

AXIS P1465-LE-3 License Plate Verifier Kit

시작하기

네트워크에서 장치 찾기

네트워크에서 Axis 장치를 찾고 Windows®에서 해당 장치에 IP 주소를 할당하려면 AXIS IP Utility 또는 AXIS Device Manager를 사용합니다. 두 애플리케이션은 axis.com/support에서 무료로 다운로드할 수 있습니다.

IP 주소를 할당하고 장치에 액세스하는 방법으로 이동하여 어떻게 IP 주소를 찾아 할당하는지 자세히 알아보십시오.

브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
기타 운영 체제	*	*	*	*

✓: 권장

*: 제한을 두고 지원

장치의 웹 인터페이스 열기

1. 브라우저를 열고 Axis 장치의 IP 주소 또는 호스트 이름을 입력합니다.
IP 주소를 모르는 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다.
2. 사용자 이름과 패스워드를 입력합니다. 장치에 처음 액세스하는 경우, 관리자 계정을 생성해야 합니다. *관리자 계정 생성, on page 2*을 참조하십시오.

AXIS OS가 탑재된 장치의 웹 인터페이스에 있는 모든 기능과 설정에 대한 설명은 *AXIS OS 웹 인터페이스 도움말*을 참조하십시오.

관리자 계정 생성

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 사용자 이름을 입력하십시오.
2. 패스워드를 입력합니다. *안전한 패스워드, on page 3*을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이선스 계약을 수락하십시오.
5. **Add account(계정 추가)**를 클릭합니다.

중요 사항

장치에 기본 계정이 없습니다. 관리자 계정의 패스워드를 잊어버린 경우, 장치를 재설정해야 합니다. *공장 출하 시 기본 설정으로 재설정, on page 47*을 참조하십시오.

안전한 패스워드

중요 사항

네트워크를 통해 패스워드 또는 기타 민감한 구성을 설정하려면 HTTPS(기본적으로 활성화됨)를 사용하십시오. HTTPS는 보안 및 암호화된 네트워크 연결을 활성화하여 패스워드와 같은 민감한 데이터를 보호합니다.

장치 패스워드는 데이터 및 서비스에 대한 기본 보호입니다. Axis 장치는 다양한 설치 유형에 사용될 수 있으므로 해당 장치에는 패스워드 정책을 적용하지 않습니다.

데이터 보호를 위해 적극 권장되는 작업은 다음과 같습니다.

- 최소 8자 이상의 패스워드를 사용합니다. 패스워드 생성기로 패스워드를 생성하는 것이 더 좋습니다.
- 패스워드를 노출하지 않습니다.
- 최소 일 년에 한 번 이상 반복되는 간격으로 패스워드를 변경합니다.

아무도 장치 소프트웨어를 조작하지 않았는지 확인

장치에 원래 AXIS OS가 있는지 확인하거나 보안 공격 후 장치를 완전히 제어하려면 다음을 수행합니다.

1. 공장 출하 시 기본 설정으로 재설정합니다. *공장 출하 시 기본 설정으로 재설정, on page 47*을 참조하십시오.
재설정 후 Secure Boot는 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

웹 인터페이스 개요

이 영상은 장치의 웹 인터페이스에 대한 개요를 제공합니다.



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

Axis 장치 웹 인터페이스

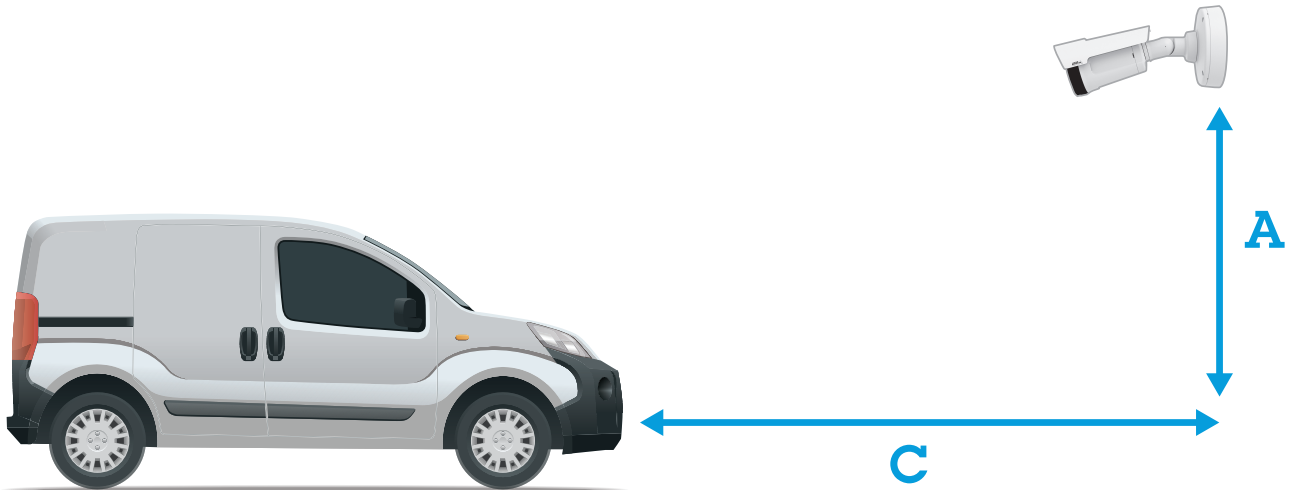
기본 설정

이러한 설정 지침은 모든 시나리오에 유효합니다.

- 1.
- 2.
3. 관심 영역 조정, on page 8
4. 지역 선택, on page 9
5. 이벤트 저장 설정, on page 9

카메라 마운팅 권장 사항

- 장착 위치를 선택할 때 일출 및 일몰과 같은 직사광선이 이미지를 왜곡시킬 수 있음을 기억하십시오.
- **Access control(접근 제어)** 시나리오에서 카메라의 장착 높이는 차량과 카메라 사이 거리의 절반이어야 합니다.
- **Free flow(자유 흐름)**(저속 교통 번호판 인식) 시나리오에서 카메라의 장착 높이는 차량과 카메라 사이 거리의 절반 미만이어야 합니다.



접근 제어 캡처 거리: 2~7m(6.6~23ft). 이 예는 AXIS P3265-LVE-3 License Plate Verifier Kit를 기반으로 합니다.

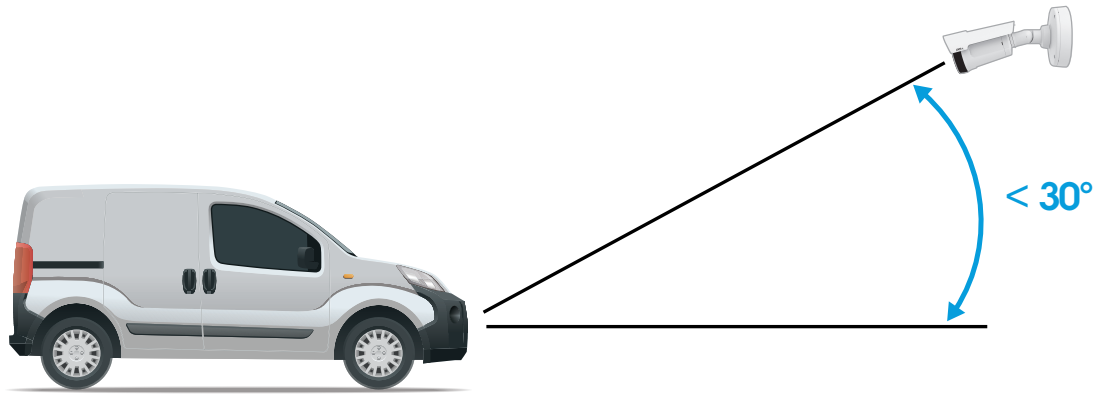
캡처 거리: (C)	마운팅 높이(A)
2.0m(6.6ft)	1.0m(3.3ft)
3.0m(9.8ft)	1.5m(4.9ft)
4.0m(13ft)	2.0m(6.6ft)
5.0m(16ft)	2.5m(8.2ft)
7.0m(23ft)	3.5m(11ft)

자유 흐름 캡처 거리: 7~20m(23~65ft). 이 예는 AXIS P1465-LE-3 License Plate Verifier Kit를 기반으로 합니다.

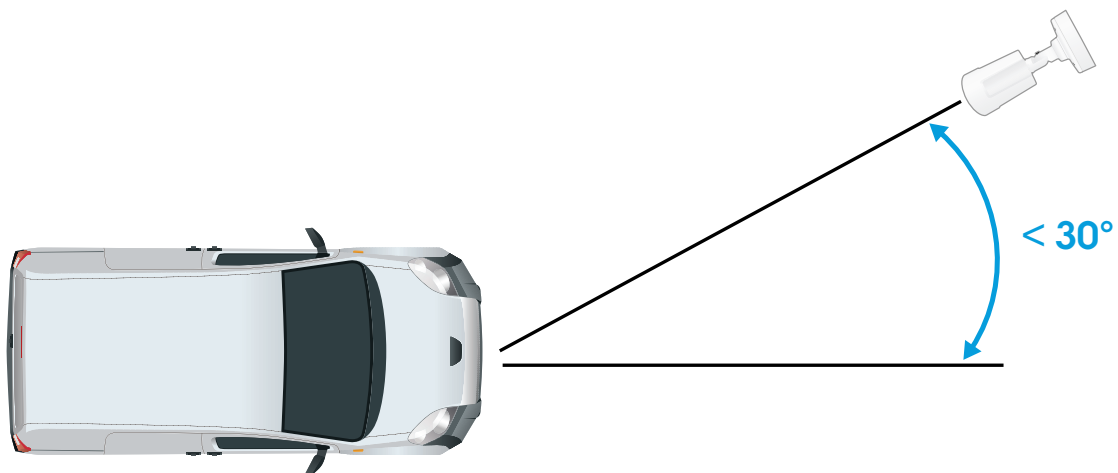
캡처 거리 (C)	마운팅 높이(A)
7.0m(23ft)	3.0m(9.8ft)
10.0m(33ft)	4.0m(13ft)

15.0m(49ft)	6.0m(19.5ft)
20.0m(65ft)	10.0m(33ft)

- 카메라의 장착 각도는 어떤 방향으로든 30°보다 크면 안 됩니다.

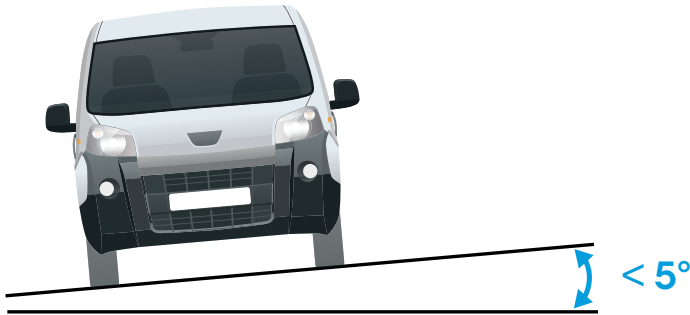


측면에서의 장착 각도.



위쪽에서의 장착 각도.

- 번호판의 이미지가 수평으로 5° 이상 기울어져서는 안 됩니다. 이미지가 5° 이상 기울어진 경우 번호판이 실시간 스트림에 수평으로 표시되도록 카메라를 조정하는 것이 좋습니다.



롤 각도.

설정 도우미

애플리케이션을 처음 실행할 때 설정 도우미를 사용하여 **Free flow(자유 흐름)** 또는 **Access control(접근 제어)**을 설정합니다. 나중에 변경하려면 **Settings(설정) > Maintenance(유지 관리)**로 이동하고 **Setup assistant(설치 도우미)**에서 **Start(시작)**를 누릅니다.

자유 흐름

자유 흐름에서 애플리케이션은 넓은 접근 도로와 캠퍼스, 항구 또는 공항과 같은 도심과 폐쇄된 지역에서 느린 속도로 통행할 때 번호판을 감지하고 읽을 수 있습니다. 이를 통해 VMS에서 LPR 포렌식 검색과 LPR 트리거된 이벤트가 가능합니다.

1. **Free flow(자유 흐름)**를 선택하고 **Next(다음)**를 클릭합니다.
2. 카메라가 장착된 방식에 해당하는 이미지 회전을 선택합니다.
3. 관심 영역의 수를 선택합니다. 한 영역에서 양방향으로 번호판을 감지할 수 있습니다.
4. 카메라가 있는 지역을 선택합니다.
5. 캡처 유형을 선택합니다.
 - **License plate crop(번호판 자르기)**은 번호판만 저장합니다.
 - **Vehicle crop(차량 자르기)**은 캡처한 차량 전체를 저장합니다.
 - **Frame downsized 480x270(480x270으로 축소된 프레임)**은 전체 이미지를 저장하고 해상도를 480x270으로 줄입니다.
 - **Full frame(풀 프레임)**은 전체 이미지를 전체 해상도로 저장합니다.
6. 앵커 포인트를 끌어 관심 영역을 조정합니다. *관심 영역 조정, on page 8*을 참조하십시오.
7. 관심 영역의 방향을 조정합니다. 화살표를 클릭하고 회전하여 방향을 설정합니다. 방향은 애플리케이션이 해당 영역에 진입하거나 나가는 차량을 등록하는 방법을 결정합니다.
8. **Next(다음)**를 클릭합니다.
9. **Protocol(프로토콜)** 드롭다운 목록에서 다음 프로토콜 중 하나를 선택합니다.
 - TCP
 - HTTP POST
10. **Server URL(서버 URL)** 필드에 서버 주소 및 포트를 127.0.0.1:8080 형식으로 입력합니다.
11. **Device ID(장치 ID)** 필드에 장치의 이름을 입력하거나 그대로 둡니다.
12. **Event types(이벤트 유형)**에서 다음 옵션 중 하나 이상을 선택합니다.
 - **New(신규)**란 번호판의 첫 번째 감지를 의미합니다.

- **Update(업데이트)**는 이전에 감지된 번호판의 문자를 수정하거나 번호판이 이동하고 이미지에서 추적될 때 방향이 감지되는 것입니다.
 - **Lost(손실)**는 이미지를 종료하기 전에 번호판에서 마지막으로 추적된 이벤트입니다. 번호판의 방향도 포함되어 있습니다.
13. 이 기능을 켜려면 **Send event data to server(서버에 이벤트 데이터 보내기)**를 선택합니다.
 14. HTTP POST를 사용할 때 대역폭을 줄이기 위해 **Do not to send images through HTTP POST (HTTP POST를 통해 이미지를 전송하지 않음)**를 선택할 수 있습니다.
 15. **Next (다음)**를 클릭합니다.
 16. 등록된 번호판 목록이 이미 있는 경우 **blocklist(차단 목록)** 또는 **allowlist(허용 목록)**로 가져오도록 선택합니다.
 17. **Finish (마침)**를 클릭합니다.

접근 제어

빠르고 쉬운 구성을 위해 설정 마법사를 사용합니다. **Skip(건너뛰기)**을 선택하여 언제든지 가이드에서 나갈 수 있습니다.

1. **Access control(접근 제어)**을 선택하고 **Next(다음)**를 클릭합니다.
2. 사용할 접근 제어 유형을 선택합니다.
 - **Internal I/O(내부 I/O)** - 카메라에서 목록 관리를 유지하려면 경우. *카메라의 I/O를 사용하여 알려진 차량에 대해 장벽 개방, on page 28*을 참조하십시오.
 - **Controller(컨트롤러)** - 도어 컨트롤러를 연결하려는 경우. 을 참조하십시오.
 - **Relay(릴레이)** 릴레이 모듈에 연결하려는 경우. 을 참조하십시오.
3. **Barrier mode(장벽 모드)** 드롭다운 목록의 **Open from lists(목록에서 열기)**에서 **Allowlist(허용 목록)**를 선택합니다.
4. **Vehicle direction(차량 방향)** 드롭다운 목록에서 **out(출차)**을 선택합니다.
5. **ROI** 드롭다운 목록에서 사용할 관심 영역 또는 모두를 사용할지 여부를 선택합니다.
6. **Next (다음)**를 클릭합니다.

Image settings(이미지 설정) 페이지에서:

1. 관심 영역의 수를 선택합니다.
2. 카메라가 있는 지역을 선택합니다.
3. 캡처 유형을 선택합니다. *이미지 캡처 설정 조정, on page 9*을 참조하십시오.
4. 앵커 포인트를 끌어 관심 영역을 조정합니다. *관심 영역 조정, on page 8*을 참조하십시오.
5. 관심 영역의 방향을 조정합니다. 방향은 애플리케이션이 해당 영역에 진입하거나 나가는 차량을 등록하는 방법을 결정합니다.
6. **Next(다음)**를 클릭합니다.

이벤트 데이터 페이지에서:

비고

자세한 설정은 다음을 참조하십시오. *타사 소프트웨어에 이벤트 정보 푸시, on page 36*

1. **Protocol(프로토콜)** 드롭다운 목록에서 다음 프로토콜 중 하나를 선택합니다.
 - TCP
 - HTTP POST
2. **Server URL(서버 URL)** 필드에 서버 주소 및 포트를 다음 형식으로 입력합니다.
127.0.0.1:8080
3. **Device ID(장치 ID)** 필드에 장치의 이름을 입력하거나 그대로 둡니다.
4. **Event types(이벤트 유형)**에서 다음 옵션 중 하나 이상을 선택합니다.

- **New(신규)**란 번호판의 첫 번째 감지를 의미합니다.
 - **Update(업데이트)**는 이전에 감지된 번호판의 문자를 수정하거나 번호판이 이동하고 이미지에서 추적될 때 방향이 감지되는 것입니다.
 - **Lost(손실)**는 이미지를 종료하기 전에 번호판에서 마지막으로 추적된 이벤트입니다. 번호판의 방향도 포함되어 있습니다.
5. 이 기능을 켜려면 **Send event data to server(서버에 이벤트 데이터 보내기)**를 선택합니다.
 6. HTTP POST를 사용할 때 대역폭을 줄이기 위해 **Do not to send images through HTTP POST (HTTP POST를 통해 이미지를 전송하지 않음)**를 선택할 수 있습니다.
 7. **Next(다음)**를 클릭합니다.

.csv 파일에서 목록 가져오기 페이지에서:

1. 등록된 번호판 목록이 이미 있는 경우 **blocklist(차단 목록)** 또는 **allowlist(허용 목록)**로 가져오도록 선택합니다.
2. **Finish (마침)**를 클릭합니다.

애플리케이션 설정 액세스

1. 카메라의 웹 인터페이스에서 **Apps(앱)**로 이동하고 애플리케이션을 시작한 후 **Open(열기)**을 클릭합니다.

관심 영역 조정

관심 영역은 애플리케이션이 번호판을 찾는 실시간 보기 영역입니다. 최적의 성능을 위해 관심 영역을 최대한 작게 유지하십시오. 관심 영역을 조정하려면 다음을 수행합니다.

1. **Settings(설정)**로 이동합니다.
2. **Image(이미지)**를 클릭합니다.
3. 통행 모니터링 또는 접근 제어 관리를 수행하려는 위치를 1:1로 확대하려면 1:1을 클릭합니다.
4. 인증 및 캡처된 이미지 품질을 개선하려면 **AF**를 클릭합니다.
5. 카메라가 차량에 자동으로 초점을 맞추게 하려면 **AF**를 클릭합니다. 수동으로 초점을 맞추려면 슬라이더를 사용하여 조정합니다.
6. 보기 영역에 표시하려면 **Area of interest(관심 영역)**를 클릭합니다.
7. 관심 영역을 이동하려면 영역 내 아무 곳이나 클릭하여 선택한 후 번호판이 가장 잘 보이는 위치로 드래그합니다. 설정을 저장한 후에 관심 영역이 올바른 위치에 있는지 확인하십시오.
8. 관심 영역을 조정하려면 영역 내 아무 곳이나 클릭하여 선택한 후 파란색으로 강조된 앵커 포인트를 드래그합니다.
 - 관심 영역을 재설정하려면 번호 아이콘 옆 왼쪽 하단 모서리에 있는 재설정 버튼을 클릭합니다.
 - 앵커 포인트를 추가하려면 어두운 색의 앵커 포인트 중 하나를 클릭합니다. 앵커 포인트가 노란색으로 변하며 조작 가능함을 나타냅니다. 새로운 어두운 지점들이 노란색 앵커 포인트 옆에 자동으로 추가됩니다. 노란색 앵커 포인트는 최대 8개까지 가능합니다.
9. 변경 사항을 저장하려면 관심 영역 외부의 아무 곳이나 클릭합니다.
10. **Event log(이벤트 로그)**에서 올바른 방향 피드백을 얻으려면 화살표를 주행 방향에 맞도록 돌려야 합니다.
 - 10.1. 화살표 아이콘을 클릭합니다.
 - 10.2. 앵커 포인트를 선택하고 화살표를 회전하여 주행 방향에 맞춥니다.
 - 10.3. 변경 사항을 저장하려면 관심 영역 외부를 클릭합니다.

한 영역에서 양방향으로 번호판을 감지할 수 있습니다. **Direction(방향)** 열에 방향 피드백이 표시됩니다.

11. 최상의 결과를 위해 관심 영역이 충분히 큰지 확인하려면 픽셀 카운터를 사용합니다.

- 픽셀 카운터를 표시하려면 계산기 아이콘을 클릭합니다.
- 전체 크기 픽셀 카운터 영역을 조정하려면 노란색으로 강조된 영역의 오른쪽 하단 모서리를 드래그합니다.
- 픽셀 카운터 영역을 이동하려면 영역 내 아무 곳이나 클릭하고 원하는 위치로 드래그합니다.
- 두 번째 관심 영역을 추가하려면 **1** 옆에 있는 **+**를 클릭합니다.
- 독립형 카메라를 사용하는 경우, 앱에서 번호판 인식에 대한 권장 설정을 지정하도록 할 수 있습니다.
 1. 마술 지팡이 아이콘을 클릭하면 번호판 인식에 최적화된 설정이 적용됩니다.
 2. 설정된 값을 확인하려면 마술 지팡이 옆의 메뉴 버튼을 클릭합니다.

지역 선택

1. **Settings(설정) > Recognition(인식)**으로 이동합니다.
2. **Region(지역)** 드롭다운 목록에서 지역을 선택합니다.

이미지 캡처 설정 조정

1. **Settings(설정) > Image(이미지)**로 이동합니다.
2. 캡처된 이미지의 해상도를 변경하려면 **Image resolution(이미지 해상도)**으로 이동합니다.
3. 캡처된 이미지의 회전 방향을 변경하려면 **Rotation(회전)**으로 이동합니다.

이벤트 저장 설정

이벤트는 캡처된 이미지, 번호판, 관심 영역 번호, 차량방향, 출입, 날짜와 시간으로 구성됩니다.

이 예의 사용 사례에서는 허용 목록에 있는 번호판 번호의 이벤트를 30일 동안 저장하는 방법을 설명합니다.

요구 사항:

- 물리적으로 설치되고 네트워크에 연결된 카메라.
- AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
- 내부 저장소 또는 카메라에 설치된 SD 카드.

1. **Settings(설정) > Storage(스토리지)**로 이동합니다.
2. **Retain events(이벤트 보존)**에서 **Allowlisted(허용 목록에 포함됨)**를 선택합니다.
3. **Retention period(보존 기간)**에서 **30 days(30일)**를 선택합니다.
4. 캡처한 이미지를 저장하는 방법을 변경하려면 **Save full frame(풀 프레임 저장)**으로 이동합니다.
 - **License plate crop(번호판 자르기)**은 번호판만 저장합니다.
 - **Vehicle crop(차량 자르기)**은 캡처한 차량 전체를 저장합니다.
 - **Frame downsized 480x270(480x270으로 축소된 프레임)**은 전체 이미지를 저장하고 해상도를 480x270으로 줄입니다.
 - **Full frame(풀 프레임)**은 전체 이미지를 전체 해상도로 저장합니다.

비고

앱 실행 시 삽입된 SD 카드를 감지하려면 앱을 재시작해야 합니다. 카메라에 SD 카드가 설치되어 있으면 앱이 자동으로 SD 카드를 기본 저장소로 선택합니다.

AXIS License Plate Verifier는 카메라 내부 메모리를 사용하여 번호판 자르기를 프레임으로 사용하여 최대 1,000개의 이벤트를 저장합니다. 더 큰 프레임을 사용하는 경우 저장할 수 있는 이벤트의 양이 달라집니다.

SD 카드는 모든 유형의 프레임 사용하여 최대 100,000개의 이벤트를 저장할 수 있습니다.

설치



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

제품 설치 영상

미리 보기 모드

미리 보기 모드는 설치 중 카메라 보기를 미세 조정할 때 설치자에게 이상적입니다. 미리 보기 모드에서 카메라 보기에 액세스하는 데 로그인 필요하지 않습니다. 장치 전원을 켜 후 제한된 시간 동안 공장 출하 시 기본 설정 상태로만 사용할 수 있습니다.



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

이 영상은 미리 보기 모드를 사용하는 방법을 보여줍니다.

장치 구성

AXIS Camera Station 사용자의 경우

AXIS License Plate Verifier 설정

AXIS License Plate Verifier로 장치가 구성되면 영상 관리 시스템에서 외부 데이터 소스로 간주됩니다. 보기를 데이터 소스에 연결하고 장치에서 캡처한 번호판을 검색하고 관련 이미지를 볼 수 있습니다.

비고

- 이 경우 AXIS Camera Station 5.38 이상이 필요합니다.
 - AXIS License Plate Verifier는 라이선스가 필요합니다.
1. 장치에 애플리케이션을 다운로드하여 설치합니다.
 2. 애플리케이션을 구성합니다. *AXIS License Plate Verifier 사용자 설명서*를 참조하십시오.
 3. 기존 AXIS Camera Station 설치 시 클라이언트 통신에 사용되는 서버 인증서를 갱신하십시오. *인증서 갱신*을 참조하십시오.
 4. 시간 동기화를 커서 AXIS Camera Station 서버를 NTP 서버로 사용합니다. *서버 설정*을 참조하십시오.
 5. AXIS Camera Station에 장치를 추가합니다. *장치 추가*를 참조하십시오.
 6. 첫 번째 이벤트가 수신되면 **Configuration > Devices > External data sources(구성 > 장치 > 외부 데이터 소스)** 아래에 데이터 소스가 자동으로 추가됩니다.
 7. 데이터 소스를 보기에 연결합니다. *외부 데이터 소스* 항목을 참고하십시오.
 8. 장치에서 캡처한 번호판을 검색합니다. *데이터 검색* 항목을 참조하십시오.
 9.  을 클릭하여 검색 결과를 .txt 파일로 내보냅니다.

기본 설정

장면 프로파일 설정

1. **Video > Image > Appearance(비디오 > 이미지 > 모양)**으로 이동합니다.
2. **Scene profile(장면 프로파일)**에서 **Change(변경)**를 클릭합니다.

전력선 주파수 설정

1. **Video > Installation > Power line frequency(비디오 > 설치 > 전력선 주파수)**로 이동합니다.
2. 전력선 주파수를 선택하고 **Save and restart(저장 후 재시작)**를 클릭합니다.

이미지 조정

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다.

카메라 수평 맞추기

참조 영역 또는 물체와 관련하여 보기를 조정하려면 레벨 그리드를 카메라의 기계적 조정과 함께 사용합니다.

1. **Video(비디오) > Image(이미지) >** 로 이동하여  을 클릭합니다.
2. 수평 그리드를 표시하려면  을 클릭합니다.
3. 참조 영역 또는 물체의 위치가 레벨 그리드와 정렬될 때까지 카메라를 기계적으로 조정합니다.

낮은 지연 시간 모드로 이미지 처리 시간 단축

낮은 지연 시간 모드를 켜서 라이브 스트림의 이미지 처리 시간을 최적화할 수 있습니다. 라이브 스트림의 지연 시간이 최소로 단축됩니다. 낮은 지연 시간 모드를 사용하면 평소보다 이미지 품질이 저하됩니다.

1. **System > Plain config(시스템 > 일반 구성)**로 이동합니다.
2. 드롭다운 목록에서 **ImageSource(이미지소스)**를 선택합니다.
3. **ImageSource/I0/Sensor > Low latency mode(낮은 지연 모드)**로 이동하여 **On(켜기)**를 선택합니다.
4. **Save(저장)**를 클릭합니다.

노출 모드 선택

특정 감시 장면에 대한 이미지 품질을 향상시키려면 노출 모드를 사용하십시오. 노출 모드를 사용하면 조리개, 셔터 속도 및 게인을 제어할 수 있습니다. **Video > Image > Exposure(비디오 > 이미지 > 노출)**로 이동하여 다음 노출 모드 중에서 선택합니다.

- 대부분의 경우에 **Automatic exposure(자동 노출)**를 선택합니다.
- 형광등 조명과 같이 특정 인공 조명이 있는 환경에서는 **Flicker-free(깜박임 제거)**를 선택합니다.
전력선 주파수와 동일한 주파수를 선택합니다.
- 특정 인공 조명 및 밝은 조명이 있는 환경(예: 밤에 형광등 조명이 있는 야외, 낮에 태양광이 있는 야외)에서는 **Flicker-reduced(깜박임 감소)**를 선택하십시오.
전력선 주파수와 동일한 주파수를 선택합니다.
- 현재 노출 설정을 잠그려면 **Hold current(현재 설정 유지)**를 선택합니다.

술통형 왜곡 보정

술통형 왜곡은 직선이 프레임의 가장자리에 가까워 질수록 나타나는 현상입니다. 넓은 화각은 종종 이미지에서 술통형 왜곡을 만듭니다. 술통형 왜곡 보정은 이 왜곡을 보정합니다.

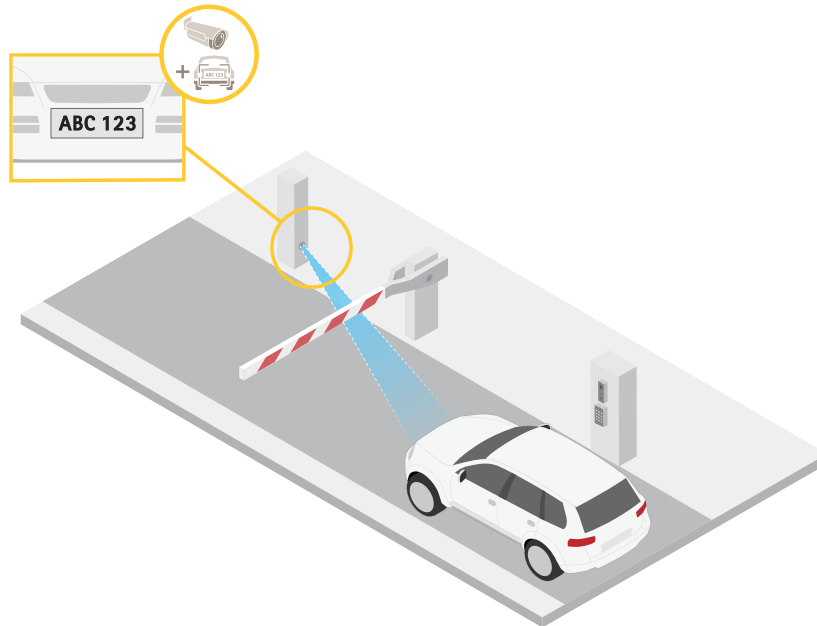
비고

술통형 왜곡 보정은 이미지 해상도 및 화각에 영향을 줍니다.

1. **Video > Installation > Image correction(비디오 > 설치 > 이미지 보정)**으로 이동합니다.
2. **Barrel distortion correction (BDC)(술통형 왜곡 보정)**을 켭니다.

픽셀 해상도 확인

예를 들어, 이미지의 정의된 부분에 자동차 번호판을 인식하기에 충분한 픽셀이 포함되어 있는지 확인하려면 픽셀 카운터를 사용할 수 있습니다.



1. **비디오 > 이미지**로 이동합니다.
2.  을 클릭합니다.
3. **Pixel counter(픽셀 카운터)**에 대해  을 클릭합니다.
4. 카메라의 라이브 뷰에서 관심 영역 주변의 직사각형 크기와 위치를 조정합니다 (예: 번호판이 표시될 것으로 예상되는 위치).
5. 직사각형의 각 변에 대한 픽셀 수를 볼 수 있고, 값이 요건에 충분히 맞는지 결정할 수 있습니다.

비디오 보기 및 녹화

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다. 스트리밍 및 저장 작동 방식에 대해 자세히 알아보려면 [으로 이동하십시오](#).

대역폭 및 저장 공간 감소

중요 사항

대역폭을 줄이면 이미지의 세부 정보가 손실될 수 있습니다.

1. **Video > Stream(비디오 > 스트림)**으로 이동합니다.
2. 실시간 보기에서  을 클릭합니다.
3. 장치에서 지원하는 경우 **Video format(비디오 형식) AV1**을 선택합니다. 그렇지 않으면 **H.264**를 선택합니다.
4. **Video > Stream > General(비디오 > 스트림 > 일반)**으로 이동하고 **Compression(압축)**을 높입니다.
5. **Video > Stream > Zipstream(비디오 > 스트림 > Zipstream)**으로 이동하고 다음 중 하나 이상을 수행합니다.

비고

Zipstream 설정은 MJPEG를 제외한 모든 비디오 엔코더에 사용됩니다.

- 사용할 Zipstream **Strength(강도)**를 선택합니다.
- **Optimize for storage(스토리지 최적화)**를 켭니다. 영상 관리 소프트웨어가 B-프레임을 지원하는 경우에만 사용할 수 있습니다.

- **Dynamic FPS(동적 FPS)**를 켭니다.
- **Dynamic GOP(동적 DOP(group of pictures))** 기능을 켜고 높은 **Upper limit(상한)** GOP 길이 값을 설정합니다.

비고

대부분의 웹 브라우저는 H.265 디코딩을 지원하지 않으며, 이 때문에 장치는 웹 인터페이스에서 H.265 디코딩을 지원하지 않습니다. 대신 H.265 디코딩을 지원하는 영상 관리 시스템 또는 애플리케이션을 사용할 수 있습니다.

네트워크 스토리지 설정

네트워크에 녹화를 저장하려면 사용자의 네트워크 스토리지를 설정해야 합니다.

1. **System(시스템) > Storage(스토리지)**로 이동합니다.
2. **Network storage(네트워크 스토리지)**에서  **Add network storage(네트워크 스토리지 추가)**를 클릭합니다.
3. 호스트 서버의 IP 주소를 입력합니다.
4. **Network Share(네트워크 공유)** 아래에서 호스트 서버에 공유 위치의 이름을 입력합니다.
5. 사용자 이름과 패스워드를 입력합니다.
6. SMB 버전을 선택하거나 **Auto(자동)**에 그대로 둡니다.
7. 일시적인 연결 문제가 발생하거나 공유가 아직 구성되지 않은 경우 **Add share even if connection fails(테스트 없이 공유 추가)**를 선택합니다.
8. **추가**를 클릭합니다.

비디오 녹화 및 시청

카메라에서 직접 비디오 녹화

1. **Video > Stream(비디오 > 스트림)**으로 이동합니다.
2. 녹화를 시작하려면  을 클릭합니다.
스토리지를 설정하지 않은 경우,  및  을 클릭합니다. 네트워크 스토리지를 설정하는 방법의 지침은 **네트워크 스토리지 설정, on page 15**을 참조하십시오.
3. 녹화를 중지하려면 다시  을 클릭합니다.

동영상 보기

1. **Recordings(녹화)**로 이동합니다.
2. 목록에 있는 녹화에 대해  을 클릭합니다.

비디오를 조작한 사람이 없는지 확인

서명된 비디오를 사용하면 카메라에 녹화된 영상을 누군가 변조하지 않았는지 확인할 수 있습니다.

1. **Video > Stream > General(비디오 > 스트림 > 일반)**로 이동하여 **Signed video(서명된 비디오)**를 켭니다.
2. 장치에서 직접 비디오를 녹화하거나 AXIS Camera Station Pro 또는 기타 호환 가능한 비디오 매니지먼트 소프트웨어를 사용합니다. AXIS Camera Station Pro 지침은 **AXIS Camera Station Pro 사용자 설명서**를 참조하십시오.
3. 녹화된 영상을 내보냅니다.
4. 녹화 영상을 확인하려면 *Axis signed media verifier* 도구를 사용하십시오.

이벤트의 룰 설정

특정 이벤트가 발생하면 장치에서 액션을 수행하도록 룰을 생성할 수 있습니다. 룰은 조건과 액션으로 구성됩니다. 조건을 사용하여 액션을 트리거할 수 있습니다. 예를 들어, 장치는 녹화를 시작하거나 모션이 감지되면 이메일을 보내거나 장치가 녹화하는 동안 오버레이 텍스트를 표시할 수 있습니다.

자세한 내용은 *이벤트 룰 시작하기*를 참조하십시오.

액션 트리거

1. **System > Events(시스템 > 이벤트)**로 이동하고 룰을 추가합니다. 룰은 장치가 특정 액션을 수행하는 시간을 정의합니다. 규칙을 예약, 반복 또는 수동 트리거로 설정할 수 있습니다.
2. **Name(이름)**을 입력합니다.
3. 작업을 트리거하려면 충족해야 하는 **Condition(조건)**을 선택합니다. 룰에 하나 이상의 조건을 지정하려면 모든 조건이 액션을 트리거하도록 충족해야 합니다.
4. 조건이 충족되면 수행할 **Action(액션)**을 선택합니다.

비고

- 룰에서 사용하는 스트림 프로파일의 정의를 변경하면, 해당 스트림 프로파일을 사용하는 모든 룰을 다시 시작해야 합니다.

카메라가 번호판을 감지하면 비디오 녹화

이 예에서는 카메라가 객체를 감지했을 때 SD 카드에 녹화를 시작하도록 카메라를 설정하는 방법을 설명합니다. 해당 녹화에는 감지 전 5초와 감지 종료 후의 1분이 포함됩니다.

시작하기 전:

- SD 카드가 설치되어 있는지 확인하십시오.

AXIS Licence Plate Verifier가 실행 중인지 확인하십시오.

1. **Apps > AXIS License Plate Verifier(앱 > AXIS License Plate Verifier)**로 이동합니다.
2. 아직 실행되고 있지 않으면 애플리케이션을 시작합니다.
3. 필요에 따라 애플리케이션을 설정했는지 확인하십시오.

룰 생성:

1. **System > Events(시스템 > 이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록의 **Application(애플리케이션)**에서 **ALPV.PlateInView**를 선택합니다.
4. 액션 목록의 **Recordings(녹음)**에서 **Record video while the rule is active(룰이 활성 상태인 동안 비디오 녹화)**를 선택합니다.
5. 스토리지 옵션 목록에서 **SD_DISK**를 선택합니다.
6. 카메라와 스트림 프로파일을 선택합니다.
7. 사전 버퍼 시간을 5초로 설정합니다.
8. 사후 버퍼 시간을 1분으로 설정합니다.
9. **Save(저장)**를 클릭합니다.

카메라 렌즈가 탬퍼링될 때 알림 트리거

이 예에서는 카메라 렌즈가 스프레이 페인트가 묻거나, 가려지거나, 흐려질 때 이메일 알림을 설정하는 방법을 설명합니다.

탬퍼링 감지 활성화:

1. **System > Detectors > Camera tampering(시스템 > 감지기 > 카메라 탬퍼링)**으로 이동합니다.

2. **Trigger delay(트리거 지연)**의 값을 설정합니다. 값은 이메일을 보내기 전에 통과해야 하는 시간을 나타냅니다.
3. 렌즈에 스프레이가 뿌려져 있는지, 덮혀 있는지 또는 초점이 심하게 흐려졌는지 감지하기 위해 **Trigger on dark images(어두운 이미지에서 트리거)**를 켭니다.

이메일 수신자 추가:

4. **System > Events > Recipients(시스템 > 이벤트 > 수신자)**로 이동하고 수신자를 추가합니다.
5. 수신자의 이름을 입력합니다.
6. 알림 유형으로 **Email(이메일)**을 선택합니다.
7. 수신자의 이메일 주소를 입력합니다.
8. 카메라에서 알림을 보낼 때 사용할 이메일 주소를 입력합니다.
9. 보내는 이메일 계정의 로그인 정보와 함께 SMTP 호스트 이름 및 포트 번호를 입력합니다.
10. 이메일 설정을 테스트하려면 **Test(테스트)**를 클릭합니다.
11. **Save(저장)**를 클릭합니다.

룰 생성:

12. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 룰을 추가합니다.
13. 룰에 대한 이름을 입력합니다.
14. 조건 목록에서 **Video(비디오)** 아래에서 **Tampering(탐퍼링)**을 선택합니다.
15. 액션 목록의 **Notifications(알림)** 아래에서 **Send notification to email(이메일로 알림 전송)**을 선택한 다음, 목록에서 수신자를 선택합니다.
16. 이메일의 제목과 메시지를 입력합니다.
17. **Save(저장)**를 클릭합니다.

오디오

네트워크 스피커에 연결

네트워크 스피커 페어링을 사용하면 카메라에 직접 연결된 것처럼 호환 가능한 Axis 네트워크 스피커를 사용할 수 있습니다. 페어링된 스피커는 오디오 클립을 재생하고 카메라를 통해 사운드를 전송할 수 있는 오디오 출력 장치 역할을 수행합니다.

중요 사항

이 기능을 영상 관리 소프트웨어(VMS)와 함께 사용하려면 먼저 카메라를 네트워크 스피커와 페어링한 다음 카메라를 VMS에 추가해야 합니다.

카메라와 네트워크 스피커 페어링

1. **시스템 > 에지 투 에지 > 페어링**으로 이동합니다.
2.  **Add(추가)**를 클릭하고 드롭다운 목록에서 페어링 유형으로 **Audio(오디오)**를 선택합니다.
3. **Speaker pairing(스피커 페어링)**을 선택합니다.
4. 네트워크 스피커의 IP 주소, 사용자 이름 및 패스워드를 입력합니다.
5. **Connect(연결)**를 클릭합니다. 확인 메시지가 나타납니다.

네트워크 마이크에 연결

네트워크 마이크 페어링을 사용하면 카메라에 직접 연결된 것처럼 호환 가능 Axis 네트워크 마이크를 사용할 수 있습니다. 페어링이 이루어지면 네트워크 마이크는 주변 구역의 사운드를 수신하여 오디오 입력 장치로 사용할 수 있도록 하여 미디어 스트림 및 녹음에 사용할 수 있습니다.

중요 사항

이 기능을 영상 관리 소프트웨어(VMS)와 함께 사용하려면 먼저 카메라를 네트워크 마이크와 페어링한 다음 카메라를 VMS에 추가해야 합니다.

카메라와 네트워크 스피커 마이크

1. **시스템 > 에지 투 에지 > 페어링**으로 이동합니다.
2.  **Add(추가)**를 클릭하고 드롭다운 목록에서 페어링 유형으로 **Audio(오디오)**를 선택합니다.
3. **마이크 페어링**을 선택합니다.
4. 네트워크 마이크의 IP 주소, 사용자 이름 및 패스워드를 입력합니다.
5. **Connect(연결)**를 클릭합니다. 확인 메시지가 나타납니다.

목록 관리

목록에 감지된 번호판 추가

번호판은 애플리케이션에서 감지된 후 목록에 직접 추가할 수 있습니다.

1. **Home(홈)**을 클릭합니다.
2. **Live(라이브)**로 이동합니다.
3. 목록에 등록된 번호판의 화살표 아이콘을 클릭합니다.
4. **Append plate to list(목록에 번호판 추가)**를 클릭합니다.
5. 대화 상자에서 번호판을 추가할 목록을 선택합니다.
6. **Append(추가)**를 클릭합니다.

비고

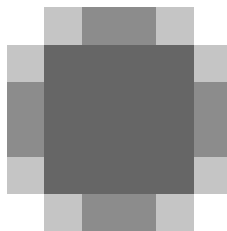
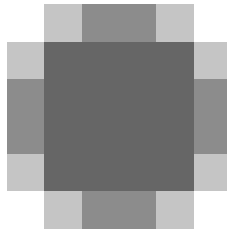
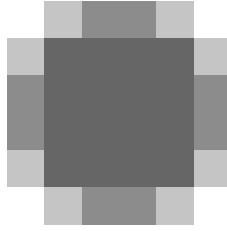
번호판 번호나 설명에 <, > 및 & 기호가 사용되지 않았는지 확인합니다.

번호판에 설명 추가

목록의 번호판에 설명을 추가하려면:

- **List management(목록 관리)**로 이동합니다.

- 번호판을 선택하고



을 클릭한 다음 드롭다운 메뉴에서 **Edit(편집)**을 선택합니다.

- **Description(설명)** 필드에 관련 정보를 입력합니다.
- **Save(저장)**를 클릭합니다.

비고

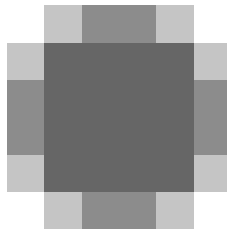
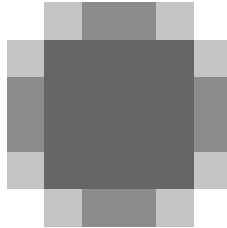
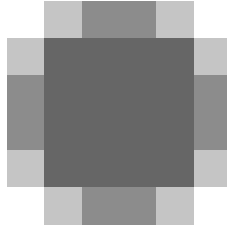
<, > 및 & 기호가 번호판이나 설명에 사용되지 않았는지 확인합니다.

목록 이름 사용자 지정

특정 사용 사례에 맞게 목록의 이름을 변경할 수 있습니다.

1. **List management(목록 관리)**로 이동합니다.

2. 변경하려는 목록 옆의



을 클릭합니다.

3. **Edit(편집)**를 선택합니다.
4. 목록 이름을 입력하십시오.
5. **Submit(제출)**을 클릭합니다.

새 목록 이름은 기존 구성에서 업데이트됩니다.

허용 목록 번호판 번호 가져오기

컴퓨터에 있는 .csv 파일에서 허용 목록 번호판 번호를 가져올 수 있습니다. 번호판 번호 외에도 .csv 파일에 각 번호판 번호에 대한 설명을 추가할 수도 있습니다.

.csv 파일의 구조는 다음과 같아야 합니다. `license plate,date,description`

예:

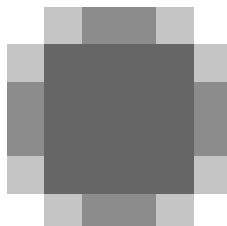
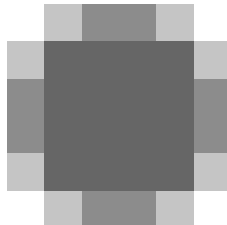
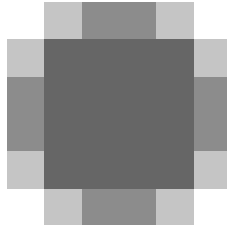
번호판만: `AXIS123`

번호판+설명: `AXIS123,, John Smith`

번호판+날짜+설명: `AXIS123,2022-06-08, John Smith`

비고

- <, > 및 & 기호가 번호판이나 설명에 사용되지 않았는지 확인합니다.
1. **List management(목록 관리)**로 이동합니다.
 2. **Allowlist(허용 목록)** 옆의



을 클릭하고 드롭다운 메뉴에서 **Import(가져오기)**를 선택합니다.

3. 컴퓨터에서 .csv 파일을 찾아 선택합니다.
4. **OK(확인)**를 클릭합니다.
5. 가져온 번호판 번호가 **Allowlist(허용 목록)**에 나타나는지 확인합니다.

번호판 목록을 다른 카메라와 공유

번호판 목록을 네트워크의 다른 카메라와 공유할 수 있습니다. 동기화는 다른 카메라의 모든 현재 번호판 목록보다 우선합니다.

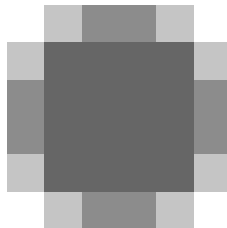
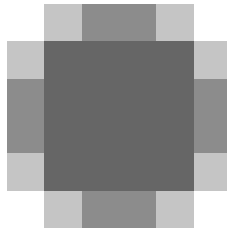
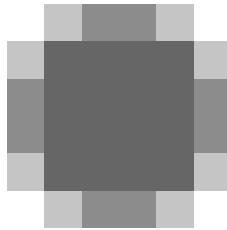
1. **List management(목록 관리) > List synchronization(목록 동기화)**으로 이동합니다.
2. **Remote connected devices(원격 연결 장치)**에 IP 주소, 사용자 이름 및 패스워드를 입력합니다.
3. **추가**를 클릭합니다.

4. **Synchronize list(목록 동기화)**를 클릭합니다.
5. 그에 따라 **Last sync(마지막 동기화)** 업데이트 아래에서 날짜 및 시간을 확인합니다.

일정 목록

목록은 특정 요일의 특정 시간에만 활성화되도록 예약할 수 있습니다. 목록을 예약하려면:

- **List management(목록 관리)**로 이동합니다.
- 변경하려는 목록 옆의



을 클릭합니다.

- 드롭다운 메뉴에서 **Schedule(일정)**을 선택합니다.
- 시작 및 종료 시간과 목록이 활성화되어야 하는 날짜를 선택합니다.
- **Enabled(활성화)** 옆에 있는 버튼을 클릭합니다.
- **Save(저장)**를 클릭합니다.

추가 설정

텍스트 오버레이 구성

실시간 보기에서 텍스트 오버레이가 보여주는 이벤트 정보는 weekday, month, time, year, license plate number입니다.

1. **Settings(설정) > Image(이미지)**로 이동합니다.
2. **Text overlay(텍스트 오버레이)**를 활성화합니다.
3. **Timestamp and license plate(타임스탬프 및 번호판)** 또는 **License plate only(번호판만)** 중에서 선택합니다.
4. **Overlay duration(오버레이 기간)**을 1초에서 9초 사이의 값으로 설정합니다.
5. 실시간 보기에 오버레이가 나타나는지 확인하십시오.

저조도 조건에서 번호판 감지

각 감지는 알고리즘에 의해 점수가 매겨지며 이를 신뢰도 임계값이라고 합니다. 선택한 수준보다 점수가 낮은 감지는 이벤트 목록에 표시되지 않습니다.

조명이 어두운 장면의 경우 신뢰도 임계값을 낮게 설정하면 더 많은 번호판을 감지할 수 있습니다.

1. **Settings(설정) > Recognition(인식)**으로 이동합니다.
2. **Confidence threshold(신뢰도 임계값)**의 슬라이더를 조정합니다.
3. 알고리즘이 예상대로 번호판을 감지하는지 확인합니다.

번호판에 더 적은 문자 수 허용

애플리케이션에는 번호판 감지를 위한 기본 최소 문자 수가 있습니다. 기본 최소 문자 수는 5입니다. 문자 수가 더 적은 번호판을 감지하도록 애플리케이션을 구성할 수 있습니다.

1. **Settings(설정) > Recognition(인식)**으로 이동합니다.
2. **Number of characters(문자 수)** 아래의 슬라이더를 조정하여 허용할 최소 문자 수를 설정합니다.
3. 애플리케이션이 번호판을 예상대로 감지하는지 확인합니다.

정확히 일치하는 번호판만 허용

감지된 번호판을 허용 목록이나 차단 목록과 대조할 때 매칭 알고리즘이 자동으로 한 문자 차이를 허용합니다. 하지만 번호판의 모든 문자가 정확히 일치해야 하는 상황도 있습니다.

1. **List management(목록 관리)**로 이동합니다.
2. **Strict matching(엄격한 일치)**을 활성화하려면 클릭하십시오.
3. 애플리케이션이 번호판과 예상대로 일치하는지 확인합니다.

번호판을 대조할 때 두 문자 이상 차이 허용

감지된 번호판을 허용 목록이나 차단 목록과 대조할 때 매칭 알고리즘이 자동으로 한 문자 차이를 허용합니다. 그러나 두 문자 이상 차이를 허용할 수 있습니다.

1. **Settings(설정) > Recognition(인식)**으로 이동합니다.
2. **Allowed character deviation(허용되는 문자 차이)**에서 다르게 허용되도록 문자 수를 선택합니다.
3. 애플리케이션이 번호판과 예상대로 일치하는지 확인합니다.

운영자에게 제한된 액세스 권한 부여

운영자에게 URL을 통해 앱에 대한 제한된 액세스 권한을 부여할 수 있습니다. 이를 통해 운영자는 **Event log(이벤트 로그)**와 **List management(목록 관리)**에만 액세스할 수 있습니다. URL은 **Settings > User rights(설정 > 사용자 권한)**에서 찾을 수 있습니다.

보안 연결 설정

카메라와 도어 컨트롤러 간과 같이 장치 간 통신 및 데이터를 보호하려면 인증서를 사용하여 HTTPS로 보안 연결을 설정합니다.

1. **Settings(설정) > Security(보안)**로 이동합니다.
2. HTTPS에서 **Self-signed(자체 서명)** 또는 **CA-signed(CA 서명)** 중 하나를 선택합니다.

비고

HTTPS 및 그 사용 방법에 대한 자세한 내용은 에서 확인할 수 있습니다.

백업 및 앱 설정 복구

앱에서 설정한 이미지 캡처, 보안, 탐지 및 통합과 관련된 설정을 백업 및 복구할 수 있습니다. 문제가 발생하면 이제 백업한 설정을 복구할 수 있습니다.

앱 설정을 백업하려면:

- **Settings > Maintenance(설정 > 유지보수)**로 이동합니다.
- **Download backup configuration(백업 구성 다운로드)**를 클릭합니다.

JSON 파일이 다운로드 폴더에 다운로드됩니다.

앱 설정으로 복구하려면:

- **Settings > Maintenance(설정 > 유지보수)**로 이동합니다.
- **Restore configuration(구성 복구)**를 클릭합니다.

백업이 포함된 JSON 파일을 선택합니다.

설정이 자동으로 복구됩니다.

모든 이벤트 지우기

앱을 설정한 후 설정 프로세스에서 이미지 또는 캡처된 플레이트의 기록을 지우는 것이 좋습니다.

데이터베이스에서 모든 이미지와 플레이트를 지우려면:

Settings > Maintenance(설정 > 유지보수)로 이동합니다.

- **Clear all recognition results(모든 인식 결과 지우기)**를 클릭합니다.
- **예**를 클릭합니다.

가상 포트를 사용하여 작업 트리거

가상 포트를 접근 제어와 함께 사용하여 모든 종류의 작업을 트리거할 수 있습니다. 이 예에서는 가상 포트를 사용하여 텍스트 오버레이를 표시하기 위해 카메라의 I/O 포트와 함께 AXIS License Plate Verifier를 설정하는 방법을 설명합니다.

요구 사항:

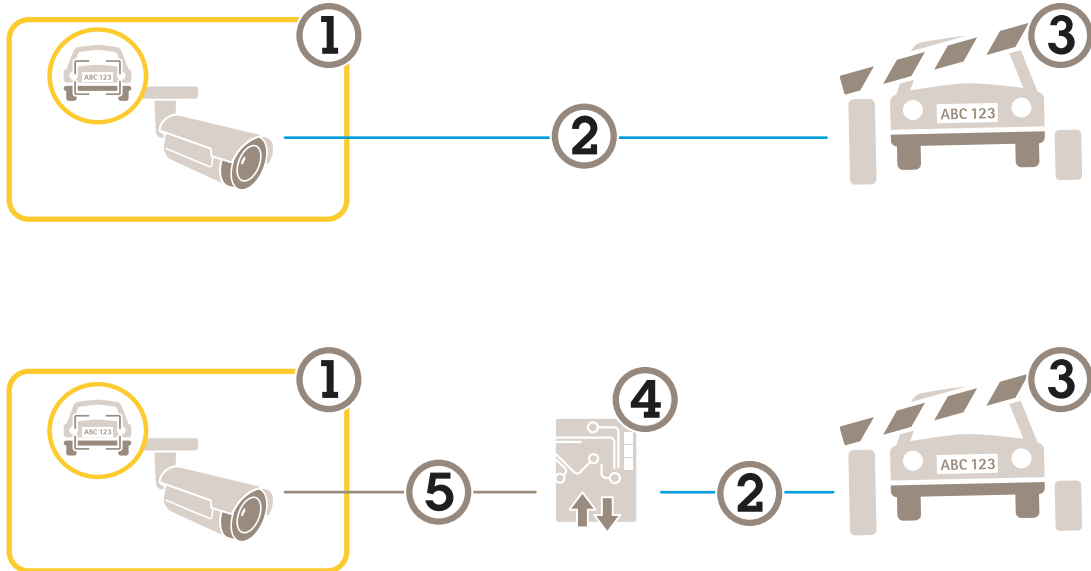
- 물리적으로 설치되고 네트워크에 연결된 카메라.
 - AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
 - 장벽과 카메라의 I/O 포트 사이에 케이블이 연결되어야 합니다.
 - 기본 설정이 완료되어야 합니다. 을 참조하십시오.
1. 애플리케이션의 웹 페이지로 이동하여 **Settings(설정)** 탭을 선택합니다.
 2. **Access control(접근 제어)**로 이동합니다.

3. **Access control**(접근 제어)에서 **Internal I/O**(내부 I/O)를 선택합니다.
4. **I/O output #**(I/O 출력 번호)을 선택합니다.
5. 드롭 다운 목록에서 **Virtual port**(가상 포트)를 선택합니다.
6. **Barrier mode**(차단기 모드)에서 **Open to all**(모두에게 열기)를 선택합니다.
7. **Vehicle direction**(차량 방향)에서 **Any**(모든 방향)를 선택합니다.
8. 사용하려는 **Area of interest**(관심 영역)를 선택합니다.
9. 카메라의 웹 페이지에서 **System > Events**(시스템 > 이벤트)로 이동합니다.
10. **Add rule**(룰 추가)를 클릭합니다.
11. **Condition**(조건)에서 **Virtual input is active**(가상 입력이 활성화됨)와 선택한 포트 번호를 선택합니다.
12. **Action**(액션)에서, **Use overlay text**(오버레이 텍스트 사용)을 선택합니다.
13. **Video channel**(비디오 채널)을 선택합니다.
14. 표시할 텍스트를 입력합니다.
15. 텍스트의 지속 시간을 추가합니다.
16. **Save**(저장)를 클릭합니다.
17. **Video > Overlays**(비디오 > 오버레이)로 이동합니다.
18. **Overlays**(오버레이)로 이동합니다.
19. 드롭다운 메뉴에서 **Text**(텍스트)를 선택하고 **+**를 클릭합니다.
20. #D를 입력하거나 **Modifiers**(수정자) 드롭 다운 목록에서 수정자를 선택합니다.
21. 실시간 보기에서 차량이 관심 영역에 진입할 때 텍스트 오버레이가 표시되는지 확인합니다.

차량 출입 시나리오

차량 출입 시나리오에서 애플리케이션은 카메라로 캡처한 차량의 번호판을 읽고 카메라에 저장된 승인된 번호판 번호 또는 승인되지 않은 번호판 번호 목록과 비교하여 번호판을 확인합니다.

이 시나리오에서는 장벽을 열고 닫기 위해 I/O 지원 또는 연결된 I/O 릴레이 모듈이 있는 애플리케이션이 카메라에 포함되어야 합니다.



차량 출입 시나리오를 위한 두 가지 가능한 설정.

- 1 AXIS License Plate Verifier가 있는 Axis 카메라
- 2 I/O 통신
- 3 장벽
- 4 Axis I/O 릴레이 모듈
- 5 IP 통신

릴레이 모듈을 사용하여 알려진 차량에 대해 장벽 개방

이 예시 사용 사례는 AXIS License Plate Verifier를 릴레이 모듈과 함께 설정하여 특정 ROI(관심 영역)를 통과해 주행하는 알려진 차량에 대한 장벽을 개방하는 방법을 설명합니다. 주차 영역을 예로 들 수 있습니다.

요구 사항:

- 물리적으로 설치되고 네트워크에 연결된 카메라.
 - AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
 - 장벽과 릴레이 모듈 사이에 케이블이 연결되어야 합니다.
 - 기본 설정이 완료되어야 합니다. 기본 설정, on page 4을 참조하십시오.
1. 카메라의 웹 페이지로 이동하여 **Settings(설정)**를 선택하고 AXIS License Plate Verifier를 엽니다.
 2. 릴레이 모듈의 웹 페이지로 이동하여 릴레이 포트가 카메라의 I/O 포트에 연결되어 있는지 확인합니다.
 3. 릴레이 모듈의 IP 주소를 복사합니다.
 4. AXIS License Plate Verifier로 돌아갑니다.
 5. **Settings(설정) > Access control(접근 제어)**로 이동합니다.
 6. **Type(유형)**으로 이동하고 드롭다운 목록에서 **Relay(릴레이)**를 선택합니다.
 7. **I/O output(I/O 출력)** 드롭다운 목록에서 장벽에 연결된 I/O 포트를 선택합니다.

8. **Barrier mode(장벽 모드)** 드롭다운 목록의 **Open from lists(목록에서 열기)**를 선택하고 **Allowlist(허용 목록)**를 확인합니다.
9. **Vehicle direction(차량 방향)** 드롭다운 목록에서 **in(입차)**를 선택합니다.
10. **ROI** 드롭다운 목록에서 차선을 포함하는 관심 영역을 선택합니다.
11. 다음 정보를 입력합니다.
 - 192.168.0.0 형식의 릴레이 모듈 IP 주소
 - 릴레이 모듈의 사용자 이름
 - 릴레이 모듈의 패스워드
12. 연결이 제대로 작동하는지 확인하려면 **Connect(연결)**를 클릭합니다.
13. 연결을 활성화하려면 **Turn on integration(통합 켜기)**를 클릭합니다.
14. **List management(목록 관리)** 탭으로 이동합니다.
15. 번호판 번호를 **Allowlist(허용 목록)** 필드에 입력합니다.

비고

릴레이 모듈의 물리적 입력 포트 1 ~ 8은 드롭다운 목록의 포트 1 ~ 8에 해당합니다. 그러나 릴레이 모듈의 릴레이 포트 1 ~ 8은 드롭다운 목록의 포트 9 ~ 16에 해당합니다. 릴레이 모듈에 포트가 8개 밖에 없는 경우에도 유효합니다.

16. 애플리케이션이 허용 목록의 번호판 번호를 알려진 차량으로 식별하고 장벽이 예상대로 열리는지 확인합니다.

카메라의 I/O를 사용하여 알려진 차량에 대해 장벽 개방

이 예에서는 주차장으로 들어오는 알려진 차량에 대해 장벽을 열기 위해 AXIS License Plate Verifier를 카메라의 I/O 포트와 함께 설정하는 방법을 설명합니다.

요구 사항:

- 물리적으로 설치되고 네트워크에 연결된 카메라.
 - AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
 - 장벽과 카메라의 I/O 포트 사이에 케이블이 연결되어야 합니다.
 - 기본 설정이 완료되어야 합니다. 을 참조하십시오.
1. 애플리케이션 웹 페이지에서 **Home(홈)**으로 이동하여 감지된 번호판을 목록에 추가합니다. 목록에 감지된 번호판 추가, on page 19를 참조하십시오.
 2. 목록을 직접 편집하려면 **List management(목록 관리)**로 이동합니다.
 3. 허가된 번호판 번호를 **Allowlist(허용 목록)** 필드에 입력합니다.
 4. **Settings(설정)**로 이동합니다.
 5. **Access control(접근 제어)**에서 **Internal I/O(내부 I/O)**를 선택합니다.
 6. **I/O output #(I/O 출력 번호)**를 선택합니다.
 7. **Barrier mode(차단기 모드)**에서 **Open from lists(목록에서 열기)**를 선택한 다음 **Allowlist(허용 목록)**를 선택합니다.
 8. **Vehicle direction(차량 방향)** 드롭다운 목록에서 **in(입차)**를 선택합니다.
 9. **Area of interest(관심 영역)**에서 사용하려는 관심 영역을 선택하거나 전체를 선택합니다.
 10. 애플리케이션이 허용 목록의 번호판 번호를 알려진 차량으로 식별하고 장벽이 예상대로 열리는지 확인합니다.

비고

특정 사용 사례에 맞게 목록의 이름을 변경할 수 있습니다.

허가되지 않은 차량에 대해 알림 받기

이 예에서는 알림을 트리거하는 이벤트를 카메라에서 생성할 수 있도록 애플리케이션을 설정하는 방법을 설명합니다.

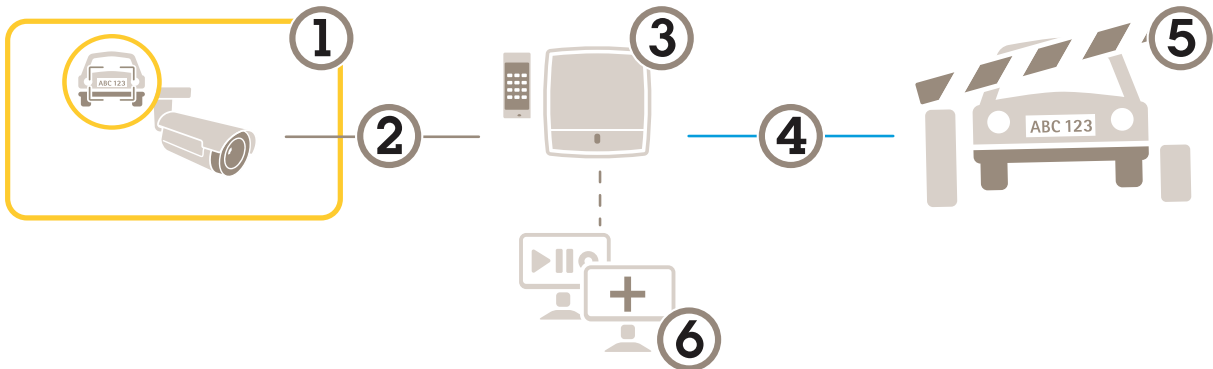
요구 사항:

- 기본 설정이 완료되어야 합니다. *기본 설정, on page 4*를 참조하십시오.
1. **List management(목록 관리)**로 이동합니다.
 2. 번호판 번호를 **Blocklist(차단 목록)** 필드에 입력합니다.
 3. 카메라의 웹 페이지로 이동합니다.
 4. **Settings(설정) > Events(이벤트)**로 이동하고 애플리케이션을 조건으로, 알림을 액션으로 하여 액션 룰을 설정합니다.
 5. 애플리케이션이 추가된 번호판 번호를 허가되지 않은 차량으로 식별하고 액션 룰이 예상대로 실행되는지 확인합니다.

차량 접근 제어 시나리오

차량 접근 제어 시나리오에서 Axis 네트워크 도어 컨트롤러에 애플리케이션을 연결하여 접근 룰을 구성하고, 액세스 시간을 생성하고, 직원뿐만 아니라 방문자 및 공급업체와 같은 차량 액세스를 손쉽게 처리할 수 있습니다.

백업을 위해 도어 컨트롤러 및 카드 리더와 관련된 접근 시스템을 사용하십시오. 도어 컨트롤러와 카드 리더를 설정하려면 axis.com의 사용자 설명서를 참조하십시오.



- 1 AXIS License Plate Verifier가 있는 Axis 카메라
- 2 IP 통신
- 3 카드 리더가 장착된 Axis 네트워크 도어 컨트롤러
- 4 I/O 통신
- 5 장벽
- 6 타사 소프트웨어(선택 사항)

도어 컨트롤러에 연결

이 예에서는 카메라가 센서로 작동하도록 네트워크 도어 컨트롤러에 카메라를 연결합니다. 카메라는 정보를 컨트롤러로 전달하여 정보를 분석하고 이벤트를 트리거합니다.

비고

AXIS License Plate Verifier와 AXIS Entry Manager 간에 전환할 때 모든 매개변수에 액세스하려면 웹 페이지를 새로 고침 해야 합니다.

요구 사항:

- 카메라 및 도어 컨트롤러는 물리적으로 설치되고 네트워크에 연결됩니다.
- AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
- 기본 설정이 완료되어야 합니다. 기본 설정, on page 4을 참조하십시오.



AXIS A1001 도어 컨트롤러로 애플리케이션을 시작하고 실행하는 방법.

AXIS Entry Manager의 하드웨어 구성

1. AXIS Entry Manager로 이동하여 **설정**에서 새 하드웨어 구성을 시작합니다.
2. 하드웨어 구성에서 네트워크 도어 컨트롤러의 이름을 "Gate controller"로 바꿉니다.
3. **Next (다음)**를 클릭합니다.
4. **Configure locks connected to this controller**(이 컨트롤러에 연결된 잠금 구성)에서 **Door monitor**(도어 모니터) 옵션 선택을 취소합니다.
5. **Next (다음)**를 클릭합니다.

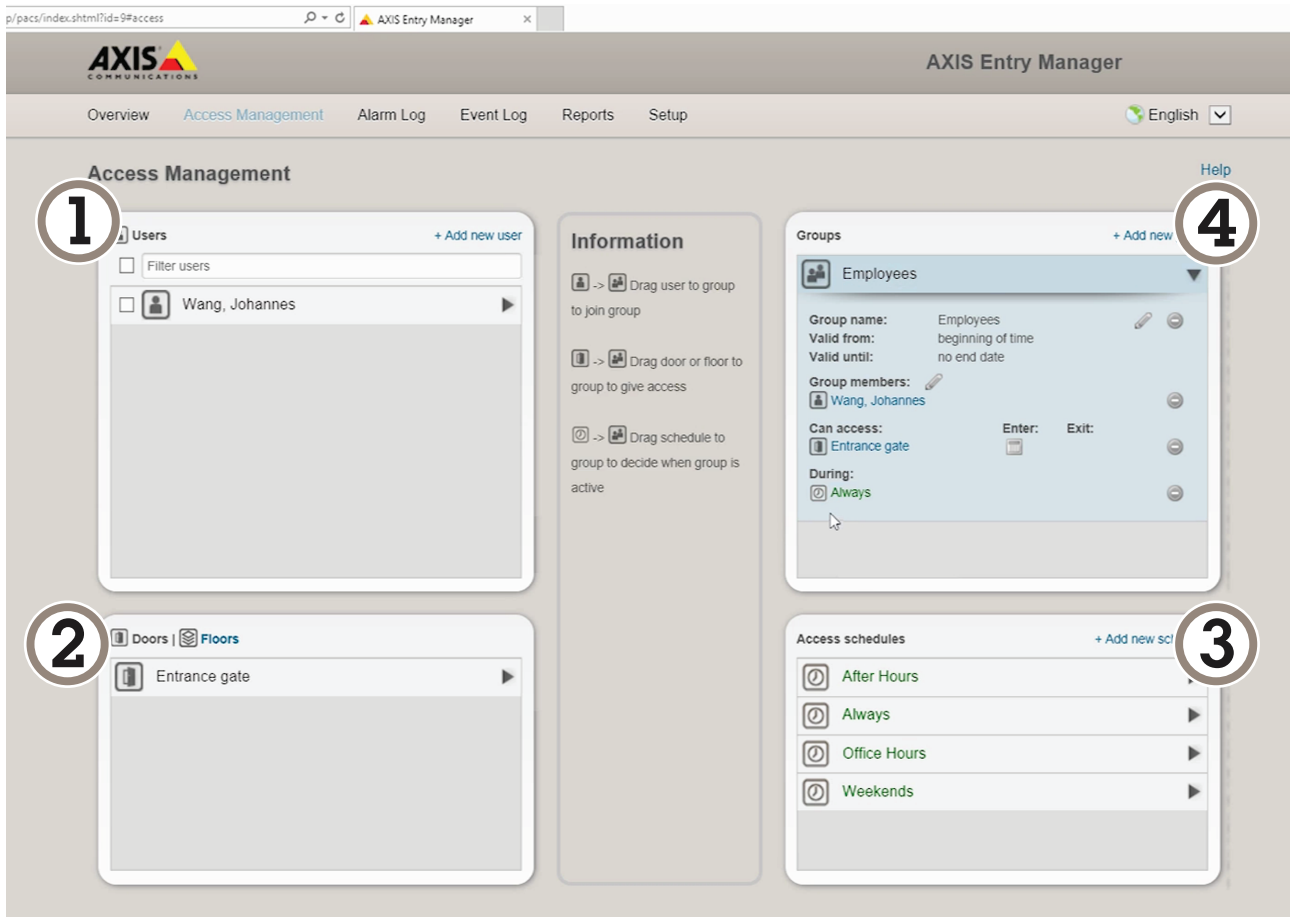
6. **Configure readers connected to this controller**(이 컨트롤러에 연결된 리더 구성)에서 **Exit reader**(리더 나가기) 옵션 선택을 취소합니다.
7. **Finish** (마침)를 클릭합니다.

AXIS License Plate Verifier의 구성

1. AXIS License Plate Verifier 웹 페이지로 이동합니다.
2. **Settings(설정) > Access control(접근 제어)**로 이동합니다.
3. **Type(유형)**으로 이동하고 드롭다운 목록에서 **Controller(컨트롤러)**를 선택합니다.
4. 다음 정보를 입력합니다.
 - 192.168.0.0 형식의 컨트롤러 IP 주소
 - 컨트롤러의 사용자 이름
 - 컨트롤러의 패스워드
5. **Connect(연결)**를 클릭합니다.
6. 연결이 성공하면 **Network Door Controller name(네트워크 도어 컨트롤러 이름)** 드롭다운 목록에 "Gatecontroller"가 나타납니다. "Gatecontroller"를 선택합니다.
7. **Reader name(리더 이름)** 드롭다운 목록에서 "Gatecontroller(게이트 컨트롤러)" 도어에 연결된 리더를 선택합니다(예: "Reader entrance(리더 입구)"). 이 이름은 AXIS Entry Manager에서 변경할 수 있습니다.
8. 연결을 활성화하려면 **Turn on integration(통합 켜기)**을 선택합니다.
9. 테스트 필드에 사용자의 번호판 번호 중 하나를 입력하거나 기본 설정을 사용하고 **Test integration(통합 테스트)**을 클릭합니다. 테스트가 성공했는지 확인합니다.

AXIS Entry Manager에서 사용자, 그룹, 도어 및 일정 구성

1. AXIS Entry Manager로 이동합니다.
2. **Access Management(접근 관리)**로 이동합니다.
3. **Doors > Add identification type(도어 > 식별 유형 추가)**으로 이동합니다.
4. **Credentials needed(필요한 자격 증명)** 드롭다운 목록에서 **License plate only(번호판만)**를 선택합니다.
5. 식별 유형을 사용할 수 있는 시간에 대한 제한을 설정하려면 **Schedule(일정)**을 도어로 끌어서 놓습니다.
6. 사용자를 추가하고 각 사용자에게 대해 자격 증명 **License plate(번호판)**를 추가합니다.
7. **Add credential(자격 증명 추가)**을 다시 클릭하고 번호판 정보를 입력합니다.
8. **Add new group(새 그룹 추가)**을 클릭하고 정보를 입력합니다.
9. 그룹에 사용자를 추가하려면 **Users(사용자)**를 사용자 그룹에 끌어서 놓습니다.
10. 사용자에게 접근 권한을 부여하려면 **Door(도어)**를 사용자 그룹에 끌어서 놓습니다.
11. 액세스 시간을 제한하려면 **Schedule(일정)**을 사용자 그룹에 드래그 앤 드롭 합니다.



AXIS Entry Manager 사용자 인터페이스 오버뷰.

- 1 사용자
- 2 도어
- 3 일정
- 4 사용자 그룹

AXIS Secure Entry에 연결

이 예에서는 AXIS Camera Station의 Axis 도어 컨트롤러와 AXIS License Plate Verifier를 사용하여 AXIS Secure Entry를 연결하는 방법을 설명합니다.

요구 사항:

- 카메라 및 도어 컨트롤러는 물리적으로 설치되고 네트워크에 연결됩니다.
- AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
- AXIS Camera Station 클라이언트 버전 5.49.449 이상.
- 기본 설정이 완료되어야 합니다. 기본 설정, on page 4을 참조하십시오.

AXIS Camera Station에서 Add a reader(리더 추가)를 참조합니다.

AXIS License Plate Verifier 앱에서:

1. **Settings(설정)** 탭에서 **Configuration wizard(구성 마법사)**로 이동하고 **Start(시작)**를 클릭합니다.
2. **Access Control(접근 제어)**을 선택합니다.
3. **Secure Entry(보안 항목)**를 선택하고 **Next(다음)**를 클릭합니다.

AXIS Camera Station 내에서:

4. **AXIS Camera Station>Configuration>Other Devices(AXIS Camera Station>구성>기타 장치)**의 장치 목록에서 사용할 수 있는 도어 컨트롤러의 IP 주소를 입력합니다.

5. 인증 키를 추가하려면 **AXIS Camera Station>Configuration>Encrypted communication (AXIS Camera Station>구성>암호화된 통신)**으로 이동합니다.
6. **External Peripheral Authentication Key(외부 주변 장치 인증 키)**로 이동하여 **Show authentication key(인증 키 표시)**를 클릭합니다.
7. **Copy key(키 복사)**를 클릭합니다.

AXIS License Plate Verifier 앱에서:

8. 구성 마법사에서 **Authentication key(인증 키)**로 이동하여 키를 붙여넣습니다.
9. **Connect(연결)**를 클릭합니다.
10. 드롭다운 메뉴에서 **Door controller name(도어 컨트롤러 이름)**을 선택합니다.
11. 드롭다운 메뉴에서 **Reader name(리더 이름)**을 선택합니다.
12. **Turn on integration(통합 켜기)**를 확인합니다.
13. **Next(다음)**를 클릭합니다.
14. 관심 영역을 조정합니다. *관심 영역 조정, on page 8*을 참조하십시오.
15. **Next(다음)**을 두 번 클릭한 후 **Finish(마침)**를 클릭합니다.

속도 측정을 통한 자유 흐름 시나리오

속도 측정을 통한 자유 흐름 시나리오에서 카메라는 엣지 투 엣지 기술을 통해 Axis 레이더와 페어링됩니다. 카메라는 두 개의 차선을 커버하며 지나가는 차량의 번호판을 판독하고, 페어링된 레이더는 동일한 두 개의 차선을 커버하여 차량의 속도를 측정합니다. 또한 *AXIS Speed Monitor* 애플리케이션은 카메라 실시간 보기의 오버레이를 통해 각 차선의 최대 속도를 시각화할 수 있습니다.

엣지 투 엣지에 대해 자세히 알아보려면 *엣지 투 엣지 기술*, on page 42 항목을 참고하십시오.

요구 사항:

- AXIS License Plate Verifier 카메라 키트와 *AXIS D2210-VE Radar*가 설치되어 있고 네트워크에 연결되었습니다.

시나리오 설정

먼저 카메라를 구성한 다음, 레이더를 페어링하고 구성한 후 마지막으로 *AXIS Speed Monitor*를 사용하여 오버레이를 추가하는 4단계로 시나리오를 설정합니다.

시작하기 전:

- 카메라와 레이더가 동일한 관심 영역을 향하고 있는지 확인합니다.
- 카메라와 레이더의 시간이 동기화되어 있는지 확인합니다. 상태를 확인하려면 각 장치의 **Installation > Time sync status(설치 > 시간 동기화 상태)**로 이동합니다.
- 카메라의 두 번째 보기 영역(**View area 2(보기 영역 2)**)은 사용하지 않아야 합니다. 레이더가 페어링 후에 사용할 것이기 때문입니다.

카메라 구성:

1. 기본 설정, on page 4의 지침에 따라 카메라를 설정합니다.
2. 설정 도우미를 따를 때 자유 흐름을 선택해야 합니다. 자세한 내용은 *자유 흐름*, on page 6를 참조하십시오.

카메라를 레이더와 페어링:

1. 카메라의 웹 인터페이스에서 **System > Edge-to-edge > Radar pairing(시스템 > 엣지 투 엣지 > 레이더 페어링)**으로 이동합니다.
2. 레이더의 호스트 이름, 사용자 이름, 패스워드를 입력합니다.
3. **Connect(연결)**를 클릭하여 장치를 페어링합니다.
연결이 설정되면 카메라의 웹 인터페이스에서 레이더 설정을 사용할 수 있습니다.

비고

페어링된 레이더의 기본 해상도는 1280x720입니다. 카메라의 웹 인터페이스에서 레이더의 기본 해상도를 유지하고, VMS에 레이더를 추가하는 경우 이를 유지합니다.

레이더 구성:

1. 카메라의 웹 인터페이스에서 **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
2. 한 차선을 커버하는 레이더 시나리오 하나와 다른 차선을 커버하는 또 다른 레이더 시나리오를 추가합니다.
3. 두 시나리오 모두 **Movement in area(영역 내 이동)**를 선택하고, **Vehicles(차량)**에 대해 트리거하고, **Speed limit(속도 제한)**를 설정합니다.
자세한 내용은 *AXIS D2210-VE Radar* 사용자 설명서의 시나리오 추가를 참조하십시오.

비고

*AXIS License Plate Verifier*를 통해 번호판 정보가 포함된 오버레이를 추가하려면 *AXIS Speed Monitor*에서 오버레이를 추가하기 전에 이를 추가해야 합니다.

AXIS Speed Monitor를 사용하여 속도 오버레이 추가:

1. 카메라에 *AXIS Speed Monitor*를 다운로드하여 설치합니다.
2. 각 차선에 대해 오버레이 하나를 추가하면 카메라의 실시간 보기에 최대 속도가 표시됩니다.
설치 및 구성 지침은 *AXIS Speed Monitor* 사용자 설명서를 참조하십시오.

특정 이벤트 검색

검색 기능을 사용하여 다양한 기준으로 이벤트를 검색합니다.

1. 애플리케이션 웹 페이지로 이동하여 **Search(검색)** 페이지를 선택합니다.
2. **From(시작)** 및 **To(끝)** 캘린더 메뉴의 날짜를 선택합니다.
3. **AOI(관심 영역)** 드롭다운 메뉴를 클릭하여 검색에 포함할 관심 영역을 선택합니다.
4. **Direction(방향)**을 선택하여 입구 또는 출구별로 필터링합니다.
5. 번호판을 검색하려면 **Plate(번호판)** 필드에 번호판을 입력합니다.
6. 특정 국가에 속한 번호판을 찾으려면 **Country(국가)** 드롭다운 목록에서 국가를 선택합니다.
7. 차량 보기를 기준으로 이미지를 필터링하려면 **Vehicle view(차량 보기)** 드롭다운 목록에서 **Front(전면)** 또는 **Rear(후면)**를 선택합니다.
8. 차량 제조사, 모델, 차종 또는 색상을 기준으로 검색 결과를 필터링하려면 **Vehicle details(차량 상세 정보)** 드롭다운 메뉴에서 원하는 항목을 선택합니다.
9. 검색 결과를 보려면 **Apply filters(필터 적용)**를 클릭합니다.

검색 결과 내보내기 및 공유

검색 결과를 해당 시점의 통계와 함께 CSV 파일로 내보내려면 **Export(내보내기)**를 클릭하여 결과를 CSV 파일로 저장합니다.

타사 시스템으로 데이터를 내보내는 데 사용할 수 있는 링크로 API를 복사하려면 **Copy search link(검색 링크 복사)**를 클릭합니다.

통합

여러 서버에 이벤트 푸시하기 위해 프로파일을 사용

프로파일을 사용하면 동시에 다른 프로토콜을 사용하여 다른 서버에 이벤트를 푸시할 수 있습니다. 프로파일을 사용하려면:

1. **Integration(통합)** 및 **Push events(푸시 이벤트)** 페이지로 이동합니다.
2. **Profile 1(프로파일 1)**을 선택합니다.
3. 룰을 구성합니다. *타사 소프트웨어에 이벤트 정보 푸시, on page 36*을 참조하십시오.
4. 룰 테스트.
5. 새 규칙을 구성하려면 새 프로파일 탭을 선택합니다.

타사 소프트웨어에 이벤트 정보 푸시

비고

애플리케이션은 이벤트 정보를 JSON 형식으로 보냅니다. 자세한 내용을 보려면 *MyAxis 계정을 사용하여 로그인하고 AXIS VAPIX Library*로 이동한 다음 **AXIS License Plate Verifier**를 선택하십시오.

이 기능을 사용하면 TCP 또는 HTTP POST를 통해 이벤트 데이터를 푸시하여 타사 소프트웨어와 통합할 수 있습니다.

시작하기 전:

- 카메라가 물리적으로 설치되고 네트워크에 연결되어야 합니다.
- **AXIS License Plate Verifier**가 카메라에서 실행되어야 합니다.

1. **Integration(통합) > Push events(이벤트 푸시)**로 이동합니다.
2. 빈 프로파일을 선택합니다
3. **Protocol(프로토콜)** 드롭다운 목록에서 **HTTP POST**를 선택합니다.
4. **Server URL(서버 URL)** 필드에 서버 주소 및 포트를 127.0.0.1:8080 형식으로 입력합니다.
5. 사용자 이름 및 패스워드를 입력합니다.
6. 프록시를 사용하는 경우 프록시를 켜고 호스트 이름, 사용자 이름 및 패스워드를 입력합니다.
7. **Device ID(장치 ID)** 필드에 장치의 이름을 입력하거나 그대로 둡니다.
8. **Push conditions(푸시 조건)**에서 푸시 이벤트를 트리거할 방향을 선택합니다.
9. **LPR Event types(LPR 이벤트 유형)**에서 다음 옵션 중 하나 이상을 선택합니다.
 - **New(신규)**란 번호판의 첫 번째 감지를 의미합니다.
 - **Update(업데이트)**는 이전에 감지된 번호판의 문자를 수정하거나 번호판이 이동하고 이미지에서 추적될 때 방향이 감지되는 것입니다.
 - **Lost(손실)**는 이미지를 종료하기 전에 번호판에서 마지막으로 추적된 이벤트입니다. 번호판의 방향도 포함되어 있습니다.
 - **Conditional(조건부)** 설정은 조건이 충족될 때 하나의 객체에 대해 하나의 이벤트를 푸시합니다.
10. HTTP POST 사용 시 대역폭을 줄이려면 **Do not to send images(이미지 전송 안 함)**를 선택할 수 있습니다.
11. 서버가 중단될 경우 이벤트를 버퍼링하고 서버를 다시 사용할 수 있을 때 전송하려면 **Event buffer(이벤트 버퍼)**를 활성화합니다.
12. **Retention settings(보존 설정)**에서 이미지 외에 번호판 크롭 이미지를 포함하려면 **Send two images(두 개의 이미지 전송)**를 선택합니다.
13. 이벤트를 base64 대신 멀티파트(multipart) 형식으로 전송하려면 **Multipart(멀티파트)**를 선택합니다.

14. 가상 번호판으로 통합을 테스트하려면 **Test(테스트)**를 클릭합니다.
15. 기능을 켜려면 **Activate(활성화)**를 선택합니다.

비고

HTTP POST를 사용하여 이벤트를 푸시할 때 사용자 이름과 패스워드 대신 권한 부여 헤더를 사용하면 **Auth-Header(인증 헤더)**로 이동하여 인증 API 경로를 추가합니다.

번호판 이미지를 서버로 전송

이 기능을 사용하면 FTP를 통해 번호판의 이미지를 서버로 푸시할 수 있습니다.

시작하기 전:

- 카메라가 물리적으로 설치되고 네트워크에 연결되어야 합니다.
 - AXIS License Plate Verifier가 카메라에서 실행되어야 합니다.
1. **Integration(통합) > Push events(이벤트 푸시)**로 이동합니다.
 2. **Protocol(프로토콜)** 드롭다운 목록에서, **FTP**를 선택합니다.
 3. **Server URL(서버 URL)** 필드에 서버 주소를 다음 형식으로 입력합니다. ftp://10.21.65.77/LPR
 4. FTP 서버의 사용자 이름 및 패스워드를 입력하십시오.
 5. 파일 이름에 대한 경로 및 이름 수정자를 선택합니다.
 6. **Device ID(장치 ID)** 필드에 장치의 이름을 입력합니다. 이 이름의 폴더가 이미지용으로 생성됩니다. 이미지는 timestamp_area of interest_direction_carID_license plate text_country.jpg 형식을 사용하여 생성됩니다.
 7. **Push conditions(푸시 조건)**에서 푸시 이벤트를 트리거할 방향을 선택합니다.
 8. **Event types(이벤트 유형)**에서 다음 옵션 중 하나 이상을 선택합니다.
 - **New(신규)**란 번호판의 첫 번째 감지를 의미합니다.
 - **Update(업데이트)**는 이전에 감지된 번호판의 문자를 수정하거나 번호판이 이동하고 이미지에서 추적될 때 방향이 감지되는 것입니다.
 - **Lost(손실)**는 이미지를 종료하기 전에 번호판에서 마지막으로 추적된 이벤트입니다. 번호판의 방향도 포함되어 있습니다.
 - **Conditional(조건부)** 설정은 조건이 충족될 때 하나의 객체에 대해 하나의 이벤트를 푸시합니다.

비고

방향은 **Lost(손실)** 또는 **Update(업데이트)**를 선택한 경우에만 파일 이름에 포함됩니다.

9. 가상 번호판으로 통합을 테스트하려면 **Test(테스트)**를 클릭합니다.
10. 기능을 켜려면 **Activate(활성화)**를 클릭합니다.

비고

이미지는 선택한 캡처 모드 유형에 따라 달라지므로 *이미지 캡처 설정 조정, on page 9* 항목을 참고하십시오.

비고

푸시 이벤트가 실패하면 앱은 실패한 이벤트를 최대 100개까지 서버로 다시 전송합니다. Windows 서버로 푸시 이벤트 시 FTP를 사용하는 경우 날짜와 시간을 제공하는 이미지 이름 지정에 %c를 사용하지 마십시오. 이는 Windows에서 날짜 및 시간에 대해 %c 함수로 설정된 이름 지정 형식을 허용하지 않기 때문입니다. Linux 서버를 사용할 때는 이 문제가 발생하지 않습니다.

2N과 직접 통합

이 예는 2N IP 장치와의 직접 통합을 설명합니다.

2N 장치에서 계정 설정:

1. 2N IP Verso로 이동합니다.

2. **Services(서비스) > HTTP API > Account 1(계정 1)**로 이동합니다.
3. **Enable account(계정 활성화)**를 선택합니다.
4. **Camera access(카메라 액세스)**를 선택합니다.
5. **번호판 인식**을 선택합니다.
6. IP 주소를 복사합니다.

AXIS License Plate Verifier 앱에서:

1. **Integration(통합) > Direct integration(직접 통합)**으로 이동합니다.
2. **2N IP Device**를 선택합니다.
3. 2N 장치에 IP 주소 또는 URL을 추가합니다.
4. 사용자 이름 및 패스워드를 입력합니다.
5. **연결 유형**을 선택합니다.
6. **장벽 용도**를 선택합니다.
7. **Enable integration(통합 활성화)**을 클릭합니다.
8. 차량의 진행 방향을 선택합니다.
9. 기능을 켜려면 **Activate(활성화)**를 선택합니다.

통합이 작동하는지 확인하려면:

1. 2N IP Verso로 이동합니다.
2. **Status(상태) > Events(이벤트)**로 이동합니다.

Genetec Security Center와 통합

이 예는 Genetec Security Center와의 직접 통합 설정에 대해 설명합니다.

Genetec Security Center에서:

1. **Overview(개요)**로 이동합니다.
2. **Database(데이터베이스), Directory(디렉토리)** 및 **License(라이선스)**가 온라인인지 확인합니다. 그렇지 않은 경우 Windows에서 모든 Genetec 및 SQLEXPRESS 서비스를 실행하십시오.
3. **Genetec Config Tool > Plugins(Genetec 구성 도구 > 플러그인)**로 이동합니다.
4. **Add an entity(엔터티 추가)**를 클릭합니다.
5. **Plugin(플러그인)**으로 이동하고 **LPR plugin(LPR 플러그인)**을 선택합니다.
6. **Next (다음)**를 클릭합니다.
7. **Next (다음)**를 클릭합니다.
8. **Next (다음)**를 클릭합니다.
9. 추가한 LPR 플러그인을 선택하고 **Data sources(데이터 소스)**로 이동합니다.

ALPR reads API(ALPR이 API 읽기) 아래에서:

10. **Enabled(사용)**을 확인합니다.
11. **Name(이름)**에서, 다음을 입력합니다. **Plugin REST API.**
12. **API path prefix(API 경로 접두사)**에서 **lpr**를 입력합니다.
13. **REST port(REST 포트)**에서 **443**을 선택합니다.
14. **WebSDK host(WebSDK 호스트)**에서 **localhost**를 입력합니다.
15. **WebSDK port(WebSDK 포트)**에서 **443**을 선택합니다.
16. **Allow self signed certificates(자체 서명된 인증서 허용)**를 확인합니다.

Security Center events data source(보안 센터 이벤트 데이터 소스)에서:

17. **Enabled(사용)**을 확인합니다.
18. **Name(이름)**에서, **Security Center Lpr Events(보안 센터 Lpr 이벤트)**를 입력합니다.
19. **Processing frequency(처리 빈도)**에서, **5sec(5초)**를 드롭다운 메뉴에서 선택합니다.
20. **Data sinks(데이터 싱크)** 탭으로 이동합니다.
21. **+**를 클릭합니다.
22. **Type(유형)**에서, **Database(데이터 베이스)**를 선택합니다.
23. **Select and configure the database(데이터베이스 선택 및 구성):**
 - **Enabled(사용)**을 확인합니다.
 - **Source(소스)**에서, **Plugin REST API(플러그인 REST API)** 및 **Native ALPR Events(네이티브 ALPR 이벤트)**를 확인합니다.
 - **Name(이름), Reads DB(DB 읽기)**를 입력합니다.
 - **Include(포함)**에서 **Reads(읽기), Hits(조회수)** 및 **Images(이미지)**를 확인합니다.
 - **Resources(리소스)** 탭으로 이동합니다.
 - **Delete the database(데이터베이스 삭제)**를 클릭하고 **Create a database(데이터베이스 생성)**를 클릭합니다.

Create an API user(API 사용자 생성):

24. **Config Tool > User Management(구성 도구 > 사용자 관리)**로 이동합니다.
25. **Add an entity(엔터티 추가)**를 클릭합니다.
26. **User(사용자)**를 선택합니다.
27. 사용자 이름 및 패스워드를 입력하십시오. 다른 필드는 변경하지 않은 상태로 둡니다.
28. 추가된 사용자를 선택하고 **Privileges(권한)** 탭으로 이동합니다.
29. **Application privileges(애플리케이션 권한)** 아래의 모든 것을 허용하려면 확인하십시오.
30. **Third-party ALPR reads API(타사 ALPR API 읽기)**를 허용하려면 확인합니다.
31. **적용**을 클릭합니다.

AXIS License Plate Verifier 앱에서:

1. **Integration(통합) > Direct integration(직접 통합)**으로 이동합니다.
2. **Genetec Security Center**를 선택합니다.
3. **URL/IP**에서 다음 템플릿에 따라 주소를 입력합니다. `https://server-address/api/v1/lpr/lpringestion/reads`
4. Genetec 사용자 이름 및 패스워드를 입력하십시오.
5. **연결 유형**을 선택합니다.
6. 기능을 켜려면 **Activate(활성화)**를 선택합니다.
7. 가상 번호판으로 통합을 테스트하려면 **Test(테스트)**를 클릭합니다.
8. HTTPS를 선택한 경우 **Settings(설정)** 탭으로 이동합니다.
9. **Security > HTTPS(보안 > HTTPS)**에서.
10. Genetec Security Center의 설정에 따라 **Self-signed(자체 서명)** 또는 **CA-signed(CA 서명)**를 선택합니다.

Genetec Security Center에서:

1. **Genetec Security desk**로 이동합니다.
2. **Investigation(검색)**에서, **Reads(읽기)**를 클릭합니다.
3. **Reads(읽기)** 탭으로 이동합니다.
4. 필요에 따라 결과를 필터링합니다.

5. **Generate report(보고서 생성)**를 클릭합니다.

비고

타사 ALPR 플러그인 통합에 대한 Genetec의 문서도 읽을 수 있습니다. *여기에서* 할 수 있습니다 (등록 필요).

웹 인터페이스

AXIS OS가 탑재된 장치의 웹 인터페이스에서 사용할 수 있는 모든 기능과 설정에 대해 알아보려면 *AXIS OS 웹 인터페이스 도움말*로 이동합니다.

상세 정보

에지 투 에지 기술

에지 투 에지는 IP 장치가 서로 직접 통신하도록 하는 기술입니다. 이 기술은 예를 들어, Axis 카메라와 Axis 오디오 또는 레이더 제품들 간의 스마트 페어링 기능을 제공합니다.

비고

페어링된 장치들이 동일한 AXIS OS 버전을 실행 중인지 확인하십시오.

자세한 내용은 whitepapers.axis.com/edge-to-edge-technology에서 "엣지 투 엣지 기술" 백서를 참조하십시오.

스피커 페어링

에지 투 에지 스피커 페어링을 사용하면 호환 가능 Axis 네트워크 스피커를 카메라의 일부인 것처럼 사용할 수 있습니다. 페어링되면 스피커 기능이 카메라의 웹 인터페이스에 통합되고 네트워크 스피커는 오디오 클립을 재생하고 카메라를 통해 사운드를 전송할 수 있는 오디오 출력 장치 역할을 합니다.

카메라는 VMS에 오디오 출력이 통합된 카메라로 식별되고 재생되는 모든 오디오를 스피커로 리디렉션합니다.

마이크 페어링

엣지 투 엣지 마이크 페어링을 사용하면 호환 가능 Axis 마이크를 카메라의 일부인 것처럼 사용할 수 있습니다. 페어링이 이루어지면 네트워크 마이크는 주변 구역의 사운드를 수신하여 오디오 입력 장치로 사용할 수 있도록 하여 미디어 스트림 및 녹음에 사용할 수 있습니다.

레이더 페어링

에지 투 에지 레이더 페어링을 사용하면 호환 가능 Axis 레이더에 카메라를 연결하고 속도 감지와 같은 통합 기능을 활용할 수 있습니다.

레이더 페어링은 하나의 카메라를 하나의 레이더와 페어링하고 카메라를 사용하여 두 장치를 모두 구성 및 유지보수하는 단방향 설정입니다. 페어링되면 레이더의 설정에 액세스하고 카메라의 웹 인터페이스에서 직접 레이더 관련 이벤트에 대한 룰을 생성할 수 있습니다. 또한 카메라는 레이더 기능이 통합된 카메라로 VMS에 자체 식별됩니다.

또한 레이더 스트림은 **보기 영역 2**라고 하는 카메라의 두 번째 보기 영역에서 시각화됩니다. 레이더에서 생성된 메타데이터는 **채널 2**라고 하는 카메라의 두 번째 메타데이터 생산자 채널을 통해 사용할 수 있습니다.

보기 영역

보기 영역은 전체 보기의 잘라진 영역입니다. 전체 보기 대신 보기 영역을 스트리밍하고 저장하여 대역폭 및 스토리지 요구를 최소화할 수 있습니다. 보기 영역에서 PTZ를 활성화하면 그 안에서 팬/틸트/줌할 수 있습니다. 보기 영역을 사용하면 전체 보기의 일부(예: 하늘)를 제거할 수 있습니다.

보기 영역을 설정할 때 비디오 스트림 해상도를 보기 영역 크기보다 작거나 같은 크기로 설정하는 것이 좋습니다. 비디오 스트림 해상도를 보기 영역 크기보다 크게 설정하면 센서 캡처 후 영상이 디지털 방식으로 확대된다는 의미이므로 이미지 정보는 추가되지 않으면서 더 많은 대역폭이 필요합니다.

비고

카메라를 엣지 투 엣지를 통해 레이더와 페어링하면 레이더 스트림이 카메라의 두 번째 보기 영역에 시각화됩니다.

분석 및 앱

분석 및 앱을 통해 Axis 장치를 더욱 폭넓게 활용할 수 있습니다. AXIS Camera Application Platform (ACAP)은 타사 개발자가 Axis 장치용 분석 및 기타 앱을 개발할 수 있도록 지원하는 개방형 플랫폼입니다.

니다. 앱은 장치에 사전 설치되어 제공되거나, 무료 또는 유료(라이선스 구매)로 다운로드할 수 있습니다.

Axis 분석 및 앱에 대한 사용자 설명서는 help.axis.com에서 확인할 수 있습니다.

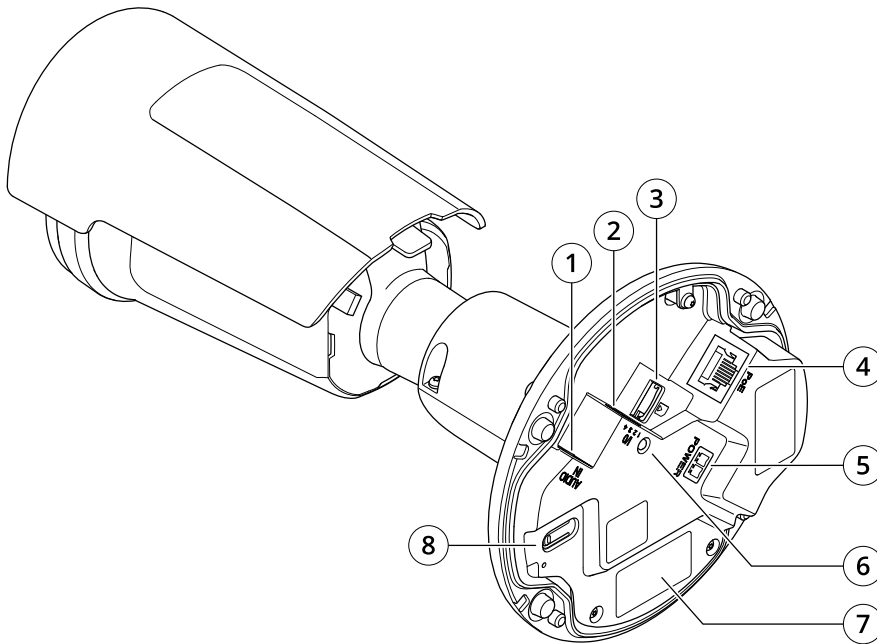
AXIS Image Health Analytics

AXIS Image Health Analytics는 이미지 품질 저하 또는 변조 시도를 감지하는 데 사용할 수 있는 AI 기반 애플리케이션입니다. 이 애플리케이션은 장면의 동작을 분석하고 학습하여 이미지의 흐릿함이나 노출 부족을 감지하거나 시야가 가려지거나 방향이 바뀐 것을 감지합니다. 이러한 감지에 대해 이벤트를 전송하고 카메라의 이벤트 시스템 또는 타사 소프트웨어를 통해 액션을 트리거하도록 애플리케이션을 설정할 수 있습니다.

애플리케이션의 작동 방식에 대한 자세한 내용은 *AXIS Image Health Analytics 사용자 설명서*를 참조하십시오.

사양

제품 개요



- 1 오디오 커넥터
- 2 I/O 커넥터
- 3 microSD 카드 슬롯
- 4 네트워크 커넥터
- 5 DC 전원 입력
- 6 상태 LED 표시기
- 7 부품 번호(P/N) 및 일련 번호(S/N)
- 8 제어 버튼

LED 표시

상태 LED	표시
켜져 있지 않음	연결 및 정상 작동
녹색	시작 완료 후 정상 작동 시 10초 동안 녹색이 계속 표시됩니다.
주황색	시작 시 켜져 있습니다. 장치 소프트웨어 업그레이드 중 또는 공장 출하 시 기본값으로 재설정 시 깜박입니다.
주황색/빨간색	네트워크 연결을 사용할 수 없거나 연결이 끊어진 경우 주황색/빨간색으로 깜박입니다.
빨간색	장치 소프트웨어 업그레이드 실패 상태입니다.

SD 카드 슬롯

통지

- SD 카드 손상 위험이 있습니다. SD 카드를 삽입하거나 분리할 때 날카로운 도구, 금속 객체 또는 과도한 힘을 가하지 마십시오. 손가락을 사용하여 카드를 삽입하고 분리하십시오.
- 데이터 손실 및 손상된 녹화 위험. 장치를 분리하기 전에 장치의 웹 인터페이스에서 SD 카드 마운트를 해제하십시오. 제품이 실행 중일 때는 SD 카드를 분리하지 마십시오.

이 장치는 microSD/microSDHC/microSDXC 카드를 지원합니다.

SD 카드 권장 사항은 axis.com을 참조하십시오.

 microSD, microSDHC 및 microSDXC 로고는 SD-3C LLC의 상표입니다. microSD, microSDHC, microSDXC는 미국이나 기타 국가에서 SD-3C, LLC의 상표이거나 등록 상표입니다.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. 공장 출하 시 기본 설정으로 재설정, on page 47을 참조하십시오.
- 인터넷을 통해 원 클릭 클라우드 연결(O3C) 서비스에 연결합니다. 연결하려면 버튼을 누른 후 놓고, 상태 LED가 녹색으로 세 번 깜박일 때까지 기다립니다.

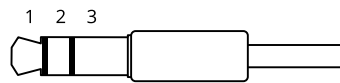
커넥터

네트워크 커넥터

PoE(Power over Ethernet)를 지원하는 RJ45 이더넷 커넥터

오디오 커넥터

- **오디오 입력** - 모노 마이크 또는 라인 입력 모노 신호를 위한 3.5mm 입력 단자입니다(왼쪽 채널은 스테레오 신호에 사용됨).
- **오디오 입력** - 모노 마이크 2개 또는 라인 입력 모노 신호 2개를 위한 3.5mm 입력 단자입니다(제공된 스테레오-모노 어댑터 사용).



오디오 입력

1 팁	2 링	3 슬리브
비평형 마이크(일렉트릭 전원 유무에 관계 없음) 또는 라인 입력	선택된 경우 일렉트릭 전원	접지

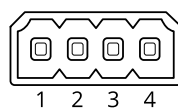
I/O 커넥터

모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 I/O 커넥터를 사용합니다. I/O 커넥터는 0 VDC 기준점 및 전원(12V DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

디지털 입력 - PIR 센서, 도어/윈도우 감지기, 유리 파손 감지기 등의 개방 회로와 폐쇄 회로 사이를 전환할 수 있는 장치를 연결하는 데 사용합니다.

디지털 출력 - 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface로 이벤트를 통해 또는 장치의 웹 인터페이스에서 활성화할 수 있습니다.

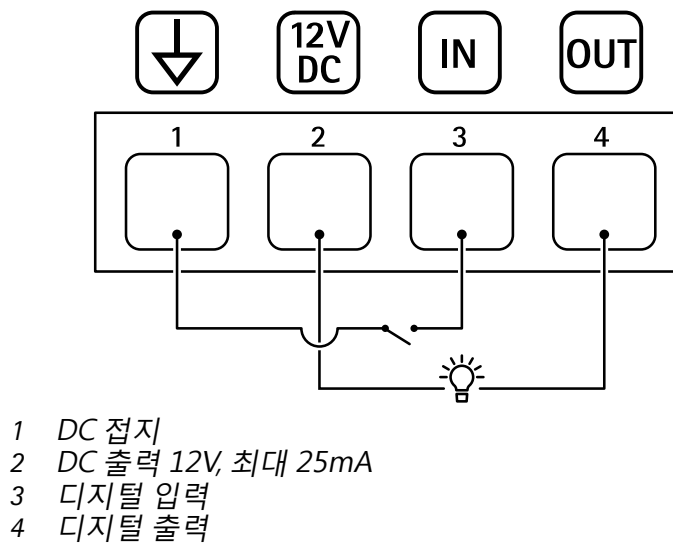
4핀 터미널 블록



기능	핀	비고	사양
DC 접지	1		0 VDC

DC 출력	2	 보조 장비에 전원을 공급할 때 사용 가능합니다. 참고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	12 VDC 최대 부하 = 25mA
디지털 입력	3	활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30 VDC
디지털 출력	4	활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30 VDC, 개방 드레인, 100mA

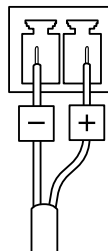
예:



연결 예

전원 커넥터

DC 전원 입력용 2핀 터미널 블록입니다. 정격 출력 전력이 $\leq 100W$ 로 제한되거나 정격 출력 전류가 $\leq 5A$ 로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.



문제 해결

공장 출하 시 기본 설정으로 재설정

▲ 경고

⚠ 이 제품에서는 유해한 광학적 방사선이 방출될 수 있습니다. 눈에 유해할 수 있습니다. 작동하는 램프를 응시하지 마십시오.

중요 사항

공장 출하 시 기본값으로 재설정은 주의해서 사용해야 합니다. 공장 출하 시 기본값으로 재설정하면 IP 주소를 비롯한 모든 설정이 공장 출하 시 기본값으로 재설정됩니다.

비고

카메라는 AXIS License Plate Verifier로 사전 구성되어 있습니다. 공장 출하 시 기본값으로 재설정할 경우 라이선스 키가 유지됩니다. 공장 초기화 후 애플리케이션을 다시 설치할 필요가 없습니다.

제품을 공장 출하 시 기본 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끕니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 개요, on page 44*을 참조하십시오.
3. 상태 LED 표시기가 주황색으로 깜박일 때까지 15-30초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시등이 녹색으로 바뀌면 과정이 완료됩니다. 제품이 공장 출하 시 기본 설정으로 재설정되었습니다. 네트워크에서 사용할 수 있는 DHCP 서버가 없는 경우 기본 IP 주소는 192.168.0.90입니다.
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 장치에 액세스합니다.
설치 및 관리 소프트웨어 도구는 axis.com/support의 지원 페이지에서 제공됩니다.

또한 장치의 웹 페이지를 통해 매개변수를 공장 출하 시 프리셋으로 재설정할 수 있습니다.

Maintenance(유지 보수) > Factory default(공장 출하 시 기본 설정)로 이동하고 **Default(기본)**를 클릭합니다.

AXIS OS 옵션

Axis는 활성 트랙 또는 LTS(장기 지원) 트랙에 따라 장치 소프트웨어 관리를 제공합니다. 활성 트랙에 있다는 것은 모든 최신 제품 기능에 지속적으로 액세스한다는 의미이며, LTS 트랙은 주로 버그 수정과 보안 업데이트에 중점을 두는 주기적 릴리즈와 함께 고정 플랫폼을 제공합니다.

최신 기능에 액세스하려고 하거나 Axis 엔드 투 엔드 시스템 제품을 사용하는 경우 활성 트랙의 AXIS OS를 사용하는 것이 좋습니다. 최신 활성 트랙에 대해 지속적으로 검증되지 않는 타사 통합을 사용하는 경우 LTS 트랙을 사용하는 것이 좋습니다. LTS를 사용하면 제품이 중요한 기능적 변경 사항을 도입하거나 기존 통합에 영향을 주지 않고 사이버 보안을 유지 관리할 수 있습니다. Axis 장치 소프트웨어 전략에 대한 자세한 내용은 axis.com/support/device-software를 참조하십시오.

현재 AXIS OS 버전 확인

AXIS OS는 당사 장치의 기능을 결정합니다. 문제를 해결할 때는 현재 AXIS OS 버전을 확인하여 시작하는 것이 좋습니다. 최신 버전에 특정 문제를 해결하는 수정 사항이 포함되어 있을 수 있습니다.

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

1. 장치의 웹 인터페이스 > **Status(상태)**로 이동합니다.
2. **Device info(장치 정보)**에서 AXIS OS 버전을 확인합니다.

AXIS OS 업그레이드

중요 사항

- 장치 소프트웨어를 업그레이드하면, 사전 구성된 설정과 사용자 지정 설정이 저장됩니다. Axis Communications AB는 새 AXIS OS 버전에서 해당 기능을 사용할 수 있더라도 설정이 저장된다고 보장할 수 없습니다.
- AXIS OS 12.6부터는 장치의 현재 버전과 목표 버전 사이에 있는 모든 LTS 버전을 설치해야 합니다. 예를 들어 현재 설치된 장치 소프트웨어 버전이 AXIS OS 11.2인 경우, 장치를 AXIS OS 12.6으로 업그레이드하기 전에 LTS 버전 AXIS OS 11.11을 설치해야 합니다. 자세한 내용은 *AXIS OS Lifecycle 가이드: 업그레이드 경로*를 참조하십시오.
- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

- 활성 트랙의 최신 AXIS OS 버전으로 장치를 업그레이드하면 제품이 사용 가능한 최신 기능을 수신합니다. 업그레이드하기 전에 항상 새 릴리스마다 제공되는 릴리즈 정보와 업그레이드 지침을 참조하십시오. 최신 AXIS OS 버전과 릴리즈 정보를 찾으려면 axis.com/support/device-software로 이동합니다.
1. axis.com/support/device-software에서 무료로 제공되는 AXIS OS 파일을 컴퓨터에 다운로드합니다.
 2. 장치에 관리자로 로그인합니다.
 3. **Maintenance > AXIS OS upgrade(유지보수 > AXIS OS 업그레이드)**로 이동하여 **Upgrade(업그레이드)**를 클릭합니다.

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

귀하가 사용할 수 있는 AXIS 장치 관리자는 동시에 여러 장치를 업그레이드합니다. axis.com/products/axis-device-manager에서 자세한 내용을 참고하십시오.

기술적 문제 및 가능한 해결책

AXIS OS 업그레이드 문제

AXIS OS 업그레이드 실패

업그레이드에 실패하면 장치가 이전 버전을 다시 로드합니다. 가장 일반적인 원인은 잘못된 AXIS OS 파일이 업로드된 것입니다. 장치에 해당하는 AXIS OS 파일 이름을 확인하고 다시 시도하십시오.

AXIS OS 업그레이드 후 문제

업그레이드 후 문제가 발생하면 **Maintenance(유지보수)** 페이지에서 이전에 설치된 버전으로 롤백하십시오.

IP 주소 설정 문제

IP 주소를 설정할 수 없음

- 장치에 설정하려는 IP 주소와 장치에 액세스하는 데 사용하는 컴퓨터의 IP 주소가 서로 다른 서브넷에 있는 경우, IP 주소를 설정할 수 없습니다. 네트워크 관리자에게 문의하여 IP 주소를 받으십시오.
- 해당 IP 주소를 다른 장치가 사용하고 있을 수 있습니다. 확인 방법:
 1. 네트워크에서 Axis 장치를 분리합니다.
 2. Command/DOS 창에서, ping을 입력한 후 장치의 IP 주소를 입력합니다.
 3. Reply from <IP address>: bytes=32; time=10...이라는 응답을 받는 경우, 이는 해당 IP 주소가 이미 네트워크의 다른 장치에서 사용 중일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 장치를 다시 설치하십시오.
 4. Request timed out을 수신하는 경우 이는 Axis 장치에 IP 주소를 사용할 수 있음을 의미합니다. 모든 케이블 배선을 확인하고 장치를 다시 설치하십시오.
- 동일한 서브넷에 있는 다른 장치와 IP 주소 충돌이 발생할 수 있습니다. DHCP 서버에서 다이내믹 주소를 설정하기 전에 Axis 장치의 고정 IP 주소가 사용되었습니다. 즉, 동일한 기본 고정 IP 주소를 다른 장치에서도 사용하는 경우, 해당 장치에 액세스하는 데 문제가 발생할 수 있습니다.

장치 액세스 관련 문제

브라우저로 장치에 액세스할 때 로그인할 수 없음

HTTPS가 활성화된 경우, 로그인 시 올바른 프로토콜(HTTP 또는 HTTPS)을 사용해야 합니다. 브라우저 주소창에 http 또는 https를 직접 입력해야 할 수 있습니다.

root 계정의 패스워드를 분실한 경우, 장치를 공장 초기화 설정으로 재설정해야 합니다. 지침에 대해서는 공장 출하 시 기본 설정으로 재설정, on page 47 항목을 참조하십시오.

IP 주소가 DHCP에 의해 변경됨

DHCP 서버가 할당한 IP 주소는 유동 IP 주소이므로 변경될 수 있습니다. IP 주소가 변경된 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다. 해당 모델이나 일련 번호 또는 DNS 이름을 이용하여 장치를 식별합니다(이름이 구성된 경우).

필요한 경우, 고정 IP 주소를 수동으로 할당할 수 있습니다. 지침에 대한 자세한 내용은 axis.com/support로 이동하여 확인하십시오.

IEEE 802.1X를 사용하는 동안 발생하는 인증 오류

인증이 제대로 작동하려면 Axis 장치의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. **System > Date and time(시스템 > 날짜 및 시간)**으로 이동합니다.

브라우저가 지원되지 않음

권장 브라우저 목록은 *브라우저 지원*, on page 2을 참조하십시오.

외부에서 장치에 액세스할 수 없음

외부에서 장치에 액세스하려면 Windows®용 다음 애플리케이션 중 하나를 사용하는 것이 좋습니다.

- AXIS Camera Station Edge: 무료이며, 기본 감시가 필요한 소규모 시스템에 적합합니다.
- AXIS Camera Station Pro: 90일 무료 평가판이며, 중규모 시스템에 적합합니다.

지침 및 다운로드를 axis.com/vms로 이동합니다.

스트리밍 문제

로컬 클라이언트에서 멀티캐스트 H.264만 액세스할 수 있습니다.

라우터가 멀티캐스팅을 지원하는지 또는 클라이언트와 장치 간에 라우터 설정을 구성해야 하는지 확인하십시오. TTL(Time To Live) 값을 늘려야 할 수도 있습니다.

클라이언트에 표시된 멀티캐스트 H.264가 없음

Axis 장치에서 사용된 멀티캐스트 주소가 네트워크에 유효한지 네트워크 관리자와 확인하십시오. 보기를 차단하는 방화벽이 있는지 네트워크 관리자에게 문의하십시오.

H.264 이미지의 렌더링 불량

그래픽 카드가 최신 드라이버를 사용하는지 확인하십시오. 일반적으로 제조사의 웹사이트에서 최신 드라이버를 다운로드할 수 있습니다.

색 채도는 H.264 및 Motion JPEG에서 차이가 있음

그래픽 어댑터의 설정을 수정하십시오. 자세한 내용은 어댑터 설명서를 참조하십시오.

예상보다 낮은 프레임 레이트

- 성능 고려 사항, on page 52을 참조하십시오.
- 클라이언트 컴퓨터에서 실행 중인 애플리케이션의 수를 줄이십시오.
- 동시 보기의 수를 제한하십시오.
- 네트워크 관리자를 통해 사용할 수 있는 대역폭이 충분한지 확인하십시오.
- 이미지 해상도를 낮추십시오.
- 장치의 웹 인터페이스에 로그인하고 프레임 레이트를 우선으로 하는 캡처 모드를 설정합니다. 캡처 모드를 변경하여 프레임 레이트를 우선시하면 사용된 장치와 사용 가능한 캡처 모드에 따라 최대 해상도가 낮아질 수 있습니다.
- 초당 최대 프레임은 Axis 장치의 유틸리티 주파수(60/50Hz)에 따라 다릅니다.

실시간 보기에서 H.265 인코딩을 선택할 수 없음

웹 브라우저는 H.265 디코딩을 지원하지 않습니다. H.265 디코딩을 지원하는 비디오 관리 시스템 또는 애플리케이션을 사용합니다.

MQTT 관련 문제

MQTT SSL 보안 포트 8883을 통해 연결할 수 없음

방화벽이 8883 포트를 안전하지 않은 것으로 간주하여 이 포트를 사용하는 트래픽을 차단합니다.

경우에 따라 서버/브로커는 MQTT 통신에 필요한 특정 포트를 제공하지 않을 수도 있습니다. HTTP/HTTPS 트래픽에 보통 사용되는 포트를 통해 MQTT를 사용하는 것은 가능할 수 있습니다.

- 서버/브로커에서 주로 포트 443으로 지정되는 WS/WSS(WebSocket/WebSocket Secure) 프로토콜이 지원되는 경우 이를 대신 사용하십시오. WS/WSS가 지원되는지와 어느 포트 및 베이스패스를 사용할지는 서버/브로커 공급자에게 확인하십시오.
- 서버/브로커가 ALPN을 지원하는 경우, 443과 같은 개방형 포트를 통해 MQTT 사용을 협상할 수 있습니다. 서버/브로커 제공업체에 문의하여 ALPN이 지원되는지, 어떤 ALPN 프로토콜과 포트를 사용할지 확인합니다.

찾는 내용이 여기에 없는 경우에는 axis.com/support에서 장애 처리 섹션을 확인해 보십시오.

알 수 없는 차량이 허용된 것으로 표시됨

애플리케이션이 허용 목록에 없는 번호판의 차량을 통과시킨 경우 비교에서 한 문자의 차이를 허용하기 때문일 수 있습니다.

예를 들어, **AXI S1234**가 허용 목록에 있는 경우 애플리케이션에서 **AXI SI234**를 허용합니다.

마찬가지로 **AXIS 1234**가 허용 목록에 있으면 애플리케이션에서 **AXI 1234**를 허용합니다.

허용되는 문자를 설정하려면 추가 설정, on page 24 항목으로 이동합니다.

애플리케이션과 컨트롤러 또는 릴레이 모듈 간의 연결이 작동하지 않음

컨트롤러 또는 릴레이 모듈이 HTTP를 통한 데이터 트래픽을 허용하는지 확인합니다. 이 설정을 변경하는 방법을 알아보려면 해당 장치의 사용자 설명서로 이동합니다.

레이더 페어링 문제

카메라와 레이더를 페어링할 수 없습니다.

카메라의 두 번째 보기 영역(**View area 2(보기 영역 2)**)은 사용하지 않아야 합니다. 레이더가 자동으로 이 영역에 할당되기 때문입니다.

두 번째 보기 영역이 사용되면 **Video > View areas(비디오 > 보기 영역)**로 이동하여 제거한 후 장치를 다시 페어링합니다.

카메라 보기의 움직임은 차량은 속도 오버레이 또는 레이더 보기의 트랙과 동기화되지 않습니다.

카메라와 레이더의 시간이 동기화되어 있는지 확인합니다.

상태를 확인하려면 각 장치의 웹 인터페이스에서 **Status > Time sync status(상태 > 시간 동기화 상태)**로 이동합니다. 상태가 **Synchronized: No(동기화됨: 아니요)**로 표시되면 **NTP settings(NTP 설정)**를 클릭하고 장치 동기화를 위한 시간 소스를 선택합니다. 두 장치 모두에 동일한 시간 소스를 사용해야 합니다.

카메라의 두 번째 보기 영역에 레이더 스트림이 올바르게 표시되지 않습니다.

옛지 투 옛지 페어링 후 레이더의 기본 해상도는 카메라의 웹 인터페이스와 VMS 모두에서 1280x720입니다. 다른 해상도를 선택하면 레이더 스트림이 잘못 표시됩니다.

레이더의 해상도를 조정하려면 카메라의 웹 인터페이스에서 **Video > Stream > General(비디오 > 스트림 > 일반)**로 이동하여 **View area 2(보기 영역 2)**를 선택합니다.

오버레이 문제

카메라의 웹 인터페이스를 통해 추가한 오버레이가 레이더 페어링 후 사라집니다.

카메라에 보기 영역을 두 개 이상 추가한 경우 이전에 추가한 오버레이는 카메라의 웹 인터페이스에서 사라집니다. 레이더는 레이더 페어링 후 두 번째 보기 영역을 차지하므로 카메라의 웹 인터페이스에 있는 기존 오버레이가 모두 사라집니다.

오버레이는 웹 인터페이스에서만 사라집니다. 여전히 VMS에서와 같이 오버레이가 포함된 스트림을 요청할 수 있습니다.

AXIS License Plate Verifier에 추가한 번호판 오버레이가 표시되지 않습니다.

AXIS Speed Monitor에서 차량 속도를 표시하는 오버레이를 추가한 다음 AXIS License Plate Verifier에서 번호판 오버레이를 켜면 번호판 오버레이가 나타나지 않습니다.

AXIS Speed Monitor를 통해 속도 오버레이를 추가하기 전에 먼저 AXIS License Plate Verifier에서 오버레이를 켜야 합니다.

성능 고려 사항

시스템을 설정할 때는 서로 다른 설정과 상황이 성능에 어떤 영향을 미치는지 고려하는 것이 중요합니다. 어떤 요소는 대역폭(비트 레이트)에, 어떤 요소는 프레임 레이트에 영향을 미치며, 두 가지 모두에 영향을 미치는 요소도 있습니다.

고려해야 할 가장 중요한 요소:

- 높은 이미지 해상도 또는 낮은 압축 수준으로 인해 대역폭에 영향을 주는 데이터가 많이 포함된 이미지가 생성될 수 있습니다.
- GUI에서 이미지를 회전하면 제품의 CPU 부하가 증가할 수 있습니다.
- 여러 Motion JPEG 클라이언트나 유니캐스트 H.264/H.265/AV1 클라이언트로 액세스하면 대역폭에 영향을 줍니다.
- 여러 클라이언트로 여러 스트림(해상도, 압축)을 동시에 보면 프레임 레이트와 대역폭 모두에 영향을 줍니다.
높은 프레임 레이트를 유지해야 하는 곳에서는 동일한 스트림을 사용합니다. 스트림 프로파일은 동일한 스트림을 보장하는데 사용할 수 있습니다.
- 서로 다른 코덱으로 비디오 스트림에 동시에 액세스하면 프레임 레이트와 대역폭에 모두 영향을 미칩니다. 최적의 성능을 위해 동일한 코덱을 사용하는 스트림을 사용하십시오.
- 이벤트 설정의 과도한 사용은 프레임 레이트에 영향을 줄 수 있는 제품의 CPU 부하에 영향을 줍니다.
- HTTPS를 사용하면 프레임 레이트가 낮아질 수 있으며 특히 Motion JPEG를 스트리밍하는 경우입니다.
- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.
- 성능이 낮은 클라이언트 컴퓨터에서 보기는 인식한 성능을 떨어뜨리고 프레임 레이트에 영향을 줍니다.
- 동시에 여러 AXIS Camera Application Platform(ACAP) 애플리케이션을 실행하면 프레임 레이트 및 일반적인 성능에 영향을 줍니다.

지원 센터 문의

추가 도움이 필요하면 axis.com/support로 이동하십시오.

사이버 보안

사이버 보안은 위험을 최소화하여 성공적인 제품 수명 주기를 지원합니다. Axis의 사이버 보안 접근 방식에 대한 심층 정보와 문서는 axis.com/about-axis/cybersecurity에서 확인할 수 있습니다. 아래 사이버 보안 지침에 따라 Axis의 제품 보안 알리를 받고 보안 수명 주기 및 폐기를 위해 제품을 구성하십시오.

Axis Trust Center에서 Axis가 보안 규정 준수, 투명성, 데이터 보호 및 개인정보 보호를 구현하는 방법에 대한 정보를 확인할 수 있습니다.

취약성 관리

Axis는 공통 취약점 및 노출(CVE) 번호 부여 기관(Common Vulnerability and Exposures (CVE) Numbering Authority: CNA)입니다. 노출 위험을 최소화하기 위해 Axis는 장치, 소프트웨어 및 서비스의 취약점을 식별하고 해결할 때 업계 표준을 따릅니다. Axis의 취약점 관리 정책에 대한 정보 또는 취약점 보고는 axis.com/vulnerability-management를 참조하십시오.

보안 알림

axis.com/security-notification-service에서 Axis 보안 알림 이메일을 구독하십시오. Axis 제품의 취약점, 해당 보안 권고 및 기타 보안 관련 사항에 대한 정보를 보내드립니다.

보안 제품 수명 주기

Axis는 보안 수명 주기 관리를 통해 제품 수명 전반에 걸쳐 위험을 최소화합니다. help.axis.com의 보안 강화 가이드를 사용하여 Axis 제품을 더 안전하게 구성하고 운영하며 다음에 대한 정보를 확인하십시오.

안전한 최초 사용 - Axis 제품은 처음부터 안전한 초기화와 암호화된 통신이 가능하도록 높은 기본 보호 수준으로 사전 구성되어 있습니다.

용도 및 일반적인 구성 실수 - Axis 보안 강화 가이드는 Axis 제품의 올바른 사용 방법에 대한 정보를 제공하며, 여기에는 피해야 할 일반적인 보안 관련 오용 및 구성 실수가 포함됩니다.

취약점 관리 및 공급망 투명성 - 취약점을 공개하고 공급망 투명성을 개선하기 위해 모든 소프트웨어 릴리스마다 axis.com에 소프트웨어 구성품 명세서(SBOM)가 게시됩니다.

폐기 및 데이터의 안전한 삭제 - 제품이 수명 주기 종료에 도달했을 때 안전하게 폐기하려면 제품을 공장 출하 시 기본 설정으로 재설정하십시오. 그러면 구성, 저장된 데이터 및 민감한 정보가 지워집니다.

T10191704_ko

2026-07 (M18.2)

© 2023 – 2026 Axis Communications AB