AXIS A9210 Network I/O Relay Module

사용자 설명서

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.

장치의 웹 인터페이스 열기

1. 브라우저를 열고 Axis 장치의 IP 주소 또는 호스트 이름을 입력합니다.
   IP 주소를 모르는 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다.
2. 사용자 이름과 패스워드를 입력합니다. 장치에 처음 액세스하는 경우, 관리자 계정을 생성해야 합니다. 을 참조하십시오.

에서 장치의 웹 인터페이스에서 볼 수 있는 모든 컨트롤과 옵션에 대한 설명을 살펴보십시오.

관리자 계정 생성

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 사용자 이름을 입력하십시오.
2. 패스워드를 입력합니다. 을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이센스 계약을 수락하십시오.
5. **Add account(계정 추가)**를 클릭합니다.

중요 사항

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

안전한 패스워드

중요 사항

네트워크를 통해 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.

장치 소프트웨어를 조작한 사람이 없는지 확인

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

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

웹 인터페이스 개요

이 영상은 장치의 웹 인터페이스에 대한 개요를 제공합니다.

Axis 장치 웹 인터페이스

장치 구성

I/O 포트 구성

1. **Device > I/Os and relays > AXIS A9210 > I/Os(장치 > I/O 및 릴레이 > AXIS A9210 > I/O)**로 이동합니다.
2. I/O 포트 설정을 확장하려면 을 클릭합니다.
3. 포트 이름을 바꾸십시오.
4. 정상 상태를 구성합니다. 개방 회로의 경우 을 클릭하고, 폐쇄 회로의 경우 을 클릭합니다.
5. I/O 포트를 입력으로 구성하려면 다음을 수행합니다.
   5.1. **Direction(방향)**에서 을 클릭합니다.
   5.2. 입력 상태를 모니터링하려면 **Supervised(관리됨)**를 켭니다. 을 참조하십시오.

   비고
   API에서 관리된 I/O 포트는 감독되는 입력 포트와 다르게 작동합니다. 자세한 내용은 *VAPIX® 라이브러리*를 참조하십시오.
6. I/O 포트를 출력으로 구성하려면 다음을 수행합니다.
   6.1. **Direction(방향)**에서 을 클릭합니다.
   6.2. 연결된 장치를 활성화 및 비활성화하는 URL을 보려면 **Toggle port URL(포트 URL 전환)**으로 이동합니다.

릴레이 구성

1. **Device > I/Os and relays > AXIS A9210 > Relays(장치 > I/O 및 릴레이 > AXIS A9210 > 릴레이)**로 이동합니다.
2. 릴레이 설정을 확장하려면 을 클릭합니다.
3. **Relay(릴레이)**를 켜십시오.
4. 릴레이 이름을 바꿉니다.
5. 릴레이를 활성화 및 비활성화하는 URL을 보려면 **Toggle port URL(포트 URL 전환)**로 이동합니다.

이벤트의 룰 설정

자세히 알아보려면 *이벤트 규칙 시작하기* 가이드를 확인하세요.

액션 트리거

1. **System > Events(시스템 > 이벤트)**로 이동하고 룰을 추가합니다. 룰은 장치가 특정 액션을 수행하는 시간을 정의합니다. 규칙을 예약, 반복 또는 수동 트리거로 설정할 수 있습니다.
2. **Name(이름)**을 입력합니다.
3. 작업을 트리거하려면 충족해야 하는 **Condition(조건)**을 선택합니다. 룰에 하나 이상의 조건을 지정하려면 모든 조건이 액션을 트리거하도록 충족해야 합니다.
4. 조건이 충족되었을 때 장치가 수행해야 하는 **Action(액션)**을 선택합니다.

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

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

비고

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

기본 메뉴를 표시하거나 숨깁니다.

릴리스 정보에 액세스합니다.

제품 도움말에 액세스합니다.

언어를 변경합니다.

밝은 테마 또는 어두운 테마를 설정합니다.

사용자 메뉴에는 다음이 포함됩니다.

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

상황에 맞는 메뉴에는 다음이 포함됩니다.

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

상태

장치 정보

AXIS OS 버전 및 일련 번호를 포함한 장치 정보를 표시합니다.

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

시간 동기화 상태

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

NTP settings(NTP 설정): NTP 설정을 보고 업데이트합니다. NTP 설정을 변경할 수 있는 **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.

장치

I/O 및 릴레이

입력

- **이름**: 포트 이름을 바꾸려면 텍스트를 편집합니다.
- **방향**: 입력 포트임을 나타냅니다.
- **Normal state(정상 상태)**: 개회로의 경우 을 클릭하고 폐회로의 경우 을 클릭합니다.
- **Supervised(관리됨)**: 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.
  - 병렬 우선 연결을 사용하려면 **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor(22KΩ 병렬 저항 및 4.7KΩ 직렬 저항으로 병렬 우선 연결)**를 선택합니다.
  - 직렬 우선 연결을 사용하려면 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 목록에서 저항 값을 선택합니다.

출력: 연결된 장치를 활성화하려면 켭니다.

- **이름**: 포트 이름을 바꾸려면 텍스트를 편집합니다.
- **방향**: 출력 포트임을 나타냅니다.
- **Normal state(정상 상태)**: 개회로의 경우 을 클릭하고 폐회로의 경우 을 클릭합니다.
- **Toggle port URL(포트 URL 전환)**: VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 연결된 장치를 활성화 및 비활성화하는 URL을 표시합니다.

I/O: 포트가 출력으로 구성된 경우 연결된 장치를 활성화하려면 켭니다.

- **이름**: 포트 이름을 바꾸려면 텍스트를 편집합니다.
- **방향**: 또는 을 클릭하여 입력 또는 출력으로 구성합니다.
- **Normal state(정상 상태)**: 개회로의 경우 을 클릭하고 폐회로의 경우 을 클릭합니다.
- **Supervised(관리됨)**: 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. 포트가 입력으로 구성된 경우에만 나타납니다.
  - 병렬 우선 연결을 사용하려면 **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor(22KΩ 병렬 저항 및 4.7KΩ 직렬 저항으로 병렬 우선 연결)**를 선택합니다.
  - 직렬 우선 연결을 사용하려면 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 목록에서 저항 값을 선택합니다.
- **Toggle port URL(포트 URL 전환)**: VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 연결된 장치를 활성화 및 비활성화하는 URL을 표시합니다. 포트가 출력으로 구성된 경우에만 나타납니다.

릴레이

- **Relay(릴레이)**: 릴레이를 켜거나 끕니다.
- **이름**: 릴레이 이름을 바꾸려면 텍스트를 편집합니다.
- **방향**: 출력 릴레이임을 나타냅니다.
- **Toggle port URL(포트 URL 전환)**: VAPIX® 애플리케이션 프로그래밍 인터페이스를 통해 릴레이를 활성화 및 비활성화하는 URL을 표시합니다.

알람

Device motion(장치 모션): 장치의 움직임이 감지될 때 시스템에서 알람을 트리거하려면 켭니다.

Casing open(케이스 열림) : 도어 컨트롤러의 케이스 열림을 감지하면 시스템에서 알람을 트리거하기 위해 켜십시오. barebone 도어 컨트롤러에 대해 이 설정을 끕니다.

External tamper(외부 변조) : 외부 변조가 감지될 때 시스템에서 알람을 트리거하려면 켭니다. 예를 들어 누군가 외부 캐비닛을 열거나 닫을 때가 해당됩니다.

- **Supervised input(관리형 입력)** : 입력 상태를 모니터링하고 EOL 저항기를 구성하려면 켭니다.
  - 병렬 우선 연결을 사용하려면 **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor(22KΩ 병렬 저항 및 4.7KΩ 직렬 저항으로 병렬 우선 연결)**를 선택합니다.
  - 직렬 우선 연결을 사용하려면 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 목록에서 저항 값을 선택합니다.

주변장치

센서

연결된 센서의 개요를 표시합니다. RS485 커넥터를 통해 최대 8개의 Modbus 센서를 직접 연결하거나, 최대 16개의 *AXIS A9910* I/O 릴레이 확장 모듈로 확장하여 단일 PoE 케이블을 통해 총 128개의 I/O 및 64개의 릴레이를 사용할 수 있습니다.

- **Name(이름):** 센서 이름을 바꾸려면 텍스트를 편집합니다.
- **Device/Port(장치/포트):** 센서가 연결된 Modbus ID 및 포트 번호입니다.
- **Type(유형):** 온도, 습도 또는 휘도 등 센서가 수행하는 측정 또는 기능의 유형입니다.
- **Model(모델):** 센서의 모델명입니다.
- **Last value(마지막 값):** 센서의 가장 최근 측정값입니다.
- **Last event(마지막 이벤트):** 선택한 매개변수에 대해 설정된 한계값 초과 또는 미달과 같이 마지막으로 트리거된 이벤트의 원인입니다.
- **Status(상태):** 센서가 현재 온라인 상태인지 오프라인 상태인지 표시합니다.

앱

Add app(앱 추가): 새 앱을 설치합니다.

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

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

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.

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.

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.

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.

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.

상세 정보

사이버 보안

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

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

Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 장치의 ID 및 무결성을 보장하고 무단 액세스로부터 중요한 정보를 보호하는 기능을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

Signed OS

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

Secure Boot

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

보안 키 저장소

개인 키 보호 및 암호화 작업의 안전한 실행을 위한 변조 방지 환경입니다. 보안 침해 발생 시 무단 액세스 및 악의적인 추출을 방지합니다. 보안 요구 사항에 따라, Axis 장치에는 하드웨어로 보호되는 보안 키 저장소를 제공하는 하드웨어 기반 암호화 컴퓨팅 모듈이 하나 또는 여러 개 있을 수 있습니다. 보안 요구 사항에 따라 Axis 장치에는 TPM 2.0(Trusted Platform Module)이나 보안 요소 및/또는 하드웨어를 제공하는 TEE(Trusted Execution Environment)와 같은 하드웨어 기반 암호화 컴퓨팅 모듈이 하나 또는 여러 개 있을 수 있으며, 이는 하드웨어로 보호되는 보안 키 저장소를 제공합니다. 또한 일부 Axis 제품에는 FIPS 140-2 레벨 2 인증 보안 키 저장소가 있습니다.

Axis device ID

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

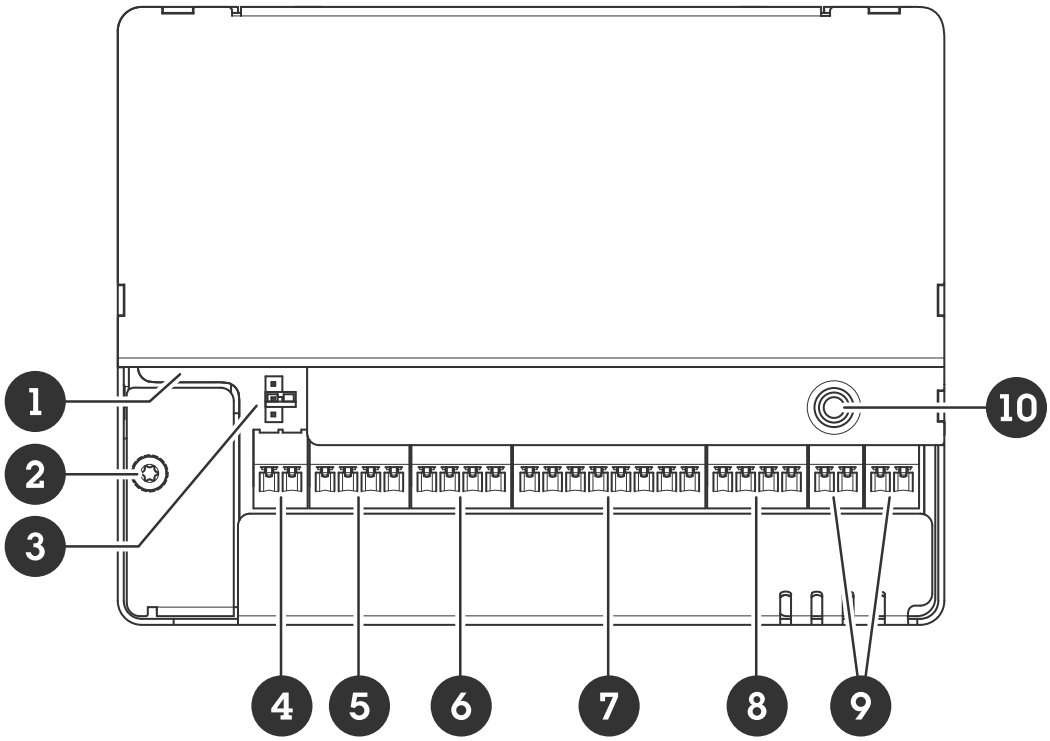
암호화된 파일 시스템

보안 키 저장소는 파일 시스템에 강력한 암호화를 적용하여 악의적인 정보 유출을 방지하고 구성 변조를 방지합니다. 이렇게 하면 장치를 사용하지 않거나 장치에 대한 인증되지 않은 액세스가 이루어지거나 Axis 장치를 도난당했을 때 파일 시스템에 저장된 데이터를 추출하거나 탬퍼링할 수 없습니다. Secure Boot 프로세스 중에 읽기-쓰기 파일 시스템이 해독되어 Axis 장치에서 마운트하고 사용할 수 있습니다.

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

사양

제품 개요



1 네트워크 커넥터
2 접지 위치
3 릴레이 점퍼
4 전원 커넥터
5 릴레이 커넥터
6 입력 1 커넥터
7 RS485 및 I/O 커넥터
8 I/O 커넥터
9 입력 2 커넥터
10 제어 버튼

LED 표시

LED	색상	표시
상태	녹색	정상 작동 시 녹색이 계속 표시됩니다.
	주황색	시작 시 및 설정값 복원 시 켜져 있습니다.
	빨간색	업그레이드 실패하면 느리게 깜박입니다.
네트워크	녹색	100Mbit/s 네트워크에 연결된 경우 켜져 있습니다. 네트워크 작업 시 깜박입니다.
	주황색	10Mbit/s 네트워크에 연결된 경우 켜져 있습니다. 네트워크 작업 시 깜박입니다.

	켜져 있지 않음	네트워크 연결이 없습니다.
전원	녹색	정상 작동 중입니다.
	주황색	펌웨어 업그레이드 중에는 녹색/주황색으로 깜박입니다.
릴레이	녹색	릴레이 활성화.[1]
	켜져 있지 않음	릴레이가 비활성화되었습니다.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

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

커넥터

네트워크 커넥터

PoE+(Power over Ethernet Plus)를 지원하는 RJ45 이더넷 커넥터

UL: PoE(Power over Ethernet)에 Ethernet IEEE 802.3af/802.3at Type 1 Class 3 또는 PoE+(Power over Ethernet Plus) IEEE 802.3at Type 2 Class 4 전력 제한 인젝터(44 ~ 57V DC, 15.4W/30W 제공)로 전원을 공급해야 합니다. PoE(Power over Ethernet)는 AXIS T8133 Midspan 30 W 1-port를 사용하여 UL에 의해 평가되었습니다.

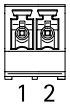
전원 우선 순위

이 장치는 PoE 또는 DC 입력으로 전원을 공급받을 수 있습니다. 자세한 내용은 및 항목을 참조하십시오.

- 장치에 전원이 공급되기 전에 PoE와 DC가 모두 연결된 경우, 전원 공급에 PoE를 사용합니다.
- PoE와 DC가 모두 연결되어 있으며 현재 PoE에 전원이 공급되고 있습니다. PoE가 끊기면 장치는 재시작하지 않고 DC로 전원을 공급합니다.
- PoE와 DC가 모두 연결되어 있고, 현재 PoE에 전원이 공급되고 있습니다. DC가 끊기면 장치가 재시작되고 PoE로 전원을 공급합니다.
- 시동 중에 DC를 이용하고 장치를 시동한 후 PoE를 연결하면 전원 공급에 DC를 사용합니다.
- 시동 중에 PoE를 이용하고 장치를 시동한 후 DC를 연결하면 전원 공급에 PoE를 사용합니다.

전원 커넥터

DC 전원 입력용 2핀 단자대입니다. 정격 출력 전력이 ≤100W로 제한되거나 정격 출력 전류가 ≤5A로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.



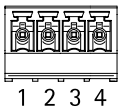
1. *COM*이 *NO*에 연결되면 릴레이가 활성화됩니다.

기능	핀	비고	사양
DC 접지(GND)	1		0V DC
DC 입력	2	PoE(Power over Ethernet) 미사용 시 장치에 전원을 공급하는 데 사용됩니다. 참고: 이 핀은 전원이 공급된 경우에만 사용할 수 있습니다.	12V DC, 최대 36W

UL: 적용 분야에 따라 UL 603 등재 전원 공급 장치에 적절한 정격의 DC 전원이 공급됩니다.

릴레이 커넥터

예를 들어 잠금 장치 또는 게이트에 대한 인터페이스를 제어하는 데 사용할 수 있는 C형 릴레이를 위한 1개의 4핀 터미널 블록입니다. 예를 들어 잠금과 같은 유도 부하와 함께 사용할 경우, 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.



기능	핀	비고	사양
DC 접지(GND)	1		0V DC
NO	2	정상 개방. 릴레이 장치 연결에 사용됩니다. NO와 DC 접지 사이에 페일 시큐어 잠금 장치를 연결합니다. 점퍼를 사용하지 않더라도, 릴레이 핀 2개는 나머지 회로와 전기적으로 분리됩니다.	최대 전류 = 2A 최대 전압 = 30V DC
COM	3	공통	
NC	4	정상 폐쇄 릴레이 장치 연결에 사용됩니다. NC와 DC 접지 사이에 페일 세이프 잠금 장치를 연결합니다. 점퍼를 사용하지 않더라도, 릴레이 핀 2개는 나머지 회로와 전기적으로 분리됩니다.	

릴레이 전원 점퍼

릴레이 전원 점퍼를 장착한 경우 12V DC 또는 24V DC를 릴레이 COM 핀에 연결합니다.

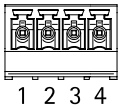
GND와 NO 핀 또는 GND와 NC 핀 사이에 잠금 장치를 연결하는 데 사용할 수 있습니다.

전원	12V DC에서의 최대 전력	24V DC에서의 최대 전력
DC IN	2,000mA	1,000mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

입력 1 커넥터

입력용 4핀 터미널 블록 1개.

EOL 레지스터를 통한 관리를 지원합니다. 연결이 중단되면 알람이 트리거됩니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 관리된 입력에 대한 연결 다이어그램을 사용합니다. 을 참조하십시오.



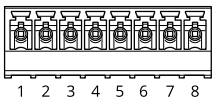
기능	핀	비고	사양
DC 접지	1, 3		0V DC
입력	2, 4	디지털 입력 또는 관리된 입력 - 활성화하려면 각각 핀 1 또는 3에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC

중요 사항

다음 케이블 요구 사항 AWG 24가 충족되는 경우 적격 케이블 길이는 최대 200m(656ft)입니다.

RS485 및 I/O 커넥터

4핀 RS485 및 4핀 I/O를 포함하는 8핀 터미널 블록 1개.



RS485

기능	핀	비고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	Modbus 센서와 같은 보조 장치에 전원을 공급합니다.	12V DC, 최대 200mA
A	3		
B	4		

I/O

기능	핀	비고	사양
디지털 출력	5	예를 들어 릴레이와 같은 유도 부하와 함께 사용할 경우, 전압 과도	0 ~ 최대 30V DC, 개방 드레인, 100mA

		현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	
디지털 출력	6	예를 들어 릴레이와 같은 유도 부하와 함께 사용할 경우, 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA
입력	7	디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC
디지털 출력	8	예를 들어 릴레이와 같은 유도 부하와 함께 사용할 경우, 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

중요 사항

- RS485의 허용 가능한 케이블 길이는 최대 1000m(3281ft)이며, 다음 케이블 요구 사항을 충족해야 합니다: 차폐 연선 1쌍, AWG 24, 120옴 임피던스.
- I/O에 적합한 케이블 길이는 최대 200m(656피트)입니다.

I/O 커넥터

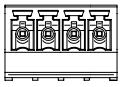
모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 보조 커넥터를 사용합니다. 보조 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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

관리된 입력 - 디지털 입력에 대한 탬퍼링을 감지할 수 있습니다.

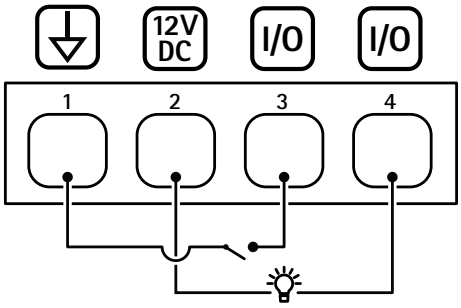
디지털 출력 - 릴레이 및 LED와 같은 외부 장치 연결용. 연결된 장치는 VAPIX® Application Programming Interface 또는 제품 웹페이지에서 활성화할 수 있습니다.

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 = 총 50mA

구성 가능(입력 또는 출력)	3–4	디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 레지스터를 연결하는 방법에 대한 자세한 내용은 연결 다이어그램을 참조하십시오.	0 ~ 최대 30V DC
		디지털 출력 - 활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도성 부하와 함께 사용하는 경우, 전압 과도 상태로부터 보호하기 위해 부하와 병렬로 다이오드를 연결합니다. 내부 12V DC 출력(핀 2)을 사용하는 경우 I/O는 12V DC, 50mA(결합 최대)의 외부 부하를 구동할 수 있습니다. 외부 전원 공급 장치와 함께 개방 드레인 연결을 사용하는 경우 I/O가 각각 DC 공급 0~30V DC, 100mA를 관리할 수 있습니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

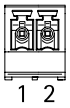


1 DC 접지
2 DC 출력 12V
3 I/O가 입력으로 구성됨
4 I/O가 출력으로 구성됨

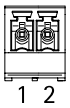
입력 2 커넥터

유리 파손 감지기 또는 화재 감지기와 같은 외부 장치용 2핀 터미널 블록 2개입니다.

UL: 절도범 또는 화재 알람용 UL에 의해 커넥터가 평가되지 않았습니다.



기능	핀	비고	사양
DC 접지	1		0V DC
입력	2	디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC



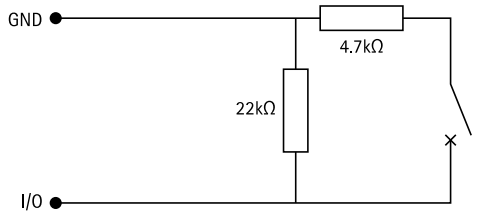
기능	핀	비고	사양
DC 접지	1		0V DC
입력	2	디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC

관리된 입력

관리된 입력을 사용하려면 아래의 다이어그램에 따라 EOL 레지스터를 설치하십시오.

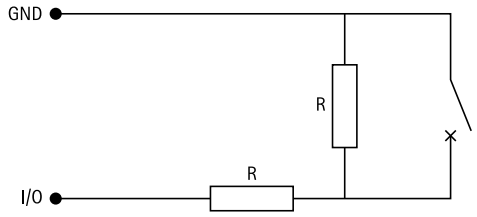
병렬 우선 연결

저항 값은 4.7kΩ 및 22kΩ이어야 합니다.



직렬 우선 연결

저항 값은 동일해야 하며 가능한 값은 1kΩ, 2.2kΩ, 4.7kΩ 및 10kΩ, 1%, ¼와트 표준입니다.



비고

트위스트 및 차폐 케이블을 사용하는 것이 좋습니다. 차폐물을 0V DC에 연결하십시오.

상태	설명
개방적	감시되는 스위치가 개방 모드에 있습니다.
종료됨	감시되는 스위치가 폐쇄 모드에 있습니다.
단락	I/O 또는 입력 1~5 케이블이 GND에 단락되었습니다.
차단	I/O 또는 입력 1~5 케이블이 절단되어 GND에 대한 전류 경로 없이 열린 상태로 유지됩니다.

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 25초 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.

AXIS OS 옵션

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

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

현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

AXIS OS 업그레이드

중요 사항

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

비고

활성 트랙의 최신 AXIS OS 버전으로 장치를 업그레이드하면 제품이 사용 가능한 최신 기능을 수신합니다. 업그레이드하기 전에 항상 새 릴리스마다 제공되는 릴리즈 정보와 업그레이드 지침을 참

조하십시오. 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 다운로드 합니다.
2. 장치에 관리자로 로그인합니다.
3. **Maintenance > AXIS OS upgrade(유지보수 > AXIS OS 업그레이드)**로 이동하여 **Upgrade (업그레이드)**를 클릭합니다.

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

기술적 문제, 단서 및 해결 방안

찾는 내용이 여기에 없는 경우에는 *axis.com/support*에서 문제 해결 섹션을 확인해 보십시오.

AXIS OS 업그레이드 문제

AXIS OS 업그레이드 실패	업그레이드에 실패하면 장치가 이전 버전을 다시 로드합니다. 가장 일반적인 원인은 잘못된 AXIS OS 파일이 업로드된 것입니다. 장치에 해당하는 AXIS OS 파일 이름을 확인하고 다시 시도하십시오.
AXIS OS 업그레이드 후 문제	업그레이드 후 문제가 발생하면 **Maintenance(유지보수)** 페이지에서 이전에 설치된 버전으로 롤백하십시오.

IP 주소 설정 문제

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

장치를 브라우저에서 액세스할 수 없음

로그인할 수 없음	HTTPS가 활성화된 경우 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 필드에 `http` 또는 `https`를 수동으로 입력해야 할 수도 있습니다. root 계정의 패스워드를 분실한 경우에는 장치를 공장 출하 시 기본값으로 재설정해야 합니다. 을 참조하십시오.

IP 주소가 DHCP에 의해 변경됨	DHCP서버에서 획득한 IP 주소는 동적이며 변경될 수 있습니다. IP 주소가 변경된 경우에는 AXIS IP Utility 또는 AXIS Device Manager를 사용하여 네트워크에서 장치를 찾습니다. 해당 모델이나 일련 번호 또는 DNS 이름을 이용하여 장치를 식별합니다(이름이 구성된 경우). 필요한 경우 고정 IP 주소를 수동으로 할당할 수 있습니다. 지침에 대한 자세한 내용은 *axis.com/support*로 이동하여 확인하십시오.
IEEE 802.1X를 사용하는 동안 발생하는 인증 오류	인증이 제대로 작동하려면 Axis 장치의 날짜 및 시간이 NTP 서버와 동기화되어야 합니다. **System > Date and time(시스템 > 날짜 및 시간)**으로 이동합니다.

장치에 로컬로 액세스할 수 있지만 외부에서 액세스할 수 없음

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

- AXIS Camera Station Edge: 무료이며, 기본 감시가 필요한 소규모 시스템에 적합합니다.
- AXIS Camera Station 5: 30일 무료 평가판이며, 중규모 시스템에 적합합니다.
- AXIS Camera Station Pro: 90일 무료 평가판이며, 중규모 시스템에 적합합니다.

지침 및 다운로드는 *axis.com/vms*로 이동합니다.

MQTT SSL 보안 포트 8883을 통해 연결할 수 없음

포트 8883을 사용하는 트래픽은 안전하지 않다고 간주되어 방화벽에서 차단됩니다.	경우에 따라 서버/브로커는 MQTT 통신에 필요한 특정 포트를 제공하지 않을 수도 있습니다. 그래도 HTTP/HTTPS 트래픽에 일반적으로 사용되는 포트를 통해 MQTT를 사용할 수 있습니다. • 서버/브로커에서 주로 포트 443으로 지정되는 WS/WSS(WebSocket/WebSocket Secure) 프로토콜이 지원되는 경우 이를 대신 사용하십시오. WS/WSS가 지원되는지와 어느 포트 및 베이스패스를 사용할지는 서버/브로커 공급자에게 확인하십시오. • 서버/브로커가 ALPN을 지원하는 경우, 443과 같은 개방형 포트를 통해 MQTT 사용을 협상할 수 있습니다. 서버/브로커 제공업체에 문의하여 ALPN이 지원되는지, 어떤 ALPN 프로토콜과 포트를 사용할지 확인합니다.

지원 센터 문의

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

T10202445_ko

2025-05 (M4.3)

© 2023 – 2025 Axis Communications AB