

AXIS OS Hardening Guide

AXIS OS Hardening Guide

AXIS OS Portal | AXIS OS 릴리스 정보 | AXIS OS Knowledge 기반 | AXIS OS 보안 권고

AXIS OS Hardening Guide

소개

소개



AXIS OS Hardening Guide for Axis edge devices

Axis Communications는 장치의 설계, 개발, 테스트에 사이버 보안 모범 사례를 적용하여 해커가 공격에 악용할 수 있는 결함의 위험을 최소화하는 데 최선을 다하고 있습니다. 하지만 공급업체들의 전체 공급망과 최종 사용자 조직이 네트워크, 해당 장치 및 네트워크에서 지원하는 서비스 보안에 동참해야 합니다. 보안 환경은 사용자, 프로세스 및 기술에 따라 달라집니다. 이 가이드의 목적은 네트워크, 장치 및 서비스를 안전하게 유지하도록 지원하는 것입니다.

Axis 장치에 대한 가장 명백한 위협은 물리적 파괴, 기물 파손 및 템퍼링입니다. 이러한 위협으로부터 제품을 보호하려면 파손 방지 모델 또는 케이스를 선택하고, 권장 방식으로 장착하고, 케이블을 보호하는 것이 중요합니다.

Axis 장치는 컴퓨터나 휴대 전화와 마찬가지로 네트워크의 엔드포인트입니다. 이 가운데 상당수는 연결된 시스템에 취약점을 노출할 수 있는 웹 인터페이스를 보유하고 있습니다. 이 가이드에서는 이러한 위협을 완화하는 방안을 설명합니다.

이 가이드는 Axis 솔루션 배포와 관련 있는 모든 사람에게 기술적인 조언을 합니다. 여기에는 권장 기본 구성과 진화하는 위협 환경을 고려한 강화 가이드가 포함되어 있습니다. 특정한 설정을 구성하는 방법을 알아보기 위해 제품 사용자 설명서를 참조해야 할 수도 있습니다. Axis 장치는 AXIS OS 7.10 및 10.9에서 웹 인터페이스 업데이트를 받았으며, 이로 인해 구성 경로가 바뀌었습니다.

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	Settings > System > Security(설정 > 시스템 > 보안)
≥ 10.9	System > Security(시스템 > 보안)

영역

본 가이드는 4.xx 및 5.xx를 실행하는 레거시 제품만이 아니라 AXIS OS(LTS 또는 활성 트랙)를 실행하는 모든 AXIS OS 기반 제품에 적용됩니다.







The operating system for Axis edge devices.

AXIS OS Security Architecture

AXIS OS Security Architecture 다이어그램은 보안 기반, 실리콘 지원 보안, AXIS OS 운영 체제, 애플리케이션 및 접근 제어 레이어에 대한 포괄적인 보기를 제공하는 다양한 계층의 AXIS OS 사이버 보안 기능을 간략히 설명합니다.

AXIS OS Hardening Guide

소개

 <p>Access control</p>	<p>Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as Password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality</p>	<p>Privacy Use of diagnostics data Minimalistic approach to how much customer-specific should be stored</p>											
 <p>Application</p>	<p>Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog</p>												
 <p>Operating system</p>	<p>Encryption and data protection</p> <table border="0"> <tr> <td>OpenSSL 1.1.1 and 3.0</td> <td>1 0 1 0</td> </tr> <tr> <td>X.509 certificate PKI and cryptography</td> <td>0 1 0 1</td> </tr> <tr> <td>Transport layer security (TLS 1.2/TLS 1.3)</td> <td>1 0 1 0</td> </tr> <tr> <td>SD card encryption (AES-XTS-Plain64 256bit)</td> <td></td> </tr> <tr> <td>Encrypted file system (AES-XTS-Plain64 256bit), Signed video</td> <td></td> </tr> </table>	OpenSSL 1.1.1 and 3.0	1 0 1 0	X.509 certificate PKI and cryptography	0 1 0 1	Transport layer security (TLS 1.2/TLS 1.3)	1 0 1 0	SD card encryption (AES-XTS-Plain64 256bit)		Encrypted file system (AES-XTS-Plain64 256bit), Signed video		<p>Default security HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled</p>	<p>Enterprise network security IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec)</p>
OpenSSL 1.1.1 and 3.0	1 0 1 0												
X.509 certificate PKI and cryptography	0 1 0 1												
Transport layer security (TLS 1.2/TLS 1.3)	1 0 1 0												
SD card encryption (AES-XTS-Plain64 256bit)													
Encrypted file system (AES-XTS-Plain64 256bit), Signed video													
<p>AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-Year Long-Term Support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.</p>													
 <p>Silicon assisted security (chip)</p>	<p>Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element</p>	<p>Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.</p>											
<p>Security foundation</p> <table border="0"> <tr> <td data-bbox="459 833 778 931"> <p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p> </td> <td data-bbox="778 833 1107 931"> <p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p> </td> <td data-bbox="1107 833 1449 931"> <p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p> </td> </tr> </table>			<p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p>	<p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p>	<p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p>								
<p>Secure software development Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)</p>	<p>Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645</p>	<p>Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)</p>											

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

보안 알림

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

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. ciscsecurity.org의 18 CIS Critical Security Controls에서 CSC 범주에 대한 세부 정보를 참고하십시오.

AXIS OS Hardening Guide

기본 보호

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.

기본으로 비활성화

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

Axis 장치는 관리자 패스워드를 설정할 때까지 작동하지 않습니다.

AXIS OS Knowledge 기반의 장치 액세스에서 장치 액세스를 구성하는 방법을 알아보십시오.

자격 증명 액세스

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.

네트워크 프로토콜

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

Axis 장치에서는 기본적으로 최소한의 네트워크 프로토콜 및 서비스만 활성화됩니다. 이 표에서 어떤 항목이 있는지 확인할 수 있습니다.

프로토콜	포트	전송	설명
HTTP	80	TCP	웹 인터페이스 액세스, VAPIX 및 ONVIF API 인터페이스와 같은 일반 HTTP 트래픽 또는 에지 투 에지 통신*
HTTPS	443	TCP	웹 인터페이스 액세스, VAPIX 및 ONVIF API 인터페이스와 같은 일반 HTTPS 트래픽 또는 에지 투 에지 통신*
RTSP	554	UDP	Axis 장치에서 비디오/오디오 스트리밍을 위해 사용됨
RTP	임시 포트 범위*	UDP	Axis 장치에서 비디오/오디오 스트리밍을 위해 사용됨
UPnP	49152	TCP	타사 애플리케이션에서 UPnP 검색 프로토콜을 통해 Axis 장치를 검색하는 데 사용됨
Bonjour	5353	UDP	타사 애플리케이션에서 mDNS 검색 프로토콜 (Bonjour)을 통해 Axis 장치를 검색하는 데 사용됨

AXIS OS Hardening Guide

기본 보호

프로토콜	포트	전송	설명
SSDP	1900	UDP	타사 애플리케이션에서 SSDP(UPnP)를 통해 Axis 장치를 검색하는 데 사용됨
WS-Discovery	3702	UDP	타사 애플리케이션에서 WS-Discovery 프로토콜 (ONVIF)을 통해 Axis 장치를 검색하는 데 사용됨

* *에지 투 에지* 기술 백서에서 에지 투 에지의 세부 정보를 참고하십시오.

* *RFC 6056에 따라 사전 정의된 포트 번호 범위 안에서 자동 할당됩니다.* Wikipedia 문서 *Ephemeral port*에서 자세한 내용을 살펴보십시오.

사용하지 않는 네트워크 프로토콜과 서비스는 가급적 비활성화하는 것이 좋습니다. AXIS OS Knowledge 기반의 일반적으로 사용되는 네트워크 포트에서 기본적으로 사용되거나 구성에 따라 사용 가능한 서비스의 전체 목록을 살펴보십시오.

예를 들면, 네트워크 카메라 등의 Axis 영상 감시 제품에서는 오디오 입/출력 및 마이크 기능을 수동으로 활성화해야 하지만, Axis 인터콤 및 네트워크 스피커에서는 오디오 입/출력 및 마이크 기능이 필수적이므로 기본적으로 활성화되어 있습니다.

UART/디버그 인터페이스

CS# 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 장치의 광범위한 해체를 통해서만 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.

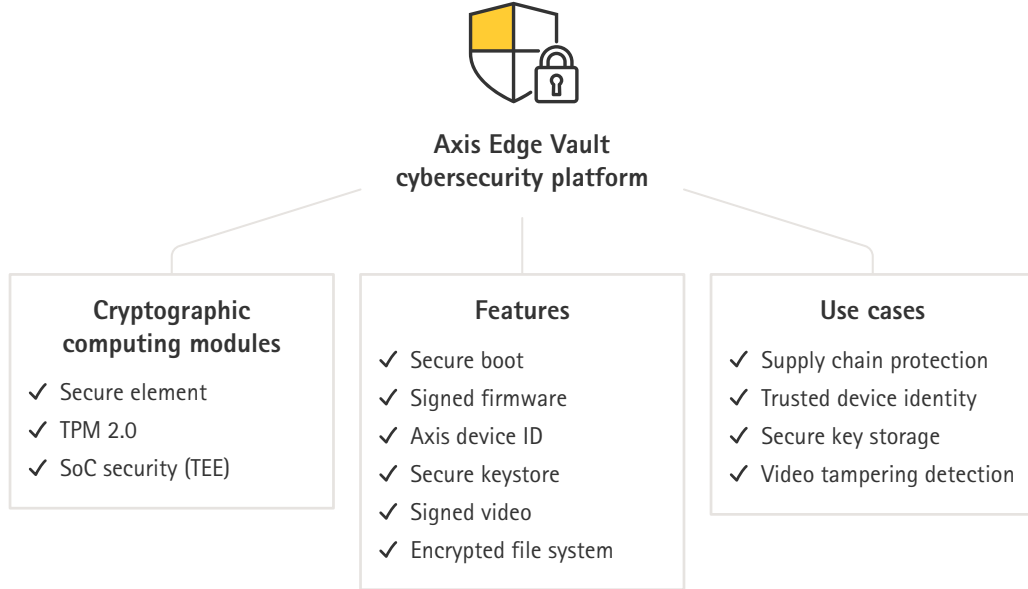
Axis Edge Vault

Axis Edge Vault는 Axis 장치를 보호하는 하드웨어 기반의 사이버 보안 플랫폼을 제공합니다. 이는 암호화 컴퓨팅 모듈(보안 요소 및 TPM) 및 SoC 보안(TEE 및 Secure Boot)의 강력한 기반을 에지 장치 보안에 대한 전문 지식과 결합하여 사용됩니다. Axis Edge Vault는 Secure boot 및 Signed firmware를 통해 구축된 강력한 신뢰 root를 기반으로 합니다. 이러한 기능을 통해 모든 보안 작업이 의존하는 신뢰 체인에 대해 암호학적으로 검증된 소프트웨어의 중단 없는 체인이 가능합니다.

Axis Edge Vault가 적용된 Axis 장치는 민감한 정보의 도청 및 악의적인 추출을 방지하여 고객이 사이버 보안 위협에 노출되는 것을 최소화합니다. 또한 Axis Edge Vault는 Axis 장치가 고객 네트워크 내에서 신뢰할 수 있고 믿을 수 있는 장치임을 보장합니다.

AXIS OS Hardening Guide

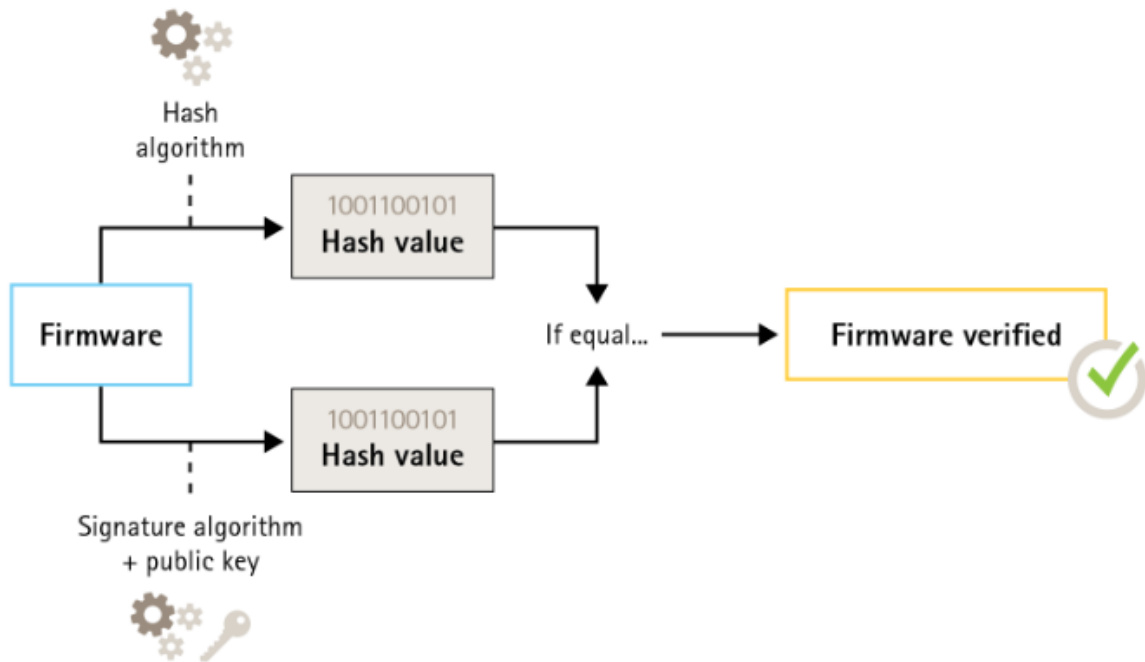
기본 보호



Signed firmware

CSC #2: 소프트웨어 자산의 재고 및 제어

AXIS OS는 버전 9.20.1에서 서명되었습니다. 장치에서 AXIS OS 버전을 업그레이드할 때마다, 장치가 암호화 서명 확인을 통해 업데이트 파일의 무결성을 확인하고 변조된 파일은 거부합니다. 이렇게 하면 공격자가 손상된 파일을 설치하도록 사용자를 유인하는 것을 방지합니다.



AXIS OS Hardening Guide

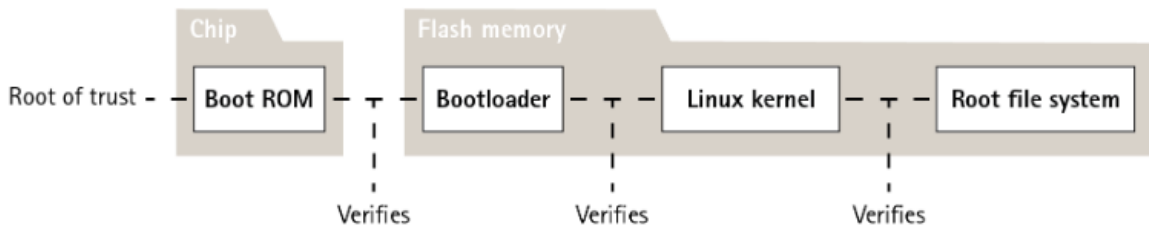
기본 보호

Axis Edge Vault 백서에서 자세한 내용을 알아보십시오.

Secure Boot

CSC #2: 소프트웨어 자산의 재고 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 백서에서 자세한 내용을 알아보십시오.

보안 키 저장소

CSC #6: 접근 제어 관리

보안 키 저장소는 암호화 정보에 대한 하드웨어 기반의 변조 방지 스토리지를 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 백서에서 자세한 내용을 알아보십시오.

암호화된 파일 시스템

CSC #3: 데이터 보호

악의적인 공격자는 플래시 메모리를 마운트 해제하고 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. 보안 부팅 프로세스 중에 읽기-쓰기 파일 시스템은 암호가 해독되며 Axis 장치에서 마운트 및 사용할 수 있습니다.

AXIS OS Hardening Guide

기본 보호

Axis Edge Vault 백서에서 자세한 내용을 알아보십시오.

HTTPS 활성화

CSC #3: 데이터 보호

AXIS OS 7.20부터는 자체 서명 인증서로 장치 패스워드를 안전하게 설정할 수 있는 HTTPS가 기본으로 활성화되었습니다. AXIS OS 10.10부터 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	Settings > System > Security > HTTP and HTTPS(설정 > 시스템 > 보안 > HTTP 또는 HTTPS)
≥ 10.9	System > Network > HTTP and HTTPS(시스템 > 네트워크 > HTTP 또는 HTTPS)

기본 HTTP(S) 헤더

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 9.80부터는 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.

AXIS OS Knowledge 기반의 *기본 HTTP(S) 헤더*에서 기본 HTTP(S) 헤더에 대해 자세히 알아보십시오.

다이제스트 인증

CSC #3: 데이터 보호

장치에 액세스하는 클라이언트는 패스워드를 사용하여 인증되며, 이 패스워드는 네트워크를 통해 전송될 때 암호화됩니다. 따라서 기본 인증 대신 다이제스트 인증만 사용하거나 기본 및 다이제스트 인증을 모두 사용하는 것이 좋습니다. 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	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 보

AXIS OS Hardening Guide

기본 보호

호하는 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	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.

AXIS OS 11.5부터 무차별 대입 지연 보호가 기본적으로 활성화됩니다. AXIS OS Knowledge 기반의 무차별 대입 지연 보호에서 자세한 구성 예와 권장 사항을 알아보십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 사항 없음
≥ 7.10	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)

폐기

CSC #3: 데이터 보호

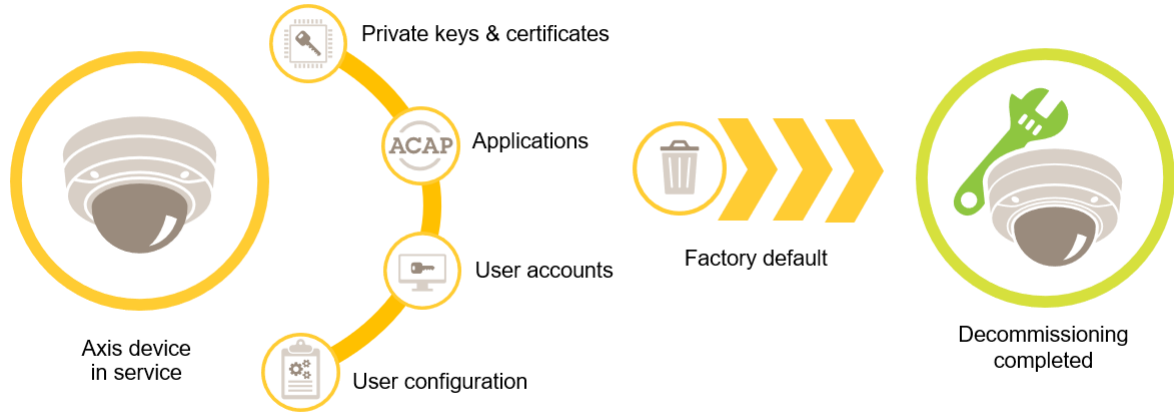
Axis 장치는 휘발성 메모리와 비휘발성 메모리를 모두 사용하며, 휘발성 메모리는 전원에서 장치를 분리할 때마다 지워지지만, 비휘발성 메모리에 저장된 정보는 남아 있다가 시작 시 다시 사용할 수 있습니다. 파일 시스템에서 저장된 데이터가 보이지 않게 하려고 단순히 데이터 포인터를 제거하는 일반적인 관행을 피하기 위해 공장 초기화가 필요합니다. NAND 플래시 메모리의 경우 UBI 기능인 볼륨 제거가 사용되며, eMMC 플래시 메모리에는 저장 블록이 더 이상 사용되지 않는다는 신호를 전달하는 같은 기능이 사용됩니다. 그러면 저장 공간 컨트롤러가 그에 따라 해당 저장 공간 블록을 지웁니다.

Axis 장치를 폐기할 때는 장치를 공장 출하 시 기본값으로 초기화하여 장치의 비휘발성 메모리에 저장된 모든 데이터를 지우는 것을 권장합니다.

공장 출하 시 기본값 명령을 실행해도 데이터가 즉시 삭제되는 것이 아니라 장치가 재부팅되고 시스템 부팅 중에 데이터 삭제가 이루어집니다. 따라서 단순히 공장 출하 시 기본값 명령을 실행하는 것만으로는 충분하지 않으며, 데이터 삭제가 완료되었는지 확인하려면 전원을 끄기 전에 장치를 재부팅하고 부팅을 완료해야 합니다.

AXIS OS Hardening Guide

기본 보호



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

이 표에는 비휘발성 메모리에 저장된 데이터의 세부 정보가 포함되어 있습니다.

정보 및 데이터	공장 출하 시 기본 설정 복원 후 지워짐
VAPIX 및 ONVIF 사용자 이름과 비밀번호	있음
인증서 및 개인 키	있음
자체 서명 인증서	있음
TPM 및 Axis Edge Vault에 저장된 정보	있음
WLAN 설정 및 사용자/패스워드	있음
사용자 정의 인증서*	없음
SD 카드 암호화 키	있음
SD 카드 데이터**	없음
네트워크 공유 설정 및 사용자/패스워드	있음
네트워크 공유 데이터**	없음
사용자 구성***	있음
업로드된 애플리케이션(ACAP)****	있음
생산 데이터 및 수명 통계*****	없음

AXIS OS Hardening Guide

기본 보호

업로드된 그래픽 및 오버레이	있음
RTC 시계 데이터	있음

* Signed firmware 프로세스는 사용자가 (무엇보다) AXIS OS를 업로드 할 수 있는 사용자 정의 인증서를 사용합니다.

** 에지 스토리지(SD 카드, 네트워크 공유)에 저장된 녹화 및 이미지는 사용자가 별도로 삭제해야 합니다. AXIS OS Knowledge 기반의 Axis SD 카드 포맷에서 자세한 내용을 알아보십시오.

*** 계정 생성에서 네트워크, O3C, 이벤트, 이미지, PTZ 및 시스템 구성에 이르기까지 모든 사용자가 만든 구성입니다.

**** 장치는 사전 설치한 모든 애플리케이션을 유지하지만, 모든 사용자가 만든 구성을 삭제합니다.

***** 생산 데이터(보정, 802.1AR 생산 인증서) 및 수명 통계에는 민감하지 않으며, 사용자와 관련이 없는 정보가 포함됩니다.

AXIS OS Hardening Guide

기본 강화

기본 강화

기본 강화는 Axis 장치에 권장되는 최소한의 보호 수준입니다. 기본 강화의 주제는 "에지에서 구성 가능"입니다. 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. [페이지 10](#)에서 자세한 내용을 알아보십시오.

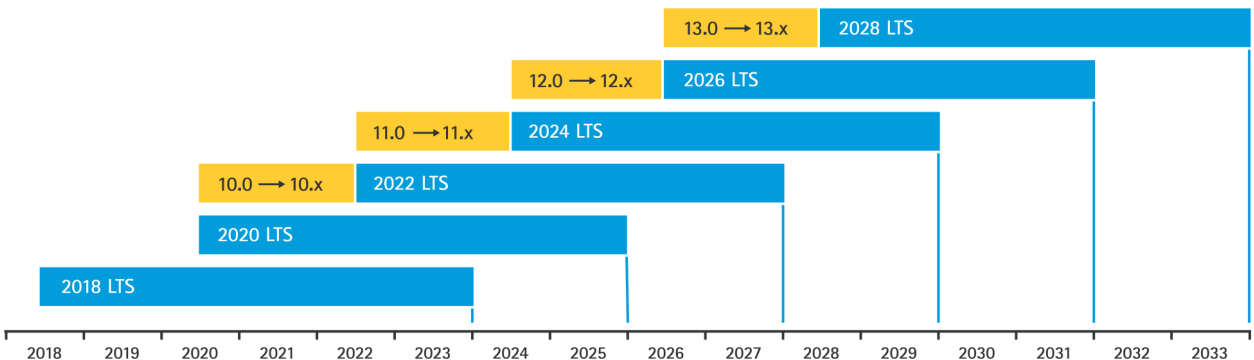
AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > System Options > Maintenance > Default(설정 > 시스템 옵션 > 유지 보수 > 기본 설정)
≥ 7.10	Settings > System > Maintenance > Default(설정 > 시스템 > 유지 보수 > 기본 설정)
≥ 10.9	Maintenance > Default(유지 보수 > 기본 설정)

최신 AXIS OS로 업그레이드

CSC #2: 소프트웨어 자산의 재고 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 취약성에 대한 보안 패치가 포함될 수 있으므로 항상 최신 AXIS OS를 사용하십시오. 특정 버전에 대한 릴리스 정보에는 중요 보안 수정 사항이 명시적으로 언급될 수 있지만, 모든 일반 수정 사항에 적용되는 것은 아닙니다.

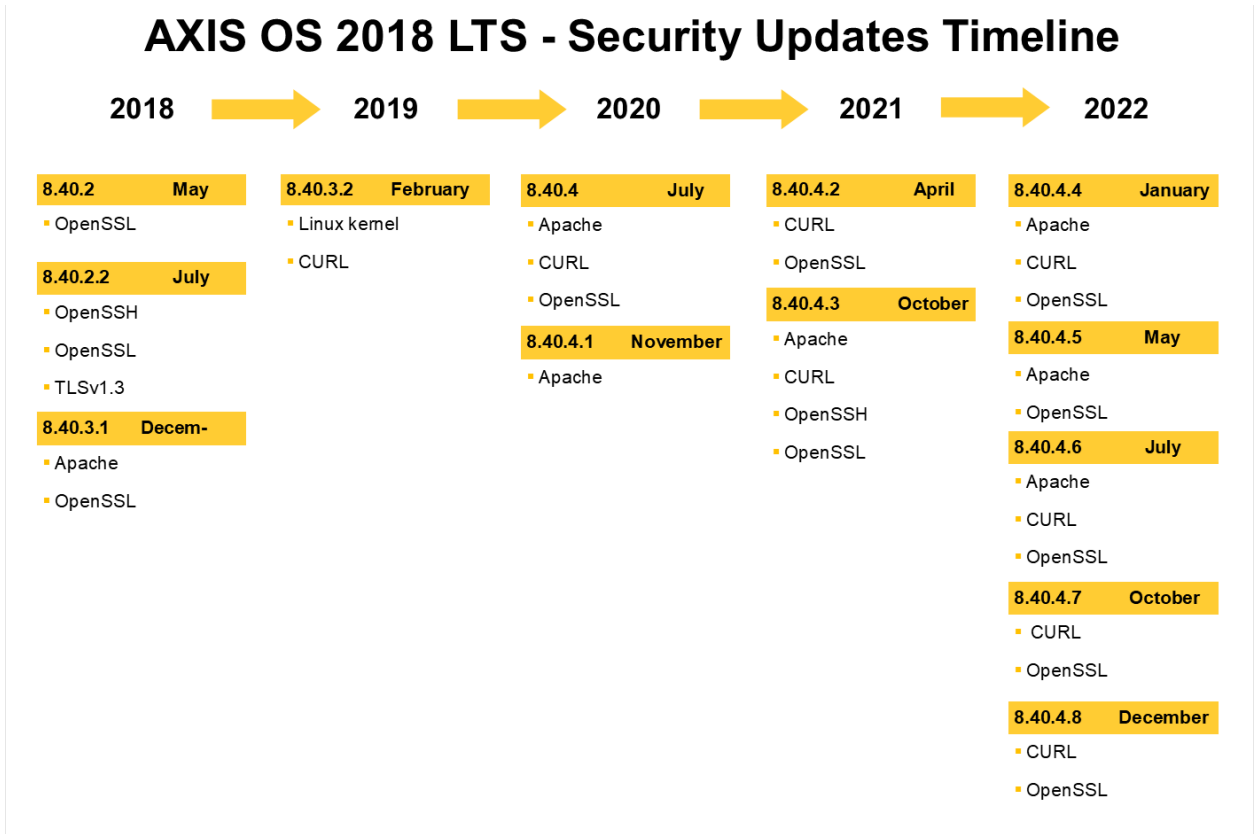
Axis는 두 가지 유형의 AXIS OS 트랙을 유지합니다. 바로 활성 트랙 및 장기 지원(LTS) 트랙입니다. 두 가지 유형 모두 최신의 중요한 취약성 패치를 포함하고 있지만, 호환성 문제의 위험을 최소화하는 것이 목적이기 때문에 LTS 트랙에는 새로운 기능이 포함되어 있지 않습니다. AXIS OS 정보의 [AXIS OS 수명 주기](#)에서 자세한 내용을 살펴보세요.



Axis는 중요한 새로운 기능, 버그 수정 및 보안 패치에 대한 정보와 함께 향후 출시에 대한 예측을 제공합니다. AXIS OS 정보의 [향후 출시](#)에서 자세한 내용을 알아보십시오. 장치에 맞는 AXIS OS를 다운로드하려면 [axis.com](#)의 [편위어](#)를 방문하십시오.

이 차트는 Axis 장치를 최신 상태로 유지하는 것의 중요성을 나타냅니다.

기본 강화



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

장치 root 패스워드 설정

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

장치 root 계정은 기본 장치 관리 계정입니다. root 계정을 사용하려면 먼저 장치 패스워드를 설정해야 합니다. 강력한 패스워드를 사용하고, root 계정의 사용을 관리 작업으로만 제한해야 합니다. 일상적인 생산 환경에서는 root 계정을 사용하지 않는 것이 좋습니다.

Axis 장치를 가동할 때 동일한 패스워드를 사용하면 관리가 간편해지지만, 침입 및 데이터 유출에 대한 취약성이 커집니다. 각 Axis 장치마다 고유한 패스워드를 사용하면 보안이 강화되지만 장치 관리는 더 복잡해집니다. 장치의 패스워드를 정기적으로 변경하시기 바랍니다.

AXIS OS Hardening Guide

기본 강화

NIST 패스워드 권장 사항과 같이 새 패스워드가 충분히 길고 복잡해야 한다는 지침을 적용하는 것이 좋습니다. Axis 장치는 최대 64자의 패스워드를 지원합니다. **8자 미만**의 패스워드는 취약한 것으로 간주됩니다.

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

전용 계정 생성

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

기본 root 계정이 전체 권한을 가지고 있으며 관리 작업용으로 예약되어야 합니다. 일상적인 작업을 위해 제한된 권한을 가진 클라이언트 사용자 계정을 생성하는 것이 좋습니다. 이렇게 하면 장치 관리자 패스워드가 손상될 위험이 줄어듭니다.

영상 보안 감시 시스템의 ID 및 액세스 관리백서에서 자세한 내용을 알아보십시오.

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

웹 인터페이스 액세스 제한

CSC #5: 계정 관리

Axis 장치에는 사용자가 표준 웹 브라우저를 통해 장치에 액세스할 수 있는 웹 서버가 있습니다. 웹 인터페이스는 구성, 유지 보수 및 문제 해결을 위한 것입니다. 영상을 보기 위한 클라이언트 등 일상적인 작업에는 적합하지 않습니다.

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. [웹 인터페이스 액세스 비활성화 페이지 15](#)에서 자세한 내용을 알아보십시오.

웹 인터페이스 액세스 비활성화

CSC #4: 엔터프라이즈 자산 및 소프트웨어의 안전한 구성

AXIS OS 9.50부터는 Axis 장치의 웹 인터페이스를 비활성화해도 됩니다. 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 Hardening Guide

기본 강화

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 사항 없음
≥ 7.10	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)

네트워크 설정 구성

CSC #12: 네트워크 인프라 관리

장치 IP 구성은 IPv4/IPv6, 정적 또는 동적(DHCP) 네트워크 주소, 서브넷 마스크 및 기본 라우터와 같은 네트워크 구성에 따라 달라집니다. 새로운 유형의 구성 요소를 추가할 때마다 네트워크 토폴로지를 검토하길 권장합니다.

또한 네트워크 연결 가능성을 보장하고 공격 대상이 될 수 있는 네트워크 내 서버(예: DHCP 서버)에 대한 종속성을 없애기 위해 Axis 장치에 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	Settings > System > TCP/IP(시스템 > 설정 > TCP/IP)
≥ 10.9	System > Network(시스템 > 네트워크)

날짜 및 시간 설정 구성

CSC #8: 감사 로그 관리

보안 관점에서 보면 정확한 날짜와 시간을 설정하는 것이 중요합니다. 예를 들어, 시스템 로그에 정확한 타임스탬프가 표시되고 실행 시간 중에 디지털 인증서의 유효성을 검사 및 사용할 수 있습니다. 시간이 적절하게 동기화되지 않으면 HTTPS, IEEE 및 802.1x 같은 디지털 인증서를 사용하는 서비스가 제대로 작동하지 않을 수 있습니다.

Axis 장치 시간은 NTP(Network Time Protocol, 암호화되지 않음) 서버 또는 가급적이면 NTS(Network Time Security, 암호화된) 서버와 동기화하기를 권장합니다. AXIS OS 11.1에는 NTP(Network Time Protocol), 암호화 및 보안 변형인 NTS(Network Time Security)가 추가되었습니다. 시간 동기화의 정확도를 높이기 위해 여러 시간 서버를 구성하는 것이 좋지만, 구성된 시간 서버 중 하나를 사용할 수 없는 페일오버 시나리오도 고려하는 것이 좋습니다.

공용 NTP 또는 NTS 서버를 사용하는 것은 로컬 시간 서버 인스턴스 자체를 용이하게 할 수 없는 개인 및 소규모 조직의 대안이 될 수 있습니다. AXIS OS Knowledge 기반의 NTP 및 NTS에서 Axis 장치의 NTP/NTS에 대해 자세히 알아보십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	Setup > Basic Setup > Date & Time(설정 > 기본 설정 > 날짜 및 시간)
≥ 7.10	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)

에지 스토리지 암호화

CSC #3: 데이터 보호

AXIS OS Hardening Guide

기본 강화

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 영상을 재생할 수 없습니다.

AXIS OS Knowledge 기반의 *SD 카드 지원*에서 Axis 장치의 SD 카드 암호화에 대해 자세히 알아보십시오.

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

네트워크 공유(NAS)

녹화 장치로 네트워크 연결 스토리지(NAS)를 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 OS Knowledge 기반의 *네트워크 공유*에서 Axis 장치를 네트워크 공유에 연결할 때 올바른 SMB 구성에 대해 자세히 알아보십시오.

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

녹화물 암호화 내보내기

CSC #3: 데이터 보호

AXIS OS 10.10부터는 Axis 장치가 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 사항 없음
≥ 7.10	해당 사항 없음
≥ 10.9	녹화물

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 *본서*에서 Axis 애플리케이션에 대한 세부 정보를 참고하십시오.

AXIS OS Hardening Guide

기본 강화

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	Settings > Apps(설정 > 앱)
≥ 10.9	앱

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.

미사용 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 위협을 초래할 수 있습니다.

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

네트워크 검색 프로토콜

Bonjour, UPnP, ZeroConf 및 WS-Discovery와 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)*
	해당 사항 없음

AXIS OS Hardening Guide

기본 강화

AXIS OS 버전	웹 인터페이스 구성 경로
≥ 7.10	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)

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

오래된 TLS 버전

Axis 장치를 운영 체제로 전환하기 전에 이전 버전, 오래된 버전 및 안전하지 않은 TLS 버전을 비활성화하는 것이 좋습니다. 오래된 TLS 버전은 대개 기본적으로 비활성화되어 있지만, 아직 TLS 1.2 및 TLS 1.3을 구현하지 않은 타사 애플리케이션과의 역호환성을 허용하기 위해 Axis 장치에서 이를 활성화할 수 있습니다.

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	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	System > Plain config > HTTPS > Allow TLSv1.0 and/or Allow TLSv1.1(시스템 > 일반 구성 > HTTPS > TLSv1.0 허용 및/또는 TLSv1.1 허용)

스크립트 편집기 환경

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

스크립트 편집기는 AXIS OS 7.10에서 제거되었고, 이후 버전에서는 사용하지 못합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 사항 없음
≥ 7.10	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))

AXIS OS Hardening Guide

기본 강화

HTTP(S) 서버 헤더

기본적으로 Axis 장치는 네트워크에서 클라이언트와의 HTTP(S) 연결 중에 현재 Apache 및 OpenSSL 버전을 알립니다. 이 정보는 특정 AXIS OS 버전에서 발견된 취약점에 대한 상세 보고서를 생성하므로, 네트워크 보안 스캐너를 정기적으로 사용할 때 도움이 됩니다.

HTTP(S) 서버 헤더를 비활성화하여 HTTP(S) 연결 중 정보 노출을 감소시킬 수 있습니다. 하지만 권장 사항에 따라 장치를 작동하며 항상 최신 상태로 유지하는 경우에만 헤더를 비활성화하는 것이 좋습니다.

AXIS OS 10.6부터 HTTP(S) 서버 헤더를 비활성화하는 옵션을 사용할 수 있습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 사항 없음
≥ 7.10	Settings > System > Plain config > System > HTTP Server Header Comments(설정 > 시스템 > 일반 구성 > 시스템 > HTTP 서버 헤더 설명)
≥ 10.9	System > Plain config > System > HTTP Server Header Comments(시스템 > 일반 구성 > 시스템 > HTTP 서버 헤더 설명)

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	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 에지 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.

AXIS OS Knowledge 기반의 *SD 카드 비활성화*에서 자세한 내용을 알아보십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	해당 사항 없음
≥ 7.10	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)

AXIS OS Hardening Guide

기본 강화

FTP 액세스

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

AXIS OS Portal의 *SSH 액세스*에서 SSH에 대한 세부 정보를 참고하십시오. FTP를 사용한 디버깅 옵션에 대한 자세한 내용은 AXIS OS Portal의 *FTP 액세스*를 참고하십시오.

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	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)

SSH 액세스

SSH는 문제 해결 및 디버깅 목적으로만 사용되는 보안 통신 프로토콜입니다. AXIS OS 5.50부터 Axis 장치에서 지원됩니다. SSH 액세스는 비활성화하는 편이 좋습니다.

AXIS OS Knowledge 기반의 *SSH 액세스*에서 SSH를 사용한 디버깅 옵션에 대해 자세히 알아보십시오.

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	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)

텔넷 액세스

텔넷은 문제 해결 및 디버깅 목적으로만 사용되는 안전하지 않은 통신 프로토콜입니다. AXIS OS 5.50보다 이전 버전의 Axis 장치에서 지원됩니다. 텔넷 액세스는 비활성화하는 편이 좋습니다.

AXIS OS 버전	웹 인터페이스 구성 경로
5.50 미만	AXIS OS Knowledge 기반의 <i>장치 액세스</i> 에서 자세한 내용을 알아보십시오.
7.10 미만	해당 사항 없음
≥ 7.10	해당 사항 없음
≥ 10.9	해당 사항 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 Hardening Guide

기본 강화

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	해당 사항 없음
≥ 10.9	해당 사항 없음

IP 주소 필터

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

IP 주소 필터링은 권한이 없는 클라이언트가 Axis 장치에 접근하지 못하게 합니다. 권한이 부여된 네트워크 호스트의 IP 주소를 허용하거나 권한이 없는 네트워크 호스트의 IP 주소를 거부하도록 장치를 구성하는 것이 좋습니다.

IP 주소 허용을 선택한 경우, 목록에 권한이 부여된 모든 클라이언트(VMS 서버 및 관리 클라이언트)를 추가해야 합니다.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	설정 > 시스템 옵션 > 보안 > IP 주소 필터
≥ 7.10	설정 > 시스템 > TCP/IP > IP 주소 필터
≥ 10.9*	설정 > 보안 > IP 주소 필터

AXIS OS 11.9 이상인 버전에서는 IP 주소 필터가 새로운 호스트 기반 방화벽으로 대체되었습니다.

호스트 기반 방화벽

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

사용자는 방화벽을 통해 IP 주소 및/또는 TCP/UDP 포트 번호별로 장치에 유입되는 트래픽을 규제하는 규칙을 생성할 수 있습니다. 따라서 권한이 없는 클라이언트가 Axis 장치 또는 장치의 특정 서비스에 접근하는 것을 방지할 수 있습니다.

기본 정책을 "거부"로 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	설정 > 보안 > 방화벽

HTTPS

CSC #3: 데이터 보호

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

HTTPS [한정 페이지/23](#) 및 [HTTPS 암호 페이지/23](#)에서 구성 지침을 살펴보세요.

AXIS OS Hardening Guide

기본 강화

HTTPS 한정

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 장치에는 자체 서명 인증서가 함께 제공됩니다. 자체 서명 인증서는 설계상 신뢰할 수 없지만, 초기 구성 중이나 사용 가능한 공개 키 인프라(PKI)가 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	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. Axis 장치를 공장 출하 시 기본 설정 설정으로 초기화하면, Axis에서 제공하는 사용 가능한 최신 모범 사례 구성에 따라 암호 목록이 자동 업데이트될 수 있습니다.

참조 및 투명성을 위해 *TLS 1.2 이하 페이지/23* 및 *TLS 1.3 페이지/23*에 나열된 안전하고 강력한 암호 제품군을 사용하십시오.

TLS 1.2 이하

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 : DHE-RSA-AES128-GCM-SHA256 : DHE-RSA-AES256-GCM-SHA384

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	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.

액세스 로그

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

AXIS OS Hardening Guide

기본 강화

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

AXIS OS Knowledge 기반의 *장치 액세스 로깅*에서 자세한 내용을 알아보십시오.

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	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)

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 Door Switch A*

확장된 강화

확장된 강화

확장된 강화의 지침은 *기본 보호 페이지 5* 및 *기본 강화 페이지 13*에서 설명하는 강화 주제를 기반으로 합니다. 그러나 Axis 장치에는 기본 및 기본 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 노출 제한

CSC #12: *네트워크 인프라 관리*

Axis 장치를 공용 웹 서버로 노출하거나 알 수 없는 클라이언트에게 장치에 대한 네트워크 액세스 권한을 주는 것은 권장하지 않습니다. VMS를 운영하지 않거나 원격 위치에서 영상에 접근해야 하는 소규모 조직 및 개인의 경우, AXIS Companion의 사용을 추천합니다.

AXIS Companion은 Windows/iOS/Android 클라이언트 소프트웨어를 사용하고, 무료로 제공되며, 인터넷에 Axis 장치를 노출하지 않고도 영상에 안전하게 액세스할 수 있는 간편한 방법이 됩니다. axis.com/companion에서 AXIS Companion에 대한 세부 정보를 참고하십시오.

참고

VMS를 사용하는 모든 조직은 VMS 공급업체에 원격 영상 접근에 관한 모범 사례를 문의해야 합니다.

네트워크 노출 제한

CSC #12: *네트워크 인프라 관리*

네트워크 노출의 위험을 감소시키는 보편적인 방법은 네트워크 장치와 관련 인프라 및 애플리케이션을 물리적으로나 가상으로 격리하는 것입니다. 이러한 인프라와 애플리케이션의 사례로는 영상 관리 소프트웨어(VMS), 네트워크 비디오 레코더(NVR) 및 각종 보안 감시 장비를 들 수 있습니다.

운영 및 업무 네트워크에 연결되지 않은 로컬 네트워크에서 Axis 장치와 관련 인프라 및 애플리케이션을 격리하는 것이 좋습니다.

기본 강화를 적용하려면 네트워크 보안 메커니즘의 다중 계층을 추가하여 무단 액세스로부터 로컬 네트워크와 해당 인프라(라우터, 스위치)를 보호합니다. 이러한 메커니즘의 예로는 VLAN 세분화, 제한적인 라우팅 기능, 사이트 간 또는 WAN 접근용 가상 사설망(VPN), 네트워크 계층 2/3 방화벽, 접근 제어 목록(ACL) 등이 있습니다.

기본 강화 기능을 확장하려면 심층 패킷 검사 및 침입 탐지와 같은 고급 네트워크 검사 기술을 활용하는 것이 좋습니다. 이렇게 하면 네트워크 내에서 일관성 있고 포괄적인 위협 보호 기능까지 추가됩니다. 확장된 네트워크 강화에는 전용 소프트웨어 및/또는 하드웨어 어플라이언스가 필요합니다.

네트워크 취약성 스캐닝

CSC #1: *엔터프라이즈 자산의 재고 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. 스캔 시작 전에, Axis 장치가 LTS 또는 활성 트랙에서 사용 가능한 최신 AXIS OS 버전으로 업데이트되었는지 확인합니다.

또한 스캔 보고서를 검토하여 Axis 장치에서 알려진 오답지를 필터링하는 것이 좋으며, 이는 *AXIS OS 취약성 스캐너 가이드*에서 확인할 수 있습니다. 웹포데스크 티켓에 보고서와 추가 의견을 담아 axis.com의 *Axis 지원팀*에 제출합니다.

AXIS OS Hardening Guide

확장된 강화

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 HTTPS를 통해 연결할 때 브라우저 인증서 경고를 제거하는 데 도움이 됩니다. CA 서명 인증서는 또한 네트워크 접근 제어(NAC) 솔루션의 배포 시 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.

IEEE 802.1X 네트워크 접근 제어

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	Settings > System > Security > IEEE 802.1X(설정 > 시스템 > 보안 > IEEE 802.1X)
≥ 10.9	System > Security > IEEE 802.1X(시스템 > 보안 > IEEE 802.1X)

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.

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 Vault를 갖춘 Axis 장치는 네트워크 표준 IEEE 802.1AR을 지원합니다. 이렇게 하면 생산 과정에서 장치에 설치된 고유 인증서인 Axis device ID를 통해 네트워크에 Axis 장치를 안전하게 자동으로 온보딩할 수 있습니다. *Aruba 네트워크에 Axis 장치를 안전하게 통합*에서 보안 장치 온보딩의 예를 살펴보십시오.

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

AXIS OS Hardening Guide

확장된 강화

SNMP 모니터링

CSC #8: 감사 로그 관리

Axis 장치는 다음 SNMP 프로토콜을 지원합니다.

- SNMP v1: 레거시 용도로만 지원되므로, 사용하지 마십시오.
- SNMP v2c: 보호되는 네트워크 세그먼트에서 사용할 수 있습니다.
- SNMP v3: 모니터링 목적으로 권장됩니다.

Axis 장치는 모니터링 MIB-II 및 AXIS Video MIB도 지원합니다. AXIS Video MIB를 다운로드하려면 AXIS OS Knowledge 기반의 *AXIS Video MIB*을 참고하십시오.

AXIS OS에서 SNMP를 구성하는 방법을 자세히 알아보려면 AXIS OS Knowledge 기반의 *SNMP(Simple Network Management Protocol)*를 참고하십시오.

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

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 방법을 알아보려면 AXIS OS Knowledge 기반의 *Syslog*를 참고하십시오.

AXIS OS 버전	웹 인터페이스 구성 경로
7.10 미만	AXIS OS Portal의 <i>Syslog</i> 에서 자세한 내용을 알아보십시오.
≥ 7.10	Settings > System > TCP/IP(시스템 > 설정 > TCP/IP)
≥ 10.9	System > Logs(시스템 > 로그)

보안 비디오 스트리밍(SRTP/RTSPS)

CSC #3: 데이터 보호

Axis 장치는 AXIS OS 7.40부터 SRTP/RTSPS라고도 부르는 RTP를 통해 보안 비디오 스트리밍을 지원합니다. SRTP/RTSPS는 안전한 엔드 투 엔드 암호화 전송 방식으로 승인을 받은 클라이언트만 Axis 장치에서 비디오 스트림을 수신할 수 있게 합니다. 영상 관리 시스템(VMS)에서 SRTP/RTSPS를 지원한다면 이를 활성화하는 것을 권장합니다. 가능한 경우 암호화되지 않은 RTP 비디오 스트리밍 대신 SRTP를 사용하십시오.

참고

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

AXIS OS Hardening Guide

확장된 강화

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	Settings > System > Plain config > Network > RTSPS(설정 > 시스템 > 일반 구성 > 네트워크 > RTSPS)
≥ 10.9	System > Plain config > Network > RTSPS(시스템 > 일반 구성 > 네트워크 > RTSPS)

서명 비디오

CSC #3: 데이터 보호

AXIS OS 10.11부터 Axis Edge Vault가 탑재된 Axis 장치는 서명 비디오를 지원합니다. 서명 비디오를 사용하면, Axis 장치는 비디오 스트림에 서명을 추가하여 영상이 손상되지 않았는지 확인하고, 해당 영상을 생성한 장치로 역추적하여 원본을 확인합니다. 영상 관리 시스템(VMS) 또는 증거 관리 시스템(EMS)도 Axis 장치에서 제공하는 영상의 진위 여부를 확인할 수 있습니다.

Axis Edge Vault 백서에서 자세한 내용을 알아보십시오. 서명된 비디오 인증을 확인하는 데 사용되는 Axis 루트 인증서를 찾으려면 AXIS OS Knowledge 기반의 *장치 액세스*를 참고하십시오.

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

AXIS OS Hardening Guide

빠른 시작 가이드

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 강화 페이지/13](#)에서는 살펴볼 수 있는 강화 주제를 다루지만, [확장된 강화 페이지/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

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. [인터넷 노출 제한 페이지/25](#)에서 자세한 내용을 알아보십시오.

일반 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. [장치/root 패스워드 설정 페이지/14](#) 및 [전용 계정 생성 페이지/15](#)에서 지침을 살펴보십시오.

익명 접근

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. [자격 증명 액세스 페이지/5](#)에서 자세한 내용을 알아보십시오.

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. [HTTPS 활성화 페이지/9](#)에서 자세한 내용을 알아보십시오. [다이제스트 인증 페이지/9](#)에서 구성 권장 사항을 참고하십시오.

오래된 AXIS OS 버전

CSC #2: [소프트웨어 자산의 재고 및 제어](#)

LTS 또는 활성 트랙에서 사용 가능한 최신 AXIS OS 버전으로 Axis 장치를 운영하는 것을 적극 권장합니다. 두 트랙 모두 최신 보안 패치와 버그 수정을 제공합니다. [최신 AXIS OS로 업그레이드 페이지/13](#)에서 자세한 내용을 알아보십시오.

VAPIX API를 통한 기본 강화

VAPIX API를 사용하여 [기본 강화 페이지/13](#)에서 다루는 주제에 따라 Axis 장치를 강화할 수 있습니다. 이 표에서 Axis 장치의 AXIS OS 버전과 상관없이 기본 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.

AXIS OS Hardening Guide

빠른 시작 가이드

목적	VAPIX API 호출
미사용 네트워크 포트의 POE 비활성화*	<code>http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabl=no</code>
미사용 네트워크 포트의 네트워크 트래픽 비활성화**	<code>http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }</code>
Bonjour 검색 프로토콜 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.Bonjour.Enabled=no</code>
UPnP 검색 프로토콜 비활성화	<code>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</code>
WebService 검색 프로토콜 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &WebService.DiscoveryMode.Discoverable=no</code>
O3C(One-Click Cloud Connection) 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &RemoteService.Enabled=no</code>
장치/SSH 유지 보수 액세스 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.SSH.Enabled=no</code>
장치/FTP 유지 보수 액세스 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.FTP.Enabled=no</code>
ARP-Ping IP 주소 구성 비활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &Network.ARPPingIPAddress.Enabled=no</code>
Zero-Conf IP 주소 구성 비활성화	<code>http://ip-address/axis-cgi/param.cgi?action=update &Network.ZeroConf.Enabled=no</code>
HTTPS만 활성화	<code>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</code>
TLS 1.2 및 TLS 1.3만 활성화	<code>https://ip-address/axis-cgi/param.cgi?action=update &HTTPS.AllowTLS1=no https://ip-address/axis-cgi/param.cgi?action=update &HTTPS.AllowTLS11=no</code>

AXIS OS Hardening Guide

빠른 시작 가이드

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:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
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 관찰자 및 PTZ 접근 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

AXIS OS Hardening Guide

빠른 시작 가이드

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 교체합니다. 예시: "port=1"은 포트 1을, "port=2"는 포트 2를 비활성화합니다.

** "1"을 "eth1.1"의 실제 포트 번호로 교체합니다. 예: "eth1.1"은 포트 1을, "eth1.2"는 포트 2를 비활성화합니다.

*** 1초 이내에 로그인 시도가 20회 실패하면 클라이언트 IP 주소가 10초간 차단됩니다. 페이지 간격 30초 이내에 실패한 요청이 있을 때마다 DoS 차단 기간이 10초 더 연장됩니다.

AXIS Device Manager를 통한 기본 강화(확장)

AXIS Device Manager 및 AXIS Device Manager Extend를 사용하여 *기본 강화 페이지/13*에서 다룬 주제에 따라 Axis 장치를 강화할 수 있습니다. 이 구성 파일을 사용하십시오. 이는 VAPIX API를 통한 *기본 강화 페이지/29*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.

참고

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

