AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

사용자 설명서

목차

AXIS Optimizer 7
AXIS Optimizer의 사용 목적 7
시스템 요구 사항 7
연합 시스템을 지원 7
상호 연계 시스템을 지원 7
릴리스 정보 7
AXIS Optimizer 설치 또는 업데이트 8
AXIS Optimizer 설치 8
내 시스템에는 어떤 버전이 설치되어 있습니까? 8
고급 설치 옵션 8
VMS 마이그레이션 9
설치 프로그램 무결성 확인 9
AXIS Optimizer 업데이트 9
수동 업데이트 10
자동으로 시스템 업그레이드 10
자동 업그레이드 켜기 10
자동 업그레이드 끄기 11
상세 정보 11
AXIS Optimizer 제거 11
Factory default(공장 출하 시 기본값): 11
안전한 폐기 11
사용자 권한 12
접근 장치 설정 13
장치 도우미 13
Axis 장치 구성 13
Axis 장치에 애플리케이션 설치 13
Axis 장치에서 애플리케이션 구성 13
Axis 장치에서 애플리케이션 업데이트 13
Axis 장치 재시작 13
Axis 장치의 IP 주소 복사 14
자동화 수행 15
Axis 장치에 대한 액션을 생성 15
이벤트 서버 플러그인 15
이벤트 서버에 플러그인 설치 15
한 번의 클릭으로 여러 대의 카메라 건조 15
한 번의 클릭으로 여러 대의 카메라에 대한 오토 포커스 켜기 16
한 번의 클릭으로 여러 개의 스트로브 사이렌을 트리거 17
여러 대의 카메라에서 자동으로 특정 영역 감시 차단(프라이버시 마스크) 끄기 18
카메라가 모션을 감지하면 스트로브 사이렌을 활성화 20
카메라가 모션을 감지하면 스피커 또는 스피커 영역에서 오디오 클립 재생 21
룰 문제 해결 23
번호판 목록을 중앙에서 관리 23
목록 만들기 23
목록 권한 구성 23
목록 편집 24
목록 가져오기 24
목록 내보내기 25
목록에 대해 자세히 알아보기 26
실시간 이벤트에 대응 27
장치 컨트롤을 사용 27
운영자 제어 27
운영자 제어에 액세스 27
PTZ 카메라의 포커스 영역 저장 27

카메라 오토 포커스 ... 28
Speed Dry 또는 와이퍼 켜기 ... 28
스팟 온도 측정 ... 29
움직이는 물체를 자동으로 확대하고 추적합니다 ... 29
사용자 지정 운영자 컨트롤 생성 ... 30
운영자 제어에 대한 액세스 구성 ... 30
스피커를 통해 상호 작용 ... 30
스피커 관리자 ... 30
모드 ... 31
AXIS Audio Manager Pro 모드 ... 31
AXIS Audio Manager Edge 모드 ... 32
Legacy mode(레거시 모드) ... 33
스피커에서 오디오 재생 ... 35
카메라 보기에서 스피커로 오디오 재생 ... 35
알람에서 스피커로 오디오 재생 ... 35
스피커 상호 작용에 대한 시각적 동작 설정 ... 35
카메라 보기 또는 알람의 오디오 클립 북마크 ... 36
방문자 관리 ... 36
인터콤 플러그인 ... 36
인터콤 설정 ... 36
인터콤에 대한 권한 설정 ... 37
테스트 전화 걸기 ... 38
통화 중 에코 방지 ... 38
실시간 보기에서 인터콤 제어 ... 39
실시간 보기에서 콜에 응답 ... 41
호출 창에 여러 대의 카메라 표시 ... 42
통화 창 액션 ... 43
호출 창에 페이지 표시 ... 43
콜 내선 번호 필터링 ... 43
콜 기록 보기 ... 44
활성화된 호출가 없을 때 마이크 끄기 ... 45
강제로 도어가 열리면 알람을 수신 ... 46
도어가 너무 오래 열려 있을 경우 알람 수신 ... 46
클라이언트의 전화 수신 방지 ... 46
오디오 시각화 ... 46
마이크 보기 ... 46
마이크 보기용 VMS 구성 ... 47
Smart Client에 마이크 보기 추가 ... 47
마이크 보기 사용 ... 47
동시에 여러 마이크 듣기 ... 48
오디오로 사건을 디텍션 ... 48
사건이 발생한 후 조사 ... 48
포렌식 검색 ... 49
포렌식 검색 ... 49
시작하기 전 ... 49
포렌식 검색 구성 ... 49
검색 수행 ... 50
검색 미세 조정 ... 51
제한 사항 ... 51
차량 검색 ... 52
차량 검색 구성 ... 54
차량 검색 ... 54
검색 미세 조정 ... 54
검색 속도 최적화 ... 55
영역 속도 검색 ... 55
구역 속도 검색 구성 ... 55

구역 속도 이벤트 검색 ... 56
검색 미세 조정 ... 56
컨테이너 검색 ... 57
컨테이너 검색 구성 ... 57
컨테이너 검색 ... 57
검색 미세 조정 ... 58
고품질 PDF 보고서 생성 ... 58
Axis 번호판 ... 58
시작하기 전 ... 59
Axis 번호판 구성 ... 59
번호판 검색 ... 59
실시간 번호판 검색 ... 59
검색 미세 조정 ... 60
검색 속도 최적화 ... 60
번호판 검색 결과를 PDF 보고서로 내보내기 ... 60
번호판 검색 결과를 CSV 보고서로 내보내기 ... 61
Axis insights ... 61
Axis insights 접근 ... 61
새 스케줄 생성 ... 61
대시보드 드롭다운 목록 구성 ... 62
특정 카메라 보기의 인사이트 표시 ... 62
Axis insights 구성 ... 62
Axis insights 문제 해결 ... 63
비디오 디워핑 ... 64
디워핑 보기 생성 ... 64
멀티 센서 파노라마 카메라를 위한 디워핑 보기 생성 ... 65
와이드 뷰 ... 66
홈 위치 설정 ... 66
운영자가 디워핑 보기를 제어하고 편집할 수 있도록 허용 ... 67
성능 및 문제 해결 ... 67
신체 착용 통합 ... 69
상세 정보 ... 69
접근 제어 ... 70
접근 제어 구성 ... 70
시스템에 Axis 네트워크 도어 컨트롤러 추가 ... 70
도어 라이센스 활성화 ... 71
접근 제어를 구성합니다 ... 71
접근 제어 통합 ... 71
도어 및 영역 ... 72
도어 및 영역의 예 ... 73
도어를 추가합니다 ... 73
도어 설정 ... 75
도어 보안 수준 ... 75
시간 옵션 ... 77
도어 모니터 추가 ... 77
모니터링 도어 추가 ... 78
리더 추가 ... 78
REX 장치 추가 ... 80
영역 추가 ... 80
영역 보안 수준 ... 81
관리된 입력 ... 82
수동 액션 ... 83
카드 형식 및 PIN ... 83
카드 형식 설정 ... 85
식별 프로파일 ... 86
암호화된 통신 ... 87

OSDP 보안 채널 ... 87
다중 서버 BETA ... 88
작업 흐름 ... 88
하위 서버에서 구성 파일 생성 ... 88
구성 파일을 주 서버로 가져오기 ... 88
하위 서버 취소 ... 88
하위 서버 제거 ... 88
접근 관리 ... 89
접근 관리의 작업 흐름 ... 89
카드 소지자 추가 ... 89
자격 증명 추가 ... 90
그룹 추가 ... 92
접근 룰을 추가합니다 ... 93
도어 및 구역 수동 잠금 해제 ... 93
시스템 구성 보고서 내보내기 ... 93
카드 소지자 활동 보고서 생성 ... 94
액세스 관리 설정 ... 95
가져오기 및 내보내기 ... 95
백업 및 복원 ... 96
Smart Client에서 접근 관리 ... 97
AXIS Secure Entry 역할 설정 ... 97
시스템 관리 및 보안 통제 ... 98
운영자의 기능 액세스를 위한 사용자 정의 ... 98
역할 설정 ... 98
역할 설정을 구성 ... 98
장치 관리 ... 99
AXIS Device Manager Extend ... 99
엣지 호스트 설치 ... 99
에지 호스트를 요청하고 장치 동기화 ... 99
AXIS Device Manager Extend를 사용하여 장치 구성 ... 100
에지 호스트에 장치 추가 문제 해결 ... 101
AXIS Site Designer 가져오기 ... 101
설계 프로젝트 가져오기 ... 101
가져온 설정 ... 102
제한 사항 ... 102
계정 관리 ... 102
XProtect 서비스 계정으로 장치에 연결 ... 102
Axis 이벤트 ... 103
여러 장치의 이벤트 설정 ... 103
이벤트 정보 ... 103
메타데이터와 검색 ... 103
메타데이터 설정 구성 ... 104
Axis 검색 카테고리 구성 ... 105
사이버 보안 ... 106
취약성 관리 ... 106
보안 알림 ... 106
보안 제품 수명 주기 ... 106
보안 강화 가이드 ... 106
도움이 더 필요하십니까? ... 107
FAQ ... 107
문제 해결 ... 107
지원 센터 문의 ... 107
팁과 요령 ... 108
Smart Client 보기에서 웹 페이지 추가 ... 108
내장된 검색 기능으로 비디오 내보내기 ... 108
XProtect 형식으로 비디오 내보내기 ... 108

수신 컴퓨터에서 내보내기 블럭 해제 108
내보낸 Axis 디워프 보기 재생하기 108

AXIS Optimizer

AXIS Optimizer는 XProtect 또는 Siemens Siveillance Video에서 Axis 솔루션의 다양한 기능을 사용할 수 있도록 해줍니다. 이 애플리케이션은 이러한 비디오 관리 시스템에서 Axis 장치의 성능을 최적화하므로 시스템을 구성하거나 일상적인 작업 중에 시간과 노력을 모두 절약할 수 있습니다. 애플리케이션은 무료입니다.

AXIS Optimizer의 사용 목적

이 제품은 VMS(영상 관리 시스템) 운영에 대한 폭넓은 지식을 갖춘 전문가가 사용하도록 설계되었습니다.

시스템 요구 사항

AXIS Optimizer는 다음 플랫폼에서 완벽하게 지원됩니다.

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

최신 버전의 Management Client 및 Smart Client 사용을 권장합니다. AXIS Optimizer의 최신 버전은 항상 테스트를 거쳤으며, VMS의 최신 버전과 호환됩니다. 자세한 내용은 *릴리스 정보, on page 7*을 참조하십시오.

비고

최소 지원 플랫폼

- VMS 버전 2019 R3.

도움말에서 Smart Client는 Siemens 시스템의 XProtect Smart Client와 Video Client를 모두 의미합니다.

연합 시스템을 지원

AXIS Optimizer는 연합 시스템에서 완벽하게 지원됩니다.

상호 연계 시스템을 지원

AXIS Optimizer는 상호 연계 시스템에서 완전히 지원됩니다.

비고

요구 사항

- VMS 버전 2022 R3 이상.

릴리스 정보

최신 릴리스 정보를 보려면 *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*로 이동하십시오.

AXIS Optimizer 설치 또는 업데이트

AXIS Optimizer 설치



비고

AXIS Optimizer를 업데이트하려면 관리자 권한이 있어야 합니다.

1. VMS의 올바른 클라이언트 버전이 있는지 확인하십시오.
2. MyAxis 계정에 로그인합니다.
3. *axis.com/products/axis-optimizer-for-milestone-xprotect*에서 Management Client 또는 Smart Client를 실행하는 각 장치에 AXIS Optimizer를 다운로드합니다.
4. 다운로드한 파일을 실행하고 단계별 가이드의 지침을 따릅니다.

내 시스템에는 어떤 버전이 설치되어 있습니까?

System overview(시스템 오버뷰)에서 시스템의 다른 서버와 클라이언트에 설치된 AXIS Optimizer 및 AXIS Optimizer Body Worn Extension 버전을 확인할 수 있습니다.

비고

System overview(시스템 오버뷰)에서 시스템의 클라이언트 또는 서버를 보려면 AXIS Optimizer 버전 3.7.17.0, AXIS Optimizer Body Worn Extension 버전 1.1.11.0 이상이 있어야 합니다.

활성 서버 및 클라이언트를 보려면:

1. Management Client에서 **Site Navigation > AXIS Optimizer > System overview(사이트 탐색 > AXIS Optimizer > 시스템 개요)**로 이동합니다.

특정 서버 또는 클라이언트를 업그레이드하려면:

1. 해당 특정 서버 또는 클라이언트로 이동하여 로컬로 업그레이드하십시오.

고급 설치 옵션

사용자 상호 작용 없이 동시에 여러 장치에 AXIS Optimizer를 설치하려면:

1. **Start(시작)** 메뉴를 마우스 오른쪽 버튼으로 클릭합니다.
2. **실행**을 클릭합니다.
3. 다운로드한 설치 파일을 탐색하고 **Open(열기)**을 클릭합니다.
4. 경로 끝에 하나 이상의 매개변수를 추가합니다.

매개변수	설명
`/SILENT`	자동 설치 중에는 단계별 가이드와 배경 창이 표시되지 않습니다. 그러나 설치 진행률 창이 표시됩니다.
`/VERYSILENT`	매우 자동 설치 중에는 단계별 가이드와 배경 창 또는 설치 진행률 창이 표시되지 않습니다.
`/FULL`	선택 사항인 이벤트 서버 플러그인과 Secure Entry 플러그인 등 모든 구성 요소를 설치하십시

	오. 이는 /VERYSILENT와 함께 사용하면 유용합니다.
/SUPPRESSMSGBOXES	모든 메시지 상자를 표시하지 않습니다. 이는 일반적으로 /VERYSILENT와 함께 사용됩니다.
/log=<filename>	로그 파일을 생성합니다.
/NORESTART	설치 중에 컴퓨터가 다시 시작되지 않도록 합니다.
/EVENTSERVERPLUGIN	대상 시스템이 이벤트 서버인 경우 이벤트 서버 플러그인을 설치하십시오.
/SECUREENTRY	대상 시스템이 이벤트 서버인 경우 Secure Entry 접근 제어 서비스를 설치하십시오.

5. **Enter(입력)**을 누릅니다.

예:
컴퓨터를 다시 시작하지 않고 매우 자동 설치, output.txt에 기록됨

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

VMS 마이그레이션

AXIS Optimizer는 대부분의 데이터를 VMS 데이터베이스에 저장하므로 VMS를 다른 서버로 마이그레이션할 때 정보가 유지됩니다.

VMS를 다른 서버로 마이그레이션하려면 *기존 서버에서 새 서버로 XProtect VMS 설치본/버전을 이동하는 방법*을 참조하십시오.

설치 프로그램 무결성 확인

AXIS Optimizer 설치 프로그램의 무결성을 확인하는 방법:

1. 설치 프로그램 파일을 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 선택합니다.
2. **Digital Signatures(디지털 서명)**로 이동하고 **Details(세부 정보)**를 클릭합니다.
3. 다음을 확인합니다.
   - **Digital Signature Information(디지털 서명 정보)**에 This digital signature is OK(이 디지털 서명은 정상입니다)라고 표시됩니다.
   - **Signer information(서명자 정보)** > **Name(이름)**에 Axis Communications AB라고 표시됩니다.

AXIS Optimizer 업데이트

AXIS Optimizer는 새로운 기능, 개선 사항 및 보안 업그레이드를 통해 정기적으로 업데이트됩니다. AXIS Optimizer는 단일 릴리스 트랙(최신 버전)만 제공하며, axis.com에서 다운로드할 수 있는 것은 이 최신 버전뿐입니다. 항상 최신 버전의 AXIS Optimizer를 사용할 것을 권장합니다.

AXIS Optimizer에는 VMS의 모든 클라이언트를 업데이트할 수 있는 기능도 포함되어 있습니다. 자세한 내용은 *시스템 자동 업그레이드*를 참조하십시오.

비고
AXIS Optimizer를 업데이트하려면 관리자 권한이 있어야 합니다.

업데이트 알림

AXIS Optimizer는 자체적으로 새 버전을 정기적으로 확인하고 새 업데이트가 있을 때 알려줍니다. 네트워크에 연결되어 있으면 Smart Client에서 업데이트 알림을 받게 됩니다.

수신하는 알림 유형을 변경하는 방법:

1. Smart Client에서 **Settings(설정)** > **Axis general options(Axis 일반 옵션)** > **Notification preference(알림 기본 설정)**로 이동합니다.
2. **All(모두)**, **Major(주요)** 또는 **None(없음)**을 선택합니다.

VMS 내의 모든 클라이언트에 대해 이러한 알림을 구성하는 방법:

1. **Management Client** > **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **System overview(시스템 오버뷰)**로 이동합니다.
2. **System upgrade settings(시스템 업그레이드 설정)**를 클릭합니다.
3. **Show upgrade notifications on all clients(모든 클라이언트에 업그레이드 알림 표시)**를 켜거나 끕니다.

수동 업데이트

Management Client와 Smart Client 모두에서 AXIS Optimizer를 수동으로 업데이트할 수 있습니다.

비고

AXIS Optimizer를 업데이트하려면 관리자 권한이 있어야 합니다.

Management Client에서

1. **Site Navigation > Basics > AXIS Optimizer(사이트 탐색 > 기본 > AXIS Optimizer)**로 이동합니다.
2. **Update(업데이트)**를 클릭합니다.

Smart Client에서

1. **Settings > Axis general options(설정 > Axis 일반 옵션)**으로 이동합니다.
2. **Update(업데이트)**를 클릭합니다.

자동으로 시스템 업그레이드

VMS 관리 서버에서 로컬 AXIS Optimizer 버전을 시스템에 게시할 수 있습니다. 이렇게 하면, AXIS Optimizer가 모든 클라이언트 장비에서 자동으로 업그레이드됩니다. 자동 업그레이드는 작업자의 작업을 방해하지 않습니다. 자동 설치는 시스템 또는 VMS 클라이언트가 재시작되는 동안 수행됩니다. 클라이언트가 인터넷에 연결되어 있지 않은 경우에도 자동 업그레이드가 지원됩니다.

비고

AXIS Optimizer 4.4 이상을 실행하는 클라이언트에 대해 자동 업그레이드가 지원됩니다.

자동 업그레이드 켜기



비고

요구 사항

- Management Client가 VMS 관리 서버와 동일한 시스템에서 실행되는 시스템입니다.
- VMS 관리 서버에 대한 PC 관리자 권한.

자동 업그레이드를 켜려면 특정 AXIS Optimizer 버전을 시스템에 게시해야 합니다.

1. VMS 관리 서버에서 전체 시스템에 게시하려는 AXIS Optimizer 버전을 설치합니다.

2. VMS 관리 서버 시스템에서 Management Client를 엽니다.
3. **Site Navigation > AXIS Optimizer > System Overview(사이트 탐색 > AXIS Optimizer > 시스템 오버뷰)**로 이동합니다.
4. **System upgrade settings(시스템 업그레이드 설정)**를 클릭합니다.
5. **Local version(로컬 버전)**이 정확한지 확인하고 **Publish(게시)**를 클릭합니다.
   게시된 AXIS Optimizer 버전이 이미 있는 경우 새 버전으로 대체됩니다.

비고

4.4보다 이전 버전의 AXIS Optimizer가 설치된 클라이언트 시스템은 수동으로 업그레이드해야 합니다.

자동 업그레이드 끄기

자동 업그레이드를 끄려면 게시된 버전을 재설정해야 합니다.

1. VMS 관리 서버 시스템에서 Management Client를 엽니다.
2. **Site Navigation > AXIS Optimizer > System Overview(사이트 탐색 > AXIS Optimizer > 시스템 오버뷰)**로 이동합니다.
3. **System upgrade settings > Reset published version(시스템 업그레이드 설정 > 게시된 버전 재설정)**을 클릭합니다.

상세 정보

- AXIS Optimizer가 없는 Smart Clients는 관리 서버 웹 페이지(*http://[serveradress]/installation/*) 인터넷에 연결되어 있지 않은 경우에도 마찬가지입니다.
- AXIS Optimizer 설치 패키지는 VMS의 다운로드 관리자에서 사용 가능하고 구성할 수 있습니다.
- 연합 또는 상호 연결된 시스템에서는 각 관리 서버에 AXIS Optimizer를 게시해야 합니다.
- AXIS Optimizer의 새 버전을 게시한 후 어떤 클라이언트가 게시된 버전으로 업데이트되었는지 모니터링할 수 있습니다. **System overview(시스템 오버뷰)**에서 게시된 버전을 실행할 때 장치 페이지는 녹색 확인 기호가 표시됩니다.
- VMS 관리 서버를 실행하는 시스템에서는 자동 업그레이드가 해제됩니다.

AXIS Optimizer 제거

Factory default(공장 출하 시 기본값):

AXIS Optimizer를 기본 상태로 재설정하려면 VMS에서 제거한 후 다시 설치합니다.

안전한 폐기

VMS에서 AXIS Optimizer와 저장된 데이터를 완전히 제거하려면 로컬 컴퓨터에서 제거하기 전에 해당되는 경우 다음 단계를 먼저 수행해야 합니다.

1. 번호판 목록을 제거하는 방법:
   - Management Client를 열고 **AXIS Optimizer** > **License plate lists(번호판 목록)**로 이동합니다.
   - 목록에서 모든 사이트를 제거합니다.
2. AXIS Audio Manager Pro 서버의 연결을 끊는 방법:
   - Management Client를 열고 **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동합니다.
   - **Disconnect(연결 해제)**를 클릭합니다.

로컬 컴퓨터에서 AXIS Optimizer와 로컬 컴퓨터에 저장된 데이터를 제거하는 방법:

1. **Start menu(시작 메뉴)** > **Settings(설정)** > **Apps(앱)** > **Installed apps(설치된 앱)**를 클릭합니다.
2. **AXIS Optimizer**로 이동합니다.
3. p,255mm,sfx)=″graphics:graphicBEF7A01B23D95F074530E51119754E17″를 클릭하고 **Uninstall(제거)**을 선택합니다.

비고

AXIS Optimizer를 제거한 후 일부 VMS 서비스를 다시 시작해야 할 수 있습니다.

사용자 권한

AXIS Optimizer에는 특정 Axis Optimizer 사용자 역할이 포함됩니다. 목적은 사용자가 AXIS Optimizer의 기능을 사용하는 데 필요한 Smart Client 권한을 쉽게 부여할 수 있도록 하는 것입니다.

XProtect 2018 R3 또는 이전 버전을 실행하는 경우 이 역할은 XProtect Corporate에서만 사용할 수 있습니다.

XProtect 2019 R1 이상을 실행하는 경우 이 역할은 다음 XProtect 에디션에서 사용할 수 있습니다.

- 기업
- 전문가
- 프로페셔널+
- 에센셜+
- Express+

권한을 수동으로 구성하려면, 이 구성을 사용하여 Smart Client 운영자가 AXIS Optimizer에 포함된 모든 기능을 사용할 수 있도록 합니다.

- 하드웨어: 드라이버 명령
- 카메라: AUX 명령

비고

고급 사용자 역할 처리는 *운영자의 기능 액세스를 위한 사용자 정의, on page 98*을(를) 참조하십시오.

접근 장치 설정

장치 도우미

장치 도우미를 사용하여 VMS Management Client에서 직접 모든 Axis 장치 설정에 쉽게 액세스할 수 있습니다. VMS 내에서 Axis 장치 웹 페이지를 쉽게 찾아 접속하여 다양한 장치 설정을 변경할 수 있습니다. 장치에 설치된 애플리케이션을 구성할 수도 있습니다.

중요 사항

- 장치 도우미를 사용하려면 Axis 장치가 관리 클라이언트와 동일한 네트워크에 연결되어 있어야 합니다.
- Device Assistant는 IPv6 네트워크에서 지원되지 않습니다.

Axis 장치 구성

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 선택하고 **장치 설정** 으로 이동하십시오. 장치 웹 페이지가 열립니다.
3. 원하는 설정을 구성합니다.

Axis 장치에 애플리케이션 설치

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 선택하고 **장치 설정** 으로 이동하십시오. 장치 웹 페이지가 열립니다.
3. **Apps(앱)**로 이동합니다. **앱** 기능이 있는 곳은 장치의 소프트웨어 버전에 따라 다릅니다. 자세한 내용은 애플리케이션 도움말을 참조하십시오.
4. 원하는 애플리케이션을 설치합니다.

Axis 장치에서 애플리케이션 구성

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 선택하고 **애플리케이션**으로 이동하십시오. 장치에 설치된 애플리케이션이 있으면 여기에 표시됩니다.
3. 관련 애플리케이션으로 이동합니다(예: AXIS Object Analytics).
4. 필요에 맞게 애플리케이션을 구성합니다.

Axis 장치에서 애플리케이션 업데이트

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 마우스 오른쪽 버튼으로 클릭하고 **Show updates(업데이트 나타내기)**를 선택합니다. 업데이트할 수 있는 애플리케이션이 있으면 사용 가능한 업데이트 목록이 표시됩니다.
3. 업데이트 파일을 다운로드합니다.
4. **How to update(업데이트하는 방법)**을 클릭하고 지시를 따르십시오.

Axis 장치 재시작

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 마우스 오른쪽 버튼으로 클릭하고 **Restart device(장치 다시 시작)**를 선택합니다.

Axis 장치의 IP 주소 복사

1. 관리 클라이언트에서 **사이트 탐색 > AXIS Optimizer > 장치 도우미(Site Navigation > AXIS Optimizer > Device assistant)**로 이동합니다.
2. 장치를 마우스 오른쪽 버튼으로 클릭하고 **Copy device address(장치 주소 복사)**를 선택합니다.

자동화 수행

Axis 장치에 대한 액션을 생성

이벤트 서버 플러그인

AXIS Optimizer 이벤트 서버 플러그인을 사용하면 Axis 장치에 대한 사용자 정의 작업을 생성할 수 있습니다. XProtect 룰 엔진과 이벤트 서버 플러그인을 사용할 때 다음을 수행할 수 있습니다.

- 운영자가 Smart Client에서 버튼을 클릭할 때 사용자 지정 액션을 수행합니다. 설정 예는, *한 번의 클릭으로 여러 대의 카메라 건조, on page 15*을(를) 참조하십시오.
- 사람의 개입 없이 액션을 수행합니다(자동화). 설정 예는, *여러 대의 카메라에서 자동으로 특정 영역 감시 차단(프라이버시 마스크) 끄기, on page 18*을(를) 참조하십시오.

이벤트 서버 플러그인은 두 부분으로 구성됩니다.

- 이벤트 서버에서 실행되는 별도의 플러그인입니다. 그러면 룰 엔진이 새로운 액션으로 채워집니다.
- 새로운 **액션 프리셋**을 생성할 수 있는 관리 서버의 Axis 액션이라는 페이지입니다.

Axis 장치에 대한 사용자 지정 작업은 다음과 같습니다. 운영자 제어 실행, 레이더 켜기/끄기, 인터콤 호출 시작 및 카메라 건조(SpeedDry/wiper).

이벤트 서버 플러그인은 AXIS Optimizer에 포함되어 있습니다. 다중 PC 시스템에서는 관리 클라이언트 시스템과 이벤트 서버 시스템 모두에 AXIS Optimizer를 설치해야 합니다.

이벤트 서버에 플러그인 설치

이벤트 서버 플러그인은 AXIS Optimizer 설치 프로그램에 포함된 선택적 구성 요소입니다. 비디오 관리 시스템(VMS) 이벤트 서버에만 설치할 수 있습니다. 요구 사항이 충족되면 AXIS Optimizer 설치 프로그램을 실행할 때 이벤트 서버 플러그인을 설치하라는 옵션이 표시됩니다.

비고

VMS 이벤트 서버는 설치 중 그리고 때때로 AXIS Optimizer를 업그레이드하는 동안 잠시 다시 시작해야 합니다. 이 경우 알림을 받게 됩니다.

한 번의 클릭으로 여러 대의 카메라 건조

이벤트 서버 플러그인을 사용하면 운영자가 더 쉽게 사용할 수 있도록 사용자 정의 룰을 설정할 수 있습니다. 이 예에서는 오버레이 버튼을 클릭하여 특정 영역의 모든 카메라를 건조시키는 방법을 보여줍니다.



비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.0 이상
- SpeedDry 또는 Wiper를 지원하는 하나 이상의 카메라(예: AXIS Q86, Q87 또는 Q61 시리즈).

1. 사용자 정의 이벤트 추가:
   1.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **User-defined Event(사용자 정의 이벤트)**를 우클릭합니다.

1.2. **Add User-defined Event(사용자 정의 이벤트 추가)**를 선택하고 이름을 입력합니다(이 예에서는 'Dry all cameras(모든 카메라 건조)').

2. 새 룰을 생성합니다:
   2.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **룰(Rules)**을 우클릭합니다.
   2.2. **Add Rule(룰 추가)**를 선택하고 이름을 입력합니다(이 예에서는 'Dry all cameras(모든 카메라 건조)').
   2.3. **Perform an action on <event>(<이벤트>에 대한 액션 수행)**를 선택합니다.
   2.4. **Edit the rule description(룰 설명을 편집)** 필드에서, **event(이벤트)**를 클릭합니다.
   2.5. **Events > External Events > User-defined Events(이벤트 > 외부 이벤트 > 사용자 정의 이벤트)**로 이동하고 **Dry all cameras(모든 카메라 건조)**를 선택합니다.
   2.6. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.
   2.7. **Axis: Dry <camera>(Axis: <카메라> 건조)** 액션을 선택합니다.
   2.8. **Edit the rule description(룰 설명 편집)** 필드에서 **Axis: Dry camera(Axis: 카메라 건조)**를 클릭합니다.
   2.9. **Select Triggering Devices(트리거 장치 선택)** 창에서, **Select devices(장치 선택)**을 선택하고 **OK**를 클릭합니다.
   2.10. 액션을 트리거할 장치를 선택하고 **OK**를 클릭하면, 그 다음에 **Finish(마침)**을 합니다.
3. Smart Client에서 사용자 정의 이벤트를 지도 또는 비디오 보기에 오버레이 버튼으로 추가합니다.
4. 오버레이 버튼을 클릭하고 룰이 원하는 대로 작동하는지 확인하십시오.

한 번의 클릭으로 여러 대의 카메라에 대한 오토 포커스 켜기

이벤트 서버 플러그인을 사용하면 운영자가 더 쉽게 사용할 수 있도록 사용자 정의 룰을 설정할 수 있습니다. 이 예에서는 한 번의 클릭으로 모든 카메라에 대해 오토 포커스를 켜는 방법을 보여줍니다.

비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.1 이상
- 오토 포커스를 지원하는 하나 이상의 카메라

1. 사용자 정의 이벤트 추가:
   1.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **User-defined Event(사용자 정의 이벤트)**를 우클릭합니다.
   1.2. **Add User-defined Event(사용자 정의 이벤트 추가)**를 선택하고 이름을 입력합니다(이 예에서는 'Autofocus(오토 포커스)').
2. 새 룰을 생성합니다:
   2.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **룰(Rules)**을 우클릭합니다.
   2.2. **Add Rule(룰 추가)**를 선택하고 이 예에서는 'Perform autofocus(오토 포커스 수행)'이라는 이름을 입력합니다.
   2.3. **Perform an action on <event>(<이벤트>에 대한 액션 수행)**를 선택합니다.
   2.4. **Edit the rule description(룰 설명을 편집)** 필드에서, **event(이벤트)**를 클릭합니다.
   2.5. **Events > External Events > User-defined Events(이벤트 > 외부 이벤트 > 사용자 정의 이벤트)**으로 이동하고 **Autofocus(오토 포커스)**를 선택합니다. **확인**을 클릭합니다.
   2.6. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.
   2.7. **Axis: Run autofocus on <camera>(Axis: <카메라>에서 오토 포커스 실행)** 액션을 선택합니다.

2.8. **Edit the rule description(룰 설명 편집)** 필드에서 **Axis: Run autofocus on camera (Axis: 카메라에서 오토 포커스 실행)**를 클릭합니다.

2.9. **Select Triggering Devices(트리거 장치 선택)** 창에서, **Select devices(장치 선택)**을 선택하고 **OK**를 클릭합니다.

2.10. 액션을 켜고 트리거할 장치를 선택하고 **OK**를 클릭하면, 그 다음에 **Finish(마침)**을 합니다.

3. Smart Client에서 사용자 정의 이벤트 'Autofocus(오토 포커스)'를 지도 또는 비디오 보기에 오버레이 버튼으로 추가합니다.
4. 오버레이 버튼을 클릭하고 룰이 원하는 대로 작동하는지 확인하십시오.

한 번의 클릭으로 여러 개의 스트로브 사이렌을 트리거

이벤트 서버 플러그인을 사용하면 운영자가 더 쉽게 사용할 수 있도록 사용자 정의 룰을 설정할 수 있습니다. 이 예시에서는 Smart Client에서 한 번의 클릭으로 여러 개의 스트로브 사이렌을 활성화하는 방법을 보여줍니다.

비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.4 이상
- 하나 또는 여러 개의 Axis 스트로브 사이렌
- Axis 스트로브 사이렌의 출력 1 활성화 및 Management Client에서 출력 장치에 추가됨

1. 사용자 정의 이벤트 생성:
   1.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **User-defined Event(사용자 정의 이벤트)**를 우클릭합니다.

   1.2. **Add User-defined Event(사용자 정의 이벤트 추가)**를 선택하고 예를 들어 'Trigger all strobe sirens(모든 스트로브 사이렌을 트리거)'와 같은 이름을 입력합니다.
2. 장치 도우미에서 스트로브 사이렌 프로파일을 생성합니다.
   2.1. **Site Navigation > AXIS Optimizer > Device assistant(사이트 탐색 > AXIS Optimizer > 장치 도우미)**로 이동합니다.

   2.2. 스트로보 사이렌을 선택합니다. 스트로브 사이렌의 웹페이지가 열립니다.

   2.3. **Profiles(프로파일)**을 이동하고 **Add profile(프로파일 추가)**를 클릭합니다.

   2.4. 운영자가 Smart Client에서 스트로브 사이렌을 트리거할 때 스트로브 사이렌이 수행할 액션을 구성합니다.

   2.5. 다른 스트로브 사이렌에서 동일한 프로파일을 생성합니다. 모든 장치에서 동일한 프로파일 이름을 사용해야 합니다.
3. Axis 액션에서 액션 프리셋을 만듭니다.
   3.1. **Site Navigation(사이트 탐색) > Rules and Events(룰 및 이벤트) > Axis actions(Axis 액션)**로 이동합니다.

   3.2. **Add new preset(새 프리셋 추가)**을 클릭합니다.

   3.3. **Select strobe siren(스트로보 사이렌 선택)**을 클릭하고**Strobe siren(스트로브 사이렌)**을 클릭합니다.

   3.4. 사용하려는 스트로브 사이렌을 선택하고 **OK**을 클릭합니다.
   스트로브 사이렌의 프로파일 목록이 표시됩니다.

   3.5. 이전 단계에서 생성한 스트로브 사이렌 프로파일을 선택합니다. 작업 프리셋은 자동으로 저장됩니다.

   3.6. F5를 눌러 서버 구성을 새로 고침합니다. 이제 생성한 새 액션 프리셋을 사용할 수 있습니다.
4. 룰 만들기:

4.1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **룰(Rules)**을 우클릭합니다.

4.2. **Add Rule(룰 추가)**를 선택하고 예를 들어 'Trigger all strobe sirens rule(모든 스트로브 사이렌 룰 트리거)'와 같은 이름을 입력합니다.

4.3. **Perform an action on <event>(<이벤트>에 대한 액션 수행)**를 선택합니다.

4.4. **Edit the rule description(룰 설명을 편집)** 필드에서, **event(이벤트)**를 클릭합니다.

4.5. **Events > External Events > User-defined Events(이벤트 > 외부 이벤트 > 사용자 정의 이벤트)**로 이동하고 **Trigger all strobe sirens(모든 스트로브 사이렌 트리거)**를 선택합니다.

4.6. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.

4.7. **Axis: Run a profile on a strobe siren <preset>(Axis: 스트로브 사이렌 <프리셋>에서 프로파일 실행)** 액션을 선택합니다.

4.8. **Edit the rule description(룰 설명을 편집)** 필드에서, **preset(프리셋)**을 클릭합니다.

4.9. 사용할 프리셋을 선택합니다.

4.10. **Next(다음)**를 클릭한 후 **Finish(마침)**를 클릭합니다.

5. Smart Client에서 사용자 정의 이벤트를 지도 또는 비디오 보기에 오버레이 버튼으로 추가합니다.
6. 오버레이 버튼을 클릭하고 룰이 원하는 대로 작동하는지 확인하십시오.

여러 대의 카메라에서 자동으로 특정 영역 감시 차단(프라이버시 마스크) 끄기

이벤트 서버 플러그인을 사용하면 특정 작업을 자동화할 수 있습니다. 이 예에서는 분석 이벤트가 발생할 때 여러 카메라에서 개인 정보 보호 마스크를 자동으로 끄는 방법을 보여줍니다. 예제의 이벤트는 사람이나 차량이 평소에는 있어서는 안 되는 영역에 진입하는 것입니다. 따라서 우리는 무슨 일이 일어나고 있는지 더 잘 볼 수 있도록 특정 영역 감시 차단(프라이버시 마스크)를 자동으로 해제하려고 합니다.



워크플로는 다음과 같습니다.

1. AXIS Object Analytics(또는 선택한 다른 분석 애플리케이션)의 *분석 시나리오 구성, on page 19*
2. *관련 카메라에 운영자 컨트롤 추가, on page 19*
3. *작업 프리셋 만들기, on page 19*
4. *분석 이벤트가 발생할 때 특정 영역 감시 차단(프라이버시 마스크)를 해제하는 룰 만들기, on page 19*
5. *특정 영역 감시 차단(프라이버시 마스크)를 다시 켜는 룰 만들기, on page 20*
6. *룰 테스트, on page 20*을(를) 하고 모든 것이 원하는 대로 작동하는지 확인합니다.

비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.0 이상
- AXIS OS 7.40 이상이 설치된 카메라
- 이벤트를 생성할 수 있는 카메라(이 예에서는 AXIS Object Analytics가 있는 카메라)

분석 시나리오 구성

1. **Site Navigation > AXIS Optimizer > Device assistant(사이트 탐색 > AXIS Optimizer > 장치 도우미)**로 이동하고 사용하려는 분석이 포함된 장치를 찾습니다.
2. **Applications(애플리케이션**을 클릭하고 액션을 트리거할 분석 시나리오를 만듭니다.
3. **Devices > Cameras(장치 > 카메라)**로 이동하고 분석 시나리오를 생성한 카메라를 찾습니다.
4. **Properties(속성)** 창에서, **Events > Add(이벤트 > 추가)**룰 클릭합니다.
5. 드라이버 이벤트를 선택하고(이 예에서 "객체 분석: 이벤트 테스트 라이징') **OK**를 클릭합니다.
6. **Add(추가)**를 클릭하고 드라이버 이벤트 '객체 분석: 이벤트 테스트 실패'를 선택합니다. 그런 다음 **OK(확인)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

관련 카메라에 운영자 컨트롤 추가

1. **AXIS Optimizer > Operator controls(AXIS Optimizer > 운영자 제어)**로 이동하고 제어 라이브러리를 엽니다.
2. **Configuration(구성)** 창에서 해당 폴더를 선택하고 **Turn off privacy mask(특정 영역 감시 차단(프라이버시 마스크) 끄기)** 및 **Turn off privacy mask(특정 영역 감시 차단(프라이버시 마스크) 켜기)** 둘 다를 활성화합니다.

작업 프리셋 만들기

1. **Rules and Events > Axis actions(룰 및 이벤트 > Axis 액션)**으로 이동하고 **Add new preset (신규 프리셋 추가)**를 클릭합니다.
2. **Cameras(카메라)**를 클릭하고 관련 카메라를 선택합니다. 이 예에서는: AXIS P1375 및 AXIS Q6075-E. 그런 다음 **Turn on privacy mask(프라이버시 마스크 켜기)** 제어를 선택합니다.
3. **Add new preset > Cameras(신규 프리셋 추가 > 카메라)**를 클릭하고 관련 카메라를 선택합니다. 이 예에서는: AXIS P1375 및 AXIS Q6075-E. 그런 다음 **Turn off privacy mask(프라이버시 마스크 끄기)** 제어를 선택합니다.

분석 이벤트가 발생할 때 특정 영역 감시 차단(프라이버시 마스크)를 해제하는 룰 만들기

1. **Site Navigation > Rules and Events(사이트 탐색 > 룰 및 이벤트)**로 이동하고 **룰(Rules)**을 우클릭합니다.
2. **Add Rule(룰 추가)**를 선택하고 이 예에서는 'Turn on privacy mask on analytics stop(분석 중지 시 특정 영역 감시 차단(프라이버시 마스크) 끄기)'와 같은 이름을 입력합니다.
3. **Perform an action on <event>(<이벤트>에 대한 액션 수행)**를 선택합니다.
4. **Edit the rule description(룰 설명을 편집)** 필드에서, **event(이벤트)**를 클릭합니다. **Devices (장치) > Configurable Events(구성 가능한 이벤트)**로 이동하여 **Object Analytics: Event test Rising(객체 분석: 이벤트 테스트 상승)**을 선택합니다.
5. **Edit the rule description(룰 설명 편집)** 필드에서 장치를 선택합니다(이 예에서는 AXIS P1375).
6. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.
7. **Axis: Run operator control: <preset>(Axis: 운영자 제어 실행: <프리셋>)** 액션을 선택합니다.
8. **Edit the rule description(룰 설명을 편집)** 필드에서, **preset(프리셋)**을 클릭합니다. 그런 다음 해당 **Turn on privacy mask on 2 cameras(2대의 카메라에서 특정 영역 감시 차단(프라이버시 마스크) 끄기)**를 추가하고 **OK**를 클릭합니다.
9. **Finish(마침)**를 클릭.

특정 영역 감시 차단(프라이버시 마스크)를 다시 켜는 룰 만들기

1. **Add Rule(룰 추가)**를 선택하고 이 예에서는 'Turn on privacy mask on analytics stop(분석 중지 시 특정 영역 감시 차단(프라이버시 마스크) 켜기)'와 같은 이름을 입력합니다.
2. **Perform an action on <event>(<이벤트>에 대한 액션 수행)**를 선택합니다.
3. **Edit the rule description(룰 설명을 편집)** 섹션에서, **event(이벤트)**를 클릭합니다. **Devices (장치) > Configurable Events(구성 가능한 이벤트)**로 이동하여 **Object Analytics: Event test Failing(객체 분석: 이벤트 테스트 실패)**을 선택합니다.
4. **Edit the rule description(룰 설명 편집)** 섹션에서 장치를 선택합니다(이 예에서는 AXIS P1375).
5. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.
6. **Axis: Run operator control: <preset>(Axis: 운영자 제어 실행: <프리셋>)** 액션을 선택합니다.
7. **Edit the rule description(룰 설명을 편집)** 섹션에서, **프리셋(preset)**을 클릭합니다. 그런 다음 해당 **Turn on privacy mask on 2 cameras(2대의 카메라에서 특정 영역 감시 차단(프라이버시 마스크) 켜기)**를 추가하고 **OK**를 클릭합니다.
8. **Finish(마침)**를 클릭.

룰 테스트

1. **AXIS Optimizer > Device assistant(AXIS Optimizer > 장치 어시스턴트)**로 이동하고 자동화를 생성하는 데 사용한 분석이 포함된 장치를 찾습니다. 이 예에서는 AXIS P1375.
2. 해당 시나리오를 열고 **Test alarm(테스트 알람)**을 클릭합니다.

카메라가 모션을 감지하면 스트로브 사이렌을 활성화

이벤트 서버 플러그인을 사용하여 사용자 설정 룰을 설정하여 프리셋을 자동화할 수 있습니다. 이 예에서는 카메라가 모션을 감지할 때 자동으로 스트로브 사이렌을 활성화하는 방법을 보여 줍니다.

비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.4 이상
- 하나 또는 여러 개의 Axis 스트로브 사이렌
- Axis 스트로브 사이렌의 출력 1 활성화 및 Management Client에서 출력 장치에 추가됨.
- VMS version 2022 R2 이전 버전의 경우 Axis 액션을 정지 액션으로 사용할 수 없습니다. 이전 버전의 경우 스트로브 사이렌을 실행 및 중지하기 위한 두 개의 개별 룰을 만들어야 합니다.

1. 스트로브 사이렌 프로파일 생성:
   1.1. **Site Navigation > AXIS Optimizer > Device assistant(사이트 탐색 > AXIS Optimizer > 장치 도우미)**로 이동합니다.
   1.2. **Axis output devices**(Axis 출력 장치)로 이동하고 스트로브 사이렌을 선택하십시오. 스트로브 사이렌의 웹페이지가 열립니다.
   1.3. **Profiles(프로파일)**을 이동하고 **Add profile(프로파일 추가)**를 클릭합니다.
   1.4. 모든 사이렌에 대해 동일한 프로파일 이름을 선택해야 합니다.
   1.5. 스트로브 사이렌이 모션을 감지할 때 수행할 작업을 구성합니다.
2. 시작 및 정지에 대한 액션 프리셋 만들기:
   2.1. **Site Navigation(사이트 탐색) > Rules and Events(룰 및 이벤트) > Axis actions(Axis 액션)**로 이동합니다.
   2.2. 시작 프리셋을 만들려면 **스트로브 사이렌**으로 이동하고 **새 프리셋 추가**를 클릭합니다.
   2.3. **Select strobe siren(스트로보 사이렌 선택)**을 클릭하고**Strobe siren(스트로브 사이렌)**을 클릭합니다.

2.4. 목록에서 하나 이상의 스트로브 사이렌을 선택합니다.

2.5. 목록에서 이전에 생성한 사이렌 프로파일을 선택합니다. 작업 프리셋은 자동으로 저장됩니다.

2.6. 정지 프리셋을 만들려면 **새 프리셋 추가**를 클릭합니다.

2.7. **Select strobe siren(스트로보 사이렌 선택)**을 클릭하고**Strobe siren(스트로브 사이렌)**을 클릭합니다.

2.8. 시작 프리셋에 대해 선택된 동일한 스트로브 사이렌을 목록에서 선택합니다.

2.9. **액션 선택**으로 이동하고 **정지**를 선택하십시오.

2.10. 시작 액션에 대해 생성된 것과 동일한 사이렌 프로파일을 선택합니다. 작업 프리셋은 자동으로 저장됩니다.

2.11. **click to refresh(클릭하여 새로 고침)**를 클릭하거나 F5를 눌러 서버 구성을 새로 고침합니다.

3. 룰 만들기:

3.1. **Site Navigation(사이트 탐색) > Rules and Events(룰 및 이벤트) > Rules(룰)**로 이동합니다.

3.2. **Rules(룰)**를 마우스 오른쪽 버튼으로 클릭하고 **Add Rule(룰 추가)**를 선택한 후 이름을 입력합니다.

3.3. **Edit the rule description(룰 설명 편집)**에서 **event(이벤트)**를 클릭합니다.

3.4. **Devices(장치) > Predefined Events(사전 정의된 이벤트)**로 이동하고 **Motion Started(모션 시작됨)**를 선택합니다.

3.5. **Edit the rule description(룰 설명 편집)**에서 **devices/recording_server/management_server**를 클릭합니다.

3.6. 스트로브 사이렌을 작동시킬 카메라를 선택합니다.

3.7. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.

3.8. **Axis: Start or stop a profile on a strobe siren: <preset>(Axis: 스트로브 사이렌에서 프로파일 시작 또는 중지: <프리셋>)** 액션을 선택합니다.

3.9. **Edit the rule description(룰 설명 편집)**에서 **preset(프리셋)**을 클릭합니다.

3.10. 이전에 만든 시작 프리셋을 선택합니다.

3.11. **Next(다음)**를 클릭하고 **Perform stop action on <event>**를 선택합니다.

3.12. **Next(다음)**를 클릭하고 **Axis: Start or stop a profile on strobe siren: <event>(Axis: 스트로브 사이렌에서 프로파일 시작 또는 중지: <이벤트>)**를 선택합니다.

3.13. **Edit the rule description(룰 설명 편집)**에서 **preset(프리셋)**을 클릭합니다.

3.14. 이전에 만든 정지 프리셋을 선택합니다.

3.15. **Finish(마침)**를 선택합니다.

4. 카메라에서 모션이 감지되면 스트로브 사이렌이 올바르게 작동하는지 테스트합니다.

카메라가 모션을 감지하면 스피커 또는 스피커 영역에서 오디오 클립 재생



이벤트 서버 플러그인을 사용하여 사용자 설정 룰을 설정하여 프리셋을 자동화할 수 있는데 이를 액션 프리셋이라고 합니다. 이 예는 카메라가 모션을 감지하면 오디오 스피커 또는 스피커 영역에서 자동으로 오디오 클립을 재생하는 방법을 보여줍니다.

비고

요구 사항

- 이벤트 서버 및 Management Client의 AXIS Optimizer 버전 4.6 이상.
- 스피커가 내장된 하나 이상의 전용 Axis 스피커 또는 Axis 장치.
- 스피커 구역에서 오디오 클립을 재생하려면 올바르게 구성된 AXIS Audio Manager Edge 또는 AXIS Audio Manager Pro 시스템이 필요합니다. 이러한 시스템을 구성하는 방법에 대한 자세한 내용은 *모드 구성, on page 31*을 참조하십시오.

1. 오디오 클립을 업로드하려면:
   1.1. AXIS Audio Manager Edge 모드 또는 Legacy mode(레거시 모드)에서는 스피커에 업로드할 오디오 클립을 기본 폴더 **C:₩Users₩Public₩Documents₩AXIS Optimizer for Milestone XProtect - Audio Clips₩**에 넣습니다.
   AXIS Audio Manager Pro 모드에서는 AXIS Audio Manager Pro 웹 인터페이스에서 오디오 클립을 업로드합니다.
   1.2. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동한 후 목록에서 스피커, 장치 그룹 또는 스피커 구역을 선택합니다.

   비고

   스피커 관리자 모드 선택 방법에 대한 자세한 내용은 *모드 구성, on page 31*을 참조하십시오.

   1.3. **Audio clips(오디오 클립)**로 이동하여 업로드할 오디오 클립 앞의**+**를 클릭합니다.
   1.4. Legacy mode(레거시 모드)에서는 오디오 클립을 재생할 각 스피커에 대해 1.2~1.3단계를 반복합니다. 각 스피커에 동일한 오디오 파일을 업로드해야 합니다.
2. 스피커 또는 스피커 영역에서 오디오 클립을 재생하기 위한 액션 프리셋 만들기:
   2.1. **Site Navigation(사이트 탐색)** > **Rules and Events(룰 및 이벤트)** > **Axis actions(Axis 액션)**로 이동합니다.
   2.2. 프리셋을 생성하려면 **Audio clips(오디오 클립)**로 이동하여 **Add new preset(새 프리셋 추가)**를 클릭합니다.
   2.3. AXIS Audio Manager Edge 또는 AXIS Audio Manager Pro 모드에서는 **Select playback destination(재생 대상 선택)**으로 이동합니다.
   Legacy mode(레거시 모드)에서는 **Select speaker(스피커 선택)**로 이동합니다.
   2.4. 스피커 또는 스피커 영역을 선택합니다.
   2.5. 목록에서 1단계에서 업로드한 오디오 클립을 선택하세요. 작업 프리셋은 자동으로 저장됩니다.
   2.6. AXIS Audio Manager Pro 모드에서는 **Select visual profile(시각적 프로파일 선택)**로 이동하여 시각적 프로파일과 텍스트를 구성합니다.

   비고

   오디오 클립 액션이 트리거될 때 AXIS Audio Manager Pro 서버의 기본 시각적 프로파일 동작을 사용하려면 시각적 프로파일 목록에서 **Default(기본값)**를 선택합니다.

   2.7. 서버 구성을 새로 고치려면 **refresh(새로 고침)**를 클릭하거나 F5를 누릅니다.
3. 룰 생성 방법:
   3.1. **Site Navigation(사이트 탐색)** > **Rules and Events(룰 및 이벤트)** > **Rules(룰)**로 이동합니다.
   3.2. **Rules(룰)**를 마우스 오른쪽 버튼으로 클릭하고 **Add Rule(룰 추가)**를 선택한 후 이름을 입력합니다.
   3.3. **Edit the rule description(룰 설명 편집)**에서 **event(이벤트)**를 클릭합니다.

3.4. **Devices(장치)**> **Predefined Events(사전 정의된 이벤트)**로 이동하고 **Motion Started (모션 시작됨)**를 선택합니다.
3.5. **Edit the rule description(룰 설명 편집)**에서 **devices/recording_server/ management_server**를 클릭합니다.
3.6. 액션 프리셋 또는 오디오 클립을 트리거해야 하는 카메라를 선택합니다.
3.7. **Step 3: Actions(3단계: 액션)**에 도달할 때까지 **Next(다음)**를 클릭합니다.
3.8. **Axis: Play audio clip: <preset>(Axis: 오디오 클립 재생: <preset>)** 액션을 선택합니다.
3.9. **Edit the rule description(룰 설명 편집)**에서 **preset(프리셋)**을 클릭합니다.
3.10. 이전 단계에서 생성한 프리셋을 선택합니다.
3.11. **Finish(마침)**를 선택합니다.
4. 카메라가 움직임을 감지했을 때 오디오 클립이 올바르게 재생되는지 테스트합니다.

룰 문제 해결

룰이 작동하지 않으면 먼저 이벤트 서버 메시지를 확인하여 이벤트 서비스가 실행 중인지 확인하십시오.

이벤트 서버에서 AXIS Optimizer 로그를 확인할 수도 있습니다. Management Client 또는 Smart Client를 사용할 수 있는 경우 이를 사용하여 로그를 활성화하고 저장합니다.

번호판 목록을 중앙에서 관리

AXIS Optimizer 목록 관리자를 사용하면 모든 카메라의 번호판 목록을 한 번에 중앙에서 관리할 수 있습니다. VMS에서 직접 허용 목록, 차단 목록, 사용자 설정 목록을 만들고 관리할 수 있습니다. 시스템은 목록 결합을 지원합니다. 즉, 시스템의 모든 카메라에 적용되는 전역 목록과 특정 카메라에 적용되는 로컬 목록을 가질 수 있습니다.

중앙 집중식 목록 관리는 예를 들어 자동 주차 출입을 원하거나 시스템이 특정 번호판을 등록할 때 알람을 받고 싶을 때 유용합니다.

목록을 만들고 편집하려면 관리자여야 합니다. 다른 역할에 읽기 및 편집 권한을 부여하고 *목록 권한 구성, on page 23* 섹션을 참조합니다.

목록 만들기

비고

요구 사항

- 카메라에서 AXIS License Plate Verifier 1.8 이상이 실행되어야 합니다.
- 사용자 지정 목록을 생성하려면 AXIS License Plate Verifier 2.0 이상이 필요합니다.

1. Management Client에서 **Site Navigation > AXIS Optimizer > License plate lists(사이트 탐색 > AXIS Optimizer > 번호판 목록)**으로 이동합니다.
2. 허용 목록, 차단 목록 및 사용자 설정 목록을 보낼 카메라를 선택합니다.
3. (선택 사항) 허용 목록, 차단 목록, 사용자 설정 목록을 보고 수정할 수 있는 사용자 역할을 추가합니다.
4. 허용 목록, 차단 목록 및 사용자 설정 목록에 번호판을 추가합니다.
   기존 번호판 목록을 가져올 수도 있습니다.
   목록이 **동기화된** 상태를 가져오면, 선택한 카메라에 푸시되었습니다.

목록 권한 구성

허용 목록, 차단 목록, 사용자 정의 목록을 편집할 수 있는 사용자 역할을 구성할 수 있습니다. 이는 예를 들어 관리자가 목록을 설정했지만 운영자가 일일 필요에 따라 방문자를 추가하기를 원하는 경우에 유용합니다.

Management Client에서

목록을 보고 편집할 수 있는 모든 권한은 각 목록별로 선택될 수 있습니다.

1. **Security > Roles(보안 > 역할)**로 이동한 후 역할을 선택합니다.
2. **AXIS Optimizer** 탭으로 이동합니다.
3. **Role settings(역할 설정)** > **AXIS Optimizer** > **License plate lists(번호판 목록)**로 이동합니다.
4. **License plate lists(node)(번호판 목록(노드)** 필드에서 **Read(읽기)**를 선택합니다.
5. **License plate lists(번호판 목록)**에서 목록을 선택하고**Edit license plates(번호판 편집)**를 선택합니다.
   - XProtect 2023 R2 이전 버전의 경우 **MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists(MIP > AXIS Optimizer > AXIS Optimizer Security > 번호판 목록)**로 이동하고 **Edit license plate lists(번호판 목록 편집)**를 선택합니다.

목록 편집

Management Client에서

1. **Site Navigation > AXIS Optimizer > License plate lists(사이트 탐색 > AXIS Optimizer > 번호판 목록)**로 이동합니다.
2. 편집할 사이트를 선택합니다.
3. 필요에 따라 **Cameras(카메라)** 또는 **License plates(번호판)**를 업데이트합니다.
   목록이 **동기화된** 상태를 가져오면, 변경 사항이 선택한 카메라로 푸시되었습니다.

Smart Client에서

1. *Axis 번호판, on page 58*으로 이동하고 **번호판 목록**을 클릭합니다.
   탭이 보이지 않으면, **Settings > Axis search options(설정 > Axis 검색 옵션)**로 이동하고 **Show license plate tab(번호판 탭 표시)**을 선택합니다.
2. 편집할 사이트를 선택합니다.
3. 허용 목록, 차단 목록 및 사용자 설정 목록에 번호판을 추가합니다.
   기존 번호판 목록을 가져올 수도 있습니다.
   목록이 **동기화된** 상태를 가져오면, 선택한 카메라에 푸시되었습니다.

목록 가져오기

여러 텍스트 또는 CSV 형식의 목록을 가져올 수 있습니다.

- 허용되는 텍스트 형식: 각 줄에 번호판 하나
- 허용되는 CSV 형식:
  - 각 줄에 번호판 하나
  - 두 필드: 번호판과 날짜
  - 세 가지 필드: 번호판, 소유자 및 설명
  - 4개 필드: 번호판, 소유자, 설명 및 '활성' 또는 '비활성' 문자열. (목록을 내보낼 때와 동일한 형식입니다.)

Management Client에서

1. **Site Navigation > AXIS Optimizer > License plate lists(사이트 탐색 > AXIS Optimizer > 번호판 목록)**로 이동합니다.
2. 편집할 사이트를 선택합니다.
3. **Allowed(허용됨)**, **Blocked(차단됨)** 또는 **Custom(사용자 설정)**으로 이동하십시오.

4. ⋮ 을 클릭한 다음 **Import to allow list(허용 목록으로 가져오기)**, **Import to block list(차단 목록으로 가져오기)** 또는 **Import to custom list(사용자 지정 목록으로 가져오기)**를 선택합니다.
5. **목록 재설정** 대화 상자 내:
   – **예**를 클릭하여 기존 번호판을 모두 제거하고 목록에는 새로 가져온 번호판만 추가합니다.
   – **아니요**를 클릭하여 새로 가져온 번호판을 목록의 기존 번호판과 병합합니다.

Smart Client에서

1. *Axis 번호판, on page 58*으로 이동하고 **번호판 목록**을 클릭합니다.
   탭이 보이지 않으면, **Settings > Axis search options(설정 > Axis 검색 옵션)**로 이동하고 **Show license plate tab(번호판 탭 표시)**을 선택합니다.
2. 편집할 사이트를 선택합니다.
3. **Allowed(허용됨)**, **Blocked(차단됨)** 또는 **Custom(사용자 설정)**으로 이동하십시오.
4. ⋮ 을 클릭한 다음 **Import to allow list(허용 목록으로 가져오기)**, **Import to block list(차단 목록으로 가져오기)** 또는 **Import to custom list(사용자 지정 목록으로 가져오기)**를 선택합니다.
5. **목록 재설정** 대화 상자 내:
   – **예**를 클릭하여 기존 번호판을 모두 제거하고 목록에는 새로 가져온 번호판만 추가합니다.
   – **아니요**를 클릭하여 새로 가져온 번호판을 목록의 기존 번호판과 병합합니다.

목록 내보내기

비고

번호판 목록을 내보내려면, 관리자 권한이 있어야 합니다.

Management Client에서

1. **Site Navigation > AXIS Optimizer > License plate lists(사이트 탐색 > AXIS Optimizer > 번호판 목록)**로 이동합니다.
2. 편집할 사이트를 선택합니다.
3. **Allowed(허용됨)**, **Blocked(차단됨)** 또는 **Custom(사용자 설정)**으로 이동하십시오.
4. ⋮ 을 클릭한 다음 **Export allow list(허용 목록 내보내기)**, **Export block list(차단 목록 내보내기)** 또는 **Export custom list(사용자 지정 목록 내보내기)**를 선택합니다.
   내보낸 목록은 4개의 필드가 있는 CSV 형식입니다. 번호판, 소유자, 설명 및 활성 또는 비활성 상태.

Smart Client에서

1. *Axis 번호판, on page 58*으로 이동하고 **번호판 목록**을 클릭합니다.
   탭이 보이지 않으면, **Settings > Axis search options(설정 > Axis 검색 옵션)**로 이동하고 **Show license plate tab(번호판 탭 표시)**을 선택합니다.
2. 편집할 사이트를 선택합니다.
3. **Allowed(허용됨)**, **Blocked(차단됨)** 또는 **Custom(사용자 설정)**으로 이동하십시오.
4. ⋮ 을 클릭한 다음 **Export allow list(허용 목록 내보내기)**, **Export block list(차단 목록 내보내기)** 또는 **Export custom list(사용자 지정 목록 내보내기)**를 선택합니다.
   내보낸 목록은 4개의 필드가 있는 CSV 형식입니다. 번호판, 소유자, 설명 및 활성 또는 비활성 상태.

목록에 대해 자세히 알아보기

- 여러 사이트를 만들 수 있습니다.
- 각 사이트는 AXIS License Plate Verifier가 설치된 하나 이상의 카메라와 연결됩니다.
- 각 사이트는 하나 이상의 VMS 사용자 역할과 연결됩니다. 사용자 역할은 번호판 목록을 읽고 편집할 권한이 있는 사람을 정의합니다.
- VMS 데이터베이스에 모든 목록이 저장됩니다.
- 사이트에 카메라를 추가하면 카메라에 이미 존재하는 번호판을 덮어씁니다.
- 동일한 카메라가 여러 사이트에 있는 경우 카메라는 모든 목록의 합계를 받습니다.
- 동일한 번호판이 여러 목록에 있는 경우 "차단"이 가장 높은 우선 순위를 가지며 "허용"이 중간 우선 순위를 가지며 "사용자 설정"이 가장 낮은 우선 순위를 갖습니다.
- 각 번호판에 대해 차량 소유자에 대한 정보를 추가할 수 있습니다. 그러나 이 정보는 카메라와 동기화되지 않습니다.

실시간 이벤트에 대응

장치 컨트롤을 사용

운영자 제어

운영자 제어를 사용하면 Smart Client에서 직접 Axis 카메라의 특정 기능에 액세스할 수 있습니다. 액세스할 수 있는 기능은 시스템에 있는 카메라와 기능에 따라 다릅니다. 사전 설치된 운영자 제어 외에도 사용자 정의 제어를 생성할 수 있습니다. 운영자가 액세스할 수 있는 제어를 구성할 수도 있습니다.

운영자 제어의 몇 가지 예는 다음과 같습니다.

- 와이퍼 켜기 또는 끄기
- 히터 켜기 또는 끄기
- IR 켜기 또는 끄기
- 포커스 리콜
- WDR 켜기 또는 끄기
- 흔들림 보정을 켜기 또는 끄기
- 특정 영역 감시 차단(프라이버시 마스크)를 켜기 또는 끄기.

카메라의 특정 운영자 제어에 대한 정보는 데이터시트를 참조하십시오.

운영자 제어에 액세스

비고

요구 사항

- AXIS OS 7.10, 7.40 이상이 설치된 Axis 장치. (버전 7.20 및 7.30은 운영자 제어를 지원하지 않습니다.)

1. Smart Client에서 **실시간(Live)**를 클릭하고 Axis 카메라로 이동합니다.
2. 을 클릭하고 사용할 기능을 선택합니다.

PTZ 카메라의 포커스 영역 저장

포커스 리콜 기능을 사용하면 PTZ 카메라가 장면의 해당 영역으로 이동할 때 자동으로 반환되는 포커스 영역을 저장할 수 있습니다. 이것은 카메라가 포커스를 찾는 데 문제가 있는 저조도 조건에서 특히 유용합니다.



1. Smart Client에서 포커스를 맞추고 싶은 영역으로 카메라를 이동하세요.

비고

포커스 영역을 설정할 때 조명 조건이 좋아야 합니다.

2. 카메라에 포커스를 맞춥니다.
3. **포커스 리콜 영역 추가**를 선택합니다.

나중에 카메라를 팬 또는 틸트하고 뷰를 특정 영역으로 이동하면 카메라가 해당 뷰에 대해 사전 설정된 포커스를 자동으로 불러옵니다. 확대 또는 축소해도 카메라는 동일한 포커스 위치를 유지합니다.

영역이 잘못 구성된 경우, **포커스 리콜 영역 제거**를 선택하십시오.

카메라 오토 포커스



오토 포커스 기능이 있는 카메라는 렌즈를 기계적으로 자동으로 조정할 수 있으므로 보기가 변경될 때 이미지 초점이 관심 영역에 유지됩니다.

PTZ 카메라 오토 포커스 설정

1. Smart Client에서 카메라 보기를 선택합니다.
2. 을 클릭하고 **Set Focus(포커스 설정) > AF**로 이동합니다.
   포커스 제어는 포커스를 더 가까이 또는 더 멀리 이동할 수 있습니다.
   - 큰 단계의 경우, 큰 막대를 클릭합니다.
   - 작은 단계를 수행하려면 작은 막대를 클릭합니다.

고정형 카메라 및 고정형 돔 카메라 오토 포커스 설정

1. Smart Client에서 카메라 보기를 선택합니다.
2. 을 클릭하여 **Autofocus(오토 포커스)**로 이동합니다.

Speed Dry 또는 와이퍼 켜기



Speed Dry 기능은 돔이 젖었을 때 스스로 흔들어 떨어뜨리도록 합니다. 돔이 고속으로 진동하면 물의 표면 장력이 깨지면서 물방울을 제거합니다. 이를 통해 카메라는 우천 시에도 선명한 이미지를 녹화할 수 있습니다.

Speed Dry 기능을 켜려면

1. Smart Client에서 카메라 보기를 선택합니다.
2. 을 클릭하고 **PTZ > Speed Dry**로 이동합니다.

중요 사항

Speed Dry 기능은 AXIS Q61 시리즈 카메라에서만 사용할 수 있습니다.

와이퍼 기능을 켜려면

와이퍼는 Axis 포지셔닝 카메라의 렌즈에서 과도한 물과 비를 제거합니다.

1. Smart Client에서 카메라 보기를 선택합니다.
2. 을 클릭합니다.

중요 사항

와이퍼 기능은 AXIS Q86 시리즈 카메라에서만 사용할 수 있습니다.

스팟 온도 측정



시스템에 스팟 온도 판독이 내장된 카메라가 있는 경우 카메라 보기에서 직접 온도를 측정할 수 있습니다. 스팟 온도 판독 기능이 있는 AXIS 카메라는 AXIS Q1961-TE, AXIS Q2101-E 및 AXIS Q2901-E입니다.

1. Smart Client에서 스팟 온도 판독이 내장된 카메라에서 카메라 보기를 엽니다.
2. 스팟 온도를 측정하려면, 을 클릭하고 다음을 선택합니다.
   - AXIS Q2901-E용 **Measure spot temperature(스팟 온도 측정)**.
   - AXIS Q1961-TE 및 AXIS Q2101-E용 **Enable temperature spot meter(온도 스팟 미터 활성화)**.
3. 보기에서 아무 영역이나 클릭하면, 현재 스팟 온도가 표시됩니다.
   Q1961-TE 및 AXIS Q2101-E의 경우 **Done(완료)**을 클릭합니다.
4. AXIS Q1961-TE 및 AXIS Q2101-E의 경우, 스팟 온도는 비활성화될 때까지 이미지에 남아 있습니다.
   - > **Disable temperature spot meter(스팟 온도 측정기 비활성화)**를 선택합니다.

비고

디지털 줌을 사용하면 온도 측정이 잘못된 결과를 줄 수 있습니다.

움직이는 물체를 자동으로 확대하고 추적합니다.

오토트래킹

오토트래킹 기능을 사용하면 카메라가 자동으로 확대되어 움직이는 물체(예: 차량 또는 사람)를 추적합니다. 추적할 물체를 수동으로 선택하거나 트리거 영역을 설정하고 카메라가 움직이는 물체를 감지하도록 할 수 있습니다. 카메라가 객체를 추적하지 않으면 5초 후 홈 포지션으로 돌아갑니다.

- PTZ 카메라 웹 인터페이스에서 트리거 영역을 구성합니다.
- Smart Client에서 다음을 볼 수 있습니다.
  - 레드 정사각형: 추적한 객체.
  - 블루 영역: 현재 추적 중은 아니지만, 트리거 구역에 진입하거나 마우스 오른쪽 버튼으로 클릭하면 추적할 수 있는 객체.

오토트래킹 구성

비고

요구 사항

- AXIS OS 12.0
- 오토트래킹 2를 지원하는 Axis 카메라(예: AXIS Q6075 PTZ Dome Network Camera) 1대 이상.

1. 카메라 및 메타데이터 장치가 활성화되어 있는지 확인합니다.
2. 카메라의 메타데이터 1을 선택하고 **Settings(설정)**를 클릭합니다.
3. **Metadata stream > Event data(메타데이터 스트림 > 이벤트 데이터)**로 이동하고 **Yes(예)**를 선택합니다.
4. **Save(저장)**를 클릭합니다.
5. PTZ 카메라 웹 인터페이스에서 오토트래킹을 구성합니다.

오토트래킹을 켜거나 끕니다.

1. Smart Client에서 을 클릭합니다.
2. **Turn on autotracking(오토트래킹 켜기)** 또는 **Turn off autotracking(오토트래킹 끄기)**를 선택합니다.

비고

오토트래킹 켜기/끄기 옵션이 여러 개 있으면 목록의 마지막 옵션을 사용하십시오.

수동으로 오토트래킹 시작

객체 위로 마우스를 가져가면 오버레이가 채워집니다. 객체를 가리킬 때 마우스 오른쪽 버튼을 클릭하면 해당 객체를 대상으로 설정하고 카메라가 대상 객체를 추적하기 시작합니다. 객체를 더 이상 추적할 수 없는 경우, 카메라는 5초 후에 재설정됩니다.

파란 상자 밖을 마우스 오른쪽 클릭하면 오토트래킹이 중지됩니다.

사용자 지정 운영자 컨트롤 생성

1. Management Client에서 **Site Navigation > AXIS Optimizer > Operator controls(사이트 탐색 > AXIS Optimizer > 운영자 제어)**로 이동합니다.
2. 장치 또는 장치 그룹을 선택합니다.
3. **Add new control(새 제어 추가)**을 클릭합니다.
4. **이름**과 **설명**을 입력합니다.
5. 운영자 제어를 관리자 권한이 있는 사용자만 사용할 수 있도록 하려는 경우 **Administrator(관리자)**를 선택합니다.
6. 특정 제어에 대한 VAPIX URL을 추가합니다.
   예: Defog on(디포그 켜기) 운영자 제어를 추가하려면 다음 URL을 입력합니다. `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Axis 네트워크 장치 API에 대한 자세한 내용은 를 참조하십시오.
7. Smart Client로 이동하여 운영자 제거가 예상대로 작동하는지 테스트하십시오.

운영자 제어에 대한 액세스 구성

Smart Client에서 운영자가 액세스할 수 있는 운영자 제어를 구성할 수 있습니다.

1. Management Client에서 **Site Navigation > AXIS Optimizer > Operator controls(사이트 탐색 > AXIS Optimizer > 운영자 제어)**로 이동합니다.
2. 장치 또는 장치 그룹을 선택합니다.
3. 운영자가 Smart Client에서 액세스할 수 있도록 하려는 운영자 제어를 선택합니다.

스피커를 통해 상호 작용

스피커 관리자

Axis 오디오 제품을 VMS에 통합하여 Axis 장치의 모든 기능을 원활하게 사용할 수 있도록 지원합니다.

- 카메라와 관련된 스피커에 액세스
  카메라를 스피커 또는 스피커 그룹에 연결하면 실시간 보기에서 스피커에 액세스할 수 있습니다. 더 이상 수동으로 스피커를 찾을 필요가 없습니다.
- 스피커 그룹에 오디오 보내기
  한 번의 클릭으로 많은 스피커에 오디오를 보냅니다.
- 오디오 클립 관리
  오디오 클립을 손쉽게 관리할 수 있습니다.

- 스피커로 즉각적인 조치를 취하십시오.
  알람 관리자를 종료하지 않고 알람에 신속하게 대응합니다.
- 스피커 간 오디오 동기화
  오디오 시스템을 배경 음악용으로 사용하려는 경우, Speaker manager(스피커 관리자)를 통해 구역을 설정하여 스피커 간의 오디오를 동기화할 수 있습니다(AXIS Audio Manager Pro 및 Edge 모드에서만 지원).

모드

Speaker manager(스피커 관리자)는 다양한 유형의 스피커 설정을 위해 세 가지 모드를 지원합니다.

- AXIS Audio Manager Pro 시스템용 **Pro**
  대규모 또는 고급 구내 방송 시스템을 위해 설계된 포괄적인 소프트웨어 솔루션입니다. 최대 5,000대 이상의 스피커와 500개 이상의 구역을 지원하며 라이센스 및 설치에 대한 유연한 옵션을 제공합니다. 더 큰 규모의 시스템 또는 고급 스케줄링 요구 사항이 있는 사용자에게 권장됩니다.
- AXIS Audio Manager Edge 시스템용 **Edge**
  20개 구역에 걸쳐 최대 200대의 스피커를 관리하는 간소화된 소프트웨어 솔루션입니다. Axis 네트워크 스피커에 직접 내장되어 있으며 서버나 추가 라이센스가 필요하지 않습니다. 고급 스케줄링 요구 사항이 없는 소규모 시스템에 권장됩니다.
- **레거시**
  레거시 모드는 기본 스피커 통합을 사용하여 스피커 그룹에 오디오를 브로드캐스트하거나 오디오 클립을 트리거합니다. 동기화된 브로드캐스트는 지원하지 않습니다. 개별 스피커가 있고 동기화된 브로드캐스트 요구 사항이 없는 시스템에 권장됩니다.

모드 구성

이 페이지에 처음 들어가면 모드를 선택하라는 메시지가 표시되지만 언제든지 모드를 변경할 수 있습니다. 각 모드에서 수행한 구성은 별도로 분리되지만 모드 간에 전환해도 유지됩니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동합니다.
2. **Mode(모드)**에서 현재 사용 중인 모드를 클릭하고 팝업 창에서 원하는 모드를 선택합니다.
3. **Switch mode(모드 전환)**를 클릭합니다.

AXIS Audio Manager Pro 모드

이 모드를 사용하는 방법:

- 녹화 서버와 같은 서버 시스템에 AXIS Audio Manager Pro 소프트웨어를 설치합니다.
- API 액세스로 AXIS Audio Manager Pro의 라이센스를 부여하고 구성합니다.
- 옵션: 웹 인터페이스용 서버 인증서를 설정합니다. 자세한 내용은 *인증서*를 참조하십시오.
- VMS 서버 시스템에 설치된 경우 AXIS Audio Manager Pro 서버를 포트 443에서 변경합니다.

이 모드에서는 VMS에 스피커를 추가하거나 라이센스를 부여할 필요가 없지만 AXIS Audio Manager Pro 서버에 연결하기 위한 하드웨어가 자동으로 생성됩니다(VMS 장치 라이센스 하나 필요). AXIS Audio Manager Pro에 대해 자세히 알아보려면 *AXIS Audio Manager Pro 사용자 설명서*를 참조하십시오.

비고

AXIS Audio Manager Pro 모드는 단일 로컬 사이트 지원으로 제한됩니다. 다중 사이트, 연합형 및 상호 연결된 사이트 아키텍처는 이 통합 범위에 포함되지 않습니다.

Pro 모드에서 AXIS Audio Manager Pro 서버에 연결

1. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer**> **Speaker manager(스피커 관리자)**로 이동합니다.

2. **Connect(연결)**를 클릭합니다.
3. 대화 상자에서:
   - AXIS Audio Manager Pro 서버 하드웨어를 추가할 녹화 서버를 선택합니다.
   - AXIS Audio Manager Pro 서버의 주소와 HTTPS 포트를 입력합니다.
   - API 사용자 이름과 패스워드를 입력합니다(API 액세스는 AXIS Audio Manager Pro 서버에서 활성화되어 있어야 함).
   - **Connect(연결)**를 클릭합니다.

왼쪽에서 AXIS Audio Manager Pro에서 사용 가능한 모든 대상 및 구역을 볼 수 있습니다. **AXIS Audio Manager Pro Server**를 클릭하면 오른쪽에 AXIS Audio Manager Pro의 웹 인터페이스가 표시됩니다.

비고

웹 인터페이스에 액세스하려면 Management Client 시스템과 AXIS Audio Manager Pro 서버 간에 직접 연결이 필요합니다.

AXIS Audio Manager Pro 웹 인터페이스에서 구역, 대상, 오디오 클립 또는 시각적 프로파일을 변경한 경우:

- **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동합니다.
- **Update(업데이트)**를 클릭합니다.

카메라를 대상 또는 구역에 연결

카메라를 특정 대상 또는 구역에 연결하고 Smart Client의 카메라 보기에서 직접 사용할 수 있습니다.

1. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 대상 또는 구역을 선택합니다.
2. **Associated camera(s)(연결된 카메라)**에서 **Add cameras...(카메라 추가...)**를 클릭하고 대상 또는 구역과 연결할 카메라를 선택합니다.

카메라가 대상 또는 구역에 연결되면 Smart Client의 카메라 보기 도구 모음에 가 표시됩니다.

시각적 프로파일 생성

- Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동합니다.
- **Audio Manager Pro 서버**를 클릭하여 웹 인터페이스를 표시합니다.
- **Visual profiles(시각적 프로파일)**를 클릭하여 시각적 프로파일을 생성하거나 편집합니다.

시각적 프로파일에 대한 자세한 내용은 *AXIS Audio Manager Pro 사용자 설명서*를 참조하십시오.

AXIS Audio Manager Edge 모드

AXIS Audio Manager Edge 는 대부분의 Axis 스피커에 사전 설치되어 있으며 이 모드를 선택하면 자동으로 감지됩니다. AXIS Audio Manager Edge 모드가 제대로 작동하려면 사이트 리더, 페이징 소스용 중개 장치 및 독립형 스피커를 VMS에 추가해야 합니다.

비고

AXIS Audio Manager Edge 모드에서는 내장 카메라 오디오 출력 및 기타 호환되지 않는 오디오 장치를 사용할 수 없습니다.

AXIS Audio Manager Edge에 대해 자세히 알아보려면 *AXIS Audio Manager Edge 사용자 설명서*를 참조하십시오.

AXIS Audio Manager Edge 모드에서 스피커 및 구역 구성

오디오 클립을 재생하고 실시간으로 말하려면 먼저 구역에 대한 페이징을 켜야 합니다.

1. Management Client에서 **Site Navigation(사이트 탐색)** > **Devices(장치)** > **Speakers(스피커)**로 이동하여 장치 그룹을 추가하거나 장치 그룹에서 스피커를 추가 및 제거합니다.
2. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 **Edge** 모드가 선택되어 있는지 확인합니다.
   그러면 Speaker 관리자가 VMS시스템의 모든 스피커를 검색하고 Smart Client에서 사용할 수 있는 모든 AXIS Audio Manager Edge 사이트 및 영역을 표시합니다.
3. 사이트 목록에서 페이징 오프가 있는 영역을 선택합니다.
4. **Turn on paging for the zone(영역에 대한 페이징을 켜기)**를 선택합니다.

구역 또는 페이징 소스를 변경할 경우:

5. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동합니다.
6. **Update(업데이트)**를 클릭합니다.

비고

설정에 실패하면 AXIS Audio Manager Edge 구성을 확인하고 다시 시도하십시오.



카메라를 스피커 또는 구역에 연결

Smart Client의 카메라 보기에서 특정 스피커 또는 구역을 직접 사용하려면 해당 스피커 또는 구역을 카메라에 연결할 수 있습니다.

1. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 스피커 또는 구역을 선택합니다.
2. **Associated cameras(연결된 카메라)** 창에서 **+ Add cameras(+ 카메라 추가)**를 클릭하고 스피커 또는 구역과 연결할 카메라를 선택합니다.

카메라가 스피커, 장치 그룹 또는 구역에 연결되면 Smart Client의 카메라 보기 도구 모음에 가 표시됩니다.

스피커에 오디오 클립 업로드

Smart Client의 스피커 또는 구역에서 오디오 클립을 재생하려면 먼저 Management Client의 스피커에 오디오 클립을 업로드해야 합니다.

1. 스피커에 업로드하려는 오디오 클립을 기본 폴더 **C:₩Users₩Public₩Documents₩AXIS Optimizer for Milestone XProtect - Audio Clips₩**에 넣습니다.
2. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 스피커 또는 구역을 선택합니다.
3. **Audio clips(오디오 클립)**으로 이동하고 스피커에 업로드하려는 클립 앞에 **+**를 클릭합니다.

Legacy mode(레거시 모드)

Legacy mode(레거시 모드)는 VMS에 추가된 Axis 스피커 및 기타 오디오 지원 Axis 장치의 기본 기능을 확장합니다. 다른 모드와 달리 Legacy mode(레거시 모드)는 여러 스피커에 대한 동기화된 방송을 지원하지 않습니다.

Legacy mode(레거시 모드)에서 스피커 구성

1. Management Client에서 **Site Navigation(사이트 탐색)** > **Devices(장치)** > **Speakers(스피커)**로 이동하여 장치 그룹을 추가하거나 장치 그룹에서 스피커를 추가 및 제거합니다.
2. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 legacy mode(레거시 모드)가 선택되어 있는지 확인합니다.
3. 을 클릭합니다.
   3.1. **Manage Side Panel(사이드 패널 관리)** 창에서 Smart Client에 표시할 스피커를 선택합니다.
   3.2. **Add(추가)**를 클릭하고 **OK**를 클릭합니다.
   Visible(가시적인) 패널에 액세스할 수 있는 모든 사용자에 대해 패널이 Smart Client에 표시됩니다.
4. 스피커를 제거하려면:
   4.1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 를 클릭합니다.
   4.2. **Manage Side Panel(사이드 패널 관리)** 창에서 제거할 스피커를 선택합니다.
   4.3. **Remove(제거)**와 **OK**를 클릭합니다.

카메라를 스피커 또는 스피커 그룹에 연결

카메라를 특정 대상 또는 구역에 연결하고 Smart Client의 카메라 보기에서 직접 사용할 수 있습니다.

1. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 스피커 또는 스피커 그룹을 선택합니다.
2. **Associated camera(s)(연결된 카메라)**에서 **Add cameras...(카메라 추가...)**를 클릭하고 스피커 또는 스피커 그룹과 연결할 카메라를 선택합니다.

카메라가 스피커 또는 스피커 그룹에 연결되면 Smart Client의 카메라 보기 도구 모음에 가 표시됩니다.

스피커에 오디오 클립 업로드

Smart Client의 스피커 또는 구역에서 오디오 클립을 재생하려면 먼저 Management Client의 스피커에 오디오 클립을 업로드해야 합니다.

1. 스피커에 업로드하려는 오디오 클립을 기본 폴더 **C:₩Users₩Public₩Documents₩AXIS Optimizer for Milestone XProtect - Audio Clips₩**에 넣습니다.
2. Management Client에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Speaker manager(스피커 관리자)**로 이동하고 스피커 또는 스피커 그룹을 선택합니다.
3. **Audio clips(오디오 클립)**으로 이동하고 스피커에 업로드하려는 클립 앞에 **+**를 클릭합니다.



볼륨 변경

스피커의 볼륨을 변경하려면:

1. Management Client에서 **Site Navigation(사이트 탐색)** > **Speaker manager(스피커 관리자)**로 이동하고 스피커 또는 스피커 그룹을 선택합니다.

2. **Volume(볼륨)**으로 이동하고 원하는 볼륨으로 조정합니다.



스피커에서 오디오 재생

1. Smart Client에서 **Live(라이브)** > **MIP plug-ins(MIP 플러그인)** > **Axis speaker control(Axis 스피커 제어)**로 이동하고 드롭다운 목록에서 스피커 또는 구역을 선택합니다.
2. 마이크가 스피커로 오디오를 내보내게 하려면:
   2.1. 말하는 동안 을 길게 누릅니다.
   마이크 레벨 미터에 음성 활동이 표시되는지 확인합니다.
3. 스피커에서 오디오 클립 재생:
   3.1. **Media clip(미디어 클립)**으로 이동하고 드롭다운 목록에서 오디오 클립을 선택합니다.
   3.2. 선택한 스피커에서 오디오 클립 재생을 시작하려면 재생을 클릭합니다.

카메라 보기에서 스피커로 오디오 재생

1. Smart Client에서 카메라 보기로 이동합니다.
2. 스피커, 장치 그룹 또는 구역에 연결이 있는 경우, 도구 모음에 이 표시됩니다.
3. 을 클릭하여 **Axis speaker control(Axis 스피커 제어)** 창을 엽니다.
4. 마이크가 스피커로 오디오를 내보내게 하려면:
   4.1. 말하는 동안 을 길게 누릅니다.
   마이크 레벨 미터에 음성 활동이 표시되는지 확인합니다.
5. 스피커에서 오디오 클립 재생:
   5.1. **Media clip(미디어 클립)**으로 이동하고 드롭다운 목록에서 오디오 클립을 선택합니다.
   5.2. 선택한 스피커에서 오디오 클립 재생을 시작하려면 재생을 클릭합니다.

알람에서 스피커로 오디오 재생

1. Smart Client에서 **Alarms(알람)**로 이동합니다.
2. 카메라를 소스로 사용하는 알람을 선택합니다.
   스피커 또는 구역에 연결이 설정되어 있으면 스피커 컨트롤이 표시됩니다.
3. 마이크가 스피커로 오디오를 내보내게 하려면:
   – 말하는 동안 을 길게 누릅니다.
   마이크 레벨 미터에 음성 활동이 표시되는지 확인합니다.
4. 스피커에서 오디오 클립 재생:
   – **Media clip(미디어 클립)**으로 이동하고 드롭다운 목록에서 오디오 클립을 선택합니다.
   – 선택한 스피커에서 오디오 클립 재생을 시작하려면 재생을 클릭합니다.

스피커 상호 작용에 대한 시각적 동작 설정

Smart Client에서는 Axis speaker control(Axis 스피커 제어), 카메라 보기 또는 Alarm Manager(알람 관리자)에서 직접 장치의 시각적 동작 방식을 설정할 수 있습니다.

비고

시각적 프로파일은 AXIS Audio Manager Pro 모드에서만 지원됩니다.

- **Axis speaker control(Axis 스피커 제어)** 사이드 패널에서:
  - 를 클릭합니다.
  - 드롭다운 목록에서 시각적 프로파일을 선택합니다.
  - 선택한 시각적 프로파일과 연결된 현재 텍스트를 재정의하려면 텍스트 상자에 입력합니다.
- 카메라 보기에서:
  - 특정 카메라 보기로 이동합니다.
  - 스피커, 장치 그룹 또는 구역에 연결이 있는 경우, 도구 모음에 이 표시됩니다.
  - 을 클릭하여 **Axis speaker control(Axis 스피커 제어)** 창을 엽니다.
  - 를 클릭합니다.
- **Alarm Manager(알람 관리자)**에서:
  - 이벤트를 선택하고 카메라 보기로 이동한 다음 을 클릭합니다.

카메라 보기 또는 알람의 오디오 클립 북마크

카메라 보기 또는 Alarms(알람)에서 스피커 컨트롤로 오디오 클립을 재생하면 누가 어떤 장치에서 오디오 클립을 재생했는지에 대한 정보가 포함된 북마크가 생성됩니다.

오디오 클립 북마크를 검색하려면 다음을 수행합니다.

1. Smart Client에서 **Search(검색)**으로 이동합니다.
2. 시간 간격과 하나 이상의 카메라를 선택합니다.
3. **Search for(검색)** > **Bookmarks(북마크)** > **New search(새 검색)**를 클릭합니다.

방문자 관리

인터콤 플러그인

Axis 네트워크 인터콤은 하나의 장치로 통신, 영상 감시 및 원격 출입 통제를 결합합니다. AXIS Optimizer로 VMS와 함께 Axis 인터콤을 쉽게 구성 및 사용할 수 있습니다. 예를 들어 콜을 받고 도어를 열 수 있습니다.

인터콤 설정



도어 잠금은 일반적으로 인터콤의 첫 번째 릴레이에 연결해야 합니다. AXIS Optimizer는 **Usage(용도)** 정보를 기반으로 사용할 출력 포트를 결정합니다. **Usage = Door(용법 = 도어)**(기본적으로 RELAY1)를 가진 첫 번째 포트를 사용합니다.

비고

요구 사항

- Axis 인터콤
- 전화를 받는 PC에 설치된 마이크
- Smart Client 시작 및 실행

비고

버전 5.0.X.X부터 AXIS Optimizer는 이전 버전과 다른 구성 방법으로 VMS에서 인터콤을 구성합니다. 입력 1 대신 메타데이터 장치를 통화 감지에 사용할 수 있습니다. 기존 구성 방법도 계속 지원하지만, 신규 설치에는 새 구성 방법을 권장합니다.

1. 콜을 받고 도어를 제어하려는 각 클라이언트에 AXIS Optimizer의 최신 버전을 설치하십시오.
2. Management Client에 로그인합니다.
3. Recording Server에 Axis 인터콤을 추가합니다.
4. Management Client에서 필요한 모든 장치를 활성화합니다. Smart Client에서 전화를 받으려면 다음이 필요합니다.
   - 카메라 1
   - 마이크
   - 스피커
   - 메타데이터
   - 입력 2(포트 2의 인터콤에 보안 릴레이가 연결된 경우의 선택 사항)
   - 도어에 연결된 출력. 도어에 연결된 출력을 알고 있다면 해당 출력을 선택합니다. 그렇지 않은 경우 모든 출력을 선택합니다.
5. **Site Navigation > Devices > Metadata(사이트 탐색 > 장치 > 메타데이터)**로 이동하여 설치하려는 인터콤의 메타데이터 장치를 선택합니다.
6. **Settings(설정)**를 클릭합니다.
7. **Event data(이벤트 데이터)**를 **Yes(예)**로 설정합니다.
8. **Save(저장)**를 클릭합니다.
9. 입력 2를 활성화한 경우에도 설정해야 합니다.
   9.1. **Site Navigation > Devices > Input(사이트 탐색 > 장치 > 입력)**으로 이동하여 입력 2를 선택합니다.
   9.2. **Events(이벤트)**를 클릭한 다음 **Add(추가)**를 클릭합니다.
   9.3. **Input Falling event(떨어지는 이벤트 입력)**를 선택하고 활성화된 입력에 추가합니다. **Input Rising event(상승하는 이벤트 입력)**에 대해 반복합니다.
   9.4. **Save(저장)**를 클릭합니다.
10. *인터콤에 대한 권한 설정, on page 37*에서 특정 역할에 대한 권한 설정에 관해 알아보십시오.
11. *테스트 전화 걸기, on page 38*.

인터콤에 대한 권한 설정

통화를 처리하려면 먼저 권한을 활성화해야 합니다.

1. **사이트 탐색 > 보안 > 역할**로 이동합니다.
2. 역할을 선택합니다.
3. **전반적인 보안**으로 이동합니다.
4. 각 보안 그룹에 필요한 권한이 설정되어 있는지 확인하십시오. **Hardware(하드웨어)**로 이동하고 **Driver commands(드라이버 명령)**를 선택합니다.
5. 시스템 수준에서 권한을 설정하려면 **Overall Security**(전반적인 보안)로 이동하십시오.
   장치 수준에서 권한을 설정하려면 **Device(장치)**로 이동합니다.
6. 보안 그룹에 대한 권한 설정:

6.1. **Cameras(카메라)**로 이동합니다. **Read(읽기)** 및 **View live(실시간 보기)**를 선택합니다.

6.2. **Microphones(마이크)**로 이동합니다. **Read(읽기)** 및 **Listen(듣기)**을 선택합니다.

6.3. **Overall Security(전반적인 보안)**를 위해 **Speakers(스피커)**로 이동합니다. **Read(읽기)** 및 **Speak(말하기)**를 선택합니다.
Device(장치)의 경우 **Speakers(스피커)**로 이동하여 **Read(읽기)**를 선택합니다. 그런 다음 **Speech(음성)**를 탭하고 **Speak(말하기)**를 선택합니다.

6.4. **Metadata(메타데이터)**로 이동합니다. **Read(읽기)** 및 **Live(실시간)**를 선택합니다.

6.5. **Input(입력)**으로 이동합니다. **Read(읽기)**를 선택합니다.

6.6. **Output(출력)**으로 이동합니다. **Read(읽기)** 및 **Activate(활성화)**를 선택합니다.

특정 인터콤의 호출을 처리하는 교환원을 제어하기 위해 권한을 할당하는 방법:

1. 특정 인터콤의 메타데이터 장치 1에 대해 **Read(읽기)** 권한을 선택합니다.
2. 다른 모든 역할에 대해 이 권한을 지웁니다. 권한이 없는 사용자는 전화를 받을 수 없습니다.

통화 기록을 보려면 추가 권한이 필요합니다.

1. 시스템 수준에서 권한을 설정하려면 **Overall Security**(전반적인 보안)로 이동하십시오.
장치 수준에서 권한을 설정하려면 **Device(장치)**로 이동합니다.
2. 보안 그룹에 대해 다음 권한을 선택합니다.
2.1. **Cameras(카메라)**로 이동합니다. **Playback(재생)** 및 **Read sequences(순서 읽기)**를 선택합니다.
2.2. **Microphones(마이크)**로 이동합니다. **Playback(재생)** 및 **Read sequences(순서 읽기)**를 선택합니다.
2.3. **Speakers(스피커)**로 이동합니다. **Listen(듣기)**, **Playback(재생)**, **Read sequences(순서 읽기)**를 선택합니다.

테스트 전화 걸기

1. Smart Client에서 **Settings > Axis intercom options(설정 > Axis 인터콤 옵션)**로 이동합니다.
2. **Test call(콜 테스트)**을 클릭합니다.
3. 인터콤을 선택하고 **Make call(전화 걸기)**을 클릭합니다.

통화 중 에코 방지

푸쉬-투-토크를 사용하면 인터콤을 통해 한 번에 한 방향으로만 오디오를 보낼 수 있습니다. 통화 중에 에코가 있을 때 푸쉬-투-토크를 켤 수 있습니다.

Push-to-talk(푸시-투-토크)을 켜려면 다음 단계를 따르십시오.

- Smart Client에서 **Settings(설정)** > **Axis intercom options(Axis 인터콤 옵션)**로 이동합니다.
- **Call(통화)**로 이동하여 **Push-to-talk(푸시-투-토크)**를 선택합니다.

실시간 보기에서 인터콤 제어

각 인터콤 및 인터콤 보기의 장치를 빠르게 제어하기 위해



을 클릭합니다.

내가 어떻게 해야 하나요?	지침	의견
잠금을 열기	 > **Access(액세스)** 또는 **Extended access(확장된 액세스)**를 클릭합니다.	잠금이 해제되면 **Access(액세스)** 또는 **Extended access(확장된 액세스)**를 클릭할 수 없습니다.
도어가 잠겨 있는지 또는 잠겨 있지 않은지 확인	 을 클릭하고 메뉴 하단의 상태를 읽습니다.	-

내가 어떻게 해야 하나요?	지침	의견
인터콤 앞에 있는 사람과 대화	 > **Start call(호출 시작)**을 클릭합니다.	호출 창이 열리고 인터콤과 양방향 통신이 시작됩니다.
어제 호출한 사람 찾기	 > **Call history(호출 기록)**를 클릭합니다.	현재 인터콤과의 호출 목록이 표시됩니다.

실시간 보기에서 콜에 응답

방문자가 인터콤의 호출 버튼을 누르면 실행 중인 각 Smart Client에 호출 창이 나타납니다. 호출 창은 창 크기를 조정하면 적절한 카메라 보기(예: 코리더 또는 가로 보기)를 자동으로 선택합니다.

내가 어떻게 해야 하나요?	지침	의견
호출에 답하기	**Accept(수락)**를 클릭합니다	운영자와 인터콤 옆 사람 사이의 양방향 오디오 채널이 열립니다.
내가 바쁘기 때문에 다른 운영자에게 전화 걸기	**X**를 클릭하여 창 닫기	전화를 끊으면 다른 교환원이 다른 클라이언트의 전화를 받을 수 있습니다. 인터콤은 누군가가 전화를 받을 때까지 계속 울리고 깜박입니다. 아무도 응답하지 않으면 통화 기록에서 통화 상태가 부재중이 됩니다.
시각적 확인으로 이미 도어를 열었고 그 사람과 이야기 할 필요가 없기 때문에 통화를 거부합니다. 원치 않는 방문자와 통화하고 싶지 않아 전화를 거부	**거절**을 클릭하기	통화를 거부하면 다른 클라이언트의 통화 창이 자동으로 닫힙니다. 다른 운영자는 콜을 받을 수 없습니다. 인터콤이 멈추고 벨이 울리며 깜박이면 호출 창이 닫힙니다.

내가 어떻게 해야 하나요?	지침	의견
		통화 기록에서 통화 상태가 응답함으로 표시됩니다.
도어 열기	**Access(액세스)**를 클릭합니다	인터콤 잠금 장치가 7초 동안 열립니다. 도어가 열린 상태로 유지되는 시간을 구성하는 방법: 1. Smart Client에서 **Settings > Axis intercom options > Door access(설정 > Axis 인터콤 옵션 > 도어 액세스)**로 이동합니다. 2. **Access time(액세스 시간)**을 변경합니다.
운영자에서 인터콤까지의 오디오를 일시적으로 중지합니다.	**Mute(무음)**를 클릭합니다.	-
PTT(push-to-talk)이 활성화되면 방문자와 대화하십시오.	**Talk(대화)**를 클릭하기	방문자가 말하는 것을 들으려면 말하기 버튼을 놓습니다.
콜을 종료합니다.	**Hang up(끊기)**을 클릭합니다.	기본 자동 닫기 설정은 통화를 거절하거나 끊을 때 통화 창이 닫히는 것입니다. 기본 통화 창 동작을 변경하는 방법: 1. Smart Client에서 **Settings > Axis intercom options > Call(설정 > Axis 인터콤 옵션 > 콜)**로 이동합니다. 2. **Auto-close window(자동 닫기 창)**를 선택 해제합니다.

호출 창에 여러 대의 카메라 표시

호출 창에 카메라를 최대 3개까지 동시에 표시할 수 있습니다. 즉, 동일한 호출 창 내에서 인터콤의 비디오 스트림과 다른 두 카메라의 비디오 스트림을 볼 수 있습니다. 예를 들어 배달원과 배달 도어 주변을 동시에 보고 싶을 때 유용합니다.

호출 창에서 여러 카메라를 구성하는 방법:

1. Smart Client에서 **Settings > Axis intercom options(설정 > Axis 인터콤 옵션)**로 이동합니다. **Call > Intercom settings(통화 > 인터콤 설정)**로 이동합니다.
2. **Selected device(선택한 장치)**로 이동하고 구성하려는 장치를 선택합니다.
3. **Multiple cameras(다중 카메라)**로 이동하십시오. 어떤 인터콤으로 보고 싶은지 통화 창에서 **camera 1(카메라 1)**을 선택합니다.
4. 인터콤 호출 시 통화 창에서 **camera 2(카메라 2)** 및 **camera 3(카메라 3)**으로 표시할 연결된 카메라를 선택합니다.

5. **Intercom settings(인터콤 설정)** 창을 닫습니다.

통화 창 액션

호출 창 액션을 사용하면 XProtect 룰 엔진의 룰에 연결된 사용자 정의 이벤트를 설정할 수 있습니다. 설정하고 사용할 수 있는 이벤트는 역할에 따라 다릅니다.

통화 창 액션을 설정하려면:

1. Smart Client에서 **Settings > Axis intercom options(설정 > Axis 인터콤 옵션)**로 이동합니다.
2. **Call > Intercom settings(통화 > 인터콤 설정)**로 이동합니다.
3. **Selected device(선택한 장치)**로 이동하고 구성하려는 장치를 선택합니다.
4. 사용하려는 통화 창 작업을 선택하려면 **Call window actions(통화 창 액션)**를 클릭합니다.

통화 창 작업에는 두 가지 유형이 있습니다.

- **Access button action(액세스 버튼 액션)**: 액세스 버튼 동작을 설정하면, **Access(액세스)** 버튼의 기본 액션이 재정의됩니다. 예를 들어, **Access(액세스)** 버튼으로 일련의 도어를 열도록 설정할 수 있습니다.
- **Custom action(사용자 지정 액션)**: 사용자 정의 액션을 설정하면 통화 창에 버튼이 표시됩니다. 이 버튼을 클릭하면 사용자 정의 액션을 실행할 수 있습니다. 사용자 지정 액션은 이메일 보내기, 알람 실행, 연속 녹화 시작 등 반드시 출입 도어 액세스와 관련되지 않은 액션입니다.

호출 창에 페이지 표시

AXIS I8307-VE Network Intercom 사용 시 호출 창에 페이지를 표시할 수 있습니다. 이는 인터콤 앞에 서 있는 사람에게 지도나 영업 시간과 같은 정보를 표시하는 데 유용합니다.

먼저 인터콤의 웹 인터페이스에서 이 페이지들을 구성합니다. *AXIS I8307-VE Network Intercom*을 참조하십시오.

인터콤에서 수신 호출이 올 때:

1. **Show page(페이지 표시)**를 클릭하여 장치에 구성된 모든 페이지의 대화 상자를 봅니다.
2. **Load previews(미리 보기 로드)**를 클릭하여 모든 페이지의 미리 보기를 봅니다.
   구성된 페이지 하나의 미리 보기를 보려면 페이지 위로 마우스를 가져가 이미지 아이콘을 클릭합니다.
3. 구성된 페이지를 클릭하여 인터콤에 표시합니다.

카메라 1은 카메라 피드용, 카메라 2는 페이지 표시용과 같이 서로 다른 연결된 카메라를 사용하여 인터콤 카메라 피드와 페이지를 모두 표시하도록 호출 창을 설정할 수 있습니다. *호출 창에 여러 대의 카메라 표시, on page 42*를 참조하십시오.

호출이 종료되면 페이지가 닫힙니다. 새 호출용 페이지를 표시하려면 위의 단계를 반복합니다.

콜 내선 번호 필터링

기본적으로 인터콤에 연결된 모든 PC가 콜을 수신합니다. VMS에서 내선 번호를 추가하고 필터링하여 VMS 시스템의 특정 스마트 클라이언트로 통화를 라우팅하도록 인터콤을 구성할 수 있습니다. 통화 라우팅 일정을 설정하고 대체 연락처를 추가할 수 있습니다. SIP 기반 연락처로 통화를 라우팅하고 대체 연락처로 추가해도 됩니다.

인터콤 웹 인터페이스에서

1. **Communication(통신)** > **SIP**로 이동합니다.
2. **Enable SIP(SIP 활성화)**를 선택합니다.
3. **Save(저장)**를 클릭합니다.
4. **Communication(통신)** > **VMS Calls(VMS 통화)**로 이동합니다.

5. **Allow calls in the video management system (VMS)(영상 관리 시스템(VMS)에서 통화 허용)**가 켜져 있는지 확인합니다.
6. **Communication(통신)** > **Contact list(연락처 목록)**로 이동합니다.
7. **Recipients(수신자)**에서 + 을 클릭하여 새 연락처를 추가합니다. 새 연락처 정보를 입력하고 **Save(저장)**를 클릭합니다. 여러 연락처를 추가해도 됩니다.
   - **SIP address(SIP 주소)**에서 `VMS_CALL:<extension>`을 입력합니다. `<extension>`을 연락처의 통화 내선 번호 이름(예: `ReceptionA`)으로 바꿉니다.
   - 연락처의 일정을 설정하려면 해당 연락처의 **Availability(가용성)**를 선택합니다.
   - 본래 연락처에서 응답하지 않는 경우 전화를 받을 대체 연락처를 추가할 수 있습니다(예: `ReceptionB`).
8. **Communication(통신)** > **Calls(통화)**로 이동합니다.
9. AXIS OS 11.6 이전 버전이 설치된 장치의 경우 **Make calls in the video management system (VMS)(비디오 관리 시스템(VMS)에서 통화하기)**를 끕니다.
10. **Recipients(수신자)**에서 **VMS** 연락처를 제거하고, 생성한 새 연락처를 추가합니다.

Management Client에서

통화 감지를 위해 메타데이터 장치를 사용하도록 VMS의 인터콤을 구성하는 것이 좋습니다. *인터콤 설정, on page 36*를 참조하십시오.

Smart Client에서

콜을 받아야 하는 모든 사용자에 대해 착신 내선을 설정합니다. 사용자 수준에 이 설정이 저장됩니다. 이는 사용자가 어떤 PC를 사용하든지 상관없이 콜을 받을 수 있다는 의미입니다.

1. 콜을 받아야 하는 사용자로 Smart Client에 로그인합니다.
2. **Settings > Axis intercom options(설정 > Axis 인터콤 옵션)**으로 이동합니다.
3. **Call(통화) > Call extension(통화 내선)**에서 연락처의 통화 내선 이름을 입력합니다(예: `ReceptionA`). 이제 사용자는 통화 내선 번호가 필터 값과 일치하는 경우에만 콜을 받게 됩니다.
   여러 통화 내선 이름을 추가하려면 세미콜론으로 구분합니다(예: `ReceptionA;ReceptionC`).

콜 기록 보기

call history(호출 기록)에서 응답 및 부재중 전화 및 도어가 잠금 해제되었는지 확인할 수 있습니다. 통화 중 선택하고, 가능한 경우 해당 재생 비디오를 볼 수 있습니다.

1. Smart Client에서 인터콤 보기로 이동합니다.

2. 
> **Call history(호출 기록)**를 클릭합니다.

비고

콜 내역은 통화 39개 및 액세스 로그 기록 1000개로 제한됩니다. 대화를 자주 음소거하면 제한된 콜 수를 줄일 수 있습니다.

도어가 잠금 해제되었을 때 등록하려면 Axis 인터콤의 유지 시간(일)을 설정해야 합니다.

1. Management Client에서 **Tools > Options > Alarm and Events > Event retention(도구 > 옵션 > 알람 및 이벤트 > 이벤트 보존)**으로 이동합니다.
2. **Output Activated(출력 활성화)** 및 **Output Deactivated(출력 비활성화)**에 대한 시간을 설정합니다.

활성화된 호출가 없을 때 마이크 끄기

Axis 인터콤으로 전화가 오지 않을 때 마이크를 끌 수 있습니다. 활성화된 호출이 있으면 마이크가 켜집니다.

비고

- 마이크를 끄려면 관리자 권한이 필요합니다.
- 이는 페더레이션 아키텍처에서 또는 대체 연락처를 사용하는 경우 지원되지 않습니다.

1. Smart Client에서 **Settings(설정)** > **Axis intercom options(Axis 인터콤 옵션)**로 이동합니다.
2. **Turn off intercom microphone when no active call(활성화된 호출이 없을 때 인터콤 마이크 끄기)**을 선택합니다.

강제로 도어가 열리면 알람을 수신

도어에 보안 릴레이(입력 2)가 있는 경우 Smart Client의 호출 창에 있는 도어 오버레이는 문이 열리거나 닫힐 때 표시됩니다. 즉, 도어가 잠겨 있는 상태에서 누군가가 강제로 도어를 열면 알람을 받을 수 있습니다.

비고

알람을 수신하려면 하나 이상의 Smart Client가 실행 중이어야 합니다.

알람을 구성하는 방법:

1. Smart Client에서 **Settings > Axis intercom options > Administrator options(설정 > Axis 인터콤 옵션 > 관리자 옵션)**로 이동합니다.
2. **Trigger an alarm when a door has been forced open(도어가 강제로 열렸을 때 알람 트리거)**을 선택합니다.

도어가 너무 오래 열려 있을 경우 알람 수신

도어에 보안 릴레이(입력 2)가 있는 경우 Smart Client의 호출 창에 있는 도어 오버레이는 문이 열리거나 닫힐 때 표시됩니다. 즉, 누군가가 도어를 열고 도어가 너무 오랫동안 열려 있으면 알람을 받을 수 있습니다.

비고

알람을 수신하려면 하나 이상의 Smart Client가 실행 중이어야 합니다.

알람을 구성하는 방법:

1. Smart Client에서 **Settings > Axis intercom options > Administrator options(설정 > Axis 인터콤 옵션 > 관리자 옵션)**로 이동합니다.
2. **Trigger an alarm when a door has been open longer than (s)(도어가 (초)보다 오래 열려 있으면 알람 트리거)**를 선택합니다.
3. 알람이 울리기 전에 문이 열려 있을 수 있는 시간을 입력합니다.

클라이언트의 전화 수신 방지

호출을 받지 않도록 클라이언트를 구성할 수 있습니다. 즉, 누군가가 호출할 때 특정 클라이언트에서 호출 창이 열리지 않습니다.

1. Smart Client에서 **Settings > Axis intercom options > Call(설정 > Axis 인터콤 옵션 > 콜)**로 이동합니다.
2. **Receive calls on this client(이 클라이언트에서 호출 받기)**를 지웁니다.

오디오 시각화

마이크 보기

Smart Client에 하나 이상의 마이크 보기를 추가하여 시스템의 오디오를 시각화할 수 있습니다. 그런 다음 실시간 보기와 재생 모두에서 오디오를 모니터링할 수 있습니다. Axis 장치에 내장된 오디오 디텍션을 사용하여 오디오 레벨이 특정 레벨 이상으로 상승하는 경우를 확인할 수 있습니다. 일반적으로 사용 사례는 다음과 같습니다.

- *동시에 여러 마이크 듣기, on page 48*
- *오디오로 사건을 디텍션, on page 48*
- *사건이 발생한 후 조사, on page 48*

비고

요구 사항

- VMS Smart Client 2020 R2 이상.

마이크 보기용 VMS 구성

1. 감지 수준 설정:
   1.1. Management Client에서 **Site Navigation > AXIS Optimizer > Device assistant(사이트 탐색 > AXIS Optimizer > 장치 도우미)**로 이동하고 장치를 선택합니다.
   1.2. **디텍터** 설정을 엽니다. 이러한 설정을 여는 방법은 장치의 소프트웨어 버전에 따라 다릅니다.
   1.3. **오디오 디텍션**으로 이동하고 **입력 1 사운드 수준**을 필요에 맞게 수정합니다.
2. 카메라에서 VMS로 이벤트 가져오기:
   2.1. Management Client에서 **사이트 탐색 > 장치 > 마이크**로 이동합니다.
   2.2. 마이크를 클릭한 다음 **Events(이벤트)**를 클릭합니다.
   2.3. **Audio Falling(오디오 폴링)Audio Rising(오디오 라이징)** 이벤트를 추가합니다.
3. 시스템이 감지된 오디오에 대한 메타데이터를 유지하는 기간을 구성:
   3.1. **Tools > Options > Alarm and Events > Device events(도구 > 옵션 > 알람 및 이벤트 > 장치 이벤트)**를 이동합니다.
   3.2. **Audio Falling(오디오 폴링)**을 찾고 유지 시간을 설정합니다.
   3.3. **Audio Raising(오디오 레이징)**을 찾고 유지 시간을 설정합니다.
4. 오디오 녹음을 설정했는지 확인합니다. 예를 들어 오디오를 항상 녹음하거나 오디오 레이징 또는 오디오 폴링 이벤트를 기반으로 녹음 룰을 생성할 수 있습니다.
5. 마이크 보기와 함께 사용하려는 각 마이크에 대해 위의 단계를 반복합니다.
6. Smart Client에서**Settings > Timeline > Additional data(설정 > 타임라인 > 추가 데이터)**를 이동하고 **Show(표시)**를 선택합니다.

Smart Client에 마이크 보기 추가

1. Smart Client를 열고 **Setup(설정)**을 클릭합니다.
2. **Views(보기)**로 이동합니다.
3. **Create new view(새로 보기 만들기)**를 클릭하고 형식을 선택합니다.
4. **System overview > AXIS Optimizer(시스템 오버뷰 > AXIS Optimizer)**로 이동합니다.
5. **Microphone view(마이크 보기)**를 클릭하고 보기에 드래그합니다.
6. 마이크를 선택합니다.
7. **설정**을 클릭합니다.

마이크 보기 사용

- 실시간 보기
  - 오디오 레벨은 현재 레벨이 오른쪽으로 이동하고 최대 60초 오디오 기록이 왼쪽으로 이동하는 막대 그래프로 표시됩니다.
  - 마이크에서 오디오를 듣는 보기 in(인)을 클릭합니다.
  - 각 마이크 보기에는 헤드폰 아이콘이 있습니다. 보기 자체를 선택하지 않고도 각 보기에서 오디오를 음소거 또는 음소거 해제하려면 아이콘을 클릭합니다. 이렇게 하면 여러 마이크를 동시에 들을 수 있습니다.
- 재생
  - 마이크에 사용할 수 있는 오디오가 감지되면 아이콘이 강조 표시됩니다.
  - 노란색 막대는 장치에 설정한 디텍션 레벨에 따라 오디오가 감지되었음을 나타냅니다.
  - 마이크에서 오디오를 듣는 보기 in(인)을 클릭합니다.

– 각 마이크 보기에는 헤드폰 아이콘이 있습니다. 보기 자체를 선택하지 않고도 각 보기에서 오디오를 음소거 또는 음소거 해제하려면 아이콘을 클릭합니다. 이렇게 하면 여러 마이크를 동시에 들을 수 있습니다.

동시에 여러 마이크 듣기

마이크 보기를 사용하면 실시간 보기와 재생에서 동시에 여러 마이크를 들을 수 있습니다.

1. *마이크 보기용 VMS 구성, on page 47*.
2. Smart Client를 열고 **Setup(설정)**을 클릭합니다.
3. **Views(보기)**로 이동합니다.
4. **Create new view(신규 보기 생성)**를 클릭하고 분할 보기를 선택합니다.
5. **System overview > AXIS Optimizer(시스템 오버뷰 > AXIS Optimizer)**로 이동합니다.
6. 듣고 싶은 각 마이크에 대한 설명:
   6.1. **Microphone view(마이크 보기)**를 클릭하고 보기에 드래그합니다.
   6.2. 마이크를 선택합니다.
7. **설정**을 클릭합니다.
8. 각 마이크에 대해 각 마이크 보기에서 헤드폰 아이콘을 클릭하여 음소거 또는 음소거 해제를 결정합니다. 이제 음소거 해제된 모든 마이크를 동시에 들을 수 있습니다.

오디오로 사건을 디텍션

예를 들어 화장실과 같이 카메라 설치가 허용되지 않는 영역에서 작업을 모니터링할 수 있습니다. 마이크 보기에서 사건이 발생했을 때, 즉 사운드 수준이 디텍션 수준을 초과할 때를 빠르게 확인할 수 있습니다.

1. *마이크 보기용 VMS 구성, on page 47*. 모니터링하려는 장치 및 영역에 대한 관련 디텍션 레벨을 설정하는 것을 잊지 마십시오.
2. Smart Client에서 실시간 보기에 장치와 함께 마이크 보기 추가하고, *Smart Client에 마이크 보기 추가, on page 47*을(를) 참조하십시오.

사건이 발생한 후 조사

사고가 발생한 후 마이크에서 오디오가 디텍션 시간을 재생 타임라인에서 빠르게 식별할 수 있습니다.

1. *마이크 보기용 VMS 구성, on page 47*.
2. Smart Client에서 재생할 관련 장치와 함께 하나 또는 여러 개의 마이크 보기를 추가하고 *Smart Client에 마이크 보기 추가, on page 47*을(를) 참조하십시오.

포렌식 검색

AXIS Optimizer는 중앙 집중식 검색에서 Axis 장치에 대해 네 가지 검색 범주를 제공합니다.

- *포렌식 검색, on page 49* (객체 검색)
- *차량 검색, on page 52*
- *영역 속도 검색, on page 55*
- *컨테이너 검색, on page 57*

또한 Smart Client에 별도의 번호판 검색 탭을 추가할 수 있습니다. *Axis 번호판, on page 58*을(를) 참조하십시오.

중앙 집중식 패널에서 이러한 검색 카테고리를 구성할 수 있습니다. *Axis 검색 카테고리 구성, on page 105*을 참조하십시오.

포렌식 검색

AXIS OS 9.50 이상이 설치된 Axis 카메라는 카메라의 화각에서 현재 움직이는 모든 객체를 설명하는 메타데이터를 생성합니다. VMS는 이 데이터를 해당 비디오 및 오디오와 함께 기록할 수 있습니다. AXIS Optimizer의 포렌식 검색 기능을 사용하면 이 데이터를 분석하고 검색할 수 있습니다. 포렌식 검색을 사용하여 장면의 모든 활동에 대한 개요를 얻거나 관심 있는 특정 개체 또는 이벤트를 빠르게 찾을 수 있습니다.

시작하기 전

1. 카메라에 최신 AXIS OS 버전이 있는지 확인하십시오.
2. VMS의 버전이 올바른지 확인:
   - Corporate 2019 R3 이상 또는 Expert 2019 R3 이상
   - Professional+ 2022 R3 이상 또는 Express+ 2022 R3 이상
3. 카메라 시간은 NTP와 동기화됩니다.
4. 객체 유형인 **사람**, **차량**, **자전거**, **버스**, **자동차** 또는 **트럭**으로 필터하려면:
   4.1. AXIS Object Analytics를 지원하는 Axis 장치를 사용합니다. *제품 선택기*에서 분석 필터를 참조하십시오.
   4.2. **System > Analytics metadata(시스템 > 분석 메타데이터)**로 이동하고 카메라 웹 페이지에서 **Analytics Scene Description(분석 장면 설명)**을 활성화합니다.
5. **차량** 색상 **Upper body clothing color(상반신 옷 색상)** 또는 **Lower body clothing color(하반신 옷 색상)**를 필터링하려면:
   5.1. AXIS Object Analytics를 지원하는 Axis 장치를 사용합니다. *제품 선택기*에서 분석 필터를 참조하십시오.
   5.2. ARTPEC-8 또는 CV25 지원 Axis 장치를 사용합니다. *제품 선택기*에서 SoC(System-on-chip) 필터를 참조하십시오.

포렌식 검색 구성



1. Management Client에서 카메라에 대해 메타데이터 장치가 활성화되어 있는지 확인하십시오.
2. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.

- **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
- **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.

3. **Site Navigation > Devices > Metadata(사이트 탐색 > 장치 > 메타데이터)**를 이동합니다.
4. 장치를 선택하고 **Record(녹화)**를 클릭합니다. **녹화**가 활성화되었는지 확인합니다.
   기본적으로 메타데이터는 VMS가 장면에서 움직임을 감지할 때만 기록됩니다. 따라서 객체의 움직임을 놓치지 않도록 모션 임계값을 환경에 맞게 조정하는 것이 좋습니다.
5. **Settings(설정)**를 클릭하고 **Analytics data(분석 데이터)**가 활성화되어 있는지 확인합니다.
6. Smart Client의 실시간 보기를 열고 개체 위에 바운딩 박스가 표시되고 박스가 올바르게 디스플레이되는지 확인합니다.
   시계가 NTP 시간에 적응하는 데 시간이 걸릴 수 있습니다.
7. 시스템이 비디오 및 메타데이터를 녹화할 수 있도록 최소 15분을 기다립니다. 그런 다음 검색을 시작하고 *검색 수행, on page 50*을(를) 참조하십시오.
8. AXIS OS 11.10 이상을 실행하는 장치에서 검색 속도를 개선하려면 **통합 메타데이터**를 켭니다. *메타데이터와 검색, on page 103*을 참조하십시오.

검색 수행



비고

이 검색 기능을 사용하기 전에 Management Client에서 구성해야 합니다. 이 작업을 수행하는 방법을 알아보려면 *포렌식 검색 구성, on page 49*을(를) 참조하십시오.

1. Smart Client에서 **Search(검색)**으로 이동합니다.
2. 시간 간격과 하나 이상의 카메라를 선택합니다.
3. **Search for > Forensic search > New search(검색 > 포렌직 검색 > 신규 검색)**을 클릭합니다. 각 검색 결과에 대해 미리보기에 객체와 객체의 이동 경로가 표시됩니다.
   - 썸네일은 객체가 가장 잘 보였을 때의 비디오 프레임을 보여줍니다.
   - 녹색 점은 카메라가 물체를 처음 감지한 위치를 표시합니다.
   - 빨간 점은 카메라가 객체를 마지막에 감지한 위치를 표시합니다.
   - 검색 결과에 대한 전체 비디오 시퀀스를 보려면 선택하고 미리 보기 패널에서 **Play forward(앞으로 재생)**를 클릭합니다.
   - 그래픽 오버레이를 숨기려면 **Bounding boxes(바운딩 박스)**로 이동하고 **Hide(숨장치)**를 선택합니다.

   비고

   카메라에서 실행되는 분석 응용 프로그램(예: AXIS Object Analytics 및 AXIS Loitering Guard)도 비디오의 오버레이를 번인할 수 있습니다. 이러한 오버레이를 제거하려면 애플리케이션의 웹 구성 페이지로 이동하십시오.
4. 검색 결과의 수를 좁히려면 검색 필터를 선택하십시오.
   다양한 필터를 사용하는 방법에 대한 자세한 내용은 *검색 미세 조정, on page 51*을(를) 참조하십시오.
5. 자세히 살펴보고 싶은 검색 결과를 선택하십시오. 예를 들어 북마크에 추가하거나 *고품질 PDF 보고서 생성, on page 58*(을)를 할 수 있습니다.

검색 미세 조정

검색 결과를 좁히기 위해 하나 이상의 검색 필터를 사용할 수 있습니다.

- **Region of interest(관심 영역)**
  특정 영역에서 이동한 객체를 감지합니다.
- **Object direction(객체 방향)**
  장면에서 특정 경로를 따라 이동한 객체 감지: 왼쪽으로, 오른쪽으로, 아래로 또는 위로.
- **객체 유형**
  특정 유형의 객체 감지: 사람, 차량, 자전거, 버스, 자동차 또는 트럭.

비고

- 속도(km/h 또는 mph) 및 번호판는 AXIS Q1686–DLE Radar-Video Fusion Camera에서만 지원됩니다.
- 이를 사용하려면 먼저 속도(km/h 또는 mph)와 번호판을 활성화해야 합니다. 이렇게 하려면 *Axis 검색 카테고리 구성, on page 105*을 참조하십시오.
- **속도(km/h 또는 mph)**
  일정 속도 내에서 이동하는 차량을 감지합니다.
- **번호판**
  특정 번호판이 있는 차량을 감지합니다. 또한 이를 사용하여 특정 알파벳이나 숫자가 포함된 번호판을 검색할 수 있습니다.
- **차량 색상**
  선택한 색상의 차량을 감지합니다.
- **Upper body clothing color(상체 옷 색상)**
  사람의 상반신에서 선택한 색상의 옷을 감지합니다.
- **Lower body clothing color(하체 옷 색상)**
  사람의 하반신에서 선택한 색상의 옷을 감지합니다.
- **Time-of-day(하루의 시간)**
  하루 중 특정 시간에 감지된 객체를 감지합니다. 이 필터는 여러 날에 걸쳐 검색할 때 유용하지만 매일 특정 시간(예: 오후)의 객체에만 관심이 있습니다.
- **Minimum time in scene (s)(장면의 최소 시간)**
  최소 시간(초) 동안 감지 및 추적된 객체를 감지합니다. 이 필터는 관심 없는 객체, 예를 들어 멀리 있는 객체 및 잘못된 객체(조명 효과)를 필터링합니다. 기본값은 1초입니다. 즉, 필터가 설정되지 않은 경우 지속 시간이 1초 미만인 객체는 제외됩니다.
- **흔들리는 객체(이미지의 %)**
  바람에 흔들리는 깃발이나 나무와 같이 제약 조건 영역에서만 이동한 객체를 제외합니다. 기본값은 5~100%입니다. 즉, 필터가 설정되지 않은 경우 이미지 영역의 5% 이상 이동하지 않은 객체는 제외됩니다.

제한 사항

- 검색 결과에 대한 올바른 비디오 장면을 얻으려면 정확한 시계 동기화가 중요합니다.
- 포렌식 검색으로 분석된 데이터는 장면의 관점을 고려하지 않습니다. 즉, 객체가 카메라에 얼마나 가까이 있느냐에 따라 객체의 크기와 속도가 달라집니다.
- 폭우나 폭설 같은 기상 조건이 감지 정확도에 영향을 미칠 수 있습니다.
- 저조도 장면에서 객체의 대비가 좋은 경우 분석이 더욱 정확해집니다.
- 경우에 따라 단일 객체가 여러 결과를 생성할 수 있습니다. 예를 들어 객체가 다른 객체에 의해 일시적으로 가려질 때 추적이 손실되는 경우가 있습니다.
- 오버레이는 XProtect 버전에 따라 다를 수 있습니다. 이에 대한 예는 다음과 같습니다. 비디오 미리 보기의 오버레이에는 XProtect 2020 R3이 필요하고 오버레이 색상에는 XProtect 2020 R2가 필요합니다.
- 포렌식 검색이 180도 회전된 비디오 스트림에서 작동하게 하는 방법:

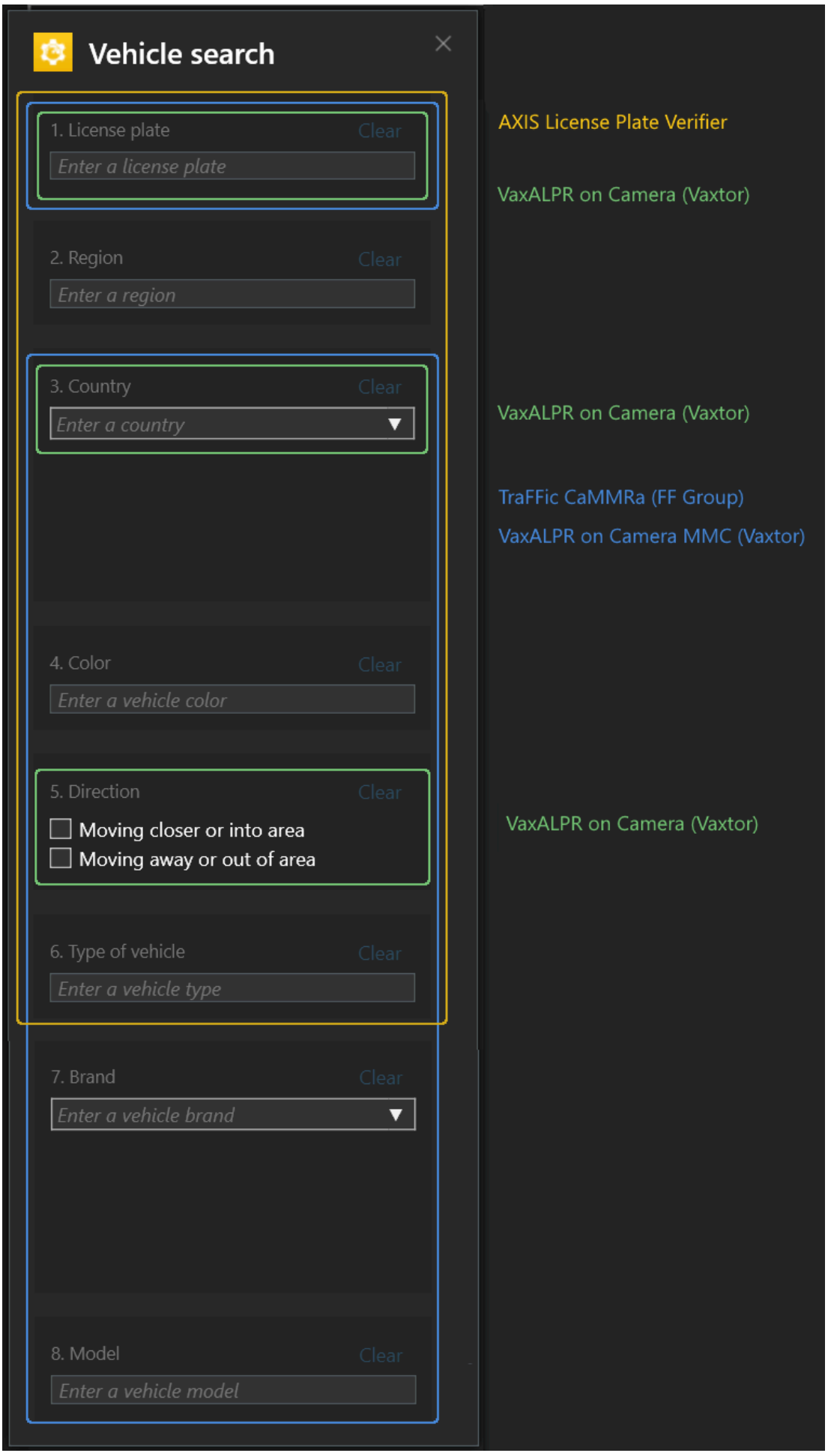
  - 카메라에서 AXIS OS 10.6 이상을 사용하거나
  - 녹화 서버에서 Device Pack 11.0 이상 사용
- 좋은 색상 감지를 얻으려면 카메라의 화이트 밸런스 설정이 정확해야 합니다

차량 검색

AXIS Optimizer를 카메라에 설치된 특정 애플리케이션과 함께 사용하면 차량에 대한 비디오 증거를 검색, 식별 및 공유할 수 있습니다. 차량 검색은 다음 애플리케이션의 번호판 데이터를 지원합니다.

- Axis Communications의 *AXIS License Plate Verifier*
- *CAMMRA AI* by FF Group(버전 1.3 이상 필요)
- Vaxtor Recognition Technologies의 *VaxALPR On Camera*
- Vaxtor Recognition Technologies의 *VaxALPR On Camera MMC*

사용할 수 있는 검색 필터는 카메라에 설치한 애플리케이션에 따라 다르며 *검색 미세 조정, on page 54*을(를) 참조하십시오.


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

차량 검색 구성

비고

요구 사항

- VMS 시스템:
  - Corporate 또는 Expert 2019 R3 이상
  - Professional+ 또는 Express+ 2022 R3 이상
- NTP와 동기화된 카메라 시간
- 에 나열된 애플리케이션 중 하나

1. Management Client에서 선택한 애플리케이션을 실행하는 카메라를 추가합니다.
2. 필요한 모든 장치를 활성화하십시오. AXIS License Plate Verifier를 사용하려면 Camera 1과 Metadata 1이 필요합니다.
3. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.
   - **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
   - **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.
4. 메타데이터 구성:
   4.1. **Site Navigation(사이트 탐색) > Recording Server(녹화 서버)**로 이동하고 장치를 찾습니다.
   4.2. 메타데이터 1을 선택하고 **Settings(설정)**을 클릭합니다.
   4.3. **Metadata stream > Event data(메타데이터 스트림 > 이벤트 데이터)**로 이동하고 **Yes (예)**를 선택합니다.
5. **Record settings(녹화 설정)** 탭으로 이동하고 메타데이터에 대해 녹화가 활성화되어 있는지 확인합니다.
6. **Save(저장)**를 클릭합니다.
7. 표준 사용자에 대해 작동하도록 애플리케이션을 구성합니다.
   7.1. 특정 카메라 및 사용자에 대한 읽기 및 재생 권한을 추가합니다.
   7.2. 특정 카메라와 사용자를 위해 메타데이터에서 읽기 및 재생 권한을 추가합니다.

차량 검색

1. Smart Client에서 **Search(검색)**으로 이동합니다.
2. 시간 간격과 하나 이상의 카메라를 선택합니다.
3. **Search for > Vehicle search > New search(검색 > 차량 검색 > 신규 검색)**을 클릭합니다.
4. 검색 결과의 수를 좁히려면 검색 필터를 선택하십시오.
   다양한 필터에 대해 자세히 알아보려면 *검색 미세 조정, on page 54*을(를) 참조하십시오.
5. 자세히 살펴보고 싶은 검색 결과를 선택하십시오. 예를 들어 북마크에 추가하거나 *고품질 PDF 보고서 생성, on page 58*(을)를 할 수 있습니다.

검색 미세 조정

검색 결과를 좁히기 위해 하나 이상의 검색 필터를 사용할 수 있습니다. 다른 애플리케이션은 다른 필터 옵션을 제공합니다.

- **번호판**
  특정 번호판 번호를 찾습니다.
  애플리케이션: AXIS License Plate Verifier, VaxALPR On Camera, CAMMRA AI 또는 VaxALPR On Camera MMC.
- **지역**

특정 지역의 차량을 찾습니다.
애플리케이션: AXIS License Plate Verifier 2.9.19.

비고

최적의 지역 인식을 위해 Axis License Plate Verifier 설정에서 카메라 위치를 설정합니다.

- **국가**
  특정 국가의 차량을 찾습니다.
  애플리케이션: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI 또는 VaxALPR On Camera MMC.
- **색상**
  특정 색상의 차량을 찾습니다.
  애플리케이션: Axis License Plate Verifier 2.9.19, CAMMRA AI 또는 VaxALPR On Camera MMC.
- **방향**
  특정 방향으로 움직이는 차량을 찾습니다.
  애플리케이션: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI 또는 VaxALPR On Camera MMC.
- **차량의 종류**
  특정 종류의 차량을 찾습니다.
  애플리케이션: Axis License Plate Verifier 2.9.19, CAMMRA AI 또는 VaxALPR On Camera MMC.
- **브랜드**
  특정 브랜드의 차량을 찾습니다.
  애플리케이션: CAMMRA AI 또는 VaxALPR On Camera MMC.
- **모델**
  특정 모델의 차량을 찾습니다.
  애플리케이션: CAMMRA AI 또는 VaxALPR On Camera MMC.

검색 속도 최적화

시스템이 VMS 메타데이터 장치에 저장하는 데이터를 제어하여 검색 속도를 개선할 수 있습니다.

- 분석 데이터가 필요하지 않은 경우 분석 데이터를 비활성화합니다.
  - **Devices** > **Metadata(장치 > 메타데이터)**로 이동하고 장치를 선택하세요.
  - **Settings(설정)**를 클릭하고 **Analytics data(분석 데이터)**를 비활성화합니다.
- 분석 데이터가 필요한 경우, 사용할 수 있다면 통합 메타데이터를 대신 사용할 수 있습니다. *메타데이터와 검색, on page 103*을 참조하십시오.
- AXIS License Plate Verifier에서 필요하지 않은 이벤트를 비활성화합니다. AXIS Optimizer가 작동하려면 **Lost(손실)** 이벤트만 필요합니다. *AXIS License Plate Verifier*를 참조하십시오.
- AXIS OS 12.8 이상을 사용해야 합니다.

영역 속도 검색

AXIS Optimizer에서 구역 속도 검색을 사용하여 카메라 보기에서 미리 결정된 구역에 들어갈 때 감지된 과속 차량을 검색할 수 있습니다. Zone speed search(구역 속도 검색)는 *AXIS Speed monitor* 애플리케이션과 함께 작동하여 카메라의 실시간 보기에서 레이더 감지 구역에 있는 차량의 속도를 시각화합니다. AXIS Zone 속도 검색을 사용하면 특정 필터를 설정하여 검색 범위를 좁히고 조사 중에 비디오 증거를 내보내고 공유할 수 있습니다.

구역 속도 검색 구성

비고

요구 사항

- VMS 시스템:

  - Corporate 또는 Expert 2019 R3 이상
  - Professional+ 또는 Express+ 2022 R3 이상
- NTP와 동기화된 카메라 시간

1. Management Client에서 선택한 애플리케이션을 실행하는 카메라를 추가합니다.
2. 필요한 모든 장치를 활성화하십시오. AXIS Zone 속도 검색을 사용하려면 Camera 1과 Metadata 1이 필요합니다.
3. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.
   - **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
   - **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.
4. 메타데이터를 구성하려면:
   4.1. **Site Navigation(사이트 탐색) > Recording Server(녹화 서버)**로 이동하고 장치를 찾습니다.
   4.2. 메타데이터 1을 선택하고 **Settings(설정)**을 클릭합니다.
   4.3. **Metadata stream > Event data(메타데이터 스트림 > 이벤트 데이터)**로 이동하고 **Yes (예)**를 선택합니다.
5. **Record settings(녹화 설정)** 탭으로 이동하고 메타데이터에 대해 녹화가 활성화되어 있는지 확인합니다.
6. **Save(저장)**를 클릭합니다.
7. 표준 사용자에 대해 작동하도록 애플리케이션을 구성하려면:
   7.1. 특정 카메라 및 사용자에 대한 읽기 및 재생 권한을 추가합니다.
   7.2. 특정 카메라와 사용자를 위해 메타데이터에서 읽기 및 재생 권한을 추가합니다.

구역 속도 이벤트 검색



1. Smart Client에서 **Search(검색)**으로 이동합니다.
2. 시간 간격과 하나 이상의 카메라를 선택합니다.
3. **Search for > Zone speed search > New search(검색 > 영역 속도 검색 > 신규 검색)**을 클릭합니다.
4. 검색 결과의 수를 좁히려면 검색 필터를 선택하십시오.
   다양한 필터에 대해 자세히 알아보려면 *검색 미세 조정, on page 56*을(를) 참조하십시오.
5. 자세히 살펴보고 싶은 검색 결과를 선택하십시오. 예를 들어 북마크에 추가하거나 *고품질 PDF 보고서 생성, on page 58*(을)를 할 수 있습니다.

검색 미세 조정

과속 사건의 검색 결과를 좁히기 위해 하나 이상의 검색 필터를 사용할 수 있습니다.

- **최대 속도**
  이벤트 기간 동안 영역에 있는 모든 객체의 최대 속도를 필터링합니다. 최대 속도의 하한과 상한을 모두 설정할 수 있습니다.
- **객체 유형**

만약에 **Vehicle(차량)**을 선택하면 해당 구역에서 가장 빠른 물체가 차량으로 분류된 과속 이벤트만 검색에 표시됩니다.

- **영역 이름**
  이름으로 영역을 검색하고 필터링합니다.

컨테이너 검색

AXIS Optimizer를 특정 애플리케이션과 함께 사용하면 컨테이너에 대한 비디오 증거를 검색, 식별 및 공유할 수 있습니다. 컨테이너 검색은 이 애플리케이션의 데이터를 지원합니다.

- Vaxtor Recognition Technologies의 *VaxOCR Containers*

컨테이너 검색 구성

비고

요구 사항

- VMS 시스템:
  - Corporate 또는 Expert 2019 R3 이상
  - Professional+ 또는 Express+ 2022 R3 이상
- NTP와 동기화된 카메라 시간
- 에 나열된 애플리케이션

1. Management Client에서 선택한 애플리케이션을 실행하는 카메라를 추가합니다.
2. 필요한 모든 장치를 활성화하십시오.
3. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.
   - **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
   - **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.
4. 메타데이터 구성:
   4.1. **Site Navigation(사이트 탐색) > Recording Server(녹화 서버)**로 이동하고 장치를 찾습니다.
   4.2. 메타데이터 1을 선택하고 **Settings(설정)**을 클릭합니다.
   4.3. **Metadata stream > Event data(메타데이터 스트림 > 이벤트 데이터)**로 이동하고 **Yes (예)**를 선택합니다.
5. **Record settings(녹화 설정)** 탭으로 이동하고 메타데이터에 대해 녹화가 활성화되어 있는지 확인합니다.
6. **Save(저장)**를 클릭합니다.
7. 표준 사용자에 대해 작동하도록 애플리케이션을 구성합니다.
   7.1. 특정 카메라 및 사용자에 대한 읽기 및 재생 권한을 추가합니다.
   7.2. 특정 카메라와 사용자를 위해 메타데이터에서 읽기 및 재생 권한을 추가합니다.

컨테이너 검색

1. Smart Client에서 **Search(검색)**으로 이동합니다.
2. 시간 간격과 하나 이상의 카메라를 선택합니다.
3. **Search for > Container search > New search(검색 > 컨테이너 검색 > 신규 검색)**을 클릭합니다.
4. 검색 결과의 수를 좁히려면 검색 필터를 선택하십시오.
   다양한 필터에 대해 자세히 알아보려면 *검색 미세 조정, on page 58*을(를) 참조하십시오.

5. 자세히 살펴보고 싶은 검색 결과를 선택하십시오. 예를 들어 북마크에 추가하거나 *고품질 PDF 보고서 생성, on page 58*(을)를 할 수 있습니다.

검색 미세 조정

검색 결과를 좁히기 위해 하나 이상의 검색 필터를 사용할 수 있습니다. 모든 필터 옵션은 애플리케이션 VaxOCR Containers에서 가져옵니다.

- **컨테이너 코드**
  특정 컨테이너 코드를 찾습니다.
- **소유자**
  특정 소유자의 컨테이너를 찾습니다.
- **소유자 코드**
  특정 소유자의 컨테이너를 찾습니다.
- **크기**
  특정 크기 및 유형의 컨테이너를 찾습니다.
- **사이즈 코드**
  특정 크기 및 유형의 컨테이너를 찾습니다.
- **도시 또는 국가**
  특정 도시 또는 국가의 컨테이너를 찾습니다.
- **검증**
  소유자 코드 또는 제어 숫자를 통해 이미 검증된 컨테이너를 찾으십시오.

고품질 PDF 보고서 생성



검색 결과를 기반으로 보고서를 생성합니다. 이 기능을 사용하여 결과에 고해상도 이미지를 포함할 수 있습니다.

1. Smart Client에서 검색을 수행합니다.
2. 보고서에 포함할 검색 결과를 선택합니다.
3. p,255mm,sfx)=″graphics:graphicBEF7A01B23D95F074530E51119754E17″ > **Create high quality PDF report(고품질 PDF 보고서 생성)**를 클릭합니다.
4. (선택 사항)**Report name(보고서 이름)**, **Report destination(보고 대상)** 및 **Notes(참고)**를 입력합니다.
5. 각 검색 결과에 대해 보고서에 포함할 프레임을 선택하십시오. 이미지를 확대하려면 더블 클릭합니다.
6. **Create(생성)**를 클릭합니다. 보고서가 준비되면 알림을 받게 됩니다.

Axis 번호판

Smart Client에서 번호판 검색 및 관리용으로 별도의 탭을 추가할 수 있습니다. 이 탭은 LPR 지원 Axis 카메라에서 제공하는 정보를 기반으로 번호판 관리, 검색 및 내보내기와 관련된 모든 운영자 작업을 중앙 집중화합니다.



시작하기 전

- VMS 버전 2018 R3 이상이 있는지 확인
- VMSe 장치 팩 10.1 이상이 있는지 확인
- 카메라 시간은 NTP와 동기화됩니다
- 에 나열된 애플리케이션 중 하나를 사용합니다.

Axis 번호판 구성

1. Management Client에서 선택한 애플리케이션을 실행하는 카메라를 추가합니다.
2. 필요한 모든 장치를 활성화하십시오. AXIS License Plate Verifier를 사용하려면 Camera 1과 Metadata 1이 필요합니다.
3. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.
   - **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
   - **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.
4. 메타데이터 구성:
   4.1. **Site Navigation(사이트 탐색) > Recording Server(녹화 서버)**로 이동하고 장치를 찾습니다.
   4.2. 메타데이터 1을 선택하고 **Settings(설정)**을 클릭합니다.
   4.3. **Metadata stream > Event data(메타데이터 스트림 > 이벤트 데이터)**로 이동하고 **Yes (예)**를 선택합니다.
5. **Record settings(녹화 설정)** 탭으로 이동하고 메타데이터에 대해 녹화가 활성화되어 있는지 확인합니다.
6. **Save(저장)**를 클릭합니다.

번호판 검색

1. Smart Client에서, **Axis license plates(Axis 번호판)**로 이동합니다.
   탭이 보이지 않으면, **Settings > Axis search options(설정 > Axis 검색 옵션)**로 이동하고 **Show license plate tab(번호판 탭 표시)**을 선택합니다.
2. **Add camera...(카메라 추가...)**를 클릭하고 관련 카메라를 선택한 다음 > **Close(닫기)**를 클릭합니다.
   시스템에 카메라를 추가하려면 관리자여야 합니다. 카메라가 번호판을 감지하면 카메라가 촬영한 번호판의 크롭 이미지를 포함하여 목록에 실시간으로 표시됩니다. 검색 결과는 5000개가 넘는 결과를 표시하지 않습니다.
3. 번호판과 **Time interval(시간 간격)**을 입력하여 검색 결과를 필터링합니다.
   - 선택한 두 날짜 사이의 사용자 지정 **Time interval(시간 간격)**을 입력하여 검색 결과를 필터링합니다.

실시간 번호판 검색

1. Smart Client에서, **Axis license plates(Axis 번호판)**로 이동합니다.

탭이 보이지 않으면, **Settings > Axis search options(설정 > Axis 검색 옵션)**로 이동하고 **Show license plate tab(번호판 탭 표시)**을 선택합니다.

2. **Add camera...(카메라 추가...)**를 클릭하고 관련 카메라를 선택한 다음 > **Close(닫기)**를 클릭합니다.
   시스템에 카메라를 추가하려면 관리자여야 합니다. 카메라가 번호판을 감지하면 카메라가 촬영한 번호판의 크롭 이미지를 포함하여 목록에 실시간으로 표시됩니다. 검색 결과는 5000개가 넘는 결과를 표시하지 않습니다.
3. 번호판을 입력하고 **Time interval(시간 간격)** > **Live(실시간)**를 선택하여 검색 결과를 필터링합니다.

검색 미세 조정

검색 결과를 좁히기 위해 하나 이상의 검색 필터를 사용할 수 있습니다.

- **시간 간격**
  일정 기간 내의 검색 적중을 필터링합니다.
- **번호판**
  부분 또는 전체 번호판 텍스트를 필터링합니다.
- **카메라**
  특정 카메라에서 감지한 검색 히트를 필터링합니다.
- **방향**
  특정 방향으로 움직이는 차량을 필터링합니다.
- **Lists(목록)**
  특정 사이트에서 검색 적중을 필터링하고 허용, 차단 및 사용자 지정 목록에서 검색 적중을 필터링합니다. 설정 방법에 대한 더 자세한 내용은 *번호판 목록을 중앙에서 관리, on page 23*을(를) 참조하십시오.

검색 속도 최적화

시스템이 VMS 메타데이터 장치에 저장하는 데이터를 제어하여 검색 속도를 개선할 수 있습니다.

- 분석 데이터가 필요하지 않은 경우 분석 데이터를 비활성화합니다.
  - **Devices** > **Metadata(장치 > 메타데이터)**로 이동하고 장치를 선택하세요.
  - **Settings(설정)**를 클릭하고 **Analytics data(분석 데이터)**를 비활성화합니다.
- 분석 데이터가 필요한 경우, 사용할 수 있다면 통합 메타데이터를 대신 사용할 수 있습니다. *메타데이터와 검색, on page 103*을 참조하십시오.
- AXIS License Plate Verifier에서 필요하지 않은 이벤트를 비활성화합니다. AXIS Optimizer가 작동하려면 **Lost(손실)** 이벤트만 필요합니다. *AXIS License Plate Verifier*를 참조하십시오.
- AXIS OS 12.8 이상을 사용해야 합니다.

번호판 검색 결과를 PDF 보고서로 내보내기

이 기능을 사용하여 고품질 이미지가 포함된 PDF 보고서로 관심 영역의 검색 결과를 컴파일하십시오.

1. **Export(내보내기)를 클릭합니다...**.
2. **PDF...**를 선택합니다
3. (선택 사항)**Report name(보고서 이름)**, **Report destination(보고 대상)** 및 **Notes(참고)**를 입력합니다.
4. 각 검색 결과에 대해 보고서에 포함할 프레임을 선택하십시오. 이미지를 확대하려면 이미지를 두 번 클릭합니다.
5. **Create(생성)**를 클릭합니다. 보고서가 준비되면 알림을 받게 됩니다.

번호판 검색 결과를 CSV 보고서로 내보내기

이 기능을 사용하여 대량의 검색 결과를 CSV 보고서로 컴파일합니다.

1. **Export(내보내기)를 클릭합니다...**.
2. **CSV...**를 선택합니다
3. 내보낼 파일의 대상을 선택합니다.

Axis insights

Axis Insight는 차트와 대시보드를 통해 장치의 데이터 오버뷰를 제공합니다. 이를 통해 모든 장치의 메타데이터를 볼 수 있습니다. 감지된 물체, 식별된 차량, 경보에 대한 데이터를 볼 수 있습니다. 새 대시보드를 만들고 다른 사용자와 공유할 수도 있습니다.

Axis insights는 기본 관리자 및 운영자 보기에서 사용할 수 있습니다. Axis insights의 기본 관리자 보기는 관리자 권한이 있는 사용자만 사용할 수 있으며, 기본 운영자 보기는 적절한 권한이 있는 모든 운영자가 사용할 수 있습니다. *역할 설정을 구성, on page 98*을 참조하십시오. 운영자 보기는 사용자가 설정한 선택된 카메라 보기의 특정 데이터를 제공하며, 관리자 보기는 전체 시스템의 개요를 제공합니다.

Axis insights 접근

- **Smart Client**로 이동하여 **Axis insights**를 클릭합니다.
- **Dashboard(대시보드)**: 드롭다운 목록에서 대시보드를 선택합니다.
- **Camera view(카메라 보기)**: 데이터 개요를 보려면 특정 카메라 보기를 선택합니다.
- **Time range(시간 범위)**: 특정 시간 범위를 선택합니다.
- **Auto-update(자동 업데이트)**: 데이터를 자동으로 새로 고치려면 켭니다.

••• 상황에 맞는 메뉴에는 다음이 포함됩니다.

- **Edit dashboard(대시보드 편집)**: 대시보드를 편집, 공유 또는 제거합니다.
- **Add chart(차트 추가)**: 대시보드에서 새 차트를 만듭니다.
- **Axis insights 정보**: Axis insights에 대해 알아봅니다.

••• 각 차트의 컨텍스트 메뉴에 포함된 항목:

- **Maximize chart(차트 최대화)**: 차트를 확대하려면 클릭합니다.
- **Copy as image(이미지로 복사)**: 차트를 클립보드에 복사하려면 클릭합니다.
- **Export(내보내기)**: 차트를 PNG 또는 CSV로 내보내려면 클릭합니다.
- **Edit chart(차트 편집)**: 차트를 편집하려면 클릭합니다.
- **Remove chart(차트 제거)**: 차트를 제거하려면 클릭합니다.

비고

- 일부 차트에서 그림을 클릭하면 추가 정보를 볼 수 있습니다.
- : 대시보드의 각 차트에 현재 적용되는 선택 항목을 표시합니다.

새 스케줄 생성

1. **Dashboard(대시보드)**: 드롭다운 목록에서 **Add dashboard(대시보드 추가)**를 선택합니다.
2. **Empty(비어 있음)**를 클릭하여 새 대시보드를 생성하거나 **From existing dashboard(기존 대시보드에서)**를 클릭하여 시스템에서 사용할 수 있는 대시보드와 유사한 대시보드를 생성합니다.

3. **Name(이름)**: 대시보드 이름을 입력합니다.
4. **Allow other users to view this dashboard(다른 사용자가 이 대시보드를 볼 수 있도록 허용)**: 읽기 전용 모드로 다른 사용자와 대시보드를 공유하려면 클릭합니다.
5. **Apply(적용)**을 클릭합니다.
6. **Add chart(차트 추가)**: 새 차트를 추가하려면 클릭합니다.
   - **차트 유형 선택**: 원하는 차트 유형을 선택하고 **Next(다음)**를 클릭합니다. 비디오 분석, 차량, 꺾은선형 차트 등의 태그 또는 차트 제목을 사용하여 차트 유형을 검색할 수 있습니다.
   - **데이터 선택 항목 수정**: 각 카테고리에 적용 가능한 필터를 선택합니다.
   - **모양 조정**: 텍스트를 편집하고 차트 크기를 선택합니다.

대시보드 드롭다운 목록 구성

비고

- 기본적으로 사용자가 생성한 대시보드만 볼 수 있습니다.

Dashboard(대시보드) 드롭다운 목록에서 다른 사용자가 공유한 대시보드를 보는 방법:

1. **Shared dashboards(공유 대시보드)**로 이동합니다.
2. 드롭다운 목록에 추가하려는 각 공유 대시보드의 토글을 켭니다.

특정 카메라 보기의 인사이트 표시

카메라 보기에서 실시간 및 재생 비디오를 보는 동안 활성 카메라 보기가 미리 선택된 상태로 Axis insights를 열 수 있습니다.

특정 카메라 보기에 대해 Axis insights를 열려면 다음을 수행합니다.

1. **Smart Client**로 이동하고 보기를 엽니다.
2. **Show insights(인사이트 표시)**를 클릭합니다.

Axis insights 구성

1. 카메라가 Axis Object Analytics를 지원하는지 확인합니다. *Axis Product Selector*에서 분석을 확인하세요.
2. 카메라의 날짜와 시간이 올바르게 설정되어 있는지 확인하십시오.
3. Management Client에서 카메라에 대해 메타데이터 장치가 활성화되어 있는지 확인하십시오.
4. 메타데이터 장치가 카메라와 관련되어 있는지 확인합니다.
   - **Devices(장치)** > **Camera(카메라)**로 이동하여 장치를 선택합니다.
   - **Client(클라이언트)** 탭으로 이동하여 카메라의 메타데이터 장치가 **Related metadata (관련 메타데이터)**에서 선택되어 있는지 확인합니다.
5. Axis insights에서 사용 가능한 모든 데이터를 보려면 *AXIS Scene Metadata*를 사용하여 카메라에서 장면 분석을 활성화합니다.
   5.1. **Devices** > **Metadata(장치 > 메타데이터)**로 이동하고 장치를 선택하세요.
      - **Record(녹화)**을 클릭하고 **Recording(녹화)**이 활성화되어 있는지 확인하세요.
      - **Settings(설정)**를 클릭하고 **Analytics data(분석 데이터)**가 활성화되어 있는지 확인합니다.

   5.1. 가능한 경우 **Consolidated metadata(통합 메타데이터)**를 켜서 로딩 시간을 단축하세요. *메타데이터와 검색, on page 103*을 참조하십시오.
6. *AXIS Object Analytics*, *AXIS Image Health Analytics* 또는 *Environmental sensors(환경 센서)*를 사용하는 차트 유형에 데이터를 활성화하는 방법:
   - **Devices** > **Metadata(장치 > 메타데이터)**로 이동하고 장치를 선택하세요.

- **Record(녹화)**을 클릭하고 **Recording(녹화)**이 활성화되어 있는지 확인하세요.
- **Settings(설정)**를 클릭하고 **Event data(이벤트 데이터)**가 활성화되어 있는지 확인합니다.
- VMS에서 이 장치의 메타데이터를 항상 기록하도록 룰을 생성할 것을 권장합니다.

7. 보안 그룹에 대한 권한 설정:
   7.1. **Site Navigation** > **Security** > **Roles(사이트 탐색 > 보안 > 역할)**로 이동합니다.
   7.2. 역할을 선택하세요.
   7.3. **Cameras(카메라)**로 이동합니다. **Read(읽기)**를 선택합니다.
   7.4. **Metadata(메타데이터)**로 이동합니다. **Read(읽기)**, **Live(라이브)**, **Playback(재생)**을 선택합니다.
8. Axis insights에 번호판 메타데이터를 추가하려면 *Axis 번호판 구성, on page 59*을 참조하세요

Axis insights 문제 해결

문제	해결책
차트에는 "no data(데이터 없음)"이 표시됩니다.	Axis insight를 구성해야 합니다. *Axis insights 구성, on page 62*을 참조하세요.
운영자 보기를 로드하는 데 시간이 매우 오래 걸립니다.	• 시간 범위를 줄이세요. • 더 적은 수의 장면 분석 카메라로 카메라 보기를 생성하고 사용합니다. • 통합 메타데이터를 활성화하려면 *메타데이터와 검색, on page 103*을 참조하세요.

비디오 디워핑

디워핑은 광각 또는 어안 렌즈로 인해 기하학적으로 왜곡된 이미지의 원근감을 평평하게 보정합니다. VMS의 Axis 디워핑은 모든 Axis 360° 파노라마 카메라와 함께 사용할 수 있습니다. 디워핑은 카메라에서 직접 실행하거나 Smart Client에서 실행합니다.

디워핑에 대한 자세한 내용:

- 클라이언트 측 디워핑을 사용하면 라이브 및 녹화된 비디오 모두에서 부드러운 디워핑을 얻을 수 있습니다.
- 보기로 돌아가면 자동으로 최신 디워핑 위치로 이동합니다.
- 비디오를 내보낼 때 디워핑이 포함됩니다.
- 홈 포지션을 저장할 수 있습니다. *홈 위치 설정, on page 66*을(를) 참조하십시오.
- 운영자가 디워핑 보기를 제어하고 편집할 수 있는지 여부를 구성할 수 있습니다. *운영자가 디워핑 보기를 제어하고 편집할 수 있도록 허용, on page 67*을(를) 참조하십시오.

디워핑 보기 생성

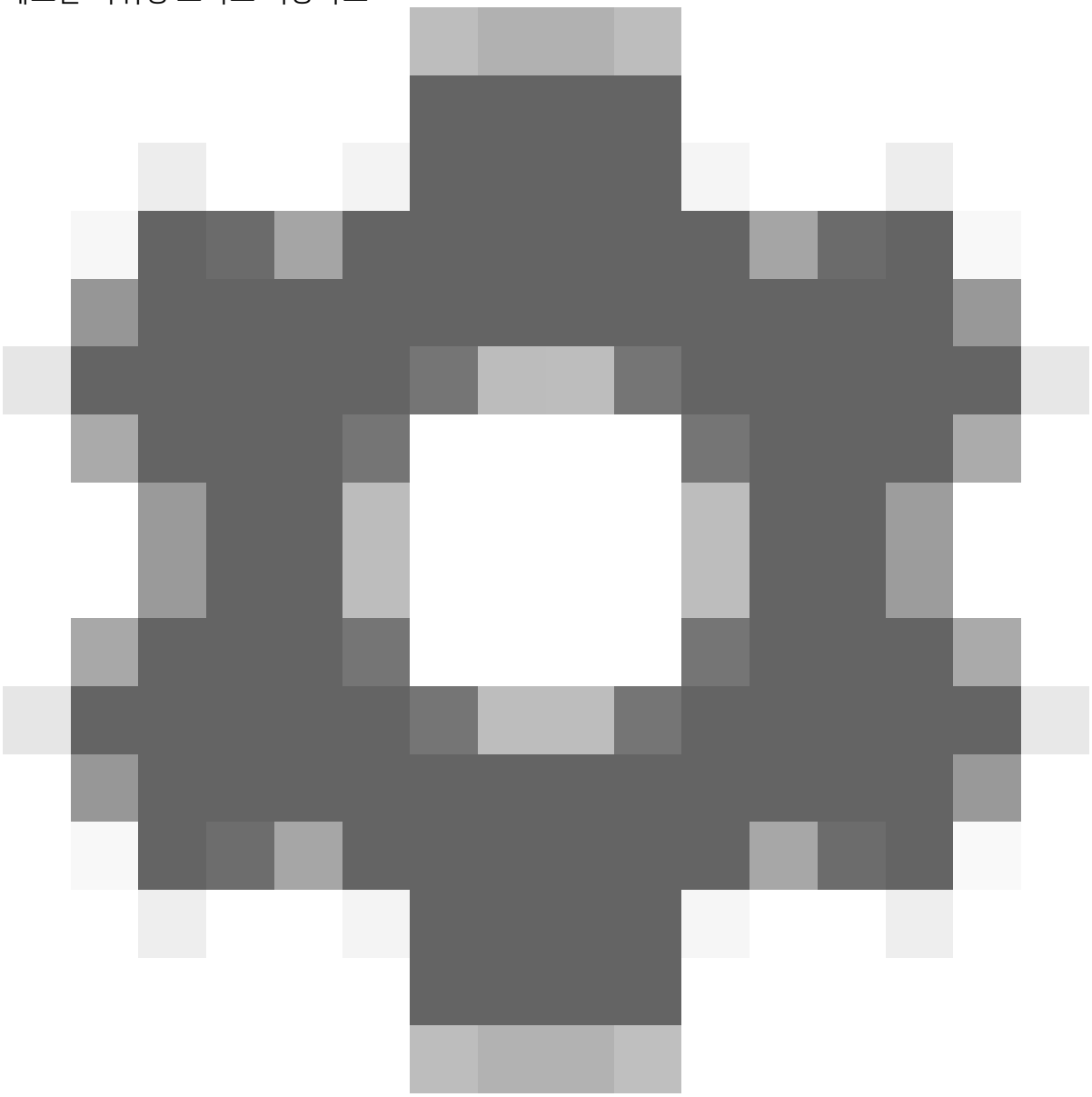


비고

디워핑을 위해 스트림을 최적화하려면 관리 클라이언트에서 **카메라 1**의 **비디오 스트림 1**에 대해 사용 가능한 최대 해상도를 선택하십시오. 자세한 내용은 *성능 및 문제 해결, on page 67*을 참조하십시오.

1. Smart Client를 열고 **Setup(설정)**을 클릭합니다.
2. **Views(보기)**로 이동합니다.
3. **Create new view(새로 보기 만들기)**를 클릭하고 형식을 선택합니다.
4. **System overview > AXIS Optimizer(시스템 오버뷰 > AXIS Optimizer)**로 이동합니다.
5. **Dewarping view(디워핑 보기)**를 클릭하고 보기에 드래그합니다.
6. 카메라와 카메라의 현재 마운트 위치를 선택합니다.
7. **설정**을 클릭합니다.

8. 새로운 디워핑 보기로 이동하고



을 클릭합니다.

9. **보기 유형 설정**을 클릭하고 하나의 옵션을 선택합니다. 카메라 장착 방식에 따라 **쿼드**, **일반**, **오버뷰가 포함된 일반** 또는 **파노라마**를 선택합니다.

비고

100% DPI를 사용하는 것이 좋습니다. 해상도가 100%가 아닌 경우 두 번째 디스플레이에서 Axis 디워핑이 완전히 표시되지 않을 수 있습니다.

다른 DPI 설정을 사용하는 경우 디워프 창이 부분적으로만 보일 수 있습니다. 이 문제를 해결하려면 다음 외부 문서의 지침을 따르세요.

- *고해상도 디스플레이(4K 이상)에서 XProtect 관련 문제*
- *하이 DPI 디스플레이에서 클라이언트 GUI 확장*

멀티 센서 파노라마 카메라를 위한 디워핑 보기 생성

다중 센서 파노라마 카메라(예: AXIS P3807-PVE Network Camera 및 AXIS Q3819-PVE Panoramic Camera)에 대해 디워핑 보기를 사용할 수 있습니다.

- 클라이언트 측 스티칭. 카메라가 캡처 모드 클라이언트 디워프로 설정된 경우 AXIS Optimizer는 4개의 이미지를 하나의 매끄러운 파노라마로 스티칭합니다(AXIS P3807-PVE만 해당).

- 수평 조정. 파노라마의 수평선을 조정할 수 있습니다. 카메라가 지면으로 기울어져 있고 좌표의 수평선이 구부러져 있는 경우에 이 기능이 필요할 수 있습니다. 또한 이것은 가상 PTZ 제어를 보다 직관적으로 만듭니다.
- PTZ 제어. PTZ 카메라처럼 이미지를 확대하고 이동할 수 있습니다.



비고

요구 사항

- 다음 사용자 권한 중 하나를 보유한 사용자:
  - 옵티마이저 역할
  - 하드웨어 > 드라이버 명령 = 허용
- Axis 다중 센서 파노라마 카메라

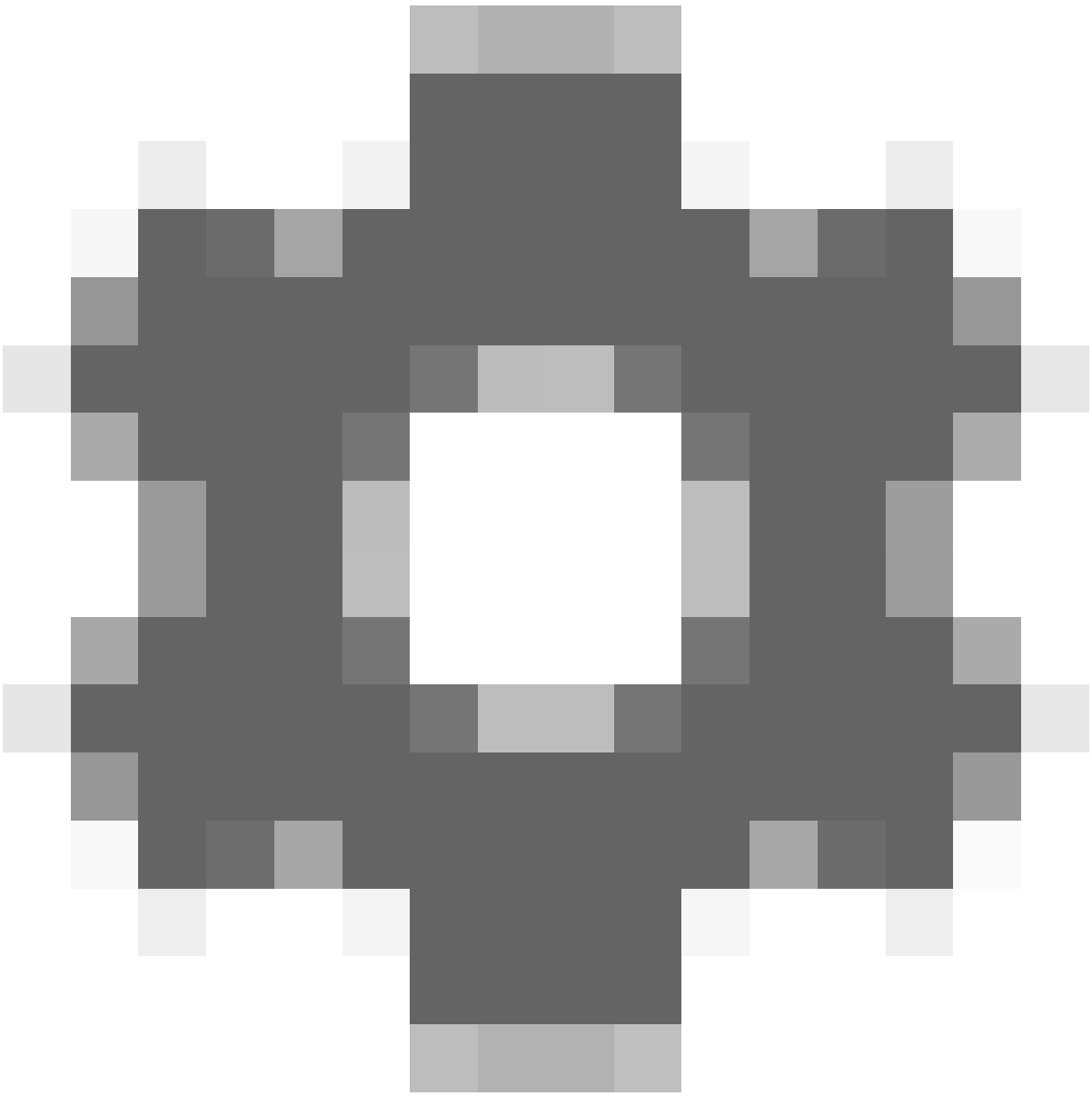
1. 해당하는 경우, 초기 장치 설정 중에 캡처 모드를 **Client Dewarp(클라이언트 디워프)**로 설정합니다.
2. Smart Client를 열고 **Setup(설정)**을 클릭합니다.
3. **Views(보기)**로 이동합니다.
4. **Create new view(새로 보기 만들기)**를 클릭하고 형식을 선택합니다.
5. **System overview > AXIS Optimizer(시스템 오버뷰 > AXIS Optimizer)**로 이동합니다.
6. **Dewarping view(디워핑 보기)**를 클릭하고 보기에 드래그합니다.
7. 다중 센서 파노라마 카메라를 선택하십시오.
   디워핑 보기에 처음으로 다중 센서 파노라마 카메라를 추가하면 보기 위에 수평선 보정 창이 표시됩니다.
8. 화살표를 클릭하여 빨간색 선을 좌표 수평선에 맞춥니다.
9. 설정을 저장하고 보정 모드를 종료하려면 **Done(완료)**을 클릭합니다.

와이드 뷰

와이드 뷰는 다중 센서 파노라마 카메라의 보기 유형입니다. 일반적인 120° 화각이 충분하지 않은 경우, **wide view(와이드 뷰)**를 켭니다. 와이드 뷰에서는 이미지가 항상 왜곡됩니다. 완전히 줌-아웃할 때 일반 보기로 전환하려면 **wide view(와이드 뷰)**를 끕니다.

홈 위치 설정

1. Smart Client에서 디워핑 보기를 엽니다.
2. 홈 포지션으로 저장하려는 위치로 이동합니다.



3. 을 클릭한 다음 **Set home position(홈 위치 설정)**을 선택합니다.

운영자가 디워핑 보기를 제어하고 편집할 수 있도록 허용

운영자가 디워핑 보기를 제어하고 편집해야 하는지 여부를 구성할 수 있으며 *운영자의 기능 액세스를 위한 사용자 정의, on page 98*을(를) 참조하십시오.

성능 및 문제 해결

성능 고려 사항

- Axis 비디오 디워핑은 가능한 경우 GPU에서 수행되지만 비디오 디워핑은 CPU에도 부하를 줍니다.
- 디워핑 보기가 많은 큰 보기에서 프레임 레이트가 떨어지는 것을 방지하려면 다음을 고려하십시오.
  - 카메라 해상도. 2880x2880 같은 고해상도 카메라는 1920x1920 같은 해상도에 비해 더 많은 컴퓨터 성능을 필요로 합니다.
  - 카메라 프레임 레이트. 높은 프레임 레이트가 필요하지 않은 경우 낮은 프레임 레이트를 변경하면 디워핑 보기 및 기타 보기에서 끊김 현상이 방지될 수 있습니다.

- 모니터 해상도. 예를 들어 4K와 같은 고해상도 모니터는 비디오를 표시하는 데 많은 리소스가 필요합니다. 더 높은 해상도가 필요하지 않은 경우 모니터 해상도를 낮추면 끊김 없이 왜곡된 보기를 더 많이 실행할 수 있습니다.

동적 해상도

- 비디오 스트림은 가능한 경우 비디오 품질을 저하시키지 않고 자동으로 축소됩니다. 이것은 디워핑 뷰의 성능을 향상시킬 수 있습니다.
- 오버뷰에서 확대할 때 깜박임이 발생하면 동적 해상도를 끄는 데 도움이 될 수 있습니다.
- 동적 해상도를 켜거나 끄려면: Smart Client에서 **Settings(설정) > Axis dewarping options (Axis 디워핑 옵션) > Rendering options(렌더링 옵션)**로 이동하여 **Dynamic resolution(동적 해상도)**을 선택하거나 선택 취소합니다.
- **Dynamic resolution(동적 해상도)**가 기본적으로 활성화되어 있습니다.

호환성 렌더링

- 예를 들어 검정 이미지와 같이 디워핑 이미지에 시각적 오류가 있거나 성능이 예상보다 좋지 않은 경우 호환성 렌더링을 활성화합니다. 호환성 렌더링의 부정적인 영향은 재생 시 보기와 스크러빙 간의 전환이 깜박일 수 있다는 점입니다.
- 호환성 렌더링을 켜거나 끄려면: Smart Client를 열고 **Settings(설정) > Axis dewarping options(Axis 디워핑 옵션) > Rendering options(렌더링 옵션)**로 이동하여 **Use compatibility rendering(호환성 렌더링 사용)**선택하거나 선택 취소합니다.
- **Use compatibility rendering(호환성 렌더링 사용)**이 기본적으로 비활성화되어 있습니다.

기대하는 점

Intel i7 8700 NVIDIA Gefore 1050 GTX와 3개의 1920x1080 모니터가 있는 참조 시스템에서 다음을 기대할 수 있습니다.

- 1920x1920 해상도 및 25fps에서 7개의 디워핑 보기를 프레임 드롭 없이 실행할 수 있거나
- 2880x2880 해상도 및 25fps에서 4개의 디워핑 보기를 실행할 수 있습니다

3개의 디스플레이 중 하나가 1920x1080 대신 4K 해상도로 실행되는 경우 다음을 기대할 수 있습니다.

- 1920x1920 해상도 및 25fps에서 5개의 디워핑 보기를 프레임 드롭 없이 실행하거나
- 3개의 디워핑 보기를 2880x2880 해상도 및 25fps에서 실행할 수 있습니다. 각 모니터에 하나의 디워핑 보기.

프레임 레이트와 해상도 스케일은 선형입니다. 30fps로 5개의 디워프된 보기를 실행할 수 있는 컴퓨터는 프레임 레이트를 15fps로 줄이면 10개의 보기를 실행할 수 있습니다.

신체 착용 통합

AXIS Optimizer Body Worn Extension을 사용하면 현장 카메라 사용자가 VMS를 사용하여 비디오 증거를 검색하고 관리할 수 있는 사무실 기반 조사자와 비디오를 녹화, 태그 지정 및 공유할 수 있습니다. 이 서비스는 Axis 신체 착용 시스템과 VMS 간의 안전한 연결 및 전송을 가능하게 합니다. AXIS Body Worn Extension은 녹화 서버에 설치해야 하는 독립 실행형 무료 서비스입니다.

비고

지원되는 버전은 다음과 같습니다.

- VMS 버전 2020 R1 Corporate 또는 최신 버전
- VMS 버전 2020 R1 Professional+ 또는 최신 버전
- VMS 버전 2020 R1 Expert 또는 최신 버전

항상 최신 VMS 핫픽스 및 누적 패치 설치 프로그램을 사용하십시오.

상세 정보

- 서비스 자체를 다운로드하거나 통합 가이드 및 솔루션 노트를 읽으려면, *axis.com*으로 이동하십시오.
- 사용자 설명서를 읽으려면, *axis.help.com*으로 이동하십시오.

접근 제어

접근 제어는 물리적 접근 제어와 영상 감시를 결합한 솔루션입니다. 이 통합을 통해 Management Client에서 직접 Axis 접근 제어 시스템을 구성할 수 있습니다. 이 시스템은 XProtect와 매끄럽게 통합되어 운영자가 Smart Client에서 접근을 모니터링하고 접근 제어 작업을 수행할 수 있게 합니다.

비고

요구 사항

- VMS 버전 2024 R1 이상.
- XProtect Access 라이센스에 대한 자세한 내용은 *액세스 라이센스*를 참조하십시오.
- 이벤트 서버와 Management Client에 AXIS Optimizer를 설치합니다.

AXIS Secure Entry를 통해 AXIS Optimizer를 설치하면 인바운드 트래픽(TCP)용 53459 및 53461 포트가 열립니다.

AXIS Secure Entry에서 도어를 사용하려면 도어당 라이센스가 필요합니다. *도어 라이센스 활성화, on page 71*를 참조하십시오.

접근 제어 구성

비고

시작하기 전에 다음을 수행합니다.

- 도어 컨트롤러 소프트웨어를 업그레이드합니다. 사용 중인 VMS 버전에 대한 최소 및 권장 AXIS OS 버전은 아래 표를 참조하십시오.
- 날짜와 시간이 올바른지 확인하십시오.

AXIS Optimizer 버전	최소 AXIS OS 버전	권장 AXIS OS 버전
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

시스템에 Axis 네트워크 도어 컨트롤러 추가

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)**로 이동합니다.
2. **Configuration(구성)**에서 **Devices(장치)**를 선택합니다.
3. **Discovered devices(검색된 장치)**를 선택하여 시스템에 추가할 수 있는 장치 목록을 확인합니다.
4. 추가할 장치를 선택합니다.
5. 팝업 창에서 **+ Add(+ 추가)**를 클릭하고 컨트롤러 자격 증명을 입력합니다.

비고

- 추가된 컨트롤러가 **Management(관리)** 탭에 표시됩니다.
- 컨트롤러를 수동으로 시스템에 추가하려면 **Management(관리)** 탭에서 **+ Add(+ 추가)**를 클릭합니다.
- 도어 컨트롤러 이름을 추가, 제거 또는 편집할 때마다 변경 사항을 VMS에 통합하는 방법:
  - **Site Navigation(사이트 탐색)** > **Access control(접근 제어)**로 이동하여 Access Control integration(접근 제어 통합)을 클릭합니다.
  - **General settings(일반 설정)** 탭에서 **Refresh Configuration(구성 새로 고침)**을 클릭합니다.

도어 라이센스 활성화

도어를 추가하려면 먼저 시스템에 있는 라이센스를 활성화해야 합니다.

1. **Site Navigation(사이트 탐색)**에서 **License Information(라이센스 정보)**로 이동합니다.
2. **Activate License Manually(수동으로 라이센스 활성화)**를 클릭하고 **Online(온라인)** 또는 **Offline(오프라인)**을 선택합니다.
3. 도어 라이센스를 온라인으로 활성화하는 방법:
   – 사용자 이름 및 패스워드를 입력합니다.
4. 도어 라이센스를 오프라인으로 활성화하려면 *오프라인으로 라이센스 활성화*를 참조하십시오.

활성화할 도어 라이센스 수를 조정해야 하는 경우:

1. **AXIS Optimizer** > **Access control(접근 제어)**로 이동합니다.
2. **Configuration(구성)**에서 **Devices(장치)**를 선택합니다.
3. **Allocated door licenses(할당된 도어 라이센스)** > **Custom license allocation(사용자 지정 라이센스 할당)**로 이동하여 사용할 도어 라이센스 수를 입력합니다.
4. **Apply(적용)**을 클릭합니다.
5. **License Information(라이센스 정보)**로 이동하여 라이센스를 다시 활성화합니다.

접근 제어를 구성합니다

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)**로 이동합니다.
2. 사전 정의된 식별 프로파일을 편집하거나 새 식별 프로파일을 만들려면 *식별 프로파일, on page 86*를 참조하십시오.
3. 카드 형식 및 PIN 길이의 사용자 지정 설정을 사용하려면 *카드 형식 및 PIN, on page 83*를 참조하십시오.
4. 도어에 특정 도어를 추가하고 식별 프로파일을 적용합니다. *도어를 추가합니다, on page 73*를 참조하십시오.
5. 영역을 추가하고 해당 영역에 도어를 추가합니다. *영역 추가, on page 80*를 참조하십시오.

도어 컨트롤러용 장치 소프트웨어 호환성

중요 사항

도어 컨트롤러에서 AXIS OS를 업그레이드할 때는 다음 사항에 유의하십시오.

- **지원되는 AXIS OS 버전:** 위에 나열된 지원 AXIS OS 버전은 원래 권장 VMS 버전에서 업그레이드하고 시스템에 도어가 있는 경우에만 적용됩니다. 시스템이 이 조건을 충족하지 않으면, 해당 VMS 버전에 권장되는 AXIS OS 버전으로 업그레이드해야 합니다.
- **최소 지원 AXIS OS 버전:** 시스템에 설치된 가장 오래된 AXIS OS 버전이 최소 지원 AXIS OS 버전을 결정하며, 이전 두 개 버전까지로 제한됩니다. AXIS Optimizer 버전 6.0을 사용 중이며 모든 장치를 권장 AXIS OS 버전 12.10.73.4로 업그레이드한다고 가정해 보겠습니다. 그러면 이후 시스템에서 AXIS OS 버전 12.6.94.1이 최소 지원 버전이 됩니다.
- **권장 AXIS OS 버전보다 높은 버전으로 업그레이드:** 특정 VMS 버전에 대해 권장되는 AXIS OS 버전보다 높은 버전으로 업그레이드한다고 가정해보겠습니다. VMS 버전에 설정된 지원 범위 내라면, 언제든지 문제 없이 권장 AXIS OS 버전으로 다시 다운그레이드할 수 있습니다.
- **향후 AXIS OS 권장 사항:** 시스템 안정성과 완전한 호환성을 보장하려면 항상 해당 VMS 버전에 권장되는 AXIS OS 버전을 따르십시오.

접근 제어 통합

VMS에 접근 제어를 통합하는 방법:

1. **Site Navigation(사이트 탐색)** > **Access Control(접근 제어)**로 이동합니다.
2. **Access Control(접근 제어)**를 마우스 오른쪽 버튼으로 클릭하고 **Create new...(새로 만들기...)**를 클릭합니다.
3. **Create Access Control System Integration(접근 제어 시스템 통합 만들기)** 대화 상자에서:
   - 통합의 이름을 입력합니다.
   - **Integration plug-in(통합 플러그인)**에서 드롭다운 메뉴에서 **AXIS Secure Entry**를 선택합니다.
   - **Associate cameras(카메라 연결)** 대화 상자가 표시될 때까지 **Next(다음)**를 클릭합니다.
     도어 액세스 포인트에 카메라를 연결하는 방법:
     - **Cameras(카메라)**에서 장치를 클릭하여 XProtect 시스템에 구성된 카메라 목록을 확인합니다.
     - 카메라를 선택하여 연결하려는 출입 지점으로 드래그합니다.
     - **Close(닫기)**를 클릭하여 대화 상자를 닫습니다.

비고

- XProtect의 접근 제어 통합에 대한 자세한 내용은 *XProtect Smart Client에서 접근 제어 사용하기*를 참조하십시오.
- 일반 설정, 도어 및 연결 카메라, 접근 제어 이벤트 등 접근 제어 속성에 대한 자세한 내용은 *접근 제어 속성*을 참조하십시오.

도어 및 영역

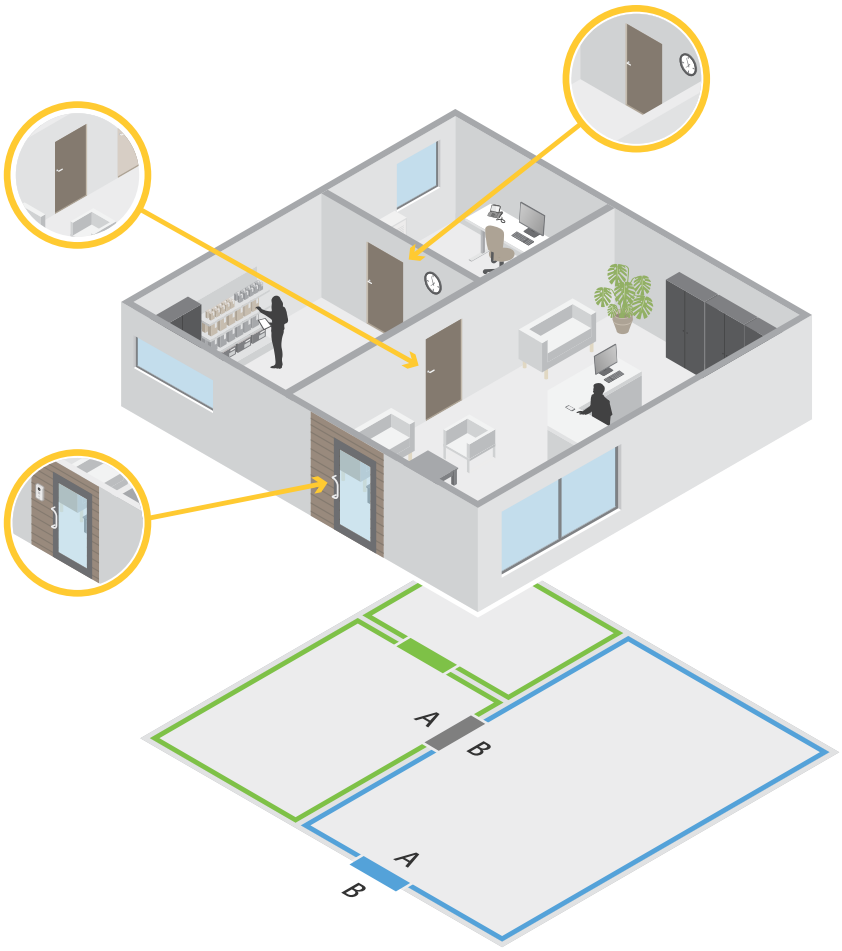
오버뷰를 확인하고 도어 및 구역을 구성하려면 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.

PIN 차트	도어와 관련된 컨트롤러 핀 차트를 봅니다. 핀 차트를 인쇄하려면 **Print(인쇄)**를 클릭합니다.
식별 프로파일	도어의 식별 프로파일을 변경합니다.
보안 채널	특정 리더에 대한 OSDP 보안 채널을 켜거나 끕니다.

도어	
이름	도어의 이름입니다.
도어 컨트롤러	도어에 연결된 도어 컨트롤러입니다.
A 사이드	도어의 측면 A가 속해 있는 영역입니다.
측면 B	도어의 측면 B가 속해 있는 영역입니다.
식별 프로파일	도어에 적용된 식별 프로파일입니다.
카드 형식 및 PIN	카드 형식 유형이나 핀 길이를 표시합니다.
상태	도어의 상태입니다. • **온라인:** 도어가 온라인 상태이며 올바르게 작동합니다. • **리더 오프라인:** 도어 구성의 리더가 오프라인 상태입니다. • **리더 오류:** 도어 구성의 리더가 보안 채널을 지원하지 않거나 리더에 대한 보안 채널이 꺼져 있습니다.
영역	

이름	영역의 이름입니다.
도어 수	영역에 포함된 도어의 수입니다.

도어 및 영역의 예



- 영역은 녹색 구역 및 파란색 구역 두 가지로 나뉩니다.
- 도어는 녹색 도어, 파란색 도어 및 갈색 도어입니다.
- 녹색 도어는 녹색 영역의 내부 도어입니다.
- 파란색 도어는 파란색 영역 전용 경계구역 도어입니다.
- 갈색 도어는 녹색 영역 및 파란색 영역 양쪽의 경계구역 도어입니다.

도어를 추가합니다

비고

- 도어 하나에 잠금 두 개가 있는 도어 또는 도어 두 개에 각각 잠금이 하나씩 있는 도어 컨트롤러로 구성할 수 있습니다.
- 도어 컨트롤러에 도어가 없고 최신 AXIS Optimizer와 구형 도어 컨트롤러 소프트웨어를 함께 사용하는 경우 시스템은 도어 추가를 허용하지 않습니다. 다만, 기존 도어가 이미 있는 경우 구형 소프트웨어를 사용하는 시스템 컨트롤러에서 새 도어를 허용합니다.

새 도어 구성을 생성하여 도어를 추가합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. **Add door(도어 추가)**를 클릭합니다.
3. 도어 이름을 입력합니다.
4. **Controller(컨트롤러)** 드롭다운 메뉴에서 도어 컨트롤러를 선택합니다. 다른 도어를 추가할 수 없거나, 오프라인 상태이거나, HTTPS가 활성화되지 않은 경우 컨트롤러가 회색으로 표시됩니다.
5. **Door type(도어 유형)** 드롭다운 메뉴에서 생성하려는 도어 유형을 선택합니다.
6. **Next(다음)**를 클릭하여 도어 구성 페이지로 이동합니다.
7. **Primary lock(기본 잠금)** 드롭다운 메뉴에서 릴레이 포트를 선택합니다.
8. 도어에 잠금 두 개를 구성하려면 **Secondary lock(보조 잠금)** 드롭다운 메뉴에서 릴레이 포트 하나를 선택합니다.
9. 식별 프로파일을 선택합니다. *식별 프로파일, on page 86*를 참조하십시오.
10. 도어 설정을 구성합니다. *도어 설정, on page 75*을 참조하십시오.
11. 모니터링 도어를 설정합니다. *모니터링 도어 추가, on page 78*를 참조하십시오.
12. **Save(저장)**를 클릭합니다.

기존 도어 구성을 복사하여 도어를 추가합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. **Add door(도어 추가)**를 클릭합니다.
3. 도어 이름을 입력합니다.
4. **Controller(컨트롤러)** 드롭다운 메뉴에서 도어 컨트롤러를 선택합니다.
5. **Next(다음)**를 클릭합니다.
6. **Copy configuration(구성 복사)** 드롭다운 메뉴에서 기존 도어 구성을 선택합니다. 연결된 도어가 표시되며, 도어가 두 개로 구성된 경우 컨트롤러가 회색으로 표시되고, 잠금 두 개가 있는 도어가 하나 있으면 컨트롤러가 회색으로 표시됩니다.
7. 원하는 경우 설정을 변경합니다.
8. **Save(저장)**를 클릭합니다.

도어를 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer**> **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Doors(도어)**로 이동합니다.
2. 목록에서 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. 설정을 변경하고 **Save(저장)**를 클릭합니다.

도어를 제거하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer**> **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Doors(도어)**로 이동합니다.
2. 목록에서 도어를 선택합니다.
3. **Remove(제거)**를 클릭합니다.
4. **Yes(예)**를 클릭합니다.

도어 이름을 추가, 제거 또는 편집할 때마다 변경 사항을 VMS에 통합하는 방법:

1. **Site Navigation(사이트 탐색)** > **Access control(접근 제어)**로 이동하여 Access Control integration(접근 제어 통합)을 클릭합니다.
2. **General settings(일반 설정)** 탭에서 **Refresh Configuration(구성 새로 고침)**을 클릭합니다.

도어 설정

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 편집할 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.

접근 시간(초)	접근 권한이 부여된 후 도어가 잠금 해제된 상태로 유지되는 시간(초)을 설정합니다. 도어가 열릴 때까지 또는 설정된 시간이 끝날 때까지 도어의 잠금 해제 상태를 유지합니다. 접근 시간이 남아 있어도 도어가 닫히면 잠깁니다.
Open-too-long time (sec)(장시간 개방(초))	도어 모니터를 구성한 경우에만 유효합니다. 도어가 열려 있는 시간(초)을 설정합니다. 설정된 시간이 끝날 때 도어가 열려 있으면 도어가 장시간 개방되어 있다는 알람이 트리거됩니다. 액션 룰을 설정하여 장시간 개방 이벤트가 트리거하는 작업을 구성합니다.
긴 접근 시간(초)	접근 권한이 부여된 후 도어가 잠금 해제된 상태로 유지되는 시간(초)을 설정합니다. 긴 접근 시간은 이 설정이 켜진 상태인 카드 소지자의 접근 시간을 재정의합니다.
Long open-too-long time (sec)(긴 장시간 개방(초))	도어 모니터를 구성한 경우에만 유효합니다. 도어가 열려 있는 시간(초)을 설정합니다. 설정된 시간이 끝날 때 도어가 열려 있으면 도어가 장시간 개방되어 있다는 이벤트가 트리거됩니다. **Long access time(긴 접근 시간)** 설정을 켜면 너무 오래 열려 있는 경우 카드 소지자에 대해 이미 설정된 긴 장시간 개방을 재정의합니다.
다시 잠금 지연 시간(ms)	도어가 열리거나 닫힌 후 도어가 잠기지 않은 상태로 유지되는 시간(밀리초)을 설정합니다.
다시 잠그다	• **After opening(열린 후):** 도어 모니터를 추가한 경우에만 유효합니다. • **After closing(닫힌 후):** 도어 모니터를 추가한 경우에만 유효합니다.

도어 보안 수준

도어에 다음 보안 기능을 추가할 수 있습니다.

2인 룰 - 2인 룰은 두 사람이 유효한 자격 증명을 사용하여 접근해야 합니다.

카드 두 번 대기 - 두 번 댄 카드 소지자는 도어의 현 상태를 무시할 수 있습니다. 예를 들어, 정규 시간 외에 도어를 잠금 또는 잠금 해제하는 데 사용할 수 있어 시스템으로 들어가서 도어를 잠금 해제하는 것보다 더 편리합니다. 카드 두 번 대기는 기존 일정에 영향을 주지 않습니다. 예를 들어, 도어가 닫히는 시간에 잠기도록 예약되어 있고 직원이 점심 시간에 퇴근하는 경우에도 도어는 일정에 따라 잠깁니다.

새 도어를 추가하는 동안 보안 수준을 구성하거나 기존 도어에서 보안 수준을 구성해도 됩니다.

기존 문에 **2인 룰**을 추가하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 보안 수준을 구성하려는 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. **Two-person rule(2인 룰)**을 켭니다.
6. **Apply(적용)**을 클릭합니다.

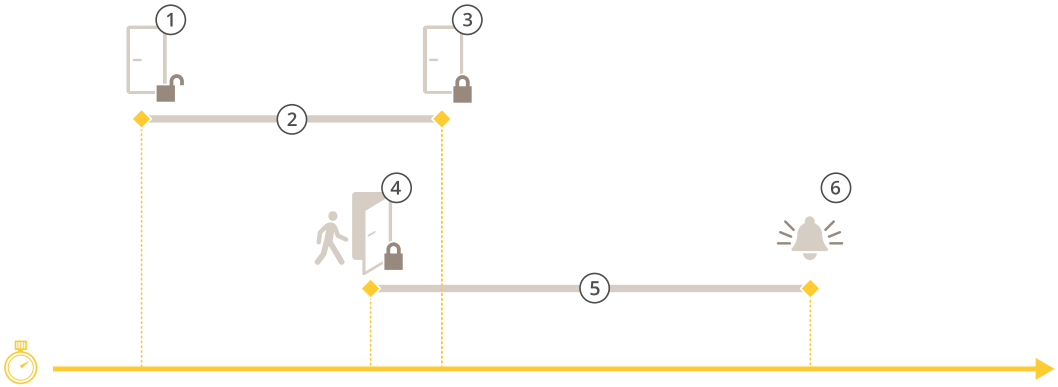
2인 룰	
Side A(측면 A) 및 **Side B(측면 B)**	룰을 사용할 도어의 측면을 선택합니다.
일정	룰이 활성화되는 시기를 선택합니다.
시간 초과(초)	시간 초과는 카드 긁기 또는 다른 유형의 유효한 자격 증명 사이에 허용되는 최대 시간입니다.

기존 도어에 **카드 두 번 대기**를 추가하려면 다음을 수행합니다.

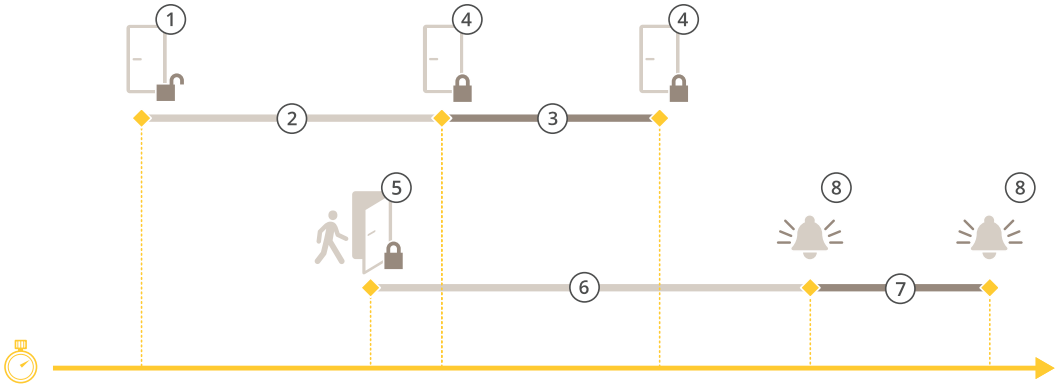
1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 보안 수준을 구성하려는 도어를 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. **Double-swipe(카드 두 번 대기)**를 켭니다.
6. **Apply(적용)**을 클릭합니다.
7. 카드 소지자에게 **Double-swipe(카드 두 번 대기)**를 적용합니다.
   7.1. **Cardholder management(카드 소지자 관리)**로 이동합니다.
   7.2. 편집할 카드 소지자를 선택하고 **Edit(편집)**를 클릭합니다.
   7.3. **고급**을 클릭합니다.
   7.4. **Allow double-swipe(카드 두 번 대기 허용)**를 선택합니다.
   7.5. **Save(저장)**를 클릭합니다.

카드 두 번 대기	
시간 초과(초)	시간 초과는 카드 긁기 또는 다른 유형의 유효한 자격 증명 사이에 허용되는 최대 시간입니다.

시간 옵션



1 접근 권한 부여됨 - 잠금장치 잠금 해제
2 접근 시간
3 취한 액션 없음 - 잠금장치 잠금
4 취한 액션(도어 열림) - 도어가 닫힐 때까지 잠금장치 잠금 또는 잠금 해제 유지
5 장시간 개방
6 장시간 개방 알람 해제



1 접근 권한 부여됨 - 잠금장치 잠금 해제
2 접근 시간
3 2+3: 긴 접근 시간
4 취한 액션 없음 - 잠금장치 잠금
5 취한 액션(도어 열림) - 도어가 닫힐 때까지 잠금장치 잠금 또는 잠금 해제 유지
6 장시간 개방
7 6+7: 긴 장시간 개방
8 장시간 개방 알람 해제

도어 모니터 추가

도어 모니터는 도어의 물리적 상태를 모니터링하는 도어 위치 스위치입니다. 사용자는 도어에 도어 모니터를 추가하고 도어 모니터 연결 방식을 구성할 수 있습니다.

1. 도어 구성 페이지로 이동합니다. *도어를 추가합니다, on page 73*를 참조하십시오
2. **Sensors(센서)**에서 **Add(추가)**를 클릭합니다.
3. **Door position sensor(도어 위치 센서)**를 선택합니다.
4. 도어 모니터를 연결할 I/O 포트를 선택합니다.

5. **Door open if(도어가 열리면)**에서 도어 모니터 회로의 연결 방법을 선택합니다.
6. 새로운 안정 상태에 도달하기 전에 디지털 입력의 상태 변경을 무시하려면 **Debounce time (디바운스 시간)**을 설정하십시오.
7. 도어 컨트롤러 및 도어 모니터 간에 연결이 중단되었을 때 이벤트를 트리거하려면 **Supervised input(관리된 입력)**을 켭니다. *관리된 입력, on page 82*을 참조하십시오.

도어가 열리면	
회로가 개방되었습니다	도어 모니터 회로는 정상 폐쇄 상태입니다. 회로가 열리면 도어 모니터가 도어 개방 신호를 보냅니다. 회로가 닫히면 도어 모니터가 도어 폐쇄 신호를 보냅니다.
회로가 폐쇄되었습니다	도어 모니터 회로는 정상 개방 상태입니다. 회로가 닫히면 도어 모니터가 도어 개방 신호를 보냅니다. 회로가 열리면 도어 모니터가 도어 폐쇄 신호를 보냅니다.

모니터링 도어 추가

모니터링 도어는 도어가 열려 있는지 또는 닫혀 있는지 확인할 수 있는 도어 유형입니다. 예를 들어 잠금 장치가 필요하지 않지만 도어가 열려 있는지 확인해야 하는 방화문에 이 기능을 사용할 수 있습니다.

모니터링 도어는 도어 모니터가 있는 일반 도어와 다릅니다. 도어 모니터가 있는 일반 도어는 잠금 장치와 리더를 지원하지만 도어 컨트롤러가 필요합니다. 모니터링 도어는 하나의 도어 위치 센서를 지원하지만 도어 컨트롤러에 연결된 네트워크 I/O 릴레이 모듈만 있으면 됩니다. 하나의 네트워크 I/O 릴레이 모듈에 최대 5개의 도어 위치 센서를 연결할 수 있습니다.

비고

모니터링 도어에는 AXIS Monitoring Door ACAP 애플리케이션을 포함한 최신 소프트웨어가 설치된 AXIS A9210 Network I/O Relay Module이 필요합니다.

모니터링 도어를 설정하려면 다음을 수행합니다.

1. AXIS A9210을 설치하고 최신 버전의 AXIS OS로 업그레이드합니다.
2. 도어 위치 센서를 설치합니다.
3. VMS에서 **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
4. **Add door(도어 추가)**를 클릭합니다.
5. 이름을 입력합니다.
6. **Type(유형)**에서 **Monitoring door(모니터링 도어)**를 선택합니다.
7. **Device(장치)**에서 네트워크 I/O 릴레이 모듈을 선택합니다.
8. **Next(다음)**를 클릭합니다.
9. **Sensors(센서)**에서 **+ Add(+ 추가)**를 클릭하고 **Door position sensor(도어 위치 센서)**를 선택합니다.
10. 도어 위치 센서에 연결된 I/O를 선택합니다.
11. **추가**를 클릭합니다.

리더 추가

도어 컨트롤러를 유선 리더 2개를 사용하도록 구성할 수 있습니다. 사용자는 도어 한 측면이나 양면에 리더를 추가하려면 선택합니다.

리더에 **Card formats(카드 형식)** 또는 핀 길이의 사용자 지정 설정을 적용하는 경우 **Configuration > Access control > Doors and zones(구성 > 접근 제어 > 도어 및 영역)**의 카드 형식에서 확인할 수 있습니다. *도어 및 영역, on page 72*을 참조하십시오.

1. 도어 구성 페이지로 이동합니다. *도어를 추가합니다, on page 73*를 참조하십시오.
2. 도어의 한 측면에서 **Add(추가)**를 클릭합니다.
3. **Card reader(카드 리더)**를 선택합니다.
4. **Reader type(리더 유형)**을 선택합니다.
5. 이 리더에 사용자 지정 핀 길이 설정을 사용합니다.
   5.1. **고급**을 클릭합니다.
   5.2. **Custom PIN length(사용자 지정 핀 길이)**를 켭니다.
   5.3. **Min PIN length(최소 핀 길이)**, **Max PIN length(최대 핀 길이)** 및 **End of PIN character(핀 문자 끝)**를 설정합니다.
6. 이 리더에 사용자 지정 카드 형식을 사용합니다.
   6.1. **고급**을 클릭합니다.
   6.2. **Custom card formats(사용자 지정 카드 형식)**를 켭니다.
   6.3. 리더에 사용하려는 카드 형식을 선택합니다. 비트 길이가 동일한 카드 형식을 이미 사용 중인 경우 먼저 이를 비활성화해야 합니다. 카드 형식 설정이 구성된 시스템 설정과 다르면 클라이언트에서 경고 아이콘이 표시됩니다.
7. **추가**를 클릭합니다.
8. 도어 반대편에 리더를 추가하려면 이 절차를 다시 반복합니다.

리더 유형	
OSDP RS485 half duplex(OSDP RS485 반이중)	RS485 리더의 경우 **OSDP RS485 half duplex (OSDP RS485 반이중)** 및 리더 포트를 선택합니다.
Wiegand	Wiegand 프로토콜을 사용하는 리더의 경우 **Wiegand** 및 리더 포트를 선택합니다.

Wiegand	
LED 제어	**Single wire(단일 와이어)** 또는 **Dual wire (R/G) (이중 와이어(R/G))**를 선택합니다. 이중 LED 컨트롤을 가진 리더는 빨간색 LED와 녹색 LED에 서로 다른 와이어를 사용합니다.
탬퍼 경보	리더 변조 입력이 활성화된 경우를 선택합니다. • **Open circuit(개방 회로)**: 회로가 개방되면 리더가 도어에 변조 신호를 보냅니다. • **Closed circuit(폐쇄 회로)**: 회로가 폐쇄되면 리더가 도어에 변조 신호를 보냅니다.
Tamper debounce time(탬퍼 디바운스 시간)	새로운 안정 상태에 도달하기 전에 리더 탬퍼 입력의 상태 변경을 무시하려면 **Tamper debounce time(탬퍼 디바운스 시간)**을 설정합니다.
감시 입력	도어 컨트롤러 및 리더 간에 연결이 중단되었을 때 이벤트를 트리거하려면 켭니다. *관리된 입력, on page 82*을 참조하십시오.

REX 장치 추가

사용자는 도어 한쪽 면이나 양면에 퇴실 요청(REX) 장치 추가를 선택할 수 있습니다. REX 장치는 PIR 센서, REX 버튼 또는 푸시 바일 수 있습니다.

1. 도어 구성 페이지로 이동합니다. *도어를 추가합니다, on page 73*를 참조하십시오.
2. 도어의 한 측면에서 **Add(추가)**를 클릭합니다.
3. **REX device(REX 장치)**를 선택합니다.
4. REX 장치를 연결하려는 I/O 포트를 선택합니다. 사용 가능한 포트가 하나뿐인 경우 이 포트가 자동으로 선택됩니다.
5. 도어가 REX 신호를 수신할 때 트리거할 **Action(액션)**을 선택합니다.
6. **REX active(REX 활성)**에서 도어 모니터 회로 연결을 선택합니다.
7. 새로운 안정 상태에 도달하기 전에 디지털 입력의 상태 변경을 무시하려면 **Debounce time (디바운스 시간(ms))**을 설정합니다.
8. 도어 컨트롤러와 REX 장치 간의 연결이 중단될 때 이벤트를 트리거하려면 **Supervised input (관리된 입력)**을 켭니다. *관리된 입력, on page 82*을 참조하십시오.

액션	
도어 잠금 해제	REX 신호가 수신되어 도어의 잠금을 해제하려면 선택합니다.
없음	도어가 REX 신호를 수신할 때 어떤 액션도 트리거하지 않으려면 선택합니다.

REX 활성화	
회로가 개방되었습니다	REX 회로가 정상 폐쇄된 경우에 선택합니다. REX 장치는 회로가 개방되었을 때 신호를 보냅니다.
회로가 폐쇄되었습니다	REX 회로가 정상 개방된 경우에 선택합니다. REX 장치는 회로가 폐쇄되었을 때 신호를 보냅니다.

영역 추가

영역은 도어 그룹이 속해 있는 특정한 물리적 영역입니다. 사용자는 영역을 생성하고 영역에 도어를 추가할 수 있습니다. 두 가지 유형의 도어가 있습니다.

- **경계구역 도어:** 카드 소지자가 이 도어를 통해 구역에 출입합니다.
- **내부 도어:** 구역 내의 내부 도어입니다.

비고

경계구역 도어는 두 영역에 속할 수 있습니다. 내부 도어는 한 영역에만 속할 수 있습니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.
2. + **Add zone(영역 추가)**을 클릭합니다.
3. 영역 이름을 입력합니다.
4. **Add door(도어 추가)**를 클릭합니다.
5. 영역에 추가할 도어를 선택하고 **Add(추가)**를 클릭합니다.

6. 도어는 기본적으로 경계구역 도어로 설정되어 있습니다. 이를 변경하려면 드롭다운 메뉴에서 **Internal door(내부 도어)**를 선택합니다.
7. 경계구역 도어는 기본적으로 도어 측면 A를 영역 입구로 사용합니다. 이를 변경하려면 드롭다운 메뉴에서 **Leave(나가기)**를 선택합니다.
8. 영역에서 도어를 제거하려면 도어를 선택하고 **Remove(제거)**를 클릭합니다.
9. **Save(저장)**를 클릭합니다.

영역을 편집하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.
2. 목록에서 영역을 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. 설정을 변경하고 **Save(저장)**를 클릭합니다.

영역을 제거하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)** > **Zones(구역)**로 이동합니다.
2. 목록에서 영역을 선택합니다.
3. **Remove(제거)**를 클릭합니다.
4. **Yes(예)**를 클릭합니다.

영역 보안 수준

영역에 다음 보안 기능을 추가할 수 있습니다.

지정 통로 출입 방식 - 다른 사람들이 자신보다 먼저 구역에 입장한 사람과 동일한 자격 증명을 사용하는 것을 방지합니다. 자격 증명을 다시 사용하려면 먼저 해당 구역에서 나가야 합니다.

비고

- 지정 통로 출입 방식을 사용하면 해당 영역의 모든 도어에 도어 위치 센서가 있어야 사용자가 카드를 대고 도어를 열었다는 사실을 시스템에서 등록할 수 있습니다.
- 도어 컨트롤러가 오프라인 상태가 되면 해당 영역의 모든 도어가 동일한 도어 컨트롤러에 속해 있는 한 지정 통로 출입 방식이 작동합니다. 하지만 해당 영역의 도어가 서로 다른 도어 컨트롤러에 속해 오프라인 상태가 되면 지정 통로 출입 방식이 작동하지 않습니다.

새 영역을 추가하는 동안 보안 수준을 구성하거나 기존 영역에서 구성할 수 있습니다. 기존 영역에 보안 수준을 추가하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 보안 수준을 구성하려는 영역을 선택합니다.
3. **Edit(편집)**를 클릭합니다.
4. **Security level(보안 수준)**을 클릭합니다.
5. 도어에 추가하려는 보안 기능을 켭니다.
6. **Apply(적용)**을 클릭합니다.

지정 통로 출입 방식	
Log violation only (Soft)(로그 위반만(소프트))	두 번째 사람이 첫 번째 사람과 동일한 자격 증명을 사용하여 도어에 들어갈 수 있도록 하려면 이 옵션을 사용합니다. 이 옵션은 시스템 알람만 발생시킵니다.

Deny access (Hard)(액세스 거부(하드))	두 번째 사용자가 첫 번째 사람과 동일한 자격 증명을 사용하는 경우 두 번째 사용자가 도어에 들어가는 것을 방지하려면 이 옵션을 사용합니다. 이 옵션도 시스템 알람을 발생시킵니다.
시간 초과(초)	시스템이 사용자의 재진입을 허용할 때까지의 시간입니다. 시간 초과를 원하지 않을 경우 0을 입력합니다. 이제, 사용자가 해당 영역을 떠날 때까지 해당 영역에 지정 통로 출입 방식이 적용됩니다. 해당 영역의 모든 도어 양쪽에 리더가 있는 경우 **Deny access (Hard)(액세스 거부(하드))**와 함께 **0** 타임아웃만 사용하십시오.

관리된 입력

관리된 입력은 도어 컨트롤러로의 연결이 중단될 때 이벤트를 트리거할 수 있습니다.

- 도어 컨트롤러와 도어 모니터 간의 연결. *도어 모니터 추가, on page 77*를 참조하십시오.
- 도어 컨트롤러와 Wiegand 프로토콜을 사용하는 리더 간의 연결. *리더 추가, on page 78*를 참조하십시오.
- 도어 컨트롤러와 REX 장치 간의 연결. *REX 장치 추가, on page 80*를 참조하십시오.

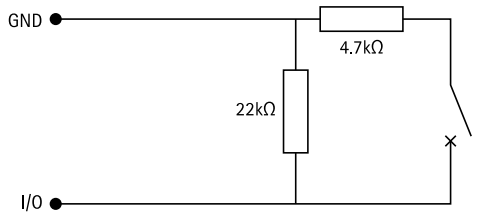
관리된 입력을 사용하려면

1. 연결 다이어그램에 따라 EOL 레지스터를 주변 장치에 최대한 가깝게 설치하십시오.
2. 리더, 도어 모니터 또는 REX 장치의 구성 페이지로 이동하여 **Supervised input(관리된 입력)**을 켭니다.
3. 병렬 우선 연결 다이어그램을 따른 경우 **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor(22KΩ 병렬 저항 및 4.7KΩ 직렬 저항으로 병렬 우선 연결)**를 선택합니다.
4. 직렬 우선 연결 다이어그램을 따른 경우 **Serial first connection(직렬 우선 연결)**을 선택하고 **Resistor values(저항 값)** 드롭다운 메뉴에서 저항 값을 선택합니다.

연결 다이어그램

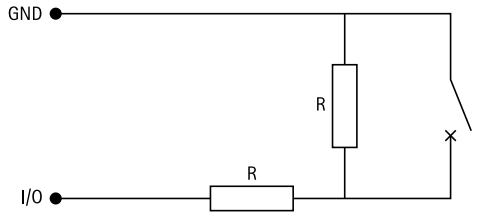
병렬 우선 연결

저항 값은 4.7kΩ 및 22kΩ이어야 합니다.



직렬 우선 연결

저항 값은 동일해야 하며 1-10 kΩ 범위 내에 있어야 합니다.



수동 액션

도어 및 영역에 대해 다음과 같은 수동 액션을 수행할 수 있습니다.

재설정 - 구성된 시스템 룰로 돌아갑니다.

액세스 권한 부여 - 7초 동안 도어 또는 영역의 잠금을 해제했다가 다시 잠급니다.

잠금 해제 - 재설정할 때까지 도어를 잠금 해제 상태로 유지합니다.

잠금 - 시스템에서 카드 소지자의 액세스를 허용할 때까지 도어를 잠금 상태로 유지합니다.

차단 - 재설정하거나 잠금을 해제할 때까지 아무도 출입할 수 없습니다.

수동 액션을 수행하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Doors and zones(도어 및 구역)**로 이동합니다.
2. 수동 액션을 수행할 도어 또는 영역을 선택합니다.
3. 수동 액션을 클릭합니다.

비고

도어는 일반 일정으로 다시 재설정할 때까지 수동 재정의 모드라고도 하는 수동 액션 상태로 유지됩니다.

카드 형식 및 PIN

카드 형식은 카드에 데이터가 저장되는 방식을 정의합니다. 이는 들어오는 데이터 및 시스템에서 유효성이 검사된 데이터 간의 변환 표입니다. 각 카드 형식에는 저장된 정보를 구성하는 방법에 대한 서로 다른 룰이 있습니다. 카드 형식을 정의함으로써 컨트롤러가 카드 리더로부터 받는 정보를 어떻게 해석할지를 시스템에 알려줄 수 있습니다.

일반적으로 사용되는 카드 형식이 미리 정의되어 있어 그대로 사용하거나 필요에 따라 편집할 수 있습니다. 사용자 지정 카드 형식을 만들 수도 있습니다.

Site Navigation(사이트 탐색) > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동하여 카드 형식을 생성, 편집 또는 활성화합니다. 또한, 핀을 구성할 수 있습니다.

사용자 지정 카드 형식에는 자격 증명 확인에 사용되는 다음 데이터 필드가 포함될 수 있습니다.

카드 번호 - 10진수 또는 16진수로 인코딩된 자격 증명 이진 데이터의 하위 집합입니다. 카드 번호로 특정 카드 또는 카드 소지자를 식별합니다.

시설 코드 - 10진수 또는 16진수로 인코딩된 자격 증명 이진 데이터의 하위 집합입니다. 시설 코드로 특정 최종 고객 또는 사이트를 식별합니다.

카드 형식을 만들려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. **Add card format(카드 형식 추가)**을 클릭합니다.
3. 카드 형식 이름을 입력합니다.
4. **Bit length(비트 길이)** 필드에서 1에서 256 사이의 비트 길이를 입력합니다.
5. 카드 리더로부터 수신한 데이터의 비트 순서를 역순으로 바꾸고자 하는 경우 **Invert bit order (비트 순서 반전)**를 선택합니다.
6. 카드 리더로부터 수신한 데이터의 바이트 순서를 역순으로 바꾸고자 하는 경우 **Invert byte order(바이트 순서 반전)**를 선택합니다. 이 옵션은 8로 나눌 수 있는 비트 길이를 지정하는 경우에만 사용할 수 있습니다.

7. 카드 형식에서 활성화할 데이터 필드를 선택하고 구성합니다. **Card number(카드 번호)** 또는 **Facility code(시설 코드)** 중 하나는 반드시 카드 형식으로 활성화되어야 합니다.
8. **확인**을 클릭합니다.
9. 카드 형식을 활성화하려면 카드 형식 이름 앞의 확인란을 선택합니다.

비고

- 비트 길이가 동일한 두 카드 형식을 동시에 활성화할 수 없습니다. 가령 32비트 카드 형식 두 개를 정의한 경우 이 중 하나만 활성화할 수 있습니다. 한 카드 형식을 비활성화하면 다른 형식을 활성화할 수 있습니다.
- 도어 컨트롤러에 하나 이상의 리더가 구성된 경우에만 카드 형식을 활성화 및 비활성화할 수 있습니다.

ⓘ	비트 순서를 반전한 후 출력의 예시를 보려면 ⓘ 을 클릭합니다.
범위	데이터 필드에 대한 데이터의 비트 범위를 설정합니다. 범위는 사용자가 **Bit length(비트 길이)**로 지정한 분량 이내여야 합니다.
출력 형식	데이터 필드에 대한 데이터의 출력 형식을 선택합니다. **Decimal(십진수)**: 기본 10진법이라고도 하며 숫자 0-9로 구성됩니다. **Hexadecimal(16진수)**: 16진 위치 기수법이라고도 하며 16개의 고유 기호인 숫자 0-9 및 문자 a-f로 구성됩니다.
하위 범위의 비트 순서	비트 순서를 선택합니다. **Little-endian**: 첫 번째 비트는 가장 작은(최하위) 비트입니다. **Big-endian**: 첫 번째 비트가 가장 큰(최상위) 비트입니다.

카드 형식을 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. 카드 형식을 선택하고 을 클릭합니다.
3. 사전 정의된 카드 형식을 편집하면 **Invert bit order(비트 순서 반전)** 및 **Invert byte order(바이트 순서 반전)**만 편집할 수 있습니다.
4. **확인**을 클릭합니다.

사용자는 사용자 지정 카드 형식만 제거할 수 있습니다. 사용자 지정 카드 형식을 제거하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. 사용자 지정 카드 형식을 선택하고, 및 **Yes(예)**를 클릭합니다.

사전 정의된 카드 형식을 재설정하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.

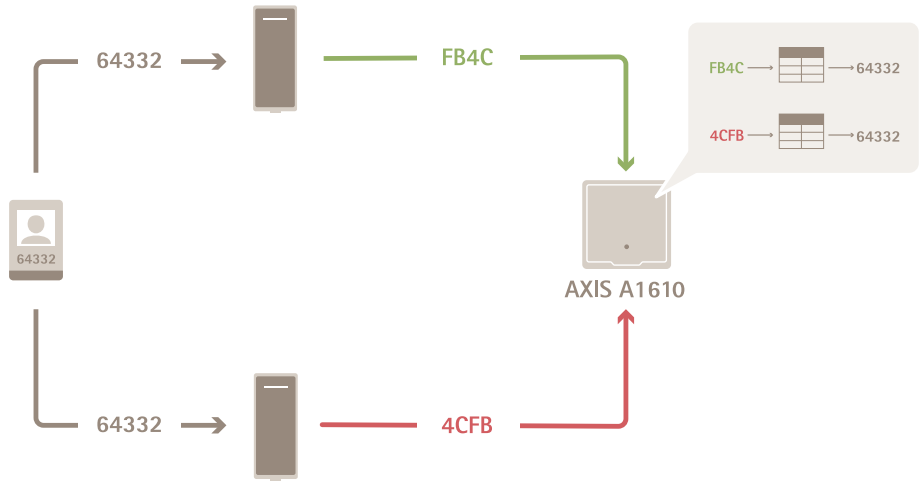
2. 카드 형식을 기본 필드 지도로 재설정하려면 을 클릭합니다.

핀 길이를 구성하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Card formats and PIN(카드 형식 및 PIN)**으로 이동합니다.
2. **PIN configuration(PIN 구성)**에서 을 클릭합니다.
3. **Min PIN length(최소 PIN 길이)**, **Max PIN length(최대 PIN 길이)** 및 **End of PIN character (PIN 문자 끝)**를 지정합니다.
4. **확인**을 클릭합니다.

카드 형식 설정

개요



- 십진수로 표시된 카드 번호는 `64332`입니다.
- 어느 한 리더에 의해 카드 번호가 16진수 `FB4C`로 변환됩니다. 다른 한 리더는 이를 16진수 `4CFB`로 변환합니다.
- AXIS A1610 Network Door Controller는 `FB4C`를 수신하고 해당 리더의 카드 형식 설정에 따라 이를 십진수 `64332`로 변환합니다.
- AXIS A1610 Network Door Controller는 `4CFB`를 수신하고, 바이트 순서를 반전시켜 `FB4C`로 변경한 후, 리더의 카드 포맷 설정에 따라 이를 십진수 `64332`로 변환합니다.

비트 순서 반전

비트 순서를 반전한 후 해당 리더로부터 수신된 카드 데이터는 비트 단위로 오른쪽에서 왼쪽으로 판독됩니다.



바이트 순서 반전

8비트를 하나로 묶어서 바이트라고 합니다. 바이트 순서를 반전한 후 해당 리더로부터 수신된 카드 데이터는 바이트 단위로 오른쪽에서 왼쪽으로 판독됩니다.



26비트 표준 Wiegand 카드 형식



1 *선행 패리티*
2 *시설 코드*
3 *카드 번호*
4 *후행 패리티*

식별 프로파일

식별 프로파일은 식별 유형 및 일정의 조합입니다. 도어 하나 이상에 식별 프로파일을 적용하여 카드 소지자가 도어에 접근할 수 있는 방법과 시기를 설정할 수 있습니다.

식별 유형은 도어에 접근하는 데 필요한 자격 증명 정보의 전달자입니다. 일반적인 식별 유형으로는 토큰, 개인 식별 번호(핀), 지문, 안면 인식, REX 장치 등이 있습니다. 식별 유형에는 정보 유형이 하나 이상 포함될 수 있습니다.

Time profiles(시간 프로파일)라고도 하는 스케줄은 Management Client에서 생성됩니다. 시간 프로파일 설정 방법은 *시간 프로파일(설명)*을 참조하십시오.

지원되는 식별 유형: 카드, PIN 및 REX.

Site Navigation(사이트 탐색) > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.

사용자가 그대로 사용하거나 필요에 따라 편집할 수 있는 기본 식별 프로파일이 다섯 개 있습니다.

카드 - 카드 소지자가 도어에 접근하려면 카드를 대야 합니다.

카드 및 PIN - 카드 소지자는 도어에 접근하기 위해 카드를 대고 핀을 입력해야 합니다.

PIN - 카드 소지자는 도어에 접근하기 위해 PIN을 입력해야 합니다.

카드 또는 PIN - 카드 소지자는 도어에 접근하기 위해 카드를 대거나 PIN을 입력해야 합니다.

번호판 - 카드 소지자는 승인된 번호판을 부착한 차량으로 카메라를 향해 운전해야 합니다.

식별 프로파일을 생성하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.
2. **Create identification profile(식별 프로파일 생성)**을 클릭합니다.
3. 식별 프로파일 이름을 입력합니다.
4. **Include facility code for card validation(카드 검증용 시설 코드 포함)**을 선택하여 시설 코드를 자격 증명 확인 필드 중 하나로 사용합니다. **Access management** > **Settings(접근 관리 > 설정)**에서 **Facility code(시설 코드)**를 켜는 경우에만 이 필드를 사용할 수 있습니다.
5. 도어의 한 측면에 대한 식별 프로파일을 구성합니다.
6. 도어 반대편에서 이전 단계를 다시 반복합니다.
7. **확인**을 클릭합니다.

식별 프로파일을 편집하려면

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.
2. 식별 프로파일을 선택하고 을 선택합니다.
3. 식별 프로파일 이름을 변경하려면 새 이름을 입력합니다.
4. 도어의 측면을 편집합니다.
5. 도어 반대편의 식별 프로파일을 편집하려면 이전 단계를 다시 반복합니다.
6. **확인**을 클릭합니다.

식별 프로파일을 제거하려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Identification profiles(식별 프로파일)**로 이동합니다.
2. 식별 프로파일을 선택하고 을 선택합니다.
3. 도어에 식별 프로파일이 적용된 경우 해당 도어의 다른 식별 프로파일을 선택합니다.
4. **확인**을 클릭합니다.

식별 프로파일 편집	
×	식별 유형 및 관련 일정을 제거합니다.
식별 유형	식별 유형을 변경하려면 **Identification type(식별 유형)** 드롭다운 메뉴에서 유형을 하나 이상 선택합니다.
Schedule	일정을 변경하려면 **Schedule(일정)** 드롭다운 메뉴에서 일정을 하나 이상 선택합니다.
+ **추가**	식별 유형 및 관련 일정을 추가하려면 **Add(추가)**를 클릭하고 식별 유형 및 일정을 설정합니다.

암호화된 통신

OSDP 보안 채널

Secure Entry는 OSDP(Open Supervised Device Protocol) Secure Channel을 지원하여 컨트롤러와 AXIS 리더 사이에 회선 암호화를 활성화합니다.

전체 시스템에 대해 OSDP 보안 채널을 켜려면 다음을 수행합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Encrypted communication(암호화 통신)**으로 이동합니다.
2. 기본 암호화 키를 입력하고 **OK(확인)**를 클릭합니다.
3. **OSDP Secure Channel(OSDP 보안 채널)**을 켭니다. 기본 암호화 키를 입력한 후에만 이 옵션을 사용할 수 있습니다.
4. 기본적으로 기본 암호화 키는 OSDP 보안 채널 키를 생성합니다. 다음과 같이 OSDP 보안 채널 키를 수동으로 설정합니다.
   4.1. **OSDP Secure Channel(OSDP 보안 채널)**에서, 을 클릭합니다.
   4.2. **Use main encryption key to generate OSDP Secure Channel key(기본 암호화 키를 사용하여 OSDP 보안 채널 키 생성)**를 지웁니다.
   4.3. OSDP 보안 채널 키를 입력하고 **OK(확인)**를 클릭합니다.

특정 리더에 대해 OSDP Secure Channel을 켜거나 끄려면 *도어 및 영역*을 참조하십시오.

다중 서버 BETA

연결된 하위 서버는 다중 서버를 통해 기본 서버의 전역 카드 소지자 및 카드 소지자 그룹을 사용할 수 있습니다.

비고

- 한 시스템은 하위 서버를 최대 64개까지 지원할 수 있습니다.
- 주 서버와 하위 서버가 동일한 네트워크에 있어야 합니다.
- 주 서버 및 하위 서버에서 보안 항목 포트에서 들어오는 TCP 연결을 허용하도록 Windows 방화벽을 구성해야 합니다. 기본 포트는 53461입니다.

작업 흐름

1. 서버를 하위 서버로 구성하고 구성 파일을 생성합니다. *하위 서버에서 구성 파일 생성, on page 88*을 참조하십시오.
2. 서버를 주 서버로 설정하고 하위 서버의 설정 파일을 가져옵니다. *구성 파일을 주 서버로 가져오기, on page 88*를 참조하십시오.
3. 주 서버에서 글로벌 카드 소지자 및 카드 소지자 그룹을 구성합니다. *카드 소지자 추가, on page 89* 및 *그룹 추가, on page 92*를 참조하십시오.
4. 하위 서버에서 글로벌 카드 소지자 및 카드 소지자 그룹을 보고 모니터링합니다. *접근 관리, on page 89*를 참조하십시오.

하위 서버에서 구성 파일 생성

1. 하위 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Sub server(하위 서버)**를 클릭합니다.
3. **Generate logs(생성)**를 클릭합니다. .json 형식의 구성 파일을 생성합니다.
4. **Download(다운로드)**를 클릭하고 파일을 저장할 위치를 선택합니다.

구성 파일을 주 서버로 가져오기

1. 주 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Main server(주 서버)**를 클릭합니다.
3. + **Add(추가)**를 클릭하고 하위 서버에서 생성된 구성 파일로 이동합니다.
4. 하위 서버의 서버 이름, IP 주소 및 포트 번호를 입력합니다.
5. **Import(가져오기)**를 클릭하여 하위 서버를 추가합니다.
6. 하위 서버의 상태가 `Connected`로 표시됩니다.

하위 서버 취소

기본 서버로 구성 파일을 가져오기 전에만 하위 서버를 취소할 수 있습니다.

1. 주 서버에서 **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
2. **Sub server(서브 서버)**를 클릭하고 **Revoke server(서버 취소)**를 클릭합니다.
이제 이 서버를 주 서버 또는 하위 서버로 구성할 수 있습니다.

하위 서버 제거

하위 서버의 구성 파일을 가져오면 기본 서버에 하위 서버를 연결합니다.

하위 서버 제거를 제거하려면 다음을 수행합니다.

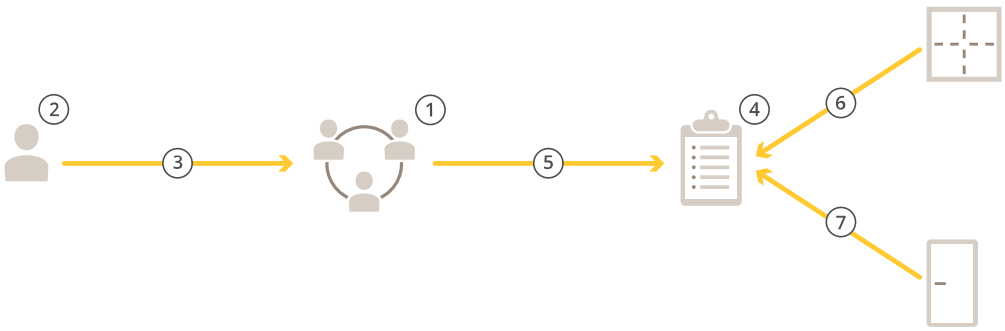
1. 주 서버에서:
   1.1. **Access management(접근 관리)** > **Dashboard(대시보드)**로 이동합니다.
   1.2. 전역 카드 소지자 및 그룹을 로컬 카드 소지자 및 그룹으로 변경합니다.
   1.3. **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
   1.4. **Main server(기본 서버)**를 클릭하여 하위 서버 목록을 표시합니다.
   1.5. 하위 서버를 선택하고 **Delete(삭제)**를 클릭합니다.
2. 기본 서버에서:
   – **AXIS Optimizer** > **Access control(접근 제어)** > **Multi server(다중 서버)**로 이동합니다.
   – **Sub server(하위 서버)**와 **Revoke server(서버 취소)**를 차례로 클릭합니다.

접근 관리

Access management(접근 관리) 탭에서는 시스템의 카드 소지자, 그룹 및 접근 룰을 구성 및 관리할 수 있습니다.

접근 관리의 작업 흐름

접근 관리 구조가 유연하여 필요에 맞는 작업 흐름을 개발할 수 있습니다. 다음은 작업 흐름의 예입니다.



1. 그룹을 추가합니다. *그룹 추가, on page 92*를 참조하십시오.
2. 카드 소지자를 추가합니다. *카드 소지자 추가, on page 89*를 참조하십시오.
3. 그룹에 카드 소지자를 추가합니다.
4. 접근 룰을 추가합니다. *접근 룰을 추가합니다, on page 93*를 참조하십시오.
5. 접근 룰에 그룹을 적용합니다.
6. 접근 룰에 영역을 적용합니다.
7. 접근 룰에 도어를 적용합니다.

카드 소지자 추가

카드 소지자는 시스템에 등록된 고유 ID를 지닌 사람입니다. 카드 소지자를 식별하는 자격 증명으로 카드 소지자를 구성하고 해당 사용자에게 도어에 대한 접근 권한을 부여하는 시기와 방법을 설정합니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.

2. **Cardholders(카드 소지자)**로 이동하여 **+ Add(+ 추가)**를 클릭합니다.
3. 카드 소지자의 이름과 성을 입력하고 **Next(다음)**를 클릭합니다.
4. 원하는 경우 **Advanced(고급)**를 클릭하고 옵션을 선택합니다.
5. 카드 소지자에게 자격 증명을 추가합니다. *자격 증명 추가, on page 90*를 참조하십시오
6. **Save(저장)**를 클릭합니다.
7. 카드 소지자를 그룹에 추가합니다.
   7.1. **Groups(그룹)**에서 카드 소지자를 추가할 그룹을 선택하고 **Edit(편집)**을 클릭합니다.
   7.2. **+ Add(추가)**를 클릭하고 그룹에 추가할 카드 소지자를 선택합니다. 여러 카드 소지자를 선택할 수 있습니다.
   7.3. **추가**를 클릭합니다.
   7.4. **Save(저장)**를 클릭합니다.

고급 수준	
긴 접근 시간	도어 모니터가 설치된 경우 카드 소지자의 접근 시간과 장시간 개방이 길어지게 하려면 선택합니다.
카드 보유자 정지	카드 소지자를 정지하려면 선택합니다.
카드 두 번 대기	카드 소지자가 도어의 현재 상태를 재정의할 수 있도록 허용하려면 선택합니다. 예를 들어, 정규 일정 외의 시간에 도어를 여는 데 사용할 수 있습니다.
차단 면제	차단 기간에 카드 소지자가 접근할 수 있게 하려면 선택합니다.
Exempt from anti-passback(지정 통로 출입 방식 제외)	카드 소지자에게 지정 통로 출입 방식 룰의 면제를 제공하려면 선택합니다. 지정 통로 출입 방식은 다른 사람들이 자신보다 먼저 구역에 입장한 사람과 동일한 자격 증명을 사용하는 것을 방지합니다. 자격 증명을 다시 사용하려면 첫 번째 사용자가 먼저 해당 영역을 나가야 합니다.
전역 카드 소지자	하위 서버에서 카드 소지자를 보고 모니터링할 수 있게 하려면 선택합니다. 이 옵션은 주 서버에서 생성된 카드 소지자만 사용할 수 있습니다. 를 참조하십시오.

자격 증명 추가

카드 소지자에게 다음 유형의 자격 증명을 추가할 수 있습니다.

- PIN
- 카드
- 번호판
- 휴대폰

카드 소지자에게 번호판 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **License plate(번호판)**를 선택합니다.
2. 차량을 설명하는 자격 증명 이름을 입력합니다.
3. 차량의 번호판 번호를 입력합니다.
4. 자격 증명의 시작 날짜와 종료 날짜를 설정합니다.

5. **추가**를 클릭합니다.

*번호판 번호를 자격 증명으로 사용, on page 92*의 예시를 참조하십시오.

카드 소지자에게 PIN 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **PIN**을 선택합니다.
2. 핀을 입력합니다.
3. 감금 핀을 사용하여 무음 알람을 트리거하려면 **Duress PIN(감금 핀)**을 켜고 감금 핀을 입력합니다.
4. **추가**를 클릭합니다.

핀 자격 증명은 항상 유효합니다. 또한 도어를 열고 시스템에서 무음 알람을 트리거하는 감금 핀을 구성할 수도 있습니다.

카드 소지자에게 카드 자격 증명을 추가하려면 다음을 수행합니다.

1. **Credentials(자격 증명)**에서 **+ Add(추가)**를 클릭하고 **Card(카드)**를 선택합니다.
2. 카드 데이터를 수동으로 입력하려면 카드 이름, 카드 번호 및 비트 길이를 입력합니다.

비고

비트 길이는 시스템에 없는 특정 비트 길이로 카드 형식을 생성할 때만 구성될 수 있습니다.

3. 마지막으로 긁은 카드의 카드 데이터를 자동으로 가져오려면 다음을 수행합니다.
   3.1. **Select reader(리더 선택)** 드롭다운 메뉴에서 도어를 선택합니다.
   3.2. 해당 도어에 연결된 리더에 카드를 댑니다.
   3.3. **Get last swiped card data from the door's reader(s)(도어의 리더에서 마지막으로 긁은 카드 데이터 가져오기)**를 클릭합니다.
4. 시설 코드를 입력합니다. 이 필드는 **Access management > Settings(접근 관리 > 설정)**에서 **Facility code(시설 코드)**를 활성화한 경우에만 사용될 수 있습니다.
5. 자격 증명의 시작 날짜와 종료 날짜를 설정합니다.
6. **추가**를 클릭합니다.

만료일	
유효 기간 시작:	자격 증명의 유효 기간을 날짜와 시간으로 설정합니다.
유효 기간 종료:	드롭다운 메뉴에서 옵션을 선택합니다.

유효 기간 종료:	
종료 날짜 없음	자격 증명은 만료되는 일이 없습니다.
날짜	자격 증명이 만료되는 날짜와 시간을 설정합니다.
최초 사용 이후	첫 번째 사용 후 자격 증명이 만료되는 기간을 선택합니다. 첫 사용 후 일수, 월수 또는 연수 또는 횟수를 선택합니다.
마지막 사용 이후	마지막 사용 후 자격 증명이 만료되는 기간을 선택합니다. 마지막 사용 후 일수, 월수 또는 연수를 선택합니다.

번호판 번호를 자격 증명으로 사용

이 예에서는 도어 컨트롤러, AXIS License Plate Verifier가 설치된 카메라, 번호판 번호를 자격 증명으로 사용하여 접근 권한을 부여하는 방법을 설명합니다.

1. AXIS Optimizer에 도어 컨트롤러 및 카메라를 추가합니다.
2. **Synchronize with server computer time(서버 컴퓨터 시간과 동기화)**을 사용하여 새 장치의 날짜와 시간을 설정합니다.
3. 사용 가능한 최신 버전으로 새 장치의 소프트웨어를 업그레이드합니다.
4. 도어 컨트롤러에 연결된 새 도어를 추가합니다. *도어를 추가합니다, on page 73*를 참조하십시오.
   4.1. **Side A(A면)**에 리더를 추가합니다. *리더 추가, on page 78*를 참조하십시오.
   4.2. **Door settings(도어 설정)**에서 **AXIS License Plate Verifier**를 **Reader type(리더 유형)**으로 선택하고 해당 리더의 이름을 입력합니다.
   4.3. 원하는 경우 **Side B(측면 B)**에 리더 또는 REX 장치를 추가합니다.
   4.4. **Ok(확인)**를 클릭합니다.
5. 카메라에 AXIS License Plate Verifier를 설치하고 활성화합니다. *AXIS License Plate Verifier* 사용자 설명서를 참조하십시오.
6. AXIS License Plate Verifier를 시작합니다.
7. AXIS License Plate Verifier를 구성합니다.
   7.1. **Configuration > Access control > Encrypted communication(구성 > 접근 제어 > 암호화된 통신)**으로 이동합니다.
   7.2. **External Peripheral Authentication Key(외부 주변 장치 인증 키)**에서 **Show authentication key(인증 키 표시)** 및 **Copy key(키 복사)**를 클릭합니다.
   7.3. 카메라의 웹 인터페이스에서 AXIS License Plate Verifier를 엽니다.
   7.4. 설정하지 마십시오.
   7.5. **Settings(설정)**로 이동합니다.
   7.6. **Access control(접근 제어)**에서 **Secure Entry(보안 진입)**를 **Type(유형)**으로 선택합니다.
   7.7. **IP address(IP 주소)**에서 도어 컨트롤러의 IP 주소를 입력합니다.
   7.8. **Authentication key(인증 키)**에서 이전에 복사한 인증 키를 붙여넣습니다.
   7.9. **Connect(연결)**를 클릭합니다.
   7.10. **Door controller name(도어 컨트롤러 이름)**에서 도어 컨트롤러를 선택합니다.
   7.11. **Reader name(리더 이름)**에서 이전에 추가한 리더를 선택합니다.
   7.12. 통합을 켭니다.
8. 접근 권한을 부여받을 카드 소지자를 추가합니다. *카드 소지자 추가, on page 89*를 참조하십시오.
9. 새 카드 소지자에게 번호판 자격 증명을 추가합니다. *자격 증명 추가, on page 90*를 참조하십시오.
10. 접근 룰을 추가합니다. *접근 룰을 추가합니다, on page 93*를 참조하십시오.
    10.1. 일정을 추가합니다.
    10.2. 번호판 접근 권한을 부여받을 카드 소지자를 추가합니다.
    10.3. AXIS License Plate Verifier 리더가 장착된 도어를 추가합니다.

그룹 추가

그룹을 사용하면 카드 소지자와 그의 접근 룰을 모두 함께 효율적으로 관리할 수 있습니다.

1. **Site Navigation(사이트 탐색)** > **AXIS Optimizer** > **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.
2. **Groups(그룹)**로 이동하여 **+ Add(+ 추가)**를 클릭합니다.
3. 그룹의 이름을 입력하고 필요에 따라 이니셜을 선택적으로 입력합니다.
4. 하위 서버에서 카드 소지자 그룹을 보고 모니터링하기 위해 **Global group(글로벌 그룹)**을 선택합니다. 이 옵션은 주 서버에서 생성된 카드 소지자만 사용할 수 있습니다. *다중 서버 BETA, on page 88*를 참조하십시오.
5. 그룹에 카드 소지자를 추가하려면 다음을 수행합니다.
   5.1. **+ 추가**를 클릭합니다.
   5.2. 추가할 카드 소지자를 선택하고 **Add(추가)**를 클릭합니다.
6. **Save(저장)**를 클릭합니다.

접근 룰을 추가합니다

접근 룰은 접근 권한 부여를 위해 충족되어야 하는 조건을 정의한 것입니다.

접근 룰은 다음으로 구성됩니다.

카드 소지자 및 카드 소지자 그룹 - 접근 권한을 부여할 대상입니다.

도어 및 영역 - 접근 권한이 적용되는 장소입니다.

일정 - 접근 권한을 부여하는 시간 계획입니다.

접근 룰을 추가하려면 다음을 수행합니다.

1. **Access control(접근 제어)** > **Cardholder management(카드 소지자 관리)**로 이동합니다.
2. **Access rules(접근 룰)**에서 **+ Add(추가)**를 클릭합니다.
3. 접근 룰의 이름을 입력하고 **Next(다음)**를 클릭합니다.
4. 카드 소지자와 그룹을 구성합니다.
   4.1. **Cardholders(카드 소지자)** 또는 **Groups(그룹)**에서 **+ Add(추가)**를 클릭합니다.
   4.2. 카드 소지자 또는 그룹을 선택하고 **Add(추가)**를 클릭합니다.
5. 도어 및 영역을 구성합니다.
   5.1. **Doors(도어)** 또는 **Zones(영역)**에서 **+ Add(추가)**를 클릭합니다.
   5.2. 도어 또는 영역을 선택하고 **Add(추가)**를 클릭합니다.
6. 일정을 구성합니다.
   6.1. **Schedules(일정)**에서 **+ Add(추가)**를 클릭합니다.
   6.2. 일정을 하나 이상 선택하고 **Add(추가)**를 클릭합니다.
7. **Save(저장)**를 클릭합니다.

위에서 설명한 구성 요소 중 하나 이상이 누락된 접근 룰은 불완전한 것입니다. **Incomplete(불완전)** 탭에서 모든 불완전한 접근 룰을 확인할 수 있습니다.

도어 및 구역 수동 잠금 해제

도어 수동 잠금 해제와 같은 수동 액션에 대한 자세한 내용은 *수동 액션, on page 83*을 참조하십시오.

구역 수동 잠금 해제와 같은 수동 액션에 대한 자세한 내용은 *수동 액션, on page 83*을 참조하십시오.

시스템 구성 보고서 내보내기

시스템에 대한 다양한 유형의 정보를 포함하는 보고서를 내보낼 수 있습니다. AXIS Optimizer은(는) 보고서를 쉼표로 구분된 값(CSV) 파일로 내보내고 기본 다운로드 폴더에 저장합니다. 보고서를 내보내려면 다음을 수행합니다.

1. **Reports(보고서)** > **System configuration(시스템 구성)**으로 이동합니다.
2. 내보낼 보고서를 선택한 후 **Download(다운로드)**를 클릭합니다.

카드 소지자 세부 정보	카드 소지자, 자격 증명, 카드 인증 및 마지막 트랜잭션에 대한 정보를 포함합니다.
카드 소지자 접근	카드 소지자 정보 및 카드 소지자 그룹, 접근 룰, 도어 및 카드 소지자와 관련된 영역에 대한 정보를 포함합니다.
카드 소지자 그룹 접근	카드 소지자 그룹 이름과 카드 소지자, 접근 룰, 도어 및 카드 소지자 그룹과 관련된 영역에 대한 정보를 포함합니다.
접근 룰	접근 룰 이름은 물론 접근 룰과 관련된 카드 소지자, 카드 소지자 그룹, 도어 및 영역에 대한 정보를 포함합니다.
도어 접근	도어 이름과 도어와 관련된 카드 소지자, 카드 소지자 그룹, 접근 룰 및 영역에 대한 정보를 포함합니다.
구역 접근	영역 이름은 물론 영역과 관련된 카드 소지자, 카드 소지자 그룹, 접근 룰 및 도어에 대한 정보를 포함합니다.

카드 소지자 활동 보고서 생성

점호 보고서는 지정된 영역 내의 카드 소지자를 나열하여 특정 시점에 누가 있는지 확인하는 데 도움을 줍니다.

소집 보고서는 지정된 영역 내의 카드 소지자를 나열하여 긴급 상황에서 누가 안전하며 누가 없는지 파악하는 데 도움이 됩니다. 건물 관리자가 대피 후 직원과 방문객의 위치를 파악하는 데 도움이 됩니다. 소집 지점은 긴급 상황 시 담당자가 보고하는 지정된 리더로, 사이트 안팎의 인원에 대한 보고서를 생성합니다. 시스템은 카드 소지자가 소집 지점에서 체크인하거나 누군가가 수동으로 안전하다고 표시할 때까지 카드 소지자를 부재중으로 표시합니다.

점호 보고서 및 소집 보고서 모두 카드 소지자를 추적하기 위한 영역이 필요합니다.

점호 보고서 또는 소집 보고서를 생성하고 실행하려면 다음을 수행합니다.

1. **Reports(보고서)** > **Cardholder activity(카드 소지자 활동)**로 이동합니다.
2. **+ Add(추가)**를 클릭하고 **Roll call / Mustering(점호 / 소집)**을 선택합니다.
3. 보고서의 이름을 입력합니다.
4. 보고서에 포함할 영역을 선택합니다.
5. 보고서에 포함할 그룹을 선택합니다.
6. 소집 보고서가 필요한 경우 **Mustering point(소집 지점)**와 소집 지점 리더를 선택합니다.
7. 보고서의 기간을 선택합니다.
8. **Save(저장)**를 클릭합니다.
9. 보고서를 선택하고 **Run(실행)**을 클릭합니다.

점호 보고서 상태	설명
있음	카드 소지자가 지정된 영역에 들어갔으며 보고서를 실행하기 전에 나오지 않았습니다.
없음	카드 소지자가 지정된 영역에서 나왔으며 보고서를 실행하기 전에 다시 들어가지 않았습니다.

소집 보고서 상태	설명
안전	카드 소지자가 소집 지점에서 카드를 댔습니다.
누락	카드 소지자가 소집 지점에서 카드를 대지 않았습니다.

액세스 관리 설정

액세스 관리 대시보드에서 사용되는 카드 소지자 필드를 사용자 지정하려면 다음을 수행합니다.

1. **Access management(접근 관리)** 탭에서 **Settings(설정)** > **Custom cardholder fields(사용자 지정 카드 소지자 필드)**를 클릭합니다.
2. **+ Add(추가)**를 클릭하고 이름을 입력합니다. 사용자 지정 필드를 최대 6개까지 추가할 수 있습니다.
3. **추가**를 클릭합니다.

시설 코드를 사용하여 접근 제어 시스템을 확인하려면 다음을 수행합니다.

1. **Access management(접근 관리)** 탭에서 **Settings(설정)** > **Facility code(시설 코드)**를 클릭합니다.
2. **Facility code on(시설 코드 켜짐)**을 선택합니다.

비고

식별 프로파일을 구성할 때 **Include facility code for card validation(카드 검증에 시설 코드 포함)**도 선택해야 합니다. 를 참조하십시오.

가져오기 및 내보내기

카드 소지자 가져오기

이 옵션은 CSV 파일에서 카드 소지자, 카드 소지자 그룹 자격 증명 및 카드 소지자 사진을 가져옵니다. 카드 소지자 사진을 가져오려면 서버가 사진에 액세스할 수 있는지 확인하십시오.

카드 소지자를 가져올 때는 액세스 관리 시스템에서 자동으로 모든 하드웨어 구성을 포함한 시스템 구성을 저장하며 이전에 저장된 모든 구성을 삭제합니다.

가져오기 옵션	
새로 만들기	이 옵션은 기존 카드 소지자를 제거하고 새 카드 소지자를 추가합니다.
업데이트	이 옵션으로 기존 카드 소지자를 업데이트하고 새 카드 소지자를 추가합니다.
추가	이 옵션은 기존 카드 소지자를 유지하고 새 카드 소지자를 추가합니다. 카드 번호와 카드 소지자 ID는 고유하며 한 번만 사용할 수 있습니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Import cardholders(카드 소지자 가져오기)**를 클릭합니다.
3. **New(새로 만들기)**, **Update(업데이트)** 또는 **Add(추가)**를 선택합니다.
4. **Next(다음)**를 클릭합니다.
5. **Choose a file(파일 선택)**을 클릭하고 CSV 파일로 이동합니다. **Open(열기)**을 클릭합니다.
6. 열 구분자를 입력하고 고유 식별자를 선택한 후 **Next(다음)**를 클릭합니다.

7. 각 열에 방향을 할당합니다.
8. **Import(가져오기)**를 클릭합니다.

가져오기 설정	
첫 번째 행은 머리글입니다.	CSV 파일에 열 머리글이 포함되어 있으면 선택합니다.
열 구분자	CSV 파일의 열 구분자 형식을 입력합니다.
고유 식별자	시스템은 기본적으로 **Cardholder ID(카드 소지자 ID)**를 사용하여 카드 소지자를 식별합니다. 또한, 성과 이름 또는 이메일 주소를 사용할 수 있습니다. 고유 식별자는 중복된 인사 기록의 가져오기를 방지합니다.
카드 번호 형식	**16진수와 숫자 모두 허용**이 기본으로 선택됩니다.

카드 보유자 내보내기

이 옵션은 시스템의 카드 소지자 데이터를 CSV 파일로 내보냅니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Export cardholders(카드 소지자 내보내기)**를 클릭합니다.
3. 다운로드 위치를 선택한 후 **Save(저장)**를 클릭합니다.

AXIS Optimizer은(는) 구성이 변경될 때마다 `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`에서 카드 소지자 사진을 업데이트합니다.

가져오기 실행 취소

카드 소지자 가져오기를 할 때 시스템에서 자동으로 해당 구성을 저장합니다. **Undo import(가져오기 실행 취소)** 옵션은 카드 소지자 데이터와 모든 하드웨어 구성을 마지막 카드 소지자 가져오기 이전 상태로 재설정합니다.

1. **Access management(접근 관리)** 탭에서 **Import and export(가져오기 및 내보내기)**를 클릭합니다.
2. **Undo import(가져오기 실행 취소)**를 클릭합니다.
3. **Yes(예)**를 클릭합니다.

백업 및 복원

자동 백업은 매일 밤 수행됩니다. 최신 백업 파일 3개는 C:₩ProgramData₩Axis Communications₩AXIS Optimizer Secure Entry₩backup에 저장됩니다. 이 파일들을 복구하는 방법:

1. 백업 파일을 C:₩ProgramData₩Axis Communications₩AXIS Optimizer Secure Entry₩restore로 이동합니다.
2. 다음 방법 중 하나로 AXIS Secure Entry를 다시 시작합니다.
   - MSC(서비스) 프로그램을 시작하고 'AXIS Optimizer Secure Entry Service'를 찾아 재시작합니다.
   - 컴퓨터를 재시작합니다.
3. 이벤트 서버 컴퓨터에서 AXIS Optimizer 설치 프로그램을 다시 실행합니다.

Smart Client에서 접근 관리

운영자는 Smart Client를 통해 접근 제어 시스템과 관련된 작업을 수행할 수 있습니다. 수동 도어 제어와 같은 접근 제어의 대부분의 기능은 Smart Client에서 사용할 수 있습니다. 이러한 기능에 대한 자세한 내용은 *Smart Client에서 접근 제어 사용하기*를 참조하십시오.

Smart Client에서 직접 액세스를 관리할 수도 있습니다. Management Client에 있는 다음 기능은 Smart Client에서도 사용할 수 있습니다.

- 카드 소지자 관리
- 일반 설정
- 사용자 정의 카드 소지자 필드
- 시설 코드
- 이메일 템플릿
- 배지 템플릿 BETA

Smart Client에서 Axis 접근 관리 탭을 표시하는 방법:

1. Smart Client 컴퓨터에 AXIS Optimizer를 설치합니다.
2. 활성화된 도어 라이센스가 없으면 도어 라이센스 하나를 활성화합니다. 도어 라이센스를 활성화하려면 *도어 라이센스 활성화, on page 71*를 참조하십시오.
3. 로그인한 사용자에게 접근 관리 권한이 있는지 확인합니다. *AXIS Secure Entry 역할 설정, on page 97*을 참조하십시오.

AXIS Secure Entry 역할 설정

1. Management Client에서 **Site Navigation(사이트 탐색)** > **Security(보안)** > **Roles(역할)**로 이동합니다.
2. 시스템에서 특정 역할을 선택합니다.
3. **AXIS Optimizer**를 선택합니다.
4. 목록을 확장하고 **Access control(접근 제어)**을 클릭합니다.
5. 접근 제어 보안 설정에 대해 **Read(읽기)**를 선택합니다.
6. 역할에 권한을 부여할 기능을 클릭하고 **Grant(부여)**를 선택합니다.
   - **Access control configuration(접근 제어 구성):** 운영자 역할에 Configuration(구성) 탭의 모든 기능에 대한 권한을 부여합니다.
   - **Access management(접근 관리):** 운영자 역할에 Access Management(접근 관리) 탭의 모든 기능에 대한 권한을 부여합니다.

시스템 관리 및 보안 통제

운영자의 기능 액세스를 위한 사용자 정의

역할 설정

기본적으로 운영자는 VMS에서 장치에 대한 접근 권한이 있으면 모든 AXIS Optimizer 기능에도 액세스할 수 있습니다. 하지만 Management Client에서 운영자는 역할 설정을 통해 액세스할 수 있는 기능을 설정할 수 있습니다.

역할 설정을 구성

Role settings(역할 설정)을 켜기:

1. Management Client에서 **Site Navigation > Security > AXIS Optimizer Security(사이트 탐색 > 보안 > AXIS Optimizer 보안)**로 이동합니다.

비고

역할 설정은 한 번 켜면 끌 수 없습니다. 이 설정은 영구적입니다.

2. **Turn on role settings(역할 설정 켜기)**를 선택합니다.
3. Management Client를 다시 시작하십시오.

역할 설정을 구성:

1. Management Client에서 **Site Navigation > Security > Roles(사이트 탐색 > 보안 > 역할)**로 이동합니다.
2. 역할을 선택하고 **Overall security(전반적인 보안)**으로 이동합니다.
3. **AXIS Optimizer Security**를 클릭합니다.
4. 역할이 액세스할 수 있는 기능을 선택합니다.
   - **전체 제어**운영자 역할에 모든 AXIS Optimizer 기능에 대한 전체 액세스 권한을 부여합니다.
   - **편집(해당 없음)**AXIS Optimizer Role 설정에 적용할 수 없는 VMS 기능.
   - **Management Client에서 AXIS Optimizer에 액세스.**운영자 역할은 Management Client에서 모든 AXIS Optimizer 관리 기능을 사용할 수 있습니다.
   - **AXIS Optimizer 보안 관리.**운영자 역할은 **Site Navigation > Security > AXIS Optimizer Security**에서 설정을 변경할 수 있습니다.
   - **동적 카메라 운영자 컨트롤.**운영자 역할은 시스템이 장치에서 찾은 사전 설치된 모든 기능에 액세스할 수 있습니다.
   - **원격 포커스 운영자 컨트롤.**운영자 역할은 고정형 돔 카메라에 원격 포커스를 설정할 수 있습니다.
   - **PTZ 운영자 컨트롤.**운영자 역할은 특정 운영자 PTZ 제어에 액세스할 수 있습니다. 포커스 제어, PTZ 사전 설정, 오토트래킹 2용 운영자 제어, 워셔 및 SpeedDry/Wiper 버튼
   - **온도 스팟 측정 컨트롤.**운영자 역할은 AXIS Q2901-E에서 스팟 온도를 측정할 수 있습니다.
   - **스피커 운영자 컨트롤.**운영자 역할은 Smart Client의 모든 Speaker manager 기능에 액세스할 수 있습니다.
   - **방문자 관리 액세스.**운영자 역할은 방문자 관리와 관련된 모든 것(예: 호출 받기 및 실시간 보기에서 도어 열기)에 액세스할 수 있습니다.
   - **통화 기록 액세스.**운영자 역할은 인터콤의 호출 기록에 액세스할 수 있습니다. 이 설정을 사용하기 위해 **Access visitor management(방문자 관리 액세스)**를 허용해야 합니다.

- **확장된 검색 기능.Deny**를 선택하면 AXIS License Plate Verifier 탭이 Smart Client에서 숨겨집니다. 또한 중앙 집중식 검색에서는 차량 및 컨테이너 검색을 사용할 수 없습니다.
- **디워핑 보기 제어**운영자 역할은 디워핑 보기 내에서 이동할 수 있습니다.
- **디워핑 보기의 홈 위치 편집**운영자는 카메라의 홈 위치를 편집할 수 있습니다.
- **웹 페이지**운영자 역할은 웹 브라우저로 보기를 생성할 수 있습니다.
- **Axis 심층 정보 대시보드**
  운영자 역할은 Axis 인사이트 대시보드 액세스 권한을 가집니다.

5. **Save(저장)**를 클릭합니다.
6. 시스템에서 실행 중인 모든 Smart Clients를 재시작합니다.

장치 관리

AXIS Device Manager Extend

AXIS Optimizer에서 AXIS Device Manager Extend를 사용하여 여러 사이트의 장치를 관리할 수 있습니다. 녹화 서버에 에지 호스트를 설정하면 AXIS Device Manager Extend가 VMS 시스템의 장치에 연결할 수 있습니다. 보증 정보를 쉽게 검토하고, 단일 사용자 인터페이스의 여러 장치 및 사이트에서 소프트웨어 업그레이드를 수행할 수 있습니다.

AXIS Device Manager Extend에 대한 자세한 내용은 *사용자 설명서*를 참조하십시오.

비고

요구 사항

- *MyAxis 계정*에 로그인합니다.
- 녹화 서버는 인터넷에 연결되어 있어야 합니다.
- AXIS OS 6.50을 실행하는 장치에서만 지원됩니다. 지원되는 장치를 알아보려면 *FAQ*를 참조하십시오.

엣지 호스트 설치

에지 호스트는 AXIS Device Manager Extend가 VMS 시스템의 로컬 장치와 통신할 수 있게 만드는 사내 관리 서비스입니다.

VMS에서 AXIS Device Manager Extend를 사용하려면 에지 호스트와 데스크톱 클라이언트를 설치해야 합니다. 에지 호스트와 데스크톱 클라이언트 모두 AXIS Device Manager Extend 설치 프로그램에 포함되어 있습니다.

1. AXIS Device Manager Extend *설치 관리자*를 다운로드합니다.
   VMS 녹화 서버에 에지 호스트를 설치해야 합니다.
2. 녹화 서버에서 설치 프로그램을 실행하고 에지 호스트만 설치하도록 선택합니다.

열린 네트워크 포트 및 기타 요구 사항에 대한 자세한 내용은 *Axis Device Manager Extend 사용자 설명서*를 참조하십시오.

에지 호스트를 요청하고 장치 동기화



1. Management Client를 엽니다.

2. **Site Navigation > AXIS Optimizer > System Overview(사이트 탐색 > AXIS Optimizer > 시스템 오버뷰)**로 이동합니다.
3. 을 선택하고 MyAxis에 로그인합니다.
4. 소유권을 주장할 준비가 된, 설치된 에지 호스트가 있는 녹화 서버 타일을 클릭합니다.
5. 사이드바에서 새 조직을 생성하거나 이전에 만든 조직을 선택합니다.
6. 에지 호스트를 클릭하고 요청합니다.
7. 페이지가 다시 로드될 때까지 기다렸다가 **Synchronize(동기화)**를 클릭합니다.
   이제 녹화 서버의 모든 Axis 장치가 에지 호스트에 추가되고, 사용자가 선택한 조직에 속하게 됩니다.

비고

AXIS Device Manager Extend는 VMS에서 Axis 하드웨어에 액세스할 수 있어야 합니다. 지원되는 장치에 대한 자세한 내용은 *에지 호스트에 장치 추가 문제 해결, on page 101*을 참조하십시오.

8. 녹화 서버에 새 장치를 추가하거나 장치 정보를 변경하는 경우 7단계를 다시 수행하여 변경 사항을 AXIS Device Manager Extend 시스템과 동기화해야 합니다.
9. AXIS Device Manager Extend에 추가하려는 장치가 있는 모든 녹화 서버에 대해 4~7단계를 반복합니다.

에지 호스트 상태

System overview(시스템 오버뷰)의 각 녹화 서버에서 에지 호스트가 아직 설치 또는 요청되었는지 여부를 확인할 수 있습니다. **Show machines that need edge host action(에지 호스트 작업이 필요한 장치 표시)**을 켜서 보기를 필터링할 수 있습니다.

- - 녹화 서버에서 에지 호스트가 감지되지 않았습니다.
  - 에지 호스트가 설치되지 않은 경우 녹화 서버에 에지 호스트를 다운로드하여 설치합니다. *엣지 호스트 설치, on page 99*를 참조하십시오.
  - 에지 호스트가 설치되어 있는 경우, 에지 호스트를 감지하려면 MyAxis 계정에 로그인해야 한다는 의미입니다.
- - 에지 호스트가 설치되었지만, 청구되지 않았습니다. 새 조직을 생성하여 에지 호스트를 요청하거나 이전에 생성된 조직을 선택합니다. *에지 호스트를 요청하고 장치 동기화, on page 99*를 참조하십시오.
-  - 에지 호스트가 설치 및 청구되었지만, 연결할 수 없습니다. 녹화 서버가 인터넷에 연결되어 있는지 확인합니다.
-  - Edge 호스트가 동기화되었습니다.
-  – 에지 호스트에 동기화가 필요합니다. 에지 호스트에 추가할 수 있는 VMS의 새 장치 또는 동기화가 필요한 업데이트된 장치 정보일 수도 있습니다.

AXIS Device Manager Extend를 사용하여 장치 구성

장치가 에지 호스트와 동기화되면 AXIS Device Manager Extend에서 장치를 구성할 수 있습니다. 인터넷에 연결된 모든 PC에서 이 작업을 수행할 수 있습니다.

비고

원격 연결을 통해 장치를 관리하려면 *각 에지 호스트에서 원격 액세스*를 켜야 합니다.

1. *AXIS Device Manager Extend 데스크탑 애플리케이션*을 설치하고 엽니다.
2. 에지 호스트를 요청하는 데 사용된 조직을 선택합니다.
3. 동기화된 장치는 VMS 녹화 서버와 이름이 같은 사이트에서 찾을 수 있습니다.

에지 호스트에 장치 추가 문제 해결

에지 호스트에 장치를 추가하는 데 문제가 있는 경우 다음과 같이 합니다.

- AXIS Optimizer는 VMS에서 활성화된 하드웨어만 추가합니다.
- VMS에서 하드웨어와의 연결이 끊어지지 않았는지 확인합니다.
- 장치에 AXIS OS 6.50 이상이 설치되어 있는지 확인합니다.
- 장치가 다이제스트 인증으로 설정되어 있는지 확인합니다. 기본적으로 AXIS Device Management는 기본 인증을 지원하지 않습니다.
- AXIS Device Manager Extend 애플리케이션에서 직접 장치를 추가해 보십시오.
- AXIS Device Manager Extend에서 로그를 수집하고 Axis 지원에 문의하십시오.
  1. AXIS Device Manager Extend 애플리케이션에서 카메라가 설치된 녹화 서버의 특정 사이트로 이동합니다.
  2. **Settings(설정)**으로 이동하여 **Download sitelog(사이트로그 다운로드)**를 클릭합니다.

AXIS Site Designer 가져오기

AXIS Optimizer에서는 손쉬운 가져오기 프로세스 한 번으로 VMS에 AXIS Site Designer 설계 프로젝트를 가져와 구성을 적용할 수 있습니다. *AXIS Site Designer*를 사용해 시스템을 설계 및 구성합니다. 프로젝트를 마치면 AXIS Optimizer를 통해 AXIS Site Designer에서 Management Client로 카메라 및 기타 장치의 설정을 모두 가져올 수 있습니다.

*사용자 설명서*에서 AXIS Site Designer에 대한 세부 정보를 참조하십시오.

비고

요구 사항
- VMS 버전 2020 R2 이상

설계 프로젝트 가져오기



AXIS Site Designer에서

1. 프로젝트를 생성하고 장치를 구성합니다.
2. 프로젝트를 마치면 코드를 생성하거나 설정 파일을 다운로드합니다.

비고

설계 프로젝트를 업데이트한다면 새 코드를 생성하거나 새 설정 파일을 다운로드해야 합니다.

Management Client에서

1. VMS에 관련 장치가 추가되었는지 확인하세요.
2. **Site Navigation > AXIS Optimizer > Import design project(사이트 탐색 > AXIS Optimizer > 설계 프로젝트 가져오기)**로 이동합니다.
3. 단계별 가이드가 열립니다. 액세스 코드를 입력하거나 프로젝트의 설정 파일을 선택하여 가져오려는 프로젝트를 선택합니다. **Next(다음)**를 클릭합니다.
4. **Project overview(프로젝트 오버뷰)**에서 AXIS Site Designer 프로젝트에서 발견된 장치 수와 VMS에서 발견된 장치 수에 대한 정보를 확인할 수 있습니다. **Next(다음)**를 클릭합니다.

5. 다음 단계에서는 VMS의 장치를 AXIS Site Designer 설계 프로젝트의 장치와 일치시킵니다. 매칭될 수 있는 항목이 하나만 있는 장치가 자동으로 선택됩니다. 매칭되는 장치만 가져옵니다. 일치시키는 것을 마치면 **Next(다음)**를 클릭합니다.
6. 일치하는 모든 장치의 설정을 가져와 VMS에 적용합니다. 설계 프로젝트의 규모에 따라 몇 분이 소요될 수 있습니다. **Next(다음)**를 클릭합니다.
7. **Results of import(가져오기 결과)**에서 가져오기 프로세스의 여러 단계에 대한 세부 정보를 살펴볼 수 있습니다. 일부 설정을 가져올 수 없으면 문제를 해결하고 가져오기를 다시 실행합니다. 결과 목록을 파일로 저장하려면 **Export...(내보내기...)**를 클릭합니다. **Done(완료)**을 클릭하여 단계별 가이드를 닫습니다.

가져온 설정

VMS와 설계 프로젝트 사이의 일치하는 장치만 가져오기의 일부가 됩니다. 모든 장치 유형을 위해 다음 설정을 가져와 VMS에 적용합니다.

- 설계 프로젝트에 사용한 장치 이름
- 설계 프로젝트에 사용한 장치 설명
- 지도에 장치가 배치된 경우의 위치 정보 설정

장치에서 영상을 지원하는 경우 다음 설정도 적용됩니다.

- VMS에 구성된 비디오 스트림(해상도, 프레임 레이트, 코덱, 압축 및 Zipstream 설정) 하나 또는 두 개
  - 비디오 스트림 1은 실시간 보기 및 녹화용으로 구성됩니다.
  - 설계 프로젝트의 스트림 설정이 실시간 보기와 녹화 간에 상이하다면, 비디오 스트림 2가 녹화용으로 구성됩니다.
- 설계 프로젝트에 따라 모션 디텍션 또는 연속 녹화 룰을 설정합니다. VMS에 내장된 모션 디텍션을 사용하고, 룰에 대한 시간 프로파일을 생성하며, 녹화 서버에 여러 보존 시간에 대한 저장소 프로파일을 생성합니다.
- 설계 프로젝트의 오디오 설정에 따라 마이크가 켜지거나 꺼집니다.

제한 사항

VMS에는 AXIS Site Designer 설계 프로젝트를 가져올 때 제한 사항이 있습니다.

- VMS의 기본 모션 녹화 룰은 가져오기로 생성된 녹화 룰을 재정의할 수 있습니다. 충돌하는 룰을 모두 끄거나 룰에서 영향을 받는 장치를 제외합니다.
- VMS 모션 트리거 녹화의 경우 녹화 추정치가 부정확할 수도 있습니다.
- 현재 버전에서는 평면도를 지원하지 않습니다.
- 설계 프로젝트에서 모션 트리거 녹화와 연속 녹화를 동시에 구성한 경우 모션 트리거 녹화 설정의 스트림 설정만 사용합니다.
- VMS에서는 Zipstream에 대한 최소 프레임 레이트 구성이 불가능합니다.

계정 관리

계정 관리는 XProtect에서 사용하는 모든 Axis 장치의 계정과 패스워드를 관리하는 데 도움이 됩니다.

Axis 지침에 따르면 root 계정을 사용하여 장치에 연결하면 안 됩니다. 계정 관리를 사용하면 XProtect 서비스 계정을 만들 수 있습니다. 각 장치마다 고유한 16자 패스워드가 생성됩니다. XProtect 계정이 이미 있는 장치에는 새 패스워드가 부여됩니다.

XProtect 서비스 계정으로 장치에 연결

1. **Site Navigation > AXIS Optimizer > Account management(사이트 탐색 > AXIS Optimizer > 계정 관리)**를 이동합니다.

그래프는 온라인 상태인 장치 수, XProtect 서비스 계정이 있는 장치 수, XProtect 서비스 계정이 없는 장치 수를 보여줍니다.

2. 장치에 대한 자세한 정보를 보려면 **Show device details(장치 세부 정보 표시)**를 클릭합니다. 온라인 상태인 장치는 목록 상단에 표시됩니다. 패스워드를 생성할 특정 장치를 선택할 수 있습니다. 아무 것도 선택하지 않으면 온라인 상태인 모든 장치에 새 패스워드가 부여됩니다. **확인**을 클릭합니다.

비고

하드웨어 구성에서 HTTP를 선택하면 녹화 서버와 Axis 장치 간에 패스워드가 일반 텍스트로 전송됩니다. VMS와 장치 간의 통신을 보호하려면 HTTPS를 설정할 것을 권장합니다.

3. **Generate passwords(패스워드 생성)**를 클릭합니다. 생성된 패스워드에는 32~126자 범위의 ASCII 문자 16개로 이루어진 임의의 텍스트가 포함됩니다.
   프로세스의 실시간 상태 업데이트를 확인하기 위해 **Show device details(장치 세부 정보 표시)**를 클릭합니다. 프로세스가 진행되는 동안 활성 실시간 보기 및 보류 중인 녹화가 잠시 중단되는 것을 볼 수 있습니다.
4. 온라인 상태인 장치는 XProtect 서비스 계정과 새 패스워드를 받습니다. 온라인 상태이고 이미 XProtect 서비스 계정이 있는 장치는 새 패스워드만 받습니다.

Axis 이벤트

Axis 이벤트 기능은 VMS에서 Axis 장치에 사용 가능한 이벤트에 대한 개요를 제시합니다. 특정 장치에서 이벤트를 테스트하고, 이벤트에 대한 세부 정보를 보고, 여러 장치에 이벤트를 추가할 수 있습니다.

사이트 탐색에서 **룰 및 이벤트 > Axis 이벤트**로 이동합니다. **구성** 창에 사용 가능한 모든 이벤트 목록이 표시됩니다. 시스템에서 활성화된 이벤트 및 활성화되지 않은 이벤트를 확인할 수 있습니다.

각 이벤트에 대해 이벤트가 추가되는 장치의 장치 이름을 볼 수 있습니다. 이벤트 표시 이름, 이벤트 상태 및 이벤트가 마지막으로 트리거된 시간도 확인 가능합니다.

비고

요구 사항

- VMS 버전 2023 R2 이상.

여러 장치의 이벤트 설정

1. **구성**으로 이동하여 이벤트를 선택합니다.
2. **장치 추가(Add devices)** 를 클릭합니다.
3. **장치 추가** 창에는 이벤트를 추가할 수 있는 장치 목록이 표시됩니다. 장치를 하나 이상 선택하고 **장치 추가**를 클릭합니다.

장치에서 이벤트를 제거하려면 **제거**를 클릭합니다.

이벤트 정보

Axis 이벤트에서는 사용자 인터페이스의 마지막으로 알려진 발생, 이벤트 상태 및 실시간 업데이트를 볼 수 있습니다. 이렇게 하려면 관리 클라이언트에서 보존 시간을 설정해야 합니다.

1. **도구 > 옵션 > 알람 및 이벤트 > 장치 이벤트**로 이동합니다.
2. 전체 장치 이벤트 그룹 또는 그룹 내의 특정 이벤트에 대한 보존 시간을 설정합니다.

메타데이터와 검색

메타데이터 및 검색은 VMS에 추가한 모든 장치의 오버뷰, 해당 장치의 메타데이터 기능, 그리고 운영자에게 표시되는 Axis 검색 범주를 제공합니다.

메타데이터 및 검색을 사용하면 해당 장치의 특정 기능을 활성화할 수 있습니다. 즉, 여러 장치의 데이터, 분석 데이터, 통합 데이터 활성화하고, 장치에서 지원하는 분석 기능을 볼 수도 있습니다. Axis 검

색 카테고리를 사용하면 모든 운영자의 검색 옵션을 제어하여 VMS에서 사용 가능한 분석 기능을 반영할 수 있습니다. 검색 카테고리와 필터에 대한 지원은 카메라 모델과 설치된 분석 애플리케이션에 따라 다릅니다.

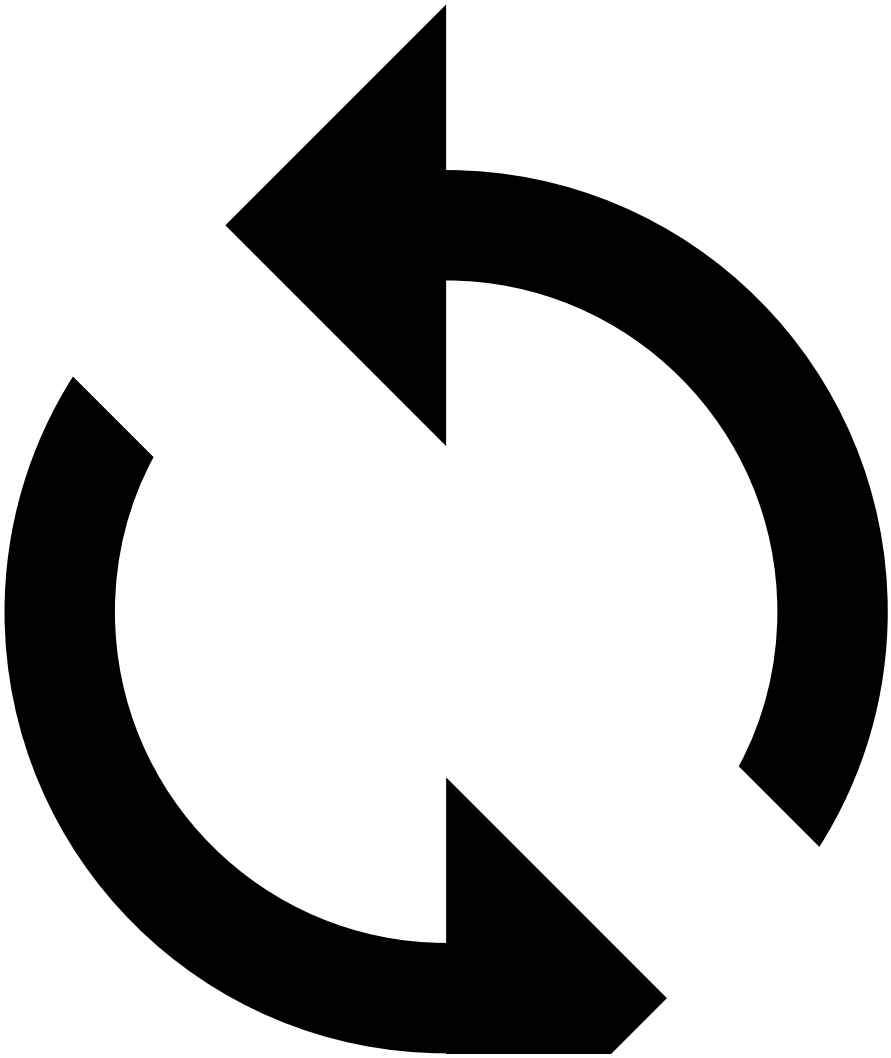
메타데이터 설정 구성

1. **관리 클라이언트** > **사이트 탐색** > **AXIS Optimizer** > **메타데이터 및 검색**으로 이동합니다.
   - **이벤트 데이터**: 장치에서 이벤트 데이터를 검색하려면 VMS를 켭니다. AXIS Optimizer의 여러 기능에 필요합니다.
   - **분석 데이터**: 포렌식 검색 기능을 사용하려면 켜고 실시간 보기 및 재생에서 바운딩 박스를 표시합니다.
   - **분석 기능**: 현재 장치에서 지원하는 객체 유형(사람, 차량) 및 객체 색상과 같은 영상 분석 기능을 확인합니다. 장치 소프트웨어를 업그레이드하면 더 많은 분석 기능이 제공될 수 있습니다.
   - **통합 메타데이터**: 활성화하여 Axis 인사이트에서 포렌식 검색을 더욱 빠르게 수행하고 로딩 시간을 단축하십시오.

   비고

   통합 메타데이터 요건
   - AXIS OS 11.10 이상 버전이 설치된 Axis 장치.

   통합 메타데이터 제한 사항
   - 실시간 보기 및 녹화에서 바운딩 박스와 VMS 내장 검색 옵션은 사용 불가능합니다.



– : 장치 구성을 변경한 후 클릭하여 다시 로드합니다.

Axis 검색 카테고리 구성

1. **관리 클라이언트** > **사이트 탐색** > **AXIS Optimizer** > **메타데이터 및 검색**으로 이동합니다.
2. **Axis 검색 카테고리** 대화 상자에서 사용하고 싶은 검색 카테고리 활성화:
   – 포렌식 검색
   – 차량 검색
   – 영역 속도 검색
   – 컨테이너 검색
3. 각 검색 카테고리에 적용 가능한 필터를 선택합니다.

비고

Axis 검색 카테고리 요구 사항

- Smart 클라이언트에서 AXIS Optimizer 버전 5.3 이상

사이버 보안

사이버 보안은 위험을 최소화하여 성공적인 제품 수명 주기를 지원합니다. 당사의 사이버 보안 접근 방식에 대한 자세한 정보와 문서는*axis.com/about-axis/cybersecurity*에서 확인하실 수 있습니다. Axis로부터 제품 보안 알림을 수신하고, 제품의 안전한 수명 주기 및 폐기를 위해 제품을 구성하려면 아래의 사이버 보안 지침을 따르십시오.

*Axis Trust Center*에서 Axis가 보안 규정 준수, 투명성, 데이터 보호 및 개인정보 보호를 구현하는 방법에 대한 정보를 확인할 수 있습니다.

취약성 관리

Axis는 *공통 취약점 및 노출(CVE) 번호 부여 기관(Common Vulnerability and Exposures (CVE) Numbering Authority: CNA)*입니다. 노출 위험을 최소화하기 위해 Axis는 장치, 소프트웨어 및 서비스의 취약점을 식별하고 해결할 때 업계 표준을 따릅니다. Axis의 취약점 관리 정책에 대한 정보 또는 취약점 보고는 *axis.com/vulnerability-management*를 참조하십시오.

보안 알림

*axis.com/security-notification-service*에서 Axis 보안 알림 이메일을 구독하세요. 귀하가 사용 중인 Axis 제품과 관련된 취약점, 관련 보안 권고 사항 및 기타 보안 관련 정보를 보내드리겠습니다.

보안 제품 수명 주기

Axis는 보안 수명 주기 관리를 통해 제품 수명 전반에 걸쳐 위험을 최소화합니다. *help.axis.com*의 보안 강화 가이드를 사용하여 Axis 제품을 더 안전하게 구성하고 운영하며 다음에 대한 정보를 확인하십시오.

안전한 최초 사용 - Axis 제품은 처음부터 안전한 초기화와 암호화된 통신이 가능하도록 높은 기본 보호 수준으로 사전 구성되어 있습니다.

용도 및 일반적인 구성 실수 - Axis 보안 강화 가이드는 Axis 제품의 올바른 사용 방법에 대한 정보를 제공하며, 여기에는 피해야 할 일반적인 보안 관련 오용 및 구성 실수가 포함됩니다.

취약점 관리 및 공급망 투명성 - 취약점을 공개하고 공급망 투명성을 개선하기 위해 모든 소프트웨어 릴리스마다 *axis.com*에 소프트웨어 구성품 명세서(SBOM)가 게시됩니다.

폐기 및 데이터의 안전한 삭제 - 제품이 수명 주기 종료에 도달했을 때 안전하게 폐기하려면 제품을 공장 초기화 설정으로 재설정하십시오. 그러면 구성, 저장된 데이터 및 민감한 정보가 지워집니다.

보안 강화 가이드

AXIS Optimizer는 VMS 인프라의 필수 구성 요소이므로 안전한 환경을 유지하려면 특정 구성이 필요합니다. 장치 패스워드를 보호하고 개인 정보를 보호하며 시스템에 대한 무단 액세스를 방지하려면 다음 권장 설정을 따르는 것이 필수적입니다.

- VMS에 Axis 장치를 추가할 때 HTTPS를 사용합니다.
- VMS 클라이언트와 서버 간의 암호화를 활성화합니다.
- VMS에서 암호화된 데이터 저장을 활성화합니다.
- 모든 VMS 역할을 검토하고 필요 이상의 권한을 사용하고 있지 않은지 확인합니다.

도움이 더 필요하십니까?

FAQ

질문	응답
클라이언트 PC가 인터넷에 액세스할 수 없을 때 AXIS Optimizer를 어떻게 업데이트합니까?	VMS 관리 서버에 새 버전을 게시합니다. *자동으로 시스템 업그레이드, on page 10*을(를) 참조하십시오.
AXIS Optimizer의 새 버전으로 업그레이드하기 전에 설정을 백업해야 합니까?	아니요, 백업할 필요가 없습니다. 새 버전으로 업그레이드해도 아무 것도 변경되지 않습니다.
AXIS Optimizer가 설치된 클라이언트 PC가 30대 이상인 경우 하나씩 업그레이드해야 합니까?	클라이언트를 개별적으로 업그레이드할 수 있습니다. 로컬 AXIS Optimizer 버전을 시스템에 게시하여 업그레이드를 자동으로 푸시할 수도 있습니다. *자동으로 시스템 업그레이드, on page 10*을(를) 참조하십시오.
AXIS Optimizer 내에서 각 플러그인을 개별적으로 활성화 또는 비활성화할 수 있습니까?	아니요, 하지만 적극적으로 사용하지 않는 경우 리소스를 사용하지 않습니다.
AXIS Optimizer는 어떤 포트를 사용합니까?	포트 80과 443은 모두 axis.com와 통신하는 데 필요하므로 시스템이 새 릴리스에 대한 정보를 얻고 업데이트를 다운로드할 수 있습니다. AXIS Secure Entry를 통해 AXIS Optimizer를 설치하면 인바운드 트래픽(TCP)용 53459 및 53461 포트가 열립니다.

문제 해결

기술적인 문제가 있는 경우 디버그 로깅을 켜고 문제를 재현한 다음 이 로그를 Axis 지원 센터와 공유하십시오. Management Client 또는 Smart Client에서 디버그 로깅을 켤 수 있습니다.

Management Client에서:

1. **Site Navigation(사이트 탐색)** > **Basics(기본)** > **AXIS Optimizer**로 이동합니다.
2. **Turn on debug logging(디버그 로깅 켜기)**을 선택합니다.
3. **Save report(보고서 저장)**를 클릭하여 장치에 로그를 저장합니다.

Smart Client에서:

1. **Settings(설정)** > **Axis general options(Axis 일반 옵션)**로 이동합니다.
2. **Turn on debug logging(디버그 로깅 켜기)**을 선택합니다.
3. **Save report(보고서 저장)**를 클릭하여 장치에 로그를 저장합니다.

지원 센터 문의

추가 도움이 필요하면 *axis.com/support*로 이동하십시오.

팁과 요령

Smart Client 보기에서 웹 페이지 추가

AXIS Optimizer를 사용하면 html 페이지뿐만 아니라 거의 모든 웹 페이지를 Smart Client에 직접 표시할 수 있습니다. 이 웹 보기는 최신 브라우저 엔진으로 구동되며 대부분의 웹 페이지와 호환됩니다. 예를 들어 Smart Client에서 AXIS Body Worn Manager에 액세스하거나 실시간 보기 옆에 AXIS Store Reporter의 대시보드를 표시하려는 경우에 유용합니다.

1. Smart Client에서 **Setup(설정)**을 클릭합니다.
2. **Views(보기)**로 이동합니다.
3. 신규 보기를 생성하거나 기존 보기를 선택합니다.
4. **System overview > AXIS Optimizer(시스템 오버뷰 > AXIS Optimizer)**로 이동합니다.
5. **웹 보기(Web view)**를 클릭하고 보기에 드래그합니다.
6. 주소를 입력하고 **OK**를 클릭합니다.
7. **설정**을 클릭합니다.

내장된 검색 기능으로 비디오 내보내기

XProtect 형식으로 비디오 내보내기

AXIS Optimizer 검색 기능 및/또는 Axis 디워프 기능이 내장된 비디오를 보려면 비디오를 XProtect 형식으로 내보내야 합니다. 예를 들어 데모용으로 유용할 수 있습니다.

비고

AXIS Optimizer 5.3 이상 버전의 경우 3단계부터 시작하십시오.

1. Smart Client에서 **Settings(설정)** > **Axis search options(Axis 검색 옵션)**로 이동합니다.
2. **Include search plugins in exports(내보내기에 검색 플러그인 포함)**을 켭니다.
3. Smart Client에서 내보내기를 생성할 때 **XProtect format(XProtect 형식)**을 선택합니다.

수신 컴퓨터에서 내보내기 블럭 해제

다른 컴퓨터에서 내보내기를 성공적으로 사용하려면 내보내기 파일 아카이브를 블럭 해제해야 합니다.

1. 수신 컴퓨터에서 내보내기 파일(zip)을 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 선택합니다.
2. **General(일반)**에서 **Unblock(차단 해제)** > **OK(확인)**를 클릭합니다.
3. 내보내기를 추출하고 'SmartClient-Player.exe' 파일을 엽니다.

내보낸 Axis 디워프 보기 재생하기

1. 내보낸 프로젝트를 엽니다.
2. Axis 디워프 보기가 포함된 보기를 선택합니다.

T10134385_ko

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB