AXIS S3008 Mk II Recorder

사용자 설명서

장치 정보

AXIS S3008 Mk II Recorder는 설치가 쉬운 PoE 스위치가 내장된 소형 네트워크 비디오 레코더입니다. 이 장치에는 보안 감시 등급의 하드 드라이브가 있습니다. 또한 비디오 영상을 쉽게 내보낼 수 있는 USB 포트도 포함되어 있습니다. 레코더는 2TB, 4TB 또는 8TB 하드 드라이브를 비롯해 세 가지 모델로 제공됩니다.

레코더에 몇 대의 카메라를 연결할 수 있습니까?

레코더의 PoE 스위치에 최대 8 개의 장치를 연결할 수 있습니다.

레코더가 카메라에 얼마나 많은 전력을 공급할 수 있습니까?

PoE (Power over Ethernet)에 대한 제한 사항은 다음과 같습니다.

- 레코더는 PoE를 사용하여 최대 8 개의 장치를 지원합니다.
- 사용 가능한 총 전력량은 124W입니다.
- 각 네트워크 포트는 PoE 포트 (PSE)에서 최대 15.4W (PoE 클래스 3) 및 카메라 측 (PD)에서 12.95W를 지원합니다.
- 스위치는 연결된 장치의 PoE 클래스를 기반으로 PoE 전원을 할당합니다.

브라우저 지원

Windows®

- Chrome™(권장)
- Firefox®
- Edge®

OS X®

- Chrome™(권장)
- Safari®

기타

- Chrome™
- Firefox®

장치 사용 방법에 대한 자세한 내용은 *문서 | Axis Communications*에서 설명서를 참조하십시오.

권장하는 브라우저에 대한 자세한 내용은 *Axis OS 브라우저 지원 | Axis Communications*를 참조하십시오.

설치

AXIS S3008 Recorder Mk II는 AXIS Companion 영상 관리 소프트웨어의 버전 4와 함께 사용됩니다.

시작하기

비고

시스템 설정 시 인터넷 접속이 필요합니다.

1.
2.
3.
4.
5.

설치 완료 시:

- 시스템의 모든 Axis 장치에 최신 AXIS OS가 설치되어 있습니다.
- 모든 장치에는 패스워드가 있습니다.
- 기본 설정을 사용한 녹화가 활성화됩니다.
- 원격 액세스를 사용할 수 있습니다.

My Axis 계정 등록

1. *axis.com/my-axis/login*에서 **My Axis** 계정을 등록하십시오.
2. 다단계 인증(MFA) 방법으로 **Authenticator App (TOTP)(인증 앱(TOTP))** 또는 **Email(이메일)** 중 하나를 선택하고 화면의 안내를 따르십시오. MFA는 사용자의 신원을 확인하기 위해 또 하나의 인증 계층을 추가하는 보안 시스템입니다.

하드웨어 설치

1. 카메라 하드웨어를 설치하십시오.
2. LAN 포트를 통해 레코더를 네트워크에 연결하십시오.
3. 카메라를 레코더의 내장 PoE 스위치 또는 외부 PoE 스위치에 연결하십시오.
4. 컴퓨터를 레코더와 동일한 네트워크에 연결하십시오.
5. 전원을 레코더에 연결합니다.

중요 사항

먼저 전원 코드를 레코더에 연결한 다음 전원 코드를 콘센트에 연결해야 합니다.

6. 계속 진행하기 전에 레코더와 카메라가 부팅 될 때까지 몇 분 정도 기다리십시오.

⚠ 주의

과열을 피하려면 레코더를 통풍이 잘되는 환경과 레코더 주변에 충분 빈 공간을 두십시오.

AXIS Camera Station Edge 설치

1. *axis.com/products/axis-camera-station-edge*로 이동하여 **Download(다운로드)**를 클릭합니다.
2. 설치 파일을 열고 설정 도우미를 따릅니다.
3. *My Axis 계정*으로 로그인합니다.

사이트 생성

1. AXIS Camera Station Edge를 시작합니다.
2. *My Axis 계정*으로 로그인합니다.
3. **Create new site(사이트 새로 만들기)**를 클릭하고 사이트 이름을 지정합니다.

4. **Next (다음)**를 클릭합니다.
5. 사이트에 추가할 장치를 선택합니다.
6. **Next (다음)**를 클릭합니다.
7. 저장 장치를 선택합니다.
8. **Next (다음)**를 클릭합니다.
9. **Install(설치)**을 클릭하고 AXIS Camera Station Edge가 장치를 구성하는 동안 기다립니다. 구성은 몇 분 정도 걸릴 수 있습니다.

설치 완료 시:

- 시스템의 모든 Axis 장치에 최신 AXIS OS가 설치되어 있습니다.
- 모든 장치에는 패스워드가 있습니다.
- 기본 설정을 사용한 녹화가 활성화됩니다.
- 원격 액세스를 사용할 수 있습니다.

모바일 앱 설치

Android용

*다운로드*를 클릭하거나 다음 QR Code®를 스캔합니다.

iOS용

*다운로드*를 클릭하거나 다음 QR 코드를 스캔합니다.

AXIS Camera Station Edge 모바일 앱을 열고 Axis 자격 증명으로 로그인합니다.

My Axis 계정이 없으면 *axis.com/my-axis*로 이동하여 새 계정을 등록합니다.

QR Code는 일본 및 기타 국가에서 Denso Wave Incorporated의 등록 상표입니다.

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

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

시간 동기화 상태

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

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

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.

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.

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.

앱

Add app(앱 추가): 새 앱을 설치합니다.

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

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

AXIS OS 및 ACAP 앱의 보안 업데이트를 확인하십시오.

비고

동시에 여러 앱을 실행하면 장치의 성능에 영향을 미칠 수 있습니다.

앱 이름 옆에 있는 스위치를 사용하여 앱을 시작하거나 중지합니다.

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

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

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

시스템

시간과 장소

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

비고

장치의 날짜와 시간을 NTP 서버와 동기화하는 것이 좋습니다.

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

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

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

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

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.

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

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

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

DNS 서버

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

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

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

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):

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

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

호스트: 프록시 서버의 주소를 입력합니다.

Port(포트): 액세스에 사용되는 포트 번호를 입력하십시오.

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

Authentication method(인증 방법):

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

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

SNMP

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

SNMP: 사용할 SNMP 버전을 선택합니다.

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

비고

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

- **v3**: SNMP v3는 암호화 및 보안 암호를 제공하는 보다 안전한 버전입니다. SNMP v3를 사용하려면 암호가 HTTPS를 통해 전송되므로 HTTPS를 활성화하는 것이 좋습니다. 또한 권한이 없는 당사자가 암호화되지 않은 SNMP v1 및 v2c 트랩에 액세스하는 것을 방지합니다. SNMP v3를 사용하는 경우 SNMP v3 관리 애플리케이션을 통해 트랩을 설정할 수 있습니다.
  - **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.

네트워크 포트

PoE(Power over Ethernet)

- **Allocated power(할당된 전력)**: 현재 할당된 와트(W) 수입니다.
- **Total PoE consumption(총 PoE 소비량)**: 소비되는 와트(W) 수입니다.
- **Keep PoE active during recorder restart(레코더를 다시 시작하는 동안 PoE를 활성 상태로 유지)**: 레코더를 재시작하는 동안 연결된 장치에 전원을 공급하려면 이 옵션을 켭니다.

포트 이미지를 표시하거나 숨기려면 클릭합니다.

- 이미지에서 포트를 클릭하면 포트 목록에서 포트 세부 정보를 볼 수 있습니다.

포트 목록

- **Port(포트)**: 포트 번호.
- **PoE**: 포트에 대해 PoE를 켜거나 끕니다.
- **Network(네트워크)**: 각 포트에 대해 네트워크를 켜거나 끕니다.
- **Security(보안)**: 각 포트에 필요한 네트워크 보안 유형을 선택합니다.
- **Status(상태)**: 이 포트에 연결된 장치가 있는지 표시합니다.
- **Friendly name(친숙한 이름)**: 친숙한 이름이 **Network settings(네트워크 설정)**로 설정되어 있습니다. 기본 이름은 모델과 연결된 장치의 미디어 접근 제어 주소(MAC 주소)의 조합입니다.
- **전력 소비량**: 연결된 장치에서 현재 소비하고 할당하는 와트(W) 수입니다.

PoE(Power over Ethernet)

Allocated power(할당된 전력): 현재 할당된 와트(W) 수입니다.

Total PoE consumption(총 PoE 소비량): 소비되는 와트(W) 수입니다.

Keep PoE active during recorder restart(레코더를 다시 시작하는 동안 PoE를 활성 상태로 유지): 레코더를 재시작하는 동안 연결된 장치에 전원을 공급하려면 이 옵션을 켭니다.

Used space(사용된 공간): 사용된 공간의 백분율입니다.

Free space(여유 공간): 녹화에 사용할 수 있는 공간의 백분율입니다.

Free space(여유 공간): MB(메가바이트), GB(기가바이트) 또는 TB(테라바이트)로 표시된 사용 가능한 디스크 공간입니다.

디스크 상태: 현재 디스크 상태입니다.

Disk temperature(디스크 온도): 현재 작동 온도입니다.

PoE: 각 포트에 대해 PoE를 켜거나 끕니다. 장치가 연결되면 다음 정보가 표시됩니다.

- **Friendly name(친숙한 이름)**: 친숙한 이름이 **Network settings(네트워크 설정)**로 설정되어 있습니다. 기본 이름은 모델과 연결된 장치의 미디어 접근 제어 주소(MAC 주소)의 조합입니다.
- **전력 소비량**: 현재 소비되고 할당된 와트(W) 수입니다.

보안

인증서

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

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

지원되는 형식은 다음과 같습니다.

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

중요 사항

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

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

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

상황에 맞는 메뉴에는 다음이 포함됩니다.

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

Secure keystore(보안 키 저장소):

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

네트워크 접근 제어 및 암호화

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

인증서

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

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

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

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

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

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

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

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

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

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

- **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.

방화벽

Firewall(방화벽): 방화벽을 활성화하려면 켭니다.

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

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

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

+ New rule(새 룰 추가): 룰을 생성하려면 클릭합니다.

Rule type(룰 유형):

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

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

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

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

사용자 지정 서명된 AXIS OS 인증서

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

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

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

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

계정

가상 호스트

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

활성화: 이 가상 호스트를 사용하려면 선택합니다.

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

Port(포트): 서버가 연결된 포트를 입력합니다.

Type(유형): 사용할 인증 유형을 선택합니다. **기본**, **다이제스트**, **오픈 ID** 중에서 선택합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

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

비활성화: 서버가 비활성화되었습니다.

클라이언트 자격 증명 부여 구성

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

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

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

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

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

Save(저장): 값을 저장하려면 클릭합니다.

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.

수신 장치

이벤트에 대해 수신자에게 알리거나 파일을 보내도록 장치를 설정할 수 있습니다.

비고

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

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

비고

최대 20개의 수신자를 생성할 수 있습니다.

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

이름: 수신자의 이름을 입력합니다.

Type(유형): 목록에서 선택:

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

- **패스워드**: 로그인하려면 패스워드를 입력하십시오.

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

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

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

비고

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

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

Test(테스트): 설정을 테스트하려면 클릭합니다.

⋮ 상황에 맞는 메뉴에는 다음이 포함됩니다.

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

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

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

일정

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

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

수동 트리거

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

저장

온보드 스토리지

하드 드라이브

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

도구

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

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

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

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

로그

SSH 서버

Secure Shell (SSH)(보안 셸(SSH)): 활성화하면 사용자가 네트워크를 통해 안전하게 로그온하고 셸 및 네트워크 서비스를 수행할 수 있습니다.

유지보수

유지보수

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

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

중요 사항

복원 후 저장되는 유일한 설정은 다음과 같습니다.

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

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

비고

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

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

업그레이드할 때 다음 세 가지 옵션 중에서 선택할 수 있습니다.

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

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

문제 해결

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

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

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

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

네트워크 추적

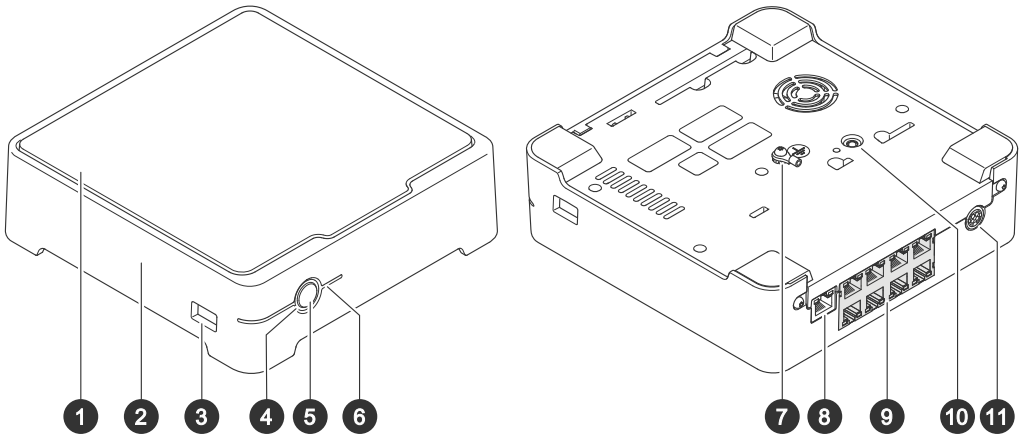
중요 사항

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

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

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

제품 개요



1 하드 드라이브
2 알람 버저
3 USB 포트
4 상태 LED
5 전원 버튼
6 하드 드라이브 LED
7 접지
8 LAN 포트
9 PoE 포트 (8x)
10 제어 버튼
11 전원 입력

전원 버튼

- 레코더를 종료하려면 버저에서 짧은 소리가 날 때까지 전원 버튼을 길게 누르십시오.
- 버저를 끄려면 전원 버튼을 짧게 누르십시오.

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. 을 참조하십시오.
- 인터넷을 통해 원 클릭 클라우드 연결(O3C) 서비스에 연결합니다. 연결하려면 상태 LED가 녹색으로 깜박일 때까지 약 3초 동안 이 버튼을 누르고 있습니다.

문제 해결

상태 LED는 다음 정보를 제공합니다.

상태 LED	표시
녹색	레코더가 켜져 있고 정상 상태입니다.
오렌지	레코더가 시작 중이거나 펌웨어가 업그레이드 중입니다. LED가 녹색으로 바뀔 때까지 기다리십시오.
빨간색	이는 PoE 최대 전력량이 초과되었음을 의미 할 수 있습니다. 장치를 레코더에 방금 연결 한 경우 다시 제거하십시오. 항목에서 PoE 제한에 대해 자세히 알아보십시오.

하드 드라이브 LED는 다음 정보를 제공합니다.

하드 드라이브 LED	표시
녹색	데이터가 하드 드라이브에 기록되면 LED가 녹색으로 깜박입니다.
빨간색	기록 중단이 발생했습니다. **시스템** > **스토리지**에서 자세한 내용을 알아보십시오.

이러한 이유로 버저 소리가 납니다.

- PoE 최대 전력량 초과. 장치를 방금 레코더에 연결한 경우 다시 제거합니다. 항목에서 PoE 제한에 대해 자세히 알아보십시오.

비고

전원 버튼을 짧게 누르면 버저를 멈출 수 있습니다.

레코더가 꺼지는 이유:

- 레코더가 심하게 과열되었습니다.

기술적 문제, 단서 및 해결 방안

발급자	솔루션
녹화물을 사용할 수 없습니다.	항목으로 이동합니다.
카메라에 연결할 수 없습니다.	항목으로 이동합니다.
“No contact(연락처 없음)” 오류 알림을 받습니다.	항목으로 이동합니다.
내 사이트가 모바일 앱에 나타나지 않습니다.	AXIS Companion 모바일 앱 버전 4가 있는지 확인하십시오.

일반적인 문제 해결

장치를 재시작, 구성 또는 재설정하기 전에 시스템 보고서를 저장하는 것이 권장됩니다.

을 참조하십시오.

1. 카메라와 레코더에 전원이 공급되는지 확인하십시오.
2. 인터넷에 연결되어 있는지 확인하십시오.
3. 네트워크가 작동하는지 확인하십시오.
4. 원격 상태가 아닌 경우 카메라가 컴퓨터와 동일한 네트워크에 연결되어 있는지 확인하십시오.

아직도 작동하지 않습니까?

5. 카메라, 레코더 및 AXIS Companion 데스크톱 앱에 최신 펌웨어 및 소프트웨어 업데이트가 설치되어 있는지 확인하십시오.
   를 참조하십시오.
6. AXIS Companion 데스크톱 앱을 재시작하십시오.
7. 카메라와 레코더를 재시작 하십시오.

아직도 작동하지 않습니까?

8. 카메라와 레코더를 하드 리셋하여 장치를 공장 초기화 상태로 되돌리십시오.
   을 참조하십시오.
9. 재설정된 카메라를 다시 사이트에 추가하십시오.

아직도 작동하지 않습니까?

10. 최신 드라이버로 그래픽 카드를 업데이트하십시오.

아직도 작동하지 않습니까?

11. 시스템 보고서를 저장하고 *Axis 기술 지원 서비스*에 문의하십시오.
    을 참조하십시오.

AXIS OS 업그레이드

새 장치 소프트웨어 업데이트는 최신의 향상된 특장점, 기능 및 보안 강화를 제공합니다.

1. 리더 장치의 웹 인터페이스로 이동합니다.
2. **Maintenance > AXIS OS upgrade(유지보수 > AXIS OS 업그레이드)**로 이동하여 **Upgrade (업그레이드)**를 클릭합니다.
3. 화면의 지침을 따릅니다.

레코더 하드 리셋

중요 사항

레코더가 켜진 상태에서는 조심스럽게 움직이십시오. 갑작스런 움직임이나 충격은 하드 드라이브에 손상을 입힐 수 있습니다.

비고

- 하드 리셋은 IP 주소를 포함한 모든 설정을 재설정합니다.
- 하드 리셋 시 녹화물을 제거하지 않습니다.

1. 레코더를 끕니다.
   신호음이 들릴 때까지 레코더 전면의 전원 버튼을 4~5초 동안 누릅니다.
2. 레코더가 꺼질 때까지 기다렸다가 뒤집어서 제어 버튼을 찾으십시오.
3. 제어 버튼을 길게 누릅니다. 전원 버튼을 눌렀다 떼어 레코더를 시작하십시오. 15-30초 후에 LED 표시기가 주황색으로 깜박이면 제어 버튼을 놓습니다.
4. 레코더를 조심스럽게 원위치에 두십시오.
5. 상태 LED 표시등이 녹색으로 바뀌면 과정이 완료됩니다. 제품이 공장 출하 시 기본 설정으로 재설정되었습니다. 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

6. 레코더에 연결된 장치를 재설정합니다.
7. 하드 드라이브가 암호화된 경우, 레코더를 재설정한 후 수동으로 장착해야 합니다.
   7.1. 장치의 웹 인터페이스로 이동합니다.
   7.2. **System(시스템)** > **Storage(스토리지)**로 들어가서 **Mount(설치)**를 클릭합니다.
   7.3. 하드 드라이브를 암호화 할 때 사용되는 암호화 패스워드를 입력합니다.

제품의 웹 인터페이스에 로그인할 수 없습니다

구성 중에 제품에 대한 패스워드를 설정한 후 나중에 해당 제품을 사이트에 추가하면 설정한 패스워드로 더 이상 제품의 웹 인터페이스에 로그인할 수 없습니다. AXIS Camera Station Edge가 사이트 내 모든 장치의 패스워드를 변경하기 때문입니다.

사이트 내 장치에 로그인하려면 사용자 이름 **root**와 사이트 패스워드를 입력하십시오.

모든 녹화물을 지우는 방법

1. 장치의 웹 인터페이스에서 **System(시스템)** > **Storage(스토리지)**로 이동합니다.
2. **Format(포맷)**을 선택하고 **Use tool(도구 사용)**을 클릭합니다.

비고

이 절차를 수행하면 하드 드라이브에서 모든 녹화물이 지워지지만 레코더와 사이트의 구성은 변경되지 않습니다.

Axis 지원 문의

문제 해결 방법을 시도했지만 성공하지 못했거나 문제에 대한 해결책을 찾을 수 없는 경우, *Axis 지원*에 문의하여 지원을 받으십시오.

시스템 보고서 저장:

1. AXIS S3008 Mk II Recorder에서  > **Save system report(시스템 보고서 저장)**로 이동합니다.
2. Axis 헬프데스크 에서 제출 할 때 시스템 보고서를 첨부하십시오.

도움이 더 필요하십니까?

유용한 링크

- *AXIS Companion 사용자 설명서*

지원 센터 문의

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

T10191657_ko

2025-10 (M10.2)