MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R3

관리자 설명서

milestone

목차

Copyright, 상표 및 면책 조항

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

XProtect Mobile (설명됨)

XProtect Mobile 은(는) 다섯 가지 요소로 구성되어 있습니다.

- XProtect Mobile 클라이언트

  XProtect Mobile 클라이언트는 Android 또는 Apple 기기에서 설치하여 사용할 수 있는 모바일 감시 앱입니다. XProtect Mobile 클라이언트를 필요한 만큼 설치하여 사용할 수 있습니다.

  자세한 내용은 Milestone Systems 웹 사이트에서 XProtect Mobile 클라이언트 사용자 안내서를 다운로드하십시오(https://www.milestonesys.com/support/help-yourself/manuals-and-guides/).

- XProtect Web Client

  XProtect Web Client 에서 웹 브라우저 상의 라이브 비디오를 보고 레코딩을 다운로드할 수 있습니다. XProtect Web Client 은(는) XProtect Mobile 서버를 설치할 때 자동으로 같이 설치됩니다.

  자세한 내용은 Milestone Systems 웹 사이트에서 XProtect Web Client 사용자 안내서를 다운로드하십시오(https://www.milestonesys.com/support/help-yourself/manuals-and-guides/).

- XProtect Mobile 서버
- XProtect Mobile 플러그 인
- Mobile Server Manager

본 설명서에서는 XProtect Mobile 서버와 XProtect Mobile 플러그 인 및 Mobile Server Manager 에 대해 다룹니다.

XProtect Mobile 서버 (설명됨)

XProtect Mobile 서버는 XProtect Mobile 클라이언트 또는 XProtect Web Client 에서 시스템으로의 로그인을 처리합니다.

XProtect Mobile 서버는 레코딩 서버에서 XProtect Mobile 클라이언트 또는 XProtect Web Client (으)로 비디오 스트림을 배포합니다. 이렇게 함으로써 레코딩 서버가 인터넷에 연결되지 않는 안전한 환경이 구성됩니다. XProtect Mobile 서버가 레코딩 서버로부터 비디오 스트림을 수신한 후 복잡한 코덱 및 형식 변환도 처리하므로 모바일 장치에서 비디오를 스트리밍할 수 있습니다.

레코딩 서버에 액세스하고자 할 때 이용할 모든 컴퓨터에 XProtect Mobile 서버를 설치해야 합니다. XProtect Mobile 서버를 설치할 때 관리자 권한이 있는 계정으로 로그인해야 합니다. 그렇지 않으면 설치가 성공적으로 완료되지 않습니다(페이지 12의 XProtect Mobile 서버 설치 참조).

XProtect Mobile 서버는 라이브 모드로 직접 스트리밍과 적응 스트리밍을 지원합니다(XProtect Expert 및 XProtect Corporate 에 대해서만).

제품 비교 차트

XProtect VMS 에는 다음 제품들이 포함됩니다.

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

전체 기능 목록은 Milestone 웹사이트의 제품 개요 페이지에서 확인할 수 있습니다 (https://www.milestonesys.com/solutions/platform/product-index/).

다음 목록에는 제품 간의 주요 차이가 나와 있습니다.

이름	**XProtect Essential+**	**XProtect Express+**	**XProtect Professional+**	**XProtect Expert**	**XProtect Corporate**
SLC 당 사이트	1	1	멀티 사이트	멀티 사이트	멀티 사이트
SLC 당 레코딩 서버	1	1	무제한	무제한	무제한
레코딩 서버 당 하드웨어 장치	8	48	무제한	무제한	무제한
Milestone Interconnect™	-	원격 사이트	원격 사이트	원격 사이트	중앙/원격 사이트
Milestone Federated Architecture™	-	-	-	원격 사이트	중앙/원격 사이트
레코딩 서버 장애 조치	-	-	-	수동 및 상시 대기	수동 및 상시 대기
원격 연결 서비스	-	-	-	-	✓
에지 저장소 지원	-	-	✓	✓	✓
다단계 비디오 저장소	라이브 데이터베이스 + 1 아카이	라이브 데이터베이스 + 1 아카이	라이브 데이터베이스 + 1 아카이브	라이브 데이터베이스 + 무제한 아카이브	라이브 데이터베이스 + 무제한 아카이브

이름	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
	브	브			
SNMP 알림	-	-	-	✓	✓
시간 제어 사용자 액세스 권한	-	-	-	-	✓
프레임 속도 줄이기(정리)	-	-	-	✓	✓
비디오 데이터 암호화(레코딩 서버)	-	-	-	✓	✓
데이터베이스 서명(레코딩 서버)	-	-	-	✓	✓
PTZ 우선순위 수준	1	1	3	32000	32000
확장 PTZ(PTZ 세션 보존 및 XProtect Smart Client (으)로부터 순찰)	-	-	-	✓	✓
증거물 잠금	-	-	-	-	✓
북마크 기능	-	-	수동 전용	수동 및 규칙 기반	수동 및 규칙 기반
라이브 멀티 스트리밍 또는 멀티캐스팅 / 적응 스트리밍	-	-	-	✓	✓
직접 스트리밍	-	-	-	✓	✓
전체 보안	클라이언트 사용자 권한	클라이언트 사용자 권한	클라이언트 사용자 권한	클라이언트 사용자 권한	클라이언트 사용자 권한/ 관리자 사용자

이름	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
					권한
XProtect Management Client 프로파일	-	-	-	-	✓
XProtect Smart Client 프로파일	-	-	3	3	무제한
XProtect Smart Wall	-	-	-	선택 사항	✓
시스템 모니터	-	-	-	✓	✓
스마트 맵	-	-	-	✓	✓
단2계 확인	-	-	-	-	✓
DLNA 지원	-	✓	✓	✓	✓
사생활 보호	-	✓	✓	✓	✓
장치 암호 관리			✓	✓	✓

요구사항 및 고려사항

XProtect Mobile 사용을 위한 전제조건

XProtect Mobile 의 사용을 시작하기 전에 다음이 준비되어 있는지 확인해야 합니다.

- VMS 설치본이 실행 중이고 최소 한 명 이상의 사용자가 구성됨.
- XProtect Smart Client 에서 카메라 및 뷰 설정
- Android 또는 iOS에서 운영되고 XProtect Mobile 클라이언트 응용 프로그램을 다운로드할 수 있는 Google Play 또는 App Store℠에 액세스할 수 있는 모바일 기기
- XProtect Web Client 실행을 위한 웹 브라우저

요구사항에 대한 자세한 내용은 페이지 10의 XProtect Mobile 시스템 요구사항을 참조하십시오.

XProtect Mobile 시스템 요구사항

시스템의 여러 구성 요소에 대한 시스템 요구 사항에 대한 자세한 내용을 보려면 Milestone 웹사이트를 방문하십시오(https://www.milestonesys.com/systemrequirements/).

- XProtect Mobile 클라이언트에 대한 요구 사항을 보려면 **XProtect Mobile** 제품 아이콘을 선택합니다.
- XProtect Web Client 에 대한 요구 사항을 보려면 **XProtect Web Client** 제품 아이콘을 선택합니다.
- XProtect Mobile 서버에 대한 요구사항을 보려면 설치한 XProtect 제품의 아이콘을 선택합니다.
- XProtect Mobile 플러그 인에 대한 요구사항:
    - 실행 중인 Management Client
    - VMS와 통합하기 위한 Milestone 플러그 인이 설치되어 있음.

알림 설정 요구사항

- 하나 이상의 알람을 하나 이상의 이벤트 및 규칙과 연결시켜야 합니다. 이것은 시스템 알림을 위한 조건은 아닙니다.
- Milestone Care™ 와(과) Milestone Systems 의 부합 여부가 최신 상태여야 합니다.
- 시스템은 반드시 인터넷에 접속 가능해야 합니다

자세한 내용은 다음을 참조하십시오.

페이지 47의 XProtect Mobile 서버에서 푸시 알림 설정

페이지 24의 알림 탭

스마트 연결 설정 요구사항

- XProtect Mobile 서버는 공용 IP 주소를 사용해야 합니다. 주소는 고정 또는 동적 주소일 수 있지만 일반적으로 고정 IP 주소를 이용하는 것이 좋습니다.
- 스마트 연결을 위한 유효한 라이선스가 있어야 합니다

사용자의 2단계 확인 설정에 대한 요구 사항

- SMTP 서버를 설치하였습니다
- 사이트 탐색 창의 역할 노드에 Management Client 에서 XProtect 시스템에 사용자 및 그룹을 추가합니다. 관련 역할에서 사용자 및 그룹 탭을 선택합니다.
- XProtect 의 이전 버전에서 시스템을 업그레이드한 경우, 2단계 확인 기능을 활성화하기 위해 모바일 서버를 재시작해야 합니다.

자세한 내용은 다음을 참조하십시오.

페이지 53의 2단계 이메일 확인을 위해 사용자 설정

페이지 25의 단계 확인 탭

비디오 푸시 설정에 대한 요구사항

- 각 채널에 하드웨어 장치 라이선스가 필요합니다
- 비디오 푸시와 함께 오디오를 활성화하는 방법:
  1. Milestone XProtect Device Pack 10.3a 버전 또는 그 이후 버전을 다운로드하고 설치합니다.
  2. XProtect Mobile Server Installer.exe 13.2a 또는 그 이후 버전을 다운로드하고 설치합니다.
  3. Recording Server 서비스를 재시작합니다.

직접 스트리밍을 위한 요건

XProtect Mobile 은(는) 라이브 모드로 직접 스트리밍을 지원합니다(XProtect Expert 및 XProtect Corporate 에 대해서만).

직접 스트리밍을 위한 카메라 구성 요건

XProtect Web Client 및 XProtect Mobile 클라이언트에서 직접 스트리밍을 사용하려면, 다음과 같이 카메라를 구성해야 합니다.

- 해당 카메라는 H.264 코덱(모든 클라이언트용)이나 H.265 코덱(XProtect Mobile 클라이언트 전용)을 지원해야 합니다.
- 권장 **GOP** 크기 설정값은 **1**초 이며 **FPS** 설정값은 **10** FPS보다 커야만 합니다.

설치

XProtect Mobile 서버 설치

XProtect Web Client 서버를 설치했으면 XProtect Mobile 클라이언트와 XProtect Mobile 을(를) 시스템에서 사용할 수 있습니다. 관리 서버를 실행하는 컴퓨터에서 전체 시스템 리소스 사용을 줄이려면 별도의 컴퓨터에 XProtect Mobile 서버를 설치하십시오.

관리 서버에는 공용 설치 웹 페이지가 내장되어 있습니다. 이 웹 페이지에서 관리자와 최종 사용자는 관리 서버 또는 시스템의 다른 컴퓨터에서 필요한 XProtect 시스템 구성 요소를 다운로드한 다음 설치할 수 있습니다.

> XProtect Mobile 서버는 "단일 컴퓨터 옵션"을 설치하면 자동으로 설치됩니다.

XProtect Mobile 서버를 설치하려면:

1. 브라우저에 다음 URL을 입력합니다. *http://[관리 서버 주소]/installation/admin*, 여기서 [관리 서버 주소]는 관리 서버의 IP 주소나 호스트 이름입니다.
2. XProtect Mobile 서버 설치 프로그램에 대해 모든 언어 를 클릭합니다.
3. 다운로드한 파일을 실행합니다. 그다음 예 를 클릭합니다. 그다음 압축이 풀리기 시작합니다.
4. 설치 프로그램에 사용할 언어를 선택합니다. 그다음 계속 을 클릭합니다.
5. 사용권 계약 내용을 읽고 동의합니다. 그다음 계속 을 클릭합니다.
6. 설치 유형 선택:
   - 일반 을 클릭해서 XProtect Mobile 서버와 플러그 인을 설치합니다
   - 사용자 정의 을 클릭해 서버나 플러그 인 중 하나만 설치합니다. 예를 들어, Management Client 을(를) 사용하여 XProtect Mobile 서버를 관리하려고 하지만 해당 컴퓨터에서 XProtect Mobile 서버가 필요하지 않은 경우에는 플러그인만 설치하는 것이 유용합니다

     > XProtect MobileManagement Client 의 XProtect Mobile 서버를 관리하기 위해 Management Client 가 구동되는 컴퓨터에 플러그인이 필요합니다.

7. 사용자 정의 설치 전용: 설치하고자 하는 구성 요소를 선택합니다. 그다음 계속 을 클릭합니다.
8. 모바일 서버에 대한 서비스 계정을 선택합니다. 그다음 계속 을 클릭합니다.

   > 마지막 단계에서 서비스 계정 자격 증명을 변경하거나 편집하려면 모바일 서버를 다시 설치해야 합니다.

9. 서버 **URL** 필드에서 주요 관리 서버 주소를 입력합니다.

10. 사용자 정의 설치 전용: 모바일 서버와 통신을 위한 포트를 지정합니다. 그다음 계속 을 클릭합니다.

> 일반적인 설치에서 연결 포트는 기본 포트 번호를 부여받습니다(HTTP 포트에는 8081 및 HTTPS 포트에는 8082).

11. 모바일 서버 암호화를 지정합니다. 그다음 계속 을 클릭합니다.

    암호화 선택 페이지에서 다음과 같이 통신 흐름을 암호화할 수 있습니다.

    - 모바일 서버와 레코딩 서버, 데이터 수집기, 그리고 관리 서버 간. 내부 통신 흐름 암호화를 활성화하려면 서버 인증서 섹션에서 인증서를 선택합니다.
    - 모바일 서버와 클라이언트 간. 모바일 서버에서 데이터 스트림을 검색하는 모바일 서버 및 클라어언트 구성 요소 간의 암호화를 활성화하려면 스트리밍 미디어 인증서 섹션에서 인증서를 선택합니다.

> 암호화를 활성화하지 않는 경우 일부 클라이언트 내 일부 기능은 사용할 수 없게 됩니다. 더 자세한 정보는 페이지 37의 클라이언트를 위한 모방리 서버 암호화 요건을 참조하십시오.

    시스템 내 보안 통신 준비에 관한 자세한 정보는 페이지 35의 모바일 서버 데이터 암호화(설명됨) 또는 인증서에 관한 Milestone 안내서 를 참조하십시오.

    또한 설치를 완료한 후 운영 체제의 태스크바에 있는 Mobile Server Manager 트레이 아이콘에서 암호화를 활성화할 수도 있습니다(페이지 42의 모바일 서버 암호화를 활성화합니다 참조).

12. 파일 위치 및 제품 언어를 선택한 다음, 설치 를 클릭합니다.
13. 설치가 끝나면 성공적으로 설치된 구성 요소 목록이 표시됩니다. 그다음 닫기 를 클릭합니다.

XProtect Mobile 을(를) 구성할 준비가 되었습니다(페이지 14의 모바일 서버 설정 참조).

구성

모바일 서버 설정

Management Client 에서는 모바일 서버 속성 섹션의 맨 아래 도구 모음에 있는 탭을 통해 액세스할 수 있는 XProtect Mobile 서버 설정의 목록을 구성하고 편집할 수 있습니다. 여기에서 다음을 수행할 수 있습니다.

- 서버 기능 일반 구성 활성화 또는 비활성화합니다(페이지 14의 일반 탭 참조)
- 서버 연결 설정을 구성하고 스마트 연결 기능을 설정합니다(페이지 16의 연결성 탭 참조)
- 서버 현재 상태 및 나열된 활성 사용자 확인합니다(페이지 18의 서버 상태 탭 참조)
- 성능 매개변수를 설정하여 직접 스트리밍과 적응 스트리밍을 활성화하거나 트랜스코딩된 비디오 스트림 제한을 설정합니다(페이지 19의 성능 탭 참조).
- 조사 설정을 구성합니다(페이지 22의 조사 탭 참조)
- 비디오 푸시 설정을 구성합니다(페이지 23의 비디오 푸시 탭 참조)
- 시스템 및 푸시 알림을 설정하고 켜고 끕니다(페이지 24의 알림 탭 참조)
- 사용자에 대한 추가적인 로그인 단계를 활성화하고 구성합니다(페이지 25의 단계 확인 탭 참조)

일반 탭

다음 표에 이 탭의 설정이 설명되어 있습니다.

일반

이름	설명
서버 이름	XProtect Mobile 서버의 이름을 입력합니다.
설명	선택적으로 XProtect Mobile 서버에 대한 설명을 입력합니다.
모바일 서버	현재 선택된 XProtect Mobile 서버의 이름을 확인하십시오.
로그인 방법	사용자가 서버에 로그인할 때 사용할 인증 방법을 선택합니다. 다음 중 선택 가능: • 자동 • **Windows** 인증 • 기본 인증

기능

다음 표에서는 어떻게 XProtect Mobile 기능을 통제하는지를 설명해줍니다.

이름	설명
활성화 **XProtect Web Client**	XProtect Web Client 에 대한 액세스를 활성화합니다. 이 기능은 기본으로 활성화됩니다.
모든 카메라 뷰 활성화	모든 카메라 뷰를 포함합니다. 이 뷰에는 사용자가 레코딩 서버에서 보도록 허용된 모든 카메라가 표시됩니다. 이 기능은 기본으로 활성화됩니다.
동작 활성화(출력 및 이벤트)	XProtect Mobile 클라이언트 및 XProtect Web Client 에서 동작 액세스를 활성화합니다. 이 기능은 기본으로 활성화됩니다. 이 기능을 비활성화할 경우, 클라이언트 사용자는 올바르게 구성되더라도 출력 및 이벤트를 확인할 수 없습니다.
수신 오디오 활성화	XProtect Web Client 및 XProtect Mobile 클라이언트에서 수신 오디오 기능을 활성화합니다. 이 기능은 기본으로 활성화됩니다.
푸시투톡 활성화	XProtect Web Client 및 XProtect Mobile 클라이언트에서 푸시투톡(PTT) 기능을 활성화합니다. 이 기능은 기본으로 활성화됩니다.
XProtect Mobile 서버에 대한 내장된 관리자 역할 액세스를 거부합니다.	XProtect Mobile 클라이언트 또는 XProtect Web Client 에서 내장된 관리자 역할에 할당된 사용자가 비디오에 액세스하지 못하도록 하려면 활성화합니다.

로그 설정(L)

로그 설정에 관한 정보를 볼 수 있습니다.

이름	설명
로그 파일 위치	시스템이 로그 파일을 저장하는 곳을 확인합니다.
다음 기간 동안 로그 유지	로그 보관 일수를 확인합니다. 기본값은 30일입니다.

구성 백업

시스템이 여러 XProtect Mobile 서버를 가지는 경우, 현재 설정을 내보내기 위해 백업 기능을 사용하고 다른 XProtect Mobile 서버에 가져올 수 있습니다.

이름	설명
가져오기	새 XProtect Mobile 서버 구성을 가진 XML 파일을 가져옵니다.
내보내기	XProtect Mobile 서버 구성을 내보냅니다. 시스템은 XML 파일에 구성을 저장합니다.

연결성 탭

연결성 탭의 설정은 다음 작업에 사용됩니다.

- 페이지 46의 연결 설정 구성
- 페이지 46의 사용자에게 이메일 메시지 보내기
- 페이지 46의 복잡한 네트워크에서 연결 활성화
- 페이지 45의 라우터에서 범용 플러그 앤 플레이 검색 기능 활성화

자세한 정보는 페이지 45의 스마트 연결(설명됨)을 참조하십시오.

> 설치 중에 **Server Configurator** 을(를) 열거나 설치 후 마우스 오른쪽 단추로 Mobile Server Manager 트레이 아이콘을 클릭하여 XProtect Mobile 클라이언트 및 XProtect Web Client 사용자가 XProtect Mobile 서버에 연결하는 방법을 구성할 수 있습니다. 연결 유형은 HTTPS 또는 HTTP 둘 중에 하나일 수 있습니다. 자세한 정보는 페이지 58의 모바일 서버 암호화를 활성화합니다 를 참조하십시오.

일반

이름	설명
클라이언트 제한 시간**(HTTP)**	XProtect Mobile 클라이언트 및 XProtect Web Client 이(가) XProtect Mobile 서버에 자신이 실행 중임을 나타내어야 하는 빈도에 대한 시간 프레임을 설정합니다. 기본값은 30초입니다.

이름	설명
	Milestone 에서는 이 시간 프레임을 증가시키지 않도록 권장합니다.
UPnP 검색 기능 활성화	이를 통해 UPnP 프로토콜을 사용하여 네트워크에서 XProtect Mobile 서버를 검색할 수 있습니다. XProtect Mobile 클라이언트는 UPnP에 기반하여 XProtect Mobile 서버 검색을 위한 스캔 기능을 가지고 있습니다.
자동 포트 매핑 사용	XProtect Mobile 서버가 방화벽 뒤에 설치된 경우, 클라이언트가 인터넷에서 서버에 액세스할 수 있도록 라우터에서 포트 매핑이 필요합니다. 자동 포트 매핑 사용 옵션을 통해 라우터가 구성된 경우에 XProtect Mobile 서버가 스스로 이 포트 매핑을 할 수 있습니다.
스마트 연결 사용	스마트 연결을 이용하면 모바일 장치나 태블릿에 로그인하여 검증할 필요 없이 XProtect Mobile 서버를 올바르게 구성했는지 확인할 수 있습니다. 또한 클라이언트 사용자의 연결 프로세스를 단순화시킵니다.

인터넷 액세스

이름	설명
사용자 정의 인터넷 액세스 구성	특정 연결에 대한 직접 연결을 위해 UPnP 포트 매핑을 사용하는 경우, 사용자 정의 인터넷 연결 구성 확인란을 선택합니다. 그런 다음 **IP** 주소나 호스트 이름 그리고 연결에 사용할 포트를 제공합니다. 예를 들어, 라우터가 UPnP를 지원하지 않거나 라우터 체인을 사용하는 경우에 이렇게 해야 할 수 있습니다.
기본 주소 비활성화	사용자 지정 IP 주소 또는 호스트 이름으로만 모바일 서버에 접속하기 위해 기본 IP 주소를 비활성화하ㅏㅂ니다.
IP 주소를 동적으로 가져오려면 선택	IP 주소가 종종 바뀔 경우, **IP** 주소 동적 검색을 위해 선택 상자를 선택합니다.

이름	설명
HTTP 포트	HTTP 연결을 위한 포트 번호를 입력합니다. 기본 포트 번호는 8081입니다.
HTTPS 포트	HTTPS 연결을 위한 포트 번호를 입력합니다. 기본 포트 번호는 8082입니다.
서버 주소	모바일 서버에 연결된 모든 IP 주소를 표시합니다.

스마트 연결 알림

이름	설명
다음 수신자에게 이메일 초대장 보내기	스마트 연결 알림의 수신자에 대한 이메일 주소를 입력합니다.
이메일 언어	이메일에서 사용된 언어를 지정합니다.
스마트 연결 토큰	모바일 장치 사용자가 XProtect Mobile 서버에 연결하기 위해 사용할 수 있는 고유한 식별자.
스마트 연결에 대한 링크	모바일 장치 사용자가 XProtect Mobile 서버에 연결하기 위해 사용할 수 있는 링크.

서버 상태 탭

XProtect Mobile 서버의 상태 세부 정보를 확인하십시오. 이 세부 정보는 읽기 전용입니다:

이름	설명
서버가 처음 활성 상태가 된 시기	XProtect Mobile 서버가 마지막으로 시작되었을 때의 시간과 날짜를 표시합니다.
CPU 사용량	모바일 서버에서 현재 CPU 사용량을 표시합니다.
외부 대역폭	XProtect Mobile 클라이언트 또는 XProtect Web Client 및 모바일 서버 간에 현재 사용되는 대역폭을 표시합니다.

활성 사용자

현재 XProtect Mobile 서버에 연결된 XProtect Mobile 클라이언트 또는 XProtect Web Client 의 상태 세부 정보를 확인합니다.

이름	설명
사용자 이름	모바일 서버에 연결된 각 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자의 사용자 이름을 표시합니다.
상태	XProtect Mobile 서버와 해당 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자 사이의 현재 관계를 나타냅니다. 가능한 상태: • 연결됨: 클라이언트와 서버가 키와 암호화 자격 증명을 교환할 때의 최초 상태 • 로그인됨: XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자가 XProtect 시스템에 로그인됩니다.
비디오 대역폭 사용량 **(kB/s)**	각 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자에 대하여 현재 개방된 비디오 스트림의 총 대역폭을 표시합니다.
오디오 대역폭 사용량 **(kB/s)**	각 XProtect Web Client 사용자에 대하여 현재 개방된 오디오 스트림의 총 대역폭을 표시합니다.
트랜스코드된 비디오 스트림	현재 각 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자에 개방되어 있으며 트랜스코드된 비디오 스트림의 총 개수를 표시합니다.
직접 비디오 스트림	현재 각 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자에게 개방된 직접 비디오 스트림의 총 개수를 표시합니다(XProtect Expert 및 XProtect Corporate 에 대해서만 가능).
트랜스코드된 오디오 스트림	현재 각 XProtect Web Client 사용자에 대하여 개방되어 있으며 트랜스코드된 오디오 스트림의 총 개수를 표시합니다.

성능 탭

성능 탭에서 XProtect Mobile 서버의 성능에 대해 다음 설정과 제한을 설정할 수 있습니다:

비디오 스트리밍 설정 **(XProtect Expert** 및 **XProtect Corporate** 에 대해서만**)**

이름	설명
직접 스트리밍 활성화	XProtect Web Client 과 XProtect Mobile 클라이언트에서 직접 스트리밍 활성화(XProtect Expert 및 XProtect Corporate 에서만 가능). 이 기능은 기본으로 활성화됩니다.
적응 스트리밍 활성화	XProtect Web Client 및 XProtect Mobile 클라이언트에서 적응 스트리밍을 활성화합니다(XProtect Expert 및 XProtect Corporate 용으로만). 이 기능은 기본으로 활성화됩니다.
스트리밍 모드	적응 스트리밍 기능을 활성화 한 후, 목록에서 다음과 같이 스트리밍 유형을 선택할 수 있습니다: • 비디오 품질 최적화**(**기본**)** - 요청된 해상도값과 동일하거나 높은 값의 사용 가능한 가장 낮은 햇아도의 스트림을 선택합니다. • 서버 성능 최적화 - 요청된 해상도를 줄이고 감소된 요청값과 동일하거나 높은 값의 사용 가능한 가장 낮은 해상도의 스트림을 선택합니다. • 낮은 대역폭에서 해상도 최적화 - 사용 가능한 가장 낮은 해상도의 스트림을 선택합니다(3G 또는 불안정한 네트워크 사용 시 권장).

트랜스코드된 비디오 스트림 제한

수준 **1**

수준 **1**은 XProtect Mobile 서버에 지정된 기본 제한입니다. 여기에서 설정한 제한 사항은 XProtect Mobile 의 트랜스코딩된 비디오 스트림에 항상 적용됩니다.

이름	설명
수준 **1**	XProtect Mobile 서버 성능에 대해 첫 번째 제한 수준을 활성화하려면 확인란을 선택합니다.
최대 **FPS**	XProtect Mobile 서버에서 클라이언트로 전송할 최대 초당 프레임 수(FPS)에 대한 제한

이름	설명
	을 설정합니다.
최대 이미지 해상도	XProtect Mobile 서버에서 클라이언트로 전송할 이미지 해상도의 제한을 설정합니다.

수준 **2**

수준 **1**의 기본값 대신 다른 제한 수준을 적용하려는 경우, 수준 **2** 확인란을 선택합니다. 어떤 설정이든 첫 번째 수준에서 설정한 내용보다 높게 지정할 수 없습니다. 예를 들어 수준 1에서 최대 FPS를 45로 설정한 경우, 수준 2의 최대 FPS는 44 미만으로만 설정할 수 있습니다.

이름	설명
수준 **2**	XProtect Mobile 서버 성능에 대한 두 번째 제한 수준을 활성화하려면 확인란을 선택합니다.
CPU 임계값	시스템이 비디오 스트림 제한을 강제로 시행하기 전에 XProtect Mobile 서버에서 CPU 부하의 임계값을 설정합니다.
대역폭 임계값	시스템이 비디오 스트림 제한을 강제로 시행하기 전에 XProtect Mobile 서버에서 대역폭 부하의 임계값을 설정합니다.
최대 **FPS**	XProtect Mobile 서버에서 클라이언트로 전송할 최대 초당 프레임 수(FPS)에 대한 제한을 설정합니다.
최대 이미지 해상도	XProtect Mobile 서버에서 클라이언트로 전송할 이미지 해상도의 제한을 설정합니다.

수준 **3**

또한 수준 3 확인란을 선택하여 세 번째 제한 수준을 만들 수 있습니다. 어떤 설정이든 수준 **1** 및 수준 **2** 에서 설정한 내용보다 높게 지정할 수 없습니다. 예를 들어 수준 **1** 에서 최대 **FPS** 를 45로, 수준 **2** 에서 32로 설정한 경우, 수준 **3** 에서 최대 **FPS** 는 31 이하로만 설정할 수 있습니다.

이름	설명
수준 **3**	XProtect Mobile 서버 성능에 대해 세 번째 제한 수준을 활성화하려면 확인란을 선택합니다.
CPU 임계값	시스템이 비디오 스트림 제한을 강제로 시행하기 전에 XProtect Mobile 서버에서 CPU 부하의 임계값을 설정합니다.
대역폭 임계값	시스템이 비디오 스트림 제한을 강제로 시행하기 전에 XProtect Mobile 서버에서 대역폭 부하의 임계값을 설정합니다.
최대 **FPS**	XProtect Mobile 서버에서 클라이언트로 전송할 초당 프레임 수(FPS)에 대한 제한을 설정합니다.
최대 이미지 해상도	XProtect Mobile 서버에서 클라이언트로 전송할 이미지 해상도의 제한을 설정합니다.

시스템이 한 수준에서 다른 수준으로 즉시 전환되지 않습니다. CPU 또는 대역폭 임계값이 표시된 수준의 위, 아래로 5% 미만으로 변동하면 현재 수준이 그대로 사용됩니다.

조사 탭

조사 설정

사용자가 XProtect Mobile 클라이언트 또는 XProtect Web Client 을(를) 사용하여 레코딩된 비디오에 액세스하고 사건을 조사하여 비디오 증거물을 준비 및 다운로드하도록 조사를 활성화할 수 있습니다.

이름	설명
조사 활성화	사용자가 조사를 만들도록 이 확인란을 선택합니다.
조사 폴더	비디오 내보내기가 하드 드라이브의 어느 위치에 저장되는지 표시합니다.
조사 폴더의 크기 제한 활성화	이 확인란을 선택하여 조사 폴더의 크기 제한을 설정하며 조사 폴더에 허용되는 최대 용량을 MB 단위로 입력합니다. 기본 크기는 2000MB 입니다.

이름	설명
다른 사용자가 만든 조사 보기	사용자가 자신이 만들지 않는 조사에 액세스할 수 있게 하려면 이 확인란을 선택합니다.
AVI 내보내기에 대한 타임스탬프 포함	AVI 파일이 다운로드된 날짜와 시간을 포함시키려면 이 확인란을 선택합니다.
AVI 내보내기에 사용된 코덱	다운로드를 위한 AVI 패키지를 준비할 때 사용할 압축 형식을 선택합니다. 선택할 수 있는 코덱은 운영 체제에 따라 다를 수 있습니다. 필요한 코덱이 보이지 않으면 XProtect Mobile 서버가 실행 중인 컴퓨터에 해당 코덱을 설치하여 목록에 코덱을 추가할 수 있습니다.
AVI 내보내기에 사용된 오디오 비트	오디오가 비디오 내보내기에 포함되어 있을 때 목록에서 적합한 오디오 비트 전송률을 선택합니다. 기본값은 160000 Hz입니다.
내보내기 실패 시 데이터 유지 또는 삭제**(MKV** 및 **AVI)**	조사에서 다운로드에 적합하게 준비되지 않은 데이터를 유지할지, 아니면 삭제할지 여부를 선택합니다.

조사

이름	설명
조사	지금까지 시스템에 설정된 조사의 목록을 보여줍니다. 더이상 조사를 보관하고 싶지 않은 경우 삭제 또는 모두 삭제 버튼을 사용하십시오. 이 작업은 예를 들어 서버의 가용 디스크 공간을 늘리려는 경우에 유용할 수 있습니다.
세부 정보	조사를 위해 내보낸 개별 비디오 파일을 삭제하되 조사를 유지하려면 목록에서 조사를 선택합니다. 조사 세부 정보 그룹에서 내보내기를 위한 데이터베이스, **AVI** 또는 **MKV** 필드 오른쪽에 있는 삭제 아이콘을 선택합니다.

비디오 푸시 탭

비디오 푸시를 활성화하는 경우, 다음 설정을 지정할 수 있습니다:

이름	설명
비디오 푸시	모바일 서버에서 비디오 푸시를 활성화합니다.
채널 수	XProtect 시스템에서 활성화된 비디오 푸시 채널의 수를 표시합니다.
채널	관련 채널에 대한 채널 번호를 표시합니다. 편집할 수 없습니다.
포트	관련 비디오 푸시 채널에 대한 포트 번호입니다.
MAC 주소	관련 비디오 푸시 채널에 대한 MAC 주소입니다.
사용자 이름	관련 비디오 푸시 채널과 연관된 사용자 이름을 입력하십시오.
카메라 이름	카메라가 확인된 경우 카메라의 이름을 표시합니다.

필요한 모든 단계를 완료했으면(페이지 50의 비디오를 스트리밍하도록 비디오 푸시 설정 참조), 카메라 찾기 를 선택하여 관련 카메라를 검색합니다.

알림 탭

알림 탭을 이용하여 시스템 알림 및 푸시 알림을 설정하거나 해제합니다.

알림을 설정하고 하나 이상의 알람과 이벤트를 구성하면 이벤트 발생 시 XProtect Mobile 이(가) 사용자에게 알림을 보냅니다. 앱이 열려 있으면 모바일 장치의 XProtect Mobile (으)로 알림이 전달됩니다. 푸시 알림은 XProtect Mobile 이(가) 열려 있지 않은 사용자에게 알림을 제공합니다. 이러한 알림은 모바일 장치로 전달됩니다.

자세한 내용은 다음을 참조하십시오. 페이지 48의 특정 모바일 장치 또는 모든 모바일 장치로 푸시 알림 보내기 활성화

다음 표에 이 탭의 설정이 설명되어 있습니다.

이름	설명
알림	알림을 설정하려면 이 확인란을 선택합니다.
장치 등록 관리	이 서버에 연결하는 장치와 사용자에 관한 정보를 저장하려면 이 확인란을 선택합니다. 시스템이 이러한 장치로 알림을 보냅니다. 이 확인란을 선택 취소하면 장치 목록도 삭제됩니다. 사용자가 다시 알림을 수신하려면 이 확인란을 선택하고 사용자가 서버에 장치를 다시 연결해야 합니다.

등록된 장치

이름	설명
활성화됨	장치로 알림을 보내려면 이 확인란을 선택합니다.
장치 이름	이 서버에 연결한 모바일 장치 목록입니다. 활성화됨 확인란을 선택하거나 선택 취소하여 특정 장치로 알림 보내기를 시작 또는 중지할 수 있습니다.
사용자	알림을 받을 사용자의 이름

단계 확인 탭

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 자세한 정보는 https://www.milestonesys.com/solutions/platform/product-index/ 을(를) 참조하십시오.

2단계 확인 탭을 사용하여 다음의 사용자에 대한 추가적인 로그인 단계를 활성화하고 지정합니다:

- XProtect Mobile 앱(iOS 또는 Android 모바일 기기)
- XProtect Web Client

첫 번째 확인 유형은 암호입니다. 두 번째 확인 유형은 이메일을 통해 사용자에게 발송되도록 구성할 수 있는 확인 코드입니다.

자세한 내용은 페이지 53의 2단계 이메일 확인을 위해 사용자 설정을 참조하십시오.

다음 표에 이 탭의 설정이 설명되어 있습니다.

제공자 설정 > 이메일

이름	설명
SMTP 서버	2단계 확인 이메일을 위한 간이 전자 우편 전송 프로토콜(SMTP) 서버의 IP 주소나 호스트 이름을 입력합니다.

이름	설명
SMTP 서버 포트	이메일 발송을 위한 SMTP 서버의 포트를 지정합니다 기본 포트 번호는 25(SSL 제외) 및 465(SSL 사용)입니다.
SSL 사용	SMTP가 SSL 암호화를 지원할 경우 이 확인을 선택합니다.
사용자 이름	SMTP 서버에 로그인할 사용자 이름을 지정합니다.
암호	SMTP 서버에 로그인할 암호를 지정합니다.
Secure Password Authentication(SPA) 사용	SMTP 서버가 SPA를 지원할 경우 이 확인란을 선택합니다.
보내는 사람 이메일 주소	확인 코드를 전송할 이메일 주소를 지정합니다.
이메일 제목	이메일에 대한 제목을 지정합니다. 예: 귀하의 2단계 확인 코드.
이메일 본문	보낼 이메일 메시지를 입력합니다. 예: 귀하의 코드는 {0}입니다. {0} 변수를 포함시키지 않을 경우, 기본으로 본문의 맨 끝에 코드가 추가됩니다.

확인 코드 설정

이름	설명
재연결 시간 제한**(0-30** 분**)**	네트워크가 연결 해제된 경우 XProtect Mobile 클라이언트 사용자가 로그인을 재확인할 필요가 없는 기간을 지정합니다. 기본 기간은 3분입니다. 이 설정은 XProtect Web Client 에는 적용되지 않습니다.
코드 만료 기간**(1-10**분**)**	사용자가 수신된 확인 코드를 사용할 수 있는 기간을 지정합니다. 이 기간 후에 코드를 무효화되며 사용자는 새 코드를 다시 요청해야 합니다. 기본 기간은 5분입니다.
코드 입력 시	제공된 코드가 무효화되기 전에 코드 입력 시도의 최대 횟수를 지정합니다. 기본 횟수는 3

이름	설명
도(1-10회)	회입니다.
코드 길이(4-6자)	코드의 문자 수를 지정합니다. 기본 길이는 6입니다.
코드 합성	시스템이 생성할 코드의 복잡성을 지정합니다. 다음 중 선택할 수 있습니다. • 라틴어 대문자(A-Z) • 라틴어 소문자(a-z) • 숫자(0-9) • 특수문자(!@#...)

사용자 설정

이름	설명
사용자 및 그룹	XProtect 시스템에 추가된 사용자와 그룹을 나열합니다. Active Directory에 하나의 그룹이 구성된 경우, 모바일 서버는 Active Directory에서 이메일 주소와 같은 세부 정보를 사용합니다. Windows 그룹은 2단계 확인을 지원하지 않습니다.
인증 방법	각 사용자나 그룹의 확인 설정을 선택합니다. 다음 중 선택할 수 있습니다. • 로그인 없음: 사용자가 로그인할 수 없습니다 • 2단계 확인 없음: 사용자가 사용자 이름과 암호를 입력해야 합니다 • 이메일: 사용자가 사용자 이름 및 암호 이외에 확인 코드를 입력해야 합니다
사용자 정보	각 사용자가 코드를 받을 이메일 주소를 입력합니다.

직접 스트리밍(설명됨)

XProtect Mobile 은(는) 라이브 모드로 직접 스트리밍을 지원합니다(XProtect Expert 및 XProtect Corporate 에 대해서만).

직접 스트리밍은 최근의 IP 카메라 대부분에서 지원하는 H.264 코덱으로 XProtect 시스템에서 클라이언트에 비디오를 전송하는 비디오 스트리밍 기술입니다. 직접 스트리밍에는 어떤 전환코딩도 필요하지 않으므로 XProtect 시스템상의 부하를 어느 정도 줄여줍니다.

직접 스트리밍 기술은 XProtect 시스템이 카메라에서 사용하는 코덱에서 비디오를 디코딩하여 JPEG 파일로 만들어주는 XProtect 의 전환코딩 설정과는 다릅니다. 이 기능을 활성화하면 카메라와 비디오 스트림의 동일한 구성에 대해 CPU 사용량을 감소해줍니다. 직접 스트리밍은 또한 동일한 하드웨어에 대한 스트리밍 성능을 높여 전환 코딩 대비 최대 5배까지 동시 비디오 스트림을 할 수 있게 해줍니다.

또한 직접 스트리밍 기능을 사용하여 H.265 코덱을 지원하는 카메라에서 XProtect Mobile 클라이언트로 직접 비디오를 전송할 수 있습니다.

Management Client 에서, 클라이언트에 대한 직접 스트리밍을 활성화/비활성화할 수 있습니다(페이지 14의 모바일 서버 설정 참조).

다음과 같은 경우 비디오 스트림은 직접 스트리밍에서 트랜스코딩으로 전환됩니다.

- Management Client 에서 직접 스트리밍 기능이 비활성화되었거나 요건이 충족되지 않았습니다(페이지 11의 직접 스트리밍을 위한 요건 참조).
- 스트리밍 카메라의 코덱은 H.264(모든 클라이언트용) 또는 H.265 (XProtect Mobile 클라이언트 전용)과 다른 것이어야 합니다.
- 해당 비디오는 10초 이상 재생할 수 없습니다.
- 스트리밍 카메라의 프레임 속도는 1초당 **1** 프레임(1FPS)로 설정되어 있습니다.
- 서버 또는 카메라와의 연결이 끊어졌습니다.
- 라이브 비디오를 하는 동안 개인정보 보호 가리기 기능을 사용했습니다.

적응 스트리밍(설명됨)

XProtect Mobile 은(는) 라이브 모드로 적응 스트리밍을 지원합니다 (XProtect Expert 및 XProtect Corporate 에 대해서만).

적응 스트리밍은 동일한 카메라 뷰에서 다중 라이브 비디오 스트림을 볼 때에 유용합니다. 이 기능은 XProtect Mobile 서버의 성능을 최적화해주며 XProtect Mobile 클라이언트와 XProtect Web Client 을(를) 실행하는 장치의 디코딩 능력과 성능을 개선해줍니다.

적응 스트리밍을 이용하려면 카메라가 다른 해상도로 정의된 멀티 스트림을 갖고 있어야 합니다. 이러한 경우, 이 기능으로 다음을 수행할 수 있습니다:

- 비디오 품질 최적화 - 요청된 해상도값과 동일하거나 높은 값의 사용 가능한 가장 낮은 햇아도의 스트림을 선택합니다.
- 서버 성능 최적화 - 요청된 해상도를 줄이고 감소된 요청값과 동일하거나 높은 값의 사용 가능한 가장 낮은 해상도의 스트림을 선택합니다.
- 낮은 대역폭에서 해상도 최적화 - 사용 가능한 가장 낮은 해상도의 스트림을 선택합니다(3G 또는 불안정한 네트워크 사용 시 권장).

줌을 할 때 요청된 라이브 비디오 스트림은 항상 최고 가용 해상도입니다.

대역폭 사용량은 종종 요청된 스트림의 해상도가 감소했을 때 감소합니다. 대역폭 사용량은 또한 정의된 스트림 구성 내 기타 설정에 따릅니다.

Management Client 에서 모바일 서버 설정의 성능 탭 에서 적응 스트리밍을 활성화/비활성화할 수 있으며 해당 기능의 선호하는 스트리밍 모드를 설정할 수 있습니다(페이지 14의 모바일 서버 설정 참조).

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 SSL/TLS 프로토콜을 사용하여 보안 통신을 확보합니다.

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

인증 기관(CA)는 CA 인증서를 사용하여 서버 상의 웹 서비스에 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 SSL/TLS 연결을 수립할 수 있습니다.

TLS에 관한 자세한 정보: https://en.wikipedia.org/wiki/Transport_Layer_Security

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.

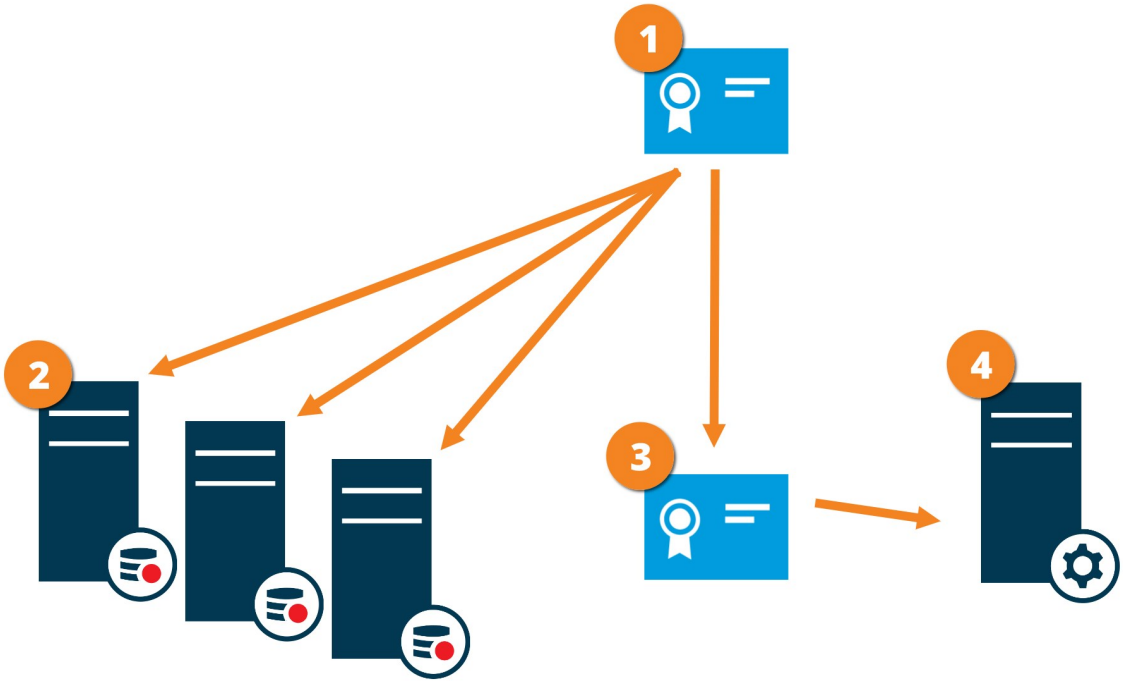
동일한 주체 이름을 가진 인증서로 갱신하고 Windows Certificate Store에 추가할 경우, 해당 서버는 자동으로 새 인증서를 선택합니다. 각 레코딩 서버에 대한 인증서를 다시 선택할 필요 없이 그리고 서비스를 재시작하지 않고도 많은 레코딩 서버에 대해 인증서를 더 쉽게 갱신할 수 있습니다.

관리 서버 암호화(설명됨)

관리 서버와 레코딩 서버 간의 쌍방향 연결을 암호화할 수 있습니다. 관리 서버에서 암호화를 활성화할 때, 관리 서버에 연결된 모든 레코딩 서버로부터의 연결에 적용됩니다. 관리 서버 상의 암호화를 활성화하면 반드시 모든 레코딩 서버의 암호화를 활성화해야 합니다. 암호화를 활성화하기 전 반드시 관리 서버와 모든 레코딩서버에 보안 인증서를 설치해야 합니다.

관리 서버를 위한 인증서 배포

이 그림은 관리 서버로부터 통신을 보호하기 위해 인증서가 XProtect VMS 에서 서명되고 신뢰받고 배포되는 방법에 대한 기본 개념을 보여줍니다.



❶ CA 인증은 신뢰할 수 있는 제자의 역할을 하며, 주체/소유자(관리 서버) 모두에 의해 그리고 인증서를 확인하는 당사자(레코딩 서버)가 신뢰합니다.

❷ CA 인증서는 모든 레코딩 서버에서 신뢰할 수 있어야 합니다. 이 방법으로 레코딩 서버는 CA가 발급한 인증서의 유효성을 확인할 수 있습니다.

❸ CA 인증서는 관리 서버와 레코딩 서버간에 보안 연결을 수립하기 위해 사용합니다.

❹ CA 인증서는 반드시 관리 서버를 실행하는 컴퓨터에 설치되어야 합니다.

개인 관리 서버 인증서를 위한 요구 사항:

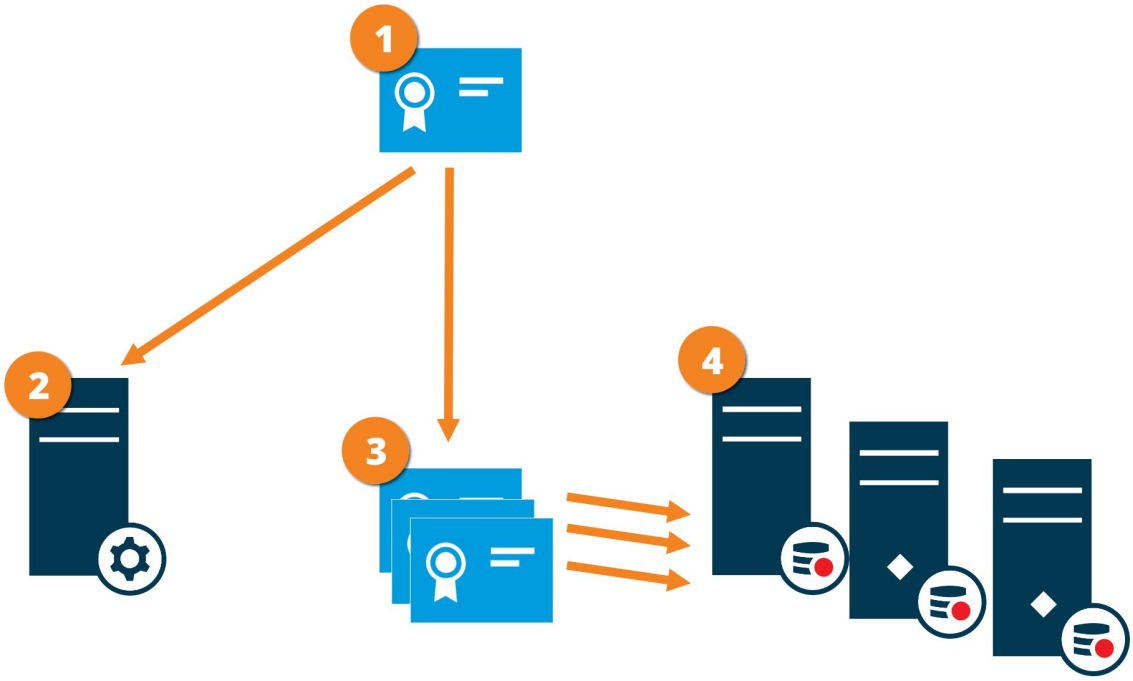
- 관리 서버의 호스트 이름이 인증서에 하나의 주체(소유자) 또는 인증서가 발급되는 DNS 이름의 목록으로서 포함되도록 관리서버에 발급됩니다.
- 관리 서버 인증 발급에 사용된 CA 인증을 신뢰하여 관리 서버 자체를 신뢰
- 관리 서버 인증 발급에 사용된 CA 인증을 신뢰하여 관리 서버에 연결된 모든 레코딩 서버를 신뢰

관리 서버에서 레코딩 서버까지 연결 암호화(설명됨)

관리 서버와 레코딩 서버 간의 쌍방향 연결을 암호화할 수 있습니다. 관리 서버에서 암호화를 활성화할 때, 관리 서버에 연결된 모든 레코딩 서버로부터의 연결에 적용됩니다. 이 통신의 암호화는 반드시 관리 서버의 암호화 설정을 따라야 합니다. 그러므로 관리 서버 암호화가 활성화되어 있으면 이는 레코딩 서버에서도 활성화되어 있으며 그 반대도 동일합니다. 암호화를 활성화하기 전 반드시 장애 조치 레코딩 서버를 비롯하여 관리 서버와 모든 레코딩 서버에 보안 인증서를 설치해야 합니다.

인증서 배포

이 그림은 관리 서버로부터 통신을 보호하기 위해 인증서가 XProtect VMS 에서 서명되고 신뢰받고 배포되는 방법에 대한 기본 개념을 보여줍니다.



❶ CA 인증은 신뢰할 수 있는 제3자의 역할을 하며, 주체/소유자(레코딩 서버) 모두가 그리고 인증서를 확인하는 당사자(관리 서버)가 신뢰합니다.

❷ CA 인증서는 관리 서버에서 신뢰할 수 있어야 합니다. 이 방법으로 관리 서버가 CA가 발행한 인증서의 유효성을 확인합니다.

❸ CA 인증서는 관리 서버와 레코딩 서버 간에 보안 연결을 수립하기 위해 사용합니다.

❹ CA 인증서는 반드시 레코딩 서버를 실행하는 컴퓨터에 설치되어야 합니다.

개인 레코딩 서버 인증서에 대한 요구 사항:

- 레코딩 서버의 호스트 이름이 하나의 주체(소유자)로서 인증서의 이름에 포함되도록 또는 인증서가 발행된 DNS 이름의 목록에 포함되도록 레코딩 서버에 발급됩니다.
- 레코딩 서버 인증 발급에 사용된 CA 인증을 신뢰하여 관리 서버를 신뢰

관리 서버와 Data Collector Server 간의 암호화(설명됨)

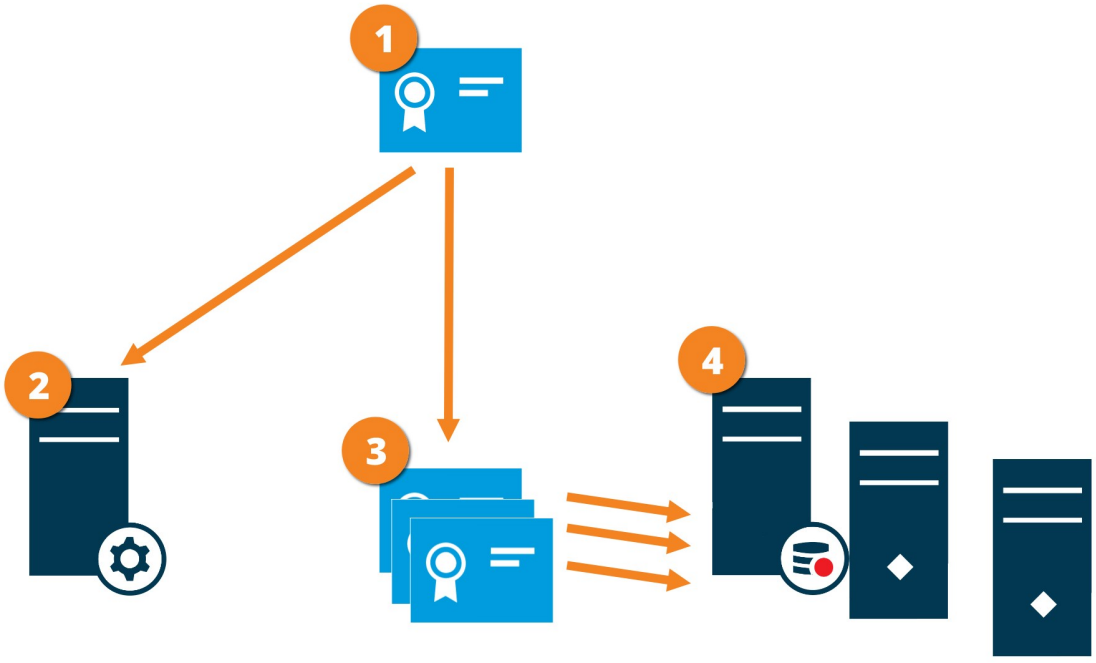
다음과 같은 유형의 원격 서버가 있는 경우 관리 서버 및 관련된 Data Collector 간의 쌍방향 연결을 암호화할 수 있습니다.

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

관리 서버에서 암호화를 활성화할 때, 관리 서버에 연결된 모든 Data Collector 서버로부터의 연결에 적용됩니다. 이 통신의 암호화는 반드시 관리 서버의 암호화 설정을 따라야 합니다. 그러므로 관리 서버 암호화가 활성화되어 있으면 원격 서버와 관련된 Data Collector 서버에서도 활성화되어 있어야 하며 그 반대도 동일합니다. 암호화를 활성화하기 전 반드시 관리 서버 및 원격 서버와 관련된 모든 Data Collector 서버에 보안 인증서를 설치해야 합니다.

인증서 배포

이 그림은 관리 서버로부터 통신을 보호하기 위해 인증서가 XProtect VMS 에서 서명되고 신뢰받고 배포되는 방법에 대한 기본 개념을 보여줍니다.



❶ CA 인증서는 신뢰할 수 있는 제3자의 역할을 하며, 주체/소유자(데이터 수집기 서버) 모두가 그리고 인증서를 확인하는 당사자(관리 서버)가 신뢰합니다.

❷ CA 인증서는 관리 서버에서 신뢰할 수 있어야 합니다. 이 방법으로 관리 서버가 CA가 발행한 인증서의 유효성을 확인합니다.

❸ CA 인증서는 데이터 수집기 서버와 관리 서버 간에 보안 연결을 수립하기 위해 사용합니다.

❹ CA 인증서는 반드시 데이터 수집기 서버를 실행하는 컴퓨터에 설치되어야 합니다.

개인 데이터 수집기 서버 인증서에 대한 요구 사항:

- 데이터 수집기 서버의 호스트 이름이 주체(소유자)로서 인증서에 포함되도록 또는 인증서가 발급된 DNS 이름의 목록에 포함되도록 데이터 수집기 서버에 발급될 것
- 데이터 수집기 서버 인증 발급에 사용된 CA 인증을 신뢰하여 관리 서버를 신뢰

레코딩 서버로부터 데이터를 검색하는 클라이언트와 서버 암호화(설명됨)

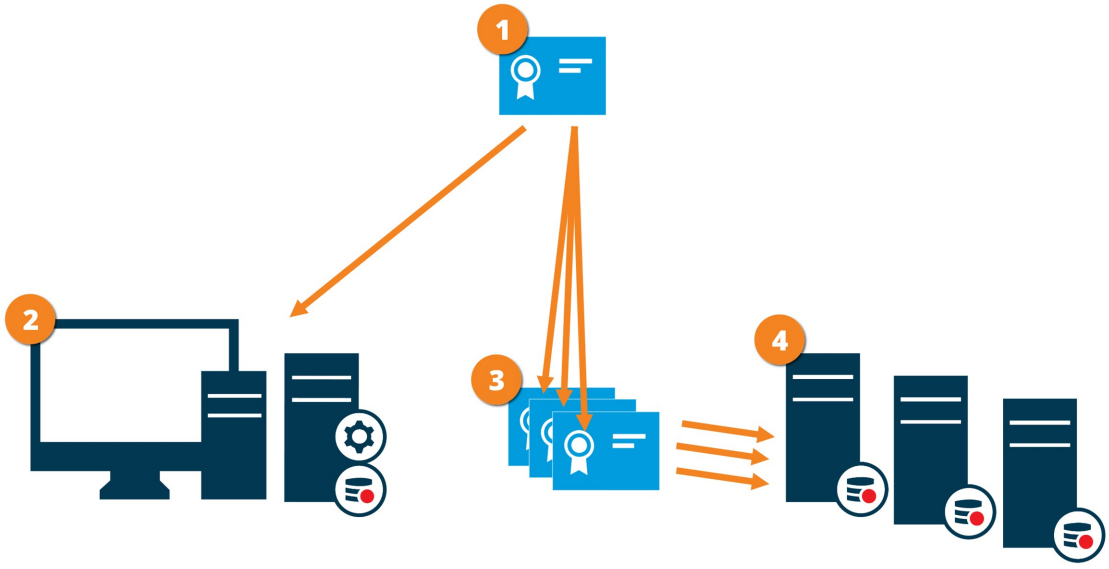
레코딩 서버에서 암호화를 활성화할 때, 모든 클라이언트, 서버 및 레코딩 서버로부터 데이터 스트림을 검색하는 통합에 대한 통신을 보호할 수 있습니다. 이 문서에서 '클라이언트로' 지칭됨:

- XProtect Smart Client
- Management Client
- Management Server (시스템 모니터에 대해 그리고 전자메일 통보의 이미지 및 AVI 비디오 클립에 대해)
- XProtect Mobile 서버
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Milestone Interconnect 을(를) 통해 레코딩 서버로부터 데이터 스트림을 검색하는 사이트
- 일부 타사 MIP SDK 통합

> ⚠ 레코딩 서버에 액세스하는 MIP SDK 2018 R3 또는 그 이전 버전으로 빌드된 솔루션에 대해: MIP SDK 라이브러리를 사용하여 통합하는 경우, MIP SDK 2019 R1을 리빌드해야 합니다. 만일 통합이 MIP SDK 라이브러리를 사용하지 않고 Recording Server API와 직접 통신하는 경우 통합자는 직접 HTTPS 지원을 추가해야 합니다.

인증서 배포

이 그림은 레코딩 서버로의 통신을 보호하기 위해 인증서가 XProtect VMS 에서 서명되고 신뢰받고 배포되는 방법에 대한 기본 개념을 보여줍니다.



❶ CA는 신뢰할 수 있는 제3자의 역할을 하며, 주체/소유자(레코딩 서버) 모두가 그리고 인증서를 확인하는 당사자(클라이언트)가 신뢰합니다.

❷ CA 인증서는 모든 클라이언트 컴퓨터에서 신뢰할 수 있어야 합니다. 이 방법으로 클라이언트는 CA가 발급한 인증서의 유효성을 확인할 수 있습니다.

❸ CA 인증서는 레코딩 서버와 모든 클라이언트 및 서비스 간에 보안 연결을 수립하기 위해 사용합니다.

❹ CA 인증서는 반드시 레코딩 서버를 실행하는 컴퓨터에 설치되어야 합니다.

개인 레코딩 서버 인증서에 대한 요구 사항:

- 레코딩 서버의 호스트 이름이 하나의 주체(소유자)로서 인증서의 이름에 포함되도록 또는 인증서가 발행된 DNS 이름의 목록에 포함되도록 레코딩 서버에 발급됩니다.
- 레코딩 서버 인증 발급에 사용된 CA 인증을 신뢰하여 레코딩 서버로부터 데이터 스트림을 검색하는 서비스를 구동하는 모든 컴퓨터를 신뢰
- 레코딩 서버를 실행하는 서비스 계정은 레코딩 서버에서 인증서의 개인 키에 액세스 권한을 가져야 합니다.

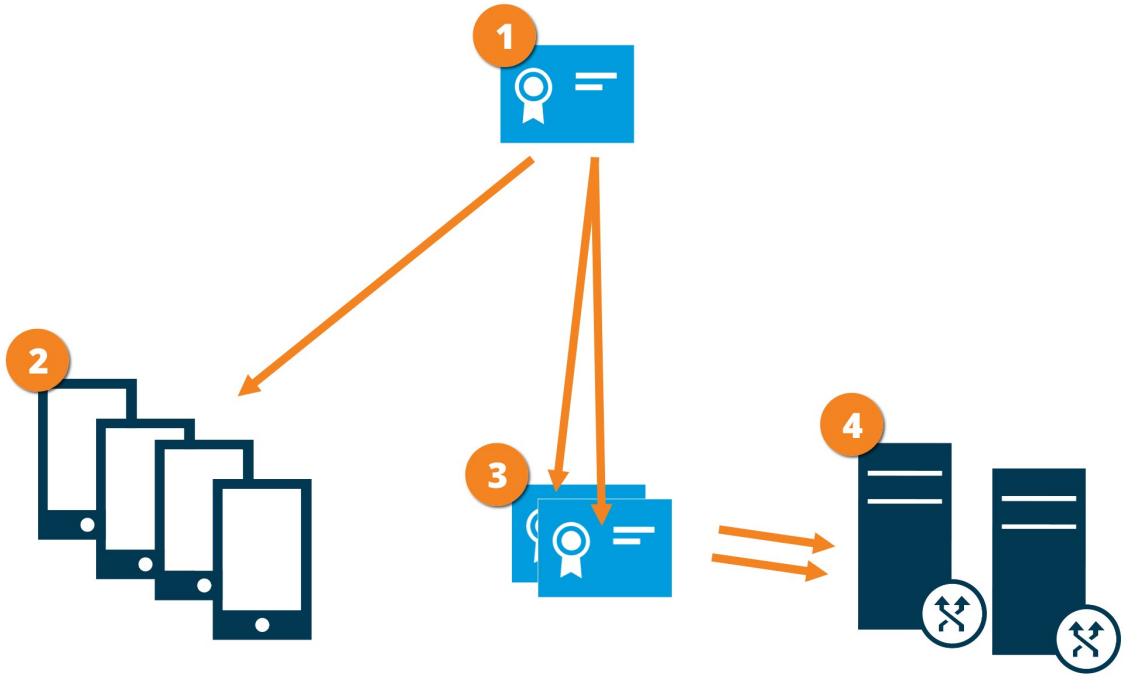
장애 조치 레코딩 서버에 적용되는 레코딩 서버와 시스템 상의 암호화를 활성화하는 경우 Milestone 에서는 장애 조치 레코딩 서버도 암호화를 사용하도록 준비할 것을 권장합니다.

모바일 서버 데이터 암호화(설명됨)

XProtect VMS 에서 암호화는 모바일 서버별로 활성화/비활성화됩니다. 모바일 서버에서 암호화를 활성화할 때, 모든 클라이언트, 서비스 및 데이터 스트림을 검색하는 통합에 대한 암호화된 통신을 사용하는 옵션을 얻게 됩니다.

모바일 서버를 위한 인증서 배포

이 그림은 모바일 서버로부터 통신을 보호하기 위해 인증서가 XProtect VMS 에서 서명되고 신뢰받고 배포되는 방법에 대한 기본 개념을 보여줍니다.



❶CA는 신뢰할 수 있는 제자의 역할을 하며, 주체/소유자(모바일 서버)모두에 의해 그리고 인증서를 확인하는 당사자(모든 클라이언트)가 신뢰합니다.

❷CA 인증서는 모든 클라이언트 컴퓨터에서 신뢰할 수 있어야 합니다. 이 방법으로 클라이언트는 CA가 발행한 인증서의 유효성을 확인합니다.

❸CA 인증서는 모바일 서버와 클라이언트 및 서비스 간에 보안 연결을 수립하기 위해 사용합니다.

❹CA 인증서는 반드시 모바일 서버를 실행하는 컴퓨터에 설치되어야 합니다

CA 인증서에 대한 요구사항**:**

- 모바일 서버의 호스트 이름은 하나의 주체/소유자로서 또는 인증서가 발행된 DNS 이름의 목록으로서 인증서에 반드시 포함되어야 합니다.
- 모바일 서버로부터 데이터 스트림을 검색하는 서비스를 실행 중인 모든 컴퓨터에서 인증서는 반드시 신뢰되어야 합니다.
- 레코딩 서버를 실행하는 서비스 계정은 CA 인증서의 개인 키에 액세스 권한을 가져야 합니다.

클라이언트를 위한 모바일 서버 암호화 요건

암호화를 활성화하지 않고 HTTP 연결을 사용하는 경우 XProtect Web Client 의 푸시 투 톡 기능은 사용할 수 없게 됩니다.

암호화 활성화

서버 그룹에 대한 암호화를 구성할 때에는 동일한 CA 인증서에 포함된 인증서로 활성화하거나, 비활성화된 경우라면 서버 그룹 내 모든 컴퓨터를 비활성화해야 합니다.

관리 서버로 및 관리서버로부터 암호화 활성화

관리 서버와 레코딩 서버 또는 기타 데이터 수집기가 있는 원격 서버 간의 쌍방향 연결을 암호화할 수 있습니다(Event Server , Log Server , LPR Server 및 Mobile Server).

시스템에 다수의 레코딩 서버 또는 원격 서버가 포함된 경우 반드시 포함된 모든 서버에 대해 암호화를 활성화해야 합니다. 자세한 정보는 페이지 30의 관리 서버 암호화(설명됨)을 참조하십시오.

전제 조건:

- 서버 인증 인증서는 관리 서버를 호스트하는 컴퓨터에서 신뢰된 것이어야 합니다.

우선 관리 서버상의 암호화를 활성화합니다.

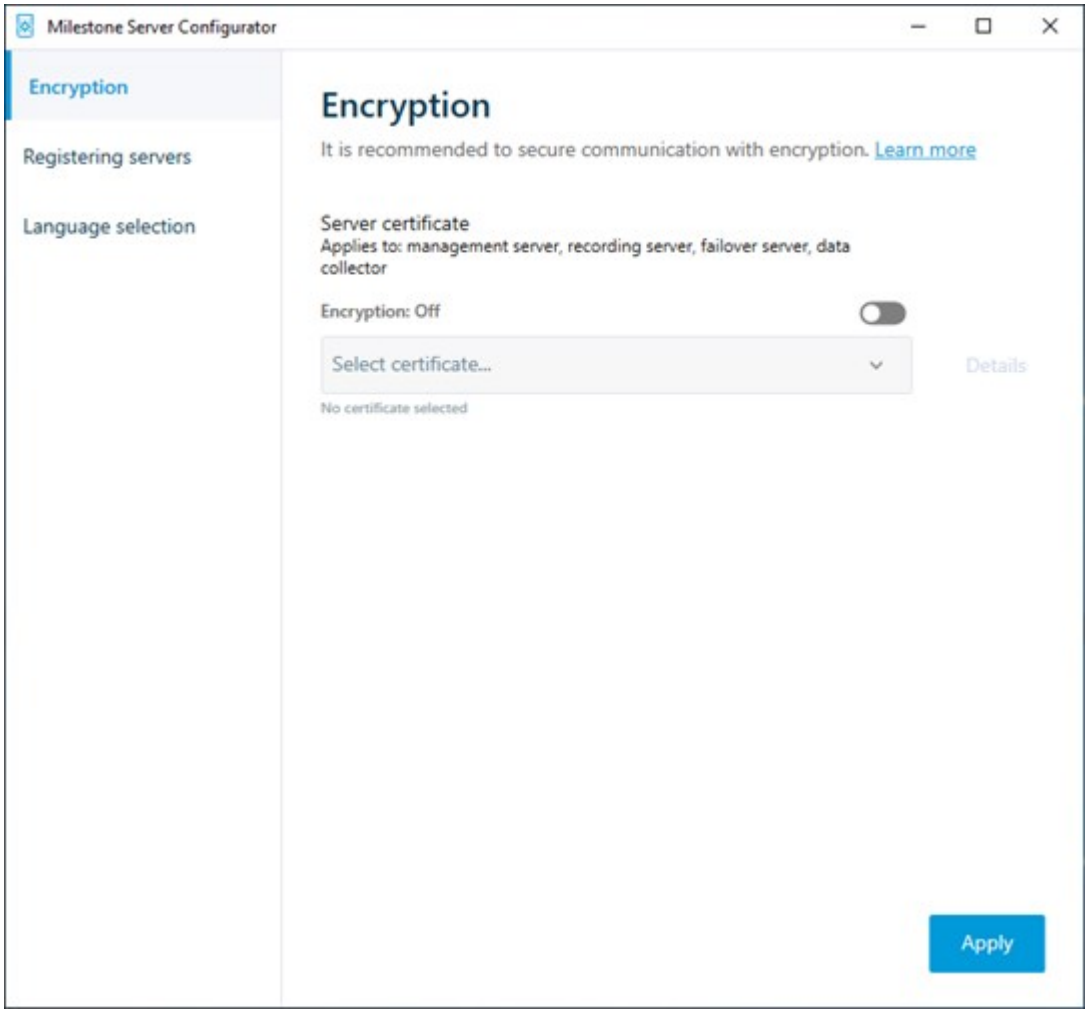
단계:

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 Store상에 설치되어 있는 인증서의 고유한 주체 이름 목록을 열려면 인증서 선택 을 클릭합니다.
4. 레코딩 서버, 관리 서버, 장애 조치 서버 및 데이터 수집기 서버 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 데이터 수집기가 설치된 각 서버상의 암호화 설정을 업데이트하는 것입니다(Event Server , Log Server , LPR Server 및 Mobile Server).

자세한 내용은 페이지 38의 레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화를 참조하십시오.

레코딩 서버 또는 원격 서버에 대한 서버 암호화 활성화

관리 서버와 레코딩 서버 또는 기타 데이터 수집기가 있는 원격 서버 간의 쌍방향 연결을 암호화할 수 있습니다(Event Server , Log Server , LPR Server 및 Mobile Server).

시스템에 다수의 레코딩 서버 또는 원격 서버가 포함된 경우 반드시 포함된 모든 서버에 대해 암호화를 활성화해야 합니다. 자세한 정보는 페이지 31의 관리 서버에서 레코딩 서버까지 연결 암호화(설명됨) 및 페이지 32의 관리 서버와 Data Collector Server 간의 암호화(설명됨)을 참조하십시오.

전제 조건:

- 관리 서버 상의 암호화 기능을 활성화했습니다. 페이지 37의 암호화 활성화를 참조하십시오.

단계:

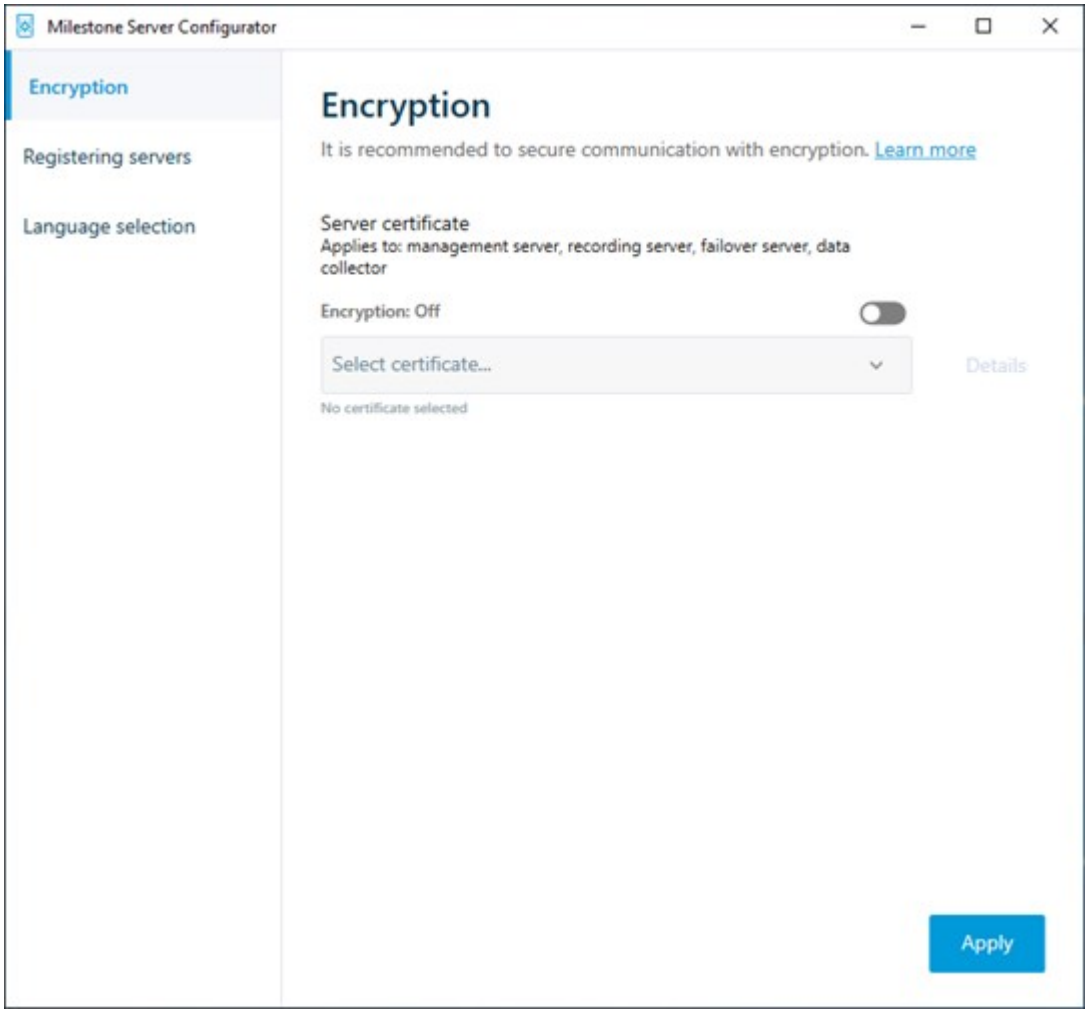
1. 레코딩 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   또는

   - Recording Server Manager (컴퓨터 작업 표시줄에서 Recording Server Manager 아이콘 우클릭)
2. **Server Configurator** 의 서버 인증 아래에서 암호화 를 켭니다.
3. 개인 키를 가졌으며 Windows Certificate Store상에 설치되어 있는 인증서의 고유한 주체 이름 목록을 열려면 인증서 선택 을 클릭합니다.
4. 레코딩 서버, 관리 서버, 장애 조치 서버 및 데이터 수집기 서버 간의 통신을 암호화하는 데 사용할 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.



2. 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.

클라이언트 및 서비스에 암호화 활성화

레코딩 서버로부터 데이트를 스트리밍하는 클라이언트와 서버에 레코딩 서버로부터 연결을 암호화할 수 있습니다. 자세한 정보는 페이지 34의 레코딩 서버로부터 데이터를 검색하는 클라이언트와 서버 암호화(설명됨)을 참조하시기 바랍니다.

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:

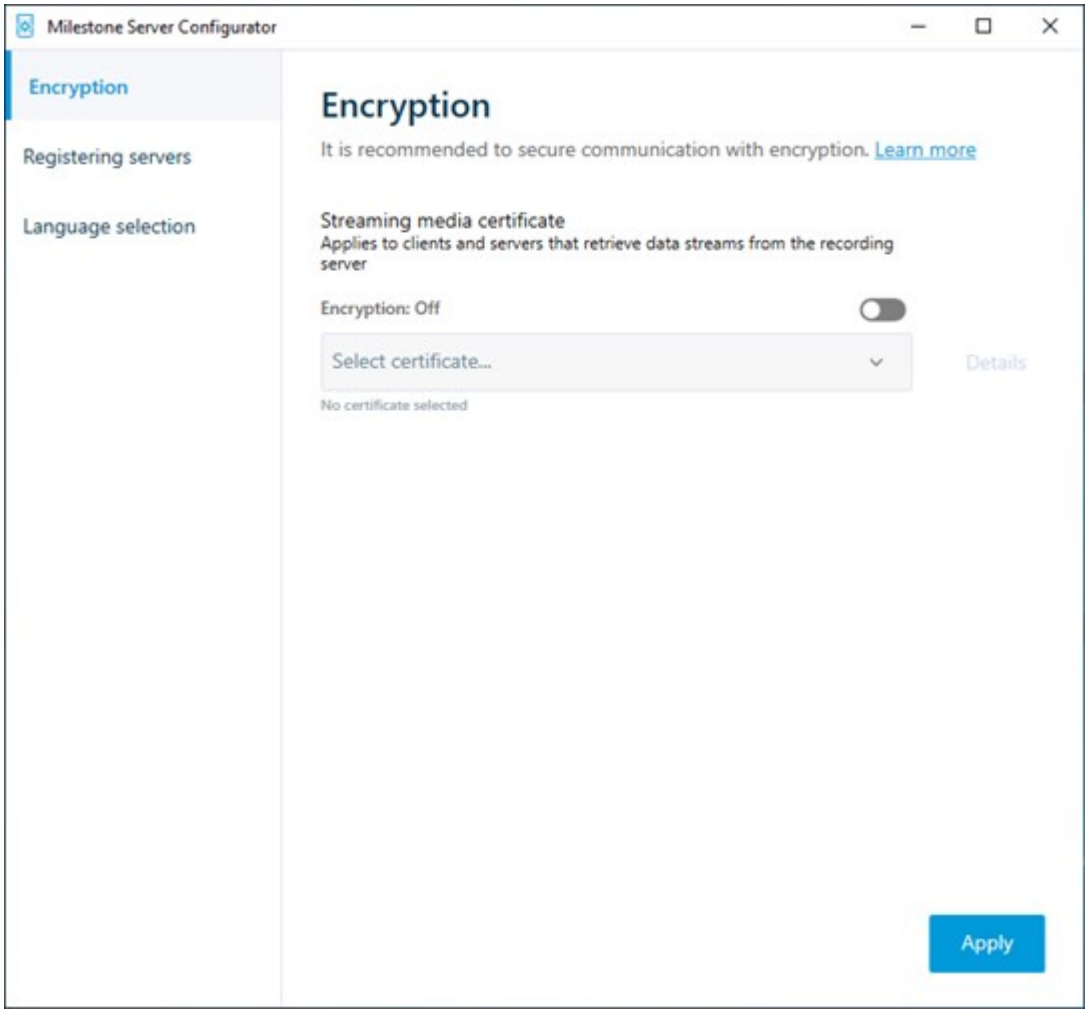
1. 레코딩 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   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 Store상에 설치되어 있는 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.



2. 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 확인해줍니다. 자세한 정보는 페이지 35의 모바일 서버 데이터 암호화(설명됨)과 페이지 37의 클라이언트를 위한 모방리 서버 암호화 요건을 참조하십시오.

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:

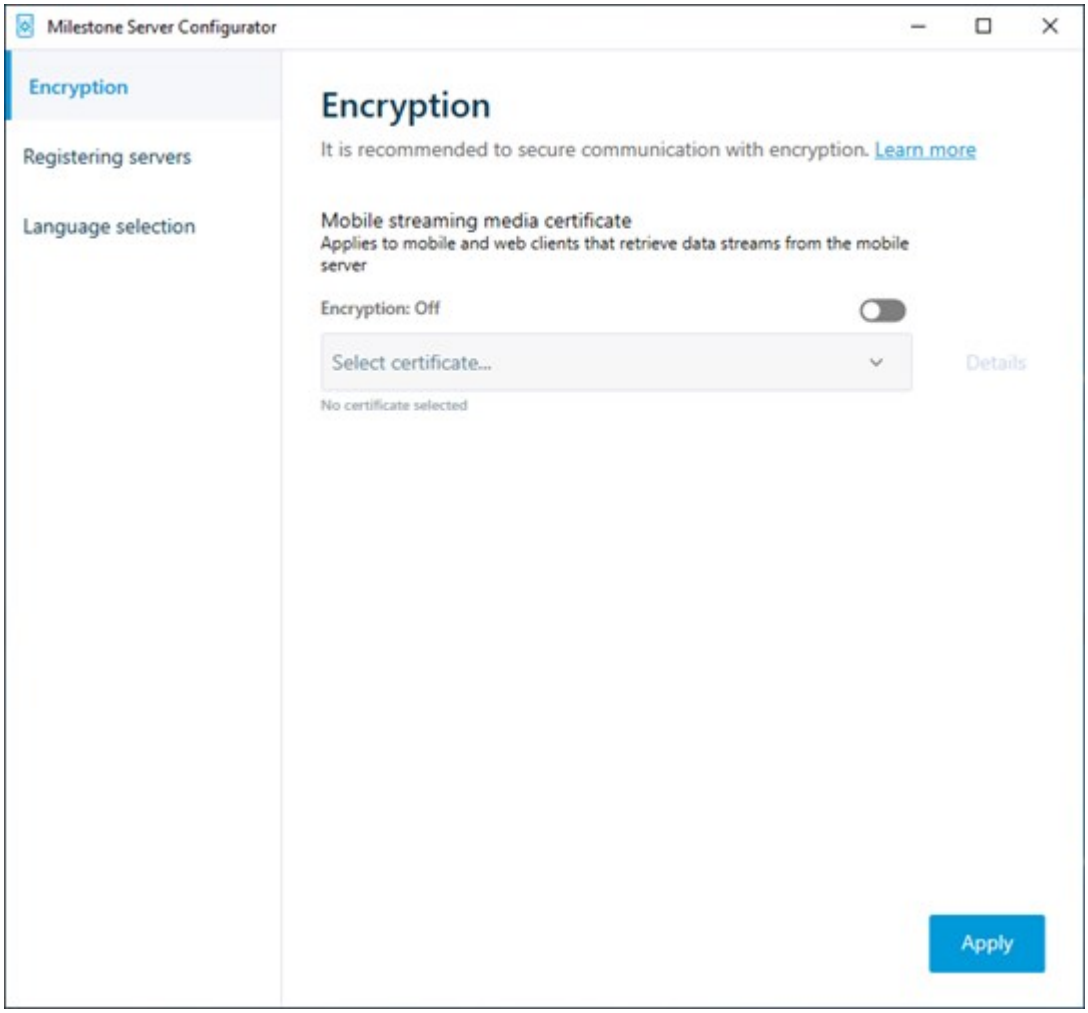
1. 모바일 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   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. Windows개인 키를 가졌으며 Certificate Store상에 설치되어 있는 인증서의 고유한 주체 이름 목록을 열려면 인증서 선택 을 클릭합니다.
4. 인증서를선택하여XProtectMobile클라이언트와모바일서버의XProtectWebClient간통신을암호화합니다.

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 신뢰될 필요가 있습니다.



2. 적용하기 를 클릭합니다.

인증서 적용 시 Mobile Server 서비스가 다시 시작됩니다.

Milestone Federated Architecture 및 마스터/슬레이브 서버(설명됨)

해당 시스템이 마스터/슬레이브 설정에서 Milestone Federated Architecture 또는 서버를 지원하는 경우, XProtect Mobile 클라이언트 또는 XProtect Web Client 에서 이러한 서버에 액세스할 수 있습니다. 이 기능을 이용하면 마스터 서버에 로그인하여 모든 슬레이브 서버의 모든 카메라에 액세스할 수 있습니다.

Milestone Federated Architecture 설정이 구성되었을 때는 중앙 사이트를 통해 하위 사이트에 액세스할 수 있습니다. XProtect Mobile 서버는 중앙 사이트에만 설치합니다.

즉 XProtect Mobile 클라이언트 또는 XProtect Web Client 사용자가 해당 시스템에 있는 모든 서버의 카메라를 보기 위해 하나의 서버에 로그인할 때 마스터 서버의 IP 주소에 연결해야 합니다. 사용자에게 시스템의 모든 서버에 대한 관리자 권한이 있어야 XProtect Mobile 클라이언트 또는 XProtect Web Client 에 카메라가 표시됩니다.

스마트 연결(설명됨)

스마트 연결을 이용하면 모바일 장치나 태블릿에 로그인하여 검증할 필요 없이 XProtect Mobile 을(를) 올바르게 구성했는지 확인할 수 있습니다. 또한 XProtect Mobile 클라이언트 및 XProtect Web Client 사용자의 연결 프로세스를 단순화시킵니다.

이 기능을 이용하려면 XProtect Mobile 서버가 공용 IP 주소를 사용해야 하며, 시스템이 Milestone Care Plus 구독 패키지 라이선스를 받아야 합니다.

이 시스템은 원격 연결 설정이 성공적으로 이루어지고 인터넷에서 XProtect Mobile 서버에 액세스할 수 있는 경우 Management Client 에서 즉각적인 피드백을 제공합니다.

스마트 연결을 이용하면 XProtect Mobile 서버가 내부와 외부 IP 주소 사이에 매끄럽게 전환할 수 있고 어느 위치에서나 XProtect Mobile 에 연결할 수 있습니다.

고객의 모바일 클라이언트를 더 간편하게 설치할 수 있도록 Management Client 안에서 최종 사용자에게 직접 이메일을 보낼 수 있습니다. 이메일에는 XProtect Mobile (으)로 직접 서버를 추가하는 링크가 포함됩니다. 이 링크를 통해 네트워크 주소나 포트를 입력할 필요 없이 설정을 완료합니다.

스마트 연결 설정

스마트 연결 기능을 설정하려면 다음을 수행하십시오.

1. Management Client 의 탐색 창에서 서버 를 확장하고 모바일 서버 를 선택합니다.
2. 모바일 서버를 선택하고 연결 탭을 클릭합니다.
3. 라우터에서 범용 플러그 앤 플레이 검색 기능을 활성화합니다.
4. 연결 설정을 구성합니다.
5. 사용자에게 이메일 메시지를 보냅니다.
6. 복잡한 네트워크에서 연결을 활성화합니다.

라우터에서 범용 플러그 앤 플레이 검색 기능 활성화

XProtect Mobile 서버에 모바일 장치를 쉽게 연결하기 위해 라우터에서 범용 플러그 앤 플레이(UPnP)를 활성화할 수 있습니다. UPnP를 사용하면 XProtect Mobile 서버가 포트 전달을 자동으로 구성할 수 있습니다. 그러나, 웹 인터페이스를 이용하여 라우터에서 포트 전달을 수동으로 설정할 수도 있습니다. 라우터에 따라 포트 매핑을 설정하는 프로세스는 다를 수 있습니다. 해당 라우터에서 포트 전달 설정 방법을 잘 모르겠으면 해당 장치의 설명서를 참조하십시오.

XProtect Mobile 서버 서비스가 5분마다 사용자가 인터넷에서 서버를 사용할 수 있는지 확인합니다. 속성 창 상단 왼쪽 구석에 상태가 표시됩니다: Server accessible through internet: .

복잡한 네트워크에서 연결 활성화

사용자정의설정을사용하는복잡한네트워크환경에서는연결을위해사용자에게필요한정보를보낼수있습니다.

연결 탭에 인터넷 액세스 그룹에서 다음을 지정합니다.

- 특정 연결에 대한 직접 연결을 위해 UPnP 포트 매핑을 사용하는 경우, 사용자 정의 인터넷 액세스 구성 확인란을 선택합니다. 그런 다음 **IP** 주소나 호스트 이름 그리고 연결에 사용할 포트를 제공합니다. 예를 들어, 라우터가 UPnP를 지원하지 않거나 라우터 체인을 사용하는 경우에 이렇게 해야 할 수 있습니다
- IP 주소를 자주 변경하는 경우, **IP** 주소 동적 검색을 위해 선택 확인란을 선택합니다

연결 설정 구성

1. Management Client 의 탐색 창에서 서버 를 확장하고 모바일 서버 를 선택합니다.
2. 서버를 선택하고 연결 탭을 클릭합니다.
3. 일반 그룹의 옵션을 사용하여 다음 내용을 지정합니다:
   - XProtect Mobile 클라이언트와 XProtect Web Client 사용자가 XProtect Mobile 서버에 쉽게 연결하도록 하려면, 스마트 연결 활성화 확인란을 선택합니다.
   - XProtect Mobile 클라이언트 및 XProtect Web Client 이(가) 모바일 서버에 자신이 실행 중임을 나타내어야 하는 빈도에 대한 시간 프레임을 설정합니다.
   - UPNp 프로토콜을 사용하여 네트워크에서 XProtect Mobile 서버를 검색할 수 있도록 하려면, **UPNp** 검색 기능 활성화 확인란을 선택합니다
   - 라우터가 구성되어 있는 경우, XProtect Mobile 서버가 스스로 포트 매핑을 수행하도록 활성화하려면 자동 포트 매핑 사용 확인란을 선택합니다

사용자에게 이메일 메시지 보내기

XProtect Mobile 클라이언트 및 XProtect Web Client 을(를) 더 간편하게 설정할 수 있도록 Management Client 에서 최종 사용자에게 직접 이메일을 보낼 수 있습니다. 이메일에는 XProtect Mobile (으)로 직접 서버를 추가하는 링크가 포함됩니다. 이 링크를 통해 네트워크 주소나 포트를 입력할 필요 없이 설정을 완료합니다.

1. 이메일 초대장 보내기 필드에서 스마트 연결 알림 수신자의 이메일 주소를 입력한 다음 언어를 지정합니다.
2. 그리고 다음 중 하나를 수행합니다:
   - 메시지를 보내려면 보내기 를 클릭합니다
   - 정보를 사용하는 메시징 프로그램에 복사합니다

자세한 내용은 다음을 참조하십시오.

페이지 11의 스마트 연결 설정 요구사항

페이지 16의 연결성 탭

알림 전송(설명됨)

알람이 트리거되거나 장치나 서버에 문제가 발생하는 등의 이벤트가 발생할 때 XProtect Mobile 에서 사용자에게 알림을 보내도록 지정할 수 있습니다. 알림은 앱이 실행 중이든 아니든 항상 전달됩니다. 모바일 장치에서 XProtect Mobile 이(가) 열려 있는 경우, 앱이 알림을 제공합니다. 또한 앱이 실행되고 있지 않더라도 시스템 알림이 전송됩니다. 사용자가 수신하려는 알림의 종류를 지정할 수 있습니다. 예를 들어, 사용자는 다음에 대한 알림 수신을 선택할 수 있습니다.

- 모든 알람
- 사용자에게 할당된 알람만
- 시스템에 관련된 알람만

  서버가 오프라인으로 전환되거나 다시 온라인 전환되는 경우가 이에 해당될 수 있습니다.

XProtect Mobile 이(가) 열려 있지 않은 사용자에게 알림을 보내기 위해 푸시 알림을 이용할 수도 있습니다. 이 방식을 푸시 알림이라고 합니다. 푸시 알림은 모바일 장치로 전달되며 이동 중인 사용자에게 지속적으로 정보를 제공하기에 좋은 방법입니다.

푸시 알림 사용

> 푸시 알림을 사용하려면 시스템이 인터넷에 액세스할 수 있어야 합니다.

푸시 알림에는 Apple, Microsoft 및 Google의 클라우드 서비스가 이용됩니다:

- Apple Push Notification(APN) 서비스
- Microsoft Azure Notification 허브
- Google Cloud Messaging Push Notification 서비스

일정 기간 동안 시스템에서 보낼 수 있는 알림 수에는 제한이 있습니다. 시스템이 이 제한을 초과하면 다음 기간 동안 15분마다 하나의 알림만 보낼 수 있습니다. 알림에는 15분 동안 발생한 이벤트의 요약 정보가 포함됩니다. 다음 기간이 경과하면 제한이 해제됩니다.

또한 페이지 10의 알림 설정 요구사항 및 페이지 24의 알림 탭을 참조하십시오.

XProtect Mobile 서버에서 푸시 알림 설정

푸시 알림을 설정하려면 다음 단계를 따릅니다.

1. Management Client 에서 모바일 서버를 선택한 다음 알림 탭을 클릭합니다.
2. 서버에 연결하는 모든 모바일 장치로 알림을 보내려면 알림 확인란을 선택합니다.
3. 서버에 연결하는 사용자 및 모바일 장치에 관한 정보를 저장하려면 장치 등록 관리 확인란을 선택합니다.

서버는 이 목록에 있는 모바일 장치로만 알림을 보냅니다. 장치 등록 관리 확인란의 선택을 취소하고 변경 내용을 저장하면 시스템이 목록을 삭제합니다. 푸시 알림을 다시 수신하려면 사용자가 장치를 다시 연결해야 합니다.

특정 모바일 장치 또는 모든 모바일 장치로 푸시 알림 보내기 활성화

XProtect Mobile 을(를) 활성화하려면 이벤트가 발생할 경우 특정 또는 모든 모바일 장치에 푸시 알림을 전송하여 사용자에게 알립니다.

1. Management Client 에서 모바일 서버를 선택한 다음 알림 탭을 클릭합니다.
2. 다음 중 하나를 수행하십시오.
   - 개별 장치의 경우, 등록된 장치 표에 나열된 각 모바일 장치에 대해 활성화됨 확인란을 선택합니다
   - 모든 모바일 장치에 대해 알림 확인란을 선택합니다

특정 모바일 장치 또는 모든 모바일 장치로 푸시 알림 보내기 중단

특정 모바일 장치 또는 모든 모바일 장치로 푸시 알림 보내기를 중단하는 방법에는 여러 가지가 있습니다.

1. Management Client 에서 모바일 서버를 선택한 다음 알림 탭을 클릭합니다.
2. 다음 중 하나를 수행하십시오.
   - 개별 장치에 대해 각 모바일 장치의 활성화됨 확인란 선택을 취소합니다. 사용자는 다른 장치를 이용하여 XProtect Mobile 서버에 연결할 수 있습니다.
   - 모든 장치에 대해 알림 확인란 선택을 취소합니다.

모든 장치에 대해 일시적으로 중단하려면 장치 등록 관리 확인란 선택을 취소한 다음 변경 내용을 저장하십시오. 사용자가 다시 연결하면 시스템에서 알림을 다시 보냅니다.

조사 설정

사용자가 XProtect Web Client 및 XProtect Mobile 을(를) 사용하여 레코딩된 비디오에 액세스하고 사건을 조사하여 비디오 증거를 준비 및 다운로드할 수 있도록 조사를 설정합니다.

조사를 설정하려면 다음 단계를 따릅니다.

1. Management Client 에서 모바일 서버를 클릭한 다음 조사 탭을 클릭합니다.
2. 조사 활성화 확인란을 선택합니다. 기본적으로 확인란이 선택됩니다.
3. 조사 폴더 필드에서 조사를 위해 비디오를 저장할 위치를 지정합니다.
4. 조사 폴더 크기 제한 활성화 확인란을 선택하여 조사 폴더에 허용되는 최대 용량을 MB 단위로 설정합니다.
5. 선택 사항: 사용자가 다른 사용자들이 만든 조사에 액세스할 수 있게 하려면 다른 사용자가 만든 조사 보기 확인란을 선택합니다. 이 확인란을 선택하지 않으면 사용자가 자신의 조사만 볼 수 있습니다.

6. 선택 사항: 비디오가 다운로드된 날짜와 시간을 포함시키려면 AVI 내보내기에 대한 타임스탬프 포함 확인란을 선택합니다.
7. **AVI** 내보내기에 사용된 코덱 필드에서 다운로드할 AVI 패키지를 준비할 때 사용할 압축 형식을 선택합니다.

   이 목록의 코덱은 운영 체제에 따라 다를 수 있습니다. 사용하려는 코덱이 보이지 않을 경우 Management Client 이(가) 실행 중인 컴퓨터에 해당 코덱을 설치하면 이 목록에 표시됩니다.

   또한, 코덱에 사용되는 압축 비율도 서로 다를 수 있어 비디오 품질에 영향을 미칠 수 있습니다. 압축 비율이 높으면 저장 공간이 줄어들지만 동시에 품질이 떨어질 수 있습니다. 압축 비율이 낮으면 필요한 저장 공간과 네트워크 용량이 많아지지만 품질은 향상될 수 있습니다. 코덱에 대해 충분히 알아본 후에 선택하는 것이 좋습니다.

8. **AVI** 내보내기에 사용된 오디오 비트 전송률 목록에서 오디오가 비디오 내보내기에 포함되어 있을 때 적합한 오디오 비트율을 선택하십시오. 기본값은 160000 Hz입니다.
9. 실패한 내보내기 데이터**(MKV** 및 **AVI)** 유지 또는 삭제 필드에서 불완전하더라도 성공적으로 다운로드된 데이터를 유지할지, 아니면 삭제할지 여부를 지정합니다.

   사용자가 조사를 저장할 수 있게 하려면 사용자에게 할당된 보안 역할에 대해 내보내기 권한을 부여해야 합니다.

조사 정리

더 이상 유지할 필요가 없는 조사 또는 비디오 내보내기가 있는 경우 이를 삭제할 수 있습니다. 이 작업은 예를 들어 서버의 가용 디스크 공간을 늘리려는 경우에 유용할 수 있습니다.

- 조사와 이를 위해 생성된 모든 비디오 내보내기를 삭제하려면 목록에서 조사를 선택한 다음 삭제 를 클릭합니다.
- 조사를 위해 내보낸 개별 비디오 파일을 삭제하되 조사를 유지하려면 목록에서 조사를 선택합니다. 조사 세부 정보 그룹에서 내보내기를 위한 데이터베이스, **AVI** 또는 **MKV** 필드 오른쪽에 있는 삭제 아이콘을 클릭합니다.

비디오 푸시를 이용한 비디오 스트리밍(설명됨)

비디오 푸시를 설정하면 사용자가 다른 사용자에게 상황을 지속적으로 알려주거나 모바일 장치의 카메라에서 XProtect 감시 시스템으로 비디오를 스트리밍하여 비디오를 녹화한 다음 나중에 조사할 수 있습니다. 비디오 스트림은 오디오를 포함하고 있을 수 있습니다.

또한 페이지 23의 비디오 푸시 탭 및 페이지 11의 비디오 푸시 설정에 대한 요구사항을 참조하십시오.

비디오를 스트리밍하도록 비디오 푸시 설정

사용자가 모바일 장치에서 XProtect 시스템으로 비디오를 스트리밍하도록 하려면 XProtect Mobile 서버에서 비디오 푸시를 설정합니다.

Management Client 에서 다음 순서로 아래의 단계를 수행합니다.

1. 비디오 푸시 탭에서 비디오 푸시 확인란을 선택하여 이 기능을 활성화합니다.
2. 비디오 스트리밍을 위해 비디오 푸시 채널을 추가합니다.
3. 비디오 푸시 드라이버를 Recording Server 에서 하드웨어 장치로서 추가합니다. 이 드라이버는 Recording Server (으)로 비디오를 스트리밍할 수 있도록 카메라 장치를 시뮬레이션합니다.
4. 비디오 푸시 드라이버 장치를 비디오 푸시 채널에 추가합니다.

비디오 스트리밍를 위한 비디오 푸시 채널 추가

채널을 추가하려면 다음 단계를 따릅니다.

1. 탐색 창에서 **Mobile Servers** 를 선택하고 모바일 서버를 선택합니다.
2. 비디오 푸시 탭에서 비디오 푸시 확인란을 선택합니다.
3. 채널 매핑 아래 하단 좌측 모서리에서 추가 를 클릭하여 비디오 푸시 채널을 추가합니다.
4. 나타난 대화 상자에서 채널에서 사용할 사용자 계정의 사용자 이름(역할 아래 추가)을 입력합니다. 이 사용자 계정은 XProtect Mobile 서버와 레코딩 서버에 액세스가 허용되어야 합니다(전체 보안 탭에서).

   > 비디오 푸시를 사용하려면 해당 계정에 대한 사용자 이름과 암호를 이용하여 모바일 장치에서 XProtect Mobile 에 로그인해야 합니다.

   > 모바일 서버에 신규 비디오 푸시 채널을 추가할 시, 시스템은 해당 채널이 하드웨어 장치로 레코딩 서버에 추가될 때 사용되는 채널의 포트 번호와 MAC 주소를 생성합니다. 또한 시스템은 Mobile Server 와(과) Recording Server 을(를) 연결하는 데 사용하는 암호를 생성합니다. 기본 암호는 **Milestone** 입니다.

5. 포트 번호를 기록해 둡니다. 레코딩 서버에서 비디오 푸시를 하드웨어 장치로 추가할 때 이 정보가 필요합니다.
6. 확인 을 클릭하여 비디오 푸시 채널 대화 상자를 닫습니다.
7. 채널을 저장하려면 탐색 창의 상단 좌측 모서리에 있는 저장 을 클릭합니다.

비디오 푸시 채널 편집

추가한 비디오 푸시 채널의 구성 상세 사항을 다음과 같이 편집할 수 있습니다.

1. 채널 매핑 아래에서 편집할 채널을 선택한 후 편집 을 클릭합니다.
2. 편집을 마무리한 후 확인 을 클릭할여 비디오 푸시 채널 대화 상자를 닫습니다.
3. 편집을 저장하려면 탐색 창의 상단 좌측 모서리에 있는 저장 을 클릭합니다.

비디오 푸시 채널의 포트 번호와 MAC 주소 편집 시 새로운 정보와 함께 레코딩 서버에 예전에 추가한 비디오 푸시 채널 구성 상세 사항도 바꾸도록 합니다. 그렇지 않으면 Recording Server 와(과) Mobile Server 의 연결이 끊어집니다.

비디오 푸시 채널 제거

더 이상 사용하지 않는 채널도 제거할 수 있습니다.

1. 채널 매핑 아래에서 제거할 채널을 선택한 후 제거 를 클릭합니다.
2. 변경 사항을 저장하려면 탐색 창의 상단 좌측 모서리에 있는 저장 을 클릭합니다.

암호 변경

Recording Server 와(과) Mobile Server 을(를) 연결하는 데 사용한 자동 생성된 암호를 다음과 같은 방법으로 변경할 수 있습니다.

1. 채널 매핑 아래 하단 우측 모서리에서 암호 변경 을 클릭합니다.
2. 비디오 푸시 암호 변경 대화 상자에서 첫 필드에 새 암호를 입력한 후 두 번째 필드에 새 암호를 다시 입력한 후 확인 을 클릭합니다.
3. 변경 사항을 저장하려면 탐색 창의 상단 좌측 모서리에 있는 저장 을 클릭합니다.

빋오 푸시 채널 암호 변경 시 해당 변경 사항은 목록에 이미 있거나 향후 추가될 모든 비디오 푸시 채널에 적용됩니다. 목록에 있는 기존의 모든 비디오 푸시 채널을 제거하더라도 신규 암호는 활성화된 상태 그대로 남아있게 되며 향후 생성되는 채널에 적용됩니다.

변경 사항을 저장한 후에는 Recording Server 와(과) Mobile Server 의 연결이 끊어지므로 기존의 모든 비디오 푸시 채널은 작동을 중단합니다. 이 연결을 복원하려면 탐색 창에서 마우스 오른쪽 단추로 레코딩 서버 탭을 클릭하여 하드웨어 대체 마법사를 실행하고 Recording Server 의 하드웨어 장치로 추가한 비디오 푸시 드라이버에 대한 새 암호를 입력해야 합니다.

다음에 하드웨어 장치로 비디오 푸시 드라이버 추가: Recording Server

1. 탐색 창에서 레코딩 서버 를 클릭합니다.
2. 비디오를 스트리밍할 서버를 우클릭하고 하드웨어 추가 를 클릭하여 하드웨어 추가 마법사를 엽니다.
3. 하드웨어 감지 방법으로 수동 을 선택하고 다음 을 클릭합니다.
4. 다음과 같이 카메라에 대한 로그인 자격 증명을 입력합니다.
   - 사용자 이름: 공장 출하 기본 값 또는 카메라에 지정된 사용자 이름을 입력합니다.
   - 암호: **Milestone** 을(를) 입력합니다. 이 암호는 시스템이 생성한 것입니다. 모바일 서버에서 비디오 푸시 채널 추가 시 이를 변경한 경우 사용하고자 하는 암호를 입력한 후 다음 을 클릭합니다.

   이러한 자격 증명은 사용자용이 아닌 하드웨어용입니다. 이 자격 증명은 비디오 푸시 채널 액세스에 사용되는 사용자 계정과는 관련이 없습니다.

5. 드라이버 목록에서 **Milestone**을(를) 확장하고 비디오 푸시 드라이버 확인란을 선택한 후 다음을 클릭합니다.
6. 주소 필드에 XProtect Mobile 서버가 설치된 컴퓨터의 IP 주소를 입력합니다.

   시스템이 생성한 MAC 주소를 사용할 것을 권장합니다. 예를 들어 모바일 서버의 비디오 푸시 채널의 포트 번호와 MAC 주소를 편집한 경우나 비디오 푸시 드라이버 장치에 문제가 있는 경우에만 변경하십시오.

7. 포트 필드에 비디오 스트리밍을 위해 생성한 채널의 포트 번호를 입력합니다. 이 포트 번호는 채널을 만들 때 이미 할당되었습니다.
8. 하드웨어 모델 열에서 비디오 푸시 드라이버 를 선택한 후 다음 을 클릭합니다.
9. 시스템이 새 하드웨어를 감지하면 다음 을 클릭합니다.
10. 하드웨어 이름 템플릿 필드에서 하드웨어 모델과 IP 주소를 모두 표시할지, 아니면 모델만 표시할지 여부를 지정합니다.
11. 활성화됨 확인란을 선택하여 관련 장치를 활성화할지 여부를 지정합니다. 활성화되지 않았더라도 관련 장치를 비디오 푸시 드라이버 목록에 추가할 수 있습니다. 나중에 활성화할 수 있습니다.

    비디오를 스트리밍할 때 위치 정보를 사용하려면 메타데이터 포트를 활성화해야 합니다.

    비디오를 스트리밍할 때 오디오를 재생하고자 하는 경우 비디오 스트리밍에 사용하는 카메라에 관련된 마이크로폰을 반드시 활성화해야 합니다.

12. 왼쪽에서 관련 장치에 대한 기본 그룹을 선택하거나 그룹에 추가 필드에서 지정 그룹을 선택합니다. 여러 장치를 그룹에 추가하면 모든 장치에 한꺼번에 설정을 적용하거나 장치를 교체하기가 쉽습니다.

비디오 푸시 드라이버 장치를 비디오 푸시 채널에 추가합니다

비디오 푸시 드라이버 장치를 비디오 푸시 채널에 추가하려면 다음 단계를 따르십시오.

1. 사이트 탐색 창에서 모바일 서버 를 클릭한 다음 비디오 푸시 탭을 클릭합니다.
2. 카메라 찾기 를 클릭합니다. 문제가 없으면 카메라 이름 필드에 비디오 푸시 드라이버 카메라의 이름이 표시됩니다.
3. 구성을 저장합니다.

기존 비디오 푸시 채널에 대한 오디오 활성화

비디오 푸시 내 오디오 활성화를 위한 요건을 충족 한 후(페이지 11의 비디오 푸시 설정에 대한 요구사항 참조), Management Client 에서:

1. 사이트 탐색 창에서 서버 노드를 확장한 후 레코딩 서버 를 클릭합니다.
2. 개요 창에서 관련 레코딩 서버 폴더를 선택한 후 비디오 푸시 드라이버 폴더를 열고 비디오 푸시 관련 마이크로폰을 오른쪽 클릭합니다.
3. 활성화 를 선택하여 마이크로폰을 활성화합니다.
4. 동일한 폴더에서 비디오 푸시와 관련된 카메라를 선택합니다.
5. 속성 창에서 클라이언트 탭을 클릭합니다(클라이언트 탭(장치) 참조).
6. 관련 마이크로폰 필드의 오른편에서 ••• 를 클릭합니다. 선택된 장치 대화 상자가 열립니다.
7. **Recording Servers** 탭에서 레코딩 서버 폴더를 열고 비디오 푸시와 관련된 마이크로폰을 선택합니다.
8. 확인 을 클릭합니다.

2단계 이메일 확인을 위해 사용자 설정

사용 가능한 기능은 사용 중인 시스템에 따라 다릅니다. 자세한 정보는 https://www.milestonesys.com/solutions/platform/product-index/ 을(를) 참조하십시오.

XProtect Mobile 클라이언트나 XProtect Web Client 의 사용자에 추가적인 로그인 단계를 부여하려면 XProtect Mobile 서버에서 2단계 확인을 설정합니다. 표준 사용자 이름 및 암호 외에, 사용자는 이메일로 수신한 확인 코드를 입력해야 합니다.

2단계 확인은 감시 시스템의 보호 수준을 높여 줍니다.

Management Client 에서 다음 단계를 실행합니다.

1. 페이지 54의 SMTP 서버에 대한 정보를 입력합니다.
2. 페이지 54의 사용자에게 발송될 확인 코드 지정.
3. 페이지 54의 사용자와 Active Directory 그룹에 로그인 방법 할당.

또한 페이지 11의 사용자의 2단계 확인 설정에 대한 요구 사항 및 페이지 25의 단계 확인 탭을 참조하십시오.

SMTP 서버에 대한 정보를 입력합니다

제공자는 SMTP 서버에 대한 정보를 사용합니다.

1. 탐색 창에서 모바일 서버 를 선택하고, 관련 모바일 서버를 선택합니다.
2. **2**단계 확인 탭에서 **2**단계 확인 활성화 확인란을 선택합니다.
3. 제공자 설정 아래에 이메일 탭에서 SMTP 서버에 대한 정보를 입력하고, 클라이언트 사용자가 로그인할 때 및 보조 로그인을 위해 설정될 때 시스템이 보낼 이메일을 지정합니다. 각 매개변수에 대한 자세한 내용은 페이지 25의 단계 확인 탭을 참조하십시오.

자세한 정보는 페이지 25의 단계 확인 탭을 참조하십시오.

사용자에게 발송될 확인 코드 지정

확인 코드의 복잡성을 지정하려면:

1. **2**단계 확인 탭의 확인 코드 설정 섹션에서, 예를 들어 연결 해제된 네트워크에서의 경우와 같이 클라이언트 사용자는 로그인을 재확인할 필요가 없는 XProtect Mobile 기간을 지정합니다. 기본 기간은 3분입니다.
2. 사용자가 수신된 확인 코드를 사용할 수 있는 기간을 지정합니다. 이 기간 후에 코드는 무효화되며, 사용자는 새 코드를 다시 요청해야 합니다. 기본 기간은 5분입니다.
3. 제공된 코드가 무효화되기 전에 코드 입력 시도의 최대 횟수를 지정합니다. 기본 횟수는 3회입니다.
4. 코드의 문자 수를 지정합니다. 기본 길이는 6입니다.
5. 시스템이 생성할 코드의 복잡성을 지정합니다.

자세한 정보는 페이지 25의 단계 확인 탭을 참조하십시오.

사용자와 Active Directory 그룹에 로그인 방법 할당

2단계 확인 탭의 사용자 설정 섹션에서 XProtect 시스템에 추가된 사용자와 그룹 목록이 나타납니다.

1. 로그인 방법 열에서, 각 사용자 또는 그룹에 대한 확인 방법을 선택합니다.
2. 세부 정보 필드에서 개별 사용자의 이메일 주소와 같은 전달 세부 정보를 추가합니다. 다음에 사용자가 XProtect Web Client 또는 XProtect Mobile 앱에 로그인할 때, 보조 로그인을 요청 받게 됩니다.
3. Active Directory에 하나의 그룹이 구성된 경우, XProtect Mobile 서버는 Active Directory에서 이메일 주소

와 같은 세부 정보를 사용합니다.

> Windows 그룹은 2단계 확인을 지원하지 않습니다.

4. 구성을 저장합니다.

이메일을 통한 2단계 확인을 위해 사용자를 설정하는 단계를 완료했습니다.

자세한 정보는 페이지 25의 단계 확인 탭을 참조하십시오.

동작 (설명됨)

일반 탭의 동작 을 활성화하거나 비활성화함으로써 XProtect Mobile 클라이언트 또는 XProtect Web Client 에 있는 동작 탭의 가용성을 관리할 수 있습니다. 동작 은 기본적으로 활성화되며 연결된 장치에 사용할 수 있는 모든 동작이 여기에 표시됩니다.

자세한 내용은 페이지 14의 일반 탭을 참조하십시오.

XProtect Mobile 클라이언트 및 XProtect Web Client 에서 사용할 출력 이름 지정(설명됨)

현재 카메라와 함께 동작을 올바르게 표시하려면 카메라와 같은 이름을 가진 출력 그룹을 생성해야 합니다.

예:

“AXIS P3301, P3304 - 10.100.50.110 - Camera 1”이란 이름을 가진 카메라에 출력이 연결되는 출력 그룹을 생성하려면, 이름 필드에 같은 이름을 입력해야 합니다 (장치 그룹 정보 아래).

설명 필드 에서 나중에 설명을 추가할 수 있습니다(예: “AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch”).

> 이러한 명명 규칙을 따르지 않으면 관련 카메라 뷰에서 동작 목록에 동작이 표시되지 않습니다. 대신, 동작이 동작 탭의 다른 동작 목록에 표시됩니다.

자세한 내용은 출력 장치(설명됨) 를 참조하십시오.

유지관리

Mobile Server Manager (설명됨)

Mobile Server Manager 은(는) 모바일 서버에 연결된 기능으로서 트레이에서 제어됩니다. 알림 영역에서 Mobile Server Manager 트레이 아이콘을 우클릭하면 모바일 서버 기능에 액세스하는 메뉴가 열립니다.

다음을 수행할 수 있습니다.

- 페이지 56의 XProtect Web Client 액세스
- 페이지 57의 Mobile Server 서비스 시작, 중지 및 재시작
- 페이지 57의 관리 서버 주소 쓰기/편집
- 페이지 57의 포트 번호 표시/편집
- 다음을 사용하여 페이지 58의 모바일 서버 암호화를 활성화합니다: **Server Configurator**
- 오늘의 로그 파일을 엽니다(페이지 59의 로그 및 조사 액세스(설명됨) 참조)
- 로그 폴더를 엽니다(페이지 59의 로그 및 조사 액세스(설명됨) 참조)
- 조사 폴더를 엽니다(페이지 59의 로그 및 조사 액세스(설명됨) 참조)
- 페이지 60의 조사 폴더 변경
- XProtect Mobile 서버 상태를 확인합니다(페이지 60의 상태 표시(설명됨) 참조)

XProtect Web Client 액세스

컴퓨터에 XProtect Mobile 서버를 설치하면, XProtect Web Client 을(를) 사용하여 카메라와 뷰에 액세스할 수 있습니다. XProtect Web Client 을(를) 설치가 필요 없기 때문에, XProtect Mobile 서버를 설치한 컴퓨터나 이 용도로 사용하려는 다른 어떤 컴퓨터에서도 여기에 액세스할 수 있습니다.

1. XProtect Mobile 에서 Management Client 서버를 설정합니다.
2. XProtect Mobile 서버가 설치된 컴퓨터를 사용하는 경우, 알림 영역에서 Mobile Server Manager 트레이 아이콘을 우클릭하고 **XProtect Web Client** 열기 를 선택합니다.
3. XProtect Mobile 서버가 설치된 컴퓨터를 사용하고 있지 않은 경우, 브라우저에서 여기에 액세스할 수 있습니다. 이 프로세스의 4 단계를 계속 진행합니다.
4. 인터넷 브라우저(Internet Explorer, Mozilla Firefox, Google Chrome 또는 Safari)를 엽니다.

5. 외부 IP 주소, 즉 XProtect Mobile 서버가 실행 중인 서버의 외부 주소와 포트를 입력합니다.

   예: XProtect Mobile 서버는 IP 주소가 127.2.3.4인 서버에 설치되고, 포트 8081에서 HTTP 연결을 수락하고 포트 8082에서 HTTPS 연결을 수락하도록 구성됩니다(설치 프로그램의 기본 설정).

   브라우저의 주소 표시줄에서, 다음을 입력합니다: 표준 HTTP 연결을 사용하고자 할 경우 **http://127.2.3.4:8081**, 보안 HTTPS 연결을 사용할 경우 **https://127.2.3.4:8082**. 이제 XProtect Web Client 사용을 시작할 수 있습니다.

6. 나중에 XProtect Web Client 에 쉽게 액세스하도록 주소를 브라우저의 북마크로 추가하십시오. XProtect Mobile 서버를 설치한 로컬 컴퓨터에서 XProtect Web Client 을(를) 사용하는 경우, 설치 프로그램이 생성하는 바탕 화면 바로가기를 사용할 수도 있습니다. 바로가기를 클릭하여 기본 브라우저를 실행하고 XProtect Web Client 을(를) 엽니다.

> 새 버전의 XProtect Web Client 을(를) 사용하려면 우선 XProtect Web Client 을(를) 실행하는 인터넷 브라우저의 캐시를 삭제해야 합니다. 시스템 관리자는 반드시 XProtect Web Client 사용자에게 업그레이드 후 브라우저의 캐시를 삭제하도록 요청하거나 이 작업을 원격으로 강제 실행해야 합니다(도메인에 있는 Internet Explorer에서만 이 작업을 수행할 수 있음).

Mobile Server 서비스 시작, 중지 및 재시작

필요한 경우, Mobile Server Manager 에서 Mobile Server 서비스를 시작, 중지 및 재시작할 수 있습니다.

- 이러한 작업을 수행하려면 Mobile Server Manager 아이콘을 마우스 오른쪽 버튼으로 클릭하고 각각 **Mobile Server** 서비스 시작, **Mobile Server** 서비스 중지 또는 **Mobile Server** 서비스 재시작 을 선택합니다

관리 서버 주소 쓰기/편집

1. 마우스 오른쪽 단추로 Mobile Server Manager 아이콘을 클릭하고 관리 서버 주소 를 선택합니다.
2. 서버 **URL** 필드에서, 서버의 URL 주소를 입력합니다.
3. 확인 을 클릭합니다.

포트 번호 표시/편집

1. Mobile Server Manager 아이콘을 마우스 오른쪽 버튼으로 클릭하고 포트 번호 표시/편집 을 선택합니다.
2. 포트 번호를 편집하려면 관련 포트 번호를 입력합니다. HTTP 연결용 표준 포트 번호 및/또는 HTTPS 연결용 보안 포트 번호를 나타낼 수 있습니다.
3. 확인 을 클릭합니다.

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 확인해줍니다. 자세한 정보는 페이지 35의 모바일 서버 데이터 암호화(설명됨)과 페이지 37의 클라이언트를 위한 모방리 서버 암호화 요건을 참조하십시오.

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:

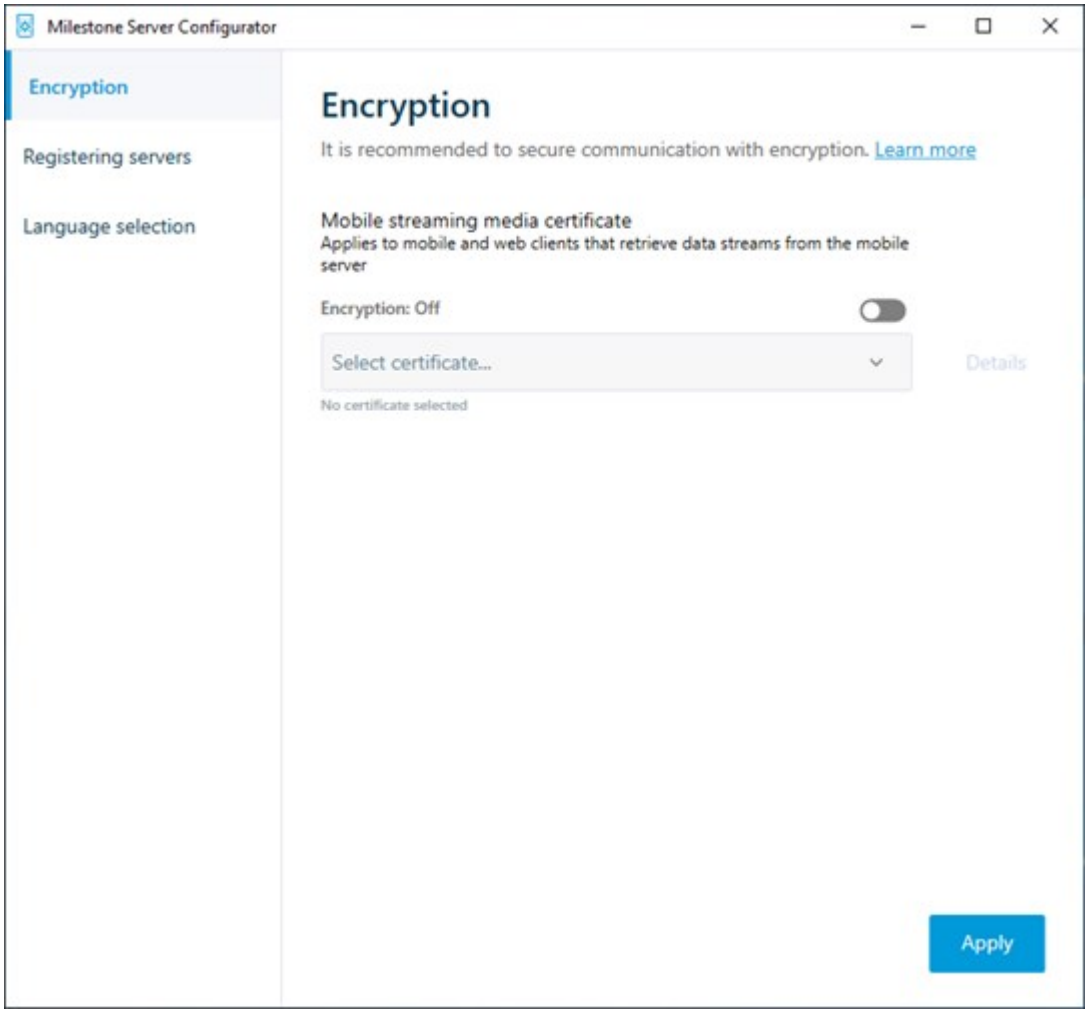
1. 모바일 서버가 설치된 컴퓨터에서 다음으로부터 **Server Configurator** 을(를) 엽니다.
   - Windows 시작 메뉴

   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. Windows개인 키를 가졌으며 Certificate Store상에 설치되어 있는 인증서의 고유한 주체 이름 목록을 열려면 인증서 선택 을 클릭합니다.
4. 인증서를선택하여XProtectMobile클라이언트와모바일서버의XProtectWebClient간통신을암호화합니다.

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 신뢰될 필요가 있습니다.



2. 적용하기 를 클릭합니다.

인증서 적용 시 Mobile Server 서비스가 다시 시작됩니다.

로그 및 조사 액세스(설명됨)

Mobile Server Manager 을(를) 이용하면 해당 일자의 로그 파일에 신속히 액세스하고, 로그 파일이 저장된 폴더를 열고, 조사가 저장된 폴더를 열 수 있습니다.

이 중 하나를 열려면 Mobile Server Manager 아이콘을 마우스 오른쪽 버튼으로 클릭하고 다음을 선택합니다:

- 오늘 로그 파일 열기
- 로그 폴더 열기
- 조사 폴더 열기

시스템에서 XProtect Mobile 을(를) 제거해도 해당 로그 파일은 삭제되지 않습니다. 적합한 사용자 권한을 가진 관리자가 나중에 이러한 로그 파일에 액세스하거나, 더 이상 필요하지 않은 경우 삭제할 수 있습니다. 로그 파일의 기본 위치는 **ProgramData** 폴더입니다. 로그 파일의 기본 위치를 변경하는 경우, 기존 로그는 새 위치로 복사되지 않으며 삭제되지도 않습니다.

조사 폴더 변경

조사의 기본 위치는 **ProgramData** 폴더입니다. 조사 폴더의 기본 위치를 변경하면 기존의 조사는 새로운 위치에 자동으로 복사되지 않으며 삭제되지도 않습니다. 하드 디스크의 조사 내보내기 저장 위치를 변경하려면:

1. 마우스 오른쪽 버튼으로 Mobile Server Manager 아이콘을 클릭하고 조사 폴더 변경 을 선택합니다.

   조사 위치 창이 나타납니다.

2. 현재 위치를 나타내는 폴더 필드 옆에서 폴더 아이콘을 클릭하여 기존 폴더를 검색하거나 새로운 폴더를 생성한 후 **OK** 를 클릭합니다.

3. 이전 조사 목록에서 현재 위치에 저장된 기존의 조사에 적용하고자 하는 동작을 선택합니다. 해당 옵션은 다음과 같습니다.

   - 이동: 기존 조사를 새로운 폴더로 이동시킵니다.

     기존 조사를 새로운 폴더로 이동시키지 않으면 더이상 볼 수 없게 됩니다.

   - 삭제: 기존 조사를 삭제합니다.
   - 조치 없음: 기존 조사는 현재 폴더 위치에 남아 있습니다. 조사 폴더의 기본 위치를 변경한 후에는 더 이상 이를 볼 수 없습니다

4. 적용 을 클릭한 후 **OK** 를 클릭합니다.

상태 표시(설명됨)

Mobile Server Manager 아이콘을 마우스 오른쪽 버튼으로 클릭하고 상태 표시 를 선택하거나 Mobile Server Manager 아이콘을 두 번 클릭하여 XProtect Mobile 서버의 상태를 나타내는 창을 엽니다. 다음 정보를 볼 수 있습니다:

이름	설명
서버가 실행되기 시작한 시기	XProtect Mobile 서버가 마지막으로 시작되었을 때의 시간과 날짜입니다.

이름	설명
연결된 사용자	현재 XProtect Mobile 서버에 연결된 사용자의 수입니다.
하드웨어 디코딩	XProtect Mobile 서버에서 하드웨어 속도증진 디코딩이 작동 중인지 여부를 나타냅니다.
CPU 사용량	현재 XProtect Mobile 서버에 의해 사용 중인 CPU의 % 비율입니다.
CPU 사용량 기록	XProtect Mobile 서버에 의한 CPU 사용 기록을 세부적으로 보여주는 그래프입니다.

문제 해결

문제 해결 XProtect Mobile

연결

1. 왜 **XProtect Mobile** 클라이언트에서 레코딩**/XProtect Mobile** 서버로 연결할 수 없나요?

   레코딩을 연결하기 위해 XProtect Mobile 서버가 XProtect 시스템을 구동하는 서버 또는 전용 서버에 설치되어 있어야 합니다. 관련 XProtect Mobile 설정은 또한 XProtect 비디오 관리 설정에서 필요합니다. 이러한 설정은 플러그인 또는 제품 설치나 업그레이드의 일부로서 설치됩니다. XProtect Mobile 서버를 받는 방법과 사용 중인 XProtect 시스템에서 XProtect Mobile 을(를) 통합하는 방법에 관한 자세한 내용은 구성 섹션을 참조하십시오(페이지 14의 모바일 서버 설정 참조).

2. 방화벽을 켰는데 모바일 장치에서 서버에 연결할 수 없습니다. 왜 안되나요?

   XProtectMobile서버를설치할때방화벽이꺼져있었던경우,TCP와UDP통신을수동으로활성화해야합니다.

3. **HTTPS** 연결을 통해 **XProtect Web Client** 을**(**를**)** 구동할 때 보안 경고를 어떻게 피할 수 있습니까?

   인증서에 다긴 서버 주소 정보가 부정확하므로 경고가 표시됩니다. 연결은 여전히 암호화될 것입니다. XProtect Mobile 서버에서 자체 서명된 인증서는 XProtect Mobile 서버 접속에 사용된 서버 주소와 일치하는 전용 인증서로 대체되어야 합니다. 이러한 인증서는 Verisign과 같은 공인 인증서 서명 제공사를 통해 획득할 수 있습니다. 더 자세한 내용은 선택된 서명 권한 보유자와 상담하십시오.
   XProtect Mobile 서버는 Microsoft IIS를 사용하지 않습니다. 이는 IIS를 사용하는 서명 권한에 의한 인증 서명 요청(CSR) 생성을 위해 제공된 지침을 XProtect Mobile 서버에서는 사용할 수 없음을 의미합니다. 명령줄 인증서 도구 또는 기타 유사한 타사 응용 프로그램을 사용하여 CSR-파일을 수동으로 생성해야 합니다. 이 과정은 시스템 관리자 및 고급 사용자만 수행해야 합니다.

이미지 품질

1. 왜 **XProtect Mobile** 클라이언트에서 비디오를 볼 때 때때로 이미지 품질이 나쁜가요?

   XProtect Mobile 서버는 서버와 클라이언트 간에 사용 가능한 대역폭에 따라 자동으로 이미지의 품질을 조정합니다. XProtect® Smart Client에서 낮은 이미지 품질을 경험한다면, XProtect Mobile 클라이언트를 통해 최대 해상도의 이미지를 받기에는 너무 작은 대역폭일 수도 있습니다. 이렇게 되는 이유는 서버로부터 업스트림 대역폭이 너무 적거나 클라이언트에서 다운스트림 대역폭이 너무 적기 때문입니다. 자세한 정보는 XProtect Smart Client 에 관한 사용자 설명서 를 참조하십시오.

   다중 무선 인터넷 대역폭이 제공되는 구역에 있는 경우, 더 나은 대역폭이 제공되는 구역에 들어갔을 때 이미지 품질이 향상되는 것을 볼 수 있습니다.

2. 왜 **Wi-Fi**를 통해 가정 내 **XProtect** 비디오 관리 시스템에서 사무실로 연결할 때 이미지 품질이 나쁜가요?

   홈 인터넷 대역폭을 확인합니다. 많은 사설 인터넷 연결이 설명된 것과 같이(예: 20 Mbit/2 Mbit) 각기 다른 다운로드 및 업로드 대역폭을 가지고 있습니다. 이는 가정 사용자가 대용량 데이터를 인터넷에 업로드할 필요가 거의 없지만 그 대신 많은 데이터를 소비하기 때문입니다. XProtect 비디오 관리 시스템은 XProtect Mobile 클라이언트에 비디오를 전송해야 하며 인터넷 연결 속도의 제한을 받습니다. 품질이 낮은 이미지가 XProtect Mobile 클라이언트의 네트워크에서 다운로드 속도가 좋은 다수의 위치에서 지속되는 경우, 사용 중인 홈 인터넷 연결의 업로드 속도를 업그레이드하면 문제가 해결될 수도 있습니다.

하드웨어 가속 디코딩

1. 사용 중인 프로세서가 하드웨어 가속 디코딩을 지원하나요?

   Intel의 새 프로세서만이 하드웨어 가속 디코딩을 지원합니다. Intel 웹사이트(https://ark.intel.com/Search/FeatureFilter?productType=processors/)에서 사용 중인 프로세서가 지원되는지 확인합니다.

   메뉴에서 기술 > **Intel Quick Sync Video** 가 예로 설정되어 있는지 확인합니다.

   사용 중인 프로세서가 지원하는 경우, 하드웨어 가속 디코딩은 기본으로 활성화되어 있을 것입니다. 현재 상태를 Mobile Server Manager 의 상태 표시 에서 볼 수 있습니다(페이지 60의 상태 표시(설명됨)).

2. 사용 중인 운영 체제가 하드웨어 가속 디코딩을 지원하나요?

   XProtect 을(를) 지원하는 모든 운영 체제는 또한 하드웨어 가속을 지원합니다.

   Intel 웹사이트에서 받은 가장 최신의 그래픽 드라이브를 시스템에 설치해야 합니다. 이러한 드라이버는 Windows 업데이트에서 사용할 수 없습니다.

   모바일 서버가 가상 공간에 설치되지 않은 경우 하드웨어 가속 디코딩이 지원되지 않습니다.

3. 모바일 서버상의 하드웨어 가속 디코딩을 어떻게 비활성화할 수 있습니까**?(**고급**)**

   만일 모바일 서버상의 프로세서가 하드웨어 가속 디코딩을 지원한다면 이는 기본으로 활성화되어 있을 것입니다. 하드웨어 가속 디코딩 기능을 끄려면 다음을 수행하십시오:

   1. VideoOS.MobileServer.Service.exe.config 파일을 찾습니다. 일반적 경로: C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
   2. 노트패드 또는 유사한 텍스트 편집기에서 파일을 엽니다. 필요한 경우 노트패드에서 파일 유형을 .config로 바꿉니다.
   3. <add key="HardwareDecodingMode" value="Auto" /> 필드를 찾습니다.
   4. "Auto" 값을 "Off"로 대체합니다.
   5. 저장하고 파일을 닫습니다.

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 Systems 은(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.