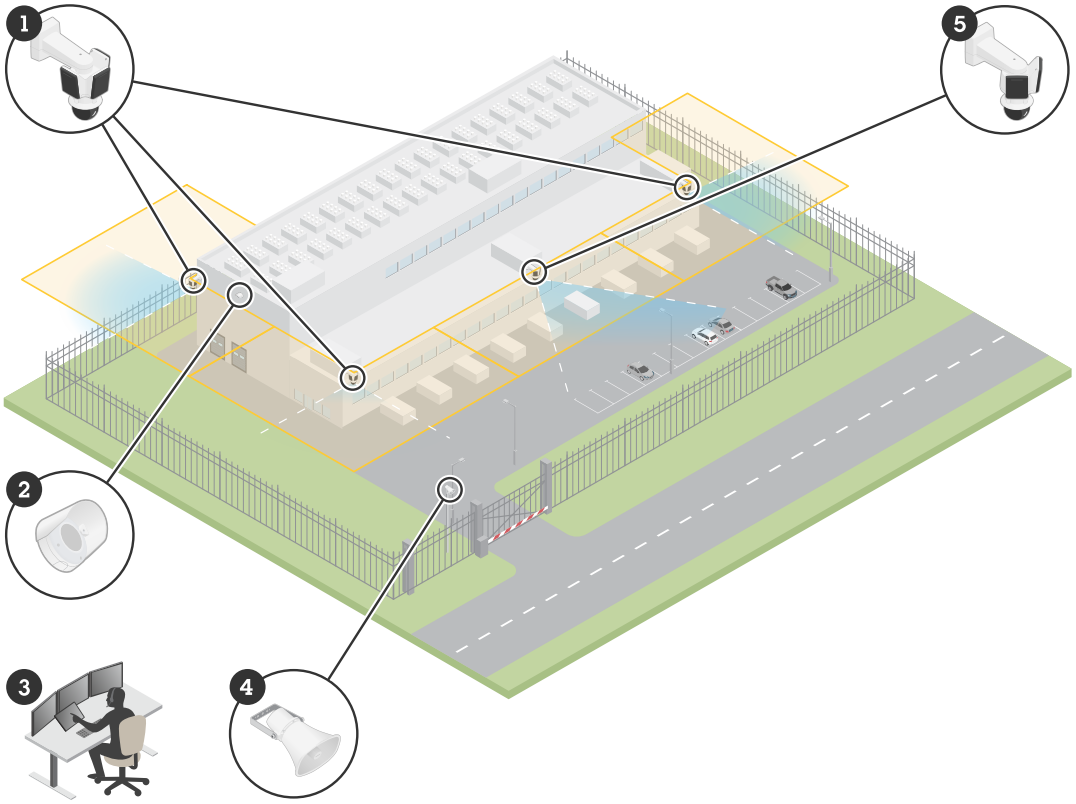
AXIS D21-VE Radar Series

AXIS D2122-VE Radar
AXIS D2123-VE Radar

사용자 설명서

목차

솔루션 개요



데이터 센터의 감시 솔루션 예시.

1 *AXIS Q6358-LE PTZ Camera와 페어링된 AXIS D2123–VE Radar*
2 *AXIS D4200-VE 스트로브 스피커*
3 *감시 센터*
4 *AXIS C1310-E 혼 스피커*
5 *AXIS Q6358-LE PTZ Camera와 페어링된 AXIS D2122–VE Radar*

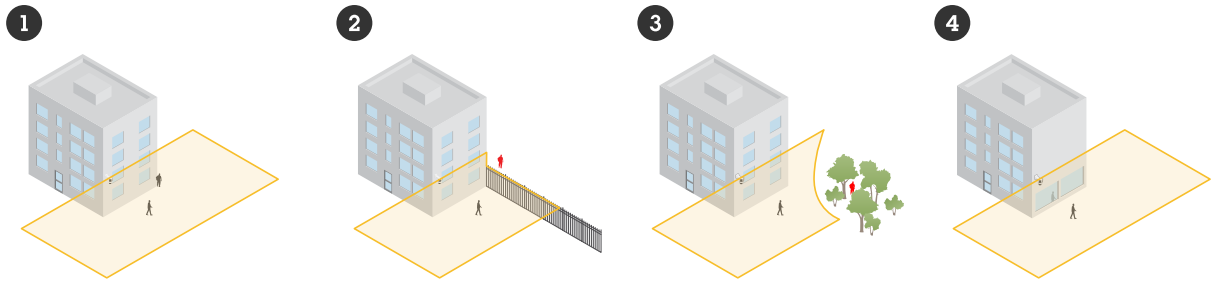
설치

이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

이 비디오는 AXIS D21-VE 레이더 시리즈 설치 방법의 예를 보여줍니다. 모든 설치 시나리오에 대한 지침 및 안전 정보는 설치 가이드를 참조하십시오.

고려 사항

- 레이더는 개방된 영역을 모니터링하도록 설계되었습니다(1). 장면 내 벽, 울타리, 나무 또는 큰 덤불과 같은 고체 객체는 그 뒤에 이른바 레이더 그림자(사각지대)를 생성합니다(2, 3). 장착 높이는 레이더 그림자의 크기에 영향을 미칩니다.
- 예를 들어 반사 표면이 존재하는 등 더 복잡한 장면의 경우, 선택된 PTZ 카메라와 함께 레이더-비디오 융합 기술을 권장합니다.
- 레이더는 지면이 아스팔트와 같은 포장 표면으로 덮여 있을 때 가장 잘 작동합니다. 지면이 자갈이나 잔디로 덮여 있으면 감지 성능이 영향을 받을 수 있습니다.
- 레이더를 벽에 설치하는 경우, 레이더 좌우 1m(3ft) 이내에 다른 객체나 설치물이 없도록 합니다. 이러한 객체는 전파를 반사할 수 있으며, 이는 레이더의 성능에 영향을 미칠 수 있습니다.
- 레이더를 기둥에 설치하는 경우, 기둥이 안정적인지 확인합니다. 레이더에는 활성화할 수 있는 안정화 메커니즘이 있지만, 이는 레이더 감도 또는 움직이는 객체를 감지하는 데 걸리는 시간에 영향을 미칠 수 있습니다.
- 장면 내 금속 객체 또는 반사 표면은 그 근처를 이동하는 사람이나 차량을 반사하여 반사된 레이더 트랙 또는 고스트 트랙(4)을 발생시킬 수 있습니다. 이는 레이더의 정확한 분류 수행 능력에 영향을 미쳐 거짓 경보를 유발할 수 있습니다. 제외 구역을 사용하여 이러한 반사를 걸러낼 수 있습니다. 카메라를 레이더와 페어링하면 반사의 영향을 최소화할 수도 있습니다.
- 권장 장착 높이는 *axis.com*의 장치 데이터시트에 나와 있습니다.

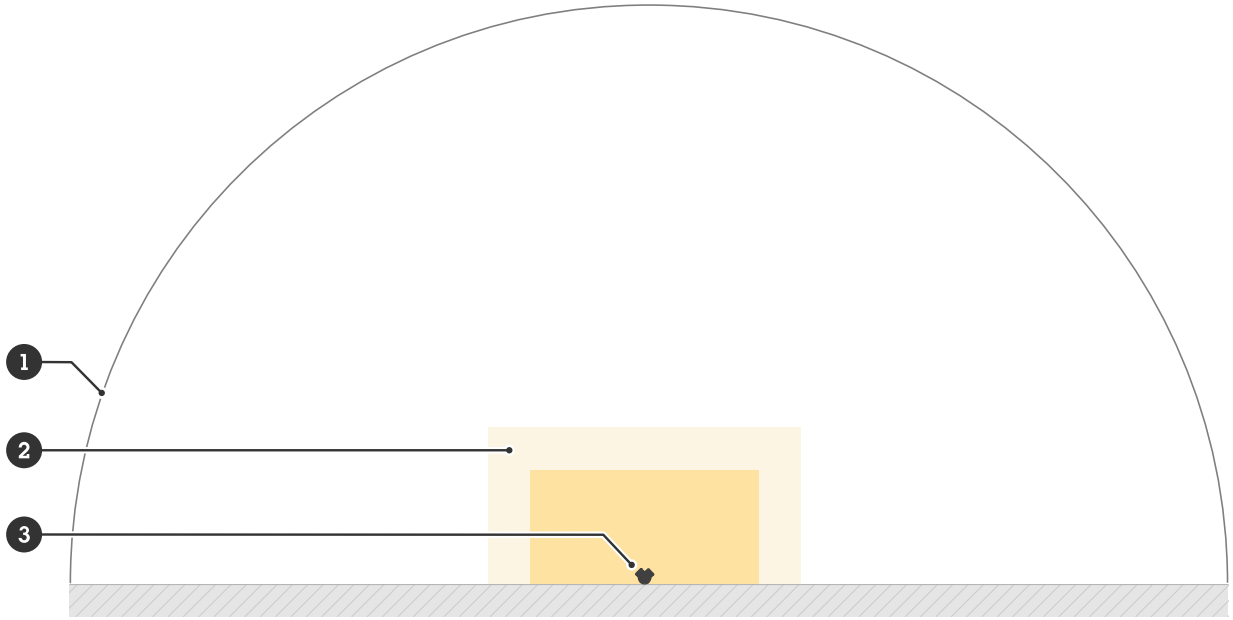


장면 모니터링

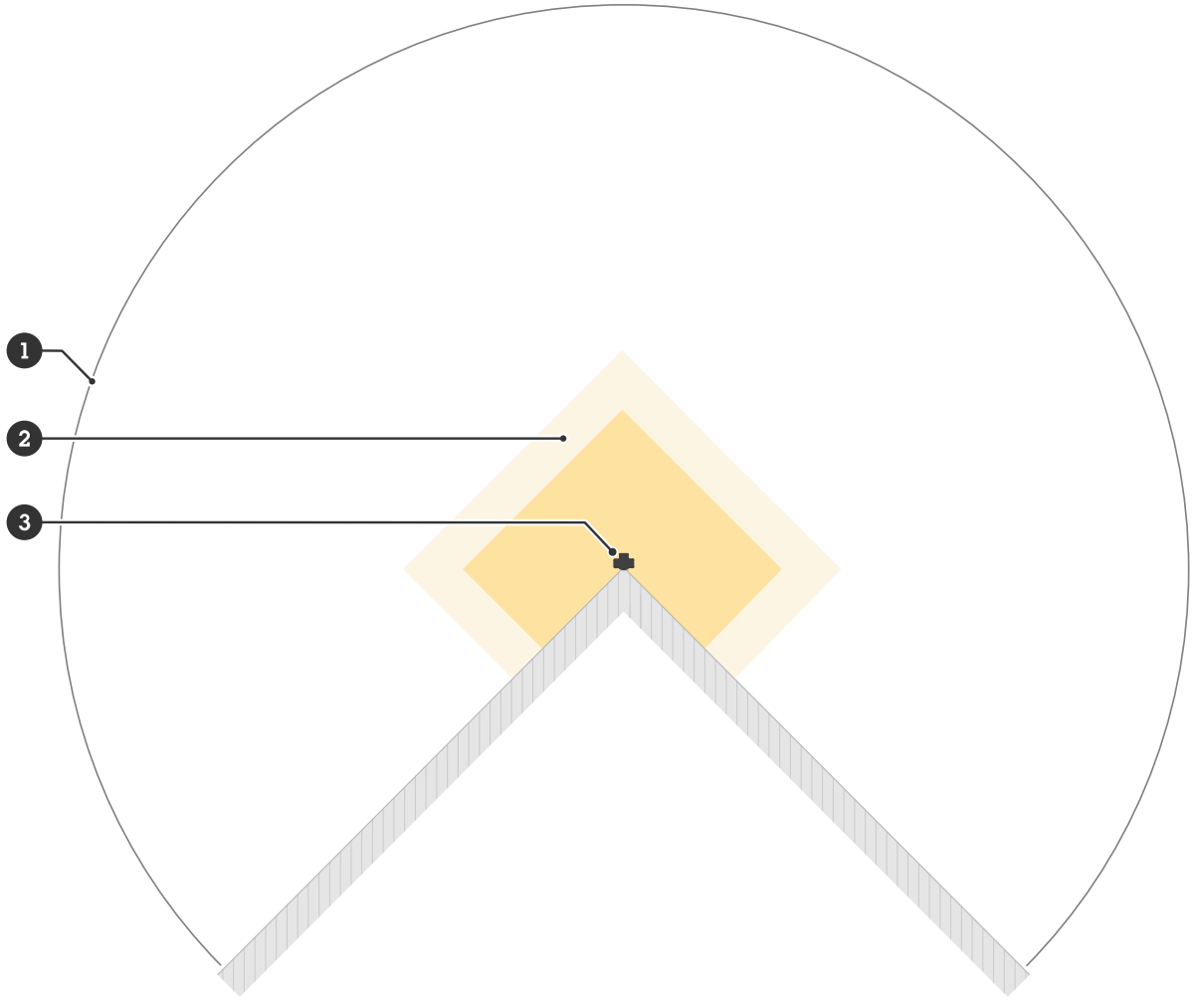
레이더는 움직이는 객체를 감지하고 이를 사람, 차량 또는 미확인으로 분류할 수 있습니다. 영역을 모니터링할 때는 **Area monitoring(영역 모니터링)** 프로파일을 사용합니다.

여러 레이더 설치

건물 주변이나 울타리 바깥의 버퍼 구역과 같은 영역을 모니터링하려면 여러 대의 레이더를 서로 가깝게 설치할 수 있습니다. 각 레이더는 공존 구역을 형성하는 반경 500m(1640ft) 내에서 최대 11대의 다른 AXIS D2122-VE 또는 AXIS D2123-VE 레이더와 공존할 수 있습니다. 이 레이더 모델은 기존 Axis 레이더 모델과 서로 간섭하지 않으므로 기존 Axis 레이더 모델의 공존 구역에도 설치할 수 있습니다. 공존 구역에 대한 자세한 내용은 *공존 구역, on page 71*을 참조하십시오.



1 공존 구역
2 감지 영역
3 Axis D2122–VE Radar



1 공존 구역

2 감지 영역
3 Axis D2123–VE Radar

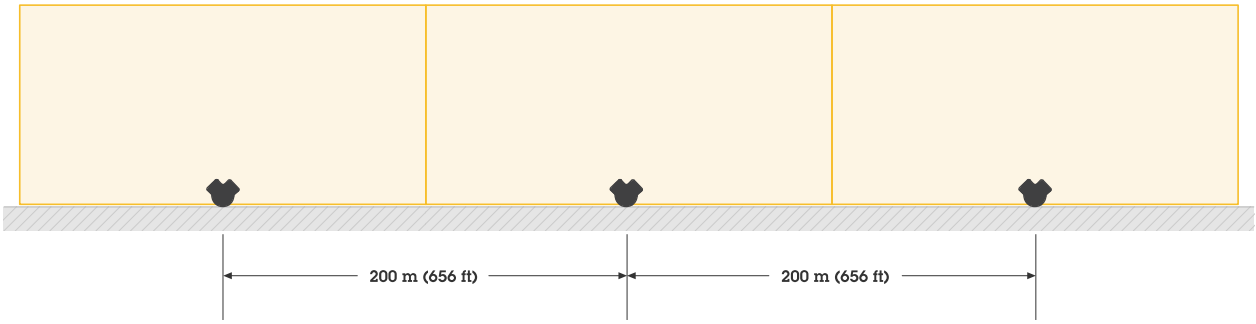
비고

공존 구역에서 레이더의 성능은 환경과 울타리, 건물 또는 인접 레이더를 향한 레이더의 방향에 의해 영향을 받을 수 있습니다.

설치 예

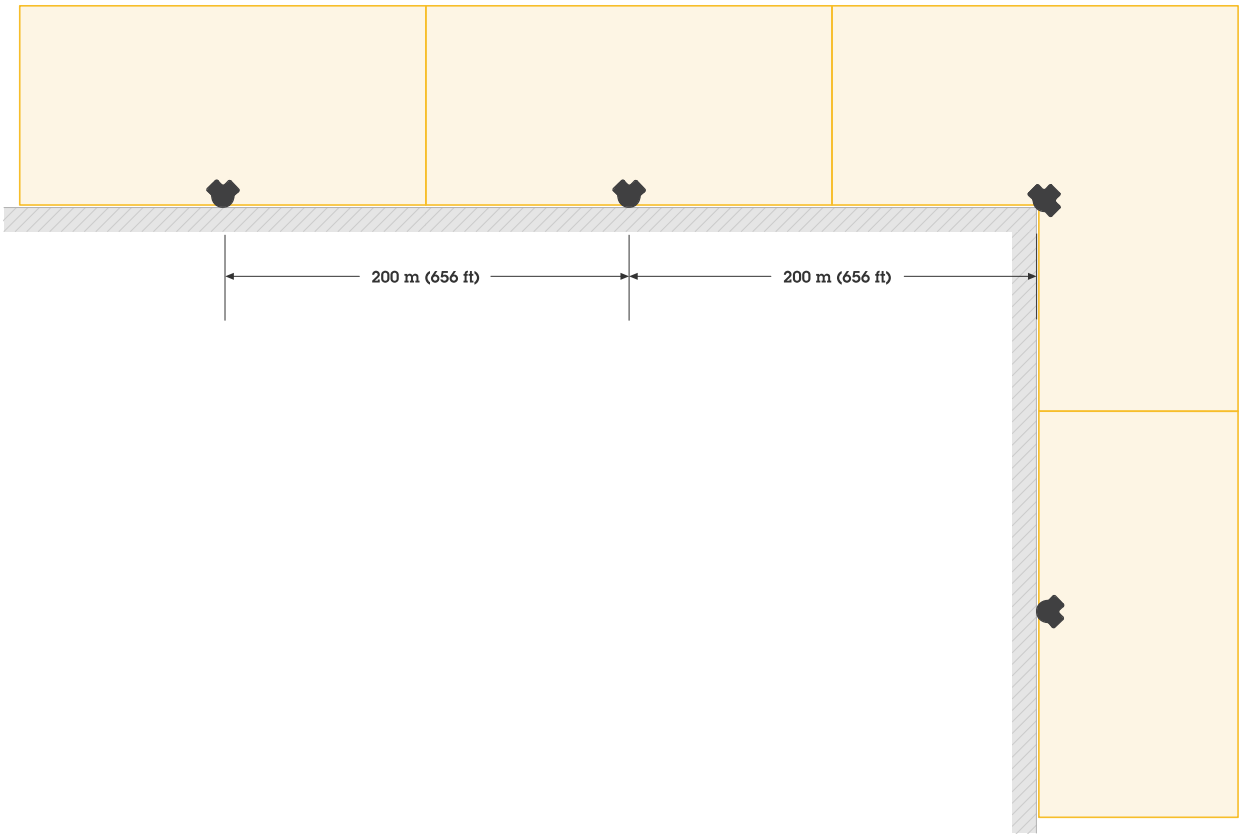
여러 레이더로 가상 펜스 생성

예를 들어 건물을 따라 가상 울타리를 만들려면 여러 대의 레이더를 나란히 배치합니다. 레이더 간 간격은 200m(656ft)로 배치할 것을 권장합니다.



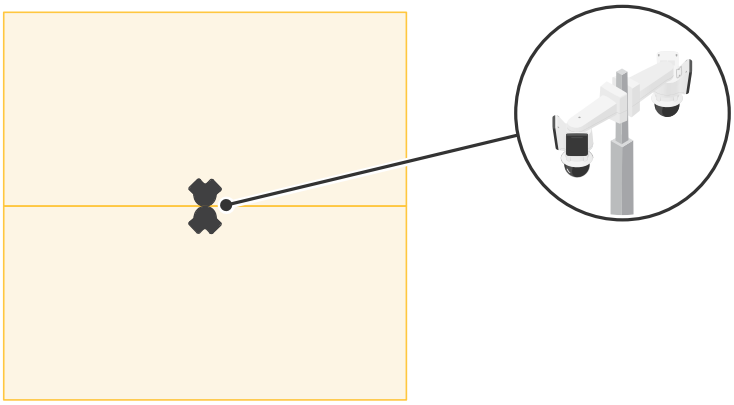
건물 주변 영역 커버

건물 주변 영역을 모니터링하려면 건물 벽면에 레이더를 바깥쪽을 향하도록 설치합니다.



오픈 영역을 커버

넓은 개방 영역을 모니터링하려면 폴 마운트 2개를 사용하여 AXIS D2122-VE Radar 2대를 등지고 반대 방향으로 설치합니다.

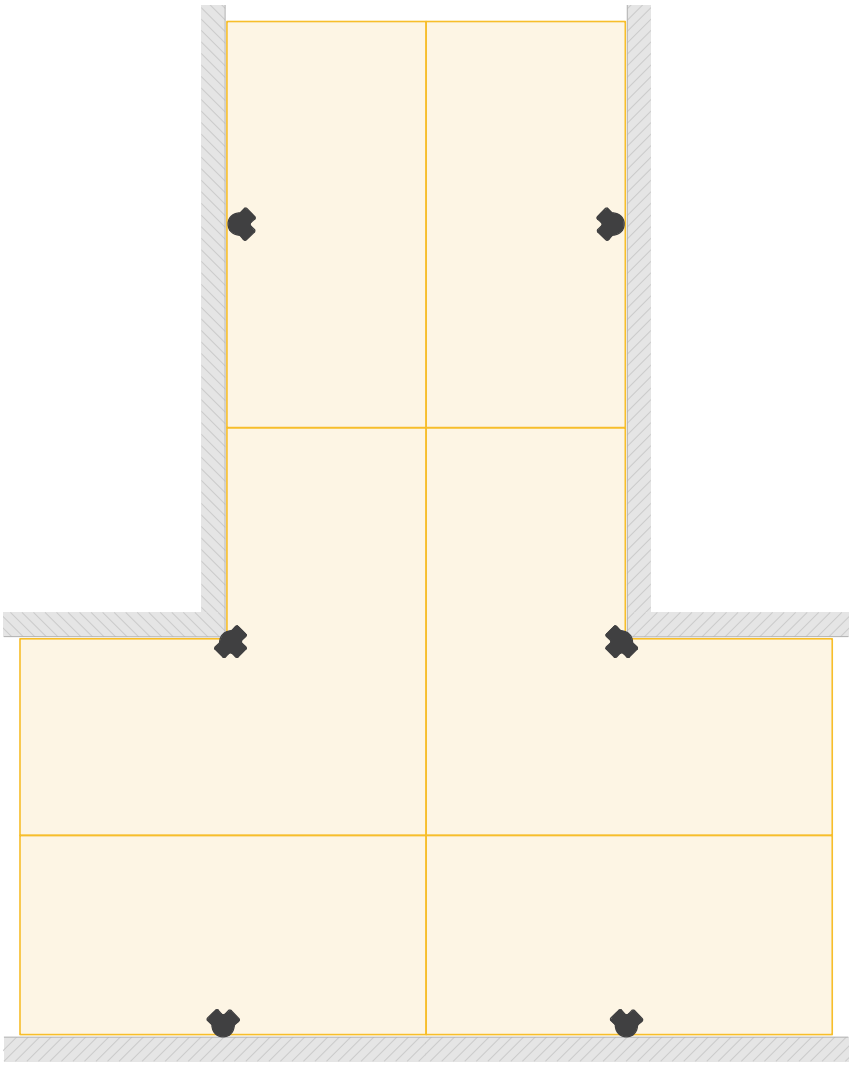


비고

각 레이더는 90W 미드스팬으로 전원이 공급될 때 최대 60W의 PoE 출력을 제공할 수 있습니다. PoE 출력에는 PoE(Power over Ethernet) IEEE 802.3bt, Type 4 Class 8이 필요합니다.

서로 마주보는 다수의 레이더 설치

예를 들어 건물 사이 영역을 모니터링하려면 레이더를 서로 마주보게 배치합니다. 동일한 공존 구역 내에서 서로 마주보는 레이더는 최대 12대까지 있을 수 있습니다.

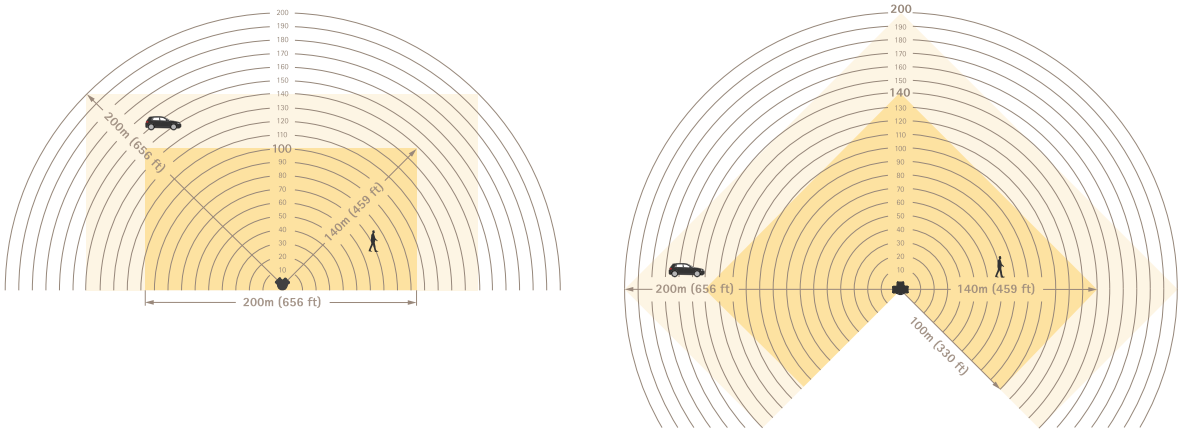


인식 및 감지 거리

레이더를 최적의 설치 높이에 마운트한 경우:

- 인식 구역에서는 레이더에 대한 사람의 위치에 따라 레이더로부터 최대 100~140m (330~459ft) 거리에서 사람을 감지하고 분류할 수 있습니다.
- 감지 구역에서는 다음 요소에 따라 레이더로부터 최대 140~200m(459~656ft) 거리에서 차량을 감지할 수 있습니다.
  - 차량 속도
  - 레이더에 대한 차량의 진행 방향
  - 지면의 평탄도
  - 지면 재질

구역에 대한 자세한 내용은 *인식 및 감지 구역, on page 71*을 참조하십시오.



인식 및 감지 거리

비고

- 레이더를 보정할 때 장치의 웹 인터페이스에 실제 장착 높이를 입력합니다.
- 인식 및 감지 거리는 장면에 따라 달라집니다.
- 인식 및 감지 거리는 객체 유형에 따라 다릅니다.

인식 및 감지 거리는 다음과 같은 조건에서 측정되었습니다.

- 거리는 평평하고 수평인 지면에서 측정되었습니다.
- 레이더는 기울지 않게 마운트되었습니다.
- 객체는 키가 170cm(5ft 7in)인 사람이었습니다.
- 레이더에서 사람까지 시야가 명확하게 확보되어 있었습니다.
- 레이더 감도는 **Medium(중간)**으로 설정되었습니다.

레이더는 최소 감지 거리보다 가까운 객체를 감지할 수 없습니다. 최소 감지 거리는 레이더의 장착 높이에 따라 달라집니다.

장착 높이	최소 감지 거리
4m (9.8ft)	4m (9.8ft)
5m (16.4ft)	6m (19.7ft)
6m (19.7ft)	8m (26ft)
7m (23ft)	11m (36ft)
8m (26ft)	13m (42.7ft)
9m (29.5ft)	15m (49.2ft)
10m (32.85ft)	18m (59ft)

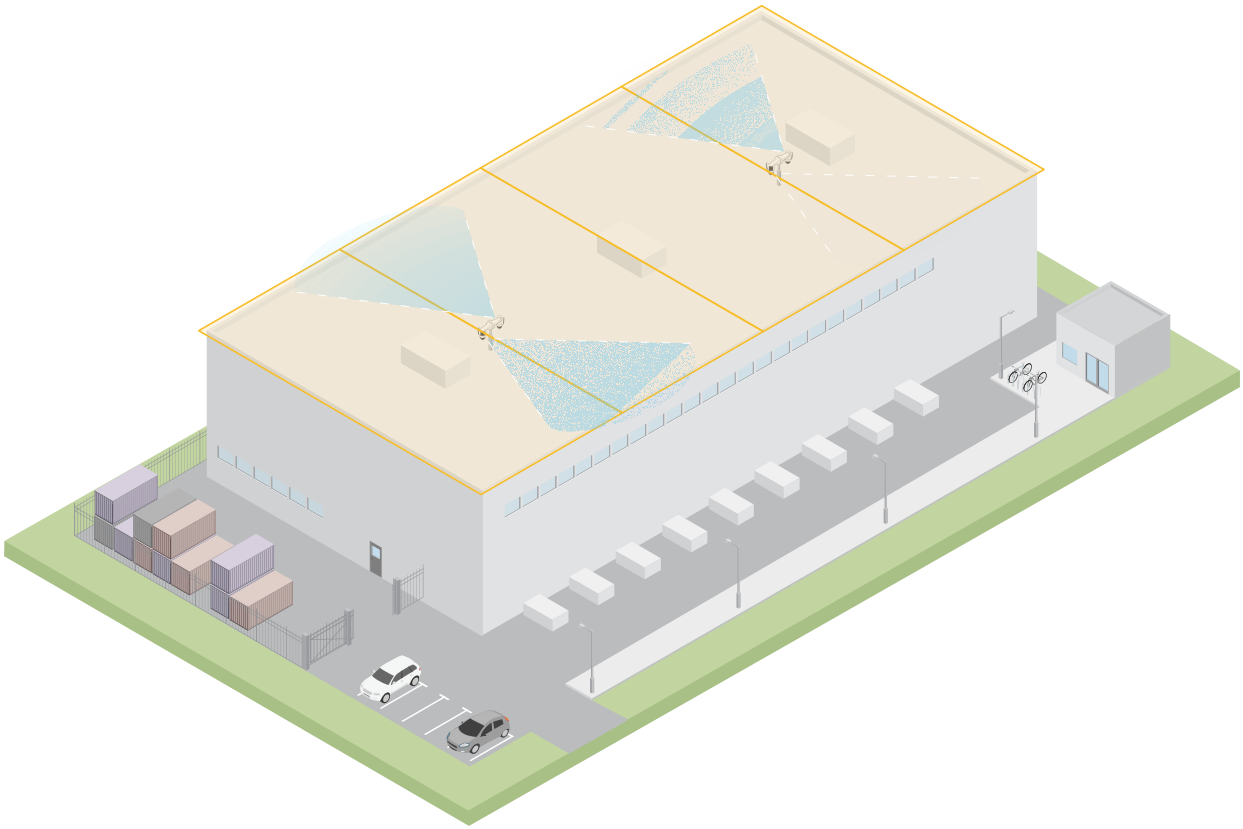
비고

레이더를 PTZ 카메라와 페어링하면, 카메라가 레이더의 최소 감지 거리 내에서도 객체를 계속 추적할 수 있습니다.

사용 사례

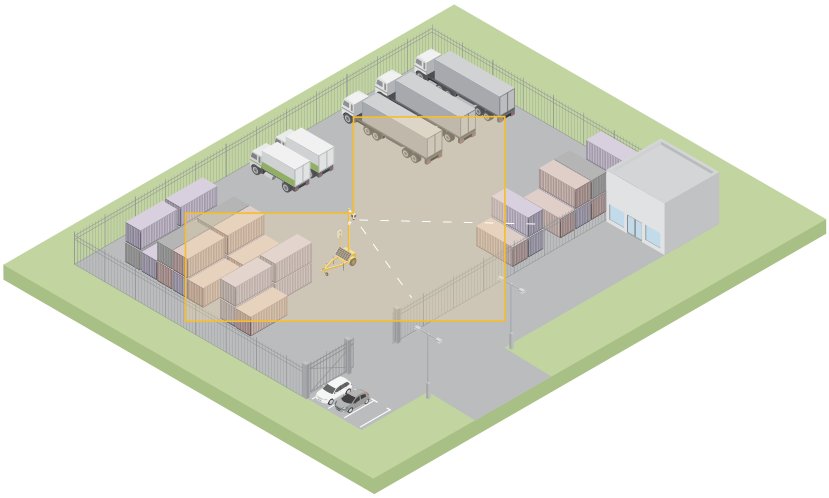
옥상 영역 커버리지

대형 유통 센터가 옥상 영역을 커버하기 위해 레이더를 사용하려고 합니다. 레이더는 ARTPEC-9 PTZ 카메라와 페어링되어 기둥에 등지고 반대 방향으로 마운트되며 옥상 전체를 커버합니다. 레이더가 옥상 위의 움직이는 객체를 발견하고 분류하며, 카메라를 해당 객체로 향하게 하고 카메라가 분류 결과를 검증하도록 합니다. 카메라는 오토트래킹을 사용하여 객체를 계속 추적합니다.



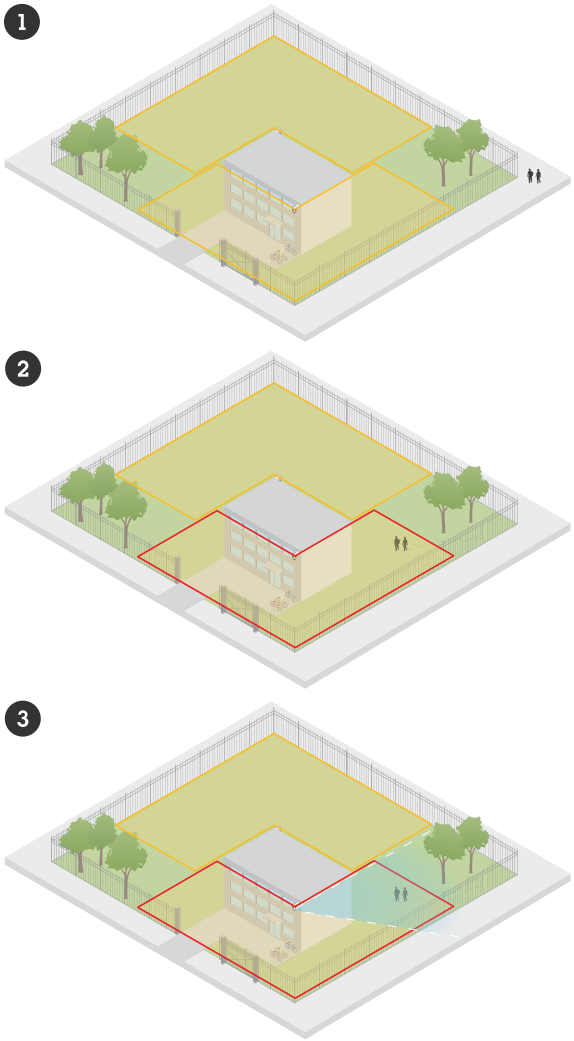
모바일 감시 트레일러로 넓은 개방 영역 커버

하드웨어 매장의 야외 마당에서 영업 종료 후 여러 차례 침입이 발생했습니다. 한 번에 한 명의 경비원이 근무하지만, 추가 인력 고용 비용 없이 야간 보안을 강화해야 합니다. 해당 매장은 전체 마당을 커버하기 위해 모바일 감시 트레일러에 레이더 2대를 등지고 반대 방향으로 마운트하여 설치하기로 결정했습니다. 레이더는 근무 중인 경비원에게 의심스러운 행동을 알리도록 구성되어 경비원이 현장을 확인할 수 있습니다. 또한 침입자를 억제하기 위해 레이더가 트리거하는 스트로브 스피커 설치를 고려합니다.



울타리가 있는 건물 포함

다음 시나리오에서는 알람을 검증하고 레이더-비디오 융합 기술로 정확한 분류를 제공하기 위해 PTZ 카메라가 레이더와 함께 마운트되었습니다.



1. 침입자가 울타리 밖을 걷고 있지만 알람이 트리거되지 않습니다.
2. 침입자가 울타리를 뚫고 침입하면 레이더가 이를 발견하고 알람을 트리거합니다.
3. 레이더가 PTZ 카메라를 침입자 쪽으로 향하게 하고, 카메라가 비디오 분석으로 알람을 검증하도록 합니다.

자세한 내용은 *오토트래킹, on page 72*를 참조하십시오.

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 14*을 참조하십시오.

*웹 인터페이스, on page 23*에서 장치의 웹 인터페이스에서 볼 수 있는 모든 컨트롤과 옵션에 대한 설명을 살펴보십시오.

관리자 계정 생성

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 사용자 이름을 입력하십시오.
2. 패스워드를 입력합니다. *안전한 패스워드, on page 15*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 79*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.

장치 구성

장치를 최대한 활용하려면 다음 단계를 수행할 것을 권장합니다.

1. *장착 높이 설정, on page 16*
2. 여러 대의 레이더를 서로 가깝게 설치하는 경우: *인접 레이더 수 설정, on page 16*
3. *참조용 지도 추가, on page 16*
4. *객체 감지 시나리오 생성, on page 17*
5. *허위 알람을 최소화하는 방법, on page 18*
6. *설치 확인, on page 19*

장착 높이 설정

웹 인터페이스에서 레이더의 장착 높이를 설정합니다. 올바른 장착 높이는 레이더가 지나가는 객체의 속도를 정확히 감지하고 측정할 수 있도록 하는 데 중요합니다. 오토트래킹이 작동하는 데도 매우 중요합니다.

지면에서 레이더까지의 높이를 최대한 정확하게 측정합니다. 표면이 고르지 않은 장면의 경우 장면의 평균 높이를 나타내는 값을 설정합니다.

1. **Radar > Settings > General(레이더 > 설정 > 일반)**로 이동합니다.
2. **Mounting height(장착 높이)**에서 높이를 설정합니다.

인접 레이더 수 설정

이 레이더의 공존 구역에 동일 모델의 다른 레이더를 설치하는 경우, 각 레이더의 웹 인터페이스에서 인접 레이더 수를 지정합니다. 이는 레이더 성능을 향상시키고 간섭 위험을 최소화합니다.

1. **Radar > Settings > Coexistence(레이더 > 설정 > 공존)**로 이동합니다.
2. 이 레이더의 공존 구역 내 인접 레이더 수를 선택합니다.

참조용 지도 추가

시나리오 설정을 더 쉽게 하고 장면 내에서 객체가 이동하는 위치를 이해하기 위해, 레이더 스트림의 배경으로 지도를 사용할 수 있습니다. 레이더가 커버하는 영역을 보여주는 평면도나 항공사진을 사용할 수 있습니다. 레이더 보기가 지도의 위치, 방향 및 축척에 맞도록 지도를 조정하고 보정합니다. 장면의 특정 부분이 관심 대상이면 지도에서 줌인합니다.

지도 보정을 단계별로 안내하는 설정 마법사를 사용하거나, 각 설정을 개별적으로 편집할 수 있습니다.

설정 도우미 사용:

1. **Radar > Map calibration(레이더 > 지도 보정)**으로 이동합니다.
2. **Setup assistant(설정 도우미)**를 클릭하고 지침을 따릅니다.

업로드한 지도와 추가한 설정을 제거하려면 **Reset calibration(보정 재설정)**을 클릭합니다.

각 설정을 개별적으로 편집:
각 설정을 조정한 후 지도가 점진적으로 보정됩니다.

1. **Radar(레이더) > Map calibration(지도 보정) > Map(지도)**으로 이동합니다.
2. 업로드할 이미지를 선택하거나 지정된 영역에 끌어다 놓습니다.
   현재 팬 및 줌 설정으로 지도 이미지를 재사용하려면 **Download map(지도 다운로드)**을 클릭합니다.
3. **Rotate map(지도 회전)**에서 슬라이더를 사용하여 지도를 원하는 위치로 회전합니다.
4. **Scale and distance on a map(지도의 축척 및 거리)**으로 이동하여 지도에서 미리 지정한 두 지점을 클릭합니다.

5. **Distance(거리)**에서 지도에 추가한 두 지점 사이의 실제 거리를 추가합니다.
6. **Pan and zoom map(지도 이동 및 확대/축소)**으로 이동하여 버튼을 사용하여 지도 이미지를 이동하거나 지도 이미지를 확대 및 축소합니다.

비고

- 줌 기능은 레이더의 보기를 변경하지 않습니다. 확대 후 보기의 일부가 보이지 않더라도, 레이더는 전체 보기에서 움직이는 객체를 계속 감지합니다. 감지된 움직임을 배제하는 유일한 방법은 제외 구역을 추가하는 것입니다.
- **Map calibration(지도 보정)**, **Exclusion zones(제외 구역)** 또는 **Scenarios(시나리오)** 페이지에서 을 클릭하여 언제든지 팬 및 줌을 조정할 수 있습니다.

7. **Radar position(레이더 위치)**으로 이동하여 버튼을 사용하여 지도에서 레이더의 위치를 이동하거나 회전합니다.

업로드한 지도와 추가한 설정을 제거하려면 **Reset calibration(보정 재설정)**을 클릭합니다.

이 비디오는 Axis 레이더 또는 레이더-비디오 융합 카메라에서 기준 지도를 보정하는 방법의 예를 보여줍니다.

객체 감지 시나리오 생성

시나리오를 사용하면 장면 내에서 움직이는 객체를 감지하거나 인식할 수 있습니다. 시나리오의 조건이 충족될 때 동작을 트리거하려면 **Events(이벤트)**에서 룰을 생성합니다. 여러 시나리오를 생성하여 서로 다른 동작을 감지하거나 장면의 서로 다른 부분을 커버할 수 있습니다.

1. **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
2. **Add scenario(시나리오 추가)**를 클릭합니다.
3. 시나리오 이름을 입력하십시오.
4. 영역 내에서 이동하는 객체에서 트리거할지, 선을 가로지르는 객체에서 트리거할지 선택합니다.
5. **Next (다음)**를 클릭합니다.
6. **Movement in area(영역 내 이동)** 시나리오의 경우:
   6.1. 구역 형태를 선택합니다.
   마우스를 사용하여 구역을 이동하고 조정하여 레이더 보기 또는 참조 지도의 원하는 부분을 커버합니다.
7. **Line crossing(선 넘기)** 시나리오의 경우:
   7.1. 장면에 라인을 배치합니다.
   마우스를 사용하여 선을 이동하고 조정합니다.
   7.2. 감지 방향을 변경하려면 **Change direction(방향 전환)**을 켭니다.
   7.3. 객체가 두 개의 선을 교차해야 동작이 트리거되도록 하려면 **Require crossing of two lines(두 개의 선 교차 필요)**를 켭니다.
   장면에 두 번째 선을 배치합니다.
8. **Next (다음)**를 클릭합니다.
9. 감지 설정을 추가합니다.
   9.1. **Movement in area(영역 내 이동)** 시나리오 및 선 1개가 있는 **Line crossing(선 넘기)** 시나리오의 경우, **Ignore short-lived objects(짧게 나타나는 객체 무시)**에서 지연 시간을 추가하여 거짓 경보를 최소화합니다.

9.2. 선 2개가 있는 **Line crossing(선 넘기)** 시나리오의 경우, **Max time between crossings (교차 간 최대 시간)**에서 첫 번째 선과 두 번째 선 사이를 교차하는 시간 제한을 설정합니다.

9.3. **Trigger on object type(객체 유형에 대한 트리거)** 아래에서 트리거할 객체 유형을 선택합니다.

9.4. **Speed limit(속도 제한)**에서 속도 범위를 추가합니다.

10. **Next (다음)**를 클릭합니다.
11. **Minimum trigger duration(최소 트리거 기간)** 아래에서 알람의 최소 지속 시간을 설정합니다.
Line crossing(선 넘기) 시나리오에서 객체가 선을 넘는 즉시 동작이 트리거되게 하려면 지속 시간을 0초로 낮춥니다.
12. **Save(저장)**를 클릭합니다.

허위 알람을 최소화하는 방법

거짓 경보가 많이 발생하면 여러 설정을 변경하여 이를 최소화해 볼 수 있습니다. 예를 들어 특정 유형의 움직임 또는 객체를 필터링하거나, 객체가 알람을 트리거하는 구역을 조정하거나, 감지 민감도를 조정할 수 있습니다.

- 레이더의 감지 감도를 조정합니다.
Radar(레이더) > Settings(설정) > Detection(감지)로 이동한 다음 **Detection sensitivity(감지 민감도)**를 낮춥니다.
감도 설정은 모든 영역에 영향을 미칩니다.
  - 장면에 금속 객체 또는 대형 차량이 많을 때는 낮은 감지 민감도가 적합합니다. 이는 거짓 경보 위험을 줄이지만, 레이더의 소형 객체 분류 능력도 감소시킵니다.
  - 금속 객체가 없는 들판과 같은 개방된 장면에는 높은 감지 민감도가 적합합니다.
- 포함 구역 및 제외 구역 수정:
장면 내 단단한 표면은 반사를 일으켜 하나의 물리적 객체에 대해 여러 번 감지되게 할 수 있습니다. 시나리오에서 포함 구역의 형태를 조정하거나, 장면의 특정 부분을 무시하기 위해 일반 제외 구역을 추가할 수 있습니다.
- 하나가 아닌 두 개의 선을 교차하는 객체에 대해 트리거합니다.
선 넘기 시나리오의 장면에 흔들리는 객체 또는 동물이 있으면, 해당 객체가 선을 교차하여 거짓 경보를 트리거할 위험이 있습니다. 이 경우 객체가 두 개의 선을 넘을 때만 트리거되도록 시나리오를 조정할 수 있습니다.
- 특정 움직임 필터링:
  - 장면 내 나무, 덤불, 깃발로 인한 거짓 경보를 최소화하려면 **Radar(레이더) > Settings (설정) > Detection(감지)**로 이동한 다음 **Ignore swaying objects(흔들리는 객체 무시)**를 켭니다.
  - 장면 내 고양이, 토끼와 같은 작은 객체로 인한 거짓 경보를 최소화하려면 **Radar(레이더) > Settings(설정) > Detection(감지)**으로 이동한 다음 **Ignore small objects(작은 객체 무시)**를 켭니다. 이 설정은 영역 모니터링 프로파일에서 사용할 수 있습니다.
- 시간에 대한 필터:
  - **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
  - 시나리오를 선택하고 ⋮ 을 클릭하여 설정을 수정합니다.
  - **Seconds until trigger(트리거까지 남은 초)**를 늘립니다. 이는 레이더가 객체 추적을 시작한 시점부터 알람을 트리거할 수 있을 때까지의 지연 시간입니다. 타이머는 객체가 시나리오의 포함 구역에 들어갈 때가 아니라 레이더가 객체를 감지할 때 시작됩니다.
- 객체 유형에 대한 필터:
  - **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
  - 시나리오를 선택하고 ⋮ 을 클릭하여 설정을 수정합니다.

– 특정 객체 유형에서 트리거되지 않도록 하려면, 시나리오에서 알람을 트리거하지 않아야 하는 객체 유형을 지웁니다.

설치 확인

레이더 설치 확인

레이더 사용을 시작하기 전에 설치를 검증할 것을 권장합니다. 검증은 설치 문제를 식별하거나 장면 내 나무 또는 반사 표면과 같은 정적 객체를 관리하는 데 도움이 될 수 있습니다.

비고

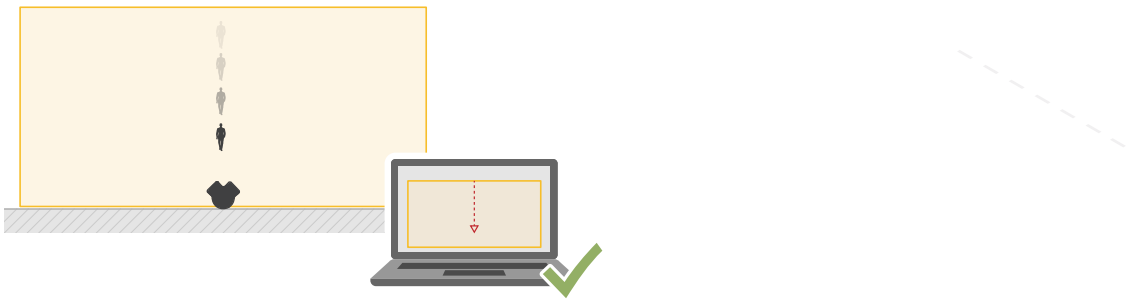
설치는 검증 시점에 적용되는 조건에서 검증됩니다. 장면의 조건이 변경되면 설치의 일상적인 성능에 영향을 미칠 수 있습니다.

잘못된 감지가 없는지 확인

1. 인식 구역에 사람의 활동이 없는지 확인합니다.
2. 레이더가 인식 구역에서 정적 객체를 감지하지 않는지 확인하기 위해 몇 분간 기다립니다.
3. 원치 않는 감지가 있으면 특정 유형의 움직임 또는 객체를 필터링하거나, 객체가 알람을 트리거하는 구역을 조정하거나, 감지 민감도를 조정할 수 있습니다. 지침에 대해서는 *허위 알람을 최소화하는 방법, on page 18* 항목을 참조하십시오.

올바른 기호, 이동 방향 및 지도상의 위치를 확인합니다.

1. 레이더의 웹 인터페이스에서 녹화를 시작합니다. 지침에 대해서는 *비디오 녹화 및 시청, on page 20* 항목을 참조하십시오.
2. 인식 구역 바로 바깥에서 걷기 시작한 다음 레이더를 향해 곧바로 걸어갑니다.
3. 사람이 인식 구역에 들어갈 때 사람 분류 기호가 표시되는지 확인합니다.
4. 레이더의 웹 인터페이스가 올바른 이동 방향을 표시하는지 확인합니다.



5. 사람의 실제 위치가 지도상의 위치와 일치하는지 확인합니다.

검증 데이터를 기록하는 데 도움이 되도록 아래 테이블과 유사한 테이블을 만듭니다.

테스트	통과/실패	의견
1. 영역이 비어 있을 때 원치 않는 감지가 없는지 확인합니다.		
2. 사람이 인식 구역에 들어갈 때 사람 분류 기호가 표시되는지 확인합니다.		

3. 이동 방향이 올바른지 확인합니다.		
4. 사람의 실제 위치가 지도상의 위치와 일치하는지 확인합니다.		

검증 완료

유효성 검사의 첫 번째 부분을 성공적으로 완료했으면 다음 테스트를 수행하여 유효성 검사 프로세스를 완료합니다.

1. 지침에 따라 레이더를 구성했는지 확인합니다.
2. 참조 지도를 추가하고 보정했는지 확인합니다.
3. 사람이 감지될 때 트리거되도록 레이더 시나리오를 설정합니다. 기본적으로 **Seconds until trigger(트리거까지 남은 초)**는 2초로 설정되지만, 필요하면 변경할 수 있습니다.
4. 적절한 객체가 감지되면 비디오를 녹화하도록 레이더를 설정합니다.
   지침에 대해서는 *비디오 녹화 및 시청, on page 20* 항목을 참조하십시오.
5. **Radar(레이더) > Settings(설정) > Object visualization(객체 시각화)**로 이동한 다음 **Trail lifetime(트레일 유지 시간)**을 1시간으로 설정하여, 자리를 떠나 감시 구역을 한 바퀴 둘러보고 다시 자리로 돌아오는 데 걸리는 시간을 충분히 초과하도록 합니다. 트레일 유지 시간은 설정된 시간 동안 레이더의 실시간 보기에서 트랙을 유지하며, 검증을 완료한 후에는 비활성화할 수 있습니다.
6. 인식 구역의 경계를 따라 걸으면서 시스템의 트레일링이 본인이 걸은 경로와 일치하는지 확인합니다.
7. 검증 결과가 만족스럽지 않으면 참조 지도를 다시 보정한 후 검증을 반복합니다.

레이더 이미지를 조정

이 섹션에는 레이더 이미지 구성에 관한 지침이 포함되어 있습니다. 특정 기능의 작동 방식에 대해 자세히 알아보려면 *상세 정보, on page 71*로 이동하십시오.

이미지 오버레이 표시

레이더 스트림에서 오버레이로 이미지를 추가할 수 있습니다.

1. **Radar > Overlays(레이더 > 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.

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 72*으로 이동하십시오.

비디오 녹화 및 시청

레이더에서 직접 비디오 녹화

1. **Radar > Stream(레이더 > 스트림)**으로 이동합니다.

2. 녹화를 시작하려면 을 클릭합니다.

   스토리지를 설정하지 않은 경우, 및 을 클릭합니다. 네트워크 스토리지를 설정하는 방법의 지침은 을 참조하십시오.

3. 녹화를 중지하려면 다시 을 클릭합니다.

동영상 보기

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

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

- 활성 룰을 변경하는 경우 변경 사항을 적용하려면 규칙을 다시 켜야 합니다.
- 룰에서 사용하는 스트림 프로파일의 정의를 변경하면, 해당 스트림 프로파일을 사용하는 모든 룰을 다시 시작해야 합니다.

레이더의 빨간색 신호등을 활성화

레이더 전면의 동적 LED 스트립을 사용하여 해당 지역이 모니터링되고 있음을 나타낼 수 있습니다.

이 예시는 평일 근무 시간 이후에 빨간색 스윕 조명을 활성화하는 방법을 설명합니다.

일정 생성:

1. **System > Events > Schedules(시스템 > 이벤트 > 일정)**로 이동한 후 새 일정을 추가합니다.
2. 스케줄 이름을 입력합니다. 예: `Weekday nights`.
3. **Type(유형)** 아래에서 **Schedule(일정)**을 선택합니다.
4. **Recurrence(반복)**에서 **Daily(일간)**를 선택합니다.
5. 18:00로 시작 시간을 설정합니다.
6. 06:00로 종료 시간을 설정합니다.
7. **Days(요일)**에서 월요일부터 금요일까지를 선택합니다.
8. **Save(저장)**를 클릭합니다.

룰 생성:

1. **System > Events(시스템 > 이벤트)**로 이동하고 룰을 추가합니다.
2. 룰 이름을 입력합니다. 예: `Red sweeping light`.
3. 조건 목록의 **Scheduled and recurring(예약 및 반복)**에서 **Schedule(일정)**을 선택합니다.

4. 스케줄 목록에서 **Weekday nights(평일 야간)**를 선택합니다.
5. **Radar(레이더)**의 액션 목록에서 **Dynamic LED strip(동적 LED 스트립)**을 선택합니다.
6. **Sweeping red(빨간색 스윕)** 패턴을 선택합니다.
7. 기간을 12시간으로 설정합니다.
8. **Save(저장)**를 클릭합니다.

누군가가 금속 물체로 레이더를 가리면 이메일 보내기

이 예에서는 누군가가 레이더를 금속 호일이나 금속 시트와 같은 금속 물체로 덮어 조작할 때 이메일 알림을 보내는 룰을 생성하는 방법을 설명합니다.

이메일 수신자 추가:

1. **System > Events > Recipients(시스템 > 이벤트 > 수신자)**로 이동하고 수신자를 추가합니다.
2. 수신자의 이름을 입력합니다.
3. **Type(유형)**에서 **Email(이메일)**을 선택합니다.
4. 이메일을 보낼 이메일 주소를 입력합니다.
5. 이메일 제공업체에 따라 나머지 정보를 작성합니다.
   레이더 장치에는 자체 이메일 서버가 없으므로 이메일을 보내려면 이메일 서버에 로그인해야 합니다.
6. 테스트 이메일을 보내려면 **Test(테스트)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

룰 생성:

8. **System > Events(시스템 > 이벤트)**로 이동하고 룰을 추가합니다.
9. 룰 이름을 입력합니다. 예: `Tampering mail`.
10. 조건 목록의 **Device status(장치 상태)**에서 **Radar data failure(레이더 데이터 오류)**를 선택합니다.
11. **Reason(이유)**에서 **Tampering(탬퍼링)**을 선택합니다.
12. 액션 목록의 **Notifications(알림)**에서 **Send notification to email(이메일로 알림 전송)**을 선택합니다.
13. 생성한 수신자를 선택합니다.
14. 이메일 제목과 메시지를 입력합니다.
15. **Save(저장)**를 클릭합니다.

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

비고

이 섹션에서 설명하는 기능 및 설정에 대한 지원은 장치마다 다릅니다. 이 아이콘 은 일부 장치에서만 기능이나 설정을 사용할 수 있음을 나타냅니다.

기본 메뉴를 표시하거나 숨깁니다.

릴리스 정보에 액세스합니다.

제품 도움말에 액세스합니다.

언어를 변경합니다.

밝은 테마 또는 어두운 테마를 설정합니다.

사용자 메뉴에는 다음이 포함됩니다.

- 로그인한 사용자에 대한 정보.
- **Change account(계정 변경)**: 현재 계정에서 로그아웃하고 새 계정에 로그인합니다.
- **Log out(로그아웃)**: 현재 계정에서 로그아웃합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **분석 데이터**: 개인용이 아닌 브라우저 데이터를 공유하려면 수락하십시오.
- **Feedback(피드백)**: 사용자 경험을 개선하는 데 도움이 되는 피드백을 공유하십시오.
- **Legal(법률)**: 쿠키 및 라이센스에 대한 정보를 봅니다.
- **About(정보)**: AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 봅니다.

상태

장치 정보

AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 표시합니다.

Upgrade AXIS OS(AXIS OS 업그레이드): 장치의 소프트웨어를 업그레이드합니다. 업그레이드를 수행할 수 있는 유지보수 페이지로 이동합니다.

시간 동기화 상태

장치가 NTP 서버와 동기화되었는지 여부 및 다음 동기화까지 남은 시간을 포함하여 NTP 동기화 정보를 표시합니다.

NTP settings(NTP 설정): NTP 설정을 보고 업데이트합니다. NTP 설정을 변경할 수 있는 **Time and location(시간 및 위치)** 페이지로 이동합니다.

보안

활성 장치에 대한 액세스 유형과 사용 중인 암호화 프로토콜, 서명되지 않은 앱의 허용 여부를 표시합니다. 설정에 대한 권장 사항은 AXIS OS 강화 가이드를 기반으로 합니다.

Hardening guide(보안 강화 가이드): Axis 장치의 사이버 보안과 모범 사례에 대해 자세히 알아볼 수 있는 *AXIS OS 강화 가이드* 링크입니다.

연결된 클라이언트

연결 및 연결된 클라이언트 수를 표시합니다.

View details(세부 사항 보기): 연결된 클라이언트 목록을 보고 업데이트합니다. 목록에는 각 연결의 IP 주소, 프로토콜, 포트, 상태 및 PID/프로세스가 표시됩니다.

녹화/녹음 진행 중

진행 중인 녹화와 지정된 저장 공간을 표시합니다.

녹화물: 진행 중이고 필터링된 녹화물과 해당 소스를 봅니다. 자세한 내용은 *녹화 영상, on page 33* 를 참조하십시오.

녹화물이 저장되는 저장 공간을 표시합니다.

전원 상태

현재 전력, 평균 전력 및 최대 전력을 포함한 전력 상태 정보를 표시합니다.

Power settings(전원 설정): 장치의 전원 설정을 보고 업데이트합니다. 전원 설정을 변경할 수 있는 전원 설정 페이지로 이동합니다.

레이더

설정

일반사항

Radar transmission(레이더 전송): 완전히 레이더 모듈을 끄려면 이를 사용하십시오.

Channel(채널) : 여러 장치가 서로 간섭하는 문제가 있는 경우 서로 가까이 있는 최대 4개의 장치에 대해 같은 채널을 선택합니다. 설치의 경우 대개는 **Auto(자동)**를 선택하여 어느 채널을 사용할지 장치가 자동으로 협상하게 합니다.

Mounting height(장착 높이): 제품의 장착 높이를 입력합니다.

비고

장착 높이를 입력할 때 되도록 구체적으로 입력하십시오. 이렇게 하면 장치가 이미지의 올바른 위치에서 레이더 감지를 시각화하는 데 도움이 됩니다.

공존

Number of neighboring radars(주변 레이더 수): 동일한 공존 영역 내에 마운트된 인접 레이더의 수를 선택합니다. 이렇게 하면 간섭을 피하는 데 도움이 됩니다.

- **0–3**: 동일한 공존 구역에 레이더를 1~4대 마운트하는 경우 이 옵션을 선택합니다.
- **4–5**: 동일한 공존 구역에 레이더를 5~6대 마운트하는 경우 이 옵션을 선택합니다.
- **6–11**: 동일한 공존 구역에 레이더를 7~12대 마운트하는 경우 이 옵션을 선택합니다.

감지

Detection sensitivity(디텍션 감도): 레이더의 감도를 선택합니다. 값이 높을수록 감지 범위가 길어지지만 허위 알람의 위험도 높아집니다. 감도가 낮을수록 허위 알람의 수는 줄어들지만 감지 범위가 짧아질 수도 있습니다.

Radar profile(레이더 프로파일): 관심 영역에 적합한 프로파일을 선택합니다.

- **Area monitoring(영역 모니터링)**: 개방된 영역에서 저속으로 움직이는 크고 작은 객체를 모두 추적합니다.
  - **Ignore stationary rotating objects(회전하는 고정 객체 무시)** : 팬이나 터빈 등 회전 동작을 하는 고정 물체로 인한 허위 알람을 최소화하려면 켭니다.
  - **Ignore small objects(작은 객체 무시)**: 고양이나 토끼와 같은 작은 객체의 허위 알람을 최소화하려면 켭니다.
  - **Ignore swaying objects(흔들리는 객체 무시)**: 나무, 덤불 또는 깃대와 같이 흔들리는 객체로 인한 허위 알람을 최소화하려면 켭니다.
  - **Ignore unknown objects(알 수 없는 객체 무시)**: 레이더가 분류할 수 없는 물체로 인한 거짓 경보를 최소화하려면 켭니다.
- **Road monitoring(도로 모니터링)** : 도심 지역 및 교외 도로에서 고속으로 주행하는 차량을 추적합니다.
  - **Ignore stationary rotating objects(회전하는 고정 객체 무시)** : 팬이나 터빈 등 회전 동작을 하는 고정 물체로 인한 허위 알람을 최소화하려면 켭니다.
  - **Ignore swaying objects(흔들리는 객체 무시)**: 나무, 덤불 또는 깃대와 같이 흔들리는 객체로 인한 허위 알람을 최소화하려면 켭니다.
  - **Ignore unknown objects(알 수 없는 객체 무시)**: 레이더가 분류할 수 없는 물체로 인한 거짓 경보를 최소화하려면 켭니다.

보기

Information legend(정보 범례) : 레이더가 감지하고 추적할 수 있는 객체 유형이 포함된 범례를 표시하려면 켭니다. 끌어서 놓기하여 정보 범례를 이동합니다.

Zone opacity(영역 불투명도): 감시 영역의 불투명도 또는 투명도를 선택합니다.

Grid opacity(그리드 불투명도): 그리드의 불투명도 또는 투명도를 선택합니다.

Color scheme(색 구성표): 레이더 시각화의 테마를 선택합니다.

Rotation(회전) : 레이더 이미지의 기본 방향을 선택합니다.

객체 시각화

Trail lifetime(트레일 수명): 추적된 객체에 대한 추적이 레이더 보기에서 표시되는 시간을 선택합니다.

Icon style(아이콘 스타일): 레이더 보기에서 추적된 객체의 아이콘 스타일을 선택합니다. 일반 삼각형의 경우 **Triangle(삼각형)**을 선택합니다. 대표 기호의 경우 **Symbol(기호)**을 선택합니다. 아이콘은 스타일에 관계없이 추적된 객체가 움직이는 방향을 가리킵니다.

Show information with icon(아이콘으로 정보 표시): 추적된 객체의 아이콘 옆에 표시할 정보를 선택합니다.

- **Object type(객체 유형)**: 레이더가 감지한 객체 유형을 표시합니다.
- **Classification probability(분류 확률)**: 객체 분류의 정확도에 대한 레이더의 확신 정도를 보여줍니다.
- **Velocity(속도)**: 객체가 얼마나 빠르게 움직이는지 보여줍니다.

스트림

일반사항

해상도: 감시 장면에 적합한 이미지 해상도를 선택하십시오. 해상도가 높을수록 대역폭과 저장 공간이 늘어납니다.

프레임 레이트: 네트워크에서 대역폭 문제를 피하거나 스토리지 크기를 줄이기 위해 프레임 속도를 고정된 양으로 제한할 수 있습니다. 프레임 레이트를 0으로 두면 현재 조건에서 가능한 최고 속도로 프레임 레이트가 유지됩니다. 프레임 레이트가 높을수록 더 많은 대역폭과 저장 용량이 필요합니다.

P-frames(P-프레임): P-프레임은 이전 프레임에서 이미지의 변화만 보여주는 예측 이미지입니다. 원하는 P-프레임 수를 입력합니다. 숫자가 높을수록 더 적은 대역폭이 필요합니다. 그러나 네트워크가 정체되는 경우 비디오 품질이 눈에 띄게 저하될 수 있습니다.

Compression(압축): 슬라이더를 사용하여 이미지 압축을 조정합니다. 압축률이 높으면 비트 레이트가 낮아지고 이미지 품질이 낮아집니다. 압축 수준이 낮으면 이미지 품질은 향상되지만 녹화할 때 더 많은 대역폭과 저장 공간을 사용합니다.

Signed video : 비디오에 서명된 비디오 기능을 추가하려면 켜십시오. 서명 비디오는 비디오에 암호화 서명을 추가하여 비디오가 변조되지 않도록 보호합니다.

비트 레이트 제어

- **Average(평균)**: 더 오랜 기간 동안 자동으로 비트 레이트를 조정하고 사용 가능한 저장 공간을 기반으로 최상의 이미지 품질을 제공하려면 선택합니다.
  -  사용 가능한 스토리지, 보존 시간 및 비트 레이트 제한을 기반으로 대상 비트 레이트를 계산하려면 클릭합니다.
  - **Target bitrate(대상 비트 레이트)**: 원하는 타겟 비트 레이트를 입력합니다.
  - **Retention time(보존 시간)**: 녹화물을 보관할 일 수를 지정합니다.
  - **저장 장치**: 스트림에 사용할 수 있는 예상 스토리지를 표시합니다.
  - **Maximum bitrate(최대 비트 레이트)**: 비트 레이트 제한을 설정하려면 켭니다.
  - **Bitrate limit(비트 레이트 제한)**: 비트 레이트 제한을 대상 비트 레이트보다 더 높게 입력하십시오.
- **Maximum(최대)**: 네트워크 대역폭을 기준으로 스트림의 최대 인스턴트 비트 레이트를 설정하려면 선택합니다.
  - **Maximum(최대)**: 최대 비트 레이트를 입력합니다.
- **Variable(변수)**: 장면의 활동 수준에 따라 비트 레이트가 달라지도록 하려면 선택합니다. 더 많은 활동에는 더 많은 대역폭이 필요합니다. 대부분의 상황에서 이 옵션을 사용하는 것이 좋습니다.

지도 보정

지도 보정을 사용하여 참조 지도를 업로드하고 보정합니다. 보정 결과는 레이더 커버리지를 적절한 축척으로 표시하는 참조 지도이며, 이를 통해 객체가 움직이는 위치를 쉽게 확인할 수 있습니다.

Setup assistant(설정 도우미): 클릭하면 보정을 단계별로 안내하는 설정 도우미가 열립니다.

Reset calibration(보정 재설정): 지도에서 현재 지도 이미지와 레이더 위치를 제거하려면 클릭합니다.

지도

Upload map(지도 업로드): 업로드하려는 지도 이미지를 선택하거나 끌어다 놓습니다.

Download map(지도 다운로드): 지도를 다운로드하려면 클릭합니다.

Rotate map(지도 회전): 슬라이더를 사용하여 지도 이미지를 회전합니다.

지도의 축척 및 거리

Distance(거리): 지도에 추가한 두 지점 사이의 거리를 추가합니다.

지도 이동 및 줌

Pan(팬): 버튼을 클릭하여 지도 이미지를 이동합니다.

Zoom(줌): 버튼을 클릭하여 지도 이미지를 확대하거나 축소합니다.

Reset pan and zoom(이동 및 줌 재설정): 이동 및 줌 설정을 제거하려면 클릭합니다.

레이더 위치

Position(위치): 버튼을 클릭하여 지도에서 레이더를 이동합니다.

Rotation(회전): 버튼을 클릭하여 지도에서 레이더를 회전합니다.

제외 구역

exclusion zone(제외 구역)은 움직이는 객체가 무시되는 영역입니다. 시나리오 내에 원치 않는 알람을 많이 트리거하는 영역이 있으면 제외 구역을 사용합니다.

+ 새 제외 구역을 생성하려면 클릭합니다.

제외 구역을 수정하려면 목록에서 해당 구역을 선택합니다.

Track passing objects(지나가는 객체 추적): 제외 구역을 통과하는 객체를 추적하려면 켭니다. 통과하는 객체의 추적 ID가 유지되며, 구역 전체에서 볼 수 있습니다. 제외 구역 내에서 나타나는 객체는 추적이 불가능합니다.

Zone shape presets(구역 형태 프리셋): 제외 구역의 초기 형태를 선택합니다.

- **Cover everything(전체 커버)**: 전체 레이더 적용 범위를 포함하는 제외 구역을 설정하려면 선택합니다.
- **Reset to box(박스로 재설정)**: 적용 범위 영역 중앙에 직사각형 제외 영역을 배치하려면 선택합니다.

영역의 형태를 수정하려면 선에 있는 점을 끌어서 놓습니다. 포인트를 제거하려면 마우스 오른쪽 버튼으로 클릭합니다.

시나리오

시나리오는 트리거링 조건과 장면 및 감지 설정의 조합입니다.

+ : 새 시나리오를 생성하려면 클릭합니다. 최대 20개의 시나리오를 생성할 수 있습니다.

Triggering conditions(트리거링 조건): 알람을 트리거하는 조건을 선택합니다.
- **Movement in area(영역 내 이동)**: 한 영역에서 이동하는 객체에 대해 시나리오가 트리거되도록 하려면 선택합니다.
- **선 넘기**: 하나 또는 두 개의 라인을 교차하는 객체에 대해 시나리오를 트리거하려면 선택합니다.

Scene(장면): 움직이는 객체가 알람을 트리거하는 시나리오에서 영역 또는 라인을 정의합니다.
- **Movement in area(영역 내 이동)**의 경우, 모양 프리셋 중 하나를 선택하여 영역을 수정합니다.
- **Line crossing(선 넘기)**의 경우, 장면에서 라인을 끌어서 놓습니다. 한 라인에 더 많은 포인트를 생성하려면 라인의 아무 곳이나 클릭한 후 끕니다. 포인트를 제거하려면 마우스 오른쪽 버튼으로 클릭합니다.
  - **Require crossing of two lines(두 라인을 횡단해야 함)**: 시나리오가 알람을 트리거하기 전에 객체가 두 라인을 통과해야 하는 경우 켜집니다.
  - **Change direction(방향 변경):** 객체가 다른 방향으로 라인을 통과할 때 시나리오에서 알람을 트리거하려면 켭니다.

Detection settings(감지 설정): 시나리오에 대한 트리거 기준을 정의합니다.
- **Movement in area(영역 내 이동)**의 경우:
  - **Ignore short-lived objects(빠른 객체 무시)**: 레이더가 객체를 감지한 시점부터 시나리오가 알람을 트리거하는 시점까지의 지연 시간(초)을 설정합니다. 이렇게 하면 허위 알람을 줄일 수 있습니다.
  - **Trigger on object type(객체 유형에 대한 트리거)**: 시나리오를 트리거할 객체 유형(사람, 차량, 알 수 없음)을 선택합니다.
  - **Speed limit(속도 제한)**: 특정 범위 내에서 속도로 움직이는 객체에 대해 트리거합니다.
    - **Invert(반전)**: 설정된 속도 제한보다 높거나 낮은 속도로 트리거하려면 선택합니다.
- **Line crossing(선 넘기)**의 경우:
  - **Ignore short-lived objects(빠른 객체 무시)**: 레이더가 객체를 감지한 시점부터 시나리오가 액션을 트리거하는 시점까지의 지연 시간(초)을 설정합니다. 이렇게 하면 허위 알람을 줄일 수 있습니다. 두 선을 교차하는 객체에는 이 옵션을 사용할 수 없습니다.
  - **Max time between crossings(교차로 간 최대 시간)**: 첫 번째 라인과 두 번째 라인의 교차로 간 최대 시간을 설정합니다. 두 선을 교차하는 객체에만 이 옵션을 사용할 수 있습니다.
  - **Trigger on object type(객체 유형에 대한 트리거)**: 시나리오를 트리거할 객체 유형(사람, 차량, 알 수 없음)을 선택합니다.
  - **Speed limit(속도 제한)**: 특정 범위 내에서 속도로 움직이는 객체에 대해 트리거합니다.
    - **Invert(반전)**: 설정된 속도 제한보다 높거나 낮은 속도로 트리거하려면 선택합니다.

Alarm settings(알람 설정): 알람 기준을 정의합니다.
- **Minimum trigger duration(최소 트리거 기간)**: 트리거된 알람의 최소 지속 시간을 설정합니다.

오버레이

+ : 오버레이를 추가하려면 클릭합니다. 드롭다운 목록에서 오버레이 유형을 선택합니다.

- **Text(텍스트)**: 실시간 보기 이미지에 통합되고 모든 보기, 녹화 및 스냅샷에서 볼 수 있는 텍스트를 표시하려면 선택합니다. 고유한 텍스트를 입력할 수 있으며 미리 구성된 수정자를 포함하여 시간, 날짜, 프레임 레이트 등을 자동으로 표시할 수도 있습니다.
  - : yyyy-mm-dd를 표시하기 위해 날짜 수정자 `%F`를 추가하려면 클릭합니다.
  - : hh:mm:ss(24시간 시계)를 표시하기 위해 시간 수정자 `%X`를 추가하려면 클릭합니다.
  - **Modifiers(수정자)**: 텍스트 상자에 추가하기 위해 목록에 나타난 수정자를 선택하려면 클릭합니다. 예를 들어, `%a`는 요일을 표시합니다.
  - **Size(크기)**: 원하는 글꼴 크기를 선택합니다.
  - **Appearance(모양)**: 검정 배경에 흰색 텍스트(기본값)와 같이 텍스트 색과 배경색을 선택합니다.
  - : 이미지에서 오버레이의 위치를 선택하거나, 실시간 보기에서 오버레이를 클릭하고 드래그하여 이동합니다.
- **Image(이미지)**: 비디오 스트림 위에 중첩된 정적 이미지를 표시하려면 선택합니다. .bmp, .png, .jpeg 또는 .svg 파일을 사용할 수 있습니다.
  이미지를 업로드하려면 **Manage images(이미지 관리)**를 클릭합니다. 이미지를 업로드하기 전에 다음을 선택할 수 있습니다.
  - **Scale with resolution(해상도를 사용하여 확장)**: 비디오 해상도에 맞게 오버레이 이미지의 크기를 자동으로 조정하려면 선택합니다.
  - **Use transparency(투명성 사용)**: 해당 색상에 대한 RGB 16진수 값을 선택하고 입력합니다. RRGGBB 형식을 사용합니다. 16진수 값에 대한 예로 흰색은 FFFFFF, 검정색은 000000, 빨간색은 FF0000, 파란색은 6633FF, 녹색은 669900입니다. .bmp 이미지에만 해당됩니다.
- **Scene annotation(장면 주석)** : 비디오 스트림에서 카메라가 다른 방향으로 팬 또는 틸트를 수행하더라도 같은 위치를 유지하는 텍스트 오버레이 표시를 선택합니다. 특정 줌 레벨 내에서만 오버레이가 표시되도록 선택할 수 있습니다.
  - : yyyy-mm-dd를 표시하기 위해 날짜 수정자 `%F`를 추가하려면 클릭합니다.
  - : hh:mm:ss(24시간 시계)를 표시하기 위해 시간 수정자 `%X`를 추가하려면 클릭합니다.
  - **Modifiers(수정자)**: 텍스트 상자에 추가하기 위해 목록에 나타난 수정자를 선택하려면 클릭합니다. 예를 들어, `%a`는 요일을 표시합니다.
  - **Size(크기)**: 원하는 글꼴 크기를 선택합니다.
  - **Appearance(모양)**: 검정 배경에 흰색 텍스트(기본값)와 같이 텍스트 색과 배경색을 선택합니다.
  - : 이미지에서 오버레이의 위치를 선택하거나, 실시간 보기에서 오버레이를 클릭하고 드래그하여 이동합니다. 오버레이가 저장되고 이 위치의 팬 및 틸트 좌표 내로 유지됩니다.
  - **Annotation between zoom levels (%)(줌 레벨 사이에 각주 표시(%))**: 오버레이가 표시되도록 할 줌 레벨을 설정합니다.

- **Annotation symbol(주석 기호)**: 카메라가 설정된 줌 레벨 이내에 있지 않은 경우 오버레이 대신 표시될 기호를 선택합니다.

- **Streaming indicator(스트리밍 표시기)** : 비디오 스트림 위에 겹쳐진 애니메이션을 표시하려면 선택합니다. 애니메이션은 장면에 모션이 포함되지 않은 경우에도 비디오 스트림이 라이브임을 나타냅니다.
  - **Appearance(모양)**: 애니메이션 색상과 배경 색상을 선택합니다(예: 투명한 배경의 빨간색 애니메이션(기본 설정)).
  - **Size(크기)**: 원하는 글꼴 크기를 선택합니다.
  - : 이미지에서 오버레이의 위치를 선택하거나, 실시간 보기에서 오버레이를 클릭하고 드래그하여 이동합니다.

- **Widget: Linegraph(위젯: 선그래프)** : 측정된 값이 시간에 따라 어떻게 바뀌는지 보여주는 그래프 차트를 표시합니다.
  - **Title(제목)**: 위젯의 제목을 입력합니다.
  - **Overlay modifier(오버레이 수정자)**: 데이터 소스로 사용할 오버레이 수정자를 선택합니다. MQTT 오버레이를 생성한 경우 목록의 끝 부분에 위치하게 됩니다.
  - : 이미지에서 오버레이의 위치를 선택하거나, 실시간 보기에서 오버레이를 클릭하고 드래그하여 이동합니다.
  - **Size(크기)**: 오버레이의 크기를 선택합니다.
  - **Visible on all channels(전체 채널에 표시)**: 현재 선택한 채널에서만 표시되도록 하려면 끕니다. 모든 활성 채널에 표시되도록 하려면 켭니다.
  - **Update interval(업데이트 간격)**: 데이터 업데이트 간격을 선택합니다.
  - **Transparency(투명도)**: 전체 오버레이의 투명도를 설정합니다.
  - **Background transparency(백그라운드 투명도)**: 오버레이의 백그라운드 투명도만 설정합니다.
  - **Points(점들)**: 데이터가 업데이트될 때 그래프 선에 점을 추가하려면 켭니다.
  - **X축**
    - **Label(라벨)**: X축에 대한 텍스트 라벨을 입력합니다.
    - **Time window(시간 창)**: 데이터 시각화 기간을 입력합니다.
    - **Time unit(시간 단위)**: X축에 대한 시간 단위를 입력합니다.
  - **Y축**
    - **Label(라벨)**: Y축에 대한 텍스트 라벨을 입력합니다.
    - **Dynamic scale(동적 배율)**: 이 기능을 켜면 배율이 데이터 값에 따라 자동으로 변동됩니다. 이 기능을 끄면 고정 배율 값을 직접 입력할 수 있습니다.
    - **Min alarm threshold(최소 알람 임계값)** 및 **Max alarm threshold(최대 알람 임계값)**: 이 값들은 그래프에 수평 참조선을 추가하여 데이터 값이 너무 높거나 너무 낮아지는 경우 쉽게 판독할 수 있게 해줍니다.

- **Widget: Meter(위젯: 측정기)** : 가장 최근 측정된 데이터 값을 보여주는 막대 차트를 표시합니다.
  - **Title(제목)**: 위젯의 제목을 입력합니다.
  - **Overlay modifier(오버레이 수정자)**: 데이터 소스로 사용할 오버레이 수정자를 선택합니다. MQTT 오버레이를 생성한 경우 목록의 끝 부분에 위치하게 됩니다.
  - : 이미지에서 오버레이의 위치를 선택하거나, 실시간 보기에서 오버레이를 클릭하고 드래그하여 이동합니다.

- **Size(크기)**: 오버레이의 크기를 선택합니다.
- **Visible on all channels(전체 채널에 표시)**: 현재 선택한 채널에서만 표시되도록 하려면 끕니다. 모든 활성 채널에 표시되도록 하려면 켭니다.
- **Update interval(업데이트 간격)**: 데이터 업데이트 간격을 선택합니다.
- **Transparency(투명도)**: 전체 오버레이의 투명도를 설정합니다.
- **Background transparency(백그라운드 투명도)**: 오버레이의 백그라운드 투명도만 설정합니다.
- **Points(점들)**: 데이터가 업데이트될 때 그래프 선에 점을 추가하려면 켭니다.
- **Y축**
  - **Label(라벨)**: Y축에 대한 텍스트 라벨을 입력합니다.
  - **Dynamic scale(동적 배율)**: 이 기능을 켜면 배율이 데이터 값에 따라 자동으로 변동됩니다. 이 기능을 끄면 고정 배율 값을 직접 입력할 수 있습니다.
  - **Min alarm threshold(최소 알람 임계값)** 및 **Max alarm threshold(최대 알람 임계값)**: 이 값들은 막대 그래프에 수평 참조선을 추가하여 데이터 값이 너무 높거나 너무 낮아지는 경우 쉽게 판독할 수 있게 해줍니다.

동적 LED 스트립

동적 LED 스트립 패턴

이 페이지를 사용하여 동적 LED 스트립의 패턴을 테스트하십시오.

Pattern(패턴): 테스트하고 싶은 패턴을 선택합니다.

Duration(기간): 테스트 기간을 지정합니다.

Test(테스트): 테스트하려는 패턴을 시작하려면 클릭합니다.

Stop(중지): 테스트를 중지하려면 클릭하십시오. 패턴 재생 중에 페이지를 벗어나면 자동으로 중지됩니다.

표시 또는 억제 목적으로 패턴을 활성화하려면 **System > Events(시스템 > 이벤트)**로 이동하여 룰을 생성하십시오. 설정 예는 *레이더의 빨간색 신호등을 활성화, on page 21* 항목을 참조하십시오.

분석 애플리케이션

메타데이터 구성

RTSP 메타데이터 생성자

메타데이터를 스트리밍하는 데이터 채널과 해당 채널이 사용하는 채널을 보고 관리합니다.

비고

이 설정은 ONVIF XML을 사용하는 RTSP 메타데이터 스트림에 대한 설정입니다. 여기서 변경한 내용은 메타데이터 시각화 페이지에 영향을 미치지 않습니다.

Producer(생산자): 실시간 스트리밍 프로토콜(RTSP)을 사용하여 메타데이터를 전송하는 데이터 채널.

채널: 생산자로부터 메타데이터를 전송하는 데 사용되는 채널. 메타데이터 스트림을 활성화하려면 켭니다. 호환성 또는 리소스 관리상의 이유로 끕니다.

녹화 영상

Ongoing recordings(녹화 진행 중): 장치에서 진행 중인 모든 녹화를 표시합니다.

● 장치에서 녹화를 시작합니다.

저장할 스토리지 장치를 선택합니다.

● 장치에서 녹화를 중지합니다.

수동으로 중지하거나 장치를 종료하면 **Triggered recordings(트리거 녹화)**가 종료됩니다.

Continuous recordings(연속 녹화)는 수동으로 중지할 때까지 계속됩니다. 장치가 꺼져 있어도 장치를 다시 시작하면 녹화가 계속됩니다.

녹화물을 재생합니다.

녹화물 재생을 중지합니다.

녹화물에 대한 정보와 옵션을 표시하거나 숨깁니다.

Set export range(내보내기 범위 설정): 녹화물의 일부만 내보내려면 기간을 입력합니다. 장치의 위치와 다른 시간대에서 작업한다면, 시간 범위는 장치의 시간대를 기준으로 합니다.

Encrypt(암호화): 내보낸 녹화물에 대한 패스워드를 설정하려면 선택합니다. 내보낸 파일은 패스워드 없이 열 수 없습니다.

녹화물을 삭제하려면 클릭합니다.

Export(내보내기): 녹화물 전체 또는 일부를 내보냅니다.

녹화를 필터링하려면 클릭합니다.

From(시작): 특정 시점 이후에 실행된 녹화를 표시합니다.

To(끝): 특정 시점까지 녹화를 표시합니다.

Source(소스): 소스를 기반으로 녹화를 표시합니다. 소스는 센서를 말합니다.

Event(이벤트): 이벤트를 기반으로 녹화를 표시합니다.

저장 장치: 스토리지 유형에 따라 녹화를 표시합니다.

앱

Add app(앱 추가): 새 앱을 설치합니다.

Find more apps(추가 앱 찾기): 설치할 앱을 더 찾습니다. Axis 앱의 개요 페이지로 이동됩니다.

Allow unsigned apps(서명되지 않은 앱 허용) : 서명되지 않은 앱 설치를 허용하려면 켭니다.

AXIS OS 및 ACAP 앱의 보안 업데이트를 확인하십시오.

비고

동시에 여러 앱을 실행하면 장치의 성능에 영향을 미칠 수 있습니다.

앱 이름 옆에 있는 스위치를 사용하여 앱을 시작하거나 중지합니다.

열기: 앱의 설정에 액세스합니다. 사용 가능한 설정은 애플리케이션에 따라 달라집니다. 일부 애플리케이션에는 설정이 없습니다.

상황에 맞는 메뉴에는 다음 옵션 중 하나 이상이 포함될 수 있습니다.

- **Open-source license(오픈 소스 라이센스)**: 앱에서 사용되는 오픈 소스 라이센스에 대한 정보를 봅니다.
- **App log(앱 로그)**: 앱 이벤트의 로그를 봅니다. 로그는 지원 서비스에 문의할 때 유용합니다.
- **Activate license with a key(키로 라이센스 활성화)**: 앱에 라이센스가 필요한 경우 활성화해야 합니다. 장치가 인터넷에 연결할 수 없는 경우 이 옵션을 사용합니다.
  라이센스 키가 없다면 *axis.com/products/analytics*로 이동합니다. 라이센스 키를 생성하려면 라이센스 코드와 Axis 제품 일련 번호가 필요합니다.
- **Activate license automatically(라이센스를 자동으로 활성화)**: 앱에 라이센스가 필요한 경우 활성화해야 합니다. 장치가 인터넷에 연결할 수 있는 경우 이 옵션을 사용합니다. 라이센스를 활성화하려면 라이센스 코드가 필요합니다.
- **라이센스 비활성화**: 예를 들어 체험판 라이센스에서 정식 라이센스로 변경하는 경우, 라이센스를 비활성화하여 다른 라이센스로 교체합니다. 라이센스를 비활성화하면 장치에서도 제거됩니다.
- **Settings(설정)**: 매개변수를 구성합니다.
- **삭제**: 장치에서 앱을 영구적으로 삭제하십시오. 먼저 라이센스를 비활성화하지 않으면 활성 상태로 유지됩니다.

시스템

시간과 장소

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

Synchronization(동기화): 장치의 날짜 및 시간 동기화 옵션을 선택합니다.

- **Automatic date and time (PTP)(자동 날짜 및 시간(PTP))**: 정밀 시간 프로토콜을 사용하여 동기화합니다.
- **Automatic date and time (manual NTS KE servers)(자동 날짜 및 시간(수동 NTS KE 서버))**: DHCP 서버에 연결된 보안 NTP 키 설정 서버와 동기화합니다.
  - **수동 NTS KE 서버**: 하나 또는 두 개의 NTP 서버의 IP 주소를 입력합니다. 두 개의 NTP 서버를 사용하는 경우 장치는 두 서버에 입력된 내용을 기반으로 시간을 동기화하고 조정합니다.
  - **Trusted NTS KE CA certificates(신뢰할 수 있는 NTS KE CA 인증서)**: 보안 NTS KE 시간 동기화에 사용할 신뢰할 수 있는 CA 인증서를 선택하거나 선택하지 않은 상태로 둡니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Automatic date and time (NTP server using DHCP)(자동 날짜 및 시간(DHCP를 사용하는 NTP 서버))**: DHCP 서버에 연결된 NTP 서버와 동기화합니다.
  - **Fallback NTP servers(대체 NTP 서버)**: 하나 또는 두 개의 대체 서버의 IP 주소를 입력합니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Automatic date and time (manual NTP server)(자동 날짜 및 시간(수동 NTP 서버))**: 선택한 NTP 서버와 동기화합니다.
  - **수동 NTP 서버**: 하나 또는 두 개의 NTP 서버의 IP 주소를 입력합니다. 두 개의 NTP 서버를 사용하는 경우 장치는 두 서버에 입력된 내용을 기반으로 시간을 동기화하고 조정합니다.
  - **Max NTP poll time(최대 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최대 시간을 선택합니다.
  - **Min NTP poll time(최소 NTP 폴링 시간)**: 업데이트된 시간을 얻기 위해 NTP 서버를 폴링할 때까지 장치가 기다려야 하는 최소 시간을 선택합니다.
- **Custom date and time(사용자 지정 날짜 및 시간)**: 수동으로 날짜 및 시간을 설정합니다. **Get from system(시스템에서 가져오기)**을 클릭하여 컴퓨터 또는 모바일 장치에서 날짜 및 시간 설정을 한 차례 가져옵니다.

시간대: 사용할 시간대를 선택합니다. 일광 절약 시간 및 표준 시간에 맞춰 시간이 자동으로 조정됩니다.

- **DHCP**: DHCP 서버의 시간대를 채택합니다. 이 옵션을 선택하려면 먼저 장치를 DHCP 서버(v4 또는 v6)에 연결해야 합니다. 두 버전을 모두 사용할 수 있는 경우, 장치는 POSIX보다 IANA 시간대를, DHCPv6보다 DHCPv4를 우선합니다.
  - DHCPv4는 POSIX 시간대에 Option 100(옵션 100)을 사용하고 IANA 시간대에 Option 101(옵션 101)을 사용합니다.
  - DHCPv6는 POSIX에 Option 41(옵션 41)을 사용하고 IANA에 Option 42(옵션 42)를 사용합니다.
- **Manual(수동)**: 드롭다운 목록에서 시간대를 선택합니다.

비고

시스템에서는 모든 녹화, 로그 및 시스템 설정에 날짜 및 시간 설정이 사용됩니다.

장치 위치

장치가 있는 위치를 입력합니다. 영상 관리 시스템에서 이 정보를 사용하여 지도에서 장치를 찾습니다.

- **Latitude(위도)**: 양수 값은 적도 북쪽을 나타냅니다.
- **Longitude(경도)**: 양수 값은 본초자오선 동쪽을 나타냅니다.
- **Heading(방향)**: 장치가 향하는 나침반 방향을 입력합니다. 0은 정북을 나타냅니다.
- **Label(라벨)**: 장치에 대한 설명이 포함된 이름을 입력합니다.
- **Save(저장)**: 장치 위치를 저장하려면 클릭합니다.

Regional settings(지역 설정)

모든 시스템 설정에서 사용할 측정 시스템을 설정합니다.

Metric (m, km/h)(미터법(m, km/h)): 거리 측정은 미터 단위로, 속도 측정은 시속 킬로미터 단위로 선택합니다.

U.S. customary (ft, mph)(미국식 단위(ft, mph)): 거리 측정은 피트 단위로, 속도 측정은 시속 마일 단위로 선택합니다.

네트워크

IPv4

Assign IPv4 automatically(IPv4 자동 할당): 수동 구성 없이 네트워크에서 IP 주소, 서브넷 마스크, 라우터를 자동으로 할당하도록 하려면 IPv4 자동 IP(DHCP)를 선택합니다. 대부분의 네트워크에서는 자동 IP 할당(DHCP)을 사용하는 것이 좋습니다.

IP 주소: 장치의 고유한 IP 주소를 입력하십시오. 고정 IP 주소는 각 주소가 고유한 경우 격리된 네트워크 내에서 무작위로 할당될 수 있습니다. 충돌을 방지하려면 고정 IP 주소를 할당하기 전에 네트워크 관리자에게 문의하는 것이 좋습니다.

서브넷 마스크: 서브넷 마스크를 입력하여 LAN(Local Area Network) 내부에 있는 주소를 정의합니다. LAN 외부의 모든 주소는 라우터를 통과합니다.

Router(라우터): 다른 네트워크 및 네트워크 세그먼트에 연결된 장치를 연결하는 데 사용되는 기본 라우터(게이트웨이)의 IP 주소를 입력합니다.

Fallback to static IP address if DHCP isn't available(DHCP를 사용할 수 없는 경우 고정 IP 주소로 폴백): DHCP를 사용할 수 없고 IP 주소를 자동으로 할당할 수 없는 경우 대체로 사용할 고정 IP 주소를 추가하려면 선택합니다.

비고

DHCP를 사용할 수 없고 장치가 고정 주소 대체를 사용하는 경우, 고정 주소는 제한된 범위로 구성됩니다.

IPv6

Assign IPv6 automatically(IPv6 자동 할당): IPv6을 켜고 네트워크 라우터가 장치에 IP 주소를 자동으로 할당하도록 하려면 선택합니다.

호스트 이름

호스트 이름을 자동으로 할당: 네트워크 라우터가 장치에 호스트 이름을 IP 주소를 자동으로 할당하도록 하려면 선택합니다.

호스트 이름: 장치에 액세스하는 다른 방법으로 사용하려면 호스트 이름을 수동으로 입력합니다. 서버 보고서 및 시스템 로그는 호스트 이름을 사용합니다. 허용되는 문자는 A~Z, a~z, 0~9, -입니다.

동적 DNS 업데이트 활성화: IP 주소가 변경될 때마다 장치에서 도메인 네임 서버 녹화를 자동으로 업데이트하도록 허용합니다.

DNS 이름 등록: 장치의 IP 주소를 가리키는 고유한 도메인 이름을 입력합니다. 허용되는 문자는 A~Z, a~z, 0~9, -입니다.

TTL: TTL(Time to Live)은 DNS 레코드가 업데이트되어야 할 때까지 유효하게 유지되는 기간을 설정합니다.

DNS 서버

Assign DNS automatically(DNA 자동 할당): DHCP 서버가 검색 도메인 및 DNS 서버 주소를 장치에 자동으로 할당하게 하려면 선택합니다. 대부분의 네트워크에 대해 자동 DNS(DHCP)를 권장합니다.

Search domains(도메인 검색): 정규화되지 않은 호스트 이름을 사용하는 경우 **Add search domain(검색 도메인 추가)**을 클릭하고 장치가 사용하는 호스트 이름을 검색할 도메인을 입력합니다.

DNS servers(DNS 서버): **Add DNS server(DNS 서버 추가)**를 클릭하고 DNS 서버의 IP 주소를 입력합니다. 이 서버는 네트워크에서 호스트 이름을 IP 주소로 변환하여 제공합니다.

비고

DHCP를 비활성화하면 호스트 이름, DNS 서버, NTP 등 자동 네트워크 구성에 의존하는 기능이 작동하지 않을 수 있습니다.

HTTP 및 HTTPS

HTTPS는 사용자의 페이지 요청 및 웹 서버에서 반환된 페이지에 대한 암호화를 제공하는 프로토콜입니다. 암호화된 정보 교환은 서버의 신뢰성을 보장하는 HTTPS 인증서를 사용하여 관리됩니다.

장치에서 HTTPS를 사용하려면 HTTPS 인증서를 설치해야 합니다. 인증서를 생성하고 설치하려면 **System > Security(시스템 > 보안)**로 이동합니다.

Allow access through(액세스 허용): 사용자가 **HTTP**, **HTTPS** 또는 **HTTP and HTTPS(HTTP 및 HTTPS)** 프로토콜 둘 다를 통해 장치에 연결하도록 허용할지 선택합니다.

비고

HTTPS를 통해 암호화된 웹 페이지를 보는 경우 특히 페이지를 처음 요청할 때 성능이 저하될 수 있습니다.

HTTP port(HTTP 포트): 사용할 HTTP 포트를 입력합니다. 장치는 포트 80 또는 1024-65535 범위의 모든 포트를 허용합니다. 관리자로 로그인한 경우 1-1023 범위의 포트를 입력할 수도 있습니다. 이 범위의 포트를 사용하면 경고가 표시됩니다.

HTTPS port(HTTPS 포트): 사용할 HTTPS 포트를 입력합니다. 장치는 포트 443 또는 1024-65535 범위의 모든 포트를 허용합니다. 관리자로 로그인한 경우 1-1023 범위의 포트를 입력할 수도 있습니다. 이 범위의 포트를 사용하면 경고가 표시됩니다.

Certificate(인증서): 장치에 HTTPS를 활성화하려면 인증서를 선택합니다.

네트워크 검색 프로토콜

Bonjour®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

Bonjour 이름: 네트워크에 표시할 이름을 입력합니다. 기본 이름은 장치 이름과 MAC 주소입니다.

UPnP®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

UPnP 이름: 네트워크에 표시할 이름을 입력합니다. 기본 이름은 장치 이름과 MAC 주소입니다.

WS-검색: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

LLDP 및 CDP: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다. LLDP 및 CDP를 끄면 PoE 전원 협상에 지장이 생길 수 있습니다. PoE 전원 협상과 관련한 문제를 해결하려면 하드웨어 PoE 전원 협상 전용으로 PoE 스위치를 구성합니다.

네트워크 포트

Power and ethernet(전원과 이더넷): 스위치 포트의 네트워크를 켜려면 이 옵션을 선택합니다.

Power only(전원 전용): 스위치 포트의 네트워크를 끄려면 이 옵션을 선택합니다. 포트는 여전히 이더넷을 통한 전원 공급을 제공합니다.

글로벌 프록시

Http proxy(Http 프록시): 허용된 형식에 따라 글로벌 프록시 호스트 또는 IP 주소를 지정합니다.

Https proxy(Https 프록시): 허용된 형식에 따라 글로벌 프록시 호스트 또는 IP 주소를 지정합니다.

HTTP 및 HTTPS 프록시에 허용되는 형식:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

비고

장치를 재시작하여 글로벌 프록시 설정을 적용합니다.

No proxy(프록시 없음): 글로벌 프록시를 우회하려면 **No proxy(프록시 없음)**를 사용합니다. 목록에 있는 옵션 중 하나를 입력하거나 쉼표로 구분하여 여러 개를 입력합니다.

- 비워두기
- IP 주소 지정
- CIDR 형식의 IP 주소 지정
- 도메인 이름 지정(예: www.<도메인 이름>.com).
- 특정 도메인의 모든 하위 도메인 지정(예: .<도메인 이름>.com).

One-Click Cloud Connection

One-click cloud connection(O3C)과 O3C 서비스는 어느 위치에서나 실시간 및 녹화 영상에 쉽고 안전한 인터넷 액세스를 제공합니다. 자세한 내용은 *axis.com/end-to-end-solutions/hosted-services*를 참조하십시오.

Allow O3C(O3C 허용):

- **One-click(원클릭)**: 기본 옵션입니다. O3C에 연결하려면 장치의 제어 버튼을 누릅니다. 장치 모델에 따라 상태 LED가 깜박일 때까지 버튼을 눌렀다 놓거나, 길게 누릅니다. **Always(항상)**를 활성화하고 연결 상태를 유지하려면 24시간 이내에 장치를 O3C 서비스에 등록합니다. 등록하지 않으면 장치의 O3C 연결이 끊어집니다.
- **항상**: 장치가 인터넷을 통해 O3C 서비스에 대한 연결을 지속적으로 시도합니다. 장치를 등록하면 연결 상태가 유지됩니다. 제어 버튼에 손이 닿지 않는 경우 이 옵션을 사용하십시오.
- **No(아니요)**: O3C 서비스를 연결 해제합니다.

Proxy settings (프록시 설정): 필요한 경우 프록시 설정을 입력하여 프록시 서버에 연결합니다.

호스트: 프록시 서버의 주소를 입력합니다.

Port(포트): 액세스에 사용되는 포트 번호를 입력하십시오.

로그인 및 **패스워드**: 필요한 경우 프록시 서버에 대한 사용자 이름 및 패스워드를 입력합니다.

Authentication method(인증 방법):

- **기본**: 이 방법은 HTTP에 대해 가장 호환성이 뛰어난 인증 체계입니다. 암호화되지 않은 사용자 이름과 패스워드를 서버로 전송하기 때문에 **Digest(다이제스트)** 방법보다 안전하지 않습니다.
- **다이제스트**: 이 방법은 항상 네트워크를 통해 암호화된 패스워드를 전송하기 때문에 더 안전합니다.
- **자동**: 이 옵션을 사용하면 지원되는 방법에 따라 장치가 인증 방법을 선택할 수 있습니다. 우선순위는 **다이제스트** 방법, **기본** 방법 순서로 설정합니다.

소유자 인증 키(OAK): 소유자 인증 키를 가져오려면 **Get key(키 가져 오기)**를 클릭합니다. 이것은 장치가 방화벽이나 프록시없이 인터넷에 연결된 경우에만 가능합니다.

SNMP

SNMP(Simple Network Management Protocol)를 이용하여 네트워크 장치를 원격으로 관리할 수 있습니다.

SNMP: 사용할 SNMP 버전을 선택합니다.

- **v1 및 v2c**:
  - **Read community(읽기 커뮤니티)**: 지원되는 모든 SNMP 객체에 대해 읽기 전용 권한이 있는 커뮤니티 이름을 입력합니다. 기본값은 **공개**입니다.
  - **Write community(쓰기 커뮤니티)**: 지원되는 모든 SNMP 객체에 대해 읽기 또는 쓰기 권한이 있는 커뮤니티 이름을 입력합니다(읽기 전용 객체 제외). 기본값은 **쓰기**입니다.
  - **Activate traps(트랩 활성화)**: 트랩보고를 활성화하려면 켜십시오. 장치는 트랩을 사용하여 중요한 이벤트 또는 상태 변경에 대한 메시지를 관리 시스템에 보냅니다. 웹 인터페이스에서 SNMP v1 및 v2c에 대한 트랩을 설정할 수 있습니다. SNMP v3으로 변경하거나 SNMP를 끄면 트랩이 자동으로 꺼집니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **Trap address(트랩 주소)**: 관리 서버의 IP 주소 또는 호스트 이름을 입력하십시오.
  - **Trap community(트랩 커뮤니티)**: 장치가 관리 시스템에 트랩 메시지를 보낼 때 사용할 커뮤니티를 입력합니다.
  - **Traps(트랩)**:
    - **Cold start(콜드 부팅)**: 장치가 시작될 때 트랩 메시지를 보냅니다.
    - **Link up(링크 업)**: 링크가 다운에서 업으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Link down(링크 다운)**: 링크가 업에서 다운으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Authentication failed(인증 실패)**: 인증 시도가 실패하면 트랩 메시지를 보냅니다.

비고

SNMP v1 및 v2c 트랩을 켜면 모든 Axis 비디오 MIB 트랩이 활성화됩니다. 자세한 내용은 *AXIS OS Portal> SNMP*를 참조하세요.

- **v3**: SNMP v3는 암호화 및 보안 암호를 제공하는 보다 안전한 버전입니다. SNMP v3를 사용하려면 암호가 HTTPS를 통해 전송되므로 HTTPS를 활성화하는 것이 좋습니다. 또한 권한이 없는 당사자가 암호화되지 않은 SNMP v1 및 v2c 트랩에 액세스하는 것을 방지합니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **개인정보 보호**: SNMP 데이터를 보호하는 데 사용할 암호화 방식을 선택하십시오.
  - **Password for the account "initial"('초기' 계정의 패스워드)**: 이름이 'initial'인 계정의 SNMP 패스워드를 입력합니다. HTTPS를 활성화하지 않고도 패스워드를 전송할 수 있지만 권장하지 않습니다. SNMP v3 패스워드는 한 번만 설정할 수 있고 HTTPS가 활성화된 경우에만 설정하는 것이 좋습니다. 패스워드를 설정하면 패스워드 필드가 더 이상 표시되지 않습니다. 패스워드를 다시 설정하려면 장치를 공장 기본 설정으로 재설정해야 합니다.

보안

인증서

인증서는 네트워크상의 장치를 인증하는 데 사용됩니다. 이 장치는 두 가지 유형의 인증서를 지원합니다.

- **Client/server certificates(클라이언트/서버 인증서)**
  클라이언트/서버 인증서는 장치의 ID를 검증하며 자체 서명할 수 있으며 CA(인증 기관)에서 발급할 수 있습니다. 자체 서명 인증서는 제한된 보호를 제공하며 CA 발행 인증서를 얻기 전까지 사용할 수 있습니다.
- **CA 인증서**
  CA 인증서를 사용하여 피어 인증서를 인증합니다. 예를 들어, 장치가 IEEE 802.1X로 보호되는 네트워크에 연결된 경우 인증 서버의 ID를 검증합니다. 장치에는 여러 개의 사전 설치된 CA 인증서가 있습니다.

지원되는 형식은 다음과 같습니다.

- 인증서 형식: .PEM, .CER, .PFX
- 개인 키 형식: PKCS#1 및 PKCS#12

중요 사항

장치를 공장 출하 시 기본값으로 재설정하면 모든 인증서가 삭제됩니다. 사전 설치된 CA 인증서가 다시 설치됩니다.

Add certificate(인증서 추가) : 인증서를 추가하려면 클릭합니다. 단계별 가이드가 열립니다.

- **More(더 보기)** : 작성하거나 선택할 추가 필드를 표시합니다.
- **Secure keystore(보안 키 저장소)**: 개인 키를 안전하게 저장하려면 **Trusted Execution Environment (SoC TEE)**, **Secure element(보안 요소)** 또는 **Trusted Platform Module 2.0**을 선택합니다. 선택할 보안 키 저장소에 대한 자세한 내용을 보려면 *help.axis.com/axis-os#cryptographic-support*를 참조하십시오.
- **Key type(키 유형)**: 인증서를 보호하려면 드롭다운 목록에서 기본 암호화 알고리즘이나 다른 암호화 알고리즘을 선택합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Certificate information(인증서 정보)**: 설치된 인증서의 속성을 봅니다.
- **Delete certificate(인증서 삭제)**: 인증서를 삭제하십시오.
- **Create certificate signing request(인증서 서명 요청 생성)**: 디지털 ID 인증서를 신청하기 위해 등록 기관에 보낼 인증서 서명 요청을 생성합니다.

Secure keystore(보안 키 저장소):

- **Trusted Execution Environment (SoC TEE)**: 보안 키 저장소로 SoC TEE를 사용하려면 선택합니다.
- **Secure element(보안 요소)(CC EAL6+, FIPS 140-3 Level 3)**: 보안 키 저장소에 보안 요소를 사용하려면 선택합니다.
- **Trusted Platform Module 2.0(CC EAL4+, FIPS 140-2 레벨 2)**: 보안 키 저장소에 TPM 2.0을 사용하려면 선택합니다.

암호화 정책

암호화 정책은 데이터 보호를 위해 암호화를 사용하는 방법을 정의합니다.

Active(활성화): 장치에 적용할 암호화 정책을 선택합니다.

- **Default — OpenSSL(기본값 — OpenSSL)**: 일반적인 사용을 위한 균형 잡힌 보안 및 성능.
- **FIPS — Policy to comply with FIPS 140–2(FIPS — FIPS 140-2를 준수하는 정책)**: 규제 대상 산업을 위한 FIPS 140-2를 준수하는 암호화입니다.

네트워크 접근 제어 및 암호화

IEEE 802.1x

IEEE 802.1x는 유선 및 무선 네트워크 장치의 보안 인증을 제공하는 포트 기반 네트워크 승인 제어를 위한 IEEE 표준입니다. IEEE 802.1x는 EAP(Extensible Authentication Protocol)를 기준으로 합니다.

IEEE 802.1X로 보호되는 네트워크에 액세스하려면 네트워크 장치가 자체적으로 인증되어야 합니다. 인증은 인증 서버에서 수행되며, 일반적으로 RADIUS 서버(예: FreeRADIUS 및 Microsoft Internet Authentication Server)입니다.

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec은 미디어 액세스 독립 프로토콜을 위한 비연결형 데이터 기밀성 및 무결성을 정의하는 IEEE의 MAC(미디어 액세스 컨트롤) 보안 표준입니다.

인증서

CA 인증서 없이 구성하면 서버 인증서 유효성 검사가 비활성화되고 장치는 연결된 네트워크에 관계없이 자체 인증을 시도합니다.

인증서를 사용할 때 Axis 구현 시 장치 및 인증 서버는 EAP-TLS(확장 가능 인증 프로토콜 - 전송 계층 보안)를 사용하여 디지털 인증서로 자체적으로 인증합니다.

장치가 인증서를 통해 보호되는 네트워크에 액세스할 수 있도록 하려면 서명된 클라이언트 인증서를 장치에 설치해야 합니다.

Authentication method(인증 방법): 인증에 사용되는 EAP 유형을 선택합니다.

Client Certificate(클라이언트 인증서): IEEE 802.1x를 사용할 클라이언트 인증서를 선택합니다. 인증 서버는 인증서를 사용하여 클라이언트의 ID를 확인합니다.

CA 인증서: CA 인증서를 선택하여 인증 서버의 ID를 확인합니다. 인증서를 선택하지 않으면 장치는 연결된 네트워크에 관계없이 자체 인증을 시도합니다.

EAP identity(EAP ID): 클라이언트 인증서와 연관된 사용자 ID를 입력하십시오.

EAPOL version(EAPOL 버전): 네트워크 스위치에서 사용되는 EAPOL 버전을 선택합니다.

Use IEEE 802.1x(IEEE 802.1x 사용): IEEE 802.1x 프로토콜을 사용하려면 선택합니다.

인증 방법으로 **IEEE 802.1x PEAP-MSCHAPv2**를 사용하는 경우에만 이러한 설정을 이용할 수 있습니다.

- **패스워드**: 해당 사용자 ID의 패스워드를 입력합니다.
- **Peap version(Peap 버전)**: 네트워크 스위치에서 사용되는 Peap 버전을 선택합니다.
- **Label(라벨)**: 클라이언트 EAP 암호화를 사용하려면 1을 선택하고, 클라이언트 PEAP 암호화를 사용하려면 2를 선택합니다. Peap 버전 1을 사용하는 경우 네트워크 스위치가 사용하는 라벨을 선택합니다.

IEEE 802.1ae MACsec(정적 CAK/사전 공유 키)를 인증 방법으로 사용하는 경우에만 이러한 설정을 이용할 수 있습니다.

- **키 일치 연결 관련 키 이름**: 연결 관련 이름(CKN)을 입력합니다. 2 ~ 64자(2로 분할 가능) 16진수여야 합니다. CKN은 연결 관련에서 수동으로 구성해야 하며, 처음에 MACsec을 활성화하려면 링크의 양쪽 끝에서 일치해야 합니다.
- **키 일치 연결 관련 키**: 연결 관련 키(CAK)를 입력합니다. 32자 또는 64자의 16진수여야 합니다. CAK는 연결 관련에서 수동으로 구성해야 하며, 처음에 MACsec을 활성화하려면 링크의 양쪽 끝에서 일치해야 합니다.

무차별 대입 공격 방지

Blocking(차단 중): 무차별 대입 공격을 차단하려면 켜십시오. 무차별 대입 공격은 시행 착오를 통해 로그인 정보 또는 암호화 키를 추측합니다.

차단 기간: 무차별 대입 공격을 차단할 시간(초)을 입력합니다.

차단 조건: 블록이 시작되기 전에 허용되는 초당 인증 실패 횟수를 입력합니다. 페이지 수준과 장치 수준 모두에서 허용되는 실패 수를 설정할 수 있습니다.

방화벽

Firewall(방화벽): 방화벽을 활성화하려면 켭니다.

Default Policy(기본 정책): 룰에서 다루지 않는 연결 요청을 방화벽이 어떻게 처리할지 선택합니다.

- **ACCEPT(수락):** 장치에 대한 모든 연결을 허용합니다. 이 옵션은 기본 설정되어 있습니다.
- **DROP(거부):** 장치에 대한 모든 연결을 차단합니다.

기본 정책에 예외를 적용하려면 특정 주소, 프로토콜 및 포트에서 장치에 대한 연결을 허용하거나 차단하는 룰을 생성할 수 있습니다.

+ New rule(새 룰 추가): 룰을 생성하려면 클릭합니다.

Rule type(룰 유형):

- **FILTER(필터)**: 룰에 정의된 기준과 일치하는 장치의 연결을 허용하거나 차단하도록 선택합니다.
  - **정책**: 방화벽 룰에 대해 **Accept(수락)** 또는 **Drop(거부)**을 선택합니다.
  - **IP range(IP 범위)**: 허용하거나 차단할 주소 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에서 IPv4/IPv6를 사용합니다.
  - **IP 주소**: 허용하거나 차단하려는 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
  - **Protocol(프로토콜)**: 허용하거나 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우, 포트도 지정해야 합니다.
  - **MAC**: 허용하거나 차단하려는 장치의 MAC 주소를 입력합니다.
  - **Port range(포트 범위)**: 허용하거나 차단할 포트 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
  - **Port(포트)**: 허용하거나 차단하려는 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
  - **Traffic type(트래픽 유형)**: 허용하거나 차단하려는 트래픽 유형을 선택합니다.
    - **UNICAST(유니캐스트)**: 단일 발신자가 단일 수신자에게 보내는 트래픽입니다.
    - **BROADCAST(브로드캐스트)**: 단일 발신자가 네트워크의 모든 장치로 보내는 트래픽입니다.
    - **MULTICAST(멀티캐스트)**: 하나 이상의 발신자가 하나 이상의 수신자에게 보내는 트래픽입니다.
- **LIMIT(제한)**: 룰에 정의된 기준과 일치하는 장치의 연결을 수락하지만 과도한 트래픽을 줄이기 위해 제한을 적용하려면 선택합니다.
  - **IP range(IP 범위)**: 허용하거나 차단할 주소 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에서 IPv4/IPv6를 사용합니다.
  - **IP 주소**: 허용하거나 차단하려는 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
  - **Protocol(프로토콜)**: 허용하거나 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우, 포트도 지정해야 합니다.
  - **MAC**: 허용하거나 차단하려는 장치의 MAC 주소를 입력합니다.
  - **Port range(포트 범위)**: 허용하거나 차단할 포트 범위를 지정하도록 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
  - **Port(포트)**: 허용하거나 차단하려는 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
  - **Unit(단위)**: 허용하거나 차단할 연결의 유형을 선택합니다.
  - **Period(기간)**: **Amount(횟수)**와 관련된 시간 기간을 선택합니다.
  - **Amount(횟수)**: 설정된 **Period(기간)** 내에 장치가 연결할 수 있는 최대 횟수를 설정합니다. 최대 값은 65535입니다.

- **Burst(버스트)**: 설정된 **Period(기간)** 동안 한 번 설정된 **Amount(횟수)**를 초과할 수 있는 연결 횟수를 입력합니다. 설정된 횟수에 도달하면, 이후에는 설정된 기간 동안 설정된 횟수만 허용됩니다.
- **Traffic type(트래픽 유형)**: 허용하거나 차단하려는 트래픽 유형을 선택합니다.
  - **UNICAST(유니캐스트)**: 단일 발신자가 단일 수신자에게 보내는 트래픽입니다.
  - **BROADCAST(브로드캐스트)**: 단일 발신자가 네트워크의 모든 장치로 보내는 트래픽입니다.
  - **MULTICAST(멀티캐스트)**: 하나 이상의 발신자가 하나 이상의 수신자에게 보내는 트래픽입니다.

Test rules(룰 테스트): 정의한 룰을 테스트하려면 클릭합니다.

- **Test time in seconds(초 단위 테스트 시간)**: 룰 테스트에 대한 시간 제한을 설정합니다.
- **Roll back(롤백)**: 룰을 테스트하기 전의 이전 상태로 방화벽을 롤백하려면 클릭합니다.
- **Apply rules(룰 적용)**: 테스트하지 않고 룰을 활성화하려면 클릭합니다. 이렇게 하는 것은 권장하지 않습니다.

사용자 지정 서명된 AXIS OS 인증서

장치에 Axis의 테스트 소프트웨어 또는 기타 사용자 지정 소프트웨어를 설치하려면 사용자 지정 서명된 AXIS OS 인증서가 필요합니다. 인증서는 소프트웨어가 장치 소유자와 Axis 모두에 의해 승인되었는지 확인합니다. 소프트웨어는 고유한 일련 번호와 칩 ID로 식별되는 특정 장치에서만 실행할 수 있습니다. Axis가 서명을 위한 키를 보유하고 있으므로 Axis만이 사용자 지정 서명된 AXIS OS 인증서를 생성할 수 있습니다.

Install(설치): 인증서를 설치하려면 클릭합니다. 소프트웨어를 설치하기 전에 인증서를 설치해야 합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Delete certificate(인증서 삭제)**: 인증서를 삭제하십시오.

계정

계정

Add account(계정 추가): 새 계정을 추가하려면 클릭합니다. 최대 100개의 계정을 추가할 수 있습니다.

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 패스워드): 계정의 패스워드를 입력합니다. 패스워드는 1~64자 길이여야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 패스워드에 사용할 수 있습니다.

Repeat password(패스워드 반복): 동일한 패스워드를 다시 입력하십시오.

Privileges(권한):

- **Administrator(관리자)**: 모든 설정에 완전히 액세스합니다. 관리자는 다른 계정을 추가, 업데이트 및 제거할 수 있습니다.
- **Operator(운영자)**: 다음을 제외한 모든 설정에 액세스할 수 있습니다.
  - 모든 **System(시스템)** 설정
- **Viewer(뷰어)**: 설정을 변경할 수 있는 권한이 없습니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Update account(계정 업데이트): 계정 속성을 편집합니다.

Delete account(계정 삭제): 계정을 삭제합니다. root 계정은 삭제할 수 없습니다.

익명의 액세스

Allow anonymous viewing(익명 보기 허용): 계정으로 로그인하지 않고도 누구나 관찰자로 장치에 액세스할 수 있도록 설정합니다.

Allow anonymous PTZ operating(익명의 PTZ 운영 허용) : 익명의 사용자가 이미지에 대해 팬, 틸트 및 줌을 할 수 있도록 하려면 켭니다.

SSH 계정

Add SSH account(SSH 계정 추가): 새 SSH 계정을 추가하려면 클릭합니다.

- **Enable SSH(SSH 활성화)**: SSH 서비스를 사용하려면 켭니다.

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 패스워드): 계정의 패스워드를 입력합니다. 패스워드는 1~64자 길이여야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 패스워드에 사용할 수 있습니다.

Repeat password(패스워드 반복): 동일한 패스워드를 다시 입력하십시오.

설명: 설명을 입력합니다(옵션).

상황에 맞는 메뉴에는 다음이 포함됩니다.

Update SSH account(SSH 계정 업데이트): 계정 속성을 편집합니다.

Delete SSH account(SSH 계정 삭제): 계정을 삭제합니다. root 계정은 삭제할 수 없습니다.

가상 호스트

Add virtual host(가상 호스트 추가): 새 가상 호스트를 추가하려면 클릭합니다.

활성화: 이 가상 호스트를 사용하려면 선택합니다.

서버 이름: 서버의 이름을 입력합니다. 숫자 0-9, 문자 A-Z 및 하이픈(-)만 사용합니다.

Port(포트): 서버가 연결된 포트를 입력합니다.

Type(유형): 사용할 인증 유형을 선택합니다. **Basic(기본)**, **Digest(다이제스트)**, **Open ID**, **Client Credential Grant(클라이언트 자격 증명 부여)** 중에서 선택합니다.

HTTPS: HTTPS를 사용하려면 선택합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **가상 호스트 업데이트**
- **가상 호스트 삭제**

클라이언트 자격 증명 부여 구성

Admin claim(관리자 요청): 관리자 역할의 값을 입력합니다.

Verification URI(검증 URI): API 엔드포인트 인증을 위한 웹 링크를 입력합니다.

Operator claim(운영자 요청): 운영자 역할의 값을 입력합니다.

Require claim(요청 필요): 토큰에 있어야 하는 데이터를 입력합니다.

Viewer claim(관찰자 요청): 관찰자 역할의 값을 입력합니다.

Save(저장): 값을 저장하려면 클릭합니다.

OpenID 구성

중요 사항

OpenID를 사용하여 로그인할 수 없는 경우 OpenID를 구성하여 로그인할 때 사용한 다이제스트 또는 기본 자격 증명을 사용합니다.

Client ID(클라이언트 ID): OpenID 사용자 이름을 입력합니다.

Outgoing Proxy(발신 프록시): 프록시 서버를 사용하려면 OpenID 연결을 위한 프록시 주소를 입력합니다.

Admin claim(관리자 요청): 관리자 역할의 값을 입력합니다.

Provider URL(공급자 URL): API 엔드포인트 인증을 위한 웹 링크를 입력합니다. https://[insert URL]/.well-known/openid-configuration 형식이어야 함

Operator claim(운영자 요청): 운영자 역할의 값을 입력합니다.

Require claim(요청 필요): 토큰에 있어야 하는 데이터를 입력합니다.

Viewer claim(관찰자 요청): 관찰자 역할의 값을 입력합니다.

Remote user(원격 사용자): 원격 사용자를 식별하는 값을 입력합니다. 이는 장치의 웹 인터페이스에 현재 사용자를 표시하는 데 유용합니다.

Scopes(범위): 토큰의 일부가 될 수 있는 선택적 범위입니다.

Client secret(클라이언트 비밀): OpenID 패스워드 입력

Save(저장): OpenID 값을 저장하려면 클릭합니다.

Enable OpenID(OpenID 활성화): 현재 연결을 닫고 공급자 URL에서 장치 인증을 허용하려면 켭니다.

이벤트

룰

룰은 액션을 수행하기 위해 제품에 대해 트리거되는 조건을 정의합니다. 목록에는 제품에 현재 구성된 모든 룰이 표시됩니다.

비고

최대 256개의 액션 룰을 생성할 수 있습니다.

Add a rule(룰 추가): 룰을 생성합니다.

이름: 룰에 대한 이름을 입력합니다.

Wait between actions(액션 대기 간격): 룰 활성화 사이에 통과해야 하는 최소 시간(hh:mm:ss)을 입력합니다. 룰이 예를 들어 주야간 모드 조건에 의해 활성화된 경우, 일출과 일몰 동안 작은 조명 변화가 룰을 반복적으로 활성화하는 것을 피하기 위해 유용합니다.

Condition(조건): 목록에서 조건을 선택합니다. 장치가 작업을 수행하려면 조건이 충족되어야 합니다. 여러 조건이 정의된 경우 액션을 트리거하려면 모든 조건이 충족되어야 합니다. 특정 조건에 대한 정보는 *이벤트 규칙 시작하기*를 참조하십시오.

Use this condition as a trigger(이 조건을 트리거로 사용): 이 첫 번째 조건이 시작 트리거로만 작동하도록 하려면 선택합니다. 이는 룰이 활성화되면 첫 번째 조건의 상태에 관계없이 다른 모든 조건이 충족되는 한 활성 상태를 유지한다는 의미입니다. 이 옵션을 선택하지 않으면 모든 조건이 충족될 때마다 룰이 활성 상태가 됩니다.

Invert this condition(이 조건 반전): 선택한 것과 반대되는 조건을 원하면 선택하십시오.

Add a condition(조건 추가): 추가 조건을 추가하려면 클릭하세요.

Action(액션): 목록에서 작업을 선택하고 필수 정보를 입력합니다. *이벤트 규칙 시작하기*에서 특정 액션에 대한 정보를 알아보십시오.

제품에는 다음과 같은 사전 구성된 룰 중 일부가 있을 수 있습니다.

Front-facing LED Activation: LiveStream(전면 LED 작동: LiveStream): 마이크가 켜져 있고 라이브 스트림이 수신되면 오디오 장치의 전면 LED가 녹색으로 바뀝니다.

Front-facing LED Activation: Recording(전면 LED 작동: 녹화): 마이크가 켜져 있고 녹음이 진행 중이면 오디오 장치의 전면 LED가 녹색으로 바뀝니다.

Front-facing LED Activation: SIP(전면 LED 작동: SIP) : 마이크가 켜져 있고 SIP 통화가 활성화되면 오디오 장치의 전면 LED가 녹색으로 바뀝니다. 오디오 장치에서 SIP를 활성화해야 이 이벤트를 트리거할 수 있습니다.

Pre-announcement tone: Play tone on incoming call(안내 방송 전 신호음: 전화 수신 시 신호음 재생): 오디오 장치에 SIP 호출이 이루어지면 장치가 사전 정의된 오디오 클립을 재생합니다. 오디오 장치에 대해 SIP를 활성화해야 합니다. 오디오 장치에서 오디오 클립이 재생되는 동안 SIP 발신자가 벨소리를 듣게 하려면 장치가 자동으로 통화에 응답하지 않도록 SIP 계정을 구성해야 합니다.

Pre-announcement tone: Answer call after incoming call-tone(안내 방송 전 신호음: 수신 전화 신호음 후 전화 응답): 오디오 클립이 끝나면 수신 SIP 호출에 응답합니다. 오디오 장치에 대해 SIP를 활성화해야 합니다.

Loud ringer(시끄러운 벨소리): 오디오 장치에 SIP 호출이 발생하면 룰이 활성화되어 있는 동안 사전 정의된 오디오 클립이 재생됩니다. 오디오 장치에 대해 SIP를 활성화해야 합니다.

수신 장치

이벤트에 대해 수신자에게 알리거나 파일을 보내도록 장치를 설정할 수 있습니다.

비고

FTP 또는 SFTP를 사용하도록 장치를 설정한 경우 파일 이름에 추가된 고유 시퀀스 번호를 변경하거나 제거하지 마십시오. 변경하거나 제거하면 이벤트당 하나의 이미지만 전송할 수 있습니다.

목록에는 구성에 대한 정보와 함께 현재 제품에 구성된 모든 수신자가 표시됩니다.

비고

최대 20개의 수신자를 생성할 수 있습니다.

Add a recipient(수신자 추가): 수신자를 추가하려면 클릭합니다.

이름: 수신자의 이름을 입력합니다.

Type(유형): 목록에서 선택:

- **FTP**
  - **호스트**: 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System > Network > IPv4 and IPv6(시스템 > 네트워크 > IPv4 및 IPv6)** 아래에 지정되어 있는지 확인하십시오.
  - **Port(포트)**: FTP 서버가 사용하는 포트 번호를 입력합니다. 기본값은 21입니다.
  - **Folder(폴더)**: 파일을 저장할 디렉토리의 경로를 입력하십시오. 디렉토리가 FTP 서버에 이미 존재하지 않으면, 파일을 업로드할 때 오류 메시지가 표시됩니다.
  - **Username(사용자 이름)**: 로그인하려면 사용자 이름을 입력하십시오.
  - **패스워드**: 로그인하려면 패스워드를 입력하십시오.
  - **Use temporary file name(임시 파일 이름 사용)**: 자동으로 생성된 임시 파일 이름으로 파일을 업로드하려면 선택합니다. 업로드를 완료하면 파일 이름이 원하는 이름으로 바뀝니다. 업로드가 중단된 경우 손상된 파일이 없습니다. 그러나 여전히 임시 파일을 얻을 수 있습니다. 이렇게 하면 원하는 이름을 가진 모든 파일이 올바른지 알 수 있습니다.
  - **Use passive FTP(수동 FTP 사용)**: 정상적인 상황에서 제품은 단순히 대상 FTP 서버에 데이터 연결을 열도록 요청합니다. 장치가 대상 서버에 대한 FTP 제어 및 데이터 연결을 모두 적극적으로 시작합니다. 이는 일반적으로 장치와 대상 FTP 서버 사이에 방화벽이 있는 경우에 필요합니다.
- **HTTP**
  - **URL**: HTTP 서버에 대한 네트워크 주소와 요청을 처리할 스크립트를 입력합니다. 예를 들면 http://192.168.254.10/cgi-bin/notify.cgi입니다.
  - **Username(사용자 이름)**: 로그인하려면 사용자 이름을 입력하십시오.
  - **패스워드**: 로그인하려면 패스워드를 입력하십시오.
  - **Proxy(프록시)**: HTTP 서버에 연결하기 위해 프록시 서버를 통과해야 하는 경우 필요한 정보를 켜고 입력합니다.
- **HTTPS**
  - **URL**: HTTPS 서버에 대한 네트워크 주소와 요청을 처리할 스크립트를 입력합니다. 예를 들면 https://192.168.254.10/cgi-bin/notify.cgi입니다.
  - **Validate server certificate(서버 인증서 확인)**: 이 상자를 선택하여 HTTPS 서버가 생성한 인증서를 선택합니다.
  - **Username(사용자 이름)**: 로그인하려면 사용자 이름을 입력하십시오.
  - **패스워드**: 로그인하려면 패스워드를 입력하십시오.
  - **Proxy(프록시)**: HTTPS 서버에 연결하기 위해 프록시 서버를 통과해야 하는 경우 필요한 정보를 켜고 입력합니다.
- **네트워크 스토리지**
  NAS(Network-Attached Storage)와 같은 네트워크 스토리지를 추가하여 파일을 저장하는 수신자로 사용할 수 있습니다. 파일은 MKV(Matroska) 파일 형식으로 저장됩니다.
  - **호스트**: 네트워크 스토리지의 IP 주소나 호스트 이름을 입력합니다.
  - **Share(공유)**: 호스트에서 공유 이름을 입력합니다.
  - **Folder(폴더)**: 파일을 저장할 디렉토리의 경로를 입력하십시오.
  - **Username(사용자 이름)**: 로그인하려면 사용자 이름을 입력하십시오.

- **패스워드**: 로그인하려면 패스워드를 입력하십시오.

- **SFTP**
  - **호스트**: 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System > Network > IPv4 and IPv6(시스템 > 네트워크 > IPv4 및 IPv6)** 아래에 지정되어 있는지 확인하십시오.
  - **Port(포트)**: SFTP 서버가 사용하는 포트 번호를 입력합니다. 기본값은 22입니다.
  - **Folder(폴더)**: 파일을 저장할 디렉토리의 경로를 입력하십시오. 디렉토리가 SFTP 서버에 이미 존재하지 않으면, 파일을 업로드할 때 오류 메시지가 표시됩니다.
  - **Username(사용자 이름)**: 로그인하려면 사용자 이름을 입력하십시오.
  - **패스워드**: 로그인하려면 패스워드를 입력하십시오.
  - **SSH 호스트 공개 키 유형(MD5)**: 원격 호스트 공개 키(32자리 16진수 문자열)의 지문을 입력합니다. SFTP 클라이언트는 RSA, DSA, ECDSA 및 ED25519 호스트 키 유형의 SSH-2를 사용하는 SFTP 서버를 지원합니다. 협상 시 RSA가 선호되는 방법이며 ECDSA, ED25519 및 DSA가 그 뒤를 따릅니다. SFTP 서버에서 사용하는 올바른 MD5 호스트 키를 입력해야 합니다. Axis 장치는 MD5 및 SHA-256 해시 키를 모두 지원하지만 MD5보다 강력한 보안을 위해 SHA-256를 사용하는 것이 좋습니다. Axis 장치로 SFTP 서버를 구성하는 방법에 대한 자세한 내용은 *AXIS OS 포털*을 참고하십시오.
  - **SSH 호스트 공개 키 유형(SHA256)**: 원격 호스트 공개 키(43자리 Base64 인코딩 문자열)의 지문을 입력합니다. SFTP 클라이언트는 RSA, DSA, ECDSA 및 ED25519 호스트 키 유형의 SSH-2를 사용하는 SFTP 서버를 지원합니다. 협상 시 RSA가 선호되는 방법이며 ECDSA, ED25519 및 DSA가 그 뒤를 따릅니다. SFTP 서버에서 사용하는 올바른 MD5 호스트 키를 입력해야 합니다. Axis 장치는 MD5 및 SHA-256 해시 키를 모두 지원하지만 MD5보다 강력한 보안을 위해 SHA-256를 사용하는 것이 좋습니다. Axis 장치로 SFTP 서버를 구성하는 방법에 대한 자세한 내용은 *AXIS OS 포털*을 참고하십시오.
  - **Use temporary file name(임시 파일 이름 사용)**: 자동으로 생성된 임시 파일 이름으로 파일을 업로드하려면 선택합니다. 업로드를 완료하면 파일 이름이 원하는 이름으로 바뀝니다. 업로드가 중단된 경우, 손상된 파일이 없습니다. 그러나 여전히 임시 파일을 얻을 수 있습니다. 이렇게 하면 원하는 이름을 가진 모든 파일이 올바른지 알 수 있습니다.

- **SIP or VMS(SIP 또는 VMS)** :
  SIP: SIP 전화를 걸려면 선택합니다.
  VMS: VMS 전화를 걸려면 선택합니다.
  - **From SIP account(발신자 SIP 계정)**: 목록에서 선택합니다.
  - **To SIP address(수신자 SIP 주소)**: SIP 주소를 입력합니다.
  - **Test(테스트)**: 통화 설정이 작동하는지 테스트하려면 클릭합니다.
- **이메일**
  - **Send email to(이메일 전송 대상)**: 이메일을 전송할 이메일 주소를 입력합니다. 주소를 여러 개 입력하려면 쉼표로 이메일 주소를 구분하십시오.
  - **Send email from(이메일 발신)**: 보내는 서버의 이메일 주소를 입력합니다.
  - **Username(사용자 이름)**: 메일 서버의 사용자 이름을 입력합니다. 이메일 서버에서 인증을 요구하지 않는 경우 이 필드를 비워 둡니다.
  - **패스워드**: 메일 서버의 패스워드를 입력합니다. 이메일 서버에서 인증을 요구하지 않는 경우 이 필드를 비워 둡니다.
  - **Email server (SMTP)(이메일 서버(SMTP))**: 예를 들어 smtp.gmail.com, smtp.mail.yahoo.com과 같은 SMTP 서버 이름을 입력합니다.
  - **Port(포트)**: 0-65535 범위의 값을 사용하여 SMTP 서버의 포트 번호를 입력합니다. 기본값은 587입니다.

- **Encryption(암호화)**: 암호화를 사용하려면, SSL 또는 TLS를 선택하십시오.
- **Validate server certificate(서버 인증서 확인)**: 암호화를 사용하는 경우 장치의 ID를 확인하도록 선택합니다. 이 인증서는 CA(인증 기관)에서 자체 서명하거나 발행할 수 있습니다.
- **POP authentication(POP 인증)**: POP 서버 이름을 입력하려면 켜십시오(예: pop.gmail.com).

비고

일부 이메일 공급자는 예약된 이메일과 그와 유사한 형태를 수신하면서 사용자가 용량이 큰 첨부 파일을 받거나 보는 것을 제한하기 위해 보안 필터를 사용합니다. 이메일 제공업체의 보안 정책을 확인하여 이메일 계정이 잠기거나 예상 이메일을 놓치는 일이 없도록 하십시오.

- **TCP**
  - **호스트**: 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System > Network > IPv4 and IPv6(시스템 > 네트워크 > IPv4 및 IPv6)** 아래에 지정되어 있는지 확인하십시오.
  - **Port(포트)**: 서버 액세스에 사용되는 포트 번호를 입력합니다.

Test(테스트): 설정을 테스트하려면 클릭합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

View recipient(수신자 보기): 모든 수신자 세부 정보를 보려면 클릭합니다.

Copy recipient(수신자 복사): 수신자를 복사하려면 클릭하세요. 복사할 때 새로 수신자를 변경할 수 있습니다.

Delete recipient(수신자 삭제): 수신자를 영구적으로 삭제하려면 클릭합니다.

일정

일정과 펄스를 룰에서 조건으로 사용할 수 있습니다. 목록에는 구성에 대한 정보와 함께 현재 제품에 구성된 모든 일정과 펄스가 표시됩니다.

+ **Add schedule(스케줄 추가)**: 일정 또는 펄스를 생성하려면 클릭합니다.

수동 트리거

수동 트리거를 사용하여 룰을 수동으로 트리거할 수 있습니다. 예를 들어 수동 트리거로 제품 설치 및 구성하는 동안 액션을 검증할 수 있습니다.

MQTT

MQTT(Message Queuing Telemetry Transport)는 사물 인터넷(IoT)을 위한 표준 메시징 프로토콜입니다. 단순화된 IoT 통합을 위해 설계되었으며 작은 코드 공간(small code footprint)과 최소 네트워크 대역폭으로 원격 장치를 연결하기 위해 다양한 산업에서 사용됩니다. Axis 장치 소프트웨어의 MQTT 클라이언트를 통해 장치에서 생성된 데이터 및 이벤트를 영상 관리 소프트웨어(VMS)가 아닌 시스템에 간편하게 통합할 수 있습니다.

장치를 MQTT 클라이언트로 설정합니다. MQTT 통신은 클라이언트와 브로커라는 두 엔터티를 기반으로 합니다. 클라이언트는 메시지를 보내고 받을 수 있습니다. 브로커는 클라이언트 간의 메시지 라우팅을 담당합니다.

*AXIS OS 지식 베이스*에서 MQTT에 대해 자세히 알아볼 수 있습니다.

ALPN

ALPN은 클라이언트 및 서버 간 연결의 핸드셰이크 단계에서 애플리케이션 프로토콜을 선택할 수 있게 하는 TLS/SSL 확장입니다. 이는 HTTP와 같이 다른 프로토콜에 사용되는 동일한 포트를 통해 MQTT 트래픽을 활성화하는 데 사용됩니다. 경우에 따라 MQTT 통신 전용으로 개방된 포트가 없을 수도 있습니다. 그러한 경우의 해결책은 ALPN을 사용해서 방화벽에서 허용되는 표준 포트에서 MQTT를 애플리케이션 프로토콜로 사용할지를 결정하는 것입니다.

MQTT 클라이언트

Connect(연결): MQTT 클라이언트를 켜거나 끕니다.

Status(상태): MQTT 클라이언트의 현재 상태를 표시합니다.

브로커

호스트: MQTT 서버의 호스트 이름 또는 IP 주소를 입력하십시오.

Protocol(프로토콜): 사용할 프로토콜을 선택합니다.

Port(포트): 포트 번호를 입력합니다.

- 1883은 **MQTT over TCP(TCP를 통한 MQTT)**의 기본값입니다.
- 8883은 **SSL를 통한 MQTT**의 기본값입니다.
- 80은 **웹 소켓을 통한 MQTT**의 기본값입니다.
- 443은 **웹 소켓 보안을 통한 MQTT**의 기본값입니다.

ALPN protocol(ALPN 프로토콜): MQTT 브로커 공급자가 제공한 ALPN 프로토콜 이름을 입력합니다. 이는 SSL을 통한 MQTT 및 웹 소켓 보안을 통한 MQTT에만 적용됩니다.

Username(사용자 이름): 클라이언트에서 서버에 액세스하기 위해 사용할 사용자 이름을 입력합니다.

패스워드: 사용자 이름의 패스워드를 입력합니다.

Client ID(클라이언트 ID): 클라이언트 ID를 입력하십시오. 클라이언트 식별자는 클라이언트가 서버에 연결할 때 서버로 전송됩니다.

Clean session(클린 세션): 연결 및 연결 해제 시의 동작을 제어합니다. 선택하면 연결 및 연결 해제 시 상태 정보가 삭제됩니다.

HTTP proxy(HTTP 프록시): 최대 길이가 255바이트인 URL입니다. HTTP 프록시를 사용하지 않으려면 필드를 비워 둘 수 있습니다.

HTTPS proxy(HTTPS 프록시): 최대 길이가 255바이트인 URL입니다. HTTPS 프록시를 사용하지 않으려면 필드를 비워 둘 수 있습니다.

Keep alive interval(간격 유지): 클라이언트가 긴 TCP/IP 시간 제한를 기다릴 필요 없이 서버를 더 이상 사용할 수 없는 시점을 감지할 수 있습니다.

Timeout(시간 제한): 연결이 완료되는 시간 간격(초)입니다. 기본값: 60

장치 항목 접두사: **MQTT 클라이언트** 탭의 연결 메시지 및 LWT 메시지의 주제에 대한 기본값과 **MQTT 발행** 탭의 게시 조건에서 사용됩니다.

Reconnect automatically(자동으로 재연결): 연결 해제 후 클라이언트가 자동으로 다시 연결해야 하는지 여부를 지정합니다.

메시지 연결

연결이 설정될 때 메시지를 보낼지 여부를 지정합니다.

Send message(메시지 전송): 메시지를 보내려면 사용 설정하세요.

Use default(기본값 사용): 자신의 기본 메시지를 입력하려면 끄십시오.

Topic(주제): 기본 메시지의 주제를 입력합니다.

Payload(페이로드): 기본 메시지의 내용을 입력합니다.

Retain(유지): 이 **Topic(주제)**에서 클라이언트 상태를 유지하려면 선택합니다.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

마지막 유언 메시지

마지막 유언(LWT)을 사용하면 클라이언트가 브로커에 연결될 때 자격 증명과 함께 유언을 제공할 수 있습니다. 클라이언트가 나중에 어느 시점에서 비정상적으로 연결이 끊어지면(전원이 끊어졌기 때문일 수 있음) 브로커가 다른 클라이언트에 메시지를 전달할 수 있습니다. 이 LWT 메시지는 일반 메시지와 동일한 형식이며 동일한 메커니즘을 통해 라우팅됩니다.

Send message(메시지 전송): 메시지를 보내려면 사용 설정하세요.

Use default(기본값 사용): 자신의 기본 메시지를 입력하려면 끄십시오.

Topic(주제): 기본 메시지의 주제를 입력합니다.

Payload(페이로드): 기본 메시지의 내용을 입력합니다.

Retain(유지): 이 **Topic(주제)**에서 클라이언트 상태를 유지하려면 선택합니다.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

MQTT 발행

기본 주제 접두사 사용: **MQTT client(MQTT 클라이언트)** 탭에서 장치 주제 접두사에 정의된 기본 주제 접두사를 사용하려면 선택합니다.

Include condition(조건 포함): MQTT 주제에서 조건을 설명하는 주제를 포함하려면 선택합니다.

Include namespaces(네임스페이스 포함): MQTT 주제에 ONVIF 주제 네임스페이스를 포함하려면 선택합니다.

일련 번호 포함: MQTT 페이로드에 장치의 일련 번호를 포함하려면 선택합니다.

Add condition(조건 추가): 조건을 추가하려면 클릭합니다.

Retain(유지): 어떤 MQTT 메시지가 보유로 전송되는지 정의합니다.

- **None(없음)**: 모든 메시지가 비유지 상태로 전송합니다.
- **Property(속성)**: 상태 추적 가능 메시지만 보관된 상태로 보냅니다.
- **All(모두)**: 상태 추적 가능 및 상태를 추적할 수 없음 메시지를 모두 보관된 상태로 보냅니다.

QoS: MQTT 발행에 대해 원하는 레벨을 선택합니다.

MQTT 구독

Add subscription(구독 추가): 새 MQTT 구독을 추가하려면 클릭합니다.

Subscription filter(구독 필터): 구독하려는 MQTT 주제를 입력하십시오.

Use device topic prefix(장치 항목 접두사 사용): 구독 필터를 MQTT 주제에 접두사로 추가합니다.

Subscription type(구독 유형):

- **Stateless(상태 추적 불가능)**: MQTT 메시지를 상태 추적 불가능 메시지로 변환하려면 선택합니다.
- **Stateful(상태 추적 가능)**: MQTT 메시지를 조건으로 변환하려면 선택합니다. 페이로드는 상태로 사용됩니다.

QoS: MQTT 구독에 대해 원하는 레벨을 선택합니다.

MQTT 오버레이

비고

MQTT 오버레이 수정자를 추가하기 전에 MQTT 브로커에 연결하십시오.

Add overlay modifier(오버레이 수정자 추가): 새 오버레이 수정자를 추가하려면 클릭합니다.

Topic filter(주제 필터): 오버레이에 표시하려는 데이터가 포함된 MQTT 주제를 추가합니다.

Data field(데이터 필드): 메시지가 JSON 형식이라고 가정하고 오버레이에 표시하려는 메시지 페이로드의 키를 지정합니다.

Modifier(수정자): 오버레이를 만들 때 결과 수정자를 사용합니다.

- **#XMP**로 시작하는 수정자는 주제에서 받은 모든 데이터를 표시합니다.
- **#XMD**로 시작하는 수정자는 데이터 필드에 지정된 데이터를 표시합니다.

저장

네트워크 스토리지

Network storage(네트워크 스토리지): 네트워크 스토리지를 사용하려면 켭니다.

Add network storage(네트워크 스토리지 추가): 녹화를 저장할 수 있는 네트워크 공유를 추가하려면 클릭합니다.

- **Address(주소)**: 호스트 서버의 IP 주소 또는 호스트 이름을 입력합니다. 일반적으로 NAS (Network Attached Storage)입니다. 고정 IP 주소(동적 IP 주소는 변경될 수 있으므로 DHCP 제외)를 사용하도록 호스트를 구성하거나 DNS를 사용하는 것이 좋습니다. Windows SMB/CIFS 이름은 지원되지 않습니다.
- **Network share(네트워크 공유)**: 호스트 서버에 공유 위치의 이름을 입력합니다. 각 장치에는 고유한 폴더가 있으므로 여러 Axis 장치가 동일한 네트워크 공유를 사용할 수 있습니다.
- **User(사용자)**: 서버에 로그인이 필요한 경우, 사용자 이름을 입력합니다. 특정 도메인 서버에 로그인하려면 `DOMAIN\username`을 입력합니다.
- **패스워드**: 서버에 로그인이 필요한 경우 패스워드를 입력하십시오.
- **SMB version(SMB 버전)**: NAS에 연결할 SMB 스토리지 프로토콜 버전을 선택합니다. **Auto(자동)**를 선택하면 장치는 보안 버전 SMB 중 하나를 협상하려고 시도합니다. 3.02, 3.0, 또는 2.1. 상위 버전을 지원하지 않는 이전 NAS에 연결하려면 1.0 또는 2.0을 선택하십시오. Axis 장치의 SMB 지원에 대해 *여기*에서 자세히 알아볼 수 있습니다.
- **Add share without testing(테스트 없이 공유 추가)**: 연결 테스트 중에 오류가 발견된 경우에도 네트워크 공유를 추가하려면 선택합니다. 예를 들어, 서버에 패스워드가 필요하지만 이를 입력하지 않았기 때문에 오류가 발생할 수 있습니다.

네트워크 스토리지 제거: 네트워크 공유에 대한 연결을 마운트 해제, 바인딩 해제 및 제거하려면 클릭합니다. 이렇게 하면 네트워크 공유에 대한 모든 설정이 제거됩니다.

Unbind(바인딩 해제): 네트워크 공유를 바인딩 해제하고 연결을 끊으려면 클릭합니다.
Bind(바인딩): 네트워크 공유를 바인딩하고 연결하려면 클릭합니다.

Unmount(마운트 해제): 네트워크 공유를 마운트 해제하려면 클릭합니다.
Mount(마운트): 네트워크 공유를 마운트하려면 클릭합니다.

Write protect(쓰기 방지): 네트워크 공유에 쓰기를 중단하고 녹화물이 제거되지 않도록 하려면 켭니다. 쓰기 방지 네트워크 공유는 포맷할 수 없습니다.

Retention time(보존 시간): 녹화 보관 기간, 오래된 녹화의 양 한도 또는 데이터 저장과 관련된 규정 준수를 선택합니다. 네트워크 스토리지가 가득 차면 선택한 기간이 지나기 전에 이전 녹화가 삭제됩니다.

도구

- **Test connection(연결 테스트)**: 네트워크 공유에 대한 연결을 테스트합니다.
- **Format(포맷)**: 예를 들어 모든 데이터를 빠르게 지워야 하는 경우, 네트워크 공유를 포맷합니다. CIFS는 사용 가능한 파일 시스템 옵션입니다.

Use tool(도구 사용): 클릭하여 선택한 도구를 활성화합니다.

온보드 스토리지

중요 사항

데이터 손실 및 손상된 녹화 위험. 장치가 실행되고 있는 동안에는 SD 카드를 분리하지 마십시오. SD 카드를 제거하기 전에 마운트를 해제하십시오.

Unmount(마운트 해제): 클릭하여 SD 카드를 안전하게 제거하십시오.

Write protect(쓰기 방지): SD 카드에 쓰기가 중지되고 녹화물이 제거되는 것을 보호하려면 이 옵션을 켭니다. 쓰기 방지된 SD 카드는 포맷할 수 없습니다.

Autoformat(자동 포맷): 새로 삽입한 SD 카드를 자동으로 포맷하려면 켜십시오. 파일 시스템을 ext4로 포맷합니다.

Ignore(무시): SD 카드에 녹화 저장을 중지하려면 켜십시오. SD 카드를 무시하면 카드가 있음을 장치가 더 이상 인식하지 못합니다. 이 설정은 관리자만 사용할 수 있습니다.

Retention time(보존 시간): 오래된 녹화의 양을 제한하거나 데이터 저장 규정을 준수하기 위해 녹화를 보관할 기간을 선택합니다. SD 카드가 가득 차면 보존 기간이 지나기 전에 오래된 녹화물을 삭제합니다.

도구

- **Check(확인)**: SD 카드 오류를 확인하십시오.
- **Repair(복구)**: 파일 시스템에 복구 오류가 발생했습니다.
- **Format(포맷)**: SD 카드를 포맷하여 파일 시스템을 변경하고 모든 데이터를 지웁니다. SD 카드는 ext4 파일 시스템으로만 포맷할 수 있습니다. Windows®에서 파일 시스템에 액세스하려면 타사 ext4 드라이버 또는 애플리케이션이 필요합니다.
- **Encrypt(암호화)**: 이 도구를 사용하여 SD 카드를 포맷하고 암호화를 활성화하십시오. 이렇게 하면 SD 카드에 저장된 모든 데이터가 삭제됩니다. SD 카드에 저장하는 모든 새로운 데이터는 암호화됩니다.
- **Decrypt(암호화 해제)**: 이 도구를 사용하여 암호화 없이 SD 카드를 포맷하십시오. 이렇게 하면 SD 카드에 저장된 모든 데이터가 삭제됩니다. SD 카드에 저장하는 어떤 새로운 데이터도 암호화되지 않습니다.
- **Change password(패스워드 변경)**: SD 카드를 암호화하는 데 필요한 패스워드를 변경합니다.

Use tool(도구 사용): 클릭하여 선택한 도구를 활성화합니다.

Wear trigger(마모 트리거): 액션을 트리거하려는 SD 카드 마모 수준 값을 설정합니다. 마모 수준 범위는 0~200%입니다. 한 번도 사용하지 않은 새 SD 카드의 마모 수준은 0%입니다. 100% 마모 수준은 SD 카드가 예상 수명에 가깝다는 것을 나타냅니다. 마모도가 200%에 도달하면 SD 카드가 오작동할 위험이 높습니다. 마모 트리거를 80~90% 사이로 설정하는 것이 좋습니다. 이렇게 하면 녹화를 다운로드하고 SD 카드가 잠재적으로 마모되기 전에 제때에 교체할 수 있습니다. 마모 트리거를 사용하면 이벤트를 설정하고 마모 수준이 설정 값에 도달하면 알림을 받을 수 있습니다.

온보드 스토리지

하드 드라이브

- **Free(여유 공간)**: 여유 디스크 공간의 용량입니다.
- **Status(상태)**: 디스크가 마운트되었는지 여부입니다.
- **파일 시스템**: 디스크에서 사용하는 파일 시스템입니다.
- **암호화됨**: 디스크가 암호화되었는지 여부입니다.
- **Temperature(온도)**: 하드웨어의 현재 온도입니다.
- **Overall heath test(전반적인 상태 테스트)**: 디스크의 상태를 확인한 후의 결과입니다.

도구

- **Check(확인)**: 저장 장치의 오류를 확인하고 자동으로 복구를 시도합니다.
- **Repair(복구)**: 저장 장치를 수리합니다. 활성 녹화는 복구하는 동안 일시 중지됩니다. 저장 장치를 수리하면 데이터가 손실될 수 있습니다.
- **Format(포맷)**: 모든 녹화를 지우고 저장 장치를 포맷합니다. 파일 시스템을 선택합니다.
- **Encrypt(암호화)**: 저장된 데이터를 암호화합니다.
- **Decrypt(암호화 해제)**: 저장된 데이터의 암호화를 해제합니다. 시스템이 저장 장치의 모든 파일을 지웁니다.
- **Change password(패스워드 변경)**: 디스크 암호화에 대한 패스워드를 변경합니다. 패스워드를 변경해도 진행 중인 녹화는 중단되지 않습니다.
- **Use tool(도구 사용)**: 선택한 도구를 실행하려면 클릭합니다.

Unmount(마운트 해제) : 시스템에서 장치를 분리하기 전에 클릭합니다. 진행 중인 모든 녹화가 중지됩니다.

Write protect(쓰기 방지): 저장 장치를 덮어쓰지 않도록 설정합니다.

Autoformat(자동 포맷) : 디스크는 ext4 파일 시스템을 사용하여 자동 포맷됩니다.

온보드 스토리지

RAID

- **Free(여유 공간)**: 여유 디스크 공간의 용량입니다.
- **Status(상태)**: 디스크가 마운트되었는지 여부입니다.
- **파일 시스템**: 디스크에서 사용하는 파일 시스템입니다.
- **암호화됨**: 디스크가 암호화되었는지 여부입니다.
- **Temperature(온도)**: 하드웨어의 현재 온도입니다.
- **Overall heath test(전반적인 상태 테스트)**: 디스크의 상태를 확인한 후의 결과입니다.
- **RAID level(RAID 레벨)**: 스토리지에 사용되는 RAID 레벨. 지원되는 RAID 레벨은 0, 1, 5, 6, 10입니다.
- **RAID status(RAID 상태)**: 스토리지의 RAID 상태. 가능한 값은 **Online(온라인)**, **Degraded (성능 저하)**, **Syncing(동기화 중)** 및 **Failed(실패)**입니다. 동기화 과정은 몇 시간이 걸릴 수 있습니다.

도구

비고

다음 도구를 실행할 때 작업이 완료될 때까지 기다렸다가 페이지를 닫으십시오.

- **Check(확인)**: 저장 장치의 오류를 확인하고 자동으로 복구를 시도합니다.
- **Repair(복구)**: 저장 장치를 수리합니다. 활성 녹화는 복구하는 동안 일시 중지됩니다. 저장 장치를 수리하면 데이터가 손실될 수 있습니다.
- **Format(포맷)**: 모든 녹화를 지우고 저장 장치를 포맷합니다. 파일 시스템을 선택합니다.
- **Encrypt(암호화)**: 저장된 데이터를 암호화합니다. 저장 장치의 모든 파일이 지워집니다.
- **Decrypt(암호화 해제)**: 저장된 데이터를 암호화 해제합니다. 저장 장치의 모든 파일이 지워집니다.
- **Change password(패스워드 변경)**: 디스크 암호화에 대한 패스워드를 변경합니다. 패스워드를 변경해도 진행 중인 녹화는 중단되지 않습니다.
- **Change RAID level(RAID 레벨 변경)**: 모든 녹화 영상을 지우고 스토리지의 RAID 레벨을 변경합니다.
- **Use tool(도구 사용)**: 선택한 도구를 실행하려면 클릭합니다.

Hard drive status(하드 드라이브 상태): 하드 드라이브 상태, 용량 및 일련 번호를 보려면 클릭하십시오.

Write protect(쓰기 방지): 쓰기 방지를 켜서 저장 장치를 덮어쓰지 않도록 보호합니다.

스트림 프로파일

스트림 프로파일은 비디오 스트림에 영향을 미치는 설정 그룹입니다. 이벤트를 생성하고 룰을 사용하여 녹화하는 경우와 같이 다양한 상황에서 스트림 프로파일을 사용할 수 있습니다.

Add stream profile(스트림 프로파일 추가): 클릭하여 새 스트림 프로파일을 생성합니다.

Preview(미리 보기): 선택한 스트림 프로파일 설정을 사용하여 비디오 스트림을 미리 봅니다. 페이지의 설정을 변경하면 미리 보기가 업데이트됩니다. 장치에 다른 보기 영역이 있는 경우 이미지의 좌측 하단에 있는 드롭다운에서 보기 영역을 변경할 수 있습니다.

이름: 프로파일의 이름을 추가합니다.

Description(설명): 프로파일에 대한 설명을 추가합니다.

Video codec(비디오 코덱): 프로파일에 적용해야 하는 비디오 코덱을 선택합니다.

해상도: 이 설정에 대한 설명은 항목을 참고하십시오.

프레임 레이트: 이 설정에 대한 설명은 항목을 참고하십시오.

Compression(압축): 이 설정에 대한 설명은 항목을 참고하십시오.

Zipstream : 이 설정에 대한 설명은 항목을 참고하십시오.

Optimize for storage(스토리지용 최적화) : 이 설정에 대한 설명은 항목을 참고하십시오.

Dynamic FPS(동적 FPS) : 이 설정에 대한 설명은 를 참조하십시오.

Dynamic GOP(동적 GOP) : 이 설정에 대한 설명은 를 참조하십시오.

Mirror(미러) : 이 설정에 대한 설명은 항목을 참고하십시오.

GOP length(GOP 길이) : 이 설정에 대한 설명은 항목을 참고하십시오.

Bitrate control(비트 레이트 제어): 이 설정에 대한 설명은 항목을 참고하십시오.

Include overlays(오버레이 포함) : 포함할 오버레이 유형을 선택합니다. 오버레이를 추가하는 방법에 대한 자세한 내용은 *오버레이, on page 30* 항목을 참고하십시오.

Include audio(오디오 포함) : 이 설정에 대한 설명은 항목을 참고하십시오.

ONVIF

ONVIF 계정

ONVIF(Open Network Video Interface Forum)는 최종 사용자, 통합자, 컨설턴트 및 제조사가 네트워크 비디오 기술을 통한 가능성을 쉽게 활용할 수 있게 해주는 글로벌 인터페이스 표준입니다. ONVIF를 통해 서로 다른 벤더 제품 간의 상호운용성, 유연성 향상, 비용 절감 및 시스템의 미래 경쟁력을 높일 수 있습니다.

ONVIF 계정을 생성하면 ONVIF 통신이 자동으로 활성화됩니다. 장치와의 모든 ONVIF 통신에 사용자 계정 이름과 패스워드를 사용합니다. 자세한 내용은 *axis.com*의 Axis 개발자 커뮤니티를 참조하십시오

Add accounts(계정 추가): 새 ONVIF 계정을 추가하려면 클릭합니다.

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 패스워드): 계정의 패스워드를 입력합니다. 패스워드는 1~64자 길이여야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 패스워드에 사용할 수 있습니다.

Repeat password(패스워드 반복): 동일한 패스워드를 다시 입력하십시오.

Privileges(권한):

- **Administrator(관리자)**: 모든 설정에 완전히 액세스합니다. 관리자는 다른 계정을 추가, 업데이트 및 제거할 수 있습니다.
- **Operator(운영자)**: 다음을 제외한 모든 설정에 액세스할 수 있습니다.
  - 모든 **System(시스템)** 설정
  - 앱 추가.
- **Media account(미디어 계정)**: 비디오 스트림에만 액세스할 수 있습니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Update account(계정 업데이트): 계정 속성을 편집합니다.

Delete account(계정 삭제): 계정을 삭제합니다. root 계정은 삭제할 수 없습니다.

ONVIF 미디어 프로파일

ONVIF 미디어 프로파일은 미디어 스트림 설정을 변경하는 데 사용할 수 있는 구성 집합으로 이루어져 있습니다. 자신만의 구성 세트로 새 프로파일을 생성하거나 빠른 설정을 위해 사전 구성된 프로파일을 사용할 수 있습니다.

Add media profile(미디어 프로파일 추가): 새 ONVIF 미디어 프로파일을 추가하려면 클릭합니다.

Profile name(프로파일 이름): 미디어 프로파일의 이름을 추가합니다.

Video source(비디오 소스): 구성에 맞는 비디오 소스를 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택합니다. 드롭다운 목록의 구성은 멀티 뷰, 보기 영역 및 가상 채널을 포함한 장치의 비디오 채널에 해당합니다.

Video encoder(비디오 엔코더): 구성에 맞는 비디오 인코딩 형식을 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 인코딩 설정을 조정합니다. 드롭다운 목록의 구성은 비디오 엔코더 구성의 식별자/이름 역할을 합니다. 사용자 0~15를 선택하여 자신만의 설정을 적용하거나, 특정 인코딩 형식에 대해 사전 정의된 설정을 사용하려면 기본 사용자 중 하나를 선택합니다.

비고

오디오 소스 및 오디오 엔코더 구성을 선택하는 옵션을 얻으려면 장치에서 오디오를 활성화하십시오.

Audio source(오디오 소스) : 구성에 맞는 오디오 입력 소스를 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 오디오 설정을 조정합니다. 드롭다운 목록의 구성은 장치의 오디오 입력에 해당합니다. 장치에 하나의 오디오 입력이 있는 경우 user0입니다. 장치에 여러 개의 오디오 입력이 있는 경우 목록에 추가 사용자가 표시됩니다.

Audio encoder(오디오 엔코더) : 구성에 맞는 오디오 인코딩 형식을 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 오디오 인코딩 설정을 조정합니다. 드롭다운 목록의 구성은 오디오 엔코더 구성의 식별자/이름 역할을 합니다.

Audio decoder(오디오 디코더) : 구성에 맞는 오디오 디코딩 형식을 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 설정을 조정합니다. 드롭다운 목록의 구성은 오디오 구성의 식별자/이름 역할을 합니다.

Audio output(오디오 출력) : 구성에 맞는 오디오 출력 형식을 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 설정을 조정합니다. 드롭다운 목록의 구성은 오디오 구성의 식별자/이름 역할을 합니다.

Metadata(메타데이터): 구성에 포함할 메타데이터를 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 메타데이터 설정을 조정합니다. 드롭다운 목록의 구성은 오디오 메타데이터 구성의 식별자/이름 역할을 합니다.

PTZ : 구성에 맞는 PTZ 설정을 선택합니다.

- **Select configuration(구성 선택)**: 목록에서 사용자 지정 구성을 선택하고 PTZ 설정을 조정합니다. 드롭다운 목록의 구성은 PTZ를 지원하는 장치의 비디오 채널에 해당합니다.

Create(생성): 설정을 저장하고 프로파일을 생성하려면 클릭합니다.

Cancel(취소): 구성을 취소하고 모든 설정을 지우려면 클릭합니다.

profile_x(프로파일_x): 프로파일 이름을 클릭하면 사전 구성된 프로파일을 열고 편집할 수 있습니다.

디텍터

충격 감지

Shock detector(충격 감지기): 장치가 물체에 부딪히거나 조작된 경우 알람을 생성하려면 켭니다.

Sensitivity level(감도 수준): 슬라이더를 이동하여 장치가 알람을 생성해야 하는 민감도 수준을 조정합니다. 낮은 값은 히트가 강력한 경우에만 장치가 알람을 생성함을 의미합니다. 값이 높으면 장치가 약간의 변조에도 알람을 생성한다는 의미입니다.

전원 설정

전원 상태

전력 상태 정보를 표시합니다. 정보는 제품에 따라 다릅니다.

전원 설정

Delayed shutdown(지연 종료) : 전원이 꺼지기 전의 지연 시간을 설정하려면 켭니다.

Delay time(지연 시간) : 지연 시간을 1분에서 60분 사이로 설정합니다.

Power saving mode(절전 모드) : 장치를 절전 모드로 전환하려면 켭니다. 절전 모드를 켜면 IR 조명 범위가 줄어듭니다.

Set power configuration(전원 구성 설정) : 다른 PoE 클래스 옵션을 선택하여 전원 구성을 변경하십시오. 변경 사항을 저장하기 위해 **Save and restart(저장하고 다시 시작)**를 클릭합니다.

비고

전원 구성을 PoE 클래스 3으로 설정하면, **Low power profile(저전력 프로파일)**(장치에 해당 옵션이 있는 경우)을 선택하는 것이 좋습니다.

Dynamic power mode(동적 전원 모드) : 장치가 비활성 상태일 때 전력 소비를 줄이려면 켭니다.

전력 경고 오버레이 : 장치에 충분한 전력이 없을 때 전력 경고 오버레이를 표시하려면 켜십시오.

I/O port power(I/O 포트 전원) : I/O 포트에 연결된 외부 장치에 12V 전원을 공급하려면 켭니다. IR, 난방 및 냉방과 같은 내부 기능에 우선순위를 두려면 해제합니다. 그 결과 12V 전원이 필요한 장치와 센서가 제대로 작동하지 않습니다.

파워 미터

에너지 사용량

현재 전력 사용량, 평균 전력 사용량, 최대 전력 사용량 및 시간 경과에 따른 전력 소비량을 표시합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Export(내보내기)**: 차트 데이터를 내보내려면 클릭합니다.

에지 투 에지

페어링

페어링하면 호환 가능 Axis 장치를 기본 장치의 일부인 것처럼 사용할 수 있습니다.

추가: 페어링할 장치를 추가합니다.

Discover devices(장치 검색): 네트워크에서 장치를 찾으려면 클릭합니다. 네트워크를 스캔하면 사용 가능한 장치 목록이 표시됩니다.

비고

목록에는 페어링할 수 있는 장치뿐만 아니라 발견된 모든 Axis 장치가 표시됩니다.

Bonjour가 활성화된 장치만 찾을 수 있습니다. 장치에 대해 **Bonjour**를 활성화하려면 장치의 웹 인터페이스를 열고 **System(시스템) > Network(네트워크) > Network discovery protocols (네트워크 검색 프로토콜)**로 이동합니다.

비고

이미 페어링된 장치의 경우 정보 아이콘이 표시됩니다. 이미 활성화된 페어링에 대한 정보를 얻으려면 아이콘 위로 마우스를 가져갑니다.

오디오 페어링을 통해 네트워크 스피커 또는 마이크와 페어링할 수 있습니다. 페어링된 네트워크 스피커는 오디오 클립을 재생하고 카메라를 통해 사운드를 전송할 수 있는 오디오 출력 장치 역할을 수행합니다. 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 스피커 또는 마이크와 페어링한 다음 VMS에 카메라를 추가해야 합니다.

'오디오 디텍션'을 조건으로 하고 '오디오 클립 재생'을 액션으로 하는 이벤트 룰에서 네트워크에 페어링된 오디오 장치를 사용할 때 이벤트 룰에 '액션 대기 간격(hh:mm:ss)' 제한을 설정합니다. 그러면 캡처 마이크가 스피커에서 오디오를 포착하는 경우 반복 감지를 피할 수 있습니다.

목록에서 장치를 페어링하려면 을 클릭합니다.

Select pairing type(페어링 유형 선택): 드롭다운 목록에서 선택합니다.

Speaker pairing(스피커 페어링): 네트워크 스피커를 페어링하려면 선택합니다.

마이크 페어링 : 마이크를 페어링하려면 선택합니다.

Address(주소): 네트워크 스피커에 호스트 이름 또는 IP 주소를 입력합니다.

Username(사용자 이름): 사용자 이름을 입력합니다.

패스워드: 사용자의 패스워드를 입력합니다.

Close(닫기): 모든 필드를 지우려면 클릭합니다.

Connect(연결): 페어링할 장치에 연결을 설정하려면 클릭합니다.

PTZ pairing(PTZ 페어링)으로 오토트래킹을 사용하도록 레이더를 PTZ 카메라와 페어링할 수 있습니다. 레이더 PTZ 오토트래킹을 사용하면 PTZ 카메라가 객체 위치에 대한 레이더 정보를 기반으로 객체를 추적합니다.

목록에서 장치를 페어링하려면 + 을 클릭합니다.

Select pairing type(페어링 유형 선택): 드롭다운 목록에서 선택합니다.

Address(주소): PTZ 카메라의 IP 주소 또는 호스트 이름을 입력합니다.

Username(사용자 이름): PTZ 카메라의 사용자 이름을 입력합니다.

패스워드: PTZ 카메라의 패스워드를 입력합니다.

Close(닫기): 모든 필드를 지우려면 클릭합니다.

Connect(연결): PTZ 카메라에 대한 연결을 설정하려면 클릭합니다.

Configure radar autotracking(레이더 오토트래킹 구성): 오토트래킹을 열고 구성하려면 클릭합니다. 구성하려면 **Radar > Radar PTZ autotracking(레이더 > 레이더 PTZ 오토트래킹)**으로 이동할 수도 있습니다.

Generic pairing(일반 페어링)을 사용하면 조명 및 사이렌 기능이 있는 장치와 페어링할 수 있습니다.

목록에서 장치를 페어링하려면 + 을 클릭합니다.

Select pairing type(페어링 유형 선택): 드롭다운 목록에서 선택합니다.

Address(주소): 장치의 호스트 이름 또는 IP 주소를 입력합니다.

Username(사용자 이름): 사용자 이름을 입력합니다.

패스워드: 패스워드를 입력하세요.

Certificate name(인증서 이름): 인증서 이름을 입력합니다.

Close(닫기): 모든 필드를 지우려면 클릭합니다.

Connect(연결): 페어링할 장치에 연결을 설정하려면 클릭합니다.

로그

보고서 및 로그

보고서

- **View the device server report(장치 서버 보고서 보기)**: 팝업 창에서 제품 상태에 대한 정보를 봅니다. 액세스 로그는 자동으로 서버 보고서에 포함됩니다.
- **Download the device server report(장치 서버 보고서 다운로드)**: 현재 실시간 보기 이미지의 스냅샷뿐 아니라 UTF-8 형식의 전체 서버 보고서 텍스트 파일이 포함된 .zip 파일이 생성됩니다. 지원 서비스에 문의할 때 항상 서버 보고서 .zip 파일을 포함하십시오.
- **Download the crash report(충돌 보고서 다운로드)**: 서버 상태에 대한 자세한 정보가 있는 아카이브를 다운로드합니다. 충돌 보고서에는 자세한 디버그 정보와 서버 보고서에 있는 정보가 포함됩니다. 이 보고서에는 네트워크 추적과 같은 민감한 정보가 있을 수 있습니다. 보고서를 생성하는 데 몇 분 정도 소요될 수 있습니다.

로그

- **View the system log(시스템 로그 보기)**: 장치 시작, 경고 및 중요한 메시지와 같은 시스템 이벤트에 대한 정보를 표시하려면 클릭합니다.
- **View the access log(액세스 로그 보기)**: 잘못된 로그인 패스워드를 사용한 경우 등 실패한 장치 액세스 시도를 모두 표시하려면 클릭합니다.
- **View the audit log(감사 로그 보기)**: 클릭하면 성공 또는 실패한 인증 및 구성과 같은 사용자 및 시스템 활동에 대한 정보가 표시됩니다.

원격 시스템 로그

Syslog는 메시지 로깅의 표준입니다. Syslog에서는 메시지를 생성하는 소프트웨어, 메시지를 저장하는 시스템, 메시지를 보고 및 분석하는 소프트웨어를 분리할 수 있습니다. 각 메시지별로 그 메시지를 생성하는 소프트웨어 유형을 나타내는 시설 코드가 표시되고 심각도 수준이 할당됩니다.

+ **Server(서버)**: 새 서버를 추가하려면 클릭합니다.

호스트: 서버의 호스트 이름 또는 IP 주소를 입력합니다.

Format(포맷): 사용할 syslog 메시지 포맷을 선택합니다.

- Axis
- RFC 3164
- RFC 5424

Protocol(프로토콜): 사용할 프로토콜 선택:

- UDP(기본 설정 포트: 514)
- TCP(기본 설정 포트: 601)
- TLS(기본 설정 포트: 6514)

Port(포트): 다른 포트를 사용하려면 포트 번호를 편집합니다.

Severity(심각도): 트리거될 때 전송할 메시지를 선택합니다.

Type(유형): 전송하려는 로그 유형을 선택합니다.

Test server setup(서버 설정 테스트): 설정을 저장하기 전에 모든 서버에 테스트 메시지를 보냅니다.

CA certificate set(CA 인증서 설정): 현재의 설정을 확인하거나 인증서를 추가합니다.

일반 구성

일반 구성은 Axis 장치 구성 경험이 있는 고급 사용자를 위한 항목입니다. 이 페이지에서 대부분의 매개변수를 설정하고 편집할 수 있습니다.

유지보수

유지보수

Restart(재시작): 장치를 재시작합니다. 이는 현재 설정에 영향을 주지 않습니다. 실행 중인 애플리케이션이 자동으로 재시작됩니다.

Restore(복구): 대부분의 설정을 공장 출하 시 기본값으로 되돌리십시오. 나중에 장치와 앱을 다시 구성하고 사전 설치되지 않은 모든 앱을 다시 설치하고 이벤트 및 프리셋을 다시 만들어야 합니다.

중요 사항

복원 후 저장되는 유일한 설정은 다음과 같습니다.

- 부팅 프로토콜(DHCP 또는 고정)
- 고정 IP 주소
- 기본 라우터
- 서브넷 마스크
- 802.1X 설정
- O3C 설정
- DNS 서버 IP 주소

Factory default(공장 출하 시 기본값): 모든 설정을 공장 출하 시 기본값으로 되돌리십시오. 그런 후에 장치에 액세스할 수 있도록 IP 주소를 재설정해야 합니다.

비고

모든 Axis 장치 소프트웨어는 디지털 서명되어 장치에 검증된 소프트웨어만 설치할 수 있습니다. 이렇게 하면 Axis 장치의 전반적인 최소 사이버 보안 수준을 더욱 높일 수 있습니다. 자세한 내용은 *axis.com*에서 백서 "Axis Edge Vault"를 참조하십시오.

AXIS OS upgrade(AXIS OS 업그레이드): 새 AXIS OS 버전으로 업그레이드합니다. 새 릴리스에는 향상된 기능, 버그 수정 및 완전히 새로운 기능이 포함됩니다. 항상 최신 AXIS OS 릴리즈를 사용하는 것이 좋습니다. 최신 릴리즈를 다운로드하려면 *axis.com/support*로 이동합니다.

업그레이드할 때 다음 세 가지 옵션 중에서 선택할 수 있습니다.

- **Standard upgrade(표준 업그레이드)**: 새 AXIS OS 버전으로 업그레이드합니다.
- **Factory default(공장 출하 시 기본값)**: 업그레이드하고 모든 설정을 공장 출하 시 기본값으로 되돌리십시오. 이 옵션을 선택하면 업그레이드 후에 이전 AXIS OS 버전으로 되돌릴 수 없습니다.
- **Automatic rollback(자동 롤백)**: 설정된 시간 내에 업그레이드하고 업그레이드를 확인하십시오. 확인하지 않으면 장치가 이전 AXIS OS 버전으로 되돌아갑니다.

AXIS OS rollback(AXIS OS 롤백): 이전에 설치된 AXIS OS 버전으로 되돌립니다.

문제 해결

Reset PTR(PTR 재설정) : **Pan(팬)**, **Tilt(틸트)** 또는 **Roll(롤)** 설정이 예상대로 작동하지 않는 경우 PTR을 재설정합니다. PTR 모터는 항상 새 카메라에서 보정됩니다. 그러나 카메라의 전원이 꺼지거나 모터가 손으로 움직이는 경우에는 보정이 손실될 수 있습니다. PTR을 재설정하면 카메라가 다시 보정되고 공장 출하 시 기본값으로 돌아갑니다.

보정 : **Calibrate(보정)**를 클릭하여 팬, 틸트 및 롤 모터를 기본 위치로 다시 보정합니다.

Ping: 장치에서 특정 주소에 연결할 수 있는지 확인하려면 핑하려는 호스트의 호스트 이름 또는 IP 주소를 입력하고 **Start(시작)**를 클릭합니다.

Port check(포트 확인): 장치에서 특정 IP 주소 및 TCP/UDP 포트로 이어지는 연결을 확인하려면, 확인하려는 호스트 이름 또는 IP 주소와 포트 번호를 입력하고 **Start(시작)**를 클릭합니다.

네트워크 추적

중요 사항

네트워크 추적 파일에는 인증서 또는 패스워드와 같은 민감한 정보가 포함될 수 있습니다.

네트워크 추적 파일은 네트워크 활동을 기록하여 문제를 해결하는 데 도움을 줄 수 있습니다.

Trace time(추적 시간): 추적 기간(초 또는 분)을 선택하고 **Download(다운로드)**를 클릭합니다.

상세 정보

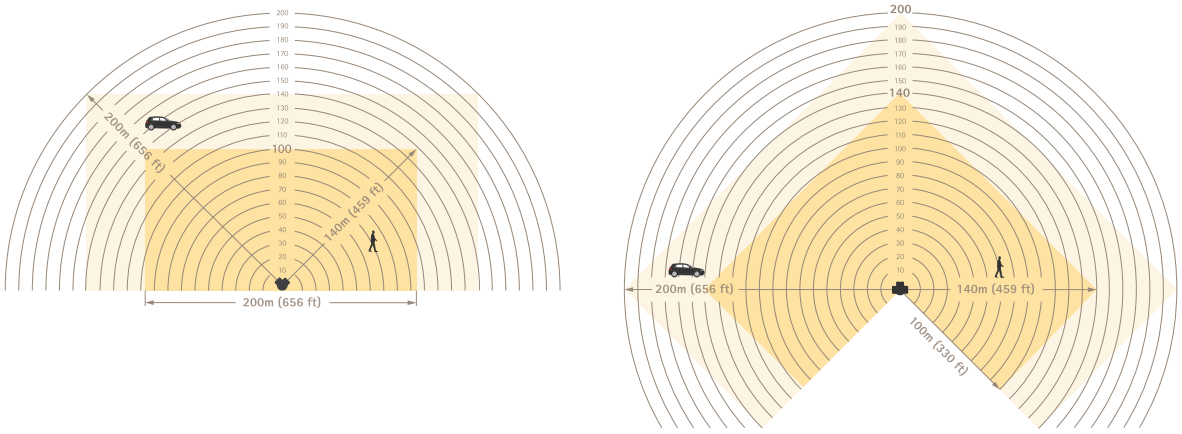
레이더

인식 및 감지 구역

인식 구역은 레이더가 객체를 사람 또는 차량으로 확실하게 분류할 수 있는 구역입니다.

감지 구역은 레이더가 빠르게 이동하는 차량을 감지할 수 있는 구역입니다.

각 구역의 크기는 설치 높이 및 기타 요인에 따라 달라집니다.



인식 구역은 진한 노란색이고, 감지 구역은 연한 노란색입니다.

시나리오, 포함 구역 및 제외 구역

시나리오는 이벤트 시스템에서 룰을 트리거하기 위해 움직이는 객체가 충족해야 하는 조건 집합으로 구성됩니다. 일부 조건은 다음과 같습니다.

- 객체 유형(사람, 차량, 미확인)
- 객체 동작(영역 내 이동 또는 선 넘기)
- 장면의 일부(포함 구역 또는 가상 선)
- 객체 속도

포함 구역은 영역 내 이동 시나리오에서 객체가 감지되고 분류되는 장면의 일부입니다.

장면 내에서 움직이는 객체가 알람을 트리거하지 않도록 할 영역이 있으면 **제외 구역**을 생성할 수 있습니다. 포함 구역 내부에 원치 않는 알람을 많이 유발하는 영역이 있으면 제외 구역을 사용할 수도 있습니다. 제외 구역에서는 움직이는 객체가 무시됩니다. 예를 들어 도로변에서 흔들리는 잎사귀 또는 금속 울타리와 같이 레이더 반사 재질로 만들어진 객체로 인해 발생하는 고스트 트랙을 걸러내는 데 사용합니다.

공존 구역

단일 레이더의 지정된 감지 구역보다 더 넓은 영역을 커버하려면 여러 대의 레이더를 설치할 수 있습니다. 동일한 무선 주파수를 사용하는 레이더는 전자기 간섭을 일으켜 성능에 영향을 미칠 수 있습니다. 각 Axis 레이더 모델에는 지정된 공존 구역이 있습니다. 이 범위 내에서는 간섭을 일으키지 않고 일정 수의 레이더를 설치할 수 있습니다. 공존 구역의 반경과 권장 최대 레이더 수를 확인하려면 *axis.com*의 장치 데이터시트를 참조하십시오.

레이더-비디오 융합 기술

레이더-비디오 융합은 Axis 레이더의 장점과 Axis 카메라의 장점을 결합합니다. 이 조합은 탁월한 상황 인식을 제공하고 거짓 경보를 줄입니다. 카메라의 웹 인터페이스에서 ARTPEC-9 PTZ 카메라와 ARTPEC-9 레이더를 페어링하면, 레이더가 움직이는 객체를 발견하고 분류하며 카메라를 해당 객체로 향하게 하고 카메라가 분류 결과를 검증하도록 할 수 있습니다. 그런 다음 카메라는 오토트래킹으로 객체를 계속 추적할 수 있으며, 이에 대한 내용은 PTZ 카메라 사용자 설명서에서 확인할 수 있습니다.

오토트래킹

서로 다른 객체의 위치에 대한 레이더 데이터를 사용하여 PTZ 카메라가 객체를 추적하도록 할 수 있습니다. 세 가지 옵션이 있습니다.

- 여러 대의 PTZ 카메라와 레이더를 연결하려면 AXIS Radar Autotracking for PTZ 애플리케이션을 사용합니다. 자세한 내용은 *AXIS Radar Autotracking for PTZ로 PTZ 카메라 제어, on page 72*를 참조하십시오.
- 서로 가깝게 마운트된 레이더 1대와 ARTPEC-7 PTZ 카메라 1대를 연결하려면, 카메라 페어링을 사용하여 내장 레이더 오토트래킹을 사용합니다.
- 함께 마운트된 레이더 1대와 ARTPEC-9 PTZ 카메라 1대를 연결하려면, 레이더 페어링을 사용하여 내장 레이더-비디오 융합 오토트래킹을 사용합니다. 이 옵션은 AI 기반 레이더 및 비디오 분석을 결합하여 거짓 경보를 최소화합니다. 레이더-비디오 융합 오토트래킹 설정 방법은 *help.axis.com/axis-q6325-le*의 PTZ 카메라 사용자 설명서를 참조하십시오.

AXIS Radar Autotracking for PTZ로 PTZ 카메라 제어

AXIS Radar Autotracking for PTZ는 객체를 추적할 때 다양한 설정을 처리할 수 있는 서버 기반 솔루션입니다.

- 하나의 레이더로 여러 PTZ 카메라를 제어합니다.
- 여러 레이더로 하나의 PTZ 카메라를 제어합니다.
- 여러 레이더로 여러 PTZ 카메라를 제어합니다.
- 동일한 영역을 커버하는 다른 위치에 장착된 경우 하나의 레이더로 하나의 PTZ 카메라를 제어합니다.

이 애플리케이션은 특정 PTZ 카메라 세트와 호환됩니다. 자세한 내용은 *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*를 참조하십시오.

애플리케이션을 다운로드하고 애플리케이션 설정 방법에 대한 자세한 내용은 사용자 설명서를 참조하십시오. 자세한 내용은 *axis.com/products/axis-radar-autotracking-for-ptz/support*를 참조하십시오.

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.

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

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.

AV1

AV1(AOMedia Video 1)은 스트리밍 미디어에 최적화된 라이센스 없는 비디오 코딩 형식으로, 대역폭이 제한된 환경에서도 고품질 비디오 스트리밍을 지원합니다. AV1은 비디오의 비트 레이트를 줄임으로써 비디오 품질을 보존하는 동시에 데이터 사용량을 최소화합니다.

AV1은 모든 주요 브라우저, 컴퓨터 운영 체제 및 모바일 플랫폼을 지원합니다.

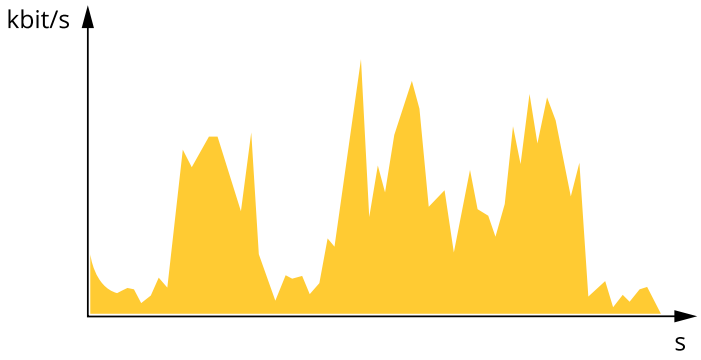
비고

AV1은 다른 코덱에 비해 인코딩 및 디코딩에 더 많은 처리 능력을 요구합니다.

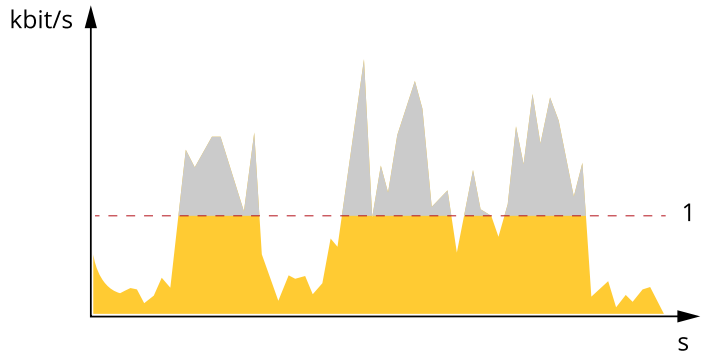
비트 레이트 제어

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.



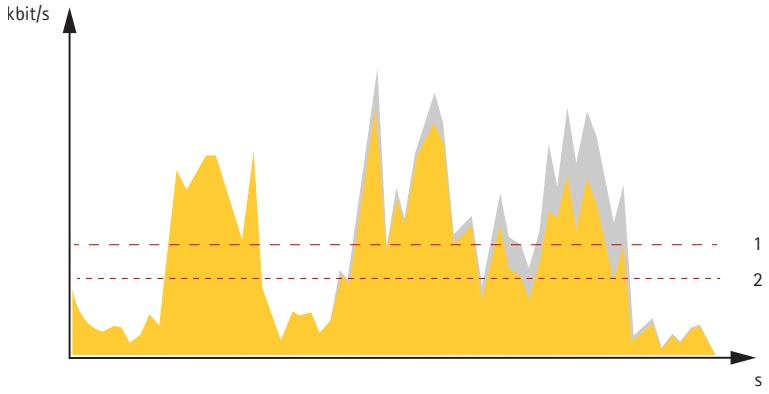
최대 비트 레이트(MBR)
최대 비트 레이트는 시스템의 비트 레이트 제한을 처리하기 위해 목표 비트 레이트를 설정하도록 합니다. 순간 비트 레이트가 지정된 목표 비트 레이트 미만으로 유지되면 이미지 품질이나 프레임 속도가 저하될 수 있습니다. 이미지 품질 또는 프레임 레이트를 우선시하도록 선택할 수 있습니다. 대상 비트 레이트를 예상 비트 레이트보다 높은 값으로 구성하는 것이 좋습니다. 이것은 장면에 높은 수준의 활동이 있는 경우 여백을 제공합니다.



1 대상 비트 레이트

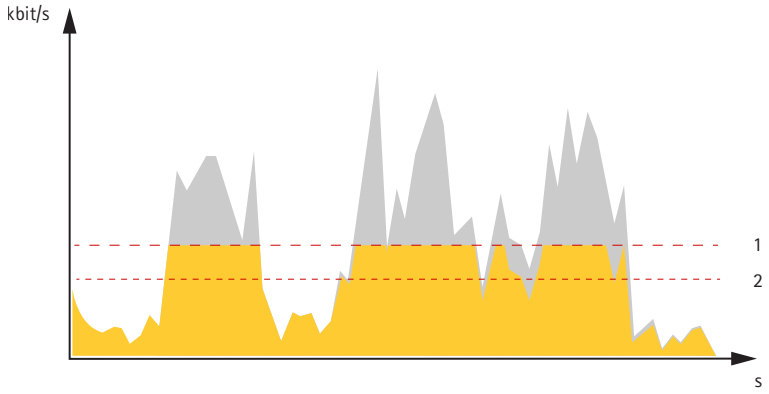
평균 비트 레이트(ABR)
평균 비트 레이트를 사용하면 더 오랜 기간에 비트 레이트가 자동으로 조정됩니다. 지정된 대상을 충족하고 사용 가능한 스토리지를 기반으로 최상의 비디오 품질을 제공할 수 있습니다. 정적 장면에 비해 활동량이 많은 장면에서 비트 레이트가 더 높습니다. 평균 비트 레이트 옵션을 사용하면 활동이 많은 장면에서 더 나은 이미지 품질을 얻을 가능성이 더 큽니다. 이미지 품질이 지정된 대상 비트 레이트에 맞게 조정될 때 지정된 시간(보존 시간) 동안 비디오 스트림을 저장하는 데 필요한 총 스토리지를 정의할 수 있습니다. 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

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.

자세한 내용은 *whitepapers.axis.com/edge-to-edge-technology*에서 "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.

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 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

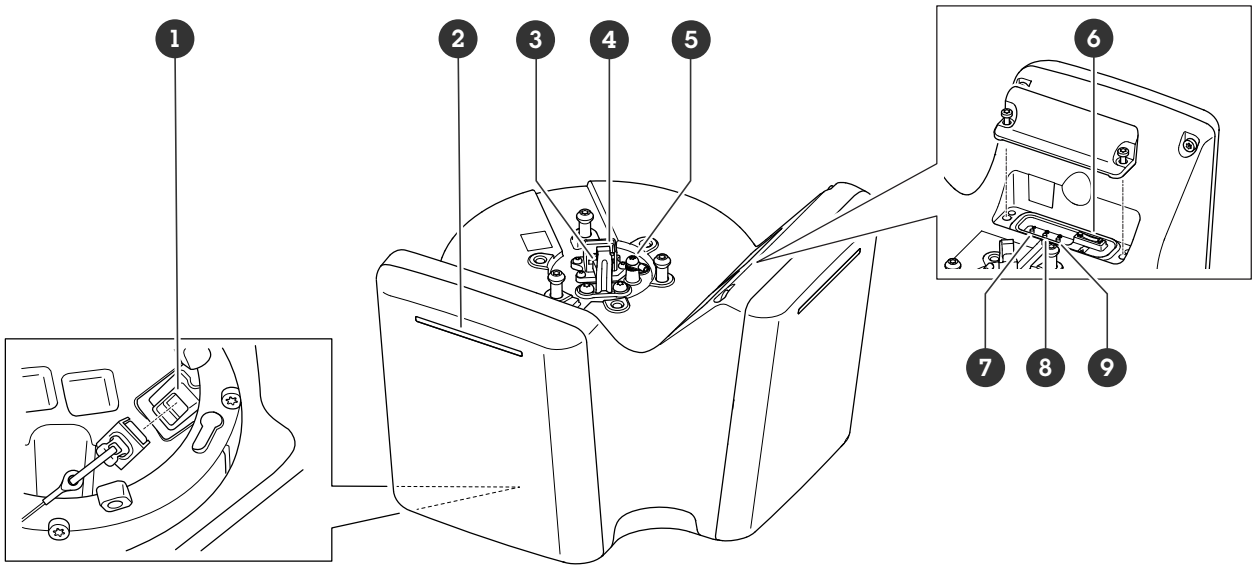
Axis는 고객의 노출 위험을 최소화하기 위해 **CVE(공통 취약성 및 노출) CNA(번호 지정 기관)**로서 업계 표준을 준수하여 장치, 소프트웨어 및 서비스에서 발견된 취약점을 관리하고 이에 대응합니다. Axis 취약성 관리 정책, 취약성을 보고하는 방법, 이미 공개된 취약성 및 해당 보안 권고에 대한 자세한 내용은 *axis.com/vulnerability-management*를 참조하십시오.

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 *네트워크 커넥터(PoE 출력)*
2 *동적 LED 스트립*
3 *안전선 고리*
4 *네트워크 커넥터(PoE 입력)*
5 *접지 나사*
6 *microSD 카드 슬롯*
7 *제어 버튼*
8 *액션 버튼*
9 *기능 버튼(사용되지 않음)*

LED 표시

상태 LED	표시
녹색	정상 작동 시 녹색이 계속 표시됩니다.
주황색	시작 시 켜져 있습니다. 장치 소프트웨어 업그레이드 중 또는 공장 출하 시 기본값으로 재설정 시 깜박입니다.

동적 LED 스트립 패턴
빨간색
파란색
녹색
노란색
화이트
스위핑 레드
스위핑 블루
스위핑 그린
깜박이는 빨간색, 파란색, 흰색

SD 카드 슬롯

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 79*을 참조하십시오.

커넥터

네트워크 커넥터(PoE 입력)

PoE(Power over Ethernet) IEEE 802.3bt, Type 4 Class 8을 지원하는 RJ45 이더넷 커넥터입니다.

비고

PoE 출력에는 PoE(Power over Ethernet) IEEE 802.3bt, Type 4 Class 8이 필요합니다. 두 번째 장치에 전원을 공급하지 않을 때는 PoE(Power over Ethernet) IEEE 802.3at, Type 2 Class 4이면 충분합니다.

네트워크 커넥터(PoE 출력)

PoE(Power over Ethernet) IEEE 802.3bt, Type 3 Class 6.

이 커넥터를 사용하여 다른 PoE 장치(예: 카메라, 혼 스피커 또는 두 번째 Axis 레이더)에 전원을 공급하십시오.

비고

- PoE(Power over Ethernet) IEEE 802.3bt, Type 4 Class 8로 레이더에 전원을 공급하면 PoE (Power over Ethernet) IEEE 802.3bt, Type 3 Class 6을 사용하는 두 번째 장치를 연결할 수 있습니다.
- PoE(Power over Ethernet) IEEE 802.3bt, Type 3 Class 6로 레이더에 전원을 공급하면 PoE (Power over Ethernet) IEEE 802.3bt, Type 2 Class 4를 사용하는 두 번째 장치를 연결할 수 있습니다.
- PoE(Power over Ethernet) IEEE 802.3bt, Type 2 Class 4로 레이더에 전원을 공급하는 경우 PoE 출력이 비활성화됩니다.

비고

PoE 출력 및 PoE 결합시 최대 이더넷 케이블 길이는 총 100m입니다. PoE 익스텐더를 사용하여 늘릴 수 있습니다.

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 76*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.

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 79*을 참조하십시오.
   재설정 후 Secure Boot는 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

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.
- 설치가 실패하지 않도록 업그레이드 중에 커버가 부착되어 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.

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 79* 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 14*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.

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/support*에서 문제 해결 섹션을 확인해 보십시오.

이미지 문제

이미지 저하 또는 이미지 손실

- 센서 장치에 대한 링크가 손실된 횟수에 대한 장치 서버 리포트를 확인하십시오.
- 센서 유닛과 메인 유닛 사이의 커넥터 케이블이 팽팽한지 확인하십시오.
- 새 센서 유닛 케이블로 변경하십시오.

장치가 스스로 꺼지는 문제

장치가 종료됩니다.

- 장치의 전원을 분리했다가 다시 연결하십시오.
- **Delayed shutdown(종료 지연)**이 켜져 있는지 확인합니다. 켜져 있으면 설정된 지연 시간에 따라 본체가 꺼집니다. 장치가 다시 스스로 꺼지기 전에 **Delayed shutdown(지연 종료)**을 끌 수 있는 시간은 300초입니다.

성능 고려 사항

시스템을 설정할 때는 서로 다른 설정과 상황이 요구되는 대역폭(비트 레이트)에 어떤 영향을 미치는지 고려하는 것이 중요합니다.

고려해야 할 가장 중요한 요소:

- 커버를 분리하거나 연결하면 카메라가 다시 시작됩니다.
- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.

지원 센터 문의

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

T10223326_ko

2026-01 (M1.36)