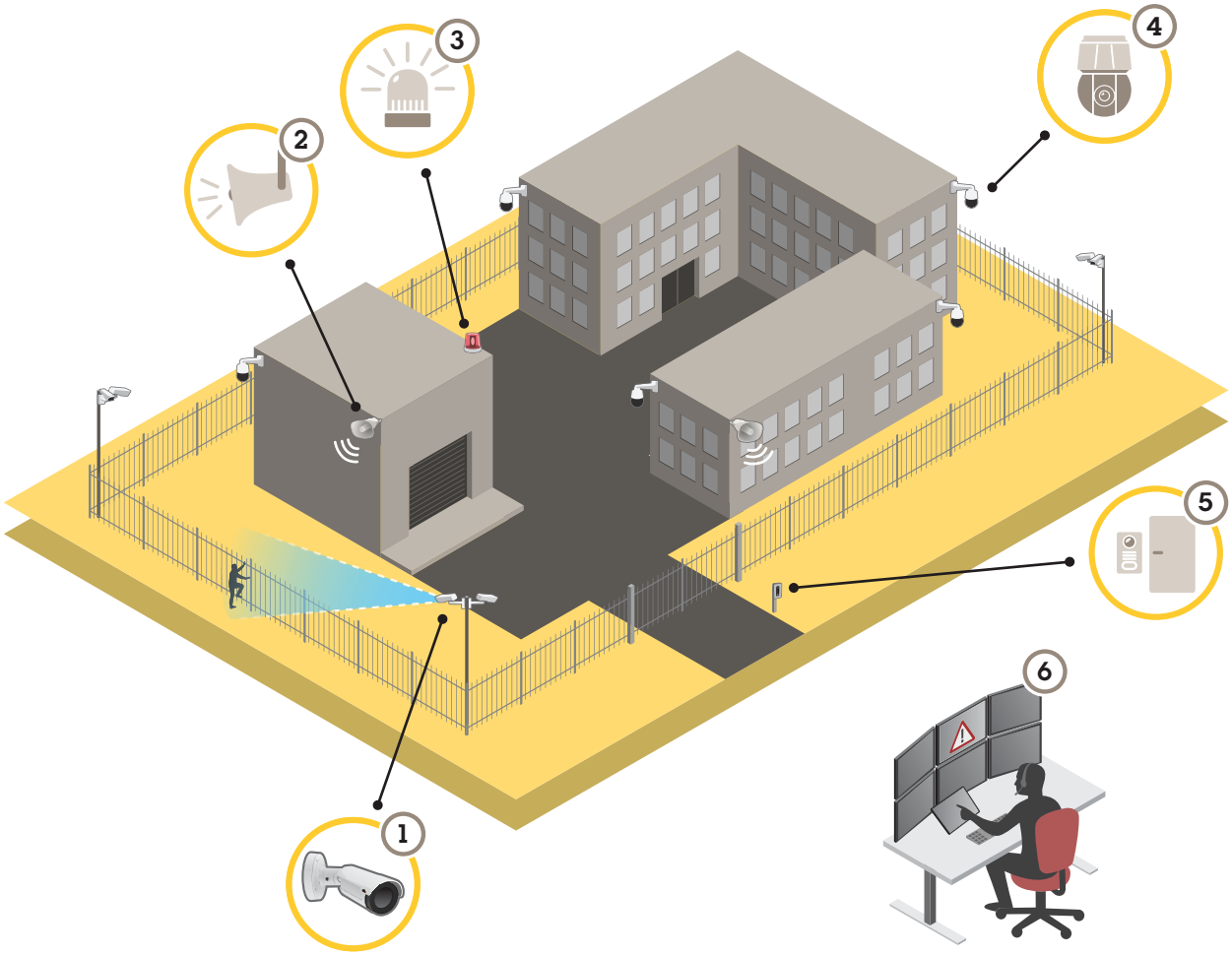
AXIS Q21 열상 카메라 시리즈

AXIS Q2111-E Thermal Camera
AXIS Q2112-E Thermal Camera

사용자 설명서

목차

솔루션 개요



1 *AXIS Perimeter Defender가 탑재된 열상 카메라*
2 *혼 스피커*
3 *깜박이는 비콘으로 지정합니다*
4 *PTZ 네트워크 카메라*
5 *도어 컨트롤러*
6 *감시 센터*

경계 구역 보호

침입 감지가 필요한 영역의 경우 분석 기능이 있는 열상 카메라를 사용하여 경계구역 보호를 설정할 수 있습니다. 경계구역 보호의 주요 목표는 가능한 한 초기 단계에서 위협 또는 실제 침입을 감지하는 것입니다.

경계구역 보호를 설정하려면 열상 카메라에 경계구역 감시 및 보호를 위한 분석 애플리케이션을 설치해야 합니다. Axis는 이 용도를 위해 AXIS Perimeter Defender 애플리케이션을 제공합니다. axis.com/products/axis-perimeter-defender에서 *AXIS Perimeter* Defender에 대한 자세한 내용을 읽을 수 있습니다.

- 침입자에게 경계구역이 보호되고 있음을 알리려면 깜박이는 비콘(3)을 사용하십시오. *깜박이는 비콘으로 침입자를 제지, on page 11*을 참조하십시오.
- 경고하고 저지하려면 미리 녹음된 경고 메시지를 재생하는 혼 스피커(2)를 연결하십시오. *오디오로 침입자 저지, on page 12*을 참조하십시오.

설치

장치의 설치 비디오.

미리 보기 모드

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

이 영상은 미리 보기 모드를 사용하는 방법을 보여줍니다.

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/support*에서 무료로 다운로드할 수 있습니다.

*IP 주소를 할당하고 장치에 액세스하는 방법*으로 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 6*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 7*을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이센스 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 34*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 34*을 참조하십시오.
   재설정 후 Secure Boot는 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

장치 구성

이 섹션에서는 하드웨어 설치가 완료된 후 제품을 시작하고 실행하기 위해 설치 프로그램이 수행해야 하는 모든 중요한 구성에 대해 설명합니다.

기본 설정

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.

방향 설정

1. **Video> Installation > Rotate(비디오 > 설치 > 회전)**로 이동합니다.
2. **0**, **90**, **180** 또는 **270**도를 선택합니다.
   길고 좁은 영역을 모니터링, on page 8 항목을 참고하십시오.

이미지 조정

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다. 특정 기능의 작동 방식에 대해 자세히 알아보려면 *상세 정보, on page 18*로 이동하십시오.

흔들림 보정으로 흔들리는 이미지 안정화

이미지 안정화는 바람이나 지나가는 차량 등으로 인해 진동이 발생할 수 있는 노출된 위치에 제품을 마운트하는 환경에 적합합니다.

이 기능은 이미지를 더 부드럽고 안정적이며 덜 흐릿하게 만듭니다. 또한 압축된 이미지의 파일 크기를 줄이고 비디오 스트림의 비트 레이트를 낮춰줍니다.

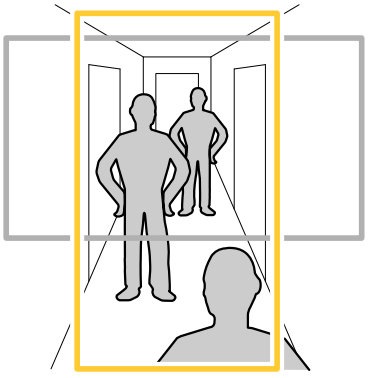
비고

이미지 안정화를 켜면 이미지가 약간 잘려 최대 해상도가 낮아집니다.

1. **Video > Installation > Image correction(비디오 > 설치 > 이미지 보정)**으로 이동합니다.
2. **Image stabilization(흔들림 보정)**을 켭니다.

길고 좁은 영역을 모니터링

Corridor Format을 사용하여 계단, 복도, 도로 또는 터널과 같이 길고 좁은 영역에서 전체 화각을 효과적으로 활용하십시오.



1. 장치에 따라 카메라 또는 카메라의 3축 렌즈를 90° 또는 270°로 돌립니다.
2. 장치에 보기의 자동 회전이 없으면 **Video > Installation(비디오 > 설치)**으로 이동합니다.
3. 보기를 90° 또는 270° 돌립니다.

이미지 오버레이 표시

비디오 스트림에서 오버레이로 이미지를 추가할 수 있습니다.

1. **Video > Overlays(비디오 > 오버레이)**로 이동합니다.
2. **Manage images(이미지 관리)**를 클릭합니다.
3. 이미지를 업로드하거나 끌어다 놓습니다.
4. **Upload(업로드)**를 클릭합니다.
5. 드롭다운 목록에서 **Image(이미지)**를 선택하고 + 을 클릭합니다.
6. 이미지와 위치를 선택합니다. 실시간 보기에서 오버레이 이미지를 끌어 위치를 변경할 수도 있습니다.

텍스트 오버레이 표시

비디오 스트림에서 텍스트 필드를 오버레이로 추가할 수 있습니다. 이것은 예를 들어 비디오 스트림에 날짜, 시간 또는 회사 이름을 표시하려는 경우에 유용합니다.

1. **Video > Overlays(비디오 > 오버레이)**로 이동합니다.
2. **Text(텍스트)**를 선택하고 + 을 클릭합니다.
3. 표시할 텍스트를 입력하거나, 수정자를 선택하여 (예: 현재 날짜)를 표시합니다.
4. 위치를 선택합니다. 실시간 보기에서 오버레이를 클릭한 후 드래그하여 위치를 변경할 수도 있습니다.

비디오 보기 및 녹화

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다. 스트리밍 및 저장 작동 방식에 대해 자세히 알아 보려면 *스트리밍 및 저장, on page 18*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 10*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. AXIS Camera Station(5.46 이상) 또는 다른 호환 가능한 영상 관리 소프트웨어를 사용하여 비디오를 녹화하십시오. 지침에 대해서는 *AXIS Camera Station 사용자 설명서*를 참조하십시오.
3. 녹화된 영상을 내보냅니다.
4. AXIS File Player를 사용하여 비디오를 재생합니다. *AXIS File Player를 다운로드합니다.*

   은 비디오를 조작한 사람이 없음을 나타냅니다.

비고

비디오에 대한 자세한 정보를 보려면 비디오를 마우스 오른쪽 버튼으로 클릭하고 **Show digital signature(디지털 서명 표시)**를 선택합니다.

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.

깜박이는 비콘으로 침입자를 제지

깜박이는 신호등을 사용하여 침입 가능성이 있는 사용자에게 경계가 보호되고 있음을 알립니다.

이 예에서는 비콘 라이트를 연결하고 열상 카메라가 침입을 감지할 때마다 깜박이도록 설정하는 방법을 설명합니다. 이 예에서 비컨 라이트는 근무 시간 외에 월요일~금요일 18:00~08:00에만 깜박이도록 활성화할 수 있으며 활성화될 때마다 30초 동안 깜박입니다.

필수 하드웨어

- 연결 와이어(파란색과 빨간색 각 1개, 최소 면적: 0.25mm^2, 최대 면적: 0.5mm^2)
- 깜박이는 비콘(12V DC, 최대 25mA)

비고

연결 와이어의 최대 길이는 와이어 영역과 깜박이는 비콘의 전력 소비에 따라 다릅니다.

물리적으로 장치 연결

1. 빨간색 와이어를 카메라 I/O 커넥터의 핀 2(DC 출력, 12V DC)에 연결합니다.
2. 빨간색 와이어의 다른 쪽 끝을 깜박이는 비콘에 **+**로 표시된 커넥터에 연결합니다.
3. 파란색 와이어를 카메라 I/O 커넥터의 핀 4(디지털 출력)에 연결합니다.
4. 파란색 와이어의 다른 쪽 끝을 깜박이는 비콘에 **-**로 표시된 커넥터에 연결합니다.

I/O 포트 구성

카메라의 웹 인터페이스에서 카메라에 깜박이는 비콘 연결:

1. **시스템 > 액세서리 > I/O 포트**로 이동합니다.
2. **Port(포트 2)**의 경우, Flashing beacon(깜박이는 비콘)으로 이름을 지정합니다.
3. **Normal state(정상 상태)**에서  을 클릭하여 포트의 정상 상태를 개방 회로(NO)로 설정합니다. 이벤트가 발생하면 비콘이 깜박이기 시작합니다.

룰 만들기

무언가 감지되면 깜박이기 시작하도록 카메라가 비콘으로 알림을 전송하려면 카메라에서 룰을 생성해야 합니다.

1. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 룰을 추가합니다.
2. **Name(이름)**에서, Flashing beacon(깜박이는 비콘)을 입력합니다.
3. **작업 사이에 대기**(hh:mm:ss 형식)를 30초까지 설정합니다.
4. 조건 목록에서 **Application(애플리케이션)**에서 경계구역 보호(perimeter defender) 애플리케이션을 선택합니다.
5. **Use this condition as a trigger(이 조건을 트리거로 사용)**을 선택합니다.
6. 다른 조건을 추가하기 위해  을 클릭합니다.
7. 조건 목록의 **Scheduled and recurring(예약 및 반복)**에서 **Schedule(일정)**을 선택합니다.
8. 스케줄 목록에서 **After hours(근무 시간 후)**를 선택합니다.
9. 작업 목록의 **I/O**에서 **룰이 활성화되는 동안 토글 I/O**를 선택합니다.
10. 포트 목록에서 **깜박임 비콘** 포트를 선택합니다.
11. **활성화**하기 위해 **상태**를 설정합니다.

12. **Save(저장)**를 클릭합니다.

오디오로 침입자 저지

침입자에게 경고하고 저지하려면 네트워크 혼 스피커를 사용하십시오.

이 예에서는 Axis 네트워크 혼 스피커를 연결하고 열상 카메라가 침입을 감지할 때마다 오디오 클립을 재생하도록 설정하는 방법을 설명합니다. 이 예에서 혼 스피커는 근무 시간 외에 월요일~금요일 18:00~08:00에만 활성화할 수 있습니다.

장치를 연결

1. **시스템 > 에지 투 에지 > 페어링**으로 이동합니다.
2. 스피커의 IP 주소, 사용자 이름 및 패스워드를 입력합니다. 관리자 또는 운영자 계정을 사용해야 합니다.
3. **Connect(연결)**를 클릭합니다.

카메라에 오디오 클립 업로드

1. **Audio(오디오) > Audio clips(오디오 클립)**로 이동하여 을 클릭합니다.
2. **+ 클립 추가**를 클릭합니다.
3. 오디오 클립을 찾아 업로드합니다.
4. **Close(닫기)**를 클릭합니다.

룰 만들기

카메라에 무언가가 감지될 때 스피커가 오디오 클립을 재생하도록 하려면 카메라에서 룰을 생성해야 합니다.

1. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 룰을 추가합니다.
2. **Name(이름)**에서, Deter with audio(오디오로 억제)를 입력합니다.
3. 조건 목록에서 **Application(애플리케이션)**에서 경계구역 보호(perimeter defender) 애플리케이션을 선택합니다.
4. **Use this condition as a trigger(이 조건을 트리거로 사용)**을 선택합니다.
5. 다른 조건을 추가하기 위해 을 클릭합니다.
6. 조건 목록의 **Scheduled and recurring(예약 및 반복)**에서 **Schedule(일정)**을 선택합니다.
7. 스케줄 목록에서 **After hours(근무 시간 후)**를 선택합니다.
8. 액션 목록의 **Audio clips(오디오 클립)**에서 **Play audio clip(오디오 클립 재생)**을 선택합니다.
9. **Clip(클립)**에서 업로드한 오디오 클립을 선택합니다.
10. **Audio output(오디오 출력)**에서 페어링된 네트워크 스피커에 대해 **1**을 선택합니다.
11. **Save(저장)**를 클릭합니다.

카메라가 모션을 감지하면 가상 입력을 통해 스트로브 사이렌 활성화

Axis 스트로브 사이렌을 사용하면 침입자에게 경계구역이 보호되고 있음을 알릴 수 있습니다.

이 예에서는 AXIS Motion Guard가 움직임을 감지할 때마다 스트로브 사이렌에서 프로파일을 활성화하는 방법을 설명합니다.

시작하기 전:

- 스트로브 사이렌에서 운영자 또는 관리자 권한으로 새 계정을 생성합니다.
- 스트로브 사이렌에서 프로파일을 생성합니다.
- 카메라에서 AXIS Motion Guard를 설정하고 "카메라 프로파일"이라는 프로파일을 생성합니다.

카메라에 두 명의 수신자를 생성:

1. 카메라의 장치 인터페이스에서 **System > Events > Recipients(시스템 > 이벤트 > 수신자)**로 이동하고 수신자를 추가합니다.
2. 다음 정보를 입력합니다.
   - **이름**: 가상 포트 활성화
   - **Type(유형)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi <IPaddress>를 스트로브 사이렌의 주소로 바꿉니다.
   - 새로 만든 스트로브 사이렌 계정의 계정 및 패스워드입니다.
3. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
4. **Save(저장)**를 클릭합니다.
5. 다음 정보를 사용하여 두 번째 수신자를 추가합니다.
   - **이름**: 가상 포트 비활성화
   - **Type(유형)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi <IPaddress>를 스트로브 사이렌의 주소로 바꿉니다.
   - 새로 만든 스트로브 사이렌 계정의 계정 및 패스워드입니다.
6. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

카메라에 두 룰을 생성:

1. **Rules(룰)**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.
   - **이름**: 가상 IO1 활성화
   - **Condition(조건)**: **Applications(애플리케이션) > Motion Guard: Camera profile(모션 가드: 카메라 프로파일)**
   - **Action(액션)**: **Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)**
   - **Recipient(수신자)**: **가상 포트 활성화**
   - **Query string suffix(쿼리 문자열 접미사)**: schemaversion=1&port=1
3. **Save(저장)**를 클릭합니다.
4. 다음 정보가 포함된 다른 룰을 추가합니다.
   - **이름**: 가상 IO1 비활성화
   - **Condition(조건)**: **Applications(애플리케이션) > Motion Guard: Camera profile(모션 가드: 카메라 프로파일)**
   - **Invert this condition(이 조건을 반전하기)**을 선택합니다.
   - **Action(액션)**: **Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)**
   - **Recipient(수신자)**: **가상 포트 비활성화**
   - **Query string suffix(쿼리 문자열 접미사)**: schemaversion=1&port=1
5. **Save(저장)**를 클릭합니다.

스트로브 사이렌에서 룰 생성:

1. 스트로브 사이렌의 웹 인터페이스에서 **시스템 > 이벤트**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.

- **이름**: 가상 입력 1에서 트리거
- **Condition(조건)**: **I/O > Virtual input(가상 입력)**
- **Port(포트)**: **1**
- **Action(액션)**: **Light and siren(조명 및 사이렌) > Run light and siren profile while the rule is active(룰이 활성 상태인 동안 조명 및 사이렌 프로파일 실행)**
- **Profile(프로파일)**: 새로 생성된 프로파일 선택

3. **Save(저장)**를 클릭합니다.

입력 신호로 탬퍼링 감지

이 예는 입력 신호가 끊기거나 합선되었을 때 이메일을 보내는 방법을 설명합니다. I/O 커넥터에 대한 자세한 내용은 *page 27* 항목을 참조하십시오.

1. **System(시스템) > Accessories(액세서리) > I/O ports(I/O 포트)**로 이동하여 해당 포트의 **Supervised(감시됨)**을 켭니다.

이메일 수신자 추가:

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

룰 생성:

1. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록의 **I/O**에서 **Supervised input(관리된 입력)**을 선택합니다.
4. 해당 포트를 선택합니다.
5. 액션 목록의 **Notifications(알림)** 아래에서 **Send notification to email(이메일로 알림 전송)**을 선택한 다음, 목록에서 수신자를 선택합니다.
6. 이메일의 제목과 메시지를 입력합니다.
7. **Save(저장)**를 클릭합니다.

인클로저가 열릴 때 알림 트리거

이 예에서는 장치의 하우징이나 케이싱이 열릴 때 이메일 알림을 설정하는 방법을 설명합니다.

이메일 수신자 추가:

1. **System > Events > Recipients(시스템 > 이벤트 >수신자)**로 이동하고 **Add recipient(수신자 추가)**를 클릭합니다.
2. 수신자의 이름을 입력합니다.
3. 알림 유형으로 **Email(이메일)**을 선택합니다.
4. 수신자의 이메일 주소를 입력합니다.
5. 카메라에서 알림을 보낼 때 사용할 이메일 주소를 입력합니다.
6. 보내는 이메일 계정의 로그인 정보와 함께 SMTP 호스트 이름 및 포트 번호를 입력합니다.
7. 이메일 설정을 테스트하려면 **Test(테스트)**를 클릭합니다.

8. **Save(저장)**를 클릭합니다.

룰 생성:

9. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 **Add a rule(룰 추가)**을 클릭합니다.
10. 룰에 대한 이름을 입력합니다.
11. 조건 목록에서 **Casing open(케이스 열림)**을 선택합니다.
12. 액션 목록에서 **Send notification to email(이메일로 알림 전송)**을 선택합니다.
13. 목록에서 수신자를 선택합니다.
14. 이메일의 제목과 메시지를 입력합니다.
15. **Save(저장)**를 클릭합니다.

스프레이로 렌즈를 페인트하면 자동으로 이메일 보내기

탬퍼링 감지 활성화:

1. **System(시스템) > Detectors(감지기) > Camera tampering(카메라 탬퍼링)**으로 이동합니다.
2. **Trigger delay(트리거 지연)**의 값을 설정합니다. 값은 이메일을 보내기 전에 통과해야 하는 시간을 나타냅니다.

이메일 수신자 추가:

3. **System > Events > Recipients(시스템 > 이벤트 > 수신자)**로 이동하고 수신자를 추가합니다.
4. 수신자의 이름을 입력합니다.
5. **Email(이메일)**을 선택합니다.
6. 이메일을 보낼 이메일 주소를 입력합니다.
7. 카메라에는 자체 이메일 서버가 없으므로 메일을 전송하려면 다른 이메일 서버에 로그인해야 합니다. 이메일 제공업체에 따라 나머지 정보를 작성합니다.
8. 테스트 이메일을 보내려면 **Test(테스트)**를 클릭합니다.
9. **Save(저장)**를 클릭합니다.

룰 생성:

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

오디오

녹화 영상에 오디오 추가

오디오 켜기:

1. **Video > Stream > Audio(비디오 > 스트림 > 오디오)**로 이동하여 오디오를 포함합니다.
2. 장치에 둘 이상의 입력 소스가 있는 경우 **Source(소스)**에서 올바른 소스를 선택하십시오.
3. **Audio > Device settings(오디오 > 장치 설정)**으로 이동하고 올바른 입력 소스를 켜십시오.
4. 입력 소스를 변경하려면 **Apply changes(변경 사항 적용)**을 클릭합니다.

녹화 시 사용되는 스트림 프로파일을 편집합니다.

5. **System > Stream profiles(시스템 > 스트림 프로파일)**로 이동하고 스트림 프로파일을 선택합니다.
6. **Include audio(오디오 포함)**을 선택하고 전원을 켭니다.
7. **Save(저장)**를 클릭합니다.

웹 인터페이스

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

상세 정보

색상 팔레트

육안으로 열화상에서 세부 사항을 구분할 수 있도록 이미지에 색상 팔레트를 적용할 수 있습니다. 팔레트의 색상은 온도 차이를 강조하는 인공적으로 제작된 의사 색상입니다.

이 제품에는 선택할 수 있는 몇 가지 색상 팔레트가 있습니다. 운영자가 비디오 스트림을 보는 경우, 모든 팔레트를 선택할 수 있습니다. 비디오 스트림이 애플리케이션에서만 사용되는 경우, 흰색 열 팔레트를 선택합니다.

오버레이

오버레이는 비디오 스트림 위에 중첩 표시됩니다. 녹화나 제품을 설치 및 구성하는 동안 타임스탬프와 같은 추가 정보를 제공하는 데 사용됩니다. 텍스트나 이미지를 추가할 수 있습니다.

비디오 스트리밍 표시기는 다른 유형의 오버레이입니다. 라이브 뷰 비디오 스트림이 라이브임을 보여줍니다.

스트리밍 및 저장

비디오 압축 형식

어떤 압축 방법을 사용할지는 보기 요구 사항과 네트워크 속성에 따라 다르게 결정됩니다. 다음과 같은 옵션을 사용할 수 있습니다.

Motion JPEG

비고

Opus 오디오 코덱에 대한 지원을 받기 위해 Motion JPEG 스트림은 항상 RTP를 통해 전송됩니다.

Motion JPEG 또는 MJPEG는 디지털 비디오 시퀀스로 개별 JPEG 이미지의 시리즈로 구성됩니다. 이런 이미지는 업데이트된 모션을 지속적으로 보여주는 스트림을 생성하기에 충분한 레이트로 표시되고 업데이트됩니다. 동영상을 인식하는 뷰어에서 레이트는 초당 최소 16개의 이미지 프레임이어야 합니다. 초당 30(NTSC) 또는 25(PAL) 프레임은 완전한 동영상으로 인식됩니다.

Motion JPEG 스트림은 상당한 양의 대역폭을 사용하지만 탁월한 이미지 품질을 제공하며 스트림에 포함된 모든 이미지에 액세스합니다.

H.264 또는 MPEG-4 Part 10/AVC

비고

H.264는 라이센스가 부여된 기술입니다. Axis 제품에는 1개의 H.264 보기 클라이언트 라이센스가 포함되어 있습니다. 라이센스가 없는 추가 클라이언트 사본을 설치하는 것은 금지되어 있습니다. 추가 라이센스를 구입하려면 Axis 리셀러에게 문의하십시오.

H.264는 이미지 품질 저하 없이 디지털 비디오 파일의 크기를 Motion JPEG 형식에 비해 80% 이상, 이전 MPEG 형식에 비해 50%까지 줄일 수 있습니다. 이는 비디오 파일에 필요한 네트워크 대역폭과 저장 공간을 훨씬 더 줄일 수 있다는 것을 의미합니다. 즉, 주어진 비트 레이트에서 높은 수준의 비디오 품질을 제공할 수 있습니다.

H.265 또는 MPEG-H Part 2/HEVC

H.265는 화질 저하 없이 H.264에 비해 디지털 비디오 파일의 크기를 25% 이상 줄일 수 있습니다.

비고

- H.265는 라이센스가 부여된 기술입니다. Axis 제품에는 1개의 H.265 보기 클라이언트 라이센스가 포함되어 있습니다. 라이센스가 없는 추가 클라이언트 사본을 설치하는 것은 금지되어 있습니다. 추가 라이센스를 구입하려면 Axis 리셀러에게 문의하십시오.
- 대부분의 웹 브라우저는 H.265 디코딩을 지원하지 않으며, 이 때문에 카메라는 웹 인터페이스에서 H.265 디코딩을 지원하지 않습니다. 대신 H.265 디코딩을 지원하는 영상 관리 시스템 또는 애플리케이션을 사용할 수 있습니다.

이미지, 스트림 및 스트림 프로파일 설정은 서로 어떤 관련이 있습니까?

Image(이미지)탭에는 제품의 모든 비디오 스트림에 영향을 주는 카메라 설정이 포함되어 있습니다. 이 탭에서 내용을 변경하면 모든 비디오 스트림 및 녹화에 즉시 영향을 줍니다.

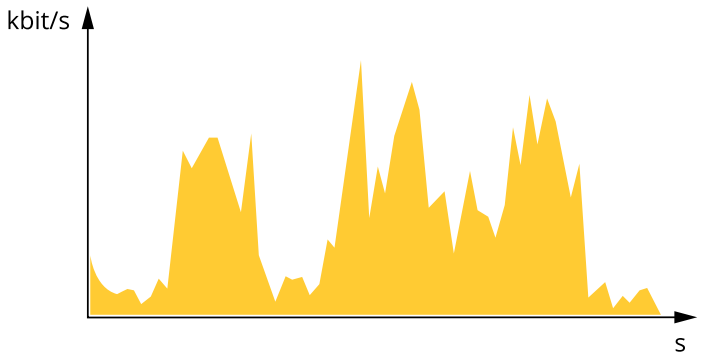
Stream(스트림)탭에는 비디오 스트림 설정이 포함되어 있습니다. 제품에서 비디오 스트림을 요청하고 예를 들어 해상도 또는 프레임 레이트를 지정하지 않으면 이러한 설정을 얻을 수 있습니다. **Stream(스트림)**탭에서 설정을 변경하면 진행 중인 스트림에는 영향을 미치지 않지만 새 스트림을 시작할 때 적용됩니다.

Stream profiles(스트림 프로파일) 설정은 **Stream(스트림)** 탭의 설정보다 우선합니다. 특정 스트림 프로파일이 있는 스트림을 요청하면 해당 프로파일의 설정이 스트림에 포함됩니다. 스트림 프로파일을 지정하지 않고 스트림을 요청하거나 제품에 존재하지 않는 스트림 프로파일을 요청하는 경우 스트림은 **Stream(스트림)** 탭의 설정을 포함합니다.

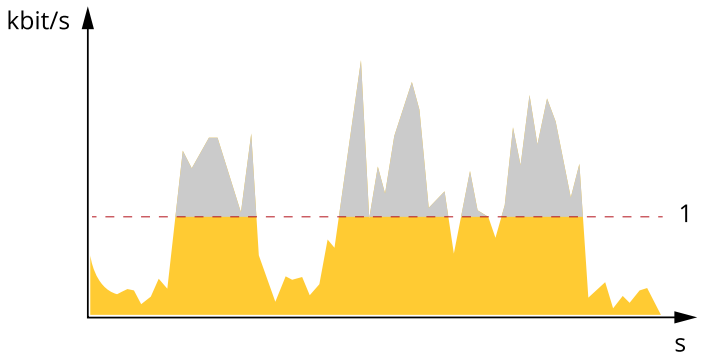
비트 레이트 제어

비트 레이트 제어가 비디오 스트림의 대역폭 소비를 관리하도록 지원합니다.

가변 비트 레이트(VBR)
가변 비트 레이트를 사용하면 장면의 활동 수준에 따라 대역폭 소모가 달라질 수 있습니다. 움직임이 많을수록 많은 대역폭이 필요합니다. 가변 비트 레이트를 사용하면 일정한 이미지 품질이 보장되지만 더 많은 스토리지가 있는지 확인해야 합니다.



최대 비트 레이트(MBR)
최대 비트 레이트는 시스템의 비트 레이트 제한을 처리하기 위해 목표 비트 레이트를 설정하도록 합니다. 순간 비트 레이트가 지정된 목표 비트 레이트 미만으로 유지되면 이미지 품질이나 프레임 속도가 저하될 수 있습니다. 이미지 품질 또는 프레임 레이트를 우선시하도록 선택할 수 있습니다. 대상 비트 레이트를 예상 비트 레이트보다 높은 값으로 구성하는 것이 좋습니다. 이것은 장면에 높은 수준의 활동이 있는 경우 여백을 제공합니다.

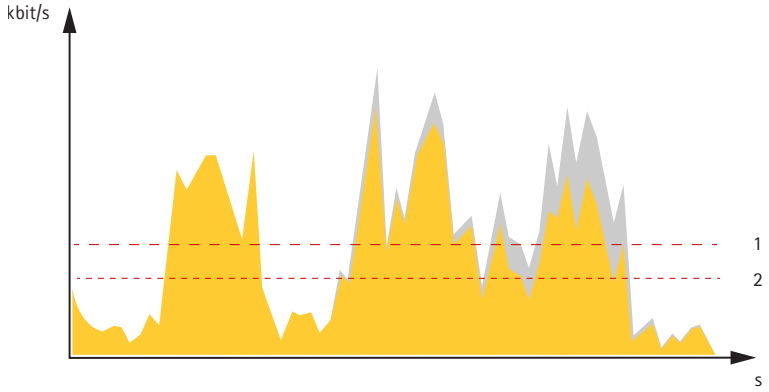


1 대상 비트 레이트

평균 비트 레이트(ABR)
평균 비트 레이트를 사용하면 더 오랜 기간에 비트 레이트가 자동으로 조정됩니다. 지정된 대상을 충족하고 사용 가능한 스토리지를 기반으로 최상의 비디오 품질을 제공할 수 있습니다. 정적 장면에 비해 활동량이 많은 장면에서 비트 레이트가 더 높습니다. 평균 비트 레이트 옵션을 사용하면 활동이 많

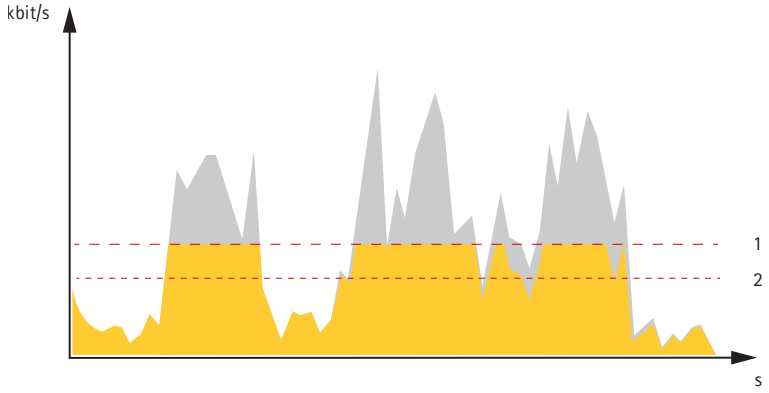
은 장면에서 더 나은 이미지 품질을 얻을 가능성이 더 큽니다. 이미지 품질이 지정된 대상 비트 레이트에 맞게 조정될 때 지정된 시간(보존 시간) 동안 비디오 스트림을 저장하는 데 필요한 총 스토리지를 정의할 수 있습니다. 다음 방법 중 하나로 평균 비트 레이트 설정을 지정하십시오.

- 예상 스토리지 요구량을 계산하려면 대상 비트 레이트와 보존 시간을 설정하십시오.
- 사용 가능한 저장 공간과 필요한 보존 시간을 기준으로 평균 비트 레이트를 계산하려면 대상 비트 레이트 계산기를 사용하십시오.



1 대상 비트 레이트
2 실제 평균 비트 레이트

최대 비트 레이트를 설정하고 평균 비트 레이트 옵션 내에서 대상 비트 레이트를 지정할 수도 있습니다.



1 대상 비트 레이트
2 실제 평균 비트 레이트

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

Axis 분석 및 앱에 대한 사용자 설명서는 *help.axis.com*에서 확인할 수 있습니다.

비고

- 여러 앱을 동시에 실행할 수 있지만 일부 앱은 서로 호환되지 않을 수 있습니다. 특정 앱의 조합은 동시에 실행할 때 처리 능력 또는 메모리 리소스가 너무 많이 필요할 수도 있습니다. 배포하기 전에 앱이 서로 원활하게 작동하는지 확인하십시오.

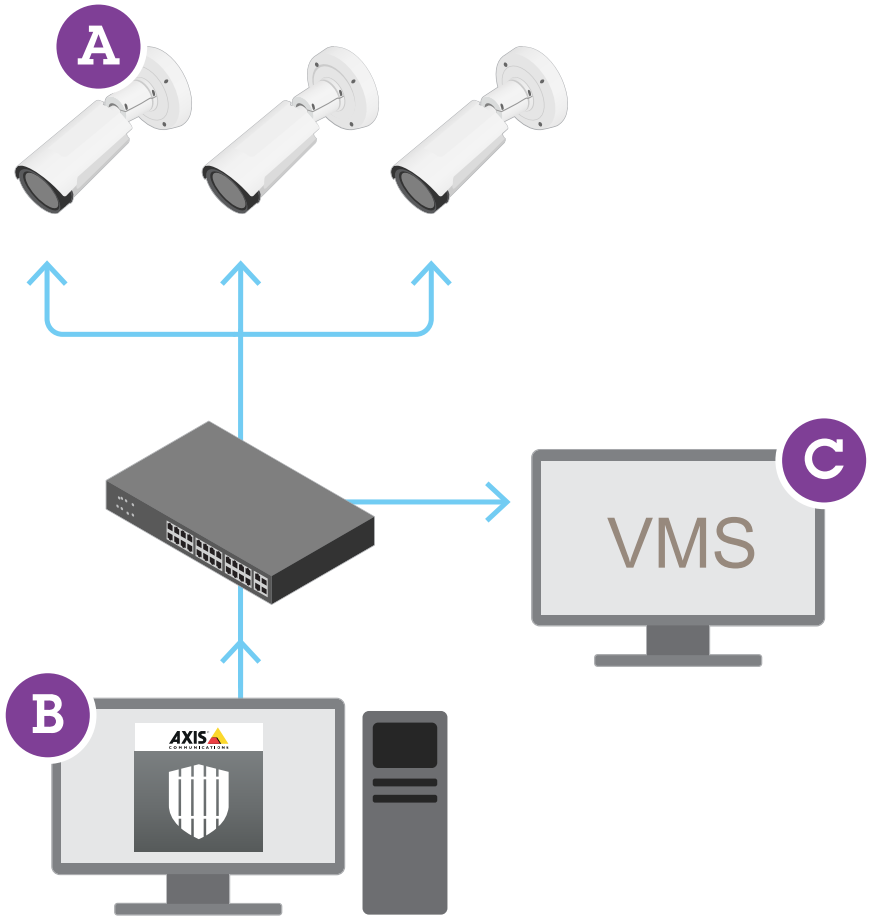
AXIS Perimeter Defender

AXIS Perimeter Defender는 경계구역 감시 및 보호를 위한 애플리케이션입니다. 신뢰할 수 있는 침입 감지 기능을 통해 물리적 접근 제어 시스템을 강화해야 하는 높은 보안 경계구역 보호에 이상적입니다.

AXIS Perimeter Defender는 주로 경계를 표시하는 펜스를 따라 소위 경계 영역 보호를 위해 설계되었습니다. 경계 영역이라는 용어는 사람들이 없어야 하는 영역을 말합니다.

실외 환경에서 AXIS Perimeter Defender를 사용하여 다음을 수행하십시오.

- 움직이는 사람을 감지합니다.
- 차량 유형을 구별하지 않고 움직이는 차량을 감지합니다.



이 카메라는 보정 모드, AI 모드 또는 두 가지 모드를 결합한 상태로 애플리케이션 실행이 가능합니다. AI 모드에서만 실행하도록 선택하면 카메라 장착이 더 유연해지며 카메라를 보정할 필요가 없습니다.

AXIS Perimeter Defender는 카메라(A)에 애플리케이션을 설치 및 설정하는 데스크톱 인터페이스(B)로 구성됩니다. 그런 다음 영상 관리 소프트웨어(C)로 알람을 보내도록 시스템을 구성할 수 있습니다.

AXIS Perimeter Defender PTZ Autotracking은 동일한 데스크톱 인터페이스를 사용하는 AXIS Perimeter Defender 애플리케이션의 플러그인입니다. 플러그인을 사용하면 고정형 영상 카메라 또는 열상 카메라와 Axis Q-line PTZ 카메라를 페어링할 수 있습니다. 그런 다음 고정형 카메라로 장면의 감지 범위를 지속적으로 유지하면서 PTZ 카메라가 감지된 객체를 자동으로 추적하고 더 자세히 표시하도록 할 수 있습니다.

중요 사항

AXIS Perimeter Defender PTZ Autotracking을 사용하려면 고정 카메라와 PTZ 카메라를 모두 보정해야 합니다.

AXIS Perimeter Defender는 다음 유형의 감지 시나리오를 제공합니다.

- **침입**: 사람이나 차량이 지면에 정의된 영역에 진입할 때(모든 방향과 모든 궤적으로) 알람을 트리거합니다.
- **배회**: 사람 또는 차량이 사전 정의된 시간(초) 동안 지면에 정의된 영역에 머물 때 알람을 트리거합니다.
- **영역 통과**: 사람이나 차량이 지정된 순서로 지면에 정의된 둘 이상의 영역을 통과할 때 알람을 트리거합니다.
- **조건**: 사람이나 차량이 지면에 정의된 다른 영역을 먼저 통과하지 않고 지면에 정의된 영역에 진입할 때 알람을 트리거합니다.

사이버 보안

제품별 사이버 보안 정보는 axis.com에서 해당 제품의 데이터시트를 참조하십시오.

AXIS OS의 사이버 보안에 대한 자세한 내용은 *AXIS OS 보안 강화 가이드*를 참조하십시오.

Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 장치의 ID 및 무결성을 보장하고 무단 액세스로부터 중요한 정보를 보호하는 기능을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

Signed OS

서명된 OS는 소프트웨어 공급업체가 개인 키로 AXIS OS 이미지에 서명하여 구현됩니다. 서명이 운영 체제에 첨부되면 장치는 소프트웨어를 설치하기 전에 소프트웨어를 확인합니다. 장치에서 소프트웨어 무결성이 손상되었음을 감지하면 AXIS OS 업그레이드가 거부됩니다.

Secure Boot

Secure Boot는 변경 불가능 메모리(부트 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부트 프로세스입니다. 서명된 OS 사용을 기반으로 하는 Secure Boot는 장치가 승인된 소프트웨어로만 부팅할 수 있도록 합니다.

보안 키 저장소

개인 키 보호 및 암호화 작업의 안전한 실행을 위한 변조 방지 환경입니다. 보안 침해 발생 시 무단 액세스 및 악의적인 추출을 방지합니다. 보안 요구 사항에 따라, Axis 장치에는 하드웨어로 보호되는 보안 키 저장소를 제공하는 하드웨어 기반 암호화 컴퓨팅 모듈이 하나 또는 여러 개 있을 수 있습니다. 보안 요구 사항에 따라 Axis 장치에는 TPM 2.0(Trusted Platform Module)이나 보안 요소 및/또는 하드웨어를 제공하는 TEE(Trusted Execution Environment)와 같은 하드웨어 기반 암호화 컴퓨팅 모듈이 하나 또는 여러 개 있을 수 있으며, 이는 하드웨어로 보호되는 보안 키 저장소를 제공합니다. 또한 일부 Axis 제품에는 FIPS 140-2 레벨 2 인증 보안 키 저장소가 있습니다.

Axis device ID

장치의 출처를 확인할 수 있는 것은 장치 ID에 대한 신뢰를 구축하는 데 핵심적인 것입니다. 생산 과정에서 Axis Edge Vault가 설치된 장치에는 공장에서 프로비저닝된 고유하고 IEEE 802.1AR을 준수하는 Axis 장치 ID 인증서가 할당됩니다. 이는 장치의 출처를 증명하는 여권과 같은 역할을 합니다. 장치 ID는 Axis 루트 인증서로 서명된 인증서로 보안 키 저장소에 안전하고 영구적으로 저장됩니다. 자동화된 보안 장치 온보딩 및 보안 장치 식별을 위해 고객의 IT 인프라에서 장치 ID를 활용할 수 있습니다.

Signed Video

Signed Video는 비디오 파일의 보관 연속성을 증명하지 않고도 비디오 증거가 변조되지 않은 것으로 검증될 수 있도록 합니다. 각 카메라는 보안 키 저장소에 안전하게 저장된 고유한 비디오 서명 키를 사용하여 비디오 스트림에 서명을 추가합니다. 비디오가 재생될 때 파일 플레이어는 비디오의 손상 여

부를 표시합니다. Signed Video를 통해 비디오의 원본 촬영 카메라를 추적하고 비디오가 카메라를 떠난 후 변조되지 않았는지 확인할 수 있습니다.

암호화된 파일 시스템

보안 키 저장소는 파일 시스템에 강력한 암호화를 적용하여 악의적인 정보 유출을 방지하고 구성 변조를 방지합니다. 이렇게 하면 장치를 사용하지 않거나 장치에 대한 인증되지 않은 액세스가 이루어지거나 Axis 장치를 도난당했을 때 파일 시스템에 저장된 데이터를 추출하거나 탬퍼링할 수 없습니다. Secure Boot 프로세스 중에 읽기-쓰기 파일 시스템이 해독되어 Axis 장치에서 마운트하고 사용할 수 있습니다.

Axis 장치의 사이버 보안 기능에 대해 자세히 알아보려면 *axis.com/learning/white-papers*로 이동하여 사이버 보안을 검색하십시오.

Axis 보안 알림 서비스

Axis는 Axis 장치의 취약성 및 기타 보안 관련 문제에 대한 정보를 제공하는 알림 서비스를 제공합니다. 알림을 받으려면 *axis.com/security-notification-service*에서 구독하면 됩니다.

취약성 관리

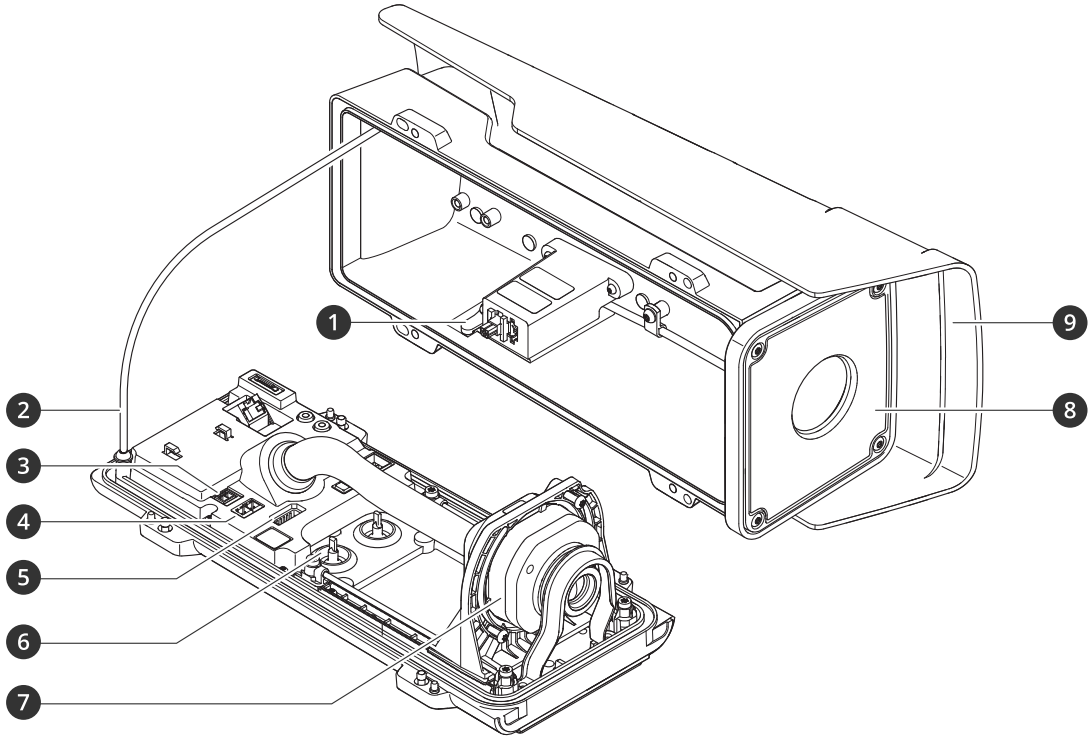
Axis는 고객의 노출 위험을 최소화하기 위해 **CVE(공통 취약성 및 노출) CNA(번호 지정 기관)**로서 업계 표준을 준수하여 장치, 소프트웨어 및 서비스에서 발견된 취약점을 관리하고 이에 대응합니다. Axis 취약성 관리 정책, 취약성을 보고하는 방법, 이미 공개된 취약성 및 해당 보안 권고에 대한 자세한 내용은 *axis.com/vulnerability-management*를 참조하십시오.

Axis 장치의 안전한 작동

공장 출하 시 기본값이 설정된 Axis 장치는 보안 기본 보호 메커니즘으로 사전 구성되어 있습니다. 장치를 설치할 때 더 많은 보안 구성을 사용하는 것이 좋습니다. 모범 사례, 리소스 및 장치 보안을 위한 지침을 포함하여 사이버 보안에 대한 Axis의 접근 방식에 대해 자세히 알아보려면 *axis.com/about-axis/cybersecurity*로 이동하십시오.

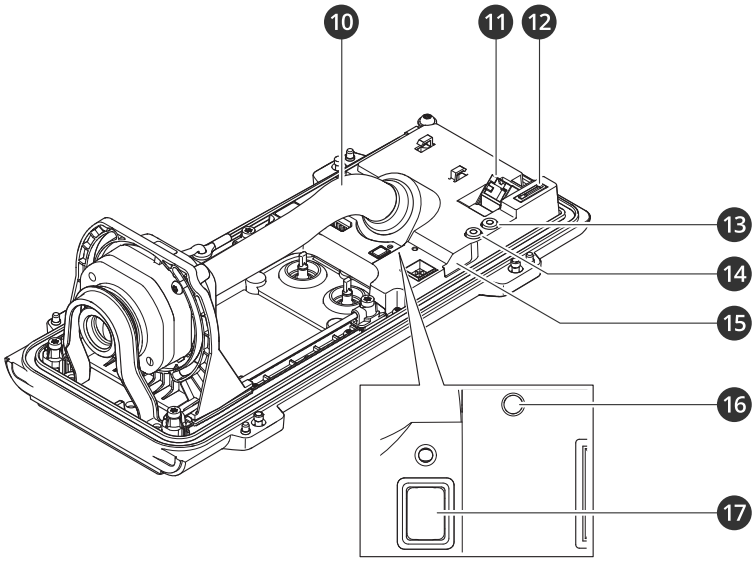
사양

제품 개요



1 *침입 알람 자석*
2 *안전선*
3 *전원 커넥터*
4 *RS485/422 커넥터*
5 *I/O 커넥터*
6 *케이블 개스킷 M20(2개)*
7 *광학 유닛**
8 *전면 창*
9 *기상 보호막*

*광학 장치의 외관은 선택한 렌즈에 따라 달라질 수 있습니다.



1 케이블 커버
2 네트워크 커넥터(PoE)
3 microSD 카드 슬롯
4 오디오 출력
5 오디오 입력
6 침입 알람 센서
7 상태 LED
8 제어 버튼

LED 표시

비고

- 이벤트가 활성 상태인 동안 상태 LED가 깜박이도록 구성할 수 있습니다.
- 케이스를 닫으면 LED가 꺼집니다.

상태 LED	표시
켜져 있지 않음	연결 및 정상 작동
녹색	연결 및 정상 작동
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.

버저

수평 보조 장치에 대한 버저 신호

이미지 수평에 사용되는 제어 버튼에 대한 정보는 *page 26*을 참조하십시오.

버저	카메라 위치
연속 알람음	수평
빠른 알람음	거의 수평
중간 알람음	수평 아님
느린 알람음	수평에서 멀어짐

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.com*을 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 34*을 참조하십시오.
- 카메라가 수평인지 확인합니다. 수평 보조 장치를 시작하려면 2초 정도 버튼을 누르고 멈추려면 다시 누릅니다. 버저 신호(*page 25* 참조)는 카메라의 수평 조정을 지원합니다. 버저 알람음이 지속되면 카메라가 수평 상태입니다.

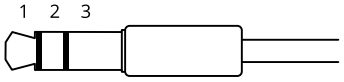
커넥터

네트워크 커넥터

PoE(Power over Ethernet)를 지원하는 RJ45 이더넷 커넥터

오디오 커넥터

- **오디오 입력** – 디지털 마이크, 아날로그 모노 마이크 또는 라인 입력 모노 신호를 위한 3.5mm 입력 단자입니다(왼쪽 채널은 스테레오 신호에 사용됨).
- **오디오 출력** - PA(공용 주소) 시스템 또는 앰프가 내장된 액티브 스피커에 연결할 수 있는 오디오(라인 수준)를 위한 3.5mm 출력 단자입니다. 오디오 출력에는 스테레오 커넥터를 사용해야 합니다.



오디오 입력

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

오디오 출력

1 팁	2 링	3 슬리브
채널 1, 비평형 라인, 모노	채널 1, 비평형 라인, 모노	접지

I/O 커넥터

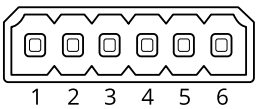
모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 I/O 커넥터를 사용합니다. I/O 커넥터는 0 VDC 기준점 및 전원(12V DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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

관리된 입력 - 디지털 입력에 대한 탬퍼링을 감지할 수 있습니다.

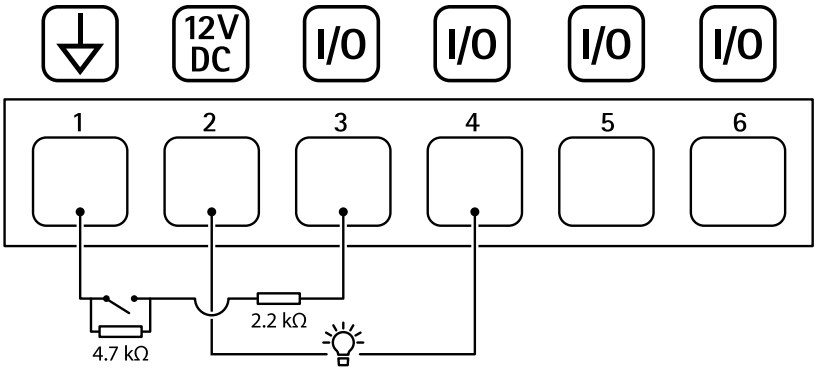
디지털 출력 - 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface로 이벤트를 통해 또는 장치의 웹 인터페이스에서 활성화할 수 있습니다.

6핀 단자대입니다.



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 = 50mA
구성 가능(입력 또는 출력)	3–6	디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 레지스터를 연결하는 방법에 대한 자세한 내용은 연결 다이어그램을 참조하십시오.	0 ~ 최대 30 VDC
		디지털 출력 - 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

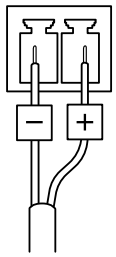
예:



1 DC 접지
2 DC 출력 12V, 최대 50mA
3 I/O가 관리된 입력으로 구성됨
4 I/O가 출력으로 구성됨
5 구성 가능한 I/O
6 구성 가능한 I/O

전원 커넥터

DC 전원 입력용 2핀 단자대입니다. 정격 출력 전력이 ≤100W로 제한되거나 정격 출력 전류가 ≤5A로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.

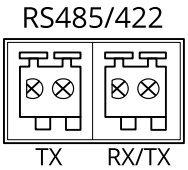


RS485/RS422 커넥터

RS485/RS422 직렬 인터페이스용 2핀 단자대 2개입니다.

다음 항목을 지원하도록 시리얼 포트를 구성할 수 있습니다.

- 2개 와이어 RS485 반이중
- 4개 와이어 RS485 전이중
- 2개 와이어 RS422 단방향
- 4개 와이어 RS422 전이중 지점 간 통신



기능	비고
RS485/RS422 TX(A)	RS422 및 4개 와이어 RS485에 대한 TX 쌍
RS485/RS422 TX(B)	
RS485A alt RS485/422 RX(A)	모든 모드에 대한 RX 쌍(2개 와이어 RS485에 대해 결합된 RX/TX)

RS485B alt RS485/422 RX(B)	

비고

AXIS T99 Positioning Unit과 함께 카메라를 사용하려면 RS485A 및 RS485B(RX/TX)에 연결하십시오.

PTZ 드라이버

APTP

이 드라이버가 지원하는 모델 목록입니다. 물리적 설치는 Axis 제품과 PTZ 장치에 따라 다릅니다.

중요 사항

Axis 제품과 PTZ 장치가 지원하는 직렬 통신을 확인하십시오.

RS485 2선 인터페이스가 있는 지원 모델:

- AXIS T99A Positioning Unit Series.
  호환 가능 Axis 제품에 대한 자세한 내용은 *axis.com*을 참조하십시오.

다른 모델이 지원될 수 있지만, 이것은 Axis에서 확인되지 않았습니다.

기술 정보

PTZ 드라이버의 기본 기능:

드라이버	APTP
버전	1.1.0

기본 직렬 구성:

포트 모드	RS485
보 레이트	115,200
데이터 비트	8
스톱 비트	1
패리티:	없음

이 PTZ 드라이버에서 기본 지원 기능:

비고

다른 PTZ 장치에는 다른 기능이 있을 수 있습니다(더 적거나 더 많음).

움직임	최대	상대	지속
팬	예	예	예
틸트	예	예	예

Pelco

이 드라이버가 지원하는 모델 목록입니다. 물리적 설치는 Axis 제품과 PTZ 장치에 따라 다릅니다.

중요 사항

Axis 제품과 PTZ 장치가 지원하는 직렬 통신을 확인하십시오.

지원 모델:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

다른 모델이 지원될 수 있지만, 이것은 Axis에서 확인되지 않았습니다.

기술 정보

PTZ 드라이버의 기본 기능:

드라이버	Pelco
버전	4.17

기본 직렬 구성:

포트 모드	RS485
보 레이트	2,400
데이터 비트	8
스톱 비트	1
패리티:	없음

이 PTZ 드라이버에서 기본 지원 기능:

비고

다른 PTZ 장치에는 다른 기능이 있을 수 있습니다(더 적거나 더 많음).

움직임	최대	상대	지속
팬	아니요	예	예
틸트	아니요	예	예
줌	아니요	예	예
포커스	아니요	예	예
홍채	아니요	예	예

오토 아이리스	예
오토 포커스	예
적외선 차단 필터	아니요

역광	예
OSD 메뉴	예

Visca

이 드라이버가 지원하는 모델 목록입니다. 물리적 설치는 Axis 제품과 PTZ 장치에 따라 다릅니다.

중요 사항

Axis 제품과 PTZ 장치가 지원하는 직렬 통신을 확인하십시오.

RS422 4선 인터페이스가 있는 지원 모델:

- Sony EVI-D70/D70P
- WISKA DCP-27(PT-헤드)

RS232 인터페이스가 있는 지원 모델(외부 RS422-4-와이어/RS232 변환기가 필요할 수 있음):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

다른 모델이 지원될 수 있지만, 이것은 Axis에서 확인되지 않았습니다.

기술 정보

PTZ 드라이버의 기본 기능:

드라이버	Visca/EVI
버전	4.11

기본 직렬 구성:

포트 모드	RS422
보 레이트	9,600
데이터 비트	8
스톱 비트	1
패리티:	없음

이 PTZ 드라이버에서 기본 지원 기능:

비고

다른 PTZ 장치에는 다른 기능이 있을 수 있습니다(더 적거나 더 많음).

움직임	최대	상대	지속
팬	예	예	예
틸트	예	예	예
줌	예	예	예

움직임	최대	상대	지속
포커스	예	예	예
홍채	예	예	아니요

오토 아이리스	예
오토 포커스	예
적외선 차단 필터	예
역광	예
OSD 메뉴	아니요

장치 세척

미지근한 물과 순한 비연마성 비누로 장치를 세척하면 됩니다.

통지

- 자극적인 화학 물질로 인해 장치가 손상될 수 있습니다. 창문 세정제나 아세톤과 같은 화학 물질을 사용하여 장치를 세척하지 마십시오.
- 장치에 직접 세제를 분사하면 안 됩니다. 대신 비마모성 천에 세제를 뿌려 장치 세척에 사용합니다.
- 직사광선이나 고온에서 세척하면 얼룩이 생길 수 있으므로 주의해서 피해야 합니다.

1. 압축된 공기통을 사용하여 장치에서 먼지와 느슨한 오물을 제거하십시오.
2. 필요한 경우 미지근한 물과 순한 비마모성 비누로 적신 부드러운 극세사 천으로 장치를 닦으십시오.
3. 얼룩이 생기지 않도록 깨끗한 비마모성 천으로 장치를 건조시키십시오.

문제 해결

공장 출하 시 기본 설정으로 재설정

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.

제품을 공장 출하 시 기본 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끊습니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 개요, on page 24*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. 네트워크에서 DHCP 서버를 이용할 수 없는 경우, 장치의 IP 주소는 다음 중 하나로 기본 설정됩니다.
   - **AXIS OS 12.0 이상이 설치된 장치:** 링크-로컬 주소 서브넷(169.254.0.0/16)에서 가져온 주소
   - **AXIS OS 11.11 이하가 설치된 장치:** 192.168.0.90/24
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 장치에 액세스합니다.
   설치 및 관리 소프트웨어 도구는 *axis.com/support*의 지원 페이지에서 제공됩니다.

또한 장치의 웹 인터페이스를 통해 매개변수를 공장 출하 시 기본값으로 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-software*를 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 Portal: Upgrade path*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-software*로 이동합니다.

1. *axis.com/support/device-software*에서 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 있는AXIS 장치 관리자는 동시에 여러 장치를 업그레이드합니다. *axis.com/products/axis-device-manager*에서 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, `ping`을 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 out`을 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 `https`를 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 34* 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/support*로 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 6*에서 확인하십시오.

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 다운로드는 *axis.com/vms*로 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 랜더링 불량

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

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.

장치 작동 문제

전면 히터 및 와이퍼가 작동하지 않음

전면 히터나 와이퍼가 켜지지 않을 경우 상단 커버가 하우징 유닛 하단에 제대로 고정되었는지 확인하십시오.

찾는 내용이 여기에 없는 경우에는 *axis.com/support*에서 문제 해결 섹션을 확인해 보십시오.

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 과다한 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.
- 팔레트를 사용하면 제품의 CPU 로드에 영향을 미치므로 결국 프레임 레이트에 영향을 주게 됩니다.

지원 센터 문의

추가 도움이 필요하면 *axis.com/support*로 이동하십시오.

T10208523_ko

2026-02 (M7.2)