

AXIS Camera Station S2224 Mk II Appliance

목차

시작하기	4
장치 설치	5
.....	5
설정 예	5
독립 감시 네트워크의 설정	5
기존 네트워크의 설정	6
스위치를 회사 네트워크에 직접 연결하기	7
장치 구성	9
초기 Axis 레코더 설정	9
서버에 접속	9
원격 서버에 연결	10
AXIS Secure Remote Access 로그인	10
AXIS Camera Station Pro 구성	10
영상 관리 시스템 시작하기	11
장치 추가	11
녹화 방법 구성	11
실시간 영상 보기	11
녹화 영상 보기	12
북마크 추가	12
녹화 내보내기	12
AXIS File Player에서 녹화 영상 재생 및 확인하기	12
네트워크 구성	12
서버 포트 구성	13
보안 고려 사항	13
시스템에 온라인 라이선스 부여	13
오프라인 상태인 시스템에 라이선스 부여	13
로컬 Windows® 사용자 계정 관리	15
사용자 계정 생성	15
관리자 계정을 생성합니다	15
로컬 사용자 그룹 생성	15
사용자 계정 삭제	15
사용자 계정 패스워드 변경	15
사용자 계정에 대한 패스워드 재설정 디스크 생성	16
AXIS Camera Station Pro 사용자 계정 관리	17
사용자 권한	17
사용자 또는 그룹 추가	17
사용자 또는 그룹 권한	18
장치 관리	21
Secure Boot 인증서 업데이트	21
인증서 상태 확인	21
권장 조치	22
BIOS를 통한 인증서 업데이트	22
Windows 업데이트를 통한 인증서 업데이트	22
현재 BIOS 버전 확인	23
BIOS 업데이트	23
Windows® 업데이트	23
Windows® 업데이트 설정 구성	23
추가적 스토리지 추가	24
베젤 분리	24
하드 드라이브 설치	24
새 녹화 스토리지 추가	25
RAID 볼륨 생성	25
Microsoft Windows®에서 RAID 볼륨 시작	26

내장 스위치 관리	27
내장 스위치 정보.....	27
스위치 관리 페이지에 로그인	27
실행 구성	27
개요.....	27
전원 관리	28
전력 할당.....	28
PoE 켜기 및 끄기	30
네트워크 오버뷰	30
포트 잠금 및 잠금 해제.....	30
설정.....	31
네트워크 설정 구성	31
날짜 및 시간 구성	31
DHCP 서버 구성	31
SNMP 구성	32
유지보수	32
펌웨어 업데이트.....	32
스위치를 재부팅합니다.....	32
스위치 설정 백업.....	32
스위치 설정 복원.....	32
인증서 관리	33
비밀번호 변경	33
웹 설정 구성	33
공장 초기화 설정으로 재설정합니다.....	33
로그.....	33
스위치 보고서 생성	34
사양	35
제품 오버뷰.....	35
전면 및 후면.....	35
LED 표시	35
문제 해결	37
서버 재설정.....	37
시스템 복구 수행.....	37
.....	37
AXIS Camera Station Pro 문제 해결	38
도움이 더 필요하십니까?	39
유용한 링크.....	39
지원 센터 문의	39

시작하기

AXIS Camera Station Pro 녹화 서버를 구성하는 표준 작업 흐름은 다음과 같습니다.

1. 장치 설치.
2. 초기 Windows® 설정: 장치를 설치한 후 지역, 언어, 키보드 레이아웃, 관리자 계정 및 패스워드를 설정하는 몇 가지 단계를 안내합니다.
3. 초기 Axis 레코더 설정: 초기 Windows 설정 후 AXIS Recorder Toolbox가 열리고 컴퓨터 이름, 날짜 및 시간, 네트워크와 같은 기본 및 필수 설정을 지정하는 몇 가지 단계가 안내됩니다. 초기 Axis 레코더 설정, on page 9을 참조하십시오.
4. Windows® 구성. 권장 사항은 다음과 같습니다.
 - Windows®를 최신 버전으로 업데이트합니다. *Windows® 업데이트, on page 23*를 참조하십시오.
 - 표준 사용자 계정을 생성합니다. *사용자 계정 생성, on page 15*를 참조하십시오.
5. AXIS Camera Station Pro를 최신 버전으로 업데이트합니다.
 - 시스템이 온라인 상태인 경우: AXIS Recorder Toolbox 앱을 열고 **Update AXIS Camera Station Pro(AXIS Camera Station Pro 업데이트)**를 클릭합니다.
 - 시스템이 오프라인 상태인 경우: *axis.com*으로 이동하여 최신 버전을 다운로드합니다.
6. AXIS Camera Station Pro 클라이언트를 시작합니다.
7. *AXIS Camera Station Pro 서버에 연결.*
8. *AXIS Camera Station Pro 구성, on page 10.*

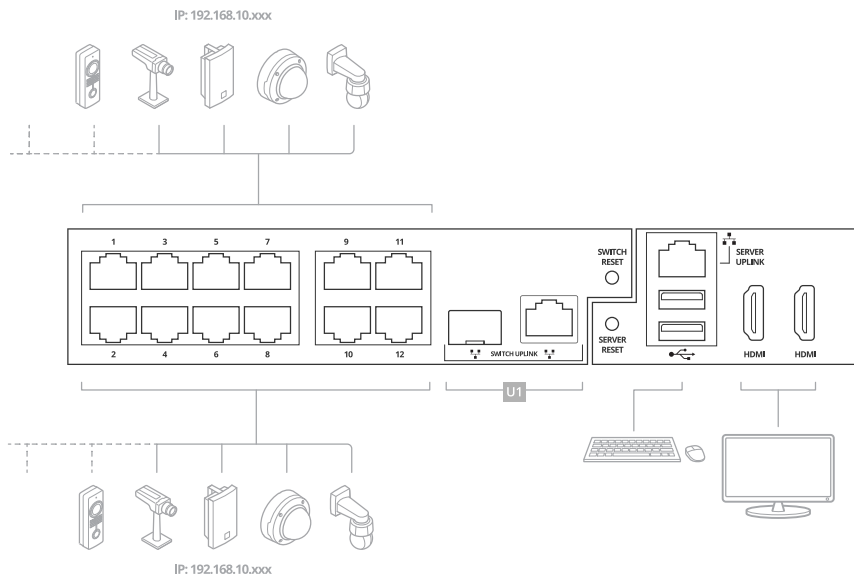
장치 설치

제품 설치 방법은 제품 상자에 동봉된 설치 가이드 또는 axis.com의 제품 지원 페이지에 있는 설치 가이드를 참조하십시오.

설정 예

독립 감시 네트워크의 설정

다른 외부 네트워크와 상호 연결되지 않은 독립 감시 네트워크를 생성할 수 있습니다. 이 설정은 기본 플러그 앤 플레이 설치입니다. 내장 스위치의 DHCP 서버는 기본적으로 활성화되어 있습니다. 카메라를 PoE 포트에 꽂으면 카메라 전원이 켜지고 IP 주소를 얻고 AXIS Camera Station Pro를 통해 해당 카메라에 액세스할 수 있습니다.



난이도	기본
이점	다른 외부 네트워크와의 상호 연결이 없는 전용 감시 네트워크 플러그 앤 플레이 설치
제한 사항	대역폭 PoE 가용량 원격 액세스 없음
필요한 조치	내장 스위치의 기본 패스워드 변경 AXIS Camera Station Pro 라이선스 등록

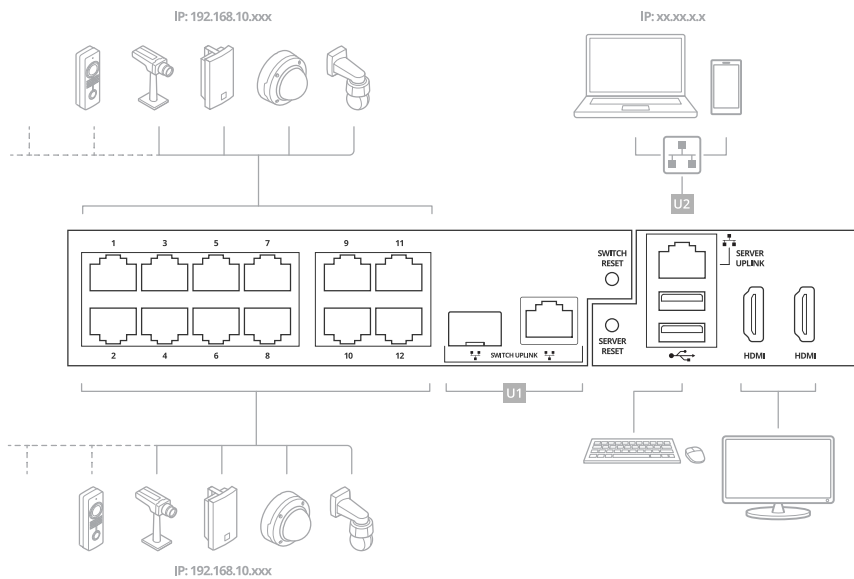
사용된 커넥터	PoE 이더넷 포트 USB 2.0 포트 (키보드용과 마우스용 각각 한 개씩) Displayport™ 또는 HDMI 커넥터
사용되지 않은 커넥터	스위치 업링크 포트 서버 업링크 포트 USB 3.2 포트 (전면) 범용 오디오 잭 (전면)

기존 네트워크의 설정

기존 네트워크 내에 감시 네트워크를 생성할 수 있습니다. 이는 감시 네트워크가 기존 네트워크와 분리됨을 의미합니다.

비고

추가 레코더(예: AXIS S30 레코더)를 사용하는 경우 기기는 녹화를 위해 네트워크 데이터를 감시 네트워크에서 서버 네트워크로 라우팅하지 않습니다. AXIS S30 Recorder가 카메라와 동일한 네트워크에 연결되어 있는지 확인하십시오.

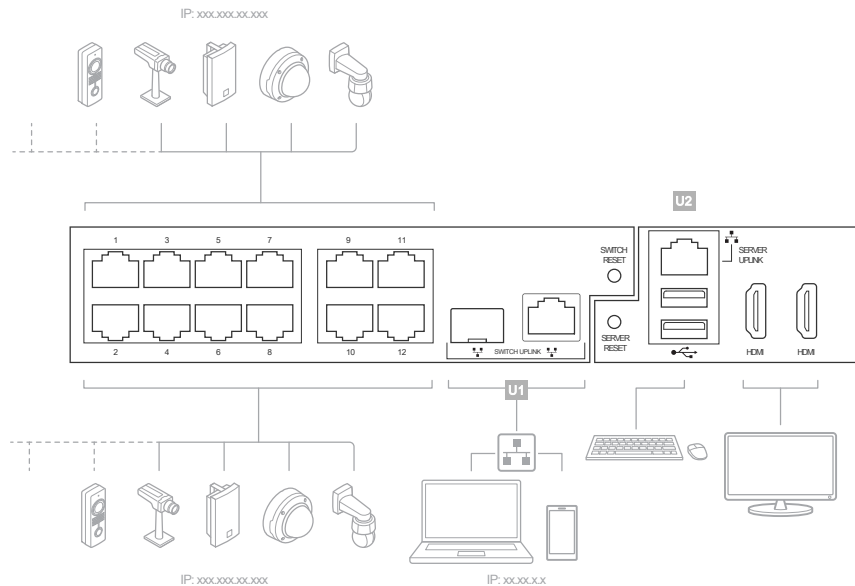


난이도	고급 수준
이점	AXIS Camera Station Pro 클라이언트를 사용하여 네트워크를 통해 S22 시리즈에 연결하는 기능. 네트워크 분리
제한 사항	회사 네트워크 정책을 따라야 할 수도 있음
필요한 조치	내장 스위치의 기본 패스워드 변경 AXIS Camera Station Pro 라이선스 등록

사용된 커넥터	PoE 이더넷 포트 이더넷 포트 - 네트워크 연결을 위한 서버 업링크 (선택 사항) USB 2.0 포트 (키보드용과 마우스용 각각 한 개씩) (선택 사항) Displayport™ 또는 HDMI 커넥터
사용되지 않은 커넥터	스위치 업링크 포트 USB 3.2 포트 (전면) 범용 오디오 잭 (전면)

스위치를 회사 네트워크에 직접 연결하기

이 설정을 사용하면 시스템이 기존 기업 네트워크에 직접 통합되어 네트워크의 어느 곳에서나 카메라에 액세스하고 모니터링할 수 있습니다.



난이도	고급 수준
이점	카메라는 회사 네트워크에서 액세스/접근할 수 있으며 SNMP 서버로 모니터링할 수 있습니다.
제한 사항	회사 네트워크 정책을 따라야 할 수도 있음
필요한 조치	스위치에서 DHCP 끄기 스위치의 IP 주소를 회사 네트워크의 고정 IP 주소로 변경합니다. PC의 내부 NIC를 DHCP 또는 회사 네트워크의 정적 IP로 설정하세요. 스위치의 기본 패스워드를 변경합니다. AXIS Camera Station Pro 구성 및 등록하기

사용된 커넥터	PoE 이더넷 포트 스위치 업링크 포트 (U1) (선택 사항) USB 2.0 포트 (키보드용과 마우스용 각각 한 개씩) (선택 사항) Displayport™ 또는 HDMI 커넥터
사용되지 않은 커넥터	PC 업링크 포트(U2) USB 3.2 포트 (전면) 범용 오디오 잭 (전면)

장치 구성

초기 Axis 레코더 설정

Windows®를 구성하면 AXIS Recorder Toolbox가 자동으로 열리고 최초 구성 설정 도우미를 통해 안내를 시작합니다. 이 설정 도우미에서는 AXIS Recorder Toolbox에서 장치를 관리하기 전에 몇 가지 기본 및 필수 설정을 구성할 수 있습니다.

비고

서버에 대한 설정입니다. 스위치의 설정을 변경하려면 스위치의 관리 페이지로 이동하십시오. 설정, on page 31를 참조하십시오.

1. **Light(밝게)** 또는 **Dark(어둡게)** 테마를 선택하고 **Next(다음)**를 클릭합니다(귀하의 제품에 사용 가능한 경우).
2. 원하는 경우 컴퓨터 이름을 변경하고 **Next(다음)**를 클릭합니다.
3. **Date and time(날짜 및 시간)**에서 다음 설정을 구성하고 **Next(다음)**를 클릭합니다.
 - 시간대를 선택합니다.
 - NTP 서버를 설정하려면 **NTP server(NTP 서버)**를 선택하고 NTP 서버 주소를 입력합니다.
 - 수동으로 설정하려면 **Manual(수동)**을 선택하고 날짜 및 시간을 선택합니다.
4. **Network settings(네트워크 설정)**에서 다음 설정을 구성하고 **Next(다음)**를 클릭합니다.
 - **Use automatic IP settings (DHCP)(자동 IP 설정 사용(DHCP))** 및 **Use automatic DNS settings(자동 DNS 설정 사용)**는 기본적으로 설정되어 있습니다.
 - DHCP 서버가 있는 네트워크에 장치가 연결되어 있으면 할당된 IP 주소, 서브넷 마스크, 게이트웨이 및 기본 설정 DNS가 자동으로 표시됩니다.
 - 네트워크에 장치가 연결되어 있지 않거나 사용 가능한 DHCP 서버가 없으면 네트워크 요구 사항에 따라 IP 주소, 서브넷 마스크, 게이트웨이 및 기본 DNS를 수동으로 입력합니다.
5. **Finish(마침)**를 클릭. 컴퓨터 이름을 변경한 경우 AXIS Recorder Toolbox에서 장치를 다시 시작하라는 메시지를 표시합니다.

서버에 접속

AXIS Camera Station S2224 Mk II Appliance 클라이언트를 사용하면 다음과 같은 다양한 방법으로 단일 서버 또는 여러 서버에 연결할 수 있습니다.

최근 사용한 서버 - 이전 세션에서 사용했던 서버에 연결합니다.

이 컴퓨터 - 클라이언트와 동일한 컴퓨터에 설치된 서버에 연결합니다.

원격 서버 - 원격 서버에 연결, on page 10를 참조하십시오.

비고

- 서버에 처음 연결할 때 클라이언트는 서버 인증서 ID를 확인합니다. 올바른 서버에 연결하고 있는지 확인하려면 인증서 ID를 AXIS Camera Station S2224 Mk II Appliance 서비스 제어에 표시된 ID와 비교합니다.

Server list(서버 목록)	서버 목록에서 서버에 연결하려면 서버 목록 드롭다운 메뉴에서 서버를 선택합니다.  을 선택하여 서버 목록을 생성하거나 편집합니다.
서버 목록 내보내기	AXIS Camera Station에서 내보낸 서버 목록 파일을 가져오려면 Import server list(서버 목록 가져오기) 를 클릭하고 .msl 파일을 찾습니다.

Delete saved passwords(저장된 패스워드 삭제)	연결된 모든 서버에 저장된 사용자 이름 및 패스워드를 삭제하려면 Delete saved passwords(저장된 패스워드 삭제) 를 클릭합니다.
Change client proxy settings(클라이언트 프록시 설정 변경)	서버에 연결할 수 없는 경우, 클라이언트 프록시 설정을 업데이트해야 할 수도 있습니다. 클라이언트 프록시 설정 변경 을 클릭합니다.

원격 서버에 연결

1. **원격 서버**를 선택합니다.
2. **Remote server(원격 서버)** 드롭다운 목록에서 서버를 선택하거나 IP 주소 또는 DNS 주소를 입력합니다. 서버가 목록에 없는 경우, 을(를) 클릭하여 사용할 수 있는 모든 원격 서버 목록을 새로 고칩니다. 서버가 기본 포트 번호 55754와 다른 포트 번호를 가진 클라이언트를 허용하도록 구성하려면 192.168.0.5:46001과 같이 IP 주소를 포트 번호와 붙여서 입력합니다.
3. 다음 중 하나를 시도하십시오.
 - 현재 Windows® 사용자로 로그인하려면 **Log in as current user(현재 사용자로 로그인)**를 선택합니다.
 - **Log in as current user(현재 사용자로 로그인)** 선택을 취소하고 **Log in(로그인)**을 클릭합니다. 다른 자격 증명으로 로그인하려면 **Other user(다른 사용자)**를 선택하고 다른 사용자 이름 및 패스워드를 입력합니다.

AXIS Secure Remote Access 로그인

중요 사항

보안과 기능을 향상하기 위해 **Axis Secure Remote Access(v1)**를 **Axis Secure Remote Access v2**로 업그레이드하고 있습니다. 현재 버전은 2025년 12월 1일에 지원이 중단되므로 그 전에 Axis Secure Remote Access v2로 업그레이드할 것을 적극 권장합니다.

이것이 AXIS Camera Station S2224 Mk II Appliance 시스템에 어떤 의미가 있나요?

- 2025년 12월 1일 이후에는 **Axis Secure Remote Access(v1)**를 사용하여 시스템에 원격으로 액세스할 수 없습니다.
- **Axis Secure Remote Access v2**를 사용하려면 AXIS Camera Station Pro 버전 6.8로 업그레이드해야 합니다. 이 업그레이드는 현재 2026년 3월 1일까지 모든 AXIS Camera Station 5 사용자에게 무료로 제공됩니다.

비고

- Axis Secure Remote Access를 사용하여 서버에 연결하려고 할 때 서버가 클라이언트를 자동으로 업그레이드할 수는 없습니다.
 - 프록시 서버가 네트워크 장치와 AXIS Camera Station S2224 Mk II Appliance 서버 사이에 있는 경우, AXIS Secure Remote Access를 사용하여 서버에 액세스하려면 AXIS Camera Station S2224 Mk II Appliance 서버의 Windows에서 프록시 설정을 구성해야 합니다.
1. **AXIS Secure Remote Access 로그인** 링크를 클릭합니다.
 2. MyAxis 계정 자격 증명을 입력합니다.
 3. **Sign in(로그인)**을 클릭합니다.
 4. **Grant(허용)**을 클릭합니다.

AXIS Camera Station Pro 구성

시작하기 전:

- 설치에 따라 네트워크를 구성하십시오. **네트워크 구성**을 참조하십시오.
- 필요한 경우 서버 포트를 구성하십시오. **서버 포트 구성**을 참조하십시오.

- 보안 문제를 고려하십시오. 보안 고려 사항을 참조하십시오.

필요한 구성을 마쳤으면 AXIS Camera Station Pro로 작업을 시작할 수 있습니다.

1. 영상 관리 시스템 시작하기
2. 장치 추가
3. 녹화 방법 구성, on page 11
4. 실시간 영상 보기, on page 11
5. 녹화 영상 보기, on page 12
6. 북마크 추가, on page 12
7. 녹화 내보내기, on page 12
8. AXIS File Player에서 녹화 영상 재생 및 확인하기, on page 12

영상 관리 시스템 시작하기

AXIS Camera Station Pro 클라이언트 아이콘을 두 번 클릭하여 클라이언트를 시작합니다. 클라이언트를 처음 시작할 때 클라이언트와 동일한 컴퓨터에 설치된 AXIS Camera Station Pro 서버에 로그인을 시도합니다.

다양한 방법으로 다수의 AXIS Camera Station Pro 서버에 연결할 수 있습니다.

장치 추가

AXIS Camera Station S2224 Mk II Appliance을 처음 시작하면 **Add devices(장치 추가)** 페이지가 열리고 네트워크에서 추가할 장치를 검색합니다.

1. 목록에서 추가하려는 장치를 선택합니다. 장치를 찾을 수 없는 경우 **Manual search(수동 검색)**를 클릭하거나 입력하여 필터링합니다.
2. **추가**를 클릭합니다.
3. 구성을 건너뛰고 나중에 계속하려면 **Close(닫기)**를 클릭합니다. 지금 구성을 계속하는 방법:
 - 3.1. **Quick configuration(빠른 구성)** 또는 **Site Designer configuration(Site Designer 구성)**을 선택합니다. 자세한 내용은 을(를) 참조하십시오.
 - 3.2. 오버레이가 아직 없는 Axis 카메라에 날짜, 시간 및 텍스트 오버레이를 추가하려면 **Add image overlay for date, time, and text(날짜, 시간 및 텍스트용 이미지 오버레이 추가)**를 선택합니다.
 - 3.3. **Next(다음)**를 클릭합니다.
 - 3.4. **Recording method(녹화 방법)** 기본 설정을 선택합니다.
 - 3.5. **Next(다음)**를 클릭합니다.
 - 3.6. **Retention time(보존 기간)** 및 **Recording storage(녹화 스토리지)**를 선택하고 **Finish(마침)**를 클릭하여 구성을 적용합니다.

녹화 방법 구성

1. 구성 > 녹화 및 이벤트 > 녹화 방법으로 이동합니다.
2. 카메라를 선택합니다.
3. **Motion detection(모션 디텍션)** 또는 **Continuous(연속)** 아니면 둘 다 켭니다.
4. **Apply(적용)**를 클릭합니다.

실시간 영상 보기

1. **Live view(실시간 보기)** 탭을 엽니다.
2. 실시간 영상을 보려면 카메라를 선택합니다.

녹화 영상 보기

1. **Recordings(녹화)** 탭을 엽니다.
2. 녹화 영상을 보려는 카메라를 선택합니다.

북마크 추가

1. 녹화 영상으로 이동.
2. 타임라인을 확대하거나 축소하고 이동하여 마커를 원하는 위치에 놓습니다.
3.  을 클릭합니다.
4. 북마크 이름과 설명을 입력합니다. 키워드를 사용하여 북마크를 쉽게 찾을 수 있도록 합니다.
5. 녹화 영상을 잠그려면 **녹화 영상 삭제 방지**를 선택합니다.

비고

Prevent recording deletion(녹화 영상 삭제 방지)의 선택을 취소하거나 북마크를 삭제하면 녹화 영상 잠금이 해제됩니다.

6. **OK(확인)**를 클릭하여 북마크를 저장합니다.

녹화 내보내기

1. **Recordings(녹화)** 탭을 엽니다.
2. 녹화 영상을 내보내려는 카메라를 선택합니다.
3.  을 클릭하여 선택 마커를 표시합니다.
4. 마커를 끌어서 내보낼 녹화 영상을 포함시킵니다.
5.  을 클릭하여 **Export(내보내기)** 탭을 엽니다.
6. **Export(내보내기)**를 클릭합니다...

AXIS File Player에서 녹화 영상 재생 및 확인하기

1. 내보낸 녹화 영상이 있는 폴더로 이동합니다.
2. AXIS File Player를 두 번 클릭합니다.
3.  을 클릭하여 녹화의 메모를 표시합니다.
4. 디지털 서명을 확인하려면 다음을 수행합니다.
 - 4.1. **Tools > Verify digital signature(도구 > 디지털 서명 확인)**로 이동합니다.
 - 4.2. **Validate with password(패스워드로 확인)**를 선택하고 패스워드를 입력합니다.
 - 4.3. **Verify(검증)**를 클릭하여 검증 결과를 확인합니다.

비고

- 디지털 서명은 signed video와 다릅니다. Signed video를 사용하면 녹화 영상이 생성된 카메라까지 추적할 수 있으므로 녹화 영상이 변조되지 않았는지 확인할 수 있습니다. 카메라의 사용자 설명서에서 자세한 내용은 **서명된 영상**을 참조하십시오.
- 저장된 파일이 AXIS Camera Station 데이터베이스와 연결되지 않은 경우(인덱싱되지 않은 파일), AXIS File Player에서 재생할 수 있도록 변환해야 합니다. 파일 변환에 대한 도움이 필요하다면 Axis 기술 지원에 문의하십시오.

네트워크 구성

클라이언트, 서버 및 연결된 네트워크 장치가 서로 다른 네트워크에 있는 경우 AXIS Camera Station S2224 Mk II Appliance를 사용하기 전에 프록시 또는 방화벽 설정을 구성합니다.

클라이언트 프록시 설정

클라이언트와 서버 사이에 프록시 서버가 있는 경우 클라이언트 컴퓨터의 Windows에서 프록시 설정을 구성합니다. 자세한 내용은 Axis 지원 센터에 문의하십시오.

서버 프록시 설정

프록시 서버가 네트워크 장치와 서버 사이에 있는 경우 서버의 Windows에서 프록시 설정을 구성해야 합니다. 자세한 내용은 Axis 지원 센터에 문의하십시오.

NAT 및 방화벽

NAT 또는 방화벽이 클라이언트와 서버를 분리하는 경우 AXIS Camera Station S2224 Mk II Appliance Service Control에 지정된 HTTP 포트, TCP 포트 및 스트리밍 포트가 통과할 수 있도록 NAT 또는 방화벽을 구성합니다. 도움이 필요하면 네트워크 관리자에게 문의하십시오.

서버 포트 구성

AXIS Camera Station S2224 Mk II Appliance 서버는 서버와 클라이언트 간 통신에 55752(HTTP), 55754(TCP), 55756(모바일 통신), 55757(모바일 스트리밍) 포트를 사용합니다. 필요하다면 AXIS Camera Station Service Control에서 포트를 변경할 수 있습니다.

보안 고려 사항

카메라 및 녹화 영상에 대한 무단 접근을 방지하는 방법:

- 모든 네트워크 장치(카메라, 비디오 엔코더 및 보조 장치)에 강력한 패스워드를 사용하십시오.
- AXIS Camera Station S2224 Mk II Appliance 서버, 카메라, 비디오 엔코더 및 보조 장치를 사물 네트워크와 분리된 보안 네트워크에 설치합니다. 인터넷에 접속된 네트워크와 같은 다른 네트워크의 컴퓨터에 AXIS Camera Station S2224 Mk II Appliance 클라이언트를 설치할 수 있습니다.
- 모든 사용자가 강력한 패스워드를 사용해야 합니다.

시스템에 온라인 라이선스 부여

자동 라이선스를 사용하려면 시스템을 등록하고 조직에 이를 연결해야 합니다.

1. **Configuration(구성) > Licenses(라이선스) > Management(관리)**로 이동합니다.
2. **Automatic licensing(자동 라이선스)**이 켜져 있는지 확인합니다.
3. **Register...(등록...)**를 클릭합니다.
4. My Axis 계정을 사용하여 로그인하고 화면의 지침을 따릅니다.
5. **Go to AXIS License Manager(AXIS License Manager로 이동)**를 클릭하여 라이선스를 관리합니다. 자세한 내용은 *help.axis.com*의 *My Systems 사용자 설명서*를 참조하십시오.

오프라인 상태인 시스템에 라이선스 부여

시스템에 수동으로 라이선스를 부여하려면 다음을 수행합니다.

1. **Configuration(구성) > Licenses(라이선스) > Management(관리)**로 이동합니다.
2. **Automatic licensing(자동 라이선스)**을 끕니다.
3. **Export system file...(시스템 파일 내보내기...)**을 클릭하고 컴퓨터에 파일을 저장합니다.

비고

AXIS License Manager에 접근하려면 인터넷에 연결해야 합니다. 클라이언트 컴퓨터에 인터넷이 없는 경우 인터넷이 있는 컴퓨터로 시스템 파일을 복사합니다.

4. *AXIS License Manager*를 엽니다.
5. AXIS License Manager에서 다음을 수행합니다.

- 5.1. 정확한 조직을 선택하거나 아직 만들지 않았다면 생성합니다. 자세한 내용은 *help.axis.com*의 *My Systems* 사용자 설명서를 참조하십시오.
- 5.2. **System setup(시스템 설정)**으로 이동합니다.
- 5.3. **Upload system file(시스템 파일 업로드)**을 클릭합니다.
- 5.4. **Upload system file(시스템 파일 업로드)**을 클릭하고 시스템 파일을 선택합니다.
- 5.5. **Upload system file(시스템 파일 업로드)**을 클릭합니다.
- 5.6. **Download license file(라이선스 파일 다운로드)**을 클릭합니다.
6. AXIS Camera Station S2224 Mk II Appliance 클라이언트로 돌아갑니다.
7. **Import license file...(라이선스 파일 가져오기...)**을 클릭하고 라이선스 파일을 선택합니다.
8. **Go to AXIS License Manager(AXIS License Manager로 이동)**를 클릭하여 라이선스를 관리합니다.

로컬 Windows® 사용자 계정 관리

사용자 계정 생성

개인 데이터 및 정보를 보다 안전하게 유지하려면 각 로컬 계정에 대한 패스워드를 추가하는 것이 좋습니다.

중요 사항

로컬 계정의 패스워드를 생성했으면 잊어버리지 마십시오. 로컬 계정의 패스워드를 잊어버렸을 때 복구할 방법은 없습니다.

1. **Settings (설정) > Accounts (계정) > Other users (다른 사용자) > Add other user (다른 사용자 추가)** 그리고 **Add account (계정 추가)**를 클릭합니다.
2. **I don't have this person's sign-in information(이 사용자의 로그인 정보가 없습니다.)**을 클릭합니다.
3. **Add a user without a Microsoft account(Microsoft 계정 없이 사용자 추가)**를 클릭합니다.
4. 사용자 이름, 패스워드 및 패스워드 힌트를 입력합니다.
5. **Next(다음)**를 클릭하고 지침을 따릅니다.

관리자 계정을 생성합니다

1. **Settings > Accounts > Other people(설정 > 계정 > 다른 사용자)**로 이동합니다.
2. 변경할 계정으로 이동하고 **Change account type(계정 유형 변경)**을 클릭합니다.
3. **Account type(계정 유형)**으로 이동하고 **Administrator(관리자)**를 선택합니다.
4. **확인**을 클릭합니다.
5. 장치를 재시작하고 새 관리자 계정으로 로그인합니다.

로컬 사용자 그룹 생성

1. **Computer Management(컴퓨터 관리)**로 이동합니다.
2. **Local Users and Groups > Group(로컬 사용자 및 그룹 > 그룹)**으로 이동합니다.
3. **Group(그룹)**을 마우스 오른쪽 버튼으로 클릭하고 **New Group(새 그룹)**을 선택합니다.
4. 그룹 이름 및 설명을 입력합니다.
5. 다음을 통해 그룹 구성원을 추가합니다.
 - 5.1. **추가**를 클릭합니다.
 - 5.2. **고급**을 클릭합니다.
 - 5.3. 그룹에 추가할 사용자 계정을 찾고 **OK(확인)**를 클릭합니다.
 - 5.4. 다시 **OK(확인)**를 클릭합니다.
6. **Create(생성)**를 클릭합니다.

사용자 계정 삭제

중요 사항

계정을 삭제할 때 로그인 화면에서 사용자 계정을 제거합니다. 또한 사용자 계정에 저장된 모든 파일, 설정 및 프로그램 데이터를 제거합니다.

1. **Settings > Accounts > Other people(설정 > 계정 > 다른 사용자)**로 이동합니다.
2. 제거할 계정으로 이동하고 **Remove(제거)**를 클릭합니다.

사용자 계정 패스워드 변경

1. 관리자 계정으로 로그인합니다.

2. **User Accounts > User Accounts > Manage another account in sequence(사용자 계정 > 사용자 계정 > 순서대로 다른 계정 관리)**로 이동합니다.
장치의 모든 사용자 계정이 있는 목록이 표시됩니다.
3. 패스워드를 변경할 사용자 계정을 선택합니다.
4. **Change the password(패스워드 변경)**를 클릭합니다.
5. 새 패스워드를 입력하고 **Change password(패스워드 변경)**를 클릭합니다.

사용자 계정에 대한 패스워드 재설정 디스크 생성

USB 플래시 드라이브에서 패스워드 재설정 디스크를 생성하는 것이 좋습니다. 이를 통해 패스워드를 재설정할 수 있습니다. 패스워드 재설정 디스크가 없으면 패스워드를 재설정할 수 없습니다.

비고

Windows® 10 이상을 사용 중인 경우에는 패스워드를 잊어버렸을 경우를 대비하여 로컬 계정에 보안 질문을 추가할 수 있으므로 패스워드 재설정 디스크를 생성할 필요가 없습니다. 이렇게 하려면 **Start(시작)**로 이동하고 **Settings > Sign-in options > Update your security questions(설정 > 로그인 옵션 > 보안 질문 업데이트)**를 클릭합니다.

1. 로컬 사용자 계정으로 장치에 로그인합니다. 연결된 계정의 경우 패스워드 재설정 디스크를 생성할 수 없습니다.
2. 빈 USB 플래시 드라이브를 장치에 연결합니다.
3. Windows® 검색 필드에서 **Create a password reset disk(패스워드 재설정 디스크 만들기)**로 이동합니다.
4. **Forgotten Password(패스워드를 잊은 경우)** 설정 도우미에서 **Next(다음)**을 클릭하십시오.
5. USB 플래시 드라이브를 선택하고 **Next(다음)**를 클릭합니다.
6. 현재 패스워드를 입력하고 **Next(다음)**를 클릭합니다.
7. 화면의 지침을 따릅니다.
8. USB 플래시 드라이브를 제거하고 안전한 곳에 보관하십시오. 패스워드를 여러 번 변경해도 패스워드를 변경할 때 새 디스크를 생성할 필요가 없습니다.

AXIS Camera Station Pro 사용자 계정 관리

사용자 권한

Configuration(구성) > Security(보안) > User permissions(사용자 권한)로 이동하여 AXIS Camera Station S2224 Mk II Appliance의 사용자 및 그룹을 확인합니다.

비고

AXIS Camera Station S2224 Mk II Appliance 서버를 실행하는 컴퓨터의 관리자에게는 AXIS Camera Station S2224 Mk II Appliance의 관리자 권한이 자동으로 부여됩니다. 관리자 그룹의 권한을 변경하거나 제거할 수 없습니다.

사용자 또는 그룹을 추가하기 전에 해당 사용자 또는 그룹이 로컬 컴퓨터에 등록되어 있거나 Windows® Active Directory 사용자 계정이 있는지 확인합니다. 사용자나 그룹을 추가하려면 **사용자 또는 그룹 추가**를 참조하십시오.

사용자가 그룹에 속한 경우 개인 또는 그룹에 할당된 역할 권한 중 가장 높은 권한이 해당 사용자에게 부여됩니다. 예를 들어, 카메라 X에 대한 접근 권한이 있는 사용자가 카메라 Y와 Z에 대한 접근 권한이 있는 그룹에도 속해 있으면 세 카메라 모두에 접근할 수 있습니다.

	입력 항목이 단일 사용자인 경우입니다.
	해당 항목이 그룹임을 표시합니다.
이름:	로컬 컴퓨터 또는 Active Directory에 나타나는 사용자 이름입니다.
도메인	사용자 또는 그룹이 속한 도메인입니다.
역할	사용자 또는 그룹에 할당된 접근 권한입니다. 가능한 값은 다음과 같습니다. 관리자, 조작자, 관찰자
세부항목	로컬 컴퓨터 또는 Active Directory에 표시되는 상세 사용자 정보입니다.
서버	사용자 또는 그룹이 속한 서버입니다.

사용자 또는 그룹 추가

Microsoft Windows®와 Active Directory 사용자 및 그룹은 AXIS Camera Station S2224 Mk II Appliance에 접근할 수 있습니다. AXIS Camera Station S2224 Mk II Appliance에 사용자를 추가하려면 Windows®에 사용자 또는 그룹을 추가해야 합니다.

Windows® 10 및 11에서 사용자를 추가하려면 다음과 같이 하십시오.

- Windows 키 + X를 누르고 **Computer Management(컴퓨터 관리)**를 선택합니다.
- **Computer Management(컴퓨터 관리)** 창에서 **Local Users and Groups(로컬 사용자 및 그룹) > Users(사용자)**로 이동합니다.
- **Users(사용자)**를 마우스 오른쪽 버튼으로 클릭하고 **New User(새 사용자)**를 선택합니다.
- 팝업 대화 상자에서 새 사용자의 세부 정보를 입력하고 **User must change password at next login(다음 로그인 시 사용자가 패스워드를 변경해야 함)** 확인란의 선택을 취소합니다.
- **Create(생성)**를 클릭합니다.

Active Directory 도메인을 사용하는 경우 해당 네트워크 관리자에게 문의하십시오.

사용자 또는 그룹 추가

1. **Configuration > Security > User permissions(구성 > 보안 > 사용자 권한)**로 이동합니다.
2. **추가**를 클릭합니다. 사용 가능한 사용자와 그룹이 목록에 표시됩니다.
3. **Scope(범위)**에서 사용자와 그룹을 검색할 위치를 선택합니다.

4. **Show(표시)**에서 사용자 또는 그룹 표시를 선택합니다. 사용자나 그룹이 너무 많으면 검색 결과가 표시되지 않을 수 있습니다. 필터를 사용하여 검색 결과의 범위를 좁힙니다.
5. 사용자 또는 그룹을 선택하고 **Add(추가)**를 클릭합니다.

범위	
서버	로컬 컴퓨터에서 사용자 또는 그룹을 검색하려면 선택합니다.
도메인	Active Directory 사용자 또는 그룹을 검색하려면 선택합니다.
선택된 서버	여러 AXIS Camera Station S2224 Mk II Appliance 서버에 연결된 경우 서버를 선택하여 해당 서버의 사용자나 그룹을 검색합니다.

사용자 또는 그룹 구성

1. 목록에서 사용자 또는 그룹을 선택합니다.
2. **Role(역할)**에서 **Administrator(관리자)**, **Operator(운영자)** 또는 **Viewer(관찰자)**를 선택합니다.
3. **Operator(운영자)** 또는 **Viewer(관찰자)**를 선택하면 사용자 또는 그룹 권한을 구성할 수 있습니다. *사용자 또는 그룹 권한*을 참조하십시오.
4. **Save(저장)**를 클릭합니다.

사용자 또는 그룹 제거

1. 사용자 또는 그룹을 선택합니다.
2. **Remove(제거)**를 클릭합니다.
3. 팝업 대화 상자에서 **예**를 클릭하여 사용자 또는 그룹을 제거합니다.

사용자 또는 그룹 권한

사용자 또는 그룹에 할당할 수 있는 역할은 세 가지입니다. 사용자 또는 그룹에 대한 역할을 정의하는 방법은 *사용자 또는 그룹 추가(를)* 참조하십시오.

Administrator(관리자): - 모든 카메라의 실시간 및 녹화 영상, 모든 I/O 포트 및 보기에 대한 접근을 포함하여 전체 시스템에 대한 전체 접근 권한이 주어집니다. 시스템 구성에 접근하려면 이 역할이 필요합니다.

Operator(운영자): - 실시간 및 녹화 영상에 접근할 수 있도록 카메라, 보기 및 I/O 포트를 선택합니다. 운영자는 시스템 구성을 제외한 AXIS Camera Station S2224 Mk II Appliance의 모든 기능에 접근할 수 있습니다.

Viewer(관찰자): - 특정 카메라, I/O 포트 및 보기의 실시간 영상에 접근합니다. 관찰자는 녹화된 영상 또는 시스템 구성에 접근할 수 없습니다.

카메라

Operator(운영자) 또는 **Viewer(관찰자)** 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다.

액세스	카메라와 모든 카메라 기능에 접근하도록 허용합니다.
비디오	카메라에서 실시간 영상에 접근하도록 허용합니다.
오디오 듣기	카메라에서 듣기에 접근하도록 허용합니다.

오디오 말하기	카메라와의 대화를 허용합니다.
Manual Recording(수동 녹화)	녹화를 수동으로 시작하고 중지할 수 있도록 허용합니다.
Mechanical PTZ(기계식 PTZ)	기계식 PTZ 컨트롤에 대한 접근을 허용합니다. 기계식 PTZ가 있는 카메라에서만 사용할 수 있습니다.
PTZ 우선 순위	PTZ 우선 순위를 설정합니다. 숫자가 작을수록 우선 순위가 높습니다. 할당된 우선 순위가 0으로 설정되지 않았습니다. 관리자의 우선 순위가 가장 높습니다. 우선 순위가 높은 역할이 PTZ 카메라를 작동하면 다른 카메라는 기본적으로 10초 동안 동일한 카메라를 작동할 수 없습니다. 기계식 PTZ가 있으며 Mechanical PTZ(기계식 PTZ) 가 선택된 카메라에서만 사용할 수 있습니다.

보기

Operator(운영자) 또는 **Viewer(관찰자)** 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다. 여러 보기를 선택하고 접근 권한을 설정할 수 있습니다.

액세스	AXIS Camera Station S2224 Mk II Appliance의 보기에 대한 액세스를 허용합니다.
Edit(편집):	AXIS Camera Station S2224 Mk II Appliance에서 보기를 편집할 수 있도록 허용합니다.

I/O

Operator(운영자) 또는 **Viewer(관찰자)** 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다.

액세스	I/O 포트에 대한 전체 권한을 허용합니다.
읽기	I/O 포트의 상태를 변경하지 않고 확인할 수 있도록 허용합니다.
Write(쓰기)	I/O 포트의 상태를 변경할 수 있도록 허용합니다.

시스템

목록에서 회색으로 표시된 접근 권한은 구성할 수 없습니다. 확인 표시는 해당 사용자 또는 그룹이 기본적으로 이 권한을 가지고 있음을 의미합니다.

Operator(운영자) 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다. **Take snapshots(스냅샷 촬영)**는 **Viewer(관찰자)** 역할에도 사용 가능합니다.

스냅샷 찍기	실시간 보기 및 녹화 모드에서 스냅샷을 촬영할 수 있도록 허용합니다.
녹화 내보내기	녹화 내보내기를 허용합니다.
사고 보고서 생성	사고 보고서 생성을 허용합니다.

Prevent access to recordings older than(오래된 녹화 영상에 접근 방지)	지정된 기간(분)보다 오래된 녹화 영상에는 접근하지 못하게 합니다. 사용자가 검색할 때 이러한 녹화 영상은 검색 결과에 나타나지 않습니다.
알람, 작업 및 로그에 접근	알람 알림을 받고 Alarms and tasks(알람 및 작업) 바와 Logs(로그) 탭에 접근을 허용합니다.
접근 데이터 검색	이벤트 발생 시 발생한 상황을 추적하기 위해 데이터 검색을 허용합니다.
이벤트에 카테고리 추가	Recordings(녹화 영상) 탭에서 이벤트에 카테고리를 추가할 수 있도록 허용합니다.
이벤트에서 카테고리 제거	Recordings(녹화 영상) 탭에서 이벤트에서 카테고리를 제거할 수 있도록 허용합니다.

접근 제어

Operator(운영자) 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다.
Access Management(접근 관리)는 **Viewer(관찰자)** 역할에서도 사용할 수 있습니다.

접근 제어 구성	도어와 구역, 식별 프로파일, 카드 형식 및 PIN, 암호화 통신, 다중 서버를 구성할 수 있도록 허용합니다.
접근 관리	접근 관리 기능을 사용하고 Active Directory 설정에 접근할 수 있도록 허용합니다.

Viewer(관찰자) 역할을 가진 사용자 또는 그룹은 다음 액세스 권한을 사용할 수 있습니다.

시스템 상태 모니터링

Operator(운영자) 역할을 통해 사용자 또는 그룹에 대해 다음 접근 권한을 사용할 수 있습니다.
Viewer(관찰자) 역할은 **시스템 상태 모니터링에 접근**할 수도 있습니다.

시스템 상태 모니터링의 구성	시스템 상태 모니터링을 구성할 수 있도록 허용합니다.
시스템 상태 모니터링에 접근	시스템 상태 모니터링에 접근할 수 있도록 허용합니다.

장치 관리

Secure Boot 인증서 업데이트

Microsoft는 2026년 6월에 2011년 Secure Boot 인증서의 사용을 종료하고 새로운 2023년 인증서로 대체합니다. 레코더를 안전하게 보호하려면 그 전에 2023년 인증서를 설치합니다.

2023년 인증서를 설치하려면 Windows 10 LTSC(Long-Term Servicing Channel) 또는 Windows 11 LTSC가 필요합니다. 기기가 보증 기간 내에 있지만 LTSC 버전 대신 Windows 10 SAC(Semi-Annual Channel)를 실행 중인 경우, Axis 기술 지원에 문의하십시오. Axis 기술 지원팀에서는 BIOS를 업데이트하거나 인증서를 변경하기 전에 LTSC 버전으로 업그레이드할 수 있는지 확인해 줄 수 있습니다.

비고

2023년 인증서가 없는 장치는 2026년 6월 이후에도 정상적으로 계속 작동하지만 Windows Boot Manager 업데이트 및 새로운 취약점에 대한 해지 목록을 비롯한 초기 부팅 프로세스의 새로운 보안 보호 기능은 제공받지 못합니다.

인증서 상태 확인

2023년 인증서가 설치되고 Windows 부트로더가 업데이트되었는지 확인하려면 다음 방법 중 하나를 사용합니다.

방법 1:

1. **Registry Editor(레지스트리 편집기)**를 엽니다.
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Service로 이동합니다.
3. **UEFICA2023Status** 값을 확인합니다. 값이 **Updated(업데이트됨)**으로 표시되면 2023년 인증서가 설치된 것입니다.

(Default)	REG_SZ	(value not set)
BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
ConfidenceLevel	REG_SZ	No Data Observed - Action Required
ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
UEFICA2023Status	REG_SZ	Updated
WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

방법 2:

1. **Windows Security(Windows 보안)**를 엽니다.
2. **Device security(장치 보안)**로 이동합니다.
3. **Secure boot**에서 상태 메시지를 확인합니다. 인증서가 최신 상태이면 카드에 다음 메시지가 표시됩니다. "Secure Boot가 켜져 있으며 필요한 모든 인증서 업데이트가 적용되었습니다." 더 이상 인증서 변경이 필요하지 않습니다."

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

비고

Windows 보안은 장치에 2026년 4월 14일 누적 업데이트 또는 그 이후 업데이트가 설치된 경우에만 인증서 상태를 표시합니다. 인증서 상태 메시지가 표시되지 않으면 최신 Windows 업데이트를 설치하거나 방법 1을 사용합니다.

권장 조치

BIOS 업데이트를 수행하면 2023년 인증서가 펌웨어에 영구적으로 저장됩니다. 이 방법이 가장 신뢰할 수 있으며 Windows 업데이트를 통해 인증서를 이미 설치한 경우에도 이 방법을 권장합니다.

중요 사항

Windows 업데이트를 통해서만 인증서를 설치한 후 BIOS Secure Boot 키를 공장 출하 시 기본값으로 재설정하면 인증서가 손실되고 Secure Boot가 켜진 상태에서 장치가 시작되지 않습니다. Secure Boot 키를 재설정하기 전에 BIOS를 업데이트하여 인증서를 영구적으로 저장합니다.

BIOS를 통한 인증서 업데이트

사용 중인 모델에 명시된 BIOS 버전 이상을 설치합니다. Axis.com의 제품 페이지에서 다운로드할 수 있습니다.

모델	최소 BIOS 버전
AXIS S2208	TBC
AXIS S2212	TBC
AXIS S2216	TBC
AXIS S2224	TBC
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Windows 업데이트를 통한 인증서 업데이트

해당 모델의 BIOS 업데이트가 아직 제공되지 않는 경우에는 대신 Windows 업데이트를 통해 2023년 인증서를 받을 수 있습니다.

중요 사항

이 방법으로 설치한 인증서는 펌웨어가 아닌 현재 Secure Boot 데이터베이스에 저장됩니다. BIOS Secure Boot 키를 공장 출하 시 기본값으로 재설정하면 인증서가 손실되며 Secure Boot가 켜진 상태에서 장치가 시작되지 않을 수 있습니다. 이미 이 방법을 사용했더라도 해당 모델의 BIOS 업데이트가 제공되는 즉시 설치합니다.

이 경로를 사용하는 방법:

1. 장치에서 Windows 10 LTSC 또는 Windows 11 LTSC를 실행하고 있는지 확인합니다.
2. 2026년 4월 14일 또는 그 이후에 릴리스된 모든 Windows 업데이트를 설치합니다.
3. **Windows Security(Windows 보안) > Device security(장치 보안) > Secure Boot**로 이동하여 인증서 상태를 확인합니다.
4. 최신 업데이트를 설치한 후에도 인증서가 업데이트되지 않으면 **UEFICA2023Status** 레지스트리 값을 확인합니다. 장치가 계속 자동 업데이트 대상이 아닌 경우 BIOS를 업데이트하거나 Axis 기술 지원팀에 문의하십시오.

중요 사항

사용 중인 환경의 모든 복구 미디어, 부팅 환경 및 드라이버가 2023년 인증서로 서명되었는지 확인하기 전에는 2011년 인증서를 수동으로 해지하지 마십시오. 2011년 인증서를 너무 일찍 해지하면 Secure Boot가 켜진 상태에서 장치를 시작할 수 없게 됩니다.

현재 BIOS 버전 확인

현재 BIOS를 확인하려면:

1. 장치 전원을 켜고 Axis 로고가 나타날 때까지 **DEL** 키를 반복해서 누릅니다.
2. 버전 번호는 **Main(메인)** 아래의 첫 번째 항목에 표시됩니다.

BIOS 업데이트

BIOS 파일 다운로드 페이지에서 제공되는 BIOS 가이드의 지침을 따릅니다.

Windows® 업데이트

Windows®는 정기적으로 업데이트를 확인합니다. 사용 가능한 업데이트가 있으면 장치에서 업데이트를 자동으로 다운로드하지만 수동으로 설치해야 합니다.

비고

예약된 시스템 재시작을 수행하는 동안에는 녹화가 중단됩니다.

수동으로 업데이트를 확인하려면 다음을 수행합니다.

1. **Settings (설정) > Windows Update (윈도우 업데이트)**로 이동합니다.
2. **Check for updates(업데이트 확인)**를 클릭합니다.

Windows® 업데이트 설정 구성

필요에 따라 Windows® 업데이트 수행 방법과 시기를 변경할 수 있습니다.

비고

예약된 시스템 재시작을 수행하는 동안 진행 중인 모든 녹화가 중지됩니다.

1. 앱 실행을 엽니다.
 - **Windows System > Run(Windows 시스템 > 실행)**으로 이동
2. gpedit.msc를 입력하고 **OK**를 클릭합니다. 로컬 그룹 정책 편집기가 열립니다.
3. **Computer Configuration > Administrative Templates > Windows Components > Windows Update(컴퓨터 구성 > 관리 템플릿 > Windows 구성 요소 > Windows 업데이트)**로 이동합니다.
4. 원하는 대로 설정을 구성합니다(예 참조).

예:

사용자 개입 없이 업데이트를 자동으로 다운로드하여 설치하고 필요할 때 업무 시간 외에 장치를 재시작하려면 다음 구성을 사용합니다.

1. **Always automatically restart at the scheduled time(항상 예약된 시간에 자동으로 다시 시작)**을 열고 다음을 선택합니다.
 - 1.1. **활성화**
 - 1.2. **<screen-element>The restart timer will give users this much time to save their work (minutes)(작업 저장을 위해 사용자에게 주어지는 다시 시작 대기 시간(분))**: 15.
 - 1.3. **확인**을 클릭합니다.
2. **Configure Automatic Updates(자동 업데이트 구성)**를 열고 다음을 선택합니다.
 - 2.1. **활성화**
 - 2.2. **Configure Automatic updates(자동 업데이트 구성)**: Auto download and schedule the install(자동으로 다운로드하고 설치를 예약)
 - 2.3. **Schedule Install day(예약된 설치 날짜)**: Every Sunday(매주 일요일)
 - 2.4. **Schedule Install time(예약된 설치 시간)**: 00:00
 - 2.5. **확인**을 클릭합니다.

3. **Allow Automatic Updates immediate installation(자동 업데이트로 바로 설치 허용)**을 열고 다음을 선택합니다.
 - 3.1. **활성화**
 - 3.2. **확인**을 클릭합니다.

추가적 스토리지 추가

저장 요구 사항은 다를 수 있습니다. 저장된 데이터의 보존 기간이나 고해상도 녹화 영상을 저장하기 위해 더 많은 스토리지를 설치해야 하는 경우가 종종 있습니다. 이 섹션에서는 AXIS S22 Series 제품에 추가 하드 드라이브를 설치하는 방법에 대해 설명합니다.

비고

해당 AXIS S22 제품에 추가 스토리지를 추가하려면 아래 지침을 따르십시오. 이 지침은 있는 그대로 제공되며 Axis Communications AB는 이 단계 동안 데이터 또는 잘못된 구성의 손실에 대해 책임을 지지 않습니다. 업무상 중요한 데이터를 백업하려면 표준 예방 조치를 취해야 합니다. 다음 스토리지 확장 절차는 Axis 기술 지원에서 지원되지 않습니다.

비고

정전기 방전을 방지하기 위해, 내부 시스템 구성 요소 작업 시 항상 정전기 방지 매트와 정전기 방지 스트랩을 사용하는 것이 좋습니다.

보증

보증에 대한 자세한 정보는 www.axis.com/support/warranty에서 확인할 수 있습니다.



이 비디오를 시청하려면 이 문서의 웹 버전으로 이동하십시오.

베젤 분리

1. 베젤 양쪽에 있는 두 개의 엄지 나사를 풀니다.
2. 베젤 분리.

하드 드라이브 설치

▲ 주의

- AXIS S22 시리즈와 함께 사용하도록 테스트 및 승인된 하드 드라이브만 사용하십시오.
- 하드 드라이브를 설치할 때 하드 드라이브 캐리어를 끝까지 밀어 넣었는지 확인하세요. 드라이브 캐리어가 잠기면 클릭 소리가 들립니다.
- 하드 드라이브를 설치하기 전에 전원 코드가 분리되어 있는지 확인하십시오.
 1. 시스템을 종료하고 전원이 꺼져 있는지 확인하십시오.
 2. 전원 코드 연결을 끊습니다.
 3. 하드 드라이브 캐리어 전면의 분리 단추를 누르고 하드 드라이브 캐리어 핸들을 엽니다.
 4. 손잡이를 사용하여 하드 드라이브 캐리어를 당겨 빼냅니다.
 5. 하드 드라이브 캐리어에 하드 드라이브를 삽입하십시오.
 6. 나사 4개를 사용하여 하드 드라이브를 하드 드라이브 캐리어에 고정합니다.
 7. 캐리어가 후면 판에 연결될 때까지 하드 드라이브 캐리어를 하드 드라이브 슬롯에 삽입하십시오.
 8. 하드 드라이브 캐리어 핸들을 닫아 하드 드라이브를 제자리에 고정시킵니다.

9. 전면 베젤을 부착합니다.
10. 시스템을 시작하십시오.

새 녹화 스토리지 추가

1. Windows에서 하드 디스크 파티션을 새로 만들고 포맷합니다:
 - 1.1. **Start menu(시작 메뉴)**를 마우스 오른쪽 버튼으로 클릭하고 **Disk Management(디스크 관리)**를 선택합니다.
 - 1.2. **디스크 초기화** 팝업이 나타나면 **확인**을 클릭합니다. 그렇지 않은 경우 새로 만들기 하드 드라이브를 마우스 오른쪽 버튼으로 클릭하고 **디스크 초기화**를 선택합니다.
 - 1.3. 새로 초기화한 디스크의 할당되지 않은 영역을 마우스 오른쪽 버튼으로 클릭하고 **New Simple Volume(새로운 단순 볼륨)**을 선택합니다.
 - 1.4. 마법사에 따라 볼륨 크기를 설정하고, 드라이브 문자를 할당하고, 파티션을 포맷합니다.
 - 1.5. 마법사를 완료하여 심플 볼륨을 새로 만드세요.
2. AXIS Camera Station Pro에서 새 녹화 스토리지 추가:
 - 2.1. AXIS Camera Station Pro를 엽니다.
 - 2.2. **Storage(스토리지) > Management(관리)**로 이동합니다.
 - 2.3. **Add(추가)...**를 클릭합니다
 - 2.4. 새로 추가한 드라이브를 선택하고 **확인**을 선택합니다.
 - 2.5. **Storage(스토리지) > Selection(선택)**으로 이동합니다.
 - 2.6. 녹화 데이터를 새로 만들 드라이브에 전송할 장치를 선택합니다.
 - 2.7. **저장 위치** 드롭다운 목록에서 새 드라이브를 선택하고 **적용**을 클릭합니다.

스토리지 관리에 대한 자세한 내용은 *AXIS Camera Station Pro - 사용자 설명서*를 참조하십시오.

RAID 볼륨 생성

1. RAID 볼륨에 사용할 디스크가 감지되었는지 확인합니다.
 - 1.1. 장치를 켜고 Axis 로고가 나타날 때까지 즉시 F12를 누릅니다.
 - 1.2. UEFI 부팅 메뉴에서 **Device Configuration(장치 구성)**을 선택하고 Enter를 누릅니다.
 - 1.3. Intel® Rapid Storage Technology 메뉴에서 디스크가 **Non-RAID Physical Disks(비 RAID 물리적 디스크)** 항목에 올바르게 표시되는지 확인합니다.

비고

- 추가 단일 드라이브를 위한 물리적 공간이 있는 장치에서는 RAID 0 및 RAID 1만 사용할 수 있습니다.
2. Intel Rapid Storage Technology 메뉴에서 **Create RAID Volume(RAID 볼륨 생성)**을 선택하고 Enter를 누릅니다.
 3. 볼륨에 대한 이름을 입력합니다.
 4. RAID 레벨을 선택합니다.
 - 4.1. **RAID Level(RAID 레벨)**을 선택하고 Enter를 누릅니다.
 - 4.2. 팝업 대화 상자에서 사용하려는 RAID 레벨을 선택하고 Enter를 누릅니다.
 5. 볼륨에 사용할 디스크를 포함합니다.
 - 5.1. 디스크를 선택하고 Enter를 누릅니다.
 - 5.2. **X**를 선택하여 이 디스크를 볼륨에 포함시킵니다.
 - 5.3. 사용하려는 모든 디스크를 선택할 때까지 반복합니다.
 6. 별도로 지정되지 않은 한 **Stripe Size(스트라이프 크기)** 및 **Capacity(용량)**는 기본값으로 둡니다.

7. **Create Volume(볼륨 생성)**을 선택하고 Enter를 누릅니다.
8. Intel Rapid Storage Technology 메뉴의 **RAID Volumes(RAID 볼륨)** 항목에 새로 생성된 RAID 볼륨이 나타납니다.
9. **Esc**를 누른 다음 **Y**를 눌러 저장하고 UEFI 메뉴를 종료합니다.
10. CTRL + ALT+ DELETE를 눌러 장치를 재시작합니다.

Microsoft Windows®에서 RAID 볼륨 시작

새 볼륨을 구성하려면:

1. **Start menu(시작 메뉴)**를 마우스 오른쪽 버튼으로 클릭하고 **Disk Management(디스크 관리)**를 선택합니다.
2. **'Initialize Disk(디스크 초기화)'** 팝업에서, **GPT**를 선택하고 **OK(확인)**를 클릭합니다.
3. 할당되지 않은 디스크를 마우스 오른쪽 버튼으로 클릭하고 **New Simple Volume(새 단순 볼륨)**을 선택합니다.
 - 설정 도우미의 지침을 따릅니다.
4. 설정 도우미가 완료되면 **Disk Management(디스크 관리)**가 새로운 볼륨을 보여줍니다. 시스템이 새 볼륨을 사용하도록 **Disk Management(디스크 관리)**를 닫습니다.

내장 스위치 관리

내장 스위치 정보

AXIS Camera Station S22 Mk II Appliance Series에는 PoE(Power over Ethernet) 스위치가 통합되어 있습니다. 내장 스위치를 구성하고 관리할 수 있습니다.

스위치의 목적은 스위치에서 관리하는 보안 카메라 및 관련 트래픽(PoE 및 스위치 업링크 포트)이 다른 네트워크와 공유되지 않도록 네트워크의 트래픽을 분리하는 것입니다.

스위치의 전원 관리는 다음 룰을 따릅니다.

- 각 포트는 연결된 전원 장치의 PoE 클래스에 따라 전력을 예약할 수 있습니다. 포트에 수동으로 전원을 할당할 수도 있습니다.
- 제공된 포트에 대한 실제 전력 소비량이 해당 포트에 대해 예약된 전력량을 초과하면 포트가 종료됩니다.
- 모든 포트에 대한 실제 전력 소비량이 전원 공급 장치가 제공할 수 있는 총 전력량을 초과하면 포트가 종료됩니다. 포트 우선 순위에 따라 포트가 종료되며, 포트 번호가 낮을수록 우선 순위가 더 높습니다.

스위치 관리 페이지에 로그인

1. 메뉴 표시줄로 이동
 - 웹 브라우저에서 스위치의 IP 주소를 입력합니다. 기본값: 192.168.10.1
 - AXIS Recorder Toolbox에서 **Switch > Open the switch configuration(스위치 > 스위치 구성 열기)**으로 이동합니다.
2. 해당 사용자 이름 및 패스워드로 로그인합니다.
 - 사용자 이름은 admin입니다
 - 패스워드는 장치 상단에 부착된 스티커에 있거나, 자체 접착 스티커 형태로 상자 내용에 포함되어 있습니다.

메뉴 표시줄에서 **로그아웃**하여 스위치의 관리 지원 페이지를 종료합니다.

실행 구성

실행 구성은 네트워크 장치에서 현재 활성 상태로 실행 중인 설정 집합입니다. 장치의 현재 상태와 작동 방식을 실시간으로 반영합니다. 그러나 기기를 재부팅하면 이러한 변경 사항은 저장되지 않습니다.

이에 비해 시작 구성은 기기의 비휘발성 메모리에 저장되는 설정 집합입니다. 이 구성은 기기를 시작하거나 재시작할 때 로드되어 적용됩니다.

웹 인터페이스에서 설정을 변경한 후 **Save(저장)**를 클릭하면 변경 사항이 실행 중인 구성에 적용됩니다.

시작 구성에 설정을 저장하려면 웹 인터페이스의 오른쪽 상단에 있는 저장 아이콘을 사용하세요.

실행 중인 구성에 저장되지 않은 변경 사항이 있는 경우 아이콘이 노란색으로 깜박입니다.

개요

메뉴 표시줄에서 **Overview (개요)**를 클릭합니다.

일반 정보

카테고리	항목	설명
포트 요약	활성 포트	사용 중인 포트 수입니다.

	PoE를 사용하는 포트	사용 중인 PoE 지원 포트 수입니다.
	잠긴 포트	잠긴 포트의 수입니다.
전원 소비량	현재 PoE 사용량	장치에서 사용하는 PoE 전력(와트) 및 총 전용 PoE 전력 중 소비된 PoE 전력의 백분율입니다.
	전력이 요청되었습니다	장치에 할당된 총 전력(와트) 및 백분율입니다.
포트 상태	액티브	포트가 사용 중입니다.
	비활성화	포트를 사용할 준비가 되었습니다.
	차단됨	포트가 차단되었습니다.

비고

포트를 클릭하면 해당 포트에 대한 자세한 정보를 볼 수 있습니다.

전원 관리

메뉴 표시줄에서 **Power management (전원 관리)**를 클릭합니다.

포트 목록

항목	설명
포트	장치가 연결된 포트 번호입니다.
PoE	PoE 상태입니다. 아이콘을 클릭하여 포트에서 PoE를 켜거나 끌 수 있습니다.
PoE 클래스	연결된 장치의 PoE 클래스입니다.
우선 순위	연결된 장치에 대한 전원 할당의 우선 순위입니다. 기본적으로 우선 순위는 포트 번호입니다.
전력 소비량(W)	포트에 연결된 장치가 소비하는 전력(와트)입니다.
요청된 전력(W)	포트에 연결된 장치에서 요청한 전력(와트)입니다.
할당된 전력(W)	포트에 할당된 전력을 수동으로 조정합니다. 전력 할당 방법으로 Manual(수동) 을 선택한 경우에만 사용할 수 있습니다.

전력 할당

다음과 같은 방법으로 연결된 장치에 PoE 전력이 할당될 수 있습니다.

- **PoE 클래스:** 스위치는 연결된 장치의 PoE 클래스를 기반으로 PoE 전원을 할당합니다.
- **Manual(수동):** 연결된 장치에 할당된 PoE 전력을 수동으로 조정할 수 있습니다.
- **LLDP-MED:** 스위치가 연결된 장치와 통신하고 필요에 따라 PoE 전력을 동적으로 할당합니다.

비고

LLDP-MED 전력 할당 방법은 AXIS OS 9.20 이상이 설치된 카메라에서만 작동합니다.

전력 할당 방법을 변경하려면 다음을 수행합니다.

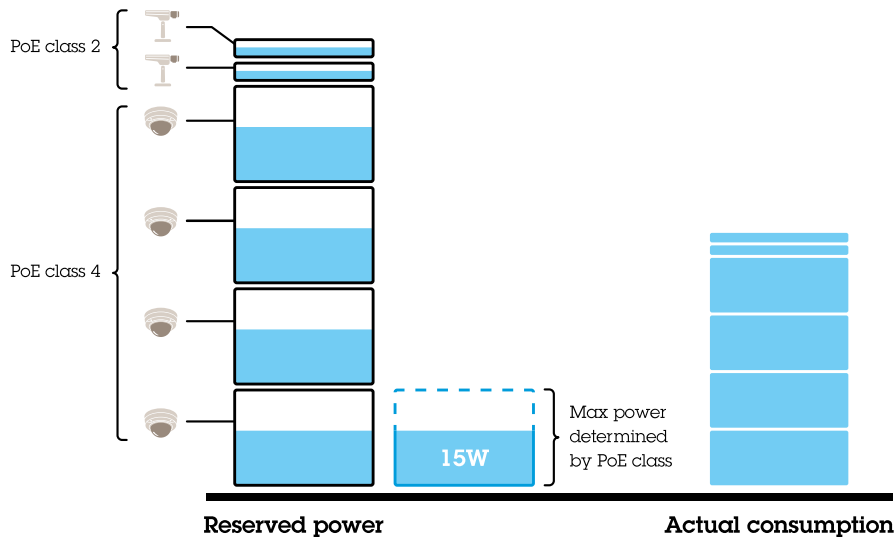
1. 스위치 전원 관리 페이지에서 **Power management(전원 관리)**로 이동합니다.

2. **Allocate power(전력 할당)** 아래에서 **PoE Class(PoE 클래스)**, **Manual(수동)** 또는 **LLDP-MED**를 선택합니다
3. **수동**을 선택한 경우 **전력 할당** 열에서 연결된 장치에 할당된 전원을 변경할 수 있습니다.
4. 연결된 장치의 우선 순위를 변경하려면 해당 장치의 우선 순위를 선택합니다. 다른 장치의 우선 순위는 자동으로 변경됩니다.

예:

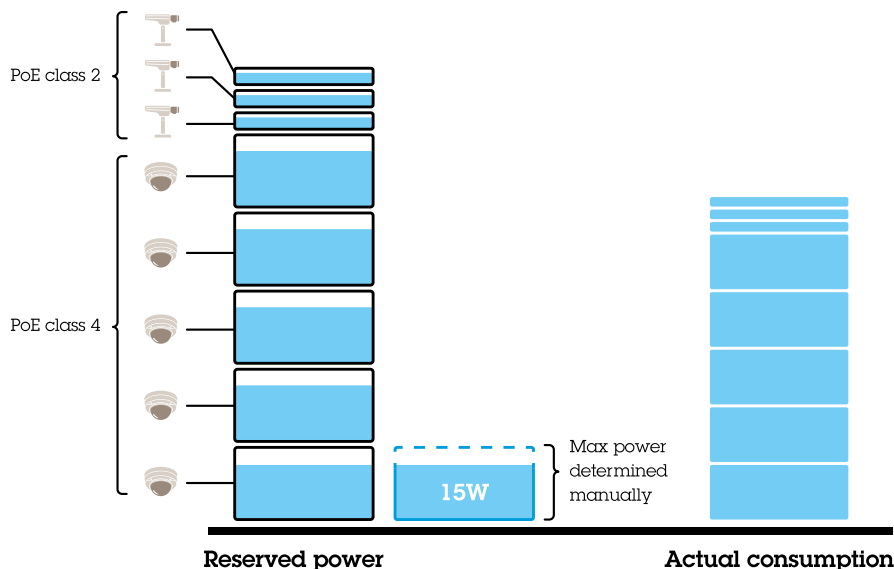
이 예에서 스위치는 총 135W의 전원 가용량을 가지고 있습니다. PoE 클래스 4 장치는 30W 전력을 요청하지만 15W만 소비하고, PoE 클래스 2 장치는 7W 전력을 요청하지만 5W 전력만 소비합니다.

PoE 클래스별로 전력 할당



각 장치에서 요청한 전력은 PoE 클래스별로 결정됩니다. 스위치는 PoE 클래스 4 장치 4개 및 PoE 클래스 2 장치 2개에 전력을 공급할 수 있습니다. 요청된 총 전력은 $(4 \times 30) + (2 \times 7) = 134W$ 입니다. 실제 소비된 전력은 $(4 \times 15) + (2 \times 5) = 70W$ 입니다. 이러한 방식으로 연결된 모든 장치에 전력이 충분히 보장되며 우선 순위는 덜 중요합니다.

수동으로 전력 할당



PoE 클래스 4 장치의 경우 요청된 전력은 수동으로 20W로 조정됩니다. 스위치는 PoE 클래스 4 장치 5개 및 PoE 클래스 2 장치 3개에 전력을 공급할 수 있습니다. 요청된 총 전력은 $(5 \times 20) + (3 \times 7) = 121W$ 입니다. 실제 소비된 전력은 $(5 \times 15) + (3 \times 5) = 90W$ 입니다. 이러한 방식으로 연결된 모든 장치에 전력이 충분히 보장되며 우선 순위는 덜 중요합니다.

PoE 켜기 및 끄기

포트에서 PoE 켜기

1. 메뉴 표시줄에서 **Overview (개요)**를 클릭합니다.
2. PoE 열에서  을 클릭하여 특정 포트에서 PoE를 켭니다.

포트에서 PoE 끄기

1. 메뉴 표시줄에서 **Overview (개요)**를 클릭합니다.
2. PoE 열에서  을 클릭하여 특정 포트에서 PoE를 끕니다.

모든 포트에서 PoE 켜기 및 끄기

1. 메뉴 표시줄에서 **Power management (전원 관리)**을 클릭합니다.
2. 모든 포트에서 PoE를 끄려면 **PoE ports state (PoE 포트 상태)** 드롭다운 메뉴로 이동하여 **Turn off all (모두 끄기)**를 선택합니다.
3. 모든 포트에서 PoE를 켜려면 **PoE ports state (PoE 포트 상태)** 드롭다운 메뉴로 이동하여 **Turn off all (모두 끄기)**를 선택합니다.

네트워크 오버뷰

네트워크 오버뷰는 각 포트의 네트워크 트래픽 상태에 대한 자세한 정보를 제공합니다.

PoE 포트

항목	설명
포트	장치가 연결된 포트 번호입니다.
장치	포트에 연결된 장치의 이름입니다.
IP 주소	포트에 연결된 장치의 IP 주소입니다.
MAC 주소	포트에 연결된 장치의 MAC 주소입니다.
수신	포트의 인바운드 데이터에 대한 초당 현재 데이터 속도(Mbit)입니다.
전송	포트의 아웃바운드 데이터에 대한 초당 현재 데이터 속도(Mbit)입니다.
패킷 전송	스위치가 네트워크로 전송한 데이터 패킷 수입니다.
패킷 수신	스위치가 네트워크로부터 수신한 데이터 패킷 수입니다.
패킷 손실	네트워크 문제로 인해 목적지에 도달하지 못한 데이터 패킷의 수와 백분율입니다.
잠금	포트가 잠겨 있는지 여부를 표시합니다. 아이콘을 클릭하여 포트를 잠그거나 잠금 해제할 수 있습니다.

포트 잠금 및 잠금 해제

해당 MAC 주소에서 들어오는 트래픽만 전달되도록 MAC 주소를 포트에 잠글 수 있습니다. 이렇게 하면 보안이 향상되고 권한이 없는 사용자가 노트북이나 다른 장치를 보안 네트워크에 연결하지 못합니다.

포트에 MAC 주소 잠그기

1. 메뉴 표시줄에서 **Network overview (네트워크 오버뷰)**를 클릭합니다.
2. **Lock(잠금)** 열에서  을 클릭하여 특정 포트를 잠급니다.

포트에서 MAC 주소 잠금 해제

1. 메뉴 표시줄에서 **Network overview (네트워크 오버뷰)**를 클릭합니다.
2. **Lock(잠금)** 열에서  을 클릭하여 특정 포트를 잠금 해제합니다.

모든 포트 잠금 또는 잠금 해제하기

1. 메뉴 표시줄에서 **Network overview (네트워크 오버뷰)**를 클릭합니다.
2. 모든 포트를 잠그려면 **Lock ports (포트 잠금)** 드롭다운 메뉴로 이동하여 **Lock all (모두 잠금)** 을 선택합니다.
3. 모든 포트를 잠금 해제하려면 **Lock ports (포트 잠금)** 드롭다운 메뉴로 이동하여 **Unlock all (모두 잠금 해제)**을 선택합니다.

설정

네트워크 설정 구성

스위치의 IP 주소를 변경할 수 있습니다. 그러나 대부분의 카메라 설치에는 기본 설정을 사용하는 것이 좋습니다. 그 이유는 감시 네트워크가 일반적으로 회사 LAN과 같은 다른 네트워크와 격리되어 있기 때문입니다. 이 경우 감시 네트워크만 사용하여 서버에 설치된 영상 관리 소프트웨어에서 감시 장치를 관리하고 데이터를 수집합니다.

1. 메뉴 표시줄에서 **Settings (설정) > Network settings (네트워크 설정)**로 이동합니다.
2. 연결 유형, IP 주소, 서브넷 마스크, 게이트웨이, 일차 DNS, 이차 DNS 및 호스트 이름을 입력합니다.

비고

공장 출하 시 기본 설정은 주소가 192.168.10.1인 고정 IP 연결 및 주소가 255.255.255.0인 서브넷 마스크입니다.

3. **Save(저장)**를 클릭합니다.

날짜 및 시간 구성

1. 메뉴 표시줄에서 **Settings (설정) > Date and time (날짜 및 시간)**으로 이동합니다.
2. 국가 및 시간대를 선택합니다.
3. 수동으로 시간을 설정하려면 **Manual(수동)**을 선택하고 수동으로 시간을 조정합니다.
4. NTP 서버를 설정하려면 **NTP server(NTP 서버)**를 선택하고 NTP 서버 주소를 입력합니다.

비고

NTP는 스위치가 네트워크에 연결되어 있고 인터넷 액세스로 구성된 경우에만 작동합니다.

5. **Save(저장)**를 클릭합니다.

DHCP 서버 구성

연결된 장치에 IP 주소를 할당하기 위해 내부 DHCP 서버를 사용하도록 스위치를 구성할 수 있습니다. 스위치 업링크 연결을 사용하여 장치가 외부 애플리케이션에 액세스하거나 외부 애플리케이션에서 장치에 액세스할 수 있게 하려면 게이트웨이 및 DNS 주소를 지정해야 합니다.

1. 메뉴 표시줄에서 **Settings (설정) > DHCP 서버**로 이동합니다.
2. **Enable DHCP server(DHCP 서버 활성화)**를 선택합니다.
3. 시작 IP 주소, 끝 IP 주소, 서브넷 마스크, 게이트웨이, 일차 DNS, 이차 DNS, 사용 기간 및 도메인 이름을 입력합니다.
4. **Save(저장)**를 클릭합니다.

SNMP 구성

1. 메뉴 표시줄에서 **Settings (설정) > SNMP**으로 이동합니다.
2. SNMP 연결에 사용되는 서버 이름, 연락처 및 위치를 입력합니다.
3. SNMPV1 또는 SNMPV2c를 사용하려면 **SNMPV1/SNMPV2c**를 선택하고 Read community (읽기 커뮤니티)로 이동합니다.
4. SNMPV3을 사용하려면 **SNMPV3 (MD5)**을 선택하고 사용자 이름 및 패스워드를 입력합니다.

비고

현재 SNMP에 사용되는 MD5 인증만 지원합니다.

5. **Save(저장)**를 클릭합니다.

유지보수

펌웨어 업데이트

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Update firmware (펌웨어 업데이트)**로 이동합니다.
2. 펌웨어 파일을 끌어다 놓거나 **Browse(찾아보기)**를 클릭하고 펌웨어 파일로 이동합니다.
3. **Upload(업로드)**를 클릭합니다.
4. 펌웨어 업데이트가 완료되면 스위치를 재부팅합니다.

스위치를 재부팅합니다

중요 사항

스위치가 재부팅되는 동안 연결된 모든 장치와 PoE를 포함한 스위치의 연결이 일시적으로 끊어집니다.

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Reboot switch (스위치 재부팅)**로 이동합니다.
2. **Reboot(재부팅)** 및 **Yes(예)**를 클릭합니다.
3. 몇 분 후에 스위치가 재부팅되면 사용자 이름 및 패스워드를 입력하여 로그인합니다.

스위치 설정 백업

비고

사용자 이름 및 패스워드가 백업 파일에 포함되어 있습니다.

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Backup and restore (백업 및 복구)**로 이동합니다.
2. **Create a backup file(백업 파일 생성)**을 클릭합니다. 이렇게 하면 .bin 형식의 백업 파일이 생성되어 **다운로드** 폴더에 저장됩니다.

스위치 설정 복원

비고

스위치 설정을 복원하려면 이전에 백업 파일을 생성했어야 합니다.

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Backup and restore (백업 및 복구)**로 이동합니다.
2. 백업 파일을 끌어다 놓거나 **Browse(찾아보기)**를 클릭하고 백업 파일로 이동합니다.
3. **Upload(업로드)**를 클릭합니다.

백업 파일에서 스위치를 복원하는 데 몇 분이 걸릴 수 있습니다. 설정이 복원되면 스위치가 자동으로 재부팅되며 다시 로그인해야 합니다.

인증서 관리

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Manage certificates (인증서 관리)**로 이동합니다.
2.  을 클릭하고 비밀 키 파일로 이동합니다.
3.  을 클릭하고 인증서 파일로 이동합니다.
4.  을 클릭하고 CA 번들 파일로 이동합니다.
5. **Save(저장)**를 클릭합니다.
6. 스위치를 재부팅합니다.

비밀번호 변경

스위치의 기본 패스워드를 사용자가 선택한 패스워드로 변경할 수 있습니다.

중요 사항

기억할 수 있는 패스워드를 선택해야 합니다. 패스워드를 잊어버린 경우 공장 초기화 설정으로 재 설정합니다, on page 33을 참조하여 공장 초기화 패스워드를 복구하세요.

1. 메뉴 표시줄에서 **Maintenance (유지 관리) > Change password (패스워드 변경)**로 이동합니다.
2. 필요에 따라 현재 패스워드와 사용자의 새 패스워드를 입력합니다.
3. **Save(저장)**를 클릭합니다.

웹 설정 구성

1. 메뉴 표시줄에서 **Settings (설정) > Web settings (웹 설정)**로 이동합니다.
2. 포트 번호를 입력합니다.

비고

- 포트 번호를 변경하기로 결정한 경우, 새로운 포트 번호를 꼭 적어두세요. 새로 만든 포트 번호를 잊어버린 경우 공장 초기화 설정으로 재설정합니다, on page 33을 참조하여 공장 초기화 포트 번호를 복구하세요.
- 이 HTTPS는 계속 활성화하는 것을 권장합니다.

공장 초기화 설정으로 재설정합니다

리셋 버튼을 5초간 길게 누르면 스위치가 공장 초기화 설정으로 초기화됩니다.

웹 인터페이스를 통해 스위치를 재설정할 수도 있습니다:

1. 메뉴 표시줄에서 **Maintenance (유지보수) > Reset to factory default settings (공장 초기화 설정으로 리셋)**로 이동합니다.
2. **Reset(재설정)** 및 **Yes(예)**를 클릭합니다.

재설정이 완료되면 스위치가 자동으로 재부팅됩니다.

로그

메뉴 표시줄에서 **Logs (로그)**를 클릭하여 로그 목록을 확인합니다. 알파벳 순서로 정렬하려면 열 제목을 클릭합니다.

항목	설명
시간	로그 이벤트가 발생한 날짜 및 시간입니다.

수준	경고 아이콘으로 표시되는 심각도 수준입니다.
사용자	로그 이벤트를 시작한 사용자입니다.
IP 주소	로그 이벤트를 시작하는 사용자의 IP 주소입니다.
서비스	로그 이벤트와 관련된 서비스입니다. 가능한 값은 데스크톱, 네트워크, 시스템, ntpd, 스토리지, dhcp 등입니다.
이벤트	로그 이벤트에 대한 설명입니다.

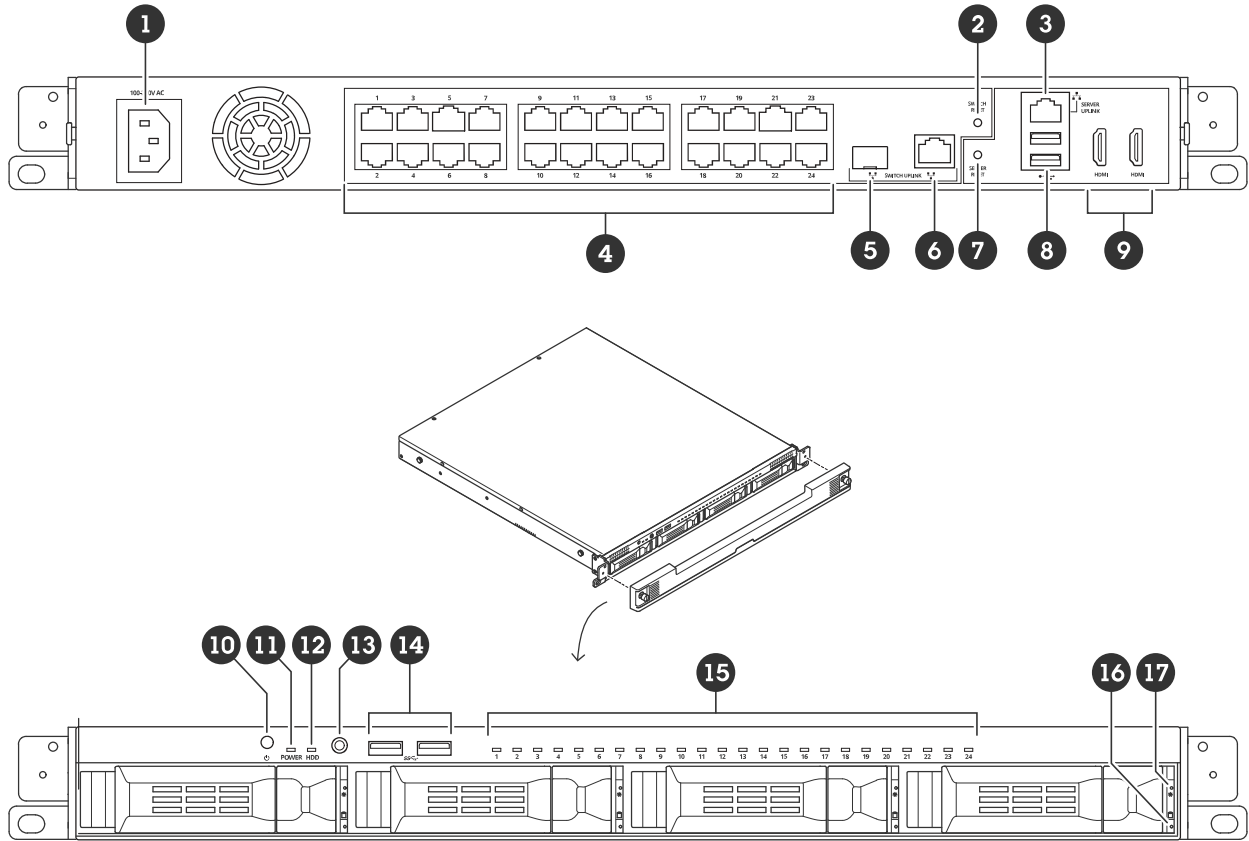
스위치 보고서 생성

로그 페이지에서 **Export (내보내기)**를 클릭하여 로그 페이지의 로그 항목을 포함한 스위치 정보가 포함된 텍스트 파일이 생성됩니다.

사양

제품 오버뷰

전면 및 후면



- 1 전원 커넥터
- 2 스위치 재설정 버튼
- 3 1GbE 이더넷 포트 — 서버 업링크
- 4 1GbE PoE 이더넷 포트
- 5 1GbE 이더넷 포트 — 스위치 업링크(SFP)
- 6 1GbE 이더넷 포트 — 스위치 업링크(RJ45)
- 7 서버 재설정 버튼
- 8 USB 2.0 포트
- 9 HDMI 포트
- 10 전원 버튼
- 11 전원 LED
- 12 하드 드라이브 작동 LED
- 13 범용 오디오 잭
- 14 USB 3.2 포트
- 15 PoE 이더넷 포트 상태 LED
- 16 하드 드라이브 작동 LED
- 17 하드 드라이브 상태 LED

LED 표시

전면 LED

전원 버튼	전원 LED	표시
누르지 않음	꺼짐	PC 및 스위치가 꺼져 있습니다.
	주황색	PC가 켜져 있고 스위치가 꺼져 있습니다.
	주황색으로 깜박임	PC가 켜져 있고 스위치가 부팅 중
	녹색	PC가 켜져 있고 스위치 부팅 완료
누름	최대 0초	스위치와 PC가 모두 꺼져 있는 경우 전원 켜기
	황색으로 깜박일 때까지 (3초)	스위치가 정상 종료 시작
	빨간색으로 깜박일 때까지 (6초)	PC 및 스위치가 자동 종료 시작
	빨간색으로 바뀔 때까지 (9초)	PC가 정상적이지 않은 종료를 시작하고 스위치가 정상적인 종료를 시작합니다.

LED 표시기	색상	표시
하드 드라이브 (HDD)	녹색으로 깜박임	하드 드라이브 활동
	빨간색	하드 드라이브 고장 가능성
PoE 이더넷 포트 상태	녹색	연결 상태
	주황색	구동 장치, 링크 상태 없음
	빨간색	PoE 예산 초과
하드 드라이브 상태	녹색	하드 드라이브 존재
	빨간색	하드 드라이브 고장 가능성

후면 LED

네트워크 속도 및 활동	색상	표시
오른쪽 LED	주황색	10/100Mbit/초
	녹색	1000Mbit/초
왼쪽 LED	녹색	PoE 연결 정상
	빨간색	PoE 예산 초과

문제 해결

서버 재설정

서버 재설정 버튼을 사용하여 서버를 재설정할 수 있습니다. 서버를 재설정하는 데 1시간 넘게 걸립니다.

1. 장치의 전원을 끕니다.
2. 서버 재설정 버튼을 5초 동안 누르고 있습니다. Windows® RE가 시작됩니다.
3. **Troubleshoot(문제 해결)**를 선택합니다.
4. **Reset your PC(PC 재설정)**를 선택합니다.
5. **Keep my files(내 파일 유지)** 또는 **Remove everything(모두 제거)**을 선택합니다. **Keep my files(내 파일 유지)**를 선택하는 경우 관리자 자격 증명을 제공해야 합니다.
6. 화면의 지침을 따릅니다.
7. 서버가 재부팅되고 Windows®를 공장 초기화 설정으로 복원하는 절차가 시작됩니다.



서버를 공장 초기화 설정으로 재설정

시스템 복구 수행

장치에 전체 시스템 장애가 발생한 경우 복구 이미지를 사용하여 Windows® 시스템을 다시 생성해야 합니다. AXIS Network Video Recorder Recovery Kit를 다운로드하려면 Axis 기술 지원에 연락하여 장치의 일련 번호를 제공하십시오.

비고

AXIS Network Video Recorder Recovery Kit는 두 가지 버전으로 제공됩니다.

- **sb11** — 2011년 인증서를 계속 사용하는 장치용.
- **sb23** — 2023년 인증서로 전환한 장치용.

Recovery Kit를 다운로드하기 전에 인증서 상태를 확인하고 해당하는 버전을 선택합니다. 잘못된 버전을 선택하면 설치 후 부팅 가능한 시스템이 생성되지 않으므로 올바른 이미지로 처음부터 다시 시작해야 합니다. 이로 인해 장치가 손상되지는 않습니다.

장치에 2023년 인증서가 이미 설치되어 있어도 2011년 인증서를 수동으로 해지하지 않았다면 sb11 버전을 안전하게 사용할 수 있습니다. 2011년 인증서가 해지되면 sb23만 사용할 수 있습니다.

시스템을 다시 생성하는 방법:

1. AXIS Network Video Recorder Recovery Kit and AXIS Network Video Recorder Recovery: ISO to USB Tool을 다운로드합니다.
2. 컴퓨터에 USB 드라이브를 삽입합니다.
 - 최소 16 GB의 USB 드라이브를 사용하십시오.
 - USB 드라이브가 포맷되고 기존의 모든 데이터가 지워집니다.
3. AXIS Network Video Recorder Recovery: ISO to USB Tool을 실행하고 화면의 지침을 따릅니다. USB 드라이브에 데이터를 쓰는 데 약 10 ~ 15분이 걸립니다. 프로세스가 완료될 때까지 USB 드라이브를 제거하지 마십시오.

4. AXIS Network Video Recorder Recovery: ISO to USB Tool 작업이 완료되면 USB 드라이브를 분리하여 장치에 연결합니다.
5. 장치를 시작합니다.
6. Axis 시작 화면이 표시되면 F12를 누릅니다.
7. **UEFI: USB Drive**를 클릭합니다.
8. USB 드라이브로 이동하여 Enter를 누릅니다. 시스템이 AXIS Network Video Recorder Recovery Kit로 부팅됩니다.
9. **Reinstall Operating System(운영 체제 다시 설치)**을 클릭합니다.
복구를 완료하는 데 약 10 ~ 15분이 걸립니다. 복구 키트 다운로드에 대한 자세한 지침이 있습니다.

AXIS Camera Station Pro 문제 해결

AXIS Camera Station Pro 장애를 처리하는 방법에 대한 자세한 내용은 *AXIS Camera Station Pro 사용자 설명서*를 참조하십시오.

도움이 더 필요하십니까?

유용한 링크

- *AXIS Camera Station Pro* 사용자 설명서
- *AXIS Secure Remote Access* 로그인
- *AXIS Secure Remote Access v2* 로그인
- *AXIS Camera Station*에 대한 바이러스 백신 허용 목록에 포함할 내용

지원 센터 문의

추가 도움이 필요하면 axis.com/support로 이동하십시오.

T10207039_ko

2026-09 (M5.2)

© 2024 – 2026 Axis Communications AB