AXIS I8307-VE Network Intercom

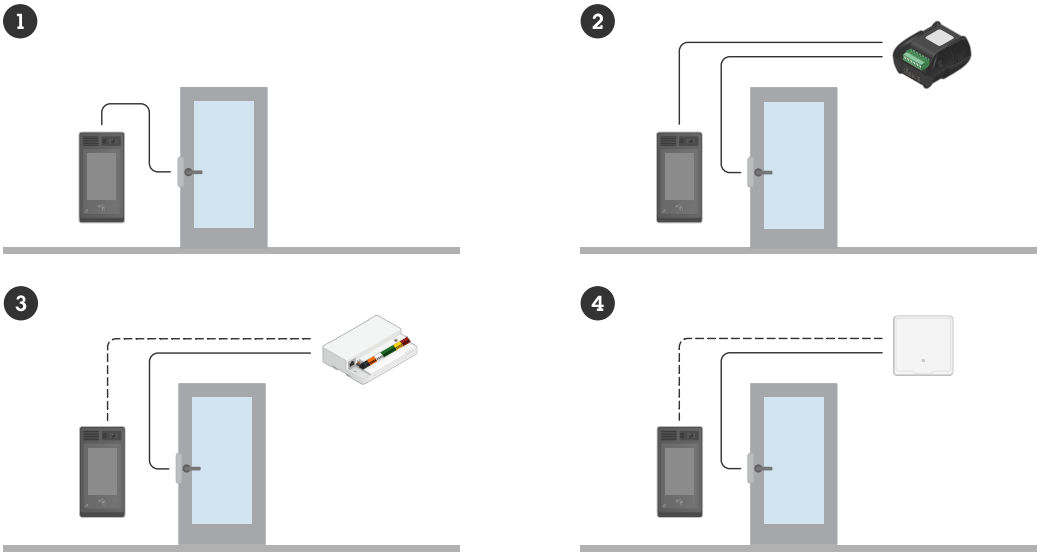
사용자 설명서

목차

솔루션 오버뷰 4
설치 5
미리보기 모드 5
시작하기 6
네트워크에서 장치 찾기 6
브라우저 지원 6
장치의 웹 인터페이스 열기 6
관리자 계정을 생성합니다 6
안전한 패스워드 7
아무도 장치 소프트웨어를 조작하지 않았는지 확인 7
장치 구성 8
원격 스피커 테스트 보정 및 실행 8
다이렉트 SIP(P2P) 설정 8
서버(PBX)를 통해 SIP 설정 9
연락처 만들기 9
디스플레이에 통화 버튼 추가하기 10
리더로 설정 10
Entry list(출입 목록)를 사용하여 자격 증명 소지자가 도어를 열 수 있도록 허용합니다. 10
도어 컨트롤러를 사용하여 카드 리더로 설정 11
카드의 보호된 데이터를 사용하여 보안 강화 12
DTMF를 사용하여 디스플레이에 지도 표시하기 13
웹 인터페이스 15
상세 정보 16
VoIP(Voice over IP) 16
SIP(Session Initiation Protocol) 16
Peer-to-peer SIP(피어 투 피어 SIP) 16
PBX(Private Branch Exchange) 17
NAT 통과 기능 18
이벤트의 룰 설정 18
분석 및 앱 18
AXIS Client for Unified Communication Systems 18
사양 19
제품 오버뷰 19
LED 표시 20
SD 카드 슬롯 21
버튼 21
제어 버튼 21
커넥터 21
네트워크 커넥터 21
오디오 커넥터 21
릴레이 커넥터 21
리더 커넥터 22
I/O 커넥터 22
전원 커넥터 23
장비 연결 25
PoE(12V)로 구동되는 릴레이 1개 25
PoE(12V)로 구동되는 릴레이 2개 25
PoE(12V)로 구동되는 릴레이 1개 + 외부 전원 공급 장치로 구동되는 릴레이 1개 26
PoE(12V)로 구동되는 릴레이 1개 + 무전위 접점 릴레이 1개 26
인터콤에서 PoE+로 전원이 공급되는 12V 페일 시큐어 잠금 장치 27
외부 전원 공급 장치에서 전원이 공급되는 페일 시큐어 잠금 장치 27
PoE(24V)로 구동되는 릴레이 1개 + 무전위 접점 릴레이 1개 28
OSDP를 사용하여 도어 컨트롤러에 연결된 리더 28

Wiegand를 사용하여 도어 컨트롤러에 연결된 리더 29
VAPIX 리더를 사용하여 Axis 도어 컨트롤러에 연결된 리더 29
문제 해결 30
공장 초기화 설정으로 재설정합니다 30
AXIS OS 옵션 30
현재 AXIS OS 버전 확인 30
AXIS OS 업그레이드 30
기술적 문제 및 가능한 해결책 31
성능 고려 사항 33
지원 센터 문의 33
안전 정보 34
위험 레벨 34
기타 메시지 레벨 34
사이버 보안 35
취약성 관리 35
보안 알림 35
보안 제품 수명 주기 35

솔루션 오버뷰



1 *인터콤*
2 *AXIS A9801과 결합된 인터콤*
3 *AXIS A9210과 결합된 인터콤*
4 *접근 제어 시스템과 결합된 인터콤*

설치



미리보기 모드

미리 보기 모드는 설치 중 카메라 보기를 미세 조정할 때 설치자에게 이상적입니다. 미리 보기 모드에서 카메라 보기에 액세스하는 데 로그인이 필요하지 않습니다. 장치 전원을 켠 후 제한된 시간 동안 공장 초기화 설정 상태로만 사용할 수 있습니다.



이 영상은 미리 보기 모드를 사용하는 방법을 보여줍니다.

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 6* 항목을 참조하십시오.

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

관리자 계정을 생성합니다

장치에 처음 로그인하는 경우 관리자 계정을 생성해야 합니다.

1. 계정을 입력합니다.
2. 패스워드를 입력합니다. *안전한 패스워드, on page 7* 항목을 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 30* 항목을 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 30* 항목을 참조하십시오.
   재설정 후 Secure Boot는 장치의 상태를 보장합니다.
2. 장치를 구성하고 설치합니다.

장치 구성

이 섹션에서는 하드웨어 설치가 완료된 후 제품을 시작하고 실행하기 위해 설치 프로그램이 수행해야 하는 모든 중요한 구성에 대해 설명합니다.

원격 스피커 테스트 보정 및 실행

스피커 테스트를 실행하여 원격 위치에서 스피커가 의도한 대로 작동하는지 확인할 수 있습니다. 스피커는 내장 마이크로 등록된 일련의 테스트 톤을 재생하여 테스트를 수행합니다. 테스트를 실행할 때마다 등록된 값이 보정 중에 등록된 값과 비교됩니다.

비고

테스트는 설치 장소의 장착 위치에서 보정해야 합니다. 스피커를 옮기거나 주변 환경이 달라지면 (예: 벽을 세우거나 없애는 경우) 스피커를 다시 보정해야 합니다

보정하는 동안 누군가가 실제로 설치 현장에 있으면서 테스트 톤을 듣고, 스피커 음향 경로에 의도하지 않은 방해물이 있어 테스트 톤이 지워지거나 막히지 않도록 해야 합니다.

1. 장치 인터페이스 >**Audio(오디오) > Speaker test(스피커 테스트)**로 이동합니다.
2. 오디오 장치를 보정하려면 **Calibrate(보정)**를 클릭합니다.

비고

Axis 제품이 보정되면 언제든지 스피커 테스트를 실행할 수 있습니다.

3. 스피커 테스트를 실행하려면 **Run the test(테스트 실행)**를 클릭합니다.

비고

물리적 장치에서 제어 버튼을 눌러 보정을 실행할 수도 있습니다. 제어 버튼을 식별하려면 *제품 오버뷰, on page 19*를 참조하십시오.

다이렉트 SIP(P2P) 설정

VoIP(음성 IP)는 IP 네트워크를 통한 음성 및 멀티미디어 통신을 활성화하는 기술 그룹입니다. 자세한 내용은 *VoIP(Voice over IP), on page 16*을 참조하십시오.

이 장치에서는 SIP 프로토콜을 통해 VoIP가 활성화됩니다. SIP에 대한 자세한 내용은 *SIP(Session Initiation Protocol), on page 16*을(를) 참조하십시오.

두 가지 유형의 SIP 설정이 있습니다. 직접 또는 피어 투 피어(P2P)가 그중 하나입니다. 동일한 IP 네트워크에 있는 소수의 사용자 에이전트 간에 통신이 이루어지고 PBX 서버가 제공할 수 있는 별도의 기능이 필요 없으면 피어 투 피어를 사용하십시오. 설정 방법은 *Peer-to-peer SIP(피어 투 피어 SIP), on page 16*을(를) 참조하십시오.

1. **Communication > SIP > Settings(통신 > SIP > 설정)**로 이동하여 **Enable SIP(SIP 활성화)**를 선택합니다.
2. 장치가 수신 콜을 받게 하려면 **Allow incoming calls(수신 콜 허용)**를 선택합니다.

통지

수신 콜을 허용하면 장치가 네트워크에 연결된 모든 장치로부터 오는 콜을 수락합니다. 공용 네트워크나 인터넷에서 장치에 액세스할 수 있으면 수신 통화를 허용하지 않는 것이 좋습니다.

3. **Call handling(콜 처리)**을 클릭합니다.
4. **Call timeout(콜 시간 초과)**에서 응답이 없을 경우 콜이 끝나기 전까지 지속되는 시간(초)을 설정합니다.
5. 수신 통화를 허용한 경우 수신 통화에 대한 시간 초과 전의 시간(초)을 **Incoming call timeout (수신 콜 시간 초과)**에서 설정하십시오.
6. **Ports(포트)**를 클릭합니다.
7. **SIP port(SIP 포트)** 번호와 **TLS port(TLS 포트)** 번호를 입력합니다.

비고

- **SIP port(SIP 포트)** - SIP 세션에 사용됩니다. 이 포트를 통한 신호 트래픽은 암호화되지 않습니다. 기본 포트 번호는 5060입니다.
- **TLS port(TLS 포트)** - SIPS 및 TLS 보안 SIP 세션에 사용됩니다. 이 포트를 통한 신호 트래픽은 전송 계층 보안(TLS)으로 암호화됩니다. 기본 포트 번호는 5061입니다.
- **RTP 시작 포트** - SIP 콜에서 첫 번째 RTP 미디어 스트림에 사용되는 포트입니다. 기본 시작 포트는 4000입니다. 일부 방화벽은 특정 포트 번호의 RTP 트래픽을 차단할 수 있습니다. 포트 번호는 1024~65535 사이여야 합니다.

8. **NAT 통과**를 클릭합니다.
9. NAT 통과에 사용할 프로토콜을 선택합니다.

비고

장치가 NAT 라우터 또는 방화벽 뒤에 있는 네트워크에 연결되어 있는 경우 NAT 통과를 사용하십시오. 자세한 내용은 *NAT 통과 기능, on page 18*을 참조하십시오.

10. **Save(저장)**를 클릭합니다.

서버(PBX)를 통해 SIP 설정

VoIP(음성 IP)는 IP 네트워크를 통한 음성 및 멀티미디어 통신을 활성화하는 기술 그룹입니다. 자세한 내용은 *VoIP(Voice over IP), on page 16*을 참조하십시오.

이 장치에서는 SIP 프로토콜을 통해 VoIP가 활성화됩니다. SIP에 대한 자세한 내용은 *SIP(Session Initiation Protocol), on page 16*을(를) 참조하십시오.

두 가지 유형의 SIP 설정이 있습니다. PBX 서버가 그 중 하나입니다. IP 네트워크 안팎에서 무한대의 사용자 에이전트 사이에 통신이 이루어져야 할 경우 PBX 서버를 사용하십시오. PBX 공급자에 따라서 설정에 기능이 더 추가될 수 있습니다. 자세한 내용은 *PBX(Private Branch Exchange), on page 17*을 참조하십시오.

1. PBX 공급자에게 다음 정보를 요청합니다.
   - 사용자 ID
   - 도메인
   - 패스워드
   - 인증 ID
   - 발신자 ID
   - 등록자
   - RTP 시작 포트
2. **통신 > SIP > 계정**으로 이동하여 **+ 계정 추가**를 클릭합니다.
3. 계정 **Name(이름)**을 입력합니다.
4. **Registered(등록됨)**를 선택합니다.
5. 전송 모드를 선택합니다.
6. PBX 공급자가 제공하는 계정 정보를 추가합니다.
7. **Save(저장)**를 클릭합니다.
8. 피어 투 피어와 같은 방법으로 SIP 설정을 지정하고 *다이렉트 SIP(P2P) 설정, on page 8*을(를) 참조하십시오. PBX 공급자의 RTP 시작 포트를 사용합니다.

연락처 만들기

이 예는 연락처 목록에서 새 연락처를 생성하는 방법을 설명합니다. 시작하기 전에 **Communication > SIP(통신 > SIP)**에서 SIP를 활성화하십시오.

새 연락처를 생성하려면:

1. **Communication > Contact list(통신 > 연락처 목록)**로 이동합니다.
2. **+ Add contact(+ 연락처 추가)**를 클릭합니다.
3. 연락처의 성 및 이름을 입력합니다.
4. 연락처의 SIP 주소를 입력합니다.

비고

SIP 주소에 대한 자세한 내용은 *SIP(Session Initiation Protocol), on page 16*을(를) 참조하십시오.

5. 전화를 걸 SIP 계정을 선택합니다.

비고

가용성 옵션은 **System(시스템)** >**Events(이벤트)** >**Schedules(일정)**에서 정의됩니다.

6. 연락처의 **Availability(가용성)**을 선택합니다. 연락처가 없을 때 통화하면 대체 연락처가 없는 한 통화가 취소됩니다.

비고

대체는 원래 연락처가 응답하지 않거나 사용할 수 없는 경우 통화가 전달되는 연락처입니다.

7. **Fallback(대체)**에서 **None(없음)**을 선택합니다.
8. **Save(저장)**를 클릭합니다.

디스플레이에 통화 버튼 추가하기

이 예에서는 방문자가 리셉션을 호출하기 위해 누를 수 있는 버튼을 표시하도록 디스플레이를 구성하는 방법을 설명합니다.

시작하기 전

- 리셉션 연락처를 만듭니다. 자세한 내용은 *연락처 만들기, on page 9* 항목을 참조하십시오.

1. **Display(디스플레이) > Pages(페이지)**로 이동합니다.
2. **Default Homepage(기본 홈페이지)**에서 ⋮ 를 클릭하고 **Edit(편집)**을 선택합니다.
3. **+ 추가**를 클릭합니다.
4. **Type(유형)** 목록에서 **Button(버튼)**을 선택합니다.
5. 연락처 목록에서 리셉션을 선택합니다.
6. 버튼 크기를 선택합니다.
7. 버튼을 저장하려면 **Save(저장)**를 클릭합니다.
8. 기본 홈페이지를 저장하려면 **Save(저장)**를 클릭합니다.

리더로 설정

인터콤을 리더로 설정하여 자격 증명 소지자가 도어를 열 수 있도록 할 수 있습니다.

Entry list(출입 목록)를 사용하면 인터콤이 자격 증명을 로컬에 저장하고 최대 50명의 자격 증명 소지자에 대해 독립형 리더로 동작할 수 있습니다.

인터콤을 도어 컨트롤러에 연결할 때도 인터콤은 최대 50개의 자격 증명을 저장할 수 있으며, 요청된 자격 증명이 Entry list(출입 목록)에 있는 경우 인터콤이 접근 권한을 관리합니다. 요청된 자격 증명이 Entry list(출입 목록)에 없고 **Use connected door controller(연결된 도어 컨트롤러 사용)** 옵션이 활성화되어 있으면, 요청이 도어 컨트롤러로 전달되고 도어 컨트롤러가 접근 권한을 관리합니다.

Entry list(출입 목록)를 사용하여 자격 증명 소지자가 도어를 열 수 있도록 허용합니다.

Entry list(출입 목록)를 사용하면 자격 증명 소지자가 자신의 자격 증명을 사용하여 도어 열기와 같은 작업을 트리거하도록 설정할 수 있습니다. 이 예에서는 카드를 사용하여 도어를 10번 열 수 있는 자격 증명 소지자를 추가하는 방법을 설명합니다.

전제 조건

- **리더 > 칩 유형**에서 올바른 칩 유형이 활성화되었는지 확인합니다.

항목 목록을 켜고 자격 증명 소지자를 추가합니다.

1. **리더 > 항목 목록**으로 이동합니다.
2. **항목 목록 사용**을 켭니다.
3. **+ 자격 증명 소지자 추가**를 클릭합니다.
4. 자격 증명 소지자의 이름과 성을 입력합니다. 이름은 고유해야 합니다.
5. **카드**를 선택합니다.
6. 장치에 자격 증명 소지자의 카드를 대고 **최신 항목 가져오기**를 클릭합니다.
7. 이벤트 조건을 **접근 허용**으로 유지합니다.
8. **만료**에서 **횟수**를 선택합니다.
9. **Number of times(횟수)**에 10을 입력합니다.
10. **Save(저장)**를 클릭합니다.

룰 만들기:

1. **System > Events(시스템 > 이벤트)**로 이동합니다.
2. **룰**에서 **+ 룰 추가**를 클릭합니다.
3. **Name(이름)**에 Open door(도어 열기)를 입력합니다.
4. 조건 목록에서 **항목 목록 > 접근 허용**을 선택합니다.
5. 액션 목록에서 **I/O > I/O 한 번 토글**을 선택합니다.
6. 포트 목록에서 **도어**를 선택합니다.
7. **상태**에서 **활성**을 선택합니다.
8. 지속 시간을 00:00:07로 설정합니다.
9. **Save(저장)**를 클릭합니다.

도어 컨트롤러를 사용하여 카드 리더로 설정

네트워크 연결

인터콤을 카드 리더로 사용하려면 도어 컨트롤러에 연결하십시오. 도어 컨트롤러는 모든 자격 증명을 저장하고 도어를 통해 출입하는 사람을 추적합니다. 이 예에서는 네트워크를 통해 장치를 연결합니다. 허용되는 카드 유형도 수정합니다.

중요 사항

네트워크 연결은 Axis 도어 컨트롤러에서만 작동합니다. Axis 이외의 도어 컨트롤러에 연결하려면 장치를 와이어로 물리적으로 연결해야 합니다. *유선 연결, on page 12* 항목을 참조하십시오.

인터콤을 카드 리더로 설정

1. **Reader(리더) > Connection(연결)**으로 이동합니다.
2. **VAPIX reader(VAPIX 리더)** 프로토콜 유형을 선택합니다.
3. 도어 컨트롤러와 통신하기 위한 프로토콜을 선택합니다.

비고

HTTPS를 사용한다면 **Verify certificate(인증서 확인)**를 켜는 것이 좋습니다.

4. 도어 컨트롤러의 IP 주소를 입력합니다.
5. 도어 컨트롤러의 자격 증명을 입력합니다.
6. **Connect(연결)**를 클릭합니다.
7. 알맞은 도어에 대한 입구 리더를 선택합니다.
8. **Save(저장)**를 클릭합니다.

유선 연결

도어 스테이션을 카드 리더로 사용하려면 도어 컨트롤러에 연결하십시오. 도어 컨트롤러는 모든 자격 증명을 저장하고 도어를 통해 출입하는 사람을 추적합니다. 이 예에서는 장치를 와이어로 연결하고 Wiegand 프로토콜을 사용하고 알람음을 활성화하고 LED에 하나의 I/O 포트를 사용합니다. 허용되는 카드 유형도 수정합니다.

중요 사항

아직 사용하지 않는 I/O 포트를 사용하십시오. 이미 사용 중인 I/O 포트를 사용하는 경우 해당 포트에 대해 생성된 모든 이벤트가 작동을 멈춥니다.

시작하기 전

- 인터콤을 도어 컨트롤러에 연결합니다.
  전기 배선도는 *장비 연결, on page 25*에서 확인할 수 있습니다.
- 리더용 Wiegand 프로토콜을 사용하여 도어 컨트롤러의 하드웨어를 구성합니다. 지침은 도어 컨트롤러의 사용자 설명서를 참조하십시오.

인터콤을 카드 리더로 설정

1. **Reader(리더) > Connection(연결)**으로 이동합니다.
2. **Wiegand**를 프로토콜 유형으로 선택합니다.
3. **Beeper(알람음)**를 켭니다.
4. **Input for beeper(알람음 입력)**에서 **I3**을 선택합니다.
5. **Input used for LED control(LED 제어에 사용되는 입력)**에서 **1**을 선택합니다.
6. **Input for LED1(LED1 입력)**에서 **I1**을 선택합니다.
7. 각 상태에 사용할 색상을 선택합니다.
8. **Keypress format(키 누르기 형식)** 아래에서 **FourBit(포비트)**를 선택합니다.
9. **Save(저장)**를 클릭합니다.
10. **Reader > Chip types(리더 > 칩 유형)**로 이동하고 사용하려는 칩 유형을 활성화합니다.

비고

기본 칩 유형 세트를 유지할 수 있지만 특정 요구 사항에 따라 목록을 수정하는 것이 좋습니다.

11. **Add data set(데이터 세트 추가)**를 클릭하여 다른 칩 유형에 대한 데이터 세트를 지정합니다.
12. **Save(저장)**를 클릭합니다.

카드의 보호된 데이터를 사용하여 보안 강화

접근 제어 시스템의 보안을 강화하기 위해 일부 유형의 카드에 저장된 보안 카드 데이터를 사용하도록 선택할 수 있습니다. 데이터는 비밀 키로 보호됩니다. 카드 데이터를 읽으려면 비밀 키와 카드에 대한 기타 정보를 장치에 저장해야 합니다.

1. **Reader > Chip types(리더 > 칩 유형)**로 이동합니다.
2. **Data sets(데이터 세트)** 항목에서 편집할 칩 유형을 선택하고 **Add data set(데이터 세트 추가)**를 클릭합니다.
3. 카드 데이터에 대한 정보를 입력합니다. 입력할 정보는 카드 유형 및 카드 등록 방법에 따라 다릅니다.
4. OSDP 또는 Wiegand 프로토콜을 사용하는 경우, 일반 카드 UID/CSN 대신 UID/CSN으로 보안 데이터를 전송하기 위해 **Use as UID(UID로 사용)**를 선택합니다.
5. 지정된 카드 데이터와 일치하는 카드만 접근 제어로 보내도록 허용하려면 **Required data(필요한 데이터)**를 선택합니다. 준수하지 않는 카드는 리더가 조용히 무시합니다.
6. **Save(저장)**를 클릭합니다.

DTMF를 사용하여 디스플레이에 지도 표시하기

방문자가 인터콤으로 전화를 걸어 길 안내가 필요한 경우, 응답자는 DTMF(듀얼 톤 다중 주파수) 신호를 사용하여 인터콤의 디스플레이에 지도를 표시할 수 있습니다.

이 예제는 다음을 수행하는 방법을 설명합니다.

- 인터콤에 지도 이미지를 업로드합니다.
- 인터콤에 지도 이미지가 포함된 페이지를 만듭니다.
- 인터콤에서 DTMF 시퀀스를 정의합니다.
- DTMF 시퀀스에 대한 응답으로 30초 동안 지도 페이지를 표시하도록 인터콤을 설정합니다.

시작하기 전

- 장치에서 SIP 호출을 허용하고 SIP 계정을 생성합니다. 지침은 *다이렉트 SIP(P2P) 설정, on page 8* 및 *서버(PBX)를 통해 SIP 설정, on page 9* 항목을 참조하십시오.

지도 이미지 업로드

1. **Media(미디어)**로 이동합니다.
2. **+ 추가**를 클릭합니다.
3. 건물 지도가 표시된 이미지를 끌어다 놓습니다. 권장 이미지 해상도는 480x800픽셀이며, 최대 해상도는 2048x2048픽셀입니다.
4. **Save(저장)**를 클릭합니다.

디스플레이용 지도 페이지를 만듭니다.

5. **Display(디스플레이) > Pages(페이지)**로 이동합니다.
6. **+ 추가**를 클릭합니다.
7. 페이지의 이름을 입력합니다(예: Map page(지도 페이지)).
8. **+ 추가**를 클릭합니다.
9. 유형 목록에서 **Image(이미지)**를 선택합니다.
10. 이미지의 이름을 입력합니다(예: Map image(지도 이미지)).
11. 이미지 목록에서 지도 이미지를 선택합니다.
12. **Save(저장)**를 클릭합니다.
13. **Save(저장)**를 다시 클릭합니다.

DTMF 시퀀스 정의

14. **통신 > SIP > DTMF**로 이동합니다.
15. **+ 시퀀스 추가**를 클릭합니다.
16. **Sequence(시퀀스)**에서 9를 입력합니다.
17. **Description(설명)**에 Show map(지도 표시)을 입력합니다.
18. 계정을 선택합니다.
19. **Save(저장)**를 클릭합니다.

룰 만들기

20. **System(시스템) > Events(이벤트) > Rules(룰)**로 이동하고 룰을 추가합니다.
21. 룰의 이름을 입력합니다(예: Use DTMF to show map(TMF를 사용하여 지도 표시)).
22. 조건 목록에서 **Call(호출) > DTMF**를 선택합니다.
23. DTMF 이벤트 ID 목록에서 **Show map(지도 표시)**을 선택합니다.
24. 액션 목록에서 **Display(디스플레이) > Show page(페이지 표시)**를 선택합니다.
25. 페이지 목록에서 **Map page(지도 페이지)**를 선택합니다.
26. **Duration(기간)**에 00:00:30을 입력하여 30초 동안 지도를 표시합니다.

27. **Save(저장)**를 클릭합니다.

웹 인터페이스

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

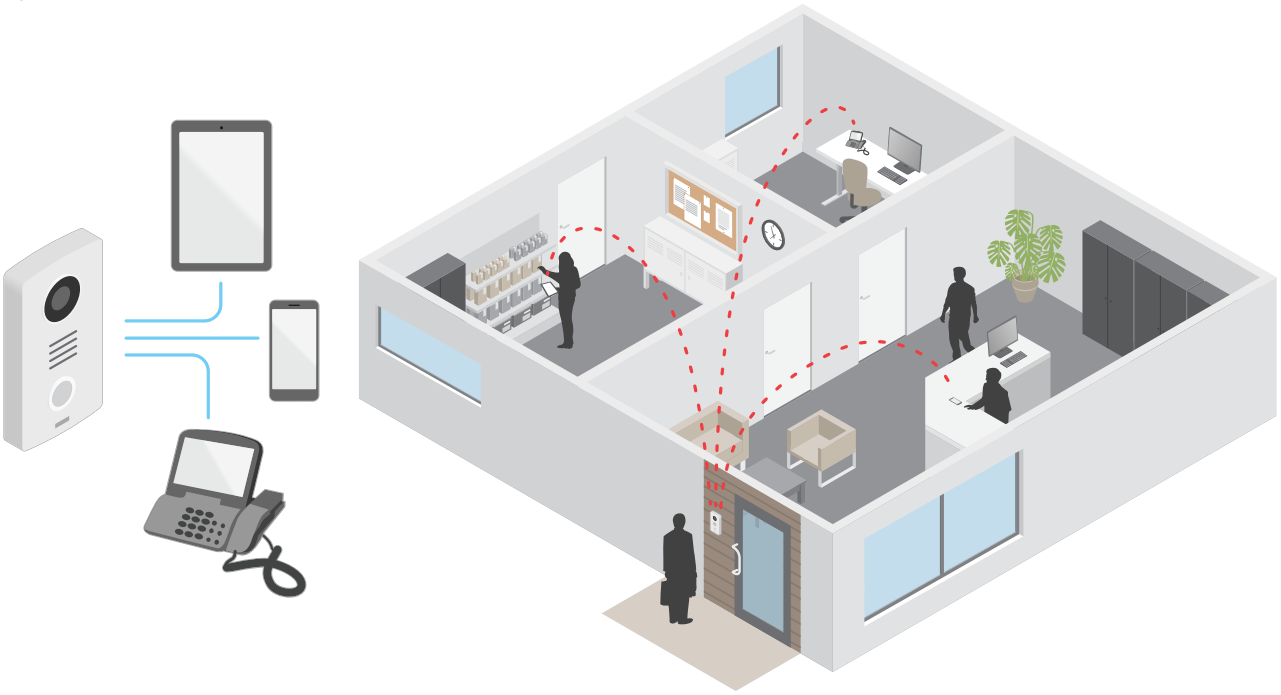
상세 정보

VoIP(Voice over IP)

VoIP(Voice over IP)는 IP 네트워크(예: 인터넷)를 통한 음성 통신 및 멀티미디어 세션을 활성화하는 기술 그룹입니다. 일반적인 전화 통화에서는 PSTN(공중 교환 전화망, Public Switched Telephone Network)에서 회로 전송을 통해 아날로그 신호가 전달됩니다. VoIP 콜에서는 로컬 IP 네트워크나 인터넷을 통해 데이터 패킷으로 보낼 수 있도록 아날로그 신호가 디지털 신호로 바뀝니다.

Axis 제품에서 VoIP는 SIP(Session Initiation Protocol) 및 DTMF(Dual-Tone Multi-Frequency) 신호를 통해 활성화됩니다.

예:



Axis 인터콤에서 통화 버튼을 누르면 사전 정의된 수신자 한 명 이상과 통화가 시작됩니다. 수신자가 응답하면 통화가 됩니다. 음성 및 영상이 VoIP 기술을 통해 전송됩니다.

SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)는 VoIP 호출을 설정, 유지 및 종료하는 데 사용됩니다. 둘 이상의 파티즉, SIP 사용자 에이전트 간에 콜을 수행할 수 있습니다. SIP 콜을 수행하려면 SIP 전화기, 소프트폰 또는 SIP 지원 Axis 장치 등을 사용할 수 있습니다.

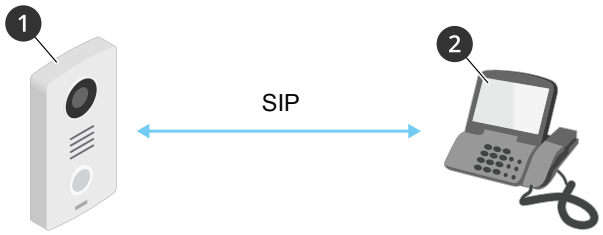
RTP(Real-Time Transport Protocol) 등의 전송 프로토콜을 사용하여 실제 오디오나 비디오가 SIP 사용자 에이전트 간에 교환됩니다.

피어 투 피어 설정을 사용하여 로컬 네트워크에서 또는 PBX를 사용하여 네트워크 간에 콜을 수행할 수 있습니다.

Peer-to-peer SIP(피어 투 피어 SIP)

가장 기본적인 유형의 SIP 통신은 둘 이상의 SIP 사용자 에이전트 간에 직접 이루어집니다. 이 통신을 peer-to-peer SIP(피어 투 피어 SIP)라고 합니다. 로컬 네트워크에서 이 통신이 이루어지면 사용자 에이전트의 SIP 주소만 있으면 됩니다. 이 경우 일반적인 SIP 주소는 `sip:<local-ip>`입니다.

예:



1 *사용자 에이전트 A - 인터콤. SIP 주소: sip:192.168.1.101*
2 *사용자 에이전트 B - SIP 지원 전화기. SIP 주소: sip:192.168.1.100*

피어 투 피어 SIP 설정을 사용하는 동일한 네트워크의 SIP 지원 전화기 등을 호출하도록 Axis 인터콤을 설정할 수 있습니다.

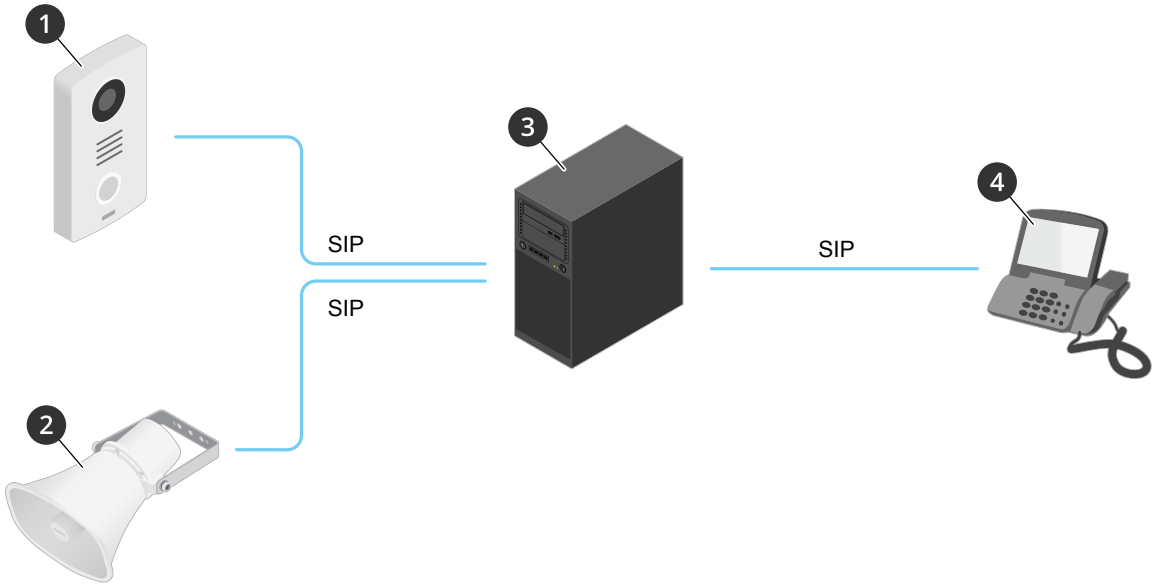
PBX(Private Branch Exchange)

로컬 IP 네트워크 외부에서 SIP 콜을 수행할 때 PBX(Private Branch Exchange)가 중앙 허브 역할을 수행할 수 있습니다. PBX의 주요 구성 요소는 SIP 프록시 또는 등록자라고도 하는 SIP 서버입니다. PBX는 기존의 스위치보드처럼 작동하며 클라이언트의 현재 상태를 표시하고 콜 전송, 음성 메일, 리디렉션 등을 허용합니다.

PBX SIP 서버는 로컬 엔터티 또는 오프 사이트로 설정됩니다. 인트라넷에서 또는 타사 공급자가 이 서버를 호스팅할 수 있습니다. 네트워크 간에 SIP 콜을 수행할 때 도달할 SIP 주소 위치를 쿼리하는 PBX 세트를 통해 콜이 라우팅됩니다.

각 SIP 사용자 에이전트는 PBX로 등록한 후 올바른 내선 번호로 전화를 걸어 다른 사용자 에이전트에 연결할 수 있습니다. 이 경우 일반적인 SIP 주소는 `sip:<user>@<domain>` 또는 `sip:<user>@<registrar-ip>`입니다. SIP 주소는 IP 주소와 별개이며, PBX는 PBX에 등록되어 있는 한 장치에 액세스할 수 있게 해줍니다.

예:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Axis 인터콤의 통화 버튼을 누르면 하나 이상의 PBX를 통해 로컬 IP 네트워크나 인터넷의 SIP 주소로 콜이 전달됩니다.

NAT 통과 기능

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

비고

라우터가 NAT 통과 및 UPnP®를 지원해야 합니다.

각 NAT 통과 프로토콜을 개별적으로 사용하거나 네트워크 환경에 따라 다른 조합으로 사용할 수 있습니다.

- **ICE** ICE(Interactive Connectivity Establishment) 프로토콜을 사용하면 피어 장치 간에 원활한 통신이 이루어지도록 가장 효율적인 경로를 찾기 쉬워집니다. STUN 및 TURN을 활성화해도 ICE 프로토콜에서 가장 효율적인 경로를 찾을 수 있는 기회가 향상됩니다.
- **STUN** - STUN(Session Traversal Utilities for NAT)은 Axis 제품이 NAT 또는 방화벽 뒤에 있는지 확인하고 그럴 경우 원격 호스트 연결용으로 할당된 매핑되어진 공용 IP 주소와 포트 번호를 가져올 수 있게 해주는 클라이언트-서버 네트워크 프로토콜입니다. IP 주소 같은 STUN 서버 주소를 입력합니다.
- **TURN** - TURN(Traversal Using Relays around NAT)은 NAT 라우터 또는 방화벽 뒤에 있는 장치가 TCP 또는 UDP를 통해 다른 호스트에서 들어오는 데이터를 수신할 수 있도록 해주는 프로토콜입니다. TURN 서버 주소 및 로그인 정보를 입력합니다.

이벤트의 룰 설정

특정 이벤트가 발생하면 장치에서 액션을 수행하도록 룰을 생성할 수 있습니다. 룰은 조건과 액션으로 구성됩니다. 조건을 사용하여 액션을 트리거할 수 있습니다. 예를 들어, 장치는 녹화를 시작하거나 모션이 감지되면 이메일을 보내거나 장치가 녹화하는 동안 오버레이 텍스트를 표시할 수 있습니다.

자세한 내용은 *이벤트 룰 시작하기*를 참조하십시오.

분석 및 앱

분석 및 앱을 통해 Axis 장치를 더욱 폭넓게 활용할 수 있습니다. AXIS Camera Application Platform (ACAP)은 타사 개발자가 Axis 장치용 분석 및 기타 앱을 개발할 수 있도록 지원하는 개방형 플랫폼입니다. 앱은 장치에 사전 설치되어 제공되거나, 무료 또는 유료(라이센스 구매)로 다운로드할 수 있습니다.

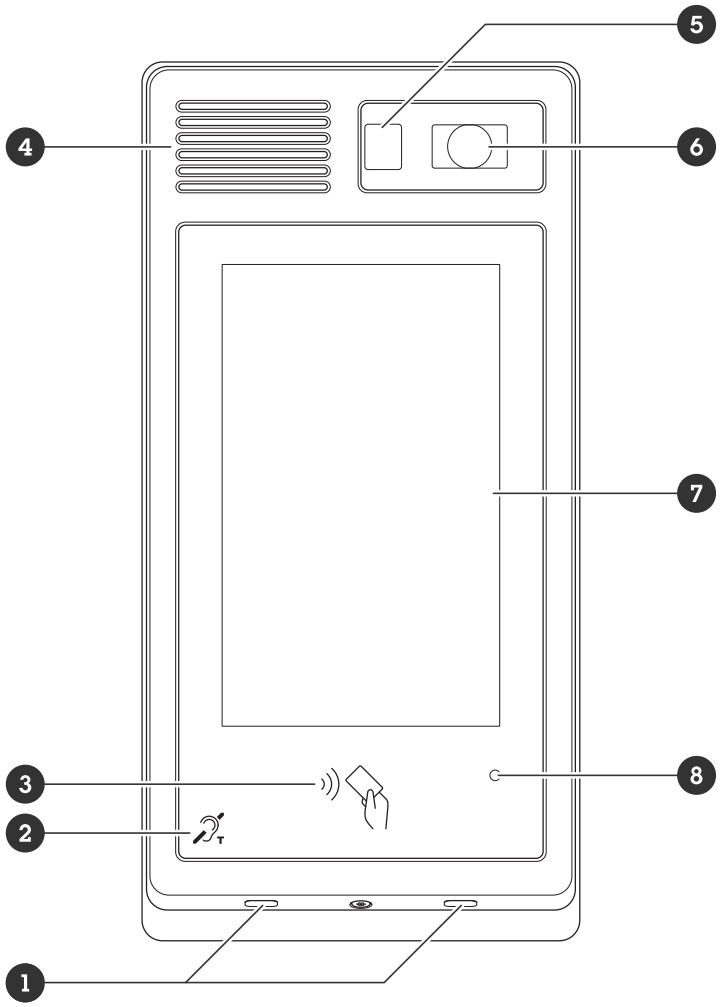
Axis 분석 및 앱에 대한 사용자 설명서는 *help.axis.com*에서 확인할 수 있습니다.

AXIS Client for Unified Communication Systems

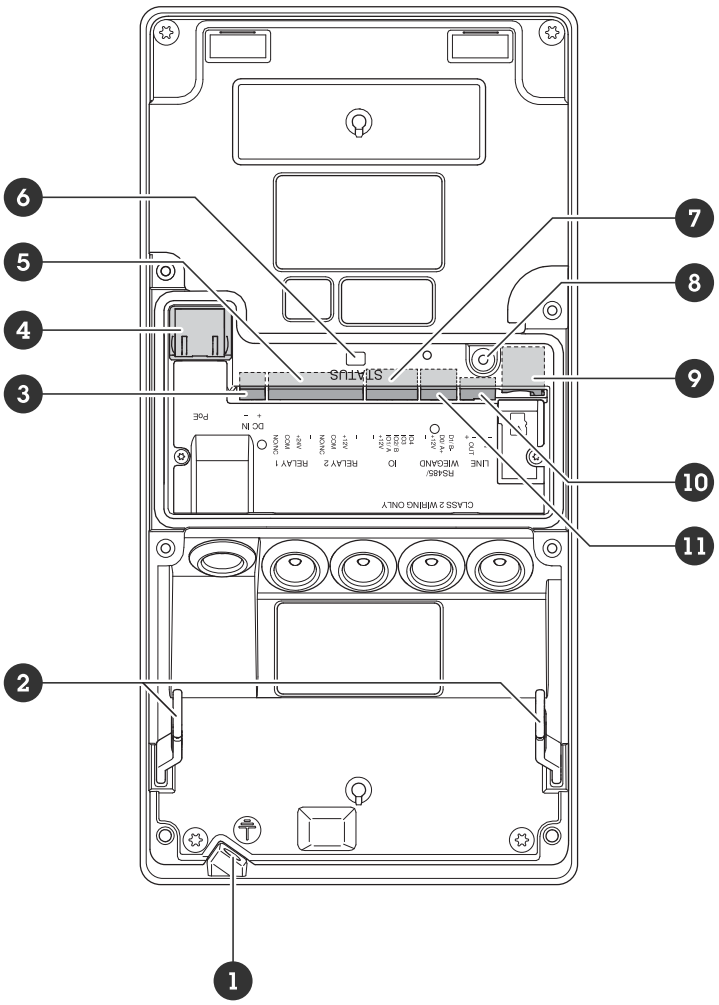
이 애플리케이션을 사용하면 SIP 지원 Axis 장치와 연결된 Microsoft® Teams 계정 간에 통화를 할 수 있습니다. 자세한 내용은 *AXIS Client for Unified Communication Systems 사용자 설명서*를 참조하십시오.

사양

제품 오버뷰



1 *마이크(2개)*
2 *T-coil*
3 *RFID 리더*
4 *스피커*
5 *PIR 센서*
6 *카메라*
7 *디스플레이*
8 *광센서*



1 *접지 나사*
2 *설치 힌지*
3 *전원 커넥터*
4 *네트워크 커넥터*
5 *릴레이 커넥터(2개)*
6 *상태 LED*
7 *I/O 커넥터*
8 *제어 버튼*
9 *SD 카드 슬롯(microSD)*
10 *오디오 커넥터*
11 *리더 커넥터*

LED 표시

상태 LED	표시
녹색	정상 작동 시 녹색이 계속 표시됩니다.

SD 카드 슬롯

통지

- SD 카드 손상 위험. SD 카드를 삽입하거나 제거할 때 날카로운 도구나 금속 물체를 사용하거나 과도한 힘을 가하지 마십시오. 손가락을 사용하여 카드를 삽입하고 제거하십시오.
- 데이터 손실 및 손상된 녹화 위험. 장치를 분리하기 전에 장치의 웹 인터페이스에서 SD 카드 마운트를 해제하십시오. 제품이 실행 중일 때는 SD 카드를 분리하지 마십시오.

이 장치는 microSD/microSDHC/microSDXC 카드를 지원합니다.

SD 카드 권장 사항은 *axis.com*을 참조하십시오.

microSD, microSDHC 및 microSDXC 로고는 SD-3C LLC의 상표입니다. microSD, microSDHC, microSDXC는 미국이나 기타 국가에서 SD-3C, LLC의 상표이거나 등록 상표입니다.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정합니다, on page 30* 항목을 참조하십시오.

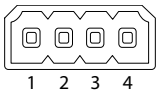
커넥터

네트워크 커넥터

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

오디오 커넥터

오디오 입력 및 출력용 4핀 단자대.

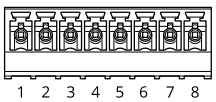


기능	핀	비고
라인 입력	1	라인 입력(모노)
GND	2	오디오 접지
라인 출력	3	라인 출력
GND	4	오디오 접지

릴레이 커넥터

다음과 같은 방식으로 사용할 수 있는 솔리드 스테이트 릴레이용 8핀 터미널 블록:

- 보조 회로를 열고 닫는 표준 릴레이.
- 잠금을 직접 제어합니다.
- 안전 릴레이를 통해 잠금을 제어합니다. 도어의 안전한 쪽에 안전 릴레이를 사용하면 핫 와이어링을 방지할 수 있습니다.



기능	핀	비고	사양
NO/NC	1	정상 개방/정상 폐쇄 릴레이 장치 연결에 사용됩니다. 두 개의 릴레이 핀은 나머지 회로와 전기적으로 분리되어 있습니다.	최대 전류 1A 최대 전압 30V DC
COM	2	공통	
24V DC	3	보조 장비에 전원을 공급하기 위해 사용합니다. 비고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	출력 전압24V DC 최대 전류 50mA[1] 최대 전류 300mA[2]
DC 접지	4		0V DC
NO/NC	5	정상 개방/정상 폐쇄 릴레이 장치 연결에 사용됩니다. 두 개의 릴레이 핀은 나머지 회로와 전기적으로 분리되어 있습니다.	최대 전류 1A 최대 전압 30V DC
COM	6	공통	
12 V DC	7	보조 장비에 전원을 공급하기 위해 사용합니다. 비고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	출력 전압 12V DC 최대 전류 100mA[1] 최대 전류 600mA[2]
DC 접지	8		0V DC

리더 커넥터

외부 리더 연결을 위한 4핀 터미널 블록.

기능	핀	비고	사양
DC 접지	1		0V DC
12 V DC	2	보조 장비에 전원을 공급하기 위해 사용합니다. 비고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	출력 전압12V DC
D0/A+	3	Wiegand: DATA0 출력 RS485: A+	
D1/B-	4	Wiegand: DATA1 출력 RS485: B-	

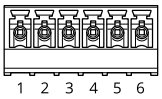
I/O 커넥터

모션 디텍션, 이벤트 트리거, 알람 알림 등과 함께 외부 장치에 I/O 커넥터를 사용합니다. I/O 커넥터는 0 VDC 기준점 및 전원(12V DC 출력) 이외에 다음에 대한 인터페이스도 제공합니다.

1. *PoE(Power over Ethernet) IEEE 802.3af/802.3at Type 1 Class 3*을 통해 전원이 공급되는 경우.
2. *PoE+(Power over Ethernet Plus) IEEE 802.3at Type 2 Class 4* 또는 *DC* 전원 입력을 통해 전원이 공급되는 경우.

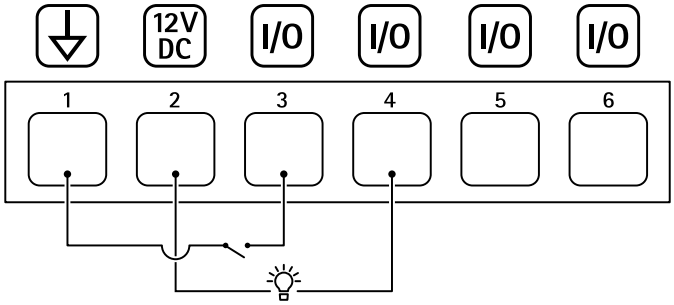
디지털 입력 - PIR 센서, 도어/윈도우 감지기, 유리 파손 감지기 등의 개방 회로와 폐쇄 회로 사이를 전환할 수 있는 장치를 연결하는 데 사용합니다.

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



기능	핀	비고	사양
DC 접지	1		0 VDC
DC 출력	2	⚠ 보조 장비에 전원을 공급할 때 사용 가능합니다. 비고: 이 핀은 정전된 경우에만 사용할 수 있습니다.	12 VDC 최대 부하 = 50mA
구성 가능(입력 또는 출력)	3–6	디지털 입력 - 활성화하려면 핀 1에 연결하고 비활성화하려면 부동 상태(연결되지 않음)로 둡니다.	0 ~ 최대 30 VDC
		디지털 출력 - 활성화된 경우 핀 1에 연결되며(DC 접지) 비활성화된 경우 부동 상태(연결되지 않음)입니다. 릴레이와 같은 유도 부하와 함께 사용할 경우 전압 과도 현상을 방지하도록 다이오드를 부하와 병렬로 연결해야 합니다.	0 ~ 최대 30 VDC, 개방 드레인, 100mA

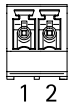
예:



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

전원 커넥터

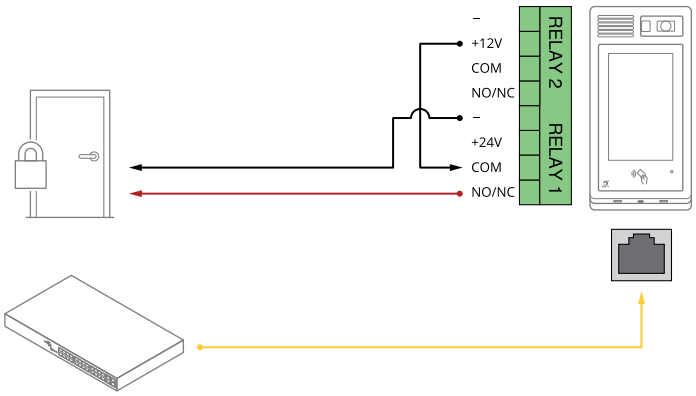
DC 전원 입력용 2핀 단자대. 정격 출력 전력이 ≤100W로 제한되거나 정격 출력 전류가 ≤5A로 제한되는 SELV(Safety Extra Low Voltage) 준수 LPS(제한된 전원)를 사용하십시오.



기능	핀	비고	사양
DC 접지	1		0V DC
DC 입력	2	PoE(Power over Ethernet) 미사용 시 컨트롤러에 전원을 공급하는 데 사용됩니다. 비고: 이 핀은 전원이 공급된 경우에만 사용할 수 있습니다.	18 ~ 28V DC, 최대 22W 출력의 최대 부하 9W

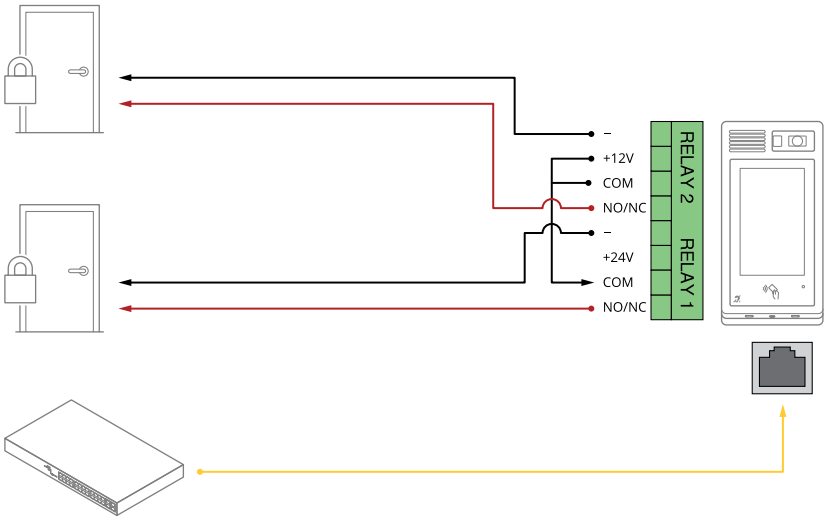
장비 연결

PoE(12V)로 구동되는 릴레이 1개



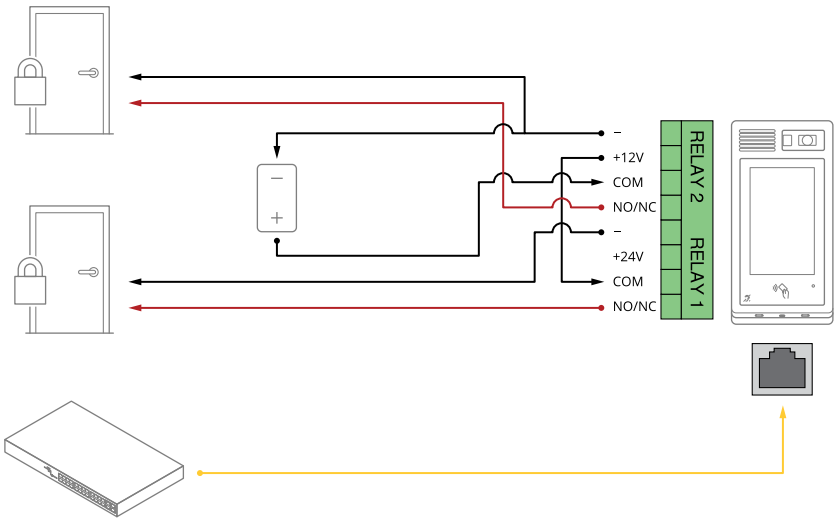
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

PoE(12V)로 구동되는 릴레이 2개



1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

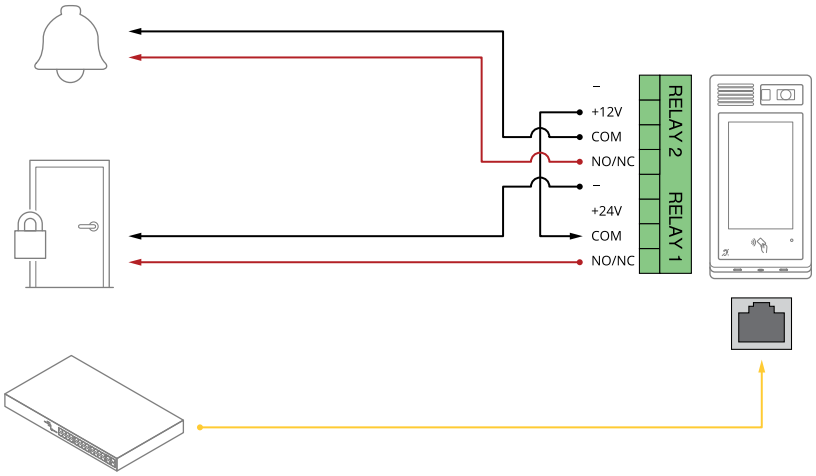
PoE(12V)로 구동되는 릴레이 1개 + 외부 전원 공급 장치로 구동되는 릴레이 1개



1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

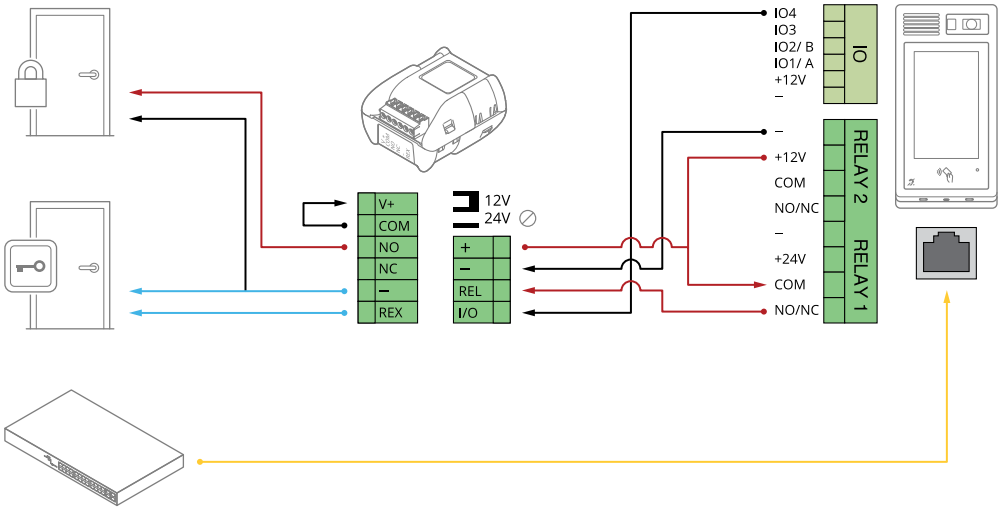
PoE(12V)로 구동되는 릴레이 1개 + 무전위 접점 릴레이 1개

예를 들어, 무전위 접점은 도어 차임벨이 될 수 있습니다.



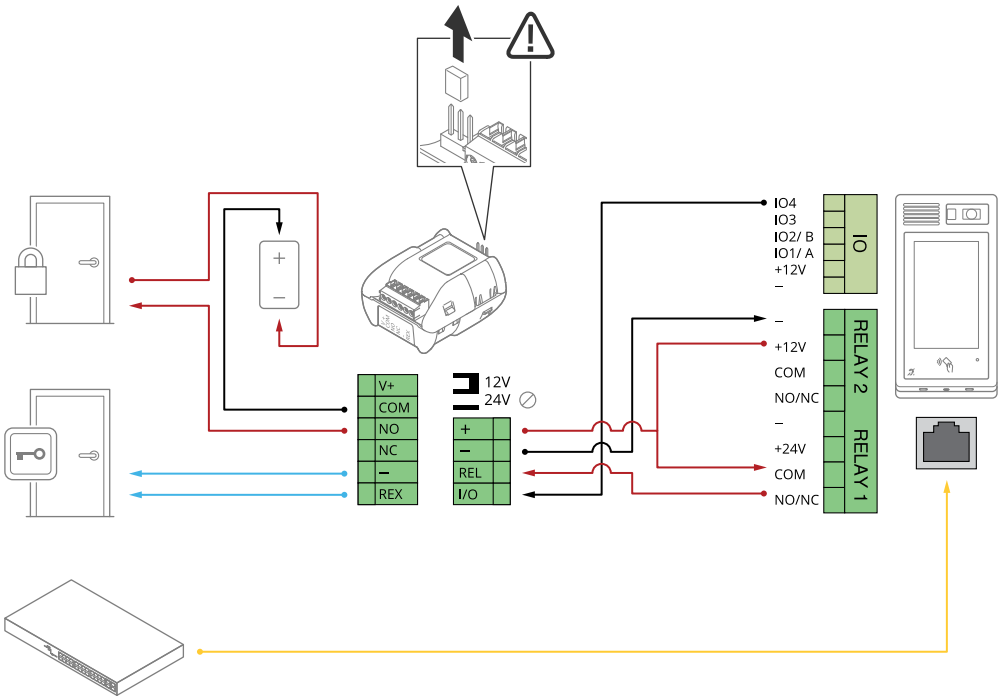
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

인터콤에서 PoE+로 전원이 공급되는 12V 페일 시큐어 잠금 장치



1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.
   - 페일 세이프 잠금용.

외부 전원 공급 장치에서 전원이 공급되는 페일 시큐어 잠금 장치

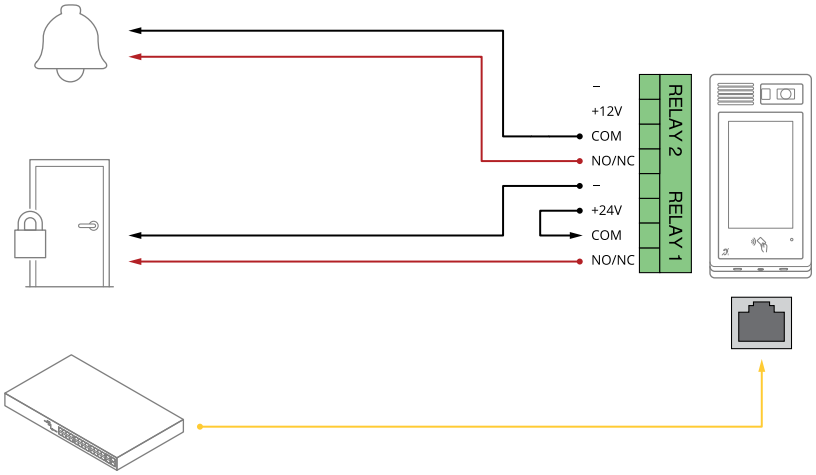


1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   - 페일 시큐어용.

– 페일 세이프 잠금용.

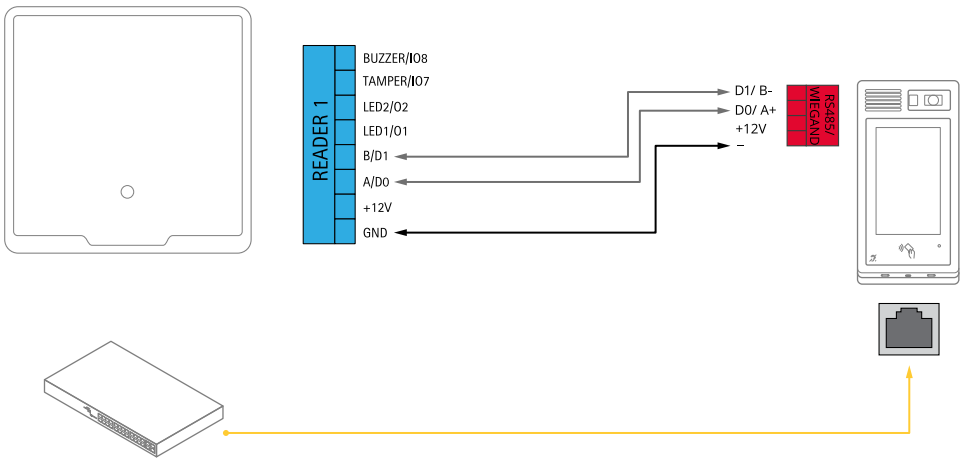
PoE(24V)로 구동되는 릴레이 1개 + 무전위 접점 릴레이 1개

예를 들어, 무전위 접점은 도어 차임벨이 될 수 있습니다.



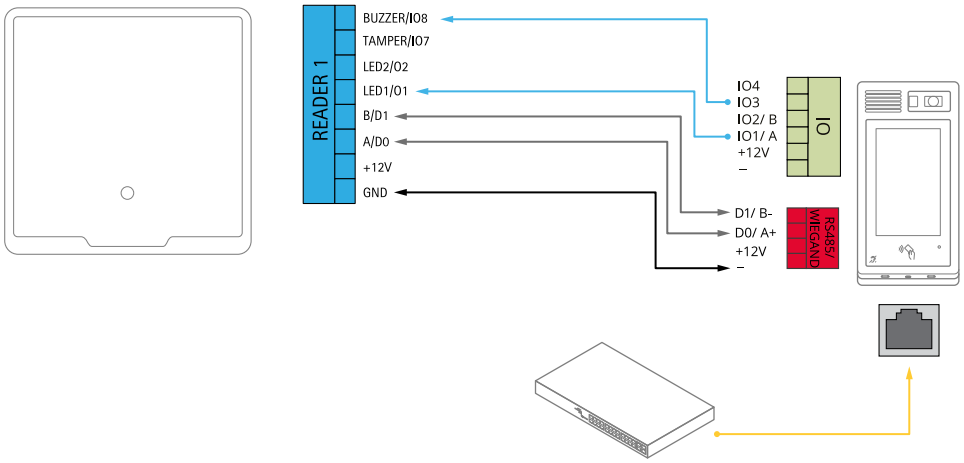
1. 릴레이 상태를 확인하려면 다음**System > Accessories(시스템 > 액세서리)**로 이동하고 릴레이 포트를 찾습니다.
2. **Normal state(기본 상태)**로 설정합니다.
   – 페일 시큐어용.
   – 페일 세이프 잠금용.

OSDP를 사용하여 도어 컨트롤러에 연결된 리더



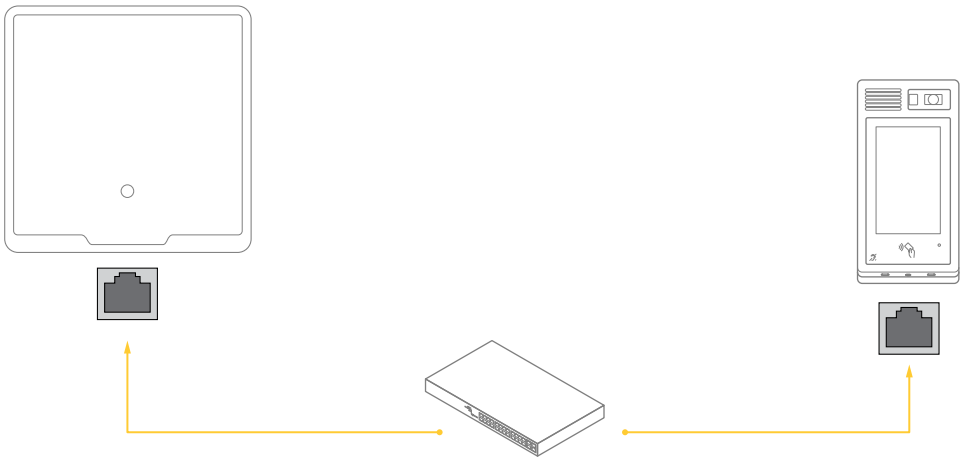
1. **Reader(리더) > Connection(연결) > Reader protocol(리더 프로토콜)**로 이동합니다.
2. **Reader protocol type(리더 프로토콜 유형)**을 **OSDP**로 설정하고 **Save(저장)**를 클릭합니다.

Wiegand를 사용하여 도어 컨트롤러에 연결된 리더



1. **Reader(리더) > Connection(연결) > Reader protocol(리더 프로토콜)**로 이동합니다.
2. **Reader protocol type(리더 프로토콜 유형)**을 **Wiegand**로 설정합니다.
3. **Beeper(알람음)**를 켭니다.
4. **Input for beeper(알람음 입력)**에서 **I3**을 선택합니다.
5. **Input used for LED control(LED 제어에 사용되는 입력)**에서 **1**을 선택합니다.
6. **Input for LED1(LED1 입력)**에서 **I1**을 선택합니다.
7. 다른 설정을 조정하고 **Save(저장)**를 클릭합니다.

VAPIX 리더를 사용하여 Axis 도어 컨트롤러에 연결된 리더



1. **Reader(리더) > Connection(연결) > Reader protocol(리더 프로토콜)**로 이동합니다.
2. **Reader protocol type(리더 프로토콜 유형)**을 **VAPIX reader(VAPIX 리더)**로 설정합니다.
3. Axis 도어 컨트롤러에 연결합니다.

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 19* 항목을 참조하십시오.
3. 상태 LED 표시기가 주황색으로 깜박일 때까지 15-30초 동안 제어 버튼을 누르고 있습니다.
4. 제어 버튼을 놓습니다. 상태 LED 표시등이 녹색으로 바뀌면 과정이 완료됩니다. 네트워크에 DHCP 서버를 이용할 수 없는 경우, 장치의 IP 주소는 다음 중 하나로 기본 설정됩니다.
   - **AXIS OS 12.0 이상이 설치된 장치:** 링크 로컬 주소 서브넷(169.254.0.0/16)에서 할당받음
   - **AXIS OS 11.11 이하가 설치된 장치:** 192.168.0.90/24
5. 설치 및 관리 소프트웨어 도구를 사용하여 IP 주소를 할당하고, 패스워드를 설정하고, 장치에 액세스합니다.
   설치 및 관리 소프트웨어 도구는 *axis.com/support*의 지원 페이지에서 제공됩니다.

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

AXIS OS 옵션

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

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

현재 AXIS OS 버전 확인

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

현재 AXIS OS 버전을 확인하려면 다음을 수행합니다.

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

AXIS OS 업그레이드

중요 사항

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

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

- 업그레이드 프로세스 중에 장치가 전원에 연결되어 있는지 확인합니다.

비고

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

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

업그레이드가 완료되면 제품이 자동으로 재시작됩니다.

기술적 문제 및 가능한 해결책

AXIS OS 업그레이드 문제

AXIS OS 업그레이드 실패

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

AXIS OS 업그레이드 후 문제

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

IP 주소 설정 문제

IP 주소를 설정할 수 없음

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

장치 액세스 관련 문제

브라우저로 장치에 액세스할 때 로그인할 수 없음

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

root 계정의 패스워드를 분실한 경우, 장치를 공장 초기화 설정으로 재설정해야 합니다. 자세한 내용은 *공장 초기화 설정으로 재설정합니다, on page 30* 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 6*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.

성능 고려 사항

시스템을 설정할 때는 서로 다른 설정과 상황이 성능에 어떤 영향을 미치는지 고려하는 것이 중요합니다. 어떤 요소는 대역폭(비트 레이트)에, 어떤 요소는 프레임 레이트에 영향을 미치며, 두 가지 모두에 영향을 미치는 요소도 있습니다.

고려해야 할 가장 중요한 요소:

- 높은 이미지 해상도 또는 낮은 압축 수준으로 인해 대역폭에 영향을 주는 데이터가 많이 포함된 이미지가 생성될 수 있습니다.
- 여러 Motion JPEG 클라이언트나 유니캐스트 H.264/H.265/AV1 클라이언트로 액세스하면 대역폭에 영향을 줍니다.
- 여러 클라이언트로 여러 스트림(해상도, 압축)을 동시에 보면 프레임 레이트와 대역폭 모두에 영향을 줍니다.
  높은 프레임 레이트를 유지해야 하는 곳에서는 동일한 스트림을 사용하십시오. 스트림 프로파일은 동일한 스트림을 보장하는데 사용할 수 있습니다.
- 서로 다른 코덱을 사용하는 비디오 스트림에 동시에 접근하면 프레임 레이트와 대역폭 모두에 영향을 미칩니다. 최적의 성능을 위해서는 동일한 코덱을 사용하는 스트림을 사용합니다.
- 이벤트 설정의 과다한 사용은 프레임 레이트에 영향을 줄 수 있는 제품의 CPU 부하에 영향을 줍니다.
- HTTPS를 사용하면 프레임 레이트가 낮아질 수 있으며 특히 Motion JPEG를 스트리밍하는 경우입니다.
- 좋지 않은 인프라로 인해 네트워크 점유율이 과중되면 대역폭에 영향을 줍니다.
- 성능이 낮은 클라이언트 컴퓨터에서 보기는 인식한 성능을 떨어뜨리고 프레임 레이트에 영향을 줍니다.
- 동시에 여러 AXIS Camera Application Platform(ACAP) 애플리케이션을 실행하면 프레임 레이트 및 일반적인 성능에 영향을 줍니다.

지원 센터 문의

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

안전 정보

위험 레벨

⚠ 위험
피하지 못한 경우 사망이나 심각한 부상이 발생하는 위험한 상황을 나타냅니다.

⚠ 경고
피하지 못한 경우 사망이나 심각한 부상이 발생할 수 있는 위험한 상황을 나타냅니다.

⚠ 주의
피하지 못한 경우 경미하거나 심하지 않은 부상이 발생할 수 있는 위험한 상황을 나타냅니다.

통지
피하지 못한 경우 재산상 손해가 발생할 수 있는 상황을 나타냅니다.

기타 메시지 레벨

중요 사항
제품이 올바르게 작동하는 데 필수적인 중요 정보를 나타냅니다.

비고
제품을 최대한으로 활용하는 데 도움이 되는 유용한 정보를 나타냅니다.

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.

T10213214_ko

2026-10 (M12.2)

© 2025 – 2026 Axis Communications AB