AXIS OS

보안 강화 가이드

AXIS OS Lifecycle 가이드 | AXIS OS 포렌식 가이드 | AXIS OS 취약점 스캐너 가이드 | 보안 권고 | AXIS OS 릴리스 노트 | AXIS OS 기술 자료 | AXIS OS YouTube 재생 목록

서론

AXIS OS 보안 강화 가이드는 AXIS OS를 실행하는 Axis 장치의 보안을 강화하기 위한 실질적인 지침을 제공합니다. 이 가이드에서는 공격 표면을 줄이고, 데이터를 보호하며, 장치 수명 주기 전반에 걸쳐 안정적인 운영을 보장하는 데 도움이 되는 권장 구성 설정, 기능 및 운영 방식을 설명합니다. 이 가이드는 업계 모범 사례에 맞춰 Axis 제품을 안전하고 복원력이 높은 방식으로 배포하고 유지 관리하려는 시스템 관리자, 통합업체 및 보안 전문가를 대상으로 합니다.

웹 인터페이스 구성
이 가이드는 Axis 장치의 웹 인터페이스 내에서 장치 설정을 구성하는 방법을 설명합니다. 구성 경로는 장치에 설치된 AXIS OS 버전에 따라 달라집니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Security > IEEE 802.1X(설정 > 시스템 옵션 > 보안 > IEEE 802.1X)
7.10 미만	Settings > System > Security(설정 > 시스템 > 보안)
≥ 10.9	System > Security(시스템 > 보안)

영역

이 가이드는 AXIS OS(LTS 또는 액티브 트랙)를 실행하는 모든 AXIS OS 기반 제품과 장치 소프트웨어 4.xx 및 5.xx를 실행하는 레거시 제품에 적용됩니다.

AXIS OS 기반 제품은 전문 보안 또는 비즈니스 인텔리전스 시스템에서 사용하도록 설계되었으며, 영상 관리 시스템(VMS) 및 장치 관리 애플리케이션과 같은 다른 제품과 통합되도록 고안되었습니다.

이 제품은 기술 역량을 갖춘 개인이 비전문 환경에서 사용할 수는 있지만, 일반 소비자의 가정용으로 설계되거나 의도된 제품은 아닙니다.

이 제품은 기본 보안 설정(secure-by-default) 접근 방식을 따르지만, 더 높은 수준의 보안을 달성하려면 이 보안 강화 가이드를 따르는 것이 중요합니다. 선택된 통합 시스템에 대해서는 보안 시스템 설계 예시 가이드가 제공되며, *help.axis.com*에서 확인할 수 있습니다.

CIS 보호 수준

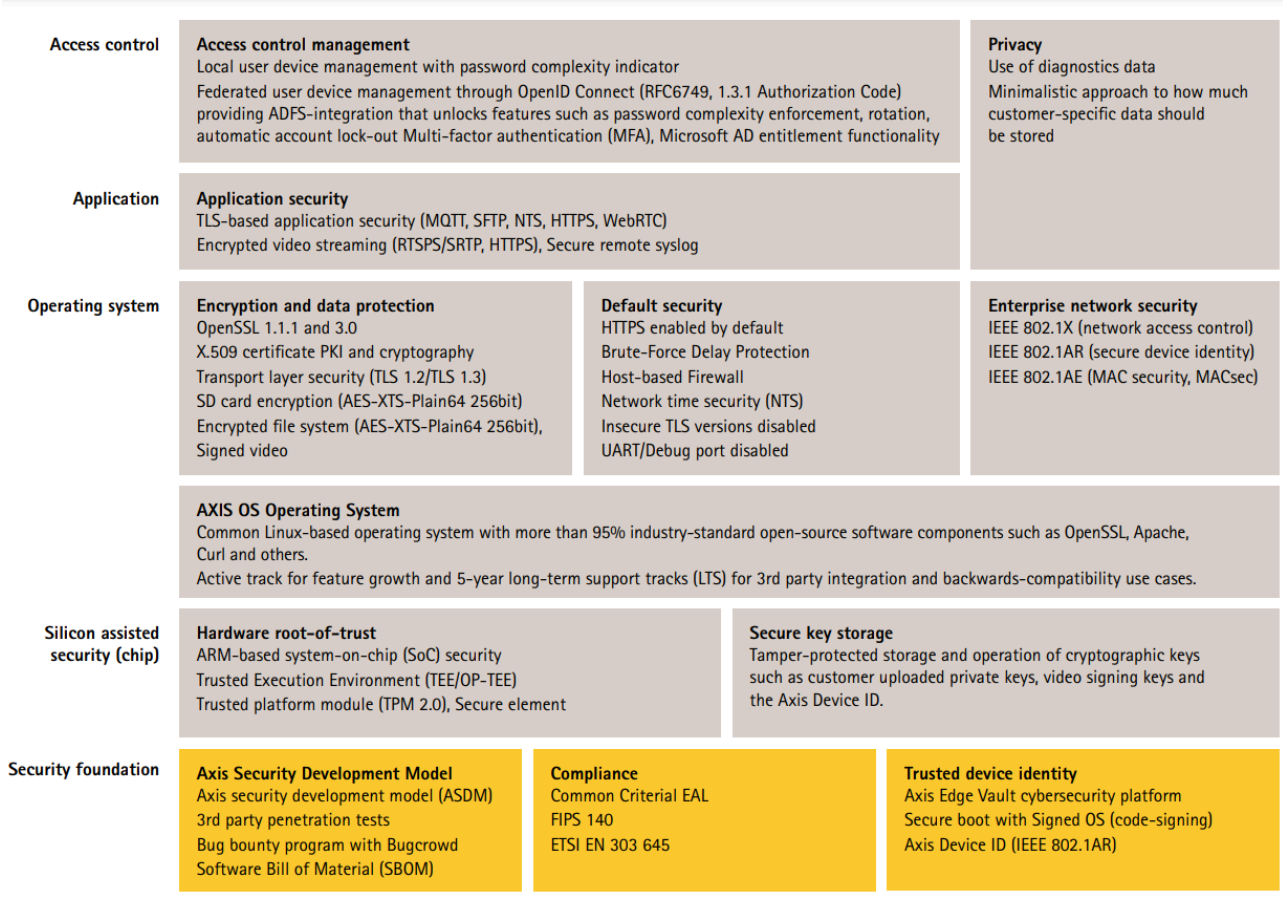
Axis는 사이버 보안 프레임워크 권장 사항을 구성하기 위해 Center for Internet Safety(CIS) Controls Version 8에 설명된 방법을 따릅니다. 이전에는 SANS Top 20 Critical Security Controls로 알려진 CIS Controls는 조직에서 가장 일반적인 사이버 보안 위험 범주에 초점을 맞춘 18개의 Critical Security Controls(CSC)를 제공합니다.

이 가이드에서는 각 강화 주제에 대한 CSC 번호(**CSC #**)를 추가하여 Critical Security Controls를 설명합니다. cisecurity.org의 *18 CIS Critical Security Controls*에서 CSC 범주에 대한 세부 정보를 참고하십시오.

기본 보호

Axis 장치에는 기본 보호 설정이 있습니다. 구성할 필요가 없는 몇 가지 보안 제어 기능이 있습니다. 이러한 제어 기능은 기본 수준의 장치 보호 기능을 제공하며, 더욱 광범위한 보안 강화를 위한 기반이 됩니다.

AXIS OS Security Architecture 다이어그램은 다양한 계층에 걸친 AXIS OS 사이버 보안 기능을 간략하게 보여줍니다. 보안 기반, silicon-assisted security, AXIS OS 운영 체제, 애플리케이션 및 접근 제어 계층에 대한 포괄적인 개요를 제공합니다.



더욱 향상된 시각적 경험을 위해 이미지를 마우스 오른쪽 버튼으로 클릭하여 새 탭에서 엽니다.

인증

기본으로 비활성화

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

Axis 장치는 관리자 패스워드를 설정할 때까지 작동하지 않습니다.

관리자 패스워드를 설정한 후에는 유효한 사용자 이름과 패스워드 자격 증명을 인증해야만 관리자 기능 및/또는 영상 스트림에 액세스할 수 있습니다. 익명 보기 및 상시 멀티캐스트 모드와 같이 인증되지 않은 접근을 허용하는 기능은 사용하지 않는 편이 좋습니다.

장치 액세스를 구성하는 방법에 대해서는 AXIS OS 기술 자료(Knowledge base)에서 *장치 액세스*를 참조하십시오.

다이제스트 인증

CSC #3: 데이터 보호

장치에 액세스하는 클라이언트는 패스워드를 사용하여 인증되며 이 패스워드는 네트워크를 통해 전송될 때 암호화됩니다. 여기에 설명된 대로 HTTPS를 활성화하는 것이 좋습니다. 이것이 불가능한 경

우, Basic 인증 또는 Basic과 Digest 인증을 모두 사용하는 대신 Digest 인증만 사용하는 것을 권장합니다. 이렇게 하면 네트워크 스니퍼가 패스워드를 알아낼 위험이 줄어듭니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > Network > Network HTTP Authentication policy(설정 > 시스템 옵션 > 고급 > 일반 구성 > 네트워크 > 네트워크 HTTP 인증 정책)
7.10 미만	Settings > System > Plain config > Network > Network HTTP Authentication policy(설정 > 시스템 > 일반 구성 > 네트워크 > 네트워크 HTTP 인증 정책)
≥ 10.9	System > Plain config > Network > Network HTTP Authentication policy(시스템 > 일반 구성 > 네트워크 > 네트워크 HTTP 인증 정책)

ONVIF 재생 공격 보호

CSC #3: 데이터 보호

재생 공격 보호는 Axis 장치에서 기본으로 활성화되는 표준 보안 기능입니다. 이는 UsernameToken, 유효한 타임스탬프, nonce 및 패스워드 다이제스트를 포함하는 추가 보안 헤더를 추가하여 ONVIF 기반 사용자 인증을 충분히 보호하는 데 목적이 있습니다. 패스워드 다이제스트는 시스템에 이미 저장된 패스워드, nonce 및 타임스탬프에서 계산됩니다. 패스워드 다이제스트의 목적은 사용자를 검증하고 리플레이 공격을 방지하는 것이며, 이는 다이제스트가 캐시되는 이유입니다. 이 설정은 계속 활성화하는 것을 권장합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > System > Enable Replay Attack Protection(설정 > 시스템 옵션 > 고급 > 일반 구성 > 시스템 > 재생 공격 보호 활성화)
7.10 미만	Settings > System > Plain config > WebService > Enable Replay Attack Protection(설정 > 시스템 > 일반 구성 > WebService > 재생 공격 보호 활성화)
≥ 10.9	System > Plain config > WebService > Enable Replay Attack Protection(시스템 > 일반 구성 > WebService > 재생 공격 보호 활성화)

무차별 대입 공격 방지

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #13: 네트워크 모니터링 및 방어

Axis 장치에는 패스워드 추측 등 네트워크에서 발생하는 무차별 대입 공격을 식별 및 차단하는 방지 메커니즘이 있습니다. AXIS OS 7.30 이상에서는 무차별 대입 지연 보호라는 기능을 사용할 수 있습니다.

무차별 대입 지연 보호는 AXIS OS 11.5부터 기본적으로 활성화됩니다. 자세한 구성 예제 및 권장 사항은 AXIS OS 기술 자료에서 *무차별 대입 지연 보호*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	Settings > System > Plain config > System > PreventDosAttack(설정 > 시스템 > 일반 구성 > 시스템 > PreventDosAttack)
≥ 10.9	System > Security > Prevent brute-force attacks(시스템 > 보안 > 무차별 대입 공격 방지)

감사 로그

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #8: 감사 로그 관리

감사 로그는 사고 대응과 같은 사이버 보안 관련 목적에 사용되며, 관련 이벤트와 작업에 대한 장기 모니터링 체계를 구축하는 데에도 도움이 됩니다. Axis 장치가 로그를 중앙 로깅 환경으로 전송할 수 있도록 원격 syslog 서버 또는 기타 네트워크 모니터링 애플리케이션을 사용하는 것이 좋습니다. 이렇게 하면 로그 메시지의 저장 및 보존 시간이 간소화됩니다.

자세한 내용은 AXIS OS 기술 자료(Knowledge base)의 *Audit Log(감사 로그)*를 참조하십시오.

AXIS OS 버전	**웹 인터페이스 구성 경로**
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 12.5	System > Logs(시스템 > 로그)

엣지 스토리지

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

CSC #3: 데이터 보호

AXIS OS 12.0부터 마운트된 네트워크 공유에 대해 noexec 마운트 옵션이 기본 옵션으로 추가되었습니다. 이렇게 하면 마운트된 네트워크 공유에서 바이너리를 직접 실행할 수 없게 됩니다. SD 카드는 이미 AXIS OS의 이전 버전에서 이 옵션이 추가되었습니다.

또한 AXIS OS 10.10 이상 버전이 설치된 Axis 장치는 에지 녹화물의 암호화된 내보내기를 지원합니다. 이 기능은 권한이 없는 사용자가 내보낸 영상 자료를 재생할 수 없도록 방지하므로, 사용을 권장합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 10.9	녹화물

네트워크 보안

네트워크 프로토콜

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

아래에 나열된 대로 Axis 장치에서는 최소한의 네트워크 프로토콜 및 서비스만 기본적으로 활성화되어 있습니다.

프로토콜	포트	전송	설명
HTTP	80	TCP	웹 인터페이스 액세스, VAPIX 및 ONVIF API 인터페이스와 같은 일반 HTTP 트래픽 또는 엣지 투 엣지 통신.*
HTTPS	443	TCP	웹 인터페이스 액세스, VAPIX 및 ONVIF API 인터페이스와 같은 일반 HTTPS 트래픽 또는 엣지 투 엣지 통신.*
RTSP	554	TCP	Axis 장치에서 비디오/오디오 스트리밍을 위해 사용.
RTP	임시 포트 범위**	UDP	Axis 장치에서 비디오/오디오 스트리밍을 위해 사용.
UPnP	49152	TCP	타사 애플리케이션에서 UPnP 검색 프로토콜을 통해 Axis 장치를 검색하는 데 사용됨. **참고:** AXIS OS 12부터 기본적으로 비활성화되어 있습니다.0.
Bonjour	5353	UDP	타사 애플리케이션에서 mDNS 검색 프로토콜(Bonjour)을 통해 Axis 장치를 검색하는 데 사용됩니다.
SSDP	1900	UDP	타사 애플리케이션에서 SSDP(UPnP)를 통해 Axis 장치를 검색하는 데 사용됩니다. **참고:** AXIS OS 12부터 기본적으로 비활성화되어 있습니다.0.
WS-Discovery***	3702	UDP	타사 애플리케이션에서 WS-Discovery 프로토콜(ONVIF)을 통해 Axis 장치를 검색하는 데 사용됩니다.

* 에지 투 에지에 대한 자세한 내용은 백서를 참조하십시오. *에지 투 에지 기술*.

** RFC 6056에 따라 사전 정의된 포트 번호 범위 안에서 자동 할당됩니다. 자세한 내용은 Wikipedia 문서 *Ephemeral port(임시 포트)*를 참조하십시오.

*** WebService Discovery (WS-Discovery) 프로토콜은 AXIS OS 12.1 이상에서 기본적으로 비활성화되어 있습니다.

가능한 경우 사용하지 않는 네트워크 프로토콜 및 서비스는 비활성화하는 것이 좋습니다. 기본적으로 사용되거나 구성에 따라 활성화할 수 있는 전체 서비스 목록은 AXIS OS 기술 자료(Knowledge base)의 *Commonly used network ports(일반적으로 사용되는 네트워크 포트)*를 참조하십시오.

예를 들어 네트워크 카메라와 같은 Axis 영상 감시 제품에서는 오디오 입력/출력 및 마이크 기능을 수동으로 활성화해야 하는 반면, Axis 인터콤과 네트워크 스피커에서는 오디오 입력/출력 및 마이크 기능이 핵심 기능이므로 기본적으로 활성화되어 있습니다.

HTTPS 활성화

CSC #3: 데이터 보호

AXIS OS 7.20부터는 자체 서명 인증서로 장치 패스워드를 안전하게 설정할 수 있는 HTTPS가 기본으로 활성화되었습니다. AXIS OS 10.10 이상의 버전에서는 자체 서명 인증서가 IEEE 802.1AR 보안 장치 ID 인증서로 대체되었습니다.

AXIS OS에는 공장 출하 시 기본 설정 상태의 사이버 보안 기본 수준을 향상시키기 위해 가장 일반적인 보안 관련 HTTP(S) 헤더가 기본적으로 활성화되어 있습니다. AXIS OS 9.80 이상의 버전에서는 사용자 지정 HTTP 헤더 VAPIX API를 사용하여 추가 HTTP(S) 헤더를 구성할 수 있습니다.

HTTP 헤더 VAPIX API에 대한 자세한 내용은 *VAPIX Library*를 참고하십시오.

기본 HTTP(S) 헤더에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *기본 HTTP(S) 헤더*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Security > HTTPS(설정 > 시스템 옵션 > 보안 > HTTPS)
7.10 미만	Settings > System > Security > HTTP and HTTPS(설정 > 시스템 > 보안 > HTTP 또는 HTTPS)
≥ 10.9	System > Network > HTTP and HTTPS(시스템 > 네트워크 > HTTP 또는 HTTPS)

IEEE 802.1X 네트워크 액세스 컨트롤

CSC #6: 접근 제어 관리
CSC #13: 네트워크 모니터링 및 방어

Axis 장치는 EAP-TLS 방식을 통해 IEEE 802.1X 포트 기반의 네트워크 접근 제어를 지원합니다. 최적의 보호를 위해, Axis 장치를 인증할 때 신뢰도 높은 CA(인증 기관)에서 서명한 클라이언트 인증서를 사용하는 것이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Security > IEEE 802.1X(설정 > 시스템 옵션 > 보안 > IEEE 802.1X)
7.10 미만	Settings > System > Security > IEEE 802.1X(설정 > 시스템 > 보안 > IEEE 802.1X)
≥ 10.9	System > Security > IEEE 802.1X(시스템 > 보안 > IEEE 802.1X)

AXIS OS 12.6에서는 S3008 및 S3008 MK II 레코더에 802.1x 인증 기능을 추가했습니다. AXIS 장치 ID는 있지만 MACsec을 지원하지 않는 장치를 연결하는 경우, **System(시스템) > Network ports(네트**

워크 포트)로 이동하여 해당 포트의 **Security(보안)**에서 "Authentication required(인증 필요)"를 선택하십시오. 이렇게 하면 AXIS 장치 ID를 가진 장치만 연결이 허용됩니다.

IEEE 802.1AE MACsec

CSC #3: 데이터 보호
CSC #6: 접근 제어 관리

Axis 장치는 네트워크 레이어 2의 지점 간 이더넷 링크를 암호화 방식으로 보호하여 두 호스트 간의 데이터 전송의 기밀성과 무결성을 보장하는 잘 정의된 네트워크 프로토콜인 802.1AE MACsec을 지원합니다. MACsec은 네트워크 스택의 하위 레이어 2에서 작동하므로 비슷한 기능을 제공하는 것(HTTPS, TLS) 뿐만 아니라 기본 암호화 기능(ARP, NTP, DHCP, LLDP, CDP...)을 제공하지 않는 네트워크 프로토콜과 이를 제공하는 네트워크 프로토콜에 추가 보안 레이어를 추가합니다.

IEEE 802.1AE MACsec 표준은 수동으로 구성 가능한 PSK(사전 공유 키)/정적 CAK 모드와 IEEE 802.1X EAP-TLS 세션을 사용하는 자동 마스터 세션/동적 CAK 모드의 두 가지 작동 모드를 설명합니다. Axis 장치는 두 가지 모드를 모두 지원합니다.

AXIS OS 12.6에서는 S3008 및 S3008 MK II 레코더에 802.1AE MACsec 지원을 추가했습니다. AXIS 장치 ID와 MACsec을 지원하는 장치를 연결하는 경우, **System(시스템) > Network ports(네트워크 포트)**로 이동하여 해당 포트의 **Security(보안)**에서 "MACsec secured required(보안 적용 MACsec 필요)"를 선택하십시오. 이렇게 하면 802.1x 인증과 MACsec 암호화가 모두 적용됩니다.

802.1AE MACsec 및 AXIS OS 장치에서 이를 구성하는 방법을 알아보려면 AXIS OS 기술 자료의 *IEEE 802.1AE*를 참고하십시오.

IEEE 802.1AR 보안 장치 ID

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #13: 네트워크 모니터링 및 방어

Axis Edge Vault가 포함된 Axis 장치는 네트워크 표준 IEEE 802.1AR을 지원합니다. 이를 통해 생산 중에 장치에 설치된 고유한 인증서인 Axis 장치 ID를 통해 Axis 장치를 네트워크에 자동으로 안전하게 온보딩할 수 있습니다. *Aruba 네트워크에 Axis 장치를 안전하게 통합*에서 보안 장치 온보딩의 예를 살펴보십시오.

*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오. Axis 장치의 장치 ID를 검증하는 데 사용되는 Axis 장치 ID 인증서 체인을 다운로드하려면 axis.com의 *공개 키 인프라 저장소*를 참고하십시오.

UART/디버그 인터페이스

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

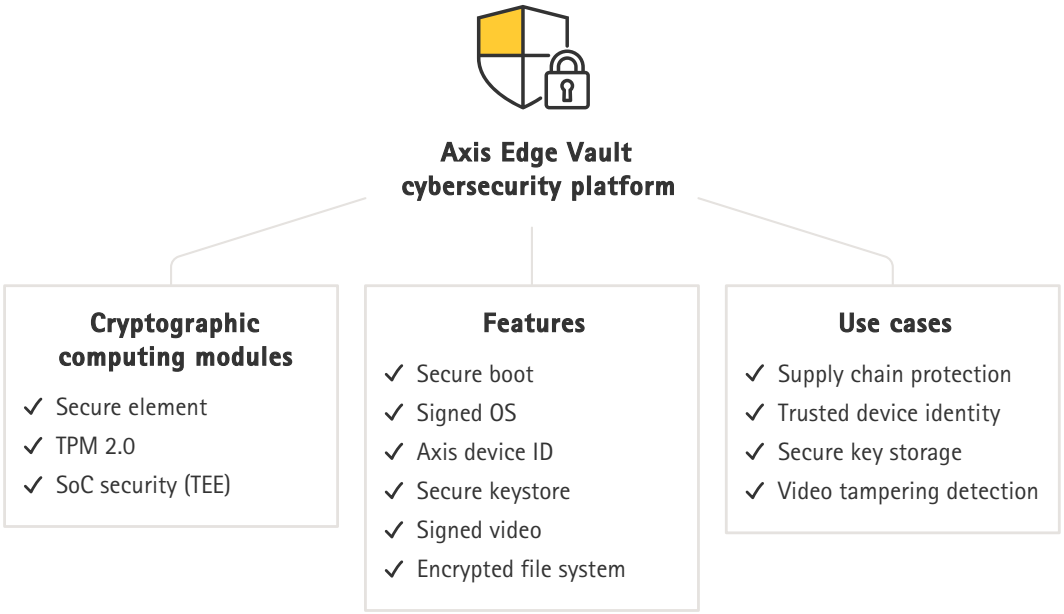
모든 Axis 장치에는 '디버그 포트' 또는 '시리얼 콘솔'이라고도 하는 물리적 UART(Universal Asynchronous Receiver Transmitter) 인터페이스가 함께 제공됩니다. 인터페이스 자체는 Axis 장치를 광범위하게 분해해야만 물리적으로 접근할 수 있습니다. UART/디버그 인터페이스는 Axis 내부 R&D 엔지니어링 프로젝트 중에 제품 개발 및 디버깅 목적으로만 사용됩니다.

UART/디버그 인터페이스는 AXIS OS 10.10 및 이전 버전이 설치된 Axis 장치에서 기본적으로 활성화되어 있지만, 인증된 액세스가 필요하며 인증되지 않은 상태에서는 민감한 정보가 노출되지 않습니다. AXIS OS 10.11부터 UART/디버그 인터페이스가 기본으로 비활성화됩니다. 인터페이스 활성화의 유일한 방법은 Axis에서 제공하는 장치 고유의 사용자 지정 인증서를 통해 잠금을 해제하는 것입니다.

Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반의 사이버 보안 플랫폼을 제공합니다. 이 플랫폼은 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반에 의존하며, 에지 장치 보안에 대한 전문 지식이 결합되어 있습니다. Axis Edge Vault는 Secure boot 및 Signed OS로 구축된 강력한 신뢰점(root of trust)을 기반으로 합니다. 이러한 기능들은 모든 보안 운영이 의존하는 신뢰 체인을 위해, 암호화적으로 검증된 소프트웨어의 끊김 없는 연결 고리를 제공합니다.

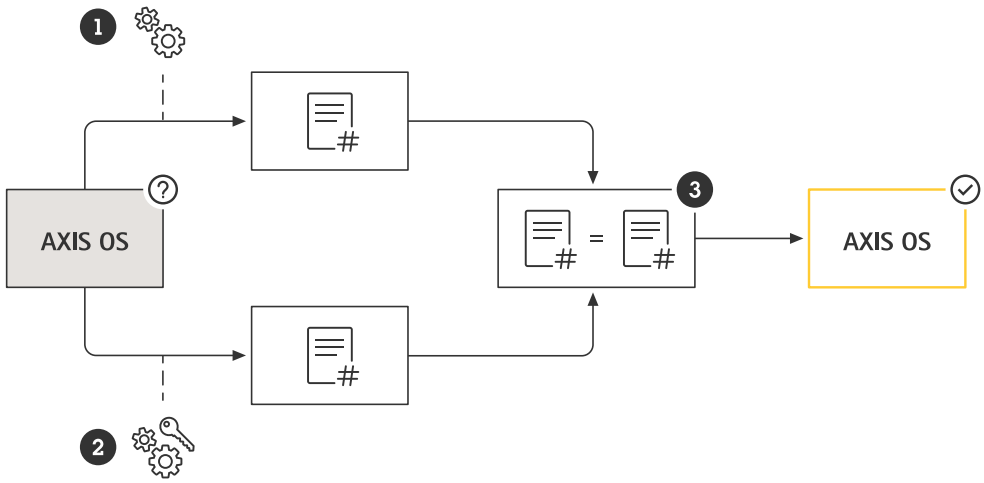
Axis Edge Vault가 탑재된 장치는 도청 및 민감한 정보의 악의적인 추출을 방지하여 사이버 보안 위험 노출을 최소화합니다. 또한 Axis Edge Vault는 Axis 장치가 네트워크상에서 신뢰할 수 있고 안정적인 장치임을 보장합니다.



Signed OS

CSC #2: 소프트웨어 자산의 인벤토리 및 제어

AXIS OS는 버전 9.20.1부터 서명됩니다. 버전을 업그레이드할 때 장치는 암호화 서명 검증을 통해 업데이트 파일의 무결성을 확인하며, 변조된 파일은 거부합니다. 이를 통해 공격자가 사용자를 속여 손상된 파일을 설치하게 하는 것을 방지합니다.



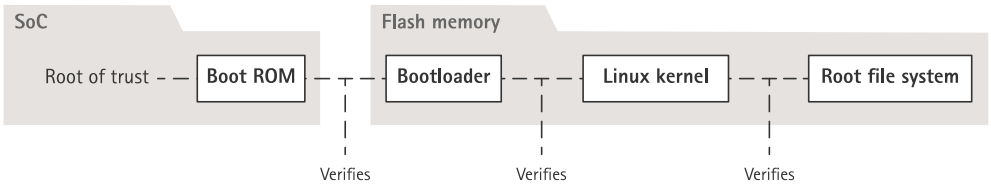
1) 장치는 AXIS OS의 해시 값을 계산합니다. 2) 장치는 공개 키를 사용하여 서명을 복호화하여 해시 값을 얻습니다. 3) 결과가 일치하면 OS 서명이 검증됩니다.

*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오.

Secure Boot

CSC #2: 소프트웨어 자산의 인벤토리 및 제어

대다수 Axis 장치에는 해당 장치의 무결성을 지키기 위한 보안 부팅 시퀀스가 있습니다. 보안 부팅을 사용하면 변조된 Axis 장치의 배포를 차단합니다.

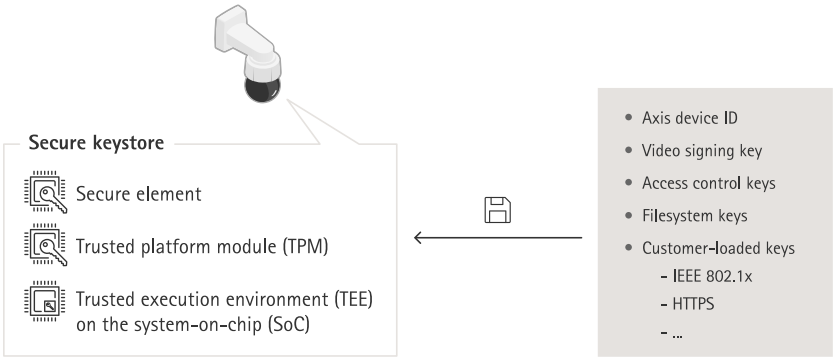


*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오.

보안 키 저장소

CSC #6: 접근 제어 관리

보안 키 저장소는 하드웨어 기반의 변조 방지 암호화 정보 저장을 제공합니다. 보안 침해 발생 시 무단 접근 및 악의적인 유출을 방지하는 동시에 고객이 업로드한 암호화 정보와 더불어 Axis 장치 ID를 보호합니다. 보안 요구 사항에 따라 Axis 장치에는 Trusted Platform Module (TPM) 2.0, 보안 요소 및/또는 TEE(Trusted Execution Environment)와 같은 모듈이 하나 또는 여러 개 포함될 수 있습니다.



*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오.

암호화된 파일 시스템

CSC #3: 데이터 보호

악의적인 공격자는 플래시 메모리를 분리하고 플래시 리더 장치를 통해 액세스하여 파일 시스템에서 정보를 추출하려고 시도할 수 있습니다. 그러나 Axis 장치는 누군가가 파일 시스템에 물리적으로 액세스하거나 이를 도용할 경우 악의적인 데이터 유출 및 구성 변조로부터 파일 시스템을 보호할 수 있습니다. Axis 장치의 전원이 꺼지면 파일 시스템의 정보가 AES-XTS-Plain64 256비트로 암호화됩니다. Secure Boot 프로세스 중에 읽기-쓰기 파일 시스템이 해독되어 Axis 장치에서 마운트하고 사용할 수 있습니다.

*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오.

소프트웨어 구성품 명세서(SBOM)

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어

취약점을 관리하고 공급망 투명성을 높이기 위한 소프트웨어 구성품 명세서(SBOM)는 Axis 제품에 대한 신뢰를 높이는 핵심 도구입니다. SBOM은 axis.com에 게시되는 모든 장치 소프트웨어 릴리스와 함께 제공됩니다.

폐기

CSC #3: 데이터 보호

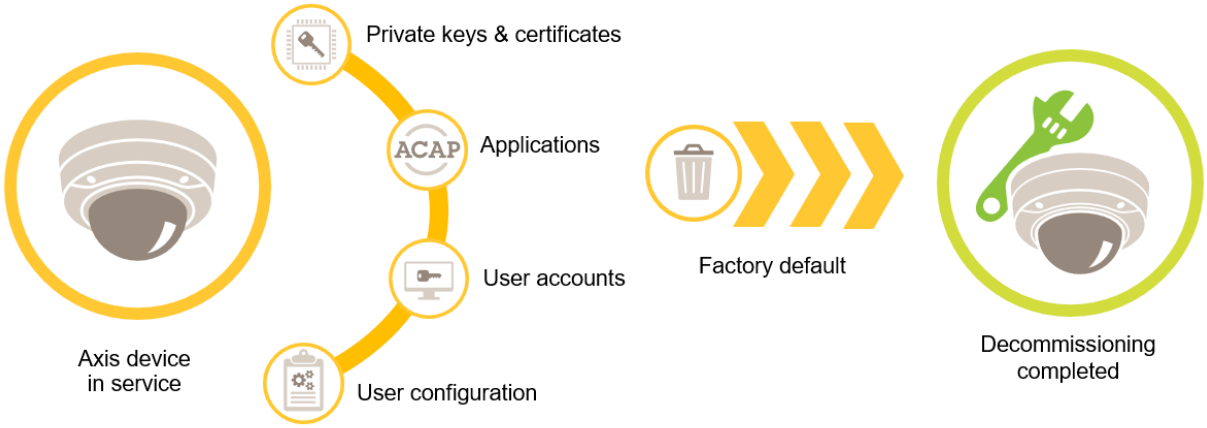
Axis 장치는 휘발성 메모리와 비휘발성 메모리를 모두 사용합니다. 휘발성 메모리는 장치의 전원을 분리할 때마다 지워지지만, 비휘발성 메모리에 저장된 정보는 유지되어 시작 시 다시 사용할 수 있습니다. 파일 시스템에서 저장된 데이터가 보이지 않게 하려고 단순히 데이터 포인터를 제거하는 일반

적인 관행을 피하기 위해 공장 초기화가 필요합니다. NAND 플래시 메모리의 경우 UBI 기능인 "Remove Volume(볼륨 제거)"가 사용됩니다. eMMC 플래시 메모리에도 동등한 기능이 사용되어 저장 블록이 더 이상 사용되지 않음을 알립니다. 그러면 스토리지 컨트롤러가 해당 스토리지 블록을 삭제합니다.

Axis 장치를 폐기할 때는 장치를 공장 출하 시 기본값으로 재설정하여 장치의 비휘발성 메모리에 저장된 모든 데이터를 삭제하는 것이 좋습니다.

공장 초기화 명령을 실행해도 데이터가 즉시 삭제되는 것이 아니라 장치가 재부팅되고 시스템 부팅 중에 데이터가 삭제됩니다. 따라서 단순히 공장 초기화 명령을 내리는 것만으로는 충분하지 않습니다. 데이터 삭제가 완료되었음을 보장하려면 장치가 재부팅되고 부팅이 완료된 후 전원을 꺼야 합니다.

이러한 고객 데이터 삭제 절차는 NIST SP-800-88 Revision 1에 설명된 '클리어' 삭제 기술을 따릅니다.



AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Maintenance > Default(설정 > 시스템 옵션 > 유지보수 > 기본값)
7.10 미만	Settings > System > Maintenance > Default(설정 > 시스템 > 유지보수 > 기본값)
≥ 10.9	Maintenance > Default(유지보수 > 기본값)

이 표에는 비휘발성 메모리에 저장된 데이터에 대한 세부 정보가 포함되어 있습니다.

정보 및 데이터	**공장 출하 시 기본값 복원 후 지워짐**
VAPIX 및 ONVIF 사용자 이름과 패스워드	예
인증서 및 개인 키	예
자체 서명 인증서	예
TPM 및 Axis Edge Vault에 저장된 정보	예
WLAN 설정 및 사용자/패스워드	예
사용자 정의 인증서*	아니요
SD 카드 암호화 키	예

SD 카드 데이터**	아니요
네트워크 공유 설정 및 사용자/패스워드	예
네트워크 공유 데이터**	아니요
사용자 구성***	예
업로드된 애플리케이션(ACAP)****	예
생산 데이터 및 수명 통계*****	아니요
업로드된 그래픽 및 오버레이	예
RTC 시계 데이터	예

* Signed OS 프로세스는 사용자가 AXIS OS(및 기타 항목)를 업로드할 수 있도록 허용하는 사용자 지정 인증서를 사용합니다.
** 엣지 스토리지(SD 카드, 네트워크 공유)에 저장된 녹화물과 이미지는 사용자가 별도로 삭제해야 합니다. SD 카드의 고객 데이터는 NIST SP-800-88 Revision 1 Cryptographic Erase(CE)에 따라 삭제되며, HDD(S30 Recorder Series)의 데이터는 NIST SP-800-88 Revision 1 Clear에 따라 삭제됩니다. 자세한 내용은 AXIS OS 기술 자료의 를 참조하십시오.
*** 계정 생성부터 네트워크, O3C, 이벤트, 이미지, PTZ 및 시스템 구성에 이르기까지 모든 사용자 구성이 가능합니다.
**** 장치는 사전 설치된 애플리케이션을 유지하지만 사용자가 만든 모든 구성은 삭제합니다.
***** 생산 데이터(보정, 802.1AR 생산 인증서) 및 수명 통계에는 민감하지 않고 사용자와 관련이 없는 정보가 포함됩니다.

기본 보안 강화

기본 보안 강화는 Axis 장치에 권장되는 최소한의 보호 수준입니다. 기본 보안 강화 주제는 "엣지에서 구성 가능"합니다. 즉, 타사 네트워크 인프라, 영상 또는 증거 관리 시스템(VMS, EMS), 장비 또는 애플리케이션에 대한 추가 종속성 없이 Axis 장치에서 직접 구성이 가능합니다.

공장 출하 시 기본 설정

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

장치를 구성하기 전에 장치가 공장 출하 시 기본 설정 상태인지 확인하십시오. 사용자 데이터에서 장치를 지우거나 폐기해야 할 때는 장치를 공장 출하 시 기본 설정 설정으로 초기화하는 것도 중요합니다. 자세한 내용은 *폐기, on page 11*를 참조하십시오.

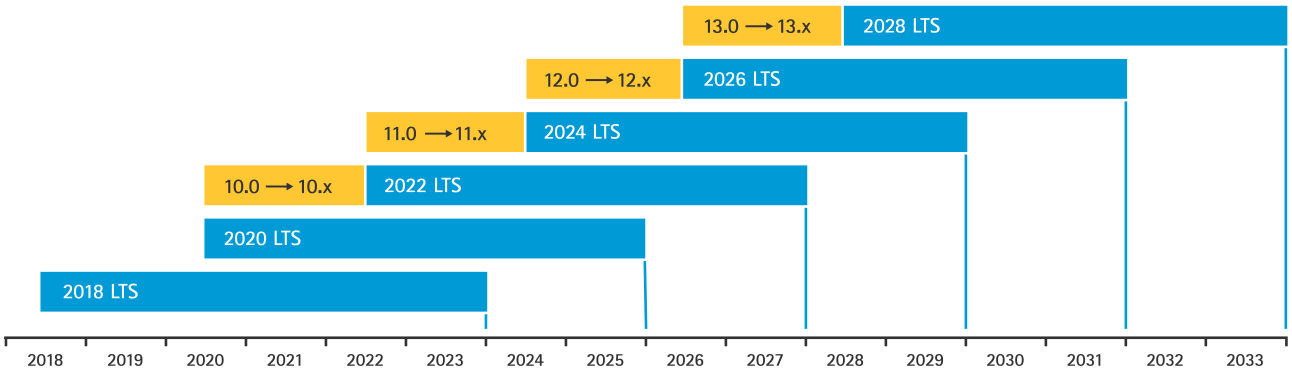
AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Maintenance > Default(설정 > 시스템 옵션 > 유지보수 > 기본값)
7.10 미만	Settings > System > Maintenance > Default(설정 > 시스템 > 유지보수 > 기본값)
≥ 10.9	Maintenance(유지 관리) > Factory default(공장 출하 시 기본값)

최신 AXIS OS로 업그레이드

CSC #2: 소프트웨어 자산의 인벤토리 및 제어

소프트웨어 패치는 사이버 보안의 중요한 부분입니다. 공격자들은 흔히 일반적으로 알려진 취약성을 악용하려고 시도하며, 패치가 적용되지 않은 서비스에 대한 네트워크 액세스 권한을 확보하면 공격에 성공할 수 있습니다. 알려진 취약점에 대한 보안 패치가 포함되어 있을 수 있으므로 항상 최신 AXIS OS 버전을 사용해야 합니다. 특정 버전에 대한 릴리스 정보에는 중요 보안 수정 사항이 명시적으로 언급될 수 있지만, 모든 일반 수정 사항에 적용되는 것은 아닙니다.

Axis는 Active 트랙과 LTS(Long Term Support) 트랙이라는 두 가지 유형의 AXIS OS 트랙을 유지 관리합니다. 두 트랙 모두 최신 치명적 취약점 패치를 포함하지만, LTS 트랙은 호환성 문제의 위험을 최소화하는 것을 목표로 하므로 새로운 기능은 포함하지 않습니다. AXIS OS 정보의 *AXIS OS 수명 주기*에서 자세한 내용을 살펴보십시오.



Axis는 중요한 새 기능, 버그 수정 및 보안 패치 관련 정보와 함께 향후 릴리스에 대한 예측을 제시합니다. 자세한 내용은 AXIS OS 정보의 *향후 출시*를 참조하십시오. 장치용 AXIS OS를 다운로드하려면 axis.com의 *장치 소프트웨어*를 방문하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Maintenance > Upgrade Server(설정 > 시스템 옵션 > 유지보수 > 서버 업그레이드)
7.10 미만	Setup > System > Maintenance > Firmware upgrade(설정 > 시스템 > 유지보수 > 펌웨어 업그레이드)
≥ 10.9	Maintenance(유지 관리) > AXIS OS upgrade (AXIS OS 업그레이드)

전용 계정 생성

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #5: 계정 관리

Axis 장치에는 관리자 계정과 클라이언트 사용자 계정이라는 두 가지 유형의 계정이 있을 수 있습니다. 관리자 계정은 장치 관리를 위한 기본 계정으로, 관리 작업에만 사용하도록 지정해야 합니다. 장치를 설정할 때 관리자 계정의 사용자 이름 및 패스워드를 만들어야 합니다.

관리자 계정 외에 일상적인 운영을 위해 제한된 권한을 가진 클라이언트 사용자 계정을 만듭니다. 이렇게 하면 장치를 안전하게 관리할 수 있어 장치 관리자 패스워드가 유출될 위험을 줄일 수 있습니다. 전체 관리 권한이 필요하지 않은 작업에는 클라이언트 사용자 계정을 사용해야 합니다.

두 계정의 패스워드를 만들 때는, 새 패스워드를 충분히 길고 복잡하게 만들 것을 요구하는 NIST 또는 BSI 패스워드 권장 사항과 같은 가이드라인을 따르는 것이 좋습니다. Axis 장치는 최대 64자의 패스워드를 지원합니다. 8자 미만의 패스워드는 약한 것으로 간주됩니다. 자세한 내용은 AXIS OS 기술 자료의 *ID 및 액세스 관리*를 참조하십시오.

AXIS OS 11.6 이상 버전이 설치된 Axis 장치는 OAuth 2.0을 지원합니다. 이를 통해 중앙 집중식 ID 및 액세스 관리(IAM)와 연합 ID를 사용하여 장치에 인증할 수 있습니다. 따라서 로컬 장치의 사용자를 별도로 관리할 필요가 없어집니다. 자세한 내용은 *OAuth 2.0, on page 27*을 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > Basic Setup > Users(설정 > 기본 설정 > 사용자)
7.10 미만	Settings > System > Users(설정 > 시스템 > 사용자)
≥ 10.9	System > Users(시스템 > 사용자)
≥ 11.6	System > Accounts(시스템 > 계정)

네트워크, 날짜 및 시간 설정 구성

CSC #4: CSC #8: 감사 로그 관리
CSC #12: 네트워크 인프라 관리

Axis 장치의 기능 및 보안을 유지하려면 장치의 네트워크, 날짜 및 시간 설정을 올바르게 구성하는 것이 중요합니다. 이러한 설정은 네트워크 통신, 로깅, 인증서 유효성 검사를 포함한 장치 동작의 다양한 측면에 영향을 줍니다.

장치 IP 구성은 IPv4/IPv6, 정적 또는 동적(DHCP) 네트워크 주소, 서브넷 마스크 및 기본 라우터와 같은 네트워크 구성에 따라 달라집니다. 새 구성 요소를 추가할 때마다 네트워크 토폴로지를 검토하십시오. 네트워크 접근성을 보장하고 DHCP 서버와 같이 공격에 취약할 수 있는 네트워크 서버에 대한 의존성을 최소화하기 위해 고정 IP 주소 구성을 사용하는 것이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > Basic Setup > TCP/IP(설정 > 기본 설정 > TCP/IP)
7.10 미만	Settings > System > TCP/IP(시스템 > 설정 > TCP/IP)
≥ 10.9	System > Network(시스템 > 네트워크)

정확한 시간 기록은 시스템 로그를 유지하고, 디지털 인증서의 유효성을 검사하고, HTTPS, IEEE, 802.1x와 같은 서비스를 지원하는 데 필수적입니다. NTP(Network Time Protocol) 또는 NTS(Network Time Security) 서버와 장치의 시계를 동기화하는 것이 좋습니다. NTP(Network Time Protocol)의 암호화되고 안전한 변형인 NTS(Network Time Protocol)가 AXIS OS 11.1에 추가되었습니다. 정확도를 높이도록 다중 시간 서버를 구성하고 잠재적인 장애를 고려하는 것이 좋습니다. 현지 시간 서버를 호스팅할 수 없는 경우, 공용 NTP 또는 NTS 서버를 사용하는 것이 좋습니다. Axis 장치의 NTP/NTS에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *NTP 및 NTS*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > Basic Setup > Date & Time(설정 > 기본 설정 > 날짜 및 시간)
7.10 미만	Settings > System > Date and time(설정 > 시스템 > 날짜 및 시간)
≥ 10.9	System > Date and time(시스템 > 날짜 및 시간)
≥ 11.6	System > Time and location(시스템 > 시간 및 위치)

엣지 스토리지 암호화

CSC #3: 데이터 보호

SD 카드
Axis 장치가 SD(보안 디지털) 카드를 지원하고 이를 사용하여 영상 녹화를 저장하는 경우, 암호화를 적용하는 것이 좋습니다. 이렇게 하면 권한이 없는 사용자가 제거된 SD 카드에서 저장된 비디오를 재생할 수 없습니다.

Axis 장치의 SD 카드 암호화에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *SD 카드 지원*을 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Storage(설정 > 시스템 옵션 > 스토리지)
7.10 미만	Settings > System > Storage(설정 > 시스템 > 스토리지)
≥ 10.9	System > Storage(시스템 > 스토리지)

네트워크 공유(NAS)
네트워크 연결 스토리지(NAS)를 녹화 장치로 사용하는 경우, 접근이 제한된 잠금 구역에 보관하고 하드 디스크 암호화를 활성화하는 것이 좋습니다. Axis 장치는 영상 녹화물을 저장하기 위해 NAS에 연결할 때 네트워크 프로토콜로 SMB를 활용합니다. 이전 버전의 SMB(1.0 및 2.0)는 보안 또는 암호화를 제공하지 않지만, 이후 버전(2.1 이상) 에서는 제공하므로, 생성 시에는 최신 버전의 사용을 권장합니다.

Axis 장치를 네트워크 공유에 연결할 때 올바른 SMB 구성에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *네트워크 공유*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Storage(설정 > 시스템 옵션 > 스토리지)
7.10 미만	Settings > System > Storage(설정 > 시스템 > 스토리지)
≥ 10.9	System > Storage(시스템 > 스토리지)

애플리케이션(ACAP)

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

Axis 장치에 애플리케이션을 업로드하여 기능을 확장할 수 있습니다. 대다수는 특정 기능과 상호 작용할 수 있는 자체 사용자 인터페이스와 함께 제공됩니다. 애플리케이션은 AXIS OS에서 제공하는 보안 기능을 사용할 수 있습니다.

Axis 장치에는 *ASDM(Axis Security Development Model)*에 따라 개발한 여러 Axis 개발 애플리케이션이 사전 로드되어 있습니다. axis.com의 *분석*에서 Axis 애플리케이션에 대한 세부 정보를 참고하십시오.

타사 애플리케이션의 경우, 운영 및 테스트 측면에서 애플리케이션의 보안과 일반적인 모범 보안 개발 모델에 따른 개발 여부에 관해서는 공급업체에 문의하여 확인하는 것이 좋습니다. 타사 애플리케이션에서 발견된 취약성은 타사 공급업체에 직접 보고해야 합니다.

신뢰할 수 있는 애플리케이션만 실행하고, Axis 장치에서 미사용 애플리케이션을 제거하는 것이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > Applications(설정 > 애플리케이션)
7.10 미만	Settings > Apps(설정 > 앱)
≥ 10.9	앱

AXIS OS 12.0(2024년 9월)부터 ACAP 서명이 필수이며 기본으로 활성화되어 있으나, 비활성화할 수 있는 옵션이 제공됩니다. AXIS OS 13.0(2026년 9월)부터 ACAP 서명은 필수 사항이며, 비활성화 옵션이 없습니다. ACAP는 스웨덴 룬드 소재 Axis 데이터 센터 내 Thales Luna Network HSM 7에 안전하게 저장된 4096비트 RSA 개인 키와 SHA-512를 사용하여 ACAP 포털에서 서명됩니다. Axis 네트워크 장치에는 ACAP 설치 전에 ACAP 서명을 검증하기 위해 4096비트 RSA 공개 키가 사전 로드되어 있습니다. 공개 키는 Linux 파일 시스템 상의 Axis 네트워크 장치에 저장됩니다.

사용하지 않는 서비스/기능 비활성화

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

사용하지 않는 서비스 및 기능이 당장 보안에 위협이 되지는 않지만, 불필요한 위험을 줄이기 위해 미사용 서비스 및 기능을 비활성화하는 것이 좋습니다. 사용하지 않는 경우 비활성화할 수 있는 서비스 및 기능을 자세히 알아보려면 계속 읽어보십시오.

웹 인터페이스 액세스

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

CSC #5: 계정 관리

Axis 장치에는 사용자가 표준 브라우저를 통해 장치에 액세스할 수 있도록 하는 웹 서버가 있습니다. 웹 인터페이스는 구성, 유지 관리 및 문제 해결을 위한 용도이며, 영상을 보기 위한 클라이언트와 같은 일상적인 운영을 위한 것은 아닙니다.

일상적인 작업 중에 Axis 장치와 상호 작용하도록 허용되는 클라이언트는 영상 관리 시스템(VMS) 또는 장치 관리 도구(예: AXIS Device Manager)뿐입니다. 시스템 사용자가 Axis 장치에 직접 접근하도록 허용해서는 안 됩니다.

AXIS OS 9.50부터는 Axis 장치의 웹 인터페이스를 비활성화할 수 있습니다. 시스템에 Axis 장치를 배포(또는 AXIS Device Manager에 추가)한 후에는 조직 내 사용자가 웹 브라우저를 통해 장치에 접근할 수 있는 옵션을 제거하기를 권장합니다. 이렇게 하면 조직 내에서 장치 계정 패스워드가 공유되는 경우 추가적인 보안 계층이 형성됩니다. 더 안전한 선택은 고급 ID 접근 관리(IAM) 아키텍처, 강화된 추적성, 계정 유출 방지를 위한 보호 기능을 제공하는 전용 애플리케이션을 통해 Axis 장치에 대한 접근을 독점적으로 설정하는 것입니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	Settings > System > Plain config > System > Web Interface Disabled(설정 > 시스템 > 일반 구성 > 시스템 > 웹 인터페이스 비활성화)
≥ 10.9	System > Plain config > System > Web Interface Disabled(시스템 > 일반 구성 > 시스템 > 웹 인터페이스 비활성화)

사용되지 않은 물리적 네트워크 포트

AXIS OS 11.2부터는 AXIS S3008처럼 여러 네트워크 포트가 있는 장치에 네트워크 포트의 PoE 및 네트워크 트래픽을 모두 비활성화할 수 있는 옵션이 주어집니다. 사용하지 않는 네트워크 포트를 활성 상태로 방치하면 심각한 보안 위험을 초래할 수 있습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 11.2	System > Power over Ethernet(시스템 > PoE (Power over Ethernet))

네트워크 검색 프로토콜

Bonjour, UPnP, ZeroConf 및 WS-Discovery 및 LLDP/CDP와 같은 검색 프로토콜은 네트워크에서 Axis 장치와 해당 서비스를 쉽게 찾을 수 있도록 지원하는 서비스입니다. 장치를 배포하고 VMS에 추가한 후에는 검색 프로토콜을 비활성화하여, Axis 장치가 네트워크에서 존재한다는 사실을 알리지 못하게 하는 것이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled (설정 > 시스템 옵션 > 고급 > 일반 구성 > 네트워크 > 네트워크 Bonjour 활성화, 네트워크 UPnP 활성화, 네트워크 ZeroConf 활성화, 네트워크 UPnP NATTraversal 활성화)*

AXIS OS 버전	웹 인터페이스 구성 경로
	해당 없음
7.10 미만	Settings > System > Plain config > Network > Network Bonjour Enabled, Network UPnP Enabled, Network ZeroConf Enabled, Network UPnP NATTraversal Enabled(설정 > 시스템 > 일반 구성 > 네트워크 > 네트워크 Bonjour 활성화, 네트워크 UPnP 활성화, 네트워크 ZeroConf 활성화, 네트워크 UPnP NATTraversal 활성화)*
	Settings > System > Plain config > WebService > Discovery Mode(설정 > 시스템 > 일반 구성 > WebService > 검색 모드)
≥ 10.9	Settings > Plain config -> Network > Bonjour Enabled, UPnP Enabled, ZeroConf Enabled(설정 > 일반 구성 -> 네트워크 > Bonjour 활성화, UPnP 활성화, ZeroConf 활성화)
	System > Plain config > WebService > DiscoveryMode > Enable WS-Discovery discoverable mode(시스템 > 일반 구성 > WebService > 검색 모드 > WS-Discovery 검색 가능 모드 활성화)
≥ 11.11	System(시스템) > Network(네트워크) > Network discovery protocols(네트워크 검색 프로토콜) > Bonjour, UPnP, WS-Discovery, LLDP 및 CDP**
	Settings(설정) > Plain config(일반 구성) > Network(네트워크) > ZeroConf Enabled (ZeroConf 활성화됨)
≥12.1***	System(시스템) > Network(네트워크) > Network discovery protocols(네트워크 검색 프로토콜) >Bonjour, LLDP 및 CDP**

* 기능은 AXIS 10.12에서 제거되었으며, 이후 버전에서는 사용할 수 없습니다.

** LLDP 및 CDP를 비활성화하면 PoE 전력 협상에 영향을 줄 수 있습니다.
*** 이 버전부터는 기본적으로 ZeroConf를 비활성화할 필요가 없습니다. DHCP를 사용할 수 없고 고정 IP 주소가 구성되어 있지 않은 경우 링크 로컬 주소가 대체 수단으로 사용됩니다.

정보 공개

기본적으로 Axis 장치는 네트워크상의 클라이언트와 HTTP(S) 연결을 수행할 때, 또는 Basic Device Info VAPIX API(*https://developer.axis.com/vapix/network-video/basic-device-information/*)를 통해 현재 사용 중인 Apache, OpenSSL 및 AXIS OS 소프트웨어의 기본 버전 정보를 공개합니다.

이 정보는 Rapid7, Tenable Nessus 등의 네트워크 보안 스캐너 또는 네트워크 모니터링 시스템이 Axis 장치의 미해결 취약점을 스캔하는 데 필수적입니다. 이 정보가 없으면 이러한 애플리케이션이 Axis 장치에서 올바르게 작동하지 않을 수 있습니다. 일반적으로 Axis는 정보 공개를 활성화하고 정상적으로 작동하도록 유지할 것을 권장합니다. 이는 소프트웨어 업데이트, 상황 인식, 모니터링 및 Axis 장치의 안전한 운영을 유지하는 데 도움이 되기 때문입니다.

그러나 일부 사이버 보안 접근 방식에서는 정보 공개를 최소화하거나 완전히 비활성화해야 합니다. 이 요구 사항을 준수할 수 있도록 정보 공개를 비활성화하는 구성 파라미터가 마련되어 있습니다. 그

러나 Axis 권장 사항에 따라 장치를 운영하고 항상 최신 상태로 유지하는 경우에만 이 기능을 비활성화할 것을 권장합니다.

Apache/OpenSSL 버전

HTTP(S) 연결 중 정보 노출을 줄이기 위해 HTTP(S) 서버 헤더를 비활성화하는 옵션은 AXIS OS 10.6부터 제공됩니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	Settings > System > Plain config > System > HTTP Server Header Comments(설정 > 시스템 > 일반 구성 > 시스템 > HTTP 서버 헤더 설명)

≥ 11.11	*https://IP_OR_HOSTNAME/config/web-ui/swagger-ui/?url=/config/discover/apis/basic-device-info/v2/openapi.json#/basic-device-info.v2beta/patch_basic_device_info_v2beta_allowAnonymous*
	
	{
	"data": false
	}

오디오

네트워크 카메라와 같이 Axis 영상 감시 위주의 제품에서는 기본적으로 오디오 입/출력 및 마이크 기능이 비활성화되어 있습니다. 오디오 기능이 필요하다면 사용 전에 해당 기능을 활성화해야 합니다. Axis 인터콤과 네트워크 스피커 등 오디오 입/출력 및 마이크 기능이 핵심적인 Axis 제품에서는 오디오 기능이 기본적으로 활성화되어 있습니다.

오디오 기능을 사용하지 않는다면 비활성화하는 것을 권장합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > Audio > Audio A* > Enabled(설정 > 시스템 옵션 > 고급 > 일반 구성 > 오디오 > 오디오 A* > 활성화)
7.10 미만	Settings > Audio > Allow Audio(설정 > 오디오 > 오디오 허용)
≥ 10.9	Audio > Device settings(오디오 > 장치 설정)

SD 카드 슬롯

Axis 장치는 주로 영상 녹화의 로컬 엣지 스토리지를 제공하기 위해 SD 카드를 하나 이상 지원합니다. SD 카드를 사용하지 않는다면 SD 카드 슬롯을 완전히 비활성화하는 것이 좋습니다. AXIS OS 9.80에서 SD 카드 슬롯을 비활성화하는 옵션을 사용할 수 있습니다.

자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *SD 카드 비활성화*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	Settings > System > Plain config > Storage > SD Disk Enabled(설정 > 시스템 > 일반 구성 > 저장소 > SD 디스크 활성화)
≥ 10.9	System > Plain config > Storage > SD Disk Enabled(시스템 > 일반 구성 > 저장소 > SD 디스크 활성화)

SSH 액세스

SSH는 문제 해결 및 디버깅 목적으로만 사용되는 보안 통신 프로토콜입니다. 이 기능은 AXIS OS 5.50부터 시작하는 Axis 장치에서 지원됩니다. SSH 액세스를 비활성화하는 것이 좋습니다.

SSH를 사용한 디버깅 옵션에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *SSH 액세스*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Plain Config > Network > SSH Enabled(설정 > 시스템 옵션 > 일반 구성 > 네트워크 > SSH 활성화)
7.10 미만	Settings > System > Plain config > Network > SSH Enabled(설정 > 시스템 > 일반 구성 > 네트워크 > SSH 활성화)
≥ 10.9	System > Plain config > Network > SSH Enabled(시스템 > 일반 구성 > 네트워크 > SSH 활성화)

USB

AXIS OS 12.1부터 AXIS D1110에는 USB 포트를 비활성화하는 옵션이 제공됩니다. 사용하지 않는 USB 포트를 활성 상태로 방치하면 심각한 보안 위험을 초래할 수 있습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 12.1	System(시스템) > > Accessories(액세서리) > USB Configuration(USB 구성)

Wi-Fi 기능

일부 Axis 장치는 USB Wi-Fi 동글을 통한 내장 액세스 포인트를 사용하여 Wi-Fi 기능을 제공합니다. Wi-Fi는 물리적 RJ45 네트워크 연결이 없는 상태에서 물리적 WLAN 설정 버튼을 눌러야만 활성화됩니다. 이는 장치가 공장 초기화 상태이든 작동 중이든 관계없이 적용됩니다. AXIS M1075에서 사용자는 제품 라벨에 있는 SSID 및 장치 고유 SSID 패스워드를 사용하여 액세스 포인트에 연결할 수 있습니다. 최신 일부 Axis 제품에서는 SSID만 필요하며(패스워드 불필요), 이는 사이버 보안을 타협하지 않으면서도 설치 편의성을 향상시킵니다.

Axis 장치 설정 및 Wi-Fi 기능에 대해서는 사용자 설명서를 참조하십시오. 다음은 Wi-Fi를 지원하는 일부 Axis 제품의 내장 액세스 포인트 기능 작동 방식을 설명합니다.

- 내장 액세스 포인트는 Wi-Fi SSID/패스워드가 구성되지 않았고 물리적 RJ45 네트워크 연결이 없는 조건에서 물리적 WLAN 설정 버튼을 눌러야만 활성화할 수 있습니다. 이는 장치가 공장 초기화 상태이든 작동 중이든 관계없이 적용됩니다.
- 카메라가 사용자가 구성한 액세스 포인트에 연결되면 내장 액세스 포인트는 비활성화됩니다. 또는 설치 중 사용자가 물리적 WLAN 설정 버튼을 누른 후 15분이 지나면 자동으로 비활성화됩니다.

장치가 연결된 Wi-Fi 동글을 사용하는 경우, 가장 강력한 보안을 위해 장치 초기 구성 시 SSID + 패스워드를 사용하여 Wi-Fi 기능을 적절히 구성하는 것이 좋습니다.

블루투스

일부 Axis 장치에는 내장형 블루투스 기능이 제공됩니다. 이 기능은 공장 초기화 후 이미지 및 렌즈 조정 등 장치의 초기 설정 단계에서 원활한 사용자 경험을 제공하기 위해 사용할 수 있습니다.

설정 방법 및 블루투스 기능은 해당 장치의 사용자 설명서를 참조하십시오. 다음은 Axis 제품의 일반적인 블루투스 기능에 대한 설명입니다.

- 블루투스는 구성된 사용자가 없는 한 공장 초기화 상태에서 자동으로 활성화되며, 최초 부팅 후 최대 2시간 동안 유지됩니다. 블루투스는 사용자가 구성되면 또는 최초 부팅 후 2시간이 지나면, 물리적 RJ45 네트워크 연결의 유무와 관계없이 자동으로 비활성화됩니다.
- 블루투스가 비활성화된 후에는 사용자가 이를 수동으로 활성화할 수 없습니다. 블루투스 기능을 복원하려면 장치를 다시 공장 초기화 상태로 재설정해야 합니다.
- 사용 중인 장치와 Axis 장치 간의 블루투스 연결은 최신 TLS 1.2/1.3 암호화를 사용하는 HTTPS 터널을 사용합니다. Axis 제품은 Bluetooth Security Mode 1 Level 2(인증되지 않은 페어링을 통한 암호화, Just Works)를 사용합니다.

네트워크 액세스 제한

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #13: 네트워크 모니터링 및 방어

AXIS OS 11.9에는 IP 주소 및/또는 TCP/UDP 포트 번호별로 인바운드 트래픽을 규제하는 규칙을 생성할 수 있는 보안 기능인 호스트 기반 방화벽이 도입되었습니다. 이를 통해 장치 또는 해당 서비스에 대한 무단 접근을 방지할 수 있습니다.

기본 정책을 "Drop(차단)"으로 설정한 경우, 목록에 인증을 받은 모든 클라이언트(VMS 및 관리 클라이언트) 및/또는 포트를 추가해야 합니다.

AXIS OS 버전	**웹 인터페이스 구성 경로**
≥ 11.9	System(시스템) > Security(보안) > Firewall(방화벽)

IP 주소 필터링

AXIS OS 11.8 이하의 버전이 설치된 장치는 IP 주소 필터링을 사용하여 승인되지 않은 클라이언트의 액세스를 방지합니다. 장치를 승인된 네트워크 호스트 IP 주소를 허용하도록 구성하거나 승인되지 않은 네트워크 호스트 IP 주소를 거부하도록 구성하는 것이 좋습니다.

IP 주소를 허용하기로 선택하는 경우, VMS 서버와 관리 클라이언트를 포함하여 승인된 모든 클라이언트를 목록에 반드시 추가해야 합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Security > IP Address Filter(설정 > 시스템 옵션 > 보안 > IP 주소 필터)
7.10 미만	Settings > System > TCP/IP > IP address filter (설정 > 시스템 > TCP/IP > IP 주소 필터)
10.9 — 11.8	Settings > Security > IP address filter(설정 > 보안 > IP 주소 필터)

비고

네트워크 액세스 시도에 대한 자세한 로그를 활성화하여 다른 네트워크 호스트의 원치 않는 액세스 시도를 식별하는 데 도움을 받을 수 있습니다. 이를 수행하려면 **System(시스템)** > **Plain config (일반 구성)** > **Network(네트워크)** 및 Network Filter Log(네트워크 필터 로그)로 이동합니다.

HTTPS

CSC #3: 데이터 보호

HTTP 및 HTTPS는 AXIS OS 7.20부터 Axis 장치에서 기본적으로 활성화됩니다. HTTP 액세스는 전혀 암호화되지 않아 안전하지 않은 반면, HTTPS는 클라이언트와 Axis 장치 간의 트래픽을 암호화합니다. Axis 장치의 모든 관리 작업에는 HTTPS를 사용하는 것이 좋습니다.

HTTPS만, on page 23 및 *HTTPS 암호, on page 23*에서 구성 지침을 살펴보십시오.

HTTPS만

HTTPS만 사용할 수 있게(HTTP 접근은 불가능) Axis 장치를 구성하는 것이 좋습니다. 이렇게 하면 자동으로 HSTS(HTTP Strict Transport Security)가 활성화되어 장치의 보안이 더 강화됩니다.

AXIS OS 7.20부터 Axis 장치는 2038년 1월 19일까지 유효한 자체 서명 인증서와 함께 제공됩니다. 자체 서명 인증서는 설계상 신뢰할 수 없지만, 초기 구성 시 또는 공개 키 기반 구조(PKI)를 사용할 수 없는 경우 Axis 장치에 안전하게 액세스하는 데 적합합니다. 가능한 경우, 자체 서명 인증서를 제거하고, 선택한 PKI 기관에서 발급한 적절한 서명 클라이언트 인증서로 교체해야 합니다. AXIS OS 10.10부터 자체 서명 인증서가 IEEE 802.1AR 보안 장치 ID 인증서로 대체되었습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Security > HTTPS(설정 > 시스템 옵션 > 보안 > HTTPS)
7.10 미만	Settings > System > Security > HTTP and HTTPS(설정 > 시스템 > 보안 > HTTP 또는 HTTPS)
≥ 10.9	System > Network > HTTP and HTTPS(시스템 > 네트워크 > HTTP 또는 HTTPS)

HTTPS 암호

Axis 장치는 TLS 1.2 및 TLS 1.3 암호화 모음을 지원 및 사용하여 HTTPS 연결을 안전하게 암호화합니다. 사용하는 특정 TLS 버전 및 암호 모음은 Axis 장치에 연결하는 클라이언트에 따라 달라지며, 그에 따라 협상하게 됩니다. 정기적인 AXIS OS 업데이트를 통해, 실제 암호 구성이 변경되지 않더라도 Axis 장치의 사용 가능한 암호 목록이 업데이트될 수 있습니다. 암호 구성의 변경은 사용자가 시작해야 하며, Axis 기기/장치의 공장 출하 시 기본 설정을 수행하거나 수동 사용자 구성을 통해 시작해야 합니다. AXIS OS 10.8 이상부터는 사용자가 AXIS OS 업데이트를 수행할 때 암호 목록이 자동으로 업데이트됩니다.

TLS 1.2 이하

TLS 1.2 이하 버전을 사용하는 경우, Axis 기기/장치가 다시 시작되면 HTTPS 암호를 사용하도록 지정할 수 있습니다. 선택할 수 있는 암호에는 제한이 없지만 다음 강력한 암호 중 일부 또는 전부를 선택하는 것이 좋습니다.

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305
```

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > HTTPS > Ciphers(설정 > 시스템 옵션 > 고급 > 일반 구성 > HTTPS > 암호)
7.10 미만	Settings > System > Plain config > HTTPS > Ciphers(설정 > 시스템 > 일반 구성 > HTTPS > 암호)
≥ 10.9	System > Plain config > HTTPS > Ciphers(시스템 > 일반 구성 > HTTPS > 암호)

TLS 1.3

기본적으로 TLS 1.3 사양에 따른 강력한 암호 모음만 사용할 수 있습니다:

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_
SHA384
```

이 모음은 사용자가 구성할 수 없습니다.

확장 보안 강화

확장된 강화의 지침은 *기본 보호, on page 4* 및 *기본 보안 강화, on page 14*에서 설명하는 강화 주제를 기반으로 합니다. 그러나 Axis 장치에는 기본 및 기본 보안 강화 지침을 직접 적용할 수 있지만, 확장 강화에는 전체 공급업체 공급망, 최종 사용자 조직 및 기본 IT 및/또는 네트워크 인프라의 적극적인 참여가 필요합니다.

인터넷 및 네트워크 노출 제한

CSC #12: 네트워크 인프라 관리

Axis 장치를 공용 웹 서버로 노출하거나 알 수 없는 클라이언트가 장치에 네트워크 접근을 허용하는 것을 방지하는 것이 좋습니다. 비디오 매니지먼트 소프트웨어(VMS)를 사용하지 않거나 원격 위치에서 비디오에 액세스해야 하는 소규모 조직 및 개인에게는 AXIS Camera Station Edge가 좋은 선택입니다.

AXIS Camera Station Edge는 Windows, iOS, Android에서 무료로 이용할 수 있으며, 장치를 인터넷에 노출하지 않고도 비디오에 안전하게 액세스할 수 있는 간편한 방법을 제공합니다. 자세한 내용은 *axis.com/products/axis-camera-station-edge*를 참조하십시오.

비고

조직에서 VMS를 사용하는 경우 원격 비디오 액세스에 대한 모범 사례는 VMS 공급업체에 문의하십시오.

네트워크 장치와 관련 인프라와 애플리케이션을 격리하면 네트워크 노출 위험이 줄어듭니다.

생산 및 비즈니스 네트워크에 연결되지 않은 로컬 네트워크에서 Axis 장치와 관련 인프라 및 애플리케이션을 격리하는 것이 좋습니다.

기본 보안 강화를 적용하려면 다중 네트워크 보안 메커니즘을 사용하여 무단 액세스로부터 로컬 네트워크와 해당 인프라(라우터, 스위치)를 보호합니다. 여기에는 VLAN 세분화, 제한된 라우팅 기능, 사이트 간 또는 WAN 액세스를 위한 VPN, 네트워크 계층 2/3 방화벽, 접근 제어 목록(ACL)이 포함될 수 있습니다.

기본 보안 강화 기능을 확장하려면 심층 패킷 검사 및 침입 감지와 같은 고급 네트워크 검사 기술을 적용합니다. 이를 통해 네트워크 내의 위협 보호 기능이 강화됩니다. 확장 네트워크 보안 강화에는 일반적으로 특수 소프트웨어 및/또는 하드웨어 장비가 필요합니다.

네트워크 취약성 스캐닝

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #12: 네트워크 인프라 관리

네트워크 보안 스캐너로 네트워크 장치의 취약성 평가를 실시할 수 있습니다. 취약성 평가의 목적은 잠재적인 보안 취약성과 구성 오류를 체계적으로 검토하는 것입니다.

Axis 장치 및 관련 인프라에 대한 정기적인 취약성 평가 수행을 권장합니다. 스캔을 시작하기 전에 Axis 장치가 LTS 또는 액티브 트랙에서 사용 가능한 최신 AXIS OS 버전으로 업데이트되었는지 확인하십시오.

또한 스캔 보고서를 검토하여 Axis 장치에서 알려진 오탐지를 필터링하는 것이 좋으며, 이는 *AXIS OS 취약성 스캐너 가이드*에서 확인할 수 있습니다. 보고서와 추가 의견을 axis.com의 *Axis 지원*에 티켓으로 제출하십시오.

신뢰할 수 있는 공개 키 인프라(PKI)

CSC #3: 데이터 보호
CSC #12: 네트워크 인프라 관리

Axis 장치에는 신뢰성 있고 공인 또는 사설 인증 기관(CA)에서 서명 웹 서버 및 클라이언트 인증서를 배포하는 것을 권장합니다 신뢰 체인이 검증된 CA 서명 인증서는 HTTPS로 연결할 때 발생하는 브라우저 인증서 경고를 제거하는 데 도움이 됩니다. 또한, 네트워크 접근 제어(NAC) 솔루션을 도입할 때

CA 서명 인증서는 Axis 장치의 신뢰성을 보장합니다. 이렇게 하면 Axis 장치를 사칭하는 컴퓨터의 공격 위험을 줄일 수 있습니다.

CA 서비스가 내장된 AXIS Device Manager를 사용하여 Axis 장치에 서명 인증서를 발급할 수 있습니다.

원격 syslog

CSC #8: 감사 로그 관리

암호화된 모든 로그 메시지를 중앙 syslog 서버로 보내도록 Axis 장치를 구성할 수 있습니다. 이렇게 하면 감사가 더 쉬워지고 고의적/악의적으로 또는 실수로 Axis 장치에서 로그 메시지가 삭제되는 것을 막을 수 있습니다. 회사 정책에 따라서 장치 로그의 보존 기간을 연장할 수도 있습니다.

다양한 AXIS OS 버전에서 원격 syslog 서버를 활성화하는 방법에 대한 자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *Syslog*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	지침은 AXIS OS Lifecycle 가이드의 *Syslog*를 참조하십시오.
7.10 미만	Settings > System > TCP/IP(시스템 > 설정 > TCP/IP)
≥ 10.9	System > Logs(시스템 > 로그)

SNMP

CSC #3: 데이터 보호
CSC #8: 감사 로그 관리

Axis 장치를 구성하여 SNMPv3를 통해 중앙 SNMP 서버로 암호화된 SNMP 상태 모니터링 데이터를 전송할 수 있습니다. SNMP 기반 네트워크 모니터링을 사용하면 경보를 생성하고 장치를 장기간 모니터링할 수 있습니다. 암호화와 프라이버시를 제공하는 것은 SNMPv3뿐이므로, SNMPv1 및 SNMPv2c보다 SNMPv3 사용을 강력히 권장합니다.

AXIS OS 기술 자료(Knowledge base)에서 *SNMP*에 대해 자세히 알아보십시오.

AXIS OS 버전	**웹 인터페이스 구성 경로**
7.10 미만	지침은 AXIS OS 기술 자료(Knowledge base)에서 *SNMP*를 참조하십시오.
7.10 미만	Settings(설정) > System(시스템) > Network(네트워크) > SNMP
≥ 10.9	System > Network > SNMP(시스템 > 네트워크 > SNMP)

보안 비디오 스트리밍(SRTP/RTSPS)

CSC #3: 데이터 보호

AXIS OS 7.40부터, Axis 장치는 RTP를 통한 Secure Video 스트리밍을 지원합니다. 이는 SRTP/RTSPS라고도 합니다. SRTP/RTSPS는 안전한 엔드 투 엔드 암호화 전송 방법을 사용하여 인증된 클라이언트만 Axis 장치의 비디오 스트림을 수신하도록 합니다. 영상 관리 시스템(VMS)에서 SRTP/RTSPS를 지원한다면 이를 활성화하는 것을 권장합니다. 가능한 경우 암호화되지 않은 RTP 비디오 스트리밍 대신 SRTP를 사용하십시오.

비고

SRTP/RTSPS는 비디오 스트림 데이터만을 암호화합니다. 관리 구성 작업에서는 이러한 유형의 통신을 암호화하는 용도로만 HTTPS를 활성화하는 편이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > Network > RTSPS(설정 > 시스템 옵션 > 고급 > 일반 구성 > 네트워크 > RTSPS)
7.10 미만	Settings > System > Plain config > Network > RTSPS(설정 > 시스템 > 일반 구성 > 네트워크 > RTSPS)
≥ 10.9	System > Plain config > Network > RTSPS(시스템 > 일반 구성 > 네트워크 > RTSPS)

Signed Video

CSC #3: 데이터 보호

AXIS OS 10.11부터 Axis Edge Vault가 탑재된 Axis 장치는 Signed video(서명된 비디오)를 지원합니다. 이를 통해 Axis 장치는 비디오 스트림에 서명을 추가하여 비디오가 변조되지 않았음을 보장하고, 비디오를 생성한 장치까지 추적하여 출처를 확인할 수 있습니다.

Axis는 Axis 장치에서 녹화된 비디오의 진위 여부를 확인하는 데 사용할 수 있는 *Axis Signed media verifier* 도구를 제공합니다. 이 도구를 살펴보는 데 사용할 수 있는 세 가지 샘플 파일을 제공합니다.

- *원본이지만 서명되지 않은 비디오*
- *원본이며 서명된 비디오*
- *조작된 비디오*

영상 관리 시스템(VMS) 또는 증거 관리 시스템(EMS)에서도 Axis 장치가 제공하는 비디오의 진위 여부를 확인할 수 있습니다.

*Axis Edge Vault*의 백서에서 자세한 내용을 참조하십시오. 서명된 비디오 인증을 확인하는 데 사용되는 Axis 루트 인증서를 찾으려면 AXIS OS 기술 자료(Knowledge base)에서 *장치 액세스*를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 10.9	System > Plain config > Image > Signed video(시스템 > 일반 구성 > 이미지 > 서명 비디오)

OAuth 2.0

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #5: 계정 관리

OAuth 2.0을 사용하면 AXIS OS 11.6 이상을 실행하는 AXIS OS 장치를 중앙 집중식 ID 및 액세스 관리(IAM) 서비스가 있는 IT 인프라에 통합할 수 있습니다. 이를 통해 연합 ID를 사용하여 Axis 장치에 인증할 수 있으므로, 로컬 장치에서 사용자를 관리할 필요가 없어집니다.

OAuth는 고유한 토큰을 사용하여 각 요청이 유효함을 보장함으로써 CSRF 공격을 완화합니다.

서비스 제공업체의 기능에 따라, 다음과 같은 보안 메커니즘을 사용하여 Axis 장치에 대한 향상된 ID 기반 인증을 사용할 수 있습니다.

- 다단계 인증(MFA)
- 패스워드 복잡성 강제 적용
- 패스워드 순환
- 시간 제한 인증
- 중앙 집중식 ID(사용자/서비스 계정) 관리

AXIS OS 장치에서 OAuth 2.0을 활성화하고 구성하는 방법에 대한 자세한 내용은 AXIS OS 기술 자료의 *OAuth 2.0 OpenID Connect*를 참조하십시오.

AXIS OS 버전	**웹 인터페이스 구성 경로**
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 11.6	System(시스템) > Accounts(계정) > OpenID Configuration(OpenID 구성)

물리적 탬퍼링 방지 액세서리

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #12: 네트워크 인프라 관리

Axis는 Axis 장치의 물리적 보호를 강화하기 위해 물리적 침입 및/또는 탬퍼링 스위치를 옵션 액세서리로 제공합니다. 이러한 스위치는 알람을 트리거하여 Axis 장치가 선택한 클라이언트에 알림 또는 알람을 전송하게 할 수 있습니다.

사용 가능한 변조 방지 액세서리 대한 자세한 내용은 다음 참조:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXIS 도어 스위치 A*

레거시 보안 강화

이 섹션에서는 레거시 AXIS OS 버전 또는 제품에서 찾을 수 있는 파라미터 구성의 보안을 강화하기 위한 보안 강화 지침을 다룹니다. 이러한 파라미터는 최신 LTS 트랙 또는 액티브 트랙에서는 찾을 수 없습니다.

스크립트 편집기 환경

스크립트 편집기 환경에 대한 액세스는 비활성화하는 편이 좋습니다. 스크립트 편집기는 문제 해결 및 디버깅 목적으로만 사용됩니다.

스크립트 편집기는 AXIS OS 10.11에서 제거되었고, 이후 버전에서는 사용하지 못합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 없음
7.10 미만	Settings > System > Plain config > System > Enable the script editor (editcgi)(설정 > 시스템 > 일반 구성 > 시스템 > 스크립트 편집기 활성화(editcgi))
≥ 10.9	System > Plain config > System > Enable the script editor (editcgi)(시스템 > 일반 구성 > 시스템 > 스크립트 편집기 활성화(editcgi))

FTP 액세스

FTP는 문제 해결 및 디버깅 목적으로만 사용되는 안전하지 않은 통신 프로토콜입니다. FTP 액세스는 AXIS OS 11.1에서 제거되었으며 이후 버전에서는 이용할 수 없습니다. 문제 해결을 위해 FTP 액세스를 비활성화하고, 보안 SSH 액세스를 사용하는 것이 좋습니다.

SSH에 대한 자세한 내용은 AXIS OS Lifecycle 가이드의 *SSH 액세스* 를 참조하십시오. FTP를 사용하는 디버깅 옵션에 대한 자세한 내용은 AXIS OS Lifecycle 가이드의 *FTP 액세스* 를 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Plain Config > Network > FTP Enabled(설정 > 시스템 옵션 > 일반 구성 > 네트워크 > FTP 활성화)
7.10 미만	Settings > System > Plain config > Network > FTP Enabled(설정 > 시스템 > 일반 구성 > 네트워크 > FTP 활성화)
≥ 10.9	System > Plain config > Network > FTP Enabled(시스템 > 일반 구성 > 네트워크 > FTP 활성화)

텔넷 액세스

텔넷은 문제 해결 및 디버깅 목적으로만 사용되는 안전하지 않은 통신 프로토콜입니다. 이 기능은 AXIS OS 5.50 이전 버전이 탑재된 Axis 장치에서 지원됩니다. Telnet 액세스를 비활성화하는 것이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
5.50 미만	자세한 내용은 AXIS OS 기술 자료(Knowledge base)에서 *장치 액세스*를 참조하십시오.
7.10 미만	해당 없음
7.10 미만	해당 없음
≥ 10.9	해당 없음

ARP/Ping

ARP/Ping은 AXIS IP Utility와 같은 도구를 사용하여 Axis 장치의 IP 주소를 설정하는 방식이었습니다. 이 기능은 AXIS OS 7.10에서 제거되었고, 이후 버전에서는 사용하지 못합니다. AXIS OS 7.10 및 이전 버전이 설치된 Axis 장치에서는 이 기능을 비활성화하는 것을 권장합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > Network > ARP/Ping(설정 > 시스템 옵션 > 고급 > 일반 구성 > 네트워크 > ARP/Ping)
7.10 미만	해당 없음
≥ 10.9	해당 없음

오래된 TLS 버전

Axis 장치를 운영 체제로 전환하기 전에 이전 버전, 오래된 버전 및 안전하지 않은 TLS 버전을 비활성화하는 것이 좋습니다. 구형 TLS 버전은 일반적으로 기본적으로 비활성화되어 있지만, 아직 TLS 1.2 및 TLS 1.3을 구현하지 않은 타사 애플리케이션과의 하위 호환성을 제공하기 위해 Axis 장치에서 활성화할 수 있습니다.

구형 TLS 버전은 AXIS OS 12.0부터 제거되었으며 이후 버전에서는 사용할 수 없습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1(설정 > 시스템 옵션 > 고급 > 일반 구성 > HTTPS > TLSv1.0 허용 및/또는 TLSv1.1 허용)
7.10 미만	Settings > System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1(설정 > 시스템 > 일반 구성 > HTTPS > TLSv1.0 허용 및/또는 TLSv1.1 허용)
≥ 10.9 – 11.11.X	System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1(시스템 > 일반 구성 > HTTPS > TLSv1.0 허용 및/또는 TLSv1.1 허용)

액세스 로그

CSC #1: 엔터프라이즈 자산의 인벤토리 및 제어
CSC #8: 감사 로그 관리

액세스 로그는 Axis 장치에 액세스하는 사용자의 세부 로그를 제공하므로, 감사 및 접근 제어 관리가 모두 간편해집니다. Axis 장치가 로그를 중앙 로깅 환경으로 보낼 수 있도록 이 기능을 사용하도록 설

정하고 원격 syslog 서버와 결합하는 것이 좋습니다. 이렇게 하면 로그 메시지의 저장 및 보존 시간이 간소화됩니다.

자세한 내용은 AXIS OS 기술 자료(Knowledge base)의 *장치 액세스 로깅*을 참조하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Advanced > Plain Config > System > Access log(설정 > 시스템 옵션 > 고급 > 일반 구성 > 시스템 > 액세스 로그)
7.10 미만	Settings > System > Plain config > System > Access log(설정 > 시스템 > 일반 구성 > 시스템 > 액세스 로그)
≥ 10.9	System > Plain config > System > Access log (시스템 > 일반 구성 > 시스템 > 액세스 로그)

빠른 시작 가이드

빠른 시작 가이드는 AXIS OS 5.51 이상 버전의 AXIS 장치를 강화할 때 구성해야 하는 설정에 대한 간략한 개요를 제공합니다. 이 문서의 *기본 보안 강화, on page 14*에서는 살펴볼 수 있는 강화 주제를 다루지만, *확장 보안 강화, on page 25*에서는 광범위하고 사례별로 고객당 구성이 필요한 관계로 이 주제를 다루지 않습니다.

신속하고 비용 효율적인 방법으로 다수의 Axis 장치를 강화하려면 AXIS Device Manager를 사용하는 것이 좋습니다. 장치 구성에 다른 애플리케이션을 이용해야 하거나 몇 대의 Axis 장치만 강화해야 한다면, VAPIX API 사용을 권장합니다.

일반적인 구성 실수

비고

아래에 나열된 일반적인 구성 실수는 잠재적으로 Axis 장치의 공격 표면을 증가시키고 사이버 보안 방어 계층을 감소시켜 장치의 악용, 오용 또는 안전하지 않은 작동의 위험을 높일 수 있습니다.

인터넷에 노출된 장치
CSC #12: 네트워크 인프라 관리

Axis 장치를 공용 웹 서버로 노출하거나 다른 방식으로 알지 못하는 클라이언트에게 장치에 대한 네트워크 접근 권한을 부여하는 것은 권장하지 않습니다. 자세한 내용은 *폐기, on page 11*를 참조하십시오.

공용 패스워드
CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #5: 계정 관리

모든 장치에 일반적인 패스워드 대신 각 장치마다 고유한 패스워드를 사용하는 것을 적극 권장합니다. 지침은 AXIS OS 기술 자료의 *ID 및 액세스 관리*와 *전용 계정 생성, on page 15*를 참조하십시오.

익명의 액세스
CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성
CSC #5: 계정 관리.

익명 사용자가 로그인 자격 증명을 제시하지 않고도 장치의 영상 및 구성 설정에 접근하도록 허용하는 것은 권장하지 않습니다. 자세한 내용은 *기본으로 비활성화, on page 4*을 참조하십시오.

보안 통신 비활성화
CSC #3: 데이터 보호

암호화 없이 패스워드가 전송되는 HTTP 또는 기본 인증과 같이 보안이 취약한 통신 및 접근 방식을 사용하여 장치를 운영하는 것은 권장하지 않습니다. 자세한 내용은 *폐기, on page 11*를 참조하십시오. *다이제스트 인증, on page 4*에서 구성 권장 사항을 참고하십시오.

오래된 AXIS OS 버전
CSC #2: 소프트웨어 자산의 인벤토리 및 제어

LTS 또는 Active 트랙에서 사용 가능한 최신 AXIS OS 버전으로 Axis 장치를 운영하는 것을 적극 권장합니다. 두 트랙 모두 최신 보안 패치와 버그 수정을 제공합니다. 자세한 내용은 *폐기, on page 11*를 참조하십시오.

VAPIX API를 통한 기본 보안 강화

VAPIX API를 사용하여 *기본 보안 강화, on page 14*에서 다루는 주제에 따라 Axis 장치를 강화할 수 있습니다. 이 표에서 Axis 장치의 AXIS OS 버전과 상관없이 기본 보안 강화 구성 설정을 모두 확인할 수 있습니다.

시간 경과에 따라 보안 강화를 위해 일부 기능이 제거되었으므로, 장치의 AXIS OS 버전에서 일부 구성 설정을 더 이상 사용하지 못할 수 있습니다. VAPIX 호출을 실행할 때 오류가 발생하면, AXIS OS 버전에서 더 이상 해당 기능을 사용할 수 없다는 뜻일 수 있습니다.

목적	VAPIX API 호출
*미사용 네트워크 포트의 POE 비활성화**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*미사용 네트워크 포트의 네트워크 트래픽 비활성화***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Bonjour 검색 프로토콜 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
UPnP 검색 프로토콜 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
WebService 검색 프로토콜 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
O3C(One-Click Cloud Connection) 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
장치 SSH 유지 보수 액세스 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
장치 FTP 유지 보수 액세스 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
ARP-Ping IP 주소 구성 비활성화	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Zero-Conf IP 주소 구성 비활성화	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`

HTTPS만 활성화	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`

TLS 1.2 및 TLS 1.3만 활성화	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

목적	VAPIX API 호출
TLS 1.2 보안 암호 구성	https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305
*무차별 대입 공격 보호 활성화****	https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20 https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1
스크립트 편집기 환경 비활성화	https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no
향상된 사용자 액세스 로깅 활성화	https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On
ONVIF 재생 공격 보호 활성화	https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes
장치 웹 인터페이스 액세스 비활성화	https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes
HTTP/OpenSSL 서버 헤더 비활성화	https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no
익명 뷰어 및 PTZ 액세스 비활성화	https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password

목적	VAPIX API 호출
루트 권한이 필요한 ACAP 애플리케이션의 설치 방지	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
서명되지 않은 ACAP 애플리케이션 설치 방지	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

* “port=X”에서 “X”를 실제 포트 번호로 바꿉니다. 예: “port=1”은 포트 1을 비활성화하고 “port=2”는 포트 2를 비활성화합니다.
** “eth1.1”에서 “1”을 실제 포트 번호로 바꿉니다. 예: “eth1.1”은 포트 1을 비활성화하고 “eth1.2”는 포트 2를 비활성화합니다.
*** 1초 이내에 20번의 로그인 시도 실패 시 클라이언트 IP 주소가 10초 동안 차단됩니다. 페이지 간격 30초 이내에 실패한 요청이 있을 때마다 DoS 차단 기간이 10초 더 연장됩니다.

AXIS Device Manager (Extend)를 통한 기본 보안 강화

AXIS Device Manager 및 AXIS Device Manager Extend를 사용하여 *기본 보안 강화, on page 14*에서 다룬 주제에 따라 Axis 장치를 강화할 수 있습니다. 이 *구성 파일*을 사용하십시오. 이는 *VAPIX API를 통한 기본 보안 강화, on page 32*에 나열된 것과 동일한 구성 설정으로 이루어져 있습니다.

시간 경과에 따라 보안 강화를 위해 일부 기능이 제거되었으므로, 장치의 AXIS OS 버전에서 일부 구성 설정을 더 이상 사용하지 못할 수 있습니다. AXIS Device Manager 및 AXIS Device Manager Extend는 강화 구성에서 이러한 설정을 자동으로 제거합니다.

비고

구성 파일을 업로드한 후 Axis 장치는 HTTPS로만 구성되며, 웹 인터페이스는 비활성화됩니다. 매개변수를 제거하거나 추가하는 등 필요에 따라 구성 파일의 수정이 가능합니다.

보안 알림

*Axis security notification service*를 구독하여 Axis 제품, 솔루션 및 서비스에서 새로 발견된 취약성 관련 정보와 Axis 장치를 안전하게 보호하는 방법을 받아보는 것이 좋습니다.

T10177717_ko

2026-03 (M64.2)