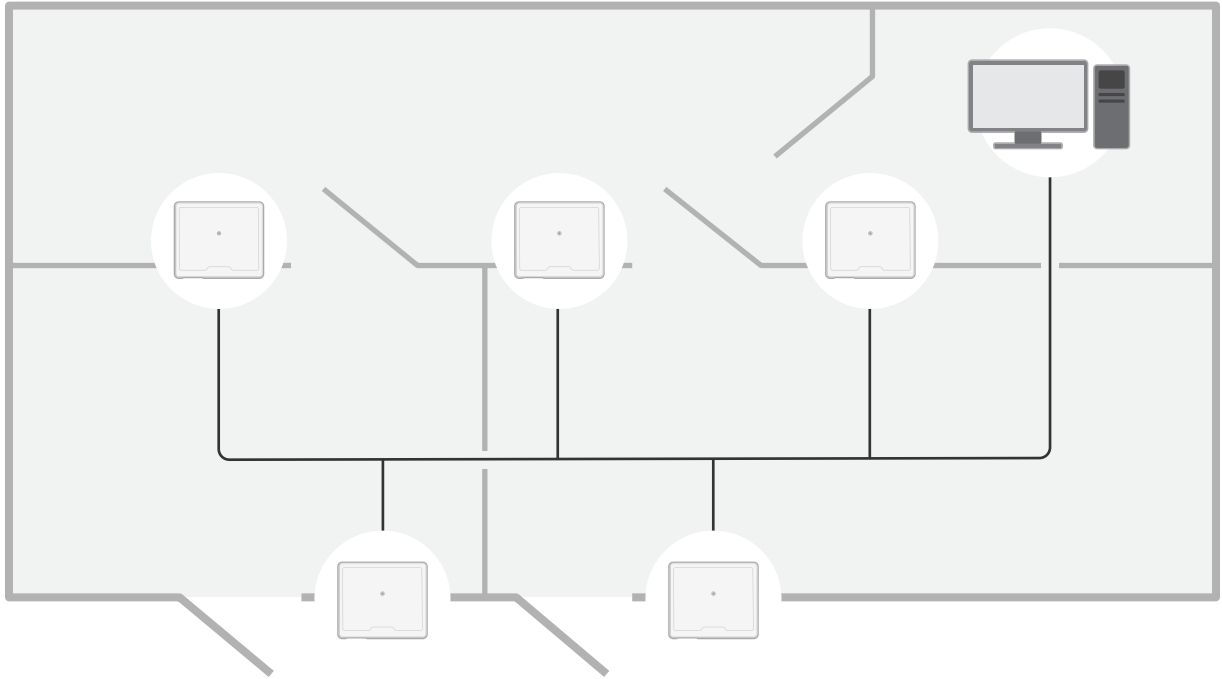


AXIS A1210 Network Door Controller

AXIS A1210-B Network Door Controller

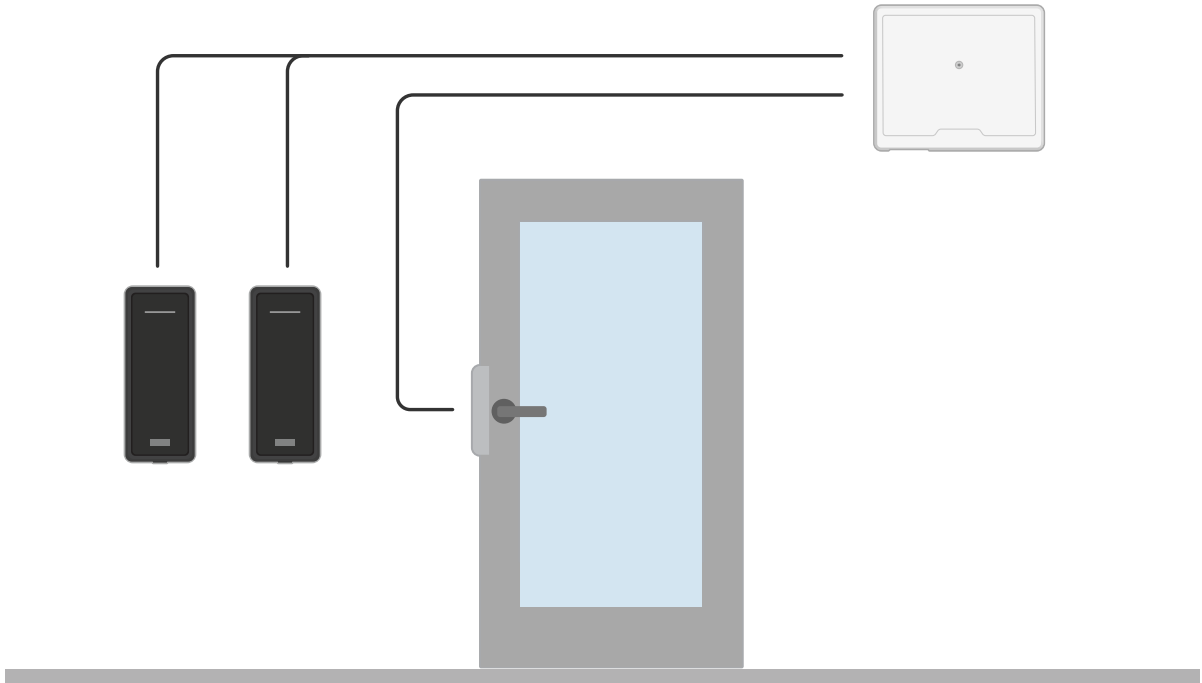
사용자 설명서

솔루션 개요



특별한 배선 없이 네트워크 도어 컨트롤러에 쉽게 연결하고 기존의 IP 네트워크로 전원을 공급할 수 있습니다.

솔루션 개요



각 네트워크 도어 컨트롤러는 도어 근처에 쉽게 장착할 수 있는 지능형 장치입니다. 최대 2개의 리더에 전원을 공급하고 제어할 수 있습니다.

설치



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

help.axis.com/?&pid=74266§ion=solution-overview

시작하기

네트워크에서 장치 찾기

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

IP 주소를 찾아 할당하는 방법에 대한 자세한 내용은 [IP 주소를 할당하고 장치에 액세스하는 방법](#)에 방문하십시오.

브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

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

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

권장되는 브라우저에 대한 자세한 정보가 필요하면 [AXIS OS Portal](#)로 이동하십시오.

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. [관리자 계정 생성 페이지 6](#) 항목을 참조하십시오.

관리자 계정 생성

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 사용자 이름을 입력합니다.
2. 패스워드를 입력합니다. [안전한 패스워드 페이지 6](#)을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. **Add user(사용자 추가)**를 클릭합니다.

중요 사항

장치에 기본 계정이 없습니다. 관리자 계정의 패스워드를 잊어버린 경우, 장치를 재설정해야 합니다. [공장 출하 시 기본 설정으로 재설정 페이지 30](#) 항목을 참조하십시오.

안전한 패스워드

중요 사항

Axis 장치가 초기에 설정된 패스워드를 평문 형식으로 네트워크를 통해 전송합니다. 처음 로그인한 후 장치를 보호하려면 안전하고 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.

펌웨어를 조작한 사람이 없는지 확인

장치에 원래 Axis 펌웨어가 있는지 확인하거나 보안 공격 후 장치를 완전히 제어하려면:

1. 공장 출하 시 기본 설정으로 재설정합니다. *공장 출하 시 기본 설정으로 재설정 페이지 30* 항목을 참조하십시오.
재설정 후 보안 부팅은 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

웹 인터페이스 개요

이 비디오는 장치의 웹 인터페이스에 대한 개요를 제공합니다.



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

help.axis.com/?&pid=74266§ion=web-interface-overview

Axis 장치 웹 인터페이스

장치 구성


장치 구성










장치를 구성하는 방법은 *AXIS Camera Station 사용자 설명서* 또는 타사 솔루션을 참조하십시오.

웹 인터페이스

장치의 웹 인터페이스에 접근하려면 웹 브라우저에 장치의 IP 주소를 입력하십시오.

참고

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

-  기본 메뉴를 표시하거나 숨깁니다.
-  릴리스 노트에 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.
 - Analytics data(분석 데이터)**: 개인용이 아닌 브라우저 데이터를 공유하려면 수락하십시오.
 - Feedback(피드백)**: 사용자 경험을 개선하는 데 도움이 되는 피드백을 공유하십시오.
 - Legal(법률)**: 쿠키 및 라이선스에 대한 정보를 봅니다.
 - About(정보)**: 펌웨어 버전 및 일련 번호를 포함한 장치 정보를 봅니다.
 - Legacy device interface(레거시 장치 인터페이스)**: 장치의 웹 인터페이스를 레거시 버전으로 변경합니다.

Status(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 **Date and time(날짜 및 시간)** 페이지로 이동합니다.

장치 정보

펌웨어 버전 및 일련 번호를 포함한 장치 정보를 표시합니다.

Upgrade firmware(펌웨어 업그레이드): 장치의 펌웨어를 업그레이드합니다. 펌웨어 업그레이드를 수행할 수 있는 유지 관리 페이지로 이동합니다.

접근 제어

알람

장치 모션: 도어 컨트롤러의 움직임이 감지될 때 시스템에서 알람을 트리거하려면 켭니다.

케이스 열기: 도어 컨트롤러의 케이스 열림을 감지하면 시스템에서 알람을 트리거하기 위해 켜십시오. 베어본 도어 컨트롤러에 대해서는 이 설정을 끕니다.

외부 탬퍼: 외부 탬퍼가 감지될 때 시스템에서 알람을 트리거하려면 켭니다. 예를 들어 누군가 외부 캐비닛을 열거나 닫을 때가 해당됩니다.

- **관리된 입력:** 입력 상태를 모니터링하고 EOL 저항기를 구성하려면 켭니다.
 - 병렬 첫 번째 연결을 사용하려면 **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor**(22K Ω 병렬 저항과 4.7K Ω 직렬 저항을 사용한 병렬 첫 번째 연결)를 선택하십시오.
 - 직렬 첫 번째 연결을 사용하려면 **Serial first connection**(직렬 첫 번째 연결)을 선택하고 **Resistor values**(저항 값) 드롭 다운 목록에서 저항 값을 선택합니다.

주변장치

리더 업그레이드: 새 펌웨어 버전으로 리더를 업그레이드하려면 클릭합니다. 이 기능은 지원되는 리더가 온라인 상태일 때만 업그레이드할 수 있습니다.

시스템

시간 및 위치

날짜 및 시간

시간 형식은 웹 브라우저의 언어 설정에 따라 다릅니다.

참고

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.
- **Automatic date and time (NTP server using DHCP)(자동 날짜 및 시간(DHCP를 사용하는 NTP 서버)):** DHCP 서버에 연결된 NTP 서버와 동기화합니다.
 - **대체 NTP 서버:** 하나 또는 두 개의 대체 서버의 IP 주소를 입력합니다.
- **Automatic date and time (manual NTP server)(자동 날짜 및 시간(수동 NTP 서버)):** 선택한 NTP 서버와 동기화하십시오.
 - **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.
- **Custom date and time(사용자 정의 날짜 및 시간):** 수동으로 날짜 및 시간을 설정합니다. **Get from system**(시스템에서 가져오기)을 클릭하여 컴퓨터 또는 모바일 장치에서 날짜 및 시간 설정을 한 차례 가져옵니다.

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

참고

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

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

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

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

참고

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.

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

DNS 서버

Assign DNS automatically(DNS 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)**를 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. **System > Security(시스템 > 보안)**로 이동하여 인증서를 생성하고 설치합니다.

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

참고

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 선택하십시오.

네트워크 검색 프로토콜

Bonjour®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

UPnP®: 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

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

WS-Discovery(WS-검색): 네트워크에서 자동 검색을 허용하려면 이 옵션을 켭니다.

One-Click Cloud Connection

One-click cloud connection(O3C)과 O3C 서비스는 어느 위치에서나 라이브 및 녹화 된 비디오에 쉽고 안전한 인터넷 액세스를 제공합니다. 이 서비스에 대한 자세한 내용은 axis.com/end-to-end-solutions/hosted-services를 참조하십시오.

Allow O3C(O3C 허용):

- **One-click(원클릭):** 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.
- **Always(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.
- **No(아니요):** O3C 서비스를 비활성화합니다.

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

Host(호스트): 프록시 서버의 주소를 입력합니다.

Port(포트): 액세스에 사용되는 포트 번호를 입력하십시오.

Login(로그인) 및 Password(패스워드): 필요한 경우 프록시 서버에 대한 사용자 이름 및 패스워드를 입력합니다.

Authentication method(인증 방법):

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

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

SNMP

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

SNMP: 사용할 SNMP 버전을 선택합니다.

- **v1 and v2c(v1 및 v2c):**

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

참고

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 v3을 사용하려면 패스워드가 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.

Connected clients(연결된 클라이언트)

연결 및 연결된 클라이언트 수를 표시합니다.

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

보안

인증서

인증서는 네트워크에서 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 발급 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.



목록에서 인증서를 필터링하십시오.



Add certificate(인증서 추가): 인증서를 추가하려면 클릭합니다.

- **More(추가)** : 작성하거나 선택할 추가 필드를 표시합니다.
- **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-support로 이동하십시오.
- **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.

보안 키 저장소 ⓘ :

- **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.

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)을 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.

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.

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

CA Certificate(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.

Prevent brute-force attacks(무차별 대입 공격 방지)

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

Blocking period(차단 기간): 무차별 대입 공격을 차단할 시간(초)을 입력합니다.

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

IP 주소 필터

Use filter(필터 사용): 장치에 액세스할 수 있는 IP 주소를 필터링하려면 선택합니다.

Policy(정책): 특정 IP 주소에 대한 접근을 허용할지 또는 거부할지 선택합니다.

주소: 장치에 대한 접근이 허용되거나 거부된 IP 번호를 입력합니다. CIDR 형식을 사용할 수도 있습니다.

사용자 정의 Signed Firmware 인증서

장치에 Axis의 테스트 펌웨어 또는 기타 사용자 지정 펌웨어를 설치하려면 사용자 지정 서명 펌웨어 인증서가 필요합니다. 인증서는 펌웨어가 장치 소유자와 Axis 모두에 의해 승인되었는지 확인합니다. 펌웨어는 고유한 일련 번호와 칩 ID로 식별되는 특정 장치에서만 실행할 수 있습니다. Axis만이 사용자 정의 서명 펌웨어의 인증서를 생성할 수 있으므로, Axis만 해당 인증서를 작성할 수 있습니다.

설치: 인증서를 설치하려면 클릭합니다. 펌웨어를 설치하기 전에 인증서를 설치해야 합니다.

Accounts(계정)

Accounts(계정)

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

Account(계정): 고유한 계정 이름을 입력합니다.

New password(새 비밀번호): 계정의 비밀번호를 입력합니다. 비밀번호는 1~64자 길이어야 합니다. 문자, 숫자, 구두점, 일부 기호 등 인쇄 가능한 ASCII 문자(코드 32~126)만 비밀번호에 사용할 수 있습니다.

Repeat password(비밀번호 반복): 동일한 비밀번호를 다시 입력합니다.

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.

- 앱 추가.
- **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.

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 펌웨어의 MQTT 클라이언트를 통해 장치에서 생성된 데이터 및 이벤트를 영상 관리 소프트웨어(VMS)가 아닌 시스템에 간편하게 통합할 수 있습니다.

장치를 MQTT 클라이언트로 설정합니다. MQTT 통신은 클라이언트와 브로커라는 두 엔티티를 기반으로 합니다. 클라이언트는 메시지를 보내고 받을 수 있습니다. 브로커는 클라이언트 간의 메시지 라우팅을 담당합니다.

*AXIS OS Porta*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 client(MQTT 클라이언트)

Connect(연결): MQTT 클라이언트를 켜거나 끕니다.

Status(상태): MQTT 클라이언트의 현재 상태를 표시합니다.

Broker(브로커)

Host(호스트): MQTT 서버의 호스트 이름 또는 IP 주소를 입력하십시오.

Protocol(프로토콜): 사용할 프로토콜을 선택합니다.

Port(포트): 포트 번호를 입력합니다.

- 1883은 TCP를 통한 MQTT의 기본값입니다.
- 8883은 SSL를 통한 MQTT의 기본값입니다.
- 80은 웹 소켓을 통한 MQTT의 기본값입니다.
- 443은 웹 소켓 보안을 통한 MQTT의 기본값입니다.

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

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

Password(패스워드): 사용자 이름의 패스워드를 입력합니다.

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

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

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.

Connect message(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 선택하십시오.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

Last Will and Testament message(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 선택하십시오.

QoS: 패킷 흐름에 대한 QoS 계층을 변경합니다.

MQTT publication(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 subscriptions(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.

액세서리



I/O ports(I/O 포트)



디지털 입력을 사용하여 개방 및 폐쇄 회로 사이를 전환할 수 있는 외부 장치(예: PIR 센서, 도어 또는 창 접점, 유리 파손 감지기)를 연결하십시오.

디지털 출력을 사용하여 릴레이 및 LED 등의 외부 장치와 연결합니다. VAPIX® 애플리케이션 프로그래밍 인터페이스 또는 웹 인터페이스를 통해 연결된 장치를 활성화할 수 있습니다.

포트

Name(이름): 포트 이름을 바꾸려면 텍스트를 편집합니다.


방향:  포트가 입력 포트임을 나타냅니다.  는 출력 포트임을 나타냅니다. 포트를 구성할 수 있는 경우 아이콘을 클릭하여 입력과 출력 간에 변경할 수 있습니다.

정상 상태:  를 클릭하여 개방 회로와 폐쇄 회로용  을 엽니다.

현재 상태: 포트의 현재 상태를 표시합니다. 현재 상태가 정상 상태와 같지 않을 때 입력 또는 출력이 활성화됩니다. 장치의 입력은 연결이 끊어지거나 1V DC 이상의 전압이 있을 때 개방 회로가 됩니다.

참고

재시작하는 동안 출력 회로가 개방됩니다. 재시작을 마치면 회로가 정상 위치로 돌아갑니다. 이 페이지에서 설정을 변경하면 출력 회로는 활성 트리거에 관계없이 원래 위치로 돌아갑니다.

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 번조했는지(즉, 잘리거나 단락되었는지) 감지할 수 있습니다. 연결을 감시하려면 외부 I/O 루프에 추가 하드웨어(EOL 레지스터)가 필요합니다.

로그

보고서 및 로그

보고서

- **장치 서버 리포트 보기:** 팝업 창에서 제품 상태에 대한 정보를 봅니다. 액세스 로그는 자동으로 서버 리포트에 포함됩니다.
- **장치 서버 리포트 다운로드:** 현재 실시간 보기 이미지의 스냅샷뿐 아니라 UTF-8 형식의 전체 서버 리포트 텍스트 파일이 포함된 .zip 파일이 생성됩니다. 지원 서비스에 문의할 때 항상 서버 리포트 .zip 파일을 포함하십시오.
- **Download the crash report(충돌 보고서 다운로드):** 서버 상태에 대한 자세한 정보가 있는 아카이브를 다운로드합니다. 충돌 리포트에는 자세한 디버그 정보와 서버 리포트에 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.
- **액세스 로그 보기:** 잘못된 로그인 패스워드를 사용한 경우 등 실패한 장치 액세스 시도를 모두 표시하려면 클릭하십시오.

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 클릭하십시오.

Host(호스트): 서버의 호스트 이름 또는 IP 주소를 입력합니다.

Format(포맷): 사용할 syslog 메시지 포맷을 선택합니다.

- Axis
- RFC 3164
- RFC 5424

Protocol(프로토콜): 사용할 프로토콜 및 포트를 선택합니다.

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

Severity(심각도): 트리거될 때 전송할 메시지를 선택합니다.

CA certificate set(CA 인증서 설정): 현재의 설정을 확인하거나 인증서를 추가하십시오.

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 PTZ 사전 설정을 다시 만들어야 합니다.

중요 사항

복원 후 저장되는 유일한 설정은 다음과 같습니다.

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

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

참고

장치에 확인된 펌웨어만 설치되도록 모든 Axis 장치 펌웨어가 디지털로 서명됩니다. 이렇게 하면 Axis 장치의 전반적인 최소 사이버 보안 수준을 더욱 높일 수 있습니다. 자세한 내용은 axis.com에서 "서명된 펌웨어, 보안 부팅 및 개인 키의 보안" 백서를 참조하십시오.

Firmware upgrade(펌웨어 업그레이드): 새 펌웨어 버전으로 업그레이드하십시오. 새로운 펌웨어 릴리즈에는 향상된 기능, 버그 수정 및 완전히 새로운 기능이 포함될 수 있습니다. 항상 최신 릴리즈를 사용하는 것이 좋습니다. 최신 릴리즈를 다운로드하려면 axis.com/support로 이동합니다.

업그레이드할 때 다음 세 가지 옵션 중에서 선택할 수 있습니다.

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

Firmware rollback(펌웨어 롤백): 이전에 설치된 펌웨어 버전으로 되돌립니다.

상세 정보

사이버 보안

Signed Firmware

Signed Firmware는 소프트웨어 공급업체가 개인 키로 펌웨어 이미지에 서명하여 구현됩니다. 펌웨어에 이 서명이 첨부되어 있으면 장치는 펌웨어 설치를 수락하기 전에 펌웨어의 유효성을 검사합니다. 장치에서 펌웨어 무결성이 손상되었음을 감지하면 펌웨어 업그레이드가 거부됩니다.

Secure Boot

Secure Boot는 변경 불가능 메모리(부팅 ROM)에서 시작하여 암호화로 검증된 소프트웨어의 손상되지 않은 체인으로 구성된 부팅 프로세스입니다. Signed Firmware 사용을 기반으로 하는 Secure Boot는 장치가 승인된 펌웨어로만 부팅할 수 있도록 합니다.

Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 장치의 ID 및 무결성을 보장하고 무단 액세스로부터 중요한 정보를 보호하는 기능을 제공합니다. 이는 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반을 엣지 장치 보안에 대한 전문 지식과 결합하여 구축합니다.

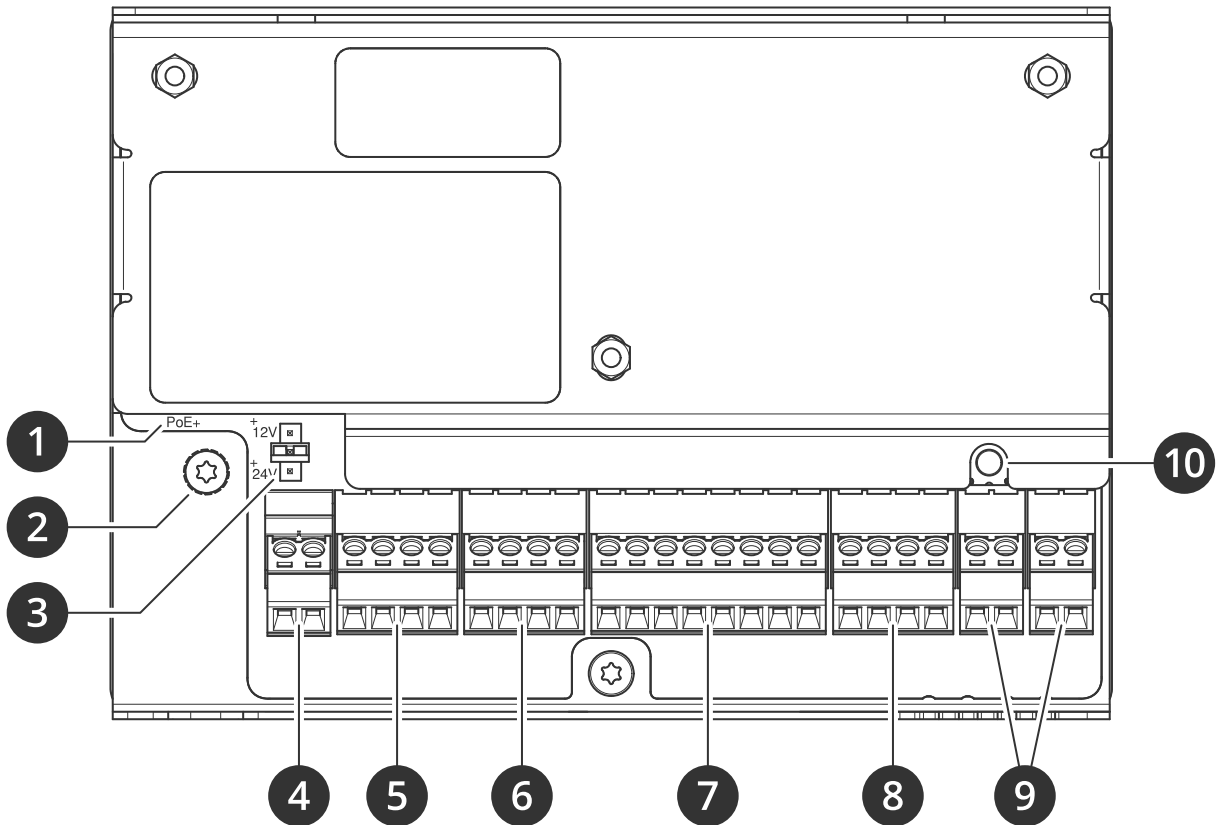
Axis device ID

장치의 출처를 확인할 수 있다는 것은 장치 ID에 대한 신뢰를 구축하는 데 중요합니다. 생산 중에 Axis Edge Vault가 있는 장치에는 공장에서 프로비저닝된 고유한 IEEE 802.1AR 호환 Axis 장치 ID 인증서가 할당됩니다. 이것은 장치의 출처를 증명하는 여권과 같은 역할을 합니다. 장치 ID는 Axis root 인증서에서 서명한 인증서로 보안 키 저장소에 안전하고 영구적으로 저장됩니다. 자동화된 보안 장치 온보딩 및 보안 장치 식별을 위해 고객의 IT 인프라에서 장치 ID를 활용할 수 있습니다.

Axis 장치의 Axis Edge Vault 및 사이버 보안 기능에 대해 자세히 알아보려면 axis.com/learning/white-papers로 이동하여 사이버 보안을 검색하십시오.

사양

제품 개요



- 1 네트워크 커넥터
- 2 접지 위치
- 3 릴레이 접퍼
- 4 전원 커넥터
- 5 릴레이 커넥터
- 6 도어 커넥터
- 7 리더 커넥터
- 8 보조 커넥터
- 9 외부 커넥터
- 10 제어 버튼

LED 표시기

LED	컬러	표시
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.
상태	녹색	정상 작동 시 녹색이 계속 표시됩니다.
	주황색	시작 시 및 설정값 복원 시 계속 표시됩니다.
	빨간색	업그레이드에 실패한 경우 느리게 깜박입니다.
전원	녹색	정상 작동 중입니다.
	주황색	펌웨어 업그레이드 중에는 녹색/주황색으로 깜박입니다.
릴레이	녹색	릴레이가 활성화되었습니다. ¹
	켜져 있지 않음	릴레이가 비활성화되었습니다.

1. COM이 NO에 연결된 경우 릴레이가 활성화됩니다.

버튼

Control button(제어 버튼)

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 출하 시 기본 설정으로 재설정합니다. **공장 출하 시 기본 설정으로 재설정 페이지 30** 항목을 참조하십시오.

커넥터

네트워크 커넥터

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

UL: PoE(Power over Ethernet)(PoE)는 44~57V DC, 15.4W/30W를 제공하는 이더넷 IEEE 802.3af/802.3at Type 1 Class 3 또는 PoE(Power over Ethernet) Plus(PoE+) IEEE 802.3at Type 2 Class 4 전원 제한 인젝터를 통해 이루어집니다. PoE(Power over Ethernet)(PoE)는 UL에서 AXIS T8133 Midspan 30 W 1-port로 평가되었습니다.

전원 우선 순위

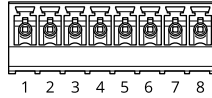
이 장치는 PoE 또는 DC 입력으로 전원을 공급받을 수 있습니다. **네트워크 커넥터 페이지 23** 및 **전원 커넥터 페이지 28** 항목을 참조하십시오.

- 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 다시 시작하지 않고 DC로 전원을 공급합니다.
- PoE와 DC가 모두 연결되어 있고, 현재 PoE에 전원이 공급되고 있습니다. DC가 끊기면 장치가 다시 시작되고 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.

리더 커넥터

리더와 통신하도록 OSDP 및 Wiegand 프로토콜을 둘 다 지원하는 1개의 8핀 터미널 블록입니다.

최대 2개의 OSDP 리더(멀티 드롭) 또는 1개의 Wiegand 리더를 연결할 수 있습니다. 도어 컨트롤러에 연결된 모든 리더에 12V DC에서 500mA가 예약됩니다.



1개의 OSDP 리더용으로 구성됨

기능	핀	참고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	리더에 전원을 공급합니다.	12V DC, 최대 500mA
A	3	반이중	
B	4	반이중	

2개의 OSDP 리더용으로 구성됨(멀티 드롭)

기능	핀	참고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	두 리더에 전원을 공급합니다.	12V DC, 최대 500mA가 두 리더에 대해 결합
A	3	반이중	
B	4	반이중	

중요 사항

- 리더에 컨트롤러에 의해 전원이 공급되는 경우 적격 케이블 길이는 최대 200m(656피트)입니다. Axis 리더에 대해서만 검증되었습니다.
- 리더에 컨트롤러에 의해 전원이 공급되지 않는 경우 다음 케이블 요구 사항이 충족되는 경우 리더 데이터에 대한 적격 케이블 길이는 최대 1000m(3280.8피트)입니다. 실드가 있는 트위스트 페어 1개, AWG 24, 120Ω 임피던스가 필요합니다. Axis 리더에 대해서만 검증되었습니다.

1개의 Wiegand 리더용으로 구성됨

기능	핀	참고	사양
DC 접지(GND)	1		0V DC
DC 출력(+12V)	2	리더에 전원을 공급합니다.	12V DC, 최대 500mA
D0	3		
D1	4		
LED 1	5	빨간색 LED	
LED 2	6	녹색 LED	

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

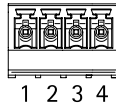
중요 사항

- 판독기에 컨트롤러에 의해 전원이 공급되는 경우, 적격 케이블 길이는 최대 150m(500피트)입니다.
- 판독기에 컨트롤러에 의해 전원이 공급되지 않는 경우 다음 케이블 요구 사항이 충족되는 경우 판독기 데이터에 대한 적격 케이블 길이는 최대 150m(500피트)입니다. AWG 22.

도어 커넥터

도어 모니터링 장치(디지털 입력)용 1개의 4핀 터미널 블록입니다.

도어 모니터는 EOL 레지스터를 통한 관리를 지원합니다. 연결이 중단되면 알람이 트리거됩니다. 관리된 입력을 사용하려면 EOL 레지스터를 설치하십시오. 관리된 입력에 대한 연결 다이어그램을 사용합니다. *페이지 28* 항목을 참조하십시오.



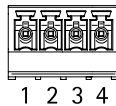
기능	핀	참고	사양
DC 접지	1, 3		0V DC
입력	2, 4	도어 모니터와 통신하는 데 사용됩니다. 디지털 입력 또는 관리된 입력 - 활성화하려면 핀 1 또는 3에 각각 연결하고, 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30V DC

중요 사항

다음 케이블 요구 사항이 충족되는 경우 적격 케이블 길이는 최대 200m(656피트)입니다. AWG 24.

릴레이 커넥터

예를 들어 잠금 장치 또는 게이트에 대한 인터페이스를 제어하는 데 사용할 수 있는 C형 릴레이를 위한 1개의 4핀 터미널 블록입니다.



기능	핀	참고	사양
DC 접지(GND)	1		0V DC

NO	2	정상 개방. 릴레이 장치를 연결하는 데 사용됩니다. NO와 DC 접지 간에 페일 시큐어 잠금 장치를 연결합니다. 점퍼를 사용하지 않을 경우 두 릴레이 핀이 나머지 회로와 전기적으로 분리됩니다.	최대 전류 = 2A 최대 전압 = 30V DC
COM	3	공통	
NC	4	정상 폐쇄. 릴레이 장치를 연결하는 데 사용됩니다. NC와 DC 접지 간에 페일 세이프 잠금 장치를 연결합니다. 점퍼를 사용하지 않을 경우 두 릴레이 핀이 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	1,600mA	800mA
PoE	900mA	450mA

통지

잠금 장치가 극성이 없는 경우 외부 플라이백 다이오드를 추가하는 것이 좋습니다.

보조 커넥터

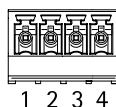
모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 보조 커넥터를 사용합니다. 보조 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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 탭퍼링을 감지할 수 있습니다.

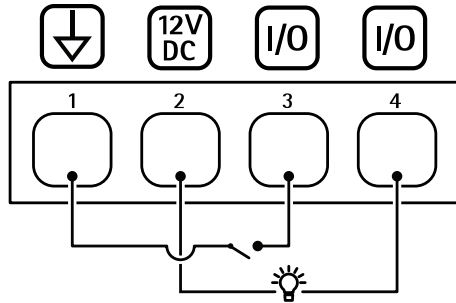
디지털 출력 - 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface 또는 제품의 웹 페이지를 통해 활성화할 수 있습니다.

4핀 터미널 블록



기능	핀	참고	사양
DC 접지	1		0V DC

DC 출력	2	보조 장비에 전원을 공급할 때 사용 가능합니다. 참고: 이 핀은 전원 출력에만 사용할 수 있습니다.	12V 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 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다. 내부 12V DC 출력(핀 2)이 사용될 경우 각 I/O는 12V DC, 50mA(최대) 외부 부하를 유도합니다. 외부 전원 공급 장치와 함께 개방 드레인 연결을 사용하는 경우 I/O가 DC 공급 0 ~ 30V DC, 100mA를 관리할 수 있습니다.	0 ~ 최대 30V DC, 개방 드레인, 100mA

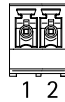


- 1 DC 접지
- 2 DC 출력 12V
- 3 I/O가 입력으로 구성됨
- 4 I/O가 출력으로 구성됨

외부 커넥터

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

UL: 커넥터는 도난 또는 화재 경보용으로 UL에서 평가되지 않았습니다.



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



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

전원 커넥터

DC 전원 입력용 2핀 터미널 블록입니다. 정격 출력 전력이 $\leq 100W$ 로 제한되거나 정격 출력 전류가 $\leq 5A$ 로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.



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

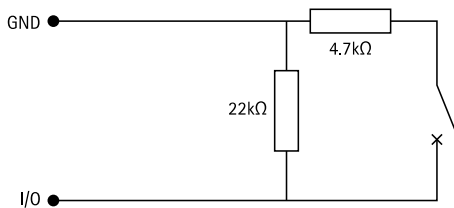
UL: 애플리케이션에 따라 UL 603에 등재된 전원 공급 장치에 적절한 정격의 DC 전원이 공급됩니다.

관리된 입력

관리된 입력을 사용하려면 아래의 다이어그램에 따라 EOL 레지스터를 설치하십시오.

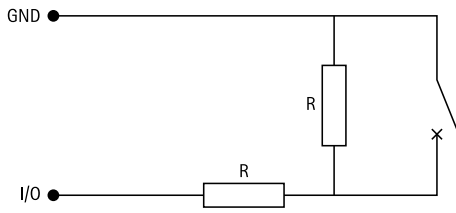
Parallel first connection(병렬 우선 연결)

저항 값은 $4.7k\Omega$ 및 $22k\Omega$ 이어야 합니다.



Serial first connection(직렬 우선 연결)

저항 값은 동일해야 하며 가능한 값은 $1k\Omega$, $2.2k\Omega$, $4.7k\Omega$ 및 $10k\Omega$ 이어야 합니다.



참고

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

장애 처리

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 끕니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 개요 페이지 22* 항목을 참조하십시오.
3. 상태 LED 표시기가 다시 주황색으로 바뀔 때까지 25초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시기가 녹색으로 바뀌면 프로세스가 완료됩니다. 제품이 공장 출하 시 기본 설정으로 재설정되었습니다. 네트워크에서 사용할 수 있는 DHCP 서버가 없는 경우 기본 IP 주소는 192.168.0.90입니다.
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.

펌웨어 옵션

Axis는 활성 트랙 또는 LTS(장기 지원) 트랙에 따라 제품 펌웨어 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 펌웨어를 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 제품 펌웨어 전략에 대한 자세한 내용은 axis.com/support/firmware를 참조하십시오.

현재 펌웨어를 버전 확인

펌웨어는 네트워크 장치의 기능을 결정하는 소프트웨어입니다. 문제를 해결할 때 현재 펌웨어 버전을 확인하여 시작하는 것이 좋습니다. 최신 펌웨어 버전에는 특정 문제를 수정하는 수정 사항이 포함될 수 있습니다.

현재 펌웨어를 확인하려면:

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

펌웨어 업그레이드

중요 사항

- Axis Communications AB에서 이를 보장하지는 않지만(새 펌웨어에서 기능을 사용할 수 있는 경우) 펌웨어를 업그레이드할 때 사전 구성되고 사용자 정의된 설정이 저장됩니다.
- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

참고

활성 트랙의 최신 펌웨어로 장치를 업그레이드하면 제품이 사용 가능한 최신 기능을 수신합니다. 펌웨어를 업그레이드하기 전에 항상 각각의 새로운 릴리즈에서 사용할 수 있는 릴리즈 정보와 업그레이드 지침을 참조하십시오. 최신 버전의 펌웨어와 릴리즈 노트를 찾으려면 axis.com/support/firmware로 이동하십시오.

참고

사용자, 그룹, 자격 증명 및 기타 데이터의 데이터베이스가 펌웨어 업그레이드 이후에 업데이트되었기 때문에 처음 시작 시 완료하는 데 몇 분 정도 소요될 수 있습니다. 소요되는 시간은 데이터 양에 따라 달라집니다.

1. 펌웨어 파일을 컴퓨터에 다운로드합니다. axis.com/support/firmware에서 무료로 사용할 수 있습니다.
2. 장치에 관리자로 로그인합니다.
3. **Maintenance > Firmware upgrade(유지 관리 > 펌웨어 업그레이드)**로 이동하여 **Upgrade(업그레이드)**를 클릭합니다.

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

4. 제품이 재시작되면 웹 브라우저의 캐시를 지우십시오.

기술적 문제, 단서 및 해결 방안

찾는 내용이 여기에 없는 경우에는 axis.com/support에서 문제 해결 섹션을 확인해 보십시오.

펌웨어 업그레이드 문제

펌웨어 업그레이드 실패	펌웨어 업그레이드에 실패하면 장치가 이전 펌웨어를 다시 로드합니다. 가장 일반적인 원인은 잘못된 펌웨어 파일이 업로드된 것입니다. 장치에 해당하는 펌웨어 파일 이름을 확인하고 다시 시도하십시오.
펌웨어 업그레이드 후의 문제	펌웨어 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/DOS 창에서 ping 및 장치의 IP 주소 입력). <ul style="list-style-type: none">• 다음과 같이 Reply from <IP address>: bytes=32; time=10...이라는 메시지를 받는 경우 이는 IP 주소가 이미 네트워크의 다른 장치에서 사용 중일 수 있음을 의미합니다. 네트워크 관리자에게 새 IP 주소를 받아 장치를 다시 설치하십시오.• 다음과 같이 Request timed out이라는 메시지를 받는 경우 이는 Axis 장치에 IP 주소를 사용할 수 있음을 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 활성화 되면, 로그인을 시도할 때 올바른 프로토콜(HTTP 또는 HTTPS)이 사용되는지 확인하십시오. 브라우저의 주소 입력란에 <code>http</code> 또는 <code>https</code> 를 수동으로 입력해야 할 수도 있습니다. root 계정의 패스워드를 분실한 경우에는 장치를 공장 출하 시 기본 설정으로 재설정해야 합니다. <i>공장 출하 시 기본 설정으로 재설정 페이지 30</i> 항목을 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 Companion: 무료이며, 기본 감시가 필요한 소규모 시스템에 적합합니다.
- AXIS Camera Station: 30일 무료 평가판이며, 중규모 시스템에 적합합니다.

지침 및 다운로드를 axis.com/vms로 이동하십시오.

MQTT SSL 보안 포트 8883을 통해 연결할 수 없음

포트 8883을 사용하는 트래픽은 안전하지 않고 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. <ul style="list-style-type: none">• 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/브로커에서 ALPN이 지원되는 경우 443과 같이 개방된 포트를 통해 MQTT 사용을 협상할 수 있습니다. ALPN이 지원되는지와 어떤 ALPN 프로토콜 및 포트를 사용할지는 서버/브로커 공급자에게 확인하십시오.
--	---

연락처 지원

axis.com/support의 지원 부서에 문의하십시오.

