AXIS Device Manager를 통한 보안 제어

버전 1.0

목차

1. 소개 **3**

1.1 세 가지 사이버 보안 보호 계층 3

1.2 이 문서의 목적 3

1.3 AXIS Device Manager 정보 3

2. 장치 인벤토리 **4**

3. 계정 및 패스워드 정책 **5**

4. 펌웨어 업그레이드 **6**

5. 추가 보안 강화 **7**

6. 인증 기관 서비스 **7**

7. 인증서 수명 주기 관리 **8**

8. 결론 **9**

1. 소개

감시 및 보안 분야에서 사이버 보안의 중요성이 계속 커지고 있습니다. 효과적인 사이버 보안을 위해서는 선택한 제품은 물론, 함께 일하는 파트너부터 파트너 및 고객이 정한 요건에 이르는 모든 수준에서 IP 네트워크를 철저히 보호해야 합니다.

1.1 세 가지 사이버 보안 보호 계층

Axis는 세 가지 사이버 보안 보호 계층을 제공합니다.

1. 보안 관리: 여러분이 직면한 위협을 완화하는 데 필요한 보안 제어를 적용해야 합니다. 보안 관리는보안 제어와 비용 효율적인 관리, 두 부분으로 나눌 수 있습니다. 보안 제어는 물리적 재산, 정보, 컴퓨터 시스템 또는 그 밖의 자산에 대한 보안 위험을 피하거나 감지하거나 대처하거나 최소화하기 위해 사용되는 보호 수단 또는 대책입니다.

2. 취약성 관리: 악용될 수 있는 결함의 위험을 최소화하기 위해 제품의 설계, 개발 및 테스트에 사이버 보안 모범 관행을 적용하고자 Axis에서 수행하는 모든 노력이 포함됩니다. Axis에서는 취약성이 발견될 경우 중대한 취약성을 즉시 수정하고 보안 공지를 발령하여 관리합니다.

3. 학습 및 공동 작업: Axis, 여러분, 그리고 여러분의 IP 네트워크와 관계된 파트너들이 여러분이 직면한 위협과 그 잠재적인 영향, 네트워크를 보호하는 방법을 분명하게 이해하고 함께 공유할 수 있도록 합니다.

1.2 이 문서의 목적

이 애플리케이션 가이드에서는 AXIS Device Manager를 사용하여 시스템을 강화하고 보안을 향상시킬 수 있는 방법을 설명하고 핵심적인 측면을 중심으로 권장 사항을 제시합니다.

1.3 AXIS Device Manager 정보

AXIS Device Manager는 모든 주요 설치, 보안 및 유지 보수 장치 관리 작업(아래 표 참조)을 간편하고 비용 효율적이며 안전하게 관리할 수 있는 방법을 제공하는 온프레미스 도구입니다. 이 도구는 하나의 사이트에서는 최대 2천대, 여러 사이트의 경우에는 수천 대의 Axis 장치를 관리하는 데 적합합니다. AXIS Device Manager를 사용하면 사이버 보안 제어를 효율적으로 배포하여 네트워크 장치를 보호하고 보안 기반 시설에 맞출 수 있습니다.

장치 관리 기능, AXIS Device Manager

설치	유지보수
> IP 주소 할당 > 장치 목록 내보내기 및 자산 추적* > 사용자 및 패스워드 관리* > ACAP 관리 > 펌웨어 업그레이드* > HTTPS 인증서 관리* > IEEE 802.1x 인증서 배포* > 장치 태깅	> 장치 상태 > 장치 데이터 수집 > 장치 구성 및 여러 장치에 구성 복사 > 여러 서버/시스템에 연결 > 복구 지점 > 공장 출하 시 기본 설정으로 복구 > 장치 교체 > 인증서 갱신 및 관리* > 사이버 보안 강화*

*사이버 보안 제어 기능을 나타냄
그림 1. 다중 사이트 관리

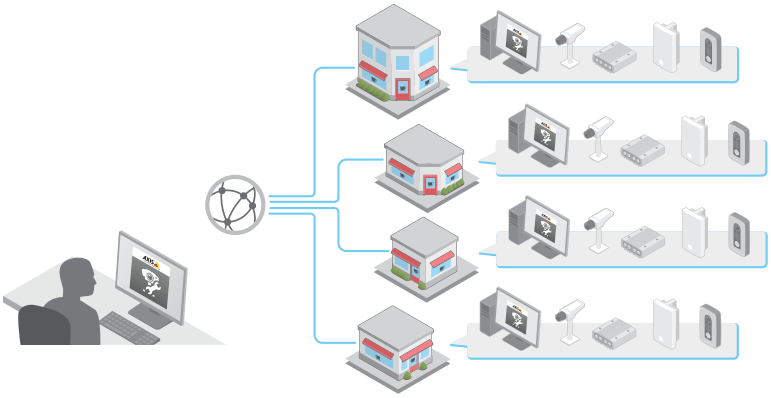


그림 2. 펌웨어 업그레이드

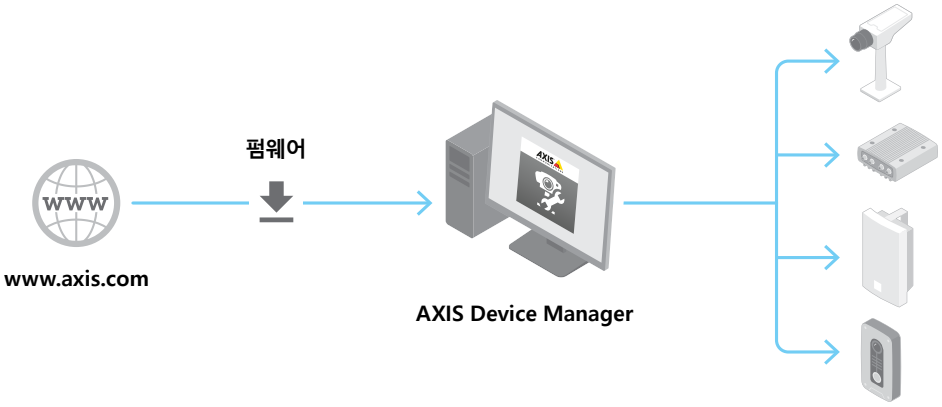
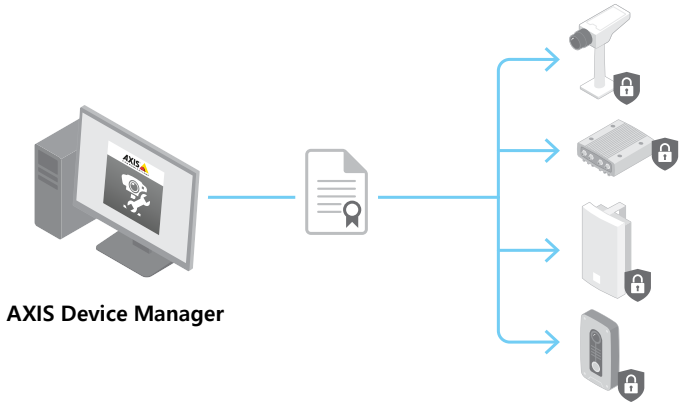


그림 3. 인증서 관리



2. 장치 인벤토리

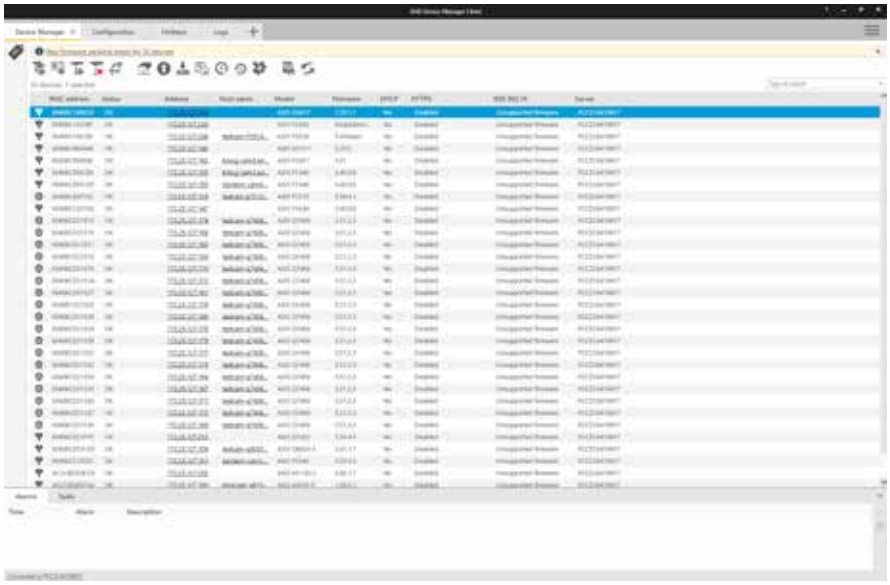
엔터프라이즈 네트워크의 보안을 보장하는 핵심은 네트워크 상에 있는 장치의 전체 인벤토리를 유지하는 일입니다. 전체 보안 정책을 만들거나 검토할 때 중요한 자산뿐 아니라 각 장치에 대한 지식과 명확한 설명서가 있어야 합니다. 장치를 하나라도 간과할 경우 공격자의 진입 수단이 될 수 있기 때문입니다. 간과하거나 완전히 알지 못하는 장치를 보호할 수는 없습니다.

장치 인벤토리는 엔터프라이즈 네트워크 보안의 필수적인 단계를 보여줍니다. AXIS Device Manager는 다음과 같이 그 역할을 담당합니다.

> 감사 및 사건 대응자와 작업할 때 네트워크 장치의 현재 전체 인벤토리에 쉽게 액세스할 수 있도록 해줍니다.
> 총 개수, 유형, 모델 번호 등을 기준으로 정렬하여 장치의 전체 목록을 제공합니다.

> 네트워크에 있는 각 장치의 상태를 제공합니다.

권장 사항
AXIS Device Manager는 Axis 네트워크 장치의 실시간 인벤토리에 액세스할 수 있는 자동화된 수단을 제공하여 장치를 자동으로 식별, 나열 및 정렬하도록 해줍니다. 무엇보다, 태그를 사용하여 자체 기준을 기반으로 장치를 그룹화하고 정렬할 수 있으므로 네트워크에 있는 모든 Axis 장치의 개요를 파악하고 문서화하는 일이 쉬워집니다.



AXIS Device Manager를 통해 장치 인벤토리를 분명하게 볼 수 있습니다.

3. 계정 및 패스워드 정책

인증 및 권한 제어는 네트워크 리소스 보호의 중요한 부분입니다. 정책 구현을 통해 더 오랫동안 우연히 또는 고의적으로 잘못 사용하는 위험을 줄일 수 있습니다. 제대로 기능하지 못하는 패스워드의 위험을 줄이는 것이 핵심입니다. 강력한 패스워드가 중요합니다. 하지만, 장치 패스워드는 조직 내에서 두루 통용될 수 있습니다. 그렇게 되면 장치에 액세스하는 사용자를 제어할 수 없게 됩니다. AXIS Device Manager를 사용하면 Axis 장치의 여러 계정과 패스워드를 간편하게 관리할 수 있습니다.

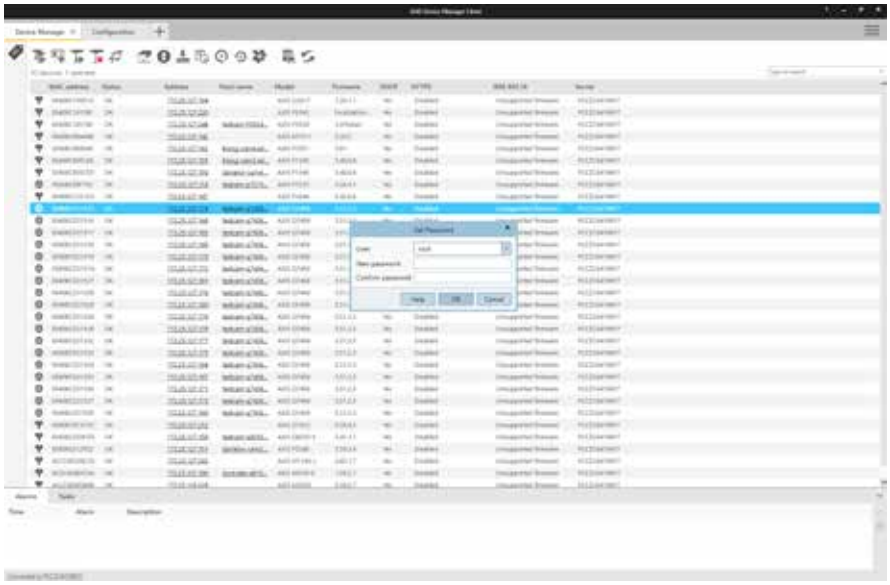
장치의 사용자 계정이 2개 이상 있어야 하는 이유
> 여러 사용자 유형의 권한 수준을 제어합니다(기계 및 사람).
> 루트(마스터) 패스워드 손상 위험을 줄입니다.
> 다른 사용자에게 영향을 주지 않으면서 사용자 유형 하나의 자격 증명을 재설정할 수 있습니다.

AXIS Device Manager에서 권한 사용
AXIS Device Manager에서는 Axis 장치가 여러 계정을 지원하고 서로 다른 세 가지 권한 수준(관찰자, 운영자, 관리자)에 속할 수 있습니다. 다음은 Axis 네트워크 카메라의 권한 관리 방법입니다.

관찰자 권한을 가진 사용자는 비디오에 액세스하고 PTZ를 제어할 수 있습니다. 운영자 권한을 가진 사용자는 카메라 설정과 비디오 스트림 프로파일을 최적화할 수 있습니다. 관리자는 계정을 관리하고 네트워크 설정을 수정하며 장치의 여러 가지 서비스를 제어할 수 있습니다. 카메라에 액세스하는 역할마다 고유한 계정이 있어야 합니다.

권장 단계

> VMS에 카메라를 추가하기 전에 AXIS Device Manager에 카메라를 추가하는 것이 좋습니다.
> AXIS Device Manager에서 모든 카메라를 선택하고 새로운 사용자 계정("vms" 또는 이와 유사한 계정)을 만든 후 강력한 패스워드를 설정합니다. 권한이 VMS 요구 사항에 맞아야 합니다. 이 권한은 운영자이거나 관리자일 수 있으며 제조업체에 문의하십시오.
> "vms" 계정과 정의한 패스워드로 VMS에 장치를 추가합니다.
> AXIS Device Manager로 돌아가 다시 모든 카메라를 선택하고 "root" 계정 패스워드를 강력한 새 패스워드로 재설정(변경)합니다. "root" 계정 패스워드는 AXIS Device Manager를 사용하는 제한된 인원만 알고 있어야 합니다.
> 조직의 누군가가 유지보수나 장애 처리를 위해 웹 브라우저를 사용하여 장치에 액세스해야 한다면 root 패스워드를 주지 말고, AXIS Device Manager를 사용하여 관리자나 운영자 권한으로 선택한 장치의 새로운 임시 계정을 만드십시오. 작업이 끝나면 AXIS Device Manager를 사용하여 임시 계정을 제거합니다.
> 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 유지관리하는 사람이 원격 클라이언트를 사용한다면 도메인 사용자를 사용하는 것이 좋습니다.



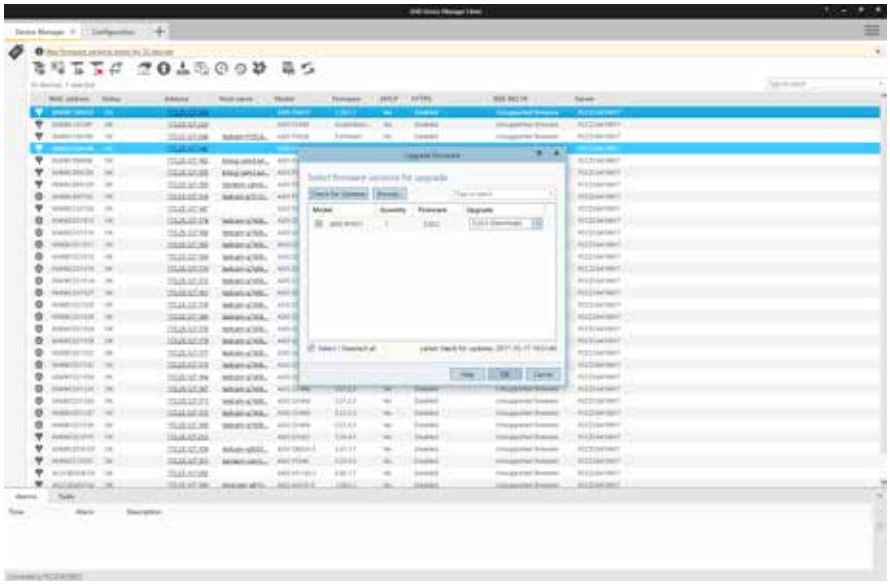
AXIS Device Manager에서 사용자 역할 및 패스워드를 변경합니다.

4. 펌웨어 업그레이드

최신 펌웨어 버전에는 알려진 취약성에 대한 패치가 포함됩니다. 공격자가 알려진 취약성을 이용하려고 할 수 있으므로 항상 최신 소프트웨어를 사용해야 합니다. 무엇보다, 새로운 펌웨어를 신속히 배포하면 운영 능력이 강화되고 새로운 릴리즈 업그레이드의 수동 롤아웃과 관련된 정체가 제거됩니다. AXIS Device Manager는 www.axis.com에 연결하여 해당되는 최신 펌웨어나 서비스 릴리즈를 다운로드합니다. 인터넷에서 네트워크에 직접 다운로드하지 않으려면 업그레이드를 USB 스틱에 저장한 후 AXIS Device Manager 클라이언트에 업로드할 수 있습니다. 또한 펌웨어가 공개되면 알려주고 Axis 장치에 신속하게 배포할 수 있도록 합니다.

항상 최신 펌웨어 버전을 실행해야 하는 이유

> 최신 패치가 알려진 취약성, 특히 중요한 취약성으로부터 네트워크와 장치를 보호합니다.
> 알려진 버그나 결함을 해결할 뿐 아니라 최신 성능으로 개선하기 위해 장치가 업데이트됩니다.
> 최신 기능과 기능 향상에 즉시 액세스할 수 있습니다.



온스크린 알림과 직관적인 대화 상자를 통해 진행되므로 AXIS Device Manager에서 간편하게 펌웨어를 업그레이드할 수 있습니다.

5. 추가 보안 강화

최신 펌웨어 버전으로 장치를 실행할 뿐 아니라 좋은 사용자/패스워드 정책을 사용하면 장치에 가해지는 일반적인 위험이 줄어듭니다. Axis 보안 강화 가이드에서는 중요한 대규모 조직에서 위험을 줄일 수 있는 추가 조치를 설명합니다. 사용하지 않는 서비스를 비활성화하고 공격이나 위반의 징후를 감지 및 모니터링하는 데 유익한 서비스를 활성화하는 작업이 여기에 포함됩니다.

AXIS Device Manager를 사용하여 이 정책 중 일부를 간단하게 배포할 수 있습니다. Axis에서는 기본적인 권장 설정을 위한 구성 템플릿을 제공합니다. 자세한 내용은 www.axis.com/products/axis-device-manager/support-and-documentation을 참조하십시오.

Axis 보안 강화 가이드에 따라 장치 보안을 강화하는 방법

> www.axis.com/products/axis-device-manager/support-and-documentation에서 보안 강화 템플릿 구성 파일을 다운로드합니다.
> 구성 파일을 편집하여 관련 항목을 선택합니다.
> 장치를 선택합니다.
> 마우스 오른쪽 버튼을 클릭하고 "장치 구성 | 구성..."을 선택합니다.
> "구성 파일"을 클릭하고 다운로드한 파일을 선택합니다.
> 필요에 따라 설정을 조정합니다.

6. 인증 기관 서비스

CA(인증 기관)는 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.

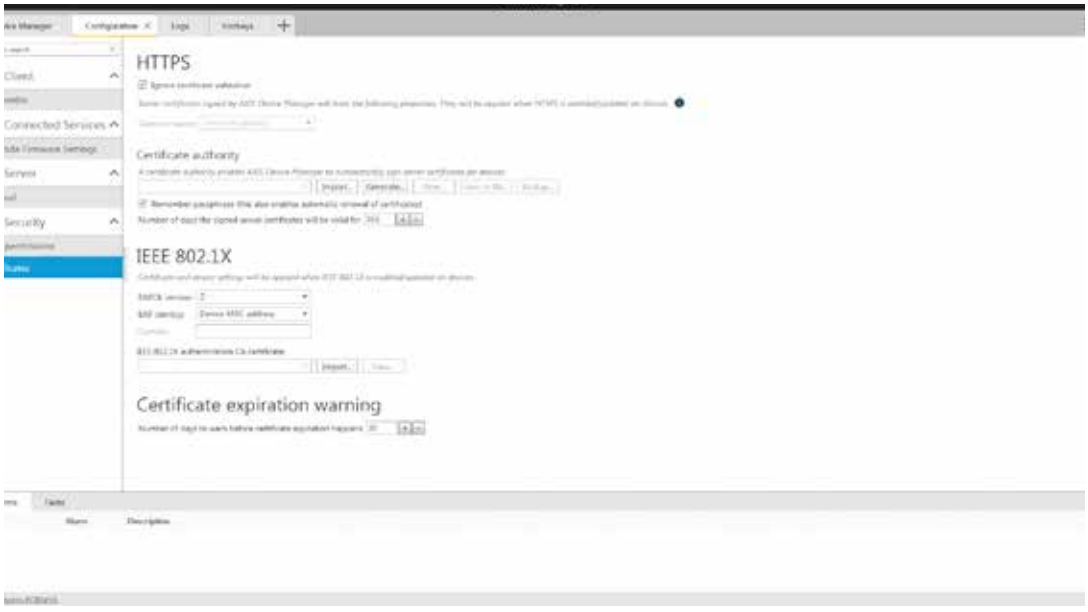
개인 CA(일반적으로 액티브 디렉터리/인증서 서비스)는 내부/개인 네트워크 서비스용 인증서를 발급합니다. 비디오 관리 시스템에서 이 인증서는 주로 HTTPS(Hyper Text Transfer Protocol Secure)(네트워크 암호화) 및 IEEE 802.1x(네트워크 접근 제어)에 사용됩니다. AXIS Device Manager는 Axis 장치용 CA 서비스를 포함하며 개인 루트 CA 또는 개인 중간 CA(엔터프라이즈 PKI(공개 키 인프라)의 일부)로 사용될 수 있습니다.

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 인증서는 암호화된 연결을 하기에 충분합니다. 자체 서명 인증서와 CA 서명 인증서의 암호화 수준에는 차이가 없습니다. 자체 서명 인증서는 공격하는 컴퓨터가 합법적인 서버를 가장하려고 시도하는 네트워크 스푸핑으로부터 보호하지 않는다는 점이 다릅니다. CA 서명 인증서는 신뢰할 수 있는 장치를 액세스하고 있음을 클라이언트가 인증하기 위한 신뢰 지점을 추가합니다. 비디오를 암호화하려면 비디오 클라이언트(VMS)가 HTTPS(RTP over RTSP over HTTPS)를 통한 비디오 요청을 지원해야 합니다.

IEEE 802.1X
802.1X로 불리는 이 표준은 권한이 없는 네트워크 장치가 로컬 네트워크에 액세스하는 것을 막아줍니다. 장치가 네트워크와 그 리소스에 액세스할 수 있으려면 먼저 자신을 인증해야 합니다. MAC 주소(MAC 필터링), 사용자/패스워드 또는 클라이언트 인증서와 같이 다양한 인증 방법을 사용할 수 있습니다. 시스템 소유자가 위협, 위험 및 비용에 따라 어떤 방법을 사용할지 적절히 선택할 수 있습니다.

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 기반 시설에는 이를 유지보수하고 모니터링할 인력이 있어야 합니다.



AXIS Device Manager의 인증서 구성입니다.

7. 인증서 수명 주기 관리

인증서 수명 주기 관리는 오랫동안 인증서를 발급, 설치, 검사, 보완, 갱신하는 데 관련된 모든 프로세스와 작업을 비용 효율적으로 처리할 수 있는 방법입니다. AXIS Device Manager를 사용하면 관리자가 다음과 같은 작업을 수행할 수 있어 효율적으로 인증서를 관리할 수 있습니다.

> 다른 CA를 사용할 수 없을 때 CA 서명 인증서를 발급할 수 있습니다.
> IEEE 802.1X 인증서를 쉽게 배포합니다.
> HTTPS 인증서를 쉽게 배포합니다.
> 인증서 만료 날짜를 모니터링합니다.
> 만료 전에 인증서를 쉽게 갱신합니다.

개인 루트 및 중간 CA 권장 사항
대중을 상대로 Axis 장치를 공용 서버로 노출하는 것은 좋지 않습니다. 개인 리소스에 공용 CA를 사용하는 것은 비용 효율적인 방법이 아니기 때문입니다.

HTTPS의 경우 VMS 서버에 한해서 서버가 신뢰할 수 있는 카메라에 액세스하고 있음을 검증해야 합니다. VMS 서버가 라이브 및 녹화 비디오를 제공하므로 운영자 클라이언트는 카메라에 직접 액세스하지 않습니다. 이 경우 기존의 엔터프라이즈 PKI에 카메라 서버 인증서를 통합하는 것은 그 가치가 제한적입니다.

AXIS Device Manager를 개인 CA로 사용하는 것이 가장 비용 효율적인 해결책입니다. 루트 CA 인증서를 생성한 후 VMS 서버의 인증서 스토어에 AXIS Device Manager 인증서를 설치하십시오. 유지보수나 장애 처리를 위해 카메라에 직접 액세스하는 다른 클라이언트가 있는 경우 이 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.

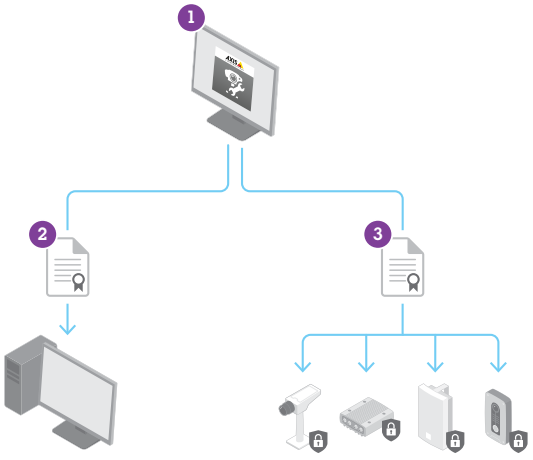


그림 4, 왼쪽: HTTPS 인증서 관리에는
1) AXIS Device Manager에서 중간 또는 루트 CA 인증서 생성 2) VMS에 CA 인증서 내보내기 3) 장치에 서버 인증서 업로드가 포함됩니다.

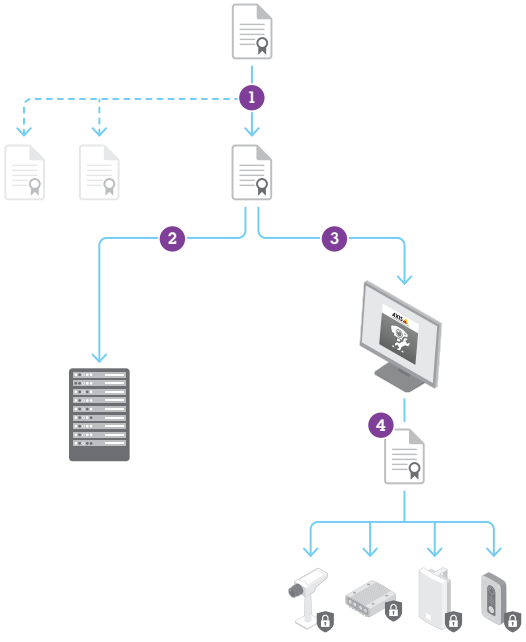


그림 5, 오른쪽: IEEE 802.1X 인증서 배포에는 1) 중간 CA 및 클라이언트 인증서 생성 2) Radius 서버에 CA 인증서 설치 3) AXIS Device Manager에서 CA 인증서 가져오기 4) 장치에 CA 및 클라이언트 인증서 업로드가 포함됩니다.

8. 결론

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

Axis Communications 정보

Axis에서는 보다 스마트하고 안전한 세상을 실현하는 지능형 보안 솔루션을 제공합니다. 네트워크 비디오 시장을 선도하는 Axis는 개방형 플랫폼을 기반으로 혁신적인 네트워크 제품을 지속적으로 선보이며 글로벌 파트너 네트워크를 통해 고객에게 높은 가치를 전달하고자 노력합니다. 오랜 기간 파트너와 긴밀한 관계를 유지해온 Axis는 기존 시장은 물론 새로운 시장에서 풍부한 지식과 획기적인 네트워크 제품을 제공해왔습니다.

Axis는 전 세계 50개국 이상에 2,700명이 넘는 정직원을 두고 90,000개 업체가 넘는 파트너사와 이룩한 글로벌 네트워크를 통해 든든한 지원을 받고 있습니다. 1984년에 설립되어 스웨덴에 본사를 두고 있는 Axis는 현재 NASDAQ Stockholm에 상장되어 있습니다.

Axis에 대한 자세한 내용은 www.axis.com을 참조하십시오.

©2018 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC 및 VAPIX는 관련 법규에 따른 Axis AB의 등록 상표 또는 상표 출원입니다. 모든 회사명과 제품은 해당 회사의 상표이거나 등록 상표입니다. Axis는 사전 통지 없이 수정할 권한이 있습니다.