AXIS C1310-E Network Horn Speaker

사용자 설명서

솔루션 개요

이 설명서는 오디오 시스템에서 장치에 액세스할 수 있도록 하는 방법과 인터페이스에서 직접 장치를 구성하는 방법(예: 오디오 또는 영상 관리 소프트웨어 없이 장치를 사용하는 경우)에 대해 설명합니다.

오디오 또는 비디오 매니지먼트 소프트웨어를 사용하는 경우 해당 소프트웨어를 사용하여 장치를 구성할 수 있습니다. 다음 관리 소프트웨어를 사용하여 오디오 시스템을 제어할 수 있습니다.

- **AXIS Audio Manager Edge** — 소규모 시스템용 오디오 관리 소프트웨어. 펌웨어가 10.0 이상인 모든 오디오 장치에 사전 설치된 상태로 제공됩니다.
  - *AXIS Audio Manager Edge 사용자 설명서*
- **AXIS Audio Manager Pro** — 더 규모가 시스템용 고급 오디오 관리 소프트웨어
  - *AXIS Audio Manager Pro 사용자 설명서*
- **AXIS Camera Station** — 대규모 시스템을 위한 고급 영상 관리 소프트웨어.
  - *AXIS Camera Station 사용자 설명서*
- **AXIS Companion** — 영상 관리 소프트웨어 소규모 시스템용.
  - *AXIS Companion 사용자 설명서*

자세한 내용은 *오디오 관리 소프트웨어*를 참조하십시오.



네트워크 오디오 작동 방식의 개요입니다.

설치



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	✓	✓	✓	✓*

*iOS 15 또는 iPadOS 15에서 AXIS OS 웹 인터페이스를 사용하려면
Settings(설정) > Safari > Advanced(고급) > Experimental Feature(실험적 기능)으로 이동하고 NSURLSession Websocket을 비활성화합니다.

권장되는 브라우저에 대한 자세한 정보가 필요하면 *AXIS OS Portal*로 이동합니다.

장치 액세스

1. 브라우저를 열고 Axis 장치의 IP 주소 또는 호스트 이름을 입력합니다.
2. 사용자 이름과 패스워드를 입력합니다. 처음으로 장치에 액세스하는 경우 root 패스워드를 설정해야 합니다. 을 참조하십시오.

root 계정에 대한 새 패스워드 설정

중요 사항

기본 관리자의 사용자 이름은 **root**입니다. root에 대한 패스워드를 잃어버리면, 장치를 공장 출하 시 기본 설정으로 재설정합니다. 을 참조하십시오.



지원 팁: 패스워드 보안 확인 점검

1. 패스워드를 입력합니다. 안전한 패스워드에 대한 지침을 따릅니다. 을 참조하십시오.
2. 패스워드를 다시 입력하여 철자를 확인합니다.
3. **저장**을 클릭합니다. 패스워드가 이제 구성되었습니다.

안전한 패스워드

중요 사항

네트워크를 통해 Axis 장치가 초기에 설정된 패스워드를 평문 형식으로 전송합니다. 처음 로그인한 후 장치를 보호하려면 안전하고 및 암호화된 HTTPS 연결을 설정한 다음 패스워드를 변경합니다.

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.

추가 설정

원격 스피커 테스트 보정 및 실행

스피커 테스트를 실행하여 원격 위치에서 스피커가 의도한 대로 작동하는지 확인할 수 있습니다. 스피커는 내장 마이크로 등록된 일련의 테스트 톤을 재생하여 테스트를 수행합니다. 테스트를 실행할 때마다 등록된 값이 보정 중에 등록된 값과 비교됩니다.

비고

테스트는 설치 장소의 장착 위치에서 보정해야 합니다. 스피커를 옮기거나 주변 환경이 달라지면 (예: 벽을 세우거나 없애는 경우) 스피커를 다시 보정해야 합니다.

보정하는 동안 누군가가 실제로 설치 현장에 있으면서 테스트 톤을 듣고, 스피커 음향 경로에 의도하지 않은 방해물이 있어 테스트 톤이 지워지거나 막히지 않도록 해야 합니다.

1. 장치 인터페이스 >**Audio(오디오) > Speaker test(스피커 테스트)**로 이동합니다.
2. 오디오 장치를 보정하려면 **Calibrate(보정)**를 클릭합니다.

비고

Axis 제품이 보정되면 언제든지 스피커 테스트를 실행할 수 있습니다.

3. 스피커 테스트를 실행하려면 **Run the test(테스트 실행)**를 클릭합니다.

비고

물리적 장치에서 제어 버튼을 눌러 보정을 실행할 수도 있습니다. 제어 버튼을 식별하려면 항목을 참조하십시오.

다이렉트 SIP(P2P) 설정

동일한 IP 네트워크에 있는 소수의 사용자 에이전트 간에 통신이 이루어지고 PBX 서버가 제공할 수 있는 별도의 기능이 필요 없으면 피어 투 피어를 사용하십시오. P2P 작동 방식을 더 잘 이해하려면 항목을 참고하십시오.

설정 옵션에 대한 자세한 내용은 항목을 참고하십시오.

1. **System(시스템)** > **SIP** > **SIP settings(SIP 설정)**로 이동하고 **Enable SIP(SIP 활성화)**를 선택합니다.
2. 장치가 수신 콜을 받게 하려면 **Allow incoming calls(수신 콜 허용)**를 선택합니다.
3. **Call handling(통화 처리)**에서 통화 시간 초과 및 지속 시간을 설정합니다.
4. **포트(Ports)** 아래에서 포트 번호를 입력합니다.
   - **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 사용되는 포트를 입력합니다. 미디어 전송의 기본 시작 포트는 4000입니다. 일부 방화벽은 특정 포트 번호에서 RTP 트래픽을 차단할 수 있습니다. 포트 번호는 1024 ~ 65535여야 합니다.
5. **NAT traversal(NAT 통과)** 아래에서 NAT 통과에 사용할 프로토콜을 선택합니다.

비고

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

6. **Audio(오디오)** 아래에서 SIP 콜에 대해 원하는 오디오 품질을 가진 하나 이상의 오디오 코덱을 선택합니다. 우선 순위 순서를 변경하려면 끌어서 놓습니다.
7. **Additional(추가)**에서 옵션 추가를 선택합니다.

- **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.

8. **저장**을 클릭합니다.

서버(PBX)를 통해 SIP 설정

IP 네트워크 안팎에서 무한대의 사용자 에이전트 사이에 통신이 이루어져야 할 경우 PBX 서버를 사용하십시오. PBX 공급자에 따라서 설정에 기능이 더 추가될 수 있습니다. P2P 작동 방식을 더 잘 이해하려면 항목을 참고하십시오.

설정 옵션에 대한 자세한 내용은 항목을 참고하십시오.

1. PBX 공급자에게 다음 정보를 요청합니다.

- 사용자 ID
- 도메인
- 패스워드
- 인증 ID
- 발신자 ID
- 등록자
- RTP 시작 포트

2. 새 계정을 추가하려면, **System(시스템)** > **SIP** > **SIP accounts(SIP 계정)**로 이동하고 **+ Account(+계정)**를 클릭합니다.
3. PBX 제공업체로부터 받은 세부정보를 입력합니다.
4. **Registered(등록됨)**를 선택합니다.
5. 전송 모드를 선택합니다.
6. **저장**을 클릭합니다.
7. 피어 투 피어와 같은 방법으로 SIP 설정을 지정합니다. 자세한 내용은 를 참조하십시오.

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, 장치가 스케줄에 따라 또는 콜을 수신하면 오디오 클립을 재생하거나 장치의 IP 주소가 변경되면 이메일을 보낼 수 있습니다.

자세히 알아보려면 *이벤트 규칙 시작하기* 가이드를 확인하세요.

스피커 테스트가 실패할 겨우 이메일 전송

이 예에서는 스피커 테스트가 실패하면 정의된 수신자에게 이메일을 보내도록 오디오 장치가 구성됩니다. 스피커 테스트는 매일 18:00에 이루어지도록 구성됩니다.

1. 스피커 테스트 일정 설정:

1.1. 장치 인터페이스 > **System(시스템)** >**Events(이벤트)** > **Schedules(일정)**으로 이동합니다.

1.2. 매일 18:00에 시작하고 18:01에 종료되는 일정을 생성합니다. 이름을 'Daily at 6pm(매일 오후 6시)'로 지정합니다.

2. 이메일 수신자 생성:

2.1. 장치 인터페이스 > **System(시스템)** >**Events(이벤트)** > **Recipients(수신자)**로 이동합니다.

2.2. **Add Recipient(수신자 추가)**를 클릭합니다.

2.3. 받는 사람 이름을 'Speaker test recipients(스피커 테스트 받는 사람)'으로 지정

2.4. **Type(유형)**에서 **Email(이메일)**을 선택합니다.

2.5. **Send email to(이메일 보내기)** 아래에서 수신자의 이메일 주소를 입력합니다. 쉼표를 사용하여 여러 주소를 구분하십시오.

2.6. 보낸 사람의 이메일 계정에 대한 세부 정보를 입력합니다.

2.7. **Test(테스트)**를 클릭하여 테스트 이메일을 보냅니다.

비고

일부 이메일 공급자는 예약된 이메일과 그와 유사한 형태를 수신하면서 사용자가 큰 첨부 파일을 받거나 보는 것을 제한하기 위해 보안 필터를 사용합니다. 배달 문제 및 이메일 계정 잠김을 방지하려면 이메일 공급자의 보안 정책을 확인하십시오.

2.8. **저장**을 클릭합니다.

3. 자동 스피커 테스트 설정:

3.1. 장치 인터페이스 > **System(시스템)** >**Events(이벤트)** > **Rules(룰)**로 이동합니다.

3.2. **Add a rule(룰 추가)**를 클릭합니다.

3.3. 룰에 대한 이름을 입력합니다.

3.4. **Condition(상태)** 아래에서 **Schedule(일정)**을 선택하고 트리거 목록에서 선택

3.5. **Schedule(일정)** 아래에서 일정('Daily at 6pm(매일 오후 6시)')을 선택합니다.

3.6. **Action(액션)** 아래에서 **Run automatic speaker test(자동 스피커 테스트 실행)**을 선택합니다.

3.7. **저장**을 클릭합니다.

4. 스피커 테스트가 실패할 때 이메일을 보내는 조건을 설정합니다.

4.1. 장치 인터페이스 > **System(시스템)** >**Events(이벤트)** > **Rules(룰)**로 이동합니다.

4.2. **Add a rule(룰 추가)**를 클릭합니다.

4.3. 룰에 대한 이름을 입력합니다.

4.4. **Condition(상태)** 아래에서 **Speaker test result(스피커 테스트 결과)**를 선택합니다.

4.5. **Speaker test status(스피커 테스트 상태)** 아래에서 **Didn't pass the test(테스트를 통과하지 못했습니다)**를 선택합니다.

4.6. **Action(액션)** 아래에서 **Send notification to email(이메일로 알림 전송)**을 선택합니다.

4.7. **Recipient(수신자)** 아래에서 수신자('(Speaker test recipients)스피커 테스트 수신자')를 선택합니다.

4.8. 제목과 메시지를 입력하고 **Save(저장)**를 클릭합니다.

카메라가 동작을 감지하면 오디오 재생

이 예에서는 Axis 네트워크 카메라가 모션을 감지할 때 오디오 클립을 재생하도록 오디오 장치를 설정하는 방법을 설명합니다.

전제 조건

- Axis 오디오 장치와 Axis 네트워크 카메라가 동일한 네트워크에 있어야 합니다.
- 모션 디텍션 애플리케이션이 구성되어 있고 카메라에서 실행 중이어야 합니다.

1. 오디오 클립 링크 준비:
   1.1. **Audio(오디오)** > **Audio clips(오디오 클립)**로 이동합니다.
   1.2. 오디오 클립의 경우 ⋮ > **Create link(링크 만들기)**를 클릭합니다.
   1.3. 클립을 반복할 볼륨과 횟수를 설정합니다.
   1.4. 복사 아이콘을 클릭하여 링크를 복사합니다.
2. 액션 룰 생성:
   2.1. **Settings(설정)** > **Events(이벤트)** > **Recipients(수신자)**로 이동합니다.
   2.2. **+ Add Recipient(수신자 추가)**를 클릭합니다.
   2.3. 수신자의 이름(예: "발표자")을 입력합니다.
   2.4. **Type(유형)** 드롭다운 목록에서 **HTTP**를 선택합니다.
   2.5. **URL** 필드에 오디오 장치의 구성된 링크를 붙여넣습니다.
   2.6. 오디오 장치의 사용자 이름 및 패스워드를 입력합니다.
   2.7. **저장**을 클릭합니다.
   2.8. **Rules**(룰)로 이동하고 **+ Add a rule**(룰 추가)을 클릭합니다.
   2.9. 액션 룰의 이름(예: "클립 재생")을 입력합니다.
   2.10. **Condition(조건)** 목록의 **Applications(애플리케이션)** 아래에서 비디오 모션 디텍션 대안을 선택합니다.

   비고

   비디오 모션 디텍션에 대한 옵션이 없는 경우 **Apps(앱)**로 이동하고 **AXIS Video Motion Detection**을 클릭한 다음 모션 디텍션을 켭니다.

   2.11. **Action(액션)** 목록에서 **Send notification through HTTP(HTTP를 통해 알림 전송)**를 선택합니다.
   2.12. **Recipient(수신자)** 아래에서 수신자를 선택합니다.
   2.13. **Save(저장)**를 클릭합니다.

DTMF로 오디오 중지

이 예제는 다음을 수행하는 방법을 설명합니다.

- 장치에서 DTMF 구성
- DTMF 명령이 장치에 전송되면 오디오를 중지하도록 이벤트 설정

1. **System(시스템)** > **SIP** > **SIP settings(SIP 설정)**으로 이동합니다.
2. **Enable SIP(SIP 활성화)**가 켜져 있는지 확인합니다.
   켜야 하는 경우, 나중에 **Save(저장)**을 클릭하는 것을 잊지 마십시오.
3. **SIP accounts(SIP 계정)**으로 이동합니다.
4. SIP 계정 옆에 있는, ⋮ > **Edit(편집)**을 클릭합니다.
5. **DTMF** 아래에서 **+ DTMF sequence(+ DTMF 시퀀스)**를 클릭합니다.
6. **Sequence(시퀀스)** 아래에서 '1'을 입력합니다.
7. **Description(설명)** 아래에서 'stop audio(오디오 중지)'를 입력합니다.
8. **저장**을 클릭합니다.
9. **System(시스템)** > **Events(이벤트)** > **Rules(룰)**로 이동하고 **Add a rule(룰 추가)**을 클릭합니다.

10. **Name(이름)** 아래에서 'DTMF stop audio(DTMF 오디오 중지)'를 입력합니다.
11. **Condition(상태)** 아래에서 **DTMF**를 선택합니다.
12. **DTMF Event ID(DTMF 이벤트 ID)** 아래에서 **stop audio(오디오 중지)**를 선택합니다.
13. **Action(액션)** 아래에서 **Stop playing audio clip(오디오 클립 재생 중지)**를 선택합니다.
14. **저장**을 클릭합니다.

수신 SIP 통화에 대한 오디오 설정

SIP 전화를 받을 때 오디오 클립을 재생하는 룰을 설정할 수 있습니다.

오디오 클립이 종료된 후 SIP 통화에 자동으로 응답하는 추가 룰을 설정할 수도 있습니다. 이는 알람 교환원이 오디오 장치 근처에 있는 사람의 주의를 환기시키고 통신 회선을 설정하려는 경우에 유용할 수 있습니다. 이는 오디오 장치에 SIP 호출을 하여 수행되며 오디오 장치는 오디오 장치 근처에 있는 사람에게 경고하기 위해 오디오 클립을 재생합니다. 오디오 클립 재생이 중지되면 오디오 장치에서 SIP 통화에 자동으로 응답하고 알람 교환원과 오디오 장치 근처에 있는 사람 간의 통신이 이루어질 수 있습니다.

SIP 설정 활성화:
1. 웹 브라우저에 IP 주소를 입력하여 스피커의 장치 인터페이스로 이동합니다.
2. **System(시스템)** > **SIP** > **SIP settings(SIP 설정)** 로 이동하여 **Enable SIP(SIP 활성화)**를 선택합니다.
3. 장치가 수신 콜을 받게 하려면 **Allow incoming calls(수신 콜 허용)**를 선택합니다.
4. **Save(저장)**를 클릭합니다.
5. **SIP accounts(SIP 계정)**로 이동합니다.
6. SIP 계정 옆에 있는, ⋮ > **Edit(편집)**을 클릭합니다.
7. **자동 응답**을 체크 해제합니다.

SIP 통화 수신 시 오디오 재생:
1. **Settings(설정) > System(시스템) > Events(이벤트) > Rules(룰)**로 이동하여 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **State(상태)**를 선택합니다.
4. 상태 목록에서 **신호 울림**을 선택합니다.
5. 액션 목록에서 **Play audio clip(오디오 클립 재생)**을 선택합니다.
6. 클립 목록에서 재생하려는 오디오 클립을 선택합니다.
7. 오디오 클립을 반복할 횟수를 선택합니다. 0은 "한 번 재생"을 의미합니다.
8. **Save(저장)**를 클릭합니다.

오디오 클립이 종료된 후 SIP 통화에 자동으로 응답:
1. **Settings(설정) > System(시스템) > Events(이벤트) > Rules(룰)**로 이동하여 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **Audio clip playing(오디오 클립 재생)**을 선택합니다.
4. **Use this condition as a trigger(이 조건을 트리거로 사용)을 클릭합니다.**
5. **Invert this condition(이 조건 반전)**에 표시합니다.
6. **+ 조건 추가**를 클릭하여 이벤트에 두 번째 조건을 추가합니다.
7. 조건 목록에서 **State(상태)**를 선택합니다.
8. 상태 목록에서 **신호 울림**을 선택합니다.

9. 액션 목록에서 **Answer call(통화 응답)**을 선택합니다.
10. **Save(저장)**를 클릭합니다.

상세 정보

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.

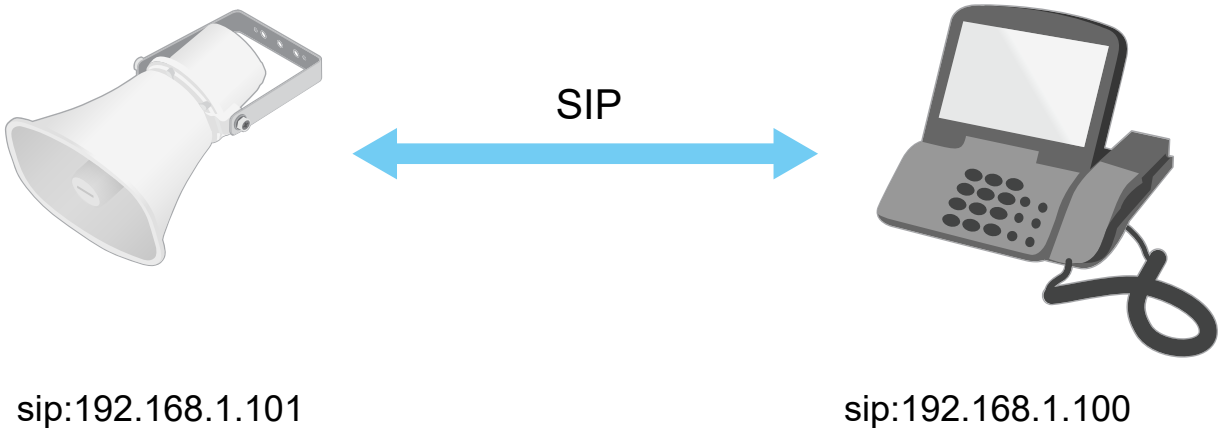
RTP(Real-Time Transport Protocol) 등의 전송 프로토콜을 사용하여 실제 오디오나 비디오가 SIP 사용자 에이전트 간에 교환됩니다.

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:



피어 투 피어 SIP 설정을 사용하는 동일한 네트워크에서 오디오 장치를 호출하도록 SIP 지원 전화기를 설정할 수 있습니다.

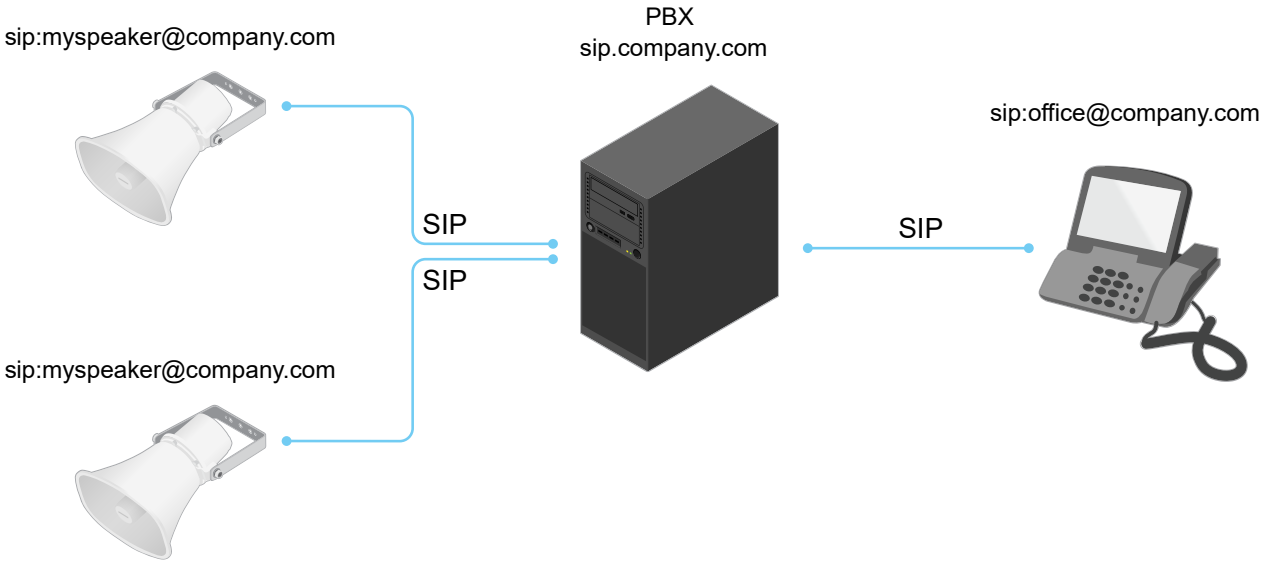
PBX(Private Branch Exchange)

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:



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.

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.

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

오디오 시스템 정보

이 정보는 AXIS Audio Manager Edge 사이트에 속한 장치에 대해서만 표시됩니다.

AXIS Audio Manager Edge: AXIS Audio Manager Edge를 시작합니다.

장치 찾기

일련 번호 및 IP 주소를 포함한 장치 찾기 정보를 표시합니다.

Locate device(장치 찾기): 스피커를 식별하는 데 도움이 되는 소리를 재생합니다. 일부 제품의 경우, 장치에서 LED가 깜박입니다.

스피커 테스트

스피커가 보정되었는지 여부를 표시합니다.

Speaker test(스피커 테스트): : 스피커를 보정합니다. 보정을 수행하고 스피커 테스트를 실행할 수 있는 **Speaker test(스피커 테스트)** 페이지로 이동합니다.

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 **Date and time(날짜 및 시간)** 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.

오디오

AXIS Audio Manager Edge

AXIS Audio Manager Edge: 애플리케이션을 시작합니다.

오디오 사이트 보안

CA Certificate(CA 인증서): 오디오 사이트에 장치를 추가할 때 사용할 인증서를 선택합니다. AXIS Audio Manager Edge에서 TLS 인증을 활성화해야 합니다.

Save(저장): 선택 항목을 활성화하고 저장합니다.

장치 설정

입력: 오디오 입력을 켜거나 끕니다. 입력 유형을 표시합니다.

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

Input type(입력 유형) : 입력 유형을 선택합니다.

Power type(전원 유형) : 전원 유형을 선택합니다.

출력: 출력 유형을 표시합니다.

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

스트림

Encoding(인코딩): 입력 소스 스트리밍에 사용할 인코딩을 선택합니다. 오디오 입력이 켜져 있는 경우에만 인코딩을 선택할 수 있습니다. 오디오 입력이 꺼져 있을 경우 켜려면 **Enable audio input (오디오 입력 활성화)**을 클릭합니다.

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.
- **삭제**: 장치에서 오디오 클립을 삭제합니다.

청취 및 녹음

들으려면 클릭합니다.

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

비고

장치 입력이 켜져 있어야만 듣고 녹음할 수 있습니다. 입력을 켜려면 **Audio > Device settings (오디오 > 장치 설정)**로 이동합니다.

장치에 대해 구성된 스토리지를 표시합니다. 스토리지를 구성하려면 관리자로 로그인해야 합니다.

스피커 테스트

스피커 테스트를 사용하여 원격으로 스피커가 의도한 대로 작동하는지 확인할 수 있습니다.

Calibrate(보정): 첫 번째 테스트 전에 스피커를 보정해야 합니다. 보정하는 동안 스피커는 내장 마이크에 의해 등록된 일련의 테스트 톤을 재생합니다. 스피커를 보정할 때 최종 위치에 설치해야 합니다. 나중에 스피커를 옮기거나 벽을 만들거나 제거하는 등 주변 환경이 바뀌면 스피커를 다시 보정해야 합니다.

Run the test(테스트 실행): 보정 중에 재생된 일련의 테스트 톤을 재생하고 보정의 등록된 값과 비교합니다.

녹화물

녹화를 필터링하려면 클릭합니다.

From(시작): 특정 시점 이후에 실행된 녹화를 표시합니다.

To(끝): 특정 시점까지 녹화를 표시합니다.

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

Event(이벤트): 이벤트를 기반으로 녹화를 표시합니다.

저장 장치: 스토리지 유형에 따라 녹화를 표시합니다.

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.

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.

Allow root-privileged apps(root 권한이 있는 앱 허용) : root 권한이 있는 앱이 장치에 대한 전체 권한을 허용하려면 켭니다.

AXIS OS 및 ACAP 앱의 보안 업데이트를 확인하십시오.

비고

동시에 여러 앱을 실행하면 장치의 성능에 영향을 미칠 수 있습니다.

앱 이름 옆에 있는 스위치를 사용하여 앱을 시작하거나 중지합니다.

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

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

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

시스템

시간과 장소

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

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

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

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

- **DHCP**: DHCP 서버의 시간대를 채택합니다. 이 옵션을 선택하려면 먼저 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.

- **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.

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

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

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

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

비고

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

IPv6

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

호스트 이름

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

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

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 > Security(시스템 > 보안)**로 이동합니다.

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

비고

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

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

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

Certificate(인증서): 장치에 HTTPS를 활성화하려면 인증서를 선택합니다.

네트워크 검색 프로토콜

Bonjour®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

UPnP®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

WS-검색: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

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):

- **원클릭**: 이것이 기본 설정입니다. 인터넷을 통해 O3C 서비스에 연결하려면 장치의 제어 버튼을 길게 누릅니다. 제어 버튼을 누른 후 24시간 이내에 O3C 서비스에 장치를 등록해야 합니다. 그렇지 않으면 장치가 O3C 서비스에서 연결 해제됩니다. 장치를 등록되면 **Always(항상)**가 활성화되고 장치가 O3C 서비스에 연결된 채 유지됩니다.
- **항상**: 장치가 인터넷을 통해 O3C 서비스에 대한 연결을 지속적으로 시도합니다. 장치를 등록하면 O3C 서비스에 연결된 채 유지됩니다. 장치의 제어 버튼이 닿지 않는 경우 이 옵션을 사용합니다.
- **아니요**: O3C 서비스를 비활성화합니다.

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

호스트: 프록시 서버의 주소를 입력합니다.

포트: 액세스에 사용되는 포트 번호를 입력하십시오.

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

Authentication method(인증 방법):

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

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

SNMP

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

SNMP: 사용할 SNMP 버전을 선택합니다.

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

- **More(더 보기)** : 작성하거나 선택할 추가 필드를 표시합니다.
- **Secure keystore(보안 키 저장소)**: 개인 키를 안전하게 저장하려면 **Secure element(보안 요소)** 또는 **Trusted Platform Module 2.0**을 선택합니다. 선택할 보안 키 저장소에 대한 자세한 내용을 보려면 *help.axis.com/en-us/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) :

- **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.

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

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

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

무차별 대입 공격 방지

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

차단 기간: 무차별 대입 공격을 차단할 시간(초)을 입력합니다.

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

방화벽

Activate(활성화): 방화벽을 켭니다.

Default Policy(기본 정책): 방화벽의 기본 상태를 선택합니다.
- **Allow(허용):** 장치로의 모든 연결을 허용합니다. 이 옵션은 기본 설정되어 있습니다.
- **Deny(거부):** 장치로의 모든 연결을 거부합니다.

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

- **Address(주소)**: 접근을 허용하거나 거부할 IPv4/IPv6 또는 CIDR 형식의 주소를 입력합니다.
- **Protocol(프로토콜)**: 접근을 허용 또는 거부할 프로토콜을 선택합니다.
- **포트**: 접근을 허용 또는 거부할 포트 번호를 입력합니다. 1~65535 사이의 포트 번호를 추가할 수 있습니다.
- **정책**: 룰의 정책을 선택합니다.

+ : 다른 룰을 생성하려면 클릭합니다.

Add rules(룰 추가): 정의한 룰을 추가하려면 클릭합니다.
- **Time in seconds(초 단위의 시간):** 룰 테스트에 대한 시간 제한을 설정합니다. 기본 시간 제한은 300초로 설정되어 있습니다. 룰을 즉시 활성화하려면 시간을 0초로 설정합니다.
- **Confirm rules(룰 확인):** 룰과 시간 제한을 확인합니다. 1초 이상의 시간 제한을 설정한 경우 이 시간 동안 룰이 활성화됩니다. 시간을 0으로 설정하면 룰이 바로 활성화됩니다.

Pending rules(보류 중인 룰): 아직 확인되지 않은 최신 테스트 룰에 대한 오버뷰입니다.

비고

시간 제한을 둔 룰은 표시된 타이머가 끝나거나 사용자가 확인할 때까지 **활성 규칙** 아래에 표시됩니다. 확인하지 않으면 타이머가 끝난 후 **보류 중인 룰** 아래에 표시되며, 방화벽은 이전에 정의한 설정으로 되돌아갑니다. 이를 확인하면 현재 활성 상태인 룰을 대체합니다.

Confirm rules(룰 확인): 보류 중인 룰을 활성화하려면 클릭합니다.

Active rules(룰 활성화): 현재 장치에서 실행 중인 룰에 대한 오버뷰입니다.

: 활성 룰을 삭제하려면 클릭합니다.

: 보류 중인 룰과 활성 룰을 모두 삭제하려면 클릭합니다.

사용자 지정 서명된 AXIS OS 인증서

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

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

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

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

계정

계정

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

Account(계정): 고유한 계정 이름을 입력합니다.

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

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

Privileges(권한):

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

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

Update account(계정 업데이트): 계정 속성을 편집합니다.

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

익명의 액세스

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

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

SSH 계정

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

- **Restrict root access(root 액세스 제한)**: root 액세스가 필요한 기능을 제한하려면 켭니다.
- **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.

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.
- **삭제**: 가상 호스트를 삭제합니다.

비활성화: 서버가 비활성화되었습니다.

OpenID 구성

중요 사항

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

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

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

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

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

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

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

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

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

Scopes(범위): 토큰의 일부가 될 수 있는 선택적 범위입니다.

Client secret(클라이언트 비밀): OpenID 패스워드 입력

Save(저장): OpenID 값을 저장하려면 클릭합니다.

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

이벤트

룰

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

비고

최대 256개의 액션 룰을 생성할 수 있습니다.

Add a rule(룰 추가): 룰을 생성합니다.

이름: 룰에 대한 이름을 입력합니다.

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

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

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

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

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

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

제품에는 다음과 같은 사전 구성된 룰 중 일부가 있을 수 있습니다.

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

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

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

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

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

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

수신 장치

이벤트에 대해 수신자에게 알리거나 파일을 보내도록 장치를 설정할 수 있습니다.

비고

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

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

비고

최대 20개의 수신자를 생성할 수 있습니다.

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

이름: 수신자의 이름을 입력합니다.

Type(유형): 목록에서 선택:

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

- **패스워드**: 로그인하려면 패스워드를 입력하십시오.

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

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

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

비고

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

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

Test(테스트): 설정을 테스트하려면 클릭합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

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

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

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

일정

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

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

수동 트리거

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

MQTT

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

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 Portal*에서 MQTT에 대해 자세히 알아볼 수 있습니다.

ALPN

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

MQTT 클라이언트

Connect(연결): MQTT 클라이언트를 켜거나 끕니다.

Status(상태): MQTT 클라이언트의 현재 상태를 표시합니다.

브로커

호스트: MQTT 서버의 호스트 이름 또는 IP 주소를 입력하십시오.

Protocol(프로토콜): 사용할 프로토콜을 선택합니다.

포트: 포트 번호를 입력합니다.

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

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

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

패스워드: 사용자 이름의 패스워드를 입력합니다.

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

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

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

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

Keep alive interval(간격 유지): 클라이언트가 긴 TCP/IP 시간 초과를 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 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.

주제 이름 포함: MQTT 주제에서 조건을 설명하는 주제를 포함하려면 선택합니다.

주제 네임스페이스 포함: MQTT 주제에 ONVIF 주제 네임스페이스를 포함하려면 선택합니다.

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

Add condition(조건 추가): 조건을 추가하려면 클릭합니다.

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

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

QoS: MQTT 발행에 대해 원하는 레벨을 선택합니다.

MQTT 구독

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

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

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

Subscription type(구독 유형):

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

QoS: MQTT 구독에 대해 원하는 레벨을 선택합니다.

MQTT 오버레이

비고

MQTT 오버레이 수정자를 추가하기 전에 MQTT 브로커에 연결하십시오.

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

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

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

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

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

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.

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 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

- **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.

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.
- **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 콜하는 데 사용됩니다.
- **Registered(등록됨)**: SIP 서버를 통해 로컬 네트워크 외부의 SIP 장치를 콜하는 데 사용됩니다.
- **도메인**: 사용 가능할 경우 공용 도메인 이름을 입력합니다. 도메인 이름은 다른 계정을 호출할 때 SIP 주소의 일부로 표시됩니다.
- **패스워드**: SIP 서버에 대해 인증하기 위한 SIP 계정과 연결된 패스워드를 입력합니다.
- **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.
  - **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.
  - **해상도**: 화상 통화에 사용할 해상도를 선택합니다. 해상도는 필요한 대역폭에 영향을 줍니다.
  - **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.

멀티캐스트 컨트롤러

User multicast controller(사용자 멀티캐스트 컨트롤러): 멀티캐스트 컨트롤러를 활성화하려면 켭니다.

Audio codec(오디오 코덱): 오디오 코덱을 선택합니다.

Source(소스): 새 멀티캐스트 컨트롤러 소스를 추가합니다.

- **Label(라벨)**: 소스에서 아직 사용하지 않은 라벨의 이름을 입력합니다.
- **Source(소스)**: 소스를 입력합니다.
- **포트**: 포트를 입력합니다.
- **Priority(우선 순위)**: 우선 순위를 선택합니다.
- **Profile(프로파일)**: 프로파일을 선택합니다.
- **SRTP key(SRTP 키)**: SRTP 키를 입력합니다.

상황에 맞는 메뉴에는 다음이 포함됩니다.

Edit(편집): 멀티캐스트 컨트롤러 소스를 편집합니다.

삭제: 멀티캐스트 컨트롤러 소스를 삭제합니다.

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.
- **패스워드**: 서버에 로그인이 필요한 경우 패스워드를 입력하십시오.
- **SMB version(SMB 버전)**: NAS에 연결할 SMB 스토리지 프로토콜 버전을 선택합니다. **Auto(자동)**를 선택하면 장치는 보안 버전 SMB 중 하나를 협상하려고 시도합니다. 3.02, 3.0, 또는 2.1. 상위 버전을 지원하지 않는 이전 NAS에 연결하려면 1.0 또는 2.0을 선택하십시오. Axis 장치의 SMB 지원에 대해 *여기*에서 자세히 알아볼 수 있습니다.
- **Add share without testing(테스트 없이 공유 추가)**: 연결 테스트 중에 오류가 발견된 경우에도 네트워크 공유를 추가하려면 선택합니다. 예를 들어, 서버에 패스워드가 필요하지만 이를 입력하지 않았기 때문에 오류가 발생할 수 있습니다.

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

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

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

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

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

도구

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

Use tool(도구 사용): 클릭하여 선택한 도구를 활성화합니다.

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

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.

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

이름: 포트 이름을 바꾸려면 텍스트를 편집합니다.

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

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

Current state(현재 상태): 포트의 현재 상태를 표시합니다. 현재 상태가 정상 상태와 같지 않을 때 입력 또는 출력이 활성화됩니다. 장치의 입력은 연결이 끊어지거나 1V DC 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.

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.

원격 시스템 로그

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

+ **Server(서버)**: 새 서버를 추가하려면 클릭합니다.

호스트: 서버의 호스트 이름 또는 IP 주소를 입력합니다.

Format(포맷): 사용할 syslog 메시지 포맷을 선택합니다.

- Axis
- RFC 3164
- RFC 5424

Protocol(프로토콜): 사용할 프로토콜 선택:

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

포트: 다른 포트를 사용하려면 포트 번호를 편집합니다.

Severity(심각도): 트리거될 때 전송할 메시지를 선택합니다.

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

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

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 다시 주황색으로 바뀔 때까지 10초 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, 제품에 액세스합니다.

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

현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

AXIS OS 업그레이드

중요 사항

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

비고

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

펌웨어 업그레이드 문제	
펌웨어 업그레이드 실패	펌웨어 업그레이드에 실패하면 장치가 이전 펌웨어를 다시 로드합니다. 가장 일반적인 원인은 잘못된 펌웨어 파일이 업로드된 것입니다. 장치에 해당하는 펌웨어 파일 이름을 확인하고 다시 시도하십시오.

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. 사용자 root의 비밀번호를 분실한 경우에는 장치를 공장 출하 시 기본 설정으로 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).

장치에 로컬로 액세스할 수 있지만 외부에서 액세스할 수 없음

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

- AXIS Camera Station: 30일 무료 평가판이며, 중소규모 시스템에 적합합니다.

지침 및 다운로드는 *axis.com/vms*로 이동합니다.

사운드 파일 문제

미디어 클립을 업로드할 수 없습니다	다음 오디오 클립 형식이 지원됩니다. • µ-law로 인코딩되고 8 또는 16kHz로 샘플링된 au 파일 형식.

- wav 파일 형식으로, PCM 오디오로 인코딩됩니다. 8비트 또는 16비트 모노 또는 스테레오 인코딩과 8~48kHz의 샘플 속도를 지원합니다.
- 64kbps~320kbps의 비트 레이트과 8~48kHz의 샘플 속도를 가진 모노 또는 스테레오의 mp3 파일 형식.

특정 볼륨으로 파일을 재생합니다. 오디오 클립이 다른 게인으로 생성된 경우 다른 음량으로 재생됩니다. 게인이 동일한 클립을 사용하는지 확인하십시오.

성능 고려 사항

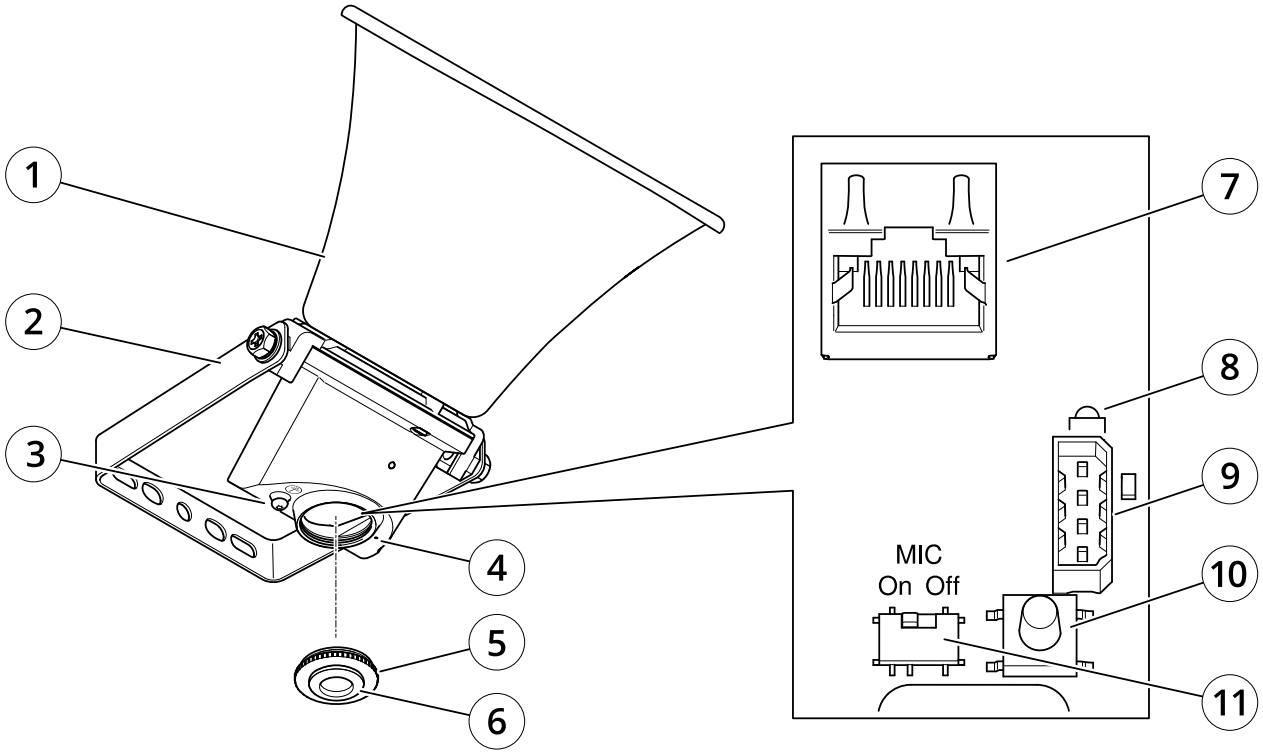
시스템을 설정할 때, 필요한 대역폭의 양(비트 레이트)에 다양한 설정과 상황이 성능에 어떠한 영향을 주는지 고려해야 합니다.

가장 중요하게 고려해야 할 요인은 다음과 같습니다.

- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.
- 동시에 여러 AXIS Camera Application Platform(ACAP) 애플리케이션을 실행하면 일반적인 성능에 영향을 줍니다.

사양

제품 개요



1 혼
2 브래킷
3 보호 접지 단자
4 마이크
5 캡
6 개스킷
7 네트워크 커넥터
8 상태 LED 표시기
9 I/O 포트
10 제어 버튼
11 마이크 비활성화 스위치

LED 표시

상태 LED	**표시**
켜져 있지 않음	정상 작동 시 켜져 있지 않음
녹색	시작 완료 후 정상 작동 시 10초 동안 계속 표시됩니다.
주황색	시작 시 켜져 있습니다. 장치 소프트웨어 업그레이드 중 또는 공장 출하 시 기본값으로 재설정 시 깜박입니다.
주황색/빨간색	네트워크 연결을 사용할 수 없거나 연결이 끊어진 경우 깜박입니다.
빨간색	업그레이드에 실패하면 천천히 깜박입니다.
빨간색/녹색	**Locate device(장치 찾기)**를 선택하면 빠르게 깜박입니다.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.
- 스피커 테스트를 보정합니다. 제어 버튼을 눌렀다 손을 떼면 테스트 톤이 재생됩니다.
- 제품을 공장 출하 시 기본 설정으로 재설정합니다. 을 참조하십시오.

마이크 비활성화 스위치

마이크 비활성화 스위치 위치는 항목을 참조하십시오.

마이크 비활성화 스위치는 기계적으로 마이크를 **켜기** 또는 **끄기**로 설정하는 데 사용됩니다. 이 스위치의 공장 출하 시 기본 설정은 **켜기**입니다.

커넥터

보호 접지 단자

⚠ 위험

감전 위험. 접지 와이어를 사용하여 제품을 올바르게 접지해야 합니다. 접지 와이어의 양 끝이 각 접지 표면과 접촉하고 있는지 확인합니다.

접지 와이어를 최대한 짧게 하여 전류 경로를 최단 거리로 설정해야 합니다.

네트워크 커넥터

PoE(Power over Ethernet)를 지원하는 RJ45 이더넷 커넥터

통지

차폐 네트워크 케이블(STP)을 사용하여 제품을 연결해야 합니다. 제품을 네트워크에 연결하는 모든 케이블은 특정 용도를 위한 케이블입니다. 네트워크 장치가 제조사의 지침에 따라 설치되었는지 확인하십시오. *www.axis.com*의 설치 가이드에서 규정 요건에 대해 자세히 알아보십시오.

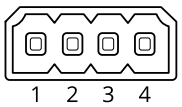
I/O 커넥터

모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 I/O 커넥터를 사용합니다. 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 웹 인터페이스에서 활성화할 수 있습니다.

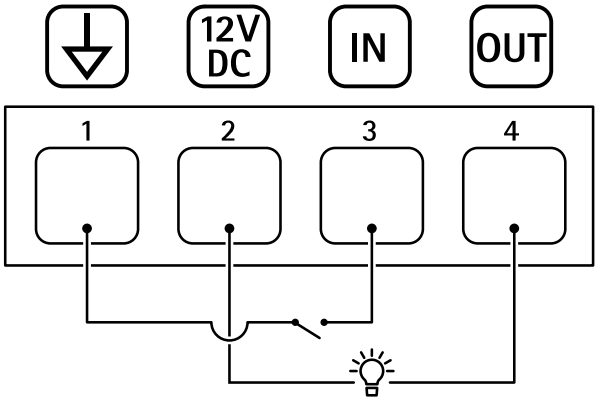
4핀 터미널 블록



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 최대 부하 = 25mA

디지털 입력	3	활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
디지털 출력	4	활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

예:



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

API 명령

VAPIX®는 Axis의 공개 API(애플리케이션 프로그래밍 인터페이스)입니다. VAPIX®를 통해 Axis 장치에 있는 거의 모든 기능을 제어할 수 있습니다. 전체 VAPIX® 설명서에 액세스하려면 Axis Developer Community(*axis.com/developer-community*)에 가입하십시오.

웹 브라우저에 명령을 입력하고, `<deviceIP>`를 사용자 장치의 IP 주소 또는 호스트 이름으로 바꿉니다.

중요 사항

API 명령이 즉시 실행됩니다. 장치를 복구하거나 재설정하면 모든 설정이 사라집니다. 예를 들어, 액션 룰을 잃게 됩니다.

예: Request
장치 재시작
Request
`http://<deviceIP>/axis-cgi/restart.cgi`

예: Request
장치 복구 요청은 대부분의 설정을 기본값으로 되돌리지만 IP 주소는 유지합니다.
Request
`http://<deviceIP>/axis-cgi/factorydefault.cgi`

예: Request
장치 재설정. 요청은 IP 주소를 포함한 모든 설정을 기본값으로 되돌립니다.
Request
`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

예: Request
모든 장치 매개변수 목록 보기
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=list`

예: Request
디버그 아카이브 가져오기
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz`

예: Request
서버 보고서 가져오기
Request
`http://<deviceIP>/axis-cgi/serverreport.cgi`

예: Request
300초 네트워크 추적 캡처
Request
`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

예: Request
FTP 활성화
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

예: Request
FTP 비활성화
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

예: Request
SSH 활성화
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

예: Request
SSH 비활성화
Request
`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

T10145506_ko

2024-09 (M20.2)

© 2020 – 2024 Axis Communications AB