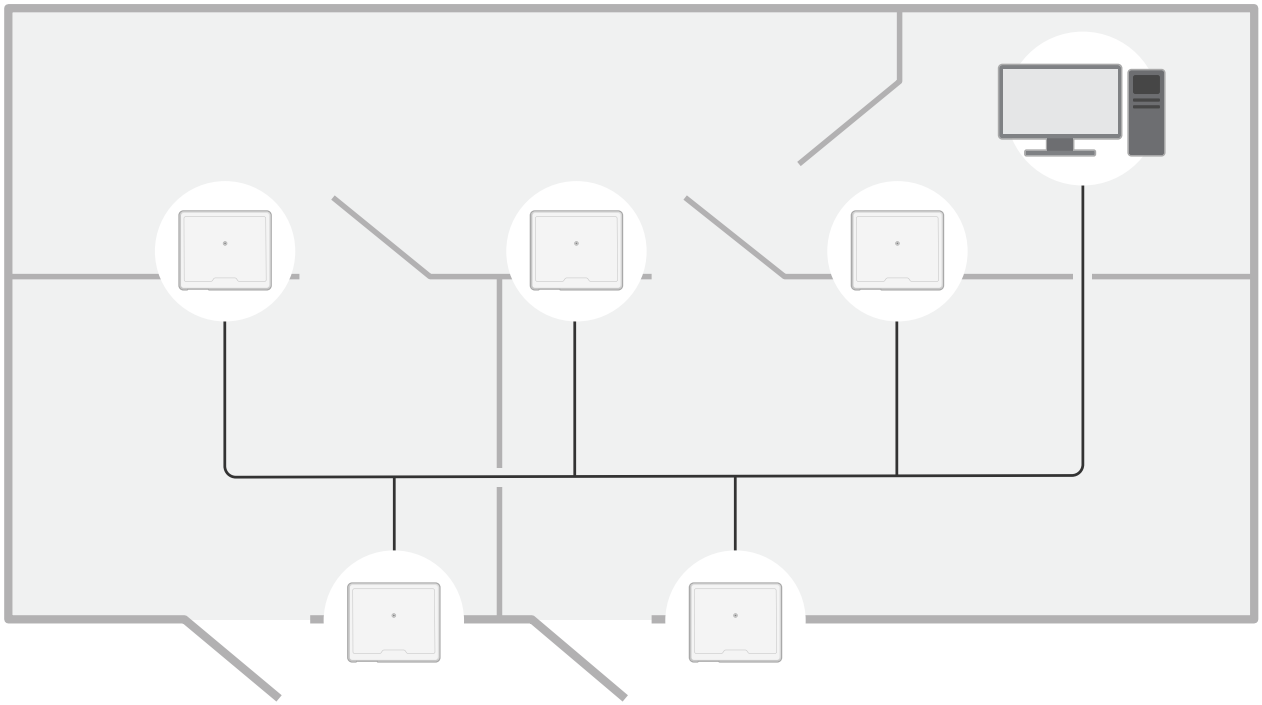
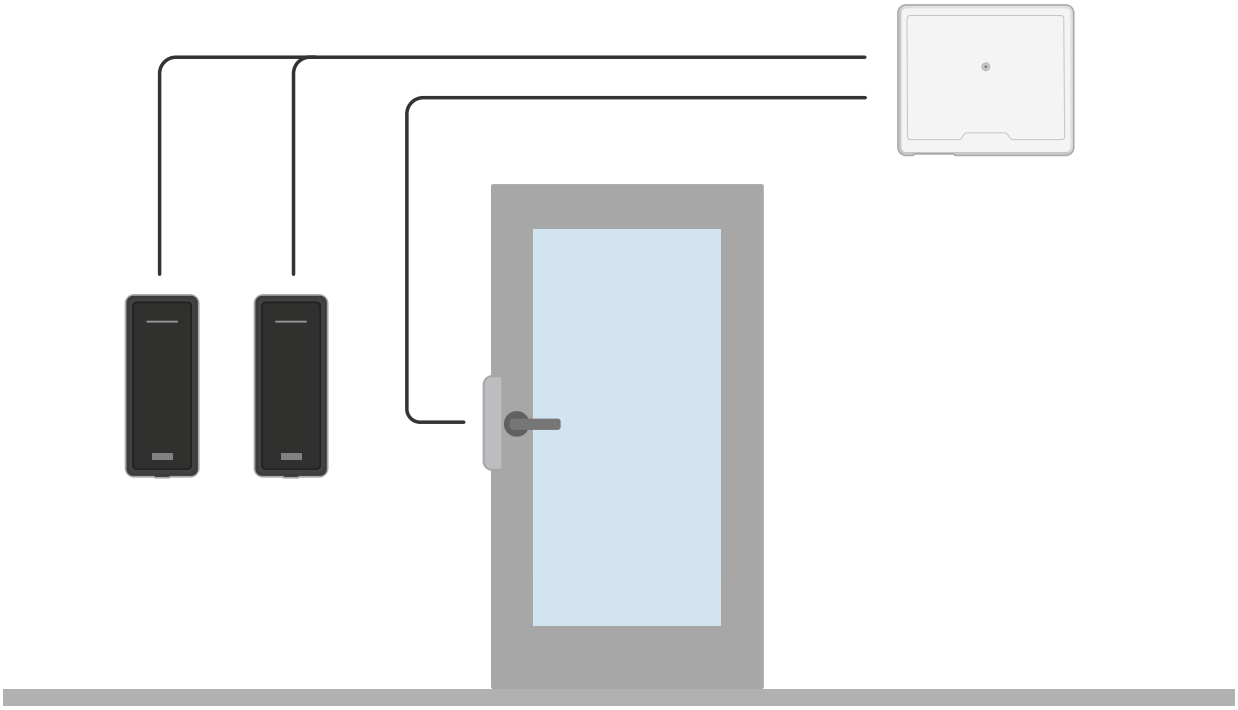
목차


솔루션 오버뷰 ..... 2
설치 ..... 3
..... 3
시작하기 ..... 4
네트워크에서 장치 찾기 ..... 4
브라우저 지원 ..... 4
장치의 웹 인터페이스 열기 ..... 4
관리자 계정을 생성합니다 ..... 4
안전한 패스워드 ..... 5
아무도 장치 소프트웨어를 조작하지 않았는지 확인 ..... 5
웹 인터페이스 오버뷰 ..... 5
장치 구성 ..... 6
Door override(도어 오버라이드) ..... 6
OSDP LED 프로필 ..... 6
카드 형식 ..... 7
웹 인터페이스 ..... 8
상세 정보 ..... 9
사이버 보안 ..... 9
Signed OS ..... 9
Secure Boot ..... 9
Axis Edge Vault ..... 9
Axis device ID ..... 9
사양 ..... 10
제품 오버뷰 ..... 10
..... 10
LED 표시 ..... 10
버튼 ..... 11
제어 버튼 ..... 11
커넥터 ..... 11
네트워크 커넥터 ..... 11
전원 우선 순위 ..... 11
리더 커넥터 ..... 11
도어 커넥터 ..... 13
릴레이 커넥터 ..... 13
보조 커넥터 ..... 14
외부 커넥터 ..... 15
전원 커넥터 ..... 15
관리된 입력 ..... 16
문제 해결 ..... 17
공장 초기화 설정으로 재설정합니다 ..... 17
AXIS OS 옵션 ..... 17
현재 AXIS OS 버전 확인 ..... 17
AXIS OS 업그레이드 ..... 17
기술적 문제 및 가능한 해결책 ..... 18
지원 센터 문의 ..... 20
사이버 보안 ..... 21
취약성 관리 ..... 21
보안 알림 ..... 21
보안 제품 수명 주기 ..... 21

## 솔루션 오버뷰



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



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

## 설치



## 시작하기

### 네트워크에서 장치 찾기

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

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

### 브라우저 지원

다음 브라우저에서 장치를 사용할 수 있습니다.

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

✓: 권장

*: 제한적으로 지원됨

### 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 계정을 생성합니다, on page 4*를 참조하십시오.

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

### 관리자 계정을 생성합니다

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 계정을 입력합니다.
2. 패스워드를 입력합니다. *안전한 패스워드, on page 5*를 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. *공장 초기화 설정으로 재설정합니다, on page 17*를 참조하십시오.

## 안전한 패스워드

중요 사항

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

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

데이터 보호를 위해 적극 권장되는 작업은 다음과 같습니다.

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

## 아무도 장치 소프트웨어를 조작하지 않았는지 확인

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

1. 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정합니다, on page 17*를 참조하십시오.
   재설정 후 Secure Boot는 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

## 웹 인터페이스 오버뷰

이 영상은 장치의 웹 인터페이스에 대한 오버뷰를 제공합니다.




*Axis 장치 웹 인터페이스*

## 장치 구성

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

### Door override(도어 오버라이드)

중요 사항

이 기능은 도어 릴레이를 직접 제어하고 AXIS Camera Station의 릴레이 구성을 오버라이드합니다. Axis 지원 부서에서 지시한 경우에만 사용합니다.

1. AXIS Camera Station에서 Secure Entry 서비스를 중지합니다.
2. 도어 컨트롤러의 웹 인터페이스에서 **Advanced(고급) > Door override(도어 오버라이드)**로 이동합니다.
3. 페이지의 정보를 주의 깊게 읽은 다음 **I understand(이해함)**를 클릭합니다.
4. **Door override(도어 오버라이드)**를 켜고 **Enable(활성화)**을 클릭합니다.
5. 도어 릴레이로 이동하여 **Lock(잠금)**, **Unlock(잠금 해제)** 또는 **Access(액세스)**를 클릭해 도어를 잠그거나 잠금을 해제하거나 액세스 권한을 부여합니다.
6. 구성할 릴레이로 이동하고 **Activate(활성화)** 또는 **Deactivate(비활성화)**를 클릭하여 릴레이를 활성화하거나 비활성화합니다.

### OSDP LED 프로필

OSDP 리더의 LED 프로파일을 사용자 지정하여 다양한 이벤트에 사용되는 조명과 소리를 정의할 수 있습니다. 전체 프로파일 목록은 *LED 프로파일*을 참조하십시오.

#### 조명 및 오디오 레벨 설정

1. **Peripherals(주변 장치)** > **Readers(리더)** > **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
2. **Light and audio levels(조명 및 오디오 레벨)** 드롭다운 메뉴를 펼칩니다.
3. 슬라이더를 사용하여 LED 스트립, LED 백라이트 및 소리의 강도를 조정합니다.
4. **Save(저장)**를 클릭합니다.

비고

조명 및 오디오 레벨을 변경하면 컨트롤러에 연결된 모든 리더의 설정이 업데이트됩니다.

#### OSDP LED 설정 테스트:

**OSDP LED test(OSDP LED 테스트)** 메뉴를 사용하여 모든 리더 프로파일의 오디오 및 조명 설정을 확인할 수 있습니다.

OSDP LED 프로파일 설정을 테스트하는 방법:

1. **Peripherals(주변 장치)** > **Readers(리더)** > **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
2. **OSDP LED test(OSDP LED 테스트)** 드롭다운 메뉴를 펼칩니다.
3. LED 피드백을 선택합니다.
4. 테스트할 리더를 선택합니다.
5. **시작**을 클릭합니다.
6. **Edit feedback(피드백 편집)**을 클릭하여 프로파일의 조명 및 오디오 설정을 변경합니다.
   - **Color(색상)** 드롭다운 메뉴에서 새 색상을 선택합니다.
   - 해당하는 경우 **Audio(오디오)** 드롭다운 메뉴에서 오디오 주파수를 선택합니다.
   - **Reset to default values(기본값으로 재설정)**를 클릭하여 프로파일 설정을 재설정할 수도 있습니다.

- **Save(저장)**를 클릭합니다.

**OSDP LED 프로파일 설정 변경:**

1. **Peripherals(주변 장치)** > **Readers(리더)** > **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
2. **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
3. 편집할 프로파일 옆의 을 클릭합니다.
4. 해당 설정을 편집합니다:
   - **Behavior(동작)** 드롭다운 메뉴에서 LED가 따를 동작을 선택합니다.
   - **Color(색상)** 드롭다운 메뉴에서 LED 색상을 선택합니다.
   - LED의 **Duration on(켜짐 지속 시간)** 및 **Duration off(꺼짐 지속 시간)**를 설정합니다.
   - LED 응답의 **Recurrence(반복)**를 설정합니다.
   - **Audio(오디오)** 드롭다운 메뉴에서 **Beep duration, on(신호음 지속 시간, 켜짐)** 및 **Beep duration, off(신호음 지속 시간, 꺼짐)**를 선택하고 버저 응답의 **Recurrence(반복)**를 설정합니다. **Beep duration, on(신호음 지속 시간, 켜짐)**과 **Beep duration, off(신호음 지속 시간, 꺼짐)**가 동일한 시간인지 확인하십시오.
5. **Save(저장)**를 클릭합니다.

**다른 컨트롤러에서 기존 설정 가져오기**

1. **Peripherals(주변 장치)** > **Readers(리더)** > **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
2. **Import(가져오기)**를 클릭합니다.
3. 업로드할 파일을 선택합니다.
4. **Import(가져오기)**를 클릭합니다.

**현재 설정 내보내기**

1. **Peripherals(주변 장치)** > **Readers(리더)** > **OSDP LED profile(OSDP LED 프로파일)**로 이동합니다.
2. **Export(내보내기)**를 클릭합니다.
3. JSON 파일을 저장할 위치를 선택하고 **Save(저장)**를 클릭합니다.

## 카드 형식

이 기능은 전문가 전용입니다. **Card format(카드 형식)**을 켜는 즉시:

- 37비트 자격 증명을 사용하는 경우 마지막 5비트가 제거됩니다.
- 64비트 자격 증명(QR 코드)을 사용하는 경우 첫 번째 24비트 시퀀스가 제거됩니다.

샘플 데이터 또는 카드 리더를 사용하여 자격 증명을 볼 수 있습니다.

1. **Advanced(고급)** > **Card format(카드 형식)**으로 이동합니다.
2. 경고를 읽고 **I understand(이해함)**를 클릭하여 **Card format(카드 형식)**을 활성화합니다.
3. **Reader data visualization(리더 데이터 시각화)** 드롭다운 메뉴에서 리더를 선택합니다.
4. **Get reader data(리더 데이터 가져오기)** 또는 **Use sample data(샘플 데이터 사용)**를 클릭하여 카드 출력을 생성합니다. 이는 장치의 모든 카드 소지자에게 적용됩니다.
5. 카드 자격 증명에서 끝 비트를 제거하려면 **Trim reader data(리더 데이터 트리밍)**를 켭니다.
6. **Enable(활성화)**을 클릭합니다.

## 웹 인터페이스

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

## 상세 정보

### 사이버 보안

사이버 보안에 관한 제품별 정보는 axis.com에 있는 제품 데이터시트를 참조하십시오.

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

### 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.

### Axis Edge Vault

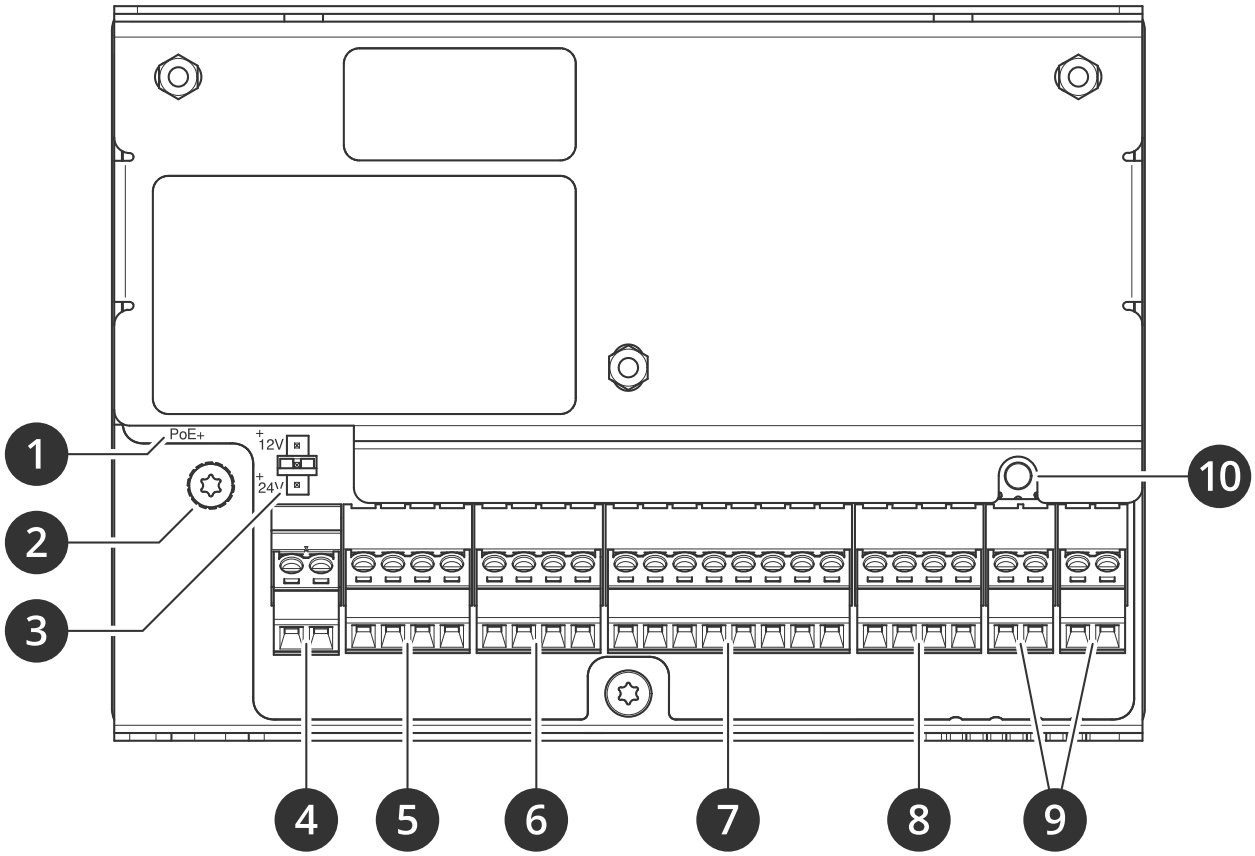
Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반 사이버 보안 플랫폼을 제공합니다. 장치의 ID 및 무결성을 보장하고 무단 액세스로부터 중요한 정보를 보호하는 기능을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반 위에 구축되며, 엣지 장치 보안에 대한 전문 지식이 결합되어 있습니다.

### 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.

## 사양

### 제품 오버뷰




*1 네트워크 커넥터*
*2 접지 위치*
*3 릴레이 점퍼*
*4 전원 커넥터*
*5 릴레이 커넥터*
*6 도어 커넥터*
*7 리더 커넥터*
*8 보조 커넥터*
*9 외부 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. |
| | 주황색 | 펌웨어 업그레이드 중에는 녹색/주황색으로 깜박입니다. |
| Relay(릴레이): | 녹색 | 릴레이 활성화.[1] |
| | 켜져 있지 않음 | 릴레이가 비활성화되었습니다. |

## 버튼

## 제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정합니다, on page 17*를 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

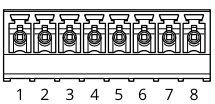
이 장치는 PoE 또는 DC 입력으로 전원을 공급받을 수 있습니다. 자세한 내용은 *네트워크 커넥터, on page 11* 및 *전원 커넥터, on page 15*를 참조하십시오.

- 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.

## 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. 12V DC 기준 500mA는 도어 컨트롤러에 연결된 모든 리더를 위해 예비 지정되어 있습니다.




**1개의 OSDP 리더용으로 구성됨**

1. *COM*이 *NO*에 연결되면 릴레이가 활성화됩니다.

| 기능 | 핀 | 비고 | 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 | 비고 | 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

- 판독기에 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 | 비고 | 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 | |
| 탬퍼 | 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 |

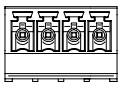
중요 사항

- 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. *page 16* 항목을 참조하십시오.



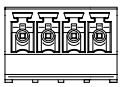

| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지 | 1, 3 | | 0V DC |
| 입력 | 2, 4 | 도어 모니터와 통신하는 데 사용됩니다. 디지털 입력 또는 관리된 입력 — 활성화하려면 각각 핀 1 또는 3에 연결하고, 비활성화하려면 플로팅 상태(연결되지 않음)로 둡니다. | 0 ~ 최대 30V DC |

중요 사항

다음 케이블 요구 사항을 충족하는 경우 적격 케이블 길이는 최대 200m(656ft)입니다: AWG 24.

## 릴레이 커넥터

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




| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지(GND) | 1 | | 0V DC |
| NO | 2 | 정상 개방.<br>릴레이 장치 연결에 사용됩니다. NO와 DC 접지 사이에 페일 시큐어 잠금장치를 연결합니다.<br>점퍼를 사용하지 않더라도, 릴레이 핀 2개는 나머지 회로와 전기적으로 분리됩니다. | 최대 전류 = 2A<br>최대 전압 = 30V DC |
| COM | 3 | 공통 | |

| | | | |
|---|---|---|---|
| NC | 4 | 정상 폐쇄<br>릴레이 장치 연결에 사용됩니다. NC와 DC 접지 사이에 페일 세이프 잠금장치를 연결합니다.<br>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 잠금장치를 연결하는 데 사용할 수 있습니다.

| 전원 | 12V DC에서의 최대 전력 | 24V DC에서의 최대 전력 |
|---|---|---|
| **DC IN** | 1,600mA | 800mA |
| **PoE** | 900mA | 450mA |

*통지*

잠금장치가 극성이 없는 경우 외부 플라이백 다이오드를 추가하는 것이 좋습니다.

## 보조 커넥터

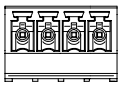
모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 보조 커넥터를 사용합니다. 보조 커넥터는 0V DC 참조점 및 전원(DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

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

**감시 입력 -** 디지털 입력에 대한 탬퍼링을 감지할 수 있습니다.

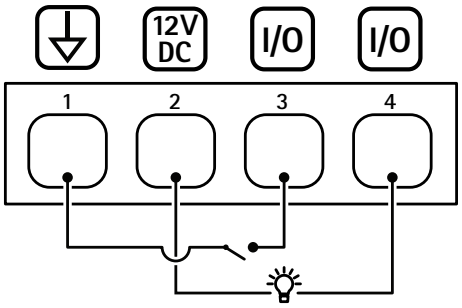
**디지털 출력 -** 릴레이 및 LED 등의 외부 장치와 연결하는 데 사용합니다. 연결된 장치는 VAPIX® Application Programming Interface 또는 제품의 웹 페이지를 통해 활성화할 수 있습니다.

4핀 단자대




| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지 | 1 | | 0V DC |
| DC 출력 | 2 | 보조 장비에 전원을 공급할 때 사용 가능합니다.<br>비고: 이 핀은 정전된 경우에만 사용할 수 있습니다. | 12 V DC<br>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 I/O는 12V DC, 50mA(결합된 최대) 외부 부하를 유도합니다. 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*

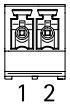
### 외부 커넥터

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

**UL**: 커넥터는 도난 또는 화재 경보용으로 UL에서 평가되지 않았습니다.



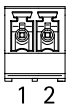

| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지 | 1 | | 0V DC |
| 탬퍼 | 2 | 디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다. | 0 ~ 최대 30V DC |




| 기능 | 핀 | 비고 | 사양 |
|---|---|---|---|
| DC 접지 | 1 | | 0V DC |
| 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 단자대. 정격 출력 전력이 ≤100W로 제한되거나 정격 출력 전류가 ≤5A로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.




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

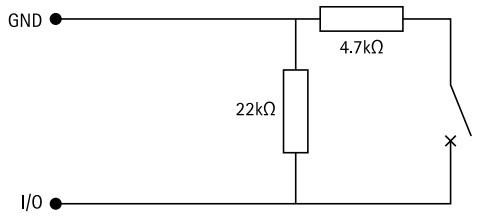
**UL**: 애플리케이션에 따라 UL 603에 등재된 전원 공급 장치에 적절한 정격의 DC 전원이 공급됩니다.

## 관리된 입력

관리된 입력을 사용하려면 아래의 다이어그램에 따라 EOL 레지스터를 설치하십시오.

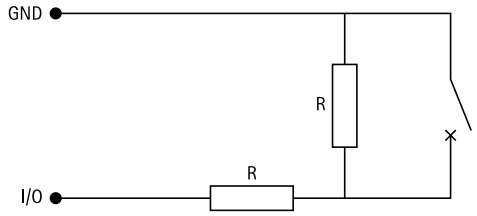
### 병렬 우선 연결

저항 값은 4.7kΩ 및 22kΩ이어야 합니다.




### 직렬 우선 연결

저항 값은 동일해야 하며 가능한 값은 1kΩ, 2.2kΩ, 4.7kΩ 및 10kΩ이어야 합니다.




비고

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

## 문제 해결

### 공장 초기화 설정으로 재설정합니다

중요 사항

공장 출하 시 기본값으로 재설정은 주의해서 사용해야 합니다. 공장 출하 시 기본값으로 재설정하면 IP 주소를 비롯한 모든 설정이 공장 출하 시 기본값으로 재설정됩니다.

제품을 공장 초기화 설정으로 재설정하려면 다음을 수행하십시오.

1. 제품의 전원을 끊습니다.
2. 제어 버튼을 누른 상태에서 전원을 다시 연결합니다. *제품 오버뷰, on page 10*를 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. 네트워크에 DHCP 서버를 이용할 수 없는 경우, 장치의 IP 주소는 다음 중 하나로 기본 설정됩니다.
   - **AXIS OS 12.0 이상이 설치된 장치:** 링크 로컬 주소 서브넷(169.254.0.0/16)에서 할당받음
   - **AXIS OS 11.11 이하가 설치된 장치:** 192.168.0.90/24
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 제품에 액세스합니다.

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

### AXIS OS 옵션

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

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

### 현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

### AXIS OS 업그레이드

중요 사항

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

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

- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

- 활성 트랙의 최신 AXIS OS 버전으로 장치를 업그레이드하면 제품이 사용 가능한 최신 기능을 수신합니다. 업그레이드하기 전에 항상 새 릴리스마다 제공되는 릴리즈 정보와 업그레이드 지침을 참조하십시오. 최신 AXIS OS 버전과 릴리즈 정보를 찾으려면 *axis.com/support/device-software*로 이동하십시오.
- 사용자, 그룹, 자격 증명 및 기타 데이터의 데이터베이스가 AXIS OS 업그레이드 이후에 업데이트되었기 때문에 처음 시작 시 완료하는 데 몇 분 정도 소요될 수 있습니다. 소요되는 시간은 데이터 양에 따라 달라집니다.

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

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

4. 제품이 재시작되면 웹 브라우저의 캐시를 지우십시오.

## 기술적 문제 및 가능한 해결책

### AXIS OS 업그레이드 문제

**AXIS OS 업그레이드 실패**

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

**AXIS OS 업그레이드 후 문제**

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

### IP 주소 설정 문제

**IP 주소를 설정할 수 없음**

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

### 장치 액세스 관련 문제

**브라우저로 장치에 액세스할 때 로그인할 수 없음**

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

root 계정의 패스워드를 분실한 경우, 장치를 공장 초기화 설정으로 재설정해야 합니다. 자세한 내용은 *공장 초기화 설정으로 재설정합니다, on page 17* 항목을 참조하십시오.

**IP 주소가 DHCP에 의해 변경됨**

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

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

**IEEE 802.1X를 사용하는 동안 발생하는 인증 오류**

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

**브라우저가 지원되지 않음**

권장 브라우저 목록은 *브라우저 지원, on page 4*을 참조하십시오.

**외부에서 장치에 액세스할 수 없음**

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

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

지침 및 다운로드는 *axis.com/vms*로 이동하십시오.

### MQTT 관련 문제

**MQTT SSL 보안 포트 8883을 통해 연결할 수 없음**

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

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

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

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

## 지원 센터 문의

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

## 사이버 보안

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

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

### 취약성 관리

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

### 보안 알림

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

### 보안 제품 수명 주기

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

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

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

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

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

T10181041_ko

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB