AXIS D8204-E PoE++ Switch

사용자 설명서

목차

이 설명서 정보 3
약어 3
솔루션 오버뷰 4
시작하기 5
브라우저에서 제품에 액세스 5
제품의 웹페이지 알아보기 5
제품의 내장 도움말 알아보기 6
설정 예 7
액세스 VLAN 설정 7
MAC 주소를 기반으로 IP 주소 예약 8
네트워크 리던던시를 위해 스위치 간에 중복 링크를 생성 8
VAPIX를 사용하여 포트의 PoE 켜기 또는 끄기 9
MACsec 구성 9
정적 CAK 9
동적 CAK 10
1Gbps SFP 모듈 연결 11
시스템 유지 12
제품을 재시작하기 12
공장 초기화 설정으로 재설정합니다 12
장치 소프트웨어 업그레이드 13
대체 소프트웨어 이미지로 되돌리기 13
사양 14
제품 오버뷰 14
문제 해결 15
사이버 보안 16
취약성 관리 16
보안 알림 16
보안 제품 수명 주기 16

이 설명서 정보

비고

이 제품은 네트워크 장비의 작동 및 유지 관리를 담당하는 네트워크 관리자를 위한 것입니다. 일반 스위치 기능, 보안, 인터넷 프로토콜(IP) 및 단순 네트워크 관리 프로토콜(SNMP)에 대한 기본 작업 지식이 있다고 가정합니다.

이 사용자 설명서는 다음 방법에 대한 정보를 제공합니다.

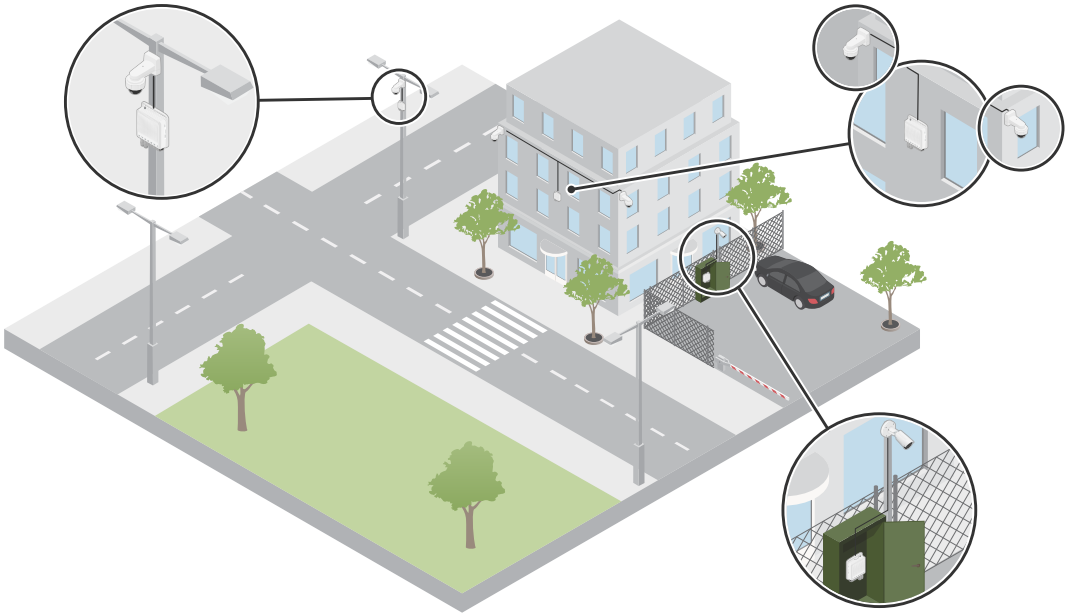
- 제품에 액세스
- 선택한 설정 예 구성
- 제품에 대한 유지 관리 수행

제품 기능 및 설정은 제품의 상황에 맞는 내장 도움말에서 자세히 다룹니다.

약어

Abbreviation(약어)	**설명**
MACsec	미디어 접근 제어 보안
802.1X	네트워크 접근 제어
802.1AE	MACsec과 동일
CAK	연결 연관 키
CKN	연결 키 이름
DHCP	동적 호스트 구성 프로토콜
OpenSSL	오픈 소스 소프트웨어 라이브러리
PoE	PoE(Power over Ethernet)
반경	원격 인증 전화 접속 사용자 서비스
SFP	파이버 인터페이스, 소형 폼 팩터 플러그
SFP+	향상된 소형 폼 팩터 플러그
SNMP	단순 네트워크 관리 프로토콜
SSL	보안 소켓 레이어
TLS	전송 레이어 보안(Transport Layer Security)
VLAN	가상 근거리 통신망

솔루션 오버뷰



Axis 엣지 장치는 현장에 설치되며 이더넷을 통해 Axis 스위치에 연결됩니다. 스위치는 파이버를 통해 연결됩니다.

시작하기

브라우저에서 제품에 액세스

비고

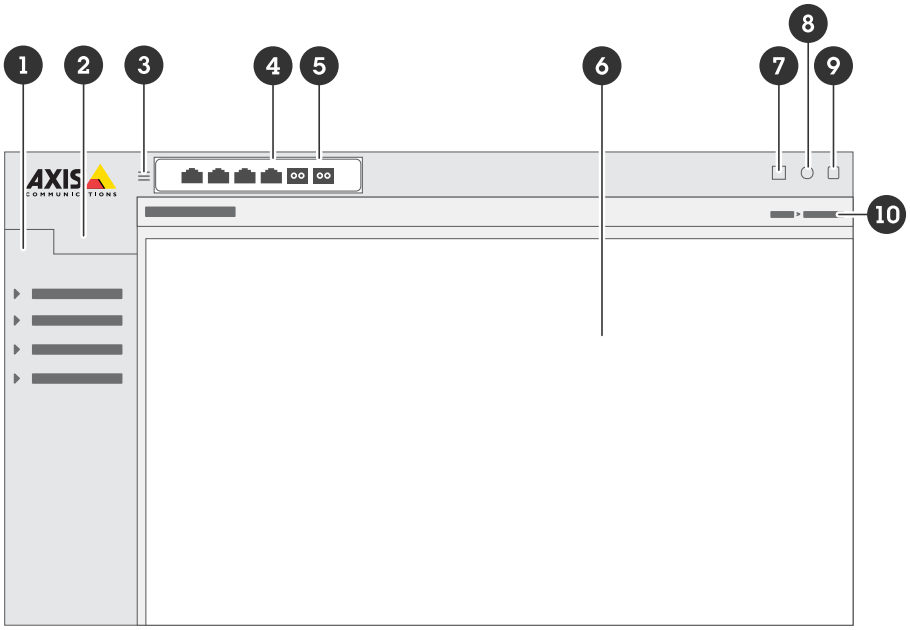
- 설치 가이드에 명시된 대로 장치를 설치 및 연결하고 전원을 켭니다.
- 이 섹션의 단계를 따르면 제품의 웹 페이지에 접속하여 제품을 구성하고 관리할 수 있습니다.

1. 네트워크에서 장치를 검색하기 위해 AXIS IP Utility 또는 AXIS Device Manager를 사용합니다. 장치를 검색하는 방법에 대한 자세한 내용은 *axis.com/support*를 참조하십시오.
2. 제품 라벨에 제공된 사용자 이름 및 패스워드를 입력합니다. 기본 사용자 이름은root입니다.
3. 다음을 위해 설정 마법사에서 다음 단계를 따릅니다.

– 패스워드 변경(보안상의 이유로 권장)
– DHCP를 통해 또는 수동으로 IP 주소 설정
– 날짜 및 시간 정보를 설정
– 시스템 정보 설정

4. **Save(저장)**를 클릭합니다.
5. 새 패스워드를 사용하여 다시 로그인하십시오.

제품의 웹페이지 알아보기



1 기본 기능
2 고급 기능
3 전환 버튼 - 메뉴 숨김 또는 숨김 해제
4 RJ45 포트 상태 표시기
5 SFP 포트 상태 표시기
6 기본/고급 기능을 위한 콘텐츠 영역
7 저장 버튼 - 시작 구성 파일에 설정을 저장합니다.
8 도움말 버튼-상황에 맞는 내장 도움말에 액세스
9 로그아웃 버튼
10 메뉴 경로

제품의 내장 도움말 알아보기

제품에는 상황에 맞는 내장 도움말이 있습니다. 도움말은 제품의 기본 및 고급 기능 및 제품의 설정에 대한 상세 정보를 제공합니다. 각 보기의 도움말 콘텐츠에 액세스하려면

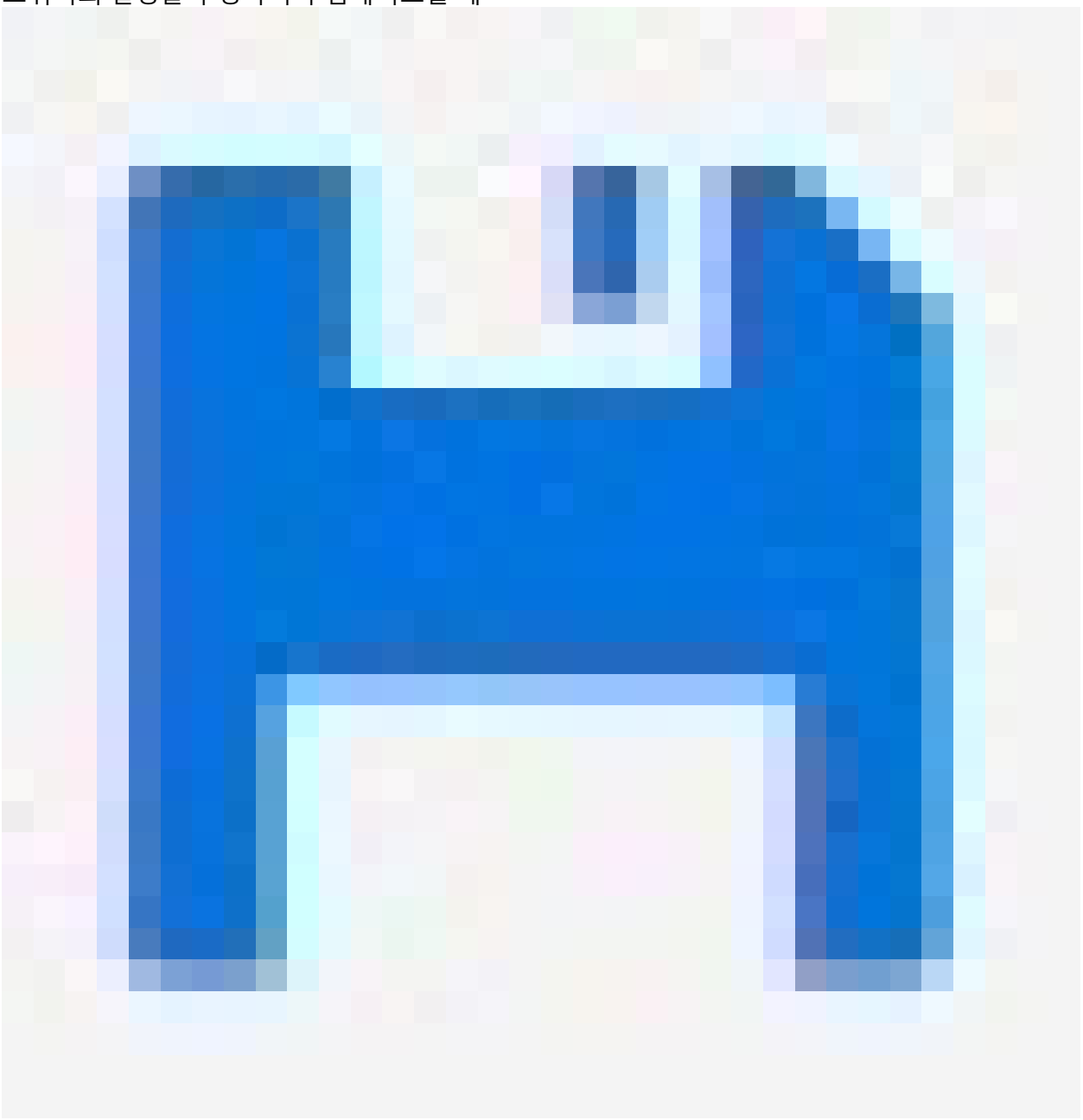


을 클릭합니다. 일부 도움말 콘텐츠에는 내장 용어집에서 자세히 설명하는 클릭 가능한 용어와 머리글자어도 포함되어 있습니다.

설정 예

비고

스위치의 설정을 구성하거나 업데이트할 때



을 클릭하여 시작 구성 파일에 업데이트를 저장하십시오.

시작 구성 파일은 스위치를 재시작하거나 재부팅할 때 유지되지만, 스위치를 공장 초기화 설정으로 재설정한 후에는 유지되지 않습니다.

액세스 VLAN 설정

VLAN은 일반적으로 대규모 네트워크에서 여러 브로드캐스트 도메인을 만드는 데 사용되지만, 네트워크 트래픽을 분리하는 데 사용할 수도 있습니다. 예를 들어 비디오 트래픽은 한 VLAN의 일부가 될 수 있고 다른 네트워크 트래픽은 다른 VLAN의 일부가 될 수 있습니다.

1. **Advanced(고급)** > **VLANs** > **Configuration(구성)**으로 이동합니다.
2. **Global VLAN Configuration(글로벌 VLAN 구성)**의 **Allowed Access VLANs(허용된 액세스 VLAN)** 필드에 생성할 VLAN ID를 입력합니다. 예를 들어, 다음과 같이 입력하면: 1, 10-13, 200, 300, 다음과 같은 VLAN ID가 생성됩니다: 1, 10, 11, 12, 13, 200과 300.

3. **Port VLAN Configuration(포트 VLAN 구성)**에서 특정 포트를 생성된 VLAN ID에 할당하려면 **Port VLAN(포트 VLAN)** 필드에 ID를 입력합니다.
4. **Save(저장)**를 클릭합니다.

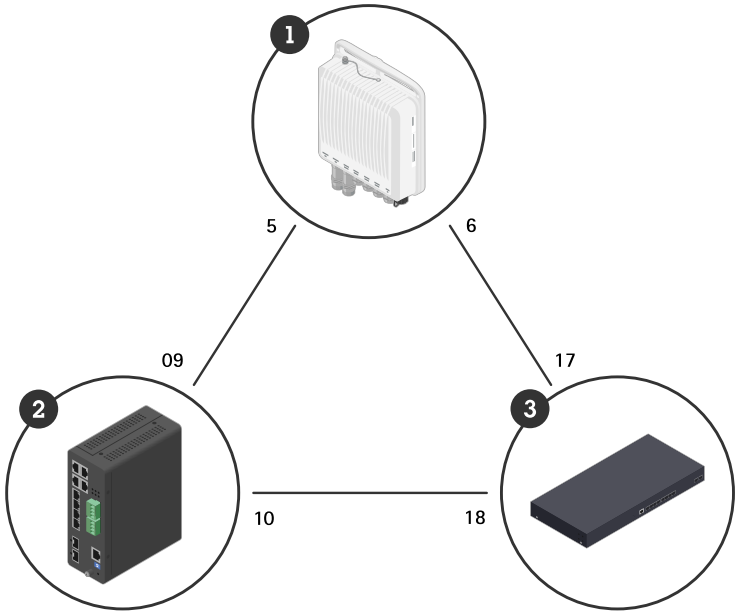
MAC 주소를 기반으로 IP 주소 예약

1. **Advanced(고급)** > **DHCP** > **Server(서버)** > **Configuration(구성)** > **Pool(풀)**로 이동합니다.
2. **새 풀 추가**를 클릭합니다.
3. 풀 이름을 입력하고 **Save(저장)**를 클릭합니다. 이름에는 공백이 허용되지 않습니다.
4. 풀 설정에 액세스하려면 추가된 이름을 클릭하십시오.
5. 드롭다운 메뉴 **유형**에서 **호스트**를 선택합니다.
6. **IP** 주소, **서브넷 마스크**와 **기본 라우터**와 같은 기타 필수 설정을 입력하십시오.
7. 드롭다운 메뉴 **클라이언트 식별자**에서 **MAC**을 선택합니다.
8. **Hardware Address(하드웨어 주소)** 필드에 장치의 MAC 주소를 입력합니다.
9. **Save(저장)**를 클릭합니다.

네트워크 리던던시를 위해 스위치 간에 중복 링크를 생성

네트워크 리던던시가 필요한 경우 스패닝 트리 구성을 사용하여 스위치 간에 중복 링크를 생성할 수 있습니다.

예:
이 예시에서는 AXIS D8204-E(1), AXIS D8208-R(2), AXIS T8516(3) 스위치가 중복 링크로 연결되어 있으며 추가 VLAN은 없습니다. 스위치 간의 업링크 중 하나라도 실패하면 중복 링크가 활성화되고 네트워크 연결을 제공합니다.



Device name(장치 이름):	모델 이름	CIST 포트
스위치 - 01	AXIS D8204-E	5, 6
스위치 - 02	AXIS D8208-R	9, 10
스위치 - 03	AXIS T8516	17, 18

각 스위치의 웹페이지에 중복 링크를 생성하려면:

1. **Advanced(고급)** > **Spanning Tree(스패닝 트리)** > **Configuration(구성)** > **Bridge Settings (브리지 설정)**로 이동합니다.
2. **Basic Settings(기본 설정)**의 **Protocol Version(프로토콜 버전)** 드롭다운 메뉴에서 **RSTP**를 선택하고 **Save(저장)**를 클릭합니다.
3. **Advanced(고급)** > **Spanning Tree(스패닝 트리)** > **Configuration(구성)** > **CIST Port(CIST 포트)**로 이동합니다.
4. **CIST 일반 포트 구성**에서, 다음과 같이 스위치의 포트에 대해 **STP 사용**이 선택되었는지 확인합니다.

– 스위치 – 01: 포트 5 및 6
– 스위치 – 02: 포트 9 및 10
– 스위치 – 03: 포트 17 및 18

5. **Save(저장)**를 클릭합니다.

비고

특정 포트가 기본 통신 링크로 사용되는지 확인하려면, **CIST 일반 포트 구성** 아래에 그 포트를 위한 **경로 비용**을 입력하십시오. 지정하지 않으면 스위치가 자동으로 포트를 선택합니다. 예를 들어 포트 17을 기본 통신 링크로 사용하려면 포트 6에 **Path Cost(경로 비용)** 값 10을 입력하고 포트 18에 **Path Cost(경로 비용)** 값 50을 입력합니다.

VAPIX를 사용하여 포트의 PoE 켜기 또는 끄기

VAPIX에서 다음 명령을 사용하여 특정 포트에 대해 PoE를 켜거나 끌 수 있습니다.

- PoE 켜기:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- PoE 끄기:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

MACsec 구성

MACsec 구성은 MACsec을 지원하는 두 장치 간에 보안 관계를 설정하여 장치 간 통신의 기밀성과 인증을 보장하고 재전송 공격으로부터 보호합니다.

정적 CAK

CAK(Connectivity Association Key)는 장치 간 보안 통신을 보장하는 암호화 키입니다. 128비트 키의 경우 16진수 32자, 256비트 키의 경우 16진수 64자여야 합니다.

CKN(Connectivity Key Name)은 장치 간 보안 MACsec 연결을 설정하는 데 사용할 키를 식별하며, 인증된 장치만 보안 통신에 참여할 수 있도록 합니다. CKN은 16진수 2~64자여야 하며, 문자 길이는 짝수여야 합니다. CKN은 사용할 CAK를 식별하며, MACsec 통신을 설정하려면 링크 양단에서 CAK와 CKN이 모두 일치해야 합니다.

CAK와 CKN은 수동으로 생성하거나 OpenSSL로 생성할 수 있습니다.

OpenSSL로 CAK 및 CKN 생성

1. OpenSSL이 설치된 컴퓨터에서 명령 프롬프트를 엽니다.
2. CAK를 생성하는 방법:
   – `openssl rand -hex 16`을 입력합니다.
   – Enter(입력)을 누릅니다.
3. CKN을 생성하는 방법:
   – `openssl rand -hex 8`을 입력합니다.

– Enter(입력)을 누릅니다.

4. CAK와 CKN을 저장합니다. 나중에 필요합니다.

AXIS OS 장치 구성

1. 장치의 웹 인터페이스에서 **System(시스템)** > **Security(보안)** > **Network access control and encryption(네트워크 액세스 제어 및 암호화)**으로 이동합니다.
2. **Authentication method(인증 방법)**에서 **IEEE 802.1AE MACsec (Static CAK/Pre-Shared Key)**를 선택합니다.
3. **Key agreement connectivity association key name(키 합의 연결 연관 키 이름)**에 CKN을 입력합니다.
4. **Key agreement connectivity association key(키 합의 연결 연관 키)**에 CAK를 입력합니다.
5. **Save(저장)**를 클릭합니다.

스위치 구성

1. 스위치의 웹 인터페이스에서 **Advanced(고급)** > **Security(보안)** > **MACsec** > **Configuration(구성)** > **Policies(정책)**로 이동합니다.
2. **Add Policy(정책 추가)**를 클릭합니다.
3. 정책 이름을 입력합니다.
4. **Enable(활성화)**을 선택하고 생성한 CAK와 CKN을 입력합니다.
5. **Save(저장)**를 클릭합니다.
6. **Advanced(고급)** > **Security(보안)** > **MACsec** > **Configuration(구성)** > **Interfaces(인터페이스)**로 이동합니다.
   – 장치에 연결된 **Interface(인터페이스)**에 대해 드롭다운 목록에서 새 정책을 선택합니다.
   – **Save(저장)**를 클릭합니다.

연결 확인

1. 스위치의 웹 인터페이스에서 **System(시스템)** > **Security(보안)** > **MACsec** > **Status(상태)** > **Status(상태)**로 이동합니다.
2. **State(상태)**에 녹색 상태 표시기가 표시되는지 확인합니다.

동적 CAK

CAK는 IEEE 802.1X와 인증 서버를 사용하는 인증 및 키 관리 프로세스를 통해 생성됩니다. 이를 통해 키를 동적으로 생성하고 관리할 수 있으므로 장기 키를 수동으로 구성할 필요가 없습니다.

비고

- RADIUS 서버가 구성되어 있고 네트워크에서 액세스할 수 있는지 확인합니다.
- RADIUS 서버에 *Axis 장치 ID CA 인증서*를 설치합니다.

연결된 장치 구성

1. 장치의 웹 인터페이스에서 **System(시스템)** > **Security(보안)** > **Network access control and encryption(네트워크 액세스 제어 및 암호화)**으로 이동합니다.
2. **Authentication method(인증 방법)**에서 **IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (Dynamic CAK)**를 선택합니다.
3. **Client certificate(클라이언트 인증서)**에서 RADIUS 서버가 신뢰하는 Axis 장치 ID 인증서를 선택합니다. 인증 서버는 인증서를 사용하여 클라이언트의 ID를 확인합니다.
4. **CA certificates(CA 인증서)**의 경우, 인증서를 선택하지 않으면 장치가 연결된 네트워크에 관계없이 자체 인증을 수행합니다.
5. **EAP Identity(EAP ID)**에 클라이언트 인증서와 연결된 사용자 ID를 입력합니다. EAP ID는 선택한 클라이언트 인증서의 CN(Common Name) 필드와 일치해야 합니다.

6. **EAPOL Version(EAPOL 버전)** 목록에서 네트워크 스위치가 사용하는 버전을 선택합니다.
7. IEEE 802.1X 프로토콜을 사용하려면 **Use IEEE 802.1X(IEEE 802.1X 사용)**를 켭니다.
8. **Save(저장)**를 클릭합니다.

스위치에서 802.1X 구성

1. 스위치의 웹 인터페이스에서 **Advanced(고급)** > **Security(보안)** > **Radius** > **Configuration (구성)**으로 이동합니다.
2. **Add new server(새 서버 추가)**를 클릭하고 호스트 이름과 패스워드를 입력합니다.
3. **Save(저장)**를 클릭합니다.
4. **Advanced(고급)** > **Spanning Tree(스패닝 트리)** > **Configuration(구성)** > **CIST Ports(CIST 포트)**로 이동합니다.
5. 장치에 연결된 포트의 **STP Enabled(STP 사용)** 확인란을 선택 해제합니다.
6. **Save(저장)**를 클릭합니다.
7. **Advanced(고급)** > **Security(보안)** > **802.1X** > **Configuration(구성)**으로 이동합니다.
8. **Mode(모드)** 목록에서 **Enabled(활성화됨)**를 선택합니다.
9. 해당 포트의 **Admin state(관리 상태)**를 **Port-based 802.1X(포트 기반 802.1X)**로 설정합니다.
10. **Save(저장)**를 클릭합니다.

802.1x 연결 확인

1. 장치의 웹 인터페이스에서 **System(시스템)** > **Security(보안)**로 이동합니다.
2. **802.1X Authorized(802.1X 인증됨)**에 녹색 상태 표시기가 표시되는지 확인합니다.

스위치에서 MACsec 구성

1. 스위치의 웹 인터페이스에서 **Advanced(고급)** > **Security(보안)** > **MACsec** > **Configuration (구성)** > **Policies(정책)**로 이동합니다.
2. **Add policy(정책 추가)**를 클릭하고 정책 이름을 입력합니다.
3. **Save(저장)**를 클릭합니다.
4. **Advanced(고급)** > **Security(보안)** > **MACsec** > **Configuration(구성)** > **Interfaces(인터페이스)**로 이동합니다.
5. 장치에 연결된 인터페이스에 대해 목록에서 새로 만든 정책을 선택합니다.
6. **Save(저장)**를 클릭합니다.

MACsec 연결 확인

1. **System(시스템)** > **Security(보안)** > **MACsec** > **Status(상태)** > **Status(상태)**로 이동합니다.
2. **State(상태)**에 녹색 상태 표시기가 표시되는지 확인합니다.

비고

연결 상태가 계속 보류 중이면 장치를 재시작합니다.

1Gbps SFP 모듈 연결

1. **Advanced(고급)** > **Ports(포트)** > **Configuration(구성)**으로 이동합니다.
2. 모듈을 연결한 포트(5 또는 6)에 대해 **Configured(구성됨)**를 **1 Gbps FDX**로 설정합니다.

비고

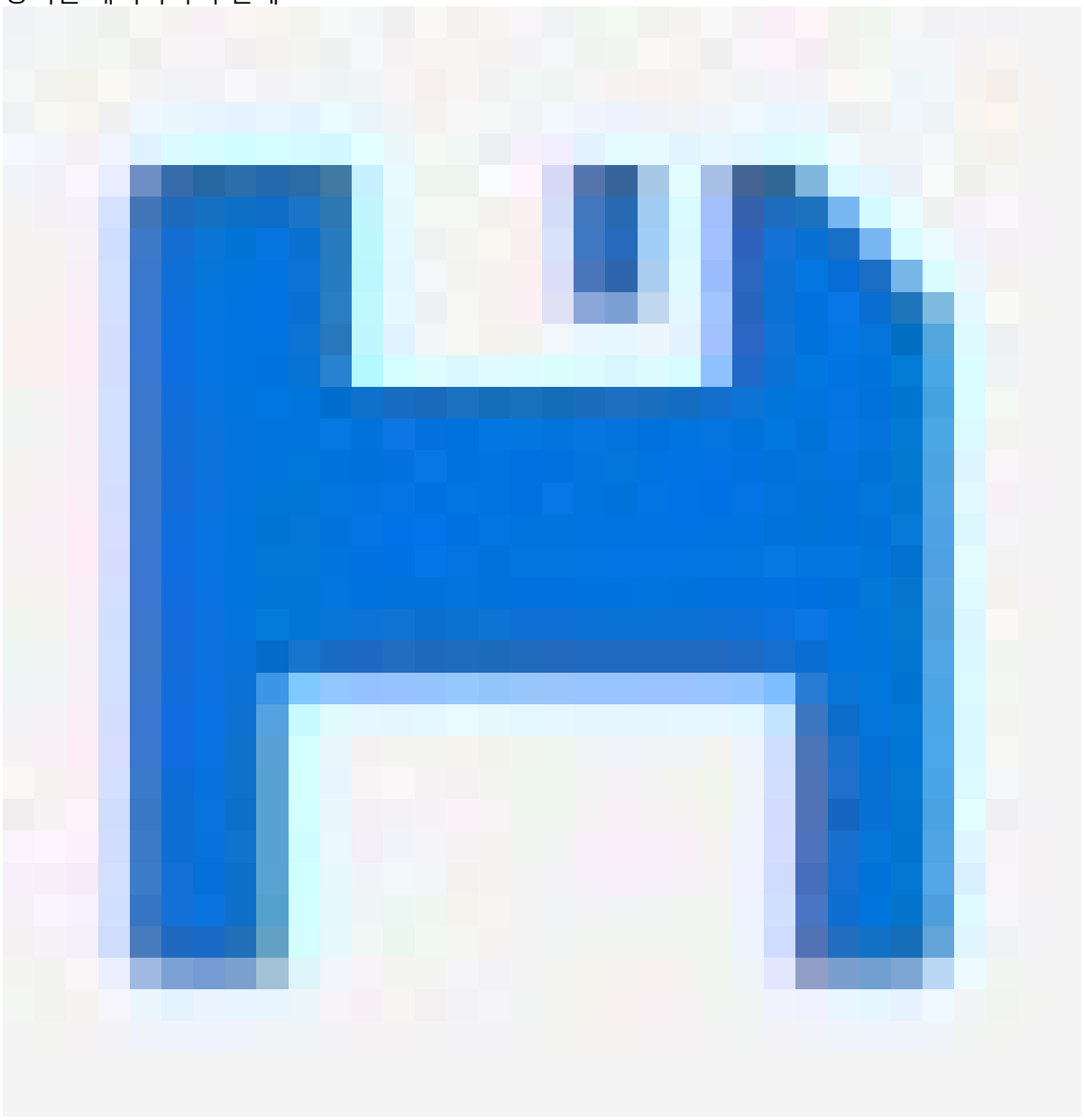
포트를 **Auto(자동)**으로 설정하면 SFP와 SFP+가 모두 작동합니다.

시스템 유지

제품을 재시작하기

비고

- 재시작 중에는 제품을 통한 트래픽이 영향을 받습니다.
- 장치를 재시작하기 전에



을 클릭하여 시작 구성 파일에 설정을 저장하십시오.

1. **Advanced(고급)** > **Maintenance(유지보수)** > **Restart Device(장치 재시작)**로 이동합니다.
2. **Yes(예)**를 클릭합니다. 재시작하면 제품이 정상적으로 부팅됩니다.

공장 초기화 설정으로 재설정합니다

중요 사항

저장된 모든 구성은 공장 출하 시 기본값으로 복원됩니다.

1. **Advanced(고급)** > **Maintenance(유지보수)** > **Factory Defaults(공장 출하 시 기본값)**로 이동합니다.
2. **Yes(예)**를 클릭합니다.

패스워드를 분실한 경우 공장 출하 시 기본값으로 재설정하려면 다음 단계를 따릅니다.

1. 전원을 포함하여 스위치에 연결된 모든 것을 분리합니다.
2. 포트 1과 포트 2를 RJ45 케이블로 연결합니다.
3. 전원 케이블을 연결하고 스위치 전원을 켭니다.
4. 5분 후 RJ45 케이블을 분리합니다. 전원 케이블은 연결된 상태로 두어야 합니다.
5. 장치를 컴퓨터에 연결하면 IP 주소가 기본 IP 주소인 192.168.0.254로 돌아가야 합니다.
6. **Advanced(고급)** > **Maintenance(유지보수)** > **Factory Defaults(공장 출하 시 기본값)**로 이동합니다.
7. **Yes(예)**를 클릭합니다.

장치 소프트웨어 업그레이드

중요 사항

소프트웨어 업그레이드는 최대 10분이 소요됩니다. 이 시간 동안 장치를 재시작하거나 전원을 끄지 마십시오.

비고

업그레이드 중에는 제품을 통한 트래픽이 영향을 받습니다.

1. **Advanced(고급)** > **Maintenance(유지보수)** > **Device Software(장치 소프트웨어)** > **Software Upgrade(소프트웨어 업그레이드)**로 이동합니다.
2. 지정된 위치에서 소프트웨어 파일을 선택하려면 **Select file...(파일 선택...)**을 클릭합니다.
3. **업그레이드**를 클릭합니다.

소프트웨어 업그레이드 후 제품이 정상적으로 재시작됩니다.

대체 소프트웨어 이미지로 되돌리기

제품의 활성(기본) 소프트웨어 이미지 대신 대체(백업) 소프트웨어 이미지를 사용하도록 선택할 수 있습니다. 두 이미지에 대한 정보 표는 **Advanced(고급) > Maintenance(유지보수) > Device Software(장치 소프트웨어) > Software Selection(소프트웨어 선택)**에 나와 있습니다.

비고

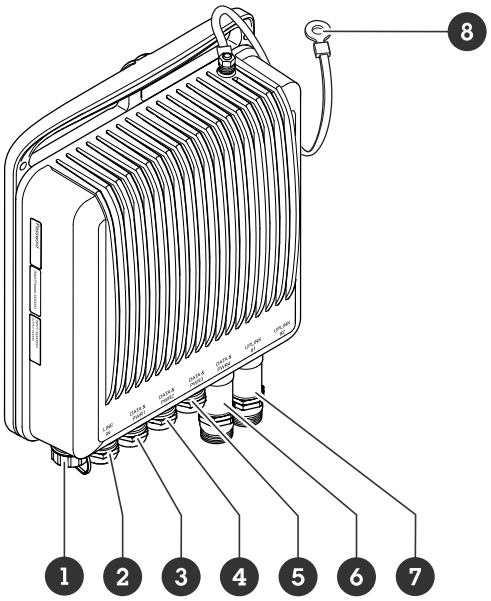
- 활성 이미지가 이미 대체 이미지로 설정된 경우 **활성 이미지** 표가 표시되고 **대체 이미지 활성화** 버튼이 비활성화됩니다.
- 대체 이미지가 이미 활성 이미지로 설정되어 있고 (수동 또는 손상된 기본 이미지로 인해) 새 소프트웨어 이미지가 제품에 업로드되면 새 이미지가 자동으로 활성 이미지로 설정됩니다.
- 이전 소프트웨어 릴리즈의 경우 소프트웨어 버전 및 날짜 정보가 없을 수도 있습니다. 이것은 정상입니다.

대체 이미지를 활성 이미지로 설정하려면:

1. **Advanced(고급) > Maintenance(유지보수) > Device Software(장치 소프트웨어) > Software Selection(소프트웨어 선택)**으로 이동합니다.
2. **Activate Alternate Image(대체 이미지 활성화)**를 클릭합니다.

사양

제품 오버뷰



1 전원 커넥터 포트
2 – 5. RJ45 PoE 포트
6 – 7. SFP 슬롯
8 접지 케이블

문제 해결

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 12* 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).

추가 도움이 필요하면 *axis.com/support* 또는 *Axis 네트워크 스위치 구성 가이드*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.

T10231182_ko

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB