MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2023 R3

관리자 설명서

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

목차

Copyright, 상표 및 면책 조항 **26**

개요 **27**

새로운 기능 27

Management Client 2023 R3에서 27

로그인(설명됨) 29

로그인 인증(설명됨) 30

비보안 연결을 사용해 로그인 30

기본 사용자 암호 변경 30

제품 개요 32

시스템 구성 요소 32

관리 서버(설명됨) 32

SQL Server 설치 및 데이터베이스(설명됨) 32

레코딩 서버(설명됨) 33

모바일 서버(설명됨) 34

이벤트 서버(설명됨) 35

로그 서버(설명됨) 35

API Gateway (설명됨) 35

장애 조치 36

XProtect Management Server Failover 36

장애 조치 관리 서버(설명됨) 36

장애 조치 레코딩 서버(설명됨) 37

장애 조치 레코딩 서버 기능(설명됨) 38

장애 조치 단계(설명됨) 40

장애 조치 레코딩 서버 서비스(설명됨) 41

클라이언트 41

Management Client (설명됨) 41

XProtect Smart Client (설명됨) 42

XProtect Mobile 클라이언트(설명됨) 42

XProtect Web Client (설명됨) 43

XProtect 확장 44

XProtect Access (설명됨) 44
XProtect Incident Manager 45
XProtect LPR (설명됨) 46
XProtect Smart Wall (설명됨) 46
XProtect Transact (설명됨) 48
Milestone Open Network Bridge (설명됨) 48
XProtect DLNA Server (설명됨) 49
장치 49
하드웨어(설명됨) 49
하드웨어 사전 구성(설명됨) 50
장치(설명됨) 50
카메라 51
마이크 51
스피커 51
메타데이터 51
입력 51
출력 52
장치 그룹(설명됨) 52
미디어 저장소 53
저장 및 아카이빙(설명) 53
아카이브 구조(설명됨) 57
사전 버퍼링 및 레코딩 저장소(설명됨) 59
임시 사전 버퍼 레코딩 저장소 59
인증 59
Active Directory(설명됨) 59
사용자(설명됨) 59
Windows 사용자 60
기본 사용자 60
Identity Provider (설명됨) 61
외부 IDP(설명됨) 61
클레임(설명됨) 61
외부 IDP의 XProtect VMS에 대한 로그인 권한을 사용자에게 부여하기 61

URI 리디렉션 61
외부 IDP 사용자의 고유 사용자 이름 62
외부 IDP의 클레임 예시에서 확인하십시오. 62
클레임 일련 번호를 사용하여 XProtect 에서 사용자 이름 생성 62
XProtect 에서의 사용자 이름 생성을 위한 특정 클레임 정의 63
외부 IDP 사용자 삭제 63
보안 64
역할 및 역할의 권한(설명됨) 64
역할의 권한 64
사생활 보호(설명됨) 65
사생활 보호(설명됨) 65
Management Client 프로필(설명됨) 68
Smart Client 프로필(설명됨) 68
증거물 잠금(설명됨) 69
규칙 및 이벤트 70
규칙(설명됨) 70
규칙 복잡성 71
규칙 및 이벤트(설명됨) 72
시간 프로파일(설명됨) 74
주간 길이 시간 프로파일(설명됨) 74
알림 프로파일(설명됨) 75
알림 프로파일 생성 요구 사항 75
사용자 정의 이벤트(설명됨) 75
분석 이벤트(설명됨) 76
일반 이벤트(설명됨) 77
웹후크(설명됨) 77
알람 78
알람(설명됨) 78
알람 구성 79
스마트 맵 80
스마트 맵(설명됨) 80
스마트 맵과 Google Maps 통합(설명됨) 80

디지털 서명을 정적 맵 API 키에 추가 81
스마트 맵과 Bing Maps 통합(설명됨) 81
캐시된 스마트 맵 파일(설명됨) 81
아키텍처 82
배포형 시스템 설정 82
Milestone Interconnect (설명됨) 83
Milestone Interconnect 또는 Milestone Federated Architecture 선택(설명됨) 84
Milestone Interconnect 및 라이센싱 85
Milestone Interconnect 설치(설명됨) 85
Milestone Federated Architecture 구성하기 86
시스템에서 사용되는 포트 89
애플리케이션 풀 102
Milestone XProtect의 애플리케이션 풀 102
애플리케이션 풀 작업 103
애플리케이션 풀 페이지 열기 103
제품 비교 103
라이센싱 105
라이선스(설명됨) 105
자유 XProtect Essential+ 105
XProtect 비디오 관리 소프트웨어 제품을 위한 라이선스 (XProtect Essential+ 제외) 105
라이선스 유형 106
기본 라이선스 106
장치 라이선스 106
다음을 위한 카메라 라이선스: Milestone Interconnect™ 106
XProtect 확장의 라이선스 107
라이선스 활성화(설명됨) 107
자동 라이선스 활성화(설명됨) 107
라이선스 활성화 유예 기간(설명됨) 108
활성화 없이 장치 변경(설명됨) 108
활성화 없이 변경 가능한 장치의 수 계산(설명됨) 108
Milestone Care™ (설명됨) 109
라이선스 및 하드웨어 교체(설명됨) 110

라이선스에 관한 개요 받기 111
라이선스 활성화 111
자동 라이선스 활성화 111
자동 라이선스 활성화 사용 안 함 112
온라인으로 라이선스 활성화 112
오프라인으로 라이선스 활성화 112
유예 기간 후 라이선스 활성화 113
추가 라이선스 구입 113
소프트웨어 라이선스 코드 변경 113
관리 서버 트레이 아이콘에서 114
Management Client 에서 114
라이선스 정보 창 114
요구사항 및 고려사항 118
일광 절약 시간(설명됨) 118
시간 서버(설명됨) 118
데이터베이스 크기 제한 119
IPv6 및 IPv4(설명됨) 119
IPv6 주소 쓰기(설명됨) 121
URL에 IPv6 주소 사용 121
가상 서버 122
다중 관리 서버 정보(클러스터링)(설명됨) 122
클러스터링 요구 사항 122
레코딩 데이터베이스의 손상 보호 123
하드 디스크 장애: 드라이브 보호 123
Windows 작업 관리자: 프로세스를 종료할 때 주의하십시오 123
정전: UPS 사용 124
SQL Server 데이터베이스 트랜잭션 로그(설명됨) 124
최소 시스템 요구사항 124
설치를 시작하기 전에 124
서버와 네트워크 준비 125
Active Directory 준비 125
설치 방법 126

SQL Server 에디션에서 결정 ... 128
서비스 계정 선택 ... 129
Kerberos 인증(설명됨) ... 129
바이러스 검사 제외(설명됨) ... 131
XProtect VMS 을(를) FIPS 140-2 규격 모드에서 실행되도록 하려면 어떻게 해야 합니까? ... 132
FIPS가 활성화된 시스템에서 XProtect VMS 을(를) 설치하기 전 ... 133
소프트웨어 라이선스 코드 등록 ... 133
장치 드라이버(설명됨) ... 133
오프라인 설치를 위한 요구 사항 ... 134
보안 통신(설명됨) ... 134
설치 ... 135
신규 XProtect 시스템 설치 ... 135
XProtect Essential+ 설치 ... 135
시스템 설치 - 단일 컴퓨터 옵션 ... 139
시스템 설치 - 사용자 정의 옵션 ... 144
신규 XProtect 구성 요소 설치 ... 149
Download Manager 을(를) 통해 설치(설명됨) ... 149
Download Manager 을(를) 통해 Management Client 설치 ... 150
다음을 통해 레코딩 서버 설치: Download Manager ... 151
다음을 통해 장애 조치 레코딩 서버 설치: Download Manager ... 153
기본이 아닌 포트를 사용하여 XProtect VMS 설치 ... 155
명령줄 셸을 통해 자동 설치(설명됨) ... 155
레코딩 서버 자동 설치 ... 156
XProtect Smart Client 자동 설치 ... 157
로그 서버 자동 설치 ... 158
전용 서비스 계정을 사용하여 자동으로 설치 ... 159
전용 서비스 계정 사용 ... 160
예: 자동 모드로 설치를 시작하는 명령줄: ... 160
예: 전용 서비스 계정 사용을 기준으로 하는 인수 파일 ... 160
설치하기 전에 완료해야 할 사전 요구 사항: ... 162
작업 그룹에 대한 설치 ... 163
클러스터 내 설치 ... 163

클러스터 환경에서 외부 IDP를 위한 인증서 사용 166
외부 IDP 구성이 인증서로 보호되는 상황에서 문제 해결 167
Download Manager/다운로드 웹 페이지 168
Download Manager의 기본 구성 170
Download Manager의 표준 설치 관리자(사용자) 172
Download Manager 설치 프로그램 구성 요소 추가/게시 172
Download Manager 설치 프로그램 구성 요소 숨기기/제거 173
장치 팩 설치 관리자 - 반드시 다운로드 필요 174
설치 로그 파일 및 문제 해결 175
구성 176
초기 구성 작업 목록 176
레코딩 서버 177
레코딩 서버의 기본 구성 변경 또는 확인 177
레코딩 서버 등록 179
클라이언트에 대한 암호화 상태 보기 180
레코딩 저장소를 사용할 수 없을 때 행동 지정 181
새로운 저장소 추가 182
저장소 내에 아카이브 생성 183
저장소에 장치 또는 장치 그룹 연결 183
장치 비활성화됨 183
선택한 저장소 또는 아카이브의 설정 편집 184
내보내기 위해 디지털 서명 사용 184
레코딩 암호화 185
아카이브된 레코딩 백업 188
저장소에서 아카이브 삭제 189
저장소 삭제 189
저장소 내의 아카이브되지 않은 레코딩을 다른 저장소로 이동 190
장애 조치 레코딩 서버 할당 190
레코딩 서버에 대한 멀티캐스팅 활성화 191
개별 카메라의 멀티캐스팅 활성화 192
공용 주소 및 포트 정의 192
로컬 IP 범위 할당 193

장치 트리 필터링 193
장치 트리 필터링 193
필터 기준 특성 193
여러 필터 기준 지정 194
필터 재설정 194
장치 비활성화됨 194
장애 조치 서버 194
장애 조치 레코딩 서버 설치 및 활성화 194
수동 대기를 위한 장애 조치 레코딩 서버 그룹 195
장애 조치 레코딩 서버의 암호화 상태 보기 195
상태 메시지 보기 196
버전 정보 보기 196
하드웨어 197
하드웨어 추가 197
하드웨어 추가(대화) 197
하드웨어 비활성화 / 활성화 198
하드웨어 편집 199
하드웨어 수정(대화) 199
개별 장치 활성화 / 비활성화 202
하드웨어에 보안 연결 설정 202
비디오 인코더에서 PTZ 활성화 203
하드웨어 장치의 암호 변경 204
하드웨어 장치에서 펌웨어 업데이트 205
외부 IDP 추가 및 구성 207
장치 - 그룹 207
장치 그룹 추가 207
장치 그룹에 포함시킬 장치 지정 207
장치 비활성화됨 208
장치 그룹의 모든 장치에 대한 공통 속성 지정 208
장치 비활성화됨 208
장치 그룹을 통한 장치 활성화/비활성화 209
장치 - 카메라 설정 209

카메라 설정 보기 또는 편집 ... 209
미리보기 ... 210
성능 ... 210
하드웨어 추가 중 ... 210
어안 렌즈 지원 활성화 및 비활성화 ... 210
어안 렌즈 설정 지정 ... 210
장치 - 레코딩 ... 210
레코딩 활성화/비활성화 ... 210
관련 장치에서 레코딩 활성화 ... 211
수동 레코딩 관리 ... 211
역할에 추가: ... 211
규칙에 사용: ... 211
레코딩 프레임 속도 지정 ... 212
키프레임 레코딩 활성화 ... 212
관련 장치에서 레코딩 활성화 ... 212
원격 레코딩 저장 및 검색 ... 213
녹화 삭제 ... 213
장치 - 스트리밍 ... 214
적응 스트리밍(설명됨) ... 214
적응형 재생(설명됨) ... 214
가용성 ... 214
어댑티브 스트리밍 활성화 ... 214
원격 레코딩 ... 214
재생된 비디오의 해상도 ... 215
스트림 추가 ... 215
다중 스트림 관리 ... 216
레코딩에 사용할 스트림 변경하기 ... 216
데이터 송신 제한 ... 216
예시 ... 216
장치 - 저장소 ... 217
사전 버퍼링 관리 ... 217
사전 버퍼링 활성화 및 비활성화 ... 217

저장 위치와 사전 버퍼 기간 지정 218
규칙에서 사전 버퍼 사용 218
장치에 대한 데이터 베이스 상태 모니터링 218
한 저장소에서 다른 저장소로 장치 이동 220
장치 - 모션 감지 220
모션 감지(설명됨) 220
이미지 품질 220
사생활 보호 221
모션 감지 활성화 및 비활성화 221
카메라에 대한 동작 감지의 기본 설정 지정 221
특정 카메라에 대한 동작 감지 활성화 또는 비활성화 221
하드웨어 가속화 활성화 또는 비활성화 221
하드웨어 가속화 활성화 또는 비활성화하기 221
GPU 자원 이용 221
로드 밸런싱 및 성능 222
수동 감도를 활성화하여 동작 정의 222
모션 정의를 위한 임계값 지정 223
모션 감지에 대한 제외 영역 지정 223
장치 - 프리셋 카메라 위치 224
홈 사전 설정 위치 224
프리셋 위치(유형 1) 추가 224
카메라의 프리셋 위치 사용(유형 2) 226
카메라의 기본 프리셋 위치를 기본으로 할당 226
기본 사전 설정을 PTZ 홈 위치로 지정 227
PTZ 홈 위치 설정 활성화 227
카메라에 대한 프리셋 위치 편집(유형 1만 해당) 227
카메라에 대한 프리셋 위치 이름 변경(유형 2만 해당) 229
프리셋 위치 테스트(유형 1만 해당) 229
장치 - 순찰 230
순찰 프로파일 및 수동 순찰(설명됨) 230
수동 순찰 230
순찰 프로파일 추가 230

순찰 프로파일에 프리셋 위치 지정 ... 231
각 프리셋 위치에서 시간 지정 ... 231
전환 사용자 정의(PTZ) ... 232
순찰 시 종료 위치 지정 ... 233
PTZ 세션 보존 및 해제 ... 233
PTZ 세션 보존 ... 234
PTZ 세션 해제 ... 234
PTZ 세션 시간 제한 지정 ... 234
장치 - 규칙에 대한 이벤트 ... 235
장치에 대한 이벤트 추가 또는 삭제 ... 235
이벤트 추가 ... 235
이벤트 삭제 ... 235
이벤트 속성을 지정합니다. ... 235
이벤트의 여러 인스턴스 사용 ... 235
장치 - 사생활 보호 ... 236
사생활 보호 활성화/비활성화 ... 236
사생활 보호 정의 ... 236
해제된 사생활 보호의 제한 시간 변경 ... 238
사용자에게 사생활 보호 해제 권한 부여 ... 239
사생활 보호 구성에 대한 보고서 생성 ... 239
클라이언트 ... 240
뷰 그룹(설명됨) ... 240
뷰 그룹 추가 ... 241
Smart Client profiles ... 241
Smart Client 프로파일 추가 및 구성 ... 241
Smart Client 프로파일 복사 ... 242
Smart Client 프로필과 역할, 시간 프로필 생성 및 설정 ... 242
검색 중 허용된 카메라의 수 설정 ... 243
기본 내보내기 설정 변경 ... 247
Management Client profiles ... 248
Management Client 프로파일 추가 및 구성 ... 248
Management Client 프로파일 복사 ... 249

Management Client 프로파일에 대한 기능 표시 관리 ... 249
역할과 Management Client 프로파일 연결 ... 249
역할에 대한 전반적인 시스템 기능 액세스 관리 ... 249
프로파일에 대한 기능 표시 제한 ... 250
Matrix ... 250
Matrix 및 Matrix 수신자(설명됨) ... 250
Matrix 수신자에게 비디오를 전송하는 규칙 정의 ... 250
Matrix 수신자 추가 ... 251
동일 비디오를 여러 XProtect Smart Client 뷰로 전송 ... 251
규칙 및 이벤트 ... 251
규칙 추가 ... 251
이벤트 ... 251
동작 및 중지 동작 ... 252
규칙 만들기 ... 252
규칙 유효성 검증 ... 253
규칙 유효성 검증 ... 254
모든 규칙 유효성 검증 ... 254
규칙 편집, 복사 및 이름 바꾸기 ... 254
규칙 비활성화 및 활성화 ... 255
시간 프로파일 지정 ... 255
단일 시간 추가 ... 255
반복 시간 추가 ... 256
반복 시간 ... 257
시간 프로파일 편집 ... 257
낮 길이 시간 프로파일 만들기 ... 257
하루 길이 시간 프로파일 속성 ... 258
알림 프로파일 추가 ... 258
규칙에서 이메일 알림 트리거하기 ... 260
사용자 정의 이벤트 추가 ... 260
사용자 정의 이벤트 이름 변경 ... 261
분석 이벤트 추가 및 편집 ... 261
분석 이벤트 추가 ... 261

분석 이벤트 편집 261
분석 이벤트 설정 편집 261
분석 이벤트 테스트 261
일반 이벤트 추가 262
일반 이벤트를 추가하려면: 262
인증 263
외부 IDP의 클레임 등록 263
XProtect에서 외부 IDP의 클레임을 역할에 매핑하기 263
외부 IDP를 통한 로그인 263
보안 264
역할 추가 및 관리 264
역할 복사, 이름 바꾸기 또는 삭제 264
역할 복사 264
역할 이름 바꾸기 264
역할 삭제 265
유효 역할 보기 265
역할에 사용자 및 그룹 할당/제거 265
역할에 Windows 사용자 및 그룹 할당 265
역할에 기본 사용자 할당 266
역할에서 사용자 및 그룹 제거 266
기본 사용자 만들기 266
기본 사용자에 대한 로그인 설정 구성 266
시스템에서 기본 사용자를 만들려면: 267
클라이언트에 대한 암호화 상태 보기 268
시스템 대시보드 269
레코딩 서버 상의 현재 진행 중인 작업 보기 269
시스템 모니터(설명됨) 269
시스템 모니터 대시보드(설명됨) 269
시스템 모니터 임계치(설명됨) 270
하드웨어의 현재 상태를 조회하고 필요한 경우 문제를 해결합니다 270
하드웨어의 이력 상태를 조회하고 보고서를 출력합니다 271
하드웨어 상태의 이력 데이터 수집 272

시스템 모니터 대시보드에서 새 카메라 또는 서버 타일 추가 272
시스템 모니터 대시보드에서 카메라 또는 서버 타일 편집 272
시스템 모니터 대시보드에서 카메라 또는 서버 타일 삭제 273
하드웨어 상태가 변경되어야 할 때에 대한 임계값 편집 273
시스템 내 증거물 잠금 보기 274
시스템 구성이 포함된 보고서 출력 274
메타데이터 274
메타데이터 검색 카테고리 및 검색 필터 표시 또는 숨기기 274
알람 275
알람 추가 275
개별 알람 정의에 대한 권한 수정 276
암호화 활성화 277
관리 서버로 및 관리서버로부터 암호화 활성화 277
레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화 278
이벤트 서버 암호화 활성화 280
클라이언트 및 서비스에 암호화 활성화 281
모바일 서버 암호화를 활성화합니다 283
Milestone Federated Architecture 284
연합 사이트 실행을 위한 시스템 설정 284
계층 구조에 사이트 추가 286
계층에 포함 허용 286
사이트 속성 설정 287
사이트 계층 새로 고침 288
계층 구조의 다른 사이트에 로그인합니다. 288
하위 사이트의 사이트 정보 업데이트 288
계층에서 사이트 분리 289
Milestone Interconnect 289
중앙 Milestone Interconnect 사이트에 원격 사이트 추가 289
사용자 권한 할당 290
원격 사이트 하드웨어 업데이트 290
원격 사이트 카메라에서 직접 재생 활성화 290
원격 사이트 카메라에서 원격 레코딩 검색 291

원격 사이트의 이벤트에 응답하도록 중앙 사이트 구성 ... 291
원격 연결 서비스 ... 293
원격 연결 서비스(설명됨) ... 293
One-Click 카메라 연결에 대한 보안 터널 서버 환경 설치 ... 293
보안 터널 서버 추가 또는 편집 ... 294
신규 Axis One-Click 카메라 등록 ... 294
스마트 맵 ... 294
지리적 배경(설명됨) ... 294
Bing Maps 또는 Google Maps를 다음에서 활성화: Management Client ... 296
Bing Maps 또는 Google Maps를 다음에서 활성화: XProtect Smart Client ... 296
Milestone Map Service 활성화 ... 296
OpenStreetMap 타일 서버 지정 ... 297
스마트 맵 편집 활성화 ... 298
스마트 맵상의 장치 편집 활성화 ... 299
장치 위치 및 카메라 방향, 시계, 깊이(스마트 맵) 정의 ... 300
스마트 맵을 Milestone Federated Architecture 와(과) 함께 구성 ... 302
유지관리 ... **304**
시스템 구성 백업 및 복원 ... 304
시스템 구성 백업 및 복원(설명됨) ... 304
공유 백업 폴더 선택 ... 304
수동으로 시스템 구성 백업 ... 305
수동 백업에서 시스템 구성 복원 ... 305
시스템 구성 암호(설명됨) ... 306
시스템 구성 암호 설정 ... 306
시스템 구성 암호 설정 변경 ... 307
시스템 구성 암호 설정 입력(복원) ... 308
수동으로 시스템 구성 백업(설명됨) ... 308
이벤트 서버 구성 백업 및 복원(설명됨) ... 309
시스템 구성의 백업 및 복원 예약(설명됨) ... 309
예약 백업을 사용하여 시스템 구성 백업 ... 309
예약 백업에서 시스템 구성 복원 ... 310
로그 서버의 데이터베이스 백업 ... 311

실패 및 문제 시나리오 백업 및 복원(설명됨) ... 311
관리 서버 이동 ... 311
이용 불가능한 관리 서버(설명됨) ... 312
시스템 구성 이동 ... 312
레코딩 서버 교체 ... 313
하드웨어 이동 ... 314
하드웨어 이동(마법사) ... 315
하드웨어 교체 ... 317
하드웨어 데이터 업데이트 ... 320
SQL Server 데이터베이스의 위치 및 이름 변경 ... 321
서버 서비스 관리 ... 322
서버 관리자 트레이 아이콘(설명됨) ... 322
Management Server 서비스 시작 또는 중지 ... 324
Recording Server 서비스 시작 또는 중지 ... 325
관리 서버 또는 레코딩 서버에 대한 상태 메시지 보기 ... 326
다음을 사용한 암호화 관리: Server Configurator ... 326
Event Server 서비스 시작, 중지 또는 재시작 ... 326
Event Server 서비스 중지 ... 327
Event Server 또는 MIP 로그 보기 ... 327
현재 시스템 구성 암호 입력 ... 329
등록된 서비스 관리 ... 329
등록된 서비스 추가 및 편집 ... 330
네트워크 구성 관리 ... 330
등록된 서비스 속성 ... 330
장치 드라이버 제거(설명됨) ... 331
레코딩 서버 제거 ... 331
레코딩 서버에서 모든 하드웨어 삭제 ... 332
관리 서버 컴퓨터의 호스트 이름 변경 ... 332
인증서의 유효성 ... 332
등록된 서비스에 대한 고객 데이터 속성 손실 ... 332
Milestone Customer Dashboard 에서, 호스트 이름은 변경되지 않은 것으로 표시됩니다 ... 333
호스트 이름을 변경하면 SQL Server 주소도 변경됩니다 ... 333

다음에서의 호스트 이름 변경: Milestone Federated Architecture 333
사이트의 호스트는 아키텍처의 루트 노드입니다 333
사이트의 호스트는 아키텍처의 하위 노드입니다 333
서버 로그 관리 334
사용자 활동, 이벤트, 동작 및 오류 식별 334
로그 필터 335
로그 내보내기 336
로그 검색 337
로그 언어 변경 337
로그를 작성하려면 2018 R2 및 조기 구성 요소를 허용하십시오 338
문제 해결 339
디버깅 로그(설명됨) 339
문제: SQL Server 및 데이터베이스 위치 변경으로 인한 데이터베이스 액세스 불가 339
문제: 포트 충돌로 인한 레코딩 서버 시작 실패 339
문제: Recording Server 이(가) Management Server 클러스터 노드로 변경 시 오프라인이 됩니다. 341
문제: 하위 노드에 연결할 수 없는 Milestone Federated Architecture 설정의 상위 노드 341
상위 노드와 사이트 간 연결을 재설정하기 342
문제: Azure SQL 데이터베이스 서비스를 사용할 수 없음 342
업그레이드 343
업그레이드(설명됨) 343
업그레이드 요구 사항 344
FIPS 140-2 규격 모드에서의 실행을 위한 XProtect VMS 업그레이드 344
권장 업그레이드 방식 346
클러스터에서 업그레이드 348
사용자 인터페이스 상세 내용 349
메인 창 349
창 레이아웃 351
시스템 설정(옵션 대화 상자) 353
일반 탭(옵션) 353
서버 로그 탭(옵션) 356
Mail Server 탭(옵션) 356
AVI 생성 탭(옵션) 357

네트워크 탭(옵션) 358
북마크 탭(옵션) 358
사용자 설정 탭(옵션) 359
외부 IDP 탭(옵션) 359
외부 IDP 구성 360
클레임 등록 361
웹 클라이언트용 리디렉션 URI 추가 361
고객 대시보드 탭(옵션) 362
증거물 잠금 탭(옵션) 362
오디오 메시지 탭(옵션) 363
사생활 보호 설정 탭 363
액세스 제어 설정 탭(옵션) 364
분석 이벤트 탭(옵션) 364
알람 및 이벤트 탭(옵션) 365
일반 이벤트 탭(옵션) 366
구성 요소 메뉴 368
Management Client 메뉴 368
파일 메뉴 368
편집 메뉴 368
뷰 메뉴 369
동작 메뉴 369
도구 메뉴 369
도움말 메뉴 370
Server Configurator (유틸리티) 370
암호화 탭 속성 370
서버 등록 371
언어 선택 372
트레이 아이콘 상태 372
트레이 아이콘의 서비스 시작 및 정지 374
Management Server Manager(트레이 아이콘) 374
기본 노드 375
라이선스 정보(기본 노드) 375

사이트 정보(기본 노드) 376
원격 연결 서비스 노드 376
Axis One-click 카메라 연결(원격 연결 서비스 노드) 376
서버 노드 377
서버(노드) 377
레코딩 서버(서버 노드) 377
레코딩 서버 설정 창 378
레코딩 서버 속송 379
저장소 탭(레코딩 서버) 381
장애 조치 탭(레코딩 서버) 385
멀티캐스트 탭(레코딩 서버) 387
네트워크 탭(레코딩 서버) 389
장애 조치 서버(서버 노드) 390
정보 탭 속성(장애 조치 서버) 391
멀티캐스트 탭(장애 조치 서버) 393
정보 탭 속성(장애 조치 그룹) 393
시퀀스 탭 속성(장애 조치 그룹) 394
Milestone Interconnect에 대한 원격 서버 394
정보 탭(원격 서버) 394
설정 탭(원격 서버) 395
이벤트 탭(원격 서버) 395
원격 검색 탭 395
장치 노드 396
장치(장치 노드) 396
장치의 상태 아이콘 397
카메라(장치 노드) 398
마이크(장치 노드) 398
스피커(장치 노드) 398
메타데이터(장치 노드) 399
입력(장치 노드) 399
출력(장치 노드) 399
장치 탭 400

정보 탭(장치) 400
정보 탭 속성 401
설정 탭(장치) 402
스트림 탭(장치) 403
스트림 랩 상의 작업 404
레코드 탭(장치) 404
녹화 탭 상의 작업 406
모션 탭(장치) 406
모션 탭 상의 작업 407
프리셋 탭(장치) 409
프리셋 탭 상의 작업 411
PTZ 세션 속성 412
순찰 탭(장치) 413
순찰 탭 상의 작업 414
수동 순찰 속성 415
어안 렌즈 탭(장치) 416
어안 렌즈 탭 상의 작업 416
이벤트 탭(장치) 416
이벤트 탭 상의 작업 417
이벤트 탭(속성) 417
클라이언트 탭(장치) 417
클라이언트 탭 속성 418
사생활 보호 탭(장치) 420
사생활 보호 탭 상의 작업 421
사생활 보호와 관련된 작업 421
사생활 보호 탭(속성) 421
하드웨어 속성 창 423
정보 탭(하드웨어) 423
설정 탭(하드웨어) 424
PTZ 탭(비디오 인코더) 424
클라이언트 노드 425
클라이언트(노드) 425

Smart Wall (클라이언트 노드) 425
Smart Wall 속성 425
모니터 속성 427
Smart Client 프로파일(클라이언트 노드) 428
정보 탭(Smart Client 프로필) 428
일반 탭(Smart Client 프로필) 429
고급 탭(Smart Client 프로파일) 429
라이브 탭(Smart Client 프로필) 430
재생 탭(Smart Client 프로필) 430
설정 탭(Smart Client 프로필) 431
내보내기 탭(Smart Client 프로필) 431
타임라인 탭 (Smart Client 프로필) 431
액세스 제어 탭(Smart Client 프로필) 431
알람 관리자 탭(Smart Client 프로필) 432
스마트 맵 탭(Smart Client 프로필) 432
Management Client 프로파일(클라이언트 노드) 433
정보 탭(Management Client 프로필) 433
프로필 탭(Management Client 프로필) 434
탐색 434
세부 정보 435
도구 메뉴 435
연합 사이트 436
규칙 및 이벤트 노드 436
규칙(규칙 및 이벤트 노드) 436
기본 규칙 재생성 437
알림 프로파일(규칙 및 이벤트 노드) 438
이벤트 개요 440
하드웨어: 440
하드웨어 - 구성 가능한 이벤트: 440
하드웨어 - 사전 정의된 이벤트: 440
장치 - 구성 가능한 이벤트: 441
장치 - 사전 정의된 이벤트: 441

외부 이벤트 - 사전 정의된 이벤트: 444
외부 이벤트 - 일반 이벤트: 444
외부 이벤트 - 사용자 정의 이벤트: 444
레코딩 서버: 445
시스템 모니터 이벤트 446
시스템 모니터 - 서버: 446
시스템 모니터 - 카메라: 448
시스템 모니터 - 디스크: 448
시스템 모니터 - 저장소: 449
기타: 449
XProtect 확장 및 통합의 이벤트: 449
동작 및 중지 동작 449
규칙 마법사 관리 450
테스트 분석 이벤트(속성) 459
일반 이벤트 및 데이터 소스(속성) 461
일반 이벤트(속성) 461
웹후크(규칙 및 이벤트 노드) 462
보안 노드 463
역할(보안 노드) 463
정보 탭(역할) 463
사용자 및 그룹 탭(역할) 465
외부 IDP(역할) 465
전체 보안 탭(역할) 465
장치 탭(역할) 491
카메라 관련 권한 492
마이크 관련 권한 494
스피커 관련 권한 497
메타데이터 관련 권한 499
입력 관련 권한 501
출력 관련 권한 501
PTZ 탭(역할) 501
음성 탭(역할) 503

원격 녹화 탭(역할) 503
Smart Wall 탭(역할) 503
외부 이벤트 탭(역할) 504
뷰 그룹 탭(역할) 504
서버 탭(역할) 505
Matrix 탭(역할) 505
알람 탭(역할) 505
액세스 제어 탭(역할) 506
LPR 탭(역할) 507
인시던트 탭(역할) 507
MIP 탭(역할) 508
기본 사용자(보안 노드) 508
시스템 대시보드 노드 508
시스템 대시보드 노드 508
현재 작업(시스템 대시보드 노드) 509
시스템 모니터(시스템 대시보드 노드) 509
시스템 모니터 대시보드 창 509
타일 509
모니터링 매개변수를 포함하는 하드웨어 목록 509
대시보드 창 사용자 정의 509
상세 내용 창 510
시스템 모니터 임계값(시스템 대시보드 노드) 511
증거물 잠금(시스템 대시보드 노드) 514
구성 보고서(시스템 대시보드 노드) 514
서버 로그 노드 515
서버 로그 노드 515
시스템 로그(탭) 515
감사 로그(탭) 516
규칙 트리거 로그(탭) 516
메타데이터 사용 노드 517
메타데이서 및 메타데이터 검색 517
메타데이터란 무엇입니까? 517

메타 데이터 검색 517
메타데이터 검색 요건 517
액세스 제어 노드 518
액세스 제어 속성 518
일반 설정 탭(액세스 제어) 518
도어 및 연결된 카메라 탭(액세스 제어) 519
액세스 제어 이벤트 탭(액세스 제어) 519
액세스 요청 알림 탭(액세스 제어) 521
카드 소유자 탭(액세스 제어) 521
사건 노드 522
사건 속성(사건 노드) 522
트랜잭트 노드 523
트랜잭션 소스(트랜잭션 노드) 523
트랜잭션 소스(속성) 523
트랜잭션 정의(트랜잭션 노드) 524
트랜잭션 정의(속성) 525
알람 노드 527
알람 정의(알람 노드) 527
알람 정의 설정: 527
알람 트리거: 528
운영자 동작 필요: 528
맵: 528
기타: 529
알람 데이터 설정(알람 노드) 529
알람 데이터 수준 탭 529
상태 530
닫는 이유 탭 531
사운드 설정(알람 노드) 531
연합 사이트 계층 532
연합 사이트 속성 532
일반 탭 532
상위 사이트 탭 532

Copyright, 상표 및 면책 조항

Copyright © 2023 Milestone Systems A/S

상표

XProtect 는 Milestone Systems A/S 의 등록 상표입니다.

Microsoft 및 Windows는 Microsoft Corporation의 등록 상표입니다. App Store는 Apple Inc.의 서비스 마크입니다. Android는 Google Inc.의 상표입니다.

이 문서에 언급된 기타 모든 상표는 해당 소유자의 상표입니다.

면책

이 텍스트는 일반적인 정보용으로만 사용되며 준비하는 동안 합당한 주의를 기울였습니다.

이 정보를 사용함으로써 발생하는 모든 위험은 사용자에게 귀속되며 여기에 있는 어떠한 내용도 보증으로 해석하지 않아야 합니다.

Milestone Systems A/S 에서는 사전 통지 없이 수정할 권한을 보유합니다.

이 텍스트의 용례에 사용된 모든 인명과 조직명은 실제가 아닙니다. 실제 조직 이름이나 생존 또는 사망한 사람의 이름과 유사한 경우 이는 전적으로 우연의 일치이며 의도된 것이 아닙니다.

이 제품은 특정 약관이 적용될 수 있는 타사 소프트웨어가 사용될 수 있습니다. 이 경우에 해당할 때, Milestone 시스템 설치 폴더에 있는 `3rd_party_software_terms_and_conditions.txt` 파일에서 자세한 정보를 확인할 수 있습니다.

개요

새로운 기능

Management Client 2023 R3에서

XProtect Management Client

이제 인증에 Azure Active Directory를 사용할 수 있습니다. 설치 시 통합 보안에 대해 **Windows 인증**과 **Azure Active Directory 통합** 중에 선택할 수 있습니다.

Azure 통합 보안을 사용하여 XProtect을(를) 설치하는 방법에 대한 자세한 내용은 페이지 144의 시스템 설치 - 사용자 정의 옵션을(를) 참조하십시오.

XProtect Management Client

이제 Windows 인증 및 Azure Active Directory 통합에 (서버 인증서 신뢰 안 함) 옵션을 사용할 수 있습니다. Azure Active Directory 통합의 경우 이 옵션은 필수입니다. (서버 인증서 신뢰 안 함) 옵션을 사용하면 설치 전에 서버 인증서의 유효성을 검사하고 확인할 수 있습니다.

XProtect Management Client:

알람에 대한 새로운 **알람 설정 편집** 사용자 권한이 도입되어 관리자가 알람 정의, 알람 상태, 알람 카테고리, 알람 소리, 알람 보존, 이벤트 보존을 편집할 수 있습니다. 알람 정의에 대한 해당 편집 권한이 기존 **관리** 사용자 권한에서 제거되었으며, 관리자가 알림 설정을 관리하려면 두 가지 사용자 권한(**알람 설정 편집** 및 **관리**)이 모두 필요합니다.

새로운 **알람 설정 편집** 사용자 권한은 기존 사용자에게 적용되지 않으며, 설치 또는 업그레이드 후 알람을 구성할 수 있도록 관리자 수준의 액세스가 필요한 사용자에게 수동으로 할당되어야 합니다.

사용자 정의 설치에 대한 자세한 내용은 페이지 463의 역할(보안 노드)을(를) 참조하십시오.

Management Client 2023 R2

XProtect Management Client:

이제 적응형 스트리밍을 재생 모드에서 사용하도록 구성할 수 있습니다. 이 방법을 적응형 재생이라고 합니다. 자세한 정보는 페이지 214의 적응형 재생(설명됨)를 참조하십시오.

XProtect Management Client:

XProtect 구성 요소를 설치할 때 사용자 지정 설치의 일부로 사전 생성된 데이터베이스를 사용하도록 선택할 수 있습니다. 사용자 정의 설치에 대한 자세한 내용은 페이지 144의 시스템 설치 - 사용자 정의 옵션을(를) 참조하십시오.

XProtect Management Client:

비디오 제한에 대한 새로운 사용자 권한이 도입되어 관리자가 생성, 보기, 편집, 삭제 권리를 구성하고 사용자에게 할당할 수 있습니다. 자세한 정보는 페이지 463의 역할(보안 노드)을(를) 참조하십시오.

Management Client 2023 R1

XProtect Incident Manager:

- 이제 개인 데이터에 관한 GDPR 또는 기타 해당 법률 준수를 위해 XProtect Management Client의 관리자는 사건 프로젝트의 보존 기간을 정의할 수 있습니다.

Management Client 2022 R3

XProtect Incident Manager:

- XProtect Incident Manager 확장은 이제 XProtect Expert, XProtect Professional+, XProtect Express+ 2022 R3 이상 버전과도 호환됩니다.
- 이제 XProtect Incident Manager은(는) 10,000개 이상의 사건 프로젝트를 표시할 수 있습니다.

Management Client 2022 R2에서

XProtect Incident Manager:

- 이 확장의 첫 번째 버전
- XProtect Incident Manager 확장은 XProtect Corporate 버전 2022 R2 이상 및 XProtect Smart Client 버전 2022 R2 이상과 호환됩니다.

XProtect LPR:

- 국가 모듈의 일부인 자동차 번호판 형식이 이제 한 곳에 나열됩니다. 를 참조하십시오
- 자동차 번호판 형식을 보다 쉽게 관리할 수 있도록 번호판 인식 요구에 따라 별칭으로 그룹화할 수 있습니다. 를 참조하십시오
- 이제 자동차번호판 일치 목록이 별칭을 지원합니다. 를 참조하십시오

Management Client 2022 R1에서

이벤트 서버 암호화:

- 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간에 쌍방향으로 암호화를 할 수 있습니다.

  자세한 정보는 페이지 280의 이벤트 서버 암호화 활성화를 참조하십시오.

외부 IDP를 통한 로그온:

- 이제 외부 IDP를 사용하여 Milestone XProtect VMS 에 로그온할 수 있습니다. 외부 IDP를 통한 로그온은 Active Directory 사용자 또는 기본 사용자 로그온 대신에 사용할 수 있습니다. 외부 IDP 로그온 방식으로 사용자는 기본 사용자에 대한 설정 요건을 우회할 수 있으며 여전히 XProtect 의 구성 요소와 장치 액세스를 위한 승인을 받을 수 있습니다.

  자세한 정보는 외부 IDP(설명됨) 을 참조하십시오.

하드웨어 데이터 업데이트

- 이제 Management Client의 시스템이 감지한 하드웨어 장치의 현재 펌웨어 버전을 볼 수 있습니다.

  자세한 정보는 페이지 320의 하드웨어 데이터 업데이트를 참조하십시오.

XProtect Management Server Failover

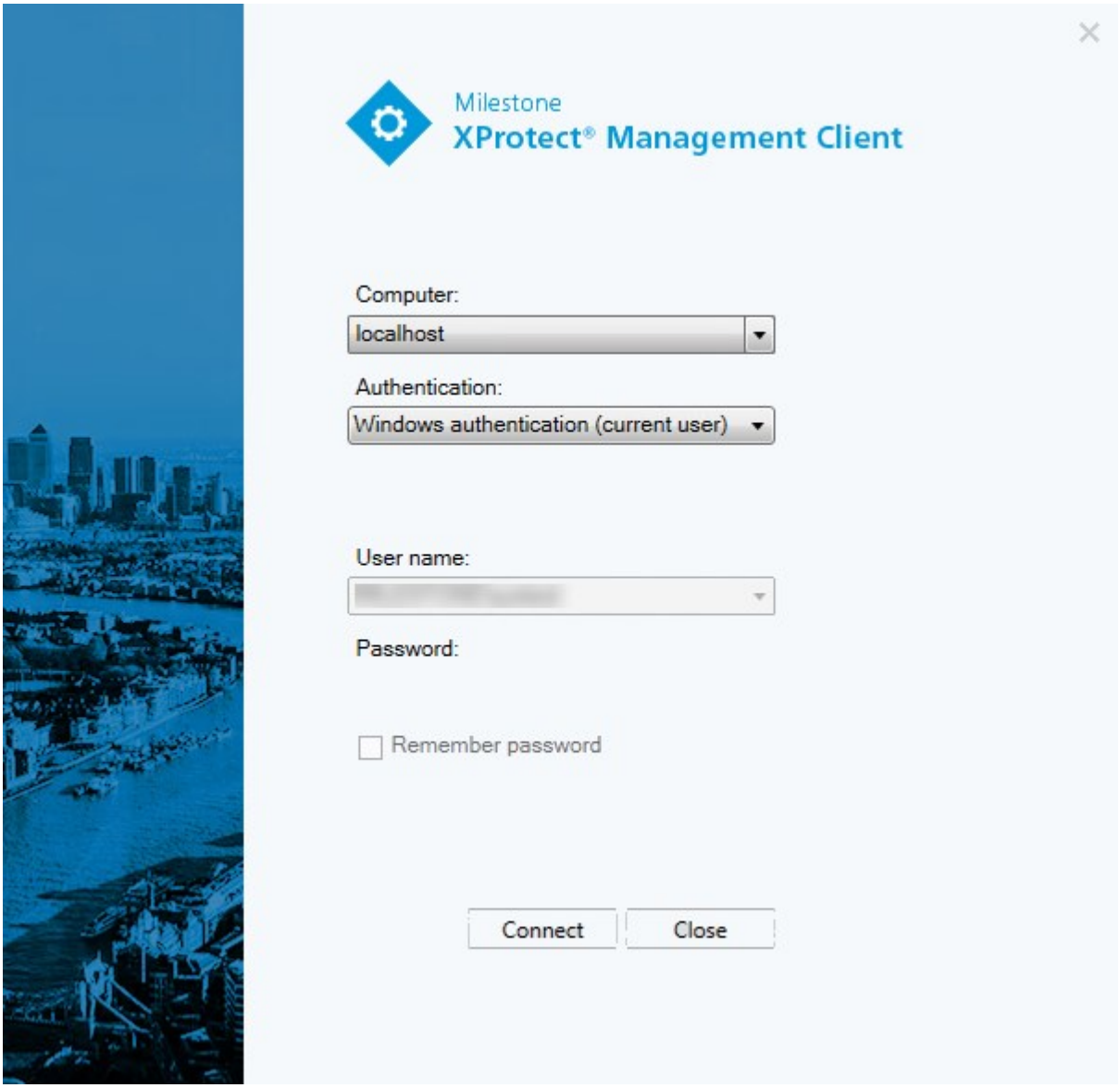
- 이제 2개의 중복 컴퓨터 간에 장애 조치 관리 서버를 구성하여 시스템의 고가용성을 달성할 수 있습니다. 관리 서버를 구동하는 컴퓨터가 장애를 일으키면 두 번째 컴퓨터가 역할을 대신합니다. 실시간 데이터 복제로 관리 서버와 로그 서버, 이벤트 서버의 데이터베이스가 두 컴퓨터에서 동일하게 유지됩니다.

  자세한 정보는 페이지 36의 XProtect Management Server Failover 를 참조하십시오.

로그인(설명됨)

Management Client 를 실행할 때는 시스템에 연결하기 위해 우선 로그인 정보를 입력해야 합니다.

XProtect Corporate 2016 또는 XProtect Expert 2016 이나 새로 설치된 버전으로 패치를 설치한 후 오래된 버전의 제품을 구동하는 시스템에 로그인을 할 수 있습니다. 지원되는 버전은 XProtect Corporate 2013 및 XProtect Expert 2013 이상입니다.



로그인 인증(설명됨)

시스템에서 관리자는 충분한 권한을 가진 두 번째 사용자가 로그인을 승인하는 경우에만 시스템에 로그인이 가능하도록 사용자를 설정할 수 있습니다. 이 경우, XProtect Smart Client 또는 Management Client 이(가) 로그인 과정에서 두 번째 인증을 요청합니다.

기본 제공 **관리자** 역할과 연결된 사용자는 항상 인증 권한을 가지므로 두 번째 로그인이 요청되지 않지만, 이 사용자가 두 번째 로그인을 요청하는 다른 역할과 연결된 경우는 예외입니다.

외부 IDP를 통해 로그인하는 사용자는 두 번째 사용자가 승인해야 하는 요구 사항을 설정할 수 없습니다.

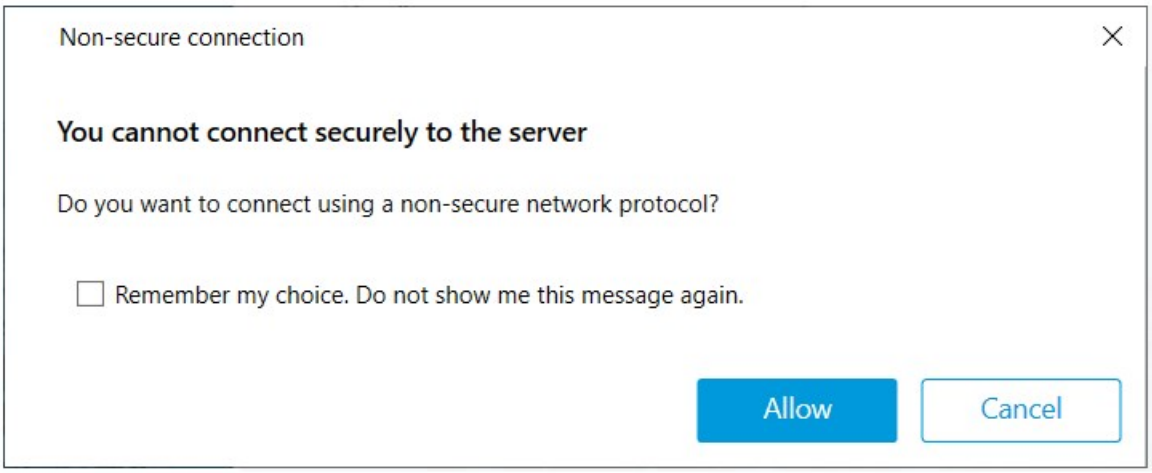
로그인 인증을 역할과 연결시키려면:

- **역할** 아래 **정보** 탭에서 선택된 역할에 대해 **필요한 로그인 승인** 을 설정하여(역할 설정) 해당 사용자에게 로그인 시 추가 승인이 요청되도록 합니다.
- **역할** 아래 **전체 보안** 탭에서 선택된 역할에 대해 **사용자 승인** 을 설정하여(역할 설정 참조) 해당 사용자가 다른 사용자의 로그인을 승인할 수 있게 합니다.

동일 사용자에 대해 두 옵션을 모두 선택할 수 있습니다. 즉, 사용자가 로그인 과정에서 추가 인증 요구를 받지만 자신을 제외하고 다른 사용자의 로그인을 인증할 수도 있습니다.

비보안 연결을 사용해 로그인

Management Client에 로그인할 때 비보안 네트워크 프로토콜을 사용하여 로그인할지 묻는 메시지가 표시될 수 있습니다.



- 알림을 무시하고 로그인하려면 **허용**을 클릭합니다. 앞으로 이 알림을 받지 않으려면 **내 선택 기억을 선택합니다. 이 메시지를 다시 표시하지 않거나 도구** > **옵션** 을 클릭한 다음, **서버에 대한 비보안 연결 허용(Management Client를 다시 시작해야 함)**을 선택합니다.

보안 통신에 관한 자세한 정보는 페이지 134의 보안 통신(설명됨) 을(를) 참조하십시오.

기본 사용자 암호 변경

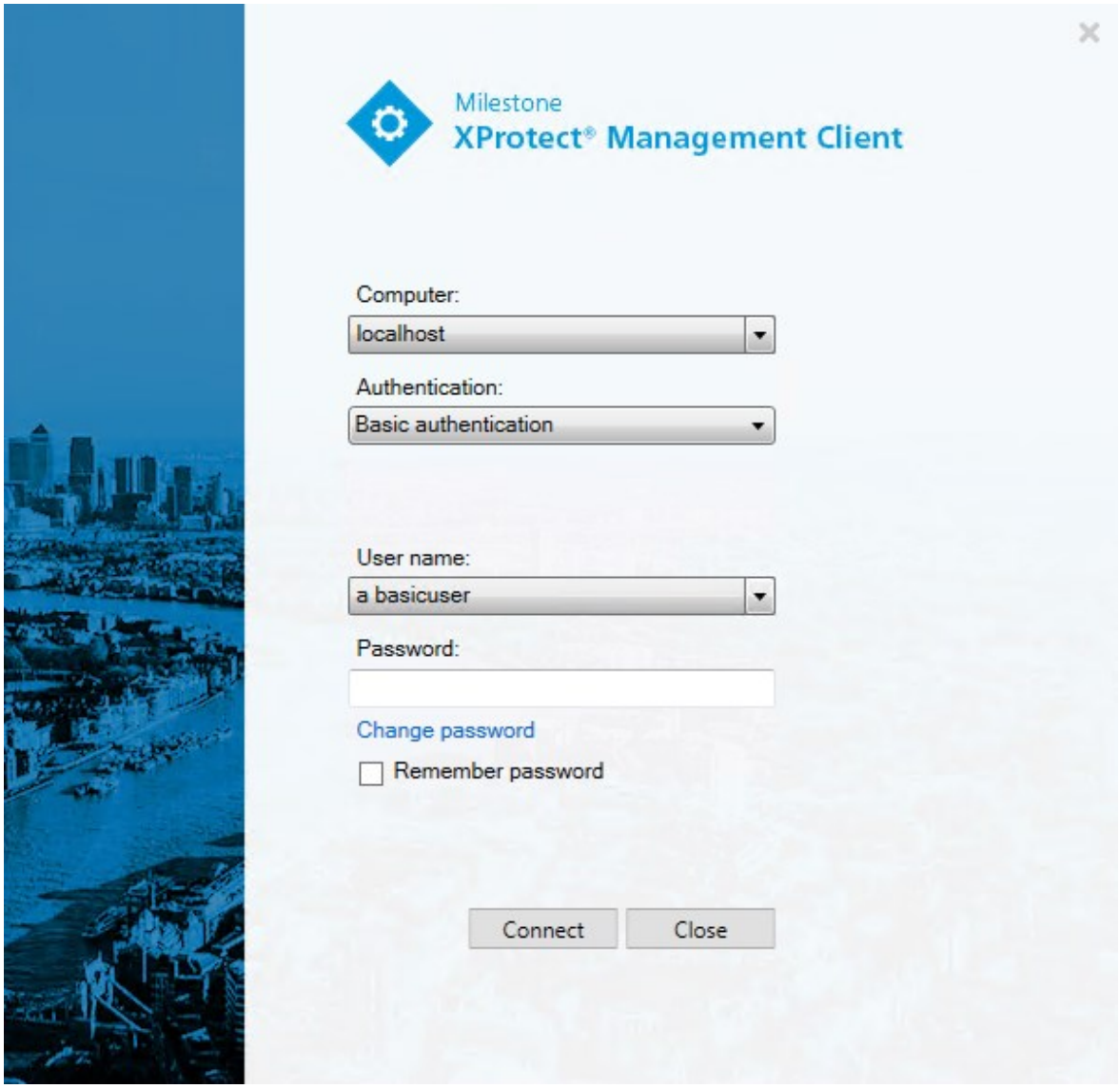
기본 사용자 로 로그인하는 경우, 사용자는 암호를 변경할 수 있습니다. 다른 인증 방식을 선택하는 경우, 시스템 관리자만 암호를 변경할 수 있습니다. 암호 변경은 종종 XProtect VMS 시스템의 보안성을 높여줍니다.

요구사항

XProtect VMS 시스템의 버전이 2021 R1 또는 이후 버전이어야 합니다.

단계:

1. Management Client 을(를) 시작합니다. 로그인 창이 열립니다.
2. 로그인 정보를 지정합니다. **인증** 목록에서 **기본 인증** 을 선택합니다. 텍스트가 포함된 링크 **암호 변경** 이 표시됩니다.



3. 링크를 클릭합니다. 브라우저 창이 열립니다.
4. 지시를 따라 변경 사항을 저장합니다.
5. 이제 새 암호를 사용하여 Management Client 에 로그인할 수 있습니다.

제품 개요

XProtect VMS 제품은 모든 형태와 크기의 설치를 위해 설계된 비디오 관리 소프트웨어입니다. 상점을 반달리즘으로부터 보호하거나 여러 사이트의 경비가 철저한 시설을 관리하고자 할 경우, XProtect 을(를) 이용하면 가능합니다. 이 솔루션은 모든 장치, 서버 및 사용자에 대해 중앙 집중식 관리 기능과 함께 일정과 이벤트로 구동되는 매우 유연한 규칙 시스템을 제공합니다.

해당 시스템은 다음의 기본 구성 요소로 이루어집니다.

- **관리 서버** - 설치의 중심 요소로, 여러 서버로 이루어집니다.
- 하나 이상의 **레코딩 서버**
- 하나 이상의 **XProtect Management Client** 설치
- **XProtect Download Manager**
- 하나 이상의 **XProtect® Smart Client** 설치
- 하나 이상의 **XProtect Web Client** 사용 및/또는 필요한 경우 **XProtect Mobile** 클라이언트의 설치

또한 시스템에는 감시 시스템의 모든 카메라에서 Matrix 이(가) 설치된 컴퓨터로 비디오의 분산된 보기를 위해 완벽히 통합된 XProtect Smart Client 기능이 포함되어 있습니다.

분산 설치에서 시스템을 가상 서버 또는 여러 물리적 서버에 설치할 수 있습니다. 또한 페이지 82의 배포형 시스템 설정를 참조하십시오.

시스템은 또한 XProtect® Smart Client – Player 에서 비디오 증거물을 내보내기할 때 독립 실행형 XProtect Smart Client를 포함시킬 수도 있습니다. XProtect Smart Client – Player 을(를) 사용하면 비디오 증거 수신자(예: 경찰관, 내부 또는 외부 조사관 등)가 자신의 컴퓨터에 감시 소프트웨어를 설치하지 않고도 내보낸 레코딩을 찾아 재생할 수 있습니다.

가장 기능이 다양한 제품을 설치함으로써(페이지 103의 제품 비교 참조), 귀하의 시스템은 카메라, 서버 및 사용자를 필요한 경우 다중 사이트에 걸쳐 수에 제한 없이 취급을 할 수 있게 됩니다. 또한 IPv4와 IPv6를 처리할 수 있습니다.

시스템 구성 요소

관리 서버(설명됨)

관리 서버는 비디오 관리 소프트웨어 시스템의 핵심 구성 요소입니다. 관리 서버는 SQL Server 데이터베이스의 감시 시스템 구성을 관리 서버 컴퓨터 자체의 SQL Server 또는 네트워크의 별도 SQL Server에 저장합니다. 또한 사용자 인증, 사용자 권한, 규칙 시스템 등을 처리합니다. 시스템 성능을 개선하기 위해 여러 관리 서버를 Milestone Federated Architecture™ (으)로 실행할 수 있습니다. 관리 서버는 서비스로 실행되며, 일반적으로 전용 서버에 설치됩니다.

사용자는 최초 인증 시 관리 서버에 연결한 다음 비디오 녹화 등을 위해 레코딩 서버에 투명하게 연결할 수 있습니다.

SQL Server 설치 및 데이터베이스(설명됨)

관리 서버와 이벤트 서버, 로그 서버는 하나 이상의 SQL Server 설치에서 시스템 구성과 알람, 이벤트, 로그 메시지를 SQL Server 데이터베이스에 저장합니다. 관리 서버와 이벤트 서버는 동일한 SQL Server 데이터베이스를 공유하는 반면, 로그 서버 및 XProtect Incident Manager, Identity Provider 은(는) 독자적인 SQL Server 데이터베이스를 갖습니다.

Identity Provider에 대한 자세한 내용은 페이지 61의 Identity Provider (설명됨)를 참고하십시오. XProtect Incident Manager 데이터베이스 및 로깅에 대한 자세한 내용은 별도의 XProtect Incident Manager 관리자 설명서를 참조하십시오.

시스템 설치 프로그램에는 SQL Server 의 무료 에디션인 Microsoft SQL Server Express 이(가) 포함됩니다.

매우 큰 시스템 또는 SQL Server 데이터베이스에서 발생하는 트랜잭션이 많은 시스템의 경우, Milestone에서는 네트워크의 전용 컴퓨터 및 다른 목적으로 사용되지 않는 전용 하드 디스크 드라이브에 설치된 Microsoft® SQL Server® Standard 또는 SQL Server의 Microsoft® SQL Server® Enterprise 에디션을 사용할 것을 권장합니다. 자체 드라이브에 SQL Server을(를) 설치하면 전반적인 시스템 성능이 개선됩니다.

레코딩 서버(설명됨)

레코딩 서버는 네트워크 카메라 및 비디오 인코더와의 통신, 검색된 오디오 및 비디오 녹화를 비롯하여 라이브 및 기록된 오디오와 비디오에 클라이언트 액세스 제공 기능을 담당합니다. 또한 레코딩 서버는 Milestone 기술을 통해 연결된 다른 Milestone Interconnect 제품과의 통신도 담당합니다.

장치 드라이버

- 네트워크 카메라 및 비디오 인코더는 동일 제조업체에서 개별 장치 또는 일련의 유사 장치용으로 특별히 개발한 장치 드라이버를 통해 통신합니다
- 2018 R1 릴리스부터 장치 드라이버는 최신 드라이버가 포함된 정기 Device Pack(장치 팩)과 기존 드라이버가 포함된 레거시 Device Pack(장치 팩)으로 나누어 집니다
- 정기 Device Pack(장치 팩)은 레코딩 서버를 설치할 때 자동으로 설치됩니다. 나중에, 최신 버전의 Device Pack(장치 팩)을 다운로드하고 설치하여 드라이버를 업데이트할 수 있습니다
- 레거시 Device Pack(장치 팩)은 시스템에 정기 Device Pack(장치 팩)이 설치된 경우에만 설치할 수 있습니다. 이전 버전이 이미 시스템에 설치된 경우 레거시 Device Pack(장치 팩)의 드라이버는 자동으로 설치됩니다. 소프트웨어 다운로드 페이지(https://www.milestonesys.com/downloads/)에서 수동으로 다운로드 및 설치할 수 있습니다.

미디어 데이터베이스

- 레코딩 서버는 검색된 오디오 및 비디오 데이터를 오디오와 비디오 데이터의 기록 및 보관에 최적화된 맞춤형 고성능 미디어 데이터베이스에 저장합니다
- 미디어 데이터베이스는 멀티스테이지 아카이브, 비디오 다듬기, 암호화, 레코딩에 디지털 서명 추가 등의 여러 가지 고유한 기능을 지원합니다

시스템은 비디오 피드의 레코딩과 카메라 및 기타 기기와의 통신을 위해 레코딩 서버를 사용합니다. 감시 시스템은 일반적으로 여러 개의 레코딩 서버로 구성됩니다.

레코딩 서버는 Recording Server 소프트웨어를 설치하고 관리 서버와 통신하기 위해 구성한 컴퓨터입니다. **서버** 폴더를 확장한 다음 **레코딩 서버** 를 선택할 경우 **개요** 창에서 레코딩 서버를 볼 수 있습니다.

이 관리 서버 버전 이전의 레코딩 서버 버전과의 역호환성은 제한됩니다. 이전 버전으로 레코딩 서버의 레코딩에 여전히 액세스할 수 있지만, 구성을 변경하기 위해서는 이 관리 서버의 버전과 동일한 버전이어야 합니다. Milestone 에서는 시스템에 모든 레코딩 서버를 관리 서버와 동일한 버전으로 업그레이드 하도록 권장합니다.

레코딩 서버는 클라이언트 및 서비스에 대한 데이터 스트림의 암호화를 지원합니다.

- 페이지 281의 클라이언트 및 서비스에 암호화 활성화
- 페이지 268의 클라이언트에 대한 암호화 상태 보기

또한 레코딩 서버는 관리 서버와의 연결 암호화를 지원합니다.

- 페이지 277의 관리 서버로 및 관리서버로부터 암호화 활성화

레코딩 서버 관리와 관련하여 다음과 같은 몇 가지 옵션이 있습니다.

- 페이지 197의 하드웨어 추가
- 페이지 314의 하드웨어 이동
- 페이지 332의 레코딩 서버에서 모든 하드웨어 삭제
- 페이지 331의 레코딩 서버 제거

> ⚠ Recording Server 서비스가 실행 중인 경우, Windows Explorer 또는 다른 프로그램이 시스템 설정과 관련된 미디어 데이터베이스 파일이나 폴더에 액세스하지 않아야 합니다. 만약 액세스할 경우, 레코딩 서버가 관련 미디어 파일의 이름을 바꾸거나 파일을 이동할 수 없을 가능성이 높습니다. 이로 인해 레코딩 서버 작동이 중단될 수도 있습니다. 중지된 레코딩 서버를 다시 시작하려면, Recording Server 서비스를 중지하고, 해당 미디어 파일(들) 또는 폴더(들)를 액세스하는 프로그램을 닫은 후, Recording Server 서비스를 다시 시작하십시오.

모바일 서버(설명됨)

모바일서버는XProtectMobile클라이언트및XProtectWebClient사용자에게시스템액세스권한을부여하는역할을합니다.

모바일 서버는 두 클라이언트를 위한 시스템 게이트웨이로 기능하는 것 외에도, 비디오를 트랜스코딩할 수 있습니다. 많은 경우에 원본 카메라 비디오 스트림은 클라이언트 사용자가 사용할 수 있는 대역폭에 맞추기에 너무 크기 때문입니다.

분산 또는 **사용자 지정** 설치를 실행하는 경우, Milestone 에서는 전용 서버에 모바일 서버를 설치할 것을 권장합니다.

이벤트 서버(설명됨)

이벤트 서버는 이벤트, 알람 및 맵 그리고 MIP SDK 을(를) 통한 타사 통합에 관련된 다양한 작업을 취급합니다.

이벤트

- 모든 시스템 이벤트는 이벤트 서버에서 통합되므로 파트너가 시스템 이벤트를 활용하는 통합을 만들 수 있는 장소와 인터페이스가 하나뿐입니다
- 또한 이벤트 서버는 일반 이벤트 또는 분석 이벤트 인터페이스를 통해 시스템으로 이벤트를 전송할 수 있는 제3자 액세스를 제공합니다

알람

- 이벤트 서버는 알람 기능, 알람 논리, 알람 상태를 비롯하여 알람 데이터베이스 처리를 호스팅합니다. 알람 데이터베이스는 관리 서버가 사용하는 것과 동일한 SQL Server 데이터베이스에 저장됩니다.

메시지

- 메시지 통신은 이벤트 서버가 처리하며, 플러그 인이 XProtect Smart Client, Management Client, 이벤트 서버, 독립형 서비스와 같은 환경 간에 실시간으로 메시지를 전송할 수 있습니다.

맵

- 이벤트 서버는 XProtect Smart Client 에서 구성되어 사용되는 맵을 호스팅합니다

MIP SDK

- 마지막으로타사에서개발한플러그인을이벤트서버에설치하여시스템이벤트에대한액세스를활용할수있습니다

로그 서버(설명됨)

로그 서버는 SQL Server 데이터베이스 내 모든 시스템의 모든 로그 메시지를 저장합니다. 이러한 로그 메시지 데이터베이스는 관리 서버의 시스템 구성 데이터베이스와 동일한 SQL Server 또는 별도의 SQL Server에 있을 수 있습니다. 로그 서버는 보통 관리 서버와 같이 동일한 서버에 설치되지만 관리 서버 및 로그 서버의 성능을 향상시키기 위해 별도의 서버에 설치할 수 있습니다.

API Gateway (설명됨)

MIP VMS API은(는) OpenAPI와(과) 같은 산업 표준 프로토콜을 기반으로 하는 통합 RESTful API를 제공하여 XProtect VMS 기능에 액세스하고 통합 프로젝트를 단순화하며 클라우드 연결 통신의 기반 역할을 합니다.

XProtect VMS API Gateway은(는) Milestone Integration Platform VMS API (MIP VMS API)을(를) 통해 이러한 통합 옵션을 지원합니다.

API Gateway은(는) 온프레미스에 설치되며 현재 모든 비디오 관리 소프트웨어 서버 구성 요소(관리 서버, 이벤트 서버, 레코딩 서버, 로그 서버 등)에서 RESTful API 및 WebSocket 메시징 API 서비스의 프런트 엔드 및 공통 엔트리 포인트로 사용됩니다. API Gateway 서비스는 관리 서버와 동일한 호스트에 설치하거나 별도로 설치할 수 있으며 둘 이상(각각 자체 호스트)에 설치할 수 있습니다.

RESTful API는 각 특정 VMS 서버 구성 요소에 의해 부분적으로 구현되며, API Gateway은(는) 이러한 요청과 응답을 간단히 전달할 수 있지만, 다른 요청의 경우 API Gateway은(는) 요청과 응답을 적절하게 변환합니다.

현재 관리 서버에서 호스팅하는 구성 API는 RESTful API로 사용할 수 있습니다. 이벤트 서버에서 호스팅한 RESTful 이벤트 API, Websockets 메시징 API, RESTful 알람 API도 사용할 수 있습니다.

자세한 내용은 API Gateway 관리자 설명 서 및 Milestone Integration Platform VMS API참조 문서를 참조하십시오.

장애 조치

XProtect Management Server Failover

Management Server 서비스 또는 SQL Server을(를) 실행하는 독립 실행형 컴퓨터에 하드웨어 오류가 발생하더라도 레코딩 또는 레코딩 서버에는 영향을 미치지 않습니다. 그러나 이러한 하드웨어 오류로 인해 클라이언트에 로그인하지 않은 운영자와 관리자에게 시스템 중단이 발생할 수 있습니다.

XProtect Management Server Failover은(는) 관리 서버에 고가용성 및 재해 복구 기능을 제공합니다. 한 컴퓨터에서 관리 서버를 사용할 수 없게 되면 다른 컴퓨터가 시스템 구성 요소를 실행하는 작업을 인계받습니다.

SQL Server 데이터베이스의 안전한 실시간 복제를 사용하여 하드웨어 장애 발생 시 데이터 손실이 발생하지 않도록 할 수 있습니다.

XProtect Management Server Failover은(는) 시스템 중단을 완화하는 데 도움이 될 수 있습니다. 다음과 같은 경우 장애 조치 클러스터의 이점을 누릴 수 있습니다.

- 서버 실패 – 문제를 해결하는 동안 다른 컴퓨터에서 Management Server 서비스 및 SQL Server을(를) 실행할 수 있습니다.
- 시스템 업데이트 및 보안 패치를 적용해야 합니다. 독립 실행형 관리 서버에 보안 패치를 적용하면 시간이 오래 걸릴 수 있으므로 가동 중지 시간이 길어질 수 있습니다. 장애 조치 클러스터가 있는 경우 가동 중지 시간을 최소화하면서 시스템 업데이트 및 보안 패치를 적용할 수 있습니다.
- 원활한 연결이 필요합니다. 이를 통해 사용자는 라이브 및 재생 비디오와 시스템 구성에 항상 지속적으로 액세스할 수 있습니다.

두 컴퓨터 간에 XProtect Management Server Failover을(를) 구성합니다. 장애 극복 시스템이 작동하도록 하려면 각 컴퓨터에 다음 사항을 설치합니다.

- XProtect Management Server
- XProtect Event Server 서비스
- XProtect Log Server 서비스
- Microsoft SQL Server(권장)

장애 조치 관리 서버(설명됨)

관리 서버의 장애 조치 지원은 Microsoft Windows 클러스터에 관리 서버를 설치하면 구현됩니다. 그러면 이 클러스터를 통해 첫 번째 서버가 실패할 경우 다른 서버가 관리 서버 기능을 인계하도록 보장됩니다.

장애 조치 레코딩 서버(설명됨)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

장애 조치 레코딩 서버는 표준 레코딩 서버가 사용 불가능할 경우 전환되는 추가적인 레코딩 서버입니다. **수동 대기 서버** 또는 **상시 대기 서버** 와 같은 두 가지 모드로 장애 조치 레코딩 서버를 구성할 수 있습니다.

표준 레코딩 서버와 같은 장애 조치 레코딩 서버를 설치합니다(페이지 153의 다음을 통해 장애 조치 레코딩 서버 설치: Download Manager 참조). 장애 조치 레코딩 서버를 설치하면 Management Client 에서 볼 수 있습니다. Milestone 에서는 모든 장채 조치 레코딩 서버를 별도 컴퓨터에 설치하도록 권장합니다. 관리 서버의 정확한 IP 주소/호스트 이름과 함께 장애 조치 레코딩 서버를 구성해야 합니다. 장애 조치 서버 서비스에서 실행되는 사용자 계정에 대한 사용자 권한은 설치 과정 중에 제공됩니다. 이러한 권한은 다음과 같습니다:

- 장애 조치 레코딩 서버 시작 또는 중지를 위한 시작/중지 권한
- RecorderConfig.xml 파일을 읽거나 쓰기 위한 읽기 및 쓰기 접근 권한

인증이 암호화를 위해 선택된 경우 관리자는 반드시 읽기 접근 권한을 선택된 인증 개인 키에 대한 장애 조치 사용자에게 허용해야 합니다.

장애 조치 레코딩 서버가 암호화를 사용하는 레코딩 서버로부터 인계할 경우, Milestone 에서는 장애 조치 레코딩 서버도 암호화를 사용하도록 준비할 것을 권장합니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 및 페이지 153의 다음을 통해 장애 조치 레코딩 서버 설치: Download Manager를 참조하십시오.

장치 수준에서 원하는 장애 조치 지원 유형을 지정할 수 있습니다. 레코딩 서버의 각 장치에 대해 전체, 라이브만 또는 장애 조치 지원 없음을 선택합니다. 이를 통해 장애 조치 리소스의 우선순위를 손쉽게 정할 수 있습니다. 예를 들어 오디오를 제외한 비디오에 대해서만 장애 조치를 설정하거나 불필요한 카메라를 제외한 필수 카메라에 대해서만 장애 조치를 설정할 수 있습니다.

시스템이 장애 조치 모드에 있는 동안, 하드웨어를 대체하거나 이동하거나 레코딩 서버를 업데이트하거나 스토리지 설정이나 비디오 스트림 설정 같은 기기 구성을 변경할 수 없습니다.

수동 대기 장애 조치 레코딩 서버

수동 대기 장애 조치 레코딩 서버 설정에서, 여러 장애 조치 레코딩 서버를 하나의 장애 조치 그룹에 그룹화합니다. 전체 장애 조치 그룹은 사전 선택한 여러 레코딩 서버 중 하나를 사용할 수 없을 때 해당 서버의 작업을 전담하여 인수합니다. 필요한 만큼 많은 그룹을 생성할 수 있습니다(페이지 195의 수동 대기를 위한 장애 조치 레코딩 서버 그룹 참조).

그룹화는 명확한 이점이 있습니다: 나중에 레코딩 서버의 작업을 인수할 장애 조치 레코딩 서버를 지정할 때 장애 조치 레코딩 서버 그룹을 선택합니다. 선택한 그룹에 둘 이상의 장애 조치 레코딩 서버가 포함된 경우, 한 레코딩 서버를 사용할 수 없을 때 둘 이상의 장애 조치 레코딩 서버가 해당 작업을 인수할 수 있는 확실한 보안 조치를 마련할 수 있습니다. 기본 그룹의 모든 레코딩 서버가 사용 중일 경우 기본 그룹에서 작업을 인수하는 보조 장애 조치 서버 그룹을 지정할 수 있습니다. 장애 조치 레코딩 서버는 한 번에 한 그룹의 구성원만 될 수 있습니다.

하나의 장애 조치 그룹에서 장애 조치 레코딩 서버는 순서대로 정렬됩니다. 이 순서는 장애 조치 레코딩 서버가 레코딩 서버로부터 작업을 인수하는 순서를 결정합니다. 기본적으로 이 순서는 장애 조치 그룹에 장애 조치 레코딩 서버를 포함한 순서를 반영합니다. 먼저 포함된 것이 우선입니다. 필요한 경우 이 순서를 변경할 수 있습니다.

상시 대기 장애 조치 레코딩 서버

상시 대기 장애 조치 레코딩 서버 설정에서는 전담 장애 조치 레코딩 서버가 **하나의** 레코딩 서버에서만 작업을 인수합니다. 이 때문에, 시스템은 이 장애 조치 레코딩 서버를 "대기" 모드로 유지할 수 있으며, 이는 전담된 레코딩 서버의 올바른/현재 구성과 동기화되며, 수동 대기 장애 조치 레코딩 서버보다 훨씬 빨리 인수할 수 있다는 의미입니다. 언급한 바와 같이 상시 대기 서버를 하나의 레코딩 서버에만 할당하고, 서버를 그룹화할 수는 없습니다. 이미 상시 대기 레코딩 서버로서 장애 조치 그룹에의 일부인 장애 조치 서버를 할당할 수 없습니다.

장애 조치 레코딩 서버 유효성 확인

장애 조치 서버에서 레코딩 서버로의 비디오 데이터 통합 유효성을 확인하려면 레코딩 서버 서비스를 중단하거나 레코딩 서버 컴퓨터를 끔으로써 레코딩 서버를 사용할 수 없는 상태로 만들어야 합니다.

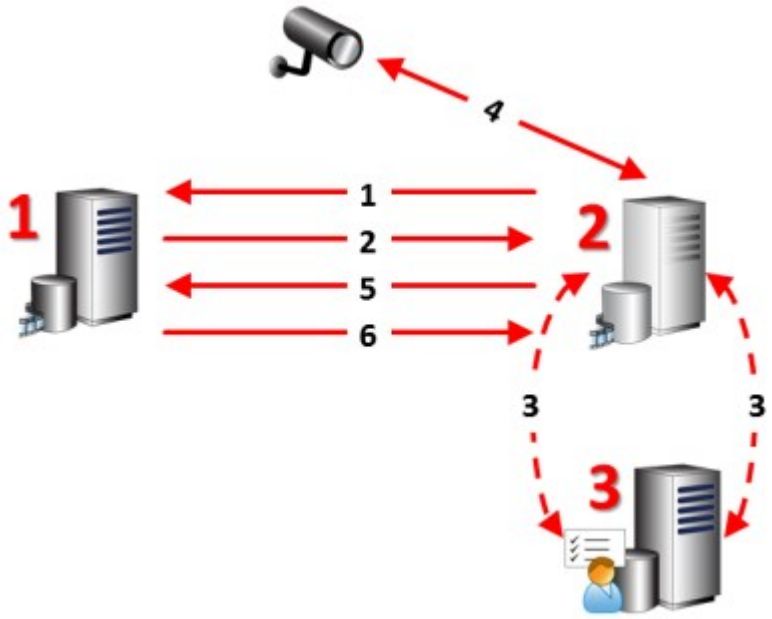
네트워크 케이블를 뽑거나 테스트 도구를 사용하여 네트워크를 막음으로써 야기되는 수동 네트워크 차단은 유효한 방법이 아닙니다.

장애 조치 레코딩 서버 기능(설명됨)

- 장애 조치 레코딩 서버는 0.5초마다 관련 레코딩 서버의 상태를 확인합니다. 레코딩 서버가 2초 내에 회신하지 않으면 레코딩 서버가 사용할 수 없는 것으로 간주되고 장애 조치 레코딩 서버가 해당 작업을 인수합니다
- 수동 대기 장애 조치 레코딩 서버는 장애 조치 레코딩 서버의 Recording Server 서비스를 시작하는 데 소요되는 시간, 카메라에 연결하는 데 소요되는 시간에 5초를 합친 시간 후 사용 불가 상태가 된 레코딩 서버 작업을 인수합니다. 이와 대조적으로, 상시 대기 장애 조치 레코딩 서버는 Recording Server 서비스가 올바른 구성으로 이미 실행 중이고 피드를 전달하기 위해 카메라만 시작하면 되므로 보다 빠르게 작업을 인수할 수 있습니다. 시작 기간 중에는 영향 받는 카메라로부터 레코딩을 저장하거나 라이브 비디오를 볼 수 없습니다

- 레코딩 서버를 다시 이용할 수 있게 될 경우, 장애 조치 레코딩 서버로부터 자동으로 작업을 인수합니다. 장애 조치 레코딩 서버에 의해 저장된 레코딩은 표준 레코딩 서버의 데이터베이스에 자동으로 병합됩니다. 병합 프로세스에 걸리는 시간은 레코딩의 양, 네트워크 용량 등에 따라 다릅니다. 병합 프로세스 중에는 장애 조치 레코딩 서버가 작업을 인수하는 동안의 기간에 레코딩을 검색할 수 없습니다
- 장애 조치 레코딩 서버가 수동 대기 장애 조치 레코딩 서버 설정에서 병합 프로세스 중 다른 레코딩 서버의 작업을 인수해야 하는 경우, 레코딩 서버 A의 병합 프로세스가 연기되고 레코딩 서버 B의 작업을 인수합니다. 레코딩 서버 B를 다시 사용할 수 있게 되면 장애 조치 레코딩 서버가 병합 프로세스를 시작하여 레코딩 서버 A와 레코딩 서버 B 모두 동시에 레코딩을 다시 병합할 수 있게 해줍니다.
- 상시 대기 설정에서는 단일 레코딩 서버에 대해서만 상시 대기가 가능하므로 상시 대기 서버가 다른 레코딩 서버의 작업을 인수할 수 없습니다. 하지만 레코딩 서버가 다시 실패하면 상시 대기 서버가 다시 인수하여 이전 기간에서부터 레코딩을 유지합니다. 레코딩 서버는 기본 레코더에 다시 병합되거나 또는 장애 조치 레코딩 서버의 디스크 공간이 부족해질 때까지 레코딩을 보관합니다
- 장애 조치 솔루션은 완벽한 중복 관리를 제공하지 않습니다. 가동 중단 시간을 최소화하는 데 중점을 두고 사용됩니다. 레코딩 서버를 다시 사용할 수 있게 되면, Failover Server 서비스에서 레코딩 서버가 레코딩을 다시 저장할 준비가 되었는지 확인합니다. 그런 후에만 레코딩 저장 책임을 표준 레코딩 서버로 인수합니다. 따라서, 이 프로세스 단계에서 레코딩이 손실될 확률은 거의 없습니다
- 클라이언트 사용자는 장애 조치 레코딩 서버가 작업을 인수하고 있음을 거의 알아채지 못합니다. 장애 조치 레코딩 서버가 작업을 인수할 때는 보통 몇 초에 불과한 짧은 중단이 발생합니다. 이 중단 기간 중 사용자는 영향을 받는 레코딩 서버에서 비디오에 액세스할 수 없습니다. 클라이언트 사용자는 장애 조치 레코딩 서버가 작업을 인수한 즉시 라이브 비디오를 시청할 수 있습니다. 최근 레코딩이 장애 조치 레코딩 서버에 저장되므로 장애 조치 레코딩 서버가 작업을 인수한 후 해당 레코딩을 재생할 수 있습니다. 클라이언트는 레코딩 서버가 다시 기능하고 장애 조치 레코딩 서버로부터 작업을 인수할 때까지는 영향을 받는 레코딩 서버에만 저장된 이전 레코딩을 재생할 수 없습니다. 아카이브된 레코딩에도 액세스할 수 없습니다. 레코딩 서버가 다시 기능하면 장애 조치 레코딩이 레코딩 서버의 데이터베이스에 병합되는 기간 동안 병합 프로세스가 이루어집니다. 이 프로세스 중에, 장애 조치 레코딩 서버가 작업을 인수한 기간 중의 레코딩을 재생할 수 없습니다
- 수동 대기 설정에서, 장애 조치 레코딩 서버를 다른 장애 조치 레코딩 서버의 백업으로 설정하는 작업은 필요하지 않습니다. 이는 장애 조치 그룹을 할당하지만 특정 레코딩 서버의 작업을 인수하도록 특정 장애 조치 레코딩 서버를 할당하지 않기 때문입니다. 장애 조치 그룹에는 최소 하나 이상의 장애 조치 레코딩 서버가 포함되어야 하지만, 필요한 수만큼의 장애 조치 레코딩 서버를 추가할 수 있습니다. 장애 조치 그룹에 둘 이상의 장애 조치 레코딩 서버가 포함된 경우, 둘 이상의 장애 조치 레코딩 서버가 작업을 인수할 수 있습니다.
- 상시 대기 설정에서는 상시 대기 서버에 대해 장애 조치 레코딩 서버 또는 상시 대기 서버를 설정할 수 없습니다

장애 조치 단계(설명됨)



설명
포함된 서버(빨간색으로 표시된 번호): 1. Recording Server 2. Failover Recording Server 3. Management Server
수동 대기 설정에 대한 장애 조치 단계: 1. 실행 여부를 확인하기 위해 장애 조치 레코딩 서버는 레코딩 서버에 대해 논스톱 TCP 연결을 사용합니다. 2. 이 연결이 중단되었습니다. 3. 장애 조치 레코딩 서버가 관리 서버로부터 레코딩 서버의 현재 구성을 요청합니다. 관리 서버가 요청된 구성을 전송하고, 장애 조치 레코딩 서버가 해당 구성을 수신한 후 레코딩 서버를 대신하여 서버를 가동하여 레코딩을 시작합니다. 4. 장애 조치 레코딩 서버 및 해당 카메라가 비디오 데이터를 교환합니다. 5. 장애 조치 레코딩 서버가 계속해서 레코딩 서버에 대한 연결 재설정을 시도합니다.

설명
6. 레코딩 서버에 대한 연결이 재설정되면 장애 조치 레코딩 서버가 종료되고, 레코딩 서버가 가동 중단 시간 중 녹화된 비디오 데이터(있는 경우)를 전달하고, 해당 비디오 데이터가 레코딩 서버 데이터베이스에 다시 병합됩니다.
상시 대기 설치에 대한 장애 조치 단계: 1. 실행 여부를 확인하기 위해 상시 대기 서버는 할당된 레코딩 서버에 대해 논스톱 TCP 연결을 사용합니다. 2. 이 연결이 중단되었습니다. 3. 관리 서버를 통해 상시 대기 서버는 할당된 레코딩 서버에 대한 현재 구성을 이미 알고 있으며, 레코딩 서버를 대신하여 레코딩을 시작합니다. 4. 상시 대기 서버 및 해당 카메라가 비디오 데이터를 교환합니다. 5. 상시 대기 서버가 계속해서 레코딩 서버에 대한 연결 재설정을 시도합니다. 6. 레코딩 서버에 대한 연결이 다시 설정되고 상시 대기 서버가 다시 상시 대기 모드로 돌아간 경우, 레코딩 서버가 가동 중단 시간 중 녹화된 비디오 데이터(있는 경우)를 가져오고, 해당 비디오 데이터가 레코딩 서버 데이터베이스에 다시 병합됩니다.

장애 조치 레코딩 서버 서비스(설명됨)

장애 조치 레코딩 서버에는 두 가지 서비스가 설치되어 있습니다:

- Failover Server 서비스 - 레코딩 서버로부터 인수하는 프로세스를 처리합니다. 이 서비스는 항상 실행 중이며, 해당 레코딩 서버의 상태를 지속적으로 점검합니다
- Failover Recording Server 서비스 - 장애 조치 레코딩 서버가 레코딩 서버로 작동하도록 활성화합니다.

  수동 대기 설정에서, 이 서비스는 필요한 경우 즉, 수동 대기 장애 조치 레코딩 서버가 레코딩 서버로부터 작업을 인수할 때만 시작됩니다. 이 서비스의 시작은 일반적으로 몇 초 정도 소요되지만 로컬 보안 설정에 따라 더 오래 걸릴 수 있습니다.
  상시 대기 설정에서, 이 서비스는 항상 실행 중으로서, 상시 대기 서버가 수동 대기 장애 조치 레코딩 서버보다 빠르게 인수할 수 있습니다.

클라이언트

Management Client (설명됨)

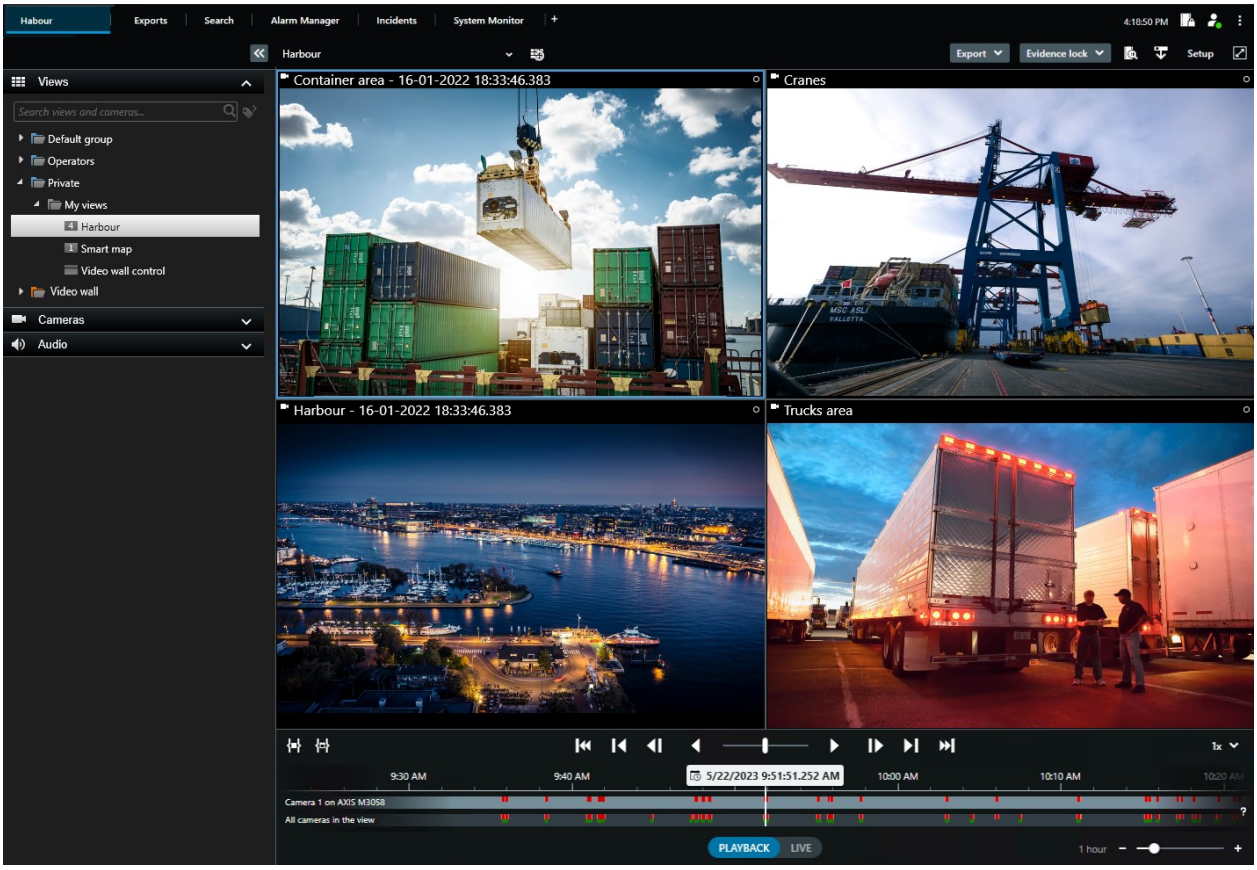
Management Client 은(는) 시스템의 구성 및 일상적 관리를 위한 기능이 풍부한 관리 클라이언트입니다. 여러 언어로 사용할 수 있습니다.

일반적으로 감시 시스템 관리자의 워크스테이션이나 유사 시스템에 설치됩니다.

XProtect Smart Client (설명됨)

XProtect Smart Client 은(는) IP 감시 카메라 관리를 도와주는 데스크톱 응용 프로그램입니다. 이 응용 프로그램은 사용자에게 라이브 및 레코딩된 비디오에 액세스하고, 카메라 및 연결된 보안 장치를 즉각적으로 제어하며, 레코딩 및 메타데이터에 대한 고급 검색 능력을 부여하여 보안 설치에 대해 직관적인 제어를 할 수 있도록 해줍니다.

다수의 현지 언어로 제공되는 XProtect Smart Client 에는 개별 운영자에 맞게 최적화되고 특정 기술과 권한 수준에 따른 조정을 가능하게 해주는 조절형 사용자 인터페이스가 사용됩니다.



인터페이스를 통해 밝거나 어두운 테마를 선택해 특정 작업 환경에 맞게 자신의 보기 환경을 맞춤화할 수 있습니다. 또한, 작업에 최적화된 탭과 메인 타임라인을 통해 감시 작업을 쉽게 할 수 있습니다.

MIP SDK을(를) 사용하면 사용자는 다양한 유형의 보안 및 비즈니스 시스템과 비디오 분석 응용 프로그램을 통합하고 XProtect Smart Client을(를) 통해 관리할 수 있습니다.

XProtect Smart Client 은(는) 운영자의 컴퓨터에 설치되어 있어야 합니다. 감시 시스템 관리자는 Management Client 을(를) 통해 감시 시스템에 액세스 권한을 관리합니다. XProtect 시스템의 Image Server 서비스에 의해 클라이언트가 본 레코딩이 제공됩니다. 이 서비스는 감시 시스템 서버에서 백그라운드로 실행됩니다. 별도의 하드웨어가 필요 없습니다.

XProtect Mobile 클라이언트(설명됨)

XProtect Mobile 클라이언트는 XProtect 시스템의 나머지 부분과 긴밀하게 통합되는 모바일 감시 솔루션입니다. Android 태블릿이나 스마트폰 또는 Apple® 태블릿, 스마트폰이나 휴대용 뮤직 플레이어를 켜고 카메라, 뷰 및 관리 클라이언트에서 설정한 기타 기능에 액세스 권을 제공합니다.

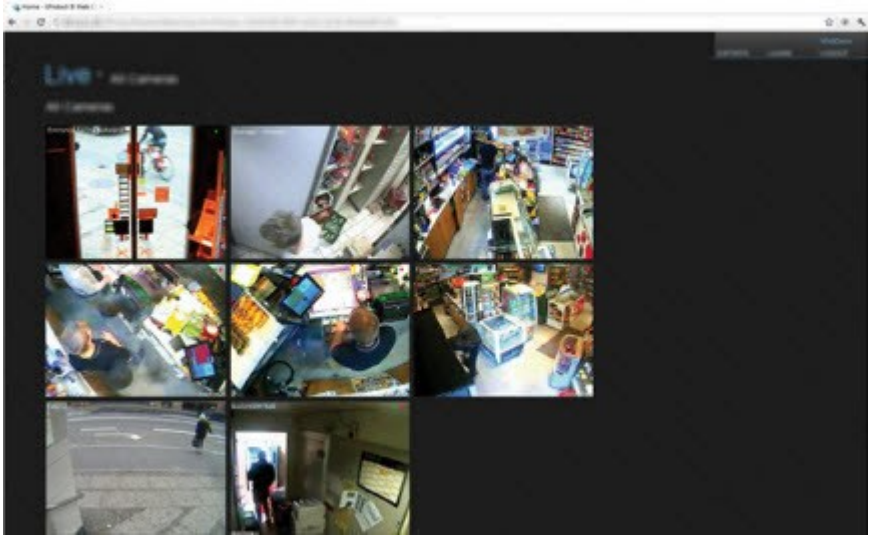
XProtect Mobile 클라이언트를 사용하면 하나 또는 여러 카메라의 실시간 및 녹화 비디오를 보거나 재생하고, PTZ(팬/기울기/줌) 카메라를 제어하고, 출력과 이벤트를 트리거하고, 비디오 푸시 기능을 사용하여 해당 장치에서 XProtect 시스템으로 비디오를 보낼 수 있습니다.

해당 시스템에서 XProtect Mobile 클라이언트를 사용하려면 XProtect Mobile 서버에서 XProtect Mobile 클라이언트와 시스템 사이에 연결을 설정해야 합니다. XProtect Mobile 서버가 설정되면, XProtect Mobile 클라이언트를 Google Play 또는 App Store에서 무료로 다운로드하여 XProtect Mobile 의 사용을 시작합니다.

XProtect 시스템에 비디오를 푸시할 수 있는 장치 하나당 장치 라이선스 1개가 필요합니다.

XProtect Web Client (설명됨)

XProtect Web Client 은(는) 비디오를 보고 재생하고 공유하기 위한 웹 기반 클라이언트 응용 프로그램입니다. 이 응용 프로그램은 라이브 비디오 보기, 녹화된 비디오 재생, 증거물 인쇄 및 내보내기 등 가장 일반적으로 사용되는 감시 기능에 대한 즉각적인 액세스를 제공합니다. 기능에 대한 액세스는 개별 사용자 권한에 따라 다르며 Management Client 에서 이러한 권한을 설정합니다.



XProtect Web Client 에 액세스할 수 있으려면 XProtect Mobile 서버를 설치하여 XProtect Web Client 및 해당 시스템 사이에서 연결을 구성해야 합니다. XProtect Web Client 자체는 어떤 설치도 필요하지 않으며 대부분의 인터넷 브라우저에서 작동합니다. XProtect Mobile 서버를 설정한 후에는 인터넷에 연결된 모든 컴퓨터나 태블릿을 통해 어디서든 XProtect 시스템을 모니터링할 수 있습니다(단, 올바른 외부/인터넷 주소, 사용자 이름 및 암호를 알고 있어야 함).

XProtect 확장

XProtect Access (설명됨)

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

> 을(를) 사용하려면 해당 XProtect Access 시스템 XProtect 내에서 이 기능에 액세스할 수 있는 기본 라이선스를 구입해야 합니다. 또한 제어하려는 각 도어에 대해 액세스 제어 도어 라이선스가 필요합니다.

> XProtect Access 용 해당 플러그 인이 존재하는 공급업체의 액세스 제어 시스템을 이용해 XProtect Access 을(를) 사용할 수 있습니다.

액세스 제어 통합 기능은 고객의 액세스 제어 시스템을 XProtect 과(와) 쉽게 통합할 수 있는 새로운 기능을 제공합니다. 제공 내용:

- XProtect Smart Client 의 여러 액세스 제어 시스템에 대한 공통 운영자 사용자 인터페이스
- 액세스 제어 시스템의 보다 빠르고 강력한 통합
- 더욱 풍부한 운영자 기능(아래 참조)

XProtect Smart Client 에서 운영자가 수행할 수 있는 작업:

- 액세스 지점에서 이벤트 실시간 모니터링
- 액세스 요청의 운영자 지원 전달
- 맵 통합
- 액세스 제어 이벤트에 대한 알람 정의
- 액세스 지점에서 이벤트 조사
- 도어 상태를 중앙에서 개괄적으로 확인하고 제어
- 카드 소유자 정보 및 관리

감사 로그 에는 각 사용자가 XProtect Smart Client (으)로부터 액세스 제어 시스템에서 실행하는 명령이 기록됩니다.

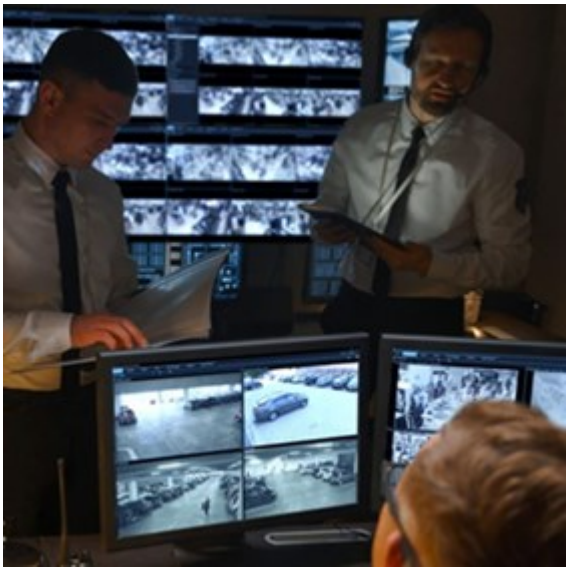
XProtect Access 기본 라이선스와는 별도로, 통합을 시작하기 전에 이벤트 서버에 특정 제공업체의 통합 플러그인이 설치되어 있어야 합니다.

XProtect Incident Manager

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

XProtect Incident Manager은(는) 조직에서 사건을 문서화하고 XProtect 비디오 관리 소프트웨어의 시퀀스 증거물(비디오 및 가능성 있는 오디오)과 결합할 수 있도록 지원하는 확장입니다.



XProtect Incident Manager의 사용자는 모든 사건 정보를 사건 프로젝트에 저장할 수 있습니다. 사건 프로젝트에서 각 사건의 상태와 활동을 추적할 수 있습니다. 이러한 방식으로 사용자는 사건을 효과적으로 관리하고 강력한 사건 증거를 내부적으로 동료와, 외부적으로 당국과 공유할 수 있습니다.

XProtect Incident Manager은(는) 조직이 설문조사 영역에서 발생하는 사건에 대한 개요와 이해를 얻을 수 있도록 도와줍니다. 이러한 지식을 통해 조직은 향후 유사한 사건이 발생할 가능성을 최소화하는 단계를 구현할 수 있습니다.

XProtect Management Client에서 조직의 VMS XProtect 관리자는 조직의 요구 사항에 따라 XProtect Incident Manager에서 사용 가능한 사건 속성을 정의할 수 있습니다. XProtect Smart Client의 작업자들은 사건 프로젝트를 시작, 저장 및 관리하고 사건 프로젝트에 다양한 정보를 추가합니다. 여기에는 자유 텍스트, 관리자가 정의한 사건 속성 및 XProtect 비디오 관리 소프트웨어(VMS)의 시퀀스가 포함됩니다. 완전한 추적성을 위해 XProtect VMS는 관리자가 사건 속성을 정의 및 편집할 때와 관리자가 사건 프로젝트를 생성 및 업데이트할 때 기록됩니다.

XProtect LPR (설명됨)

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

XProtect LPR 에서는 비디오 기반 콘텐츠 분석(VCA) 및 자동차번호판 인식을 제공하며 감시 시스템 및 XProtect Smart Client 와(과) 상호 작용합니다.

번호판의 문자를 판독하기 위해 XProtect LPR 에서는 특별한 카메라 설정을 통해 이미지에 대한 광학 문자 인식을 사용합니다.

LPR(자동차번호판인식) 기능을 출력의 레코딩 및 이벤트 기반 활성화와 같은 기타 감시 기능과 결합시킬 수 있습니다.

XProtect LPR 에서 이벤트의 예:

- 특정 품질로 감시 시스템 레코딩을 트리거합니다
- 알람을 활성화합니다
- 음수/양수 자동차번호판 일치 목록과 비교합니다
- 게이트를 엽니다
- 조명을 켭니다
- 사건 비디오를 특정 보안 담당 직원의 컴퓨터 화면으로 푸시합니다
- 휴대폰 문자 메시지를 전송합니다

이벤트를 가지고 XProtect Smart Client 에서 알람을 활성화할 수 있습니다.

XProtect Smart Wall (설명됨)

XProtect Smart Wall 설명서도 참조하십시오.

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

XProtect Smart Wall은(는) 고급 확장으로, 조직이 특정 보안 요구 사항에 부합하는 비디오 월을 생성할 수 있도록 해줍니다. XProtect Smart Wall은(는) XProtect 비디오 관리 소프트웨어[1] 시스템의 모든 비디오 데이터에 대한 개요를 제공하며 모니터 수나 조합에 상관없이 지원합니다.

XProtect Smart Wall 은(는) 운영자가 시스템 관리자가 고정된 카메라 및 모니터 레이아웃 세트로 정의한 정적인 비디오 월을 볼 수 있게 해줍니다. 그러나 비디오 월은 또한 운영자가 표시될 항목을 제어할 수 있는 식으로 운영자 중심적이기도 합니다. 다음이 포함됩니다.

- 카메라와 기타 유형의 콘텐츠를 비디오 월로 푸시(예: 이미지, 텍스트, 알람, 스마트맵)
- 전체 뷰를 모니터로 보내기
- 특정 이벤트가 진행되는 과정 중에 대체 프리셋[2]을 적용

마지막으로, 특정 이벤트나 시간 스케줄에 기반하여 자동으로 프리셋을 변경하는 규칙으로 디스플레이 변경 내용을 통제할 수 있습니다.

---

[1]"비디오 관리 소프트웨어"의 줄임말.

[2]Smart Wall 에서 사전 지정된 XProtect Smart Client 하나 이상의 모니터. 프리셋은 비디오 월의 각 모니터상에서 어떤 카메라가 표시되고 콘텐츠가 구성될지를 결정합니다.

XProtect Transact (설명됨)

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

XProtect Transact은(는) Milestone의 IP 비디오 감시 솔루션에 대한 확장입니다.

XProtect Transact 은(는) 현재 진행 중인 트랜잭션을 관찰하고 이전 트랜잭션을 조사하기 위한 도구입니다. 트랜잭션은 예를 들어, 사기를 입증하거나 범행자에 대한 증거물을 제공하기 위해 트랜잭션을 모니터링하는 디지털 감시 비디오와 연결됩니다. 트랜잭션 라인과 비디오 이미지 사이에는 1대1 관계가 존재합니다.

트랜잭션 데이터는 여러 종류의 트랜잭션 소스로부터 기인할 수 있습니다. POS 시스템 또는 자동 현금 인출기(ATM)가 일반적인 예입니다.

Milestone Open Network Bridge (설명됨)

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

Milestone Open Network Bridge 은(는) XProtect VMS 시스템에서 IP기반 보안 시스템으로 표준화된 비디오 공유를 할 수있게 해주는 공개 ONVIF 호환 인터페이스입니다. 이를 통해 법 집행 기관이나 감시 센터, 유사 기관(ONVIF 클라이언트)이 XProtect VMS 시스템에서 중앙 모니터링 솔루션으로 라이브 및 녹화 비디오 스트림에 액세스할 수 있게 해줍니다. 비디오 스트림은 인터넷을 통해 RTSP 스트림으로 전송됩니다.

핵심 이점은 다음과 같습니다.

- 진정한 상호운용성과 대규모 멀티 벤더 보안 배포를 위한 선택의 자유, 비공개에서 공개로 매끄럽게 비디오 통합을 가능하게 해줍니다.
- XProtect VMS 시스템에서 H.264 및 H.265 비디오 스트리밍에 대해 외부 액세스(라이브 비디오와 재생 모두)를 제공합니다.
- 알람 센터와 모니터링 스테이션을 갖춘 XProtect VMS 솔루션 통합으로 간편하고 오류가 없는 방법을 제공하는 표준화된 인터페이스를 제공합니다.

이 문서에서는 다음 내용을 제공합니다.

- ONVIF 표준에 대한 정보와 참조 자료 링크
- XProtect VMS 제품에 Milestone Open Network Bridge 을(를) 설치하고 구성하기 위한 지침
- 다양한 유형의 ONVIF 클라이언트가 XProtect VMS 제품에서 라이브 및 레코딩된 비디오를 스트리밍할 수 있도록 활성화하는 방법을 보여주는 예

XProtect DLNA Server (설명됨)

이 제품은 Milestone에서 더 이상 지원하지 않습니다.

Milestone에서는 다양한 확장을 개발했습니다. 확장은 전문화된 기능을 추가하여 XProtect 비디오 관리 소프트웨어 제품의 기능을 확장하는 제품입니다. XProtect 라이선스 파일은 확장에 대한 액세스를 제어합니다.

DLNA(Digital Living Network Alliance)는 멀티미디어 장치 연결을 위한 표준입니다. 전자 장치 제조업체는 여러 공급업체 및 장치 사이에 상호운용성을 보장하기 위해 제품에 DLNA 인증을 받아, 비디오 콘텐츠를 배포할 수 있습니다.

공용 디스플레이 및 TV는 대개 DLNA 인증을 받고 네트워크에 연결됩니다. 또한 네트워크에서 미디어 콘텐츠를 검색하고, 장치에 연결하며, 내장된 미디어 플레이어로 미디어 스트림을 요청할 수 있습니다. XProtect DLNA Server 은(는) 특정 DLNA 인증 장치에 의해 검색될 수 있으며, 선택된 카메라로부터 미디어 플레이어를 가진 DLNA 인증 장치로 라이브 비디오 스트림을 전달할 수 있습니다.

DLNA 장치에는 1~10초의 라이브 비디오 지연이 있습니다. 이는 장치의 다양한 버퍼 크기로 인해 발생합니다.

XProtect DLNA Server은(는) XProtect 시스템과 동일한 네트워크에 연결되어야 하며, DLNA 장치는 XProtect DLNA Server와(과) 동일한 네트워크에 연결되어야 합니다.

장치

하드웨어(설명됨)

하드웨어는 다음을 나타냅니다.

- IP를 통해 감시 시스템의 레코딩 서버에 직접 연결되는 물리적 장치(예: 카메라, 비디오 인코더, I/O 모듈)
- Milestone Interconnect 설정에서 원격 사이트에 있는 레코딩 서버

시스템 내 각 레코딩 서버에 하드웨어를 추가하기 위한 여러 가지 옵션이 있습니다.

하드웨어가 NAT 지원 라우터 또는 방화벽 뒤에 위치한 경우, 다른 포트 번호를 지정하고 하드웨어가 사용하는 포트 및 IP 주소를 매핑하도록 라우터/방화벽을 구성해야 할 수 있습니다.

하드웨어 추가 마법사를 이용하면 네트워크에서 카메라와 비디오 인코더와 같은 하드웨어를 손쉽게 감시하여 시스템상의 레코딩 서버에 추가할 수 있습니다. 또한 마법사는 Milestone Interconnect 설치에 대한 원격 레코딩 서버 추가하는 것을 도와줍니다. 한 번에 **하나의 레코딩 서버** 만 추가하십시오.

하드웨어 사전 구성(설명됨)

특정 제조사는 처음으로 VMS 시스템에 하드웨어를 추가하기 전에 공장 출시 구성의 하드웨어에 자격 증명을 설정하도록 요구합니다. 이는 하드웨어 사전 구성으로 간주되며 그러한 하드웨어가 페이지 197의 하드웨어 추가 마법사에 감지되었을 시 표시되는 **하드웨어 장치 사전 구성** 마법사를 통해 완료됩니다.

사전 구성 하드웨어 장치 마법사와 관련한 중요한 정보 몇 가지:

- VMS 시스템에 추가되지 전에 첫 자격 증명이 필요한 하드웨어는 일반적인 기본 자격 증명을 이용하여 추가할 수 없으며, 마법사를 통해서 또는 하드웨어에 직접 연결하여 구성해야 합니다.
- 자격 증명(사용자 이름 또는 암호)는 **설정되지 않음** 으로 표시된 필드에만 적용할 수 있습니다.
- 일단 하드웨어 **상태** 가 **구성됨** 으로 설정된 경우, 해당 자격 증명(사용자 이름 또는 암호)를 변경할 수 없습니다.
- 사전 구성이 공장 초기 출시 상태인 하드웨어에 적용되며 이는 한 번만 수행하면 됩니다. 일단 사전 구성이 완료되면 다음에 있는 기타 하드웨어처럼 해당 하드웨어를 관리할 수 있습니다.Management Client
- **하드웨어 장치 사전 구성** 마법사를 닫은 후 페이지 197의 하드웨어 추가 마법사에 사전 구성 하드웨어가 표시되며 시스템에 하드웨어가 추가될 수 있게 됩니다.

> **하드웨어 장치 사전 구성** 마법사를 닫은 후 페이지 197의 하드웨어 추가 마법사를 완료하여 시스템에 사전 구성 하드웨어를 추가하는 것을 권장합니다. Management Client 은(는) 시스템에 하드웨어를 추가하지 않는 경우 사전 구성 자격 증명을 보관하지 않습니다.

장치(설명됨)

하드웨어에는 개별적으로 관리할 수 있는 여러 장치가 포함됩니다. 예를 들면 다음과 같습니다.

- 물리적 카메라 한 대는 카메라 부분(렌즈)을 비롯하여 연결되었거나 내장된 마이크로폰, 스피커, 메타데이터, 입력 및 출력을 나타내는 장치를 포함합니다
- 비디오 인코더에는 카메라 부분(렌즈)을 비롯하여 연결되었거나 내장된 마이크로폰, 스피커, 메타데이터, 입력 및 출력을 나타내는 장치의 한 목록에 나타나는 여러 아날로그 카메라가 연결되어 있습니다
- I/O 모듈에는 입력 및 출력 채널(예: 조명)을 나타내는 장치가 포함됩니다
- 전용 오디오 모듈에는 마이크로폰 및 스피커 입력과 출력을 나타내는 장치가 포함됩니다
- Milestone Interconnect 설정에서 원격 시스템은 한 목록에 나열된 원격 시스템의 모든 장치를 포함하는 하드웨어로 나타납니다

시스템은 사용자가 하드웨어를 추가할 때 해당 하드웨어의 장치를 자동으로 추가합니다.

> 지원되는 하드웨어에 대한 자세한 내용은 Milestone 웹사이트 (https://www.milestonesys.com/support/tools-and-references/supported-devices/)에서 지원되는 하드웨어 페이지를 참조하십시오.

다음 섹션은 추가할 수 있는 각 장치 유형을 설명합니다.

카메라

카메라 장치는 클라이언트 사용자가 라이브 비디오를 보기 위해 사용할 수 있는 시스템으로 비디오 스트림을 전달합니다. 그렇지 않으면 나중에 클라이언트 사용자가 재생할 수 있도록 시스템이 비디오 스트림을 녹화할 수 있습니다. 역할은 사용자가 비디오를 볼 수 있는 권한을 결정합니다.

마이크

많은 장치에서 외부 마이크로폰을 연결할 수 있습니다. 일부 장치에는 마이크가 내장되어 있습니다.

마이크 장치는 클라이언트 사용자가 라이브를 청취할 수 있는 시스템으로 오디오 스트림을 전달합니다. 그렇지 않으면 나중에 클라이언트 사용자가 재생할 수 있도록 시스템이 오디오 스트림을 기록할 수 있습니다. 시스템을 설정하여 관련 동작을 트리거하는 마이크 지정 이벤트를 수신할 수 있습니다.

역할은 사용자가 마이크를 들을 수 있는 권한을 결정합니다. Management Client 에서는 마이크를 들을 수 없습니다.

스피커

많은 장치에서 외부 스피커를 연결할 수 있습니다. 일부 장치에는 스피커가 내장되어 있습니다.

사용자가 XProtect Smart Client에서 말하기 버튼을 누르면 시스템이 오디오 스트림을 스피커로 XProtect Web Client전송합XProtect® Mobile니다. 스피커 오디오는 사용자가 말할 때에만 레코딩됩니다. 역할은 사용자가 스피커를 통해 말할 수 있는 권한을 결정합니다. Management Client 의 스피커를 통해서는 말할 수 없습니다.

두 명의 사용자가 동시에 말하기를 원하는 경우, 역할에 따라 스피커를 통해 말할 수 있는 사용자의 권한이 결정됩니다. 역할 정의의 일부로 사용자가 매우 높음에서 매우 낮음까지 스피커 우선순위를 지정할 수 있습니다. 두 명의 사용자가 동시에 말하기를 원하는 경우, 최고 우선순위의 역할을 가진 사용자가 말하기 기능을 갖게 됩니다. 동일 역할을 가진 두 명의 사용자가 동시에 말하기를 원하는 경우, 선착순 원칙이 적용됩니다.

메타데이터

메타데이터 장치는 클라이언트 사용자가 비디오 이미지, 이미지 내 콘텐츠 또는 개체, 이미지가 녹화된 위치를 설명하는 데이터와 같이 데이터에 관한 정보를 보는 데 사용할 수 있는 시스템으로 데이터 스트림을 전달합니다. 메타데이터는 카메라, 마이크 또는 스피커에 연결될 수 있습니다.

메타데이터는 다음에 의해 생성될 수 있습니다:

- 데이터를 전달하는 장치 자체(예: 비디오를 전달하는 카메라)
- 일반 메타데이터 드라이버를 통한 타사 시스템 또는 통합

장치에서 생성된 메타데이터는 동일 하드웨어에 있는 하나 이상의 장치에 자동으로 연결됩니다.

역할은 사용자가 메타데이터를 볼 수 있는 권한을 결정합니다.

입력

많은 장치에서 외부 장치를 장치의 입력 포트에 연결할 수 있습니다. 일반적으로 입력 장치는 외부 센서에 해당합니다. 그러한 외부 센서를 예를 들어 문, 창문 또는 대문이 열렸는지를 감지하는 데 사용할 수 있습니다. 해당 외부 입력 장치의 입력은 시스템에서 이벤트로 처리됩니다.

규칙에서 그러한 이벤트를 사용할 수 있습니다. 예를 들어 입력이 활성화되면 카메라가 레코딩을 시작하고 입력이 비활성화되고 30초 후에 레코딩을 중지하도록 지정하는 규칙을 만들 수 있습니다.

출력

많은 장치에서 외부 장치를 장치의 출력 포트에 연결할 수 있습니다. 그러면 시스템을 통해 조명, 사이렌 등을 활성화/비활성화할 수 있습니다.

규칙을 만들 때 출력을 사용할 수 있습니다. 출력을 자동으로 활성화 또는 비활성화하는 규칙과 출력 상태가 변경될 때 동작을 트리거하는 규칙을 만들 수 있습니다.

장치 그룹(설명됨)

장치를 장치 그룹으로 그룹화하는 작업은 **하드웨어 추가** 마법사의 일부지만, 필요 시 언제든지 그룹을 수정하고 다른 그룹을 더 추가할 수 있습니다.

시스템에서 여러 가지 유형의 장치(카메라, 마이크, 스피커, 메타데이터, 입력 및 출력)를 그룹화하여 편리하게 사용할 수 있습니다:

- 장치 그룹은 시스템에서 장치에 대한 직관적인 개요를 유지하도록 도와줍니다
- 장치는 여러 그룹 내에 존재할 수 있습니다
- 하위 그룹을 만들고 해당 하위 그룹 내에 하위 그룹을 만들 수 있습니다
- 장치 그룹 내의 모든 장치에 대한 공통 속성을 한 번에 지정할 수 있습니다
- 그룹을 통해 설정된 장치 속성은 그룹에 저장되지 않고 개별 장치에 저장됩니다
- 역할을 처리할 때 장치 그룹 내의 모든 장치에 대한 공통 보안 설정을 한 번에 지정할 수 있습니다
- 역할을 처리할 때 장치 그룹 내의 모든 장치에 하나의 규칙을 한 번에 적용할 수 있습니다

필요한 수만큼의 많은 장치 그룹을 추가할 수 있지만, 서로 다른 유형의 장치(예: 카메라와 스피커)를 한 장치 그룹에 혼합할 수는 없습니다.

모든 속성을 보고 편집할 수 있도록 400개 **미만** 의 장치를 포함한 장치 그룹을 만듭니다.

한 장치 그룹을 삭제할 경우, 해당 장치 그룹 자체만 삭제됩니다. 시스템에서 장치(예: 카메라)를 삭제하려는 경우, 레코딩 서버 수준에서 삭제를 수행하십시오.

다음 예시는 장치 그룹으로 카메라를 그룹화하는 것에 기반하지만 원리는 모든 장치에 대해 동일하게 적용됩니다.

장치 그룹 추가

장치 그룹에 포함시킬 장치 지정

장치 그룹의 모든 장치에 대한 공통 속성 지정

미디어 저장소

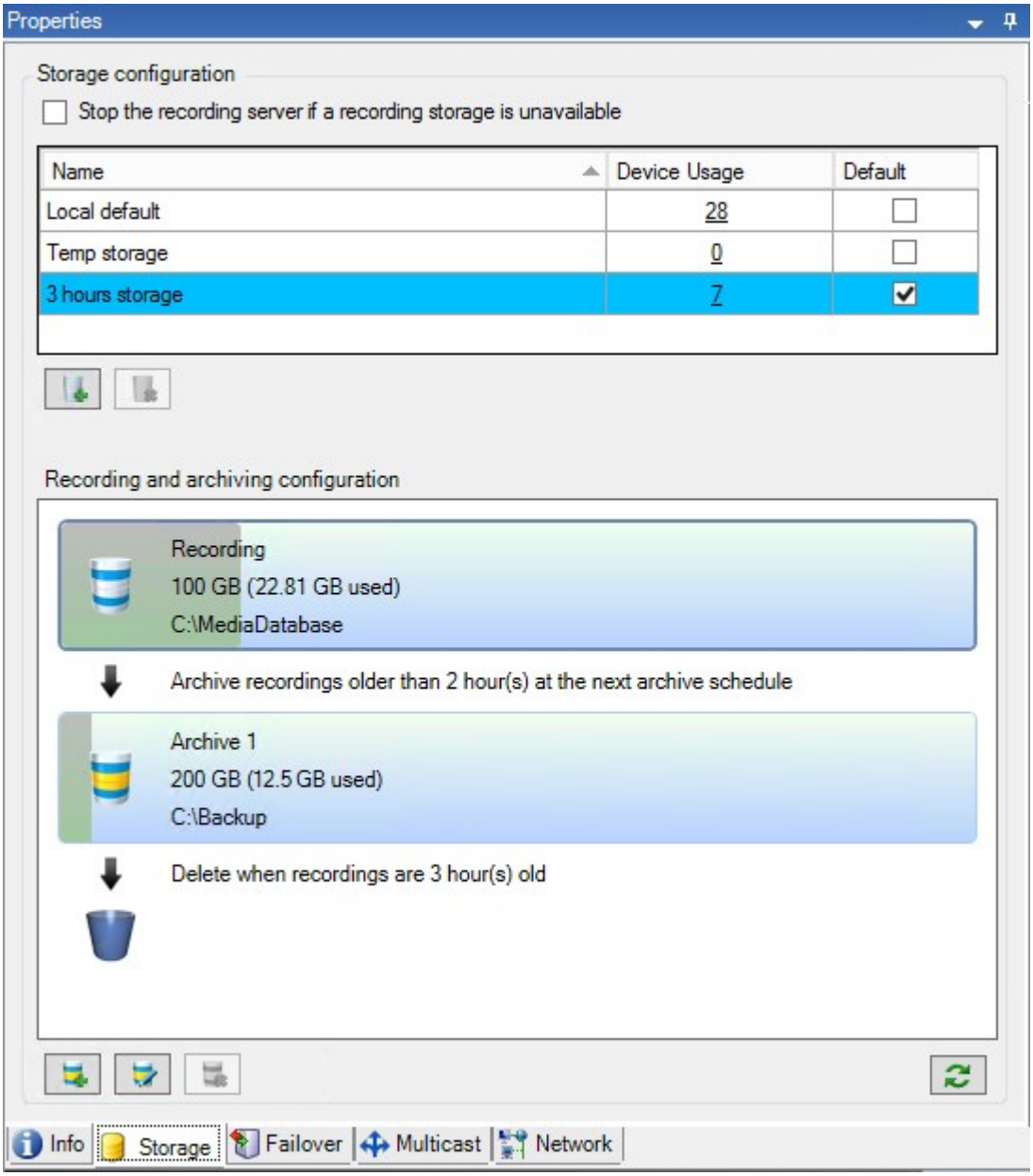
저장 및 아카이빙(설명)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

저장소 탭에서 선택한 레코딩 서버의 저장소를 설정, 관리 및 확인이 가능합니다.

레코딩 저장소 및 아카이브에 대해서는 수평 표시줄에서 현재 여유 공간을 보여줍니다. 레코딩 저장소를 사용할 수 없는 경우 레코딩 서버의 동작을 결정해 줄 수 있습니다. 이는 대부분 시스템에 장애 조치 서버가 있는 경우와 관련 있습니다.

증거물 잠금 을 사용하는 경우, 증거물 잠금 바닥글에 사용된 공간을 보여주는 빨간색 새로 선이 나타납니다.



카메라가 비디오 또는 오디오를 기록하면 지정된 모든 기록물이 기본 설정에 따라 그 장치용으로 지정된 저장소에 저장됩니다. 각 저장소는 기록물을 녹화 데이터베이스인 **Recording** 에 저장하는 레코딩 스토리지로 구성되어 있습니다. 저장소에는 기본 아카이브가 없지만 새로 만들 수 있습니다.

레코딩 데이터베이스가 가득 찬 채로 구동되는 것을 방지하기 위해 추가 저장소를 생성할 수 있습니다(페이지 182의 새로운 저장소 추가 참조). 또한 각 저장소 내에 아카이브를 생성하고(페이지 183의 저장소 내에 아카이브 생성 참조) 데이터 저장을 위한 아카이브 프로세스를 시작할 수 있습니다.

아카이브는 예를 들어 카메라의 녹화 데이터베이스에서 다른 위치로 레코딩을 자동 전송합니다. 이러한 방식으로 저장할 수 있는 레코딩의 크기가 레코딩 데이터베이스 크기로 제한되지 않습니다. 아카이브를 사용하면 레코딩을 다른 미디어로 백업할 수도 있습니다.

레코딩 서버에 대해 저장소와 아카이브를 구성합니다.

아카이브된 레코딩을 로컬로 또는 액세스 가능한 네트워크 드라이브에 저장하면 XProtect Smart Client 를 사용하여 해당 레코딩을 볼 수 있습니다.

디스크 드라이브가 고장나서 레코딩 저장소를 사용할 수 없게 되면 가로 표시줄이 빨간색으로 바뀝니다. XProtect Smart Client 에서 라이브 비디오를 볼 수는 있지만, 디스크 드라이브가 복원 될 때까지는 레코딩 및 아카이빙이 중지됩니다. 시스템이 장애 조치 레코딩 서버로 구성되어 있다면 레코딩 서버의 실행이 중지되도록 지정하여 장애 조치 서버가 인계받도록 할 수 있습니다(페이지 181의 레코딩 저장소를 사용할 수 없을 때 행동 지정 참조).

다음에서는 주로 카메라와 비디오가 언급되나, 스피커, 마이크, 오디오 및 사운드도 적용됩니다.

Milestone 은(는) 레코딩 저장소와 아카이브의 디스크 성능 저하를 방지할 수 있도록 전용 하드 디스크 드라이브 사용을 권장합니다. **하드 디스크를 포맷할 때** 할당 단위 크기 설정을 4 킬로바이트에서 64 킬로바이트로 변경해야 합니다. 이렇게 하면 하드 디스크의 레코딩 성능이 크게 개선됩니다. Microsoft 웹 사이트(https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95)에서 할당 단위 크기에 대한 자세한 내용을 읽고 도움말을 찾아볼 수 있습니다.

여유 공간이 5GB 미만이 되면 데이터베이스에서 가장 오래된 데이터가 항상 자동 아카이브됩니다(또는 다음 아카이브가 정의되지 않은 경우 삭제됨). 여유 공간이 1GB 미만일 경우, 데이터가 삭제됩니다. 데이터베이스에는 항상 250MB의 여유 공간이 필요합니다. 데이터 삭제 속도가 느린 이유로 이 제한에 도달하면 데이터베이스에 대한 쓰기 시도가 실패할 수 있으며 이 경우 충분한 공간을 확보할 때까지 데이터베이스에 더 이상 데이터가 기록되지 않습니다. 데이터베이스의 실제 최대 크기는 지정한 기가바이트 크기에서 5GB를 뺀 값에 해당합니다.

FIPS비 규격 암호로 암호화된 2017 R1 이전의 XProtect VMS 버전의 내보내기와 저장된 미디어 데이터베이스가 있는 FIPS 140-2 규격 시스템의 경우, FIPS를 활성화한 후에도 액세스할 수 있는 위치에 데이터를 저장해야 합니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

저장소에 장치 연결

레코딩 서버에 대한 저장소와 아카이브를 구성한 후에는 개별 카메라 또는 카메라 그룹에 대한 저장소와 아카이브를 활성화할 수 있습니다. 이 작업은 개별 장치 또는 장치 그룹에서 수행하게 됩니다. 페이지 183의 저장소에 장치 또는 장치 그룹 연결를 참조하십시오.

효과적인 아카이브

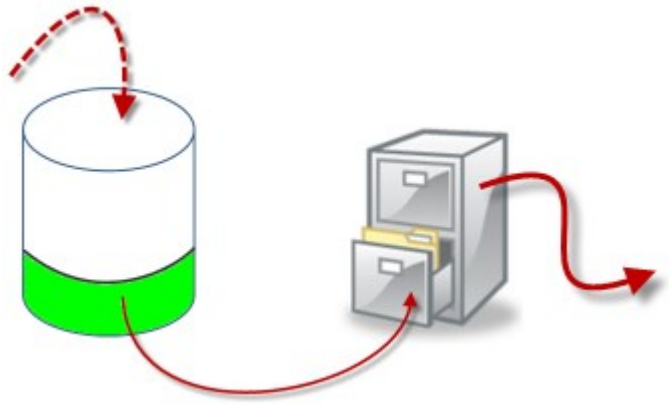
카메라 또는 카메라 그룹에 대한 아카이브를 활성화하면, 정의한 간격에 따라 레코딩 저장소의 내용이 먼저 아카이브로 자동으로 이동합니다.

요구 조건에 따라, 각 저장소에 대해 하나 이상의 아카이브를 구성할 수 있습니다. 아카이브는 레코딩 서버 컴퓨터 자체에 위치하거나 시스템에서 접근할 수 있는 다른 위치(예: 네트워크 드라이브)에 있을 수 있습니다.

아카이빙을 효과적인 방식으로 설정함으로써 저장소를 최적화할 수 있습니다. 경우에 따라 보관한 레코딩이 특히 장기간 보관할 경우 가능한 적은 공간을 차지하게 하고 싶을 때가 있습니다. 이는 이미지 품질을 약간 저하시키는 것만으로 가능할 수 있습니다. 여러 상호의존적인 설정을 조정함으로써 레코딩 서버의 **저장소** 탭에서 아카이빙 작업을 효과적으로 처리할 수 있습니다:

- 레코딩 저장소 보존
- 레코딩 저장소 크기
- 아카이브 보존
- 아카이브 크기
- 아카이브 일정
- 암호화
- 초당 프레임 수(FPS).

크기 필드에서는 레코딩 저장소(실린더로 표시)와 아카이브 크기를 각각 정의합니다:



레코딩 저장소의 보존 시간 및 크기 설정을 이용하여(실린더의 백색 영역으로 예시됨), 아카이브하기 전까지 레코딩을 얼마나 오래 보존해야 하는지를 정의할 수 있습니다. 이 예제에서 아카이브할 정도로 충분히 오래되었을 때 레코딩을 아카이브합니다.

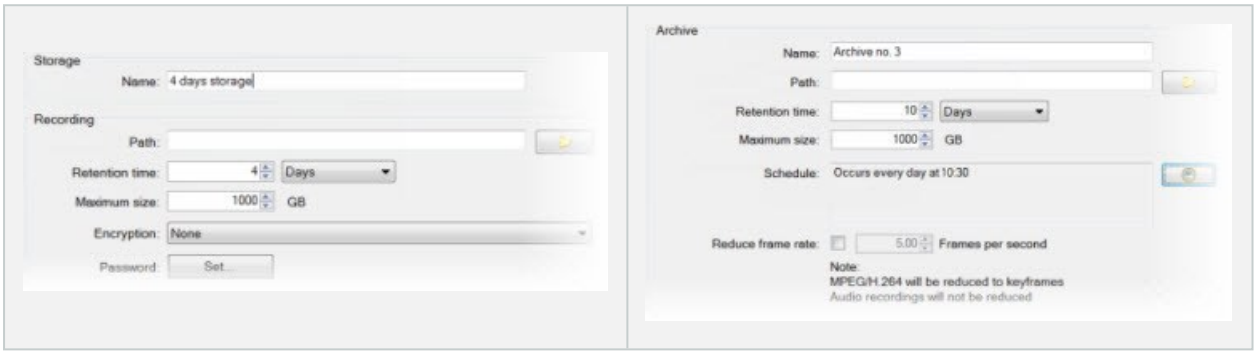
아카이브의 보존 시간과 크기 설정은 레코딩이 아카이브에서 유지되는 시간 길이를 정의합니다. 레코딩은 지정된 시간 동안 또는 아카이브가 지정된 크기 제한에 도달할 때까지 아카이브에 유지됩니다. 이러한 설정이 충족하면 시스템이 아카이브에서 오래된 레코딩을 덮어쓰기 시작합니다.

아카이브 일정은 아카이브가 발생하는 빈도와 횟수를 정의합니다.

FPS는 데이터베이스에서 데이터의 크기를 결정합니다.

레코딩을 아카이브하려면 각각에 따라 이러한 모든 매개변수를 설정해야 합니다. 즉, 다음 번 아카이브의 보존 기간은 항상 현재 아카이브 또는 레코딩 데이터베이스의 보존 기간보다 길어야 합니다. 이는 아카이브에 대해 명시된 보존 일수에 프로세스에서 이전에 명시된 모든 보존이 포함되기 때문입니다. 또한 아카이브는 보존 기간보다 항상 자주 발생해야 합니다. 그렇지 않으면 데이터를 잃을 위험이 있습니다. 보존 기간이 24시간일 경우, 24시간이 지난 데이터는 삭제됩니다. 따라서 데이터를 안전하게 다음 아카이브로 이동하기 위해서는 24시간보다 자주 아카이브를 실행해야 합니다.

예: 이러한 저장소(왼쪽 이미지)의 보존 시간은 4일이고, 다음 아카이브(오른쪽 이미지)의 보존 시간은 10일입니다. 보존 시간보다 훨씬 더 자주 아카이브가 실행되도록 아카이브가 매일 10:30에 발생하도록 설정되었습니다.



또한 규칙 및 이벤트를 사용하여 아카이브를 제어할 수 있습니다.

아카이브 구조(설명됨)

레코딩을 아카이브할 때는 아카이브 내의 특정 하위 디렉토리 구조에 해당 내용이 저장됩니다.

> 시스템의 모든 일반적인 사용 중에, XProtect Smart Client 에서 전체 레코딩을 검색할 때 레코딩이 아카이브되었는지 여부에 상관없이 하위 디렉토리 구조는 시스템 사용자에게 완전히 숨겨집니다. 아카이브된 레코딩을 백업하려는 경우 하위 디렉토리 구조를 파악하는 것이 중요합니다.

레코딩 서버 아카이브 디렉토리 각각에서 시스템이 자동으로 별도의 하위 디렉토리를 생성합니다. 이러한 하위 디렉토리는 장치 및 아카이브 데이터베이스의 이름을 따라 명명됩니다.

동일 아카이브에 다른 카메라의 레코딩을 저장할 수 있고, 각 카메라의 아카이브가 정기적으로 수행될 가능성이 있으므로 또 다른 부가 하위 디렉토리 역시 자동으로 추가됩니다.

이러한 하위 디렉토리 각각은 약 1시간 분량의 레코딩을 나타냅니다. 1시간 분량으로 분할되므로 허용된 최대 아카이브 크기에 도달한 경우 아카이브 데이터에서 비교적 적은 부분만 삭제될 수 있습니다.

하위 디렉토리는 장치 이름을 따서 명명되고, 그 다음에 레코딩 카메라의 위치(에지 저장소 또는 SMTP를 통해) **와** 하위 디렉토리에 포함된 가장 최근 데이터베이스의 날짜와 시간이 표시됩니다.

명명 구조

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

에지 저장소의 경우:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

SMTP의 경우:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

실제 예시

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

하위 디렉토리

또 다른 부가 하위 디렉토리가 자동으로 추가됩니다. 이러한 하위 디렉토리의 수와 특성은 실제 레코딩의 특성에 달라집니다. 예를 들어, 레코딩이 기술적으로 시퀀스에 따라 분할된 경우 여러 개의 다른 하위 디렉토리가 추가됩니다. 모션 감지를 사용하여 레코딩을 트리거한 경우가 흔히 이러한 경우에 해당됩니다.

- **미디어**: 이 폴더에는 비디오 또는 오디오(둘 모두는 아님)인 실제 미디어가 들어 있습니다
- **MotionLevel**: 이 폴더에는 당사의 모션 감지 알고리즘을 이용하여 비디오 데이터로부터 생성된 모션 레벨 그리드가 포함되어 있습니다. 이 데이터를 통해 XProtect Smart Client 의 스마트 검색 기능이 매우 빠른 검색을 수행할 수 있습니다.
- **모션**: 이 폴더에는 시스템이 모션 시퀀스를 저장합니다. 모션 시퀀스는 비디오 데이터에서 모션이 감지되는 시간 조각입니다. 이 정보는 예를 들어 XProtect Smart Client 에서 타임라인에 이용됩니다.
- **녹화**: 이 폴더에는 시스템이 레코딩 시퀀스를 저장합니다. 레코딩 시퀀스는 미디어 데이터의 통합 레코딩이 들어 있는 시간 조각입니다. 이 정보는 예를 들어 XProtect Smart Client 에서 타임라인을 그리는 데 이용됩니다.
- **서명**: 이 폴더에는 미디어 데이터(Media 폴더에 있음)에 대해 생성된 서명을 저장합니다. 이 정보를 이용해 미디어 데이터가 레코딩된 이후에 조작되었는지 여부를 확인할 수 있습니다

아카이브를 백업하려는 경우, 하위 디렉토리 구조에 대한 기본적인 내용을 알고 있으면 백업의 대상을 지정할 수 있습니다.
백업의 예시:

전체 아카이브 내용을 백업하려면 필요한 아카이브 디렉토리와 해당하는 모든 내용을 백업합니다. 예를 들어, 다음에 있는 모든 항목을 백업합니다.

```
...F:\OurArchive\
```

일정 기간 동안 특정 카메라의 레코딩을 백업하려면 해당하는 하위 디렉토리의 내용만 백업합니다. 예를 들어, 다음에 있는 모든 항목을 백업합니다.

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

사전 버퍼링 및 레코딩 저장소(설명됨)

사전 버퍼링은 실제 트리거 이벤트가 발생하기 전에 오디오와 비디오를 레코딩하는 기능입니다. 이 기능은 레코딩을 트리거하는 이벤트(예: 도어 열기)의 원인이 되는 오디오 또는 비디오 레코딩을 원할 때 유용합니다.

사전 버퍼링은 시스템이 연결된 장치에서 오디오 및 비디오 스트림을 연속해서 수신하고, 정의된 사전 버퍼 기간 동안 해당 스트림을 일시적으로 저장하기 때문에 가능합니다.

- 레코딩 규칙이 트리거되면 규칙에 구성된 사전 레코딩 시간에 해당하는 임시 레코딩이 영구 레코딩으로 바뀝니다
- 레코딩 규칙이 트리거되지 않으면 사전 버퍼의 임시 레코딩은 정의된 사전 버퍼 시간 후 자동으로 삭제됩니다

임시 사전 버퍼 레코딩 저장소

임시 사전 버퍼 레코딩의 저장 위치를 선택할 수 있습니다.

- 메모리 내; 사전 버퍼 기간이 15초로 제한됩니다.
- 디스크상(미디어 데이터베이스 내); 모든 값을 선택할 수 있습니다.

디스크 대신 메모리에 저장하면 시스템 성능이 개선되지만, 사전 버퍼 기간이 더 짧은 경우에만 가능합니다.

레코딩이 메모리에 저장되고 임시 레코딩의 일부를 영구적으로 설정하면 남은 임시 레코딩이 삭제되고 복원할 수 없게 됩니다. 남은 레코딩을 보존해야 할 경우, 해당 레코딩을 디스크에 저장하십시오.

인증

Active Directory(설명됨)

Active Directory는 Microsoft 에서 Windows 도메인 네트워크용으로 구현한 분산 디렉토리 서비스입니다. 대부분의 Windows Server운영 체제에 포함되어 있습니다. 사용자 또는 응용 프로그램이 액세스할 수 있도록 네트워크상에 있는 리소스를 식별합니다.

Active Directory가 설치되어 있으면 Active Directory에서 Windows 사용자를 추가할 수 있지만 Active Directory 없이도 기본 사용자를 추가하는 옵션이 있습니다. 기본 사용자와 관련하여 특정한 시스템 제한이 있습니다.

사용자(설명됨)

사용자 라는 용어는 기본적으로 해당 클라이언트를 통해 감시 시스템에 연결하는 사용자를 말합니다. 두 가지 방식으로 이러한 사용자를 구성할 수 있습니다:

- 사용자 이름/암호 조합으로 인증을 받는 **기본 사용자**
- Windows 로그인을 바탕으로 인증을 받는 **Windows 사용자**

Windows 사용자

Active Directory를 사용하여 Windows 사용자를 추가합니다. Active Directory (AD)는 Microsoft에서 Windows 도메인 네트워크용으로 구현한 디렉토리 서비스입니다. 대부분의 Windows Server운영 체제에 포함되어 있습니다. 사용자 또는 응용 프로그램이 액세스할 수 있도록 네트워크상에 있는 리소스를 식별합니다. Active Directory는 사용자 및 그룹 개념을 사용합니다.

사용자는 사용자 계정을 가진 개인을 나타내는 Active Directory 개체입니다. 예:

그룹은 여러 사용자를 포함한 Active Directory 개체입니다. 이 예에서 관리 그룹에는 3명의 사용자가 있습니다:

그룹에는 하나 또는 여러 명의 사용자가 포함될 수 있습니다. 시스템에 그룹을 추가하여 모든 구성원을 한 번에 추가할 수 있습니다. 그룹을 시스템에 추가한 후에는 나중에 추가한 신규 구성원이나 제거한 이전 구성원 등 Active Directory의 그룹에 적용한 모든 변경 내용이 즉시 시스템에 반영됩니다. 사용자는 한 번에 둘 이상의 그룹 구성원이 될 수 있습니다.

Active Directory를 사용하여 기존 사용자 및 그룹 정보를 시스템에 추가할 수 있으며 다음과 같은 몇 가지 이점을 얻을 수 있습니다:

- 사용자와 그룹은 Active Directory에서 중앙 집중적으로 지정되므로 처음부터 사용자 계정을 만들 필요가 없습니다
- Active Directory가 인증을 처리하므로 시스템에서 사용자 인증을 구성할 필요가 없습니다

Active Directory 서비스를 통해 사용자와 그룹을 추가하기 전에 네트워크에 Active Directory가 설치된 서버가 있어야 합니다.

기본 사용자

귀하의 시스템이 Active Directory에 대한 액세스가 없는 경우, 기본 사용자를 생성하십시오. 기본 사용자 설정 방법에 관한 정보는 페이지 266의 기본 사용자 만들기를 참조하십시오.

Identity Provider (설명됨)

Identity Provider app pool (IDP) 은(는) 기본 사용자에 대한 신원 확인 정보를 생성, 유지 및 관리하는 시스템 개체입니다.

Identity Provider 은(는) 다음과 같은 경우에 의존하는 애플리케이션 또는 서비스에 인증 및 등록 서비스도 제공합니다. 레코딩 서버, 관리 서버, Data Collector 및 보고 서버.

기본 사용자로 XProtect 클라이언트 및 서비스에 로그인하면 요청이 Identity Provider(으)로 전달됩니다. 인증되면 사용자는 관리 서버를 호출할 수 있습니다.

Identity Provider은(는) 별도의 데이터베이스가 있는 동일한 SQL Server을(를) 사용하는 관리 서버의 일부로서 IIS에서 실행되며, 통신할 때 서비스가 사용하는 OAuth 통신 토큰(Surveillance_IDP)을 생성하고 처리하는 역할을 합니다.

Identity Provider 로그는 다음 항목에서 찾을 수 있습니다. `\\ProgramData\Milestone\IDP\Logs`

외부 IDP(설명됨)

IDP 은(는) Identity Provider 의 약어입니다. 외부 IDP는 사용자 ID 정보를 저장하고 관리하며 다른 시스템에 사용자 인증 서비스를 제공하는 외부 응용 프로그램과 서비스입니다. 외부 IDP를 XProtect 비디오 관리 소프트웨어와 연결할 수 있습니다.

XProtect VMS은 OpenID 연결(OIDC)과 호환되는 외부 IDP를 지원합니다.

클레임(설명됨)

클레임은 외부 IDP와 XProtect VMS 간의 링크를 형성합니다.

클레임은 사용자 또는 응용 프로그램과 같은 엔터티가 만드는 명령문입니다. XProtect VMS에서, 클레임은 사용자의 XProtect 권한을 결정하는 역할과 연결될 수 있습니다.

클레임은 클레임 이름과 클레임 값으로 구성된 키 값입니다. 예를 들어 클레임은 클레임 값 콘텐츠를 설명하는 일반적인 이름일 수 있으며, 클레임 값은 그룹명일 수 있습니다. 외부 IDP의 클레임에 대한 추가 예를 참조하십시오. 외부 IDP의 클레임 예시 에서 확인하십시오.

외부 IDP의 XProtect VMS에 대한 로그인 권한을 사용자에게 부여하기

- 외부 IDP에서 사용자를 생성합니다. 또한 XProtect 비디오 관리 소프트웨어와 XProtect와(과) 외부 IDP 간의 상호작용을 식별해야 합니다. 마지막으로 XProtect 비디오 관리 소프트웨어에서 사용자를 외부 IDP 사용자로 식별하는 클레임을 만듭니다.
- XProtect VMS에서 Identity Provider이(가) 외부 IDP에 연결할 수 있도록 구성을 만듭니다. 외부 IDP에 대한 구성을 만드는 방법에 대한 자세한 내용은 외부 IDP 추가 및 구성을 참고하십시오.
- XProtect VMS에서 사용자 클레임을 외부 IDP에서 XProtect 역할로 매핑하여 사용자 인증을 설정합니다. 클레임을 역할에 매핑하는 방법에 관한 자세한 내용은 Map claims from an external IDP to roles in XProtect를 참조하십시오.

URI 리디렉션

URI 리디렉션은 인증에 성공한 후 사용자가 전송되는 페이지를 지정합니다. 외부 IDP에서 관리 서버의 주소를 정의한 후에 XProtect Management Client에서 정의한 **콜백 경로**를 추가해야 합니다. 예: https://management-server-computer.company.com/idp/signin-oidc

외부 IDP 사용자의 고유 사용자 이름

외부 IDP를 통해 Milestone XProtect에 로그인하는 사용자에 대해 사용자 이름이 자동으로 생성됩니다.

외부 IDP는 XProtect의 사용자에게 자동으로 이름을 생성해주는 클레임 세트를 제공하며, XProtect에서는 VMS 데이터베이스에서 특별한 외부 IDP에서 나온 이름을 선택하는데 알고리즘이 사용됩니다.

외부 IDP의 클레임 예시에서 확인하십시오.

클레임은 클레임 이름과 클레임 값으로 구성됩니다. 예:

클레임 이름	클레임 값
name	Raz Van
email	123@domain.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_username	321@domain.com
vmsRole	운영자
locale	en-US
given_name	Raz
family_name	Lindberg
zoneinfo	America/Los_Angeles
email_verified	참

클레임 일련 번호를 사용하여 XProtect 에서 사용자 이름 생성

XProtect 에서, XProtect VMS에서 사용자 생성 시 검색 우선 순위는 아래 표에 있는 클레임 일련 번호에 따라 제어됩니다. 가장 먼저 이용 가능한 클레임 이름이 XProtect VMS에서 사용됩니다.

클레임 이름	일련 번호	설명
UserNameClaimType	1	사용자 이름 정의를 위한 하나의 클레임과의 구성된 매핑. 클레임은 **도구** > **옵션** 아래 **외부 IDP** 탭의 **사용자 이름 생성에 사용할 클레임** 필드에서 정의된 것입니다.
preferred_username	2	외부 IDP에서 올 수 있는 클레임. Oidc(OpenID Connect)에서 이를 위해 일반적으로 사용되는 표준 클레임입니다.
name	3	
given_name family_name	4	Bob Johnson과 같은 성과 이름의 조합.
email	5	
가장 먼저 이용할 수 있는 클레임 + #(가장 먼저 이용할 수 있는 숫자)	6	예를 들어, Bob#1

XProtect 에서의 사용자 이름 생성을 위한 특정 클레임 정의

XProtect 관리자는 XProtect VMS에서 사용자 이름 생성에 사용되어야 하는 외부 IDP에서 특정 클레임을 정의할 수 있습니다. 관리자가 XProtect VMS에서 사용자 이름 생성에 사용하기 위해 클레임을 정의할 때, 그러한 클레임은 외부 IDP에서 나온 클레임 이름과 정확히 일치하도록 입력해야 합니다.

- 사용자 이름에 사용할 클레임은 **도구** > **옵션** 아래 **외부 IDP** 탭의 **사용자 이름 생성에 사용할 클레임** 필드에서 정의된 것입니다.

외부 IDP 사용자 삭제

외부 IDP 로그인으로 XProtect에서 생성된 사용자는 기본 사용자와 같은 방식으로 삭제할 수 있으며 그러한 사용자는 생성 후 언제든지 삭제할 수 있습니다.

사용자가 XProtect에서 삭제되고 해당 사용자가 외부 IDP에서 다시 로그인하면, XProtect에서 새로운 사용자가 생성됩니다. 그러나 XProtect 의 사용자와 관련된 데이터(예: 개인 뷰 및 역할)은 상실되며 이 정보는 XProtect 에서의 사용자를 위해 다시 생성되어야 합니다.

Management Client에서 외부 IDP가 삭제되면 외부 IDP를 통해 VMS에 연결된 모든 사용자도 삭제됩니다.

보안

역할 및 역할의 권한(설명됨)

Milestone XProtect VMS에 있는 모든 사용자는 하나의 역할을 가지고 있습니다.

역할은 사용자가 액세스할 수 있는 장치를 포함하여 사용자의 권한을 정의합니다. 또한, 역할은 비디오 관리 시스템에서의 보안과 액세스 권한을 정의합니다.

이 시스템에는 모든 시스템 기능에 대해 전체 액세스 권한이 있는 기본 **관리자** 역할이 제공되지만, 대부분은 사용자 및 이들이 가져야 하는 액세스 권한을 구별하기 위해 시스템에 두 개 이상의 역할이 필요합니다. 필요한 만큼 역할을 추가할 수 있습니다. 페이지 265의 역할에 사용자 및 그룹 할당/제거를 참조하십시오.

예를 들어, 사용자가 액세스하도록 하고 싶은 장치에 따라 또는 사용자 간에 차이를 두어야 하는 비슷한 유형의 제한에 따라 XProtect Smart Client의 사용자에 대해 다른 유형의 역할을 설정하는 것이 필요할 수 있습니다.

사용자 간 차이를 만드려면 다음 작업을 수행해야 합니다.

- 조직의 비즈니스 요구 사항에 맞는 역할을 만들고 설정합니다.
- 속해야 하는 역할에 할당한 사용자 및 사용자 그룹을 추가합니다.
- Smart Client 프로필 및 Management Client 프로필을 만들어서 XProtect Smart Client 및 Management Client 사용자 인터페이스에서 사용자가 볼 수 있는 내용을 정의합니다.

  역할은 액세스 권한만 제어하며 사용자가 XProtect Smart Client 또는 Management Client의 사용자 인터페이스에서 볼 수 있는 내용은 제어하지 않습니다. Management Client를 절대로 사용하지 않을 사용자를 위해 특정한 Management Client 프로필을 만들 필요는 없습니다.

Management Client 기능에 액세스가 제한된 XProtect Smart Client 사용자나 Management Client 사용자에게 최상의 사용자 환경을 제공하려면 역할에서 제공하는 권한과 Smart Client 또는 Management Client 프로필에서 제공하는 사용자 인터페이스 요소 사이에 일관성이 있는지 확인해야 합니다.

> ⚠ Management Server에 액세스하려면, 모든 역할이 **연결** 보안 권한을 활성화된 상태를 가지고 있는 것이 중요합니다. 이 권한은 **역할 설정** > **Management Server** > 페이지 465의 전체 보안 탭(역할)에 있습니다.

시스템에서 역할을 설정하려면 **보안** > **역할** 을 확장합니다.

역할의 권한

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

시스템에서 역할 생성 시, 시스템 구성 요소 또는 관련된 역할이 액세스하고 사용할 수 있는 기능에 대해 일련의 권한을 역할에 부여할 수 있습니다.

예를 들어, XProtect Smart Client 또는 다른 Milestone 보기 클라이언트의 기능에 대해 액세스하는 권한만 보유하고 특정 카메라만 볼 수 있는 권한을 보유한 역할을 생성하고 싶을 수도 있습니다. 그러한 역할을 생성하는 경우, 이러한 역할은 Management Client 을(를) 액세스하고 사용할 권한이 없어야 하지만, XProtect Smart Client 또는 다른 클라이언트에 있는 일부 또는 모든 기능에만 액세스하도록 해야 합니다.

이러한 차이를 두려면, 일부 또는 가장 일반적인 관리자 권한을 보유한 역할을 설정합니다.(예: 카메라, 서버, 비슷한 기능을 추가 및 삭제할 권한). 시스템 관리자의 일부 또는 대부분의 권한을 보유한 역할을 생성할 수 있습니다. 예를 들어, 조직이 시스템 하위 세트를 관리할 수 있는 직원과 전체 시스템을 관리할 수 있는 직원을 구분하길 원하는 경우가 해당될 수 있습니다.

역할은 다양한 시스템 기능에 액세스, 편집 또는 변경할 수 있는 차별화된 관리자 권한을 제공할 수 있는 기능을 제공합니다. 예를 들면, 시스템의 서버나 카메라에 대한 설정을 편집하는 권한입니다. **전반적인 보안** 탭에서 이러한 권한을 지정합니다(페이지 465의 전체 보안 탭(역할) 참고). 차별화된 시스템 관리자가 Management Client을(를) 실행할 수 있도록 해당 역할에 대해 관리 서버에서 읽기 권한을 부여해야 합니다.

> Management Server에 액세스하려면, 모든 역할이 **연결** 보안 권한을 활성화된 상태를 가지고 있는 것이 중요합니다. 이 권한은 **역할 설정** > **Management Server** > 페이지 465의 전체 보안 탭(역할)에 있습니다.

또한 역할을 사용자 인터페이스에서 해당 시스템 기능을 제거한 Management Client 프로파일과 연결함으로써 각 역할에 대해 Management Client 의 사용자 인터페이스에서 동일한 제한을 반영할 수 있습니다. 자세한 정보는 페이지 68의 Management Client 프로필(설명됨)를 참조하십시오.

역할에 이와 같이 차별화된 관리자 권한을 부여하려면 기본적인 전체 관리자 역할을 가진 사람이 **보안** > **역할** > **정보 탭** > **새로 추가** 에서 역할을 설정해야 합니다. 새 역할을 설정했으면, 시스템의 다른 역할을 설정할 때와 유사하게 해당 역할을 사용자 본인의 프로파일에 연결할 수 있습니다. 그렇지 않으면 시스템의 기본 프로파일을 사용합니다. 자세한 정보는 페이지 264의 역할 추가 및 관리를 참조하십시오.

역할을 연결할 프로필을 지정한 후에는 **전체 보안** 탭으로 이동하여 역할의 권한을 지정합니다.

> 역할에 대해 설정할 수 있는 권한은 제품 사이에서 서로 다릅니다. XProtect Corporate 에서 역할에만 이용 가능한 모든 권한을 부여할 수 있습니다.

사생활 보호(설명됨)

사생활 보호(설명됨)

사생활 보호를 이용해, 클라이언트에 표시될 때 사생활 보호 처리를 원하는 카메라의 비디오 영역을 정의할 수 있습니다. 예를 들어, 감시 카메라가 거리를 촬영하는 경우, 거주민의 사생활 보호를 위해 사생활 보호 기능을 사용하여 건물의 특정 영역(예: 창문과 문)을 가릴 수 있습니다. 일부 국가에서, 이는 법적 요구사항입니다.

진하게 또는 흐리게 사생활 보호를 지정할 수 있습니다. 보호 처리는 라이브, 레코드 및 내보내기 비디오에서 모두 가능합니다.

사생활 보호는 카메라 이미지 영역에 적용되고 잠김 처리되므로 가려진 영역은 팬-틸-줌 동작을 따르지 않지만 카메라 이미지의 동일한 영역을 지속적으로 커버합니다. 일부 PTZ 카메라에서는 카메라 자체에 위치 기반 사생활 보호를 활성화할 수 있습니다.

두 가지 유형의 사생활 보호가 있습니다.

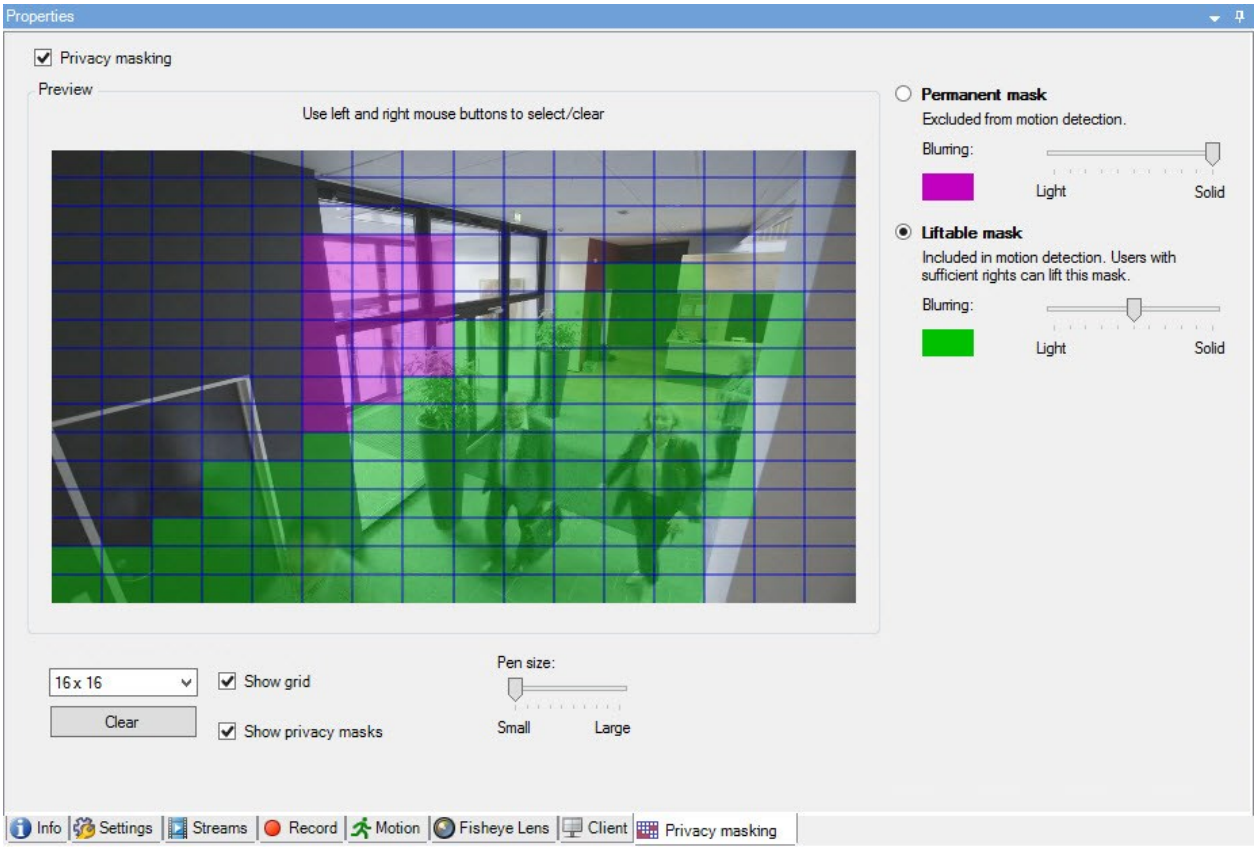
- **영구 사생활 보호**: 이 유형의 보호 영역은 항상 클라이언트에서 가려집니다. 공공 구역이나 감시가 허용되지 않는 영역 같이 감시가 필요하지 않은 비디오 영역에 적용하기 위해 사용할 수 있습니다. 모션 감지는 영구 사생활 보호를 갖는 영역에서 제외됩니다
- **해제 가능한 사생활 보호**: 이러한 유형의 보호 영역은 사생활 보호 해제 권한을 가진 사용자에 의해 XProtect Smart Client 에서 일시적으로 감시 해제될 수 있습니다. 로그인한 XProtect Smart Client 사용자가 사생활 보호 해제 권한이 없을 경우, 시스템은 해제를 승인할 권한을 가진 사용자에게 요청합니다.
  사생활 보호는 타임 아웃되거나 사용자가 이를 다시 적용할 때까지 해제됩니다. 사생활 보호는 사용자가 액세스 권한을 가진 모든 카메라의 비디오에서 해제된다는 점을 유의하십시오

사생활 보호가 적용된 2017 R3 이하 버전의 시스템에서 업그레이드하는 경우, 보호는 해제 가능 보호로 변환됩니다.

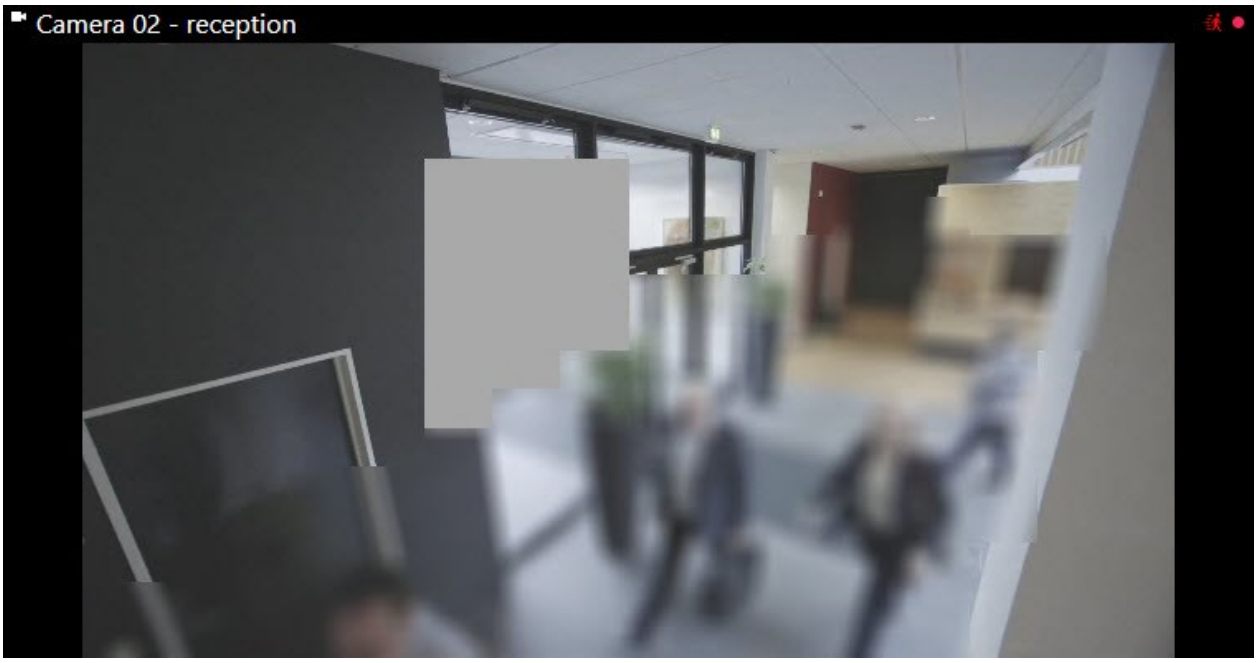
사용자가 클라이언트에서 레코드된 비디오를 내보내기하거나 재생할 경우에는, 나중에 사생활 보호를 변경하거나 제거하더라도 비디오에는 레코딩 시 구성된 사생활 보호가 포함됩니다. 내보내기할 때 사생활 보고가 해제된 경우, 내보낸 비디오는 해제 가능 사생활 보호를 포함하지 **않습니다**.

일주일에 한 번씩 등 자주 사생활 보호 설정을 변경하는 경우, 시스템이 잠재적으로 과부하될 수 있습니다.

사생활 보호가 구성된 **사생활 보호** 탭의 예:



그리고 클라이언트에 표시되는 방식:



클라이언트 사용자에게 영구 및 해제 가능 사생활 보호의 설정에 대해 알릴 수 있습니다.

Management Client 프로필(설명됨)

Management Client 프로파일을 통해 시스템 관리자가 다른 사용자에 Management Client 대한 사용자 인터페이스를 수정할 수 있습니다. 각 관리자 역할에서 사용 가능한 기능을 표시하도록 사용자 인터페이스를 제한하려면 Management Client 프로파일을 해당 역할에 연결합니다.

Management Client 프로필은 실제 액세스가 아닌 시스템 기능의 시각적 표시만 처리합니다. 전반적인 시스템 기능 액세스는 개별 사용자와 연결된 역할을 통해 허용됩니다. 역할에 대한 전반적인 시스템 기능 액세스를 관리하는 방법에 대한 정보는 Management Client 프로파일에 대한 기능 표시 관리 를 참조하십시오.

Management Client 모든 요소의 표시 여부에 대한 설정을 변경할 수 있습니다. Management Client 기본적으로 Management Client 프로파일은 의 모든 기능을 볼 수 있습니다.

Smart Client 프로필(설명됨)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

Milestone XProtect VMS의 모든 사용자는 Smart Client 프로필이 연결된 역할을 가지고 있습니다.

역할은 사용자의 권한을 정의하고 Smart Client 프로필은 사용자가 XProtect Smart Client 사용자 인터페이스에서 볼 수 있는 내용을 정의합니다.

모든 Milestone XProtect VMS 설치에는 조직의 시스템에서 사용 가능한 대부분의 구성을 표시하기 위해 기본 구성으로 설정된 Smart Client 프로필이 포함되어 있습니다. 이 포함되어 있습니다.일부 설정은 기본 설정으로 항상 비활성화되어 있습니다.

조직에 여러 개의 다른 역할이 있는 경우에는 특정 역할이 XProtect Smart Client에 액세스할 수 없거나 액세스하면 안 되는 기능을 비활성화하고 싶어질 수도 있습니다.

예를 들어, 비디오 재생을 실행할 필요가 없는 일상적인 작업 의 역할을 가지고 있는 경우가 있을 수 있습니다. 이러한 목적을 위해서는 **재생** 모드를 비활성화하는 역할에 대한 새 Smart Client 프로필을 만들 수 있습니다. Smart Client 프로필에서 이 설정을 비활성화하면 이 Smart Client 프로필을 사용하는 역할을 가진 XProtect Smart Client 사용자는 더 이상 XProtect Smart Client 사용자 인터페이스에서 **재생** 모드를 볼 수 없습니다.

Smart Client 프로필은 사용자가 XProtect Smart Client 사용자 인터페이스에서 볼 수 있는 내용을 대부분 제어하고 역할의 실제 액세스 권한을 제어하지 않는다는 점을 유의하는 것이 중요합니다. 읽기, 수정 또는 삭제에 대한 액세스 등, 이러한 액세스 권한은 역할 설정에서 제어됩니다. 그러므로 XProtect Smart Client 사용자는 Smart Client 프로필에서 비활성화되어 있기 때문에 사용자 인터페이스에서 볼 수 없는 역할을 통해 기능에 대한 권한을 가질 수 있습니다.

XProtect Smart Client 사용자에게 최상의 사용자 환경을 제공하려면, 역할에서 제공하는 권한과 Smart Client 프로필에서 제공하는 사용자 인터페이스 요소 사이에 일관성이 있는지 확인해야 합니다.

Smart Client 프로필을 만들거나 편집하려면 **클라이언트**를 확장하여 **Smart Client프로필**을 선택합니다.

또한 Smart Client 프로필, 역할 및 시간 프로파일 간의 관계와 이러한 프로필을 함께 사용하는 방식에 대한 자세한 내용을 살펴볼 수 있습니다(페이지 242의 Smart Client 프로필과 역할, 시간 프로필 생성 및 설정 참조).

증거물 잠금(설명됨)

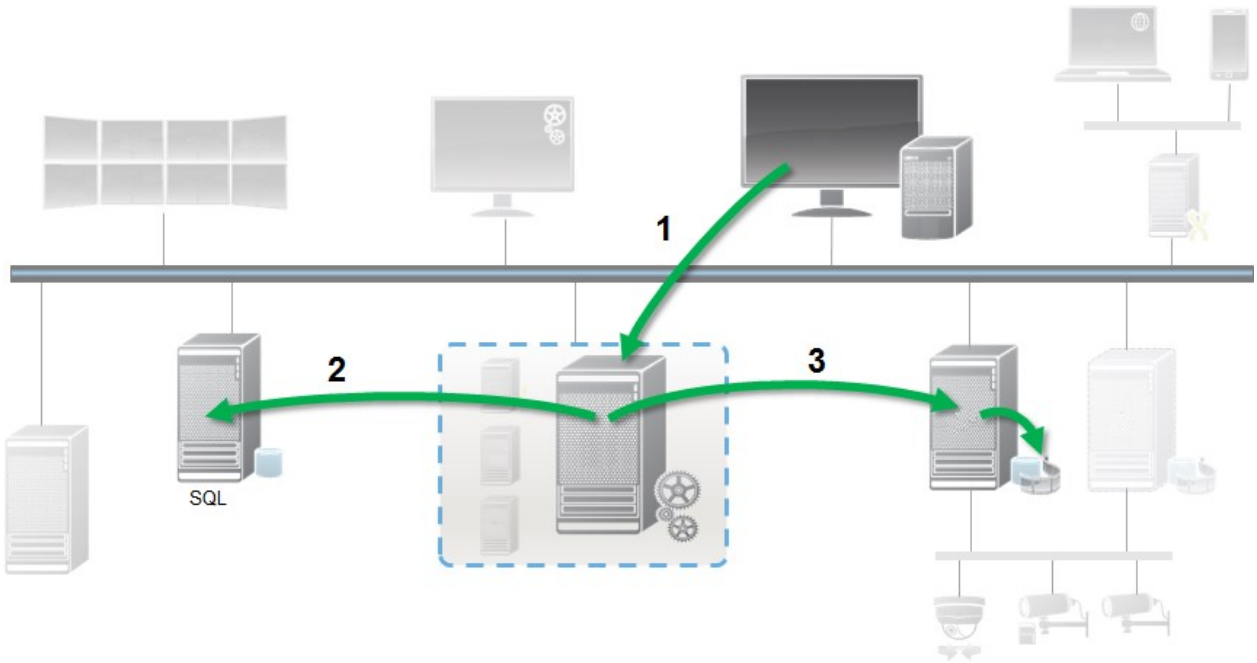
사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

XProtect VMS버전 2020 R2부터, 이전 버전에서 관리 서버를 업그레이드하면, 이러한 레코딩 서버를 업그레이드하기 전까지는 2020 R1 또는 그 이전 버전인 레코딩 서버상의 증거물 잠금을 생성하거나 수정할 수 없게됩니다.
이는 또한 한 레코딩 서버(2020 R1 또는 그 이전 버전)에서 다른 레코딩 서버로 하드웨어를 이전한 경우, 그리고 여전히 하드웨어에 레코딩이 담겨 있는 경우, 증거물 잠금이 생성되거나 수정될 수 없음을 의미합니다.

증거물 잠금 기능을 사용하면 클라이언트 운영자가 오디오 및 기타 데이터를 포함한 비디오 시퀀스가 필요 시 삭제되지 않도록 보호할 수 있습니다(예: 조사나 평가가 진행 중일 때). 자세한 정보는 XProtect Smart Client 에 관한 사용자 설명서 를 참조하십시오.

데이터가 보호되면 시스템의 기본 보존 시간 후나 기타 상황에서 시스템에 의해 자동으로 또는 클라이언트 사용자에 의해 수동으로 데이터가 삭제될 수 없습니다. 충분한 사용자 권한을 가진 사용자가 증거물 잠금을 해제할 때까지 시스템이나 사용자가 데이터를 삭제할 수 없습니다.

증거물 잠금에 대한 흐름도:



1. XProtect Smart Client사용자가 증거물 잠금을 생성했습니다. 관리 서버로 정보가 보내집니다.
2. Management Server가 증거물 잠금에 관한 정보를 SQL Server 서버에 저장합니다.
3. 관리 서버가 레코딩 서버에 보호된 녹화물을 데이터베이스에 저장하고 보호하라고 알립니다.

운영자가 증거물 잠금을 생성하면 보호된 데이터는 이 데이터가 기록된 레코딩 저장소에서 유지되고 보호된 데이터가 아니라 보호되지 않은 데이터와 함께 아카이브 디스크로 이동됩니다.

- 증거물 잠금에 대해 구성된 보존 시간을 따릅니다. 잠재적으로 무기한
- 비보호 데이터에 대해 정리가 구성된 경우에도 레코딩의 원래 품질을 유지합니다

운영자가 잠금을 생성할 때 최소 시퀀스 크기는 데이터베이스가 기록된 파일을 분할하는 기간이며, 기본적으로 1시간 시퀀스입니다. 이 기본값을 변경할 수 있지만 그러려면 레코딩 서버의 RecorderConfig.xml 파일을 사용자 지정해야 합니다. 작은 시퀀스가 두 개의 1시간 기간에 걸쳐 있는 경우 시스템이 두 기간 모두에서 레코딩을 잠급니다.

Management Client의 감사 로그에서 사용자가 증거물 잠금 생성, 편집 또는 삭제한 시기를 조회할 수 있습니다.

디스크 공간이 부족해지는 경우 보호된 데이터에는 영향을 미치지 않습니다. 그 대신 보호되지 않은 오래된 데이터는 삭제될 것입니다. 삭제할 비보호 데이터가 더 이상 없으면 시스템이 녹화를 중지합니다. 디스크 꽉 참 이벤트에 의해 트리거되는 규칙과 알람을 생성하여 자동 알림을 받을 수 있습니다.

따라서 긴 기간 동안 추가 데이터가 저장되어 디스크 저장소에 영향을 미칠 가능성이 있는 경우를 제외하고 증거물 잠금 기능은 시스템 성능에 영향을 미치지 않습니다.

하드웨어(페이지 314의 하드웨어 이동 참조)를 다른 레코딩 서버로 옮기는 경우:

- 증거물 잠금으로 보호된 레코딩은 증거물 잠금 생성 시 정의된 보존 기간이 설정된 오래된 레코딩 서버에 남게 됩니다.
- XProtect Smart Client사용자는 카메라에서 만든 레코딩이 다른 레코딩 서버로 이동하기 전에 증거물 잠금으로 데이터를 보호할 수 있습니다. 카메라를 여러 번 이동하고 레코딩이 여러 레코딩 서버에 저장되는 경우에도

기본으로 모든 운영자는 기본 증거물 잠금 프로파일을 할당받았으나 해당 기능에 대한 사용자 액세스 권한은 없습니다. 역할에 대해 증거물 잠금 액세스 권한을 지정하려면 역할 설정에 대한 장치 탭(역할) 을 참조하십시오. 역할에 대해 증거물 잠금 프로파일을 지정하려면 정보 탭(역할) 에서 역할 설정에 대한 내용을 참조하십시오.

Management Client에서 기본 증거물 잠금 프로파일의 속성을 편집하고 추가 증거물 잠금 프로파일을 만들어 해당 프로파일을 대신 역할에 할당할 수 있습니다.

규칙 및 이벤트

규칙(설명됨)

규칙은 특정 조건 하에서 수행할 동작을 지정합니다. 예: 모션이 감지될 때(조건) 카메라가 레코딩을 시작합니다(동작).

다음은 규칙으로 할 수 있는 항목에 대한 **예** 입니다.

- 레코딩 시작 및 중지
- 기본이 아닌 라이브 프레임 속도 설정
- 기본이 아닌 레코딩 프레임 속도 설정

- PTZ 순찰 시작 및 중지
- PTZ 순찰 일시 중지 및 다시 시작
- 특정 위치로 PTZ 카메라 이동
- 출력을 활성화/비활성화 상태로 설정
- 이메일을 통해 알림 전송
- 로그 항목 생성
- 이벤트 생성
- 새로운 장치 설정 적용(예: 카메라에 다른 해상도 설정)
- Matrix 수신자에 비디오가 나타나게 설정
- 플러그 인 시작 및 중지
- 장치에서 피드 시작 및 중지

장치 중지는 비디오가 장치에서 시스템으로 더 이상 전송되지 않음을 의미하며, 이 경우 라이브 비디오 또는 녹화된 비디오를 볼 수 없습니다. 반대로 피드를 중지한 장치는 레코딩 서버와 계속해서 통신할 수 있고, 장치를 Management Client 에서 수동으로 비활성화한 경우와 대조적으로 규칙을 통해 장치에서 자동으로 피드를 시작할 수 있습니다.

> ⚠ 일부 규칙 내용의 경우에는 해당 장치에 대해 특정 기능을 활성화해야 할 수 있습니다. 예를 들어 해당 카메라에 대해 레코딩이 활성화되지 않은 경우, 카메라가 레코딩하도록 지정하는 규칙이 의도대로 작동하지 않습니다. 규칙을 만들기 전에 Milestone 은 포함된 장치가 계획대로 기능을 수행할 수 있는지 확인할 것을 권장합니다.

규칙 복잡성

정확한 옵션의 수는 생성하려는 규칙의 유형과 시스템에서 사용 가능한 장치 수에 따라 다릅니다. 규칙은 높은 유연성을 제공하므로 이벤트와 시간 조건을 결합하고, 단일 규칙에 여러 조건을 지정하고, 시스템 상의 여러 장치 또는 모든 장치를 포괄하는 규칙을 수시로 생성할 수 있습니다.

필요에 따라 규칙을 단순하게 또는 복잡하게 설정할 수 있습니다. 예를 들어, 매우 단순한 시간 기반 규칙을 생성할 수 있습니다:

예제	설명
매우 단순한 시간 기반 규칙	월요일 오전 8시 30분 ~ 오전 11시 30분 사이(시간 조건), 시간 기간이 시작할 때 카메라 1과 카메라 2가 레코딩을 시작하고(동작) 시간 기간이 종료하면 레코딩을 중지합니다(중지 동작).
매우 단순한 이벤트 기	카메라 1에서 모션이 감지되면(이벤트 조건), 카메라 1이 즉시 레코딩을 시작한 다음(동

예제	설명
반 규칙	작) 10초 후 레코딩을 중지합니다(중지 동작). 이벤트 기반 규칙이 한 장치의 이벤트에 의해 활성화된 경우라도 하나 이상의 다른 장치에서 해당 동작이 발생하도록 지정할 수 있습니다.
여러 장치가 포함된 규칙	카메라 1에서 모션이 감지되면(이벤트 조건), 카메라 2가 즉시 레코딩을 시작하고(동작) 출력 3에 연결된 사이렌이 즉시 울립니다(동작). 그리고 나서 60초 후, 카메라 2가 레코딩을 중지하고(중지 동작) 출력 3에 연결된 사이렌에서 소리가 멈춥니다(중지 동작).
시간, 이벤트 및 장치를 결합한 규칙	카메라 1에서 동작이 감지되고(이벤트 조건) 요일이 토요일이거나 일요일일 경우(시간 조건), 카메라 1과 카메라 2가 즉시 레코딩을 시작하고(동작) 알림이 보안 관리자로 전송됩니다(동작). 그리고 나서 카메라 1 또는 카메라 2에서 더 이상 동작이 감지되지 않으면 5초 후 카메라 2가 레코딩을 중지합니다(중지 동작).

조직의 필요에 따라 소수의 복잡한 규칙보다 단순한 여러 규칙을 만드는 것이 좋은 경우가 많습니다. 시스템에 더 많은 규칙이 있다는 것을 의미하더라도, 규칙의 정하는 바에 대한 개요를 간단히 유지할 수 있습니다. 또한, 규칙을 단순하게 유지하면 개별 규칙 요소를 비활성화/활성화할 때 유연성이 훨씬 높아집니다. 단순 규칙을 사용하면 필요 시 전체 규칙을 비활성화/활성화할 수 있습니다.

규칙 및 이벤트(설명됨)

규칙 은 시스템에서 가장 중요한 요소입니다. 규칙은 카메라의 레코딩 시기, PTZ 카메라의 순찰 시기, 알림 전송 시기 등 매우 중요한 설정을 결정합니다.

예제 - 모션 감지 시 특정 카메라의 레코딩 시작을 지정하는 규칙:

이벤트 는 **규칙 관리** 마법사를 사용할 때 가장 중요한 요소에 해당합니다. 마법사에서 이벤트는 주로 동작을 트리거하는 데 사용됩니다. 예를 들어, 모션이 감지된 **이벤트** 가 발생한 경우, 감시 시스템이 특정 카메라의 비디오 레코딩 시작 **동작** 을 취하는 규칙을 만들 수 있습니다.

다음 두 가지 유형의 조건이 규칙을 트리거할 수 있습니다.

이름	설명
이벤트	감시 시스템에서 이벤트가 발생할 때(예: 모션이 감지될 때 또는 시스템이 외부 센서로부터 입력을 수신할 때).
시간 간격	특정 기간(예: `Thursday 16th August 2007 from 07.00 to 07.59` 또는 `every Saturday and Sunday`)
장애 조치 시간 간격	장애 조치가 활성화 또는 비활성화되는 시간 간격.
반복 시간	상세한 반복 스케쥴에서 실행될 동작을 설정할 때. 예: • 매주 화요일 15:00~15:30 사이 1시간 동안 • 매 3개월마다 15일 11:45에 • 매일 15:00~19:00 사이 1시간 동안 시간은 Management Client 이(가) 설치된 서버의 현지 시간 설정을 따릅니다.

규칙 및 이벤트 에서 다음을 사용할 수 있습니다.

- **규칙**: 규칙은 시스템에서 가장 중요한 요소입니다. 감시 시스템의 동작은 매우 넓은 범위까지 규칙에 의해 결정됩니다. 규칙을 만들 때 모든 유형의 이벤트를 사용할 수 있습니다
- **시간 프로파일**: 시간 프로파일은 Management Client 에 정의된 기간입니다. 특정 시간 프로파일 내에 특정 동작이 발생하는 규칙을 만들 때 등과 같이 Management Client 에서 규칙을 만들 때 이러한 프로파일을 사용합니다.
- **알림 프로파일**: 알림 프로파일을 사용하여 맞춤형 이메일 알림을 설정할 수 있고, 규칙에 의해 자동으로 트리거할 수 있습니다(예: 특정 이벤트가 발생할 때)
- **사용자 정의 이벤트**: 사용자 정의 이벤트는 사용자가 시스템에서 이벤트를 수동으로 트리거하거나 시스템의 입력에 반응할 수 있게 하는 맞춤형 이벤트입니다
- **분석 이벤트**: 분석 이벤트는 외부의 제3자 비디오 콘텐츠 분석(VCA) 제공업체에서 수신한 데이터입니다. 분석 이벤트를 알람의 기초로 사용할 수 있습니다
- **일반 이벤트**: 일반 이벤트를 이용하면 IP 네트워크를 통해 시스템으로 단순 문자열을 전송하여 XProtect 이벤트 서버에서 동작을 트리거할 수 있습니다

시간 프로파일(설명됨)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

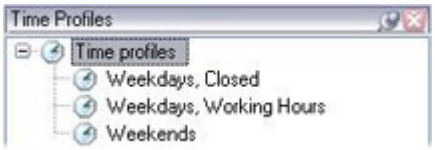
시간 프로파일은 관리자가 정의한 기간입니다. 예를 들어, 특정 시간 길이 내에 특정 동작이 발생하도록 지정하는 규칙과 같이 규칙을 만들 때 시간 프로파일을 사용할 수 있습니다.

또한 시간 프로파일은 Smart Client 프로파일과 함께 역할에 할당됩니다. 기본적으로 모든 역할에는 **항상** 이 기본 시간 프로파일로 할당됩니다. 즉, 이 기본 시간 프로파일이 연결된 역할 구성원은 시스템의 사용자 권한에 시간 기반 제한이 없음을 의미합니다. 또한 다른 시간 프로파일을 역할에 할당할 수 있습니다.

시간 프로파일은 매우 유연하게 설정할 수 있습니다. 하나 이상의 단일 기간, 하나 이상의 되풀이 기간 또는 단일 및 되풀이 시간의 조합을 기반으로 시간 프로파일을 지정할 수 있습니다. 대부분의 사용자는 Microsoft® Outlook의 응용 프로그램과 같이 달력 응용 프로그램에서 단일 및 반복 기간의 개념에 익숙할 수 있습니다.

시간 프로파일은 항상 현지 시간으로 적용됩니다. 즉, 시스템에 다른 시간대의 레코딩 서버가 배치된 경우 시간 프로파일과 연결된 모든 동작(예: 카메라의 레코딩)은 각 레코딩 서버의 현지 시간에 수행됩니다. 예: 오전 8시 30분 ~ 오전 9시 30분 사이를 포함하는 시간 프로파일의 경우, 뉴욕에 배치된 레코딩 서버에서 관련된 모든 동작은 뉴욕의 현지 시간 오전 8시 30분 ~ 오전 9시 30분 사이에 수행되는 반면, 로스앤젤레스에 배치된 레코딩 서버에서 동일한 동작은 몇 시간 이후인 로스앤젤레스의 현지 시간 오전 8시 30분 ~ 오전 9시 30분 사이에 수행됩니다.

규칙 및 이벤트 > **시간 프로파일** 을 확장하여 시간 프로파일을 만들고 관리할 수 있습니다. **시간 프로파일** 목록이 열립니다. 예시용으로만 사용됩니다.



시간 프로파일의 대안으로는 주간 길이 시간 프로파일 을 참조하십시오.

주간 길이 시간 프로파일(설명됨)

카메라를 바깥에 배치한 경우 흔히 카메라 해상도를 낮추고, 흑백을 활성화하기도 하고, 어둡거나 밝을 때 그 밖의 설정을 변경해야 합니다. 적도에서 북쪽 또는 남쪽으로 더 먼 지역에 카메라가 배치된 경우, 그에 따라 연중 일출과 일몰 시간이 달라집니다. 이 때문에 일반 고정 시간 프로파일을 사용하여 광원 조건에 따라 카메라 설정을 조정하기가 불가능해집니다.

그러한 상황에서는 지정된 지리적 영역에서 일출과 일몰을 정의하는 대신 하루 길이 시간 프로파일을 만들 수 있습니다. 지리적 좌표를 통해 시스템이 일출과 일몰 시간을 계산하며, 일일 기준 일광 절약 시간도 사용됩니다. 따라서 시간 프로파일이 자동으로 선택한 지역에서 일출/일몰의 연중 변화를 따르므로 필요한 경우에만 프로파일을 활성화할 수 있습니다. 모든 시간과 날짜는 관리 서버 시간 및 날짜 설정을 기반으로 합니다. 또한 시작(일출) 및 종료 시간(일몰)에 대해 양수 또는 음수 오프셋(분 단위)을 설정할 수 있습니다. 시작/종료 시간의 오프셋은 동일할 수도 있고 다를 수도 있습니다.

규칙과 역할을 만들 때 모두 하루 길이 프로파일을 사용할 수 있습니다.

알림 프로파일(설명됨)

알림 프로파일에서 준비된 이메일 알림을 설정할 수 있습니다. 특정 이벤트가 발생할 때와 같이 알림은 규칙에 따라 자동으로 트리거할 수 있습니다.

알림 프로필을 생성할 때, 메시지 문자를 지정하고 스틸 이미지와 AVI 비디오 클립을 이메일 알림에 포함시킬지 결정합니다.

> ⚠ 또한 응용 프로그램이 이메일 알림을 전송하지 못하게 차단하는 이메일 스캐너를 비활성화해야 할 수도 있습니다.

알림 프로파일 생성 요구 사항

알림 프로파일을 만들기 전에 이메일 알림에 대한 메일 서버 설정을 지정해야 합니다.

메일 서버상에 필수 보안 인증을 설치하면 메일 서버에 대한 통신을 보호할 수 있습니다.

이메일 알림에 AVI 동영상 클립을 포함시키고자 할 경우, 사용할 압축 설정도 지정해야 합니다:

1. **도구** > **옵션** 으로 이동합니다. 그러면 **맵 설정** 창이 열립니다.
2. **메일 서버** 탭에서 메일 서버를 구성하고(페이지 356의 Mail Server 탭(옵션)) **AVI 생성** 탭에서 압축 설정을 구성합니다(페이지 357의 AVI 생성 탭(옵션)).

사용자 정의 이벤트(설명됨)

필요한 이벤트가 **이벤트 개요** 목록에 없는 경우, 자체적으로 사용자 정의 이벤트를 만들 수 있습니다. 그러한 사용자 정의 이벤트를 사용하여 다른 시스템을 감시 시스템에 통합합니다.

사용자 정의 이벤트를 사용하면 타사 액세스 제어 시스템에서 수신한 데이터를 시스템에서 이벤트로 사용할 수 있습니다. 이후 이벤트는 동작을 트리거할 수 있습니다. 이러한 방식으로 누군가 건물에 들어왔을 때 해당 카메라에서 비디오 레코딩을 시작할 수 있습니다.

또한 XProtect Smart Client 에서 라이브 비디오를 보는 동안 이벤트를 수동으로 트리거하거나 규칙에서 사용하는 경우 자동으로 트리거하는 데 사용자 정의 이벤트를 사용할 수 있습니다. 예를 들어, 사용자 정의 이벤트 37이 발생하면 PTZ 카메라 224가 순찰을 중지하고 프리셋 위치 18로 이동하도록 할 수 있습니다.

역할을 통해 사용자 정의 이벤트를 트리거할 수 있는 사용자를 정의합니다. 필요에 따라 두 가지 방식으로, 동시에 사용자 정의 이벤트를 사용할 수 있습니다:

이벤트	설명
XProtect Smart Client 에서 이벤트를 수동으로 트리거하는 기능 제공	이 경우 사용자 정의 이벤트를 통해 최종 사용자가 XProtect Smart Client 에서 라이브 비디오를 보는 동안 이벤트를 수동으로 트리거할 수 있습니다. XProtect Smart Client 사용자가 수동으로 이벤트를 트리거하여 사용자 정의 이벤트가 발생하면 규칙에 의해 하나 이상의 동작이 시스템에 발생하도록 트리거할 수 있습니다.

이벤트	설명
API를 통해 이벤트를 트리거하는 기능 제공	이 경우 감시 시스템 외부에서 사용자 정의 이벤트를 트리거할 수 있습니다. 이러한 방식으로 사용자 정의 이벤트를 사용하기 위해서는 사용자 정의 이벤트를 트리거할 때 별도의 API(응용 프로그램 프로그램 인터페이스. 소프트웨어 응용 프로그램을 생성하거나 사용자 정의하기 위한 일련의 빌딩 블록)를 사용해야 합니다. Active Directory를 통한 인증이 필요합니다. 이를 통해 사용자 정의 이벤트를 감시 시스템 외부에서 트리거할 수 있는 경우라도 권한이 있는 사용자만이 해당 작업을 수행할 수 있습니다. 또한 API를 통해 사용자 정의 이벤트를 메타데이터와 연결하여 특정 장치 또는 장치 그룹을 정의할 수 있습니다. 사용자 정의 이벤트를 사용하여 규칙을 트리거할 때 매우 유용하여, 각 장치에 대해 기본적으로 동일한 작업을 수행하는 규칙을 가질 필요가 없습니다. 예: 회사에서 액세스 제어 기능을 사용하는데, 입구가 35개이고 각각에 액세스 제어 장치가 설치되어 있습니다. 액세스 제어 장치가 활성화되면 사용자 정의 이벤트가 시스템에서 트리거됩니다. 이 사용자 정의 이벤트는 활성화된 액세스 제어 장치와 관련된 카메라에서 레코딩을 시작하는 규칙에 사용됩니다. 어떤 카메라가 어떤 규칙에 연결되는지는 메타데이터에서 정의됩니다. 이러한 방식으로 이 회사는 사용자 정의 이벤트 35개와 사용자 정의 이벤트에 의해 트리거되는 규칙 35개를 지정할 필요가 없습니다. 단일 사용자 정의 이벤트와 단일 규칙만으로도 충분합니다. 이런 방식으로 사용자 정의 이벤트를 사용하면, XProtect Smart Client 에서 수동 트리거를 위해 항상 해당 이벤트를 사용하지 않아도 됩니다. 역할을 사용하여 XProtect Smart Client 에 표시되는 사용자 정의 이벤트를 정의할 수 있습니다.

분석 이벤트(설명됨)

분석 이벤트는 일반적으로 외부의 제3자 비디오 콘텐츠 분석(VCA) 제공업체에서 수신한 데이터입니다.

알람의 기초로 분석 이벤트 사용은 기본적으로 세 단계 프로세스로 이루어집니다:

- 첫째, 분석 이벤트 기능을 활성화하고 보안을 설정합니다. 허용된 주소 목록을 사용하여, 이벤트 데이터를 시스템으로 전송할 수 있는 사람과 서버가 수신하는 포트를 제어합니다
- 둘째, 분석 이벤트를 만들고(가능하면 이벤트에 대한 설명 포함) 테스트합니다
- 셋째, 분석 이벤트를 알람 정의의 소스로 사용합니다

사이트 탐색 창의 **규칙 및 이벤트** 목록에서 분석 이벤트를 설정합니다.

VCA 기반 이벤트를 사용하려면 타사 VCA 도구를 사용하여 데이터를 시스템에 공급해야 합니다. 사용할 VCA 도구 선택은 도구에서 제공되는 데이터가 해당 형식을 준수하는 한 전적으로 사용자에게 달려 있습니다. 이 형식은 분석 이벤트의 MIP SDK 문서 에서 설명합니다.

자세한 내용은 시스템 제공업체로 문의하십시오. 타사 VCA 도구는 Milestone 개방형 플랫폼을 토대로 솔루션을 제공하는 독립 파트너에서 개발됩니다. 이러한 솔루션은 시스템의 성능에 영향을 줄 수 있습니다.

일반 이벤트(설명됨)

일반 이벤트를 이용하면 IP 네트워크를 통해 시스템으로 단순 문자열을 XProtect 로 전송하여 동작을 트리거할 수 있습니다.

TCP 또는 UDP 를 통해 문자열을 전송할 수 있는 하드웨어나 소프트웨어를 사용하여 일반 이벤트를 트리거할 수 있습니다. 사용 중인 시스템은 수신한 TCP 또는 UDP 데이터 패키지를 분석하여 특정 기준을 충족할 때 일반 이벤트를 자동으로 트리거할 수 있습니다. 이러한 방식으로 시스템을 외부 소스와 통합할 수 있습니다(예: 액세스 제어 시스템과 알람 시스템). 이것의 목표는 가능한 한 많은 외부 소스가 시스템과 상호 작용할 수 있게 하기 위함입니다.

데이터 소스의 개념을 활용하면 시스템 표준을 충족하기 위해 타사 도구를 채택하지 않아도 됩니다. 데이터 소스를 이용하면 구체적인 IP 포트에서 하드웨어 또는 소프트웨어의 특정 부분과 통신하여 해당 포트에 도달하는 바이트의 해석 방식을 미세하게 조정할 수 있습니다. 각 일반 이벤트 유형은 데이터 소스와 쌍을 이뤄 하드웨어 또는 소프트웨어의 특정 부분과 통신하는 데 사용되는 언어를 구성합니다.

데이터 소스를 사용하려면 IP 네트워킹에 대한 일반적인 지식과 인터페이스를 연결하려는 개별 하드웨어 또는 소프트웨어에 대한 구체적인 지식이 있어야 합니다. 사용 가능한 여러 매개변수가 있으며, 이를 수행하기 위한 맞춤형 솔루션은 없습니다. 기본적으로 시스템은 도구를 제공하지, 솔루션을 제공하지는 않습니다. 사용자 정의 이벤트와 달리, 외부 이벤트는 인증이 없습니다. 이 때문에 보다 쉽게 트리거할 수 있지만 보안 위협을 피하기 위해서 로컬 호스트에서만 이벤트가 수락됩니다. **옵션** 메뉴의 **일반 이벤트** 탭에서 다른 클라이언트 IP 주소를 허용할 수 있습니다.

웹후크(설명됨)

웹후크는 웹 응용 프로그램이 서로 통신할 수 있게 하는 HTTP 요청으로, 사전 정의된 이벤트가 발생할 때 한 응용 프로그램에서 다른 응용 프로그램으로의 실시간 데이터 전송을 용이하게 해 줍니다. 예를 들어, 사용자가 시스템에 로그인하거나 카메라가 오류를 보고할 때 미리 정의된 웹후크 엔드포인트로 이벤트 데이터를 보냅니다.

웹후크 엔드포인트(웹후크 URL)는 이벤트 데이터가 전송되는 미리 정의된 주소이며 이는 단방향 전화번호와 매우 비슷합니다.

웹후크를 사용하여 XProtect에서 선택한 이벤트를 구독하는 통합을 구축할 수 있습니다. 이벤트가 트리거되면 해당 이벤트에 대해 정의한 웹후크 엔드포인트로 HTTP POST가 전송됩니다. HTTP POST 본문에는 JSON에 있는 이벤트 데이터가 포함되어 있습니다.

웹후크는 데이터 또는 트리거된 이벤트에 대해 시스템을 폴링하지 않습니다. 그 대신 이벤트가 발생하면 시스템이 폴링 솔루션에 비해 웹후크를 리소스 요구가 적고 설정 속도를 더 빠르게 만들어주는 웹후크 엔드포인트로 이벤트 데이터를 푸시합니다.

코드 스크립트를 사용하거나 사용하지 않은 상태에서 통합하도록 웹후크를 설정할 수 있습니다.

> XProtect에서 전송된 이벤트 데이터가 귀하가 계신 국가의 기존 데이터 및 개인정보보호 법률을 준수하는지 확인해야 합니다.

웹후크 기능은 기본적으로 설치되어 있으며 XProtect 2023R1 이상에서 바로 사용할 수 있습니다. 그리고 Management Client의 **규칙** 탭에 **웹후크** 작업을 표시합니다.

알람

알람(설명됨)

이 기능은 XProtect Event Server을(를) 설치한 경우에만 작동합니다.

이 문서는 이벤트에 의해 트리거되어 시스템에 표시될 알람을 설정하는 방법에 대해 설명합니다.

이벤트 서버에서 처리되는 기능을 토대로, 알람 기능은 조직 내에 설치한 수와 상관없이 (다른 XProtect 시스템 포함) 알람에 대한 중앙 개요, 제어 및 확장성을 제공합니다. 다음을 기준으로 알람을 생성하도록 구성할 수 있습니다.

- **내부 시스템 관련 이벤트**

  예를 들어, 모션, 서버 응답/무응답, 아카이브 문제, 디스크 공간 부족 등을 들 수 있습니다.

- **외부 통합 이벤트**

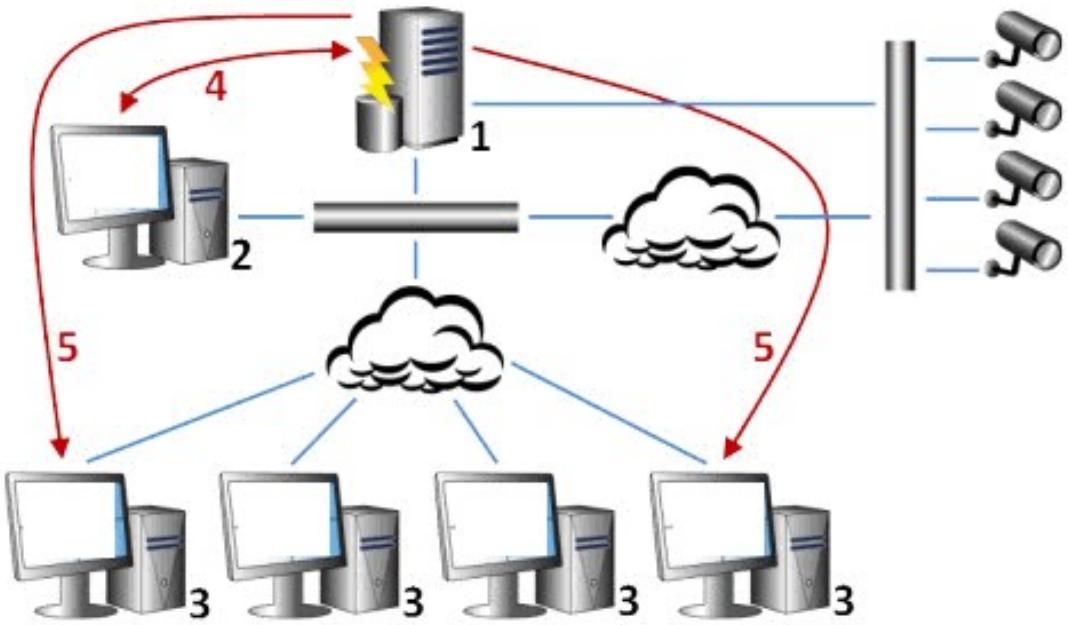
  이 그룹은 다양한 유형의 외부 이벤트를 포함합니다.

  - **분석 이벤트**

    일반적으로 외부의 제3자 비디오 콘텐츠 분석(VCA) 제공업체에서 수신한 데이터입니다.

  - **MIP 플러그 인 이벤트**

    MIP SDK 을(를) 통해 타사 공급업체가 시스템에 대한 사용자 정의 플러그 인(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합)을 개발할 수 있습니다.



범례:

1. 감시 시스템
2. Management Client
3. XProtect Smart Client
4. 알람 구성
5. 알람 데이터 흐름

XProtect Smart Client의 알람 목록에 있는 알람을 처리하고 할당합니다. 또한 알람을 XProtect Smart Client의 스마트 맵 및 맵 기능과 통합할 수 있습니다.

알람 구성

알람 구성에는 다음이 포함됩니다.

- 알람 처리에 대한 동적 역할 기반 설정
- 서버, 카메라 및 외부 장치와 같은 모든 구성 요소에 대한 중앙 기술 개요
- 모든 수신 알람 및 시스템 정보에 대한 중앙 로깅 설정
- 외부 액세스 제어 또는 VCA 기반 시스템과 같이 다른 시스템의 사용자 정의 통합을 허용하는 플러그 인 처리

일반적으로 알람은 해당 알람을 유발하는 개체의 가시성에 따라 제어됩니다. 즉, 알람, 알람을 제어/관리하는 사람, 알람의 정도 등과 관련해서 4가지 가능한 요소가 해당 역할을 수행할 수 있습니다.

이름	설명
소스/장치 가시성	알람을 유발하는 장치가 사용자 역할에 보이도록 설정되지 않은 경우, 사용자가 XProtect Smart Client 의 알람 목록에서 해당 알람을 볼 수 없습니다.
사용자 정의 이벤트를 트리거하는 권한	이 권한은 사용자 역할이 XProtect Smart Client 에서 선택한 사용자 정의 이벤트를 트리거할 수 있는지 여부를 결정합니다.
외부 플러그 인	시스템에 외부 플러그 인이 설정된 경우, 알람을 처리하는 사용자 권한을 제어할 수 있습니다.
일반 역할 권한	사용자가 알람을 볼 수만 있는지, 관리할 수도 있는지를 결정합니다. **알람** 사용자가 알람으로 할 수 있는 작업은 사용자의 역할과 특정 역할에 대해 구성된 설정에 따라 다릅니다.

옵션 의 **알람 및 이벤트** 탭에서 알람, 이벤트 및 로그의 설정을 지정할 수 있습니다.

스마트 맵

스마트 맵(설명됨)

XProtect® Smart Client 및 XProtect Mobile에서 스마트 맵 기능을 통해 지리적으로 정확한 방식으로 전 세계 여러 위치에 있는 장치를 확인하고 액세스할 수 있습니다. 각 위치에 대해 서로 다른 맵을 보유하는 맵과 달리, 스마트 맵은 단일 뷰로 큰 그림을 제공합니다.

다음의 스마트 맵 기능 구성은 Management Client 에서 완료됩니다.

- 사용 중인 스마트 맵에서 선택할 수 있는 지리적 배경을 구성합니다. 여기에는 스마트 맵을 다음 중 하나의 서비스와 통합하는 것이 포함됩니다.
    - Bing Maps
    - Google Maps
    - Milestone Map Service
    - OpenStreetMap
- XProtect Management Client 또는 XProtect Smart Client 에서 Bing Maps 또는 Google Maps 활성화
- XProtect Smart Client 에서 장치를 포함하여 스마트 맵 편집을 활성화
- XProtect Management Client 에서 지리적으로 장치 배치
- 다음과 함께 스마트맵을 설정: Milestone Federated Architecture

스마트 맵과 Google Maps 통합(설명됨)

Google Maps을 스마트 맵에 포함하려면 Google의 정적 지도 API 키가 필요합니다. API 키를 받으려면 우선 Google 클라우드 청구 계정을 생성해야 합니다. 매월 맵 사용량에 따라 청구를 받게 됩니다.

API 키를 받은 후에는 XProtect Management Client 에서 입력해야 합니다. 또한 페이지 296의 Bing Maps 또는 Google Maps를 다음에서 활성화: Management Client를 참조하십시오.

> 제한적인 방화벽을 사용하고 있는 경우에는 사용된 도메인에 대한 액세스를 허용하는 것이 중요합니다. Smart Client가 실행 중인 각 시스템에서 maps.googleapis.com을 사용하는 Google Maps에 대해 나가는 트래픽을 허용하는 것이 필요할 수도 있습니다.

자세한 내용은 다음을 참조하십시오.

- Google Maps Platform - 시작하기: https://cloud.google.com/maps-platform/
- Google Maps 플랫폼 청구서 안내:https://developers.google.com/maps/billing/gmp-billing
- 정적 지도 API를 위한 개발자 안내 서:https://developers.google.com/maps/documentation/maps-static/dev-guide

디지털 서명을 정적 맵 API 키에 추가

XProtect Smart Client 운영자가 하루에 25,000개의 맵 요청을 할 것으로 예상되는 경우, Maps Static API 키에 대한 디지털 서명이 필요합니다. 디지털 서명은 Google 서버가 사용자의 API 키를 사용한 사이트 생성 요청이 그렇게 하도록 승인되었음을 확인하도록 해줍니다. 그러나 사용량 요건과는 상관 없이, Google은 디지털 서명을 추가 보안 레이어로서 사용하는 것을 권장합니다. 디지털 서명을 받으려면 URL 서명 비밀번호를 검색해야 합니다. 자세한 정보는 https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual를 참조하십시오.

스마트 맵과 Bing Maps 통합(설명됨)

Bing Maps을 스마트 맵에 포함하려면 기본 키 또는 엔터프라이즈 키가 필요합니다. 기본 키는 무료라는 차이점이 있지만, 트랜잭션이 청구 가능해지기 전까지 또는 맵 서비스에 대한 액세스가 거부될 때까지 제한된 수의 트랜잭션만 허용됩니다. 엔터프라이즈 키는 유료이지만 무제한 트랜잭션이 허용됩니다.

Bing Maps에 관한 자세한 정보는 https://www.microsoft.com/en-us/maps/licensing/ 을(를) 참조하십시오.

API 키를 받은 후에는 XProtect Management Client 에서 입력해야 합니다. 페이지 296의 Bing Maps 또는 Google Maps를 다음에서 활성화: Management Client를 참조하십시오.

제한적인 방화벽을 사용하고 있는 경우에는 사용된 도메인에 대한 액세스를 허용하는 것이 중요합니다. Smart Client가 실행 중인 각 시스템에서 *.virtualearth.net을 사용하는 Bing 맵에 대해 나가는 트래픽을 허용하는 것이 필요할 수도 있습니다.

캐시된 스마트 맵 파일(설명됨)

지리적 배경으로 Google Maps을 사용하는 경우, 파일은 캐시되지 않습니다.

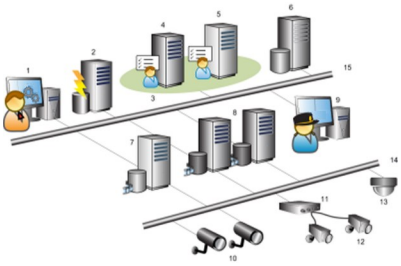
지리적 배경으로 사용하는 파일은 타일 서버에서 검색됩니다. 파일이 캐시 폴더에 저장되는 시간은 XProtect Smart Client 의 **설정** 대화 상자 안에 **제거된 캐시 스마트 맵 파일** 목록에서 선택된 값에 따라 다릅니다. 파일은 다음 중 하나로 저장됩니다.

- 무기한(**안함**)
- 파일이 사용되지 않은 경우 30일 동안(**30일 동안 사용되지 않을 때**)
- 운영자가 XProtect Smart Client 에서 나갈 경우(**종료 시**)

타일 서버 주소를 변경할 경우 새 캐시 폴더가 자동으로 생성됩니다. 이전 맵 파일은 로컬 컴퓨터의 연결된 캐시 폴더에 보관됩니다.

아키텍처

배포형 시스템 설정



분산 시스템 설정의 예. 카메라, 레코딩 서버 및 연결된 클라이언트의 수를 원하는 만큼 지정할 수 있습니다.

> 배포 설정 내 모든 컴퓨터는 도메인 또는 워크 그룹에 있어야 합니다.

범례:

1. Management Client(s)
2. 이벤트 서버
3. Microsoft 클러스터
4. 관리 서버
5. 장애 조치 관리 서버
6. 다음이 포함된 서버: SQL Server
7. 장애 조치 레코딩 서버
8. 레코딩 서버
9. XProtect Smart Client(s)
10. IP 비디오 카메라
11. 비디오 인코더
12. 아날로그 카메라

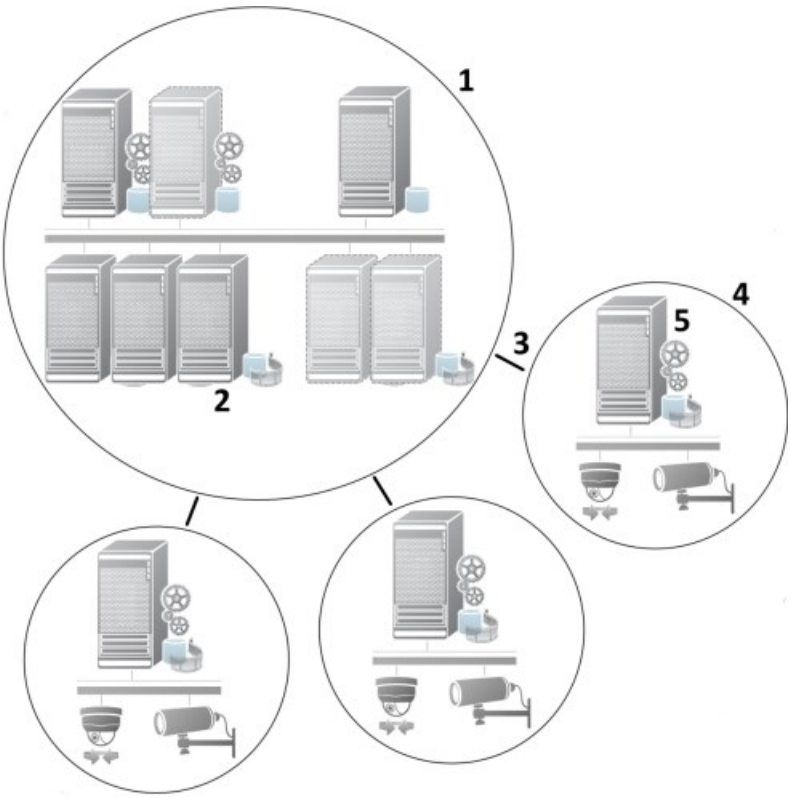
13. PTZ IP 카메라
14. 카메라 네트워크
15. 서버 네트워크

Milestone Interconnect (설명됨)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

Milestone Interconnect™ 을(를) 통해 소규모로 물리적으로 나눠진 많은 원격 XProtect 설치와 하나의 XProtect Corporate 중앙 사이트를 통합할 수 있습니다. 원격 사이트라고 하는 이러한 소규모 사이트를 이동식 유닛(예: 보트, 버스 또는 기차)에 설치할 수 있습니다. 즉, 그러한 사이트를 네트워크에 영구히 연결할 필요가 없습니다.

다음 삽화는 시스템에 을(를) 설치하는 방법을 Milestone Interconnect 보여줍니다.



1. Milestone Interconnect 중앙 XProtect Corporate 사이트
2. Milestone Interconnect 드라이버(중앙 사이트의 레코딩 서버와 원격 사이트 간의 연결을 처리하며, **하드웨어 추가** 마법사를 통해 원격 시스템을 통합할 때 드라이버 목록에서 선택해야 함)

3. Milestone Interconnect 연결
4. Milestone Interconnect 원격 사이트(시스템 설치, 사용자, 카메라 등을 포함한 전체 원격 사이트)
5. Milestone Interconnect 원격 시스템(원격 사이트의 실제 기술적 설치)

중앙 사이트에서 **하드웨어 추가** 마법사를 이용하여 중앙 사이트에 원격 사이트를 추가합니다(페이지 289의 중앙 Milestone Interconnect 사이트에 원격 사이트 추가 참조).

각 원격 사이트는 독립적으로 실행되고 일반적인 감시 작업을 수행할 수 있습니다. 네트워크 연결 및 적절한 사용자 권한에 따라(페이지 290의 사용자 권한 할당 참조), Milestone Interconnect 은(는) 원격 사이트 카메라에 대한 직접 라이브 뷰와 중앙 사이트에서 원격 사이트 레코딩 재생 기능을 제공합니다.

중앙 사이트는 지정된 사용자 계정이 (원격 사이트를 추가할 때) 액세스할 수 있는 장치만 인식하고 여기에 액세스할 수 있습니다. 따라서 로컬 시스템 관리자는 중앙 사이트와 그 사용자가 이용할 수 있는 장치를 제어할 수 있습니다.

중앙 사이트에서 상호 연결된 카메라의 시스템 고유 상태를 볼 수 있지만 원격 사이트의 상태를 직접 보지는 못합니다. 대신에, 원격 사이트를 모니터링하려면, 원격 사이트 이벤트를 이용하여 중앙 사이트에서 알람이나 다른 알림을 트리거할 수 있습니다(페이지 291의 원격 사이트의 이벤트에 응답하도록 중앙 사이트 구성 참조).

또한 이벤트, 규칙/일정 또는 XProtect Smart Client 사용자의 수동 요청을 기반으로 원격 사이트 레코딩을 중앙 사이트로 전송할 수 있는 기회를 제공합니다.

오로지 XProtect Corporate 시스템만 중앙 사이트 역할을 할 수 있습니다. 다른 모든 제품들은 XProtect Corporate 을(를) 포함하여 원격 사이트 역할만 할 수 있습니다. 중앙 사이트에서 처리되는 버전, 카메라 수, 원격 사이트에서 발생한 장치 및 카메라가 처리되는 방식은 설치마다 다릅니다. 특정 XProtect 제품이 Milestone Interconnect 설정에서 상호 작용하는 방식에 대한 자세한 내용은 Milestone Interconnect 웹사이트(https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/)에 나와 있습니다.

Milestone Interconnect 또는 Milestone Federated Architecture 선택(설명됨)

중앙 사이트의 사용자가 원격 사이트의 비디오에 액세스해야 하는 물리적으로 분산된 시스템에서, Milestone Interconnect™ 또는 Milestone Federated Architecture™ 사이에 선택할 수 있습니다.

Milestone 은 다음과 같은 경우 Milestone Federated Architecture 을(를) 권장합니다:

- 중앙 및 연합 사이트 간의 네트워크 연결이 안정적입니다
- 네트워크가 동일 도메인을 사용합니다
- 대형 사이트 수가 적습니다
- 요구되는 용도에 대역폭이 충분합니다

Milestone 은 다음과 같은 경우 Milestone Interconnect 을(를) 권장합니다:

- 중앙 및 원격 사이트 간의 네트워크 연결이 불안정합니다
- 사용자 또는 조직이 원격 사이트에서 다른 XProtect 제품을 사용하고자 합니다
- 네트워크에 여러 도메인 또는 작업 그룹이 사용됩니다
- 소형 사이트 수가 많습니다

Milestone Interconnect 및 라이센싱

Milestone Interconnect 을(를) 실행하려면 원격 사이트에 있는 하드웨어 장치의 비디오를 보기 위해 중앙 사이트에 Milestone Interconnect 카메라 라이선스가 필요합니다. 필수 Milestone Interconnect 카메라 라이선스 수는 데이터 수신을 원하는 원격 사이트의 하드웨어 장치 수에 따라 달라집니다. 오로지 XProtect Corporate 만 중앙 사이트 역할을 할 수 있습니다.

Milestone Interconnect 카메라 라이선스 상태는 중앙 사이트의 **라이선스 정보** 페이지에 나열됩니다.

Milestone Interconnect 설치(설명됨)

세 가지 방식으로 Milestone Interconnect 을(를) 실행할 수 있습니다. 설정 실행 방법은 네트워크 연결, 레코딩 재생 방법, 원격 레코딩 검색 여부 및 검색 정도 등에 따라 다릅니다.

다음에서는 가장 가능성이 높은 3가지 설정에 대해 설명합니다.

원격 사이트에서 직접 재생(양호한 네트워크 연결)

가장 단순한 설치. 중앙 사이트는 원격 사이트와 지속적으로 온라인 상태를 유지하며 중앙 사이트 사용자는 원격 사이트에서 직접 원격 레코딩을 재생합니다. 이는 **원격 시스템에서 레코딩 재생** 옵션을 사용해야 합니다(페이지 290의 원격 사이트 카메라에서 직접 재생 활성화 참조).

원격 사이트에서 선택한 원격 레코딩 시퀀스의 규칙 또는 XProtect Smart Client 기반 검색(주기적으로 제한된 네트워크 연결)

원격 사이트로부터의 독립성을 보장하기 위해 선택한 레코딩 시퀀스(원격 사이트에서 발생)를 중앙으로 저장해야 할 경우 사용합니다. 독립성은 네트워크 장애나 네트워크 제한 발생 시 중대한 요소입니다. **원격 검색** 탭에서 원격 레코딩 검색 설정을 구성합니다(페이지 395의 원격 검색 탭 참조).

필요 시 원격 레코딩 검색을 XProtect Smart Client 에서 시작하거나 규칙을 설정할 수 있습니다. 시나리오에 따라서 원격 사이트가 온라인 상태일 수도 있고 대부분의 시간 동안 오프라인일 수도 있습니다. 업종마다 차이가 나는 경우가 많습니다. 일부 산업의 경우, 중앙 사이트가 원격 사이트와 영구적으로 온라인 상태를 유지하는 것이 일반적입니다(예: 소매 HQ(중앙 사이트)와 다수의 매장(원격 사이트)). 운송과 같은 다른 산업의 경우에는 원격 사이트가 이동형(예: 버스, 기차, 배 등)이므로 임시로만 네트워크 연결을 설정할 수 있습니다. 시작된 원격 레코딩 검색 중 네트워크 연결이 실패하면 작업이 다음 번 지정된 기회에 계속됩니다.

만일 시스템에서 사용자가 XProtect Smart Client 원격 검색 **탭에서 지정한 시간 간격을 이외에 자동 검색 또는** 에서 검색 요청을 감지한다면, 해당 요청이 수락되나 선택한 시간 간격에 도달하기 전에는 검색이 시작되지 않습니다. 새로운 원격 레코딩 검색 작업이 대기열에 지정되고 허용된 시간 간격이 되면 시작됩니다. **시스템 대시보드** -> **현재 작업** 에서 보류 중인 원격 레코딩 검색 작업을 볼 수 있습니다.

연결이 실패 후에, 누락된 원격 레코딩이 원격 사이트에서 기본으로 검색됩니다

원격 서버와 같이 원격 사이트는 카메라에서 에지 저장소를 사용합니다. 일반적으로 원격 사이트는 해당 중앙 사이트와 온라인 상태를 유지하여 중앙 사이트가 기록하는 라이브 스트림을 전달합니다. 특정 이유로 네트워크가 실패하면, 중앙

사이트에서 레코딩 시퀀스가 누락됩니다. 그러나 네트워크가 재설정되면 중앙 사이트가 가동 중단 기간에 해당하는 원격 레코딩을 자동으로 검색합니다. 이를 위해 카메라에 대한 **레코딩** 탭에서 **연결이 복원될 때 원격 레코딩을 자동으로 검색** 옵션을 사용해야 합니다(페이지 291의 원격 사이트 카메라에서 원격 레코딩 검색 참조).

특수한 필요성에 따라 위의 솔루션을 혼합하여 사용할 수 있습니다.

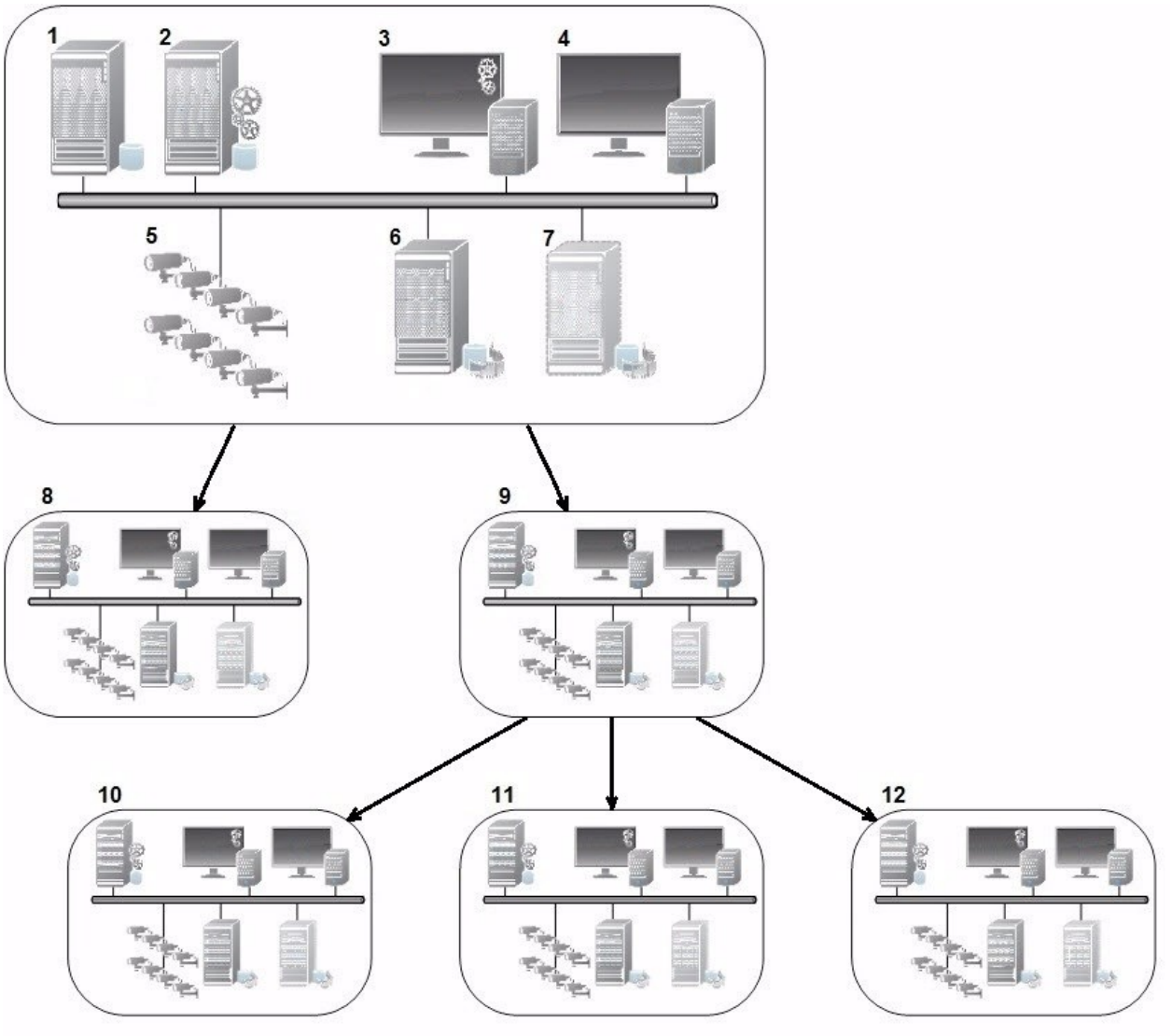
Milestone Federated Architecture 구성하기

XProtect Expert 은(는) 하위 사이트로만 연합시킬 수 있습니다.

Milestone Federated Architecture 은(는) 상위/하위 사이트의 연합 사이트 계층 구조에 여러 개의 개별 표준 시스템을 연결합니다. 충분한 권한을 가진 클라이언트 사용자가 개별 사이트 전체에서 비디오, 오디오 및 기타 리소스에 원활하게 액세스할 수 있습니다. 관리자는 개별 사이트에 대한 관리자 권한에 기초해 버전 2018 R1 이상부터 연합 계층 내의 모든 사이트를 중앙에서 관리할 수 있습니다.

기본 사용자는 Milestone Federated Architecture 시스템에서 지원되지 않으므로, Active Directory 서비스를 통해 사용자를 Windows 사용자로 추가해야 합니다.

Milestone Federated Architecture 은(는) 하나의 중앙 사이트(최상위 사이트)와 무제한 연합 사이트를 갖도록 설정됩니다(페이지 284의 연합 사이트 실행을 위한 시스템 설정 참조). 사이트에 로그인하면 모든 하위 사이트와 하위 사이트의 하위 사이트에 관한 정보에 액세스할 수 있습니다. 상위 사이트로부터 링크를 요청하면 두 사이트 사이에 링크가 설정됩니다(페이지 286의 계층 구조에 사이트 추가 참조). 하위 사이트 한 개를 상위 사이트 한 개에만 연결할 수 있습니다. 하위 사이트를 연합 사이트 계층 구조에 추가할 때 이 하위 사이트의 관리자가 아닌 경우, 하위 사이트 관리자가 요청을 수락해야 합니다.



Milestone Federated Architecture 설치의 구성 요소:

1. 다음이 포함된 서버: SQL Server
2. 관리 서버
3. Management Client
4. XProtect Smart Client
5. 카메라
6. 레코딩 서버
7. 장애 조치 레코딩 서버
8. 12까지. 연합 사이트

계층 구조 동기화

상위 사이트에는 현재 연결된 모든 하위 사이트, 해당 하위 사이트의 하위 사이트 등에 대한 업데이트 목록이 포함됩니다. 연합 사이트 계층 구조에서는 사이트 간의 예약된 동기화를 비롯하여 시스템 관리자가 사이트를 추가 또는 제거할 때마다 동기화가 이루어집니다. 시스템이 계층 구조를 동기화할 때 정보를 요청한 서버에 도달할 때까지 각 레벨별로 전달 및 회신 커뮤니케이션이 발생합니다. 시스템은 매번 1MB 미만을 전송합니다. Management Client 레벨 수에 따라 계층 구조의 변경 내용이 에 표시되기까지 약간의 시간이 걸릴 수 있습니다. 자체적인 동기화 일정을 예약할 수 없습니다.

데이터 트래픽

사용자 또는 관리자가 라이브/녹화 비디오를 보거나 사이트를 구성할 때 시스템이 통신 또는 구성 데이터를 전송합니다. 데이터의 양은 조회 또는 구성 내용과 크기에 따라 다릅니다.

Milestone Federated Architecture (기타 제품 포함) 및 시스템 요건

- Management Client 에서 Milestone Federated Architecture 을(를) 여는 것은 최신 공개를 포함하여 세 가지 주요 공개 버전에서 지원됩니다. 이 범주를 넘어선 Milestone Federated Architecture 설정에서는 서버 버전과 일치하는 Management Client 을(를) 분리해야 합니다.
- 중앙 사이트에서 XProtect Smart Wall 을(를) 사용하는 경우, 연합 사이트 계층 구조에서도 XProtect Smart Wall 기능을 사용할 수 있습니다.
- 중앙 사이트에서 XProtect Access 을(를) 사용하고 XProtect Smart Client 사용자가 연합 사이트 계층 구조의 사이트에 로그인하면 연합 사이트의 액세스 요청 알림이 에도 나타납니다.XProtect Smart Client
- XProtectExpert2013이상의시스템을연합사이트계층구조에상위사이트가아니라하위사이트로추가할수있습니다
- Milestone Federated Architecture 에는 추가 라이선스가 필요하지 않습니다
- 용례와 이점에 대한 자세한 내용은 Milestone Federated Architecture 에 관한 백서 를 참조하십시오.

연합 사이트 계층 구조 설정

Management Client 에서 계층 구조의 구성을 시작하기 전에 사이트를 서로 연결하는 방법을 매핑하는 것이 좋다고 Milestone 은 권장합니다.

연합 계층 구조 내에 각 사이트를 표준 시스템 구성 요소, 설정, 규칙, 일정, 관리자, 사용자 및 사용자 권한을 가진 일반적인 독립형 시스템으로 설치하고 구성합니다. 설치된 사이트가 이미 있고 구성이 되어 있어 연합 사이트 계층 구조에 결합시키기만 하면 되는 경우 바로 시스템을 설정할 수 있습니다.

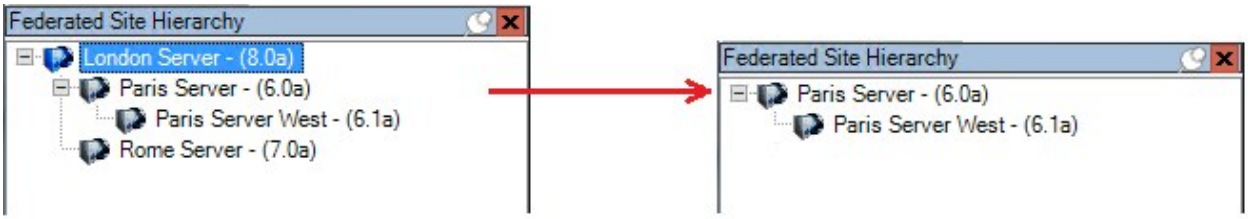
개별 사이트가 설치된 경우, 이러한 사이트를 연합 사이트로 실행되도록 설정해야 합니다(페이지 284의 연합 사이트 실행을 위한 시스템 설정 참조).

계층 구조를 시작하려면, 중앙 사이트로 사용할 사이트에 로그인하고 첫 연합 사이트를 추가할 수 있습니다(페이지 286의 계층 구조에 사이트 추가 참조). 링크가 설정되면 Management Client 의 **연합 사이트 계층 구조** 창에서 두 개의 사이트가 자동으로 연합 사이트 계층 구조를 형성하며, 여기에 사이트를 추가하여 연합 계층 구조를 확장시킬 수 있습니다.

연합 사이트 계층 구조를 생성하면 사용자와 관리자가 사이트에 로그인하여 이 사이트와 여기에 있을 수 있는 모든 연합 사이트에 액세스할 수 있습니다. 연합 사이트 액세스는 사용자 권한에 따라 다릅니다.

연합 계층 구조에 추가할 수 있는 사이트 수에는 제한이 없습니다. 또한 이전 제품 버전의 사이트를 새 버전에 연결할 수 있고 그 반대도 마찬가지입니다. 버전 번호는 자동으로 표시되며 삭제할 수 없습니다. 로그인하는 사이트는 항상 **연합 사이트 계층 구조** 창에서 최상위에 있고 이를 홈 사이트라고 부릅니다.

다음은 Management Client 에서 연합 사이트의 예입니다. 왼쪽에서 사용자는 최상위 사이트에 로그인했습니다. 오른쪽에서 사용자는 하위 사이트 중 하나인 파리 서버(홈 사이트)에 로그인했습니다.



Milestone Federated Architecture 의 상태 아이콘

아이콘은 사이트의 가능한 상태를 나타냅니다.

설명	아이콘
전체 계층 구조의 최상위 사이트가 작동하고 있습니다.	
전체 계층 구조의 최상위 사이트가 아직 작동하지만 하나 이상의 문제에 주의가 필요합니다. 최상위 사이트 아이콘의 위에 표시됩니다.	
사이트가 작동하고 있습니다.	
사이트가 계층 구조에서 수락을 대기 중입니다.	
사이트가 연결 중이나 아직 작동하지 않습니다.	

시스템에서 사용되는 포트

모든 XProtect 구성 요소와 필요한 포트는 아래 목록에 나열됩니다. 예를 들어, 방화벽이 원치 않는 트래픽만 차단하도록 하려면 시스템이 사용하는 포트를 지정해야 합니다. 오직 이러한 포트만 활성화해야 합니다. 또한 목록은 로컬 프로세스에 사용된 포트를 포함합니다.

두 그룹으로 정렬됩니다.

- **서버 구성 요소** (서비스)는 특정 포트에 서비스를 제공하며, 이러한 포트에서 클라이언트 요청을 대기해야 하는 이유입니다. 따라서, 이러한 포트는 수신 및 발신 연결을 위해 Windows 방화벽에서 열려 있어야 합니다
- **클라이언트 구성 요소** (클라이언트)는 서버 구성 요소에서 특정 포트에 연결을 개시합니다. 따라서, 이러한 포트는 발신 연결을 위해 열려 있어야 합니다. 발신 연결은 보통 Windows 방화벽에서 기본값으로 열려 있습니다

달리 언급되지 않는 경우, 서버 구성 요소의 포트는 수신 연결에 열려 있어야 하며, 클라이언트 구성 요소에 대한 포트는 발신 연결을 위해 열려 있어야 합니다.

서버 구성 요소는 또한 다른 서버 구성 요소의 클라이언트로 작용할 수 있음을 염두에 두어야 합니다. 이러한 내용은 본 문서에 명시적으로 언급되어있지 않습니다.

포트 번호는 기본 번호이지만 변경할 수 있습니다. Milestone 을(를) 통해 구성할 수 없는 포트를 변경해야 하는 경우 Management Client 지원 부서에 문의하십시오.

서버 구성 요소(수신 연결)

다음 섹션의 각각은 특정 서비스를 위해 열려 있어야 하는 포트를 나열합니다. 특정 컴퓨터에서 열려 있어야 하는 포트를 결정하려면, 이 컴퓨터에서 실행 중인 모든 서비스를 고려해야 합니다.

Management Server 서비스 및 관련 프로세스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
80	HTTP	IIS	모든 서버 및 XProtect Smart Client와(과) Management Client	포트 80과 포트 443의 목적은 동일합니다. 그러나 비디오 관리 소프트웨어가 사용하는 포트는 통신 보안을 위해 인증서를 사용했는지 여부에 따라 다릅니다. • 인증서로 통신을 보호하지 않은 경우 비디오 관리 소프트웨어는 포트 80을 사용합니다. • 인증서로 통신을 보호하면 비디오 관리 소프트웨어는 이벤트 서버에서 관리 서버로의 통신을 제외하고 포트 443을 사용합니다. 이벤트 서버에서 관리 서버로의 통신은 포트 80에서 Windows 보안 프레임워크(WCF) 및 Windows 인증을 사용합니다.
443	HTTPS	IIS		
6473	TCP	Management Server 서비스	Management Server Manager 트레이 아이콘, 로컬 연결만 해	상태 표시 및 서비스 관리.

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
			당.	
8080	TCP	관리 서버	로컬 연결 전용.	서버의 내부 프로세스 사이의 통신.
9000	HTTP	관리 서버	Recording Server 서비스	서버 간 내부 통신을 위한 웹 서비스.
12345	TCP	Management Server 서비스	XProtect Smart Client	시스템과 Matrix 수신자 사이에 통신. Management Client 에서 포트 번호를 변경할 수 있습니다.
12974	TCP	Management Server 서비스	Windows SNMP 서비스	SNMP 확장 에이전트를 이용한 통신. 사용 중인 시스템이 SNMP를 적용하지 않더라도 포트를 다른 목적으로 사용하지 마십시오. XProtect 2014 시스템이나 그 이전 버전에서 포트 번호는 6475이었습니다. XProtect 2019 R2 시스템을 포함한 이전 버전에서 포트 번호는 7475였습니다.

SQL Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
1433	TCP	SQL Server	Management Server 서비스	Identity Provider 을(를) 통한 구성 저장 및 검색.
1433	TCP	SQL Server	Event Server 서비스	Identity Provider 을(를) 통한 이벤트의 저장 및 검색.
1433	TCP	SQL Server	Log Server 서비스	Identity Provider 을(를) 통한 로그 엔트리의 저장 및 검색.

Data Collector 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
7609	HTTP	IIS	관리 서버 컴퓨터에서: 다른 모든 서버에 Data Collector 서비스. 다른 컴퓨터에서: 관리 서버에 Data Collector 서비스.	시스템 모니터.

Event Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
1234	TCP/UDP	Event Server 서비스	일반 이벤트를 사용 중인 XProtect 시스템에 전송하는 서버.	외부 시스템 또는 장치에서 일반 이벤트 수신. 관련 데이터 소스가 사용 가능한 경우만.
1235	TCP	Event Server 서비스	일반 이벤트를 사용 중인 XProtect 시스템에 전송하는 서버.	외부 시스템 또는 장치에서 일반 이벤트 수신. 관련 데이터 소스가 사용 가능한 경우만.
9090	TCP	Event Server 서비스	XProtect 시스템에 분석 이벤트를 전송하는 시스템 또는 서비스.	외부 시스템 또는 장치에서 분석 이벤트 수신. 분석 이벤트 기능이 활성화된 경우에만 적절.
22331	TCP	Event Server 서비스	XProtect Smart Client 및 Management Client	구성, 이벤트, 알람 및 맴 데이터.
22332	WS/WSS HTTP/HTTPS*	Event Server 서비스	API Gateway 및 Management Client	이벤트/상태 구독, 이벤트 REST API, Websockets 메시징 API, 알람 REST API
22333	TCP	Event Server 서비스	MIP 플러그 인 및 애플리케이션.	MIP 메시징.

*HTTPS 전용 엔드포인트에 액세스하기 위해 HTTP에 액세스할 때 403 오류가 반환됩니다.

Recording Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
25	SMTP	Recording Server 서비스	카메라, 인코더 및 I/O 장치.	장치에서 이벤트 메시지 수신. 이 포트는 기본적으로 비활성화되어 있습니다. (사용되지 않음) 이를 활성화하면 비암호화된 연결에 대해 포트가 개방되며 권장되지 않습니다.
5210	TCP	Recording Server 서비스	장애 조치 레코딩 서버.	장애 조치 레코딩 서버가 실행된 후 데이터베이스 병합.
5432	TCP	Recording Server 서비스	카메라, 인코더 및 I/O 장치.	장치에서 이벤트 메시지 수신. 이 포트는 기본적으로 비활성화되어 있습니다.
7563	TCP	Recording Server 서비스	XProtect Smart Client, Management Client	비디오 및 오디오 스트림, PTZ 명령 검색.
8966	TCP	Recording Server 서비스	Recording Server Manager 트레이 아이콘, 로컬 연결만 해당.	상태 표시 및 서비스 관리.
9001	HTTP	Recording Server 서비스	관리 서버	서버 간 내부 통신을 위한 웹 서비스. 다중 레코딩 서버 인스턴스가 사용 중인 경우 모든 인스턴스는 각자 고유한 포트가 필요합니다. 추가 포트는 9002, 9003 등등입니다.
11000	TCP	Recording Server 서비스	장애 조치 레코딩 서버	레코딩 서버의 상태 폴링.

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
12975	TCP	Recording Server 서비스	Windows SNMP 서비스	SNMP 확장 에이전트를 이용한 통신. 사용 중인 시스템이 SNMP를 적용하지 않더라도 포트를 다른 목적으로 사용하지 마십시오. XProtect 2014 시스템이나 그 이전 버전에서 포트 번호는 6474이었습니다. XProtect 2019 R2 시스템을 포함한 이전 버전에서 포트 번호는 7474였습니다.
65101	UDP	Recording Server 서비스	로컬 연결 전용	드라이버에서 이벤트 알림 수신.

위에 나열된 Recording Server 서비스로의 수신 연결 외에도, Recording Server 서비스는 다음에 대한 발신 연결을 설정합니다:

- 카메라
- NVR
- 원격 상호 연결 사이트(Milestone 상호 연결 ICP)

Failover Server 서비스 및 Failover Recording Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
25	SMTP	Failover Recording Server 서비스	카메라, 인코더 및 I/O 장치.	장치에서 이벤트 메시지 수신. 이 포트는 기본적으로 비활성화되어 있습니다. (사용되지 않음) 이를 활성화하면 비암호화된 연결에 대해 포트가 개방되며 권장되지 않습니다.

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
5210	TCP	Failover Recording Server 서비스	장애 조치 레코딩 서버	장애 조치 레코딩 서버가 실행된 후 데이터베이스 병합.
5432	TCP	Failover Recording Server 서비스	카메라, 인코더 및 I/O 장치.	장치에서 이벤트 메시지 수신. 이 포트는 기본적으로 비활성화되어 있습니다.
7474	TCP	Failover Recording Server 서비스	Windows SNMP 서비스	SNMP 확장 에이전트를 이용한 통신. 사용 중인 시스템이 SNMP를 적용하지 않더라도 포트를 다른 목적으로 사용하지 마십시오.
7563	TCP	Failover Recording Server 서비스	XProtect Smart Client	비디오 및 오디오 스트림, PTZ 명령 검색.
8844	UDP	Failover Recording Server 서비스	장애 조치 레코딩 서버 서비스 간의 통신.	서버 사이의 통신.
8966	TCP	Failover Recording Server 서비스	Failover Recording Server Manager 트레이 아이콘, 로컬 연결만 해당.	상태 표시 및 서비스 관리.
8967	TCP	Failover Server 서비스	Failover Server Manager 트레이 아이콘, 로컬 연결만 해당.	상태 표시 및 서비스 관리.
8990	HTTP	Failover Server 서비스	Management Server 서비스	Failover Server 서비스의 상태 모니터링.
9001	HTTP	Failover Server 서비스	관리 서버	서버 간 내부 통신을 위한 웹 서비스.

위에 나열된 Failover Server / Failover Recording Server 서비스로의 수신 연결 외에도, Failover Server / Failover Recording Server 서비스는 일반 레코다, 카메라와 비디오 푸시에 대한 발신 연결을 설정합니다.

Log Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
22337	HTTP	Log Server 서비스	Management Client 을(를) 제외한 모든 XProtect 구성 요소 및 레코딩 서버.	로그 서버에 쓰기, 읽기 및 구성.

Mobile Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
8000	TCP	Mobile Server 서비스	Mobile Server Manager 트레이 아이콘, 로컬 연결만 해당.	SysTray 애플리케이션.
8081	HTTP	Mobile Server 서비스	모바일 클라이언트, 웹 클라이언트 및 Management Client.	데이터 스트림, 비디오 및 오디오 전송.
8082	HTTPS	Mobile Server 서비스	모바일 클라이언트 및 웹 클라이언트.	데이터 스트림, 비디오 및 오디오 전송.
40001~40099	HTTP	Mobile Server 서비스	레코딩 서버 서비스	Mobile Server 비디오 푸시. 이 포트 범위는 기본적으로 비활성화되어 있습니다.

LPR Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
22334	TCP	LPR Server 서비스	이벤트 서버	인식되는 자동차번호판 및 서버 상태 검색. 연결하려면, 이벤트 서버가 LPR 플러그인을 설치해야 합니다.
22334	TCP	LPR Server 서비스	LPR Server Manager 트레이 아이콘, 로컬 연결만 해당.	SysTray 애플리케이션

Milestone Open Network Bridge 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
580	TCP	Milestone Open Network Bridge 서비스	ONVIF 클라이언트	비디오 스트림 구성에 대한 인증 및 요청.
554	RTSP	RTSP 서비스	ONVIF 클라이언트	ONVIF 클라이언트로 요청된 비디오의 스트리밍.

XProtect DLNA Server 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
9100	HTTP	DLNA Server 서비스	DLNA 장치	장치 검색 및 DLNA 채널 구성 제공. 비디오 스트림 요청.
9200	HTTP	DLNA Server 서비스	DLNA 장치	DLNA 장치로 요청된 비디오의 스트리밍.

XProtect Screen Recorder 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
52111	TCP	XProtect Screen Recorder	Recording Server 서비스	모니터로부터 비디오를 제공합니다. 레코딩 서버에 카메라와 동일한 방법으로 표시되고 작동합니다. Management Client 에서 포트 번호를 변경할 수 있습니다.

XProtect Incident Manager 서비스

포트 번호	프로토콜	프로세스	다음으로부터 연결...	목적
80	HTTP	IIS	XProtect Smart Client 및 Management Client	포트 80과 포트 443의 목적은 동일합니다. 그러나 비디오 관리 소프트웨어가 사용하는 포트는 통신 보안을 위해 인증서를 사용했는지 여부에 따라 다릅니다. • 인증서로 통신을 보호하지 않은 경우 비디오 관리 소프트웨어는 포트 80을 사용합니다. • 인증서로 통신을 보호하면 비디오 관리 소프트웨어는 포트 443을 사용합니다.
443	HTTPS	IIS		

서버 구성 요소(발신 연결)

Management Server 서비스

포트 번호	프로토콜	다음에 연결...	목적
443	HTTPS	라이선스 관리 서비스를 호스팅하는 라이선스 서버입니다. 통신은 https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx 를 통해 이루어집니다.	라이선스 활성화.

Recording Server 서비스

포트 번호	프로토콜	다음에 연결...	목적
80	HTTP	카메라, NVR, 인코더 상호 연결된 사이트	인증, 구성, 데이터 스트림, 비디오 및 오디오. 로그인
443	HTTPS	카메라, NVR, 인코더	인증, 구성, 데이터 스트림, 비디오 및 오디오.
554	RTSP	카메라, NVR, 인코더	데이터 스트림, 비디오 및 오디오.
7563	TCP	상호 연결된 사이트	데이터 스트림 및 이벤트.
11000	TCP	장애 조치 레코딩 서버	레코딩 서버의 상태 폴링.
40001~40099	HTTP	Mobile Server 서비스	Mobile Server 비디오 푸시. 이 포트 범위는 기본적으로 비활성화되어 있습니다.

Failover Server 서비스 및 Failover Recording Server 서비스

포트 번호	프로토콜	다음에 연결...	목적
11000	TCP	장애 조치 레코딩 서버	레코딩 서버의 상태 폴링.

Event Server 서비스

포트 번호	프로토콜	다음에 연결...	목적
80	HTTP	API Gateway 및 Management Server	API Gateway에서 구성 API에 액세스
443	HTTPS	API Gateway 및 Management Server	API Gateway에서 구성 API에 액세스
443	HTTPS	Milestone Customer Dashboard 다음을 통해 https://service.milestonesys.com/	상태, 이벤트 및 오류 메시지를 XProtect 시스템으로부터 Milestone Customer Dashboard (으)로 전송합니다.

Log Server 서비스

포트 번호	프로토콜	다음에 연결...	목적
443	HTTP	로그 서버	로그 서버로 메시지 전달.

API Gateway

포트 번호	프로토콜	다음에 연결...	목적
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	이벤트/상태 구독, 이벤트 REST API, Websockets 메시징 API, 알람 REST API

카메라, 인코더 및 입출력 장치(수신 연결)

포트 번호	프로토콜	다음으로부터 연결...	목적
80	TCP	레코딩 서버 및 장애 조치 레코딩 서버	인증, 구성 및 데이터 스트림; 비디오 및 오디오.
443	HTTPS	레코딩 서버 및 장애 조치 레코딩 서버	인증, 구성 및 데이터 스트림; 비디오 및 오디오.
554	RTSP	레코딩 서버 및 장애 조치 레코딩 서버	데이터 스트림, 비디오 및 오디오.

카메라, 인코더 및 입출력 장치(발신 연결)

포트 번호	프로토콜	다음에 연결...	목적
25	SMTP	레코딩 서버 및 장애 조치 레코딩 서버	이벤트 알림 전송(사용되지 않음).
5432	TCP	레코딩 서버 및 장애 조치 레코	이벤트 알림 전송.

포트 번호	프로토콜	다음에 연결...	목적
		딩 서버	이 포트는 기본적으로 비활성화되어 있습니다.
22337	HTTP	로그 서버	로그 서버로 메시지 전달.

몇 개의 카메라 모델만 발신 연결을 설정할 수 있습니다.

클라이언트 구성 요소(발신 연결)

XProtect Smart Client, XProtect Management Client, XProtect Mobile 서버

포트 번호	프로토콜	다음에 연결...	목적
80	HTTP	API Gateway 및 Management Server 서비스	인증 및 API Gateway의 기타 API
443	HTTPS	API Gateway 및 Management Server 서비스	암호화가 활성화된 경우의 기본 사용자 인증 및 API Gateway의 기타 API
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com at 52.178.114.226)	Management Client 및 Smart Client 은(는) 도움말 URL에 액세스하여 온라인 도움말이 사용 가능한지 체크합니다.
7563	TCP	Recording Server 서비스	비디오 및 오디오 스트림, PTZ 명령 검색.
22331	TCP	Event Server 서비스	알람.

XProtect Web Client, XProtect Mobile 클라이언트

포트 번호	프로토콜	다음에 연결...	목적
8081	HTTP	XProtect Mobile 서버	비디오 및 오디오 스트림 검색.
8082	HTTPS	XProtect Mobile 서버	비디오 및 오디오 스트림 검색.

API Gateway

포트 번호	프로토콜	다음에 연결...	목적
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

애플리케이션 풀

VMS에는 .NET v4.5, .NET v4.5 Classic, DefaultAppPool. 등의 표준 애플리케이션 풀이 포함되어 있습니다. 시스템에서 사용할 수 있는 애플리케이션 풀은 인터넷 정보 서비스(IIS) 관리자에 나타납니다. 위에 언급된 표준 애플리케이션 풀 외에도 일련의 VideoOS 애플리케이션 풀이 Milestone XProtect VMS와(과) 함께 제공됩니다.

Milestone XProtect의 애플리케이션 풀

아래 표에서 Milestone XProtect와(과) 함께 제공되는 VideoOS 애플리케이션 풀의 개요를 확인할 수 있습니다.

이름	ID	목적
.NET v4.5	ApplicationPoolId	표준 IIS 기능
.NET v4.5 Classic	ApplicationPoolId	표준 IIS 기능
DefaultAppPool	ApplicationPoolId	표준 IIS 기능
VideoOS ApiGateway	NetworkService	미래의 공용 XProtect API이자 VMS에 대한 게이트웨이인 API 게이트웨이를 호스팅합니다.
VideoOS Classic	NetworkService	주로 역호환성을 준수하기 위해 로컬 도움말과 같은 레거시 구성 요소를 호스팅합니다.
VideoOS IDP	NetworkService	Identity Provider API를 호스팅합니다. Identity Provider은(는) 기본 사용자를 위한 ID 정보를 생성, 유지, 관리하고 애플리케이션 또는 서비스에 의존하는 인증 및

이름	ID	목적
		등록 서비스를 제공합니다.
VideoOS IM	NetworkService	XProtect Incident Manager API를 호스팅합니다. XProtect Incident Manager 문서는 사고를 문서화하고 XProtect VMS의 시퀀스 증거(비디오 및 오디오)와 결합합니다.
VideoOS Management Server	NetworkService	구성 API, 서버 구성 요소 API, 기타 Management Server 서비스를 호스팅하고 사용자 인증을 관리합니다.
VideoOS ReportServer	NetworkService	알람 및 이벤트에 대한 보고서를 수집하고 생성하는 웹 응용 프로그램을 호스팅합니다.
VideoOS ShareService	NetworkService	XProtect Mobile 클라이언트 사용자 간에 북마크 및 라이브 비디오 공유를 촉진하는 서비스를 호스팅합니다.

애플리케이션 풀 작업

인터넷 정보 서비스(IIS) 창의 **애플리케이션 풀** 페이지에서 애플리케이션 풀을 추가하거나 애플리케이션 풀 기본값을 설정할 수 있으며 각 애플리케이션 풀이 호스팅하는 애플리케이션을 볼 수 있습니다.

애플리케이션 풀 페이지 열기

1. Windows **시작** 메뉴에서 **인터넷 정보 서비스(IIS) 관리자**를 엽니다.
2. **연결** 창에서 환경 이름을 클릭한 다음 **애플리케이션 풀**을 클릭합니다.
3. **작업** 아래에서 **애플리케이션 풀 추가** 또는 **애플리케이션 풀 기본값 설정**을 클릭하여 이러한 작업을 수행합니다.
4. **애플리케이션 풀** 페이지에서 애플리케이션 풀을 선택하여 각 애플리케이션 풀에 대한 **작업** 아래에 추가 옵션을 표시합니다.

제품 비교

XProtect VMS 에는 다음 제품들이 포함됩니다.

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

라이센싱

라이선스(설명됨)

자유 XProtect Essential+

XProtect Essential+ 을(를) 설치한 경우, 시스템과 8개의 장치 라이선스를 무료로 구동할 수 있습니다. 자동 라이선스 활성화를 사용할 수 있으며 하드웨어를 시스템에 추가하면 바로 활성화됩니다.

보다 개선된 XProtect 제품으로 업그레이드하는 경우 및 SLC(소프트웨어 라이선스 코드)를 변경해야 하는 경우에만(페이지 113의 소프트웨어 라이선스 코드 변경 참조), 본 주제의 나머지 부분과 본 문서에서 다루는 다른 라이선싱 관련 내용이 적용될 수 있습니다.

XProtect 비디오 관리 소프트웨어 제품을 위한 라이선스 (XProtect Essential+ 제외)

소프트웨어 라이선스 파일 및 SLC

소프트웨어와 라이선스를 구매할 때, 다음 사항이 제공됩니다.

- 주문 확인서 및 SLC(소프트웨어 라이선스 코드)의 이름을 따서 명명되고 이메일 하나 당 수신한 .lic 확장자를 가진 소프트웨어 라이선스 파일
- Milestone Care 적용 범위

SLC는 주문 확인서에도 인쇄되어 있으며 다음과 같이 하이픈으로 묶인 여러 개의 숫자와 문자로 구성되어 있습니다.

- 제품 버전 2014 이하: xxx-xxxx-xxxx
- 제품 버전 2016 이상: xxx-xxx-xxx-xx-xxxxxx

소프트웨어 라이선스 파일에는 구입한 비디오 관리 소프트웨어 제품, XProtect 확장, 라이선스에 관한 모든 정보가 들어 있습니다. Milestone 은(는) SLC 및 소프트웨어 라이선스 파일의 사본을 나중에 사용할 수 있도록 안전한 장소에 보관해 둘 것을 권장합니다. 또한, Management Client의 **라이선스 정보** 창에서 SLC을(를) 확인할 수 있습니다. **사이트 탐색** 창에서 **라이선스 정보** 창 -> **기본** 노드 -> **라이선스 정보** 를 엽니다. 예를 들어 My Milestone 사용자 계정을 생성하거나 지원을 위해 리셀러에 연락하거나 시스템을 변경해야 하는 경우, 소프트웨어 라이선스 파일 또는 SLC가 필요할 수 있습니다.

설치 및 라이선싱에 대한 전반적인 프로세스

시작하려면 당사 웹사이트(https://www.milestonesys.com/downloads/)에서 소프트웨어를 다운로드하십시오. 소프트웨어를 설치하는 동안(페이지 135의 신규 XProtect 시스템 설치 참조) 소프트웨어 라이선스 파일을 제공하도록 요청받게 됩니다. 소프트웨어 라이선스 파일 없으면 설치를 완료할 수 없습니다.

설치가 완료되고 일부 카메라를 추가한 후에는 라이선스를 활성화해야 합니다(페이지 107의 라이선스 활성화(설명됨) 참조). 라이선스는 **의** 라이선스 정보Management Client 창에서 활성화할 수 있습니다. 또한 여기서 동일한 SLC 상의 모든 설치에 대한 라이선스의 개요를 확인할 수 있습니다. **사이트 탐색** 창에서 **라이선스 정보** 창 -> **기본** 노드 -> **라이선스 정보** 를 엽니다.

라이선스 유형

XProtect 라이선스 시스템에는 다양한 라이선스 유형이 있습니다.

기본 라이선스

최소한 귀하는 XProtect 비디오 관리 소프트웨어 제품 중 하나에 대한 기본 라이선스를 보유하게 됩니다. 또한 XProtect 확장에 대해 기본 라이선스가 하나 이상 있을 수 있습니다.

장치 라이선스

최소한 귀하는 다양한 장치 라이선스를 보유하게 됩니다. 일반적으로 시스템에 추가할 카메라가 있는 하드웨어 장치 하나당 장치 라이선스 하나가 필요합니다. 하지만 이는 하드웨어에 따라 그리고 Milestone 지원 하드웨어인 하드웨어 장치인지의 여부에 따라 달라집니다. 자세한 정보는 페이지 106의 지원되는 하드웨어 장치 및 를 참조하십페이지 106의 지원되지 않는 하드웨어 장치시오.

비디오 푸시 기능을 XProtect Mobile 에서 사용하려는 경우, 귀하는 또한 시스템에 비디오를 푸시할 수 있는 모바일 장치 또는 태블릿 하나당 장치 라이선스 하나가 필요합니다.

장치 라이선스는 스피커, 마이크 또는 카메라에 부착된 입출력 장치에는 필요하지 않습니다.

지원되는 하드웨어 장치

일반적으로 시스템에 추가할 카메라가 있는 하드웨어 장치 하나당 장치 라이선스 하나가 필요합니다. 그러나 일부 지원되는 하드웨어 장치에는 하나 이상의 장치 라이선스가 필요합니다. 하드웨어 장치에 필요한 장치 라이선스 수는 Milestone 웹사이트(https://www.milestonesys.com/support/tools-and-references/supported-devices/)의 지원되는 하드웨어 목록에서 확인할 수 있습니다.

최대 16채널을 지원하는 비디오 인코더의 경우, 비디오 인코더 IP 주소 하나당 장치 라이선스 하나만 있으면 됩니다. 비디오 인코더에는 하나 이상의 IP 주소가 있을 수 있습니다.

그러나 16채널 이상 지원되는 비디오 인코더인 경우, 비디오 인코더의 활성화된 카메라당 하나의 장치 라이선스가 필요하며 또한 16개의 처음 활성화된 카메라에 대해서도 필요합니다.

지원되지 않는 하드웨어 장치

지원되지 않는 하드웨어 장치에는 비디오 채널을 사용하는 활성화된 카메라 하나당 장치 라이선스 하나가 필요합니다.

지원되지 않는 하드웨어 장치는 Milestone 웹사이트(https://www.milestonesys.com/support/tools-and-references/supported-devices/)의 지원되는 하드웨어 목록에 수록되지 않은 장치입니다.

다음을 위한 카메라 라이선스: Milestone Interconnect™

Milestone Interconnect 을(를) 실행하려면 원격 사이트에 있는 하드웨어 장치의 비디오를 보기 위해 중앙 사이트에 Milestone Interconnect 카메라 라이선스가 필요합니다. 필수 Milestone Interconnect 카메라 라이선스 수는 데이터 수신을 원하는 원격 사이트의 하드웨어 장치 수에 따라 달라집니다. 오로지 XProtect Corporate 만 중앙 사이트 역할을 할 수 있습니다.

XProtect 확장의 라이선스

대부분의 XProtect 확장에는 추가 라이선스 유형이 필요합니다. 소프트웨어 라이선스 파일에는 확장 라이선스에 대한 정보도 포함되어 있습니다. 일부 확장에는 별도의 고유 소프트웨어 라이선스 파일이 있습니다.

라이선스 활성화(설명됨)

귀하의 SLC는 설치 전에 등록되어야 합니다(페이지 133의 소프트웨어 라이선스 코드 등록 참조). SLC와 연결된 다양한 라이선스는 설치된 XProtect 비디오 관리 소프트웨어 및 XProtect 확장이 작동하도록 활성화되고 개별 하드웨어 장치가 시스템에 데이터를 전송할 수 있도록 활성화 되어야 합니다. 모든 XProtect 라이선스 유형에 대한 개요는 페이지 106의 라이선스 유형를 참조하십시오.

라이선스 활성화 방법은 다양합니다. 모든 방법은 **라이선스 정보** 창에서 이용할 수 있습니다. 최상의 활성화 방법은 귀하의 기관 정책 및 관리 서버의 인터넷 연결 여부에 따라 달라집니다. 라이선스 활성화 방법에 대해 알아보려면 페이지 111의 라이선스 활성화를 참조하십시오.

귀하의 XProtect 비디오 관리 소프트웨어의 라이선스를 처음 활성화한 후에는 XProtect 라이선싱 시스템에 자체적인 유연성을 갖게 되므로 카메라가 있는 하드웨어 장치를 추가할 때마다 장치 라이선스를 활성화할 필요가 없게 됩니다. 이러한 유연성에 관한 자세한 정보는 페이지 108의 라이선스 활성화 유예 기간(설명됨) 및 를 참조하십페이지 108의 활성화 없이 장치 변경(설명됨)시오.

자동 라이선스 활성화(설명됨)

간편한 관리 및 유연성을 위해, 그리고 귀하의 조직 정책이 허락하는 경우, Milestone 은(는) 자동 라이선스 활성화를 켜 둘 것을 권장합니다. 자동 라이선스 활성화를 할 경우 관리 서버가 온라인이어야 합니다. 자동 라이선스 활성화를 켜는 방법은 페이지 111의 자동 라이선스 활성화를 참조하십시오.

자동 라이선스 활성화를 켜면 얻게 되는 이점

- 귀하가 하드웨어 장치를 추가, 제거 또는 대체하거나 라이선스 사용에 영향을 주는 기타 변경 조치를 한 후 수 분 이내에 시스템이 하드웨어 장치를 활성화합니다. 그러므로 라이선스 활성화를 위해 수동으로 시작할 일이 거의 없게 됩니다. 일부 예외 사항은 페이지 107의 수동 라이선스 활성화가 여전히 필요한 경우를 참조하십시오.
- 활성화를 하지 않은 장치 변경에 사용된 수는 언제나 0입니다.
- 어떤 하드웨어 장치도 유예 기간의 적용을 받게 되거나 유효 기간 종료의 위험을 겪게 되지 않습니다.
- 기본 라이선스 중 하나가 14일 내에 만료되는 경우, XProtect 시스템이 추가적 사전 주의 조치로서 매일 밤 라이선스 활성화를 자동으로 시도합니다.

수동 라이선스 활성화가 여전히 필요한 경우

다음과 같은 시스템 변경을 하는 경우, 수동 라이선스 활성화가 필요합니다.

- 추가 라이선스 구입(페이지 113의 추가 라이선스 구입 참조)
- 신규 버전 또는 고급형 비디오 관리 소프트웨어 시스템으로 업그레이드(페이지 344의 업그레이드 요구 사항 참조)
- Milestone Care 구독 구입 또는 갱신
- 활성화 없이 더 많은 장치 변경을 할 수 있도록 허가받은 경우(페이지 108의 활성화 없이 장치 변경(설명됨) 참조)

라이선스 활성화 유예 기간(설명됨)

비디오 관리 소프트웨어를 설치하고 장치를 추가한 경우(하드웨어 장치, Milestone Interconnect 카메라, 또는 문 라이선스), 자동 라이선스 활성화를 켜지 않기로 했다면 장치는 30일 유예 기간 동안 구동됩니다. 30일 유예 기간 종료 전 그리고 더 이상 활성화 없이 변경할 장치가 남아있지 않은 경우에는 라이선스를 활성화해야 하며, 그렇지 않은 경우 귀하의 장치는 감시 시스템에 비디오 전송을 중단하게 됩니다.

활성화 없이 장치 변경(설명됨)

활성화 없이 기능성 장치 변경을 하게 되면 XProtect 라이선싱 시스템이 자체적인 유연성을 갖게 됩니다. 그러므로 수동으로 라이선스를 활성화하기로 했을지라도 하드웨어 장치를 추가 또는 삭제할 때마다 라이선스를 꼭 활성화해야 하는 것은 아닙니다.

활성화 없이 장치 변경 횟수는 설치 상황 마다 다르며 여러 변수에 따라 계산됩니다. 자세한 설명은 페이지 108의 활성화 없이 변경 가능한 장치의 수 계산(설명됨)를 참조하십시오.

마지막으로 라이선스를 활성화한 지 1년 후, 활성화 없이 귀하가 사용한 장치의 수는 자동으로 0으로 재설정됩니다. 재설정이 이루어지면 라이선스를 활성화하지 않고 하드웨어 장치를 계속 추가 및 교체할 수 있습니다.

장기 유람하는 선상의 감시 시스템이나 인터넷에 접속할 수 없는 오지의 감시 시스템의 경우와 같이 장기간 감시 시스템이 오프라인 상태에 있는 경우, Milestone 리셀러에게 연락하여 활성화 없이 장치 변경 횟수를 늘려달라고 요청할 수 있습니다.

활성화 없이 장치 변경 횟수를 늘려야 하는 정당한 이유를 설명해야 합니다. Milestone 은(는) 각 요청을 개별적으로 결정합니다. 활성화 없이 장치 변경 횟수를 늘리는 것이 승인되면 라이선스를 활성화하여 XProtect 시스템에서 늘어난 횟수를 등록해야 합니다.

활성화 없이 변경 가능한 장치의 수 계산(설명됨)

활성화 없이 변경 가능한 장치의 수는 세 가지 변수에 따라 계산됩니다. Milestone 소프트웨어를 여러 개 설치한 경우, 변수가 그 각각에 개별적으로 적용됩니다. 변수는 다음과 같습니다.

- **C%** - 활성화된 라이선스의 전체 수에 대한 고정된 백분율입니다.
- **Cmin** - 활성화 없이 장치 변경 횟수의 고정된 최소값입니다
- **Cmax** - 활성화 없이 장치 변경 횟수의 고정된 최대값입니다

활성화 없이 장치 변경 횟수는 **Cmin** 값보다 낮거나 **Cmax** 값보다 높을 수 없습니다. **C%** 변수에 기초한 계산 값은 시스템의 각 설치본에서 가지고 있는 활성화된 장치 수에 따라 달라집니다. 활성화 없이 장치 변경으로 추가된 장치는 **C%** 변수에 의해 활성화된 것으로 계산되지 않습니다.

Milestone 은(는) 이 세 가지 모든 변수의 값을 정의하며 고지 없이 값이 변경될 수 있습니다. 변수 값은 제품에 따라 다릅니다.

C% = 15%, Cmin = 10 및 Cmax =100을 가정했을 때의 예

100개의 장치 라이선스를 구입했습니다. 그리고 100대의 카메라를 시스템에 추가했습니다. 자동 라이선스 활성화를 켜지 않았다면 활성화 없이 변경한 장치의 수는 여전히 0입니다. 라이선스를 활성화하고 이제 15개 장치를 활성화 없이 변경했습니다.

100개의 장치 라이선스를 구입했습니다. 그리고 100대의 카메라를 시스템에 추가하고 라이선스를 활성화했습니다. 활성화 없이 변경된 장치의 수는 이제 15대입니다. 그리고 나서 시스템에서 하드웨어 장치 1대를 삭제하기로 결정합니다. 이제 99대의 장치가 남았으며 활성화 없이 변경된 장치의 수는 14대로 줄었습니다.

1000개의 장치 라이선스를 구입했습니다. 그리고 1000대의 카메라를 추가하고 라이선스를 활성화했습니다. 활성화 없이 변경된 장치는 이제 100대입니다. **C%** 변수에 따르면 이제 활성화 없이 변경된 장치를 150대 보유하게 되나, **Cmax** 변수에 따르면 활성화 없이 변경된 장치 100대만 보유하게 됩니다.

10대의 장치 라이선스를 구입했습니다. 그리고 10대의 카메라를 시스템에 추가하고 라이선스를 활성화했습니다. **Cmin** 변수에 따르면 활성화 없이 변경된 장치의 수는 10대입니다. **C%** 변수만 이용하여 장치 수가 계산된 경우, 귀하는 오직 1대만 보유하게 됩니다(10의 15% = 소수점 1째 자리까지 반올림하여 1.5).

115개의 장치 라이선스를 구입했습니다. 그리고 100대의 카메라를 시스템에 추가하고 라이선스를 활성화했습니다. 활성화 없이 변경된 장치의 수는 이제 15대입니다. 활성화 없이 변경된 장치 15대 중 15대를 사용하여 또 다른 15대의 카메라를 활성화 없이 추가합니다. 이제 50대의 카메라를 시스템에서 제거하면 활성화 없이 변경된 장치의 수는 7대입니다. 이는 곧 활성화 없이 변경된 15대의 장치에 이전에 추가된 8대의 카메라가 유예 기간에 들어감을 의미합니다. 이제 50대의 새 카메라를 추가합니다. 마지막으로 라이선스를 활성화 했을 때 시스템에 100대의 카메라를 활성화했으므로 활성화 없이 변경된 장치의 수는 15대 및 카메라 8대로 돌아가며, 유예 기간에 들어갔던 카메라 8대는 다시 활성화 없이 변경된 장치로 이동됩니다. 50개의 새 카메라가 유예 기간에 들어갑니다.

Milestone Care™ (설명됨)

Milestone Care 은(는) 제품수명주기 전체 기간 동안 제공되는 XProtect 제품에 대한 모든 서비스 및 지원 프로그램의 이름입니다.

Milestone Care을(를) 통해 당사의 지원 웹사이트(https://www.milestonesys.com/support/)의 지식베이스 기사, 안내서, 튜토리얼과 같은 다양한 종류의 도움말 자료를 이용할 수 있습니다.

추가 혜택을 받으려면 더 많은 사전 Milestone Care 구독을 구매할 수 있습니다.

Milestone Care Plus

Milestone Care Plus 구독에 가입한 경우 현재 XProtect VMS 제품에 대한 무료 업데이트도 이용할 수 있으며 더 고급 제품인 XProtect VMS 제품으로 업그레이드할 수 있습니다. Milestone Care Plus은(는) 다음과 같은 추가 기능도 제공합니다.

- 고객 대시보드 서비스
- 스마트 연결 기능
- 전체 푸시 알림 기능

Milestone Care Premium

Milestone Care Premium 구독을 가지고 있는 경우, Milestone 지원팀에 직접 연락할 수 있습니다. 귀하가 Milestone Care 지원팀에 연락할 때는 Milestone ID에 관한 정보를 첨부하십시오.

고급형 Milestone Care 구독의 만료, 갱신, 구매

고급 Milestone Care Plus 및 Milestone Care Premium 구독 유형의 유효 기간은 **설치된 제품** 표의 **라이선스 정보** 창에서 볼 수 있습니다. 페이지 115의 설치된 제품를 참조하십시오.

시스템에 설치한 후 Milestone Care 구독을 구입하거나 갱신하려는 경우, 수동으로 라이선스를 활성화해야 정확한 Milestone Care 정보가 표시됩니다. 페이지 112의 온라인으로 라이선스 활성화 또는 페이지 112의 오프라인으로 라이선스 활성화를 참조하십시오.

라이선스 및 하드웨어 교체(설명됨)

시스템의 카메라가 오작동하거나 기타 이유로 기존 카메라를 새 것으로 바꾸려고 하는 경우, 교체 방법에 관한 모범 사례를 소개해 드립니다.

레코딩 서버에서 카메라를 제거하는 경우 장치 라이선스를 이용할 수 있게 되지만 또한 모든 데이터베이스(카메라, 마이크, 입력, 출력)과 기존 카메라의 설정에 대한 액세스 권한을 잃게 됩니다. 기존 카메라의 데이터 베이스에 엑세스하고 해당 카메라의 설정을 새 카메라와 함께 재사용하려면 아래의 관련 옵션을 사용하십시오.

유사한 카메라로 기존 카메라 교체

유사한 카메라(제조사, 브랜드 및 모델)로 기존 카메라를 교체하는 경우 및 기존 카메라와 동일한 IP 주소를 새 카메라에 할당하는 경우, 기존 카메라의 모든 데이터베이스에 대한 액세스 권한을 유지할 수 있습니다. 새 카메라는 동일한 기존 카메라의 데이터 베이스와 설정을 계속 사용하게 됩니다. 이러한 경우 Management Client 의 설정을 변경하지 않고 기존 카메라에서 새 카메라로 네트워크 케이블을 옮기십시오.

다른 카메라로 기존 카메라 교체

다른 카메라(제조사, 브랜드 및 모델)로 기존 카메라를 교체하는 경우 **하드웨어 교체** 마법사를 사용하여(페이지 317의 하드웨어 교체 참조) 기존 카메라의 모든 연관 데이터베이스를 새 카메라로 매핑하고 기존 카메라의 설정을 재사용해야 합니다.

하드웨어 교체 후 라이선스 활성화

자동 라이선스 활성화를 켠 경우(페이지 111의 자동 라이선스 활성화 참조), 새 카메라가 자동으로 활성화됩니다.

자동 라이선스 활성화가 꺼진 경우 그리고 활성화 없이 변경된 이용 가능한 모든 장치가 사용된 경우(페이지 108의 활성화 없이 장치 변경(설명됨) 참조), 수동으로 라이선스를 활성화해야 합니다. 수동 라이선스 활성화에 관한 자세한 정보는 페이지 112의 온라인으로 라이선스 활성화 또는 페이지 112의 오프라인으로 라이선스 활성화를 참조하십시오.

라이선스에 관한 개요 받기

귀하가 SLC에 대한 개요와 구매한 라이선스의 수 및 상태에 대한 정보를 받고자 하는 이유는 다양합니다. 일부를 소개하자면 다음과 같습니다.

- 하나 이상의 새 하드웨어 장치를 추가하고 싶지만 사용하지 않은 장치 라이선스가 있거나 새로 하나를 구매해야 합니까?
- 일부 하드웨어 장치의 유예 기간이 곧 종료됩니까? 그렇다면 그러한 장치들이 비디오 관리 시스템에 데이터 전송을 중단하게 되기 전에 라이선스를 활성화해야 합니다.
- 귀하를 도와드리기 위해서는 SLC 및 Milestone Care ID에 관한 정보가 필요하다고 이전에 지원을 위한 연락을 받았습니다. 하지만 그게 어떤 정보인지 알고 계십니까?
- 다양한 XProtect 설치를 보유하고 있으며 모든 설치에 대해 동일한 SLC를 사용하고 있지만, 라이선스는 어디에 사용되며 현재 상태는 어떤지 알고 계십니까?

위와 같은 질문 등에 대한 모든 정보는 **라이선스 정보** 창에서 확인할 수 있습니다.

사이트 탐색 창에서 **라이선스 정보** 창 -> **기본** 노드 -> **라이선스 정보** 를 엽니다.

라이선스 정보 창에서 이용 가능한 다양한 정보 및 기능에 관한 자세한 내용을 알아보려면, 페이지 114의 라이선스 정보 창를 참조하십시오.

라이선스 활성화

라이선스 활성화 방법은 다양합니다. 모든 방법은 **라이선스 정보** 창에서 이용할 수 있습니다. 최상의 활성화 방법은 귀하의 기관 정책 및 관리 서버의 인터넷 연결 여부에 따라 달라집니다.

사이트 탐색 창에서 **라이선스 정보** 창 -> **기본** 노드 -> **라이선스 정보** 를 엽니다.

라이선스 정보 창에서 이용 가능한 다양한 정보 및 기능에 관한 자세한 내용을 알아보려면, 페이지 114의 라이선스 정보 창를 참조하십시오.

자동 라이선스 활성화

간편한 관리 및 유연성을 위해, 그리고 귀하의 조직 정책이 허락하는 경우, Milestone 은(는) 자동 라이선스 활성화를 켜 둘 것을 권장합니다. 자동 라이선스 활성화를 할 경우 관리 서버가 온라인이어야 합니다.

자동 라이선스 활성화의 모든 이점은 페이지 107의 자동 라이선스 활성화(설명됨)에서 확인하십시오.

1. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서 **자동 라이선스 활성화 켜기** 를 선택합니다.
2. 자동 라이선스 활성화에 사용할 사용자 이름과 암호를 입력합니다.
   - 기존 사용자일 경우, 사용자 이름과 암호를 입력하여 소프트웨어 등록 시스템에 로그인합니다
   - 새 사용자인경우 **새 사용자 생성** 링크를 클릭하여 새로운 사용자 계정을 설정하고 다음 등록 과정을 따릅니다. 소프트웨어 라이센스 코드(SLC)를 아직 등록하지 않은 경우, 반드시 등록해야 합니다

   자격 증명은 관리 서버에 파일로 저장됩니다.

3. **확인** 을 클릭합니다.

나중에 자동 활성화를 위한 사용자 이름 및/또는 암호를 변경하려는 경우, **활성화 자격 증명 편집** 링크를 클릭하십시오.

자동 라이선스 활성화 사용 안 함

귀하의 기관에서 자동 라이선스 활성화 사용을 허용하지 않거나 사용하지 않기로 결정하신 경우, 자동 라이선스 활성화를 끌 수 있습니다.

끄기 방법은 나중에 자동 라이선스 활성화를 다시 사용할지 여부에 따라 달라집니다.

활성화를 끄지만 나중에 사용하도록 암호를 유지합니다.

1. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서 **자동 라이선스 활성화 켜기** 를 선택합니다. 그래도 사용자 이름과 암호는 계속 관리 서버에 저장됩니다.

활성화를 끄고 암호를 삭제합니다.

1. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서 **활성화 자격 증명 편집** 을 클릭합니다.
2. **암호 삭제** 를 클릭합니다.
3. 관리 서버에서 사용자 이름과 암호를 삭제하기 원하는지 확인합니다.

온라인으로 라이선스 활성화

관리 서버가 인터넷에 연결되어 있으나 활성화 과정을 수동으로 시작하고자 하는 경우, 이 방법이 가장 편리한 라이선스 활성화 옵션입니다.

1. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서, **수동으로 라이선스 활성화** 를 선택한 후 **온라인** 을 선택합니다.
2. **온라인 활성화** 대화 상자가 열립니다.
   - 기존 사용자인 경우, 사용자 이름과 암호를 입력합니다
   - 신규 사용자인 경우, **새 사용자 만들기** 링크를 클릭하여 새로운 사용자 계정을 설정합니다. 소프트웨어 라이센스 코드(SLC)를 아직 등록하지 않은 경우, 반드시 등록해야 합니다
3. **확인** 을 클릭합니다.

온라인 활성화 중 오류 메시지가 표시되면 화면에 나타나는 지침을 따라 문제를 해결하거나 Milestone 지원 부서로 연락하십시오.

오프라인으로 라이선스 활성화

귀하의 기관이 관리 서버에 대한 인터넷 연결을 허용하지 않는 경우, 귀하는 오프라인에서 수동으로 라이선스를 활성화해야 합니다.

1. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서, **수동으로 라이선스 활성화** > **오프라인** > **활성화를 위해 라이선스 내보내기** 를 선택하여 추가된 하드웨어 장치 및 기타 라이선스에 필요한 구성 요소에 관한 정보가 포함된 라이선스 요청 파일(.lrq)을 내보내기 합니다.
2. 라이선스 요청 파일(.lrq)은 자동으로 SLC와 동일한 이름을 부여 받습니다. 다수의 사이트를 보유한 경우 어떤 파일이 어떤 사이트에 속한 것인지 쉽게 확인할 수 있도록 이 이름을 변경하십시오.
3. 인터넷에 접근할 수 있는 컴퓨터에 라이선스 요청 파일을 복사해 두고 당사 웹사이트 (https://online.milestonesys.com/)에 로그인하여 활성화된 소프트웨어 라이선스 파일(.lic)을 받으십시오.
4. 다운 받은 .lic 파일을 Management Client 이(가) 있는 컴퓨터에 복사하십시오. 이 파일은 라이선스 요청 파일과 동일한 이름을 부여받습니다.
5. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서, **오프라인에서 라이선스 활성화** > **활성화된 라이선스 가져오기** 를 선택한 후, 활성화된 소프트웨어 라이선스 파일을 선택하여 가져기를 완료하면 라이선스가 활성화됩니다.
6. **마침** 을 클릭하여 활성화 프로세스를 종료합니다.

유예 기간 후 라이선스 활성화

수동으로 라이선스 활성화를 하기로 했으나 유예 기간 내에 라이선스 활성화를 하는 것을 잊은 경우(하드웨어 장치, Milestone Interconnect 카메라, 문 라이선스, 기타), 해당 라이선스를 사용하는 장치는 이용할 수 없게 되며 감시 시스템에 데이터를 전송할 수 없게 됩니다.

라이선스유예기간이만료되었다고하더라도귀하가완료한장치구성및설정은저장되어라이선스활성화시에사용됩니다.

이용할 수 없는 장치를 다시 활성화하려면 선호하는 방식을 통해 수동으로 라이선스를 활성화하십시오. 자세한 정보는 페이지 112의 오프라인으로 라이선스 활성화 또는 페이지 112의 온라인으로 라이선스 활성화를 참조하십시오.

추가 라이선스 구입

현재 보유한 장치 라이선스보다 더 많은 하드웨어 장치, Milestone Interconnect 시스템, 문 또는 기타 구성 요소를 추가하거나 이미 추가한 경우, 시스템에 데이터를 보내기 위해 이들을 켜려면 추가 라이선스를 구입해야 합니다.

- 시스템의 추가 라이선스를 구매하려면, XProtect 제품 리셀러에게 문의하십시오

기존 감시 시스템 버전에 대한 신규 라이선스를 구입한 경우:

- 간단히 라이선스를 수동으로 활성화하여 새 라이선스를 이용합니다. 자세한 정보는 페이지 112의 온라인으로 라이선스 활성화 또는 페이지 112의 오프라인으로 라이선스 활성화를 참조하십시오.

신규 라이선스를 구압하고 감시 시스템 버전을 업그레이드한 경우:

- 새 라이선스 및 새 버전과 함께 업데이트된 소프트웨어 라이선스 파일(.lic)을 받습니다. 새 버전을 설치할 때 새 소프트웨어 라이선스 파일을 사용해야 합니다. 자세한 정보는 페이지 344의 업그레이드 요구 사항를 참조하십시오.

소프트웨어 라이선스 코드 변경

사용자가 일시적으로 소프트웨어 라이선스 코드(SLC)상에서 설치하거나 더욱 고급형인 XProtect 제품으로 업그레이드한 경우, SLC를 영구 또는 고급 SLC로 변경할 수 있습니다. 신규 소프트웨어 라이선스를 받은 경우, 프로그램 삭제 또는 재설치를 할 필요 없이 SLC를 변경할 수 있습니다.

관리 서버상에서 또는 Management Client 에서 원격으로 할 수 있습니다.

관리 서버 트레이 아이콘에서

1. 관리 서버에서 작업 표시줄의 알림 영역으로 이동합니다.

2. **관리 서버** 아이콘을 마우스 오른쪽 단추로 클릭하고 **라이선스 변경** 을 선택합니다.
3. **라이선스 가져오기** 를 클릭합니다.
4. 다음으로, 이 용도로 저장한 소프트웨어 라이선스를 선택합니다. **끝나면 선택한 소프트웨어 라이선스 파일 위치가** 라이선스 가져오기 단추 바로 아래에 추가됩니다.
5. **확인** 을 클릭하면 SLC를 등록할 수 있게 됩니다. 페이지 133의 소프트웨어 라이선스 코드 등록를 참조하십시오.

Management Client 에서

1. 다운 받은 .lic 파일을 Management Client 이(가) 있는 컴퓨터에 복사하십시오.
2. **사이트 탐색** 창 -> **기본** 노드 -> **라이선스 정보** 에서, **오프라인에서 라이선스 활성화** > **활성화된 라이선스 가져오기** 를 선택한 후, 소프트웨어 라이선스 파일을 선택하여 가져오기를 수행합니다.
3. 열린 후에는 '해당 소프트웨어 라이선스 파일이 현재 사용 중인 것과 다름'을 허용합니다.
4. 이제 SLC를 등록할 준비가 되었습니다. 페이지 133의 소프트웨어 라이선스 코드 등록를 참조하십시오.

해당 소프트웨어 라이선스 파일은 가져오기 후 변경되었을 뿐 활성화되지는 않았습니다. 라이선스를 활성화하는 것을 잊지 마십시오. 자세한 정보는 페이지 111의 라이선스 활성화를 참조하십시오.

XProtect Essential+ 을(를) 구동하면, 관리 서버 트레이 아이콘에서만 라이선스를 변경할 수 있습니다. Management Client 에서는 라이선스를 변경할 수 없습니다.

라이선스 정보 창

라이선스 정보 창에서 이 사이트 및 다른 모든 사이트 모두에서 동일한 소프트웨어 라이선스 파일을 공유하는 모든 라이선스, Milestone Care 구독을 계속 추적할 수 있으며 라이선스 활성화 방법을 결정할 수 있습니다.

사이트 탐색 창에서 **라이선스 정보** 창 -> **기본** 노드 -> **라이선스 정보** 를 엽니다.

XProtect라이선싱시스템작동방식에대한전반적인내용을알고싶은경우페이지105의라이선스(설명됨)를참조하십시오.

라이선스 소유자

라이선스 정보 창의 이 영역에서 소프트웨어 등록 시 입력했던 라이선스 소유자의 연락처 상세 내용을 나열합니다.

다음에 대한 라이선스 영역이 보이지 않는 경우, 창 우측 하단 코너에 있는 **새로 고침** 버튼을 클릭하십시오.

세부 정보 편집 을 클릭하여 라이선스 소유자 정보를 편집합니다. **최종 사용자 사용권 계약** 을 클릭하여 설치 전 수락한 최종 사용자 사용권 계약을 조회합니다.

Milestone Care

현재 Milestone Care™ 구독에 관한 정보는 여기에서 확인할 수 있습니다. 구독 유효 기간은 아래 **설치된 제품** 표에 표시되어 있습니다.

Milestone Care 에 관한 자세한 정보는 링크를 사용하거나 페이지 109의 Milestone Care™ (설명됨)를 참조하십시오.

설치된 제품

다음은 XProtect VMS에 대한 설치된 모든 기본 라이선스 및 동일한 소프트웨어 라이선스 파일을 공유하는 XProtect 확장에 관한 정보입니다.

- 제품 및 버전
- 제품의 소프트웨어 라이선스 코드(SLC)
- SLC 유효 기간. 보통 무제한임
- Milestone Care Plus 구독의 만료일
- Milestone Care Premium 구독의 만료일

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

라이선스 개요 - 모든 사이트

소프트웨어 라이선스 파일 내 활성화된 장치 라이선스 및 기타 라이선스의 수와 시스템 상의 이용 가능한 라이선스의 총 수의 목록. 여기서, 추가 라이선스 구입 없이 아직 시스템을 확장할 수 있는지 여부를 쉽게 확인할 수 있습니다.

다른 사이트에서 활성화된 라이선스의 상태에 대한 상세 개요 정보를 보려면 **라이선스 세부 정보 - 모든 사이트** 링크를 클릭하십시오. 아래 **라이선스 상세 내용 - 현재 사이트** 섹션에서 표시되는 이용 가능한 정보에 대한 내용을 확인하십시오.

License Overview - All sites License Details - All Sites...

License Type	Activated
Device Licenses	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

XProtect 확장의 라이선스를 보유한 경우 **사이트 탐색** 창의 XProtect 확장 관련 노드에서 라이선스에 관한 추가 세부 정보를 확인할 수 있습니다.

라이선스 세부 정보 - 현재 사이트

활성화됨 줄은 이 사이트의 활성화된 장치 라이선스 또는 기타 라이선스의 목록을 표시합니다.

또한 **활성화 없이 변경** 줄에서 활성화 없이 변경한 사용한 장치의 수(페이지 108의 활성화 없이 장치 변경(설명됨) 참조) 및 연간 이용 가능한 장치의 수를 확인할 수 있습니다.

아직 활성화하지 않아 유예 기간으로 실행 중인 라이선스가 있는 경우, 이러한 라이선스는 **유예 기간 중** 열에 나열됩니다. 만료되는 첫 번째 라이선스의 만료일이 표 아래에 빨간색으로 표시됩니다.

잊어버리고 유예 기간이 만료되기 전에 라이선스를 활성화하지 않으면 시스템으로 비디오 전송이 중단됩니다. 이러한 라이선스는 **유예 기간 만료됨** 열에 표시됩니다. 자세한 정보는 페이지 113의 유예 기간 후 라이선스 활성화를 참조하십시오.

이용 가능한 수보다 많이 사용된 라이선스는 **라이선스 없음** 열에 나열되고 시스템에서 사용할 수 없습니다. 자세한 정보는 페이지 113의 추가 라이선스 구입를 참조하십시오.

유효 기간이 있는 라이선스를 보유한 경우. 유효 기간이 만료된 라이선스를 보유하고 있거나 라이선스가 없는 경우, 메시지를 통해 Management Client 에 로그인할 때마다 알려드립니다.

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

하나 이상의 라이선스를 이용하는 하드웨어 장치를 보유한 경우, **라이선스 상세 내용 - 현재 사이트** 표 아래 **전체 장치 라이선스 보고서를 열려면 여기를 클릭하세요** 라는 링크가 표시됩니다. 이 링크를 클릭하면 귀하가 보유한 장치 라이선스 수와 각 하드웨어 장치에 필요한 라이선스를 확인할 수 있습니다.

라이선스가 없는 하드웨어 장치는 Management Client 에 느낌표로 표시됩니다. 느낌표는 다른 용도로도 사용됩니다. 느낌표 위로 마우스를 가져가면 목적이 표시됩니다.

라이선스 활성화를 위한 기능

아래에 세 개의 테이블이 있습니다.

- 자동 라이선스 활성화를 사용하기 위한 확인란 및 자동 활성화를 위해 사용자 자격 증명을 편집하기 위한 링크. 자세한 정보는 페이지 107의 자동 라이선스 활성화(설명됨) 및 를 참조하십페이지 111의 자동 라이선스 활성화시오.
  자동 활성화에 실패한 경우, 실패를 알리는 메시지가 빨간색으로 표시됩니다. 자세한 정보는 **상세 정보** 링크를 클릭하십시오.
  XProtect Essential+ 와(과) 같은 일부 라이선스는 자동 라이선스 활성화가 켜진 상태에서 설치되며 이를 끌 수는 없습니다.
- 온라인 또는 오프라인에서 라이선스를 수동으로 활성화하기 위한 드롭다운 목록. 자세한 정보는 페이지 112의

온라인으로 라이선스 활성화 및 를 참조하십페이지 112의 오프라인으로 라이선스 활성화시오.

- 창의 우측 하단 구석에서 언제 자동 및 수동과 상관 없이 마지막으로 라이선스를 활성화 했는지 그리고 창의 정보가 언제 새로 고침되었는지를 확인할 수 있습니다. 타임스탬프는 로컬 컴퓨터가 아니라 서버 시간을 기준으로 합니다

요구사항 및 고려사항

일광 절약 시간(설명됨)

일광 절약 시간제(DST)는 낮 시간이 더 길어지고 아침이 빨라지도록 시계를 앞당겨 놓는 것을 말합니다. DST 사용은 국가/지역마다 다릅니다.

본질적으로 시간에 민감한 감시 시스템을 사용할 경우, 시스템이 DST를 처리하는 방식을 반드시 숙지하고 있어야 합니다.

DST 기간에 있는 경우 또는 DST 기간부터 녹화하는 경우 DST 설정을 변경하지 마십시오.

봄: 표준시간에서 DST로 전환

표준시간을 DST로 변경하면 시계를 1시간 앞당기면 되므로 그다지 문제가 되지 않습니다.

예:

시계가 02:00 표준시에서 03:00 DST로 앞당겨지고, 그 날은 하루가 23시간이 됩니다. 이 경우, 아침 02:00 및 03:00 사이는 이 날에 존재하지 않으므로 이 시간 동안의 데이터가 없습니다.

가을: DST에서 표준시간으로 전환

가을에 DST에서 표준시간으로 전환할 경우, 시계를 1시간 뒤로 이동합니다.

예:

시계가 02:00 DST에서 01:00 표준시로 느려져 해당 시간이 반복되므로 이 날은 하루가 25시간이 됩니다. 01:59:59에 도달하면, 즉시 01:00:00으로 돌려 놓으십시오. 시스템이 반응하지 않는다면 시간을 다시 기록해야 합니다. 01:30의 첫 번째 인스턴스를 01:30의 두 번째 인스턴스로 덮어쓰게 됩니다.

이러한 문제가 발생하지 않게 하기 위해 시스템 시간이 5분 이상 변경되는 경우 시스템이 현재 비디오를 보관합니다. 어떤 클라이언트에서도 01:00 시간의 첫 인스턴스를 직접적으로 볼 수 없지만 데이터가 기록되어 있으므로 안전합니다. 아카이브된 데이터베이스를 직접 열어 XProtect Smart Client 에서 이 비디오를 찾아볼 수 있습니다.

시간 서버(설명됨)

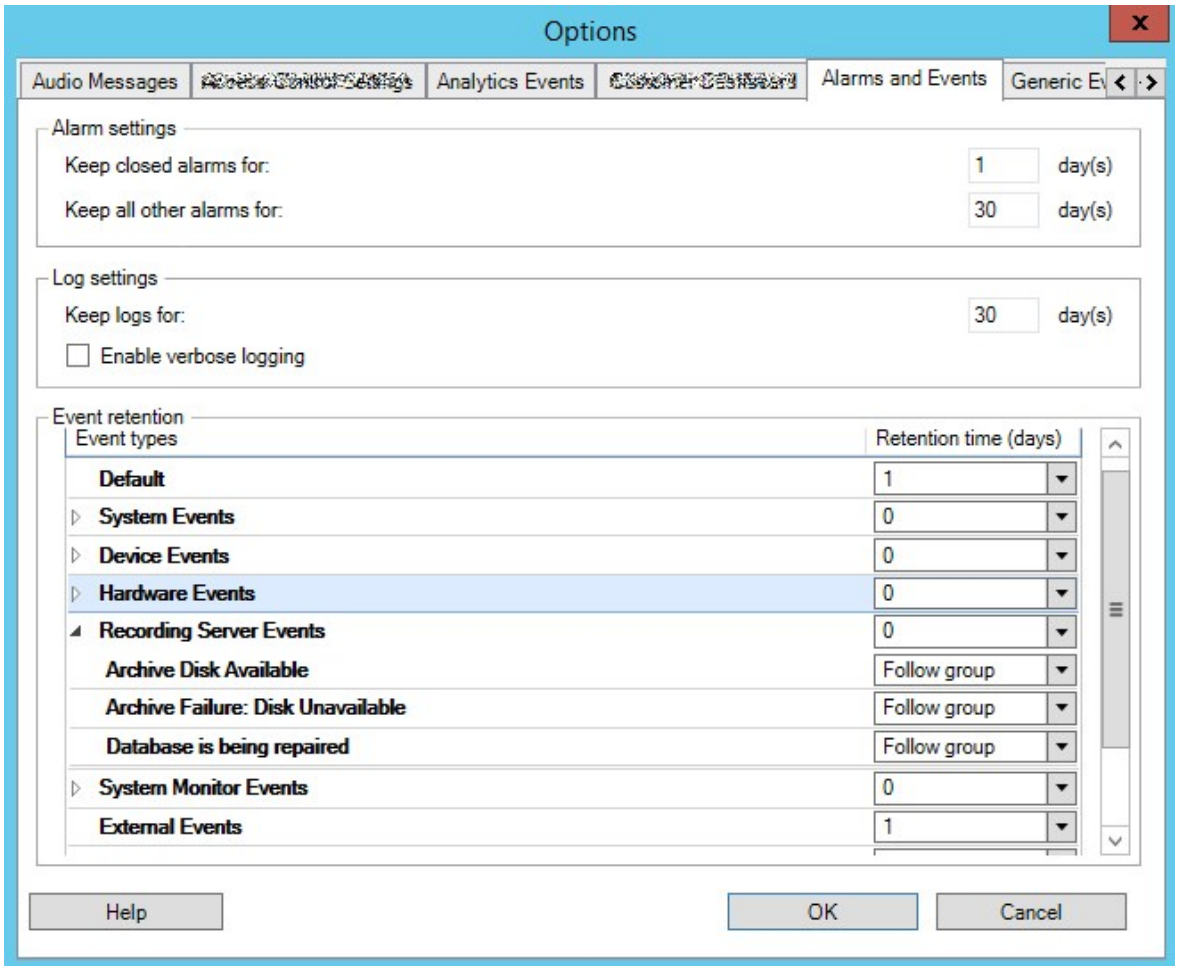
시스템에서 이미지를 수신하면 즉시 타임스탬프가 적용됩니다. 카메라는 개별 타이밍 장치를 포함할 수 있는 개별 장치이기 때문에 카메라 시간과 시스템 시간이 완벽하게 일치하지 않을 수 있습니다. 이 때문에 가끔 혼란이 초래될 수 있습니다. 사용하는 카메라가 타임스탬프를 지원하는 경우, Milestone 에서는 시간 서버를 통해 카메라와 시스템 시간을 자동으로 동기화하여 일관된 동기화를 유지할 것을 권장합니다.

시간 서버 구성 방법에 관한 자세한 정보는 Microsoft 웹사이트(https://www.microsoft.com/)에서 '**시간 서버**', '**시간 서비스**', 또는 유사한 용어를 검색하십시오.

데이터베이스 크기 제한

SQL Server데이터베이스(페이지 32의 SQL Server 설치 및 데이터베이스(설명됨) 참조)가 시스템 성능에 영향을 주는 크기로 커지는 것을 막기 위해 다른 유형의 이벤트와 알람이 데이터베이스에 며칠까지 저장할지를 지정할 수 있습니다.

1. **도구** 메뉴를 엽니다.
2. **옵션** > **알람 및 이벤트** 탭을 클릭합니다.



3. 필요한 설정을 변경합니다. 자세한 정보는 페이지 365의 알람 및 이벤트 탭(옵션)를 참조하십시오.

IPv6 및 IPv4(설명됨)

이 시스템은 IPv6과 IPv4를 지원합니다. XProtect Smart Client 도 마찬가지입니다.

IPv6은 인터넷 프로토콜(IP)의 최신 버전입니다. 인터넷 프로토콜은 IP 주소의 형식과 사용을 결정합니다. IPv6은 여전히 훨씬 광범위하게 사용되는 IP 버전인 IPv4와 공존합니다. IPv6은 IPv4의 주소 고갈을 해결하기 위해 개발되었습니다. IPv6 주소의 길이는 128비트인 반면, IPv4 주소는 32비트에 불과합니다.

인터넷의 주소록 크기가 43억 고유 주소에서 340언데실리온(340 x 10의 36제곱) 주소로 증가했다는 것을 의미합니다. 79옥틸리옹(1, 000의 9제곱)의 증가 비율에 해당합니다.

점점 더 많은 기업들이 회사 네트워크에서 IPv6을 구현하고 있습니다. 예를 들어, 모든 미국 연방기관 인프라의 경우에는 IPv6 규격을 준수해야 합니다. 이 설명서에 나온 예제와 삽화는 IPv4가 아직까지 가장 널리 사용되는 IP 버전이기 때문에 IPv4 용례를 반영하고 있습니다. IPv6도 마찬가지로 시스템에서 효과적으로 작동합니다.

IPv6를 가진 시스템 사용(설명됨)

IPv6을 갖춘 시스템을 사용할 경우 다음의 조건이 적용됩니다:

서버

서버는 종종 IPv4를 비롯한 IPv6을 사용할 수 있습니다. 그러나 시스템 내에 한 대의 서버(예: 관리 서버 또는 레코딩 서버)에 특정 IP 버전이 필요한 경우, 시스템에 있는 다른 모든 서버는 동일 IP 버전을 사용하여 통신해야 합니다.

예: 한 서버를 제외하고 시스템 내의 모든 서버가 IPv4와 IPv6을 사용할 수 있습니다. 예외는 IPv6만을 사용할 수 있는 서버가 해당됩니다. 즉, 모든 서버가 IPv6을 사용하여 서로 통신해야 함을 의미합니다.

장치

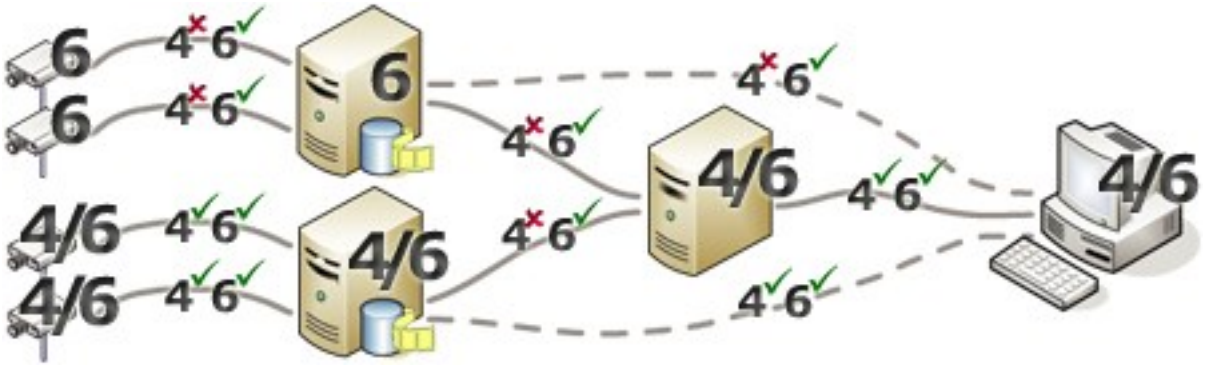
네트워크 장비와 레코딩 서버가 장치의 IP 버전을 지원하는 경우, 서버 통신에 사용된 것과 다른 IP 버전으로 장치(카메라, 입력, 출력, 마이크, 스피커)를 사용할 수 있습니다. 아래 삽화를 참조하십시오.

클라이언트

시스템이 IPv6를 사용하는 경우, 사용자가 XProtect Smart Client 에 연결해야 합니다. XProtect Smart Client 은(는) IPv6와 IPv4를 모두 지원합니다.

시스템 내 하나 이상의 서버가 IPv6 **만** 사용할 수 있는 경우, XProtect Smart Client 사용자는 **반드시** 해당 서버와 통신할 때 IPv6를 사용해야 합니다. 이와 관련해서, XProtect Smart Client 이(가) 초기 인증 시 기술적으로 관리 서버에 연결한 다음 레코딩 액세스를 위해 필요한 레코딩 서버에 연결해야 함을 유념해야 합니다.

그러나 네트워크 장비가 여러 IP 버전 간의 통신을 지원하고, 해당 컴퓨터에 IPv6 프로토콜을 설치한 경우에는 XProtect Smart Client 사용자가 직접 IPv6 네트워크상에 있을 필요가 없습니다. 삽화를 참조하십시오. 클라이언트 컴퓨터에 IPv6을 설치하려면 명령 프롬프트를 열고 ***Ipv6 install*** 을 입력한 다음 **ENTER** 키를 누릅니다.
사례 그림



예: 시스템 내의 한 서버가 IPv6만 사용할 수 있으므로 해당 서버와의 모든 통신이 IPv6를 사용해야 합니다. 그러나 또한 해당 서버가 시스템 내의 다른 모든 서버 간의 통신에 사용할 IP 버전을 결정하기도 합니다.

IPv6 주소 쓰기(설명됨)

IPv6 주소는 일반적으로 4자리 16진수 숫자의 8개 블록으로 작성되며, 각 블록은 콜론으로 구분됩니다.

예: *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

블록에서 선행하는 0을 삭제하여 주소를 줄일 수 있습니다. 또한 4자릿수 블록 중 일부는 0만으로 구성할 수 있습니다. 임의 수의 0000 블록이 연속되는 경우, 주소에서 이중 콜론이 하나뿐일 때에만 0000 블록을 콜론 2개로 대체하여 주소를 줄일 수 있습니다.

예:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB 다음과 같이 짧아 질 수 있습니다

2001:B80:0000:0000:0000:F80:3FA8:18AB 선행하는 0 제거

2001:0B80::0F80:3FA8:18AB - 0000 블록 제거

2001:B80::F80:3FA8:18AB - 선행하는 0과 0000 블록 모두 제거.

URL에 IPv6 주소 사용

IPv6 주소에는 콜론이 포함되어 있습니다. 그러나 콜론은 네트워크 주소 구문의 다른 유형에도 사용됩니다. 예를 들어, IPv4는 URL 에 IP 주소와 포트 번호가 모두 사용될 경우 둘을 구분할 때 콜론을 사용합니다. IPv6에도 이 원리가 상속됩니다. 따라서 혼동을 피하기 위해 URL에서 IPv6 주소를 사용하는 경우 IPv6 주소 주위에 꺾쇠 괄호를 추가합니다.

IPv6 주소를 가진 URL 의 **예**:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], 이는 물론 예를 들어 *http://[2001:B80::F80:3FA8:18AB]*로 축소 가능

IPv6 주소와 포트 번호를 가진 URL 의 **예**:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, 이는 물론 예를 들어 *http://[2001:B80::F80:3FA8:18AB]:1234*로 축소 가능

IPv6에 관한 자세한 정보는 예를 들어 IANA 웹사이트(https://www.iana.org/numbers/)를 참조하십시오. IANA(Internet Assigned Numbers Authority)는 전 세계 IP 주소 지정 조정을 담당하는 조직입니다.

가상 서버

VMware® 및 Microsoft® Hyper-V®와 같이 가상화된 Windows® 서버에서 모든 시스템 구성 요소를 실행할 수 있습니다.

하드웨어 리소스를 보다 효과적으로 활용하기 위해 가상화를 이용하는 경우가 종종 있습니다. 일반적으로 하드웨어 호스트 서버에서 실행되는 가상 서버는 가상 서버를 최대 한도로 로드하지 않으며, 동시에 그렇지 않은 경우도 종종 있습니다. 그러나 레코딩 서버는 모든 카메라와 비디오 스트림을 기록합니다. 이로 인해 CPU, 메모리, 네트워크 및 저장소 시스템에 많은 부하가 걸립니다. 따라서 가상 서버에서 실행할 때 가상화로 얻을 수 있는 표준 이득이 최대 범위까지 사라지므로 많은 경우 사용 가능한 모든 리소스를 사용합니다.

가상 환경에서 실행하는 경우, 하드웨어 호스트가 가상 서버에 할당된 것과 동일한 양의 물리적 메모리를 갖고 레코딩 서버를 실행하는 가상 서버에 충분한 CPU와 메모리가 할당되어야 합니다(기본적으로 그렇지 않음). 일반적으로 레코딩 서버에는 구성에 따라 2-4 GB가 필요합니다. 또 다른 병목 현상은 네트워크 어댑터 할당과 하드 디스크 성능입니다. 레코딩 서버를 실행하는 가상 서버의 호스트 서버에 물리적 네트워크 어댑터 할당을 고려하십시오. 이렇게 하면 보다 쉽게 다른 가상 서버에 비해 네트워크 어댑터에 트래픽 과부하가 걸리지 않게 할 수 있습니다. 네트워크 어댑터가 여러 가상 서버에 사용된 경우, 네트워크 트래픽으로 인해 레코딩 서버가 구성된 수의 이미지를 검색하거나 레코딩하지 못할 수 있습니다.

다중 관리 서버 정보(클러스터링)(설명됨)

관리 서버는 서버 클러스터 내에서 여러 서버에 설치할 수 있습니다. 이는 시스템의 가동 중단이 거의 발생하지 않도록 해줍니다. 클러스터의 서버가 실패하면 클러스터 내의 다른 서버가 관리 서버를 실행 중인 실패한 서버의 작업을 자동으로 인수합니다.

하나의 감시 설정에는 하나의 활성 관리 서버만 있을 수 있지만, 실패할 경우를 대비하여 작업을 인수하도록 다른 관리 서버를 설정할 수 있습니다.

> 기본으로 Management Server 서비스는 장애 조치가 6시간 이내에 2회 발생하도록 발생 횟수를 제한합니다. 이를 초과하면, Management Server 서비스가 클러스터링 서비스에 의해 자동으로 시작되지 않습니다. 필요에 따라 이러한 제한을 변경할 수 있습니다.

클러스터링 요구 사항

- Microsoft Windows Server 2016 이상이 설치된 두 대의 기기. 다음 사항을 반드시 충족해야 합니다:
  - 클러스터 노드로 추가하고자 하는 모든 서버는 동일한 버전의 Windows Server에서 구동되어야 합니다
  - 클러스터 노드로 추가하고자 하는 모든 서버는 동일 도메인에 추가되어야 합니다
  - 로컬 관리자로서 Windows 계정에 로그인 액세스 권한을 지니고 있어야 합니다

  Microsoft Windows 서버 내 클러스터에 대해서는 장애 조치 클러스터 https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster를 참조하십시오.

- Microsoft SQL Server 설치

  서버 클러스터 **외부**에 설치된 외부 SQL Server 및 데이터베이스 **또는** 서버 클러스터 내 **내부** SQL Server 서비스(클러스터됨) 중 **하나**(내부 SQL Server 서비스를 생성하려면 클러스터된 SQL Server(으)로 작동할 수 있는 Microsoft® SQL Server® Standard 또는 Microsoft® SQL Server® Enterprise 에디션을 사용해야 함)

  > 관리 서버를 데이터베이스에 연결할 때에는 시스템 구성 암호 설정 여부에 따라 현재 시스템 구성 암호를 제공하도록 요청받을 수도 있습니다. 페이지 306의 시스템 구성 암호(설명됨)를 참조하십시오.

> 장애 조치 클러스터 환경에서 작업하는 경우, Server Configurator 에서 작업을 시작하기 전에 클러스터를 정지하는 것을 권장합니다. Server Configurator 이(가) 변경을 적용하는 동안 서비스를 멈추고 장애 조치 클러스터 환경이 이 작업을 중단시킬 수 있기 때문입니다.

레코딩 데이터베이스의 손상 보호

카메라 데이터베이스가 손상될 수 있습니다. 이러한 문제를 해결하기 위해 여러 데이터베이스 복구 옵션이 존재합니다. 하지만, Milestone 에서는 카메라 데이터베이스가 손상되지 않도록 조치를 취할 것을 권장합니다.

하드 디스크 장애: 드라이브 보호

하드 디스크 드라이브는 기계적 장치로, 외부 요인에 취약합니다. 다음은 하드 디스크 드라이브를 손상시키고 카메라 데이터베이스의 손상을 초래할 수 있는 외부적 요인의 예에 해당합니다.

- 진동(감시 시스템 서버와 주변 요소들이 안정적인지 확인할 것)
- 강한 열(서버에 충분한 환기가 이루어지는지 확인할 것)
- 강한 자기장(피할 것)
- 정전(무중단 전원 공급장치(UPS)를 사용할 것)
- 정전기(하드 디스크 드라이브를 취급하는 경우 사용자 본인의 몸을 접지할 것)
- 화재, 물 등. (회피)

Windows 작업 관리자: 프로세스를 종료할 때 주의하십시오

Windows 작업 관리자에서 작업 중일 경우, 감시 시스템에 영향을 주는 어떤 프로세스도 종료하지 않도록 주의하십시오. Windows 작업 관리자에서 **프로세스 종료** 를 클릭해서 응용 프로그램 또는 시스템 서비스를 종료한 경우, 해당 프로세스가 종료되기 전에 상태나 데이터를 저장할 기회가 사라집니다. 이는 카메라 데이터베이스 손상으로 이어질 수 있습니다.

일반적으로 프로세스 종료를 시도할 경우 Windows 작업 관리자에 경고가 표시됩니다. 해당 프로세스를 종료해도 감시 시스템에 영향을 주지 않음을 절대적으로 확신하지 않는 한, 프로세스 종료를 묻는 경고 메시지가 나타날 때 **아니오** 를 클릭하십시오.

정전: UPS 사용

데이터 손상의 한 가지 가장 흔한 이유는 파일이 저되거나 운영 체제가 올바로 종료되지 않은 상태로 레코딩 서버가 갑자기 종료되기 때문입니다. 이는 정전이나 누군가가 서버의 전원 케이블 등을 실수로 뽑았기 때문에 발생할 수 있습니다.

레코딩 서버가 갑자기 종료되지 않도록 보호하기 위한 가장 좋은 방법은 각 레코딩 서버에 UPS(무중단 전원 공급장치)를 탑재하는 것입니다.

UPS는 배터리 구동식 보조 전원 소스로 작동하여 전원 문제 발생 시 열려 있는 파일을 저장하고 시스템의 전원을 안전하게 끄는 데 필요한 전원을 공급합니다. UPS는 세부적 구성이 다르지만, 대부분의 UPS에는 열려 있는 파일을 자동으로 저장하고 시스템 관리자에게 경고를 보내는 등의 기능을 수행하는 소프트웨어가 포함되어 있습니다.

조직의 환경에 정확한 유형의 UPS를 선택하는 것은 개별적인 절차입니다. 하지만 필요 사항을 평가할 때 정전 발생 시 UPS가 공급할 수 있는 가동 시간의 크기를 고려해야 합니다. 열려 있는 파일 저장과 올바른 운영 체제 종료 작업은 몇 분 정도 걸릴 수 있습니다.

SQL Server 데이터베이스 트랜잭션 로그(설명됨)

변경 사항이 SQL Server 데이터베이스에 기록될 때마다 해당 SQL Server 데이터베이스는 이 변경 사항을 트랜잭션 로그에 기록합니다.

트랜잭션 로그를 사용하면 Microsoft® SQL Server Management Studio 을(를) 통해 SQL Server 데이터베이스를 이전 상태로 돌리거나 변경 사항을 취소할 수 있습니다. 기본적으로 SQL Server 데이터베이스는 트랜잭션 로그를 무한정 저장하며, 시간이 지날수록 트랜잭션 로그에 점점 더 많은 항목이 쌓이게 됩니다. 트랜잭션 로그는 기본적으로 시스템 드라이브에 위치하며, 트랜잭션 로그가 계속해서 증가하면 Windows가 제대로 실행되지 못하게 만들 수도 있습니다.

이러한 상황을 피하기 위해 정기적으로 트랜잭션 로그를 플러시하는 것이 좋습니다. 플러시 자체로는 트랜잭션 로그 파일을 작게 만들 수 없지만 로그 파일의 콘텐츠를 정리하여 제어 불가능한 상황을 막을 수는 있습니다. 사용 중인 VMS 시스템은 트랜잭션 로그를 플러시하지 않습니다. SQL Server 에서 트랜잭션 로그를 플러싱할 수 있습니다. Microsoft 지원 페이지 https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 을(를) 방문하여 *트랜잭션 로그 잘림* 을 검색하십시오.

최소 시스템 요구사항

여러 VMS 응용 프로그램 및 시스템 구성 요소의 시스템 요구 사항에 대한 자세한 내용을 보려면 Milestone 웹사이트 (https://www.milestonesys.com/systemrequirements/)를 방문하십시오.

설치를 시작하기 전에

Milestone 에서는 실제 설치를 시작하기 전에 다음 섹션에 기술된 요구 사항을 살펴 보도록 권장합니다.

서버와 네트워크 준비

운영 체제

모든서버에서MicrosoftWindows운영체제를새로설치했고모든최신Windows업데이트로업데이트되었는지확인합니다.

여러 VMS 응용 프로그램 및 시스템 구성 요소의 시스템 요구 사항에 대한 자세한 내용을 보려면 Milestone 웹사이트(https://www.milestonesys.com/systemrequirements/)를 방문하십시오.

Microsoft® .NET Framework

모든 서버에 Microsoft .NET Framework 4.8 또는 그 이상 버전이 설치되어 있는지 확인하십시오.

네트워크

고정 IP 주소를 할당하거나 모든 시스템 구성 요소 및 카메라에 DHCP를 예약합니다. 네트워크에서 충분한 대역폭이 확보되도록 하기 위해 시스템이 대역폭을 사용하는 방식과 시기에 대해 알고 있어야 합니다. 네트워크에서 처리 부하를 일으키는 요소에는 크게 세 가지가 있습니다.

- 카메라 비디오 스트림
- 비디오를 표시하는 클라이언트
- 녹화된 비디오 보관

레코딩 서버는 카메라로부터 비디오 스트림을 가져오므로 네트워크에 지속적인 부하를 일으킵니다. 비디오를 표시하는 클라이언트가 네트워크 대역폭을 사용합니다. 클라이언트 뷰 내용에 변화가 없으면 부하가 일정합니다. 뷰 내용의 변화, 비디오 검색 또는 재생 시에는 부하가 동적으로 바뀝니다.

녹화된 비디오의 아카이브는 옵션인 기능이며, 컴퓨터의 내부 저장소 시스템에 충분한 공간이 없을 경우 시스템은 레코딩을 네트워크 저장소로 이동할 수 있습니다. 보관은 사용자가 정의하는 예약 작업입니다. 네트워크 드라이브에 보관하는 것이 일반적이기 때문에 예약된 시간에 네트워크에서 동적인 부하가 발생하게 됩니다.

이러한 트래픽 증가를 처리하기에 충분한 네트워크 대역폭 여유가 있어야 합니다. 그래야 시스템의 응답 속도와 전반적인 사용 환경이 개선됩니다.

Active Directory 준비

Active Directory 서비스를 통해 시스템에 사용자를 추가하려는 경우, Active Directory가 설치되고 도메인 컨트롤러 역할을 하는 서버를 네트워크에서 사용할 수 있어야 합니다.

간편한 사용자 및 그룹 관리를 위해, Milestone 에서는 XProtect 시스템을 설치하기 전에 Microsoft Active Directory® 를 설치하고 구성하도록 권장합니다. 시스템 설치 후 관리 서버를 Active Directory에 추가할 경우, 관리 서버를 다시 설치하고 사용자를 Active Directory에 정의된 신규 Windows 사용자로 대체해야 합니다.

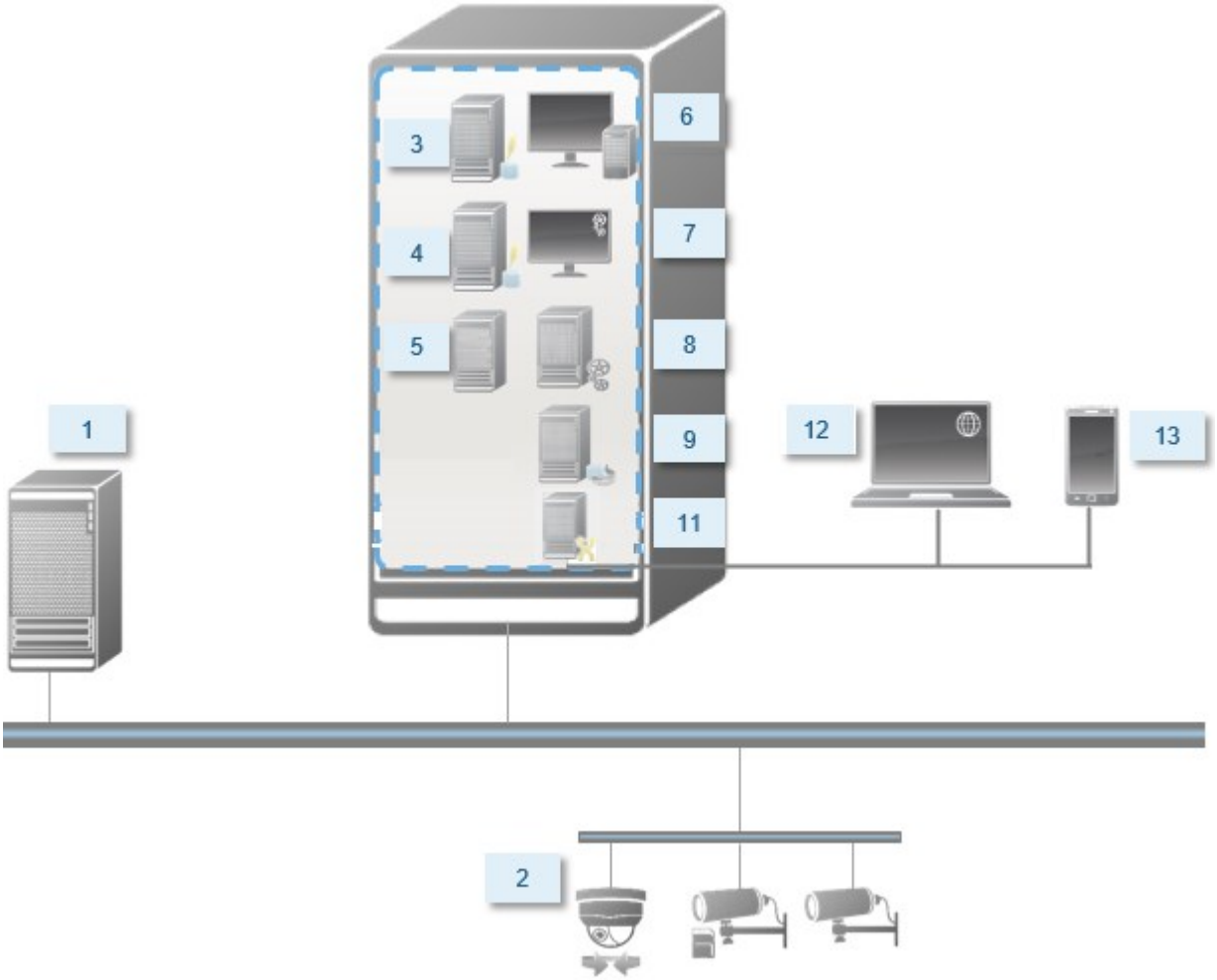
기본 사용자는 Milestone Federated Architecture 시스템에서 지원되지 않으므로, Milestone Federated Architecture 을(를) 사용하려면, 사용자를 Active Directory 서비스를 통해 Windows 사용자로 추가해야 합니다. Active Directory를 설치하지 않은 경우 설치 시 페이지 163의 작업 그룹에 대한 설치 의 단계를 따르십시오.

설치 방법

설치 마법사의 일부로, 사용할 설치 방법을 결정해야 합니다. 조직의 필요성에 기초하여 선택을 해야겠지만 시스템 구입 당시 이미 방법을 결정했을 것으로 생각합니다.

옵션	설명
단일 컴퓨터	현재 컴퓨터에 SQL Server뿐만 아니라 모든 서버 및 클라이언트 구성 요소를 설치합니다. 설치가 완료되면 마법사를 통해 시스템을 구성할 수 있게 될 수도 있습니다. 계속하기로 동의하면 레코딩 서버가 하드웨어를 위한 네트워크를 스캔하며 어떤 하드웨어 장치를 시스템에 추가할 지 선택할 수 있게 됩니다. 구성 마법사에서 추가할 수 있는 하드웨어 장치의 최대 수는 기본 라이선스에 따라 다릅니다. 또한 뷰에서 카메라가 사전 구성되며 기본 운영자 역할이 생성됩니다. 설치 후 XProtect Smart Client 이(가) 열리고 시스템을 사용할 준비가 됩니다.
사용자 정의	관리 서버는 시스템 구성 요소 목록에서 항상 선택되고 항상 설치되지만, 다른 서버 및 클라이언트 구성 요소 가운데 현재 컴퓨터 상에 설치할 내용을 자유롭게 선택할 수 있습니다. 기본적으로 레코딩 서버는 구성 요소 목록에서 선택되어 있지 않지만 이를 변경할 수 있습니다. 이후에 다른 컴퓨터에 선택되지 않은 구성 요소를 설치할 수 있습니다.

단일 컴퓨터 설치

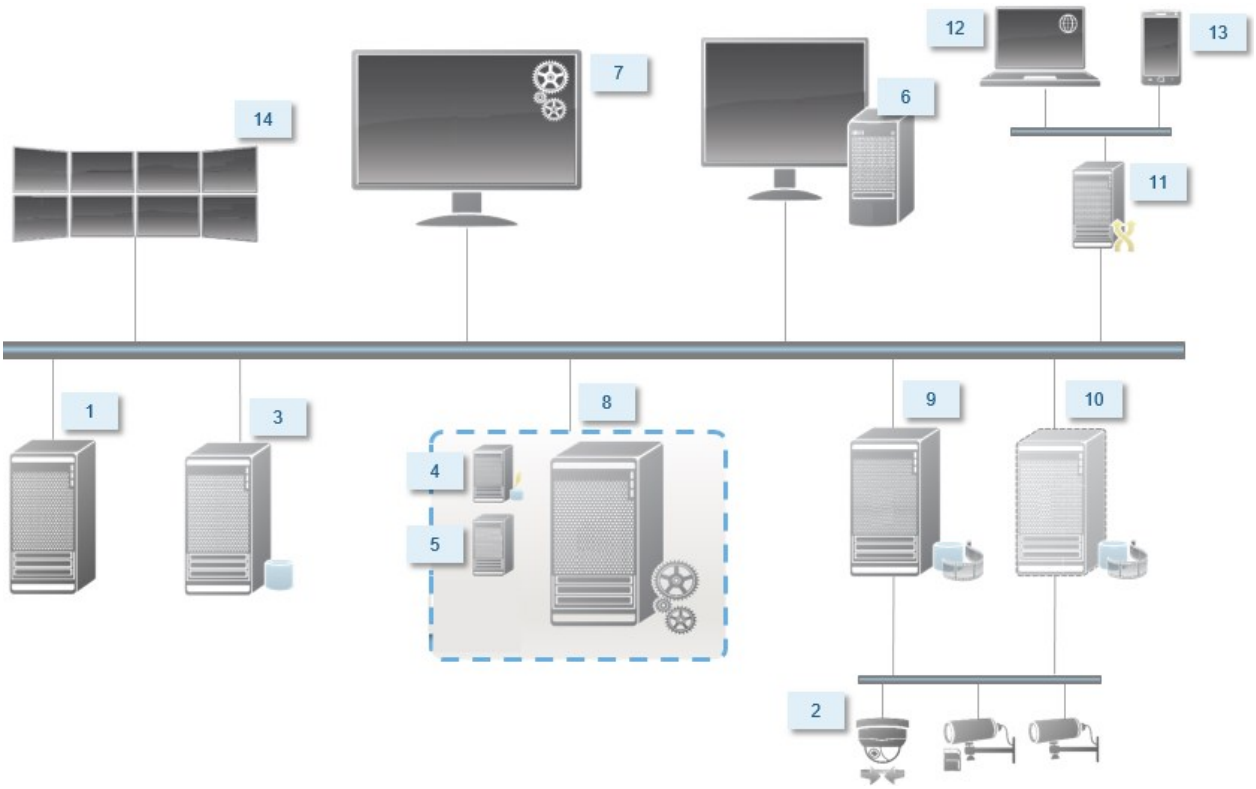


시스템의 일반적 시스템 구성 요소:

1. **Active Directory**
2. **장치**
3. **다음이 포함된 서버: SQL Server**
4. **이벤트 서버**
5. **로그 서버**
6. **XProtect Smart Client**
7. **Management Client**
8. **관리 서버**
9. **레코딩 서버**

10. **장애 조치 레코딩 서버**
11. **XProtect Mobile 서버**
12. **XProtect Web Client**
13. **XProtect Mobile 클라이언트**
14. **XProtect Smart Client 와 함께 XProtect Smart Wall**

사용자 정의 설치 - 분산 시스템 구성 요소의 예시



SQL Server 에디션에서 결정

Microsoft® SQL Server® Express 은(는) SQL Server 의 무료 에디션이며 다른 SQL Server 에디션과 달리 설치 및 사용 준비하기에 편리합니다. SQL Server이(가) 컴퓨터에 설치되어 있지 않은 경우 **단일 컴퓨터** 설치 중에 Microsoft SQL Server Express이(가) 설치됩니다.

XProtect VMS 설치에는 Microsoft SQL Server Express 2019년도 버전이 포함되어 있습니다. 모든 Windows 운영 체제가 이 버전의 SQL Server 을(를) 지원하는 것은 아닙니다. XProtect VMS 을(를) 설치하기 전, 사용 중인 운영 체제가 SQL Server 2019를 지원하는지 확인하십시오. 사용 중인 운영 체제가 이 버전의 SQL Server 을(를) 지원하지 않는 경우, SQL Server 설치를 시작하기 전에 시스템이 지원하는 XProtect VMS 을(를) 설치하십시오. 지원되는 SQL Server 버전에 관한 정보는, https://www.milestonesys.com/systemrequirements/ 을(를) 참조하십시오.

매우 큰 시스템 또는 SQL Server 데이터베이스에서 발생하는 트랜잭션이 많은 시스템의 경우, Milestone에서는 네트워크의 전용 컴퓨터 및 다른 목적으로 사용되지 않는 전용 하드 디스크 드라이브에 설치된 Microsoft® SQL Server® Standard 또는 SQL Server의 Microsoft® SQL Server® Enterprise 에디션을 사용할 것을 권장합니다. 자체 드라이브에 SQL Server을(를) 설치하면 전반적인 시스템 성능이 개선됩니다.

서비스 계정 선택

설치의 일부로 이 컴퓨터에서 Milestone 서비스를 실행하기 위한 계정을 지정하라는 요청을 받게 됩니다. 어떤 사용자가 로그인 되어 있든 이 서비스는 항상 이 계정에서 실행됩니다. 예를 들어, 작업을 수행할 적절한 권한, 적합한 네트워크 및 파일 액세스 권한 및 네트워크 공유 폴더에 액세스할 권한 등 모든 필요한 사용자 권한이 있어야 합니다.

사전 정의된 계정 또는 사용자 계정 중 하나를 선택할 수 있습니다. 시스템을 설치하려는 환경에 맞게 선택해야 합니다:

도메인 환경

도메인 환경의 경우:

- Milestone 은(는) 내장된 네트워크 서비스 계정의 사용을 권장합니다.

  시스템을 여러 컴퓨터로 확장해야 하는 경우에도 사용이 간편합니다.

- 도메인 사용자 계정도 사용할 수 있지만, 잠재적으로 구성하기가 좀 더 어려울 수 있습니다

작업 그룹 환경

작업 그룹 환경의 경우 Milestone 은 필요한 모든 권한을 가진 로컬 사용자 계정의 사용을 권장합니다. 관리자 계정인 경우가 많습니다.

> ⚠ 시스템 구성 요소를 다수의 컴퓨터에 설치하는 경우, 선택한 사용자 계정이 동일한 사용자 이름, 암호 및 액세스 권한이 설치된 모든 컴퓨터에 구성되어야 합니다.

Kerberos 인증(설명됨)

Kerberos는 티켓 기반 네트워크 인증 프로토콜입니다. 클라이언트/서버 또는 서버/서버 응용 프로그램에 대한 강력한 인증을 제공하도록 설계되었습니다.

이전의 Microsoft NT LAN(NTLM) 인증 프로토콜을 대체하는 수단으로 Kerberos 인증을 사용하십시오.

Kerberos 인증은 클라이언트가 서비스에 인증하고 서비스가 클라이언트에 인증하는 상호 인증이 필요합니다. 이렇게 하면 암호를 노출하지 않고 XProtect 클라이언트에서 XProtect 서버로 보다 안전하게 인증을 수행할 수 있습니다.

XProtect VMS 에서 상호 인증을 가능하게 하려면, Active Directory에서 서비스 사용자 이름(SPN)을 등록해야 합니다. SPN은 XProtect 서버 서비스 같은 엔터티를 고유하게 식별하는 별칭입니다. 클라이언트가 네트워크에서 서비스를 식별할 수 있게 하려면 상호 인증을 사용하는 모든 서비스에 SPN을 등록시켜야 합니다. SPN을 올바르게 등록하지 않으면 상호 인증이 불가능합니다.

아래 표에는 여러 가지 Milestone 서비스와 등록해야 하는 해당 포트 번호가 나와 있습니다.

서비스	포트 번호
Management Server - IIS	80 - 구성 가능
Management Server - 내부	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

Active Directory에 등록해야 하는 서비스의 수는 현재 설치에 따라 결정됩니다. Data Collector는 Management Server, Recording Server, Event Server 또는 Failover Server 서비스를 설치할 때 자동으로 설치됩니다.

서비스를 실행하는 사용자에 대해 두 개의 SPN을 등록해야 합니다. 하나는 호스트 이름을 가지며 다른 하나는 정규화된 도메인 이름을 가집니다.

네트워크 사용자 서비스 계정 하에서 서비스를 실행 중인 경우, 이 서비스를 실행하는 각 컴퓨터에 대해 두 개의 SPN을 등록해야 합니다.

이것은 Milestone SPN 명명 체계입니다.

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

다음은 다음과 같은 세부 정보를 가진 컴퓨터에서 실행되는 Recording Server 서비스에 대한 SPN의 예입니다.

```
Hostname: Record-Server1
Domain: Surveillance.com
```

등록할 SPN:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

바이러스 검사 제외(설명됨)

다른 데이터베이스 소프트웨어의 경우와 마찬가지로 XProtect 소프트웨어를 실행하는 컴퓨터에 안티바이러스 프로그램이 설치된 경우, 특정 파일 형식과 폴더 뿐 아니라 특정 네트워크 트래픽을 제외시키는 것이 중요합니다. 이러한 예외를 지정해두지 않으면 바이러스 검사에 상당한 시스템 리소스가 사용됩니다. 뿐만 아니라 검사 프로세스에서 파일이 일시적으로 잠겨 녹화 프로세스가 중단되거나, 심지어 데이터베이스가 손상되는 일까지 생길 수 있습니다.

바이러스 검사를 수행해야 하는 경우, 레코딩 데이터베이스를 포함한 레코딩 서버 폴더(기본적으로 `C:\mediadatabase\` 및 그 하위에 있는 모든 폴더)는 검사하지 마십시오. 또한, 아카이브 저장소 디렉토리에서도 바이러스 검사를 수행하지 마십시오.

추가적으로 다음 예외도 지정하십시오.

- 파일 형식: .blk, .idx, .pic
- 폴더 및 하위 폴더:
  - `C:\Program Files\Milestone` 또는 `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\Milestone\MIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Event Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Log Server`
  - `C:\ProgramData\Milestone\XProtect Management Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`

- 다음 TCP 포트에서 네트워크 검사 제외:

제품	TCP 포트
XProtect VMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

또는

- 다음 프로세스의 네트워크 검사 제외:

제품	프로세스
XProtect VMS	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

조직에서 바이러스 검사와 관련하여 엄격한 가이드라인을 마련해놓고 있을 수 있지만 상기 폴더와 파일을 바이러스 검사에서 제외시키는 것이 중요합니다.

XProtect VMS 을(를) FIPS 140-2 규격 모드에서 실행되도록 하려면 어떻게 해야 합니까?

FIPS 140-2 모드 작업에서 XProtect VMS 을(를) 실행하려면 반드시 다음과 같이 해야 합니다.

- Windows 운영 체제를 FIPS 140-2 승인 모드 작업에서 실행해야 합니다. FIPS 활성화에 관한 정보는 Microsoft 사이트 를 참조하십시오.
- 독립형 타사 통합이 FIPS가 활성화된 Windows 운영 체제에서 실행되도록 해야 합니다.
- FIPS 140-2 규격 모드 운영을 보장하는 방식으로 장치를 연결해야 합니다.
- 미디어 데이터베이스의 데이터가 FIPS 140-2 규격 암호로 암호화되도록 해야 합니다.

  이 작업은 미디어 데이터베이스 업그레이드 도구를 실행하면 이뤄집니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

FIPS가 활성화된 시스템에서 XProtect VMS 을(를) 설치하기 전

FIPS가 활성화된 컴퓨터에서 신규 XProtect VMS 설치가 이뤄질 수 있는 반면, Windows 운영 체제에 FIPS가 활성화되어 있는 경우 XProtect VMS 을(를) 업그레이드할 수 없습니다.

업그레이드하는 경우, 설치하기 전에 SQL Server을(를) 호스팅하는 컴퓨터를 비롯하여 비디오 관리 소프트웨어의 일부인 모든 컴퓨터의 Windows FIPS 보안 정책을 비활성화하십시오.

XProtect VMS 설치 프로그램은 FIPS 보안 정책을 확인하며 FIPS가 활성화되어 있는 경우 시작부터 설치를 방지합니다.

그러나 2020 R3 이후 버전인 XProtect VMS 에서 업그레이드하는 경우, FIPS를 비활성화할 필요가 없습니다.

모든 컴퓨터에서 XProtect VMS 구성 요소를 설치하고 FIPS에 대해 시스템을 준비한 후, VMS 내 모든 컴퓨터상의 Windows에서 FIPS 보안 정책을 활성화할 수 있습니다.

XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

소프트웨어 라이선스 코드 등록

설치 전, Milestone (으)로부터 받은 소프트웨어 라이선스 파일의 이름과 위치를 알고 있어야 합니다.

XProtect Essential+ 의 무료 버전을 설치할 수 있습니다. 이 버전은 한정된 수의 카메라에 XProtect VMS 의 제한된 기능을 제공합니다. XProtect Essential+ 을(를) 설치하려면 인터넷에 연결해야 합니다.

소프트웨어 라이센스 코드(SLC)는 주문 확인서에 인쇄되어 있으며 SCL이 소프트웨어 라이센스 파일의 이름으로 이용됩니다.

Milestone 은(는) 설치 전 당사 웹사이트(https://online.milestonesys.com/)에서 귀하의 SLC를 등록할 것을 권장합니다. 리셀러가 대신 할 수 있습니다.

장치 드라이버(설명됨)

이 시스템은 비디오 장치 드라이버를 사용하여 레코딩 서버에 연결된 카메라 장치와 통신하고 해당 장치를 제어합니다. 시스템에서 각 레코딩 서버에 장치 드라이버를 설치해야 합니다.

2018 R1 릴리스부터 장치 드라이버는 최신 드라이버가 포함된 정기 Device Pack(장치 팩)과 기존 드라이버가 포함된 레거시 Device Pack(장치 팩)으로 나누어 집니다.

정기 Device Pack(장치 팩)은 레코딩 서버를 설치할 때 자동으로 설치됩니다. 나중에 새 버전의 장치 드라이버를 다운로드 및 설치하여 드라이버를 업데이트할 수 있습니다. Milestone에서는 정기적으로 새 버전의 장치 드라이버를 릴리스하며 당사 웹 사이트의 다운로드 페이지(https://www.milestonesys.com/downloads/)에서 Device Pack(장치 팩)으로 제공합니다. Device Pack(장치 팩)을 업데이트하면 이미 설치한 버전 위에 최신 버전을 설치할 수 있습니다.

레거시 Device Pack(장치 팩)은 시스템에 정기 Device Pack(장치 팩)이 설치된 경우에만 설치할 수 있습니다. 이전 버전이 이미 시스템에 설치된 경우 레거시 Device Pack(장치 팩)의 드라이버는 자동으로 설치됩니다. 소프트웨어 다운로드 페이지(https://www.milestonesys.com/downloads/)에서 수동으로 다운로드 및 설치할 수 있습니다.

설치하기 전에 Recording Server 서비스를 중지하거나 컴퓨터를 재시작해야 합니다.

최상의 성능을 얻으려면 항상 최신 버전의 장치 드라이버를 사용하십시오.

오프라인 설치를 위한 요구 사항

오프라인 상태인 서버에 시스템을 설치하는 경우 다음 사항이 필요합니다.

- `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 파일
- XProtect 시스템에 관한 소프트웨어 라이선스 파일(SLC)
- 필수 .NET 버전(https://www.milestonesys.com/systemrequirements/)을 포함한 OS 설치 미디어

보안 통신(설명됨)

하이퍼텍스트 전송 프로토콜 보안(Hypertext Transfer Protocol Secure, HTTPS)은 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol, HTTP)의 연장으로 컴퓨터 네트워크 상의 보안 통신을 위한 것입니다. HTTPS에서 통신 프로토콜은 전송 레이어 보안(Transport Layer Security, TLS), 또는 그보다 먼저 나온 보안 소켓 레이어(Secure Sockets Layer, SSL)를 사용하여 암호화됩니다.

XProtect VMS 에서 비대칭 암호화(RSA)와 함께 TLS/SSL 프로토콜을 사용하여 보안 통신을 확보합니다.

TLS/SSL 프로토콜은 한 쌍의 키(하나는 개인 키, 하나는 공용 키)를 사용하여 보안 연결을 인증, 보호 및 관리합니다.

인증 권한(CA)은 루트 인증서를 발급할 수 있는 자입니다. 이는 루트 인증서를 발급할 수 있는 인터넷 서비스이거나 인증서를 수동으로 생성하고 배포하는 자일 수 있습니다. CA는 웹 서비스, 즉 https 통신을 사용하는 모든 소프트웨어에 대해 인증서를 발급할 수 있습니다. 이 인증서는 개인용 키 및 공공 키 2개를 포함합니다. 공개 키는 공개 인증서를 설치함으로써 웹 서비스의 클라이언트(서비스 클라이언트)에 설치됩니다. 개인 키는 서버에 설치되어있는 서명된 서버 인증서에 사용됩니다. 서비스 클라이언트가 웹 서비스를 호출할 때마다, 웹서비스는 공공 키를 포함한 서버 인증을 클라이언트에 전송합니다. 이미 설치된 공개 CA 인증서를 사용하여 서비스 클라이언트는 서버 인증서를 확인할 수 있습니다. 클라이언트와 서버는 이제 공개 및 개인 서버 인증서를 사용하여 비밀 키 교환 및 서버에서 보안 TLS/SSL 연결을 수립할 수 있습니다.

수동으로 배포된 인증서인 경우, 인증서는 클라이언트에서 확인하기 전에 설치되어야 합니다.

TLS에 대한 자세한 내용은 전송 계층 보안을 참조하십시오.

> ⚠ 인증서는 만료 날짜가 있습니다. XProtect VMS 에서는 인증서가 만료될 때를 경고하지 않습니다. 인증서의 기한이 만료된 경우:
> 클라이언트는 더 이상 기한이 만료된 인증서가 있는 레코딩 서버를 신뢰하지 않으므로 레코딩 서버와 통신할 수 없습니다.
> • 레코딩 서버는 더 이상 기한이 만료된 인증서가 있는 관리 서버를 신뢰하지 않으므로 관리 서버와 통신할 수 없습니다.
> • 모바일 장치는 더 이상 기한이 만료된 인증서가 있는 모바일 서버를 신뢰하지 않으므로 모바일 서버와 통신할 수 없습니다.
>
> 인증서를 갱신하려면 인증서를 생성했을 때처럼 본 지침상의 단계를 따르십시오.

자세한 정보는 XProtect VMS 설치 보호 방법에 관한 인증 안내서 를 참조합니다.

설치

신규 XProtect 시스템 설치

XProtect Essential+ 설치

XProtect Essential+ 의 무료 버전을 설치할 수 있습니다. 이 버전은 한정된 수의 카메라에 XProtect VMS 의 제한된 기능을 제공합니다. XProtect Essential+ 을(를) 설치하려면 인터넷에 연결해야 합니다.

이 버전은 **단일 컴퓨터** 설치 옵션을 이용해 한 대의 컴퓨터에 설치됩니다. **단일 컴퓨터** 옵션은 현재 컴퓨터에 모든 서버 및 클라이언트 구성 요소를 설치합니다.

> Milestone 설치 전에 다음 섹션을 자세히 읽어보실 것을 권장합니다. 페이지 124의 설치를 시작하기 전에 .

> FIPS 설치의 경우, Windows 운영 체제에서 FIPS가 활성화되어 있으면 XProtect VMS 을(를) 업그레이드할 수 없습니다. 설치하기 전, SQL Server을(를) 호스팅하는 컴퓨터를 비롯하여 비디오 관리 소프트웨어의 일부인 모든 컴퓨터에서 Windows FIPS 보안 정책을 비활성화하십시오. 그러나 2020 R3 이후 버전인 XProtect VMS 에서 업그레이드하는 경우, FIPS를 비활성화할 필요가 없습니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

최초 설치 후, 구성 마법사를 계속할 수 있습니다. 하드웨어 및 구성에 따라, 레코딩 서버는 네트워크에서 하드웨어를 검색합니다. 그런 다음 시스템에 추가할 하드웨어 장치를 선택할 수 있습니다. 카메라는 뷰에 사전 구성되며, 마이크로폰과 스피커 같은 기타 장치를 활성화하는 옵션이 있습니다. 또한 운영자 역할이나 관리자 역할을 가진 사용자를 시스템에 추가하는 옵션도 있습니다. 설치 후 XProtect Smart Client 이(가) 열리고 시스템을 사용할 준비가 됩니다.

또는, 설치 마법사를 닫으면, XProtect Management Client 을(를) 열어 시스템에 하드웨어와 사용자 추가하기 같은 구성 작업을 수동으로 수행할 수 있습니다.

> 이전 버전의 제품에서 업그레이드하는 경우, 시스템은 하드웨어를 검색하지 않거나 새 뷰와 사용자 프로필을 생성하지 않습니다.

1. 인터넷(https://www.milestonesys.com/downloads/)에서 소프트웨어를 다운로드하고 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 파일을 실행합니다.
2. 설치 파일의 압축이 풀립니다. 보안 설정에 따라 하나 이상의 Windows® 보안 경고가 나타납니다. 해당 내용을 수락하고 압축 풀기를 계속 진행합니다.
3. 완료 시 **Milestone XProtect VMS** 설치 마법사가 나타납니다.

1. 설치 중 사용할 **언어** 를 선택합니다(설치 완료 후 시스템에서 사용하는 언어가 아님. 시스템에서 사용하는 언어는 나중에 선택할 수 있음). **계속** 을 클릭합니다.
2. *Milestone 최종 사용자 사용권 계약* 을 읽습니다. **라이선스 계약의 조건에 동의** 확인란을 선택하고 **계속** 을 클릭합니다.
3. **사생활 보호 설정** 페이지에서 공유하고자 하는 사용량 데이터를 선택하고 **계속** 을 클릭합니다.

   > 시스템에서 EU GDPR을 준수하는 설치를 하려면 데이터 수집을 활성화해서는 안 됩니다. 데이터 보호 및 사용량 데이터 수집에 관한 자세한 내용은 GDPR 개인정보 보호지침을 참조하십시오.

   > 개인 정보 보호 설정을 나중에 언제든지 변경할 수 있습니다. 시스템 설정(옵션 대화 상자)도 참조하십시오.

4. **XProtect Essential+** 링크를 클릭하여 무료 라이선스 파일을 다운로드합니다.

   무료 라이선스 파일이 다운로드되고 **라이선스 파일의 위치 입력 또는 검색** 필드에 나타납니다. **계속** 을 클릭합니다.

4. **단일 컴퓨터** 를 선택합니다.

   설치할 구성 요소의 목록이 나타납니다(이 목록을 편집할 수 없음). **계속** 을 클릭합니다.

5. **시스템 구성 암호 할당** 페이지에서 시스템 구성을 보호해주는 암호를 입력합니다. 시스템 복구 또는 클러스터 추가와 같이 시스템을 확장할 경우 이 암호가 필요합니다.

   > 이 암호를 저장하고 안전하게 보관하십시오. 이 암호를 잃게 되는 경우, 시스템 구성을 복구할 수 없게 될 수도 있습니다.

   시스템 구성을 암호로 보호하고 싶지 않은 경우, **시스템 구성 암호를 사용하지 않기로 선택하며 시스템 구성이 암호화되지 않음을 이해했습니다** 를 선택하십시오.

   계속 을 클릭합니다.

6. **모바일 서버 데이터 보호 암호 할당** 페이지에서 암호를 입력하여 조사를 암호화합니다. 시스템 관리자로서 시스템 복구 시 또는 추가 모바일 서버로 시스템 확장 시 모바일 서버에 액세스하도록 암호를 입력해야 하게 됩니다.

   > ⚠ 이 암호를 저장하고 안전하게 보관해야 합니다. 그렇게 하지 않는 경우 모바일 서버 데이터를 복구하지 못하게 될 수 있습니다.

   조사를 암호로 보호하지 않으려면 **모바일 서버 데이터 보호 암호를 사용하지 않기로 선택하며 조사가 암호화되지 않게 될 것임을 이해했습니다** 를 선택하십시오.

   계속 을 클릭합니다.

7. **레코딩 서버 설정 지정** 페이지에서 다른 레코딩 서버 설정을 지정합니다.
   1. **레코딩 서버 이름** 필드에서 레코딩 서버의 이름을 입력합니다. 컴퓨터의 이름이 기본값입니다.
   2. **관리 서버 주소** 필드는 관리 서버의 주소와 포트 번호를 나타냅니다: localhost:80.
   3. **미디어 데이터베이스 위치 선택** 필드에서 비디오 레코딩을 저장할 위치를 선택합니다. Milestone 은(는) 비디오 레코딩을 시스템 드라이브가 아닌, 소프트웨어를 설치한 곳과 다른 위치에 저장하도록 권장합니다. 기본 위치는 이용 가능한 공간이 가장 많은 드라이브입니다.
   4. **비디오 레코딩 보존 시간** 필드에서, 레코딩의 저장 기간을 정의합니다. 1일부터 365,000 일까지 입력할 수 있으며, 기본 보존 기간은 7일입니다.
   5. **계속** 을 클릭합니다.

8. **암호화 선택** 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.

   - 레코딩 서버와 데이터 수집기, 관리 서버 간

     내부 통신 흐름을 암호화하려면 **서버 인증서** 섹션에서 인증서를 선택합니다.

     > 레코딩 서버에서 관리 서버로의 연결을 암호화하는 경우, 시스템은 또한 관리 서버에서 레코딩 서버로의 연결을 암호화할 것을 요구합니다.

   - 레코딩 서버와 클라이언트 간

     레코딩 서버와 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트 구성 요소 간의 암호화를 활성화하려면 **스트리밍 데이터 인증서** 섹션에서 인증서를 선택합니다.

   - 모바일 서버와 클라이언트 간

     모바일 서버에서 데이터 스트림을 검색하는 클라어언트 구성 요소 간의 암호화를 활성화하려면 **모바일 스트리밍 미디어 인증서** 섹션에서 인증서를 선택합니다.

   - 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소 사이

     이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간 암호화를 활성화하려면, **이벤트 서버 및 확장** 섹션에서 인증서를 선택합니다.

   동일한 인증 파일을 모든 시스템 구성 요소에 사용하거나 시스템 구성 요소에 따라 다른 인증 파일을 사용할 수도 있습니다.

   보안 통신을 위한 시스템 준비에 관한 자세한 내용은 다음을 참조하십시오.

   - 페이지 134의 보안 통신(설명됨)
   - 인증서에 관한 Milestone 지침

   또한 알림 영역에 있는 Server Configurator 트레이 아이콘의 Management Server Manager 에서 설치 후 암호화를 활성화할 수도 있습니다.

9. **파일 위치 및 제품 언어 선택** 창에서 다음을 수행하십시오.

   1. **파일 위치** 필드에서, 소프트웨어를 설치할 위치를 선택합니다.

      > 컴퓨터에 Milestone XProtect VMS 제품이 이미 설치되어 있는 경우, 이 필드는 비활성화됩니다. 이 필드에서는 해당 구성 요소가 설치된 곳의 위치가 표시됩니다.

   2. **제품 언어** 에서 XProtect 제품을 설치할 언어를 선택합니다.
   3. **설치** 를 클릭합니다.

   이제 소프트웨어가 설치됩니다. 컴퓨터에서 이미 설치되지 않은 경우 설치 중에 Microsoft® SQL Server® Express 및 Microsoft IIS가 자동으로 설치됩니다.

10. 컴퓨터를 다시 시작하라는 메시지가 표시될 수 있습니다. 컴퓨터를 재시작한 후, 보안 설정에 따라 하나 이상의 Windows 보안 경고가 나타날 수 있습니다. 해당 내용을 수락하고 설치를 완료합니다.
11. 설치가 완료되면, 하나의 목록에서 컴퓨터에 설치된 구성 요소를 보여줍니다.

    계속 클릭해 시스템에 하드웨어와 사용자를 추가합니다.

    > 지금 **닫기** 클릭하면 구성 마법사를 우회해서 XProtect Management Client 이(가) 열립니다. Management Client 에서 시스템에 대한 하드웨어 및 사용자 추가와 같이 시스템을 구성할 수 있습니다.

12. **하드웨어 사용자 이름 및 암호 입력** 창에서, 제조업체의 기본값에서 변경한 하드웨어의 사용자 이름과 암호를 입력합니다.

    설치프로그램은네트워크에서이러한하드웨어뿐만아니라제조업체기본자격증명을가진하드웨어도검색합니다.

    계속 을 클릭한 후 시스템이 하드웨어를 스캔하는 동안 대기하십시오.
13. **시스템에 추가할 하드웨어 선택** 페이지에서, 시스템에 추가할 하드웨어를 선택합니다. **계속** 을 클릭한 후 시스템이 하드웨어를 추가하는 동안 대기하십시오.
14. **장치 구성** 페이지에서, 하드웨어 이름 옆 아이콘 편집을 클릭하여 하드웨어를 설명하는 이름을 부여할 수 있습니다. 이 이름은 하드웨어 장치 앞에 표시됩니다.

    카메라, 스피커 및 마이크로폰과 같은 하드웨어 장치를 활성화 또는 비활성화 할 수 있도록 하드웨어 노드를 확장하십시오.

    > 카메라는 기본으로 활성화되며, 스피커와 마이크로폰은 기본으로 비활성화됩니다.

    계속 을 클릭한 후 시스템이 하드웨어를 구성하는 동안 대기하십시오.
15. **사용자 추가** 페이지에서 시스템에 사용자를 Windows 사용자 또는 기본 사용자로 추가할 수 있습니다. 사용자는 관리자 역할이나 운영자 역할을 가질 수 있습니다.

    사용자를 정의하고 **추가** 를 클릭합니다.

    사용자 추가를 완료하면 **계속** 을 클릭합니다.
16. 설치 및 최초 구성이 완료되면, **구성 완료** 페이지가 나타나고 해당 페이지에서 다음 사항을 볼 수 있습니다.
    - 시스템에 추가된 하드웨어 장치 목록
    - 시스템에 추가된 사용자 목록
    - 사용자와 공유할 수 있는 XProtect Web Client 및 XProtect Mobile 클라이언트에 대한 주소

    닫기 를 클릭하면, XProtect Smart Client 이(가) 열리고 사용할 준비가 됩니다.

시스템 설치 - 단일 컴퓨터 옵션

단일 컴퓨터 옵션은 현재 컴퓨터에 모든 서버 및 클라이언트 구성 요소를 설치합니다.

Milestone 설치 전에 다음 섹션을 자세히 읽어보실 것을 권장합니다. 페이지 124의 설치를 시작하기 전에 .

FIPS 설치의 경우, Windows 운영 체제에서 FIPS가 활성화되어 있으면 XProtect VMS 을(를) 업그레이드할 수 없습니다. 설치하기 전, SQL Server을(를) 호스팅하는 컴퓨터를 비롯하여 비디오 관리 소프트웨어의 일부인 모든 컴퓨터에서 Windows FIPS 보안 정책을 비활성화하십시오. 그러나 2020 R3 이후 버전인 XProtect VMS 에서 업그레이드하는 경우, FIPS를 비활성화할 필요가 없습니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

최초 설치 후, 구성 마법사를 계속할 수 있습니다. 하드웨어 및 구성에 따라, 레코딩 서버는 네트워크에서 하드웨어를 검색합니다. 그런 다음 시스템에 추가할 하드웨어 장치를 선택할 수 있습니다. 카메라는 뷰에 사전 구성되며, 마이크로폰과 스피커 같은 기타 장치를 활성화하는 옵션이 있습니다. 또한 운영자 역할이나 관리자 역할을 가진 사용자를 시스템에 추가하는 옵션도 있습니다. 설치 후 XProtect Smart Client 이(가) 열리고 시스템을 사용할 준비가 됩니다.

또는, 설치 마법사를 닫으면, XProtect Management Client 을(를) 열어 시스템에 하드웨어와 사용자 추가하기 같은 구성 작업을 수동으로 수행할 수 있습니다.

이전 버전의 제품에서 업그레이드하는 경우, 시스템은 하드웨어를 검색하지 않거나 새 뷰와 사용자 프로필을 생성하지 않습니다.

1. 인터넷(https://www.milestonesys.com/downloads/)에서 소프트웨어를 다운로드하고 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 파일을 실행합니다.
2. 설치 파일의 압축이 풀립니다. 보안 설정에 따라 하나 이상의 Windows® 보안 경고가 나타납니다. 해당 내용을 수락하고 압축 풀기를 계속 진행합니다.
3. 완료 시 **Milestone XProtect VMS** 설치 마법사가 나타납니다.
    1. 설치 중 사용할 **언어** 를 선택합니다(설치 완료 후 시스템에서 사용하는 언어가 아님. 시스템에서 사용하는 언어는 나중에 선택할 수 있음). **계속** 을 클릭합니다.
    2. *Milestone 최종 사용자 사용권 계약* 을 읽습니다. **라이선스 계약의 조건에 동의** 확인란을 선택하고 **계속** 을 클릭합니다.
    3. **사생활 보호 설정** 페이지에서 공유하고자 하는 사용량 데이터를 선택하고 **계속** 을 클릭합니다.

        시스템에서 EU GDPR을 준수하는 설치를 하려면 데이터 수집을 활성화해서는 안 됩니다. 데이터 보호 및 사용량 데이터 수집에 관한 자세한 내용은 GDPR 개인정보 보호지침을 참조하십시오.

> 개인 정보 보호 설정을 나중에 언제든지 변경할 수 있습니다. 시스템 설정(옵션 대화 상자)도 참조하십시오.

4. **라이선스 파일의 위치 입력 또는 찾아보기** 에서, XProtect 제공업체로부터 받은 라이선스 파일을 입력합니다. 또한, 무료 라이선스 파일을 다운로드하려면 파일 위치 검색 또는 **XProtect Essential+** 링크를 클릭합니다. 무료 XProtect Essential+ 제품에 대한 제한 사항은 페이지 103의 제품 비교를 참조하십시오. 시스템은 계속 진행하기 전에 라이선스의 유효성을 확인합니다. **계속** 을 클릭합니다.

4. **단일 컴퓨터** 를 선택합니다.

   설치할 구성 요소의 목록이 나타납니다(이 목록을 편집할 수 없음). **계속** 을 클릭합니다.

5. **시스템 구성 암호 할당** 페이지에서 시스템 구성을 보호해주는 암호를 입력합니다. 시스템 복구 또는 클러스터 추가와 같이 시스템을 확장할 경우 이 암호가 필요합니다.

   > 이 암호를 저장하고 안전하게 보관하십시오. 이 암호를 잃게 되는 경우, 시스템 구성을 복구할 수 없게 될 수도 있습니다.

   시스템 구성을 암호로 보호하고 싶지 않은 경우, **시스템 구성 암호를 사용하지 않기로 선택하며 시스템 구성이 암호화되지 않음을 이해했습니다** 를 선택하십시오.

   계속 을 클릭합니다.

6. **모바일 서버 데이터 보호 암호 할당** 페이지에서 암호를 입력하여 조사를 암호화합니다. 시스템 관리자로서 시스템 복구 시 또는 추가 모바일 서버로 시스템 확장 시 모바일 서버에 액세스하도록 암호를 입력해야 하게 됩니다.

   > 이 암호를 저장하고 안전하게 보관해야 합니다. 그렇게 하지 않는 경우 모바일 서버 데이터를 복구하지 못하게 될 수 있습니다.

   조사를 암호로 보호하지 않으려면 **모바일 서버 데이터 보호 암호를 사용하지 않기로 선택하며 조사가 암호화되지 않게 될 것임을 이해했습니다** 를 선택하십시오.

   계속 을 클릭합니다.

7. **레코딩 서버 설정 지정** 페이지에서 다른 레코딩 서버 설정을 지정합니다.
    1. **레코딩 서버 이름** 필드에서 레코딩 서버의 이름을 입력합니다. 컴퓨터의 이름이 기본값입니다.
    2. **관리 서버 주소** 필드는 관리 서버의 주소와 포트 번호를 나타냅니다: localhost:80.
    3. **미디어 데이터베이스 위치 선택** 필드에서 비디오 레코딩을 저장할 위치를 선택합니다. Milestone 은(는) 비디오 레코딩을 시스템 드라이브가 아닌, 소프트웨어를 설치한 곳과 다른 위치에 저장하도록 권장합니다. 기본 위치는 이용 가능한 공간이 가장 많은 드라이브입니다.
    4. **비디오 레코딩 보존 시간** 필드에서, 레코딩의 저장 기간을 정의합니다. 1일부터 365,000 일까지 입력할 수 있으며, 기본 보존 기간은 7일입니다.
    5. **계속** 을 클릭합니다.
8. **암호화 선택** 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.
    - 레코딩 서버와 데이터 수집기, 관리 서버 간

      내부 통신 흐름을 암호화하려면 **서버 인증서** 섹션에서 인증서를 선택합니다.

      > ⚠ 레코딩 서버에서 관리 서버로의 연결을 암호화하는 경우, 시스템은 또한 관리 서버에서 레코딩 서버로의 연결을 암호화할 것을 요구합니다.

    - 레코딩 서버와 클라이언트 간

      레코딩 서버와 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트 구성 요소 간의 암호화를 활성화하려면 **스트리밍 데이터 인증서** 섹션에서 인증서를 선택합니다.

    - 모바일 서버와 클라이언트 간

      모바일 서버에서 데이터 스트림을 검색하는 클라어언트 구성 요소 간의 암호화를 활성화하려면 **모바일 스트리밍 미디어 인증서** 섹션에서 인증서를 선택합니다.

    - 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소 사이

      이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간 암호화를 활성화하려면, **이벤트 서버 및 확장** 섹션에서 인증서를 선택합니다.

    동일한 인증 파일을 모든 시스템 구성 요소에 사용하거나 시스템 구성 요소에 따라 다른 인증 파일을 사용할 수도 있습니다.

    보안 통신을 위한 시스템 준비에 관한 자세한 내용은 다음을 참조하십시오.

    - 페이지 134의 보안 통신(설명됨)
    - 인증서에 관한 Milestone 지침

    또한 알림 영역에 있는 Server Configurator 트레이 아이콘의 Management Server Manager 에서 설치 후 암호화를 활성화할 수도 있습니다.

9. **파일 위치 및 제품 언어 선택** 창에서 다음을 수행하십시오.

    1. **파일 위치** 필드에서, 소프트웨어를 설치할 위치를 선택합니다.

    > 컴퓨터에 Milestone XProtect VMS 제품이 이미 설치되어 있는 경우, 이 필드는 비활성화됩니다. 이 필드에서는 해당 구성 요소가 설치된 곳의 위치가 표시됩니다.

    2. **제품 언어** 에서 XProtect 제품을 설치할 언어를 선택합니다.
    3. **설치** 를 클릭합니다.

    이제 소프트웨어가 설치됩니다. 컴퓨터에서 이미 설치되지 않은 경우 설치 중에 Microsoft® SQL Server® Express 및 Microsoft IIS가 자동으로 설치됩니다.

10. 컴퓨터를 다시 시작하라는 메시지가 표시될 수 있습니다. 컴퓨터를 재시작한 후, 보안 설정에 따라 하나 이상의 Windows 보안 경고가 나타날 수 있습니다. 해당 내용을 수락하고 설치를 완료합니다.

11. 설치가 완료되면, 하나의 목록에서 컴퓨터에 설치된 구성 요소를 보여줍니다.

    계속 클릭해 시스템에 하드웨어와 사용자를 추가합니다.

    > 지금 **닫기** 클릭하면 구성 마법사를 우회해서 XProtect Management Client 이(가) 열립니다. Management Client 에서 시스템에 대한 하드웨어 및 사용자 추가와 같이 시스템을 구성할 수 있습니다.

12. **하드웨어 사용자 이름 및 암호 입력** 창에서, 제조업체의 기본값에서 변경한 하드웨어의 사용자 이름과 암호를 입력합니다.

    설치프로그램은네트워크에서이러한하드웨어뿐만아니라제조업체기본자격증명을가진하드웨어도검색합니다.

    계속 을 클릭한 후 시스템이 하드웨어를 스캔하는 동안 대기하십시오.

13. **시스템에 추가할 하드웨어 선택** 페이지에서, 시스템에 추가할 하드웨어를 선택합니다. **계속** 을 클릭한 후 시스템이 하드웨어를 추가하는 동안 대기하십시오.

14. **장치 구성** 페이지에서, 하드웨어 이름 옆 아이콘 편집을 클릭하여 하드웨어를 설명하는 이름을 부여할 수 있습니다. 이 이름은 하드웨어 장치 앞에 표시됩니다.

    카메라, 스피커 및 마이크로폰과 같은 하드웨어 장치를 활성화 또는 비활성화 할 수 있도록 하드웨어 노드를 확장하십시오.

    > 카메라는 기본으로 활성화되며, 스피커와 마이크로폰은 기본으로 비활성화됩니다.

    계속 을 클릭한 후 시스템이 하드웨어를 구성하는 동안 대기하십시오.

15. **사용자 추가** 페이지에서 시스템에 사용자를 Windows 사용자 또는 기본 사용자로 추가할 수 있습니다. 사용자는 관리자 역할이나 운영자 역할을 가질 수 있습니다.

    사용자를 정의하고 **추가** 를 클릭합니다.

    사용자 추가를 완료하면 **계속** 을 클릭합니다.

16. 설치 및 최초 구성이 완료되면, **구성 완료** 페이지가 나타나고 해당 페이지에서 다음 사항을 볼 수 있습니다.
    - 시스템에 추가된 하드웨어 장치 목록
    - 시스템에 추가된 사용자 목록
    - 사용자와 공유할 수 있는 XProtect Web Client 및 XProtect Mobile 클라이언트에 대한 주소

    닫기 를 클릭하면, XProtect Smart Client 이(가) 열리고 사용할 준비가 됩니다.

시스템 설치 - 사용자 정의 옵션

사용자 정의 옵션의 경우 관리 서버를 설치하지만, 현재 컴퓨터에 설치하고자 하는 다른 서버 및 클라이언트 구성 요소를 선택할 수 있습니다. 기본적으로 레코딩 서버는 구성 요소 목록에서 선택되어 있지 않습니다. 선택 항목에 따라 이후에 다른 컴퓨터에 선택되지 않은 시스템 구성 요소를 설치할 수 있습니다. 각 시스템 구성 요소 및 역할에 관한 자세한 정보는 페이지 32의 제품 개요를 참조하십시오. 다른 컴퓨터에 대한 설치는 Download Manager 로 명명된 관리 서버 다운로드 웹 페이지를 통해 이뤄집니다. Download Manager 을(를) 통한 설치에 관한 자세한 정보는, 페이지 168의 Download Manager/다운로드 웹 페이지를 참조하십시오.

> Milestone 설치 전에 다음 섹션을 자세히 읽어보실 것을 권장합니다. 페이지 124의 설치를 시작하기 전에 .

> FIPS 설치의 경우, Windows 운영 체제에서 FIPS가 활성화되어 있으면 XProtect VMS 을(를) 업그레이드할 수 없습니다. 설치하기 전, SQL Server을(를) 호스팅하는 컴퓨터를 비롯하여 비디오 관리 소프트웨어의 일부인 모든 컴퓨터에서 Windows FIPS 보안 정책을 비활성화하십시오. 그러나 2020 R3 이후 버전인 XProtect VMS 에서 업그레이드하는 경우, FIPS를 비활성화할 필요가 없습니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

1. 인터넷(https://www.milestonesys.com/downloads/)에서 소프트웨어를 다운로드하고 `Milestone XProtect VMS Products 2023 R3 System Installer.exe` 파일을 실행합니다.
2. 설치 파일의 압축이 풀립니다. 보안 설정에 따라 하나 이상의 Windows® 보안 경고가 나타납니다. 해당 내용을 수락하고 압축 풀기를 계속 진행합니다.
3. 완료 시 **Milestone XProtect VMS** 설치 마법사가 나타납니다.

1. 설치 중 사용할 **언어** 를 선택합니다(설치 완료 후 시스템에서 사용하는 언어가 아님. 시스템에서 사용하는 언어는 나중에 선택할 수 있음). **계속** 을 클릭합니다.
2. *Milestone 최종 사용자 사용권 계약* 을 읽습니다. **라이선스 계약의 조건에 동의** 확인란을 선택하고 **계속** 을 클릭합니다.
3. **사생활 보호 설정** 페이지에서 공유하고자 하는 사용량 데이터를 선택하고 **계속** 을 클릭합니다.

   > 시스템에서 EU GDPR을 준수하는 설치를 하려면 데이터 수집을 활성화해서는 안 됩니다. 데이터 보호 및 사용량 데이터 수집에 관한 자세한 내용은 GDPR 개인정보 보호지침을 참조하십시오.

   > 개인 정보 보호 설정을 나중에 언제든지 변경할 수 있습니다. 시스템 설정(옵션 대화 상자)도 참조하십시오.

4. **라이선스 파일의 위치 입력 또는 찾아보기** 에서, XProtect 제공업체로부터 받은 라이선스 파일을 입력합니다. 또한, 무료 라이선스 파일을 다운로드하려면 파일 위치 검색 또는 **XProtect Essential+** 링크를 클릭합니다. 무료 XProtect Essential+ 제품에 대한 제한 사항은 페이지 103의 제품 비교를 참조하십시오. 시스템은 계속 진행하기 전에 라이선스의 유효성을 확인합니다. **계속** 을 클릭합니다.

4. **사용자 정의** 를 선택합니다. 설치할 구성 요소 목록이 나타납니다. 관리 서버와는 별도로, 목록의 모든 요소는 선택 항목입니다. 기본적으로 레코딩 서버와 모바일 서버는 선택되어 있지 않습니다. 설치하고자 하는 시스템 구성 요소를 선택하고 **계속** 을 클릭하십시오.

   > 시스템이 제대로 작동하도록 하려면 XProtect API Gateway의 인스턴스를 하나 이상 설치해야 합니다.

   > 아래의 단계에서 모든 시스템 구성 요소가 설치됩니다. 더 분산된 시스템을 위해, 컴퓨터에 적은 시스템 구성 요소를 설치하고 남은 시스템 구성 요소는 다른 컴퓨터에 설치합니다. 설치 단계를 확인할 수 없는 경우, 이 페이지가 속한 시스템 구성 요소 설치를 선택하지 않았기 때문일 수 있습니다. 그러한 경우, 다음 단계로 계속 진행합니다. 또한 페이지 149의 Download Manager 을(를) 통해 설치(설명됨), , 페이지 151의 다음을 통해 레코딩 서버 설치: Download Manager및 를 참조하십페이지 155의 명령줄 셸을 통해 자동 설치(설명됨)시오.

5. **XProtect 시스템과 함께 사용하기 위한 IIS상의 웹사이트 선택** 페이지는 컴퓨터에서 사용 가능한 IIS 웹사이트가 한 개 이상이 있을 때에만 보입니다. XProtect 시스템과 함께 사용할 웹사이트를 반드시 선택해야 합니다. HTTPS 바인딩이 있는 사이트를 선택합니다. **계속** 을 클릭합니다.

   Microsoft® IIS가 해당 컴퓨터에 설치되지 않았다면 이제 설치되었을 것입니다.

6. **Microsoft SQL Server 선택** 페이지에서 사용할 SQL Server 을(를) 선택합니다. 또한 페이지 149의 SQL Server 사용자 정의 시 옵션를 참조하십시오. **계속** 을 클릭합니다.

   로컬 컴퓨터에 SQL Server이(가) 없는 경우 Microsoft SQL Server Express을(를) 설치하면 되는데, 보통 네트워크의 전용 SQL Server을(를) 사용하는 대형 분산 시스템에 설치합니다.

7. **데이터베이스 선택**(기존 SQL Server을(를) 선택한 경우에만 표시됨)에서 시스템 구성을 저장할 SQL Server 데이터베이스를 선택하거나 생성합니다. 기존 SQL Server 데이터베이스를 선택한 경우, **유지** 또는 기존 데이터 **덮어쓰기** 중 하나를 선택합니다. 업그레이드를 하는 경우, 기존 데이터 유지하기를 선택하여 시스템 구성을 잃지 않도록 하십시오. 또한 페이지 149의 SQL Server 사용자 정의 시 옵션를 참조하십시오. **계속을** 클릭합니다.
8. **데이터베이스 설정** 페이지에서 **설치 관리자가 데이터베이스를 생성 또는 재생성하도록 함** 또는 **사전 생성된 데이터베이스 사용**을 선택합니다.
9. 데이터베이스가 자동으로 생성 또는 재생성되도록 하려면 **설치 관리자가 데이터베이스를 생성하거나 재생성하도록 함**을 선택하고 **계속**을 클릭합니다.
10. 목적에 맞게 설정한 데이터베이스 또는 이미 생성된 데이터베이스를 사용하려면 **사전 생성된 데이터베이스 사용**을 선택합니다. 그러면 **고급 데이터베이스 설정** 페이지를 볼 수 있습니다.
11. **고급 데이터베이스 설정** 페이지에서 XProtect 구성 요소의 서버 및 데이터베이스 이름을 입력합니다.
12. **Windows 인증, 서버 인증서 신뢰 안 함(권장)** 또는 **Windows 인증, 서버 인증서 신뢰** 중 하나를 선택하거나 **Azure Active Directory 통합, 서버 인증서 신뢰 안 함(권장)**을 선택합니다.

    설치에 사용할 계정은 사용하려는 인증 유형에 따라 Azure AD 또는 Windows AD에서 생성해야 합니다. 계정에는 멀티 팩터 인증(MFA)이 지원되지 않습니다.

    Windows 인증에는 **(서버 인증서 신뢰 안 함)** 옵션이 권장되며 Azure Active Directory 통합에는 필수입니다. 이는 설치 전에 서버 인증서의 유효성을 검사하고 확인하기 위한 것입니다. 유효하지 않은 서버 인증서에 대한 자세한 정보는 설치 로그 파일에서 확인할 수 있습니다. **Windows 인증, 서버 인증서 신뢰** 옵션을 사용하면 서버 인증서의 유효성 검사를 건너뛸 수 있습니다.

13. 아이콘을 클릭하여 연결을 확인합니다. 아이콘을 클릭하면 서버 인증서의 유효성도 검사할 수 있습니다.
14. **계속** 을 클릭합니다.

15. **시스템 구성 암호 할당** 페이지에서 시스템 구성을 보호해주는 암호를 입력합니다. 시스템 복구 또는 클러스터 추가와 같이 시스템을 확장할 경우 이 암호가 필요합니다.

    > 이 암호를 저장하고 안전하게 보관하십시오. 이 암호를 잃게 되는 경우, 시스템 구성을 복구할 수 없게 될 수도 있습니다.

    시스템 구성을 암호로 보호하고 싶지 않은 경우, **시스템 구성 암호를 사용하지 않기로 선택하며 시스템 구성이 암호화되지 않음을 이해했습니다** 를 선택하십시오.

    계속 을 클릭합니다.

16. **모바일 서버 데이터 보호 암호 할당** 페이지에서 암호를 입력하여 조사를 암호화합니다. 시스템 관리자로서 시스템 복구 시 또는 추가 모바일 서버로 시스템 확장 시 모바일 서버에 액세스하도록 암호를 입력해야 하게 됩니다.

    > 이 암호를 저장하고 안전하게 보관해야 합니다. 그렇게 하지 않는 경우 모바일 서버 데이터를 복구하지 못하게 될 수 있습니다.

    조사를 암호로 보호하지 않으려면 **모바일 서버 데이터 보호 암호를 사용하지 않기로 선택하며 조사가 암호화되지 않게 될 것임을 이해했습니다** 를 선택하십시오.

    계속 을 클릭합니다.

17. **레코딩 서버에 대한 서비사 계정 선택** 에서 **이 사전 정의된 계정** 또는 **이 계정** 중 하나를 선택하여 레코딩 서버에 대한 서비스 계정을 선택합니다.

    필요한 경우 암호를 입력합니다.

    > 계정의 사용자 이름은 반드시 한 단어여야 합니다. 중간에 공백이 있으면 안 됩니다.

    계속 을 클릭합니다.

18. **레코딩 서버 설정 지정** 페이지에서 다른 레코딩 서버 설정을 지정합니다.

    1. **레코딩 서버 이름** 필드에서 레코딩 서버의 이름을 입력합니다. 컴퓨터의 이름이 기본값입니다.
    2. **관리 서버 주소** 필드는 관리 서버의 주소와 포트 번호를 나타냅니다: localhost:80.
    3. **미디어 데이터베이스 위치 선택** 필드에서 비디오 레코딩을 저장할 위치를 선택합니다. Milestone 은(는) 비디오 레코딩을 시스템 드라이브가 아닌, 소프트웨어를 설치한 곳과 다른 위치에 저장하도록 권장합니다. 기본 위치는 이용 가능한 공간이 가장 많은 드라이브입니다.
    4. **비디오 레코딩 보존 시간** 필드에서, 레코딩의 저장 기간을 정의합니다. 1일부터 365,000 일까지 입력할 수 있으며, 기본 보존 기간은 7일입니다.
    5. **계속** 을 클릭합니다.

19. **암호화 선택** 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.

    - 레코딩 서버와 데이터 수집기, 관리 서버 간

      내부 통신 흐름을 암호화하려면 **서버 인증서** 섹션에서 인증서를 선택합니다.

      > ⚠ 레코딩 서버에서 관리 서버로의 연결을 암호화하는 경우, 시스템은 또한 관리 서버에서 레코딩 서버로의 연결을 암호화할 것을 요구합니다.

    - 레코딩 서버와 클라이언트 간

      레코딩 서버와 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트 구성 요소 간의 암호화를 활성화하려면 **스트리밍 데이터 인증서** 섹션에서 인증서를 선택합니다.

    - 모바일 서버와 클라이언트 간

      모바일 서버에서 데이터 스트림을 검색하는 클라어언트 구성 요소 간의 암호화를 활성화하려면 **모바일 스트리밍 미디어 인증서** 섹션에서 인증서를 선택합니다.

    - 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소 사이

      이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간 암호화를 활성화하려면, **이벤트 서버 및 확장** 섹션에서 인증서를 선택합니다.

    동일한 인증 파일을 모든 시스템 구성 요소에 사용하거나 시스템 구성 요소에 따라 다른 인증 파일을 사용할 수도 있습니다.

    보안 통신을 위한 시스템 준비에 관한 자세한 내용은 다음을 참조하십시오.

    - 페이지 134의 보안 통신(설명됨)
    - 인증서에 관한 Milestone 지침

    또한 알림 영역에 있는 Server Configurator 트레이 아이콘의 Management Server Manager 에서 설치 후 암호화를 활성화할 수도 있습니다.

20. **파일 위치 및 제품 언어 선택** 페이지에서 프로그램 파일에 대한 **파일 위치** 를 선택합니다.

    > ✎ 컴퓨터에 Milestone XProtect VMS 제품이 이미 설치되어 있는 경우, 이 필드는 비활성화됩니다. 이 필드에서는 해당 구성 요소가 설치된 곳의 위치가 표시됩니다.

21. **제품 언어** 필드에서 XProtect 제품을 설치할 언어를 선택합니다. **설치** 를 클릭합니다.

    이제 소프트웨어가 설치됩니다. 설치가 끝나면 성공적으로 설치된 시스템 구성 요소 목록이 표시됩니다. **닫기** 를 클릭합니다.

22. 컴퓨터를 다시 시작하라는 메시지가 표시될 수 있습니다. 컴퓨터를 재시작한 후, 보안 설정에 따라 하나 이상의 Windows 보안 경고가 나타날 수 있습니다. 해당 내용을 수락하고 설치를 완료합니다.

23. Management Client 에 시스템을 구성합니다. 페이지 176의 초기 구성 작업 목록를 참조하십시오.

24. 선택 사항에 따라 Download Manager 을(를) 통해 다른 컴퓨터에 남은 시스템 구성 요소를 설치합니다. 페이지 149의 Download Manager 을(를) 통해 설치(설명됨)를 참조하십시오.

SQL Server 사용자 정의 시 옵션

아래의 옵션과 함께 어떤 SQL Server 및 데이터베이스를 사용할지 결정합니다.

SQL Server 옵션:

- **이 컴퓨터에 Microsoft® SQL Server® Express 설치**: 이 옵션은 컴퓨터에 SQL Server을(를) 설치하지 않은 경우에만 표시됩니다.
- **이 컴퓨터에 SQL Server 사용**: 이 옵션은 해당 컴퓨터에 SQL Server을(를) 이미 설치한 경우에만 표시됩니다.
- **검색을 통해 네트워크에 SQL Server 을(를) 선택**: 네트워크 서브넷에서 찾을 수 있는 모든 SQL Server 설치를 검색할 수 있습니다.
- **네트워크상에서 SQL Server 을(를) 선택**: 검색을 통해 찾을 수 없는 SQL Server의 주소(호스트 이름 또는 IP 주소)를 입력할 수 있습니다.

SQL Server 데이터베이스 옵션:

- **새 데이터베이스 만들기** : 주로 신규 설치용
- **기존 데이터베이스 사용** : 주로 기존 설치 업그레이드용. Milestone 은(는) 기존 SQL Server 데이터베이스를 재사용하고 기존 데이터를 그 안에 보존하여 시스템 구성을 상실하지 않도록 할 것을 권장합니다. 또한 SQL Server 데이터베이스에서 데이터 덮어쓰기를 선택할 수도 있습니다.

신규 XProtect 구성 요소 설치

Download Manager 을(를) 통해 설치(설명됨)

관리 서버가 설치된 곳 이외의 컴퓨터에 시스템 구성 요소를 설치하려면, Management Server 다운로드 웹사이트 Download Manager 을(를) 통해 다음의 시스템 구성 요소를 설치해야 합니다.

1. Management Server 이(가) 설치된 컴퓨터에서 Management Server 의 다운로드 웹 페이지로 이동합니다. Windows의 **시작** 메뉴에서 **Milestone** > **관리자 설치 페이지**를 선택한 후 나중에 다른 컴퓨터에 시스템 구성 요소를 설치할 때 사용하도록 인터넷 주소를 적거나 복사해놓습니다. 주소는 보통 *http://[management server address]/installation/Admin/default-en-US.htm* 입니다.
2. 각각의 다른 컴퓨터에 로그인하여 하나 이상의 기타 시스템 구성 요소를 설치합니다.
    - Recording Server(자세한 정보는 페이지 151의 다음을 통해 레코딩 서버 설치: Download Manager 또는 페이지 156의 레코딩 서버 자동 설치를 참조하십시오)
    - Management Client (자세한 정보는 페이지 150의 Download Manager 을(를) 통해 Management Client 설치를 참조하십시오)
    - Smart Client

- Event Server 설치 후 API 게이트웨이를 다시 시작해야 합니다. 나중에 컴퓨터의 이름을 변경할 경우에도 API 게이트웨이를 다시 시작해야 합니다.

  > Event Server 을(를) FIPS 규격 환경에 설치하는 경우, 설치 전 Windows FIPS 140-2 모드를 비활성화해야 합니다.

- Log Server (자세한 정보는 페이지 158의 로그 서버 자동 설치를 참조하십시오)
- Mobile Server (자세한 내용은 XProtect Mobile 서버 설명서 참조)

3. 인터넷 브라우저를 열고 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 관련 설치 프로그램을 다운로드합니다.
4. 설치 관리자를 실행합니다.

다양한 설치 단계의 선택 및 설정에 관해 궁금한 점이 있는 경우 페이지 144의 시스템 설치 - 사용자 정의 옵션를 참조하십시오.

Download Manager 을(를) 통해 Management Client 설치

XProtect 시스템에 다수의 관리자가 있거나 단지 다수의 컴퓨터에서 XProtect 시스템을 관리하고자 하는 경우, 아래 지시를 따라 Management Client 을(를) 설치할 수 있습니다.

> Management Client 은(는) 항상 관리 서버에 설치되어 있습니다.

1. Management Server 이(가) 설치된 컴퓨터에서 Management Server 의 다운로드 웹 페이지로 이동합니다. Windows의 **시작** 메뉴에서 **Milestone** > **관리자 설치 페이지**를 선택한 후 나중에 다른 컴퓨터에 시스템 구성 요소를 설치할 때 사용하도록 인터넷 주소를 적거나 복사해놓습니다. 주소는 보통 *http://[management server address]/installation/Admin/default-en-US.htm* 입니다.
2. 시스템 구성 요소를 설치하고자 하는 컴퓨터에 로그인합니다.
1. 인터넷 브라우저를 열고 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.
3. 설치 프로그램 Management Client 에 대해 **모든 언어** 를 클릭합니다. 다운로드한 파일을 실행합니다.
4. 모든 경고 메시지에 대해 **예** 를 클릭합니다. 압축이 풀리기 시작합니다.
5. 설치 프로그램에 사용할 언어를 선택합니다. **계속** 을 클릭합니다.
6. 사용권 계약 내용을 읽고 동의합니다. **계속** 을 클릭합니다.
7. 파일 위치와 제품 언어를 선택합니다. **설치** 를 클릭합니다.
8. 설치가 완료됩니다. 성공적으로 설치된 구성 요소 목록이 표시됩니다. **닫기** 를 클릭합니다.
9. Management Client 을(를) 열려면 데스크톱에서 아이콘을 클릭합니다.
10. Management Client 로그인 대화 상자가 나타납니다.
11. **컴퓨터** 필드에 관리 서버의 호스트 이름 또는 IP 주소를 지정합니다.

12. 인증을 선택하고 사용자 이름과 암호를 입력합니다. **연결** 을 클릭합니다. Management Client 이(가) 실행됩니다.

    Management Client 의 기능과 시스템을 통해 수행할 수 있는 작업에 대한 자세한 내용을 읽으려면 도구 메뉴에서 **도움말** 을 클릭하십시오.

다음을 통해 레코딩 서버 설치: Download Manager

시스템 구성 요소가 별도의 컴퓨터에 배포되면, 아래 지침에 따라 레코딩 서버를 설치할 수 있습니다.

단일 컴퓨터 설치를 하였다면 레코딩 서버가 이미 설치되었지만, 더 많은 용량을 필요로 하는 경우 동일한 지침을 사용하여 더 많은 레코딩 서버를 추가할 수 있습니다.

장애 조치 레코딩 서버를 설치해야 하는 경우 페이지 153의 다음을 통해 장애 조치 레코딩 서버 설치: Download Manager를 참조하십시오.

1. Management Server 이(가) 설치된 컴퓨터에서 Management Server 의 다운로드 웹 페이지로 이동합니다. Windows의 **시작** 메뉴에서 **Milestone** > **관리자 설치 페이지**를 선택한 후 나중에 다른 컴퓨터에 시스템 구성 요소를 설치할 때 사용하도록 인터넷 주소를 적거나 복사해놓습니다. 주소는 보통 *http://[management server address]/installation/Admin/default-en-US.htm* 입니다.
2. 시스템 구성 요소를 설치하고자 하는 컴퓨터에 로그인합니다.
3. 인터넷 브라우저를 열고 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.
4. **레코딩 서버 설치 관리자** 아래에서 **모든 언어** 를 선택하여 레코딩 서버 설치 관리자를 다운로드합니다. 설치 관리자를 저장하거나 웹 페이지에서 직접 실행합니다.
5. 설치 중 사용할 **언어** 를 선택합니다. **계속** 을 클릭합니다.
6. **설치 유형 선택** 페이지에서 다음을 선택합니다.

   일반 을 선택하면 기본값을 사용하여 레코딩 서버를 설치합니다.

   사용자 정의 를 선택하면 사용자 정의 값을 사용하여 레코딩 서버를 설치합니다.
7. **레코딩 서버 설정 지정** 페이지에서 다른 레코딩 서버 설정을 지정합니다.
   1. **레코딩 서버 이름** 필드에서 레코딩 서버의 이름을 입력합니다. 컴퓨터의 이름이 기본값입니다.
   2. **관리 서버 주소** 필드는 관리 서버의 주소와 포트 번호를 나타냅니다: localhost:80.
   3. **미디어 데이터베이스 위치 선택** 필드에서 비디오 레코딩을 저장할 위치를 선택합니다. Milestone 은(는) 비디오 레코딩을 시스템 드라이브가 아닌, 소프트웨어를 설치한 곳과 다른 위치에 저장하도록 권장합니다. 기본 위치는 이용 가능한 공간이 가장 많은 드라이브입니다.
   4. **비디오 레코딩 보존 시간** 필드에서, 레코딩의 저장 기간을 정의합니다. 1일부터 365,000 일까지 입력할 수 있으며, 기본 보존 기간은 7일입니다.
   5. **계속** 을 클릭합니다.

8. **레코딩 서버 IP 주소** 페이지는 **사용자 정의** 를 선택한 경우에만 나타납니다. 이 컴퓨터에 설치할 레코딩 서버의 수를 지정합니다. **계속** 을 클릭합니다.
9. **레코딩 서버에 대한 서비사 계정 선택** 에서 **이 사전 정의된 계정** 또는 **이 계정** 중 하나를 선택하여 레코딩 서버에 대한 서비스 계정을 선택합니다.

   필요한 경우 암호를 입력합니다.

   > 계정의 사용자 이름은 반드시 한 단어여야 합니다. 중간에 공백이 있으면 안 됩니다.

   계속 을 클릭합니다.
10. **암호화 선택** 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.

    - 레코딩 서버와 데이터 수집기, 관리 서버 간

      내부 통신 흐름을 암호화하려면 **서버 인증서** 섹션에서 인증서를 선택합니다.

      > 레코딩 서버에서 관리 서버로의 연결을 암호화하는 경우, 시스템은 또한 관리 서버에서 레코딩 서버로의 연결을 암호화할 것을 요구합니다.

    - 레코딩 서버와 클라이언트 간

      레코딩 서버와 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트 구성 요소 간의 암호화를 활성화하려면 **스트리밍 데이터 인증서** 섹션에서 인증서를 선택합니다.

    - 모바일 서버와 클라이언트 간

      모바일 서버에서 데이터 스트림을 검색하는 클라어언트 구성 요소 간의 암호화를 활성화하려면 **모바일 스트리밍 미디어 인증서** 섹션에서 인증서를 선택합니다.

    - 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소 사이

      이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간 암호화를 활성화하려면, **이벤트 서버 및 확장** 섹션에서 인증서를 선택합니다.

    동일한 인증 파일을 모든 시스템 구성 요소에 사용하거나 시스템 구성 요소에 따라 다른 인증 파일을 사용할 수도 있습니다.

    보안 통신을 위한 시스템 준비에 관한 자세한 내용은 다음을 참조하십시오.

    - 페이지 134의 보안 통신(설명됨)
    - 인증서에 관한 Milestone 지침

    또한 알림 영역에 있는 Server Configurator 트레이 아이콘의 Management Server Manager 에서 설치 후 암호화를 활성화할 수도 있습니다.

11. **파일 위치 및 제품 언어 선택** 페이지에서 프로그램 파일에 대한 **파일 위치** 를 선택합니다.

> 컴퓨터에 Milestone XProtect VMS 제품이 이미 설치되어 있는 경우, 이 필드는 비활성화 됩니다. 이 필드에서는 해당 구성 요소가 설치된 곳의 위치가 표시됩니다.

12. **제품 언어** 필드에서 XProtect 제품을 설치할 언어를 선택합니다. **설치** 를 클릭합니다.

    이제 소프트웨어가 설치됩니다. 설치가 끝나면 성공적으로 설치된 시스템 구성 요소 목록이 표시됩니다. **닫기** 를 클릭합니다.

13. 장애 조치 레코딩 서버를 설치했으면, Recording Server Manager 트레이 아이콘을 통해 서버의 상태를 확인할 수 있으며 Management Client 에서 구성할 수 있습니다. 자세한 정보는 페이지 176의 초기 구성 작업 목록를 참조하십시오.

다음을 통해 장애 조치 레코딩 서버 설치: Download Manager

> 워크그룹을 구동하려면 장애 조치 레코딩 서버 대체 설치 방법(see 페이지 163의 작업 그룹에 대한 설치)을 참조하십시오.

1. Management Server 이(가) 설치된 컴퓨터에서 Management Server 의 다운로드 웹 페이지로 이동합니다. Windows의 **시작** 메뉴에서 **Milestone** > **관리자 설치 페이지**를 선택한 후 나중에 다른 컴퓨터에 시스템 구성 요소를 설치할 때 사용하도록 인터넷 주소를 적거나 복사해놓습니다. 주소는 보통 *http://[management server address]/installation/Admin/default-en-US.htm* 입니다.

   시스템 구성 요소를 설치하고자 하는 컴퓨터에 로그인합니다.

2. 인터넷 브라우저를 열고 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.

3. **레코딩 서버 설치 관리자** 아래에서 **모든 언어** 를 선택하여 레코딩 서버 설치 관리자를 다운로드합니다. 설치 관리자를 저장하거나 웹 페이지에서 직접 실행합니다.

4. 설치 중 사용할 **언어** 를 선택합니다. **계속** 을 클릭합니다.

5. **설치 관리자 유형 선택** 에서 **장애 조치** 를 선택하여 레코딩 서버를 장애 조치 레코딩 서버로 설치합니다.

6. **레코딩 서버 설정 지정** 페이지에서 다른 레코딩 서버 설정을 지정합니다. 장애 조치 레코딩 서버의 이름, 관리 서버의 주소, 미디어 데이터베이스에 대한 경로. **계속** 을 클릭합니다.

7. **레코딩 서버에 대한 서비스 계정 선택** 페이지에서, 그리고 장애 조치 레코딩 서버를 설치할 때 **이 계정** 으로 표시된 특정 사용자 계정을 사용해야 합니다. 이렇게 하여 장애 조치 사용자 계정을 생성합니다. 필요하면 암호를 입력하고 확인합니다. **계속** 을 클릭합니다.

8. **암호화 선택** 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.

   - 레코딩 서버와 데이터 수집기, 관리 서버 간

     내부 통신 흐름을 암호화하려면 **서버 인증서** 섹션에서 인증서를 선택합니다.

     > ⚠ 레코딩 서버에서 관리 서버로의 연결을 암호화하는 경우, 시스템은 또한 관리 서버에서 레코딩 서버로의 연결을 암호화할 것을 요구합니다.

   - 레코딩 서버와 클라이언트 간

     레코딩 서버와 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트 구성 요소 간의 암호화를 활성화하려면 **스트리밍 데이터 인증서** 섹션에서 인증서를 선택합니다.

   - 모바일 서버와 클라이언트 간

     모바일 서버에서 데이터 스트림을 검색하는 클라어언트 구성 요소 간의 암호화를 활성화하려면 **모바일 스트리밍 미디어 인증서** 섹션에서 인증서를 선택합니다.

   - 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소 사이

     이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간 암호화를 활성화하려면, **이벤트 서버 및 확장** 섹션에서 인증서를 선택합니다.

   동일한 인증 파일을 모든 시스템 구성 요소에 사용하거나 시스템 구성 요소에 따라 다른 인증 파일을 사용할 수도 있습니다.

   보안 통신을 위한 시스템 준비에 관한 자세한 내용은 다음을 참조하십시오.

   - 페이지 134의 보안 통신(설명됨)
   - 인증서에 관한 Milestone 지침

   또한 알림 영역에 있는 Server Configurator 트레이 아이콘의 Management Server Manager 에서 설치 후 암호화를 활성화할 수도 있습니다.

9. **파일 위치 및 제품 언어 선택** 페이지에서 프로그램 파일에 대한 **파일 위치** 를 선택합니다.

   > ✎ 컴퓨터에 Milestone XProtect VMS 제품이 이미 설치되어 있는 경우, 이 필드는 비활성화됩니다. 이 필드에서는 해당 구성 요소가 설치된 곳의 위치가 표시됩니다.

10. **제품 언어** 필드에서 XProtect 제품을 설치할 언어를 선택합니다. **설치** 를 클릭합니다.

    이제 소프트웨어가 설치됩니다. 설치가 끝나면 성공적으로 설치된 시스템 구성 요소 목록이 표시됩니다. **닫기** 를 클릭합니다.

11. 장애 조치 레코딩 서버를 설치했으면, Failover Server 서비스 트레이 아이콘을 통해 해당 상태를 확인할 수 있으며 Management Client 에서 구성할 수 있습니다. 자세한 정보는 페이지 176의 초기 구성 작업 목록를 참조하십시오.

기본이 아닌 포트를 사용하여 XProtect VMS 설치

XProtect VMS을(를) 설치하려면 특정 포트가 필요합니다. 특히 Management Server와(과) API Gateway은(는) IIS에서 실행되며 특정 포트가 사용 가능해야 합니다. 이 항목에서는 XProtect VMS을(를) 설치하고 IIS에 기본이 아닌 포트를 사용하는 방법에 대해 설명합니다. API Gateway만 설치할 때도 마찬가지입니다.

VMS가 사용하는 모든 포트에 대한 개요는 XProtect VMS 관리자 설명서(https://doc.milestonesys.com/2023r3/ko-KR/portal/htm/chapter-page-mc-administrator-manual.htm)를 참고하십시오.

IIS이(가) 아직 시스템에 설치되지 않은 경우 XProtect VMS 설치 프로그램은 IIS을(를) 설치하고 기본 포트의 기본 웹 사이트를 사용합니다.

XProtect VMS 기본값을 사용하지 않으려면 먼저 IIS을(를) 설치하십시오. 선택적으로 새 웹사이트를 추가하거나 기본 웹 사이트를 사용하여 진행합니다.

HTTPS에 대한 바인딩이 없으면 추가하고 컴퓨터에서 유효한 인증서를 선택합니다(XProtect VMS 설치 시 선택해야 함). 선택한 사용 가능한 포트에 대한 HTTP 및 HTTPS 바인딩의 포트 번호를 편집합니다.

XProtect VMS 설치 프로그램을 실행하고 **사용자 지정** 설치를 선택합니다.

설치하는 동안 사용 가능한 웹 사이트가 두 개 이상인 경우 **XProtect 시스템과 함께 사용할 IIS의 웹사이트 선택** 페이지가 나타납니다. XProtect 시스템과 함께 사용할 웹사이트를 반드시 선택해야 합니다. 설치 프로그램은 변경된 포트 번호를 사용합니다.

명령줄 셸을 통해 자동 설치(설명됨)

자동 설치를 하면시스템 관리자는 사용자의 참여 없이 그리고 가능한 최종 사용자를 방해하지 않고 대형 네트워크에서 XProtect VMS 및 Smart Client 소프트웨어를 설치하고 업그레이드할 수 있습니다.

XProtect VMS 및 Smart Client 설치 프로그램(.exe 파일)은 다른 명령줄 인수를 가지고 있습니다. 이러한 파일은 각기 고유한 명령줄 매개변수 묶음을 가지고 있으며 명령줄 셸로 직접 또는 인수 파일을 통해 불러낼 수 있습니다. 명령줄 셸에서 명령줄 옵션을 설치 프로그램와 함께 사용할 수도 있습니다.

XProtect 설치 프로그램과 프로그램의 명령줄 매개변수, 명령줄 옵션을 Microsoft 시스템 센터 구성 관리자(ConfigMgr로도 알려져 있는 SCCM)를 사용하여 소프트웨어 자동 배포 및 설치 도구를 사용하여 결합할 수 있습니다. 그러한 도구에 관한 자세한 정보는 제조사의 웹사이트를 방문하여 확인하십시오. 또한 Milestone Software Manager의 원격 설치 및 업데이트, 장치 팩 및 XProtect VMS에 대해 Smart Client을(를) 사용할 수도 있습니다. 자세한 내용은 Milestone Software Manager에 대한 관리자 설명서를 참조하십시오.

명령줄 매개변수 및 인수 파일

자동 설치 중에 다른 VMS 시스템 구성 요소와 명령줄 매개변수 및 인수 파일이 포함된 내부 통신에 밀접히 연결된 설정을 지정할 수 있습니다. 업그레이드 동안 명령줄 매개변수를 표시해주는 설정을 변경할 수 없으므로 명령줄 매개변수 및 인수 파일은 새 설치에 대해서만 사용할 수 있습니다.

사용 가능한 명령줄 매개변수를 보고 설치 프로그램에 대한 인수 파일을 생성하려면 명령줄 셸에서 설치 프로그램이 있는 디렉토리로 이동하여 다음 명령을 입력합니다:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

예:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

저장된 인수 파일(Arguments.xml)의 각 명령줄 매개변수에는 매개변수의 목적에 대한 설명이 포함되어 있습니다. 인수 파일을 수정하고 저장하면 명령줄 매개변수 값을 설치에 필요한 대로 변경할 수 있습니다.

설치 프로그램과 함께 인수 파일을 사용하려면 다음 명령을 입력하여 `--arguments` 명령줄 옵션을 사용하십시오.

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

예:

```
Milestone XProtect VMS Products 2023 R3 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

명령줄 옵션

명령줄 셸에서는 설치 프로그램와 명령줄 옵션을 결합할 수도 있습니다. 명령줄 옵션으로는 일반적으로 명령에 대한 행동을 수정할 수 있습니다.

명령줄 옵션의 전체 목록을 보려면 명령줄 셸에서 설치 프로그램이 위치한 디렉토리로 이동하여 `[NameOfExeFile].exe --help` 를 입력합니다. 성공적으로 설치를 하려면 반드시 값이 필요한 명령줄 옵션에 대한 값을 지정해야 합니다.

명령줄 매개변수와 명령줄 옵션을 동일한 명령에 동시에 사용할 수 있습니다. `--parameters` 명령줄 옵션을 사용하고 각 명령줄 매개변수를 콜론(:)으로 나눕니다. 아래의 예시에서 `--quiet` 과 `--showconsole`, `--parameters` 는 명령줄 옵션이며 `ISFAILOVER` 와 `RECORDERNAME` 은 명령줄 매개변수입니다.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

레코딩 서버 자동 설치

자동 설치를 한 경우 설치 완료 시 알림을 받지 않게 됩니다. 알림을 받으려면 `--showconsole` 명령줄 옵션을 명령에 추가합니다. 설치가 완료되면 Milestone XProtect Recording Server 트레이 아이콘이 표시됩니다.

아래 명령 예시에서 각진 브래킷([ ]) 안의 텍스트와 각진 브래킷은 반드시 실제 값으로 대체되어야 합니다. 예시: "[path]" 대신에 `d:\program files\`나 `d:\record\`, `\\network-storage-02\surveillance`를 입력합니다. `--help` 명령줄 옵션을 사용하면 각 명령줄 옵션 값에 대한 법적 형식에 관해 읽을 수 있습니다.

1. Recording Server 구성 요소를 설치하고자 하는 컴퓨터에 로그인합니다.
2. 인터넷 브라우저를 열고 관리자를 대상으로 하는 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.

   주소는보통`http://[management server address]:[port]/installation/Admin/default-en-US.htm`입니다.
3. **Recording Server 설치 프로그램** 아래에서 **모든 언어** 를 선택하여 레코딩 서버 설치 프로그램를 다운로드합니다.
4. 선호하는 명령줄 셸을 엽니다. Windows 명령줄 프롬프트를 열려면 Windows 시작 메뉴를 열고 **cmd** 를 입력합니다.
5. 다운로드한 설치 프로그램이 있는 디렉토리로 이동합니다.
6. 아래 두 시나리오 중 하나를 따라 계속해서 설치하십시오:

시나리오 1: 기존 설치를 업그레이드하거나 기본 값으로 Management Server 구성 요소와 함께 서버에서 설치

- 다음 명령을 입력하면 설치가 시작됩니다.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

시나리오 2: 분산 시스템 설치

1. 다음 명령을 입력하여 임의 파일을 명령줄 매개변수와 함께 생성합니다.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. 특정 경로에서 인수 파일(Arguments.xml)을 열고 필요한 경우 명령줄 매개변수를 수정합니다.

> 명령줄 매개 변수에 SERVERHOSTNAME과 SERVERPORT 유효값을 입력해야 합니다. 아니라면 설치를 완료할 수 없습니다.

4. 인수 파일을 저장합니다.
5. 명령줄 셸로 돌아와 아래의 명령을 입력하여 인수 파일에 지정된 명령줄 매개변수 값과 함께 설치합니다.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

XProtect Smart Client 자동 설치

자동 설치를 한 경우 설치 완료 시 알림을 받지 않게 됩니다. 알림을 받으려면 `--showconsole` 명령줄 옵션을 명령에 추가합니다. 설치가 완료되면 데스크톱에 XProtect Smart Client 바로가기가 표시됩니다.

아래 명령 예시에서 각진 브래킷([ ]) 안의 텍스트와 각진 브래킷은 반드시 실제 값으로 대체되어야 합니다. 예시: "[path]" 대신에 `d:\program files\`나 `d:\record\`, `\\network-storage-02\surveillance`를 입력합니다. `--help` 명령줄 옵션을 사용하면 각 명령줄 옵션 값에 대한 법적 형식에 관해 읽을 수 있습니다.

1. 인터넷 브라우저를 열고 최종 사용자를 대상으로 하는 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.

   주소는 보통 `http://[management server address]:[port]/installation/default-en-US.htm` 입니다.

2. **XProtect Smart Client 설치 프로그램** 아래에서 **모든 언어** 를 선택하여 XProtect Smart Client 설치 프로그램를 다운로드합니다.
3. 선호하는 명령줄 셸을 엽니다. Windows 명령줄 프롬프트를 열려면 Windows 시작 메뉴를 열고 **cmd** 를 입력합니다.
4. 다운로드한 설치 프로그램이 있는 디렉토리로 이동합니다.
5. 아래 두 시나리오 중 하나를 따라 계속해서 설치하십시오:

시나리오 1: 기존 설치를 업그레이드하거나 기본 명령줄 매개변수 값으로 설치

- 다음 명령을 입력하면 설치가 시작됩니다.

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet
```

시나리오 2: xml 인수 파일을 입력으로 사용하여 사용자 정의 명령줄 매개변수 값과 함께 설치

1. 다음 명령을 입력하여 임의 xml 파일을 명령줄 매개변수와 함께 생성합니다.

```
"XProtect Smart Client 2023 R3 Installer.exe" --generateargsfile=
[path]
```

2. 특정 경로에서 인수 파일(Arguments.xml)을 열고 필요한 경우 명령줄 매개변수를 수정합니다.
3. 인수 파일을 저장합니다.
4. 명령줄 셸로 돌아와 아래의 명령을 입력하여 인수 파일에 지정된 명령줄 매개변수 값과 함께 설치합니다.

```
"XProtect Smart Client 2023 R3 Installer.exe" --quiet --arguments=
[path]\[filename]
```

로그 서버 자동 설치

자동 설치를 한 경우 설치 완료 시 알림을 받지 않게 됩니다. 알림을 받으려면 `--showconsole` 명령줄 옵션을 명령에 추가합니다.

아래 명령 예시에서 각진 브래킷([ ]) 안의 텍스트와 각진 브래킷은 반드시 실제 값으로 대체되어야 합니다. 예시: "[path]" 대신에 `d:\program files\`나 `d:\record\`, `\\network-storage-02\surveillance`를 입력합니다. `--help` 명령줄 옵션을 사용하면 각 명령줄 옵션 값에 대한 법적 형식에 관해 읽을 수 있습니다.

1. Log Server 구성 요소를 설치하고자 하는 컴퓨터에 로그인합니다.
2. 인터넷 브라우저를 열고 관리자를 대상으로 하는 Management Server 의 다운로드 웹 페이지 주소를 주소 필드에 입력한 후 엔터를 누릅니다.

   주소는보통`http://[management server address]:[port]/installation/Admin/default-en-US.htm`입니다.
3. **Log Server 설치 프로그램** 아래에서 **모든 언어** 를 선택하여 로그 서버 설치 프로그램를 다운로드합니다.
4. 선호하는 명령줄 셸을 엽니다. Windows 명령줄 프롬프트를 열려면 Windows 시작 메뉴를 열고 **cmd** 를 입력합니다.
5. 다운로드한 설치 프로그램이 있는 디렉토리로 이동합니다.
6. 아래 두 시나리오 중 하나를 따라 계속해서 설치하십시오:

시나리오 1: 기존 설치를 업그레이드하거나 기본 명령줄 매개변수 값으로 설치

- 다음 명령을 입력하면 설치가 시작됩니다.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --showconsole
```

시나리오 2: XML 인수 파일을 입력으로 사용하여 사용자 정의 명령줄 매개변수 값과 함께 설치

1. 다음 명령을 입력하여 임의 xml 파일을 명령줄 매개변수와 함께 생성합니다.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --generateargsfile=
[path]
```

2. 특정 경로에서 인수 파일(Arguments.xml)을 열고 필요한 경우 명령줄 매개변수를 수정합니다.
3. 인수 파일을 저장합니다.
4. 명령줄 셸로 돌아와 아래의 명령을 입력하여 인수 파일에 지정된 명령줄 매개변수 값과 함께 설치합니다.

```
"XProtect Log Server 2023 R3 Installer x64.exe" --quiet --arguments=
[path]\[filename] --showconsole
```

전용 서비스 계정을 사용하여 자동으로 설치

XProtect VMS을(를) 자동으로 설치하려면 아래 표에 있는 인수를 사용하여 설치 프로그램을 시작해야 합니다. 인수는 설치하기 전에 생성한 인수 XML 파일에 생성되고 저장되어야 합니다.

인수	설명
--quiet	자동 설치를 강제 실행합니다.
--arguments	전체 구성이 포함된 인수 XML 파일의 경로입니다. 경로는 다음일 수 있습니다. C:\Arguments.xml
--license	라이선스 파일의 경로입니다.

전용 서비스 계정 사용

이 설명은 통합 보안을 위해 전용 서비스 계정을 사용하는 것을 기준으로 합니다. 어느 사용자가 로그인하든 서비스는 항상 전용 계정에서 실행되며, 해당 계정에 작업을 수행하고 네트워크, 파일, 공유 폴더에 액세스하는 데 필요한 모든 권한이 있는지 확인해야 합니다.

다음 키에 대한 인수 XML 파일에 서비스 계정을 지정해야 합니다.

SERVICEACCOUNT
SERVICEACCOUNT_NONLOC

다음 키에 대한 값에 서비스 계정의 암호를 일반 텍스트로 지정해야 합니다.

ENCRYPTEDPASSWORD

예: 자동 모드로 설치를 시작하는 명령줄:

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

예: 전용 서비스 계정 사용을 기준으로 하는 인수 파일

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
```

```
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
```

```
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

설치하기 전에 완료해야 할 사전 요구 사항:

- 서비스 계정과 설치에 사용할 계정을 생성해야 합니다.
- 서비스 계정은 설치하는 컴퓨터에서 서비스로 로그인할 수 있도록 허용되어야 합니다. Log-on-as-a-service를 참조하십시오.
- XProtect에서 사용할 데이터베이스를 생성해야 하며, 해당 데이터베이스의 이름을 인수 XML 파일에 다음과 같이 지정해야 합니다.

데이터베이스 이름
감시
Surveillance_IDP
Surveillance_IM
Surveillance_LogServerV2

- 다음 목록에 따라 데이터베이스를 구성해야 합니다.

데이터베이스 구성
기본 조합은 'SQL_Latin1_General_CP1_CI_AS'로 설정해야 합니다.
ALLOW_SNAPSHOT_ISOLATION은(는) ON으로 설정해야 합니다.
READ_COMMITTED_SNAPSHOT은(는) ON으로 설정해야 합니다.

- 서비스 계정과 각 데이터베이스에서 설치를 수행하는 데 사용되는 계정에 대해 SQL 서버 로그인을 생성해야 합니다. 각 데이터베이스에 데이터베이스 사용자를 생성해야 하며, 해당 사용자는 각 데이터베이스에서 db_owner 역할의 구성원이어야 합니다.

작업 그룹에 대한 설치

ActiveDirectory서버로도메인설정을사용하지않지만워크그룹설정을사용하는경우,설치시다음설치방법을따르십시오.

배포 설정 내 모든 컴퓨터는 도메인 또는 워크 그룹에 있어야 합니다.

1. 일반 관리자 계정을 사용하여 Windows에 로그인합니다.

   시스템에 있는 모든 컴퓨터에서 동일한 계정을 사용해야 합니다.

2. **필요에 따라 관리 또는 레코딩 서버 설치를 시작하고** 사용자 정의를 클릭합니다.
3. 2단계에서 선택한 항목에 따라, 일반 관리자 계정을 사용하여 Management Server 또는 Recording Server 서비스 중에 설치할 것을 선택합니다.
4. 설치를 완료합니다.
5. 1-4단계를 반복하여 연결할 다른 모든 시스템을 설치합니다. 해당 시스템 모두 일반 관리자 계정을 사용하여 설치해야 합니다.

클러스터 내 설치

클러스터에 설치하기 전 페이지 122의 다중 관리 서버 정보(클러스터링)(설명됨) 페이지 122의 클러스터링 요구 사항및를 참조하십시오.

화면에서 보는 것과 설명 및 일러스트레이션이 다를 수도 있습니다.

관리 서버 설치:

1. 클러스터 내 첫 서버상의 관리 서버 및 모든 하위 구성 요소를 설치합니다.

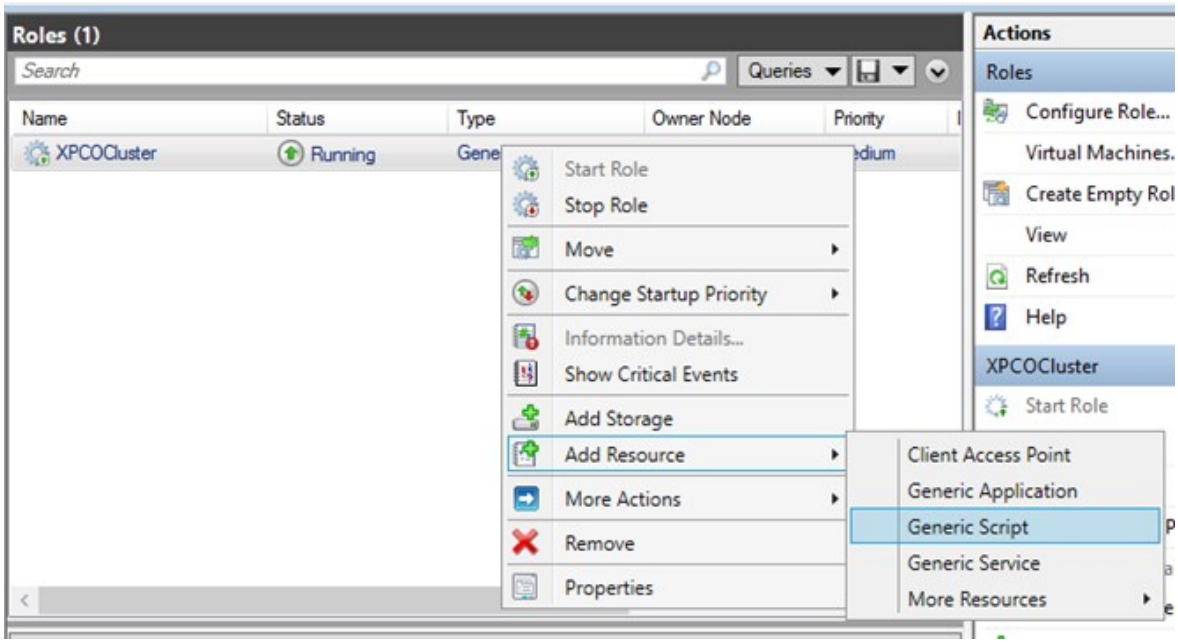
   관리 서버는 반드시 네트워크 서비스 가 아닌 지정 사용자를 통해 설치해야 합니다. 이를 위해서 **사용자 정의** 설치 옵션을 사용해야 합니다. 또한 지정 사용자는 반드시 공유 네트워크 드라이브 및 되도록이면 유효기간이 없는 암호에 접근할 수 있어야 합니다.

장애 조치 클러스터 내 일반 서비스로 Management Server 서비스 구성하기:

1. 관리 서버를 설치한 마지막 서버상에서 **시작** > **관리도구** 로 이동 후, Windows의 **장애 조치 클러스터 관리** 를 엽니다. **장애 조치 클러스터 관리** 창에서 클러스터를 확장하고 **역할**을 우클릭한 후, **역할 구성**을 선택합니다.

2. **고가용성 마법사** > **시작하기 전에**에 페이지에서 **다음**을 클릭합니다.
3. **역할 선택** 페이지에서 **일반 서비스**를 선택하고 **다음**을 클릭합니다.
4. **서비스 선택** 페이지에서 **Milestone XProtect Management Server** 서비스를 선택하고 **다음**을 클릭합니다.
5. **클라이언트 액세스 포인트** 페이지에서 서비스에 접속할 때 클라이언트가 사용할 이름(해당 클러스터의 호스트 이름)을 지정합니다. 호스트 이름은 클러스터 이름과 달라야 합니다. **다음** 을 클릭합니다.
6. **저장소 선택** 페이지에서 서비스에 저장소가 필요하지 않으므로 **다음**을 클릭합니다.
7. **레지스트리 설정 복제** 페이지에서 복제할 레지스트리 설정이 없으므로 **다음**을 클릭합니다.
8. **확인 페이지**에서 클러스터 서비스가 요구 사항에 따라 구성되었는지 확인한 후 **다음**을 클릭합니다.
9. **고가용성 구성** 페이지에서 **다음**을 클릭합니다.
10. **요약 페이지**에서 **완료**를 클릭하여 장애 조치 클러스터에서 일반 서비스로 관리 서버의 구성을 완료합니다.

11. 방금 생성한 역할을 마우스 오른쪽 버튼으로 클릭하고 **리소스 추가** > **일반 스크립트**를 클릭합니다. **Milestone XProtect Event Server** 서비스를 리소스로 **Milestone XProtect Event Server** 서비스에 추가하려면 Milestone XProtect Management Server Cluster을(를) 선택합니다.



12. 11단계를 반복하고 클러스터에서 필요한 모든 서비스, 예를 들어 Log Server을(를) 추가합니다. Milestone XProtect Event Server 및 Data Collector server은(는) 모두 최적의 배포를 달성하기 위해 서비스로 추가되어야 합니다. 또한, Milestone XProtect Event Server은(는) 관리 서버의 종속 서비스로 설정되어야 관리 서버가 중단되었을 때 이벤트 서버가 중단되지 않습니다.

13. 추가된 모든 서비스가 창의 하단 창에 표시됩니다.

클러스터 URL 업데이트:

구성 변경 시, Microsoft 장애 조치 클러스터 관리자에서, 서비스 제어 및 모니터링을 중단하여 Server Configurator 이(가) 변경 후 Management Server 서비스를 시작 및/또는 중지할 수 있게 해줍니다. 장애 조치 클러스터 서비스 시작 유형을 수동으로 변경한 경우, Server Configurator 와(과) 아무런 충돌이 일어나지 않게 됩니다.

Management Server 컴퓨터에서:

1. 관리 서버사 설치된 각 컴퓨터에서 Server Configurator 을(를) 시작합니다.
2. **등록** 페이지로 이동합니다.
3. 연필( ) 기호를 클릭하여 관리 서버 주소를 편집할 수 있도록 합니다.
4. 관리 서버 주소를 클러스터 URL로 변경합니다(예: `http://MyCluster`).
5. **등록** 을 클릭합니다.

Management Server을(를) 사용하는 구성 요소가 포함된 컴퓨터에서(예: Recording Server, Mobile Server, Event Server, API Gateway):

1. 각 컴퓨터에서 Server Configurator 을(를) 시작합니다.
2. **등록** 페이지로 이동합니다.
3. 관리 서버 주소를 클러스터 URL로 변경합니다(예: `http://MyCluster`).
4. **등록** 을 클릭합니다.

클러스터 환경에서 외부 IDP를 위한 인증서 사용

단일 서버 환경에서 XProtect을(를) 설치할 때 외부 IDP 구성 데이터는 데이터 보호 API(DPAPI)를 사용하여 보호됩니다. 클러스터에 관리 서버를 설정하는 경우, 원활하게 노드 장애 조치를 하려면 외부 IDP 구성 데이터를 인증서로 보호해야 합니다.

인증서 생성에 관한 자세한 정보는 인증서에 관한 Milestone 지침 을(를) 참조하십시오.

인증서를 개인 인증서 보관함에 가져오기한 후 컴퓨터가 해당 인증서를 신뢰하도록 해야 합니다.

데이터 보호를 설정하려면 Identity Provider 구성에 인증서 지문을 추가해야 합니다.

1. 인증서를 개인 인증서 보관함에 가져오기한 후 다음 사항을 확인합니다.
   - 인증서가 유효한지 여부
   - Identity Provider app pool (IDP) 계정이 인증서 개인 키에 대한 권한을 보유했는지 여부

   해당 계정이 인증서 개인 키에 대한 권한을 가졌는지에 대한 여부를 확인하기 위한 자세한 정보는 인증서에 관한 Milestone 지침 을(를) 참조하십시오.
2. Identity Provider의 설치 경로(`[설치 경로]\Milestone\XProtect Management Server\IIS\Identity Provider`)에서 `appsettings.json` 파일을 찾습니다.
3. 다음 섹션에서 인증서 지문을 설정합니다.

```
"DataProtectionSettings": {
 "ProtectKeysWithCertificate": {
  "Thumbprint": ""
 }

},
```

4. 모든 관리 서버 노드에서 3단계를 반복합니다.
5. 노드 장애 조치를 시행하여 인증서 설정이 올바른지 확인하십시오.
6. 관리 클라이언트를 사용하여 다시 로그인하고 외부 공급자 구성을 적용합니다. 구성이 이미 적용된 경우 관리 클라이언트의 외부 IDP에서 클라이언트 암호를 다시 입력해야 합니다.

외부 IDP 구성이 인증서로 보호되는 상황에서 문제 해결

유효하지 않은 인증서/유효 기간이 만료된 인증서

구성된 지문 인증서가 신뢰되지 않거나 유효 기간이 만료된 인증서를 나타내는 경우, Identity Provider 을(를) 시작할 수 없습니다. Identity Provider 로그(`C:\ProgramDataIdentity Provider\Milestone\ \Logs\Idp.log`)는 인증서의 유효성 여부를 분명하게 보여줍니다.

해결책:

인증서가 컴퓨터에서 유효하며 신뢰받은 것인지 확인하십시오.

인증서 개인 키에 대한 권한 없음

Identity Provider 은(는) 개인 키에 대한 권한 없이 데이터를 보호할 수 없습니다. Identity Provider에 권한이 없는 경우, 다음의 오류 메시지가 Identity Provider 로그 파일(`C:\ProgramData\Milestone\Identity Provider\Logs\Idp.log`)에 기록됩니다.

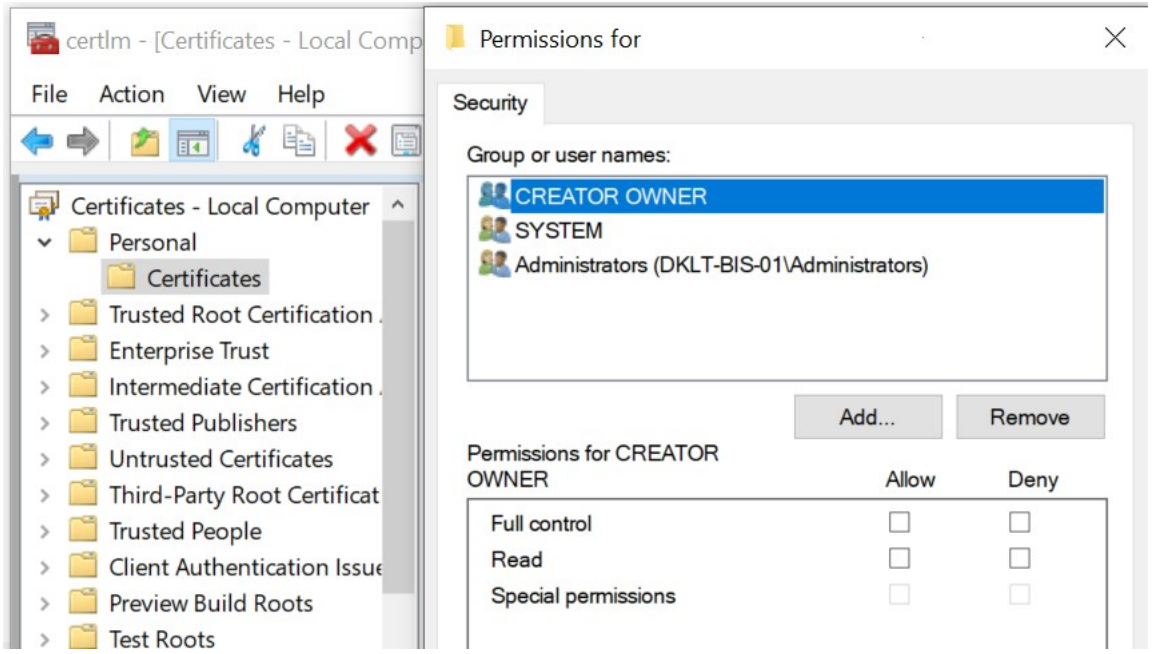
```
ERROR- An exception occurred while processing the key element '<key id="
[installation specific]" version="1" />'.
Internal.Cryptography.CryptoThrowHelper+WindowsCryptographicException:
Keyset does not exist
```

해결책:

Identity Provider app pool (IDP) 계정이 인증서 개인 키에 대한 권한을 보유했는지 여부를 확인합니다.

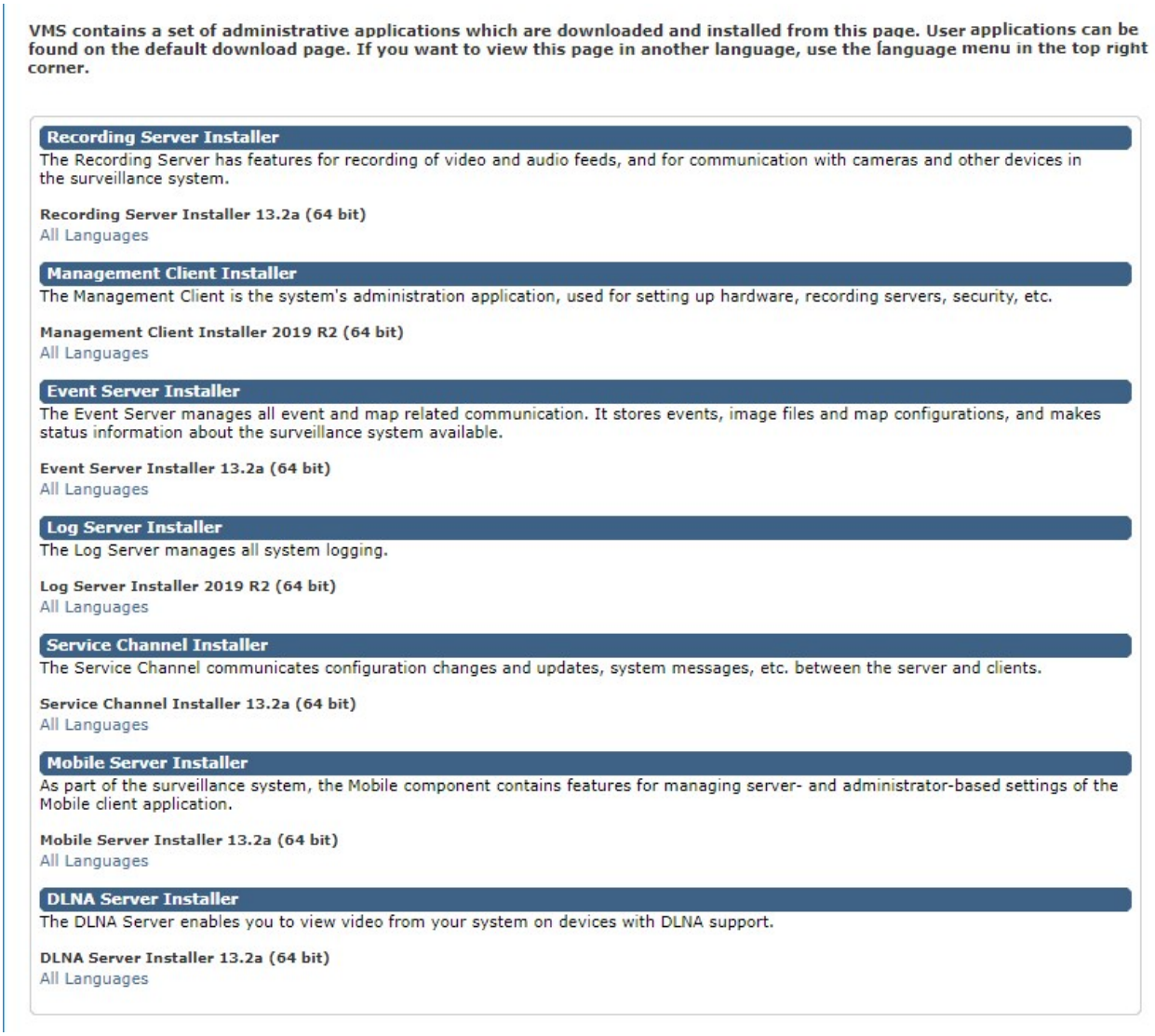
인증서 개인 키에 대한 권한을 다음과 같이 확인합니다.

1. Windows 작업 표시줄에서 **시작** 을 선택한 후 컴퓨터 인증서 도구 관리(certlm.msc)를 엽니다.
2. 개인 인증서 보관함으로 이동한 후 암호화에 사용할 인증서를 찾습니다.
3. 인증서 위에서 마우스 오른쪽 버튼을 클릭하고 **모든 작업** > **개인 키 관리** 를 선택합니다.
4. **다음에 대한 권한** 아래에서, Identity Provider app pool (IDP) 계정이 읽기 권한을 갖고 있는지 확인합니다.



Download Manager/다운로드 웹 페이지

관리 서버에는 웹 페이지가 내장되어 있습니다. 이 웹 페이지를 통해 관리자와 최종 사용자는 로컬 또는 원격 등 어떤 위치에서든 필요한 XProtect 시스템 구성 요소를 다운로드하여 설치할 수 있습니다.



웹 페이지에는 두 세트의 콘텐츠가 표시될 수 있으며, 기본적으로 두 가지 모두 시스템 설치 언어와 일치하는 언어 버전으로 나옵니다.

- 한 웹 페이지는 **관리자** 를 대상으로 한 것으로, 주요 시스템 구성 요소를 다운로드하여 설치할 수 있습니다. 대부분의 경우 이 웹 페이지는 관리 서버 설치가 끝날 때 자동으로 로드되어 기본 내용이 표시됩니다. 관리 서버에서, Windows의 **시작** 메뉴로부터 **프로그램** > **Milestone** > **관리 설치 페이지** 를 선택하여 웹 페이지에 액세스할 수 있습니다. 그렇지 않으면 URL을 입력할 수 있습니다:

  http://[관리 서버 주소]:[port]/installation/admin/

  여기서, [관리 서버 주소]는 관리 서버의 IP 주소 또는 호스트 이름이며, [포트]는 관리 서버에서 사용하도록 IIS를 구성한 포트 번호에 해당합니다.

- 한 웹 페이지는 최종 **사용자** 를 대상으로 한 것으로, 기본 구성을 사용하여 클라이언트 응용 프로그램에 대한 액세스를 제공합니다. 관리 서버에서 Windows의 **시작** 메뉴로부터 **프로그램** > **Milestone** > **공용 설치 페이지** 를 선택하여 웹 페이지에 액세스할 수 있습니다. 그렇지 않으면 URL을 입력할 수 있습니다:

  http://[관리 서버 주소]:[port]/installation/

  여기서, [관리 서버 주소]는 관리 서버의 IP 주소 또는 호스트 이름이며, [포트]는 관리 서버에서 사용하도록 IIS를 구성한 포트 번호에 해당합니다.

두 웹 페이지에는 설치 후 바로 사용할 수 있도록 몇 가지 기본적인 내용이 포함됩니다. 그러나 관리자의 경우 Download Manager 을(를) 사용하여 웹 페이지에 표시되는 내용을 사용자 정의할 수 있습니다. 또한 두 웹 페이지 버전 간에 구성 요소를 이동할 수 있습니다. 구성 요소를 이동하려면 마우스 오른쪽 단추로 클릭하고 구성 요소를 이동할 웹 페이지 버전을 선택합니다.

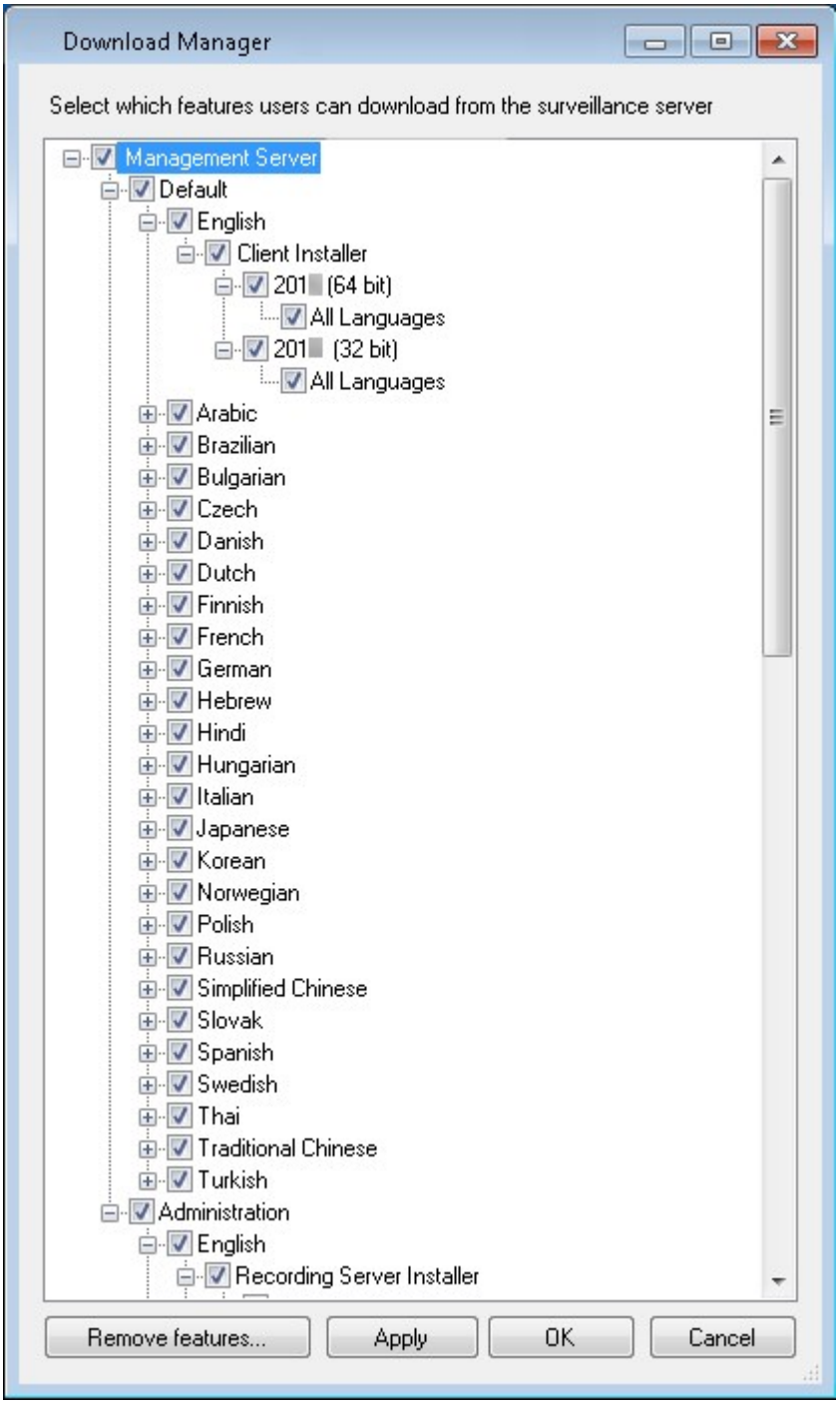
Download Manager 에서 사용자가 다운로드하여 설치할 수 있는 구성 요소를 제어할 수 있는 경우라도 사용자의 권한 관리 도구로 사용할 수는 없습니다. 그러한 권한은 Management Client 에서 정의된 역할에 의해 결정됩니다.

관리 서버에서 Windows의 **시작** 메뉴로부터 **프로그램** > **XProtect Download Manager** > **Milestone** 를 선택하여 XProtect Download Manager 에 액세스할 수 있습니다.

Download Manager의 기본 구성

DownloadManager에는기본구성이있습니다.이를통해조직의사용자가처음부터표준구성요소에액세스할수있습니다.

기본 구성은 추가 또는 선택적 구성 요소를 다운로드하기 위한 액세스 권한과 함께 기본 설치를 제공합니다. 일반적으로 관리 서버 컴퓨터에서 웹 페이지에 액세스하지만 다른 컴퓨터에서 웹 페이지에 액세스할 수도 있습니다.



- 첫 번째 수준: XProtect 제품을 지칭합니다.
- 두 번째 수준: 웹 페이지의 두 가지 대상 버전을 지칭합니다. **기본값** 은 최종 사용자가 확인한 웹 페이지 버전을 지칭합니다. **관리** 는 시스템 관리자가 확인한 웹 페이지 버전을 지칭합니다.
- 세 번째 수준: 웹 페이지를 사용할 수 있는 언어를 지칭합니다

- 네 번째 수준: 사용자에게 제공되거나 지정될 수 있는 구성 요소를 지칭합니다.
- 다섯 번째 수준: 사용자에게 제공되거나 지정될 수 있는 각 구성 요소의 특정 버전을 지칭합니다.
- 여섯 번째 수준: 사용자에게 제공되거나 지정될 수 있는 구성 요소의 언어 버전을 지칭합니다.

처음에 시스템 자체와 동일한 언어 버전으로 설정된 표준 구성 요소만 사용할 수 있다는 점은 설치 시간을 줄이고 서버 공간을 절약하는 데 도움이 됩니다. 아무도 사용하지 않는 경우에는 서버에 사용 가능한 구성 요소나 언어 버전이 필요하지 않습니다.

필요에 따라 추가 구성 요소 또는 언어를 제공할 수 있고, 원치 않는 구성 요소나 언어를 숨기거나 제거할 수 있습니다.

Download Manager의 표준 설치 관리자(사용자)

기본적으로 사용자 대상의 관리 서버 다운로드 웹 페이지에서 별도 설치에 대해 다음의 구성 요소를 사용할 수 있습니다(Download Manager 에 의해 제어).

- 장애 조치 레코딩 서버를 포함한 레코딩 서버. 장애 조치 레코딩 서버는 처음에 다운로드되어 레코딩 서버로 설치되며, 설치 절차 중 장애 조치 서버로 지정합니다.
- Management Client
- XProtect Smart Client
- 이벤트 서버, 맵 기능과 함께 사용
- 로그 서버, 시스템 정보 기록에 필요한 기능을 제공하는 데 사용
- XProtect Mobile 서버
- 조직에서 추가 옵션을 사용 가능할 수 있습니다.

장치 팩 설치에 대해서는 페이지 174의 장치 팩 설치 관리자 - 반드시 다운로드 필요를 참조하십시오.

Download Manager 설치 프로그램 구성 요소 추가/게시

두가지절차를완료하여비표준구성요소및신규버전을관리서버의다운로드페이지에서사용가능하도록설정해야합니다.

먼저 Download Manager 에 신규 및/또는 비표준 구성 요소를 추가합니다. 그런 다음 웹 페이지의 여러 언어 버전에서 사용할 구성 요소를 정밀하게 조정합니다.

Download Manager 이(가) 열려 있는 경우, 새 구성 요소를 설치하기 전에 닫으십시오.

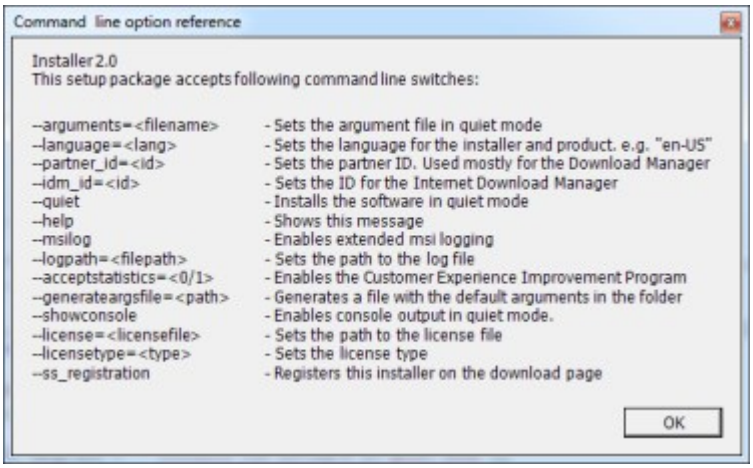
Download Manager 에 신규/비표준 파일 추가:

1. 구성 요소를 다운로드한 컴퓨터에서 Windows의 **시작** 으로 이동하고 *명령 프롬프트* 에 들어갑니다
2. *명령 프롬프트*에서 다음을 포함한 파일 이름(*.exe*)을 실행합니다:[space]*--ss_registration*

   예: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   이제 파일이 Download Manager 에 추가되지만 현재 컴퓨터에 설치되지는 않습니다.

설치 프로그램 명령에 대한 개요를 보려면 *명령 프롬프트* 에, *[space]--help* 를 입력할 때 다음 창이 나타납니다:



새 구성 요소를 설치했으면 기본적으로 Download Manager 에서 선택되어 있으며, 웹 페이지를 통해 즉시 사용자에게 제공할 수 있습니다. 언제든지 Download Manager의 트리 구조에서 확인란을 선택하거나 선택 취소하여 웹 페이지에서 기능을 표시하거나 숨길 수 있습니다.

웹 페이지에서 구성 요소가 표시되는 순서를 변경할 수 있습니다. Download Manager의 트리 구조에서 구성 요소 항목을 끌어서 필요한 위치에 놓습니다.

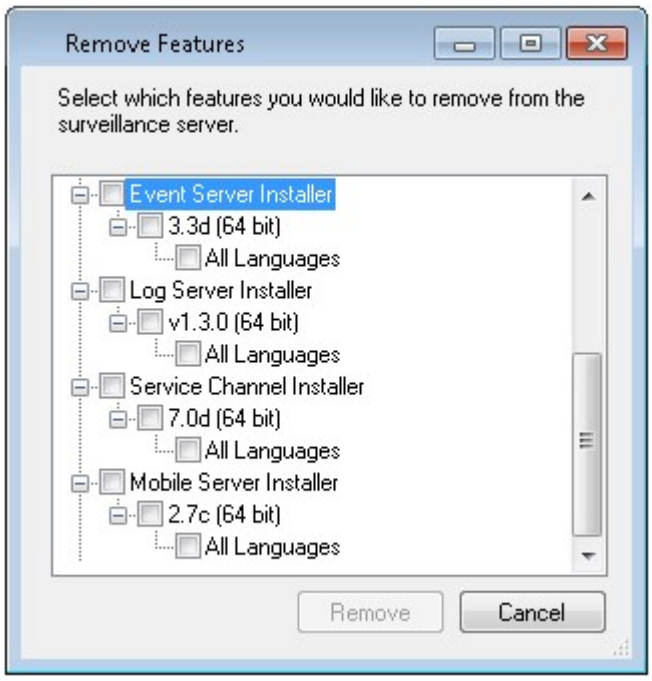
Download Manager 설치 프로그램 구성 요소 숨기기/제거

3가지 옵션이 있습니다:

- Download Manager 의 트리 구조에서 확인란의 선택을 취소하면 웹 페이지에서 **구성 요소** 가 숨겨집니다. 이 구성 요소는 관리 서버에 여전히 설치되어 있으며, Download Manager의 트리 구조에서 확인란을 선택하면 신속하게 구성 요소를 다시 사용할 수 있게 만들 수 있습니다

- 관리 서버에서 **구성 요소 설치를 제거** 합니다. 구성 요소가 Download Manager 에서 사라지지만 해당 구성 요소의 설치 파일은 `C:\Program Files (x86)\Milestone\XProtect Download Manager` 에 그대로 유지되므로, 필요 시 나중에 다시 설치할 수 있습니다

  1. Download Manager 에서 **기능 제거** 를 클릭합니다.
  2. **기능 제거** 창에서 제거할 기능을 선택합니다.



  3. **확인** 과 **예** 를 클릭합니다.

- 관리 서버에서 **필요하지 않은 기능의 설치 파일을 제거** 합니다. 사용자의 조직이 특정 기능을 사용하지 않을 경우, 이렇게 하면 서버의 디스크 공간을 절약할 수 있습니다

장치 팩 설치 관리자 - 반드시 다운로드 필요

원본 설치에 포함된 Device Pack(장치 팩)(장치 드라이버 포함)은 Download Manager 에 포함되지 않습니다. 따라서 Device Pack(장치 팩)을 다시 설치해야 하거나 Device Pack(장치 팩) 설치 관리자를 제공하려는 경우, 먼저 최신 Device Pack(장치 팩) 설치 관리자를 Download Manager 에 추가하거나 게시해야 합니다.

1. Milestone 웹사이트(https://www.milestonesys.com/downloads/)의 다운로드 페이지에서 최신 정기 장치팩을 받으십시오.
2. 동일한 페이지에서, 기존 드라이버를 가진 레거시 Device Pack(장치 팩)을 다운로드할 수 있습니다. 카메라가 레거시 장치 팩의 드라이브를 사용하는지 확인하려면 이 웹사이트 (https://www.milestonesys.com/community/business-partner-tools/device-packs/)로 이동하십시오.
3. *--ss_registration* 명령을 사용해 호출하여 해당 구성 요소를 Download Manager 에 추가/게시합니다.

네트워크에 연결되지 않은 경우, Download Manager 에서 전체 레코딩 서버를 다시 설치할 수 있습니다. 레코딩 서버의 설치 파일은 컴퓨터에 로컬로 위치하며, 이러한 방식으로 (장치 팩)의 재설치를 자동으로 가져올 수 있습니다.

설치 로그 파일 및 문제 해결

설치 또는 업그레이드, 삭제 중 로그 엔트리는 다양한 설치 로그 파일에 기록됩니다. 주 설치 로그 파일인 `installer.log` 과 귀하가 설치하는 다른 시스템 구성 요소에 속한 로그 파일에 기록됩니다. 모든 로그 엔트리에는 타임스탬프가 있으며 가장 최근의 로그인 엔트리는 로그 파일의 마지막에 표시됩니다.

사용자 는 모든 설치의 로그 파일을 `C:\ProgramData\Milestone\Installer\` 폴더에서 찾을 수 있습니다. *I.log 또는 *I[integer].log 로 명명된 로그 파일은 새로운 설치 또는 업그레이드에 관한 로그 파일입니다. 반면 *U.log 또는 *U[integer].log 로 명명된 파일은 프로그램 삭제 시 생성된 로그 파일입니다. XProtect 파트너를 통해 Milestone 시스템이 설치된 서버를 구매한 경우, 시스템 내에 설치 로그 파일이 없을 수도 있습니다.

로그 파일은 설치나 업그레이드, 삭제 중 사용된 명령줄 매개변수와 명령줄 옵션 및 해당 값에 관한 정보를 포함하고 있습니다. 로그 파일에 사용된 명령줄 매개변수를 찾으려면 로그 파일에 따라 **Command Line:** 또는 **Parameter '**를 검색합니다.

문제 해결을 하려면 주요 설치 로그 파일(installer.log)을 우선 확인해야 합니다. 설치하는 동안 예외나 오류, 경고가 있었다면 이 내용이 로그 파일에 기록되었을 것입니다. **exception** 나 **error**, **warning** 에 대한 검색을 시도해보십시오. "Exit code: 0"은 성공적으로 설치되었음을 의미하며 "Exit code: 1"은 설치에 실패했음을 의미합니다. 로그 파일에서 확인한 내용으로 Milestone 기술 자료 에서 해결책을 찾을 수도 있습니다. 아니라면 Milestone 파트너에 연락하여 관련 설치 로그 파일을 공유하십시오.

구성

초기 구성 작업 목록

아래 체크리스트는 시스템을 구성하는 초기 작업을 나열합니다. 일부는 설치 중에 이미 완료되었을 수 있습니다.

작성된 체크리스트는 그 자체가 시스템이 사용자 조직의 정확한 요구 사항과 부합함을 보증하지는 않습니다. 시스템이 조직의 요구와 일치하게 만들기 위해, Milestone 은 시스템을 지속적으로 모니터링하고 조정할 것을 권장합니다.

예를 들어, 시스템이 실행된 후 여러 물리적 조건(주간/야간, 바람이 부는 조용한 날씨 등) 하에 개별 카메라의 모션 감지 민감도 설정을 테스트하고 조정하는 것이 좋습니다.

비디오 레코딩 시기 등 시스템에서 수행되는 대부분의 동작을 결정하는 규칙 설정은 조직의 필요에 따라 변경할 수 있는 또 다른 구성의 예입니다.

단계	설명
☑	시스템 초기 설치를 마쳤습니다. 페이지 135의 신규 XProtect 시스템 설치를 참조하십시오.
☑	평가판 SLC를 영구 SLC로 변경합니다(필요한 경우). 페이지 113의 소프트웨어 라이선스 코드 변경를 참조하십시오.
☑	Management Client 에 로그인합니다. 페이지 29의 로그인(설명됨)를 참조하십시오.
☐	각 레코딩 서버의 저장소 설정이 요구에 맞는지 확인합니다. 페이지 53의 저장 및 아카이빙(설명)를 참조하십시오.
☐	각 레코딩 서버의 아카이브 설정이 필요를 충족하는지 확인합니다. 페이지 382의 저장소 및 녹화 설정 속성를 참조하십시오.
☐	각 레코딩 서버에 추가할 하드웨어, 카메라 또는 비디오 인코더를 검색합니다. 페이지 197의 하드웨어 추가를 참조하십시오.
☐	각 레코딩 서버의 개별 카메라를 구성합니다. 페이지 398의 카메라(장치 노드)를 참조하십시오.

단계	설명
☐	개별 카메라 또는 카메라 그룹에 대한 저장소와 아카이브를 활성화합니다. 이 작업은 개별 카메라 또는 장치 그룹에서 수행됩니다. 페이지 183의 저장소에 장치 또는 장치 그룹 연결를 참조하십시오.
☐	장치를 활성화하고 구성합니다. 페이지 396의 장치(장치 노드)를 참조하십시오.
☐	규칙은 넓은 범위에서 시스템 동작을 결정합니다. 사용자는 예를 들어 카메라가 레코딩되어야 할 시기, PTZ(이동/기울기/줌) 카메라가 순찰해야 하는 시기 및 알림이 전송되어야 하는 시기를 정의하는 규칙을 생성합니다. 규칙을 생성합니다. 페이지 72의 규칙 및 이벤트(설명됨)를 참조하십시오.
☐	시스템에 역할을 추가합니다. 페이지 64의 역할 및 역할의 권한(설명됨)를 참조하십시오.
☐	사용자 또는 사용자 그룹을 각 역할에 추가합니다. 페이지 265의 역할에 사용자 및 그룹 할당/제거를 참조하십시오.
☐	라이선스를 활성화합니다. 페이지 112의 온라인으로 라이선스 활성화 또는 페이지 112의 오프라인으로 라이선스 활성화를 참조하십시오.

사이트 탐색 창에서시스템을 구성하는 방법에 관한 자세한 정보는, 페이지 352의 사이트 탐색 창를 참조하십시오.

레코딩 서버

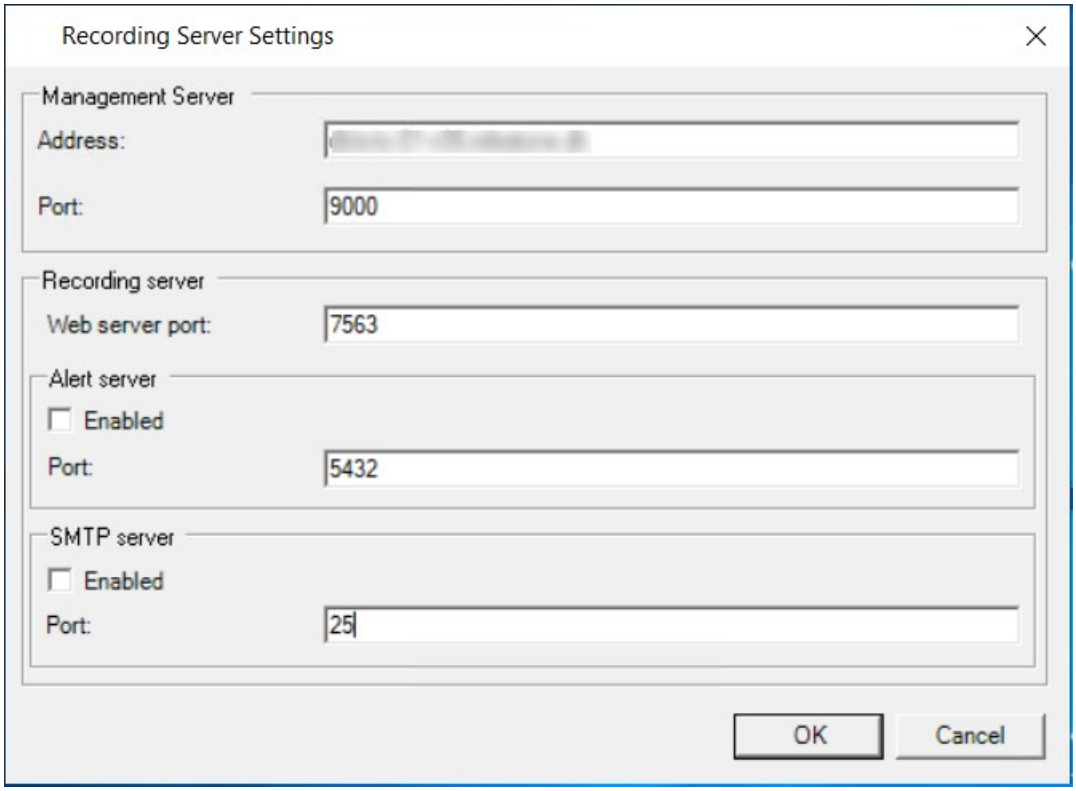
레코딩 서버의 기본 구성 변경 또는 확인

Management Client 에 설치한 모든 레코딩 서버가 나열되지 않는 경우, 가장 흔한 이유는 설치 중 설치 매개변수(예: 관리 서버의 IP 주소나 호스트 이름)를 잘못 구성했기 때문입니다.

관리 서버의 매개변수를 지정하기 위해 레코딩 서버를 다시 설치할 필요는 없으며, 기본 구성을 변경/확인할 수 있습니다:

1. 레코딩 서버를 실행하는 컴퓨터의 알림 영역에서 **레코딩 서버** 아이콘을 마우스 오른쪽 단추로 클릭합니다.
2. **Recording Server 서비스 중지** 를 선택하십시오.
3. **레코딩 서버** 아이콘을 마우스 오른쪽 단추로 다시 클릭하고 **설정 변경** 을 선택합니다.

   레코딩 서버 설정 창이 나타납니다.



4. 예를 들어 다음과 같은 설정을 확인하거나 변경합니다.
   - **관리 서버**: **주소**: 레코딩 서버가 연결되어야 하는 관리 서버의 IP 주소 또는 호스트 이름을 지정합니다.
   - **관리 서버**: **포트**: 관리 서버와 통신할 때 사용되는 포트 번호를 지정합니다. 필요한 경우 포트 번호를 변경할 수 있지만, 포트 번호는 관리 서버의 포트 번호 설정과 항상 일치해야 합니다. 페이지 89의 시스템에서 사용되는 포트를 참조하십시오.
   - **레코딩 서버**: **웹 서버 포트**: 레코딩 서버의 웹 서버와 통신 시 사용하는 포트 번호를 지정합니다. 페이지 89의 시스템에서 사용되는 포트를 참조하십시오.
   - **레코딩 서버**: **알림 서버 포트**: 레코딩 서버의 알림 서버와 통신하는 데 사용하는 포트 번호를 활성화하고 지정합니다. 알림 서버는 장치에서 이벤트 메시지를 수신합니다. 페이지 89의 시스템에서 사용되는 포트를 참조하십시오.
   - **SMTP 서버**: **포트**: 레코딩 서버의 SMTP(Simple Mail Transfer Protocol) 서비스와 통신하는 데 사용하는 포트 번호를 활성화하고 지정합니다. 페이지 89의 시스템에서 사용되는 포트를 참조하십시오.
5. **확인** 을 클릭합니다.

6. Recording Server 서비스를 다시 시작하려면 **레코딩 서버** 아이콘을 마우스 오른쪽 버튼으로 클릭하고, **Recording Server 서비스 시작** 을 선택합니다.

> Recording Server 서비스를 중지하면 레코딩 서버의 기본 구성을 확인/변경하는 동안 라이브 비디오를 레코딩하거나 볼 수 없습니다.

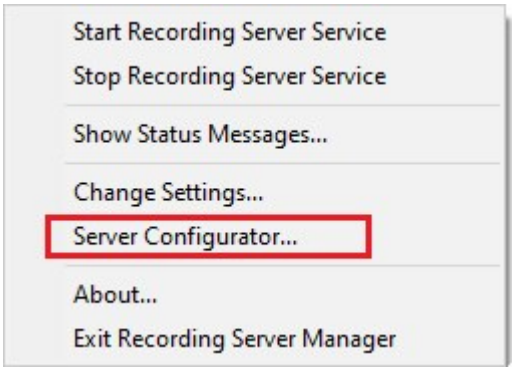
레코딩 서버 등록

레코딩 서버를 설치할 때 대부분의 경우 자동으로 인증됩니다. 그러나 다음의 경우 수동으로 등록을 해야 합니다:

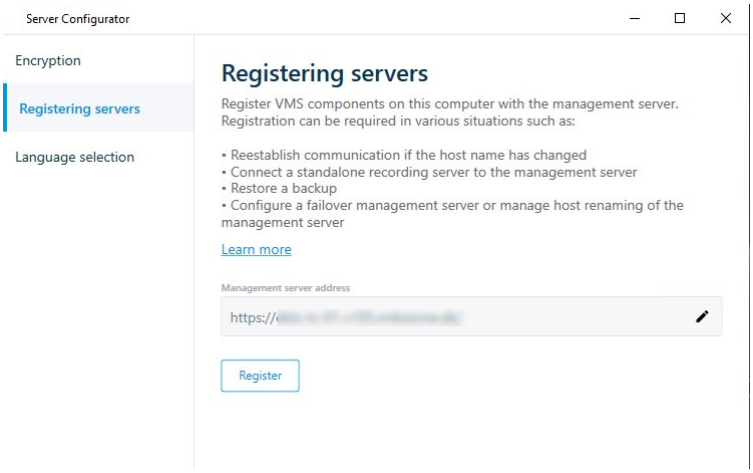
- 레코딩 서버를 교체했습니다.
- 오프라인 상태에서 레코딩 서버가 설치되었으며 후에 관리 서버가 추가되었습니다.
- 관리 서버가 기본 포트를 사용하고 있지 않습니다. 포트 번호는 암호화 구성을 따릅니다. 자세한 정보는 페이지 89의 시스템에서 사용되는 포트를 참조하십시오.
- 자동 등록에 실패했습니다(예: 관리 서버 주소를 변경한 후나 레코딩 서버가 있는 컴퓨터의 이름을 변경한 후 또는 서버 통신 암호화 설정을 활성화 또는 비활성화한 후). 관리 서버 주소 변경에 관한 자세한 정보는 관리 서버 컴퓨터의 호스트 이름 변경 을 참조하십시오.

레코딩 서버를 등록할 때 관리 서버에 연결하도록 구성합니다. 등록을 취급하는 관리 서버의 구성 요소는 Authorization Server 서비스입니다.

1. Windows 시작 메뉴 또는 레코딩 서버 트레이 아이콘 중 하나에서 Server Configurator 을(를) 엽니다.



2. Server Configurator 에서 **서버 등록** 을 선택합니다.



3. 컴퓨터상의 서버에 연결하고자 하는 관리 서버의 주소 및 구성(http 또는 https)을 확인하고 **등록** 을 클릭합니다.

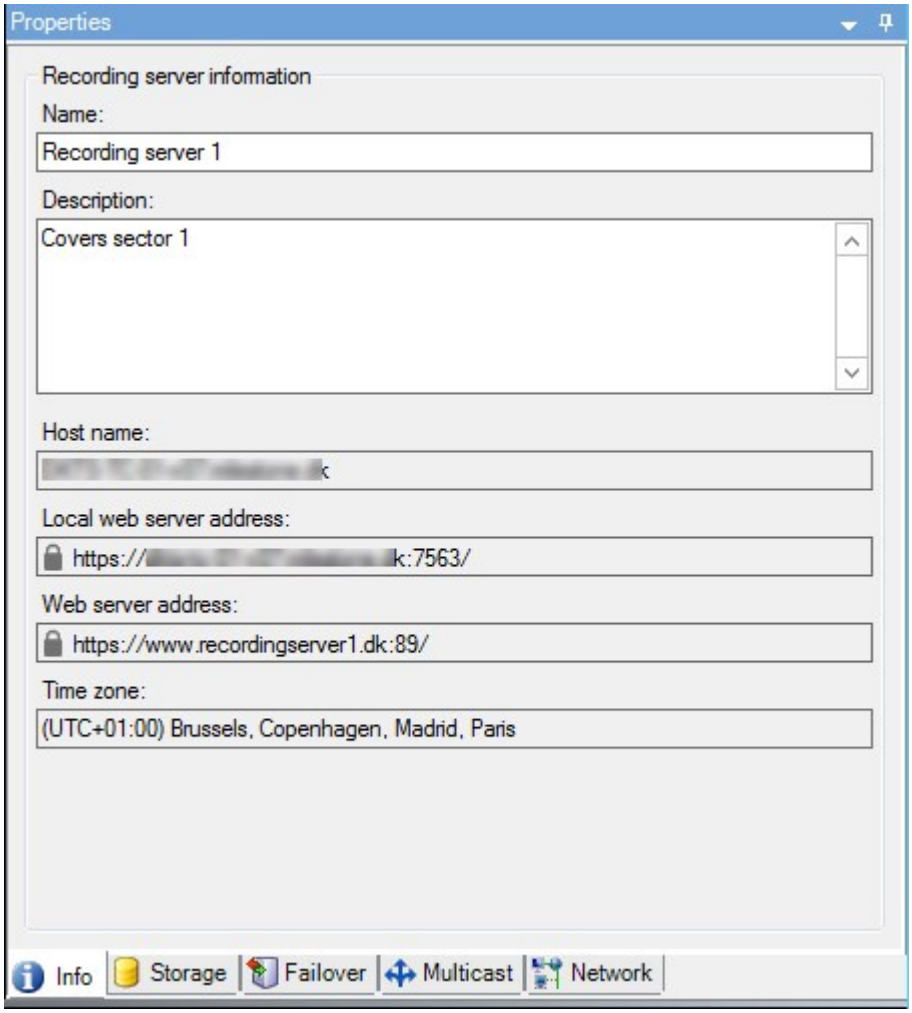
관리 서버상 등록에 성공했음을 알리는 확인창이 나타납니다.

또한 페이지 313의 레코딩 서버 교체를 참조하십시오.

클라이언트에 대한 암호화 상태 보기

레코딩 서버 암호화 연결을 확인하려면 다음을 수행:

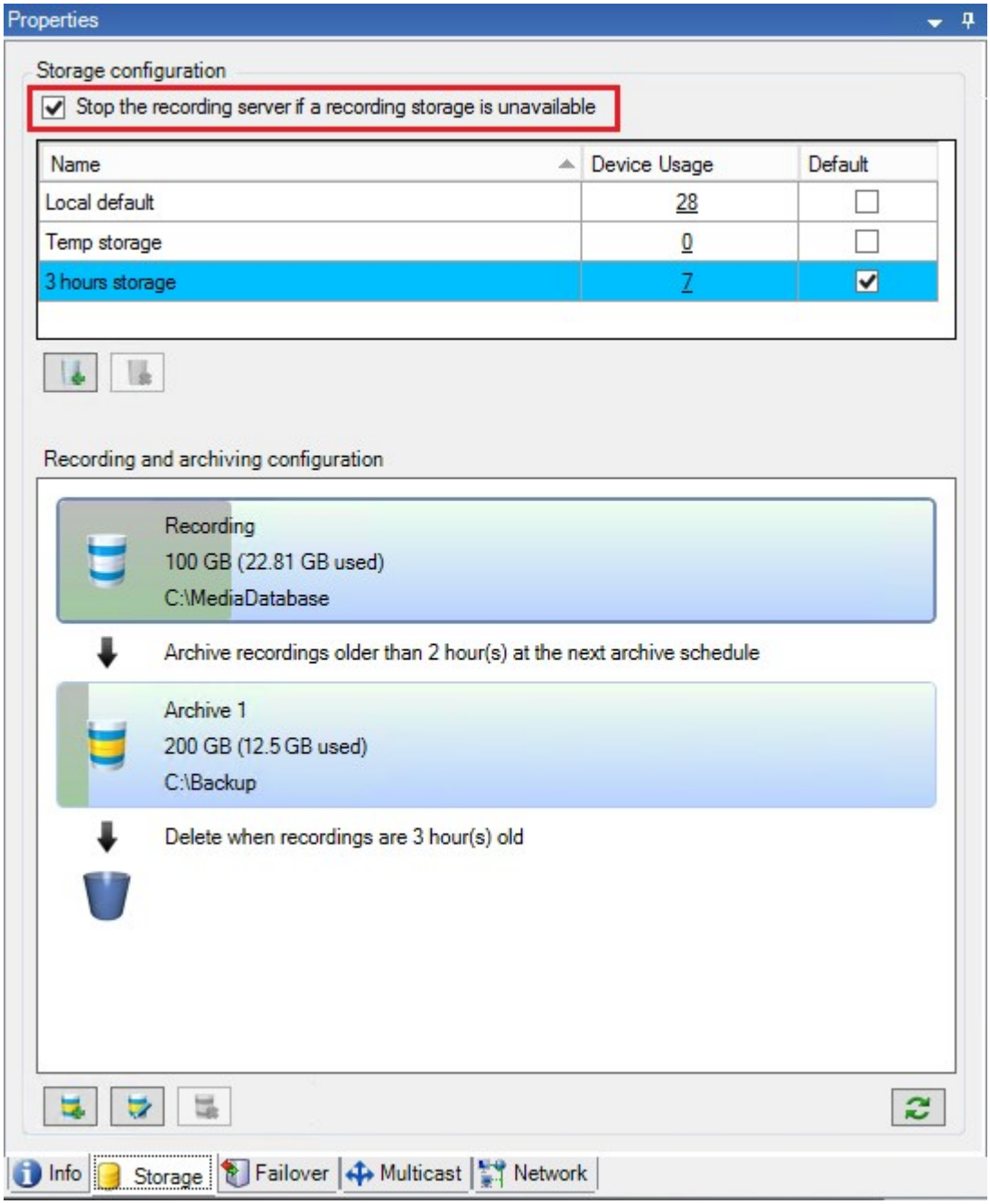
1. Management Client 을(를) 엽니다.
2. **사이트 탐색** 창에서 **서버** > **레코딩 서버** 를 선택합니다. 이렇게 하면 레코딩 서버 목록이 열립니다.
3. **개요** 창에서, 관련 레코딩 서버를 선택하고 **정보** 탭으로 이동합니다.
   레코딩 서버에서 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화가 활성화된 경우, 로컬 웹 서버 주소 및 웹 서버 주소(옵션)의 전면에 자물쇠 아이콘이 표시됩니다.



레코딩 저장소를 사용할 수 없을 때 행동 지정

기본적으로 레코딩 서버는 레코딩 저장소가 사용 불가능한 경우에도 계속 실행됩니다. 시스템이 장애 조치 레코딩 서버로 구성되어 있다면 레코딩 서버의 실행이 중지되도록 지정하여 장애 조치 서버가 인계받도록 할 수 있습니다.

1. 관련 레코딩 서버에서 **저장소** 탭으로 이동합니다.
2. **레코딩 저장소를 사용할 수 없는 경우 레코딩 서버 중지** 옵션을 선택해야 합니다.



새로운 저장소 추가

새로운 저장소를 추가할 때, 항상 **레코딩** 으로 명명된 사전 정의된 레코딩 데이터베이스와 함께 하나의 레코딩 저장소를 생성하게 됩니다. 데이터베이스의 이름을 바꿀 수 없습니다. 레코딩 저장소를 제외하고, 저장소에는 다수의 아카이브가 포함될 수 있습니다.

1. 선택한 레코딩 서버에 저장소를 더 추가하려면 저장소 구성 **목록 아래에 있는** 단추를 클릭합니다. 이렇게 하면 **저장소 및 레코딩 설정** 대화 상자가 열립니다.
2. 관련 설정을 지정합니다(페이지 382의 저장소 및 녹화 설정 속성 참조).
3. **확인** 을 클릭합니다.

필요한 경우 이제 새 저장소에 아카이브를 생성할 수 있습니다.

저장소 내에 아카이브 생성

저장소에는 디폴트 아카이브가 없지만 필요에 따라 아카이브를 생성할 수 있습니다.

1. **레코딩 및 아카이브 구성** 목록에서 해당 저장소를 선택합니다.
2. **레코딩 및 아카이브 구성** 목록 아래에 있는 단추를 클릭합니다.
3. **아카이브 설정** 대화 상자에서, 요청된 설정을 지정합니다(페이지 384의 아카이브 설정 속성 참조).
4. **확인** 을 클릭합니다.

저장소에 장치 또는 장치 그룹 연결

일단 레코딩 서버에 대한 저장소가 구성되면, 카메라, 마이크로폰, 스피커 등의 개별 장치나 장치 그룹에 대해 활성화할 수 있습니다. 또한 개별 장치 또는 그룹에 사용할 레코딩 서버의 저장소 영역을 선택할 수도 있습니다.

1. **장치** 를 확장하고 필요에 따라 **카메라**, **마이크** 또는 **스피커** 를 선택합니다.
2. 장치 또는 장치 그룹을 선택합니다.
3. **레코딩** 탭을 선택합니다.
4. **저장소** 영역에서 **선택** 을 선택합니다.
5. 나타나는 대화 상자에서 장치의 레코딩을 저장할 데이터베이스를 선택한 다음, **확인** 을 클릭합니다.
6. 도구 모음에서 **저장** 을 클릭합니다.

레코딩 서버의 저장소 탭에서 저장소 영역에 대한 장치 사용 수를 클릭하면 메시지 보고서가 나타나는데, 여기에서 해당 장치를 볼 수 있습니다.

장치 비활성화됨

비활성화된 장치는 기본적으로 **개요** 창에 표시되지 않습니다.

비활성화된 모든 장치를 표시하려면 **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 열고 **비활성화된 장치 표시**를 선택합니다.

비활성화된 장치를 다시 숨기려면 **비활성화된 장치 표시**의 선택을 지웁니다.

선택한 저장소 또는 아카이브의 설정 편집

1. 저장소를 편집하려면 **레코딩 및 아카이브 구성** 목록에서 해당 레코딩 데이터베이스를 선택합니다. 아카이브를 편집하려면 아카이브 데이터베이스를 선택합니다.
2. **레코딩 및 아카이브 구성** 목록 아래에 있는 레코딩 저장소 편집 **버튼** 을 클릭합니다.
3. 레코딩 데이터베이스를 편집하거나 아카이브를 편집합니다.

데이터베이스의 최대 크기를 변경하면 시스템이 새로운 한도를 초과하는 레코딩을 자동 아카이브합니다. 아카이브 설정에 따라 레코딩을 다음 아카이브로 자동 아카이브하거나 삭제합니다.

내보내기 위해 디지털 서명 사용

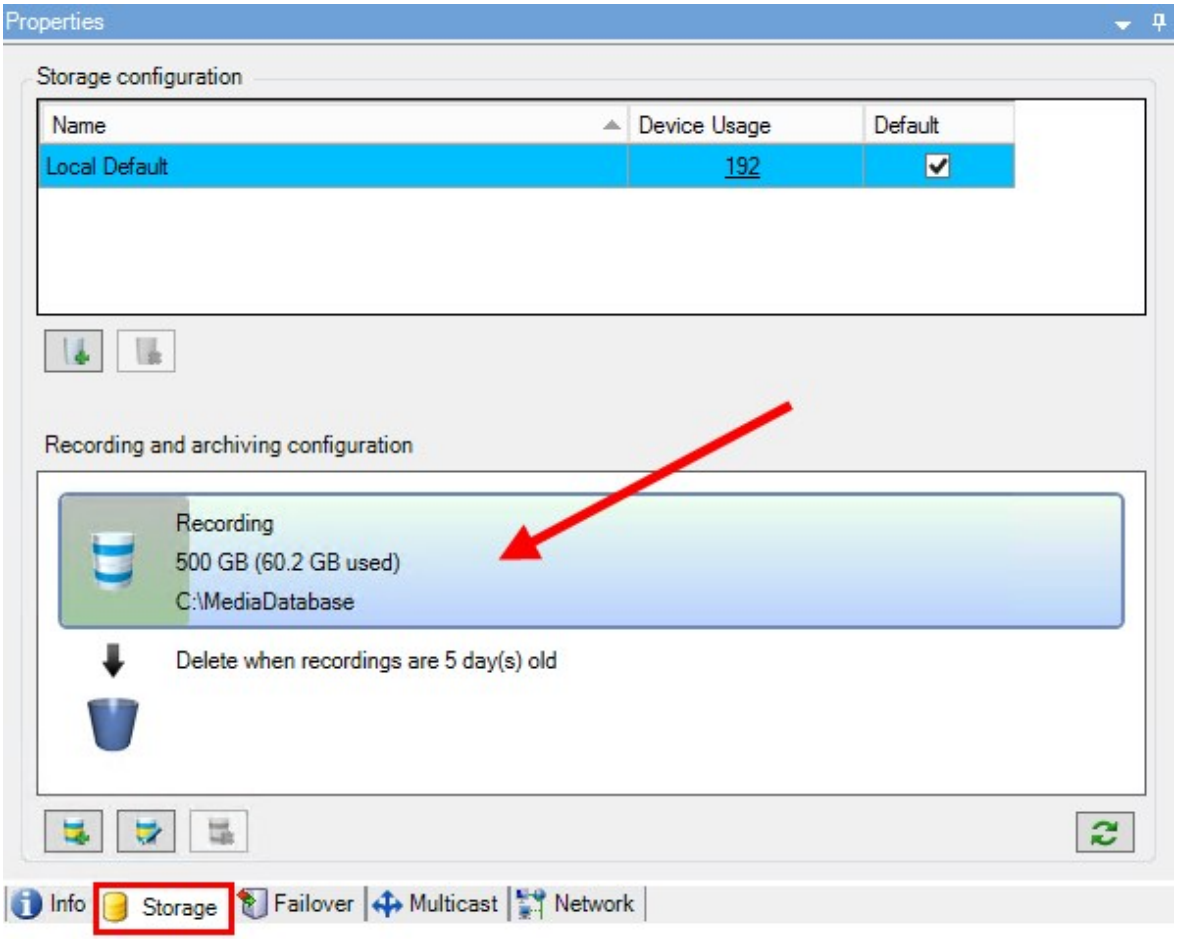
사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

녹화된 비디오에 대해 디지털 서명을 사용하여 클라이언트 사용자가 녹화된 비디오가 녹화된 이후 조작되지 않았는지 확인할 수 있습니다. 비디오의 진위를 확인하는 일은 비디오를 내보낸 후에 사용자가 XProtect Smart Client – Player 에서 수행하는 작업입니다.

서명은 또한 XProtect Smart Client > **내보내기** 탭 > **내보내기 설정** > **XProtect 형식** > **디지털 서명 포함** 에서 활성화해야 합니다. 그렇지 않을 경우, XProtect Smart Client – Player 의 **서명 확인** 버튼이 표시되지 않습니다.

1. **사이트 탐색** 창에서 **서버** 노드를 확장합니다.
2. **레코딩 서버** 를 클릭합니다.
3. 개요 창에서, 서명을 사용할 레코딩 서버를 클릭합니다.

4. **속성** 창 하단에서 **저장소** 탭을 클릭합니다.



5. **레코딩 및 아카이빙 구성** 섹션에서, 레코딩 데이터베이스를 나타내는 가로 표시줄을 두 번 클릭합니다. **저장소 및 레코딩 설정** 창이 나타납니다.
6. **서명** 확인란을 선택합니다.
7. **확인** 을 클릭합니다.

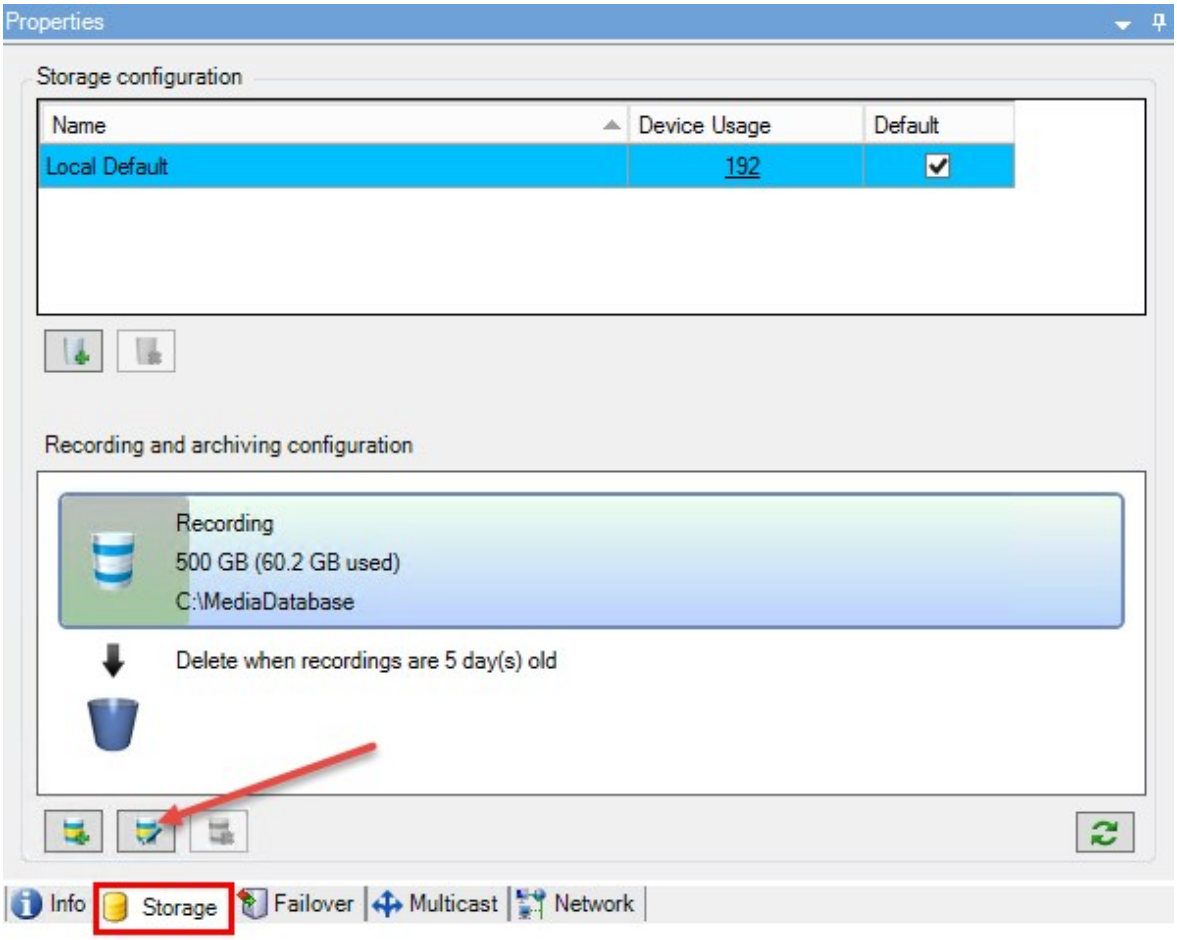
레코딩 암호화

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

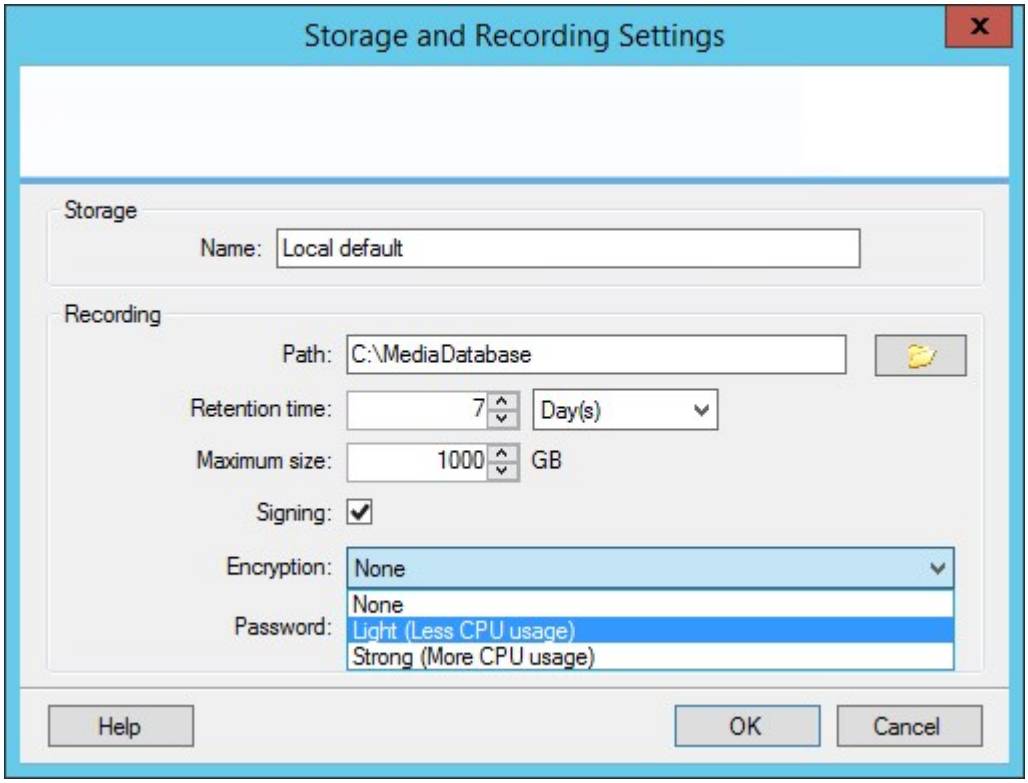
레코딩 서버 저장소 및 아카이브에서 암호화를 사용하여 레코딩을 보호할 수 있습니다. 간단한 암호화와 고급 암호화 사이에서 선택할 수 있습니다. 암호화를 사용으로 설정할 경우, 관련된 암호도 지정해야 합니다.

암호화 설정이나 암호를 사용으로 설정하거나 변경하는 작업은 데이터베이스의 크기 및 드라이브의 성능에 따라 시간이 걸릴 수 있습니다. **현재 작업** 아래에서 진행 사항을 추적할 수 있습니다.
이 작업이 진행 중인 동안 레코딩 서버를 중지하지 마십시오.

1. **레코딩 및 아카이브 구성** 목록 아래에 있는 **레코딩 저장소 편집** 버튼을 클릭합니다.



2. 표시되는 대화 상자에서, 암호화 수준을 지정합니다.



3. **암호 설정** 대화 상자로 자동으로 이동됩니다. 암호를 입력하고 **확인** 을 클릭합니다.

아카이브된 레코딩 백업

테이프 드라이브나 유사한 수단을 사용하여 레코딩을 백업할 수 있습니다. 이를 정확히 수행하는 방식은 매우 다양하며 사용하는 백업 매체에 따라 다릅니다. 그러나 다음 사항을 반드시 염두에 두어야 합니다:
카메라 데이터베이스가 아닌 아카이브 백업

항상 개별 카메라 데이터베이스가 아닌 아카이브 내용을 기반으로 백업을 만드십시오. 개별 카메라 데이터베이스 내용을 기반으로 백업을 만들 경우, 공유 위반 또는 그 밖의 오작동을 초래할 수 있습니다.

백업을 예약할 때는 백업 작업이 지정된 아카이브 시간과 겹치지 않도록 주의하십시오. 각 레코딩 서버의 저장소 영역에서 레코딩 서버 각각의 아카이브 일정을 보려면 **저장소** 탭을 참조하십시오.

백업 중에 아카이브가 발생했는지 확인하려면 아카이브를 마우트 해제하고 백업을 수행한 다음 아카이브를 다시 마운트하면 됩니다. Milestone Integration Platform VMS API을(를) 통해 아카이브를 마운트하고 마운트 해제합니다.

백업 대상을 지정할 수 있도록 아카이브 구조 파악

레코딩을 아카이브할 때는 아카이브 내의 특정 하위 디렉토리 구조에 해당 내용을 저장합니다.

시스템을 일반적으로 사용하는 경우에, 사용자가 XProtect Smart Client (으)로 레코딩을 검색할 때 하위 디렉토리 구조는 시스템 사용자에게 항상 완전히 숨겨집니다. 이는 아카이브 및 비아카이브 레코딩 모두에 적용됩니다. 아카이브된 레코딩을 백업하려는 경우(페이지 57의 아카이브 구조(설명됨) 참조), 하위 디렉토리 구조(페이지 304의 시스템 구성 백업 및 복원 참조)를 아는 것이 관련있습니다.

저장소에서 아카이브 삭제

1. **레코딩 및 아카이브 구성** 목록에서 아카이브를 선택합니다.

   목록에서 마지막 아카이브만 삭제할 수 있습니다. 이 아카이브는 비워둘 필요가 없습니다.

2. **레코딩 및 아카이브 구성** 목록 아래에 있는 단추 를 클릭합니다.
3. **예** 를 클릭합니다.

   오프라인 아카이브와 같이 사용할 수 없는 아카이브의 경우 아카이브에 증거물 잠금이 있는 미디어가 포함되어 있는지 확인할 수 없지만 사용자 확인 후 아카이브를 삭제할 수 있습니다.

   증거물 잠금이 있는 미디어가 포함된 사용 가능한 아카이브(온라인 아카이브)는 삭제할 수 없습니다.

저장소 삭제

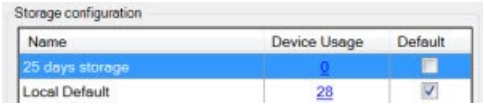
라이브 레코딩을 위한 레코딩 저장소로 사용하는 기본 저장소는 삭제할 수 없습니다.
이는 곧 장치와 저장소를 삭제하기 전에 다른 저장소에 아직 아카이브되지 않은 레코딩을 옮겨야 할 수도 있음을 의미합니다(페이지 314의 하드웨어 이동 참조).

1. 이 저장소를 사용하는 장치 목록을 보려면 장치 사용 번호를 클릭합니다.

   저장소에 다른 레코딩 서버로 이동된 장치의 데이터가 포함되어 있으면 경고가 나타납니다. 장치 목록을 보려면 링크를 클릭하십시오.

2. 페이지 190의 저장소 내의 아카이브되지 않은 레코딩을 다른 저장소로 이동에 소개된 단계를 따릅니다.
3. 모든 장치를 이동할 때까지 계속합니다.

4. 삭제할 저장소를 선택합니다.



5. **저장소 구성** 목록 아래에 있는 단추 를 클릭합니다.
6. **예** 를 클릭합니다.

저장소 내의 아카이브되지 않은 레코딩을 다른 저장소로 이동

장치의 레코딩 탭을 사용하여 하나의 실시간 레코딩 데이터베이스에서 다른 데이터베이스로 녹화물을 이동할 수 있습니다.

1. 장치 유형을 선택합니다. **개요** 창에서 장치를 선택합니다.
2. **레코드** 탭을 클릭합니다. **저장소** 영역의 상단에서 **선택** 을 클릭합니다.
3. **저장소 선택** 대화 상자에서 데이터베이스를 선택합니다.
4. **확인** 을 클릭합니다.
5. **녹화 동작** 대화 상자에서 기존에 존재하지만 **아카이브되지 않은** 녹화물을 새 저장소로 이동할지 아니면 삭제할지 여하를 선택합니다.
6. **확인** 을 클릭합니다.

장애 조치 레코딩 서버 할당

레코딩 서버의 **장애 조치** 탭에서 3가지의 장애 조치 설정 중 하나를 선택할 수 있습니다.

- 장애 조치 설정 없음
- 1차/2차 장애 조치 설정(수동 대기)
- 상시 대기 설정

b 와 **c** 를 선택한 경우, 특정 서버/그룹을 선택해야 합니다. **b** 를 사용하면 2차 장애 조치 그룹도 선택할 수 있습니다. 레코딩 서버를 사용할 수 없는 경우, 1차 장애 조치 그룹의 장애 조치 레코딩 서버가 작업을 인수합니다. 2차 장애 조치 그룹도 선택했다면 1차 장애 조치 그룹의 모든 장애 조치 레코딩 서버가 사용 중인 경우, 2차 그룹의 장애 조치 레코딩 서버가 작업을 인수합니다. 이러한 방식으로 작동하기 때문에 안정적이며, 위험 요소가 있다면 1차 및 2차 장애 조치 그룹의 모든 장애 조치 레코딩 서버가 사용 중이라서 장애 조치 솔루션이 무력화되는 경우인데 이는 매우 드문 일입니다.

1. **사이트 탐색** 창에서 **서버** > **레코딩 서버** 를 선택합니다. 이렇게 하면 레코딩 서버 목록이 열립니다.
2. **개요** 창에서 원하는 레코딩 서버를 선택하고 **장애 조치** 탭으로 이동합니다.
3. 장애 조치 설정 유형을 선택하려면, 다음 중에서 선택하십시오.
   - **없음**
   - **1차 장애 조치 서버 그룹/2차 장애 조치 서버 그룹**
   - **상시 대기 서버**

   1차/2차 장애 조치 그룹과 동일한 장애 조치 그룹을 선택하거나 이미 장애 조치 그룹의 일부인 일반 장애 조치 서버를 상시 대기 서버로 선택할 수 없습니다.
4. 다음으로 **고급 장애 조치 설정** 을 클릭합니다. 이렇게 하면 **고급 장애 조치 설정** 창이 열리고 선택한 레코딩 서버에 연결된 모든 장치가 나열됩니다. **없음** 을 선택했으면, 고급 장애 조치 설정을 사용할 수 있습니다. 시스템은 이후 장애 조치 설정에 대한 모든 선택 사항을 유지합니다.
5. 장애 조치 지원 수준을 지정하려면 목록의 각 장치에 대해 **전체 지원**, **라이브만** 또는 **비활성화됨** 을 선택합니다. **확인** 을 클릭합니다.
6. 필요 시 **장애 조치 서비스 통신 포트(TCP)** 필드에서 포트 번호를 편집합니다.

장애 조치 지원을 활성화하고, 레코딩 저장소를 사용할 수 없는 경우 레코딩 서버가 계속 실행되도록 구성하는 경우에는 장애 조치 레코딩 서버가 작업을 인수하지 않을 것입니다. 장애 조치 지원을 작동시키기려면, **저장** 탭에서 **레코딩 저장소를 사용할 수 없는 경우 레코딩 서버 중지** 를 선택해야 합니다.

레코딩 서버에 대한 멀티캐스팅 활성화

일반적인 네트워크 통신에서는 유니캐스트라는 프로세스를 통해 단일 발신자로부터 단일 수신자에게 각 데이터 패킷이 전송됩니다. 그러나 멀티캐스팅을 사용하면 단일 데이터 패킷(서버로부터)을 그룹 내의 여러 수신자(클라이언트)에게 전송할 수 있습니다. 멀티캐스팅은 대역폭을 줄이는 데 도움이 될 수 있습니다.

- **유니캐스팅** 을 사용하는 경우, 소스가 각 수신자에 대해 하나의 데이터 스트림을 전송해야 합니다
- **멀티캐스팅** 을 사용하는 경우에는 각 네트워크 세그먼트에서 단일 데이터 스트림만 필요합니다

여기서 기술한 바와 같이 멀티캐스팅은 카메라에서 서버로 비디오를 스트리밍하는 것이 **아니라** 서버에서 클라이언트로 스트리밍하는 것입니다.

멀티캐스팅을 통해 IP 주소 범위와 같은 옵션을 기반으로 정의된 수신자 그룹, 개별 카메라에 대한 멀티캐스트를 활성화/비활성화하는 기능, 최대 허용되는 데이터 패킷 크기(MTU)를 정의하는 기능, TTL 간에 데이터 패킷이 전달되어야 하는 최대 라우터 수를 정의하는 기능 등을 사용할 수 있습니다.

레코딩 서버가 암호화를 사용하더라도 멀티캐스트 스트림은 암호화되지 않습니다.

멀티캐스팅은 데이터가 모든 이에게 관련이 없을지라도 네트워크에 연결된 모든 사람에게 데이터를 전송하는 **브로드캐스팅** 과 혼동해서는 안 됩니다:

이름	설명
유니캐스팅	단일 소스에서 단일 수신자에게 데이터를 전송합니다.
멀티캐스팅	단일 소스에서 명확히 정의된 그룹 내의 여러 수신자에게 데이터를 전송합니다.
브로드캐스팅	단일 소스에서 네트워크 상에 있는 모든 사람들에게 데이터를 전송합니다. 따라서 브로드캐스팅을 이용하면 네트워크 통신 속도가 크게 저하될 수 있습니다.

멀티캐스팅을 사용하려면 사용 중인 네트워크 인프라가 IP 멀티캐스팅 표준 IGMP(Internet Group Management Protocol)를 지원해야 합니다.

- **멀티캐스트** 탭에서 **멀티캐스트** 확인란을 선택합니다

멀티캐스트를 위한 전체 IP 주소가 하나 이상의 레코딩 서버에서 이미 사용 중인 경우, 먼저 일부 멀티캐스트 IP 주소를 해제한 후 추가 레코딩 서버에서 멀티캐스팅을 활성화해야 합니다.

레코딩 서버가 암호화를 사용하더라도 멀티캐스트 스트림은 암호화되지 않습니다.

개별 카메라의 멀티캐스팅 활성화

멀티캐스팅은 필요한 카메라에 대해 설정을 활성화한 경우에만 작동합니다.

1. 레코딩 서버를 선택하고 **개요** 창에서 필요한 카메라를 선택합니다.
2. **클라이언트** 탭에서 **라이브 멀티캐스트** 확인란을 선택합니다. 모든 관련 카메라에 대해 반복합니다.

레코딩 서버가 암호화를 사용하더라도 멀티캐스트 스트림은 암호화되지 않습니다.

공용 주소 및 포트 정의

공용 또는 신뢰되지 않은 네트워크상에서 XProtect Smart Client 을(를) 갖춘 VMS에 액세스하려면, Milestone 은(는) VPN을 통해 보안 연결을 사용할 것을 권장합니다. 이렇게 하면 XProtect Smart Client 및 VMS 서버 간의 통신이 보호되도록 할 수 있습니다.

네트워크 탭에서 레코딩 서버의 공용 IP 주소를 정의합니다.

공용 주소를 사용하는 이유?

클라이언트는 로컬 네트워크를 비롯한 인터넷에서 연결될 수 있고, 두 경우 모두에서 감시 시스템은 클라이언트가 레코딩 서버로부터 라이브 및 녹화된 비디오에 액세스할 수 있도록 적합한 주소를 제공해야 합니다:

- 클라이언트가 로컬로 연결되면, 감시 시스템이 로컬 주소와 포트 번호로 회신해야 합니다.
- 클라이언트가 인터넷에서 연결할 때, 감시 시스템은 레코딩 서버의 공용 주소로 회신해야 합니다. 이는 방화벽 또는 NAT(Network Address Translation) 라우터의 주소, 그리고 종종 다른 포트 번호이기도 합니다. 그러면 이 주소와 포트가 서버의 로컬 주소와 포트로 전달될 수 있습니다.

1. 공용 액세스를 활성화하려면 **공공 액세스 활성화** 확인란을 선택합니다.
2. 레코딩 서버의 공용 주소를 정의합니다. 인터넷을 통해 감시 시스템에 액세스하는 클라이언트가 레코딩 서버에 연결할 수 있도록 방화벽 또는 NAT의 주소를 입력합니다.
3. 공용 포트 번호를 지정합니다. 항상 방화벽 또는 NAT 라우터에서 사용하는 포트 번호를 로컬로 사용하는 번호와 다르게 지정하는 것이 좋습니다.

공용 액세스를 사용하는 경우, 공용 주소 및 포트에서 전송된 요청이 해당 레코딩 서버의 로컬 주소와 포트로 전달되도록 방화벽 또는 NAT 라우터를 구성하십시오.

로컬 IP 범위 할당

감시 시스템이 로컬 네트워크로부터 수신되는 것을 인식하는 로컬 IP 범위 목록을 정의합니다.

- **네트워크** 탭에서 **구성** 을 클릭합니다

장치 트리 필터링

등록된 장치가 많은 경우, **개요** 창의 장치 트리가 매우 커질 수 있습니다. 장치 트리를 필터링하여 작업하려는 장치를 더 쉽게 찾을 수 있습니다.

몇 가지 특정 장치에 고유한 필터 용어를 제공하면 이러한 특정 장치만 효과적으로 표시할 수 있습니다.

장치 트리 필터링

- **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 엽니다.
- **장치를 필터링하려면 여기에 입력** 필드에 하나 이상의 필터 기준을 입력하고 **필터 적용**을 클릭하여 장치 목록을 필터링합니다.

필터 기준 특성

필터 기준은 장치 이름, 장치 짧은 이름, 하드웨어 주소(IP), 장치 ID 및 하드웨어 ID 필드 값에 적용됩니다.

하드웨어 ID 및 장치 ID 필드 값을 필터링할 때 부분 필터 일치는 표시되지 않습니다. 따라서 하드웨어 ID 또는 장치 ID로 필터링할 때 완전하고 정확한 식별 번호를 정의해야 합니다.

장치 이름, 장치 짧은 이름 및 하드웨어 주소 필드 값에 대해 부분 필터 일치가 표시되므로 필터 용어 'camer'는 장치 이름에 'camera'라는 단어가 포함된 모든 장치를 표시합니다.

필터 기준은 대소문자를 구분하지 않으므로 필터 기준으로 'camera' 또는 'Camera'를 사용하면 동일한 결과가 나타납니다.

여러 필터 기준 지정

여러 필터 기준을 지정하여 장치 트리의 필터링 범위를 더욱 좁힐 수 있습니다. 필터가 적용되면 정의된 모든 필터 기준이 AND(그리고)와 함께 결합된 것으로 간주되어 누적됩니다.

예를 들어 두 개의 필터 기준: 'Camera' 및 'Warehouse'를 입력한 경우, 목록에는 장치 이름에 'Camera' 및 'Warehouse'라는 단어가 포함된 모든 장치가 표시되지만, 장치 이름에 'Camera' 및 'Parking Lot'이라는 단어가 포함된 장치는 표시되지 않으며 장치 이름에 'Camera'라는 단어만 포함된 장치도 표시되지 않습니다.

너무 제한적인 필터를 지정한 경우, 필터 필드에서 각 개별 필터 기준을 제거하여 필터를 확장하십시오. 필터 기준을 제거하면 필터가 장치 트리에 자동으로 적용됩니다.

필터 재설정

필터 필드에서 모든 필터 기준을 제거하면 **개요** 창이 재설정되고 모든 장치가 다시 한 번 표시됩니다.

F5를 눌러 필터를 재설정하고 **비활성화된 장치 표시** 확인란의 선택을 취소할 수도 있습니다.

장치 비활성화됨

비활성화된 장치는 기본적으로 **개요** 창에 표시되지 않습니다.

비활성화된 모든 장치를 표시하려면 **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 열고 **비활성화된 장치 표시**를 선택합니다.

비활성화된 장치를 다시 숨기려면 **비활성화된 장치 표시**의 선택을 지웁니다.

장애 조치 서버

장애 조치 레코딩 서버 설치 및 활성화

장애 조치 레코딩 서버를 비활성화한 경우, 표준 레코딩 서버의 작업을 인수하기 전에 해당 서버를 활성화해야 합니다.

장애 조치 레코딩 서버를 활성화하고 기본 속성을 편집하려면 다음과 같이 하십시오.

1. **사이트 탐색** 창에서, **서버** > **장애 조치 서버** 를 선택합니다. 이렇게 하면 설치된 장애 조치 레코딩 서버와 장애 조치 그룹 목록이 열립니다.
2. **개요** 창에서 필요한 장애 조치 레코딩 서버를 선택합니다.
3. 서버를 마우스 오른쪽 버튼으로 클릭하고 **활성화** 를 선택합니다. 이제 장애 조치 레코딩 서버가 활성화됩니다.

4. 장애 조치 레코딩 서버 속성을 편집하려면 **정보** 탭으로 이동하십시오.
5. 끝나면 **네트워크** 탭으로 이동합니다. 여기서 장애 조치 레코딩 서버의 공용 IP 주소 등을 정의할 수 있습니다. 이는 NAT(Network Address Translation) 및 포트 전달 기능을 사용하는 경우 해당됩니다. 자세한 내용은 표준 레코딩 서버의 **네트워크** 탭을 참조하십시오.
6. **사이트 탐색** 창에서 **서버** > **레코딩 서버** 를 선택합니다. 장애 조치를 지원할 레코딩 서버를 선택하고, 장애 조치 레코딩 서버를 할당하십시오(페이지 385의 장애 조치 탭(레코딩 서버) 참조).

장애 조치 레코딩 서버의 상태를 보려면, 마우스를 알림 영역의 Failover Recording Server Manager 트레이 아이콘 위로 가져갑니다. 장애 조치 레코딩 서버의 설명 필드에 입력된 텍스트를 포함한 도구 설명이 나타납니다. 이는 장애 조치 레코딩 서버가 작업을 인수하도록 구성된 레코딩 서버가 무엇인지를 확인하는 데 도움이 될 수 있습니다.

> 장애 조치 레코딩 서버는 정기적으로 관리 서버를 핑하여 서버가 온라인 상태인지, 필요 시 표준 레코딩 서버의 구성을 요청 및 수신할 수 있는지를 확인합니다. 핑을 차단하면 장애 조치 레코딩 서버가 표준 레코딩 서버의 작업을 인계할 수 없습니다.

수동 대기를 위한 장애 조치 레코딩 서버 그룹

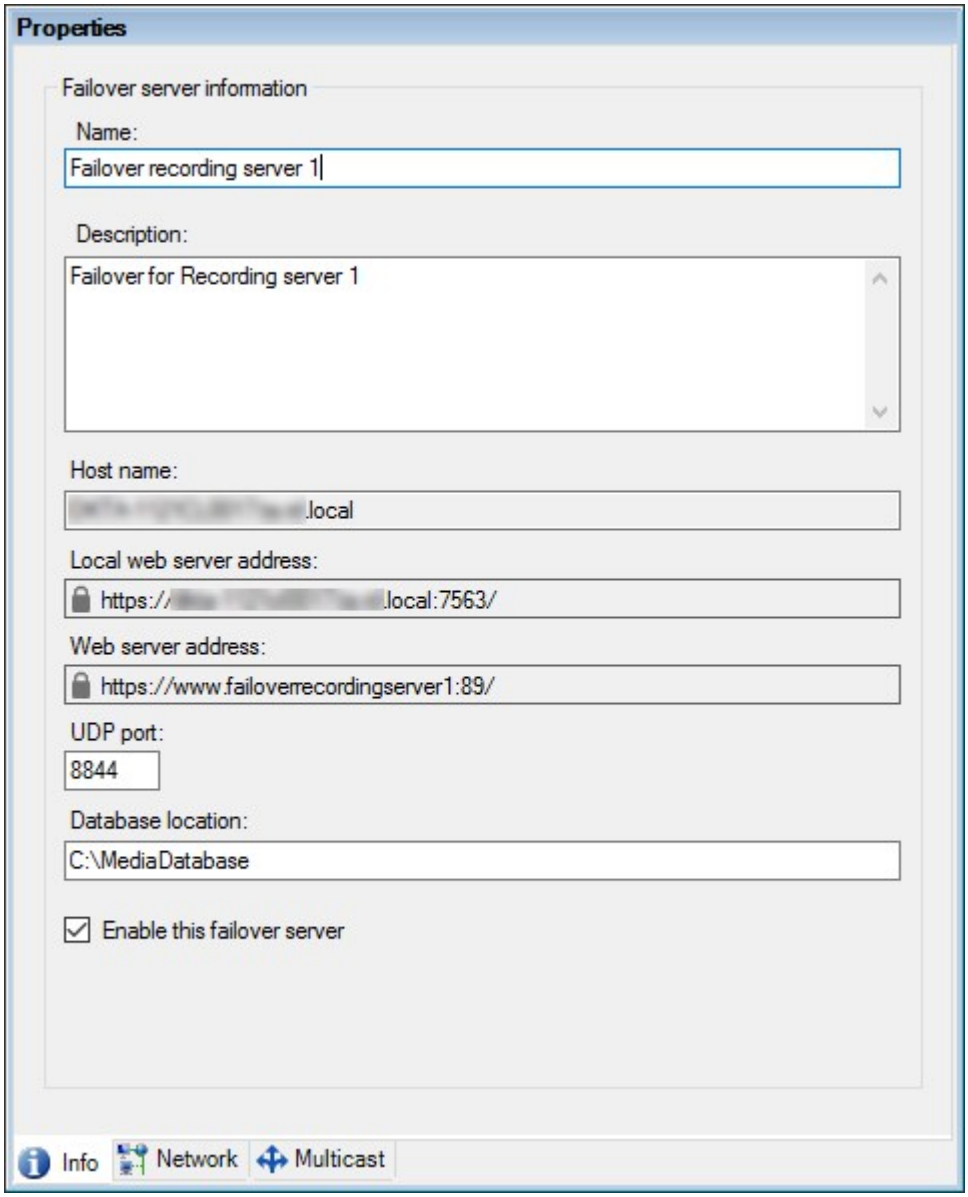
1. **서버** > **장애 조치 서버** 를 선택합니다. 이렇게 하면 설치된 장애 조치 레코딩 서버와 장애 조치 그룹 목록이 열립니다.
2. **개요** 창에서 상위 노드 **장애 조치 그룹** 을 마우스 오른쪽 단추로 클릭하고 **그룹 추가** 를 선택합니다.
3. 새 그룹의 이름(이 예에서는 *장애 조치 그룹 1*)과 설명(옵션)을 지정합니다. **확인** 을 클릭합니다.
4. 방금 만든 그룹(*장애 조치 그룹 1*)을 마우스 오른쪽 단추로 클릭합니다. **그룹 구성원 편집** 을 선택합니다. 이렇게 하면 **그룹 구성원 선택** 창이 열립니다.
5. 끌어다 놓는 방식이나 단추를 사용하여 선택한 장애 조치 레코딩 서버를 왼쪽에서 오른쪽으로 이동합니다. **확인** 을 클릭합니다. 이제 선택한 장애 조치 레코딩 서버가 방금 만든 그룹(*장애 조치 그룹 1*)에 속하게 됩니다.
6. **시퀀스** 탭으로 이동합니다. **위** 및 **아래** 를 클릭하여 그룹에서 일반 장애 조치 레코딩 서버의 내부 시퀀스를 설정합니다.

장애 조치 레코딩 서버의 암호화 상태 보기

장애 조치 레코딩 서버가 암호화를 사용하는지 확인하려면 다음과 같이 하십시오.

1. **사이트 탐색** 창에서, **서버** > **장애 조치 서버** 를 선택합니다. 이렇게 하면 장애 조치 레코딩 서버 목록이 열립니다.
2. **개요** 창에서, 관련 레코딩 서버를 선택하고 **정보** 탭으로 이동합니다.
   레코딩 서버에서 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화가 활성화된 경우, 로컬 웹 서버 주

소 및 웹 서버 주소(옵션)의 전면에 자물쇠 아이콘이 표시됩니다.



상태 메시지 보기

1. 장애 조치 레코딩 서버에서, **Milestone Failover Recording Server 서비스** 아이콘을 마우스 오른쪽 버튼으로 클릭합니다.
2. **상태 메시지 표시** 를 선택합니다. **Failover Server 상태 메시지** 창이 나타나고 타임스탬프가 표시된 상태 메시지가 나열됩니다.

버전 정보 보기

제품 지원부에 연락해야 할 경우 **Failover Recording Server 서비스** 의 정확한 버전을 알고 있으면 유리합니다.

1. 장애 조치 레코딩 서버에서, **Milestone Failover Recording Server 서비스** 아이콘을 마우스 오른쪽 버튼으로 클릭합니다.
2. **정보** 를 선택합니다.
3. **Failover Recording Server 서비스** 의 정확한 버전을 보여주는 작은 대화 상자가 열립니다.

하드웨어

하드웨어 추가

시스템 내 각 레코딩 서버에 하드웨어를 추가하기 위한 여러 가지 옵션이 있습니다.

> ⚠ 하드웨어가 NAT 지원 라우터 또는 방화벽 뒤에 위치한 경우, 다른 포트 번호를 지정하고 하드웨어가 사용하는 포트 및 IP 주소를 매핑하도록 라우터/방화벽을 구성해야 할 수 있습니다.

하드웨어 추가 마법사를 이용하면 네트워크에서 카메라와 비디오 인코더와 같은 하드웨어를 손쉽게 감시하여 시스템상의 레코딩 서버에 추가할 수 있습니다. 또한 마법사는 Milestone Interconnect 설치에 대한 원격 레코딩 서버 추가하는 것을 도와줍니다. 한 번에 **하나의 레코딩 서버** 만 추가하십시오.

1. **하드웨어 추가**에 액세스하려면 필요한 레코딩 서버를 마우스 오른쪽 단추로 클릭하고 **하드웨어 추가**를 선택합니다.
2. 마법사 옵션 중 하나(아래 참조)를 선택하고 화면에 나타나는 지침을 따릅니다.
3. 설치 후 **개요** 창에서 해당 하드웨어와 장치를 볼 수 있습니다.

> ⚠ 특정 하드웨어는 처음 하드웨어를 추가할 때 반드시 사전 구성해야 합니다. 그러한 하드웨어를 추가할 때 **사전 구성 하드웨어 장치** 마법사가 나타납니다. 자세한 정보는 페이지 50의 하드웨어 사전 구성(설명됨)를 참조하십시오.

하드웨어 추가(대화)

하드웨어는 다음을 나타냅니다.

- IP를 통해 감시 시스템의 레코딩 서버에 직접 연결되는 물리적 장치(예: 카메라, 비디오 인코더, I/O 모듈)
- Milestone Interconnect 설정에서 원격 사이트에 있는 레코딩 서버

시스템에 하드웨어를 추가하는 방법에 관한 자세한 정보는 페이지 197의 하드웨어 추가를 참조하십시오.

이름	설명
Express	시스템이 레코딩 서버의 로컬 네트워크에서 새로운 하드웨어를 자동으로 검사합니다.

이름	설명
(권장)	검색된 하드웨어가 다른 레코딩 서버에서 실행 중인지 확인하려면 **다른 레코딩 서버에서 실행 중인 하드웨어 표시** 확인란을 선택합니다. 새 하드웨어를 네트워크에 추가하고 해당 하드웨어를 시스템에서 사용하려고 할 때마다 이 옵션을 선택할 수 있습니다. Milestone Interconnect 설정에 원격 시스템을 추가할 경우에는 이 옵션을 사용할 수 없습니다. HTTP 및 HTTPS 하드웨어 모두를 추가하려면, **HTTPS(암호화)** 라디오 버튼을 선택한 상태에서 **빠른(Express)** 감지를 실행한 후, **HTTP(비암호화)** 라디오 버튼을 선택한 상태에서 다시 한 번 실행합니다.
주소 범위 스캔	시스템이 다음의 사양을 토대로 네트워크에서 관련 하드웨어 및 Milestone Interconnect 원격 시스템을 검사합니다: • 하드웨어 사용자 이름 및 암호. 하드웨어가 출하시 기본 사용자 이름과 암호를 사용하는 경우에는 필요하지 않습니다 • 드라이버 • IP 범위(IPv4 전용) • 포트 번호(기본값 = 80) 예를 들어 시스템을 확장하는 경우와 같이 네트워크 일부만 검사하려는 경우에는 이 옵션을 선택할 수 있습니다.
수동	각 하드웨어와 Milestone Interconnect 원격 시스템에 대한 세부 정보를 별도로 지정합니다. 이는 소수의 하드웨어만 추가하려는 경우와 해당 IP 주소, 관련 사용자 이름과 암호를 알고 있는 경우나 카메라가 자동 검색 기능을 지정하지 않는 경우 효과적인 선택일 수 있습니다.
원격 연결 하드웨어	시스템이 원격으로 연결된 서버를 통해 연결된 하드웨어를 검사합니다. 예를 들어, Axis One-click 카메라 연결에 대한 서버를 설치한 경우 이 옵션을 사용할 수 있습니다. Milestone Interconnect 설정에 원격 시스템을 추가할 경우에는 이 옵션을 사용할 수 없습니다.

하드웨어 비활성화 / 활성화

기본적으로 추가된 하드웨어는 **활성화** 됩니다.

다음과 같은 방식으로 하드웨어가 활성화 또는 비활성화되었는지 확인할 수 있습니다:

활성화됨
비활성화됨
예를 들어 라이선싱 또는 성능 개선 목적으로 추가한 하드웨어를 비활성화하려면 다음과 같이 합니다.

1. 레코딩 서버를 확장하고 비활성화하려는 하드웨어를 마우스 오른쪽 단추로 클릭합니다.
2. **활성화됨** 을 선택하여 선택을 취소하거나 선택합니다.

하드웨어 편집

추가된 하드웨어에서 마우스 오른쪽 버튼을 클릭한 후 **하드웨어 편집** 을 선택하여 Management Client 에서 네트워크 구성 및 하드웨어 사용자 인증 설정을 수정합니다.

하드웨어 수정(대화)

일부 하드웨어의 경우 **하드웨어 편집** 대화를 통해 하드웨어 장치에 직접 설정을 적용할 수 있습니다.

만일 **Management Client 설정 편집** 라디오 버튼이 선택된 경우, **하드웨어 편집** 대화에서 Management Client 이(가) 하드웨어에 연결하기 위해 사용하는 설정을 표시합니다. 하드웨어 장치가 시스템에 제대로 추가되었는지 확인하려면 제조사의 하드웨어 구성 인터페이스 연결에 사용했던 것과 동일한 설정을 입력합니다:

이름	설명
이름	감지된 IP 주소와 함께 하드웨어 이름을 표시합니다(괄호 안).
하드웨어 URL	제조사의 하드웨어 구성 인터페이스 웹 주소에는 보통 하드웨어의 IP 주소가 포함되어 있습니다. 네트워크에서 유효한 주소를 지정하십시오.
사용자 이름	사용자 이름은 하드웨어 연결에 사용합니다. 여기에 입력한 사용자 이름은 실제 하드웨어 장치상의 사용자 이름을 변경하지 않습니다. **Management Client 및 하드웨어 설정** 편집 라디오 버튼을 선택하여 지원되는 하드웨어 장치상의 설정을 수정합니다.
암호	암호는 하드웨어로의 연결에 사용됩니다. 여기에 입력한 암호는 실제 하드웨어 장치상의 암호를 변경하지 않습니다. **Management Client 및 하드웨어 설정** 편집 라디오 버튼을 선택하여 지원되는 하드웨어 장치상의 설정을 수정합니다.

이름	설명
	다수의 하드웨어 장치의 암호를 변경하는 방법에 관한 정보는 페이지 204의 하드웨어 장치의 암호 변경를 참조하십시오. 시스템 관리자로서 다른 사용자가 암호를 볼 수 있도록 Management Client 에서 허가해야 합니다. 자세한 정보는 하드웨어 항목 아래 역할 설정 을 참조하십시오.

만일 **Management Client 및 하드웨어 설정 편집** 라디오 버튼이 선택되어 있는 경우(지원되는 하드웨어에 대해), **하드웨어 편집** 대화에서 하드웨어 장치에도 직접 적용되는 설정을 표시합니다:

선택된 라디오 버튼으로 설정을 적용하면 하드웨어 장치상의 현재 설정을 덮어쓰기하게 됩니다. 하드웨어는 설정이 적용되는 동안 레코딩 서버와 연결이 일시적으로 끊어집니다.

이름	설명
이름	감지된 IP 주소와 함께 하드웨어 이름을 표시합니다(괄호 안).
네트워크 구성	하드웨어의 네트워크 설정. 네트워크 설정을 변경하려면 페이지 200의 구성를 참조하십시오.
구성	**IP 버전** 드롭다운 목록을 사용하여 인터넷 프로토콜(지원되는 하드웨어 장비에 대해)을 지정합니다. • IPv4의 경우, 값은 다음 형식을 따라야 합니다: **(0-999).(0-999).(0-999).(0-999)** • IPv6의 경우, 값은 콜론으로 나뉘어 있는 8 그룹의 16진수 형식이어야 합니다. 서브넷 마스크는 **0-128** 사이의 숫자여야 합니다. **체크** 버튼은 현재 입력된 IP 주소를 사용하는 다른 하드웨어 장치가 시스템에 있는지 테스트합니다. **확인** 으로는 꺼져있거나 XProtect VMS 시스템 외부에 있거나 기타 일시적으로 응답하지 않는 하드웨어 장치를 인식할 수 없습니다.
사용자 이름	사용자 이름과 수준은 하드웨어 연결에 사용합니다. 드롭다운 목록에서 다른 사용자를 선택하고 아래에 설명된 **암호** 필드를 사용하여 새로운 암호를 추가합니다.

이름	설명
	인증 섹션 하단의 밑줄 친 동작을 사용하여 사용자를 추가하거나 삭제합니다 (페이지 201의 사용자 추가 또는 페이지 201의 사용자 삭제 참조) 제조사가 지정해둔 가장 높지 않은 사용자 수준을 선택하면 일부 기능을 사용하지 못하게 될 수 있습니다.
암호	암호는 하드웨어로의 연결에 사용됩니다. **나타내기** 아이콘을 사용하여 현재 입력한 텍스트를 봅니다. 암호를 변경하는 경우, 특정 하드웨어 장치를 위한 암호 규칙에 관한 제조사의 문서를 참고하거나 **암호 생성** 아이콘을 사용하여 자동으로 요건에 부합하는 암호를 자동으로 생성합니다. 다수의 하드웨어 장치의 암호를 변경하는 방법에 관한 정보는 페이지 204의 하드웨어 장치의 암호 변경를 참조하십시오. 시스템 관리자로서 다른 사용자가 암호를 볼 수 있도록 Management Client 에서 허가해야 합니다. 자세한 정보는 하드웨어 항목 아래 역할 설정 을 참조하십시오.
사용자 **추가**	밑줄이 그어진 **추가** 링크를 선택하여 **사용자 추가** 대화를 열고 하드웨어 장치에 사용자를 추가합니다. 사용자를 추가하면 자동으로 현재 활성화된 사용자로 설정되며 이전에 입력된 자격 증명을 덮어쓰기하게 됩니다. 암호를 생성하는 경우, 특정 하드웨어 장치를 위한 암호 규칙에 관한 제조사의 문서를 참고하거나 **암호 생성** 아이콘을 사용하여 자동으로 요건에 부합하는 암호를 자동으로 생성합니다. 하드웨어 장치에서 감지된 가장 높은 사용자 수준은 자동으로 사전 선택됩니다. **사용자 수준** 을 기본 값에서 변경하는 것은 권장하지 않습니다. 제조사가 지정해둔 가장 높지 않은 **사용자 수준** 을 선택하면 일부 기능을 사용하지 못하게 될 수 있습니다.
사용자	밑줄이 그어진 **삭제** 링크를 선택하여 **사용자 삭제** 대화를 열고 하드웨어 장치에 사용자를 삭제합니다.

이름	설명
삭제	현재 활성화된 사용자를 삭제할 수 없습니다. 신규 사용자를 설정하려면 위에서 설명한 **사용자** 추가 대화를 사용하고 이 인터페이스를 사용하는 기존 사용자를 제거합니다.

개별 장치 활성화 / 비활성화

카메라 는 기본적으로 **활성화** 되어 있습니다.

마이크, 스피커, 메타데이터, 입력 및 **출력** 은 기본적으로 **비활성화** 되어 있습니다.

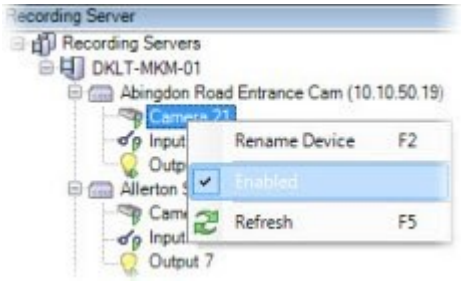
즉, 시스템에서 마이크, 스피커, 메타데이터, 입력, 출력을 사용하려면 개별적으로 활성화해야 합니다. 이러한 이유로 감시 시스템이 카메라에 의존하는 반면, 마이크 등의 사용은 각 조직의 필요에 크게 좌우됩니다.

장치가 활성화 또는 비활성화되었는지 확인할 수 있습니다(예제는 출력을 나타냄):

비활성화됨
활성화됨

카메라, 마이크, 스피커, 메타데이터, 입력 및 출력 활성화/비활성화에 동일한 방법이 사용됩니다.

1. 레코딩 서버과 해당 장치를 확장합니다. 활성화하려는 장치를 마우스 오른쪽 단추로 클릭합니다.
2. **활성화됨** 을 선택하여 선택을 취소하거나 선택합니다.



하드웨어에 보안 연결 설정

하드웨어와 레코딩 서버 간에 SSL(Secure Sockets Layer)을 사용하여 보안 HTTPS 연결을 설정할 수 있습니다.

아래 단계를 계속하기 전에 카메라 공급업체로 문의하여 하드웨어에 대한 인증서를 받아 해당 하드웨어에 업로드하십시오.

1. **개요** 창에서 레코딩 서버를 마우스 오른쪽 단추로 클릭하고 하드웨어를 선택합니다.

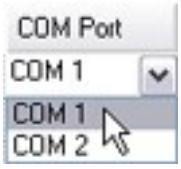
2. **설정** 탭에서 HTTPS를 활성화합니다. 이 설정은 기본적으로 활성화되어 있지 않습니다.
3. 레코딩 서버에 HTTPS 연결을 연결할 포트를 입력합니다. 포트 번호는 장치 홈페이지에 설정된 포트와 같아야 합니다.
4. 필요에 따라 변경하고 저장합니다.

비디오 인코더에서 PTZ 활성화

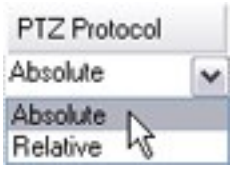
비디오 인코더에서 PTZ 카메라 사용을 활성화하려면 **PTZ** 탭에서 다음을 수행하십시오:

1. 비디오 인코더에 연결된 장치 목록에서 해당 카메라에 대해 **PTZ 활성화** 상자를 선택합니다:

2. **PTZ 장치 ID** 열에서 각 카메라의 ID를 확인합니다.
3. **COM 포트** 열에서 PTZ 기능을 제어하기 위해 사용할 비디오 인코더의 COM(직렬 통신)을 선택합니다:



4. **PTZ 프로토콜** 열에서 사용할 위치 지정 구성을 선택합니다:



   - **절대적**: 운영자가 카메라의 PTZ 제어를 사용하는 경우, 카메라가 고정 위치(종종 카메라의 홈 위치로 지칭)에 상대적으로 조정됩니다.
   - **상대적**: 운영자가 카메라의 PTZ 제어를 사용하는 경우, 카메라가 현재 위치에 상대적으로 조정됩니다.

   PTZ 프로토콜 열의 내용은 하드웨어에 따라 크게 다릅니다. 일부 하드웨어는 5 - 8가지의 프로토콜을 갖습니다. 카메라 설명서를 참조하십시오.

5. 도구 모음에서 **저장** 을 클릭합니다.

6. 각 PTZ 카메라의 프리셋 위치와 순찰 기능을 구성할 준비가 되었습니다:
   - 프리셋 위치(유형 1) 추가
   - 순찰 프로파일 추가

하드웨어 장치의 암호 변경

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

한 번에 다양한 하드웨어 장치의 암호를 변경할 수 있습니다.

원래 지원되는 장치는 Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision, ONVIF의 호환 하드웨어 장치 모델이지만 사용자 인터페이스를 통해 직접 모델이 지원되는지 여부를 볼 수 있습니다. 또한 저희 웹사이트를 방문하여 어떤 모델이 지원되는지 알아볼 수 있습니다: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> 장치 암호 관리 기능을 지원하지 않는 장치에 대해서는 반드시 해당 웹 페이지로부터 하드웨어 장치의 암호를 변경한 후, Management Client 에서 수동으로 새 암호를 입력해야 합니다. 자세한 정보는 페이지 199의 하드웨어 편집를 참조하십시오.

다음을 수행하도록 선택할 수 있습니다.

- 시스템이 각 하드웨어 장치에 대해 개별 암호를 생성하도록 합니다. 시스템은 하드웨어 장치의 제조사로부터 제공받은 요구 사항에 기반하여 암호를 생성합니다.
- 모든 하드웨어 장치에 대해 단일 사용자 정의 암호를 사용합니다. 새 암호를 적용할 때, 잠시 해당 하드웨어 장치와 레코딩 서버에 대한 연결이 끊어집니다. 새로운 암호를 적용한 후, 각 하드웨어 장치의 결과가 화면에 나타납니다. 실패한 변경에 대해 하드웨어 장치가 해당 정보를 지원하는 경우 실패 이유가 나타납니다. 마법사 내에서부터 성공/실패한 암호 변경 보고서를 생성할 수 있습니다. 그러나 **서버 로그** 에서도 결과가 기록됩니다.

  > ONVIF 드라이버가 설치된 다수 사용자 계정이 있는 하드웨어 장치에 대해 하드웨어 장치의 관리자 권한을 지닌 오직 한 XProtect 관리자만 VMS로부터 암호 변경을 할 수 있습니다.

요구사항:

- 하드웨어 장치 모델이 Milestone 를 통한 장치 암호 관리를 지원합니다.

단계:

1. **사이트 탐색** 창에서, **레코딩 서버** 노드를 선택합니다.
2. 개요 창에서 연관된 레코딩 서버를 우클릭합니다.
3. **하드웨어 암호 변경** 을 선택합니다. 마법사가 나타납니다.
4. 소문자와 대문자, 숫자, 다음 문자를 사용하여 암호를 입력합니다. **! ( ) * - . _**

   암호의 최대 길이는 64자입니다.

   > Bosch FLEXIDOME IP 실외 5000 MP NDN-50051 카메라의 암호 최대 길이는 19자입니다.

5. 변경을 완료하기 위해 화면의 지침을 따릅니다.

   > **최근 변경한 암호** 필드는 암호가 변경된 컴퓨터의 현지 시간 설정을 따라 최근 암호가 변경된 타임 스탬프를 보여줍니다.

6. 마지막 페이지는 결과를 보여줍니다. 시스템이 암호를 업데이트할 수 없는 경우 하드웨어 장비 옆 **실패함** 을 클릭하여 실패한 이유를 확인합니다.
7. 또한 **출력 보고** 버튼을 클릭하여 성공/실패한 업데이트의 모든 목록을 볼 수 있습니다.
8. 실패한 하드웨어 장치 상에서 암호를 변경하고자 하는 경우 **재시도** 를 클릭하면 마법사가 실패한 하드웨어 장치에서 재시작됩니다.

   > **재시도**를 선택하면 마법사를 처음으로 완료한 시점으로부터 더 이상 보고서에 접근할 수 없게 됩니다.

   > 보안 제한으로 인해 연속으로 암호 변경에 실패하는 경우 일부 하드웨어 장치는 일정 기간 동안 사용이 불가능할 수 있습니다. 다양한 제조사에 따라 달라지는 보안 제한.

하드웨어 장치에서 펌웨어 업데이트

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

Management Client 은(는) VMS 시스템에 추가된 하드웨어의 펌웨어를 업데이트할 수 있게 해줍니다. 동일한 펌웨어 파일과 호환되는 경우 동시에 다수의 하드웨어 장치에 대한 펌웨어 업데이트를 할 수 있습니다.

사용자 인터페이스에서 장치 모델이 펌웨어 업데이트를 지원하는지 여부를 직접 보여줍니다. Milestone 웹사이트로 이동하여 장치 모델이 지원되는지 여부를 확인할 수도 있습니다. https://www.milestonesys.com/community/business-partner-tools/supported-devices/

펌웨어 업데이트를 지원하지 않은 장치인 경우 반드시 해당 장치의 웹 페이지에서 하드웨어 장치의 펌웨어를 업데이트해야 합니다.

펌웨어를 업데이트 할 때 잠시 해당 하드웨어 장치와 레코딩 서버의 연결이 끊어집니다.

펌웨어를 업데이트한 후 각 하드웨어 장치에 대한 업데이트 결과가 화면에 나타납니다. 실패한 변경에 대해 하드웨어 장치가 해당 정보를 지원하는 경우 실패 이유가 나타납니다. 또한 해당 결과가 **서버 로그** 에도 기록됩니다.

ONVIF 드라이버 및 다수의 사용자 계정이 있는 하드웨어 장치인 경우, 해당 하드웨어 장치의 관리자 권한이 있는 XProtect 관리자만 VMS에서 펌웨어를 업데이트할 수 있습니다.

요구사항:

- 해당 하드웨어 장치 모델은 Milestone 을(를) 통한 펌웨어 업데이트를 지원합니다.

단계:

1. **사이트 탐색** 창에서, **레코딩 서버** 노드를 선택합니다.
2. 개요 창에서 연관된 레코딩 서버를 우클릭합니다.
3. **하드웨어 펌웨어 업데이트** 를 선택합니다. 마법사가 나타납니다.
4. 변경을 완료하기 위해 화면의 지침을 따릅니다.

   동일한 펌웨어 파일과 호환되는 다수의 하드웨어 장치만 업데이트할 수 있습니다. ONVIF 드라이버를 통해 추가된 하드웨어는 제조업체 이름이 아닌 **기타** 에서 확인할 수 있습니다.

6. 마지막 페이지는 결과를 보여줍니다. 시스템이 펌웨어를 업데이트할 수 없는 경우, 하드웨어 장치 옆 **실패함** 을 클릭하여 실패한 이유를 확인합니다.

Milestone은(는) 호환되지 않는 펌웨어 파일 또는 하드웨어 장치가 선택된 경우, 하드웨어 장치 오작동에 대한 책임을 지지 않습니다.

외부 IDP 추가 및 구성

1. Management Client에서 **도구** > **옵션**을 선택하고 **외부 IDP** 탭을 엽니다.
2. **외부 IDP** 섹션에서 **추가**를 선택합니다.
3. 외부 IDP에 대한 정보를 입력합니다. 필요한 정보에 대한 자세한 내용은 외부 IDP를 참고하십시오.

VMS에서 사용하고자 하는 외부 IDP에서 클레임을 등록하는 방법에 관한 정보는 외부 IDP에서 클레임 등록을 확인하십시오.

장치 - 그룹

장치 그룹 추가

1. **개요** 창에서 장치 그룹을 만들 장치 유형을 마우스 오른쪽 단추로 클릭합니다.
2. **장치 그룹 추가** 를 선택합니다.
3. **장치 그룹 추가** 대화 상자에서 새 장치 그룹의 이름과 설명을 지정합니다.

장치 그룹 목록에서 해당 장치 그룹 위에 마우스 포인터를 멈추면 설명이 나타납니다.

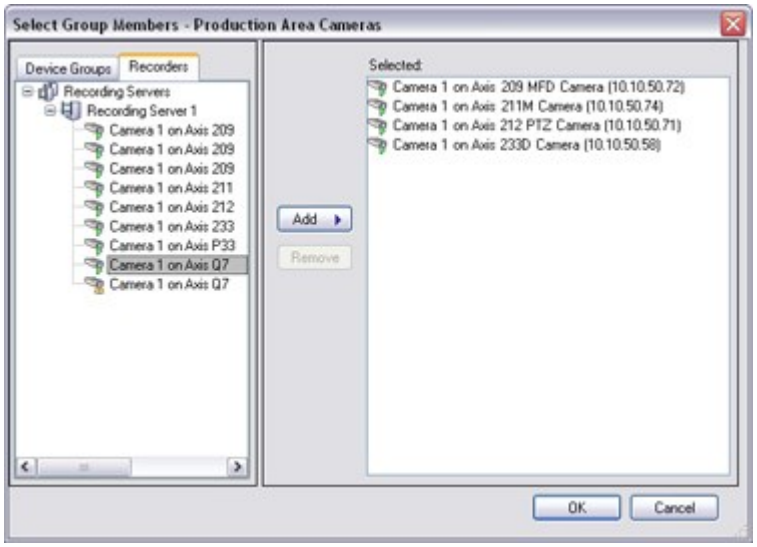
4. **확인** 을 클릭합니다. 새 장치 그룹을 나타내는 폴더가 목록에 나타납니다.
5. 계속해서 어떤 장치를 장치 그룹에 포함시킬지 지정합니다(페이지 207의 장치 그룹에 포함시킬 장치 지정 참조).

장치 그룹에 포함시킬 장치 지정

1. **개요** 창에서 해당 장치 그룹 폴더를 마우스 오른쪽 단추로 클릭합니다.
2. **장치 그룹 구성원 편집** 을 선택합니다.
3. **그룹 구성원 선택** 창에 있는 탭 중 하나를 선택하여 장치를 찾습니다.

   한 장치가 둘 이상의 장치 그룹 구성원일 수 있습니다.

4. 포함시킬 장치를 선택하고 **추가** 를 클릭하거나 장치를 두 번 클릭합니다.



5. **확인** 을 클릭합니다.
6. 한 그룹에 400개 장치 제한을 초과한 경우, 장치 그룹을 다른 장치 그룹의 하위 그룹으로 추가할 수 있습니다:

장치 비활성화됨

비활성화된 장치는 기본적으로 **개요** 창에 표시되지 않습니다.

비활성화된 모든 장치를 표시하려면 **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 열고 **비활성화된 장치 표시**를 선택합니다.

비활성화된 장치를 다시 숨기려면 **비활성화된 장치 표시**의 선택을 지웁니다.

장치 그룹의 모든 장치에 대한 공통 속성 지정

장치 그룹을 사용하면 주어진 장치 그룹 내의 모든 장치에 대해 공통 속성을 지정할 수 있습니다:

1. **개요** 창에서 장치 그룹을 클릭합니다.

   속성 창에서 **장치 그룹의 모든 장치에서 사용 가능** 한 전체 속성이 나열되고 탭에서 그룹화됩니다.

2. 해당하는 공통 속성을 지정합니다.

   설정 탭에서 **모든** 장치의 설정과 개별 장치의 설정을 상호 전환할 수 있습니다.

3. 도구 모음에서 **저장** 을 클릭합니다. 설정은 장치 그룹이 아닌 개별 장치에 저장됩니다.

장치 비활성화됨

비활성화된 장치는 기본적으로 **개요** 창에 표시되지 않습니다.

비활성화된 모든 장치를 표시하려면 **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 열고 **비활성화된 장치 표시**를 선택합니다.

비활성화된 장치를 다시 숨기려면 **비활성화된 장치 표시**의 선택을 지웁니다.

장치 그룹을 통한 장치 활성화/비활성화

구성된 하드웨어를 통해서만 장치를 활성화/비활성화할 수 있습니다. 하드웨어 추가 마법사에서 수동으로 활성화/비활성화하지 않는 한, 카메라 장치는 기본적으로 활성화되어 있고 다른 모든 장치는 기본적으로 비활성화되어 있습니다.

비활성화된 장치는 기본적으로 **개요** 창에 표시되지 않습니다.

비활성화된 모든 장치를 표시하려면 **개요** 창 상단에서 **필터**를 클릭하여 **필터** 탭을 열고 **비활성화된 장치 표시**를 선택합니다.

비활성화된 장치를 다시 숨기려면 **비활성화된 장치 표시**의 선택을 지웁니다.

장치 그룹을 통해 활성화 또는 비활성화할 장치를 찾으려면:

1. **사이트 탐색** 창에서 장치를 선택합니다.
2. **개요** 창에서 해당 그룹을 확장하고 장치를 찾습니다.
3. 장치를 마우스 오른쪽 버튼으로 클릭하고 **하드웨어로 이동** 을 선택합니다.
4. 더하기 노드를 클릭하면 하드웨어에 있는 모든 장치를 볼 수 있습니다.
5. 활성화/비활성화하려는 장치를 마우스 오른쪽 버튼으로 클릭하고 **활성화됨** 을 선택합니다.

장치 - 카메라 설정

카메라 설정 보기 또는 편집

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **설정** 탭을 엽니다.

다음과 같은 설정을 보거나 편집할 수 있습니다:

- 기본 프레임 속도
- 해상도
- 압축
- 키프레임 간 최대 프레임 수
- 선택한 카메라 또는 장치 그룹 내 모든 카메라의 화면상 날짜/시간/텍스트 표시

카메라의 드라이버에 따라 **설정** 탭의 내용이 달라집니다. 드라이버는 카메라 유형에 따라 다릅니다.

하나 이상의 스트림(예: MJPEG 및 MPEG-4/H.264/H.265)를 지원하는 카메라의 경우, 멀티 스트리밍을 사용할 수 있습니다. 페이지 216의 다중 스트림 관리를 참조하십시오.

미리보기

설정을 변경할 경우, **미리보기** 창을 활성화하면 해당 변경 내용의 영향을 빠르게 확인할 수 있습니다.

- **미리보기** 를 활성화하려면 **보기** 메뉴를 클릭하고 **미리보기 창** 을 클릭합니다.

미리보기 창의 축소판 이미지는 **옵션** 대화 상자에 정의된 다른 프레임 속도를 사용하기 때문에 프레임 속도 변경의 효과를 판단하는 데 **미리보기** 창을 사용할 수 없습니다.

성능

키프레임 간 최대 프레임 수 및 **키프레임 모드 간 최대 프레임 수**에 대한 설정을 변경한 경우, XProtect Smart Client에서 일부 기능의 성능이 저하될 수도 있습니다. 예를 들어, XProtect Smart Client 에서 비디오 표시를 시작하는 데 키프레임이 필요하므로 키프레임 간의 기간이 길어질수록 XProtect Smart Client 시작이 늦어집니다.

하드웨어 추가 중

시스템에 하드웨어를 추가하는 방법에 관한 자세한 정보는 페이지 197의 하드웨어 추가를 참조하십시오.

어안 렌즈 지원 활성화 및 비활성화

어안 렌즈 지원은 기본적으로 비활성화됩니다.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **어안 렌즈** 탭에서 **어안 렌즈 지원 활성화** 확인란을 선택하거나 선택 취소합니다.

어안 렌즈 설정 지정

1. **어안 렌즈** 탭에서 렌즈 유형을 선택합니다.
2. **카메라 위치/방향** 목록에서 카메라의 물리적 위치/방향을 지정합니다.
3. **ImmerVision Enables® panomorph RPL 번호** 목록에서 Registered Panomorph Lens(RPL) 번호를 선택합니다.

   이를 통해 카메라에 사용된 렌즈를 손쉽게 식별하고 올바르게 구성할 수 있습니다. 일반적으로 렌즈 자체나 렌즈가 들어 있던 박스에 RPL 번호가 적혀 있습니다. ImmerVision, Panomorph 렌즈 및 RPL에 관한 상세 내용은 Immervision 웹사이트(https://www.immervisionenables.com/)를 참조하십시오.

   일반 휘어짐 보정 렌즈 프로파일을 선택한 경우, 원하는 **시야** 를 구성하도록 하십시오.

장치 - 레코딩

레코딩 활성화/비활성화

레코딩은 기본적으로 활성화되어 있습니다. 레코딩을 활성화/비활성화하려면:

1. **사이트 탐색** 창에서, **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **녹화** 탭에서 **녹화** 확인란을 선택 또는 선택 취소합니다.

> 카메라에서 데이터를 기록하려면 장치에서 레코딩을 활성화해야 합니다. 장치 레코딩을 사용하지 않도록 설정한 경우, 장치가 레코딩하는 상황을 지정하는 규칙이 작동하지 않습니다.

관련 장치에서 레코딩 활성화

카메라 장치의 경우, 동일 레코딩 서버에 연결된 마이크로폰 등 관련 장치에 대해 레코딩을 사용하도록 설정할 수 있습니다. 즉, 카메라가 녹화할 때 관련 장치가 녹화를 수행합니다.

관련 장치에서 레코딩은 기본적으로 새 카메라 장치에 대해 활성화되어 있지만, 필요에 따라 비활성화하거나 활성화할 수 있습니다. 시스템의 기존 카메라 장치의 경우, 기본적으로 확인란 선택이 취소되어 있습니다.

1. **사이트 탐색** 창에서, **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 관련 카메라 장치를 선택합니다.
3. **녹화** 탭에서 **관련 장치 상의 녹화** 확인란을 선택 또는 선택 취소합니다.
4. **클라이언트** 탭에서 이 카메라와 관련된 장치를 지정합니다.

다른 레코딩 서버에 연결되어 있는 관련 장치에서 레코딩을 활성화하려는 경우, 규칙을 생성해야 합니다.

수동 레코딩 관리

다음 시간 이후 수동 레코딩 중지 는 기본적으로 5분 레코딩 시간으로 활성화되어 있습니다. 이는 시스템이 XProtect Smart Client 사용자에 의해 시작된 모든 레코딩을 자동으로 중지할 수 있게 하기 위함입니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **녹화** 탭에서 **이후 수동 레코딩 중지** 확인란을 선택 또는 선택 취소합니다.

활성화한 경우, 레코딩 시간을 지정합니다. 지정하는 분 수는 시스템에 과부하를 주지 않으면서 여러 수동 레코딩의 요구 사항을 수용할 수 있을 정도로 충분히 길어야 합니다.

역할에 추가:

장치 탭의 **규칙** 에 각 카메라의 클라이언트 사용자에게 수동 레코딩을 시작/중지할 권한을 부여해야 합니다.

규칙에 사용:

수동 레코딩과 관련된 규칙을 생성할 때 사용할 수 있는 이벤트는 다음과 같습니다:

- 수동 녹화 시작됨
- 수동 녹화 중지됨

레코딩 프레임 속도 지정

JPEG에 대한 레코딩 프레임 속도를 지정합니다.

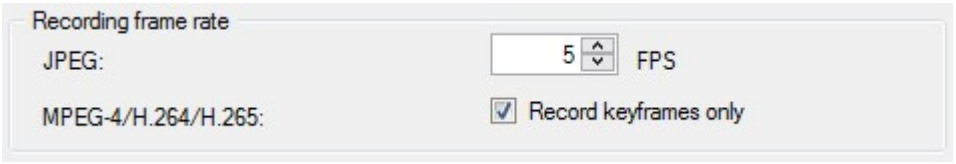
1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **녹화** 탭의 **레코딩 프레임 속도: (JPEG)** 상자, 레코딩 프레임속도를 선택하거나 입력합니다(FPS, 초당 프레임 단위로).

키프레임 레코딩 활성화

MPEG-4/H.264/H.265 스트림에 대해 키프레임 레코딩을 활성화할 수 있습니다. 즉, 시스템이 규칙 설정에 따라 키프레임만 레코딩 또는 모든 프레임 레코딩으로 전환됩니다.

예를 들어 뷰에 모션이 없을 경우 시스템이 키프레임을 레코딩하고, 저장소를 저장할 모션 감지가 있을 경우에만 모든 프레임으로 전환하게 할 수 있습니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **녹화** 탭에서 **키프레임만 녹화** 확인란을 선택합니다.



4. 기능을 활성화하는 규칙을 설정하려면 작업 및 작업 중지 를 참조하십시오.

관련 장치에서 레코딩 활성화

카메라 장치의 경우, 동일 레코딩 서버에 연결된 마이크로폰 등 관련 장치에 대해 레코딩을 사용하도록 설정할 수 있습니다. 즉, 카메라가 녹화할 때 관련 장치가 녹화를 수행합니다.

관련 장치에서 레코딩은 기본적으로 새 카메라 장치에 대해 활성화되어 있지만, 필요에 따라 비활성화하거나 활성화할 수 있습니다. 시스템의 기존 카메라 장치의 경우, 기본적으로 확인란 선택이 취소되어 있습니다.

1. **사이트 탐색** 창에서, **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 관련 카메라 장치를 선택합니다.
3. **녹화** 탭에서 **관련 장치 상의 녹화** 확인란을 선택 또는 선택 취소합니다.
4. **클라이언트** 탭에서 이 카메라와 관련된 장치를 지정합니다.

다른 레코딩 서버에 연결되어 있는 관련 장치에서 레코딩을 활성화하려는 경우, 규칙을 생성해야 합니다.

원격 레코딩 저장 및 검색

네트워크 문제 발생 시 모든 원격 레코딩이 저장되도록 하기 위해 연결이 재설정되면 자동 레코딩 검색을 활성화할 수 있습니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **원격 레코딩** 아래 **연결이 복원될 때 원격 녹화를 자동으로 검색** 을 선택합니다. 이렇게 하면 연결이 재설정되면 자동 레코딩 검색이 활성화됩니다.

원격 레코딩 옵션은 선택한 카메라가 에지 저장소를 지원하거나 Milestone Interconnect 설정에 속하는 카메라일 경우에만 사용할 수 있습니다.

선택한 하드웨어 유형에 따라 레코딩의 검색 위치가 결정됩니다:

- 로컬 레코딩 저장소가 있는 카메라의 경우, 레코딩이 카메라의 로컬 레코딩 저장소에서 검색됩니다
- Milestone Interconnect 원격 시스템의 경우는 레코딩이 원격 시스템의 레코딩 서버에서 검색됩니다.

자동 검색과는 별도로 다음의 기능을 사용할 수 있습니다:

- 수동 녹화
- **<장치>에서 원격 레코딩 검색 및 저장** 규칙
- **<장치>에서 <시작 및 종료 시간> 사이의 원격 레코딩 검색 및 저장** 규칙

녹화 삭제

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택한 후 **레코딩** 탭을 선택합니다.
3. **모든 레코딩 삭제** 버튼을 클릭하여 장치 또는 장치 그룹에서 모든 레코딩을 삭제합니다.

이 방법은 같은 서버에 그룹 내 모든 장치를 추가한 경우에만 사용할 수 있습니다. 보호된 데이터는 삭제되지 않습니다.

장치 - 스트리밍

적응 스트리밍(설명됨)

적응형 스트리밍은 여러 개의 라이브 비디오 스트림이 동일한 보기에 표시될 때 사용되는 스트리밍 방법입니다. 이는 클라이언트가 보기 항목에서 요청된 스트림에 가장 일치하는 해상도의 라이브 비디오 스트림을 자동으로 선택하는 것을 가능하게 합니다. 적응형 스트리밍은 네트워크 부하를 줄이고 디코딩 기능과 클라이언트 컴퓨터 성능을 개선합니다.

XProtect Smart Client에서 적응형 스트리밍을 활성화할 때는 보기 항목에서 요청한 해상도의 사용 가능한 비디오 스트림에 대해 가장 가깝게 일치하는 스트림을 설정할 수 있습니다. 자세한 정보는 적응형 스트리밍 활성화하기를 참고하십시오.

XProtect Smart Client에서는 적응형 스트리밍을 라이브 및 재생 모드에서 적용할 수 있습니다. 모바일 클라이언트에서는 라이브 모드에서만 사용할 수 있습니다.

재생 모드에서 적용할 때 이러한 스트리밍 방법을 적응형 스트리밍이라고 합니다. 자세한 정보는 페이지 214의 적응형 재생(설명됨)를 참조하십시오.

적응형 재생(설명됨)

적응형 재생은 재생 모드에서 적응형 스트리밍 사용을 허용하는 구성입니다.

적응형 재생을 하려면 기본 스트림과 보조 스트림이라는 이 두 가지 레코딩 스트림이 필요합니다. Management Client에서 두 스트림이 모두 활성화되어 있으면 두 스트림이 녹화됩니다.

- 보조 레코딩이 구성되기 이전 기간부터 비디오를 재생하면, 기본 레코딩만 재생됩니다.
- 보조 레코딩이 구성된 후 녹화된 비디오를 재생하면, 클라이언트 보기 크기와 가장 잘 일치하는 것에 따라 기본 또는 보조 레코딩에서 비디오가 재생됩니다.

가용성

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

어댑티브 스트리밍 활성화

Smart Client 프로필의 **고급** 탭에서 적응형 스트리밍과 함께 적응형 재생을 활성화할 수 있으며, **설정** > **고급** > **적응형 스트리밍**의 XProtect Smart Client에서도 활성화해야 합니다. XProtect Smart Client에서 적응형 스트리밍 활성화하기에 대한 자세한 정보는 적응 스트리밍 활성화를 참고하십시오.

원격 레코딩

적응형 재생을 위해 에지 레코딩을 선택하여 사용할 수 있습니다. 에지 레코딩을 사용하면 나머지 스트림과는 다른 해상도, 보통은 더 높은 해상도로 스트림 시퀀스를 볼 수 있습니다. 예를 들어, 낮은 해상도의 기본 스트림을 녹화하고 높은 해상도 소스의 레코딩을 병합할 수 있습니다. 데이터를 검색할 때 병합된 에지 레코딩을 활성화할 수 있습니다.

에지 레코딩은 미디어 데이터베이스에 저장되며 이러한 레코딩의 해상도는 개별 카메라에 설정되어 있습니다.

재생된 비디오의 해상도

적응형 재생을 사용하는 경우 재생된 비디오의 해상도는 기본 및 보조 레코딩의 현재 해상도 설정으로 결정됩니다. 즉, 재생 시 기본 스트림 또는 보조 스트림 중 하나를 선택하는 것은 각 레코딩 스트림에 대해 현재 설정된 해상도를 기반으로 합니다.

스트림 추가

레코딩을 위해 추가한 스트림은 라이브 및 재생 모드에서 볼 수 있습니다.

적응형 스트리밍이 활성화되어 있는 보기 항목에서 녹화된 비디오를 볼 수도 있습니다. 재생 모드에서의 적응형 스트리밍을 적응형 재생이라고 합니다.

1. **스트림** 탭에서 **추가** 를 클릭합니다. 이렇게 하면 목록에 두 번째 스트림이 추가됩니다.
2. **이름** 열에서 스트림의 이름을 편집합니다. 이 이름이 XProtect Smart Client 에 나타납니다.
3. **라이브 모드** 열에서 라이브 스트리밍이 필요한 때를 선택합니다:
   - **항상**: 스트림을 요청하는 XProtect Smart Client 사용자가 없더라도 스트림이 실행합니다.
   - **안 함**: 스트림이 꺼집니다. 예를 들어, 고품질의 레코딩을 원하고 대역폭이 필요한 경우, 레코딩 스트리밍에 대해서만 이 옵션을 사용하십시오
   - **필요할 때**: 클라이언트가 요청했을 때 또는 스트림이 녹화되도록 설정된 경우에 스트림이 시작됩니다.
4. **기본 라이브 스트림** 열에서 클라이언트가 특정 스트림을 요청하지 않고 적응형 스트리밍이 비활성화되어 있는 경우에 사용해야 하는 기본 스트림을 선택합니다.
5. **레코딩** 열에서 **기본** 또는 **보조**를 선택합니다. 적응형 재생을 위해 각 유형에 대한 스트림을 생성해야 합니다. 재생되는 비디오는 기본 비디오 스트림이 출처이며 필요한 경우 보조 스트리밍이 포함됩니다. 기본 레코딩은 항상 있어야 합니다. 또한, **기본**으로 구성한 스트림은 모션 감지 및 XProtect Smart Client에서 내보내기와 같은 다양한 맥락에서 사용됩니다.
6. **기본 재생**에서 어느 스트림을 기본으로 할지 선택합니다. 적응형 재생이 구성되지 않은 경우에는 기본 스트림이 클라이언트에 전달됩니다.
7. 원격 레코딩을 사용하고 싶은 경우 **원격 레코딩 사용** 열에서 확인란을 선택합니다. 에지 레코딩에 관한 자세한 정보는 페이지 214의 원격 레코딩을 참고하십시오.
8. **저장** 을 클릭하십시오.

> 다른 사람이 실시간 비디오를 시청하지 않는 한 스트림을 전혀 실행하지 않으려면 **기본 시작 피드 규칙** 을 요청할 경우 미리 정의된 **요청된 실시간 클라이언트 피드** 이벤트로 시작하도록 수정할 수 있습니다.

다중 스트림 관리

녹화된 라이브 비디오 보기와 비디오 재생의 비디오 품질 및 프레임 속도가 반드시 같아야 최상의 결과를 얻을 수 있는 것은 아닙니다.

레코딩에 사용할 스트림 변경하기

적응형 재생을 하려면 기본 스트림과 보조 스트림이라는 이 두 가지 스트림을 레코딩으로 설정해야 합니다. 라이브 스트리밍의 경우, 카메라가 지원하는 수만큼의 라이브 스트림을 설정하여 사용할 수 있습니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **스트림** 탭에서 레코딩에 사용하고 싶은 스트림을 선택합니다.
4. **라이브 모드** 목록에서 관련 옵션을 선택합니다. **필요한 경우**, **항상**, **안 함** 옵션은 클라이언트에서 스트림을 적용해야 하는 때를 의미합니다. 클라이언트에서 요청한 것이 아무것도 없으면 레코딩은 **기본 라이브 스트림** 확인란이 선택된 스트림을 사용합니다.
5. 하나의 스트림에서 녹화하려면 **레코딩** 목록에서 **기본** 또는 **보조**를 선택합니다.
6. 적응형 재생을 사용하려면 두 개의 스트림을 설정하고 스트림 중 하나를 **기본**으로 설정하고 다른 하나를 **보조**로 설정합니다.
7. 스트림에서 녹화하려면 **레코딩** 목록에서 **기본** 또는 **보조**를 선택합니다.

데이터 송신 제한

클라이언트가 볼 때에만 비디오 스트림이 작동하도록 일련의 조건을 설정할 수 있습니다.

스트리밍을 관리하고 불필요한 데이터 송신을 제한하기 위해 스트리밍은 다음 조건에서는 시작되지 않습니다:

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **스트림** 탭의 **라이브 모드** 목록에서 **필요 시** 를 선택합니다.
4. **녹화** 탭에서 **녹화** 확인란을 선택 취소합니다.
5. **모션** 탭에서 **모션 감지** 확인란을 선택 취소합니다.

이러한 조건이 맞는 경우, 비디오 스트림은 클라이언트가 볼 때에만 작동할 것입니다.

예시

예제 1, 라이브 및 레코딩된 비디오:

- **라이브** 비디오를 볼 때, 조직은 높은 프레임 속도의 H.264를 선호할 수 있습니다
- **레코딩된** 비디오 재생 시, 조직은 디스크 공간 절약을 위해 낮은 프레임 속도의 MJPEG를 선호할 수 있습니다

예제 2, 로컬 및 리모트 라이브 비디오:

- **로컬 연결 지점에서 라이브 비디오** 를 볼 때, 조직은 최고 품질의 비디오를 이용할 수 있도록 높은 프레임 속도의 H.264를 선호할 수 있습니다
- **원격으로 연결된 작동 지점에서 라이브 비디오** 를 볼 때, 조직은 네트워크 대역폭을 절약하기 위해 낮은 프레임 속도와 품질의 MJPEG를 선호할 수 있습니다

예제 3, 적응 스트리밍:

- **라이브 비디오 보기 및 XProtect Smart Client 컴퓨터의 CPU와 GPU 처리량을 줄이기 위해**, 조직은 적응 스트리밍 사용 시 XProtect Smart Client 에 의해 요청된 해상도에 일치하도록 서로 다른 해상도를 지닌 매우 높은 프레임 속도의 H.264/H.265를 선호할 수 있습니다. 자세한 정보는 페이지 428의 Smart Client 프로파일(클라이언트 노드)를 참조하십시오.

> 카메라의 **클라이언트** 탭에서 **라이브 멀티캐스트** 를 활성화하는 경우(클라이언트 탭(장치) 참조), 라이브 멀티캐스트는 기본 비디오 스트림에서만 작동합니다.

카메라가 멀티스트림을 지원하는 경우라도, 개별 멀티스트리밍 기능은 카메라마다 다를 수 있습니다. 자세한 내용은 카메라의 설명서를 참조하십시오.

카메라가 다른 유형의 스트림을 제공하는지 확인하려면 **설정 탭(장치)** 를 확인하십시오.

장치 - 저장소

사전 버퍼링 관리

카메라, 마이크 및 스피커가 사전 버퍼링을 지원합니다. 스피커의 경우, XProtect Smart Client 사용자가 **스피커에 말하기** 기능을 사용하는 경우에만 스트림이 전송됩니다. 즉, 레코딩할 스트림이 트리거되는 방식에 따라 사전 버퍼가 거의 불가능하거나 아예 사용할 수 없게 됩니다.

대부분의 경우 XProtect Smart Client 사용자가 **스피커에 말하기** 기능을 사용할 때 스피커가 레코딩하도록 설정합니다. 그러한 경우 스피커 사전 버퍼를 사용할 수 없습니다.

> 사전 버퍼 기능을 사용하려면 장치가 활성화되고 시스템으로 스트림을 전송 중이어야 합니다.

사전 버퍼링 활성화 및 비활성화

사전 버퍼링은 기본적으로 3초의 사전 버퍼 크기로 활성화되어 있으며 메모리에 저장됩니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택합니다.
3. **녹화** 탭에서 **사전 버퍼** 확인란을 선택 또는 선택 취소합니다.
4. **클라이언트** 탭에서 이 카메라와 관련된 장치를 지정합니다.

저장 위치와 사전 버퍼 기간 지정

임시 사전 버퍼 레코딩은 메모리 또는 디스크에 저장됩니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택한 후 **녹화** 탭을 선택합니다.
3. **위치** 목록에서 **메모리** 또는 **디스크** 를 선택한 후 초를 지정합니다.
4. 15초 이상의 사전 버퍼 기간이 필요한 경우, **디스크**를 선택합니다.

지정하는 초 수는 정의하는 여러 레코딩 규칙의 요구 사항을 수용할 수 있을 정도로 충분히 길어야 합니다.

위치를 **메모리** 로 변경하면 시스템이 해당 기간을 15초로 자동 축소합니다.

규칙에서 사전 버퍼 사용

레코딩을 트리거하는 규칙을 생성할 때, 실제 이벤트가 발생하기 약간 전에 레코딩이 시작하도록 선택할 수 있습니다(사전 버퍼).

예: 아래 규칙은 카메라에서 모션이 감지되기 5초 전에 카메라에서 레코딩을 시작하도록 지정하는 경우입니다.

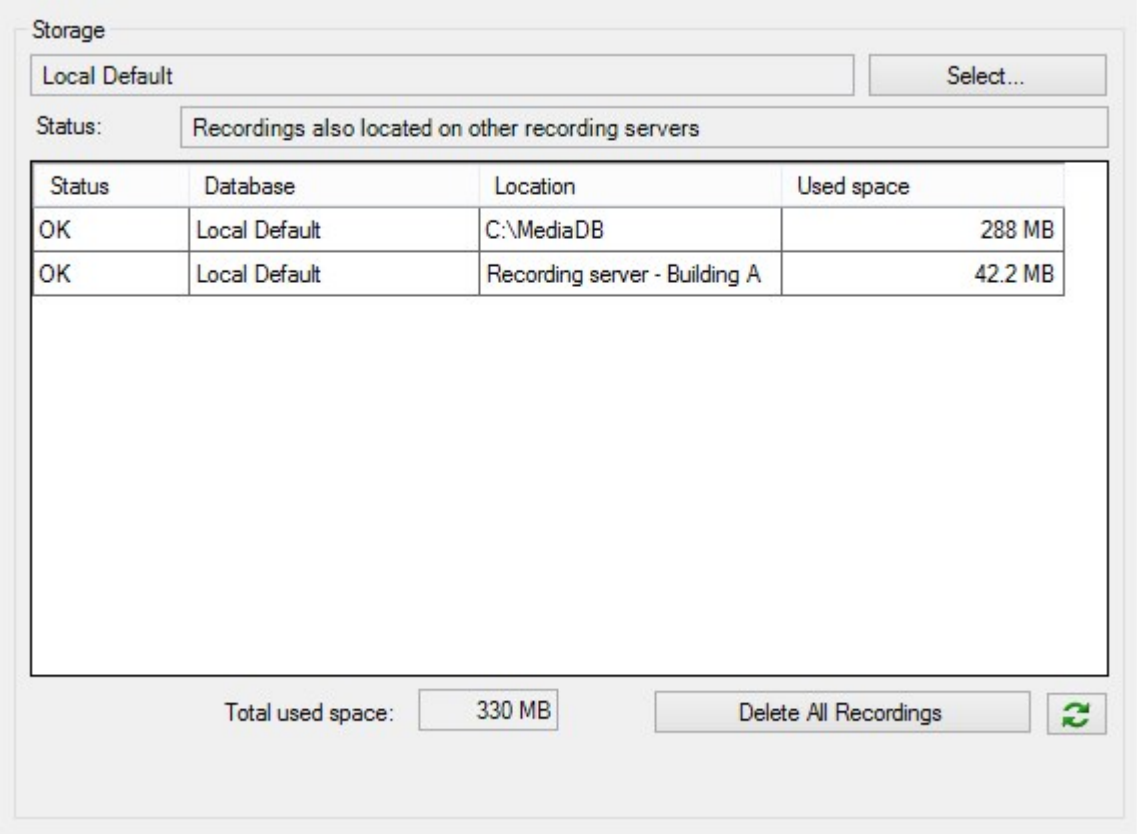
> 규칙에서 사전 버퍼 레코딩 기능을 사용하려면 레코딩할 장치에서 사전 버퍼링을 활성화하고, 최소한 규칙에 지정된 것과 동일한 길이로 사전 버퍼 길이를 설정해야 합니다.

장치에 대한 데이터 베이스 상태 모니터링

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택한 후 **레코딩** 탭을 선택합니다.

저장소 에서 동일한 레코딩 서버에 추가된 장치 또는 장치 그룹에 대한 데이터베이스를 모니터링하고 관리할 수 있습니다.

표 위에서 선택한 데이터베이스와 해당 상태를 볼 수 있습니다. 이 예제에서 선택한 데이터베이스는 **기본 로컬** 기본값이며 상태는 **녹화물이 다른 레코딩 서버에도 있음** 입니다. 다른 서버는 건물 A에 있는 레코딩 서버입니다.



선택한 데이터베이스에 대해 가능한 상태

이름	설명
다른 레코딩 서버에 이미 레코딩이 있습니다	데이터베이스가 활성 상태이고 실행 중이며 다른 레코딩 서버의 저장소에도 녹화물이 있습니다.
아카이브가 이전 저장소에도 있음	데이터베이스가 활성 상태이고 실행 중이며 다른 저장소에도 아카이브가 있습니다.
활성	데이터베이스가 활성 상태이고 실행 중입니다.
선택한 장치 중 일부에 대한 데이터가 현재 다른 위치로 이동 중입니다	데이터베이스가 활성 상태이고 실행 중이며 시스템이 그룹의 선택된 장치 하나 이상에 대한 데이터를 한 위치에서 다른 위치로 이동하는 중입니다.
장치에 대한 데이터가 현재 다른 위치로 이동 중입니다	데이터베이스가 활성 상태이고 실행 중이며 시스템이 선택한 장치의 데이터를 한 위치에서 다른 위치로 이동하는 중입니다.
장애 조치 모드에서는 정보를 사용할 수 없음	데이터베이스가 장애 조치 모드일 때는 시스템이 데이터베이스에 관한 상태 정보를 수집할 수 없습니다.

창의 더 아래 쪽에서는 각 데이터베이스의 상태(**정상**, **오프라인** 또는 **이전 저장소**), 각 데이터베이스의 위치 및 각 데이터베이스가 사용하는 공간의 양을 볼 수 있습니다.

모든 서버가 온라인이면 사용된 총 공간 필드에서 전체 저장소에 사용된 총 공간을 볼 수 있습니다.

저장소 구성에 관한 정보는 저장소 탭(레코딩 서버) 를 참조하십시오.

한 저장소에서 다른 저장소로 장치 이동

> 레코딩을 저장하기 위해 새로운 위치를 선택하면 기존 레코딩은 이동되지 않습니다. 기존 레코딩은 레코딩이 위치한 저장소의 구성에 의해 정의된 조건과 함께 현재 위치에 남아있게 됩니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 장치를 선택한 후 **레코딩** 탭을 선택합니다.
3. **저장소** 아래 **선택**을 클릭한 후 장치 레코딩이 저장될 레코딩 저장소를 선택합니다.

선택한 저장소에 대한 구성에 따라 레코딩이 아카이브됩니다.

장치 - 모션 감지

모션 감지(설명됨)

모션 감지 구성은 시스템의 주요 요소에 해당합니다: 모션 감지 구성은 시스템이 모션 이벤트를 생성할 때를 결정하며, 보통은 비디오가 녹화될 때에 해당합니다.

각 카메라에 대해 가능한 최고의 모션 감지 구성을 찾는 데 소요되는 시간은 예를 들어 이후의 불필요한 레코딩을 피하는 데 도움이 됩니다. 카메라의 물리적 위치에 따라 주간/야간, 바람 부는 날씨/고요한 날씨 등 서로 다른 물리적 조건 하에 모션 감지 설정을 테스트하는 것이 좋은 방법이 될 수 있습니다.

변경 내용을 모션으로 간주할 수 있도록 카메라의 뷰에서 필요한 변경 크기와 관련된 설정을 지정할 수 있습니다. 예를 들어, 모션 감지 분석과 모션이 무시되어야 할 뷰 영역 간의 인터벌을 지정할 수 있습니다. 모션 감지의 정확도를 조정하여 시스템 리소스에 로드할 수도 있습니다.

이미지 품질

카메라에 대한 모션 감지를 구성하기 전에 Milestone 은(는) 카메라의 이미지 품질 설정을 구성할 것을 권장합니다(예: 비디오 코덱 및 스트림 설정). 장치에 대한 윈도우의 **속성** 창의 **설정** 탭에서 구성할 수 있습니다. 나중에 이미지 품질 설정을 변경할 경우, 이후 항상 모션 감지 구성을 테스트해야 합니다.

사생활 보호

영구적 사생활 보호가 적용된 정의된 구역이 있는 경우, 이 영역 내에서는 모션을 감지하지 않습니다.

모션 감지 활성화 및 비활성화

카메라에 대한 동작 감지의 기본 설정 지정

1. **도구** 메뉴에서 **옵션** 을 클릭합니다.
2. **일반** 탭의 **새 카메라 장치 자동 추가 활성화 시** 아래, **동작 감지** 확인란을 활성화합니다.

특정 카메라에 대한 동작 감지 활성화 또는 비활성화

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **동작 탭** 탭에서 **동작 감지** 확인란을 선택하거나 선택 취소합니다.

카메라의 모션 감지를 비활성화하면 카메라에 대한 모든 감시 관련 규칙이 작동하지 않습니다.

하드웨어 가속화 활성화 또는 비활성화

동작 감지를 위한 자동 하드웨어 가속화 비디오 레코딩은 카메라 추가 시 기본 설정입니다. 레코딩 서버는 가능한 경우 GPU 자원을 사용합니다. 이 리소스는 비디오 모션 분석 중에 CPU 부하를 줄이고 레코딩 서버의 전체 성능을 개선합니다.

하드웨어 가속화 활성화 또는 비활성화하기

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **모션** 탭의 **하드웨어 가속화** 에서 **자동화** 를 선택하여 하드웨어 가속화를 활성화하거나 **끄기** 를 선택하여 설정을 비활성화합니다.

GPU 자원 이용

모션 감지 하드웨어 가속화 비디오 레코딩에는 다음과 같은 GPU 자원을 사용합니다.

- Intel Quick Sync를 지원하는 Intel CPU
- 레코딩 서버에 연결된 NVIDIA® 디스플레이 어댑터

로드 밸런싱 및 성능

서로 다른 리소스 간의 부하 밸런싱은 자동으로 수행됩니다. **시스템 모니터** 노드에서 NVIDIA GPU 리소스의 현재 모션 분석부하가 **시스템 모니터 임계치** 노드로부터 지정된 한계 내에 있는지 확인할 수 있습니다. NVIDIA GPU로드 인디케이터는 다음과 같습니다.

- NVIDIA 디코딩
- NVIDIA 메모리
- NVIDIA 렌더링

부하가 높을 경우, 멀티 NVIDIA 디스플레이 어댑터를 설치해 레코딩 서버에 GPU 리소스를 추가할 수 있습니다. Milestone 은(는) NVIDIA 디스플레이 어댑터의 Scalable Link Interface(SLI) 구성을 사용하지 않을 것을 권장합니다.

NVIDIA 제품은 다양한 연산 능력을 가지고 있습니다.

NVIDIA GPU를 사용한 모션 감지를 위한 하드웨어 가속화 비디오 레코딩에는 버전 6.x(Pascal) 또는 그 이상의 연산 능력이 필요합니다.

- NVIDIA 제품의 연산 능력 버전을 확인하려면 NVIDIA 웹사이트(https://developer.nvidia.com/cuda-gpus/)를 방문하십시오.
- 비디오 모션이 특정 카메라에 대해 하드웨어가 가속되었는지 확인하려면 레코딩 서버 로그 파일에 로깅을 활성화하십시오. 레벨을 **디버그**로 설정하십시오. 그러면 진단은 DeviceHandling.log.에 기록됩니다. 로그는 다음 패턴을 따릅니다:
  [time] [274] DEBUG – [guid] [name] 구성된 디코딩: 자동: 실제 디코딩: Intel/NVIDIA

레코딩 서버의 OS 버전과 CPU 세대는 하드웨어가 가속된 비디오 모션 감지의 성능에 영향을 줄 수 있습니다. GPU 메모리 할당은 대개 이전 버전의 병목 현상에 원인입니다(일반적인 한계는 0.5 GB ~ 1.7 GB).

Windows 10 / Server 2016 및 6세대 CPU(Skylake) 이상 기반의 시스템은 시스템 메모리의 50%를 GPU에 할당하므로 이 병목현상을 제거하거나 줄일 수 있습니다.

6세대 Intel CPU는 H.265의 하드웨어 가속 디코딩을 제공하므로, 성능은 이 버전의 CPU에 대해 H.264와 호환됩니다.

수동 감도를 활성화하여 동작 정의

감도 설정은 이미지 내의 **각 픽셀이 얼마나** 변경되어야 모션으로 간주되는지를 결정합니다.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **모션** 탭의 **수동 감도** 확인란을 선택합니다.

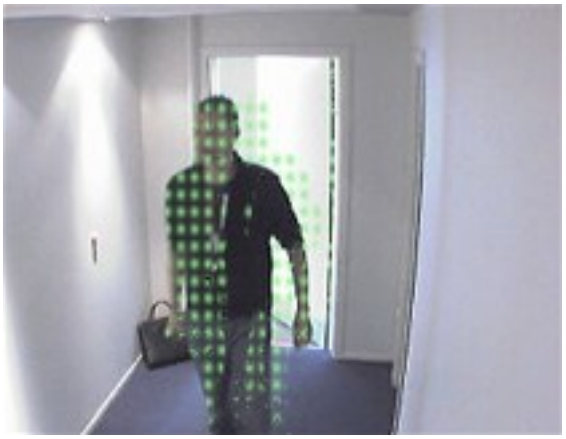
4. 감도 수준을 높이려면 슬라이더를 왼쪽으로 끌고, 감도 수준을 낮추려면 오른쪽으로 끕니다.

   감도 수준이 **높을수록** 각 픽셀에서 변경이 더 적어야 모션으로 간주됩니다.

   감도 수준이 **낮을수록** 각 픽셀에서 변경이 더 많아야 모션으로 간주됩니다.

   모션에서 감지되는 픽셀은 미리보기 이미지에서 녹색으로 강조 표시됩니다.

5. 모션이 강조 표시된 것으로 간주되는 감지에서만 슬라이더 위치를 선택합니다.



슬라이더 오른쪽의 번호를 기준으로 카메라 간의 정확한 감도 설정을 비교하고 설정할 수 있습니다.

모션 정의를 위한 임계값 지정

모션 감지 임계값은 이미지 내에서 **얼마나 많은 픽셀** 이 변경되어야 모션으로 간주되는지를 결정합니다.

1. 모션 수준을 높이려면 슬라이더를 왼쪽으로 끌고, 모션 수준을 낮추려면 오른쪽으로 끕니다.
2. 모션이 감지된 것으로 간주되는 감지에서만 슬라이더 위치를 선택합니다.

모션 표시 막대에서 검정색 세로선은 모션 감지 임계값을 나타냅니다: 선택한 감지 임계값 수준 이상의 모션이 감지될 경우, 막대의 색상이 녹색에서 빨간색으로 변경되어 감지 있음을 나타냅니다.

모션 표시 막대: 임계치 이상일 때 색상이 녹색에서 빨간색으로 변경되어 모션 감지가 있음을 나타냅니다.

모션 감지에 대한 제외 영역 지정

카메라 그룹에 대한 모든 설정을 구성할 수 있지만, 일반적으로 카메라마다 제외 영역을 설정합니다.

> 영구 사생활 보호 영역도 모션 감지에서 제외됩니다. 이를 표시하려면 **사생활 보호 표시** 확인란을 선택합니다.

특정 영역에서 모션 감지를 제외하면 관련이 없는 모션 감지를 피할 수 있습니다. 예를 들어, 바람에 의해 나무가 흔들리는 영역이나 배경에 자동차가 정기적으로 지나가는 영역을 카메라가 비추는 경우를 들 수 있습니다.

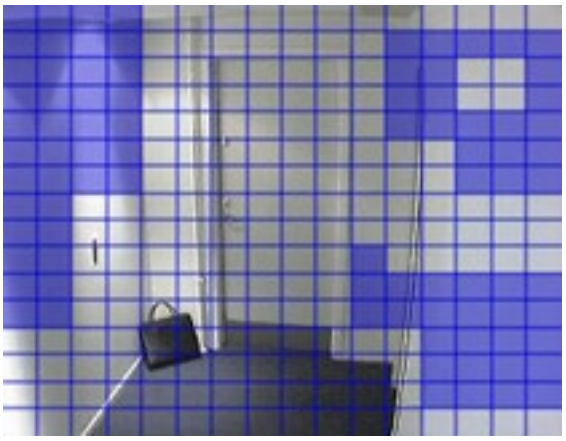
PTZ 카메라에서 제외 영역 기능을 사용하고 카메라를 이동-기울기-줌한 경우, 제외된 영역이 물체가 아닌 카메라 이미지로 잠기기 때문에 해당 영역이 카메라 이동에 따라 움직이지 **않습니다**.

1. 제외 영역을 사용하려면 **제외 영역 사용** 확인란을 선택합니다.

   그리드가 미리보기 이미지를 선택 가능한 섹션으로 나눕니다.

2. 제외 영역을 정의하려면 왼쪽 마우스 단추를 누른 상태에서 마우스 포인터를 미리보기 이미지에서 필요한 영역 위로 끕니다. 오른쪽 마우스 단추를 누르면 그리드 섹션의 선택이 취소됩니다.

필요한 수만큼 제외 영역을 정의할 수 있습니다. 제외 영역은 파란색으로 나타납니다.



파란색 제외 영역은 **모션** 탭의 미리보기 이미지에서만 나타나고, Management Client 또는 액세스 클라이언트의 다른 미리보기 이미지에서는 나타나지 않습니다.

장치 - 프리셋 카메라 위치

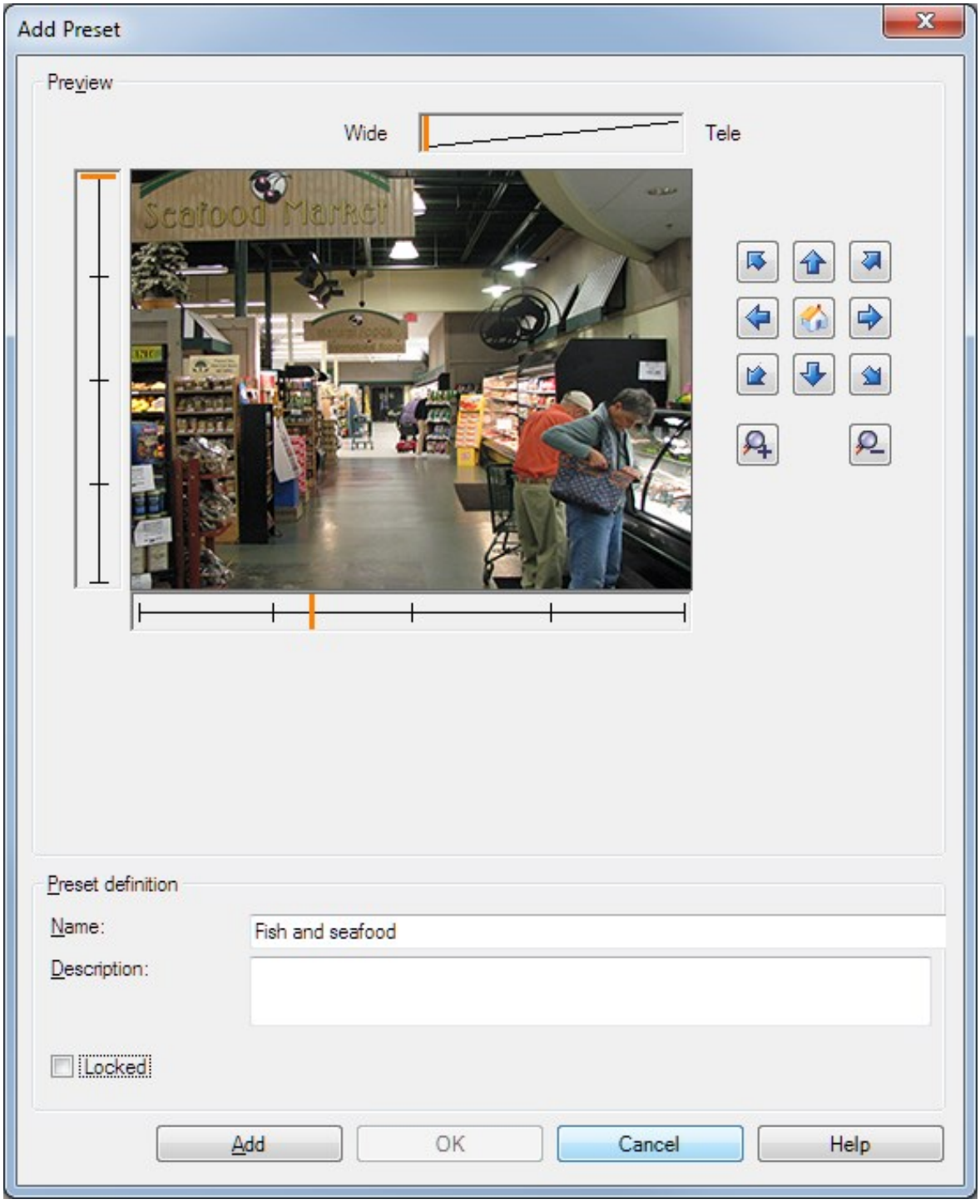
홈 사전 설정 위치

카메라 홈페이지에서 카메라의 홈 사전 설정 위치를 정의합니다. 홈페이지에서 사용할 수 있는 PTZ 기능은 카메라에 따라 다릅니다.

프리셋 위치(유형 1) 추가

카메라의 프리셋 위치를 추가하려면:

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **프리셋** 탭에서, **신규** 를 클릭합니다. **프리셋 추가** 창이 나타납니다.



4. **프리셋 추가** 창에 카메라의 라이브 미리보기 이미지가 표시됩니다. 탐색 단추 또는 슬라이더를 사용하여 카메라를 필요한 위치로 이동합니다.
5. **이름** 필드에 프리셋 위치의 이름을 지정합니다.
6. 원하는 경우 **설명** 필드에 프리셋 위치에 대한 설명을 입력합니다.
7. **프리셋** 위치를 잠그려면 잠금을 선택합니다. 충분한 권한을 가진 사용자만이 나중에 위치의 잠금을 해제할 수 있습니다.
8. 프리셋을 지정하려면 **추가** 를 클릭합니다. 필요한 프리셋이 모두 준비될 때까지 계속 추가합니다.
9. **확인** 을 클릭합니다. **프리셋 추가** 창이 닫히고, 해당 위치가 카메라에 대해 사용 가능한 프리셋 위치의 **프리셋** 탭 목록에 추가됩니다.

카메라의 프리셋 위치 사용(유형 2)

시스템에서 프리셋 위치를 지정하는 다른 방법으로, 카메라 자체에서 일부 PTZ 카메라의 프리셋 위치를 지정할 수 있습니다. 일반적으로 이 작업은 제품별 구성 웹 페이지에 액세스하여 수행할 수 있습니다.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **프리셋** 탭에서 **장치에서 프리셋 사용** 을 선택하여 시스템에 프리셋을 불러옵니다.

   이전에 카메라에 대해 정의한 모든 프리셋이 삭제되고 정의된 규칙과 순찰 일정에 영향을 끼치며, XProtect Smart Client 사용자에 대해 사용 가능한 프리셋이 제거됩니다.
4. 사용자에게 필요하지 않은 프리셋을 삭제하려면 **삭제** 를 클릭하십시오.
5. 사전설정 표시 이름을 변경하려면 **편집** 을 클릭합니다(프리셋 위치 이름 변경(유형 2만 해당) 참조).
6. 나중에 그러한 장치 정의 프리셋을 편집하려면 카메라에서 편집한 후 다시 가져오십시오.

카메라의 기본 프리셋 위치를 기본으로 할당

필요 시 PTZ 카메라의 프리셋 위치 중 하나를 카메라의 기본 프리셋 위치로 할당할 수 있습니다.

특정 상황에서 PTZ 카메라가 기본 프리셋 위치로 이동하도록(예: PTZ 카메라를 수동으로 조작한 후) 지정하는 규칙을 정의할 수 있으므로 기본 프리셋 위치를 설정하는 것이 유용할 수 있습니다.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **프리셋** 탭의 **프리셋 위치** 아래에서 정의된 프리셋 위치 목록의 프리셋을 선택합니다.
4. 목록 아래에서 **기본 프리셋** 확인란을 선택합니다.

하나의 프리셋 위치만 기본 프리셋 위치로 정의할 수 있습니다.

옵션 > **일반**에서 **기본 사전 설정을 PTZ 홈 위치로 사용**을 선택한 경우, PTZ 카메라의 정의된 홈 위치 대신 기본 사전 설정 위치가 사용됩니다.

기본 사전 설정을 PTZ 홈 위치로 지정

필요한 사용자 권한이 있는 Management Client 및 XProtect Smart Client 사용자는 클라이언트에서 **홈** 버튼으로 PTZ 카메라의 홈 위치 대신 기본 사전 설정 위치를 사용하도록 시스템을 설정할 수 있습니다.

카메라에 대해 기본 사전 설정 위치를 정의해야 합니다. 기본 사전 설정 위치가 정의되어 있지 않으면 클라이언트에서 **홈** 버튼을 활성화해도 아무 일도 일어나지 않습니다.

PTZ 홈 위치 설정 활성화

1. **도구** > **옵션**을 선택합니다.
2. **일반** 탭의 **레코딩 서버** 그룹에서 **기본 사전 설정을 PTZ 홈 위치로 사용**을 선택합니다.
3. 사전 설정 위치를 카메라의 기본 사전 설정 위치로 지정합니다.

기본 프리셋 위치를 지정하려면 페이지 226의 카메라의 기본 프리셋 위치를 기본으로 할당을(를) 참조하십시오.

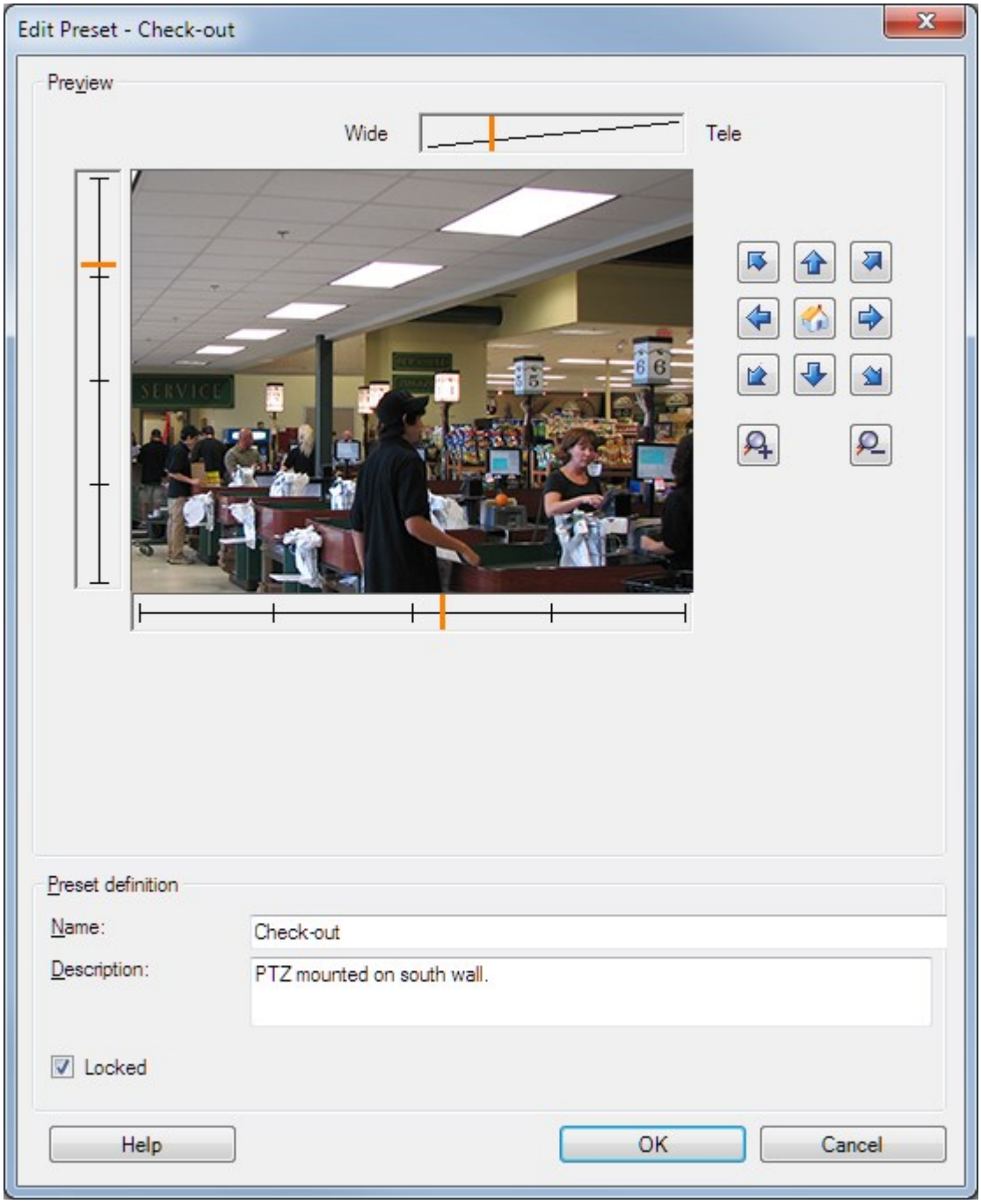
또한 페이지 353의 시스템 설정(옵션 대화 상자)를 참조하십시오.

카메라에 대한 프리셋 위치 편집(유형 1만 해당)

시스템에 정의된 기존의 프리셋 위치를 편집하려면:

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **프리셋** 탭의 프리셋 위치 아래에서 카메라에 대해 사용 가능한 프리셋 위치 목록 내 프리셋 위치를 선택합니다.

4. **편집** 을 클릭합니다. 이렇게 하면 **프리셋 편집** 창이 열립니다:



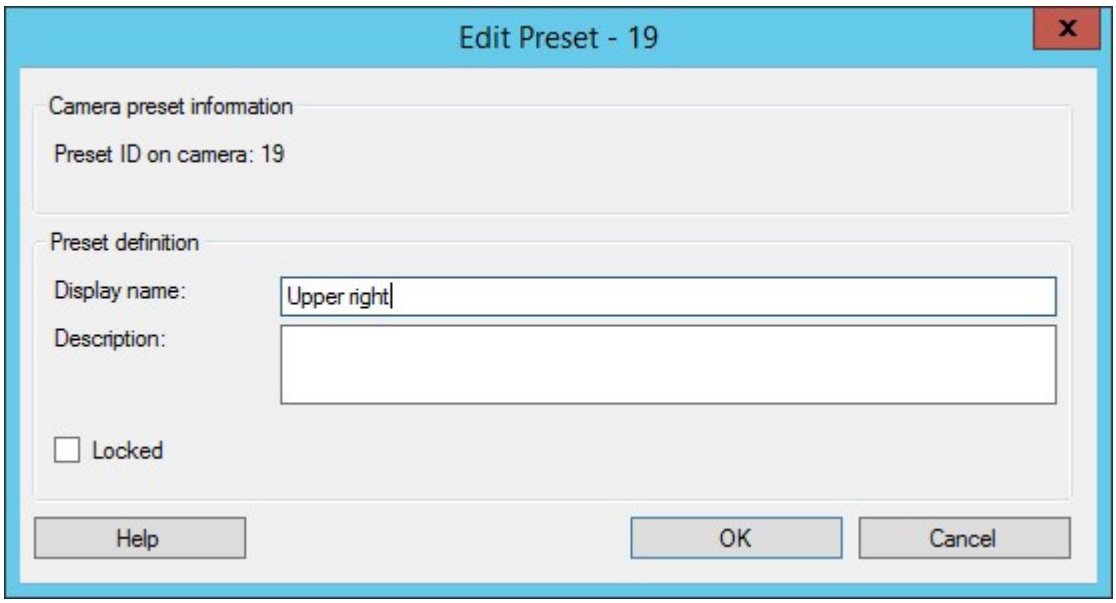
5. **프리셋 편집** 창에 프리셋 위치의 실시간 비디오가 표시됩니다. 탐색 단추 또는 슬라이더를 사용하여 필요에 따라 프리셋 위치를 변경합니다.
6. 필요 시 프리셋 위치의 이름/번호 및 설명을 변경합니다.
7. **프리셋**위치를잠그려면잠김을선택합니다.충분한권한을가진사용자만이나중에위치의잠금을해제할수있습니다.

8. **확인** 을 클릭합니다.

카메라에 대한 프리셋 위치 이름 변경(유형 2만 해당)

카메라에 정의된 프리셋 위치의 이름을 편집하려면:

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. 카메라에 대해 사용 가능한 프리셋의 **프리셋** 탭 목록에서 프리셋을 선택합니다.
4. **편집** 을 클릭합니다. 이렇게 하면 **프리셋 편집** 창이 열립니다:



5. 프리셋 위치의 이름을 변경하고 필요 시 설명을 추가합니다.
6. 프리셋 이름을 잠그려면 **잠김** 을 선택합니다. XProtect Smart Client 의 사용자 또는 제한적 보안 권한을 가진 사용자가 프리셋 이름을 업데이트하거나 프리셋을 삭제하지 못하게 하려는 경우 프리셋 이름을 잠글 수 있습니다.

   잠긴 프리셋은 아이콘으로 표시됩니다. 충분한 권한을 가진 사용자만이 나중에 프리셋 이름의 잠금을 해제할 수 있습니다.
7. **확인** 을 클릭합니다.

프리셋 위치 테스트(유형 1만 해당)

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **카메라에 대해 사용 가능한 프리셋의** 프리셋 탭 목록에서 프리셋 위치를 선택합니다.
4. **활성화** 를 클릭합니다.
5. 카메라가 선택한 프리셋 위치로 이동합니다.

장치 - 순찰

순찰 프로파일 및 수동 순찰(설명됨)

순찰 프로파일은 순찰이 이루어지는 방식에 대한 정의한 것입니다. 여기에는 프리셋 위치 간에 카메라가 이동하는 순서, 각 위치에서 카메라가 유지되는 길이가 포함됩니다. 무제한 수의 순찰 프로파일을 생성하여 규칙에서 사용할 수 있습니다. 예를 들어, 주간 영업 시간에 사용할 순찰 프로파일 하나와 야간 중에 사용할 또 다른 프로파일 하나를 지정하는 규칙을 만들 수 있습니다.

수동 순찰

예를 들어, 규칙의 순찰 프로파일을 적용하기 전에 수동 순찰을 이용해 순찰 프로파일을 테스트할 수 있습니다. 또한 PTZ 우선순위가 더 높다면 수동 순찰을 이용해 다른 사용자 또는 규칙에 따라 활성화된 순찰로부터 순찰을 가져올 수도 있습니다.

카메라가 이미 순찰 중이거나 다른 사용자가 제어 중인 경우, 더 높은 우선순위를 가진 경우에만 수동 순찰을 시작할 수 있습니다.

카메라가 규칙-활성화된 시스템 순찰을 실행하는 중에 수동 순찰을 시작하면, 사용자가 수동 순찰을 중지할 때 시스템은 이 순찰을 재개합니다. 다른 사용자가 수동 순찰을 실행할 때 더 높은 우선순위로 수동 순찰을 시작하면 다른 사용자의 수동 순찰이 다시 시작되지 않습니다.

수동 순찰을 직접 중단시키지 않으면 규칙 기반 순찰이 시작되거나 우선선위가 더 높은 사용자가 제어권을 가져갈 때까지 순찰이 계속됩니다. 규칙 기반 시스템 순찰이 중단되면 시스템이 사용자의 수동 순찰을 다시 시작합니다. 다른 사용자가 수동 순찰을 시작하면 사용자의 수동 순찰이 중단되고 다시 시작되지 않습니다.

수동 순찰을 중단하고 순찰 프로파일에 대한 종료 위치를 정의한 경우, 카메라는 이 위치로 돌아옵니다.

순찰 프로파일 추가

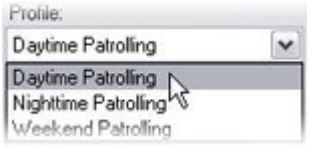
> 순찰 업무를 하기 전 카메라에 대한 프리셋 위치를 **프리셋** 탭에서 최소한 2개를 지정해야 합니다. 프리셋 위치 추가(유형 1) 을 참조하십시오.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **순찰** 탭에서, **추가** 를 클릭합니다. **프로파일 추가** 대화 상자가 나타납니다.
4. **프로파일 추가** 대화 상자에서 순찰 프로파일의 이름을 지정합니다.
5. **확인** 을 클릭합니다. 이름이 고유하지 않으면 버튼이 비활성화됩니다.

새로운 순찰 프로파일이 프로파일 목록에 추가됩니다. 이제 순찰 프로파일에 대한 프리셋 위치와 기타 설정을 지정할 수 있습니다.

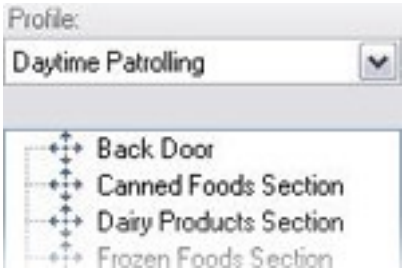
순찰 프로파일에 프리셋 위치 지정

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **순찰** 탭의 **프로파일** 목록에서 순찰 프로파일을 선택합니다.



4. **추가** 를 클릭합니다.
5. **PTZ 프리셋 선택** 대화 상자에서 순찰 프로파일에 대한 프리셋 위치를 선택합니다.

6. **확인** 을 클릭합니다. 선택한 프리셋 위치가 순찰 프로파일에 대한 프리셋 위치 목록에 추가됩니다.



7. 카메라는 순찰 프로파일에 따라 순찰할 때 목록 맨 위에 있는 프리셋 위치를 첫 번째 중지 위치로 사용합니다. 위에서 두 번째 위치에 있는 프리셋 위치가 두 번째 중지 위치로 사용되는 방식으로 계속됩니다.

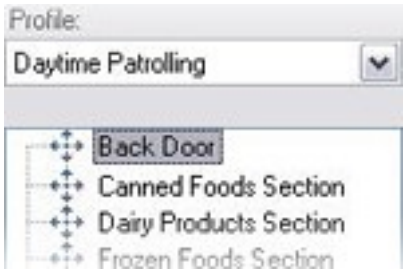
각 프리셋 위치에서 시간 지정

순찰 시 PTZ 카메라는 기본적으로 순찰 프로파일에 지정된 각 프리셋 위치에서 5초 동안 유지됩니다.

초 수를 변경하려면:

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **순찰** 탭의 **프로파일** 목록에서 순찰 프로파일을 선택합니다.

4. 시간을 변경할 프리셋 위치를 선택합니다:



5. **위치에서 시간(초)** 필드에 시간을 지정합니다.
6. 필요하면 다른 프리셋 위치에 대해 작업을 반복합니다.

전환 사용자 정의(PTZ)

기본적으로 카메라가 한 프리셋 위치에서 다른 위치로 이동(**전환** 이라고 함)하는 데 필요한 시간은 3초로 추정됩니다. 이 시간 동안에는 기본적으로 카메라에서 모션 감지가 비활성화됩니다. 그렇지 않으면 카메라가 프리셋 위치 간을 이동하는 동안 관련이 없는 모션이 감지될 수 있기 때문입니다.

사용 중인 카메라가 PTZ 스캔을 지원하고, 프리셋 위치가 구성되고 시스템 서버에 저장되는 유형(유형 1 PTZ 카메라)일 경우에만 전환 속도를 사용자 정의할 수 있습니다. **그렇지 않으면** 속도 슬라이더가 회색으로 표시됩니다.

다음을 사용자 정의할 수 있습니다:

- 예상 전환 시간
- 전환 중 카메라가 이동하는 속도

여러 프리셋 위치 간의 전환을 사용자 정의하려면:

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **순찰** 탭의 **프로필** 목록에서 순찰 프로파일을 선택합니다.
4. **전환 사용자 정의** 확인란을 선택합니다.

전환 표시가 프리셋 위치 목록에 추가됩니다.

5. 목록에서 전환을 선택합니다.

6. **예상 시간(초)** 필드에 예상 전환 시간(초를 숫자로)을 지정합니다.

7. **속도** 슬라이더를 사용하여 전환 속도를 지정합니다. 슬라이더가 맨 오른쪽 위치에 있으면 카메라가 기본 속도로 이동합니다. 슬라이더를 왼쪽으로 이동할수록 선택한 전환 중 카메라가 이동하는 속도가 느려집니다.
8. 다른 전환에 필요한 경우 이 과정을 반복하십시오.

순찰 시 종료 위치 지정

선택한 순환 프로파일에 따라 순찰이 끝날 때 카메라가 특정 프리셋 위치로 이동하도록 지정할 수 있습니다.

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **순찰** 탭의 **프리셋** 목록에서 순찰 프로파일을 선택합니다.
4. **종료 시 특정 위치로 이동** 확인란을 선택합니다. **이렇게 하면** 프리셋 선택 대화 상자가 열립니다.
5. 끝 위치를 선택하고 **확인**을 클릭합니다.

> 카메라의 어떤 프리셋 위치든 종료 위치로 선택할 수 있으며, 순찰 프로파일에 사용된 프리셋 위치로 제한되지 않습니다.

6. 선택한 종료 위치가 프로파일 목록에 추가됩니다.

선택한 순찰 프로파일에 따라 순찰이 끝나면 카메라가 지정된 종료 위치로 이동합니다.

PTZ 세션 보존 및 해제

사용 중인 감시 시스템에 따라 PTZ 세션을 예약할 수 있습니다.

예약된 PTZ 세션을 실행할 보안 권한을 가진 관리자가 이 모드에서 PTZ 카메라를 실행할 수 있습니다. 그러면 다른 사용자가 카메라에 대한 제어권을 가져가지 못합니다. 예약된 PTZ 세션에서는 더 높은 PTZ 우선순위를 가진 사용자가 세션을 중단하지 못하도록 표준 PTZ 우선순위 시스템이 무시됩니다.

XProtect Smart Client 및 Management Client 모두에서 예약된 PTZ 세션의 카메라를 조작할 수 있습니다.

PTZ 세션 예약은 다른 사용자의 방해를 받지 않고 PTZ 카메라나 그 프리셋을 긴급하게 업데이트하거나 관리해야 하는 경우 유용할 수 있습니다.

PTZ 세션 보존

1. **사이트 탐색** 창에서, **장치** 를 선택한 후 **카메라** 를 선택합니다.
2. **개요** 창에서 관련 PTZ 카메라를 선택합니다.
3. **프리셋** 탭에서 PTZ 세션을 선택한 후 **보존** 을 클릭합니다.

> 사용자보다 높은 우선 순위의 사용자가 카메라를 통제하거나 다른 사용자가 이미 해당 카메라를 보존한 경우 PTZ 세션 보존 시작을 할 수 없습니다.

PTZ 세션 해제

해제 버튼을 사용하여 다른 사용자가 카메라를 제어할 수 있도록 현재 PTZ 세션을 해제할 수 있습니다. **해제** 를 클릭하면 PTZ 세션이 즉시 중단되고 첫 번째 사용자가 카메라를 작동시킬 수 있게 됩니다.

PTZ 세션 해제 보안 권한을 할당받은 관리자는 언제든지 다른 사용자의 보존된 PTZ 세션을 해제할 권리를 보유합니다. 예를 들어, PTZ 카메라나 그 프리셋을 유지해야 하거나, 긴급한 상황에서 다른 사용자가 실수로 카메라를 차단시킨 경우에 유용할 수 있습니다.

PTZ 세션 시간 제한 지정

필요한 사용자 권한을 가진 Management Client 및 XProtect Smart Client 사용자가 PTZ 카메라 순찰을 수동으로 중단할 수 있습니다.

시스템에 있는 모든 PTZ 카메라에 대해 정기 순찰이 다시 시작되기 전에 경과해야 하는 시간을 지정할 수 있습니다.

1. **도구** > **옵션** 을 선택합니다.
2. **옵션** 창의 **일반** 탭에 있는 다음 항목에서 시간을 선택합니다.
   - **수동 PTZ 세션의 시간 제한** 목록(기본값은 15초).
   - **순찰 세션 일시 중지의 시간 제한** 목록(기본값은 10분).
   - **예약된 PTZ 세션의 시간 제한** 목록(기본값은 1시간).

   이 설정은 시스템의 모든 PTZ 카메라에 적용됩니다.

각 카메라에 대해 시간 제한을 개별적으로 변경할 수 있습니다.

1. **사이트 탐색** 창에서 **카메라** 를 클릭합니다.
2. 개요 창에서 카메라를 선택합니다.
3. **프리셋** 탭에 있는 다음 항목에서 시간을 선택합니다.
   - **수동 PTZ 세션의 시간 제한** 목록(기본값은 15초).
   - **순찰 세션 일시 중지의 시간 제한** 목록(기본값은 10분).
   - **예약된 PTZ 세션의 시간 제한** 목록(기본값은 1시간).

   설정은 이 카메라에만 적용됩니다.

장치 - 규칙에 대한 이벤트

장치에 대한 이벤트 추가 또는 삭제

이벤트 추가

1. **개요** 창에서 장치를 선택합니다.
2. **이벤트** 탭을 선택하고 **추가** 를 클릭합니다. 이렇게 하면 **드라이버 이벤트 선택** 창이 열립니다.
3. 이벤트를 선택합니다. 한 번에 하나의 이벤트만 선택할 수 있습니다.
4. 모든 이벤트의 전체 목록을 보고 이미 추가된 이벤트를 추가하려면 **이미 추가된 이벤트 보기** 를 선택하십시오.
5. **확인** 을 클릭합니다.
6. 도구 모음에서 **저장** 을 클릭합니다.

이벤트 삭제

> 이벤트를 삭제하면 해당 이벤트를 사용하는 모든 규칙에 영향을 줍니다.

1. **개요** 창에서 장치를
2. **이벤트** 탭에서 **삭제** 를 클릭합니다.

이벤트 속성을 지정합니다.

추가한 각 이벤트의 속성을 지정할 수 있습니다. 속성의 수는 장치와 이벤트에 따라 다릅니다. 이벤트가 계획대로 작동하기 위해서는 장치와 **[Events]** 탭의 일부 또는 모든 속성을 동일하게 지정해야 합니다.

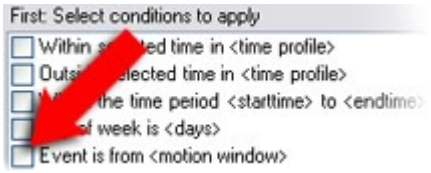
이벤트의 여러 인스턴스 사용

이벤트의 여러 인스턴스에 대해 서로 다른 속성을 지정할 수 있도록 이벤트를 한 번 이상 추가할 수 있습니다.

다음 예제는 카메라에 대한 것입니다.

예: A1 및 A2 라는 두 개의 모션 창을 사용하여 카메라를 구성했습니다. 모션 시작됨(HW) 이벤트에 대한 인스턴스 두 개를 추가했습니다. 한 인스턴스의 속성에서 모션 창 A1 사용을 지정했습니다. 다른 인스턴스의 속성에서 모션 창 A2 사용을 지정했습니다.

규칙에서 이 이벤트를 사용하는 경우, 규칙을 트리거하기 위해 이벤트가 특정 모션 창에서 발견된 모션을 기반으로 해야 함을 지정할 수 있습니다:



장치 - 사생활 보호

사생활 보호 활성화/비활성화

사생활 보호 기능은 기본적으로 비활성화되어 있습니다.

카메라의 사생활 보호 기능을 활성화/비활성화하려면:

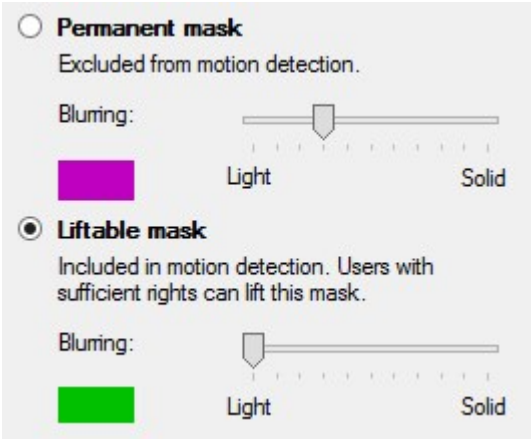
1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 카메라 장치를 선택합니다.
3. **사생활 보호** 탭에서 **사생활 보호** 확인란을 선택하거나 선택 취소합니다.

Milestone Interconnect 설치에서는 중앙 사이트가 원격 사이트에 정의된 사생활 보호를 무시합니다. 동일한 사생활 보호를 적용하려면 중앙 사이트에서 이를 다시 정의해야 합니다.

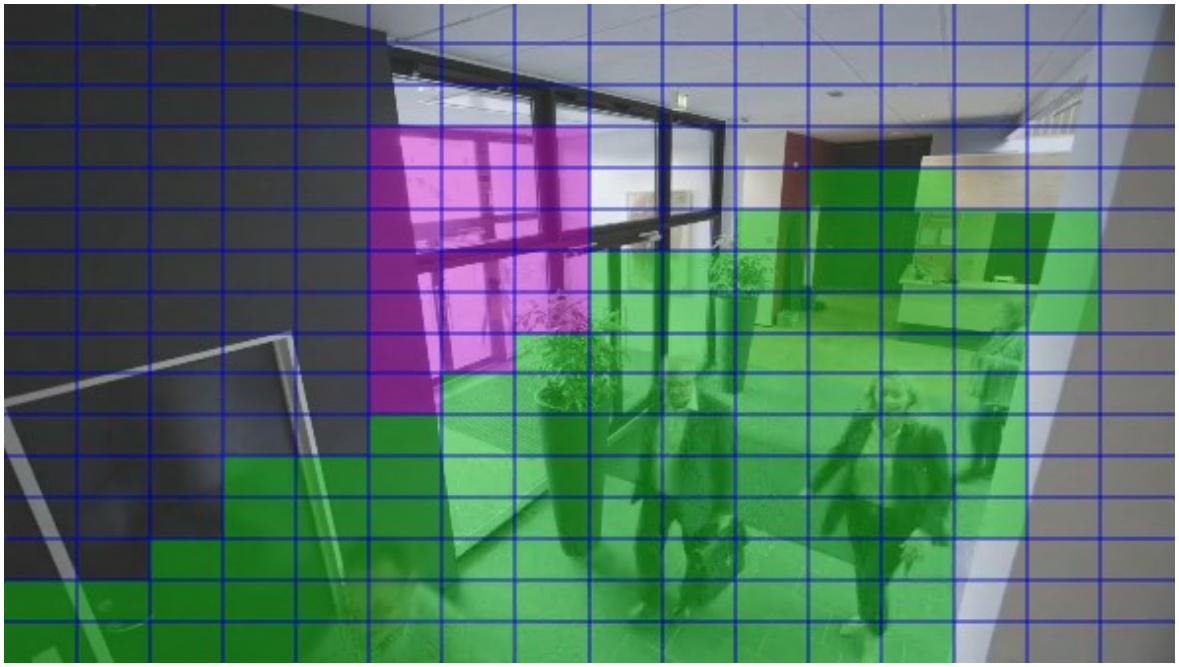
사생활 보호 정의

사생활 보호 탭에서 사생활 보호 기능을 활성화한 경우, 카메라 미리보기에 그리드가 적용됩니다.

1. **사이트 탐색** 창에서 **장치** 를 선택합니다.
2. **개요** 창에서 관련 카메라를 선택합니다.
3. **사생활 보호** 탭에서 사생활 보호 마스크로 일부 영역을 가리려면 우선 **영구적 마스크** 또는 **일시적 마스크** 를 선택하여 영구 또는 제거 가능 마스크를 원하는지 여부를 정의합니다.



4. 마우스 포인터를 미리보기로 끌어옵니다. 그리드 셀을 선택하려면 마우스 왼쪽 버튼을 클릭합니다. 그리드 셀을 비우려면 마우스 오른쪽 버튼을 클릭합니다.
5. 필요한 수만큼 사생활 보호 영역을 정의할 수 있습니다. 영구 사생활 보호 영역은 자주색으로 표시되며 해제 가능 사생활 보호는 녹색으로 표시됩니다.



6. 비디오에서 적용 영역이 클라이언트에 표시되는 방식을 정의합니다. 슬라이더를 이용해 약간 흐림에서 완전 불투명 마스크로 이동합니다.

   영구 사생활 보호는 **모션** 탭에도 표시됩니다.

7. XProtect Smart Client 에서 정의한대로 사생활 보호가 표시되는지 확인합니다.

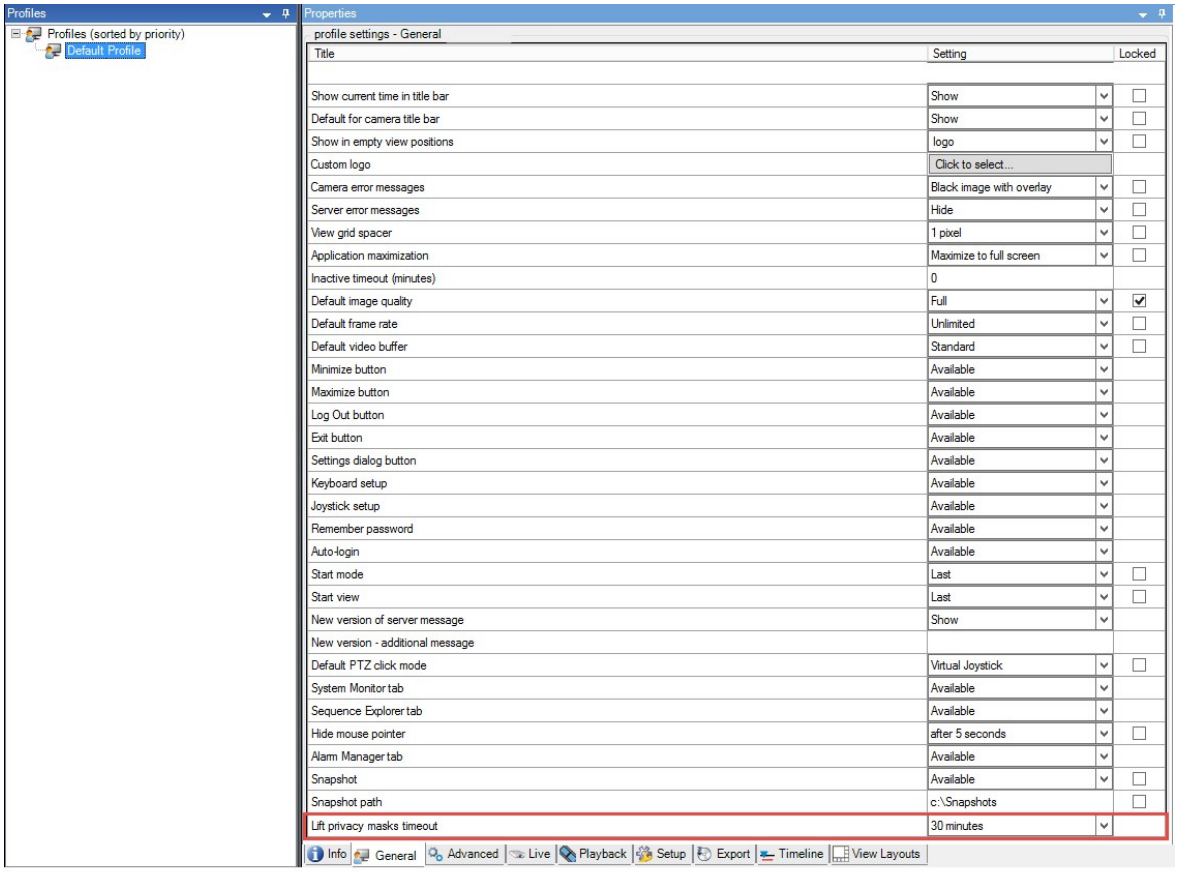
해제된 사생활 보호의 제한 시간 변경

기본적으로, 사생활 보호는 XProtect Smart Client 에서 30분 동안 해제되며 그 후 자동으로 적용되지만, 변경할 수 있습니다.

제한 시간을 변경할 경우 사생활 보호 해제 권한을 가진 역할과 연결된 Smart Client 프로파일에 대해서도 제한 시간을 변경한다는 점을 기억하십시오.

제한 시간을 변경하려면:

1. **Smart Client 프로필** 아래에서, 관련된 Smart Client 프로필을 선택합니다.
2. **일반** 탭에서, **사생활 보호 해제 제한 시간** 을 찾으십시오.



3. 다음 값 사이에서 선택합니다.
    - **2분**
    - **10분**
    - **30분**
    - **1시간**
    - **2시간**
    - **로그아웃할 때까지**
4. **저장** 을 클릭하십시오.

사용자에게 사생활 보호 해제 권한 부여

기본적으로, XProtect Smart Client 에서 사생활 보호 해제 권한을 가진 사용자는 없습니다.

권한을 활성화/비활성화하려면:

1. **사이트 탐색** 창에서, **보안** 을 선택한 후 **역할** 을 선택합니다.
2. 사생활 보호 설정을 제거할 권한을 주고자하는 역할을 선택하십시오.
3. **전체 보안** 탭에서, **카메라** 를 선택합니다.
4. **사생활 보호 해제** 권한에 대해 **허용** 을 선택합니다.

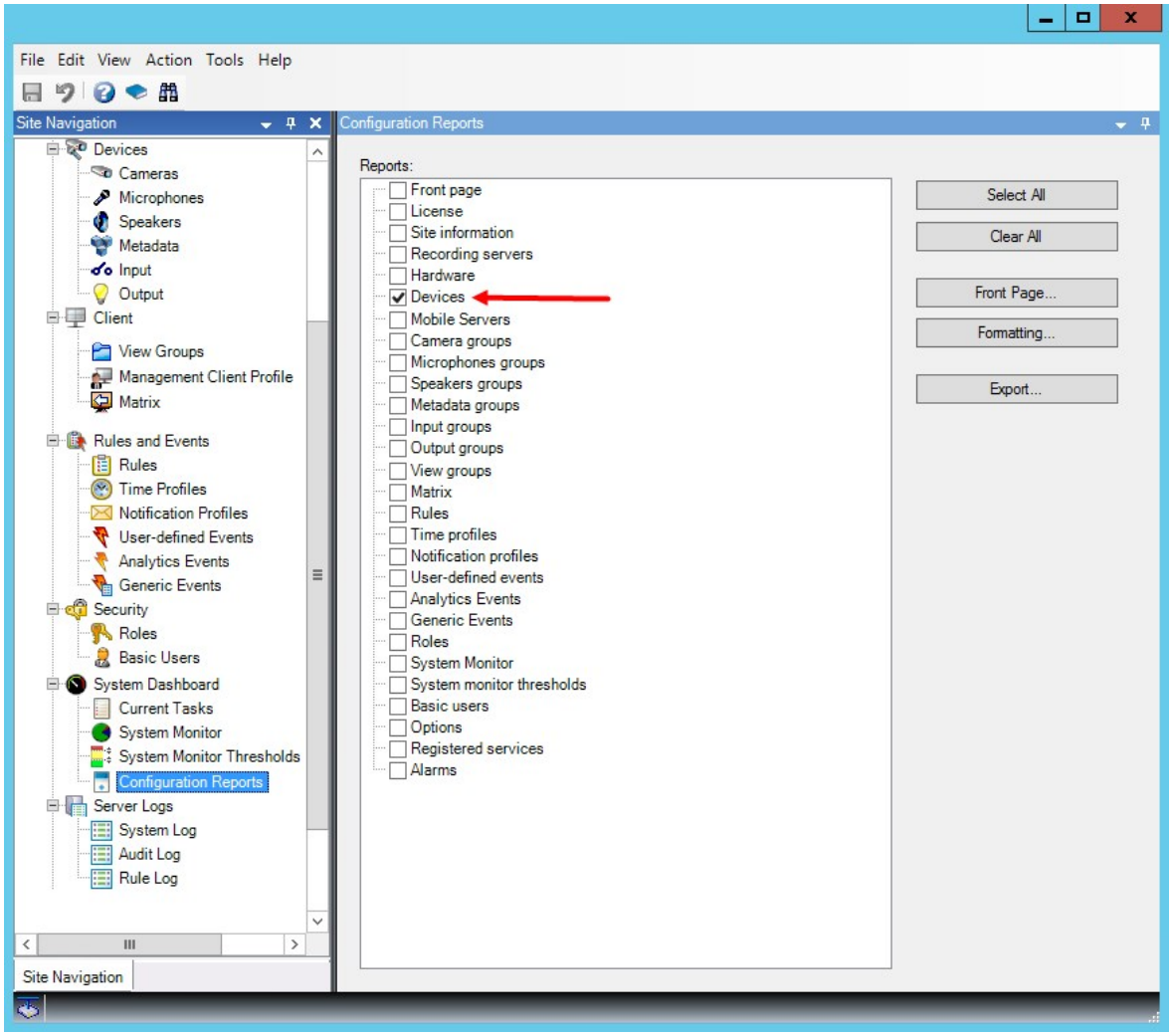
이 역할이 배정된 사용자는 자신에게 해제 가능 보호로 구성된 사생활 보호를 해제할 수 있을 뿐 아니라 기타 XProtect Smart Client 사용자에 대한 해제를 허가할 수 있습니다.

사생활 보호 구성에 대한 보고서 생성

장치 보고서에는 카메라의 현재 사생활 보호 설정에 대한 정보가 포함됩니다.

보고서를 구성하려면:

1. **사이트 탐색** 창에서 **시스템 대시보드** 를 선택합니다.
2. **구성 보고서** 아래에서, **장치** 보고서를 선택합니다.



3. 보고서를 수정하고자 할 경우, 전면 페이지와 서식을 변경할 수 있습니다.
4. **내보내기** 를 클릭하면, 시스템이 보고서를 PDF 파일로 생성합니다.

보고서에 관한 자세한 정보는 페이지 274의 시스템 구성이 포함된 보고서 출력를 참조하십시오.

클라이언트

뷰 그룹(설명됨)

시스템이 클라이언트에서 하나 이상 카메라의 비디오를 표시하는 방식을 뷰라고 합니다. 뷰 그룹은 그러한 뷰에 대한 하나 이상 논리적 그룹의 컨테이너입니다. 클라이언트에서 뷰 그룹은 사용자가 보고자 하는 그룹이나 뷰를 선택할 수 있는 확장 가능한 폴더로 나타납니다.

XProtect Smart Client 의 예: 화살표는 논리적 그룹(Amenities라고 함)을 포함하는 뷰 그룹을 나타내며, 여기에는 3개 뷰가 포함됩니다.

기본적으로 Management Client 에서 정의한 각 역할은 뷰 그룹으로도 생성됩니다. Management Client 에 역할을 추가하면 기본적으로 해당 역할이 클라이언트에서 사용할 뷰 그룹으로 나타납니다.

- 해당 역할에 할당된 사용자/그룹에 역할을 기반으로 뷰 그룹을 할당할 수 있습니다. 이후 역할에서 이 항목을 설정하여 해당 뷰 그룹 권한을 변경할 수 있습니다.
- 역할을 기반으로 한 뷰 그룹은 역할의 이름을 따릅니다.

  예: **보안 담당 직원 구성** 이라는 이름으로 역할을 만들면 XProtect Smart Client 에 **보안 담당 직원 구성** 이라는 뷰 그룹으로 나타납니다.

  역할을 추가할 때 구성한 뷰 그룹 이외에, 원하는 수만큼 다른 뷰 그룹을 생성할 수 있습니다. 또한 역할을 추가할 때 자동으로 생성된 그룹을 포함하여 뷰 그룹을 삭제할 수도 있습니다
- 뷰 그룹이 역할을 추가할 때마다 생성되지만 뷰 그룹이 역할에 해당될 필요는 없습니다. 필요한 경우 뷰 그룹을 추가하거나 이름을 바꾸거나 제거할 수 있습니다

> 뷰 그룹의 이름을 변경한 경우, 이미 연결된 클라이언트 사용자가 로그아웃한 후 다시 로그인해야 변경된 이름이 표시됩니다.

뷰 그룹 추가

1. **뷰 그룹** 을 마우스 오른쪽 단추로 클릭하고 **뷰 그룹 추가** 를 선택합니다. 이렇게 하면 **뷰 그룹 추가** 대화 상자가 열립니다.
2. 새 뷰 그룹의 이름과 선택적 설명을 입력하고 **확인** 을 클릭합니다.

> 그러한 권한을 지정하기 전까지는 역할에는 새로 추가한 뷰 그룹을 사용할 권한이 없습니다. 새로 추가한 뷰 그룹을 사용할 수 있는 역할을 지정했으면, 이미 연결되어 있으며 해당 역할과 관련된 클라이언트 사용자가 로그아웃한 후 다시 로그인해야 해당 뷰 그룹을 볼 수 있습니다.

Smart Client profiles

Smart Client 프로파일 추가 및 구성

Smart Client 프로파일을 만들어야 해당 프로파일을 구성할 수 있습니다.

1. **Smart Client 프로파일** 을 마우스 오른쪽 버튼으로 클릭합니다.
2. **Smart Client 프로파일 추가** 를 선택합니다.
3. **Smart Client 프로파일 추가** 대화 상자에서 새 프로파일의 이름과 설명을 입력하고 **확인** 을 클릭합니다.
4. **개요** 창에서 생성한 프로파일을 클릭하여 구성합니다.
5. 사용 가능한 하나 이상 또는 전체 탭에서 설정을 조정하고 **확인** 을 클릭합니다.

Smart Client 프로파일 복사

설정 또는 권한이 복잡한 Smart Client 프로파일이 있고 유사한 프로파일이 필요한 경우, 처음부터 새 프로파일을 만드는 것보다 기존의 프로파일을 복사해서 해당 복사본에 약간의 조정만 하는 편이 더 쉬울 수 있습니다.

1. **Smart Client 프로파일** 을 클릭하고 **개요** 창에서 해당 프로파일을 마우스 오른쪽 단추로 클릭하고 **Smart Client 프로파일 복사** 를 클릭합니다.
2. 나타나는 대화 상자에서 복사한 프로파일에 새로운 고유 이름과 설명을 지정합니다. **확인** 을 클릭합니다.
3. **개요** 창에서 방금 생성한 프로파일을 클릭하여 구성합니다. 사용 가능한 하나 이상 또는 전체 탭에서 설정을 조정해서 이 작업을 수행할 수 있습니다. **확인** 을 클릭합니다.

Smart Client 프로필과 역할, 시간 프로필 생성 및 설정

Smart Client 프로필을 사용할 때, Smart Client 프로필, 역할 및 시간 프로파일 간의 상호 작용을 반드시 이해해야 합니다.

- Smart Client 프로필은 XProtect Smart Client 의 사용자 권한 설정을 처리합니다.
- 역할은 클라이언트, MIP SDK 등에서 보안 설정을 처리합니다.
- 시간 프로파일은 두 가지 프로파일 유형의 시간 기능을 다룹니다.

이러한 세 가지 기능이 함께 XProtect Smart Client 사용자 권한과 관련하여 고유의 제어 및 사용자 정의 기능을 제공합니다.

예: XProtect Smart Client 설치에서 오직 일반 근무 시간(8시~16시) 중에 선택한 카메라의 라이브 뷰만 볼 수 있는(재생 없음) 사용자가 필요합니다. 이 설정의 한 가지 방식은 다음과 같이 할 수 있습니다:

1. Smart Client 프로파일을 만들고 이름을 지정합니다(예: **라이브만**).
2. **라이브만** 에서 필요한 라이브/재생 설정을 지정합니다.
3. 시간 프로파일을 만들고 이름을 지정합니다(예: **주간만**).
4. **주간만** 에서 필요한 시간 길이를 지정합니다.
5. 새 역할을 만들고 이름을 지정합니다(예: **가드(선택한 카메라)**).
6. **가드(선택한 카메라)** 가 사용할 수 있는 카메라를 지정합니다.
7. **라이브 전용** Smart Client 프로파일 및 **주간 전용** 시간 프로파일을 **가드(선택한 카메라)** 역할에 할당하여 3개 요소를 연결합니다.

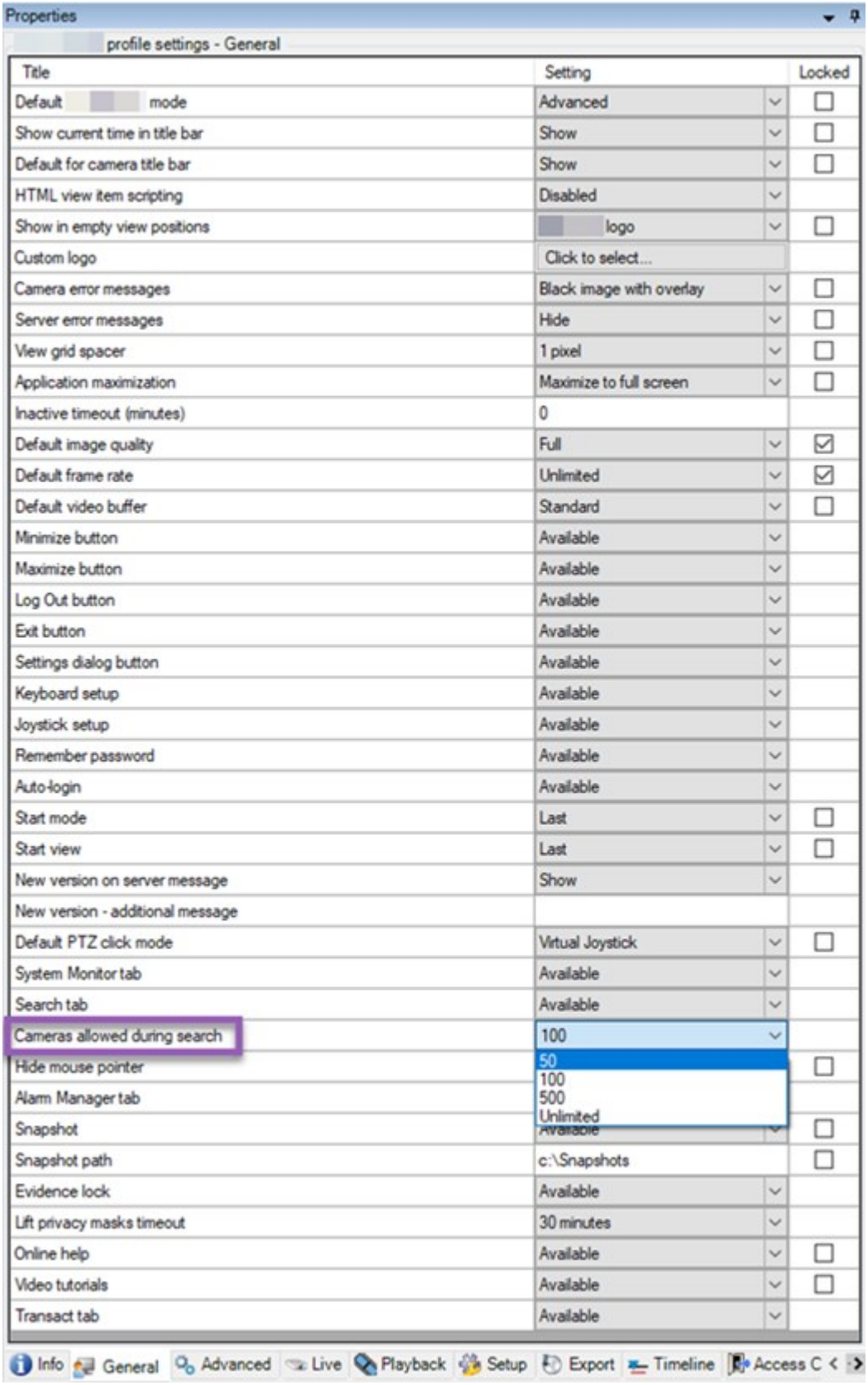
이제 3가지 기능을 혼합하여 원하는 결과를 생성하고 쉬운 미세 조절과 조정을 위한 공간을 확보할 수 있게 되었습니다. 또한 다른 순서로 설정을 수행할 수도 있습니다. 예를 들어, 역할을 먼저 만든 다음, Smart Client 프로필과 시간 프로파일을 만들거나, 기타 원하는 순서로 설정할 수 있습니다.

검색 중 허용된 카메라의 수 설정

운영자가 XProtect Smart Client 의 검색에 추가할 수 있는 카메라의 수를 구성할 수 있습니다. 기본값은 **100** 입니다. 카메라 한계치를 벗어나는 경우 운영자가 경고 메시지를 받게 됩니다.

1. XProtect Management Client에서 **클라이언트** > **Smart Client 프로필**을 확장합니다.
2. 관련 프로파일을 선택합니다.

3. **일반** 탭을 클릭합니다.


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. 검색 중에 허용된 **카메라**에서 다음 중 하나의 값을 선택합니다.
    - **50**
    - **100**
    - **500**
    - **무제한**
5. 변경 내용을 저장합니다.

기본 내보내기 설정 변경

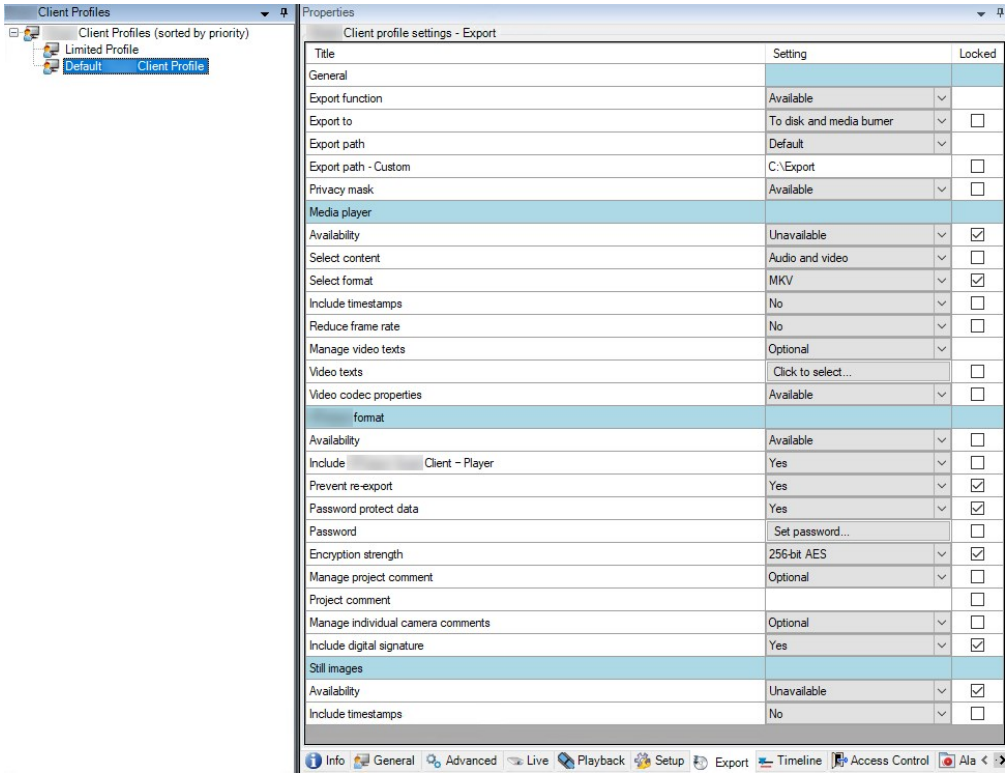
XProtect Smart Client VMS 시스템을 설치할 때 XProtect에서 내보내기 옵션을 정의하는 기본 내보내기 설정은 최고 수준의 보안을 구현하기 위해 제한됩니다. 이 설정을 변경하여 운영자에게 더 많은 옵션을 제공할 수 있습니다.

기본 설정

- XProtect 형식만 사용 가능
    - 다시 내보내기 방지
    - 내보내기는 암호로 보호됨
    - 256비트 암호화
    - 디지털 서명이 추가됨
- MKV 형식 또는 AVI 형식으로 내보낼 수 없음
- 정지 이미지를 내보낼 수 없음

단계:

1. XProtect Management Client에서 **클라이언트** > **Smart Client 프로필**을 확장합니다.
2. **기본 Smart Client 프로필**을 선택합니다.
3. **속성** 창에서 **정보** 탭을 선택합니다.



4. XProtect Smart Client에서 제한된 형식을 사용할 수 있게 하려면 설정을 찾아 **사용 가능**을 선택합니다.
5. 운영자가 XProtect Smart Client에서 설정을 변경할 수 있도록 하려면 관련 설정 옆에 있는 **잠김** 확인란의 선택을 취소합니다.
6. 해당하는 경우, 그 밖의 설정을 변경합니다.
7. (선택 사항) XProtect Smart Client에 로그인하여 설정이 적용되었는지 확인합니다.

Management Client profiles

Management Client 프로파일 추가 및 구성

기본 프로파일을 사용하지 않으려면 구성하기 전에 Management Client 프로파일을 만들 수 있습니다.

1. **Management Client 프로파일** 을 마우스 오른쪽 버튼으로 클릭합니다.
2. **Management Client 프로파일 추가** 를 선택합니다.

3. **Management Client 프로파일 추가** 대화 상자에서 새 프로파일의 이름과 설명을 입력하고 **확인** 을 클릭합니다.
4. **개요** 창에서 생성한 프로파일을 클릭하여 구성합니다.
5. **프로파일** 탭에서, Management Client 프로파일에서 기능을 선택하거나 선택 취소합니다.

Management Client 프로파일 복사

다시 사용하려는 설정을 가진 Management Client 프로파일이 있을 경우, 새 프로파일을 처음부터 만드는 대신 기존 프로파일을 복사하고 해당 복사본을 약간만 수정할 수 있습니다.

1. **Management Client 프로파일** 을 클릭하고 **개요** 창에서 해당 프로파일을 마우스 오른쪽 버튼으로 클릭한 다음 **Management Client 프로파일 복사** 를 클릭합니다.
2. 나타나는 대화 상자에서 복사한 프로파일에 새로운 고유 이름과 설명을 지정합니다. **확인** 을 클릭합니다.
3. **개요** 창에서 프로파일을 클릭하고 **정보** 탭이나 **프로파일** 탭으로 이동하여 프로파일을 구성합니다.

Management Client 프로파일에 대한 기능 표시 관리

각 관리자 역할에서 사용 가능한 기능을 표시하도록 사용자 인터페이스를 제한하려면 Management Client 프로파일을 해당 역할에 연결합니다.

역할과 Management Client 프로파일 연결

1. **보안** 노드를 확장하고 **역할** 을 클릭합니다.
2. **역할 설정** 창의 **정보** 탭에서 프로파일과 역할을 연결합니다. 자세한 정보는 정보 탭(역할) 을 참조하십시오.

역할에 대한 전반적인 시스템 기능 액세스 관리

Management Client 프로필은 실제 액세스가 아닌 시스템 기능의 시각적 표시만 처리합니다.

역할에 대한 전반적인 시스템 기능 액세스 관리:

1. **보안** 노드를 확장하고 **역할** 을 클릭합니다.
2. **전체 보안** 탭을 클릭하고 적절한 확인란을 선택합니다. 자세한 정보는 페이지 465의 전체 보안 탭(역할)를 참조하십시오.

전체 보안 탭에서 Management Server 에 대한 모든 역할 액세스를 허용하려면 **연결** 보안 권한을 올바르게 활성화하십시오.

기본 제공 관리자 역할 외에 전체 보안 Management Client 탭에서 관리 서버에 대해 보안 관리 권한을 부여 받은 역할과 연결된 사용자만 프로파일을 추가, 편집 및 삭제할 수 있습니다.

프로파일에 대한 기능 표시 제한

Management Client 모든 요소의 표시 여부에 대한 설정을 변경할 수 있습니다. Management Client 기본적으로 Management Client 프로파일은 의 모든 기능을 볼 수 있습니다.

1. 클라이언트 노드를 확장하고 Management Client 프로파일을 클릭합니다.
2. 프로파일을 선택하고 프로파일 탭을 클릭합니다.
3. 이 Management Client 프로필과 연결된 역할을 가진 모든 Management Client 사용자에 대해 Management Client 에서 기능을 시각적으로 제거할 수 있도록 관련 기능에 대한 확인란의 선택을 취소합니다.

Matrix

Matrix 및 Matrix 수신자(설명됨)

Matrix 은(는) 비디오를 원격으로 배포하기 위한 기능입니다.

Matrix 수신자는 XProtect Smart Client 가 있는 컴퓨터로 Matrix 내 Management Client 수신자로 정의됩니다.

Matrix을(를)사용하면,시스템네트워크상의모든카메라에서비디오를Matrix을(를)구동하는수신자에푸시할수있습니다.

Matrix 에 추가된 Management Client 수신자 목록을 보려면 **사이트 탐색** 창에서 **클라이언트** 를 확장한 후 **Matrix** 을(를) 선택합니다. Matrix 구성 목록은 **속성** 창에 표시됩니다.

ManagementClient에서Matrix이(가)트리거한비디오를수신할각Matrix수신자를추가해야합니다.

Matrix 수신자에게 비디오를 전송하는 규칙 정의

비디오를 Matrix 수신자에게 전송하려면 관련 Matrix 수신자에게 비디오 전송을 트리거하는 규칙에 Matrix 수신자를 포함시켜야 합니다. 이렇게 하려면 다음과 같이 하십시오.

1. **사이트 탐색** 창에서 **규칙 및 이벤트** > **규칙** 을 확장합니다. **규칙** 을 마우스 오른쪽 단추로 클릭하여 **관리 규칙** 마법사를 엽니다. 첫 번째 단계에서 규칙 유형을, 두 번째 단계에서 조건을 선택합니다.
2. **규칙 관리** 의 3단계(**3단계: 동작**)에서 **설정 Matrix 을 선택하여 <장치>** 동작을 확인합니다.
3. 초기 규칙 설명에서 Matrix 링크를 클릭합니다.
4. **Matrix 구성 선택** 대화 상자에서 해당 Matrix 수신자를 선택하고 **확인** 을 클릭합니다.
5. 초기 규칙 설명에서 **장치** 링크를 클릭하고 비디오를 Matrix 수신자에게 전송하려는 카메라를 선택한 다음, **확인** 을 클릭해서 선택을 확인합니다.
6. **규칙이 완료되면** 마침을 클릭하고, 필요하면 추가 동작 및/또는 중지 동작을 정의합니다.

Matrix 수신자를 삭제하면 Matrix 수신자를 포함하는 모든 규칙이 작동을 멈춥니다.

Matrix 수신자 추가

Matrix 내 기존 Management Client 수신인 추가하기:

1. **클라이언트** 를 확장한 다음, **Matrix** 을(를) 선택합니다.
2. **Matrix 구성** 을 마우스 오른쪽 단추로 클릭하고 **Matrix 추가** 를 선택합니다.
3. 추가 **Matrix** 대화 상자의 필드를 채웁니다.
    1. **주소** 필드에 필요한 Matrix 수신자의 IP 주소 또는 호스트 이름을 입력합니다.
    2. **포트** 영역에서 Matrix 수신자 설치에 의해 사용된 포트 번호를 입력합니다.
4. **확인** 을 클릭합니다.

이제 규칙에서 Matrix 수신자를 사용할 수 있습니다.

사용 중인 시스템은 지정한 포트 번호 또는 암호가 올바른지, 지정한 포트 번호, 암호 또는 유형이 실제 Matrix 수신자에 해당하는지 확인하지 않습니다. 올바른 정보를 입력하도록 하십시오.

동일 비디오를 여러 XProtect Smart Client 뷰로 전송

뷰의 Matrix 위치가 동일한 포트 번호 및 암호를 공유한다는 전제 하에 다수의 XProtect Smart Client 뷰에 있는 Matrix 위치로 동일한 비디오를 전송할 수 있습니다.

1. XProtect Smart Client 에서 해당 뷰 및 동일 포트 번호와 암호를 공유하는 Matrix 위치를 생성합니다.
2. Management Client 에서 해당 XProtect Smart Client 를 Matrix 수신자로 추가합니다.
3. 규칙에 Matrix 수신자를 포함시킬 수 있습니다.

규칙 및 이벤트

규칙 추가

규칙 추가 시 관련 옵션만 나열하는 **규칙 관리** 마법사의 안내를 받습니다.

이렇게 하면 필요한 요소가 규칙에서 누락되지 않게 됩니다. 또한 규칙의 내용을 토대로, 규칙이 더 이상 적용되지 않을 때 발생할 적합한 중지 동작을 자동으로 안내하므로 의도치 않게 계속해서 적용되는 규칙을 만들 염려가 없습니다.

이벤트

이벤트 기반 규칙을 추가할 때 다양한 이벤트 유형을 선택할 수 있습니다.

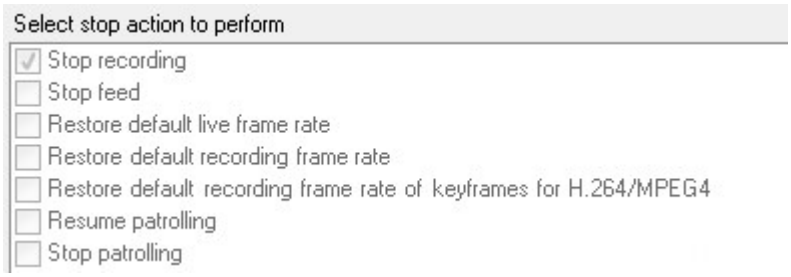
- 선택할 수 있는 이벤트 유형에 대한 개요 및 설명을 보려면 이벤트 개요 를 참조십시오.

동작 및 중지 동작

규칙을 추가할 때 다양한 동작을 선택할 수 있습니다.

일부 동작에는 중지 동작이 필요합니다. 예를 들어 **레코딩 시작** 동작을 선택하는 경우, 레코딩이 시작되며 무한대로 레코딩이 계속될 수 있습니다. 그 결과 **레코딩 시작** 동작에는 **레코딩 중지** 라는 필수 중지 동작이 포함됩니다.

규칙 관리 마법사를 통해 필요할 때 중지 동작을 지정할 수 있습니다.



중지 동작 선택. 예제에서는 필수 중지 동작(선택, 흐리게 표시), 관련되지 않은 중지 동작(흐리게 표시) 및 선택적 중지 동작(선택 가능)에 주의를 기울이십시오.

- 선택할 수 있는 시작 및 중지 동작 개요는 동작 및 중지 동작 을 참조하십시오.

규칙 만들기

1. **규칙** 항목 > **규칙 추가** 를 마우스 오른쪽 버튼으로 클릭합니다. **규칙 관리** 마법사가 열립니다. 마법사가 규칙 내용을 지정하는 절차를 안내합니다.
2. **이름** 및 **설명** 필드에 각각 새 규칙의 이름과 설명을 지정합니다.
3. 특정 이벤트가 발생할 때 하나 이상의 동작을 수행하는 규칙 또는 특정 시간 기간에 도달할 때 하나 이상의 동작을 수행하는 규칙 중에서 관련 조건 유형을 선택합니다.
4. **다음** 을 클릭하여 마법사의 두 번째 단계로 이동합니다. 마법사의 두 번째 단계에서 규칙에 대한 추가 조건을 정의합니다.

5. 하나 이상의 조건을 선택합니다(예: **요일은 <day>**).

선택에 따라 마법사 하단 부분에서 규칙 설명을 편집합니다:

굵은 기울임꼴 로 밑줄이 쳐진 항목을 클릭하여 정확한 내용을 지정합니다. 예를 들어, 이 예제에서 **요일** 을 클릭하면 규칙을 적용할 요일을 하나 이상 선택할 수 있습니다.

6. 정확한 내용을 지정했으면 **다음** 을 클릭하여 마법사의 다음 단계로 이동하고, 규칙에 포함시킬 동작을 선택합니다. 규칙의 내용과 복잡성에 따라 중지 이벤트, 중지 동작 등 추가 단계를 정의해야 할 수도 있습니다. 예를 들어 규칙이 시간 간격 동안(예: 목요일 오전 8시 ~ 오전 10시 30분 사이) 장치가 특정 동작을 수행하도록 지정할 경우, 마법사에 시간 간격이 종료할 때 어떻게 되는지를 지정하라는 메시지가 표시될 수 있습니다.
7. 기본적으로 규칙은 생성한 후 규칙 조건이 충족할 때 활성화됩니다. 규칙을 즉시 활성화하지 않으려면 **활성** 확인란의 선택을 취소하십시오.
8. **마침** 을 클릭합니다.

규칙 유효성 검증

개별 규칙 또는 모든 규칙의 내용에 대한 유효성을 한 번에 확인할 수 있습니다. 규칙 생성 시 **규칙 관리** 마법사는 모든 규칙 구성 요소가 유효하도록 해줍니다.

일정 시간 동안 규칙이 존재할 경우, 규칙 요소 중 하나 이상이 다른 구성에 영향을 받을 수 있고 해당 규칙이 더 이상 작동하지 않을 수 있습니다. 예를 들어 규칙이 특정 시간 프로파일에 의해 트리거 된 경우, 해당 시간 프로파일을 삭제하거나 더 이상 이 프로파일에 대한 권한이 없는 경우 이 규칙이 작동하지 않게 됩니다. 그러한 구성의 의도하지 않은 효과는 개략적인 내용을 유지하기가 어려울 수 있습니다.

규칙 유효성 확인은 어떤 규칙이 영향을 받는지를 손쉽게 추적할 수 있도록 도와줍니다. 유효성 확인은 규칙을 기반으로 이루어지며, 각 규칙은 자체적으로 유효성이 확인됩니다. 서로에 대해서는 규칙의 유효성을 확인할 수 없습니다. 예를 들어, **모든 규칙 유효성 확인** 기능을 사용하는 경우라도 한 규칙이 다른 규칙과 충돌하는지를 확인할 수 없습니다.

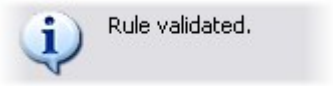
규칙 유효성 검증

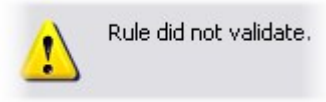
1. **규칙** 을 클릭하고 유효성을 검증할 규칙을 선택합니다.
2. 규칙에서 마우스 오른쪽 버튼을 클릭하고 **규칙 유효성 검증** 을 클릭합니다.
3. **확인** 을 클릭합니다.

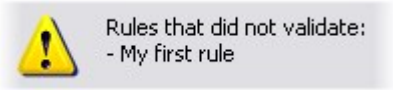
모든 규칙 유효성 검증

1. **규칙** 항목에서 마우스 오른쪽 버튼을 클릭한 후 **모든 규칙 유효성 검증** 을 클릭합니다. .
2. **확인** 을 클릭합니다.

대화 상자에 규칙의 유효성 확인 성공 여부가 나타납니다. 둘 이상의 규칙을 유효헝 검사하기로 선택하고 하나 이상의 규칙이 성공하지 못한 경우, 대화 상자가 대상 규칙의 이름을 나열합니다.







규칙 자체 이외의 요구 사항 구성이 규칙의 작동을 차단하는지는 확인할 수 없습니다. 예를 들어 특정 카메라에서 모션을 감지할 때 레코딩이 발생하도록 지정하는 규칙은 규칙 자체의 요소가 올바를 경우, 규칙이 아닌 카메라 수준에서 활성화된 모션 감지가 해당 카메라에 대해 활성화되지 않은 경우라도 정상으로 확인됩니다.

규칙 편집, 복사 및 이름 바꾸기

1. **개요** 창에서 해당 규칙을 마우스 오른쪽 단추로 클릭합니다.
2. 다음 중 하나를 선택합니다:

   규칙 편집 또는 **규칙 복사** 또는 **규칙 이름 바꾸기**. **규칙 관리** 마법사가 열립니다.
3. **규칙 복사** 를 선택하면 선택된 규칙의 사본을 표시하는 마법사가 열립니다. 사본을 만들려면 **완료** 를 클릭합니다.
4. **규칙 편집** 을 선택하면 마법사가 열린 후 변경 사항을 입력할 수 있습니다. **완료** 를 클릭하여 변경 사항을 수락합니다.
5. **규칙 이름 변경** 을 선택하면 규칙 이름 문자를 직접 변경할 수 있습니다.

규칙 비활성화 및 활성화

규칙의 조건이 적용되는 즉시 시스템이 해당 규칙을 적용합니다. 즉, 규칙이 활성화되었음을 의미합니다. 규칙을 활성화하지 않으려면 규칙을 비활성화할 수 있습니다. 규칙을 비활성화하면 규칙 조건이 적용되더라도 시스템이 해당 규칙을 적용하지 않습니다. 비활성화한 규칙을 나중에 쉽게 활성화할 수 있습니다.

규칙 비활성화

1. **개요** 창에서 규칙을 선택합니다.
2. **속성** 창에서 **활성** 확인란의 선택을 취소합니다.
3. 도구 모음에서 **저장** 을 클릭합니다.
4. 빨간색 x가 있는 아이콘은 해당 규칙이 **규칙** 목록에서 비활성화되었음을 나타냅니다:

규칙 활성화

규칙을 다시 활성화하려면 **활성화** 확인란을 선택하고 설정을 저장합니다.

시간 프로파일 지정

1. **시간 프로파일** 목록에서 **시간 프로파일** > **시간 프로파일 추가** 를 마우스 오른쪽 버튼으로 클릭합니다. 이렇게 하면 **시간 프로파일** 창이 열립니다.
2. **시간 프로파일** 창의 **이름** 필드에 새 시간 프로파일의 이름을 입력합니다. 원하는 경우 **설명** 필드에 새 시간 프로파일에 대한 설명을 입력합니다.
3. **시간 프로파일** 창의 달력에서 **일간 뷰**, **주간 뷰** 또는 **월간 뷰** 중 하나를 선택한 다음, 달력 안쪽을 마우스 오른쪽 단추로 클릭하고 **단일 시간 추가** 또는 **반복 시간 추가** 를 선택합니다.
4. 시간 프로파일에 대한 시간 길이를 지정했으면 **시간 프로파일** 창에서 **확인** 을 클릭합니다. 시스템이 새 시간 프로파일을 **시간 프로파일** 목록에 추가합니다. 이후 단계에서 시간 프로파일을 편집하거나 삭제하려는 경우에도 **시간 프로파일** 에서 해당 작업을 수행하면 됩니다.

단일 시간 추가

단일 시간 추가 를 선택한 경우, **시간 선택** 창이 나타납니다.

시간 및 날짜 형식은 시스템마다 다를 수 있습니다.

1. **시간 선택** 창에서 **시작 시간** 및 **종료 시간** 을 지정합니다. 이 시간이 전체 일을 포괄하는 경우, **전일 이벤트** 상자를 선택합니다.
2. **확인** 을 클릭합니다.

반복 시간 추가

되풀이 시간 추가 를 선택한 경우, **되풀이 시간 선택** 창이 나타납니다.

1. **시간 선택** 창에서 시간 범위, 되풀이 패턴 및 되풀이 범위를 지정합니다.
2. **확인** 을 클릭합니다.

시간 프로파일에는 여러 시간 기간이 포함될 수 있습니다. 시간 프로파일에 추가 기간을 포함시키려면 단일 시간 또는 되풀이 시간을 더 추가하십시오.

반복 시간

상세한 반복 스케줄에서 실행될 동작을 설정할 때.

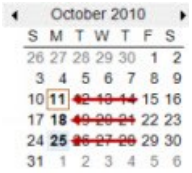
예:

- 매주 화요일 15:00~15:30 사이 1시간 동안
- 매 3개월마다 15일 11:45에
- 매일 15:00~19:00 사이 1시간 동안

시간은 Management Client 이(가) 설치된 서버의 현지 시간 설정을 따릅니다.

시간 프로파일 편집

1. **개요** 창의 **시간 프로파일** 목록에서 해당 시간 프로파일을 마우스 오른쪽 단추로 클릭하고 **시간 프로파일 편집** 을 선택합니다. 이렇게 하면 **시간 프로파일** 창이 열립니다.
2. 필요에 따라 시간 프로파일을 편집합니다. 시간 프로파일을 변경했으면 **시간 프로파일** 창에서 **확인** 을 클릭합니다. **시간 프로파일** 목록으로 돌아갑니다.



시간 프로파일 정보 창에서 필요에 따라 시간 프로파일을 편집할 수 있습니다. 시간 프로파일에는 둘 이상의 기간이 포함될 수 있고 해당 기간이 반복될 수 있음을 유념하십시오. 상단 오른쪽 모서리에 있는 작은 월 개요는 지정한 시간을 포함하는 날짜가 굵게 강조 표시되므로 시간 프로파일에 적용되는 기간에 대한 빠른 개요 정보를 확인하는 데 도움이 될 수 있습니다.

이 예에서 굵은 날짜는 여러 요일에 기간을 지정했음을, 월요일에 되풀이 시간을 지정했음을 나타냅니다.

낮 길이 시간 프로파일 만들기

1. **규칙 및 이벤트** 폴더 > **시간 프로파일** 을 확장합니다.
2. **시간 프로파일** 목록에서 **시간 프로파일** 을 마우스 오른쪽 단추로 클릭하고 **하루 길이 시간 프로파일 추가** 를 클릭합니다.

3. **낮 길이 시간 프로파일** 창에서 아래 속성표를 참조하여 필요한 정보를 입력합니다. 밝음/어둠 간의 전환 기간을 처리하기 위해 프로파일의 활성화와 비활성화를 상쇄시킬 수 있습니다. 시간 및 월 이름은 컴퓨터의 언어/국가별 설정에 사용된 언어로 표시됩니다.
4. 맵에 입력한 지리적 좌표 위치를 보려면 **브라우저에 위치 표시** 를 클릭합니다. 이렇게 하면 위치를 볼 수 있는 브라우저가 열립니다.
5. **확인** 을 클릭합니다.

하루 길이 시간 프로파일 속성

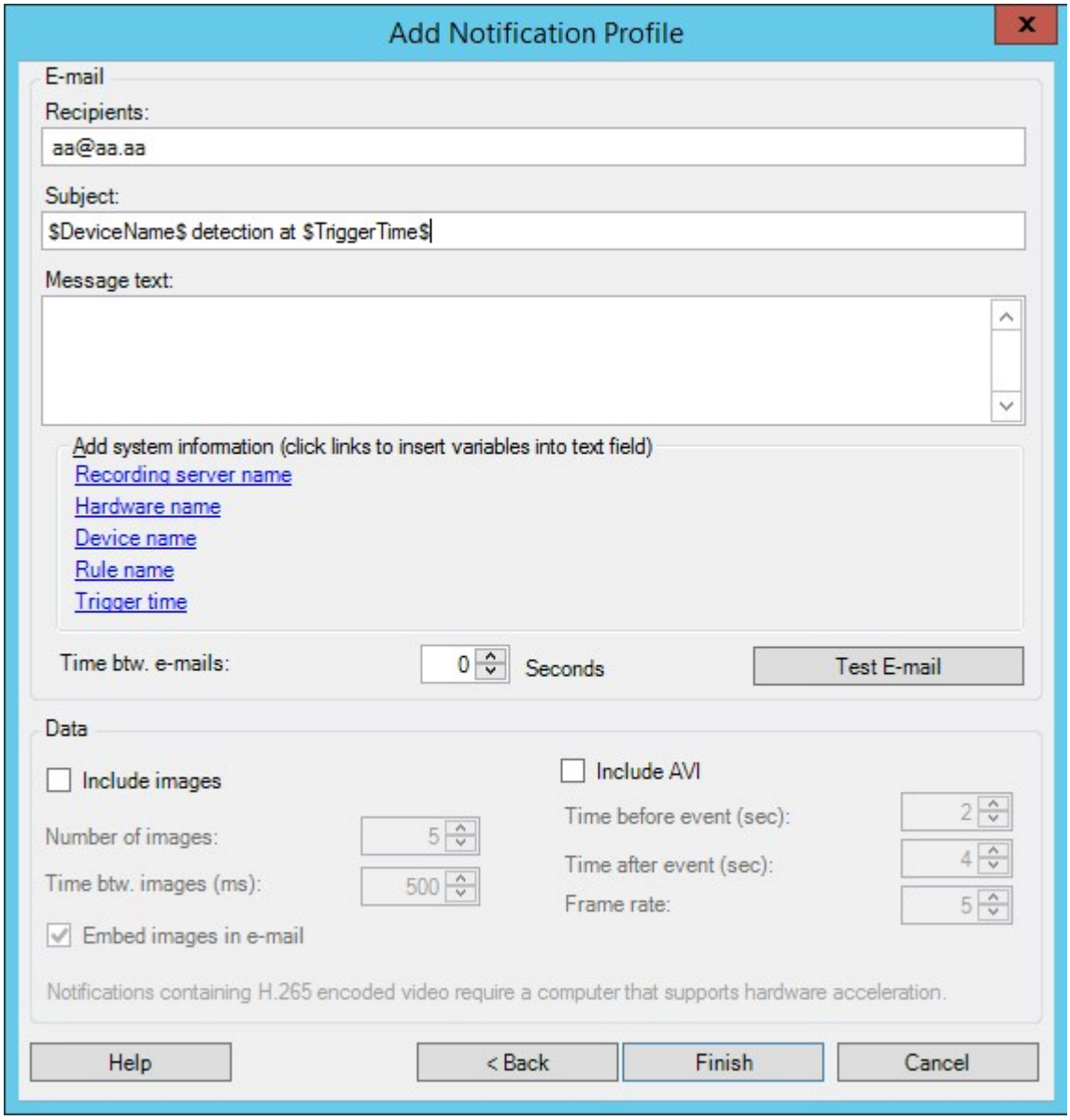
이름	설명
이름	프로파일의 이름.
설명	프로파일의 설명(옵션).
지리적 좌표	프로파일에 할당된 카메라의 물리적 위치를 나타내는 지리적 좌표.
일출 오프셋	일출에 의해 프로파일 활성화가 상쇄되는 분 단위 수(+/-).
일몰 오프셋	일몰에 의해 프로파일 비활성화가 상쇄되는 분 단위 수(+/-).
시간대	카메라의 물리적 위치를 나타내는 시간대.

알림 프로파일 추가

알림 프로파일을 만들기 전에 이메일 알림에 대한 메일 서버 설정을 지정해야 합니다. 자세한 정보는 알림 프로파일 생성 요구 사항 을 참조하십시오.

1. **규칙 및 이벤트** 를 확장하고 **알림 프로파일** > **알림 프로파일 추가** 를 마우스 오른쪽 버튼으로 클릭합니다. 이렇게 하면 **알림 프로파일 추가** 마법사가 열립니다.
2. 이름과 설명을 지정합니다. **다음** 을 클릭합니다.

3. 수신자, 제목, 메시지 텍스트, 이메일 간 시간을 지정합니다:



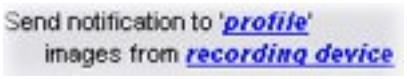
4. 지정한 수신자로 테스트 이메일 알림을 전송하려면 **테스트 이메일** 을 클릭합니다.
5. 사전 알람 정지 이미지를 포함시키려면 **이미지 포함** 을 선택하고 이미지 수, 이미지 간 시간, 이메일에 이미지 포함 여부를 지정합니다.
6. AVI 비디오 클립을 포함시키려면 **AVI 포함** 을 선택하고 이벤트 전후 시간과 프레임 속도를 지정합니다.

> H.265 인코딩 비디오를 포함하는 알림은 하드웨어 가속을 지원하는 컴퓨터가 필요합니다.

7. **마침** 을 클릭합니다.

규칙에서 이메일 알림 트리거하기

1. **규칙** 항목을 마우스 오른쪽 버튼으로 클릭한 후 클릭 > **규칙 추가** 또는 **규칙 편집**.
2. **규칙 관리** 마법사에서 **다음** 을 클릭하여 **수행할 동작 선택** 목록으로 이동한 후 **알림을 <profile>로 보내기** 를 선택합니다.
3. 관련 알림 프로파일을 선택하고 카메라를 선택하여 알림 프로파일의 이메일 알림에 녹화가 포함되도록 합니다.



실제로 녹화가 이뤄지지 않는 한 알림 프로파일의 이메일 알림에 레코딩을 포함할 수 없습니다. 이메일 알림에 스틸 이미지 또는 AVI 비디오 클립을 포함시키려면 해당 규칙이 레코딩 발생을 지정하는지 확인하십시오. 다음 예는 **레코딩 시작** 동작과 **알림 전송** 동작을 포함하는 규칙에서 가져온 것입니다:

사용자 정의 이벤트 추가

사용자 정의 이벤트를 사용하는 방식에 상관없이 Management Client 을(를) 통해 각 사용자 정의 이벤트를 추가해야 합니다.

1. **규칙 및 이벤트** > **사용자 정의 이벤트** 를 확장합니다.
2. **개요** 창에서 **이벤트** > **사용자 정의 이벤트 추가** 를 마우스 오른쪽 버튼으로 클릭합니다.
3. 새 사용자 정의 이벤트의 이름을 입력하고 **확인** 을 클릭합니다. 이제 새로 추가한 사용자 정의 이벤트가 **개요** 창의 목록에 나타납니다.

사용자가 해당 권한을 가지고 있는 경우 XProtect Smart Client 에서 이 사용자 정의 이벤트를 수동으로 트리거할 수 있습니다.

사용자 정의 이벤트를 삭제할 경우, 해당 사용자 정의 이벤트를 사용 중인 모든 규칙에 영향을 미치게 됩니다. 또한, 삭제된 사용자 정의 이벤트는 XProtect Smart Client 사용자가 로그아웃할 때만 XProtect Smart Client 에서 사라집니다.

사용자 정의 이벤트 이름 변경

사용자 정의 이벤트의 이름을 변경한 경우, 이미 연결된 XProtect Smart Client 사용자가 로그아웃한 후 다시 로그인해야 변경된 이름이 표시됩니다.

1. **규칙 및 이벤트** > **사용자 정의 이벤트** 를 확장합니다.
2. **개요** 창에서 사용자 정의 이벤트를 선택합니다.
3. **속성** 창에서 기존의 이름을 덮어씁니다.
4. 도구 모음에서 **저장** 을 클릭합니다.

분석 이벤트 추가 및 편집

분석 이벤트 추가

1. **규칙 및 이벤트** 를 확장하고 **분석 이벤트** 를 마우스 오른쪽 단추로 클릭한 다음, **새로 추가** 를 선택합니다.
2. **속성** 창의 **이름** 필드에 이벤트의 이름을 입력합니다.
3. 필요하면 **설명** 필드에 설명 텍스트를 입력합니다.
4. 도구 모음에서 **저장** 을 클릭합니다. **테스트 이벤트** 를 클릭하여 이벤트의 유효성을 테스트할 수 있습니다. 테스트에 표시된 오류를 계속해서 수정하고 원하는 수만큼, 프로세스에서 어느 위치에서든 테스트를 실행할 수 있습니다.

분석 이벤트 편집

1. 기존 분석 이벤트를 클릭해서 **속성** 창을 봅니다. 이 창에서 해당 필드를 편집할 수 있습니다.
2. **테스트 이벤트** 를 클릭하여 이벤트의 유효성을 테스트할 수 있습니다. 테스트에 표시된 오류를 계속해서 수정하고 원하는 수만큼, 프로세스에서 어느 위치에서든 테스트를 실행할 수 있습니다.

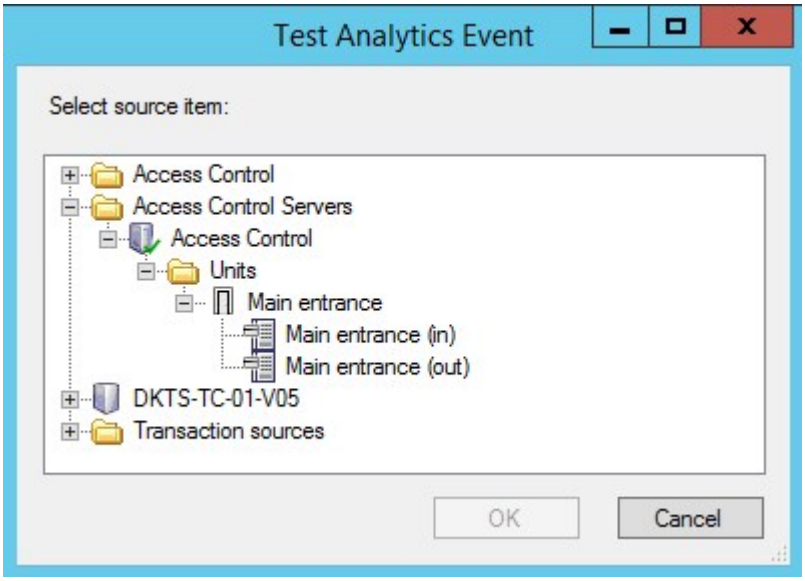
분석 이벤트 설정 편집

도구 모음에서 **도구** > **옵션** > **분석 이벤트** 탭으로 이동하여 해당 설정을 편집합니다.

분석 이벤트 테스트

예를 들어, Management Client 에서 활성화된 분석 이벤트 기능과 같이 분석 이벤트 생성 후 요건을 테스트할 수 있습니다(페이지 261의 분석 이벤트 추가 및 편집 참조).

1. 기존 분석 이벤트를 선택합니다.
2. 속성에서**테스트이벤트**버튼을클릭합니다.이벤트에대해가능한모든소스를보여주는창이나타납니다.



3. 테스트 이벤트의 소스를 선택합니다(예: 카메라). 창이 닫히고 분석 이벤트가 작동하기 위해 충족되어야 하는 4 개 조건이 표시된 새로운 창이 나타납니다.

추가 테스트로 XProtect Smart Client 에서 이벤트 서버로 전송된 분석 이벤트를 검증할 수 있습니다. 이렇게 하려면 XProtect Smart Client 를 열고 **알람 관리자** 탭에서 이벤트를 봅니다.

일반 이벤트 추가

VMS가 외부 시스템으로부터 TCP 또는 UDP 패킷의 특정 문자열을 손쉽게 인식할 수 있도록 일반 이벤트를 정의할 수 있습니다. 일반 이벤트에 기초하여 Management Client 가 작업을 트리거하도록 구성할 수 있습니다(예: 레코딩 시작 또는 알람).

요구사항
일반 이벤트를 활성화했고 허용되는 소스 대상을 지정했습니다. 자세한 정보는 페이지 366의 일반 이벤트 탭(옵션)를 참조하십시오.

일반 이벤트를 추가하려면:

1. **규칙 및 이벤트** 를 확장합니다.
2. **일반 이벤트** 를 마우스 오른쪽 버튼으로 클릭하고 **새로 추가** 를 선택합니다.
3. 필요한 정보와 속성을 채웁니다. 자세한 정보는 페이지 461의 일반 이벤트 및 데이터 소스(속성)를 참조하십시오.
4. (옵션) 검색 식이 유효한지 확인하려면 **식이 이벤트 문자열과 일치하는지 확인** 필드에 예상 패키지에 해당하는 검색 문자열을 입력합니다.
   - **일치** - 검색 식에 대해 문자열을 검증할 수 있습니다
   - **일치 없음** - 검색 식이 유효하지 않습니다. 변경하고 다시 시도하십시오

XProtect Smart Client 에서 일반 이벤트가 이벤트 서버에서 수신되었는지를 확인할 수 있습니다. 이 작업은 **알람 관리자** 탭의 **알람 목록** 에서 **이벤트** 를 선택하여 수행합니다.

인증

외부 IDP의 클레임 등록

1. Management Client에서 **도구** > **옵션**을 선택하고 **외부 IDP** 탭을 엽니다.
2. **외부 IDP** 섹션에서 **추가**를 선택합니다.
3. **등록된 클레임** 섹션에서 **추가** 를 선택합니다.
4. 클레임에 관한 정보를 입력합니다. 자세한 정보는 클레임 등록 을 확인하십시오.

XProtect에서 외부 IDP의 클레임을 역할에 매핑하기

외부 IDP 사이트에서 관리자는 이름과 값으로 구성된 클레임을 생성해야 합니다. 그렇게 하면 해당 클레임은 VMS의 역할에 대해 매핑되며 사용자의 권한은 역할에 따라 결정됩니다.

1. Management Client 의 **사이트 탐색** 창에서, **보안** 노드를 확장한 후 **역할** 을 선택합니다.
2. 역할을 선택한 후, **외부 IDP** 탭을 선택하고 **추가**를 선택합니다.
3. 외부 IDP와 클레임 이름을 선택하고 클레임 값을 입력합니다.

   클레임 이름은 외부 IDP에서 나온 클레임 이름과 정확히 일치하도록 입력해야 합니다.

4. **확인** 을 선택합니다.

외부 IDP가 삭제되면 외부 IDP를 통해 VMS에 연결된 모든 사용자도 삭제됩니다. 외부 IDP에 연결된 모든 등록된 클레임이 제거되고 역할에 대한 모든 매핑도 제거됩니다.

외부 IDP를 통한 로그인

외부 IDP를 사용하여 XProtect Smart Client, XProtect Management Client, XProtect Web Client, XProtect Mobile 클라이언트에 로그인할 수 있습니다.

1. XProtect Smart Client 또는 XProtect Management Client에 있는 로그인 대화 상자의 **승인**에서 외부 IDP를 선택한 후 **로그인**을 선택합니다. 처음 로그인하면 외부 IDP가 속한 웹 페이지로 이동하게 됩니다.
2. 사용자이름과암호를입력한후로그인하십시오.로그인한후XProtect클라이언트로돌아오면로그인이된것입니다.

도구 > **옵션** > **외부 IDP**에서 **승인** 목록에 표시된 외부 IDP의 이름을 구성할 수 있습니다.

예를 들어, 복원 또는 암호 변경으로 인해 외부 IDP가 비활성화된 경우 **인증** 목록에서 외부 IDP를 통해 로그인하는 옵션을 사용할 수 없습니다. 또한 외부 IDP가 비활성화된 경우 외부 IDP에서 수신한 클라이언트 암호는 **도구** > **옵션**의 **외부 IDP**에 있는 **클라이언트 암호**에서 사라집니다.

보안

역할 추가 및 관리

1. **보안** 을 확장하고 **역할** 을 마우스 오른쪽 버튼으로 클릭합니다.
2. **역할 추가** 를 선택합니다. **그러면** 역할 추가 대화 상자가 열립니다.
3. 새 역할의 이름과 설명을 입력하고 **확인** 을 클릭합니다.
4. **새로운 역할이** 역할 목록에 추가됩니다. 기본적으로, 새 역할에는 어떠한 사용자/그룹도 연결되지 않지만, 다수의 기본 프로파일은 연결됩니다.
5. 다른 Smart Client 및 Management Client 프로파일, 증거물 잠금 프로파일 또는 시간 프로파일을 선택하려면 드롭다운 목록을 클릭합니다.
6. 이제 사용자/그룹을 역할에 할당하고 해당 역할이 액세스할 수 있는 시스템 기능을 지정할 수 있습니다.

자세한 정보는 페이지 265의 역할에 사용자 및 그룹 할당/제거 및 페이지 463의 역할(보안 노드)를 참조하십시오.

역할 복사, 이름 바꾸기 또는 삭제

역할 복사

복잡한 설정 및/또는 권한을 가진 역할을 보유하고 있거나 유사 또는 거의 유사한 역할이 필요한 경우, 처음부터 새 역할을 생성하기보다 이미 존재하는 역할을 복사한 후 약간의 수정을 가하는 편이 편할 수도 있습니다.

1. **보안** 을 확장하고 **역할** 을 클릭한 다음, 관련 역할을 마우스 오른쪽 버튼으로 클릭하고 **역할 복사** 를 선택합니다.
2. 열리는 대화 상자에서 복사한 역할에 새로운 고유 이름과 설명을 지정합니다.
3. **확인** 을 클릭합니다.

역할 이름 바꾸기

역할의 이름을 변경해도 해당 역할을 기반으로 하는 뷰 그룹의 이름은 바뀌지 않습니다.

1. **보안** 을 확장하고 **역할** 을 마우스 오른쪽 버튼으로 클릭합니다.
2. 필요한 역할을 마우스 오른쪽 버튼으로 클릭하고 **역할 이름 바꾸기** 를 선택합니다.
3. 열리는 대화 상자에서 역할의 이름을 변경합니다.
4. **확인** 을 클릭합니다.

역할 삭제

1. **보안** 을 확장하고 **역할** 을 클릭합니다.
2. 불필요한 역할을 마우스 오른쪽 버튼으로 클릭하고 **역할 삭제** 를 선택합니다.
3. **예** 를 클릭합니다.

> ⚠ 역할을 삭제해도 해당 역할을 기반으로 하는 뷰 그룹은 삭제되지 않습니다.

유효 역할 보기

유효 역할 기능을 사용하면 선택한 사용자 또는 그룹의 모든 역할을 볼 수 있습니다. 이 기능은 그룹을 사용 중일 때 유용하며, 특정 사용자가 구성원으로 속해 있는 역할을 볼 수 있는 유일한 방법에 해당합니다.

1. **보안** 을 확장하고 **역할** 을 마우스 오른쪽 버튼으로 클릭해서 **유효 역할** 창을 열고, **유효 역할** 을 선택합니다.
2. 기본 사용자에 대한 정보를 원하는 경우, **사용자 이름** 필드에 해당 이름을 입력합니다. 사용자의 역할을 표시하려면 **새로 고침** 을 클릭합니다.
3. Active Directory의 Windows 사용자 또는 그룹을 사용하는 경우, **"..."** 개체 유형을 선택하고 이름을 입력한 다음, **확인** 을 클릭합니다. 해당 사용자의 역할이 자동으로 나타납니다.

역할에 사용자 및 그룹 할당/제거

역할에 Windows 사용자 또는 그룹이나 기본 사용자를 할당하거나 제거하려면:

1. **보안** 을 확장하고 **역할** 을 선택합니다. 그런 다음 **개요** 창에서 필요한 역할을 선택합니다:
2. **속성** 창의 하단에서 **사용자 및 그룹** 탭을 선택합니다.
3. **추가** 를 클릭하고 **Windows 사용자** 또는 **기본 사용자** 중에서 선택합니다.

역할에 Windows 사용자 및 그룹 할당

1. **Windows 사용자** 를 선택합니다. 이렇게 하면 **사용자, 컴퓨터 및 그룹 선택** 대화 상자가 열립니다:
2. 필요한 개체 유형이 지정되었는지 확인합니다. 예를 들어 컴퓨터를 추가해야 하는 경우, **개체 유형** 을 클릭하고 **컴퓨터** 를 선택 표시합니다. 또한 필요한 도메인이 **이 위치에서** 필드에 지정되었는지 확인합니다. 그렇지 않으면 **위치** 를 클릭하여 필요한 도메인을 찾습니다.
3. **선택할 개체 이름 입력** 상자에 해당 사용자 이름, 이니셜 또는 Active Directory가 인식할 수 있는 다른 유형의 식별자를 입력합니다. **이름 확인** 기능을 사용하여 Active Directory가 입력한 이름 또는 이니셜을 인식하는지 확인합니다. 또는 **"고급..."** 기능을 사용해 사용자 또는 그룹을 검색합니다.
4. **확인** 을 클릭합니다. 이제 선택한 사용자/그룹이 선택 역할을 할당한 **사용자 및 그룹** 탭의 사용자 목록에 추가됩니다. 여러 사용자 이름을 세미콜론(;)으로 구분해 입력하여 더 많은 사용자와 그룹을 추가할 수 있습니다.

역할에 기본 사용자 할당

1. **기본 사용자** 를 선택합니다. 그러면 **역할에 추가할 기본 사용자 선택** 대화 상자가 열립니다:
2. 이 역할에 할당하려는 기본 사용자를 선택합니다.
3. 선택 사항: 새 기본 사용자를 만들려면 **새로 만들기** 를 클릭합니다.
4. **확인** 을 클릭합니다. 이제 선택한 기본 사용자가 선택 역할을 할당한 **사용자 및 그룹** 탭의 기본 사용자 목록에 추가됩니다.

역할에서 사용자 및 그룹 제거

1. **사용자 및 그룹** 탭에서 제거할 사용자 또는 그룹을 선택하고 탭의 하단 부분에서 **제거** 를 클릭합니다. 필요한 경우 둘 이상의 사용자나 그룹, 또는 그룹과 개별 사용자 조합을 선택할 수 있습니다.
2. 선택한 사용자 또는 그룹 제거 여부를 확인합니다. **예** 를 클릭합니다.

> 사용자가 그룹 구성원 자격을 통해 역할을 가지고 있을 수 있습니다. 이 경우, 역할에서 해당하는 개별 사용자를 제거할 수 없습니다. 그룹 구성원은 또한 개인으로서 역할을 보유할 수 있습니다. 사용자나 그룹, 개별 그룹 회원이 보유한 역할을 찾으려면 **적용 중인 역할 보기** 기능을 사용하십시오.

기본 사용자 만들기

Milestone XProtect VMS에는 사용자 계정 유형이 다음과 같이 두 가지가 있습니다. 기본 사용자 및 Windows 사용자.

기본 사용자는 Milestone XProtect VMS에서 만든 사용자 계정입니다. 이 계정은 개별 사용자에 대해 기본 사용자 이름과 암호 인증이 있는 전용 시스템 사용자 계정입니다.

Windows 사용자는 Microsoft의 Active Directory을(를) 통해 추가하는 사용자 계정입니다.

기본 사용자 및 Windows 사용자 사이에는 다음과 같은 몇 가지 차이점이 있습니다.

- 기본 사용자는 사용자 이름 및 암호 조합으로 인증되며 하나의 시스템/사이트에 한정됩니다. 하나의 연합 사이트에서 생성된 기본 사용자가 다른 연합 사이트의 기본 사용자와 동일한 이름과 암호를 가지고 있다하더라도 기본 사용자는 생성된 사이트에만 액세스할 수 있습니다.
- Windows 사용자는 해당 Windows 로그인에 기반하여 인증을 받으며 이 인증은 하나의 시스템에 한정됩니다.

기본 사용자에 대한 로그인 설정 구성

JSON 파일에서 기본 사용자에 대한 로그인 설정을 정의할 수 있으며 위치는 다음과 같습니다. `\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json`.

그 파일에서 다음 매개 변수를 설정할 수 있습니다.

LoginSettings

"ExpireTimeInMinutes": 5	사용자가 아무런 동작을 하지 않는 경우 로그인 세션이 만료될 시간의 길이(분 단위)를 정의합니다.
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	사용자가 잠금 처리되는 시간의 길이(분 단위)를 정의합니다.
"MaxFailedAccessAttempts": 5	잠금 처리되기 전까지 사용자가 로그인을 시도할 수 있는 횟수를 정의합니다.
PasswordSettings	
"RequireDigit": true	기본 정수(0에서 9)가 암호에 필요한지 여부를 정의합니다.
"RequireLowercase": true	소문자가 암호에 필요한지 여부를 정의합니다.
"RequireNonAlphanumeric": true	특수 문자(~!@#$%^&*_-+=`\₩(){}[]:;"'<>,.?/)가 암호에 필요한지 여부를 정의합니다.
"RequireUppercase": true	대문자가 암호에 필요한지 여부를 정의합니다.
"RequiredLength": 8	암호에 필요한 문자의 수를 정의합니다. 최소 암호 길이는 {0}자이며 최대 암호 길이는 255자입니다.
"RequiredUniqueChars": 1	암호에 필요한 최소 특정 문자의 수를 정의합니다. 예를 들어 필수 특정 문자를 2개로 설정한 경우에는 aaaaaa, aa, a, b, bb, bbbbbbb와 같은 암호는 거부됩니다. 반면 abab, abc, aaab 등은 암호에 최소 2개의 특정 문자가 포함되어 있으므로 허용됩니다. 암호에 특정 문자의 수를 늘리면 쉽게 추측할 수 있는 반복적인 시퀀스를 피함으로써 암호의 강도를 높일 수 있습니다.

시스템에서 기본 사용자를 만들려면:

1. **보안** > **기본 사용자** 를 확장합니다.
2. **기본 사용자** 창에서 마우스 오른쪽 버튼을 클릭해 **기본 사용자 만들기** 를 선택합니다.
3. 사용자 이름 및 암호를 지정하십시오. 올바로 지정했는지 확인하기 위해 암호를 다시 입력해야 합니다.

   암호는 **appsettings.json** 파일에 정의된 복잡성 요구 사항을 충족해야 합니다(페이지 266의 기본 사용자에 대한 로그인 설정 구성 참조).

4. 기본 사용자가 다음 로그인 시 암호를 변경해야 하는지 지정합니다. Milestone에서는 기본 사용자가 처음 로그인할 때 암호를 지정할 수 있도록 확인란을 선택하는 것을 권장합니다.

   자신의 암호를 변경할 수 없는 기본 사용자를 만들 때에만 이 확인란을 해제해야 합니다. 예를 들어 이러한 기본 사용자는 플러그인 및 서버 서비스 인증에 사용되는 시스템 사용자입니다.

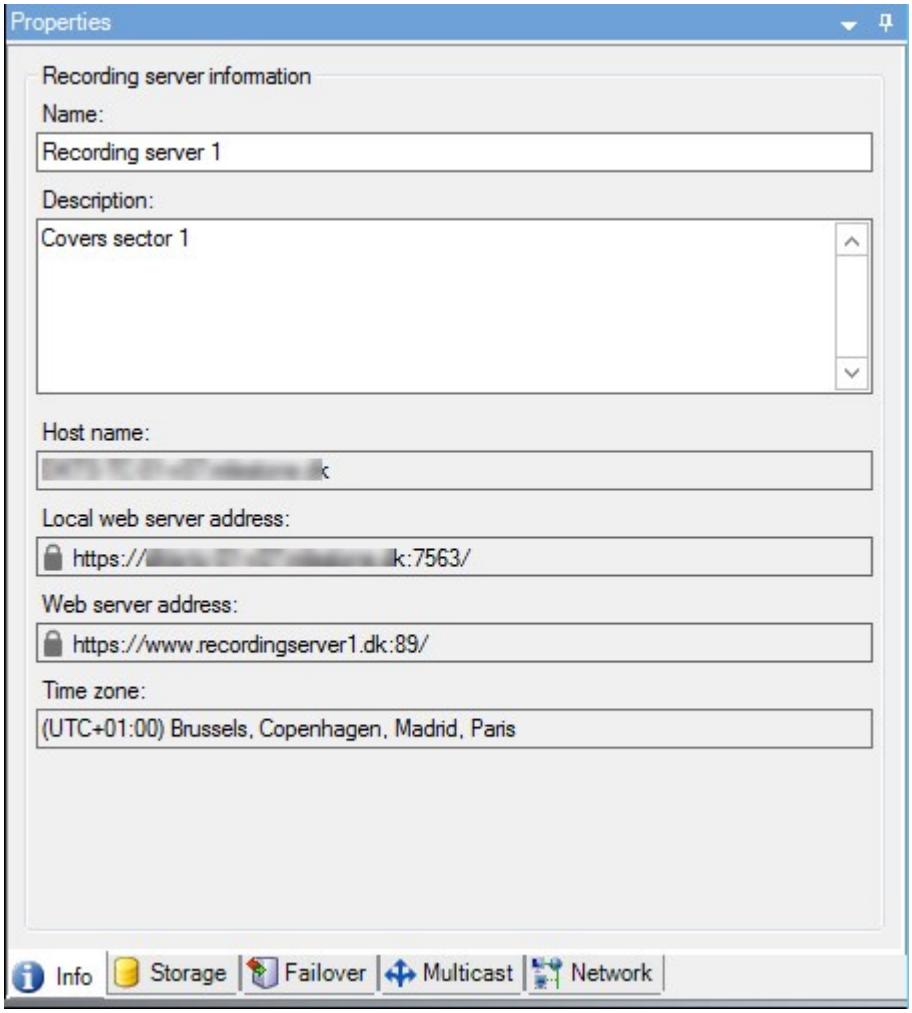
5. 기본 사용자의 상태를 **활성화** 또는 **잠김** 으로 지정합니다.

6. **확인** 을 클릭하여 기본 사용자를 만듭니다.

클라이언트에 대한 암호화 상태 보기

레코딩 서버 암호화 연결을 확인하려면 다음을 수행:

1. Management Client 을(를) 엽니다.
2. **사이트 탐색** 창에서 **서버** > **레코딩 서버** 를 선택합니다. 이렇게 하면 레코딩 서버 목록이 열립니다.
3. **개요** 창에서, 관련 레코딩 서버를 선택하고 **정보** 탭으로 이동합니다.
   레코딩 서버에서 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화가 활성화된 경우, 로컬 웹 서버 주소 및 웹 서버 주소(옵션)의 전면에 자물쇠 아이콘이 표시됩니다.



시스템 대시보드

레코딩 서버 상의 현재 진행 중인 작업 보기

현재 작업 창은 선택된 레코딩 서버 하에서 진행 중인 작업 개요를 표시합니다. 시간이 오래 걸리고 배경에서 구동되는 작업을 시작한 경우 **현재 작업** 창을 열어 작업 진행 상황을 확인할 수 있습니다. 시간이 오래 걸리는 사용자가 시작한 작업의 몇 가지 사례들로는 펌웨어 업데이트와 하드웨어 이동이 있습니다. 그러한 작업들의 시작 시간, 대략적인 종료 시간 및 진행 상황에 관한 정보를 확인할 수 있습니다.

작업이 기대했던 것처럼 진행되지 않은 경우 하드웨어 또는 네트워크에서 원인을 찾을 수도 있습니다. 그 몇 가지 사례로 서버가 구동 중이 아닌 경우, 서버 에러인 경우, 대역폭이 너무 좁은 경우 또는 연결이 상실된 경우가 있습니다.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **현재 작업** 을 선택합니다.
2. 레코딩 서버를 선택하여 현재 작업을 조회합니다.

현재 작업 창에 표시된 정보는 실시간으로 업데이트되지는 않지만 창을 연 순간에 현재 작업에 대한 스냅샷을 제공합니다. 일정 시간 동안 창을 열어 둔 경우, 창 우측 하단 코너에 있는 **새로 고침** 버튼을 선택하여 표시된 정보를 새로 고침할 수 있습니다.

시스템 모니터(설명됨)

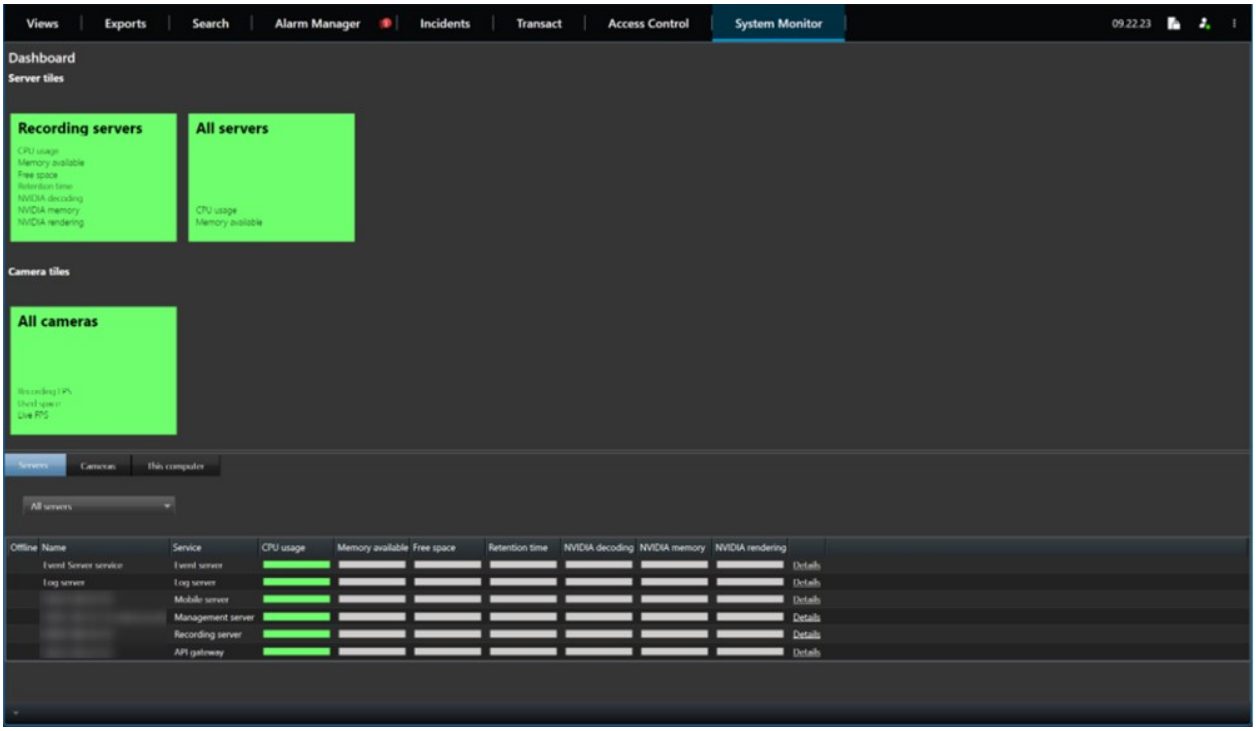
> 시스템 모니터 기능성에는 Data Collector 서비스 구동이 필요하며 그레고리안력(서력)을 사용ㅎ아는 컴퓨터에서만 작동합니다.

시스템 모니터 대시보드(설명됨)

시스템 모니터 대시보드 에서 비디오 관리 소프트웨어 시스템의 상태 개요를 쉽게 확인할 수 있습니다. 하드웨어의 상태는 타일과 색상으로 표시됩니다: 녹색(구동 중), 노란색(경고), 적색(위험). 타일은 또한 하나 이상의 하드웨어가 오작동 상태에 빠진 경우 오류 또는 경고 아이콘을 표시합니다.

기본으로 시스템은 모든 **레코딩 서버**, **모든 서버**, 및 **모든 카메라** 를 나타내는 타일을 표시합니다. 이러한 기본 타일의 모니터링 매개변수를 사용자 정의하고 새 타일을 생성할 수 있습니다. 예를 들어 단일 서버, 단일 카메라, 카메라 그룹 또는 서버 그룹을 나타내도록 타일을 설정할 수 있습니다.

모니터링 매개변수에는 서버에 사용할 수 있는 메모리 또는 CPU 사용량 등이 있습니다. 타일은 귀하가 타일에 추가한 모니터링 매개변수만 모니터링합니다. 자세한 정보페이지 272의 시스템 모니터 대시보드에서 카메라 또는 서버 타일 편집는 페이지 272의 시스템 모니터 대시보드에서 새 카메라 또는 서버 타일 추가, 및 페이지 273의 시스템 모니터 대시보드에서 카메라 또는 서버 타일 삭제를 참조하십시오.



시스템 모니터 임계치(설명됨)

시스템 모니터 임계값을 통해 **시스템 모니터 대시보드** 상의 타일이 귀하의 시스템 하드웨어가 상태를 변경하였음을 시각적으로 표시할 때의 임계값을 정의 및 조정할 수 있게 해줍니다. 예를 들어 서버의 CPU 사용량이 일반 상태(녹색)에서 경고 상태(노란색) 또는 경고 상태(노란색)에서 위험 상태(적색)으로 변경되는 경우입니다.

시스템은 동일한 유형의 모든 하드웨어에 대한 기본 임계값을 갖고 있어 시스템이 설치된 순간 및 하드웨어를 추가한 순간부터 시스템 하드웨어 상태에 대한 모니터링을 시작할 수 있습니다. 개별 서버와 카메라, 디스크, 저장소에 대한 임계값도 설정할 수 있습니다. 임계값을 변경하려면 페이지 273의 하드웨어 상태가 변경되어야 할 때에 대한 임계값 편집를 참조하십시오.

시스템 하드웨어의 사용량 또는 처리량이 높은 임계치에 수초간 도달하는 경우에 **위험** 또는 **경고** 상태를 보지 않으려면, **간격 계산** 을 사용합니다. 정확히 계산하여 간격을 설정하면 임계값 초과에 대한 오탐으로 인한 경고를 받지 않게 될 뿐만 아니라 CPU 사용량 또는 메모리 소비량과 같은 지속적인 문제에 관한 알람만 받을 수 있습니다.

또한 규칙을 설정하여(규칙(설명됨)) 임계값이 다르게 변경될 때 특정 동작을 수행하게 하거나 알람을 활성화할 수 있습니다.

하드웨어의 현재 상태를 조회하고 필요한 경우 문제를 해결합니다

시스템 모니터 대시보드 에서 비디오 관리 소프트웨어 시스템의 상태 개요를 쉽게 확인할 수 있습니다. 하드웨어의 상태는 타일과 색상으로 표시됩니다: 녹색(구동 중), 노란색(경고), 적색(위험). 타일은 또한 하나 이상의 하드웨어가 오작동 상태에 빠진 경우 오류 또는 경고 아이콘을 표시합니다.

하드웨어가 위 세 가지 상태 중 하나일 때에 대한 임계값을 편집할 수 있습니다. 자세한 정보는 페이지 273의 하드웨어 상태가 변경되어야 할 때에 대한 임계값 편집를 참조하십시오.

시스템 모니터 대시보드 는 다음과 같이 질문에 대한 답변을 제공합니다: 모든 서버 서비스 및 카메라가 구동 중입니까? 다른 서버 상의 CPU 사용량과 사용 가능한 메모리가 충분하여 모든 것이 녹화되고 조회할 수 있습니까?

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. 모든 타일이 녹색이며 경고 또는 오류 아이콘이 없는 경우, 타일이 표시하는 모든 모니터링 매개변수 및 모든 서버와 카메라는 정상적으로 구동되고 있습니다.
   하나 이상의 타일이 경고 또는 오류 아이콘을 표시하거나 완전히 노란색 또는 적색인 경우, 이러한 타일 중 하나를 선택하여 문제 해결을 시작합니다.
3. 모니터링 매개변수를 포함한 하드웨어 목록에서(창의 하단), 구동 중이 아닌 하드웨어를 찾습니다. 해당 하드웨어 옆 적색 십자가 표시 위로 마우스를 올린 후 표시된 문제가 무엇인지 읽습니다.
4. 별도로 해당 하드웨어의 우측에 있는 **상세 내용** 을 선택하여 얼마나 오래 문제가 지속되었는지 확인합니다. 오랜 시간에 걸쳐 하드웨어의 상태를 확인하기 위해 이력 데이터 수집을 활성화합니다. 자세한 정보는 페이지 272의 하드웨어 상태의 이력 데이터 수집를 참조하십시오.
5. 문제를 해결할 방법을 찾습니다. 예를 들어 컴퓨터 재시작, 서버 서비스 재시작, 오작동 중인 하드웨어 또는 기타 교체가 있습니다.

하드웨어의 이력 상태를 조회하고 보고서를 출력합니다

시스템 모니터 기능을 통해 비디오 관리 소프트웨어 시스템의 상태 개요를 쉽게 확인할 수 있습니다. 또한 오랜 기간 동안 확인할 수 있습니다.

CPU 사용량, 대역폭 또는 기타 하드웨어에 문제가 있었던 기간이 있습니까? 시스템 모니터 기능성을 통해 이에 대한 답변을 찾고 향후 동일한 문제를 피하기 위해 하드웨어 업그레이드 또는 새 하드웨어 구입이 필요한지 결정합니다.

이력 데이터 수집을 활성화하는 것을 잊지 마십시오. 페이지 272의 하드웨어 상태의 이력 데이터 수집를 참조하십시오.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. **시스템 모니터** 창에서 정상 이력 여부를 확인하고자 하는 하드웨어의 타일을 선택하거나 창의 하단에서 서버 또는 카메라를 선택합니다.
3. 관련 서버 또는 카메라의 우측에 있는 **상세 내용** 을 선택합니다.

4. 서버에 대해서는 조사하고자 하는 하드웨어의 우측에 있는 **이력** 을 선택합니다. 카메라에 대해서는 링크를 선택합니다.
5. 보고서를 출력하려면 PDF 아이콘을 선택합니다.

장치가 현재 위치하고 있는 레코딩 서버의 데이터만 포함된 이력 보고서를 생성할 수 있습니다.

서버 운영 체제에서 시스템 모니터의 세부 정보에 액세스할 경우, **Internet Explorer의 고급 보안 구성** 에 관한 메시지가 나타날 수 있습니다. 안내서를 따라 진행하기 전에 **시스템 모니터** 페이지를 **신뢰하는 사이트 영역** 에 추가합니다.

하드웨어 상태의 이력 데이터 수집

시스템 하드웨어 상의 이력 데이터 수집을 활성화하여 오랜 시간에 걸쳐 하드웨어의 상태 그래프를 조회하고 보고서를 출력할 수 있습니다. 자세한 정보는 페이지 271의 하드웨어의 이력 상태를 조회하고 보고서를 출력합니다를 참조하십시오.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. **시스템 모니터** 창에서 **사용자 정의** 를 선택합니다.
3. 열리는 **사용자 정의 대시보드** 창에서 **이력 데이터 수집** 을 선택합니다.
4. 샘플릭 간격을 선택합니다. 간격이 좁을 수록 SQL Server 데이터베이스, 대역폭 또는 기타 하드웨어에 더 많은 부하가 가해집니다. 또한 이력 데이터의 샘플링 간격은 그래프의 상세 정도를 결정해 줍니다.

시스템 모니터 대시보드에서 새 카메라 또는 서버 타일 추가

실제 배치 후 카메라 또는 서버를 작은 그룹으로 모니터하거나 다양한 모니터링 매개변수로 일부 하드웨어를 모니터하고자 하는 경우, **시스템 모니터** 창에서 타일을 추가할 수 있습니다.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. **시스템 모니터** 창에서 **사용자 정의** 를 선택합니다.
3. 열리는 **사용자 정의 대시보드** 창에서 **서버 타일** 또는 **카메라 타일** 아래 있는 **신규** 를 선택합니다.
4. **새 서버 타일/새 카메라 타일** 창에서 모니터링할 카메라나 서버를 선택합니다.
5. **모니터링매개변수**아래에서매개변수에대한확인란을선택하거나선택취소를하여타일에추가하거나제거합니다.
6. **확인** 을 선택합니다. 이제 새 서버 또는 카메라 타일이 대시보드에 표시되는 타일에 추가됩니다.

시스템 모니터 대시보드에서 카메라 또는 서버 타일 편집

다른 모니터링 매개변수로 카메라 또는 서버를 모니터링하고자 하는 경우 이를 조정할 수 있습니다.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. **시스템 모니터** 창에서 **사용자 정의** 를 선택합니다.
3. 열리는 **사용자 정의 대시보드** 창에서 **서버 타일** 또는 **카메라 타일** 아래에서 변경하고자 하는 타일을 선택한 후 **편집** 을 선택합니다.
4. **대시보드 서버/카메라 타일 편집** 창에서 모든 카메라나 서버, 카메라나 서버 그룹, 또는 개별 카메라나 서버를 선택하여 모니터링 매개변수를 변경합니다.
5. **모니터링 매개변수** 아래에서 모니터링하고자 하는 모니터링 매개변수를 선택합니다.
6. **확인** 을 선택합니다.

시스템 모니터 대시보드에서 카메라 또는 서버 타일 삭제

타일로 표시되는 하드웨어를 더 이상 모니터링할 피룡가 없을 때 해당 타일을 삭제할 수 있습니다.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. **시스템 모니터** 창에서 **사용자 정의** 를 선택합니다.
3. 열리는 **사용자 정의 대시보드** 창에서 **서버 타일** 또는 **카메라 타일** 아래에서 변경하고자 하는 타일을 선택합니다.
4. **삭제** 를 선택합니다.

하드웨어 상태가 변경되어야 할 때에 대한 임계값 편집

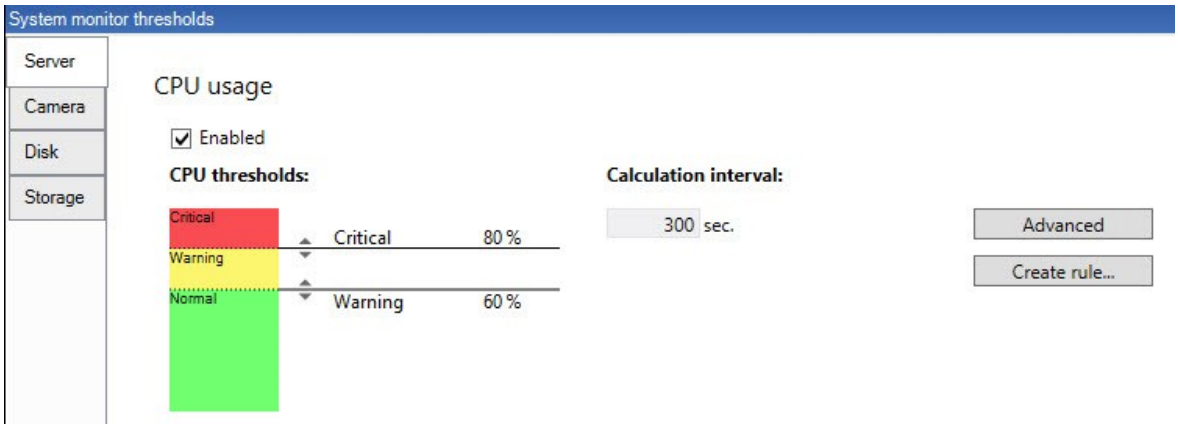
시스템 모니터 대시보드 에서 하드웨어 상태가 세 가지 상태에서 변경될 때에 대한 임계값을 편집할 수 있습니다. 자세한 정보는 페이지 270의 시스템 모니터 임계치(설명됨)를 참조하십시오.

다양한 하드웨어 유형에 대한 임계값을 변경할 수 있습니다. 자세한 정보는 페이지 511의 시스템 모니터 임계값(시스템 대시보드 노드)를 참조하십시오.

기본으로 시스템은 모든 하드웨어 유형(예: 모든 카메라 또는 서버)의 모든 유닛에 대한 임계값을 표시하도록 설정되어 있습니다. 이러한 기본 임계값은 변경할 수 있습니다.

또한 개별 서버 또는 카메라나 이러한 장치의 하위 장치에 대한 임계값을 설정하여 일부 카메라가 다른 카메라보다 높은 **라이브 FPS** 또는 **레코딩 FPS** 를 사용할 수 있게 할 수 있습니다.

1. **사이트 탐색** 창에서 **시스템 대시보드** > **시스템 모니터** 를 선택합니다.
2. 이미 활성화하지 않은 경우 관련 하드웨어에 대한 **활성화** 확인란을 선택합니다. 아래 그림에서 그 예를 볼 수 있습니다.



3. 임계값 제어 슬라이더를 위나 아래로 끌어서 임계값을 늘리거나 줄입니다. **보통**, **경고** 및 **위험** 상태로 분류된 임계값 컨트롤에 표시된 각 하드웨어에 대해 2개의 슬라이더를 이용할 수 있습니다.
4. 계산 간격에 대한 값을 입력하거나 기본값을 유지합니다.
5. 개별 하드웨어에 대한 값을 설정하고자 하는 경우, **고급** 을 선택합니다.
6. 특정 이벤트 또는 특정 시간 간격 내에 규칙을 지정하고자 하는 경우 **규칙 생성** 을 선택합니다.
7. 임계값 및 계산된 간격을 설정한 후에 메뉴에서 **파일** > **저장** 을 선택합니다.

시스템 내 증거물 잠금 보기

시스템 대시보드 노드 아래 **증거물 잠금** 에서는 현재 감시 시스템 상의 모든 보호된 데이터의 개요가 표시됩니다.

나중에 필터링을 통해 증거물 잠금을 찾습니다(예: 생성한 사용자 또는 시기).

1. **사이트 탐색** 창에서 **시스템 대시보드** > **증거물 잠금** 을 선택합니다.
2. 개요를 받고 관련된 증거물 잠금을 찾습니다. 나중에 필터를 적용하여 증거물 잠금에 관련된 다양한 메타데이터를 정렬할 수 있습니다.

증거물 잠금 창에 표시된 모든 정보는 스냅샷입니다. 새로 고치려면 F5 키를 누르십시오.

시스템 구성이 포함된 보고서 출력

비디오 관리 소프트웨어 시스템을 설치하고 구성할 때 다양한 선택을 할 수 있으며, 다음과 같은 문서가 필요할 수도 있습니다. 또한 설치 및 첫 구성 이후 또는 지난 몇 달 동안 변경한 모든 설정은 오랜 시간 기억하기 힘듭니다. 그렇기 때문에 모든 구성 선택 사항을 출력할 수 있게 한 것입니다.

구성 보고서 생성 시(PDF 형식), 시스템의 거의 모든 요소를 보고서에 포함할 수 있습니다. 예를 들어, 라이선스, 장치 구성, 알람 구성 등 다양한 항목을 포함시킬 수 있습니다. **민감한 데이터 예외** 를 선택하여 GDPR 규정을 준수하는 보고서를 생성합니다(기본으로 활성화됨). 폰트, 페이지 설정, 전면 페이지도 사용자 정의할 수 있습니다.

1. **시스템 대시보드** 를 확장한 후 **보고서 구성** 을 선택합니다.
2. 보고서에 포함하거나 제외할 요소를 선택합니다.
3. **선택 사항**: 전면 페이지를 포함하기로 선택한 경우, **전면 페이지** 를 선택하여 전면 페이지의 정보를 사용자 정의합니다. 표시되는 창에서 필요한 정보를 입력합니다.
4. **형식 설정** 을 선택하여 폰트와 페이지 크기, 여백을 사용자 정의합니다. 나타나는 창에서 원하는 설정을 선택합니다.
5. 내보내기할 준비가 되면 **내보내기** 를 선택하고 이름을 선택한 후 보고서를 저장할 위치에 저장합니다.

VMS 시스템의 관리자 권한을 보유한 사용자만 구성 보고서를 생성할 수 있습니다.

메타데이터

메타데이터 검색 카테고리 및 검색 필터 표시 또는 숨기기

사용자 권한을 지닌 XProtect Management Client 사용자는 Milestone 에서 기본 XProtect Smart Client 메타데이터 검색 카테고리 및 검색 필터를 표시하거나 숨길 수 있습니다. 기본으로 이러한 검색 카테고리와 검색 필터는 숨겨져 있습니다. 비디오 관리 시스템이 요건을 만족하는 경우 이를 표시하는 것이 유용합니다(페이지 517의 메타데이터 검색 요건 참조).

이러한 설정은 모든 XProtect Smart Client 사용자에게 영향을 줍니다.

이러한 설정은 다음에 대한 가시성에 영향을 끼치지 않습니다:

- 그 외, 비 메타데이터 Milestone 검색 카테고리 및 검색 필터, 예를 들어 **동작**, **북마크**, **알람** 및 **이벤트**
- 타사 검색 카테고리 및 검색 필터

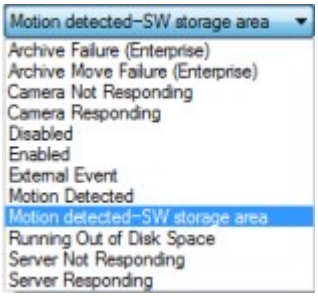
1. XProtect Management Client 의 **사이트 탐색** 창에서, **메타데이터 사용** > **메타데이터 검색** 을 선택합니다.
2. **메타데이터 검색** 창에서 변경하고자 하는 가시성 설정에 대한 검색 카테고리를 선택합니다.
3. 검색 카테고리 또는 검색 필터의 가시성을 활성화하려면 해당하는 확인란을 선택합니다. 검색 카테고리 또는 검색 필터 가시성을 비활성화하려면 확인란을 비웁니다.

알람

알람 추가

알람을 정의하려면 알람 정의를 생성하고 알람을 트리거하는 조건, 운영자가 수행해야 하는 작업에 대한 지침 및 알람이 중단되는 조건이나 시기 등을 지정해야 합니다. 설정과 관련한 자세한 정보는 알람 정의(알람 노드) 을 참조하십시오.

1. **사이트 탐색** 창에서 **알람** 을 확장하고 **알람 정의** 를 우클릭합니다.
2. **새로 추가** 를 선택합니다.
3. 다음 속성을 입력합니다.
    - **이름**: 알람 정의의 이름을 입력합니다. 알람 정의가 등록될 때마다 알람 정의 이름이 나타납니다.
    - **지침**: 알람을 받는 운영자에게 제공할 지침을 작성할 수 있습니다.
    - **트리거 이벤트**: 드롭다운 메뉴를 사용하여 알람이 트리거되는 경우에 사용할 이벤트 유형과 이벤트 메시지를 선택합니다.

      선택가능한트리거링이벤트목록.강조표시한이벤트가생성되고분석이벤트를사용하여사용자정의됩니다.
    - **소스**: 알람을 트리거하기 위해 이벤트가 발생해야 하는 카메라 또는 다른 장치를 선택합니다. 사용할 수 있는 옵션은 선택한 이벤트 유형에 따라 다릅니다.
    - **시간 프로파일**: 알람이 특정 시간 간격 동안 활성화되도록 하려면 라디오 버튼을 선택한 다음 드롭다운 메뉴에서 시간 프로파일을 선택합니다.
    - **이벤트 기반**: 이벤트에 의해 알람 정의가 활성화되도록 하려면 라디오 버튼을 선택하고 알람 정의를 활성화할 이벤트를 지정합니다.또한, 알람 정의를 비활성화할 이벤트를 지정해야 합니다.
4. **시간 제한** 드롭다운 메뉴에서 운영자의 조치가 필요한 시기에 대한 시간 제한을 지정합니다.
5. **트리거된 이벤트** 드롭다운 메뉴에서 시간 제한이 경과했을 때 트리거할 이벤트를 지정합니다.
6. 관련 카메라 및 초기 알람 소유자 등 추가 설정을 지정합니다.

개별 알람 정의에 대한 권한 수정

특정 사용자만 알람을 확인하고 관리하도록 지정하려면 XProtect Management Client에서 알람 정의에 대한 권한을 수정하면 됩니다. 이러한 방법을 사용하면 다음을 보장할 수 있습니다.

- 사용자는 사용자와 관련된 알람만 받을 수 있습니다.
- 승인되지 않은 사용자는 알람에 반응할 수 없습니다.

역할을 사용하여 모든 알람 정의에 대해 동일한 권한을 가져야 하는 사용자를 그룹화할 수 있습니다.

알람 정의에 대한 권한을 수정하려면 다음과 같이 하십시오.

1. **사이트 탐색** 창에서 **보안**을 확장하고 권한을 수정하려는 역할을 선택합니다.
2. **알람** 탭으로 이동하고 **알람 정의**를 확장하여 정의한 알람 목록을 확인합니다.
3. 알람 정의를 선택하여 권한을 수정합니다.

암호화 활성화

관리 서버로 및 관리서버로부터 암호화 활성화

다음과 같은 유형의 원격 서버가 있는 경우 관리 서버 및 관련된 Data Collector 간의 쌍방향 연결을 암호화할 수 있습니다.

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

시스템에 다수의 레코딩 서버 또는 원격 서버가 포함된 경우 반드시 포함된 모든 서버에 대해 암호화를 활성화해야 합니다.

> 서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 암호화가 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

전제 조건:

- 서버 인증 인증서는 관리 서버를 호스트하는 컴퓨터에서 신뢰된 것이어야 합니다.

우선 관리 서버상의 암호화를 활성화합니다.

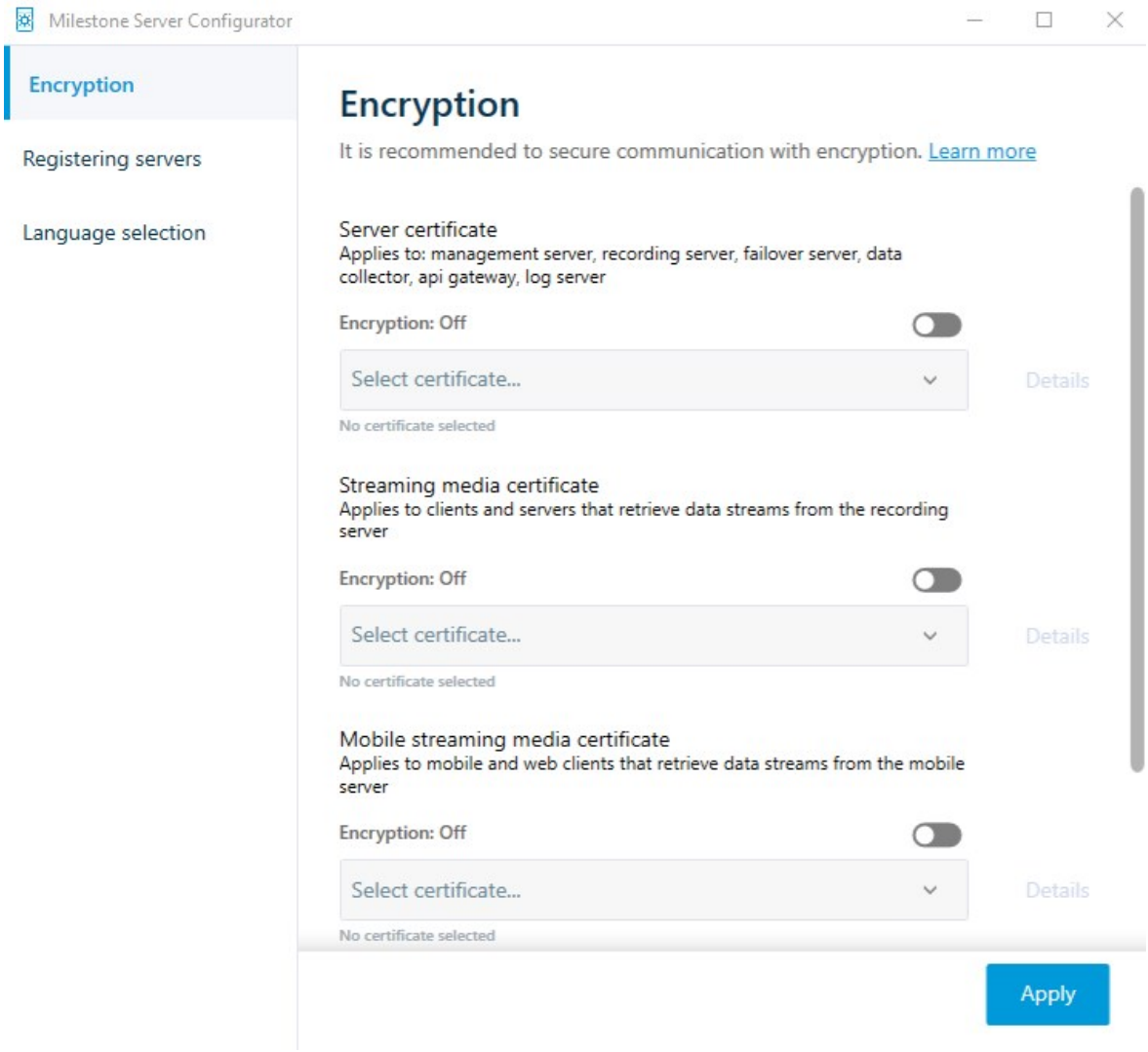
단계:

1. 관리 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   또는

   - Management Server Manager (컴퓨터 작업 표시줄에서 Management Server Manager 아이콘 우클릭)
2. **Server Configurator** 의 **서버 인증** 아래에서 **암호화** 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store의 로컬 컴퓨터에 설치된 인증서의 고유한 주체 이름 목록을 열려면 **인증서 선택**을 클릭합니다.
4. 레코딩 서버, 관리 서버, 장애 조치 서버 및 Data Collector server 간의 통신을 암호화하는 데 사용할 인증서를 선택합니다.

선택된 인증서에 관한 Windows Certificate Store 정보를 보려면 **세부 정보** 를 선택합니다.



5. **적용하기** 를 클릭합니다.

암호화 활성화를 완료하기 위한 다음 단계는 각 레코딩 서버와 Data Collector(Event Server, Log Server, LPR Server,, Mobile Server)이(가) 있는 각 서버상의 암호화 설정을 업데이트하는 것입니다.

자세한 정보는 페이지 278의 레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화를 참조하십시오.

레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화

관리 서버와 레코딩 서버 또는 Data Collector 을(를) 사용하는 기타 원격 서버 간 쌍방향 연결을 암호화할 수 있습니다.

시스템에 다수의 레코딩 서버 또는 원격 서버가 포함된 경우 반드시 포함된 모든 서버에 대해 암호화를 활성화해야 합니다.

자세한 정보는 XProtect VMS 설치 보호 방법에 관한 인증 안내서 를 참조합니다.

서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 암호화가 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

전제 조건:

- 관리 서버에서 암호화를 활성화했습니다. 페이지 277의 관리 서버로 및 관리서버로부터 암호화 활성화를 참조하십시오.

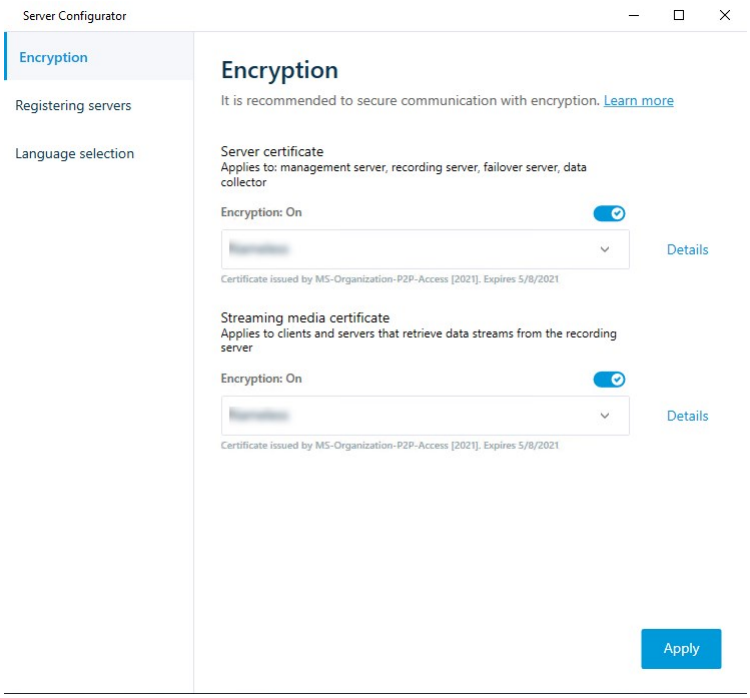
1. ManagementServer또는RecordingServer이(가)설치된컴퓨터에서다음으로부터**ServerConfigurator**을(를)엽니다.
   - Windows 시작 메뉴

   또는

   - 컴퓨터 작업 표시줄에서 서버 관리자 아이콘을 오른쪽 마우스 클릭하여 서버 관리자
2. **Server Configurator** 의 **서버 인증** 아래에서 **암호화** 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store의 로컬 컴퓨터에 설치된 인증서의 고유한 주체 이름 목록을 열려면 **인증서 선택**을 클릭합니다.
4. 레코딩서버,관리서버,장애조치서버및데이터수집기서버간의통신을암호화하는데사용할인증서를선택합니다.

   선택된 인증서에 관한 Windows Certificate Store 정보를 보려면 **세부 정보** 를 선택합니다.

   Recording Server 서비스 사용자는 개인 키에 대한 액세스를 부여받았습니다. 이 인증은 모든 클라이언트에 대해 신뢰될 필요가 있습니다.



5. **적용하기** 를 클릭합니다.

> 인증서를 적용할 경우, 레코딩 서버가 중단되고 재시작합니다. Recording Server 서비스를 중지하면 레코딩 서버의 기본 구성을 확인 또는 변경하는 동안 라이브 비디오를 레코딩하거나 볼 수 없습니다.

이벤트 서버 암호화 활성화

이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간에 쌍방향으로 암호화를 할 수 있습니다.

> 서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 암호화가 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

전제 조건:

- 서버 인증서는 이벤트 서버를 호스팅하는 컴퓨터에서 신뢰됩니다.

우선 이벤트 서버에서 암호화를 활성화합니다.

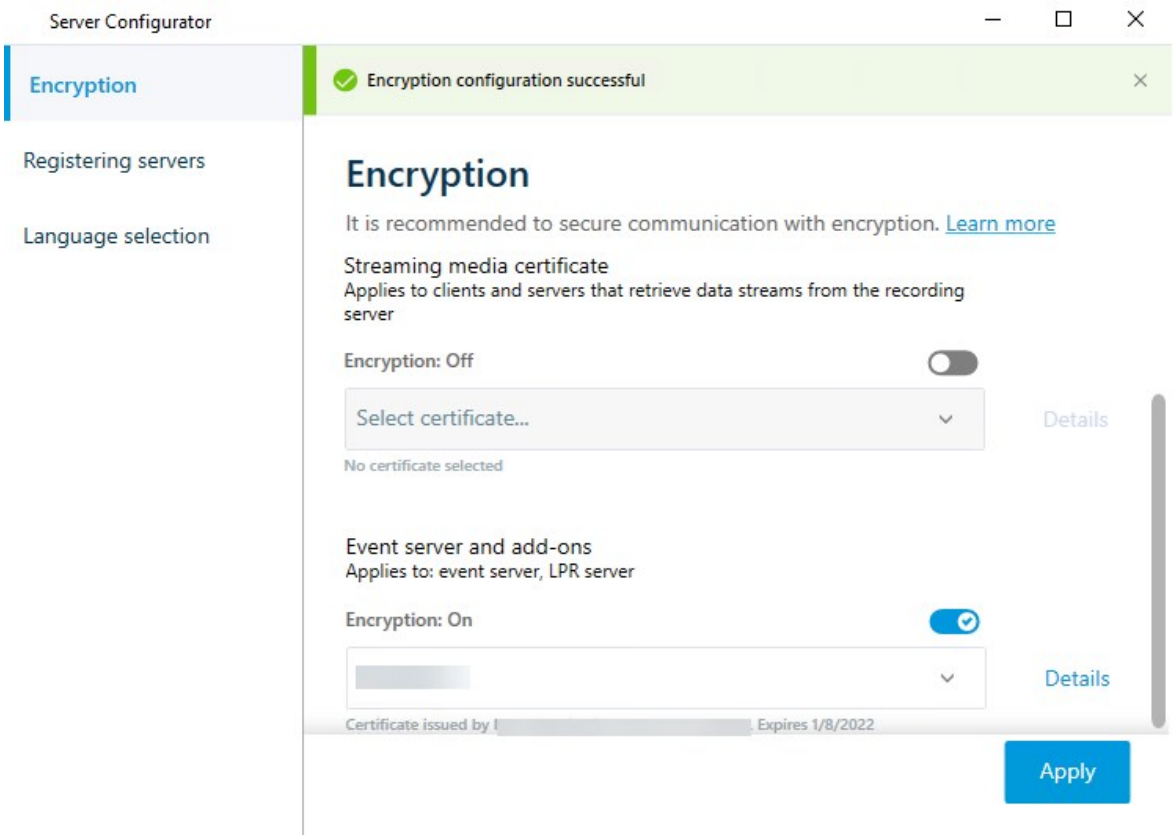
단계:

1. 이벤트 서버가 설치된 컴퓨터에서, 다음에서 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   또는

   - Event Server (컴퓨터 작업 표시줄에서 Event Server 아이콘 우클릭)
2. **Server Configurator** 의 **이벤트 서버 및 추가 기능** 아래에서 **암호화** 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store의 로컬 컴퓨터에 설치된 인증서의 고유한 주체 이름 목록을 열려면 **인증서 선택**을 클릭합니다.
4. 인증서를 선택하여 이벤트 서버와 관련 추가 기능 간 통신을 암호화합니다.

선택된 인증서에 관한 Windows Certificate Store 정보를 보려면 **세부 정보** 를 선택합니다.



5. **적용하기** 를 클릭합니다.

암호화 활성화를 완료하기 위한 다음 단계는 각 관련 확장 LPR Server의 암호화 설정을 업데이트하는 것입니다.

클라이언트 및 서비스에 암호화 활성화

레코딩 서버로부터 데이트를 스트리밍하는 클라이언트와 서버에 레코딩 서버로부터 연결을 암호화할 수 있습니다.

서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 암호화가 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

전제 조건:

- 사용될 서버 인증 인증서는 레코딩 서버에서 데이터 스트림을 검색하는 서비스를 실행 중인 모든 컴퓨터에서 신뢰되어야 합니다.
- XProtect Smart Client 및 레코딩 서버로부터 데이터 스트림을 검색하는 모든 서비스는 2019 R1 이상 버전이어야 합니다.
- 2019 R1 이전 MIP SDK 버전을 이용해 만든 일부 타사 솔루션은 업데이트가 필요할 수 있습니다.

단계:

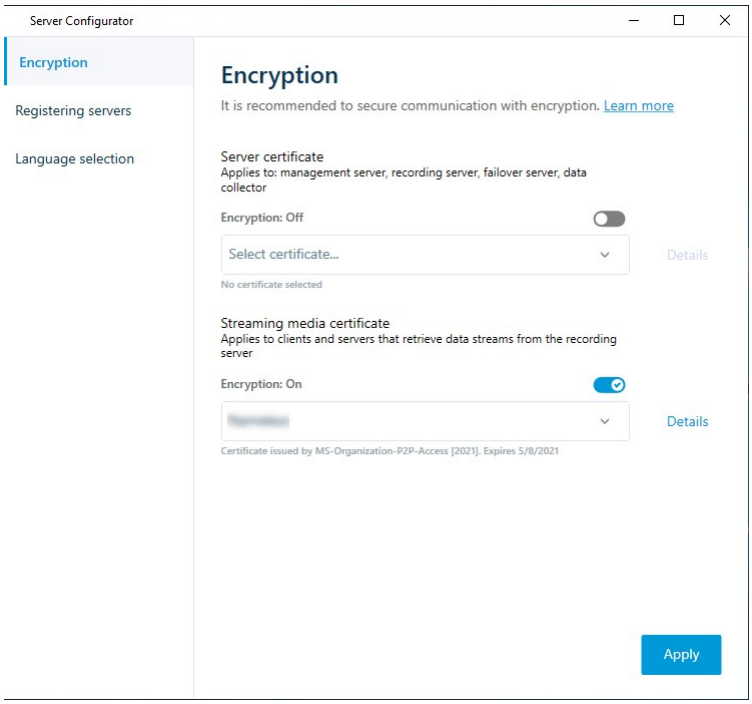
1. 레코딩 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   또는

   - Recording Server Manager (컴퓨터 작업 표시줄에서 Recording Server Manager 아이콘 우클릭)
2. **Server Configurator** 의 **스트리밍 미디어 인증** 아래에서 **암호화** 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store의 로컬 컴퓨터에 설치된 인증서의 고유한 주체 이름 목록을 열려면 **인증서 선택**을 클릭합니다.
4. 레코딩 서버에서 데이터 스트림을 검색하는 클라이언트와 서버 간의 통신을 암호화하려면 인증서를 선택합니다.

   선택된 인증서에 관한 Windows Certificate Store 정보를 보려면 **세부 정보** 를 선택합니다.

   Recording Server 서비스 사용자는 개인 키에 대한 액세스를 부여받았습니다. 이 인증은 모든 클라이언트에 대해 신뢰될 필요가 있습니다.



5. **적용하기** 를 클릭합니다.

> ⚠ 인증서를 적용할 경우, 레코딩 서버가 중단되고 재시작합니다. Recording Server 서비스를 중지하면 레코딩 서버의 기본 구성을 확인 또는 변경하는 동안 라이브 비디오를 레코딩하거나 볼 수 없습니다.

레코딩 서버가 암호화를 사용하는지 확인하려면 클라이언트에 대한 암호화 상태 보기 를 참조하십시오.

모바일 서버 암호화를 활성화합니다

모바일 서버와 클라이언트 및 서비스 간의 보안 연결을 수립하기 위한 HTTPS 프로토콜을 사용하려면 반드시 서버에서 유효한 인증서를 적용해야 합니다. 인증서는 인증서 소유자가 보안 연결을 설정할 권한이 있음을 나타냅니다.

자세한 정보는 XProtect VMS 설치 보호 방법에 관한 인증 안내서 를 참조합니다.

서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 암호화가 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

CA(인증 기관, Certificate Authority)가 발행한 인증서는 인증서 체인을 가지고 있으며, 해당 체인의 루트에는 CA 루트 인증서가 있습니다. 하나의 장치나 브라우저가 이 인증서를 발견할 경우, 루트 인증서를 OS(Android, iOS, Windows 등)에 사전 설치된 인증서와 비교합니다. 루트 인증서가 사전 설치된 인증서 목록에 나열될 경우, OS는 사용자에게 서버 연결이 충분히 안전함을 나타냅니다. 이러한 인증서는 하나의 도메인 이름에 대해 발행되며 무료입니다.

단계:

1. 모바일 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

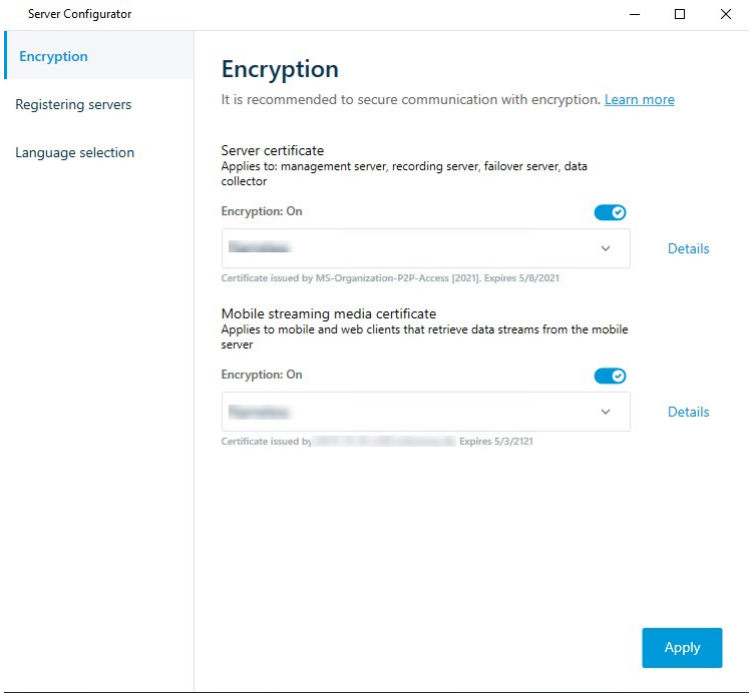
   또는

   - Mobile Server Manager (컴퓨터 작업 표시줄에서 Mobile Server Manager 아이콘 우클릭)
2. **Server Configurator** 의 **모바일 스트리밍 미디어 인증** 아래에서 **암호화** 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store의 로컬 컴퓨터에 설치된 인증서의 고유한 주체 이름 목록을 열려면 **인증서 선택**을 클릭합니다.
4. 인증서를 선택하여 XProtect Mobile 클라이언트와 모바일 서버의 XProtect Web Client 간 통신을 암호화합니다.

   선택된 인증서에 관한 Windows Certificate Store 정보를 보려면 **세부 정보** 를 선택합니다.

   Mobile Server 서비스 사용자는 개인 키에 대한 액세스를 부여받았습니다. 이 인증은 모든 클라이언트에 대해 신

뢰될 필요가 있습니다.



5. **적용하기** 를 클릭합니다.

인증서 적용 시 Mobile Server 서비스가 다시 시작됩니다.

Milestone Federated Architecture

연합 사이트 실행을 위한 시스템 설정

Milestone Federated Architecture 에 맞게 시스템을 준비하려면 관리 서버를 설치할 때 특정 선택을 해야 합니다. IT 인프라 설정 방식에 따라 세 가지 대안 중에서 선택할 수 있습니다.

대안 1: 동일 도메인으로부터 사이트 연결(공통 도메인 사용자)

관리 서버를 설치하기 전에 공통 도메인 사용자를 생성하고 연합 사이트 계층 구조에 관련된 모든 서버에서 이 사용자를 관리자로 구성해야 합니다. 사이트 접속 방법은 생성된 사용자 계정에 따라 다릅니다.

Windows 사용자 계정으로

1. 관리 서버로 사용할 서버에 제품 설치를 시작하고 **사용자 정의** 를 선택합니다.
2. 사용자 계정을 사용하여 Management Server 서비스를 설치하도록 선택합니다. 선택한 사용자 계정은 모든 관리 서버에서 사용되는 관리자 계정이어야 합니다. 연합 사이트 계층 구조에서 다른 관리 서버를 설치할 때 동일

한 사용자 계정을 사용해야 합니다.

3. 설치를 완료합니다. 1-3단계를 반복하여 연합 사이트 계층 구조에 추가하려는 다른 모든 시스템을 설치합니다.
4. 계층 구조에 사이트 추가(페이지 286의 계층 구조에 사이트 추가 참조).

Windows 내장 사용자 계정(네트워크 서비스)으로

1. 관리 서버로 사용할 첫 번째 서버에 제품 설치를 시작하고 **단일 서버** 또는 **사용자 설정** 을 선택합니다. 그러면 네트워크 서비스 계정을 사용하여 관리 서버가 설치됩니다. 연합 사이트 계층 구조에 있는 모든 사이트에 대해 이 단계를 반복합니다.
2. 연합 사이트 계층 구조에서 중앙 사이트로 사용할 사이트에 로그인합니다.
3. Management Client 에서 **보안** > **역할** > **관리자** 를 확장합니다.
4. **사용자 및 그룹** 탭에서 **추가** 를 클릭하고 **Windows 사용자** 를 선택합니다.
5. 대화 상자에서 개체 유형으로 **컴퓨터** 를 선택하고 연합 사이트의 서버 이름을 입력한 다음 **확인** 을 클릭하여 서버를 중앙 사이트의 **관리자** 역할에 추가합니다. 이런 식으로 모든 연합 사이트를 추가할 때까지 이 단계를 반복한 다음 응용 프로그램을 종료합니다.
6. 각 연합 사이트에 로그인하여 위에서와 같은 방식으로 다음 서버를 **관리자** 역할에 추가합니다.
   - 상위 사이트 서버.
   - 이 연합 사이트에 직접 연결할 하위 사이트 서버.
7. 계층 구조에 사이트 추가(페이지 286의 계층 구조에 사이트 추가 참조).

대안 2: 다른 도메인으로부터 사이트 연결

도메인 전체에서 사이트에 연결하려면 이러한 도메인이 서로 신뢰하도록 해야 합니다. Microsoft Windows 도메인 구성에서 도메인이 서로 신뢰하도록 설정합니다. 연합 사이트 계층의 각 사이트에서 서로 다른 도메인 사이에 신뢰 관계를 설정했을 때, 대안 1에 설명된 것과 동일한 설명을 따릅니다. 신뢰할 수 있는 도메인의 설정 방법에 대한 자세한 내용은 Microsoft 웹사이트(https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/)를 참조하십시오.

Milestone 은 다수의 도메인과 연결된 다중 사이트 시스템을 생성할 때 Milestone Interconnect 를 사용할 것을 권장합니다.

대안 3: 작업 그룹의 사이트 연결

작업 그룹 내의 사이트를 연결하는 경우 연합 사이트 계층 구조에서 연결하려는 모든 서버에 동일한 관리자 계정이 있어야 합니다. 시스템을 설치하기 전에 관리자 계정을 정의해야 합니다.

1. 공통 관리자 계정을 사용하여 **Windows** 에 로그인합니다.
2. 제품 설치를 시작하고 **사용자 정의** 를 클릭합니다.
3. 공통 관리자 계정을 사용하여 Management Server 서비스를 설치하도록 선택합니다.
4. 설치를 완료합니다. 1-4단계를 반복하여 연결할 다른 모든 시스템을 설치합니다. 공통 관리자 계정을 사용하여 이러한 모든 시스템을 설치해야 합니다.
5. 계층 구조에 사이트 추가(페이지 286의 계층 구조에 사이트 추가 참조).

Milestone 은 사이트가 도메인에 속하지 않은 경우 연결된 다중 사이트 시스템을 생성할 때 Milestone Interconnect 를 사용할 것을 권장합니다.

도메인과 작업 그룹을 혼합하여 사용할 수 없습니다. 즉, 도메인의 사이트를 작업 그룹의 사이트 나 그와 반대로 연결할 수 없습니다.

계층 구조에 사이트 추가

시스템이올바르게설정되어있다면이후확장함에따라상위사이트와해당하는하위사이트에사이트를추가할수있습니다.

비보안 사이트를 Milestone Federated Architecture에 추가할 때는 Management Client의 **도구** > **옵션** > **일반 설정**에서 **서버에 대한 비보안 연결 허용**이 활성화되어 있는지 확인하십시오.

1. **연합 사이트 계층** 창을 선택합니다.
2. 하위 사이트를 추가할 사이트를 선택하고 마우스 오른쪽 버튼을 클릭한 다음, **계층에 사이트 추가** 를 클릭합니다.
3. **계층에 사이트 추가** 창에서 요청된 사이트의 URL을 입력하고 **확인** 을 클릭합니다.
4. 상위 사이트가 하위 사이트로 연결 요청을 전송하고, 잠시 후 두 사이트 사이의 링크가 **연합 사이트 계층** 창에 추가됩니다.
5. 하위 사이트 관리자로부터 승인을 요청하지 않고 하위 사이트에 대한 연결을 설정할 수 있으면 7단계로 이동하십시오.

   그렇지 않으면 하위 사이트 관리자가 해당 요청을 승인할 때까지 하위 사이트에 승인 대기 아이콘이 표시됩니다.
6. 하위 사이트의 관리자가 상위 사이트의 링크 요청을 승인해야 한다는 것을 명심하십시오(페이지 286의 계층에 포함 허용 참조).
7. 새 상위/하위 연결이 설정되고 새로운 하위 사이트의 **아이콘과 함께** 연합 사이트 계층 창이 업데이트됩니다.

계층에 포함 허용

관리자에게 하위 사이트에 대한 관리자 권한이 없는 잠재적 상위 사이트로부터 하위 사이트로 링크 요청이 수신되면 승인 대기 아이콘이 표시됩니다.

연결 요청을 수락하려면:

1. 사이트에 로그인합니다.
2. **연합 사이트 계층** 창에서, 사이트를 마우스 오른쪽 버튼으로 클릭하고 **계층에 포함 허용** 을 클릭합니다.

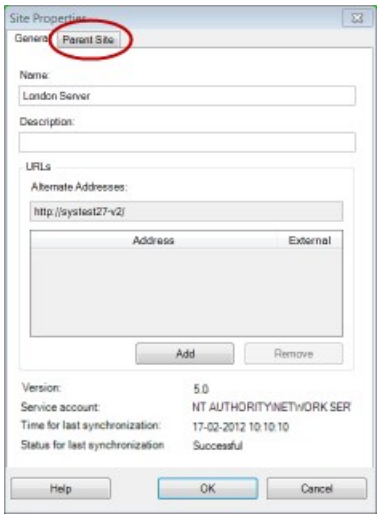
   사이트가 XProtect Expert 버전을 실행하는 경우, **사이트 탐색** 창에서 사이트를 마우스 오른쪽 버튼으로 클릭합니다.
3. **예** 를 클릭합니다.
4. 새 상위/하위 연결이 설정되고 선택한 사이트의 일반 사이트 **아이콘과 함께** 연합 사이트 계층 창이 업데이트됩니다.

> 상위 사이트에서 멀리 있는 하위 사이트에 대한 변경 내용을 **연합 사이트 계층** 창에 반영하는 데 약간의 시간이 걸릴 수 있습니다.

사이트 속성 설정

홈 사이트와 그 하위 사이트에서 속성을 표시하고, 필요 시 편집할 수 있습니다.

1. Management Client 의 **연합 사이트 계층** 창에서 관련 사이트를 선택하고, 마우스 오른쪽 버튼을 클릭한 다음 **속성** 을 선택합니다.



2. 필요한 경우, 다음을 변경합니다.

   일반 탭(페이지 532의 일반 탭 참조)

   상위 사이트 탭(페이지 532의 상위 사이트 탭 참조) **(하위 사이트에서만 사용 가능)**

> 동기화 문제로 인해 원격 하위 사이트에 이루어진 변경 내용이 **사이트 탐색** 창에 반영되려면 다소 시간이 걸릴 수 있습니다.

사이트 계층 새로 고침

시스템이 모든 상위/하위 설정 수준을 통해 정기적으로 계층 자동 동기화를 수행합니다. 계층 구조에서 변경 내용이 즉시 반영되도록 하고 다음 자동 동기화 때까지 기다리기를 원하지 않는 경우 새로 고침을 수행할 수 있습니다.

수동 새로 고침을 수행하려면 사이트에 로그인해야 합니다. 마지막 동기화 이후 이 사이트에서 저장된 변경 내용만 새로 고침에 의해 반영됩니다. 즉, 변경 내용이 아직 사이트에 도달하지 않았다면 계층 구조의 더욱 아래쪽에서 수행된 변경은 수동 업데이트로 반영되지 않을 수 있습니다.

1. 관련 사이트에 로그인합니다.
2. **연합 사이트 계층** 창에서 최상위 사이트를 마우스 오른쪽 버튼으로 클릭하고 **사이트 계층 새로 고침** 을 클릭합니다.

   이 때 몇 초 정도 걸립니다.

계층 구조의 다른 사이트에 로그인합니다.

다른 사이트에 로그인하고 이러한 사이트를 관리할 수 있습니다. 로그인한 사이트가 홈 사이트입니다.

1. **연합 사이트 계층 구조** 창에서 로그인하려는 사이트를 마우스 오른쪽 버튼으로 클릭합니다.
2. **사이트에 로그인** 을 클릭합니다.

   Management Client 해당 사이트의 이(가) 열립니다.
3. 로그인 정보를 입력하고 **확인** 을 클릭합니다.
4. 로그인이 완료되면 해당 사이트에 대한 관리 작업을 수행할 수 있습니다.

하위 사이트의 사이트 정보 업데이트

이 섹션은 XProtect Corporate 또는 XProtect Expert 2014 이상 버전을 사용하는 경우에만 관련이 있습니다.

많은 하위 사이트를 포함한 대규모 Milestone Federated Architecture 설정에서는 개요를 상실하기 쉬우며 각 하위 사이트의 관리자에 대한 연락처 정보를 찾기 힘들 수 있습니다.

이를 위해 각 하위 사이트에 추가 정보를 추가한 후 중앙 사이트의 관리자에게 이 정보 접근 권한을 허용할 수 있습니다.

연합 사이트 계층 구조 창의 사이트 이름 위에 마우스 포인터를 가져가면 해당 사이트에 관한 정보를 읽을 수 있습니다. 해당 사이트에 관한 정보를 업데이트하려면 다음과 같이 하십시오.

1. 사이트에 로그인합니다.
2. **사이트 탐색** 창을 클릭하고 **사이트 정보** 를 선택합니다.
3. **편집** 을 클릭하고 각 카테고리 내에 관련 정보를 추가합니다.

계층에서 사이트 분리

사이트를 상위 사이트에서 분리하면 사이트 간의 연결이 끊깁니다. 사이트를 중앙 사이트나, 사이트 자체 또는 그 상위 사이트에서 분리할 수 있습니다.

1. **연합 사이트 계층 구조** 창에서 분리하려는 사이트를 마우스 오른쪽 버튼으로 클릭하고 **계층에서 사이트 분리** 를 클릭합니다.
2. **예** 를 클릭하여 **연합 사이트 계층 구조** 창을 업데이트합니다.

   분리된 사이트에 하위 사이트가 있는 경우, 이 사이트가 계층의 이 지점에 대해 새로운 최상위 사이트가 되고, 일반 사이트 아이콘 이 최상위 사이트 아이콘 으로 바뀝니다.
3. **확인** 을 클릭합니다.

계층 구조의 변경 내용은 수동 새로 고침 또는 자동 동기화 이후 반영됩니다.

Milestone Interconnect

중앙 Milestone Interconnect 사이트에 원격 사이트 추가

하드웨어 추가 마법사를 이용하여 중앙 사이트에 원격 사이트를 추가합니다.
요구사항

- 충분한 Milestone Interconnect 카메라 라이선스(페이지 85의 Milestone Interconnect 및 라이센싱 참조).
- 중앙 XProtect 시스템이 액세스할 수 있어야 하는 장치에 대한 권한을 가진 사용자 계정(기본 사용자, 로컬 Windows 사용자 또는 Windows Active Directory 사용자)을 포함하고 있는 구성되어 작동하는 다른 XProtect Corporate 시스템
- 원격 사이트에서 사용되는 포트에 대한 액세스 또는 포트 전달 기능을 포함하여 중앙 XProtect Corporate 사이트와 원격 사이트 사이의 네트워크 연결

원격 사이트를 추가하려면:

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 관련 레코딩 서버를 확장하고 마우스 오른쪽 버튼을 클릭합니다.
3. **하드웨어 추가** 를 선택하여 마법사를 시작합니다.
4. 첫 페이지에서 **주소 범위 스캔** 또는 **수동** 을 선택한 후, **다음** 을 클릭합니다.
5. 사용자 이름과 암호를 지정합니다. 원격 시스템에서 사용자 계정이 사전 정의되어 있어야 합니다. **추가** 를 클릭하여 필요에 따라 사용자 이름과 암호를 추가할 수 있습니다. 준비가 되면 **다음** 을 클릭합니다.
6. 스캔할 때 사용할 드라이버를 선택합니다. 이 경우, Milestone 드라이버 중에서 선택합니다. **다음** 을 클릭합니다.

7. 스캔하려는 IP 주소와 포트 번호를 지정합니다. 기본 포트 번호는 80입니다. **다음** 을 클릭합니다.

   시스템이 원격 사이트를 감지하는 동안 기다립니다. 상태 표시기가 감지 프로세스를 나타냅니다. 성공적으로 감지되면 **상태** 열에 **성공** 메시지가 나타납니다. 추가에 실패하면 **실패** 오류 메시지를 클릭하여 이유를 볼 수 있습니다.

8. 성공적으로 감지된 시스템을 사용할지 여부를 선택합니다. **다음** 을 클릭합니다.
9. 시스템이 하드웨어를 감지하고 장치에 특정한 정보를 수집하는 동안 기다립니다. **다음** 을 클릭합니다.
10. 성공적으로 감지된 하드웨어와 장치를 사용할지 여부를 선택합니다. **다음** 을 클릭합니다.
11. 기본 그룹을 선택합니다. **마침** 을 클릭합니다.
12. 설치 후, **개요** 창에서 시스템과 장치를 볼 수 있습니다.

    원격 사이트에서 선택한 사용자의 사용자 권한에 따라 중앙 사이트가 모든 카메라와 기능 또는 해당 항목의 하위 세트에 대한 액세스 권한을 갖게 됩니다.

사용자 권한 할당

역할을 생성하고 기능에 대한 액세스를 할당함으로써 다른 카메라에 대해 했던 것처럼 상호 연결된 카메라에 대한 사용자 권한을 구성할 수 있습니다.

1. 중앙 사이트의 **사이트 탐색** 창 내에서 **보안** 을 확장하고 **역할** 을 선택합니다.
2. 개요 창에서 내장 관리자 역할을 우클릭하고 **역할 추가** 를 선택합니다(역할 추가 및 관리 를 참조하십시오).
3. 역할에 이름을 정하고 **장치** 탭(장치 탭(역할) 참조) 및 **원격 레코딩** 탭(원격 레코딩 탭(역할) 참조)에서 설정을 구성합니다.

원격 사이트 하드웨어 업데이트

카메라 및 이벤트를 추가 또는 제거하는 등 원격 사이트에서 구성이 변경된 경우, 원격 사이트의 새 구성이 반영되도록 중앙 사이트에서 구성을 업데이트해야 합니다.

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 필요한 레코딩 서버를 확장하고 해당 원격 시스템을 선택합니다. 하드웨어를 마우스 오른쪽 단추로 클릭합니다.
3. **하드웨어 업데이트** 를 선택합니다. 이렇게 하면 **하드웨어 업데이트** 대화 상자가 열립니다.
4. 대화 상자에 Milestone Interconnect 설치를 구성하거나 마지막으로 새로 고친 이후 원격 시스템에 적용된 모든 변경 내용(장치 제거, 업데이트 및 추가)이 나열됩니다. **확인** 을 클릭하여 이러한 변경 내용으로 중앙 사이트를 업데이트합니다.

원격 사이트 카메라에서 직접 재생 활성화

중앙 사이트가 원격 사이트에 계속 연결되어 있는 경우, 사용자가 원격 사이트에서 직접 레코딩을 재생하도록 시스템을 구성할 수 있습니다. 자세한 정보는 페이지 85의 Milestone Interconnect 설치(설명됨)를 참조하십시오.

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 필요한 레코딩 서버를 확장하고 해당 원격 시스템을 선택합니다. 상호 연결된 관련 카메라를 선택합니다.
3. 속성 창에서 **레코딩** 탭을 선택하고 **원격 시스템에서 레코딩 재생** 옵션을 선택합니다.
4. 도구 모음에서 **저장** 을 클릭합니다.

Milestone Interconnect 설치에서는 중앙 사이트가 원격 사이트에 정의된 사생활 보호를 무시합니다. 동일한 사생활 보호를 적용하려면 중앙 사이트에서 이를 다시 정의해야 합니다.

원격 사이트 카메라에서 원격 레코딩 검색

중앙 사이트가 원격 사이트에 연속해서 연결되지 **않는** 경우 원격 레코딩을 중앙에 저장하도록 시스템을 구성하고 네트워크 연결이 최적일 때 원격 레코딩을 가져오도록 구성할 수 있습니다. 자세한 정보는 페이지 85의 Milestone Interconnect 설치(설명됨)를 참조하십시오.

사용자가 실제로 레코딩을 검색할 수 있게 하려면, 관련 역할에 대해 이 권한을 활성화해야 합니다(역할(보안) 참조).

시스템을 구성하려면:

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 필요한 레코딩 서버를 확장하고 해당 원격 시스템을 선택합니다. 관련 원격 서버를 선택합니다.
3. 속성 창에서 **원격 검색** 탭을 선택하고 설정을 업데이트합니다(페이지 395의 원격 검색 탭 참조).

특정 이유로 네트워크가 실패하면 중앙 사이트에서 레코딩 시퀀스가 누락됩니다. 네트워크가 다시 구성되면 중단 기간 중의 레코딩을 확보하기 위해 중앙 사이트에서 원격 레코딩을 자동으로 검색하도록 시스템을 구성할 수 있습니다.

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 필요한 레코딩 서버를 확장하고 해당 원격 시스템을 선택합니다. 해당 카메라를 선택합니다.
3. **속성** 창에서, 레코딩 탭을 선택하고, **연결이 복원될 때 원격 레코딩 자동 검색** 옵션을 선택합니다(원격 레코딩 저장 및 검색 참조).
4. 도구 모음에서 **저장** 을 클릭합니다.

대체 수단으로, 규칙을 사용하거나 혹은 필요 시 XProtect Smart Client 에서 원격 레코딩 검색을 시작할 수도 있습니다.

Milestone Interconnect 설치에서는 중앙 사이트가 원격 사이트에 정의된 사생활 보호를 무시합니다. 동일한 사생활 보호를 적용하려면 중앙 사이트에서 이를 다시 정의해야 합니다.

원격 사이트의 이벤트에 응답하도록 중앙 사이트 구성

원격 사이트에서 정의된 이벤트를 사용하여 중앙 사이트에서 규칙과 알람을 트리거하고 이에 따라 원격 사이트의 이벤트에 즉시 대응할 수 있습니다. 이를 위해서는 원격 사이트가 연결되어 있고 온라인 상태여야 합니다. 이벤트 수와 유형은 원격 시스템에 구성되고 사전 정의된 이벤트에 따라 다릅니다.

지원되는 이벤트 목록은 Milestone 웹 사이트(https://www.milestonesys.com/)에서 확인할 수 있습니다.

사전 정의된 이벤트는 삭제할 수 없습니다.

요구사항:

- 원격 사이트의 사용자 정의/수동 이벤트를 트리거링 이벤트로 사용하려면, 우선 원격 사이트에서 이러한 이벤트를 생성해야 합니다
- 원격 사이트의 업데이트된 이벤트 목록을 갖고 있는지 확인하십시오(페이지 290의 원격 사이트 하드웨어 업데이트 참조).

다음과 같이 원격 사이트에서 사용자 정의/수동 이벤트를 추가합니다.

1. 중앙 사이트에서 **서버** 를 확장하고 **레코딩 서버** 를 선택합니다.
2. 개요 창에서 관련 원격 서버와 **이벤트 탭** 을 선택합니다.
3. 목록에 사전 정의된 이벤트가 포함됩니다. **추가** 를 클릭하여 목록에서 원격 사이트의 사전 정의 또는 수동 이벤트를 포함시킵니다.

원격 사이트의 이벤트를 사용하여 중앙 사이트에서 알람 트리거:

1. 중앙 사이트에서 **알람** 을 확장하고 **알람 정의** 를 선택합니다.
2. 개요 창에서 **알람 정의** 를 마우스 오른쪽 버튼으로 클릭하고 **새 항목 추가** 를 클릭합니다.
3. 필요에 따라 값을 입력합니다.
4. **트리거링 이벤트** 필드에서 지원되는 사전 정의 이벤트와 사용자 정의 이벤트 중에서 선택할 수 있습니다.
5. **소스** 필드에서 알람의 소스로 이용할 원격 사이트를 나타내는 원격 서버를 선택합니다.
6. 끝났으면 구성을 저장합니다.

원격 사이트의 이벤트를 사용하여 중앙 사이트에서 규칙 기반 동작 트리거:

1. 중앙 사이트에서 **규칙 및 이벤트** 를 확장하고 **규칙** 을 선택합니다.
2. 개요 창에서 **규칙** 을 마우스 오른쪽 버튼으로 클릭하고 **규칙 추가** 를 클릭합니다.
3. 표시되는 마법사에서 **<이벤트>상의 동작 수행** 을 선택합니다.
4. **규칙 설명 편집** 영역에서 **이벤트** 를 클릭하고 지원되는 사전 정의 이벤트와 사용자 정의 이벤트 중에서 선택합니다. **확인** 을 클릭합니다.
5. **장치/레코딩 서버/관리 서버** 를 클릭하고 중앙 사이트가 동작을 시작하게 하려는 대상 원격 사이트를 나타내는 원격 서버를 선택합니다. **확인** 을 클릭합니다.
6. **다음** 을 클릭하여 다음 마법사 페이지로 이동합니다.
7. 이 규칙에 대해 적용하려는 조건을 선택합니다. 어떤 조건도 선택하지 않으면 규칙이 항상 적용됩니다. **다음** 을 클릭합니다.

8. 동작을 선택하고 **규칙 설명 편집** 영역에서 상세 정보를 지정합니다. **다음** 을 클릭합니다.
9. 필요한 경우 중지 기준을 선택합니다. **다음** 을 클릭합니다.
10. 필요한 경우 중지 동작을 선택합니다. **마침** 을 클릭합니다.

원격 연결 서비스

원격 연결 서비스(설명됨)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

원격 연결 서비스 기능에는 Axis Communications에서 개발한 Axis One-click 카메라 연결 기술이 포함되어 있습니다. 이 기능은 시스템이 방화벽 및/또는 라우터 네트워크 구성으로 인해 해당 카메라에 대한 연결이 초기화되지 않는 외부 카메라로부터 비디오(및 오디오)를 검색할 수 있게 해줍니다. 실제 통신은 보안 터널 서버(ST 서버)를 통해 이뤄집니다. ST 서버는 VPN을 사용합니다. 유효한 키를 보유한 장비만 VPN에서 작동합니다. 이는 공공 네트워크에서 안전하게 데이터를 교환할 수 있는 보안 터널을 제공합니다.

원격 연결 서비스를 통해 다음을 수행할 수 있습니다.

- Axis 디스패치 서비스 내 인정 정보 편집
- ST 서버 추가, 편집, 제거
- Axis One-click 카메라 등록/등록해제 및 편집
- Axis One-Click 카메라와 관련 있는 하드웨어로 이동

One-Click 카메라 연결에 대한 보안 터널 서버 환경 설치

Axis One-click 카메라 연결을 사용하기 전에 적합한 ST 서버 환경을 우선 설치해야 합니다. 보안 터널 서버(ST 서버) 환경 및 Axis One-click 카메라에서 작업하려면, 우선 시스템 제공자에게 연락하여 Axis 디스패치 서비스에 필요한 사용자 이름과 암호를 얻어야 합니다.

요구사항

- Axis 디스패치 서비스에 필요한 사용자 이름과 암호를 얻으려면 시스템 제공자에게 문의하십시오.
- 카메라가 Axis 비디오 호스팅 시스템을 지원하는지 확인하십시오. Axis 웹사이트를 방문하여 지원되는 장치를 확인하십시오(https://www.axis.com/products/axis-guardian)
- 필요한 경우 Axis 카메라를 최신 펌웨어로 업데이트하십시오. Axis 웹사이트를 방문하여 펌웨어를 다운로드하십시오(https://www.axis.com/support/firmware)

1. 각 카메라의 홈페이지에서 **기본 설정**, **TCP/IP** 로 이동한 후 **AVHS 활성화** 및 **항상** 을 선택하십시오.
2. 관리 서버에서 Milestone 다운로드 페이지(https://www.milestonesys.com/downloads/)로 이동한 후 **AXIS One-Click** 소프트웨어를 다운로드합니다. 응용프로그램을 구동하여 적합한 Axis 보안 터널 프레임워크를 설정합니다.

보안 터널 서버 추가 또는 편집

원격 연결 서비스를 위한 통신은 보안 터널 서버(ST 서버)를 통해 이뤄집니다.

1. 다음 중 하나를 수행하십시오.
   - ST 서버를 추가하려면 **Axis 보안 터널 서버** 탑 노드를 우클릭한 후 **Axis 보안 터널 서버 추가** 를 선택합니다.
   - ST 서버를 편집하려면 ST 서버를 우클릭한 후 **Axis 보안 터널 서버 편집** 을 선택합니다.
2. 창이 열리면 관련 정보를 입력합니다.
3. **Axis One-Click Connection 구성요소** 설치 시 인증 정보를 사용하려면 **인증 정보 사용** 체크 상자를 선택 후 **Axis One-Click Connection 구성요소** 에 사용한 것과 동일한 사용자 이름과 암호를 입력합니다.
4. **확인** 을 클릭합니다.

신규 Axis One-Click 카메라 등록

1. ST 서버에 카메라를 등록하려면, 우클릭 후 **Axis One-Click 카메라 등록** 을 선택합니다.
2. 창이 열리면 관련 정보를 입력합니다.
3. **확인** 을 클릭합니다.
4. 이제 카메라가 관련 ST 서버에 나타납니다.

카메라는 다음과 같은 색상 코딩을 지닐 수 있습니다:

색상	설명
빨간색	초기 상태. 등록되었으나 ST 서버에 연결되지 않았습니다.
노란색	등록되었습니다. ST 서버에 연결되었으나 하드웨어로 추가되지 않았습니다.
초록색	하드웨어로 추가되었습니다. ST 서버 연결 여부가 확인되지 않았습니다.

새 카메라 추가 시, 카메라의 상태는 항상 녹색입니다. 연결 상태는 **개요** 창에 있는 **레코딩 서버** 의 **장치** 에 반영되어 있습니다. **개요** 창에서 개요를 간편하게 볼 수 있도록 카메라를 그룹화할 수 있습니다. 이 시점에서 Axis 스패치 서비스에 카메라를 등록하지 **않기로** 선택하는 경우, 우클릭 메뉴를 통해 나중에 등록할 수 있습니다(**Axis One-Click 카메라 편집** 선택).

스마트 맵

지리적 배경(설명됨)

XProtect Smart Client 의 사용자가 지리적 배경을 선택하기 전에 XProtect Management Client 에서 우선 지리적 배경을 구성해야 합니다.

- **기본 세계 지도** - XProtect Smart Client 에서 제공된 표준 지리적 배경을 사용합니다. 구성할 필요가 없습니다. 이 맵은 일반 참조로 사용하기 위한 것으로, 국경선, 도시 또는 기타 세부 정보와 같은 기능을 포함하지 않습니다. 그러나 다른 지리적 배경처럼 지리 참조 데이터는 포함되어 있습니다
- **Bing Maps** - Bing Maps에 연결
- **Google Maps** - Google Maps에 연결
- **Milestone Map Service** - 무료 맵 제공자에 연결합니다. Milestone Map Service 을(를) 활성화한 후에는 추가 설정이 필요하지 않습니다.

  Milestone Map Service 활성화 를 참조

- **OpenStreetMap** - 다음으로 연결됩니다.
  - 직접 선택한 상용 타일 서버
  - 자체 사용 중인 온라인 또는 로컬 타일 서버

  OpenStreetMap 타일 서버 지정 참조

Bing Maps 및 Google Maps 옵션은 인터넷 액세스를 필요로 하며, Microsoft 또는 Google에서 키를 구매해야 합니다.

Milestone Map Service 은(는) 인터넷 액세스가 필요합니다.

자체적으로 사용하는 중이 아니라면 로컬 타일 서버인 OpenStreetMap 또한 인터넷 접속이 필요합니다.

사용중인시스템에EUGDPR준수설치를하고자하는경우,다음서비스는사용되지않을수도있습니다.

- Bing Maps
- Google Maps
- Milestone Map Service

데이터보호및사용량데이터수집에관한자세한내용은GDPR개인정보보호지침을참조하십시오.

기본적으로, Bing Maps 및 Google Maps는 위성 이미지를 표시합니다(위성). 예를 들어 항공 또는 지형 이미지와 같이 XProtect Smart Client 에서 이미지를 변경하여 다른 세부 정보를 볼 수 있습니다.

Bing Maps 또는 Google Maps를 다음에서 활성화: Management Client

Smart Client 에서 Management Client 프로필에 대해 키를 입력함으로써 여러 사용자가 해당 키를 사용할 수 있도록 만들 수 있습니다. 프로파일에 할당된 모든 사용자가 이 키를 사용할 것입니다.

단계:

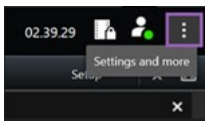
1. Management Client 의 **사이트 탐색** 창에서 **Smart Client 프로파일** 을 클릭합니다.
2. **Smart Client 프로파일** 창에서 관련된 Smart Client 프로필을 선택합니다.
3. **속성** 창에서 **스마트 맵** 탭을 클릭합니다.
    - Bing Maps의 경우, **Bing Maps 키** 필드에 기본 키 또는 기업 키를 입력합니다.
    - Google Maps의 경우, **Google Maps 개인 키** 필드에 정적 지도 API 키를 입력합니다.
4. XProtect Smart Client 운영자가 다른 키를 사용하지 않도록 방지하려면 **잠금** 확인란을 선택합니다.

Bing Maps 또는 Google Maps를 다음에서 활성화: XProtect Smart Client

XProtect Smart Client 운영자가 Smart Client 프로필에서 사용하던 것과 다른 키를 사용하도록 하려면 반드시 XProtect Smart Client 의 설정에서 키를 입력해야 합니다.

단계:

1. XProtect Smart Client 에서 **설정** 창을 여십시오.



2. **스마트 맵** 을 클릭합니다.
3. 사용하려는 맵 서비스에 따라 다음 중 하나를 수행합니다.
    - Bing Maps의 경우, **Bing Maps 키** 필드에 키를 입력합니다. 또한 페이지 81의 스마트 맵과 Bing Maps 통합(설명됨)를 참조하십시오.
    - Google Maps의 경우, **개인 키Google Maps** 필드에 키를 입력합니다. 또한 페이지 80의 스마트 맵과 Google Maps 통합(설명됨)를 참조하십시오.

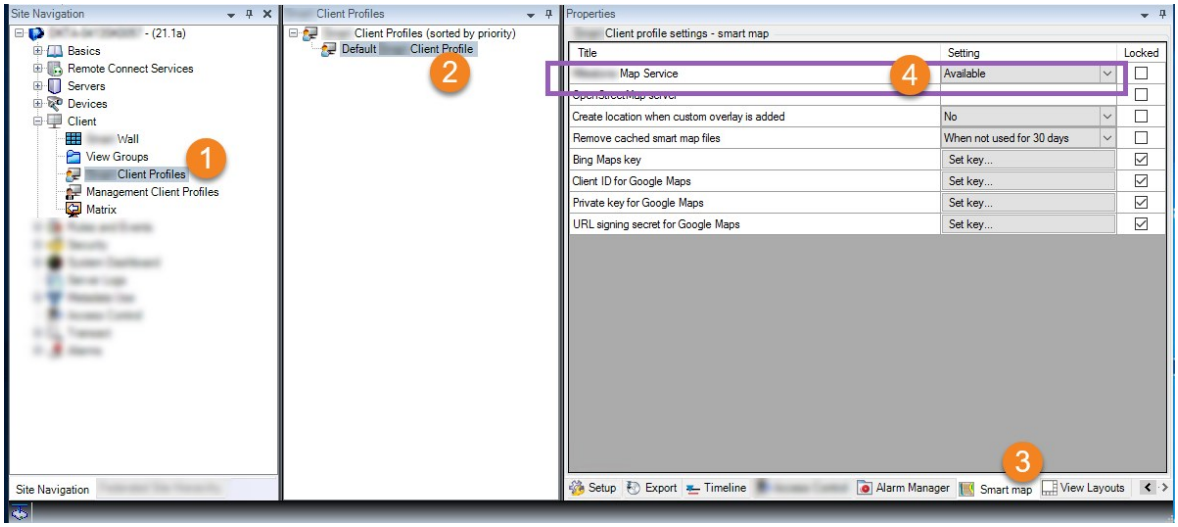
Milestone Map Service 활성화

Milestone Map Service 은(는) Milestone Systems 의 타일 서버에 연결할 수 있게 해주는 온라인 서비스입니다. 이 타일 서버는 상업적으로 이용 가능한 무료 맵 서비스를 사용합니다.

스마트 맵에서 Milestone Map Service 을(를) 활성화한 후에는 스마트 맵은 지리적 배경으로 Milestone Map Service 을(를) 사용하게 됩니다.

단계:

1. **사이트 탐색** 창에서, **클라이언트** 노드를 확장하고 **Smart Client 프로필** 을 클릭합니다.
2. 개요 창에서 관련 Smart Client 프로필을 선택합니다.
3. **속성** 창에서 **스마트 맵** 탭을 클릭합니다.



4. **Milestone Map Service** 필드에서 **이용 가능** 을 선택합니다.
5. 이러한 설정을 XProtect Smart Client 에서 강화하려면, **잠금** 확인란을 선택합니다. 그러면 XProtect Smart Client 운영자가 Milestone Map Service 을(를) 활성화 또는 비활성화할 수 없게 됩니다.
6. 변경 내용 저장.

또한 Milestone Map Service 의 **설정** 창에서 XProtect Smart Client 을(를) 활성화할 수 있습니다.

Milestone Map Service 은(는) 인터넷 액세스가 필요합니다.

제한적인 방화벽을 사용하고 있는 경우에는 사용된 도메인에 대한 액세스를 허용하는 것이 중요합니다. Milestone Map Service가 실행 중인 각 시스템에서 maps.milestonesys.com을 사용하는 Smart Client에 대해 나가는 트래픽을 허용하는 것이 필요할 수도 있습니다.

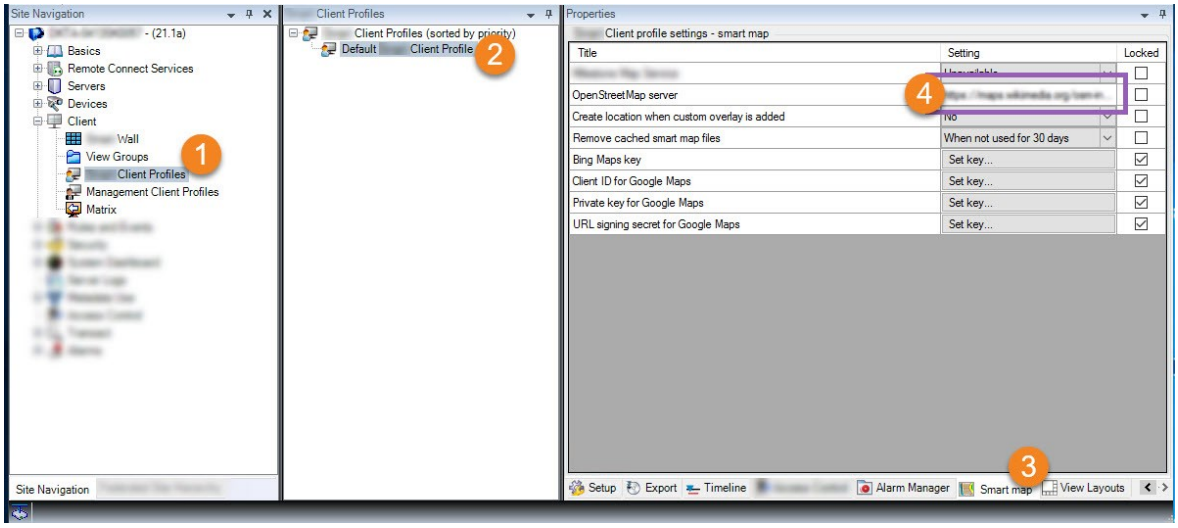
OpenStreetMap 타일 서버 지정

사용 중인 스마트 맵의 지리적 배경으로 **OpenStreetMap** 옵션을 사용 중이라면 타일 이미지가 검색되는 위치를 지정해야 합니다. 상용 타일 서버 또는 로컬 타일 서버 모두 타일 서버 주소를 지정함으로써 이렇게 할 수 있습니다(예: 공항 또는 항구과 같은 지역에 대해 조직에서 자체 맵을 보유한 경우).

또한 XProtect Smart Client 의 **설정** 창에서 타일 서버 주소를 지정할 수도 있습니다.

단계:

1. **사이트 탐색** 창에서, **클라이언트** 노드를 확장하고 **Smart Client 프로필** 을 클릭합니다.
2. 개요 창에서 관련 Smart Client 프로필을 선택합니다.
3. **속성** 창에서 **스마트 맵** 탭을 클릭합니다.



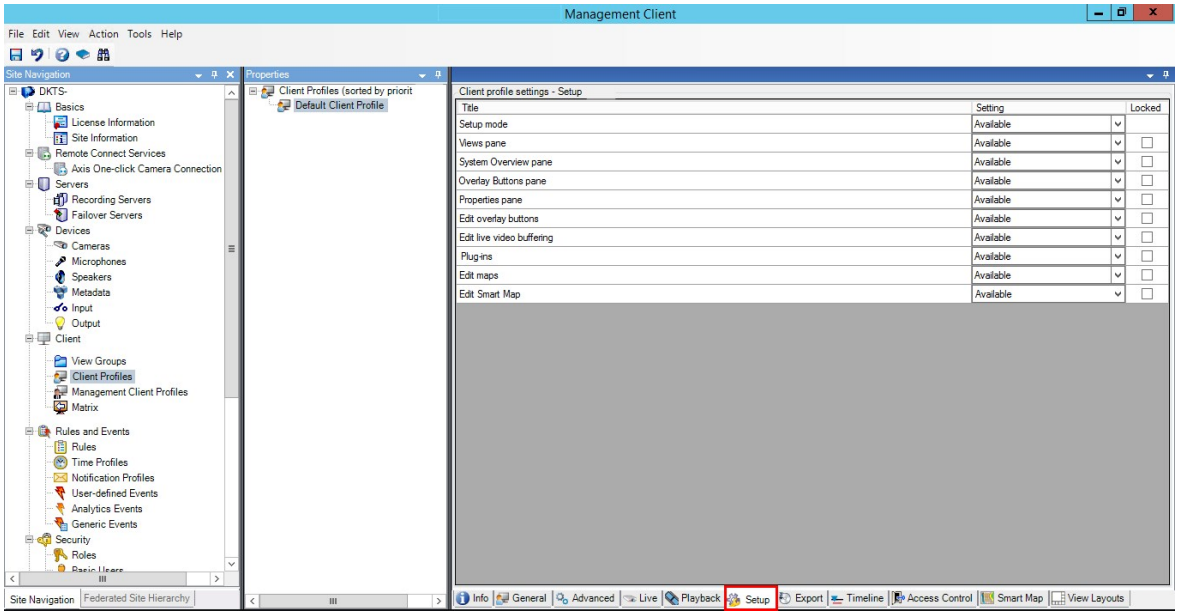
4. **OpenStreetMap 서버** 필드에서 타일 서버의 주소를 입력합니다.
5. 이러한 설정을 XProtect Smart Client 에서 강화하려면, **잠금** 확인란을 선택합니다. 그러면 XProtect Smart Client 운영자가 주소를 변경할 수 없게 됩니다.
6. 변경 내용 저장.

스마트 맵 편집 활성화

운영자는 XProtect Smart Client 에서 편집이 활성화된 경우에만 설정 모드에서 Management Client 의 스마트 맵을 편집할 수 있습니다. 이미 활성화되지 않은 경우, 각 관련된 Smart Client 프로파일에 대해 편집을 활성화해야 합니다.

단계:

1. **사이트 탐색** 창에서 **클라이언트** 노드를 확장합니다.
2. **Smart Client 프로파일** 을 클릭합니다.



3. 개요 창에서 관련 Smart Client 프로필을 선택합니다.
4. **속성** 창에서 **설정** 탭을 클릭합니다.
5. **스마트 맵 편집** 목록에서 **이용 가능** 을 선택합니다.
6. 각 관련된 Smart Client 프로파일에 이 단계를 반복합니다.
7. 변경 내용을 저장합니다. 선택한 Smart Client 프로파일에 할당된 사용자가 다음에 XProtect Smart Client 에 로그인할 때, 스마트 맵을 편집할 수 있습니다.

편집을 비활성화하려면, **스마트 맵 편집** 목록에서 **이용 불가** 를 선택합니다.

스마트 맵상의 장치 편집 활성화

운영자에게 다음을 허용하려면 역할마다 장치 편집을 활성화해야 합니다. 예를 들면 다음과 같습니다.

- 스마트 맵에 입력 장치 또는 마이크 배치
- 스마트 맵상의 카메라의 심도 조절

스마트 맵에 있는 다음과 같은 유형의 장치를 운영자가 편집하도록 할 수 있습니다.

- 카메라
- 입력 장치
- 마이크

요구사항
시작하기 전에, 스마트 맵 편집이 활성화 되었는지 확인하십시오(페이지 298의 스마트 맵 편집 활성화 참조). 운영자의 역할이 연결된 Smart Client 프로파일에서 할 수 있습니다.

단계:

1. **보안** 노드 > **역할** 을 확장합니다.
2. **역할** 창에서 운영자가 관련된 역할을 선택합니다.
3. 역할 편집 권한을 부여하려면 다음과 같이 하십시오.
    - **전체 보안** 탭에서 **역할 설정** 창을 선택하고 장치 유형을 선택합니다(예: **카메라** 또는 **입력**)
    - **허용** 열에서, **전체 제어** 또는 **편집** 확인란을 선택합니다
4. 변경 내용 저장.

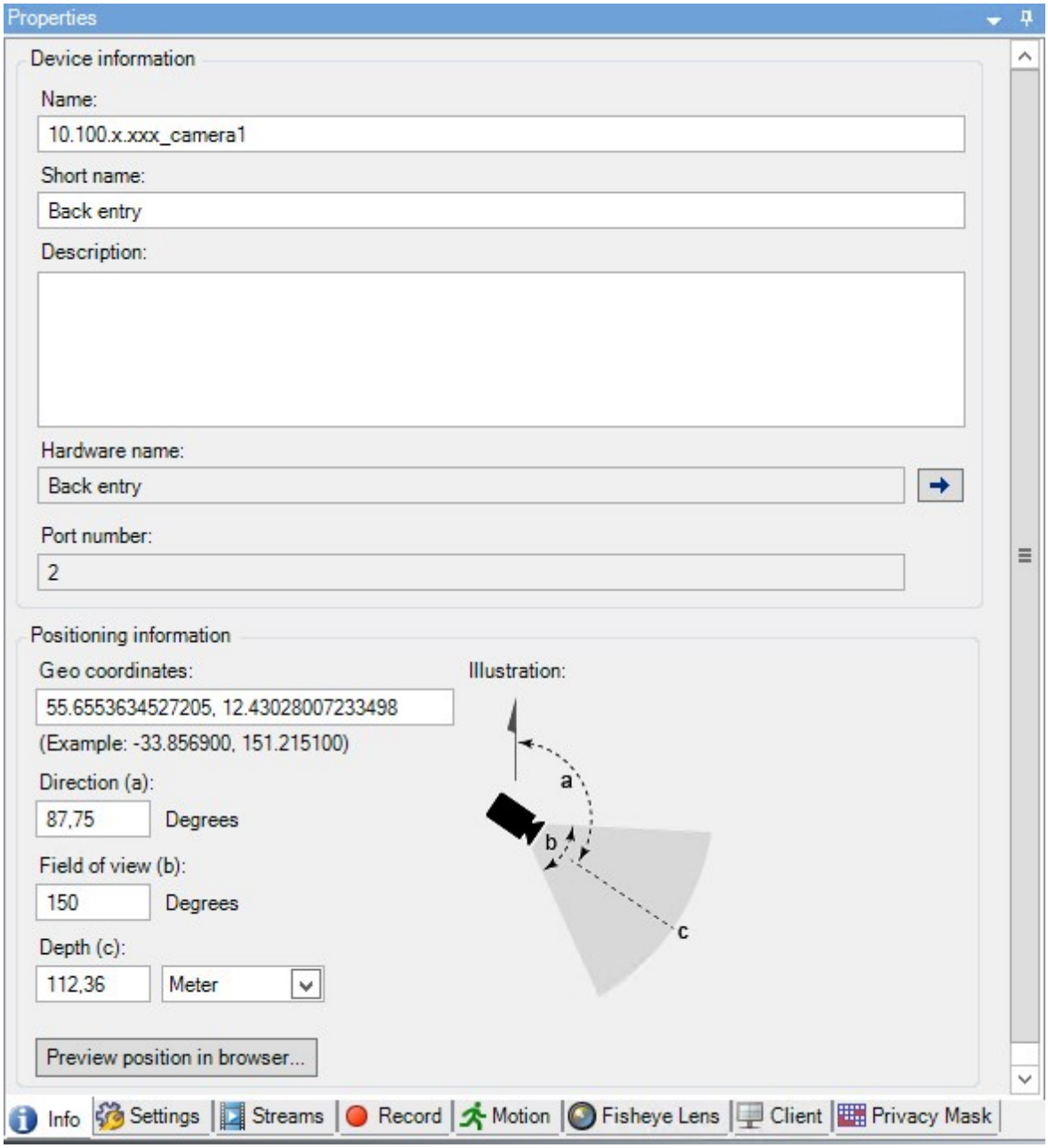
개별 장치 편집을 활성화하려면 **장치** 탭으로 이동해 관련 장치를 선택합니다.

장치 위치 및 카메라 방향, 시계, 깊이(스마트 맵) 정의

장치가 스마트 맵에 올바르게 배치되도록 하기 위해, 장치의 지리적 좌표를 설정할 수 있습니다. 카메라의 경우 방향과 시계, 심도도 설정할 수 있습니다. 이와 같은 것들 중 하나를 설정하면 다음에 운영자가 XProtect Smart Client 에 스마트 맵을 불러올 때 자동으로 장치를 스마트 맵에 추가하게 됩니다.

단계:

1. Management Client 에서 **장치** 노드를 확장하고 장치 유형을 선택합니다(예: **카메라** 또는 **입력**).
2. **장치** 창에서 관련 장치를 선택합니다.
3. **정보** 탭에서 **위치정보** 로 스크롤합니다.



4. **지리적 좌표** 필드에서 위도와 경도 좌표를 위도와 경도 순서대로 지정합니다. 마침표를 소수점으로 사용하고 쉼표를 위도와 경도 구분에 사용합니다.

- 카메라의 경우:
    1. **방향** 필드에서 0 ~ 360도의 범위로 값을 입력합니다.
    2. **시야** 필드에서 0 ~ 360도의 범위로 값을 입력합니다.
    3. **깊이** 필드에서 미터 또는 피트로 보기 깊이를 입력합니다.

5. 변경 내용 저장.

레코딩 서버의 속성도 설정할 수 있습니다.

스마트 맵을 Milestone Federated Architecture 와(과) 함께 구성

Milestone Federated Architecture 에서 스마트 맵을 사용할 때, 연결된 사이트의 모든 장치가 스마트 맵에 나타납니다. 다음 단계를 따라 연합 아키텍처에서 스마트 맵을 설정합니다.

Milestone Federated Architecture 에 대한 일반 정보는 페이지 86의 Milestone Federated Architecture 구성하기를 참조하십시오.

1. 최상위 사이트를 하위 사이트와 연결하기 전에, 지리적 좌표가 모든 사이트의 모든 장치에 지정되어 있는지 확인하십시오. 장치가 XProtect Smart Client 을(를) 통해 스마트 맵에 배치될 때 지리적 좌표가 자동으로 추가되지만, 장치 속성의 Management Client 에서 수동으로 추가할 수도 있습니다. 자세한 정보는 페이지 300의 장치 위치 및 카메라 방향, 시계, 깊이(스마트 맵) 정의를 참조하십시오.
2. 상위 사이트와 모든 연합 사이트에 Windows 사용자로서 Smart Client 운영자를 추가해야 합니다. 적어도 최상위 사이트에서, Windows 사용자가 스마트 맵 편집 권한을 가져야 합니다. 이렇게 하면 사용자가 최상위 사이트와 모든 하위 사이트에 대한 스마트 맵을 편집할 수 있습니다. 다음으로, 하위 사이트의 Windows 사용자가 스마트 맵 편집 권한이 필요한지 여부를 결정해야 합니다. Management Client 에서, 먼저 **역할** 아래에 Windows 사용자를 생성한 다음, 스마트 맵 편집을 활성화합니다. 자세한 정보는 페이지 298의 스마트 맵 편집 활성화를 참조하십시오.
3. 최상위 사이트에서 Windows 사용자로서 하위 사이트를 관리자 권한이 있는 역할에 추가합니다. 객체 유형을 지정할 때, **컴퓨터** 확인란을 선택합니다.
4. 각 하위 사이트에서, 최상위 사이트에 사용된 것과 동일한 관리자 역할에 Windows 사용자로 최상위 사이트를 추가해야 합니다. 객체 유형을 지정할 때, **컴퓨터** 확인란을 선택합니다.
5. 최상위 사이트에서 **연합 사이트 계층** 창을 볼 수 있는지 확인하십시오. Management Client 에서 **뷰** 로 이동한 다음 **연합 사이트 계층** 을 선택합니다. 각 하위 사이트를 최상위 사이트에 추가합니다. 자세한 정보는 페이지 286의 계층 구조에 사이트 추가를 참조하십시오.
6. 이제 Milestone Federated Architecture 에서 XProtect Smart Client 이(가) 작동하는지 테스트할 수 있습니다. 관리자 또는 운영자로 최상위 사이트에 로그인하고, 스마트 맵이 포함된 뷰를 엽니다. 설정이 올바르게 완료되었다면, 최상위 사이트와 모든 하위 사이트의 모든 장치가 스마트 맵에 나타납니다. 하위 사이트 중 하나에 로그인하면, 해당 사이트 및 그 하위 사이트의 장치만 표시됩니다.

스마트 맵에서 장치(예: 카메라 위치 및 각도)를 편집하려면 사용자는 장치 편집 권한이 필요합니다. 자세한 정보는 페이지 299의 스마트 맵상의 장치 편집 활성화를 참조하십시오.

유지관리

시스템 구성 백업 및 복원

Milestone 에서는 재해 복구 조치로서 시스템 구성을 정기적으로 백업하도록 권장합니다.

구성 정보가 손실되는 경우는 드물지만 우발적인 상황에서는 그럴 수 있습니다. 기술적 또는 조직적 수단을 사용해서라도 백업을 보호해야 합니다.

시스템 구성 백업 및 복원(설명됨)

이 시스템은 Management Client 에서 정의할 수 있는 모든 시스템 구성을 백업하는 내장 기능을 제공합니다. 감사 로그 파일을 포함하여 로그 서버 데이터베이스 및 로그 파일은 이 백업에 포함되지 않습니다.

시스템의 용량이 큰 경우, Milestone 은(는) 예약 백업을 정의할 것을 권장합니다. 이는 타사 도구인 Microsoft® SQL Server Management Studio. 이 백업에는 수동 백업과 동일한 데이터가 포함됩니다.

백업 중 시스템은 온라인 상태입니다.

구성을 백업하는 데 약간의 시간이 걸릴 수 있습니다. 백업 기간은 다음에 따라 다릅니다.

- 시스템 구성
- 하드웨어
- 단일 서버 또는 여러 대의 서버에 SQL Server, Event Server 및 Management Server 구성 요소를 설치했는지 여부

수동 및 예약 백업을 만들 때마다 SQL Server 데이터베이스의 트랜잭션 로그 파일이 플러시됩니다. 트랜잭션 로그파일을 플러시하는 방법에 관한 추가 정보는 페이지 124의 SQL Server 데이터베이스 트랜잭션 로그(설명됨)를 참조하십시오.

> ⚠ 백업 생성 시 시스템 구성 암호 설정을 알아두도록 하십시오.

> ⚠ FIPS비 규격 암호로 암호화된 2017 R1 이전의 XProtect VMS 버전의 내보내기와 저장된 미디어 데이터베이스가 있는 FIPS 140-2 규격 시스템의 경우, FIPS를 활성화한 후에도 액세스할 수 있는 위치에 데이터를 저장해야 합니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

공유 백업 폴더 선택

시스템 구성을 백업하고 복원하기 전에 이러한 용도로 백업 폴더를 설정해야 합니다.

1. 알림 영역의 Management Server 서비스 아이콘을 마우스 오른쪽 버튼으로 클릭하고, **공유 백업 폴더 선택** 을 선택합니다.
2. 나타나는 창에서 원하는 파일 위치로 이동합니다.

3. **확인** 을 두 번 클릭합니다.
4. 현재 백업 폴더의 파일을 삭제할지 묻는 메시지가 나타나면 필요에 따라 **예** 또는 **아니요**를 클릭합니다.

수동으로 시스템 구성 백업

1. 메뉴 표시줄에서, **파일** > **구성 백업** 을 선택합니다.
2. 대화 상자에 나온 참고 정보를 읽고, **백업** 을 클릭합니다.
3. .cnf 파일의 파일 이름을 입력합니다.
4. 폴더 대상을 입력하고 **저장** 을 클릭합니다.
5. 백업이 완료될 때까지 기다린 다음 **닫기** 를 클릭합니다.

해당하는 모든 시스템 구성 파일이 지정된 위치에 저장되는 하나의 .cnf 파일에 결합됩니다. 백업 중 먼저 모든 백업 파일이 관리 서버의 임시 시스템 백업 폴더로 내보내집니다. 알림 영역의 Management Server 서비스 아이콘을 마우스 오른쪽 버튼으로 클릭하고 공유 백업 폴더 선택을 선택하여 다른 임시 폴더를 선택할 수 있습니다.

수동 백업에서 시스템 구성 복원

중요 정보

- 설치하는 사용자와 복원하는 사용자 모두 관리 서버 **및** SQL Server에서 시스템 구성 SQL Server 데이터베이스의 로컬 관리자여야 합니다.
- 레코딩 서버를 제외하고, 복원 중 시스템이 완전히 종료되는데, 약간의 시간이 걸릴 수 있습니다
- 백업은 해당 백업이 생성된 시스템 설치에서만 복원할 수 있습니다. 백업이 만들어졌을 때와 설정이 가능한 한 유사한지 확인하십시오. 그렇지 않으면, 복원이 실패할 수 있습니다
- 복원 중 시스템 구성 암호를 입력하라는 메시지가 나오는 경우, 반드시 백업을 만들었을 시점에 유효했던 시스템 구성 암호를 제공해야 합니다. 이 암호가 없으면 백업에서 구성을 복원할 수 없습니다.
- SQL Server 데이터베이스를 백업하고 깨끗한 SQL Server에 이를 복원하는 경우, SQL Server 데이터베이스에서 발생하는 오류는 영향을 주지 않고 SQL Server의 일반 오류 메시지 하나만 수신하게 됩니다. 이를 방지하려면 우선 깨끗한 SQL Server을(를) 사용하여 XProtect 시스템을 다시 설치한 다음 그 위에 백업을 복원하십시오.
- 유효성 확인 단계에서 복구가 실패하는 경우, 변경 사항이 없으므로 이전 구성을 다시 시작할 수 있습니다
  프로세스의 다른 곳에서 복구가 실패하는 경우, 이전 구성으로 롤백할 수 없습니다
  백업 파일이 손상되지 않은 경우, 다른 복구를 수행할 수 있습니다
- 복원은 현재 구성을 대체합니다. 즉, 마지막 백업 이후 구성의 변경 내용을 모두 잃게 됩니다
- 감사 로그를 포함한 로그는 복원되지 않습니다
- 일단 복원이 시작되면 취소할 수 없습니다.

복원

1. 알림 영역의 Management Server 서비스 아이콘을 마우스 오른쪽 버튼으로 클릭하고, **구성 복원** 을 선택합니다.
2. **중요 참고 정보를 읽고** 복원을 클릭합니다.
3. 파일 열기 대화상자에서 시스템 구성 백업 파일의 위치를 찾아 선택한 후 **열기** 를 클릭합니다.

   백업 파일은 Management Client 컴퓨터에 있습니다. Management Client 이(가) 다른 서버에 설치된 경우, 대상을 선택하기 전에 백업 파일을 이 서버로 복사합니다.

4. **구성 복원** 창이 열립니다. **복원이 완료될 때까지 기다린 다음** 닫기를 클릭합니다.

시스템 구성 암호(설명됨)

시스템 구성 암호를 할당하여 시스템 구성 전반을 보호하도록 선택할 수 있습니다. 시스템 구성 암호를 할당한 후부터 백업은 암호로 보호됩니다. 이 암호 설정은 보호 폴더에서 관리 서버를 실행하는 컴퓨터에 저장됩니다. 이러한 상황에서 암호가 필요합니다.

- 현재 암호 설정과는 다른 암호 설정으로 만들어진 구성 백업으로부터 구성을 복원하는 경우
- 하드웨어 오류로 인해 다른 컴퓨터에 관리 서버를 이전하거나 설치하는 경우(복원)
- 클러스터링된 시스템에서 추가 관리 서버를 구성하는 경우

시스템 구성 암호는 설치 중 또는 설치 후에 할당될 수 있습니다. 이 암호는 Windows 복잡성 요건에 부합해야 하며, 이 요건은 Windows 암호 정책에 정의되어 있습니다.

시스템 관리자는 이 암호를 저장하고 안전하게 보관하십시오. 시스템 구성 암호를 할당하고 백업으로 복원 중인 경우, 시스템 구성 암호 제공을 요청받을 수도 있습니다. 이 암호가 없으면 백업에서 구성을 복원할 수 없습니다.

시스템 구성 암호 설정

시스템 구성 암호 설정은 변경될 수 있습니다. 시스템 구성 암호 설정에서 다음과 같은 옵션을 선택할 수 있습니다.

- 시스템 구성 암호를 할당하여 암호로 시스템 구성을 보호하도록 선택
- 시스템 구성 암호 변경
- 할당된 시스템 구성 암호를 제고하여 암호로시스템 구성을 보호하지 않도록 선택

시스템 구성 암호 설정 변경

암호를 만들 때 시스템 관리자가 다른 백업과 연관된 암호를 저장하고 안전하게 보관해야 합니다. 백업에서 복원하는 경우, 백업을 만들었을 시점에 유효했던 시스템 구성 암호를 제공하도록 요청받을 수도 있습니다. 이 암호가 없으면 백업에서 구성을 복원할 수 없습니다.

암호를 변경한 후, 그리고 별도의 컴퓨터에 관리 서버 및 이벤트 서버가 설치된 경우, 이벤트 서버에도 현재 시스템 구성 암호를 입력해야 합니다. 자세한 정보는 현재 시스템 구성 암호 입력 (이벤트 서버) 를 참조하십시오.

이 변경을 적용하려면 관리 서버 서비스를 다시 시작해야 합니다.

1. 관리 서버 트레이 아이콘을 찾고 관리 서버 서비스가 실행 중인지 확인합니다.
2. 알림 영역의 Management Server 서비스 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **시스템 구성 암호 설정 변경** 을 선택합니다.
3. 시스템 구성 암호 변경하기 창이 나타납니다.

암호를 할당합니다

1. **신규 암호** 필드에 신규 암호를 입력합니다.
2. **신규 암호 확인** 필드에서 신규 암호를 재입력하고 **Enter** 를 선택합니다.
3. 알림을 읽고 변경 사항을 수락하려면 **예** 를 클릭합니다.
4. 변경 확인을 기다린 후 **닫기** 를 선택합니다.
5. 이 변경을 적용하려면 관리 서버 서비스를 다시 시작해야 합니다.
6. 다시 시작한 후 관리 서버가 실행 중인지 확인합니다.

암호 보호 제거

암호 보호가 필요 없는 경우 옵트아웃을 선택할 수 있습니다.

1. 확인란 선택: **시스템 구성 암호를 사용하지 않기로 선택하며 시스템 구성이 암호화되지 않음을 이해했습니다** 를 선택 후 **Enter** 를 클릭합니다.
2. 알림을 읽고 변경 사항을 수락하려면 **예** 를 클릭합니다.

3. 변경 확인을 기다린 후 **닫기** 를 선택합니다.
4. 이 변경을 적용하려면 관리 서버 서비스를 다시 시작해야 합니다.
5. 다시 시작한 후 관리 서버가 실행 중인지 확인합니다.

시스템 구성 암호 설정 입력(복원)

하드웨어 오류 또는 다른 원인으로 암호 설정이 기록된 파일이 삭제된 경우, 시스템 구성이 기록된 데이터베이스에 액세스하려면 시스템 구성 암호 설정을 제공해야 합니다. 신규 컴퓨터에 설치를 하는 동안 시스템 구성 암호 설정을 요청받게 됩니다.

그러나 암호 설정이 기록된 파일이 삭제되거나 손상된 경우, 그리고 해당 컴퓨터가 여타 문제가 없는 관리 서버를 실행 중인 경우, 다음과 같이 시스템 구성 암호 설정을 입력할 수 있습니다.

1. 관리 서버 트레이 아이콘을 찾습니다.
2. 알림 영역의 Management Server 서비스 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **시스템 구성 암호 입력** 을 선택합니다.
3. 시스템 구성 암호 설정 입력하기 창이 나타납니다.

시스템 구성이 암호로 보호됩니다.

1. **암호** 필드에서 암호를 입력하고 **Enter** 를 선택합니다.
2. 암호가 수락될 때까지 기다립니다. **닫기** 를 선택합니다.
3. 관리 서버가 실행 중인지 확인합니다.

시스템 구성이 암호로 보호되지 않고 있습니다.

1. 확인란 선택: **이 시스템은 시스템 구성 암호를 사용하지 않습니다** 를 선택 후 **Enter** 를 선택합니다.
2. 설정이 수락될 때까지 기다립니다. **닫기** 를 선택합니다.
3. 관리 서버가 실행 중인지 확인합니다.

수동으로 시스템 구성 백업(설명됨)

시스템 구성을 포함한 관리 서버의 데이터베이스 수동 백업을 수행하려면 시스템이 계속 온라인 상태를 유지하도록 해야 합니다. 관리 서버의 데이터베이스 기본 이름은 **Surveillance**입니다.

백업을 시작하기 전에 다음과 같은 몇 가지 사항을 고려해야 합니다:

- SQL Server데이터베이스 백업을 사용하여 시스템 구성을 다른 시스템에 복사할 수 없습니다.
- SQL Server데이터베이스를 백업하는 데는 시간이 소요됩니다. 백업은 시스템 구성, 하드웨어를 비롯하여 SQL Server, 관리 서버 및 Management Client 이(가) 동일 컴퓨터에 설치되었는지 여부에 따라 달라집니다

- 감사 로그를 비롯한 로그는 로그 서버의 데이터베이스에 저장되므로 관리 서버의 데이터베이스에 있는 백업에 포함되지 **않습니다**. 로그 서버의 데이터베이스 기본 이름은 **SurveillanceLogServerV2**입니다. 두 SQL Server 데이터베이스를 동일한 방법으로 백업합니다.

이벤트 서버 구성 백업 및 복원(설명됨)

시스템 구성을 백업하고 복원할 때 이벤트 서버 구성의 내용이 포함됩니다.

처음으로 이벤트 서버를 실행하면 모든 구성 파일이 자동으로 SQL Server 데이터베이스로 이동됩니다. 이벤트 서버를 다시 시작할 필요없이 복원된 구성을 이벤트 서버에 적용할 수 있으며, 구성 복원이 로드되는 동안 이벤트 서버가 모든 외부 통신을 시작하고 중지할 수 있습니다.

시스템 구성의 백업 및 복원 예약(설명됨)

관리 서버는 시스템의 구성을 SQL Server 데이터베이스에 저장합니다. Milestone에서는 재해 복구 조치로서 이 데이터베이스를 정기적으로 백업할 것을 권장합니다. 시스템 구성이 손실되는 경우는 드물지만 우발적인 상황에서는 그럴 수 있습니다. 다행히도 이는 1분 밖에 걸리지 않으며, 백업에는 SQL Server 데이터베이스의 트랜잭션 로그를 플러시한다는 추가적인 장점이 있습니다.

설치 규모가 작고 예약 백업이 필요하지 않은 경우에는 시스템 구성을 수동으로 백업할 수 있습니다. 관련 지침은 페이지 308의 수동으로 시스템 구성 백업(설명됨)를 참조하십시오.

관리 서버를 백업/복원할 때 시스템 구성이 포함된 SQL Server 데이터베이스가 백업/복원에 포함되었는지 확인하십시오.

예약 백업 및 복원 사용을 위한 요구 사항

Microsoft® SQL Server Management Studio, 웹사이트(https://www.microsoft.com/downloads/)에서 무료로 도구를 다운로드할 수 있습니다.

이 도구에는 SQL Server 및 해당 데이터베이스 관리 이외에도 사용하기 쉬운 백업 및 복원 기능이 포함되어 있습니다. 도구를 다운로드하여 관리 서버에 설치합니다.

예약 백업을 사용하여 시스템 구성 백업

1. Windows 시작 메뉴에서 Microsoft® SQL Server Management Studio 을(를) 시작합니다.
2. 연결 시 필요한 SQL Server 의 이름을 지정합니다. SQL Server 데이터베이스를 생성한 계정을 사용합니다.
    1. 사용 중인 전체 시스템 구성을 비롯하여 이벤트 서버, 레코딩 서버, 카메라, 입력, 출력, 사용자, 규칙, 순찰 프로필을 포함하는 SQL Server 데이터베이스를 찾습니다. 이 SQL 데이터베이스의 기본 이름은 **Surveillance** 입니다.
    2. SQL Server 데이터베이스의 백업을 만들고 다음을 확인합니다:

- 선택한 SQL Server 데이터베이스가 정확한지 확인합니다.
- 백업 유형이 **전체** 인지 확인합니다.
- 되풀이 백업의 일정을 설정합니다. Microsoft 웹사이트(https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)에서 스케줄에 따른 자동화 백업에 관한 자세한 내용을 확인할 수 있습니다.
- 제안된 경로가 괜찮은지 확인하고, 그렇지 않으면 다른 경로를 선택합니다.
- **완료 시 백업 확인** 과 **미디어에 쓰기 전에 체크섬 수행** 을 선택합니다.

3. 도구에 표시되는 지침을 끝까지 따릅니다.

또한 동일한 방법을 사용하여 로그가 포함된 로그 서버의 데이터베이스를 백업하는 것이 좋습니다. 로그 서버의 SQL Server 데이터베이스 기본 이름은 **SurveillanceLogServerV2**입니다.

예약 백업에서 시스템 구성 복원

요구사항
시스템 구성 데이터베이스를 복구하는 동안 시스템 구성이 변경되지 않도록 하려면 다음을 중지하십시오.

- Management Server 서비스(페이지 322의 서버 서비스 관리참조)
- Event Server 서비스(는 Windows **서비스** 에서 수행 가능(시스템에서 **services.msc** 를 검색하십시오. **서비스** 내에서, **Milestone XProtect Event Server** 를 찾기))
- World Wide Web Publishing 서비스, 인터넷 정보 서비스(IIS)라고도 합니다. IIS 중지 방법에 대해 알아보십시오(https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Windows **시작** 메뉴에서 Microsoft® SQL Server Management Studio 을(를) 엽니다.

도구에서 다음을 수행합니다:

1. 연결 시 SQL Server의 이름을 지정합니다. SQL Server 데이터베이스가 생성된 사용자 계정을 사용합니다.
2. 사용 중인 전체 구성을 비롯하여 이벤트 서버, 레코딩 서버, 카메라, 입력, 출력, 사용자, 규칙, 순찰 프로필 등을 포함한 SQL Server 데이터베이스를 찾습니다(기본 이름은 **Surveillance**).
3. SQL Server 데이터베이스를 복원하고 다음을 확인합니다.
   - 장치 **에서** 백업하려면 선택
   - **백업 미디어 유형** 파일 선택
   - 백업 파일(**.bak**)을 찾고 선택
   - **기존 데이터베이스 덮어쓰기** 선택
4. 도구에 표시되는 지침을 끝까지 따릅니다.

동일한 방법을 사용하여 로그가 포함된 로그 서버의 SQL Server 데이터베이스를 복구합니다. 로그 서버의 SQL Server 데이터베이스 기본 이름은 **SurveillanceLogServerV2**입니다.

시스템은 Management Server 서비스가 중단되어 있는 동안 작동되지 않습니다. 데이터베이스 복원을 마쳤으면 서비스를 다시 시작해야 합니다.

로그 서버의 데이터베이스 백업

앞에서 설명한 것과 같이 시스템 구성을 처리할 때 사용하는 방법을 통해 로그 서버의 데이터베이스를 처리합니다. 로그 서버의 데이터베이스에는 레코딩 서버와 카메라에서 보고된 오류를 비롯한 모든 시스템 로그가 포함되어 있습니다. 로그 서버의 데이터베이스 기본 이름은 **SurveillanceLogServerV2**입니다.

SQL Server데이터베이스는 로그 서버의 SQL Server 에 있습니다. 일반적으로 로그 서버와 관리 서버에는 동일한 SQL Server SQL Server 데이터베이스가 있습니다. 로그 서버 데이터베이스에는 시스템 구성이 포함되지 않으므로 백업이 필수는 아니지만, 관리 서버 백업/복원 이전의 시스템 로그에 액세스할 수 있으면 유용할 수 있습니다.

실패 및 문제 시나리오 백업 및 복원(설명됨)

- 마지막 시스템 구성 백업 후 이벤트 서버 또는 기타 등록된 서비스(예: 로그 서버)를 이동한 경우, 새로운 시스템에서 사용할 등록된 서비스 구성을 선택해야 합니다. 시스템이 이전 버전으로 복원된 후 새 구성을 유지할지를 결정할 수 있습니다. 서비스의 호스트 이름을 확인하여 결정합니다.
- 이벤트 서버가 지정된 대상에 위치하지 않아 시스템 구성 복원이 실패하는 경우(예: 이전의 등록된 서비스 설치를 선택한 경우), 다른 복원을 수행하십시오.
- 구성 백업에서 복원을 하지만 정확하지 않은 시스템 구성 암호를 입력하는 경우, 반드시 백업을 만들었을 시점에 유효했던 시스템 구성 암호를 제공해야 합니다.

관리 서버 이동

관리 서버는 시스템 구성을 SQL Server 데이터베이스에 저장합니다. 관리 서버를 한 물리적 서버에서 다른 서버로 이동하는 경우, 새로운 관리 서버 역시 이 SQL Server 데이터베이스에 대한 액세스 권한을 가지고 있는지 반드시 확인해야 합니다. 시스템 구성 데이터베이스는 두 가지 방식으로 저장될 수 있습니다:

- **네트워크 SQL Server**: 사용 중인 네트워크에서 SQL Server의 SQL Server 데이터베이스에 시스템 구성을 저장하는 경우, 새로운 관리 서버에 관리 서버 소프트웨어를 설치할 때 데이터베이스 위치를 해당 SQL Server에 지정할 수 있습니다. 이 경우, 관리 서버 호스트 이름 및 IP 주소에 대한 다음 구문만 적용되며 이 항목의 나머지 내용은 무시해야 합니다.

  관리 서버 호스트 이름 또는 IP 주소: 한 물리적 서버에서 다른 물리적 서버로 관리 서버를 이동할 경우, 새로운 서버에 이전 서버와 동일한 호스트 이름과 IP 주소를 지정하는 것이 가장 쉬운 방법입니다. 레코딩 서버가 이전 관리 서버의 호스트 이름 및 IP 주소에 자동으로 연결되기 때문입니다. 새로운 호스트 이름 및/또는 IP 주소를 새로운 관리 서버에 부여하는 경우, 레코딩 서버는 관리 서버를 찾을 수 없게 되며 반드시 수동으로 시스템의 각 Recording Server 서비스를 중단한 후 관리 서버 URL을 변경하고, 레코딩 서버를 다시 등록한 후 Recording Server 서비스를 시작합니다.

- **로컬 SQL Server**: 관리 서버 자체의 SQL Server에 있는 SQL Server 데이터베이스에 시스템 구성을 저장하는 경우, 이동하기 전에 기존 관리 서버의 시스템 구성 데이터베이스를 백업하는 것이 중요합니다. SQL Server 데이터베이스를 백업하고 이후 새 관리 서버 상의 SQL Server 에 복원함으로써, 이동 후 카메라, 규칙, 시간 프로필 등을 재구성할 필요가 없습니다

> 관리 서버를 이전하는 경우, 백업 복구를 위해 현재 시스템 구성 암호가 필요합니다. 페이지 306의 시스템 구성 암호(설명됨)를 참조하십시오.

요구사항

- **새 관리 서버에 설치하기 위한 소프트웨어 설치 파일**
- **소프트웨어 라이선스 파일(.lic)**, 시스템을 구입할 때 받고 처음에 설치합니다. 수동 오프라인 라이선스 활성화 이후에 받은 활성화된 소프트웨어 라이선스 파일은 사용하지 않아야 합니다. 활성화된 소프트웨어 라이선스 파일에는 시스템이 설치된 특정 서버에 관한 정보가 들어 있습니다. 따라서, 새 서버로 이전할 때 활성화된 소프트웨어 라이선스 파일을 재사용할 수 없습니다

이동과 함께 시스템 소프트웨어를 업그레이드하는 경우, 새 소프트웨어 라이선스 파일을 받아야 합니다. 이 파일을 사용하면 됩니다.

- **Microsoft® SQL Server Management Studio**
- 관리 서버를 사용할 수 없을 경우 어떻게 됩니까? 페이지 312의 이용 불가능한 관리 서버(설명됨))
- 로그 서버 데이터베이스를 복사합니다(페이지 311의 로그 서버의 데이터베이스 백업 참조)

이용 불가능한 관리 서버(설명됨)

- **레코딩 서버가 계속해서 레코딩할 수 있습니다.** 현재 운영 중인 레코딩 서버가 관리 서버로부터 구성 사본을 수신했으므로 관리 서버가 종료된 동안에 레코딩을 작업하고 저장할 수 있습니다. 따라서 예약 및 모션 트리거된 레코딩이 작동하며, 관리 서버 또는 다른 레코딩 서버에 관련된 이벤트에 기반하지 않는 한 관리 서버를 통해 진행되므로 기타 이벤트 트리거된 레코딩이 작동합니다
- **레코딩 서버는 일시적으로 로그 데이터를 로컬에 저장합니다**. 관리 서버를 다시 이용할 수 있을 때 로그 데이터를 관리 서버로 자동으로 전송합니다.
  - **클라이언트는 로그인 할 수 없습니다**. 클라이언트 액세스는 관리 서버를 통해 허용됩니다. 관리 서버 없이는, 클라이언트가 로그인할 수 없습니다
  - **이미 로그인한 클라이언트는 최대 4시간 동안 로그인 상태를 유지할 수 있습니다**: 클라이언트가 로그인 시 관리 서버에 의해 승인을 받으며 최대 4시간까지 레코딩 서버와 통신할 수 있습니다. 새 관리 서버사 4시간 이내로 작동하게 할 수 있는 경우, 사용자 다수는 영향을 받지 않게 됩니다.
  - **시스템 구성이 불가능**: 관리 서버 없이, 시스템 구성을 변경할 수 없습니다

Milestone 은(는) 관리 서버가 중단된 동안 감시 시스템과 연결이 끊기는 위험에 대 사용자에게 알릴 것을 권장합니다.

시스템 구성 이동

시스템 구성 이동은 3단계 프로세스로 이루어집니다:

1. 시스템 구성 백업을 만듭니다. 이는 예약된 백업 만들기와 동일합니다. 또한 페이지 309의 예약 백업을 사용하여 시스템 구성 백업를 참조하십시오.
2. 새 서버에 새로운 관리 서버를 설치합니다. 예약 백업 2단계를 참조하십시오.
3. 시스템 구성을 새 시스템으로 복원합니다. 또한 페이지 310의 예약 백업에서 시스템 구성 복원를 참조하십시오.

레코딩 서버 교체

레코딩 서버가 고장났거나 이전 레코딩 서버의 설정을 상속한 새로운 서버로 교체하려는 경우:

1. 이전 레코딩 서버에서 레코딩 서버 ID를 검색합니다:
    1. **Recording Servers** 를 선택하고 **개요** 창에서 이전 레코딩 서버를 선택합니다.
    2. **저장소** 탭을 선택합니다.
    3. 키보드에서 CTRL 키를 누른 상태에서 **정보** 탭을 선택합니다.
    4. **정보** 탭의 하단 부분에 있는 레코딩 서버 ID 번호를 복사합니다. *ID* 용어를 제외한 번호만을 복사하십시오.

2. 새 레코딩 서버에서 레코딩 서버 ID를 바꿉니다:
    1. 이전 레코딩 서버에서 Recording Server 서비스를 중지한 후, Windows의 **서비스** 에서 서비스의 **시작 유형** 을 **사용 안 함** 으로 설정합니다.

> ⚠ ID가 동일한 두 개의 레코딩 서버를 동시에 시작해서는 절대 안 됩니다.

    2. 새 레코딩 서버에서 탐색기를 열고 `C:\ProgramData\Milestone\XProtect Recording Server`로 이동하거나 레코딩 서버가 위치한 경로를 탐색합니다.
    3. `RecorderConfig.xml`파일을 엽니다.
    4. 태그 *<id>* 및 *</id>* 사이에 있는 기술된 ID를 삭제합니다.

    5. 복사한 레코딩 서버 ID를 태그 *<id>* 및 *</id>* 사이에 붙여 넣습니다. *RecorderConfig.xml*파일을 저장합니다.
    6. 레지스트리로 이동합니다: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
    7. **RecorderIDOnMachine** 을 열고 이전 레코딩 서버 ID를 새 ID로 변경합니다.

3. 관리 서버 상의 새로운 레코딩 서버를 등록합니다. 이를 수행하기 위해 Recording Server Manager 트레이 아이콘을 우클릭하고 **등록** 을 클릭하십시오. 자세한 정보는 페이지 179의 레코딩 서버 등록를 참조하십시오.
4. Recording Server 서비스를 재시작합니다. 새 Recording Server 서비스가 시동되면, 이전 레코딩 서버에서 모든 설정이 상속됩니다.

하드웨어 이동

동일 사이트에 속하는 레코딩 서버 사이에서 하드웨어를 이동할 수 있습니다. 이동 후, 새 레코딩 서버에서 실행되는 하드웨어와 그 장치 및 새 녹화물이 이 서버에 저장됩니다. 이동은 클라이언트 사용자가 모르는 사이에 이루어집니다.

이전 레코딩 서버에 있는 녹화물은 다음 조건이 충족될 때까지 그대로 유지됩니다.

- 보존 기간이 만료되어 시스템이 녹화물을 삭제합니다. 증거물 잠금으로 누군가가 보호 처리한 레코딩(페이지 69의 증거물 잠금(설명됨) 참조)은 해당 증거물 잠금 보존 기간이 만료될 때까지 삭제되지 않습니다. 증거물 잠금을 생성할 때 이에 대한 보존 기간을 정의합니다. 보존 기간은 만료되지 않을 수도 있습니다
- **레코드** 탭에서 각 장치의 새 레코딩 서버로부터 삭제할 수 있습니다

아직 녹화물이 있는 레코딩 서버를 제거하려고 하면 경고가 표시됩니다.

> 현재 하드웨어가 추가되어 있지 않은 레코딩 서버로 하드웨어를 이동하는 경우, 클라이언트 사용자가 로그아웃하고 다시 로그인해야 장치에서 데이터를 수신할 수 있습니다.

다음과 같은 목적으로 하드웨어 이동 기능을 사용할 수 있습니다.

- **로드 밸런스** : 예를 들어, 레코딩 서버의 디스크에 데이터가 너무 많으면, 새 레코딩 서버를 추가하고 하드웨어 일부를 이동할 수 있습니다
- **업그레이드** : 예를 들어, 레코딩 서버를 호스팅하는 서버를 새 모델로 교체해야 하는 경우, 새 레코딩 서버를 설치하고 이전 서버에서 새 서버로 하드웨어를 이동할 수 있습니다
- **결함이 있는 레코딩 서버 교체**: 예를 들어, 서버가 오프라인 상태에서 다시 온라인으로 전환되지 않는 경우, 하드웨어를 다른 레코딩 서버로 이동하여 시스템 작동을 유지할 수 있습니다. 이전 레코딩에는 액세스할 수 없습니다. 자세한 정보는 페이지 313의 레코딩 서버 교체를 참조하십시오.

원격 녹화

하드웨어를 다른 레코딩 서버로 이동하면 시스템이 상호 연결된 사이트나 카메라의 에지 저장소에서 진행되고 있거나 예정된 검색을 취소합니다. 녹화물이 삭제되지는 않지만 예상과 같이 데이터가 검색되어 데이터베이스에 저장되지 않습니다. 이 경우 경고 메시지가 표시됩니다. 하드웨어 이동을 시작할 때 검색을 시작한 XProtect Smart Client 사용자의 경우, 검색에 실패합니다. XProtect Smart Client 사용자에게 통보되며 나중에 다시 시도할 수 있습니다.

누군가 원격 사이트에서 하드웨어를 이동한 경우, 하드웨어 업데이트 옵션을 이용하여 원격 사이트의 새 구성을 반영하도록 중앙 사이트를 수동으로 동기화해야 합니다. 동기화하지 않으면 중앙 사이트에서 이동한 카메라가 분리된 상태로 유지됩니다.

하드웨어 이동(마법사)

레코딩 서버 사이에서 하드웨어를 이동하려면 하드웨어 이동 마법사를 실행합니다. 마법사가 하나 이상의 하드웨어 장치에 필요한 이동 수행 과정을 단계별로 안내합니다.

요구사항
마법사 시작 전:

- 새 레코딩 서버가 네트워크를 통해 물리적 카메라에 액세스할 수 있어야 합니다
- 하드웨어를 옮기고자 하는 레코딩 서버를 설치합니다(페이지 149의 Download Manager 을(를) 통해 설치(설명됨) 또는 페이지 156의 레코딩 서버 자동 설치참조)
- 새 레코딩 서버에 기존 서버에서 구동 중인 것과 동일한 장치 팩 버전을 설치합니다(페이지 133의 장치 드라이버(설명됨) 참조)

마법사를 실행하려면:

1. **사이트 탐색** 창에서, **레코딩 서버** 를 선택합니다.
2. **개요** 창에서 하드웨어를 이동하려는 원래 레코딩 서버를 마우스 오른쪽 버튼으로 클릭하거나 특정 하드웨어 장치를 마우스 오른쪽 버튼으로 클릭합니다.
3. **하드웨어 이동** 을 선택합니다.

   하드웨어를 이동하려는 원래 레코딩 서버가 연결되어 있지 않으면 오류 메시지가 나타납니다. 연결 해제된 레코딩 서버에서 하드웨어를 이동하기로 선택하는 경우에는 이 레코딩 서버가 다시 온라인 상태로 전환되지 않는다는 확실한 가정이 필요합니다. 하드웨어를 이동하고 서버가 다시 온라인 상태로 복귀되면 일정 기간 두 레코딩 서버에서 동일한 하드웨어가 실행됨으로써 시스템에 예상치 못한 동작이 발생할 위험이 있습니다. 예를 들어, 라이선스 오류 또는 올바른 레코딩 서버로 이벤트가 보내지지 않는 문제가 발생할 수 있습니다.

4. **레코딩 서버 수준에서 마법사를 시작한 경우**, 이동하려는 하드웨어 선택 페이지가 나타납니다. 이동하려는 하드웨어 장치를 선택합니다.
5. **하드웨어를 이동하려는 레코딩 서버 선택** 페이지에서 이 사이트에 설치된 레코딩 서버 목록 중 필요한 항목을 선택합니다.
6. **이후 녹화에 사용할 저장소 선택** 페이지에서 저장소 사용량 막대는 아카이브가 아니라 실시간 녹화를 위해 녹화 데이터베이스에 남은 여유 공간을 나타냅니다. 총 보존 기간은 녹화 데이터베이스와 아카이브 모두에 대한 보존 기간입니다.
7. 시스템이 요청을 처리합니다.

8. **이동이 성공적으로 수행되었으면** 닫기를 클릭합니다. Management Client 에서 새 레코딩 서버를 선택한 경우, 이동된 하드웨어를 볼 수 있고 이제 레코딩이 이 서버에 저장됩니다.

   이동에 실패한 경우, 아래에서 문제를 해결할 수 있습니다.

   > 상호 연결된 시스템에서는 자신이나 다른 시스템 관리자가 원격 사이트에서 수행한 변경 내용이 반영되도록 원격 사이트에서 하드웨어 이동 후 중앙 사이트를 수동으로 동기화해야 합니다.

하드웨어 이동 문제 해결

이동에 성공하지 못한 경우, 다음 중 한 가지가 원인일 수 있습니다:

오류 유형	문제 해결
레코딩 서버가 연결되지 않았거나 장애 조치 모드에 있습니다.	레코딩 서버가 온라인 상태인지 확인하십시오. 이를 등록해야 할 수도 있습니다. 서버가 장애 조치 모드이면 기다렸다가 다시 시도하십시오.
레코딩 서버가 최신 버전이 아닙니다.	관리 서버와 같은 버전을 실행하도록 레코딩 서버를 업데이트하십시오.
구성에서 레코딩 서버를 찾지 못했습니다.	레코딩 서버가 제거되지 않았는지 확인하십시오.
구성 업데이트 또는 구성 데이터베이스와 통신에 실패했습니다.	SQL Server 와 데이터베이스가 연결되고 실행 중인지 확인하십시오.
현재 레코딩 서버에서 하드웨어 정지 실패	다른 프로세스가 레코딩 서버를 잠갔거나 레코딩 서버가 오류 모드일 수 있습니다. 레코딩 서버가 실행 중인지 확인하고 다시 시도하십시오.
하드웨어가 없습니다.	이동하려는 하드웨어를 다른 사용자가 시스템에서 동시에 제거하려고 하지 않았는지 확인하십시오. 이러한 상황은 가능성이 매우 낮습니다.
하드웨어를 이동한 원래 레코딩 서버가 온라인 상태로 복귀했지만 오프라인일 때 이를 무시하기로 선택했습니다.	아마도 **하드웨어 이동** 마법사를 시작할 때 이전 레코딩 서버가 다시 온라인 상태로 전환되지 않는다고 확인했지만 이동 중에 서버가 다시 온라인 상태로 전환되었습니다. 마법사를 다시 시작하고 서버가 다시 온라인 상태로 전환되는지 확

오류 유형	문제 해결
	인하는 단계에서 **아니오** 를 선택하십시오.
소스 레코딩 저장 장치를 이용할 수 없습니다.	현재 오프라인 상태인 레코딩 저장소로 구성된 장치가 포함된 하드웨어를 이동하려고 합니다. 레코딩 저장소는 디스크가 오프라인이거나 사용 불가능할 때 오프라인 상태가 됩니다. 레코딩 저장소가 온라인인지 확인하고 다시 시도하십시오.
대상 레코딩 서버의 모든 레코딩 저장 장치를 이용할 수 있어야 합니다.	하드웨어를 하나 이상의 레코딩 저장소가 현재 오프라인 상태인 레코딩 서버로 이동하려고 합니다. 대상 레코딩 서버의 레코딩 저장소가 모두 온라인 상태인지 확인하십시오. 레코딩 저장소는 디스크가 오프라인이거나 사용 불가능할 때 오프라인 상태가 됩니다.

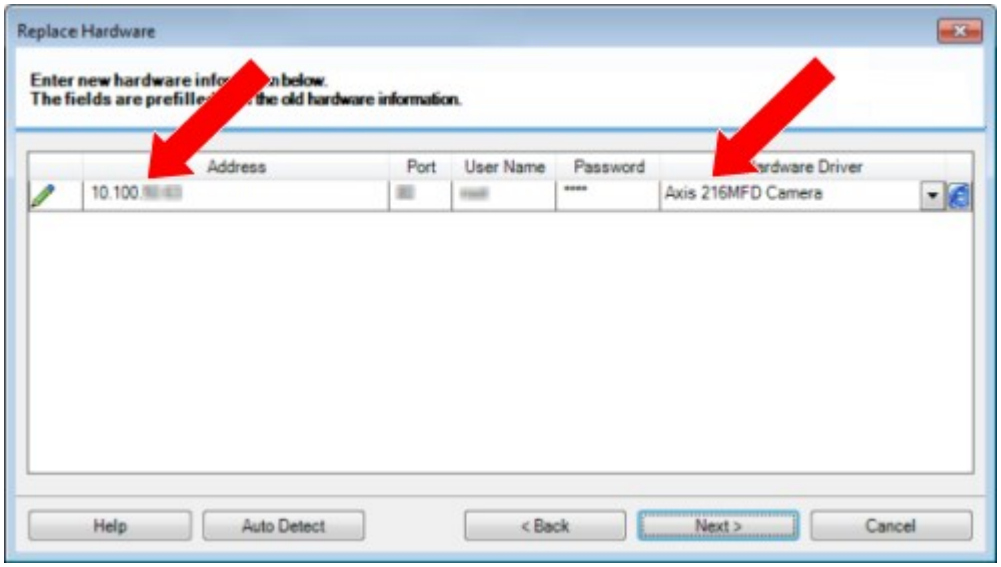
하드웨어 교체

하드웨어 장치 또는 네트워크를 다른 하드웨어 장치로 교체할 경우, 새 하드웨어 장치의 IP 주소, 포트, 사용자 이름 및 암호를 알고 있어야 합니다.

자동 라이선스 활성화를 켜지 않은 경우(페이지 107의 자동 라이선스 활성화(설명됨) 참조) 그리고 활성화 없이 모든 장치 변경이 사용된 경우(참조페이지 108의 활성화 없이 장치 변경(설명됨)), 하드웨어 장치를 교체한 **후에** 수동으로 라이선스를 활성화해야 합니다. 새로운 하드웨어 장치의 수가 장치 라이선스의 총 수를 초과하는 경우, 새 장치 라이선스를 구입해야 합니다.

1. 필요한 레코딩 서버를 확장하고 교체하려는 하드웨어를 마우스 오른쪽 단추로 클릭합니다.
2. **하드웨어 교체** 를 선택합니다.
3. **하드웨어 교체** 마법사가 나타납니다. **다음** 을 클릭합니다.

4. 마법사의 **주소** 필드(이미지에서 빨간색 화살표로 표시)에 새 하드웨어의 IP 주소를 입력합니다. 알고 있는 경우, **하드웨어 드라이버** 드롭다운 목록에서 관련 드라이버를 선택하십시오. 그렇지 않으면 **자동 검색** 을 선택합니다. 새 하드웨어의 포트, 사용자 이름 또는 암호 데이터가 다를 경우, **자동 검색 프로세스를 시작하기 전(필요한 경우)** 에 해당 정보를 수정합니다.



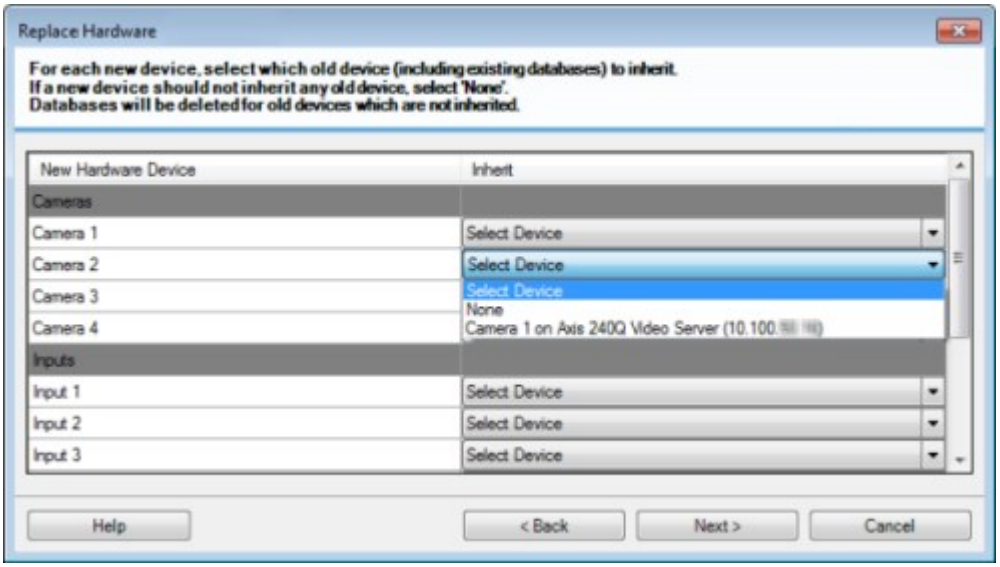
이 마법사에는 기존 하드웨어의 데이터가 미리 채워져 있습니다. 유사한 하드웨어 장치로 교체할 경우, 이 데이터의 일부(예: 포트, 드라이버 정보)를 재사용할 수 있습니다.

5. 다음 중 하나를 수행하십시오.
   - 목록에서 직접 필요한 하드웨어 장치 드라이버를 선택한 경우, **다음** 을 클릭합니다.
   - 목록에서 **자동 감지** 를 선택한 경우, **자동 감지** 를 클릭하고 프로세스가 성공할 때까지 기다린 후(맨 왼쪽에 ✔ 으로 표시), **다음** 을 클릭합니다

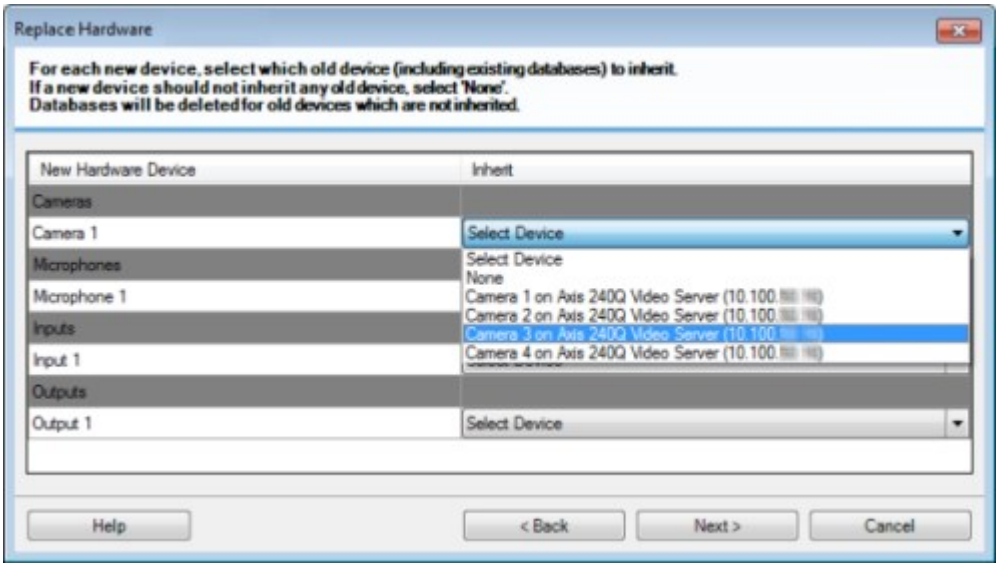
     이 단계는 이전 하드웨어 장치와 새 하드웨어 장치 각각에 연결된 개별 카메라, 마이크, 입력, 출력 등의 수에 따라 장치와 데이터베이스 매핑을 돕기 위한 것입니다.

     이전 하드웨어 장치의 데이터베이스를 새 하드웨어 장치의 데이터베이스로 **어떻게** 매핑할지 반드시 고려해야 합니다. 오른쪽 열에서 해당 카메라, 마이크, 입력, 출력을 선택하거나 **없음** 을 선택하여 실제 개발 장치의 매핑을 수행합니다.

     > **모든** 카메라, 마이크로폰, 입력, 출력 등을 매핑합니다. **없음** 으로 매핑된 콘텐츠는 **상실** 됩니다.



이전 하드웨어 장치가 새 장치보다 더 많은 수의 개별 장치를 가진 경우의 예:



다음 을 클릭합니다.

6. 추가, 교체 또는 제거할 하드웨어 목록이 표시됩니다. **확인** 을 클릭합니다.
7. 마지막 단계는 추가, 교체했거나 본래의 장치와 해당 설정에 대한 요약이 나타납니다. **클립보드로 복사** 를 클릭하여 내용을 Windows 클립보드로 복사하거나 **닫기** 를 클릭하여 마법사를 종료합니다.

하드웨어 데이터 업데이트

하드웨어 장치와 시스템이 동일한 펌웨어 버전을 사용하도록 하려면 Management Client 의 하드웨어 장치에 대한 하드웨어 데이트를 수동으로 업데이트해야 합니다. Milestone 은(는) 하드웨어 장치에 대해 펌웨어 업데이트를 수행한 후마다 하드웨어 데이터를 업데이트할 것을 권장합니다.

최신 하드웨어 데이터를 받으려면 다음과 같이 하십시오.

1. **사이트 탐색** 창에서, **레코딩 서버** 를 선택합니다.
2. 필요한 레코딩 서버를 확장한 후, 최신 정보를 받고자 하는 하드웨어를 선택합니다.
3. **정보** 탭의 **속성** 창에서, **마지막으로 업데이트된 하드웨어 데이터** 필드의 **업데이트** 버튼을 클릭합니다.
4. 시스템이 해당 하드웨어에 대해 최신 펌웨어를 구동하고 있는지 마법사가 확인합니다.

   확인 을 선택하여 Management Client 의 정보를 업데이트합니다. 업데이트가 완료되면 시스템이 감지한 해당 하드웨어 장치의 현재 펌웨어 버전이 **정ㅂ** 탭의 **펌웨어 버전** 필드에 표시됩니다.

SQL Server 데이터베이스의 위치 및 이름 변경

관리 서버, 이벤트 서버, 로그 서버, Identity Provider, XProtect Incident Manager은(는) 연결 문자열을 사용하여 다른 SQL Server 데이터베이스에 연결합니다. 이러한 연결 문자열은 Windows 레지스트리에 저장됩니다. SQL Server 데이터베이스의 위치나 이름을 변경한 경우 해당 SQL Server 데이터베이스를 가리키는 모든 연결 문자열을 편집해야 합니다.

데이터베이스	사용 주체:
감시 데이터베이스	• Management Server 서비스 • Event Server 서비스 • VideoOS Management Server 앱 풀 • VideoOS 보고서 서버 앱 풀
Surveillance_IDP	• VideoOS IDP 앱 풀
Surveilance_IM	• VideoOS IM 앱 풀
Surveillance_LogServerV2	• Log Server 서비스

진행하기 전:

- SQL Server 데이터베이스 및 Windows 레지스트리를 백업합니다.
- 관련 서비스 및 앱 풀을 실행하는 사용자가 데이터베이스의 소유자인지 확인합니다.
- 기존 SQL Server 데이터베이스에서 새 데이터베이스로의 콘텐츠 마이그레이션을 완료합니다.

연결 문자열을 SQL Server 데이터베이스의 새 위치와 이름으로 업데이트하려면 다음과 같이 하십시오.

1. SQL Server 데이터베이스를 사용하는 모든 XProtect VMS 서비스와 앱 풀을 중지합니다.

   > 시스템 아키텍처에 따라 서비스 및 앱 풀이 다른 컴퓨터에서 실행될 수 있습니다. 동일한 SQL Server 데이터베이스에 연결하는 모든 앱 풀 및 서비스를 중지해야 합니다.

2. 레지스트리편집기에서`HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`으로이동합니다.

3. 연결 문자열을 SQL Server 데이터베이스의 새 위치와 이름으로 업데이트합니다.

   모든 SQL Server 데이터베이스의 기본 연결 문자열은 다음과 같습니다.

   - **ManagementServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**: `Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**: `Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. 1단계에서 중지한 모든 XProtect 서비스 및 앱 풀을 시작합니다.

서버 서비스 관리

서버 서비스를 실행하는 컴퓨터에서, 알림 영역에 서버 관리자 아이콘이 표시됩니다. 아이콘을 통해 서비스에 대한 정보를 얻고 특정 작업을 수행할 수 있습니다. 여기에는 서비스의 상태 확인, 로그나 상태 메시지 보기 및 서비스 시작 및 중지 등이 포함됩니다.

서버 관리자 트레이 아이콘(설명됨)

표에 있는 트레이 아이콘은 관리 서버, 레코딩 서버, 장애 조치 레코딩 서버, 이벤트 서버에서 구동되는 다양한 상태의 서비스를 보여줍니다. 이는 서버가 설치된 컴퓨터의 알림 영역에서 볼 수 있습니다.

Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				실행 중

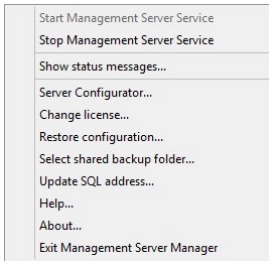
Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				서버 서비스가 활성화되고 시작된 경우 나타남. Failover Recording Server 서비스가 구동되고 있는 경우 이 서비스는 표준 레코딩 서버 오류를 처리할 수 있습니다.
				중지됨 서버 서비스가 중단된 경우 나타납니다. Failover Recording Server 서비스가 중단된 경우, 표준 레코드 서버 오류를 처리할 수 없습니다.
				시작 서버 서비스가 시작 과정에 있을 때 나타납니다. 평소 상황에서 트레이 아이콘은 잠시 후 **실행 중** 으로 변경됩니다.
				중단 서버 서비스가 중단 과정에 있을 때 나타납니다. 평소 상황에서 트레이 아이콘은

Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				잠시 후 **중단됨** 으로 변경됩니다.
				불확정적 상태 서버 서비스가 처음 로딩되고 첫 정보가 수신되기까지 나타나며, 평소 상황에서 트레이 아이콘은 **시작** 그리고 **실행 중** 으로 변경됩니다.
				오프라인 실행 중 보통 레코딩 서버 또는 장애 조치 레코딩 서버가 실행 중이나 Management Server 서비스는 실행되고 있지 않은 경우에 나타납니다.

Management Server 서비스 시작 또는 중지

Management Server Manager 트레이 아이콘은 Management Server 서비스의 상태를 나타냅니다(예: **실행 중**). 이 아이콘을 통해 Management Server 서비스를 시작하거나 중지할 수 있습니다. Management Server 서비스를 중지하면, Management Client 을(를) 사용할 수 없게 됩니다.

1. 알림 영역에서 Management Server Manager 트레이 아이콘을 마우스 오른쪽 버튼으로 클릭합니다. 상황별 메뉴가 나타납니다.



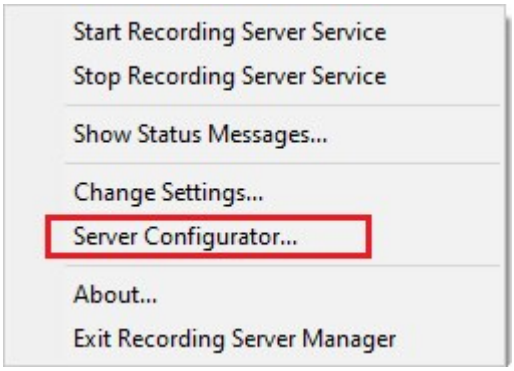
2. 서비스가 중단된 경우, **Management Server 서비스 시작** 을 클릭하여 서비스를 시작합니다. 새로운 상태를 반영하여 트레이 아이콘이 바뀝니다.
3. 서비스를 중지하려면 **Management Server 서비스 중지** 를 클릭합니다.

트레이 아이콘에 관한 자세한 정보는 페이지 322의 서버 관리자 트레이 아이콘(설명됨)를 참조하십시오.

Recording Server 서비스 시작 또는 중지

Recording Server Manager 트레이 아이콘은 Recording Server 서비스의 상태를 나타냅니다(예: **실행 중**). 이 아이콘을 통해 Recording Server 서비스를 시작하거나 중지할 수 있습니다. Recording Server 서비스를 중지하면, 시스템이 서버에 연결된 장치와 상호 작용할 수 없습니다. 즉, 라이브 비디오나 녹화된 비디오를 볼 수 없습니다.

1. 알림 영역에서 Recording Server Manager 트레이 아이콘을 마우스 오른쪽 버튼으로 클릭합니다. 상황별 메뉴가 나타납니다.

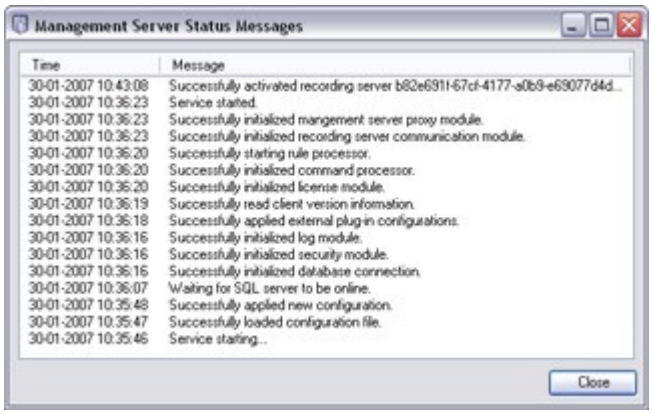


2. 서비스가 중단된 경우, **Recording Server 서비스 시작** 을 클릭하여 서비스를 시작합니다. 새로운 상태를 반영하여 트레이 아이콘이 바뀝니다.
3. 서비스를 중지하려면 **Recording Server 서비스 중지** 를 클릭합니다.

트레이 아이콘에 관한 자세한 정보는 페이지 322의 서버 관리자 트레이 아이콘(설명됨)를 참조하십시오.

관리 서버 또는 레코딩 서버에 대한 상태 메시지 보기

1. 알림 영역에서 관련 트레이 아이콘을 마우스 오른쪽 버튼으로 클릭합니다. 상황별 메뉴가 나타납니다.
2. **상태 메시지 표시** 를 선택합니다. 서버 유형에 따라 **Management Server 상태 메시지 또는 Recording Server 상태 메시지 창이** 나타나고 타임스탬프가 표시된 상태 메시지가 나열됩니다.



다음을 사용한 암호화 관리: Server Configurator

Server Configurator 을(를) 사용하여 로컬 서버에서 암호화 통신을 하기 위한 인증서를 선택하고, 서버 서비스를 등록하여 다른 서버들과 통신할 수 있는 자격을 부여할 수 있습니다.

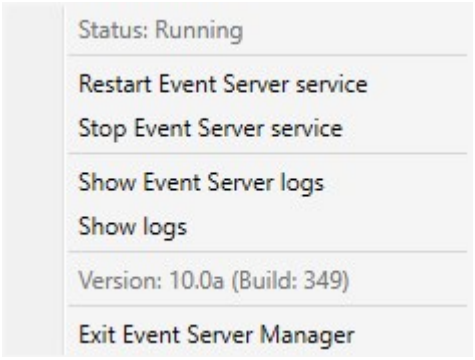
Windows시작 메뉴 또는 관리 서버 트레이 아이콘, 레코딩 서버 트레이 아이콘 중 하나에서 Server Configurator을(를) 엽니다. 페이지 370의 Server Configurator (유틸리티)를 참조하십시오.

자세한 정보는 XProtect VMS 설치 보호 방법에 관한 인증 안내서 를 참조합니다.

Event Server 서비스 시작, 중지 또는 재시작

Event Server Manager 트레이 아이콘은 Event Server 서비스의 상태를 나타냅니다(예: **실행 중**). 이 아이콘을 통해, Event Server 서비스를 시작, 중지 또는 다시 시작할 수 있습니다. 서비스를 중지하면 이벤트 및 알람을 포함하여 시스템의 일부가 작동하지 않습니다. 그러나, 비디오를 보고 녹화하는 작업은 가능합니다. 자세한 내용은 페이지 327의 Event Server 서비스 중지를 참조하십시오.

1. 알림영역에서EventServerManager트레이아이콘을마우스오른쪽버튼으로클릭합니다.상황별메뉴가나타납니다.



2. 서비스가 중단된 경우, **Event Server 서비스 시작** 을 클릭하여 서비스를 시작합니다. 새로운 상태를 반영하여 트레이 아이콘이 바뀝니다.
3. 서비스를다시시작또는중지하려면, **EventServer서비스 다시 시작**또는 **EventServer서비스 중지**를클릭합니다.

> 트레이 아이콘에 관한 자세한 정보는 페이지 322의 서버 관리자 트레이 아이콘(설명됨)를 참조하십시오.

Event Server 서비스 중지

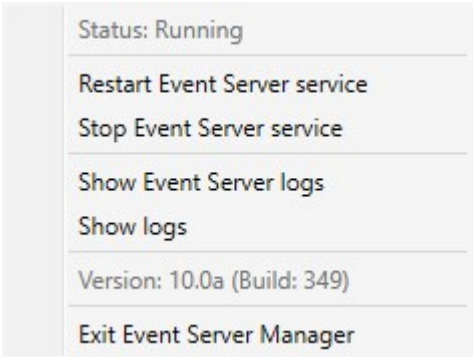
이벤트 서버에서 MIP 플러그 인을 설치할 때, 우선 Event Server 서비스를 중지하고, 나중에 다시 시작해야 합니다. 서비스가 중단되면 비디오 관리 소프트웨어 시스템의 많은 부분이 기능을 하지 않게 됩니다.

- 이벤트 서버에 이벤트나 알람이 저장되지 않습니다. 그러나, 시스템과 장치 이벤트는 여전히 예를 들어 레코딩 시작과 같은 동작을 트리거합니다
- XProtect 확장은 XProtect Smart Client에서 작동하지 않으며 Management Client에서 구성할 수 없습니다.
- 분석 이벤트가 작동하지 않습니다
- 일반 이벤트가 작동하지 않습니다
- 알람이 트리거되지 않습니다
- XProtect Smart Client 에서, 맵 항목 보기, 알람 목록 항목 보기 및 알람 관리자 작업 공간이 작동하지 않습니다
- 이벤트 서버에서 MIP 플러그 인을 실행할 수 없습니다
- MIP 및 Management Client 에서 XProtect Smart Client 플러그 인이 올바르게 작동하지 않습니다

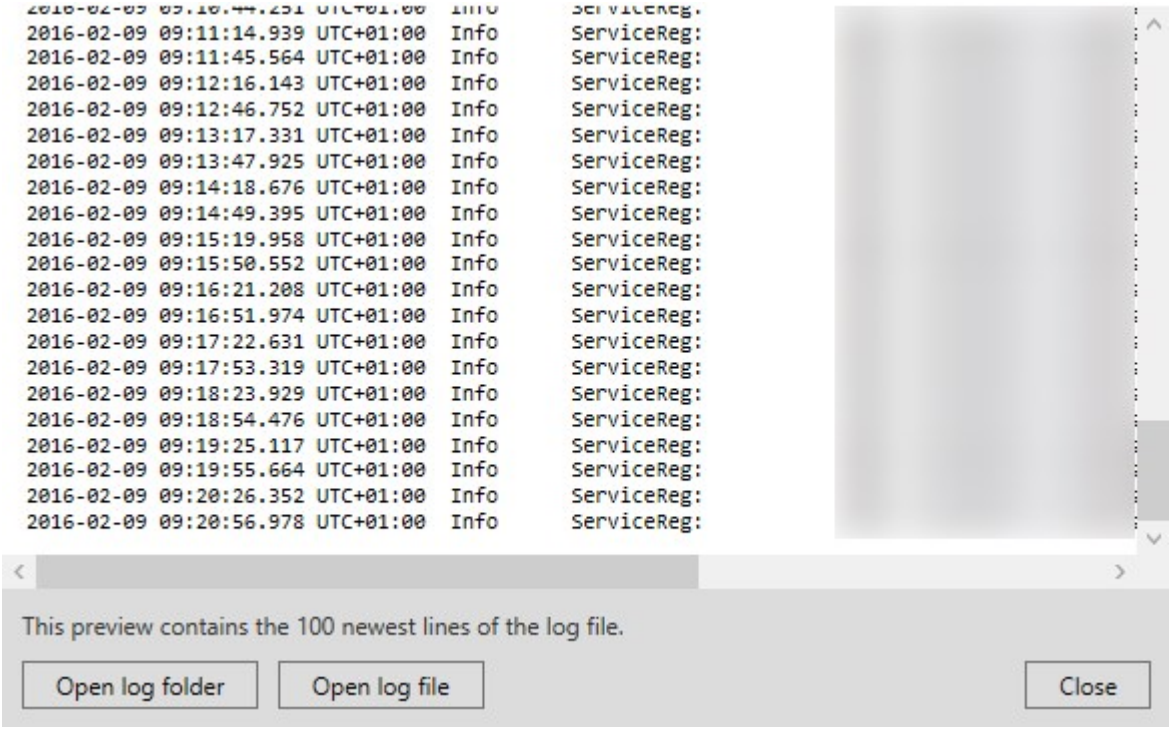
Event Server 또는 MIP 로그 보기

이벤트 서버 로그에서 이벤트 서버 활동에 관한 타임스탬프 정보를 볼 수 있습니다. 타사 통합에 관한 정보는 **이벤트 서버** 폴더의 하위 폴더에 있는 MIP 로그에 기록됩니다.

1. 알림영역에서EventServerManager트레이아이콘을마우스오른쪽버튼으로클릭합니다.상황별메뉴가나타납니다.



2. Event Server 로그에서 최근 100개의 라인을 보려면 **이벤트 서버 로그 표시** 를 클릭합니다.로그 뷰어가 나타납니다.



    1. 로그 파일을 보려면 **로그 파일 열기** 를 클릭합니다.
    2. 로그 폴더를 열려면 **로그 폴더 열기** 를 클릭합니다.

3. MIP 로그에서 최근 100개의 라인을 보려면, 상황별 메뉴로 돌아가서 **MIP 로그 표시** 를 클릭합니다. 로그 뷰어가 표시됩니다.

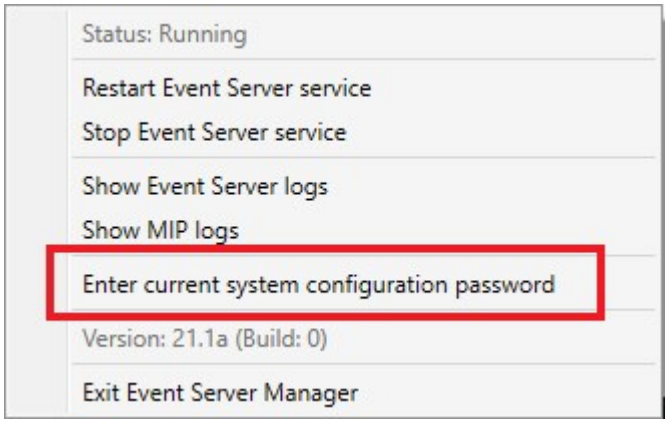
로그 디렉토리에서 로그 파일을 누군가가 삭제하면 메뉴 항목이 회색으로 표시됩니다. 로그 뷰어를 열려면 우선 로그 파일을 다음 로그 파일 폴더로 복사해야 합니다:
`C:\ProgramData\Milestone\XProtect Event Server\logs` 또는
`C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`

현재 시스템 구성 암호 입력

시스템 구성 암호가 관리 서버에서 변경된 경우, 이벤트 서버에도 현재 시스템 구성 암호를 입력해야 합니다.

이벤트 서버에서 현재 암호를 입력하지 않으면 액세스 제어와 같은 시스템 구성 요소가 작동을 중지합니다.

1. 알림 영역에서 Event Server Manager 트레이 아이콘을 마우스 오른쪽 버튼으로 클릭합니다. 상황별 메뉴가 나타납니다.



2. 현재 시스템 구성 암호를 입력하려면 **현재 시스템 구성 암호 입력** 을 클릭하십시오. 창이 표시됩니다.
3. 관리 서버에 입력한 것과 같은 동일한 시스템 구성 암호를 입력합니다.

등록된 서비스 관리

간혹 직접적으로 시스템의 일부가 아닌 경우에도 서버 및/서비스가 시스템과 통신할 수 있는 경우가 있습니다. 전부는 아니지만 일부 서비스가 시스템에서 자체적으로 등록될 수 있습니다. 자동으로 등록될 수 있는 서비스:

- Event Server 서비스
- Log Server 서비스

자동으로 등록된 서비스는 등록된 서비스 목록에 표시됩니다.

Management Client 에서 서버/서비스를 등록된 서비스로 수동으로 지정할 수 있습니다.

등록된 서비스 추가 및 편집

1. **등록된 서비스 추가/제거** 창에서 필요에 따라 **추가** 또는 **편집** 을 클릭합니다.
2. **등록된 서비스 추가** 또는 **등록된 서비스 편집** 창(앞에서 선택한 항목에 따라)에서 설정을 지정하거나 편집합니다.
3. **확인** 을 클릭합니다.

네트워크 구성 관리

네트워크 구성 설정을 사용하면 관리 서버와 트러스트된 서버가 통신할 수 있도록 관리 서버의 서버 LAN 과 WAN 주소를 지정할 수 있습니다.

1. **등록된 서비스 추가/제거** 창에서 **네트워크** 를 클릭합니다.
2. 관리 서버의 LAN 및/또는 WAN IP 주소를 지정합니다.

   관련된 모든 서버(관리 서버와 신뢰할 수 있는 서버 모두)가 로컬 네트워크에 있는 경우, 간단히 LAN 주소만 지정하면 됩니다. 하나 이상의 관련 서버가 인터넷 연결을 통해 시스템을 액세스하는 경우는 WAN 주소도 지정해야 합니다.

3. **확인** 을 클릭합니다.

등록된 서비스 속성

등록된 서비스 추가 또는 **등록된 서비스 편집** 창에서 다음을 지정합니다:

구성 요소	요구사항
유형	미리 채워진 필드.
이름	등록된 서비스의 이름. 이 이름은 Management Client 에 표시하는 용도로만 사용됩니다.
URLs	**추가**를 클릭하여 등록된 서비스의 IP 주소 또는 호스트 이름을 추가합니다. 호스트 이름을 URL 일부로 지정한 경우, 호스트가 네트워크에 존재하고 사용 가능해야 합니다. URL은 *http://* 또는 *https://*로 시작해야 하고, 다음의 문자가 포함되어서는 안 됩니다: *< > & ' " * ? | [ ] "*. 일반적인 URL 형식의 **예**: *http://ipaddress:port/directory* (여기서 포트 및 디렉토리는 선택 사항입니다). 필요한 경우 둘 이상의 URL을 추가할 수 있습니다.

구성 요소	요구사항
신뢰할 수 있음	등록된 서비스를 즉시 신뢰할 수 있는지 선택합니다(흔한 경우에 해당하나, 이 옵션은 등록된 서비스를 추가한 다음 나중에 등록된 서비스를 편집해서 신뢰할 수 있음으로 표시할 수 있는 유연성을 제공합니다). 신뢰할 수 있는 상태를 변경하면 해당 등록된 서비스에 대해 정의된 하나 이상의 URL을 공유하는 다른 등록된 서비스의 상태가 변경됩니다.
설명	등록된 서비스의 설명. 이 설명은 Management Client 에 표시하는 용도로만 사용됩니다.
고급	서비스가 고급일 경우, 정의하는 각 호스트 주소에 대해 특정 URI 구조(예: HTTP, HTTPS, TCP, 또는 UDP)를 설정해야 합니다. 따라서 호스트 주소에는 각각 자체적인 구성, 즉 해당 구성의 호스트 이름과 IP 포트를 가진 여러 끝점이 포함됩니다.

장치 드라이버 제거(설명됨)

컴퓨터에서 장치 드라이버가 더 이상 필요하지 않은 경우, 시스템에서 Device Pack(장치 팩)을 삭제할 수 있습니다. 이렇게 하려면 프로그램 제거를 위한 표준 Windows 절차를 따르십시오.

여러 Device Pack(장치 팩)을 설치했고 파일 삭제에 문제가 있을 경우, 완전히 삭제하기 위해 Device Pack(장치 팩) 설치 폴더에서 스크립트를 사용할 수 있습니다.

장치 드라이버를 제거할 경우, 레코딩 서버 및 카메라 장치는 더 이상 통신할 수 없습니다. 이전 버전 위에 새 버전을 설치할 수 있으므로 업그레이드 시 장치 팩을 제거하지 마십시오. 모든 시스템을 제거하는 경우에만 장치 팩을 제거할 수 있습니다.

레코딩 서버 제거

> ⚠ 레코딩 서버를 제거할 경우, 레코딩 서버의 관련 하드웨어(카메라, 입력 장치 등) **모두**를 포함하여 Management Client에서 레코딩 서버에 대해 지정된 모든 구성이 제거됩니다.

1. **개요** 창에서 제거할 레코딩 서버를 마우스 오른쪽 단추로 클릭합니다.
2. **Recording Server 제거** 를 선택합니다.
3. 계속하려면 **예** 를 선택합니다.
4. 레코딩 서버와 관련된 모든 하드웨어가 제거됩니다.

레코딩 서버에서 모든 하드웨어 삭제

하드웨어를 삭제하면, 해당 하드웨어와 관련된 모든 기록된 데이터가 영구적으로 삭제됩니다.

1. 모든 하드웨어를 삭제할 레코딩 서버를 마우스 오른쪽 단추로 클릭합니다.
2. **모든 하드웨어 삭제** 를 선택합니다.
3. 삭제를 확인합니다.

관리 서버 컴퓨터의 호스트 이름 변경

관리서버가 정규화된 도메인 이름(FQDN) 또는 자체 호스트 이름을 주소로 하는 경우, 컴퓨터의 호스트 이름을 변경하면 반드시 고려되고 다뤄져야 할 XProtect 내에 적용되게 됩니다.

일반적으로 관리 서버의 호스트 이름 변경은 향후 필요한 클린업 양으로 인해 주의해서 계획해야 합니다.

다음 섹션에서 호스트 이름 변경의 일부 적용 사례에 관한 개요를 확인할 수있습니다.

인증서의 유효성

인증서는 서비스 간 통신 암호화에 사용되며, 이러한 인증서는 하나 이상의 XProtect 서비스를 구동하는 모든 컴퓨터에 설치됩니다.

인증서생성방식에따라인증서를설치한컴퓨터에관련될수있으며,컴퓨터이름이동일하게유지되는경우에만유효합니다.

인증서 생성 방법에 관한 자세한 정보는 인증서 소개 를 참조하십시오.

컴퓨터의 이름이 변경된 경우, 사용된 인증서는 유효하지 않게 될 수 있으며 XProtect VMS 이(가) 시작되지 않을 수 있습니다. 시스템이 정상적으로 다시 구동되게 하려면 다음 단계를 완료하십시오.

- 새 인증서를 생성하고 사용 환경의 모든 컴퓨터에 인증서를 재설치합니다.
- Server Configurator 을(를) 사용하여 새 인증서를 각 컴퓨터에 적용하여 새 인증서로 암호화를 가능하게 합니다.

이렇게 함으로써 새 인증서 등록이 트리거되며 시스템이 다시 구동됩니다.

등록된 서비스에 대한 고객 데이터 속성 손실

후에 Server Configurator 을(를) 사용하여 등록을 완료하는 경우(예: 관리 서버 주소 변경), 등록된 서비스에 대한 정보 편집 내용은 덮어씌어지게 됩니다. 그러므로 등록된 서비스에 대한 정보를 변경한 경우, 이름이 변경된 컴퓨터 상의 관리 서버에 등록된 모든 서비스에 대해 변경 사항을 다시 적용해야 합니다.

등록된 서비스에 대해 편집될 수 있는 정보는 **도구** > **등록된 서비스** > **편집** 아래에 있습니다.

- 신뢰할 수 있음
- 고급
- 외부 플래그
- 수동 추가된 모든 URL

Milestone Customer Dashboard 에서, 호스트 이름은 변경되지 않은 것으로 표시됩니다

Milestone Customer Dashboard은(는) Milestone 소프트웨어 설치 및 라이선스를 관리하고 모니터링하기 위한 Milestone 파트너, 리셀러, XProtect VMS 사용자를 위한 무료 온라인 도구입니다.

Milestone Customer Dashboard 에 연결된 시스템 상의 관리 서버 이름 변경은 자동으로 Milestone Customer Dashboard 에 반영되지 않습니다.

기존 호스트 이름이 새 라이선스 활성화가 완료될 때까지 Milestone Customer Dashboard 에 표시됩니다. 그러나 이름 변경은 Milestone Customer Dashboard의 어떤 것도 이용 불가능하게 만들지 않으며 새 활성화가 완료되면 해당 기록은 새 호스트 이름으로 데이터베이스에 업데이트됩니다. Milestone Customer Dashboard에 관한 자세한 내용은 Milestone Customer Dashboard(설명됨)를 참조하십시오.

호스트 이름을 변경하면 SQL Server 주소도 변경됩니다

SQL Server이(가) 동일한 컴퓨터에 관리 서버로 있고 이 컴퓨터의 이름이 변경된 경우, SQL Server의 주소도 변경됩니다. 즉, SQL Server 주소는 다른 컴퓨터에 있는 구성 요소뿐만 아니라 SQL Server에 연결된 로컬호스트가 아닌 컴퓨터 이름을 사용하는 로컬 컴퓨터에 있는 구성 요소에 대해서도 업데이트되어야 합니다. 이는 특히 Event Server 로서 동일한 데이터베이스를 사용하는 Management Server 에 대해서도 적용됩니다. 또한 다른 데이터베이스를 사용하지만 동일한 SQL Server에 있을 가능성이 높은 Log Server에 대해서도 적용됩니다.

페이지 321의 SQL Server 데이터베이스의 위치 및 이름 변경를 참조하십시오.

다음에서의 호스트 이름 변경: Milestone Federated Architecture

Milestone Federated Architecture 설정 내에 있는 컴퓨터의 이름 변경에는 다음과 같은 사항이 적용되며, 이는 워크 그룹 내 및 도메인에 걸쳐 사이트가 연결될 때 모두 적용됩니다.

사이트의 호스트는 아키텍처의 루트 노드입니다

아키텍처 내 중앙 사이트가 구동되는 컴퓨터의 이름을 변경하는 경우, 모든 하위 노드는 자동으로 새 주소로 재첨부됩니다. 그러므로 이러한 경우에는 이름을 변경해도 별도의 조치가 필요하지 않게 됩니다.

사이트의 호스트는 아키텍처의 하위 노드입니다

하나 이상의 연합 사이트가 구동되고 있는 컴퓨터의 이름 변경 시 연결 문제를 피하려면 컴퓨터 이름이 변경되기 전에 영향을 받게 되는 사이트에 대한 대체 주소를 추가해야 합니다. 영향을 받는 사이트는 이름이 변경될 호스트 컴퓨터의

노드가 됩니다. 준비되지 않거나 예기하지 못한 호스트 이름 변경으로 인한 연결 문제 및 이러한 문제 해결 방법에 관한 자세한 정보는 다음을 참조하십시오. 문제: Milestone Federated Architecture 설정의 상위 노드가 하위 노드에 연결할 수 없습니다 .

대체 주소를 **사이트 탐색** 또는 **연합 사이트 계층** 창에 있는 **속성** 창에 추가해야 합니다. 다음의 전제 조건을 반드시 충족해야 합니다.

- 호스트 컴퓨터의 이름이 변경되기 전에 추가되어야 할 대체 주소가 사용 가능해야 합니다.
- 대체 주소는 향후 호스트 컴퓨터의 이름을 반영해야 합니다(이름이 변경된 후)

속성 창에 액세스하는 방법에 관한 정보는 사이트 정보 설정 을 참조하십시오.

> 매끄럽게 업데이트를 하려면 호스트 이름이 변경될 컴퓨터에 대해 상위 노드 역할을 하는 노드의 Management Client 을(를) 정지합니다. 그렇지 않으면 컴퓨터 이름이 변경된 후 클라이언트를 중지하고 재시작합니다. 자세한 정보는 Management Server 서비스 시작 또는 중지 를 참조하십시오.

> 또한 제공한 대체 주소가 중앙 사이트의 **연합 사이트 계층** 창에 반영되도록 하십시오. 그렇지 않은 경우 Management Client 을(를) 중지하고 재시작합니다.

호스트 이름을 변경하고 컴퓨터를 재시작한 후에는 연합 사이트가 자동으로 새 주소로 변경되게 됩니다.

서버 로그 관리

다음은 서버 로그의 유형입니다:

- 시스템 로그
- 감사 로그
- 규칙 트리거 로그

이는 시스템 사용량을 로깅하는데 사용합니다. 이러한 로그는 **서버 로그** 아래 Management Client 에서 사용할 수 있습니다.

문제 해결 및 소프트웨어 오류 조사에 사용되는 로그에 관한 정보는 페이지 339의 디버깅 로그(설명됨)를 참조하십시오.

사용자 활동, 이벤트, 동작 및 오류 식별

시스템의 사용자 활동, 이벤트, 동작 및 오류의 상세 기록을 얻기 위해 로그를 사용합니다.

Management Client 에서 로그를 보려면 **사이트 탐색** 창에서 **서버 로그** 를 선택합니다.

로그 유형	로그됐다는 것의 의미
시스템 로그	시스템 관련 정보
감사 로그	사용자 활동
규칙 트리거 로그	사용자가 **새로운 <로그 항목>** 만들기 동작을 지정한 규칙. <log entry> 동작에 관한 자세한 정보는 동작 및 중지 동작 을 참조합니다.

다른 언어로 로그를 보려면 **옵션** 아래 페이지 353의 일반 탭(옵션)를 참조하십시오.

로그를 콤마로 분리된 값 형태의 파일 (.csv)로 내보내려면, 로그 내보내기 를 참조하십시오.

로그 설정을 변경하려면 페이지 356의 서버 로그 탭(옵션)를 참조하십시오.

로그 필터

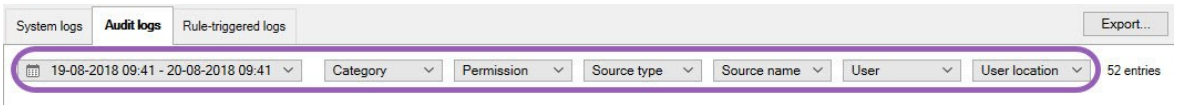
각 로그 창에서 필터를 적용하여 예를 들어 특정 시간 간격, 장치 또는 사용자의 로그 엔트리를 조회합니다.

> 필터는 현재 사용자 인터페이스에서 볼 수 있는 로그 엔트리에서 생성됩니다.

1. **사이트 탐색** 창에서 **서버 로그** 를 선택합니다. 기본 설정상 **시스템 로그** 탭이 나타납니다.

   로그 유형 간 탐색을 하고자 하는 경우, 다른 탭을 선택합니다.

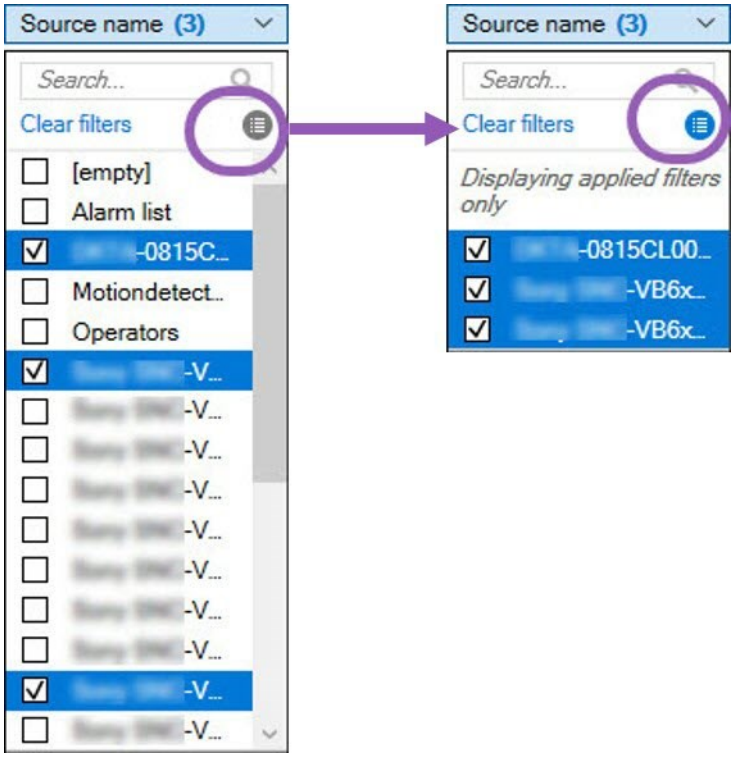
2. 탭 아래에서 필터 그룹을 선택합니다 (예: **카테고리**, **소스 유형** 또는 **사용자**).



   필터 목록이 표시됩니다. 필터 목록에는 최대 1000개의 필터가 표시됩니다.

3. 필터를 선택하여 적용합니다. 다시 필터를 선택하면 필터가 삭제됩니다.

   선택 사항: 필터 목록에서 **적용된 필터만 보기** 를 선택하여 적용한 필터만 볼 수 있습니다.



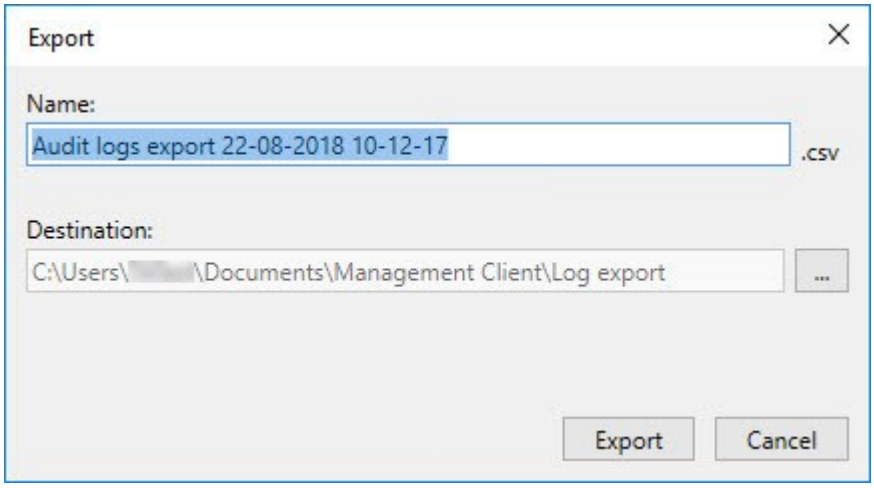
로그를 내보내기할 때에 적용한 필터에 따라 내보내기 하는 콘텐츠가 변경됩니다. 내보내기에 대한 정보는 로그 내보내기 를 참조하십시오.

로그 내보내기

로그 내보내기는 예를 들어 로그 보존 기간 이상으로 로그 항목을 저장하고자 할 때 유용합니다. 로그는 콤마로 분리된 값 형태의 파일 (.csv)로 내보낼 수 있습니다.

로그를 내보내려면:

1. 상단 우측 가장자리에 있는 **내보내기** 를 선택합니다. **내보내기** 창이 나타납니다.



2. **내보내기** 창의 **이름** 필드에서 로그 파일에 대한 이름을 지정합니다.
3. 기본적으로 내보낸 로그 파일은 **로그 내보내기** 폴더에 저장됩니다. 다른 위치를 지정하려면 **파일 경로** 필드의 오른쪽에 있는 ... 을(를) 선택합니다.
4. **내보내기** 를 선택하여 로그를 내보냅니다.

적용한 필터에 따라 내보내기하는 자료가 달라집니다. 내보내기에 대한 정보는 로그 필터 를 참조하십시오.

로그 검색

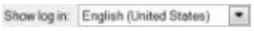
로그를 검색하려면 로그 창의 상단에서 **검색 기준** 을 사용합니다:

1. 목록에서 검색 기준을 지정합니다.
2. **새로 고침** 을 클릭하여 귀하의 검색 기준이 로그 페이지에 반영되도록 합니다. 검색 기준을 지우려면 모든 로그 콘텐츠 뷰로 돌아가서 **지우기** 를 클릭합니다.

로그 상세 내용 창에 표시된 모든 상세 내용을 보려면 모든 줄을 더블클릭하면 됩니다. 또한 이렇게 하여 한 줄에 표시되는 것보다 많은 텍스트를 포함한 로그 엔트리를 읽을 수 있습니다.

로그 언어 변경

1. 로그 창 하단의 **로그인 표시** 목록에서 원하는 언어를 선택합니다.



2. 로그가 선택된 언어로 표시됩니다. 다음에 로그를 열 때 기본 언어로 재설정됩니다.

로그를 작성하려면 2018 R2 및 조기 구성 요소를 허용하십시오

로그 서버의 2018 R3 버전은 추가적인 보안에 대한 인증을 소개합니다. 이는 2018 R2 및 그 이전 버전의 구성 요소가 로그 서버에 로그를 기록하는 것을 방지합니다.

영향을 받은 구성 요소

- XProtect Smart Client
- XProtect LPR 플러그 인
- LPR Server
- 액세스 제어 플러그 인
- Event Server
- 알람 플러그 인

위에 나열된 구성 요소에 대하여 2018 R2 또는 그 이전 버전을 사용하는 경우, 해당 구성 요소가 새로운 로그 서버에 로그를 작성하도록 할 것인지 여부를 결정해야 합니다.

1. **도구** > **옵션** 을 선택합니다.
2. **옵션**대화란의**서버 로그**탭아래쪽에서**2018 R2 및 조기 구성 요소가 로그를 작성하도록 허용하기**확인란을찾습니다.
    - 2018 R2 및 조기 구성 요소가 로그를 작성하도록 허용하려면 확인란을 선택합니다.
    - 2018 R2 및 조기 구성 요소가 로그를 작성하는 것을 금지하려면 확인란의 선택을 해제합니다.

문제 해결

디버깅 로그(설명됨)

디버깅 로그는 시스템의 결함 및 문제를 식별하는데 사용합니다.

시스템 사용량에 대해 사용된 로그에 관한 정보는 페이지 334의 서버 로그 관리를 참조하십시오.

다음은 XProtect 설치의 로그 파일 위치입니다:

- `C:\ProgramData\Milestone\IDP\Logs`

  > 이는 IIS 사용자 및 관리자만 액세스할 수 있습니다. IIS 사용자가 변경된 경우, 이러한 허가 사항은 업데이트되어야 합니다.

- `C:\ProgramData\Milestone\MIPSDK`
- `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
- `C:\ProgramData\Milestone\XProtect Event Server\Logs`
- `C:\ProgramData\Milestone\XProtect Log Server`
- `C:\ProgramData\Milestone\XProtect Management Server\Logs`
- `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
- `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
- `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`

문제:SQL Server 및 데이터베이스 위치 변경으로 인한 데이터베이스 액세스 불가

SQL Server 및 비디오 관리 소프트웨어 데이터베이스의 위치가 변경된 경우(예를 들어, SQL Server이(가) 실행되는 컴퓨터의 호스트 이름을 변경), 레코딩 서버는 데이터베이스에 액세스할 수 없습니다.

해결책: SQL Server 및 데이터베이스의 변경이 반영되도록 연결 문자열을 변경하십시오. 페이지 321의 SQL Server 데이터베이스의 위치 및 이름 변경를 참조하십시오.

문제: 포트 충돌로 인한 레코딩 서버 시작 실패

이 문제는 단순 메일 전송 프로토콜(SMTP)이 포트 25를 사용하여 실행되는 경우에만 나타납니다. 포트 25가 이미 사용 중인 경우, Recording Server 서비스를 시작할 수 없을 수도 있습니다. 포트 번호 25는 레코딩 서버의 SMTP 서비스를 위해 사용 가능해야 합니다.

SMTP 서비스: 확인 및 해결책

다음과 같이 SMTP 서비스 설치 여부를 확인하십시오.

1. Windows의 **시작** 메뉴에서 **제어판** 을 선택합니다.
2. **제어판** 에서 **프로그램 추가 또는 제거** 를 더블 클릭합니다.
3. **프로그램 추가 또는 제거** 창의 왼편에서 **Windows 구성 요소 추가/제거** 를 클릭합니다.
4. **Windows 구성 요소** 마법사에서 **인터넷 정보 서비스(IIS)** 를 선택 후 **상세 내용** 을 클릭합니다.
5. **인터넷 정보 서비스(IIS)** 창에서 **SMTP 서비스** 체크 상자가 선택되었는지 확인합니다. 선택되었다면 SMTP 서비스는 설치된 상태입니다.

SMTP 서비스가 설치되었다면 다음 해결책 중 하나를 선택합니다.

해결책 1: SMTP 서비스를 비활성화하거나 수동 시작으로 설정

이 해결책을 통해 레코딩 서버가 SMTP 서비스를 항상 중단하지 않고 시작될 수 있도록 할 수 있습니다:

1. Windows의 **시작** 메뉴에서 **제어판** 을 선택합니다.
2. **제어판** 에서 **관리자 도구** 를 더블 클릭합니다.
3. **관리자 도구** 창에서 **서비스** 를 더블 클릭합니다.
4. **서비스** 창에서 **단순 메일 전송 프로토콜(SMTP)** 을 더블 클릭합니다.
5. **SMTP 속성** 창에서 **중지** 를 클릭한 후 **시작 유형** 을 **수동** 또는 **비활성화** 중 하나로 설정합니다.

   수동 으로 설정할 경우, SMTP 서비스를 **서비스** 창에서 수동으로 또는 명령 프롬프트에서 *net start SMTPSVC* 명령어를 사용하여 시작할 수 있습니다.
6. **확인** 을 클릭합니다.

해결책 2: SMTP 서비스 제거

SMTP 서비스를 제거하면 다른 애플리케이션이 SMTP 서비스를 사용하는 데 영향을 줄 수 있습니다.

1. Windows의 **시작** 메뉴에서 **제어판** 을 선택합니다.
2. **제어판** 에서 **프로그램 추가 또는 제거** 를 더블 클릭합니다.
3. **프로그램 추가 또는 제거** 창의 왼편에서 **Windows 구성 요소 추가/제거** 를 클릭합니다.
4. **Windows 구성 요소** 마법사에서 **인터넷 정보 서비스(IIS)** 를 선택 후 **상세 내용** 를 클릭합니다.
5. **인터넷 정보 서비스(IIS)** 창에서 **SMTP 서비스** 체크 상자가 해제되었는지 확인합니다.
6. **OK**, **다음**, **완료** 를 차례대로 클릭합니다.

문제: Recording Server 이(가) Management Server 클러스터 노드로 변경 시 오프라인이 됩니다.

Management Server 중복을 위한 Microsoft 클러스터를 설정하는 경우, Recording Server 또는 Recording Server 은(는) 클러스터 노드간 Management Server 변경 시 오프라인이 될 수도 있습니다.

이를 수정하려면 다음을 수행하십시오.

> 구성 변경 시, Microsoft 장애 조치 클러스터 관리자에서, 서비스 제어 및 모니터링을 중단하여 Server Configurator 이(가) 변경 후 Management Server 서비스를 시작 및/또는 중지할 수 있게 해줍니다. 장애 조치 클러스터 서비스 시작 유형을 수동으로 변경한 경우, Server Configurator 와(과) 아무런 충돌이 일어나지 않게 됩니다.

Management Server 컴퓨터에서:

1. 관리 서버사 설치된 각 컴퓨터에서 Server Configurator 을(를) 시작합니다.
2. **등록** 페이지로 이동합니다.
3. 연필( ) 기호를 클릭하여 관리 서버 주소를 편집할 수 있도록 합니다.
4. 관리 서버 주소를 클러스터 URL로 변경합니다(예: `http://MyCluster`).
5. **등록** 을 클릭합니다.

Management Server을(를) 사용하는 구성 요소가 포함된 컴퓨터에서(예: Recording Server, Mobile Server, Event Server, API Gateway):

1. 각 컴퓨터에서 Server Configurator 을(를) 시작합니다.
2. **등록** 페이지로 이동합니다.
3. 관리 서버 주소를 클러스터 URL로 변경합니다(예: `http://MyCluster`).
4. **등록** 을 클릭합니다.

문제: 하위 노드에 연결할 수 없는 Milestone Federated Architecture 설정의 상위 노드

Milestone Federated Architecture 에서 하위 노드 역할을 담당하는 사이트의 호스트 컴퓨터 이름을 변경한 경우, 상위 노드가 해당 컴퓨터에 연결할 수 없게 됩니다.

상위 노드와 사이트 간 연결을 재설정하기

- 영향을 받은 사이트를 상위 노드에서 분리합니다. 자세한 정보는 계층에서 사이트 분리 를 참조하십시오.
- 호스트의 새 이름을 사용하여 해당 사이트를 다시 추가합니다. 자세한 내용은 계층 구조에 사이트 추가 를 참조하십시오.

변경 사항을 적용하도록 하려면 호스트 이름이 변경된 컴퓨터에 대해 상위 노드 역할을 하는 노드의 Management Client 을(를) 중지하고 재시작해야 할 수도 있습니다. 자세한 정보는 Management Server 서비스 시작 또는 중지 를 참조하십시오.

Milestone Federated Architecture 설정에서 호스트 이름 변경 적용에 관한 자세한 정보는 Milestone Federated Architecture 내 호스트 이름 변경 을 참조하십시오.

문제: Azure SQL 데이터베이스 서비스를 사용할 수 없음

Azure SQL 데이터베이스를 사용하며 설치 또는 정상 작동 중에 연결 문제가 발생하는 경우, 그 이유는 Azure SQL 데이터베이스 서비스를 일시적으로 사용할 수 없기 때문일 수 있습니다.

Azure SQL 데이터베이스는 기존 데이터베이스 유지 관리의 대부분을 Microsoft에서 처리하는 서비스입니다. 짧은 기간 동안 서비스를 사용할 수 없을 수 있으며, 사용자 개입 없이도 어느 정도 복구되도록 설계되었습니다.

데이터베이스 오류는 관련 사건 ID와 함께 XProtect VMS 로그 파일에 작성되며, 이는 확장된 Azure SQL 데이터베이스를 사용할 수 없는 경우 Microsoft 지원팀에 제공될 수 있습니다.

자세한 내용은 Azure SQL 데이터베이스에 대한 일반적인 연결 문제 해결을 참조하십시오.

업그레이드

업그레이드(설명됨)

업그레이드 시 컴퓨터에 현재 설치된 모든 구성 요소가 업그레이드됩니다. 업그레이드를 하는 동안에는 설치된 구성 요소를 제거할 수 없습니다. 설치된 구성 요소를 제거하려면 업그레이드 전이나 후에 Windows의 **프로그램 추가 및 제거** 기능을 사용하십시오. 업그레이드 시 관련 서버 데이터베이스를 제외한 모든 구성 요소가 자동으로 제거되어 대체됩니다. 여기에는 Device Pack(장치 팩)의 드라이버가 포함됩니다.

관리 서버 데이터베이스에는 전체 시스템 구성(레코딩 서버 구성, 카메라 구성, 규칙 등)이 들어 있습니다. 관리 서버 데이터베이스를 제거하지 않는 한, 신규 버전의 새로운 기능 중 일부를 구성하려는 경우에도 시스템 구성을 재구성할 필요가 없습니다.

현재 버전 이전의 XProtect 레코딩 서버 버전과의 역호환성은 제한됩니다. 그러한 기존 레코딩 서버의 레코딩에 액세스할 수 있지만, 구성을 변경하려면 현재 버전과 동일한 버전이어야 합니다. Milestone 에서는 시스템에 모든 레코딩 서버를 업그레이드 하도록 권장합니다.

레코딩 서버를 포함한 업그레이드를 수행할 때 비디오 장치 드라이버를 업데이트 또는 유지할지 여부를 묻는 메시지가 표시됩니다. 업데이트를 선택한 경우, 시스템을 다시 시작한 후 하드웨어 장치가 새로운 비디오 장치 드라이버와 연결되기까지 몇 분 정도 걸릴 수 있습니다. 이는 새로 설치된 드라이버에서 여러 내부 검사가 수행되기 때문입니다.

2017 R3버전 또는 이전 버전에서 2018 R1 이상 버전으로 업그레이드하거나 시스템에 기존 카메라가 있다면, 당사 웹사이트의 다운로드 페이지에서 레거시 드라이버를 가진 장치 팩을 수동으로 다운로드해야 합니다(https://www.milestonesys.com/downloads/). 레거시 장치 팩의 드라이버를 사용하는 카메라가 있는지 확인하려면 당사 웹사이트에서 이 페이지를 확인하십시오(https://www.milestonesys.com/community/business-partner-tools/device-packs/).

버전 2018 R1 또는 이전 버전에서 2018 R2 이상의 버전으로 업그레이드하려면, 업그레이드하기 전에 시스템의 모든 레코딩 서버를 보안 패치로 업데이트해야 합니다. 보안 패치 없이 업그레이드하면 레코딩 서버가 작동하지 않게 됩니다.

레코딩 서버에 보안 패치를 설치하는 방법은 당사 웹사이트https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/ 에서 제공됩니다.

관리서버와 레코딩 서버간의 연결을 암호화하고자 하는 경우 모든 레코딩 서버는 2019 R2 또는 그 이상 버전으로 반드시 업그레이드 되어야 합니다.

권장 업그레이드 시퀀스에 대한 개요는 페이지 346의 권장 업그레이드 방식을(를) 참조하십시오.

업그레이드 요구 사항

- 소프트웨어 라이선스 파일(페이지 105의 라이선스(설명됨) 참조) (.lic)를 준비하십시오.
  - **서비스 팩 업그레이드**: 관리 서버 설치 과정에서 마법사가 소프트웨어 라이선스 파일의 위치를 지정하도록 요청할 수 있습니다. 시스템 구입(또는 마지막 업그레이드) 후 받은 소프트웨어 라이선스 파일 및 마지막 라이선스 활성화 후 받은 활성화된 소프트웨어 라이선스 파일을 모두 사용할 수 있습니다
  - **버전 업그레이드**: 새 버전을 구매한 후 새 소프트웨어 라이선스 파일이 제공됩니다. 관리 서버 설치 과정에서 마법사가 새 소프트웨어 라이선스 파일의 위치를 지정하도록 요청합니다

  계속하기 전에 시스템이 소프트웨어 라이선스 파일의 유효성을 확인합니다. 라이선스가 필요한, 이미 추가된 하드웨어 장치와 기타 장치에는 유예 기간이 적용됩니다. 자동 라이선스 활성화를 켜지 않은 경우(페이지 111의 자동 라이선스 활성화 참조), 유예 기간이 만료되기 전에 수동으로 라이선스를 활성화하는 것을 잊지 마십시오. 소프트웨어 라이선스 파일이 없을 경우 XProtect 리셀러에게 문의하십시오.
- **새 제품 버전** 의 소프트웨어를 준비합니다. Milestone 웹사이트에 다운로드 페이지에서 다운로드할 수 있습니다.
- 시스템 구성(페이지 304의 시스템 구성 백업 및 복원(설명됨) 참조)을 백업했는지 확인하십시오.

  관리 서버는 시스템 구성을 SQL Server 데이터베이스에 저장합니다. SQL Server 데이터베이스는 관리 서버 기기 자체의 SQL Server 인스턴스나 네트워크의 SQL Server 인스턴스에 있을 수 있습니다.

  사용 중인 네트워크의 SQL Server 인스턴스에서 SQL Server 데이터베이스를 사용하는 경우, SQL Server 데이터베이스 생성 또는 이동, 업그레이드를 할 때마다 해당 관리 서버에 SQL Server 인스턴스의 관리자 권한이 있어야 합니다. SQL Server 데이터베이스의 일반 사용 및 관리를 위해 관리 서버는 데이터베이스를 보유하고 있기만 하면 됩니다.
- 설치 중에 암호화를 활성화할 계획이라면, 관련된 컴퓨터 상에 설치되고 신뢰받은 적절한 인증서가 필요합니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 을(를) 참조하십시오.

업그레이드를 시작할 준비가 되면 페이지 346의 권장 업그레이드 방식의 절차를 따르십시오.

FIPS 140-2 규격 모드에서의 실행을 위한 XProtect VMS 업그레이드

2020 R3에서부터 XProtect VMS 은(는) FIPS 140-2 인증 알고리즘 인스턴스만 사용하여 실행하도록 구성되었습니다.

XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

FIPS비 규격 암호로 암호화된 2017 R1 이전의 XProtect VMS 버전의 내보내기와 저장된 미디어 데이터베이스가 있는 FIPS 140-2 규격 시스템의 경우, FIPS를 활성화한 후에도 액세스할 수 있는 위치에 데이터를 저장해야 합니다.

다음프로세스는XProtectVMS이(가)FIPS140-2규격모드에서실행되도록구성하는데필요한것이무엇인지설명해줍니다.

1. SQL Server을(를) 호스팅하는 컴퓨터를 비롯하여 비디오 관리 소프트웨어의 일부인 모든 컴퓨터의 Windows FIPS 보안 정책을 비활성화하십시오.

   업그레이드 시 FIPS가 Windows 운영 체제에서 활성화되어 있으면 XProtect VMS 을(를) 설치할 수 없습니다.

2. 독립형 타사 통합이 FIPS가 활성화된 Windows 운영 체제에서 실행되도록 해야 합니다.

   독립형 통합이 FIPS 140-2 규격이 아닌 경우, Windows 운영 체제를 FIPS 모드에서 운영되도록 설정한 후에는 통합을 실행할 수 없습니다.

   이를 막으려면 다음과 같이 해야 합니다.

   - 다음에 대한 모든 독립형 통합의 인벤토리 작성: XProtect VMS
   - 이러한 통합의 공급업체에 문의하여 해당 통합이 FIPS 140-2 규격인지 확인
   - FIPS 140-2 규격 독립형 통합을 배포

3. 장치에 대한 통신인 드라이버가 FIPS 140-2 규격을 준수하도록 합니다.

   XProtect VMS 은(는) 다음 기준에 부합하는 경우 FIPS 140-2 규격 모드 운영을 보장하며 강화할 수 있습니다.

   - 장치는 규격을 준수하는 드라이버만 사용하여 다음에 연결: XProtect VMS

     규정 준수를 보장하고 강화하는 드라이버에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 준수 섹션을 참조하십시오.

   - 장치 팩 버전 11.1 이상을 사용하는 장치

     레거시 드라이버 장치 팩의 드라이버는 FIPS 140-2 규격 연결을 보장하지 않습니다.

   - 장치는 HTTPS에서 연결되었으며 HTTPS상의 비디오 스트림을 위한 SRTP(Secure Real-Time Transport Protocol) 또는 RTSP(Real Time Streaming Protocol) 둘 중 하나에 연결됨

     드라이버 모듈은 HTTP상의 FIPS 140-2 연결 규격을 보장하지 않습니다. 해당 연결은 규격을 준수할 수도 있지만 실제로 규격에 맞는지 여부는 보장할 수 없습니다.

   - 레코딩 서버를 실행하는 컴퓨터는 FIPS 모드가 활성화된 Windows 운영 체제를 실행

4. 미디어 데이터베이스의 데이터가 FIPS 140-2 규격 암호로 암호화되도록 해야 합니다.

   이 작업은 미디어 데이터베이스 업그레이드 도구를 실행하면 이뤄집니다. XProtect VMS이(가) FIPS 140-2 호환 모드에서 구동하도록 구성하는 방법에 관한 자세한 내용은 강화 안내서의 FIPS 140-2 호환 섹션을 참조하십시오.

5. FIPS를 Windows 운영 체제에서 활성화하기 전, 그리고 XProtect VMS 시스템을 구성한 후 및 모든 구성 요소와 장치가 FIPS가 활성화된 환경에서 실행되는 것을 확인한 후, XProtect Management Client 에서 기존 하드웨어 암호를 업데이트합니다.

   이렇게 하려면 Management Client의 **레코딩 서버** 노드의 선택된 레코딩 서버에서 마우스 오른쪽 단추로 **하드웨어 추가**를 클릭하여 선택합니다. **하드웨어 추가** 마법사를 통해 진행합니다. 이렇게 하면 모든 기존 자격 증명 및 이에 대한 암호화가 FIPS 규격으로 업데이트됩니다.

모든 클라이언트를 비롯하여 전체 VMS를 업그레이드한 후에만 FIPS를 활성화할 수 있습니다.

권장 업그레이드 방식

실제로 업그레이드를 시작하기 전에 SQL Server 데이터베이스 백업을 비롯한 업그레이드 요건(페이지 344의 업그레이드 요구 사항 참조)에 관해 읽어 보십시오.

장치 드라이버는 최신 드라이버가 포함된 정기 Device Pack(장치 팩)과 기존 드라이버가 포함된 레거시 Device Pack(장치 팩)으로 나누어 집니다. 정기 Device Pack(장치 팩)은 항상 업데이트 또는 업그레이드와 함께 자동으로 설치됩니다. 레거시 Device Pack(장치 팩)의 장치 드라이버를 사용하는 기존 카메라가 있는 경우, 그리고 레거시 Device Pack(장치 팩)이 아직 설치되지 않은 경우, 시스템은 레거시 Device Pack(장치 팩)을 자동으로 설치하지 않습니다.

시스템에 기존 카메라가 있는 경우, Milestone 은(는) 카메라가 레거시 장치 팩의 드라이버를 사용하는지 여부를 이 페이지에서 확인하도록 권고합니다 (https://www.milestonesys.com/community/business-partner-tools/device-packs/). 이미 레거시 팩이 설치되었는지 확인하려면 XProtect 시스템 폴더를 살펴 보십시오. 레거시 장치 팩을 다운로드해야 할 경우 다운로드 페이지로 이동합니다 (https://www.milestonesys.com/downloads/).

시스템이 **단일 컴퓨터** 시스템일 경우, 기존 설치 위에 새 소프트웨어를 설치할 수 있습니다.

Milestone Interconnect 또는 Milestone Federated Architecture 시스템에서는 중앙 사이트의 업그레이드를 시작하고 원격 사이트를 나중에 업그레이드해야 합니다.

분산 시스템에서, 다음 순서로 업그레이드하십시오.

1. 설치 프로그램의 **사용자 정의** 옵션으로 관리 서버 업그레이드(페이지 144의 시스템 설치 - 사용자 정의 옵션 참조).
    1. 구성 요소를 선택하는 마법사 페이지에서 모든 관리 서버 구성 요소가 사전 선택되어 있습니다.
    2. SQL Server 및 데이터베이스를 지정합니다. 이미 사용 중인 SQL Server 데이터베이스 유지 여부 및 데이터베이스 내 기존 데이터 유지 여부를 결정합니다.

    > 설치를 시작하면 장애 조치 레코딩 서버 기능을 잃게 됩니다(페이지 37의 장애 조치 레코딩 서버(설명됨) 참조).

    > 관리 서버 상의 암호화 기능을 활성화하는 경우 레코딩 서버는 관리 서버가 완전히 업그레이드 될 때까지 그리고 관리 서버 암호화를 활성화하기까지 오프라인 상태가 됩니다(페이지 134의 보안 통신(설명됨) 참조).

2. 장애 조치 레코딩 서버를 업그레이드합니다. 관리 서버의 다운로드 웹 페이지에서 Download Manager 에 의해 제어됨), Recording Server 을(를) 설치합니다.

    > 장애 조치 레코딩 서버에서 암호화를 활성화할 계획이고 장애 조치 기능을 유지하고자 할 경우, 장애 조치 레코딩 서버를 암호화 없이 업그레이드하고, 레코딩 서버를 업그레이드한 후에 암호화를 활성화합니다.

    이 시점에서 장애 조치 서버 기능이 다시 작동합니다.

3. 클라이언트에 대해 레코딩 서버 또는 장애 조치 레코딩 서버에서 암호화를 활성화할 계획이고 클라이언트가 업그레이드 중 데이터를 검색할 수 있는 것이 중요할 경우, 레코딩 서버를 업그레이드하기 전에 레코딩 서버로부터 데이터 스트림을 검색하는 모든 클라이언트와 서비스를 업그레이드하십시오. 다음의 클라이언트 및 서버는:
    - XProtect Smart Client
    - Management Client
    - Management Server
    - XProtect Mobile 서버
    - XProtect Event Server
    - DLNA Server Manager
    - Milestone Open Network Bridge
    - Milestone Interconnect 을(를) 통해 레코딩 서버로부터 데이터 스트림을 검색하는 사이트
    - 일부 MIP SDK 타사 통합

4. 레코딩 서버를 업그레이드합니다. 설치 마법사를 사용하여(페이지 151의 다음을 통해 레코딩 서버 설치: Download Manager 참조) 또는 자동으로 (페이지 156의 레코딩 서버 자동 설치see) 레코딩 서버를 설치할 수 있습니다. 자동 설치는 원격으로 수행할 수 있다는 장점이 있습니다.

   > 암호화를 활성화하였으나 선택된 서버 인증 인증서가 구동 중인 모든 관련 컴퓨터에서 신뢰받지 않은 경우, 연결이 끊어집니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 을(를) 참조하십시오.

시스템의 다른 사이트에 대해 이러한 단계를 계속합니다.

클러스터에서 업그레이드

클러스터를 업데이트하기 전에 데이터베이스를 백업하도록 하십시오.

1. 클러스터 내의 모든 관리 서버에서 Management Server 서비스를 중지합니다.
2. 클러스터 내의 모든 서버에서 관리 서버를 제거합니다.
3. 클러스터 내 설치 항목에서 설명한 대로 클러스터에 다중 관리 서버 설치를 위한 절차를 사용합니다. 페이지 163의 클러스터 내 설치를 참조하십시오.

> 설치 시 현재 시스템 구성을 저장하는 기존 SQL Server 및 기존 SQL Server 데이터베이스를 다시 사용해야 합니다. 시스템 구성은 자동으로 업그레이드됩니다.

사용자 인터페이스 상세 내용

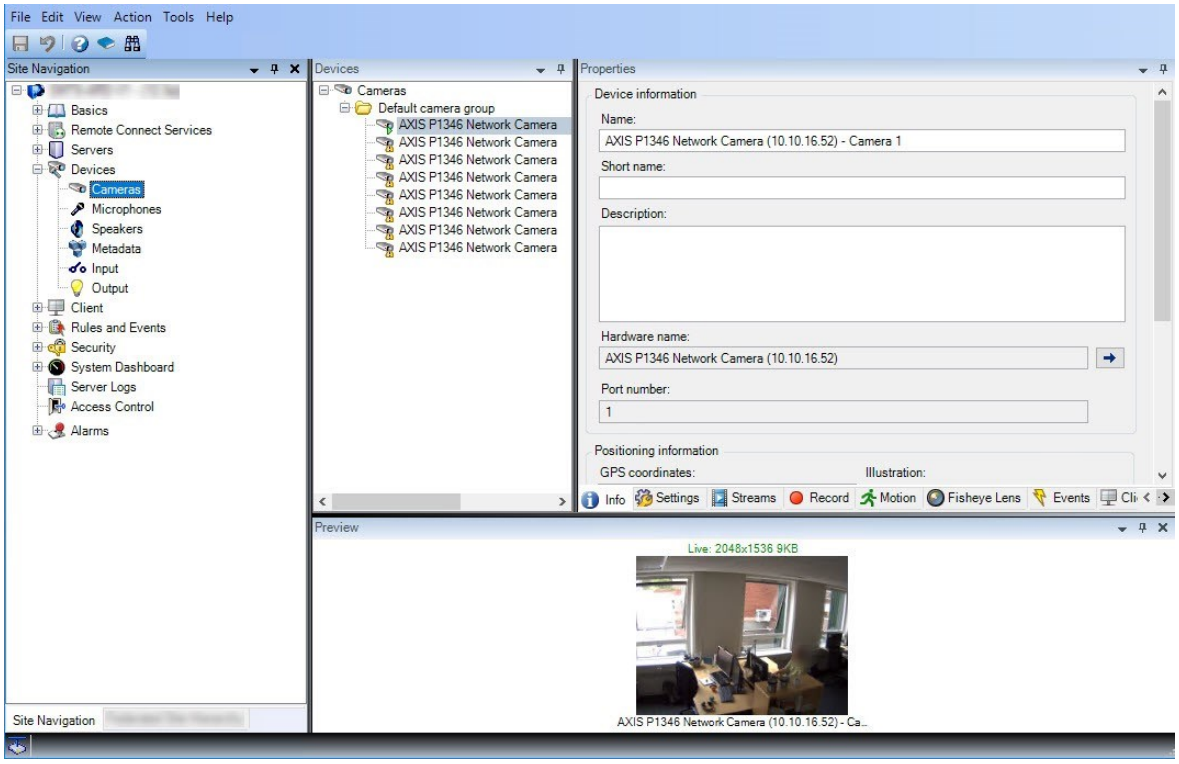
메인 창

Management Client 창은 여러 개의 창으로 나뉩니다. 창의 수와 레이아웃은 다음에 따라 다릅니다:

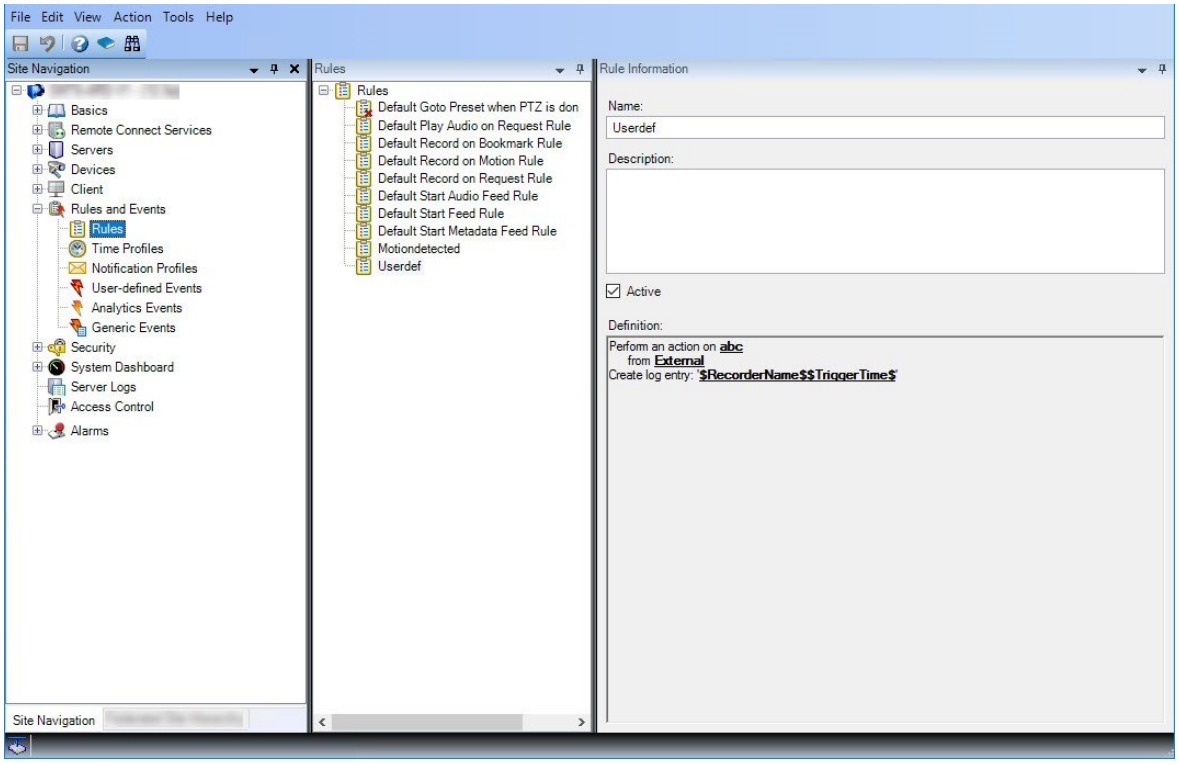
- 시스템 구성
- 작업
- 사용 가능한 기능

다음에는 일반적인 레이아웃에 대한 몇 가지 예가 나와 있습니다:

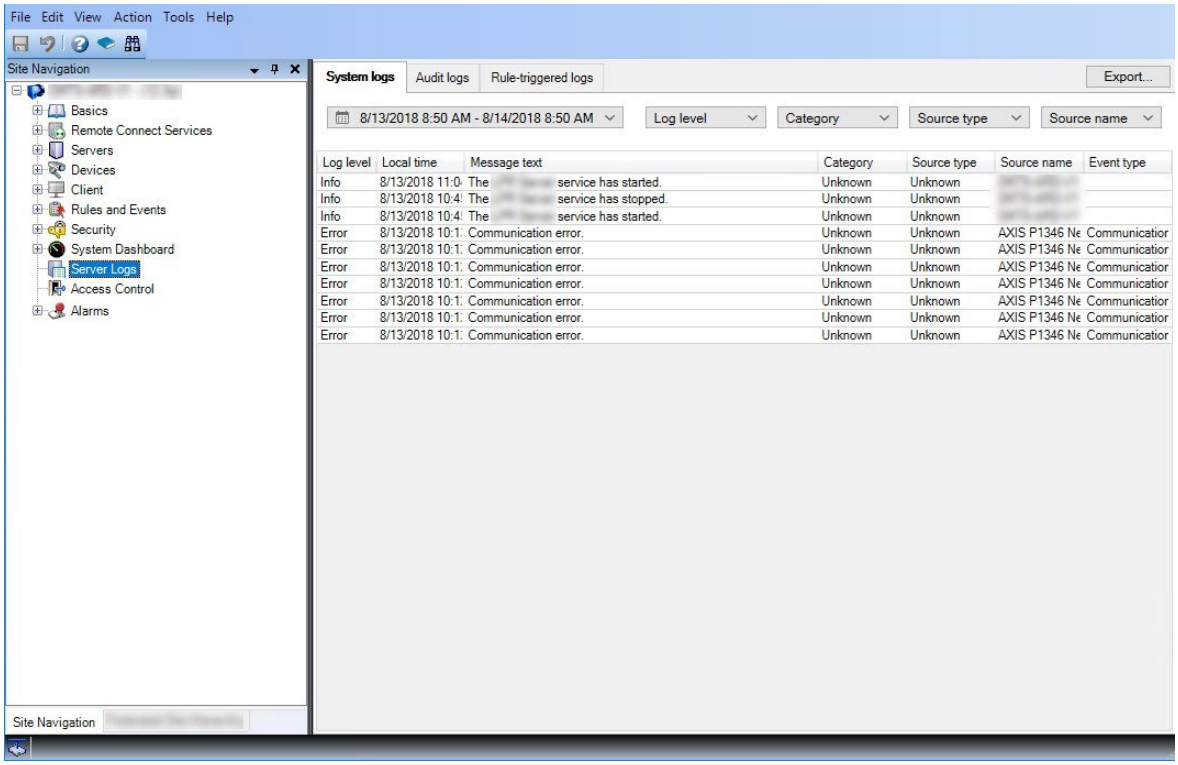
- 레코딩 서버와 장치를 사용하는 경우:



- 규칙, 시간 및 알림 프로파일, 사용자, 역할을 사용하는 경우:

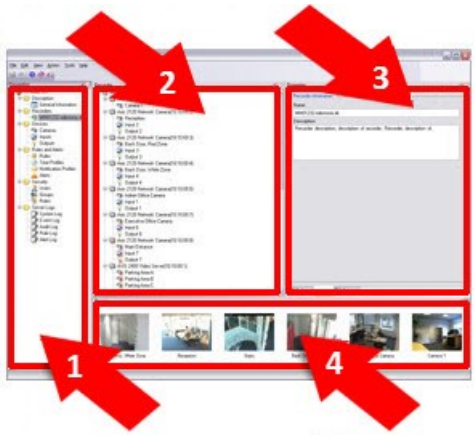


- 로그를 보는 경우:



창 레이아웃

이 삽화는 일반적인 창 레이아웃을 나타낸 것입니다. 레이아웃은 원하는 대로 사용자 정의할 수 있으므로 사용 중인 컴퓨터에서 다르게 나타날 수 있습니다.



1. 사이트 탐색 창 및 연합 사이트 계층 창
2. 개요 창
3. 속성 창
4. 미리보기 창

사이트 탐색 창

Management Client 의 주요 탐색 요소로, 로그인한 사이트의 이름, 설정 및 구성을 반영합니다. 사이트 이름은 창의 맨 위에 표시됩니다. 기능은 소프트웨어 기능을 반영한 카테고리로 그룹화됩니다.

사이트 탐색 창에서, 필요에 맞게 시스템을 구성하고 관리할 수 있습니다. 시스템이 단일 사이트 시스템이 아니라, 연합 사이트를 포함하고 있는 경우, **연합 사이트 계층** 창에서 이 사이트를 관리한다는 점을 유의하십시오.

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

연합 사이트 계층 창

상위/하위 사이트 계층 구조에 있는 모든 Milestone Federated Architecture 사이트를 표시하는 탐색 요소입니다.

사이트를 선택하고 로그인하면 해당 사이트의 Management Client 이(가) 실행됩니다. 로그인한 사이트는 항상 계층 구조의 맨 위에 위치합니다.

개요 창

사이트 탐색 창에서 선택한 요소의 개요를 제공합니다(예: 세부 목록). **개요** 창에서 요소를 선택하면 일반적으로 **속성** 창에 해당 속성이 표시됩니다. **개요** 창에서 요소를 마우스 오른쪽 단추로 클릭하면 관리 기능에 액세스할 수 있게 됩니다.

속성 창

개요 창에서 선택한 요소의 속성을 표시합니다. 다음과 같은 여러 개의 전용 탭에 속성이 표시됩니다.

미리보기 창

미리보기 창은 레코딩 서버와 장치를 사용할 때 나타납니다. 이 창은 선택한 카메라의 미리보기 이미지를 보여주거나 장치 상태에 대한 정보가 표시됩니다. 이 예제는 카메라 라이브 스트림의 해상도 및 데이터 속도에 대한 정보와 함께 카메라 미리보기 이미지를 보여줍니다.

기본적으로 카메라 미리보기 이미지에 표시된 정보는 라이브 스트림과 관련이 있습니다. 이는 미리보기 위에 녹색 텍스트로 표시됩니다. 대신 레코딩 스트림 정보를 원하는 경우(빨간색 텍스트), 메뉴에서 **표시를** > **뷰 레코딩 스트림** 선택합니다.

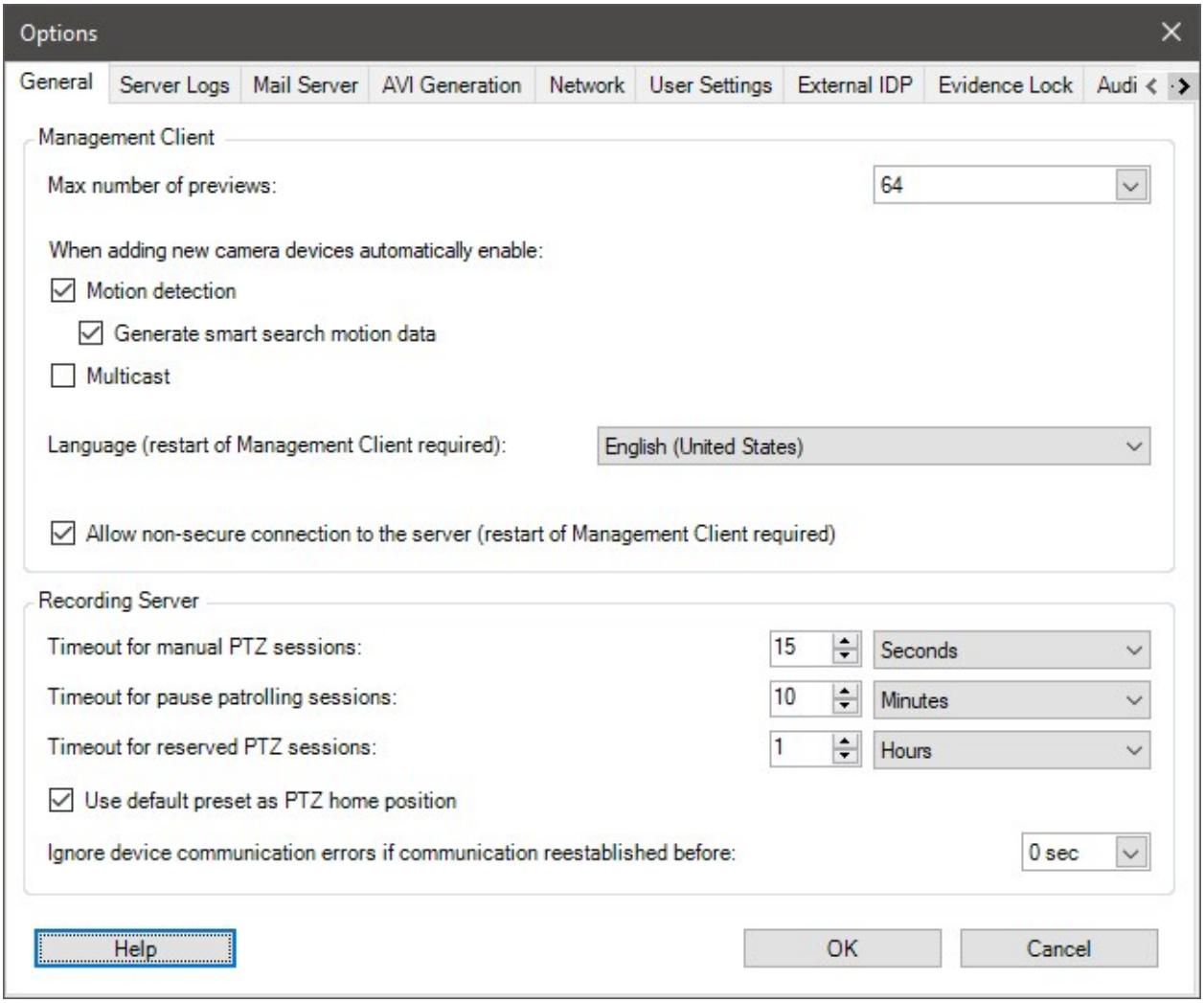
미리보기 창에 다수의 카메라에서 높은 프레임 속도로 미리보기 이미지가 표시되는 경우, 성능이 영향을 받을 수 있습니다. 미리보기 이미지 수와 해당 프레임 속도를 제어하려면 메뉴에서 **옵션** > **일반을** 선택합니다.

시스템 설정(옵션 대화 상자)

옵션 대화 상자에서 시스템의 일반적인 모양 및 기능과 관련된 다수의 설정을 지정할 수 있습니다.

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

대화 상자에 액세스하려면 도구 **옵션**을 선택합니다.



일반 탭(옵션)

일반 탭에서는 Management Client 및 레코딩 서버에 대한 일반 설정을 지정할 수 있습니다.

Management Client

이름	설명
최대 미리보기 수	**미리보기** 창에 표시되는 축소판 이미지의 최대 수를 선택합니다. 기본값은 64개 축소판 이미지입니다. 변경 내용을 적용하려면 메뉴에서 **동작** > **새로 고침** 을 선택합니다. 높은 프레임 속도와 함께 다수의 섬네일 이미지를 사용할 경우 시스템이 느려질 수 있습니다.
새 카메라 장치 추가를 자동으로 활성화할 경우: 모션 감지	**하드웨어 추가** 마법사를 사용하여 새 카메라를 시스템에 추가할 때 새 카메라에서 모션 감지를 활성화하려면 확인란을 선택합니다. 이 설정은 기존 카메라의 모션 감지 설정에 영향을 주지 않습니다. 카메라 장치의 **모션** 탭에서 카메라의 모션 감지를 활성화하거나 비활성화합니다.
새 카메라 장치 추가를 자동으로 활성화할 경우: 스마트 검색의 모션 데이터 생성	스마트 검색의 모션 데이터 생성 시에는 카메라에 대해 모션 감지가 활성화되어 있어야 합니다. **하드웨어 추가** 마법사를 사용하여 새 카메라를 시스템에 추가할 때 새 카메라에서 스마트 검색 모션 데이터 생성을 활성화하려면 확인란을 선택합니다. 이 설정은 기존 카메라의 모션 감지 설정에 영향을 주지 않습니다. 카메라 장치의 **모션** 탭에서 카메라의 스마트 검색 모션 데이터 생성을 활성화하거나 비활성화합니다.
새 카메라 장치 추가를 자동으로 활성화할 경우: 멀티캐스트	**하드웨어 추가** 마법사를 사용하여 새 카메라를 추가할 때 새 카메라에서 멀티캐스트를 활성화하려면 확인란을 선택합니다. 이 설정은 기존 카메라의 멀티캐스트 설정에 영향을 주지 않습니다. 카메라 장치의 **클라이언트** 탭에서 카메라의 라이브 멀티캐스팅을 활성화하거나 비활성화합니다.
언어	Management Client 의 언어를 선택합니다. 새 언어를 사용하려면 Management Client 을(를) 다시 시작합니다.
서버에 대한 비보안 연결을 허용합니	확인란을 선택하여 HTTP 프로코톨에 의한 비보안 서버 연결을 허용합니다.

이름	설명
다	(어떤 사용자에게도 비보안 서버 연결을 허용하도록 메시지를 표시하지 않습니다). 이 설정을 사용하려면 Management Client 을(를) 재시작합니다.

레코딩 서버

이름	설명
수동 PTZ 세션의 시간 제한	필요한 사용자 권한을 가진 클라이언트 사용자가 PTZ 카메라 순찰을 수동으로 중단할 수 있습니다. 수동 중단 후 일반 순찰이 다시 시작되기 전까지 경과해야 하는 시간을 선택합니다. 이 설정은 시스템의 모든 PTZ 카메라에 적용됩니다. 기본 설정은 15초입니다. **카메라에 개별 시간 제한을 적용하려면 카메라의** 프리셋 탭에서 이를 지정합니다.
순찰 세션 일시 중지의 시간 제한	충분한 PTZ 우선순위를 가진 클라이언트 사용자가 PTZ 카메라에 대한 순찰을 일시 중지할 수 있습니다. 일시 중지 후 일반 순찰이 다시 시작되기 전까지 경과해야 하는 시간을 선택합니다. 이 설정은 시스템의 모든 PTZ 카메라에 적용됩니다. 기본 설정은 10분입니다. **카메라에 개별 시간 제한을 적용하려면 카메라의** 프리셋 탭에서 이를 지정합니다.
예약된 PTZ 세션의 시간 제한	예약된 PTZ 세션에 대한 기본 시간 제한 기간을 설정합니다. 사용자가 예약된 PTZ 세션을 실행하면 세션이 수동으로 해제되거나 기간이 초과될 때까지 다른 사람이 PTZ 카메라를 사용할 수 없습니다. 기본 설정은 1시간입니다. **카메라에 개별 시간 제한을 적용하려면 카메라의** 프리셋 탭에서 이를 지정합니다.
기본 사전 설정을 PTZ 홈 위치로 사용	클라이언트에서 **홈** 버튼을 활성화할 때 PTZ 카메라의 홈 위치 대신 기본 사전 설정 위치를 사용하려면 이 확인란을 선택합니다. 카메라에 대해 기본 사전 설정 위치를 정의해야 합니다. 기본 사전 설정 위치가 정의되어 있지 않으면 클라이언트에서 **홈** 버튼을 활성화해도 아무 일도 일어나지 않습니다. 기본으로 이 확인란은 비워진 상태입니다. 기본 프리셋 위치를 지정하려면 페이지 226의 카메라의 기본 프리셋 위치를 기본으로 할당을 (를) 참조하십시오.
다음 이전에 통신이 재설정된 경우 장치 통신 오류 무시	시스템은 하드웨어와 서비스에 대한 모든 통신 오류를 기록하지만, 여기서 규칙 엔진이 **통신 오류** 이벤트를 트리거하기 전에 얼마나 오래 통신 오유가 존재해야 하는지 선택합니다.

서버 로그 탭(옵션)

서버 로그 탭에서는 시스템의 관리 서버 로그에 대한 설정을 지정할 수 있습니다.

자세한 정보는 사용자 활동, 이벤트, 동작 및 오류 식별 을 참조하십시오.

이름	설명
로그	구성할 로그 유형을 선택합니다. • 시스템 로그 • 감사 로그 • 규칙 트리거 로그
설정	로그를 비활성화 또는 활성화하고 보존 기간을 지정합니다. 로그 작성을 위해 2018 R2 이하의 구성 요소를 허용하십시오. 자세한 정보는 로그 작성을 위한 2018 R2 이하의 구성 요소 허용 을 참조하십시오. **시스템** 로그의 경우, 기록을 원하는 메시지 수준을 지정합니다. • 모두(정의되지 않은 메시지 포함) • 정보, 경고 및 오류 • 경고 및 오류 • 오류(기본 설정) **감사** 로그의 경우, 시스템이 XProtect Smart Client 의 모든 사용자 동작을 기록하기 원할 경우, 사용자 액세스 로그를 활성화합니다. 예를 들어, 내보내기, 출력 활성화, 라이브 또는 재생 중인 카메라 보기 등이 해당됩니다. 지정: • 재생 시퀀스의 길이 이는 사용자가 이 기간 내에서 재생하는 경우 시스템이 하나의 로그 항목만 생성한다는 것을 의미합니다. 기간 범위 밖에서 재생할 경우, 시스템이 새로운 로그 항목을 생성합니다. • 시스템이 로그 항목을 생성하기 전 사용자가 확인한 레코드(프레임)의 수

Mail Server 탭(옵션)

메일 서버 탭에서, 시스템의 메일 서버의 설정을 지정할 수 있습니다.
자세한 내용은 페이지의 알림 프로필(설명됨) 을 참조하십시오.

이름	설명
보낸 사람 이메일 주소	모든 알림 프로파일에 대해 이메일 알림의 보낸 사람으로 나타나게 할 이메일 주소를 입력합니다. 예: **sender@organization.org**.
메일 서버 주소	이메일 알림을 전송하는 SMTP 메일 서버 이름을 입력합니다. 예: **mailserver.organization.org**.
메일 서버 포트	메일 서버로의 연결에 사용된 TCP 포트. 기본 포트는 암호화되지 않은 연결에는 25, 암호화된 연결에는 일반적으로 465 또는 587 포트를 사용합니다.
서버에 대한 연결 암호화	관리 서버와 SMTP 메일 서버 간의 통신을 보호하고자 하는 경우 확인 상자를 선택합니다. TLS 시작 이메일 프로토콜 명령을 사용하여 연결이 보안되었습니다. 이 모드에서 암호화되지 않은 연결에서 세션이 시작되면 SSL을 사용한 보안 통신으로 전환하기 위해 SMTP 메일 서버 에서 관리 서버로 발급된 TLS 명령을 시작합니다.
서버에 로그인 필요	활성화된 경우 사용자가 메일 서버에 로그인하는 데 필요한 사용자 이름과 암호를 반드시 지정합니다.

AVI 생성 탭(옵션)

AVI 생성 탭에서 AVI 비디오 클립 파일 생성을 위한 압축 설정을 지정할 수 있습니다. 규칙 트리거 알림 프로파일에 의해 전송된 이메일 알림에 AVI 파일을 포함시키려는 경우 설정이 필요합니다.

또한 규칙에서 이메일 알림 트리거하기 를 참조하십시오.

이름	설명
압축 프로그램	적용할 코덱(압축/압축 해제 기술)을 선택합니다. 목록에 보다 많은 코덱을 포함시키려면 관리 서버에 해당 코덱을 설치하십시오. 모든 카메라가 모든 코덱을 지원하지는 않습니다.
압축 품질	(일부 코덱에 사용 불가). 슬라이더를 사용하여 코덱에서 수행할 압축 정도(**0** - **100**)를 선택합니다. **0**은 압축이 없음을 의미하며, 일반적으로 높은 이미지 품질과 대용량 파일 크기가 결과로 나타납니다. **100**은 최대 압축을 의미하며, 일반적으로 낮은 이미지 품질과 작은 파일 크기가 결과로 나타납니다.

이름	설명
	슬라이더를 사용할 수 없는 경우, 압축 품질이 전적으로 선택한 코덱에 의해 결정됩니다.
키프레임 주기	(일부 코덱에 사용 불가). 키프레임을 사용하려면 확인란을 선택하고 키프레임 사이에 필요한 프레임 수를 지정합니다. 키프레임은 지정한 간격에 저장되는 단일 프레임입니다. 키프레임에는 전체 카메라 뷰가 포함되지만, 다음 프레임에는 변화하는 픽셀만 포함됩니다. 따라서 파일의 크기를 상당히 줄일 수 있습니다. 확인란을 사용할 수 없거나 선택하지 않은 경우, 각 프레임에는 전체 카메라 뷰가 포함됩니다.
데이터 속도	(일부 코덱에 사용 불가). 특정 데이터 속도를 사용하려면 확인란을 선택하고 초당 킬로바이트 수를 지정합니다. 데이터 속도는 첨부된 AVI 파일의 크기를 지정합니다. 확인란을 사용할 수 없거나 선택하지 않은 경우, 데이터 속도가 선택한 코덱에 의해 결정됩니다.

네트워크 탭(옵션)

네트워크 탭에서 클라이언트가 인터넷을 통해 레코딩 서버에 연결될 경우 로컬 클라이언트의 IP 주소를 지정할 수 있습니다. 그러면 감시 시스템이 로컬 네트워크에서 나오는 주소를 인식합니다.

또한 시스템의 IP 버전을 지정할 수 있습니다: IPv4 또는 IPv6. 기본값은 IPv4입니다.

북마크 탭(옵션)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

북마크 탭에 XProtect Smart Client 에서 북마크에 대한 설정, ID 및 기능을 지정할 수 있습니다.

이름	설명
북마크 ID 접두어	XProtect Smart Client 의 사용자가 만든 모든 북마크의 접두어를 지정하십시오.
기본 북마크 시간	XProtect Smart Client 에 설정된 북마크의 기본 시작 및 종료 시간을 지정하십시오.

이름	설명
	이 설정은 다음과 일치해야 합니다: • 기본 북마크 규칙은 규칙(규칙 및 이벤트 노드) 를 참조하십시오. • 각 카메라에 대한 사전 버퍼 기간은 사전 버퍼 관리 를 참조하십시오.

역할에 대한 북마크 권한을 지정하려면 페이지 491의 장치 탭(역할)를 참조하십시오.

사용자 설정 탭(옵션)

사용자 설정 탭에서 사용자 기본 설정을 지정할 수 있습니다(예: 원격 레코딩이 활성화될 때 메시지가 표시되는 경우).

외부 IDP 탭(옵션)

Management Client의 **외부 IDP** 탭에서 외부 IDP를 추가 및 구성하고 외부 IDP에서 클레임을 등록할 수 있습니다.

이름	설명
활성화됨	외부 IDP는 기본적으로 활성화되어 있습니다.
이름	외부 IDP 이름. 여기에 입력한 이름이 클라이언트 로그인 창의 **인증** 항목에 표시됩니다.
인증 권한	외부 IDP의 URL
추가	외부 IDP를 추가하고 구성합니다. **추가**를 선택하는 경우, **외부 IDP** 대화 상자가 열려 구성에 대한 정보를 입력할 수 있습니다. 표 아래의 **외부 IDP 구성**을 참고하십시오.
편집	외부 IDP의 구성을 편집합니다.
제거	외부 IDP 구성을 제거합니다. 외부 IDP 구성을 삭제하면, 이 외부 IDP를 통해 인증된 사용자는 XProtect VMS에 로그인할 수 없게 됩니다. 외부 IDP를 다시 추가하면, 외부 IDP의 ID가 변경되었기 때문에 새로운 사용자가 로그인에 생성됩니다.

외부 IDP 구성

- 외부 IDP를 추가하려면, **외부 IDP** 섹션에서 **추가**를 선택하고 아래 표에 정보를 입력합니다.

이름	설명
이름	여기에 입력한 외부 IDP의 이름은 클라이언트 로그인 창의 **인증** 항목에 표시됩니다.
클라이언트 ID 및 클라이언트 암호	외부 IDP에서 획득해야 합니다. 외부 IDP와 안전하게 통신하려면 클라이언트 ID와 클라이언트 암호가 필요합니다.
콜백 경로	사용자의 로그인을 위한 인증 리디렉션 흐름에 대한 URL의 일부분. 사용자는 외부 IDP가 호스팅하는 로그인 페이지에서 로그인됩니다. 인증 프로세스가 완료되면 이 경로가 호출되고 사용자는 XProtect VMS로 리디렉션됩니다. 기본 값은 "/signin-oidc"입니다. 리디렉션 형식 콜백 경로의 URI은(는) 관리 서버 FQID와 /idp/ 및 외부 공급자에서 구성된 콜백 경로에 의해 구성됩니다. 예: • XProtect Smart Client 및 XProtect Management Client의 URI 형식 리디렉션: [스키마]://[관리 서버 주소]/idp/[콜백 경로] • XProtect Web Client 및 XProtect Mobile 클라이언트의 URI 형식 리디렉션: ["/index.html" 없이 Uri 리디렉션]/idp/[콜백 경로] 콜백 경로의 "idp" 부분은 대소문자를 구분하며 소문자로 입력해야 합니다.
로그인 프롬프트	사용자가 로그인 상태를 유지해야 하거나 사용자 확인이 필요한 경우 외부 IDP에 지정합니다. 외부 IDP에 따라, 인증에는 암호 확인이나 로그인 과정 전체가 포함될 수 있습니다.
사용자 이름 생성에 사용하기 위한 클레임	필요한 경우, VMS에서 자동으로 프로비저닝되는 사용자에 대한 고유한 사용자 이름 생성에 어떤 외부 IDP의 클레임을 사용해야 하는지 지정합니다. 클레임에 의해 생성되는 고유한 사용자 이름에 관한 자세한 내용은 외부 IDP 사용자에 대한 고유한 사용자 이름을 참고하십시오.
범주	필요에 따라, 외부 IDP에서 확보한 클레임 수를 제한할 범위를 사용하십시오. VMS에 대해 관련 있는 클레임이 특정 범위 내에 있음을 알고 있는 경우, 범위를 사용하여 외부 IDP에서 받는 클레임의 수를 제한할 수 있습니다.

클레임 등록

외부 IDP에서 클레임을 등록하면, VMS에서 클레임을 역할에 매핑하여 VMS에서의 사용자 권한을 결정할 수 있습니다. 자세한 내용은 외부 IDP에서 클레임 매핑을 참고하십시오.

- 외부 IDP에서 클레임을 등록하려면, **등록된 클레임** 섹션에서 **추가**를 선택하고 아래 표의 정보를 입력합니다.

이름	설명
외부 IDP	외부 IDP의 이름
클레임 이름	자유롭게 입력한 클레임 이름. 이름은 역할 선택 시 입력 가능합니다.
표시 이름	클레임의 표시된 이름.
대소문자 구분	클레임 값이 대/소문자를 구분하는지 표시합니다. 일반적으로 대/소문자를 구분하는 값의 예시: - GUID와 같은 ID의 문자 표현: F951B1F0-2FED-48F7-88D3-49EB5999C923 or OadFgrDesdFesff= 일반적으로 대/소문자를 구분하지 않는 값의 예시: - 이메일 주소 - 역할 이름 - 그룹 이름 .
추가, 편집, 제거	클레임을 등록하고 관리합니다. 외부 IDP 웹 사이트에서 클레임을 수정한 경우, 사용자는 XProtect 클라이언트에 다시 로그인을 해야 합니다. 예를 들어, 사용자 Bob이 운영자가 되어야 한다고 가정합니다. 그러고 나면 클레임이 외부 IDP 웹 사이트의 Bob에 추가되지만, Bob은 이미 XProtect에 로그인되어 있으므로, 변경 사항이 적용되게 하려면 Bob은 다시 로그인을 해야 합니다.

웹 클라이언트용 리디렉션 URI 추가

리디렉션 URI은(는) 로그인 성공 후 사용자가 리디렉션되는 위치입니다. 리디렉션 URI는 웹 클라이언트 주소와 정확히 일치해야 합니다. 예를 들어 **https://localhost:8082/index.html**에서 XProtect Web Client을(를) 열고 추가한 웹 클라이언트에 대한 URI 리디렉션이 **https://127.0.0.1:8082/index.html**이면 외부 IDP를 통해 로그인할 수 없게 됩니다.

이름	설명
URI	XProtect Web Client의 URI는 **https://[mobile server]:[port]/index.html** 형식입니다. 리디렉션 URI는 대소문자를 구분하지 않습니다.
추가, **편집**, **제거**	리디렉션 URI를 등록하고 유지 관리합니다. URI를 제거할 때 시스템이 작동하려면 최소한 하나의 URI 리디렉션을 유지해야 합니다.

고객 대시보드 탭(옵션)

CustomerDashboard(고객대시보드)탭에서,MilestoneCustomerDashboard을(를)활성화또는비활성화할수있습니다.

Customer Dashboard는 사용자의 시스템 설치에 관한 정보에 액세스할 수 있는 시스템 관리자나 다른 사람에게 가능한 기술적 문제(예: 카메라 고장) 등 사용자 시스템의 현재 상태에 대한 개요를 그래픽으로 표시해주는 온라인 모니터링 서비스입니다.

확인란을 선택하거나 선택 취소하여 언제든지 고객 대시보드 설정을 변경할 수 있습니다.

증거물 잠금 탭(옵션)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

증거물 잠금 탭에서 증거물 잠금 프로파일 및 클라이언트 사용자가 데이터 보호를 유지하기 위해 선택할 수 있는 기간을 정의하고 편집합니다.

이름	설명
증거물 잠금 프로파일	정의된 증거물 잠금 프로파일을 포함한 목록. 기존 증거물 잠금 프로파일을 추가하고 제거할 수 있습니다. 기본 증거물 잠금 프로파일을 제거할 수 없지만 해당 시간 옵션과 이름은 변경할 수 있습니다.
잠금 시간 옵션	클라이언트 사용자가 증거물을 잠그도록 선택할 수 있는 기간. 사용 가능한 시간 옵션에는 시간, 일, 주, 월, 년, 무기한 또는 사용자 정의가 있습니다.

역할에 대해 증거물 잠금 액세스 권한을 지정하려면 페이지 491의 장치 탭(역할)에서 역할 설정을 참조하십시오.

오디오 메시지 탭(옵션)

오디오 메시지 탭에서, 규칙에 의해 트리거되는 메시지 브로드캐스팅을 위해 사용된 오디오 메시지를 가진 파일을 업로드할 수 있습니다.

업로드된 파일의 최대 개수는 50개이며 각 파일에 할당된 최대 크기는 1 MB입니다.

이름	설명
이름	메시지 이름을 제공합니다. 메시지를 추가할 때 이름을 입력합니다. 시스템에 메시지를 업로드하려면 **추가**를 클릭합니다.
설명	메시지의 설명을 제공합니다. 메시지를 추가할 때 설명을 입력합니다. 목적 또는 실제 메시지를 기술하기 위해 설명 필드를 사용할 수 있습니다.
추가	시스템에 오디오 메시지를 업로드할 수 있습니다. 지원되는 형식은 다음의 표준 Windows 오디오 파일 형식입니다. • .wav • .wma • .flac
편집	이름과 설명을 수정하거나 실제 파일을 교체할 수 있습니다.
제거	목록에서 오디오 메시지를 삭제합니다.
재생	이 버튼을 클릭하여 Management Client 을(를) 실행하는 컴퓨터에서 오디오 메시지를 듣습니다.

오디오 메시지 재생을 트리거하는 규칙을 생성하려면 규칙 추가 를 참조하십시오.

규칙에서 사용할 수 있는 동작 일반에 관한 자세한 내용을 알아보려면 동작 및 중지 동작 을 참조하십시오.

사생활 보호 설정 탭

사생활 보호 설정 탭에서 XProtect Mobile Server, XProtect Mobile 클라이언트, XProtect Web Client 및 XProtect Smart Client에서의 사용량 데이터 수집을 활성화 또는 비활성화할 수 있습니다. 그리고 나서 **확인** 을 클릭하십시오.

사용량 데이터 수집을 활성화함으로써 귀하는 미국에서 데이터 처리를 배제할 수 없는 제3자 제공업체로서 Google의 Milestone Systems 기술 사용에 동의하는 것입니다. 데이터 보호 및 사용량 데이터 수집에 관한 자세한 내용은 GDPR 개인정보 보호지침을 참조하십시오.

액세스 제어 설정 탭(옵션)

XProtect Access 을(를) 사용하려면 이 기능에 액세스할 수 있는 기본 라이선스를 구입해야 합니다.

이름	설명
개발 속성 패널 표시	선택하면, **액세스 제어** > **일반 설정** 에 대한 추가 개발자 정보가 나타납니다. 이 설정은 액세스 제어 시스템 통합을 담당하는 개발자만 사용하도록 고안되었습니다.

분석 이벤트 탭(옵션)

분석 이벤트 탭에서 분석 이벤트 기능을 활성화하고 지정할 수 있습니다.

이름	설명
활성화	분석 이벤트의 사용 여부를 지정합니다. 기본적으로 이 기능은 비활성화되어 있습니다.
포트	이 기능에 사용되는 포트를 지정합니다. 기본 포트는 9090입니다. 관련 VCA 도구 제공자도 이 포트 번호를 사용해야 합니다. 포트 번호를 변경할 경우, 제공업체의 포트 번호도 변경하도록 하십시오.
모든 네트워크 주소 또는 **지정된 네트워크 주소**	모든 IP 주소/호스트 이름의 이벤트가 허용되는지, **주소 목록** (아래 참조)에 지정된 IP 주소/호스트 이름의 이벤트만 허용되는지 지정합니다.
주소 목록	신뢰할 수 있는 IP 주소/호스트 이름 목록을 지정합니다. 이 목록은 수신 데이터를 필터링하므로 특정 IP 주소/호스트 이름의 이벤트만이 허용됩니다. 도메인 이름 시스템(DNS), IPv4 및 IPv6 주소 형식을 모두 사용할 수 있습니다.

이름	설명
	IP 주소나 호스트 이름을 수동으로 입력하거나 외부 주소 목록을 가져와 목록에 주소를 추가할 수 있습니다. • **수동 입력**: 주소 목록에 IP 주소/호스트 이름을 입력합니다. 필요한 각 주소에 대해 작업을 반복합니다 • **가져오기**: 외부 주소 목록을 검색하려면 **가져오기** 를 클릭합니다. 외부 목록은 .txt 파일이어야 하며, IP 주소나 호스트 이름은 별도의 줄에 있어야 합니다.

알람 및 이벤트 탭(옵션)

알람 및 이벤트 탭에서 알람, 이벤트 및 로그에 대한 설정을 지정할 수 있습니다. 또한 이러한 설정과 관련해서는 페이지 119의 데이터베이스 크기 제한를 참조하십시오.

이름	설명
다음 기간 동안 닫힌 알람 유지	데이터베이스에서 알람을 **닫힘** 상태로 보관할 일 수를 지정합니다. **0** 으로 값을 설정할 경우, 알람이 닫힌 후 삭제됩니다. 알람에는 항상 타임스탬프가 있습니다. 알람이 카메라에 의해 트리거된 경우, 타임스탬프에는 알람 시간으로부터의 이미지가 포함됩니다. 알람 정보 자체는 이벤트 서버에 저장되는 반면, 첨부된 이미지에 해당하는 비디오 레코딩은 해당 감시 시스템 서버에 저장됩니다. 알람의 이미지를 보려면 최소한 이벤트 서버에 알람을 보관하려는 시간 동안 비디오 레코딩을 유지해야 합니다.
다음 기간 동안 다른 모든 알람 유지	알람을 **신규**, **진행 중** 또는 **보류** 상태로 보관할 일 수를 지정합니다. 값을 0으로 설정하면 알람이 시스템에 표시되지만 보관되지 않습니다.

이름	설명
	알람에는 항상 타임스탬프가 있습니다. 알람이 카메라에 의해 트리거된 경우, 타임스탬프에는 알람 시간으로부터의 이미지가 포함됩니다. 알람 정보 자체는 이벤트 서버에 저장되는 반면, 첨부된 이미지에 해당하는 비디오 레코딩은 해당 감시 시스템 서버에 저장됩니다. 알람의 이미지를 보려면 최소한 이벤트 서버에 알람을 보관하려는 시간 동안 비디오 레코딩을 유지해야 합니다.
다음 기간 동안 로그 유지	이벤트 서버 로그를 보관할 일 수를 지정합니다. 장기간 동안 로그를 보관할 경우, 이벤트 서버가 설치된 장비에 충분한 디스크 공간이 있는지 확인하십시오.
상세 로깅 활성화	이벤트 서버 통신에 대한 보다 자세한 로그를 보관하려면 확인란을 선택합니다. **로그 보관 기간** 필드에서 지정된 일 수 동안 보관됩니다.
이벤트 유형	데이터베이스에 이벤트를 보관할 일 수를 지정합니다. 두 가지 방법으로 할 수 있습니다. • 전체 이벤트 그룹에 대한 보존 시간을 지정할 수 있습니다. **그룹 추종** 값을 가진 이벤트 유형은 이벤트 그룹의 값을 상속합니다 • 이벤트 그룹에 대한 값을 설정하더라도, 개별 이벤트 그룹에 대한 보존 시간을 지정할 수 있습니다. 값을 **0**으로 설정하면 이벤트가 데이터베이스에 보관되지 않습니다. 외부 이벤트(사용자 정의 이벤트, 일반 이벤트 및 입력 이벤트)는 기본값인 **0**으로 설정되며 이 값을 변경할 수 없습니다. 이러한 유형의 이벤트가 상당히 자주 발생하므로 데이터베이스에 보관하면 성능 문제가 야기될 수 있기 때문입니다.

일반 이벤트 탭(옵션)

일반 이벤트 탭에서 일반 이벤트와 데이터 소스 관련 설정을 지정할 수 있습니다.

실제 일반 이벤트 구성 방법에 대한 자세한 내용은 일반 이벤트 (설명됨) 를 참조하십시오.

이름	설명
데이터 소스	두 가지 기본 데이터 소스 중에서 선택하고 사용자 정의 데이터 소스를 정의할 수 있습니다. 선택할 항목은 인터페이스를 연결할 타사 프로그램 및/또는 하드웨어나 소프트웨어에 따라 다릅니다: **호환 가능**: 출하 시 기본 설정이 활성화되고, 모든 바이트, TCP 및 UDP, IPv4 전용, 1234 포트, 구분 기호 없음, 로컬 호스트 전용, 현재 코드 페이지 인코딩(ANSI)을 반영합니다. **국제**: 출하 시 기본 설정이 활성화되고, 통계 전용, TCP 전용, IPv4+6, 1235 포트, 구분 기호로서 <CR><LF>, 로컬 호스트 전용, UTF-8 인코딩을 반영합니다. (<CR><LF> = 13,10). [데이터 소스 A] [데이터 소스 B] 등.
새로 만들기	새 데이터 소스를 정의하려면 클릭합니다.
이름	데이터 소스의 이름.
활성화됨	데이터 소스는 기본적으로 비활성화되어 있습니다. 데이터 소스를 활성화하려면 확인란을 선택하십시오.
재설정	선택한 데이터 소스의 모든 설정을 재설정하려면 클릭합니다. **이름** 필드에 입력한 이름은 그대로 유지됩니다.
포트	데이터 소스의 포트 번호.
프로토콜 유형 선택기	일반 이벤트를 검색하기 위해 시스템이 수신하고 분석하는 프로토콜입니다: **모두**: UDP 뿐만 아니라 TCP. **TCP**: TCP만 가능. **UDP**: UDP만 가능. 일반 이벤트에 사용되는 TCP 및 UDP 패키지에는 @, #, +, ~ 등의 특수 문자가 포함될 수 있습니다.
IP 유형 선택기	선택 가능한 IP 주소 유형: IPv4, IPv6 또는 둘 다.
구분 기호 바이트	개별 일반 이벤트 레코딩을 분리하는 데 사용되는 구분 기호 바이트를 선택합니다. 데이터 소스 유형 **국제** 의 기본값(앞에 나온 **데이터 소스** 참조)은 **13,10** 입니다. (13,10 = <CR><IF>).

이름	설명
에코 유형 선택기	사용 가능한 에코 반환 형식: • **에코 통계**: 다음 형식을 에코합니다. **[X],[Y],[Z],[일반 이벤트 이름]** **[X]** = 요청 번호. **[Y]** = 문자 수. **[Z]** = 일반 이벤트와 일치하는 수. **[일반 이벤트 이름]** = **이름** 필드에 입력된 이름. • **모든 바이트 에코**: 모든 바이트를 에코합니다 • **에코 없음**: 모든 에코를 억제합니다
인코딩 유형 선택기	기본적으로 목록에는 가장 관련이 있는 옵션만 표시됩니다. 사용 가능한 모든 인코딩을 표시하려면 **모두 표시** 확인란을 선택하십시오.
허용된 외부 IPv4 주소	외부 이벤트를 관리하기 위해 관리 서버가 통신해야 하는 IP 주소를 지정합니다. 또한 데이터를 원치 않는 IP 주소를 제외시키는 데 이 항목을 사용할 수도 있습니다.
허용된 외부 IPv6 주소	외부 이벤트를 관리하기 위해 관리 서버가 통신해야 하는 IP 주소를 지정합니다. 또한 데이터를 원치 않는 IP 주소를 제외시키는 데 이 항목을 사용할 수도 있습니다.

구성 요소 메뉴

Management Client 메뉴

파일 메뉴

구성에 변경 내용을 저장하고 응용 프로그램을 종료할 수 있습니다. 또한 구성을 백업할 수 있습니다. 페이지 304의 시스템 구성 백업 및 복원(설명됨)를 참조하십시오.

편집 메뉴

변경 내용을 실행 취소할 수 있습니다.

뷰 메뉴

이름	설명
응용 프로그램 레이아웃 재설정	Management Client 에서 서로 다른 창의 레이아웃을 기본 설정으로 재설정합니다.
미리보기 창	레코딩 서버 및 장치를 사용할 때 **미리보기** 창을 켜고 끕니다.
레코딩 스트림 표시	기본적으로 **미리보기** 창에서 미리보기 이미지와 함께 표시되는 정보는 카메라의 라이브 스트림과 관련이 있습니다. 대신 레코딩 스트림에 관한 정보를 원할 경우, **레코딩 스트림 표시** 를 선택하십시오.
연합 사이트 계층	기본적으로 **연합 사이트 계층** 창은 활성화되어 있습니다.
사이트 탐색	기본적으로 **사이트 탐색** 창은 활성화되어 있습니다.

동작 메뉴

동작 메뉴의 내용은 **사이트 탐색** 창에서 선택한 요소에 따라 다릅니다. 선택 가능한 동작은 요소를 마우스 오른쪽 단추로 클릭할 때와 같습니다.

각 카메라에 대한 사전 버퍼 기간은 사전 버퍼 관리 를 참조하십시오.

이름	설명
새로 고침	항상 사용 가능하며 관리 서버로부터 요청된 정보를 다시 로드합니다.

도구 메뉴

이름	설명
등록된 서비스	등록된 서비스를 관리합니다. 페이지 329의 등록된 서비스 관리를 참조하십시오.
유효 역	선택한 사용자 또는 그룹의 모든 역할을 표시합니다.

이름	설명
할	
옵션	옵션 대화 상자를 열면 전체 시스템 설정을 정의하고 편집할 수 있습니다. 자세한 정보는 페이지 353의 시스템 설정(옵션 대화 상자)를 참조하십시오.

도움말 메뉴

Management Client 버전에 대한 도움말 시스템과 정보를 이용할 수 있습니다.

Server Configurator (유틸리티)

암호화 탭 속성

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

> 클러스터 환경에서는 클러스터 환경 내 모든 컴퓨터에 대한 인증서를 생성하기 전에 클러스터를 설정하여 구동하도록 해야 합니다. 그 후에 인증서를 설치하고 클러스터 내 모든 노드에 대해 Server Configurator을(를) 사용하여 등록을 수행할 수 있습니다. 자세한 정보는 XProtect VMS 설치 보호 방법에 관한 인증 안내서 를 참조합니다.

이름	설명	작업
서버 인증서	관리 서버와 데이터 수집기, 로그 서버, 레코딩 서버 간 쌍방향 연결을 암호화하는데 사용할 인증서를 선택합니다.	관리 서버로 및 관리서버로부터 암호화 활성화 레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화
이벤트 서버 및 확장	인증서를 선택하여 이벤트 서버 및 이벤트 서버와 통신하는 구성 요소(LPR Server 포함) 간에 쌍방향으로 암호화를 하는데 사용합니다.	페이지 280의 이벤트 서버 암호화 활성화
스트리밍 미디어 인증서	레코딩 서버와 모든 클라이언트 및 서버 간 통신과, 레코딩 서버에서 데이터 스트림을 검색하는 통합을 암호화하는데 사용할 인증서를 선택합니다.	클라이언트 및 서비스에 암호화 활성화

이름	설명	작업
모바일 스트리밍 미디어 인증서	모바일 서버와 모바일 서버에서 데이터 스트림을 검색하는 모바일 및 웹 클라이언트 간 통신을 암호화하는 데 사용할 인증서를 선택합니다.	모바일 서버 암호화를 활성화합니다

서버 등록

이름	설명	작업
관리 서버 주소	관리 서버의 주소는 보통 호스트 이름이나 해당 컴퓨터의 정규화된 도메인 이름(FQDN)을 포함합니다. 기본으로 이 주소는 관리 서버가 설치되어 있지 않은 XProtect VMS 에 있는 컴퓨터에서만 활성화됩니다. 경험에 따르면 관리 서버 주소는 관리 서버가 설치된 컴퓨터에서 변경될 수 없습니다. 하지만 예를 들어 장애 조치 설정에서 Server Configurator 을(를) 사용하는 경우, 관리 서버 컴퓨터에서 주소를 변경해야 할 수 있습니다. 이는 클러스터 장애 조치 환경 또는 그 외 장애 조치 설정 시나리오일 수 있습니다. • 관리 서버가 설치된 컴퓨터에서 **관리 서버 주소** 를 활성화하려면 펜( ) 기호를 클릭하십시오. ⚠ 관리 서버 주소를 업데이트하는 경우, 구성 요소가 설치된 컴퓨터 각각에 액세스하여 관리 서버 주소를 새 주소 정보로 업데이트해야 합니다.	관리 서버가 설치된 컴퓨터에서 관리 서버 주소 변경 적용에 관한 자세한 정보는 다음을 클릭하십시오. 관리 서버 컴퓨터의 호스트 이름 변경
등록	지정된 관리 서버가 설치된 컴퓨터에서 구동되는 서버를 등록합니다.	레코딩 서버 등록

언어 선택

이 탭을 사용하여 Server Configurator 에 대한 언어를 선택하십시오. Server Configurator 에 대한 언어 세트는 Management Client 에 대한 언어 세트에 상응합니다.

이름	설명
언어 선택	사용자 인터페이스의 언어를 선택합니다.

장애 조치 클러스터 환경에서 작업하는 경우, Server Configurator 에서 작업을 시작하기 전에 클러스터를 정지하는 것을 권장합니다. Server Configurator 이(가) 변경을 적용하는 동안 서비스를 멈추고 장애 조치 클러스터 환경이 이 작업을 중단시킬 수 있기 때문입니다.

트레이 아이콘 상태

표의 트레이 아이콘은 XProtect VMS의 서버에서 구동되는 서비스의 다양한 상태를 표시합니다. 아이콘은 서버가 설치된 컴퓨터에서 사용할 수 있습니다.

Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				실행 중 서버 서비스가 활성화되고 시작된 경우 나타남.

Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				Failover Recording Server 서비스가 구동되고 있는 경우 이 서비스는 표준 레코딩 서버 오류를 처리할 수 있습니다.
				중지됨 서버 서비스가 중단된 경우 나타납니다. Failover Recording Server 서비스가 중단된 경우, 표준 레코드 서버 오류를 처리할 수 없습니다.
				시작 서버 서비스가 시작 과정에 있을 때 나타납니다. 평소 상황에서 트레이 아이콘은 잠시 후 **실행 중** 으로 변경됩니다.
				중단 서버 서비스가 중단 과정에 있을 때 나타납니다. 평소 상황에서 트레이 아이콘은 잠시 후 **중단됨** 으로 변경됩니다.

Management Server Manager 트레이 아이콘	Recording Server Manager 트레이 아이콘	Event Server Manager 트레이 아이콘	Failover Recording Server Manager 트레이 아이콘	설명
				불확정적 상태 서버 서비스가 처음 로딩되고 첫 정보가 수신되기까지 나타나며, 평소 상황에서 트레이 아이콘은 **시작** 그리고 **실행 중** 으로 변경됩니다.
				오프라인 실행 중 보통 레코딩 서버 또는 장애 조치 레코딩 서버가 실행 중이나 Management Server 서비스는 실행되고 있지 않은 경우에 나타납니다.

트레이 아이콘의 서비스 시작 및 정지

알림 영역의 아이콘에서 마우스 오른쪽 버튼을 클릭하여 서비스를 시작 및 중지할 수 있는 트레이 아이콘을 엽니다.

- Management Server 서비스 시작 또는 중지
- Recording Server 서비스 시작 또는 중지

Management Server Manager(트레이 아이콘)

Management Server Manager 트레이 아이콘에서 메뉴 항목을 사용하여 Management Server Manager 에서 작업을 수행합니다.

이름	설명
Management Server 시작 및 **Management Server** 정지	적절한 메뉴 항목을 클릭하여 Management Server 서비스를 시작하거나 정지합니다. Management Server 서비스를 중지하면 Management Client 을(를) 사용할 수 없게 됩니다. 서비스 상태는 트레이 아이콘에 반영됩니다. 트레이 아이콘의 상태에 관한 자세한 정보는 서버 관리자 트레이 아이콘(설명됨) 을 참조하십시오.

이름	설명
상태 메시지 표시	타임 스탬프가 찍힌 상태 메시지 목록을 봅니다.
시스템 구성 암호 설정 변경	시스템 구성 암호를 할당하거나 변경합니다. 할당된 시스템 구성 암호를 제거하여 암호로 시스템 구성을 보호하지 않도록 선택합니다. 시스템 구성 암호 설정 변경
시스템 구성 암호 입력	암호를 입력합니다. 예를 들어 이는 암호 설정이 포함된 파일이 삭제되거나 망가진 경우에 적용됩니다. 자세한 정보는 시스템 구성 암호 설정 입력 을 참조하십시오.
장애 조치 관리 서버 구성	장애 조치 관리 서버용 구성 마법사를 실행하거나 **구성 관리** 페이지를 열어 기존 구성을 관리합니다. 장애 조치 클러스터에 관한 자세한 정보는 페이지 36의 XProtect Management Server Failover 를 참조하십시오.
Server Configurator	**Server Configurator**을(를) 열어 서버를 등록하고 암호화를 관리합니다. 암호화 관리에 관한 자세한 정보는 Server Configurator를 사용한 암호화 관리 를 참조하십시오.
라이선스 변경	관리 서버 컴퓨터에서 소프트웨어 라이선스 코드를 변경합니다. 예를 들어 새로운 라이선스 코드를 XProtect 시스템 업그레이드를 위해 입력해야 할 수 있습니다. 자세한 정보는 소프트웨어 라이선스 코드 변경 을 참조하십시오.
구성 복구	시스템 구성을 저장할 수 있는 곳에서 대화 상자를 엽니다. **복구** 를 클릭하기 전에 대화 상자의 정보를 반드시 읽으십시오. 자세한 정보는 수동 백업에서 시스템 구성 복원 을 참조하십시오.
공유 백업 폴더 선택	시스템 구성을 백업하기 전에 백업을 저장할 백업 폴더를 설정하십시오. 자세한 정보는 공유 백업 폴더 선택 을 참조하십시오.
SQL 주소 업데이트	마법사를 열어 SQL Server 주소를 변경합니다. 호스트 이름을 변경해야만 하는 경우, SQL Server 주소를 해당 변경 사항과 일치시켜야 할 수도 있습니다. 자세한 정보는 호스트 이름을 변경하면 SQL 서버 주소도 변경됩니다 항목을 참조하십시오.

기본 노드

라이선스 정보(기본 노드)

라이선스 정보 창에서 이 사이트 및 다른 모든 사이트 모두에서 동일한 소프트웨어 라이선스 파일을 공유하는 모든 라이선스, Milestone Care 구독을 계속 추적할 수 있으며 라이선스 활성화 방법을 결정할 수 있습니다.

라이선스 정보 창에서 이용 가능한 다양한 정보 및 기능에 관한 자세한 내용을 알아보려면, 페이지 114의 라이선스 정보 창를 참조하십시오.

사이트 정보(기본 노드)

많은 하위 사이트를 포함한 대규모 Milestone Federated Architecture 설정에서는 개요를 상실하기 쉬우며 각 하위 사이트의 관리자에 대한 연락처 정보를 찾기 힘들 수 있습니다.

이를 위해 각 하위 사이트에 추가 정보를 추가한 후 중앙 사이트의 관리자에게 이 정보 접근 권한을 허용할 수 있습니다.

다음 정보는 추가할 수 없습니다.

- 사이트 이름
- 주소/위치
- 관리자
- 추가 정보

원격 연결 서비스 노드

Axis One-click 카메라 연결(원격 연결 서비스 노드)

다음은 Axis One-Click 카메라 연결 속성입니다.

이름	설명
카메라 암호	입력/편집합니다. 카메라 구매 시 제공되었습니다. 추가 상세 내용은 카메라 사용설명서를 참조하거나 Axis 웹사이트(https://www.axis.com/)에서 확인하십시오.
카메라 사용자	**카메라 암호** 에 대한 상세 내용을 확인합니다.
설명	카메라에 대한 설명을 입력/편집합니다.
외부 주소	카메라가 연결되어 있는 ST 서버의 웹 주소를 입력/편집합니다.
내부 주소	레코딩 서버가 연결되어 있는 ST 서버의 웹 주소를 입력/편집합니다.
이름	필요한 경우, 항목의 이름을 편집합니다.
소유자 인증 키	**카메라 암호** 를 확인합니다.
암호 (디스패치 서버용)	암호를 입력합니다. 암호는 시스템 제공자에게서 받은 것과 일치해야 합니다.

이름	설명
암호 (ST 서버용)	암호를 입력합니다. Axis One-Click Connection 구성요소 설치 시 입력했던 암호와 동일해야 합니다.
Axis 디스패치 서비스에서 등록/등록취소	Axis 카메라와 Axis 디스패치 서비스를 함께 등록하기 원하는지 표시합니다. 설정 시 또는 나중에 할 수 있습니다.
시리얼 번호	제조업체가 지정한 하드웨어 일련 번호입니다. 항상 그렇지는 않지만 일련 번호가 간혹 MAC 주소와 동일한 경우가 있습니다.
자격 증명 사용	ST 서버를 설치하는 동안 자격 증명을 사용하려는 경우 체크 상자를 선택합니다.
사용자 이름 (디스패치 서버용)	사용자 이름을 입력하십시오. 사용자 이름은 시스템 제공자에게서 받은 것과 일치해야 합니다.
사용자 이름 (ST 서버용)	사용자 이름을 입력하십시오. **Axis One-Click Connection 구성요소** 설치 시 입력했던 암호와 동일해야 합니다.

서버 노드

서버(노드)

이 섹션은 레코딩 서버 및 장애 조치 레코딩 서버의 설치 및 구성 방법에 대해 설명합니다. 또한 시스템에 새 하드웨어 추가 및 다른 사이트와 상호 연결 방법에 대해 배웁니다.

- 페이지 377의 레코딩 서버(서버 노드)
- 페이지 390의 장애 조치 서버(서버 노드)

레코딩 서버(서버 노드)

시스템은 비디오 피드의 레코딩과 카메라 및 기타 기기와의 통신을 위해 레코딩 서버를 사용합니다. 감시 시스템은 일반적으로 여러 개의 레코딩 서버로 구성됩니다.

레코딩 서버는 Recording Server 소프트웨어를 설치하고 관리 서버와 통신하기 위해 구성한 컴퓨터입니다. **서버** 폴더를 확장한 다음 **레코딩 서버** 를 선택할 경우 **개요** 창에서 레코딩 서버를 볼 수 있습니다.

이 관리 서버 버전 이전의 레코딩 서버 버전과의 역호환성은 제한됩니다. 이전 버전으로 레코딩 서버의 레코딩에 여전히 액세스할 수 있지만, 구성을 변경하기 위해서는 이 관리 서버의 버전과 동일한 버전이어야 합니다. Milestone 에서는 시스템에 모든 레코딩 서버를 관리 서버와 동일한 버전으로 업그레이드 하도록 권장합니다.

레코딩 서버 설정 창

Recording Server Manager 트레이 아이콘을 우클릭하고 **설정 변경** 을 선택하면 다음을 지정할 수 있습니다.

이름	설명
주소	레코딩 서버가 연결되어야 하는 관리 서버의 IP 주소(예: 123.123.123.123) 또는 호스트 이름(예: ourserver). 이 정보는 레코딩 서버가 관리 서버와 통신할 수 있도록 하는 데 필요합니다.
포트	포트 번호는 관리 서버와 통신 시에 사용합니다. 기본값은 포트 9000입니다. 필요한 경우 이를 변경할 수 있습니다.
웹 서버 포트	포트 번호는 웹 서버 요청을 처리하는 데 사용합니다(예: PTZ 카메라 제어 명령과 XProtect Smart Client 에서 탐색 및 라이브 요청 처리를 위해). 기본값은 포트 7563입니다. 필요한 경우 이를 변경할 수 있습니다.
알림 서버 포트	레코딩 서버가 TCP 정보를 수신 시 사용하는 포트 번호(일부 장치는 이벤트 메시지 전송 시 TCP를 사용함). 기본값은 포트 5432입니다(기본적으로 비활성화되어 있음). 필요한 경우 이 순서를 변경할 수 있습니다.
SMTP 서버 포트	레코딩 서버가 SMTP(Simple Mail Transfer Protocol) 정보 수신 시 사용하는 포트 번호. SMTP는 서버 간 이메일 메시지를 전송하는 표준입니다. 일부 장치는 SMTP를 이벤트 메시지나 이미지를 메일로 감시 시스템 서버에 전송하는 데 사용합니다. 기본값은 포트 25이며 활성화/비활성화할 수 있습니다. 필요한 경우 포트 번호를 변경할 수 있습니다.
관리 서버에서 레코딩 서버로 연결 암	암호화를 활성화하고 목록의 서버 인증 인증서를 선택하기 전에 우선 관리 서버의 암호화를 활성화하고 레코딩 서버에서 관리 서버의 인증서를 신뢰하도록 해야 합니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 을(를) 참조하십시오.

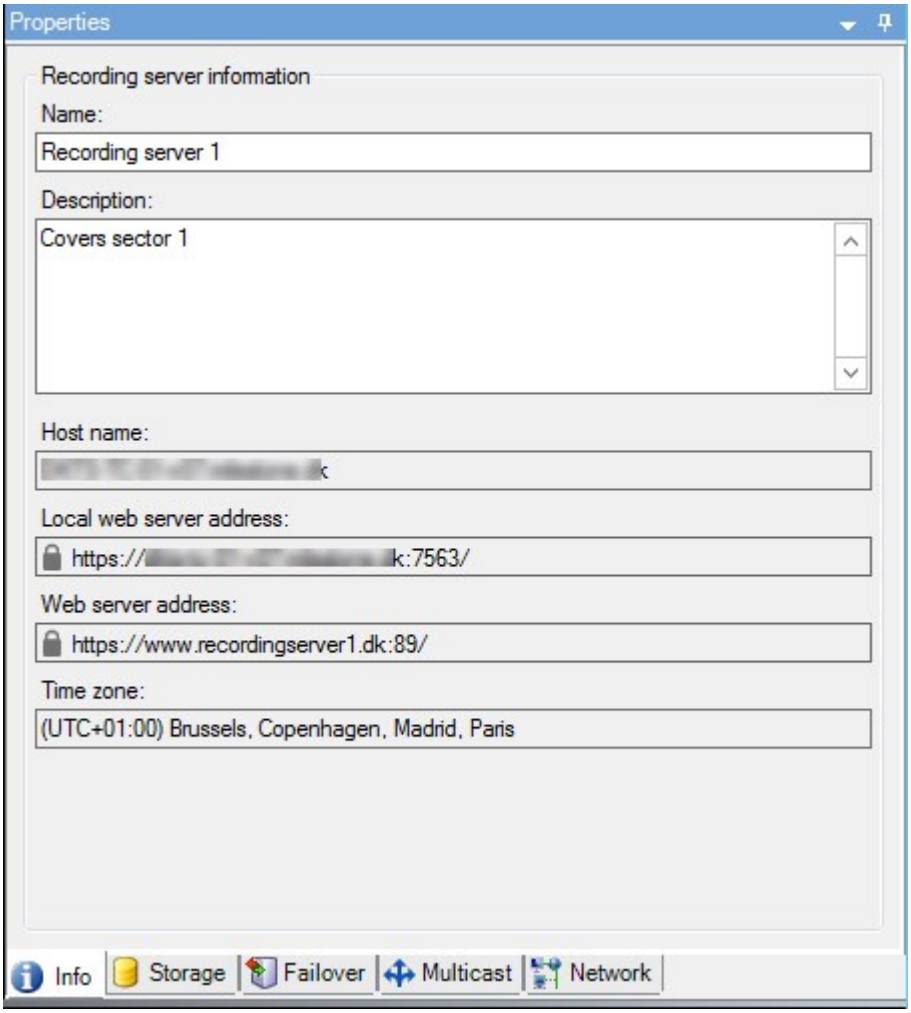
이름	설명
호화	
데이터를 스트리밍하는 클라이언트와 서버에 연결 암호화	암호화를 활성화하고 목록의 서버 인증 인증서를 선택하기 전에 레코딩 서버에서 데이터 스트림을 검색하는 서비스를 실행하는 모든 컴퓨터에서 해당 인증서를 신뢰하도록 해야 합니다. XProtect Smart Client 및 레코딩 서버에서 데이터 스트림을 검색하는 모든 서비스는 2019 R1 이후 버전으로 업그레이드해야 합니다. 2019 R1보다 오래된 버전의 MIP SDK 을(를) 사용하여 만든 일부 타사 솔루션은 업데이트가 필요할 수도 있습니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 을(를) 참조하십시오. 레코딩 서버가 암호화를 사용하는지 여부를 확인하려면 페이지 268의 클라이언트에 대한 암호화 상태 보기를 참조하십시오.
세부 정보	선택한 인증서에 관한 Windows Certificate Store 정보를 봅니다.

레코딩 서버 속송

정보 탭(레코딩 서버)

정보 탭에서, 레코딩 서버의 이름 및 설명을 확인하거나 편집할 수 있습니다.

호스트 이름 및 주소를 볼 수 있습니다. 웹 서버 주소 앞의 자물쇠 아이콘은 이 레코딩 서버로부터 데이터 스트림을 검색하는 클라이언트와 서버의 암호화된 통신을 나타냅니다.



이름	설명
이름	레코딩 서버에 대한 이름을 입력하도록 선택할 수 있습니다. 시스템과 클라이언트에 레코딩 서버가 나열될 때 이 이름이 사용됩니다. 이 이름은 고유할 필요가 없습니다. 레코딩 서버의 이름을 변경한 경우, Management Client 에서 전역으로 이름이 변경됩니다.
설명	시스템 내 다수의 목록에 나타나는 설명을 입력하도록 선택할 수 있습니다. 설명은 필수 항목이 아닙니다.
호스트 이름	레코딩 서버의 호스트 이름을 표시합니다.
로컬 웹	레코딩 서버 웹 주소의 로컬 주소를 표시합니다. 예를 들어 PTZ 카메라 제어 명령의 처리를 위해 그리고

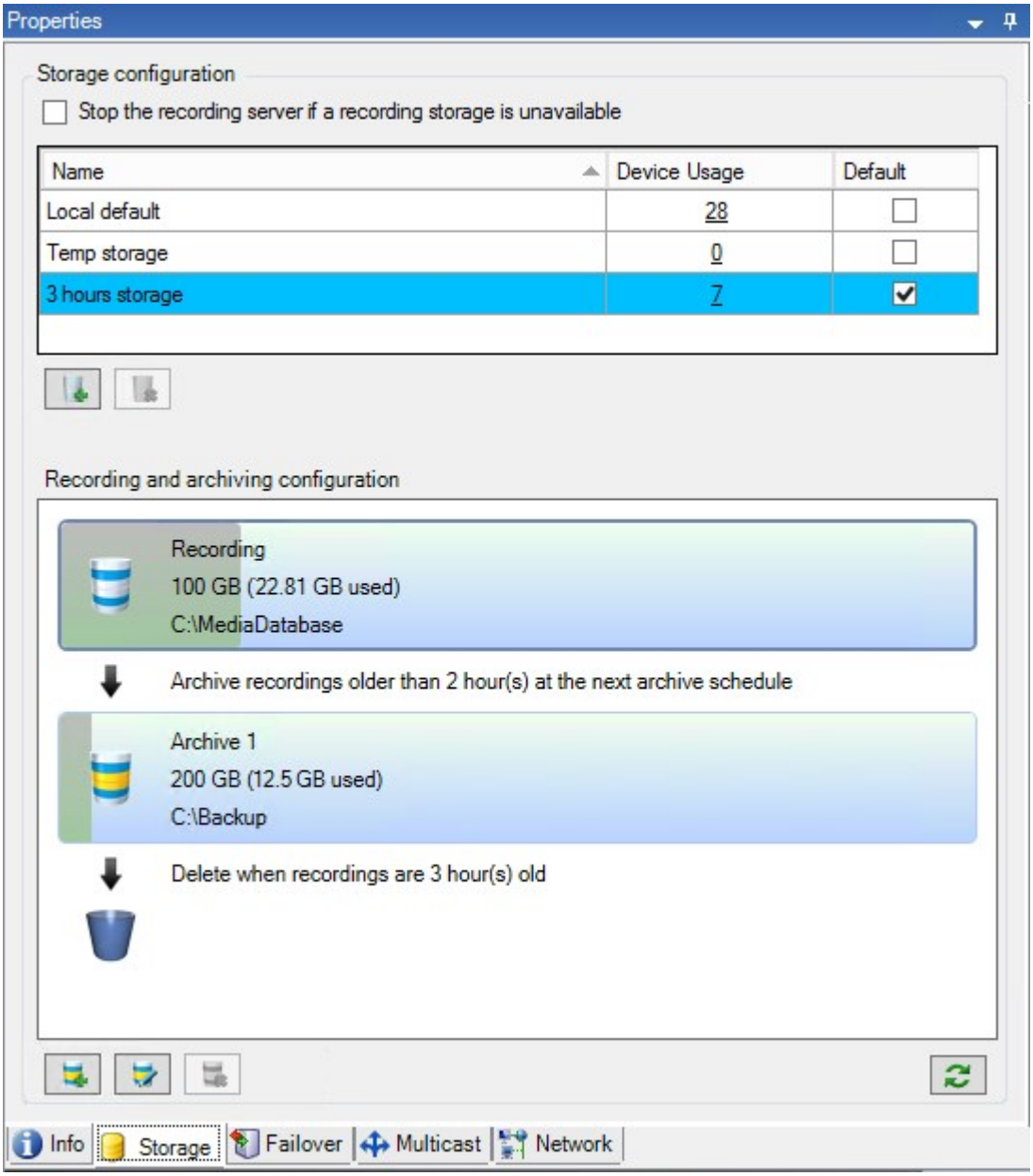
이름	설명
서버 주소	XProtect Smart Client 에서 브라우징 및 라이브 요청을 처리하기 위해 로컬 주소를 사용합니다. 주소에는 웹 서버 통신에 사용되는 포트 번호가 포함됩니다(일반적인 포트 7563). 레코딩 서버로부터 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화를 활성화할 경우 자물쇠 아이콘이 나타나고 주소는 **http** 대신에 **https** 를 포함하게 됩니다.
웹 서버 주소	인터넷 상에 레코딩 서버 웹 주소의 공용 주소를 표시합니다. 설치에서 방화벽이나 NAT 라우터를 이용하는 경우, 인터넷을 통해 감시 시스템에 액세스하는 클라이언트가 레코딩 서버에 연결할 수 있도록 방화벽 또는 NAT의 주소를 입력합니다. **네트워크** 탭에서 공용 주소 및 포트 번호를 지정합니다. 레코딩 서버로부터 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화를 활성화할 경우 자물쇠 아이콘이 나타나고 주소는 **http** 대신에 **https** 를 포함하게 됩니다.
시간대	레코딩 서버가 위치한 시간대를 표시합니다.

저장소 탭(레코딩 서버)

저장소 탭에서 선택한 레코딩 서버의 저장소를 설정, 관리 및 확인이 가능합니다.

레코딩 저장소 및 아카이브에 대해서는 수평 표시줄에서 현재 여유 공간을 보여줍니다. 레코딩 저장소를 사용할 수 없는 경우 레코딩 서버의 동작을 결정해 줄 수 있습니다. 이는 대부분 시스템에 장애 조치 서버가 있는 경우와 관련 있습니다.

증거물 잠금 을 사용하는 경우, 증거물 잠금 바닥글에 사용된 공간을 보여주는 빨간색 새로 선이 나타납니다.



저장소 및 녹화 설정 속성

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

저장소 및 녹화 설정 대화 상자에서 다음을 지정합니다.

이름	설명
이름	필요 시 저장소 이름을 바꿉니다. 이름은 반드시 고유해야 합니다.
경로	이 저장소에서 레코딩을 저장할 디렉토리의 경로를 지정합니다. 반드시 저장소가 레코딩 서버 컴퓨터에 위치할 필요는 없습니다. 디렉토리가 존재하지 않는 경우, 새로 만들 수 있습니다. 네트워크 드라이브는 UNC(범용 명명 규칙) 형식을 사용하여 지정해야 합니다. 예: `\\server\volume\directory\`.
보존 기간	삭제하거나 다음 아카이브로 이동(아카이브 설정에 따라 다름)하기 전에 레코딩이 아카이브에서 유지되는 시간을 지정합니다. 보존 기간은 항상 이전 아카이브 또는 기본 레코딩 데이터베이스의 보존 기간보다 길어야 합니다. 이는 아카이브에 대해 지정된 보존 일수에 프로세스에서 이전에 명시된 모든 보존 기간이 포함되기 때문입니다.
최대 크기	레코딩 데이터베이스에 저장하기 위한 레코딩 데이터의 최대 기가바이트 수를 선택합니다. 지정된 기가바이트 수를 초과하는 레코딩 데이터는 목록에서 첫 번째 아카이브(지정된 경우)로 자동 이동되거나 삭제됩니다. ⚠ 여유 공간이 5GB 미만일 경우, 시스템이 항상 데이터베이스에서 가장 오래된 데이터베이스를 자동 아카이브합니다(또는 다음 아카이브가 정의되지 않은 경우 삭제). 여유 공간이 1GB 미만일 경우, 데이터가 삭제됩니다. 데이터베이스에는 항상 250MB의 여유 공간이 필요합니다. 이 제한에 도달하면(데이터 삭제 속도가 느려지는 경우), 충분한 여유 공간을 확보하기 전까지는 데이터베이스에 어떤 데이터도 기록되지 않습니다. 데이터베이스의 실제 최대 크기는 지정한 기가바이트 크기에서 5GB를 뺀 값에 해당합니다.
서명	레코딩에 대한 디지털 서명을 활성화합니다. 이는 예컨대 재생 시 시스템이 내보낸 비디오가 수정되거나 변경되지 않았음을 확인한다는 의미입니다. 시스템은 디지털 서명을 위해 SHA-2 알고리즘을 사용합니다.
암호화	레코딩의 암호화 수준 선택: • 없음 • 약함(CPU 사용량 적음) • 강함(CPU 사용량 많음) 시스템은 암호화를 위해 AES-256 알고리즘을 사용합니다. **약하게** 를 선택할 경우 레코딩의 일부가 암호화됩니다. **강하게** 를 선택할 경우 전체 레코딩이 암호화됩니

이름	설명
	다. 암호화를 사용으로 설정할 경우, 아래에서 암호도 지정해야 합니다.
암호	사용자가 암호화된 데이터를 볼 수 있도록 암호를 입력합니다. Milestone 에서는 강한 암호를 사용하도록 권장합니다. 강한 암호는 사전에서 찾을 수 있거나 사용자의 이름 중 일부인 단어를 포함하지 않습니다. 여기에는 8자 이상의 영숫자, 대소문자 및 특수 문자가 포함됩니다.

아카이브 설정 속성

아카이브 설정 대화 상자에서 다음을 지정합니다:

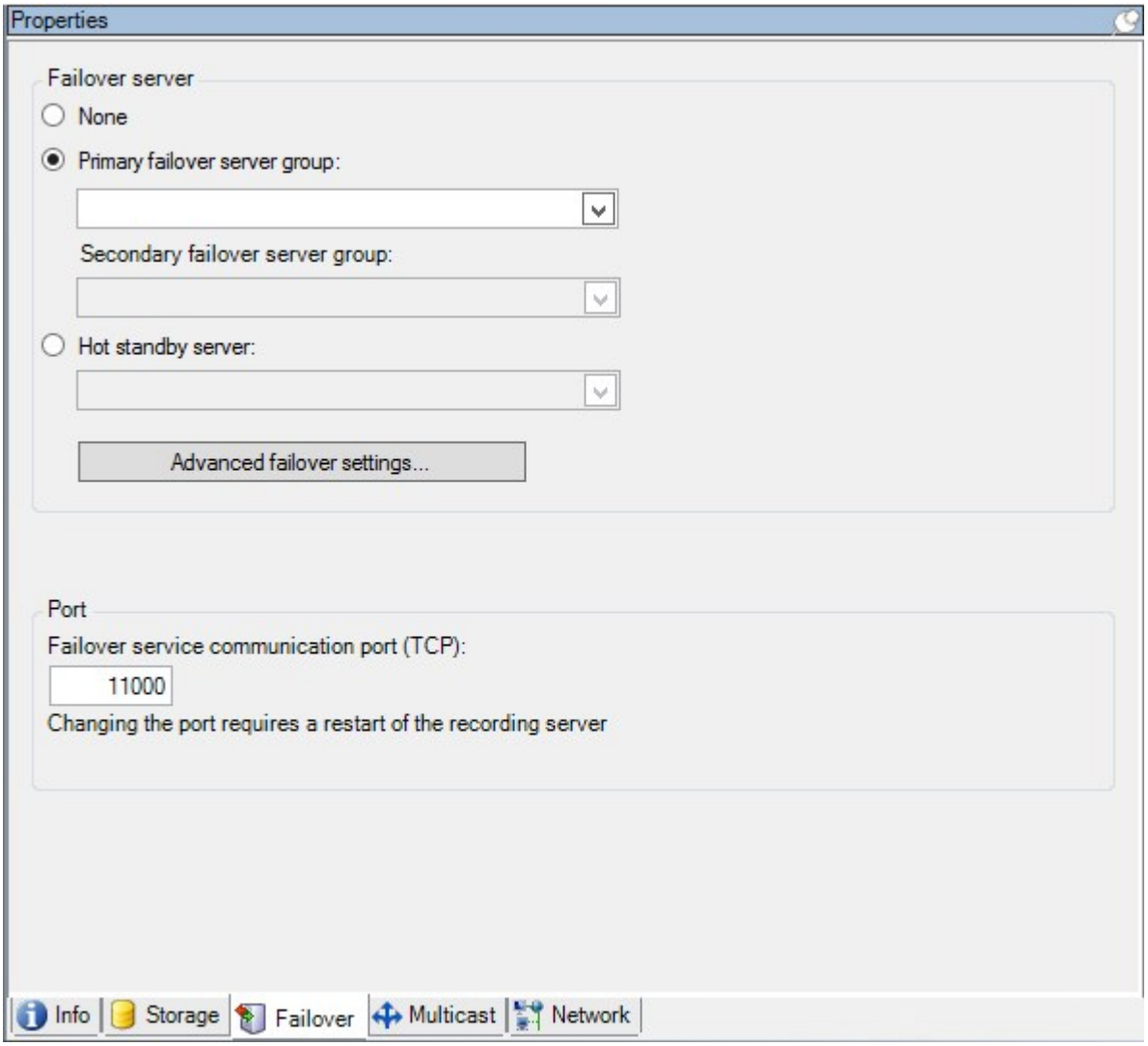
이름	설명
이름	필요 시 저장소 이름을 바꿉니다. 이름은 반드시 고유해야 합니다.
경로	이 저장소에서 레코딩을 저장할 디렉토리의 경로를 지정합니다. 반드시 저장소가 레코딩 서버 컴퓨터에 위치할 필요는 없습니다. 디렉토리가 존재하지 않는 경우, 새로 만들 수 있습니다. 네트워크 드라이브는 UNC(범용 명명 규칙) 형식을 사용하여 지정해야 합니다. 예: `\\server\volume\directory\`.
보존 기간	삭제하거나 다음 아카이브로 이동(아카이브 설정에 따라 다름)하기 전에 레코딩이 아카이브에서 유지되는 시간을 지정합니다. 보존 기간은 항상 이전 아카이브 또는 기본 레코딩 데이터베이스의 보존 기간보다 길어야 합니다. 이는 아카이브에 대해 지정된 보존 일수에 프로세스에서 이전에 명시된 모든 보존 기간이 포함되기 때문입니다.
최대 크기	레코딩 데이터베이스에 저장하기 위한 레코딩 데이터의 최대 기가바이트 수를 선택합니다. 지정된 기가바이트 수를 초과하는 레코딩 데이터는 목록에서 첫 번째 아카이브(지정된 경우)로 자동 이동되거나 삭제됩니다.

이름	설명
	여유 공간이 5GB 미만일 경우, 시스템이 항상 데이터베이스에서 가장 오래된 데이터베이스를 자동 아카이브합니다(또는 다음 아카이브가 정의되지 않은 경우 삭제). 여유 공간이 1GB 미만일 경우, 데이터가 삭제됩니다. 데이터베이스에는 항상 250MB의 여유 공간이 필요합니다. 이 제한에 도달하면(데이터 삭제 속도가 느려지는 경우), 충분한 여유 공간을 확보하기 전까지는 데이터베이스에 어떤 데이터도 기록되지 않습니다. 데이터베이스의 실제 최대 크기는 지정한 기가바이트 크기에서 5GB를 뺀 값에 해당합니다.
일정	아카이브 프로세스가 시작하는 간격을 나타내는 아카이브 일정을 지정합니다. 매우 자주(원칙적으로 일년 내내 매 시간마다) 또는 매우 드물게(예: 매 36개월의 첫째 월요일마다) 아카이브할 수 있습니다.
프레임 속도 줄이기	아카이브 시 FPS를 줄이려면 **프레임 속도 줄이기** 확인란을 선택하고 초당 프레임(FPS)을 설정합니다. 선택한 FPS 수로 프레임 속도를 줄이면 레코딩이 아카이브에서 더 적은 공간을 차지하게 되지만, 아카이브의 품질 또한 저하됩니다. MPEG-4/H.264/H.265로 설정하면 주요 프레임이 최소한으로 자동 축소됩니다. 0.1 = 10초당 1개 프레임.

장애 조치 탭(레코딩 서버)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

조직에서 장애 조치 레코딩 서버를 사용하는 경우, 장애 조치 탭을 사용하여 장애 조치 서버를 레코딩 서버에 할당합니다. 장애 조치 탭 속성을 참조하십시오.



장애 조치 레코딩 서버, 설치 및 설정, 장애 조치 그룹과 이의 설치에 관한 자세한 사항은 페이지 37의 장애 조치 레코딩 서버(설명됨)를 참조하십시오.

장애 조치 탭 속성

이름	설명
없음	장애 조치 레코딩 서버를 사용하지 않고 설정을 선택합니다.
1차 장애 조치 서버 그룹/2차 장애 조치	하나의 기본 및 하나의 보조(가능한 경우) 장애 조치 서버 그룹과 함께 일반 장애 조치 설정을 선택합니다.

이름	설명
서버 그룹	
상시 대기 서버	하나의 전용 레코딩 서버를 상시 대기 서버로 하여 상시 대기 설정을 선택합니다.
고급 장애 조치 설정	**고급 장애 조치 설정** 창을 엽니다. • **전체 지원**: 장치에 대한 완벽한 장애 조치 지원을 활성화합니다 • **라이브만**: 장치의 라이브 스트림에 대해서만 장애 조치 지원을 활성화합니다 • **비활성화**: 장치에 대한 장애 조치 지원을 비활성화합니다
장애 조치 서비스 통신 포트(TCP)	기본 포트 번호는 11000입니다. 레코딩 서버와 장애 조치 레코딩 서버 간의 통신에 이 포트를 사용합니다. 포트를 변경하려면 레코딩 서버를 **반드시** 실행하고 관리 서버에 **반드시** 연결 해야 합니다.

멀티캐스트 탭(레코딩 서버)

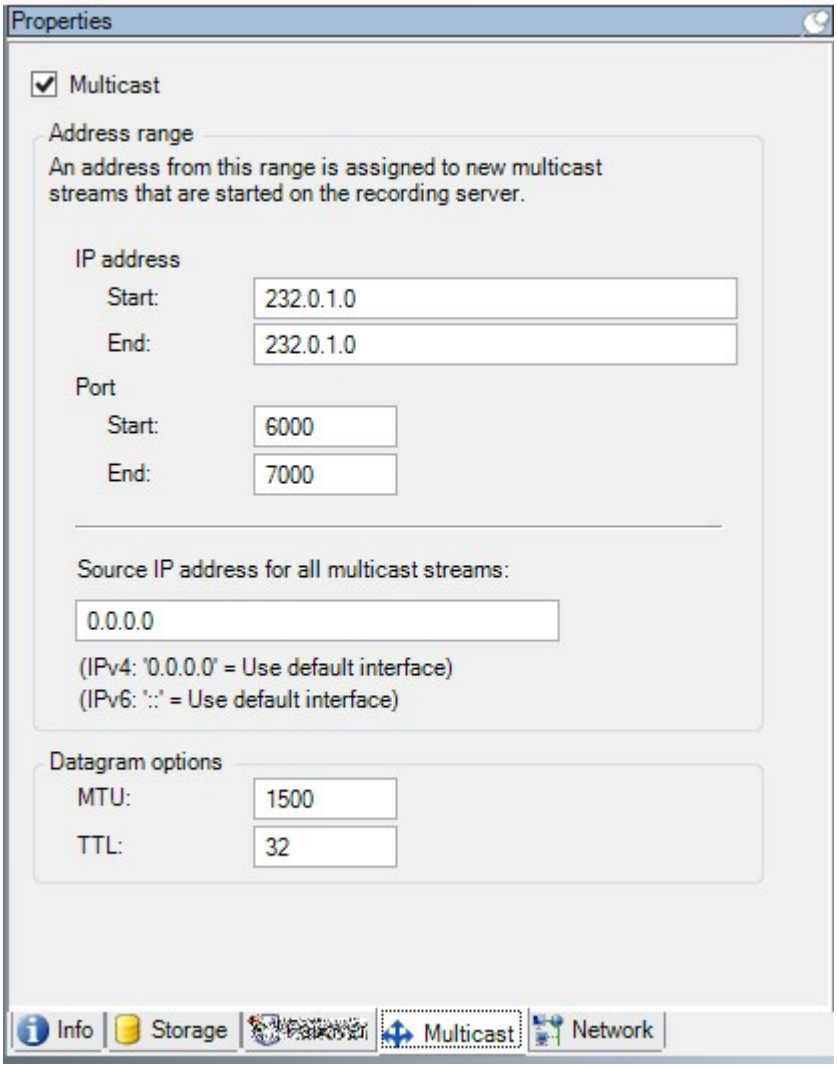
사용 중인 시스템은 레코딩 서버로부터 라이브 스트림의 멀티캐스팅을 지원합니다. 여러 XProtect Smart Client 사용자가 동일 카메라에서 라이브 비디오를 보려는 경우, 멀티캐스팅을 통해 시스템 리소스를 크게 절약할 수 있습니다. 멀티캐스팅은 특히 여러 클라이언트가 동일 카메라에서 라이브 비디오를 필요로 하는 경우 Matrix 기능을 사용할 때 유용합니다.

멀티캐스팅은 녹화된 비디오/오디오가 아닌 라이브 스트림에 대해서만 가능합니다.

레코딩 서버에 둘 이상의 인터페이스 카드가 있는 경우, 하나의 카드에서만 멀티캐스트를 사용할 수 있습니다. Management Client 을(를) 통해 사용할 카드를 지정할 수 있습니다.

장애 조치 서버를 사용하는 경우, 장애 조치 서버의 네트워크 인터페이스 카드 IP 주소도 지정하십시오(페이지 393의 멀티캐스트 탭(장애 조치 서버) 참조).

멀티캐스팅을 성공적으로 구현하려면 멀티캐스트 데이터 패킷을 필요한 수신자 그룹에게만 전달하도록 네트워크 장비를 구성해야 합니다. 그렇지 않으면 멀티캐스팅이 브로드캐스팅과 다르지 않으므로 네트워크 통신 속도가 현저히 저하될 수 있습니다.



IP 주소 범위 할당

선택한 레코딩 서버에서 멀티캐스트 스트림에 대한 주소로 할당할 범위를 지정합니다. 사용자가 레코딩 서버에서 멀티캐스트 비디오를 시청할 때 클라이언트가 이러한 주소에 연결합니다.

각각의 멀티캐스트 카메라 피드에 대해 IP 주소와 포트 조합이 고유해야 합니다(IPv4 예: 232.0.1.0:6000). 하나의 IP 주소와 여러 포트 또는 여러 IP 주소와 소수의 포트 조합을 사용할 수 있습니다. 기본적으로 시스템은 단일 IP 주소와 1000개 포트 범위를 제안하지만, 필요에 따라 이 설정을 변경할 수 있습니다.

멀티캐스팅을 위한 IP 주소는 IANA에 의한 동적 호스트 할당에 대해 정의된 범위 내에 속해야 합니다. IANA는 글로벌 IP 주소 할당을 감독하는 기관입니다.

이름	설명
IP 주소	**시작** 필드에 필수 범위 내의 첫 번째 IP 주소를 지정합니다. 그런 다음 **끝** 필드에 해당 위의 마지막 IP 주소를 지정합니다.
포트	**시작** 필드에 필수 범위 내의 첫 번째 포트 번호를 지정합니다. 그런 다음 **끝** 필드에 해당 범위 내의 마지막 포트 번호를 지정합니다.
모든 멀티캐스트 스트림의 소스 IP 주소	하나의 네트워크 인터페이스 카드에서만 멀티캐스팅할 수 있으므로, 이 필드는 사용 중인 레코딩 서버에 둘 이상의 네트워크 인터페이스 카드가 있거나 둘 이상의 IP 주소를 가진 네트워크 인터페이스 카드가 있을 경우에만 관련이 있습니다. 레코딩 서버의 기본 인터페이스를 사용하려면 값 0.0.0.0(IPv4) 또는 :: (IPv6)을 필드에 그대로 두십시오. 다른 네트워크 인터페이스 카드를 사용하거나 동일 네트워크 인터페이스 카드의 다른 IP 주소를 사용하려면 필요한 인터페이스의 IP 주소를 지정합니다. • IPv4: 224.0.0.0 ~ 239.255.255.255. • IPv6, IANA 웹사이트(https://www.iana.org/)에서 설명된 범주.

데이터그램 옵션 지정

멀티캐스팅을 통해 전송되는 데이터 패킷(데이터그램)의 설정을 지정합니다.

이름	설명
MTU	최대 전송 단위, 허용된 최대 물리적 데이터 패킷 크기(측정 단위: 바이트). 지정된 MTU 이상의 메시지는 전송 전에 더 작은 크기의 패킷으로 분할됩니다. 기본값은 1500이며, 이는 대부분의 Windows 컴퓨터와 이더넷 네트워크에서 기본값으로 사용됩니다.
TTL	TTL (Time To Live), 데이터 패킷이 삭제되거나 반환되기 전에 이동할 수 있는 허용된 최대 홉 수입니다. 홉은 두 네트워크 장치 사이의 지점으로, 보통 라우터에 해당합니다. 기본값은 128입니다.

네트워크 탭(레코딩 서버)

> ⚠ 공용 또는 신뢰되지 않은 네트워크상에서 XProtect Smart Client 을(를) 갖춘 VMS에 액세스하려면, Milestone 은(는) VPN을 통해 보안 연결을 사용할 것을 권장합니다. 이렇게 하면 XProtect Smart Client 및 VMS 서버 간의 통신이 보호되도록 할 수 있습니다.

네트워크 탭에서 레코딩 서버의 공용 IP 주소를 정의합니다.

공용 주소를 사용하는 이유?

클라이언트는 로컬 네트워크를 비롯한 인터넷에서 연결될 수 있고, 두 경우 모두에서 감시 시스템은 클라이언트가 레코딩 서버로부터 라이브 및 녹화된 비디오에 액세스할 수 있도록 적합한 주소를 제공해야 합니다:

- 클라이언트가 로컬로 연결되면, 감시 시스템이 로컬 주소와 포트 번호로 회신해야 합니다.
- 클라이언트가 인터넷에서 연결할 때, 감시 시스템은 레코딩 서버의 공용 주소로 회신해야 합니다. 이는 방화벽 또는 NAT(Network Address Translation) 라우터의 주소, 그리고 종종 다른 포트 번호이기도 합니다. 그러면 이 주소와 포트가 서버의 로컬 주소와 포트로 전달될 수 있습니다.

장애 조치 서버(서버 노드)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

장애 조치 레코딩 서버는 표준 레코딩 서버가 사용 불가능할 경우 전환되는 추가적인 레코딩 서버입니다. **수동 대기 서버** 또는 **상시 대기 서버** 와 같은 두 가지 모드로 장애 조치 레코딩 서버를 구성할 수 있습니다.

표준 레코딩 서버와 같은 장애 조치 레코딩 서버를 설치합니다(페이지 153의 다음을 통해 장애 조치 레코딩 서버 설치: Download Manager 참조). 장애 조치 레코딩 서버를 설치하면 Management Client 에서 볼 수 있습니다. Milestone 에서는 모든 장채 조치 레코딩 서버를 별도 컴퓨터에 설치하도록 권장합니다. 관리 서버의 정확한 IP 주소/호스트 이름과 함께 장애 조치 레코딩 서버를 구성해야 합니다. 장애 조치 서버 서비스에서 실행되는 사용자 계정에 대한 사용자 권한은 설치 과정 중에 제공됩니다. 이러한 권한은 다음과 같습니다:

- 장애 조치 레코딩 서버 시작 또는 중지를 위한 시작/중지 권한
- RecorderConfig.xml 파일을 읽거나 쓰기 위한 읽기 및 쓰기 접근 권한

인증이 암호화를 위해 선택된 경우 관리자는 반드시 읽기 접근 권한을 선택된 인증 개인 키에 대한 장애 조치 사용자에게 허용해야 합니다.

> 장애 조치 레코딩 서버가 암호화를 사용하는 레코딩 서버로부터 인계할 경우, Milestone 에서는 장애 조치 레코딩 서버도 암호화를 사용하도록 준비할 것을 권장합니다. 자세한 내용은 페이지 134의 보안 통신(설명됨) 및 페이지 153의 다음을 통해 장애 조치 레코딩 서버 설치: Download Manager를 참조하십시오.

장치 수준에서 원하는 장애 조치 지원 유형을 지정할 수 있습니다. 레코딩 서버의 각 장치에 대해 전체, 라이브만 또는 장애 조치 지원 없음을 선택합니다. 이를 통해 장애 조치 리소스의 우선순위를 손쉽게 정할 수 있습니다. 예를 들어 오디오를 제외한 비디오에 대해서만 장애 조치를 설정하거나 불필요한 카메라를 제외한 필수 카메라에 대해서만 장애 조치를 설정할 수 있습니다.

시스템이 장애 조치 모드에 있는 동안, 하드웨어를 대체하거나 이동하거나 레코딩 서버를 업데이트하거나 스토리지 설정이나 비디오 스트림 설정 같은 기기 구성을 변경할 수 없습니다.

수동 대기 장애 조치 레코딩 서버

수동 대기 장애 조치 레코딩 서버 설정에서, 여러 장애 조치 레코딩 서버를 하나의 장애 조치 그룹에 그룹화합니다. 전체 장애 조치 그룹은 사전 선택한 여러 레코딩 서버 중 하나를 사용할 수 없을 때 해당 서버의 작업을 전담하여 인수합니다. 필요한 만큼 많은 그룹을 생성할 수 있습니다(페이지 195의 수동 대기를 위한 장애 조치 레코딩 서버 그룹 참조).

그룹화는 명확한 이점이 있습니다: 나중에 레코딩 서버의 작업을 인수할 장애 조치 레코딩 서버를 지정할 때 장애 조치 레코딩 서버 그룹을 선택합니다. 선택한 그룹에 둘 이상의 장애 조치 레코딩 서버가 포함된 경우, 한 레코딩 서버를 사용할 수 없을 때 둘 이상의 장애 조치 레코딩 서버가 해당 작업을 인수할 수 있는 확실한 보안 조치를 마련할 수 있습니다. 기본 그룹의 모든 레코딩 서버가 사용 중일 경우 기본 그룹에서 작업을 인수하는 보조 장애 조치 서버 그룹을 지정할 수 있습니다. 장애 조치 레코딩 서버는 한 번에 한 그룹의 구성원만 될 수 있습니다.

하나의 장애 조치 그룹에서 장애 조치 레코딩 서버는 순서대로 정렬됩니다. 이 순서는 장애 조치 레코딩 서버가 레코딩 서버로부터 작업을 인수하는 순서를 결정합니다. 기본적으로 이 순서는 장애 조치 그룹에 장애 조치 레코딩 서버를 포함한 순서를 반영합니다. 먼저 포함된 것이 우선입니다. 필요한 경우 이 순서를 변경할 수 있습니다.

상시 대기 장애 조치 레코딩 서버

상시 대기 장애 조치 레코딩 서버 설정에서는 전담 장애 조치 레코딩 서버가 **하나의** 레코딩 서버에서만 작업을 인수합니다. 이 때문에, 시스템은 이 장애 조치 레코딩 서버를 "대기" 모드로 유지할 수 있으며, 이는 전담된 레코딩 서버의 올바른/현재 구성과 동기화되며, 수동 대기 장애 조치 레코딩 서버보다 훨씬 빨리 인수할 수 있다는 의미입니다. 언급한 바와 같이 상시 대기 서버를 하나의 레코딩 서버에만 할당하고, 서버를 그룹화할 수는 없습니다. 이미 상시 대기 레코딩 서버로서 장애 조치 그룹에의 일부인 장애 조치 서버를 할당할 수 없습니다.

장애 조치 레코딩 서버 유효성 확인

장애 조치 서버에서 레코딩 서버로의 비디오 데이터 통합 유효성을 확인하려면 레코딩 서버 서비스를 중단하거나 레코딩 서버 컴퓨터를 끔으로써 레코딩 서버를 사용할 수 없는 상태로 만들어야 합니다.

네트워크 케이블을 뽑거나 테스트 도구를 사용하여 네트워크를 막음으로써 야기되는 수동 네트워크 차단은 유효한 방법이 아닙니다.

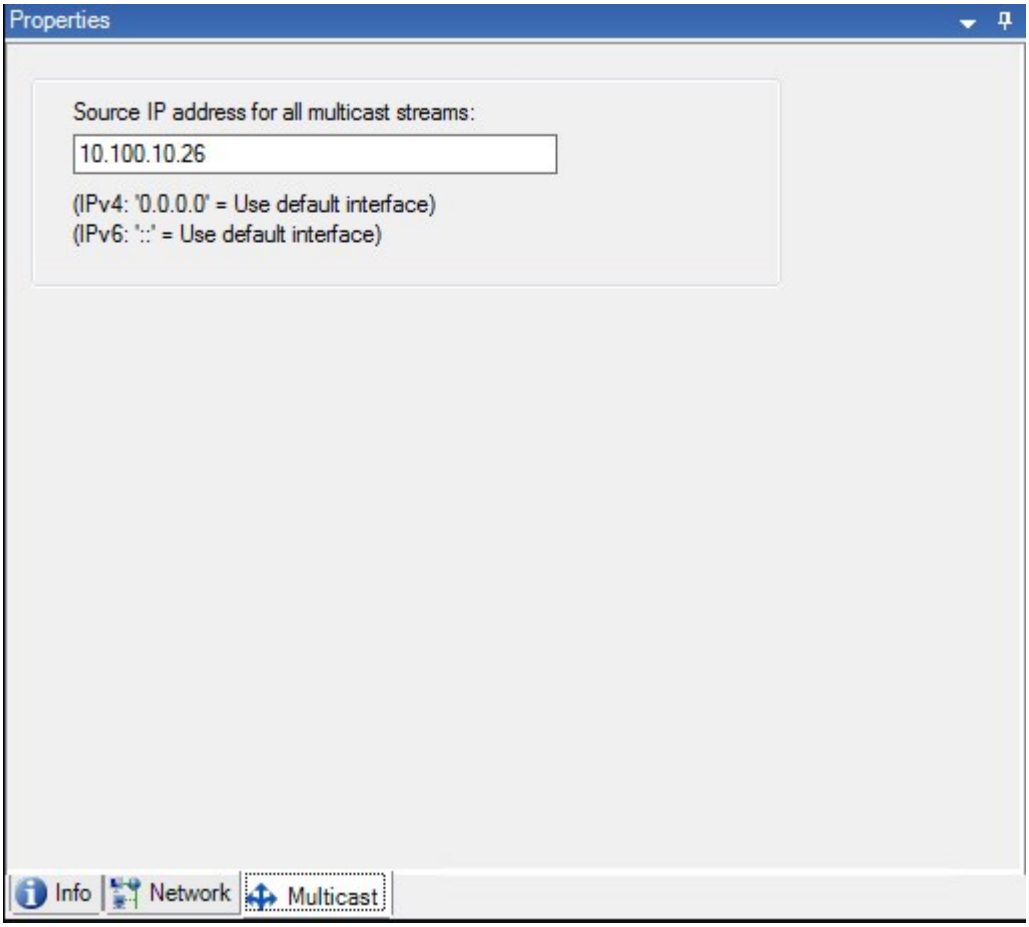
정보 탭 속성(장애 조치 서버)

다음의 장애 조치 레코딩 서버 속성을 지정합니다.

이름	설명
이름	Management Client, 로그 등에 나타나는 장애 조치 레코딩 서버의 이름.
설명	장애 조치 레코딩 서버를 설명하는 데 사용할 수 있는 옵션 필드(예: 작업을 인계한 레코딩 서버).
호스트 이름	장애 조치 레코딩 서버의 호스트 이름을 표시합니다. 이 항목은 변경할 수 없습니다.
로컬 웹 서버 주소	장애 조치 레코딩 서버 웹 주소의 로컬 주소를 표시합니다. 예를 들어 PTZ 카메라 제어 명령의 처리를 위해 그리고 XProtect Smart Client 에서 브라우징 및 라이브 요청을 처리하기 위해 로컬 주소를 사용합니다. 주소에는 웹 서버 통신에 사용되는 포트 번호가 포함됩니다(일반적인 포트 7563). 장애 조치 레코딩 서버가 암호화를 사용하는 레코딩 서버로부터 인계할 경우, 장애 조치 레코딩 서버도 암호화를 사용하도록 준비해야 합니다. 레코딩 서버로부터 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화를 활성화할 경우 자물쇠 아이콘이 나타나고 주소는 **http** 대신에 **https** 를 포함하게 됩니다.
웹 서버 주소	인터넷 상에 장애 조치 레코딩 서버 웹 주소의 공용 주소를 표시합니다. 설치에서 방화벽이나 NAT 라우터를 이용하는 경우, 인터넷을 통해 감시 시스템에 액세스하는 클라이언트가 장애 조치 레코딩 서버에 연결할 수 있도록 방화벽 또는 NAT의 주소를 입력합니다. **네트워크** 탭에서 공용 주소 및 포트 번호를 지정합니다. 레코딩 서버로부터 데이터 스트림을 검색하는 클라이언트와 서버에 대한 암호화를 활성화할 경우 자물쇠 아이콘이 나타나고 주소는 **http** 대신에 **https** 를 포함하게 됩니다.
UDP 포트	장애 조치 레코딩 서버 간의 통신에 사용되는 포트 번호. 기본 포트는 8844입니다.
데이터베이스 위치	레코딩을 저장하기 위해 장애 조치 레코딩 서버에서 사용되는 데이터베이스의 경로를 지정합니다. 장애 조치 레코딩 서버가 레코딩 서버의 작업을 인수하는 동안에는 데이터베이스 경로를 변경할 수 없습니다. 장애 조치 레코딩 서버가 더 이상 레코딩 서버의 작업을 인수하지 않을 때 시스템이 변경 내용을 적용합니다.
이 장애 조치 서버 활성화	장애 조치 레코딩 서버를 비활성화하려면 선택을 취소합니다(기본적으로 선택되어 있음). 장애 조치 레코딩 서버를 비활성화해야 레코딩 서버로부터 작업을 인수할 수 있습니다.

멀티캐스트 탭(장애 조치 서버)

장애 조치 서버를 사용하고 있고, 라이브 스트리밍의 멀티캐스를 활성화한 경우, 레코딩 서버 및 장애 조치 서버 모두에서 사용 중인 네트워크 인터페이스 카드의 IP 주소를 지정해야 합니다.



멀티캐스팅에 관한 자세한 정보는 페이지 191의 레코딩 서버에 대한 멀티캐스팅 활성화를 참조하십시오.

정보 탭 속성(장애 조치 그룹)

필드	설명
이름	Management Client, 로그 등에 나타나는 장애 조치 그룹의 이름.
설명	옵션 설명(예: 서버의 물리적 위치).

시퀀스 탭 속성(장애 조치 그룹)

필드	설명
장애 조치 시퀀스 지정	**위** 및 **아래** 를 사용하여 그룹 내에서 일반 장애 조치 레코딩 서버의 원하는 시퀀스를 설정합니다.

Milestone Interconnect에 대한 원격 서버

Milestone Interconnect™ 을(를) 통해 소규모로 물리적으로 나눠진 많은 원격 XProtect 설치와 하나의 XProtect Corporate 중앙 사이트를 통합할 수 있습니다. 원격 사이트라고 하는 이러한 소규모 사이트를 이동식 유닛(예: 보트, 버스 또는 기차)에 설치할 수 있습니다. 즉, 그러한 사이트를 네트워크에 영구히 연결할 필요가 없습니다.

정보 탭(원격 서버)

이름	설명
이름	원격 서버가 시스템과 클라이언트에 나열될 때마다 시스템이 이 이름을 사용합니다. 이 이름은 고유할 필요가 없습니다. 서버의 이름을 변경한 경우, Management Client 에서 전역으로 이름이 변경됩니다.
설명	원격 서버의 설명을 입력합니다(선택 사항). 설명은 시스템 내 다수의 목록에 나타납니다. 예를 들어, **개요** 창의 하드웨어 이름 위에 마우스 포인터를 멈추면 나타납니다.
모델	원격 사이트에 설치된 XProtect 제품을 표시합니다.
버전	원격 시스템의 버전을 표시합니다.
소프트웨어 라이선스 코드	원격 시스템의 소프트웨어 라이선스 코드.
드라이버	원격 서버에 대한 연결을 처리하는 드라이버를 식별합니다.
주소	하드웨어 장치의 호스트 이름 또는 IP 주소입니다.
IE	하드웨어 공급업체의 기본 홈 페이지를 엽니다. 하드웨어 또는 시스템 관리 시 이 페이지를 사

이름	설명
	용할 수 있습니다.
원격 시스템 ID	예를 들어, 라이선스를 관리하기 위해 XProtect 에서 사용되는 원격 사이트의 고유 시스템 ID 입니다.

설정 탭(원격 서버)

설정 탭에서, 원격 시스템의 이름을 볼 수 있습니다.

이벤트 탭(원격 서버)

규칙을 생성하여 원격 시스템으로부터의 이벤트에 즉시 반응할 수 있도록 원격 시스템에서 중앙 사이트로 이벤트를 추가할 수 있습니다. 이벤트 수는 원격 시스템에 구성된 이벤트에 따라 다릅니다. 기본 이벤트는 삭제할 수 없습니다.

목록이 완료되지 않은 것으로 나타나는 경우:

1. **개요** 창에서 해당 원격 서버를 마우스 오른쪽 단추로 클릭하고 **하드웨어 업데이트** 를 선택합니다.
2. 대화 상자에, Milestone Interconnect 설정을 구성하거나 마지막으로 새로 고친 이후 원격 시스템에 적용된 모든 변경 내용(장치 제거, 업데이트 및 추가)이 나열됩니다. **확인** 을 클릭하여 이러한 변경 내용으로 중앙 사이트를 업데이트합니다.

원격 검색 탭

원격 검색 탭에서 Milestone Interconnect 설치의 원격 사이트에 대한 원격 레코딩 검색 설정을 처리할 수 있습니다:

다음의 속성을 지정합니다:

이름	설명
최대한으로 레코딩 검색	원격 사이트에서 레코딩을 검색하는 데 사용할 최대 대역폭(Kbits/s 단위)을 결정합니다. 확인란을 선택하여 한도 검색을 활성화합니다.
레코딩 검색 범위	원격 사이트에서 레코딩 검색을 특정 시간 간격으로 제한할지 여부를 결정합니다. 종료 시간에 미완료 작업은 완료될 때까지 계속되므로 종료 시간이 중대한 요소일 경우, 미완료 작업이 완료될 수 있도록 시간을 더 빨리 설정해야 합니다. 시스템에서 시간 간격 이외에 자동 검색 또는 XProtect Smart Client 에서 검색 요청을 수신한 경우,

이름	설명
	해당 요청이 수락되나 선택한 시간 간격에 도달하기 전에는 검색이 시작되지 않습니다. **시스템 대시보드** -> **현재 작업** 에서 사용자가 시작한 보류 중인 원격 레코딩 검색 작업을 확인할 수 있습니다.
동시에 장치 검색	동시에 레코딩을 검색할 장치의 최대 수를 결정합니다. 시스템 용량에 따라 더 많거나 더 적은 용량이 필요할 경우 기본값을 변경합니다.

설정을 변경하면 변경 내용이 시스템에 반영될 때까지 몇 분 정도 걸릴 수 있습니다.

위의 어느 것도 원격 레코딩을 직접 재생하는 데 적용되지 않습니다.
직접 재생되도록 설정된 모든 카메라를 직접 재생에 사용할 수 있고 필요에 따른 대역폭을 사용하게 됩니다.

장치 노드

장치(장치 노드)

장치는 Management Client하드웨어 추가 **마법사를 사용하여 하드웨어를 추가하면** 에 나타납니다. 페이지 197의 하드웨어 추가를 참조하십시오.

동일한 속성을 지니고 있는 경우 장치 그룹을 통해 장치를 관리할 수 있습니다(페이지 52의 장치 그룹(설명됨) 참조).

또한 장치를 개별적으로 관리할 수 있습니다.

개별 장치의 활성화/비활성화 및 이름 변경은 레코딩 서버 하드웨어에서 이루어집니다. 장치 그룹을 통한 장치 활성화/비활성화 를 참조하십시오.

카메라에 대한 모든 기타 구성 및 관리의 경우, 사이트 탐색 창에서 **장치** 를 확장한 후 다음과 같은 장치를 선택합니다.

- **카메라**
- **마이크**
- **스피커**
- **메타데이터**
- **입력**
- **출력**

개요 창에서 카메라 개요를 간편하게 확인할 수 있게 카메라를 그룹화합니다. 초기 그룹화는 **하드웨어 추가** 마법사의 일부로 이루어집니다.

지원되는 하드웨어에 대한 자세한 내용은 Milestone 웹사이트 (https://www.milestonesys.com/support/tools-and-references/supported-devices/)에서 지원되는 하드웨어 페이지를 참조하십시오.

장치의 상태 아이콘

장치를 선택하면 현재 상태에 관한 정보가 **미리보기** 창에 나타납니다.
다음 아이콘은 장치의 상태를 나타냅니다:

카메라	마이크로폰	스피커	메타데이터	입력	출력	설명
						장치 활성화됨 및 데이터 검색 중: 장치가 활성화되었고 라이브 스트림을 검색합니다.
						장치 레코딩 중: 장치가 시스템에 데이터를 기록하는 중입니다.
						장치가 일시적으로 중지됨 또는 피드 없음: 중지된 경우, 정보가 시스템으로 전송되지 않습니다. 카메라의 경우, 라이브 비디오를 볼 수 없습니다. 중지된 장치는 장치가 비활성화되었을 때와는 대조적으로 이벤트 검색, 설정 지정 등을 위해 레코딩 서버와 계속해서 통신할 수 있습니다.
						장치 비활성화됨: 규칙을 통해 자동으로 시작할 수 없고 레코딩 서버와 통신할 수 없습니다. 카메라가 비활성화된 경우, 라이브 또는 녹화된 비디오를 볼 수 없습니다.
						장치 데이터베이스 복구 중.
						장치에 주의 요함: 장치가 올바로 기능하지 않습니다. 장치 아이콘 위에 마우스 포인터를 멈추면 도구 설명에서 해당 문제에 대한 설명을 확인할 수 있습니다.
						상태 알 수 없음: 장치의 상태를 알 수 없습니다(예: 레코딩 서버가 오프라인인 경우).
						이 예제에서 **장치 활성화됨 및 데이터 검색 중** 이 **장치 레코딩 중** 과 결합된 경우와 같이 일부 아이콘을 조합하여 사용할 수 있습니다.

카메라(장치 노드)

카메라 장치는 하드웨어를 시스템에 추가할 때 자동으로 추가되며, 기본적으로 활성화되어 있습니다.

이 시스템은 연결된 모든 카메라의 비디오 피드가 자동으로 시스템으로 공급될 수 있도록 보장하는 기본 시작 피드 규칙이 함께 제공됩니다. 기본 규칙은 필요한 대로 비활성화 및/또는 수정할 수 있습니다.

이 구성 순서를 따라 카메라 장치 구성과 관련된 가장 일반적인 작업을 완료합니다:

1. 카메라 설정을 구성하려면 설정 탭(장치) 을 참조하십시오.
2. 스트림을 구성하려면 스트림 탭(장치) 을 참조하십시오.
3. 모션을 구성하려면 모션 탭(장치) 을 참조하십시오.
4. 레코딩을 구성하려면 레코딩 탭(장치) 및 장치에 대한 데이터베이스 모니터링 을 참조하십시오.
5. 나머지 설정을 필요에 따라 구성합니다.

마이크(장치 노드)

마이크 장치는 하드웨어를 시스템에 추가할 때 자동으로 추가됩니다. 이들 장치는 기본적으로 비활성화되어 있으므로 사용 전에 **하드웨어 추가** 마법사의 일부로 또는 그 이후에 활성화해야 합니다. 마이크에는 별도의 라이선스가 필요하지 않습니다. 시스템에서 필요한 수만큼의 마이크를 사용할 수 있습니다.

또한 카메라와 완전히 독립적으로 마이크를 사용할 수 있습니다.

이 시스템은 연결된 모든 마이크의 오디오 피드가 자동으로 시스템으로 공급될 수 있도록 보장하는 기본 시작 오디오 피드 규칙이 함께 제공됩니다. 기본 규칙은 필요한 대로 비활성화 및/또는 수정할 수 있습니다.

다음의 탭에서 마이크 장치를 구성할 수 있습니다:

- 정보 탭, 정보 탭(장치) 참조
- 설정 탭, 설정 탭(장치) 참조
- 레코드 탭, 레코드 탭(장치) 참조
- 이벤트 탭, 이벤트 탭(장치) 참조

스피커(장치 노드)

스피커 장치는 하드웨어를 시스템에 추가할 때 자동으로 추가됩니다. 이들 장치는 기본적으로 비활성화되어 있으므로 사용 전에 **하드웨어 추가** 마법사의 일부로 또는 그 이후에 활성화해야 합니다. 스피커에는 별도의 라이선스가 필요하지 않습니다. 시스템에서 필요한 수만큼의 스피커를 사용할 수 있습니다.

또한 카메라와 완전히 독립적으로 스피커를 사용할 수 있습니다.

이 시스템은 장치가 사용자 활성 오디오를 스피커로 전송할 수 있도록 장치를 시작하는 기본 시작 오디오 피드 규칙이 함께 제공됩니다. 기본 규칙은 필요한 대로 비활성화 및/또는 수정할 수 있습니다.

다음의 탭에서 스피커 장치를 구성할 수 있습니다:

- 정보 탭, 정보 탭(장치) 참조
- 설정 탭, 설정 탭(장치) 참조
- 레코드 탭, 레코드 탭(장치) 참조

메타데이터(장치 노드)

이 시스템은 메타데이터를 지원하는 연결된 모든 하드웨어의 메타데이터 피드가 자동으로 시스템으로 공급될 수 있도록 보장하는 기본 시작 피드 규칙이 함께 제공됩니다. 기본 규칙은 필요한 대로 비활성화 및/또는 수정할 수 있습니다.

다음의 탭에서 메타데이터 장치를 구성할 수 있습니다:

- 정보 탭, 정보 탭(장치) 참조
- 설정 탭, 설정 탭(장치) 참조
- 레코드 탭, 레코드 탭(장치) 참조

입력(장치 노드)

또한 카메라와 완전히 독립적으로 입력 장치를 사용할 수 있습니다.

장치에 외부 입력 장치 사용을 지정하기 전에 장치 자체가 센서 작동을 인식하는지 확인합니다. 대부분의 장치는 해당 구성 인터페이스 또는 CGI(Common Gateway Interface) 스크립트 명령을 통해 이 정보를 표시할 수 있습니다.

입력 장치는 하드웨어를 시스템에 추가할 때 자동으로 추가됩니다. 이들 장치는 기본적으로 비활성화되어 있으므로 사용 전에 **하드웨어 추가** 마법사의 일부로 또는 그 이후에 활성화해야 합니다. 입력 장치에는 별도의 라이선스가 필요하지 않습니다. 시스템에서 필요한 수만큼의 입력 장치를 사용할 수 있습니다.

다음의 탭에서 입력 장치를 구성할 수 있습니다:

- 정보 탭, 정보 탭(장치) 참조
- 설정 탭, 설정 탭(장치) 참조
- 이벤트 탭, 이벤트 탭(장치) 참조

출력(장치 노드)

출력은 Management Client 및 XProtect Smart Client 에서 수동으로 트리거할 수 있습니다.

장치에서 외부 출력 장치 사용을 지정하기 전에 장치 자체가 출력에 연결된 장치를 제어할 수 있는지 확인합니다. 대부분의 장치는 해당 구성 인터페이스 또는 CGI(Common Gateway Interface) 스크립트 명령을 통해 이 정보를 표시할 수 있습니다.

출력 장치는 하드웨어를 시스템에 추가할 때 자동으로 추가됩니다. 이들 장치는 기본적으로 비활성화되어 있으므로 사용 전에 **하드웨어 추가** 마법사의 일부로 또는 그 이후에 활성화해야 합니다. 출력 장치에는 별도의 라이선스가 필요하지 않습니다. 시스템에서 필요한 수만큼의 출력 장치를 사용할 수 있습니다.

다음의 탭에서 출력 장치를 구성할 수 있습니다:

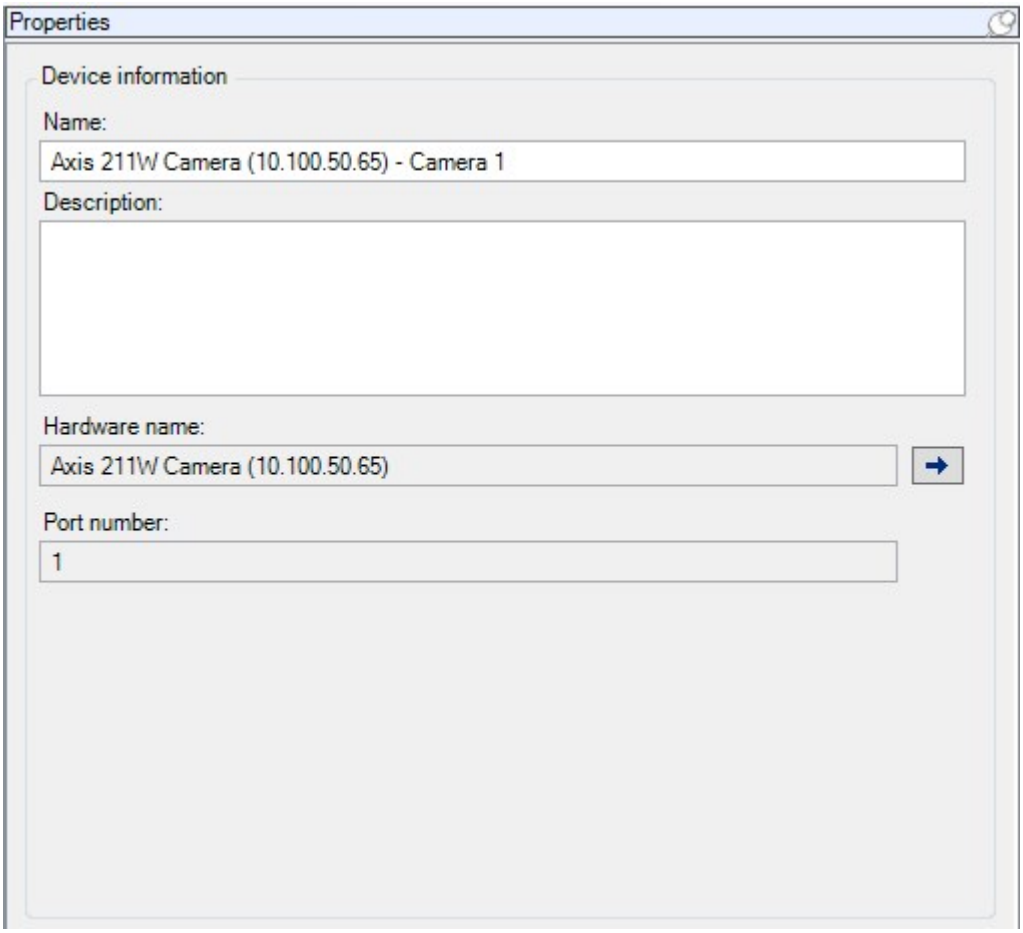
정보 탭, 다음을 참조하십시오

- 정보 탭, 정보 탭(장치) 참조
- 설정 탭, 설정 탭(장치) 참조

장치 탭

정보 탭(장치)

정보 탭에서는 여러 필드에서 장치에 대한 기본 정보를 보고 편집할 수 있습니다.
모든 장치에는 **정보** 탭이 있습니다.



정보 탭 속성

이름	설명
이름	장치가 시스템과 클라이언트에 나열될 때마다 이 이름이 사용됩니다. 장치의 이름을 변경한 경우, Management Client 에서 전역으로 이름이 변경됩니다.
설명	장치의 설명을 입력합니다(옵션). 설명은 시스템 내 다수의 목록에 나타납니다. 예를 들어, **개요** 창의 이름 위로 마우스 포인터를 멈추면 나타납니다.
하드웨어 이름	장치가 연결되는 하드웨어의 이름을 표시합니다. 이 필드는 여기서 편집할 수 없지만, 옆에 있는 **이동**을 클릭해서 변경할 수 있습니다. 이렇게 하면 이름을 변경할 수 있는 하드웨어 정보로 이동합니다.
포트 번호	하드웨어에 장치가 연결되어 있는 포트를 표시합니다. 단일 장치 하드웨어의 경우, 일반적으로 포트 번호는 **1**입니다. 채널이 여러 개인 비디오 서버와 같은 다중 장치 하드웨어의 경우, 일반적으로 포트 번호는 장치가 연결되어 있는 채널(예: **3**)을 나타냅니다.
짧은 이름	카메라에 짧은 이름을 적용하려면 여기에 입력합니다. 최대 길이는 128자입니다. 스마트 맵을 사용하는 경우 짧은 이름이 카메라와 함께 자동으로 스마트 맵에 표시됩니다. 그렇지 않을 경우 전체 이름이 표시됩니다.
지리적 좌표	카메라의 지리적 위치를 **latitude, longitude** 형식으로 입력합니다. 입력하는 값은 XProtect Smart Client 및 XProtect Mobile 클라이언트 에서 스마트 맵에 카메라 아이콘 위치를 결정합니다. 이 필드는 주로 스마트 맵과 써드파티 연동을 위한 것입니다.
방향	세로축의 정북 지점 대비 측정된 카메라의 보기 방향을 입력합니다. 입력하는 값은 XProtect Smart Client 및 XProtect Mobile 클라이언트 에서 스마트 맵에 카메라 아이콘 방향을 결정합니다. 기본값은 0.0입니다. 이 필드는 주로 스마트 맵과 써드파티 연동을 위한 것입니다.
시계	화각의 너비를 도 단위로 입력합니다. 입력하는 값에 따라 XProtect Smart Client 및 XProtect Mobile 클라이언트에서 스마트 맵에 있는 카메라 아이콘의 화각 각도가 결정됩니다. 기본값은 0.0입니다.

이름	설명
	이 필드는 주로 스마트 맵과 써드파티 연동을 위한 것입니다.
깊이	화각의 깊이를 미터나 피트로 입력합니다. 입력하는 값에 따라 XProtect Smart Client 및 XProtect Mobile 클라이언트에서 스마트 맵에 있는 카메라 아이콘의 화각 길이가 결정됩니다. 기본값은 0.0입니다. 이 필드는 주로 스마트 맵과 써드파티 연동을 위한 것입니다.
브라우저에 위치 미리 보기	올바른 지리적 좌표를 입력했는지 확인하려면 버튼을 클릭합니다. Google Maps는 지정한 위치로 표준 인터넷 브라우저에 열립니다. 이 필드는 주로 스마트 맵과 써드파티 연동을 위한 것입니다.

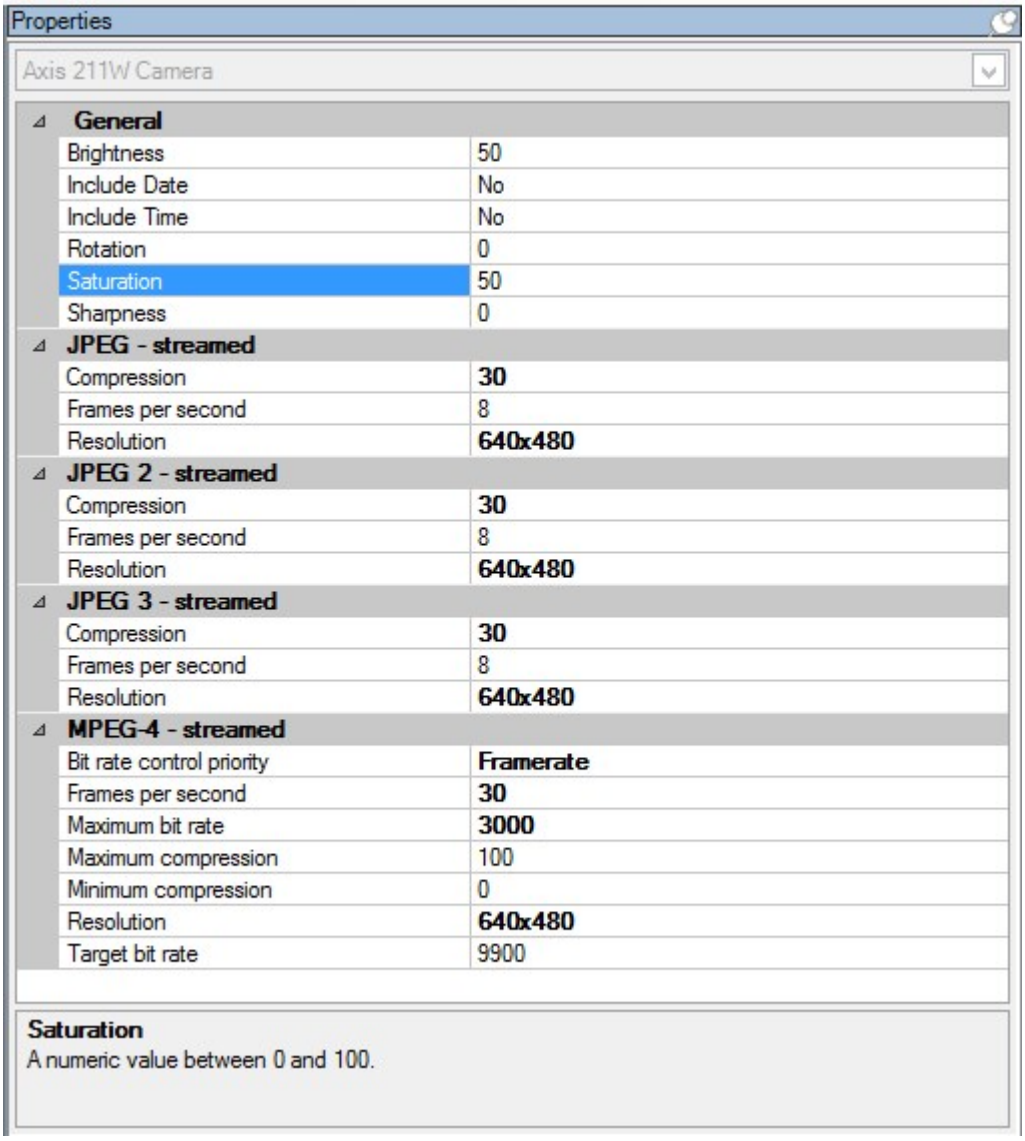
설정 탭(장치)

설정 탭에서는 여러 필드에서 장치에 대한 설정을 보고 편집할 수 있습니다.
모든 장치에는 **설정** 탭이 있습니다.

해당 값은 표에서 변경 가능하거나 읽기 전용으로 나타납니다. 설정을 기본값 이외의 값으로 변경하면 해당 값이 굵게 나타납니다.

표의 내용은 장치 드라이버에 따라 다릅니다.

허용된 범위는 설정 표 아래의 정보 상자에 나타납니다:



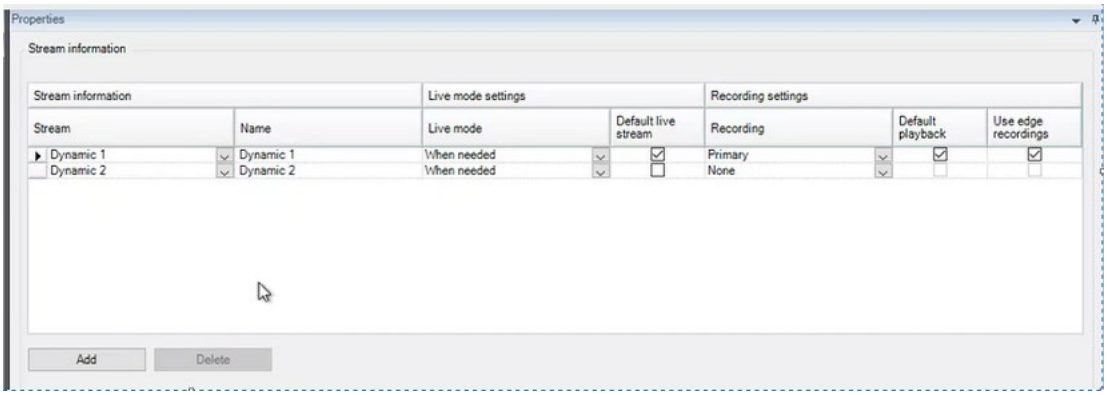
카메라 설정에 관한 자세한 정보는 카메라 설정 보기 또는 편집 을 참조하십시오.

스트림 탭(장치)

다음 장치에는 **스트림** 탭이 있습니다:

- 카메라

스트림 탭에는 기본적으로 단일 스트림이 나열됩니다. 이는 선택한 카메라의 기본 스트림으로, 라이브 및 녹화된 비디오에 사용됩니다. 적응형 재생을 사용하는 경우, 두 개의 스트림을 만들어야 합니다.



스트림 랩 상의 작업

이름	설명
추가	클릭하여 목록에 스트림을 추가합니다. 스트림 추가

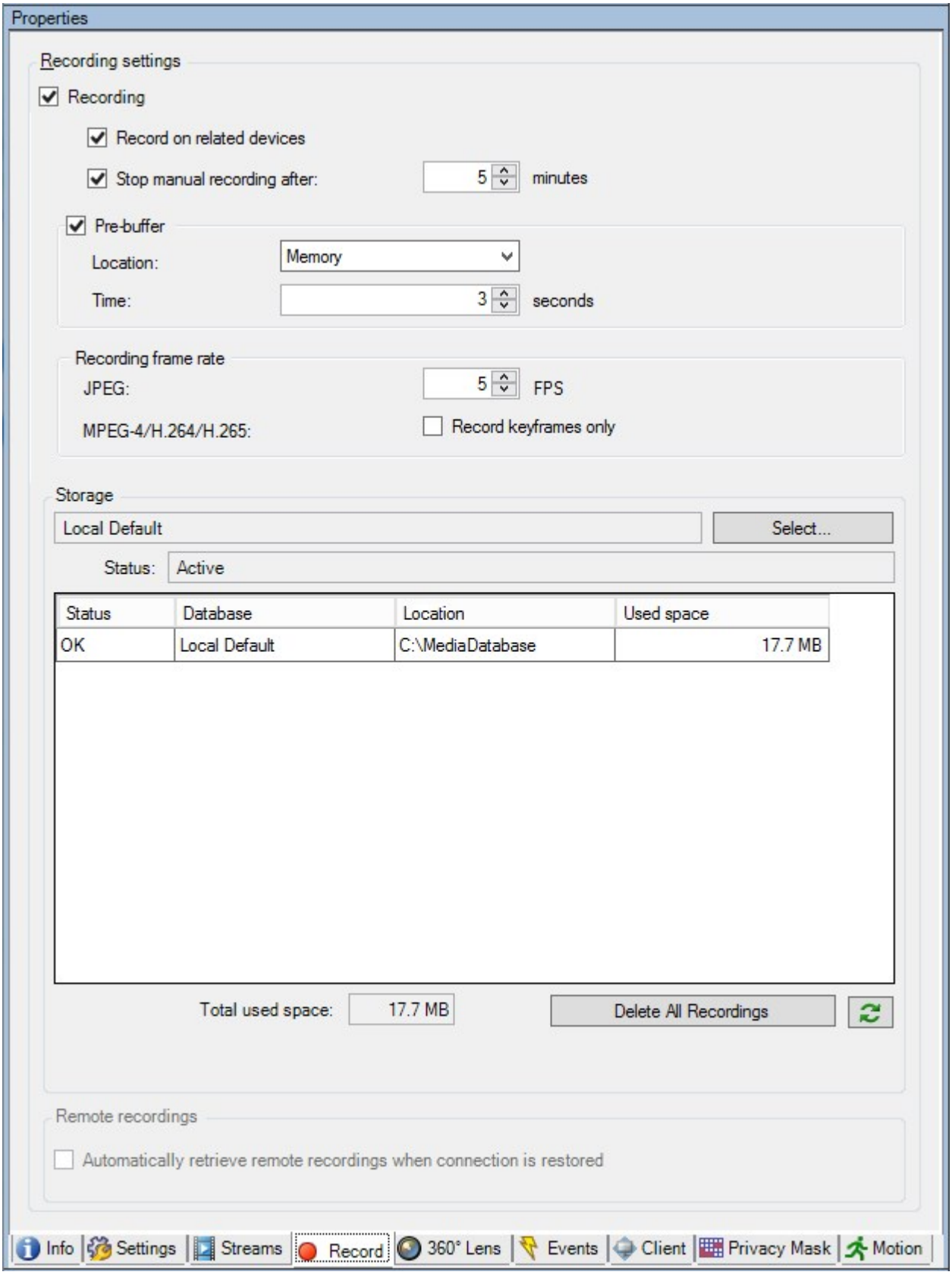
레코드 탭(장치)

다음 장치에는 레코딩 탭이 있습니다:

- 카메라
- 마이크
- 스피커
- 메타데이터

장치의 레코딩은 레코딩을 활성화하고 레코딩 관련 규칙 기준을 충족하는 경우에만 데이터베이스에 저장됩니다.

장치에 대해 구성할 수 없는 매개변수는 회색으로 표시됩니다.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

녹화 탭 상의 작업

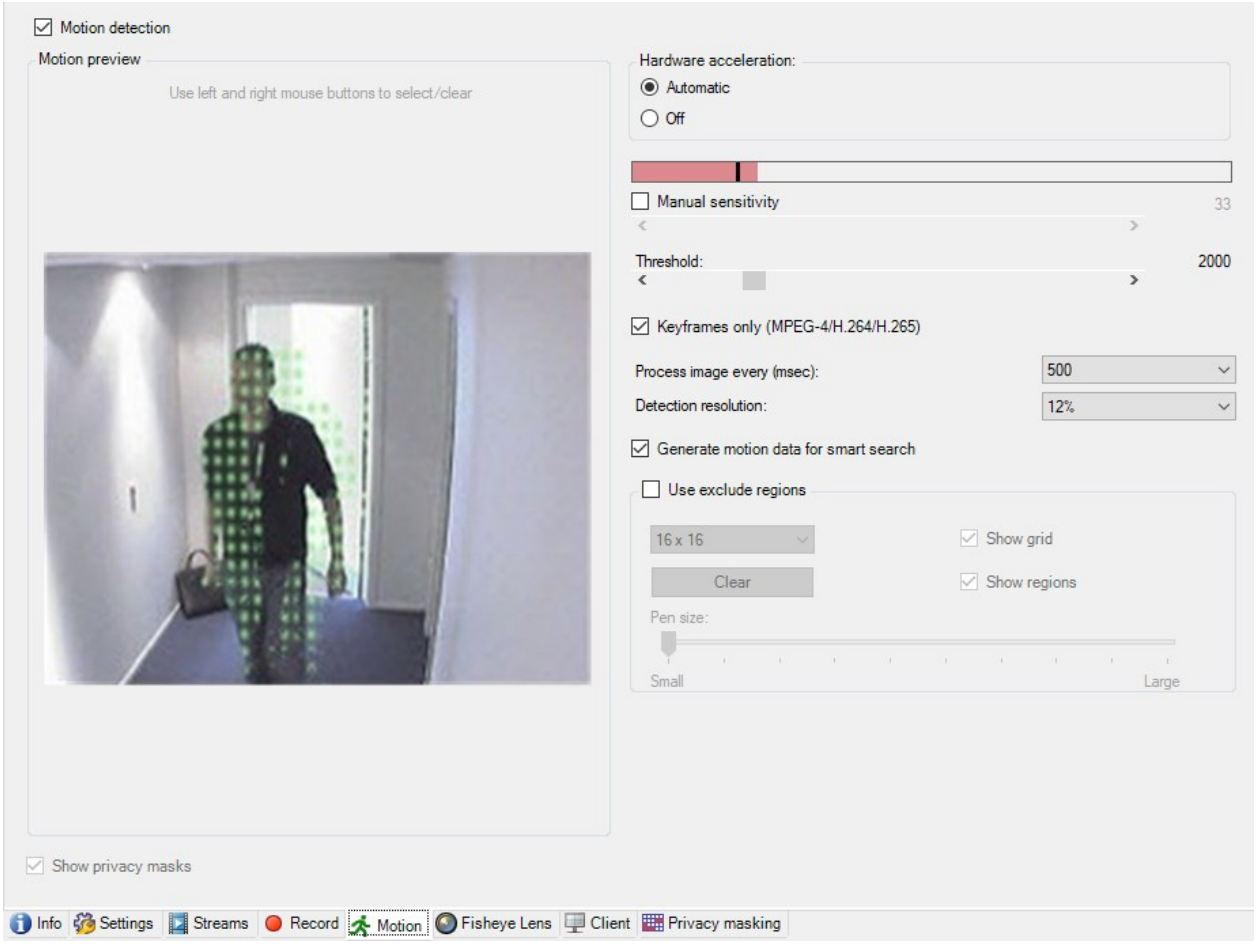
이름	설명
레코딩	레코딩 활성화/비활성화 관련 장치에서 레코딩 활성화
사전 버퍼	사전 버퍼링 및 사전 버퍼 레코딩 저장소(설명됨) 사전 버퍼링 관리 수동 레코딩 관리
녹화 프레임 속도	레코딩 프레임 속도 지정 키프레임 레코딩 활성화
저장소	장치에 대한 데이터베이스 상태 모니터링
선택	한 저장소에서 다른 저장소로 장치 이동
모든 레코딩 삭제	같은 서버에 그룹 내 모든 장치를 추가한 경우에 이 버튼을 사용하십시오. 녹화 삭제
연결이 복원될 때 원격 녹화를 자동으로 검색	원격 레코딩 저장 및 검색

모션 탭(장치)

다음 장치에는 **모션** 탭이 있습니다:

- 카메라

모션 탭에서, 선택한 카메라에 대한 모션 감지를 활성화하고 구성할 수 있습니다.



모션 탭 상의 작업

이름	설명
모션 감지	모션 감지 활성화 및 비활성화
하드웨어 가속	**자동화** 를 선택하여 하드웨어 가속화를 활성화하거나 **끄기** 를 선택하여 설정을 비활성화합니다. 자세한 정보는 하드웨어 가속화 활성화 또는 비활성화 를 참조하십시오.
사생활 보호	영구적인 사생활 보호로 정의된 영역이 있는 경우 **사생활 보호** 확인란을 선택하여 **모션** 탭에서 사생활 보호를 표시할 수 있습니다. 페이지 420의 사생활 보호 탭(장치)에서 사생활 보호로 영역을 정의할 수 있습니다. 영구적 사생활 보호 대상 영역 내에서는 모션 감지가 없습니다.

이름	설명
수동 감도	이미지 내의 **각 픽셀의 양이 얼마나** 변경되어야 모션으로 간주되는지를 결정합니다. 수동 감도를 활성화하여 모션 정의
임계치	이미지 내의 **각 픽셀의 수가 얼마나** 많이 변경되어야 모션으로 간주되는지를 결정합니다. 모션 정의를 위한 임계값 지정
키프레임만(MPEG-4/H.264/H.265)	이 확인란을 선택하여 전체 비디오 스트림 대신 키프레임 상의 모션 감지를 수행합니다. MPEG-4/H.264/H.265에만 적용합니다. 키프레임에서 모션 감지 시 분석을 수행하는 데 사용되는 처리력이 줄어듭니다.
이미지 처리 주기(msec)	이 목록에서 이미지 처리 간격을 선택하여 시스템의 모션 감지 분석을 주기를 결정합니다. 예를 들어, 매 1000밀리초는 초당 한 번입니다. 기본값은 매 500밀리초입니다. 이 간격은 실제 프레임 속도가 여기서 설정한 간격보다 높을 경우 적용됩니다.
감지 분해능	이 목록에서 감지 분해능을 선택하여 모션 감지 성능을 최적화합니다. 선택된 이미지의 퍼센티지만 분석됩니다(예: 25%). 25%를 분석하면 이미지에서 모든 픽셀이 아닌 매 4번째 픽셀만 분석됩니다. 최적화된 감지를 사용하면 분석을 수행하는 데 사용되는 처리 능력의 양이 줄어들지만, 이로 인하여 모션 감지의 정확도가 저하되기도 합니다.
스마트 검색의 모션 데이터 생성	이 확인란을 활성화하면 시스템이 모션 감지에 사용한 이미지에 대한 모션 데이터를 생성합니다. 예를 들어, 키프레임에 대해서만 모션 감지를 선택하면 키프레임에 대해서만 모션 데이터가 생성됩니다. 추가 모션 데이터를 사용하면 스마트 검색 기능을 통해 클라이언트 사용자가 이미지에서 선택한 영역의 모션을 기반으로 관련 레코딩을 빠르게 검색할 수 있습니다. 시스템은 영구적인 사생활 보호가 적용된 영역 내에서 모션 데이터를 생성하지 않지만 일시적 사생활 보호가 적용된 영역에는 생성합니다(모션 감지(설명됨) 참조). 모션 감지 임계값 및 제외 영역은 생성된 모션 데이터에 영향을 주지 않습니다. • **도구** > **옵션** > **일반** 에서 카메라에 대한 스마트 검색 데이터 생성의 기본 설정을 지정합니다.
제외 영역 사용	카메라 뷰의 특정 영역에서의 모션 감지를 제외합니다. 모션 감지에 대한 제외 영역 지정

프리셋 탭(장치)

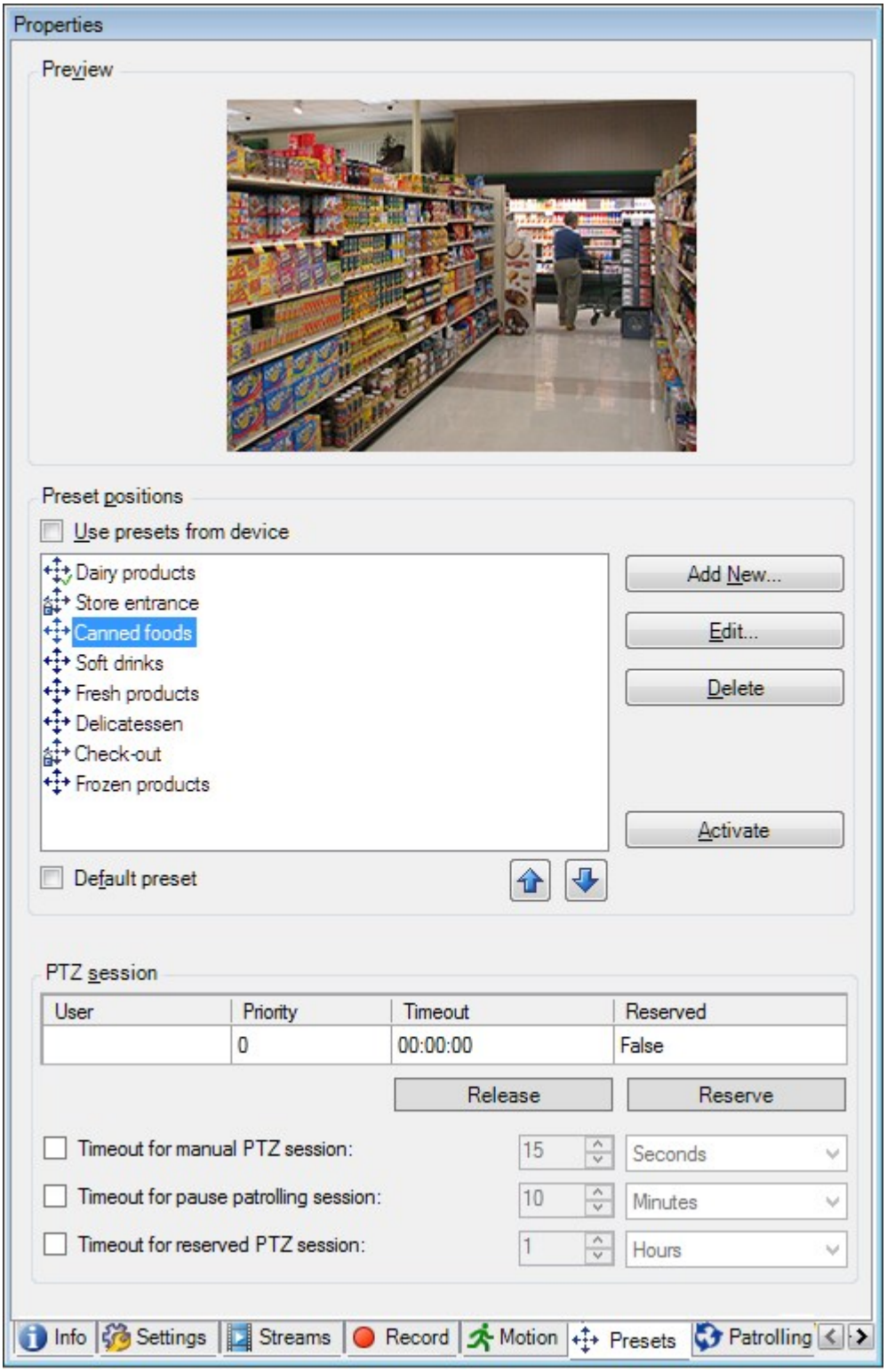
다음 장치에는 프리셋 탭이 있습니다:

- 프리셋 위치를 지원하는 PTZ 카메라

프리셋 탭에서 프리셋 위치를 만들거나 가져올 수 있습니다. 예를 들면 다음과 같습니다:

- PTZ(이동/기울기/줌) 카메라를 만드는 규칙에서 이벤트가 발생할 때 특정 프리셋 위치로 이동
- 순찰 시, 다수의 프리셋 위치 사이에서 PTZ 카메라가 자동 이동
- XProtect Smart Client 사용자에 의한 수동 활성화

전체 보안 탭 상의 역할에 대해 PTZ 권한을 할당합니다(페이지 465의 전체 보안 탭(역할) 참조) 또는 PTZ 탭(참조페이지 501의 PTZ 탭(역할)).


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

프리셋 탭 상의 작업

이름	설명
새로 만들기	시스템 내 카메라에 대한 프리셋 위치 추가: 프리셋 위치(유형 1) 추가
장치에서 프리셋 사용	카메라 자체에서 PTZ 카메라에 대한 프리셋 위치 추가: 카메라의 프리셋 위치 사용(유형 2)
기본 프리셋	PTZ 카메라의 프리셋 위치 중 하나를 카메라의 기본 프리셋 위치로 할당할 수 있습니다. 카메라의 기본 프리셋 위치를 기본으로 할당
편집	시스템에 정의된 기존의 프리셋 위치를 편집하려면: 카메라에 대한 프리셋 위치 편집(유형 1만 해당) 카메라에 정의된 프리셋 위치의 이름을 편집하려면: 카메라에 대한 프리셋 위치 이름 변경(유형 2만 해당)
잠김	프리셋 위치를 잠그려면 이 확인란을 선택합니다. XProtect Smart Client 의 사용자 또는 제한적 보안 권한을 가진 사용자가 프리셋을 업데이트 또는 삭제하지 못하게 하려면 프리셋 위치를 잠글 수 있습니다. 잠긴 프리셋은 아이콘으로 표시됩니다. 추가(프리셋 위치 추가(유형 1) 참조) 및 편집(프리셋 위치 편집(유형 1만) 참조)의 일부로 프리셋을 잠급니다.
활성화	카메라 프리셋 위치를 테스트하려면 이 버튼을 클릭합니다. 프리셋 위치 테스트(유형 1만 해당).
보존 및 해제	다른 사용자가 카메라에 대한 제어권을 가져가지 못하며 보존을 해제하지 못하게 합니다. 예약된 PTZ 세션을 실행할 보안 권한을 가진 관리자가 이 모드에서 PTZ 카메라를 실행할 수 있습니다. 그러면 다른 사용자가 카메라에 대한 제어권을 가져가지 못합니다. 충분한 권한이 있으면 다른 사용자가 보존한 PTZ 세션을 해제할 수 있습니다.

이름	설명
	PTZ 세션 보존 및 해제.
PTZ 세션	시스템이 현재 순찰 중이거나 사용자가 통제 중인 경우 모니터링: 페이지 412의 PTZ 세션 속성. PTZ 카메라 상태를 조회하고 카메라에 대한 시간 제한을 관리합니다. PTZ 세션 시간 제한 지정.

PTZ 세션 속성

PTZ 세션 표에 PTZ 카메라의 현재 상태가 표시됩니다.

이름	설명
사용자	**예약됨** 버튼을 누르고 현재 PTZ 카메라를 제어하는 사용자를 표시합니다. **시스템에 의해 순찰 세션이 활성화된 경우**, 순찰이 표시됩니다.
우선순위	사용자의 PTZ 우선순위를 표시합니다. 자신보다 우선순위가 낮은 사용자의 PTZ 세션만 가져올 수 있습니다.
시간 제한	현재 PTZ 세션의 남은 시간을 표시합니다.
예약됨	현재 세션이 예약된 PTZ 세션인지 여부를 나타냅니다. • **참**: 예약됨 • **거짓**: 예약되지 않음

PTZ 세션 섹션 내 확인란으로 각 PTZ 카메라에 대한 다음과 같은 시간 제한을 변경할 수 있습니다.

이름	설명
수동 PTZ 세션의 시간 제한	기본 기간과 다른 시간 제한이 필요한 경우 이 카메라에서 수동 PTZ 세션에 대한 시간 제한 기간을 지정합니다. **옵션** 에 있는 **도구** 에서 기본 기간을 지정합니다.
순찰 PTZ 세션 일시 중지의 시간 제한	기본 기간과 다른 시간 제한이 필요한 경우 이 카메라에서 순찰 PTZ 세션 일시 중지에 대한 시간 제한 기간을 지정합니다. **옵션** 에 있는 **도구** 에서 기본 기간을 지정합니다.
예약된 PTZ 세션의 시간 제한	기본 기간과 다른 시간 제한이 필요한 경우 이 카메라에서 예약된 PTZ 세션에 대한 시간 제한 기간을 지정합니다. **옵션** 에 있는 **도구** 에서 기본 기간을 지정합니다.

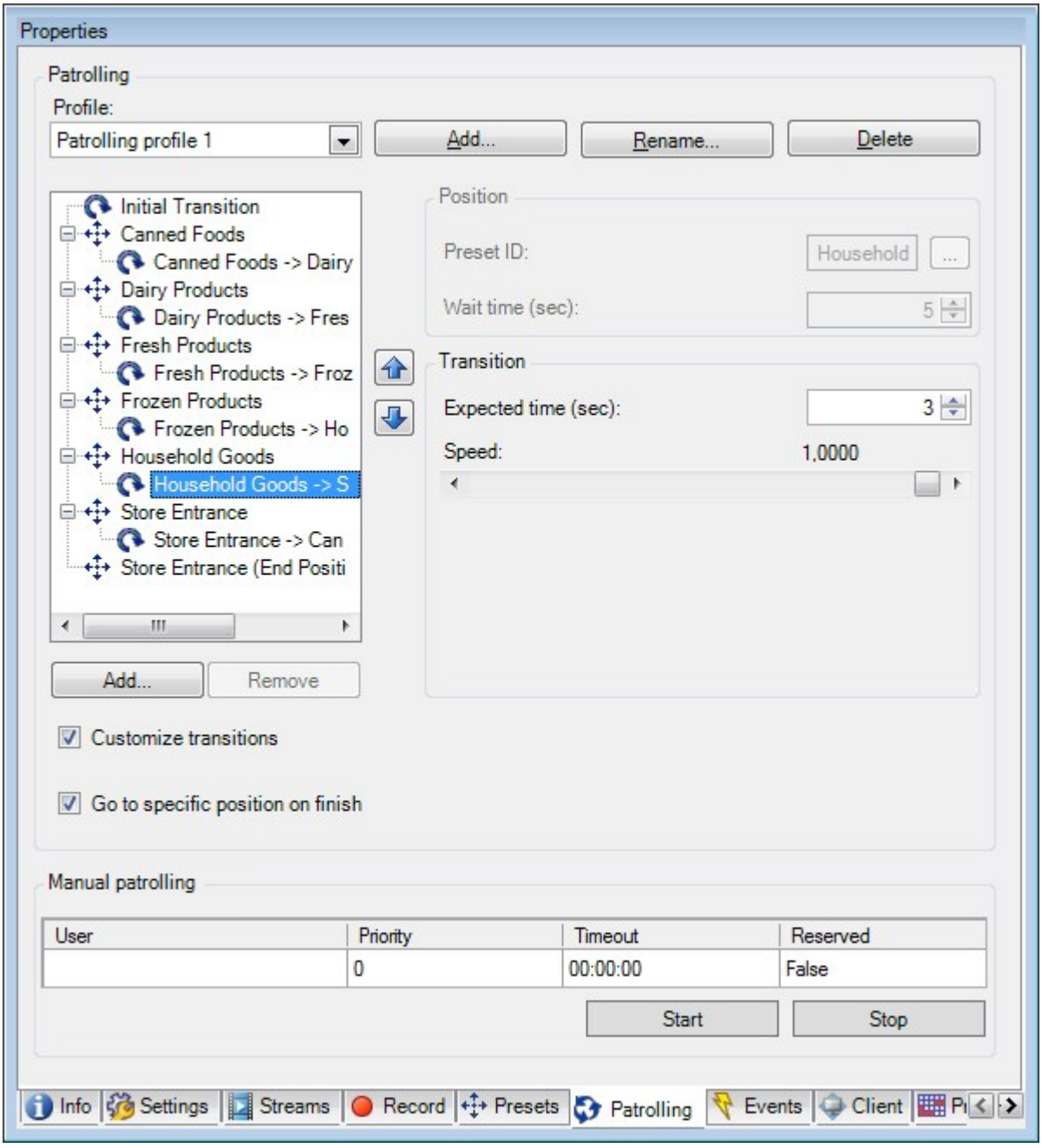
순찰 탭(장치)

다음 장치에는 순찰 탭이 있습니다.

- PTZ 카메라

순찰 탭을 사용하면, 순찰 프로파일을 생성하여 여러 프리셋 위치 간에 PTZ(이동/기울기/줌) 카메라의 자동 이동이 가능합니다.
순찰 업무를 하기 전 카메라에 대한 프리셋 위치를 **프리셋** 탭에서 최소한 2개를 지정해야 합니다. 프리셋 위치 추가(유형 1) 을 참조하십시오.

순찰 탭, 사용자 정의된 전환이 포함된 순찰 프로파일 표시:



순찰 탭 상의 작업

이름	설명
추가	순찰 프로파일 추가

이름	설명
프리셋 ID	순찰 프로파일에 프리셋 위치 지정
대기 시간(초)	각 프리셋 위치에서 시간 지정
전환 사용자 정의	전환 사용자 정의(PTZ)
완료 시 특정 위치로 이동	순찰 시 종료 위치 지정
수동 순찰	시스템이 현재 순찰 중이거나 사용자가 통제 중인 경우 모니터링합니다.
시작 및 **정지**	**시작** 및 **정지** 버튼을 사용하여 수동 순찰을 시작하고 정지합니다. 모든 또는 개별 PTZ 카메라에 대해 정기 순찰이 재개되려면 얼마나 많은 시간이 소요되어야 하는지 지정하는 방법에 관한 자세한 정보는 PTZ 카메라 세션 시간 제한 지정 을 참조하십시오.

수동 순찰 속성

수동 순찰 표에 PTZ 카메라의 현재 상태가 표시됩니다.

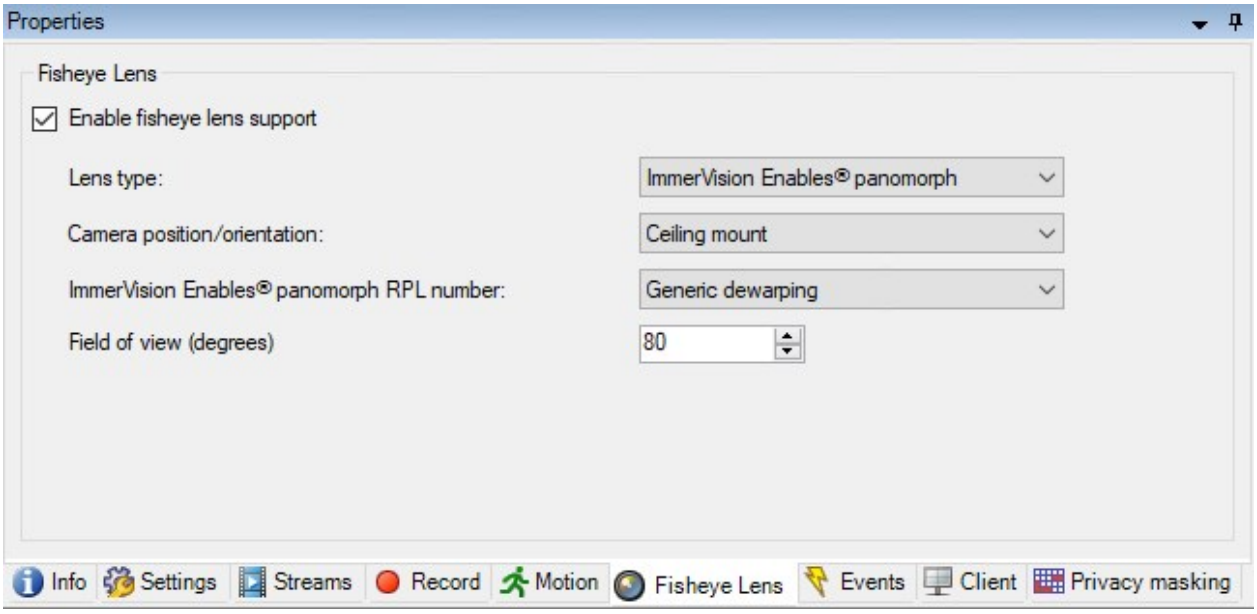
이름	설명
사용자	PTZ 세션을 예약했거나 수동 순찰을 시작하고 현재 카메라를 제어하는 사용자를 표시합니다. **시스템에 의해 순찰 세션이 활성화된 경우**, 순찰이 표시됩니다.
우선순위	사용자의 PTZ 우선순위를 표시합니다. 자신보다 우선순위가 낮은 사용자나 순찰 프로파일로부터만 PTZ 세션을 가져올 수 있습니다.
시간 제한	현재 예약된 또는 수동 PTZ 세션의 남은 시간을 표시합니다.
예약됨	현재 세션이 예약된 PTZ 세션인지 여부를 나타냅니다. • **참**: 예약됨 • **거짓**: 예약되지 않음

어안 렌즈 탭(장치)

다음 장치에는 **어안 렌즈** 탭이 있습니다:

- 어안 렌즈를 탑재한 고정형 카메라

어안 렌즈 탭에서 선택한 카메라에 대한 어안 렌즈 지원을 활성화하고 구성할 수 있습니다.



어안 렌즈 탭 상의 작업

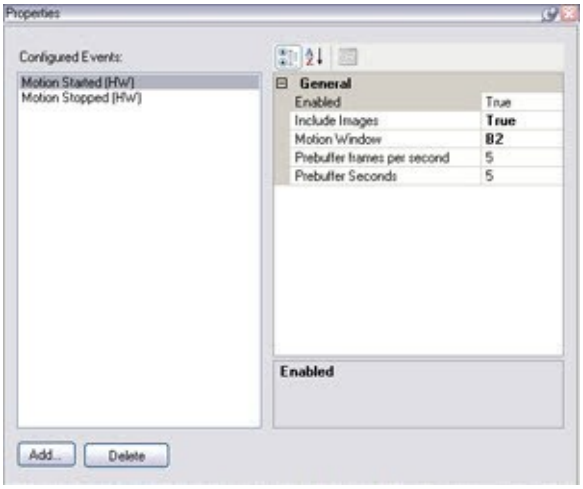
이름	설명
어안 렌즈 지원 사용	어안 렌즈 지원 활성화 및 비활성화

이벤트 탭(장치)

다음 장치에는 **이벤트** 탭이 있습니다:

- 카메라
- 마이크
- 입력

시스템의 이벤트 이외에 이벤트를 트리거하도록 일부 장치를 구성할 수 있습니다. 시스템에서 이벤트 기반 규칙을 만들 때 이러한 이벤트를 사용할 수 있습니다. 기술적으로 이러한 작업은 감시 시스템이 아닌 실제 하드웨어/장치에서 발생합니다.



이벤트 탭 상의 작업

이름	설명
추가 및 **삭제**	장치에 대한 이벤트 추가 또는 삭제

이벤트 탭(속성)

이름	설명
구성된 이벤트	**구성된 이벤트** 목록에서 선택 및 추가할 수 있는 이벤트는 전적으로 장치와 해당 구성에 따라 결정됩니다. 일부 장치 유형의 경우, 이 목록이 비어 있습니다.
일반	속성 목록은 장치와 이벤트에 따라 다릅니다. 이벤트가 계획대로 작동하기 위해서는 장치와 이 탭의 일부 또는 모든 속성을 동일하게 지정해야 합니다.

클라이언트 탭(장치)

다음 장치에는 **클라이언트** 탭이 있습니다:

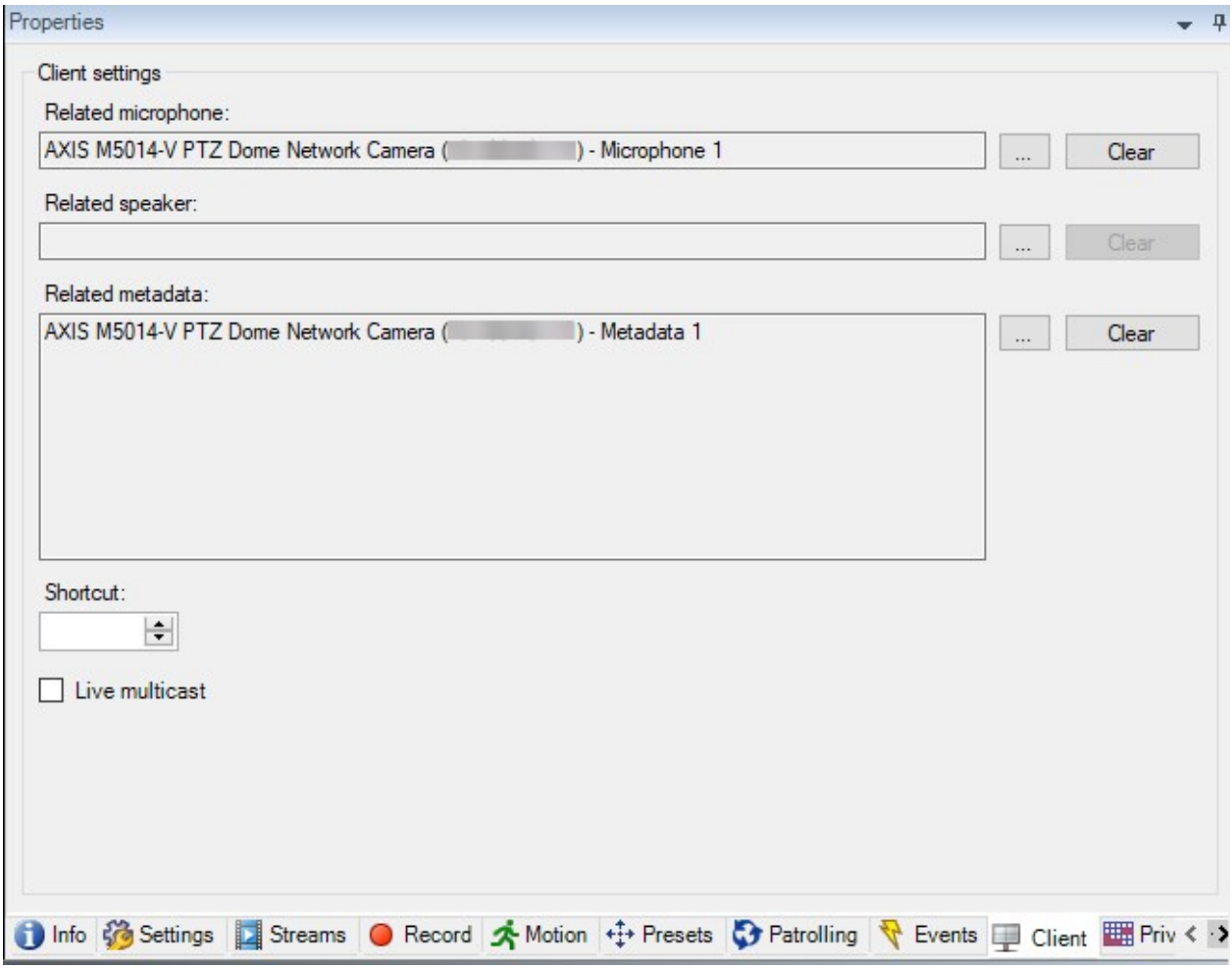
- 카메라

클라이언트 탭의 경우, XProtect Smart Client 에서 카메라를 사용할 때 보고 들을 다른 장치를 지정할 수 있습니다.

카메라가 녹화할 때 관련 장치가 녹화를 수행합니다. 페이지 212의 관련 장치에서 레코딩 활성화를 참조하십시오.

또한 카메라에서 **라이브 멀티캐스트** 를 활성화할 수도 있습니다. 카메라가 레코딩 서버를 통해 라이브 스트림을 클라이언트로 멀티캐스트한다는 의미입니다.

> 레코딩 서버가 암호화를 사용하더라도 멀티캐스트 스트림은 암호화되지 않습니다.



클라이언트 탭 속성

이름	설명
관련 마이크	카메라의 마이크로폰 중에서 XProtect Smart Client 사용자가 기본적으로 오디오를 수신하는 마이크을 지정합니다. XProtect Smart Client 사용자는 필요에 따라 다른 마이크로폰에서 수신하도록 수동

이름	설명
	으로 선택할 수 있습니다. 오디오와 함께 비디오를 스트리밍할 비디오 푸시 카메라와 관련된 마이크로폰을 지정합니다. 카메라가 녹화할 때 관련 마이크가 녹음을 수행합니다.
관련 스피커	카메라의 스피커 중에서 XProtect Smart Client 사용자가 기본적으로 말을 하는 스피커를 지정합니다. XProtect Smart Client 사용자는 필요에 따라 다른 스피커를 수동으로 선택할 수 있습니다. 카메라가 녹화할 때 관련 스피커가 녹음을 수행합니다.
관련 메타데이터	카메라에서 XProtect Smart Client 사용자가 데이터를 수신하는 하나 이상의 메타데이터 장치를 지정합니다. 카메라가 녹화할 때 관련 메타데이터 장치가 녹화를 수행합니다.
단축키	XProtect Smart Client 사용자에 대한 카메라 선택을 용이하게 하려면 카메라에 키보드 단축키를 정의합니다. • 고유하게 카메라를 식별하도록 각각의 단축키를 생성합니다 • 카메라 단축 번호는 4자리를 넘을 수 없습니다
라이브 멀티캐스트	이 시스템은 레코딩 서버에서 XProtect Smart Client 로 라이브 스트림의 멀티캐스트를 지원합니다. 카메라의 라이브 스트림의 멀티캐스트를 활성화하려면 확인란을 선택하십시오. 라이브 멀티캐스팅은 오직 **스트림** 탭에서 카메라의 기본 스트림으로 지정한 스트림에 대해서만 작동합니다. 또한 레코딩 서버에 대한 멀티캐스팅을 구성해야 합니다. 페이지 191의 레코딩 서버에 대한 멀티캐스팅 활성화를 참조하십시오. 레코딩 서버가 암호화를 사용하더라도 멀티캐스트 스트림은 암호화되지 않습니다.

사생활 보호 탭(장치)

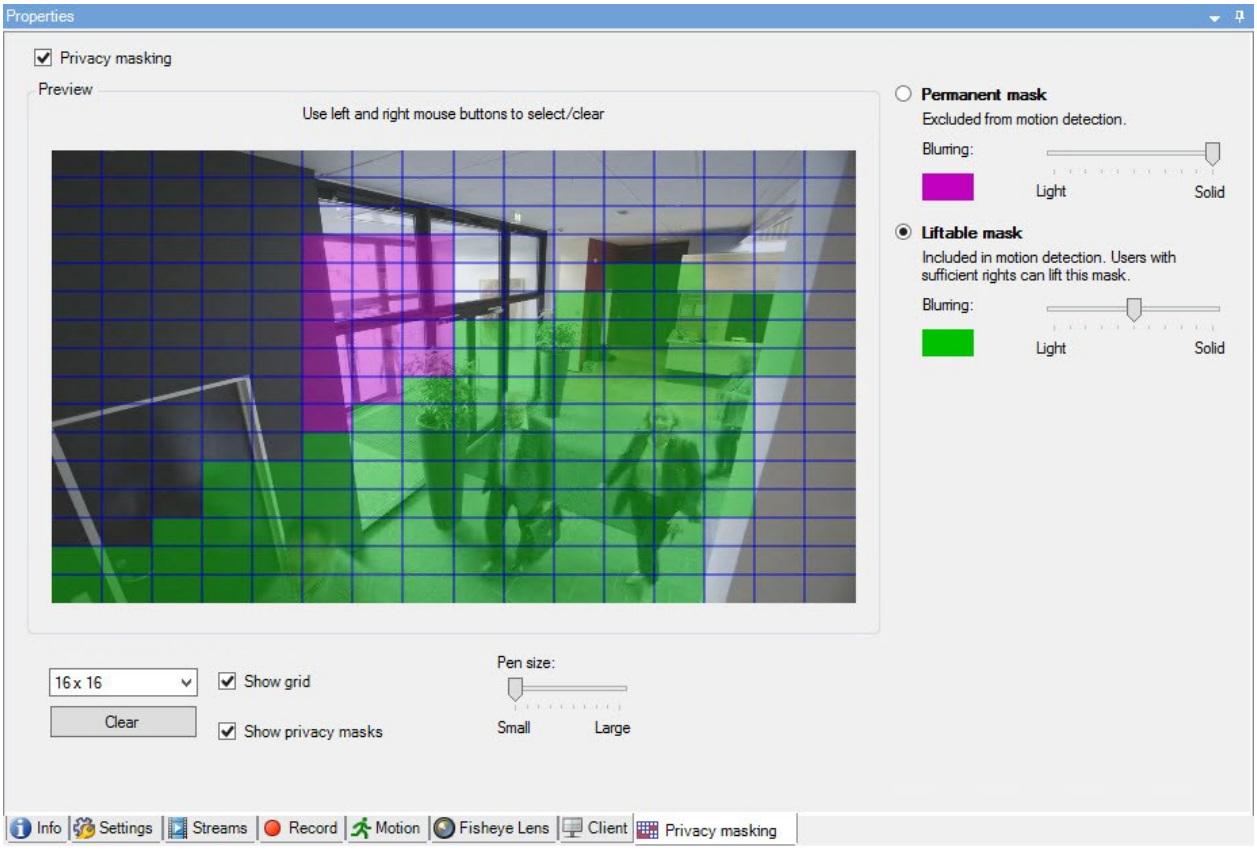
> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

XProtect Essential+ 2018 R1 이상은 사생활 보호를 지원하지 않으므로, 사생활 보호가 적용된 시스템에서 업그레이드 할 경우, 보호가 제거됩니다.

다음 장치에는 **사생활 보호** 탭이 있습니다:

- 카메라

사생활 보호 탭에서 선택한 카메라에 대해 사생활 보호를 활성화하고 구성할 수 있습니다.



사생활 보호 탭 상의 작업

이름	설명
사생활 보호	사생활 보호 활성화/비활성화 사생활 보호(설명됨)
영구적 보호 및 **일시적 보호**	영구적 또는 일시적 사생활 보호가 필요한 경우 정의합니다. 사생활 보호 정의

사생활 보호와 관련된 작업

작업	설명
사생활 보호 해제 권한을 가진 역할과 관련된 Smart Client 프로파일에 대한 일시적인 사생활 보호에 대한 시간 제한을 변경합니다.	해제된 사생활 보호의 제한 시간 변경
역할에 대한 사생활 보호 해제 권한을 활성화 또는 비활성화합니다.	사용자에게 사생활 보호 해제 권한 부여
카메라의 현재 사생활 보호 설정에 대한 정보가 포함된 장치 보고서를 생성합니다.	사생활 보호 구성에 대한 보고서 생성

사생활 보호 탭(속성)

이름	설명
그리드 크기	선택한 그리드 크기는 미리보기에 그리드의 표시 여부에 상관없이 그리드의 밀도를 결정합니다. 8×8, 16×16, 32×32 또는 64×64 중에서 값을 선택하십시오.

이름	설명
지우기	지정한 **모든** 사생활 보호를 지웁니다.
그리드 표시	그리드를 표시하려면 **그리드 표시** 확인란을 선택합니다.
사생활 보호 표시	**사생활 보호 표시** 확인란(기본)을 선택할 경, 우, 영구 사생활 보호가 미리보기에 자주색으로 표시되며 해제 가능 사생활 보호는 녹색으로 표시됩니다. Milestone 에서는 사용자와 사용자의 동료가 현재 사생활 보호 구성을 확인할 수 있도록 **사생활 보호 표시** 상자를 선택된 상태로 유지하도록 권장합니다.
펜 크기	그리드를 클릭해서 선택한 영역으로 끌 때 지정하려는 선택 크기를 나타내려면 **펜 크기** 슬라이더를 사용합니다. 기본값은 '작게'로 설정되어 있고, 이는 그리드에서 정사각형 하나와 동일합니다.
영구 보호	이 탭과 **모션** 탭에 미리보기에서 자주색으로 표시됩니다. 영구 사생활 보호는 XProtect Smart Client 에서 항상 적용되며 해제할 수 없습니다. 감시가 허용되지 않는 공공 장소와 같이 감시가 필요 없는 보호 영역에 사용될 수 있습니다. 모션 감지는 영구 보호에서 제외됩니다. 진하게 또는 약간 흐릿한 수준으로 사생활 보호의 적용 범위를 지정합니다. 적용 범위 설정은 라이브 및 레코딩된 비디오 모두에 적용됩니다.
해제 가능 보호	이 탭의 미리보기에 녹색으로 표시됩니다. 해제 가능 사생활 보호는 충분한 사용자 권한을 가진 사용자에 의해 XProtect Smart Client 에서 해제할 수 있습니다. 기본적으로, 사생활 보호는 30분 동안 또는 사용자가 다시 적용할 때까지 해제됩니다. 사생활 보호는 사용자가 액세스 권한을 가진 모든 카메라의 비디오에서 해제된다는 점을 유의하십시오. XProtect Smart Client 사용자가 사생활 보호 해제 권한이 없을 경우, 시스템은 해제를 승인할 권한을 가진 사용자에게 요청합니다. 진하게 또는 약간 흐릿한 수준으로 사생활 보호의 적용 범위를 지정합니다. 적용 범위 설정은 라이브 및 레코딩된 비디오 모두에 적용됩니다.
흐림 효과	슬라이더를 사용해 클라이언트에서 사생활 보호의 흐릿한 수준을 선택하거나 적용 범위를 진하게 설정합니다. 기본적으로, 영구 사생활 보호가 적용된 영역은 진한 불투명으로 표시됩니다. 기본적으로, 해제 가능 사생활 보호는 중간 정도로 흐릿하게 표시됩니다. 클라이언트 사용자가 구분할 수 있도록 영구 및 해제 가능 사생활 보호가 어떻게 표시되는지 알려줄 수 있습니다.

하드웨어 속성 창

시스템 내 각 레코딩 서버에 하드웨어를 추가하기 위한 여러 가지 옵션이 있습니다.

> ⚠ 하드웨어가 NAT 지원 라우터 또는 방화벽 뒤에 위치한 경우, 다른 포트 번호를 지정하고 하드웨어가 사용하는 포트 및 IP 주소를 매핑하도록 라우터/방화벽을 구성해야 할 수 있습니다.

하드웨어 추가 마법사를 이용하면 네트워크에서 카메라와 비디오 인코더와 같은 하드웨어를 손쉽게 감시하여 시스템상의 레코딩 서버에 추가할 수 있습니다. 또한 마법사는 Milestone Interconnect 설치에 대한 원격 레코딩 서버 추가하는 것을 도와줍니다. 한 번에 **하나의 레코딩 서버** 만 추가하십시오.

정보 탭(하드웨어)

원격 서버에 대한 **정보** 탭에 관한 정보는 페이지 394의 정보 탭(원격 서버)를 참조하십시오.

이름	설명
이름	이름을 입력하십시오. 하드웨어가 시스템과 클라이언트에 나열될 때마다 시스템이 이 이름을 사용합니다. 이 이름은 고유할 필요가 없습니다. 하드웨어의 이름을 변경한 경우, Management Client 에서 전역으로 이름이 변경됩니다.
설명	하드웨어의 설명을 입력합니다(선택 사항). 설명은 시스템 내 다수의 목록에 나타납니다. 예를 들어, **개요** 창의 하드웨어 이름 위에 마우스 포인터를 움직이면 나타납니다.
모델	하드웨어 모델을 식별합니다.
시리얼 번호	제조업체가 지정한 하드웨어 일련 번호입니다. 항상 그렇지는 않지만 일련 번호가 간혹 MAC 주소와 동일한 경우가 있습니다.
드라이버	하드웨어에 대한 연결을 처리하는 드라이버를 식별합니다.
IE	하드웨어 공급업체의 기본 홈 페이지를 엽니다. 하드웨어 관리 시 이 페이지를 사용할 수 있습니다.
주소	하드웨어 장치의 호스트 이름 또는 IP 주소입니다.

이름	설명
MAC 주소	시스템 하드웨어의 미디어 액세스 제어(MAC) 주소를 지정합니다. MAC 주소는 12자 16진수 숫자로, 네트워크상에 있는 각 하드웨어 부분을 고유하게 식별합니다.
펌웨어 버전:	하드웨어 장치의 펌웨어 버전. 시스템이 현재 버전을 표시하도록 하려면 펌웨어 업데이트를 한 후마다 **하드웨어 데이터 업데이트** 마법사를 실행합니다.
마지막에 변경된 암호	**최근 변경한 암호** 필드는 암호가 변경된 컴퓨터의 현지 시간 설정을 따라 최근 암호가 변경된 타임 스탬프를 보여줍니다.
마지막으로 업데이트된 하드웨어 데이터:	하드웨어 데이터의 마지막 업데이트 시간 및 일자.

설정 탭(하드웨어)

설정 탭에서 하드웨어의 설정을 확인하거나 편집할 수 있습니다.

> **설정** 탭의 내용은 선택한 하드웨어에 의해 결정되며, 하드웨어 유형에 따라 다릅니다. 일부 하드웨어 유형의 경우, **설정** 탭에 아무 내용이 표시되지 않거나 읽기 전용 내용만 표시됩니다.

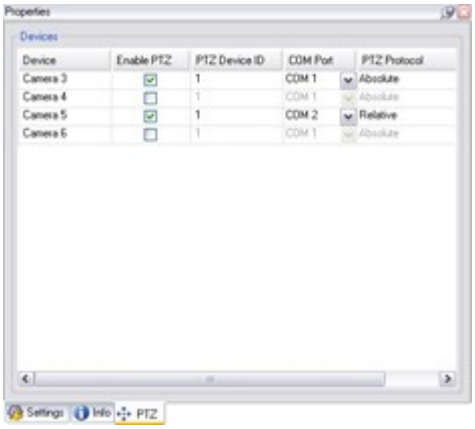
원격 서버에 대한 **설정** 탭에 관한 정보는 페이지 395의 설정 탭(원격 서버)를 참조하십시오.

PTZ 탭(비디오 인코더)

PTZ 탭에서 비디오 인코더에 대해 PTZ(이동-기울기-줌)를 활성화할 수 있습니다. 이 탭은 선택한 장치가 비디오 인코더이거나 드라이버가 비-PTZ 및 PTZ 카메라 모두를 지원하는 경우 사용할 수 있습니다.

비디오 인코더에 연결된 PTZ 카메라의 PTZ 기능을 사용하려면 **PTZ** 탭에서 각 비디오 인코더 채널에 대해 PTZ 사용을 별도로 활성화해야 합니다.

> 일부 비디오 인코더는 PTZ 카메라 사용을 지원하지 않습니다. PTZ 카메라 사용을 지원하는 비디오 인코더의 경우에도 PTZ 카메라를 사용하기 전에 구성이 필요할 수 있습니다. 일반적으로 장치의 IP 주소에서 브라우저 기반 구성 인터페이스를 통해 추가 드라이버를 설치하면 됩니다.



PTZ 탭, 비디오 인코더에서 두 채널에 대해 PTZ가 활성화된 상태.

클라이언트 노드

클라이언트(노드)

이 문서는 XProtect Smart Client 운영자 및 Management Client 의 시스템 관리자에 대한 사용자 인터페이스 사용자 정의 방법에 대해 설명합니다.

Smart Wall (클라이언트 노드)

Smart Wall 속성

정보 탭

Smart Wall 에 대한 **정보** 탭에서 Smart Wall 속성을 추가하고 편집할 수 있습니다.

이름	설명
이름	Smart Wall 정의의 이름. XProtect Smart Client 뷰 그룹 이름으로 Smart Wall 에 표시됩니다.
설명	Smart Wall 정의의 설명. 이 설명은 XProtect Management Client 에서 내부적으로만 사용됩니다.
상태 텍스트	카메라 뷰 항목에서 카메라와 시스템 상태 정보를 표시합니다.
제목 표시줄 없음	비디오 월의 모든 뷰 항목상의 제목 표시줄을 숨깁니다.
제목 표시줄	비디오 월의 모든 뷰 항목상의 제목 표시줄을 표시합니다.

프리셋 탭

Smart Wall 정의에 대한 **프리셋** 탭에서 Smart Wall 프리셋[1]을 추가하고 편집할 수 있습니다.

이름	설명
새로 추가	프리셋을 Smart Wall 정의에 추가합니다. 프리셋의 이름과 설명을 입력합니다.
편집	프리셋의 이름과 설명을 편집합니다.
삭제	프리셋을 삭제합니다.
활성화	프리셋을 사용하도록 구성된 Smart Wall 모니터에 프리셋을 적용합니다. 자동으로 프리셋을 적용하려면 프리셋을 사용하는 규칙을 생성해야 합니다.

레이아웃 탭

Smart Wall 정의에 대한 **레이아웃** 탭에서 모니터의 위치가 비디오 월에 있는 물리적 모니터의 장착 지점과 비슷한 곳에 자리하도록 모니터의 위치를 설정합니다. 또한 레이아웃은 XProtect Smart Client 에서도 사용됩니다.

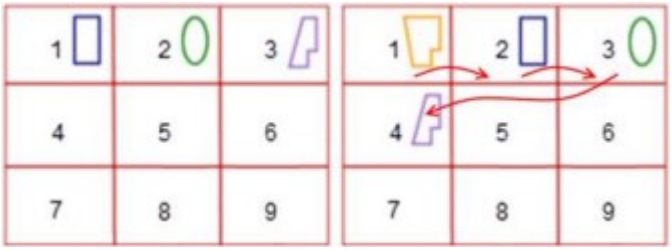
이름	설명
편집	모니터의 위치를 조정합니다.
이동	모니터를 새 위치로 이동하려면 모니터를 선택하고 원하는 위치로 드래그하거나 화살표 버튼 중 하나를 클릭하여 모니터를 선택한 방향으로 이동합니다.
줌 버튼	Smart Wall 레이아웃 미리보기를 줌인 줌아웃하여 모니터의 위치가 정확한지 확인합니다.
이름	모니터의 이름. 이 이름은 XProtect Smart Client 에 표시됩니다.
크기	비디오 벽에 있는 물리적 모니터의 크기.
종횡비	비디오 벽에 있는 물리적 모니터의 높이/너비 관계.

[1]Smart Wall 에서 사전 지정된 XProtect Smart Client 하나 이상의 모니터. 프리셋은 비디오 월의 각 모니터상에서 어떤 카메라가 표시되고 콘텐츠가 구성될지를 결정합니다.

모니터 속성

정보 탭

Smart Wall 프리셋의 모니터에 대한 **정보** 탭에서 모니터를 추가하고 모니터 설정을 편집할 수 있습니다.

이름	설명
이름	모니터의 이름. 이 이름은 XProtect Smart Client 에 표시됩니다.
설명	모니터에 대한 설명. 이 설명은 XProtect Management Client 에서 내부적으로만 사용됩니다.
크기	비디오 벽에 있는 물리적 모니터의 크기.
종횡비	비디오 벽에 있는 물리적 모니터의 높이/너비 관계.
빈 프리셋	Smart Wall 에서 새 XProtect Smart Client 프리셋이 트리거되거나 선택되었을 때 빈 프리셋 레이아웃이 포함된 모니터 상에 무엇을 표시해야 하는지 정의합니다. • 모니터에 현재 콘텐츠를 유지하려면 **보존** 을 선택합니다. • 모든 콘텐츠를 지워서 모니터에 아무 것도 표시되지 않게 하려면 **지우기** 를 선택합니다.
빈 프리셋 항목	Smart Wall 에서 새 XProtect Smart Client 프리셋이 트리거되거나 선택되었을 때 빈 프리셋 항목에서 무엇을 표시해야 하는지 정의합니다. • 레이아웃 항목에 현재 콘텐츠를 유지하려면 **보존** 을 선택합니다. • 콘텐츠를 지워서 레이아웃 항목에 아무 것도 표시되지 않게 하려면 **지우기** 를 선택합니다.
요소 삽입	카메라가 XProtect Smart Client 에서 조회되었을 때 카메라가 모니터 레이아웃이 삽입되는 방식을 정의합니다. • **독립** - 영향을 받은 레이아웃 항목 변경의 콘텐츠만, 레이아웃의 나머지 콘텐츠는 그대로 남아있게 됩니다. • **연결됨** - 레이아웃 항목의 콘텐츠가 왼쪽에서 오른쪽으로 푸시됩니다. 예를 들어 카메라가 위치 1에 삽입되었을 때 위치 1의 이전 카메라는 위치 2로 푸시되고 위치 2의 이전 카메라는 위치 3으로 푸시되며 이후 카메라에도 동일하게 적용됩니다. 그림은 이 예시를 보여줍니다. 

프리셋 탭

Smart Wall 프리셋에 있는 모니터의 **프리셋** 탭에서, 선택한 Smart Wall 프리셋의 모니터 뷰 레이아웃과 콘텐츠를 편집할 수 있습니다.

이름	설명
프리셋	선택한 Smart Wall 정의에 대한 Smart Wall 프리셋 목록.
편집	선택한 모니터의 레이아웃과 컨텐츠를 편집하려면 **편집** 을 클릭합니다. 카메라를 두 번 클릭하여 제거합니다. 새 레이아웃을 정의하거나 모니터를 Smart Wall 프리셋에서 제어되지 않는 다른 콘텐츠에 사용할 수 있도록 Smart Wall 프리셋에서 해당 모니터를 제외하려면 **지우기** 를 클릭합니다. 을(를) 클릭하여 사용 중인 모니터와 함께 사용하고자 하는 레이아웃을 선택한 후 **확인** 을 클릭합니다.

Smart Client 프로파일(클라이언트 노드)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

다음 탭에서 각 Smart Client 프로필의 속성을 지정할 수 있습니다. Management Client 의 사용자가 설정을 변경할 수 없도록 필요한 경우 XProtect Smart Client 에서 설정을 잠글 수 있습니다.

Smart Client 프로필을 만들거나 편집하려면 **클라이언트**를 확장하여 **Smart Client프로필**을 선택합니다.

정보 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
정보	기존 프로파일의 이름 및 설명, 우선순위, 해당 프로파일을 사용하는 역할에 대한 개요입니다. 사용자가 둘 이상 역할의 구성원이고, 각각이 개별 Smart Client 프로파일을 가진 경우, 해당 사용자는 최고 우선순위를 가진 Smart Client 프로파일을 사용합니다.

일반 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
일반	메뉴 설정 표시/숨기기, 최소화 및 최대화, 로그인/로그아웃, 시작, 시간 제한, 정보 및 메시징 옵션, XProtect Smart Client 내 특정 탭 활성화/비활성화 등과 같은 설정입니다. **카메라 오류 메시지**, **서버 오류 메시지** 및 **라이브 비디오 오류 메시지** 설정을 통해 이러한 오류 메시지가 오버레이로 표시되는지, 오버레이가 있는 검은색 이미지로 표시되는지 또는 숨겨져 있는지 제어할 수 있습니다. 카메라 라이브 피드가 중지되면 XProtect Smart Client에 **라이브 비디오 중지 메시지**가 표시됩니다. 예를 들어 카메라가 연결되어 있는데도 이미지 전송을 중지한 경우입니다. ⚠ 카메라 오류 메시지를 **숨기기** 하는 경우, 카메라 연결이 끊긴 상황을 운영자가 간과하게 될 위험이 있습니다. **검색 중 허용된 카메라** 설정으로 운영자가 XProtect Smart Client 에서의 검색에 추가할 수 있는 카메라의 수를 제어할 수 있습니다. 카메라 제한을 설정하여 시스템 과부하를 막을 수 있습니다. **온라인 도움말** 설정을 통해 XProtect Smart Client 에서 도움말 시스템을 비활성화할 수 있습니다. **비디오 튜토리얼** 설정을 통해 XProtect Smart Client 에 있는 **비디오 튜토리얼** 버튼을 비활성화할 수 있습니다. 운영자가 해당 버튼을 사용하면 비디오 튜토리얼 페이지로 이동하게 됩니다: https://www.milestonesys.com/support/help-yourself/video-tutorials/

고급 탭(Smart Client 프로파일)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
고급	최대 디코딩 스레드, 디인터레이스, 시간대 설정 등과 같은 고급 설정입니다. **최대 디코딩 스레드** 는 비디오 스트림을 디코딩하는 데 사용되는 디코딩 스레드 수를 제어합니다. 이 설정을 사용하면 라이브 및 재생 모드에서 멀티 코어 컴퓨터의 성능이 향상됩니다. 정확한 성능 향상은 비디오 스트림에 따라 다릅니다. 이 설정은 주로 성능이 크게 향상될 가능성이 있는 H.264/H.265와 같은 코딩된 고

탭	설명
	해상도 비디오 스트림을 사용하는 경우와 관련되어 있으며, JPEG나 MPEG-4 등을 사용하는 경우와는 관련이 별로 없습니다. **디인터레이스** 를 사용하여 비디오를 비인터레이스 형식으로 변환합니다. 인터레이스는 이미지가 화면에서 새로 고쳐지는 방식을 결정합니다. 이미지의 홀수 선을 먼저 스캔한 다음, 짝수 선을 스캔하는 방식으로 이미지가 새로 고쳐집니다. 따라서 각 스캔 중에 처리되는 정보가 적기 때문에 새로 고침 속도가 더 빠릅니다. 하지만 인터레이스로 인해 깜박임이 발생하거나 이미지 선의 절반에서 수행된 변경 사항만 표시될 수 있습니다. **적응 스트리밍** 은 XProtect Smart Client 이(가) 뷰 항목을 따라 요청된 스트림에 대해 가장 일치하는 해상도의 라이브 비디오 스트림을 자동으로 선택하게 해줍니다. 이렇게 함으로써 CPU와 GPU의 처리량이 줄어들며 컴퓨터의 디코딩 기능과 성능이 개선됩니다. 여기에는 각기 다른 해상도로 구성된 라이브 비디오 스트림의 멀티스트리밍이 필요합니다. 멀티스트리밍 관리 를 참조하십시오. 적응형 스트리밍은 라이브 및 재생 모드에서 적용할 수 있습니다. 재생 모드에서는 적응형 스트리밍을 적응형 재생이라고 합니다. 적응형 재생을 하려면 두 가지 스트림을 레코딩으로 설정해야 합니다. 라이브 모드에서 적응형 스트리밍을 위해 스트림 추가하기 및 적응형 재생을 위해 스트림 추가하는 방법에 대한 자세한 내용은 페이지 215의 스트림 추가을 참고하십시오.

라이브 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
실시간	라이브 모드 및 기타 라이브 기능, 카메라 재생, 카메라 오버레이 버튼, 바운딩 박스, 라이브 관련 MIP플러그인의 이용 가능 여부.

재생 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
재생	재생 모드 및 기타 재생 기능, 인쇄 보고서 레이아웃, 독립적 재생, 북마크, 바운딩 박스, 재생 관련 MIP플러그 인의 이용 가능 여부.

설정 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
설정	일반 설정/창/버튼, 설정 관련 MIP 플러그 인 및 맵 편집과 라이브 비디오 버퍼링 편집 권한의 이용 가능 여부.

내보내기 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
내보내기	경로, 사생활 보호, 비디오 및 스틸 이미지 형식 그리고 이들을 내보내기 할 때 포함시킬 사항, XProtect Smart Client – Player 에 대한 내보내기 형식 등입니다.

타임라인 탭 (Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
타임라인	오디오 포함 여부, 시간 및 모션 표시 여부, 재생 간격 처리 방법. 다른 소스의 추가 데이터 또는 추가 마커를 표시할 것인지 여부를 선택할 수도 있습니다.

액세스 제어 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
액세스 제어	이벤트에 의해 트리거될 때 XProtect Smart Client 화면에 액세스 요청 알림을 팝업으로 표시할지 여부를 선택합니다.

알람 관리자 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
알람 관리자	다음 사항의 여부를 지정합니다. • 알람에 대한 데스크톱 알림은 XProtect Smart Client이(가) 설치된 컴퓨터에 표시되어야 합니다. 알림은 XProtect Smart Client이(가) 구동 중(최소화되었을 때 포함)일 때에만 표시됩니다. 알람을 위한 데스크톱 알림은 알람이 특정 우선순위를 지닐 때(예: **중간** 또는 **높음**)에만 표시됩니다. 알림을 트리거하는 알람의 우선순위를 구성하려면 **알람** > **알람 데이터 설정** > **알람 데이터 수준** 으로 이동하십시오. 각 필수 알람 우선순위에 대해 **데스크톱 알림 활성화** 체크박스를 선택합니다. 알람 데이터 설정(알람 노드) 를 참조하십시오. • 알람에 대한 경고음은 XProtect Smart Client이(가) 설치된 컴퓨터에서 재생되어야 합니다. 경고음은 XProtect Smart Client이(가) 구동 중(최소화되었을 때 포함)일 때에만 재생됩니다. 알람에 대한 경고음은 소리가 알람과 연결된 경우에만 재생됩니다. 소리를 알람과 연결하려면 **알람** > **알람 데이터 설정** > **알람 데이터 레벨**로 이동합니다. 각 필수 알람 우선순위에 대해 알람과 연관시킬 사운드를 선택합니다. 알람 데이터 설정(알람 노드) 를 참조하십시오.

스마트 맵 탭(Smart Client 프로필)

이 탭은 다음과 같은 속성을 지정할 수 있도록 합니다:

탭	설명
스마트 맵	스마트 맵 기능에 대한 설정을 지정합니다. 다음 사항의 여부를 지정할 수 있습니다. • Milestone Map Service 이(가) 지리적 배경으로 사용 가능한지 여부

탭	설명
	• OpenStreetMaps을 지리적 배경으로 사용 가능한지 여부 • XProtect Smart Client 이(가) 사용자가 스마트 맵에 사용자 정의 오버레이 추가 시 자동으로 위치를 생성할지 여부. 또는 시스템이 컴퓨터에서 스마트 맵과 관련된 데이터를 삭제할 빈도를 지정할 수 있습니다. XProtect Smart Client 이(가) 스마트 맵을 더 빠르게 표시하도록 하기 위해, 클라이언트는 컴퓨터의 캐시에 맵의 데이터를 저장합니다. 시간이 지남에 따라 컴퓨터 속도가 느려질 수 있습니다. 캐싱은 Google Maps에는 적용되지 않습니다. Bing Maps 또는 Google Maps 를 지리적 배경으로 사용하고자 하는 경우, Bing Maps API 키 또는 Google 에서 Maps Static API 키를 입력합니다.

Management Client 프로파일(클라이언트 노드)

이 기능은 XProtect Corporate에서만 사용할 수 있습니다.

정보 탭(Management Client 프로필)

정보 탭에서 Management Client 프로파일에 대해 다음을 설정할 수 있습니다:

구성 요소	요구사항
이름	Management Client 프로파일의 이름을 입력합니다.
우선순위	위/아래 화살표를 사용하여 Management Client 프로파일의 우선순위를 설정합니다.
설명	프로파일의 설명을 입력합니다. 이것은 옵션입니다.
Management Client 프로파일 을 사용하는 역할	이 필드에는 Management Client 프로파일과 연결한 역할이 표시됩니다. 이 항목은 편집할 수 없습니다.

프로필 탭(Management Client 프로필)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

프로파일 탭에서, ManagementClient의 사용자 인터페이스에 다음 요소의 표시 여부를 활성화하거나 비활성화할 수 있습니다:

탐색

이 섹션에서는 Management Client 프로파일에 연결된 관리자 사용자가 **탐색** 창에 있는 여러 특징과 기능을 볼 수 있는지 결정합니다.

탐색 요소	설명
기본	Management Client 프로파일에 연결된 관리자 사용자가 **라이선스 정보** 와 **사이트 정보** 를 볼 수 있습니다.
원격 연결 서비스	Management Client 프로필에 연결된 관리자 사용자가 **Axis One-click 카메라 연결** 을 볼 수 있도록 허용합니다.
서버	Management Client 프로파일에 연결된 관리자 사용자가 **레코딩 서버** 와 **장애 조치 서버** 를 볼 수 있습니다.
장치	Management Client 프로파일에 연결된 관리자 사용자가 **카메라**, **마이크**, **스피커**, **메타데이터**, **입력** 및 **출력** 을 볼 수 있습니다.
클라이언트	Management Client 프로파일에 연결된 관리자 사용자가 **Smart Wall**, **뷰 그룹**, **Smart Client 프로파일**, **Management Client 프로파일** 및 **Matrix** 을(를) 볼 수 있습니다.
규칙 및 이벤트	Management Client 프로파일에 연결된 관리자 사용자가 **규칙**, **시간 프로파일**, **알림 프로파일**, **사용자 정의 이벤트**, **분석 이벤트** 및 **일반 이벤트** 를 볼 수 있습니다.
보안	Management Client 프로파일에 연결된 관리자 사용자가 **역할** 및 **기본 사용자** 를 볼 수 있습니다.
시스템 대시보드	Management Client 프로필에 연결된 관리자 사용자가 **시스템 모니터**, **시스템 모니터 임계값**, **증거물 잠금**, **현재 작업** 및 **구성 보고서** 를 볼 수 있도록 허용합니다.

탐색 요소	설명
서버 로그	Management Client 프로필에 연결된 관리자 사용자가 시스템, 감사 및 규칙 트리거 로그를 볼 수 있도록 허용합니다.
액세스 제어	시스템에 액세스 제어 시스템 통합 또는 플러그인을 추가한 경우, Management Client 프로파일에 연결된 관리자 사용자가 **액세스 제어** 기능을 볼 수 있습니다.

세부 정보

이 섹션에서는 Management Client 프로파일에 연결된 관리자 사용자가 특정 장치 채널에 대한 여러 탭을 볼 수 있는지 여부를 결정합니다(예: 카메라의 **설정** 탭 또는 **레코드** 탭).

장치 채널	설명
카메라	Management Client 프로파일에 연결된 관리자 사용자가 카메라 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.
마이크	Management Client 프로파일에 연결된 관리자 사용자가 마이크 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.
스피커	Management Client 프로파일에 연결된 관리자 사용자가 스피커 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.
메타데이터	Management Client 프로파일에 연결된 관리자 사용자가 메타데이터 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.
입력	Management Client 프로파일에 연결된 관리자 사용자가 입력 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.
출력	Management Client 프로파일에 연결된 관리자 사용자가 출력 관련 설정 및 탭의 일부나 전체를 볼 수 있습니다.

도구 메뉴

이 섹션에서는 Management Client 프로파일에 연결된 관리자 사용자가 **도구** 메뉴에 포함된 요소를 볼 수 있는지 여부를 결정합니다.

도구 메뉴 옵션	설명
등록된 서비스	Management Client 프로파일에 연결된 관리자 사용자가 **등록된 서비스** 를 볼 수 있습니다.
유효 역할	Management Client 프로파일에 연결된 관리자 사용자가 **유효 역할** 을 볼 수 있습니다.
옵션	Management Client 프로파일에 연결된 관리자 사용자가 **옵션** 을 볼 수 있습니다.

연합 사이트

이 섹션에서는 Management Client 프로파일에 연결된 관리자 사용자가 **연합 사이트 계층** 구조 창을 볼 수 있는지 여부를 결정합니다.

규칙 및 이벤트 노드

규칙(규칙 및 이벤트 노드)

시스템에는 아무 것도 설치하지 않고 기본적인 기능을 사용할 수 있는 여러 기본 규칙이 포함되어 있습니다. 필요에 따라 기본 규칙을 비활성화하거나 수정할 수 있습니다. 기본 규칙을 수정하거나 비활성화할 경우, 시스템이 원하는 대로 작동하지 않을 수 있고 비디오 피드 또는 오디오 피드가 시스템으로 자동 전송되지 않을 수도 있습니다.

기본 규칙	설명
PTZ 완료 시 프리셋으로 이동	PTZ 카메라를 수동으로 조작한 후 카메라가 해당하는 기본 프리셋 위치로 이동합니다. 이 규칙은 기본적으로 활성화되어 있지 않습니다. 규칙을 활성화한 경우라도 규칙이 작동하기 위해서는 해당 PTZ 카메라의 기본 프리셋 위치가 정의되어 있어야 합니다. 이 작업은 **프리셋** 탭에서 수행합니다.
요청 시 오디오 재생	외부 요청이 발생할 때 비디오가 자동으로 녹화됩니다. 요청은 항상 사용 중인 시스템과 외부적으로 통합된 시스템에 의해 트리거되며, 이 규칙은 주로 외부 시스템 또는 플러그 인 통합자에 의해 사용됩니다.
북마크 시 레코딩	운영자가 XProtect Smart Client 에서 북마크를 설정할 때 비디오가 자동으로 녹화됩니다. 이는 해당 카메라에 대한 레코딩을 활성화한 경우 해당합니다. 레코딩은 기본적으로 활성화되어 있습니다. 이 규칙의 기본 레코딩 시간은 북마크가 설정되기 3초 전과 북마크가 설정된 후 30초입니다. 규칙에서 기

기본 규칙	설명
	본 레코딩 시간을 편집할 수 있습니다. 레코딩 탭에서 설정한 사전-버퍼가 사전-레코딩 시간과 같거나 더 길어야 합니다.
모션 시 레코딩	해당 카메라에 대해 레코딩이 활성화된 경우, 카메라의 비디오에서 모션이 감지되면 비디오가 녹화됩니다. 레코딩은 기본적으로 활성화되어 있습니다. 기본 규칙에 따라 모션이 감지되면 레코딩이 되지만, 하나 이상의 카메라에 대해 개별 카메라 레코딩을 비활성화했을 수 있으므로 시스템이 비디오를 반드시 녹화한다고 보장할 수는 없습니다. 레코딩을 활성화한 경우라도 레코딩 품질이 개별 카메라의 레코딩 설정에 의해 영향을 받을 수 있다는 점을 유념하십시오.
요청 시 레코딩	해당 카메라에 대해 레코딩이 활성화된 경우, 외부 요청이 발생하면 비디오가 자동으로 녹화됩니다. 레코딩은 기본적으로 활성화되어 있습니다. 요청은 항상 사용 중인 시스템과 외부적으로 통합된 시스템에 의해 트리거되며, 이 규칙은 주로 외부 시스템 또는 플러그 인 통합자에 의해 사용됩니다.
시작 오디오 피드	연결된 모든 마이크 및 스피커의 오디오 피드가 시스템으로 자동으로 전달됩니다. 기본 규칙에 따라 시스템 설치 후 바로 연결된 마이크 및 스피커의 오디오 피드에 대한 액세스가 활성화되지만, 레코딩 설정을 별도로 지정해야 하므로 오디오가 녹음된다는 보장이 없습니다.
시작 피드	연결된 카메라의 비디오 피드가 시스템으로 자동으로 전달됩니다. 기본 규칙에 따라 시스템 설치 후 바로 연결된 카메라의 비디오 피드에 대한 액세스가 활성화되지만, 카메라의 레코딩 설정을 별도로 지정해야 하므로 비디오가 녹화된다는 보장이 없습니다.
시작 메타데이터 피드	연결된 카메라의 데이터 피드가 시스템으로 자동으로 전달됩니다. 기본 규칙에 따라 시스템 설치 후 바로 연결된 카메라의 데이터 피드에 대한 액세스가 활성화되지만, 카메라의 레코딩 설정을 별도로 지정해야 하므로 데이터가 반드시 기록되지는 않습니다.
액세스 요청 알림 표시	XProtect Smart Client 프로파일에서 알림 기능이 비활성화된 경우가 아니면 '액세스 요청'으로 분류된 모든 액세스 제어 이벤트로 인해 Smart Client 에 액세스 요청 알림이 팝업으로 표시되게 합니다.

기본 규칙 재생성

실수로 기본 규칙을 삭제한 경우 다음 내용을 입력해서 해당 규칙을 다시 생성할 수 있습니다:

기본 규칙	입력할 텍스트
PTZ 완료 시 프리셋으로 이동	PTZ 수동 세션 중지됨 발생 시 모든 카메라에서 작업 수행 이벤트가 발생한 장치의 기본 프리셋으로 즉시 이동
요청 시 오디오 재생	외부에서 오디오 메시지 재생 요청에 대한 동작을 수행 우선 순위 1을 가진 메타데이터에서 장치의 메타데이터로부터 오디오 메시지를 재생합니다
북마크 시 레코딩	북마크 참조 요청 시 모든 카메라, 모든 마이크, 모든 스피커에서 작업을 수행. 장치에서 이벤트가 발생하기 3초 전 레코딩 시작 레코딩 중지하고 30초 후 즉시 작업 수행
모션 시 레코딩	모션 시작 시 모든 카메라에서 작업 수행. 장치에서 이벤트가 발생하기 3초 전 레코딩 시작 모션이 중지된 경우 모든 카메라에서 3초 후 중지 작업 수행
요청 시 레코딩	레코딩 시작 요청 시 외부에서 작업 수행. 메타데이터로부터 장치에 즉시 레코딩 시작 레코딩 중지 요청 시 외부에서 중지 작업 수행. 레코딩 즉시 중지
시작 오디오 피드	시간 간격을 두고 작업 수행. 모든 마이크, 모든 스피커에서 항상 시작 피드 시간 간격 종료 시 작업 수행. 피드 즉시 중지
시작 피드	시간 간격을 두고 작업 수행. 모든 카메라에서 항상 시작 피드 시간 간격 종료 시 작업 수행. 피드 즉시 중지
시작 메타데이터 피드	시간 간격을 두고 작업 수행. 모든 메타데이터에서 항상 시작 피드 시간 간격 종료 시 작업 수행. 피드 즉시 중지
액세스 요청 알림 표시	액세스 요청 시(액세스 제어 카테고리) 시스템[+ 장치]에서 동작 수행 기본 제공 액세스 요청 알림 표시

알림 프로파일(규칙 및 이벤트 노드)

알림 프로파일에 대해 다음 속성을 지정합니다:

구성 요소	요구사항
이름	알림 프로파일의 설명 이름을 입력합니다. 이 이름은 나중에 규칙 생성 프로세스 중 알림 프로파일을 선택할 때마다 나타납니다.
설명(옵션)	알림 프로파일의 설명을 입력합니다. 이 설명은 개요 창의 **알림 프로파일** 목록에 있는 알림 프로파일 위로 마우스 포인터를 가져가면 나타납니다.
수신자	알림 프로파일의 이메일 알림을 전송할 이메일 주소를 입력합니다. 둘 이상의 주소를 입력하려면 세미콜론으로 주소를 구분하십시오. 예: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
제목	이메일 알림의 제목에 나타날 텍스트를 입력합니다. 제목 및 메시지 텍스트 필드에 **장치 이름** 등의 시스템 변수를 삽입할 수 있습니다. 변수를 삽입하려면 필드 아래 상자에서 필요한 변수 링크를 클릭합니다.
메시지 텍스트	이메일 알림의 본문에 나타날 텍스트를 입력합니다. 메시지 텍스트 이외에 각 이메일 알림의 본문에는 이 정보가 자동으로 포함됩니다: • 이메일 알림을 트리거한 요인 • 첨부된 스틸 이미지 또는 AVI 비디오 클립의 소스
이메일 사이의 시간	각 이메일 알림 전송 사이에 경과되는 최소 필요 시간(초 단위)을 지정합니다. 예: • **120** 값을 지정한 경우, 2분이 경과하기 전에 규칙에 의해 알림 프로파일이 다시 트리거된 경우라도 각 이메일 알림 전송 사이에 최소 2분이 경과합니다 • **0** 값을 지정하면 알림 프로파일이 규칙에 의해 트리거될 때마다 이메일 알림이 전송됩니다. 이는 잠재적으로 매우 많은 수의 이메일 알림이 전송되는 결과를 가져올 수 있습니다. 따라서 **0** 값을 사용하는 경우, 자주 트리거될 수 있는 규칙에서 알림 프로파일을 사용할지 여부를 신중히 고려해야 합니다
이미지 수	알림 프로파일의 이메일 알림 각각에 포함시킬 최대 스틸 이미지 수를 지정합니다. 기본값은 이미지 5개입니다.
이미지 사이의 시간 (ms)	포함된 이미지에 나타나는 레코딩 사이에 원하는 밀리초 수를 지정합니다. 예: 기본값 500밀리초를 사용할 경우, 포함된 이미지에서 1/2초 간격으로 레코딩을 표시합니다.
이벤트 이전 시	이 설정은 AVI 파일의 시작을 지정하는 데 사용됩니다. 기본적으로 AVI 파일에는 알림 프로파일이 트리거되기 2초 전부터의 레코딩이 포함됩니다. 이 설정을 필요한 초 수로 변경할 수 있습니다.

구성 요소	요구사항
간(초)	
이벤트 이후 시간(초)	이 설정은 AVI 파일의 끝을 지정하는 데 사용됩니다. 기본적으로 AVI 파일은 알림 프로파일이 트리거되고 4초 후에 종료됩니다. 이 설정을 필요한 초 수로 변경할 수 있습니다.
프레임 속도	AVI 파일을 포함시킬 초당 프레임 수를 지정합니다. 기본값은 초당 5개 프레임입니다. 프레임 속도가 높을수록 이미지 품질이 높아지고 AVI 파일 크기가 커집니다.
이메일에 이미지 포함	선택하면(기본값) 이미지가 이메일 알림의 본문에 삽입됩니다. 선택하지 않을 경우, 이미지가 이메일 알림에 첨부 파일로 포함됩니다.

이벤트 개요

규칙 관리 마법사에서 이벤트 기반 규칙을 추가할 때 여러 다른 이벤트 유형 중에서 선택할 수 있습니다. 올바른 개요를 확인할 수 있도록 다음 기준에 따라 선택할 수 있는 이벤트가 그룹에 나열됩니다.

하드웨어:

일부 하드웨어는 자체적으로 이벤트(예: 모션 감지)를 생성할 수 있습니다. 이들을 이벤트로 사용할 수 있지만, 시스템에서 사용하려면 하드웨어에서 해당 항목을 구성해야 합니다. 일부 카메라 유형은 조작 또는 온도 변화를 감지할 수 없기 때문에 일부 하드웨어에 나열된 이벤트만 사용할 수 있습니다.

하드웨어 - 구성 가능한 이벤트:

하드웨어에서 구성 가능한 이벤트는 장치 드라이버에서 자동으로 가져옵니다. 즉, 이러한 이벤트는 하드웨어마다 다르므로 여기서 설명하지 않습니다. 구성 가능한 이벤트는 시스템에 추가하여 하드웨어에 대한 **이벤트** 탭에서 구성하기 전까지는 트리거되지 않습니다. 또한 구성 가능한 일부 이벤트를 사용하려면 카메라(하드웨어) 자체를 구성해야 합니다.

하드웨어 - 사전 정의된 이벤트:

이벤트	설명
통신 오류(하드웨어)	하드웨어 연결이 끊겼을 때 발생합니다.
통신 시작됨(하드웨어)	하드웨어와의 통신이 성공적으로 설정될 때 발생합니다.
통신 중단됨(하드웨어)	하드웨어와의 통신이 성공적으로 중지될 때 발생합니다.

장치 - 구성 가능한 이벤트:

장치에서 구성 가능한 이벤트는 장치 드라이버에서 자동으로 가져옵니다. 즉, 이러한 이벤트는 장치마다 다르므로 여기서 설명하지 않습니다. 구성 가능한 이벤트는 시스템에 추가하여 장치의 **이벤트** 탭에서 구성하기 전까지는 트리거되지 않습니다.

장치 - 사전 정의된 이벤트:

이벤트	설명
북마크 참조 요청됨	클라이언트 내에서 라이브 모드로 북마크가 생성될 시 발생합니다. 또한 북마크 규칙의 디폴트 레코드를 사용하기 위한 요구 사항에 해당합니다.
통신 오류(장치)	장치 연결이 끊겼거나 장치와의 통신 시도가 이루어졌으나 실패했을 때 발생합니다.
통신 시작됨(장치)	장치와의 통신이 성공적으로 설정될 때 발생합니다.
통신 중지됨(장치)	장치와의 통신이 성공적으로 중지될 때 발생합니다.
증거물 잠금 변경됨	클라이언트 사용자에 의해 또는 MIP SDK 을(를) 통해 장치에 대한 증거물 잠금이 변경될 때 발생합니다.
증거물 잠김	클라이언트 사용자에 의해 또는 MIP SDK 을(를(통해 장치에 대한 증거물 잠금이 생성될 때 발생합니다.
증거물 잠금 해제됨	클라이언트 사용자에 의해 또는 MIP SDK 을(를) 통해 장치에 대한 증거물 잠금이 제거될 때 발생합니다.
피드 오버플로 시작됨	피드 오버플로(미디어 오버플로)는 레코딩 서버가 수신된 데이터를 구성에 지정된 대로 신속히 처리할 수 없어 강제로 일부 레코딩을 삭제할 때 발생합니다. 서버 상태가 양호한 경우, 일반적으로 피드 오버플로는 느린 디스크 쓰기 속도로 인해 발생합니다. 기록

이벤트	설명
	된 데이터 양을 줄이거나 저장소 시스템의 성능을 개선하여 이 문제를 해결할 수 있습니다. 카메라에서 프레임 속도, 해상도 또는 이미지 품질을 낮춰 기록된 데이터 양을 줄일 수 있지만, 이렇게 하면 레코딩 품질이 저하될 수 있습니다. 이를 원치 않으면 부하를 공유할 추가 드라이브를 설치하거나 더 빠른 디스크나 컨트롤러를 설치해 저장소 시스템의 성능을 개선하십시오. 이 이벤트를 사용해 문제를 방지하는 데 도움이 되는 동작(예: 레코딩 프레임 속도 낮추기)을 트리거할 수 있습니다.
피드 오버플로 중지됨	피드 오버플로가(페이지 441의 피드 오버플로 시작됨 참조) 종료 시 발생합니다.
라이브 클라이언트 피드 요청됨	클라이언트 사용자가 장치에서 라이브 스트림을 요청할 때 발생합니다. 이 이벤트는 클라이언트 사용자에게 요청한 라이브 피드를 볼 수 있는 권한이 없거나 특정 이유로 피드가 중지된 경우 등과 같이 클라이언트 사용자의 요청이 나중에 실패한 것으로 나타난 경우라도 요청 시 발생하게 됩니다.
라이브 클라이언트 피드 중단됨	클라이언트 사용자가 더 이상 장치에서 라이브 스트림을 요청하지 않을 때 발생합니다.
수동 녹화 시작됨	클라이언트 사용자가 카메라에 대한 레코딩 세션을 시작할 때 발생합니다. 이 이벤트는 장치가 이미 규칙 동작을 통해 레코딩 중이라도 트리거됩니다.
수동 녹화 중지됨	클라이언트 사용자가 카메라에 대한 레코딩 세션을 중지할 때 발생합니다. 또한 규칙 시스템이 레코딩 세션을 시작한 경우, 수동 레코딩이 중지된 후에도 레코딩이 계속됩니다.
표시된 데이터 참조 요청됨	증거물 잠금이 클라이언트의 재생 모드 또는 MIP SDK 을(를) 통해 이루어질 때 발생합니다. 규칙에서 사용 가능한 이벤트가 만들어집니다.
모션 시작됨	시스템이 카메라에서 수신된 비디오에서 모션을 감지할 때 발생합니다. 이 이벤트 유형을 사용하려면 이벤트가 연결된 카메라에 대해 시스템의 모션 감지가 활성화되어 있어야 합니다.

이벤트	설명
	시스템의 모션 감지 이외에 일부 카메라는 자체적으로 모션을 감지하여 **모션 시작됨(HW)** 이벤트를 트리거할 수 있지만, 이는 시스템 및 카메라 하드웨어의 구성에 따라 다릅니다. 또한 페이지 440의 하드웨어 - 구성 가능한 이벤트:를 참조하십시오.
모션 중지됨	수신된 비디오에서 모션이 더 이상 감지되지 않을 때 발생합니다. 또한 페이지 442의 모션 시작됨를 참조하십시오. 이 이벤트 유형을 사용하려면 이벤트가 연결된 카메라에 대해 시스템의 모션 감지가 활성화되어 있어야 합니다. 시스템의 모션 감지 이외에 일부 카메라는 자체적으로 모션을 감지하여 모션 중지됨(HW) 이벤트를 트리거할 수 있지만, 이는 시스템 및 카메라 하드웨어의 구성에 따라 다릅니다. 또한 페이지 440의 하드웨어 - 구성 가능한 이벤트:를 참조하십시오.
출력 활성화됨	장치의 외부 출력 포트가 활성화될 때 발생합니다. 이 이벤트 유형을 사용하려면 시스템에 있는 하나 이상의 장치가 출력 포트를 지원해야 합니다.
출력 변경됨	장치의 외부 출력 포트 상태가 변경될 때 발생합니다. 이 이벤트 유형을 사용하려면 시스템에 있는 하나 이상의 장치가 출력 포트를 지원해야 합니다.
출력 비활성화됨	장치의 외부 출력 포트가 비활성화될 때 발생합니다. 이 이벤트 유형을 사용하려면 시스템에 있는 하나 이상의 장치가 출력 포트를 지원해야 합니다.
PTZ 수동 세션 시작됨	카메라에서 수동으로 조작한 PTZ 세션(예약된 순찰 또는 이벤트에 의해 자동으로 트리거되는 PTZ 세션과 반대)이 시작될 때 발생합니다. 이 이벤트 유형을 사용하려면 해당 이벤트가 연결되는 장치가 PTZ 장치여야 합니다.
PTZ 수동 세션 중지됨	카메라에서 수동으로 조작한 PTZ 세션(예약된 순찰 또는 이벤트에 의해 자동으로 트리거되는 PTZ 세션과 반대)이 중지될 때 발생합니다. 이 이벤트 유형을 사용하려면 해당 이벤트가 연결되는 장치가 PTZ 장치여야 합니다.
녹화 시작됨	레코딩이 시작할 때 발생합니다. 시작된 수동 녹화에 대한 별도의 이벤트가 있습니다.
녹화 중지됨	레코딩이 중지할 때 발생합니다. 중지된 수동 녹화에 대한 별도의 이벤트가 있습니다.
설정 변	장치의 설정이 성공적으로 변경될 때 발생합니다.

이벤트	설명
경됨	
설정 변경 오류	장치의 설정을 변경하는 시도가 이루어졌으나 해당 시도가 실패했을 때 발생합니다.

외부 이벤트 - 사전 정의된 이벤트:

이벤트	설명
오디오 메시지 재생 요청	오디오 메시지 재생이 MIP SDK 를 통해 요청될 때 활성화됩니다. MIP SDK 를 통해 타사 공급업체가 사용 중인 시스템에 대한 사용자 정의 플러그 인을 개발할 수 있습니다(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합).
녹화 시작 요청	MIP SDK 를 통해 레코딩 시작이 요청될 때 활성화됩니다. MIP SDK 를 통해 타사 공급업체가 사용 중인 시스템에 대한 사용자 정의 플러그 인을 개발할 수 있습니다(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합).
녹화 중지 요청	MIP SDK 를 통해 레코딩 중지가 요청될 때 활성화됩니다. MIP SDK 를 통해 타사 공급업체가 사용 중인 시스템에 대한 사용자 정의 플러그 인을 개발할 수 있습니다(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합).

외부 이벤트 - 일반 이벤트:

일반 이벤트를 이용하면 IP 네트워크를 통해 단순 문자열을 시스템으로 전송하여 시스템에서 동작을 트리거할 수 있습니다. 일반 이벤트의 용도는 가능한 한 많은 외부 소스가 시스템과 상호 작용할 수 있게 하기 위한 것입니다.

외부 이벤트 - 사용자 정의 이벤트:

시스템에 맞게 만들어진 여러 사용자 정의 이벤트를 선택할 수 있습니다. 해당 사용자 정의 이벤트는 다음과 같은 용도로 사용할 수 있습니다.

- 클라이언트 사용자가 클라이언트에서 라이브 비디오를 보면서 수동으로 이벤트를 트리거할 수 있도록 지원
- 기타 다양한 용도. 예를 들어, 특정 데이터 유형이 장치에서 수신될 때 발생하는 사용자 정의 이벤트를 만들 수 있습니다

  또한 페이지 75의 사용자 정의 이벤트(설명됨)를 참조하십시오.

레코딩 서버:

이벤트	설명
아카이브 사용 가능	사용 불가능했던 레코딩 서버에 대한 아카이브가 다시 사용할 수 있을 때 발생합니다. 또한 페이지 445의 아카이브를 사용할 수 없음를 참조하십시오.
아카이브를 사용할 수 없음	레코딩 서버의 아카이브를 사용할 수 없을 때 발생합니다. 예를 들면, 네트워크 드라이브에 위치한 아카이브 연결이 끊긴 경우가 있습니다. 이러한 경우 레코딩을 보관할 수 없습니다. 예를 들어 전자메일 통보가 조직 내 해당 담당자에게 자동 전송되도록 알람이나 알림 프로필을 트리거하는 데 이벤트를 사용할 수 있습니다.
아카이브 미완료	다음 번 예약이 시작될 때 지난 보관 순서에서 레코딩 서버의 아카이브가 완료되지 않은 경우 발생합니다.
설정된 보존 크기 이전의 데이터베이스 녹화 삭제	데이터베이스 크기 한계 이전에 보존 기간 한계에 도달하면 발생합니다.
설정된 보존 기간 이전의 데이터베이스 녹화 삭제	보존 기간 한계 이전에 데이터베이스 크기 한계에 도달 할 때 발생합니다.
데이터베이스 디스크 가득 참 – 자동 보관	데이터베이스 디스크가 가득 찰 때 발생합니다. 데이터베이스 디스크는 디스크에 남은 공간이 5GB 미만일 때 가득 찬 것입니다. 여유 공간이 5GB 미만이 되면 데이터베이스에서 가장 오래된 데이터가 항상 자동 아카이브됩니다(또는 다음 아카이브가 정의되지 않은 경우 삭제됨).
데이터베이스 디스크 가득 참 - 삭제	데이터베이스 디스크가 꽉 차서 1GB 미만의 여유 공간이 있을 때 발생합니다. 다음 아카이브가 정의된 경우에도 데이터가 삭제됩니다. 데이터베이스에는 항상 250MB의 여유 공간이 필요합니다. 이 제한에 도달하면(데이터 삭제 속도가 느려지는 경우), 충분한 여유 공간을 확보하기 전까지는 데이터베이스에 어떤 데이터도 기록되지 않습니다. 데이터베이스의 실제 최대 크기는 지정한 기가바이트 수에서 5GB를 뺀 값에 해당합니다.
데이터베이스 가득 참 - 자동 보관	레코딩 서버의 아카이브가 가득 찼고 저장소에서 아카이브로 자동 보관이 필요할 때 발생합니다.
데이터베이스 복구	데이터베이스가 손상되었을 때 발생합니다. 이 경우 시스템은 자동으로 두 가지 다른 데

이벤트	설명
	이터베이스 복구 방법인 빠른 복구와 전체 복구를 시도합니다.
데이터베이스 저장소를 사용할 수 있음	사용 불가능했던 레코딩 서버에 대한 저장소가 다시 사용할 수 있을 때 발생합니다. 또한 페이지 446의 데이터베이스 저장소를 사용할 수 없음를 참조하십시오. 예를 들어, **데이터베이스 저장소 사용 불가** 이벤트에 의해 중지된 경우 이 이벤트를 사용하여 녹화를 시작할 수 있습니다.
데이터베이스 저장소를 사용할 수 없음	레코딩 서버의 저장소를 사용할 수 없을 때 발생합니다. 예를 들면, 네트워크 드라이브에 위치한 저장소 연결이 끊긴 경우가 있습니다. 이러한 경우 레코딩을 보관할 수 없습니다. 예를 들어 녹화를 중지하거나, 이메일 알림이 조직 내 해당 담당자에게 자동으로 전송되도록 알람이나 알림 프로필을 트리거하는 데 이벤트를 사용할 수 있습니다.
장애 조치 암호화 통신 오류	장애 조치 서버와 모니터된 레코딩 서버 간의 SSL 통신 오류가 발생했을 때 일어납니다.
장애 조치 시작됨	장애 조치 레코딩 서버가 레코딩 서버의 작업을 인계할 때 발생합니다. 또한 장애 조치 서버(노드) 를 참조하십시오.
장애 조치 중지됨	레코딩 서버를 다시 사용할 수 있고 장애 조치 레코딩 서버로부터 작업을 인계할 수 있을 때 발생합니다.

시스템 모니터 이벤트

시스템 모니터 이벤트는 **시스템 모니터 임계값** 노드에서 구성된 초과 임계값으로 트리거됩니다. 또한 페이지 270의 하드웨어의 현재 상태를 조회하고 필요한 경우 문제를 해결합니다를 참조하십시오.

이 기능은 Data Collector 서비스가 실행 중이어야 합니다.

시스템 모니터 - 서버:

이벤트	설명
CPU 사용 위험	CPU 사용량이 위험 CPU 임계치를 초과할 때 발생합니다.
CPU 사용 정상	CPU 사용량이 경고 CPU 임계치 미만으로 떨어질 때 발생합니다.

이벤트	설명
CPU 사용량 경고	CPU 사용량이 경고 CPU 임계치를 초과하거나 위험 CPU 임계치 미만으로 떨어질 때 발생합니다.
메모리 사용량 위험	메모리 사용량이 위험 메모리 임계치를 초과할 때 발생합니다.
메모리 사용량 정상	메모리 사용량이 경고 메모리 임계치 미만으로 떨어질 때 발생합니다.
메모리 사용량 경고	메모리 사용량이 경고 메모리 임계치를 초과하거나 위험 메모리 사용 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 디코딩 위험	NVIDIA 디코딩 사용이 위험 NVIDIA 디코딩 임계치를 초과할 때 발생합니다.
NVIDIA 디코딩 정상	NVIDIA 디코딩 사용량이 경고 NVIDIA 디코딩 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 디코딩 경고	NVIDIA 디코딩 사용이 경고 NVIDIA 디코딩 임계치를 초과하거나 위험 NVIDIA 디코딩 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 메모리 위험	NVIDIA 메모리 사용량이 위험 NVIDIA 메모리 임계치를 초과할 때 발생합니다.
NVIDIA 메모리 정상	NVIDIA 메모리 사용량이 경고 NVIDIA 메모리 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 메모리 경고	NVIDIA 메모리 사용량이 경고 NVIDIA 메모리 임계치를 초과하거나 위험 NVIDIA 메모리 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 렌더링 위험	NVIDIA 렌더링 사용이 위험 NVIDIA 렌더링 임계치를 초과할 때 발생합니다.
NVIDIA 렌더링 정상	NVIDIA 렌더링 사용량이 경고 NVIDIA 렌더링 임계치 미만으로 떨어질 때 발생합니다.
NVIDIA 렌더링 경고	NVIDIA 렌더링 사용량이 경고 NVIDIA 렌더링 임계치를 초과하거나 위험 NVIDIA 렌더링 임계치 미만으로 떨어질 때 발생합니다.
사용 가능한 서비스 위험	서버 서비스가 중지될 때 발생합니다. 이 이벤트에 대한 임계치는 없습니다.
사용 가능한 서비스 정상	서버 서비스 상태가 실행으로 변경될 때 발생합니다. 이 이벤트에 대한 임계치는 없습니다.

시스템 모니터 - 카메라:

이벤트	설명
라이브 FPS 위험	라이브 FPS 속도가 위험 라이브 FPS 임계치 미만으로 떨어질 때 발생합니다.
라이브 FPS 정상	라이브 FPS 속도가 경고 라이브 FPS 임계치를 초과할 때 발생합니다.
라이브 FPS 경고	라이브 FPS 속도가 경고 라이브 FPS 임계치 미만으로 떨어지거나 위험 라이브 FPS 임계치를 초과할 때 발생합니다.
레코딩 FPS 위험	레코딩 FPS 속도가 위험 레코딩 FPS 임계치 미만으로 떨어질 때 발생합니다.
레코딩 FPS 정상	레코딩 FPS 속도가 경고 레코딩 FPS 임계치를 초과할 때 발생합니다.
레코딩 FPS 경고	레코딩 FPS 속도가 경고 레코딩 FPS 임계치 미만으로 떨어지거나 위험 레코딩 FPS 임계치를 초과할 때 발생합니다.
사용된 공간 위험	특정 카메라의 레코딩에 사용된 저장소가 위험 사용 공간 임계치를 초과할 때 발생합니다.
사용된 공간 정상	특정 카메라의 레코딩에 사용된 저장소가 경고 사용 공간 임계치 미만으로 떨어질 때 발생합니다.
사용된 공간 경고	특정 카메라의 레코딩에 사용된 저장소가 경고 사용 공간 임계치를 초과하거나 위험 사용 공간 임계치 미만으로 떨어질 때 발생합니다.

시스템 모니터 - 디스크:

이벤트	설명
여유 공간 위험	디스크 공간 사용량이 위험 여유 공간 임계치를 초과할 때 발생합니다.
여유 공간 정상	디스크 공간 사용량이 경고 여유 공간 임계치 미만으로 떨어질 때 발생합니다.
여유 공간 경고	디스크 공간 사용량이 경고 여유 공간 임계치를 초과하거나 위험 여유 공간 임계치 미만으로 떨어질 때 발생합니다.

시스템 모니터 - 저장소:

이벤트	설명
보존 기간 위험	시스템이 저장소가 위험 보존 기간 임계치보다 빠르게 채워질 것으로 예측할 때 발생합니다. 예를 들어, 비디오 스트림의 데이터가 예상보다 빠르게 저장소를 가득 채울 때입니다.
보존 기간 정상	시스템이 저장소가 경고 보존 기간 임계치보다 느리게 채워질 것으로 예측할 때 발생합니다. 예를 들어, 비디오 스트림의 데이터가 예상 속도로 저장소를 채울 때입니다.
보존 기간 경고	시스템이 저장소가 경고 보존 기간 임계치보다 빠르게 채워지거나 위험 보존 기간 임계치보다 느리게 채워질 것으로 예측할 때 발생합니다. 예를 들어, 비디오 스트림의 데이터가 동작 기록을 위해 구성된 카메라에 감지된 움직임이 더 많아 예상보다 빠른 속도로 저장소를 가득 채울 때입니다.

기타:

이벤트	설명
자동 라이선스 활성화 실패	온라인 자동 라이선스 활성화가 실패할 때 발생합니다. 이 이벤트에 대한 임계치는 없습니다.
시작된 암호 변경 예약	암호 변경 예약이 시작될 때 발생합니다.
완전히 성공한 암호 변경 예약	암호 변경 예약이 오류를 포함하여 완료되었을 때 발생합니다.
오류를 포함하여 완료된 암호 변경 예약	암호 변경 예약이 오류를 포함하여 완료되었을 때 발생합니다.

XProtect 확장 및 통합의 이벤트:

XProtect 확장 및 통합의 이벤트를 규칙 시스템에서 사용할 수 있습니다. 예:

- 또한 분석 이벤트를 규칙 시스템에서 사용할 수 있습니다

동작 및 중지 동작

동작 및 중지 동작의 세트는 **규칙 관리** 마법사의 규칙 생성에서 사용할 수 있습니다. 시스템 설치에서 XProtect 확장 또는 공급업체별 플러그 인을 사용하는 경우 더 많은 동작을 사용할 수 있습니다. 각 동작 유형에 대해 관련이 있는 경우 중지 동작 정보가 나열됩니다.

규칙 마법사 관리

동작	설명
<장치>에서 녹화 시작	레코딩 및 선택한 장치의 데이터베이스에 데이터 저장을 시작합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 다음을 지정하라는 메시지가 표시됩니다. 레코딩이 시작해야 하는 경우. 동작이 발생하는 장치에서 이벤트 트리거/트리거 시간 간격 시작 바로 직전이나 수초 전에 나타납니다. 이 동작 유형을 사용하려면 해당 동작이 연결된 장치에서 레코딩을 활성화해야 합니다. 해당 장치에 대해 사전 버퍼를 활성화한 경우, 이벤트 또는 시간 간격 이전부터만 데이터를 저장할 수 있습니다. **레코드** 탭에서 장치에 대한 레코딩을 활성화하고 사전 버퍼링 설정을 지정합니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **레코딩 중지**. 이 중지 동작을 사용하지 않을 경우, 레코딩이 잠재적으로 무한대로 계속됩니다. 또한 추가 중지 동작을 지정하는 옵션이 있습니다.
<장치>에서 피드 시작	장치에서 시스템으로 데이터 피드를 시작합니다. 장치에서 피드가 시작되면 데이터가 장치에서 시스템으로 전송되며, 이 경우 데이터 유형에 따라 데이터를 보고 기록할 수 있습니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 피드를 시작할 장치를 지정하라는 메시지가 표시됩니다. 해당 시스템에는 항상 모든 카메라에서 피드가 시작되도록 하는 디폴트 규칙이 포함되어 있습니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **피드 중지**. 또한 추가 중지 동작을 지정할 수 있습니다. 필수 중지 동작인 **피드 중지** 를 사용하여 장치에서 피드를 중지하면 데이터가 더 이상 장치에서 시스템으로 전송되지 않고, 이 경우 비디오 라이브 보기 및 레코딩 등이 더 이상 가능하지 않습니다. 그러나 피드를 중지한 장치는 레코딩 서버와 계속해서 통신할 수 있고, 장치를 수동으로 비활성화한 경우와 대조적으로 규칙을 통해 자동으로 피드를 시작할 수 있습니다. ⚠ 이러한 동작 유형으로 선택한 장치의 데이터 피드에 대한 액세스가 가능하지만 레코딩 설정을 별도로 지정해야 하므로 데이터가 기록됨이 보장되지는 않습니다.
<Smart Wall>을	XProtect Smart Wall 을(를) 선택한 프리셋으로 설정합니다. **Smart Wall 프리셋** 탭에서 프

동작	설명
(를) <프리셋>으로 설정	리셋을 지정합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<카메라> 표시를 위해 <Smart Wall> <모니터> 설정	이 사이트 또는 XProtect Smart Wall 에 구성된 임의의 하위 사이트에서 선택한 카메라의 라이브 비디오를 표시할 특정 Milestone Federated Architecture 모니터를 설정합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<messages> 텍스트를 나타내도록 Smart Wall <monitor> 설정	최대 200자의 사용자 정의 텍스트 메시지를 표시하도록 특정 XProtect Smart Wall 모니터를 설정합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<Smart Wall> 모니터 <모니터>에서 <카메라> 제거	특정 카메라의 비디오 표시를 중단합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 라이브 프레임 속도 설정	시스템이 카메라의 디폴트 프레임 속도를 대체하는 선택된 카메라의 라이브 비디오를 표시할 때 사용할 특정 프레임 속도를 설정합니다. **설정** 탭에서 이 속도를 지정합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 설정할 프레임 속도와 장치를 지정하라는 메시지가 표시됩니다. 항상 지정하는 프레임 속도가 해당 카메라에서 사용할 수 있는지 확인하십시오. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **디폴트 라이브 프레임 속도 복원**. 이 중지 동작을 사용하지 않을 경우, 디폴트 프레임 속도가 잠재적으로 전혀 복원되지 않습니다. 또한 추가 중지 동작을 지정하는 옵션이 있습니다.
<장치>에서 녹화 프레임 속도 설정	시스템이 카메라의 디폴트 레코딩 프레임 속도 대신 선택한 카메라의 녹화 비디오를 데이터베이스에 저장할 때 사용할 특정 프레임 속도를 설정합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 설정할 레코딩 프레임 속도와 카메라를 지정하라는 메시지가 표시됩니다. 각 프레임이 별도로 JPEG 이미지로 압축되는 비디오 코덱인 JPEG에 대해서만 레코딩 프레임 속도를 지정할 수 있습니다. 이 동작 유형을 사용하려면 해당 동작이 연결된 카메라에서 레

동작	설명
	코딩을 활성화해야 합니다. **레코드** 탭에서 카메라에 대한 레코딩을 활성화합니다. 지정할 수 있는 최대 프레임 속도는 해당 카메라 유형과 선택한 이미지 해상도에 따라 다릅니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **디폴트 레코딩 프레임 속도 복원**. 이 중지 동작을 사용하지 않을 경우, 디폴트 레코딩 프레임 속도가 잠재적으로 전혀 복원되지 않습니다. 또한 추가 중지 동작을 지정하는 옵션이 있습니다.
<장치>에서 MPEG-4/H.264/H.265에 대해 레코딩 프레임 속도를 모든 프레임으로 설정	시스템이 선택한 카메라의 녹화 비디오를 데이터베이스에 저장할 때 키프레임 대신 모든 프레임을 레코딩하도록 프레임 속도를 설정합니다. **레코드** 탭에서 레코딩 키프레임만 기능을 활성화합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 해당 동작을 적용할 장치를 선택하라는 메시지가 표시됩니다. MPEG-4/H.264/H.265에 대해 키프레임 레코딩만을 활성화할 수 있습니다. 이 동작 유형을 사용하려면 해당 동작이 연결된 카메라에서 레코딩을 활성화해야 합니다. **레코드** 탭에서 카메라에 대한 레코딩을 활성화합니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **MPEG-4/H.264/H.265에 대한 키프레임의 디폴트 녹화 프레임 속도 복원** 이 중지 동작을 사용하지 않을 경우, 디폴트 설정이 잠재적으로 전혀 복원되지 않습니다. 또한 추가 중지 동작을 지정하는 옵션이 있습니다.
PTZ 우선순위 <우선순위>가 있는 <프로파일>을 사용하여 <장치>에서 순찰 시작	특정 우선순위를 가진 특정 PTZ 카메라에 대한 해당 순찰 프로파일에 따라 PTZ 순찰을 시작합니다. 이는 프리셋 위치 시퀀스, 타이밍 설정 등을 포함하여 순찰이 이루어지는 방식에 대한 정확한 정의에 해당합니다. 시스템을 이전 버전에서 업그레이드한 경우, 이전 값(**매우 낮음**, **낮음**, **보통**, **높음** 및 **매우 높음**)이 다음과 같이 해석됩니다. • 매우 낮음 = 1000 • 낮음 = 2000 • 보통 = 3000 • 높음 = 4000 • 매우 높음 = 5000 이 동작 유형을 선택하면 **규칙 관리** 마법사에 순찰 프로파일을 선택하라는 메시지가 표시됩

동작	설명
	니다. 한 장치에서 순찰 프로파일을 하나만 선택할 수 있고, 여러 순찰 프로파일을 선택할 수는 없습니다. 이러한 유형의 동작에서는 해당 동작이 연결되는 장치가 PTZ 장치여야 합니다. 이 장치에 대해 하나 이상의 순찰 프로파일을 정의해야 합니다. **순찰** 탭에서 PTZ 카메라에 대한 순찰 프로파일을 정의합니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **순찰 중지** 이 중지 동작을 사용하지 않을 경우, 순찰이 잠재적으로 전혀 중지되지 않습니다. 또한 추가 중지 동작을 지정할 수 있습니다.
<장치>에서 순찰 일시 중지	PTZ 순찰을 일시 중지합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 순찰을 일시 중지할 장치를 지정하라는 메시지가 표시됩니다. 이러한 유형의 동작에서는 해당 동작이 연결되는 장치가 PTZ 장치여야 합니다. 이 장치에 대해 하나 이상의 순찰 프로파일을 정의해야 합니다. **순찰** 탭에서 PTZ 카메라에 대한 순찰 프로파일을 정의합니다. **중지 동작 필요**: 이 유형의 동작에는 하나 이상의 중지 동작이 필요합니다. 다음 단계 중 하나에서 마법사가 중지 동작을 지정하라는 메시지를 자동으로 표시합니다: **순찰 다시 시작** 이 중지 동작을 사용하지 않을 경우, 순찰이 잠재적으로 무한대로 일시 중지됩니다. 또한 추가 중지 동작을 지정하는 옵션이 있습니다.
<장치>를 PTZ 우선순위 <우선순위>를 가진 <프리셋> 위치로 이동	특정 카메라를 특정 프리셋 위치로 이동합니다. 단, 이 이동은 항상 **우선**순위에 따라 이루어집니다. 하나의 카메라에서 프리셋 위치를 하나만 선택할 수 있습니다. 하나의 카메라에서 프리셋 위치를 하나만 선택할 수 있습니다.

동작	설명
	여러 프리셋 위치 선택은 불가능합니다. 이러한 유형의 동작에서는 해당 동작이 연결되는 장치가 PTZ 장치여야 합니다. 이 동작에서는 해당 장치에 대해 하나 이상의 프리셋 위치를 정의해야 합니다. **프리셋** 탭에서 PTZ 카메라에 대한 프리셋 위치를 정의합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
PTZ 우선순위 <우선순위>를 가진 <장치>의 기본 프리셋으로 이동	하나 이상의 특정 카메라를 해당 디폴트 프리셋 위치로 이동합니다. 단, 이 이동은 항상 우선순위에 따라 이루어집니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 해당 동작을 적용할 장치를 선택하라는 메시지가 표시됩니다. 이러한 유형의 동작에서는 해당 동작이 연결되는 장치가 PTZ 장치여야 합니다. 이 동작에서는 해당 장치에 대해 하나 이상의 프리셋 위치를 정의해야 합니다. **프리셋** 탭에서 PTZ 카메라에 대한 프리셋 위치를 정의합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
장치 출력을 <상태>로 설정	장치의 출력을 특정 상태(활성화됨 또는 비활성화됨)로 설정합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 설정할 상태와 장치를 지정하라는 메시지가 표시됩니다. 이 동작 유형의 경우에는 해당 동작이 연결된 장치 각각에서 하나 이상의 외부 출력 장치가 출력 포트에 연결되어 있어야 합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 북마크 생성	선택한 장치의 라이브 스트리밍 또는 레코딩에 북마크를 만듭니다. 북마크는 특정 이벤트 또는 기간을 손쉽게 추적할 수 있게 해줍니다. 북마크 설정은 **옵션** 대화 상자에서 제어합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 북마크 세부 정보를 지정하고 장치를 선택하라는 메시지가 표시됩니다.

동작	설명
	필수 중지 동작 없음: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<우선순위>로 <장치>의 오디오 <메시지> 재생	선택한 장치에서 이벤트에 의해 트리거된 오디오 메시지를 재생합니다. 장치는 대개 스피커나 카메라입니다. 이러한 유형의 작업은 **도구** > **옵션** > **오디오 메시지** 탭에서 시스템으로 메시지를 업로드해야 합니다. 동일한 이벤트에 추가 규칙을 생성하고 각 장치에 서로 다른 메시지를 보낼 수 있지만, 항상 우선 순위에 따라야 합니다. 시퀀스를 제어하는 우선 순위는 **음성** 탭에서 하나의 역할에 대해 규칙 및 장치에 설정된 값입니다. • 하나의 메시지가 재생되고, 동일한 우선 순위를 가지는 다른 메시지가 동일한 스피커로 보내질 경우, 첫 메시지가 완료된 다음 두 번째 메시지가 시작됩니다 • 하나의 메시지가 재생되고, 높은 우선 순위를 가지는 다른 메시지가 동일한 스피커로 보내질 경우, 첫 메시지가 중단되고 두 번째 메시지가 즉시 시작됩니다
알림을 <프로파일>로 보내기	특정 알림 프로필을 사용하여 알림을 전송합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 알림 프로필과 사전 알람 이미지를 포함시킬 장치를 선택하라는 메시지가 표시됩니다. 알림 프로필을 하나만 선택할 수 있고 여러 개의 알림 프로필을 선택할 수는 없습니다. 단일 알림 프로필에 여러 수신자가 포함될 수 있습니다. 동일 이벤트에 대해 추가 규칙을 만들어 각각의 알림 프로필로 서로 다른 알림을 보낼 수도 있습니다. **규칙** 목록에서 규칙을 마우스 오른쪽 버튼으로 클릭해서 해당 규칙의 내용을 복사해 다시 사용할 수 있습니다. 이 동작 유형을 사용하려면 하나 이상의 알림 프로필을 정의해야 합니다. 사전 알람 이미지는 해당 알림 프로필에 대해 **이미지 포함** 옵션을 활성화한 경우에만 포함됩니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
새 <로그 항목> 만들기	규칙 로그에 항목을 생성합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 로그 항목의 텍스트를 지정하라는 메시지가 표시됩니다. 로그 텍스트를 지정할 때 **$DeviceName$**, **$EventName$** 등의 변수를 로그 메시지에 삽입할 수 있습니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 플러그인 시작	하나 이상의 플러그 인을 시작합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 필요한 플러그 인과 해당 플러그 인을 시작할 장치를 선택하라는 메시지가 표시됩니다.

동작	설명
	이 동작 유형을 사용하려면 시스템에 하나 이상의 플러그 인이 설치되어 있어야 합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 플러그 인 중지	하나 이상의 플러그 인을 중지합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 필요한 플러그 인과 해당 플러그 인을 중지할 장치를 선택하라는 메시지가 표시됩니다. 이 동작 유형을 사용하려면 시스템에 하나 이상의 플러그 인이 설치되어 있어야 합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 새 설정 적용	하나 이상의 장치에서 장치 설정을 변경합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 해당 장치를 선택하라는 메시지가 표시되며, 지정한 장치에서 해당 설정을 정의할 수 있습니다. 둘 이상의 장치에 대한 설정을 정의하는 경우, 지정한 모든 장치에 대해 사용 가능한 설정만 변경할 수 있습니다. **예**: 동작이 장치 1과 장치 2에 연결되도록 지정합니다. 장치 1에는 설정 A, B, C가 있고, 장치 2에는 설정 B, C, D가 있습니다. 이 경우, 두 장치 모두에 대해 사용 가능한 설정, 즉 설정 B와 C만 변경할 수 있습니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>를 보려는 Matrix 설정	Matrix 을(를) 설치한 컴퓨터와 같이 XProtect Smart Client 이(가) 트리거한 비디오를 표시할 수 있는 컴퓨터에 표시된 선택된 카메라에서 비디오를 만듭니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 Matrix 수신자와 선택한 Matrix 수신자에 비디오를 표시할 하나 이상의 장치를 선택하라는 메시지가 표시됩니다. 이 동작 유형을 사용하면 한 번에 하나의 Matrix 수신자만 선택할 수 있습니다. 선택한 장치의 비디오가 둘 이상의 Matrix 수신자에 나타나게 하려면 필요한 각 Matrix 수신자에 대해 규칙을 만들거나 XProtect Smart Wall 기능을 사용해야 합니다. **규칙** 목록에서 규칙을 마우스 오른쪽 버튼으로 클릭해서 해당 규칙의 내용을 복사해 다시 사용할 수 있습니다. 이러한 방식으로 거의 동일한 규칙을 처음부터 다시 만들 필요가 없습니다.

동작	설명
	Matrix 수신자 자체의 구성 일부로 사용자가 Matrix 통신에 필요한 포트 번호와 암호를 지정해야 합니다. 사용자에게 이 정보에 대한 액세스 권한이 있는지 확인하십시오. 일반적으로 사용자가 Matrix 트리거 비디오 표시와 관련한 명령을 수락하는 허용된 호스트의 IP 목록도 정의해야 합니다. 이 경우 사용자가 관리 서버 또는 사용된 라우터나 방화벽의 IP 주소를 알고 있어야 합니다.
SNMP 트랩 보내기	선택한 장치에 이벤트를 기록하는 단문 메시지를 생성합니다. SNMP 트랩 텍스트는 자동으로 생성되며 사용자 정의할 수 없습니다. 여기에는 소스 유형, 이벤트가 발생한 장치의 이름이 포함될 수 있습니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 원격 녹화를 검색하고 저장합니다	이벤트 트리거 이전/이후의 지정된 기간 동안 선택한 장치(에지 레코딩 지원 장치)에서 원격 레코딩을 검색하여 저장합니다. 이 규칙은 **연결 복원 시 원격 레코딩 자동 검색 설정** 과 독립적입니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<장치>에서 <시작 및 종료 시간> 사이의 원격 녹화를 검색하고 저장합니다	선택한 장치(에지 레코딩 지원 장치)에서 지정된 기간의 원격 레코딩을 검색하여 저장합니다. 이 규칙은 **연결 복원 시 원격 레코딩 자동 검색 설정** 과 독립적입니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
첨부된 이미지 저장	이미지 수신 이벤트에서 이미지가 수신되면(카메라에서 SMTP 이메일을 통해 전송) 나중에 사용할 수 있도록 해당 이미지가 저장됩니다. 나중에 다른 이벤트가 이 동작을 트리거할 수도 있습니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<아카이브>에서 보관 활성화	하나 이상의 아카이브에서 보관을 시작합니다. 이 동작 유형을 선택하면 **규칙 관리** 마법사에 해당 아카이브를 선택하라는 메시지가 표시됩니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.

동작	설명
<사이트>에서 <사용자 정의 이벤트> 트리거	대부분 Milestone Federated Architecture 내에서 관련이 있지만, 단일 사이트 설치에서도 이 설정을 사용할 수 있습니다. 사이트(보통 연합 계층 내의 원격 사이트)에서 사용자 정의 이벤트를 트리거하려면 이 규칙을 사용합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
<액세스 요청 알림> 표시	이벤트 트리거의 기준을 충족할 때 XProtect Smart Client 화면에 액세스 요청 알림을 팝업으로 표시할 수 있습니다. Milestone은 일반적으로 관련 액세스 제어 명령 및 카메라에서 작동을 위해 액세스 요청 알림이 구성되기 때문에 이 동작에 대해 액세스 제어 이벤트를 이벤트 트리거로 사용할 것을 권장합니다. 이 동작 유형을 사용하려면 시스템에 하나 이상의 액세스 제어 플러그 인이 설치되어 있어야 합니다. **필수 중지 동작 없음**: 이 유형의 동작에는 중지 동작이 필요하지 않습니다.이벤트에서 또는 일정 기간 후 수행할 선택적인 중지 동작을 지정할 수 있습니다.
하드웨어 장치의 암호 변경	선택된 하드웨어 장치의 암호를 특정 하드웨어 장치에 필요한 암호 요건에 기반하여 임의 생성된 암호로 변경합니다. 지원되는 하드웨어 장치 목록은 하드웨어 찾기 를 참조하십시오. 이 동작은 **<recurring time>에 동작 수행하기** 규칙 유형을 사용하는 규칙을 설정할 때만 사용할 수 있습니다. 다음 이벤트는 동작으로 사용 가능합니다. • 페이지 449의 시작된 암호 변경 예약 • 페이지 449의 완전히 성공한 암호 변경 예약 • 페이지 449의 오류를 포함하여 완료된 암호 변경 예약 이러한 유형의 동작에는 중지 동작이 없습니다. 이러한 동작의 진행 과정을 **현재 작업** 노드에서 확인할 수 있습니다. 자세한 정보는 페이지 269의 레코딩 서버 상의 현재 진행 중인 작업 보기를 참조하십시오. 동작 결과를 보려면 **서버 로그** 노드에서 **시스템 로그** 탭으로 이동합니다. 자세한 정보는 페이지 356의 서버 로그 탭(옵션)를 참조하십시오. 자세한 정보는 시스템 로그(탭) 을 참조하십시오.

테스트 분석 이벤트(속성)

분석 이벤트의 요구 사항을 테스트할 때 4가지 조건을 확인하고 가능한 오류 설명 및 솔루션을 제공하는 창이 나타납니다.

조건	설명	오류 메시지 및 해결 방법
변경 내용이 저장됨	이벤트가 새 항목일 경우, 저장되었습니까? 또는 이벤트 이름을 변경한 경우, 해당 변경 내용을 저장했습니까?	**분석 이벤트를 테스트하기 전에 변경 내용을 저장하십시오**. 해결 방법/설명: 변경 내용을 저장합니다.
분석 이벤트 활성화	분석 이벤트 기능이 활성화되었습니까?	**분석 이벤트가 활성화되지 않았습니다**. 해결 방법/설명: 분석 이벤트 기능을 활성화하십시오. 이렇게 하려면 **도구** > **옵션** > **분석 이벤트** 를 클릭하고 **활성화됨** 확인란을 선택합니다.
허용된 주소	기기의 IP 주소/호스트 이름이 허용된 이벤트를 보내고 있습니까(분석 이벤트 주소 목록에 나열됨)?	**로컬 호스트 이름을 분석 이벤트 서비스에 대한 허용된 주소로 추가해야 합니다**. 해결 방법/설명: 기기를 허용된 IP 주소 또는 호스트 이름의 분석 이벤트 주소 목록에 추가하십시오. **로컬 호스트 이름을 확인하는 중 오류 발생**. 해결 방법/설명: 기기의 IP 주소 또는 호스트 이름을 찾을 수 없거나 유효하지 않습니다.
분석 이벤트 보내기	이벤트 서버로 테스트 이벤트가 성공적으로 보내졌습니까?	아래 표를 참조하십시오.

각 단계는 실패:❌ 또는 성공:✔.

분석 이벤트 보내기 조건에 대한 오류 메시지와 해결 방법:

오류 메시지	해결책:
이벤트 서버를 찾을 수 없음	등록된 서비스 목록에서 이벤트 서버를 찾을 수 없습니다.
이벤트 서버 연결 중 오류	명시된 포트에서 이벤트 서버에 연결할 수 없습니다. 이 오류는 네트워크 문제 또는

오류 메시지	해결책:
	Event Server 서비스의 중지 등으로 인해 발생할 가능성이 높습니다.
분석 이벤트 전송 중 오류	이벤트 서버의 연결이 설정되었지만 이벤트를 전송할 수 없습니다. 이 오류는 시간 초과 등의 네트워크 문제로 인해 발생할 가능성이 높습니다.
이벤트 서버에서 응답 수신 중 오류	이벤트가 이벤트 서버로 전송되었지만 회신이 수신되지 않습니다. 이 오류는 네트워크 문제나 사용 중인포트로 인해 발생할 가능성이 높습니다. 이벤트 서버 로그(보통 ProgramData\Milestone\XProtect Event Server\Logs\에 위치)를 참조하십시오.
이벤트 서버에서 분석 이벤트를 알 수 없음	Event Server 서비스가 이벤트를 인식하지 못합니다. 이 오류는 이벤트 또는 이벤트의 변경 내용이 저장되지 않았기 때문에 발생할 가능성이 높습니다.
이벤트 서버에서 유효하지 않은 분석 이벤트 수신	이벤트 형식이 올바르지 않습니다.
보낸 사람이 이벤트 서버에서 인증되지 않음	사용자의 기기가 허용된 IP 주소 또는 호스트 이름의 목록에 존재하지 않을 가능성이 높습니다.
이벤트 서버의 내부 오류	이벤트 서버 오류입니다. 이벤트 서버 로그(보통 ProgramData\Milestone\XProtect Event Server\Logs\에 위치)를 참조하십시오.
이벤트 서버에서 유효하지 않은 응답 수신	응답이 유효하지 않습니다. 포트가 사용 중이거나 네트워크 문제가 존재할 수 있습니다. 이벤트 서버 로그(보통 ProgramData\Milestone\XProtect Event Server\Logs\에 위치)를 참조하십시오.
이벤트 서버의 알 수 없는 응답	응답이 유효하지만 인식되지 않습니다. 이 오류는 네트워크 문제나 사용 중인포트로 인해 발생할 가능성이 있습니다. 이벤트 서버 로그(보통 ProgramData\Milestone\XProtect Event Server\Logs\에 위치)를 참조하십시오.
예기치 않은 오류	Milestone 지원부로 문의하여 도움을 요청하십시오.

일반 이벤트 및 데이터 소스(속성)

이 기능은 XProtect 이벤트 서버가 설치된 경우에만 작동합니다.

일반 이벤트(속성)

구성 요소	요구사항
이름	일반 이벤트의 고유 이름. 이름은 사용자 정의 이벤트, 분석 이벤트 등 모든 유형의 이벤트에 대해 고유해야 합니다.
활성화됨	일반 이벤트는 기본적으로 활성화되어 있습니다. 이벤트를 비활성화하려면 확인란 선택을 취소하십시오.
식	데이터 패키지를 분석할 때 시스템이 주의해야 하는 식. 다음 연산자를 사용할 수 있습니다: • ( ): 관련 항목이 논리적 단위로 함께 처리되었는지 확인하는 데 사용됩니다. 분석에서 특정 처리 순서를 강제로 실행하는 데 사용할 수 있습니다 **예**: (User001 OR Door053) AND Sunday 검색 기준은 괄호 안에 있는 두 용어를 먼저 처리한 후, 해당 결과를 문자열 마지막 부분과 결합합니다. 따라서 시스템이 먼저 User001 또는 Door053 항목을 포함하는 패키지를 찾은 다음 해당 결과를 가져오고 실행하여 Sunday 항목도 포함하는 패키지를 찾습니다. • AND: AND 연산자를 사용하여 AND 연산자 양쪽에 있는 항목이 존재해야 함을 지정합니다. **예**: User001 AND Door053 AND Sunday 검색 조건은 식에 User001, Door053 및 Sunday 항목이 모두 포함된 경우에만 결과를 반환합니다. 항목 중 하나 또는 두 개만 존재하는 것으로는 충분하지 않습니다. AND를 사용해 조합한 항목이 많을수록 검색하는 결과의 수가 적어집니다. • OR: OR 연산자를 사용하여 어떤 항목 중 하나가 존재해야 함을 지정합니다. **예**: User001 OR Door053 OR Sunday 검색 조건은 User001, Door053 또는 Sunday 중 하나를 포함하는 모든 결과를 반환합니다. OR을 사용해 조합한 항목이 많을수록 검색하는 결과의 수가 많아집니다.
식 유형	수신된 데이터 패키지를 분석할 때 시스템의 특이도를 나타냅니다. 다음과 같은 옵션이 있습니다: • **검색**: 이벤트를 발생시키려면 수신한 데이터 패키지가 **수식** 필드에서 지정한 텍스트를 포함하고 있어야 하지만, 더 많은 내용을 가질 수도 있습니다 **예**: 수신된 패키지에 User001 및 Door053 항목이 포함되어야 하는 것으로 지정한 경우, 수신된 패키지에 User001 및 Door053 및 Sunday 항목이 포함되어 있으면 이벤트가 트리거됩니다. 필요한 두 개의 항목이 수신 패키지에 포함되어 있기 때문입니다

구성 요소	요구사항
	• **일치 항목**: 이벤트를 발생시키려면 수신한 데이터 패키지에 **수식** 필드에 지정한 텍스트만 포함하고 있어야 합니다 • **정규식**: 이벤트를 발생시키려면 수신한 데이터 패키지에 **수식** 필드에 지정한 텍스트가 수신한 데이터 패키지에서 특정 패턴을 식별해야 합니다 **검색** 또는 **일치 항목** 에서 **정규식** 으로 전환하면 **식** 필드의 텍스트는 자동으로 정규식으로 해석됩니다.
우선순위	0(최고 우선순위) ~ 999999(최저 우선순위) 사이의 번호로 우선순위를 지정해야 합니다. 동일 데이터 패키지가 서로 다른 이벤트에 대해 분석될 수 있습니다. 각 이벤트에 우선순위를 할당하는 기능을 통해 수신된 패키지가 여러 이벤트의 기준과 일치할 경우 트리거할 이벤트를 관리할 수 있습니다. 시스템이 TCP 및/또는 UDP 패키지를 수신하면 패킷 분석이 최고 우선순위를 가진 이벤트의 분석부터 시작합니다. 이러한 방식으로 패키지가 여러 이벤트의 기준과 일치할 때 최고 우선순위를 가진 이벤트만 트리거됩니다. 패키지가 우선순위가 동일한 여러 이벤트의 기준과 일치할 경우(예: 우선순위가 999인 이벤트 2개), 이 우선순위를 가진 모든 이벤트가 트리거됩니다.
식이 이벤트 문자열과 일치하는지 확인	**수식** 필드에 입력된 수식에 대해 테스트할 이벤트 문자열.

웹후크(규칙 및 이벤트 노드)

웹후크 노드에서 웹후크 엔드포인트를 생성, 편집 및 삭제할 수 있습니다.

웹후크를 만들고 편집할 때 다음과 같은 필드를 사용할 수 있습니다.

필드	설명
이름	웹후크 엔드포인트의 고유한 이름을 입력합니다. 웹후크 이름은 비워둘 수 없습니다.
주소	이벤트 데이터를 보내고 싶은 웹 서버 또는 애플리케이션의 URL. 웹 서버의 URL이(가) 업데이트되면 웹

필드	설명
	후크 노드에서 웹 후크 URL을(를) 업데이트해야 합니다. 안전하지 않은 네트워크(예: 개방형 인터넷)를 HTTP을(를) 사용하면 모든 이벤트가 일반 텍스트로 노출됩니다.
토큰	HTTP POST 소스를 검증하여 다른 애플리케이션과의 통신을 보호하는 데 사용되는 토큰을 입력합니다. 보안 통신을 위해 토큰을 사용하는 것은 선택 사항이지만 권장 사항입니다.
API 버전	웹후크 기능에 사용되는 웹후크 플러그인 및 API의 버전입니다.

보안 노드

역할(보안 노드)

정보 탭(역할)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

역할의 **정보** 탭에서 다음을 설정할 수 있습니다.

이름	설명
이름	역할의 이름을 입력합니다.
설명	역할의 설명을 입력합니다.
Management Client 프로파일	역할에 연결할 Management Client 프로파일을 선택합니다. **기본** 관리자 역할에는 이 설정을 적용할 수 없습니다.

이름	설명
	관리 서버에서 보안을 관리하기 위한 권한이 필요합니다.
Smart Client 프로파일	역할에 연결할 Smart Client 프로파일을 선택합니다. 관리 서버에서 보안을 관리하기 위한 권한이 필요합니다.
기본 시간 프로파일	역할에 연결할 기본 시간 프로파일을 선택합니다. **기본** 관리자 역할에는 이 설정을 적용할 수 없습니다.
증거물 잠금 프로파일	역할에 연결할 증거물 잠금 프로파일을 선택합니다.
Smart Client 은(는) 시간 프로파일 내에 로그인합니다.	이 역할에 연결된 XProtect Smart Client 사용자가 로그인할 수 있는 기간에 대한 시간 프로파일을 선택합니다. 기간이 만료될 때 XProtect Smart Client 사용자가 로그인되어 있는 경우 자동으로 로그오프됩니다. **기본** 관리자 역할에는 이 설정을 적용할 수 없습니다.
Smart Client 로그인 허용	이 역할과 관련된 사용자가 XProtect Smart Client 에 로그인하려면 확인란을 선택합니다. Smart Client 에 대한 액세스는 기본으로 허용되어 있지 않습니다. XProtect Smart Client 에 액세스를 거부하려면 확인란을 선택 취소합니다.
XProtect Mobile 클라이언트 로그인 허용	이 역할과 관련된 사용자가 XProtect Mobile 클라이언트에 로그인하도록 허용하려면 확인란을 선택합니다. XProtect Mobile 클라이언트에 대한 액세스는 기본으로 허용되어 있지 않습니다. XProtect Mobile 클라이언트에 액세스를 거부하려면 확인란을 선택 취소합니다.
XProtect Web Client 로그인 허용	이 역할과 관련된 사용자가 XProtect Web Client 에 로그인하려면 확인란을 선택합니다. XProtect Web Client 에 대한 액세스는 기본으로 허용되어 있지 않습니다. XProtect Web Client 에 액세스를 거부하려면 확인란을 선택 취소합니다.
로그인 인증 필요함	로그인 인증을 역할에 연결하려면 이 확인란을 선택합니다. 즉, 사용자가 로그인하면

이름	설명
	XProtect Smart Client 또는 Management Client 에서 보통 감독자나 관리자에 의한 이차 인증을 요구합니다. 관리자가 사용자를 인증할 수 있게 하려면 **전체 보안** 탭에서 관리 서버의 **사용자 인증** 권한을 구성하십시오. **기본** 관리자 역할에는 이 설정을 적용할 수 없습니다.
PTZ 세션 중 사용자를 익명 처리	PTZ 세션을 제어할 때 이 역할과 연결된 사용자의 이름이 숨겨지도록 하려면 이 확인란을 선택합니다.

사용자 및 그룹 탭(역할)

사용자 및 그룹 탭에서 사용자와 그룹에 역할을 할당합니다(페이지 265의 역할에 사용자 및 그룹 할당/제거 참조). Windows 사용자 및 그룹 또는 기본 사용자를 할당할 수 있습니다(페이지 59의 사용자(설명됨) 참조).

외부 IDP(역할)

외부 IDP 탭에서, 기존 클레임을 조회하고 새로운 클레임을 역할에 추가할 수 있습니다.

이름	설명
외부 IDP	외부 IDP의 이름
클레임 이름	외부 IDP에서 정의된 변수.
클레임 값	사용자에게 적절한 역할을 할당하는데 사용할 수 있는 클레임의 값(예: 그룹 이름).

전체 보안 탭(역할)

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

전체 보안 탭에서 역할에 대한 전체 권한을 설정합니다. 시스템에서 사용할 수 있는 모든 구성 요소에 대해 **허용** 또는 **거부** 를 설정하여 역할에 대한 액세스 권한을 정의합니다. 사용자의 역할에 대해 구성 요소에 대해 액세스가 거부된 경우 **전체 보안** 탭은 해당 역할의 사용자에게 보이지 않습니다.

전체 보안 탭은 무료 XProtect Essential+ 에서 이용할 수 없습니다.

기타 XProtect Corporate VMS 제품보다 XProtect 에 대해 더 많은 액세스 권한을 정의할 수 있습니다. 이는 XProtect Corporate 에서는 상이한 관리자 권한만 설정할 수 있는 반면, 모든 제품에서 XProtect Smart Client, XProtect Web Client 또는 XProtect Mobile 클라이언트를 사용하는 역할에 대해 전체적인 권한을 설정할 수 있기 때문입니다.

전체 보안 설정은 현재 사이트에만 적용됩니다.

둘 이상의 역할과 사용자를 연결하고 한 역할에 대해 보안 설정에서 **거부** 를 선택하고, 다른 역할에 대해서는 **허용** 을 선택하면, **거부** 권한이 **허용** 권한보다 우선합니다.

다음에 나온 설명은 해당 역할에 대해 **허용** 을 선택한 경우 여러 시스템 구성 요소에서 각각의 개별 권한에 발생하는 상황을 보여줍니다. XProtect Corporate 를 사용하는 경우, 각 시스템 구성 요소에서 **오직** 사용자의 시스템에만 사용할 수 있는 설정을 볼 수 있습니다.

각각의 시스템 구성 요소 또는 기능에 대해 전체 시스템 관리자가 **허용** 또는 **거부** 확인란을 사용하여 해당 역할에 대한 보안 권한을 설정할 수 있습니다. 여기서 설정하는 모든 보안 권한은 전체 시스템 구성 요소 또는 기능에 대해 설정됩니다. 가령 **카메라** 의 **거부** 확인란을 선택하는 경우, 시스템에 추가된 모든 카메라는 해당 역할을 수행할 수 없게 됩니다. 이와 반대로 **허용** 확인란을 선택하면 해당 역할이 시스템에 추가된 모든 카메라를 볼 수 있습니다. 카메라에서 **허용** 또는 **거부** 선택 결과에 따라 **장치** 탭의 카메라 설정이 **전체 보안** 탭의 선택을 상속하므로 특정 역할에 대해 모든 카메라를 사용할 수 있거나 사용할 수 없게 됩니다.

전체 보안 탭에서 시스템 구성 요소 또는 기능에 대해 **어떤 전체 권한도 설정하지 않았을 때 개별** 카메라나 유사한 장치에 대해 보안 권한을 설정하려는 경우, 관련 시스템 구성 요소 또는 기능의 탭에서 이러한 각각의 권한만 설정할 수 있습니다.

아래 설명은 MIP SDK 을(를) 통해 구성할 수 있는 권한에도 적용됩니다.

기본 라이선스를 XProtect Corporate 에서 다른 제품 중 하나로 전환하려면 XProtect Corporate 에만 이용할 수 있는 모든 보안 권한을 제거해야 합니다. 이러한 권한을 제거하지 않으면 전환을 완료할 수 없습니다.

관리 서버

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
연결	사용자가 Management Server 에 연결할 수 있도록 해줍니다. 이 허가는 기본적으로 활성화되어 있습니다. 관리 목적으로 역할에 대한 연결 허가를 잠시 거부한 후 시스템에 대한 액세스를 재적용할 수 있습니다. ⚠ 이 허가는 반드시 선택되어야 시스템에 대한 액세스를 허용할 수 있게 됩니다.
판독	⚠ 이 권한은 시스템에서 구성된 자격 증명과 같이 민감한 데이터에 대한 액세스를 비롯하여 XProtect VMS 에 대한 상당한 액세스 권한을 부여하는 높은 특권을 보유한 관리자 권한입니다. 다음을 포함한 다양한 기능에 액세스할 수 있는 권한을 활성화합니다. • Management Client 을(를) 사용하여 로그인 • 현재 작업 목록 • 서버 로그 또한 다음에 대한 접근을 활성화 합니다: • 원격 연결 서비스 • Smart Client 프로파일 • Management Client 프로파일 • Matrix • 시간 프로파일 • 등록된 서버 및 서비스 등록 API 또한 이 권한은 다음과 같이 클라이언트에 대한 일부 민감한 정보를 드러냅니다. • 구성된 모든 외부 IDP에 대한 자격 증명 • XProtect VMS 의 모든 카메라를 위한 자격 증명과 IP 주소, 기타 정보 • 구성된 메일 서버를 위한 자격 증명

보안 권한	설명
	• 모든 구성 매트릭스를 위한 자격 증명 • 상호 연결 기능을 위해 구성된 자격 증명 • 라이선스 활성화를 위해 구성된 자격 증명 이 권한은 XProtect VMS 사용자의 자격 증명을 드러내지 않습니다. 여기에는 Windows 사용자 및 외부 IDP의 사용자 등의 기본 사용자가 포함됩니다.
편집	다음을 포함한 다양한 기능에서 데이터를 수정할 수 있는 권한을 활성화합니다. • 옵션 • 라이선스 관리 또한 사용자가 다음을 생성, 삭제 및 편집할 수 있습니다: • 원격 연결 서비스 • 장치 그룹 • Matrix • 시간 프로파일 • 알림 프로파일 • 등록된 서버 레코딩 서버에서 네트워크를 구성할 때 로컬 IP 범위를 구성할 수 있는 권한을 활성화합니다.
시스템 모니터	시스템 모니터의 데이터를 볼 수 있는 권한을 활성화합니다.
상태 API	레코딩 서버에 있는 상태 API에서 쿼리를 수행할 수 있는 권한을 활성화합니다. 즉, 이 권한이 활성화된 역할은 레코딩 서버에 위치한 항목의 상태에 대한 읽기 권한을 갖습니다.
연합 사이트 계층 관리	현재 사이트를 연합 사이트 계층 구조에 있는 다른 사이트에 추가하고 분리할 수 있는 권한을 활성화합니다. 하위 사이트에서만 허용되도록 이 권한을 설정하는 경우에도 사용자는 상위 사이트에서 사이트를 분리시킬 수 있습니다.
구성 백업	시스템의 백업/복원 기능을 사용하여 시스템 구성의 백업을 만들 수 있는 권한을 활성화합니

보안 권한	설명
	다.
사용자 인증	XProtect Smart Client 또는 Management Client 에서 이차 로그인을 요청 받았을 때 사용자를 인증할 수 있는 권한을 활성화합니다. 역할에 로그인 인증이 필요한 경우 **정보** 탭에서 정의합니다.
보안 관리	관리 서버에 대한 권한을 관리할 수 있는 권한을 활성화합니다. 또한 사용자가 다음 기능을 생성, 삭제 및 편집할 수 있습니다: • 역할 • 기본 사용자 • Smart Client 프로파일 • Management Client 프로파일

레코딩 서버

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
편집	관리 서버에서 편집 권한이 필요한 네트워크 구성 설정을 제외하고 레코딩 서버에서 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	레코딩 서버를 삭제할 수 있는 권한을 활성화합니다. 이를 위해 사용자에게 다음에 대한 삭제 권한도 부여해야 합니다. • 레코딩 서버에 하드웨어를 추가한 경우 하드웨어 보안 그룹 레코딩 서버의 장치에 증거물 잠금이 포함되어 있는 경우, 오프라인일 때만 레코딩 서버를 삭제할 수 있습니다.

보안 권한	설명
하드웨어 관리	레코딩 서버에 하드웨어를 추가할 수 있는 권한을 활성화합니다.
저장소 관리	저장소 컨테이너를 생성, 삭제, 이동 또는 비우는 등 레코딩 서버에 있는 저장소 컨테이너를 관리할 수 있는 권한을 활성화합니다.
보안 관리	레코딩 서버에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

장애 조치 서버

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에서 장애 조치 서버를 확인하고 액세스할 수 있는 권한을 활성화합니다.
편집	Management Client 에서 장애 조치 서버를 생성, 업데이트, 삭제, 이동 및 활성화 또는 비활성화할 수 있는 권한을 활성화합니다.
보안 관리	장애 조치 서버에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

모바일 서버

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에서 모바일 서버를 확인하고 액세스할 수 있는 권한을 활성화합니다.
편집	Management Client 에서 모바일 서버를 편집하고 삭제할 수 있는 권한을 활성화합니다.
보안 관리	모바일 서버에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.
만들기	시스템에 모바일 서버를 추가할 수 있는 권한을 활성화합니다.

하드웨어

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
편집	하드웨어에 대한 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	하드웨어를 삭제할 수 있는 권한을 활성화합니다. 하드웨어 장치에 증거물 잠금이 포함되어 있는 경우, 레코딩 서버가 오프라인일 때만 하드웨어를 삭제할 수 있습니다.
드라이버 명령어	드라이버 특수 명령을 보내고 장치 자체에서 기능과 구성을 제어하는 권한을 활성화합니다. 이 **드라이버 명령** 권한은 클라이언트에서 특별히 개발된 MIP 플러그 인 전용입니다. 표준 구성 작업을 제어하지 않습니다.
암호 보기	**하드웨어 편집** 대화 상자의 하드웨어 장치에서 암호 보기 권한을 활성화합니다.
보안 관리	하드웨어에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

카메라

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트 및 Management Client 에 있는 카메라 장치를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 카메라의 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 카메라를 활성화하거나 비활성화할 수 있습니다.
라이브 보기	클라이언트 및 Management Client 에 있는 카메라에서 라이브 비디오를 볼 수 있는 권한을 활성화합니다.
제한된 라이브 보기	클라이언트 및 Management Client에 있는 카메라에서 라이브 제한된 비디오를 볼 수 있는 권한을 활성화합니다.
재생	모든 클라이언트에 있는 카메라에서 녹화 비디오를 재생할 수 있는 권한을 활성화합니다.
제한된 레코딩 재생	모든 클라이언트에 있는 카메라에서 녹화된 제한 비디오를 재생할 수 있는 권한을 활성화합니다.
원격 레코딩 검색	원격 사이트에 있는 카메라 또는 카메라의 에지 저장소에서 클라이언트의 레코딩을 검색할 수 있는 권한을 활성화합니다.
시퀀스 판독	예를 들어 클라이언트의 녹화된 비디오 재생과 같이 관련된 시퀀스 정보를 판독할 수 있는 권한을 활성화합니다.
스마트 검색	클라이언트에서 스마트 검색 기능을 사용할 수 있는 권한을 활성화합니다.
내보내기	클라이언트에서 레코딩을 내보낼 수 있는 권한을 활성화합니다.
북마크 만들기	클라이언트의 녹화 및 라이브 비디오에 북마크를 만들 수 있는 권한을 활성화합니다.
북마크 판독	클라이언트에서 북마크 세부 정보를 검색하여 판독할 수 있는 권한을 활성화합니다.

보안 권한	설명
북마크 편집	클라이언트에서 북마크를 편집할 수 있는 권한을 활성화합니다.
북마크 삭제	클라이언트에서 북마크를 삭제할 수 있는 권한을 활성화합니다.
증거물 잠금 생성 및 연장	클라이언트에서 증거물 잠금을 만들고 확장할 수 있는 권한을 활성화합니다.
증거물 잠금 판독	클라이언트에서 증거물 잠금을 검색하고 판독할 수 있는 권한을 활성화합니다.
증거물 잠금 삭제 및 줄이기	클라이언트에서 증거물 잠금을 삭제하거나 축소할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 생성 및 확장	클라이언트에서 제한을 만들고 확장할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 읽기	클라이언트에서 기존 제한 목록을 볼 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 삭제 및 축소	클라이언트에서 제한을 삭제하고 줄일 수 있는 권한을 활성화합니다.
수동 녹화 시작	클라이언트에서 비디오의 수동 녹화를 시작할 수 있는 권한을 활성화합니다.
수동 녹화 중지	클라이언트에서 비디오의 수동 녹화를 중단할 수 있는 권한을 활성화합니다.
AUX 명령	클라이언트에서 카메라의 보조(AUX) 명령을 사용할 수 있는 권한을 활성화합니다. **AUX 명령** 은 비디오 인코더를 통해 연결된 카메라의 와이퍼 등을 제어하는 기능을 사용자에게 제공합니다. 보조 연결을 통해 연결된 카메라 관련 장치는 클라이언트에서 제어됩니다.
수동 PTZ	클라이언트 및 Management Client 의 PTZ 카메라에서 PTZ 기능을 사용할 수 있는 권한을 활성화합니다.
PTZ 프리셋 또는 순찰 프로파일 활성화	클라이언트 및 Management Client 에서 PTZ 카메라를 프리셋 위치로 이동하고 순찰 프로파일을 시작 및 중지하고 순찰을 일시 중지할 수 있는 권한을 활성화합니다. 이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 프리셋 또는 순찰 프로파일 관리	클라이언트 및 Management Client 에서 PTZ 카메라에 대한 PTZ 프리셋과 순찰 프로파일을 추가, 편집 및 삭제할 수 있는 권한을 활성화합니다.

보안 권한	설명
	이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 프리셋 잠금/잠금 해제	Management Client 에서 PTZ 프리셋을 잠금 및 잠금 해제할 수 있는 권한을 활성화합니다. 그러면 다른 사용자가 클라이언트 및 Management Client 에서 프리셋 위치를 변경하지 못하거나 변경할 수 있게 됩니다.
PTZ 세션 보존	클라이언트 및 Management Client 에서 예약된 PTZ 세션 모드 상태로 PTZ 카메라를 설정할 수 있는 권한을 활성화합니다. 예약된 PTZ 세션에서 PTZ 우선순위가 더 높은 다른 사용자는 제어권을 가져갈 수 없습니다. 이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 세션 해제	Management Client 에서 다른 사용자의 PTZ 세션을 해제할 권한을 활성화합니다. 자신의 PTZ 세션은 이 권한 없이 언제든지 해제할 수 있습니다.
녹화 삭제	Management Client 을(를) 통해 시스템에서 저장된 비디오 레코딩을 삭제할 수 있는 권한을 활성화합니다.
사생활 보호 해제	XProtect Smart Client 에서 일시적으로 사생활 보호를 해제할 권한을 활성화합니다. 또한 다른 XProtect Smart Client 사용자가 사생활 보호의 해제를 승인할 권한을 활성화합니다. 사생활 보호 해제는 오직 Management Client 에서 해제 가능 사생활 보호로 구성된 사생활 보호에만 적용됩니다.
보안 관리	Management Client 에서 카메라에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

마이크

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트 및 Management Client 에 있는 마이크 장치를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 의 마이크 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 마이크를 활성화하거나 비활성화할 수 있습니다.
라이브 듣기	클라이언트 및 Management Client 에서 스피커의 라이브 오디오를 수신할 수 있는 권한을 활성화합니다.
제한된 라이브 오디오 듣기	클라이언트 및 Management Client에서 스피커에서 나오는 라이브 제한된 오디오를 수신할 수 있는 권한을 활성화합니다.
재생	클라이언트에서 마이크로부터 녹음된 오디오를 재생할 수 있는 권한을 활성화합니다.
제한된 레코딩 재생	클라이언트에서 마이크로폰으로부터 녹음된 제한된 오디오를 재생할 수 있는 권한을 활성화합니다.
원격 레코딩 검색	원격 사이트에 있는 마이크 또는 카메라의 에지 저장소에서 클라이언트의 레코딩을 검색할 수 있는 권한을 활성화합니다.
시퀀스 판독	예를 들어 클라이언트의 **재생** 탭와 같이 관련된 시퀀스 정보를 판독할 수 있는 권한을 활성화합니다.
내보내기	클라이언트에서 레코딩을 내보낼 수 있는 권한을 활성화합니다.
북마크 만들기	클라이언트에서 북마크를 생성할 수 있는 권한을 활성화합니다.
북마크 판독	클라이언트에서 북마크 세부 정보를 검색하여 판독할 수 있는 권한을 활성화합니다.
북마크 편집	클라이언트에서 북마크를 편집할 수 있는 권한을 활성화합니다.
북마크 삭제	클라이언트에서 북마크를 삭제할 수 있는 권한을 활성화합니다.
증거물 잠금 생성 및 연장	클라이언트에서 증거물 잠금을 만들거나 확장할 수 있는 권한을 활성화합니다.
증거물 잠금 판독	클라이언트에서 증거물 잠금 상세 정보를 검색하고 판독할 수 있는 권한을 활성화합니다.
증거물 잠금 삭제 및	클라이언트에서 증거물 잠금을 삭제하거나 축소할 수 있는 권한을 활성화합니다.

보안 권한	설명
줄이기	
라이브 및 재생 제한 생성 및 확장	클라이언트에서 마이크로폰의 제한을 만들고 확장할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 읽기	클라이언트에서 마이크로폰의 기존 제한 목록을 볼 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 삭제 및 축소	클라이언트에서 마이크로폰의 제한을 삭제하고 줄일 수 있는 권한을 활성화합니다.
수동 녹화 시작	클라이언트에서 오디오의 수동 녹음을 시작할 수 있는 권한을 활성화합니다.
수동 녹화 중지	클라이언트에서 오디오의 수동 녹음을 중단할 수 있는 권한을 활성화합니다.
녹화 삭제	시스템에서 저장된 레코딩을 삭제할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 마이크에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

스피커

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트 및 Management Client 에 있는 스피커 장치를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 스피커의 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 스피커를 활성화하거나 비활성화할 수 있습니다.
라이브 듣기	클라이언트 및 Management Client 에서 스피커의 라이브 오디오를 수신할 수 있는 권한을 활성화합니다.

보안 권한	설명
제한된 라이브 오디오 듣기	클라이언트 및 Management Client에서 스피커에서 나오는 라이브 제한된 오디오를 수신할 수 있는 권한을 활성화합니다.
말하기	클라이언트에서 스피커를 통해 말할 수 있는 권한을 활성화합니다.
재생	클라이언트에서 스피커로부터 녹음된 오디오를 재생할 수 있는 권한을 활성화합니다.
제한된 레코딩 재생	클라이언트에서 스피커로부터 녹음된 오디오를 재생할 수 있는 권한을 활성화합니다.
원격 레코딩 검색	원격 사이트에 있는 스피커 또는 카메라의 에지 저장소에서 클라이언트의 레코딩을 검색할 수 있는 권한을 활성화합니다.
시퀀스 판독	클라이언트의 스피커에서 녹음된 오디오를 찾으면서 시퀀스 기능을 사용할 수 있는 권한을 활성화합니다.
내보내기	클라이언트에서 스피커로부터 녹음된 오디오를 내보낼 수 있는 권한을 활성화합니다.
북마크 만들기	클라이언트에서 북마크를 생성할 수 있는 권한을 활성화합니다.
북마크 판독	클라이언트에서 북마크 세부 정보를 검색하여 판독할 수 있는 권한을 활성화합니다.
북마크 편집	클라이언트에서 북마크를 편집할 수 있는 권한을 활성화합니다.
북마크 삭제	클라이언트에서 북마크를 삭제할 수 있는 권한을 활성화합니다.
증거물 잠금 생성 및 연장	클라이언트에서 레코딩된 오디오를 보호하기 위해 증거물 잠금을 만들거나 확장할 수 있는 권한을 활성화합니다.
증거물 잠금 판독	클라이언트에서 증거물 잠금에 의해 보호되고 레코딩된 오디오를 볼 수 있는 권한을 활성화합니다.
증거물 잠금 삭제 및 줄이기	클라이언트에서 보호된 오디오에 대한 증거물 잠금을 삭제하거나 축소할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 생성 및 확장	클라이언트에서 스피커의 제한을 만들고 확장할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 읽기	클라이언트에서 스피커의 기존 제한 목록을 볼 수 있는 권한을 활성화합니다.

보안 권한	설명
라이브 및 재생 제한 삭제 및 축소	클라이언트에서 스피커의 제한을 삭제하고 줄일 수 있는 권한을 활성화합니다.
수동 녹화 시작	클라이언트에서 오디오의 수동 녹음을 시작할 수 있는 권한을 활성화합니다.
수동 녹화 중지	클라이언트에서 오디오의 수동 녹음을 중단할 수 있는 권한을 활성화합니다.
녹화 삭제	시스템에서 저장된 레코딩을 삭제할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 스피커에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

메타데이터

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트에서 메타데이터를 수신할 수 있는 권한을 활성화합니다.
편집	Management Client 의 메타데이터 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 메타데이터 장치를 활성화하거나 비활성화할 수 있습니다.
실시간	클라이언트에 있는 메타데이터 장치에서 라이브 메타데이터를 수신할 수 있는 권한을 활성화합니다.
제한된 라이브 보기	클라이언트에서 메타데이터 장치에서 라이브 제한된 메타데이터를 수신할 수 있는 권한을 활성화합니다.
재생	클라이언트에서 메타데이터 장치로부터 녹화된 데이터를 재생할 수 있는 권한을 활성화합니다.
제한된 레코딩 재생	클라이언트에서 메타데이터 장치로부터 제한된 녹화 데이터를 재생할 수 있는 권한을 활성

보안 권한	설명
	화합니다.
원격 레코딩 검색	원격 사이트에 있는 메타데이터 장치 또는 카메라의 에지 저장소에서 클라이언트의 레코딩을 검색할 수 있는 권한을 활성화합니다.
시퀀스 판독	예를 들어 클라이언트의 **재생** 탭와 같이 관련된 시퀀스 정보를 판독할 수 있는 권한을 활성화합니다.
내보내기	클라이언트에서 레코딩을 내보낼 수 있는 권한을 활성화합니다.
증거물 잠금 생성 및 연장	클라이언트에서 증거물 잠금을 만들 수 있는 권한을 활성화합니다.
증거물 잠금 판독	클라이언트에서 증거물 잠금을 볼 수 있는 권한을 활성화합니다.
증거물 잠금 삭제 및 줄이기	클라이언트에서 증거물 잠금을 삭제하거나 축소할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 생성 및 확장	클라이언트에서 메타데이터의 제한을 만들고 확장할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 읽기	클라이언트에서 메타데이터의 기존 제한 목록을 볼 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 삭제 및 축소	클라이언트에서 메타데이터의 제한을 삭제하고 줄일 수 있는 권한을 활성화합니다.
수동 녹화 시작	클라이언트에서 메타데이터의 수동 기록을 시작할 수 있는 권한을 활성화합니다.
수동 녹화 중지	클라이언트에서 메타데이터의 수동 기록을 중단할 수 있는 권한을 활성화합니다.
녹화 삭제	시스템에서 저장된 레코딩을 삭제할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 메타데이터에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

입력

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트 및 Management Client 에 있는 입력 장치를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 입력 장치의 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 입력 장치를 활성화하거나 비활성화할 수 있습니다.
보안 관리	Management Client에서 입력 장치에 대해 보안 권한을 관리할 수 있는 권한을 활성화합니다.

출력

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트에 있는 출력 장치를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 출력 장치의 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 출력 장치를 활성화하거나 비활성화할 수 있습니다.
활성화	클라이언트에서 출력을 활성화할 수 있는 권한을 활성화합니다.
보안 관리	Management Client에서 출력 장치에 대해 보안 권한을 관리할 수 있는 권한을 활성화합니다.

Smart Wall

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	XProtect Management Client 에서의 모든 보안 권한을 관리할 수 있는 권한을 활성화합니다.
판독	XProtect Smart Client 에 있는 비디오 월을 볼 수 있는 권한을 활성화합니다.
편집	Smart Wall 에서 XProtect Management Client 정의에 대한 속성을 편집할 수 있는 권한을 사용하도록 설정합니다.
삭제	Smart Wall 에서 기존 XProtect Management Client 정의를 삭제할 권한을 사용하도록 설정합니다.
작동	Smart Wall 정의를 활성화하고 수정할 권한을 사용하도록 설정합니다(예: XProtect Smart Client 및 XProtect Management Client 에서 프리셋을 변경하고 활성화하거나 뷰에 카메라를 적용). **작업** 을 사용자 권한이 적용되는 시기를 정의하는 시간 프로파일에 연결할 수 있습니다.
생성 Smart Wall	Smart Wall 에서 새 XProtect Management Client 정의를 생성할 수 있는 권한을 사용하도록 설정합니다.
보안 관리	Smart Wall 정의를 위한 XProtect Management Client에서 보안 권한을 관리할 수 있는 권한을 사용하도록 설정합니다.
재생	XProtect Smart Client 의 비디오 월에서 기록된 데이터를 재생할 수 있는 권한을 활성화합니다. **재생** 을 사용자 권한이 적용되는 시기를 정의하는 시간 프로파일에 연결할 수 있습니다.

뷰 그룹

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트와 Management Client 에서 뷰 그룹을 볼 수 있는 권한을 활성화합니다. 뷰 그룹은 Management Client 에서 만들어집니다.
편집	Management Client 에 있는 뷰 그룹의 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	Management Client 에 있는 뷰 그룹을 삭제할 수 있는 권한을 활성화합니다.
작동	XProtect Smart Client 에서 뷰 그룹을 사용, 즉 하위 그룹과 뷰를 만들고 삭제할 수 있는 권한을 활성화합니다.
뷰 그룹 만들기	Management Client 에 있는 뷰 그룹을 생성할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 뷰 그룹에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

사용자 정의 이벤트

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트에서 사용자 정의 이벤트를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 사용자 정의 이벤트의 속성을 편집할 수 있는 권한을 활성화합니다.

보안 권한	설명
삭제	Management Client 에 있는 사용자 정의 이벤트를 삭제할 수 있는 권한을 활성화합니다.
트리거	클라이언트에서 사용자 정의 이벤트를 트리거할 수 있는 권한을 활성화합니다.
보안 관리	Management Client에서 사용자 정의 이벤트에 대해 보안 권한을 관리할 수 있는 권한을 활성화합니다.
사용자 정의 이벤트 만들기	Management Client 에 있는 사용자 정의 이벤트를 생성할 수 있는 권한을 활성화합니다.

분석 이벤트

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에 있는 분석 이벤트를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 분석 이벤트의 속성을 편집할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 분석 이벤트에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

일반 이벤트

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트 및 Management Client 에서 일반 이벤트를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에 있는 일반 이벤트의 속성을 편집할 수 있는 권한을 활성화합니다.
보안 관리	Management Client에서 일반 이벤트에 대해 보안 권한을 관리할 수 있는 권한을 활성화합니다.

Matrix

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	클라이언트에서 비디오를 선택하여 Matrix 수신자에게 보낼 수 있는 권한을 활성화합니다.
편집	Matrix 에 있는 Management Client 에 대한 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	Matrix 에 있는 Management Client 을(를) 삭제할 수 있는 권한을 활성화합니다.
생성 Matrix	Matrix에 있는 새로운 Management Client 을(를) 생성할 수 있는 권한을 활성화합니다.
보안 관리	Management Client에서 모든 Matrix 에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

규칙

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에 있는 기존의 규칙을 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에서 규칙의 속성을 편집하고 규칙 동작을 정의할 수 있는 권한을 활성화합니다. 또한 해당 규칙에 의해 영향을 받는 모든 장치에서 사용자가 읽기 권한을 가지고 있어야 합니다.

보안 권한	설명
삭제	Management Client 에서 규칙을 삭제할 수 있는 권한을 활성화합니다. 또한 해당 규칙에 의해 영향을 받는 모든 장치에서 사용자가 읽기 권한을 가지고 있어야 합니다.
규칙 만들기	Management Client 에서 새로운 규칙을 생성할 수 있는 권한을 활성화합니다. 또한 해당 규칙에 의해 영향을 받는 모든 장치에서 사용자가 읽기 권한을 가지고 있어야 합니다.
보안 관리	Management Client에서 모든 규칙에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

사이트

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에 있는 다른 사이트를 볼 수 있는 권한을 활성화합니다. 연결된 사이트는 Milestone Federated Architecture 을(를) 통해 연결됩니다. 속성을 편집하려면 각 사이트의 관리 서버에서 편집 권한이 필요합니다.
보안 관리	모든 사이트에서의 보안 권한을 관리할 수 있는 권한을 활성화합니다.

시스템 모니터

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	XProtect Smart Client 에서 시스템 모니터를 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에서 시스템 모니터의 속성을 편집할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 모든 시스템 모니터에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

메타데이터 검색

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 및 관련 설정에서 **메타데이터 사용** 기능 보기에 대한 권한을 활성화할 수 있지만 설정을 변경할 권한은 활성화할 수 없습니다.
메타데이터 검색 구성 편집	메타데이터 검색 카테고리 활성화 또는 비활성화 권한을 활성화합니다(예: Management Client 에서 인물 또는 자동차에 대한 메타데이터).
보안 관리	메타데이터 검색을 위한 보안 권한 관리를 위한 권한을 활성화합니다.

검색

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트(https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
공개 검색 읽기	XProtect Smart Client 에서 저장된 공개 검색을 조회하고 열 수 있는 권한을 활성화합니다.
공개 검색 생성	XProtect Smart Client 에서 공개 검색으로서 새롭게 구성된 검색을 저장할 권한을 활성화합니다.
공개 검색 편집	상세 내용이나 XProtect Smart Client 내의 저장된 공개 검색 구성(예: 이름과 설명, 카메라, 검색 카테고리) 편집 권한을 활성화합니다.
공개 검색 삭제	저장된 공개 검색을 삭제할 권한을 활성화합니다.
보안 관리	Management Client 에서 검색에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

알람

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
관리	Smart Client 에서 알람을 관리할 수 있는 권한을 활성화합니다. 예를 들어 알람 우선순위 변경, 다른 사용자에게 알람 다시 할당, 알람 승인, 여러 알람의 알람 상태 변경(예: **신규**에서 **할당됨**으로 변경)이 있습니다. 알람 설정을 편집하려면 **알람 설정 편집** 권한도 필요합니다. 이 항목을 허용된 것으로 설정하는 경우에만 **옵션** 대화 상자에서 **알람 및 이벤트** 탭이 표시됩니다.
뷰	XProtect Smart Client의 **알람 관리자** 탭을 보고 API를 통해 알람 및 알람 설정을 검색할 수 있는 권한을 활성화합니다.

보안 권한	설명
	XProtect Smart Client에서 알람을 확인하려면 하나 이상의 알람 정의에 대해 **보기** 권한을 활성화해야 합니다. 기본적으로 써드파티 솔루션의 알람이 표시됩니다.
알람 비활성화	알람을 비활성화할 수 있는 권한을 활성화합니다.
알림 수신	XProtect Mobile 클라이언트 및 XProtect Web Client 에서 알람에 관한 알림을 수신할 수 있는 권한을 활성화합니다.
보안 관리	알람에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.
알람 설정 편집	알람 정의, 알람 상태, 알람 카테고리, 알람 소리, 알람 보존, 이벤트 보존을 편집할 수 있는 권한을 활성화합니다. 알람 설정을 편집하려면 **관리** 권한도 필요합니다.

알람 정의

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
뷰	알람 정의, 알람 상태, 알람 카테고리, 알람 소리, 알람 보존, 이벤트 보존을 편집할 수 있는 권한을 활성화합니다.
쓰기	**보기** 권한을 활성화합니다.
보안 관리	알람 정의에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

서버 로그

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
시스템 로그 엔트리 판독	시스템 로그 엔트리를 볼 수 있는 권한을 활성화합니다.
감사 로그 엔트리 판독	감사 로그 엔트리를 볼 수 있는 권한을 활성화합니다.
규칙으로 트리거된 로그 엔트리 판독	규칙으로 트리거된 로그 엔트리를 볼 수 있는 권한을 활성화합니다.
로그 구성 판독	**도구** > **옵션** > **서버 로그** 에서 로그 설정 판독 권한을 활성화합니다.
로그 구성 업데이트	**도구** > **옵션** > **서버 로그** 에서 로그 설정 변경 권한을 활성화합니다.
보안 관리	알람에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

액세스 제어

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
편집	Management Client 에서 액세스 제어 시스템에 대한 속성을 편집할 수 있는 권한을 활성화합니다.
액세스 제어 사용	사용자가 클라이언트에서 액세스 제어 관련 기능을 사용할 수 있습니다.
카드 소유자 목록 보	**사용자가 클라이언트의** 액세스 제어 탭에서 카드 소유자 목록을 볼 수 있습니다.

보안 권한	설명
기	
알림 수신	사용자가 클라이언트에서 액세스 요청에 대한 알림을 받을 수 있습니다.
보안 관리	모든 액세스 제어 시스템에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

LPR

해당 시스템이 XProtect LPR 에서 실행되는 경우, 사용자에 대해 다음 권한을 지정합니다.

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
LPR 사용	클라이언트에서 LPR 관련 기능을 사용할 수 있는 권한을 활성화합니다.
자동차 번호판 일치 목록 관리	Management Client에서 자동차번호판 일치 목록을 추가, 가져오기, 수정, 내보내기 및 삭제할 수 있는 권한을 활성화합니다.
자동차 번호판 일치 목록	자동차번호판 일치 목록을 볼 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 모든 트랜잭션 정의에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

트랜잭션 소스

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에서 트랜잭션 소스에 대한 속성을 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에서 트랜잭션 소스에 대한 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	Management Client 에서 트랜잭션 소스를 삭제할 수 있는 권한을 활성화합니다.

보안 권한	설명
만들기	Management Client 에서 새로운 트랜잭션 소스를 생성할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 모든 트랜잭션 소스에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

트랜잭션 정의

보안 권한	설명
전체 제어	이 시스템 부분에서 모든 보안 항목을 관리할 수 있는 권한을 활성화합니다.
판독	Management Client 에서 트랜잭션 정의에 대한 속성을 볼 수 있는 권한을 활성화합니다.
편집	Management Client 에서 트랜잭션 정의에 대한 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	Management Client 에서 트랜잭션 정의를 삭제할 수 있는 권한을 활성화합니다.
만들기	Management Client 에서 새로운 트랜잭션 정의를 생성할 수 있는 권한을 활성화합니다.
보안 관리	Management Client 에서 모든 트랜잭션 정의에 대한 보안 권한을 관리할 수 있는 권한을 활성화합니다.

MIP 플러그 인

MIP SDK 을(를) 통해 타사 공급업체가 사용 중인 시스템에 대한 사용자 정의 플러그 인을 개발할 수 있습니다(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합).

장치 탭(역할)

> 사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 전체 기능 목록은 Milestone 웹사이트 (https://www.milestonesys.com/products/software/product-index/)의 제품 개요 페이지에서 확인하십시오.

장치 탭에서는 XProtect Smart Client 에서 각 장치(예: 카메라) 또는 장치 그룹에 대해 선택한 역할을 가진 사용자/그룹이 사용할 수 있는 기능을 지정할 수 있습니다.

각 장치에 대해 설정을 반복해야 함을 유념하십시오. 또한 장치 그룹을 선택하고 그룹 내의 모든 장치에 대해 한 번에 역할 권한을 지정할 수도 있습니다.

사각형으로 채워진 확인란을 선택하거나 선택 취소할 수 있지만, 이 경우 해당 선택은 장치 그룹 내의 **모든** 장치에 적용됩니다. 또는 장치 그룹에서 개별 장치를 선택하여 관련 권한이 적용되는 장치를 정확히 확인하십시오.

카메라 관련 권한

카메라 장치에 대해 다음 권한을 지정합니다:

이름	설명
판독	선택한 카메라를 클라이언트에서 볼 수 있게 됩니다.
라이브 보기	클라이언트에서 선택한 카메라의 비디오 라이브 보기를 허용합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
제한된 라이브 보기	클라이언트에서 선택한 카메라의 제한된 비디오에 대한 라이브 보기를 허용합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 시간 프로파일 이내	클라이언트에서 선택한 카메라의 녹화 비디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 재생 제한	클라이언트에서 선택한 카메라의 녹화 비디오 재생을 허용합니다. 재생 제한을 지정하거나 제한 없음을 적용합니다.
제한된 레코딩 재생	클라이언트에서 선택한 카메라의 제한된 녹화 비디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
시퀀스 판독	예를 들어 클라이언트의 시퀀스 탐색기와 같이 관련된 시퀀스 정보의 판독을 허용합니다.
스마트 검색	사용자가 클라이언트에서 스마트 검색 기능을 사용할 수 있습니다.
내보내기	사용자가 클라이언트에서 레코딩을 내보낼 수 있습니다.
수동 녹화 시작	클라이언트에서 선택한 카메라의 비디오 수동 녹화 시작을 허용합니다.

이름	설명
수동 녹화 중지	클라이언트에서 선택한 카메라의 비디오 수동 녹화 중지를 허용합니다.
북마크 판독	클라이언트에서 북마크 세부 정보 검색과 판독을 허용합니다.
북마크 편집	클라이언트에서 북마크 편집을 허용합니다.
북마크 만들기	클라이언트에서 북마크 추가를 허용합니다.
북마크 삭제	클라이언트에서 북마크 삭제를 허용합니다.
AUX 명령	클라이언트에서 보조 명령 사용을 허용합니다.
증거물 잠금 생성 및 연장	클라이언트 사용자가 다음을 할 수 있습니다: • 신규 또는 기존 증거물 잠금에 카메라를 추가합니다 • 기존 증거물 잠금의 만료 시간을 연장합니다 • 기존 증거물 잠금의 보호 간격을 연장합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
증거물 잠금 삭제 및 줄이기	클라이언트 사용자가 다음을 할 수 있습니다: • 기존 증거물 잠금에서 카메라를 제거합니다 • 기존 증거물 잠금을 삭제합니다 • 기존 증거물 잠금의 만료 시간을 단축합니다 • 기존 증거물 잠금의 보호 간격을 단축합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
증거물 잠금 판독	클라이언트 사용자가 증거물 잠금 세부 정보를 검색하고 판독할 수 있습니다.
라이브 및 재생 제한 생성 및 확장	클라이언트 사용자가 다음을 할 수 있습니다: • 카메라에 라이브 제한 만들기 • 카메라 레코딩에 재생 제한 만들기

이름	설명
	• 새 카메라를 라이브 또는 재생 제한에 추가 • 카메라 레코딩 제한 기간 연장 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
라이브 및 재생 제한 읽기	클라이언트 사용자가 다음을 할 수 있습니다: • 카메라의 기존 라이브 및 재생 제한 목록 보기 • 카메라의 라이브 및 재생 제한 목록 필터링 및 검색
라이브 및 재생 제한 삭제 및 축소	클라이언트 사용자가 다음을 할 수 있습니다: • 카메라에 라이브 제한 제거하기 • 카메라 레코딩에 재생 제한 제거하기 • 카메라 레코딩 제한 기간 줄이기 • 라이브 또는 재생 제한 설정 변경하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.

마이크 관련 권한

마이크 장치에 대해 다음 권한을 지정합니다.

이름	설명
판독	선택한 마이크를 클라이언트에서 볼 수 있게 됩니다.
라이브 듣기	클라이언트에서 선택한 마이크의 라이브 오디오 수신을 허용합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
제한된 라이브 오디오 듣기	클라이언트에서 선택한 마이크로폰에서 라이브 제한된 비디오 듣기를 허용합니다.

이름	설명
	XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 시간 프로파일 이내	클라이언트에서 선택한 마이크의 녹음 오디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 재생 제한	클라이언트에서 선택한 마이크의 녹음 오디오 재생을 허용합니다. 재생 제한을 지정하거나 제한 없음을 적용합니다.
제한된 레코딩 재생	클라이언트에서 선택한 마이크로폰에서 녹음된 제한 오디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
시퀀스 판독	예를 들어 클라이언트의 시퀀스 탐색기와 같이 관련된 시퀀스 정보의 판독을 허용합니다.
내보내기	사용자가 클라이언트에서 레코딩을 내보낼 수 있습니다.
수동 녹화 시작	클라이언트에서 선택한 마이크의 오디오 수동 녹음 시작을 허용합니다.
수동 녹화 중지	클라이언트에서 선택한 마이크의 오디오 수동 녹음 중지를 허용합니다.
북마크 판독	클라이언트에서 북마크 세부 정보 검색과 판독을 허용합니다.
북마크 편집	클라이언트에서 북마크 편집을 허용합니다.
북마크 만들기	클라이언트에서 북마크 추가를 허용합니다.
북마크 삭제	클라이언트에서 북마크 삭제를 허용합니다.
증거물 잠금 생성 및 연장	클라이언트 사용자가 다음을 할 수 있습니다: • 신규 또는 기존 증거물 잠금에 마이크로폰을 추가합니다 • 기존 증거물 잠금의 만료 시간을 연장합니다 • 기존 증거물 잠금의 보호 간격을 연장합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.

이름	설명
증거물 잠금 삭제 및 줄이기	클라이언트 사용자가 다음을 할 수 있습니다: • 기존 증거물 잠금에서 마이크로폰을 제거합니다 • 기존 증거물 잠금을 삭제합니다 • 기존 증거물 잠금의 만료 시간을 단축합니다 • 기존 증거물 잠금의 보호 간격을 단축합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
증거물 잠금 판독	클라이언트 사용자가 증거물 잠금 세부 정보를 검색하고 판독할 수 있습니다.
라이브 및 재생 제한 생성 및 확장	클라이언트 사용자가 다음을 할 수 있습니다: • 마이크로폰에 라이브 제한 만들기 • 오디오 레코딩에 재생 제한 만들기 • 새 마이크로폰을 라이브 또는 재생 제한에 추가하기 • 오디오 레코딩 제한 기간 연장하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
라이브 및 재생 제한 읽기	클라이언트 사용자가 다음을 할 수 있습니다: • 마이크로폰의 기존 라이브 및 재생 제한 목록 보기 • 마이크로폰의 라이브 및 재생 제한 목록 필터링 및 검색
라이브 및 재생 제한 삭제 및 축소	클라이언트 사용자가 다음을 할 수 있습니다: • 마이크로폰에 라이브 제한 제거하기 • 오디오 레코딩에 재생 제한 제거하기 • 오디오 레코딩 제한 기간 줄이기 • 라이브 또는 재생 제한 설정 변경하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.

스피커 관련 권한

스피커 장치에 대해 다음 권한을 지정합니다.

이름	설명
판독	선택한 스피커를 클라이언트에서 볼 수 있습니다.
라이브 듣기	클라이언트에서 선택한 스피커의 라이브 오디오 수신을 허용합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
제한된 라이브 오디오 듣기	클라이언트에서 선택한 스피커의 라이브 제한된 비디오 듣기를 허용합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 시간 프로파일 이내	클라이언트에서 선택한 스피커의 녹음 오디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
재생 > 재생 제한	클라이언트에서 선택한 스피커의 녹음 오디오 재생을 허용합니다. 재생 제한을 지정하거나 제한 없음을 적용합니다.
제한된 레코딩 재생	클라이언트에서 선택한 스피커의 녹음된 제한 오디오 재생을 허용합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
시퀀스 판독	예를 들어 클라이언트의 시퀀스 탐색기와 같이 관련된 시퀀스 정보의 판독을 허용합니다.
내보내기	사용자가 클라이언트에서 레코딩을 내보낼 수 있습니다.
수동 녹화 시작	클라이언트에서 선택한 스피커의 오디오 수동 녹음 시작을 허용합니다.
수동 녹화 중지	클라이언트에서 선택한 스피커의 오디오 수동 녹음 중지를 허용합니다.
북마크 판독	클라이언트에서 북마크 세부 정보 검색과 판독을 허용합니다.
북마크 편집	클라이언트에서 북마크 편집을 허용합니다.
북마크 만들기	클라이언트에서 북마크 추가를 허용합니다.

이름	설명
북마크 삭제	클라이언트에서 북마크 삭제를 허용합니다.
증거물 잠금 생성 및 연장	클라이언트 사용자가 다음을 할 수 있습니다: • 신규 또는 기존 증거물 잠금에 스피커를 추가합니다 • 기존 증거물 잠금의 만료 시간을 연장합니다 • 기존 증거물 잠금의 보호 간격을 연장합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
증거물 잠금 삭제 및 줄이기	클라이언트 사용자가 다음을 할 수 있습니다: • 기존 증거물 잠금에서 스피커를 제거합니다 • 기존 증거물 잠금을 삭제합니다 • 기존 증거물 잠금의 만료 시간을 단축합니다 • 기존 증거물 잠금의 보호 간격을 단축합니다 증거물 잠금에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
증거물 잠금 판독	클라이언트 사용자가 증거물 잠금 세부 정보를 검색하고 판독할 수 있습니다.
라이브 및 재생 제한 생성 및 확장	클라이언트 사용자가 다음을 할 수 있습니다: • 스피커에 라이브 제한 만들기 • 오디오 레코딩에 재생 제한 만들기 • 새 마이크로폰을 라이브 또는 재생 제한에 추가하기 • 오디오 레코딩 제한 기간 연장하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
라이브 및 재생 제한 읽기	클라이언트 사용자가 다음을 할 수 있습니다: • 스피커에 기존 라이브 및 재생 제한 목록 보기

이름	설명
	• 스피커에 라이브 및 재생 제한 목록 필터링 및 검색
라이브 및 재생 제한 삭제 및 축소	클라이언트 사용자가 다음을 할 수 있습니다: • 스피커에 라이브 제한 제거하기 • 오디오 레코딩에 재생 제한 제거하기 • 오디오 레코딩 제한 기간 줄이기 • 라이브 또는 재생 제한 설정 변경하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.

메타데이터 관련 권한

메타데이터 장치에 대해 다음 권한을 지정합니다.

이름	설명
판독	클라이언트에서 메타데이터 장치를 확인하고 해당 장치에서 데이터를 검색할 수 있는 권한을 활성화합니다.
편집	메타데이터 속성을 편집할 수 있는 권한을 활성화합니다. 또한 사용자가 Management Client 에서 그리고 MIP SDK 을(를) 통해 메타데이터 장치를 활성화하거나 비활성화할 수 있습니다.
라이브 보기	클라이언트에 있는 카메라에서 라이브 메타데이터를 볼 수 있는 권한을 활성화합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다.
라이브 제한 보기	클라이언트에 있는 카메라에서 라이브 제한된 메타데이터를 볼 수 있는 권한을 활성화합니다. XProtect Smart Client 의 경우, 해당 역할에 클라이언트의 **라이브** 탭을 볼 수 있는 권한이 부여되었어야 합니다. 이 권한은 응용 프로그램 권한의 일부로 허용되었습니다.
재생	클라이언트에서 메타데이터 장치로부터 녹화된 데이터를 재생할 수 있는 권한을 활성화합니다.

이름	설명
제한된 레코딩 재생	클라이언트에서 제한된 메타데이터 장치로부터 녹화된 데이터를 재생할 수 있는 권한을 활성화합니다.
시퀀스 판독	클라이언트의 메타데이터 장치에서 녹화된 데이터를 검색하면서 시퀀스 기능을 사용할 수 있는 권한을 활성화합니다.
내보내기	클라이언트에서 메타데이터 장치로부터 녹음된 오디오를 내보낼 수 있는 권한을 활성화합니다.
증거물 잠금 생성 및 연장	클라이언트에서 메타데이터에 증거물 잠금을 만들어 확장할 수 있는 권한을 활성화합니다.
증거물 잠금 판독	클라이언트의 메타데이터에서 증거물 잠금을 볼 수 있는 권한을 활성화합니다.
증거물 잠금 삭제 및 줄이기	클라이언트의 메타데이터에서 증거물 잠금을 삭제하거나 축소할 수 있는 권한을 활성화합니다.
수동 녹화 시작	클라이언트에서 메타데이터의 수동 기록을 시작할 수 있는 권한을 활성화합니다.
수동 녹화 중지	클라이언트에서 메타데이터의 수동 기록을 중단할 수 있는 권한을 활성화합니다.
라이브 및 재생 제한 생성 및 확장	클라이언트 사용자가 다음을 할 수 있습니다: • 메타데이터 장치에 라이브 제한 만들기 • 메타데이터 장치에 재생 제한 만들기 • 새 메타데이터를 라이브 또는 재생 제한에 추가하기 • 메타데이터 장치의 제한 기간 연장하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.
라이브 및 재생 제한 읽기	클라이언트 사용자가 다음을 할 수 있습니다: • 메타데이터 장치의 기존 라이브 및 재생 제한 목록 보기 • 메타데이터 장치의 라이브 및 재생 제한 목록 필터링 및 검색하기
라이브 및 재생 제한 삭제 및 축소	클라이언트 사용자가 다음을 할 수 있습니다:

이름	설명
	• 메타데이터 장치에 라이브 제한 제거하기 • 메타데이터 장치에 재생 제한 제거하기 • 메타데이터 장치의 제한 기간 줄이기 • 라이브 또는 재생 제한 설정 변경하기 제한에 포함된 모든 장치에 대해 사용자 권한이 필요합니다.

입력 관련 권한

입력 장치에 대해 다음 권한을 지정합니다.

이름	설명
판독	선택한 입력을 클라이언트에서 볼 수 있게 됩니다.

출력 관련 권한

출력 장치에 대해 다음 권한을 지정합니다.

이름	설명
판독	선택한 출력을 클라이언트에서 볼 수 있게 됩니다. 표시되면 클라이언트의 목록에서 해당 출력을 선택할 수 있습니다.
활성화	선택한 출력을 Management Client 및 클라이언트에서 활성화할 수 있습니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.

PTZ 탭(역할)

PTZ 탭에서 이동-기울기-줌(PTZ) 카메라에 대한 권한을 설정합니다. 사용자/그룹이 클라이언트에서 사용할 수 있는 기능을 지정할 수 있습니다. 개별 PTZ 카메라 또는 PTZ 카메라가 들어 있는 장치 그룹을 선택할 수 있습니다.

PTZ에 대해 다음 권한을 지정합니다.

이름	설명
수동 PTZ	선택한 역할이 선택한 카메라에서 PTZ 기능을 사용하고 순찰을 일시 중지할 수 있는지 여부를 결정합니다. 시간 프로파일을 지정하거나, **항상** 을 선택하거나, 해당 역할에 대한 **정보** 탭에 정의된 기본 시간 프로파일을 따르는 기본값을 유지합니다.
PTZ 프리셋 또는 순찰 프로파일 활성화	선택한 역할이 선택한 카메라를 프리셋 위치로 이동하고, 순찰 프로파일을 시작 및 중지하고, 순찰을 일시 중지할 수 있는지 여부를 결정합니다. 시간 프로파일을 지정하거나, **항상** 을 선택하거나, 해당 역할에 대한 **정보** 탭에 정의된 기본 시간 프로파일을 따르는 기본값을 유지합니다. 이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 우선순위	PTZ 카메라의 우선순위를 결정합니다. 감시 시스템에서 여러 사용자가 동시에 같은 PTZ 카메라를 제어하려는 경우, 충돌이 발생할 수 있습니다. 선택한 역할을 가진 사용자/그룹을 기준으로 선택한 PTZ 카메라 사용에 대한 우선순위를 지정하여 그러한 상황을 피할 수 있습니다. 1을 가장 낮은 우선순위로 하여 1부터 32,000까지의 우선순위를 지정합니다. 기본 우선 순위는 3,000입니다. 가장 높은 우선순위 번호를 가진 역할이 PTZ 카메라를 제어할 수 있습니다.
PTZ 프리셋 또는 순찰 프로파일 관리	Management Client 및 XProtect Smart Client 모두에서 선택된 카메라에 대한 PTZ 프리셋과 순찰 프로파일을 추가, 편집 및 삭제할 수 있는 권한을 결정합니다. 이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 프리셋 잠금/잠금 해제	역할이 선택 카메라에 대한 프리셋 위치를 잠그거나 잠금 해제할 수 있는지 여부를 결정합니다.
PTZ 세션 보존	선택한 카메라를 예약된 PTZ 세션 모드로 설정할 수 있는 권한을 결정합니다. 예약된 PTZ 세션에서 PTZ 우선순위가 더 높은 다른 사용자나 순찰 세션은 제어권을 가져갈 수 없습니다. 이 역할이 카메라에서 다른 PTZ 기능을 사용하도록 허용하려면 **수동 PTZ** 권한을 활성화합니다.
PTZ 세션 해제	선택한 역할이 Management Client 에서 다른 사용자의 PTZ 세션을 해제할 수 있는지 여부를 결정합니다. 자신의 PTZ 세션은 이 권한 없이 언제든지 해제할 수 있습니다.

음성 탭(역할)

시스템에서 스피커를 사용하는 경우에만 해당됩니다. 스피커에 대해 다음 권한을 지정합니다.

이름	설명
말하기	사용자가 선택한 스피커를 통해 말할 수 있어야 하는지 결정합니다. 시간 프로파일을 지정하거나 기본값을 그대로 유지합니다.
말하기 우선순위	여러 클라이언트 사용자가 동시에 같은 스피커를 통해 말할 경우, 충돌이 발생할 수 있습니다. 선택한 역할을 가진 사용자/그룹을 기준으로 선택한 스피커 사용에 대한 우선순위를 지정하여 문제를 해결할 수 있습니다. **매우 낮음** 에서 **매우 높음** 까지 우선 순위를 지정합니다. 우선순위가 가장 높은 역할이 다른 역할보다 먼저 스피커를 사용할 수 있습니다. 동일 역할을 가진 두 명의 사용자가 동시에 말하기를 원하는 경우, 선착순 원칙이 적용됩니다.

원격 녹화 탭(역할)

원격 녹화에 대해 다음 권한을 지정합니다.

이름	설명
원격 레코딩 검색	원격 사이트에 있는 카메라, 마이크, 스피커 및 메타데이터 장치 또는 카메라의 에지 저장소에서 클라이언트의 레코딩을 검색할 수 있는 권한을 활성화합니다.

Smart Wall 탭(역할)

역할을 통해 클라이언트 사용자에게 Smart Wall 관련 사용자 권한을 허용할 수 있습니다.

이름	설명
판독	사용자가 XProtect Smart Client 에서 선택한 Smart Wall 을(를) 보도록 해줍니다.
편집	사용자가 Smart Wall 에서 선택한 Management Client 을(를) 편집할 수 있습니다.
삭제	사용자가 Smart Wall 에서 선택한 Management Client 을(를) 삭제할 수 있습니다.

이름	설명
작동	사용자가 XProtect Smart Client 에서 선택한 Smart Wall 에 레이아웃을 적용하고 프리셋을 활성화하도록 해줍니다.
재생	사용자가 XProtect Smart Client 에서 선택한 Smart Wall 로부터 기록된 데이터를 재생하게 해줍니다.

외부 이벤트 탭(역할)

다음의 외부 이벤트 권한을 지정합니다.

이름	설명
판독	사용자가 클라이언트와 Management Client 에서 선택한 외부 시스템 이벤트를 검색하고 볼 수 있습니다.
편집	사용자가 Management Client 에서 선택한 외부 시스템 이벤트를 편집할 수 있습니다.
삭제	사용자가 Management Client 에서 선택한 외부 시스템 이벤트를 삭제할 수 있습니다.
트리거	사용자가 클라이언트에서 선택한 외부 시스템 이벤트를 트리거할 수 있습니다.

뷰 그룹 탭(역할)

뷰 그룹 탭에서는 선택한 역할을 가진 사용자 및 사용자 그룹이 클라이언트에서 사용할 수 있는 뷰 그룹을 지정합니다.

뷰 그룹에 대해 다음 권한을 지정합니다.

이름	설명
판독	클라이언트와 Management Client 에서 뷰 그룹을 볼 수 있는 권한을 활성화합니다. 뷰 그룹은 Management Client 에서 만들어집니다.
편집	Management Client 에 있는 뷰 그룹의 속성을 편집할 수 있는 권한을 활성화합니다.
삭제	Management Client 에 있는 뷰 그룹을 삭제할 수 있는 권한을 활성화합니다.
작동	XProtect Smart Client에서 뷰 그룹을 사용, 즉 하위 그룹과 뷰를 만들고 삭제할 수 있는 권한을 활성화합니다.

서버 탭(역할)

서버 탭에서 역할 권한 지정은 시스템이 Milestone Federated Architecture 설치 상태에서 작동하는 경우에만 해당됩니다.

이름	설명
사이트	Management Client 에 있는 선택한 사이트를 볼 수 있는 권한을 활성화합니다. 연결된 사이트는 Milestone Federated Architecture 을(를) 통해 연결됩니다. 속성을 편집하려면 각 사이트의 관리 서버에서 편집 권한이 필요합니다.

자세한 정보는 페이지 86의 Milestone Federated Architecture 구성하기를 참조하십시오.

Matrix 탭(역할)

시스템에서 Matrix 수신자를 구성한 경우, Matrix 역할 권한을 구성할 수 있습니다. 클라이언트에서 선택한 Matrix 수신자로 비디오를 전송할 수 있습니다. Matrix 탭에서 이 비디오를 수신할 수 있는 사용자를 선택합니다.

다음 권한을 사용할 수 있습니다.

이름	설명
판독	선택한 역할을 가진 사용자 및 그룹이 클라이언트에서 Matrix 수신자를 선택하여 비디오를 전송할 수 있는지 결정합니다.

알람 탭(역할)

설치(다른 모든 XProtect 서버 포함)에 대한 중앙 개요와 제어를 제공하기 위해 시스템 설정에서 알람을 사용하는 경우, **알람** 탭을 사용하여 선택한 역할을 가진 사용자 및 그룹이 갖는 알람 권한(예: 클라이언트에서 알람을 처리하는 방법)을 지정할 수 있습니다.

알람에서 다음과 같은 알람에 대한 권한을 지정합니다.

보안 권한	설명
관리	Smart Client 에서 알람을 관리할 수 있는 권한을 활성화합니다. 예를 들어 알람 우선순위 변경, 다른 사용자에게 알람 다시 할당, 알람 승인, 여러 알람의 알람 상태 변경(예: **신규**에서 **할당됨**으로 변경)이 있습니다. 알

보안 권한	설명
	람 설정을 편집하려면 **알람 설정 편집** 권한도 필요합니다. 이 항목을 허용된 것으로 설정하는 경우에만 **옵션** 대화 상자에서 **알람 및 이벤트** 탭이 표시됩니다.
뷰	XProtect Smart Client의 **알람 관리자** 탭을 보고 API를 통해 알람 및 알람 설정을 검색할 수 있는 권한을 활성화합니다. XProtect Smart Client에서 알람을 확인하려면 하나 이상의 알람 정의에 대해 **보기** 권한을 활성화해야 합니다. 기본적으로 써드파티 솔루션의 알람이 표시됩니다.
알람 비활성화	알람을 비활성화할 수 있는 권한을 활성화합니다.
알림 수신	XProtect Mobile 클라이언트 및 XProtect Web Client 에서 알람에 관한 알림을 수신할 수 있는 권한을 활성화합니다.
알람 설정 편집	알람 정의, 알람 상태, 알람 카테고리, 알람 소리, 알람 보존, 이벤트 보존을 편집할 수 있는 권한을 활성화합니다. 알람 설정을 편집하려면 **관리** 권한도 필요합니다.

알람 정의에서 특정 알람 정의에 대한 권한을 지정합니다.

이름	설명
뷰	알람 정의, 알람 상태, 알람 카테고리, 알람 소리, 알람 보존, 이벤트 보존을 편집할 수 있는 권한을 활성화합니다.
쓰기	**보기** 권한을 활성화합니다.

액세스 제어 탭(역할)

기본 사용자, Windows 사용자 또는 그룹을 추가하거나 편집할 때 액세스 제어 설정을 지정합니다:

이름	설명
액세스 제어 사용	사용자가 클라이언트에서 액세스 제어 관련 기능을 사용할 수 있습니다.
카드 소유자 목록 보기	**사용자가 클라이언트의** 액세스 제어 탭에서 카드 소유자 목록을 볼 수 있습니다.
알림 수신	사용자가 클라이언트에서 액세스 요청에 대한 알림을 받을 수 있습니다.

LPR 탭(역할)

시스템이 XProtect LPR 에서 실행되는 경우, 사용자에 대해 다음 권한을 지정합니다.

이름	설명
LPR 사용	클라이언트에서 LPR 관련 기능을 사용할 수 있는 권한을 활성화합니다.
자동차 번호판 일치 목록 관리	Management Client에서 자동차번호판 일치 목록을 추가, 가져오기, 수정, 내보내기 및 삭제할 수 있는 권한을 활성화합니다.
자동차 번호판 일치 목록	자동차번호판 일치 목록을 볼 수 있는 권한을 활성화합니다.

인시던트 탭(역할)

XProtect Incident Manager가 있는 경우 역할에 대해 다음과 같은 권한을 지정할 수 있습니다.

Management Client 관리자 역할에 사건 속성을 관리하거나 볼 수 있는 권한을 부여하려면 **사건 속성** 노드를 선택합니다.

작업자에게 정의된 사건 속성을 볼 수 있는 XProtect Smart Client 권한을 부여하려면 **사건 속성**을 선택하고 **뷰** 권한을 부여합니다. 사건 프로젝트를 관리하거나 보기 위한 일반 권한을 부여하려면 **사건 프로젝트** 노드를 선택합니다. **사건 프로젝트** 노드를 확장하고 하나 이상의 하위 노드를 선택하여 이러한 추가 특정 특성 또는 기능에 대한 권한을 부여합니다.

이름	설명
관리	기능과 관련된 (보기, 생성, 편집 및 삭제) 설정 및 속성을 관리하거나 Management Client 또는 XProtect Smart Client에서 선택한 노드가 나타내는 사용자 인터페이스 요소를 볼 수 있는 권한
뷰	기능과 관련된 (생성, 편집 및 삭제 불가) 설정 및 속성을 보거나, 정의된 사건 속성을 보거나, Management Client 또는 XProtect Smart Client에서 선택한 노드가 나타내는 사용자 인터페이스 요소를 볼 수 있는 권한

MIP 탭(역할)

MIP SDK 을(를) 통해 타사 공급업체가 사용 중인 시스템에 대한 사용자 정의 플러그 인을 개발할 수 있습니다(예: 외부 액세스 제어 시스템 또는 유사 기능으로 통합). 써드파티 플러그 인은 개별 탭에 고유한 설정이 있습니다.

변경하는 설정은 실제 플러그 인에 따라 다릅니다. **MIP** 탭에서 플러그인에 대한 사용자 정의 설정을 찾습니다.

기본 사용자(보안 노드)

Milestone XProtect VMS에는 사용자 계정 유형이 다음과 같이 두 가지가 있습니다. 기본 사용자 및 Windows 사용자.

기본 사용자는 Milestone XProtect VMS에서 만든 사용자 계정입니다. 이 계정은 개별 사용자에 대해 기본 사용자 이름과 암호 인증이 있는 전용 시스템 사용자 계정입니다.

Windows 사용자는 Microsoft의 Active Directory을(를) 통해 추가하는 사용자 계정입니다.

기본 사용자 및 Windows 사용자 사이에는 다음과 같은 몇 가지 차이점이 있습니다.

- 기본 사용자는 사용자 이름 및 암호 조합으로 인증되며 하나의 시스템/사이트에 한정됩니다. 하나의 연합 사이트에서 생성된 기본 사용자가 다른 연합 사이트의 기본 사용자와 동일한 이름과 암호를 가지고 있다하더라도 기본 사용자는 생성된 사이트에만 액세스할 수 있습니다.
- Windows 사용자는 해당 Windows 로그인에 기반하여 인증을 받으며 이 인증은 하나의 시스템에 한정됩니다.

시스템 대시보드 노드

시스템 대시보드 노드

시스템 대시보드 노드 아래에서 시스템을 모니터하기 위한 다른 기능과 다양한 시스템 구성 요소를 확인할 수 있습니다.

이름	설명
현재 작업	선택한 레코딩 서버에서 진행 중인 작업에 대한 개요를 가져옵니다.
시스템 모니터	사용자가 정의하는 매개변수에 따라 서버와 카메라의 상태를 모니터링합니다.
시스템 모니터 임계값	시스템 모니터에 사용되는 서버와 모니터 타일에서 모니터링 매개변수의 임계값을 설정합니다.
증거물 잠금	시스템에서 보호된 모든 데이터의 개요를 확인합니다.
구성 보고서	시스템 구성이 포함된 보고서를 출력합니다. 보고서에 무엇을 포함시킬지 결정할 수 있습니다.

현재 작업(시스템 대시보드 노드)

현재 작업 창은 선택된 레코딩 서버 하에서 진행 중인 작업 개요를 표시합니다. 시간이 오래 걸리고 배경에서 구동되는 작업을 시작한 경우 **현재 작업** 창을 열어 작업 진행 상황을 확인할 수 있습니다. 시간이 오래 걸리는 사용자가 시작한 작업의 몇 가지 사례들로는 펌웨어 업데이트와 하드웨어 이동이 있습니다. 그러한 작업들의 시작 시간, 대략적인 종료 시간 및 진행 상황에 관한 정보를 확인할 수 있습니다.

현재 작업 창에 표시된 정보는 실시간으로 업데이트되지는 않지만 창을 연 순간에 현재 작업에 대한 스냅샷을 제공합니다. 일정 시간 동안 창을 열어 둔 경우, 창 우측 하단 코너에 있는 **새로 고침** 버튼을 선택하여 표시된 정보를 새로 고침할 수 있습니다.

시스템 모니터(시스템 대시보드 노드)

시스템 모니터 기능은 현재 시스템의 서버 및 카메라의 상태를 빠르게 시각적인 개요로 제공해 줍니다.

시스템 모니터 대시보드 창

타일

시스템 모니터 대시보드 창의 상단은 시스템의 서버 하드웨어와 카메라 하드웨어의 상태를 나타내는 색 타일을 표시합니다.

이들 타일은 상태에 따라 변경되며 색깔은 **시스템 모니터 임계값** 노드에서 설정된 임계값에 기반합니다. 자세한 정보는 페이지 511의 시스템 모니터 임계값(시스템 대시보드 노드)를 참조하십시오. 임계값을 정의하면 타일 색은 다음과 같은 의미를 표시합니다.

타일 색상	설명
초록색	**정상** 상태. 모두 정상 작동 중입니다.
노란색	**경고** 상태. 하나 이상의 모니터링 매개변수가 **정상** 상태에 대한 임계치 이상입니다.
빨간색	**위험** 상태. 하나 이상의 모니터링 매개변수가 **정상** 및 **경고** 상태에 대한 임계치 이상입니다.

모니터링 매개변수를 포함하는 하드웨어 목록

타일을 클릭하면 **시스템 모니터 대시보드** 창의 하단에 있는 타일로 표시되는 각 하드웨어에 대한 각 선택된 모니터링 매개변수의 상태를 조회할 수 있습니다.

예: 카메라의 라이브 FPS 모니터링 매개변수가 경고 상태에 도달했습니다.

대시보드 창 사용자 정의

창의 우측 상단에 있는 **사용자 정의** 를 선택하여 **대시보드 사용자 정의** 창을 엽니다.

사용자 정의 창에서 어떤 타일을 생성, 편집 또는 삭제할지 선택할 수 있습니다. 타일 생성 및 편집 시 어떤 하드웨어 및 어떤 모니터링 매개변수가 타일에 모니터링될 지를 선택할 수 있습니다.

상세 내용 창

타일을 선택한 후 모니터링 매개변수가 포함된 하드웨어 목록에서 카메라 또는 서버의 오른쪽에 있는 **상세 내용** 버튼을 클릭하는 경우, 선택된 하드웨어에 따라 시스템 정보를 조회하고 다음에 관한 보고서를 생성할 수 있습니다.

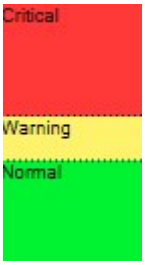
하드웨어	정보
관리 서버	다음에 관한 데이터 표시: • CPU 사용량 • 사용 가능 메모리 **이력** 을 선택하여 하드웨어의 이력 상태를 조회하거나 위 데이터에 관한 보고서를 생성합니다.
레코딩 서버	다음에 관한 데이터 표시: • CPU 사용량 • 사용 가능 메모리 • 디스크 • 저장소 • 네트워크 • 카메라 **이력** 을 선택하여 하드웨어의 이력 상태를 조회하거나 위 데이터에 관한 보고서를 생성합니다.
장애조치 레코딩 서버	다음에 관한 데이터 표시: • CPU 사용량 • 사용 가능 메모리 • 모니터링되는 레코딩 서버 **이력** 을 선택하여 하드웨어의 이력 상태를 조회하거나 위 데이터에 관한 보고서를 생성합니다.
로그	다음에 관한 데이터 표시

하드웨어	정보
서버, 이벤트 서버 등	• CPU 사용량 • 사용 가능 메모리 **이력** 을 선택하여 하드웨어의 이력 상태를 조회하거나 위 데이터에 관한 보고서를 생성합니다.
카메라	다음에 관한 데이터 표시: • 저장소 • 사용된 공간 • 라이브 FPS(기본값) • 레코딩 FPS • 라이브 비디오 형식 • 녹화 비디오 형식 • 받은 미디어 데이터(Kbit/초) • 사용 가능 메모리 카메라 이름을 선택하여 이력 상태를 조회하고 다음에 관한 보고서를 생성합니다. • 카메라에서 받은 데이터 • 카메라 디스크 사용량

서버 운영 체제에서 시스템 모니터의 세부 정보에 액세스할 경우, **Internet Explorer의 고급 보안 구성** 에 관한 메시지가 나타날 수 있습니다. 안내서를 따라 진행하기 전에 **시스템 모니터** 페이지를 **신뢰하는 사이트 영역** 에 추가합니다.

시스템 모니터 임계값(시스템 대시보드 노드)

시스템 모니터 임계값을 통해 **시스템 모니터 대시보드** 상의 타일이 귀하의 시스템 하드웨어가 상태를 변경하였음을 시각적으로 표시할 때의 임계값을 정의 및 조정할 수 있게 해줍니다. 예를 들어 서버의 CPU 사용량이 일반 상태(녹색)에서 경고 상태(노란색) 또는 경고 상태(노란색)에서 위험 상태(적색)으로 변경되는 경우입니다.



3가지 상태 간 임계값의 예시

서버,카메라,디스크및저장소에대한임계값을변경할수있으며,모든임계값은일부일반적인버튼및설정을갖추었습니다.

일반적인 사용자 인터페이스 요소

버튼 및 설정	설명	유닛
계산 간격	다른 하드웨어에 대한 연결에서 짧은 중단이 종종 있을 수 있습니다. 계산 간격을 0초로 지정하는 경우, 이러한 모든 짧은 중단은 하드웨어 상태 변경에 관한 경고를 트리거합니다. 그러므로 계산 간격을 적당한 길이로 정의하십시오. 계산 간격을 1분으로 정의하는 경우, 이는 1분에 대한 평균값이 임계값을 초과한 경우에만 경고를 받게 됨을 의미합니다. 정확히 계산하여 간격을 설정하면 초과된 임계값에 대한 오탐으로 인한 경고를 받지 않게 될 뿐만 아니라 CPU 사용량 또는 메모리 소비량과 같은 지속적인 문제에 관한 알람만 받을 수 있습니다. 계산 간격의 값을 변경하려면 페이지 273의 하드웨어 상태가 변경되어야 할 때에 대한 임계값 편집를 참조하십시오.	초
고급	**고급** 버튼을 선택하면 개별 서버, 카메라, 디스크, 저장소에 대한 임계값 및 계산 간격을 정의할 수 있습니다. 자세한 정부는 아래를 참조하십시오.	-
규칙 만들기	**시스템 모니터** 및 규칙 에벤트를 트리거 동작으로 조합할 수 있습니다(예: 서버 CUP 사용량 상태가 경고인 경우 또는 디스크 빈 공간이 거의 없는 경우). 자세한 정보는 페이지 72의 규칙 및 이벤트(설명됨) 및 를 참조하십페이지 251의 규칙 추가시오.	-

서버 임계치

임계치	설명	유닛
CPU 사용량	모니터링하는 서버상의 CPU 사용량에 대한 임계치.	%
사용 가능 메모리	모니터링하는 서버에서 사용되는 RAM에 대한 임계값.	MB
NVIDIA 디코딩	모니터링하는 서버상의 NVIDIA 디코딩 사용량에 대한 임계치.	%
NVIDIA 메모리	모니터링하는 서버에서 사용되는 NVIDIA RAM에 대한 임계값.	%
NVIDIA 렌더링	모니터링하는 서버상의 NVIDIA 렌더링사용량에 대한 임계치.	%

카메라 임계치

임계치	설명	유닛
라이브 FPS	라이브 비디오가 모니터하는 카메라에 보이는 경우 사용 중인 카메라의 FPS에 대한 임계치.	%
레코딩 FPS	시스템이 모니터링하는 카메라에서 비디오를 녹화할 때 사용하는 카메라의 FPS 임계값.	%
사용된 공간	모니터링하는 카메라에서 사용하는 공간에 대한 임계치.	GB

디스크 임계치

임계치	설명	유닛
여유 공간	모니터링하는 디스크상의 사용 가능한 공간에 대한 임계치.	GB

저장소 임계치

임계치	설명	유닛
보존 기간	임계치는 저장소에 여유 공간이 없을 때를 예측해줍니다. 표시된 상태는 시스템 설정에 기반하며 이틀에 한 번 업데이트됩니다.	일

증거물 잠금(시스템 대시보드 노드)

시스템 대시보드 노드 아래 **증거물 잠금** 에서는 현재 감시 시스템 상의 모든 보호된 데이터의 개요가 표시됩니다.

다음 메타데이터는 모든 증거물 잠금에 대해 사용할 수 있습니다.

- 보호된 데이터의 시작 및 종료 날짜
- 증거물을 잠근 사용자
- 증거물이 더 이상 잠기지 않는 때
- 데이터 저장 위치
- 각 증거물 잠금 크기

증거물 잠금 창에 표시된 모든 정보는 스냅샷입니다. 새로 고치려면 F5 키를 누르십시오.

구성 보고서(시스템 대시보드 노드)

비디오 관리 소프트웨어 시스템을 설치하고 구성할 때 다양한 선택을 할 수 있으며, 다음과 같은 문서가 필요할 수도 있습니다. 또한 설치 및 첫 구성 이후 또는 지난 몇 달 동안 변경한 모든 설정은 오랜 시간 기억하기 힘듭니다. 그렇기 때문에 모든 구성 선택 사항을 출력할 수 있게 한 것입니다.

다음 설정은 구성 보고서 생성 및 출력 시 사용할 수 있습니다.

이름	설명
보고서	구성 보고서에 첨부할 수 있는 요소의 목록.
모두 선택	**보고서** 목록의 모든 요소를 구성 보고서에 추가합니다.
모두 지우기	**보고서** 목록의 모든 요소를 구성 보고서에서 제거합니다.

이름	설명
전면 페이지	보고서의 전면 페이지를 사용자 정의합니다.
형식 지정	보고서의 형식을 지정합니다.
민감한 데이터 제외	사용자 이름, 이메일 주소 및 기타 민감한 데이터 유형과 같은 개인 데이터를 구성 보고서에서 제거하여 GDPR 규정을 준수하게 합니다. 라이선스 소유자에 관한 정보는 항상 보고서에서 제외되어 있습니다.
내보내기	보고서를 저장할 위치를 선택하고 PDF로 보고서를 생성합니다.

서버 로그 노드

서버 로그 노드

시스템 로그(탭)

로그의 각 행은 로그 항목을 나타냅니다. 로그 항목에는 여러 정보 필드가 포함되어 있습니다:

이름	설명
로그 수준	정보, 경고, 또는 에러.
로컬 시간	사용 중인 시스템 서버의 로컬 시간으로 타임스탬프가 표시됩니다.
메시지 텍스트	기록된 인시던트의 식별 번호.
카테고리	기록된 인시던트의 유형.
소스 유형	기록된 인시던트가 발생한 장비의 유형(예: 서버 또는 장치).
소스 이름	기록된 인시던트가 발생한 장치의 이름.
이벤트 유형	기록된 인시던트가 나타내는 이벤트 유형.

감사 로그(탭)

로그의 각 행은 로그 항목을 나타냅니다. 로그 항목에는 여러 정보 필드가 포함되어 있습니다:

이름	설명
로컬 시간	사용 중인 시스템 서버의 로컬 시간으로 타임스탬프가 표시됩니다.
메시지 텍스트	기록된 인시던트의 설명을 표시합니다.
권한	원격 사용자 동작이 허용(부여)되었는지 여부에 관한 정보.
카테고리	기록된 인시던트의 유형.
소스 유형	기록된 인시던트가 발생한 장비의 유형(예: 서버 또는 장치).
소스 이름	기록된 인시던트가 발생한 장치의 이름.
사용자	기록된 인시던트를 초래한 원격 사용자의 사용자 이름.
사용자 위치	원격 사용자가 기록된 인시던트를 발생시킨 컴퓨터의 IP 주소 또는 호스트 이름.

규칙 트리거 로그(탭)

로그의 각 행은 로그 항목을 나타냅니다. 로그 항목에는 여러 정보 필드가 포함되어 있습니다:

이름	설명
로컬 시간	사용 중인 시스템 서버의 로컬 시간으로 타임스탬프가 표시됩니다.
메시지 텍스트	기록된 인시던트의 설명을 표시합니다.
카테고리	기록된 인시던트의 유형.
소스 유형	기록된 인시던트가 발생한 장비의 유형(예: 서버 또는 장치).
소스 이름	기록된 인시던트가 발생한 장치의 이름.

이름	설명
이벤트 유형	기록된 인시던트가 나타내는 이벤트 유형.
규칙 이름	로그 항목을 트리거하는 규칙의 이름.
서비스 이름	기록된 인시던트가 발생한 서비스의 이름.

메타데이터 사용 노드

메타데이서 및 메타데이터 검색

메타 데이터 관리 및 구성을 하려면 페이지 274의 메타데이터 검색 카테고리 및 검색 필터 표시 또는 숨기기를 참조하십시오.

메타데이터란 무엇입니까?

메타데이터란 데이터에 관한 데이터로, 예를 들어 비디오 이미지를 설명하는 데이터 또는 이미지 내 콘텐츠나 객체를 설명하는 데이터, 이미지가 레코딩된 위치를 알려주는 데이터 등을 의미합니다.

메타데이터는 다음에 의해 생성될 수 있습니다:

- 데이터를 전달하는 장치 자체(예: 비디오를 전달하는 카메라)
- 일반 메타데이터 드라이버를 통한 타사 시스템 또는 통합

메타 데이터 검색

메타데이터 검색은 메타데이터와 관련된 검색 카테고리와 검색 필터를 사용하는 XProtect Smart Client 에서 비디오 레코딩을 검색하는 것을 의미합니다.

기본 Milestone 메타데이터 검색 카테고리는 다음과 같습니다:

- 위치:사용자는 지리적 좌표를 정의하고 이 좌표로부터 검색 반경을 정의할 수 있습니다.
- 사람: 사용자는 성별과 대략적인 키와 나이를 검색할 수 있을 뿐만 아니라 얼굴과 함께 결과를 표시하도록 선택할 수 있습니다.
- 자동차:사용자는 차량 색상, 속도, 유형, 특정 번호판을 검색할 수 있습니다.

메타데이터 검색 요건

검색 결과를 받으려면 다음 중 하나를 수행해야 합니다:

- 비디오 분석을 수행할 수 있는 비디오 감시 시스템에 최소한 한 개의 장치가 있어야 하며 바르게 구성되어야 합니다.
- 메타데이터를 생성하는 비디오 감시 시스템 내 비디오 프로세싱 서비스

어떤 경우든 메타데이터는 반드시 요청된 메타데이터 형식이어야 합니다.

자세한 정보는 메타데이터 검색의 통합에 대한 문서 를 참조하십시오.

액세스 제어 노드

액세스 제어 속성

일반 설정 탭(액세스 제어)

이름	설명
활성화	시스템은 기본적으로 활성화됩니다. 즉, 충분한 권한을 가진 사용자가 XProtect Smart Client 에서 시스템을 확인할 수 있으며, XProtect 시스템이 액세스 제어 이벤트를 수신한다는 의미입니다. 예를 들어, 유지 관리 동안에 불필요한 알람이 발생하지 않도록 시스템을 비활성화시킬 수 있습니다.
이름	Management Application과 클라이언트에 표시되는 액세스 제어 통합의 이름입니다. 기존 이름을 새 이름으로 덮어쓸 수 있습니다.
설명	액세스 제어 통합에 대한 설명을 제공합니다. 이것은 옵션입니다.
통합 플러그 인	초기 통합 과정에서 선택된 액세스 제어 시스템의 유형을 표시합니다.
마지막 구성 새로 고침	액세스 제어 시스템에서 마지막으로 구성을 가져온 날짜와 시간을 표시합니다.
구성 새로 고침	예를 들어 도어를 추가하거나 삭제한 경우, XProtect 에서 액세스 제어 시스템에 이루어진 구성 변경을 반영해야 할 때 이 버튼을 클릭합니다. 액세스 제어 시스템의 구성 변경에 대한 요약 정보가 나타납니다. 이 목록을 검토하여 새 구성을 적용하기 전에 액세스 제어 시스템이 올바르게 반영되었는지 확인하십시오.
운영자 로그인 필요	액세스 제어 시스템이 분화된 사용자 권한을 지원할 경우, 클라이언트 사용자에 대한 추가 로그인을 활성화합니다. 이 옵션을 활성화할 경우 액세스 제어 시스템을 XProtect Mobile 클라이언트에서 이용할 수 없습니다. 통합 플러그 인이 차등화된 사용자 권한을 지원하는 경우에만 이 옵션이 표시됩니다.

다음 필드의 이름과 내용은 통합 플러그 인에서 가져옵니다. 다음은 몇 개의 일반적인 필드의 예입니다:

이름	설명
주소	통합 액세스 제어 시스템을 호스팅하는 서버 주소를 입력합니다.
포트	액세스 제어 시스템이 연결되는 서버의 포트 번호를 지정합니다.
사용자 이름	액세스 제어 시스템에 정의된 대로 XProtect 에서 통합 시스템의 관리자여야 하는 사용자의 이름을 입력합니다.
암호	사용자 암호를 지정합니다.

도어 및 연결된 카메라 탭(액세스 제어)

이 탭은 도어 액세스 지점과 카메라, 마이크 또는 스피커 사이의 매핑을 제공합니다. 카메라를 통합 마법사의 일부로 연결하지만 언제든지 설정을 변경할 수 있습니다. 마이크 및 스피커에 대한 매핑은 카메라의 관련 마이크나 스피커를 통해 암시적으로 이루어집니다.

이름	설명
도어	액세스 제어 시스템에 정의된 사용 가능한 도어 액세스 지점을 도어별로 그룹화하여 나열합니다. 관련 도어로 쉽게 이동하려면 상단에 있는 드롭다운 목록을 통해 해당 액세스 제어 시스템의 도어를 필터링할 수 있습니다. **활성화됨**: 라이선스가 있는 도어는 기본적으로 활성화됩니다. 도어를 비활성화하여 라이선스를 회수할 수 있습니다. **라이선스**: 도어의 사용이 허가되었는지, 라이선스가 만료되었는지를 표시합니다. 도어가 비활성화되면 필드가 비어 있습니다. **제거**: 액세스 지점에서 카메라를 제거하려면 **제거** 를 클릭합니다. 모든 카메라를 제거하면 관련 카메라의 확인란 선택이 자동으로 취소됩니다.
카메라	XProtect 시스템에서 구성된 카메라를 나열합니다. 목록에서 카메라를 선택하고 관련 액세스 포인트로 끌어다 놓아 액세스 포인트를 카메라와 연결시킵니다.

액세스 제어 이벤트 탭(액세스 제어)

이벤트 카테고리를 통해 이벤트를 그룹화할 수 있습니다. 이벤트 카테고리의 구성은 XProtect 시스템의 액세스 제어 동작에 영향을 미치며, 이를 통해 예를 들어 여러 이벤트 유형에서 단일 알람을 트리거하도록 알람을 정의할 수 있습니다.

이름	설명
액세스 제어 이벤트	액세스 제어 시스템에서 가져온 액세스 제어 이벤트를 나열합니다. 통합 플러그 인이 이벤트의 기본 활성화 및 비활성화를 제어합니다. 통합 이후 언제든지 이벤트를 활성화 또는 비활성화할 수 있습니다. 이벤트가 활성화 되면, 해당 이벤트는 XProtect 이벤트 데이터베이스에 저장되며, 예를 들어 XProtect Smart Client 에서 필터링을 위해 사용할 수 있습니다.
소스 유형	액세스 제어 이벤트를 트리거할 수 있는 액세스 제어 장치를 표시합니다.
이벤트 카테고리	액세스 제어 이벤트에 하나 이상의 이벤트 카테고리를 할당하거나 할당을 하지 않습니다. 시스템이 통합 중에 관련 이벤트 카테고리를 이벤트에 자동으로 매핑합니다. 그러면 XProtect 시스템의 기본 설정이 활성화됩니다. 언제든지 매핑을 변경할 수 있습니다. 기본 제공되는 이벤트 카테고리: • 액세스 거부됨 • 액세스 승인됨 • 액세스 요청 • 알람 • 오류 • 경고 통합 플러그 인에 의해 정의된 이벤트와 이벤트 카테고리도 나타나지만 고유 이벤트 카테고리를 정의할 수도 있습니다. **사용자 정의 카테고리** 를 참조하십시오. ⚠ XProtect Corporate 에서 이벤트 카테고리를 변경하는 경우, 기존 액세스 제어 규칙이 여전히 작동하는지 확인해야 합니다.
사용자 정의 카테고리	사용자 정의 이벤트 카테고리를 생성, 수정 또는 삭제할 수 있습니다. 예를 들어, 액세스 제어 동작에 대한 트리거 이벤트를 정의할 때와 같이 기본 제공되는 카테고리가 요구사항을 충족시키지 못하는 경우에 이벤트 카테고리를 생성할 수 있습니다. 카테고리는 XProtect 시스템에 추가되는 모든 통합 시스템에 대해 전역으로 적용됩니다. 따라서 알람 정의에서 시스템 상호 간 처리를 설정할 수 있습니다. 사용자 정의 이벤트 카테고리를 삭제할 때 이 카테고리가 통합에 사용되고 있으면 경고가 표시됩니다. 그래도 삭제하면 액세스 제어 동작과 같이 이 카테고리를 통해 적용된 모든 구성이 더 이상 작동하지 않습니다.

액세스 요청 알림 탭(액세스 제어)

주어진 이벤트가 발생할 때 XProtect Smart Client 화면에 나타나는 액세스 요청 알림을 지정할 수 있습니다.

이름	설명
이름	액세스 요청 알림의 이름을 입력합니다.
액세스 요청 알림 추가	액세스 요청 알림을 추가하고 정의하려면 클릭합니다. 알림을 삭제하려면 오른쪽에서 **X**를 클릭합니다. XProtect Smart Client 의 사용자가 Milestone Federated Architecture 계층 구조의 상위 사이트에 로그인할 경우, XProtect Smart Client 에도 하위 사이트의 액세스 요청 알림이 표시됩니다.
액세스 요청 알림 세부 정보	주어진 이벤트가 발생할 때 액세스 요청 알림에 나타나는 카메라, 마이크 또는 스피커를 지정합니다. 또한 알림 팝업이 나타날 때 사용자에게 알릴 사운드를 지정합니다.
명령 추가	XProtect Smart Client 에서 액세스 요청 알림 대화 상자에 버튼으로 사용 가능한 명령을 선택합니다. 관련된 액세스 요청 명령: • 소스 장치에서 사용할 수 있는 액세스 요청 작업과 관련된 모든 명령을 활성화합니다. 예: **도어 열기** 관련된 모든 명령: • 소스 장치에서 모든 명령 활성화 액세스 제어 명령: • 선택된 액세스 제어 명령 활성화 시스템 명령: • XProtect 시스템에서 사전 정의된 명령 활성화 명령을 삭제하려면 오른쪽에서 **X**를 클릭합니다.

카드 소유자 탭(액세스 제어)

카드 소유자 탭을 사용하여 액세스 제어 시스템의 카드 소유자에 관한 정보를 검토합니다.

이름	설명
카드 소유자 검색	카드 소유자 이름의 문자를 입력합니다. 이 이름이 있으면 목록에 나타납니다.
이름	액세스 제어 시스템에서 검색된 카드 소유자 이름을 나열합니다.
유형	카드 소유자 유형을 나열합니다. 예: • 직원 • 경비 • 방문객

해당 액세스 제어 시스템이 XProtect 시스템에서 사진 추가/삭제를 지원하는 경우, 카드 소유자에게 사진을 추가할 수 있습니다. 이 기능은 액세스 제어 시스템에 카드 소유자의 사진이 포함되어 있지 않은 경우에 유용합니다.

이름	설명
사진 선택	카드 소유자 사진이 있는 파일 경로를 지정합니다. 액세스 제어 시스템이 사진을 관리하는 경우에는 이 버튼이 나타나지 않습니다. 허용된 파일 형식은 .bmp, .png 및 .jpg입니다. 사진은 보기를 최대화하도록 크기가 조정됩니다. Milestone 에서는 이차원 사진 사용을 권장합니다.
사진 삭제	사진을 삭제할 때 클릭합니다. 액세스 제어 시스템에 사진이 있는 경우, 삭제 후에 이 사진이 표시됩니다.

사건 노드

사건 속성(사건 노드)

다음 정보는 XProtect Incident Manager 관련 설정에 대해 설명합니다.

다음 탭에서 XProtect Smart Client 작업자에 대한 모든 사건 속성을 정의합니다.

- 유형
- 상태
- 카테고리
- 카테고리 1-5

모든 사건 속성은 다음의 설정을 가집니다.

이름	설명
이름	사건 속성 이름은 고유할 필요는 없지만, 고유하며 사건 설명을 잘 하는 속성 이름을 사용하면 여러 상황에서 이점이 있습니다.
설명	정의된 사건 속성에 대한 추가 설명 예를 들어, *위치*라는 카테고리를 생성한 경우 해당 설명은 *사건이 어디서 발생했습니까?*일 수 있습니다.

트랜잭트 노드

트랜잭션 소스(트랜잭션 노드)

다음 표는 트랜잭션 소스에 대한 속성을 설명합니다.

소스 추가에 관한 자세한 정보는 트랜잭션 소스 추가(마법사) 를 참조하십시오.

트랜잭션 소스(속성)

이름	설명
활성화	트랜잭션 소스를 비활성화하려면 이 확인란을 선택 취소하십시오. 트랜잭션 데이터의 흐름이 중단되지만 이미 가져온 데이터는 이벤트 서버에서 유지됩니다. 보존 기간 중 XProtect Smart Client 에서 비활성화된 트랜잭션 소스의 트랜잭션을 계속 볼 수 있습니다. 비활성화된 트랜잭션 소스에도 트랜잭션 소스 라이선스가 필요합니다.
이름	이름을 변경하려면 여기에 새 이름을 입력합니다.
커넥터	트랜잭션 소스를 생성할 때 선택한 커넥터는 변경할 수 없습니다. 다른 커넥터를 선택하려면 새 트랜잭션

이름	설명
	소스를 생성하고 마법사 단계에서 원하는 커넥터를 선택해야 합니다.
트랜잭션 정의	수신한 트랜잭션 데이터를 트랜잭션 및 트랜잭션 라인으로 변환하는 방법을 정의하는 다른 트랜잭션 정의를 선택할 수 있습니다. 여기에는 다음에 대한 정의가 포함됩니다. • 트랜잭션이 시작되고 끝나는 때 • XProtect Smart Client 에서 트랜잭션이 표시되는 방식
보존 기간	이벤트 서버에서 트랜잭션 데이터가 유지되는 기간을 일 수 단위로 지정합니다. 기본 보존 기간은 30일입니다. 보존 기간이 만료되면 데이터가 자동으로 삭제됩니다. 이것은 데이터베이스의 저장 용량이 초과되는 상황을 피하기 위한 조치입니다. 최소값은 1일이고 최대값은 1000일입니다.
TCP 클라이언트 커넥터	**TCP 클라이언트 커넥터** 를 선택한 경우, 다음 설정을 지정합니다. • **호스트 이름**:트랜잭션 소스와 연관된 TCP 서버의 호스트 이름을 입력합니다 • **포트**: 트랜잭션 소스와 연관된 TCP 서버의 포트 이름을 입력합니다
직렬 포트 커넥터	**직렬 포트 커넥터** 를 선택한 경우, 다음 설정을 지정하고 이 설정이 트랜잭션 소스의 설정과 일치하는지 확인하십시오. • **직렬 포트**: COM 포트를 선택합니다 • **Baud 속도**: 초당 전송되는 비트 수를 지정합니다 • **패리티**: 전송에서 오류를 감지하기 위한 방법을 지정합니다. 기본적으로 **없음** 이 선택됩니다 • **데이터 비트**: 하나의 데이터 문자를 나타내기 위해 사용되는 비트 수를 지정합니다 • **정지 비트**: 한 바이트가 전송되었음을 나타내기 위한 비트 수를 지정합니다. 대부분의 장치는 1비트가 필요합니다 • **핸드쉐이크**: 트랜잭션 소스와 이벤트 서버 간의 통신 프로토콜을 결정하는 핸드쉐이킹 방법을 지정합니다

트랜잭션 정의(트랜잭션 노드)

다음 표는 트랜잭션 소스에 사용되기 위한 정의에 대한 속성을 설명합니다.

트랜잭션 정의 생성 및 추가에 관한 자세한 정보는 트랜잭션 정의 생성 및 추가 를 참조하십시오.

트랜잭션 정의(속성)

이름	설명
이름	이름을 입력하십시오.
인코딩	현금 등록기와 같은 트랜잭션 소스에서 사용하는 문자 집합을 선택합니다. 이는 XProtect Transact 이(가) 정의를 구성할 때 사용자가 사용할 수 있는 인식 가능한 텍스트로 트랜잭션 데이터를 변환하도록 돕습니다. 잘못된 인코딩을 선택하면 데이터가 의미 없는 텍스트로 나타날 수도 있습니다.
데이터 수집 시작	연결된 트랜잭션 소스로부터 트랜잭션 데이터를 수집합니다. 이 데이터를 이용하여 트랜잭션 정의를 구성할 수 있습니다. 최소한 하나, 가능하면 몇 개의 추가 트랜잭션이 완료될 때까지 기다립니다.
데이터 수집 중지	정의를 구성하기에 충분한 데이터를 수집했으면 이 버튼을 클릭합니다.
파일에서 로드	기존 파일에서 데이터를 가져오려면 이 버튼을 클릭합니다. 일반적으로, 이 파일은 사용자가 .capture 파일 형식으로 이전에 생성했던 파일입니다. 다른 파일 형식일 수도 있습니다. 여기서 중요한 점은 가져오기 파일의 인코딩이 현재 정의에 대해 선택한 인코딩과 일치해야 한다는 것입니다.
파일에 저장	수집된 원시 데이터를 파일에 저장하려면 이 버튼을 클릭합니다. 나중에 이 파일을 재사용할 수 있습니다.
유형 일치	수집된 원시 데이터에서 시작 패턴과 중지 패턴을 검색할 때 사용할 일치 유형을 선택합니다: • 정확히 일치 사용: 검색을 하면 **시작 패턴** 및 **중지 패턴** 필드에 입력한 내용과 정확하게 일치하는 내용을 포함하는 문자열을 확인합니다. • 와일드카드 사용: 검색을 하면 와일드 카드 기호(*, #, ?)와 조합하여 **시작 패턴** 및 **중지 패턴**에 입력한 내용을 포함하는 문자열을 확인합니다 *는 모든 수의 문자와 일치를 나타냅니다. 예를 들어, "Start tra*tion"을 입력했다면 검색 시 "Start transaction"을 포함하는 문자열을 찾습니다. #는 정확하게 1 자리의 일치를 나타냅니다. 예를 들어, "# watermelon"을 입력했다면 검색 시 예를 들어 "1 watermelon"을 포함하는 문자열을 찾습니다. ? 정확하게 1개의 문자와 일치합니다. 예를 들어, "Start trans?ction"의 검색식을 이용하여 "Start transaction"을 포함하는 문자열을 확인할 수 있습니다

이름	설명
	• 정규식 사용: 이 일치 방식을 이용하여 날짜 형식이나 신용카드 번호 같은 특정한 표기법이나 규약을 포함하는 문자열을 식별합니다. 자세한 정보는 Microsoft 웹사이트를 참조하십시오(https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/)
원시 데이터	연결된 트랜잭션 소스의 트랜잭션 데이터 문자열이 이 섹션에 표시됩니다.
시작 패턴	트랜잭션이 시작되는 위치를 표시하는 시작 패턴을 지정합니다. 수평 라인이 **미리보기** 필드에 삽입되어 트랜잭션이 시작되고 끝나는 위치를 시각적으로 나타내고 개별 트랜잭션을 구분시킵니다.
중지 패턴	트랜잭션이 끝나는 위치를 표시하는 중지 패턴을 지정합니다. 중지 패턴은 필수는 아니지만 수신 데이터에 실제 트랜잭션 사이의 개장 시간이나 특별 행사 정보 등의 관련이 없는 정보가 포함되는 경우에 유용합니다. 중지 패턴을 지정하지 않으면 다음 영수증 시작 위치를 기준으로 영수증 끝이 정의됩니다. 시작은 **시작 패턴** 필드에 입력한 내용을 기준으로 결정됩니다.
필터 추가	**필터 추가** 버튼을 사용하여 XProtect Smart Client 에서 생략하려고 하거나 다른 문자 또는 줄바꿈으로 대체하려는 문자를 알려 줍니다. 문자 교체는 트랜잭션 소스 문자열에 비인쇄 목적의 제어 문자가 포함되는 경우 유용합니다. 줄바꿈 추가는 XProtect Smart Client 에서 영수증이 원본 영수증과 같아 보이도록 하기 위해 필요합니다.
필터 텍스트	**원시 데이터** 섹션에 현재 선택된 문자를 표시합니다. 생략하거나 대체하려는 문자를 알고 있지만 수집된 원시 데이터 문자열에 그 내용이 없으면 **문자** 필드에 수동으로 문자를 입력할 수 있습니다. 문자가 제어 문자인 경우, 16진수 바이트 값을 입력해야 합니다. 바이트 값에 다음 형식을 사용합니다: {XX}, 그리고 문자가 여러 바이트로 구성되는 경우 {XX,XX,...}.
동작	추가하는 각 필터에 대해 선택한 문자가 처리되는 방식을 지정해야 합니다. • 누락: 선택하는 문자가 필터링되어 제거됩니다 • 대체: 선택하는 문자가 지정하는 문자로 대체됩니다 • 줄바꿈 추가: 선택하는 문자가 줄바꿈으로 대체됩니다
대체	선택한 문자를 대체할 텍스트를 입력합니다. **대체** 동작을 선택한 경우에만 관련됩니다.
필터 텍스트	필터 추가 후 아직 제거되지 않은 인쇄되지 않는 문자 제거.

이름	설명
로 정의되지 않은 컨트롤 문자 제거	**원시 데이터** 창과 **미리보기** 섹션에서, 이 설정을 활성화 또는 비활성화할 때 거래 데이터 문자열이 어떤게 변경되는지 확인하십시오.
미리보기	**미리보기** 섹션을 이용하여 원하지 않는 문자를 식별하고 제거했는지 확인합니다. 여기에 나타나는 출력은 XProtect Smart Client 에서와 같은 실제 영수증과 유사합니다.

알람 노드

알람 정의(알람 노드)

시스템이 해당 시스템에 이벤트를 등록하면 XProtect Smart Client 에서 알람을 생성하도록 시스템을 구성할 수 있습니다. 알람을 사용하기 전에 정의해야 하며, 알람은 시스템 서버에 등록된 이벤트를 기준으로 정의됩니다. 또한 알람을 트리거하는 데 사용자 정의 이벤트를 사용하고 다른 여러 알람을 트리거하는 데 동일 이벤트를 사용할 수 있습니다.

알람 정의 설정:

이름	설명
활성화	기본적으로, 알람 정의가 사용됩니다. 사용하지 않으려면 확인란 선택을 취소하십시오.
이름	알람 이름은 고유할 필요는 없지만 고유하고 설명적인 알람 이름을 사용하면 여러 상황에서 이점이 있습니다.
지침	알람 및 알람을 발생시킨 문제의 해결 방법에 대한 설명 텍스트를 입력합니다. 사용자가 알람을 처리할 때 XProtect Smart Client 에 이 텍스트가 표시됩니다.
이벤트 트리거	알람이 트리거될 때 사용할 이벤트 메시지를 선택합니다. 두 개의 드롭다운 중에서 선택합니다. • 첫 번째 드롭다운: 분석 이벤트 및 시스템 이벤트 등 이벤트의 종류를 선택합니다 • 두 번째 드롭다운: 사용할 특정 이벤트 메시지를 선택합니다. 사용 가능한 메시지는 첫 번째 드롭다운 메뉴에서 선택한 이벤트 유형에 따라 결정됩니다
소스	이벤트의 출처가 되는 소스를 지정합니다. 카메라 또는 기타 장치 외에 VCA 및 MIP 등 플러그 인 정의된 소스를 지정할 수도 있습니다. 사용할 수 있는 옵션은 선택한 이벤트 유형에 따라 다릅니다.

알람 트리거:

이름	설명
시간 프로파일	알람 정의가 활성 상태로 유지되는 기간을 지정하려면 **시간 프로파일** 라디오 버튼을 선택합니다. **규칙 및 이벤트** 노드에서 정의한 시간 프로파일만 목록에 표시됩니다. 정의된 내용이 없으면 **항상** 옵션만 사용할 수 있습니다.
이벤트 기반	이벤트를 알람의 기반으로 이용하려면 이 라디오 버튼을 선택합니다. 선택한 후에는 시작 및 중지 이벤트를 지정합니다. 카메라, 비디오 서버 및 입력에 정의된 하드웨어 이벤트를 선택할 수 있습니다. 이벤트 개요 도 참조하십시오. 또한 전체/수동 이벤트 정의도 사용할 수 있습니다. 사용자 정의 이벤트(설명됨) 도 참조하십시오.

운영자 동작 필요:

이름	설명
시간 제한	운영자 동작이 필요한 때의 시간 제한을 선택합니다. 기본값은 1분입니다. **트리거된 이벤트** 드롭다운 메뉴에서 이벤트를 첨부하기 전에는 시간 제한이 활성화되지 않습니다.
트리거된 이벤트	시간 제한이 경과했을 때 트리거할 이벤트를 선택합니다.

맵:

이름	설명
알람 관리자 뷰	XProtect Smart Client > **알람 관리자** 에 알람이 나열된 경우, 스마트 맵이나 맵을 알람에 할당합니다. 장치가 트리거 했거나 해당 장치가 스마트 맵에 추가된 경우 스마트 맵에 알람이 표시됩니다.

기타:

이름	설명
관련 카메라	카메라가 직접 알람을 트리거하지 않는 경우라도 최대 15개의 카메라를 선택하여 알람 정의에 포함시킵니다. 이 옵션은 예를 들어, 외부 이벤트 메시지(예: 도어 열림)를 알람 소스로 선택한 경우에 해당될 수 있습니다. 도어 근처에 하나 이상의 카메라를 정의함으로써 인시던트에 대한 카메라 레코딩을 알람에 연결할 수 있습니다.
초기 알람 소유자	알람을 책임지는 기본 사용자를 선택합니다.
초기 알람 우선순위	알람의 우선순위를 선택합니다. XProtect Smart Client 에서 이러한 우선순위를 사용하여 알람의 중요도를 결정합니다.
알람 범주	알람에 대한 알람 카테고리를 선택합니다(예: **잘못된 알람** 또는 **조사 필요**).
알람에 의해 트리거된 이벤트	XProtect Smart Client 에서 알람이 트리거할 수 있는 이벤트를 정의합니다.
알람 자동 닫기	특정 이벤트로 알람이 자동 중단되도록 하려면 이 확인란을 선택합니다. 모든 이벤트가 알람을 트리거할 수 있는 것은 아닙니다. 처음부터 새로운 알람을 사용하지 않도록 설정하려면 확인란의 선택을 취소하십시오.
관리자에 할당 가능한 알람	**할당 대상** 목록에서 관리자 역할을 가진 사용자를 포함시키려면 확인란을 선택합니다. **할당 대상** 목록은 XProtect Smart Client 의 **알람 관리자** 탭에서 알람 세부 정보에 있습니다. 목록을 줄이기 위해 **할당 대상** 목록에서 관리자 역할을 가진 사용자를 필터링하기 위해 확인란을 지웁니다.

알람 데이터 설정(알람 노드)

알람 데이터 설정을 구성하는 경우, 다음을 지정합니다:

알람 데이터 수준 탭

우선순위

이름	설명
수준	선택 수준 번호로 새 우선순위를 추가하거나 기본 우선순위 수준을 사용/편집합니다(번호 1, 2 또는 3). 이 우선순위 수준은 **초기 알람 우선순위 설정** 을 구성하는 데 사용됩니다.
이름	개체의 이름을 입력합니다. 원하는 만큼 만들 수 있습니다.
사운드	알람과 연관시킬 사운드를 선택합니다. 기본 사운드 중 하나를 사용하거나 **사운드 설정** 에서 다른 사운드를 추가합니다.
사운드 반복	XProtect Smart Client 에서 운영자가 알람 목록에서 알람을 클릭할 때까지 사운드가 한 번 또는 반복 재생될 지 결정합니다.
데스크톱 알림 활성화	각 알람의 우선순위에 대해 데스크톱 알림을 활성화 또는 비활성화할 수 있습니다. 만일 XProtect 을(를) 지원하는 Smart Client VMS를 사용하는 중이라면 필수 Smart Client 프로필에서 알림을 활성화해야 합니다. 페이지 432의 알람 관리자 탭(Smart Client 프로필)를 참조하십시오.

상태

이름	설명
수준	기본 상태 수준(번호 **1**, **4**, **9** 및 **11**이며 편집 또는 재사용할 수 없음)에 더하여 선택한 수준 번호로 새 상태를 추가합니다. 이러한 상태 수준은 XProtect Smart Client의 *알람 목록*에서만 볼 수 있습니다.

카테고리

이름	설명
수준	선택한 수준 번호와 함께 새 카테고리를 추가합니다. 이러한 카테고리 수준은 **초기 알람 카테고리** 설정을 구성하는 데 사용됩니다. 수준 99는 XProtect Mobile 클라이언트의 비상 경보 알람용으로 예약되어 있습니다.
이름	개체의 이름을 입력합니다. 원하는 만큼 만들 수 있습니다.

알람 목록 구성 탭

이름	설명
사용 가능한 열	> 를 사용하여 XProtect Smart Client의 *알람 목록*에서 사용 가능한 열을 선택합니다. < 를 사용하여 선택을 해제합니다. 완료되면 **선택된 열** 에 포함시키려는 항목들이 나와 있습니다.

닫는 이유 탭

이름	설명
활성화	알람을 닫기 전에 모든 알람에 대해 닫는 이유를 지정하도록 하려면 선택합니다.
이유	알람을 닫을 때 사용자가 선택할 수 있는 닫는 이유를 추가합니다. *확인된 침입자* 또는 *허위 알람* 등을 예로 들 수 있습니다. 원하는 만큼 만들 수 있습니다.

사운드 설정(알람 노드)

사운드 설정을 구성할 때 다음을 지정합니다:

이름	설명
사운드	알람과 연관시킬 사운드를 선택합니다. 사운드 목록에는 다수의 기본 Windows 사운드가 포함되어 있습니다. 또한 새로운 사운드(.wav or .mp3)를 추가할 수 있습니다.
추가	사운드를 추가합니다. 사운드를 검색하여 하나 또는 여러 개의 .wav 또는 .mp3 파일을 업로드합니다.
제거	수동으로 추가한 사운드 목록에서 선택한 사운드를 제거합니다. 기본 사운드는 제거할 수 없습니다.
테스트	사운드를 테스트합니다. 목록에서 사운드를 선택합니다. 사운드가 한 번 재생됩니다.

연합 사이트 계층

연합 사이트 속성

이 섹션은 **일반** 탭 및 **상위 사이트** 탭을 설명합니다.

일반 탭

현재 로그인한 사이트와 관련된 일부 정보를 변경할 수 있습니다.

이름	설명
이름	사이트의 이름을 입력합니다.
설명	사이트 설명을 입력합니다.
URL	목록을 사용하여 이 사이트의 URL을 추가 및 제거하고 외부 사이트인지 여부를 나타냅니다. 로컬 네트워크 외부에서 외부 주소에 연결할 수 있습니다.
버전	사이트의 관리 서버에 대한 버전 번호.
서비스 계정	관리 서버가 실행 중인 서비스 계정.
마지막 동기화의 시간	계층의 마지막 동기화 시간과 날짜.
마지막 동기화의 상태	계층의 마지막 동기화 상태. **성공** 또는 **실패** 일 수도 있습니다.

상위 사이트 탭

이 탭에는 현재 로그인한 사이트의 상위 사이트에 대한 정보가 표시됩니다. 사이트에 상위 사이트가 없으면 이 탭이 표시되지 않습니다.

이름	설명
이름	상위 사이트의 이름을 표시합니다.

이름	설명
설명	상위 사이트의 설명을 표시합니다(옵션).
URL	상위 사이트의 URL을 나열하고 외부 사이트인지 여부를 나타냅니다. 로컬 네트워크 외부에서 외부 주소에 연결할 수 있습니다.
버전	사이트의 관리 서버에 대한 버전 번호.
서비스 계정	관리 서버가 실행 중인 서비스 계정.
마지막 동기화의 시간	계층의 마지막 동기화 시간과 날짜.
마지막 동기화의 상태	계층의 마지막 동기화 상태. **성공** 또는 **실패** 일 수도 있습니다.

helpfeedback@milestone.dk

Milestone 정보

Milestone Systems 은(는)세계가 안전을 보장하고, 자산을 보호하며, 비즈니스 효율을 증대하는 방법을 파악하는 데 유용한 기술인 개방형 플랫폼 비디오 관리 소프트웨어 분야의 선두 업체입니다. Milestone Systems은(는) 전 세계 150,000개 이상의 사이트를 통하여 검증된 신뢰성 있는 확장 가능한 솔루션을 기반으로, 네트워크 비디오 기술의 개발 및 사용에 협업과 혁신을 이끄는 개방형 플랫폼 커뮤니티를 제공하고 있습니다. 1998년에 설립된 Milestone Systems 은 Canon Group 내 독립 기업입니다. 자세한 내용은 https://www.milestonesys.com/ 에서 확인하십시오.