보안 강화 가이드

카메라

목차

1. 소개

Axis는 장치의 설계, 개발, 테스트에 사이버 보안 모범 사례를 적용하여 공격에서 악용 당할 수 있는 결함의 위험을 최소화하는 데 최선을 다하고 있습니다. 그러나 네트워크, 장치, 그리고 지원하는 서비스의 보안을 확보하려면 전체 벤더 공급 체인과 최종 사용자 조직의 적극적인 참여가 필요합니다. 보안성이 보장된 환경은 사용자, 프로세스, 기술에 달려 있습니다. Axis는 고객의 네트워크, 장치, 서비스의 보안 확보를 지원하기 위해 이 가이드를 준비했습니다.

이 가이드는 Axis 비디오 솔루션을 전개하는 데 관련된 모든 사람을 위한 기술 조언을 제공합니다. 이를 통해 베이스 라인 구성 및 진화하는 위협 환경을 다루기 위한 보안 강화 가이드를 수립할 수 있습니다. 다른 여러 보안 조직의 경우와 마찬가지로 Axis의 베이스 라인은 CIS Controls(버전 6.1)를 사용합니다. www.cisecurity.org/critical-controls.cfm 을 참조하십시오. *CIS Controls는 이전에는 SANS Top 20 Critical Security Controls로 알려지기도 했습니다.* 이 문서에서는 CSC(Critical Security Control)가 CSC#로 표시되어 사용됩니다.

특정 설정을 구성하는 방법을 배우려면 해당 제품의 사용자 설명서(User Manual)가 필요할 수 있습니다. Axis는 여러 보안 컨트롤을 보다 비용 효율적으로 관리하는 데 도움을 주는 ACM(AXIS Camera Management)을 무료로 제공합니다(www.axis.com/products/axis-camera-management).

참고: 이 문서, 문의처 정보 및 보안 공지는 다음 사이트에서 확인할 수 있습니다.
www.axis.com/support/product-security

1.1 네트워크 환경의 보안 카메라

네트워크 카메라에 대한 가장 명확한 위협은 물리적인 방해, 파손 행위, 탬퍼링입니다. 이러한 위협으로부터 제품을 보호하려면 파손 방지 모델이나 케이스를 선택하고, 권장하는 방식으로 장착해야 하며, 케이블을 보호해야 합니다.

IT/네트워크 관점에서 보면 카메라는 비즈니스용 노트북, 데스크탑, 모바일 기기 등과 유사한 네트워크 종단점입니다. 비즈니스용 노트북과 달리 네트워크 카메라는 사용자로 인한 일반적인 위협, 즉 잠재적 유해 웹사이트를 방문하거나 악의적인 이메일 첨부파일을 열거나 신뢰할 수 없는 애플리케이션을 설치하는 위협에 노출되어 있지 않습니다. 그러나 카메라는 시스템을 위험에 노출시킬 수 있는 인터페이스가 있는 네트워크 장치입니다. 이 가이드는 이러한 위험의 노출 영역을 줄이는 데 초점을 맞추고 있습니다.

1.2 인터넷 노출 제한

카메라를 공용 웹 서버로 노출시켜 알 수 없는 클라이언트가 카메라에 네트워크 액세스를 할 수 있도록 하는 것은 좋지 않습니다. VMS(Video Management System: 영상 관리 시스템)를 운영하지 않고 원격 위치에서 비디오에 액세스해야 하는 개인과 소규모 조직의 경우, AXIS Companion을 사용할 것을 권장합니다. AXIS Companion은 Windows/IOS/Android 클라이언트 소프트웨어로, 무료이며 카메라를 인터넷에 노출시키지 않으면서 보다 보안성이 높은 방식으로 비디오에 액세스할 수 있는 손쉬운 방법을 제공합니다. AXIS Companion 정보 및 다운로드는 **www.axis.com/companion** 에서 확인할 수 있습니다. VMS를 사용하는 대규모 조직은 VMS 벤더에게 원격 비디오 액세스에 관해 문의해야 합니다.

1.3 로컬 네트워크 노출 제한

VMS 환경에서 클라이언트는 항상 VMS 서버를 통해 실시간 및 녹화 비디오에 액세스합니다. 물리적 또는 가상 격리를 통해 격리된 네트워크에 VMS 서버와 카메라를 배치는 방식은 노출과 위험을 줄이기 위해 일반적으로 권장하는 조치입니다.

2. 보호 레벨 정보

이 가이드는 시스템 크기와 요구 사항에 따라 서로 다른 보호 레벨을 사용합니다. 각 레벨에서는 이전 레벨의 권장 사항이 지켜지고 있다고 가정합니다.

보호 레벨		권장 대상	절차
0	기본 보호	데모 목적과 테스트 시나리오용으로만 권장합니다.	해당 없음
1	표준 보호	최소 권장 레벨의 보호. 이 레벨은 일반적으로 운영자가 관리자를 겸하는 사무실 설치 환경 또는 소규모 비즈니스용으로 적합합니다.	> 공장 출하 시 기본 설정 > 최신 펌웨어 사용 > 마스터 패스워드 설정 > 비디오 클라이언트 계정 생성 > 네트워크 설정 구성 > 시간 및 날짜 설정 > 해당되는 경우 오디오 비활성화 > 엣지 스토리지 암호화
2	엔터프라이즈 보호	전담 시스템 관리자가 있는 기업용으로 권장하는 설정.	> HTTP 다이제스트 인증 > 도메인 및 호스트 이름 > 사용하지 않는 서비스 비활성화 > IP 주소 필터 > HTTPS 암호화
3	매니지드 엔터프라이즈 보호	IT/IS 부서가 있는 대규모 네트워크 인프라. 카메라를 엔터프라이즈 네트워크 인프라에 통합할 필요가 있을 수 있는 환경용.	> IEEE 802.1X 네트워크 액세스 제어 > SNMP 모니터링 > 원격 시스템 로그

3. 기본 보호

카메라는 사전 정의된 기본 설정 및 기본 패스워드와 함께 인도됩니다. 일상 운영에 이 설정을 사용하지 않을 것을 권장합니다.

4. 표준 보호

표준 보호 레벨은 최소한의 권장 보호 레벨입니다. 이 레벨은 일반적으로 운영자가 관리자를 겸하는 소규모 사업체와 조직용으로 적합합니다.

4.1 공장 출하 시 기본 설정

CSC #3: 하드웨어 및 소프트웨어를 위한 보안성 높은 구성.

시작하기 전에, 제품이 알려진 공장 출하 시 기본 설정 상태인지 확인하십시오. 상태에 대해 확신할 수 없는 경우 *System Options* > *Maintenance*로 이동한 후 Default를 클릭하십시오.

4.2 최신 펌웨어 사용

CSC #2: 인가 및 비인가 소프트웨어의 재고.

새로운 취약성이 발견되는 경우, 이들 대부분은 중대하지 않거나 악용하는 데 비용이 많이 듭니다. 중대한 취약성이 가끔 발견되며, 장치, 컴퓨터, 시스템 서비스에 패치를 적용해야 합니다. 소프트웨어와 펌웨어에 패치를 적용하는 것은 사이버 보안의 중요한 프로세스입니다. 공격자는 일반 (알려진) 취약성을 악용하려 하는 경우가 많으며, 패치가 적용되는 않은 서비스에 대한 네트워크 액세스를 확보하는 경우 성공할 수 있습니다. 항상 최신 펌웨어를 사용하도록 하십시오. 알려진 취약성에 대한 보안 패치가 포함되어 있을 수 있기 때문입니다. 특정 펌웨어 릴리스 정보는 중요한 보안 픽스를 명시적으로 언급할 수 있지만 모든 일반 보안 픽스를 언급하는 것은 아닙니다.

최신 펌웨어 파일을 컴퓨터로 다운로드하십시오. 최신 버전은 **www.axis.com/techsup/firmware.php**에서 항상 무료로 제공됩니다. 펌웨어를 업그레이드하기 전에, 사용자 설명서에서 지침을 읽으십시오.

4.3 마스터 패스워드 설정

CSC #5: 관리자 권한의 제어된 사용.

패스워드는 네트워크 카메라를 보호하기 위한 가장 중요한 수단입니다. 강력한 패스워드를 사용하고 이를 안전하게 유지하십시오. 여러 대의 카메라를 설치하는 경우, 카메라에 동일한 패스워드나 고유한 패스워드를 사용할 수 있습니다. 같은 패스워드를 사용하면 관리하기에 간단하지만, 한 대의 카메라의 보안이 손상되면 위험이 증가합니다.

최소 8자로 구성된, 짐작하기 어려운 패스워드를 만드십시오. 패스워드 생성기를 사용하면 좋습니다.

4.4 비디오 클라이언트 계정 생성

CSC #5: 관리자 권한의 제어된 사용.
CSC #11: 네트워크 포트, 프로토콜, 서비스의 제한 및 제어.

기본 루트 계정은 전체 권한을 가지고 있으며 관리 업무용으로 사용해야 합니다. 일상 운영을 위해서는 제한된 권한이 있는 클라이언트 사용자 계정을 생성하는 것이 좋습니다. 이렇게 하면 관리자 패스워드의 노출을 감소시킬 수 있습니다.

System Options > *Security* > *Users*로 이동하여 일상 운영을 위한 계정을 생성하십시오. 클라이언트가 사용할 카메라 서비스에 따라 Viewer 또는 Operator를 선택해야 합니다. VMS(Video Management System)는 일반적으로 Operator 권한 그룹을 사용해야 하지만 일부의 경우 관리자 권한이 필요할 수 있습니다. VMS 벤더와 확인하십시오.

4.5 네트워크 설정 구성

CSC #3: 하드웨어 및 소프트웨어를 위한 보안성 높은 구성.

장치 IP 구성은 IPv4/IPv6, 정적 또는 동적(DHCP) 네트워크 주소, 서브넷 마스크 및 기본 라우터 등과 같은 네트워크 구성에 따라 달라집니다.

System Options > Network > TCP/IP > Basic/Advanced로 이동하여 네트워크 설정을 구성하십시오.

4.6 시간 및 날짜 설정

CSC #3: 하드웨어 및 소프트웨어를 위한 보안성 높은 구성.

보안의 관점에서 봤을 때 날짜와 시간이 정확한 것이 중요합니다. 예를 들면 시스템 로그에 올바른 정보로 타임 스탬프가 지정되도록 해야 하기 때문입니다.

카메라 시계는 NTP(Network Time Protocol) 서버와 동기화할 것을 권장합니다. 로컬 NTP 서버가 없는 소규모 조직 및 개인의 경우 공용 NTP 서버를 사용할 수 있습니다. 인터넷 서비스 공급사에 확인하거나 pool.ntp.org 같은 공용 NTP 서버를 사용하십시오.

*System Options > Date & Time*으로 이동하여 시간대 및 일광절약시간을 포함하여 시간 설정을 구성하십시오.

4.7 오디오 비활성화

CSC #11: 네트워크 포트, 프로토콜, 서비스의 제한 및 제어.
CSC #13: 데이터 보호.

오디오를 지원하는 카메라 모델에서는 오디오 활성화가 기본 설정되어 있습니다. 오디오는 프라이버시와 무결성으로 인해 일반적으로 비디오에 비해 데이터 등급이 높습니다. 오디오 스트리밍을 허용하기 전에 현지 규정을 확인하는 것이 좋습니다.

*System Options > Security> Audio Support*로 이동하여 클라이언트가 오디오 스트림을 요청하는 것을 방지하십시오.

4.8 엣지 스토리지 암호화

CSC #13: 데이터 보호.

카메라가 SD 카드를 지원하고 이 저장 장치에 비디오가 녹화되는 경우, 암호화를 적용할 것을 권장합니다. 이렇게 하면 SD 카드를 제거할 수 있는 승인 받지 않은 사람이 저장된 비디오를 재생하는 것을 방지합니다. NAS(Network Attached Storage: 네트워크 연결 스토리지)를 녹화 장치로 사용하는 경우, NAS는 잠금 장치가 된 구역에서 보호해야 하며 계정/패스워드를 올바르게 구성해야 합니다.

*System Options > Storage > SD Card > Encrypt*로 이동하여 패스워드를 설정하십시오. 사용된 암호화는 AES-128입니다.

5. 엔터프라이즈 보호

전문적인 영상 감시 시스템을 운영하는 중규모 및 대규모 조직의 경우 VMS(Video Management System) 소프트웨어 또는 NVR을 사용할 것을 권장합니다. 엔터프라이즈 보호 레벨에서는 네트워크 카메라의 가능한 공격 영역을 줄여 위험을 최소화하는 것이 수반됩니다. VMS 제조사의 사이버 보안 권장 사항을 따르는 것이 좋습니다.

이 섹션에서 설명된 설정의 일부는 공장 출하 시 사전 설정되어 있습니다. 아래의 지침을 따라 이러한 설정이 올바른지 확인하십시오.

5.1 개방 포트

참고로, 카메라에는 다음과 같은 개방 포트가 사전 구성되어 있습니다.

포트	서비스
TCP-21	FTP 서버
TCP-80	HTTP 서버
TCP-554	RTSP 서버
TCP-49152	UPnP (검색 프로토콜)
TCP-1900	UPnP SSDP(Simple Service Discovery Protocol)
UDP-3702	웹 서비스 동적 검색
UDP-4815	Bonjour 검색 프로토콜 (mDNS)
UDP-57143	Bonjour (mDNSResponderPosix)

5.2 HTTP 다이제스트 인증

CSC #3: 하드웨어 및 소프트웨어를 위한 보안성 높은 구성.
CSC #13: 데이터 보호.

클라이언트가 네트워크를 통해 일반 텍스트로 로그인 패스워드를 전송하는 것을 방지하려면, 다이제스트 인증(암호화된 패스워드)만 허용할 것을 권장합니다.

*System Options > Users > Allow Password type*으로 이동하여 Encrypted Only를 선택하십시오. 다이제스트 인증을 지원하지 않는 클라이언트가 있는 경우, Encrypted & Unencrypted를 선택해야 합니다.

5.3 도메인 및 호스트 이름

CSC #1: 인가 및 비인가 장치의 재고.

네트워크 인프라가 DNS(Domain Name System)를 지원하는 경우, IP 주소 대신 FQDN(Fully Qualified Domain Name: 정규화된 도메인 이름)을 사용하여 카메라에 액세스할 것을 권장합니다. 이렇게 하면 카메라를 더욱 쉽게 관리하고 추적할 수 있습니다.

*System Options > Network > Advanced > Host Name configuration*으로 이동하여 시스템을 DNS 인프라와 일치시키십시오.

5.4 사용하지 않는 서비스 비활성화

사용하지 않는 서비스는 즉각적인 보안 위협은 아니지만, 비활성화시켜 불필요한 위험을 감소시키는 것이 좋습니다. 사용하지 않는 경우 비활성화할 수 있는 일부 서비스는 아래와 같습니다.

5.4.1 FTP 서버

FTP 서버는 기본적으로 활성화 설정되어 있으며 일반적으로 고급 유지관리와 장애 처리에 사용됩니다. 카메라 전개가 끝나면 FTP 서버를 비활성해야 합니다.

나중에 카메라 펌웨어가 이 서비스의 비활성화를 기본 설정으로 할 수 있지만, 설정을 점검할 것을 권장합니다.

System Options > *Network* > *Advanced* > *FTP*로 이동하십시오.

5.4.2 SSH – Secure Shell(보안 셸)

SSH 커맨드 라인 인터페이스는 비활성화되도록 기본 설정되어 있습니다. SSH는 고급 유지관리 및 장애 처리에 도움이 될 수 있지만, 정상적인 운영 중에는 SSH를 비활성화해야 합니다. 비활성화 상태인지 확인할 것을 권장합니다.

System Options > *Plain Config*로 이동하여 Network 그룹을 선택하십시오. SSH용 체크박스는 하단 근처에 있습니다.

5.4.3 IP 주소의 ARP/Ping 설정

ARP/Ping은 관리자가 커맨드 라인 터미널을 사용해 고정 IP 주소를 설정하여 ARP/Ping 명령 조합을 전송할 수 있게 하는 레거시 서비스입니다. 서비스는 카메라가 다시 시작된 후 2분 동안만 이용할 수 있습니다. 최근 펌웨어에서는 이 서비스가 삭제되었지만, 오래된 펌웨어를 가지고 있는 경우 이 서비스를 완전히 비활성화할 것을 권장합니다.

Services 섹션에서 System Options > *Network* > *Basic*으로 이동하십시오.

5.4.4 AXIS Device Dispatcher – AVHS

AVHS(AXIS Video Hosting Systems)는 클라우드 기반의 영상 관리 서비스입니다. 카메라의 제어 버튼을 누르면 호스팅 서비스 디스패처에 카메라가 등록됩니다. 디스패처는 카메라에 대한 액세스 권한이 있고 올바른 OAK(Owner Authentication Key: 소유자 인증 키)를 제공하는 사용자가 카메라에 액세스할 수 있도록 허용합니다. 물리적 제어 버튼을 눌렀을 때 카메라가 디스패처에 연결하는 것을 방지하려면, *System Options* > *Network* > *Basic*으로 이동하여 Enable AVHS에서 체크 표시를 지우십시오.

시스템에 카메라를 설치할 때 일부 VMS 벤더는 AXIS Device Dispatcher를 지원할 수 있다는 점을 염두에 두십시오. VMS 벤더와 확인하십시오.

AVHS 관련 상세 정보는 **www.axis.com/products/hosted-video** 에서 확인할 수 있습니다.

5.4.5 네트워크 검색 프로토콜

검색 프로토콜은 네트워크에서 카메라와 그 서비스를 더 쉽게 찾을 수 있도록 해주는 지원 서비스입니다. 카메라가 설치되어 카메라 장치 IP 주소가 확인되고 VMS에 카메라가 추가되면, 검색 프로토콜을 비활성화하여 네트워크에 있는 카메라의 존재가 공개되지 않도록 할 것을 권장합니다.

> UPnP (Universal Plug and Play)
  System Options > *Network* > *UPnP* 로 이동하십시오.
> Bonjour
  System Options > *Network* > *Bonjour* 로 이동하십시오.
> Link-local address (Zero Conf)
  System Options > *Network* > *Advanced Link-Local IPv4 Address*로 이동하십시오.

5.4.6 SOCKS

SOCKS는 비활성화되도록 기본 설정되어 있으며, 방화벽/프록시서버의 다른 쪽에서 네트워크 서비스(예: HTTP 또는 FTP 이미지 업로드)에 카메라가 도달할 수 있도록 하기 위한 특정 목적으로만 사용됩니다.

System Options > *Network* > *SOCKS*로 이동하십시오.

5.4.7 상시 멀티캐스트 비디오

상시 멀티캐스트 비디오는 비활성화되도록 기본 설정되어 있습니다. 클라이언트가 멀티캐스트 비디오를 요청하지 않은 상태에서 로컬 네트워크에서 비디오를 브로드캐스트하기 위한 특정 환경용으로 사용됩니다.

System Options > *Network* > *RTP* > *Multicast*로 이동하십시오.

5.4.8 QoS – Quality Of Service(서비스 품질)

네트워크 인프라가 QoS를 지원하지 않는 경우, *System Options* > *Network* > *QoS*로 이동하여 모든 DCSP 값을 0으로 설정하십시오.

System Options > *Network* > *QoS*로 이동하십시오.

5.5 IP 주소 필터 (IP 테이블)

CSC #1: 인가 및 비인가 장치의 재고.
CSC #13: 경계선 방어.
CSC #15: 알아야 할 필요에 기반한 제어된 액세스.

인가된 클라이언트용으로만 IP 필터링을 활성화하면 카메라가 다른 모든 클라이언트의 네트워크 트래픽에 반응하는 것을 방지합니다. 모든 인증 클라이언트(VMS 서버 및 관리 클라이언트)를 화이트 리스트에 추가하십시오.

System Options > *Security* > *IP Address Filter*로 이동하십시오.

5.6 HTTPS 암호화

CSC #13: 데이터 보호.

HTTPS는 클라이언트와 카메라 사이의 트래픽을 암호화합니다. 카메라의 모든 관리 작업에 HTTPS를 사용할 것을 권장합니다. HTTPS를 활성화해도 RTP/RTSP를 통해 전송되는 비디오는 암호화되지 않는다는 점을 염두에 두십시오. 비디오가 제한 등급으로 분류되어 암호화를 통해 보호해야 하는 경우, 비디오 클라이언트는 HTTPS를 통해 터널링된 RTP/RTSP 비디오를 요청해야 합니다. 이는 비디오 클라이언트/VMS 기능에 의해 제어되며, 해당 기능에 따라 달라집니다.

자체 서명 인증은 암호화를 제공하는 데에는 적합하지만, 중간자 공격(man-in-the-middle-attack)으로부터는 보호하지 않습니다. 클라이언트(예: 웹 브라우저)는 인증의 신뢰성이 없다는 경고를 할 것입니다.

클라이언트가 올바른 카메라에 액세스하고 있다는 점을 인증하고 이를 통해 카메라를 가장한 공격 컴퓨터의 위험을 감소시키려면 (사설 또는 공공) CA 서명 인증이 필요합니다.

6. 매니지드 엔터프라이즈 보호

매니지드 엔터프라이즈 네트워크는 일반적으로 카메라가 연계해야 하는 추가적인 관리 도구와 서비스가 있는 시스템입니다.

6.1 IEEE 802.1X 네트워크 액세스 제어

CSC #1: 인가 및 비인가 장치의 재고.
CSC #13: 경계선 방어.

IEEE 802.1X를 통해 보호되는 네트워크 인프라에서 승인되려면, 카메라에 적절한 인증서 및 설정이 필요합니다.

System Options > *Security* > *Certificates* 로 이동하여 인증서를 관리하고 CA 루트 인증서를 설치하십시오.
System Options > *Security* > *IEEE 802.1X*로 이동하십시오.

6.2 SNMP 모니터링

CSC #14: 감사 로그의 유지관리, 모니터링 및 분석.

Axis 카메라는 다음과 같은 SNMP 프로토콜을 지원합니다.

> SNMP v1: 레거시 이유로만 지원되며 사용하지 않아야 합니다.

> SNMP v2c: 보호되는 네트워크 세그먼트에서 사용할 수 있습니다.

> SNMP v3: 모니터링 목적으로 권장합니다.

카메라는 MIB-II 및 Axis 비디오 MIB 모니터링을 지원합니다.
Axis 비디오 MIB 다운로드 사이트:
www.axis.com/support/downloads/axis-video-mib

SNMP 관련 상세 정보는 사용자 설명서를 참조하십시오.

6.3 원격 시스템 로그

CSC #4: 지속적인 취약성 평가 및 수정.
CSC #6: 감사 로그의 유지관리, 모니터링 및 분석.
CSC #16: 계정 모니터링 및 제어.
CSC #18: 사고 대응 및 관리.

시스템 로그 서버는 모든 카메라가 생성한 모든 로그 메시지를 수집합니다. 이로 인해 감사가 단순화되고 카메라에서 로그 메시지가 의도적으로/악의적으로 또는 우발적으로(최대 로그 크기에 도달하여 초래된 카메라 재부팅 덮어쓰기에 의해) 삭제되는 것을 방지합니다.

원격 시스템 로그를 활성화하려면, 카메라 구성 파일을 편집해야 합니다. *System Options > Advanced > Scripting > Open Script Editor* 로 이동하십시오.

카메라 펌웨어 버전 5.70까지
내장 스크립트 편집기를 사용하여 파일 /etc/rsyslog.conf를 선택한 다음, 하단에 syslog 서버의 IP 주소(예: *.*@10.2.0.2)를 포함하여 라인을 추가하십시오.

카메라 펌웨어 버전 5.80 및 그 이후
syslog 서버의 IP 주소(예: *.*@10.2.0.2)가 포함된 행이 있는 텍스트 파일을 /etc/rsyslog.d/에서 추가해야 합니다.

본 문서 정보

이 가이드는 장치의 보안을 강화하는 방법을 설명합니다. 이 가이드는 로컬 네트워크 정책, 구성 및 제원 작업을 실시하는 전개 팀의 참고 자료로도 사용할 수 있습니다.

이 문서에서 설명된 모든 설정은 제품의 웹페이지에서 이용할 수 있습니다. 웹페이지에 액세스하려면 해당 제품의 사용자 설명서를 참조하십시오.

이 문서는 주의 깊게 준비되었습니다. 부정확한 점이나 누락된 점을 발견한 경우, 가까운 Axis 지사에 알려주십시오. Axis Communication AB는 분 문서의 기술적 오류 또는 오타에 대해 책임지지 않으며 사전 통지 없이 제품 및 설명서를 변경할 권한이 있습니다.

Axis Communications AB는 상업성 및 특정 목적 적합성에 대한 암묵적 보증 등 본 문서에 포함되어 있는 자료에 대해 어떠한 종류의 보증도 하지 않습니다.

Axis Communications AB는 본 자료의 공급, 성능 또는 사용과 관련하여 발생하는 부수적 또는 결과적 손해배상에 대해 그 어떤 책임도 지지 않습니다. 본 제품은 의도된 목적으로만 사용해야 합니다.

지적재산권

Axis AB는 본 문서에 설명된 제품에 포함된 기술과 관련하여 지적재산권을 가지고 있습니다. 특히, 그리고 제한 없이, 이러한 지적재산권에는 미국 및 기타 국가에서 **www.axis.com/patent.htm** 에 나열된 하나 이상의 특허 및 하나 이상의 추가 특허 또는 특허 출원이 포함되어 있을 수 있습니다.

본 제품에는 라이선스된 3rd party 소프트웨어가 포함되어 있습니다. 상세 정보는 제품의 사용자 인터페이스에서 "정보" 메뉴 항목을 참조하십시오.

본 제품에는 Apple Public Source License 2.0 (**www.opensource.apple.com/apsl**) 의 약관에 따라 Apple Computer, Inc.의 소스 코드 저작권이 포함되어 있습니다. 이 소스 코드는 다음 사이트에서 이용할 수 있습니다: https://developer.apple.com/bonjour/

문의처 정보

Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden
전화: +46 46 272 18 00
팩스: +46 46 13 61 30

www.axis.com

지원

기술 지원이 필요한 경우 가까운 Axis 리셀러에 연락하십시오. 고객 질문에 대해 즉시 답변해드릴 수 없는 경우 리셀러는 해당 질문에 대해 신속하게 답변해드릴 수 있는 적절한 문의처를 알려드립니다.

인터넷 이용이 가능하면 다음을 실시할 수 있습니다.

> 사용자 설명서 및 소프트웨어 업데이트 다운로드.

> FAQ 데이터베이스에서 해결된 문제들에 대한 답변 찾아보기.
제품, 카테고리 또는 문구를 사용하여 검색 가능.

> 개인 지원 영역으로 로그인하여 Axis 지원 팀에 문제 보고.

> Axis 지원 팀 직원과 채팅.

> Axis 지원 웹사이트 방문: www.axis.com/techsup/

70434/KO/R1/1706

Axis Communications에 대하여

네트워크 비디오 분야의 선도 기업인 Axis는 보다 스마트하고 안전한 세상을 위한 지능형 보안 솔루션을 제공합니다. 업계 리더로서 Axis는 개방형 플랫폼에기반한 혁신적인 네트워크 제품을 지속적으로 출시하여 시장의 성장을 이끌어 가고 있으며, 글로벌 파트너 네트워크를 통해 고객에게 한 차원 높은 가치를 제공하고 있습니다. Axis는 파트너들과 신뢰를 바탕으로 한 공고한 관계를 장기간 유지하고 있으며 기존 및 신규 시장에서 새로운 수요를 창출할 수 있도록 파트너들에게 전문 지식 제공과 함께, 혁신적인 네트워크 제품을 공급하고 있습니다.

Axis는 전 세계 50개 이상의 국가에 지사를 두고 2,700명 이상의 직원이 일하고 있으며, 90,000곳 이상의 파트너로 구성된 글로벌 네트워크를 보유하고 전세계 고객들에게 최상의 제품과 서비스를 제공하고 있습니다. 1984년에 설립된 Axis는 스웨덴에 본사를 두고 있으며 현재 NASDAQ Stockholm에 상장(AXIS)되어 있습니다.

Axis에 대한 보다 자세한 정보는 www.axis.com에서 확인하실 수 있습니다.

AXIS COMMUNICATIONS