ViOnyx Web Server
사용자 가이드

버전 1.1.0

한국어
KO 102.00.VQF12-R

suprema
SECURITY & BIOMETRICS

목차

시작하기 5

인증서 설치 5

비밀번호 설정 10

로그인 11

사용자 인터페이스 이해하기 13

메인 메뉴 바로가기 13

정보 및 도구 14

라이브 영상 보기 15

라이브 뷰 기본 구성 15

채널과 뷰 모드 선택하기 15

화면 확대 및 축소 16

화면 회전하기 17

화면 캡처 17

전체 화면 모드 18

AI 표시 옵션 18

얼굴 촬영 패널 열기 19

영상이 재생되지 않을 때 20

AI 이벤트 관리하기 21

사용자 추적 이벤트 설정하기 21

침입 감지 이벤트 설정하기 28

라인 통과 감지 이벤트 설정하기 35

인원 카운팅 이벤트 설정하기 43

출입 통제 이벤트 설정하기 50

AI 이벤트 수정 및 삭제하기 58

AI 규칙(Rule) 설정하기 59

일정 관리하기 66

고급 설정하기 70

카메라 설정하기 73

비디오 프로필 설정하기 73

카메라 설정 변경하기 76

프라이버시 및 오버레이 설정하기 80

날짜와 시간 설정하기 83

네트워크 설정하기 86

RS-485 설정하기 96

RTSP 및 ONVIF 연동하기 104

사용자 관리하기 106

얼굴 인증 설정하기 106

사용자 추가하기 106

사용자 수정 및 삭제하기 112

사용자 검색 및 보기 115

출입 통제 관리하기 119

출입문 관리하기 119

출입 레벨 관리하기 125

출입문 제어하기 131

출입문 규칙 설정하기 133

시스템 구성하기 140

카메라 정보 업데이트하기 140

펌웨어 업데이트하기 142

카메라 유지 관리하기 144

오디오 클립 업로드하기 147

관리자 계정 비밀번호 업데이트하기 150

운영자 관리하기 151

시스템 로그 확인하기 156

시스템 로그 유형 161

부록 170

면책 조항 170

저작권 공지 171

시작하기

ViOnyx 카메라를 처음 설치한 후 웹 브라우저를 통해 초기 설정을 완료해야 합니다. 이 문서는 인증서 설치, 관리자 비밀번호 설정, 로그인까지 필요한 모든 단계를 안내합니다.

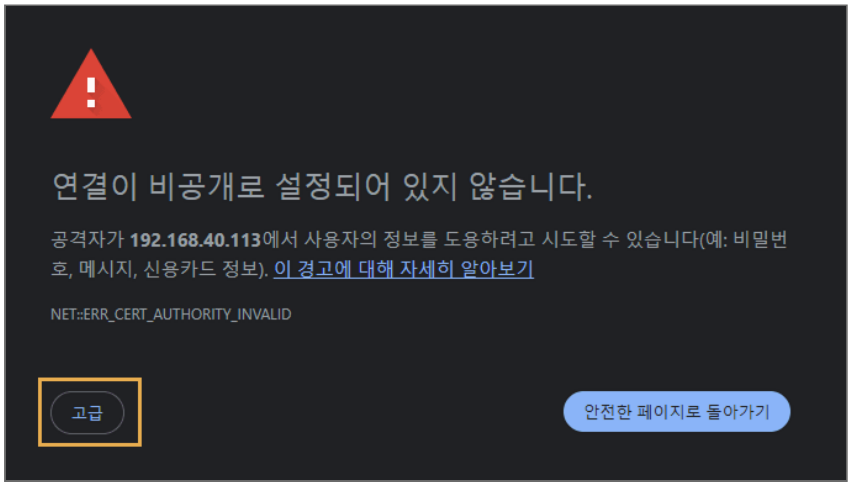
> **알아두기**
> 공장 초기화 후 IP 주소를 할당받지 못했다면 기본 IP 주소(`https://192.168.1.100`)로 변경되므로 웹 브라우저에서 해당 주소로 접속하세요.

인증서 설치

ViOnyx Web Server는 안전한 HTTPS 연결을 사용합니다. 처음 접속 시 보안 경고가 표시되지만, 이는 카메라의 자체 발급 인증서 때문입니다. 인증서를 Windows 신뢰 저장소에 등록한 후 웹 서버 접속 시, 경고 없이 안전하게 연결하는 방법을 알아보세요.

1 인증서 다운로드

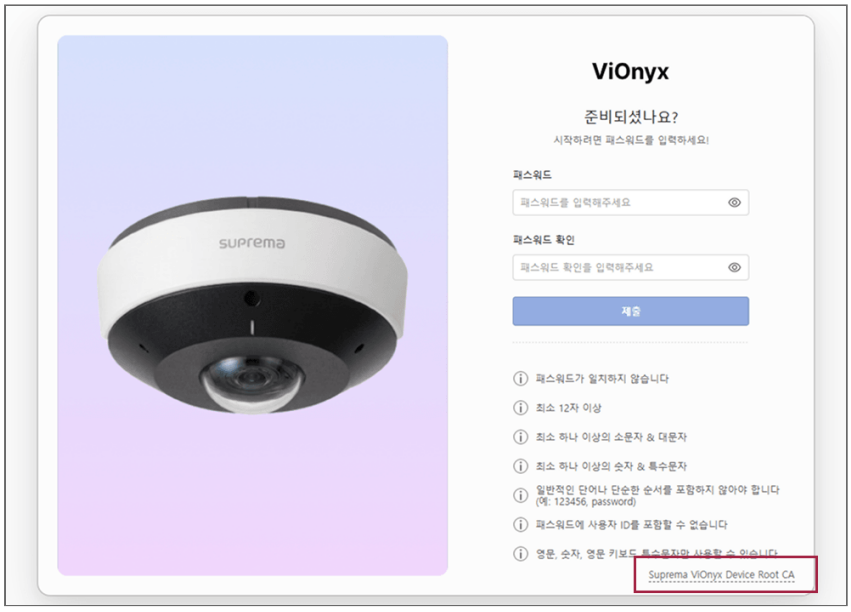
1. 웹 브라우저에서 카메라에 할당한 IP 주소(`https://{IP_address}`)로 접속하세요.
2. **연결이 비공개로 설정되어 있지 않습니다** 라는 경고 메시지가 표시되면 하단의 **고급** 버튼을 클릭하세요.



3. **고급** 섹션을 확장한 후 `https://{IP_address}` **로 이동(안전하지 않음)** 또는 유사한 링크를 클릭하여 계속 진행하세요.



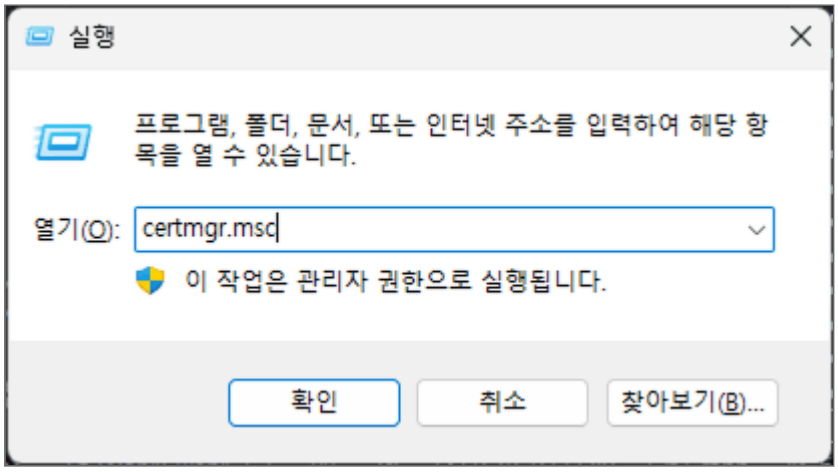
4. 비밀번호 설정 화면 하단의 **Suprema ViOnyx Device Root CA** 링크를 클릭하세요.



5. 인증서 파일 `Suprema_ViOnyx_Device_{serial-number}_Root_CA.crt`를 로컬에 저장하세요.

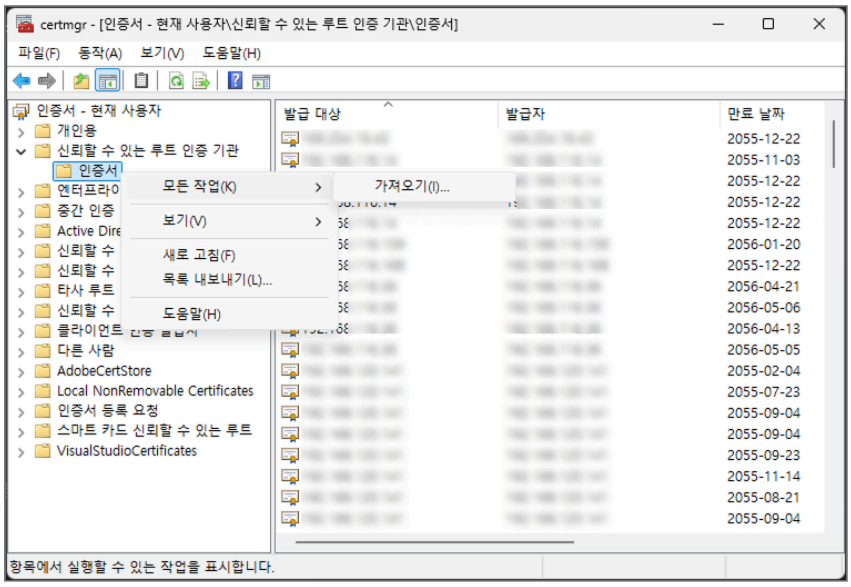
2 Windows 관리 콘솔 열기

1. 시작 + `R` 키를 눌러 실행 창을 여세요.
2. `certmgr.msc`를 입력하고 `Enter` 키를 눌러 **관리 콘솔**을 실행하세요.

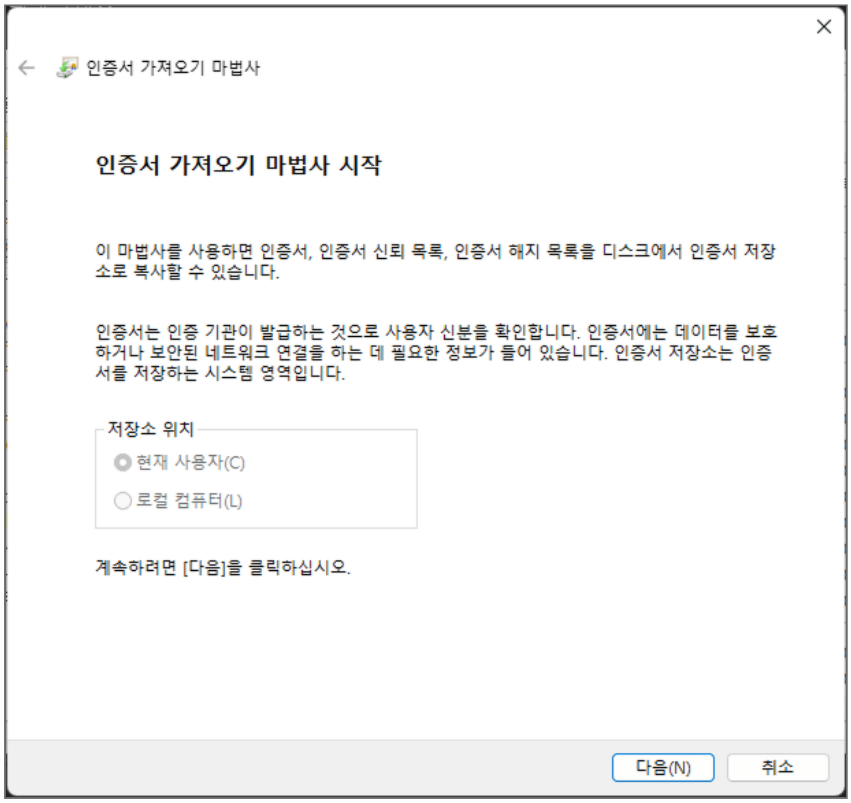


3 인증서 마법사 가져오기 실행

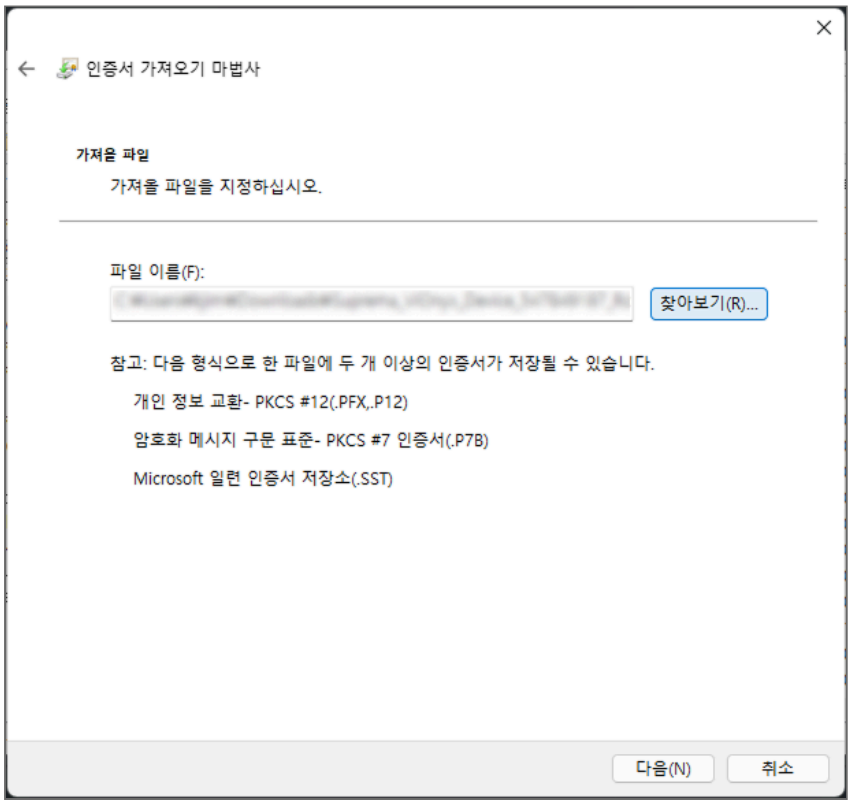
1. **관리 콘솔**의 왼쪽 패널에서 **신뢰할 수 있는 루트 인증 기관**을 확장하세요.
2. 하위의 **인증서**에서 마우스 오른쪽 버튼을 클릭하고 **모든 작업** → **가져오기**를 선택하세요.



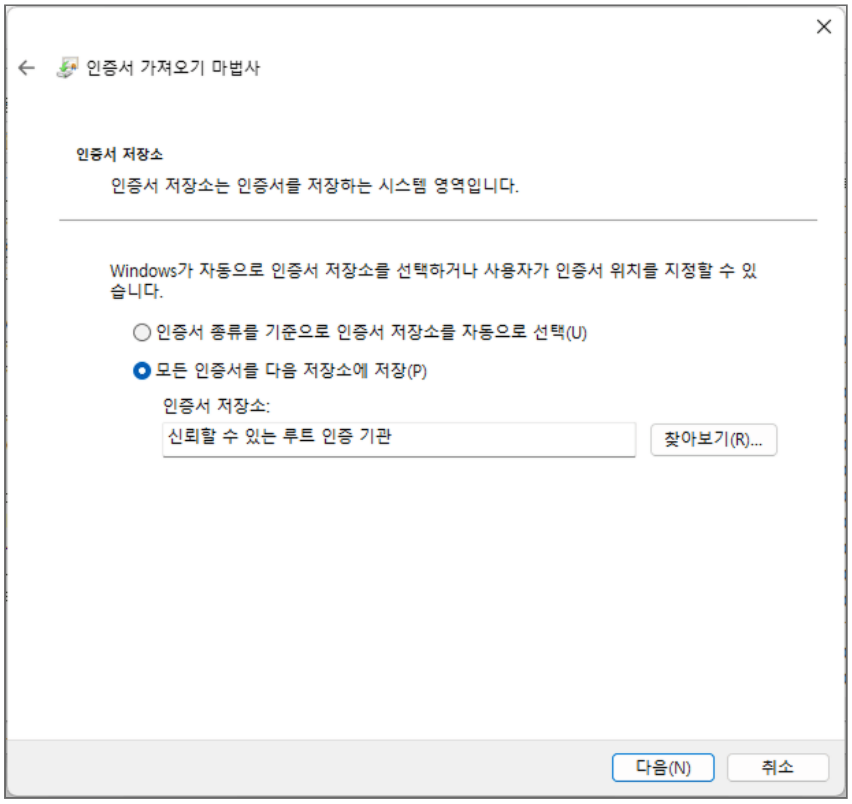
3. 인증서 가져오기 마법사에서 **다음** 버튼을 클릭하세요.



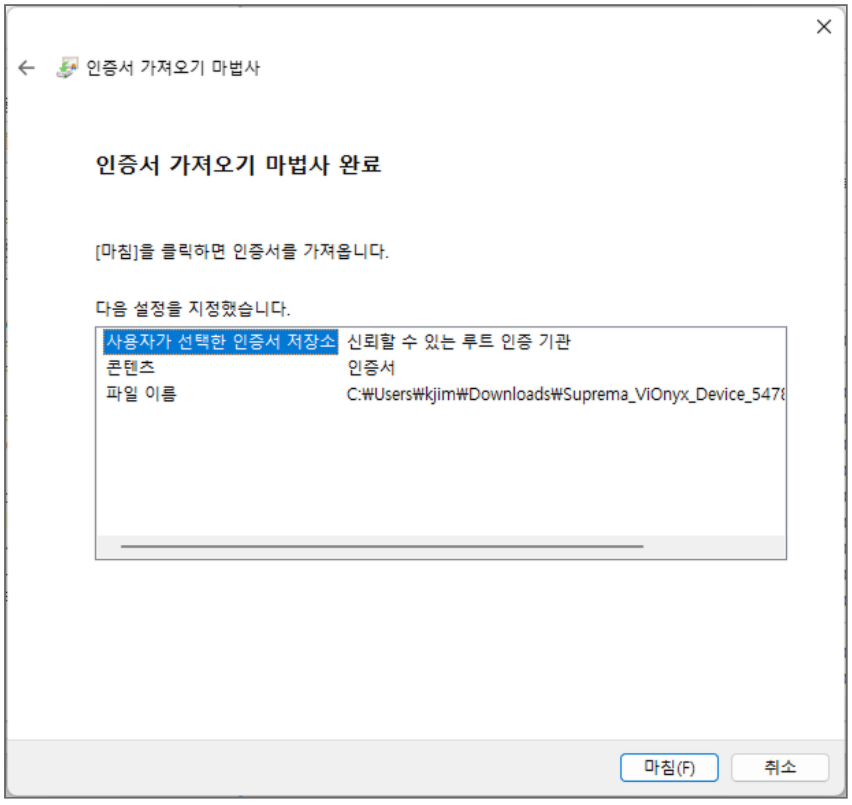
4. **찾아보기** 버튼을 클릭하여 저장한 인증서 파일 `Suprema_ViOnyx_Device_547849187_Root_CA.crt`를 선택하세요.



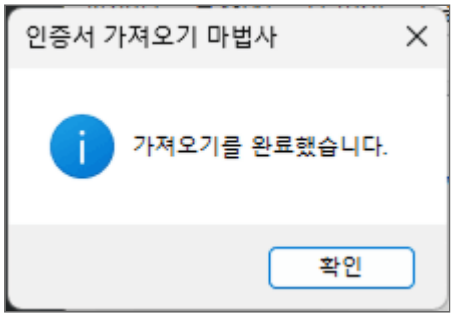
5. **다음** 버튼을 클릭하세요.
6. **모든 인증서를 다음 저장소에 저장**을 선택하세요.
7. **인증서 저장소**가 **신뢰할 수 있는 루트 인증 기관**으로 설정되어 있는지 확인하세요.



8. **다음** 버튼을 클릭하세요.
9. **마침** 버튼을 클릭하여 인증서 가져오기를 완료하세요.

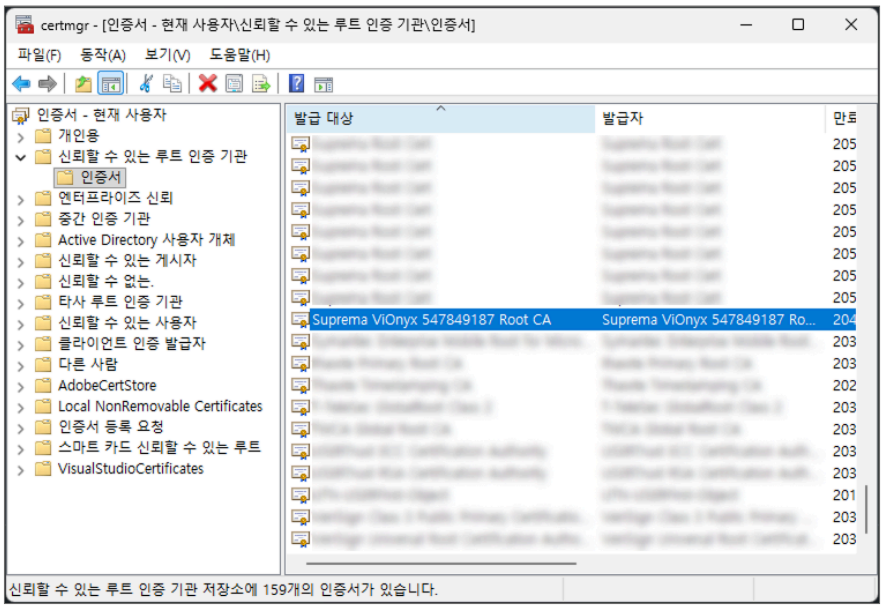


10. 보안 경고가 나타나면 **예** 버튼을 클릭하세요.
11. 인증서 가져오기 성공 메시지가 나타나면 **확인** 버튼을 클릭하세요.



4 인증서 설치 확인

관리 콘솔에서 **신뢰할 수 있는 루트 인증 기관** → **인증서**를 선택하여 앞서 가져온 인증서가 목록에 있는지 확인하세요.

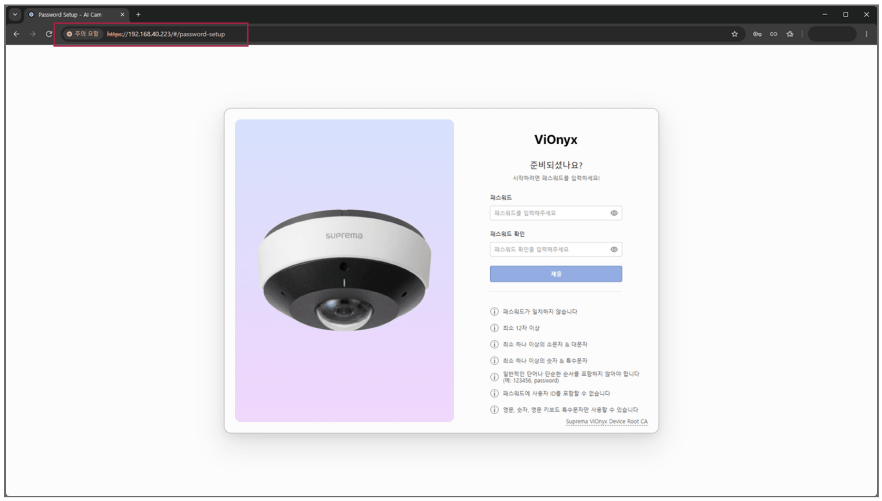


인증서 설치가 완료되면 웹 브라우저를 완전히 종료하고 다시 시작한 후, 카메라의 IP 주소로 다시 접속하세요. 이제 보안 경고 없이 안전하게 연결됩니다.

비밀번호 설정

처음 로그인할 때는 보안을 위해 강력한 비밀번호를 설정해야 합니다. ViOnyx는 강력한 비밀번호 정책을 적용하여 시스템 보안을 보장합니다.

1. 웹 브라우저에서 카메라에 할당한 IP 주소(`https://{IP_address}`)로 접속하세요.



2. 비밀번호 설정 페이지에서 **패스워드** 입력 필드에 새로운 비밀번호를 입력하세요.
3. **패스워드 확인** 필드에 동일한 비밀번호를 다시 입력하세요.
4. 입력한 비밀번호들이 아래의 모든 요구 사항을 만족하는지 확인하세요.
5. 모든 조건이 충족되면 **제출** 버튼이 활성화됩니다. 버튼을 클릭해 비밀번호 설정을 완료하세요.

비밀번호 요구 사항

비밀번호는 다음의 모든 조건을 만족해야 합니다:

- **패스워드** 필드와 **패스워드 확인** 필드의 값이 정확히 일치해야 합니다.
- 비밀번호는 최소 12자 이상이어야 합니다. 최대 64자 이하로 제한합니다.
- 최소 1개의 영어 소문자(`a-z`)와 대문자(`A-Z`)를 포함해야 합니다.
- 최소 1개의 숫자(`0-9`)와 특수문자를 포함해야 합니다.

  > *특수문자 예시:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

- `1234`, `abcd` 같이 연속 문자 4개 이상, 동일 문자 4개 이상을 포함할 수 없습니다.
- 대소문자와 무관하게 아이디는 비밀번호에 포함할 수 없습니다.

  > *admin, Admin, ADMIN, Admin123! 등*

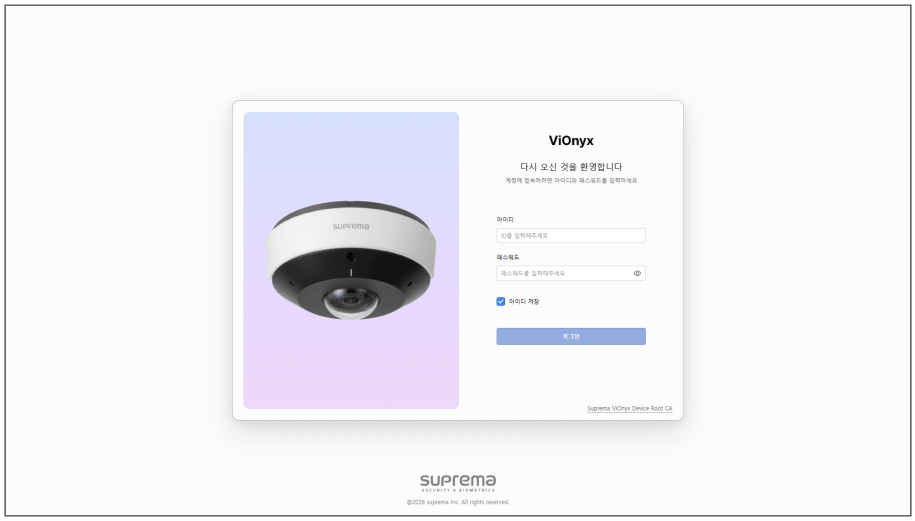
- `password`, `qwerty`, `123456` 등 흔히 사용되는 비밀번호 패턴은 사용할 수 없습니다.
- 영문, 숫자, 영문 키보드 특수 문자만 사용할 수 있습니다.

주의

설정한 비밀번호는 안전한 장소에 보관하세요. 비밀번호를 분실한 경우 카메라를 초기화해야 합니다.

로그인

비밀번호 설정이 완료되면 로그인 페이지로 자동 이동합니다. 관리자 아이디와 설정한 비밀번호를 입력하여 ViOnyx Web Server에 접속하세요.



1. **아이디** 입력 필드에 **admin**을 입력하세요.
2. **패스워드** 입력 필드에 설정한 비밀번호를 입력하세요.
3. **로그인** 버튼을 클릭하세요.

로그인에 성공하면 ViOnyx Web Server의 **라이브** 페이지로 이동합니다.

> **알아두기**
> 관리자 아이디(admin)는 **시스템** → **계정 관리**에서 변경할 수 있습니다.

다음 단계

라이브 메뉴의 주요 기능과 사용 방법을 안내합니다.
AI 이벤트를 설정하여 카메라가 감지한 특정 상황을 모니터링할 수 있습니다.
카메라의 다양한 설정을 통해 촬영 환경에 맞는 최적의 영상 품질을 유지하고, 네트워크를 구성하며, 보안 및 개인정보 보호 정책을 적용할 수 있습니다.
사용자를 등록하여 AI 얼굴 인식 기능을 활용할 수 있습니다.
카메라 시스템을 효과적으로 관리하기 위해 디바이스 정보, 펌웨어, 유지 관리, 계정, 오디오, 로그 등을 체계적으로 관리할 수 있습니다.

사용자 인터페이스 이해하기

ViOnyx Web Server에 로그인하면 상단에 주요 메뉴가 표시됩니다. 각 메뉴를 통해 원하는 기능에 빠르게 접근할 수 있습니다. 이 페이지에서는 웹 서버 인터페이스의 구조와 각 메뉴의 역할을 안내합니다.



메인 메뉴 바로가기

화면 왼쪽 상단에는 ViOnyx Web Server의 로고와 함께 주요 메뉴 아이콘이 있습니다. 각 메뉴에서 제공하는 기능은 아래와 같습니다.

메뉴 아이콘	메뉴 이름	설명
	라이브	실시간으로 카메라에서 촬영 중인 영상을 확인할 수 있습니다.
	설정	카메라와 웹 서버의 설정값을 변경할 수 있습니다.
	AI&규칙	AI 이벤트 및 규칙을 설정할 수 있습니다.
	사용자	카메라 시스템의 사용자를 추가하고 관리할 수 있습니다.
	출입	출입문, 출입 레벨, 사용자 권한 체계를 연결하여 출입 통제를 관리할 수 있습니다. 이 메뉴는 베타 버전입니다.
	시스템	장치 정보, 계정, 오디오, 로그 등 전체 시스템을 관리할 수 있습니다.

알아두기

출입 메뉴는 펌웨어 버전 1.1.0 이상에서 지원합니다.

정보 및 도구

화면 오른쪽 상단에는 카메라 정보와 언어 선택, 사용자 가이드 바로가기, 로그아웃 버튼이 있습니다.

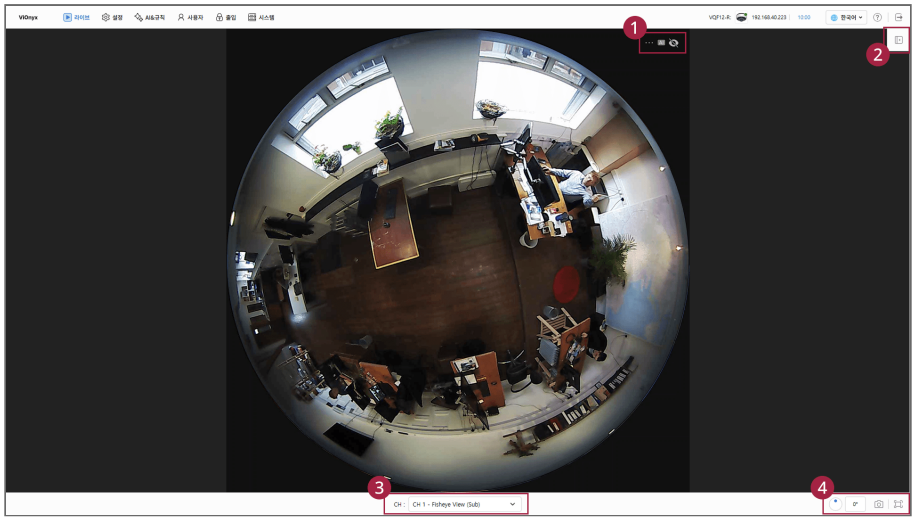
메뉴 아이콘	메뉴 이름	설명
	카메라 정보	현재 접속한 카메라의 이름과 상태, IP 주소를 확인할 수 있습니다. **IP 주소**를 클릭하면 디바이스 정보를 확인할 수 있습니다.
10:00	세션 타임	현재 로그인한 관리자의 세션 시간을 확인할 수 있습니다. 세션 시간을 초과하면 자동으로 로그아웃됩니다.
	언어 선택	웹 인터페이스의 언어를 변경할 수 있습니다.
	사용자 가이드 바로가기	사용자 가이드를 확인할 수 있습니다.
	로그아웃	로그아웃할 수 있습니다.

라이브 영상 보기

ViOnyx Web Server의 **라이브** 메뉴에서는 카메라가 촬영 중인 영상을 실시간으로 확인할 수 있습니다. 원하는 채널과 뷰 모드를 선택하고, 화면을 확대하거나 전체 화면으로 볼 수 있습니다.

라이브 뷰 기본 구성

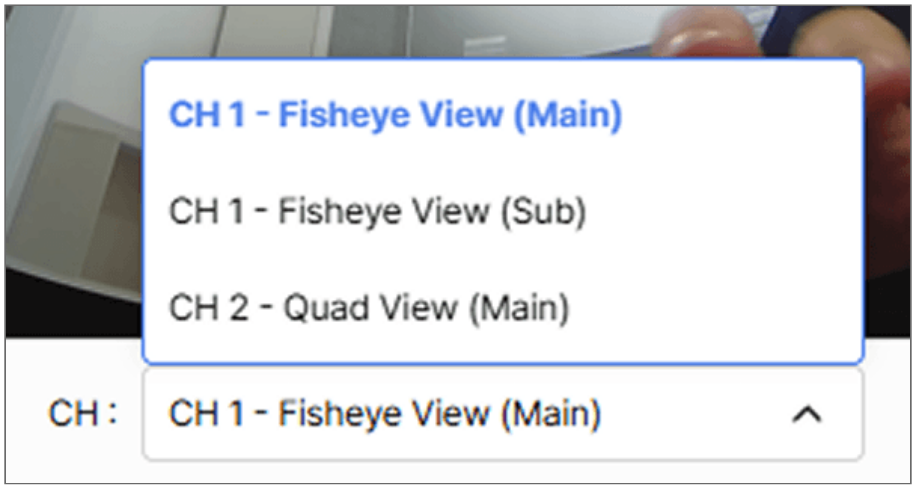
라이브 메뉴에 처음 진입하면 다음과 같은 기본 상태로 영상이 표시됩니다.



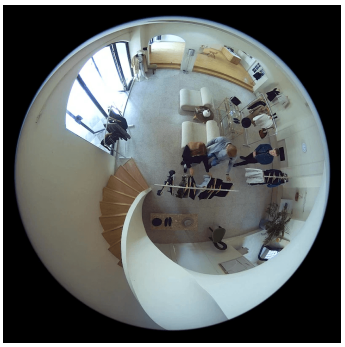
항목	구성 요소	설명
1	AI	- AI 기능이 비활성화된 상태입니다. 아이콘을 클릭해 AI 기능을 활성화할 수 있습니다. - AI 이벤트와 사용자 박스를 표시하거나 숨기려면 ••• 버튼을 클릭해 설정을 조정하세요.
2		**얼굴 촬영**(Face Shot) 패널을 열 수 있습니다.
3	CH	채널에 따라 제공하는 뷰 모드를 선택할 수 있습니다.
4		라이브로 보고 있는 영상을 회전할 수 있습니다.
		라이브 영상을 캡처할 수 있습니다.
		라이브 영상을 전체 화면으로 볼 수 있습니다.

채널과 뷰 모드 선택하기

ViOnyx Web Server는 여러 채널과 다양한 뷰 모드를 제공합니다. 화면 아래의 **CH** 드롭다운 메뉴에서 원하는 채널과 뷰 모드를 선택하세요.



지원하는 채널과 뷰 모드

채널	뷰 모드	설명	예시
1ch	Fisheye View (Main/Sub)	기본 채널의 원본 피쉬아이 렌즈 영상	
2ch	Quad View (Main)	파노라마 뷰 채널의 4분할 뷰	

알아두기

- 각 채널의 Main과 Sub는 서로 다른 해상도의 스트림을 제공합니다. Main은 고화질, Sub는 저화질 스트림입니다.
- 위 이미지는 예시 화면입니다. 실제 화면과 다를 수 있습니다.

화면 확대 및 축소

마우스를 사용해 화면을 확대하고 축소할 수 있습니다.

- 스크롤 업(위로): 화면 확대(줌 인)

- 스크롤 다운(아래로): 화면 축소(줌 아웃)
- 더블 클릭: 원래 크기로 복귀(1배)

> **알아두기**
>
> - 1배 ~ 8배까지 화면을 확대할 수 있습니다.
> - 화면 확대는 디지털 줌이므로, 높은 배율로 확대하면 영상이 흐릿해질 수 있습니다.

화면 회전하기

라이브 영상을 회전하려면 버튼을 클릭한 상태에서 드래그하세요. 또는 버튼 오른쪽에 입력 필드에 회전 각도를 직접 입력할 수도 있습니다.



화면 캡처

라이브 영상을 캡처하려면 버튼을 클릭하세요. 캡처 이미지는 `capture_{ch1|ch2}_{main|sub}_{YYYY-MM-DDTHH-MM-SS}.jpeg` 형식으로 저장됩니다.



전체 화면 모드

더 큰 영상을 확인하려면 전체 화면 모드를 사용하세요. 화면 오른쪽 하단의 ⛶ 버튼을 클릭하세요.



- 전체 화면 모드에서도 뷰 모드 변경, 줌 기능을 계속 사용할 수 있습니다.
- 전체 화면 모드를 종료하려면 ESC 키를 누르거나 ⛶ 버튼을 다시 클릭하세요.

AI 표시 옵션

라이브 영상의 AI 표시 옵션을 설정하려면 화면 오른쪽 상단의 ••• 버튼을 클릭하세요.



- **이벤트 박스 팝업**: AI 이벤트가 발생하면 라이브 영상 왼쪽 상단에 이벤트가 팝업으로 표시됩니다.

- **유저 박스 팝업**: AI 이벤트를 통해 얼굴이 감지되면 라이브 영상 오른쪽 하단에 사용자 박스가 팝업으로 표시됩니다.
- **기본 투명도**: 이벤트 팝업, 사용자 팝업의 투명도를 조절할 수 있습니다.
- **기준점**: 라이브 영상의 사람 감지 박스 위에 기준점을 표시합니다. 이 옵션을 켜면 영상 오른쪽 상단에 범례가 함께 표시됩니다.
  - 하늘색 점(🔵): 박스의 한가운데입니다.
  - 빨간색 점(🔴): 박스의 긴 축을 따라 위에서 80% 지점입니다. 카메라를 천장에 아래 방향으로 설치하면 사람의 발 근처에 표시됩니다.

> **알아두기**
>
> - **표시 시간** 옵션에서 설정한 시간(단위: 초) 동안 팝업이 유지됩니다.
> - **기준점** 옵션은 AI 기능(AI)을 켜야 사용할 수 있습니다.
> - **기본 투명도**, **기준점** 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

얼굴 촬영 패널 열기

AI 이벤트 기능을 활성화했다면 카메라를 통해서 감지된 얼굴을 확인할 수 있습니다. **얼굴 촬영**(Face Shot) 패널을 열려면 화면 오른쪽 상단의 버튼을 클릭하세요.



얼굴 촬영 패널 상단에서 제공하는 도구 아이콘을 클릭해 다음과 같은 기능을 사용할 수 있습니다.

- / : 얼굴 촬영을 일시 정지하거나 재개할 수 있습니다.
- : 얼굴 촬영 결과를 필터링할 수 있습니다.
- : **얼굴 촬영** 패널을 전체 화면으로 확대할 수 있습니다.

> **알아두기**
>
> AI 이벤트 및 규칙 설정에 대한 자세한 내용은 AI 이벤트 관리하기를 참조하세요.

영상이 재생되지 않을 때

카메라의 영상이 로드되지 않는다면 다음 단계를 따라 네트워크 연결 상태를 확인하세요.

1. 카메라와 네트워크 연결 상태를 확인하세요.
2. 웹 브라우저에서 **새로고침(F5)** 버튼을 누르세요.
3. 시스템이 자동으로 재연결을 시도합니다.

AI 이벤트 관리하기

AI 이벤트와 규칙을 설정하면 카메라가 감지한 상황에 맞춰 필요한 동작을 자동으로 실행할 수 있습니다. 먼저 감지할 상황을 AI 이벤트로 만들고, 이벤트가 발생할 때 실행할 동작을 AI 규칙으로 연결하세요.

AI 이벤트는 사람의 움직임, 구역 침입, 라인 통과, 인원 수, 출입문 접근 등 감시 목적에 맞게 만들 수 있습니다. AI 규칙에서는 이벤트가 발생할 때 실행할 오디오, 웹훅, 릴레이 동작을 지정하고, 일정을 적용해 동작이 실행될 시간대를 제한할 수 있습니다. 운영 환경에 따라 고급 설정에서 얼굴 인식과 관련된 세부 옵션을 조정하세요.

> **알아두기**
> AI 이벤트를 사용하려면 모든 이벤트에 공통으로 적용되는 얼굴 영역을 반드시 1개 이상 설정해야 합니다.

사용자 추적 이벤트 설정하기

사용자 추적 이벤트를 생성하여 진입 구역의 출입을 감지합니다. 선택적으로 얼굴 영역을 추가하면 특정 영역에서 얼굴을 우선적으로 추적할 수 있으며, 등록된 사용자는 신원을 자동 인식합니다.

언제 사용하나요?

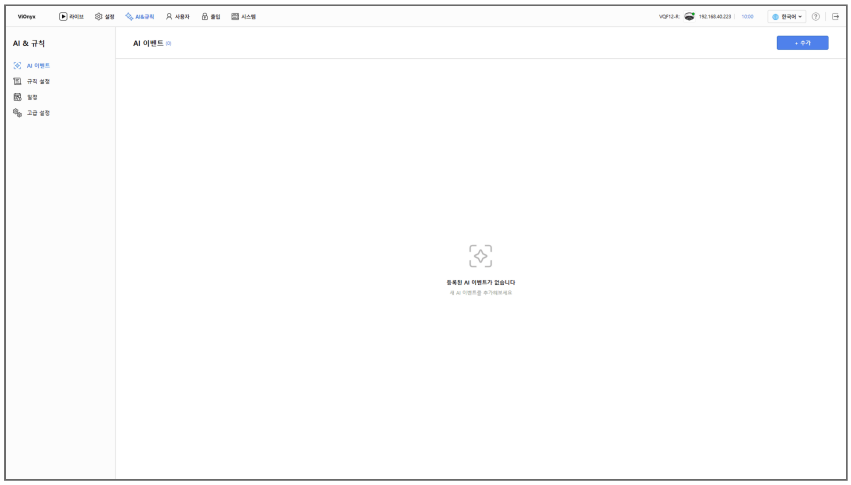
- 출입 구역에 등록된 사원 또는 고객의 출입 현황 파악
- 보안이 필요한 구역(회의실, 저장소)의 접근 모니터링
- 매장 내 특정 코너(신상품, 이벤트 존)의 고객 유입 추적

사용자 추적 이벤트 생성

사용자 추적 이벤트를 생성하면 라이브 뷰에서 실시간으로 사람의 이동을 추적할 수 있습니다. 또한 얼굴 영역을 설정하면 등록된 사용자를 인식하여 누가 이동했는지 확인할 수 있습니다.

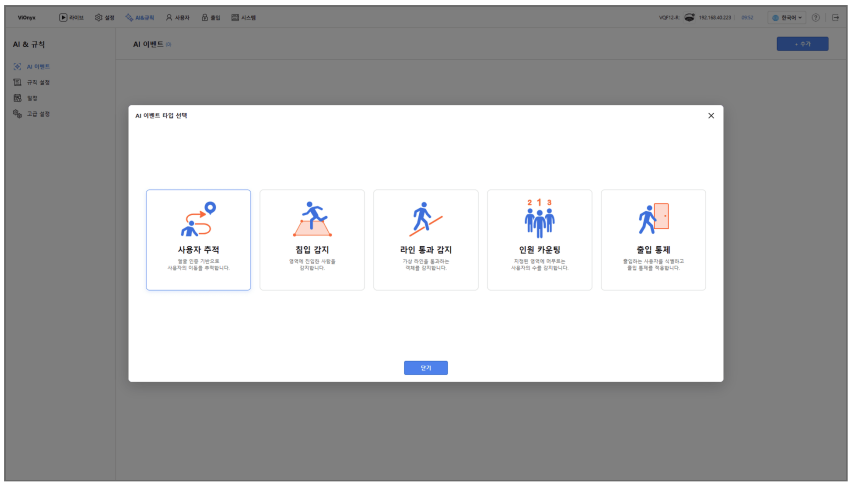
1 이벤트 생성 시작

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.

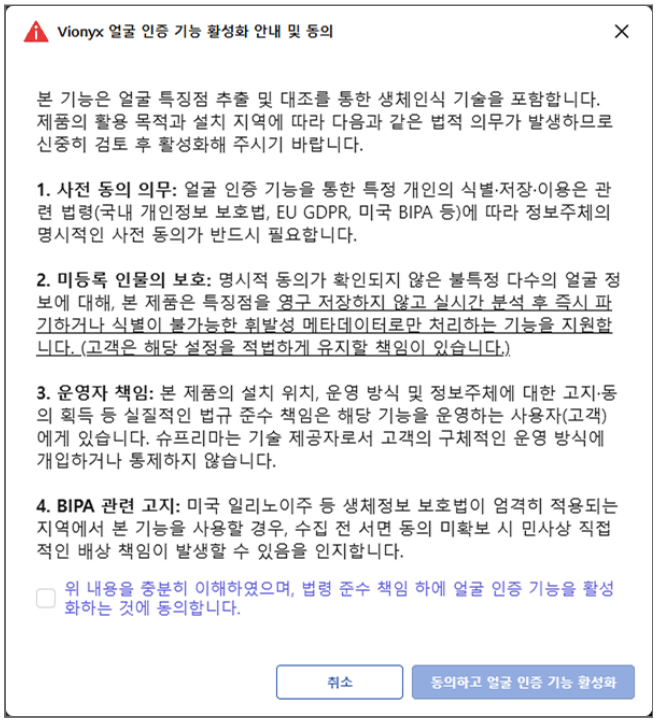


3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.

4. **AI 이벤트 타입 선택** 창에서 **사용자 추적**을 클릭하세요.

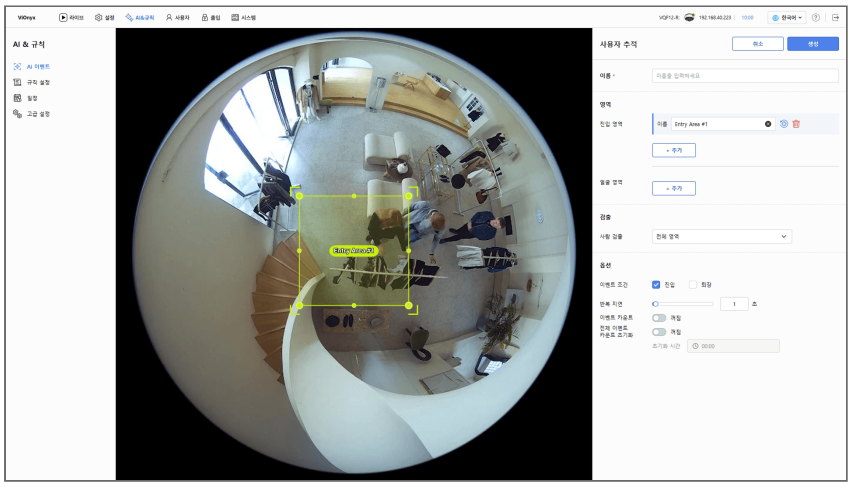


5. **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다. 동의하지 않으면 진행할 수 없습니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다. 이후 AI 이벤트 생성 시에는 동의한 것으로 간주합니다.

6. 오른쪽 **사용자 추적** 패널에서 필요한 설정을 완료하세요.



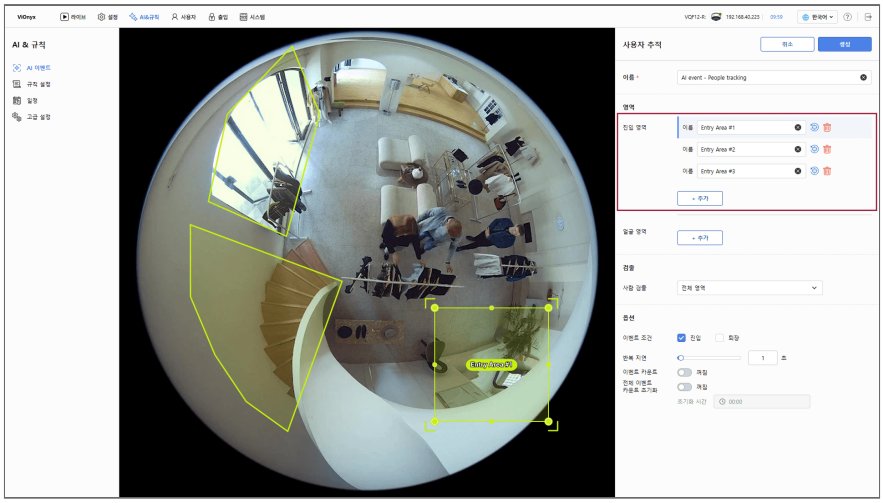
2 이벤트 이름 설정

이름 입력 필드에서 AI 이벤트 이름을 입력하세요. 이름은 최대 64자까지 입력할 수 있습니다.

3 진입 영역 설정

추적할 진입 영역을 설정하세요. 카메라가 설정한 영역의 출입을 감지합니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 노란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수

있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.

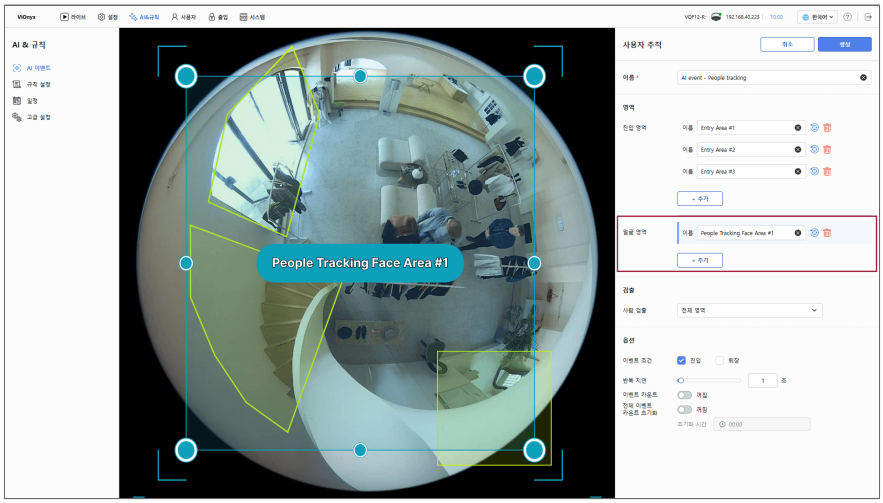


- **이름**: 진입 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 진입 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

> **알아두기**
>
> - 설정한 진입 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 진입 영역을 삭제하려면 버튼을 클릭하세요.

4 얼굴 영역 설정(선택 사항)

얼굴을 감지할 영역을 설정하세요. 설정하면 해당 영역에서 얼굴을 우선 추적합니다. 얼굴 영역은 진입 영역을 포함하도록 설정하세요. 얼굴 영역이 진입 영역을 포함하지 않으면 카메라가 얼굴을 인식하지 못합니다. **+ 추가** 버튼을 클릭해 최대 10개까지 설정할 수 있습니다. 라이브 뷰에 파란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



- **이름**: 얼굴 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 얼굴 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

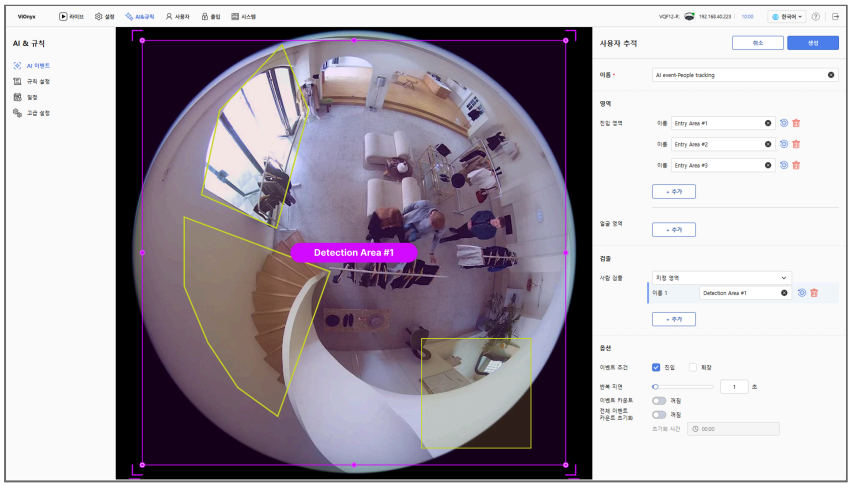
알아두기

- 등록된 사용자는 **라이브** 메뉴에서 신원을 자동 인식해 이름이 표시됩니다. 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다.
- 설정한 얼굴 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 얼굴 영역을 삭제하려면 버튼을 클릭하세요.
- 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 사람이 실제로 서 있거나 지나가면서 얼굴이 잘 보이는 위치가 얼굴 영역에 포함되도록 설정하세요.

5 사람 검출 설정(선택 사항)

검출 섹션에서 카메라가 사람을 검출할 범위를 선택할 수 있습니다. 검출 범위를 필요한 곳으로 좁히면 관심 없는 구역(통로 끝, 창문, 반사면 등)에서 사람을 잘못 검출하는 일을 줄일 수 있습니다.

- **전체 영역**: 기본값으로, 화면 전체에서 사람을 검출합니다. 얼굴 영역 설정 여부와 관계없이 사용할 수 있습니다.
- **지정 영역**: 직접 지정한 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정하지 않았을 때만 선택할 수 있습니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 보라색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



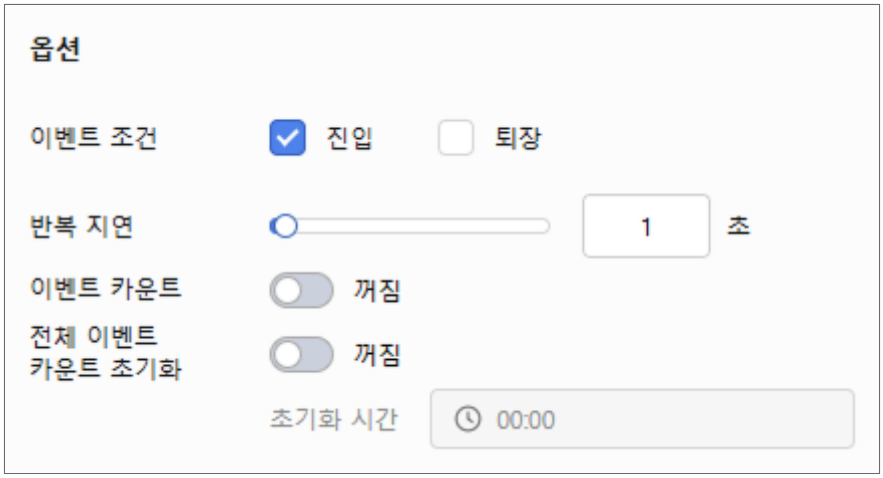
  - **이름**: 사람 검출 영역의 이름을 수정할 수 있습니다.
- **얼굴 영역만**: 얼굴 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정했을 때만 선택할 수 있습니다.

알아두기

- **지정 영역**을 선택한 상태에서 얼굴 영역을 추가하면 **알림** 팝업이 나타납니다. **확인** 버튼을 클릭하면 지정한 검출 영역이 해제되고 **얼굴 영역만**으로 변경됩니다.
- **얼굴 영역만**을 선택한 상태에서 얼굴 영역을 모두 삭제하면 **전체 영역**으로 자동 변경됩니다.
- 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 디스플레이 화면, 사진, 포스터처럼 사람 모습이 있는 물체가 검출 범위에 포함되지 않도록 **지정 영역** 또는 **얼굴 영역만**으로 범위를 좁히세요.
- 설정한 사람 검출 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 사람 검출 영역을 삭제하려면 버튼을 클릭하세요.
- 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.

6 이벤트 발생 조건 및 카운트 설정

옵션 섹션에서 이벤트 발생 조건과 이벤트 카운트를 설정하세요.



- **이벤트 조건**: 이벤트를 발생시킬 동작을 선택하세요. **진입**과 **퇴장**을 모두 선택할 수도 있습니다.
- **반복 지연**: 이벤트로 인식할 최소 시간을 설정하세요. 감지 상태가 설정한 시간보다 오래 이어져야 이벤트가 발생합니다. 최대 60초까지 설정할 수 있습니다.

  너무 많은 이벤트가 발생하면 **반복 지연** 값을 늘리세요. 설정한 시간보다 짧게 감지된 움직임은 이벤트로 인식하지 않으므로 불필요한 이벤트가 줄어듭니다.

- **이벤트 카운트**: 진입 영역에 들어오거나 나간 횟수를 계산하려면 **켜짐**으로 설정하세요. 진입 횟수와 퇴장 횟수를 따로 계산하며, 진입 영역이 여러 개일 때는 영역마다 각각 계산합니다.

  이벤트 조건에서 선택한 항목만 계산합니다. 예를 들어 **진입**만 선택하면 진입 횟수만 이벤트로 표시하고 로그에 기록합니다.

- **전체 이벤트 카운트 초기화**: 모든 진입 영역의 이벤트 카운트를 매일 지정한 시각에 초기화하려면 **켜짐**으로 설정하세요. **초기화 시간**에서 설정한 시각에 모든 진입 영역의 이벤트 카운트를 초기화합니다.

알아두기

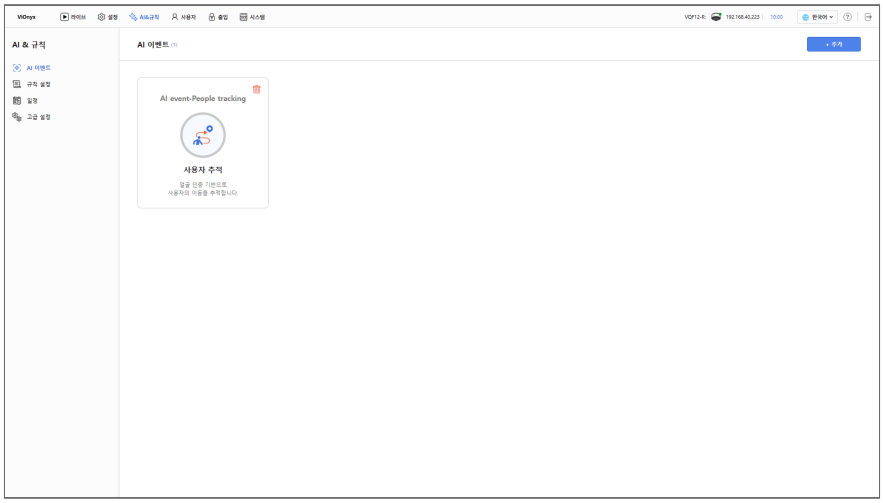
- **이벤트 카운트**를 **켜짐**으로 설정했다면 **라이브** 메뉴 영상 위의 진입 영역마다 **카운트 : N** 형식으로 표시됩니다. 이벤트 카운트를 수동으로 초기화하려면 ••• 버튼을 클릭한 후 **카운트 초기화**를 선택하세요.



- 이벤트 카운트 관련 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

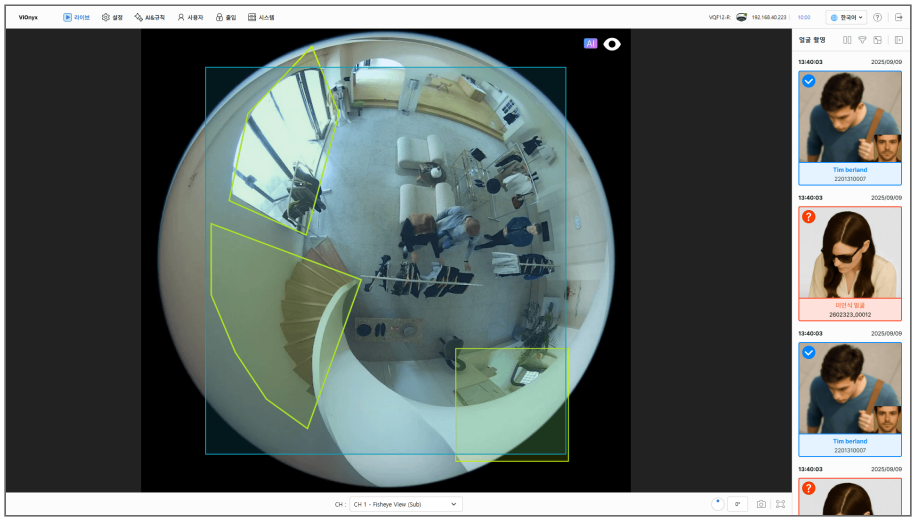
7 설정 저장

모든 설정을 완료한 후 오른쪽 상단의 **생성** 버튼을 클릭하세요. 이전 화면으로 돌아가며, 새로 생성된 AI 이벤트가 목록에 추가됩니다.



라이브에서 확인

화면 왼쪽 상단의 **라이브** 메뉴를 클릭하세요. 카메라 영상 오른쪽 상단의 AI 아이콘이 켜져 있는지 확인하세요. 설정한 진입 영역과 얼굴 영역이 영상에 오버레이로 표시됩니다. 사람이 진입 영역에 들어오거나 나갈 때마다 이벤트가 발생합니다. 얼굴 영역을 설정했다면 카메라가 해당 영역에서 얼굴을 감지하며, 등록된 사용자는 자동으로 신원이 인식되어 이름이 표시됩니다.



알아두기

- 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다. 등록된 사용자는 이름과 함께 표시됩니다.
- 카메라가 얼굴을 인식하지 못한다면 **최소 얼굴 크기 시각화** 옵션을 활성화하세요. 또는 얼굴 영역을 더 크게 설정하거나 카메라 위치를 조정하세요.
- 조명이 부족하거나 역광이 있으면 카메라가 얼굴을 인식하지 못할 수 있습니다. 촬영 공간의 조명을 개선하거나 카메라의 위치와 각도를 조정하여 얼굴이 잘 보이도록 하세요.
- 얼굴이 카메라를 향해야 인식됩니다. 옆모습 또는 뒷모습은 인식이 어려울 수 있습니다.
- 진입 영역에서 이벤트가 발생하지 않는다면 얼굴 영역이 진입 영역을 포함하는지 확인하세요.

침입 감지 이벤트 설정하기

침입 감지 이벤트를 설정하면 관리자가 정의한 구역에 사람이 출입할 때마다 실시간으로 이벤트를 발생합니다. 선택적으로 얼굴 영역을 추가하면 해당 영역에서 얼굴을 우선적으로 추적하며, 등록된 사용자는 자동으로 신원을 인식합니다. 모니터링 필요 구역에 미인가자의 침입을 신속하게 감지하고 실시간으로 알림받을 수 있습니다.

언제 사용하나요?

- 보안이 필요한 구역에 미인가자의 실시간 침입 감지
- 업무시간 외 또는 모니터링 필요 구역에 접근했을 때 실시간 알림 받기
- 모니터링 구역에 미등록자 진입 여부 감지
- 고위험 구역의 출입 현황 기록 및 추적

알아두기

출입 제한 외의 용도로도 사용할 수 있으며, 출입 제한 여부를 카메라에서 판단하지 않습니다.

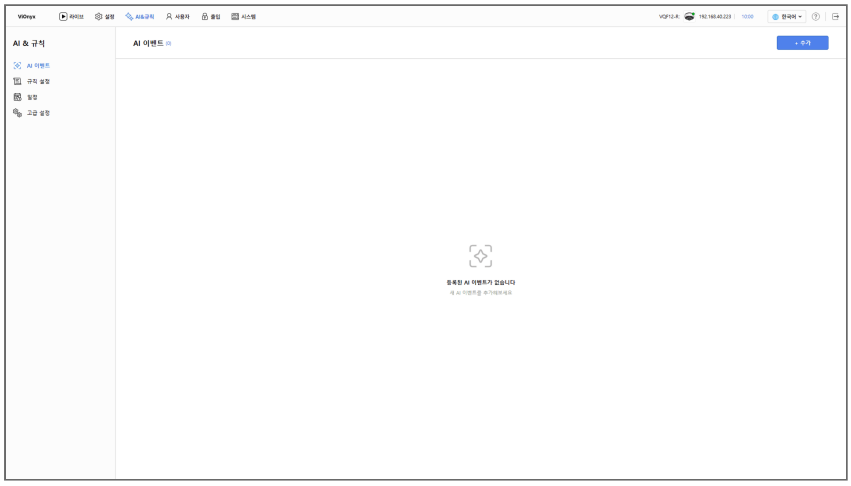
침입 감지 이벤트 생성

침입 감지 이벤트를 생성하면 **라이브** 메뉴에서 특정 구역에 사람이 침입하는 것을 감지하여 이벤트를 발생시킬 수 있습니다. 또한 얼굴 영역을

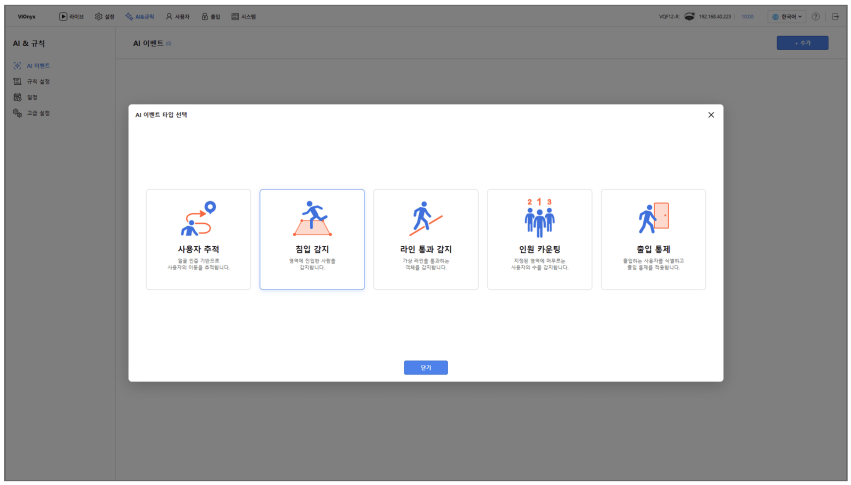
설정하면 해당 영역에서 얼굴을 우선적으로 추적할 수 있으며, 등록된 사용자는 신원을 자동 인식합니다.

1 이벤트 생성 시작

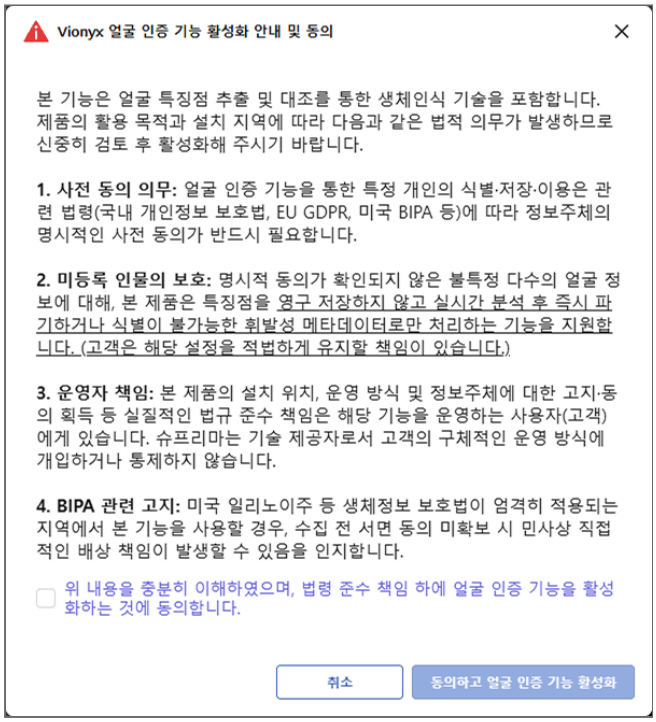
1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
4. **AI 이벤트 타입 선택** 창에서 **침입 감지**를 클릭하세요.

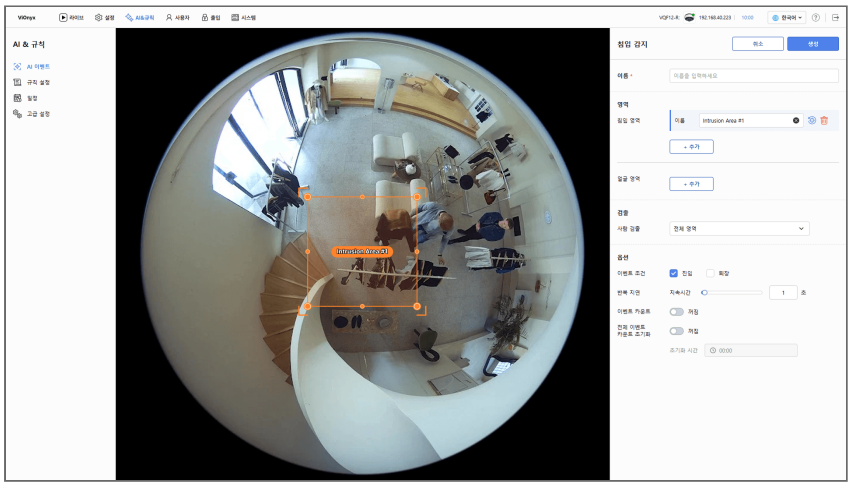


5. **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다. 동의하지 않으면 진행할 수 없습니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다. 이후 AI 이벤트 생성 시에는 동의한 것으로 간주합니다.

6. 오른쪽 **침입 감지** 패널에서 필요한 설정을 완료하세요.



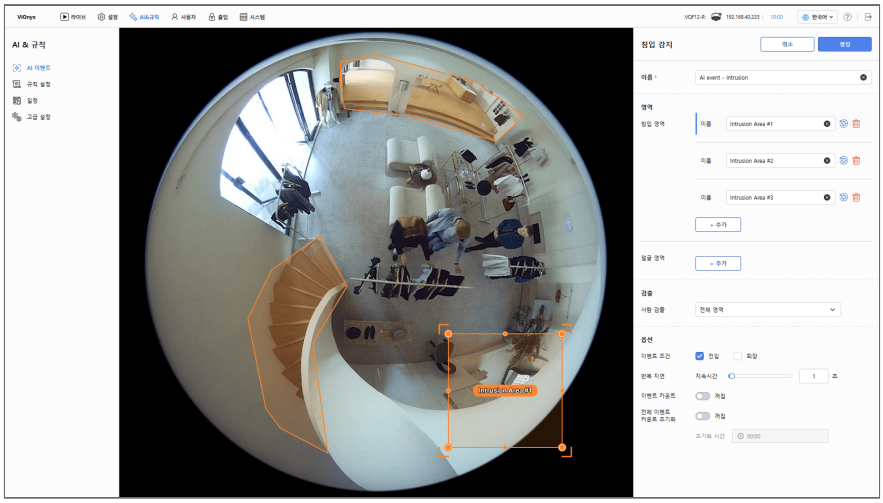
2 이벤트 이름 설정

이름 입력 필드에서 AI 이벤트 이름을 입력하세요. 이름은 최대 64자까지 입력할 수 있습니다.

3 침입 영역 설정

침입 영역을 설정하세요. 카메라가 설정한 영역의 출입을 감지합니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 주황색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다.

가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.

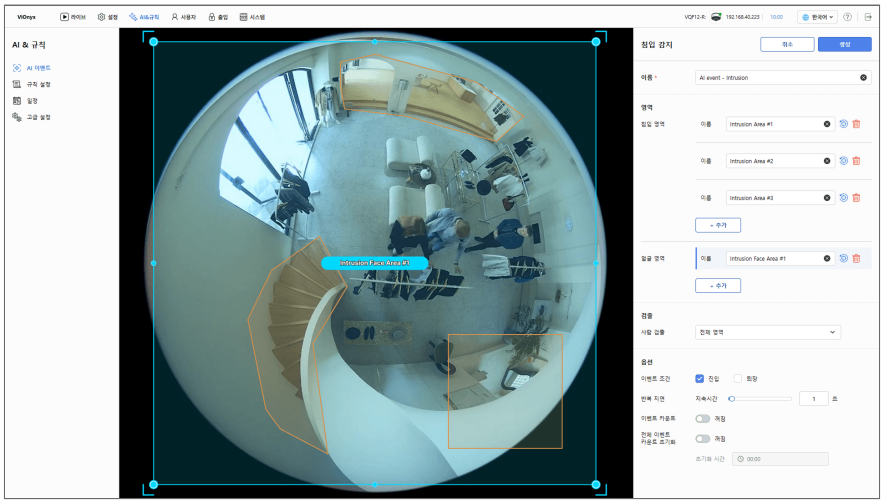


- **이름**: 침입 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 침입 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

> **알아두기**
>
> - 설정한 침입 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 침입 영역을 삭제하려면 버튼을 클릭하세요.

4 얼굴 영역 설정(선택 사항)

얼굴을 감지할 영역을 설정하세요. 설정하면 해당 영역에서 얼굴을 우선 추적합니다. 얼굴 영역에서 감지된 사람을 인증된 사용자와 미인가자로 구분하여 승인된 출입자와 미인가자를 명확하게 파악할 수 있습니다. 얼굴 영역과 침입 영역은 겹쳐서 설정할 수 있습니다. **+ 추가** 버튼을 클릭해 최대 10개까지 설정할 수 있습니다. 라이브 뷰에 파란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



- **이름**: 얼굴 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 얼굴 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

알아두기

- 등록된 사용자는 **라이브** 메뉴에서 신원을 자동 인식해 이름이 표시됩니다. 등록되지 않은 사용자는 **미등록 얼굴**으로 표시됩니다.
- 설정한 얼굴 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 얼굴 영역을 삭제하려면 버튼을 클릭하세요.
- 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 사람이 실제로 서 있거나 지나가면서 얼굴이 잘 보이는 위치가 얼굴 영역에 포함되도록 설정하세요.

5 사람 검출 설정(선택 사항)

검출 섹션에서 카메라가 사람을 검출할 범위를 선택할 수 있습니다. 검출 범위를 필요한 곳으로 좁히면 관심 없는 구역(통로 끝, 창문, 반사면 등)에서 사람을 잘못 검출하는 일을 줄일 수 있습니다.

- **전체 영역**: 기본값으로, 화면 전체에서 사람을 검출합니다. 얼굴 영역 설정 여부와 관계없이 사용할 수 있습니다.
- **지정 영역**: 직접 지정한 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정하지 않았을 때만 선택할 수 있습니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 보라색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



  - **이름**: 사람 검출 영역의 이름을 수정할 수 있습니다.

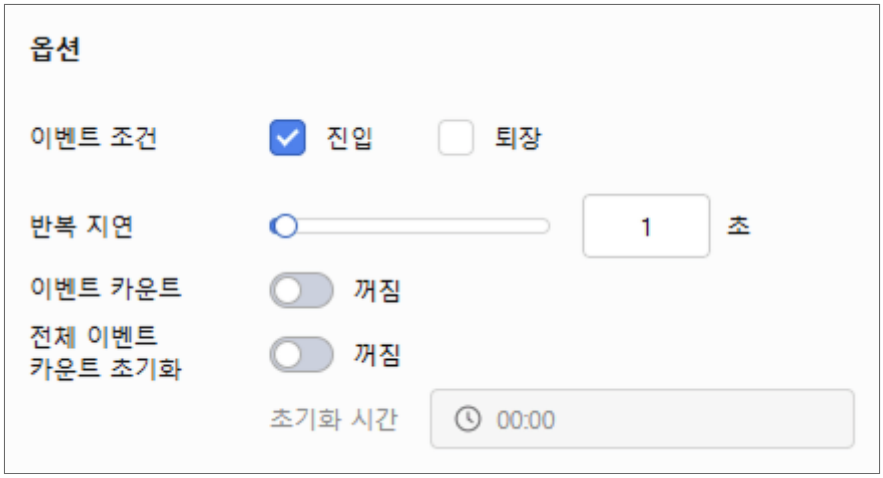
- **얼굴 영역만**: 얼굴 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정했을 때만 선택할 수 있습니다.

알아두기

- **지정 영역**을 선택한 상태에서 얼굴 영역을 추가하면 **알림** 팝업이 나타납니다. **확인** 버튼을 클릭하면 지정한 검출 영역이 해제되고 **얼굴 영역만**으로 변경됩니다.
- **얼굴 영역만**을 선택한 상태에서 얼굴 영역을 모두 삭제하면 **전체 영역**으로 자동 변경됩니다.
- 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 디스플레이 화면, 사진, 포스터처럼 사람 모습이 있는 물체가 검출 범위에 포함되지 않도록 **지정 영역** 또는 **얼굴 영역만**으로 범위를 좁히세요.
- 설정한 사람 검출 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 사람 검출 영역을 삭제하려면 버튼을 클릭하세요.
- 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.

6 이벤트 발생 조건 및 카운트 설정

옵션 섹션에서 이벤트 발생 조건과 이벤트 카운트를 설정하세요.



- **이벤트 조건**: 이벤트를 발생시킬 동작을 선택하세요. **진입**과 **퇴장**을 모두 선택할 수도 있습니다.
- **반복 지연**: 이벤트로 인식할 최소 시간을 설정하세요. 감지 상태가 설정한 시간보다 오래 이어져야 이벤트가 발생합니다. 최대 60초까지 설정할 수 있습니다.

  너무 많은 이벤트가 발생하면 **반복 지연** 값을 늘리세요. 설정한 시간보다 짧게 감지된 움직임은 이벤트로 인식하지 않으므로 불필요한 이벤트가 줄어듭니다.

- **이벤트 카운트**: 침입 영역에 들어오거나 나간 횟수를 계산하려면 **켜짐**으로 설정하세요. 진입 횟수와 퇴장 횟수를 따로 계산하며, 침입 영역이 여러 개일 때는 영역마다 각각 계산합니다.

  이벤트 조건에서 선택한 항목만 계산합니다. 예를 들어 **진입**만 선택하면 진입 횟수만 이벤트로 표시하고 로그에 기록합니다.

- **전체 이벤트 카운트 초기화**: 모든 침입 영역의 이벤트 카운트를 매일 지정한 시각에 초기화하려면 **켜짐**으로 설정하세요. **초기화 시간**에서 설정한 시각에 모든 침입 영역의 이벤트 카운트를 초기화합니다.

알아두기

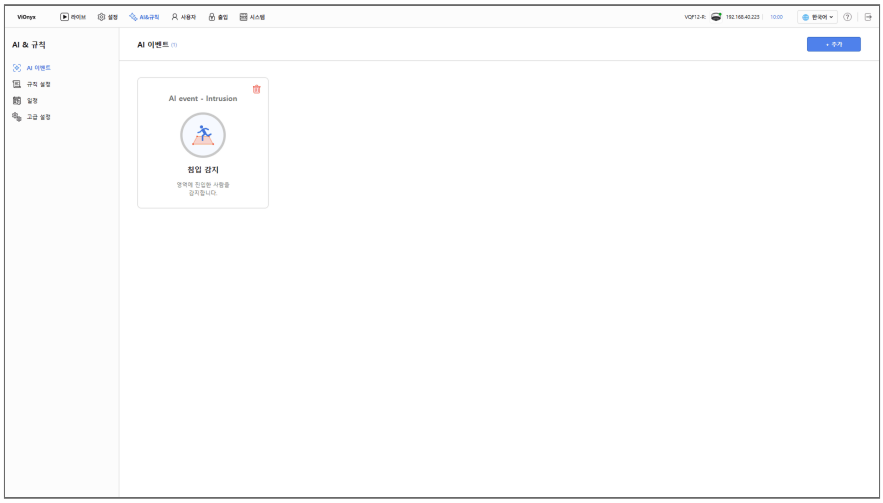
- **이벤트 카운트**를 **켜짐**으로 설정했다면 **라이브** 메뉴 영상 위의 침입 영역마다 **카운트 : N** 형식으로 표시됩니다. 이벤트 카운트를 수동으로 초기화하려면 ••• 버튼을 클릭한 후 **카운트 초기화**를 선택하세요.



- 이벤트 카운트 관련 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

7 설정 저장

모든 설정을 완료한 후 오른쪽 상단의 **생성** 버튼을 클릭하세요. 이전 화면으로 돌아가며, 새로 생성된 AI 이벤트가 목록에 추가됩니다.



라이브에서 확인

화면 왼쪽 상단의 **라이브** 메뉴를 클릭하세요. 카메라 영상의 오른쪽 상단의 AI 아이콘이 켜져 있는지 확인하세요. 설정한 침입 영역과 얼굴 영역이 영상에 오버레이로 표시됩니다. 사람이 침입 영역에 들어오거나 나갈 때마다 이벤트가 발생합니다. 얼굴 영역을 설정했다면 카메라가 해당 영역에서 얼굴을 감지하며, 등록된 사용자는 자동으로 신원이 인식되어 이름을 표시합니다.



알아두기

- 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다. 등록된 사용자는 이름과 함께 표시합니다.
- 조명이 부족하거나 역광이 있으면 카메라가 얼굴을 인식하지 못할 수 있습니다. 촬영 공간의 조명을 개선하거나 카메라의 위치와 각도를 조정하여 얼굴이 잘 보이도록 하세요.
- 얼굴이 카메라로 향해야 인식됩니다. 옆모습 또는 뒷모습은 인식이 어려울 수 있습니다.

라인 통과 감지 이벤트 설정하기

라인 통과 감지 이벤트를 설정하면 설정한 가상 라인을 통과하는 사람을 감지하여 실시간으로 이벤트를 발생합니다. 통과 방향(A→B, B→A, 양방향)을 지정하여 특정 방향의 출입만 모니터링할 수 있으며, 선택적으로 얼굴 영역을 추가하면 등록된 사용자를 자동으로 신원을 인식합니다.

언제 사용하나요?

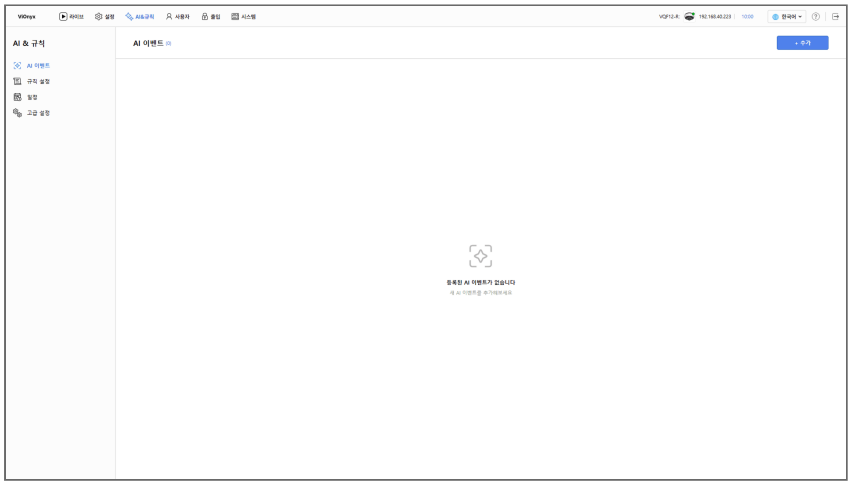
- 출입구의 통행량 모니터링 및 카운팅
- 특정 방향으로의 출입만 감시 (한 방향 통행로 감지)
- 업무시간 외 특정 영역으로의 출입 감지
- 라인을 기준으로 좌측/우측 구역 이동 추적

라인 통과 감지 이벤트 생성

라인 통과 감지 이벤트를 생성하면 **라이브** 메뉴에서 특정 구역에 사람이 라인을 통과하는 것을 감지하여 이벤트를 발생시킬 수 있습니다. 또한 얼굴 영역을 설정하면 해당 영역에서 얼굴을 우선적으로 추적할 수 있으며, 등록된 사용자는 신원을 자동 인식합니다.

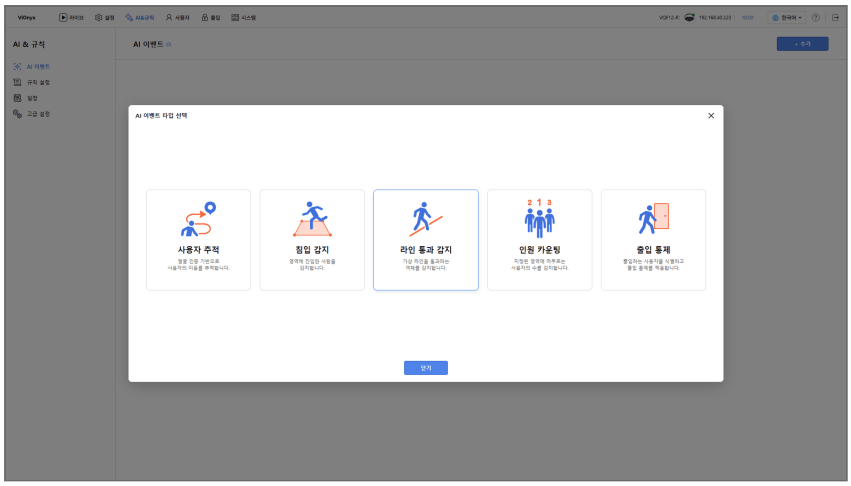
1 이벤트 생성 시작

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.

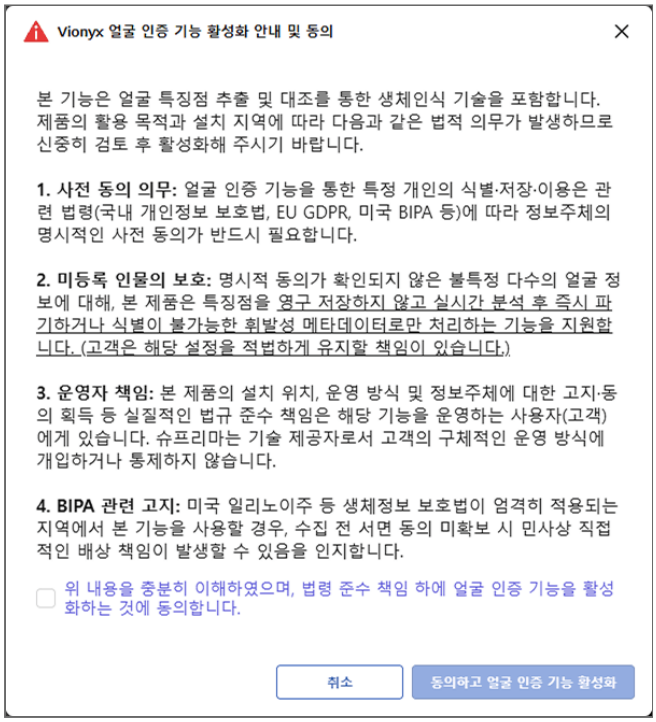


3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.

4. **AI 이벤트 타입 선택** 창에서 **라인 통과 감지**를 클릭하세요.

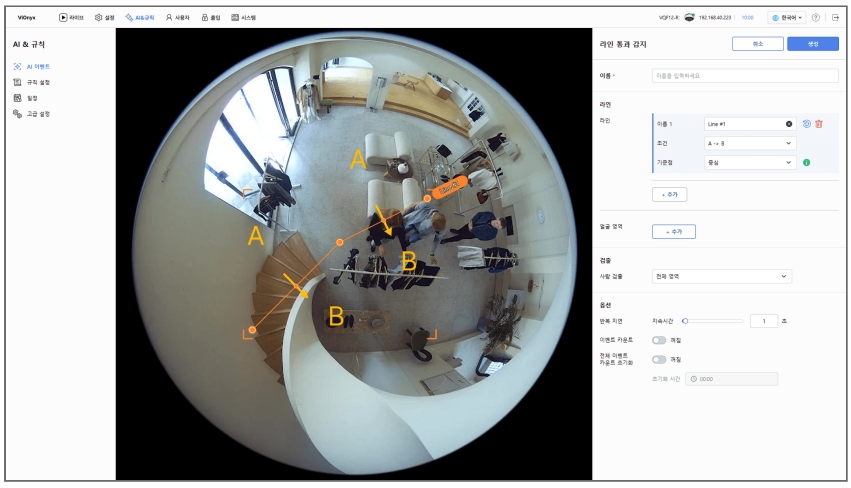


5. **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다. 동의하지 않으면 진행할 수 없습니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다. 이후 AI 이벤트 생성 시에는 동의한 것으로 간주합니다.

6. 오른쪽 **라인 통과 감지** 패널에서 필요한 설정을 완료하세요.



2 이벤트 이름 설정

이름 입력 필드에서 AI 이벤트 이름을 입력하세요. 이름은 최대 64자까지 입력할 수 있습니다.

3 가상 라인 설정

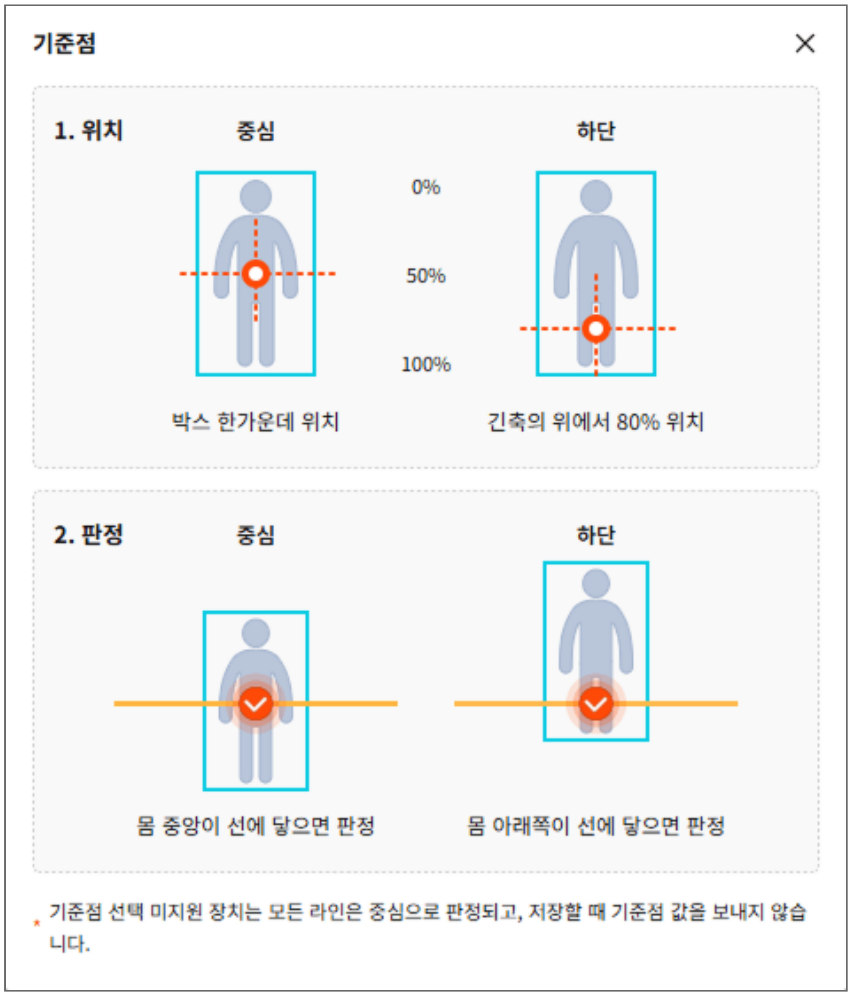
라이브 뷰에서 가상 라인을 적절한 위치에 설정하세요. 카메라에 설정한 가상 라인을 통과하는 사람을 감지하여 이벤트를 발생시킵니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 주황색 라인이 표시되며, 마우스로

모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



- **이름**: 가상 라인의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 가상 라인의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.
- **조건**: 가상 라인을 통과하는 조건을 설정하세요. 아래 3가지 방향 옵션 중 하나를 선택할 수 있습니다.
  - **A -> B**: A에서 B 방향으로 통과 시 이벤트 발생
  - **B -> A**: B에서 A 방향으로 통과 시 이벤트 발생
  - **A <-> B**: 양방향으로 통과 시 이벤트 발생
- **기준점**: 사람이 가상 라인을 통과했는지 판정할 때 사람 감지 박스의 어느 지점을 기준으로 할지 선택하세요. 라인마다 다르게 설정할 수 있으며, 기본값은 **중심**입니다.
  - **중심**: 박스의 한가운데를 기준으로 판정합니다. 몸 중앙이 라인에 닿으면 통과한 것으로 판정합니다.
  - **하단**: 박스의 긴 축을 따라 위에서 80% 지점을 기준으로 판정합니다. 몸 아래쪽이 라인에 닿으면 통과한 것으로 판정합니다. 바닥에 라인을 그렸을 때처럼 발이 라인을 넘는 시점에 이벤트를 발생시키려면 이 옵션을 선택하세요.

기준점 오른쪽의 ⓘ 아이콘을 클릭하면 각 기준점의 위치와 판정 방식을 그림으로 확인할 수 있습니다.



알아두기

- **기준점** 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다. 기준점 선택을 지원하지 않는 장치에서는 모든 라인 통과를 **중심**으로 판정합니다.
- **하단**은 사람 감지 박스를 기준으로 계산한 위치이며, 실제 발 위치를 검출하는 것은 아닙니다.
- **라이브** 메뉴에서 판정 기준점을 확인하려면 AI 표시 옵션에서 **기준점** 옵션을 켜세요.
- 설정한 가상 라인의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 가상 라인을 삭제하려면 버튼을 클릭하세요.

4 얼굴 영역 설정(선택 사항)

얼굴을 감지할 영역을 설정하세요. 설정하면 해당 영역에서 얼굴을 우선 추적합니다. 얼굴 영역과 가상 라인은 겹쳐서 설정할 수 있습니다. **+ 추가** 버튼을 클릭해 최대 10개까지 설정할 수 있습니다. 라이브 뷰에 파란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



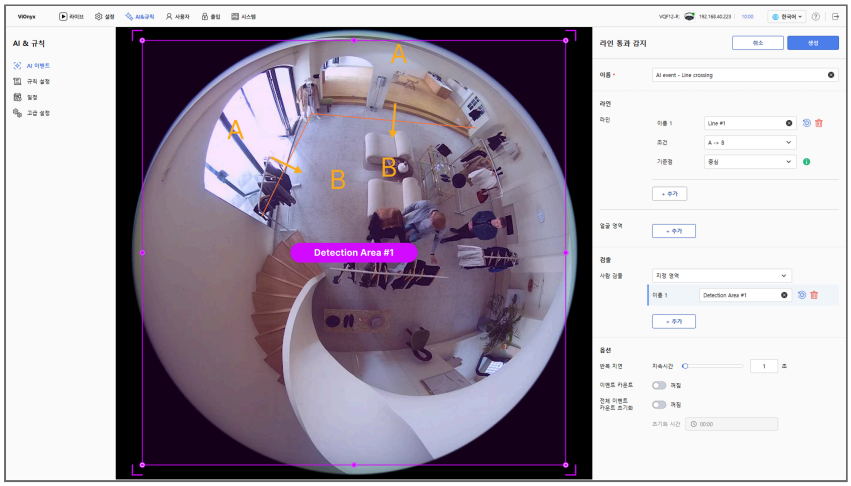
- **이름**: 얼굴 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 얼굴 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

> **알아두기**
>
> - 등록된 사용자는 **라이브** 메뉴에서 신원을 자동 인식해 이름이 표시됩니다. 등록되지 않은 사용자는 **미등록 얼굴**으로 표시됩니다.
> - 설정한 얼굴 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 얼굴 영역을 삭제하려면 버튼을 클릭하세요.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 사람이 실제로 서 있거나 지나가면서 얼굴이 잘 보이는 위치가 얼굴 영역에 포함되도록 설정하세요.

5 사람 검출 설정(선택 사항)

검출 섹션에서 카메라가 사람을 검출할 범위를 선택할 수 있습니다. 검출 범위를 필요한 곳으로 좁히면 관심 없는 구역(통로 끝, 창문, 반사면 등)에서 사람을 잘못 검출하는 일을 줄일 수 있습니다.

- **전체 영역**: 기본값으로, 화면 전체에서 사람을 검출합니다. 얼굴 영역 설정 여부와 관계없이 사용할 수 있습니다.
- **지정 영역**: 직접 지정한 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정하지 않았을 때만 선택할 수 있습니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 보라색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



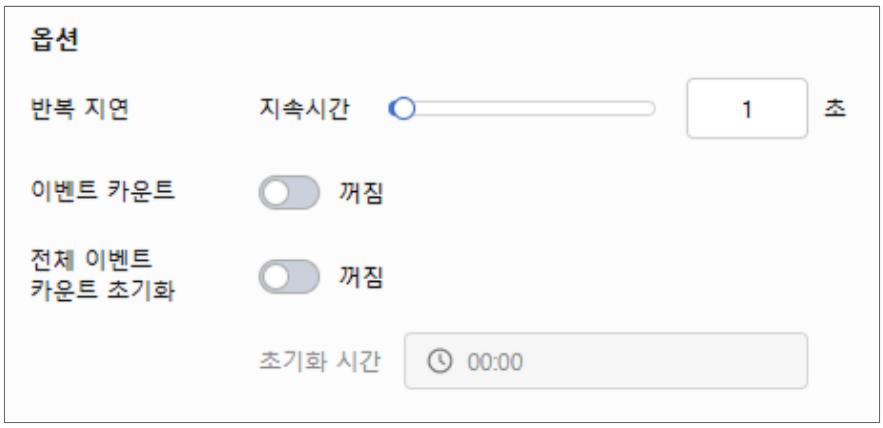
  - **이름**: 사람 검출 영역의 이름을 수정할 수 있습니다.

- **얼굴 영역만**: 얼굴 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정했을 때만 선택할 수 있습니다.

> **알아두기**
>
> - **지정 영역**을 선택한 상태에서 얼굴 영역을 추가하면 **알림** 팝업이 나타납니다. **확인** 버튼을 클릭하면 지정한 검출 영역이 해제되고 **얼굴 영역만**으로 변경됩니다.
> - **얼굴 영역만**을 선택한 상태에서 얼굴 영역을 모두 삭제하면 **전체 영역**으로 자동 변경됩니다.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 디스플레이 화면, 사진, 포스터처럼 사람 모습이 있는 물체가 검출 범위에 포함되지 않도록 **지정 영역** 또는 **얼굴 영역만**으로 범위를 좁히세요.
> - 설정한 사람 검출 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 사람 검출 영역을 삭제하려면 버튼을 클릭하세요.
> - 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.

6 이벤트 발생 조건 및 카운트 설정

옵션 섹션에서 이벤트 발생 조건과 이벤트 카운트를 설정하세요.



- **반복 지연**: 이벤트로 인식할 최소 시간을 설정하세요. 감지 상태가 설정한 시간보다 오래 이어져야 이벤트가 발생합니다. 최대 60초까지 설정할 수 있습니다.

> 너무 많은 이벤트가 발생하면 **반복 지연** 값을 늘리세요. 설정한 시간보다 짧게 감지된 움직임은 이벤트로 인식하지 않으므로 불필요한 이벤트가 줄어듭니다.

- **이벤트 카운트**: 라인을 통과할 때마다 횟수를 계산하려면 **켜짐**으로 설정하세요. 라인이 여러 개일 때는 라인마다 각각 계산합니다.
- **전체 이벤트 카운트 초기화**: 모든 라인의 이벤트 카운트를 매일 지정한 시각에 초기화하려면 **켜짐**으로 설정하세요. **초기화 시간**에서 설정한 시각에 모든 라인의 이벤트 카운트를 초기화합니다.

알아두기

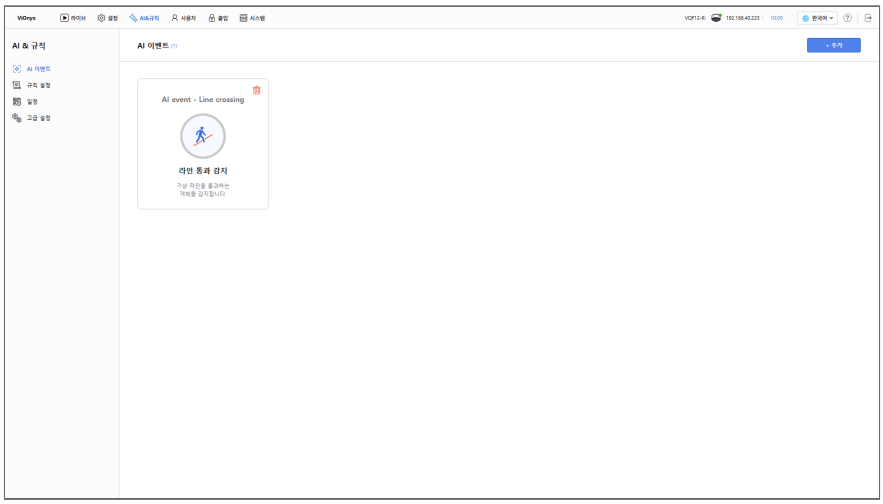
- **이벤트 카운트**를 **켜짐**으로 설정했다면 **라이브** 메뉴 영상 위의 라인마다 **카운트 : N** 형식으로 표시됩니다. 이벤트 카운트를 수동으로 초기화하려면 ••• 버튼을 클릭한 후 **카운트 초기화**를 선택하세요.



- 이벤트 카운트 관련 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

7 설정 저장

모든 설정을 완료한 후 오른쪽 상단의 **생성** 버튼을 클릭하세요. 이전 화면으로 돌아가며, 새로 생성된 AI 이벤트가 목록에 추가됩니다.



라이브에서 확인

화면 왼쪽 상단의 **라이브** 메뉴를 클릭하세요. 카메라 영상의 오른쪽 상단의 AI 아이콘이 켜져 있는지 확인하세요. 설정한 가상 라인과 얼굴 영역이 영상에 오버레이로 표시됩니다. 사람이 가상 라인을 통과할 때마다 이벤트가 발생합니다. 얼굴 영역을 설정했다면 카메라가 해당 영역에서 얼굴을 감지하며, 등록된 사용자는 자동으로 신원이 인식되어 이름을 표시합니다.



알아두기

- 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다. 등록된 사용자는 이름과 함께 표시합니다.
- 조명이 부족하거나 역광이 있으면 카메라가 얼굴을 인식하지 못할 수 있습니다. 촬영 공간의 조명을 개선하거나 카메라의 위치와 각도를 조정하여 얼굴이 잘 보이도록 하세요.
- 얼굴이 카메라로 향해야 인식됩니다. 옆모습 또는 뒷모습은 인식이 어려울 수 있습니다.

인원 카운팅 이벤트 설정하기

인원 카운팅 이벤트를 설정하면 지정된 구역에 머무르는 사람의 수를 감지할 수 있습니다. 선택적으로 얼굴 영역을 추가하면 등록된 사용자를 자동으로 신원을 인식합니다.

언제 사용하나요?

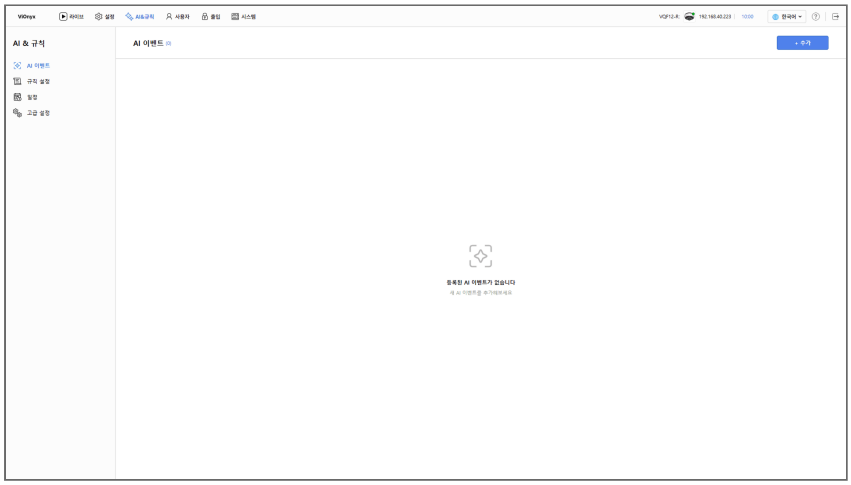
- 소매점 또는 매장의 특정 구역 방문객 수를 실시간 모니터링하고 싶을 때
- 혼잡도 관리를 위해 특정 구역의 인원 현황을 파악하고 싶을 때
- 등록된 직원/VIP 고객의 출입 현황을 추적하고 싶을 때
- 보안 목적으로 특정 구역의 출입 통계를 관리하고 싶을 때

인원 카운팅 이벤트 생성

인원 카운팅 이벤트를 생성하면 **라이브** 메뉴에서 지정된 구역에 머무르는 사람의 수를 감지할 수 있습니다. 또한 얼굴 영역을 설정하면 해당 영역에서 얼굴을 우선적으로 추적할 수 있으며, 등록된 사용자는 신원을 자동 인식합니다.

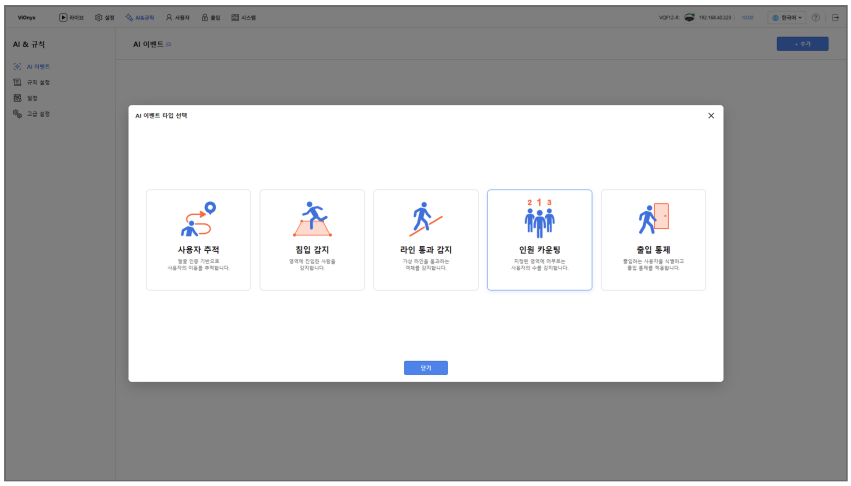
1 이벤트 생성 시작

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.

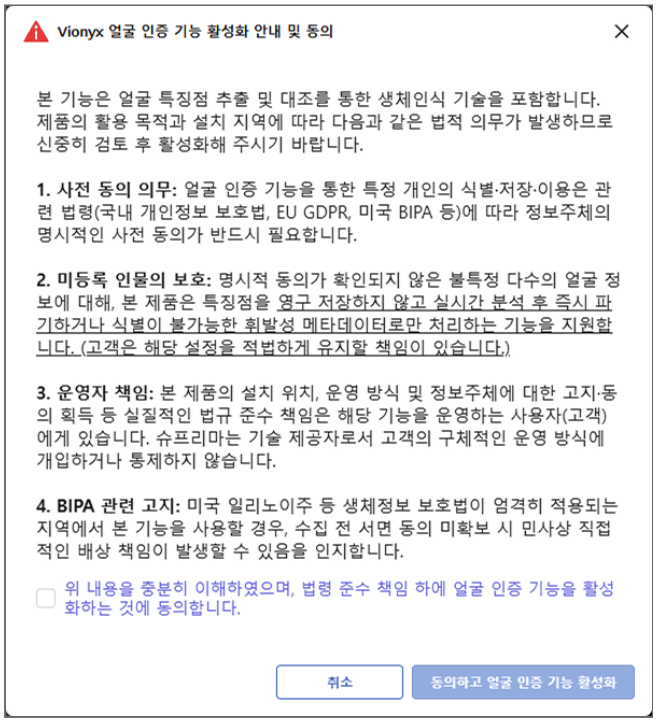


3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.

4. **AI 이벤트 타입 선택** 창에서 **인원 카운팅**을 클릭하세요.

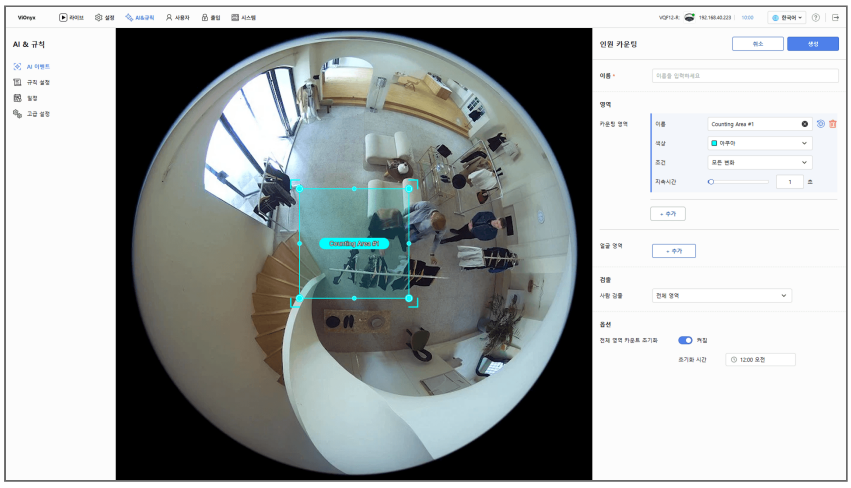


5. **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다. 동의하지 않으면 진행할 수 없습니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다. 이후 AI 이벤트 생성 시에는 동의한 것으로 간주합니다.

6. 오른쪽 **인원 카운팅** 패널에서 필요한 설정을 완료하세요.



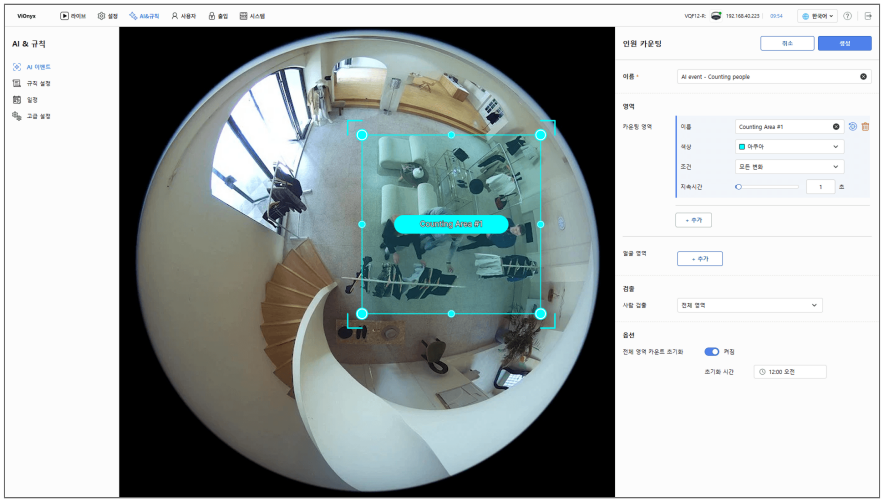
2 이벤트 이름 설정

이름 입력 필드에서 AI 이벤트 이름을 입력하세요. 이름은 최대 64자까지 입력할 수 있습니다.

3 카운팅 영역 설정

라이브 뷰에서 카운팅 영역을 설정하세요. 카메라에서 설정한 카운팅 영역에 머무르는 사람을 실시간으로 카운팅하고 이벤트를 발생시킵니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 표시되는 카운팅 영역

상자의 모서리 또는 점을 마우스로 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



- **이름**: 카운팅 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 카운팅 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.
- **색상**: 카운팅 영역의 색상을 선택할 수 있습니다. 라이브 뷰에서 카운팅 영역이 선택한 색상으로 표시됩니다.
- **조건**: 이벤트 발생 조건을 설정하세요.
  - **모든 변화**: 사람이 카운팅 영역에 들어오거나 나갈 때마다 이벤트 발생
  - **카운트 제한**: 카운팅 영역에 머무르는 사람 수가 지정한 수를 초과할 때 이벤트 발생 (기본값 10명, 최대값 100명)
- **지속시간**: 카운팅 영역에 머무르는 사람의 수가 이벤트 발생 조건을 충족해야 하는 최소 시간을 설정하세요. 예를 들어, Duration을 5초로 설정하면 사람이 카운팅 영역에 5초 이상 머물러야 이벤트가 발생합니다. 최대 60초까지 설정할 수 있습니다.

알아두기

- 설정한 카운팅 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 카운팅 영역을 삭제하려면 버튼을 클릭하세요.

4 얼굴 영역 설정(선택 사항)

얼굴을 감지할 영역을 설정하세요. 설정하면 해당 영역에서 얼굴을 우선 추적합니다. 얼굴 영역과 카운팅 영역은 겹쳐서 설정할 수 있습니다. **+ 추가** 버튼을 클릭해 최대 10개까지 설정할 수 있습니다. 라이브 뷰에 파란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



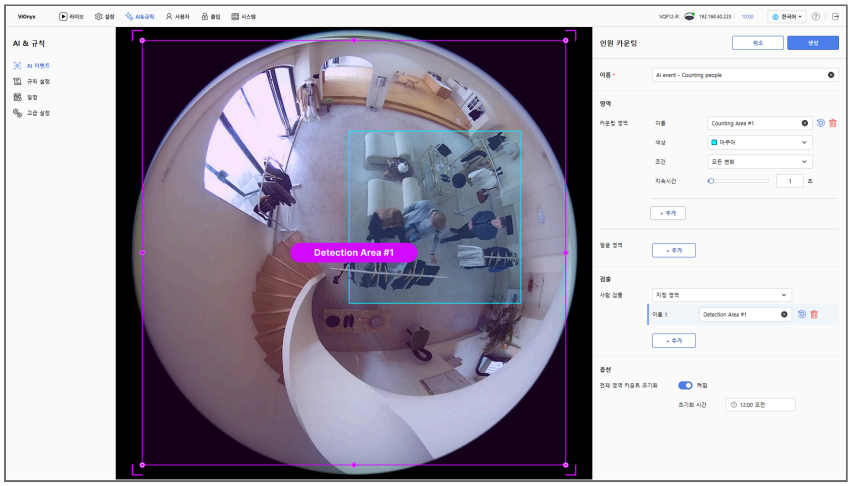
- **이름**: 얼굴 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 얼굴 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

> **알아두기**
>
> - 등록된 사용자는 **라이브** 메뉴에서 신원을 자동 인식해 이름이 표시됩니다. 등록되지 않은 사용자는 **미등록 얼굴**으로 표시됩니다.
> - 설정한 얼굴 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 얼굴 영역을 삭제하려면 버튼을 클릭하세요.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 사람이 실제로 서 있거나 지나가면서 얼굴이 잘 보이는 위치가 얼굴 영역에 포함되도록 설정하세요.

5 사람 검출 설정(선택 사항)

검출 섹션에서 카메라가 사람을 검출할 범위를 선택할 수 있습니다. 검출 범위를 필요한 곳으로 좁히면 관심 없는 구역(통로 끝, 창문, 반사면 등)에서 사람을 잘못 검출하는 일을 줄일 수 있습니다.

- **전체 영역**: 기본값으로, 화면 전체에서 사람을 검출합니다. 얼굴 영역 설정 여부와 관계없이 사용할 수 있습니다.
- **지정 영역**: 직접 지정한 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정하지 않았을 때만 선택할 수 있습니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 보라색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



  - **이름**: 사람 검출 영역의 이름을 수정할 수 있습니다.

- **얼굴 영역만**: 얼굴 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정했을 때만 선택할 수 있습니다.

> **알아두기**
>
> - **지정 영역**을 선택한 상태에서 얼굴 영역을 추가하면 **알림** 팝업이 나타납니다. **확인** 버튼을 클릭하면 지정한 검출 영역이 해제되고 **얼굴 영역만**으로 변경됩니다.
> - **얼굴 영역만**을 선택한 상태에서 얼굴 영역을 모두 삭제하면 **전체 영역**으로 자동 변경됩니다.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 디스플레이 화면, 사진, 포스터처럼 사람 모습이 있는 물체가 검출 범위에 포함되지 않도록 **지정 영역** 또는 **얼굴 영역만**으로 범위를 좁히세요.
> - 설정한 사람 검출 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 사람 검출 영역을 삭제하려면 버튼을 클릭하세요.
> - 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.

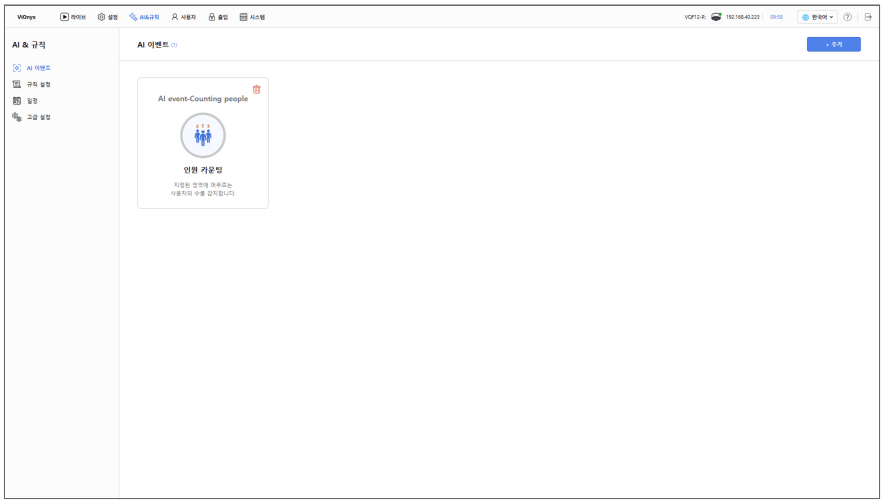
6 카운팅 초기화 설정

카운팅 영역에 머무르는 사람 수를 초기화하는 조건을 설정하세요.

- **전체 영역 카운트 초기화**: 모든 카운팅 영역의 카운팅을 정해진 시간마다 초기화하려면 **켜짐**으로 설정하세요. **초기화 시간**에서 설정한 시각에 모든 카운팅 영역의 카운팅이 초기화됩니다.

7 설정 저장

모든 설정을 완료한 후 오른쪽 상단의 **생성** 버튼을 클릭하세요. 이전 화면으로 돌아가며, 새로 생성된 AI 이벤트가 목록에 추가됩니다.



라이브에서 확인

화면 왼쪽 상단의 **라이브** 메뉴를 클릭하세요. 카메라 영상의 오른쪽 상단의 AI 아이콘이 켜져 있는지 확인하세요. 설정한 카운팅 영역과 얼굴 영역이 영상에 오버레이로 표시됩니다. 카운팅 영역에 머무르는 사람의 수를 **카운트 : N** 형식으로 표시합니다. 얼굴 영역을 설정했다면 카메라가 해당 영역에서 얼굴을 감지하며, 등록된 사용자는 자동으로 신원이 인식되어 이름을 표시합니다.



알아두기

- 카운트 값을 수동으로 초기화하려면 ··· → **카운트 초기화** 버튼을 클릭하세요.



- 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다. 등록된 사용자는 이름과 함께 표시합니다.
- 조명이 부족하거나 역광이 있으면 카메라가 얼굴을 인식하지 못할 수 있습니다. 촬영 공간의 조명을 개선하거나 카메라의 위치와 각도를 조정하여 얼굴이 잘 보이도록 하세요.
- 얼굴이 카메라로 향해야 인식됩니다. 옆모습 또는 뒷모습은 인식이 어려울 수 있습니다.

출입 통제 이벤트 설정하기

출입 통제 이벤트를 설정하면 출입문으로 접근하는 사람을 얼굴 인식으로 식별하고, 출입문 주변에 함께 있는 사람까지 검증하여 출입 허용 여부를 판단할 수 있습니다. 인증된 사용자를 뒤따라 미인가자가 함께 들어오는 테일게이팅(Tailgating)을 감지할 수 있으며, 출입문 안쪽에서 나오는 사람은 판단 대상에서 제외할 수 있습니다.

> **알아두기**
> 출입 통제 이벤트는 펌웨어 버전 1.1.0 이상에서 지원합니다.

언제 사용하나요?

- 출입문에 접근하는 사람이 등록된 사용자인지 얼굴 인식으로 확인할 때
- 인증된 사용자를 뒤따라 미인가자가 함께 들어오는 테일게이팅을 막아야 할 때
- 출입문 안쪽에서 나오는 사람을 제외하고, 들어오는 사람만 출입 판단 대상으로 삼을 때
- 출입 판단 결과에 따라 문을 열거나 경고 음성을 출력하는 등 후속 동작을 연동할 때

> **알아두기**
> 출입 통제 이벤트는 출입 허용 여부를 **판단**하는 역할만 하며, 출입문의 릴레이를 직접 제어하지 않습니다. 판단 결과에 따라 출입문을 열려면 이벤트를 생성한 후 출입문을 등록하고 이벤트를 연결하세요. 음성 안내나 웹훅 알림 같은 추가 동작이 필요하면 출입문 규칙을 설정하세요.
>
> - 출입문 등록 및 관리에 대한 자세한 내용은 출입문 관리하기를 참고하세요.
> - 출입문 규칙에 대한 자세한 내용은 출입문 규칙 설정하기를 참고하세요.

출입 통제 이벤트 동작 방식

출입 통제 이벤트는 다음 요소를 조합하여 출입 허용 여부를 판단합니다. 설정을 시작하기 전에 각 요소의 역할을 확인하세요.

구성 요소	역할	필수 여부
검증 영역	출입 통제 영역을 둘러싼 더 넓은 영역입니다. 이 영역에 있는 사람 수와 식별 상태를 확인하여 테일게이팅 여부를 판단합니다.	필수
출입 통제 영역	출입문 바로 앞 영역입니다. 사람이 이 영역에 들어오면 출입을 시도하는 것으로 보고 판단을 시작합니다.	필수
이벤트 진입 라인	출입문을 실제로 통과한 사람을 판단하는 선입니다. 선택한 방향에 따라 들어오는 사람, 나가는 사람 또는 양쪽 모두를 판단합니다.	필수
얼굴 영역	얼굴을 우선 추적하여 사용자를 식별하는 영역입니다.	선택

카메라는 영역 안의 사람을 다음 상태 중 하나로 구분합니다.

- **식별됨**: 얼굴 인식에 성공하여 등록된 사용자로 확인된 상태입니다.

- **미식별**: 얼굴을 인식하지 못했거나 등록된 사용자와 일치하지 않는 상태입니다. 등록되지 않은 사람, 얼굴이 가려지거나 카메라를 향하지 않은 사람은 라이브 메뉴에서 **미등록 얼굴**로 표시됩니다.

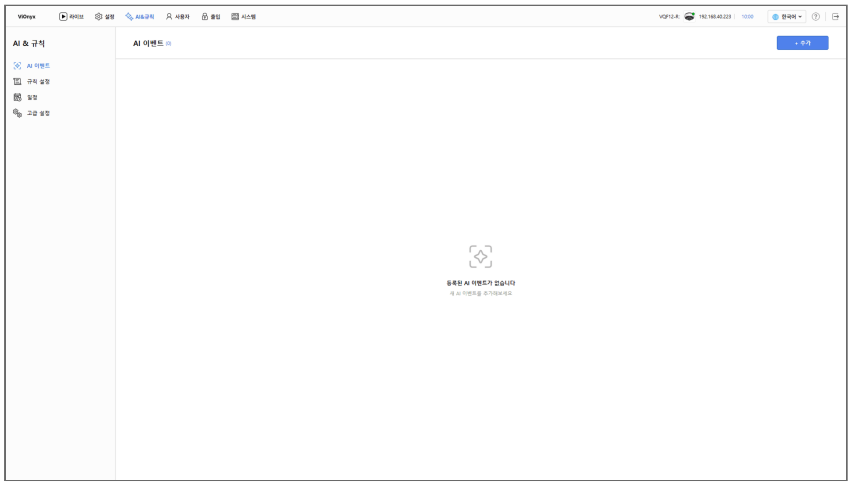
> **주의**
> 보안을 위해 얼굴을 인식하지 못한 사람은 인증된 사용자로 간주하지 않습니다. 출입 통제 영역에 들어온 사람이 미식별 상태이면 출입이 허용되지 않습니다.

출입 통제 이벤트 생성

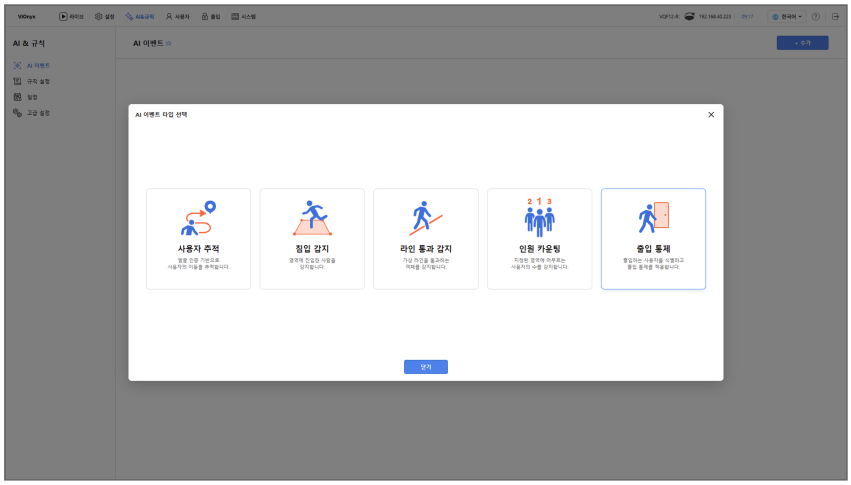
출입 통제 이벤트를 생성하면 **라이브** 메뉴에서 출입문에 접근하는 사용자를 식별하고, 뒤따라 들어오는 사람을 검증할 수 있습니다.

1 이벤트 생성 시작

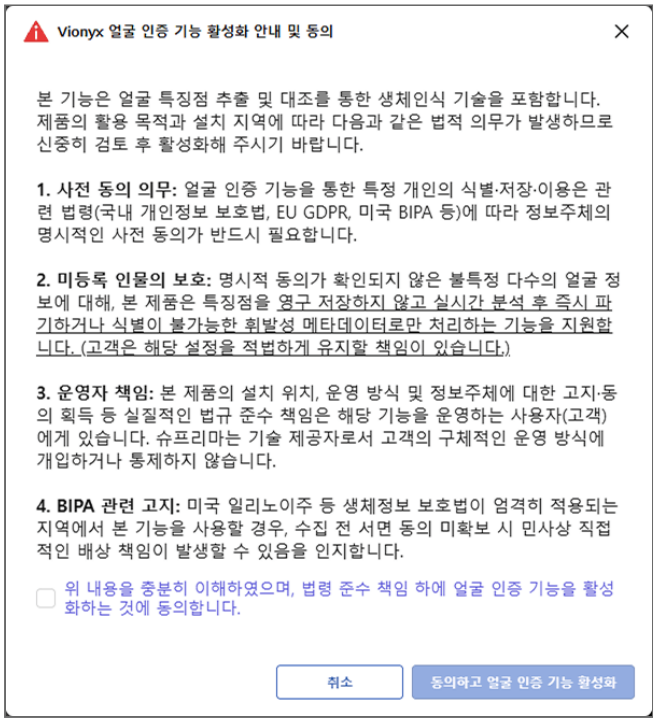
1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
4. **AI 이벤트 타입 선택** 창에서 **출입 통제**를 클릭하세요.

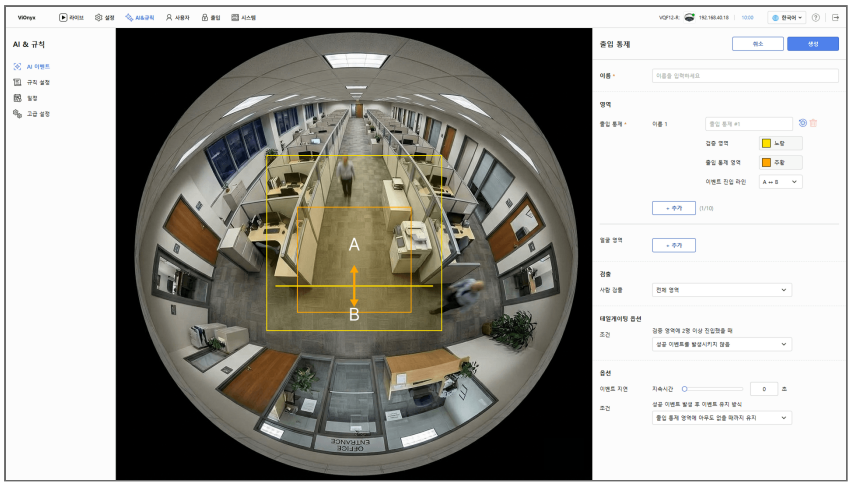


5. **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 출입 통제 이벤트는 얼굴 인식으로 사용자를 식별하므로 얼굴 인식 사용에 동의해야 생성할 수 있습니다.
- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다. 이후 AI 이벤트 생성 시에는 동의한 것으로 간주합니다.

6. 오른쪽 **출입 통제** 패널에서 필요한 설정을 완료하세요.



2 이벤트 이름 설정

이름 입력 필드에서 AI 이벤트 이름을 입력하세요. 이름은 최대 64자까지 입력할 수 있습니다.

3 출입 통제 영역 설정

영역 섹션에서 출입문 위치에 맞게 검증 영역, 출입 통제 영역, 이벤트 진입 라인을 설정하세요. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 하나를 추가할 때마다 세 요소가 한 묶음으로 라이브 뷰에 표시됩니다. 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정하고, 가운데 영역을 드래그하여 위치를 이동하세요.



- **이름**: 출입 통제 영역의 이름을 수정할 수 있습니다. 출입문 위치 등 알기 쉽게 이름을 지정하세요.
- **검증 영역**(노란색): 출입 통제 영역을 둘러싼 검증 영역입니다. 출입 통제 영역으로 빠르게 다가오거나 뒤따라오는 사람까지 확인할 수 있도록 출입 통제 영역보다 넓게 설정하세요.
- **출입 통제 영역**(주황색): 출입문 바로 앞, 출입하려는 사람이 반드시 지나가는 위치에 설정하세요. 사람이 이 영역에 들어오면 출입 판단을 시작합니다.
- **이벤트 진입 라인**: 출입문을 실제로 통과한 사람을 판단하는 라인입니다. 출입하는 사람이 반드시 지나가도록 선 양 끝의 점을 드래그하여 출입 통제 영역을 가로질러 배치하세요. 그런 다음 판단할 통과 방향을 선택하세요.
  - **A → B**: A에서 B 방향으로 통과하는 사람만 판단합니다.
  - **B → A**: B에서 A 방향으로 통과하는 사람만 판단합니다.
  - **A ↔ B**: 양방향을 모두 판단합니다. 들어오는 사람과 나가는 사람을 구분해 판단합니다.

  들어오는 사람이나 나가는 사람 중 한쪽만 판단하려면 라이브 뷰에서 A와 B의 위치를 확인한 후 **A → B** 또는 **B → A**를 선택하세요.

알아두기

- 검증 영역은 출입 통제 영역을 완전히 포함해야 합니다. 출입 통제 영역이 검증 영역을 조금이라도 벗어나면 저장할 수 없습니다.
- 이벤트 진입 라인은 출입 통제 영역 밖까지 늘릴 수 있지만, 검증 영역 밖으로는 설정할 수 없습니다.
- 설정한 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
- 추가한 출입 통제 영역을 삭제하려면 버튼을 클릭하세요.

4 얼굴 영역 설정(선택 사항)

얼굴을 감지할 영역을 설정하세요. 설정하면 해당 영역에서 얼굴을 우선 추적하여 사용자를 식별합니다. 출입문으로 다가오는 사람의

얼굴이 정면으로 잘 보이는 위치에 설정하세요. 얼굴 영역과 출입 통제 영역은 겹쳐서 설정할 수 있습니다. **+ 추가** 버튼을 클릭해 최대 10개까지 설정할 수 있습니다. 라이브 뷰에 파란색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



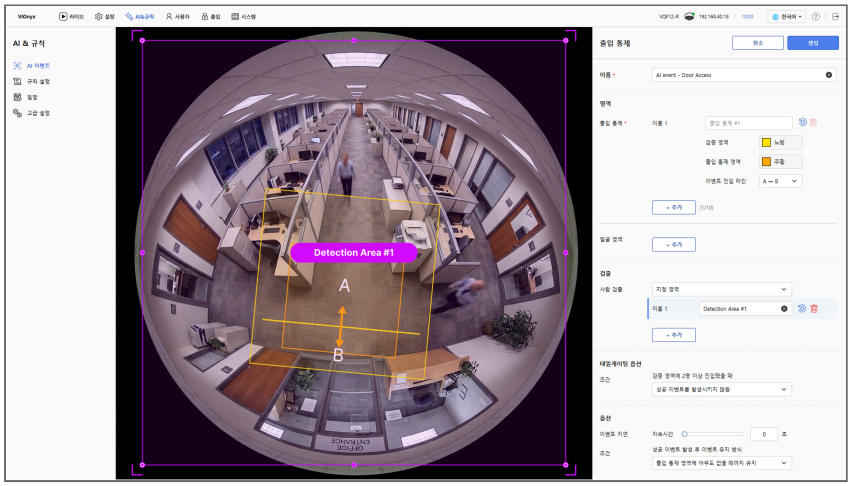
- **이름**: 얼굴 영역의 이름을 수정할 수 있습니다. 알기 쉽게 이름을 지정하세요. 얼굴 영역의 이름은 라이브 뷰에서 마우스 오버 시 표시됩니다.

> **알아두기**
>
> - 등록된 사용자는 **라이브** 메뉴에서 신원을 자동 인식해 이름이 표시됩니다. 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다.
> - 설정한 얼굴 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 얼굴 영역을 삭제하려면 버튼을 클릭하세요.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 사람이 실제로 서 있거나 지나가면서 얼굴이 잘 보이는 위치가 얼굴 영역에 포함되도록 설정하세요.

5 사람 검출 설정(선택 사항)

검출 섹션에서 카메라가 사람을 검출할 범위를 선택할 수 있습니다. 검출 범위를 필요한 곳으로 좁히면 관심 없는 구역(통로 끝, 창문, 반사면 등)에서 사람을 잘못 검출하는 일을 줄일 수 있습니다.

- **전체 영역**: 기본값으로, 화면 전체에서 사람을 검출합니다. 얼굴 영역 설정 여부와 관계없이 사용할 수 있습니다.
- **지정 영역**: 직접 지정한 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정하지 않았을 때만 선택할 수 있습니다. 최소 1개를 설정해야 하며, **+ 추가** 버튼을 클릭해 최대 10개까지 추가할 수 있습니다. 라이브 뷰에 보라색 상자가 표시되며, 마우스로 모서리 또는 점을 드래그하여 원하는 형태로 조정할 수 있습니다. 가운데 영역을 드래그하여 위치를 이동할 수도 있습니다.



  - **이름**: 사람 검출 영역의 이름을 수정할 수 있습니다.

- **얼굴 영역만**: 얼굴 영역 안에서만 사람을 검출합니다. 얼굴 영역을 설정했을 때만 선택할 수 있습니다.

> **알아두기**
>
> - **지정 영역**을 선택한 상태에서 얼굴 영역을 추가하면 **알림** 팝업이 나타납니다. **확인** 버튼을 클릭하면 지정한 검출 영역이 해제되고 **얼굴 영역만**으로 변경됩니다.
> - **얼굴 영역만**을 선택한 상태에서 얼굴 영역을 모두 삭제하면 **전체 영역**으로 자동 변경됩니다.
> - 카메라 설정에서 **적응형 자동 노출** 옵션을 사용한다면 디스플레이 화면, 사진, 포스터처럼 사람 모습이 있는 물체가 검출 범위에 포함되지 않도록 **지정 영역** 또는 **얼굴 영역만**으로 범위를 좁히세요.
> - 설정한 사람 검출 영역의 모양과 크기를 초기화하려면 버튼을 클릭하세요.
> - 추가한 사람 검출 영역을 삭제하려면 버튼을 클릭하세요.
> - 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.

6 테일게이팅 옵션 설정

테일게이팅 옵션 섹션에서 검증 영역에 2명 이상 있을 때 출입을 어떻게 판단할지 선택하세요. 보안 수준이 높은 옵션부터 순서대로 나열했습니다.

- **성공 이벤트를 발생시키지 않음**: 검증 영역에 2명 이상 있으면 식별 결과와 관계없이 출입을 허용하지 않습니다. 한 번에 한 명씩만 출입해야 하는 곳에 적합합니다.
- **전원이 유효하게 식별된 경우에만 성공**: 검증 영역에 있는 모든 사람이 등록된 사용자로 식별되어야 출입을 허용합니다. 한 명이라도 미식별 상태이면 출입을 허용하지 않습니다.
- **1명 이상 유효하게 식별되면 성공**: 검증 영역에 등록된 사용자가 한 명 이상 있으면 출입을 허용합니다. 미식별자가 함께 있어도 출입을 허용하므로 방문객 동행이 잦은 곳에 적합합니다.
- **이벤트 판정에 영향 없음**: 검증 영역의 인원수를 고려하지 않고, 출입 통제 영역에 들어온 사람의 식별 결과만으로 출입 허용 여부를 판단합니다.

다음은 출입 통제 영역에 등록된 사용자가 있고, 검증 영역에 다른 사람이 함께 있을 때 옵션별 판단 결과입니다.

옵션	출입 권한이 유효한 사용자만 있을 때	출입 권한이 유효하지 않은 사용자가 섞여 있을 때
성공 이벤트를 발생시키지 않음	출입 거부	출입 거부
전원이 유효하게 식별된 경우에만 성공	출입 허용	출입 거부
1명 이상 유효하게 식별되면 성공	출입 허용	출입 허용
이벤트 판정에 영향 없음	출입 허용	출입 허용

팁
보안이 중요한 출입문에는 **전원이 유효하게 식별된 경우에만 성공** 이상의 옵션을 사용하세요.

7 이벤트 발생 조건 설정

옵션 섹션에서 이벤트 발생 조건을 설정하세요.

- **이벤트 지연**: 이벤트로 인식할 최소 시간을 설정하세요. 감지 상태가 설정한 시간보다 오래 이어져야 이벤트가 발생합니다. 최대 60초까지 설정할 수 있습니다.

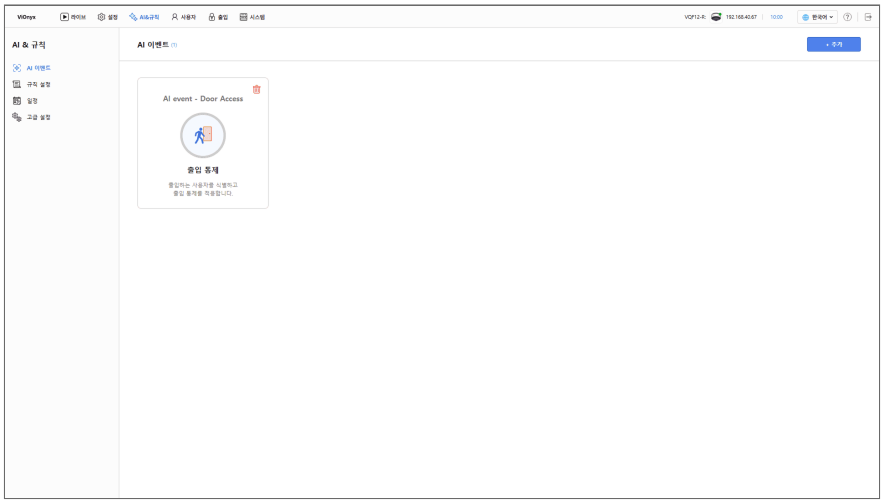
  출입문 앞을 잠시 지나가는 사람 때문에 이벤트가 자주 발생하면 **이벤트 지연** 값을 늘리세요. 설정한 시간보다 짧게 감지된 움직임은 이벤트로 인식하지 않으므로 불필요한 이벤트가 줄어듭니다.

- **조건**: 출입이 허용된 후 이벤트를 언제까지 유지할지 선택하세요. 이벤트가 유지되는 동안 연동한 동작(예: 출입문 개방)도 유지됩니다.
  - **출입 통제 영역에 아무도 없을 때까지 유지**: 출입 통제 영역에 아무도 없을 때까지 이벤트를 유지합니다. 인증된 사용자가 출입문 앞에 머무는 동안 다시 인증하지 않아도 출입문이 열린 상태로 유지됩니다.
  - **무인 또는 테일게이팅 조건 위반 시 즉시 해제**: 출입 통제 영역에 아무도 없거나, 미인가자가 검증 영역에 들어와 테일게이팅 옵션 조건을 위반하면 즉시 이벤트를 해제합니다. 출입문이 열린 사이에 미인가자가 따라 들어오는 것을 막을 수 있습니다.
  - **유지 없이 진입 기준 1회 발생**: 이벤트를 유지하지 않고, 출입 통제 영역에 들어올 때마다 한 번만 이벤트를 발생시킵니다.

알아두기
등록된 사용자가 출입문 앞에서 머뭇거리다 들어가지 못하면, 출입 통제 영역에서 나갔다가 다시 들어와야 출입문이 열립니다. 이런 불편을 줄이면서 보안도 유지하려면 **무인 또는 테일게이팅 조건 위반 시 즉시 해제**을 선택하세요.

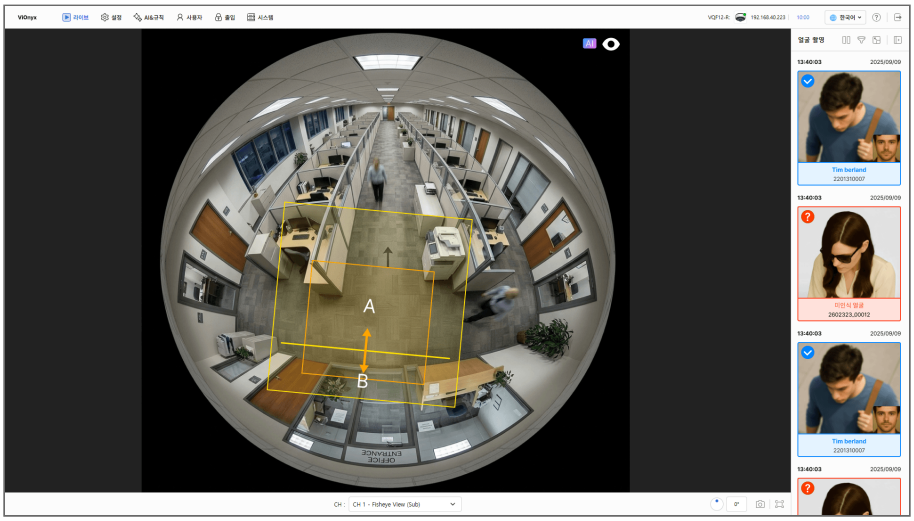
8 설정 저장

모든 설정을 완료한 후 오른쪽 상단의 **생성** 버튼을 클릭하세요. 이전 화면으로 돌아가며, 새로 생성된 AI 이벤트가 목록에 추가됩니다.



라이브에서 확인

화면 왼쪽 상단의 **라이브** 메뉴를 클릭하세요. 카메라 영상의 오른쪽 상단의 AI 아이콘이 켜져 있는지 확인하세요. 설정한 검증 영역, 출입 통제 영역, 이벤트 진입 라인과 얼굴 영역이 영상에 오버레이로 표시됩니다. 사람이 출입 통제 영역에 들어오면 식별 결과와 테일게이팅 옵션에 따라 출입 허용 또는 출입 거부 이벤트가 발생합니다.



알아두기

- 등록되지 않은 사용자는 **미등록 얼굴**로 표시됩니다. 등록된 사용자는 이름과 함께 표시합니다.
- 조명이 부족하거나 역광이 있으면 카메라가 얼굴을 인식하지 못할 수 있습니다. 촬영 공간의 조명을 개선하거나 카메라의 위치와 각도를 조정하여 얼굴이 잘 보이도록 하세요.
- 얼굴이 카메라로 향해야 인식됩니다. 옆모습 또는 뒷모습은 인식이 어려울 수 있습니다. 얼굴을 인식하지 못한 사람은 미식별 상태로 처리되어 출입이 거부됩니다.

다음 단계

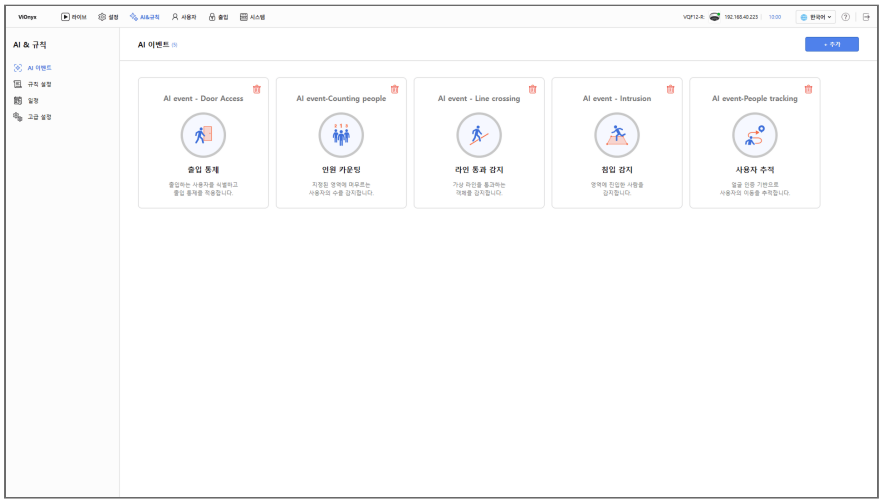
출입 통제 이벤트는 출입 허용 여부만 판단합니다. 판단 결과에 따라 음성 안내, 웹훅 알림, 비상등 같은 추가 동작을 실행하려면 출입문 규칙을 설정하세요.
출입 통제 이벤트를 생성했다면 출입문을 등록하고 이벤트를 연결하세요. 출입이 허용되면 출입문에 연결된 릴레이가 동작하여 출입문이 열립니다.

AI 이벤트 수정 및 삭제하기

생성한 AI 이벤트의 설정을 수정하거나 더 이상 필요하지 않은 이벤트를 삭제할 수 있습니다.

AI 이벤트 설정 수정

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.



3. 수정하려는 AI 이벤트를 클릭하세요.
4. 오른쪽 패널에서 AI 이벤트의 설정을 수정하세요.
5. 모든 설정을 완료한 후 오른쪽 상단의 **업데이트** 버튼을 클릭하세요.

이전 화면으로 돌아가며, AI 이벤트 목록에서 수정된 이벤트를 확인할 수 있습니다.

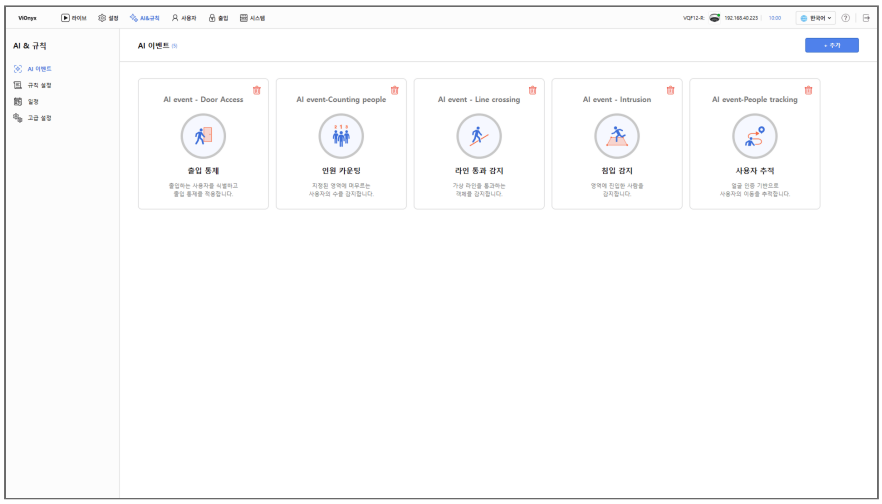
알아두기

각 이벤트 설정에 대한 자세한 내용은 다음 문서를 참조하세요.

- 사용자 추적 이벤트 설정하기
- 침입 감지 이벤트 설정하기
- 라인 통과 감지 이벤트 설정하기
- 인원 카운팅 이벤트 설정하기
- 출입 통제 이벤트 설정하기

AI 이벤트 삭제

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **AI 이벤트**를 클릭하세요.



3. 삭제하려는 AI 이벤트의 오른쪽에 있는 버튼을 클릭하세요.
4. 경고 메시지 팝업이 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.

알아두기

- 삭제한 AI 이벤트는 복구할 수 없습니다. 삭제하기 전에 AI 이벤트가 연동된 규칙(Rule)이 있다면 규칙도 함께 삭제됩니다.
- AI 이벤트 삭제 시 시스템 로그에 삭제 이벤트가 기록됩니다.

AI 규칙(Rule) 설정하기

AI 규칙을 사용하면 이벤트 유형과 조건에 따라 오디오 재생, 웹훅 전송, 릴레이 동작을 자동으로 실행할 수 있습니다. 이 문서에서는 규칙을 생성하고 운영하는 전체 절차를 안내합니다.

아래와 같은 상황에서 AI 규칙을 설정하세요.

- 특정 AI 이벤트가 발생할 때 외부 서버로 웹훅을 전송하고 싶을 때
- 특정 AI 이벤트가 발생할 때 장치에서 오디오를 재생하고 싶을 때

- 특정 AI 이벤트가 발생할 때 출입문 등에 연결된 릴레이를 동작시키고 싶을 때
- 이벤트 유형별로 다른 후속 동작을 자동화하고 싶을 때

시작하기 전에

규칙 설정을 시작하기 전에 아래 사항을 확인하세요.

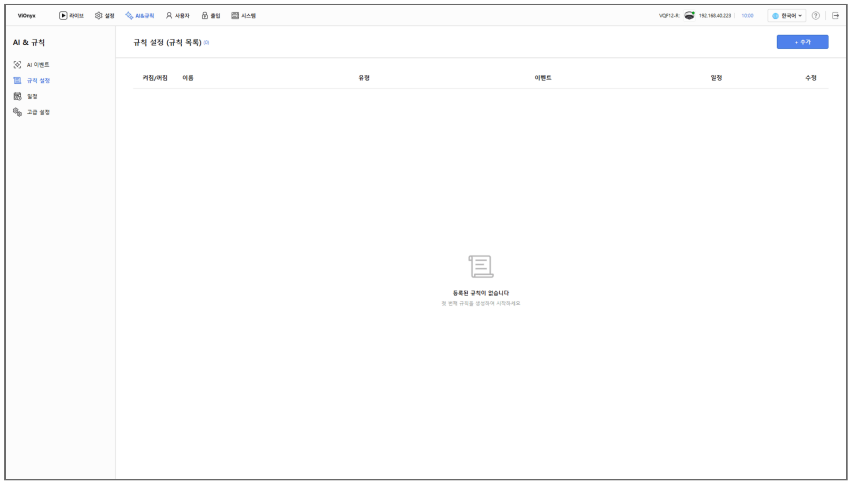
- AI 이벤트가 먼저 생성되어 있어야 합니다. 다음 문서를 참고하여 AI 이벤트를 생성하세요.
  - 사용자 추적 이벤트 설정하기
  - 침입 감지 이벤트 설정하기
  - 라인 통과 감지 이벤트 설정하기
  - 인원 카운팅 이벤트 설정하기
- 오디오를 사용할 때 재생할 오디오 클립을 미리 준비하세요.
- 웹훅을 사용할 때 수신 URL을 미리 준비하세요.
- 릴레이를 사용할 때 장치 또는 하위 장치의 릴레이 포트가 연결되어 있는지 확인하세요.
- 오디오, 웹훅, 릴레이 중 하나 이상의 동작을 설정해야 합니다.

> **알아두기**
> AI 이벤트 중 **출입 통제**는 AI 규칙의 조건으로 사용할 수 없습니다.

AI 규칙 생성

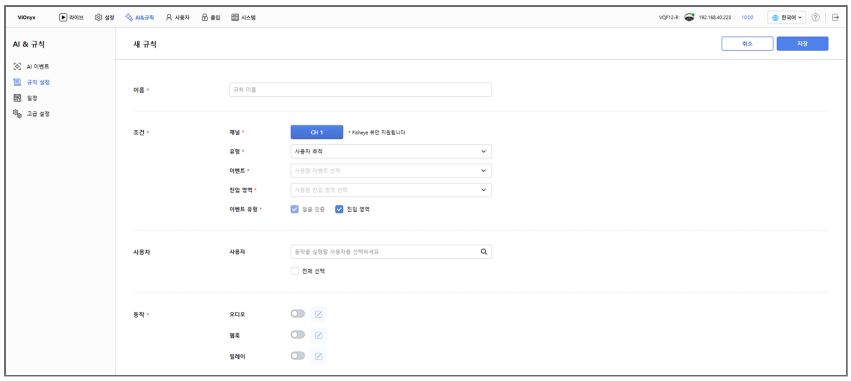
1 규칙 생성 시작

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **규칙 설정**을 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.

4. **새 규칙** 화면이 나타나면 규칙 이름을 입력하고, 조건과 동작을 설정하세요.



2 규칙 이름 입력

이름 입력 필드에 규칙 이름을 입력하세요. 규칙 이름은 필수 항목입니다. 최대 64자까지 입력할 수 있습니다.

3 조건 설정

조건은 AI 이벤트가 발생했을 때 규칙이 실행될지 결정하는 요소입니다. **조건** 섹션에서 안내에 따라 조건을 설정하세요. **유형**과 **이벤트** 옵션은 AI 이벤트 생성 시 설정한 내용에 따라 표시됩니다.

- **채널**: 채널은 CH 1로 고정되어 있습니다. Fisheye 뷰만 지원합니다.
- **유형**: AI 이벤트 유형을 선택하세요. 다음 중 하나를 선택할 수 있습니다.
  - **사용자 추적**
  - **침입 감지**
  - **라인 통과 감지**
  - **인원 카운팅**
- **이벤트**: 규칙이 실행될 AI 이벤트를 선택하세요. 이벤트 목록에는 선택한 유형에 해당하는 AI 이벤트가 표시됩니다. 이벤트 표시는 `(ID:N) event_name` 형식으로 표시됩니다.
- **진입 영역** / **침입 영역** / **라인** / **카운팅 영역**: 선택한 이벤트 유형에 따라 영역에 대한 조건을 추가할 수 있습니다.
- **이벤트 유형**: 규칙 실행 여부를 결정하는 이벤트 유형을 선택하세요. 선택한 이벤트 유형에 따라 규칙이 실행됩니다.

> 최소 1개의 이벤트 유형을 선택해야 합니다.

4 사용자 선택

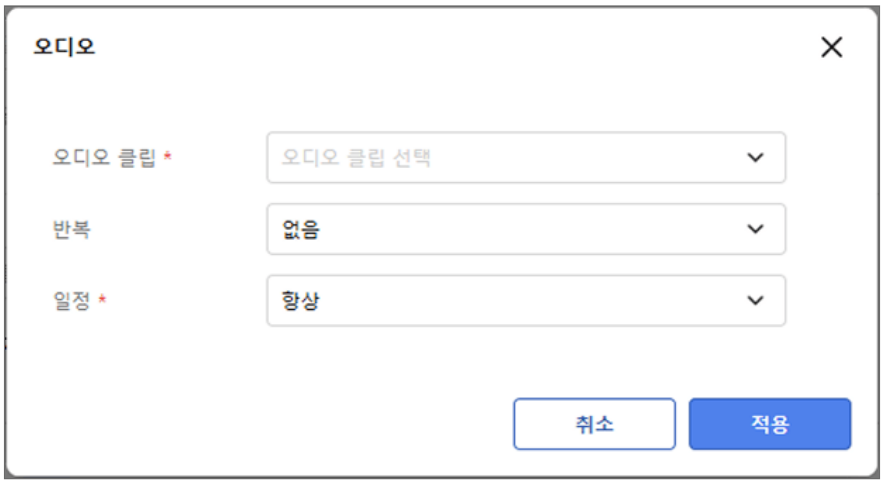
등록된 사용자 중에서 규칙 실행 여부를 결정할 사용자를 **사용자** 섹션에서 선택하세요. 선택한 사용자가 AI 이벤트에 감지되면 규칙이 실행됩니다.

- 특정 사용자를 선택하려면 **동작을 실행할 사용자를 선택하세요**를 클릭하세요. 사용자 목록이 나타나면 원하는 사용자를 선택하고 **저장** 버튼을 클릭하세요.

- 등록된 모든 사용자를 선택하려면 **전체 선택**을 클릭하세요.

5 오디오 동작 설정

오디오 동작은 AI 이벤트가 발생했을 때 카메라에서 오디오를 재생하는 기능입니다. **동작** 섹션에서 **오디오** 토글 버튼을 클릭해 동작을 활성화한 후 ✎ 버튼을 클릭하세요. 오디오 설정 팝업이 나타납니다.



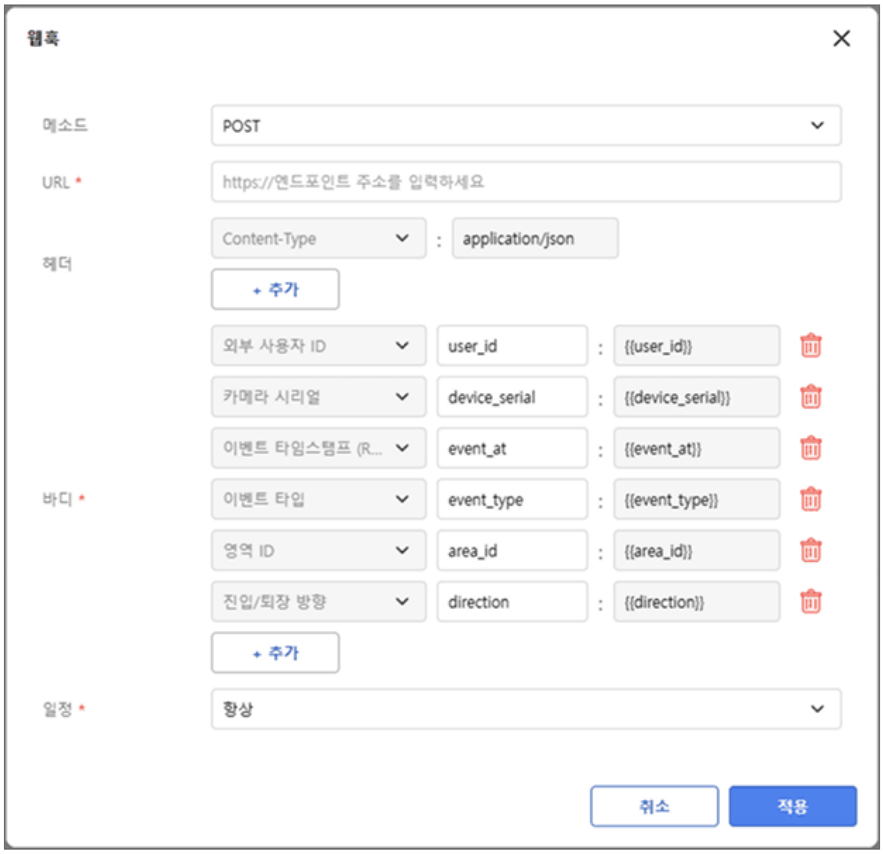
- **오디오 클립**: 재생할 오디오 클립을 선택하세요. 오디오 클립은 시스템에 업로드된 오디오 클립 목록에서 선택할 수 있습니다.
- **반복**: 오디오 재생 반복 횟수를 설정하세요. 설정한 값만큼 오디오 클립을 반복 재생합니다. 최대 10회까지 설정할 수 있습니다.
- **일정**: 규칙이 실행되고 오디오를 재생할 일정을 선택하세요.

오디오 동작 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 오디오 동작을 설정하기 전에 오디오 클립을 미리 준비해야 합니다. 오디오 클립은 **시스템** → **오디오** 메뉴에서 업로드할 수 있습니다. 자세한 내용은 오디오 클립 업로드하기를 참고하세요.
> - 일정은 **AI&규칙** → **일정**에서 생성하거나 수정, 삭제할 수 있습니다. 일정 관리에 대한 자세한 내용은 일정 관리하기를 참고하세요.

6 웹훅 동작 설정

웹훅 동작은 AI 이벤트가 발생했을 때 외부 서버로 웹훅을 전송하는 기능입니다. **동작** 섹션에서 **웹훅** 토글 버튼을 클릭해 동작을 활성화한 후 ✎ 버튼을 클릭하세요. 웹훅 설정 팝업이 나타납니다.



- **메소드**: 웹훅 전송 방식입니다. `POST` 방식만 지원합니다.
- **URL**: 웹훅을 수신할 URL을 입력하세요. `http://` 또는 `https://`로 시작하는 유효한 주소여야 합니다.
- **헤더**: 웹훅에 포함할 HTTP 헤더를 설정하세요. **+ 추가** 버튼을 클릭해 헤더를 추가할 수 있습니다. 각 헤더는 키-값 쌍으로 입력해야 합니다.
- **바디**: 웹훅에 포함할 HTTP 본문을 설정하세요. **+ 추가** 버튼을 클릭해 본문 항목을 추가할 수 있습니다. 각 본문 항목은 키-값 쌍으로 입력해야 합니다.
- **일정**: 규칙이 실행되고 웹훅을 전송할 일정을 선택하세요.

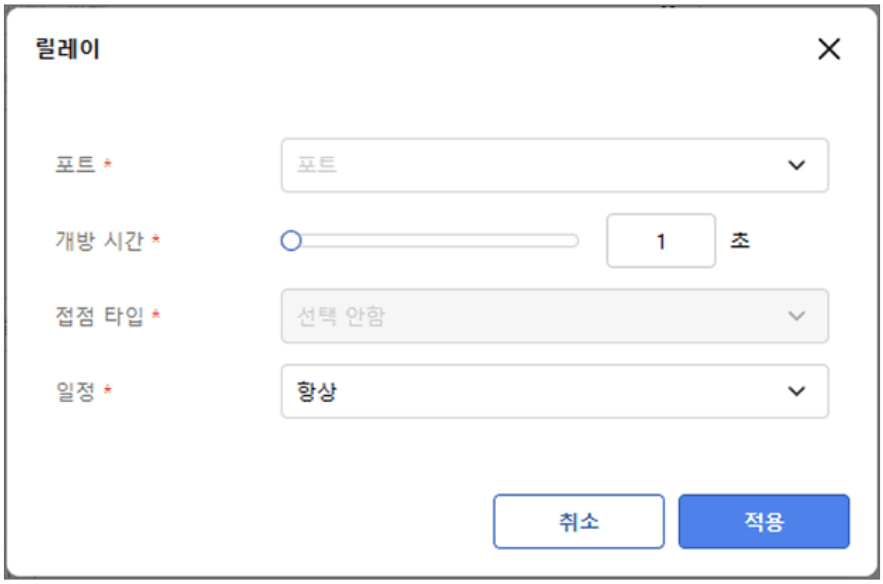
웹훅 동작 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 웹훅 발신 기록과 응답 코드는 장애 분석을 위해 시스템 로그에서 확인할 수 있습니다.
> - 일정은 **AI&규칙** → **일정**에서 생성하거나 수정, 삭제할 수 있습니다. 일정 관리에 대한 자세한 내용은 일정 관리하기를 참고하세요.

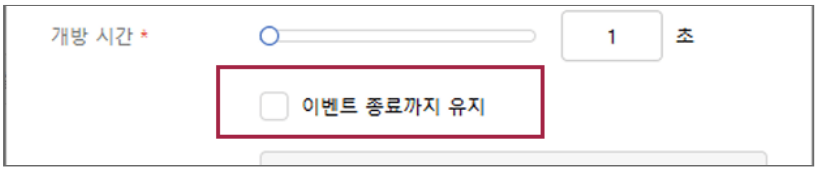
7 릴레이 동작 설정

릴레이 동작은 AI 이벤트가 발생했을 때 해당 장치 또는 하위 장치의 릴레이를 동작시키는 기능입니다. 예를 들어, 블랙 리스트 사용자에 대한 이벤트가 발생했을 때 출입문 릴레이를 동작시켜 출입을 제한할 수 있습니다.

동작 섹션에서 **릴레이** 토글 버튼을 클릭해 동작을 활성화한 후 버튼을 클릭하세요. 릴레이 설정 팝업이 나타납니다.



- **포트**: 동작시킬 릴레이 포트를 선택하세요. 장치 자체의 릴레이 포트와 장치에 연결된 하위 장치의 릴레이 포트를 선택할 수 있습니다. 다른 규칙이나 출입문에서 이미 사용 중인 포트는 목록에 사용 중으로 표시되며 선택할 수 없습니다.
- **개방 시간**: 릴레이를 개방 상태로 유지할 시간을 설정하세요. 슬라이더를 움직이거나 입력 필드에 값을 직접 입력할 수 있습니다. 1초부터 120초까지 설정할 수 있습니다.
  - **이벤트 종료까지 유지**: 조건의 **유형**을 **인원 카운팅**으로 선택하고 **카운트 제한**으로 설정된 영역을 조건으로 지정하면 **이벤트 종료까지 유지** 옵션을 사용할 수 있습니다. 이 옵션을 선택하면 개방 시간과 관계없이 카운트 제한 이벤트가 해소될 때까지 릴레이가 개방 상태로 유지됩니다.



- **접점 타입**: 릴레이의 접점 타입을 선택하세요. 릴레이 포트를 선택하면 설정할 수 있습니다. 기본값은 **Normal Close (N/C)**입니다.
  - **Normal Open (N/O)**: 평상시 열려 있다가 릴레이가 동작하면 닫히는 접점입니다.
  - **Normal Close (N/C)**: 평상시 닫혀 있다가 릴레이가 동작하면 열리는 접점입니다.
- **일정**: 규칙이 실행되고 릴레이를 동작시킬 일정을 선택하세요.

릴레이 동작 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **주의**
> **접점 타입**은 규칙이 아니라 릴레이 포트에 적용되는 설정입니다. **접점 타입**을 변경하면 해당 포트를 사용하는 모든 규칙과 출입문에 즉시 적용됩니다. 포트가 고정 잠금 또는 고정 잠금 해제 상태일 때 **접점 타입**을 변경하면 출력이 반전되어 잠긴 문이 열릴 수 있으니 주의하세요.

알아두기

- 이 기능은 펌웨어 버전 1.1.0 이상에서 지원합니다.
- 일정은 **AI&규칙** → **일정**에서 생성하거나 수정, 삭제할 수 있습니다. 일정 관리에 대한 자세한 내용은 일정 관리하기를 참고하세요.

8 규칙 저장

규칙 설정을 모두 완료하고 규칙을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요. 저장된 규칙은 규칙 목록에서 확인할 수 있습니다. 규칙 목록에서는 규칙 이름, 유형, 이벤트, 일정을 확인할 수 있습니다.



AI 규칙 활성화/비활성화

규칙 목록에서 각 규칙 항목 가장 왼쪽의 토글 버튼을 클릭하면, 해당 규칙을 활성화하거나 비활성화할 수 있습니다. 활성화된 규칙은 AI 이벤트가 발생했을 때 설정된 동작이 실행됩니다. 비활성화된 규칙은 AI 이벤트가 발생해도 동작이 실행되지 않습니다.

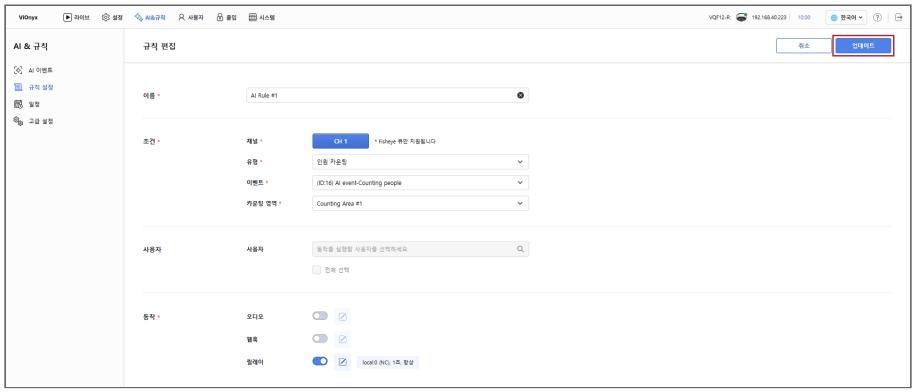


알아두기

규칙 목록에서 활성화 여부를 한눈에 구분할 수 있습니다. 파란색 토글로 표시된 규칙은 활성화 상태이고, 회색 토글로 표시된 규칙은 비활성화 상태입니다.

AI 규칙 수정

규칙 목록에서 각 규칙 항목을 클릭하면 규칙 세부 정보를 확인하거나 편집할 수 있습니다. 규칙 세부 정보 화면에서 조건과 동작을 수정한 후, 변경 사항을 저장하려면 **업데이트** 버튼을 클릭하세요.



AI 규칙 삭제

규칙 목록에서 각 규칙 항목 가장 오른쪽의  버튼을 클릭하면 해당 규칙을 삭제할 수 있습니다. 삭제된 규칙은 복구할 수 없습니다.



일정 관리하기

일정은 요일과 시간대를 조합해 만든 주간 시간표입니다. 일정을 만들어 AI 규칙의 동작에 지정하면, 해당 동작은 일정에 포함된 시간대에만 실행됩니다. 한 번 만든 일정은 여러 AI 규칙에서 함께 사용할 수 있습니다.

아래와 같은 상황에서 일정을 만드세요.

- 평일 업무 시간에만 웹훅을 전송하고 싶을 때
- 야간에만 침입 감지 경고 오디오를 재생하고 싶을 때
- 주말에는 릴레이가 동작하지 않도록 제한하고 싶을 때

> **알아두기**
> 장치에는 **Always** 일정을 기본 제공합니다. Always 일정은 매일 24시간 동작하며, 수정하거나 삭제할 수 없습니다.

일정 목록 확인

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **일정**을 클릭하세요.



일정 목록에서 등록된 일정과 각 일정을 사용하는 AI 규칙을 확인할 수 있습니다.

- 화면 상단의 **일정**(1) 옆에는 등록된 일정의 개수가 표시됩니다.
- 특정 일정을 찾으려면 검색 필드(2)에 일정 이름 또는 ID를 입력하세요.
- 한 페이지에 표시할 일정 개수를 변경하려면 화면 오른쪽 상단의 행 수 목록(3)에서 원하는 값을 선택하세요.
- 정렬 기준을 변경하려면 **이름순 정렬**(4) 목록에서 원하는 기준을 선택하세요.

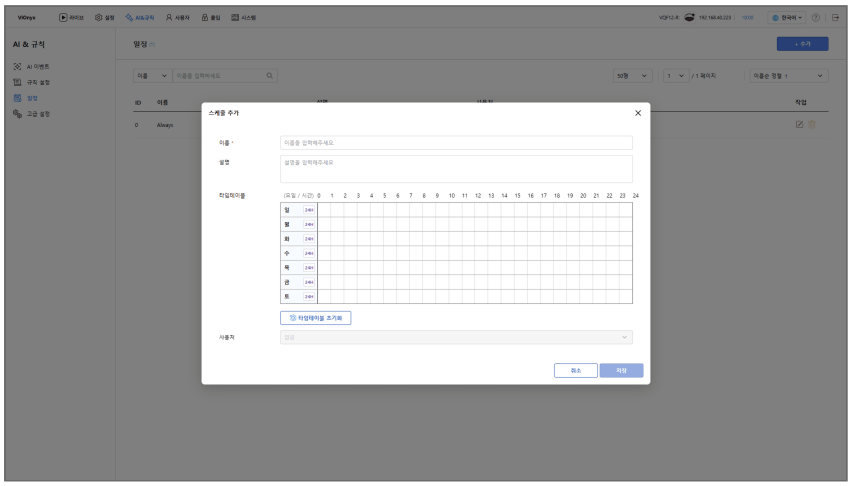
일정 목록에 표시되는 항목은 다음과 같습니다.

항목	설명
ID	일정의 고유 번호입니다. Always 일정은 `0` 입니다.
이름	일정 이름입니다.
설명	일정을 추가하거나 수정할 때 입력한 설명입니다.
사용처	일정을 사용하는 AI 규칙입니다. 사용하는 AI 규칙이 없으면 **없음**으로 표시됩니다. AI 규칙이 여러 개일 때는 **외 {count}건** 형식으로 표시됩니다.
작업	일정을 수정( )하거나 삭제( )할 수 있는 기능을 제공합니다.

일정 추가

1 일정 추가 시작

1. 일정 목록 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
2. **스케줄 추가** 팝업이 나타나면 일정 정보를 입력하세요.

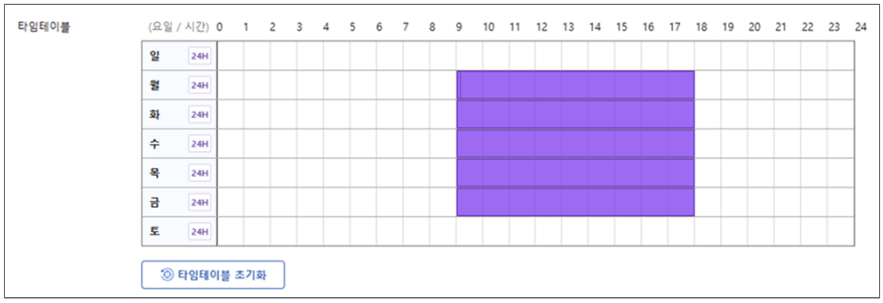


2 이름과 설명 입력

- **이름**: 일정 이름을 입력하세요. 필수 항목이며, 다른 일정과 같은 이름을 사용할 수 없습니다. 최대 48자까지 입력할 수 있습니다.
- **설명**: 일정에 대한 설명을 입력하세요. 예를 들어 **월-금 09:00-18:00**처럼 적용 시간대를 적어 두면 규칙에서 일정을 선택할 때 쉽게 구분할 수 있습니다.

3 타임테이블에서 시간대 지정

타임테이블에서 일정이 동작할 요일과 시간대를 선택하세요. 세로축은 요일(일요일~토요일), 가로축은 시간(0시~24시)입니다. 선택한 시간대는 블록으로 표시됩니다.



- **시간대 선택**: 원하는 요일 행에서 시작 시간부터 종료 시간까지 마우스로 드래그하세요. 최소 10분 단위로 선택할 수 있습니다.
- **시간대 이동**: 지정한 블록을 왼쪽 또는 오른쪽으로 드래그하면 다른 시간대로 이동할 수 있습니다.
- **24시간 선택 또는 해제**: 요일 이름 옆의 **24H** 버튼을 클릭하세요. 해당 요일의 24시간 전체가 선택되며, 다시 클릭하면 전체 해제됩니다.
- **블록 삭제**: 삭제하려는 블록을 선택하면 ✕ 버튼이 나타납니다. 이 버튼을 클릭하세요.



- **전체 초기화**: 지정한 시간대를 모두 지우고 다시 설정하려면 **타임테이블 초기화** 버튼을 클릭하세요.

4 일정 저장

모든 설정을 완료한 후 **저장** 버튼을 클릭하세요. 저장한 일정은 일정 목록에 추가되며, AI 규칙의 동작 설정에서 선택할 수 있습니다.

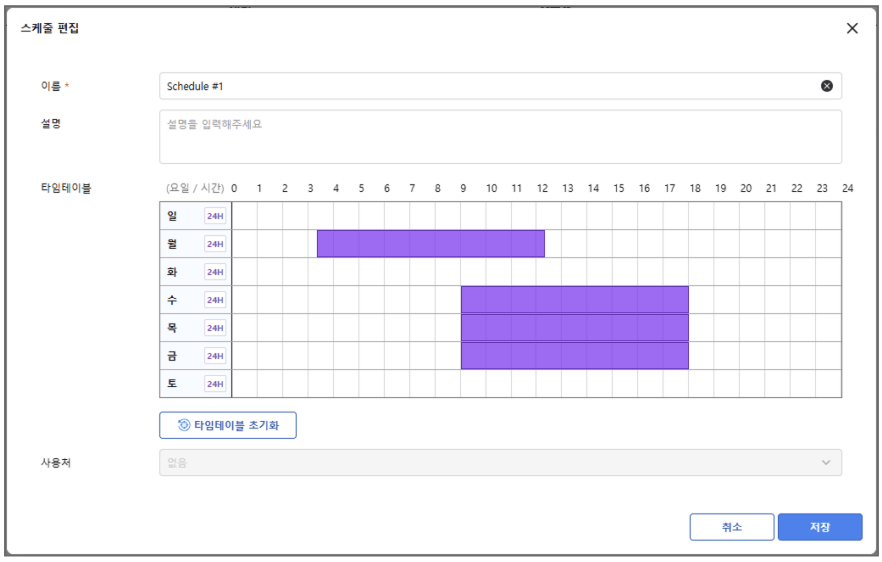
> **알아두기**
>
> - **사용처** 항목은 일정을 사용하는 AI 규칙을 보여 주는 읽기 전용 항목입니다. 새로 만든 일정은 아직 사용하는 AI 규칙이 없으므로 **없음**으로 표시됩니다.
> - 저장한 일정을 AI 규칙에 적용하는 방법은 AI 규칙(Rule) 설정하기를 참고하세요.

일정 수정

1. 일정 목록에서 수정하려는 일정의 오른쪽에 있는 ✎ 버튼을 클릭하세요.



2. **스케줄 편집** 팝업이 나타나면 이름, 설명, 타임테이블을 수정하세요.



3. 수정한 내용을 저장하려면 **저장** 버튼을 클릭하세요.

수정한 일정은 저장하는 즉시 해당 일정을 사용하는 모든 AI 규칙에 적용됩니다.

> **알아두기**
>
> - 일정을 여러 AI 규칙에서 함께 사용할 때는 수정하기 전에 **사용처** 열에서 영향을 받는 AI 규칙을 먼저 확인하세요.
> - Always 일정은 기본 일정으로 수정할 수 없습니다.

일정 삭제

1. 일정 목록에서 삭제하려는 일정의 오른쪽에 있는 버튼을 클릭하세요.



2. 확인 메시지가 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.

삭제한 일정은 복구할 수 없습니다.

> **알아두기**
>
> - AI 규칙에서 사용 중인 일정은 삭제할 수 없습니다. **사용처** 열에 표시된 AI 규칙에서 다른 일정을 선택한 후 다시 삭제하세요.
> - Always 일정은 기본 일정으로 삭제할 수 없습니다.

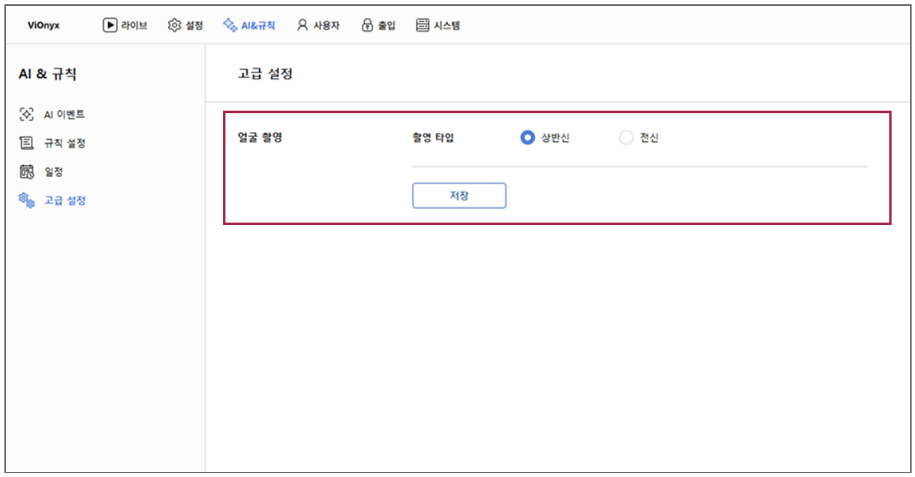
고급 설정하기

고급 설정에서는 얼굴 촬영 타입을 설정하고, 얼굴 인식 시 사용자 자동 등록 및 등록된 사용자의 보존 정책을 관리할 수 있습니다.

얼굴 촬영 타입 설정

얼굴 촬영 타입을 상반신만 촬영할지, 전신까지 촬영할지 설정할 수 있습니다.

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **고급 설정**을 클릭하세요.
3. **촬영 타입** 옵션에서 원하는 촬영 타입을 선택하고, **저장** 버튼을 클릭하세요.



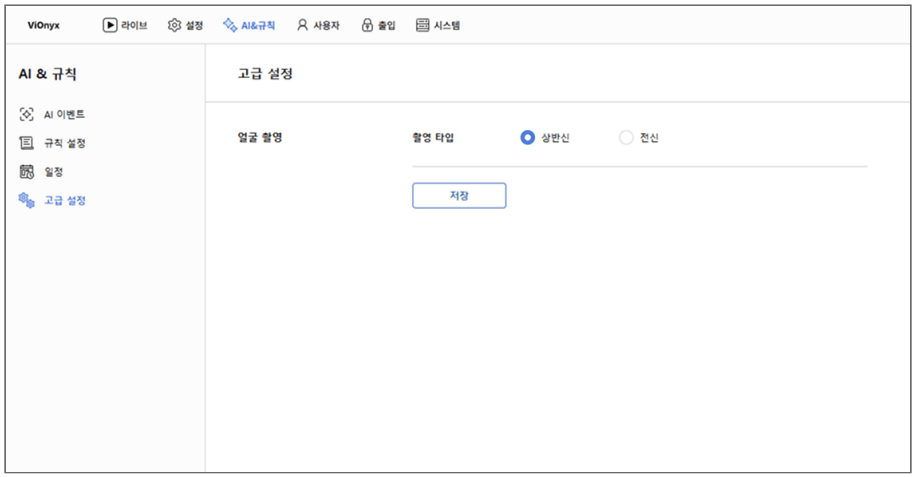
자동 사용자 등록 설정

AI 이벤트를 통해 감지된 얼굴을 사용자로 자동 등록할 수 있습니다. 수동 등록 모드로 기본 설정되어 있으며, 필요에 따라 자동 등록 모드로 전환할 수 있습니다.

> **알아두기**
> 자동 등록된 사용자도 사용자 이름, 설명 등의 정보를 수동으로 편집하고 수정할 수 있습니다. 사용자 정보 수정에 대한 자세한 내용은 사용자 수정 및 삭제하기를 참고하세요.

자동 등록 모드 활성화

1. 화면 왼쪽 상단의 **AI&규칙** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **고급 설정**을 클릭하세요.
3. **자동 사용자 등록** 섹션에서 토글 버튼을 클릭해 자동 등록 모드를 활성화하세요.



다음 안내에 따라 각 옵션을 설정하고 **저장** 버튼을 클릭해 저장하세요.

> **알아두기**
> **자동 사용자 등록** 모드 사용 시, 저품질 사진(흐림, 마스크, 측면 얼굴 등)으로 등록된 사용자는 오인증이 발생할 수 있습니다.

자동 등록 사용자 수 설정

자동 등록 사용자 수 옵션에서 자동으로 등록할 수 있는 사용자 수를 설정할 수 있습니다. 슬라이더를 드래그하거나 입력 필드에 숫자를 직접 입력하세요.

- 기본값은 50,000명이며, 최대 100,000명까지 설정할 수 있습니다.
- 자동 등록 사용자 수 설정 시 수동 등록 사용자도 설정한 수량 내에서만 등록할 수 있습니다. 예를 들어, 설정 사용자 수가 50,000명이면, 자동 등록 사용자 수와 수동 등록 사용자 수를 합산하여 최대 50,000명까지만 등록할 수 있습니다.

> **알아두기**
> - 수동으로 등록된 사용자가 있다면 자동 등록 사용자 수를 늘릴 수 없습니다.
> - 자동 등록 사용자 수를 줄이면 초과 분량의 사용자가 가장 오래된 순서부터 자동 삭제됩니다.

보존 처리 방식 설정

보존 처리 방식 옵션에서 자동으로 등록된 사용자의 보존 처리 방식을 설정할 수 있습니다. 사용자 수 한계에 도달했을 때 자동 등록된 사용자의 삭제 방식을 선택하세요.

- **가장 오래된 항목 삭제**: 할당된 사용자 수를 초과하면 가장 오래 등록된 사용자부터 자동 삭제합니다.

보존 기간 설정

보존 기간 (일) 옵션에서는 자동으로 등록된 사용자의 보존 기간을 일 단위로 설정할 수 있습니다. 보존 기간이 만료되면 가장 오래 등록된 사용자부터 자동 삭제됩니다.

- **비활성화** (기본값): 할당된 사용자 수를 초과하면 가장 오래 등록된 사용자부터 자동 삭제합니다.
- **1일**, **3일**, **7일**, **14일**, **30일**, **90일**, **365일**: 선택한 기간 경과 후 자동 등록된 사용자를 자동 삭제합니다.

> **알아두기**
> 보존 기간을 설정하면 사용자 수 한계에 도달했을 때, 기간 종료를 기다리지 않고 즉시 오래된 사용자부터 삭제합니다.

자동 등록 사용자 확인 및 관리

사용자 메뉴에서 확인

자동 등록된 사용자는 **사용자** 메뉴의 사용자 목록에서 확인할 수 있습니다.

- 사용자 아이디는 얼굴 인식 순서대로 순차적으로 자동 부여됩니다.
- **설명** 컬럼에 **자동 등록**으로 표시되어 수동 등록 사용자와 구분할 수 있습니다.
- **최종 업데이트** 컬럼에 사용자가 등록된 날짜 및 시간이 표시됩니다.

사용자 상세 정보 수정

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 자동 등록된 사용자를 클릭하세요.
3. 사용자 상세 정보 팝업이 나타나면 필요한 정보를 수정하세요.
4. 사용자 정보 수정을 완료하면 **적용** 버튼을 클릭하세요.

얼굴 인증 로그 및 얼굴 촬영 보기

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 자동 등록된 사용자를 클릭하세요.
3. 사용자 상세 정보 팝업이 나타나면 **이벤트 로그** 섹션에서 얼굴 인증 로그를 조회할 수 있습니다.

- 날짜를 선택하여 특정 기간의 얼굴 인증 로그를 조회할 수 있습니다.
- 로그의 **얼굴 촬영**을 클릭하면 해당 인증 시점의 얼굴 사진이 표시됩니다.

카메라 설정하기

카메라를 설치한 후에는 설치 환경과 운영 목적에 맞게 카메라를 설정하세요. 이 섹션에서는 영상 품질과 개인정보 보호, 시간과 네트워크 구성, 외부 장치 및 시스템 연동에 필요한 설정 방법을 안내합니다. 필요한 설정 항목을 아래에서 선택하세요.

비디오 프로필 설정하기

라이브 화면에 표시되는 영상 품질과 저장되는 녹화 영상의 품질은 비디오 프로필 설정에 따라 달라집니다. 비디오 프로필 설정에서는 채널별로 뷰 모드와 스트림 인코딩 값을 조정할 수 있습니다. 또한, 설치 환경에 따라 좌우 반전(Mirror) 설정과 채널 설정 초기화 기능도 제공합니다.

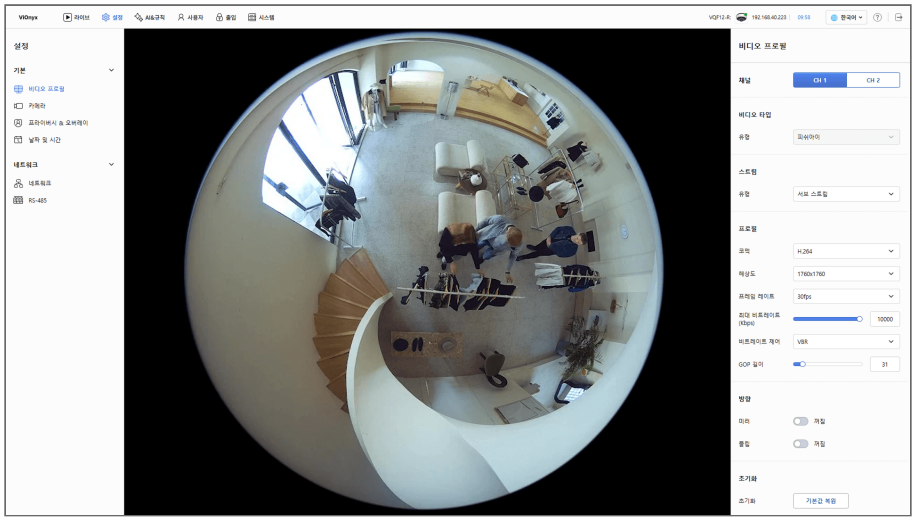
아래와 같은 상황에서 비디오 프로필을 설정해 최적의 영상 품질과 저장 용량, 네트워크 대역폭 균형을 맞추세요.

- 저장 용량과 화질 균형을 맞추고 싶을 때
- 네트워크 대역폭에 맞춰 Main/Sub 스트림을 분리해 운영하고 싶을 때
- 채널별 뷰 모드를 목적에 맞게 사용하고 싶을 때

> **알아두기**
> AI 이벤트를 이미 운영 중이라면, 좌우 반전 또는 초기화 시 AI 이벤트 설정이 삭제될 수 있습니다.

비디오 프로필 설정

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **기본** → **비디오 프로필**을 클릭하세요.



> **알아두기**
> 비디오 프로필 설정은 별도 저장 버튼 없이 변경 즉시 카메라에 반영됩니다.

채널 선택과 뷰 타입 확인

채널별 주요 목적은 다음과 같습니다.

- **CH 1**: 물리 카메라의 원본 피쉬아이 화면을 기준으로 운영하는 채널입니다.
- **CH 2**: 파노라마 또는 4분할 화면 같은 가공 뷰로 관제 효율을 높여 운영하는 채널입니다.

카메라 채널별 비디오 프로필 세부 항목을 설정할 수 있습니다.

1. 화면 오른쪽 **비디오 프로필** 패널의 **채널**에서 **CH 1** 또는 **CH 2**를 선택하세요.
2. **비디오 타입**의 **유형**에서 선택한 채널의 뷰 타입을 선택할 수 있습니다.

채널별 뷰 타입 정책은 아래와 같습니다.

- **CH 1**: 피쉬아이로 고정되어 있으며 변경할 수 없습니다.
- **CH 2**: 피쉬아이를 제외한 뷰 모드를 선택할 수 있습니다.
  - **싱글 파노라마**: 피쉬아이 카메라가 촬영한 영상을 보정하여 벽면형 파노라마 형식을 볼 수 있는 모드입니다.
  - **더블 파노라마**: 360° 영역을 촬영한 영상을 왜곡 보정하여 파노라마 형식의 상하 분할 화면으로 볼 수 있는 모드입니다.
  - **쿼드 뷰**: 사람의 시야에 적합하게 왜곡 보정한 특정 화면 4개를 동시에 볼 수 있는 모드입니다.

스트림 유형 선택

스트림에서 설정할 스트림을 선택하세요. 메인 또는 서브 스트림 중 하나를 선택하고, **프로필** 섹션에서 상세 값을 조정하세요.

- **메인 스트림**: 녹화 및 고화질 모니터링
- **서브 스트림**: 저대역폭 원격 모니터링

> **알아두기**
> **CH 2** 채널은 **메인 스트림** 유형만 지원합니다.

프로필 상세 설정

선택한 스트림 유형에 따라 코덱 및 해상도, 프레임 레이트 등 세부 설정을 조정하세요.

- **코덱**: 프로필에 적용할 코덱을 선택하세요. **H.264** 또는 **H.265**, **MJPEG** 중 하나를 선택할 수 있습니다.

  > H.265 코덱을 선택하면 Profile T가 필수로 적용됩니다.

- **해상도**: 프로필에 적용할 해상도입니다. 채널, 비디오 타입, 스트림 유형에 따라 지원하는 해상도가 다릅니다.

채널	비디오 타입	스트림 유형	지원 해상도
CH 1	**피쉬아이**	**메인 스트림**	3520 × 3520

채널	비디오 타입	스트림 유형	지원 해상도
		서브 스트림	1760 × 1760
CH 2	**싱글 파노라마**	**메인 스트림**	2048 × 512, 1920 × 480, 1280 × 320, 704 × 176
	더블 파노라마	**메인 스트림**	2048 × 2048, 1920 × 1920, 1280 × 1280, 704 × 704
	쿼드 뷰	**메인 스트림**	2048 × 2048, 1600 × 1600, 1280 × 1280, 1024 × 1024

> **CH 2** 채널은 **메인 스트림** 유형만 지원합니다.

- **프레임 레이트**: 초당 프레임 수를 설정하세요. 30, 25, 20, 15, 10 프레임 중 하나를 선택할 수 있습니다.
- **최대 비트레이트**: 영상의 최대 비트 레이트를 설정할 수 있습니다.
- **비트레이트 제어**: 영상 데이터 제어 방식을 선택하세요.
  - **VBR**: 영상의 복잡도에 따라 비트레이트가 가변하므로, 네트워크가 안정적일 때 고화질 제공합니다. 네트워크 대역폭이 충분한 환경에서 권장합니다.
  - **CBR**: 비트레이트를 고정하여 안정적인 스트리밍을 보장하지만, 복잡한 화면에서는 화질이 저하될 수 있습니다. 네트워크 대역폭이 제한적이거나 일정한 환경에서 권장합니다.
- **GOP 길이**: I-Frame 간격을 설정합니다. 1~300 사이의 값을 선택할 수 있습니다. GOV 길이가 길수록 데이터양이 감소하고, 짧을수록 증가합니다.

> **알아두기**
>
> - **가변 비트 레이트**(Variable Bitrate, VBR): 프레임의 데이터 크기를 고정하지 않고 최대 비트 레이트 내에서 영상을 전송하는 방식입니다. 영상의 복잡도에 따라 비트레이트가 가변적으로 조정되는 방식입니다. 일반적으로 고화질 영상을 제공하지만, 네트워크 대역폭이 일정하지 않은 환경에서는 영상 끊김이 발생할 수 있습니다.
> - **고정 비트 레이트**(Constant Bitrate, CBR): 프레임의 데이터 크기를 고정하여 영상을 전송하는 방식입니다. 네트워크 대역폭이 일정한 환경에서 안정적인 영상 스트리밍을 제공하지만, 영상의 복잡도에 따라 화질이 저하될 수 있습니다.
> - **GOV**(Group of Video): H.264/H.265 압축에서 I-Frame부터 다음 I-Frame 직전까지의 프레임 집합을 의미합니다. GOV 안에는 완전한 이미지 정보를 담는 I-Frame(키 프레임)과, 이전 프레임 대비 변경 정보만 담는 P-Frame이 포함됩니다. GOV 길이가 길수록 I-Frame 수가 줄어 영상 데이터양이 줄고, GOV 길이가 짧을수록 I-Frame 수가 늘어 영상 데이터양이 증가합니다.

좌우 반전 설정

카메라 설치 위치에 따라 좌우 또는 상하 반전 설정이 필요할 수 있습니다.

- **미러**: 좌우 반전 설정을 켜거나 끌 수 있습니다.
- **플립**: 상하 반전 설정을 켜거나 끌 수 있습니다.

> **알아두기**
> AI 이벤트가 설정된 상태에서는 좌우 반전 변경이 제한될 수 있습니다. 이때 안내 팝업에 따라 AI 설정을 삭제하고 진행하세요.

채널 설정 초기화

설정한 채널의 뷰 모드와 스트림 설정을 공장 초깃값으로 복원하려면, **초기화** 섹션에서 **기본값 복원** 버튼을 클릭하세요.

> **알아두기**
> - 선택한 채널만 공장 초기 설정으로 복구됩니다.
> - 피쉬아이 모드에서 AI 이벤트가 설정되어 있다면, AI 설정을 삭제하고 진행하세요.

카메라 설정 변경하기

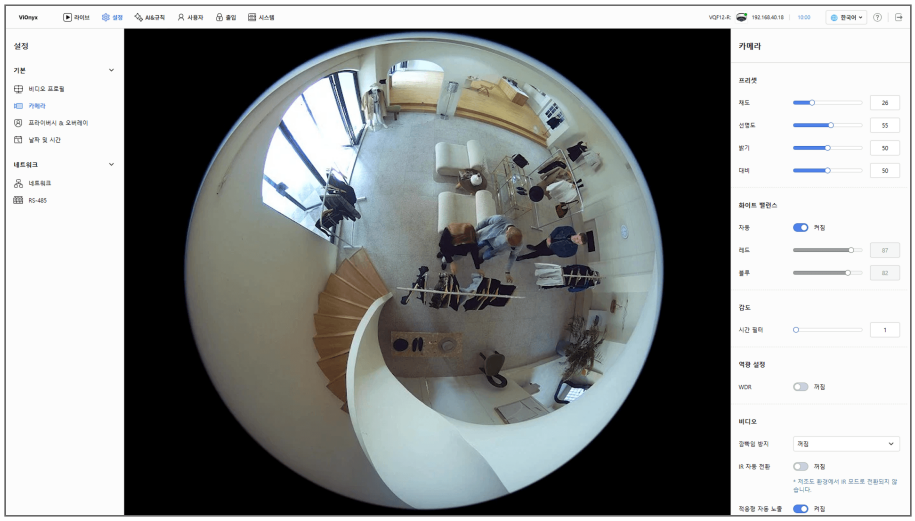
카메라가 설치된 환경에서 최적의 영상을 얻을 수 있도록 카메라 설정을 조정하세요. 설정을 변경하면 라이브 뷰에 바로 반영되므로 결과를 확인하면서 이미지 품질, 화이트 밸런스, 감도, 역광 보정 등을 조정할 수 있습니다. 또한 설치 타입(천장 또는 벽면)에 따라 사용할 수 있는 AI 기능이 달라집니다.

아래와 같은 상황에서 카메라 설정을 조정하세요.

- 촬영 환경의 밝기와 색감에 맞춰 이미지 품질을 개선하고 싶을 때
- 저조도 환경에서 노이즈를 최소화하면서 동작 감지를 유지하고 싶을 때
- 창문이나 출입문 쪽의 강한 역광 때문에 피사체가 어둡게 보일 때
- 형광등이나 LED 조명의 깜빡임을 줄이고 싶을 때
- 보조 조명이 있거나 컬러 영상이 필요해 야간 IR 전환을 막고 싶을 때
- 외광 때문에 얼굴이 너무 어둡거나 밝게 보여 얼굴 인증이 어려울 때
- 설치 위치에 따라 카메라와 AI 기능을 최적화하고 싶을 때
- 추위나 습기로 렌즈에 김이나 성에가 껴서 영상이 흐려질 때

카메라 설정

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **기본** → **카메라**를 클릭하세요.



> **알아두기**
> 카메라 설정 변경은 설정 옵션을 변경할 때마다 실시간으로 라이브 뷰에 반영되며, 변경 후 자동 저장됩니다.

이미지 품질 조정

촬영 환경에 맞춰 이미지 품질을 조정할 수 있습니다. **프리셋** 섹션의 각 슬라이더를 조절하면 미리보기 화면에 실시간으로 반영됩니다. 1에서 100 사이의 값으로 설정할 수 있습니다.

- **채도**: 색상의 선명도를 조정합니다. (기본값: 26)
- **선명도**: 이미지 경계의 선명도를 조정합니다. (기본값: 55)
- **밝기**: 이미지 전체 밝기를 조정합니다. (기본값: 50)
- **대비**: 밝은 부분과 어두운 부분의 명암 차이를 조정합니다. (기본값: 50)

> **알아두기**
> 각 설정은 슬라이더를 조작할 때마다 미리보기 화면에 즉시 반영되고, 자동으로 저장됩니다.

화이트 밸런스 설정

카메라가 촬영 환경의 조명색을 정확하게 표현하도록 화이트 밸런스를 설정하세요. **화이트 밸런스** 섹션에서 **자동** 옵션을 켜거나 끌 수 있습니다.

- **켜짐**(기본값): 카메라가 자동으로 색온도를 감지하고 조정합니다.
- **꺼짐**: **레드**와 **블루** 값을 수동으로 조정해 화이트 밸런스를 설정할 수 있습니다.

감도 설정 (Time Filter)

센서 노이즈를 줄이거나 빠른 움직임 감지 간 균형을 맞추도록 시간 필터를 조정하세요. **감도** 섹션의 **시간 필터** 슬라이더를 조절하면 노이즈 필터링 강도를 설정할 수 있습니다.

- 낮음(1~30): 노이즈 필터링이 약해져 빠르게 움직이는 객체 감지에 유리하지만, 저조도 환경에서는 노이즈가 증가할 수 있습니다.

- 중간(31~70): 균형 잡힌 필터링으로 일반적인 촬영 환경에 적합합니다.
- 높음(71~100): 노이즈 필터링이 강해져 저조도 환경에서 노이즈를 줄이는 데 유리하지만, 빠르게 움직이는 객체 감지에는 불리할 수 있습니다.

> **알아두기**
> **시간 필터**의 기본값은 1입니다.

역광 설정

카메라가 역광 환경에서 밝은 영역과 어두운 영역을 동시에 표현하도록 WDR(Wide Dynamic Range, 역광 보정)을 설정하세요. **역광 설정** 섹션에서 **WDR** 옵션을 켜면 역광 보정을 활성화할 수 있습니다. (기본값: **꺼짐**)

> **알아두기**
> **WDR**(Wide Dynamic Range) 모드는 역광 환경에서 밝은 영역과 어두운 영역을 동시에 표현할 수 있도록 카메라가 자동으로 노출을 조정하는 기능입니다. WDR 모드를 활성화하면, 밝은 영역이 과다 노출되는 것을 방지하고, 어두운 영역의 디테일을 더 잘 표현할 수 있습니다. 일반적으로 역광이 심한 환경에서 촬영할 때 유용합니다.

깜빡임 방지 설정

촬영 환경에 있는 조명과 주파수 불일치로 발생할 수 있는 화면 떨림을 줄이려면 **비디오** 섹션에서 **깜빡임 방지** 옵션을 설정하세요.

- **꺼짐**(기본값): 깜빡임 방지 기능 사용 안 함
- **50HZ**: 50Hz 형광등/LED 환경
- **60HZ**: 60Hz 형광등/LED 환경

> **알아두기**
> 촬영 환경의 조명과 주파수가 일치하는 옵션을 선택하세요. 잘못된 설정이라면 화면에 떨림이나 줄무늬가 생길 수 있습니다.

IR 자동 전환 설정

주변이 어두워질 때 카메라가 IR(야간) 모드로 자동 전환할지 설정하세요. 보조 조명이 있는 장소나 컬러 영상이 꼭 필요한 현장에서는 자동 전환을 끌 수 있습니다. **비디오** 섹션에서 **IR 자동 전환** 옵션을 켜거나 끌 수 있습니다.

- **켜짐**(기본값): 조도 센서와 영상의 밝기를 기준으로 주변이 어두워지면 IR 모드로 자동 전환합니다.
- **꺼짐**: 저조도 환경에서도 IR 모드로 전환하지 않습니다.

> **알아두기**
> **IR 자동 전환** 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

적응형 자동 노출 설정

창가처럼 외광이 강하거나 햇빛이 하루 동안 크게 바뀌는 곳에서는 얼굴이 너무 어둡거나 밝게 보여 얼굴 인증이 어려울 수 있습니다. 이럴 때 적응형 자동 노출을 사용하세요. 카메라가 얼굴이 자주 나타나는 위치를 스스로 학습하고, 그 위치의 얼굴이 알맞은 밝기로 보이도록 노출을 자동으로 조정합니다. **비디오** 섹션에서 **적응형 자동 노출** 옵션을 켜거나 끌 수 있습니다.

- **켜짐**(기본값): 얼굴 영역의 밝기를 기준으로 노출을 자동으로 조정합니다.
  - 외광이 강하거나 햇빛이 바뀌어도 얼굴 영역의 밝기를 일정하게 유지합니다.
  - 사람이 지나가거나 오래 머물러도 옷 색깔 때문에 화면 밝기가 흔들리지 않습니다.
  - 조명을 켜거나 끄면 바뀐 밝기에 맞춰 노출을 다시 조정합니다.
- **꺼짐**: 적응형 자동 노출 보정을 사용하지 않습니다. 다시 켜면 보정이 자동 동작합니다.

> **알아두기**
>
> - **적응형 자동 노출**은 AI 이벤트의 얼굴 영역과 사람 검출 범위를 기준으로 동작합니다. 영역 설정 방법은 AI 이벤트 관리하기를 참고하세요.
> - **적응형 자동 노출** 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

설치 타입 설정

카메라의 설치 위치에 따라 **설치 유형**을 설정하세요. 설치 타입에 따라 지원하는 AI 기능이 결정됩니다.

- **천장**(기본값): 천장에 설치했다면 선택하세요. 모든 AI 기능을 사용할 수 있습니다.
- **벽면**: 벽면에 설치했다면 선택하세요. 얼굴 인식 AI만 사용할 수 있으며, 객체 추적은 할 수 없습니다.

> **알아두기**
>
> - **천장에서 벽면으로 변경할 때,** 얼굴 인식만 가능하고 객체 추적 AI는 사용할 수 없다는 확인 팝업이 표시되므로 내용을 검토 후 진행하세요.
> - **벽면에서 천장으로 변경할 때,** 즉시 변경되며, 모든 AI 기능이 자동 활성화됩니다.

카메라 히터 설정

기온이 낮거나 습도가 높은 환경에서는 렌즈에 김이 서리거나 성에가 끼어 영상이 흐려지고, AI 인식 정확도가 떨어질 수 있습니다. 이럴 때 카메라 히터를 켜서 렌즈 시야를 확보하세요. **히터** 섹션에서 **히터** 옵션을 켜거나 끌 수 있습니다.

- **켜짐**: 히터가 동작합니다. 30분이 지나면 자동으로 꺼집니다.
- **꺼짐**(기본값): 히터 동작을 멈춥니다.

> **알아두기**
>
> - 히터는 과열과 불필요한 전력 소모를 막기 위해 30분 동안만 동작한 뒤 자동으로 꺼지며, 옵션도 **꺼짐**으로 변경됩니다. 히터가 꺼진 뒤에도 렌즈에 김이나 성에가 남아 있으면 옵션을 다시 켜세요.
> - **히터** 옵션은 펌웨어 버전 1.1.0 이상에서 지원합니다.

카메라 설정 초기화

모든 카메라 설정을 공장 초깃값으로 복원하려면, **초기화** 섹션에서 **기본값 복원** 버튼을 클릭하세요.

프라이버시 및 오버레이 설정하기

프라이버시 & 오버레이 설정을 사용하면 카메라 영상에 민감한 영역을 가리거나 얼굴을 자동으로 블러 처리할 수 있습니다. 또한 영상에 날짜 및 시간, 카메라 이름을 표시해 영상의 출처와 촬영 시각을 명확히 할 수 있습니다. 모든 설정은 즉시 라이브 뷰에 반영됩니다.

아래와 같은 상황에서 프라이버시 & 오버레이를 설정하세요.

- 사생활 침해가 우려되는 특정 영역을 마스킹하고 싶을 때
- 얼굴 자동 블러로 개인정보 보호 정책을 준수하고 싶을 때
- 녹화 영상에 날짜/시간을 표시해 영상 추적성을 확보하고 싶을 때
- 여러 카메라 운영 시 카메라 이름을 표시해 영상 출처를 명확히 하고 싶을 때

> **알아두기**
> 프라이버시 설정(마스킹, 얼굴 블러)은 영상 표시에만 적용되며, AI 분석은 원본 이미지를 기반으로 수행되어 AI 성능에 영향을 주지 않습니다.

프라이버시 & 오버레이 설정

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **기본** → **프라이버시 & 오버레이**를 클릭하세요.



3. 변경 사항을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

변경 사항은 저장 후 즉시 카메라에 반영됩니다.

프라이버시 영역 설정

촬영 영상에서 비공개할 특정 영역을 마스킹할 수 있습니다. 최대 10개 영역까지 설정 가능하며, 각 영역은 움직임 없이 고정됩니다.

1. **영역 설정** 섹션의 토글 버튼을 클릭하세요.
2. **+ 추가** 버튼을 클릭하세요.
3. 라이브 뷰에 마스킹할 영역이 추가됩니다. 영역의 모서리를 드래그해 크기를 조절하거나 영역 전체를 드래그해 위치를 이동할 수 있습니다.



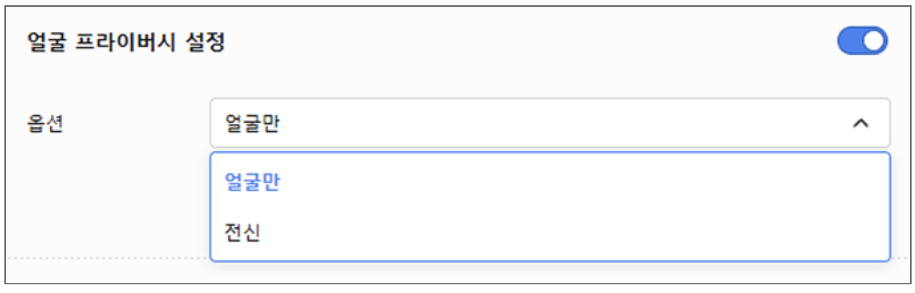
4. 마스킹 영역이 생성되면, 우측 설정 패널에서 영역 이름과 순서, 색상을 설정할 수 있습니다.
   - **이름**: 마스킹 영역 이름은 자동 생성되며, 필요에 따라 수정할 수 있습니다.
   - **순서**: 마스킹 영역이 서로 겹칠 때 표시 순서를 조정할 수 있습니다. 숫자가 클수록 위에 표시됩니다.
   - **색상**: 마스킹 영역의 색상을 선택할 수 있습니다.
5. 추가한 마스킹 영역을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

저장된 마스킹 영역은 라이브 뷰와 녹화 영상에 반영됩니다.

> **알아두기**
>
> - 마스킹된 영역은 모든 뷰 모드(피쉬아이, 싱글 파노라마, 더블 파노라마, 쿼드)에 자동 적용됩니다.
> - 마스킹 영역의 설정을 초기화하려면 버튼을 클릭하세요.
> - 마스킹 영역을 삭제하려면 버튼을 클릭하세요.

얼굴 프라이버시 설정

카메라가 감지한 얼굴 또는 전신을 자동으로 블러 처리하여 개인정보를 보호할 수 있습니다. **얼굴 프라이버시 설정** 옵션을 활성화하고 원하는 블러 처리 범위를 선택하세요.



- **얼굴만**: 감지된 모든 얼굴이 자동 블러 처리됩니다.
- **전신**: 감지된 전신이 자동 블러 처리됩니다.

> **알아두기**
> 얼굴 또는 전신이 블러 처리되어도 AI 성능에는 영향을 주지 않습니다. 카메라가 블러 처리된 영상을 표시하는 동시에, AI 분석은 원본 이미지를 기반으로 수행되므로 얼굴 인식, 객체 추적 등의 AI 기능이 정상 작동합니다.

오버레이 설정

라이브 뷰에 날짜/시간과 카메라 이름을 표시할 수 있습니다. **오버레이** 옵션을 활성화하고, **날짜 & 시간**, **카메라 이름**에서 세부 설정을 조정하세요.





> **알아두기**
> 각 설정은 변경 직후 자동 저장되어 라이브 뷰에 즉시 반영됩니다.

날짜 & 시간

라이브 뷰에 표시되는 날짜와 시간의 형식과 크기, 색상을 설정할 수 있습니다. 라이브 뷰에서 날짜/시간 위치를 확인하고, 필요하면 마우스로 드래그하여 위치나 크기를 조절하세요.

- **날짜** / **시간**: 토글 버튼을 클릭해 날짜 및 시간 오버레이를 켜거나 끌 수 있습니다.
- **날짜 형식**: 날짜 형식을 선택하세요.
  - YYYY-MM-DD (기본값, 예: 2026-01-12)
  - MM-DD-YYYY (예: 01-12-2026)
  - DD-MM-YYYY (예: 12-01-2026)
- **시간 형식**: 시간 형식을 선택하세요.
  - HH:MM:SS (기본값, 예: 13:45:56)
  - HH:MM (초 생략, 예: 13:45)

- **글자 크기**: 라이브 뷰에 표시되는 글자 크기를 선택하세요. 1부터 20까지 선택할 수 있습니다.
- **색상**: 라이브 뷰에 표시되는 글자 색상을 선택하세요.

> **알아두기**
> 날짜 및 시간 오버레이는 Fisheye View에만 표시됩니다.

카메라 이름

라이브 뷰에 카메라 이름을 표시해 영상의 출처를 명확히 할 수 있습니다. 라이브 뷰에서 카메라 이름 위치를 확인하고, 필요하면 마우스로 드래그하여 위치나 크기를 조절하세요.

- **표시**: 토글 버튼을 클릭해 카메라 이름 오버레이를 켜거나 끌 수 있습니다.
- **이름**: 카메라 이름을 입력하세요.
- **글자 크기**: 라이브 뷰에 표시되는 글자 크기를 선택하세요. 1부터 20까지 선택할 수 있습니다.
- **색상**: 라이브 뷰에 표시되는 글자 색상을 선택하세요.

설정 저장

설정한 내용은 라이브 뷰에서 바로 확인할 수 있으며, 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요. 저장된 설정은 카메라에 적용되어 라이브 뷰와 녹화 영상에 반영됩니다.

날짜와 시간 설정하기

날짜와 시간 설정을 통해 카메라의 시간을 정확하게 유지할 수 있습니다. 시간대를 선택하고 수동으로 시간을 설정하거나 NTP 서버를 통해 자동으로 시간을 동기화할 수 있습니다. 정확한 시간은 영상 타임스탬프 및 AI 이벤트 기록의 신뢰성을 보장합니다.

아래와 같은 상황에서 날짜와 시간 설정을 확인하세요.

- 카메라 설치 후 시간대를 운영 지역에 맞게 설정하고 싶을 때
- 수동으로 정확한 시간을 입력하여 카메라 시간을 동기화하고 싶을 때
- NTP 서버를 통해 장시간 정확한 시간을 자동으로 유지하고 싶을 때
- 여러 카메라의 시간을 통일하여 영상 분석 및 추적을 용이하게 하고 싶을 때

> **알아두기**
> 카메라의 시간이 부정확하면 AI 이벤트 기록, 비디오 타임스탬프, 시스템 로그의 신뢰성이 떨어질 수 있습니다. 정기적으로 시간 설정을 확인하세요.

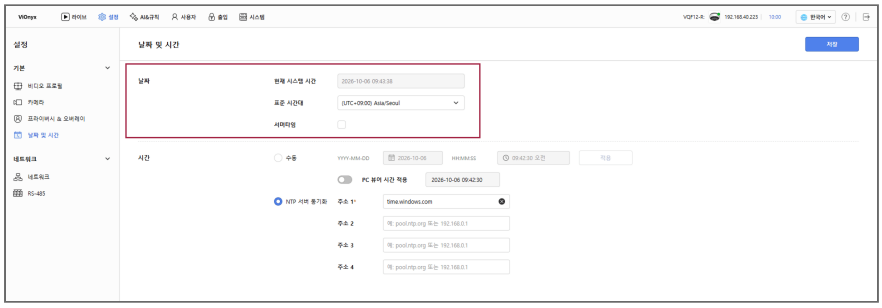
시간대 설정

먼저 카메라가 운영될 지역의 시간대를 설정하세요.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.

2. 화면 왼쪽 사이드바에서 **기본** → **날짜 및 시간**을 클릭하세요.
3. **날짜** 섹션의 **표준 시간대**에서 지역을 선택하세요.

   > *예:* `(UTC+09:00) Asia/Seoul`



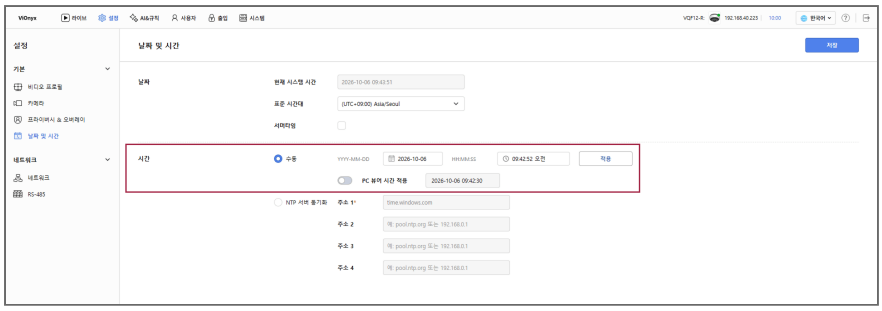
4. 시간대에 따른 서머 타임을 적용하려면 **서머타임** 옵션의 체크박스를 클릭하세요.
5. 설정한 시간대를 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

> **알아두기**
> 기본값은 `(UTC+09:00) Asia/Seoul`로 설정되어 있습니다. 운영 지역이 다르면 반드시 시간대를 변경하세요.

수동으로 시간 설정

카메라의 시간을 수동으로 설정할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **기본** → **날짜 및 시간**을 클릭하세요.
3. **시간** 섹션에서 **수동**을 선택하세요.



4. 날짜 필드에 현재 날짜를 입력하거나 달력 아이콘을 클릭해 날짜를 선택하세요.
5. 시간 필드에 현재 시각을 입력하거나 시계 아이콘을 클릭해 시간을 선택하세요.
6. 수동 시간 설정을 적용하려면 **적용** 버튼을 클릭하세요.
7. 시간 설정을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

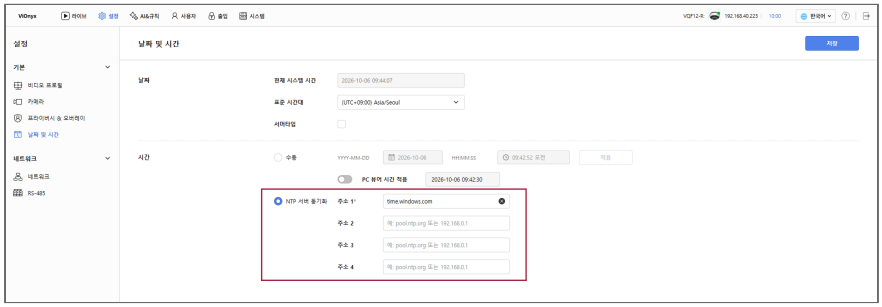
알아두기

- PC의 시간을 카메라에 자동으로 적용하려면, **PC 뷰어 시간 적용** 옵션을 활성화하세요. 웹 브라우저의 시스템 시간이 카메라에 적용됩니다.
- 수동 모드와 NTP 자동 동기화는 동시에 활성화할 수 없습니다. 수동 모드를 선택하면 NTP 자동 동기화는 비활성화됩니다.

자동 동기화 시간 설정

NTP 서버를 통해 카메라의 시간을 자동으로 정확하게 유지할 수 있습니다. 장시간 운영할 때 권장됩니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **기본** → **날짜 및 시간**을 클릭하세요.
3. **시간** 섹션에서 **NTP 서버 동기화**를 선택하세요.



4. **주소 {n}**(필수) 필드에 NTP 서버 주소를 입력하세요.
   - URL 형식: time.windows.com, time.nist.gov 등
   - IP 주소: 192.0.2.1 등
5. (선택) 필요하면 **주소 {n}**, **주소 {n}**, **주소 {n}**에 추가 NTP 서버를 입력하세요.
   - 최대 4개 서버까지 설정할 수 있습니다.
   - **주소 {n}**이 응답하지 않으면 자동으로 다음 서버로 전환됩니다.
6. 시간 설정을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

설정 완료 후 카메라는 자동으로 NTP 서버와 동기화되며, 주기적으로 시간을 갱신합니다.

알아두기

권장 NTP 서버

- time.windows.com (Windows 공용 NTP)
- time.nist.gov (NIST 공용 NTP)
- pool.ntp.org (NTP Pool 프로젝트)

네트워크 설정하기

네트워크 설정에서는 장치의 IPv4 주소, 서브넷, 게이트웨이, DNS 서버를 구성하고, 웹 UI와 실시간 영상 스트리밍에 사용되는 포트를 설정합니다. 네트워크 환경에 맞게 자동 할당(DHCP) 또는 수동 설정(Static) 중 하나를 선택하여 구성할 수 있습니다.

또한 NVR/VMS가 ONVIF로 장치에 연결할 때 사용할 프로필을 설정하고, 사용자 정보를 동기화하기 위해 외부 슈프리마 CLUe 클라우드 서비스와 연결할 수 있습니다. Cloudflare Tunnel을 사용하면 외부에서 장치의 웹 UI에 접속할 수 있습니다.

아래와 같은 상황에서 네트워크 설정을 확인하세요.

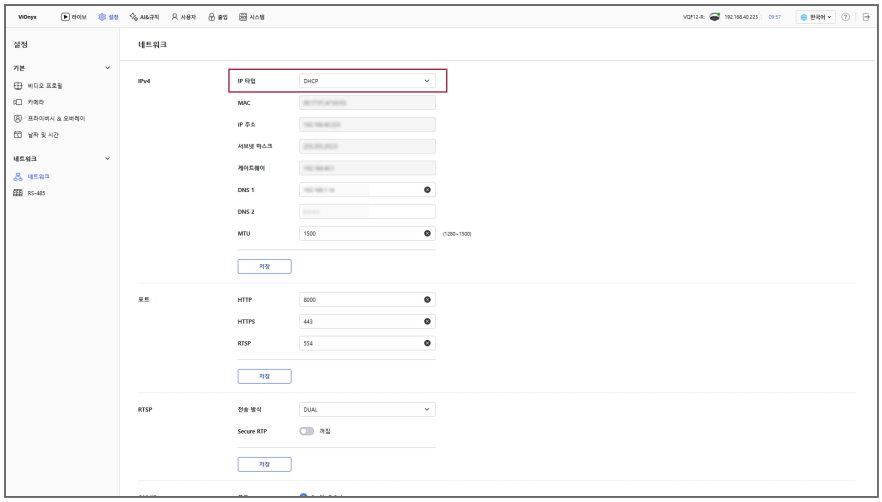
- DHCP가 지원되는 네트워크 환경에서 자동으로 IP 주소를 받아 구성하고 싶을 때
- 특정 IP 주소로 고정하여 안정적인 네트워크 접근이 필요할 때
- 기본 포트가 다른 장치와 충돌하거나 보안상 필요로 포트를 변경할 때
- Profile T를 지원하지 않는 구형 NVR/VMS와 ONVIF로 연결해야 할 때
- 슈프리마 CLUe 클라우드 서비스와 사용자 정보를 동기화해야 할 때
- 포트 포워딩이나 공인 IP 주소 없이 외부에서 장치의 웹 UI에 접속해야 할 때

> **알아두기**
> 네트워크 설정 변경, 특히 IP 주소 변경 시 기존 연결이 끊어질 수 있습니다. 변경된 IP 주소로 다시 접속해야 합니다.

IP 주소 자동 설정

DHCP는 네트워크에서 IP 주소를 자동으로 할당하는 방식입니다. 대부분의 일반적인 네트워크 환경에서 설정 없이 자동으로 구성됩니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **IP 타입**에서 **DHCP**를 선택하세요.



4. **DNS** 서버 주소가 필요하다면, **DNS {n}** 및 **DNS {n}** 입력 필드에 입력하세요.
5. **MTU** 입력 필드에서 **MTU**(Maximum Transmission Unit) 값을 필요에 따라 조정하세요.
   - 기본값은 1500입니다.

- 1280에서 1500 사이의 값으로 설정할 수 있습니다.

6. 네트워크 설정을 저장하려면 **저장** 버튼을 클릭하세요.

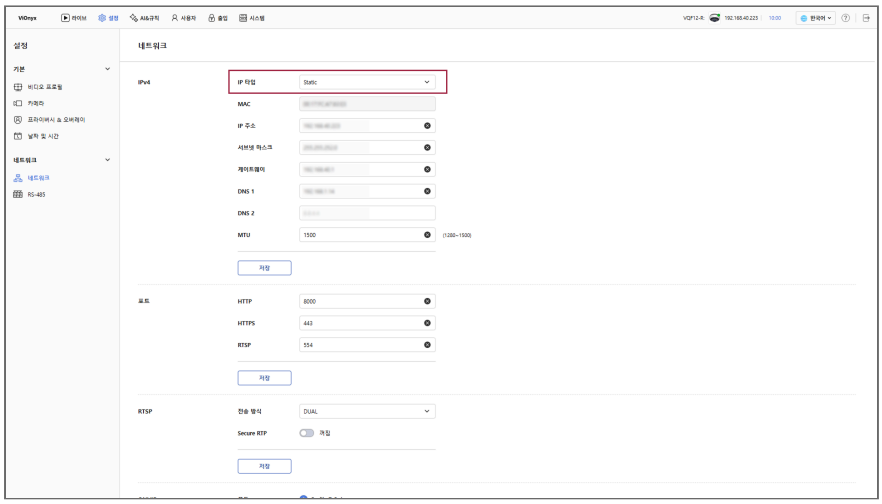
설정이 정상 저장되면 자동 할당된 IP 주소가 **IP 주소**, **서브넷 마스크**, **게이트웨이** 입력 필드에 표시됩니다.

> **알아두기**
> DHCP 모드가 기본값으로 설정되어 있으며, 대부분의 표준 네트워크 환경에서 별도 설정 없이 자동으로 작동합니다.

고정 IP 주소 설정

네트워크 환경에 따라 특정 IP 주소로 고정하여 안정적인 네트워크 접근이 필요할 때 수동으로 IP 주소를 설정할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **IP 타입**에서 **Static**을 선택하세요.



4. **IP 주소** 입력 필드에 할당받은 IPv4 주소를 입력하세요.

   예: 192.168.111.11

5. **서브넷 마스크** 입력 필드에 서브넷 마스크를 입력하세요.

   예: 255.255.255.0

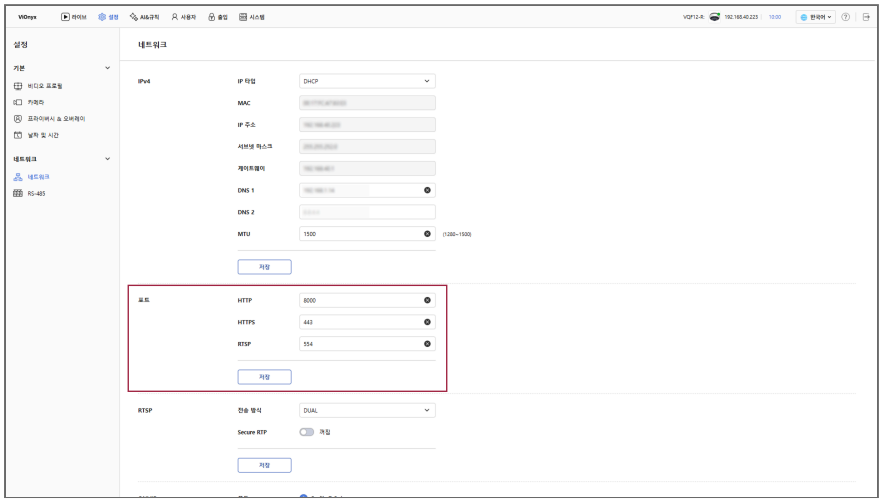
6. **게이트웨이** 입력 필드에 게이트웨이 주소를 입력하세요.
7. **DNS {n}** 및 **DNS {n}** 입력 필드에 DNS 서버 주소를 입력하세요.
8. **MTU** 입력 필드의 값을 필요에 따라 조정하세요.
   - 기본값은 1500입니다.
   - 1280에서 1500 사이의 값으로 설정할 수 있습니다.
9. 네트워크 설정을 저장하려면 **저장** 버튼을 클릭하세요.

각 입력 필드에 올바른 형식의 주소를 입력하지 않으면 입력 필드 주변에 빨간색 테두리가 표시되고, **저장** 버튼이 비활성화됩니다. 모든 입력 필드를 올바르게 입력한 후 다시 시도하세요.

포트 설정

포트 섹션에서는 웹 UI 접속(HTTP, HTTPS)과 영상 스트리밍(RTSP)에 사용되는 포트 번호를 설정할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **포트** 섹션에서 필요한 포트를 설정하세요.



- **HTTP**: 웹 UI에 비암호화하여 접속하는 포트(기본값: 8000)
- **HTTPS**: 웹 UI에 암호화하여 접속하는 포트(기본값: 443)
- **RTSP**: RTSP 프로토콜로 영상을 스트리밍하는 포트(기본값: 554)

4. 포트 설정을 저장하려면 **저장** 버튼을 클릭하세요.

알아두기

- 각 포트 입력 필드에 1~65535 범위의 번호를 입력할 수 있습니다.
- 동일한 포트 번호를 여러 개 설정할 수 없습니다. 각 포트는 고유한 번호를 가져야 합니다.
- 포트 설정이 기본값과 다른 경우, 웹 UI 접속 주소에 포트 번호를 명시해야 합니다.

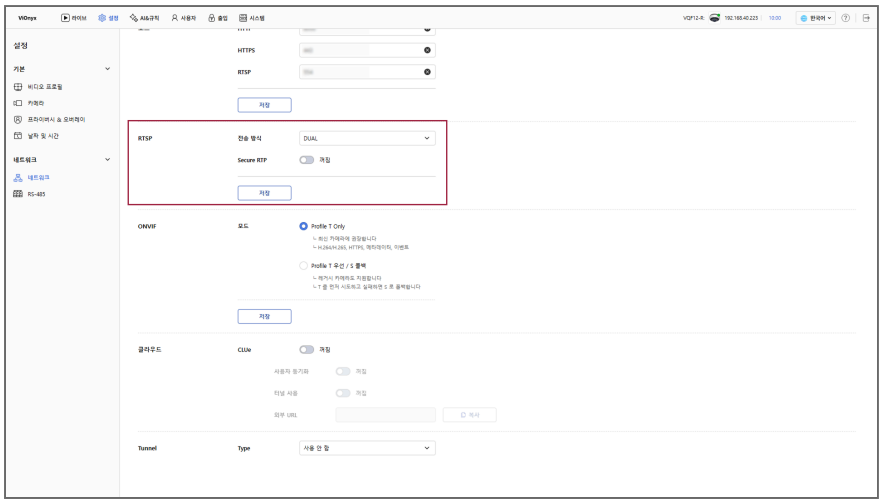
> *예: HTTPS 포트가 4000인 경우:* `https://{ip_address}:4000`

영상 전송 및 암호화 설정

RTSP 섹션에서는 영상 전송 및 암호화 설정을 구성할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.

3. **RTSP** 섹션에서 다음 옵션을 설정하세요.



- **전송 방식**: 영상 스트리밍에 사용할 전송 프로토콜을 선택하세요.
  - **UDP**: 빠른 전송이 가능하지만, 네트워크 상태에 따라 영상 끊김이나 프레임 손실이 발생할 수 있습니다.
  - **TCP**: 안정적인 전송이 가능하지만, 네트워크 상태에 따라 **UDP**보다 지연이 발생할 수 있습니다.
  - **DUAL**: 네트워크 상태에 따라 UDP와 TCP를 자동으로 선택하여 스트리밍합니다. 일반 환경에서 권장하는 기본값입니다.
  - **TLS**: RTSP 스트림을 TLS 암호화로 전송합니다. 보안을 강화하지만, CPU 부하가 증가할 수 있습니다. 연결하는 NVR/VMS가 TLS를 지원하는지 확인하세요.
- **Secure RTP**: RTSP 스트림 암호화 옵션을 활성화하세요.

4. 설정을 저장하려면 **저장** 버튼을 클릭하세요.

알아두기

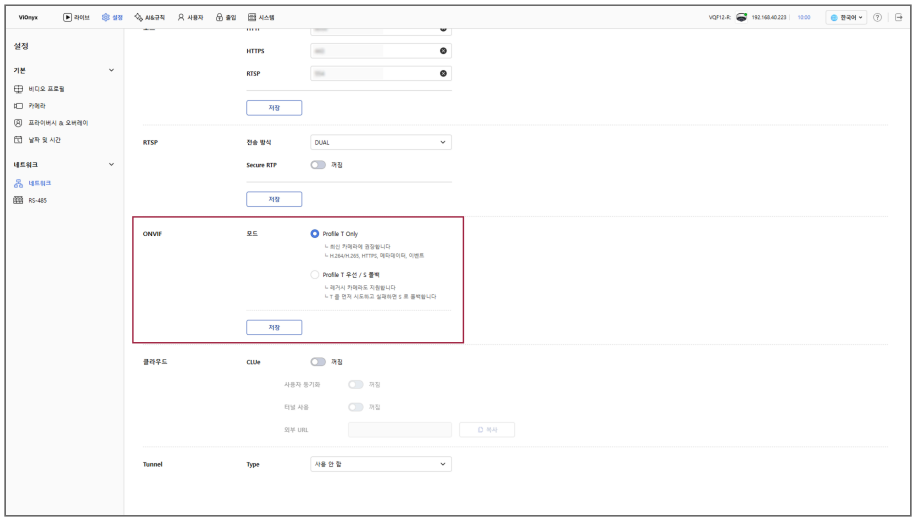
영상 및 오디오 데이터 암호화가 필요하다면 **Secure RTP** 옵션을 활성화하고, 연결하는 NVR/VMS와 호환되는지 확인하세요.

주의

Secure RTP 옵션을 변경한 후에는 기존 RTSP 세션을 다시 연결해야 할 수 있습니다. NVR/VMS에서도 선택한 전송 방식과 호환되도록 설정해야 합니다.

ONVIF 설정

ONVIF 섹션에서는 NVR/VMS가 ONVIF로 장치에 연결할 때 사용할 프로필을 설정할 수 있습니다. 기본적으로 Profile T만 사용하며, Profile T를 지원하지 않는 구형 NVR/VMS와 연결해야 할 때는 Profile S 폴백을 추가로 활성화할 수 있습니다.



다음 2가지 모드 중 하나를 선택할 수 있습니다.

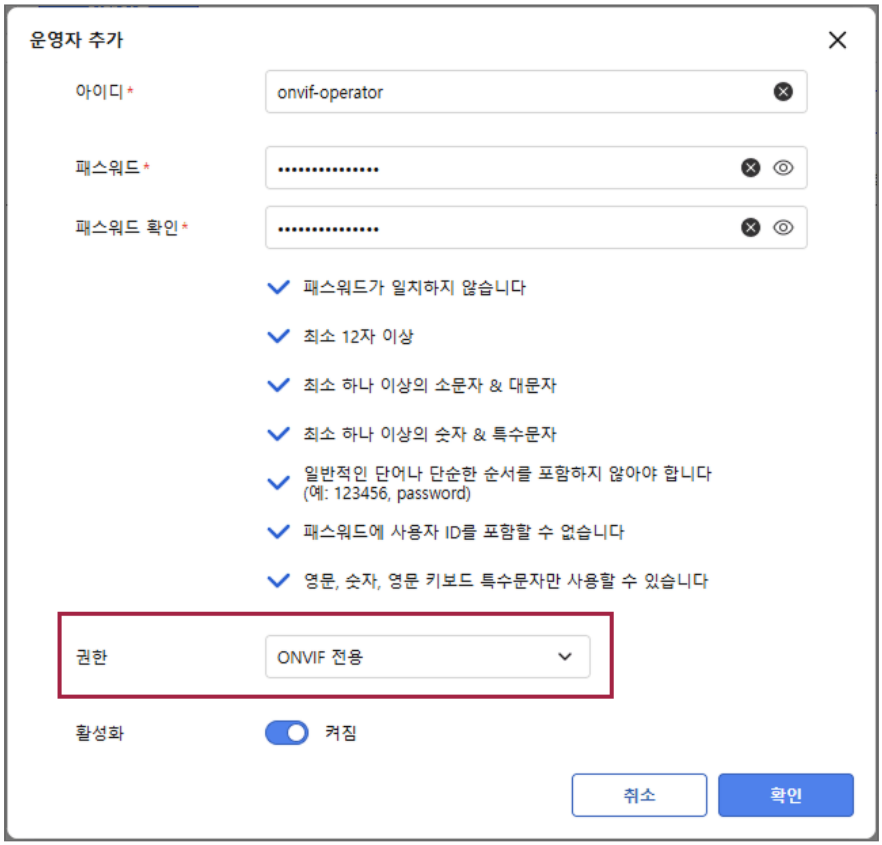
- **Profile T Only**: Profile T(Media2)로만 연결합니다. H.264/H.265 코덱, HTTPS, 메타데이터, 이벤트를 지원하며, 최신 NVR/VMS 환경에서 권장하는 기본값입니다.
- **Profile T 우선 / S 폴백**: NVR/VMS가 Profile T로 먼저 연결을 시도하고, Profile T를 지원하지 않으면 Profile S(Media1)로 연결합니다. Profile T를 지원하는 NVR/VMS는 이 모드에서도 Profile T로 연결됩니다.

항목	Profile T (Media2)	Profile S (Media1)
코덱	H.264, H.265	H.264, MJPEG
암호화 통신	HTTPS 지원	지원 안 함(평문 통신)
고급 기능	메타데이터, 이벤트	기본 영상 스트리밍
권장 환경	최신 NVR/VMS	Profile T를 지원하지 않는 구형 NVR/VMS

ONVIF 전용 계정 생성

Profile S 폴백을 활성화하려면 NVR/VMS가 ONVIF 및 RTSP 인증에 사용할 ONVIF 전용 계정이 먼저 필요합니다. 계정 없이 설정을 저장하면 **Profile S 폴백을 켜려면 ONVIF 전용 계정이 먼저 필요합니다** 메시지와 함께 설정이 저장되지 않습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.
3. **운영자** 섹션에서 **+ 추가** 버튼을 클릭하세요.
4. **운영자 추가** 팝업창에서 아이디와 패스워드를 입력하고, **권한**에서 **ONVIF 전용**을 선택하세요.



5. ONVIF 전용 계정을 생성하려면 **확인** 버튼을 클릭하세요.

Profile S 폴백 활성화

Profile S 폴백을 활성화하세요.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **ONVIF** 섹션의 **모드**에서 **Profile T 우선 / S 폴백**을 선택하세요.
4. **Profile S 폴백 활성화** 팝업창이 나타나면 Profile S 사용 시 주의 사항을 확인한 후 **확인** 버튼을 클릭하세요.



5. 설정을 저장하려면 **저장** 버튼을 클릭하세요.

설정이 정상 저장되면 화면 오른쪽 상단에 성공 메시지가 나타납니다. NVR/VMS에서 장치를 등록할 때 ONVIF 전용 계정의 아이디와 패스워드를 입력하세요.

Profile S 폴백을 비활성화하려면 **Profile T Only**를 선택한 후 **저장** 버튼을 클릭하세요.

> **주의**
> Profile S는 암호화 없이 평문으로 통신하므로 네트워크 공격에 노출될 수 있습니다. 또한 H.265 코덱과 HTTPS/TLS를 사용할 수 없습니다. Profile T를 지원하지 않는 구형 NVR/VMS와 연결할 때만 사용하세요.

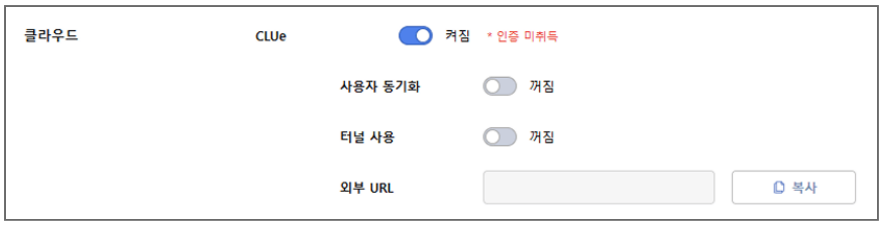
> **알아두기**
> - ONVIF 설정은 관리자만 변경할 수 있습니다.
> - ONVIF 전용 계정은 장치당 하나만 만들 수 있습니다. 웹 UI에 로그인할 수 없으며, 계정을 생성한 후에는 아이디와 패스워드를 변경할 수 없습니다.
> - ONVIF 전용 계정은 활성화 또는 비활성화, 삭제만 할 수 있습니다. 계정이 비활성 상태이면 Profile S 폴백을 활성화할 수 없습니다.
> - ONVIF 전용 계정을 삭제하려면 먼저 **Profile T Only**로 변경하세요.
> - 변경한 ONVIF 설정은 새로운 연결부터 적용됩니다. 기존에 연결된 스트림은 다시 연결할 때까지 현재 연결 방식을 유지합니다.

CLUe 클라우드 연결

슈프리마 CLUe는 클라우드 기반 출입 통제 서비스입니다. CLUe에 연결하면 CLUe 클라우드 서비스와 사용자 정보를 동기화할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **클라우드** 섹션의 **CLUe** 토글을 클릭해 활성화하세요.

4. 시스템이 인터넷 연결과 CLUe 서버 연결을 확인합니다. **CLUe** 토글 오른쪽에 연결 상태가 표시됩니다.



- *** 연결 중...**: CLUe 서버에 연결하고 있습니다.
- *** 연결됨**: CLUe 서버에 연결되었습니다.
- *** 연결 실패**: CLUe 서버에 연결하지 못했습니다. 인터넷 연결을 확인한 후 다시 시도하세요.
- *** 인증 미취득**: 장치가 CLUe 인증을 받지 않은 상태입니다.

5. 필요한 옵션을 활성화하세요. **CLUe** 토글을 활성화해야 다음 옵션을 사용할 수 있습니다.

- **사용자 동기화**: CLUe 클라우드 서비스와 사용자 정보를 동기화합니다.
- **터널 사용**: CLUe를 통해 외부에서 장치에 접속할 수 있는 터널을 사용합니다. 터널이 연결되면 **외부 URL** 필드에 URL이 표시됩니다. **복사** 버튼을 클릭하여 URL을 복사할 수 있습니다.

> **알아두기**
>
> - 연결에 성공하면 **CLUe가 활성화되었습니다** 메시지가 표시됩니다.
> - 연결에 실패하면 **CLUe가 비활성화되었습니다** 메시지가 표시됩니다. 인터넷 연결을 확인한 후 다시 시도하세요.
> - **CLUe** 토글을 비활성화하면 CLUe 서버와의 연결이 끊어지고, **사용자 동기화**와 **터널 사용** 옵션을 사용할 수 없습니다. 하지만 CLUe 서버 측의 등록 정보는 유지됩니다.
> - CLUe 연결 성공 및 실패는 시스템 로그에 기록됩니다.

Tunnel 설정

Tunnel 섹션에서는 Cloudflare Tunnel을 사용하여 외부 인터넷에서 장치의 웹 UI에 접속할 수 있는 외부 URL을 만들 수 있습니다. 공유기의 포트 포워딩이나 공인 IP 주소 없이 원격으로 장치에 접속해야 할 때 사용하세요.

Tunnel 섹션의 **Type**에서 다음 중 하나를 선택할 수 있습니다.

유형	설명	필요한 정보
사용 안 함	Tunnel을 사용하지 않습니다. 기본값입니다.	없음
Cloudflare Tunnel (Quick)	Cloudflare 계정 없이 임시 외부 URL을 발급받습니다. 장치를 재시작하면 URL이 바뀝니다.	없음
Cloudflare Tunnel (Named)	Cloudflare API Token으로 Tunnel을 만들고, 사용자의 도메인으로 고정된 외부 URL을 사용합니다.	Cloudflare 계정, 도메인
Cloudflare Tunnel (Named, Token)	Cloudflare 대시보드에서 미리 만든 Tunnel에 Connector Token으로 연결합니다.	Cloudflare 계정, 도메인, Connector Token

팁

테스트나 일시적인 원격 접속에는 **Cloudflare Tunnel (Quick)**을, 고정된 주소로 계속 접속해야 할 때는 **Cloudflare Tunnel (Named)** 또는 **Cloudflare Tunnel (Named, Token)**을 사용하세요.

알아두기

- Tunnel을 사용하지 않으려면 **Type**에서 **사용 안 함**을 선택하세요.
- Tunnel을 사용하려면 장치가 인터넷에 연결되어 있어야 합니다.
- 외부 URL을 아는 사람은 누구나 장치의 로그인 화면에 접근할 수 있습니다. 관리자와 운영자 계정에 안전한 패스워드를 사용하고, 외부 URL을 필요한 사람에게만 공유하세요.
- Tunnel 모드 변경은 시스템 로그에 기록됩니다.

임시 외부 URL 사용

Cloudflare 계정 없이 임시 외부 URL로 장치에 접속할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **Tunnel** 섹션의 **Type**에서 **Cloudflare Tunnel (Quick)**을 선택하세요.



4. 임시 외부 URL이 발급되면 **외부 URL** 필드에 표시됩니다. **복사** 버튼을 클릭하여 URL을 복사한 후 웹 브라우저에서 접속하세요.

주의

Cloudflare Tunnel (Quick)으로 발급한 외부 URL은 장치를 재시작하면 변경됩니다. 재시작 후에는 **외부 URL** 필드에서 새 URL을 확인하세요.

고정 외부 URL 사용(API Token)

Cloudflare API Token을 입력하면 장치가 Cloudflare에 Tunnel을 만들고, 지정한 호스트 이름으로 외부 URL을 연결합니다. 시작하기 전에 Cloudflare 계정과 Cloudflare에 등록된 도메인을 준비하세요.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **Tunnel** 섹션의 **Type**에서 **Cloudflare Tunnel (Named)**를 선택하세요.



4. 다음 정보를 입력하세요.
   - **Cloudflare API Token**: Cloudflare 대시보드에서 발급한 API Token을 입력하세요.
   - **Account ID**: Cloudflare 계정 ID를 입력하세요.
   - **Hostname**: 외부에서 접속할 때 사용할 호스트 이름을 입력하세요.

     > *예: cam.example.com*
   - **Tunnel Name (Option)**: Cloudflare에서 Tunnel을 구분할 이름을 입력하세요. 선택 항목입니다.
5. 입력한 정보가 올바른지 확인하려면 **검증** 버튼을 클릭하세요.
6. 설정을 적용하려면 **적용** 버튼을 클릭하세요.

Tunnel이 연결되면 **외부 URL** 필드에 외부 URL이 표시됩니다. **복사** 버튼을 클릭하면 URL을 복사할 수 있습니다.

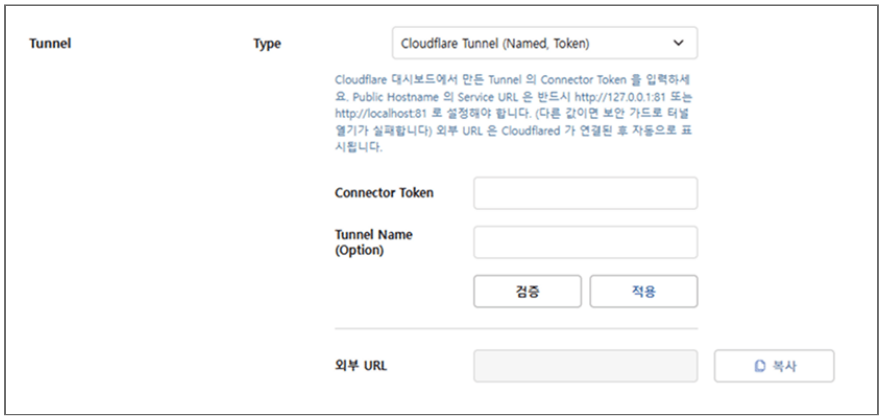
고정 외부 URL 사용(Connector Token)

Cloudflare 대시보드에서 직접 만든 Tunnel에 장치를 연결할 수 있습니다. 시작하기 전에 Cloudflare 대시보드에서 다음 작업을 완료하세요.

- Tunnel을 만들고 Connector Token을 복사하세요.
- Tunnel의 Public Hostname을 추가하고, Service URL을 `http://127.0.0.1:81` 또는 `http://localhost:81`로 설정하세요.

설정을 마쳤으면 장치에서 다음 단계를 진행하세요.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **네트워크**를 클릭하세요.
3. **Tunnel** 섹션의 **Type**에서 **Cloudflare Tunnel (Named, Token)**을 선택하세요.



4. 다음 정보를 입력하세요.
   - **Connector Token**: Cloudflare 대시보드에서 복사한 Connector Token을 입력하세요.
   - **Tunnel Name (Option)**: Tunnel을 구분할 이름을 입력하세요. 선택 항목입니다.
5. 입력한 정보가 올바른지 확인하려면 **검증** 버튼을 클릭하세요.
6. 설정을 적용하려면 **적용** 버튼을 클릭하세요.

Cloudflared가 연결되면 **외부 URL** 필드에 외부 URL이 자동으로 표시됩니다.

> **주의**
> Public Hostname의 Service URL을 `http://127.0.0.1:81` 또는 `http://localhost:81` 이외의 값으로 설정하면 보안 정책에 따라 Tunnel이 열리지 않습니다.

RS-485 설정하기

RS-485 설정에서는 카메라의 RS-485 포트에 연결된 슈프리마 I/O 장치를 슬레이브 장치로 등록하고 관리할 수 있습니다. 카메라는 RS-485 포트의 마스터로 동작하며, 등록한 슬레이브 장치의 릴레이를 AI 규칙과 연동하여 출입문 개방, 비상등 작동 등 외부 장치를 제어할 수 있습니다.

아래와 같은 상황에서 **RS-485** 설정을 확인하세요.

- 카메라에 I/O 장치를 연결하여 릴레이 출력이나 입력 포트를 늘리고 싶을 때
- AI 이벤트가 발생하면 슬레이브 장치의 릴레이로 외부 장치를 제어하고 싶을 때
- 슬레이브 장치의 연결 상태를 확인하거나 펌웨어를 업데이트해야 할 때
- 더 이상 사용하지 않는 슬레이브 장치를 제거해야 할 때

알아두기

- 펌웨어 버전 1.1.0에서는 마스터 모드만 지원합니다. 카메라를 다른 장치의 슬레이브로 연결하는 슬레이브 모드는 지원하지 않습니다.
- 슬레이브 장치는 최대 8대까지 등록할 수 있습니다.
- 지원하는 슬레이브 장치는 슈프리마 I/O 장치입니다. 지문 인식 장치와 얼굴 인식 장치는 슬레이브 장치로 연결할 수 없습니다.
  - Secure I/O 2 (SIO2)
  - Door Module (DM-20)
  - Door Interface (DI-24)
  - Output Module (OM-120)
  - Input Module (IM-120)

시작하기 전에

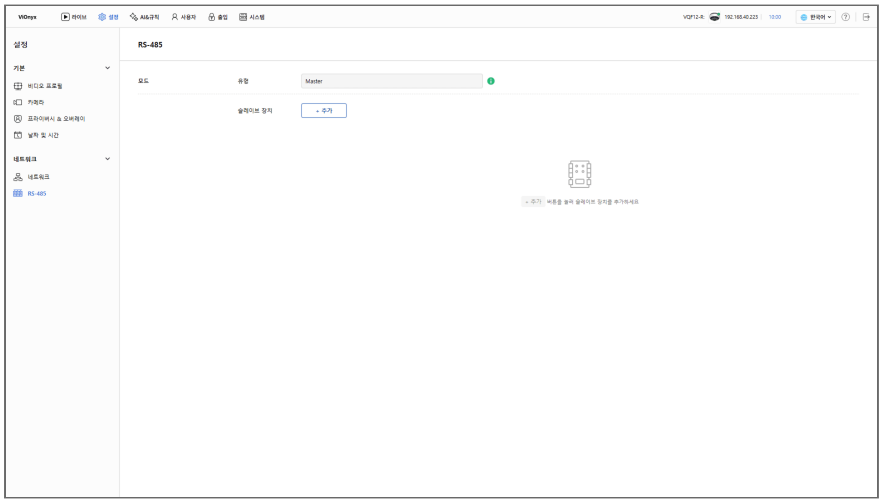
슬레이브 장치를 추가하기 전에 다음 사항을 확인하세요.

- 슬레이브 장치가 카메라의 RS-485 포트에 올바르게 배선되어 있는지 확인하세요.
- 슬레이브 장치에 OSDP ID가 할당되어 있는지 확인하세요. OSDP ID가 0(미배정)인 장치는 등록할 수 없습니다.
- 같은 RS-485 버스에 연결된 장치끼리 OSDP ID가 중복되지 않는지 확인하세요.
- 슬레이브 장치가 다른 마스터 장치에 등록되어 있었다면 장치를 초기화하세요.

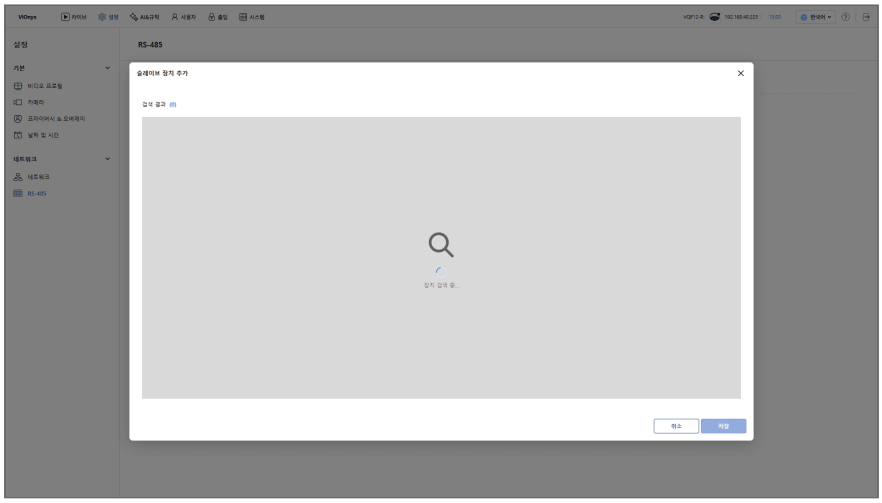
슬레이브 장치 추가

RS-485 포트에 연결된 슬레이브 장치를 검색하여 카메라에 등록하세요.

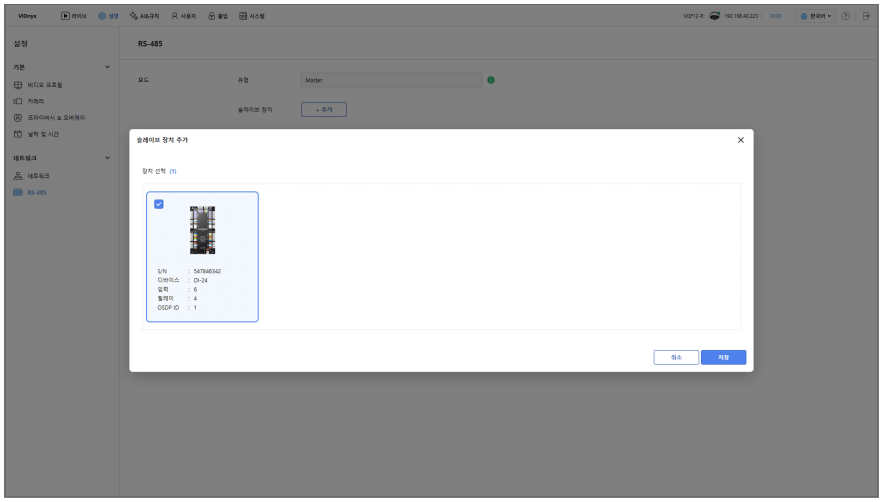
1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **RS-485**를 클릭하세요.



3. **슬레이브 장치** 항목의 **+ 추가** 버튼을 클릭하세요.
4. **슬레이브 장치 추가** 팝업창이 나타나고, 장치 검색이 자동 시작됩니다. 검색이 끝날 때까지 기다리세요.



5. 검색 결과에서 추가할 장치의 체크박스를 선택하세요. 여러 장치를 함께 선택할 수 있습니다.



검색된 장치에는 다음 정보가 포함되어 있습니다.

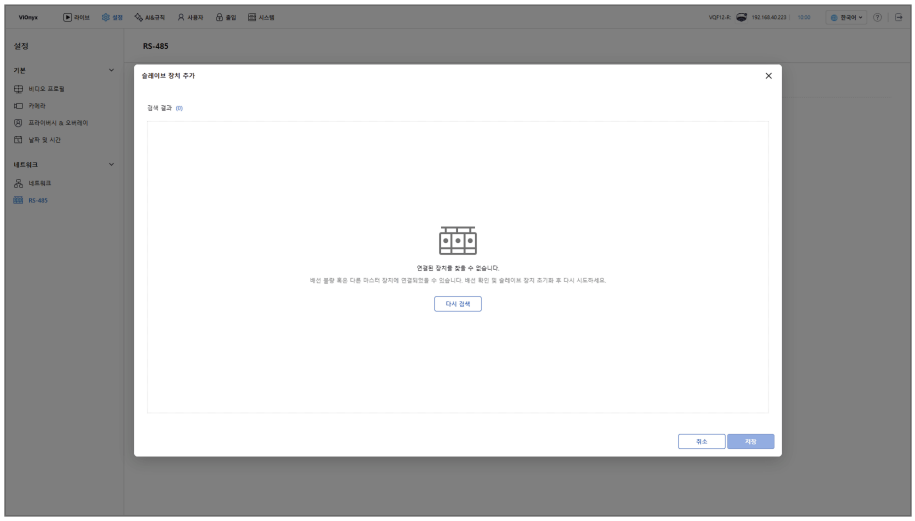
- **S/N**: 장치의 시리얼 번호
- **디바이스**: 장치 모델명
- **입력**: 입력 단자 수
- **릴레이**: 릴레이 단자 수
- **OSDP ID**: 장치에 배정된 OSDP ID

6. 선택한 장치를 등록하려면 **저장** 버튼을 클릭하세요. 장치를 하나 이상 선택해야 버튼이 활성화됩니다.

장치가 정상 등록되면 화면 오른쪽 상단에 성공 메시지가 나타납니다. **슬레이브 장치** 목록에 장치가 OSDP ID 순으로 표시됩니다. 장치 이름은 시리얼 번호로 자동 지정되며, 슬레이브 장치 수정에서 변경할 수 있습니다.

장치를 찾을 수 없을 때

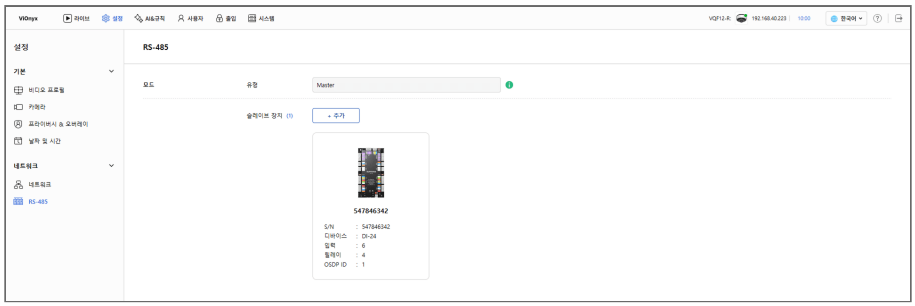
검색 결과에 **연결된 장치를 찾을 수 없습니다.** 메시지가 나타나면 다음 사항을 확인한 후 **다시 검색** 버튼을 클릭하세요.



- 슬레이브 장치의 RS-485 배선이 올바르게 연결되어 있는지 확인하세요.
- 슬레이브 장치가 다른 마스터 장치에 등록되어 있다면 장치를 초기화하세요.
- 슬레이브 장치에 OSDP ID가 할당되어 있는지 확인하세요.

슬레이브 장치 상태 확인

슬레이브 장치 목록에서 등록한 장치의 정보와 연결 상태를 확인할 수 있습니다.



장치와 카메라의 통신이 끊어지면 장치 카드에 **연결 끊김** 표시와 함께 연결이 끊어진 일시가 나타납니다. 장치의 전원과 RS-485 배선을 확인하세요. 장치가 다시 연결되면 표시가 사라집니다.



알아두기
슬레이브 장치의 연결 및 연결 끊김 기록은 시스템 로그에서 확인할 수 있습니다. 자세한 내용은 시스템 로그 확인하기를 참고하세요.

슬레이브 장치 수정

등록한 슬레이브 장치의 이름을 변경할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **RS-485**를 클릭하세요.
3. 수정할 장치 카드에 마우스 포인터를 올린 후, 오른쪽 상단의 버튼을 클릭하세요.
4. **슬레이브 설정** 팝업창에서 **이름** 입력 필드에 새 이름을 입력하세요.



5. 변경 사항을 저장하려면 **적용** 버튼을 클릭하세요.

변경 사항이 정상 저장되면 화면 오른쪽 상단에 성공 메시지가 나타납니다.

> **알아두기**
> **슬레이브 설정** 팝업창에서는 OSDP ID를 확인만 할 수 있으며, 변경할 수 없습니다.

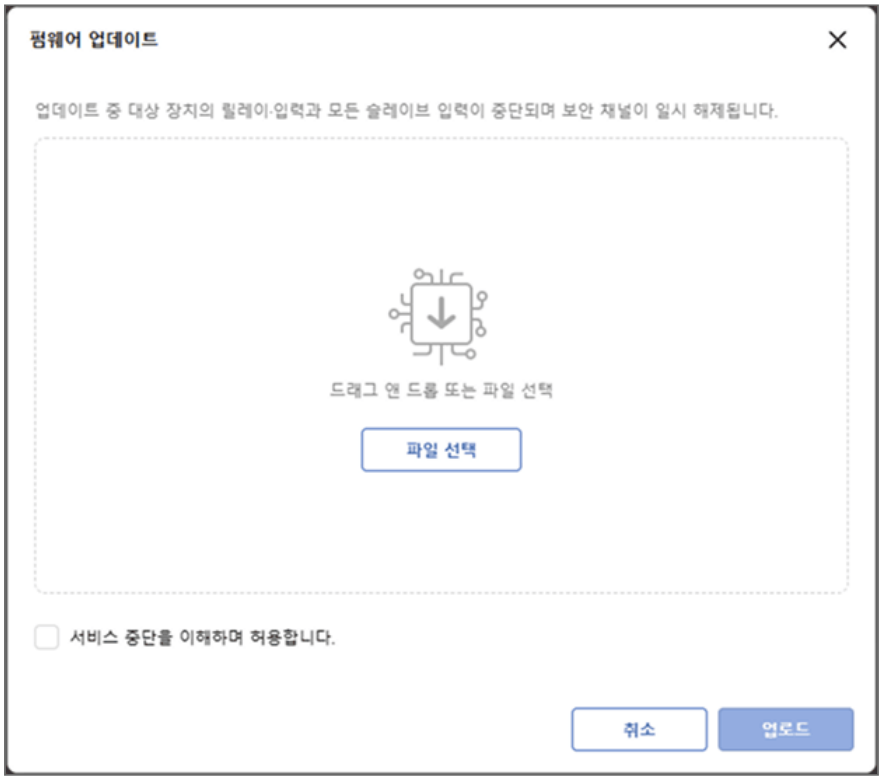
슬레이브 장치 펌웨어 업데이트

슬레이브 설정 팝업창에서 슬레이브 장치의 현재 펌웨어 버전을 확인하고 업데이트할 수 있습니다.

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **RS-485**를 클릭하세요.
3. 업데이트할 장치 카드에 마우스 포인터를 올린 후, 오른쪽 상단의 버튼을 클릭하세요.
4. **슬레이브 설정** 팝업창의 **FW 버전**에서 현재 버전을 확인하고, **업데이트** 버튼을 클릭하세요.



5. 드래그 앤 드롭 또는 **파일 선택** 버튼을 클릭해 펌웨어 파일을 선택하세요.



6. 업데이트 중 서비스 중단 안내를 확인한 후, **서비스 중단을 이해하며 허용합니다.** 체크박스를 선택하세요.
7. 업데이트를 시작하려면 **업로드** 버튼을 클릭하세요.

업데이트가 진행되는 동안 진행 상태와 진행률이 표시됩니다. 슬레이브 장치의 펌웨어 업데이트 성공 및 실패 기록은 시스템 로그에서 확인할 수 있습니다.

> **주의**
>
> - 업데이트하는 동안 대상 장치의 릴레이와 입력, 그리고 모든 슬레이브 장치의 입력이 중단되며, 보안 채널이 일시적으로 해제됩니다. 장치를 사용하지 않는 시간에 업데이트하세요.
> - 업데이트 중에는 장치의 전원을 끄거나 RS-485 배선을 분리하지 마세요.
> - 다른 펌웨어 업데이트가 진행 중이면 업데이트를 시작할 수 없습니다. 진행 중인 업데이트가 끝난 후 다시 시도하세요.

슬레이브 장치 제거

더 이상 사용하지 않는 슬레이브 장치를 제거할 수 있습니다. 장치를 하나씩 제거하거나, 여러 장치를 선택하여 한 번에 제거할 수 있습니다.

> **주의**
>
> AI 규칙에서 사용 중인 장치는 제거할 수 없습니다. 제거를 시도하면 해당 장치를 사용하는 규칙 이름이 표시됩니다. 먼저 해당 규칙에서 장치의 릴레이 설정을 제거한 후 다시 시도하세요. 규칙 수정 방법은 AI 규칙(Rule) 설정하기를 참고하세요.

장치 하나씩 제거

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **RS-485**를 클릭하세요.

3. 제거할 장치 카드에 마우스 포인터를 올린 후, 오른쪽 상단의 버튼을 클릭하세요.
   - 또는 버튼을 클릭한 후, **슬레이브 설정** 팝업창에서 **제거** 버튼을 클릭하세요.
4. **장치 제거** 팝업창이 나타나면 **적용** 버튼을 클릭하세요.

여러 장치 한 번에 제거

1. 화면 왼쪽 상단의 **설정** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **네트워크** → **RS-485**를 클릭하세요.
3. 제거할 장치 카드의 체크박스를 각각 선택하세요. **장치 선택** 옆에 선택한 장치 수가 표시됩니다.



4. **삭제** 버튼을 클릭하세요.
5. **장치 제거** 팝업창이 나타나면 **적용** 버튼을 클릭하세요.

장치가 정상 제거되면 화면 오른쪽 상단에 삭제 성공 메시지가 나타납니다.

문제 해결

슬레이브 장치를 추가하거나 수정, 제거할 때 다음 오류 메시지가 나타날 수 있습니다.

메시지	원인 및 조치
슬레이브 장치 등록에 실패했습니다. 배선을 확인한 뒤 다시 시도하세요.	장치와 통신하지 못했습니다. RS-485 배선을 확인한 후 다시 시도하세요.
슬레이브 장치는 최대 8대까지 등록할 수 있습니다.	이미 8대가 등록되어 있습니다. 사용하지 않는 장치를 제거한 후 다시 추가하세요.
같은 시리얼 번호의 장치가 이미 등록되어 있습니다.	같은 시리얼 번호의 장치가 이미 목록에 있습니다. 목록을 확인하세요.
이미 사용 중인 OSDP ID입니다.	다른 장치가 같은 OSDP ID를 사용하고 있습니다. 슬레이브 장치에서 OSDP ID를 변경한 후 다시 검색하세요.

메시지	원인 및 조치
버스의 다른 장치와 OSDP ID가 충돌합니다.	RS-485 버스의 다른 장치와 OSDP ID가 겹칩니다. 슬레이브 장치에서 OSDP ID를 변경한 후 다시 검색하세요.
OSDP ID 0(미배정) 장치는 등록할 수 없습니다. 장치에서 주소를 배정한 뒤 다시 검색하세요.	OSDP ID가 0(미배정)인 장치입니다. 장치에서 OSDP ID를 배정한 후 다시 검색하세요.
장치 검색 시간이 초과되었습니다.	검색 시간 안에 장치가 응답하지 않았습니다. 배선을 확인한 후 다시 검색하세요.
슬레이브 장치가 룰에서 사용 중입니다.	장치가 AI 규칙에서 사용 중입니다. 해당 규칙에서 장치의 릴레이 설정을 제거한 후 다시 시도하세요.
RS-485 초기화 중입니다. 잠시 기다려 주세요.	카메라가 RS-485 포트를 준비하고 있습니다. 잠시 후 다시 시도하세요.

RTSP 및 ONVIF 연동하기

카메라는 타사 NVR(Network Video Recorder) 및 VMS(Video Management Software)와의 표준 연동을 위해 RTSP(Real-Time Streaming Protocol) 스트리밍과 ONVIF(Open Network Video Interface Forum) 프로토콜을 지원합니다.

아래와 같은 상황에서 이 문서를 참고하세요.

- 타사 NVR/VMS에서 RTSP로 카메라 영상을 가져오고 싶을 때
- ONVIF를 지원하는 NVR/VMS와 카메라를 연동하고 싶을 때
- RTSP 접속 주소나 ONVIF 연동 시 필요한 계정 정보를 확인하고 싶을 때

RTSP 스트리밍

포트 및 전송 방식

RTSP 포트와 전송 방식은 **네트워크** 설정에서 변경할 수 있습니다. 포트 설정, 영상 전송 및 암호화 설정에 대한 자세한 내용은 다음 문서를 참고하세요.

- 포트 설정
- 영상 전송 및 암호화 설정

> **알아두기**
> RTSP 포트를 기본값(554)에서 변경했다면, 아래 **Connection URL**의 `{port}` 부분도 변경된 포트 번호로 입력해야 합니다.

RTSP Connection URL

타사 NVR/VMS에서 카메라 영상을 RTSP로 가져오려면 채널과 해상도에 맞는 Connection URL을 등록해야 합니다.

채널	스트림	Connection URL
Channel 1 - Fisheye(피쉬아이 영상)	메인 스트림(고해상도)	rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_primary
Channel 1 - Fisheye(피쉬아이 영상)	서브 스트림(저해상도)	rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_secondary
Channel 2 - Dewarp(평면 왜곡 보정 영상)	메인 스트림(고해상도)	rtsp://{id}:{passwd}@{IP_address}:{port}/dewarp_primary

- {id}, {passwd}: 카메라에 접속할 계정의 아이디와 비밀번호를 입력하세요.
- {IP_address}: 카메라의 IP 주소를 입력하세요.
- {port}: RTSP 포트 번호를 입력하세요. 기본값은 554입니다.

ONVIF 연동

지원 사양

카메라는 ONVIF **Profile S** 및 **Profile T**를 지원합니다.

ONVIF 전용 계정 준비

보안 표준 사양에 따라 기본 관리자(admin) 계정으로는 ONVIF 연결을 지원하지 않습니다. ONVIF로 연동하기 전에 ONVIF 전용 운영자 계정을 추가하고, 해당 계정 정보로 NVR/VMS에서 접속하세요. ONVIF 전용 운영자 계정 추가 방법은 네트워크 설정하기를 참고하세요.

연동 시 유의 사항

- **설정 동기화 보호**

  웹 설정 엔진과의 데이터 정합성을 유지하고 오동작을 방지하기 위해, ONVIF를 통해 해상도, 비트레이트, 이미지 센서 속성 등 카메라 내부 설정값을 변경하는 쓰기(Write) 동작은 지원하지 않습니다.

- **VMS 자동 최적화 기능 비활성화**

  일부 VMS는 연결 시 카메라 설정을 자동으로 변경하는 기능(Video Optimization, Auto Configuration 등)을 제공합니다. 이 기능이 켜져 있으면 연동 오류가 발생할 수 있으므로, VMS 측에서 카메라 설정 자동 수정/최적화 옵션을 비활성화하세요.

> **주의**
> RTSP 전송 방식을 변경하면 기존 RTSP 세션을 다시 연결해야 할 수 있습니다. NVR/VMS에서도 선택한 전송 방식과 호환되도록 설정해야 합니다.

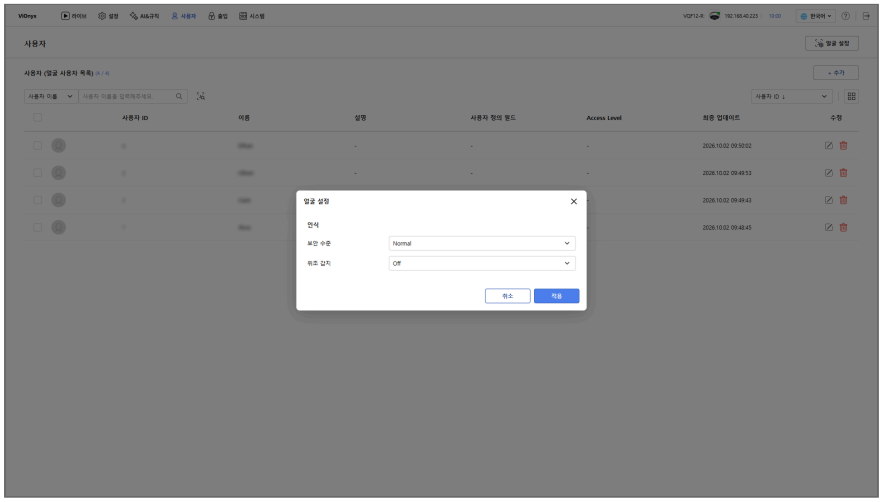
사용자 관리하기

사용자를 등록하여 AI 얼굴 인식 기능을 활용할 수 있습니다. 새로운 사용자 등록부터 기존 사용자 정보 관리, 조회까지 전체 사용자 생명주기를 효율적으로 관리하세요.

얼굴 인증 설정하기

얼굴 인증 설정을 통해 인증 효율성, 보안 수준, 위조 감지를 한 번에 관리할 수 있습니다. 조직의 보안 정책과 운영 환경에 따라 적절한 값으로 조정하세요.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 화면 오른쪽 상단의 **얼굴 설정** 버튼을 클릭하세요.
3. **얼굴 설정** 창이 나타나면 필요한 옵션을 설정하세요.



- **보안 수준**: 보안 등급을 설정할 수 있습니다. 보안 등급이 높을수록 인증이 더 엄격해집니다.
- **위조 감지**: 사진 등의 위조 얼굴을 이용한 사용자 인증을 방지할 수 있습니다.

4. 설정을 완료하면 **적용** 버튼을 클릭하세요.

> **팁**
> 높은 보안이 필요한 구역은 **보안 수준** 옵션을 **Most Secure**로 설정하는 것을 권장합니다.

사용자 추가하기

AI 얼굴 인식을 위한 사용자를 등록할 수 있습니다. 사용자를 추가할 때 기본 정보를 입력하고 세 가지 방식 중 하나로 얼굴 사진을 등록할 수 있습니다.

아래와 같은 상황에서 사용자를 추가하세요.

- 조직에 새로 입사한 사용자를 등록하고 싶을 때

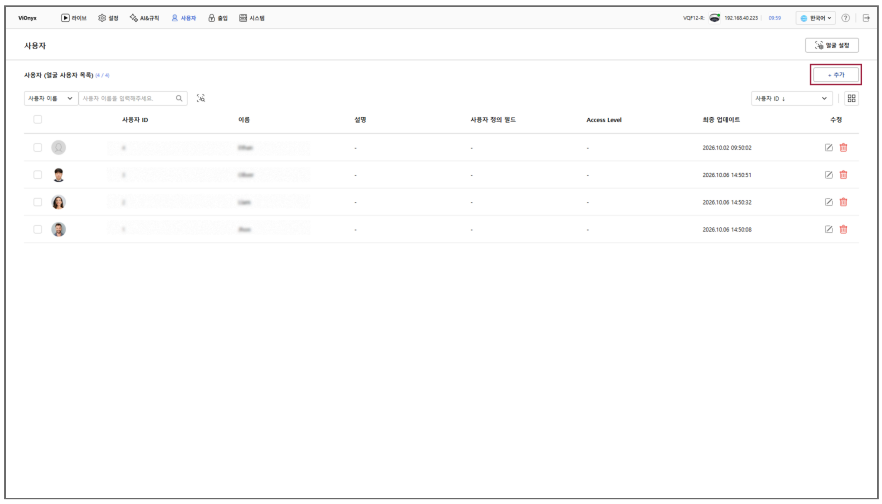
- 사용자의 얼굴 사진을 촬영하여 얼굴 인식 데이터베이스에 등록하고 싶을 때
- 여러 명의 사용자를 일괄적으로 추가하고 싶을 때
- 외부 시스템(ERP, 인사 관리 시스템)과 연동하기 위해 사용자를 등록하고 싶을 때

> **알아두기**
>
> - 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다.
> - 최초로 사용자를 추가할 때 얼굴 인식 사용 동의 팝업이 표시됩니다. 동의 기록은 시스템 로그에 저장되며, 동의 후에는 재표시되지 않습니다.
> - AI 이벤트 설정에서 미리 동의를 완료했다면 사용자 추가 시 별도의 팝업이 표시되지 않습니다.

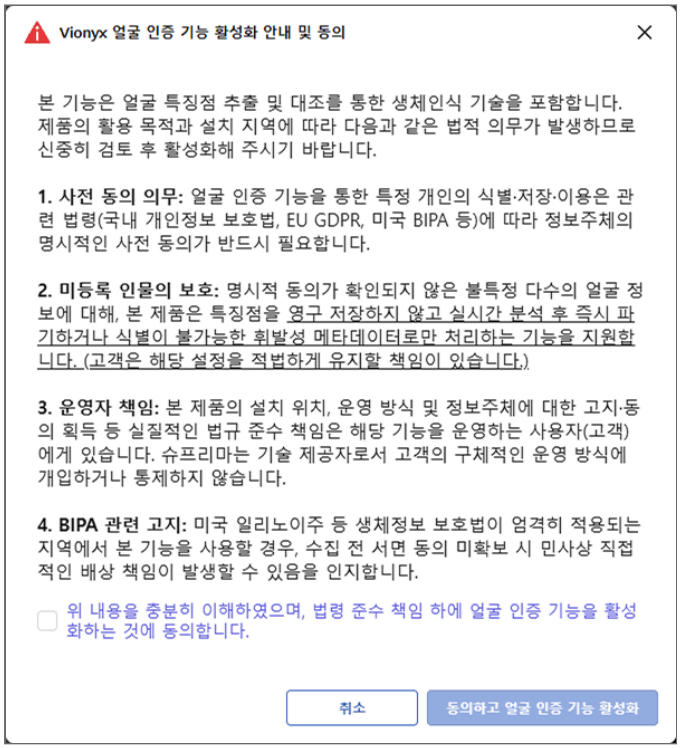
사용자 기본 정보 입력

최초 사용자 추가 시 얼굴 인식 사용 동의 팝업이 표시되면 확인하고 진행하세요. 동의 완료 후 사용자 추가 다이얼로그에서 기본 정보를 입력하세요.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 화면 오른쪽 상단의 **추가** 버튼을 클릭하세요.

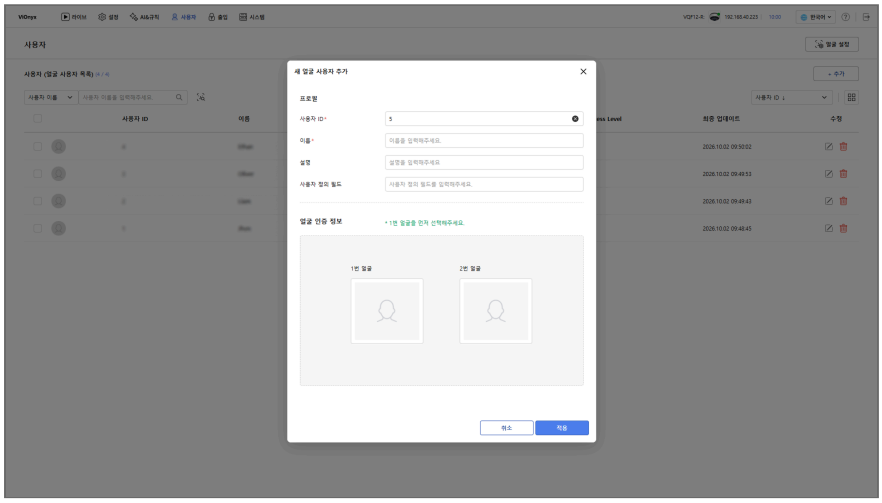


3. 최초 사용자 추가 시 **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업이 표시되면 내용을 확인하고, 동의 체크박스를 클릭한 후 **동의하고 얼굴 인증 기능 활성화** 버튼을 클릭하세요.



- 얼굴 인식 기능을 사용하려면 해당 지역의 관련 법규를 준수해야 합니다. 동의하지 않으면 진행할 수 없습니다.
- **Vionyx 얼굴 인증 기능 활성화 안내 및 동의** 팝업은 최초 한 번만 표시됩니다.

4. **새 얼굴 사용자 추가** 팝업창이 나타나면 사용자 기본 정보를 입력하세요.



5. **사용자 ID** 입력 필드에 사용자 고유 아이디를 입력하세요. 사용자 아이디는 다른 사용자와 중복될 수 없습니다.
6. **이름** 입력 필드에 사용자 이름을 입력하세요.
   - 최대 64자까지 입력할 수 있습니다.
   - 한글, 일본어, 영문 대소문자, 숫자, 특수문자(`#`, `-`, `_`, `.`, `(`, `)`), 문자 중간 공백을 포함할 수 있습니다.
7. **설명** 입력 필드에 사용자에 대한 설명을 입력하세요. 최대 256자까지 입력할 수 있습니다.
8. **사용자 정의 필드** 입력 필드는 사용자 고유의 추가 정보를 최대 64자까지 입력할 수 있습니다. 예를 들어, 부서, 직책, 유저 그룹 등 영문 형식 메모를 작성할 수 있습니다.

9. 사용자 기본 정보를 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
> 신규 사용자는 얼굴 사진 없이 먼저 생성할 수 있습니다. 추후 사용자 상세 페이지에서 얼굴 사진을 추가할 수 있습니다.

얼굴 등록

사용자를 새로 추가할 때나 사용자 상세 페이지에서 얼굴을 등록할 수 있습니다. 세 가지 방식이 제공됩니다.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 화면 오른쪽 상단의 **추가** 버튼을 클릭하거나 사용자 목록에서 기존 사용자를 클릭하여 상세 페이지로 이동하세요.
3. 사용자 추가 또는 사용자 상세 팝업창의 **얼굴 인증 정보** 섹션에서 얼굴을 등록할 수 있습니다.



4. **1번 얼굴**에 마우스를 오버하면 등록 옵션이 표시됩니다.



- : 로컬에 저장된 이미지 파일을 업로드하여 얼굴 사진을 등록할 수 있습니다.
- : 웹캠으로 얼굴 사진을 촬영하여 등록할 수 있습니다.

- : AI 이벤트를 통해 감지된 미인식 얼굴 목록에서 사용자에 맞는 얼굴을 선택하여 등록할 수 있습니다.

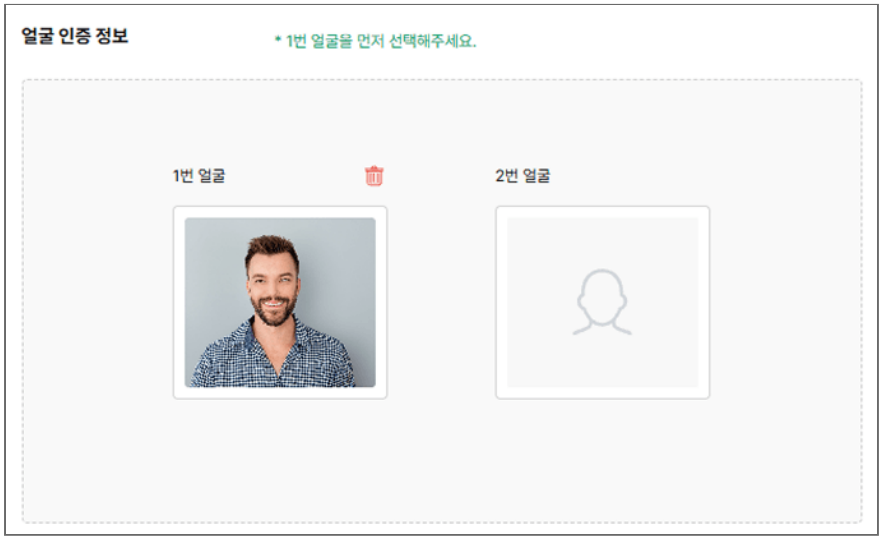
> **알아두기**
> 1번 얼굴을 먼저 선택하세요. 2번 얼굴은 선택 사항입니다.

얼굴 사진 업로드

로컬에 저장된 이미지 파일을 업로드해 얼굴 사진을 등록할 수 있습니다.



1. 다음 중 원하는 방법으로 얼굴 사진을 업로드하세요.
   - 로컬에 저장된 이미지 파일을 드래그 앤 드롭으로 얼굴 영역에 끌어오세요.
   - 로컬에 저장된 이미지 파일을 선택하려면 버튼을 클릭하고 원하는 이미지 파일을 선택하세요.
2. 얼굴이 인식되면 사진이 표시됩니다.



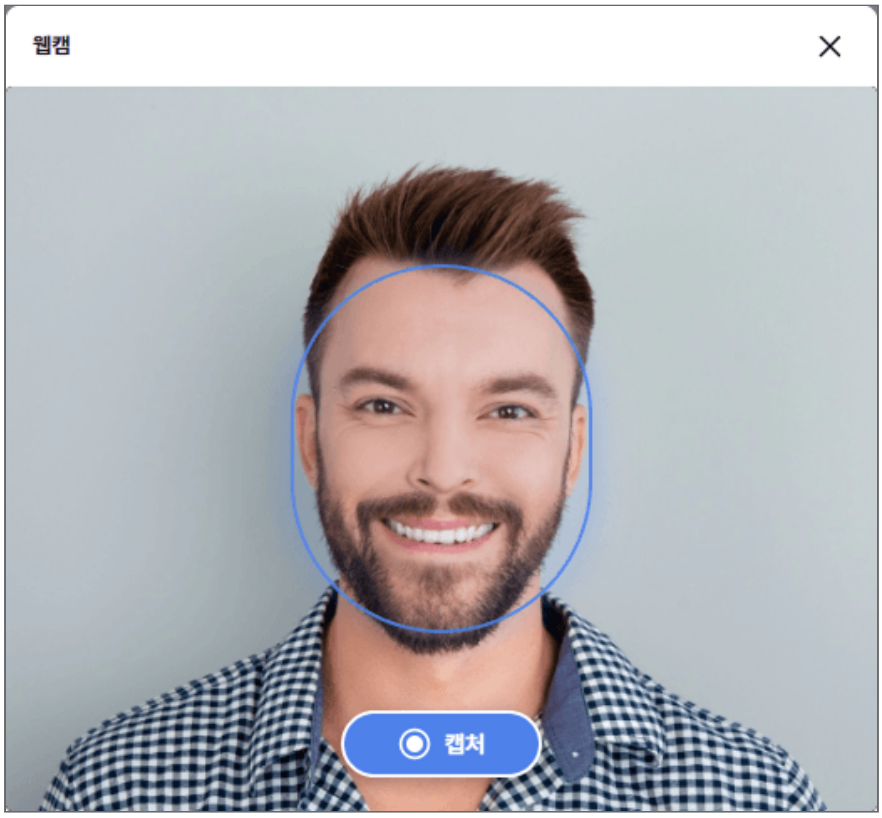
3. 업로드한 사진을 사용자에게 적용하려면 하단의 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 지원하는 이미지 파일은 PNG, JPEG, JPG 형식입니다.
> - 지원하는 이미지 파일의 최대 크기는 10MB입니다.

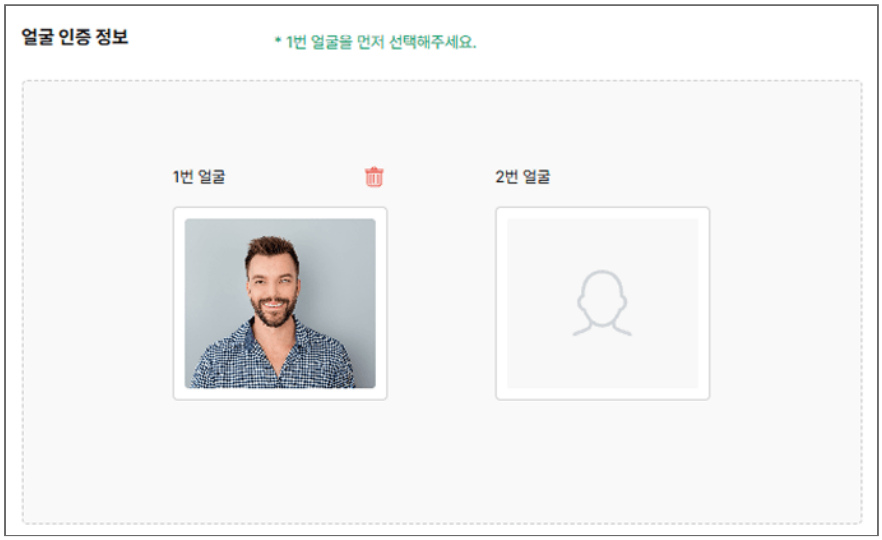
웹캠으로 얼굴 등록

웹캠을 사용해 얼굴 사진을 촬영하고 등록할 수 있습니다.

1. 버튼을 클릭하세요.
2. 웹캠 촬영 화면이 표시되면 얼굴이 화면 중앙의 원안에 오도록 위치를 조정하세요.



3. **캡처** 버튼을 클릭하세요.



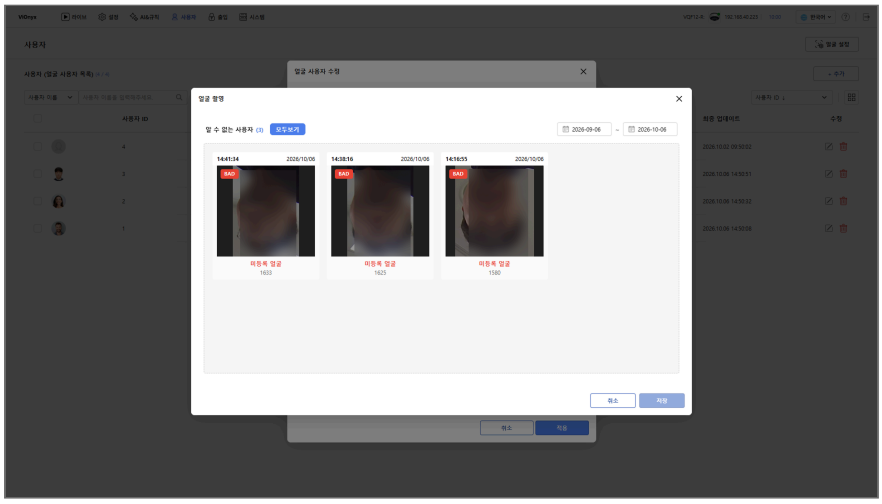
4. 촬영한 사진을 사용자에게 적용하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
> 다시 촬영하려면 얼굴 사진을 클릭하고 다시 촬영할 수 있습니다.

AI 추천 얼굴 등록

AI 분석을 통해 감지된 미등록 얼굴 목록에서 사용자에 맞는 얼굴을 선택하고 등록할 수 있습니다.

1. 버튼을 클릭하세요.
2. **얼굴 촬영** 팝업창에서 최근 인증된 미등록 얼굴 목록이 표시됩니다.



등록 가능 얼굴 목록이 표시되지 않으면 **모두보기** 버튼을 클릭하세요. 미등록 얼굴을 모두 확인할 수 있습니다.

3. 사용자에 맞는 얼굴을 선택하세요. 한 번에 1개의 얼굴만 선택할 수 있습니다.
4. **저장** 버튼을 클릭하세요.
5. 선택한 얼굴을 사용자에게 적용하려면 **적용** 버튼을 클릭하세요.

사용자 수정 및 삭제하기

등록된 사용자의 정보를 편집하거나 얼굴을 추가/변경할 수 있습니다. 또한 더 이상 필요하지 않은 사용자를 삭제할 수 있으며, 사용자의 활동 이력을 이벤트 로그로 확인할 수 있습니다.

아래와 같은 상황에서 사용자 수정 및 삭제하세요.

- 사용자의 이름, 소속 부서 등 정보를 변경해야 할 때
- 사용자의 얼굴 사진을 업데이트하거나 새로운 얼굴을 추가해야 할 때
- 사용자가 퇴사하거나 시스템에서 제거해야 할 때
- 사용자의 인증 기록 및 변경 이력을 확인하고 싶을 때
- 등록된 사용자에 대해 오인증이 발생할 때

알아두기

- 사용자 정보 수정으로 고품질 사진을 업로드해도 이전 템플릿 데이터가 남아있을 수 있으므로, 사용자 삭제 후 재등록을 권장합니다.
- 삭제 작업은 되돌릴 수 없습니다. 사용자를 삭제하기 전에 필요한 데이터를 백업하고 신중하게 확인하세요.

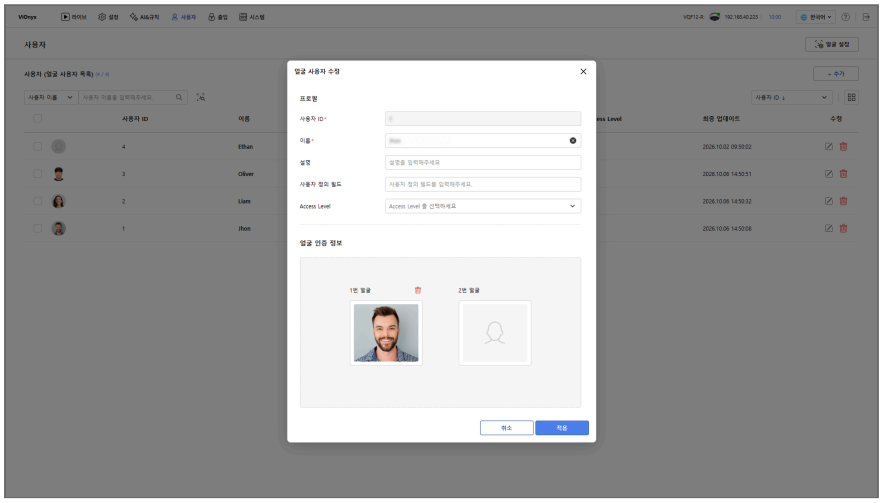
사용자 정보 수정

등록된 사용자의 정보를 편집하거나 얼굴을 추가/변경할 수 있습니다.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 수정할 사용자의 **수정** 열에서 버튼을 클릭하세요.



3. **얼굴 사용자 수정** 창이 나타나면 필요한 정보를 수정하세요.



4. 사용자 정보 수정을 완료하면 **적용** 버튼을 클릭하세요.

수정을 완료하면 오른쪽 상단에 성공 메시지가 나타나며 사용자 목록으로 돌아갑니다.

알아두기

- 사용자 상세 정보에 대한 자세한 내용은 사용자 추가하기를 참고하세요.
- **사용자 ID**는 수정할 수 없습니다.
- 얼굴 사진은 개별적으로 삭제할 수 있습니다. 해당 얼굴 사진 오른쪽 상단의 버튼을 클릭하세요.

사용자 삭제

더 이상 필요하지 않은 사용자를 삭제할 수 있습니다.

개별 사용자 삭제

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 삭제할 사용자의 가장 오른쪽에 있는 버튼을 클릭하세요.



3. 삭제 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

화면 오른쪽 상단에 삭제 확인 메시지가 나타나며 사용자 목록에서 해당 사용자가 제거됩니다.

여러 사용자 일괄 삭제

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 삭제할 사용자의 가장 왼쪽에 있는 체크박스를 클릭하세요. 여러 사용자를 선택할 수 있습니다.



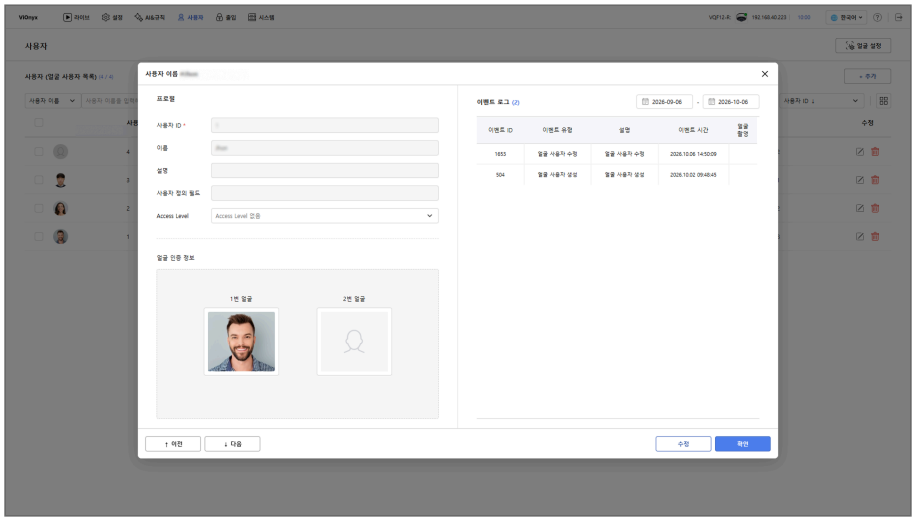
3. 화면 오른쪽 상단의 삭제 버튼이 표시되면, **삭제** 버튼을 클릭하세요.
4. 삭제 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요.

화면 오른쪽 상단에 삭제 확인 메시지가 나타나며 사용자 목록에서 해당 사용자가 제거됩니다.

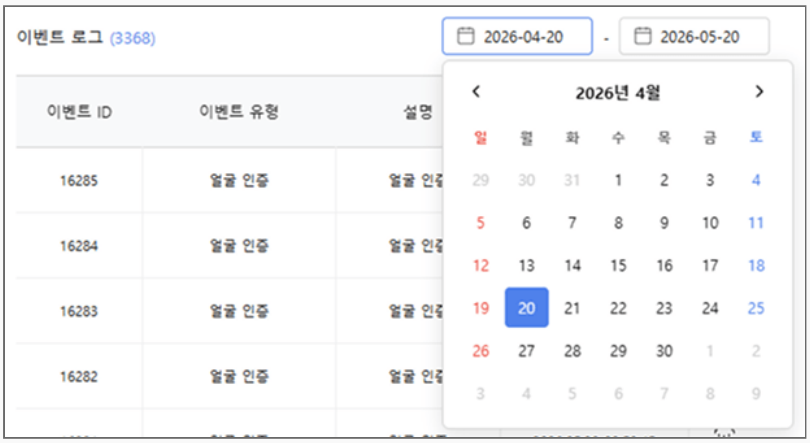
사용자 이벤트 로그 확인

등록된 사용자의 활동 이력을 이벤트 로그로 확인할 수 있습니다.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록에서 이벤트 로그를 확인할 사용자를 클릭하세요.
3. 사용자 상세 정보 팝업이 나타나면 오른쪽에 **이벤트 로그**에서 이벤트 목록을 확인할 수 있습니다.



- 오른쪽 상단에서 달력 아이콘을 사용하여 특정 날짜의 이벤트를 조회할 수 있습니다.



- 이벤트 로그는 자동 기록되며, 사용자의 모든 중요한 활동을 추적할 수 있습니다.

사용자 검색 및 보기

사용자 목록에서 이름이나 아이디를 입력하여 원하는 사용자를 신속하게 찾을 수 있습니다. 필요에 따라 테이블 또는 카드 형태로 사용자 정보를 표시할 수 있습니다.

아래와 같은 상황에서 사용자 검색 및 보기 기능을 사용하세요.

- 많은 사용자 중에서 특정 사용자를 빠르게 찾아야 할 때
- 카드 형태로 사용자 프로필을 한눈에 확인하고 싶을 때
- 사용자 목록을 이름, 아이디, 최종 업데이트 시간 기준으로 정렬하여 보고 싶을 때

사용자 검색

원하는 사용자를 찾을 수 있는 검색 기능을 제공합니다. 사용자 이름이나 아이디를 기준으로 검색할 수 있으며, 얼굴 이미지로 유사한 사용자를 찾을 수 있습니다.

키워드 검색

사용자 목록에서 이름이나 아이디를 입력하여 원하는 사용자를 검색할 수 있습니다.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 사용자 목록 왼쪽 상단의 검색 입력에서 검색 기준을 선택하세요. **사용자 이름** 또는 **사용자 ID**를 선택할 수 있습니다.



3. 검색 입력 필드에 검색어를 입력하세요.



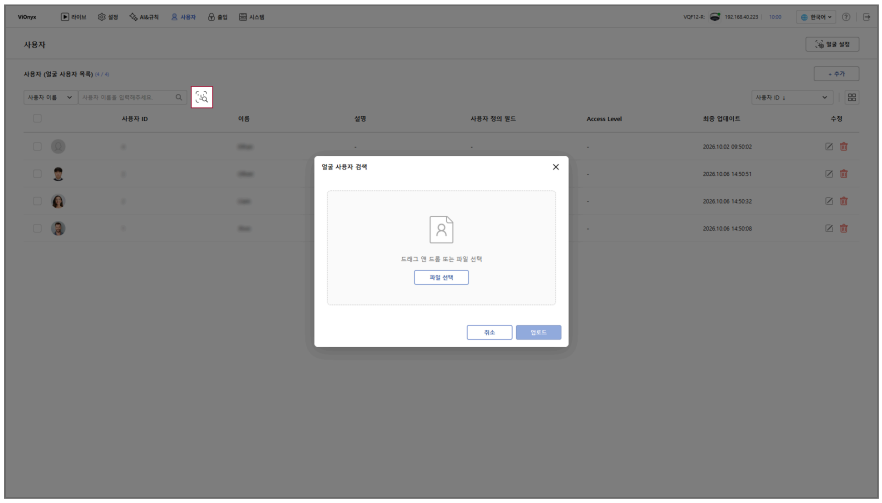
4. 입력한 검색어와 일치하는 사용자가 목록에 표시됩니다.

> **알아두기**
>
> - 부분 검색을 지원합니다. 예를 들어, 'Kim'이라고 입력하면 이름에 'Kim'을 포함한 모든 사용자가 표시됩니다.
> - 검색 결과는 현재 선택된 필터 기준에 따라 표시됩니다. 필터를 변경하면 검색 결과도 함께 업데이트됩니다.

얼굴 이미지로 찾기

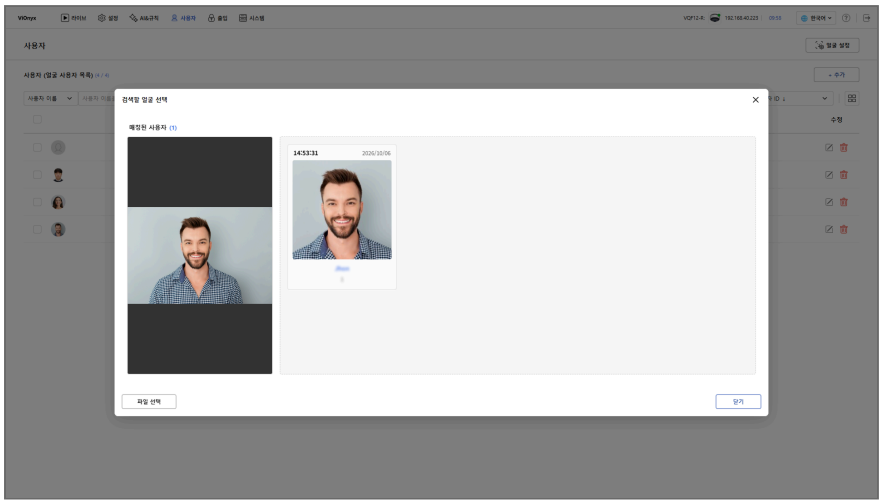
얼굴 이미지를 업로드하여 유사한 얼굴을 가진 사용자를 검색할 수 있습니다.

1. 화면 왼쪽 상단의 **사용자** 메뉴를 클릭하세요.
2. 검색 입력 필드 오른쪽의 버튼을 클릭하세요.
3. **얼굴 사용자 검색** 창이 나타나면 얼굴 이미지를 드래그 앤 드롭하거나 **파일 선택**을 통해 업로드하세요.



4. 얼굴 이미지 업로드를 완료하면 **업로드** 버튼을 클릭하세요.

5. **검색할 얼굴 선택** 창이 나타나면 업로드한 얼굴 이미지와 매칭된 사용자 목록이 표시됩니다.



- 매칭된 사용자 중에서 원하는 사용자를 선택하면 해당 사용자의 상세 정보 페이지로 이동할 수 있습니다.
- 다른 얼굴 이미지로 다시 검색하려면 왼쪽 하단의 **파일 선택** 버튼을 클릭하고, 새로운 얼굴 이미지를 업로드하세요.

> **알아두기**
> 얼굴 이미지가 아닌 다른 이미지를 업로드하면 올바른 얼굴 이미지가 아니라는 메시지가 표시됩니다. 얼굴 이미지로 다시 시도하세요.

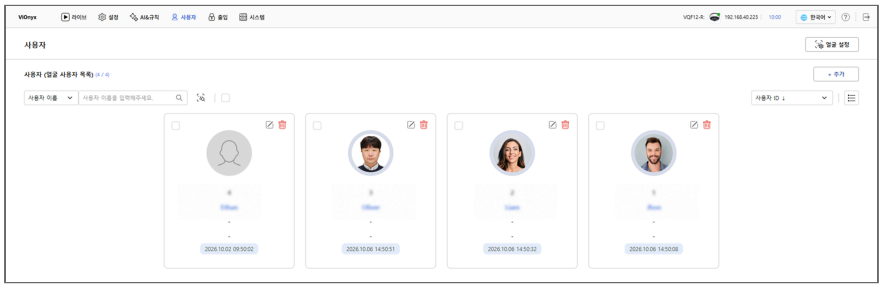
뷰 모드 변경

사용자 목록을 테이블 형태 또는 카드 형태로 표시할 수 있습니다. 사용자 목록 오른쪽 상단의 ☰ 또는 ▦ 버튼을 클릭해 원하는 뷰 모드를 선택하세요.

- **목록 보기로 전환**



- **그리드 보기로 전환**



> **알아두기**
>
> **목록 보기로 전환**, **그리드 보기로 전환**는 모두 동일한 기능을 제공합니다. 표시 방식만 다르며, 검색 및 필터, 정렬 결과는 동일합니다.

사용자 목록 정렬

사용자 목록을 사용자 이름, 아이디, 최종 업데이트 시간 기준으로 오름차순 또는 내림차순으로 정렬할 수 있습니다.

1. 사용자 목록 오른쪽 상단의 정렬 드롭다운 옵션을 클릭하세요.



2. 원하는 정렬 기준을 선택하세요.

출입 통제 관리하기

출입 메뉴에서는 카메라에 연결된 출입문을 등록하고, 어떤 사용자가 언제 출입할 수 있는지 출입 레벨로 지정할 수 있습니다. 출입 통제 이벤트가 얼굴 인식으로 출입 허용 여부를 판단하면, 카메라는 출입문에 연결된 릴레이를 열어 출입을 허용합니다. 출입문의 실시간 상태를 확인하고 원격으로 열거나 잠글 수 있으며, 출입 판단 결과에 따라 음성 안내나 웹훅 알림을 실행하도록 설정할 수도 있습니다. 출입 통제를 처음 설정할 때는 출입 통제 이벤트를 먼저 생성한 후 출입문, 출입 레벨, 출입문 규칙 순서로 설정하세요.

알아두기

- **출입** 메뉴는 펌웨어 버전 1.1.0 이상에서 지원합니다.
- **출입** 메뉴는 베타 버전으로 제공되며, 이후 펌웨어 업데이트에서 화면 구성과 동작이 변경될 수 있습니다.

출입문 관리하기

카메라를 통해 실제로 열고 잠글 출입문을 등록할 수 있습니다. 출입문을 등록할 때 어떤 출입 통제 이벤트로 출입을 판단할지, 어떤 릴레이로 잠금 장치를 제어할지, 출입문을 얼마 동안 열어 둘지를 함께 지정합니다. 출입문을 등록해야 출입 레벨과 출입문 규칙에서 해당 출입문을 선택할 수 있습니다.

아래와 같은 상황에서 출입문을 등록하세요.

- 얼굴 인식으로 출입이 허용된 사용자에게 출입문을 자동으로 열어 줄 때
- 퇴실 버튼을 눌러 안쪽에서 출입문을 열 수 있게 할 때
- 출입문이 열려 있는지 닫혀 있는지 센서로 확인할 때
- 업무 시간에는 출입문을 계속 열어 두고, 야간에는 잠가 두는 등 시간대별로 출입문을 운영할 때

시작하기 전에

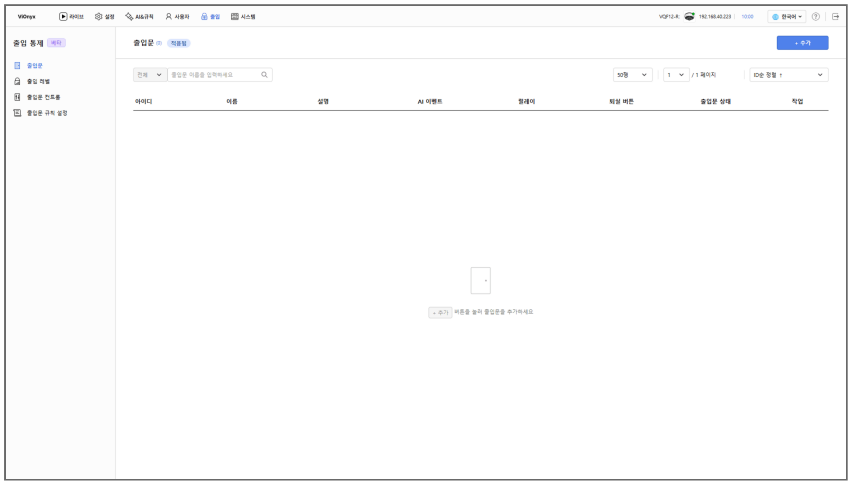
출입문을 등록하기 전에 아래 사항을 확인하세요.

- 카메라당 출입문을 최대 10개까지 등록할 수 있습니다. 카메라가 제어할 출입문 수를 미리 확인하세요.
- 출입 판단에 사용할 출입 통제 이벤트를 먼저 생성하세요. 자세한 내용은 출입 통제 이벤트 설정하기를 참고하세요.
- 출입문 잠금 장치가 카메라 또는 하위 I/O 장치의 릴레이 포트에 연결되어 있는지 확인하세요. 하위 I/O 장치를 사용하려면 먼저 RS-485로 장치를 등록해야 합니다. 자세한 내용은 RS-485 설정하기를 참고하세요.
- 퇴실 버튼이나 출입문 상태 센서를 사용하려면 해당 장치가 입력 포트에 연결되어 있는지 확인하세요.
- 개방 일정이나 잠금 일정을 사용하려면 일정을 미리 만들어 두세요. 자세한 내용은 일정 관리하기를 참고하세요.

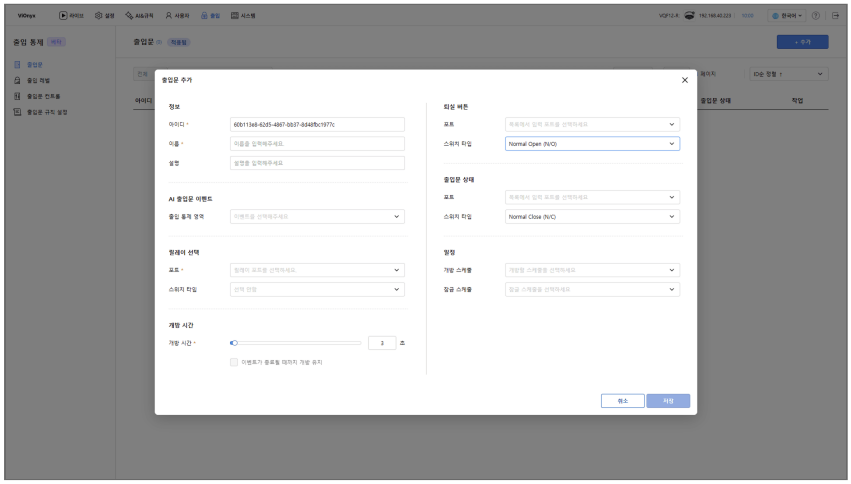
출입문 추가

1 출입문 추가 시작

1. 화면 왼쪽 상단의 **출입** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입문**을 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
4. **출입문 추가** 팝업이 나타나면 출입문 정보를 입력하세요. 필수 항목을 모두 입력해야 **저장** 버튼이 활성화됩니다.



2 기본 정보 입력

정보 섹션에서 출입문을 구분할 정보를 입력하세요.

- **아이디**: 출입문의 고유 ID입니다. 자동으로 입력되며, 필요하면 변경할 수 있습니다. 다른 출입문과 같은 ID는 사용할 수 없습니다. 최대 64자까지 입력할 수 있으며, 영문 및 숫자, 하이픈(`-`), 언더스코어(`_`)를 사용할 수 있습니다.
- **이름**: 출입문 이름을 입력하세요. 필수 항목이며, 다른 출입문과 같은 이름은 사용할 수 없습니다. **정문**, **2층 사무실** 처럼 위치를 알 수 있는 이름을 지정하면 출입 레벨과 규칙에서 출입문을 쉽게 구분할 수 있습니다.
- **설명**: 출입문에 대한 설명을 입력하세요.

알아두기

- 출입문의 ID와 이름은 시스템 내에서 고유해야 하며, 이미 사용 중인 값은 사용할 수 없습니다.
- 출입문의 ID는 한번 저장하면 변경할 수 없습니다.

3 출입 통제 이벤트 연결

AI 출입문 이벤트 섹션의 **출입 통제 영역** 목록에서 이 출입문의 출입 판단에 사용할 출입 통제 영역을 선택하세요. 출입 통제 이벤트를 생성할 때 설정한 출입 통제 영역이 목록에 표시됩니다.

알아두기

- 하나의 출입 통제 영역은 출입문 하나에만 연결할 수 있습니다. 다른 출입문에 이미 연결된 영역은 선택할 수 없습니다.
- 출입문에 연결된 출입 통제 영역은 AI 이벤트 화면에서 삭제하거나 변경할 수 없습니다. 영역을 변경하려면 먼저 출입문에서 연결을 해제하세요.
- 출입 통제 이벤트 생성에 대한 자세한 내용은 출입 통제 이벤트 설정하기를 참고하세요.

4 릴레이 설정

릴레이 선택 섹션에서 출입문 잠금 장치를 제어할 릴레이를 설정하세요.

- **포트**: 출입문 잠금 장치가 연결된 릴레이 포트를 선택하세요. 필수 항목입니다. 카메라의 릴레이 포트와 하위 I/O 장치의 릴레이 포트를 선택할 수 있습니다. 다른 출입문이나 AI 규칙에서 사용 중인 포트는 선택할 수 없습니다.
- **스위치 타입**: 잠금 장치의 접점 타입을 선택하세요.
  - **Normal Open (N/O)**: 평상시 열려 있다가 릴레이가 동작하면 닫히는 접점입니다.
  - **Normal Close (N/C)**: 평상시 닫혀 있다가 릴레이가 동작하면 열리는 접점입니다.

주의

- **스위치 타입**은 출입문이 아니라 릴레이 포트에 적용되는 설정입니다. 출입문을 저장하면 해당 포트를 사용하는 모든 출입문과 규칙에 적용됩니다.
- 사용 중인 잠금 장치의 사양을 확인하고 올바른 **스위치 타입**을 선택하세요. 잘못 선택하면 평상시에 출입문이 열린 상태로 유지될 수 있습니다.

5 개방 시간 설정

개방 시간 섹션에서 출입이 허용되었을 때 출입문을 열어 둘 시간을 설정하세요.

- **개방 시간**: 슬라이더를 움직이거나 입력 필드에 값을 직접 입력할 수 있습니다. 1초부터 120초까지 설정할 수 있으며, 기본값은 3초입니다.

- **이벤트가 종료될 때까지 개방 유지**: 이 옵션을 선택하면 개방 시간과 관계없이 출입 통제 이벤트가 종료될 때까지 출입문을 열어 둡니다. 출입 통제 영역을 선택해야 이 옵션을 사용할 수 있습니다.

> **알아두기**
> 이벤트가 종료되는 시점은 출입 통제 이벤트의 **조건** 설정에 따라 달라집니다. 예를 들어, 미인가자가 뒤따라 들어올 때 즉시 출입문을 잠그려면 출입 통제 이벤트에서 **무인 또는 테일게이팅 조건 위반 시 즉시 해제**를 선택하세요. 자세한 내용은 출입 통제 이벤트 설정하기를 참고하세요.

6 퇴실 버튼 설정(선택 사항)

출입문 안쪽에 퇴실 버튼을 설치했다면 **퇴실 버튼** 섹션에서 버튼이 연결된 입력 포트를 설정하세요. 퇴실 버튼을 누르면 얼굴 인식 없이 출입문이 열립니다.

- **포트**: 퇴실 버튼이 연결된 입력 포트를 선택하세요.
- **스위치 타입**: 퇴실 버튼의 접점 타입을 선택하세요. 기본값은 **Normal Open (N/O)**입니다.
  - **Normal Open (N/O)**: 평상시 열려 있다가 릴레이가 동작하면 닫히는 접점입니다.
  - **Normal Close (N/C)**: 평상시 닫혀 있다가 릴레이가 동작하면 열리는 접점입니다.

7 출입문 상태 설정(선택 사항)

출입문에 개폐 센서를 설치했다면 **출입문 상태** 섹션에서 센서가 연결된 입력 포트를 설정하세요. 설정하면 **출입문 컨트롤** 화면에서 출입문이 열려 있는지 닫혀 있는지 확인할 수 있습니다.

- **포트**: 출입문 개폐 센서가 연결된 입력 포트를 선택하세요.
- **스위치 타입**: 센서의 접점 타입을 선택하세요. 기본값은 **Normal Close (N/C)**입니다.
  - **Normal Open (N/O)**: 평상시 열려 있다가 릴레이가 동작하면 닫히는 접점입니다.
  - **Normal Close (N/C)**: 평상시 닫혀 있다가 릴레이가 동작하면 열리는 접점입니다.

> **알아두기**
> - 퇴실 버튼과 출입문 상태 센서는 서로 다른 입력 포트에 연결해야 합니다.
> - 다른 출입문에서 사용 중인 입력 포트는 선택할 수 없습니다.

8 일정 설정(선택 사항)

일정 섹션에서 시간대에 따라 출입문을 계속 열어 두거나 잠가 둘 수 있습니다.

- **개방 스케줄**: 선택한 일정의 시간대에는 출입문을 계속 열어 둡니다. 방문객이 많은 업무 시간에 로비 출입문을 열어 둘 때 사용하세요.
- **잠금 스케줄**: 선택한 일정의 시간대에는 출입문을 계속 잠가 둡니다. 이 시간대에는 등록된 사용자도 출입할 수 없지만, 실내에 있는 사람은 퇴실 버튼으로 출입문을 열고 나갈 수 있습니다.

> **알아두기**
> 개방 일정과 잠금 일정에는 같은 일정을 선택할 수 없으며, 두 일정의 시간대가 겹치면 저장할 수 없습니다.

9 출입문 저장

모든 설정을 완료한 후 **저장** 버튼을 클릭하세요. 저장한 출입문은 출입문 목록에 추가되며, 출입 레벨과 출입문 규칙에서 선택할 수 있습니다.



출입문 목록 확인

출입문 목록에서 등록된 출입문과 각 출입문에 연결된 이벤트와 포트를 확인할 수 있습니다.



- 특정 출입문을 찾으려면 검색 필드(1)에 출입문 이름을 입력하세요.
- 한 페이지에 표시할 출입문 개수를 변경하려면 화면 오른쪽 상단의 행 수 목록(2)에서 원하는 값을 선택하세요.
- 정렬 기준을 변경하려면 **ID순 정렬**(3)에서 원하는 기준을 선택하세요.

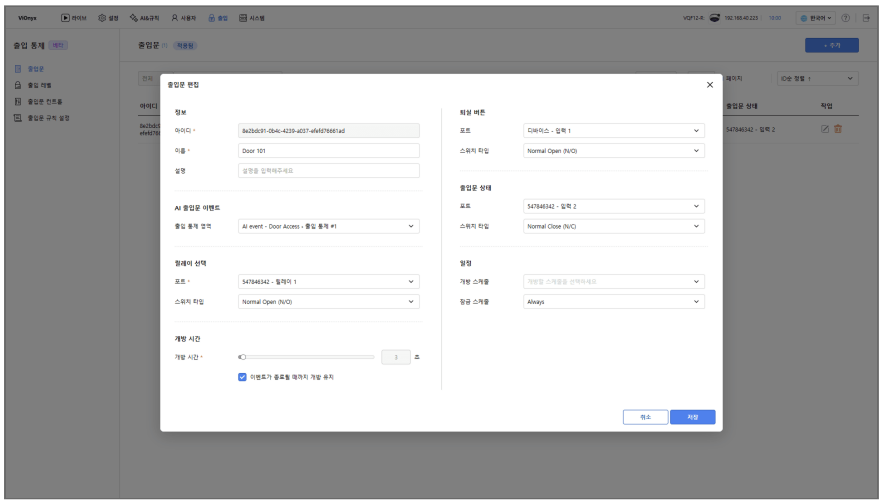
출입문 목록에 표시되는 항목은 다음과 같습니다.

항목	설명
아이디	출입문의 고유 ID입니다.
이름	출입문 이름입니다.
설명	출입문을 추가하거나 수정할 때 입력한 설명입니다.
AI 이벤트	출입문에 연결된 출입 통제 영역입니다.
릴레이	출입문 잠금 장치를 제어하는 릴레이 포트입니다.
퇴실 버튼	퇴실 버튼이 연결된 입력 포트입니다.
출입문 상태	출입문 개폐 센서가 연결된 입력 포트입니다.

항목	설명
작업	출입문을 수정( )하거나 삭제( )할 수 있는 기능을 제공합니다.

출입문 수정

1. 출입문 목록에서 수정하려는 출입문의 오른쪽에 있는 버튼을 클릭하세요.
2. **출입문 편집** 팝업이 나타나면 원하는 항목을 수정하세요.



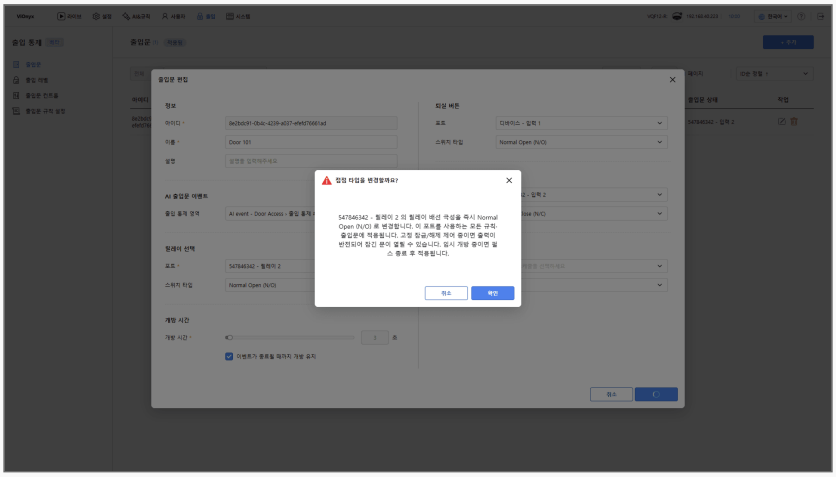
3. 수정한 내용을 저장하려면 **저장** 버튼을 클릭하세요.

수정한 내용을 저장하면, 즉시 해당 출입문을 사용하는 출입 레벨과 출입문 규칙에 적용됩니다.

> **주의**
> 출입문이 수동 잠금 또는 수동 잠금 해제 상태일 때 릴레이의 **스위치 타입**을 변경하면 릴레이 출력이 반전되어 잠긴 출입문이 열릴 수 있습니다. 변경하기 전에 **출입문 컨트롤** 메뉴에서 수동으로 제어하세요.

알아두기

릴레이의 **스위치 타입**을 변경하고 **저장** 버튼을 클릭하면 확인 메시지가 나타납니다.



- **확인** 버튼을 클릭하면 확인 메시지가 닫히고, 변경한 접점 타입이 릴레이 포트에 즉시 적용됩니다. 해당 포트를 사용하는 모든 출입문과 규칙에도 함께 적용됩니다.
- **취소** 버튼을 클릭하면 접점 타입은 변경되지 않고, 함께 수정한 다른 항목만 저장됩니다.
- 출입문이 일시적으로 열려 있는 동안 변경하면 개방 시간이 끝난 후에 적용됩니다.

출입문 삭제

1. 출입문 목록에서 삭제하려는 출입문의 오른쪽에 있는 버튼을 클릭하세요.
2. 확인 메시지가 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요.

출입문을 삭제하면 연결된 출입 통제 이벤트와 출입 레벨에서 연결이 해제됩니다. 삭제한 출입문은 **출입문 컨트롤** 목록에서도 사라지며, 복구할 수 없습니다.

알아두기

- 출입 레벨, 출입문 규칙에서 사용 중인 출입문을 삭제하면 출입 레벨과 출입문 규칙도 함께 삭제됩니다.
- 출입문을 추가, 수정, 삭제하려면 **읽기/쓰기** 권한이 필요합니다. 권한이 없으면 관리자에게 문의하세요. 운영자 권한에 대한 자세한 내용은 운영자 관리하기를 참고하세요.

다음 단계

출입문을 등록했다면 출입 레벨을 만들어 어떤 사용자가 언제 출입할 수 있는지 지정하세요.

출입 레벨 관리하기

출입 레벨은 **어떤 사용자**가 **어느 출입문**을 **언제** 출입할 수 있는지 하나로 묶은 출입 권한입니다. 출입 통제 이벤트에서 얼굴 인식으로 식별된 사용자라도, 해당 출입문의 출입 레벨에 배정되어 있지 않거나 출입 시간이 아니면 출입할 수 없습니다.

아래와 같은 상황에서 출입 레벨을 만드세요.

- 특정 부서나 팀원만 출입문에 출입할 수 있게 할 때
- 평일 업무 시간에만 출입을 허용하는 등 사용자 그룹별로 출입 시간을 다르게 지정할 때
- 야간 근무자처럼 특정 시간대에만 출입하는 사용자에게 별도 권한을 줄 때

시작하기 전에

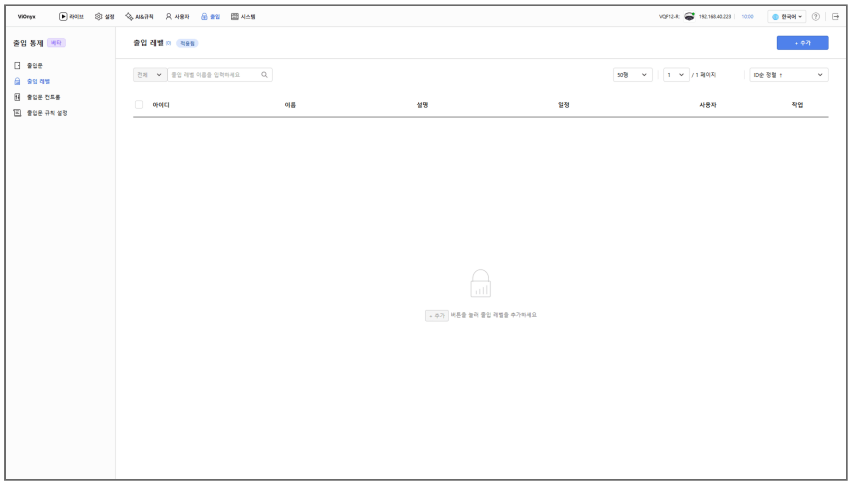
출입 레벨을 만들기 전에 아래 사항을 확인하세요.

- 출입 레벨에 지정할 출입문을 먼저 등록하세요. 자세한 내용은 출입문 관리하기를 참고하세요.
- 출입 레벨에 배정할 사용자를 얼굴 사용자로 등록하세요. 자세한 내용은 사용자 추가하기를 참고하세요.
- 출입 시간을 제한하려면 일정을 미리 만들어 두세요. 일정을 만들지 않으면 기본 제공되는 Always 일정을 사용할 수 있습니다. 자세한 내용은 일정 관리하기를 참고하세요.

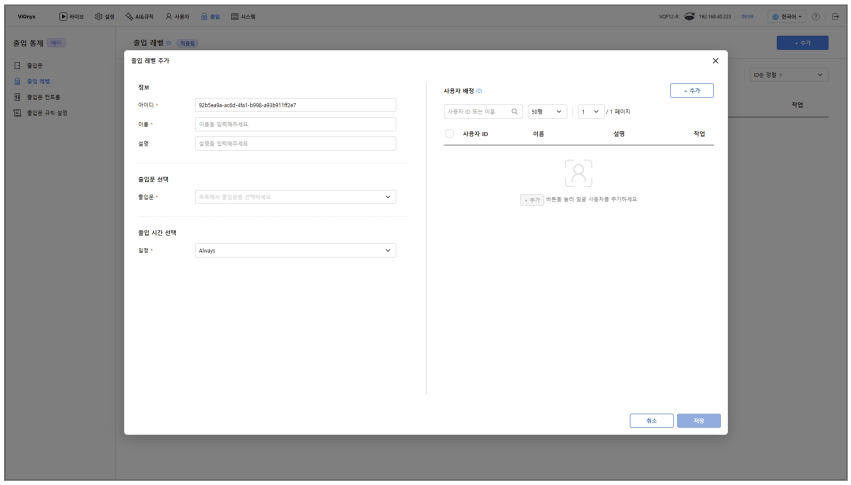
출입 레벨 추가

1 출입 레벨 추가 시작

1. 화면 왼쪽 상단의 **출입** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입 레벨**을 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
4. **출입 레벨 추가** 팝업이 나타나면 출입 레벨 정보를 입력하고, 사용자를 배정하세요.



2 기본 정보 입력

정보 섹션에서 출입 레벨을 구분할 정보를 입력하세요.

- **아이디**: 출입 레벨의 고유 ID입니다. 자동으로 입력되며, 필요하면 변경할 수 있습니다. 다른 출입 레벨과 같은 ID는 사용할 수 없습니다. 최대 64자까지 입력할 수 있으며, 영문 및 숫자, 하이픈(`-`), 언더스코어(`_`)를 사용할 수 있습니다.
- **이름**: 출입 레벨 이름을 입력하세요. 필수 항목이며, 다른 출입 레벨과 같은 이름은 사용할 수 없습니다. **개발팀 상시 출입, 야간 근무자**처럼 대상과 시간을 알 수 있는 이름을 지정하세요.
- **설명**: 출입 레벨에 대한 설명을 입력하세요.

3 출입문 선택

출입문 선택 섹션의 **출입문** 목록에서 출입을 허용할 출입문을 선택하세요. 필수 항목입니다. 1개 이상의 출입문을 선택할 수 있습니다.

> **알아두기**
> 등록된 출입문이 없으면 목록에서 출입문을 선택할 수 없습니다. **출입** → **출입문**에서 출입문을 먼저 등록하세요. 출입문 등록에 대한 자세한 내용은 출입문 관리하기를 참고하세요.

4 출입 시간 선택

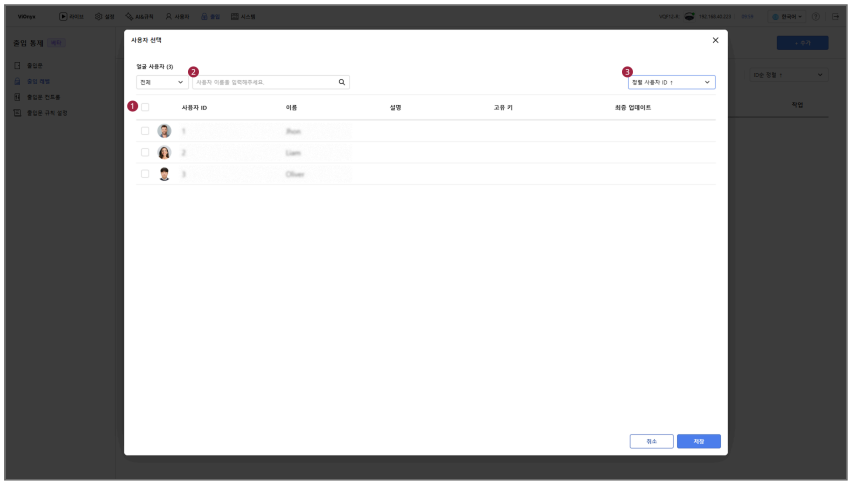
출입 시간 선택 섹션의 **일정** 목록에서 출입을 허용할 일정을 선택하세요. 필수 항목이며, 기본값은 **Always**입니다. 선택한 일정의 시간대에만 출입이 허용되며, 그 밖의 시간에는 등록된 사용자도 출입이 거부됩니다.

> **알아두기**
> 일정 관리에 대한 자세한 내용은 일정 관리하기를 참고하세요.

5 사용자 배정

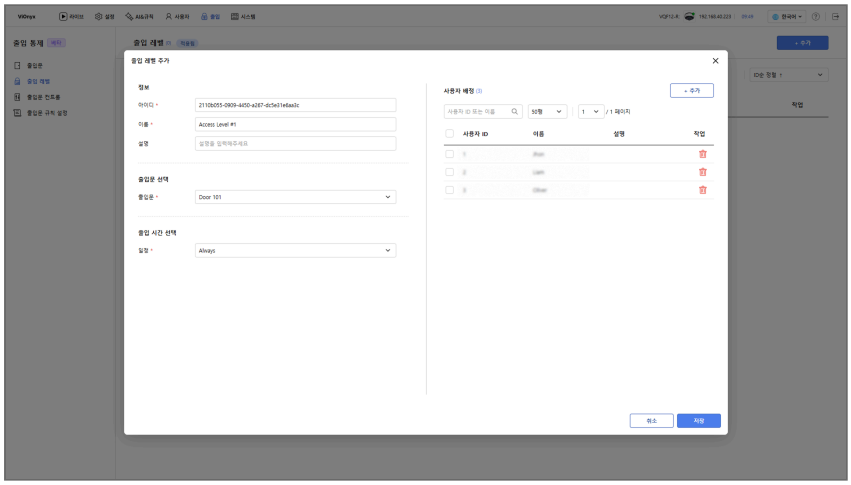
사용자 배정 섹션에서 출입 레벨을 적용할 사용자를 추가하세요.

1. **사용자 배정** 섹션 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.
2. **사용자 선택** 팝업이 나타나면 배정할 사용자의 체크박스를 클릭하세요.



- 목록의 모든 사용자를 선택하려면 목록 머리글의 체크박스(1)를 선택하세요.
- 특정 사용자를 찾으려면 검색 필드(2)에 사용자 이름을 입력하세요.
- 정렬 기준을 변경하려면 정렬 목록(3)에서 원하는 기준을 선택하세요.

3. **저장** 버튼을 클릭하세요. 선택한 사용자가 **사용자 배정** 목록에 추가됩니다.



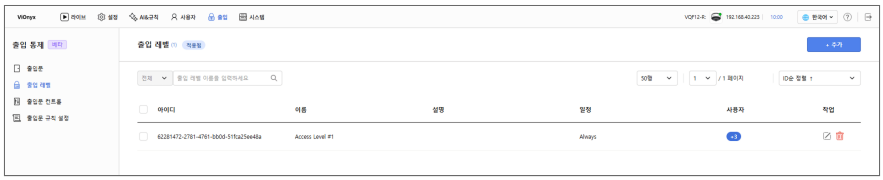
배정한 사용자를 출입 레벨에서 제외하려면 **사용자 배정** 목록에서 해당 사용자의 버튼을 클릭하세요.

알아두기

- **사용자 선택** 목록에는 얼굴 사용자로 등록된 사용자만 표시됩니다.
- 사용자 한 명은 여러 출입 레벨에 배정할 수 있습니다. 사용자당 배정할 수 있는 출입 레벨 개수에는 제한이 있습니다.

6 출입 레벨 저장

모든 설정을 완료한 후 **저장** 버튼을 클릭하세요. 저장한 출입 레벨은 출입 레벨 목록에 추가되며, 배정한 사용자에게 즉시 적용됩니다.



출입 레벨 목록 확인

출입 레벨 목록에서 등록된 출입 레벨과 각 출입 레벨의 출입 시간, 배정된 사용자를 확인할 수 있습니다.



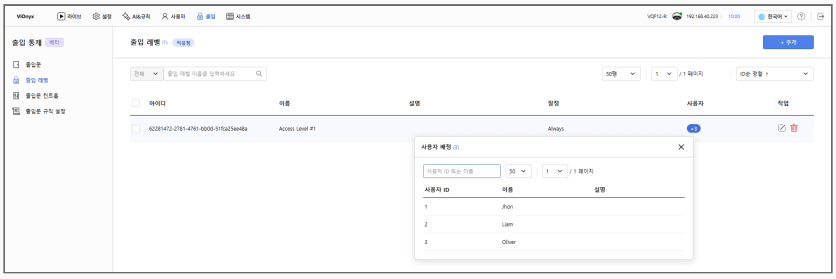
- 특정 출입 레벨을 찾으려면 검색 필드(1)에 출입 레벨 이름을 입력하세요.
- 한 페이지에 표시할 출입 레벨 개수를 변경하려면 화면 오른쪽 상단의 행 수 목록(2)에서 원하는 값을 선택하세요.
- 정렬 기준을 변경하려면 **ID순 정렬**(3)에서 원하는 기준을 선택하세요.

출입 레벨 목록에 표시되는 항목은 다음과 같습니다.

항목	설명
아이디	출입 레벨의 고유 ID입니다.
이름	출입 레벨 이름입니다.
설명	출입 레벨을 추가하거나 수정할 때 입력한 설명입니다.
일정	출입을 허용하는 일정입니다.
사용자	출입 레벨에 배정된 사용자 수입니다.
작업	출입 레벨을 수정( )하거나 삭제( )할 수 있는 기능을 제공합니다.

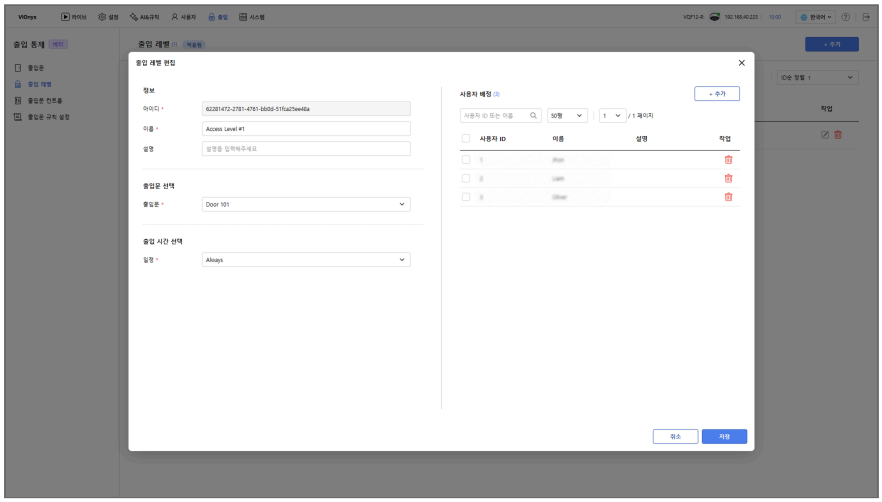
알아두기

사용자 항목의 숫자를 클릭하면 배정된 사용자 목록을 확인할 수 있습니다.



출입 레벨 수정

1. 출입 레벨 목록에서 수정하려는 출입 레벨의 오른쪽에 있는 버튼을 클릭하세요.
2. **출입 레벨 편집** 팝업이 나타나면 출입문, 출입 시간, 배정된 사용자 등을 수정하세요.



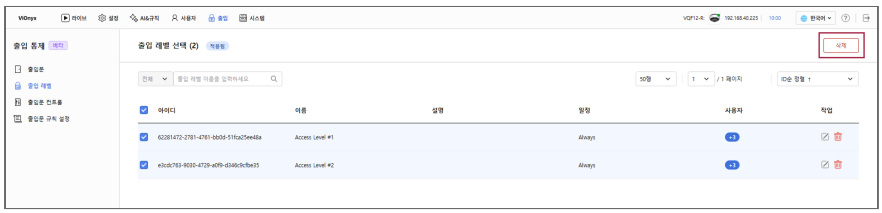
3. 수정한 내용을 저장하려면 **저장** 버튼을 클릭하세요.

수정한 내용은 저장하는 즉시 배정된 모든 사용자에게 적용됩니다.

출입 레벨 삭제

출입 레벨을 하나씩 삭제하거나, 여러 개를 선택하여 한 번에 삭제할 수 있습니다.

- **하나씩 삭제**: 출입 레벨 목록에서 삭제하려는 출입 레벨의 오른쪽에 있는 버튼을 클릭하세요.
- **여러 개 삭제**: 출입 레벨 목록에서 삭제하려는 출입 레벨의 체크박스를 선택한 후, 화면 오른쪽 상단의 **삭제** 버튼을 클릭하세요.



확인 메시지가 나타나면 내용을 확인하고 **확인** 버튼을 클릭하세요. 출입 레벨을 삭제하면 배정된 모든 사용자에게서 해당 출입 레벨이

해제됩니다. 출입문과 사용자는 삭제되지 않습니다. 삭제한 출입 레벨은 복구할 수 없습니다.

> **주의**
> 출입 레벨을 삭제하면 해당 출입 레벨로만 출입하던 사용자는 더 이상 출입문을 출입할 수 없습니다. 삭제하기 전에 배정된 사용자를 확인하세요.

다음 단계

출입 판단 결과에 따라 음성 안내, 웹훅 알림, 비상등 같은 추가 동작을 실행하려면 출입문 규칙을 설정하세요.

출입문 제어하기

출입문 컨트롤 메뉴에서는 등록된 출입문의 잠금 상태를 실시간으로 확인하고, 원격으로 출입문을 열거나 잠글 수 있습니다.

아래와 같은 상황에서 출입문을 직접 제어하세요.

- 얼굴이 등록되지 않은 방문객이나 택배 기사를 위해 출입문을 한 번 열어 줄 때
- 행사나 이사와 같은 상황에서 출입문을 계속 열어 둘 때
- 비상 상황에서 일정과 관계없이 출입문을 즉시 잠가야 할 때

> **알아두기**
> - 출입문을 제어하려면 운영자 권한이 필요합니다. 권한이 없으면 출입문 상태 확인과 제어 기능을 사용할 수 없습니다. 운영자 권한에 대한 자세한 내용은 운영자 관리하기를 참고하세요.
> - 출입문 추가 및 관리에 대한 자세한 내용은 출입문 관리하기를 참고하세요.

출입문 상태 확인

1. 화면 왼쪽 상단의 **출입** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입문 컨트롤**을 클릭하세요.



출입문 메뉴에 등록된 출입문이 목록에 표시됩니다. 출입문을 추가하거나 삭제하면 목록에도 바로 반영됩니다.

- 특정 출입문을 찾으려면 검색 필드(1)에 출입문 이름을 입력하세요.
- 한 페이지에 표시할 출입문 개수를 변경하려면 화면 오른쪽 상단의 행 수 목록(2)에서 원하는 값을 선택하세요.

- 정렬 기준을 변경하려면 **ID순 정렬**(3)에서 원하는 기준을 선택하세요.

출입문 목록에 표시되는 항목은 다음과 같습니다.

항목	설명
아이디	출입문의 고유 ID입니다.
이름	출입문 이름입니다.
설명	출입문을 추가하거나 수정할 때 입력한 설명입니다.
릴레이 상태	출입문 잠금 장치의 현재 상태입니다.
출입문 센서	출입문 센서의 현재 상태입니다. 출입문에 **출입문 상태** 입력 포트를 설정한 경우에만 표시됩니다.
제어	출입문을 열거나 수동 잠금 또는 수동 잠금 해제할 수 있는 기능을 제공합니다.

릴레이 상태

릴레이 상태 열에는 출입문이 잠겨 있는지와 함께 그 상태가 무엇에 의해 결정되었는지 표시됩니다.

상태	설명
잠김	평상시 잠긴 상태입니다.
잠금 해제	평상시 잠금 해제된 상태입니다.
스케줄 잠금	출입문의 잠금 일정에 따라 잠긴 상태입니다.
스케줄 잠금 해제	출입문의 개방 일정에 따라 잠금 해제된 상태입니다.
고정 잠김	**수동 잠금**으로 잠근 상태입니다.
고정 잠금 해제	**수동 잠금 해제**로 잠금 해제한 상태입니다.

출입문 제어

제어 열의 버튼을 클릭하여 출입문을 제어하세요.

버튼	동작
출입문 열기	출입문을 한 번 엽니다. 출입문에 설정한 개방 시간이 지나면 다시 잠깁니다.
수동 잠금 해제	출입문을 잠금 해제하고, **해제** 기능을 실행할 때까지 계속 열어 둡니다.

버튼	동작
수동 잠금	출입문을 잠그고, **해제** 기능을 실행할 때까지 계속 잠가 둡니다. 이 동안에는 등록된 사용자도 출입할 수 없으며, 퇴실 버튼으로도 출입문을 열 수 없습니다.
해제	**수동 잠금** 또는 **수동 잠금 해제**를 끝내고, 출입문을 수동 제어 이전 상태로 되돌립니다.

주의

- **수동 잠금 해제** 상태에서는 얼굴 인식과 관계없이 누구나 출입할 수 있습니다. 필요한 작업을 마치면 반드시 **해제** 버튼을 클릭하세요.
- **수동 잠금** 상태에서는 실내에 있는 사람이 퇴실 버튼으로 나갈 수 없습니다. **수동 잠금**을 실행하기 전에 실내에 사람이 남아 있지 않은지 확인하세요.

알아두기

- 출입문이 수동 잠금 또는 수동 잠금 해제 상태일 때는 **출입문 열기** 버튼이 비활성화되고 **해제** 버튼만 표시됩니다.



- 수동 제어는 출입문의 개방 일정과 잠금 일정보다 우선 적용됩니다. 예를 들어, 개방 일정 시간대에 **수동 잠금**을 실행하면 출입문은 잠긴 상태로 유지됩니다.
- **해제** 버튼을 클릭하면 현재 시간에 맞는 일정 상태 또는 평상시 상태로 돌아갑니다.

출입문 규칙 설정하기

출입문 규칙을 사용하면 출입문에서 발생한 출입 판단 결과에 따라 오디오 재생, 웹훅 전송, 릴레이 동작을 자동 실행할 수 있습니다. 출입이 허용되면 출입문은 출입문 설정에 따라 자동으로 열리므로, 출입문 규칙에서는 문을 여는 것 외에 필요한 추가 동작을 설정합니다.

아래와 같은 상황에서 출입문 규칙을 설정하세요.

- 출입이 허용되면 환영 음성을, 거부되면 안내 음성을 재생하고 싶을 때
- 미인가자가 뒤따라 들어오면 비상등이나 경고음을 동작시키고 싶을 때
- 출입 기록을 외부 출입 통제 시스템이나 관제 서버로 전송하고 싶을 때

시작하기 전에

출입문 규칙을 설정하기 전에 아래 사항을 확인하세요.

- 규칙을 적용할 출입문을 먼저 등록하세요. 자세한 내용은 출입문 관리하기를 참고하세요.
- 오디오를 사용하려면 재생할 오디오 클립을 미리 업로드하세요. 자세한 내용은 오디오 클립 업로드하기를 참고하세요.
- 웹훅을 사용하려면 수신할 서버의 URL을 미리 준비하세요.
- 릴레이를 사용하려면 비상등, 경고음 등 동작시킬 장치가 릴레이 포트에 연결되어 있는지 확인하세요. 외부 장치 연결에 대한 자세한

내용은 ViOnyx 설치 가이드를 참고하세요.

출입 판단 결과

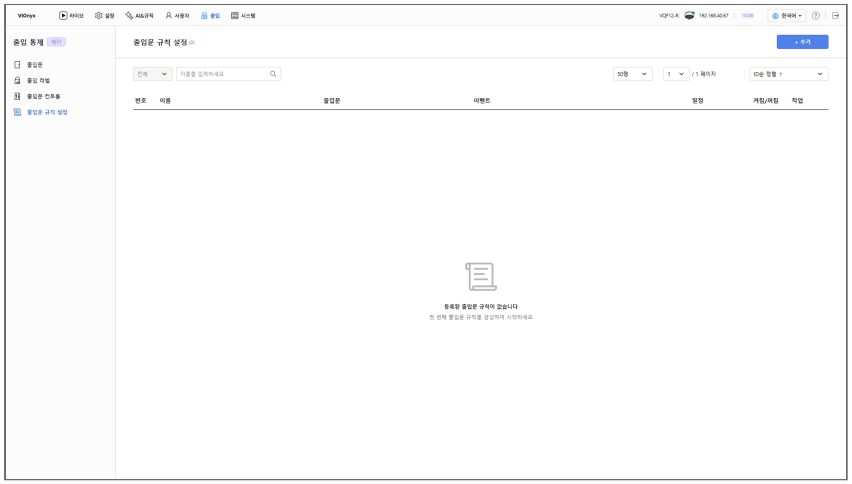
출입문 규칙에서는 다음 출입 판단 결과마다 실행할 동작을 각각 설정할 수 있습니다.

출입 판단 결과	발생 조건
출입 허용	출입 레벨이 있는 사용자가 출입 시간 안에 식별되어 출입이 허용되었습니다.
미식별로 출입 거부	출입 통제 영역에 들어온 사람의 얼굴을 인식하지 못했거나, 등록되지 않은 사람입니다.
액세스 레벨로 출입 거부	등록된 사용자로 식별되었지만, 해당 출입문의 출입 레벨이 없거나 출입 시간이 아닙니다.
출입문 모드로 출입 거부 (수동/스케줄 잠금)	출입문이 수동 잠금 상태이거나 잠금 일정 시간대여서 출입이 거부되었습니다.
안티 테일게이팅으로 출입 거부	검증 영역의 인원이 출입 통제 이벤트의 테일게이팅 옵션 조건을 충족하지 않아 출입이 거부되었습니다.
인증자 통과 (출입문 라인)	출입이 허용된 사용자가 이벤트 진입 라인을 지나 실제로 출입했습니다.
거부 후 통과 (보안 이벤트)	출입이 거부된 사람이 이벤트 진입 라인을 지나 출입했습니다. 강제 출입이 의심되는 보안 이벤트입니다.

출입문 규칙 추가

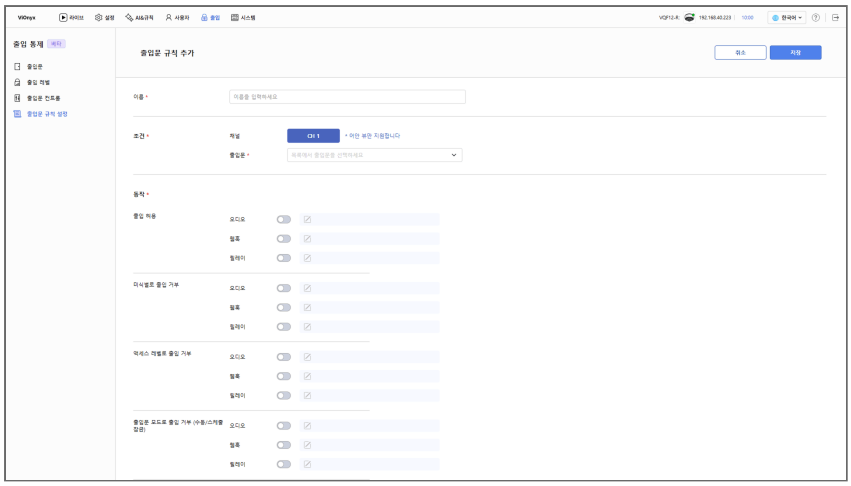
1 규칙 추가 시작

1. 화면 왼쪽 상단의 **출입** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **출입문 규칙 설정**을 클릭하세요.



3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.

4. **출입문 규칙 추가** 화면이 나타나면 규칙 이름을 입력하고, 조건과 동작을 설정하세요.



2 규칙 이름 입력

이름 입력 필드에 규칙 이름을 입력하세요. 필수 항목입니다.

3 조건 설정

조건 섹션에서 규칙을 적용할 출입문을 선택하세요.

- **채널**: 채널은 CH 1로 고정되어 있습니다. 피쉬아이 뷰만 지원합니다.
- **출입문**: 규칙을 적용할 출입문을 선택하세요. 필수 항목입니다.

4 동작 설정

동작 섹션에는 출입 판단 결과별로 **오디오**, **웹훅**, **릴레이** 동작이 표시됩니다. 동작을 실행할 출입 판단 결과에서 원하는 동작의 토글 버튼을 클릭해 활성화한 후 ✎ 버튼을 클릭하세요. 동작별 설정 팝업이 나타납니다.

최소 1개의 동작을 활성화해야 규칙을 저장할 수 있습니다. 동작별 설정 방법은 아래를 참고하세요.

> **알아두기**
> 동작별 일정의 시간대가 아니면 출입 판단 결과가 발생해도 해당 동작은 실행되지 않습니다. 일정은 **AI&규칙** → **일정**에서 관리할 수 있습니다. 자세한 내용은 일정 관리하기를 참고하세요.

5 오디오 동작 설정

출입 판단 결과가 발생하면 카메라에서 오디오 클립을 재생합니다.



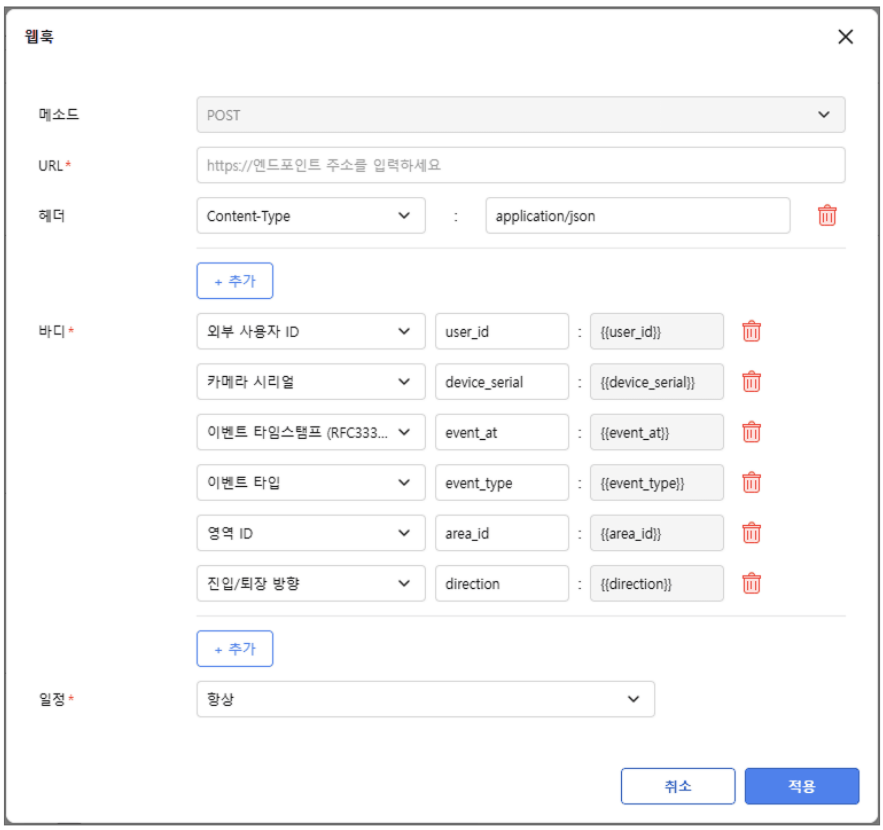
- **오디오 클립**: 재생할 오디오 클립을 선택하세요. 필수 항목입니다.
- **반복**: 오디오 클립을 반복 재생할 횟수를 선택하세요.
- **일정**: 오디오를 재생할 일정을 선택하세요. 필수 항목이며, 기본값은 **항상**입니다.

오디오 동작 설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
> 오디오 동작을 설정하기 전에 오디오 클립을 미리 준비해야 합니다. 오디오 클립은 **시스템** → **오디오** 메뉴에서 업로드할 수 있습니다. 자세한 내용은 오디오 클립 업로드하기를 참고하세요.

6 웹훅 동작 설정

출입 판단 결과가 발생하면 외부 서버로 웹훅을 전송합니다.



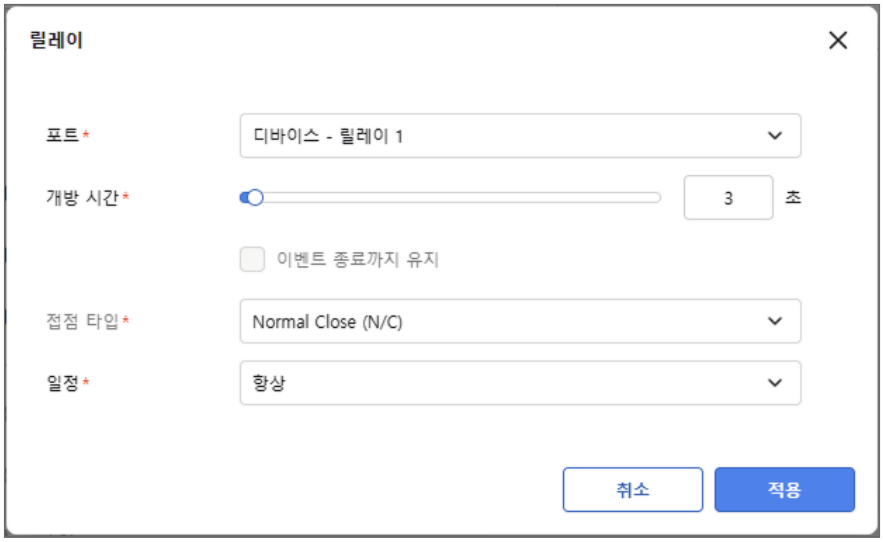
- **메소드**: 웹훅 전송 방식입니다. `POST` 방식만 지원합니다.
- **URL**: 웹훅을 수신할 URL을 입력하세요. 필수 항목입니다.
- **헤더**: 웹훅에 포함할 HTTP 헤더를 설정하세요. 기본으로 `Content-Type: application/json` 헤더가 추가되어 있습니다. **+ 추가** 버튼을 클릭해 헤더를 추가할 수 있습니다. 같은 헤더 이름은 중복해서 사용할 수 없으며, 시스템에서 예약한 헤더 이름은 사용할 수 없습니다.
- **바디**: 웹훅 본문에 포함할 항목을 설정하세요. 필수 항목입니다. 각 줄의 왼쪽 목록에서 전송할 정보를 선택하고, 가운데 필드에 JSON 키 이름을 입력하세요. 오른쪽 필드에는 이벤트가 발생할 때 실제 값으로 바뀌는 변수가 표시됩니다. **+ 추가** 버튼을 클릭해 사용자 정의 항목을 추가하거나 버튼을 클릭해 삭제할 수 있습니다. 본문 크기는 최대 64KB입니다.
- **일정**: 웹훅을 전송할 일정을 선택하세요. 필수 항목이며, 기본값은 **항상**입니다.

설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **알아두기**
>
> - 헤더와 본문에 입력한 값은 보안을 위해 저장 후 화면에 다시 표시되지 않습니다. 규칙을 수정할 때 저장된 값은 그대로 유지되며, 새로 입력하면 기존 값을 대체합니다.
> - 웹훅 전송 결과는 시스템 로그에서 확인할 수 있습니다. 자세한 내용은 시스템 로그 확인하기를 참고하세요.

7 릴레이 동작 설정

출입 판단 결과가 발생하면 선택한 릴레이를 동작시킵니다. 비상등, 경고음, 보조 잠금 장치 등을 연동할 때 사용하세요.



- **포트**: 동작시킬 릴레이 포트를 선택하세요. 필수 항목입니다. 출입문 잠금 장치로 사용 중인 릴레이 포트는 선택할 수 없습니다.
- **개방 시간**: 릴레이를 동작 상태로 유지할 시간을 설정하세요. 슬라이더를 움직이거나 입력 필드에 값을 직접 입력할 수 있습니다. 1초부터 120초까지 설정할 수 있으며, 기본값은 3초입니다.
  - **이벤트 종료까지 유지**: 이 옵션을 선택하면 개방 시간과 관계없이 출입 통제 이벤트가 종료될 때까지 릴레이를 동작 상태로 유지합니다.
- **접점 타입**: 릴레이의 접점 타입을 선택하세요. 필수 항목이며, 포트를 선택하면 설정할 수 있습니다.
  - **Normal Open (N/O)**: 평상시 열려 있다가 릴레이가 동작하면 닫히는 접점입니다.

  - **Normal Close (N/C)**: 평상시 닫혀 있다가 릴레이가 동작하면 열리는 접점입니다.

- **일정**: 릴레이를 동작시킬 일정을 선택하세요. 필수 항목이며, 기본값은 **항상**입니다.

설정을 저장하려면 **적용** 버튼을 클릭하세요.

> **주의**
> **접점 타입**은 규칙이 아니라 릴레이 포트에 적용되는 설정입니다. **접점 타입**을 변경하면 확인 메시지가 나타나며, **확인** 버튼을 클릭하면 해당 포트를 사용하는 모든 규칙과 출입문에 즉시 적용됩니다. 포트가 수동 잠금 또는 수동 잠금 해제 상태일 때 변경하면 출력이 반전되어 잠긴 문이 열릴 수 있으니 주의하세요.

8 규칙 저장

모든 설정을 완료한 후 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요. 저장한 규칙은 출입문 규칙 목록에 추가되고 바로 적용됩니다.



> **알아두기**
> 출입문 규칙은 최대 20개까지 만들 수 있습니다.

출입문 규칙 목록 확인

출입문 규칙 목록에서 등록된 규칙과 각 규칙의 적용 대상을 확인할 수 있습니다.



- 특정 출입문 규칙을 찾으려면 검색 필드(1)에 출입문 규칙 이름을 입력하세요.
- 한 페이지에 표시할 출입문 규칙 개수를 변경하려면 화면 오른쪽 상단의 행 수 목록(2)에서 원하는 값을 선택하세요.
- 정렬 기준을 변경하려면 **ID순 정렬**(3)에서 원하는 기준을 선택하세요.

출입문 규칙 목록에 표시되는 항목은 다음과 같습니다.

항목	설명
번호	규칙 번호입니다.
이름	규칙 이름입니다.

항목	설명
출입문	규칙을 적용하는 출입문입니다.
이벤트	활성화된 동작이 하나 이상 있는 출입 판단 결과입니다. 결과가 여러 개이면 일부만 표시됩니다.
일정	규칙에 적용된 일정입니다.
켜짐/꺼짐	규칙을 켜거나 끌 수 있습니다.
작업	규칙을 수정( )하거나 삭제( )할 수 있는 기능을 제공합니다.

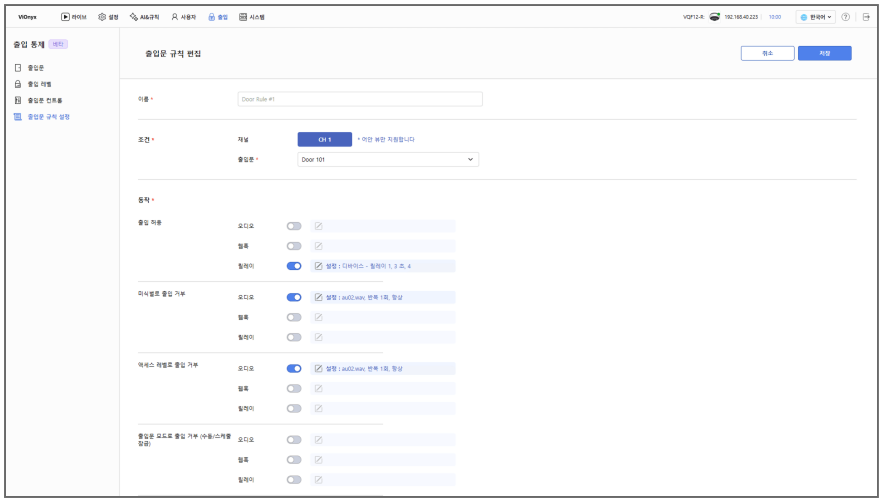
출입문 규칙 활성화/비활성화

출입문 규칙 목록에서 **켜짐/꺼짐** 열의 토글 버튼을 클릭하면 해당 규칙을 활성화하거나 비활성화할 수 있습니다. 비활성화한 규칙은 출입 판단 결과가 발생해도 동작을 실행하지 않습니다. 규칙을 삭제하지 않고 잠시 중단할 때 사용하세요.



출입문 규칙 수정

1. 출입문 규칙 목록에서 수정하려는 규칙의 오른쪽에 있는 버튼을 클릭하세요.
2. **출입문 규칙 편집** 화면이 나타나면 조건과 동작을 수정하세요.



3. 수정한 내용을 저장하려면 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

출입문 규칙 삭제

출입문 규칙 목록에서 삭제하려는 규칙의 오른쪽에 있는 버튼을 클릭하세요. 확인 메시지가 나타나면 **확인** 버튼을 클릭하세요. 삭제한 규칙은 복구할 수 없습니다.

시스템 구성하기

카메라 시스템을 효과적으로 관리하기 위해 디바이스 정보, 펌웨어, 유지 관리, 계정, 오디오, 로그 등을 체계적으로 관리할 수 있습니다. 안정적이고 안전한 카메라 운영을 위해 각 항목을 정기적으로 확인하고 업데이트하세요.

카메라 정보 업데이트하기

카메라의 기본 정보를 확인하고, 장치 이름, 설명, 위치 정보를 입력하여 조직에서 여러 대의 카메라를 효과적으로 관리할 수 있습니다.

아래와 같은 상황에서 카메라 정보를 업데이트하세요.

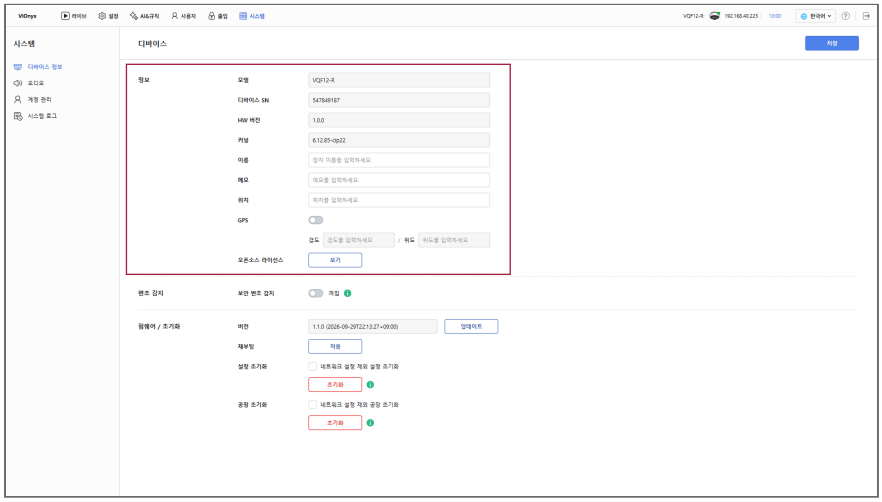
- 설치한 카메라를 조직 내 구별하기 쉬운 이름으로 변경하고 싶을 때
- 카메라의 위치나 설치 장소에 대한 추가 정보를 입력하고 싶을 때
- GPS 좌표를 입력하여 카메라의 정확한 위치를 기록하고 싶을 때
- 여러 대의 카메라를 관리할 때 카메라마다 특정 메모나 설명을 추가하고 싶을 때

> **알아두기**
>
> - 모델명, 시리얼 번호, 하드웨어 버전 등은 읽기 전용 정보로 편집할 수 없습니다.
> - 카메라 이름, 메모, 위치 정보는 유니코드를 지원하여 한글, 영문, 숫자, 특수문자를 입력할 수 있습니다.

카메라 기본 정보 확인

카메라의 모델명, 시리얼 번호, 하드웨어 버전 등 기본 정보를 확인하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.



정보 섹션에서 아래 기본 정보를 확인할 수 있습니다. 읽기 전용으로 편집할 수 없습니다.

- **모델**: 카메라 모델명

- **디바이스 SN**: 카메라 시리얼 번호
- **HW 버전**: 하드웨어 버전
- **커널**: 커널 버전
- **오픈소스 라이선스**: 오픈 소스 라이선스 정보를 확인하려면 **보기** 버튼을 클릭하세요.

카메라 정보 설정

카메라의 이름, 메모, 위치 정보를 입력하여 효과적으로 관리하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.

이름 입력

카메라를 식별하기 쉽도록 사용자 정의 이름을 입력하세요. **이름** 입력 필드에 카메라 이름을 입력하세요.

- 최대 64자까지 입력할 수 있습니다.
- 한글, 영문, 숫자, 특수문자(`.`, `-`, `(`, `)`)를 포함할 수 있습니다.

> *예: "입구-1번", "회의실-A" 등*

> **알아두기**
> 입력한 카메라 이름은 시스템 메뉴 및 웹 UI 여러 곳에서 표시되어 카메라를 쉽게 식별할 수 있습니다.

메모 추가

카메라에 대한 추가 정보나 메모를 입력하세요. **메모** 입력 필드에 메모 또는 설명을 입력하세요. 최대 64자까지 입력할 수 있습니다.

> *예: 설치 부서, 관리자 이름, 설치 날짜 등*

위치 정보 입력

카메라의 설치 위치를 텍스트로 입력하세요. **위치** 입력 필드에 카메라의 설치 위치를 입력하세요. 최대 64자까지 입력할 수 있습니다.

> *예: '1층 로비 입구', '2층 회의실 대기실'*

설정 저장

모든 정보를 입력한 후 화면 오른쪽 상단의 **저장** 버튼을 클릭하세요.

GPS 좌표 설정

카메라의 정확한 지리적 위치를 GPS 좌표로 입력하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.

3. GPS 설정을 활성화하려면 **정보** 섹션의 **GPS** 토글 버튼을 클릭하세요.



4. 경도와 위도 정보를 입력하세요.

> *예: 서울 (37.5665, 126.9780)*

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

> **알아두기**
>
> - GPS 좌표는 십진법(Decimal Degrees, DD) 형식으로 입력해야 합니다.
> - GPS 설정을 비활성화하려면 **GPS** 토글 버튼을 다시 클릭하세요.

펌웨어 업데이트하기

펌웨어 업데이트 기능을 통해 카메라의 펌웨어를 최신 버전으로 업데이트할 수 있습니다. 펌웨어 업데이트로 새로운 기능, 성능 개선, 보안 패치를 적용할 수 있습니다.

아래와 같은 상황에서 펌웨어를 업데이트하세요.

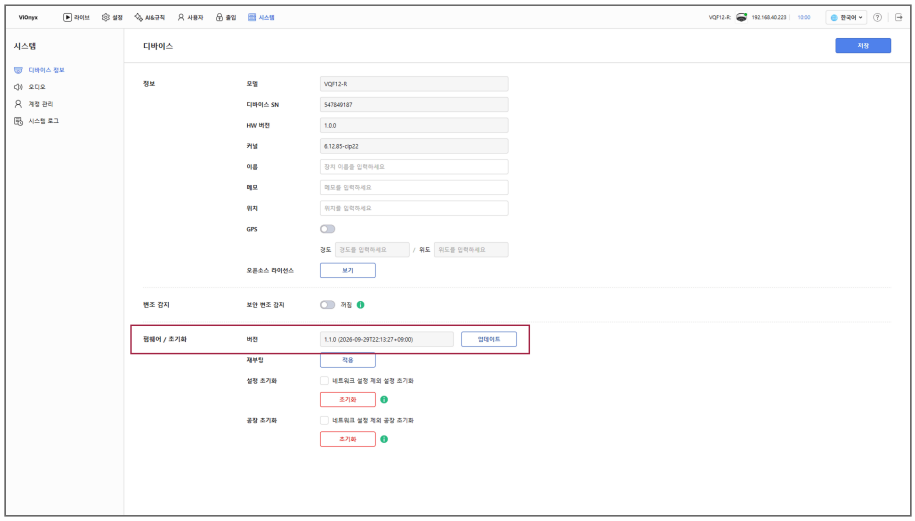
- 새로운 기능을 사용하고 싶을 때
- 보안 패치를 적용하여 카메라를 보호하고 싶을 때
- 카메라의 성능을 개선하고 싶을 때
- 기술 지원팀에서 권장하는 펌웨어 버전이 있을 때

> **알아두기**
>
> - 펌웨어 업데이트 중에는 카메라가 재시작되며, 이 기간 동안 카메라는 사용할 수 없습니다.
> - 펌웨어 업데이트를 시작하기 전에 장치에 충분한 전원이 공급되고 있는지 확인하세요.
> - 슈프리마 기술 지원팀에서 제공하는 공식 펌웨어 파일(`.bin`)만 사용하세요.

현재 펌웨어 버전 확인

카메라에 설치된 현재 펌웨어 버전을 확인하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.

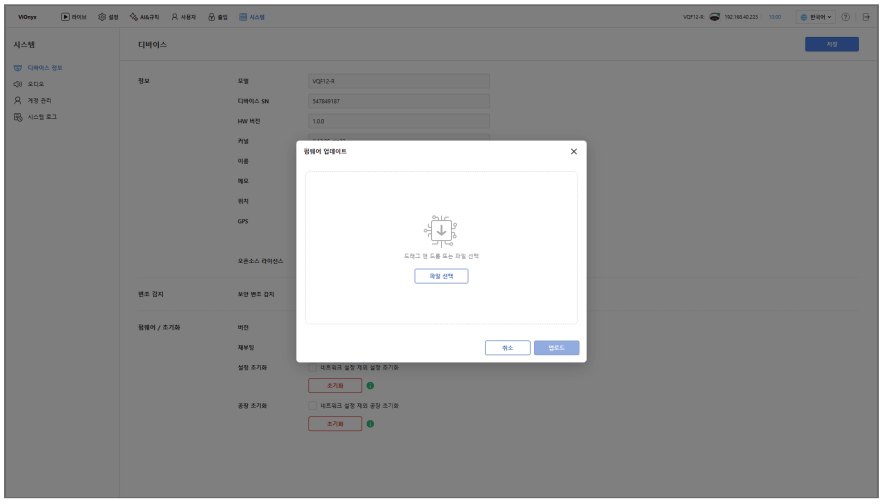


펌웨어 / 초기화 섹션의 **버전**에서 현재 설치된 펌웨어 버전을 확인할 수 있습니다.

펌웨어 업데이트

새로운 펌웨어 파일을 선택하여 장치를 업데이트하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.
3. **펌웨어 / 초기화** 섹션에서 **업데이트** 버튼을 클릭하세요.
4. **펌웨어 업데이트** 팝업이 나타나면 슈프리마에서 제공하는 펌웨어 파일(`.bin` 파일)을 선택하세요.



   - 파일 확장자는 반드시 `.bin` 이어야 합니다.
   - 업로드 영역에 파일을 드래그하거나 **파일 선택** 버튼을 클릭해 파일을 선택할 수 있습니다.
5. 파일을 선택하면 **업로드** 버튼이 활성화됩니다.
6. 펌웨어 업데이트를 진행하려면 **업로드** 버튼을 클릭하세요.
7. 업로드가 완료되면 재부팅 확인 팝업이 나타납니다. **확인** 버튼을 클릭해 카메라를 재시작하고 펌웨어 업데이트를 완료하세요.

- 카메라가 재부팅한 후 웹 UI에 다시 접속하세요. 새로운 펌웨어 버전을 확인하려면 **디바이스 정보**로 이동하세요.
- 펌웨어 업데이트가 시작된 후에는 취소할 수 없습니다. 업데이트가 완료될 때까지 기다려야 합니다.

카메라 유지 관리하기

카메라를 재부팅하거나 설정을 초기화하여 카메라를 효과적으로 관리할 수 있습니다. 재부팅, 설정 초기화, 공장 초기화 세 가지 방법을 안내합니다.

다음과 같은 상황에서 카메라 유지 관리 기능을 사용하세요.

- 관리자가 아닌 외부인이 카메라의 커버를 분리하려고 할 때, 카메라가 정상 작동하지 않도록 보안 조치를 취하고 싶을 때
- 네트워크 설정 변경 후 새로운 설정을 적용하고 싶을 때
- 카메라의 응답이 느려지거나 성능 저하가 발생했을 때
- 시스템이 정상 작동하지 않을 때
- 카메라의 설정을 모두 기본값으로 돌리고 싶을 때
- 카메라를 다른 사용자에게 인수인계하기 전에 모든 정보를 삭제하고 싶을 때
- 시스템에 문제가 발생하여 공장 기본값으로 복원해야 할 때

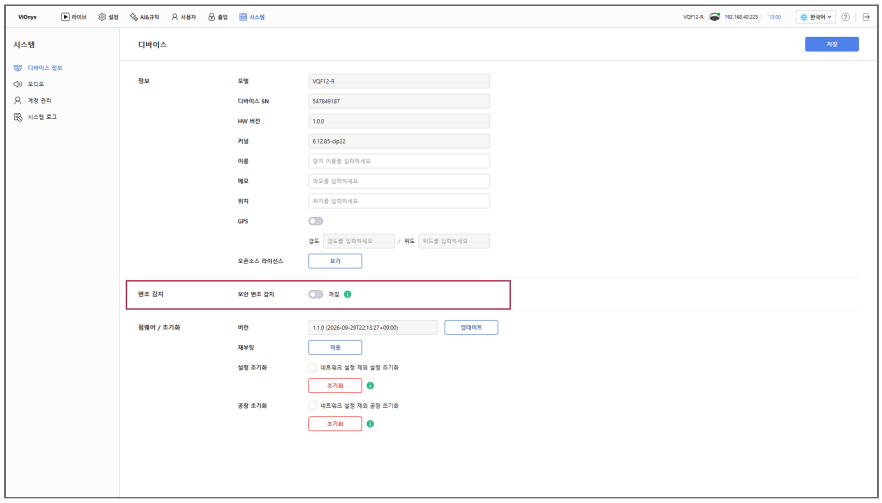
경고

- 재부팅 또는 초기화 중에 카메라의 전원을 끄지 마세요.
- **공장 초기화**는 모든 사용자 데이터, 이벤트 기록, 로그를 영구 삭제합니다. 복구할 수 없으므로 매우 신중하게 진행하세요.
- 초기화하기 전에 필요한 데이터를 백업하세요.

변조 감지

카메라의 **변조 감지** 기능을 활성화하면 관리자가 아닌 외부인이 카메라의 커버를 분리하려고 할 때, 카메라의 인증서와 키를 삭제하여 카메라가 정상 작동하지 않도록 할 수 있습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.
3. **변조 감지** 섹션의 토글 버튼을 클릭해 기능을 활성화하세요.



4. 경고 메시지가 나타나면 **확인** 버튼을 클릭하세요.

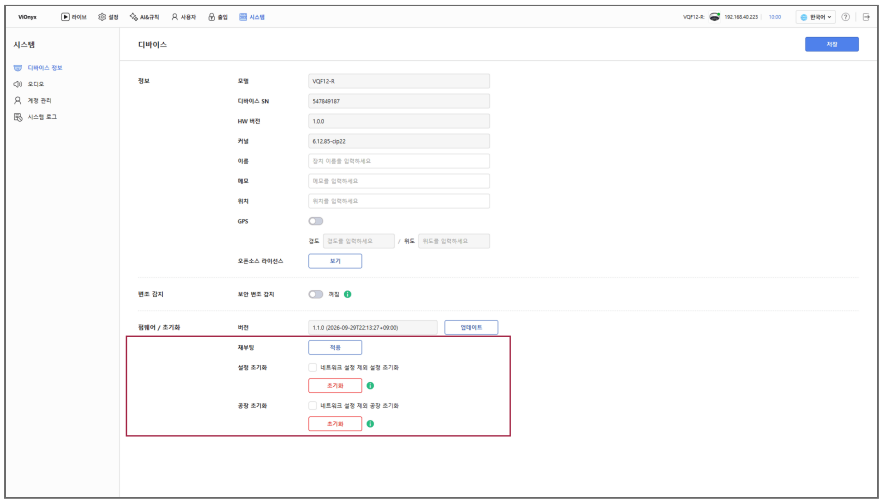
이 기능은 **저장** 버튼을 클릭하지 않아도 변경 사항이 자동 저장됩니다.

> **주의**
> **변조 감지** 기능을 활성화한 상태에서 관리자가 유지보수를 위해 카메라의 커버를 분리해야 할 때는 **변조 감지** 기능을 일시적으로 비활성화한 후 작업을 진행해야 합니다. 작업이 완료된 후에는 다시 활성화하여 보안을 유지하세요.

카메라 재부팅

카메라를 재시작하여 설정 변경사항을 적용하거나 시스템 성능을 회복시킵니다. 재부팅은 현재 설정을 유지하면서 시스템을 재초기화하는 방법입니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.
3. **펌웨어 / 초기화** 섹션의 **재부팅**에서 **적용** 버튼을 클릭하세요.



4. 재부팅 확인 팝업이 나타나면 **확인** 버튼을 클릭하세요.

알아두기

- 재부팅 중에는 카메라가 일시적으로 사용할 수 없습니다. 재부팅은 최소 1-2분 소요됩니다.
- 재부팅 중에 카메라의 전원을 끄지 마세요. 시스템 손상이 발생할 수 있습니다.
- 재부팅 후 카메라의 IP 주소가 변경되었다면 새로운 IP 주소로 접속해야 합니다.
- 재부팅이 시작되면 웹 UI 연결이 자동으로 끊깁니다. 이는 정상 동작입니다.

초기화

카메라의 설정을 초기화하거나 공장 기본값으로 완전히 복원할 수 있습니다. 두 가지 초기화 방식이 제공되며, 삭제되는 데이터가 다르므로 신중하게 선택해야 합니다.

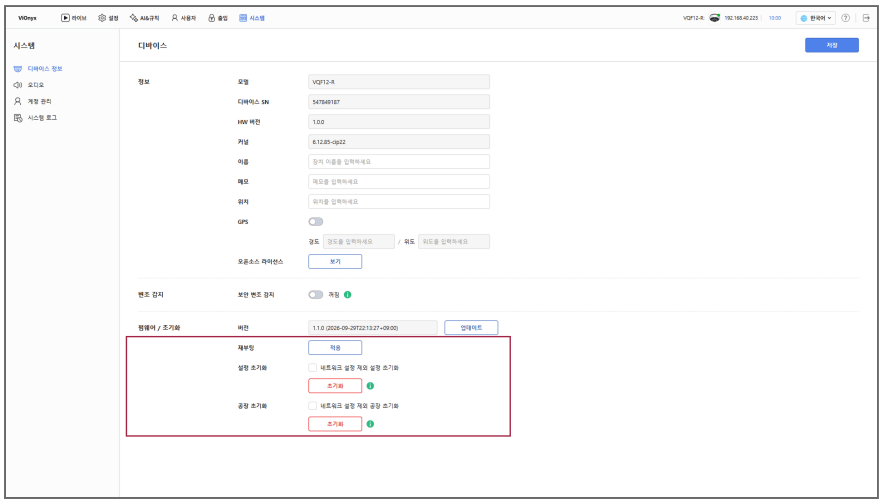
초기화 방식 비교

방식	설명	삭제 대상	유지 대상
설정 초기화	설정값만 초기화	카메라 설정, 네트워크 설정(선택 사항), 비디오 프로필, 규칙, 계정	사용자 정보, 얼굴 데이터, 이벤트/로그
공장 초기화	모든 데이터 삭제 후 공장 기본값 복원	모든 설정, 사용자 정보, 이벤트, 로그, 계정	-

설정 초기화

설정값만 초기화하고 사용자 정보 및 로그 데이터는 유지합니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.
3. **펌웨어 / 초기화** 섹션의 **설정 초기화**에서 **초기화** 버튼을 클릭하세요.



네트워크 설정 초기화를 제외하려면 **네트워크 설정 제외 설정 초기화** 옵션의 체크박스를 클릭하세요.

4. 설정 초기화 확인 팝업이 나타나면 **확인** 버튼을 클릭하세요.

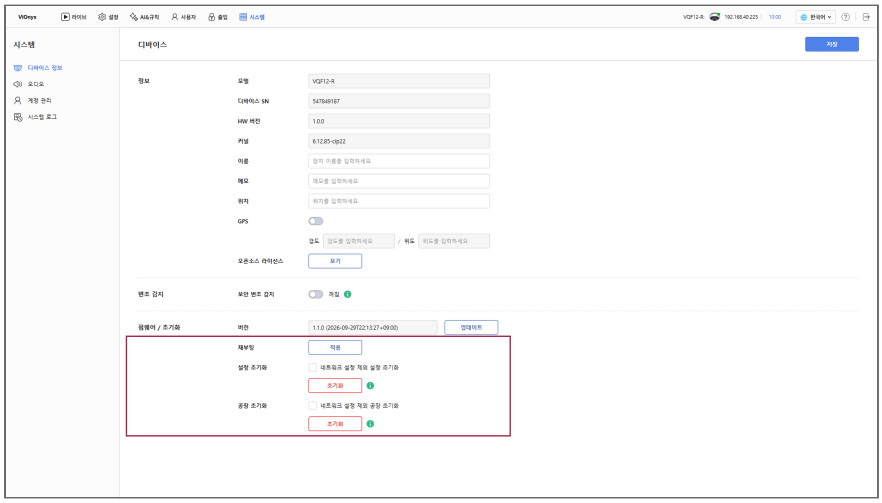
설정 초기화가 진행되고 카메라가 자동으로 재부팅됩니다.

공장 초기화

카메라를 완전히 초기화하여 공장 초기상태로 복원합니다. 이 작업은 되돌릴 수 없습니다.

> **경고**
> 공장 초기화는 모든 데이터를 완전히 삭제합니다. 이 작업은 복구할 수 없으므로 매우 신중하게 진행하세요.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **디바이스 정보**를 클릭하세요.
3. **펌웨어 / 초기화** 섹션의 **공장 초기화**에서 **초기화** 버튼을 클릭하세요.



네트워크 설정 초기화를 제외하려면 **네트워크 설정 제외 설정 초기화** 옵션의 체크박스를 클릭하세요.

4. 공장 초기화 확인 팝업이 나타나면 **확인** 버튼을 클릭하세요.
5. 최종 확인 팝업이 나타나면 관리자 비밀번호를 입력하세요.
6. **확인** 버튼을 클릭하세요.

> **알아두기**
> - 공장 초기화 완료 후 아래 항목이 기본값으로 복원됩니다.
>   - 관리자 ID: **admin**
>   - 네트워크 설정: DHCP
>   - 모든 사용자 데이터, 이벤트, 로그: 삭제됨
> - 공장 초기화 후 웹 UI에 접속할 때 새로운 기본 비밀번호를 설정해야 합니다.

오디오 클립 업로드하기

카메라에서 사용할 오디오 클립을 업로드하여 경보음이나 안내음으로 활용할 수 있습니다. WAV 형식의 오디오 파일을 업로드하고 관리할 수

있습니다.

다음과 같은 상황에서 오디오 클립을 업로드하세요.

- 이벤트 발생 시 재생할 경보음을 업로드하고 싶을 때
- 다국어 안내음을 등록하고 싶을 때
- 특정 상황에 맞는 음성 메시지를 추가하고 싶을 때

오디오 저장 용량 확인

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **오디오**를 클릭하세요.
3. **오디오 클립** 섹션에서 오디오 저장소의 남은 용량을 확인할 수 있습니다.



오디오 파일 준비

오디오 클립을 업로드하기 전에 다음 사항을 확인하세요.

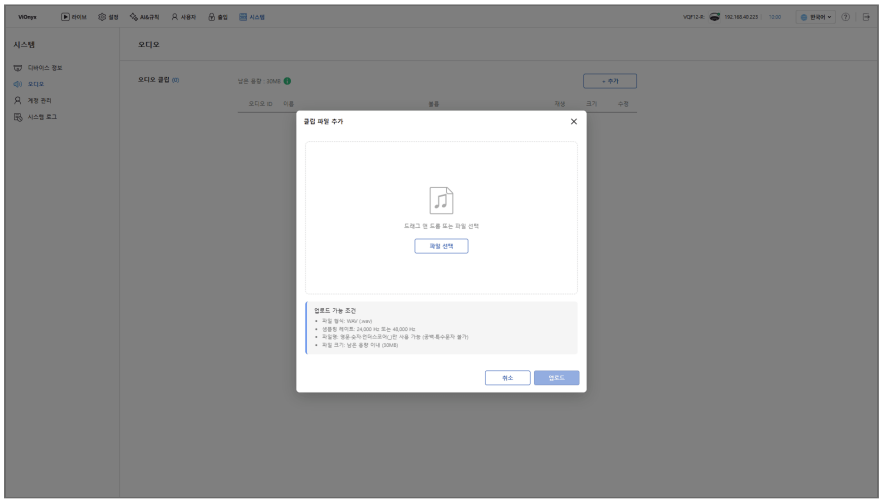
- **파일 형식**: `.wav` 확장자만 지원됩니다.
- **샘플레이트**: 48kHz 이상의 샘플레이트를 사용합니다.
- **파일명**: 영문, 숫자, 언더스코어(`_`)만 입력할 수 있으며, 최대 64자입니다. 공백이나 특수문자를 사용할 수 없습니다.
- **파일 크기**: 남은 용량 범위 내에서 업로드할 수 있습니다.

오디오 클립 업로드

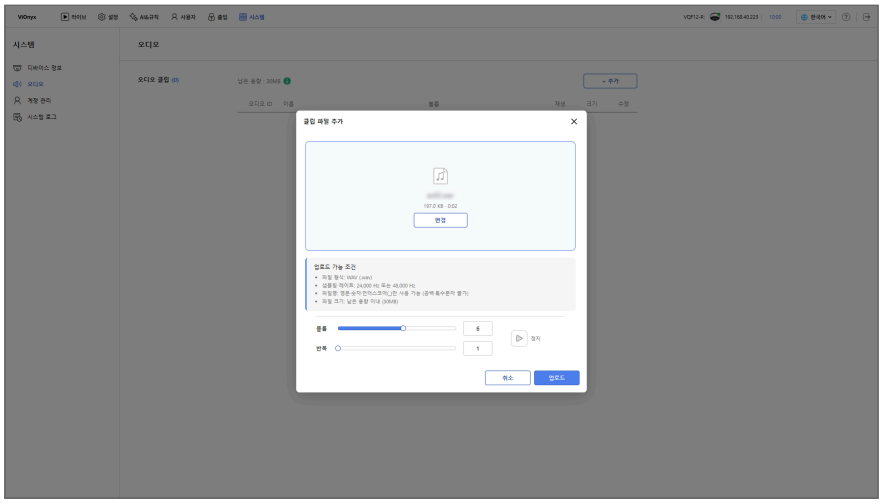
1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **오디오**를 클릭하세요.
3. 화면 오른쪽 상단의 **+ 추가** 버튼을 클릭하세요.



4. **클립 파일 추가** 팝업창이 나타납니다.



5. 업로드 영역에 WAV 파일을 드래그 앤 드롭하거나, **파일 선택** 버튼을 클릭하고 로컬에 저장된 WAV 파일을 선택하세요.
6. 업로드를 완료하면 볼륨과 반복 설정 옵션을 조정하세요.



7. 오디오 클립을 업로드하려면 **업로드** 버튼을 클릭하세요.

업로드된 오디오 클립을 목록에서 확인하세요.



알아두기

- 볼륨 슬라이더를 조정하여 오디오 클립의 재생 볼륨을 설정할 수 있습니다.
- 오디오 클립을 재생하려면 ▶ 버튼을 클릭하세요.

오디오 클립 삭제

삭제하려는 오디오 클립의 오른쪽에 버튼을 클릭하세요.



알아두기

- 삭제하려는 오디오 클립이 AI 규칙(Rule)에 적용되어 있다면, AI 규칙 설정에서 자동 제외됩니다.
- AI 규칙 설정에 대한 자세한 내용은 AI 규칙(Rule) 설정하기를 참고하세요.

관리자 계정 비밀번호 업데이트하기

관리자 계정의 비밀번호를 변경하여 카메라 접근 보안을 강화할 수 있습니다. 비밀번호는 정기적으로 변경하는 것이 보안 모범 사례입니다.

다음과 같은 상황에서 비밀번호를 변경하세요.

- 관리자 계정을 처음 설정할 때 보안을 강화하고 싶을 때
- 정기적인 보안 정책에 따라 비밀번호를 갱신하고 싶을 때
- 비밀번호가 노출되어 긴급하게 변경해야 할 때
- 관리자 교체 시 새로운 비밀번호로 설정하고 싶을 때

비밀번호 규칙 확인

비밀번호를 설정하기 전에 다음 규칙을 확인하세요. 모든 규칙을 동시에 만족해야 합니다.

- 비밀번호는 최소 12자 이상이어야 합니다. 최대 64자 이하로 제한합니다.
- 최소 1개의 영어 소문자(`a-z`)와 대문자(`A-Z`)를 포함해야 합니다.
- 최소 1개의 숫자(`0-9`)와 특수문자를 포함해야 합니다.

  > *특수문자 예시:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

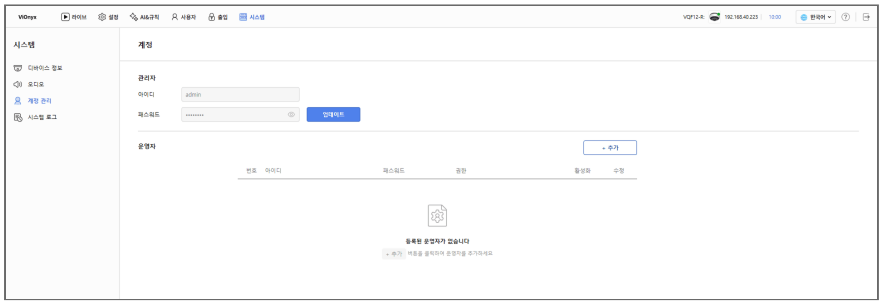
- `1234`, `abcd` 같이 연속 문자 4개 이상, 동일 문자 4개 이상을 포함할 수 없습니다.
- 대소문자와 무관하게 아이디는 비밀번호에 포함할 수 없습니다.

  > *admin, Admin, ADMIN, Admin123! 등*

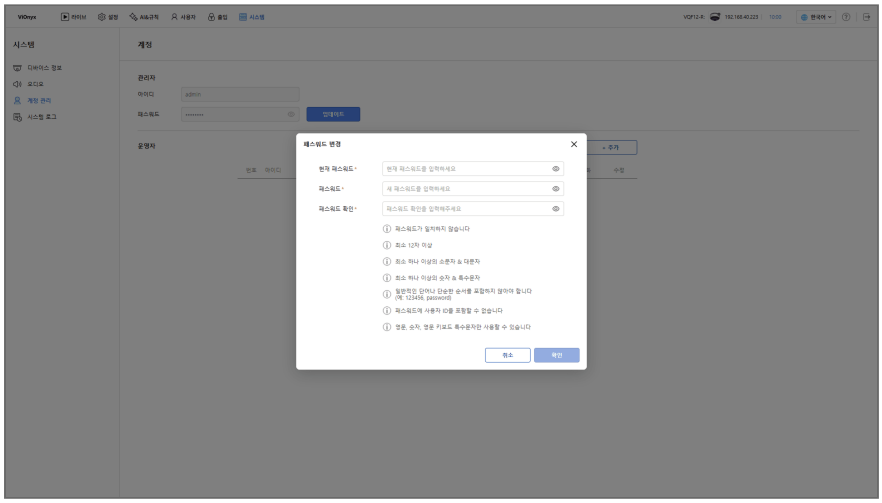
- `password`, `qwerty`, `123456` 등 흔히 사용되는 비밀번호 패턴은 사용할 수 없습니다.
- 영문, 숫자, 영문 키보드 특수 문자만 사용할 수 있습니다.

관리자 비밀번호 변경

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.



3. **관리자** 섹션에서 **업데이트** 버튼을 클릭하세요.
4. **패스워드 변경** 창이 나타나면 **현재 패스워드** 입력 필드에 현재 관리자 비밀번호를 입력하세요.



5. **패스워드** 과 **패스워드 확인** 입력 필드에 새 비밀번호를 차례로 입력하세요.
6. 새로운 비밀번호를 변경하려면 **확인** 버튼을 클릭하세요.

성공 메시지가 나타나면 비밀번호 변경이 완료됩니다.

> **알아두기**
>
> - 비밀번호 변경 후 다시 로그인해야 할 수 있습니다.
> - 비밀번호 변경 기록은 시스템 로그에 남습니다.

비밀번호를 잊어버렸을 때

관리자 비밀번호를 잊어버렸다면 다음 방법으로 해결할 수 있습니다.

- **공장 초기화**: 공장 초기화를 실행하면 관리자 계정이 기본값으로 복원됩니다. 단, 모든 데이터가 삭제됩니다. 공장 초기화 방법에 대한 자세한 내용은 ViOnyx 설치 가이드를 참고하세요.
- **기술 지원 연락**: 슈프리마 기술 지원팀(CS@suprema.co.kr)에 연락하여 도움을 받으세요.

운영자 관리하기

관리자 외에 제한된 권한을 가진 운영자(Operator) 계정을 추가 및 수정, 삭제할 수 있습니다. 운영자는 관리자를 대신하여 카메라의 일부 기능을 관리할 수 있습니다.

또한 NVR/VMS가 ONVIF 및 RTSP 인증에 사용하는 ONVIF 전용 계정을 추가할 수 있습니다. ONVIF Profile S 폴백을 활성화하려면 ONVIF 전용 계정이 필요합니다.

다음과 같은 상황에서 운영자를 추가하세요.

- 카메라 운영을 위해 추가 담당자를 배정하고 싶을 때
- 특정 권한만 제한적으로 부여하고 싶을 때
- 여러 명이 협력하여 카메라를 관리해야 할 때
- 팀 구성원에게 읽기 전용 또는 편집 권한을 부여하고 싶을 때

알아두기

- 최대 10명까지 운영자를 추가할 수 있습니다.
- 운영자는 다른 운영자를 추가할 수 없습니다. 관리자만 운영자를 추가할 수 있습니다.
- 운영자 비밀번호는 관리자 비밀번호와 동일한 규칙을 따릅니다. 자세한 내용은 관리자 계정 비밀번호 업데이트하기를 참고하세요.
- 각 운영자는 자신의 계정 정보만 변경할 수 있습니다.

운영자 권한 종류

운영자를 추가할 때 다음 3가지 권한 중 하나를 선택해야 합니다.

- **읽기 전용**: 모든 카메라 설정과 로그를 조회할 수 있으며, 설정을 변경할 수 없습니다.
- **읽기/쓰기**: 관리자 메뉴를 제외한 모든 메뉴에 접근할 수 있으며, 카메라 설정을 변경할 수 있습니다. 자신의 비밀번호를 변경할 수 있으나 다른 운영자나 관리자 계정의 비밀번호는 변경할 수 없습니다.
- **ONVIF 전용**: NVR/VMS가 ONVIF 및 RTSP 인증에 사용하는 장치 전용 계정입니다. 웹 UI에는 로그인할 수 없습니다. ONVIF Profile S 폴백을 활성화할 때 필요합니다. 자세한 내용은 네트워크 설정하기를 참고하세요.

ONVIF 전용 계정 제한 사항

ONVIF 전용 계정은 일반 운영자 계정과 달리 다음과 같은 제한이 있습니다.

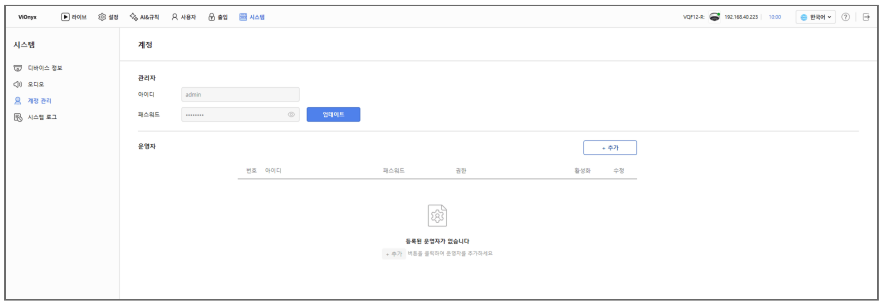
- 장치당 하나만 만들 수 있습니다.
- 계정을 만든 후에는 아이디, 패스워드, 권한을 변경할 수 없습니다. 활성화 또는 비활성화, 삭제만 할 수 있습니다.
- 계정을 비활성화하면 Profile S 폴백을 활성화할 수 없습니다.
- Profile S 폴백이 활성화된 상태에서는 계정을 삭제할 수 없습니다. 먼저 ONVIF 모드를 **Profile T Only**로 변경하세요.

주의

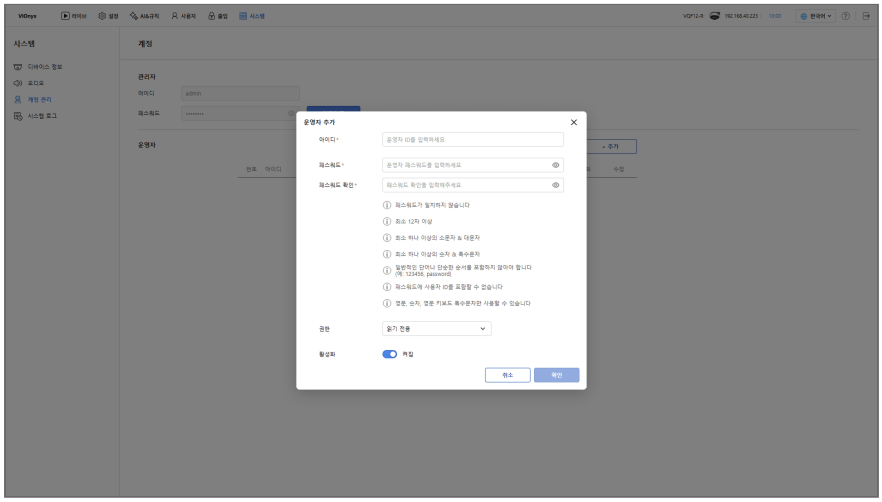
ONVIF 전용 계정은 만든 후 아이디와 패스워드를 변경할 수 없습니다. 연결할 NVR/VMS에 입력할 정보를 미리 정하고, 계정 정보를 안전하게 보관하세요. 패스워드를 변경하려면 계정을 삭제한 후 다시 만들어야 합니다.

운영자 추가

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.



3. **운영자** 섹션에서 **+ 추가** 버튼을 클릭하세요.
4. **운영자 추가** 팝업창이 나타나면 필요한 정보를 입력하세요.



- **아이디**: 운영자의 고유 아이디를 입력하세요.
  - 최대 64자까지 입력할 수 있습니다.
  - 한글, 영문, 숫자를 포함할 수 있습니다.
  - 특수문자(`_`, `.`, `-`, `(`, `)`)를 사용할 수 있습니다.
  - 다른 운영자와 중복될 수 없습니다.
- **패스워드**: 운영자의 비밀번호를 입력합니다. 관리자 비밀번호와 동일한 규칙을 따릅니다. 자세한 내용은 관리자 계정 비밀번호 업데이트하기를 참고하세요.
- **패스워드 확인**: 비밀번호를 다시 입력하세요.
- **권한**: 운영자의 권한을 선택하세요. ONVIF 전용 계정을 만들려면 **ONVIF 전용**을 선택하세요.
- **활성화**: 운영자의 계정을 활성화 또는 비활성화할 수 있습니다.

5. 모든 정보를 입력한 후 **확인** 버튼을 클릭하세요.

새로운 운영자를 추가하면 목록에 새로운 계정이 표시됩니다.

알아두기

- 운영자를 추가한 후 해당 계정으로 로그인하여 권한이 올바르게 적용되었는지 확인하세요.
- 운영자의 아이디와 비밀번호를 안전하게 운영자에게 전달하세요.

운영자 권한 변경

추가된 운영자의 권한을 변경할 수 있습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.
3. **운영자** 섹션에서 권한을 변경할 운영자의 **권한** 항목을 클릭하세요.

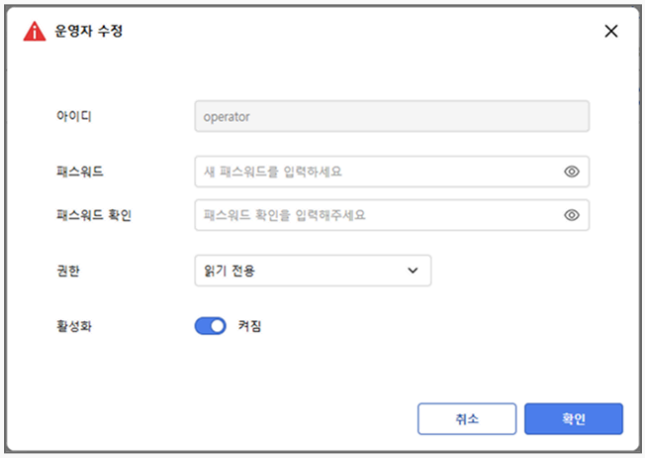


4. 선택 목록에서 원하는 권한으로 변경하세요.

권한 변경에 성공하면 화면 오른쪽 상단에 성공 메시지가 표시됩니다.

팁

버튼을 클릭하면 **운영자 수정** 창이 나타납니다. **권한** 항목에서 원하는 권한으로 변경한 후 **확인** 버튼을 클릭하세요.



알아두기

ONVIF 전용 계정은 권한을 변경할 수 없습니다. 다른 권한이 필요하면 새 운영자 계정을 추가하세요.

운영자 비활성화

운영자의 계정을 일시적으로 비활성화할 수 있습니다. 계정을 삭제하지 않고 접근만 차단합니다.

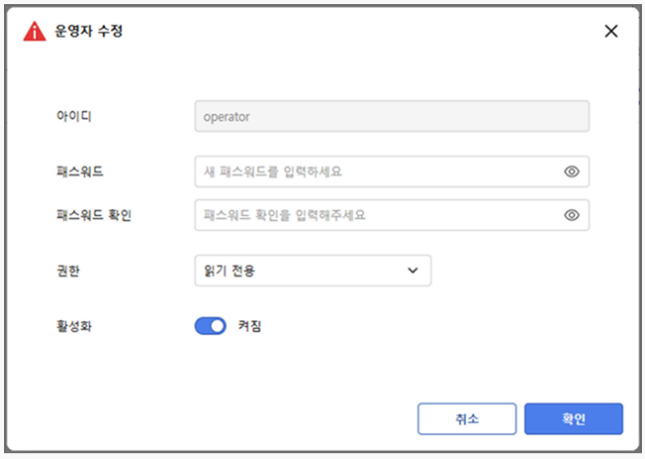
1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.
3. **운영자** 섹션에서 비활성화할 운영자의 **활성화** 항목에서 토글 버튼을 클릭하여 계정을 비활성화하세요.



비활성화에 성공하면 화면 오른쪽 상단에 성공 메시지가 표시됩니다. 운영자 계정이 비활성화되어 더 이상 로그인할 수 없습니다.

팁

버튼을 클릭하면 **운영자 수정** 창이 나타납니다. **활성화** 항목에서 토글 버튼을 클릭하여 계정을 비활성화하세요. 변경 사항을 저장하려면 **확인** 버튼을 클릭하세요.



알아두기

비활성화된 계정은 나중에 다시 활성화할 수 있습니다.

주의

운영자가 이미 로그인된 상태라면, 다음 로그인을 시도할 때 접근이 거부됩니다.

운영자 삭제

운영자 계정을 완전히 삭제할 수 있습니다. 삭제된 계정은 복구할 수 없습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.

2. 화면 왼쪽 사이드바에서 **계정 관리**를 클릭하세요.

3. **운영자** 섹션에서 삭제할 운영자의  버튼을 클릭하세요.



4. 경고 메시지가 나타나면 **확인** 버튼을 클릭하세요.

삭제에 성공하면 화면 오른쪽 상단에 성공 메시지가 표시됩니다. 운영자 계정이 목록에서 완전히 제거됩니다.

> **알아두기**
> **Profile T 우선 / S 폴백** 옵션이 활성화되어 있으면 ONVIF 전용 계정을 삭제할 수 없습니다. **설정** → **네트워크** → **네트워크**에서 ONVIF 모드를 **Profile T Only**로 변경한 후 다시 시도하세요. 자세한 내용은 네트워크 설정하기를 참고하세요.

시스템 로그 확인하기

카메라의 사용자 접속, 이벤트 발생, AI 분석, 시스템 운영 기록을 로그로 조회하고 관리할 수 있습니다. 웹 인터페이스에서 로그 종류, 레벨, 행위자 등의 조건으로 로그를 필터링하거나 CSV 형식으로 내보낼 수 있으며, 더 상세한 분석이 필요할 때는 암호화된 장치 로그를 다운로드할 수 있습니다.

다음과 같은 상황에서 로그를 확인하세요.

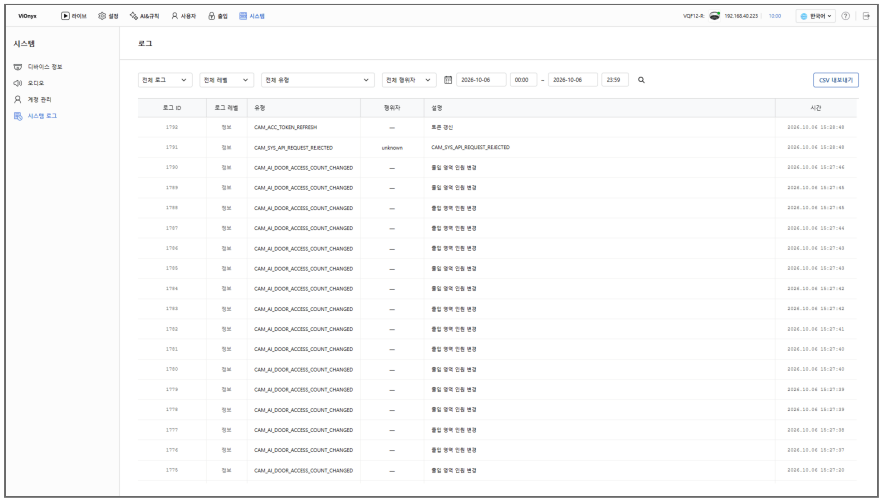
- 카메라에 누가 언제 접속했는지 확인하고 싶을 때
- 특정 이벤트의 발생 기록을 추적하고 싶을 때
- 카메라 시스템의 부팅, 재부팅 등 주요 작업을 확인하고 싶을 때
- 보안 감시 목적으로 접속 기록을 점검하고 싶을 때
- 문제 해결을 위해 시스템 로그를 수집하고 싶을 때
- 로그에 남은 작업이 관리자 또는 운영자가 직접 조작한 것인지, 카메라가 자동으로 수행한 것인지 구분하고 싶을 때

> **알아두기**
> - 로그는 장치 메모리 사이즈에 따라 자동으로 보존됩니다.
> - 각 로그 종류의 보존 기간은 약 1개월입니다.
> - 메모리가 가득 차면 가장 오래된 로그부터 자동 삭제합니다.
> - **시스템 로그** 메뉴는 관리자와 읽기/쓰기 권한을 가진 운영자만 사용할 수 있습니다. 단, 로그 종류 중 **시스템** 로그는 관리자만 조회할 수 있습니다.

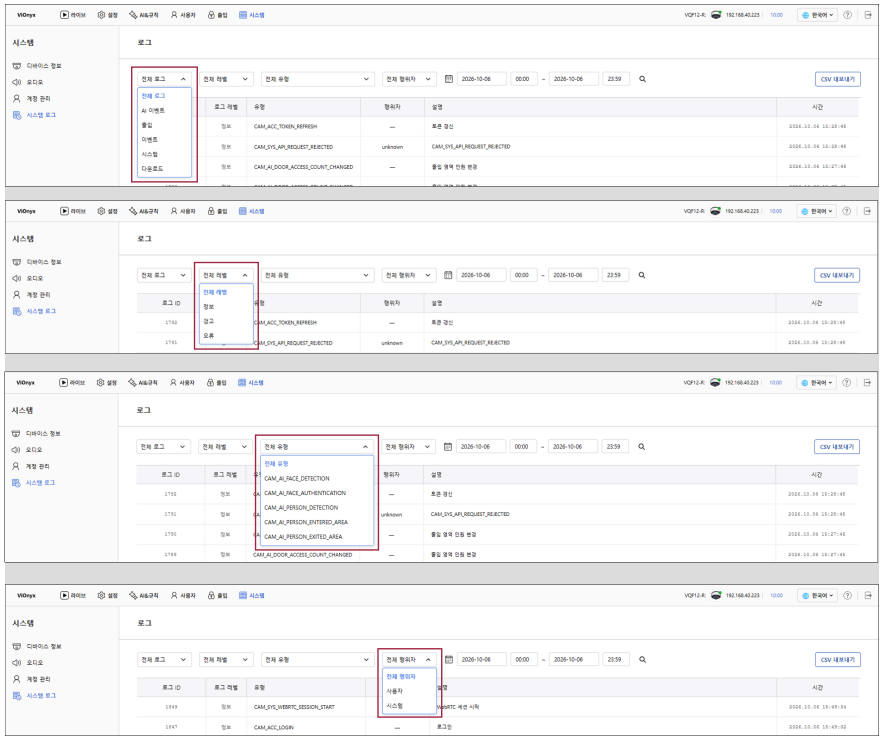
로그 조회

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.

2. 화면 왼쪽 사이드바에서 **시스템 로그**를 클릭하세요. 전체 로그를 조회할 수 있습니다.



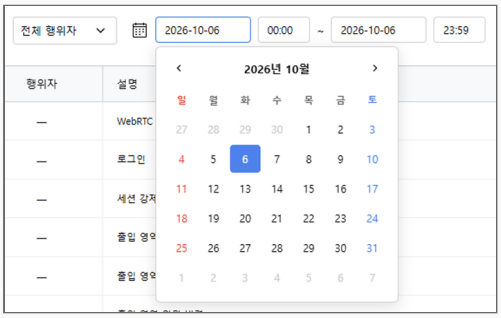
3. 로그 종류, 레벨, 유형, 행위자에 따라 로그를 필터링하려면 로그 목록 왼쪽 상단의 **전체 로그**, **전체 레벨**, **전체 유형**, **전체 행위자**에서 원하는 조건을 선택하세요.



4. 로그 목록 상단의 🔍 버튼을 클릭하면 선택한 조건에 맞춰 로그를 필터링할 수 있습니다.

알아두기

- 특정 기간의 로그를 조회하려면 날짜 및 시간 입력 필드를 클릭하세요. 달력과 시간 선택 도구가 나타나면 원하는 시작 날짜와 시간을 선택하세요. 종료 날짜와 시간도 같은 방식으로 설정할 수 있습니다.



- 목록 아래로 스크롤하면 로그 목록을 갱신하여 지난 로그를 계속해서 확인할 수 있습니다.
- 로그 유형에 대한 자세한 내용은 시스템 로그 유형을 참고하세요.

로그 종류

로그는 아래와 같이 구분할 수 있습니다.

- **AI 이벤트**: AI 분석과 관련된 이벤트 기록을 확인할 수 있습니다.
- **출입**: 로그인, 로그아웃, 계정 생성 등 사용자의 접속과 계정 관련 기록을 확인할 수 있습니다.
- **이벤트**: 이벤트 발생, Webhook 발신, 규칙 실행 등의 기록을 확인할 수 있습니다.
- **시스템**: 카메라의 부팅, 재부팅, 초기화 등 시스템 운영 기록을 확인할 수 있습니다. 이 로그는 **관리자만 조회 가능**합니다.

알아두기

다운로드 항목을 선택하면 장치의 암호화된 로그 파일을 다운로드할 수 있습니다. 자세한 내용은 장치 로그 다운로드를 참고하세요.

로그 레벨

로그는 아래의 레벨로 구분됩니다.

- **정보**: 일반적인 정보성 메시지 로그를 확인할 수 있습니다.
- **경고**: 경고 메시지 로그를 확인할 수 있습니다.
- **오류**: 오류 메시지 로그를 확인할 수 있습니다.

행위자

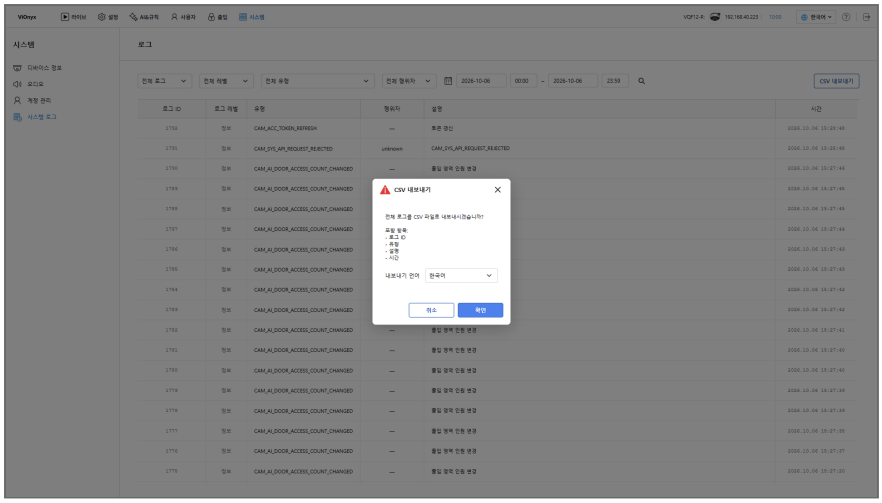
로그를 발생시킨 주체를 행위자라고 합니다. 행위자는 아래와 같이 구분됩니다.

- **사용자**: 웹 인터페이스에서 작업을 직접 수행한 관리자나 운영자입니다.
- **시스템**: AI 규칙, 스케줄 등에 따라 작업을 자동으로 수행한 카메라입니다.

로그 내보내기

로그를 CSV 형식으로 다운로드하여 외부에서 분석하거나 보관할 수 있습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템 로그**를 클릭하세요.
3. 로그 목록 왼쪽 상단의 **전체 로그**, **전체 레벨**, **전체 유형**, **전체 행위자**에서 내보낼 로그의 조건을 선택하세요. 조회 기간을 설정하여 특정 기간의 로그만 내보낼 수도 있습니다. 선택한 조건과 기간이 CSV 파일에 그대로 반영됩니다.
4. 화면 오른쪽 상단의 **CSV 내보내기** 버튼을 클릭하세요.
5. **CSV 내보내기** 팝업창이 나타나면 내보낼 언어를 선택하세요.



6. **확인** 버튼을 클릭하세요.

로그 목록을 CSV 파일로 다운로드할 수 있습니다.

> **알아두기**
>
> - CSV 파일명은 `system-logs-YYYYMMDD_HHMMSS.csv` 형식입니다.
>
>   *예: system-logs-20240326_153000.csv*
>
> - 웹 브라우저의 기본 다운로드 폴더에 저장되거나 사용자가 선택한 경로에 저장할 수 있습니다.

로그 보관 및 관리

로그 자동 삭제

카메라의 메모리 용량이 가득 차면 가장 오래된 로그부터 자동으로 삭제됩니다.

로그 종류	보존 기간
AI 이벤트	약 1개월
출입	약 1개월

로그 종류	보존 기간
이벤트	약 1개월
시스템	약 1개월

중요 로그 보관 방법

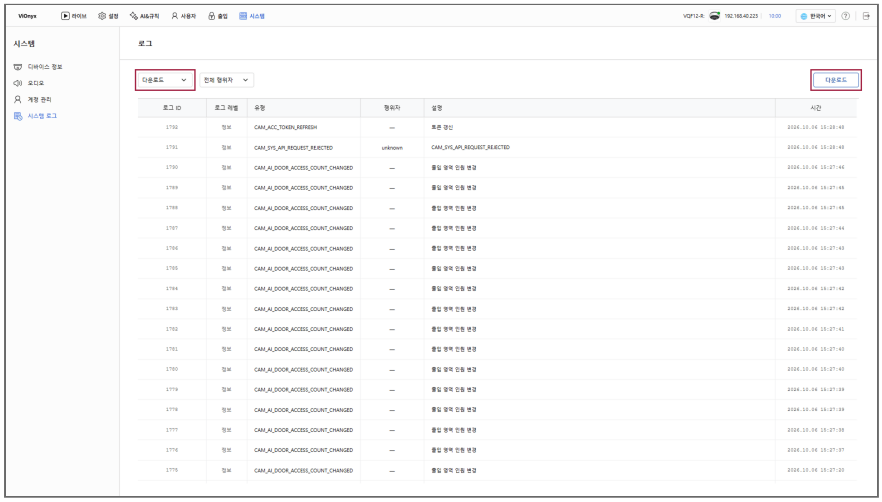
중요한 로그를 장기간 보관하고 싶다면 다음과 같이 하세요.

- 정기적으로 로그를 CSV로 내보내세요.
- 내보낸 파일을 외부 저장소(NAS, 클라우드 스토리지 등)에 보관하세요.
- 파일에 내보낸 날짜와 로그 기간을 명시하세요.

장치 로그 다운로드

장치에 저장된 로그 파일을 암호화된 형태로 다운로드할 수 있습니다. 장치 로그는 카메라 시스템에서 발생한 모든 이벤트와 운영 기록을 담은 상세 로그 파일입니다. 이 파일은 암호화되어 있어 보안이 유지되며, 필요할 때 슈프리마 기술 지원팀(CS@suprema.co.kr)에 제공하여 문제 해결에 활용할 수 있습니다.

1. 화면 왼쪽 상단의 **시스템** 메뉴를 클릭하세요.
2. 화면 왼쪽 사이드바에서 **시스템 로그**를 클릭하세요.
3. 로그 목록 왼쪽 상단의 **전체 로그**에서 **다운로드**를 선택하세요.



4. 특정 주체가 남긴 로그만 다운로드하려면 **전체 행위자**에서 행위자를 선택하세요. 선택하지 않으면 모든 행위자의 로그를 다운로드합니다. 행위자에 대한 자세한 내용은 행위자를 참고하세요.
5. 로그 목록 오른쪽 상단의 **다운로드** 버튼을 클릭하세요.

장치 로그 파일을 로컬에 다운로드할 수 있습니다. 파일 이름은 `device_logs_{device-serial-number}_YYYYMMDDTHHMMSS.zip.enc` 형식입니다.

> *예: device_logs_1234567890_20240326T153000.zip.enc*

시스템 로그 유형

시스템 로그에서 확인할 수 있는 로그 유형 정보를 안내합니다.

로그 유형	설명
CAM_AI_FACE_DETECTION	얼굴 감지
CAM_AI_FACE_AUTHENTICATION	얼굴 인증
CAM_AI_PERSON_DETECTION	사람 감지
CAM_AI_PERSON_ENTERED_AREA	영역 진입
CAM_AI_PERSON_EXITED_AREA	영역 이탈
CAM_AI_INTRUSION_ENTRY_AREA_APPEARED	침입 감지 (진입 영역)
CAM_AI_INTRUSION_EXIT_AREA_APPEARED	침입 감지 (이탈 영역)
CAM_AI_PEOPLE_COUNT_CHANGED	인원 카운트 변경
CAM_AI_PEOPLE_COUNT_LIMIT_REACHED	인원 카운트 한도 도달
CAM_AI_LINE_CROSSED	라인 크로싱
CAM_AI_FACE_AUTHENTICATION_FAILED	얼굴 인증 실패
CAM_AI_DOOR_ACCESS_EVENT_OFF	출입 이벤트 종료(재실 소진)
CAM_AI_DOOR_ACCESS_SOURCE	출입 판정 하위 신호
CAM_AI_DOOR_ACCESS_AREA_ENTERED	출입 영역 진입
CAM_AI_DOOR_ACCESS_AREA_EXITED	출입 영역 이탈
CAM_AI_DOOR_ACCESS_LINE_CROSSED	출입문 라인 통과
CAM_AI_DOOR_ACCESS_COUNT_CHANGED	출입 영역 인원 변경
CAM_EVT_RULE_TRIGGERED	룰 트리거됨
CAM_EVT_RULE_CREATED	룰 생성
CAM_EVT_RULE_UPDATED	룰 수정
CAM_EVT_RULE_DELETED	룰 삭제

로그 유형	설명
CAM_EVT_RULE_ENABLED	룰 활성화
CAM_EVT_RULE_DISABLED	룰 비활성화
CAM_EVT_RULE_USERS_ADDED	규칙 사용자 추가
CAM_EVT_RULE_USERS_REMOVED	규칙 사용자 제외
CAM_EVT_RULE_RELAY_SCHEDULE_BLOCKED	릴레이 거부 — 스케줄 미해당
CAM_EVT_WEBHOOK_SEND	웹훅 전송 시도
CAM_EVT_WEBHOOK_SENT	웹훅 전송 성공
CAM_EVT_WEBHOOK_FAILED	웹훅 전송 실패
CAM_EVT_WEBHOOK_CREATED	웹훅 생성
CAM_EVT_WEBHOOK_UPDATED	웹훅 수정
CAM_EVT_WEBHOOK_DELETED	웹훅 삭제
CAM_EVT_FACE_USER_CREATED	얼굴 사용자 생성
CAM_EVT_FACE_USER_UPDATED	얼굴 사용자 수정
CAM_EVT_FACE_USER_DELETED	얼굴 사용자 삭제
CAM_EVT_FACE_USER_CREATE_FAILED	얼굴 사용자 생성 실패
CAM_EVT_FACE_USER_UPDATE_FAILED	얼굴 사용자 수정 실패
CAM_EVT_FACE_USER_DELETE_FAILED	얼굴 사용자 삭제 실패
CAM_EVT_AI_ANALYSIS_CREATED	AI 분석 이벤트 생성
CAM_EVT_AI_ANALYSIS_UPDATED	AI 분석 이벤트 수정
CAM_EVT_AI_ANALYSIS_DELETED	AI 분석 이벤트 삭제
CAM_EVT_AI_ANALYSIS_DELETE_STARTED	AI 분석 이벤트 삭제 시작
CAM_EVT_AI_EVENT_SETTINGS_UPDATED	AI 이벤트 설정 변경
CAM_EVT_PEOPLE_COUNT_RESET_ALL	카운트 전체 초기화

로그 유형	설명
CAM_EVT_PEOPLE_COUNT_RESET	카운트 수동 초기화
CAM_EVT_PEOPLE_COUNT_AUTO_RESET	카운트 자동 초기화
CAM_EVT_AUDIO_CLIP_UPLOADED	오디오 클립 업로드
CAM_EVT_AUDIO_CLIP_DELETED	오디오 클립 삭제
CAM_EVT_AUDIO_CLIP_PLAY	오디오 클립 재생 요청
CAM_EVT_AUDIO_CLIP_PLAYED	오디오 클립 재생 성공
CAM_EVT_AUDIO_CLIP_PLAY_FAILED	오디오 클립 재생 실패
CAM_EVT_AUDIO_CLIP_API_PLAY	API 오디오 클립 재생 요청
CAM_EVT_AUDIO_CLIP_API_STOP	API 오디오 클립 정지 요청
CAM_EVT_RELAY_SENT	릴레이 신호 전송 시도
CAM_EVT_RELAY_FAILED	릴레이 통신 실패
CAM_EVT_RELAY_KEEP_STARTED	릴레이 상태 유지 시작
CAM_EVT_RELAY_KEEP_ENDED	릴레이 상태 유지 종료
CAM_EVT_RELAY_KEEP_REARM_FAILED	릴레이 상태 유지 재설정 실패
CAM_EVT_RELAY_OPENED	릴레이 일시 개방
CAM_EVT_RELAY_LOCKED	릴레이 고정 잠금
CAM_EVT_RELAY_RELEASED	릴레이 고정 제어 해제
CAM_EVT_RELAY_OPEN_REJECTED	릴레이 개방 거부(잠금 중)
CAM_EVT_RELAY_AUTO_CLOSED	릴레이 자동 재잠금
CAM_EVT_RELAY_STATE_RESTORED	릴레이 상태 복원
CAM_EVT_RELAY_UNLOCKED	릴레이 고정 개방
CAM_EVT_RELAY_IDLE_STATE_CHANGED	릴레이 극성 설정 변경
CAM_EVT_RELAY_IDLE_STATE_APPLIED	릴레이 극성 적용 완료

로그 유형	설명
CAM_EVT_RELAY_OPEN_FAILED	릴레이 개방 실패
CAM_EVT_RELAY_LOCK_FAILED	릴레이 잠금 실패
CAM_EVT_RELAY_RELEASE_FAILED	릴레이 해제 실패
CAM_EVT_RELAY_AUTO_CLOSE_FAILED	릴레이 자동 재잠금 실패
CAM_EVT_RELAY_STATE_RESTORE_FAILED	릴레이 상태 복원 실패
CAM_EVT_RELAY_UNLOCK_FAILED	릴레이 고정 개방 실패
CAM_EVT_RELAY_IDLE_STATE_CHANGE_FAILED	릴레이 극성 설정 실패
CAM_EVT_RELAY_IDLE_STATE_APPLY_FAILED	릴레이 극성 적용 실패
CAM_EVT_RELAY_TOKEN_MIGRATED	릴레이 식별자 마이그레이션
CAM_EVT_SCHEDULE_CREATED	스케줄 생성
CAM_EVT_SCHEDULE_UPDATED	스케줄 수정
CAM_EVT_SCHEDULE_DELETED	스케줄 삭제
CAM_EVT_SCHEDULE_LEGACY_MIGRATED	스케줄 데이터 이관
CAM_EVT_ACCESS_DOOR_CREATED	출입문 생성
CAM_EVT_ACCESS_DOOR_UPDATED	출입문 수정
CAM_EVT_ACCESS_DOOR_DELETED	출입문 삭제
CAM_EVT_ACCESS_DOOR_DELETE_STARTED	출입문 삭제 시작
CAM_EVT_ACCESS_DOOR_DELETE_FAILED	출입문 삭제 실패
CAM_EVT_ACCESS_LEVEL_CREATED	출입 레벨 생성
CAM_EVT_ACCESS_LEVEL_UPDATED	출입 레벨 수정
CAM_EVT_ACCESS_LEVEL_DELETED	출입 레벨 삭제
CAM_EVT_ACCESS_MEMBERSHIP_UPDATED	출입 레벨 사용자 배정 변경
CAM_EVT_ACCESS_POLICY_APPLY_STARTED	출입 정책 적용 시작

로그 유형	설명
CAM_EVT_ACCESS_POLICY_APPLIED	출입 정책 적용 완료
CAM_EVT_ACCESS_POLICY_APPLY_FAILED	출입 정책 적용 실패
CAM_EVT_ACCESS_RUNTIME_RECOVERED	출입 런타임 복구 성공
CAM_EVT_ACCESS_RUNTIME_RECOVER_FAILED	출입 런타임 복구 실패
CAM_EVT_ACCESS_POLICY_REBUILT_ON_BOOT	부팅 시 출입 정책 재구성
CAM_EVT_ACCESS_RUNTIME_DEGRADED	출입 런타임 기능 저하
CAM_EVT_ACCESS_DOOR_TRIGGER_CREATED	출입문 트리거 바인딩 생성
CAM_EVT_ACCESS_DOOR_TRIGGER_UPDATED	출입문 트리거 바인딩 수정
CAM_EVT_ACCESS_DOOR_TRIGGER_DELETED	출입문 트리거 바인딩 삭제
CAM_EVT_ACCESS_DOOR_PASSED_UNIDENTIFIED	출입 통과 — 미식별
CAM_EVT_ACCESS_DOOR_UNLOCK_REQUESTED	인증 성공 — 출입문 개방 요청
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_DOOR_MODE	출입 거부 — 문 잠금
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_UNIDENTIFIED	출입 거부 — 미식별
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED	출입 허가
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED_ALREADY_UNLOCKED	출입 허가(이미 개방 중)
CAM_EVT_ACCESS_DUAL_AUTH_PENDING	2인 인증 대기
CAM_EVT_ACCESS_DUAL_AUTH_TIMEOUT	2인 인증 시간 초과
CAM_EVT_ACCESS_DOOR_SCHEDULE_UNLOCKED	스케줄 개방 시작
CAM_EVT_ACCESS_DOOR_SCHEDULE_LOCKED	스케줄 잠금 시작
CAM_EVT_ACCESS_DOOR_SCHEDULE_RELEASED	스케줄 구간 종료
CAM_EVT_ACCESS_DOOR_HOLD_RELEASED	유지 개방 해제
CAM_EVT_ACCESS_DOOR_RULE_ACTION_SUCCEEDED	출입문 규칙 액션 성공
CAM_EVT_ACCESS_DOOR_RULE_ACTION_FAILED	출입문 규칙 액션 실패

로그 유형	설명
CAM_EVT_ACCESS_DOOR_RULE_CREATED	출입문 규칙 생성
CAM_EVT_ACCESS_DOOR_RULE_UPDATED	출입문 규칙 수정
CAM_EVT_ACCESS_DOOR_RULE_DELETED	출입문 규칙 삭제
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCKED	퇴실 버튼 개방
CAM_EVT_ACCESS_DOOR_EARLY_RELOCKED	문 닫힘 조기 재잠금
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCK_FAILED	퇴실 버튼 개방 실패
CAM_EVT_ACCESS_DOOR_PASSED	출입 통과(인증자)
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_ACCESS_LEVEL	출입 거부 — 권한 없음
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_TAILGATING	출입 거부 — 테일게이팅
CAM_EVT_ACCESS_DOOR_UNLOCK_FAILED	개방 실패(설비)
CAM_EVT_ACCESS_DOOR_PASSED_AFTER_DENIED	출입 통과 — 거부 후
CAM_EVT_ACCESS_DOOR_RULE_ACTION_RETRYING	출입문 규칙 액션 재시도
CAM_EVT_ACCESS_DOOR_RULE_MUTATION_REJECTED	출입문 규칙 변경 거부
CAM_EVT_HEATER_CONTROL_REQUESTED	히터 제어 요청
CAM_EVT_HEATER_ENABLED	히터 켬
CAM_EVT_HEATER_DISABLED	히터 끔
CAM_EVT_HEATER_AUTO_DISABLED	히터 자동 끔
CAM_EVT_HEATER_CONTROL_FAILED	히터 제어 실패
CAM_EVT_HEATER_STATE_RECONCILED	히터 상태 재조정
CAM_EVT_HEATER_BOOT_RECOVERED	히터 부팅 복구
CAM_EVT_HEATER_BOOT_RECOVERY_FAILED	히터 부팅 복구 실패
CAM_EVT_HEATER_FAULT_DISABLED	히터 장애로 끔
CAM_EVT_INPUT_IDLE_STATE_CHANGED	입력 포트 극성 변경

로그 유형	설명
CAM_EVT_INPUT_IDLE_STATE_CHANGE_FAILED	입력 포트 극성 변경 실패
CAM_SYS_NETWORK_CHANGE	네트워크 설정 변경
CAM_SYS_NETWORK_DHCP_FALLBACK	DHCP 실패 Link-local 전환
CAM_SYS_DATETIME_CHANGE	날짜/시간 설정 변경
CAM_SYS_NTP_SYNC_FAILED	NTP 동기화 실패
CAM_SYS_FIRMWARE_UPGRADE	펌웨어 업그레이드
CAM_SYS_SYSTEM_STARTED	웹서버 시작
CAM_SYS_FACTORY_RESET	공장 초기화
CAM_SYS_CONFIG_RESET	설정 초기화
CAM_SYS_SYSTEM_REBOOT	시스템 재부팅
CAM_SYS_CLUE_ENABLED	CLUe 활성화 성공
CAM_SYS_CLUE_DISABLED	CLUe 비활성화
CAM_SYS_CLUE_ENABLE_FAILED	CLUe 활성화 실패
CAM_SYS_CLUE_USER_SYNC_CHANGED	CLUe 사용자 동기화 변경
CAM_SYS_CLUE_TUNNEL_CHANGED	CLUe 터널 변경
CAM_SYS_CONSENT_ENROLLMENT_CHANGED	얼굴 등록 동의 변경
CAM_SYS_CONSENT_ANALYTICS_CHANGED	얼굴 분석 동의 변경
CAM_SYS_AI_SETTINGS_CHANGED	AI 설정 변경
CAM_SYS_AI_LOAD_FAILED	AI 기능 로딩 실패
CAM_SYS_SECURE_TAMPER_CHANGED	Secure Tamper 설정 변경
CAM_SYS_TUNNEL_MODE_CHANGED	터널 모드 변경
CAM_SYS_TUNNEL_SETTING_UPDATED	터널 설정 변경
CAM_SYS_WEBRTC_SESSION_START	WebRTC 세션 시작

로그 유형	설명
CAM_SYS_WEBRTC_SESSION_END	WebRTC 세션 종료
CAM_SYS_CRYPTO_KEYGEN_FAILED	암호 키 생성 실패
CAM_SYS_CRYPTO_OP_FAILED	암호 연산 실패
CAM_SYS_SLAVE_CONNECTED	RS485 슬레이브 연결
CAM_SYS_SLAVE_DISCONNECTED	RS485 슬레이브 연결 끊김
CAM_SYS_RS485_SLAVE_FW_UPDATE_SUCCEEDED	슬레이브 펌웨어 업데이트 성공
CAM_SYS_RS485_SLAVE_FW_UPDATE_FAILED	슬레이브 펌웨어 업데이트 실패
CAM_SYS_ONVIF_MODE_CHANGED	ONVIF 모드 변경
CAM_SYS_ONVIF_HTTP_PROXY_FAILED	ONVIF HTTP 프록시 실패
CAM_SYS_API_OPERATION_FAILED	API 작업 실패
CAM_SYS_API_COMPLETION_UNCONFIRMED	API 작업 완료 미확인
CAM_SYS_API_REQUEST_REJECTED	API 요청 거부
CAM_ACC_LOGIN	로그인
CAM_ACC_LOGOUT	로그아웃
CAM_ACC_TOKEN_REFRESH	토큰 갱신
CAM_ACC_PASSWORD_CHANGE	비밀번호 변경
CAM_ACC_AUTH_FAILURE	인증 실패
CAM_ACC_REFRESH_TOKEN_REUSE	리프레시 토큰 재사용 감지
CAM_ACC_SESSION_INVALIDATED	세션 무효화
CAM_ACC_RATE_LIMIT_EXCEEDED	요청 제한 초과
CAM_ACC_FORBIDDEN_ACCESS	권한 없는 접근
CAM_ACC_PASSWORD_SETUP	초기 비밀번호 설정
CAM_ACC_ACCOUNT_LOCKED	계정 잠금

로그 유형	설명
CAM_ACC_SESSION_EXPIRED	세션 만료
CAM_ACC_ACCOUNT_CREATED	계정 생성
CAM_ACC_ACCOUNT_UPDATED	계정 수정
CAM_ACC_ACCOUNT_DELETED	계정 삭제
CAM_ACC_ACCOUNT_DISABLED	계정 비활성화
CAM_ACC_SESSION_KICKED	세션 강제 종료
CAM_ACC_LOGIN_FAILED	로그인 실패
CAM_ACC_PERMISSION_DENIED	권한 부족 거부
CAM_ACC_SESSION_LIMIT_REJECTED	세션 한도 초과 거부
CAM_ACC_ACCOUNT_CREATE_FAILED	계정 생성 실패

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.

(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.