AXIS TP3604-E Cellular Back Box

사용자 설명서

목차

설치 3
시작하기 4
네트워크에서 장치 찾기 4
브라우저 지원 4
장치의 웹 인터페이스 열기 4
관리자 계정을 생성합니다 4
안전한 패스워드 4
아무도 장치 소프트웨어를 조작하지 않았는지 확인 5
장치 구성 6
SIM 관리 6
APN 설정 6
신호 강도 및 IP 주소 확인 6
연결 테스트 6
관리 포트 확인 6
카메라로의 포워딩 켜기 7
카메라의 IP 소유권 구성 7
Local(로컬) 모드 7
Passthrough(패스스루) 모드 8
이벤트의 룰 설정 9
액션 트리거 9
인클로저가 열릴 경우 알림 트리거하기 9
웹 인터페이스 10
사양 11
제품 오버뷰 11
LED 표시 11
버튼 12
제어 버튼 12
커넥터 12
PoE 입력 커넥터(PoE 입력) 12
네트워크 커넥터(PoE 출력) 12
전원 커넥터 12
장치 세척 13
문제 해결 14
공장 초기화 설정으로 재설정합니다 14
AXIS OS 옵션 14
현재 AXIS OS 버전 확인 14
AXIS OS 업그레이드 14
기술적 문제 및 가능한 해결책 15
지원 센터 문의 17
사이버 보안 18
취약성 관리 18
보안 알림 18
보안 제품 수명 주기 18

설치



이 비디오에서는 AXIS P32 Dome Camera Series 및 AXIS P14 Bullet Camera Series와 함께 AXIS TP3604-E Cellular Back Box를 설치하는 방법을 보여 줍니다.

모든 설치 시나리오와 안전 정보를 다루는 지침은 설치 가이드를 참조하십시오.

시작하기

네트워크에서 장치 찾기

*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. 사용자 이름과 패스워드를 입력합니다. 장치에 처음 액세스하는 경우, 관리자 계정을 생성해야 합니다. *관리자 계정을 생성합니다, on page 4* 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 4* 항목을 참조하십시오.
3. 패스워드를 다시 입력합니다.
4. 라이센스 계약을 수락하십시오.
5. **Add account(계정 추가)**를 클릭합니다.

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. 장치를 구성하고 설치합니다.

장치 구성

장치를 구성하려면 다음 단계를 거쳐야 합니다.

1. *SIM 관리, on page 6*
2. 네트워크에서 명시적인 APN(Access Point Name)을 요구하는 경우, *APN 설정, on page 6*
3. *신호 강도 및 IP 주소 확인, on page 6*
4. *연결 테스트, on page 6*
5. *관리 포트 확인, on page 6*
6. *카메라로의 포워딩 켜기, on page 7*

SIM 관리

SIM PIN이 활성화된 경우 SIM 관리는 필수입니다. SIM PIN이 비활성화된 경우 이 단계를 건너뛸 수 있습니다.

1. SIM 카드를 삽입합니다. **Modem(모뎀) > SIM management(SIM 관리) > SIM status(SIM 상태)**로 이동하여 모뎀/SIM 감지 여부를 확인합니다.
2. SIM PIN이 잠겨 있는 경우 **Modem(모뎀) > SIM management(SIM 관리) > SIM PIN > Unlock(잠금 해제)**으로 이동하여 올바른 PIN으로 잠금을 해제합니다.

APN 설정

비고

이 단계는 네트워크에서 명시적인 APN(Access Point Name)을 요구하는 경우에만 수행하면 됩니다.

명시적인 APN을 설정하려면 **Modem(모뎀) > Cellular network(셀룰러 네트워크) > APN**으로 이동합니다.

신호 강도 및 IP 주소 확인

비고

이 단계에는 셀룰러 네트워크에 대한 액세스가 필요합니다.

1. **System(시스템) > Modem(모뎀) > Cellular network(셀룰러 네트워크) > Radio parameters(무선 파라미터) > Signal strength index(신호 강도 지수)**에서 신호 강도를 확인합니다. 막대 3~4개는 양호한 신호 품질을 나타냅니다.
2. **System(시스템) > Modem(모뎀) > Cellular network(셀룰러 네트워크) > User equipment IP address(사용자 장비 IP 주소)**에서 셀룰러 네트워크 IP 주소가 수신되었는지 확인합니다.

연결 테스트

비고

이 단계에는 셀룰러 네트워크에 대한 액세스가 필요합니다.

1. **System(시스템) > Modem(모뎀) > Cellular network(셀룰러 네트워크) > Test cellular connection(셀룰러 연결 테스트)**으로 이동합니다. 호스트 이름 또는 IP 주소를 입력합니다.
2. 연결 테스트가 성공하는지 확인합니다.

관리 포트 확인

최종 라우팅 모드를 켜기 전에 백박스 관리 포트를 확인합니다.

1. **Cellular routing(셀룰러 라우팅) > Back box management ports(백박스 관리 포트)**로 이동합니다.
2. 네트워크에서 기본값을 지원하지 않는 경우 해당 포트를 변경합니다.

카메라로의 포워딩 켜기

마지막 단계는 카메라로의 포워딩을 켜는 것입니다.

1. **Cellular routing(셀룰러 라우팅) > Main mode(메인 모드)**로 이동하여 **Enable forwarding to connected device(연결된 장치로 포워딩 활성화)**를 클릭합니다.

포워딩이 활성화되면 일반 서비스 포트는 카메라로 전달되며, 백박스 관리는 예약된 관리 포트를 통해 계속 사용할 수 있습니다.

2. 카메라 액세스 테스트: 웹 브라우저에 셀룰러 IP 주소와 포트 번호 80을 `http://<cellular-ip-address>:80` 형식으로 입력합니다.
3. 백박스 액세스 테스트: 웹 브라우저에 셀룰러 IP 주소와 포트 번호 11080(HTTP용 기본 백박스 관리 포트)을 `http://<cellular-ip-address>:11080` 형식으로 입력합니다.

카메라의 IP 소유권 구성

비고

이 단계는 선택 사항이며, 기본 서브넷 동작을 변경하거나 서브넷 동작을 조정해야 하는 경우에만 필요합니다.

셀룰러 네트워크는 하나의 IP 주소만 할당하며, 해당 IP는 SIM 카드의 ID와 연결됩니다. 일반적인 설치는 백박스와 여기에 연결된 카메라로 구성됩니다. DHCP 모드는 카메라가 어떤 IP를 "소유"할지 결정합니다. 이것이 DHCP 서버 모드를 선택할 때의 핵심 판단 기준입니다.

기본적으로(Local(로컬) 모드) 셀룰러 IP는 백박스에 유지되며, 카메라에는 백박스의 로컬 네트워크에서 사설 IP가 할당됩니다. 카메라는 여전히 셀룰러 네트워크에서 완전히 액세스할 수 있습니다. 대부분의 배포 환경에서는 이것으로 충분하며, 카메라를 사설 네트워크에 안전하게 격리된 상태로 유지할 수 있습니다.

이 차이는 카메라 자체의 시각에서 IP를 확인하는 도구를 사용할 때 드러납니다. VMS가 카메라에서 보고한 IP 주소를 읽거나, 카메라가 자체 IP 주소를 비디오 오버레이에 표시하도록 구성된 경우, 해당 IP는 외부에서 카메라에 접속할 때 사용하는 공용 셀룰러 IP가 아니라 카메라의 사설 LAN IP입니다. 셀룰러 IP는 카메라가 아니라 백박스가 보유한 SIM 카드 ID에 속하므로 두 주소는 일치하지 않습니다.

Passthrough(패스스루) 모드는 셀룰러 네트워크가 백박스에 할당한 단일 IP를 카메라로 전달하여 이 문제를 해결합니다. Passthrough(패스스루)를 활성화하면 카메라가 셀룰러 네트워크에 속한 IP를 그대로 소유하므로, 카메라가 보고하는(그리고 비디오 오버레이에 표시하는) 주소는 원격 접속에 사용되는 주소와 동일합니다. 이제 카메라가 셀룰러 ID를 보유하게 되므로, 이 선택은 카메라가 셀룰러 네트워크상의 다른 사용자 장비(UE)에 액세스하는 방식에도 영향을 미칩니다.

이 섹션의 나머지 부분에서는 각 모드를 자세히 설명합니다.

백박스에 연결된 카메라에는 표준 포트(`80/443/554/22`)를 통해 셀룰러 IP로 액세스할 수 있으며, 백박스에는 예약된 관리 포트(예: `11080/11443/11554/11022`)로 계속 액세스할 수 있습니다.

Local(로컬) 모드와 Passthrough(패스스루) 모드의 차이점:

Local(로컬) 모드

- 카메라에 사설 로컬 서브넷이 할당됩니다.
- 카메라의 내부 IP 주소는 셀룰러로 액세스 가능한 IP 주소와 다릅니다.
- 확실하지 않은 경우 Local DHCP(로컬 DHCP) 모드 옵션을 사용합니다.

Passthrough(패스스루) 모드

- 카메라에 셀룰러 IP 주소가 할당됩니다.

Local(로컬) 모드

Local(로컬) 모드 켜기

1. **Cellular routing(셀룰러 라우팅) > Advanced DHCP configuration(고급 DHCP 구성) > DHCP server mode(DHCP 서버 모드)**에서 **Local(로컬)**을 선택합니다.
2. 카메라의 로컬 IP 주소가 네트워크에서 액세스 가능한 다른 IP 주소와 충돌하지 않는지 확인합니다: **Cellular routing(셀룰러 라우팅) > Advanced DHCP configuration(고급 DHCP 구성) > Local private network configuration(로컬 사설 네트워크 구성)**
3. 필요한 경우 **Cellular routing(셀룰러 라우팅) > Advanced DHCP configuration(고급 DHCP 구성) > Local private network configuration(로컬 사설 네트워크 구성)**에서 IP 주소를 변경합니다. **Starting IP address(시작 IP 주소)**와 **Ending IP address(종료 IP 주소)**에 동일한 값을 사용합니다.
4. **Save(저장)**를 클릭합니다.

Passthrough(패스스루) 모드

UE(User Equipment(사용자 장비), 즉 카메라)가 서로 통신하지 않고 트래픽이 항상 다른 VMS LAN에서 UE 쪽으로 유입되는 경우, IP 섀도잉이 발생할 수 있는 UE 간 경로가 존재하지 않습니다. 이 경우 패스스루는 IP 섀도잉 관점에서 안전한 것으로 간주됩니다.

큰 틀에서 보면 이는 셀룰러 네트워크가 카메라 쪽으로 확장된다는 의미입니다. 이 기능은 카메라가 셀룰러 외부 IP 주소에 직접 노출되어야 할 때 유용합니다.

중요 위험: 패스스루의 IP 섀도잉

이 위험 설명은 단일 카메라 설정에 적용됩니다. 카메라가 한 대뿐이더라도 패스스루에는 LAN 측 서브넷에 두 개의 IP 주소가 필요합니다.

- 하나는 카메라용 IP 주소입니다.
- 다른 하나는 이더넷 측 백박스 DHCP 서버용 IP입니다.

시나리오 1: UE당 최소 서브넷 `(/30)`

이 모델에서는 각 UE가 작고 분리된 서브넷을 갖습니다.

- `(/30)`은 사용 가능한 호스트 IP 주소 두 개를 제공합니다.
- IP 주소 하나는 카메라가 사용합니다.

남은 IP는 백박스 DHCP 서버가 내부적으로 사용합니다.

시나리오 1 권장 사항:

- 각 UE 서브넷을 분리된 상태로 유지합니다.
- 모든 UE 서브넷이 고유한지 확인합니다. UE 간에 서브넷이 중복되지 않도록 합니다.

시나리오 2: 여러 UE가 공유하는 대규모 서브넷

일부 배포 환경에서는 여러 UE가 공유하는 하나의 큰 서브넷을 사용합니다. 카메라가 백박스 DHCP 서버 IP와 동일한 IP를 사용하는 다른 UE에 접속하려고 하면 섀도잉 위험이 발생합니다. 이 경우 트래픽이 의도한 원격 UE가 아니라 로컬 백박스 측 주소로 확인될 수 있습니다.

시나리오 2 권장 사항:

- 패스스루 설정에서 백박스 DHCP 서버 IP 주소를 확인합니다.
- 이 IP 주소가 다른 UE에 할당되어 있지 않은지 확인합니다.
- 이 IP 주소가 네트워크 서비스 포털의 어떤 SIM에도 할당되어 있지 않은지 확인합니다.

Passthrough(패스스루) 모드 켜기

비고

셀룰러 네트워크에 대한 액세스가 필요합니다.

1. **Cellular routing(셀룰러 라우팅) > Advanced DHCP configuration(고급 DHCP 구성) > DHCP server mode(DHCP 서버 모드)**에서 **Passthrough(패스스루)**를 선택합니다.

2. **Cellular routing(셀룰러 라우팅) > Advanced DHCP configuration(고급 DHCP 구성) > Local private network configuration(로컬 사설 네트워크 구성) > Server IP and prefix length(서버 IP 및 접두사 길이)**에서 자동으로 선택된 서버 IP와 서브넷 접두사 길이가 액세스 가능한 다른 IP 주소와 충돌하지 않는지 확인합니다.
3. **Save(저장)**를 클릭합니다.

이벤트의 룰 설정

자세한 내용은 *이벤트 룰 시작하기*를 참조하십시오.

액션 트리거

1. **System(시스템)** > **Events(이벤트)**로 이동하여 **+ Add a rule(+ 룰 추가)**을 클릭합니다. 룰은 장치가 특정 액션을 수행하는 시간을 정의합니다. 룰을 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 충족될 때 수행할 **Action(액션)**을 선택합니다.

인클로저가 열릴 경우 알림 트리거하기

이 예시는 장치의 하우징 또는 케이스가 열렸을 때 이메일 알림을 설정하는 방법을 설명합니다.

이메일 수신자 추가:

1. **System > Events > Recipients(시스템 > 이벤트 >수신자)**로 이동하여 **Add recipient(수신자 추가)**를 클릭합니다.
2. 수신자의 이름을 입력합니다.
3. **Email(이메일)**을 알림 유형으로 선택합니다.
4. 수신자의 이메일 주소를 입력합니다.
5. 카메라에서 알림을 보낼 이메일 주소를 입력합니다.
6. 보내는 이메일 계정의 로그인 정보와 함께 SMTP 호스트 이름 및 포트 번호를 입력합니다.
7. 이메일 설정을 테스트하려면 **Test(테스트)**를 클릭합니다.
8. **Save(저장)**를 클릭합니다.

룰 만들기:

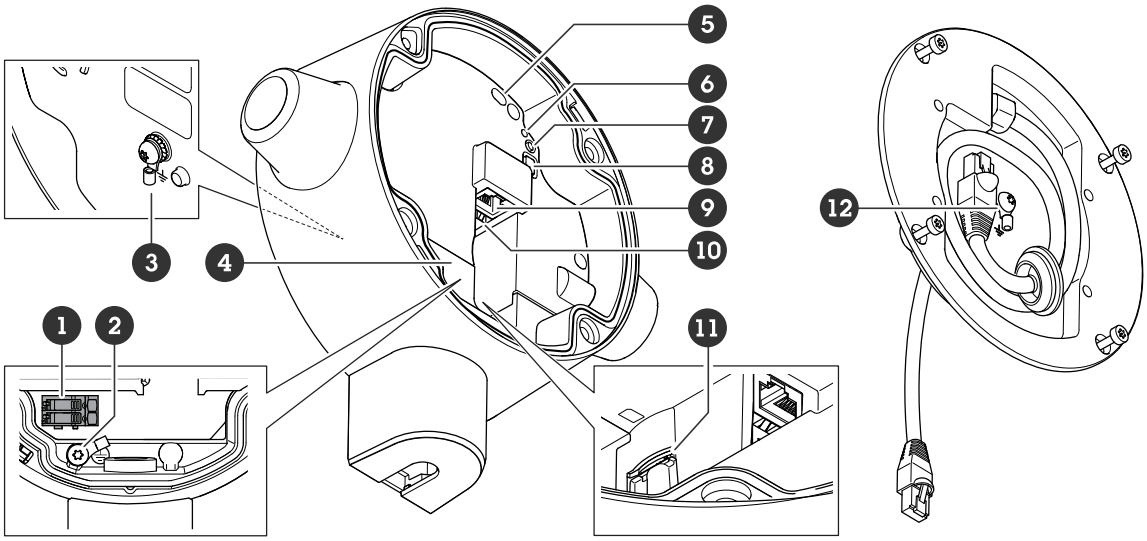
9. **System > Events > Rules(시스템 > 이벤트 > 룰)**로 이동하고 **Add a rule(룰 추가)**을 클릭합니다.
10. 룰에 대한 이름을 입력합니다.
11. 조건 목록에서 **Casing open(케이스 열림)**을 선택합니다.
12. 액션 목록에서 **Send notification to email(이메일로 알림 전송)**을 선택합니다.
13. 목록에서 수신자를 선택합니다.
14. 이메일 제목과 메시지를 입력합니다.
15. **Save(저장)**를 클릭합니다.

웹 인터페이스

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

사양

제품 오버뷰



1 *AC 커넥터*
2 *보호 접지*
3 *접지 나사*
4 *보호 커버(AC)*
5 *케이스 열림 감지기*
6 *리셋 버튼*
7 *상태 LED*
8 *제어 버튼*
9 *PoE 출력(데이터)*
10 *PoE 입력*
11 *SIM 카드 슬롯*
12 *접지 나사(카메라)*

LED 표시

설정 모드의 상태 LED

상태 LED	표시
켜져 있지 않음	케이싱 감지 IR이 가려져 있습니다.
녹색	정상 작동 중이며 이더넷 인터페이스가 준비되었습니다.
주황색	시작하는 동안 켜진 상태로 유지됩니다. 장치 소프트웨어 업그레이드 중 또는 공장 출하 시 기본값으로 재설정 시 깜박입니다.
주황색/빨간색	이더넷 연결이 없으며 시작 중에 모뎀이 구성되고 있습니다.
빨간색	장치 소프트웨어 업그레이드 실패 상태입니다.

연결 모드의 상태 LED

상태 LED	표시
켜져 있지 않음	케이싱 감지 IR이 가려져 있습니다.
녹색	모뎀이 네트워크에 연결되어 있습니다.

주황색	시작하는 동안 켜진 상태로 유지됩니다. 장치 소프트웨어 업그레이드 중 또는 공장 출하 시 기본값으로 재설정 시 깜박입니다.
주황색/빨간색	시작 중에 모뎀이 구성되고 있습니다.
빨간색	장치 소프트웨어 업그레이드 실패 상태입니다.

버튼

제어 버튼

제어 버튼의 용도는 다음과 같습니다.

- 제품을 공장 초기화 설정으로 재설정합니다. *공장 초기화 설정으로 재설정합니다, on page 14* 항목을 참조하십시오.
- 인터넷을 통해 원 클릭 클라우드 연결(O3C) 서비스에 연결합니다. 연결하려면 버튼을 누른 후 놓고, 상태 LED가 녹색으로 세 번 깜박일 때까지 기다립니다.

커넥터

PoE 입력 커넥터(PoE 입력)

PoE(Power over Ethernet) IEEE 802.3af/802.3at/802.3bt Type 3 Class 5를 지원하는 RJ45 이더넷 커넥터입니다.

비고

이 커넥터는 전원 입력에만 사용되며, 네트워크 연결은 사용할 수 없습니다.

비고

- PoE IEEE 802.3at Type 2 Class 4 출력에는 AC 입력이 필요합니다.
- PoE IEEE 802.3af Type 1 Class 3 출력을 위해서는 IEEE 802.3at Type 2 Class 4 이상이 필요합니다.
- PoE IEEE 802.3af Type 1 Class 3 입력의 경우, 장치는 작동하지만 전력을 출력하지 않습니다.

비고

이더넷 케이블의 최대 길이는 20m입니다.

네트워크 커넥터(PoE 출력)

RJ45 이더넷 커넥터

비고

- PoE IEEE 802.3at Type 2 Class 4 출력에는 AC 입력이 필요합니다.
- PoE IEEE 802.3af Type 1 Class 3 출력을 위해서는 IEEE 802.3at Type 2 Class 4 이상이 필요합니다.
- PoE IEEE 802.3af Type 1 Class 3 입력의 경우, 장치는 작동하지만 전력을 출력하지 않습니다.

비고

이더넷 케이블의 최대 길이는 20m입니다.

전원 커넥터

AC 전원을 연결하기 위한 단자대입니다.

비고

PoE IEEE 802.3at Type 2 Class 4 출력에는 AC 입력이 필요합니다.

장치 세척

미지근한 물과 순한 비연마성 비누로 장치를 세척하면 됩니다.

통지

- 자극적인 화학 물질로 인해 장치가 손상될 수 있습니다. 창문 세정제나 아세톤과 같은 화학 물질을 사용하여 장치를 세척하지 마십시오.
- 직사광선이나 고온에서 세척하면 얼룩이 생길 수 있으므로 주의해서 피해야 합니다.

1. 압축된 공기통을 사용하여 장치에서 먼지와 느슨한 오물을 제거하십시오.
2. 필요한 경우 미지근한 물과 순한 비마모성 비누로 적신 부드러운 극세사 천으로 장치를 닦으십시오.
3. 남아 있는 세척제를 제거하려면 미지근한 물에 적신 부드러운 극세사 천으로 장치를 닦으십시오.
4. 얼룩이 생기지 않도록 깨끗한 비마모성 천으로 장치를 건조시키십시오.

Axis 장치 세척에 대한 자세한 내용은 *일반 세척제에 대한 화학적 내성* 백서를 참조하십시오.

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 11* 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 14* 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.

T10233346_ko

2026-10 (M2.2)

© 2026 Axis Communications AB