

AXIS Device Manager

서론

감시 및 보안 분야에서 사이버 보안의 중요성이 계속 커지고 있습니다. 효과적인 사이버 보안을 위해서는 귀사가 선택하는 제품과 파트너부터 귀사와 파트너가 설정하는 요구사항에 이르기까지, 모든 수준에서 IP 네트워크를 적절히 보호할 수 있는 충분한 심층 방어를 보장해야 합니다.

이 가이드에서는 AXIS Device Manager를 사용하여 시스템을 강화하고 보안을 강화하는 방법을 설명합니다. 핵심적인 측면을 중심으로 권장 사항을 제시합니다.

장치 수명 주기 관리

Axis는 장치의 전체 수명 주기에 걸쳐 강력한 보안 기반을 구축하는 것이 얼마나 중요한지 잘 알고 있습니다. Axis는 사이버 보안을 매우 중요하게 생각하며, Axis의 제품과 솔루션이 잠재적인 위협으로부터 시스템을 강력하게 보호할 수 있도록 최선을 다하고 있습니다.

구현

Axis는 보안 부팅 메커니즘, 서명된 운영 체제, 암호화된 스토리지와 같은 보안 기능이 내장된 '보안 내재화(Secure-by-design)' 장치를 제공합니다. 또한, AXIS Device Manager는 설치자와 시스템 관리자가 처음부터 안전한 설정을 보장하며 장치를 보안에 맞게 구성하고 배포할 수 있도록 지원합니다.

활성 서비스

운영 단계에서 Axis는 취약점으로부터 시스템을 보호하기 위해 정기적인 장치 소프트웨어 업데이트와 보안 패치를 제공합니다. 또한 AXIS Device Manager는 원격 모니터링 및 유지보수를 지원하여 신속한 문제 해결과 다운타임 최소화를 가능하게 합니다. 뿐만 아니라, Axis가 제공하는 보안 강화 가이드는 특정 보안 요구사항을 충족하도록 장치를 구성하는 방법에 대한 권장 사항을 담고 있습니다.

폐기

장치를 폐기하거나 교체할 시점이 되면, AXIS Device Manager는 민감한 데이터를 삭제하고 장치를 공장 설정으로 복원하여 안전하게 폐기할 수 있도록 지원합니다. 이를 통해 장치에 기밀 정보가 남지 않도록 하여 사용자 데이터를 보호하고 무단 접근을 방지합니다.

AXIS Device Manager

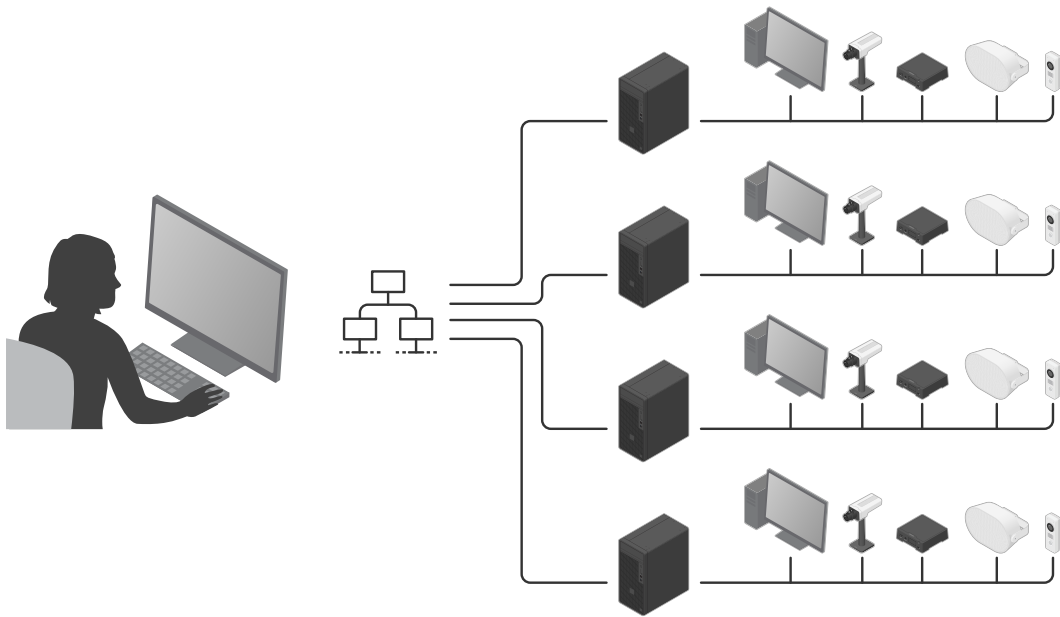
AXIS Device Manager는 모든 주요 설치, 보안 및 유지보수 작업을 간편하고 비용 효율적이며 사이버 보안을 유지하여 관리하는 방법을 제공하는 온프레미스 도구입니다(아래 표 참조). 이 도구는 단일 사이트에서 최대 2,000대의 Axis 장치를 관리하거나 여러 사이트에 분산된 수천 대의 장치를 관리하는 데 적합합니다. AXIS Device Manager를 사용하면 사이버 보안 제어를 효율적으로 배포하여 네트워크 장치를 보호하고 보안 인프라에 맞게 조정할 수 있습니다.

장치 관리 기능, AXIS Device Manager

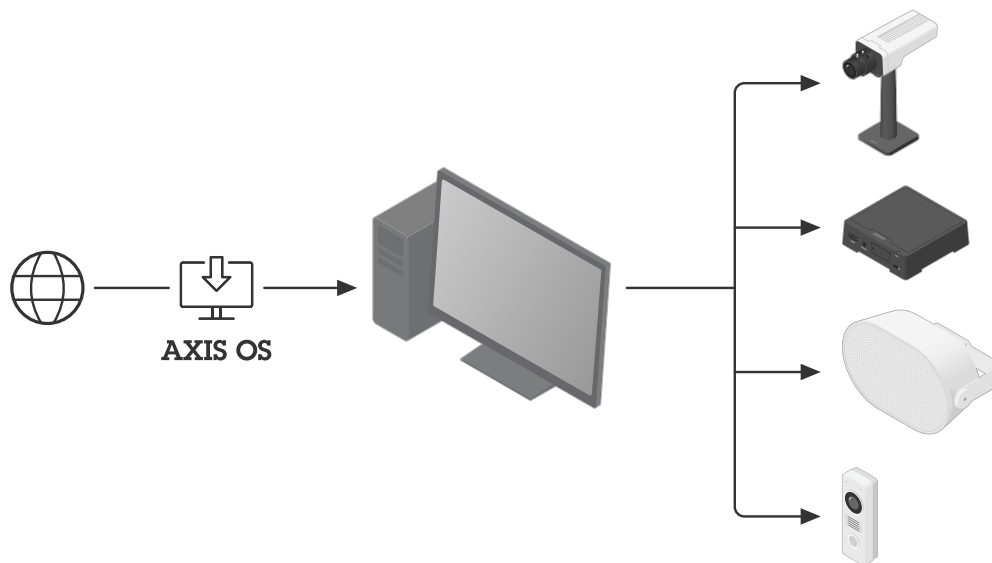
설치	유지보수
IP 주소 지정	장치 상태
장치 목록 내보내기 및 자산 추적*	장치 데이터 수집
사용자 및 비밀번호 관리*	장치 구성 및 구성을 다중 장치로 복사
ACAP 관리	다중 서버/시스템에 연결
LTS 또는 Active* 기반 AXIS OS 업그레이드	복원 지점
HTTPS 인증서 관리*	공장 초기화 설정 복원
IEEE 802.1 인증서 관리*/**	장치 교체
장치 태그 지정	인증서 갱신 및 관리*
	사이버 보안 강화*

* 사이버 보안 제어 기능을 나타냄.

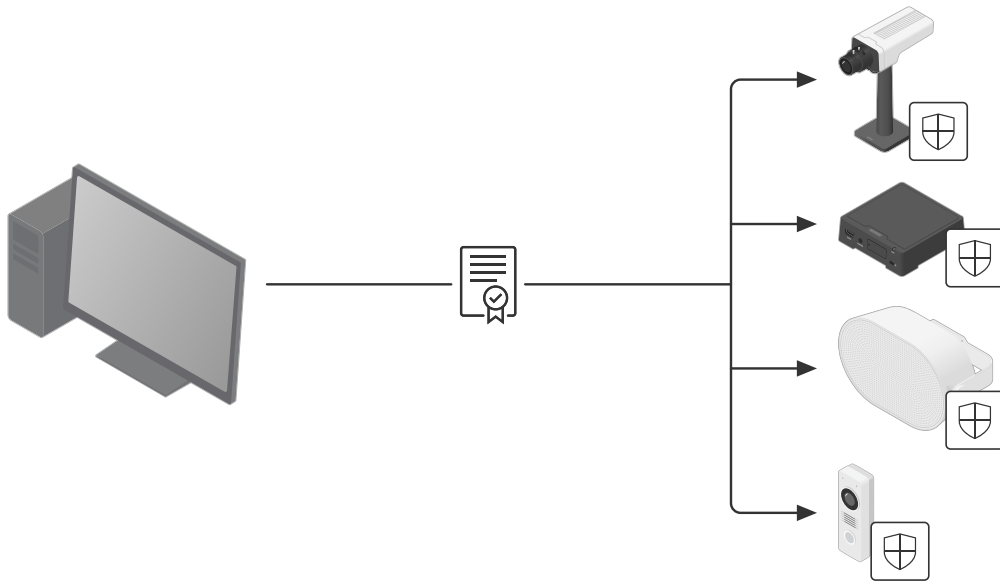
** 현재 Active Directory Certificate Services는 지원되지 않습니다. Linux에서 실행되는 FreeRADIUS에 대해 검증되었습니다.



멀티 사이트 관리.



AXIS OS 업그레이드.



인증서 관리.

장치 인벤토리

엔터프라이즈 네트워크의 보안을 보장하는 근본적인 측면은 네트워크에 있는 장치의 전체 인벤토리를 유지하는 것입니다. 전체 보안 정책을 수립하거나 검토할 때, 핵심 자산뿐만 아니라 모든 개별 장치에 대한 정보와 명확한 문서를 확보하는 것이 중요합니다. 간과된 장치 하나하나가 공격자의 침입 경로가 될 수 있기 때문입니다. 간과하거나 완전히 파악하지 못한 장치는 보호할 수 없습니다.

장치 인벤토리는 엔터프라이즈 네트워크 보안의 필수적인 단계입니다. AXIS Device Manager는 다음과 같은 기능으로 이를 지원합니다.

- 감사 및 사고 대응 작업 시 네트워크 장치의 최신 전체 인벤토리에 쉽게 접근할 수 있도록 합니다.
- 총 수량, 유형, 모델 번호 등으로 정렬할 수 있는 전체 장치 목록을 제공합니다.
- 네트워크에 있는 모든 장치의 상태를 알려줍니다.
- 장치 소프트웨어 지원 종료 예정일을 보여주고 교체 가능한 신제품 목록을 제공하여 사전 계획 수립을 돕습니다.

AXIS Device Manager Client

Device Manager Configuration Logs Hotkeys

Manage devices

250 devices, 1 selected

MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
ACCC8EF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
ACCC8EECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EEB2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
ACCC8EEA73E8	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
ACCC8EE80DB4	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
ACCC8EE24018	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M3125-LVE
ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information
ACCC8EDC1601	OK	10.21.66.50	AXIS M3215-LVE	10.12.289	Yes	Disabled	ADM	2023-02-26 (3Y)	2029-12-31	AXIS M3215-LVE

Connected to ADM

Alarms and Tasks

AXIS Device Manager를 통해 장치 인벤토리를 분명하게 볼 수 있습니다.

AXIS Device Manager는 Axis 네트워크 장치의 실시간 인벤토리에 접근할 수 있는 자동화된 수단을 제공하여 장치를 자동으로 식별, 나열 및 정렬하도록 해줍니다. 마찬가지로 중요한 점은, 태그를 사용하여 자체 기준에 따라 장치를 그룹화하고 정렬할 수 있어 네트워크의 모든 Axis 장치에 대한 개요를 파악하고 문서화하기가 쉽다는 것입니다.

계정 및 패스워드 정책

인증 및 권한 제어는 네트워크 리소스 보호의 중요한 부분입니다. 정책을 구현하면 시간이 지남에 따라 우발적이거나 의도적인 오용의 위험을 줄이는 데 도움이 됩니다. 강력한 패스워드를 사용하도록 강제하는 것도 중요하지만, 패스워드가 유출될 위험을 줄이는 것 또한 핵심적인 과제입니다. 장치 패스워드는 조직 내에서 공유되는 경우가 많으며, 그렇게 되면 누가 패스워드에 접근할 수 있는지 통제하기 어렵습니다. AXIS Device Manager는 Axis 장치의 여러 계정과 패스워드를 쉽게 관리할 수 있도록 도와줍니다.

장치의 사용자 계정이 2개 이상 있어야 하는 이유:

- 다양한 사용자 유형(기계 및 사람)에 대한 권한 수준을 제어할 수 있습니다.
- 루트(마스터) 패스워드가 유출될 위험을 줄일 수 있습니다.
- 다른 사용자에게 영향을 주지 않으면서 한 사용자 유형의 자격 증명을 재설정할 수 있습니다.

AXIS Device Manager에서 권한 사용

Axis 장치는 여러 계정을 지원하며, 각 계정은 세 가지 권한 수준 중 하나를 갖습니다.

- **Viewers(뷰어):** 이 사용자들은 비디오 및 PTZ 제어에 접근할 수 있습니다.
- **Operators(운영자):** 운영자 권한을 가진 사용자는 카메라 설정과 비디오 스트림 프로파일을 최적화할 수 있습니다.
- **Administrators(관리자):** 관리자는 계정을 관리하고, 네트워크 설정을 수정하며, 장치의 여러 서비스를 제어할 수 있습니다.

카메라에 액세스하는 역할마다 고유한 계정이 있어야 합니다. 예를 들어 "관제실 직원" 역할에는 "운영자" 권한 수준을 부여하고, "순찰 직원" 역할에는 "뷰어" 권한 수준만 부여하도록 구성할 수 있습니다.

권장 단계

- VMS에 카메라를 추가하기 전에 AXIS Device Manager에 먼저 카메라를 추가합니다.
- AXIS Device Manager에서 모든 카메라를 선택하고 새로운 사용자 계정("vms" 또는 이와 유사한 계정)을 만든 후 강력한 패스워드를 설정합니다. 권한은 VMS의 요구사항에 맞춰야 하며, 운영자 또는 관리자 권한이 될 수 있습니다(제조사에 확인).
- 생성한 계정과 패스워드를 사용하여 VMS에 장치를 추가합니다.
- 다시 AXIS Device Manager로 돌아와 모든 카메라를 선택하고 "root" 계정 패스워드를 새롭고 강력한 패스워드로 재설정(변경)합니다. "root" 계정 패스워드는 AXIS Device Manager를 사용하는 소수의 인원에게만 알려져야 합니다.
- 누군가 유지보수나 문제 해결 작업을 위해 웹 브라우저로 장치에 액세스해야 할 경우, 절대로 루트 패스워드를 **알려주지 마십시오**. 대신, AXIS Device Manager를 사용하여 선택한 장치에 대해 관리자 또는 운영자 권한을 가진 새로운(임시) 계정을 생성합니다. 작업이 완료되면 AXIS Device Manager를 사용하여 임시 계정을 삭제합니다.
- AXIS Device Manager는 도메인 사용자와 그룹뿐 아니라 로컬 관리자도 지원합니다. AXIS Device Manager 서버를 호스팅하는 동일한 시스템에서만 AXIS Device Manager 클라이언트에 액세스하는 경우 로컬 관리자를 사용할 수 있습니다. 시스템을 유지보수하는 사람이 원격 클라이언트를 사용할 경우 도메인 사용자를 이용하는 것을 권장합니다.

The screenshot shows the AXIS Device Manager Client interface. The main window has a title bar 'AXIS Device Manager Client' and a menu bar with 'Device Manager', 'Configuration', 'Logs', and 'Hotkeys'. Below the menu bar is a toolbar with various icons. The main content area is titled 'Manage devices' and shows a list of 250 devices. A 'User Management' dialog box is open in the center, titled 'Select method and action'. The dialog has two sections: 'Method' and 'Operation'. The 'Method' section has two options: 'Manually enter credentials, operate on selected devices' (selected) and 'Use a CSV file'. The 'Operation' section has four options: 'Set password' (selected), 'Add user', 'Remove user', and 'List users of selected and accessible devices'. The background shows a table of devices with columns for MAC address, Status, Address, and a list of device replacements.

MAC address	Status	Address
ACCC8EF37017	OK	10.21.66.4
ACCC8EF34AD0	OK	10.21.66.228
ACCC8EECD1E9	OK	10.21.68.61
ACCC8EECD123	OK	10.21.68.60
ACCC8EEB2B4	OK	10.21.66.209
ACCC8EEBCBD4	OK	10.21.66.194
ACCC8EEB910F	OK	10.21.66.210
ACCC8EEA73E8	OK	10.21.66.134
ACCC8EE89BF7	OK	10.21.66.53
ACCC8EE8935A	OK	10.21.66.52
ACCC8EE80DB4	OK	10.21.66.54
ACCC8EE80849	OK	10.21.68.55
ACCC8EE80816	OK	10.21.68.56
ACCC8EE56609	OK	10.21.68.80
ACCC8EE521A2	OK	10.21.66.5
ACCC8EE49D90	OK	10.21.66.211
ACCC8EE2401B	OK	10.21.66.208
ACCC8EE1C43F	OK	10.21.66.207
ACCC8EE10192	OK	10.21.66.230
ACCC8EE06247	OK	10.21.66.203
ACCC8EDE17A8	OK	10.21.66.213
ACCC8EDC1601	OK	10.21.66.50

End of software support	Device replacements
No information	No information
2029-12-31	AXIS Q1809-LE
No information	No information
No information	No information
2027-12-31	AXIS M1135 Mk II
2029-12-31	AXIS P3265-V
2027-12-31	AXIS M1137 Mk II
2027-12-31	No information
2029-12-31	AXIS P1388 AXIS P1388-B
2029-12-31	AXIS P1387 AXIS P1387-B
2027-12-31	AXIS M3085-V
2027-12-31	AXIS M3085-V
2027-12-31	AXIS M3085-V
2025-02-01	AXIS Q6075-E
2033-12-31	No information
2027-12-31	AXIS M3215-LVE
No information	No information
2033-12-31	No information
2026-11-30	AXIS M3125-LVE
2029-12-31	AXIS P3265-LVE
No information	No information
No information	No information

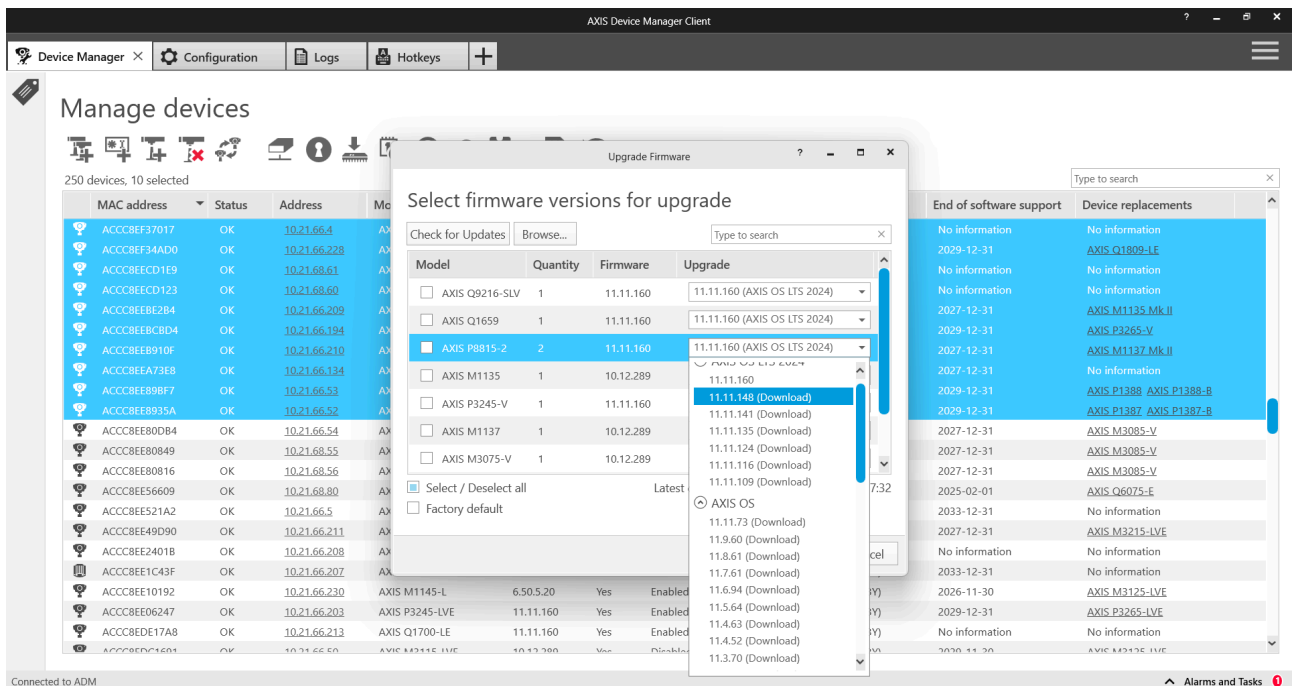
AXIS Device Manager에서 사용자 역할 및 패스워드를 변경합니다.

AXIS OS 업그레이드

업데이트된 AXIS OS 버전에는 알려진 취약점에 대한 패치가 포함되어 있습니다. 공격자가 알려진 취약점을 이용하려고 할 수 있으므로 항상 최신 소프트웨어를 사용해야 합니다. 마찬가지로 중요한 점은, 새로운 AXIS OS 버전을 신속하게 배포하면 운영 능력이 향상되고 수동으로 새 릴리스 업그레이드를 배포하는 것과 관련된 병목 현상이 제거된다는 것입니다. AXIS Device Manager는 www.axis.com에 연결하여 적용 가능한 최신 AXIS OS 또는 서비스 릴리스를 다운로드합니다. 인터넷에서 네트워크에 직접 다운로드하지 않으려면 업그레이드를 USB 스틱에 저장한 후 AXIS Device Manager 클라이언트에 업로드할 수 있습니다. 또한 새로운 AXIS OS 버전이 있는지 표시하고 Axis 장치에 신속하게 배포할 수 있도록 지원합니다.

항상 최신 AXIS OS 버전을 실행해야 하는 이유:

- 최신 패치를 통해 알려진 취약점, 특히 치명적인 취약점으로부터 네트워크와 장치를 보호할 수 있습니다.
- 장치가 최신 성능 개선 사항과 버그 및 결함 수정 사항으로 업데이트됩니다.
- 최신 기능 및 기능 향상에 즉시 액세스할 수 있습니다.



AXIS Device Manager를 통한 AXIS OS 업그레이드는 화면 알림과 직관적인 대화 상자 덕분에 간소화되었습니다.

추가 보안 강화

우수한 사용자 및 패스워드 정책을 적용하고 최신 AXIS OS 버전을 실행하면 장치에 대한 일반적인 위험을 완화할 수 있습니다. *AXIS 보안 강화 가이드*에서는 중요한 대규모 조직에서 위험을 줄일 수 있는 추가 조치를 설명합니다. 여기에는 사용하지 않을 수 있는 서비스를 비활성화하고, 공격이나 침해의 징후를 탐지하고 모니터링하는 데 도움이 되는 서비스를 활성화하는 것이 포함됩니다. AXIS Device Manager는 이러한 일부 정책을 배포하는 과정을 단순화합니다. Axis는 기본적인 권장 설정을 위한 구성 템플릿을 제공합니다.

Axis 보안 강화 가이드에 따라 장치 보안을 강화하는 방법:

- *AXIS 보안 강화 가이드* 를 읽고 문서 끝에 있는 템플릿 파일을 다운로드하십시오.
- 구성 파일을 편집하여 관련 항목을 선택합니다.
- AXIS Device Manager 인벤토리에서 장치를 선택합니다.
- 마우스 오른쪽 버튼을 클릭하고 "Configure Devices(장치 구성) > Configure(구성)..."를 선택합니다.
- "Configuration File(구성 파일)"을 클릭하고 다운로드한 파일을 선택합니다.
- 필요에 따라 설정을 조정합니다.

인증 기관 서비스

인증 기관(CA)은 서버, 클라이언트 또는 사용자에게 디지털 인증서를 발급하는 서비스입니다. CA는 공용이거나 개인일 수 있습니다. Comodo 및 Symantec(이전의 Verisign)과 같이 공개적으로 신뢰할 수 있는 CA는 일반적으로 공용 웹 사이트와 이메일 등의 공개 서비스에 사용됩니다.

사설 CA(일반적으로 Active Directory/Certificate Service)는 내부/사설 네트워크 서비스를 위한 인증서를 발급합니다. 영상 관리 시스템에서 이것은 주로 HTTPS 네트워크 암호화 및 IEEE 802.1X 네트워크 접근 제어를 위해 사용됩니다. AXIS Device Manager는 Axis 장치를 위한 CA 서비스를 포함하고 있으며, 엔터프라이즈 공개 키 기반 구조(PKI)의 일부로서 사설 루트 CA 또는 사설 중간 CA로 작동할 수 있습니다.

CA 서명 인증서는 IEEE 802.1x(클라이언트) 및 HTTPS(서버) 인증서에 둘 다 사용됩니다.

HTTPS

HTTPS는 클라이언트와 서버 사이의 통신이 암호화되는 HTTP의 보안 버전입니다. 자체 서명 인증서만으로도 암호화된 연결을 구현할 수 있습니다. 자체 서명 인증서와 CA 서명 인증서의 암호화 수준에는 차이가 없습니다. 차이점은 자체 서명 인증서의 경우 공격 컴퓨터가 합법적인 서버를 사칭하는 네트워크 스푸핑(spoofing)을 방지하지 못한다는 것입니다. CA 서명 인증서는 클라이언트가 신뢰할 수 있는 장치에 액세스하고 있음을 인증하는 신뢰 지점(trust point)을 추가합니다. 비디오를 암호화하려면 비디오 클라이언트(VMS)가 HTTPS(RTP over RTSP over HTTPS)를 통한 비디오 요청을 지원해야 합니다.

IEEE 802.1X

종종 802.1X라고도 하는 이 표준은 허가되지 않은 네트워크 장치가 로컬 네트워크에 접근하는 것을 방지합니다. 장치가 네트워크와 그 리소스에 액세스할 수 있으려면 먼저 자신을 인증해야 합니다. MAC 주소(MAC 필터링), 사용자/패스워드, 또는 클라이언트 인증서 등 다양한 인증 방법을 사용할 수 있습니다. 시스템 소유자는 위험, 위험, 비용을 고려하여 어떤 방법을 사용할지 결정합니다.

802.1X 기반 시설을 운영하려면 관리 지원 스위치와 추가 서버(일반적으로 RADIUS(Remote Authentication Dial-In User Service))가 필요합니다. 클라이언트 인증서를 사용하려면 클라이언트 인증서를 발급할 수 있는 CA(개인 또는 공용)가 필요합니다. 대부분의 경우 인프라를 유지보수하고 모니터링할 인력이 필요합니다.

The screenshot shows the AXIS Device Manager Client interface. The main window is titled 'Manage devices' and displays a list of 250 devices. A 'Secure communication' dialog box is open, showing options to 'Enable' or 'Disable' HTTPS, IEEE 802.1X, or both. The 'Enable' option is selected. The background shows a table of device details including MAC address, Model, Serial number, and Firmware version.

MAC address	Status	Address
ACCC8EF37017	OK	10.21.66.4
ACCC8EF34AD0	OK	10.21.66.22
ACCC8EED1E9	OK	10.21.68.61
ACCC8EED123	OK	10.21.68.61
ACCC8EEB2B4	OK	10.21.66.21
ACCC8EEBCBD4	OK	10.21.66.11
ACCC8EB910F	OK	10.21.66.21
ACCC8EEA73E8	OK	10.21.66.11
ACCC8EEB9BF7	OK	10.21.66.21
ACCC8EE8935A	OK	10.21.66.52
ACCC8EE80DB4	OK	10.21.66.54
ACCC8EE80849	OK	10.21.68.55
ACCC8EE80816	OK	10.21.68.54
ACCC8EE56609	OK	10.21.68.80
ACCC8EE521A2	OK	10.21.66.5
ACCC8EE49D90	OK	10.21.66.21
ACCC8EE2401B	OK	10.21.66.21
ACCC8EE1C43F	OK	10.21.66.21
ACCC8EE10192	OK	10.21.66.21
ACCC8EE06247	OK	10.21.66.203
ACCC8EE17A8	OK	10.21.66.213

AXIS Device Manager의 인증서 구성입니다.

인증서 수명 주기 관리

인증서 수명 주기 관리는 시간 경과에 따른 인증서 발급, 설치, 검사, 문제 해결 및 갱신과 관련된 모든 프로세스와 작업을 비용 효율적으로 처리하는 수단입니다. AXIS Device Manager는 관리자가 다음 작업을 수행할 수 있도록 하여 인증서를 효율적으로 관리할 수 있도록 지원합니다.

- 다른 CA를 사용할 수 없는 경우 CA 서명 인증서 발급
- IEEE 802.1X 인증서의 간편한 관리
- HTTPS 인증서의 간편한 관리
- 인증서 만료 날짜를 모니터링합니다.
- 만료 전에 인증서를 쉽게 갱신합니다.

사설 루트 및 중간 CA에 대한 권장 사항

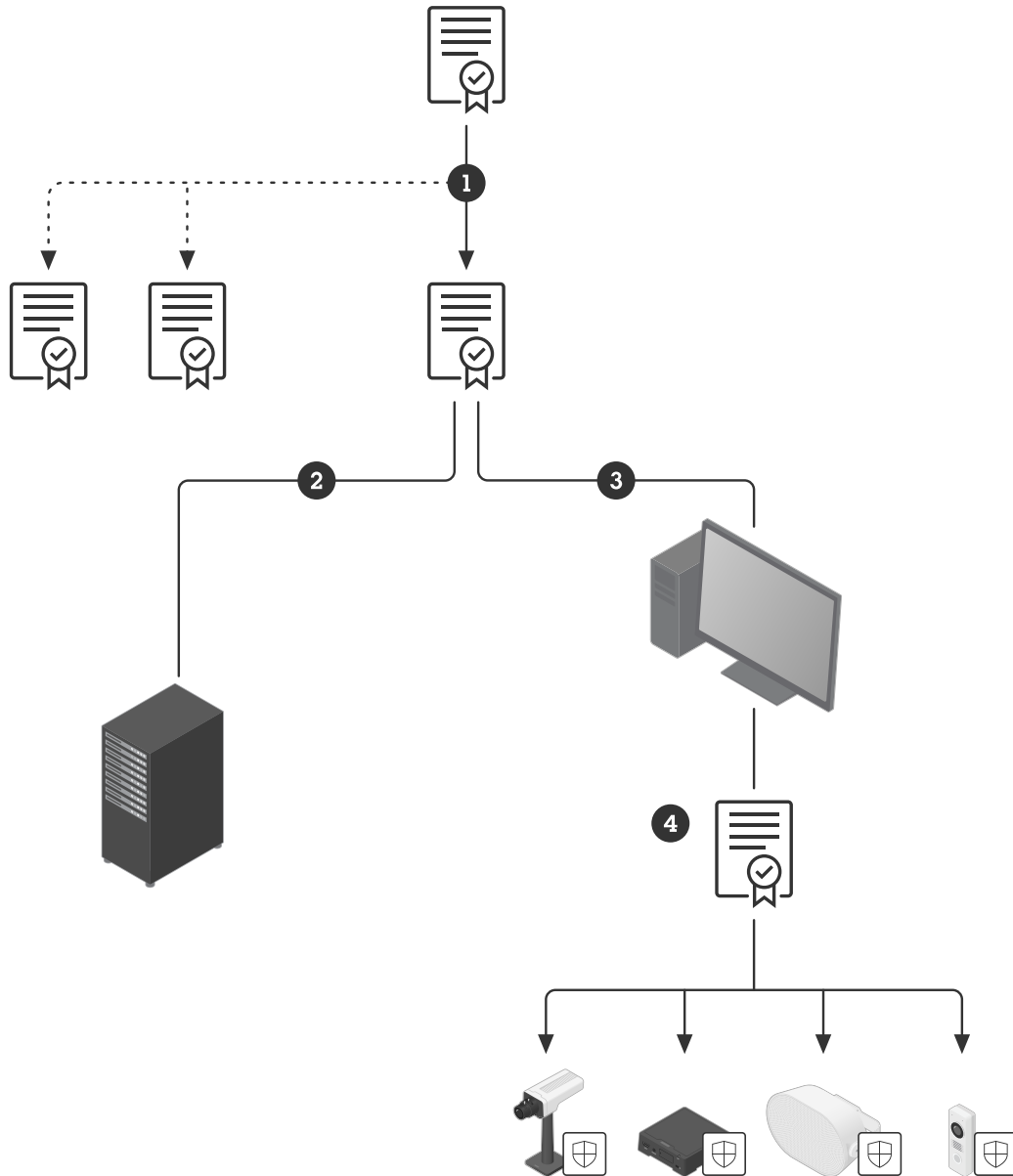
대중을 상대로 Axis 장치를 공용 서버로 노출하는 것은 좋지 않습니다. 이러한 이유로 사설 리소스에 공인 CA를 사용하는 것은 비용 효율적이지 않습니다.

HTTPS의 경우, 신뢰할 수 있는 카메라에 액세스하고 있는지 검증해야 하는 클라이언트는 VMS 서버 뿐입니다. VMS 서버가 라이브 및 녹화 비디오를 제공하므로 운영자 클라이언트는 카메라에 직접 액세스하지 않습니다. 이러한 상황에서는 기존 엔터프라이즈 PKI에 카메라 서버 인증서를 통합하는 것의 가치가 제한적입니다.

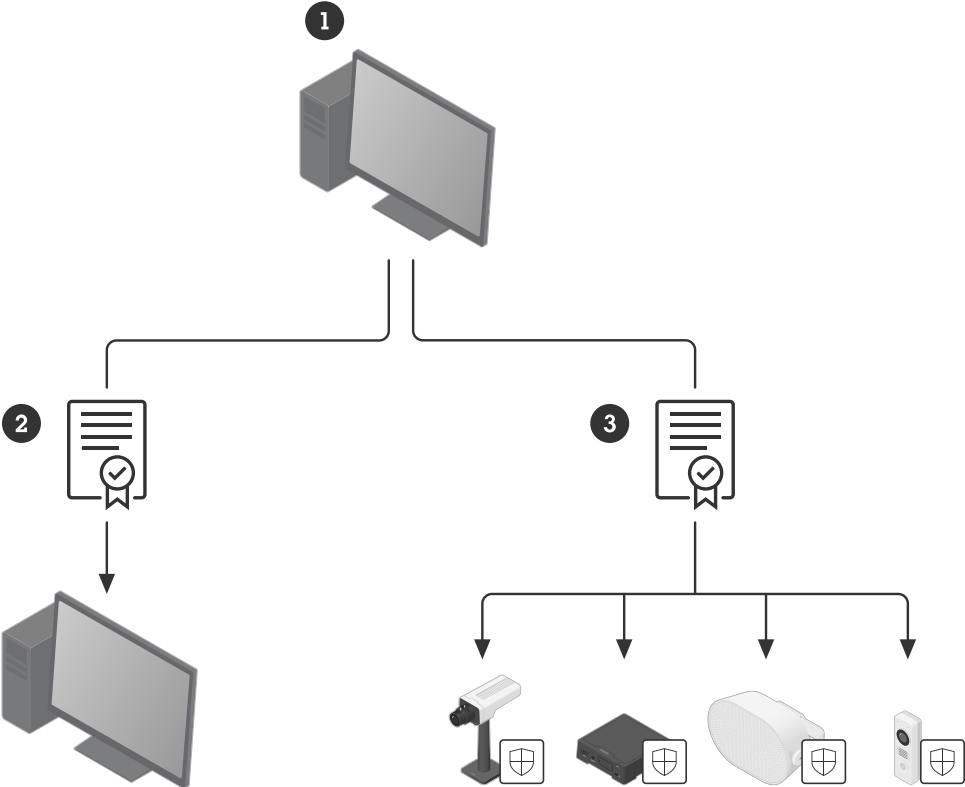
AXIS Device Manager를 개인 CA로 사용하는 것이 가장 비용 효율적인 해결책입니다. 루트 CA 인증서가 생성된 후 VMS 서버의 인증서 스토어에 AXIS Device Manager 인증서를 설치하십시오. 유지보수나 문제 해결을 위해 카메라에 직접 액세스하는 다른 클라이언트가 있는 경우, 해당 클라이언트에도 AXIS Device Manager 루트 CA를 설치합니다.

802.1X의 경우 RADIUS 서버에 자신을 인증하려면 카메라에 클라이언트 인증서가 필요합니다. 엔터프라이즈 PKI/CA에 대한 관리자가 중간 CA 인증서를 생성하여 AXIS Device Manager에 설치할 수 있는 PKCS#12(P12) 인증서로 이 인증서를 내보내도록 하는 것이 좋습니다.

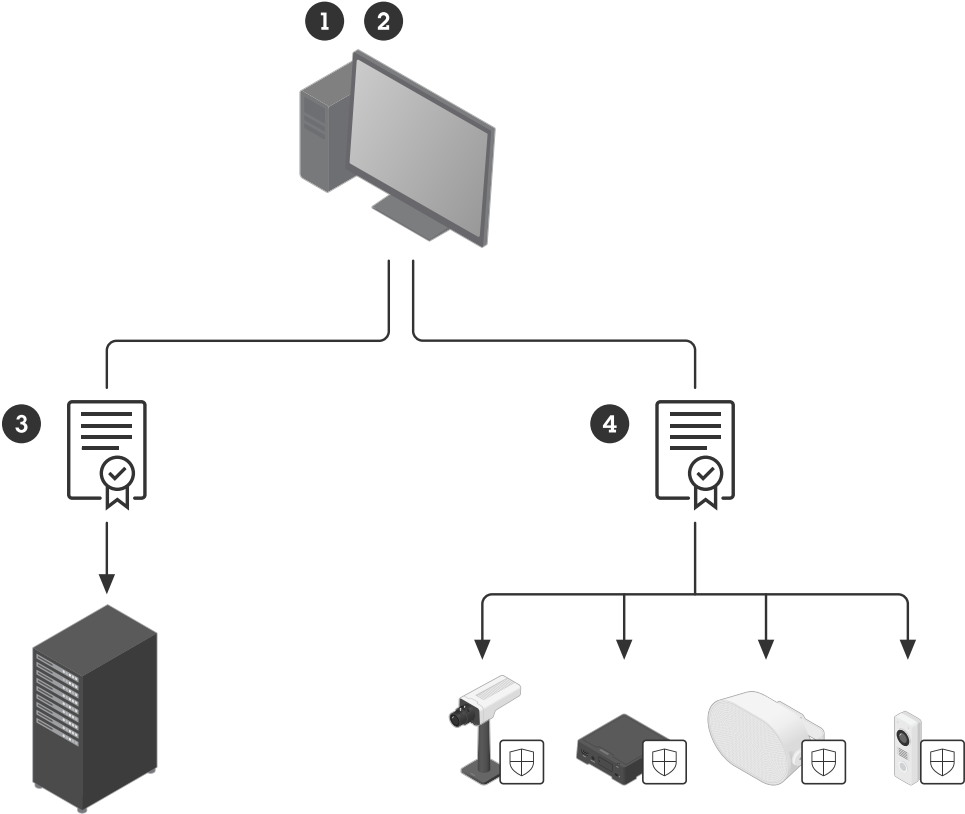
FreeRADIUS 서버 설정에 대한 지원이 필요한 경우, AXIS Device Manager의 **기술 백서** 섹션을 참조하십시오.



HTTPS 인증서 관리는 1) AXIS Device Manager에서 중간 또는 루트 CA 인증서를 생성, 2) CA 인증서를 VMS로 내보내기, 3) 서버 인증서를 장치에 업로드하기를 포함합니다.



사실 CA 사용. IEEE 802.1X 인증서 관리는 1) 중간 CA 및 클라이언트 인증서 생성, 2) RADIUS 서버에 CA 인증서 설치, 3) AXIS Device Manager로 CA 인증서 가져오기, 4) CA 및 클라이언트 인증서를 장치에 업로드하기를 포함합니다.



AXIS Device Manager를 CA로 사용. IEEE 802.1X 인증서를 관리하려면: 1) AXIS Device Manager에서 루트 CA 인증서를 생성하고, 2) AXIS Device Manager로 인증 CA 인증서를 가져오고, 3) RADIUS 서버에 CA 인증서를 설치하고, 4) CA 인증 및 클라이언트 인증서를 장치에 업로드합니다.

결론

보안 관리와 보안 제어는 효과적인 사이버 보안 방법 구현의 중요한 부분으로서, 각각은 IP 네트워크에 영향을 줄 수 있는 잠재적 위협을 완화하기 위해 명확한 상태를 유지하고 적절한 액션을 따라야 하는 지속적인 프로세스입니다. AXIS Device Manager는 장치를 관리하고 네트워크 보안을 강화할 수 있는 도구를 제공합니다. 자세한 내용이나 지원은 해당 지역 Axis 담당자에게 문의하거나 www.axis.com을 참조하십시오.

T10231485_ko

2025-09 (M4.2)

© 2025 Axis Communications AB