AXIS Device Manager

사용자 설명서

목차

AXIS Device Manager 정보

AXIS Device Manager는 Axis 제품을 위한 설치 및 관리 소프트웨어 애플리케이션입니다. 이 소프트웨어는 네트워크에서 장치를 자동으로 검색하고, IP 주소를 할당하며, 패스워드를 설정하고, 연결 상태를 표시하고, 여러 장치의 펌웨어 업그레이드, 인증서 및 구성을 관리할 수 있습니다.

AXIS Device Manager는 다음과 같이 구성됩니다.

- AXIS Device Manager Service Control - Axis 제품과의 모든 통신을 처리하는 서버
- AXIS Device Manager Client - 인터넷 또는 기업 네트워크에서 원격 관리를 할 수 있도록 하는 프런트 엔드 사용자 인터페이스

여러 클라이언트를 동일한 서버에 연결할 수 있습니다. 클라이언트는 동시에 여러 서버에 연결할 수 있습니다.

AXIS Device Manager는 시스템을 강화하고 보안을 강화하는 데에도 매우 유용합니다. 자세한 내용은 *AXIS Device Manager 보안 가이드*를 참조하십시오.

솔루션 개요

전제 조건

호환되는 운영 체제

필수: 64bit 운영 체제 Microsoft .NET 버전 4.8

지원 OS: Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

권장 사항 최신 OS 서비스 팩.

최소 시스템 권장 사항:

- 최소(최대 500대의 장치): Intel Core i5 또는 동급, 4GB RAM, 네트워크 인프라 전체에서 100Mbits/s
- 권장(500~2000대의 장치): Intel Core i7 또는 동급, 8GB RAM, 네트워크 인프라 전체에서 1000Mbits/s
- 서버당 2,000대 이상의 장치를 사용하는 것은 권장하지 않습니다.
- Axis 장치가 사용 가능한 최신 AXIS OS를 실행하고 있는지 확인합니다.

비고

Axis는 항상 최신 릴리스의 직전 두 버전을 지원합니다. 지원되는 특정 버전을 확인하려면 최신 릴리스 정보를 참조하십시오.

지원되는 장치:

AXIS OS 버전이 4.40 이상인 AXIS 제품.(지원되는 정확한 기능은 특정 제품 모델 및 펌웨어에 따라 다릅니다.)

언어:

UI + 도움말 파일: 영어, 프랑스어, 독일어, 이탈리아어

UI만 해당: 아라비아어, 체코어, 중국어(간체), 중국어(번체), 네덜란드어, 핀란드어, 일본어, 한국어, 페르시아어, 폴란드어, 포르투갈어(브라질), 러시아어, 스페인어, 스웨덴어, 태국어, 튀르키예어, 베트남어.

시작하기

소프트웨어 설치하기

AXIS Device Manager 5를 설치하려면, 설치할 컴퓨터에 대한 전체 관리자 권한이 있는지 확인한 다음, 다음 단계를 따릅니다.

1. *axis.com의 제품 페이지로 이동하여 AXIS Device Manager 데스크톱 앱을 다운로드합니다.*
2. 설치 프로그램을 실행하고 화면의 지침을 따릅니다.

비고

아직 설치되지 않은 경우, Microsoft .NET 4.8 프레임워크가 설치됩니다(설치 파일에 포함되어 있음). 이 작업은 몇 분 정도 걸립니다. Microsoft .NET 4.8 프레임워크는 AXIS Device Manager를 설치하기 전에 Windows 업데이트를 통해 설치할 수도 있습니다.

서버에 접속

AXIS Device Manager를 처음 시작하면 서버에 연결하라는 메시지가 표시됩니다. 서버는 로컬 컴퓨터 또는 원격 서버에서 실행할 수 있습니다.

로컬 Windows 사용자로 로그인하려면 다음을 수행합니다.

1. **This computer(이 컴퓨터)**를 선택합니다.
2. 현재 자격 증명을 사용하여 로그인하려면 **Log on as current user(현재 사용자로 로그인)**를 선택합니다.

서버 또는 도메인에서 다른 사용자로 로그인하려면 다음을 수행합니다.

- **Other user(다른 사용자)**를 선택합니다.
- **Other user(다른 사용자)** 항목에 해당 계정의 자격 증명을 입력합니다.
- 다음에 클라이언트를 실행할 때 이 단계를 건너뛰려면 **Remember me(내 정보 저장)**를 선택합니다.
- **로그온**을 클릭합니다.

비고

모든 서버에 대해 저장된 자격 증명을 삭제하려면 로그온 화면으로 이동하여 **Delete saved passwords(저장된 패스워드 삭제)**를 선택합니다.

원격 서버에 로그인하려면 다음을 수행합니다.

1. **원격 서버**를 선택합니다.
2. 드롭다운 목록에서 서버를 선택하거나 필드에 IP 주소 또는 DNS 주소를 입력합니다.
3. 자격 증명 입력하기
4. **로그온**을 클릭합니다.

비고

이 옵션은 Windows 도메인에 속하지 않은 컴퓨터에서 원격 서버에 로그인하는 데 사용할 수 없습니다.

여러 서버에 연결

AXIS Device Manager를 사용하면 여러 서버에 연결할 수 있습니다. 서버에 성공적으로 로그인한 후에는 메인 메뉴에서 서버 간 전환이 가능합니다.

1. 메인 메뉴 > Servers(서버) > New connection(새 연결)으로 이동합니다.
2. 위에 설명된 대로 컴퓨터 또는 원격 서버 중 하나를 선택하여 연결합니다.

초기 구성

시작하려면 다음 사항을 완료해야 합니다.

- 장치를 추가하고 사용자 계정을 생성을 생성합니다. 참조:
- 시스템에 사이버 보안 강화 조치를 적용합니다. 을 참조하십시오.

장치 관리

장치 추가

AXIS Device Manager는 네트워크에서 연결된 장치를 자동으로 검색하고, 모든 장치에 로그인하려고 시도합니다. 검색된 장치 목록에는 장치 주소(IP 주소 또는 호스트 이름), 일련 번호, 모델 및 상태가 표시됩니다. 일련 번호(S/N)는 제품 라벨에 인쇄되어 있습니다.

목록에서 장치를 추가하려면 다음을 수행합니다.

1. 추가할 장치를 선택하고 **Next(다음)**를 클릭합니다.
2. **Use host name when possible(가능한 경우 호스트 이름 사용)**을 선택합니다. 호스트 이름을 사용하여 장치를 추가한 경우 장치와의 모든 통신에서 호스트 이름을 사용합니다. 호스트 이름을 사용할 수 없는 경우 IP 주소를 사용합니다.
3. 패스워드가 없는 장치의 패스워드를 설정합니다. 패스워드가 설정되지 않은 경우 **Skip(건너뛰기)**을 선택합니다.
4. **Next (다음)**를 클릭합니다.

"Ready to add devices(장치 추가 준비 완료)" 페이지에는 추가할 장치들이 표시됩니다.

5. 장치를 추가하려면 **Finish(마침)**를 클릭합니다.

장비 제거

목록에서 장치를 제거하려면 다음을 수행합니다.

1. **Device management(장치 관리)**로 이동합니다.
2. 장치를 선택합니다.
3. 마우스 오른쪽 버튼을 클릭하고 **Remove(제거)**를 선택합니다.
4. **예**를 클릭합니다.

장치 교체하기

AXIS Device Manager에서 장치를 교체하려면 새 장치를 연결하고 기존 장치의 구성을 재사용합니다. 작업이 성공적으로 완료되면 기존 장치는 삭제됩니다. 해당 장치에는 최소 하나 이상의 복원 지점이 있어야 합니다. 를 참조하십시오. 복원 지점은 새 장치로 이동되지 않습니다.

1. **Device management(장치 관리)**로 이동합니다.
2. 도구 모음으로 이동하여 장치 교체 아이콘을 클릭합니다.
3. 교체할 기존 장치를 선택하고 **OK(확인)**를 클릭합니다.
4. 기존 장치와 교체할 새 장치를 선택하고 **OK(확인)**를 클릭합니다.
5. **Next(다음)**를 클릭하여 최신 복원 지점에서 장치 구성을 가져옵니다.
6. **Parameters(매개변수) > Additional Settings(추가 설정)**로 이동하여 적용할 매개변수와 설정을 선택합니다.
7. **Next (다음)**를 클릭합니다.
8. **Finish(마침)**를 클릭하여 설정을 적용합니다.

장치 복원

하나 이상의 장치를 이전에 생성된 복원 지점으로 복원할 수 있습니다. 장치를 복원하려면 해당 장치에 대해 하나 이상의 복원 지점이 존재해야 합니다. 기본적으로 선택한 서버의 모든 장치에 대해 매일 밤 자동 복원 지점이 생성되고 순차적으로 삭제됩니다. 복원을 위해 최근 자동 복원 지점이 정해진 수만큼 유지됩니다.

이전 복원 지점으로 장치 복원:

1. **Device management(장치 관리)** 작업 영역으로 이동합니다.

2. 복원할 장치를 하나 또는 여러 개 선택합니다.
3. 마우스 오른쪽 버튼을 클릭하고 드롭다운 메뉴에서 **Backup / Restore(백업 / 복원) > Restore to a Previous Time(이전 시점으로 복원)**을 선택합니다.
4. 가장 최근 복원 지점 목록에서 복원 지점을 선택하고 **Next(다음)**를 클릭합니다.
5. 각 장치의 설정을 검토한 후 **Finish(마침)**를 클릭합니다.

구성

복원 지점 생성하기

수동 복원 지점을 생성하려면 다음을 수행합니다.

- **Device management(장치 관리)** 작업 영역으로 이동합니다.
- 복원할 장치를 하나 또는 여러 개 선택합니다.
- 마우스 오른쪽 버튼을 클릭하고 **Backup / Restore(백업 / 복원) > Create Restore Points(복원 지점 생성)**를 선택합니다.
- 복원 지점을 식별하는 설명을 입력합니다.
- **OK(확인)**를 클릭합니다.

비고

수동으로 생성된 복원 지점은 자동으로 제거되지 않습니다.

자동 복원 지점 생성하기

서버가 두 개 이상인 경우, 서버 목록에서 구성할 서버를 선택합니다.

- **Options(옵션) > Restore point settings(복원 지점 설정)**로 이동합니다.
- **Create restore points automatically(자동으로 복원 지점 생성)**를 선택하여 자동 복원을 활성화합니다.
- 저장할 자동 복원 지점 개수를 입력하고 **OK(확인)**를 클릭합니다.

여러 자격 증명 관리하기

이 기능은 AXIS Device Manager에 장치의 관리자 계정에 대한 자격 증명을 제공합니다.

수동으로 장치 자격 증명 입력하기

장치 자격 증명을 수동으로 입력하도록 선택하면, 선택한 장치에 대한 자격 증명이 AXIS Device Manager에서 업데이트됩니다.

- 하나 또는 여러 장치 선택하기
- 마우스 오른쪽 버튼을 클릭하고 드롭다운 메뉴에서 **Advanced(고급) -> Enter Device Credentials(장치 자격 증명 입력)**를 선택합니다.

비고

장치에 대해 유효성이 확인되지 않은 자격 증명은 업데이트되지 않습니다. 이러한 작업에 참여하는 모든 장치에는 동일한 사용자 이름과 패스워드를 사용해야 합니다.

다양한 자격 증명을 위해 CSV 파일 사용하기

CSV 파일을 사용하면 각 장치마다 개별 패스워드와 사용자 이름을 사용할 수 있습니다. MAC 주소, IP 주소 또는 호스트 주소는 CSV 파일의 행을 Axis Device Manager 데이터베이스의 해당 장치에 매핑하는 데 사용됩니다.

CSV 파일을 사용할 경우, 사용자 인터페이스가 CSV 파일의 열을 어떻게 해석할지 지정하라고 요청하는 메시지가 표시됩니다.

비고

CSV 파일의 행이 속한 장치를 지정하는 방법.

CSV 파일의 하나의 열에는 MAC 주소, IP 주소 또는 호스트 주소 중 하나가 포함되어야 하므로, CSV 파일의 해당 열을 MAC 주소 또는 IP 주소 또는 호스트 주소로 해석하도록 지정합니다. 이는 CSV 파일의 각 행의 데이터가 속하는 장치를 지정하는 데 필요합니다. 추가로, 하나의 열을 서버 이름으로 해석하도록 지정할 수 있습니다. 이렇게 하면, 서로 다른 AXIS Device Manager 서버에 있지만 동일한 IP 주소 또는 호스트 주소를 사용하는 장치를 대상으로 하는 CSV 파일의 행을 구분할 수 있습니다. 이러한 구분이 필요하지 않은 경우, 서버 이름으로 해석할 열을 둘 필요는 없습니다. 하나의 서버가 여러 장치에 동일한 IP 주소 또는 호스트 주소를 사용하지만 포트를 사용하여 장

치를 구분하는 설정에서는, 해당 열을 포트로 해석하도록 지정할 수 있습니다. 포트에 따른 구분이 필요하지 않다면, 열을 포트로 해석할 필요는 없습니다. 전용 열에 포트를 제공하는 옵션은 IP 주소 또는 호스트 주소와 함께 포트를 제공하는 것입니다. 그런 다음 IP 주소 또는 호스트 주소 뒤에 콜론과 포트 번호를 입력해야 합니다.

인증서 설치

인증서 정보

AXIS Device Manager는 서버/클라이언트 인증서를 관리하기 위한 설정을 제공합니다. 클라이언트 인증서는 IEEE 802.1X에 사용되며, 서버 인증서는 HTTPS에 사용됩니다. 변경 사항을 적용하려면 Device management(장치 관리)에서 해당 장치를 선택한 후 컨텍스트 메뉴에서 Enable update(활성화/업데이트)를 선택합니다.

CA(인증 기관) 생성하기

CA를 통해 서버/클라이언트 인증서가 없는 장치에서 HTTPS 및 IEEE 802.1X를 활성화할 수 있습니다. CA는 장치에 자체 개인 키를 사용하여 인증서를 생성하고 서명한 후 설치하도록 지시합니다.

인증 기관을 생성하려면 다음을 수행합니다.

- **Configuration(구성)** 탭으로 이동합니다.
- **Security(보안) > Certificates(인증서)**로 이동합니다.
- **Certificate authority(인증 기관)**에서 **Generate(생성)를 클릭합니다...**
- 암호 문구를 입력하고 확인합니다.
- **OK(확인)**를 클릭합니다.

이제 CA가 생성되어 사용할 준비가 되었습니다.

비고

선택한 암호 문구로 보호되는 자체 서명 root 인증서와 개인 키입니다. AXIS Device Manager에서 생성된 인증서는 3년간 유효합니다. 서버/클라이언트 인증서를 자동으로 갱신하려면 **Remember passphrase(암호 문구 기억)** 상자를 선택해야 합니다. CA가 설정되어 있지 않은 경우, AXIS Device Manager 외부에서 서버/클라이언트 인증서를 생성해야 합니다. 이 경우 자동 인증서 관리의 이점을 누릴 수 없습니다.

Import(가져오기) – 가져오기 기능을 사용하면 공개 인증서와 개인 키로 구성된 기존 CA를 가져올 수 있습니다. 암호 문구를 입력해야 합니다.

Save to file(파일로 저장) – CA의 공개 인증서를 .cer 또는 .crt 형식으로 저장합니다. 파일은 개인 키가 포함되어 있지 않으므로 암호화되지 않습니다.

Backup(백업) - 하드웨어 장애가 발생할 경우 CA 백업을 권장합니다. 선택 시, Axis Device Manager에서 사용하는 CA의 인증서 및 개인 키 모두가 백업됩니다. 백업된 데이터는 CA를 생성하는 데 사용된 암호 문구로 보호됩니다.

인증서 만료 경고 – 인증서가 만료되었거나 만료 예정일 경우 시스템 알림이 생성됩니다. 이 경고는 AXIS Device Manager 외부에서 설치된 CA를 제외하고, 연결된 장치에 설치된 모든 인증서에 적용됩니다. 이 경고는 시스템 알람으로, Device management(장치 관리)의 상태 열에, "View installed certificates(설치된 인증서 보기)" 대화 상자의 아이콘으로, 그리고 Configuration(구성) 작업 영역에 표시됩니다.

인증서 만료일이 가까워질 때 AXIS Device Manager가 알림을 제공할 시점을 설정합니다. 기본적으로 AXIS Device Manager에서 생성된 서버 및 클라이언트 인증서는 만료 경고가 표시되기 7일 전에 자동으로 갱신됩니다. CA 만료 알림을 받으려면, "Remember passphrase(암호 문구 기억)"를 선택해야 합니다.

HTTPS 활성화

HTTPS를 활성화하려면 각 장치에 서버 인증서가 있어야 합니다. AXIS Device Manager는 장치용 서버 인증서를 서명하고 설치하기 위해 인증 기관(CA)을 사용할 수 있습니다.

수동으로 서명 및 설치할 수도 있습니다.

1. **Device manager(장치 관리자)** 탭으로 이동합니다.
2. 장치를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 각 장치에 대해 **Install server certificates(서버 인증서 설치)**를 선택합니다.

HTTPS를 활성화하기 전에 각 장치에는 하나의 서버 인증서만 있어야 합니다. 초과된 인증서는 컨텍스트 메뉴에서 삭제할 수 있습니다.

3. 인증서를 설치한 후, 컨텍스트 메뉴에서 HTTPS를 활성화할 수 있습니다.

비고

보안 연결(HTTPS)을 사용할 수 없는 경우, HTTPS를 사용하여 연결할 수 있습니다. 이는 아직 보안이 설정되지 않은 장치를 구성할 수 있도록 하기 위한 것입니다.

인증서 검증 무시

장치의 인증서가 검증되지 않으면 AXIS Device Manager는 해당 장치에 연결하지 않습니다. 서버 인증서는 AXIS Device Manager의 활성 CA가 서명하거나 Windows 인증서 저장소를 통해 검증되어야 합니다. Ignore certificate validation(인증서 검증 무시)를 선택하면, AXIS Device Manager는 장치에서 보낸 인증서가 신뢰할 수 있는지 여부를 검증하지 않습니다.

AXIS Device Manager가 인증서 검증을 무시하도록 설정하려면 다음을 수행합니다.

- **Configuration(구성)** 탭으로 이동합니다.
- **HTTPS** 항목에서 **Ignore certificate validation(인증서 검증 무시)**를 활성화합니다.

802.1X 활성화

IEEE 802.1X를 활성화하려면 각 장치에 클라이언트 인증서가 있어야 합니다. AXIS Device Manager는 장치용 클라이언트 인증서를 서명하고 설치하기 위해 인증 기관(CA)을 사용할 수 있습니다.

또는 Device management(장치 관리)에서 장치를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 각 장치에 대해 클라이언트 인증서 설치를 선택하여 수동으로 설치할 수도 있습니다. IEEE 802.1X를 활성화하기 전에 각 장치에는 하나의 클라이언트 인증서만 있어야 합니다. 초과된 인증서는 컨텍스트 메뉴에서 삭제할 수 있습니다. 인증서를 설치한 후, 컨텍스트 메뉴에서 IEEE 802.1X를 활성화할 수 있습니다.

IEEE 802.1X 프로토콜을 사용하려면 IEEE 802.1X 인증 CA 인증서도 필요합니다.

EAPOL 버전 - 사용할 EAP(Extensible Authentication Protocol)의 버전을 선택합니다.

EAP ID - 장치의 MAC 주소, 호스트 이름 또는 사용자 지정 텍스트 중 하나를 입력합니다.

사용자 지정 - EAP ID로 기능할 텍스트를 입력합니다.

IEEE 802.1X 인증 CA 인증서 - 클라이언트 인증서 외에도 IEEE 802.1X 인증 CA 인증서를 설치해야 합니다. IEEE 802.1X를 활성화하려면 개인 키가 아닌 공개 인증서만 필요하므로 암호 문구를 입력할 필요가 없습니다. IEEE 802.1X를 활성화하거나 업데이트하면 IEEE 802.1X 인증 CA 인증서가 설치됩니다..

Import(가져오기) – 장치에 설치되고 인증 서버를 검증하는 데 사용할 CA 인증서를 선택합니다. CA 인증서는 AXIS Device Manager의 CA에서 생성되었거나 외부 출처에서 가져올 수 있습니다.

View(보기) – IEEE 802.1X 인증 과정에서 사용되는 CA 인증서의 세부 정보.

Common name(일반 이름) – 장치 EAP ID 또는 장치 IP 주소 중 하나를 선택합니다. 사용자 지정 필드를 비워두면 호스트 이름이 선택됩니다. 호스트 이름에 문제가 있을 경우, 일반 이름으로 IP 주소가 사용됩니다.

SIP 계정 관리하기

장치 소프트웨어 관리

AXIS OS 업그레이드

새로운 AXIS OS 버전은 두 가지 방법으로 구할 수 있습니다.

- AXIS Device Manager를 사용하여 다운로드(인터넷 접속 필요)
- 하드 드라이브 또는 메모리 스틱 등의 파일에서 가져오기

비고

AXIS OS 권장 업그레이드 경로를 따르는 것이 좋습니다. 자세한 내용은 *https://help.axis.com/axis-os#upgrade-path*를 참조하십시오.

AXIS OS 수동 업그레이드

1. 새 AXIS OS 버전으로 업그레이드할 장치를 선택하고 마우스 오른쪽 버튼을 클릭한 후 **Upgrade firmware(펌웨어 업그레이드)**를 선택합니다.
2. 업그레이드 중에 장치에 액세스할 수 없게 된다는 알림이 표시되면 **Yes(예)**를 클릭합니다.
3. 다운로드 가능한 펌웨어 버전 목록을 업데이트하려면 **Upgrade firmware(펌웨어 업그레이드)** 대화 상자에서 **Check for Updates(업데이트 확인)**를 클릭합니다.
4. 로컬 클라이언트에 저장된 하나 이상의 AXIS OS 버전 파일을 찾아보려면 **Browse(찾아보기)** 버튼을 클릭합니다.
5. 업그레이드할 장치와 AXIS OS 버전을 선택합니다.
6. AXIS OS 업그레이드 중에 선택한 장치를 공장 출하 시 기본값으로 설정하려면 **Factory default checkbox(공장 출하 시 기본값 확인란)**를 클릭합니다. 이는 일부 AXIS OS 버전을 다운그레이드할 때 요구되는 사항입니다.
7. **OK(확인)**를 클릭하면 목록의 선택한 장치를 업그레이드합니다.

비고

기본적으로 선택한 모든 장치에 대한 AXIS OS 업그레이드가 동시에 수행됩니다. 업그레이드 순서는 **Configuration(구성) > Connected Services(연결된 서비스) > Firmware upgrade settings(펌웨어 업그레이드 설정)**에서 변경할 수 있습니다.

자동 업그레이드

AXIS Device Manager 5의 기본 설정은 펌웨어 업그레이드를 확인하지 않도록 되어 있지만, 서버 또는 axis.com에서 AXIS OS 업그레이드가 있는지 자동으로 확인하도록 설정할 수 있습니다.

AXIS OS 업그레이드를 수동으로 확인하려면 액션 메뉴에서 **Check now(지금 확인)** 버튼을 누릅니다.

AXIS OS 업그레이드 순서

AXIS OS 업그레이드는 모든 장치에서 동시에 완료하거나 한 장치씩 순차적으로 완료할 수 있습니다.

- 모든 장치를 한 번에 업그레이드하려면 **Parallel(병렬)** 업그레이드 순서를 선택합니다.
- 장치를 순차적으로 업그레이드하려면 **Sequential(순차)**을 선택합니다. 이 옵션은 시간이 더 오래 걸리지만 장치가 동시에 오프라인 상태로 되지 않습니다. 문제가 발생할 경우 순차 업그레이드를 중단하려면 **Cancel all remaining upgrades if one device fails(장치 하나가 실패하면 나머지 업그레이드 모두 취소)** 확인란을 선택할 수도 있습니다.

문제 해결

지원 센터 문의

지원팀에 문의할 때, 먼저 티켓을 생성하고 시스템 보고서 파일을 첨부하면 문제 해결이 수월해집니다.

1. 메인 메뉴로 이동합니다.
2. **Help(도움말) > System Report...(시스템 보고서...)**로 이동합니다.
3. 선택한 폴더에 보고서 파일을 저장합니다.
4. *axis.com/support*로 이동합니다.
5. 지원 티켓을 생성합니다.
6. 해당 파일을 지원 티켓에 첨부합니다.

비고

응답하지 않는 시스템에서 시스템 보고서를 생성하려면 다음을 수행합니다.

1. `C:\ProgramData\Axis Communications\`로 이동합니다.
2. 해당 폴더의 내용을 .zip 파일로 압축하여 지원 티켓에 첨부합니다.

에스컬레이션 프로세스

본 가이드로 해결할 수 없는 문제가 있으면 Axis 온라인 헬프데스크로 문제를 이관합니다. *Axis 온라인 헬프데스크*를 참조하십시오. 지원 부서에서 문제를 파악하여 해결할 수 있도록 다음 정보를 포함해야 합니다.

- 문제를 재현하는 방법이나 문제가 발생하는 상황에 대한 명확한 설명입니다.
- 문제가 발생한 시간과 해당 장치의 이름 또는 IP 주소가 필요합니다.
- AXIS Device Manager 시스템 보고서는 문제 발생 직후 생성되어야 합니다. 문제가 재현된 클라이언트나 서버에서 시스템 보고서를 생성해야 합니다.
- 문제를 보여주는 선택형 스크린샷 또는 녹화물
- 필요한 경우 데이터베이스 파일을 포함합니다. 업로드 속도를 높이려면 이런 항목들을 제외합니다.

일부 문제에는 필요한 경우 지원 부서에서 추가 정보를 요청하기도 합니다.

비고

네트워크 추적 또는 데이터베이스 파일과 같이 100MB보다 큰 파일은 신뢰성 있는 보안 파일 공유 서비스를 사용하여 전송합니다.

추가 정보	
디버그 수준 로그	때로는 디버그 수준 로깅을 사용하여 더 많은 정보를 수집하기도 합니다. 이는 Axis 지원 엔지니어의 요청에 따라서만 실행됩니다. *Axis 온라인 헬프데스크*에서 지침을 찾을 수 있습니다.
네트워크 추적	지원 엔지니어의 요청이 있는 경우 시스템 보고서를 만들 때 네트워크 추적을 생성합니다. 재현 가능한 경우 문제가 발생한 시간에 네트워크를 추적합니다. 여기에는 다음과 같은 내용이 포함됩니다. • 카메라에서 이루어진 60초 네트워크 추적입니다(펌웨어 5.20 이상에만 해당). 필요한 경우 다음 VAPIX 명령을 사용하여 로그인, IP 주소 및 기간(초) 변경: `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60`

추가 정보	
	• 서버와 카메라 간의 통신을 표시하는 서버에서 촬영한 10~30초 분량의 네트워크 추적입니다.
데이터베이스 파일	데이터베이스를 검사하거나 수동으로 복구해야 하는 경우입니다. 시스템 보고서를 생성하기 전에 **Include database in the report(보고서에 데이터베이스 포함)**를 선택합니다.
스크린샷	UI와 관련된 실시간 보기 문제인 경우 스크린샷을 사용합니다. 예를 들어, 녹화 타임라인을 표시하고 싶거나 설명하기 어려운 경우입니다.
화면 녹화	예를 들어, 문제를 재현하기 위해 많은 UI 상호 작용이 관련된 경우와 같이 문제를 말로 설명하기 어려우면 화면 녹화를 사용합니다.

T10211981_ko

2025-09 (M3.2)