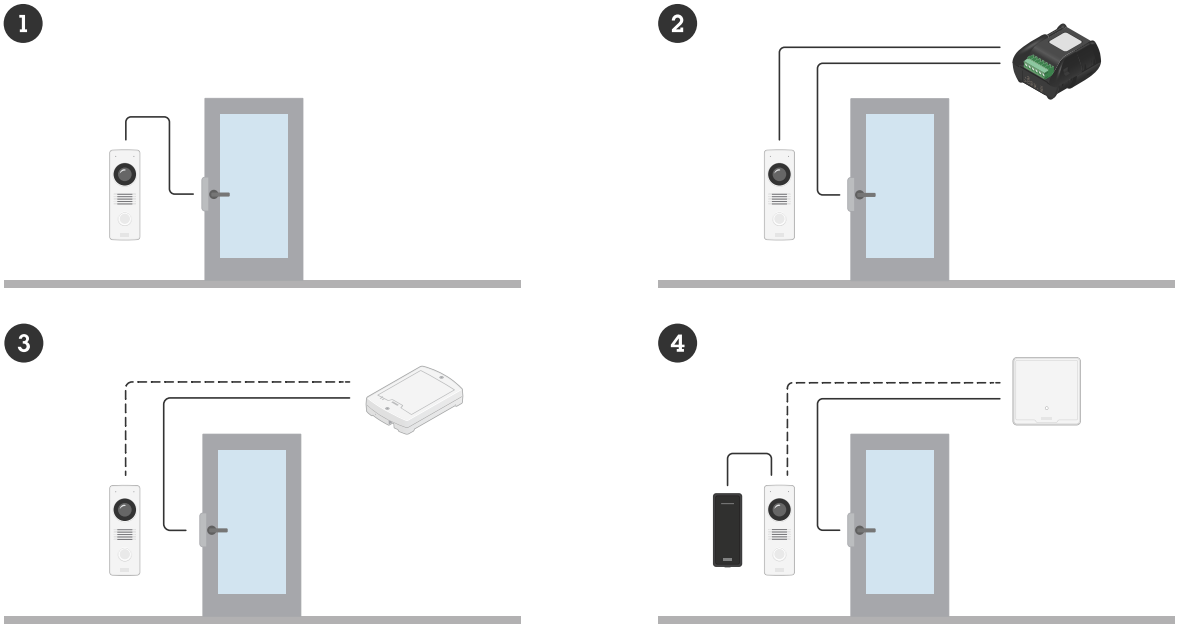
AXIS I8116-E Network Video Intercom

사용자 설명서

목차

설정 개요



1 인터콤
2 AXIS A9801과 결합된 인터콤
3 AXIS A9161과 결합된 인터콤
4 Axis 리더와 도어 컨트롤러가 결합된 인터콤

설치

이 비디오는 장치를 설치하는 방법을 보여줍니다.

미리 보기 모드

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

이 영상은 미리 보기 모드를 사용하는 방법을 보여줍니다.

시작하기

네트워크에서 장치 찾기

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

*IP 주소를 할당하고 장치에 액세스하는 방법*으로 이동하여 어떻게 IP 주소를 찾아 할당하는지 자세히 알아보십시오.

브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

	Chrome™	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. 라이센스 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

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

기본 설정

전력선 주파수 설정

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

root 패스워드 변경

1. 제품 인터페이스에 로그인하고 **System > Users(시스템 > 사용자)**로 이동합니다.
2. root 사용자의 경우 ⋮ **> Update user(사용자 업데이트)**를 클릭합니다.
3. 새 패스워드를 입력하고 저장합니다.

다이렉트 SIP(P2P) 설정

VoIP(음성 IP)는 IP 네트워크를 통한 음성 및 멀티미디어 통신을 활성화하는 기술 그룹입니다. 자세한 내용은 를 참조하십시오.

이 장치에서는 SIP 프로토콜을 통해 VoIP가 활성화됩니다. SIP에 대한 자세한 내용은 를 참조하십시오.

SIP에는 두 가지 유형의 설정이 있습니다. 직접 또는 P2P(피어 투 피어)가 그 중 하나입니다. 동일한 IP 네트워크에 있는 소수의 사용자 에이전트 간에 통신이 이루어지고 PBX 서버가 제공할 수 있는 별도의 기능이 필요 없으면 피어 투 피어를 사용하십시오. 설정 방법은 항목을 참조하십시오.

1. **Communication > SIP > Settings(통신 > SIP > 설정)**로 이동하고 **Enable SIP(SIP 활성화)**를 선택합니다.
2. 장치가 수신 콜을 받게 하려면 **Allow incoming calls(수신 콜 허용)**를 선택합니다.

통지

수신 콜을 허용하면 장치가 네트워크에 연결된 모든 장치로부터 오는 콜을 수락합니다. 공용 네트워크나 인터넷에서 장치에 액세스할 수 있으면 수신 통화를 허용하지 않는 것이 좋습니다.

3. **Call handling(콜 처리)**을 클릭합니다.
4. **Call timeout(콜 시간 초과)**에서 응답이 없을 경우 콜이 끝나기 전까지 지속되는 시간(초)을 설정합니다.
5. 수신 통화를 허용한 경우 수신 통화에 대한 시간 초과 전의 시간(초)을 **Incoming call timeout (수신 콜 시간 초과)**에서 설정하십시오.
6. **Ports(포트)**를 클릭합니다.
7. **SIP port(SIP 포트)** 번호와 **TLS port(TLS 포트)** 번호를 입력합니다.

비고

- **SIP port(SIP 포트)** - SIP 세션에 사용됩니다. 이 포트를 통한 신호 트래픽은 암호화되지 않습니다. 기본 포트 번호는 5060입니다.
- **TLS port(TLS 포트)** - SIPS 및 TLS 보안 SIP 세션에 사용됩니다. 이 포트를 통한 신호 트래픽은 전송 계층 보안(TLS)으로 암호화됩니다. 기본 포트 번호는 5061입니다.
- **RTP 시작 포트** - SIP 콜에서 첫 번째 RTP 미디어 스트림에 사용되는 포트입니다. 기본 시작 포트는 4000입니다. 일부 방화벽이 특정한 포트 번호에서 RTP 트래픽을 차단합니다. 포트 번호는 1024~65535 사이여야 합니다.

8. **NAT 통과**를 클릭합니다.
9. NAT 통과에 사용할 프로토콜을 선택합니다.

비고

장치가 NAT 라우터 또는 방화벽 뒤에 있는 네트워크에 연결되어 있는 경우 NAT 통과를 사용하십시오. 자세한 내용은 를 참조하십시오.

10. **Save(저장)**를 클릭합니다.

서버(PBX)를 통해 SIP 설정

VoIP(음성 IP)는 IP 네트워크를 통한 음성 및 멀티미디어 통신을 활성화하는 기술 그룹입니다. 자세한 내용은 를 참조하십시오.

이 장치에서는 SIP 프로토콜을 통해 VoIP가 활성화됩니다. SIP에 대한 자세한 내용은 를 참조하십시오.

SIPS 설정에는 두 가지 유형이 있습니다. PBX 서버가 그 중 하나입니다. IP 네트워크 안팎에서 무한대의 사용자 에이전트 사이에 통신이 이루어져야 할 경우 PBX 서버를 사용하십시오. PBX 공급자에 따라서 설정에 기능이 더 추가될 수 있습니다. 자세한 내용은 를 참조하십시오.

1. PBX 공급자에게 다음 정보를 요청합니다.
   - 사용자 ID
   - 도메인
   - 패스워드
   - 인증 ID
   - 발신자 ID
   - 등록자
   - RTP 시작 포트
2. **통신 > SIP > 계정**으로 이동하여 **+ 계정 추가**를 클릭합니다.
3. 계정 **Name(이름)**을 입력합니다.
4. **Registered(등록됨)**를 선택합니다.
5. 전송 모드를 선택합니다.
6. PBX 공급자가 제공하는 계정 정보를 추가합니다.
7. **Save(저장)**를 클릭합니다.
8. 피어 투 피어와 같은 방법으로 SIP 설정을 지정하고 항목을 참고하십시오. PBX 공급자의 RTP 시작 포트를 사용합니다.

연락처 만들기

이 예는 연락처 목록에서 새 연락처를 생성하는 방법을 설명합니다. 시작하기 전에 **Communication > SIP(통신 > SIP)**에서 SIP를 활성화하십시오.

새 연락처를 생성하려면:

1. **Communication > Contact list(통신 > 연락처 목록)**로 이동합니다.
2. **+ Add contact(+ 연락처 추가)**를 클릭합니다.
3. 연락처의 성 및 이름을 입력합니다.
4. 연락처의 SIP 주소를 입력합니다.

비고

SIP 주소에 대한 자세한 내용은 항목을 참고하십시오.

5. 전화를 걸 SIP 계정을 선택합니다.

비고

가용성 옵션은 **System(시스템)** >**Events(이벤트)** >**Schedules(일정)**에서 정의됩니다.

6. 연락처의 **Availability(가용성)**을 선택합니다. 연락처가 없을 때 통화하면 대체 연락처가 없는 한 통화가 취소됩니다.

비고

대체는 원래 연락처가 응답하지 않거나 사용할 수 없는 경우 통화가 전달되는 연락처입니다.

7. **Fallback(대체)**에서 **None(없음)**을 선택합니다.
8. **Save(저장)**를 클릭합니다.

통화 버튼 구성

기본적으로 통화 버튼은 영상 관리 소프트웨어(VMS) 통화를 하도록 구성되어 있습니다. 이 구성을 유지하려면 Axis 인터콤을 VMS에 추가하기만 하면 됩니다.

이 예는 방문자가 통화 버튼을 누를 때 연락처 목록에서 연락처를 호출하도록 시스템을 설정하는 방법을 설명합니다.

1. **Communication > Calls > Call button(통신 > 통화 > 통화 버튼)**으로 이동합니다.
2. **수신자**에서 **VMS**를 제거합니다.
3. **수신자**에서 기존 연락처를 선택하거나 새 연락처를 생성합니다.

통화 버튼을 비활성화하려면 **Enable call button(통화 버튼 활성화)**을 끕니다.

DTMF를 사용하여 방문자용 도어를 잠금 해제하십시오

방문자가 인터콤에서 전화를 걸면 응답자는 SIP 장치의 DTMF(Dual-Tone Multi-Frequency Signaling)를 사용하여 도어를 잠금 해제할 수 있습니다. 도어 컨트롤러는 도어를 잠금 해제하고 잠급니다.

이 예제는 다음을 수행하는 방법을 설명합니다.

- 인터콤에서 DTMF 신호 정의
- 인터콤을 설정하려면:
  - 도어 컨트롤러에 도어 잠금을 해제하도록 요청하거나 **또는**
  - 내부 릴레이를 사용하여 도어를 잠금 해제합니다.

인터콤의 웹 페이지에서 모든 설정을 합니다.

시작하기 전

- 장치에서 SIP 호출을 허용하고 SIP 계정을 생성합니다. 자세한 내용은 및 항목을 참조하십시오.

인터콤에서 DTMF 신호 정의

1. **통신 > SIP > DTMF**로 이동합니다.
2. **+ 시퀀스 추가**를 클릭합니다.
3. **Sequence(시퀀스)**에 1을 입력합니다.
4. **Description(설명)**에 Unlock door(도어 잠금 해제)를 입력합니다.

5. **계정**에서 SIP 계정을 선택합니다.
6. **Save(저장)**를 클릭합니다.

내부 릴레이를 사용하여 도어를 잠금 해제하도록 인터콤 설정

7. **System(시스템) > Events(이벤트) > Rules(룰)**로 이동하고 룰을 추가합니다.
8. **Name(이름)** 필드에 DTMF unlock door(DTMF 도어 잠금 해제)를 입력합니다.
9. 조건 목록의 **콜** 아래에서 **DTMF** 및 **도어 잠금 해제**를 선택합니다.
10. 액션 목록의 **I/O** 아래에서 **Toggle I/O once(I/O 한 번 토글)**를 선택합니다.
11. 포트 목록에서 **Relay 1(릴레이 1)**을 선택합니다.
12. **Duration(기간)**을 00:00:07으로 변경하는 것은 도어가 7초 동안 열려 있음을 의미합니다.
13. **Save(저장)**를 클릭합니다.

자격 증명 홀더가 도어를 열 수 있도록 허용

항목 목록을 사용하면 자격 증명 홀더가 카드 또는 핀으로 도어를 여는 등의 작업을 트리거하도록 설정할 수 있습니다. 이 예에서는 카드를 사용하여 도어를 10번 열 수 있는 자격 증명 홀더를 추가하는 방법을 설명합니다.

전제 조건

- **리더 > 칩 유형**에서 올바른 칩 유형이 활성화되었는지 확인합니다.

항목 목록을 켜고 자격 증명 홀더를 추가합니다.

1. **리더 > 항목 목록**으로 이동합니다.
2. **항목 목록 사용**을 켭니다.
3. **+ 자격 증명 홀더 추가**를 클릭합니다.
4. 자격 증명 홀더의 이름과 성을 입력합니다. 이름은 고유해야 합니다.
5. **카드**를 선택합니다.
6. 장치에 자격 증명 홀더의 카드를 대고 **최신 항목 가져오기**를 클릭합니다.
7. 이벤트 조건을 **접근 허용**으로 유지합니다.
8. **만료**에서 **횟수**를 선택합니다.
9. **Number of times(횟수)**에 10을 입력합니다.
10. **Save(저장)**를 클릭합니다.

룰 생성:

1. **System > Events(시스템 > 이벤트)**로 이동합니다.
2. **룰**에서 **+ 룰 추가**를 클릭합니다.
3. **Name(이름)**에 Open door(도어 열기)를 입력합니다.
4. 조건 목록에서 **항목 목록 > 접근 허용**을 선택합니다.
5. 액션 목록에서 **I/O > I/O 한 번 토글**을 선택합니다.
6. 포트 목록에서 **도어**를 선택합니다.
7. **상태**에서 **활성**을 선택합니다.
8. 지속 시간을 00:00:07로 설정합니다.
9. **Save(저장)**를 클릭합니다.

이미지 조정

이 섹션에는 장치 구성에 대한 지침이 포함되어 있습니다. 특정 기능의 작동 방식에 대해 자세히 알아보려면 로 이동하십시오.

노출 모드 선택

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

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

저조도 조건에서 노이즈를 감소

저조도 조건에서 노이즈를 감소시키려면 다음 설정 중 하나 이상을 조정하십시오.

- 노이즈와 모션 블러 간의 균형을 조정합니다. **Video > Image > Exposure(비디오 > 이미지 > 노출)**로 이동하고 **Blur-noise trade-off(블러-노이즈 균형)** 슬라이더를 **Low noise(낮은 노이즈)**쪽으로 이동합니다.
- 노출 모드를 자동으로 설정합니다.

비고

최대 셔터 값이 높으면 모션 블러가 발생할 수 있습니다.

- 셔터 속도를 늦추려면 최대 셔터를 가능한 최대 값으로 설정합니다.

비고

최대 게인을 줄이면 이미지가 어두워질 수 있습니다.

- 최대 게인을 더 낮은 값으로 설정합니다.
- **Aperture(조리개)** 슬라이더가 있는 경우 **Open(열기)** 쪽으로 이동합니다.
- **Video > Image > Appearance(비디오 > 이미지 > 모양)**에서 이미지의 선명도를 줄입니다.

텍스트 오버레이 표시

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

1. **Video(비디오) > Overlays(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.

이벤트의 룰 설정

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

자세히 알아보려면 *이벤트 룰 시작하기* 가이드를 확인하십시오.

장치가 객체를 감지하면 비디오 스트림에 텍스트 오버레이 표시

이 예는 장치가 객체를 감지할 때 '모션 감지됨' 텍스트를 표시하는 방법을 설명합니다.

AXIS Object Analytics가 실행 중인지 확인합니다.

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

오버레이 텍스트 추가:

1. **Video(비디오) > Overlays(오버레이)**로 이동합니다.
2. **Overlays(오버레이)**에서, **Text(텍스트)**를 선택하고 + 을 클릭합니다.
3. 텍스트 필드에 `#D`를 입력합니다.
4. 텍스트 크기와 모양을 선택합니다.
5. 텍스트 오버레이의 위치를 지정하려면, 을 클릭하고 옵션을 선택합니다.

룰 생성:

1. **System(시스템) > Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록의 **Application(애플리케이션)**에서 **Object Analytics**를 선택합니다.
4. 작업 목록에서**Overlay text(오버레이 텍스트)**에서 **Use overlay text(오버레이 텍스트 사용)**를 선택합니다.
5. 비디오 채널을 선택합니다.
6. **Text(텍스트)**에서 “Motion detected(움직임 감지)“를 입력합니다.
7. 기간을 설정합니다.
8. **Save(저장)**를 클릭합니다.

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

비고

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

기본 메뉴를 표시하거나 숨깁니다.

릴리스 정보에 액세스합니다.

제품 도움말에 액세스합니다.

언어를 변경합니다.

밝은 테마 또는 어두운 테마를 설정합니다.

사용자 메뉴에는 다음이 포함됩니다.

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

상황에 맞는 메뉴에는 다음이 포함됩니다.

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

상태

장치 정보

AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 표시합니다.

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

시간 동기화 상태

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

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

보안

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

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

연결된 클라이언트

연결 및 연결된 클라이언트 수를 표시합니다.

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

녹화/녹음 진행 중

진행 중인 녹화와 지정된 저장 공간을 표시합니다.

녹화물: 진행 중이고 필터링된 녹화물과 해당 소스를 봅니다. 자세한 내용은 를 참조하십시오.

녹화물이 저장되는 저장 공간을 표시합니다.

비디오

라이브 비디오 스트림을 재생하려면 클릭합니다.

라이브 비디오 스트림을 정지하려면 클릭합니다.

비디오 스트림의 스냅샷 찍기를 하려면 클릭합니다. 파일은 컴퓨터의 'Downloads' 폴더에 저장됩니다. 이미지 파일 이름은 [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]입니다. 스냅샷의 크기는 스냅샷이 수신되는 특정 웹 브라우저 엔진이 적용되는 압축에 따라 다르므로 스냅샷 크기는 장치에 구성된 실제 압축 설정과 다를 수 있습니다.

I/O 출력 포트를 표시하려면 클릭합니다. 예를 들어, 외부 장치를 테스트하기 위해 스위치를 사용하여 포트의 회로를 열거나 닫습니다.

IR 조명을 수동으로 켜거나 끄려면 클릭합니다.

백색광을 수동으로 켜거나 끄려면 클릭합니다.

화면 컨트롤에 액세스하려면 클릭합니다. 화면 컨트롤 그룹을 활성화하면, 사용자가 비디오 매니지먼트 소프트웨어(VMS)에서 라이브 스트림을 마우스 오른쪽 버튼으로 클릭하면 각 그룹의 설정을 이용할 수 있습니다.

- **Predefined controls(사전 정의된 컨트롤)**: 기본 화면 컨트롤을 나열합니다.
- **Custom controls(사용자 지정 컨트롤)**: **Add custom control(사용자 지정 컨트롤 추가)**을 클릭하여 사용자 지정 화면 컨트롤을 만들 수 있습니다.

워셔를 시작합니다. 시퀀스가 시작되면 워시 스프레이에 닿도록 구성된 위치로 카메라가 움직입니다. 워시 시퀀스가 다 끝나면 카메라가 이전의 위치로 돌아갑니다. 워셔가 연결 및 구성된 경우에만 이 아이콘이 보입니다.

와이퍼를 시작합니다.

프리셋 포지션을 클릭하고 선택하면 실시간 보기에서 해당 프리셋 포지션으로 이동합니다. 또는 **Setup(설정)**을 클릭하여 프리셋 포지션 페이지로 이동합니다.

포커스 리콜 영역을 추가하거나 제거합니다. 포커스 리콜 영역을 추가할 때 카메라가 특정 팬/틸트 범위에서 포커스 설정을 저장합니다. 포커스 리콜 영역을 설정하고 카메라가 실시간 보기에서 해당 영역으로 이동하면 카메라가 이전에 저장한 포커스를 리콜합니다. 포커스를 리콜하는 카메라에 대한 영역을 절반 정도는 충분히 덮을 수 있습니다.

클릭하여 가드 투어를 선택한 다음 **Start(시작)**를 클릭하여 가드 투어를 재생합니다. 또는 **Setup(설정)**을 클릭하여 가드 투어 페이지로 이동합니다.

선택한 시간 동안 히터를 수동으로 켜려면 클릭합니다.

라이브 비디오 스트림의 지속 녹화를 시작하려면 클릭합니다. 녹화를 중지하려면 다시 클릭합니다. 녹화가 진행 중인 경우, 재부팅 후 자동으로 다시 시작됩니다.

장치에 대해 구성된 스토리지를 표시하려면 클릭합니다. 스토리지를 구성하려면 관리자로 로그인해야 합니다.

추가 설정에 액세스하려면 클릭합니다.

- **Video format(비디오 형식)**: 실시간 보기에서 사용할 인코딩 형식을 선택합니다.
- **Autoplay(자동 재생)**: 새 세션에서 장치를 열 때마다 음소거된 비디오 스트림을 자동 재생하려면 켜십시오.
- **Client stream information(클라이언트 스트림 정보)**: 라이브 비디오 스트림을 표시하는 브라우저에서 사용하는 비디오 스트림에 대한 동적 정보를 표시하려면 켭니다. 비트 레이트 정보는 정보 소스가 다르기 때문에 텍스트 오버레이에 표시되는 정보와 다릅니다. 클라이언트 스트림 정보의 비트 레이트는 마지막 1초의 비트 레이트가며 장치의 인코딩 드라이버에서 가져옵니다. 오버레이의 비트 레이트는 지난 5초의 평균 비트 레이트가며 브라우저에서 가져옵니다. 두 값 모두 원시 비디오 스트림만 포함하며 UDP/TCP/HTTP를 통해 네트워크를 통해 전송될 때 생성되는 추가 대역폭은 포함하지 않습니다.
- **Adaptive stream(적응형 스트림)**: 이미지 해상도를 보기 클라이언트의 실제 디스플레이 해상도에 맞게 조정하여 사용자 경험을 개선하고 클라이언트 하드웨어의 과부하를 방지하려면 켭니다. 적응형 스트림은 브라우저의 웹 인터페이스에서 라이브 비디오 스트림을 볼 때만 적용됩니다. 적응형 스트림이 켜져 있을 때 최대 프레임 속도는 30fps입니다. 적응형 스트림이 켜져 있는 동안 스냅샷을 촬영하면 적응형 스트림에서 선택한 이미지 해상도가 사용됩니다.
- **Level grid(수평 그리드)**: 수평 그리드를 표시하려면 을 클릭합니다. 격자는 이미지가 수평으로 정렬되었는지 결정하는 데 도움이 됩니다. 숨기려면 을 클릭합니다.
- **Pixel counter(픽셀 카운터)**: 픽셀 카운터를 표시하려면 을 클릭합니다. 관심 영역을 포함하려면 상자를 끌어 영역 크기를 조정합니다. 또한 **Width(너비)** 및 **Height(높이)** 필드에서 상자의 픽셀 크기를 정의할 수 있습니다.
- **Refresh(새로 고침)**: 실시간 보기에서 정지 이미지를 새로 고치려면 을 클릭합니다.
- **PTZ controls(PTZ 제어)** : 실시간 보기에서 PTZ 제어를 표시하려면 켭니다.

전체 해상도로 실시간 보기를 표시하려면 클릭합니다. 전체 해상도가 화면 크기보다 큰 경우 더 작은 이미지를 사용하여 이미지를 탐색합니다.

라이브 비디오 스트림을 전체 화면으로 표시하려면 클릭합니다. 전체 화면 모드를 종료하려면 ESC 키를 누릅니다.

설치

Capture mode(캡처 모드) : 캡처 모드는 카메라가 이미지를 캡처하는 방법을 정의하는 프리셋 구성입니다. 캡처 모드를 변경하면 보기 영역 및 프라이버시 마스크와 같은 다른 많은 설정에 영향을 줄 수 있습니다.

Mounting position(장착 위치) : 카메라 장착 방법에 따라 이미지의 방향이 변경될 수 있습니다.

Power line frequency(전력선 주파수): 이미지 깜박임을 최소화하려면 해당 지역에서 사용하는 주파수를 선택합니다. 미국 지역은 보통 60Hz를 사용합니다. 세계의 나머지 지역은 대부분 50Hz를 사용합니다. 해당 지역의 전력선 주파수를 잘 모르는 경우 현지 기관에 확인하십시오.

Rotate(회전): 원하는 이미지 방향을 선택합니다.

이미지

표현

Scene profile(장면 프로파일) : 감시 시나리오에 적합한 장면 프로파일을 선택합니다. 장면 프로파일은 특정 환경이나 목적에 맞게 색상 수준, 밝기, 선명도, 대비 및 로컬 대비를 비롯한 이미지 설정을 최적화합니다.

- **Forensic(포렌직)** : 감시 목적에 적합합니다.
- **Indoor(실내)** : 실내 환경에 적합합니다.
- **Outdoor(실외)** : 실외 환경에 적합합니다.
- **Vivid(선명함)** : 데모 목적으로 유용합니다.
- **Traffic overview(트래픽 오버뷰)** : 차량 교통 모니터링에 적합합니다.
- **번호판** : 번호판 캡처에 적합합니다.

Saturation(채도): 슬라이더를 사용하여 색상 강도를 조정합니다. 예를 들어, 회색조 이미지를 얻을 수 있습니다.

Contrast(대비): 밝은 색과 어두운 색의 차이를 조정하려면 슬라이더를 사용합니다.

Brightness(밝기): 슬라이더를 사용하여 조명 강도를 조정합니다. 이렇게 하면 객체를 더 쉽게 볼 수 있습니다. 밝기는 이미지가 캡처된 후에 적용되며 이미지의 정보에는 영향을 주지 않습니다. 어두운 부분을 더 자세히 보이게 하려면 일반적으로 게인 또는 노출 시간을 증가하는 것이 좋은 경우도 있습니다.

Sharpness(선명도): 슬라이더를 사용하여 가장자리 대비를 조정하여 이미지의 개체를 더 선명하게 표시합니다. 선명도를 높이면 비트 레이트가 증가하고 필요한 저장 공간도 늘어날 수 있습니다.

광역 역광 보정(WDR)

WDR : 이미지의 밝은 영역과 어두운 영역을 모두 표시하려면 켭니다.

Local contrast(로컬 대비) : 슬라이더를 사용하여 이미지의 대비를 조정합니다. 값이 높을수록 어두운 영역과 밝은 영역 간의 대비가 높아집니다.

Tone mapping(톤 매핑) : 이미지에 적용되는 톤 매핑의 양을 조정하려면 슬라이더를 사용합니다. 값을 0으로 설정하면 표준 감마 보정만 적용되는 한편, 값이 높으면 이미지에서 가장 어두운 부분과 가장 밝은 부분의 가시성이 높아집니다.

화이트 밸런스

카메라가 들어오는 빛의 색 온도를 인식하면 이미지를 조정하여 색을 좀 더 자연스럽게 표현할 수 있습니다. 이것으로 충분하지 않으면 목록에서 적절한 광원을 선택할 수 있습니다.

자동 화이트 밸런스 설정은 변화에 서서히 적응하여 색 깜박임의 위험을 감소시켜 줍니다. 조명이 바뀌거나 카메라를 처음 시작할 때 새 광원에 적응하는 데 최대 30초가 걸릴 수 있습니다. 한 장면에서 두 가지 이상의 광원 유형이 있을 경우(즉, 색 온도가 다른 경우) 중심이 되는 광원이 자동 화이트 밸런스 알고리즘에 대해 참조 역할을 하게 됩니다. 이 동작은 참조로써 사용하고자 하는 광원과 일치하는 고정 화이트 밸런스 설정을 선택하여 무시할 수 있습니다.

Light environment(밝은 환경):

- **Automatic(자동)**: 광원 색을 자동으로 식별하고 보정합니다. 대부분의 상황에 적합한 권장 설정입니다.
- **Automatic – outdoors(자동 - 실외)** : 광원 색을 자동으로 식별하고 보정합니다. 대부분의 실외 상황에 사용될 수 있는 권장 설정입니다.
- **Custom – indoors(사용자 지정 - 실내)** : 형광등 조명 이외의 다른 인공조명이 있는 방과 2800K 정도의 일반 색 온도에 알맞은 고정 색 조정 기능입니다.
- **Custom – outdoors(사용자 지정 - 실외)** : 5500K 정도 색 온도의 맑은 날씨 조건에서 사용할 수 있는 고정 색 조정 기능입니다.
- **Fixed – fluorescent 1(고정 – 형광 1)**: 4000K 정도의 색 온도를 가진 형광등 조명을 위한 고정 색 조정 기능입니다.
- **Fixed – fluorescent 2(고정 – 형광 2)**: 3000K 정도의 색 온도를 가진 형광등 조명을 위한 고정 색 조정 기능입니다.
- **Fixed – indoors(고정 - 실내)**: 형광등 조명 이외의 다른 인공조명이 있는 방과 2800K 정도의 일반 색 온도에 알맞은 고정 색 조정 기능입니다.
- **Fixed – outdoors 1(고정 - 실외 1)**: 5500K 정도 색 온도의 맑은 날씨 조건에서 사용할 수 있는 고정 색 조정 기능입니다.
- **Fixed – outdoors 2(고정 - 실외 2)**: 6500K 정도 색 온도의 흐린 날씨 조건에서 사용할 수 있는 고정 색 조정 기능입니다.
- **Street light – mercury(가로등 - 수은)** : 가로등에서 흔히 볼 수 있는 수은등의 자외선 방출에 대한 색상 조정을 수정했습니다.
- **Street light – sodium(가로등 - 나트륨)** : 가로등에서 흔히 볼 수 있는 나트륨 등의 노란 오렌지색을 보상하는 고정 색 조정 기능입니다.
- **Hold current(현재 설정 유지)**: 현재 설정을 유지하고 조명 변경을 보정하지 않습니다.
- **Manual(수동)** : 흰색 객체를 사용하여 화이트 밸런스를 고정합니다. 실시간 보기 이미지에서 카메라가 흰색으로 해석할 만한 물체로 원을 끕니다. **Red balance(레드 밸런스)**와 **Blue balance(블루 밸런스)** 슬라이더를 사용하여 화이트 밸런스를 수동으로 조정합니다.

노출

다양한 유형의 광원에서 발생하는 깜박임과 같이 이미지에서 빠르게 변화하는 불규칙한 효과를 줄이려면 노출 모드를 선택합니다. 자동 조리개 모드 또는 전원 네트워크와 동일한 주파수를 사용하는 것이 좋습니다.

Exposure mode(노출 모드):

- **Automatic(자동)**: 카메라가 조리개, 게인 및 셔터를 자동으로 조정합니다.
- **Automatic aperture(자동 조리개)** : 카메라가 조리개 및 게인을 자동으로 조정합니다. 셔터가 고정됩니다.
- **Automatic shutter(자동 셔터)** : 카메라가 셔터와 게인을 자동으로 조정합니다. 조리개가 고정됩니다.
- **Hold current(현재 설정 유지)**: 현재 노출 설정을 잠급니다.
- **Flicker-free(깜박임 제거)** : 카메라는 조리개와 게인을 자동으로 조정하고 다음 셔터 속도만 사용합니다. 1/50초(50Hz) 및 1/60초(60Hz)
- **Flicker-free 50 Hz(깜박임 없는 50Hz)** : 카메라가 셔터 속도 1/50초를 사용하여 조리개와 게인을 자동으로 조정합니다.
- **Flicker-free 60 Hz(깜박임 없는 60Hz)** : 카메라가 셔터 속도 1/60초를 사용하여 조리개와 게인을 자동으로 조정합니다.
- **Flicker-reduced(깜박임 감소)** : 깜박임 제거와 같지만 더 밝은 장면에서 카메라가 1/100초(50Hz) 및 1/120초(60Hz)보다 빠른 셔터 속도를 사용할 수 있습니다.
- **Flicker-reduced 50 Hz(깜박임 감소 50Hz)** : 이는 깜박임 없는 것과 동일하지만 카메라는 더 밝은 장면을 위해 1/100초보다 빠른 셔터 속도를 사용할 수 있습니다.
- **Flicker-reduced 60 Hz(깜박임 감소 60Hz)** : 이는 깜박임 없는 것과 동일하지만 카메라는 더 밝은 장면을 위해 1/120초보다 빠른 셔터 속도를 사용할 수 있습니다.
- **Manual(수동)** : 조리개, 게인 및 셔터는 고정되어 있습니다.

Exposure zone(노출 영역) : 노출 영역을 사용하여 장면의 선택된 부분(예: 출입문 앞 영역)에서 노출을 최적화합니다.

비고

노출 영역은 원래 이미지(회전하지 않은 이미지)와 연관이 있으며, 존의 이름이 원래 이미지에 적용됩니다. 예를 들어 비디오 스트림을 90° 회전하면 스트림의 **Upper(위)**는 **Right(오른쪽)**가 되고 **Left(왼쪽)**는 **Lower(아래)**가 됩니다.

- **Automatic(자동)**: 대부분의 상황에 적합합니다.
- **Center(중앙)**: 이미지 중앙의 고정된 영역을 사용하여 노출을 계산합니다. 이 영역에는 실시간 보기의 고정 크기와 위치가 있습니다.
- **Full(최대)** : 전체 실시간 보기를 사용하여 노출을 계산합니다.
- **Upper(상단)** : 이미지 상단의 고정된 크기와 위치를 사용하여 노출을 계산합니다.
- **Lower(하단)** : 이미지 하단의 고정된 크기와 위치를 사용하여 노출을 계산합니다.
- **Left(왼쪽)** : 이미지 하단의 고정된 크기와 위치를 사용하여 노출을 계산합니다.
- **Right(오른쪽)** : 이미지 오른쪽의 고정된 크기와 위치를 사용하여 노출을 계산합니다.
- **Spot(스팟)**: 실시간 보기에서 크기와 위치가 고정된 영역을 사용하여 노출을 계산합니다.

- **Custom(사용자 지정)**: 실시간 보기의 영역을 사용하여 노출을 계산합니다. 영역의 크기와 위치를 조정할 수 있습니다.

Max shutter(최대 셔터): 최상의 이미지를 제공하기 위해 셔터 속도를 선택합니다. 셔터 속도가 낮을수록(노출이 길어질수록) 움직임에 모션 블러가 생길 수 있으며 셔터 속도가 너무 높으면 이미지 품질이 떨어질 수 있습니다. 최대 셔터와 최대 게인이 함께 사용되어 이미지를 개선합니다.

Max gain(최대 게인): 적절한 최대 게인을 선택하십시오. 최대 게인을 늘리면 어두운 이미지에서 볼 수 있는 부분이 증가할 수 있으나 노이즈 수준도 증가합니다. 노이즈가 높아질수록 사용 대역폭과 저장 용량이 증가할 수 있습니다. 최대 게인이 높은 값으로 설정한 경우 주간과 야간 조명 조건의 변화가 심할수록 이미지가 많이 달라질 수 있습니다. 최대 게인과 최대 셔터가 함께 사용되어 이미지를 개선합니다.

Motion-adaptive exposure(모션 적응형 노출) : 저조도 조건에서 모션 블러를 줄이기 위해 선택합니다.

Blur-noise trade-off(블러-노이즈 균형): 슬라이더를 사용하여 모션 블러와 노이즈 사이의 우선 순위를 조정합니다. 움직이는 객체의 디테일을 낮추어 낮은 대역폭을 우선 순위로 지정하고 노이즈를 줄이려면 이 매개변수를 **Low noise(낮은 노이즈)**로 조정하십시오. 노이즈와 대역폭을 희생하여 움직이는 객체의 디테일 유지를 우선 순위로 지정하려면 이 매개변수를 **Low motion blur(저모션 블러)**로 조정하십시오.

비고

노출 시간을 조정하거나 게인을 조정하여 노출을 변경할 수 있습니다. 노출 시간을 늘리면 모션 블러가 더 많이 발생하고 게인을 늘리면 노이즈가 더 많이 발생합니다. **Blur-noise trade-off(블러-노이즈 균형)**를 **Low noise(낮은 노이즈)**로 조정하면, 자동 조리개는 증가하는 게인보다 더 긴 노출 시간을 우선하게 되며, **Low motion blur(저모션 블러)**로 절충점을 조정하면 그 반대입니다. 저조도 조건에서는 이 매개변수로 설정된 우선 순위에 관계없이 게인과 노출 시간이 모두 최대값에 도달합니다.

Lock aperture(조리개 잠금) : **Aperture(조리개)** 슬라이더로 설정된 조리개 크기를 유지하려면 켭니다. 카메라가 조리개 크기를 자동으로 조정하도록 하려면 끄십시오. 예를 들어 영구 조명 조건인 장면에 대한 조리개를 잠글 수 있습니다.

Aperture(조리개) : 슬라이더를 사용하여 조리개 크기, 즉 렌즈를 통과하는 빛의 양을 조정합니다. 더 많은 빛이 센서에 들어가도록 하여 저조도 조건에서 더 밝은 이미지를 생성하려면 슬라이더를 **Open(열림)** 쪽으로 이동합니다. 조리개를 열면 피사계심도의 감소 즉, 카메라에서 가깝거나 먼 객체의 초점이 흐리게 나타날 수도 있습니다. 더 많은 이미지에 초점을 맞추려면 슬라이더를 **Closed(닫힘)** 쪽으로 이동합니다.

Exposure level(노출 수준): 슬라이더를 사용하여 이미지 노출을 조정합니다.

Defog(디포그) : 안개가 낀 날씨의 영향을 감지하고 더 선명한 이미지를 위해 자동으로 제거하려면 켜십시오.

비고

대비가 낮거나 조도 변화가 크거나 자동 초점이 약간 꺼져 있는 장면에서는 **Defog(디포그)**를 사용하지 않는 것이 좋습니다. 그러면 이미지 대비가 증가하는 등 이미지 품질이 저하될 수 있습니다. 게다가 디포그가 활성화되어 있을 때 밝기가 너무 높으면 이미지 품질이 낮아지기도 합니다.

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.

Zipstream

Zipstream은 비디오 감시에 최적화된 비트 레이트 감소 기술이며 실시간으로 H.264 또는 H.265 스트림에서 평균 비트 레이트를 줄여줍니다. Axis Zipstream은 움직이는 객체가 있는 장면과 같이 관심 영역이 여러 개 있는 장면에서 높은 비트 레이트를 적용합니다. 장면이 더 정적인 경우 Zipstream은 더 낮은 비트 레이트를 적용하여 필요한 저장 공간을 줄입니다. 자세한 내용은 *Axis Zipstream로 비트 레이트 줄이기*를 참조하십시오.

비트 레이트 감소 **Strength(강도)**를 선택합니다.

- **Off(끄기)**: 비트 레이트 감소 없음.
- **Low(낮음)**: 대부분의 장면에서 화질 저하가 없습니다. 이것은 기본 옵션이며 비트 레이트를 줄이기 위해 모든 유형의 장면에서 사용할 수 있습니다.
- **Medium(중간)**: 움직임이 없는 경우와 같이 관심이 낮은 영역에서 노이즈를 줄이고 세부 수준을 약간 낮추어 일부 장면에서 가시적인 효과를 얻을 수 있습니다.
- **High(높음)**: 움직임이 없는 경우와 같이 관심이 낮은 영역에서 노이즈를 줄이고 세부 수준을 낮추어 일부 장면에서 가시적인 효과를 얻을 수 있습니다. 클라우드 연결 장치 및 로컬 스토리지를 사용하는 장치에 이 수준을 권장합니다.
- **Higher(더 높음)**: 움직임이 없는 경우와 같이 관심이 낮은 영역에서 노이즈를 줄이고 세부 수준을 낮추어 일부 장면에서 가시적인 효과를 얻을 수 있습니다.
- **Extreme(최대)**: 대부분의 장면에서 가시적인 효과를 얻을 수 있습니다. 비트 레이트는 가능한 가장 작은 스토리지에 최적화되어 있습니다.

Optimize for storage(스토리지 최적화): 품질을 유지하면서 비트 레이트를 최소화하려면 켭니다. 웹 클라이언트에 표시된 스트림에는 최적화가 적용되지 않습니다. 이는 VMS가 B-프레임을 지원하는 경우에만 사용할 수 있습니다. **Optimize for storage(스토리지 최적화)**를 켜면 **Dynamic GOP (동적 GO)**도 켜집니다.

Dynamic FPS(동적 FPS)(초당 프레임): 장면의 활동 수준에 따라 대역폭이 달라지도록 하려면 켭니다. 더 많은 활동에는 더 많은 대역폭이 필요합니다.

Lower limit(하한): 장면 모션을 기반으로 최소 fps와 스트림 기본 fps 사이의 프레임 레이트를 조정하는 값을 입력합니다. fps가 1 이하로 떨어질 수 있는 모션이 거의 없는 장면에서는 하한을 사용하는 것이 좋습니다.

Dynamic GOP (Group of Pictures)(동적 DOP(group of pictures)): 장면의 활동 수준에 따라 I-프레임 사이의 간격을 동적으로 조정하려면 설정합니다.

Upper limit(상한): 최대 GOP 길이, 즉 두 I-프레임 사이의 최대 P-프레임 수를 입력합니다. I-프레임은 다른 프레임에 종속되지 않는 독립적인 이미지 프레임입니다.

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 켭니다.
  - **Bitrate limit(비트 레이트 제한)**: 비트 레이트 제한을 대상 비트 레이트보다 더 높게 입력하십시오.
- **Maximum(최대)**: 네트워크 대역폭을 기준으로 스트림의 최대 인스턴트 비트 레이트를 설정하려면 선택합니다.
  - **Maximum(최대)**: 최대 비트 레이트를 입력합니다.
- **Variable(가변)**: 장면의 활동 수준에 따라 비트 레이트가 달라지도록 하려면 선택합니다. 더 많은 활동에는 더 많은 대역폭이 필요합니다. 대부분의 상황에서 이 옵션을 사용하는 것이 좋습니다.

방향

Mirror(미러): 이미지를 미러링하려면 켭니다.

오디오

포함: 비디오 스트림에서 오디오를 사용하려면 켭니다.

Source(소스)  : 사용할 오디오 소스를 선택합니다.

Stereo(스테레오)  : 내장 오디오 뿐만 아니라 외부 마이크의 오디오를 포함하려면 켭니다.

오버레이

: 오버레이를 추가하려면 클릭합니다. 드롭다운 목록에서 오버레이 유형을 선택합니다.

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

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

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

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

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

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

프라이버시 마스크

: 새 프라이버시 마스크를 생성하려면 클릭합니다.

Privacy masks(프라이버시 마스크): 모든 프라이버시 마스크의 색상을 변경하거나 모든 프라이버시 마스크를 영구적으로 삭제하려면 클릭합니다.

Mask x(마스크 ×): 마스크의 이름을 바꾸거나, 비활성화하거나, 영구적으로 삭제하려면 클릭합니다.

소통

연락처 목록

문의

연락처 목록을 json 파일로 다운로드하려면 클릭합니다.

연락처 목록(json)을 가져오려면 클릭합니다.

Add contact(연락처 추가): 연락처 목록에 새 연락처를 추가하려면 클릭합니다.

Upload image(이미지 업로드) : 연락처를 나타내는 이미지를 업로드하려면 클릭합니다.

이름: 연락처의 이름을 입력합니다.

성: 연락처의 성을 입력합니다.

Speed dial(단축 다이얼) : 연락처에 사용할 수 있는 단축 다이얼 번호를 입력합니다. 이 번호는 장치에서 연락처를 호출하는 데 사용됩니다.

SIP address(SIP 주소): SIP를 사용하는 경우, 연락처의 IP 주소나 내선 번호를 입력합니다.

: 테스트 전화를 걸려면 클릭하십시오. 전화를 받으면 자동으로 종료됩니다.

SIP account(SIP 계정): SIP를 사용하는 경우, 장치에서 연락처로의 통화에 사용할 SIP 계정을 선택합니다.

Availability(가용성): 연락처의 사용 가능 일정을 선택합니다. **System(시스템) > Events(이벤트) > Schedules(스케줄)**에서 스케줄을 추가하거나 조정할 수 있습니다. 연락처가 없을 때 통화를 시도하면 대체 연락처가 없는 한 통화가 취소됩니다.

Fallback(대체): 해당하는 경우 목록에서 대체 연락처를 선택합니다.

참고: 연락처에 대한 선택적 정보를 추가합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Edit contact(연락처 편집): 연락처 속성을 편집합니다.

Delete contact(연락처 삭제): 연락처를 삭제합니다.

SIP

설정

SIP(Session Initiation Protocol)는 사용자 간의 대화식 통신 세션에 사용됩니다. 세션에 오디오와 영상을 포함할 수 있습니다.

SIP 설정 도우미 클릭하여 SIP를 단계별로 설정 및 구성합니다.

Enable SIP(SIP 활성화): SIP 통화를 시작하고 수신할 수 있도록 하려면 이 옵션을 선택합니다.

Allow incoming calls(수신 콜 허용): 다른 SIP 장치에서 들어오는 콜을 허용하려면 이 옵션을 선택합니다.

콜 처리

- **Calling timeout(콜 시간 제한)**: 아무도 응답하지 않을 경우 통화 시도의 최대 시간을 설정합니다.
- **Incoming call duration(콜 수신 기간)**: 수신 전화를 지속할 수 있는 최대 시간을 설정합니다(최대 10분).
- **End calls after(이후 콜 종료)**: 콜을 지속할 수 있는 최대 시간을 설정합니다(최대 60분). 통화 시간을 제한하지 않으려는 경우 **Infinite call duration(무제한 통화 시간)**을 선택합니다.

포트

포트 번호는 1024 ~ 65535여야 합니다.

- **SIP port(SIP 포트)**: SIP 통신에 사용되는 네트워크 포트입니다. 이 포트를 통한 신호 트래픽은 암호화되지 않습니다. 기본 포트 번호는 5060입니다. 필요한 경우 다른 포트 번호를 입력합니다.
- **TLS port(TLS 포트)**: 암호화된 SIP 통신에 사용되는 네트워크 포트입니다. 이 포트를 통한 신호 트래픽은 TLS(전송 계층 보안)를 사용하여 암호화됩니다. 기본 포트 번호는 5061입니다. 필요한 경우 다른 포트 번호를 입력합니다.
- **RTP start port(RTP 시작 포트)**: SIP 콜에서 첫 번째 RTP 미디어 스트림에 대해 사용되는 네트워크 포트입니다. 기본 시작 포트 번호는 4000입니다. 일부 방화벽은 특정 포트 번호에서 RTP 트래픽을 차단합니다.

NAT 통과 기능

장치가 사설망(LAN)에 있고 해당 네트워크 외부에서 장치를 사용할 수 있도록 하려면 NAT(네트워크 주소 변환) 통과 기능을 사용합니다.

비고

NAT 통과 기능을 사용하려면 라우터에서 지원해야 합니다. 또한 라우터가 UPnP®를 지원해야 합니다.

각 NAT 통과 프로토콜을 개별적으로 사용하거나 네트워크 환경에 따라 다른 조합으로 사용할 수 있습니다.

- **ICE**: ICE(Interactive Connectivity Establishment) 프로토콜을 사용하면 피어 장치 간에 원활한 통신이 이루어지도록 가장 효율적인 경로를 찾기 쉬워집니다. STUN 및 TURN을 활성화해도 ICE 프로토콜에서 가장 효율적인 경로를 찾을 수 있는 기회가 향상됩니다.
- **STUN**: STUN(Session Traversal Utilities for NAT)은 제품이 NAT 또는 방화벽 뒤에 있는지 확인하고 그럴 경우 매핑된 공용 IP 주소와 포트 번호를 가져올 수 있게 해주는 클라이언트-서버 네트워크 프로토콜입니다. IP 주소 같은 STUN 서버 주소를 입력합니다.
- **TURN**: TURN(Traversal Using Relays around NAT)은 NAT 라우터 또는 방화벽 뒤에 있는 장치가 TCP 또는 UDP를 통해 다른 호스트에서 들어오는 데이터를 수신할 수 있도록 해주는 프로토콜입니다. TURN 서버 주소 및 로그인 정보를 입력합니다.

오디오 및 비디오

- **Audio codec priority(오디오 코덱 우선 순위)**: SIP 콜에 대해 원하는 오디오 품질을 가진 하나 이상의 오디오 코덱을 선택합니다. 우선 순위 순서를 변경하려면 끌어서 놓습니다.

비고

콜을 수행할 때 수신자 코덱이 결정되므로 선택한 코덱이 모든 수신자 코덱과 일치해야 합니다.

- **Audio direction(오디오 방향)**: 허용된 음성 안내를 선택합니다.
- **H.264 packetization mode(H.264 패킷화 모드)**: 사용할 패킷화 모드를 선택합니다.
  - **Auto(자동)**: (권장)장치는 사용할 패킷화 모드를 결정합니다.
  - **None(없음)**: 패킷화 모드가 설정되지 않았습니다. 이 모드는 종종 **0** 모드로 해석됩니다.

  - **0**: 비인터리브 모드.
  - **1**: 단일 NAL 유닛 모드.
- **Video direction(비디오 방향)**: 허용된 비디오 길찾기를 선택합니다.
- **Show video in call(통화 중 영상 보기)** : 장치의 디스플레이에 수신되는 비디오 스트림을 표시합니다.

추가

- **UDP-to-TCP switching(UDP와 TCP 간 전환)**: UDP(사용자 데이터그램 프로토콜)에서 TCP(전송 제어 프로토콜)로 전송 프로토콜을 일시적으로 전환하는 호출을 허용하려면 선택합니다. 전환하는 이유는 200바이트 이내 또는 1300바이트 초과 MTU(최대 전송 단위) 요청이 있는 경우 단편화를 방지하기 위해서입니다.
- **Allow via rewrite(다시 쓰기를 통해 허용)**: 라우터의 공용 IP 주소 대신 로컬 IP 주소를 보내려면 선택합니다.
- **Allow contact rewrite(연락처 다시 쓰기 허용)**: 라우터의 공용 IP 주소 대신 로컬 IP 주소를 보내려면 선택합니다.
- **Register with server every(항상 서버에 등록)**: 장치를 기존 SIP 계정에 대한 SIP 서버에 등록할 빈도를 설정합니다.
- **DTMF payload type(DTMF 페이로드 유형)**: DTMF의 기본 페이로드 유형을 변경합니다.
- **Max retransmissions(최대 재전송)**: 장치가 시도를 중지하기 전에 SIP 서버에 연결을 시도하는 최대 횟수를 설정합니다.
- **Seconds until failback(장애 복구까지 남은 초)**: 보조 SIP 서버로 장애 조치한 후 장치가 기본 SIP 서버에 다시 연결을 시도할 때까지의 시간(초)을 설정합니다.

계정

모든 현재 SIP 계정이 **SIP accounts(SIP 계정)** 아래에 나열됩니다. 등록된 계정의 경우 색상이 있는 원으로 상태를 알 수 있습니다.

● 계정이 SIP 서버에 성공적으로 등록되었습니다.

● 계정에 문제가 있습니다. 인증에 실패하거나, 계정 자격 증명이 잘못되었거나, SIP 서버에서 계정을 찾을 수 없기 때문일 수 있습니다.

peer to peer(피어 투 피어, 기본 설정) 계정은 자동으로 생성된 계정입니다. 하나 이상의 다른 계정을 만들고 해당 계정을 기본값으로 설정한 경우 이 계정을 삭제할 수 있습니다. 콜을 시작할 SIP 계정을 지정하지 않고 VAPIX® API(애플리케이션 프로그래밍 인터페이스) 콜을 수행할 경우 항상 기본 계정이 사용됩니다.

Add account(계정 추가): 새 SIP 계정을 생성하려면 클릭합니다.

- **Active(활성화)**: 계정을 사용하려면 선택합니다.
- **Make default(기본값으로 지정)**: 이 계정을 기본 계정으로 지정하려면 선택합니다. 기본 계정이 있어야 하며, 기본 계정은 하나만 둘 수 있습니다.
- **Answer automatically(자동으로 응답)**: 수신 전화에 자동으로 응답하려면 선택합니다.
- **Prioritize IPv6 over IPv4(IPv4보다 IPv6를 우선하도록 설정)** : IPv6 over IPv4 주소의 우선 순위를 지정하려면 선택합니다. 이는 IPv4 및 IPv6 주소 모두에서 확인되는 P2P 계정이나 도메인 이름에 연결할 때 유용합니다. IPv6 주소에 매핑된 도메인 이름에 대해서만 IPv6의 우선 순위를 지정할 수 있습니다.
- **Name(이름)**: 설명이 포함된 이름을 입력합니다. 예를 들어 성과 이름, 역할 또는 위치일 수 있습니다. 이름이 중복되었습니다.
- **User ID(사용자 ID)**: 장치에 할당된 고유한 내선 또는 전화 번호를 입력합니다.
- **Peer-to-peer(피어 투 피어)**: 로컬 네트워크에서 다른 SIP 장치를 직접 호출하는 데 사용됩니다.
- **Registered(등록됨)**: SIP 서버를 통해 로컬 네트워크 외부의 SIP 장치를 호출하는 데 사용됩니다.
- **Domain(도메인)**: 사용 가능할 경우 공용 도메인 이름을 입력합니다. 도메인 이름은 다른 계정을 호출 할 때 SIP 주소의 일부로 표시됩니다.
- **Password(패스워드)**: SIP 서버에 대해 인증하기 위한 SIP 계정과 연결된 패스워드를 입력합니다.
- **Authentication ID(인증 ID)**: SIP 서버에 대해 인증하기 위해 사용되는 인증 ID를 입력합니다. 인증 ID가 사용자 ID와 같은 경우 인증 ID를 입력할 필요가 없습니다.
- **Caller-ID(발신자 ID)**: Axis 장치에서 보내는 통화의 수신자에게 표시되는 이름입니다.
- **Registrar(등록자)**: 등록자의 IP 주소를 입력합니다.
- **Transport mode(전송 모드)**: 계정의 SIP 전송 모드를 선택합니다(UPD, TCP 또는 TLS).
- **TLS version(TLS 버전)**(전송 모드 TLS만): 사용할 TLS 버전을 선택합니다. 버전 **v1.2** 및 **v1.3**이 가장 안전합니다. **Automatic(자동)**은 시스템에서 처리할 수 있는 가장 안전한 버전을 선택합니다.
- **Media encryption(미디어 암호화)**(전송 모드 TLS만): SIP 콜에서 미디어(오디오 및 영상)에 대한 암호화 유형을 선택합니다.
- **Certificate**(only with transport mode TLS)(인증서(전송 모드 TLS만)): 인증서를 선택합니다.
- **Verify server certificate**(only with transport mode TLS)(서버 인증서 확인(전송 모드 TLS만)): 서버 인증서를 확인하려면 선택합니다.
- **Secondary SIP server(보조 SIP 서버)**: 기본 SIP 서버에 등록이 실패한 경우 장치가 보조 SIP 서버에 등록을 시도하도록 하려면 켭니다.

- **SIP secure(SIP 보안)**: SIPS(Secure Session Initiation Protocol)를 사용하려면 선택합니다. SIPS는 TLS 전송 모드를 사용하여 트래픽을 암호화합니다.
- **프록시**
  - **Proxy(프록시)**: 프록시를 추가하려면 클릭합니다.
  - **Prioritize(우선 순위 지정)**: 두 개 이상의 프록시를 추가한 경우에 프록시의 우선 순위를 지정하려면 클릭합니다.
  - **Server address(서버 주소)**: SIP 프록시 서버의 IP 주소를 입력합니다.
  - **Username(사용자 이름)**: 필요한 경우 SIP 프록시 서버의 사용자 이름을 입력합니다.
  - **Password(패스워드)**: 필요한 경우 SIP 프록시 서버의 패스워드를 입력합니다.
- **비디오**
  - **View area(보기 영역)**: 화상 통화에 사용할 보기 영역을 선택합니다. None(없음)을 선택한 경우 원본 보기가 사용됩니다.
  - **Resolution(해상도)**: 화상 통화에 사용할 해상도를 선택합니다. 해상도는 필요한 대역폭에 영향을 줍니다.
  - **Frame rate(프레임 레이트)**: 화상 통화의 초당 프레임 수를 선택합니다. 프레임 레이트는 필요한 대역폭에 영향을 줍니다.
  - **H.264 profile(H.264 프로파일)**: 영상 통화에 사용할 프로파일을 선택합니다.

DTMF

Add sequence(시퀀스 추가): 새 DTMF(Dual-Tone Multifrequency) 시퀀스를 생성하려면 클릭합니다. 터치 톤에 의해 활성화되는 룰을 생성하려면 **Events > Rules(이벤트 > 룰)**로 이동합니다.

Sequence(시퀀스): 룰을 활성화할 문자를 입력합니다. 허용되는 문자는 0–9, A-D, #, *입니다.

Description(설명): 시퀀스로 트리거할 액션에 대한 설명을 입력합니다.

Accounts(계정): DTMF 시퀀스를 사용할 계정을 선택합니다. **peer-to-peer(피어 투 피어)**를 선택하는 경우 모든 피어 투 피어 계정은 동일한 DTMF 시퀀스를 공유합니다.

프로토콜

각 계정에 사용할 프로토콜을 선택합니다. 모든 피어 투 피어 계정은 동일한 프로토콜 설정을 공유합니다.

Use RTP (RFC2833)(RTP(RFC2833) 사용): RTP 패킷에서 DTMF(Dual-Tone Multifrequency) 신호, 다른 톤 신호 및 전화 이벤트를 허용하려면 켭니다.

Use SIP INFO (RFC2976)(SIP INFO(RFC2976) 사용): SIP 프로토콜에 INFO 메서드를 포함하려면 켭니다. INFO 메서드는 일반적으로 세션과 관련된 선택적 애플리케이션 계층 정보를 추가합니다.

테스트 콜

SIP account(SIP 계정): 테스트 전화를 걸 계정을 선택합니다.

SIP address(SIP 주소): SIP 주소를 입력하고 을 클릭하여 테스트 전화를 걸어 계정이 작동하는지 확인합니다.

액세스 목록

Use access list(액세스 목록 사용): 장치에 전화를 걸 수 있는 사람을 제한하려면 켭니다.

Policy(정책):
- **Allow(허용)**: 액세스 목록에 있는 소스로부터만 수신 전화를 허용하려면 선택합니다.
- **Block(차단)**: 액세스 목록에 있는 소스로부터 수신 전화를 차단하려면 선택합니다.

Add source(소스 추가): 액세스 목록에 새 항목을 생성하려면 클릭합니다.

SIP source(SIP 소스): 소스의 발신자 ID 또는 SIP 서버 주소를 입력합니다.

콜

통화 버튼

Use call button(통화 버튼 사용): 통화 버튼을 사용하려면 켭니다.

Button functionality during a call(통화 중 버튼 기능): 장치에서 통화가 시작된 후 통화 버튼의 기능을 선택합니다.

- **End the call(통화 종료)**: 방문자가 발신 통화 중에 통화 버튼을 누르면 통화가 종료됩니다. 방문자가 언제든지 통화를 종료할 수 있도록 하려면 이 옵션을 사용합니다.
- **No functionality until the call has ended(통화가 종료될 때까지 기능 없음)**: 방문자가 발신 통화 중에 통화 버튼을 누르면 아무 일도 일어나지 않습니다. 방문자가 통화를 종료하지 못하도록 하려면 이 옵션을 사용합니다.
- **Delay before you can end the call(통화 종료 전 지연)**: 방문자가 통화를 시작한 후 **Delay (seconds)(지연(초))**에 설정된 시간 내에 통화 버튼을 누르면 아무 일도 일어나지 않습니다. 지연 시간이 지나면 통화 버튼을 누르면 통화가 종료됩니다. 이 옵션을 사용하면 방문자가 두 번 눌러 실수로 통화를 종료하는 것을 방지할 수 있습니다.
  - **Delay (seconds)(지연(초))**: 통화 버튼을 두 번째로 눌러 통화를 종료하기까지 필요한 시간을 입력합니다.

Standby light(대기 표시등): 통화 버튼 주변의 내장 표시등에 대한 옵션을 선택합니다.

- **Auto(자동)** : 이 장치는 주변 조명에 따라 내장 표시등을 켜고 끕니다.
- **On(켜기)**: 장치가 대기 모드에 있을 때 내장 표시등이 항상 켜져 있습니다.
- **Off(끄기)**: 장치가 대기 모드에 있을 때 내장 표시등이 항상 꺼져 있습니다.

Recipients(수신자): 누군가가 통화 버튼을 누를 때 전화를 걸 연락처를 하나 이상 선택하거나 생성합니다. 두 명 이상의 수신자를 추가하면 동시에 모든 수신자에게 전화가 걸립니다. SIP 통화 수신자는 최대 6명이며, VMS 통화 수신자는 무제한입니다.

Fallback(대체): 수신자가 회신하지 않는 경우를 대비하여 목록에서 대체 연락처를 추가합니다.

일반사항

오디오

비고
- 선택한 오디오 클립은 전화가 걸려올 때만 재생됩니다.
- 진행 중인 통화 중에 오디오 클립이나 게인을 변경하면, 다음 통화까지 적용되지 않습니다.

Ringtone(벨소리): 누군가 장치에 전화를 걸 때 재생할 오디오 클립을 선택합니다. 슬라이더를 사용하여 게인을 조절합니다.

Ringback tone(통화 연결음): 누군가 장치에서 전화를 걸 때 재생할 오디오 클립을 선택합니다. 슬라이더를 사용하여 게인을 조절합니다.

VMS 통화

VMS 통화

Allow calls in the video management software (VMS)(비디오 매니지먼트 소프트웨어(VMS)에서 통화 허용): 장치에서 VMS로 통화하도록 허용하려면 선택합니다. SIP가 꺼져 있어도 VMS 통화를 할 수 있습니다.

Call timeout(콜 시간 초과): 아무도 응답하지 않을 경우 통화 시도의 최대 시간을 설정합니다.

분석 애플리케이션

AXIS Object Analytics

시작: AXIS Object Analytics를 시작하려면 클릭합니다. 백그라운드에서 애플리케이션이 실행되며 애플리케이션의 현재 설정에 따라 이벤트에 대한 룰을 생성할 수 있습니다.

Open(열기): AXIS Object Analytics를 열려면 클릭합니다. 새 브라우저 탭에서 애플리케이션이 열리고, 설정을 구성할 수 있습니다.

- **Not installed(설치되지 않음)**: 이 장치에 AXIS Object Analytics가 설치되지 않았습니다. 애플리케이션의 최신 버전을 사용하려면 AXIS OS를 최신 버전으로 업그레이드하십시오.

메타데이터 시각화

카메라는 움직이는 객체를 감지하고 객체 유형을 기준으로 분류합니다. 보기에서 분류된 개체에는 할당된 ID와 함께 주위에 색상이 지정된 바운딩 박스가 있습니다.

Id: 식별된 객체 및 유형에 대한 고유 식별 번호입니다. 목록과 보기 모두에 이 번호가 표시됩니다.

Type(유형): 움직이는 객체를 사람, 안면, 승용차, 버스, 트럭, 자전거 또는 번호판으로 분류합니다. 바운딩 박스의 색상은 유형 분류에 따라 달라집니다.

신뢰도: 막대는 객체 유형 분류에 대한 신뢰 수준을 표시합니다.

메타데이터 구성

RTSP 메타데이터 생성자

메타데이터를 스트리밍하는 앱과 해당 앱이 사용하는 채널을 나열합니다.

비고

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

Producer(생산자): 메타데이터를 생성하는 앱입니다. 앱 아래에는 앱이 장치에서 스트리밍하는 메타데이터 유형의 목록이 있습니다.

Channel(채널): 앱이 사용하는 채널입니다. 메타데이터 스트림을 활성화하려면 선택합니다. 호환성 또는 리소스 관리 상의 이유로 선택을 취소합니다.

리더

연결

외부 리더(입력)

Use external OSDP reader(외부 OSDP 리더 사용): 외부 리더와 함께 장치를 사용하려면 켭니다. 리더를 리더 커넥터(IO1, IO2, 12V 및 GND)에 연결합니다.

Status(상태):

- **Connected(연결됨)**: 장치가 활성 외부 리더에 연결되어 있습니다.
- **Connecting(연결 중)**: 장치가 외부 리더에 연결을 시도하고 있습니다.
- **Not connected(연결되지 않음)**: OSDP가 꺼져 있습니다.

리더 프로토콜

Reader protocol type(리더 프로토콜 유형): 리더 기능에 사용할 프로토콜을 선택합니다.

- **VAPIX reader(VAPIX 리더)**: Axis 도어 컨트롤러에만 사용할 수 있습니다.
  - **Protocol(프로토콜)**: **HTTPS** 또는 **HTTP**를 선택합니다.
  - **Door controller address(도어 컨트롤러 주소)**: 도어 컨트롤러의 IP 주소를 입력합니다.
  - **User name(사용자 이름)**: 도어 컨트롤러의 사용자 이름을 입력합니다.
  - **Password(패스워드)**: 도어 컨트롤러의 패스워드를 입력합니다.
  - **Connect(연결)**: 도어 컨트롤러에 연결하려면 클릭합니다.
  - **Select reader(리더 선택)**: 알맞은 도어에 대한 입구 리더를 선택합니다.
- **OSDP**:
  - **OSDP address(OSDP 주소)**: OSDP 리더 주소를 입력합니다. 0은 단일 리더의 기본 주소이자 가장 일반적인 주소입니다.
- **Wiegand** :
  - **Beeper(알람음)**: 신호음 입력을 활성화하려면 켭니다.
  - **Input for beeper(신호기 입력)**: 신호음에 사용되는 I/O 포트를 선택합니다.
  - **Input used for LED control(LED 제어에 사용되는 입력)**: 장치에서 LED 피드백을 제어하는 데 사용할 I/O 포트 수를 선택합니다.
  - **Input for LED1/LED2(LED1/LED2용 입력)**: LED 입력에 사용할 I/O 포트를 선택합니다.
  - **Idle color(유휴 색상)**: LED를 제어하는 데 사용되는 I/O 포트가 없는 경우 카드 리더 표시기 스트라이프에 표시할 정적 색상을 선택할 수 있습니다.
  - **Color for state low/high(상태 낮음/높음의 색상)**: 하나의 I/O 포트가 LED 제어에 사용되는 경우 상태 낮음 및 상태 높음을 각각 표시할 색상을 선택합니다.
  - **Idle color/LED1 color/LED2 color/LED1 + LED2 color(유휴 색상/LED1 색상/LED2 색상/LED1+LED2 색상)**: 두 개의 I/O 포트가 LED 제어에 사용되는 경우 유휴, LED1, LED2 및 LED1 + LED2에 각각 표시할 색상을 선택합니다.
  - **Keypress format(키 누르기 형식)**: 핀이 접근 제어 장치로 전송될 때 핀 형식을 지정하는 방법을 선택합니다.
    - **FourBit**: PIN `1234`는 0x1 0x2 0x3 0x4로 엔코딩되어 전송됩니다. 이는 기본적이고 가장 일반적인 동작입니다.
    - **EightBitZeroPadded**: PIN `1234`는 0x01 0x02 0x03 0x04로 엔코딩되어 전송됩니다.
    - **EightBitInvertPadded**: PIN `1234`는 0xE1 0xD2 0xC3 0xB4로 엔코딩되어 전송됩니다.
    - **Wiegand26**: PIN은 8비트 시설 코드와 16비트 ID를 사용하여 Wiegand26 형식으로 인코딩됩니다.
    - **Wiegand34**: PIN은 16비트 시설 코드와 16비트 ID를 사용하여 Wiegand34 형식으로 인코딩됩니다.
    - **Wiegand37**: PIN은 35비트 ID를 사용하여 Wiegand37 형식(H10302)으로 인코딩됩니다.
    - **Wiegand37FacilityCode**: PIN은 16비트 시설 코드와 19비트 ID를 사용하여 Wiegand37 형식(H10304)으로 인코딩됩니다.
  - **Facility code(시설 코드)**: 보낼 시설 코드를 입력하십시오. 이 옵션은 일부 키 누르기 형식에서만 사용할 수 있습니다.

출력 형식

Select data format(데이터 형식 선택): 접근 제어 장치에 카드 데이터를 보낼 형식을 선택합니다.

- **Raw(원시)**: 카드 데이터를 그대로 전송합니다.
- **Wiegand26**: 카드 데이터를 8비트 시설 코드와 16비트 ID를 사용하여 Wiegand26 형식으로 인코딩합니다.
- **Wiegand34**: 카드 데이터를 16비트 시설 코드와 16비트 ID를 사용하여 Wiegand34 형식으로 인코딩합니다.
- **Wiegand37**: 카드 데이터를 35비트 ID를 사용하여 Wiegand37 형식(H10302)으로 인코딩합니다.
- **Wiegand37FacilityCode**: 카드 데이터를 16비트 시설 코드와 19비트 ID를 사용하여 Wiegand37 형식(H10304)으로 인코딩합니다.
- **Custom(사용자 지정)**: 자신의 서식을 정의하십시오.

Facility code override mode(시설 코드 재정의 모드): 시설 코드를 재정의하는 옵션을 선택합니다.

- **Auto(자동)**: 시설 코드를 무시하지 않고 입력 데이터 자동 감지에서 시설 코드를 생성합니다. 카드의 원래 시설 코드를 사용하거나 카드 번호의 초과 비트에서 위조합니다.
- **Optional(옵션)**: 입력 데이터의 시설 코드를 사용하거나 구성된 옵션 값으로 재정의합니다.
- **Override(무시)**: 항상 지정된 시설 코드로 재정의합니다.

핀

핀 설정은 접근 제어 장치에 구성된 설정과 일치해야 합니다.

Length (0-32)(길이(0-32)): PIN의 자릿수를 입력합니다. 사용자가 리더를 사용할 때 PIN을 사용할 필요가 없는 경우 길이를 0으로 설정합니다.

Timeout (seconds, 3-50)(초과 시간(초, 3-50)): PIN을 받지 못한 경우 장치가 유휴 모드로 돌아가기 전에 경과해야 하는 시간(초)을 입력합니다.

엔트리 목록

항목 목록을 사용하면 자격 증명 홀더가 자신의 카드 또는 핀으로 도어 열기와 같은 여러 작업 실행하도록 장치를 설정할 수 있습니다. 장치에 로컬로 자격 증명을 저장합니다. 이 기능과 외부 도어 컨트롤러를 결합할 수도 있습니다.

자격 증명 홀더

항목 목록 사용: 항목 목록 기능을 사용하려면 켭니다.

연결된 도어 컨트롤러 사용: 장치가 이미 도어 컨트롤러에 연결되어 있으면 켭니다. 누군가 항목 목록에 없는 자격 증명을 제시하면 연결된 도어 컨트롤러로 요청을 보냅니다. 항목 목록에서 사용할 수 있는 자격 증명은 보내지 않습니다.

자격 증명 홀더 추가: 새 자격 증명 홀더를 추가하려면 클릭합니다.

이름: 이름을 입력하세요.

성: 성을 입력합니다.

자격 증명 유형

- **핀**:
  - **PIN**: 고유한 PIN을 입력하거나 **Generate(생성)**를 클릭하여 자동으로 생성합니다.
- **카드**:
  - **UID**: 카드의 UID와 비트 길이를 입력하거나 **Get latest(최신 항목 가져오기)**를 클릭하여 마지막에 긁은 카드에서 데이터를 가져옵니다.

이벤트 조건 자격 증명 홀더가 자격 증명 사용 시 트리거할 조건을 하나 이상 선택합니다. 결과 작업을 설정하려면 **시스템 > 이벤트**로 이동하여 여기에서 선택한 것과 동일한 조건으로 룰을 생성합니다.

시작: 자격 증명을 즉시 활성화하려면 **현재 장치 시간**을 선택합니다. 자격 증명을 활성화할 시기를 지정하려면 선택을 취소합니다.

만료:

- **종료일 없음**: 자격 증명은 무기한으로 유효합니다.
- **종료일**: 자격 증명이 무효화되는 날짜와 시간을 지정합니다.
- **횟수**: 자격 증명 홀더가 자격 증명을 얼마나 많이 사용할 수 있는지 지정합니다. 자격 증명을 사용할수록 필드의 값이 줄어들어 남은 사용 횟수를 표시합니다.

참고: 선택적 정보를 입력합니다.

정지: 일시적으로 자격 증명을 무효화하려면 선택합니다.

이벤트 로그

이벤트 로그에는 엔트리 목록 이벤트 목록이 표시됩니다. 로그 파일의 최대 크기는 2MB이며, 이는 약 6000개의 이벤트에 해당합니다.

Export all(모두 내보내기): 목록의 모든 이벤트를 내보내려면 클릭합니다. 일부만 내보내려면 관심 있는 이벤트를 선택합니다. 이벤트는 CSV 파일로 내보내집니다.

Filter(필터): 특정 시간대에 발생한 이벤트를 표시하려면 클릭합니다.

🔍: 목록에서 일치하는 모든 콘텐츠를 검색하려면 입력합니다.

오디오

장치 설정

입력: 오디오 입력을 켜거나 끕니다. 입력 유형을 표시합니다.

Input type(입력 유형) : 예를 들어, 내부 마이크 또는 라인 입력인 경우 입력 유형을 선택합니다.

Power type(전원 유형) : 입력에 대한 전원 유형을 선택합니다.

Apply changes(변경 사항 적용) : 선택 사항을 적용합니다.

Noise cancellation(노이즈 제거): 배경 노이즈를 제거하여 오디오 품질을 향상시키려면 켭니다.

Echo cancellation(에코 제거) : 양방향 통신 중에 에코를 제거하려면 켭니다.

Separate gain controls(별도 게인 제어) : 다른 입력 유형에 대해 개별적으로 게인을 조정하려면 켭니다.

Automatic gain control(자동 게인 제어) : 소리의 변화에 따라 게인을 동적으로 조정하려면 켜십시오.

Gain(게인): 슬라이더를 사용하여 게인을 변경합니다. 마이크 아이콘을 클릭하여 음소거 또는 음소거 해제합니다.

출력: 출력 유형을 표시합니다.

Gain(게인): 슬라이더를 사용하여 게인을 변경합니다. 스피커 아이콘을 클릭하여 음소거 또는 음소거 해제합니다.

Automatic volume control(자동 볼륨 조절) : 켜면 장치가 주변 노이즈 수준에 따라 자동으로 동적으로 게인을 조정합니다. 자동 볼륨 조절은 라인 및 텔레코일을 포함한 모든 오디오 출력에 영향을 줍니다.

스트림

Echo cancellation(에코 제거): 양방향 통신 중에 에코를 제거하려면 켭니다.

오디오 클립

Add clip(클립 추가): 새 오디오 클립을 추가합니다. .au, .mp3, .opus, .vorbis, .wav 파일을 사용할 수 있습니다.

오디오 클립을 재생합니다.

오디오 클립 재생을 중지합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Rename(이름 바꾸기)**: 오디오 클립 이름을 변경합니다.
- **Create link(링크 생성)**: 사용할 때 장치에서 오디오 클립을 재생하는 URL을 생성합니다. 클립을 재생할 볼륨과 횟수를 지정합니다.
- **Download(다운로드)**: 오디오 클립을 컴퓨터에 다운로드합니다.
- **Delete(삭제)**: 장치에서 오디오 클립을 삭제합니다.

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

시스템

시간과 장소

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

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

- **Automatic date and time (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.

구성 확인

대화형 장치 이미지: 이미지의 버튼을 클릭하여 실제 키 누름을 시뮬레이션합니다. 이를 통해 장치에 물리적으로 액세스하지 않고도 구성을 시도하거나 하드웨어 문제를 해결할 수 있습니다.

Latest credentials(최근 자격 증명) : 마지막으로 등록된 자격 증명에 대한 정보를 표시합니다.

최신 자격 증명 데이터를 표시합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Reverse UID(UID 반전)**: UID의 byte 순서를 반전시킵니다.
- **Revert UID(UID 되돌림)**: UID의 byte 순서를 원래 순서로 되돌립니다.
- **Copy to clipboard(클립보드에 복사)**: UID를 복사합니다.

Check credentials(자격 증명 확인) : UID 또는 핀을 입력하고 제출하여 자격 증명을 확인합니다. 시스템은 장치에서 자격 증명을 사용한 것과 동일한 방식으로 응답합니다. UID와 핀이 모두 필요한 경우 UID를 입력하는 것으로 시작합니다.

네트워크

IPv4

Assign IPv4 automatically(IPv4 자동 할당): 네트워크 라우터가 장치에 IP 주소를 자동으로 할당하도록 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-services*를 참조하십시오.

Allow O3C(O3C 허용):

- **One-click(원클릭)**: 기본 옵션입니다. O3C에 연결하려면 장치의 제어 버튼을 누릅니다. 장치 모델에 따라 상태 LED가 깜박일 때까지 버튼을 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 켜십시오. 장치는 트랩을 사용하여 중요한 이벤트 또는 상태 변경에 대한 메시지를 관리 시스템에 보냅니다. 웹 인터페이스에서 SNMP v1 및 v2c에 대한 트랩을 설정할 수 있습니다. SNMP v3으로 변경하거나 SNMP를 끄면 트랩이 자동으로 꺼집니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **Trap address(트랩 주소)**: 관리 서버의 IP 주소 또는 호스트 이름을 입력하십시오.
  - **Trap community(트랩 커뮤니티)**: 장치가 관리 시스템에 트랩 메시지를 보낼 때 사용할 커뮤니티를 입력합니다.
  - **Traps(트랩)**:
    - **Cold start(콜드 부팅)**: 장치가 시작될 때 트랩 메시지를 보냅니다.
    - **Link up(링크 업)**: 링크가 다운에서 업으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Link down(링크 다운)**: 링크가 업에서 다운으로 변경된 경우 트랩 메시지를 보냅니다.
    - **Authentication failed(인증 실패)**: 인증 시도가 실패하면 트랩 메시지를 보냅니다.

비고

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

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

보안

인증서

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

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

지원되는 형식은 다음과 같습니다.

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

중요 사항

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

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

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

상황에 맞는 메뉴에는 다음이 포함됩니다.

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

Secure keystore(보안 키 저장소):

- **Trusted Execution Environment (SoC TEE)**: 보안 키 저장소로 SoC TEE를 사용하려면 선택합니다.
- **Secure element(보안 요소)(CC EAL6+)**: 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.

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 켭니다.

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)**을 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 길이여야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 패스워드에 사용할 수 있습니다.

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

Privileges(권한):

- **Administrator(관리자)**: 모든 설정에 완전히 액세스합니다. 관리자는 다른 계정을 추가, 업데이트 및 제거할 수 있습니다.
- **Operator(운영자)**: 다음을 제외한 모든 설정에 액세스할 수 있습니다.
  - 모든 **System(시스템)** 설정
- **Viewer(뷰어)**: 다음에 대한 접근 권한이 있습니다.
  - 비디오 스트림의 스냅샷을 보고 찍습니다.
  - 녹화를 시청하고 내보냅니다.
  - 팬, 틸트 및 줌; **PTZ 계정** 액세스 포함.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Update account(계정 업데이트): 계정 속성을 편집합니다.

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

익명의 액세스

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

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

SSH 계정

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

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

Account(계정): 고유한 계정 이름을 입력합니다.

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

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

설명: 설명을 입력합니다(옵션).

상황에 맞는 메뉴에는 다음이 포함됩니다.

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

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

가상 호스트

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

활성화: 이 가상 호스트를 사용하려면 선택합니다.

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

Port(포트): 서버가 연결된 포트를 입력합니다.

Type(유형): 사용할 인증 유형을 선택합니다. **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 형식이어야 함

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

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

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

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

Scopes(범위): 토큰의 일부가 될 수 있는 선택적 범위입니다.

Client secret(클라이언트 비밀): OpenID 패스워드 입력

Save(저장): OpenID 값을 저장하려면 클릭합니다.

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

이벤트

룰

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

비고

최대 256개의 액션 룰을 생성할 수 있습니다.

Add a rule(룰 추가): 룰을 생성합니다.

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 켜십시오(예: pop.gmail.com).

비고

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

- **TCP**
  - **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 베이스*에서 MQTT에 대해 자세히 알아볼 수 있습니다.

ALPN

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

MQTT 클라이언트

Connect(연결): MQTT 클라이언트를 켜거나 끕니다.

Status(상태): MQTT 클라이언트의 현재 상태를 표시합니다.

브로커

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 제한를 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 끄십시오.

Topic(주제): 기본 메시지의 주제를 입력합니다.

Payload(페이로드): 기본 메시지의 내용을 입력합니다.

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

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

MQTT 발행

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

Include 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 켭니다.

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

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

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 켭니다. 쓰기 방지 네트워크 공유는 포맷할 수 없습니다.

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

도구

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

Use tool(도구 사용): 클릭하여 선택한 도구를 활성화합니다.

온보드 스토리지

중요 사항

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

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

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

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

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

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

도구

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

Use tool(도구 사용): 클릭하여 선택한 도구를 활성화합니다.

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

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.com*의 Axis 개발자 커뮤니티를 참조하십시오

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

Account(계정): 고유한 계정 이름을 입력합니다.

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

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

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

카메라 탬퍼링

카메라 탬퍼링 감지기는 렌즈가 덮여 있거나 분무되거나 심하게 포커스가 흐려져 **Trigger delay(트리거 지연)** 시간이 경과한 경우와 같이 장면이 바뀌면 알람을 생성합니다. 탬퍼링 감지기는 카메라가 10초 이상 움직이지 않은 경우에만 활성화됩니다. 이 기간 동안 감지기는 현재 이미지에서 탬퍼링을 감지하기 위해 비교로 사용할 장면 모델을 설정합니다. 장면 모델을 적절하게 설정하려면 카메라의 포커스가 맞게 설정되어 있는지, 조명 조건이 올바르게 설정되어 있는지, 카메라가 빈 벽과 같이 윤곽이 없는 장면을 가리키고 있지 않은지 확인하십시오. 카메라 탬퍼링은 액션을 트리거할 조건으로 사용할 수도 있습니다.

Trigger delay(트리거 지연): 알람이 트리거되기 전에 탬퍼링이 활성화되어야 하는 최소 시간을 입력합니다. 이렇게 하면 이미지에 영향을 주는 알려진 조건에 대해 잘못된 알람을 방지할 수 있습니다.

Trigger on dark images(이미지가 어두울 때 트리거): 예를 들어 조명 조건이 변경되었을 때 비슷한 수준으로 이미지가 어두워져 다른 상황과 이벤트를 구분할 수 없기 때문에 카메라 렌즈에 분무될 때 알람이 표시되기 매우 어렵습니다. 이 매개변수가 켜면 이미지가 어두워지는 모든 경우에 대해 알람이 생성됩니다. 꺼져 있으면 이미지가 어두워질 때 장치에서 알람을 생성하지 않습니다.

비고

정적이고 혼잡하지 않은 장면에서의 탬퍼링 감지.

오디오 감지

각 오디오 입력에 이 설정을 사용할 수 있습니다.

Sound level(사운드 수준): 사운드 수준은 0~100 값으로 설정할 수 있습니다. 여기서 0은 가장 민감한 수준이며 100은 가장 민감하지 않은 수준입니다. 사운드 수준을 설정할 때, 움직임 표시기를 가이드로 사용하십시오. 이벤트를 생성할 때 사운드 수준을 조건으로 사용할 수 있습니다. 사운드 수준이 설정 값 이상으로 올라가거나 내려가거나 설정 값을 초과하면 작업을 트리거하도록 선택할 수 있습니다.

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 프로그래밍 인터페이스 또는 웹 인터페이스를 통해 연결된 장치를 활성화할 수 있습니다.

포트

Name(이름): 포트 이름을 바꾸려면 텍스트를 편집합니다.

Usage(용도): 릴레이 포트의 기본 옵션은 **Door(도어)**입니다. 표시기 아이콘이 있는 장치의 경우  상태가 변경되고 도어가 잠금 해제되면 녹색으로 변합니다. 도어가 아닌 다른 용도로 릴레이를 사용하고 상태가 변경될 때 아이콘이 켜지지 않도록 하려면 포트에 대한 다른 옵션 중 하나를 선택할 수 있습니다.

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.

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.com*에서 백서 "Axis Edge Vault"를 참조하십시오.

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

업그레이드할 때 다음 세 가지 옵션 중에서 선택할 수 있습니다.

- **Standard upgrade(표준 업그레이드)**: 새 AXIS OS 버전으로 업그레이드합니다.
- **Factory default(공장 출하 시 기본값)**: 업그레이드하고 모든 설정을 공장 출하 시 기본값으로 되돌리십시오. 이 옵션을 선택하면 업그레이드 후에 이전 AXIS OS 버전으로 되돌릴 수 없습니다.
- **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.

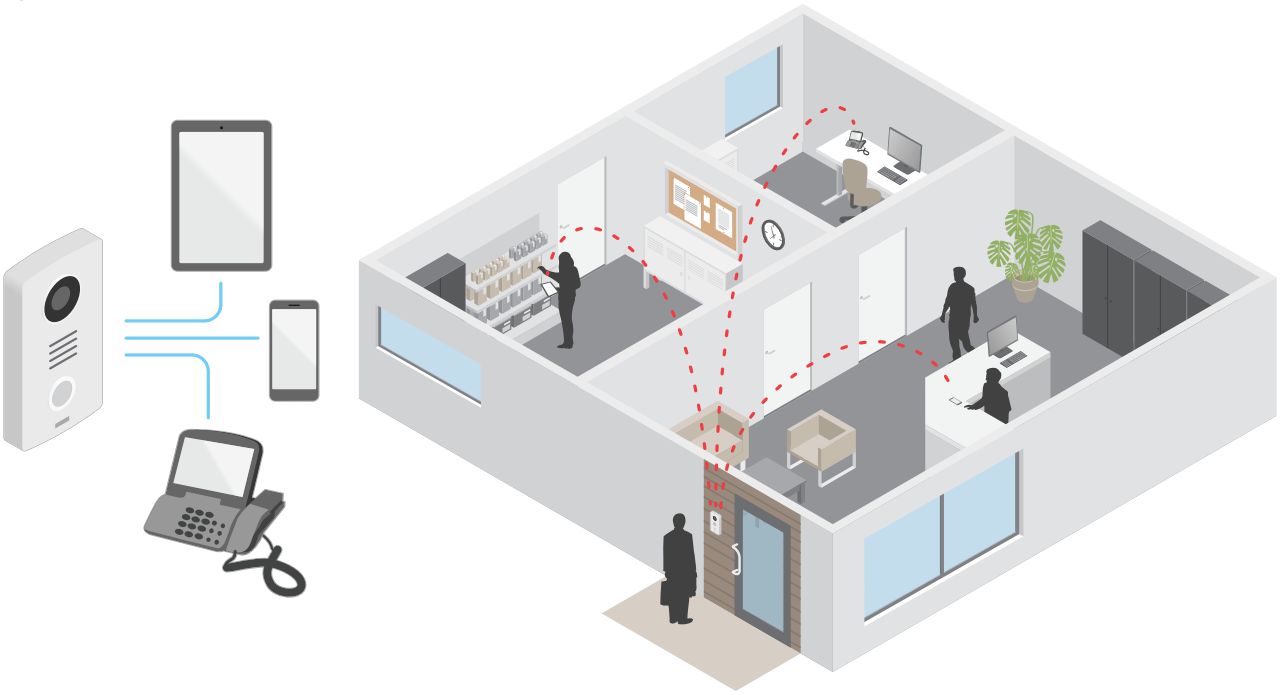
상세 정보

VoIP(Voice over IP)

VoIP(Voice over IP)는 IP 네트워크(예: 인터넷)를 통한 음성 통신 및 멀티미디어 세션을 활성화하는 기술 그룹입니다. 일반적인 전화 통화에서는 PSTN(공중 교환 전화망, Public Switched Telephone Network)에서 회로 전송을 통해 아날로그 신호가 전달됩니다. VoIP 콜에서는 로컬 IP 네트워크나 인터넷을 통해 데이터 패킷으로 보낼 수 있도록 아날로그 신호가 디지털 신호로 바뀝니다.

Axis 제품에서 VoIP는 SIP(Session Initiation Protocol) 및 DTMF(Dual-Tone Multi-Frequency) 신호를 통해 활성화됩니다.

예:



Axis 인터콤에서 통화 버튼을 누르면 사전 정의된 수신자 한 명 이상과 통화가 시작됩니다. 수신자가 응답하면 통화가 됩니다. 음성 및 영상이 VoIP 기술을 통해 전송됩니다.

SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)는 VoIP 호출을 설정, 유지 및 종료하는 데 사용됩니다. 둘 이상의 파티 즉, SIP 사용자 에이전트 간에 콜을 수행할 수 있습니다. SIP 콜을 수행하려면 SIP 전화기, 소프트폰 또는 SIP 지원 Axis 장치 등을 사용할 수 있습니다.

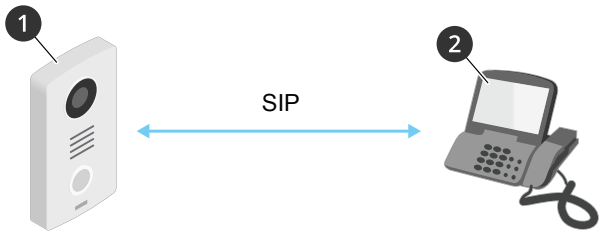
RTP(Real-Time Transport Protocol) 등의 전송 프로토콜을 사용하여 실제 오디오나 비디오가 SIP 사용자 에이전트 간에 교환됩니다.

피어 투 피어 설정을 사용하여 로컬 네트워크에서 또는 PBX를 사용하여 네트워크 간에 콜을 수행할 수 있습니다.

Peer-to-peer SIP(피어 투 피어 SIP)

가장 기본적인 유형의 SIP 통신은 둘 이상의 SIP 사용자 에이전트 간에 직접 이루어집니다. 이 통신을 peer-to-peer SIP(피어 투 피어 SIP)라고 합니다. 로컬 네트워크에서 이 통신이 이루어지면 사용자 에이전트의 SIP 주소만 있으면 됩니다. 이 경우 일반적인 SIP 주소는 `sip:<local-ip>`입니다.

예:



1 사용자 에이전트 A - 인터콤. SIP 주소: sip:192.168.1.101
2 사용자 에이전트 B - SIP 지원 전화기. SIP 주소: sip:192.168.1.100

피어 투 피어 SIP 설정을 사용하는 동일한 네트워크의 SIP 지원 전화기 등을 호출하도록 Axis 인터콤을 설정할 수 있습니다.

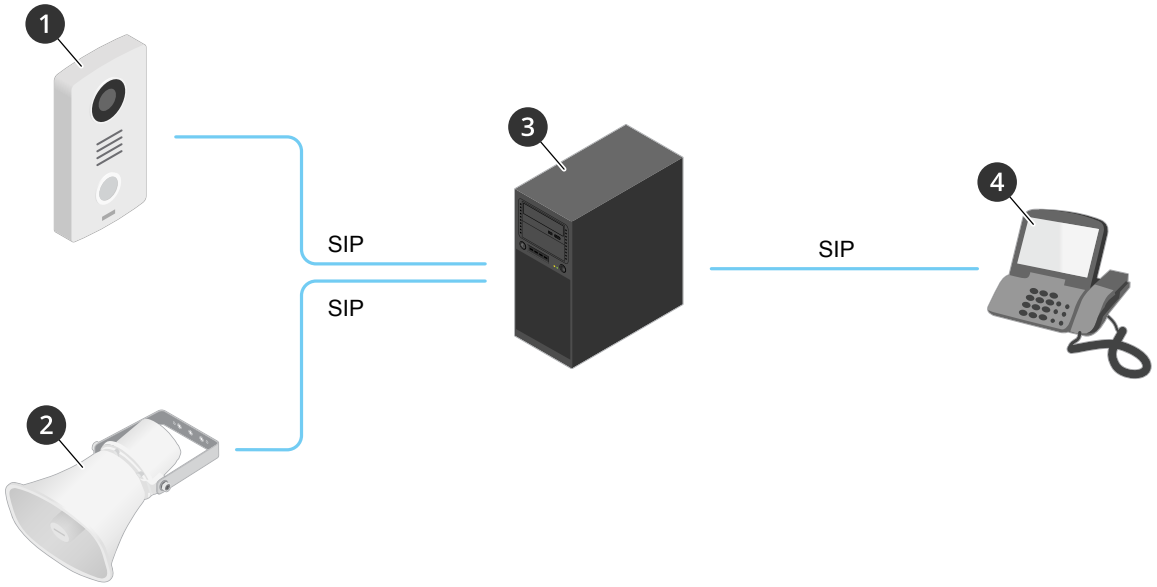
PBX(Private Branch Exchange)

로컬 IP 네트워크 외부에서 SIP 콜을 수행할 때 PBX(Private Branch Exchange)가 중앙 허브 역할을 수행할 수 있습니다. PBX의 주요 구성 요소는 SIP 프록시 또는 등록자라고도 하는 SIP 서버입니다. PBX는 기존의 스위치보드처럼 작동하며 클라이언트의 현재 상태를 표시하고 콜 전송, 음성 메일, 리디렉션 등을 허용합니다.

PBX SIP 서버는 로컬 엔터티 또는 오프 사이트로 설정됩니다. 인트라넷에서 또는 타사 공급자가 이 서버를 호스팅할 수 있습니다. 네트워크 간에 SIP 콜을 수행할 때 도달할 SIP 주소 위치를 쿼리하는 PBX 세트를 통해 콜이 라우팅됩니다.

각 SIP 사용자 에이전트는 PBX로 등록한 후 올바른 내선 번호로 전화를 걸어 다른 사용자 에이전트에 연결할 수 있습니다. 이 경우 일반적인 SIP 주소는 `sip:<user>@<domain>` 또는 `sip:<user>@<registrar-ip>`입니다. SIP 주소는 IP 주소와 별개이며, PBX는 PBX에 등록되어 있는 한 장치에 액세스할 수 있게 해줍니다.

예:



1 sip:mydoor@company.com
2 sip:myspeaker@company.com
*3 **PBX** sip.company.com*
4 sip:office@company.com

Axis 인터콤의 통화 버튼을 누르면 하나 이상의 PBX를 통해 로컬 IP 네트워크나 인터넷의 SIP 주소로 콜이 전달됩니다.

NAT 통과 기능

Axis 장치가 사설망(LAN)에 있고 해당 네트워크 외부에서 장치에 액세스하려면 NAT(네트워크 주소 변환) 통과 기능을 사용합니다.

비고

라우터가 NAT 통과 및 UPnP®를 지원해야 합니다.

각 NAT 통과 프로토콜을 개별적으로 사용하거나 네트워크 환경에 따라 다른 조합으로 사용할 수 있습니다.

- **ICE** ICE(Interactive Connectivity Establishment) 프로토콜을 사용하면 피어 장치 간에 원활한 통신이 이루어지도록 가장 효율적인 경로를 찾기 쉬워집니다. STUN 및 TURN을 활성화해도 ICE 프로토콜에서 가장 효율적인 경로를 찾을 수 있는 기회가 향상됩니다.
- **STUN** - STUN(Session Traversal Utilities for NAT)은 Axis 제품이 NAT 또는 방화벽 뒤에 있는지 확인하고 그럴 경우 원격 호스트 연결용으로 할당된 매핑되어진 공용 IP 주소와 포트 번호를 가져올 수 있게 해주는 클라이언트-서버 네트워크 프로토콜입니다. IP 주소 같은 STUN 서버 주소를 입력합니다.
- **TURN** - TURN(Traversal Using Relays around NAT)은 NAT 라우터 또는 방화벽 뒤에 있는 장치가 TCP 또는 UDP를 통해 다른 호스트에서 들어오는 데이터를 수신할 수 있도록 해주는 프로토콜입니다. TURN 서버 주소 및 로그인 정보를 입력합니다.

오버레이

비고

SIP 호출을 사용하는 경우에는 오버레이가 비디오 스트림에 포함되지 않습니다.

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

스트리밍 및 저장

비디오 압축 형식

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

Motion JPEG

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

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

H.264 또는 MPEG-4 Part 10/AVC

비고

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

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

H.265 또는 MPEG-H Part 2/HEVC

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

비고

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

애플리케이션

애플리케이션을 사용하면 Axis 장치를 최대한 활용할 수 있습니다. AXIS Camera Application Platform(ACAP)은 타사가 Axis 장치의 분석 및 기타 애플리케이션을 개발할 수 있는 개방형 플랫폼입니다. 애플리케이션은 장치에 사전 설치하거나 무료로 다운로드하거나 라이센스 비용을 지불할 수 있습니다.

Axis 애플리케이션에 대한 사용자 설명서를 찾아보려면 *help.axis.com*으로 이동합니다.

비고

- 여러 애플리케이션을 동시에 실행할 수 있지만 일부 애플리케이션은 서로 호환되지 않을 수 있습니다. 특정 애플리케이션의 조합은 병렬로 실행할 때 너무 많은 처리 능력 또는 메모리 리소스가 필요할 수 있습니다. 전개하기 전에 애플리케이션이 호환되는지 확인하십시오.

AXIS Object Analytics

AXIS Object Analytics는 카메라에 사전 설치되어 제공되는 분석 애플리케이션입니다. AXIS Object Analytics는 장면에서 움직이는 객체를 감지하고 이 객체를 사람 또는 차량으로 분류합니다. 다양한 유형의 객체에 대한 알람을 보내도록 애플리케이션을 설정할 수 있습니다. 애플리케이션의 작동 방식에 대한 자세한 내용은 *AXIS Object Analytics 사용자 설명서*를 참조하십시오.

메타데이터 시각화

장면의 움직이는 객체에 분석 메타데이터를 사용할 수 있습니다. 지원되는 객체 등급은 객체 유형 및 분류의 신뢰 수준에 대한 정보와 함께 객체를 감싸는 바운딩 박스를 통해 비디오 스트림에 시각화됩니다. *AXIS Scene Metadata 통합 가이드*에서 분석 메타데이터의 구성 및 사용 방법을 자세히 알아보십시오.

사이버 보안

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

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

Signed OS

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

Secure Boot

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

Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 장치의 ID 및 무결성을 보장하고 무단 액세스로부터 중요한 정보를 보호하는 기능을 제공합니다. 이 플랫폼은

암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

Axis device ID

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

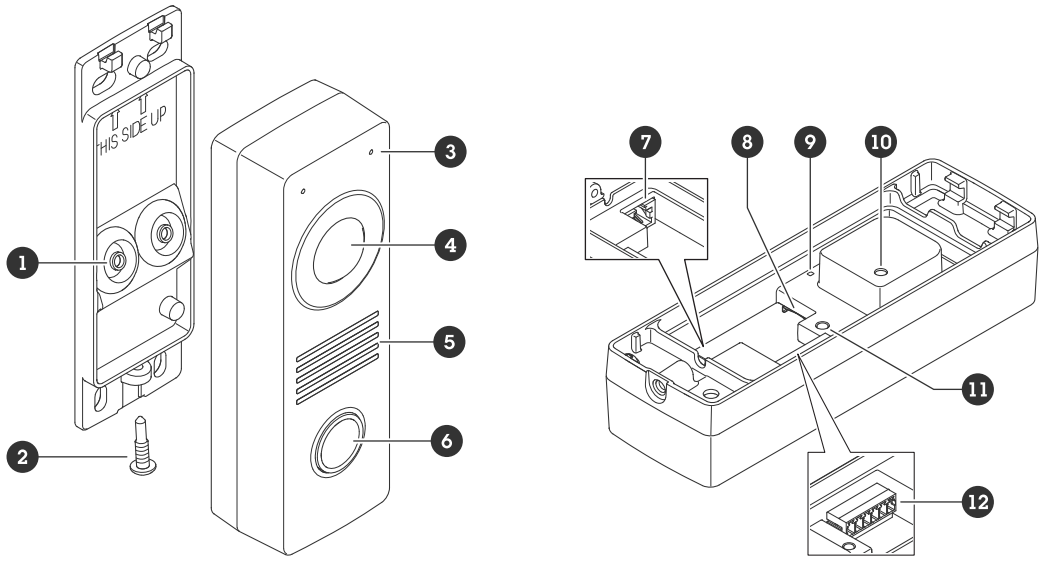
Signed Video

Signed Video는 비디오 파일의 보관 연속성을 증명하지 않고도 비디오 증거가 변조되지 않은 것으로 검증될 수 있도록 합니다. 각 카메라는 보안 키 저장소에 안전하게 저장된 고유한 비디오 서명 키를 사용하여 비디오 스트림에 서명을 추가합니다. 비디오가 재생될 때 파일 플레이어는 비디오의 손상 여부를 표시합니다. Signed Video를 통해 비디오의 원본 촬영 카메라를 추적하고 비디오가 카메라를 떠난 후 변조되지 않았는지 확인할 수 있습니다.

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

사양

제품 개요



1 개스킷(2개)
2 나사(TR20)
3 마이크(2개)
4 카메라
5 스피커
6 통화 버튼
7 네트워크 커넥터(PoE)
8 SD 카드 슬롯
9 상태 LED
10 탬퍼 버튼
11 제어 버튼
12 I/O, 릴레이 및 리더 커넥터

LED 표시

상태 LED	표시
녹색	정상 작동 시 녹색이 계속 표시됩니다.

SD 카드 슬롯

통지

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

이 장치는 microSD/microSDHC/microSDXC 카드를 지원합니다.

SD 카드 권장 사항은 *axis.com*을 참조하십시오.

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

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. 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

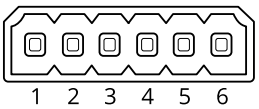
네트워크 커넥터

PoE(Power over Ethernet)를 지원하는 RJ45 이더넷 커넥터

I/O, 리더 및 릴레이 커넥터

I/O 및 릴레이 또는 리더 연결에 이 커넥터를 사용할 수 있습니다.

6핀 단자대입니다.



1 -
2 12V
3 A/IO1
4 B/IO2
5 NO/NC
6 CO

기능	핀	비고	사양
DC 접지	1		0V DC
DC 출력	2	보조 장비에 전원을 공급할 때 사용 가능합니다. 참고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	12 V DC **I/O** : 최대 부하 = 50mA **리더/릴레이**: 최대 부하 = 350mA
I/O: 구성 가능(입력 또는 출력) **리더**: A	3	**I/O**: 디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 디지털 출력 - 활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다. **리더**: RS485 - A	**I/O** : 입력 - 0 ~ 최대 30V DC 출력 - 0 ~ 최대 30V DC, 개방 드레인, 100mA
I/O: 구성 가능(입력 또는 출력) **리더**: B	4	**I/O**: 핀 3과 동일 **리더**: RS485 - B	**I/O**: 핀 3과 동일

릴레이: NO/NC	5	정상 개방/정상 폐쇄. 릴레이 장치 연결에 사용됩니다. 두 개의 릴레이 핀은 나머지 회로와 전기적으로 분리되어 있습니다.	최대 전류 700mA, 최대 전압 30V DC
Relay(릴레이): CO	6	공통	

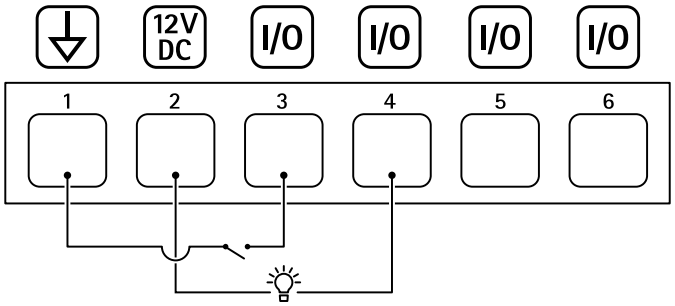
I/O 커넥터

한 가지 옵션은 커넥터를 모션 디텍션, 이벤트 트리거링, 알람 알림 등과 결합하여 외부 장치와 함께 I/O 커넥터로 사용하는 것입니다. I/O 커넥터는 0V DC 참조점 및 전원(12V DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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

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

예:



1 DC 접지
2 DC 출력 12V, 최대 50mA
3 I/O가 입력으로 구성됨
4 I/O가 출력으로 구성됨
5 릴레이 전용
6 릴레이 전용

릴레이 커넥터

I/O와 함께 커넥터를 릴레이 커넥터로 사용하여 솔리드 스테이트 릴레이를 연결하고 다음과 같이 사용할 수 있습니다.

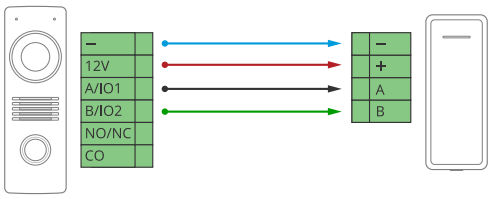
- 보조 회로를 열고 닫는 표준 릴레이
- 잠금 직접 제어
- 안전 릴레이를 통해 잠금 제어. 도어의 안전한 쪽에 안전 릴레이를 사용하면 핫 와이어링을 방지할 수 있습니다.

리더 커넥터

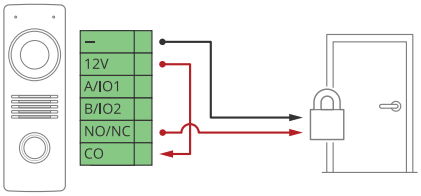
세 번째 옵션은 커넥터를 리더 커넥터로 사용하여 외부 리더를 연결하는 것입니다.

장비 연결

Axis 리더

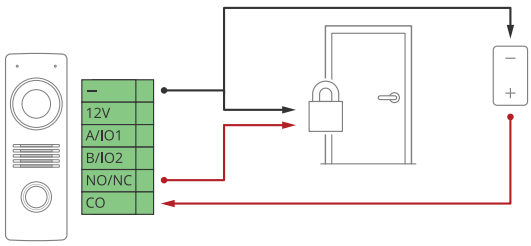


PoE(12V)로 구동되는 릴레이



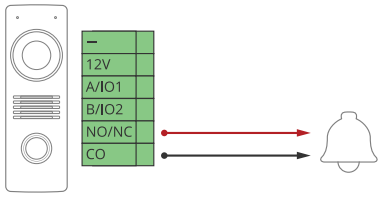
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(정상 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

별도의 전원 공급 장치로 구동되는 릴레이



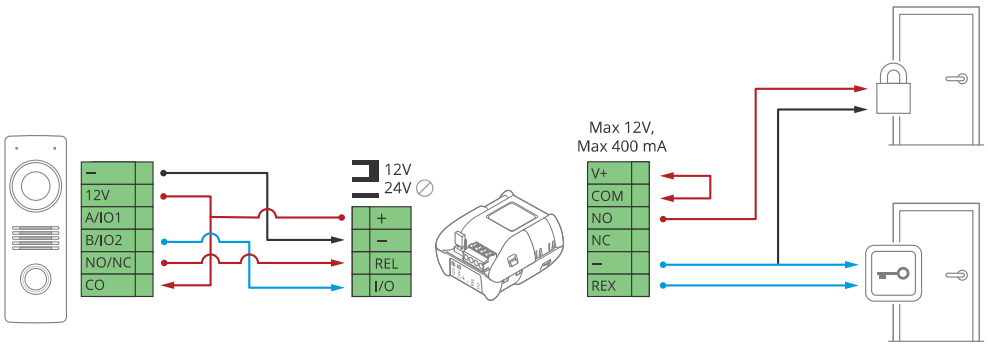
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(정상 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

자유 전위 릴레이



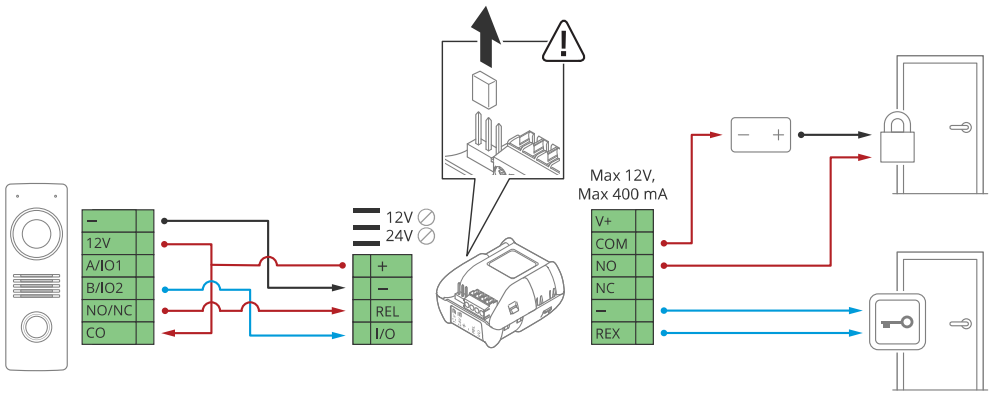
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(정상 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

인터콤에서 PoE로 전원이 공급되는 12V 페일 시큐어 잠금 장치



1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(정상 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

외부 전원 공급 장치에서 전원이 공급되는 12V 페일 시큐어 잠금 장치



1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(정상 상태)**로 설정합니다.
   -  페일 시큐어용.
   -  페일 세이프 잠금용.

문제 해결

공장 출하 시 기본 설정으로 재설정

중요 사항

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

제품을 공장 출하 시 기본 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끊습니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. 을 참조하십시오.
3. 상태 LED 표시기가 주황색으로 깜박일 때까지 15-30초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시등이 녹색으로 바뀌면 과정이 완료됩니다. 네트워크에서 DHCP 서버를 이용할 수 없는 경우, 장치의 IP 주소는 다음 중 하나로 기본 설정됩니다.
   - **AXIS OS 12.0 이상이 설치된 장치:** 링크-로컬 주소 서브넷(169.254.0.0/16)에서 가져온 주소
   - **AXIS OS 11.11 이하가 설치된 장치:** 192.168.0.90/24
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 장치에 액세스합니다.
   설치 및 관리 소프트웨어 도구는 *axis.com/support*의 지원 페이지에서 제공됩니다.

또한 장치의 웹 인터페이스를 통해 매개변수를 공장 출하 시 기본값으로 재설정할 수 있습니다. **Maintenance(유지 보수)** >**Factory default(공장 출하 시 기본 설정)**로 이동하고 **Default(기본)**를 클릭합니다.

AXIS OS 옵션

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

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

현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

AXIS OS 업그레이드

중요 사항

- 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-software*로 이동합니다.

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

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

기술적 문제, 단서 및 해결 방안

찾는 내용이 여기에 없는 경우에는 *axis.com/support*에서 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 out`이라는 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 `https`를 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 다운로드는 *axis.com/vms*로 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 다양한 설정과 상황이 성능에 어떠한 영향을 주는지를 고려하는 것이 중요합니다. 일부 요소는 필요한 대역폭(비트 레이트)의 양에 영향을 주며 다른 요인은 프레임 레이트에 영향을 주고 어떤 요인은 둘 다에 영향을 줍니다. CPU 부하가 최대치에 도달하는 경우에는 프레임 레이트에 영향을 주기도 합니다.

가장 중요하게 고려해야 할 요인은 다음과 같습니다.

- 높은 이미지 해상도 또는 낮은 압축 수준으로 인해 대역폭에 영향을 주는 데이터가 많이 포함된 이미지가 생성될 수 있습니다.
- 여러 Motion JPEG 클라이언트나 유니캐스트 H.264/H.265/AV1 클라이언트로 액세스하면 대역폭에 영향을 줍니다.
- 여러 클라이언트로 여러 스트림(해상도, 압축)을 동시에 보면 프레임 레이트와 대역폭 모두에 영향을 줍니다.
  높은 프레임 레이트를 유지해야 하는 곳에서는 동일한 스트림을 사용합니다. 스트림 프로파일은 동일한 스트림을 보장하는데 사용할 수 있습니다.

- 서로 다른 코덱으로 비디오 스트림에 동시에 액세스하면 프레임 레이트와 대역폭에 모두 영향을 미칩니다. 최적의 성능을 위해 동일한 코덱을 사용하는 스트림을 사용하십시오.
- 이벤트 설정의 과다한 사용은 프레임 레이트에 영향을 줄 수 있는 제품의 CPU 부하에 영향을 줍니다.
- HTTPS를 사용하면 프레임 레이트가 낮아질 수 있으며 특히 Motion JPEG를 스트리밍하는 경우입니다.
- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.
- 성능이 낮은 클라이언트 컴퓨터에서 보기는 인식한 성능을 떨어뜨리고 프레임 레이트에 영향을 줍니다.
- 동시에 여러 AXIS Camera Application Platform(ACAP) 애플리케이션을 실행하면 프레임 레이트 및 일반적인 성능에 영향을 줍니다.

지원 센터 문의

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

T10183848_ko

2025-06 (M11.2)