

AXIS D2210-VE Radar

목차

설치	4
고려 사항	4
제품을 설치할 위치	4
여러 레이더 설치	5
레이더 프로파일	7
Area monitoring profile(영역 모니터링 프로파일)	7
커버리지 범위	7
영역 감지 범위	7
영역 설치 예	8
영역 모니터링 사용 사례	9
도로 모니터링 프로파일	10
도로 감지 범위	10
도로 설치 예	10
도로 모니터링 사용 사례	12
시작하기	14
네트워크에서 장치 찾기	14
브라우저 지원	14
장치의 웹 인터페이스 열기	14
관리자 계정 생성	14
안전한 패스워드	14
아무도 장치 소프트웨어를 조작하지 않았는지 확인	15
웹 인터페이스 개요	15
장치 구성	16
레이더 프로파일을 선택합니다	16
장착 높이 설정	16
참조 지도로 보정	17
감지 영역 설정	17
시나리오 추가	18
제외 영역 추가	19
허위 알람을 최소화하는 방법	19
레이더 이미지를 조정	20
이미지 오버레이 표시	20
텍스트 오버레이 표시	20
비디오 보기 및 녹화	21
대역폭 및 저장 공간 감소	21
네트워크 스토리지 설정	21
비디오 녹화 및 시청	22
이벤트의 룰 설정	22
액션 트리거	22
모션이 감지되면 카메라에서 비디오를 녹화	22
차량이 잘못된 방향으로 주행할 때 카메라의 영상을 녹화	23
레이더의 빨간색 신호등을 활성화	24
누군가가 금속 물체로 레이더를 가리면 이메일 보내기	25
모션 디텍션 시 조명을 켜기	26
레이더로 PTZ 카메라를 제어	26
레이더 데이터를 전송하기 위해 MQTT 사용	27
웹 인터페이스	29
상태	29
레이더	30
설정	30
스트림	31
지도 보정	32
제외 영역	33

시나리오.....	34
오버레이.....	35
동적 LED 스트립.....	37
레이더 PTZ 오토트래킹.....	37
녹화물.....	38
앱.....	39
시스템.....	40
시간과 장소.....	40
네트워크.....	41
보안.....	45
계정.....	51
이벤트.....	54
MQTT.....	58
저장.....	62
스트립 프로파일.....	64
ONVIF.....	65
디렉터.....	68
액세서리.....	68
에지 투 에지.....	68
로그.....	70
일반 구성.....	71
유지보수.....	72
유지보수.....	72
문제 해결.....	73
설치 확인.....	74
레이더 설치 확인.....	74
검증 완료.....	75
상세 정보.....	76
스트리밍 및 저장.....	76
비디오 압축 형식.....	76
비트 레이트 제어.....	76
오버레이.....	78
사양.....	79
제품 개요.....	79
LED 표시.....	79
.....	79
SD 카드 슬롯.....	80
버튼.....	80
제어 버튼.....	80
커넥터.....	80
네트워크 커넥터(PoE 입력).....	80
네트워크 커넥터(PoE 출력).....	80
I/O 커넥터.....	81
전원 커넥터.....	82
장치 세척.....	83
문제 해결.....	84
공장 출하 시 기본 설정으로 재설정.....	84
현재 AXIS OS 버전 확인.....	84
AXIS OS 업그레이드.....	84
기술적 문제, 단서 및 해결 방안.....	85
성능 고려 사항.....	86
지원 센터 문의.....	86

설치

이 비디오는 레이더 설치 방법의 예를 보여 줍니다.

모든 설치 시나리오에 대한 전체 지침과 중요한 안전 정보는 axis.com/products/axis-d2210-ve-radar/support에서 설치 가이드를 참조하십시오



고려 사항

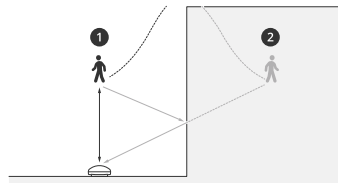
제품을 설치할 위치

영역 또는 도로 모니터링

레이더는 개방된 지역을 모니터링하기 위한 것이며 영역 모니터링이나 도로 모니터링에 사용할 수 있습니다. 레이더에는 각 시나리오에 대한 성능을 최적화하기 위한 두 가지 프로파일이 있습니다. 감지 범위, 설치 예 및 사용 사례에 대한 자세한 내용은 항목을 참조하십시오.

고체와 반사 객체 방지

적용 범위에 있는 대부분의 단단한 객체(예: 벽, 울타리, 나무 또는 큰 덩불)는 그 뒤에 사각 지대(레이더 그림자)를 생성합니다. 화각 내에 있는 금속 객체는 레이더가 분류를 수행하는 능력에 영향을 미치는 반사를 일으킵니다. 이로 인해 레이더 스트림에서 고스트 트랙과 허위 알람이 발생할 수 있습니다.



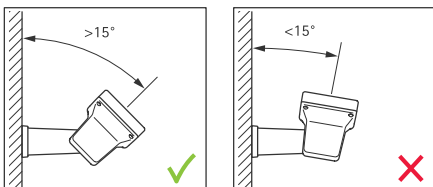
- 1 실제 감지
- 2 반사 감지(고스트 트랙)

고체와 반사 객체를 처리하는 방법에 대한 자세한 내용은 항목을 참조하십시오.

포지셔닝

안정적인 폴 또는 다른 객체나 설치물이 없는 벽면에 제품을 설치합니다. 제품의 좌우 1m(3ft) 내에 있으며 전파를 반사하는 물체는 레이더의 성능에 영향을 미칩니다.

제품을 벽에 설치하는 경우 벽과 최소 15° 각도를 유지해야 합니다.

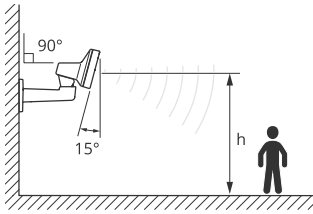


롤 각도

제품의 롤 각도는 0과 거의 같아야 합니다. 즉, 레이더가 수평선과 수평을 이루어야 합니다.

틸트 각도

레이더는 0~30°까지 기울일 수 있지만, 장치의 권장 마운트 기울기는 15°입니다. 15° 기울기를 달성하려면 그림과 같이 새시의 뒷부분이 수평을 이루도록 합니다.



레이더의 틸트 각도를 표시하는 오버레이를 레이더의 실시간 보기에 추가할 수 있습니다. 지침에 대한 자세한 내용은 항목을 참조하십시오

공존

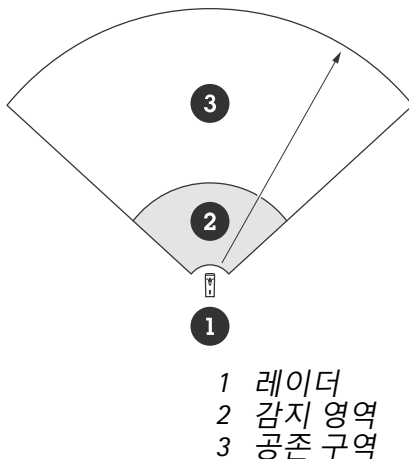
60GHz 주파수 대역에서 작동하는 8개 이상의 Axis 레이더를 서로 가깝게 마운트하면 서로 간섭할 수 있습니다. 간섭을 방지하려면, 항목을 참조하십시오.

여러 레이더 설치

건물 주변이나 펜스 밖의 완충지대 등을 감시하기 위해 여러 대의 레이더를 설치할 수 있습니다.

공존

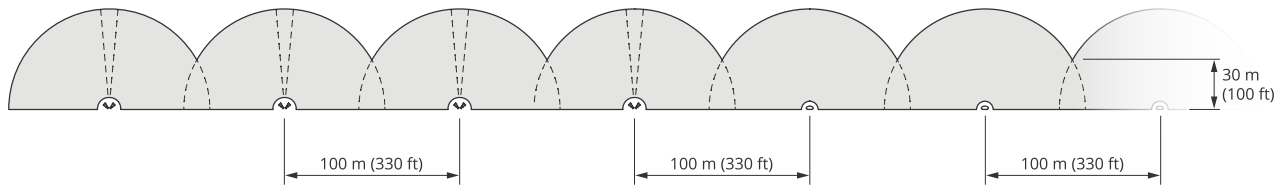
레이더는 감지 영역을 벗어나 계속 진행하며 최대 350m(380야드) 떨어진 다른 레이더에 간섭을 일으킬 수 있습니다. 이것을 공존 영역이라고 합니다.



이 레이더는 60GHz 주파수 대역에서 작동합니다. 60GHz 주파수 대역에서 작동하는 레이더를 최대 8개까지 서로 가까이 또는 서로 마주보게 설치하여 문제 없이 설치할 수 있습니다. 내장된 공존 알고리즘은 간섭을 최소화하는 적절한 시간 슬롯과 주파수 채널을 찾을 수 있습니다.

동일한 주파수 대역에서 작동하는 8개 이상의 레이더가 설치되어 있고 많은 장치가 서로 멀리 떨어져 있는 경우 간섭 위험이 줄어듭니다. 일반적으로 레이더 작동은 레이더 간섭으로 인해 중지되지 않습니다. 간섭이 있는 경우에도 레이더 신호를 복구하려고 시도하는 간섭 완화 알고리즘이 내장되어 있습니다. 동일한 공존 구역, 동일한 주파수 대역에서 많은 레이더가 작동하는 환경에서는 간섭에 대한 경고가 발생할 것으로 예상됩니다. 간섭의 주요 영향은 감지 성능 저하와 간헐적인 고스트 트랙입니다.

서로 다른 주파수 대역에서 작동하는 Axis 레이더는 서로 간섭하지 않습니다. 예를 들어 AXIS D2210-VE를 간섭 없이 24GHz 주파수 대역에서 작동하는 여러 AXIS D2110-VE Security Radar와 결합할 수 있습니다.



AXIS D2210-VE 4쌍과 여러 AXIS D2110-VE Security Radar가 나란히 마운트되어 있습니다.

비고

AXIS D2110-VE Security Radar는 두 개 이상의 AXIS D2110-VE가 동일한 공존 영역에 마운트된 경우 추가 구성이 필요합니다. 자세한 내용은 *AXIS D2110-VE Security Radar 사용자 설명서*를 참조하십시오.

환경

주변 환경, 흔들리는 객체, 깃대 및 흔들리는 초목과 같이 사이트에 여러 레이더를 배치할 때 확인해야 할 다른 설계 요소도 있습니다. 때로 허위 알람을 피하려면 레이더 스트림에서 흔들리는 객체를 필터링해야 합니다.

레이더 프로파일

영역 모니터링이나 도로 모니터링에 레이더를 사용할 수 있습니다. 각 시나리오에 최적화된 두 가지 프로파일이 있습니다.

- **영역 모니터링 프로파일:** 55km/h(34mph) 미만의 속도로 움직이는 사람, 차량 및 미확인 객체를 추적
- **도로 모니터링 프로파일:** 주로 최대 200km/h(125mph)의 속도로 움직이는 차량을 추적

레이더의 웹 인터페이스에서 영역 또는 모니터링 프로파일을 선택합니다. 자세한 내용은 항목을 참조하십시오.

Area monitoring profile(영역 모니터링 프로파일)

area monitoring profile(영역 모니터링 프로파일)은 최대 55km/h(34mph)의 속도로 움직이는 객체에 최적화되었습니다. 이 프로파일을 사용하면 객체가 사람인지, 차량인지 또는 알려지지 않은 것인지 감지할 수 있습니다. 이러한 객체가 감지되면 액션을 트리거하도록 룰을 설정할 수 있습니다. 고속으로 움직이는 차량만 추적하려면, 항목을 사용하십시오.

커버리지 범위

AXIS D2210-VE의 수평 감지 범위는 95°입니다. 커버리지 영역은 사람의 경우 2700m²(29000ft²)에 해당하고 차량의 경우 6100m²(65600ft²)에 해당합니다.

비고

레이더가 3.5~7m(11~23ft)에 마운팅된 경우 최적의 영역 범위가 적용됩니다. 장착 높이는 레이더 아래의 사각지대 크기에 영향을 미칩니다.

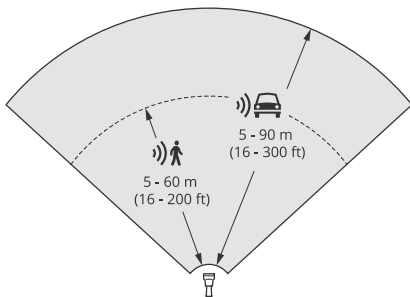
영역 감지 범위

감지 범위는 객체를 추적할 수 있고 알람을 트리거시킬 수 있는 거리 이내를 가리킵니다. 이는 근거리 감지 한도(감지가 이루어질 수 있는 장치의 최소 거리)에서 원거리 감지 한도(감지가 이루어질 수 있는 장치의 최대 거리) 사이에서 측정됩니다.

area monitoring profile(영역 모니터링 프로파일)은 사람을 감지하는 데 최적화되어 있지만 +/-2km/h(1.24mph)의 속도 오차 내에서 최대 55km/h(34mph)로 움직이는 차량이나 다른 물체를 추적할 수 있습니다.

최적의 설치 높이에 마운트할 때 감지 범위는 다음과 같습니다.

- 사람 감지 시 5~60m(16~200ft)
- 차량 감지 시 5~90m(16~300ft)



비고

- 레이더를 보정할 때 웹 인터페이스에서 장착 높이를 입력합니다.
- 감지 범위는 장면과 제품의 틸트 각도에 따라 달라집니다.
- 감지 범위는 움직이는 객체 유형과 크기에 영향을 받습니다.

레이더 감지 범위는 다음 조건에서 측정되었습니다.

- 범위는 지면을 따라 측정되었습니다.
- 객체는 키가 170cm(5피트 7인치)였습니다.
- 그 사람은 레이더 앞에서 똑바로 걷고 있었습니다.
- 사람이 감지 영역에 들어갈 때 값이 측정되었습니다.
- 레이더 감도는 **Medium(중간)**으로 설정되었습니다.

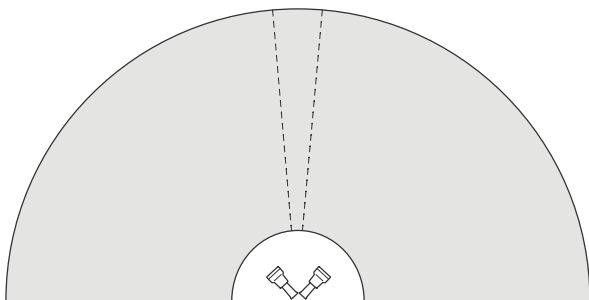
장착 높이	0° 틸트	5° 틸트	10° 틸트	15° 틸트	20° 틸트	25° 틸트	30° 틸트
3.5m (11ft)	6.0~60+m (19~196+ft)	5.0~60+m (16~196+ft)	4.0~60+m (13~196+ft)	4.0~60m (13~196f-t)	4.0~55m (13~180f-t)	4.0~40m (13~131f-t)	4.0~30m (13~98ft)
4.5m (14ft)	6.0~60+m (19~196+ft)	6.0~60+m (19~196+ft)	5.0~60+m (16~196+ft)	4.0~60+m (13~96+ft)	4.0~60m (13~196f-t)	4.0~45m (13~147f-t)	4.0~40m (13~131f-t)
6m (19ft)	10~60+m (32~196+ft)	9.0~60+m (29~196+ft)	7.0~60+m (22~196+ft)	6.0~60+m (19~196+ft)	6.0~60m (19~196ft)	5.0~55m (16~180f-t)	5.0~55m (16~180f-t)
8m (26ft)	16~60m (52~196f-t)	14~60m (45~196f-t)	10~60m (32~196f-t)	8.0~60+m (26~196+ft)	8.0~60+m (26~196+ft)	7.0~60m (22~196f-t)	7.0~60m (22~196f-t)
10m (32ft)	21~60m (68~196f-t)	19~60m (62~196f-t)	14~60m (45~196f-t)	12~60+m (39~196+ft)	10~60+m (32~196+ft)	9.0~60m (29~196f-t)	9.0~60m (29~196f-t)
12m (39ft)	25~60m (82~196f-t)	23~60m (75~196f-t)	19~60m (62~196f-t)	16~60+m (52~196+ft)	13~60+m (42~196+ft)	11~60+m (36~196+ft)	11~55m (36~180f-t)

비고

- 레이더 감도를 **Low(낮음)**로 설정하면 감지 범위가 20% 감소하고 **High(높음)**로 설정하면 감지 범위가 20% 증가합니다.

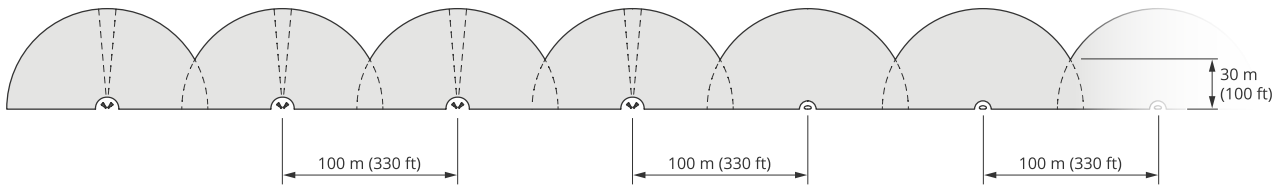
영역 설치 예

건물의 주변이나 경계에 가상 울타리를 생성하려면 최대 8개의 AXIS D2210-VE Radar를 나란히 배치할 수 있습니다. AXIS D2210-VE 두 대를 나란히 배치하면 180°의 커버리지가 제공됩니다.



180° 적용 범위를 위해 두 개의 AXIS D2210-VE가 나란히 마운트되어 있습니다.

두 쌍 이상의 AXIS D2210-VE를 나란히 설치할 경우 각 쌍 사이에 100m(330ft) 간격을 두고 배치하는 것이 좋습니다.



4쌍의 AXIS D2210-VE와 100m(330ft) 간격으로 설치된 여러 대의 AXIS D2110-VE Security Radar.

서로 다른 주파수 대역에서 작동하는 Axis 레이더는 서로 간섭하지 않습니다. 즉, 60GHz 주파수 대역에서 작동하는 AXIS D2210-VE를 AXIS D2110-VE Security Radar와 결합할 수 있으며, 동일한 공존 영역의 24GHz 주파수 대역에서 작동합니다.

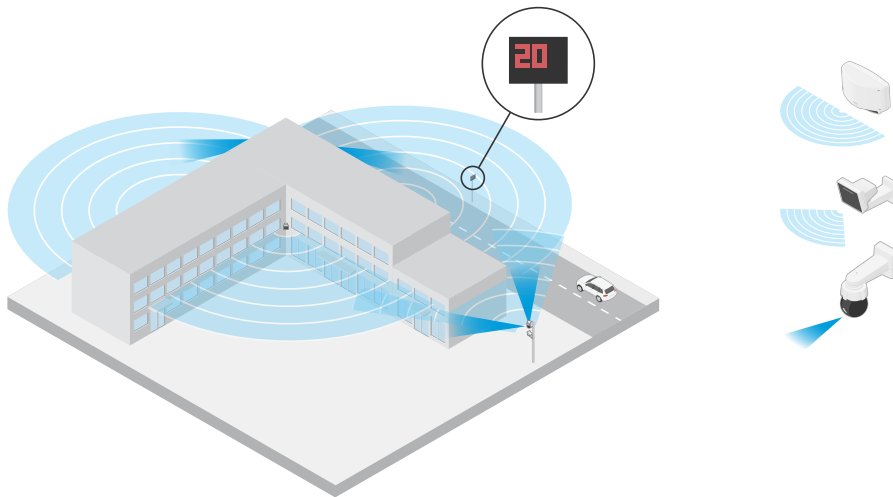
공존과 간섭에 대한 자세한 내용은 항목을 참조하십시오.

영역 모니터링 사용 사례

Cover the area around a building(건물 주변 영역 커버)

사무실 건물에 있는 회사는 특히 근무 시간 이후에 침입과 기물 파손으로부터 건물을 보호해야 합니다. 건물 주변 지역을 감시하기 위해 레이더와 PTZ 카메라를 함께 설치합니다. 건물의 긴 측면을 커버하기 위해 180° 범위를 커버하는 AXIS D2110-VE Security Radar를 사용하고, 짧은 측면과 모서리를 위해 95° 범위를 커버하는 AXIS D2210-VE Radar를 사용합니다. 근무 시간 이후 사람이 건물에 접근하면 경보가 울리도록 레이더를 구성했습니다. 잠재적인 침입자를 시각적 확인하기 위해 두 대의 PTZ 카메라를 추가합니다. 레이더는 AXIS Radar Autotracking for PTZ(PTZ용 AXIS Radar Autotracking)을 통해 PTZ 카메라를 조종할 수 있습니다.

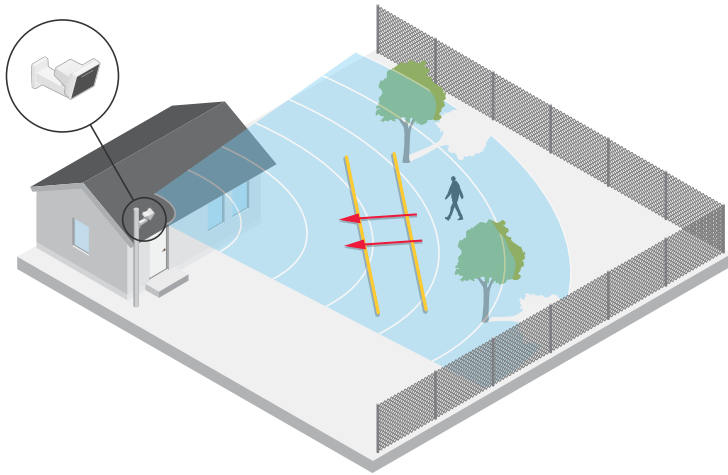
또한 회사는 근무 시간 동안 건물을 안전하게 유지하기를 원합니다. 건물 옆 도로를 지나가는 차량이 속도 제한 내에 있는지 확인하기 위해 Microbus용 AXIS Radar Integration을 사용하여 AXIS D2110-VE Security Radar 중 하나를 Microbus의 속도 표지판과 페어링합니다.



Cover a complex scene(복잡한 장면을 커버)

구내 건물에 중요 장비를 보관하는 회사는 침입자를 막기 위해 울타리로 둘러싸여 있습니다. 탬퍼링 및 방해 행위를 방지하려면 추가 보호가 필요합니다. 그들이 바라는 것은 인간이 건물에 접근할 때 알람을 울리는 것입니다. 그러나 장면에는 나뭇가지가 흔들리는 나무, 반사를 일으킬 수 있는 금속 울타리, 심지어 현장 주변을 돌아다니는 작은 동물도 포함되어 있어 모두 허위 알람을 유발할 수 있습니다.

허위 알람을 줄이기 위해 레이더의 웹 인터페이스에서 시나리오를 구성하여 접근하는 객체가 알람이 트리거되기 전에 두 개의 가상 선을 넘어야 합니다. 이렇게 하면 의도적으로 건물을 향해 이동하는 객체에 대해 트리거하는 데 도움이 되며, 가상 선 중 하나를 막 교차하는 객체는 필터링됩니다.



펜스가 없는 현장에서는 두 라인이 가상 펜스 역할을 할 수 있습니다. 레이더의 웹 인터페이스에서 시나리오에 두 라인을 추가하는 방법에 대해 자세히 알아보려면 항목을 참조하십시오.

도로 모니터링 프로파일

도로 모니터링 프로파일은 교외 도로 및 고속도로에서 최대 200km/h(125mph)로 움직이는 차량을 추적하는 데 최적화되어 있습니다. 낮은 속도로 움직이는 사람과 기타 물체를 추적하려면 영역 모니터링 프로파일을 사용합니다. 자세한 내용은 를 참조하십시오.

도로 감지 범위

road monitoring profile(도로 모니터링 프로파일)은 차량 감지에 최적화되어 있으며 최대 200km/h(125mph)의 속도로 움직이는 차량을 모니터링할 때 속도 오차는 $\pm 2\text{km/h}$ (1.24mph)입니다.

레이더의 장착 높이와 차량 속도는 감지 범위에 영향을 미칩니다. 최적의 설치 높이에 마운트되면 레이더는 다음 범위 내에서 $\pm 2\text{km/h}$ (1.24mph)의 속도 정확도로 접근 및 출발 차량을 감지합니다.

- **50km/h(31mph)**로 이동하는 차량의 경우 25 ~ 100m(82 ~ 328ft).
- **100km/h(62mph)**로 이동하는 차량의 경우 40 ~ 80m(131 ~ 262ft).
- **200km/h(125mph)**로 이동하는 차량의 경우 50 ~ 70m(164 ~ 230ft).

비고

고속으로 이동하는 차량을 감지하지 못하는 위험을 최소화하려면 **Vehicle(차량)** 및 **Unknown(알 수 없음)** 객체 유형에서 트리거되는 레이더 시나리오를 설정하십시오. 시나리오 설정 방법에 대한 자세한 내용은 항목을 참고하십시오.

도로 설치 예

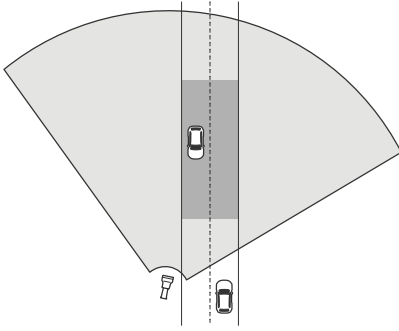
도로 및 고속도로를 모니터링할 때는 차량 뒤의 사각 지대(레이더 그림자)가 생기지 않도록 레이더를 충분한 높이에 마운트하십시오.

비고

레이더 그림자의 크기는 레이더 마운트 높이와 차량 높이 및 레이더로부터의 거리에 따라 달라집니다. 예를 들어 4.5m(15ft) 높이의 차량이 50 m(164ft) 높이에 마운트된 레이더에서 8m(26ft) 떨어져 있는 경우, 차량 뒤의 레이더 그림자는 50m(164ft)입니다. 그러나 레이더가 12m(39ft) 높이에 마운트된 경우, 동일한 차량 뒤의 그림자는 23m(74ft)만 됩니다.

측면 마운트

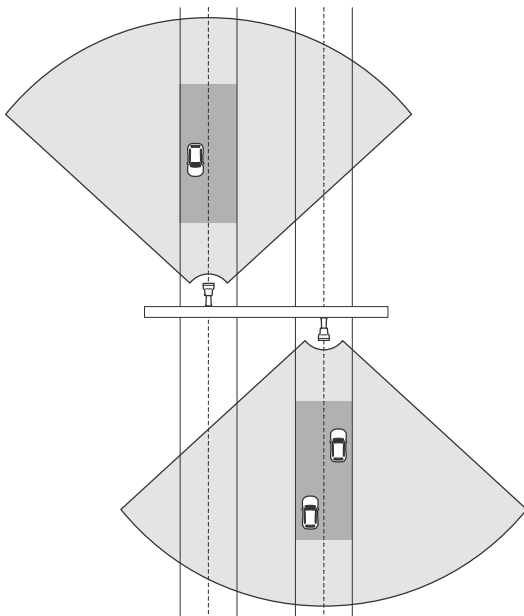
도로를 따라 이동하는 차량을 모니터링하기 위해 도로 측면(예: 기둥)에 레이더를 마운트할 수 있습니다. 이러한 설치 유형에서는 최대 25°의 팬 각도를 권장합니다.



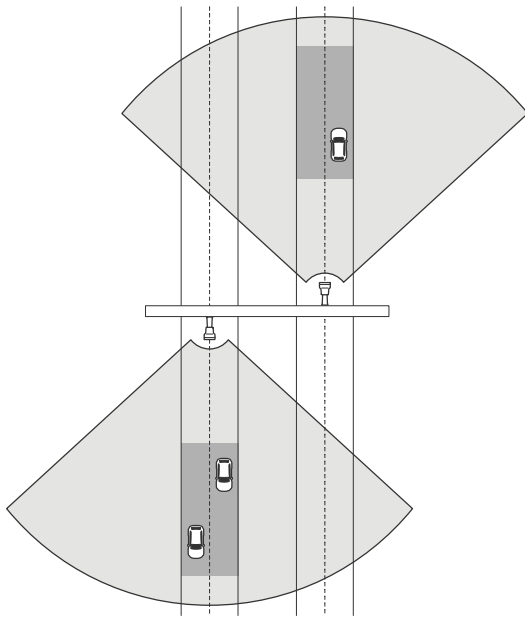
고속을 정확하게 측정하려면 차량으로부터 10m(32ft)의 측면 거리 내에 레이더를 배치하십시오. 감지 범위 및 속도 정확도에 대한 자세한 내용은 항목을 참고하십시오.

중앙 마운트

다중 차선 도로에서 차량을 모니터링하려면 도로 위의 갠트리에 하나 이상의 레이더를 마운트할 수 있습니다.



레이더를 향해 주행하는 대신 레이더에서 멀어지는 차량을 모니터링하려는 경우에도 동일한 유형의 설치가 가능합니다.



고속을 정확하게 측정하려면 차량으로부터 10m(32ft)의 측면 거리 내에 레이더를 배치하십시오. 감지 범위 및 속도 정확도에 대한 자세한 내용은 항목을 참조하십시오.

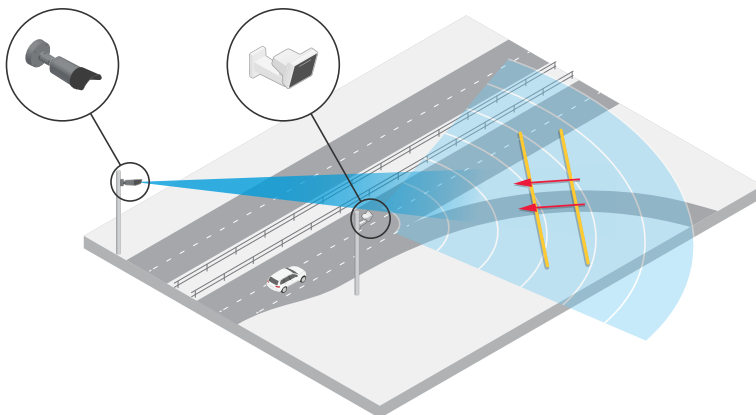
도로 모니터링 사용 사례

AXIS D2210-VE Radar와 도로 모니터링 프로파일의 일반적인 사용 사례는 차량 속도를 추적하고 측정하는 것입니다. 또한 시각적 카메라 및 AXIS Speed Monitor 애플리케이션과 함께 레이더를 사용하여 카메라의 실시간 보기에서 차량 속도를 시각화하거나 통계 처리를 위해 레이더 트랙을 기록할 수 있습니다. 자세한 내용은 *AXIS Speed Monitor 사용자 설명서*를 참조하십시오.

도로 모니터링 프로파일을 사용할 때 레이더를 설정하는 방법에 대한 추가 예는 다음 사용 사례를 참조하십시오.

Wrong-way detection on a highway ramp(고속도로 진입로에서 잘못된 방향 감지)

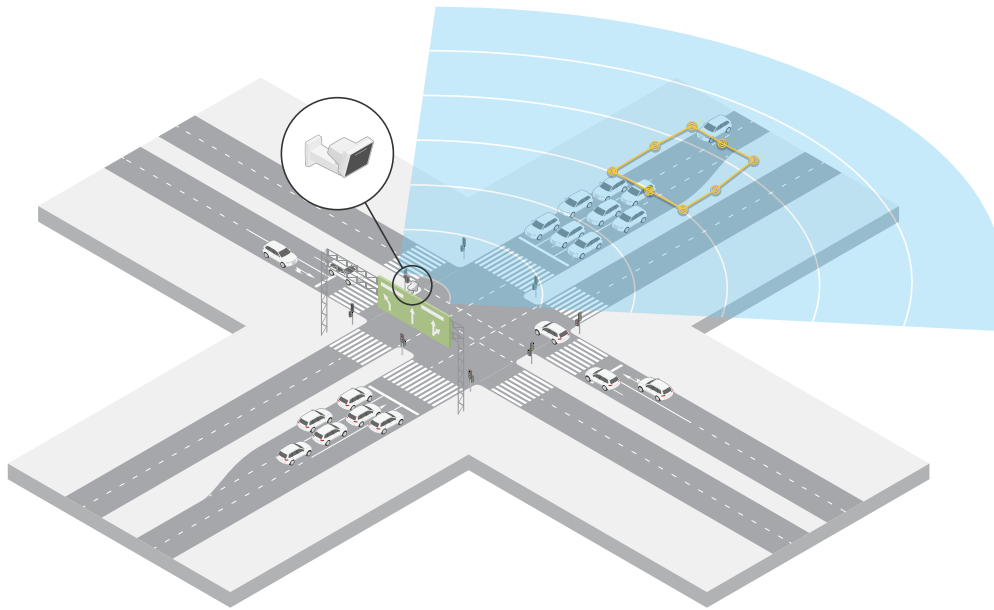
고속도로 진입로에서 잘못된 방향으로 운전하는 차량을 감지하고 식별하기 위해 교통 통제에서는 AXIS D2210-VE 및 Axis 볼릿 스타일 카메라를 사용합니다. 그들은 잘못된 방향으로 운전하는 차량을 감지하기 위해 경사로를 향한 기둥에 레이더를 마운트합니다. 안정적인 감지를 위해 선 넘기 시나리오를 설정하고 차량이 알람을 트리거하려면 두 개의 라인을 교차해야 하도록 레이더를 구성합니다. 이 시나리오에서는 그림에 표시된 대로 경사로에 두 개의 선을 배치합니다. 또한 트리거할 주행 방향과 속도를 지정합니다. 레이더가 알람을 트리거하면 Axis 볼릿 스타일 카메라가 경사로에 있는 차량을 시각적으로 식별할 수 있습니다.



Monitor traffic flow at an intersection - queue build-up(교차로 교통 흐름 모니터링 - 큐 축적)

혼잡한 교차로에 큐가 어떻게, 언제 축적되는지 모니터링하기 위해 교통 통제는 교차로 위의 갭트리에 레이더를 설치합니다. 그들은 레이더의 웹 인터페이스에서 시나리오를 설정하고 특정 지역에서 이동하는 차량에 대해 트리거되도록 구성합니다. 그들은 교차로로 이어지는 도로 부분만 포함하도록

시나리오를 형성합니다. 큐가 축적되기 시작할 때 알람을 트리거하기 위해 5km/h(3mph) 미만의 속도로 이동하는 차량에서 발생하도록 시나리오를 구성합니다.



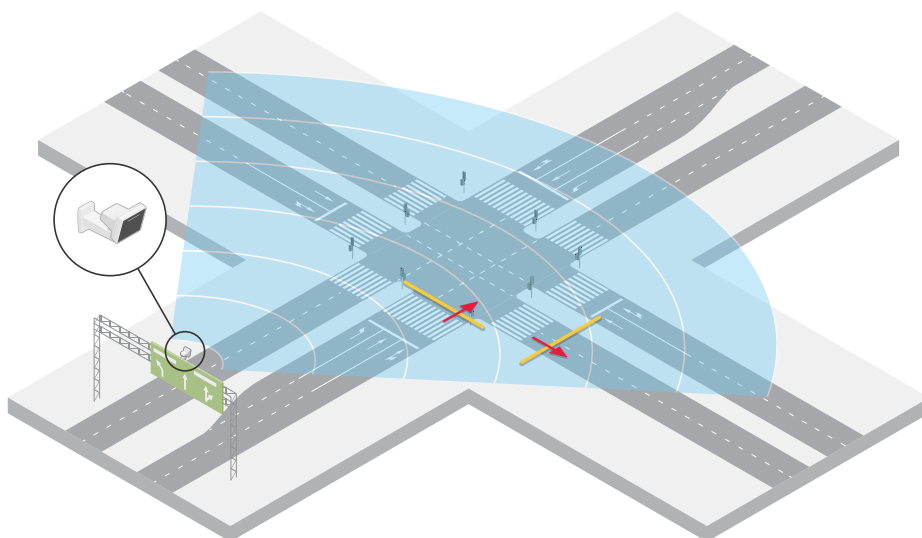
Monitor traffic flow at an intersection - direction(교차로 교통 흐름 모니터링 - 방향)

혼잡한 교차로에서 교통 흐름과 차량 이동 방향에 대한 오버뷰를 얻기 위해 교통 통제팀은 교차로로 이어지는 도로 위의 갱트리에 레이더를 설치합니다. 그들은 차량이 알람을 발령하기 위해 두 개의 라인을 횡단해야 하는 레이더의 웹 인터페이스에서 선 넘기 시나리오를 설정했습니다. 시나리오를 구성할 때 교차로로 이어지는 차선 위에 두 개의 선 중 첫 번째 선을 횡단보도 뒤에 배치하여 차량이 선에 정차하는 것을 방지합니다. 그들은 오른쪽으로 이어지는 차선 위에 두 번째 선을 배치합니다. 알람이 울리려면 차량이 지정된 방향으로 두 라인을 모두 통과해야 합니다. 가로지르기당 두 대 이상의 차량에 대한 트리거링을 방지하기 위해 시나리오의 최소 트리거 지속 시간을 2초에서 0초로 낮춥니다.

모든 방향의 교통 흐름을 모니터링하기 위해 각 방향에 대해 하나의 시나리오를 생성합니다.

비고

이 시나리오에서는 선을 넘는 차량 수를 계산하지 않습니다. 대신 레이더 웹 인터페이스의 이벤트 시스템을 사용하여 수를 유지할 수 있습니다. 차량 수를 계산하는 한 가지 방법은 시나리오가 트리거될 때마다 MQTT 메시지를 보내고 MQTT 수신자 측에서 트리거 수를 계산하는 것입니다.



시작하기

네트워크에서 장치 찾기

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

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

브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

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

*완벽하게 지원되지는 않습니다. 비디오 스트림 문제가 발생하면 다른 브라우저를 사용하십시오.

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. 을 참조하십시오.

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. 을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이선스 계약을 수락하십시오.
5. **Add account(계정 추가)**를 클릭합니다.

중요 사항

장치에 기본 계정이 없습니다. 관리자 계정의 패스워드를 잊어버린 경우, 장치를 재설정해야 합니다. 을 참조하십시오.

안전한 패스워드

중요 사항

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

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

데이터 보호를 위해 적극 권장되는 작업은 다음과 같습니다.

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

아무도 장치 소프트웨어를 조작하지 않았는지 확인

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

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

웹 인터페이스 개요

이 영상은 장치의 웹 인터페이스에 대한 개요를 제공합니다.



Axis 장치 웹 인터페이스

장치 구성

레이더 프로파일을 선택합니다.

웹 인터페이스에서:

1. **Radar > Settings > Detection(레이더 > 설정 > 감지)**으로 이동합니다.
2. **Radar profiles(레이더 프로파일)** 아래에서 프로파일을 선택합니다.

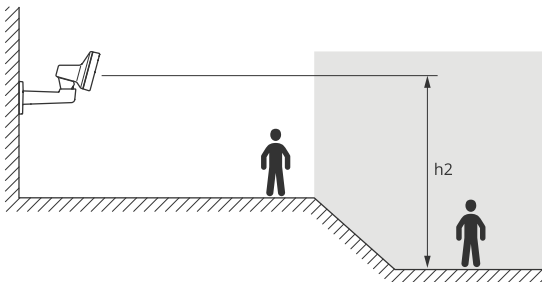
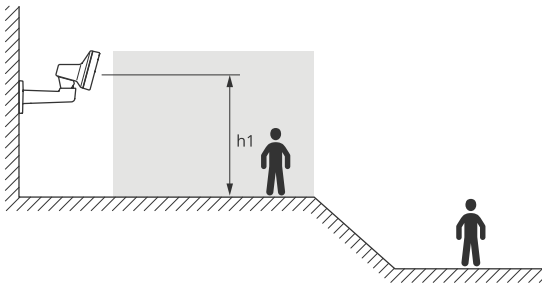
장착 높이 설정

웹 인터페이스에서 레이더의 장착 높이를 설정합니다. 이를 통해 레이더가 지나가는 객체의 속도를 정확하게 감지할 수 있습니다.

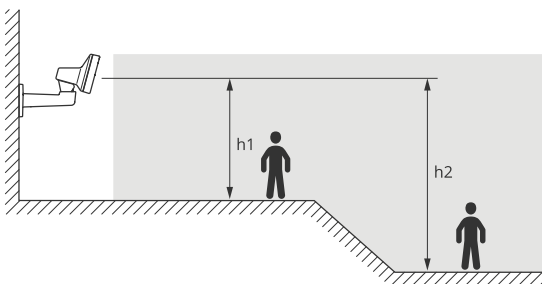
지면에서 레이더까지의 높이를 최대한 정확하게 측정합니다. 표면이 고르지 않은 장면의 경우 장면의 평균 높이를 나타내는 값을 설정합니다.

예:

관심 영역에 따라 마운트 높이(h1, h2)가 다릅니다.



관심 영역의 표면이 고르지 않은 경우 레이더를 구성할 때 평균 높이(이 경우 $(h1 + h2) / 2$)를 추가합니다.



Set the mounting height(장착 높이 설정):

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

참조 지도로 보정

참조 지도를 업로드하면 감지된 객체의 이동 경로를 더 쉽게 확인할 수 있습니다. 레이더가 커버하는 영역을 보여주는 평면도나 항공사진을 사용할 수 있습니다. 레이더 범위가 지도의 위치, 방향, 축척에 맞도록 지도를 보정하고, 레이더 범위의 특정 부분에 관심이 있는 경우 지도를 확대합니다.

지도 보정을 단계별로 안내하는 설정 도우미를 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 조정하면 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 기능을 사용해도 레이더의 커버리지 범위는 변경되지 않습니다. 확대/축소 후 커버리지의 일부가 시야에서 벗어난 경우에도, 레이더는 전체 커버리지 영역에서 움직이는 객체를 감지합니다. 감지된 움직임을 제외하는 유일한 방법은 제외 영역을 추가하는 것입니다. 자세한 내용은 를 참조하십시오.

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.

감지 영역 설정

모션을 감지할 위치를 결정하기 위해 하나 이상의 감지 영역을 추가할 수 있습니다. 다른 영역을 사용하여 다른 액션을 트리거합니다.

두 가지 유형의 영역이 있습니다.

- **scenario(시나리오)**(이전에는 포함 영역이라고 함)은 움직이는 객체가 룰을 트리거하는 영역입니다. 기본 시나리오는 레이더가 커버하는 전체 영역과 일치합니다.
- **exclude zone(제외 영역)**은 움직이는 객체가 무시되는 영역입니다. 시나리오 내에 원하지 않는 알람을 많이 트리거하는 영역이 있는 경우 제외 영역을 사용합니다.

시나리오 추가

시나리오는 이벤트 시스템에서 룰을 생성하는 데 사용할 수 있는 트리거 조건과 디텍션 설정의 조합입니다. 장면의 다른 부분에 대해 다른 룰을 생성하려면 시나리오를 추가하십시오.

시나리오 추가:

1. **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
2. **Add scenario(시나리오 추가)**를 클릭합니다.
3. 시나리오 이름을 입력하십시오.
4. 영역에서 움직이거나 하나 이상의 라인을 가로지르는 객체에 대해 트리거하려면 선택합니다.

영역에서 움직이는 객체에 대한 트리거:

1. **Movement in area(영역 내 이동)**를 선택합니다.
2. **Next (다음)**를 클릭합니다.
3. 시나리오에 포함되어야 하는 영역 유형을 선택합니다.
마우스를 사용하여 레이더 이미지나 참조 지도의 원하는 부분을 포함할 수 있도록 영역을 이동하고, 모양을 변경합니다.
4. **Next (다음)**를 클릭합니다.
5. 감지 설정을 추가합니다.
1. **Ignore short-lived objects(빠른 객체 무시)** 아래에서 트리거까지 걸리는 초를 추가합니다.
2. **Trigger on object type(객체 유형에 대한 트리거)** 아래에서 트리거할 객체 유형을 선택합니다.
3. **Speed limit(속도 제한)** 아래에서 속도 제한 범위를 추가합니다.
6. **Next (다음)**를 클릭합니다.
7. **Minimum trigger duration(최소 트리거 기간)** 아래에서 알람의 최소 지속 시간을 설정합니다.
8. **Save(저장)**를 클릭합니다.

라인을 가로지르는 객체에서 트리거:

1. **Line crossing(선 넘기)**를 선택합니다.
2. **Next (다음)**를 클릭합니다.
3. 장면에 라인을 배치합니다.
마우스를 사용하여 라인을 이동하고 모양을 조정합니다.
4. 감지 방향을 변경하려면 **Change direction(방향 전환)**을 켭니다.
5. **Next (다음)**를 클릭합니다.
6. 감지 설정을 추가합니다.
 - 6.1. **Ignore short-lived objects(빠른 객체 무시)** 아래에서 트리거까지 걸리는 초를 추가합니다.
 - 6.2. **Trigger on object type(객체 유형에 대한 트리거)** 아래에서 트리거할 객체 유형을 선택합니다.
 - 6.3. **Speed limit(속도 제한)** 아래에서 속도 제한 범위를 추가합니다.
7. **Next (다음)**를 클릭합니다.
8. **Minimum trigger duration(최소 트리거 기간)** 아래에서 알람의 최소 지속 시간을 설정합니다.
기본값은 2초로 설정되어 있습니다. 객체가 라인을 넘을 때마다 시나리오가 트리거되도록 하려면 지속 시간을 0초로 낮춥니다.
9. **Save(저장)**를 클릭합니다.

두 개의 라인을 넘는 객체에서 트리거:

1. **Line crossing(선 넘기)**를 선택합니다.

2. **Next (다음)**를 클릭합니다.
3. 알람이 트리거될 때 객체가 두 라인을 넘도록 하려면 **Require crossing of two lines(두 라인을 횡단해야 함)**를 켭니다.
4. 장면에 라인을 배치합니다.
마우스를 사용하여 라인을 이동하고 모양을 조정합니다.
5. 감지 방향을 변경하려면 **Change direction(방향 전환)**을 켭니다.
6. **Next (다음)**를 클릭합니다.
7. 감지 설정을 추가합니다.
 - 7.1. **Max time between crossings(교차로 간 최대 시간)** 아래에서 첫 번째 라인과 두 번째 라인 사이의 시간 제한을 설정합니다.
 - 7.2. **Trigger on object type(객체 유형에 대한 트리거)** 아래에서 트리거할 객체 유형을 선택합니다.
 - 7.3. **Speed limit(속도 제한)** 아래에서 속도 제한 범위를 추가합니다.
8. **Next (다음)**를 클릭합니다.
9. **Minimum trigger duration(최소 트리거 기간)** 아래에서 알람의 최소 지속 시간을 설정합니다.
기본값은 2초로 설정되어 있습니다. 객체가 두 개의 라인을 넘을 때마다 시나리오가 트리거되도록 하려면 지속 시간을 0초로 낮춥니다.
10. **Save(저장)**를 클릭합니다.

제외 영역 추가

제외 영역은 움직이는 객체가 무시되는 영역입니다. 예를 들어, 길가에 흔들리는 나뭇잎을 무시하려면 제외 영역을 추가합니다. 금속 울타리와 같은 레이더 반사가 일어나는 소재로 인해 발생하는 고스트 트랙을 무시하기 위해 제외 영역을 추가할 수도 있습니다.

제외 영역 추가:

1. **Radar > Exclude zones(레이더 > 제외 영역)**로 이동합니다.
2. **Add exclude zone(제외 영역 추가)**을 클릭합니다.
마우스를 사용하여 레이더 보기나 참조 지도의 원하는 부분을 포함할 수 있도록 영역을 이동하고 모양을 변경합니다.

허위 알람을 최소화하는 방법

허위 경보가 너무 많이 온다고 생각되면 특정한 유형의 움직임이나 물체를 필터링하거나, 커버리지를 변경하거나, 디텍션 감도를 조정할 수 있습니다. 어느 설정이 환경에 가장 적합한지 확인합니다.

- 레이더의 감지 감도를 조정합니다.
Radar > Settings > Detection(레이더 > 설정 > 디텍션)으로 이동한 후 더 낮은 **Detection sensitivity(디텍션 감도)**를 선택합니다. 이렇게 하면 허위 알람이 발생할 위험은 줄어들지만, 레이더에서 일부 움직임도 누락될 수 있습니다.
감도 설정은 모든 영역에 영향을 미칩니다.
 - **Low(낮음):** 이 감도는 영역에 금속 객체나 대형 차량이 많이 있을 때 사용합니다. 레이더는 물체를 추적하고 분류하는 데 시간이 더 오래 걸립니다. 이는 특히 빠르게 움직이는 물체의 경우 감지 범위를 줄일 수 있습니다.
 - **Medium(중간):** 이것이 기본 설정입니다.
 - **High(높음):** 이 감도는 레이더 앞에 금속 물체가 없는 노지가 있을 때 사용합니다. 이는 사람에 대한 감지 범위를 늘립니다.
- 시나리오 수정 및 영역 제외:
시나리오에 금속 벽과 같은 단단한 표면이 포함된 경우 단일 물리적 객체에 대해 여러 번 감지하는 반사가 있을 수 있습니다. 시나리오 모양을 수정하거나 시나리오의 특정 부분을 무시하는 제외 영역을 추가할 수 있습니다. 자세한 내용은 **및 항목**을 참조하십시오.

- 하나가 아닌 두 개의 선을 교차하는 객체에 대해 트리거합니다.
선 넘기 시나리오에 흔들리는 객체나 움직이는 동물이 포함된 경우, 객체가 선을 넘어 허위 알람을 트리거할 위험이 있습니다. 이 경우 객체가 두 선을 넘었을 때만 트리거되도록 시나리오를 구성할 수 있습니다. 자세한 내용은 를 참조하십시오.
- 움직임에 대한 필터:
 - **Radar > Settings > Detection(레이더 > 설정 > 감지)**으로 이동하고 **Ignore swaying objects(흔들리는 객체 무시)**를 선택합니다. 이 설정은 감시 영역의 나무, 덤불 및 깃대로 인해 유발되는 허위 알람을 최소화합니다.
 - **Radar > Settings > Detection(레이더 > 설정 > 감지)**으로 이동하고 **Ignore small objects(작은 객체 무시)**를 선택합니다. 이 설정은 영역 모니터링 프로파일에서 사용할 수 있으며 고양이와 토끼와 같이 적용 범위에 있는 작은 물체로 인한 허위 알람을 최소화합니다.
- 시간에 대한 필터:
 - **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
 - 시나리오를 선택하고  을 클릭하여 설정을 수정합니다.
 - **Seconds until trigger(트리거까지 걸리는 초)**에서 더 높은 값을 선택합니다. 이는 레이더가 객체를 추적하기 시작해서 알람을 트리거할 때까지의 지연 시간입니다. 시나리오에서 타이머는 객체가 특정 영역에 들어왔을 때 시작되는 것이 아니라 레이더가 처음 객체를 감지했을 때 시작됩니다.
- 객체 유형에 대한 필터:
 - **Radar > Scenarios(레이더 > 시나리오)**로 이동합니다.
 - 시나리오를 선택하고  을 클릭하여 설정을 수정합니다.
 - 특정 객체 유형에 대한 트리거를 방지하려면 시나리오에서 이벤트를 트리거하지 않아야 하는 객체 유형을 선택 취소합니다.

레이더 이미지를 조정

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다. 특정 기능의 작동 방식에 대해 자세히 알아보려면 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 다른 이미지를 선택하고 **Image(이미지)**를 선택하고  을 클릭합니다.
6. 이미지와 위치를 선택합니다. 실시간 보기에서 오버레이 이미지를 끌어 위치를 변경할 수도 있습니다.

텍스트 오버레이 표시

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

1. **Radar > Overlays(레이더 > 오버레이)**로 이동합니다.
2. **Text(텍스트)**를 선택하고  을 클릭합니다.

3. 비디오 스트림에 표시할 텍스트를 입력합니다.
4. 위치를 선택합니다. 실시간 보기에서 오버레이 텍스트 필드를 끌어 위치를 변경할 수도 있습니다.

레이더의 틸트 각도와 함께 텍스트 오버레이 표시

레이더의 틸트 각도를 표시하는 오버레이를 레이더의 실시간 보기에 추가할 수 있습니다. 이 기능은 설치 중이거나 장치의 틸트 각도를 알아야 할 때마다 유용합니다.

비고

장치가 수평인 경우 틸트 각도 오버레이에 "90"이 표시됩니다. 오버레이에 "75"가 표시되면 레이더의 틸트 각도가 수평선보다 15° 아래에 있습니다.

1. **Radar > Overlays(레이더 > 오버레이)**로 이동합니다.
2. **Text(텍스트)**를 선택하고  을 클릭합니다.
3. **#op**를 입력합니다.
또한 **Modifier(수정자)**를 클릭하고 목록에서 **#op**를 선택합니다.
4. 위치를 선택합니다. 실시간 보기에서 오버레이 필드를 드래그하여 위치를 변경할 수도 있습니다.

비디오 보기 및 녹화

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

대역폭 및 저장 공간 감소

중요 사항

대역폭을 줄이면 이미지의 세부 정보가 손실될 수 있습니다.

1. **Radar > Stream(레이더 > 스트림)**으로 이동합니다.
2. 실시간 보기에서  을 클릭합니다.
3. **Video format H.264(비디오 형식 H.264)**를 선택합니다.
4. **Radar > Stream > General(레이더 > 스트림 > 일반)**로 이동하고 **Compression(압축)**을 높입니다.

비고

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

네트워크 스토리지 설정

네트워크에 녹화를 저장하려면 사용자의 네트워크 스토리지를 설정해야 합니다.

1. **System(시스템) > Storage(스토리지)**로 이동합니다.
2. **Network storage(네트워크 스토리지)**에서  **Add network storage(네트워크 스토리지 추가)**를 클릭합니다.
3. 호스트 서버의 IP 주소를 입력합니다.
4. **Network Share(네트워크 공유)** 아래에서 호스트 서버에 공유 위치의 이름을 입력합니다.
5. 사용자 이름과 패스워드를 입력합니다.
6. SMB 버전을 선택하거나 **Auto(자동)**에 그대로 둡니다.

7. 일시적인 연결 문제가 발생하거나 공유가 아직 구성되지 않은 경우 **Add share even if connection fails(테스트 없이 공유 추가)**를 선택합니다.
8. 추가를 클릭합니다.

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

자세히 알아보려면 *이벤트 룰 시작하기* 가이드를 확인하십시오.

액션 트리거

1. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다. 룰은 장치가 특정 액션을 수행하는 시간을 정의합니다. 룰을 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 충족되었을 때 장치가 수행해야 하는 **Action(액션)**을 선택합니다.

비고

활성 룰을 변경하는 경우 변경 사항을 적용하려면 룰을 다시 켜야 합니다.

비고

룰에서 사용된 스트림 프로파일의 정의를 변경하려면 스트림 프로파일을 사용하는 모든 룰을 재 시작해야 합니다.

모션이 감지되면 카메라에서 비디오를 녹화

이 예에서는 레이더가 모션을 감지하고 1분 후에 정지하기 전에 카메라가 SD 카드에 녹화를 시작하도록 레이더와 카메라를 설정하는 방법을 설명합니다.

다음과 같이 장치를 연결합니다.

1. 레이더의 I/O 출력에서 카메라의 I/O 입력으로 케이블을 연결합니다.

레이더의 I/O 포트를 구성합니다.

2. **Settings > Accessories > I/O ports(설정 > 액세서리 > I/O 포트)**로 이동하고 I/O 포트를 출력으로 구성하고 정상 상태를 선택합니다.

레이더에서 다음과 같이 룰을 생성합니다.

3. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
4. 룰에 대한 이름을 입력합니다.
5. 조건 목록의 **Radar motion(레이더 모션)** 아래에서 시나리오를 선택합니다. 시나리오를 설정하려면 항목을 참고하십시오.

6. 액션 목록에서 **Toggle I/O while the rule is active**(룰이 활성화 상태인 동안 I/O 토글)를 선택하고 카메라에 연결된 포트를 선택합니다.
7. **Save(저장)**를 클릭합니다.

카메라의 I/O 포트를 구성합니다.

8. **System > Accessories > I/O ports**(시스템 > 액세서리 > I/O 포트)로 이동하고 I/O 포트를 입력으로 구성하고 정상 상태를 선택합니다.

카메라에서 룰을 생성합니다.

9. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
10. 룰에 대한 이름을 입력합니다.
11. 조건 목록에서 **Digital input is active**(디지털 입력이 활성화)를 선택한 다음 룰을 트리거할 포트를 선택합니다.
12. 액션 목록에서 **Record video**(비디오 녹화)를 선택합니다.
13. 스토리지 옵션 목록에서 **SD card**(SD 카드)를 선택합니다.
14. 기존 스트림 프로파일을 선택하거나 새로 생성합니다.
15. 사전 버퍼를 5초로 설정합니다.
16. 사후 버퍼 시간을 1분으로 설정합니다.
17. **Save(저장)**를 클릭합니다.

차량이 잘못된 방향으로 주행할 때 카메라의 영상을 녹화

이 예에서는 레이더가 잘못된 방향으로 운전하는 차량을 감지할 때 카메라가 SD 카드에 녹화를 시작하도록 레이더와 카메라를 설정하는 방법을 설명합니다.

시작하기 전

- 선 넘기 및 두 개의 라인을 넘는 차량에서 트리거되는 레이더의 웹 인터페이스에서 시나리오를 만듭니다.
자세한 내용은 를 참조하십시오.
- 잘못된 방향으로 주행하는 차량을 감지하려는 차선 위에 두 개의 선을 배치하십시오. 항공 사진과 같은 참조 지도를 사용하면 객체가 움직이는 위치를 더 쉽게 확인할 수 있습니다.
자세한 내용은 를 참조하십시오.

1. 레이더에 두 명의 수신자를 생성합니다.
 - 1.1. 레이더의 장치 인터페이스에서 **System > Events > Recipients**(시스템 > 이벤트 > 수신자)로 이동하고 첫 번째 수신자를 추가합니다.
 - 1.2. 다음 정보를 추가합니다.
 - **Name(이름)**: 가상 포트 활성화
 - **Type(유형)**: HTTP
 - **URL**: http://<IPAddress>/axis-cgi/virtualinput/activate.cgi
<IPAddress>를 녹화를 시작하려는 카메라의 주소로 바꿉니다.
 - 카메라의 사용자 이름과 비밀번호입니다.
 - 1.1. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
 - 1.2. **Save(저장)**를 클릭합니다.
 - 1.3. 다음 정보를 사용하여 두 번째 수신자를 추가합니다.
 - **Name(이름)**: 가상 포트 비활성화
 - **Type(유형)**: HTTP
 - **URL**: http://<IPAddress>/axis-cgi/virtualinput/deactivate.cgi
<IPAddress>를 카메라의 주소로 바꿉니다.
 - 카메라의 사용자 이름과 비밀번호입니다.

- 1.1. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
- 1.2. **Save(저장)**를 클릭합니다.
2. 레이더에 두 룰을 생성합니다.
 - 2.1. 레이더의 장치 인터페이스에서 **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 첫 번째 룰을 추가합니다.
 - 2.2. 다음 정보를 추가합니다.
 - **Name(이름):** 가상 IO1 활성화
 - **Condition(조건):** Radar motion(레이더 모션) 아래에서 생성된 시나리오를 선택합니다.
 - **Action(액션):** Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)
 - **Recipient(수신자):** 가상 포트 활성화
 - **Query string suffix(쿼리 문자열 접미사):** schemaversion=1&port=1
 - 2.1. **Save(저장)**를 클릭합니다.
 - 2.2. 다음 정보가 포함된 다른 룰을 추가합니다.
 - **Name(이름):** 가상 IO1 비활성화
 - **Condition(조건):** Radar motion(레이더 모션) 아래에서 생성된 시나리오를 선택합니다.
 - **Invert this condition(이 조건을 반전하기)**을 선택합니다.
 - **Action(액션):** Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)
 - **Recipient(수신자):** 가상 포트 비활성화
 - **Query string suffix(쿼리 문자열 접미사):** schemaversion=1&port=1
 - 2.1. **Save(저장)**를 클릭합니다.
3. 카메라에서 룰을 생성합니다.
 - 3.1. 카메라의 장치 인터페이스에서 **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 룰을 추가합니다.
 - 3.2. 다음 정보를 추가합니다.
 - **Name(이름):** 가상 입력 1에서 트리거
 - **Condition(조건):** I/O > Virtual input is active(가상 입력이 활성화됨)
 - **Port(포트):** 1
 - **Action(액션):** Recordings > Record video while the rule is active(녹화 > 룰이 활성 상태인 동안 비디오 녹화)
 - **Storage options(스토리지 옵션):** SD_DISK
 - **Camera(카메라)**와 **Stream profile(스트림 프로파일)**을 선택합니다.
 - 3.1. **Save(저장)**를 클릭합니다.

레이더의 빨간색 신호등을 활성화

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

이 예에서는 빨간색 신호등을 활성화하는 방법과 평일 근무 시간 이후에만 일정을 설정하는 방법을 설명합니다.

일정 생성:

1. **System > Events > Schedules(시스템 > 이벤트 > 일정)**로 이동한 후 새 일정을 추가합니다.
2. 일정의 이름을 입력합니다.

3. **Type(유형)** 아래에서 **Schedule(일정)**을 선택합니다.
4. **Recurrent(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(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록의 **Scheduled and recurring(예약 및 반복)**에서 **Schedule(일정)**을 선택합니다.
4. **Schedule(일정)** 드롭다운에서 생성한 일정을 선택합니다.
5. **Radar(레이더)**의 액션 목록에서 **Dynamic LED strip(동적 LED 스트립)**을 선택합니다.
6. **Pattern(패턴)** 드롭다운에서 **Sweeping red(스위핑 레드)** 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.

비고

레이더 탬퍼링 이벤트에 대한 룰을 생성하는 옵션은 AXIS OS 11.11에서 사용할 수 있습니다.

이메일 수신자 추가:

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

룰 생성:

8. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
9. 룰에 대한 이름을 입력합니다.
10. 조건 목록의 **Device status(장치 상태)**에서 **Radar data failure(레이더 데이터 오류)**를 선택합니다.
11. **Reason(이유)**에서 **Tampering(탐퍼링)**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.

모션 디텍션 시 조명을 켜기

침입자가 감지 영역에 진입할 때 조명을 켜면 억제 효과가 있으며 침입을 녹화하는 영상 카메라의 이미 품질이 향상됩니다.

이 예는 레이더가 모션을 감지하고 1분 후에 꺼질 때 조명기가 켜지도록 레이더와 조명기를 설정하는 방법을 설명합니다.

다음과 같이 장치를 연결합니다.

1. 레이더의 릴레이 포트를 통해 조명기 케이블 중 하나를 전원 공급 장치에 연결합니다. 다른 케이블을 전원 공급 장치와 조명기 사이에 직접 연결합니다.

레이더의 릴레이 포트를 구성합니다.

2. **System > Accessories > I/O ports(시스템 > 액세서리 > I/O 포트)**로 이동하고 릴레이 포트의 정상 상태로 **Open circuit(개방 회로)**를 선택합니다.

레이더에서 다음과 같이 룰을 생성합니다.

3. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
4. 룰에 대한 이름을 입력합니다.
5. 조건 목록의 **Radar motion(레이더 모션)** 아래에서 시나리오를 선택합니다. 시나리오를 설정하려면 항목을 참고하십시오.
6. 액션 목록에서, **Toggle I/O once(I/O를 한 번 토글)**를 선택한 다음 릴레이 포트를 선택합니다.
7. **Active(활성)**를 선택합니다.
8. **Duration(기간)**을 설정합니다.
9. **Save(저장)**를 클릭합니다.

레이더로 PTZ 카메라를 제어

레이더에서 객체의 위치 정보를 사용하여 PTZ 카메라가 객체를 추적하도록 할 수 있습니다. 이 작업을 수행하는 방법은 두 가지입니다.

- 하나의 PTZ 카메라와 하나의 레이더가 매우 가깝게 마운트된 경우 내장 옵션이 적합합니다.
- Windows 애플리케이션은 물체 추적을 위해 여러 대의 PTZ 카메라와 레이더를 사용하려는 경우에 적합합니다.

비고

카메라, 레이더, Windows 컴퓨터의 시간을 동기화하려면 NTP 서버를 사용하십시오. 시계가 동기화되지 않으면 추적이나 고스트 추적이 지연될 수도 있습니다.

내장된 레이더 오토트래킹 서비스로 PTZ 카메라 제어

내장된 레이더 오토트래킹 기능은 레이더가 PTZ 카메라를 직접 제어하는 에지 투 에지 솔루션을 생성합니다. 모든 Axis PTZ 카메라를 지원합니다.

비고

내장된 레이더 오토트래킹 서비스를 사용하여 하나의 레이더와 하나의 PTZ 카메라를 연결할 수 있습니다. 둘 이상의 레이더 또는 PTZ 카메라를 사용하려는 설정의 경우 AXIS Radar Autotracking for PTZ를 사용하십시오. 자세한 내용은 을 참조하십시오.

이 지침에서는 PTZ 카메라와 레이더를 페어링하는 방법, 장치를 교정하는 방법, 객체 추적을 설정하는 방법에 대해 설명합니다.

시작하기 전:

- 관심 영역을 정의하고 레이더에서 제외 영역을 설정하여 불필요한 알람을 방지하십시오. PTZ 카메라가 관련 없는 객체를 추적하지 않도록 하기 위해, 레이더 반사 재료나 흔들리는 객체(예: 나뭇잎)와 같은 영역을 제외하도록 설정하십시오. 자세한 내용은 항목을 참조하십시오.

레이더를 PTZ 카메라와 페어링합니다.

1. **System > Edge-to-edge > PTZ pairing(시스템 > 엣지 투 엣지 > PTZ 페어링)**으로 이동합니다.
2. PTZ 카메라의 IP 주소, 사용자 이름 및 패스워드를 입력합니다.
3. **Connect(연결)**를 클릭합니다.
4. **Configure Radar autotracking(레이더 오토트래킹 구성)**을 클릭하거나 **Radar > Radar PTZ autotracking(레이더 > 레이더 PTZ 오토트래킹)**으로 이동하여 레이더 오토트래킹을 설정합니다.

레이더와 PTZ 카메라를 보정합니다.

5. **Radar > Radar PTZ autotracking(레이더 > 레이더 PTZ 오토트래킹)**으로 이동합니다.
6. 카메라 장착 높이를 설정하려면 **Camera mounting height(카메라 장착 높이)**로 이동합니다.
7. 레이더와 동일한 방향을 가리키도록 PTZ 카메라를 팬하려면 **Pan alignment(팬 정렬)**로 이동합니다.
8. 경사진 지면을 보정하기 위해 틸트를 조정해야 하는 경우 **Ground incline offset(지면 경사 오프셋)**으로 이동하여 각도 단위로 오프셋을 추가합니다.

PTZ 추적 설정:

9. 사람, 차량 및/또는 알 수 없는 물체를 추적하려면 **Track(추적)**을 선택합니다.
10. PTZ 카메라로 객체 추적을 시작하려면 **Tracking(추적)**을 켭니다.
추적은 객체 또는 객체 그룹을 카메라의 보기에 유지하도록 자동으로 확대합니다.
11. 카메라 보기에 맞지 않는 여러 객체가 예상되는 경우 **Object switching(객체 전환)**을 켭니다.
이 설정을 사용하면 레이더는 추적할 객체에 우선 순위를 부여합니다.
12. 각 객체를 몇 초 동안 추적할지 결정하려면 **Object hold time(객체 유지 시간)**을 설정합니다.
13. 레이더가 더 이상 객체를 추적하지 않는 경우 PTZ 카메라를 홈 포지션으로 되돌리기 위해 **Return to home(홈으로 돌아가기)**을 켭니다.
14. PTZ 카메라가 홈으로 돌아가기 전에 마지막으로 알려진 추적된 객체 위치에 얼마나 오랫동안 머물러야 하는지 결정하려면 **Return to home timeout(홈으로 돌아가기 시간 초과)**를 설정합니다.
15. PTZ 카메라의 확대/축소를 미세 조정하려면 슬라이더에서 확대/축소를 조정합니다.

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-products를 참조하십시오.

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

레이더 데이터를 전송하기 위해 MQTT 사용

감지된 객체에 대한 레이더 데이터를 수집하고 MQTT를 통해 전송하도록 모니터링하려면 AXIS Speed Monitor 애플리케이션과 함께 레이더를 사용합니다.

이 예에서는 설치된 AXIS Speed Monitor 장치에서 MQTT 클라이언트를 설정하는 방법 및 MQTT 브로커에 대한 페이로드로 AXIS Speed Monitor에서 수집된 레이더 데이터를 게시하는 조건을 만드는 방법을 설명합니다.

시작하기 전:

- 레이더의 AXIS Speed Monitor를 설치하거나 레이더에 연결하는 카메라에 설치합니다. 자세한 내용은 *AXIS Speed Monitor 사용자 설명서*를 참고하십시오.
- MQTT 브로커를 설정하고 브로커의 IP 주소, 사용자 이름 및 패스워드를 가져옵니다. *AXIS OS 기술 자료*에서 MQTT 및 MQTT 브로커에 대해 자세히 알아보십시오.

설치한 AXIS Speed Monitor 장치의 웹 인터페이스에서 MQTT 클라이언트를 설정하십시오.

1. **System > MQTT > MQTT client > Broker(시스템 > MQTT > MQTT 클라이언트 > 브로커)**로 이동하고 다음 정보를 입력합니다.
 - **Host(호스트):** 브로커 IP 주소
 - **Client ID(클라이언트 ID):** 장치의 ID
 - **Protocol(프로토콜):** 브로커가 설정된 프로토콜
 - **Port(포트):** 브로커가 사용하는 포트 번호
 - 브로커 **Username(사용자 이름)**과 **Password(패스워드)**
2. **Save(저장)** 및 **Connect(연결)**을 클릭합니다.

레이더 데이터를 MQTT 브로커에 페이로드로 게시하는 조건을 생성하십시오.

3. **System > MQTT > MQTT publication(시스템 > MQTT > MQTT 게시)**으로 이동하고 **+ Add condition(+ 조건 추가)**를 클릭합니다.
4. 조건 목록의 **Application(애플리케이션)**에서 **Speed Monitor: Track exited zone(속도 모니터: 트랙 이탈 영역)**을 선택합니다.

이제 장치는 시나리오에서 나가는 모든 움직이는 객체에 대한 레이더 추적에 대한 정보를 보낼 수 있습니다. 모든 객체에는 자체 레이더 트랙 매개변수(예: **rmd_zone_name**, **tracking_id**, **trigger_count**)가 있습니다. 전체 매개변수 목록은 *AXIS Speed Monitor 사용 설명서*에서 확인할 수 있습니다.

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 라이선스에 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 를 참조하십시오.



녹화물이 저장되는 저장 공간을 표시합니다.

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.

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 켵니다.
 - **Ignore small objects(작은 객체 무시):** 고양이나 토끼와 같은 작은 객체의 허위 알람을 최소화하려면 켵니다.
 - **Ignore swaying objects(흔들리는 객체 무시):** 나무, 덩굴 또는 깃대와 같이 흔들리는 객체로 인한 허위 알람을 최소화하려면 켵니다.
- **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 켵니다.
 - **Ignore swaying objects(흔들리는 객체 무시):** 나무, 덩굴 또는 깃대와 같이 흔들리는 객체로 인한 허위 알람을 최소화하려면 켵니다.

보기

Information legend(정보 범례): 레이더가 감지하고 추적할 수 있는 객체 유형이 포함된 범례를 표시하려면 켵니다. 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

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

Frame rate(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.
 - **Storage(스토리지):** 스트림에 사용할 수 있는 예상 스토리지를 표시합니다.
 - **Maximum bitrate(최대 비트 레이트):** 비트 레이트 제한을 설정하려면 컵니다.
 - **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(가변):** 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 영역

exclude zone(제외 영역)은 움직이는 객체가 무시되는 영역입니다. 시나리오 내에 원하지 않는 알람을 많이 트리거하는 영역이 있는 경우 제외 영역을 사용합니다.



: 새로운 제외 영역을 생성하려면 클릭합니다.

제외 영역을 수정하려면 목록에서 해당 항목을 선택합니다.

Track passing objects(지나가는 객체 추적): 제외 구역을 통과하는 객체를 추적하려면 켵니다. 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 켜집니다.

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 %F를 추가하려면 클릭합니다.
 -  : hh:mm:ss(24시간 시계)를 표시하기 위해 시간 수정자 %x를 추가하려면 클릭합니다.
 - **Modifiers(수정자)**: 텍스트 상자에 추가하기 위해 목록에 나타난 수정자를 선택하려면 클릭합니다. 예를 들어, %a는 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 FFFFFFFF, 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 %F를 추가하려면 클릭합니다.
 -  : hh:mm:ss(24시간 시계)를 표시하기 위해 시간 수정자 %x를 추가하려면 클릭합니다.
 - **Modifiers(수정자)**: 텍스트 상자에 추가하기 위해 목록에 나타난 수정자를 선택하려면 클릭합니다. 예를 들어, %a는 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 장면이 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 끄십시오. 모든 활성 채널에 표시되도록 하려면 켜십시오.
 - **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 켜십시오.
 - **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 끄십시오. 모든 활성 채널에 표시되도록 하려면 켜십시오.
- **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 켜십시오.
- **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 항목을 참조하십시오.

레이더 PTZ 오토트래킹

레이더 오토트래킹을 사용하려면 레이더를 PTZ 카메라와 페어링합니다. 연결을 설정하려면 **System > Edge-to-edge(시스템 > 에지 투 에지)**로 이동합니다.

초기 설정 구성:

Camera mounting height(카메라 장착 높이): 지면에서 PTZ 카메라를 장착한 높이까지의 거리입니다.

팬 정렬: 레이더와 같은 방향을 가리키도록 PTZ 카메라를 팬합니다. PTZ 카메라의 IP 주소를 클릭하여 액세스합니다.

팬 오프셋 저장: 팬 정렬을 저장하려면 클릭합니다.

지면 경사 오프셋: 지면 경사 오프셋을 사용하여 카메라의 틸트를 미세 조정합니다. 지면이 경사진 경우 또는 카메라를 수평으로 마운트하지 않은 경우 객체를 추적할 때 카메라가 너무 높거나 낮게 조준될 수 있습니다.

Done(완료): 설정을 저장하고 구성을 계속하려면 클릭합니다.

PTZ 오토트래킹 구성:

트랙: 사람, 차량 및/또는 알 수 없는 객체를 추적하려면 선택합니다.

Tracking(추적): PTZ 카메라로 객체 추적을 시작하려면 켭니다. 추적은 객체 또는 객체 그룹을 카메라의 보기에 유지하도록 자동으로 확대합니다.

Object switching(객체 전환): 레이더가 PTZ 카메라의 보기에 맞지 않는 여러 객체를 감지할 경우, PTZ 카메라는 레이더가 우선 순위를 가장 높게 부여한 객체를 추적하고 다른 객체는 무시합니다.

Object hold time(객체 유지 시간): PTZ 카메라가 각 객체를 추적해야 하는 시간(초)을 결정합니다.

Return to home(홈으로 돌아가기): 레이더가 더 이상 객체를 추적하지 않는 경우 이를 켜서 PTZ 카메라를 홈 포지션으로 되돌립니다.

Return to home timeout(홈으로 돌아가기 시간 초과): PTZ 카메라가 홈으로 돌아가기 전에 추적한 객체의 마지막 알려진 포지션에 머물러야 할 시간을 결정합니다.

Zoom(줌): 슬라이더를 사용하여 PTZ 카메라의 줌을 미세 조정합니다.

Reconfigure installation(설치 재구성): 모든 설정을 지우고 초기 구성으로 돌아가려면 클릭합니다.

녹화물

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.

Storage(스토리지): 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.

Open(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 라이선스):** 앱에서 사용되는 오픈 소스 라이선스에 대한 정보를 봅니다.
- **App log(앱 로그):** 앱 이벤트의 로그를 봅니다. 로그는 지원 서비스에 문의할 때 유용합니다.
- **Activate license with a key(키로 라이선스 활성화):** 앱에 라이선스가 필요한 경우 활성화해야 합니다. 장치가 인터넷에 연결할 수 없는 경우 이 옵션을 사용합니다. 라이선스 키가 없다면 axis.com/products/analytics로 이동합니다. 라이선스 키를 생성하려면 라이선스 코드와 Axis 제품 일련 번호가 필요합니다.
- **Activate license automatically(라이선스를 자동으로 활성화):** 앱에 라이선스가 필요한 경우 활성화해야 합니다. 장치가 인터넷에 연결할 수 있는 경우 이 옵션을 사용합니다. 라이선스를 활성화하려면 라이선스 코드가 필요합니다.
- **Deactivate the license(라이선스 비활성화):** 예를 들어 체험판 라이선스에서 정식 라이선스로 변경하는 경우, 라이선스를 비활성화하여 다른 라이선스로 교체합니다. 라이선스를 비활성화하면 장치에서도 제거됩니다.
- **Settings(설정):** 매개변수를 구성합니다.
- **Delete(삭제):** 장치에서 앱을 영구적으로 삭제하십시오. 먼저 라이선스를 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 (manual NTS KE servers)(자동 날짜 및 시간(수동 NTS KE 서버)):** DHCP 서버에 연결된 보안 NTP 키 설정 서버와 동기화합니다.
 - **Manual NTS KE servers(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.
 - **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.
 - **Manual NTP servers(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.

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

- **DHCP:** DHCP 서버의 시간대를 채택합니다. 이 옵션을 선택하려면 먼저 장치가 DHCP 서버에 연결되어 있어야 합니다.
- **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.

- **Format(포맷):** 장치의 위도와 경도를 입력할 때 사용할 형식을 선택합니다.
- **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): 네트워크 라우터가 장치에 IP 주소를 자동으로 할당 하도록 하려면 선택합니다. 대부분의 네트워크에 대해 자동 IP(DHCP)를 권장합니다.

IP address(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.

Subnet mask(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

Assign hostname automatically(호스트 이름을 자동으로 할당): 네트워크 라우터가 장치에 호스트 이름을 IP 주소를 자동으로 할당하도록 하려면 선택합니다.

Hostname(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.

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(시스템) > Security(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 name(Bonjour 이름): 네트워크에 표시할 이름을 입력합니다. 기본 이름은 장치 이름과 MAC 주소입니다.

UPnP®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

WS-Discovery(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.

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-services를 참조하십시오.

Allow O3C(O3C 허용):

- **One-click(원클릭):** 기본 옵션입니다. O3C에 연결하려면 장치의 제어 버튼을 누릅니다. 장치 모델에 따라 상태 LED가 깜박일 때까지 버튼을 누른 후 놓거나, 길게 누릅니다. **Always(항상)**를 활성화하고 연결 상태를 유지하려면 24시간 이내에 장치를 O3C 서비스에 등록합니다. 등록하지 않으면 장치의 O3C 연결이 끊어집니다.
- **Always(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.

Host(호스트): 프록시 서버의 주소를 입력합니다.

Port(포트): 액세스에 사용되는 포트 번호를 입력하십시오.

Login(로그인) 및 Password(패스워드): 필요한 경우 프록시 서버에 대한 사용자 이름 및 패스워드를 입력합니다.

Authentication method(인증 방법):

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

Owner authentication key (OAK)(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 and v2c(v1 및 v2c):**
 - **Read community(읽기 커뮤니티):** 지원되는 모든 SNMP 객체에 대해 읽기 전용 권한이 있는 커뮤니티 이름을 입력합니다. 기본값은 **public(공개)**입니다.
 - **Write community(쓰기 커뮤니티):** 지원되는 모든 SNMP 객체에 대해 읽기 또는 쓰기 권한이 있는 커뮤니티 이름을 입력합니다(읽기 전용 객체 제외). 기본값은 **write(쓰기)**입니다.
 - **Activate traps(트랩 활성화):** 트랩보고를 활성화하려면 커십시오. 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.
 - **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 전 까지 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-support를 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+)**: 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 기기 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.

- **Password(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.

Blocking period(차단 기간): 무차별 대입 공격을 차단할 시간(초)을 입력합니다.

Blocking conditions(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 켵니다.

Default Policy(기본 정책): 방화벽에서 룰이 적용되지 않는 연결 요청을 처리하는 방법을 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.
 - **Policy(정책):** 방화벽 룰에 대해 **Accept(수락)** 또는 **Drop(거부)**를 선택합니다.
 - **IP range(IP 범위):** 허용 또는 차단할 주소 범위를 지정하려면 선택합니다. **Start(시작)** 및 **End(끝)**에 IPv4/IPv6를 사용합니다.
 - **IP address(IP 주소):** 허용하거나 차단할 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
 - **Protocol(프로토콜):** 허용 또는 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우 포트도 지정해야 합니다.
 - **MAC:** 허용 또는 차단할 장치의 MAC 주소를 입력합니다.
 - **Port range(포트 범위):** 허용 또는 차단할 포트 범위를 지정하려면 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
 - **Port(포트):** 허용 또는 차단할 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
 - **Traffic type(트래픽 유형):** 허용하거나 차단할 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 허용하되 과도한 트래픽을 줄이기 위해 제한을 적용하려면 선택합니다.
 - **IP range(IP 범위):** 허용 또는 차단할 주소 범위를 지정하려면 선택합니다. **Start(시작)** 및 **End(끝)**에 IPv4/IPv6를 사용합니다.
 - **IP address(IP 주소):** 허용하거나 차단할 주소를 입력합니다. IPv4/IPv6 또는 CIDR 형식을 사용합니다.
 - **Protocol(프로토콜):** 허용 또는 차단할 네트워크 프로토콜(TCP, UDP 또는 둘 다)을 선택합니다. 프로토콜을 선택하는 경우 포트도 지정해야 합니다.
 - **MAC:** 허용 또는 차단할 장치의 MAC 주소를 입력합니다.
 - **Port range(포트 범위):** 허용 또는 차단할 포트 범위를 지정하려면 선택합니다. **Start(시작)** 및 **End(끝)**에 추가합니다.
 - **Port(포트):** 허용 또는 차단할 포트 번호를 입력합니다. 포트 번호는 1에서 65535 사이여야 합니다.
 - **Unit(유닛):** 허용하거나 차단할 연결 유형을 선택합니다.
 - **Period(기간):** **Amount(양)**와 관련된 기간을 선택합니다.
 - **Amount(양):** 설정된 **Period(기간)** 내에서 장치의 최대 연결 허용 횟수를 설정합니다. 최대 양은 65535입니다.

- **Burst(버스트):** 설정된 **Period(기간)** 동안 설정된 **Amount(양)**를 한 번 초과할 수 있는 연결 횟수를 입력합니다. 해당 횟수에 도달하면 설정한 기간 동안 설정한 양만 허용됩니다.
- **Traffic type(트래픽 유형):** 허용하거나 차단할 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):** 룰 테스트를 완료하기 전에, 방화벽을 이전 상태로 롤백하려면 클릭합니다.
- **Apply rules(룰 적용):** 테스트하지 않고 룰을 활성화하려면 클릭합니다. 이 방법은 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 길이어야 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 켜십시오.

SSH 계정

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

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

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 패스워드): 계정의 패스워드를 입력합니다. 패스워드는 1~64자 길이어야 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. **기본, 다이제스트, 오픈 ID** 중에서 선택합니다.



상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Update(업데이트):** 가상 호스트를 업데이트합니다.
- **Delete(삭제):** 가상 호스트를 삭제합니다.

비활성화: 서버가 비활성화되었습니다.

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](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 클릭합니다.

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.

Name(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 룰 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 룰 시작하기*에서 특정 액션에 대한 정보를 알아보십시오.

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.

Name(이름): 수신자의 이름을 입력합니다.

Type(유형): 목록에서 선택:

- **FTP** 
 - **Host(호스트):** 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System(시스템) > Network(네트워크) > IPv4 and IPv6(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.
 - **Password(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.
 - **Password(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.
 - **Password(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.

 - **Host(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.

- **Password(패스워드):** 로그인하려면 패스워드를 입력하십시오.
- **SFTP** 
 - **Host(호스트):** 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System(시스템) > Network(네트워크) > IPv4 and IPv6(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.
 - **Password(패스워드):** 로그인하려면 패스워드를 입력하십시오.
 - **SSH host public key type (MD5)(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 host public key type (SHA256)(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.
 - **Password(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 커십시오(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

- **Host(호스트):** 서버의 IP 주소나 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우, DNS 서버가 **System(시스템) > Network(네트워크) > IPv4 and IPv6(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.

기기를 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 베이스에서 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

Host(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.

Password(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 제한을 기다릴 필요 없이 서버를 더 이상 사용할 수 없는 시점을 감지할 수 있습니다.

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

장치 항목 접두사: MQTT client(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 고집시오.

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 topic name(주제 이름 포함): MQTT 주제에서 조건을 설명하는 주제를 포함하려면 선택합니다.

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

Include serial number(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

Ignore(무시): 네트워크 스토리지를 무시하려면 켵니다.

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 로그인에 필요한 경우, 사용자 이름을 입력합니다. 특정 도메인 서버에 로그인하려면 DOMAIN\username을 입력합니다.
- **Password(패스워드):** 서버에 로그인에 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 여기에서 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.

Remove network storage(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 켵니다. 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.

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.

Name(이름): 프로파일의 이름을 추가합니다.

Description(설명): 프로파일에 대한 설명을 추가합니다.

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

Resolution(해상도): 이 설정에 대한 설명은 항목을 참고하십시오.

Frame rate(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 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.com의 Axis 개발자 커뮤니티를 참조하십시오.



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

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 비밀번호): 계정의 비밀번호를 입력합니다. 비밀번호는 1~64자 길이어야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 비밀번호에 사용할 수 있습니다.

Repeat password(비밀번호 반복): 동일한 비밀번호를 다시 입력하십시오.

Role(역할):

- **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.

액세서리

I/O 포트

디지털 입력을 사용하여 개방 및 폐쇄 회로 사이를 전환할 수 있는 외부 장치(예: PIR 센서, 도어 또는 창 접점, 유리 파손 감지기)를 연결하십시오.

디지털 출력을 사용하여 릴레이 및 LED 등의 외부 장치와 연결합니다. VAPIX® 애플리케이션 프로그램 래밍 인터페이스 또는 웹 인터페이스를 통해 연결된 장치를 활성화할 수 있습니다.

포트

Name(이름): 포트 이름을 바꾸려면 텍스트를 편집합니다.

Direction(방향):  은 포트가 입력 포트임을 나타냅니다.  은 포트가 출력 포트임을 나타냅니다. 포트를 구성할 수 있는 경우 아이콘을 클릭하여 입력과 출력 간에 변경할 수 있습니다.

Normal state(정상 상태): 개회로의 경우  을 클릭하고 폐회로의 경우  을 클릭합니다.

Current state(현재 상태): 포트의 현재 상태를 표시합니다. 현재 상태가 정상 상태와 같지 않을 때 입력 또는 출력이 활성화됩니다. 장치의 입력은 연결이 끊어지거나 1V VDC 이상의 전압이 있을 때 개방 회로가 됩니다.

비고

재시작하는 동안 출력 회로가 개방됩니다. 재시작이 완료되면 회로가 정상 위치로 돌아갑니다. 이 페이지에서 설정을 변경하면 출력 회로는 활성 트리거에 관계없이 원래 위치로 돌아갑니다.

Supervised(관리형)  : 누군가가 디지털 I/O 장치에 대한 연결을 변경하는 경우 작업을 감지하고 트리거할 수 있도록 하려면 켜십시오. 입력이 열렸는지 닫혔는지 감지하는 것 외에도 누군가가 입력을 변조했는지(즉, 잘리거나 단락되었는지) 감지할 수 있습니다. 연결을 감시하려면 외부 I/O 루프에 추가 하드웨어(EOL 레지스터)가 필요합니다.

에지 투 에지

페어링

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

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.



추가: 페어링할 장치를 추가합니다.

Discover devices(장치 찾기): 네트워크에서 장치를 찾으려면 클릭합니다. 네트워크가 스캔되면 이용할 수 있는 장치 목록이 표시됩니다.

비고

목록에는 페어링할 수 있는 장치뿐만 아니라 검색된 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. 아이콘 위로 마우스를 가져가면 이미 활성화된 페어링에 대한 정보를 확인할 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.

Password(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.



추가: 페어링할 장치를 추가합니다.

Discover devices(장치 찾기): 네트워크에서 장치를 찾으려면 클릭합니다. 네트워크가 스캔되면 이용할 수 있는 장치 목록이 표시됩니다.

비고

목록에는 페어링할 수 있는 장치뿐만 아니라 검색된 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. 아이콘 위로 마우스를 가져가면 이미 활성화된 페어링에 대한 정보를 확인할 수 있습니다.



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.

Password(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.

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.

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.

Host(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): 전송할 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.com에서 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/support로 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.
- **Autorollback(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.

설치 확인

레이더 설치 확인

비고

이 테스트는 현재 조건에서 설치를 확인하도록 도움이 됩니다. 설치의 일상적인 실적은 장면의 변화에 의해 영향을 받을 수 있습니다.

레이더는 설치되는 즉시 사용할 준비가 되지만 사용을 시작하기 전에 확인을 수행하는 것이 좋습니다. 이렇게 하면 설치 문제를 식별하거나 장면에 있는 객체(예: 나무 및 반사 표면)를 관리하는 데 도움을 주어 레이더의 정확도를 높일 수 있습니다.

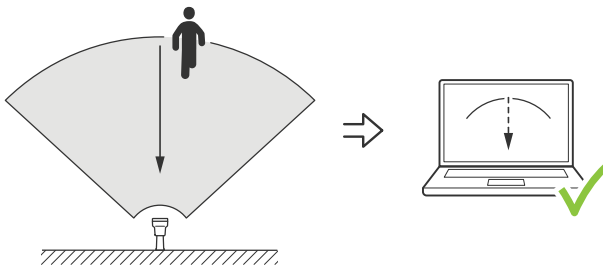
먼저 검증을 시도하기 전에 하십시오. 다음 단계를 수행합니다.

잘못된 감지가 없는지 확인

1. 감지 영역에 사람의 활동이 없는지 확인하십시오.
2. 레이더가 감지 영역에서 정적 객체를 감지하지 않도록 몇 분 동안 기다립니다.
3. 원치 않는 감지가 없으면 4단계를 건너뛸 수 있습니다.
4. 원치 않는 감지가 있는 경우에서 특정 유형의 모션이나 객체를 필터링하거나 범위를 변경하거나 디텍션 감도를 조정하는 방법을 알아봅니다.

레이더가 전방에서 접근할 때 올바른 기호와 이동 방향을 확인합니다.

1. 레이더의 웹 인터페이스로 이동하여 세션을 기록하도록 선택합니다. 이 작업에 도움이 필요하면 항목을 참조하십시오.
2. 레이더 앞에서 최대 60m(196ft)를 시작하여 레이더를 향해 직접 걸어갑니다.
3. 레이더의 웹 인터페이스에서 세션을 확인합니다. 감지되면 사람 분류 기호가 나타나야 합니다.
4. 레이더의 웹 인터페이스가 올바른 이동 방향을 표시하는지 확인합니다.



레이더가 옆면에서 접근할 때 올바른 기호와 이동 방향을 확인합니다.

1. 레이더의 웹 인터페이스로 이동하여 세션을 기록하도록 선택합니다. 이 작업에 도움이 필요하면 항목을 참조하십시오.
2. 레이더 촬영 영역에서 30m(98ft) 떨어진 곳에서 시작하여 레이더를 가로질러 똑바로 걸어갑니다.
3. 레이더의 웹 인터페이스에 사람 분류 기호가 표시되는지 확인합니다.
4. 레이더의 웹 인터페이스가 올바른 이동 방향을 표시하는지 확인합니다.

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

테스트	통과/실패	의견
1. 영역이 깨끗할 때 원치 않는 감지가 없는지 확인합니다.		
2a. 전방에서 레이더 접근 시 '인간' 기호로 객체가 감지되었는지 확인		

2b. 전방에서 레이더에 접근할 때 진행 방향이 올바른지 확인		
3a. 옆면에서 레이더 접근 시 '인간' 기호로 객체가 감지되었는지 확인		
3b. 옆면에서 레이더에 접근할 때 진행 방향이 올바른지 확인		

검증 완료

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

1. 레이더를 구성하고 지침을 따랐는지 확인합니다.
2. 추가 검증을 위해, 참조 지도를 추가하고 보정합니다.
3. 적절한 객체가 감지되면 트리거하기 위해 레이더 시나리오를 설정합니다. 기본적으로 **seconds until trigger(트리거까지 걸리는 초)**가 2초로 설정되어 있지만 필요한 경우 웹 인터페이스에서 변경할 수 있습니다.
4. 적절한 객체가 감지되면 레이더를 record data(데이터를 기록)로 설정합니다. 지침은 항목을 참고하십시오.
5. **trail lifetime(트레일 수명)**을 1시간으로 설정하여 자리에서 나와 감시 구역을 돌아보고 자리로 돌아오는 시간을 안전하게 초과하도록 합니다. **trail lifetime(트레일 수명)**은 설정된 시간 동안 레이더의 실시간 보기에 추적을 유지하며 확인이 완료되면 비활성화할 수 있습니다.
6. 레이더 감지 영역의 경계를 따라 걷고 시스템의 후행이 사용자가 걸은 경로와 일치하는지 확인합니다.
7. 검증 결과가 만족스럽지 않으면 참조 지도를 다시 보정하고 검증을 반복합니다.

상세 정보

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

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

H.265 또는 MPEG-H Part 2/HEVC

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

비고

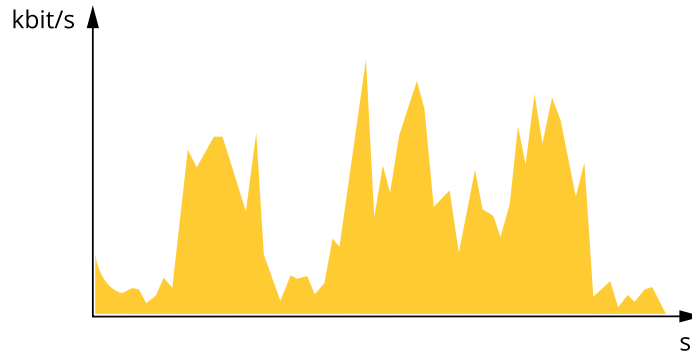
- H.265는 라이선스가 부여된 기술입니다. Axis 제품에는 1개의 H.265 보기 클라이언트 라이선스가 포함되어 있습니다. 라이선스가 없는 추가 클라이언트 사본을 설치하는 것은 금지되어 있습니다. 추가 라이선스를 구입하려면 Axis 리셀러에게 문의하십시오.
- 대부분의 웹 브라우저는 H.265 디코딩을 지원하지 않으며, 이 때문에 카메라는 웹 인터페이스에서 H.265 디코딩을 지원하지 않습니다. 대신 H.265 디코딩을 지원하는 영상 관리 시스템 또는 애플리케이션을 사용할 수 있습니다.

비트 레이트 제어

비트 레이트 제어가 비디오 스트림의 대역폭 소비를 관리하도록 지원합니다.

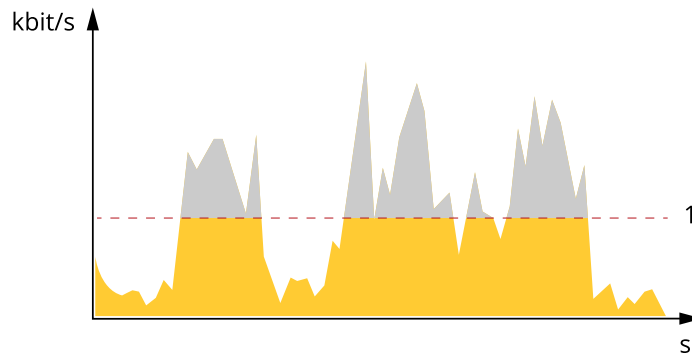
가변 비트 레이트(VBR)

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.

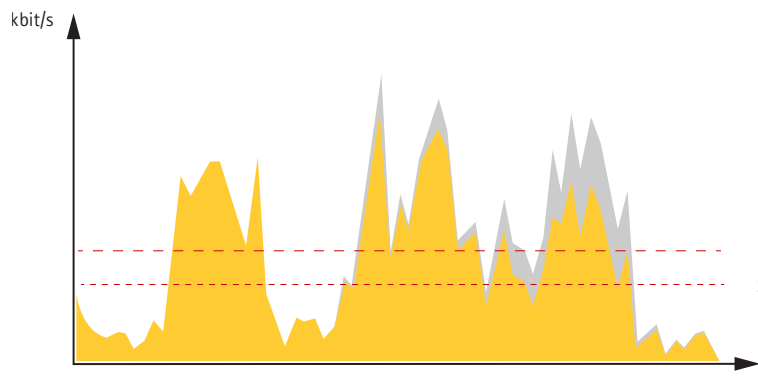


1 대상 비트 레이트

평균 비트 레이트(ABR)

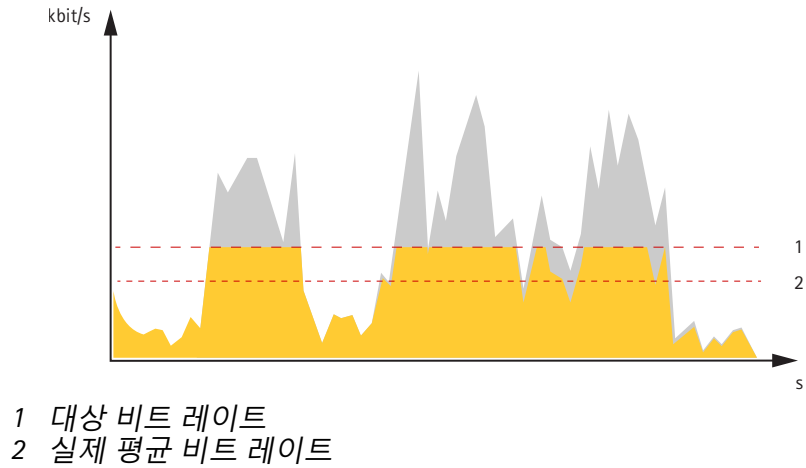
평균 비트 레이트를 사용하면 더 오랜 기간에 비트 레이트가 자동으로 조정됩니다. 지정된 대상을 충족하고 사용 가능한 스토리지를 기반으로 최상의 비디오 품질을 제공할 수 있습니다. 정적 장면에 비해 활동량이 많은 장면에서 비트 레이트가 더 높습니다. 평균 비트 레이트 옵션을 사용하면 활동이 많은 장면에서 더 나은 이미지 품질을 얻을 가능성이 더 큼니다. 이미지 품질이 지정된 대상 비트 레이트에 맞게 조정될 때 지정된 시간(보존 시간) 동안 비디오 스트림을 저장하는 데 필요한 총 스토리지를 정의할 수 있습니다. 다음 방법 중 하나로 평균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

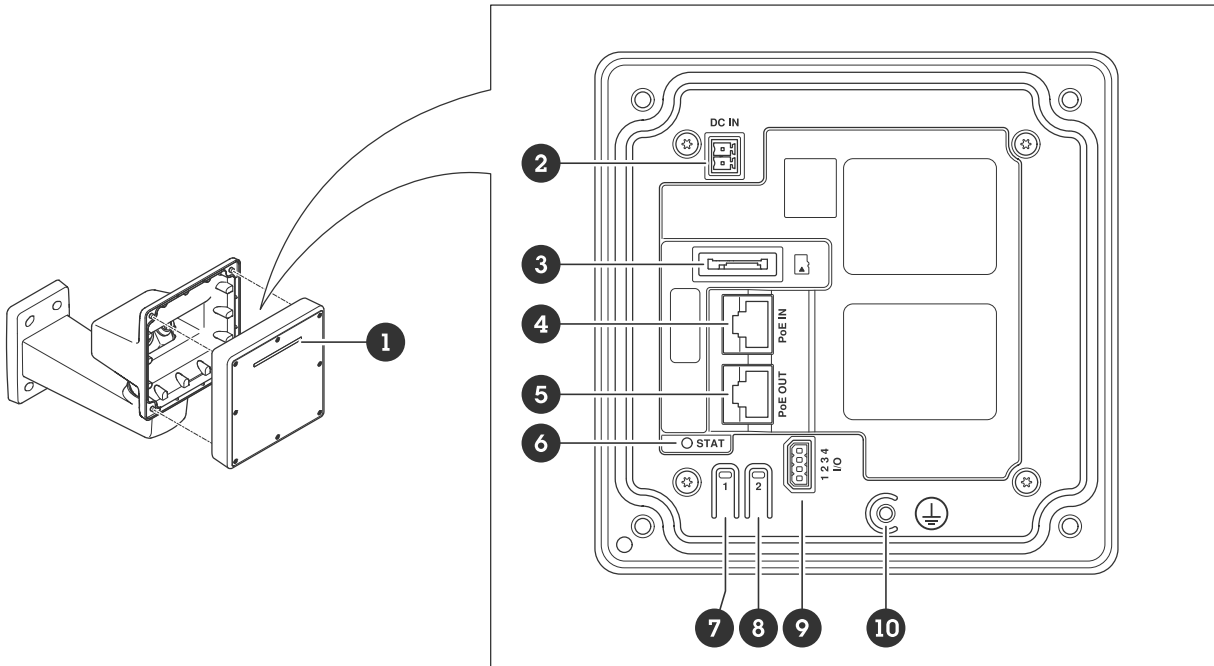


오버레이

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

사양

제품 개요



- 1 동적 LED 스트립
- 2 전원 커넥터(DC)
- 3 microSD 카드 슬롯
- 4 네트워크 커넥터(PoE 입력)
- 5 네트워크 커넥터(PoE 출력)
- 6 LED 상태 표시기
- 7 제어 버튼
- 8 액션 버튼
- 9 I/O 커넥터
- 10 접지 나사
- 11 리셋 버튼

LED 표시

비고

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

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.
빨간색	장치 소프트웨어 업그레이드 실패 상태입니다.

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.com을 참조하십시오.

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

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

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

커넥터

네트워크 커넥터(PoE 입력)

PoE(Power over Ethernet) IEEE 802.3bt, Type 3 Class 6를 지원하는 RJ45 Ethernet 커넥터입니다.

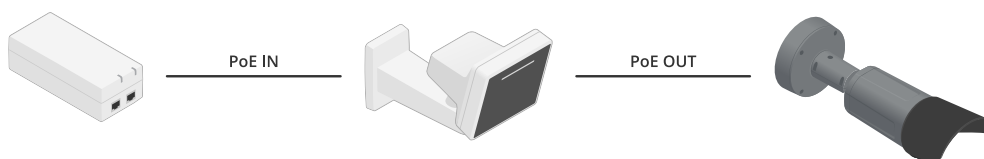
비고

PoE(Power over Ethernet)IEEE 802.3bt, Type 3 Class 6은 PoE 출력에 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 802.3at, Type 2 Class 4, 최대 30W를 공급하는 RJ45 Ethernet 커넥터입니다.

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



비고

레이더에 60W 미드스팬(Power over Ethernet IEEE 802.3bt, type 3)으로 전원을 공급하면 PoE 출력이 활성화됩니다.

비고

레이더에 30W 미드스팬 또는 DC 전원이 공급되면 PoE 출력이 비활성화됩니다.

비고

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

비고

연결된 PoE 장치에 30W 이상이 필요한 경우 레이더의 PoE 출력 포트와 장치 사이에 60W 미드스팬을 추가할 수 있습니다. 미드스팬은 장치에 전원을 공급하고 레이더는 이더넷 연결을 제공합니다.

I/O 커넥터

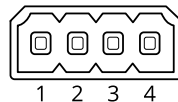
이벤트 트리거링, 알람 알림 등과 함께 외부 장치에 I/O 커넥터를 사용합니다. I/O 커넥터는 0 VDC 기준점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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

관리된 입력 - 디지털 입력에 대한 탬퍼링을 감지할 수 있습니다.

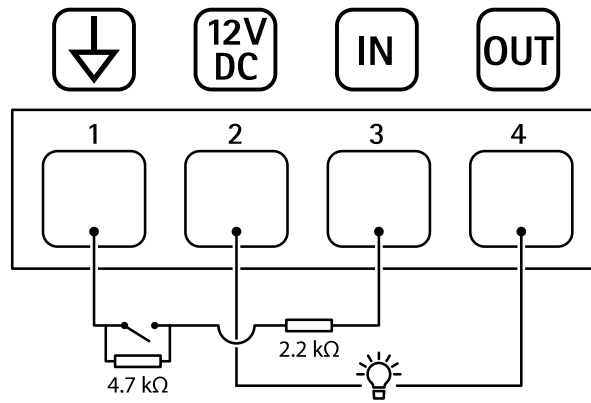
디지털 출력 - 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface로 이벤트를 통해 또는 장치의 웹 인터페이스에서 활성화할 수 있습니다.

4핀 단자대



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

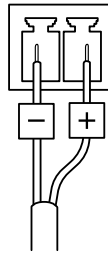
예:



- 1 DC 접지
- 2 DC 출력 12V, 최대 25mA
- 3 관리된 입력
- 4 디지털 출력

전원 커넥터

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



장치 세척

미지근한 물로 장치를 세척할 수 있습니다.

통지

- 자극적인 화학 물질로 인해 장치가 손상될 수 있습니다. 창문 세정제나 아세톤과 같은 화학 물질을 사용하여 장치를 세척하지 마십시오.
 - 직사광선이나 고온에서 세척하면 얼룩이 생길 수 있으므로 주의해서 피해야 합니다.
1. 압축된 공기통을 사용하여 장치에서 먼지와 느슨한 오물을 제거하십시오.
 2. 필요한 경우 미지근한 물에 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 끕니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. 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/support의 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.

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

- Axis Communications AB에서 이를 보장하지는 않지만(새 AXIS OS에서 기능을 사용할 수 있는 경우) 장치 소프트웨어를 업그레이드할 때 사전 구성되고 사용자 지정된 설정이 저장됩니다.
- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

활성 트랙의 최신 AXIS OS 버전으로 장치를 업그레이드하면 제품이 사용 가능한 최신 기능을 수신합니다. 업그레이드하기 전에 항상 새 릴리스마다 제공되는 릴리즈 정보와 업그레이드 지침을 참조하십시오. 최신 AXIS OS 버전과 릴리즈 정보를 찾으려면 axis.com/support/device-software로 이동합니다.

1. axis.com/support/device-software에서 무료로 제공되는 AXIS OS 파일을 컴퓨터에 다운로드합니다.
2. 장치에 관리자로 로그인합니다.
3. **Maintenance > AXIS OS upgrade(유지보수 > AXIS OS 업그레이드)**로 이동하여 **Upgrade(업그레이드)**를 클릭합니다.

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

기술적 문제, 단서 및 해결 방안

찾는 내용이 여기에 없는 경우에는 axis.com/support에서 문제 해결 섹션을 확인해 보십시오.

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

장치가 다른 서브넷에 있습니다.	장치에 해당하는 IP 주소와 장치 액세스에 사용된 컴퓨터의 IP 주소가 다른 서브넷에 있는 경우에는 IP 주소를 설정할 수 없습니다. 네트워크 관리자에게 문의하여 IP 주소를 받으십시오.
IP 주소가 다른 장치에서 사용 중입니다.	네트워크에서 Axis 장치를 분리합니다. Ping 명령을 실행합니다(명령 프롬프트/DOS 창에서 ping 및 장치의 IP 주소 입력). - Reply from <IP address>: bytes=32; time=10...이라는 메시지를 수신하는 경우, 이는 해당 IP 주소를 네트워크상의 다른 장치가 이미 사용하고 있을 수 있다는 것을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 장치를 다시 설치하십시오. - Request timed out이라는 메시지를 수신하는 경우, 이는 해당 IP 주소가 Axis 장치용으로 사용 가능하다는 것을 의미합니다. 모든 케이블 배선을 확인하고 장치를 다시 설치하십시오.
동일한 서브넷의 다른 장치와 충돌하는 가용 IP 주소	DHCP 서버에서 다이내믹 주소를 설정하기 전에 Axis 장치의 고정 IP 주소가 사용되었습니다. 이는 동일한 기본 고정 IP 주소가 다른 장치에서도 사용되는 경우 장치 액세스에 문제가 발생했을 수 있음을 의미합니다.

장치를 브라우저에서 액세스할 수 없음

로그인할 수 없음	HTTPS가 활성화된 경우 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 필드에 http 또는 https를 수동으로 입력해야 할 수도 있습니다. root 계정의 패스워드를 분실한 경우에는 장치를 공장 출하 시 기본값으로 재설정해야 합니다. 을 참조하십시오.
IP 주소가 DHCP에 의해 변경됨	DHCP서버에서 획득한 IP 주소는 동적이며 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(시스템) > Date and time(날짜 및 시간) 으로 이동합니다.

장치에 로컬로 액세스할 수 있지만 외부에서 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 5: 30일 무료 평가판이며, 중규모 시스템에 적합합니다.
- AXIS Camera Station Pro: 90일 무료 평가판이며, 중규모 시스템에 적합합니다.

지침 및 다운로드를 axis.com/vms로 이동합니다.

MQTT SSL 보안 포트 8883을 통해 연결할 수 없음

포트 8883을 사용하는 트래픽은 안전하지 않다고 간주되어 방화벽에서 차단됩니다.

경우에 따라 서버/브로커는 MQTT 통신에 필요한 특정 포트를 제공하지 않을 수도 있습니다. 그래도 HTTP/HTTPS 트래픽에 일반적으로 사용되는 포트를 통해 MQTT를 사용할 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.

성능 고려 사항

시스템을 설정할 때, 필요한 대역폭의 양(비트 레이트)에 다양한 설정과 상황이 성능에 어떠한 영향을 주는지 고려해야 합니다.

가장 중요하게 고려해야 할 요인은 다음과 같습니다.

- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.

지원 센터 문의

추가 도움이 필요하면 axis.com/support로 이동하십시오.

T10193646_ko

2025-06 (M15.2)

© 2023 – 2025 Axis Communications AB