# AXIS D4100-VE Mk II Network Strobe Siren

사용자 설명서

목차


설치 ..... 4
..... 4
시작하기 ..... 5
..... 5
네트워크에서 장치 찾기 ..... 5
브라우저 지원 ..... 5
장치의 웹 인터페이스 열기 ..... 5
관리자 계정을 생성합니다 ..... 5
안전한 패스워드 ..... 5
장치 구성 ..... 7
사이렌 설치 후 유지 보수 모드 끄기 ..... 7
유지보수 모드 켜기 ..... 7
프로파일 구성 ..... 7
프로파일 가져오기 또는 내보내기 ..... 7
다이렉트 SIP(P2P) 설정 ..... 7
서버(PBX)를 통해 SIP 설정 ..... 8
이벤트의 룰 설정 ..... 9
액션 트리거 ..... 9
알람이 트리거되면 프로파일 시작 ..... 9
SIP를 통해 프로파일 시작 ..... 9
SIP 확장을 통해 둘 이상의 프로파일 제어 ..... 10
우선 순위가 다른 두 개의 프로파일 실행 ..... 11
카메라가 모션을 감지하면 가상 입력을 통해 스트로브 사이렌 활성화 ..... 11
카메라가 모션을 감지하면 HTTP POST를 통해 스트로브 사이렌 활성화 ..... 12
카메라가 모션을 감지하면 MQTT를 통해 스트로브 사이렌을 활성화 ..... 14
웹 인터페이스 ..... 16
상세 정보 ..... 17
SIP(Session Initiation Protocol) ..... 17
Peer-to-peer SIP(피어 투 피어 SIP) ..... 17
PBX(Private Branch Exchange) ..... 17
NAT 통과 기능 ..... 17
사양 ..... 18
제품 오버뷰 ..... 18
..... 18
LED 표시 ..... 18
버튼 ..... 18
제어 버튼 ..... 18
커넥터 ..... 19
네트워크 커넥터 ..... 19
I/O 커넥터 ..... 19
조명 패턴 이름 ..... 20
사운드 패턴 이름 ..... 20
장치 세척 ..... 22
문제 해결 ..... 23
공장 초기화 설정으로 재설정합니다 ..... 23
AXIS OS 옵션 ..... 23
현재 AXIS OS 버전 확인 ..... 23
AXIS OS 업그레이드 ..... 23
기술적 문제 및 가능한 해결책 ..... 24
..... 26
성능 고려 사항 ..... 26
지원 센터 문의 ..... 26
사이버 보안 ..... 27

취약성 관리 ..... 27
보안 알림 ..... 27
보안 제품 수명 주기 ..... 27

## 설치



## 시작하기

**⚠ 경고**

번쩍이거나 깜박이는 빛은 광과민성 간질이 있는 사람에게 발작을 유발할 수 있습니다.

### 네트워크에서 장치 찾기

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

### 브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

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

✓: 권장

*: 제한적으로 지원됨

### 장치의 웹 인터페이스 열기

1. 사용자 이름과 패스워드를 입력합니다. 장치에 처음 액세스하는 경우, 관리자 계정을 생성해야 합니다. *관리자 계정을 생성합니다, on page 5* 항목을 참조하십시오.

AXIS OS가 탑재된 장치의 웹 인터페이스에 있는 모든 기능 및 설정에 대한 설명은 *AXIS OS 웹 인터페이스 도움말*을 참조하십시오.

### 관리자 계정을 생성합니다

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 계정을 입력합니다.
2. 패스워드를 입력합니다. *안전한 패스워드, on page 5* 항목을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이센스 계약을 수락하십시오.
5. **Add account(계정 추가)**를 클릭합니다.

### 안전한 패스워드

중요 사항

네트워크를 통해 패스워드나 기타 민감한 구성을 지정할 때는 HTTPS(기본적으로 활성화됨)를 사용하십시오. HTTPS는 안전하고 암호화된 네트워크 연결을 활성화하여, 패스워드와 같은 민감한 데이터를 보호합니다.

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

데이터 보호를 위해 적극 권장되는 작업은 다음과 같습니다.

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

## 장치 구성

### 사이렌 설치 후 유지 보수 모드 끄기

**⚠ 주의**

청력 손상과 밝은 조명으로 인한 눈부심으로부터 설치자를 보호하려면 장치를 설치할 때 유지 보수 모드를 켜는 것이 좋습니다.

장치를 처음 설치할 때 유지 보수 모드는 기본적으로 켜져 있습니다. 장치가 유지보수 모드에 있을 때 사이렌은 울리지 않고 조명은 흰색으로 진동하는 조명 패턴을 제공합니다.

**Maintenance mode(유지 보수 모드)**를 끄기 위해 **Overview(오버뷰)** >**Maintenance(유지 보수)**로 이동합니다.

### 유지보수 모드 켜기

장치의 서비스를 수행하려면 **Overview(오버뷰)** >**Maintenance(유지 보수)**로 이동하고 **Maintenance mode(유지 보수 모드)**를 켭니다. 그러면 일반 조명 및 사이렌 활동이 일시 중지됩니다.

### 프로파일 구성

프로파일은 설정된 구성 모음입니다. 우선 순위와 패턴이 다른 프로파일을 30개까지 가질 수 있습니다.

새 프로파일을 설정하려면:

1. **Profiles(프로파일)**로 이동하여 ＋ **Create(생성)**를 클릭합니다.
2. **Name(이름)**과 **Description(설명)**을 입력합니다.
3. 프로파일에 대해 원하는 **Light(조명)** 및 **Siren(사이렌)** 설정을 선택합니다.
4. 조명과 사이렌 **Priority(우선 순위)**를 설정하고 **Save(저장)**를 클릭합니다.

프로파일을 편집하려면 ⋮ 을 클릭하고 **Edit(편집)**을 선택합니다.

### 프로파일 가져오기 또는 내보내기

사전 정의된 구성이 있는 프로파일을 사용하려는 경우 가져올 수 있습니다.

1. **Profiles(프로파일)**로 이동하여 ＋ **Import(가져오기)**를 클릭합니다.
2. 파일을 찾아보거나 가져올 파일을 드래그합니다.
3. **Save(저장)**를 클릭합니다.

하나 이상의 프로파일을 복사하고 다른 장치에 저장하려면 다음과 같이 내보낼 수 있습니다.

1. 프로파일을 선택합니다.
2. **Export(내보내기)**를 클릭합니다.
3. .json 파일을 찾습니다.

### 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.

설정 옵션에 대한 자세한 내용은 *SIP*를 참조하십시오.

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 *NAT 통과*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. **Save(저장)**를 클릭합니다.

### 서버(PBX)를 통해 SIP 설정

사용자 에이전트가 IP 네트워크 안팎에서 통신할 때는 PBX 서버를 사용하십시오. PBX 공급자에 따라서 설정에 기능이 더 추가될 수 있습니다.

설정 옵션에 대한 자세한 내용은 *SIP*를 참조하십시오.

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. **Save(저장)**를 클릭합니다.
7. 피어 투 피어와 같은 방법으로 SIP 설정을 지정합니다. 자세한 내용은 *SIP*을 참조하십시오.

### 이벤트의 룰 설정

자세한 내용은 *이벤트 룰 시작하기*를 참조하십시오.

### 액션 트리거

1. **System(시스템)** > **Events(이벤트)**로 이동하여 **+ Add a rule(+ 룰 추가)**을 클릭합니다. 룰은 장치가 특정 액션을 수행하는 시간을 정의합니다. 룰을 예약, 반복 또는 수동 트리거로 설정할 수 있습니다.
2. **Name(이름)**을 입력합니다.
3. 작업을 트리거하려면 충족해야 하는 **Condition(조건)**을 선택합니다. 룰에 하나 이상의 조건을 지정하려면 모든 조건이 액션을 트리거하도록 충족해야 합니다.
4. 조건이 충족될 때 수행할 **Action(액션)**을 선택합니다.

### 알람이 트리거되면 프로파일 시작

이 예에서는 디지털 입력 신호가 변경될 때 알람을 트리거하는 방법을 설명합니다.

포트에 대해 입력하려면 방향을 설정합니다.

1. **System(시스템)** > **Accessories(액세서리)** > **I/O ports(I/O 포트)**로 이동합니다.
2. **Port 1(포트 1)** > **Normal state(정상 상태)**로 이동하고 **Circuit closed(회로 폐쇄)**를 클릭합니다.

룰 만들기:

1. **System(시스템)** > **Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **I/O** > **Digital input is active(디지털 입력 활성화)**를 선택합니다.
4. **Port 1(포트 1)**을 선택합니다.
5. 액션 목록에서 **Run light and siren profile while the rule is active(룰이 활성화되어 있는 동안 조명 및 사이렌 프로파일 실행)**를 선택합니다.
6. 시작하고 싶은 프로파일을 선택합니다.
7. **Save(저장)**를 클릭합니다.

### SIP를 통해 프로파일 시작

이 예에서는 SIP로 알람을 트리거하는 방법을 설명합니다.

다단계 인증(SIP) 활성화:

1. **System(시스템)** > **SIP** > **SIP settings(SIP 설정)**으로 이동합니다.
2. **Enable SIP(SIP 활성화)** 및 **Allow incoming calls(수신 호출 허용)**을 선택합니다.
3. **Save(저장)**를 클릭합니다.

룰 만들기:

1. **System(시스템)** > **Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **Call(호출)** > **State(상태)**를 선택합니다.
4. 상태 목록에서 **Active(활성화)**를 선택합니다.
5. 액션 목록에서 **Run light and siren profile while the rule is active(룰이 활성화되어 있는 동안 조명 및 사이렌 프로파일 실행)**를 선택합니다.
6. 시작하고 싶은 프로파일을 선택합니다.
7. **Save(저장)**를 클릭합니다.

### SIP 확장을 통해 둘 이상의 프로파일 제어

다단계 인증(SIP) 활성화:

1. **System(시스템)** > **SIP** > **SIP settings(SIP 설정)**으로 이동합니다.
2. **Enable SIP(SIP 활성화)** 및 **Allow incoming calls(수신 호출 허용)**을 선택합니다.
3. **Save(저장)**를 클릭합니다.

프로파일을 시작하기 위해 룰 생성:

1. **System(시스템)** > **Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **Call(호출)** > **State change(상태 변경)**를 선택합니다.
4. 이유 목록에서 **Accepted by device(장치에서 수락됨)**를 선택합니다.
5. **Call direction(통화 방향)**에서 **Incoming(수신)**을 선택합니다.
6. **Local SIP URI(로컬 SIP URI)**에 [Ext]가 프로파일에 사용되는 내선 번호이고 [IP address]가 장치 주소인 **<sip:[Ext]@[IP address]>**를 입력합니다. 예를 들어, **sip:1001@192.168.0.90**.
7. 액션 목록에서 **Light and Siren(조명 및 사이렌)** > **Run light and siren profile(조명 및 사이렌 프로파일 실행)**을 선택합니다.
8. 시작하고 싶은 프로파일을 선택합니다.
9. 액션 **Start(시작)**를 선택합니다.
10. **Save(저장)**를 클릭합니다.

프로파일을 정지하기 위해 룰 생성:

1. **System(시스템)** > **Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **Call(호출)** > **State change(상태 변경)**를 선택합니다.
4. 이유 목록에서 **Terminated(종료됨)**를 선택합니다.
5. **Call direction(통화 방향)**에서 **Incoming(수신)**을 선택합니다.
6. **Local SIP URI(로컬 SIP URI)**에서 [Ext]를 프로파일에 사용되는 확장자로, [IP address]를 장치 주소로 하여 **sip:[Ext]@[IP address]**를 입력하십시오. 예를 들어, **sip:1001@192.168.0.90**.
7. 액션 목록에서 **Light and Siren(조명 및 사이렌)** > **Run light and siren profile(조명 및 사이렌 프로파일 실행)**을 선택합니다.
8. 정지하고 싶은 프로파일을 선택합니다.
9. 액션 **Stop(정지)**을 선택합니다.
10. **Save(저장)**를 클릭합니다.

SIP를 통해 제어하려는 각 프로파일에 대한 시작 및 정지 룰을 만드는 단계를 반복합니다.

### 우선 순위가 다른 두 개의 프로파일 실행

우선 순위가 다른 두 프로파일을 실행하는 경우 우선 순위 번호가 더 높은 프로파일이 우선 순위 번호가 낮은 프로파일을 중단합니다.

비고

동일한 우선 순위로 두 개의 프로파일을 실행하면 가장 최근 프로파일이 이전 프로파일을 취소합니다.

이 예는 디지털 I/O 포트에 의해 트리거될 때 우선 순위 3을 가진 다른 프로파일보다 우선 순위 4를 가진 프로파일을 표시하도록 장치를 설정하는 방법을 설명합니다.

프로파일 생성:

1. 우선 순위 3인 프로파일을 만듭니다.
2. 우선 순위 4인 다른 프로파일을 만듭니다.

룰 만들기:

1. **System(시스템)** > **Events(이벤트)**로 이동하고 룰을 추가합니다.
2. 룰에 대한 이름을 입력합니다.
3. 조건 목록에서 **I/O** > **Digital input is active(디지털 입력 활성화)**를 선택합니다.
4. 포트를 선택합니다.
5. 액션 목록에서 **Run light and siren profile while the rule is active(룰이 활성화되어 있는 동안 조명 및 사이렌 프로파일 실행)**를 선택합니다.
6. 우선 순위 번호가 가장 높은 프로파일을 선택합니다.
7. **Save(저장)**를 클릭합니다.
8. **Profiles(프로파일)**를 이동하고 가장 낮은 우선 순위 번호로 프로파일을 시작합니다.

### 카메라가 모션을 감지하면 가상 입력을 통해 스트로브 사이렌 활성화

이 예에서는 카메라에 설치된 AXIS Motion Guard 애플리케이션이 모션을 감지할 때마다 스트로브 사이렌에 카메라를 연결하고 스트로브 사이렌에서 프로파일을 활성화하는 방법을 설명합니다.

시작하기 전:

- 스트로브 사이렌에서 운영자 또는 관리자 권한으로 새 계정을 생성합니다.
- 스트로브 사이렌에서 프로파일을 생성합니다.
- 카메라에서 AXIS Motion Guard를 설정하고 "Camera profile(카메라 프로필)"이라는 프로파일을 생성합니다.

카메라에 두 명의 수신자를 생성:

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

- **Name(이름)**: 가상 포트 비활성화
- **유형**: **HTTP**
- **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
  스트로브 사이렌의 주소와 함께 <IPaddress>를 바꿉니다.
- 새로 만든 스트로브 사이렌 계정의 계정 및 패스워드입니다.

6. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

카메라에 두 룰을 생성:

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

스트로보 사이렌에서 룰을 생성:

1. 스트로브 사이렌의 웹 인터페이스에서 **시스템 > 이벤트**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.
   - **Name(이름)**: 가상 입력 1에서 트리거
   - **Condition(조건)**: **I/O > Virtual input(가상 입력)**
   - **포트**:**1**
   - **Action(액션)**: **Light and siren(조명 및 사이렌) > Run light and siren profile while the rule is active(룰이 활성 상태인 동안 조명 및 프로파일 실행)**
   - **Profile(프로파일)**: 새로 생성한 프로파일을 선택합니다.
3. **Save(저장)**를 클릭합니다.

### 카메라가 모션을 감지하면 HTTP POST를 통해 스트로브 사이렌 활성화

이 예에서는 카메라에 설치된 AXIS Motion Guard 애플리케이션이 모션을 감지할 때마다 스트로브 사이렌에 카메라를 연결하고 스트로브 사이렌에서 프로파일을 활성화하는 방법을 설명합니다.

시작하기 전:

- 스트로브 사이렌에서 운영자 또는 관리자 역할을 가진 새 사용자를 생성합니다.
- 스트로브 사이렌에서 다음의 프로파일 생성: "Strobe siren profile".
- 카메라에서 AXIS Motion Guard를 설정하고 다음의 프로파일 생성: "Camera profile".
- 펌웨어 버전 10.8.0 이상에서 AXIS Device Assistant를 사용해야 합니다.

카메라에서 수신자를 생성:

1. 카메라의 장치 인터페이스에서 **System > Events > Recipients(시스템 > 이벤트 > 수신자)**로 이동하고 수신자를 추가합니다.
2. 다음 정보를 입력합니다.
   - **Name(이름)**: 스트로브 사이렌
   - **유형**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     스트로브 사이렌의 주소와 함께 <IPaddress>를 바꿉니다.
   - 새로 생성된 스트로브 사이렌 사용자의 사용자 이름과 패스워드입니다.
3. 모든 데이터가 유효한지 확인하기 위해 **Test(테스트)**를 클릭합니다.
4. **Save(저장)**를 클릭합니다.

카메라에 두 룰을 생성:

1. **Rules(룰)**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.
   - **Name(이름)**: 모션으로 스트로브 사이렌 활성화
   - **Condition(조건)**: **Applications(애플리케이션) > Motion Guard: Camera profile(모션 가드: 카메라 프로파일)**
   - **Action(액션)**: **Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)**
   - **Recipient(수신자)**: **Strobe siren(스트로브 사이렌)**.
     정보는 이전에 **Events > Recipients > Name(이벤트 > 수신자 > 이름)**에 입력한 것과 동일해야 합니다.
   - **Method(방법): POST**
   - **Body(본문)**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

스트로브 사이렌에서 프로파일을 만들 때 입력한 것과 동일한 정보를 '**"profile" : <>**' 항목에 입력합니다. 이 예시에서는 다음과 같습니다. "Strobe siren profile".

3. **Save(저장)**를 클릭합니다.
4. 다음 정보가 포함된 다른 룰을 추가합니다.
   - **Name(이름)**: 모션으로 스트로브 사이렌 비활성화
   - **Condition(조건)**: **Applications(애플리케이션) > Motion Guard: Camera profile(모션 가드: 카메라 프로파일)**
   - **Invert this condition(이 조건을 반전하기)**을 선택합니다.
   - **Action(액션)**: **Notifications > Send notification through HTTP(알림 > HTTP를 통해 알림 전송)**
   - **Recipient(수신자)**: **Strobe siren(스트로브 사이렌)**
     정보는 이전에 **Events > Recipients > Name(이벤트 > 수신자 > 이름)**에 입력한 것과 동일해야 합니다.
   - **Method(방법): POST**
   - **Body(본문)**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren
profile"  } }
```

스트로브 사이렌에서 프로파일을 만들 때 입력한 것과 동일한 정보를 '**"profile" : <>**' 항목에 입력합니다. 이 예시에서는 다음과 같습니다. "Strobe siren profile".

5. **Save(저장)**를 클릭합니다.

### 카메라가 모션을 감지하면 MQTT를 통해 스트로브 사이렌을 활성화

이 예에서는 카메라에 설치된 AXIS Motion Guard 애플리케이션이 움직임을 감지할 때마다 MQTT를 통해 스트로브 사이렌에 카메라를 연결하고 스트로브 사이렌에서 프로파일을 활성화하는 방법을 설명합니다.

시작하기 전:

- 스트로브 사이렌에서 프로파일을 생성합니다.
- MQTT 브로커를 설정하고 브로커의 IP 주소, 사용자 이름 및 패스워드를 가져옵니다.
- 카메라에 AXIS Motion Guard를 설정합니다.

카메라에서 MQTT 클라이언트 설정하기:

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

MQTT 게시를 위해 카메라에서 두 가지 룰을 생성:

1. **System(시스템) > Events(이벤트) > Rules(룰)**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.
   - **Name(이름)**: 움직임이 감지됨
   - **Condition(조건)**: **Applications > Motion alarm(애플리케이션 > 모션 알람)**
   - **Action(액션)**: **MQTT > Send MQTT publish message(MQTT 게시 메시지 전송)**
   - **Topic(토픽)**: 모션
   - **Payload(페이로드)**: 켜짐
   - **QoS**: 0, 1, 또는 2
3. **Save(저장)**를 클릭합니다.
4. 다음 정보가 포함된 다른 룰을 추가합니다.
   - **Name(이름)**: 모션 없음
   - **Condition(조건)**: **Applications > Motion alarm(애플리케이션 > 모션 알람)**
     - **Invert this condition(이 조건을 반전하기)**을 선택합니다.
   - **Action(액션)**: **MQTT > Send MQTT publish message(MQTT 게시 메시지 전송)**
   - **Topic(토픽)**: 모션
   - **Payload(페이로드)**: 꺼짐
   - **QoS**: 0, 1, 또는 2
5. **Save(저장)**를 클릭합니다.

스트로브 사이렌에서 MQTT 클라이언트를 설정:

1. 스트로브 사이렌의 장치 인터페이스에서 **System > MQTT > MQTT client > Broker(시스템 > MQTT > MQTT 클라이언트 > 브로커)**로 이동하고 다음 정보를 입력하십시오.
   - **Host(호스트)**: 브로커 IP 주소
   - **Client ID(클라이언트 ID)**: 사이렌 1
   - **Protocol(프로토콜)**: 브로커가 설정된 프로토콜
   - **Port(포트)**: 브로커가 사용하는 포트 번호
   - **Username(사용자 이름)** 및 **Password(패스워드)**
2. **Save(저장)** 및 **Connect(연결)**을 클릭합니다.
3. **MQTT subscriptions(MQTT 구독)**으로 이용하고 구독을 추가합니다.
   다음 정보를 입력합니다.
   - **Subscription filter(구독 필터)**: 모션
   - **Subscription type(구독 유형)**: 상태 추적 가능
   - **QoS**: 0, 1, 또는 2
4. **Save(저장)**를 클릭합니다.

MQTT 구독을 위한 스트로브 사이렌에서 룰을 생성:

1. **System(시스템) > Events(이벤트) > Rules(룰)**로 이동하고 룰을 추가합니다.
2. 다음 정보를 입력합니다.
   - **Name(이름)**: 움직임이 감지됨
   - **Condition(조건)**: **MQTT > Stateful(상태 추적 가능)**
   - **구독 필터**: **모션**
   - **Payload(페이로드)**: 켜짐
   - **Action(액션)**: **Light and siren(조명 및 사이렌) > Run light and siren profile while the rule is active(룰이 활성 상태인 동안 조명 및 프로파일 실행)**
   - **Profile(프로파일)**: 활성화하려는 프로파일을 선택합니다.
3. **Save(저장)**를 클릭합니다.

## 웹 인터페이스

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

## 상세 정보

### SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)는 VoIP 호출을 설정, 유지 및 종료하는 데 사용됩니다. 둘 이상의 파티즉, 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.

### 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.

### NAT 통과 기능

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

비고

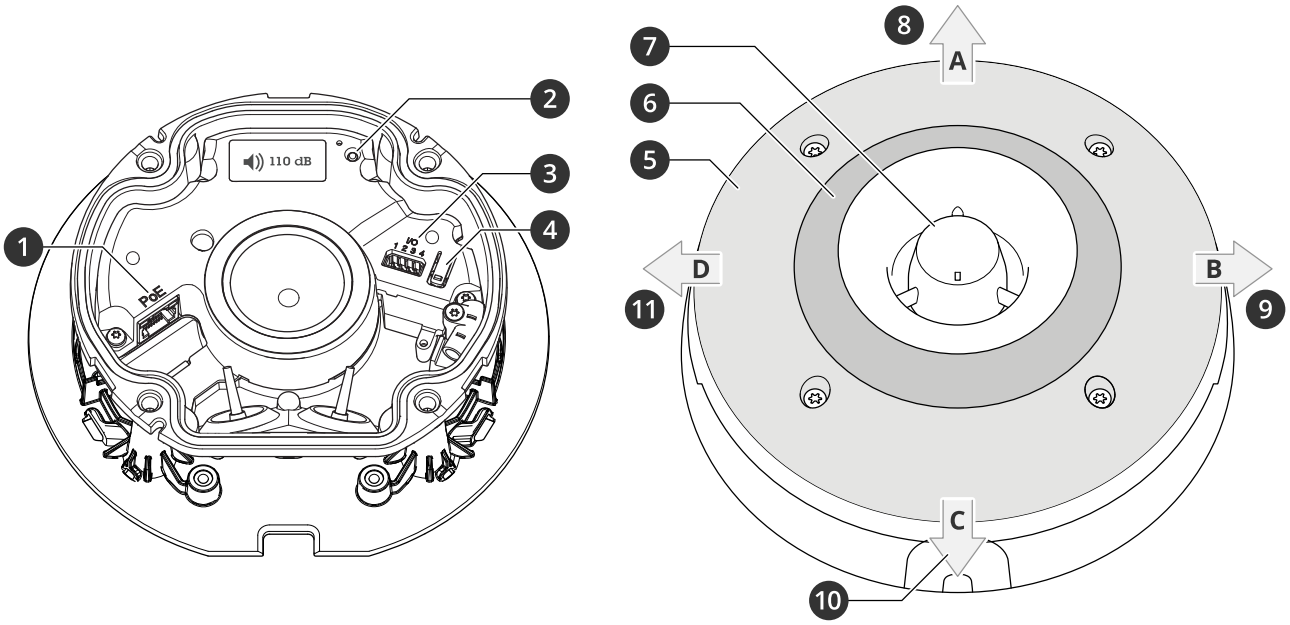
라우터가 NAT 통과 및 UPnP®를 지원해야 합니다.

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.

# 사양

## 제품 오버뷰




*1 네트워크 커넥터 PoE*
*2 상태 LED 표시기*
*3 I/O 커넥터*
*4 제어 버튼*
*5 백색 LED*
*6 빨간색, 청색, 녹색, 주황색(RGBA) LED*
*7 Siren(사이렌):*
*8 조명 방향 A*
*9 조명 방향 B*
*10 조명 방향 C*
*11 조명 방향 D*

## LED 표시

| 상태 LED | 표시 |
|---|---|
| 녹색 | 시작 완료 후 정상 작동 시 10초 동안 녹색이 계속 표시됩니다. |
| 주황색 | 시작 시, 공장 출하 시 기본값으로 재설정 시 또는 설정값 복원 시 켜져 있습니다. |

## 버튼

## 제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정합니다, on page 23* 항목을 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

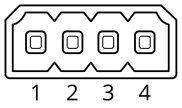
PoE(Power over Ethernet)를 지원하는 RJ45 이더넷 커넥터

### I/O 커넥터

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

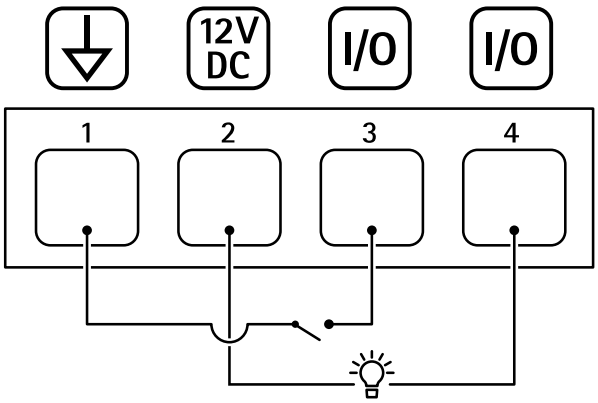
**디지털 출력 -** 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface로 이벤트를 통해 또는 장치의 웹 인터페이스에서 활성화할 수 있습니다.

4핀 단자대




| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지 | 1 | | 0 VDC |
| DC 출력 | 2 | ⚠<br>보조 장비에 전원을 공급할 때 사용 가능합니다.<br>비고: 이 핀은 정전된 경우에만 사용할 수 있습니다. | 12 VDC<br>최대 부하 = 50mA |
| 구성 가능(입력 또는 출력) | 3-4 | 디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. | 0 ~ 최대 30 VDC |
| | | 디지털 출력 - 활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다. | 0 ~ 최대 30 VDC, 개방 드레인, 100mA |

예:




1 *DC 접지*
2 *DC 출력 12V, 최대 50mA*
3 *I/O가 입력으로 구성됨*
4 *I/O가 출력으로 구성됨*

### 조명 패턴 이름

| |
|---|
| 꺼짐 |
| 점등 |
| 흰색 점등+플래시 색상 |
| 대체 |
| Pulse(펄스): |
| 3단계 에스컬레이션 |
| 깜박임 |
| 3번 깜박임 |
| 4번 깜박임 |
| 3번 깜박임 페이드 |
| 4번 깜박임 페이드 |
| 플래시 1번 |
| 플래시 3번 |
| 플래시 1번 흰색+점등 색상 |
| 플래시 3번 흰색+점등 색상 |
| 방향 A+점등 색상 |
| 방향 B+점등 색상 |
| 방향 C+점등 색상 |
| 방향 D+점등 색상 |
| 흰색 회전+점등 색상 |
| 테일 흰색 회전+점등 색상 |
| 임의의 흰색+점등 색상 |
| 스핀 화이트+점등 색상 |
| 점등 흰색+점등 색상 |

### 사운드 패턴 이름

| |
|---|
| 꺼짐 |
| 알람: 알람 고음 |
| 알람: 알람 저음 |
| 알람: 새 |
| 알람: 보트 경적 |
| 알람: 차량 알람 |
| 알람: 빠른 자동차 알람 |

| |
|---|
| 알람: 클래식 시계 |
| 알람: 첫 번째 참석자 |
| 알람: 공포 |
| 알람: 산업체 |
| 알람: 단일 경고음 |
| 알람: 부드러운 쿼드 경고음 |
| 알람: 부드러운 삼중 경고음 |
| 알람: 트리플 고음 |
| 알림: 거부됨(Denied) |
| 알림: 완료 |
| 알림: 출입 |
| 알림: 실패 |
| 알림: 서두름 |
| 알림: 메시지 |
| 알림: 다음 |
| 알림: 개방적 |
| Siren(사이렌): 대체 |
| Siren(사이렌): 탄력 |
| Siren(사이렌): 탈출 |
| Siren(사이렌): 떨어지는 음 |
| Siren(사이렌): 홈 소프트 |

## 장치 세척

미지근한 물과 순한 비연마성 비누로 장치를 세척하면 됩니다.

*통지*

- 자극적인 화학 물질로 인해 장치가 손상될 수 있습니다. 창문 세정제나 아세톤과 같은 화학 물질을 사용하여 장치를 세척하지 마십시오.
- 직사광선이나 고온에서 세척하면 얼룩이 생길 수 있으므로 주의해서 피해야 합니다.

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

Axis 장치 세척에 대한 자세한 내용은 *일반 세척제에 대한 화학적 내성* 백서를 참조하십시오.

# 문제 해결

## 공장 초기화 설정으로 재설정합니다

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 초기화 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끊습니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 오버뷰, on page 18* 항목을 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. 네트워크에 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 할당받음
   - **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 초기화 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 유지보수할 수 있습니다. Axis 장치 소프트웨어 전략에 대한 자세한 내용은 *axis.com/support/device-software*를 참조하십시오.

## 현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

## AXIS OS 업그레이드

중요 사항

- 장치 소프트웨어를 업그레이드하면, 사전 구성된 설정과 사용자 지정 설정이 저장됩니다. Axis Communications AB는 새 AXIS OS 버전에서 해당 기능을 사용할 수 있더라도 설정이 저장된다고 보장할 수 없습니다.
- AXIS OS 12.6부터는 장치의 현재 버전과 목표 버전 사이에 있는 모든 LTS 버전을 설치해야 합니다. 예를 들어 현재 설치된 장치 소프트웨어 버전이 AXIS OS 11.2인 경우, 장치를

AXIS OS 12.6으로 업그레이드하기 전에 LTS 버전 AXIS OS 11.11을 설치해야 합니다. 자세한 내용은 *AXIS OS 수명 주기 가이드: 업그레이드 경로*를 참조하십시오.

- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

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

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

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

## 기술적 문제 및 가능한 해결책

### AXIS OS 업그레이드 문제

**AXIS OS 업그레이드 실패**

업그레이드에 실패하면 장치가 이전 버전을 다시 로드합니다. 가장 일반적인 원인은 잘못된 AXIS OS 파일이 업로드된 것입니다. 장치에 해당하는 AXIS OS 파일 이름을 확인하고 다시 시도하십시오.

**AXIS OS 업그레이드 후 문제**

업그레이드 후 문제가 발생하면 **Maintenance(유지보수)** 페이지에서 이전에 설치된 버전으로 롤백하십시오.

### IP 주소 설정 문제

**IP 주소를 설정할 수 없음**

- 장치에 설정하려는 IP 주소와 장치에 액세스하는 데 사용하는 컴퓨터의 IP 주소가 서로 다른 서브넷에 있는 경우, IP 주소를 설정할 수 없습니다. 네트워크 관리자에게 문의하여 IP 주소를 받으십시오.
- 해당 IP 주소를 다른 장치가 사용하고 있을 수 있습니다. 확인 방법:
  1. 네트워크에서 Axis 장치를 분리합니다.
  2. Command/DOS 창에서, `ping`을 입력한 후 장치의 IP 주소를 입력합니다.
  3. `Reply from <IP address>: bytes=32; time=10...`이라는 메시지를 수신하는 경우, 이는 해당 IP 주소가 이미 네트워크의 다른 장치에서 사용 중일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 장치를 다시 설치하십시오.
  4. `Request timed out`이라는 메시지를 수신하는 경우, 이는 해당 IP 주소가 Axis 장치용으로 사용 가능하다는 것을 의미합니다. 모든 케이블 배선을 확인하고 장치를 다시 설치하십시오.
- 동일한 서브넷에 있는 다른 장치와 IP 주소 충돌이 발생할 수 있습니다. DHCP 서버에서 다이내믹 주소를 설정하기 전에 Axis 장치의 고정 IP 주소가 사용되었습니다. 즉, 동일한 기본 고정 IP 주소를 다른 장치에서도 사용하는 경우, 해당 장치에 액세스하는 데 문제가 발생할 수 있습니다.

### 장치 액세스 관련 문제

**브라우저로 장치에 액세스할 때 로그인할 수 없음**

HTTPS가 활성화된 경우, 로그인 시 올바른 프로토콜(HTTP 또는 HTTPS)을 사용해야 합니다. 브라우저 주소창에 `http` 또는 `https`를 직접 입력해야 할 수 있습니다.

root 계정의 패스워드를 분실한 경우, 장치를 공장 초기화 설정으로 재설정해야 합니다. 자세한 내용은 *공장 초기화 설정으로 재설정합니다, on page 23* 항목을 참조하십시오.

**IP 주소가 DHCP에 의해 변경됨**

DHCP 서버가 할당한 IP 주소는 유동 IP 주소이므로 변경될 수 있습니다. IP 주소가 변경된 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다. 해당 모델이나 일련 번호 또는 DNS 이름을 이용하여 장치를 식별합니다(이름이 구성된 경우).

필요한 경우, 고정 IP 주소를 수동으로 할당할 수 있습니다. 지침에 대한 자세한 내용은 *axis.com/support*로 이동하여 확인하십시오.

**IEEE 802.1X를 사용하는 동안 발생하는 인증 오류**

인증이 제대로 작동하려면 Axis 장치의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. **System (시스템) > Date and time(날짜 및 시간)**으로 이동합니다.

**브라우저가 지원되지 않음**

권장 브라우저 목록은 *브라우저 지원, on page 5*을 참조하십시오.

**외부에서 장치에 액세스할 수 없음**

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

- AXIS Camera Station Edge: 무료이며, 기본 감시가 필요한 소규모 시스템에 적합합니다.
- AXIS Camera Station Pro: 90일 무료 평가판이며, 중규모 시스템에 적합합니다.

지침 및 다운로드는 *axis.com/vms*로 이동하십시오.

### MQTT 관련 문제

**MQTT SSL 보안 포트 8883을 통해 연결할 수 없음**

방화벽이 8883 포트를 안전하지 않은 것으로 간주하여 이 포트를 사용하는 트래픽을 차단합니다.

경우에 따라 서버/브로커는 MQTT 통신에 필요한 특정 포트를 제공하지 않을 수도 있습니다. HTTP/HTTPS 트래픽에 보통 사용되는 포트를 통해 MQTT를 사용하는 것은 가능할 수 있습니다.

- 서버/브로커에서 주로 포트 443으로 지정되는 WS/WSS(WebSocket/WebSocket Secure) 프로토콜이 지원되는 경우 이를 대신 사용하십시오. WS/WSS가 지원되는지와 어느 포트 및 베이스패스를 사용할지는 서버/브로커 공급자에게 확인하십시오.
- 서버/브로커가 ALPN을 지원하는 경우, 443과 같은 개방형 포트를 통해 MQTT 사용을 협상할 수 있습니다. 서버/브로커 제공업체에 문의하여 ALPN이 지원되는지, 어떤 ALPN 프로토콜과 포트를 사용할지 확인합니다.

찾는 내용이 여기에 없는 경우에는 *axis.com/support*에서 장애 처리 섹션을 확인해 보십시오.

| 사운드 문제 | |
|---|---|
| 장치가 예상만큼 크지 않습니다. | 장치가 올바르게 닫혀 있고 혼이나 스피커 요소에 장애물이 없는지 확인하십시오. |
| 장치에서 소리가 나지 않음 | **Maintenance mode(유지 보수 모드)**에서 장치가 있는지 확인합니다. 유지 보수 모드에 있으면 끕니다. |

| 조명 문제 | |
|---|---|
| 장치가 예상만큼 밝지 않습니다. | PoE 클래스 4 전원 공급 장치를 사용하고 있는지 확인하십시오.<br>장치의 주변 온도를 확인합니다. 장치를 고온 환경에 설치하면 조명이 자동으로 어두워집니다. |

## 성능 고려 사항

고려해야 할 가장 중요한 요소:

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

## 지원 센터 문의

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

## 사이버 보안

사이버 보안은 위험을 최소화하여 성공적인 제품 수명 주기를 지원합니다. 당사의 사이버 보안 접근 방식에 대한 자세한 정보와 문서는*axis.com/about-axis/cybersecurity*에서 확인하실 수 있습니다. Axis로부터 제품 보안 알림을 수신하고, 제품의 안전한 수명 주기 및 폐기를 위해 제품을 구성하려면 아래의 사이버 보안 지침을 따르십시오.

*Axis Trust Center*에서 Axis가 보안 규정 준수, 투명성, 데이터 보호 및 개인정보 보호를 구현하는 방법에 대한 정보를 확인할 수 있습니다.

### 취약성 관리

Axis는 *공통 취약점 및 노출(CVE) 번호 부여 기관(Common Vulnerability and Exposures (CVE) Numbering Authority: CNA)*입니다. 노출 위험을 최소화하기 위해 Axis는 장치, 소프트웨어 및 서비스의 취약점을 식별하고 해결할 때 업계 표준을 따릅니다. Axis의 취약점 관리 정책에 대한 정보 또는 취약점 보고는 *axis.com/vulnerability-management*를 참조하십시오.

### 보안 알림

*axis.com/security-notification-service*에서 Axis 보안 알림 이메일을 구독하세요. 귀하가 사용 중인 Axis 제품과 관련된 취약점, 관련 보안 권고 사항 및 기타 보안 관련 정보를 보내드리겠습니다.

### 보안 제품 수명 주기

Axis는 보안 수명 주기 관리를 통해 제품 수명 전반에 걸쳐 위험을 최소화합니다. *help.axis.com*의 보안 강화 가이드를 사용하여 Axis 제품을 더 안전하게 구성하고 운영하며 다음에 대한 정보를 확인하십시오.

**안전한 최초 사용 -** Axis 제품은 처음부터 안전한 초기화와 암호화된 통신이 가능하도록 높은 기본 보호 수준으로 사전 구성되어 있습니다.

**용도 및 일반적인 구성 실수 -** Axis 보안 강화 가이드는 Axis 제품의 올바른 사용 방법에 대한 정보를 제공하며, 여기에는 피해야 할 일반적인 보안 관련 오용 및 구성 실수가 포함됩니다.

**취약점 관리 및 공급망 투명성 -** 취약점을 공개하고 공급망 투명성을 개선하기 위해 모든 소프트웨어 릴리스마다 *axis.com*에 소프트웨어 구성품 명세서(SBOM)가 게시됩니다.

**폐기 및 데이터의 안전한 삭제 -** 제품이 수명 주기 종료에 도달했을 때 안전하게 폐기하려면 제품을 공장 초기화 설정으로 재설정하십시오. 그러면 구성, 저장된 데이터 및 민감한 정보가 지워집니다.

T10223803_ko

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB