙은 시간당 가중치를 다르게 지정하여 사용할 수 있습니다.

시간 규칙 추가

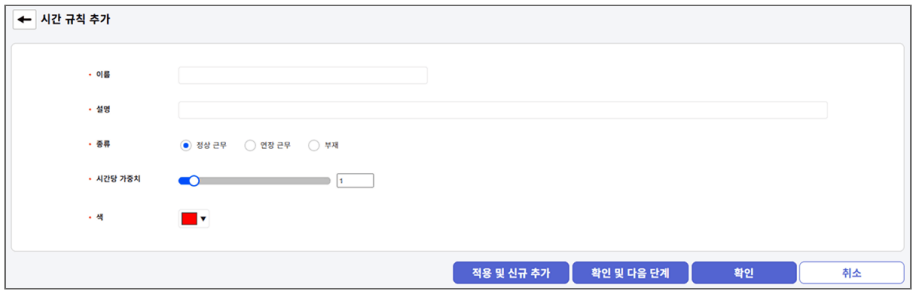
1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **일일 근무 규칙** → **시간 규칙**을 클릭하세요.
3. **시간 규칙 추가** 버튼을 클릭하세요.



4. **시간 규칙 추가** 화면이 나타나면 각 항목을 설정하세요.

> **알아두기**
>
> - 설정을 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.
> - 이어서 일일 근무 규칙을 추가하려면 **확인 및 다음 단계** 버튼을 클릭하세요.
> - 설정을 저장한 후 다른 **시간 규칙**을 추가하려면 **적용 및 신규 추가** 버튼을 클릭하세요.

설정 옵션 안내



- **이름**: 시간 규칙의 이름을 입력하세요.
- **설명**: 시간 규칙에 대한 설명을 입력하세요.
- **종류**: 시간 규칙의 종류를 선택하세요.
  - **정상 근무**: 정상 근무에 사용할 시간 규칙으로 설정합니다.
  - **연장 근무**: 연장 근무에 사용할 시간 규칙으로 설정합니다.
  - **부재**: 외출, 외근, 출장, 휴가 등에 사용할 시간 규칙으로 설정합니다.
- **시간당 가중치**: 시간 규칙에 따른 시간당 가중치를 설정하세요. **1**은 기본 가중치이며, **2**로 설정하면 설정된 시간 규칙이 적용될 때 근무 시간이 시간당 2배로 계산됩니다.
- **색**: 시간 규칙을 구분할 색상을 설정하세요.

다음 단계

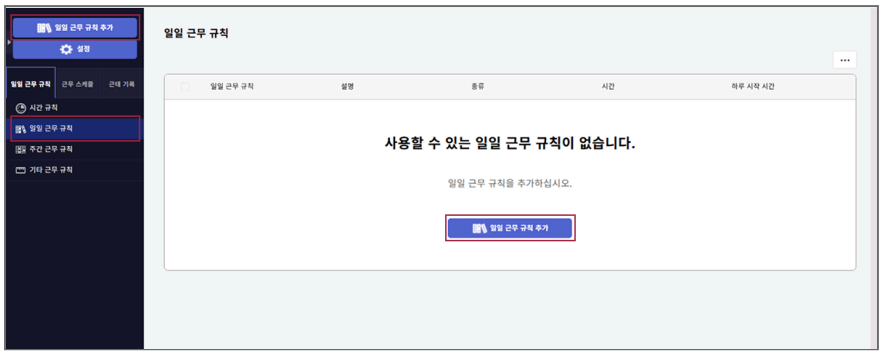
하루(24시간) 단위의 근무 규칙을 설정할 수 있습니다. 근무 규칙은 시간에 따른 시간 규칙 설정, 하루 시작 시간 설정, 시간 반올림 규칙 등을 포함합니다.

일일 근무 규칙 설정하기

24시간을 기준으로 시간에 따라 시간 규칙을 다르게 적용하여 근무 규칙을 생성할 수 있습니다. 고정 근무, 유연 근무, 유동 근무를 선택할 수 있으며, 하루 시작 시간, 시간 반올림 규칙 등을 설정할 수 있습니다.

일일 근무 규칙 추가

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **일일 근무 규칙** → **일일 근무 규칙**을 클릭하세요.
3. **일일 근무 규칙 추가** 버튼을 클릭하세요.



4. **일일 근무 규칙 추가** 화면이 나타나면 각 항목을 설정하세요.

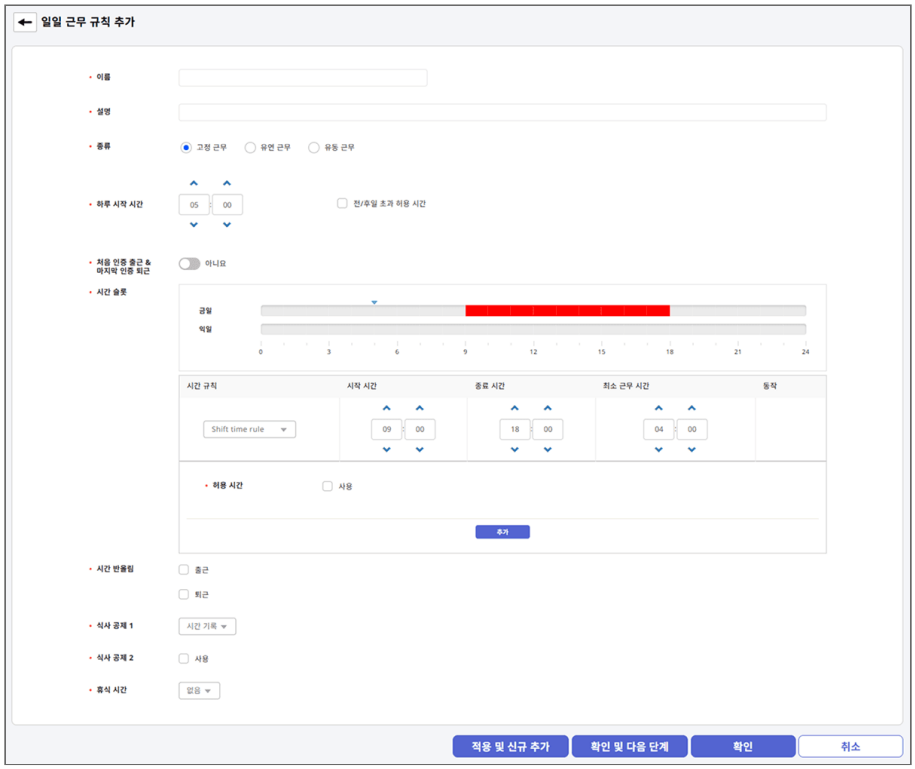
> **알아두기**
>
> - 설정을 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.
> - 이어서 주간 근무 규칙을 추가하려면 **확인 및 다음 단계** 버튼을 클릭하세요.
> - 설정을 저장한 후 다른 **일일 근무 규칙**을 추가하려면 **적용 및 신규 추가** 버튼을 클릭하세요.

설정 옵션 안내

근무 규칙 종류에 따라 **고정 근무**, **유연 근무**, **유동 근무** 중 하나를 선택할 수 있습니다. 선택한 근무 규칙 종류에 따라 설정 옵션이 다를 수 있습니다.

고정 근무

정해진 시간에 출근과 퇴근을 하는 근무 규칙입니다. 일일 근무 규칙의 이름과 설명을 입력하고 **종류**를 **고정 근무**로 선택하세요.



- **하루 시작 시간**: 하루 근무의 시작 시간을 설정하세요.

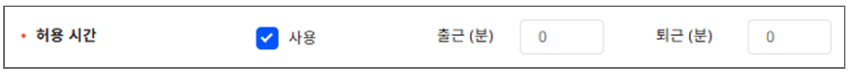
  전/후일 초과 허용 시간을 사용하면 설정된 하루 시작 시간을 기준으로 24시간을 초과한 근무 시간에 대해 근무 규칙을 설정할 수 있습니다. 최대 6시간까지 설정할 수 있습니다.



- **처음 인증 출근 & 마지막 인증 퇴근**: 이 옵션을 활성화하면, 가장 처음 사용자가 인증한 시간을 출근 시간으로 기록하며, 가장 마지막에 사용자가 인증한 시간을 퇴근 시간으로 기록합니다.

> **알아두기**
> 이 옵션을 활성화하면 사용자의 휴식 시간을 기록하기 위해 **휴식 등록**을 설정해야 합니다.

- **시간 슬롯**: **시간 규칙** 열에서 근태 기록을 설정한 항목을 선택한 후 **시작 시간**, **종료 시간**, **최소 근무 시간**을 설정하세요.
  - **허용 시간**: 설정한 시간보다 늦게 출근하거나 빨리 퇴근한 경우에도 정상 근무로 인정할 수 있는 허용 시간을 설정하세요.



- **시간 반올림**: 출근 및 퇴근 시간을 자동으로 반올림할 수 있습니다. 출근과 퇴근 각각에 대해 단위와 기준을 설정하세요.



  - **단위 (분)**: 설정된 시작 시간 보다 빠르거나 늦게 출근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.
  - **기준 (분)**: 설정된 종료 시간 보다 빠르거나 늦게 퇴근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.

> **팁**
> 예를 들어, 출근 시간이 09:00로 설정되어 있고, **단위 (분)**가 15분, **기준 (분)**이 8분으로 설정된 경우 다음과 같이 반올림됩니다.
>
> – 09:07 출근 → 09:00으로 내림 (기준 8분 미만)
>
> – 09:08 출근 → 09:15로 올림 (기준 8분 이상)

> **알아두기**
> **시간 반올림** 규칙은 **허용 시간**보다 우선 적용됩니다.

- **식사 공제 1** / **식사 공제 2**: 일일 근무 시간에서 식사 시간을 공제하도록 설정할 수 있습니다.
  - **시간 기록**: 고정된 식사 공제 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따라 공제하도록 설정할 수 있습니다.
  - **자동**: **공제 시간**과 **공제 전 최소 시간**을 설정하여 자동으로 식사 시간을 공제하도록 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 공제하도록 설정할 수 있습니다.

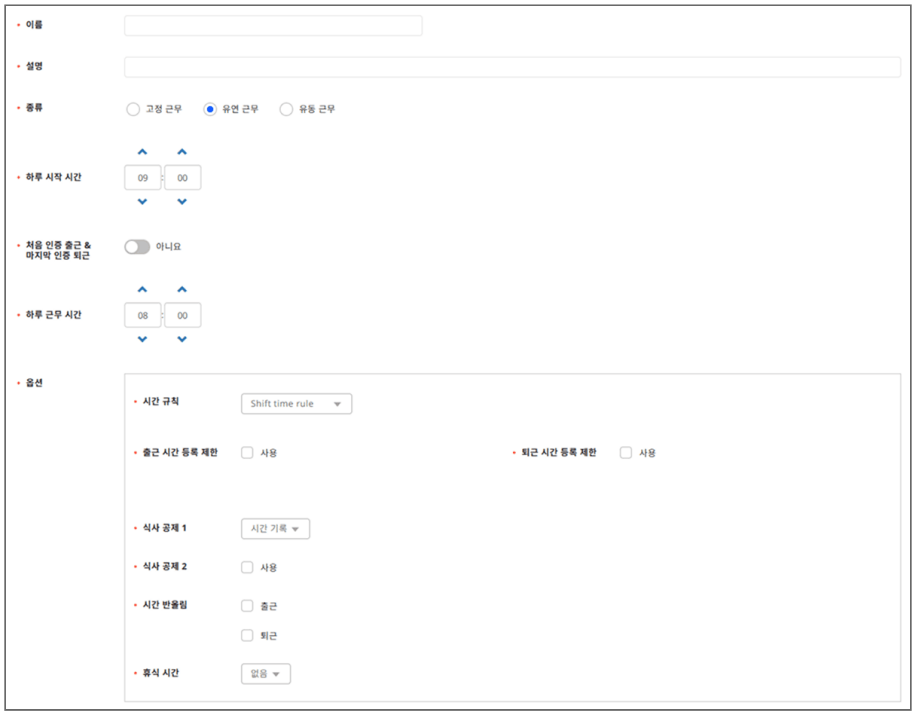
> **알아두기**
> – **식사 공제 2**를 사용하면 일일 근무 시간에서 두 번의 식사 시간을 공제할 수 있습니다.
> – 식사 공제 종류를 **자동** 또는 **고정**으로 사용하면 **식사 공제 1**과 **식사 공제 2**는 동일한 종류로만 설정할 수 있습니다.

- **휴식 시간**: 휴식 시간을 설정할 수 있습니다.
  - **시간 기록**: 고정된 휴식 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따르도록 설정할 수 있습니다. 이 옵션을 활성화하면 **최대 허용 휴식 시간 (분)**을 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 사용자의 휴식 시간으로 설정할 수 있습니다.

> **알아두기**
> - **정상 근무**로 설정된 시간 규칙은 일일 근무 규칙에 하나만 추가할 수 있습니다.
> - **연장 근무**로 설정된 시간 규칙은 **시작 시간**, **종료 시간**, **최소 근무 시간**, **시간 반올림**을 설정할 수 있습니다.

유연 근무

하루 근무 시간을 설정하고 하루 시작 시간을 기준으로 출근 및 퇴근 시간을 유연하게 조정하는 근무 규칙입니다. 일일 근무 규칙의 이름과 설명을 입력하고 **종류**를 **유연 근무**로 선택하세요.



- **하루 시작 시간**: 하루 근무의 시작 시간을 설정하세요.
- **처음 인증 출근 & 마지막 인증 퇴근**: 이 옵션을 활성화하면, 가장 처음 사용자가 인증한 시간을 출근 시간으로 기록하며, 가장 마지막에 사용자가 인증한 시간을 퇴근 시간으로 기록합니다.

> **알아두기**
> 이 옵션을 활성화하면 사용자의 휴식 시간을 기록하기 위해 **휴식 등록**을 설정해야 합니다.

- **하루 근무 시간**: 하루 총 근무 시간을 설정하세요.
- **시간 규칙**: 근태 기록을 설정한 항목을 선택하세요.
- **출근 시간 등록 제한** / **퇴근 시간 등록 제한**: 사용자가 출근 및 퇴근 시간을 인증할 수 있는 시간 범위를 설정할 수 있습니다.



- **식사 공제 1** / **식사 공제 2**: 일일 근무 시간에서 식사 시간을 공제하도록 설정할 수 있습니다.
  - **시간 기록**: 고정된 식사 공제 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따라 공제하도록 설정할 수 있습니다.
  - **자동**: **공제 시간**과 **공제 전 최소 시간**을 설정하여 자동으로 식사 시간을 공제하도록 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 공제하도록 설정할 수 있습니다.

> **알아두기**
> - **식사 공제 2**를 사용하면 일일 근무 시간에서 두 번의 식사 시간을 공제할 수 있습니다.
> - 식사 공제 종류를 **자동** 또는 **고정**으로 사용하면 **식사 공제 1**과 **식사 공제 2**는 동일한 종류로만 설정할 수 있습니다.

- **시간 반올림**: 출근 및 퇴근 시간을 자동으로 반올림할 수 있습니다. 출근과 퇴근 각각에 대해 단위와 기준을 설정하세요.



- **단위 (분)**: 설정된 시작 시간 보다 빠르거나 늦게 출근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.
- **기준 (분)**: 설정된 종료 시간 보다 빠르거나 늦게 퇴근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.

> **팁**
> 예를 들어, 출근 시간이 09:00로 설정되어 있고, **단위 (분)**가 15분, **기준 (분)**이 8분으로 설정된 경우 다음과 같이 반올림됩니다.
>
> - 09:07 출근 → 09:00으로 내림 (기준 8분 미만)
> - 09:08 출근 → 09:15로 올림 (기준 8분 이상)

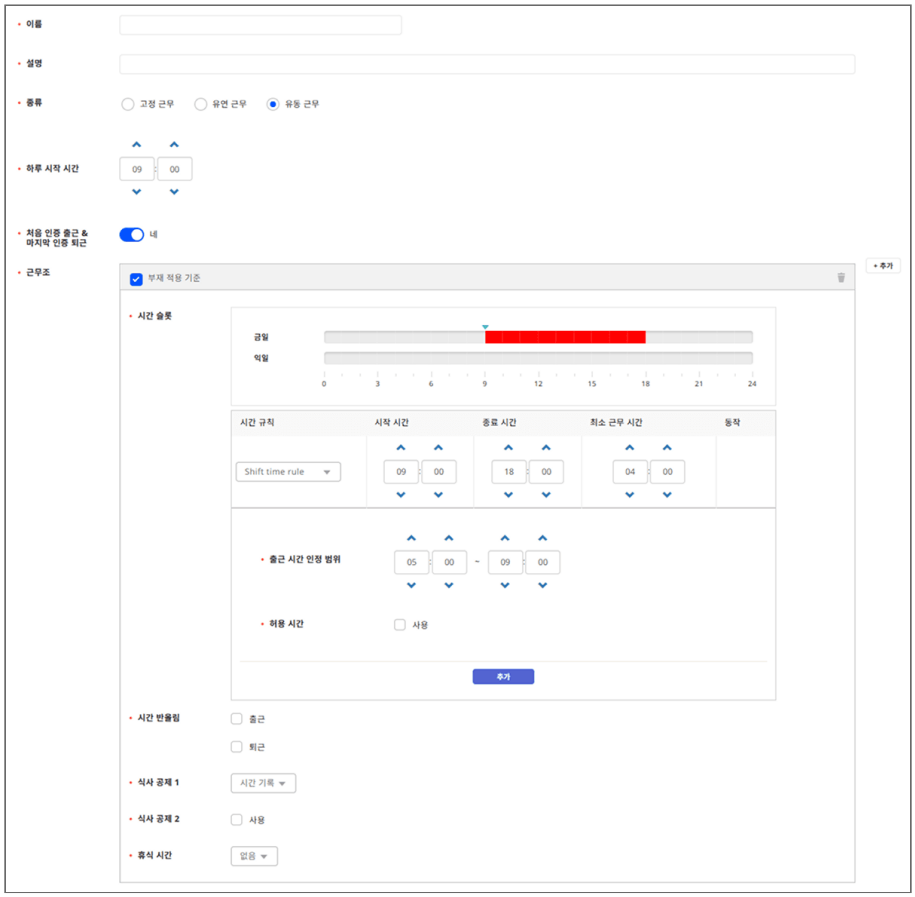
> **알아두기**
> **시간 반올림** 규칙은 **허용 시간**보다 우선 적용됩니다.

- **휴식 시간**: 휴식 시간을 설정할 수 있습니다.
  - **시간 기록**: 고정된 휴식 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따르도록 설정할 수 있습니다. 이 옵션을 활성화하면 **최대 허용 휴식 시간 (분)**을 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 사용자의 휴식 시간으로 설정할 수 있습니다.

> **알아두기**
> **연장 근무**로 설정된 시간 규칙은 추가할 수 없습니다.

유동 근무

출근 및 퇴근 시간을 자유롭게 설정할 수 있는 근무 규칙입니다. 일일 근무 규칙의 이름과 설명을 입력하고 **종류**를 **유동 근무**로 선택하세요.



- **하루 시작 시간**: 하루 근무의 시작 시간을 설정하세요.
- **처음 인증 출근 & 마지막 인증 퇴근**: 이 옵션을 활성화하면, 가장 처음 사용자가 인증한 시간을 출근 시간으로 기록하며, 가장 마지막에 사용자가 인증한 시간을 퇴근 시간으로 기록합니다.

> **알아두기**
> 이 옵션을 활성화하면 사용자의 휴식 시간을 기록하기 위해 **휴식 등록**을 설정해야 합니다.

- **시간 슬롯**: **시간 규칙** 열에서 근태 기록을 설정한 항목을 선택한 후 **시작 시간**, **종료 시간**, **최소 근무 시간**을 설정하세요.
  - **출근 시간 인정 범위**: 설정된 출근 또는 퇴근 시간보다 일찍 출근하거나 늦게 퇴근한 경우에 정상 근무로 인정할 시간 범위를 설정하세요.
  - **허용 시간**: 설정한 시간보다 늦게 출근하거나 빨리 퇴근한 경우에도 정상 근무로 인정할 수 있는 허용 시간을 설정하세요.



- **시간 반올림**: 출근 및 퇴근 시간을 자동으로 반올림할 수 있습니다. 출근과 퇴근 각각에 대해 단위와 기준을 설정하세요.



  - **단위 (분)**: 설정된 시작 시간 보다 빠르거나 늦게 출근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.
  - **기준 (분)**: 설정된 종료 시간 보다 빠르거나 늦게 퇴근 이벤트가 등록될 경우 등록된 시간을 반올림하는 규칙을 설정할 수 있습니다.

> **팁**
> 예를 들어, 출근 시간이 09:00로 설정되어 있고, **단위 (분)**가 15분, **기준 (분)**이 8분으로 설정된 경우 다음과 같이 반올림됩니다.
>
> – 09:07 출근 → 09:00으로 내림 (기준 8분 미만)
>
> – 09:08 출근 → 09:15로 올림 (기준 8분 이상)

> **알아두기**
> **시간 반올림** 규칙은 **허용 시간**보다 우선 적용됩니다.

- **식사 공제 1** / **식사 공제 2**: 일일 근무 시간에서 식사 시간을 공제하도록 설정할 수 있습니다.
  - **시간 기록**: 고정된 식사 공제 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따라 공제하도록 설정할 수 있습니다.
  - **자동**: **공제 시간**과 **공제 전 최소 시간**을 설정하여 자동으로 식사 시간을 공제하도록 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 공제하도록 설정할 수 있습니다.

> **알아두기**
> – **식사 공제 2**를 사용하면 일일 근무 시간에서 두 번의 식사 시간을 공제할 수 있습니다.
> – 식사 공제 종류를 **자동** 또는 **고정**으로 사용하면 **식사 공제 1**과 **식사 공제 2**는 동일한 종류로만 설정할 수 있습니다.

- **휴식 시간**: 휴식 시간을 설정할 수 있습니다.
  - **시간 기록**: 고정된 휴식 시간을 설정하지 않고, 근태 등록 장치에 등록된 시간 기록에 따르도록 설정할 수 있습니다. 이 옵션을 활성화하면 **최대 허용 휴식 시간 (분)**을 설정할 수 있습니다.
  - **고정**: **시작 시간** 및 **종료 시간**을 설정하여 고정된 시간을 사용자의 휴식 시간으로 설정할 수 있습니다.

> **알아두기**
> - 근무조는 최대 5개의 시간 슬롯으로 구성할 수 있습니다. **+ 추가** 버튼을 클릭하여 시간 슬롯을 추가하세요.
> - 부재를 설정할 때 **부재 적용 기준** 옵션을 선택해야 합니다. **부재 적용 기준**은 근무조로 구성한 시간 슬롯 중 선택할 수 있습니다.
>
> 
>
>
> - **연장 근무**로 설정된 시간 규칙은 **시작 시간**, **종료 시간**, **최소 근무 시간**, **시간 반올림**을 설정할 수 있습니다.

다음 단계

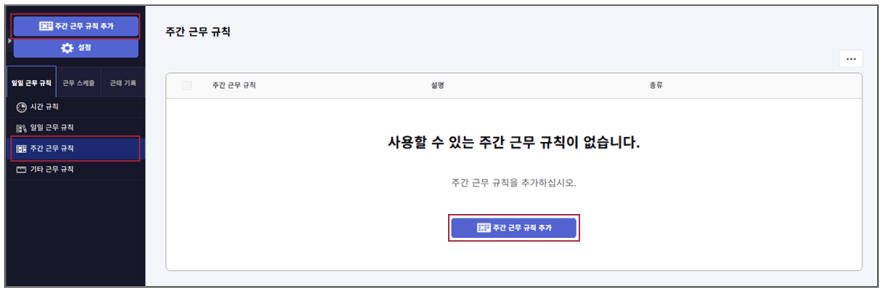
설정된 하루 단위의 근무 규칙으로 주간 근무 규칙을 설정할 수 있습니다. 주별, 일별 주간 근무 규칙을 설정할 수 있습니다.

주간 근무 규칙 설정하기

설정한 일일 근무 규칙을 기반으로 주간 단위의 근무 규칙을 생성하는 방법을 안내합니다.

주간 근무 규칙 추가

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **일일 근무 규칙** → **주간 근무 규칙**을 클릭하세요.
3. **주간 근무 규칙 추가** 버튼을 클릭하세요.

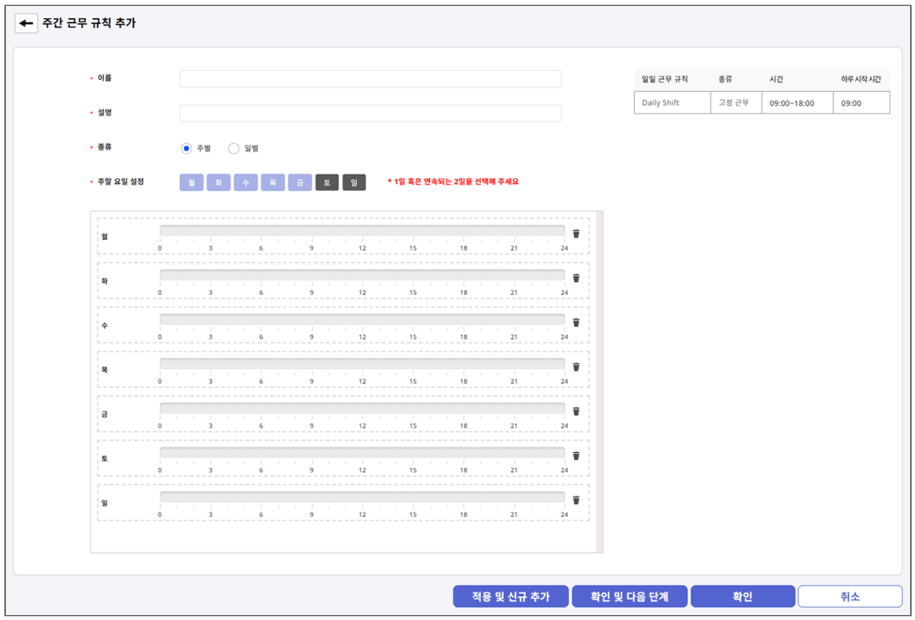


4. **주간 근무 규칙 추가** 화면이 나타나면 각 항목을 설정하세요.

알아두기

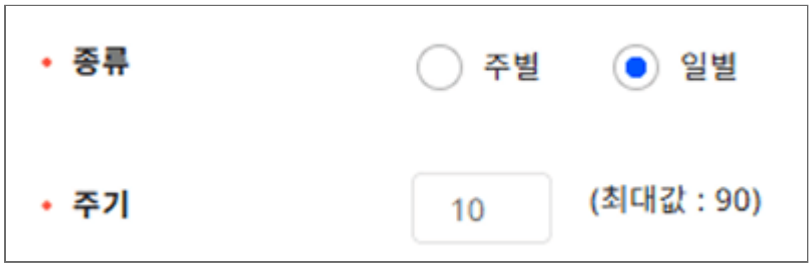
- 설정을 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.
- 이어서 근무 스케줄을 추가하려면 **확인 및 다음 단계** 버튼을 클릭하세요.
- 설정을 저장한 후 다른 **주간 근무 규칙**을 추가하려면 **적용 및 신규 추가** 버튼을 클릭하세요.

설정 옵션 안내



- **이름**: 주간 근무 규칙의 이름을 입력하세요.
- **설명**: 주간 근무 규칙에 대한 설명을 입력하세요.
- **종류**: 주간 근무 규칙을 **주별** 또는 **일별** 일별로 설정할 수 있습니다.

  일별을 선택하면 반복 사용 기간(**주기**)을 설정할 수 있습니다.



- **주말 요일 설정**: 주말로 지정할 요일을 설정하세요.
- **일일 근무 규칙**: 설정된 일일 근무 규칙 목록을 확인할 수 있습니다.
- 주별/일별 스케줄: 설정한 일일 근무 규칙을 드래그앤드랍으로 설정하세요.



> **알아두기**
>
> - 월요일부터 일요일까지 모두 적용하려면 **전체 복사** 버튼을 클릭하세요.
> - 적용한 일일 근무 규칙을 해제하려면 🗑 버튼을 클릭하세요.
> - **전/후일 초과 허용 시간**을 설정한 일일 근무 규칙을 적용하면 전일 초과 허용 시간이 전일 근무 규칙의 하루 시작 시간보다 24시간 앞에 위치하도록 설정할 수 없습니다.

다음 단계

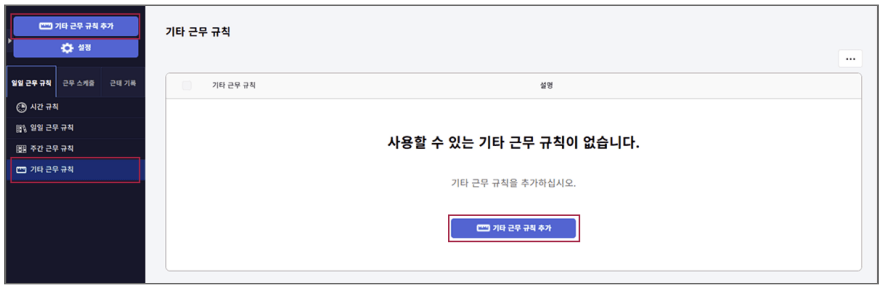
일일 근무 규칙에 초과 근무 시간 규칙을 추가 적용하여 유연한 근무 규칙 생성 방법을 안내합니다.

기타 근무 규칙 설정하기

일일 근무 규칙에 연장 근무 시간 규칙을 추가하지 않았을 때 유용하게 사용할 수 있습니다. 일일 근무 규칙에서 설정하는 연장 근무는 시작 시간과 종료 시간을 갖고 있으나 기타 근무 규칙은 정규 근무 시간 범위를 넘어선 총 시간을 계산합니다. 기타 근무 규칙은 일별/주별/월별 총 연장 근무 시간으로 관리할 때 편리하게 사용할 수 있습니다. 기타 근무 규칙을 설정하면 일일 근무 규칙에 추가된 연장 근무 시간 규칙 대신 적용됩니다.

기타 근무 규칙 추가

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **일일 근무 규칙** → **기타 근무 규칙**을 클릭하세요.
3. **기타 근무 규칙 추가** 버튼을 클릭하세요.

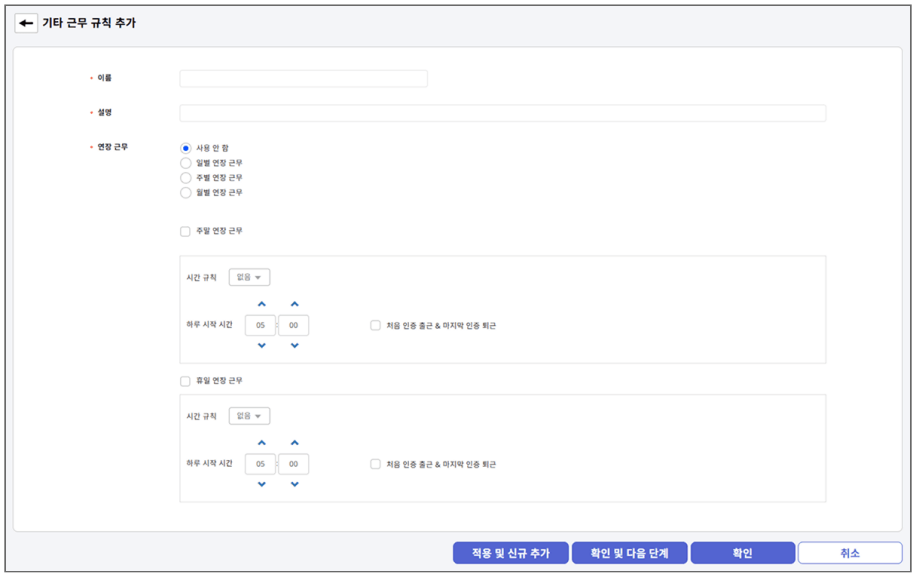


4. **기타 근무 규칙 추가** 화면이 나타나면 각 항목을 설정하세요.

> **알아두기**
>
> - 설정을 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.
> - 이어서 근무 스케줄을 추가하려면 **확인 및 다음 단계** 버튼을 클릭하세요.
> - 설정을 저장한 후 다른 **기타 근무 규칙**을 추가하려면 **적용 및 신규 추가** 버튼을 클릭하세요.

설정 옵션 안내

기타 근무 규칙을 설정하세요. 일별, 주별, 월별 단위로 적용할 연장 근무 규칙을 설정할 수 있습니다.



- **이름**: 기타 근무 규칙의 이름을 입력하세요.
- **설명**: 기타 근무 규칙에 대한 설명을 입력하세요.
- **연장 근무**: 일별, 주별, 월별 단위로 정규 근무 시간 이후 적용할 연장 근무 규칙을 선택하세요. 일정 시간 이후에 다른 연장 근무 규칙을 적용할 수 있습니다. 최대 연장 근무 시간을 설정하여 근로자가 일할 수 있는 연장 근무 시간을 제한할 수도 있습니다.

> **팁**
>
> 아래와 같이 설정하면 정규 근무 시간이 오전 8시에서 오후 5시일 때 오후 5시부터 오후 11시까지 **Overtime(1.5)** 시간 규칙이 적용되며, 오후 11시부터 오전 2시까지 **Overtime(2)** 시간 규칙이 적용됩니다. 또한, 하루 일할 수 있는 최대 초과 근무 시간이 9시간으로 제한되어 오전 2시까지 일한 기록만 사용하여 하루 급여를 계산합니다.
>
> 
>

> **알아두기**
>
> 총 근무 시간은 휴식 시간이나 식사 시간을 포함하지 않습니다.

- **주말 연장 근무** / **휴일 연장 근무**: 주말 또는 휴일에 적용할 근무 규칙을 설정하세요.
  - **시간 규칙**: 적용할 시간 규칙을 선택하세요.
  - **하루 시작 시간**: 근무 시작 시간을 설정하세요.
  - **처음 인증 출근 & 마지막 인증 퇴근**: 가장 처음 사용자가 인증한 시간을 출근 시간으로 기록하며, 가장 마지막에 사용자가 인증한 시간을 퇴근 시간으로 기록합니다.

다음 단계

기간, 사용자, 기타 근무 규칙, 휴가 일정을 구성하여 근무 스케줄 설정 방법을 안내합니다.

근무 스케줄 설정하기

설정된 일일 근무 규칙, 기타 근무 규칙, 기간, 휴일을 사용자에게 지정하여 근무 스케줄을 생성할 수 있습니다.

생성된 근무 스케줄에 임시 스케줄이나 개인 휴가도 추가할 수 있습니다.

알아두기

스케줄을 생성하기 전에 사용할 시간 규칙, 일일 근무 규칙, 일일 근무 규칙, 휴일을 올바르게 생성했는지 확인하세요.

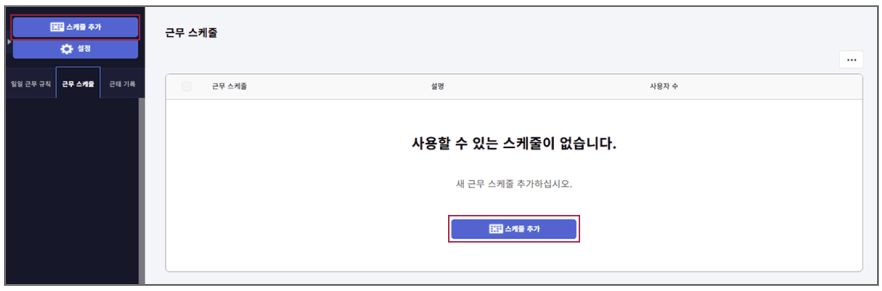
- 근무 규칙 설정에 대한 자세한 내용을 다음 문서를 참고하세요.
  - 시간 규칙 설정하기
  - 일일 근무 규칙 설정하기
  - 주간 근무 규칙 설정하기
  - 기타 근무 규칙 설정하기
- 휴일 설정에 대한 자세한 내용은 스케줄 설정하기를 참고하세요.

근무 스케줄

근무 스케줄 추가

다음 안내에 따라 등록한 사용자의 근무 스케줄을 추가하세요.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근무 스케줄** 탭을 클릭하세요.
3. **스케줄 추가** 버튼을 클릭하세요.



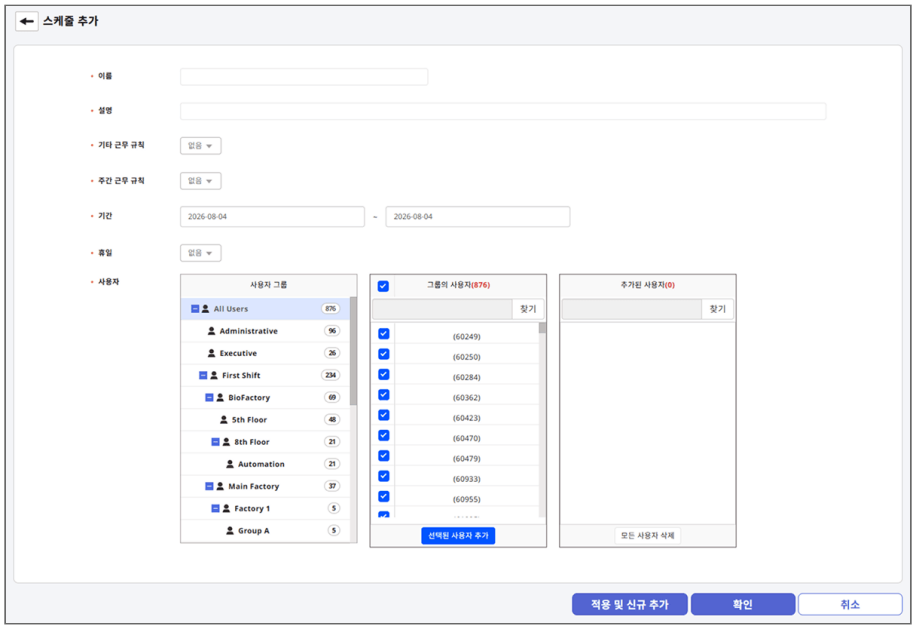
4. **스케줄 추가** 화면이 나타나면 각 항목을 설정하세요.

알아두기

- 설정을 저장하려면 화면 하단의 **확인** 버튼을 클릭하세요.
- 설정을 저장한 후 다른 **근무 스케줄**을 추가하려면 **적용 및 신규 추가** 버튼을 클릭하세요.

설정 옵션 안내

근무 스케줄 설정 옵션을 안내합니다.



- **이름**: 근무 스케줄의 이름을 입력하세요.
- **설명**: 근무 스케줄에 대한 설명을 입력하세요.
- **기타 근무 규칙**: 설정한 기타 근무 규칙을 선택하세요. 기타 근무 규칙을 설정하면 일일 근무 규칙에 설정한 초과 근무 시간 규칙이 적용되지 않습니다. 사용하지 않으려면 **없음**을 선택하세요.

> **알아두기**
> 원하는 기타 근무 규칙이 없다면 추가할 수 있습니다. 자세한 내용은 기타 근무 규칙 설정하기를 참고하세요.

- **주간 근무 규칙**: 설정한 주간 근무 규칙을 선택하세요. 한번 설정한 주간 근무 규칙은 수정할 수 없습니다.

> **알아두기**
> 원하는 주간 근무 규칙이 없다면 추가할 수 있습니다. 자세한 내용은 주간 근무 규칙 설정하기를 참고하세요.

- **기간**: 근태 이벤트를 수집할 기간을 설정하세요.

> **알아두기**
> 시작 날짜는 한 번 설정하면 나중에 변경할 수 없습니다. 종료 날짜는 나중에 변경할 수 있으며, 설정된 날짜보다 이전 날짜로 변경하면 변경된 기간만큼의 부재 이벤트가 삭제됩니다.

- **휴일**: 설정한 휴가 일정을 선택하세요. 사용하지 않으려면 **없음**을 선택하세요.

> **알아두기**
> 원하는 휴가 일정이 없다면 추가할 수 있습니다. 자세한 내용은 스케줄 설정하기를 참고하세요.

- **사용자**: 규칙을 적용할 사용자를 추가하세요.

> **알아두기**
> 전체 근무 스케줄에 포함된 사용자 수는 등록한 근태 관리 라이선스가 지원하는 최대 사용자 수를 초과할 수 없습니다. 각 라이선스당 최대 사용자는 라이선스 정책을 참고하세요.

근무 스케줄 수정

등록한 근무 스케줄 수정 방법을 안내합니다.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근무 스케줄** 탭을 클릭하세요.
3. **근무 스케줄** 목록에서 수정할 항목을 클릭하세요. 또는 화면 왼쪽 사이드바에서 수정할 항목의 ✎ 버튼을 클릭하세요.
4. 원하는 항목을 수정하고 **확인** 버튼을 클릭하세요.

근무 스케줄 삭제

등록한 근무 스케줄 삭제 방법을 안내합니다.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근무 스케줄** 탭을 클릭하세요.
3. **근무 스케줄** 목록에서 삭제할 항목의 체크박스를 클릭하세요.

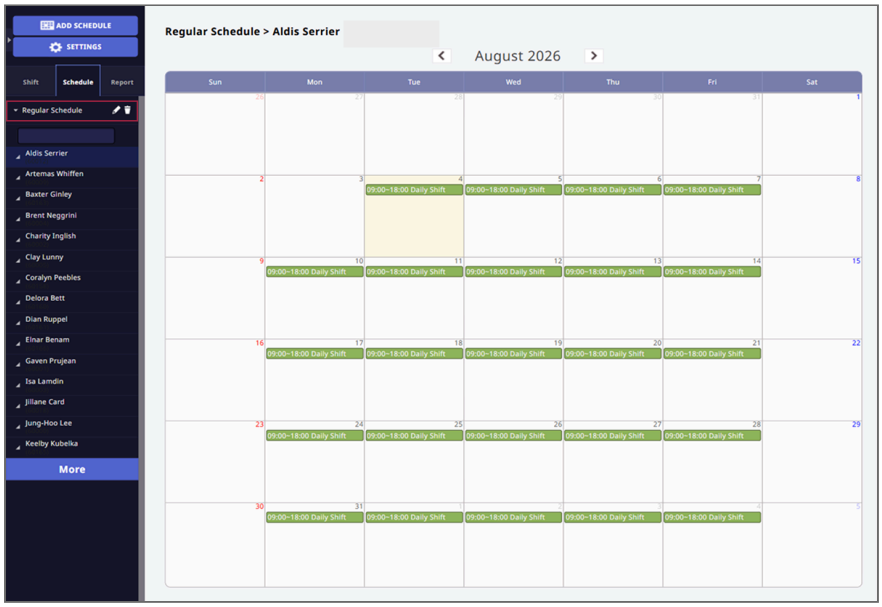


4. 화면 오른쪽 상단의 **스케줄 삭제** 버튼을 클릭하세요. 또는 화면 왼쪽 사이드바에서 삭제할 항목의 🗑 버튼을 클릭하세요.
5. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.

임시 스케줄 추가

이미 등록한 스케줄이 있다면 사용자에게 임시로 다른 근무 규칙을 적용할 수 있습니다.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근무 스케줄** 탭을 클릭하세요.
3. 화면 왼쪽 목록에서 원하는 스케줄의 ▶ 버튼을 클릭하세요.
4. 스케줄에 할당된 사용자 목록이 표시되고 임시 스케줄을 적용할 사용자를 선택하면 달력이 표시됩니다.

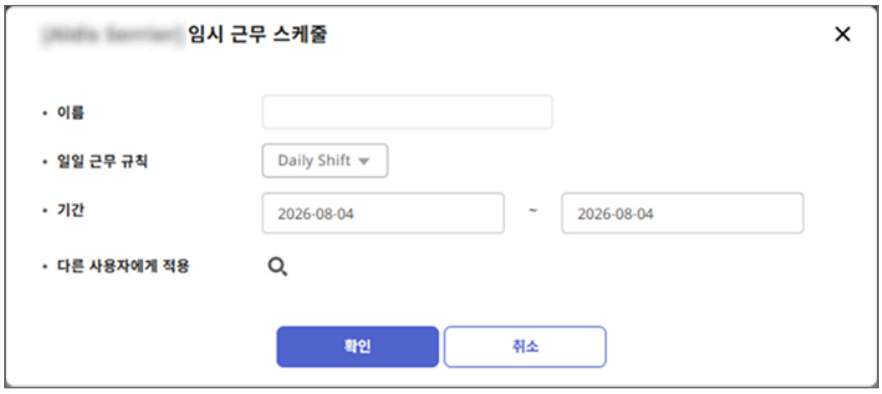


5. 달력에서 임시 스케줄을 추가할 날짜를 클릭하세요.



6. 팝업 메뉴에서 **임시 근무 스케줄 추가**를 클릭하세요.

7. **임시 근무 스케줄 추가** 설정창이 나타나면 각 항목을 설정하세요.



다른 사용자에게도 동일한 근무 스케줄을 적용하려면 🔍 버튼을 클릭한 후 사용자를 선택하세요.

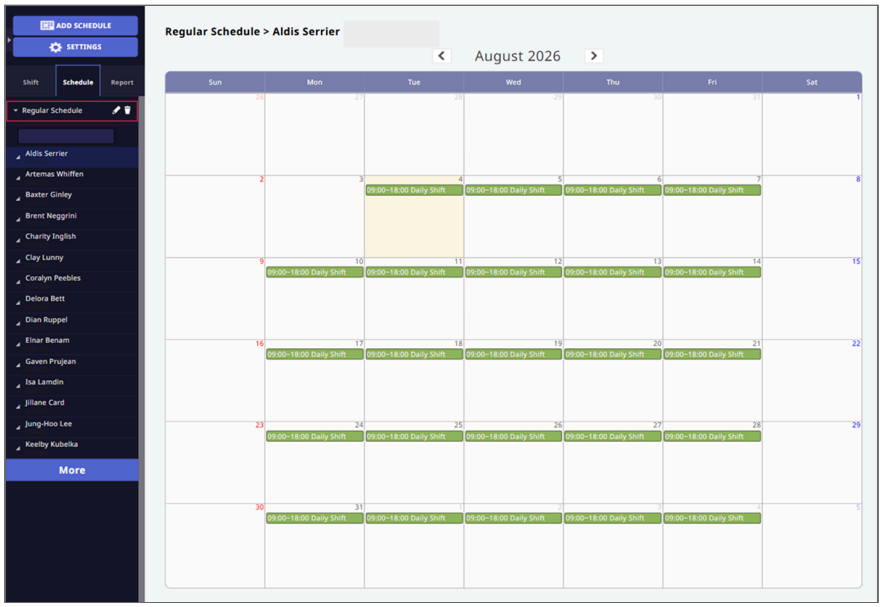
8. 설정한 근무 규칙을 적용하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
> 사용자에게 적용한 임시 스케줄을 삭제하려면 달력에서 설정된 임시 스케줄을 클릭하세요. 확인 메시지 창이 나타나면 **네** 버튼을 클릭하세요.

부재 추가 및 삭제

사용자의 부재 일정을 추가할 수 있습니다.

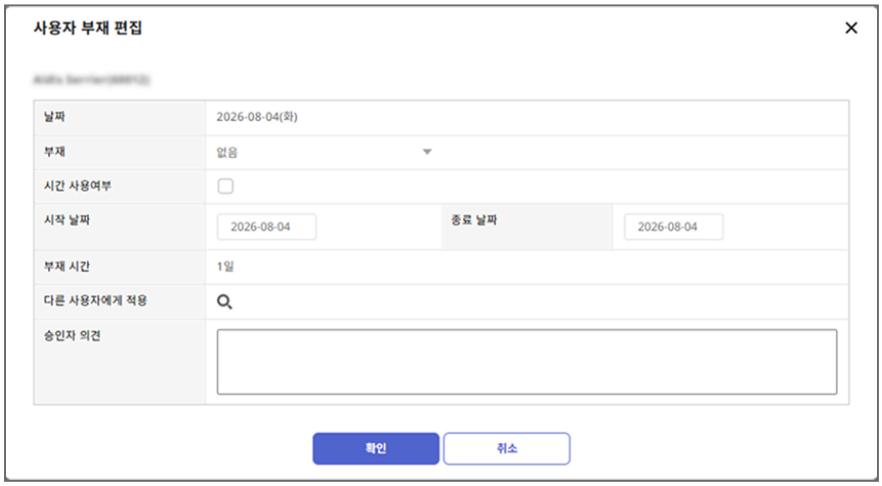
1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근무 스케줄** 탭을 클릭하세요.
3. 화면 왼쪽 목록에서 원하는 스케줄의 ▶ 버튼을 클릭하세요.
4. 스케줄에 할당된 사용자 목록이 표시되고 부재 일정을 적용할 사용자를 선택하면 달력이 표시됩니다.



5. 달력에서 사용자의 부재 일정을 추가할 날짜를 클릭하세요.

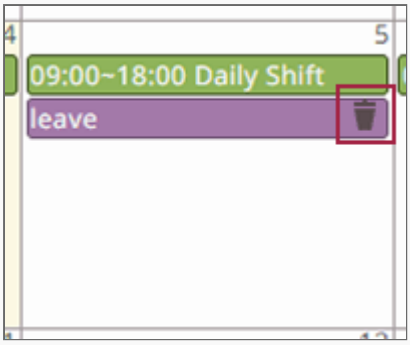


6. 팝업 메뉴에서 **사용자 부재 추가**를 클릭하세요.
7. **사용자 부재 편집** 설정창이 나타나면 각 항목을 설정하세요.



다른 사용자에게도 동일한 부재 일정을 적용하려면 🔍 버튼을 클릭한 후 사용자를 선택하세요.

8. 설정한 부재 일정을 적용하려면 **확인** 버튼을 클릭하세요.

> **알아두기**
>
> - 원하는 부재 관리 시간 규칙이 없다면 추가할 수 있습니다. 시간 규칙 추가에 대한 자세한 내용은 시간 규칙 설정하기를 참고하세요.
> - 사용자에게 적용한 부재 일정을 삭제하려면 달력에서 설정된 부재 일정의 🗑 버튼을 클릭하세요. 확인 메시지 창이 나타나면 **네** 버튼을 클릭하세요.
>
> 
>

근태 기록 확인하기

시스템을 통해 수집된 사용자의 근태 이벤트로 근태 보고서를 생성할 수 있으며, 시간 기록을 편집하거나 CSV 파일이나 PDF파일로 내보내기할 수 있습니다.

미리 설정된 7 개의 보고서 필터를 이용하여 간편하게 사용할 수 있으며, 관리자가 직접 필터를 설정할 수도 있습니다.

시작하기 전에

다국어 보고서 사용하기 전에

BioStar X에서는 한국어와 영어를 기본 지원합니다. 다국어 보고서를 사용하려면 다음 안내에 따라 원하는 언어를 설정하세요.

1. 다음 경로로 이동하세요. *C:\Program Files\BioStar X\plugin\ta\dist\setup\report_fonts*
2. 사용하려는 언어 이름으로 폴더를 생성하세요. 언어 이름은 ISO 639-1 규격을 참고하세요. 예를 들어, 스페인어를 사용하려면 폴더 이름을 "es"로 생성하세요.

3. 생성한 폴더로 글꼴을 복사하여 붙여넣기를 하세요. 하나의 트루 타입 글꼴만 지원합니다.

보고서 업데이트 전에

BioStar X는 MariaDB를 기본 데이터베이스로 사용합니다. MS SQL Server 데이터베이스를 사용한다면 아래 사항을 먼저 확인하세요.

BioStar X를 MS SQL Server 데이터베이스와 사용할 때, 등록된 사용자의 수가 많은 경우 보고서를 업데이트할 때마다 PC의 메모리 사용량이 누적될 수 있습니다. MS SQL Server 데이터베이스의 최대 서버 메모리를 다시 설정하세요.

1. **Microsoft SQL Server Management Studio**를 실행하세요.
2. 개체 탐색기에서 **BioStar X**의 데이터베이스를 마우스 오른쪽 버튼을 클릭하세요.
3. 팝업 메뉴에서 **속성**을 클릭하세요.
4. **메모리**를 클릭한 후 **최대 서버 메모리** 항목의 값을 줄이세요.

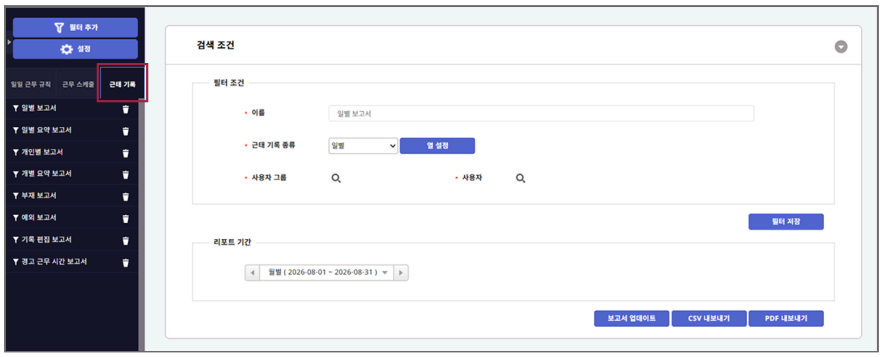
> **알아두기**
> **BioStar X** 설치 시 MariaDB 및 MS SQL Server 설정에 대한 자세한 내용은 사용자 정의 설치하기를 참고하세요.

근태 기록 확인

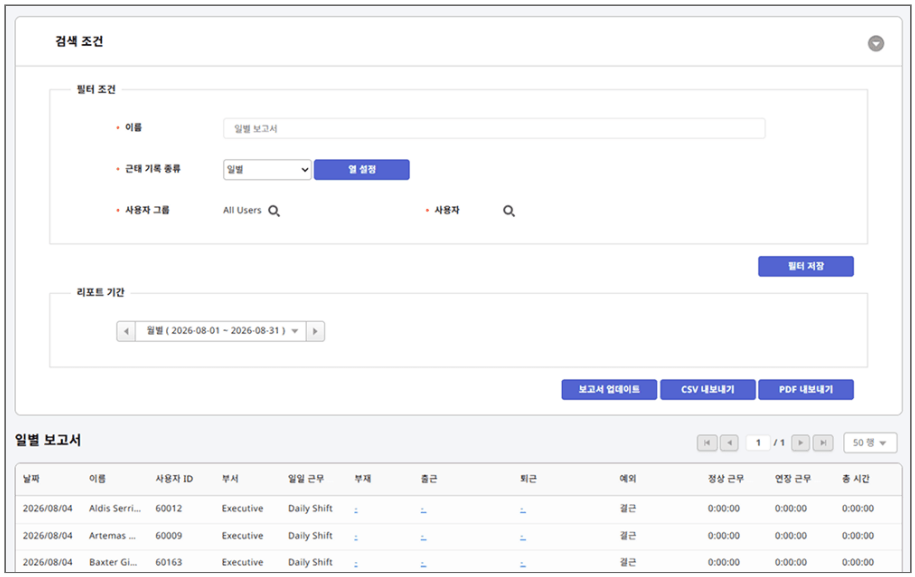
근태 보고서 생성

등록된 사용자의 근태 기록 보고서를 생성하는 방법을 안내합니다.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근태 기록** 탭을 클릭하세요.



3. 화면 왼쪽 사이드바에서 원하는 보고서 필터 항목을 클릭하세요.
4. **사용자 그룹** 또는 **사용자** 항목에서 🔍 버튼을 클릭한 후 그룹 또는 사용자를 지정하세요.
5. 보고서를 생성하려면 **보고서 업데이트** 버튼을 클릭하세요.
6. 화면 하단에 보고서 목록이 나타나면 원하는 항목을 클릭하여 세부 정보를 확인할 수 있습니다.

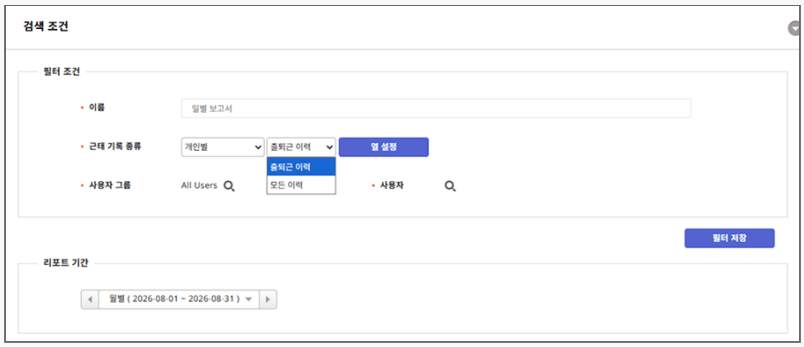


필터 조건 설정

필터 조건을 설정하여 새로운 근태 기록 보고서를 생성할 수 있습니다.



- **이름**: 보고서 이름을 입력하세요.
- **근태 기록 종류**: 원하는 보고서 종류를 선택하세요. 제공하는 보고서 종류는 아래와 같습니다.
  - **일별**, **일별 요약**, **개인별**, **개별 요약**, **부재**, **예외**, **시간 기록 로그 수정**, **경고 근무 시간**

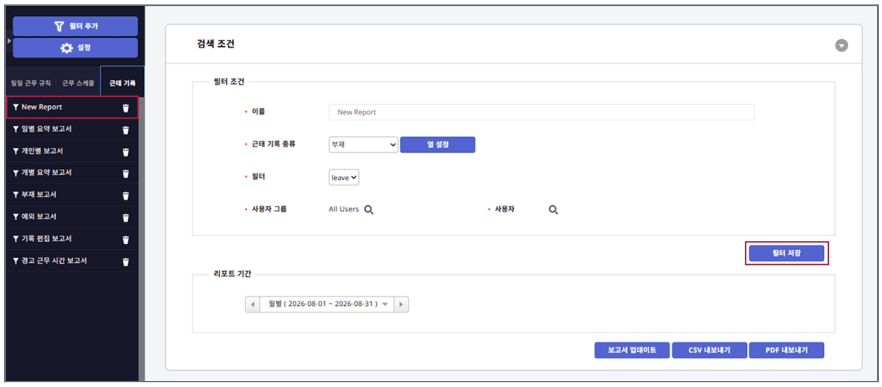
> **알아두기**
> **근태 기록 종류**를 **개인별**로 선택하면 사용자의 출입 기록 출력 여부를 설정할 수 있습니다.
>
> 
>
>
> - **출퇴근 이력**: 보고서에 사용자의 출근 및 퇴근 기록만 출력합니다.
> - **모든 이력**: 보고서에 사용자의 모든 출입 기록을 출력합니다.

- **열 설정**: 보고서 테이블의 열 순서를 변경하거나 숨길 수 있습니다.



> **알아두기**
> 열 순서를 변경한 후 기본 설정으로 복원하려면 **기본 열** 버튼을 클릭하세요.

- **필터**: **근태 기록 종류**를 **부재** 또는 **예외**로 설정했을 때만 활성화되며, 부재 기록이나 예외 기록의 세부 조건을 선택할 수 있습니다.
- **사용자 그룹** / **사용자**: 보고서를 생성할 사용자 그룹이나 사용자를 선택하세요.
- **필터 저장**: 설정한 근태 보고서를 필터로 저장할 수 있습니다.



보고서 기간 설정

보고서 기간 설정 방법을 안내합니다.



보고서 기간을 **일별**, **주별**, **월별**로 설정할 수 있습니다. 특정 기간의 보고서를 생성하려면 **사용자 정의**를 선택하세요.

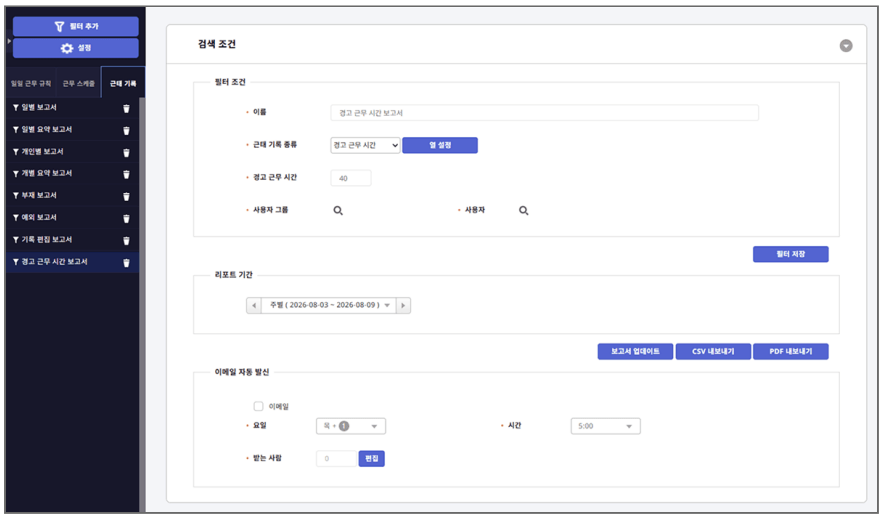
보고서 내보내기

- **CSV 내보내기**: 생성한 보고서를 CSV 파일로 저장할 수 있습니다.
- **PDF 내보내기**: 생성한 보고서를 PDF 파일로 저장할 수 있습니다.

경고 근무 시간 보고서 생성

지정된 근무 시간에 도달한 사용자의 근태 보고서를 생성하거나, 이메일로 관리자에게 알려줄 수 있습니다. 경고 근무 시간 보고서는 주별로 생성됩니다.

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **근태 기록** 탭을 클릭하세요.
3. 화면 왼쪽 사이드바의 필터 목록에서 **경고 근무 시간 보고서**를 클릭하세요.



4. **필터 조건**과 **리포트 기간**의 각 항목을 설정하세요.
5. 보고서를 생성하려면 **보고서 업데이트** 버튼을 클릭하세요.

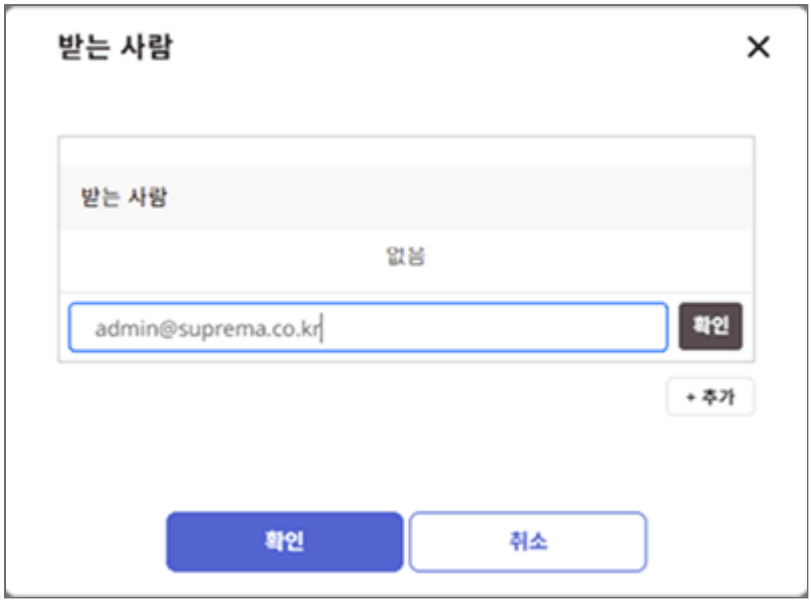
> **알아두기**
> 지정된 근무 시간에 도달한 사용자에 대한 알림을 관리자에게 이메일로 보내려면 **이메일 자동 발신**을 설정하세요. 자세한 내용은 이메일 자동 발신 설정을 참고하세요.

이메일 자동 발신 설정

지정된 근무 시간에 도달한 사용자에 대한 알람 이메일을 자동으로 관리자에게 보낼 수 있습니다.



- **이메일**: 관리자에게 이메일을 자동으로 보내려면 체크박스를 클릭하세요.
- **요일**: 관리자에게 이메일을 보낼 요일을 선택하세요.
- **시간**: 관리자에게 이메일을 보낼 시간을 설정하세요.
- **받는 사람**: 이메일을 받을 관리자를 지정할 수 있습니다. **편집** 버튼을 클릭하면 **받는 사람** 팝업창이 나타납니다. 이메일 주소를 입력하세요. 1명 이상의 관리자를 지정할 수 있습니다.



알아두기

- **이메일 자동 발신** 기능을 설정하려면 필터 조건을 설정한 후 필터를 저장해야 합니다.
- 자동 발신한 이메일의 보낸 사람 정보는 화면 왼쪽 사이드바의 **설정**(⚙) → **보낸 사람 정보**에서 설정할 수 있습니다. 자세한 내용은 근태 관리 설정하기를 참고하세요.

근태 기록 수정하기

생성된 보고서 테이블을 클릭하면 근태 기록을 수정할 수 있습니다.

알아두기

- 근태 기록을 수정하려면 보고서를 먼저 생성해야 합니다. 보고서 생성에 대한 자세한 내용은 근태 기록 확인하기를 참고하세요.
- 근태 스케줄이 등록되지 않은 사용자의 출퇴근 기록은 수정할 수 없습니다.

1. 생성된 보고서 목록에서 기록을 수정할 항목을 클릭하세요.

2. 원하는 방법에 따라 근태 기록을 수정하거나 부재를 추가하세요.

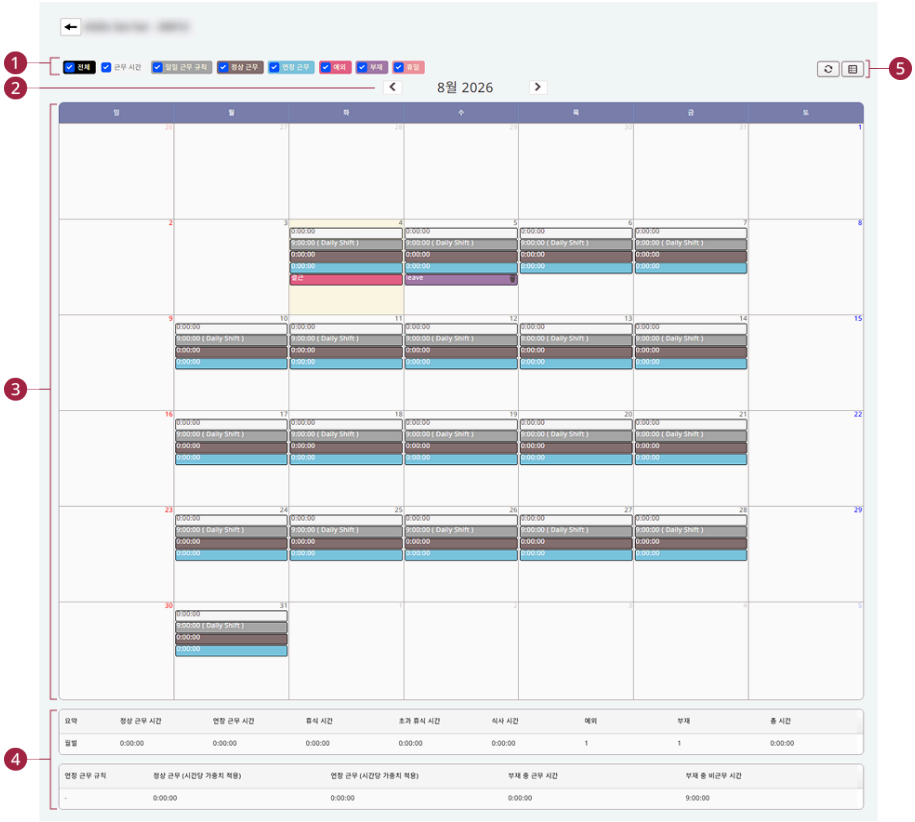
목록에서 수정하기



1. **날짜 범위**: 목록으로 표시할 근태 기록의 기간을 설정할 수 있습니다.
2. **일별 근태 기록**: 일별 근태 기록을 확인할 수 있습니다.
   - 출근/퇴근 시간을 클릭하면 근태 기록을 추가/수정/삭제할 수 있습니다. 출근/퇴근 시간을 클릭한 뒤 ✎ 버튼을 클릭하면 이미 등록된 근태 기록을 수정할 수 있으며, 변경 사항을 저장하려면 **확인** 버튼을 클릭하세요.
   - 부재를 추가하려면 ✎ 버튼을 클릭하세요. 휴가를 추가하려면 부재로 설정된 시간 규칙이 필요합니다. 추가된 사용자 부재의 🗑을 클릭하면 삭제할 수 있습니다.
3. **근태 기록 요약**: 설정한 기간에 따른 근태 기록을 확인할 수 있습니다.
4. **새로고침 / 달력으로 보기**
   - ⟳: 근태 기록 목록을 새로고침합니다.
   - 📅: 근태 기록을 달력 형식으로 확인할 수 있습니다.

> **알아두기**
> 시간 규칙 생성에 대한 자세한 내용은 시간 규칙 설정하기를 참고하세요.

달력에서 수정하기



1. **이벤트 종류**: 이벤트 종류를 선택해 달력에 표시하거나 숨길 수 있습니다.
2. **월**: 이전 달이나 다음 달로 이동하려면 ‹ 또는 › 버튼을 클릭하세요.
3. **일별 근태 기록**: 일별 근태 기록을 확인할 수 있습니다.
   - 근무 시간(흰색)을 클릭하면 근태 기록을 추가/수정/삭제할 수 있습니다. ✎ 버튼을 클릭하면 이미 등록된 근태 기록을 수정할 수 있으며, 변경 사항을 저장하려면 **확인** 버튼을 클릭하세요.
   - 근무 규칙(회색)을 클릭하면 사용자 부재 관리를 추가할 수 있습니다. 사용자 부재를 추가하려면 부재로 설정된 시간 규칙이 필요합니다. 추가된 사용자 부재의 🗑 을 클릭하면 삭제할 수 있습니다.
4. **근태 기록 요약**: 월별 근태 기록을 확인할 수 있습니다.
5. **새로고침 / 목록으로 보기**
   - ⟳: 근태 기록 목록을 새로고침합니다.
   - ▤: 근태 기록을 목록 형식으로 확인할 수 있습니다.

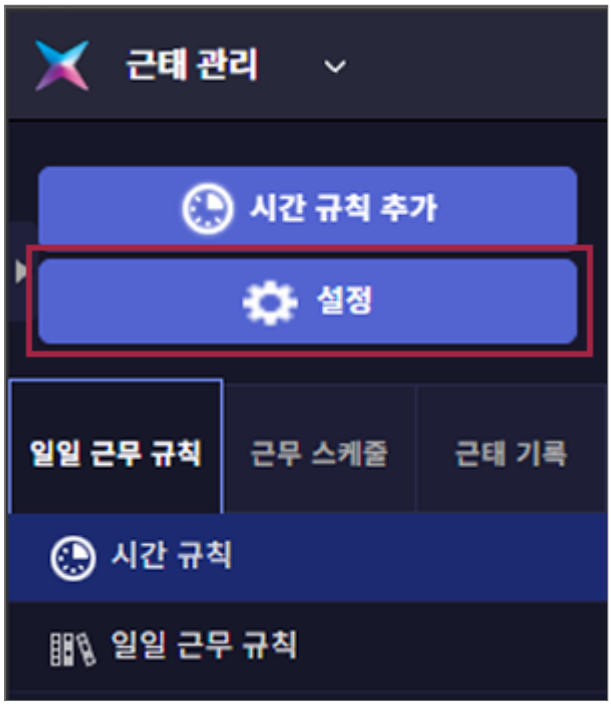
> **알아두기**
> 시간 규칙 생성에 대한 자세한 내용은 시간 규칙 설정하기를 참고하세요.

근태 관리 설정하기

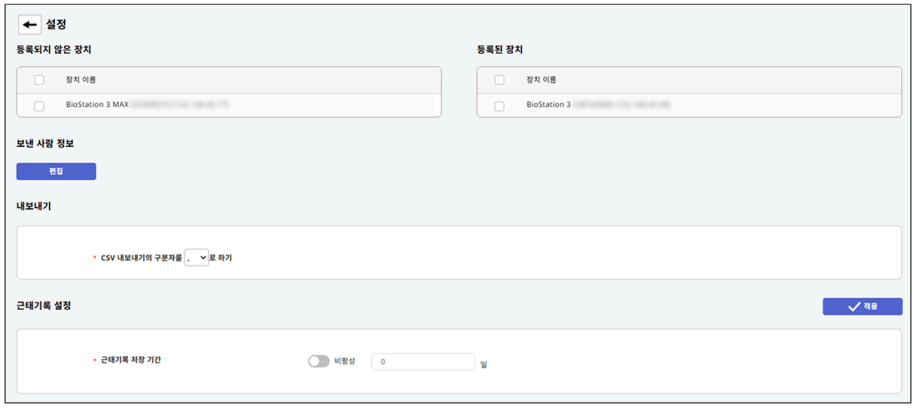
근태 관리에 사용할 장치를 등록하거나 알림 이메일을 발신할 때 사용할 발신자 정보를 설정할 수 있습니다. CSV 내보내기로 근태 보고서를 내보낼 때 문서의 구분자를 설정할 수도 있습니다.

근태 관리 설정 진입

1. **런처** 페이지에서 **근태 관리**를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **설정** 버튼을 클릭하세요.



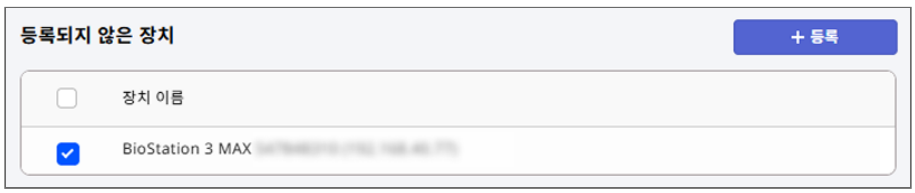
3. 각 항목을 설정하세요.



근태 관리 설정 항목

등록되지 않은 장치

근태 관리할 수 있는 장치 목록입니다. 근태 관리 장치로 등록하려면 원하는 장치를 선택한 후 **등록** 버튼을 클릭하세요.



등록된 장치

현재 사용 중인 근태 관리 장치 목록입니다.

- 등록을 해제하려면 원하는 장치를 선택한 뒤 **등록 취소** 버튼을 클릭하세요.



- 등록한 장치의 근태 설정을 편집하려면 **설정** 버튼을 클릭하세요. 근태 설정에 대한 자세한 내용은 고급 설정하기를 참고하세요.



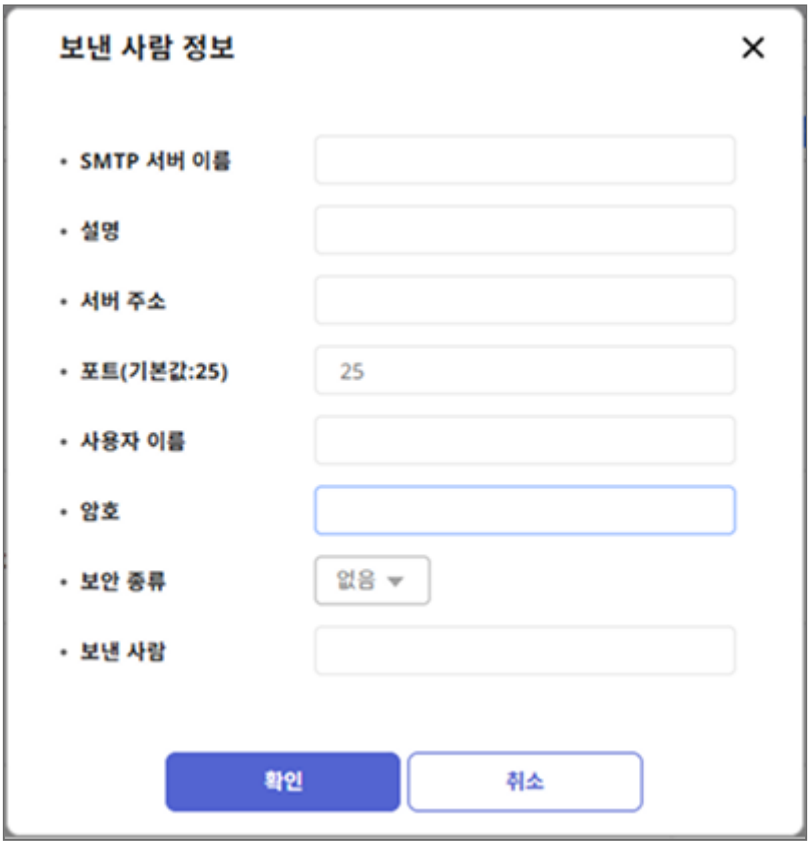
근태 유형은 **근태 키**와 근태 이벤트 종류를 매핑하는 설정입니다. 근태 이벤트 종류는 아래와 같습니다.

- **출근**
- **퇴근**
- **휴식 시작**
- **휴식 종료**
- **식사 시간 시작**
- **식사 시간 종료**

> **알아두기**
>
> - 장치와 연결된 상태에서만 장치의 근태 설정을 편집할 수 있습니다.
> - **설정** → **장치** → **장치** 메뉴에서 등록한 장치를 삭제하면, 등록된 근태 관리 장치도 자동 삭제됩니다.
> - 장치에서 **다중 얼굴 인증** 옵션을 **사용**으로 설정하면 근태 관리에 사용할 수 없습니다. **다중 얼굴 인증**에 대한 자세한 내용은 인증 설정하기를 참고하세요.

보낸 사람 정보

알림 이메일을 발신할 때 사용할 발신자 정보를 설정할 수 있습니다. **편집** 버튼을 클릭하세요.



- **SMTP 서버 이름**: SMTP 서버 이름을 입력하세요.
- **설명**: SMTP에 대한 설명을 입력하세요.
- **서버 주소**: SMTP 서버 주소를 입력하세요. SMTP 서버 주소는 `smtp.{email-service-provider}.com`과 같은 형태이며, SMTP 서버로 사용할 이메일의 설정 화면에서 확인할 수 있습니다.
- **포트(기본값:25)**: SMTP 서버의 포트 번호를 입력하세요. SMTP 서비스 공급자의 이메일 설정 화면에서 확인할 수 있습니다.
- **사용자 이름**: SMTP 서비스의 계정을 입력하세요.
- **암호**: SMTP 서비스의 계정 암호를 입력하세요.
- **보안 종류**: 보안 종류를 선택하세요.
- **보낸 사람**: 보낸 사람의 이메일 주소를 입력하세요.

> **알아두기**
>
> - SMTP에 대한 자세한 내용은 시스템 관리자에게 문의하세요.
> - SMTP 서버를 2단계 인증이 설정된 이메일 계정으로 사용할 경우 해당 계정의 비밀번호 변경 시 다음 사항에 유의하세요.
>   - 2단계 인증을 설정하면 SMTP 암호는 해당 이메일 계정의 비밀번호가 아닌 2단계 인증으로 생성된 앱 비밀번호를 사용합니다.
>   - 이때 해당 이메일 계정의 비밀번호가 변경되면 앱 비밀번호는 자동으로 삭제되며, SMTP 암호는 사용할 수 없게 됩니다.
>   - 해당 이메일 계정의 비밀번호 변경 시 앱 비밀번호를 다시 생성한 뒤 SMTP 암호를 다시 설정하세요.

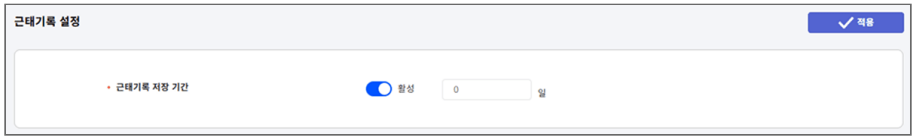
내보내기

CSV 내보내기 기능으로 근태 보고서를 내보낼 때 문서의 구분자를 선택할 수 있습니다.



근태기록 설정

근태 기록을 저장할 기간을 설정할 수 있습니다. **근태기록 저장 기간** 옵션을 **활성**으로 설정하고 기간을 입력하세요. 설정을 저장하려면 **적용** 버튼을 클릭하세요.



근태 감사 로그 조회하기

T&A 감사 로그 기능은 근무·스케줄·리포트 등 근태 관리와 관련된 모든 활동을 기록합니다. 각 기록은 언제, 누가, 무엇을, 어떻게 변경했는지 함께 보여주므로 보안 감사와 문제 해결에 활용할 수 있습니다.

> **알아두기**
> **T&A 감사 로그** 메뉴는 근태 관리(T&A) 라이선스가 활성화되어 있고, 운영 관리자에게 이 메뉴 권한이 있어야 합니다. 근태 관리 플러그인 설치 시 기본 생성되는 **근태 관리자** 계정에는 이 권한이 없으므로, 커스텀 권한을 추가하여 설정해야 합니다.

근태 감사 권한 추가

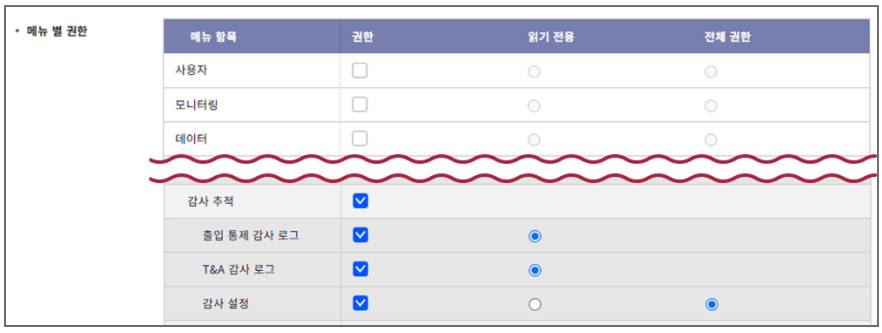
1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정** → **계정**을 클릭하세요.
3. **커스텀 권한 추가** 버튼을 클릭하세요.



4. 근태 감사 로그 조회를 위한 권한 이름과 설명을 입력하세요.



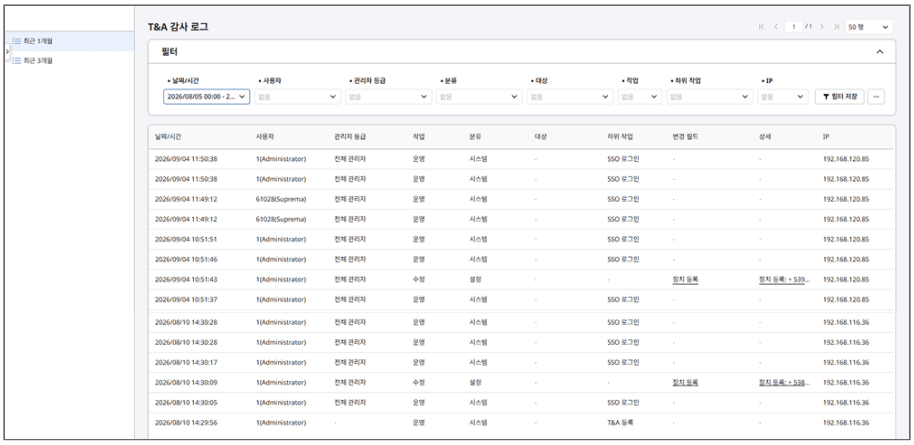
5. **메뉴 별 권한**에서 **감사 추적** 메뉴 하위의 **T&A 감사 로그** 및 **감사 설정** 항목에 권한을 설정하세요.



6. **권한 부여**에서 **+ 추가** 버튼을 클릭하고 사용자 그룹 또는 사용자를 선택하세요.
7. 커스텀 권한을 저장하려면 화면 가장 아래에 있는 **확인** 버튼을 클릭하세요.

근태 감사 로그 확인

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **감사 추적** → **T&A 감사 로그**를 클릭하세요.
3. 근태 관련 감사 로그 목록이 화면에 표시됩니다.



알아두기

- 보관 기간 등 감사 로그 정책을 변경하려면 근태 감사 설정하기를 참고하세요.
- 1.0.3 버전으로 업그레이드한 이후 새로 생성되는 감사 로그는 **설정** → **시스템** → **시스템 보안** 메뉴의 **개인 정보 DB 암호화** 옵션과 무관하게 암호화된 상태로 저장됩니다.
- BioStar 2에서 **BioStar X**로 업그레이드한 후 감사 로그가 일부 기록되지 않으면 업그레이드하기를 참고하세요.

테이블 구성

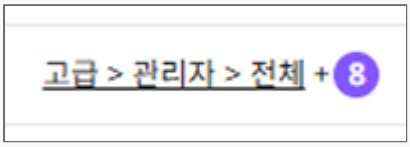
감사 로그 목록 테이블은 10개 컬럼으로 구성되며, 현재 검색 조건에 해당하는 기록을 **날짜/시간** 기준 최신순으로 표시합니다.

컬럼	설명
날짜/시간	이벤트가 발생한 날짜와 시간입니다.

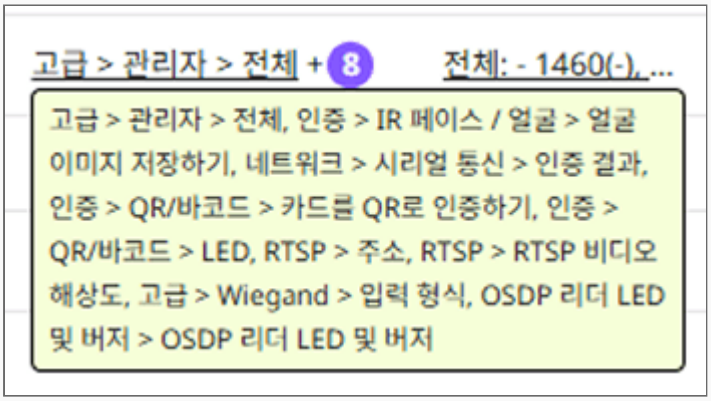
컬럼	설명
사용자	이벤트를 수행한 사용자입니다. **id(이름)** 형식으로 표시됩니다.
관리자 등급	이벤트를 수행한 사용자의 관리자 등급입니다. 시스템이 자동으로 수행한 동작은 비웁니다.
작업	수행된 동작 종류입니다. **생성**, **수정**, **삭제**, **조회**, **내보내기**, **운영** 중 하나로 분류됩니다.
분류	이벤트 대상의 도메인 분류입니다. (**일일 근무 규칙**, **스케줄**, **리포트**, **T&A 감사 로그**, **설정**, **시스템**)
대상	동작이 적용된 대상입니다. **타입: id(이름)** 형식으로 표시됩니다.
하위 작업	**운영**, **조회**, **내보내기** 동작에만 표시되는 세부 동작 이름입니다.
변경 필드	변경되거나 조회된 필드 이름입니다. **운영**은 항상 비웁니다.
상세	동작별 상세 정보입니다. (변경 값, 조회 조건, 필드 스냅샷 등)
IP	사용자가 접속한 IP 주소입니다. 시스템이 자동으로 발급한 기록은 **127.0.0.1**로 표시됩니다.

알아두기

- **작업**이 **수정**인 기록은 항상 대상 1건만 가리킵니다. 여러 대상을 한 번에 바꾸는 일괄 편집은 근태 관리에 없으므로, 대상이 여러 건으로 묶여 표시되지 않습니다.
- **사용자**, **대상**, **변경 상세**에 표시되는 이름은 그 기록이 발생한 시점의 값을 그대로 보존합니다. 이후 이름이 바뀌거나 대상이 삭제되어도 과거 기록의 표시명은 바뀌지 않습니다.
- **대상**과 **변경 필드** 값이 2건 이상이면 첫 항목만 표시되고, 나머지는 오른쪽에 잔여 건수 배지(예: **+208**)로 압축됩니다. 잔여 건수가 1,000건 이상이면 **+999**로 표기하며, 정확한 총 건수는 상세 팝업 제목에서 확인할 수 있습니다. 배지를 클릭하면 해당 셀의 상세 팝업이 열립니다.

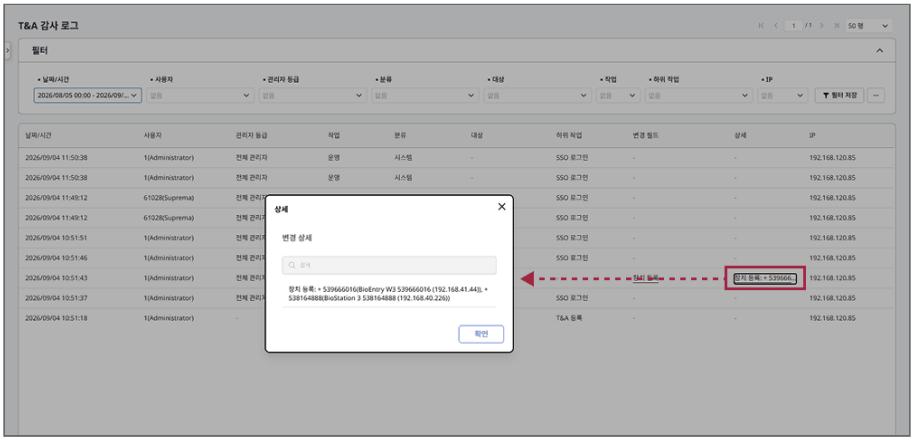


- 셀 값이 길면 한 줄로 말줄임 처리됩니다. 마우스를 오버하면 전체 값이 툴팁으로 표시되며, 툴팁을 벗어나는 길이는 **...**으로 줄여 표기됩니다.



상세 정보 확인

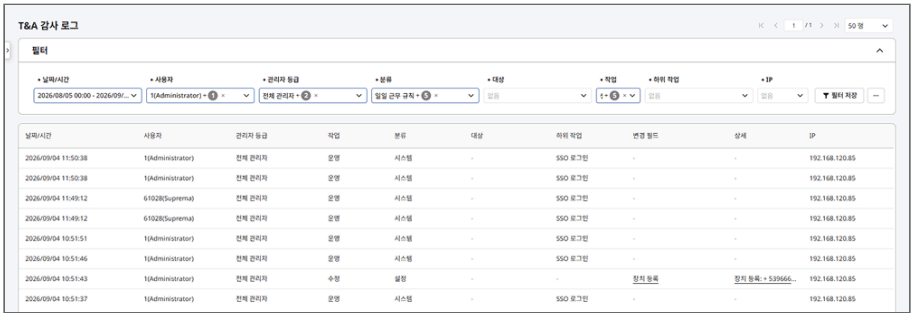
값이 있는 **대상**, **변경 필드**, **상세** 셀은 밑줄로 표시되며 클릭할 수 있습니다. 셀을 클릭하면 해당 행의 동작에 맞는 상세 팝업이 열리고, **확인** 버튼 또는 ✕ 버튼으로 닫을 수 있습니다.



팝업 상단의 **검색** 입력 필드에 검색어를 입력하면 일치하는 항목만 강조되거나 필터링됩니다. 대상 팝업은 검색 시 그룹과 그룹별 건수도 함께 갱신되지만, 제목의 전체 건수는 검색과 관계없이 그대로 유지됩니다.

필터로 원하는 기록 찾기

필터 섹션에서 제공하는 필터를 조합해 원하는 기록을 좁혀서 찾으세요. 한 필터 안에서 여러 값을 선택하면 `OR`로, 서로 다른 필터를 함께 적용하면 `AND`로 결합됩니다.



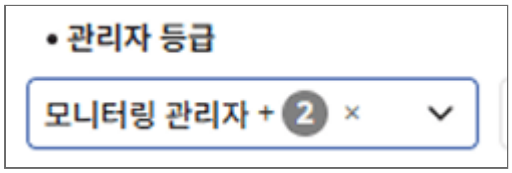
필터	동작 방식
날짜/시간	시작·종료 날짜와 시각을 지정합니다. 조회 기간에는 길이 제한이 없습니다.
사용자	검색어를 입력하고 `Enter` 키를 눌러 일치하는 사용자를 찾으세요. 처음 열면 목록이 비어 있습니다.
관리자 등급	검색어를 입력하고 `Enter` 키를 눌러 일치하는 관리자 등급을 찾으세요.
분류	검색 가능한 체크박스 목록에서 하나 이상의 분류를 선택하세요.
대상	검색어를 입력하고 `Enter` 키를 눌러 일치하는 대상을 찾으세요.
작업	체크박스 목록에서 하나 이상의 동작을 선택하세요.
하위 작업	검색 가능한 목록에서 세부 작업을 선택하세요.

필터	동작 방식
IP	검색어를 입력하고 Enter 키를 눌러 일치하는 IP를 찾으세요.

- 적용된 필터가 없으면 현재 날짜로부터 30일 전까지의 기록을 기본 표시합니다.
- 각 필터 팝업에서 원하는 값을 선택한 뒤 **조건 추가** 버튼을 클릭하면 즉시 검색에 반영됩니다. **취소**을 클릭하면 선택을 취소하고 팝업을 닫습니다.



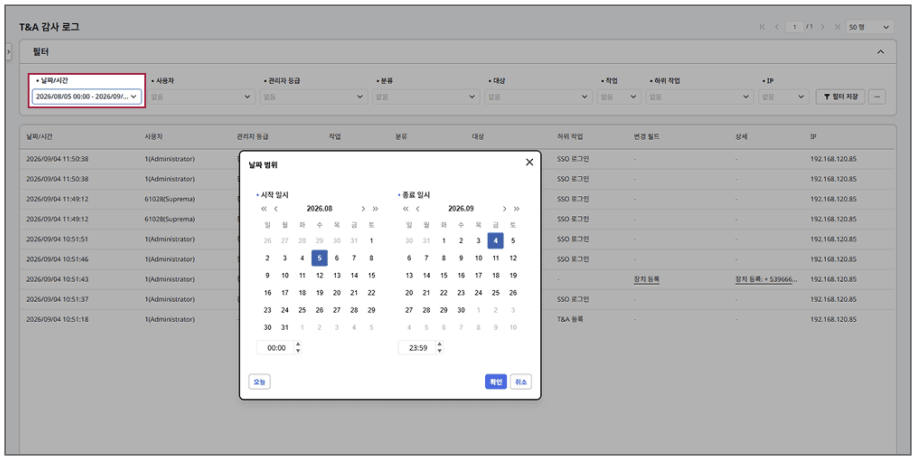
- 적용된 필터는 첫 항목과 추가 건수로 요약되어 표시됩니다. ✕를 클릭하면 해당 필터만 해제됩니다. 값을 선택하지 않은 필터는 **없음**으로 표시됩니다.



> **알아두기**
> **사용자**, **관리자 등급**, **대상**, **IP** 필터는 검색어를 입력해야 결과가 나타납니다. 부분 일치를 지원하므로 이름이나 아이디의 일부만 입력해도 됩니다. 삭제된 대상은 **삭제됨** 표기로 함께 검색됩니다.

조회 기간 지정

날짜/시간를 클릭하면 **날짜 범위** 팝업이 열립니다.

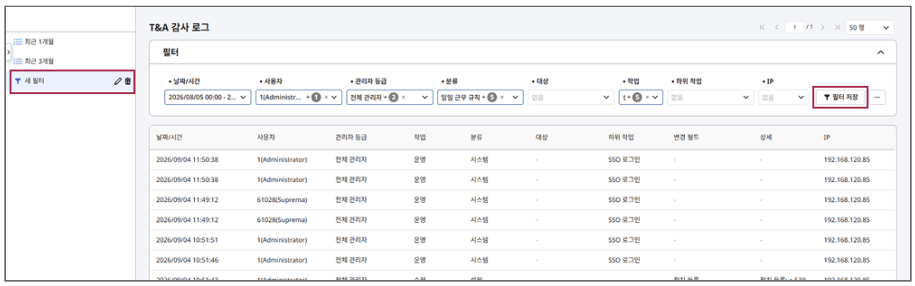


1. **시작 일시**과 **종료 일시**의 날짜와 시각을 각각 지정하세요. **오늘**를 클릭하면 오늘 날짜로 바로 이동합니다.
2. 조회 기간을 적용하려면 **확인** 버튼을 클릭하세요.

필터 저장

자주 사용하는 검색 조건은 **저장된 필터**에 저장해 두고 다시 불러올 수 있습니다.

1. 원하는 조건으로 필터를 설정하세요.
2. **필터** 섹션의 **필터 저장** 버튼을 클릭하세요.
3. 화면 왼쪽 필터 목록에 **새 필터** 항목이 추가됩니다.



- 필터 이름을 바꾸려면 ✎ 버튼을 클릭하고 새 이름을 입력한 뒤 Enter 키를 누르세요.
- 필터를 삭제하려면 🗑 버튼을 클릭하세요.

> **알아두기**
> 저장할 수 있는 필터는 최대 20개입니다. 저장한 필터는 브라우저에 보관되므로 다른 PC나 브라우저에서는 표시되지 않습니다.

연쇄 삭제로 남는 추가 기록

근무 스케줄을 수정하거나 삭제하면, 그 스케줄을 쓰던 사용자의 임시 스케줄, 부재가 함께 삭제될 수 있습니다. 이때 시스템은 근무 스케줄 자체의 변경 또는 삭제 기록과는 별개로, 실제로 삭제된 임시 스케줄, 부재마다 추가 기록을 남깁니다.

- 연쇄로 삭제된 항목이 없으면 추가 기록도 남지 않습니다.
- **대상**에는 원인이 된 근무 스케줄 1건과, 실제로 항목이 삭제된 사용자만 포함됩니다. 스케줄에 속한 사용자 전체가 아닙니다.
- **상세**에는 삭제된 건수가 표시되며, 근무 스케줄을 삭제한 경우에는 삭제 대상이 된 기간도 함께 표시됩니다.

열 설정



감사 로그 테이블의 컬럼 위치를 바꾸거나 숨길 수 있습니다. **필터** 섹션 오른쪽의 ••• → **열 설정**을 클릭하세요.

- **[열 목록]**에서 숨기려는 항목의 체크박스 선택을 해제하세요.
- 열 순서를 바꾸려면 원하는 항목을 드래그하세요.
- 열 설정을 초기화하려면 **기본 열** 버튼을 클릭하세요.

설정을 저장하려면 **적용** 버튼을 클릭하세요.

CSV로 내보내기

감사 로그를 CSV 파일로 내보내 외부 분석 도구에서 활용하세요.

1. **필터** 섹션에서 필요한 경우 필터를 설정하세요.
2. 섹션 오른쪽의 ••• → **CSV 내보내기**를 클릭하세요.
3. **CSV 내보내기** 창이 나타나면 **내보내기 사유**(선택 사항)를 입력하고 **적용** 버튼을 클릭하세요.



내보낸 CSV 파일은 레코드당 한 줄로 10개 컬럼을 모두 포함하며, 값에 쉼표가 포함된 셀만 인용 부호로 감쌉니다. **대상**과 **변경 필드**처럼 여러 값이 들어가는 셀은 버티컬 바(|)로 구분(예: Schedule: 7(Team Schedule)| User: 12(Robert))됩니다. **작업**이 **수정**인 기록의 **상세**는 말줄임 없이 전체 필드를 포함합니다.

> **주의**
> CSV 파일에는 스프레드시트 프로그램이 수식으로 해석할 수 있는 값이 원본 그대로 담깁니다. 내려받은 CSV 파일을 스프레드시트 프로그램에서 곧바로 열지 말고, 필요하면 텍스트 가져오기 기능으로 여세요.

> **팁**
> 필터를 설정했다면 필터링된 결과만 CSV 파일로 내보내집니다.

근태 감사 설정하기

감사 로그는 시간이 지날수록 계속 쌓이므로 저장 공간과 개인정보 보호 관점에서 보관 기간을 관리해야 합니다. **감사 설정**에서 **T&A 감사 로그** 기록의 보관 기간과 조회 기록 여부를 설정하세요.

권한 안내

전체 관리자는 **감사 설정** 메뉴에서 항상 조회하고 변경할 수 있습니다. 커스텀 권한 관리자는 **메뉴 별 권한**에서 **감사 설정** 메뉴 항목을 **읽기 전용**으로 적용하면 조회만, **전체 권한**으로 적용하면 조회와 변경 모두 할 수 있습니다.

> **알아두기**
>
> - 근태 관리 플러그인 설치 시 기본 생성되는 근태 관리자 계정에는 이 권한이 없으므로, 필요하면 별도로 권한을 부여해야 합니다.
> - 근태 감사 권한 추가에 대한 자세한 내용은 근태 감사 로그 조회하기를 참고하세요.

감사 설정 열기

1. **런처** 페이지에서 **설정**을 클릭하세요.
2. 화면 왼쪽 사이드바에서 **감사 추적** → **감사 설정**을 클릭하세요.
3. 화면을 아래로 스크롤하여 **근태 관리** 섹션으로 이동하세요.



보관 정책 설정

근태 관리 섹션은 다음 두 그룹으로 구성됩니다.

- **변경(생성, 수정, 삭제)**: 생성, 수정, 삭제 기록입니다. 항상 기록되며 끄거나 켤 수 없습니다.
- **조회**: 조회 기록입니다. 기록 여부를 직접 설정할 수 있습니다.

> **알아두기**
>
> - **보존 기간**은 최소 1일, 최대 2,147,483,647까지 정수로 입력할 수 있습니다.
> - **근태 관리** 섹션의 설정 변경 사항은 **T&A 감사 로그**에 **수정** 기록으로 확인할 수 있습니다.

변경 기록

변경(생성, 수정, 삭제) 그룹은 항상 기록되므로, 원하는 **보존**을 선택하세요.

- **영구**: 자동 삭제 없이 기록을 영구 보관합니다.
- **사용자 정의**: 규정이나 내부 정책에 따라 보관 기간을 제한해야 한다면 이 옵션을 선택하세요. **보존 기간** 입력칸이 활성화되면, 보관 기간을 일 단위로 입력하세요.

조회 기록

조회 그룹에서 조회 기록을 남길지 여부를 직접 정할 수 있습니다.

- **기록**: 조회 기록을 남기려면 **사용**으로 설정하세요. 필요하지 않으면 **사용 안 함** 상태로 설정하세요.
- **보존**: 원하는 보관 방식을 선택하세요.
  - **영구**: 조회 기록을 자동 삭제 없이 영구 보관합니다.
  - **사용자 정의**: **보존 기간** 입력칸이 활성화됩니다. 원하는 보관 기간을 일 단위로 입력하세요.

> **알아두기**
>
> **기록**이 **사용 안 함**으로 설정되어 있다면, 조회 이벤트 자체를 기록하지 않습니다. 이후 **사용**으로 설정해도 이전 기간의 기록은 조회할 수 없습니다.

설정 저장

변경(생성, 수정, 삭제)과 **조회** 설정을 완료했다면, **근태 관리** 섹션 하단의 **적용** 버튼을 클릭하세요. 두 그룹의 설정값을 함께 저장합니다.

자동 삭제 동작 방식

사용자 정의에서 설정한 보관 기간을 초과한 기록은 사용자 조작과 관계없이 서버가 매일 오전 1시에 실행하는 작업에서 자동 삭제합니다. 판정과 삭제는 같은 작업에서 한 번에 일어나며, 이 판정은 하루에 한 번만 이뤄집니다.

> *예를 들어, **조회** 기록을 **사용자 정의** 방식으로 30일 적용했다면, 오전 1시 작업 실행 시점을 기준으로 30일을 초과한 기록이 그 작업에서 바로 삭제됩니다. 보관 기간을 막 넘긴 기록이라도 작업이 하루에 한 번만 실행되므로, 그 시점이 지나야 다음 날 오전 1시 작업에서 삭제됩니다.*

보존을 **영구**로 설정하면 자동 삭제 작업이 동작하지 않아 기록이 영구 보존됩니다.

방문자 신청 및 관리하기

방문자 기능을 사용해 방문 신청용 PC에 방문 신청 페이지를 생성하고, 방문자 관리용 PC에서 방문자의 출입을 관리할 수 있습니다.

알아두기

- **방문자** 기능은 **에센셜**(Essential) 라이선스 이상에서 추가 옵션을 통해 사용할 수 있습니다. 라이선스 정책에 대한 자세한 내용은 라이선스 정책을 참고하세요.
- 방문자 기능을 라이선스를 통해 활성화한 후 설정 방법에 대한 자세한 내용은 방문자 설정하기를 참고하세요.

방문자 라이선스 적용

방문자 라이선스 적용 방법을 안내합니다. **BioStar X** 구입처로부터 방문자 라이선스를 구입한 후 다음 안내에 따라 라이선스를 적용하세요.

1. **BioStar X** 관리자 계정으로 로그인하세요.
2. **런처** 페이지에서 **설정**을 클릭하세요.
3. 화면 왼쪽 사이드바에서 **라이선스** → **BioStar X 라이선스**를 클릭하세요.
4. **라이선스 활성화**에서 **등록 관리자**와 **라이선스 키** 항목을 차례로 입력하세요.



5. **활성화** 버튼을 클릭하세요.

등록한 라이선스는 **활성화된 라이선스**에서 확인할 수 있습니다.

알아두기

폐쇄된 네트워크 환경이나 인터넷 연결이 제한된 오프라인 상태에서 라이선스를 활성화하려면 BioStar X 라이선스를 참고하세요.

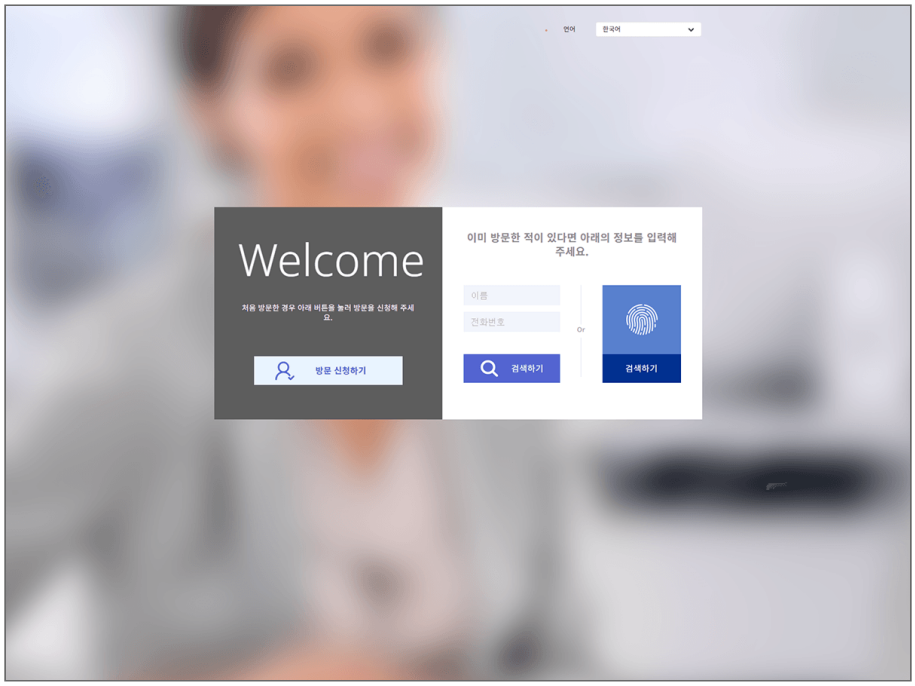
팁

방문자 라이선스를 적용하면 **설정** → **방문자** 메뉴가 활성화되고, 화면 왼쪽 상단의 바로가기 목록에서 **방문자** 관리 페이지로 이동할 수 있는 링크가 추가됩니다.

방문 신청 페이지 설정

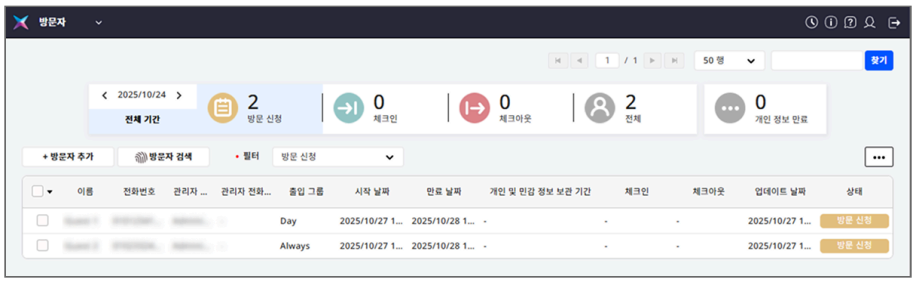
방문 신청 페이지는 방문자 설정을 우선 진행한 후 사용할 수 있습니다. 방문 신청 페이지 설정 방법에 대한 자세한 내용은 방문자 설정하기를 참고하세요.

방문 신청 페이지는 별도의 방문 신청용 PC에서 접속할 수 있으며, 방문자가 출입을 신청할 수 있습니다. 방문 신청에 대한 자세한 내용은 방문 신청하기를 참고하세요.



방문자 출입 관리

방문 신청 내역을 확인하고 방문자의 출입을 관리할 수 있습니다. 방문자 출입 관리 방법에 대한 자세한 내용은 방문 신청 관리하기를 참고하세요.



방문 신청하기

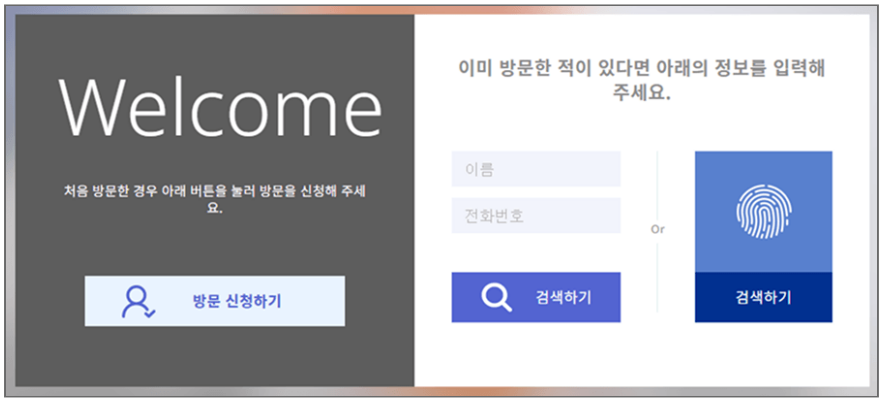
사내 사용자가 아닌 외부 방문자가 방문 신청용 PC를 통해서 출입을 신청하는 방법을 안내합니다.

> **알아두기**
>
> - 방문 신청용 PC는 별도로 구성해야 하며, 방문자 설정이 선행되어야 합니다. 방문자 설정 방법에 대한 자세한 내용은 방문자 설정하기를 참고하세요.
> - 방문 신청용 PC에 방문 신청 페이지 바로가기 아이콘이 없는 경우, 방문자 설정하기를 참고해 바로가기 아이콘을 생성하세요.

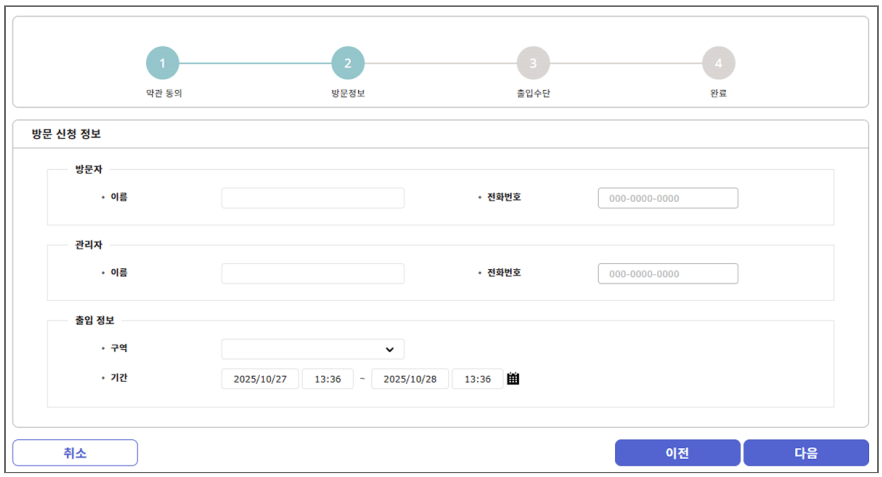
신규 방문 신청

처음 방문하는 방문자가 방문 신청용 PC에서 출입을 신청하는 방법을 안내합니다.

1. 방문 신청용 PC에서 방문 신청 페이지를 실행하세요. 방문 신청 페이지 URL 주소는 `https://{biostar_x_server_ip}/#/register-welcome` 형식입니다.

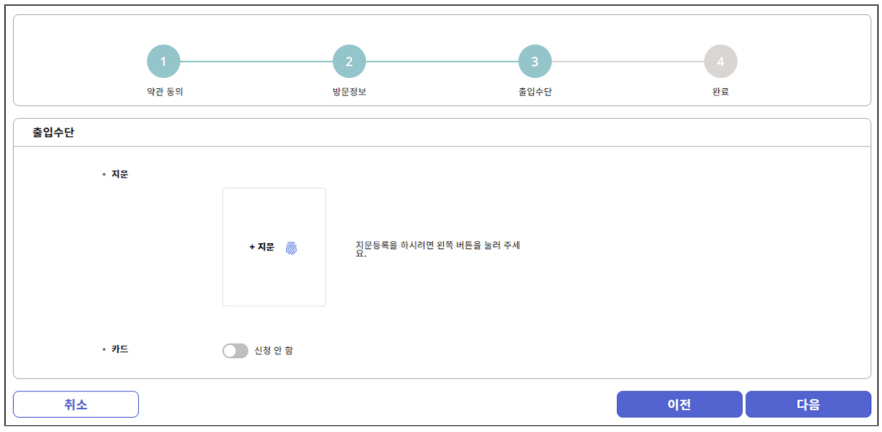


2. 화면 중앙의 **방문 신청하기**를 클릭하세요.
3. 방문처 출입에 대한 약관 및 개인 정보 처리 방침에 대한 동의를 완료한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.
4. 방문 신청에 필요한 정보를 입력하세요.



- **방문자**: 방문자의 이름과 전화번호를 입력하세요.
- **관리자**: 방문 대상 담당자의 이름과 전화번호를 입력하세요.
- **출입 정보**: 출입 구역 및 방문 기간을 설정하세요.

5. 정보 입력을 완료한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.
6. 출입 수단을 설정하세요.



- **지문**: 지문 인증을 사용하려면 **+ 지문** 버튼을 클릭한 후 지문을 등록하세요.

- **카드**: 카드 인증을 사용하려면 **신청**으로 설정한 후 관리자에게 카드를 발급 받으세요.

7. 설정을 완료한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.
8. 신청한 모든 정보를 확인한 후 화면 오른쪽 하단의 **등록** 버튼을 클릭하세요.



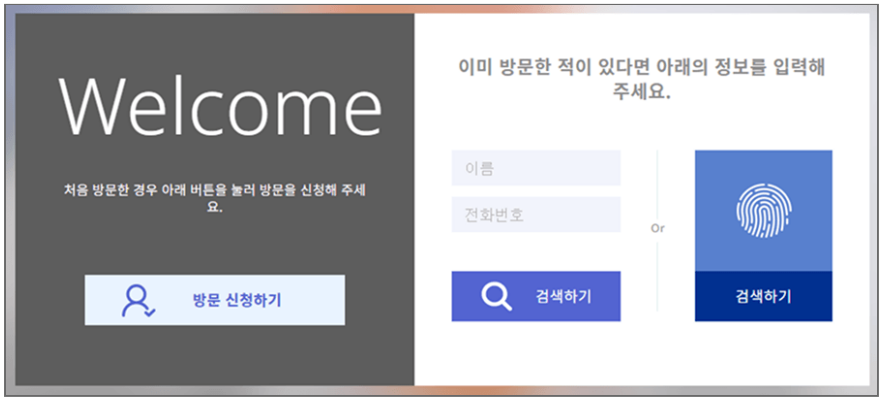
알아두기

- 방문처 출입에 대한 약관 및 개인 정보 처리 방침 작성에 대한 자세한 내용은 방문자 설정하기를 참고하세요.
- 이름은 최대 48자까지 입력할 수 있습니다.
- 방문자 정보 입력에 커스텀 필드를 추가하려면 방문자 설정하기를 참고하세요.
- 방문 PC에 할당한 방문처의 출입 그룹만 선택할 수 있습니다. 자세한 내용은 방문자 설정하기를 참고하세요.
- 출입 그룹에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.
- 이전 단계로 돌아가 방문 정보를 수정하려면 **이전** 버튼을 클릭하세요.
- 지문을 스캔하려면 방문자 신청용 PC에 지문 등록 장치가 연결되어 있어야 합니다.

기존 정보로 방문 신청

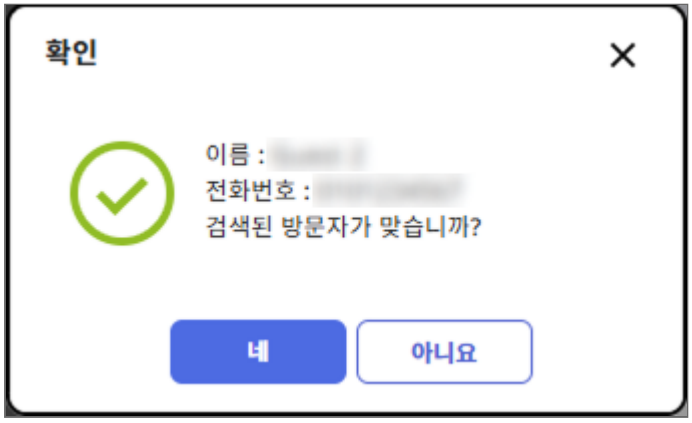
방문처에 지문이 등록되어 있다면 지문을 검색한 뒤 기존 방문 정보를 사용해 방문을 신청할 수 있습니다.

1. 방문 신청용 PC에서 방문 신청 페이지를 실행하세요. 방문 신청 페이지 URL 주소는 `https://{biostar_x_server_ip}/#/register-welcome` 형식입니다.

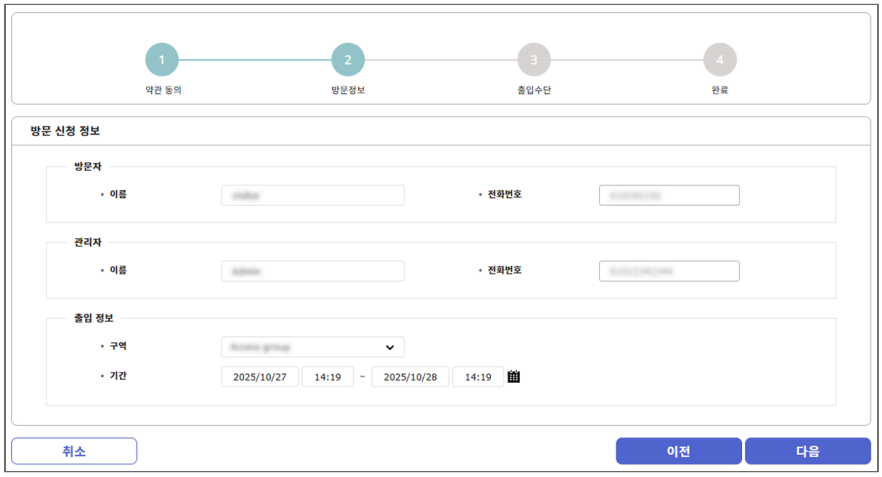


2. 화면 중앙에 있는 지문 아이콘 하단의 **검색하기**를 클릭하세요.

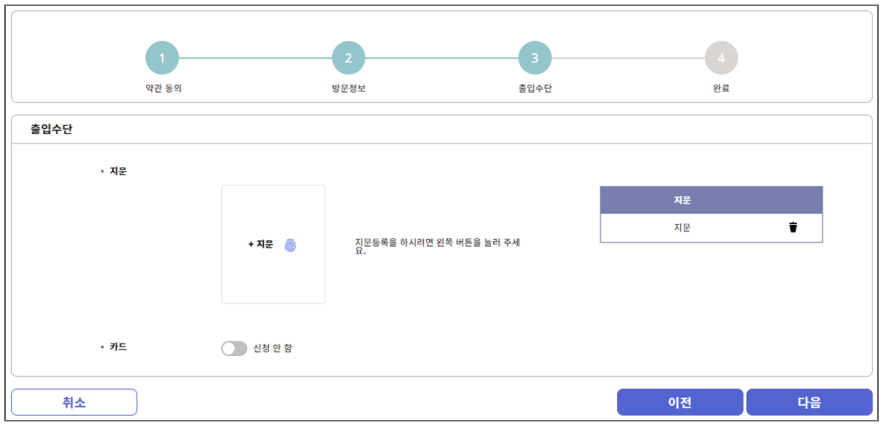
3. 지문 스캔 장치에 지문을 스캔하세요. 스캔한 지문을 이용해 등록된 사용자를 검색합니다.
4. 이전에 지문을 등록한 방문자와 일치하는 지문이 있다면 확인 메시지가 나타납니다.



5. 검색된 방문자가 맞는다면 **네** 버튼을 클릭하세요.
6. 방문처 출입에 대한 약관 및 개인 정보 처리 방침에 대한 동의를 완료한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.
7. 이전 방문 시 설정한 방문 정보를 확인하세요. 기존 정보를 수정하려면 각 항목을 수정한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.



8. 이전 방문 시 설정한 출입 수단을 확인하세요. 기존 출입 수단을 변경하려면 변경할 항목을 수정한 후 화면 오른쪽 하단의 **다음** 버튼을 클릭하세요.



9. 신청한 모든 정보를 확인한 후 화면 오른쪽 하단의 **등록** 버튼을 클릭하세요.



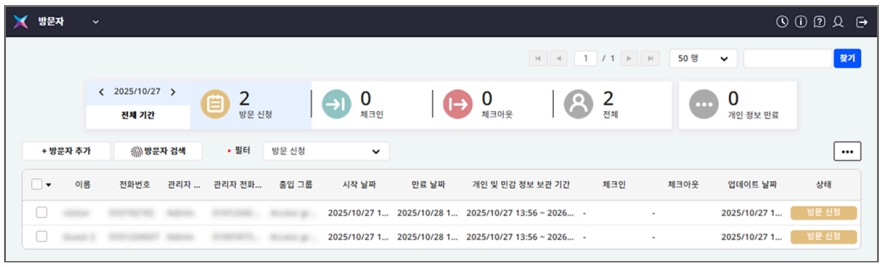
방문 신청 관리하기

방문 신청을 승인하거나 수정할 수 있습니다. 관리자가 직접 방문자를 추가하거나 삭제할 수도 있습니다.

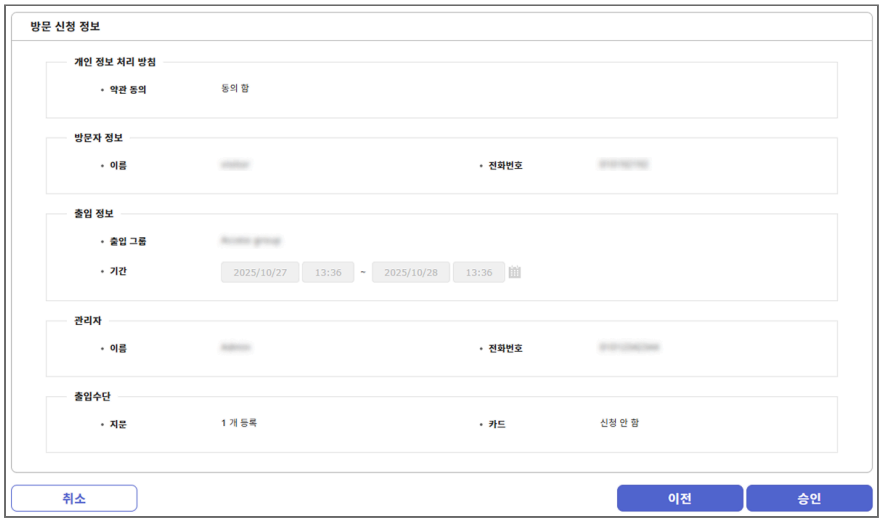
방문 승인

방문 신청 내역을 확인하고 방문자의 출입을 승인하는 방법을 안내합니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 방문자 목록에서 방문을 승인할 방문자를 클릭하세요.



3. 방문자의 방문 정보를 확인한 후 수정 필요한 항목은 수정 후 **수정** 버튼을 클릭하세요.
4. 화면 오른쪽 하단의 **체크인** 버튼을 클릭하세요.
5. **방문 신청 정보**의 내용을 확인하고 방문을 승인하려면 화면 오른쪽 하단의 **승인** 버튼을 클릭하세요.

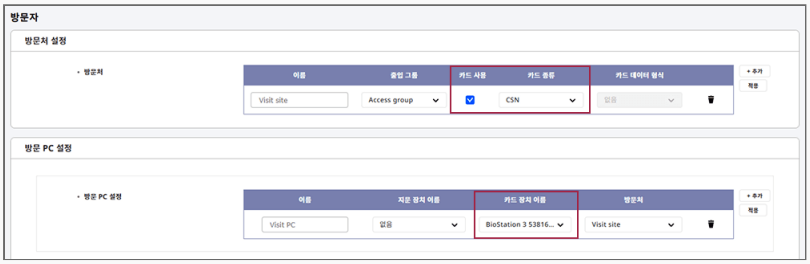


알아두기

- 방문을 신청할 때 방문자 출입 이용 약관에 동의하지 않은 신청자의 경우 **승인** 버튼이 비활성화됩니다. **약관 보기** 버튼을 클릭해 방문자에게 출입 이용 약관을 제공하고, 약관 동의를 받으세요. 방문자 출입 이용 약관에 동의하지 않는다면 방문이 제한됩니다.



- 방문 PC에 카드 등록 장치가 설정되어 있다면 **승인 및 카드등록** 버튼이 활성화됩니다. 방문자의 방문을 승인하고 출입 카드를 발급하려면 **승인 및 카드등록** 버튼을 클릭하세요. 자세한 내용은 승인 및 카드 등록을 참고하세요.
- 방문 PC에 카드 사용을 설정하려면 **설정** → **방문자** 메뉴에서 아래와 같은 최소 설정이 필요합니다. 자세한 내용은 방문자 설정하기를 참고하세요.

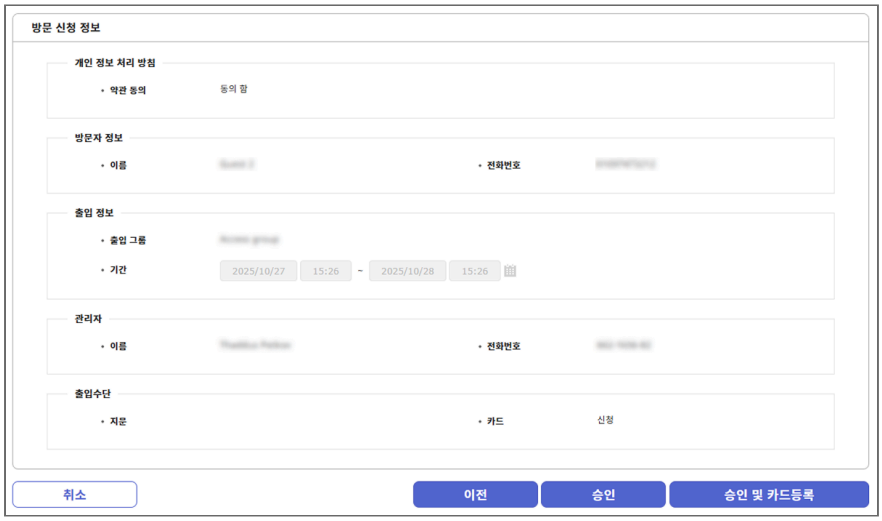


  - **방문처 설정** → **카드 사용** / **카드 종류**
  - **방문 PC 방문 PC 설정** → **카드 장치 이름**

승인 및 카드 등록

방문 신청을 승인하고 출입 카드를 발급하는 방법을 안내합니다.

1. **방문 신청 정보** 화면에서 화면 오른쪽 하단의 **승인 및 카드등록** 버튼을 클릭하세요.



2. 카드 등록 창이 나타나면 원하는 등록 방법을 선택하세요.

   - **리더로 등록**
   - **직접 입력**

리더로 등록

방문 PC에 연결된 장치로 카드 정보를 스캔하여 등록할 수 있습니다.

1. **등록 방법**을 **리더로 등록**으로 선택하세요.



2. 등록할 카드를 장치에 스캔하려면 **카드 읽기** 버튼을 클릭하세요.
3. 카드를 등록하려면 **등록** 버튼을 클릭하세요.

직접 입력

카드 번호를 직접 입력하여 등록할 수 있습니다.

1. **등록 방법**을 **직접 입력**으로 선택하세요.

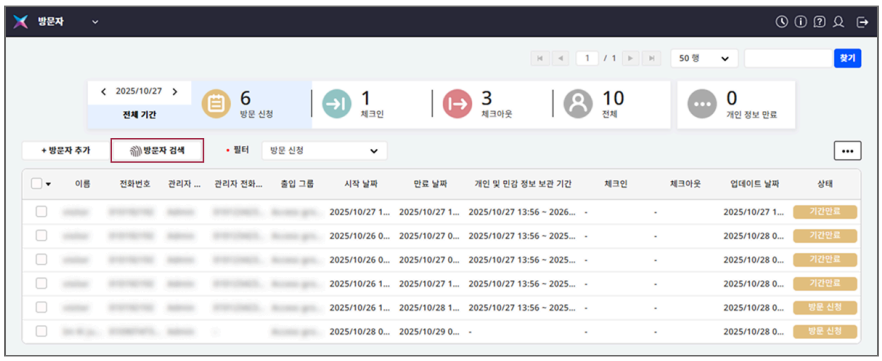


2. **카드 ID**를 직접 입력하세요.
3. 카드를 등록하려면 **등록** 버튼을 클릭하세요.

지문 검색으로 방문자 승인

지문을 등록한 방문자를 지문으로 검색한 후 승인 처리할 수 있습니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 방문 신청 목록에서 왼쪽 상단의 **방문자 검색** 버튼을 클릭하세요.



3. 지문 스캔 장치에 방문자의 지문을 스캔하세요.
4. 지문과 일치하는 방문자가 검색되면 확인 메시지가 나타납니다. **신청 정보** 버튼을 클릭하세요.

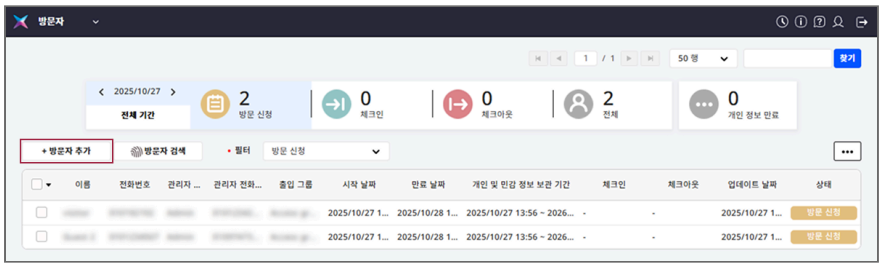


5. 방문자의 방문 정보를 확인한 후 수정 필요한 항목은 수정 후 **수정** 버튼을 클릭하세요.
6. 화면 오른쪽 하단의 **체크인** 버튼을 클릭하세요.
7. **방문 신청 정보**의 내용을 확인하고 방문을 승인하려면 화면 오른쪽 하단의 **승인** 버튼을 클릭하세요.

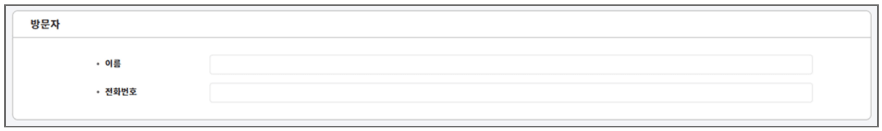
방문자 추가

관리자가 직접 방문자를 추가하는 방법을 안내합니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 방문자 목록에서 왼쪽 상단의 ＋ **방문자 추가** 버튼을 클릭하세요.



3. **방문자** 섹션에서 방문자의 이름과 전화번호를 입력하세요.

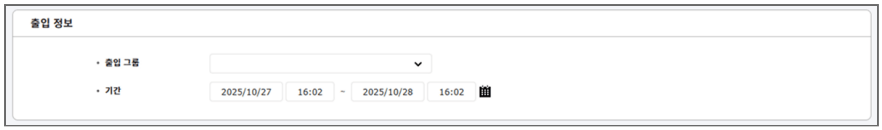


4. **관리자** 섹션에서 방문 대상 담당자의 이름과 전화번호를 입력하세요.



> 이름 또는 전화번호를 입력하면 입력 정보와 일치하는 사용자 목록이 표시됩니다. 원하는 사용자를 지정하려면 **선택** 버튼을 클릭하세요.

5. **출입 정보** 섹션에서 출입 그룹 및 방문 기간을 설정하세요.



> 방문 PC에 할당한 방문처의 출입 그룹만 선택할 수 있습니다. 자세한 내용은 방문자 설정하기를 참고하세요.

6. **크리덴셜** 섹션에서 출입 수단을 설정하세요.



- **카드**: 카드 인증을 사용하려면 **신청**으로 설정하세요.

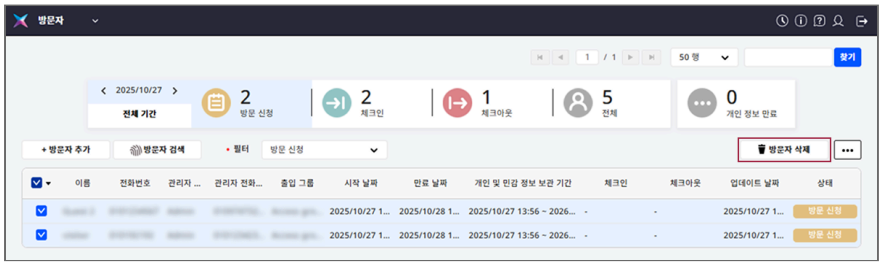
- **지문**: 지문 인증을 사용하려면 **+ 지문** 버튼을 클릭한 후 방문자의 지문을 등록하세요.

7. 방문자 추가를 완료하려면 화면 오른쪽 하단의 **등록** 버튼을 클릭하세요.

> **알아두기**
>
> - 이름은 최대 48자까지 입력할 수 있습니다.
> - 방문자 정보 입력에 커스텀 필드를 추가하려면 방문자 설정하기를 참고하세요.

방문자 삭제

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 방문 신청 목록에서 삭제할 방문자의 체크박스를 클릭하세요.



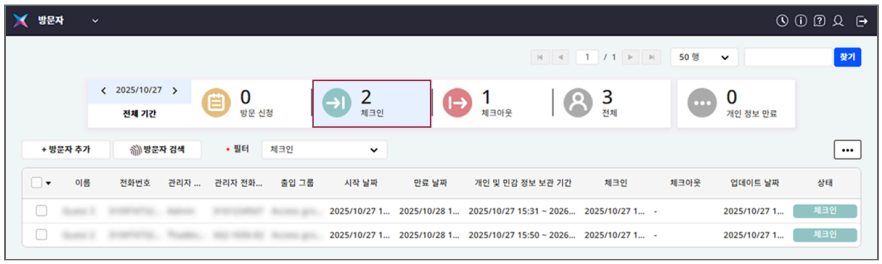
3. 화면 오른쪽 상단의 **방문자 삭제** 버튼을 클릭하세요.
4. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.

> **알아두기**
>
> - **방문자 삭제** 버튼은 방문자의 체크박스를 클릭하면 활성화됩니다.
> - 방문자는 방문 신청 목록에서만 삭제할 수 있습니다.

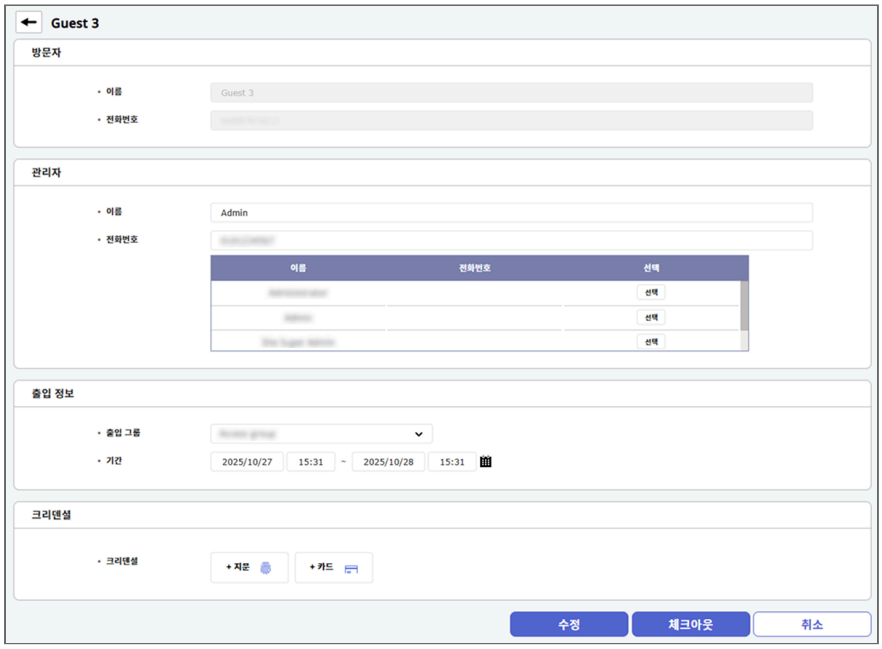
체크인 방문자 관리하기

체크인 상태의 방문자를 확인하고 방문 정보를 수정하거나 체크아웃 처리할 수 있습니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 화면 상단의 **체크인** 탭을 클릭하세요.

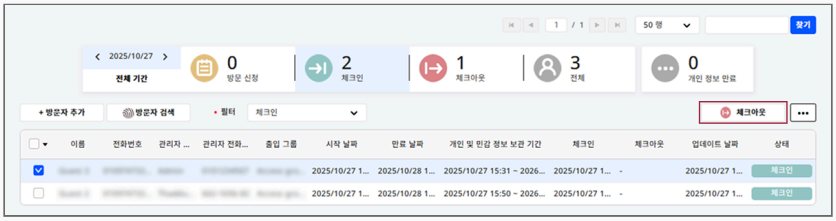


3. 방문자 목록에서 수정 또는 체크아웃할 방문자를 클릭하세요.
4. 방문자의 방문 신청 정보를 확인하세요.



- 개별 항목을 수정하고 저장하려면 화면 오른쪽 하단의 **수정** 버튼을 클릭하세요.
- 체크아웃 처리하려면 화면 오른쪽 하단의 **체크아웃** 버튼을 클릭하세요.

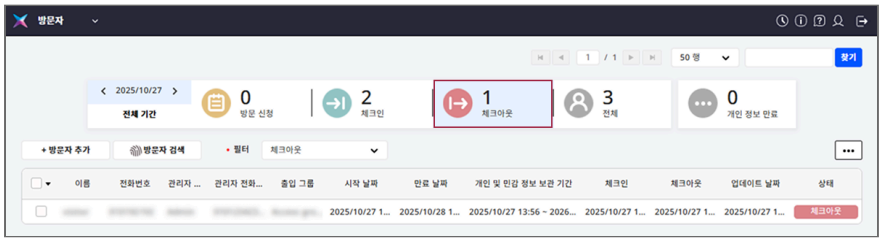
> **알아두기**
>
> **체크인** 목록에서도 방문자를 선택해 체크아웃 처리할 수 있습니다. 목록에서 체크아웃할 방문자의 체크박스를 클릭하고 화면 오른쪽 상단의 **체크아웃** 버튼을 클릭하세요.



체크아웃 방문자 관리하기

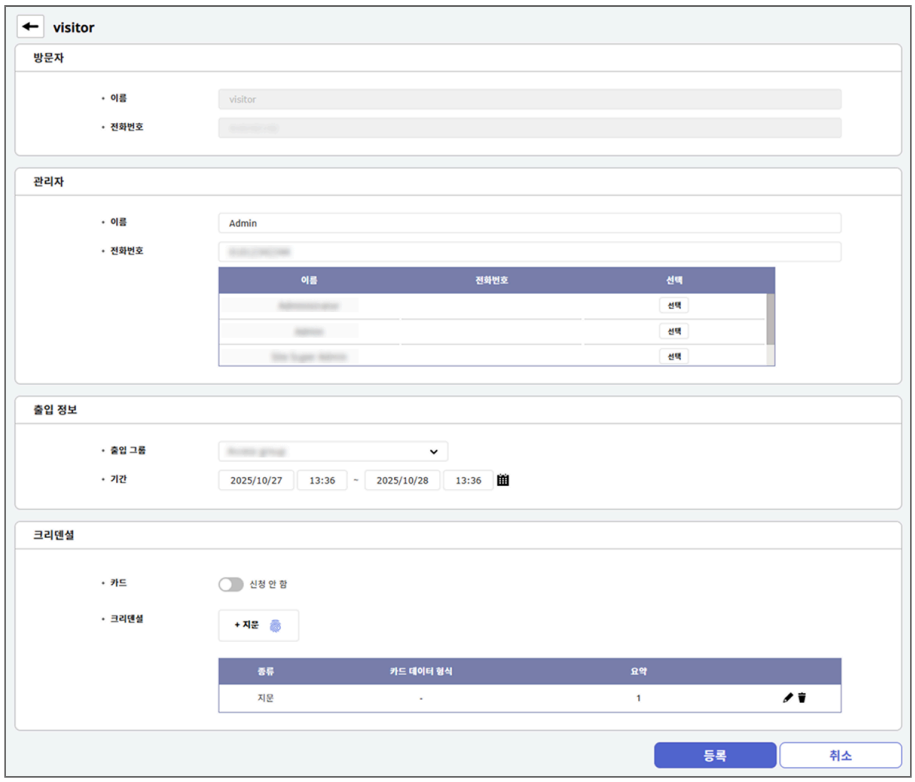
체크아웃 상태의 방문자를 확인하고 해당 방문 신청 정보를 사용해 다시 방문을 등록할 수 있습니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 화면 상단의 **체크아웃** 탭을 클릭하세요.



3. 방문자 목록에서 다시 등록할 방문자를 클릭하세요.
4. 화면 오른쪽 하단의 **수정** 버튼을 클릭하세요.

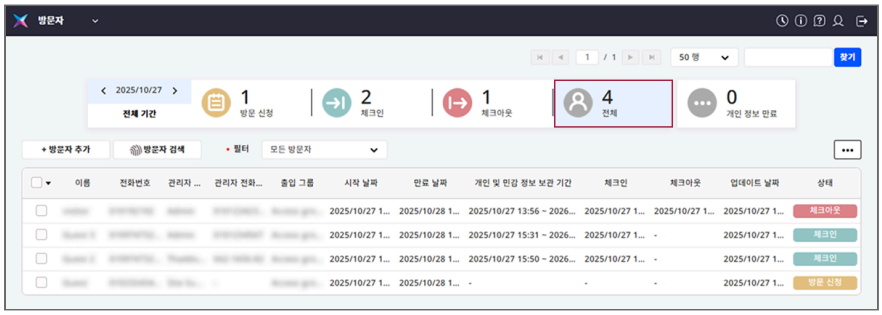
5. 수정 필요한 항목이 있다면 개별 항목을 수정한 후 **등록** 버튼을 클릭하세요.



재등록한 방문자가 방문 신청 목록에 추가됩니다. 화면 상단의 **방문 신청** 탭을 클릭해 확인하세요.

전체 방문자 관리하기

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 화면 상단의 **전체** 탭을 클릭하세요.



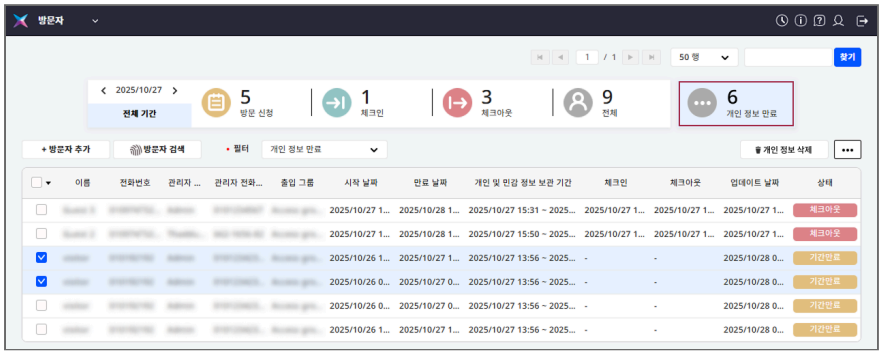
알아두기

- 전체 방문자 목록에서 방문 신청을 승인하거나 방문자를 추가할 수 있습니다. 자세한 내용은 방문 신청하기를 참고하세요.
- 전체 방문자 목록에서 체크인 또는 체크아웃 상태의 방문자를 관리할 수 있습니다. 자세한 내용은 다음 문서를 참고하세요.
  - 체크인 방문자 관리하기
  - 체크아웃 방문자 관리하기

개인 정보 만료 방문자 삭제하기

개인 정보 보관 기간이 만료된 방문자 정보를 삭제할 수 있습니다.

1. **런처** 페이지에서 **방문자**를 클릭하세요.
2. 화면 상단의 **개인 정보 만료** 탭을 클릭하세요.
3. 개인 정보 보관 기간이 초과한 방문자 목록이 표시되면 삭제할 방문자의 체크박스를 클릭하세요. 1명 이상을 선택할 수 있습니다.



4. 방문자 목록에서 오른쪽 상단의 **개인 정보 삭제** 버튼을 클릭하세요.
5. 확인 메시지가 나타나면 **네** 버튼을 클릭하세요.

> **알아두기**
>
> - **전체 관리자** 권한을 가진 사용자만 개인 정보 만료 방문자 목록을 확인할 수 있습니다. 사용자 권한에 대한 자세한 내용은 사용자 등록하기를 참고하세요.
> - 개인 정보 보관 기간 설정에 대한 자세한 내용은 방문자 설정하기를 참고하세요.

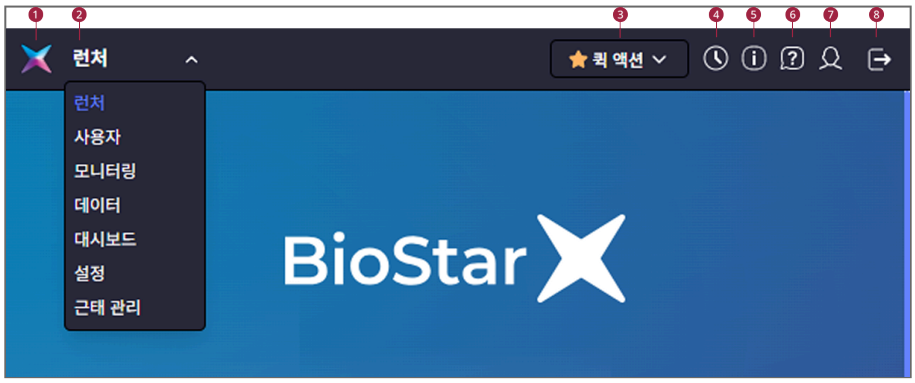
UI 알아보기

BioStar X의 각 페이지의 UI를 알아보고 사용 방법을 안내합니다. BioStar X는 다양한 기능을 제공하며, 각 기능은 사용자 인터페이스(UI)를 통해 쉽게 접근할 수 있습니다. 각 페이지의 사용자 인터페이스를 살펴보면, BioStar X의 기능을 보다 쉽게 이해하고 활용할 수 있습니다. 아래는 BioStar X의 주요 페이지와 그 UI 구성 요소에 대한 설명입니다.

공통 UI 이해하기

BioStar X의 사용자 인터페이스(User Interface, 이하 UI)는 사용자가 시스템을 쉽게 탐색하고 사용할 수 있도록 설계되었습니다. 이 문서에서는 **BioStar X**의 공통 UI 구성 요소를 안내합니다. 이 문서를 통해 **BioStar X**의 UI를 이해하고, 시스템을 보다 효율적으로 사용할 수 있습니다.

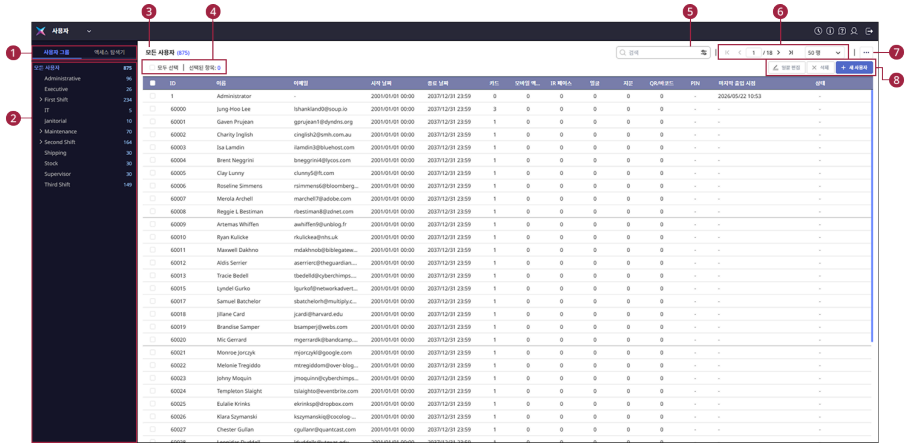
화면의 헤더 영역은 모든 페이지에서 공통으로 사용되며, **BioStar X**의 다양한 기능에 접근할 수 있는 링크 버튼을 제공합니다.



1. **BioStar X 로고**: 사용자가 **BioStar X**의 **런처** 페이지로 돌아갈 수 있는 링크 버튼입니다.
2. **바로가기**: **BioStar X**에서 제공하는 주요 페이지로 이동할 수 있는 링크를 제공합니다.
3. **퀵 액션**: 서버 사용자가 설정한 **액션**(Action) 기능을 실행할 수 있습니다. 버튼을 클릭하면 액션 목록이 나타납니다. 자세한 내용은 퀵 액션 사용하기를 참고하세요.
4. **서버 시간**: 운영 중인 **BioStar X** 서버의 서버 시간을 확인할 수 있습니다. 마우스를 버튼 위로 오버하면 현재 서버 시간이 표시됩니다.
5. **정보**: 설치된 **BioStar X**의 버전 정보를 확인할 수 있습니다.
6. **도움말**: **BioStar X**의 도움말 페이지로 이동할 수 있는 링크 버튼입니다.
7. **계정**: **기본 설정** 메뉴로 이동하거나 현재 로그인한 사용자의 비밀번호를 변경할 수 있습니다.
   - **기본 설정** 메뉴에 대한 자세한 내용은 기본 설정 구성하기를 참고하세요.
   - 현재 로그인한 사용자의 비밀번호 변경에 대한 자세한 내용은 사용자 권한 설정하기를 참고하세요.
8. **로그아웃**: 현재 로그인한 사용자의 세션을 종료하고 로그아웃할 수 있습니다.

사용자

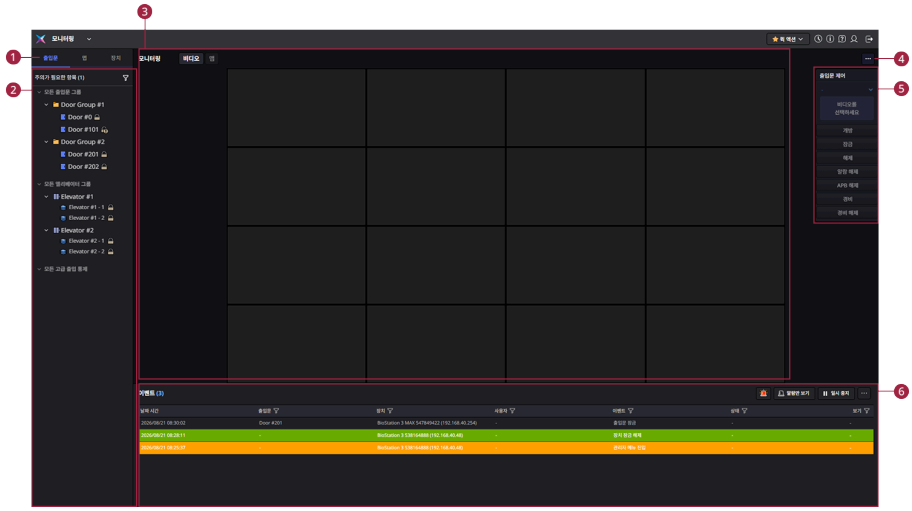
사용자 페이지의 **사용자** 메뉴에서는 사용자 그룹 관리, 사용자 관리, 출입 권한별 사용자 확인 등 다양한 기능을 통해 사용자를 효율적으로 관리하고, 권한을 통해 보안을 강화할 수 있습니다. **사용자** 페이지의 UI 구성 요소를 살펴보면 다음과 같습니다.



1. 사용자 그룹 또는 출입 그룹을 확인할 수 있습니다.
   - **사용자 그룹**에 대한 자세한 내용은 사용자 그룹 관리하기를 참고하세요.
   - **액세스 탐색기**에 대한 자세한 내용은 출입 그룹 관리하기를 참고하세요.
2. 사용자 그룹 또는 출입 그룹을 트리 구조 형식으로 확인할 수 있습니다. 트리 구조를 펼치거나 접을 수 있으며, 각 그룹을 클릭해 해당 그룹에 속한 사용자를 확인할 수 있습니다.
3. 사이드 메뉴에서 선택한 사용자 그룹의 사용자 수를 확인할 수 있습니다.
4. 사용자 목록의 표시된 모든 사용자를 선택하려면 **모두 선택** 버튼을 클릭하세요. 선택한 사용자 수는 **선택된 항목**에 표시됩니다.
5. 키워드를 입력해 사용자를 검색할 수 있습니다. 사용자 검색에 대한 자세한 내용은 사용자 탐색하기를 참고하세요.
6. 화면 오른쪽 상단에 제공하는 페이지 이동 버튼을 클릭해 다음 또는 이전 사용자 목록을 확인할 수 있습니다. 또는 원하는 페이지를 지정해 이동할 수도 있습니다. 자세한 내용은 사용자 탐색하기를 참고하세요.
7. ⋯ 버튼을 클릭하면 사용자와 관련한 다양한 기능을 사용할 수 있습니다.
   - **내보내기**: 사용자 목록을 CSV 파일 또는 Data 파일 형식으로 저장할 수 있습니다. 자세한 내용은 사용자 정보 내보내기/가져오기를 참고하세요.
   - **가져오기**: 사용자 목록을 CSV 파일 또는 Data 파일 형식으로 불러거나 얼굴 인식 정보를 불러올 수 있습니다. 자세한 내용은 사용자 정보 내보내기/가져오기를 참고하세요.
   - **장치로 전송**: 등록한 사용자 정보를 장치로 전송하는 기능입니다. 자세한 내용은 장치로 사용자 정보 전송하기를 참고하세요.
   - **얼굴 마이그레이션**: BioStar X 이전 버전에서 등록한 얼굴을 최신 알고리즘으로 업그레이드하여 인식 성능을 향상할 수 있습니다. 자세한 내용은 얼굴 마이그레이션을 참고하세요.
   - **열 레이아웃**: 사용자 목록에서 열(column)의 헤더 항목을 변경할 수 있습니다. 자세한 내용은 사용자 탐색하기를 참고하세요.
   - **인쇄**: 사용자 목록을 인쇄할 수 있습니다.
8. 사용자 등록 및 일괄 수정, 삭제 기능을 이용할 수 있습니다.
   - **일괄 편집**: 한 번에 여러 사용자의 정보나 출입 권한을 수정할 수 있습니다. 자세한 내용은 사용자 정보 수정하기를 참고하세요.
   - **삭제**: 선택한 사용자를 삭제할 수 있습니다. 자세한 내용은 사용자 삭제하기를 참고하세요.
   - **새 사용자**: 새로운 사용자를 등록할 수 있습니다. 자세한 내용은 사용자 등록하기를 참고하세요.

모니터링

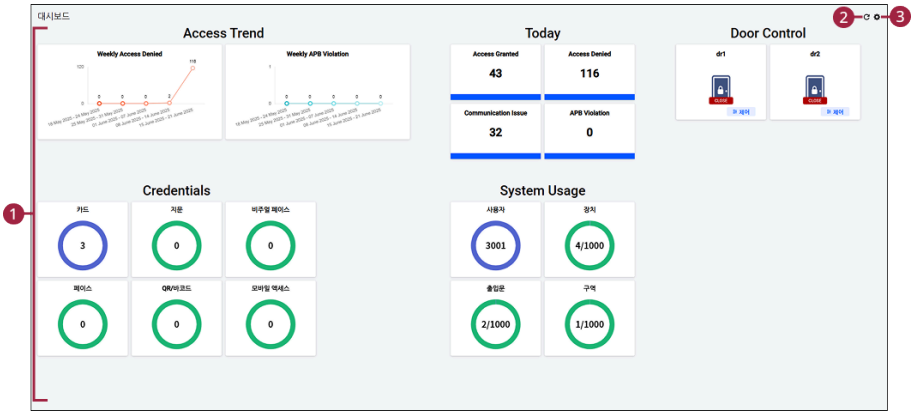
모니터링 페이지의 사용자 인터페이스(User Interface)를 안내합니다. **모니터링** 페이지에서는 출입문, 맵, 장치 기준으로 보안 상태를 실시간으로 모니터링할 수 있습니다. 또한 실시간으로 발생하는 이벤트를 확인하고 필요한 조치를 취할 수 있습니다. **모니터링** 페이지의 UI 구성 요소를 살펴보면 다음과 같습니다.



1. 검색 입력 필드에 키워드를 입력해 장치, 출입문, 카메라 등 원하는 항목을 검색할 수 있습니다.
2. **출입문**, **맵**, **장치**를 그룹 기준의 트리 구조 목록으로 확인하고 모니터링할 수 있습니다.
   - **출입문** 모니터링에 대한 자세한 내용은 출입문 모니터링하기를 참고하세요.
   - **맵** 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.
   - **장치** 모니터링에 대한 자세한 내용은 장치 모니터링하기를 참고하세요.
3. **비디오 타일**에서는 출입문, 카메라, 구역 등의 실시간 영상 또는 맵을 확인할 수 있습니다. 여러 카메라의 영상을 동시에 배치해 모니터링할 수 있습니다.
   - 카메라 영상 모니터링에 대한 자세한 내용은 비디오 모니터링하기를 참고하세요.
   - 맵 모니터링에 대한 자세한 내용은 맵 모니터링하기를 참고하세요.
4. ••• 버튼을 클릭하면 비디오 타일의 모든 요소를 닫을 수 있는 **모두 닫기** 기능을 제공합니다.
5. **제어 패널**에서는 선택한 출입문이나 장치의 기능을 제어할 수 있습니다. 자세한 내용은 출입문 제어하기를 참고하세요.
6. **이벤트 목록**에서는 실시간으로 발생하는 이벤트를 시간순으로 확인할 수 있습니다. 이벤트별로 상세 정보, 상태, 관련 사용자 및 장치 정보를 확인하고, 필요한 경우 이벤트에 대한 조치를 바로 취할 수 있습니다. 자세한 내용은 이벤트 모니터링하기를 참고하세요.

대시보드

대시보드 페이지의 사용자 인터페이스(User Interface)를 안내합니다.



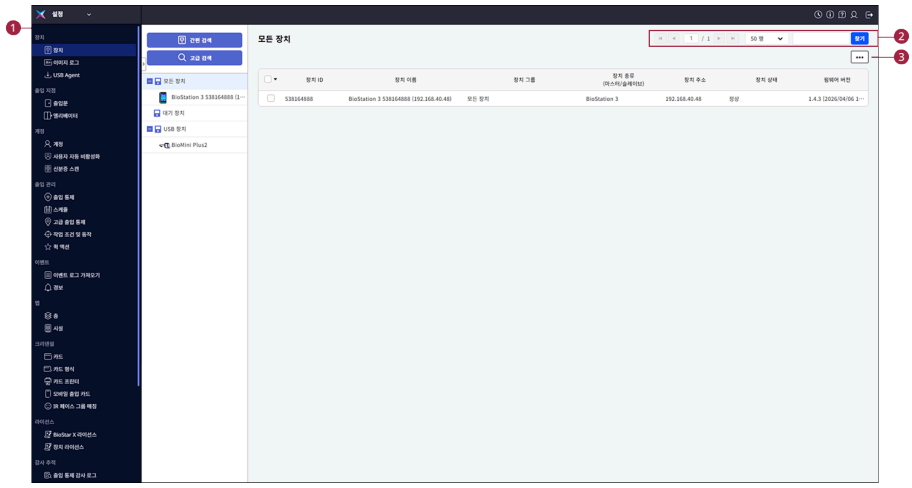
위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

1. **위젯 표시 영역**: 사용자가 추가한 위젯이 표시되는 영역입니다.
   - 각 위젯의 크기는 위젯별로 제한된 크기 내에서 자유롭게 조정할 수 있습니다.
   - 위젯은 비어있는 영역에만 배치할 수 있으며 위젯끼리 겹쳐놓을 수 없습니다.
2. **새로고침**: 대시보드 페이지를 새로고침하여 수정한 위젯의 데이터를 업데이트합니다.

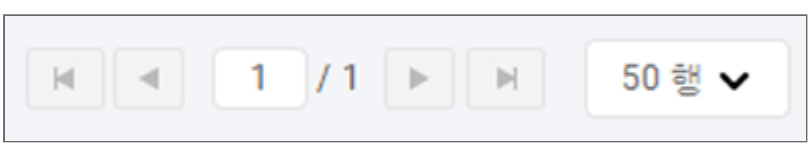
   대시보드 설정의 **자동 새로고침 주기**에서 새로고침 주기를 설정할 수 있습니다.
3. **대시보드 설정**: 새 위젯을 추가하거나 추가되어있는 위젯의 데이터와 모양을 설정할 수 있습니다.

설정

설정 페이지에서는 **BioStar X**의 다양한 설정을 관리할 수 있습니다. 이 페이지의 UI 구성 요소를 살펴보면 다음과 같습니다.



1. **설정** 메뉴에서 제공하는 다양한 설정 메뉴를 확인할 수 있습니다. 자세한 내용은 설정을 참고하세요.
2. 페이지 목록을 탐색할 수 있는 도구입니다. 페이지를 이동하거나 원하는 페이지로 이동할 수 있습니다.



- ⏮: 첫 페이지로 이동합니다.
- ◀: 이전 페이지로 이동합니다.

- ▶: 다음 페이지로 이동합니다.
- ▶|: 마지막 페이지로 이동합니다.
- 원하는 페이지로 이동하려면 숫자 입력 필드에 페이지 번호를 입력하세요.
- 한 페이지에 표시할 목록 개수를 설정하려면 행 선택 상자를 클릭하세요.

> **알아두기**
> 설정 메뉴에 따라 지원하지 않을 수 있습니다.

3. ••• 버튼을 클릭하면 추가 기능을 사용할 수 있습니다.

> **알아두기**
> 설정 메뉴에 따라 지원하는 기능은 다를 수 있습니다.

라이선스 정책

BioStar X는 **BioStar 2**의 후속 버전으로 개발된 차세대 출입통제 소프트웨어입니다. 향상된 시스템 아키텍처와 확장된 기능, 그리고 더욱 유연한 라이선스 모델을 통해 현재와 미래의 다양한 구축 환경을 지원합니다.

BioStar X는 **스타터**부터 **엘리트**까지 총 다섯 가지 확장 가능한 라이선스 등급을 제공하며, 소규모 사업장부터 대규모 기업 환경까지 다양한 환경에 맞춰 선택할 수 있습니다. 모듈형 구조로 설계되어 비디오 연동, 모바일 출입, 멀티 서버 지원 등 다양한 옵션 기능을 추가할 수 있습니다.

복잡한 라이선스 요구 사항을 해결하는 데 도움이 되는 **BioStar X 라이선스 계산기**를 사용해 보세요. 이 도구는 필요에 맞는 라이선스 유형과 수량을 결정하는 데 도움을 줍니다.

기본 라이선스

기본 라이선스는 시스템을 활성화하고 운영하기 위한 필수 구성 요소입니다. 이 라이선스는 추가 기능이나 업그레이드를 적용할 수 있는 기반 역할을 합니다.

	디바이스 매니저(Device Manager)	스타터(Starter)	에센셜(Essential)	어드밴스(Advanced)	엔터프라이즈(Enterprise)	엘리트(Elite)
최대 출입문 수	0	5	32	128	500	2000
최대 사용자 수	200	100	1,000	50,000	100,000	500,000
최대 관리자 수	1	1	10	20	40	100
최대 연결 IP 장치 수	1,000	1,000	1,000	1,000	1,000	1,000
맵(Maps)	✕	✕	✔	✔	✔	✔
비디오(Video)	✕	✕	Add on	Add on	Add on	Add on
고급 출입 통제 *(안티패스백, 화재 경보, 경비, 소집, 재실 인원 제한, 엘리베이터, 인터락)*	✕	✕	Add on	Add on	✔	✔
라이선스 업그레이드 *(출입문/사용자/관리자)*	사용자, 관리자만 해당	✕	Add on	Add on	Add on	Add on

- **디바이스 매니저** 라이선스는 타사 소프트웨어 또는 타사 시스템을 사용하는 고객이 **BioStar X**를 통해 슈프리마의 장치를 효율적으로 관리하고자 할 때 필요한 라이선스입니다.
- **최대 관리자 수**는 시스템에 접근할 수 있는 권한을 부여받은 사용자 수를 의미합니다.
- 최대 연결 IP 장치 수가 1,000대 이상일 경우 **멀티 커뮤니케이션** 서버 사용을 권장합니다.

라이선스 업그레이드

라이선스 업그레이드는 **에센셜**, **어드밴스**, **엔터프라이즈**, **엘리트** 등급의 라이선스 보유자에게 제공합니다. **디바이스 매니저** 라이선스 보유자는 사용자(User), 관리자(Operator) 업그레이드만 구매할 수 있습니다.

	수
출입문	32
사용자	5,000
관리자	10

기능 추가 옵션 (Feature Add-ons)

다음 항목은 개별적으로 구매할 수 있으며, **에센셜**, **어드밴스**, **엔터프라이즈**, **엘리트** 라이선스 등급에 추가 적용할 수 있습니다.

기능	라이선스 유형	비고
멀티 커뮤니케이션 서버 Init	기본 라이선스	멀티 커뮤니케이션 서버 1대가 포함되어 있습니다. 최대 1,000대의 IP 장치를 지원합니다.
멀티 커뮤니케이션 서버 Add-on	추가 서버	멀티 커뮤니케이션 서버 1대 추가 시 필요합니다. 라이선스 당 IP 장치 1,000대씩 확장할 수 있습니다.
GIS 지도	시스템	GIS 지도를 이용해 구역(Area) 및 시설(Facility), 층(Floor)을 설정할 수 있습니다.
비디오	카메라	타사 VMS와 연동할 때 필요합니다. 시스템당 1,000대의 카메라와 연동할 수 있습니다.
서버 매칭	ID, 카드, 지문, IR 페이스	장치에 저장된 ID와 카드, 지문, IR 페이스 정보를 서버 데이터베이스에 저장된 크리덴셜과 비교하는 서버 매칭 방식입니다.
방문자	시스템	관리자 및 운영자가 방문자 출입을 추적하거나 제어할 수 있습니다.
디렉토리 연동	시스템	중앙 집중식 사용자 관리를 위해 디렉터리 서비스와의 통합을 지원합니다.
인원 점검(Roll Call)	시스템	-

VMS에 연결된 모든 카메라를 반드시 **BioStar X**와 연동할 필요는 없습니다. 예를 들어, VMS가 32개의 카메라를 지원하더라도, 사용자는 실제로 **BioStar X**와 연동하려는 특정 카메라에 대해서만 라이선스를 구매하면 되며, 전체 카메라에 대한 라이선스 구매는 필요하지 않습니다.

다음 항목은 개별로 구매할 수 있으며 기본 라이선스와 상관없이 추가할 수 있습니다.

기능	라이선스 유형	비고
모바일 앱	시스템	-
이벤트 로그 API	시스템	시스템이 외부 API를 통해 이벤트 로그를 수신하고 기록할 수 있습니다. 이를 통해 타사 애플리케이션이나 서비스가 중앙 집중식 로깅 및 보고를 위해 출입 통제 시스템에 이벤트 데이터를 직접 추가할 수 있습니다.
리모트 액세스	시스템(연간 결제)	외부 네트워크에서 **BioStar X** 서버에 접속할 수 있는 보안 터널 기능을 제공합니다. **BioStar X** 모바일 및 API의 외부 네트워크 접근을 위한 게이트웨이 역할도 수행합니다. **얼굴 등록 모바일 링크 전송** 기능 사용에 필요합니다.
BioStar X 플러그인	시스템	외부 플러그인 통합을 지원합니다. 시스템당 최대 10개의 사용자 정의 플러그인을 사용할 수 있습니다. 자세한 내용은 플러그인을 참고하세요.
근태 관리(T&A)	Standard	최대 500명의 사용자를 지원합니다.
	Enterprise	사용자 수에 제한이 없습니다.

알아두기

근태 관리(T&A) 사용자 수는 기본 라이선스 제한을 따르며, **근태 관리** 에디션에서 허용하는 최대 사용자 수까지 허용됩니다. (예, Standard 에디션의 경우 사용자 500명)

고급 출입 통제(Advanced Access Control)

고급 출입 통제는 다음 7개의 개별 기능으로 구성되며, 필요한 기능만 선택하여 개별로 구매할 수 있습니다. **에센셜**, **어드밴스** 라이선스 등급에서는 추가 옵션으로 구매하며, **엔터프라이즈**, **엘리트** 라이선스 등급에서는 7개 기능이 모두 기본 포함됩니다.

기능	라이선스 유형	비고
안티패스백(Anti-passback)	시스템	-
화재 경보(Fire Alarm)	시스템	-
경비(Intrusion Alarm)	시스템	-
소집(Muster)	시스템	-

기능	라이선스 유형	비고
재실 인원 제한(Occupancy Limit)	시스템	-
엘리베이터(Elevator)	시스템	-
인터락(Interlock)	시스템	-

- 스케줄 잠금(Scheduled Lock)과 스케줄 개방(Scheduled Unlock)은 라이선스가 필요 없는 기본 출입 통제 기능으로, 위 7개 기능과 별도로 항상 사용할 수 있습니다.
- 기존에 고급 출입 통제 패키지를 구매한 고객은 계속 동일하게 사용할 수 있습니다. 신규 구매부터는 7개 기능을 개별로 선택 구매할 수 있습니다.

장치 라이선스

장치 라이선스는 개별로 구매할 수 있으며, 기본 라이선스와 상관없이 추가할 수 있습니다. 장치 라이선스는 일련 번호(S/N)를 기준으로 발급됩니다. 라이선스가 필요한 장치에서만 해당 기능을 활성화할 수 있습니다.

기능	라이선스 유형	지원 모델	비고
카메라 QR	장치	BioStation 3 Max, XPass Q2, BioStation 3, X-Station 2	-
다중 얼굴 인증	장치	BioStation 3	-
무선 잠금	장치	CoreStation 40	-

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 다음 링크를 참고하세요.

ffmpeg

BioStar X는 동영상 파일 변환 및 정보 확인을 위해 ffmpeg(https://ffmpeg.org)를 포함합니다. *ffmpeg.exe*와 *ffprobe.exe* 두 개의 커맨드라인 바이너리를 제공하며, 두 바이너리는 모두 아래의 ffmpeg 소스 tarball 하나로부터 빌드됩니다. ffprobe는 별도 구성 요소가 아니라 ffmpeg 프로젝트에 포함된 도구입니다.

- Component: ffmpeg (ffmpeg.exe, ffprobe.exe)
- Version: 8.1
- License: GNU Lesser General Public License v2.1

  전문: COPYING.LGPLv2.1 참고
- Source code: ffmpeg-8.1.tar.xz
- Upstream URL: ffmpeg-8.1.tar.xz
- SHA-256: b072aed6871998cce9b36e7774033105ca29e33632be5b6347f3206898e0756a

Build configuration:

```
./configure \
  --arch=x86_64 \
  --target-os=mingw64 \
  --disable-gpl \
  --disable-nonfree \
  --disable-libx264 \
  --disable-libx265 \
  --disable-libxvid \
  --enable-mediafoundation \
  --enable-libmp3lame \
  --disable-doc \
  --disable-debug \
  --enable-small \
  --pkg-config-flags=--static \
  --extra-ldflags="-static"
```

수정 사항: 없음. 업스트림 소스 tarball을 변경 없이 그대로 사용하여 빌드했습니다.

BioStar X가 사용하는 인코더는 다음과 같습니다.

- h264_mf (Windows Media Foundation을 통한 H.264)
- libmp3lame (MP3 오디오, LGPL)

libmp3lame

BioStar X는 MP3 오디오 인코딩을 위해 libmp3lame을 사용합니다.

- Component: libmp3lame (LAME MP3 Encoder)
- Version: 3.100
- License: GNU Lesser General Public License v2.1

  전문: COPYING.LGPLv2.1 참고 (ffmpeg와 동일한 LGPL v2.1 버전)
- Source code: lame-3.100.tar.gz
- Upstream URL: lame-3.100.tar.gz
- SHA-256: ddfe36cab873794038ae2c1210557ad34857a4b6bdc515785d1da9e175b1da1e

수정 사항: 없음. 업스트림 소스 tarball을 변경 없이 그대로 사용했으며, 빌드 시 `--enable-libmp3lame` 옵션을 통해 *ffmpeg.exe*와 *ffprobe.exe*에 정적으로 링크되었습니다.

(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.