한화비전

IP 카메라
네트워크 장비 보안 강화 가이드

2023.04

V4.0

Contents

개정이력

버전	개정일자	개정내용	비고
V1.0	2017.6.13	공식 버전 제정	
V2.0	2018.1.16	- HTML5 스트리밍 기반 NonPlug-in 웹뷰어 기본레벨 추가 - 안전하게 SNMP사용 안전레벨에서 보호레벨로 변경 (Default 값 off로 변경) - 미사용 SNMP 비활성화 삭제 - 카메라 웹뷰어 백업 파일 포맷 STW 삭제 - 미사용 멀티캐스트 비활성화 SVNP 프로토콜 삭제	
V3.0	2020.4.	- 개별장치인증(기기/사용자인증) 추가 - 공장초기화 상태에서 SUNAPI/ONVIF 비활성화 추가 - Secure Boot 추가 - 안전한 통신 프로토콜 사용하기(HTTP) 보호레벨에서 안전레벨로 변경 - 안전하게 SNMP 사용 보호레벨에서 안전레벨로 변경 - 미사용 SNMP 비활성화 보호레벨 추가 - 미사용 Link-Local IPv4 주소 비활성화, 미사용 UPnP 검색 비활성화, 미사용 Bonjour 비활성화 안전레벨에서 보호레벨로 변경 - HTTP 인증(Digest 인증만 사용) 항목을 안전한 통신 프로토콜 사용하기(HTTP)로 변경하여 보호레벨에 추가 - 최신 버전의 TLS 사용 추가 - 안전한 Cipher Suites 사용하기 추가 - 안전한 통신 프로토콜(RTSP) 추가 - 저장암호화/백업암호화 추가	
V4.0	2023.4	- MQTT 추가 - 안전하게 MQTT 사용하기 추가 - 관리자 계정 변경/추가 사용자 계정 생성하기 내용 변경	

1. 서론

최근 몇 년간 고객의 재산과 개인 정보를 보호하기 위해 개발된 네트워크 감시 장비들이 오히려 개인 정보를 탈취하기 위한 수단으로 사용되는 역설적인 상황이 네트워크 감시 시장에서 발생하고 있습니다. 네트워크 감시 장비는 민감한 개인 정보로 사용될 수 있는 비디오 영상을 처리 및 관리하고 있으며, 네트워크를 기반으로 통신을 하므로 네트워크가 연결된 전세계 어디서나 원격 접속이 가능합니다. 이러한 특성으로 인해 네트워크 감시 장비는 지속적인 사이버 공격의 대상이 되고 있습니다.

한화비전은 고객의 재산과 개인 정보를 소중히 생각하는 마음으로 사이버 보안 강화를 위해 지속적으로 노력하여 왔으며 본 가이드 문서를 통해 제품에 구현된 보안 기능을 이해하고 안전하게 사용할 수 있도록 안내하고자 합니다.

2. 사이버 보안 레벨 정의

본 가이드는 다음과 같은 기준을 따라 사이버 보안 레벨을 정의하였으며, 각 레벨은 이전 레벨의 달성을 전제로 합니다.

- 기본 레벨은 사용자가 별도의 설정 없이 기기에서 기본으로 제공되는 기능만으로도 달성할 수 있는 보안 수준을 의미합니다.
- 보호 레벨은 사용자가 기기를 구입한 초기 상태나 공장 초기화 직후 상태에서 기본으로 설정되어 있는 초기 설정 값 만으로도 달성할 수 있는 보안 수준을 의미합니다.
- 안전 레벨은 기기에서 제공하는 기능이나 서비스로 인해 보안이 취약해질 수 있기 때문에 필요 없는 기능이나 서비스를 사용자가 직접 사용하지 않도록 설정함으로써 보안을 향상시킬 수 있는 수준을 의미합니다.
- 최상위 안전 레벨은 기기에서 제공되는 보안 기능과 함께 외부의 추가 보안 솔루션을 연동하여 보안을 향상시킬 수 있는 수준을 의미합니다.

< 표 1 >

사이버 보안 레벨	사이버 보안 강화 기능 & 방안	초기 설정	추천 설정
기본 레벨	복잡한 비밀번호 설정 강제	Default	-
	초기 비밀번호 제거	Default	-
	연속 비밀번호 실패 시 입력 제한	Default	-
	원격서비스 (Telnet, SSH) 미사용	Default	-
	환경 설정 정보 암호화	Default	-
	펌웨어 암호화 및 안전한 업데이트	Default	-
	추출된 비디오 포맷의 워터마킹과 암호화	Default	-
	초기화 시 로그 유지	Default	-
	HTML5 스트리밍 기반 NonPlug-in 웹뷰어	Default	-
	개별장치인증(기기/사용자 인증)	Default	-
	공장 초기화 상태에서 SUNAPI/ONVIF 비활성화	Default	-
	Secure Boot	Default	-

2. 사이버 보안 레벨 정의

사이버 보안 레벨	사이버 보안 강화 기능 & 방안	초기 설정	추천 설정
보호 레벨	공장초기화 수행하기	-	-
	게스트 로그인 기능 비활성화	미설정	-
	인증 없는 RTSP 연결 허용 비활성화	미설정	-
	미사용 멀티캐스트 비활성화	비활성화	-
	미사용 DDNS 비활성화	Off	-
	미사용 QoS 비활성화	미설정	-
	미사용 FTP 비활성화	미설정	-
	미사용 SNMP 비활성화	비활성화	-
	미사용 Link-Local IPv4 주소 비활성화	비활성화	-
	미사용 UPnP 검색 비활성화	비활성화	-
	미사용 Bonjour 비활성화	비활성화	-
	최신 버전의 TLS 사용	TLS 1.2/1.3	-
	안전한 Cipher Suites 사용하기	Secure Cipher Suites	-
	미사용 오디오 입력 비활성화	미사용	-
	미사용 MQTT 비활성화	비활성화	-
안전 레벨	최신 버전의 펌웨어 사용여부 확인하기	-	-
	최신 버전의 펌웨어로 업데이트하기	-	-
	정확한 날짜/시간 설정하기	초기값	변경
	안전한 통신 프로토콜 사용하기(HTTP)	HTTP+HTTPS	HTTPS
	안전한 통신 프로토콜 사용하기(RTSP)	HTTPS+Wisenet/ONVIF	HTTPS+RTSP
	HTTPS (기기 인증서 사용)	HTTP+HTTPS	HTTPS (기기 인증서 사용)
	HTTPS (고객 인증서 사용)	HTTP+HTTPS	HTTPS (고객 인증서 사용)
	기본 포트 변경하기	초기값	변경
	IP 필터링	미설정	설정
	TLS 를 이용한 E-mail 전송하기	비활성화	활성화
	안전하게 SNMP 사용하기	미설정	SNMP v3
	안전하게 MQTT 사용하기	비활성화	TLS 설정
	관리자 계정 변경/추가 사용자 계정 생성하기	-	변경/설정
	로그 점검하기	-	-
	저장데이터 암호화(LUKS 암호화)	미설정	설정
	백업데이터 암호화(ZIP 파일 암호화)	미설정	설정
최상위 안전 레벨	802.1X 인증서 기반 접근 제어	미사용	사용

※ 초기 설정 값이 초기값으로 되어 있다면 사용자가 선택할 수 있는 옵션이 아니라 기본으로 설정되어 제공된다는 것을 의미하며, 대쉬(-)로 되어 있다면 사용자가 선택할 수 있는 옵션이 존재하지 않으며 점검/실행해야 하는 활동을 의미합니다.

3. 기본 레벨

한화비전에서 제공하는 기기들은 제품을 구입하였을 당시의 기본 기능 또는 설정된 초기값만으로도 사이버 보안의 위협으로부터 안전을 보장받을 수 있도록 고려되어 개발되었습니다.

< 표 2 >

보안 정책	사이버 보안 기능	간략한 설명
비밀번호 정책	복잡한 비밀번호 설정 강제	최소 8자 이상의 비밀번호 복잡도(2가지 또는 3가지 유형)를 갖는 문자 입력 요구
	초기 비밀번호 제거	초기 접속 UI 로그인 시 비밀번호 설정 (Install Wizzard 포함)
접근제어	연속 비밀번호 실패 시 입력 제한	웹 UI 로그인 시 비인가 자로부터의 비밀번호 무작위 입력 공격 차단
	공장 초기화 상태에서 SUNAPI/ONVIF 비활성화	비디오 영상 유출 방지
원격 접속 제어 보안	원격서비스 (Telnet, SSH) 미사용	원격으로 시스템에 접속할 수 있는 모든 서비스 제거
설정 정보 백업 보안	환경 설정 정보 암호화	백업된 환경 설정 정보를 보호
펌웨어 보안	펌웨어 암호화 및 안전한 업데이트	펌웨어의 중요 정보 노출과 분석을 방지
		펌웨어 위변조 및 악성 코드 주입 방지
추출된 영상 보안	추출된 비디오 포맷의 워터마킹과 암호화	추출된 비디오 포맷의 기밀성과 무결성 보장 및 출처 인증
로그 기록 보안	초기화 시 로그 유지	침입자로부터의 악의적인 로그 삭제 보호
HTML5 스트리밍 표준	HTML5 스트리밍 기반 NonPlug-in 웹뷰어	Plug-in(ActiveX, 실버라이트, NPAPI) 없이 최적의 영상 서비스를 제공
개별장치인증	기기 및 상호인증(서버인증/클라이언트인증)	기기인증서를 이용한 암호화 통신 시 신뢰할 수 있는 기기 식별
물리보호	Secure Boot	펌웨어 위변조 방지

3. 기본 레벨

3.1. 복잡한 비밀번호 설정 강제

한화비전 기기의 비밀번호를 설정하기 위한 최소 문자는 8자 이상이며, 비밀번호의 길이에 따라 대/소문자, 숫자, 특수문자 중 3가지(8자~9자) 또는 2가지(10자 이상) 유형의 문자 입력을 요구합니다. 이러한 강제 설정은 사용자의 부주의로 인한 취약한 비밀번호 설정을 방지하여 비인가자로부터의 비밀번호 임의 탈취 가능성을 낮추도록 도와줍니다.

3.2. 초기 비밀번호 제거

제품의 초기 비밀번호가 존재하는 상태에서 사용자가 비밀번호를 변경하지 않고 사용하거나 제조사의 초기 비밀번호 자체를 변경할 수 없는 경우 비인가 자에게 무단 접근을 허용하는 심각한 보안 취약점을 야기할 수 있습니다. 이에 한화비전의 모든 제품은 초기 비밀번호를 없애고 기기의 UI에 처음 접근 시 비밀번호를 반드시 변경한 후 사용할 수 있도록 하여 사용자의 실수로 발생할 수 있는 보안 취약점까지 사전 방지하고 있습니다.

3.3. 연속 비밀번호 실패 시 입력 제한

해커들은 기기의 비밀번호를 찾기 위해 무작위 값들을 매우 빠른 속도로 기기에 입력합니다. 이러한 작업을 허용할 경우 일정 시간이 지나면 기기의 비밀번호가 노출될 수 밖에 없는 위험을 감수해야 합니다. 보안을 향상시키기 위하여 한화비전의 기기는 비밀번호 인증 5회 연속 실패 시 30초간 입력을 제한하고 있습니다. 이로 인해 비밀번호 무작위 입력 공격(Brute force attack)을 차단하고 있으며, 단순히 모든 연결을 차단하는 방법이 아닌 기존의 인증된 연결은 유지하고 비인가된 연결 시도만 차단함으로써 무작위 입력 공격을 통해 유발될 수 있는 서비스 거부(DoS) 공격까지 예방하고 있습니다.

3. 기본 레벨

3.4. 원격서비스 (Telnet, SSH) 미사용

네트워크 기기에서 텔넷(Telnet)과 같은 원격 서비스를 지원하는 데몬들은 제조사들로 하여금 고객들에게 A/S를 편리하게 제공할 수 있는 장점을 줄 수 있지만 해커나 악의적인 의도를 갖고 있는 제조사가 존재할 경우 가장 위험한 보안 사고를 일으킬 수 있는 요인이 될 수 있습니다. 이에 한화비전의 제품은 A/S의 편의성을 포기하고 이러한 리스크를 과감히 제거하는 정책을 채택하여 보안 수준을 향상시켰습니다.

3.5. 환경 설정 정보 암호화

백업(Backup) 기능을 사용하면 현재 기기의 환경 설정 정보를 담은 바이너리 파일을 PC에 다운로드 할 수 있으며, 복원(Restore) 기능을 통해 백업한 환경 설정 정보를 복원할 수 있습니다.

- 환경설정 정보 중 아래 항목은 제외
  : 네트워크 메뉴의 IP&Port, DDNS, IP filtering, HTTPS, 802.1x, QoS, SNMP, Auto IP configure 같은 설정 정보는 제외

이러한 기능을 활용할 경우 하나의 기기 설정만으로 동일한 모델명을 갖는 모든 기기에 대해 같은 환경 설정이 가능합니다. 백업한 환경 설정 정보를 담은 해당 바이너리 파일에는 사용자 기기 환경의 중요한 정보가 포함되기 때문에 한화비전에서는 환경 설정 정보를 백업 시 안전한 암호화 알고리즘을 사용하여 저장하고 있습니다.

1) 시스템 → 업그레이드/재부팅
2) 설정 백업 & 복원

2. 기본 레벨

3.6. 펌웨어 암호화 및 안전한 업데이트

한화비전의 제품은 기능추가/버그개선 및 보안 업데이트 등을 위한 펌웨어를 제공 시 암호화된 펌웨어를 한화비전의 홈페이지를 통해 제공하고 있습니다. 또한 펌웨어 업데이트 진행 시, 위변조된 펌웨어를 식별하고 기기의 정상 동작을 보장하기 위해 무결성을 검증 후에 업데이트가 완료될 수 있도록 하고 있습니다. 이를 통해 해커가 펌웨어 안에 포함되어 있는 중요 정보들을 분석할 수 없도록 하며 펌웨어 위변조를 통해 악성코드를 주입한 이후 기기에 대한 제어권을 탈취하여 또 다른 공격용 봇으로 사용할 수 없도록 할 수 있습니다. 펌웨어 안에는 해커가 악용할 수 있는 중요한 정보들이 많이 포함되어 있습니다. 한화비전의 제품은 이러한 펌웨어의 보안과 안전한 업데이트를 위해 기밀성 및 무결성이 보장된 펌웨어를 배포하고 있습니다.

3.7. 추출된 비디오 포맷의 워터마킹과 암호화

한화비전의 NVR/VMS를 사용하여 SEC 파일 포맷으로 추출한 비디오 파일은 일반 편집용 소프트웨어로 파일 열기가 불가능하기 때문에 파일의 위변조를 예방하고 있으며, 기본적으로 재생에 필요한 플레이어가 SEC 파일에서 **자동으로 추출되어 별도로 플레이어를** 설치할 필요가 없으며 사용자가 SEC 파일을 더블 클릭함으로써 간단하게 비디오 파일을 재생시킬 수 있습니다.

비디오 파일을 법적 증거 또는 개인정보 보호 목적으로 추출하고자 할 경우 SEC 파일 형식으로 선택 후 비밀번호를 설정하여 추출이 가능합니다. 이렇게 추출된 SEC 파일에는 워터마킹 및 암호화가 적용되어 해당 비디오의 변조 여부 확인 및 기밀성을 보장할 수 있으며, VMS(SSM)에서 SEC 파일로 추출되었다면 전자서명 기능이 추가 지원되어 해당 비디오가 한화비전의 SSM에서 추출되었다는 기술적 확인이 가능합니다.

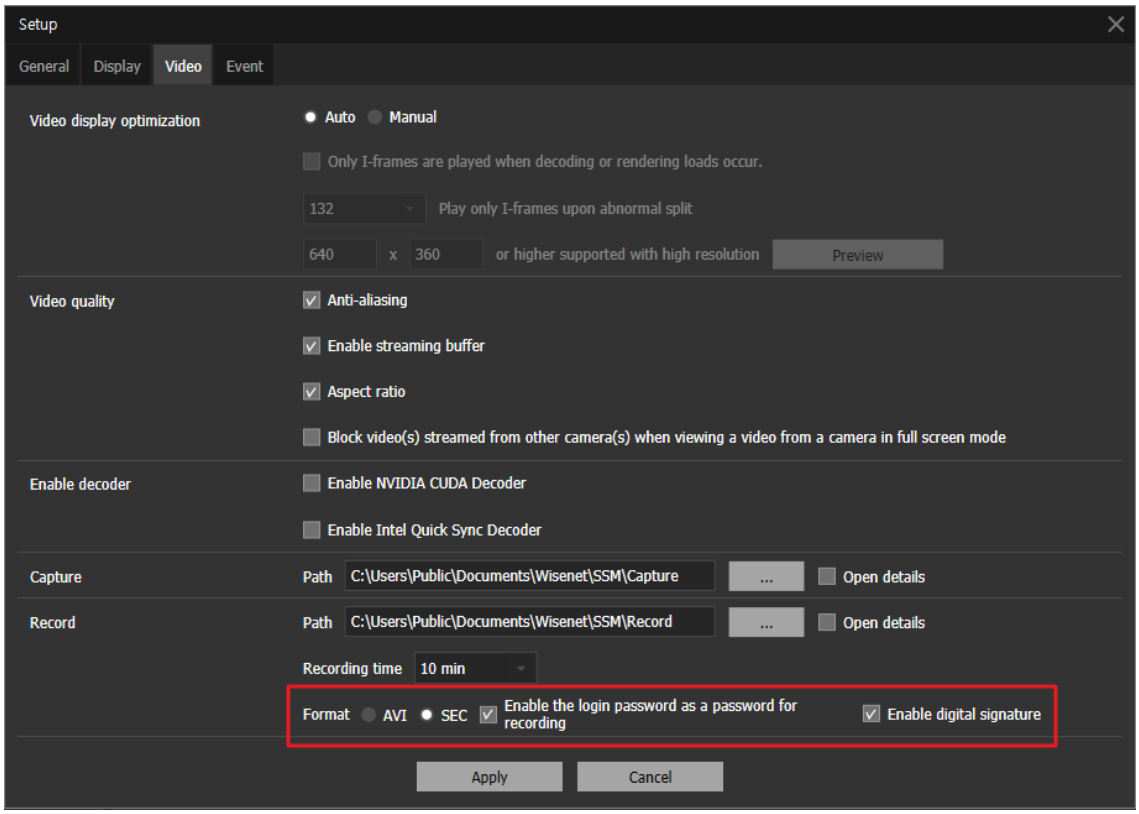
3. 기본 레벨

< 표 3 >

기기	추출 위치	백업 파일 포맷	워터마킹/ 암호화 여부	전자서명 여부	재생 플레이어
카메라	웹뷰어	AVI	X	X	범용 미디어 플레이어
NVR	세트	NVR	X	X	세트에서만 재생 가능
		SEC	O	X	백업 뷰어 (SEC에 내장)
	웹뷰어	SEC[1]	O	X	백업 뷰어 (SEC에 내장)
		AVI	X	X	범용 미디어 플레이어
VMS (SSM)	-	SEC	O	O	백업 뷰어 (SEC에 내장)
		AVI	X	X	범용 미디어 플레이어

• 설정(SSM 콘설 설정)

: 설정 → 비디오 → 형식



[1] NVR 웹뷰어 SEC 파일 추출 시 NonPlug-in 웹뷰어에서는 미지원

3. 기본 레벨

3.8 초기화 시 로그 유지

네트워크 기기에 누군가가 침입을 시도하거나 침입하였을 경우 로그를 확인하여 침입 경로를 분석하거나 사고의 경위를 파악할 수 있도록 하는 것은 네트워크 관리자 및 보안 관리자에게 매우 중요한 기능입니다. 그러나, 해커는 이러한 네트워크 기기들의 로그 기능을 알고 있기 때문에 침입할 때 기록된 로그들을 강제로 삭제하여 자신의 흔적을 남기지 않도록 하려고 합니다. 한화비전의 기기는 이러한 악의적인 로그 삭제나 기기 초기화를 통한 로그 초기화가 되지 않도록 하고 있습니다. 즉, 다음과 같이 공장초기화를 실행하더라도 카메라에 저장된 로그는 절대로 초기화가 되지 않습니다.

- 설정(IP 카메라)
  : 시스템 → 업그레이드/재시작 → 공장초기화 → 네트워크 설정 및 오픈 플랫폼 설정 유지 체크

3.9. HTML5 스트리밍 기반 NonPlug-in 웹뷰어

사용자는 카메라에서 제공하는 영상을 별도의 클라이언트 설치 없이 범용 브라우저를 통해 편하게 확인 할 수 있습니다. 업계 대부분의 웹뷰어는 브라우저에 설치되는 Plug-in(ActiveX, 실버라이트, NPAPI) 기술을 이용하여 영상 스트리밍 서비스를 제공하고 있습니다만, 이러한 Plugin-in 기술은 사용자 환경에 설치되는 구조로써 사용자 리소스에 대한 보안 취약점이 발생될 소지가 높아 최근 ActiveX 보안 취약점에 따른 악성코드 감염 사례가 빈번히 발생하고 있습니다. 이에, 브라우저 업체들은 Plug-in 설치 지원을 중단하였으며, 비디오 및 오디오와 같은 미디어 사용이 가능한 HTML 최신 표준(HTML5)을 통해 서비스를 제공하는 방향으로 표준화가 진행되고 있습니다. 이러한 흐름에 맞추어 한화비전은 Plug-in 없이 웹 표준화에 대응하면서 최적의 영상 서비스를 제공할 수 있는 HTML5 스트리밍 웹뷰어 서비스를 제공하여 보안과 사용자 편의성을 강화하였습니다.

3. 기본 레벨

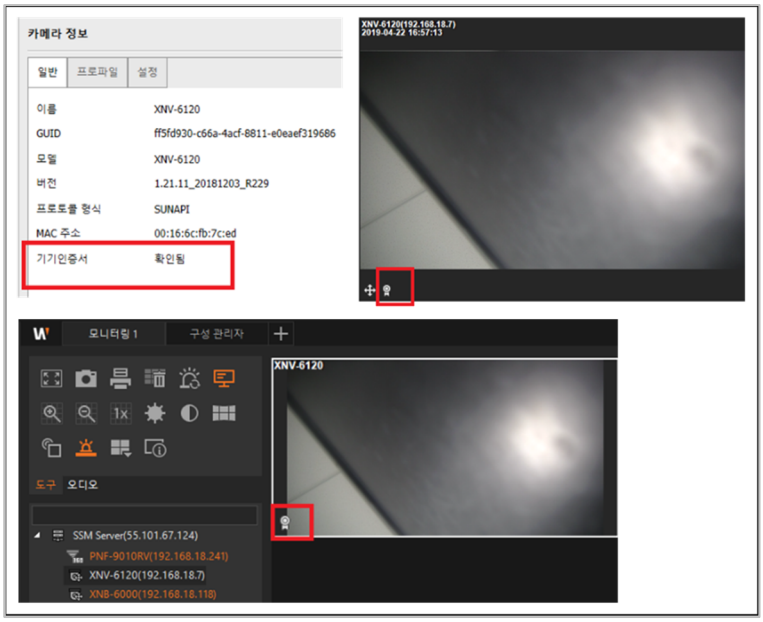
3.10. 개별장치인증(기기/상호인증(서버인증/클라이언트인증))

한화비전에서 제공하는 네트워크 기기는 암호화 통신 시 기기인증서를 이용한 기기 식별 및 상호인증 기능이 탑재되어 있습니다. 이를 통해 한화비전에서 제조한 신뢰할 수 있는 기기인지의 여부를 확인할 수 있으며 해커가 중간자 공격을 통해 임의로 보안 통신을 엿듣거나 조작할 수 없도록 하여 보안을 강화할 수 있습니다.
기기인증서 주입은 THALES HSM 장비를 사용하여 각 장치에 대한 인증서/개인키를 생성하고 제조 과정에서 각 장치에 주입합니다. 생성된 인증서는 Private Root CA에 의해 디지털 서명이 되므로, 한화비전에서 발행했음을 증명할 수 있습니다.

이 인증서를 사용하면 웹 브라우저에서 보안 경고 없이 보안 통신을 수행할 수 있으며, 아래와 같이 기기/상호 인증을 구현하는 제품에서 이를 확인 할 수 있습니다.

- 기기인증(SSM)

  : 등록 → 장치 선택 → 카메라 정보 → 일반 → 기기인증서 '확인됨' 정보 확인



3. 기본 레벨

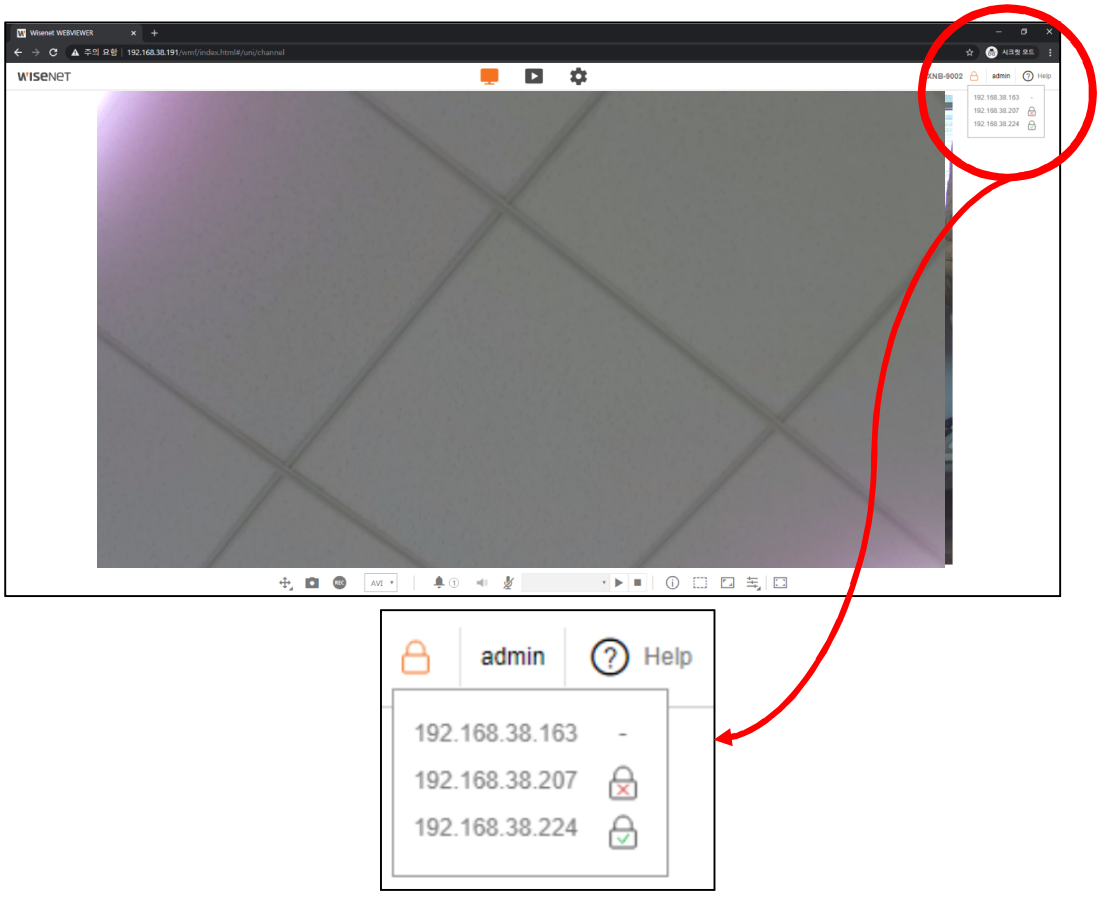
- 상호인증(카메라)

  : 라이브 화면 → 상호인증 아이콘 선택 → 인증 상태 확인

  ① 해당없음: 아이콘 없이 – 표시

  ② 상호인증 성공: 성공 아이콘

  ③ 상호인증 실패: 실패 아이콘



한화비전의 Private Root CA 인증서 설치 가이드는 당사 홈페이지에서 확인 가능합니다.

- 한화비전 사설 루트 CA인증서 사전 설치 가이드

  (https://www.hanwhavision.com/ko/support/cybersecurity/)

3. 기본 레벨

3.11. 공장 초기화 상태에서 SUNAPI/ONVIF 비활성화

한화비전은 SUNAPI/ONVIF를 통한 비디오 영상 정보의 유출을 방지하기 위하여, 비밀번호가 설정되기 전까지 SUNAPI/ONVIF 접속을 제한하고 있습니다.

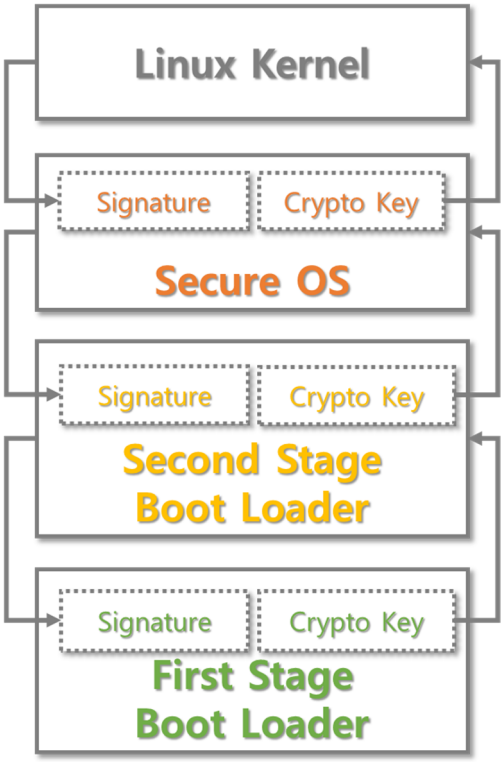
3.12. Secure Boot

한화비전은 자체 개발한 WN7 칩이 탑재된 기기를 제공하여 보안강화에 힘쓰고 있습니다. WN7에는 Secure Boot 기능이 내장되어 있습니다.

Secure Boot란, 부팅 시 로드 되는 각 부트 이미지의 전자서명(Digital Signature)를 검증하여, 위/변조된 부트 이미지가 실행되는 것을 방어하는 보안 기술입니다.

기존에는 펌웨어 이미지만을 한번 암호화 했다면, WN7에는 부트 이미지를 단계별로 검증하고 첫 번째 단계가 검증 통과되어야 다음 단계의 부트 이미지가 로드 됩니다.

검증 방법은 부트 이미지 생성 시 인증 Signature를 적재하고, 제품 부팅 시 해당 Signature를 검증하여 검증결과 이상이 없을 경우 부팅을 진행합니다.



4. 보호 레벨

한화비전의 기기들은 구입 초기 상태 또는 공장 초기화 직후 초기 설정값만으로도 기본적인 보안에 안전합니다.

< 표 4 >

보안 정책	사이버 보안 기능	간략한 설명
서비스 보호	공장 초기화	기기에 저장된 기존 정보들을 초기화
	게스트 로그인 기능 비활성화	허가 받지 않은 사용자로부터 영상 보호
	인증 없는 RTSP 연결 허용 비활성화	허가 받지 않은 사용자로부터 RTSP 영상 보호
	미사용 멀티 캐스트 비활성화	최초 활성화 되는 서비스를 최소화 하여 악의적인 공격 방지
	미사용 DDNS 비활성화	
	미사용 QoS 비활성화	
	미사용 FTP 비활성화	
	미사용 SNMP 비활성화	
	미사용 Link-Local IPv4 주소 비활성화	
	미사용 UPnP 검색 비활성화	
	미사용 Bonjour 비활성화	
	미사용 오디오 입력 비활성화	
	미사용 MQTT 비활성화	
암호	안전한 통신 프로토콜 사용하기(HTTPS)	웹뷰어상에서 송수신되는 개인정보 및 영상 보호
	최신 버전의 TLS 사용	보안에 안전한 최신버전 사용
	안전한 Cipher Suites 사용	보안에 안전한 암호 알고리즘 사용

4. 보호 레벨

4.1. 공장초기화

보안을 설정하고자 하는 기기가 사용자가 구입한 초기 상태가 아닌 사용한 상태라면 기기의 공장초기화를 수행하여 기기의 설정들을 초기화하는 것이 필요합니다. 이렇게 수행한 초기 상태만으로도 한화비전의 기기는 보호 레벨의 보안 수준을 달성할 수 있습니다.

1) 시스템 → 업그레이드/재부팅 → 공장초기화로 이동
2) 네트워크 설정 및 오픈 플랫폼 설정 유지 선택 해제
   (해당 설정을 선택 해제하지 않을 경우 네트워크 설정과 이미 설치된 Open 플랫폼이 제외된 상태로 초기화 됨.)
3) 초기화 버튼 클릭

4.2. 게스트 로그인 기능 비활성화

한화비전의 카메라에서는 사용자 이름과 비밀번호가 "guest"인 게스트 로그인 기능을 제공하고 있습니다. 이 게스트 계정은 최소한의 권한만을 허용하기 때문에 매우 제한적이지만 게스트 로그인 기능이 활성화되어 있을 경우 허가 받지 않은 사용자에게 영상 스트림이 노출될 수 있으므로 해당 기능이 불필요한 경우 반드시 게스트 로그인 기능을 비활성화시키는 것이 필요합니다.

1) Basic → 사용자 → 게스트 설정
2) 게스트 접속 허용 체크 해제

4. 보호 레벨

4.3. 인증 없는 RTSP 연결 허용 비활성화

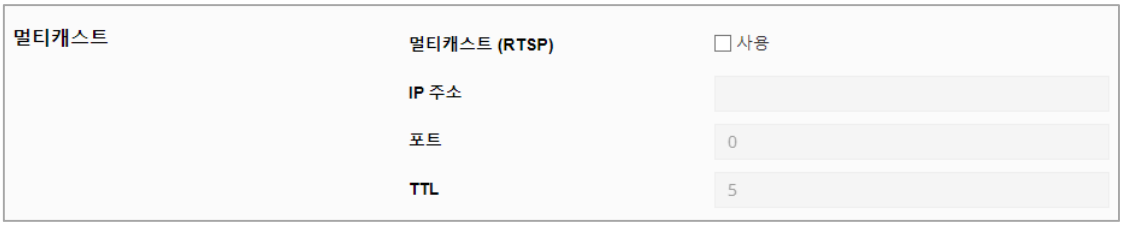
이 기능은 RTSP 영상 스트림을 인증 없이 공개적인 목적으로 제공하는 것에는 유용하지만 허가 받지 않은 사용자로부터 RTSP 영상 스트림을 보호하고 싶다면 반드시 인증 없는 RTSP 연결 허용 기능을 비활성화시키는 것이 필요합니다.

1) Basic → 사용자 → 인증 설정
2) 인증 없이 RTSP 연결 허용 체크 해제

4.4. 미사용 멀티캐스트 비활성화

멀티캐스트 사용을 지정하는 기능으로 RTSP 프로토콜에 대해 설정을 할 수 있습니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) Basic → 비디오 프로파일 → 멀티캐스트
2) 멀티캐스트(RTSP)의 사용함 체크 해제



4. 보호 레벨

4.5. 미사용 DDNS 비활성화

카메라가 DHCP 방식의 케이블 모뎀이나 DSL 모뎀 혹은 PPPoE 모뎀에 직접 연결되어 있는 경우, ISP에 연결을 시도할 때마다 IP 주소가 변경됩니다. 이 경우 사용자는 변경된 IP 주소를 알 수 없는데 DDNS 기능을 통해 제품의 ID를 사전 등록하면 변경된 IP 주소로 쉽게 접속할 수 있습니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 네트워크 → DDNS → 사용 안함 선택
2) 적용 버튼 클릭

4.6. 미사용 QoS 비활성화

QoS 기능은 특정 IP에 대하여 영상 전송 품질을 보장하도록 우선순위를 설정하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 QoS로 설정되어 있는 IP 목록을 삭제합니다.

1) 네트워크 → QoS
2) QoS로 설정되어 있는 IP 목록을 선택 후 삭제
3) 적용 버튼 클릭

4. 보호 레벨

4.7. 미사용 FTP 비활성화

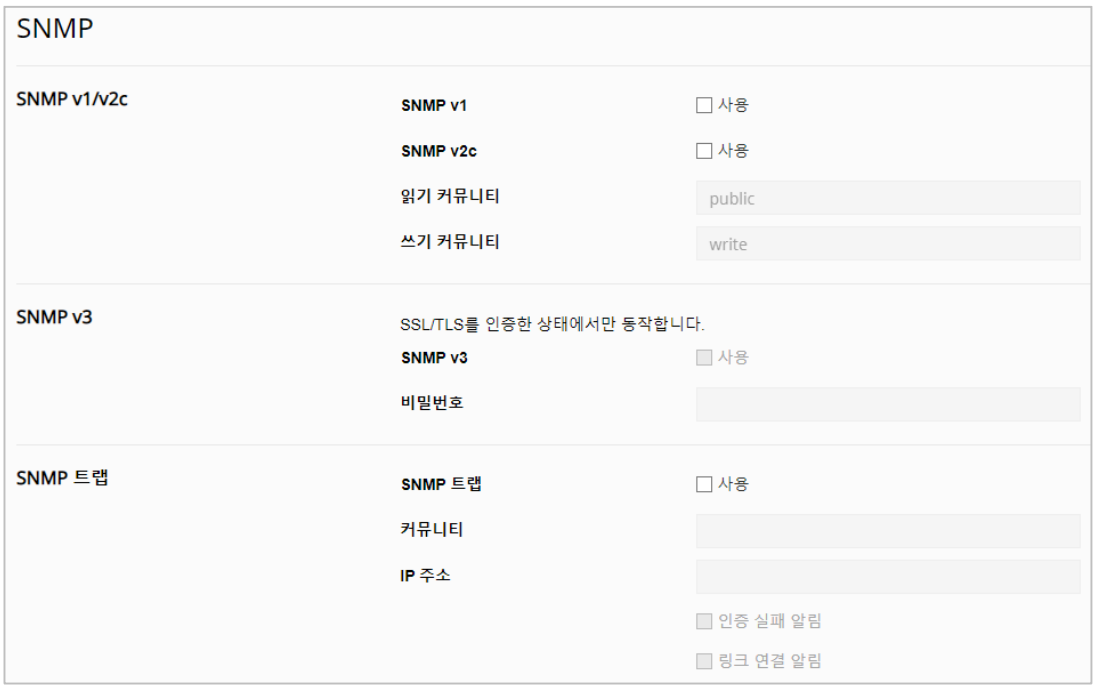
FTP 기능은 알람이나 이벤트가 발생할 경우 카메라에 의해 촬영된 이미지를 설정된 FTP 서버를 통해 전송하기 위한 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 설정된 정보를 모두 삭제합니다.

1) 이벤트 → FTP/E-mail → FTP 설정
2) 설정된 서버 주소, ID, 비밀번호 정보 삭제
3) 적용 버튼 클릭

4.8. 미사용 SNMP 비활성화

한화비전의 기기들은 SNMP v1, v2c 및 v3의 기능을 동시에 지원합니다. SNMP 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 네트워크 → SNMP
2) SNMP v1, v2c 및 v3 선택 해제

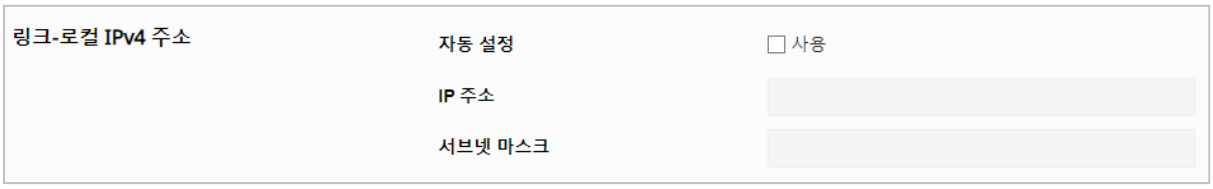


4. 보호 레벨

4.9. 미사용 Link-Local IPv4 주소 비활성화

링크-로컬 IPv4 주소 자동 구성 기능은 DHCP 서버 같은 IP를 할당 받지 못하는 링크-로컬망(같은 스위치에 연결된 카메라와 호스트처럼 하나의 링크로 연결되어 있는 망을 의미)에서 카메라에 169.254.xxx.xxx의 IP를 할당하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 네트워크 → IP 자동 설정 → 링크-로컬 IPv4 주소
2) 자동 설정 사용 체크 해제
3) 적용 버튼 클릭



4.10. 미사용 UPnP 검색 비활성화

UPnP 검색 기능은 UPnP 프로토콜을 지원하는 클라이언트와 운영체제에서 자동으로 카메라를 검색할 수 있도록 지원하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 네트워크 → IP 자동 설정 → UPnP 검색
2) UPnP 검색 사용 체크 해제
3) 적용 버튼 클릭

4. 보호 레벨

4.11. 미사용 Bonjour 비활성화

Bonjour 기능은 Bonjour 프로토콜을 지원하는 클라이언트와 운영체제에서 자동으로 카메라를 검색할 수 있도록 지원하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 네트워크 → IP 자동 설정 → Bonjour
2) Bonjour 사용 체크 해제
3) 적용 버튼 클릭

4.12. 최신 버전의 TLS 사용

TLS는 SSL 프로토콜을 기반으로 개발된 클라이언트-서버 간 안전하고 암호화된 통신 채널을 설정하는데 사용됩니다. TLS는 현재 1.0, 1.1, 1.2, 1.3으로 4개의 버전이 존재하고 있지만, TLS 초기 버전인 TLS 1.0/1.1은 POODLE[2] 및 BEAST[3]와 같은 다양한 공격에 취약합니다.

한화비전은 초기 설정값으로 TLS 1.2/1.3을 제공하고, 필요 시 특정 TLS 버전 추가 옵션을 제공하고 있습니다. 그러나 사용자들이 안전하게 제품을 사용하기 위해서는 TLS 1.0/1.1 선택을 해제하도록 하는 것이 필요합니다.

4.13. 안전한 Cipher Suites 사용

TLS 핸드쉐이크의 Cipher Suites를 통하여 TLS에서 사용하는 인증서 검증 및 비대칭키 교환방식, 대칭키 암호화 및 운용 방식, 메시지 인증에 대한 방식에 대해 클라이언트-서버간 최종 협의를 하게 되며, 구조는 다음과 같습니다.

[2] POODLE 취약점: Padding Oracle On Downgraded Legacy Encryption의 약자로, 구식 암호화 기법을 악용할 수 있게 하는 프로토콜 다운그레이드 취약점

[3] BEAST 취약점: Browser Exploit Against SSL/TLS의 약자로, 앤드 유저 브라우저에서 HTTPS의 쿠키들을 해독하고 효과적인 타킷의 세션을 하이재킹 할 수 있는 취약점

4. 보호 레벨

한화비전은 TLS 1.2/1.3 기준 Cipher Suites를 아래와 같이 제공하고 있습니다.

■ TLS 1.2 Cipher Suites

TLS_RSA_WITH_NULL_MD5	0x00,0x01	Compatible	NULL-MD5
TLS_RSA_WITH_NULL_SHA	0x00,0x02	Compatible	NULL-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	0x00,0x2F	Compatible	AES128-SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	0x00,0x32	Compatible	DHE-DSS-AES128-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	0x00,0x33	Compatible	DHE-RSA-AES128-SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA	0x00,0x34	Compatible	ADH-AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	0x00,0x35	Compatible	AES256-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	0x00,0x38	Compatible	DHE-DSS-AES256-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	0x00,0x39	Compatible	DHE-RSA-AES256-SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA	0x00,0x3A	Compatible	ADH-AES256-SHA
TLS_RSA_WITH_NULL_SHA256	0x00,0x3B	Compatible	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	0x00,0x3C	Compatible	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	0x00,0x3D	Compatible	AES256-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	0x00,0x40	Compatible	DHE-DSS-AES128-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	0x00,0x67	Compatible	DHE-RSA-AES128-SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	0x00,0x6A	Compatible	DHE-DSS-AES256-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	0x00,0x6B	Compatible	DHE-RSA-AES256-SHA256
TLS_DH_anon_WITH_AES_128_CBC_SHA256	0x00,0x6C	Compatible	ADH-AES128-SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256	0x00,0x6D	Compatible	ADH-AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	0X00, 0x9C	Secure/Compatible	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	0X00, 0x9D	Secure/Compatible	AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00, 0x9F	Secure/Compatible	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	0x00,0xBD	Compatible	DHE-DSS-CAMELLIA128-SHA256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC0	Compatible	CAMELLIA256-SHA256
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC3	Compatible	DHE-DSS-CAMELLIA256-SHA256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	0x00,0xC4	Compatible	DHE-RSA-CAMELLIA256-SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0XC0, 0x09	Compatible	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0XC0, 0x0A	Compatible	ECDHE-ECDSA-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0XC0, 0x13	Compatible	ECDHE-RSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0XC0, 0x14	Compatible	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0XC0, 0x2C	Secure/Compatible	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0XC0, 0x23	Compatible	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0XC0, 0x24	Compatible	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	0XC0, 0x27	Compatible	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0XC0, 0x28	Compatible	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0XC0, 0x2B	Secure/Compatible	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0XC0, 0x2F	Secure/Compatible	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0XC0, 0x30	Secure/Compatible	ECDHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CCM_8	0XC0, 0xA3	Secure/Compatible	DHE-RSA-AES256-CCM8
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0XCC, 0xA8	Secure/Compatible	ECDHE-RSA-CHACHA20-POLY1305
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0XCC, 0xA9	Secure/Compatible	ECDHE-ECDSA-CHACHA20-POLY1305

■ TLS 1.3 Cipher Suites

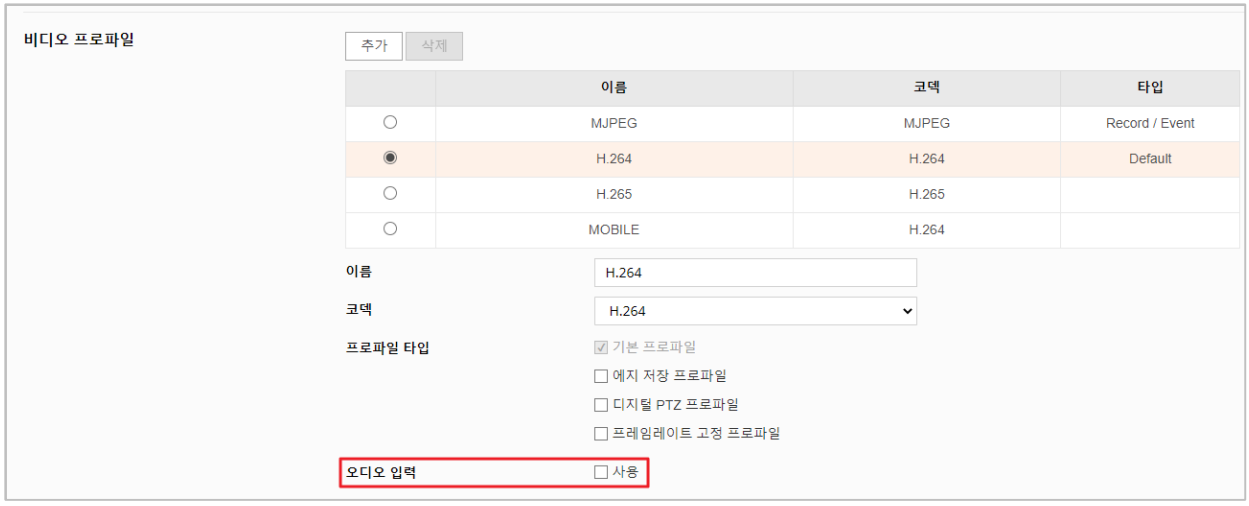
TLS_AES_128_GCM_SHA256	0x13,0x01	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	0x13,0x02	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	0x13,0x03	TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_CCM_SHA256	0x13,0x04	TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256	0x13,0x05	TLS_AES_128_CCM_8_SHA256

4. 보호 레벨

4.14. 미사용 오디오 입력 비활성화

오디오 입력 기능은 영상에 소리를 같이 입력할 수 있도록 하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다. 오디오 입력 기능은 각 비디오 프로파일마다 개별 설정이 가능하므로 이미 설정되어 있는 각 프로파일을 선택하여 선택 해제하도록 하는 것이 필요합니다.

1) 비디오 프로파일 메뉴 이동
2) 설정된 각 비디오 프로파일을 선택한 후 오디오 입력 사용 체크 해제
3) 적용 버튼 클릭



4.15. 미사용 MQTT 비활성화

MQTT(Message Queueing Telemetry Transport)는 카메라가 하나의 장치가 아닌 복수의 장치와 데이터를 쉽게 송수신 할 수 있도록 발행-구독 기반의 메시지 송수신 프로토콜입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 선택 해제하도록 합니다.

1) 이벤트 메뉴 이동
2) MQTT 메뉴 > 클라이언트 설정 > "MQTT 사용" 체크 해제
3) 적용 버튼 클릭

5. 안전 레벨

한화비전은 실제 사용하지 않는 불필요한 서비스나 포트가 열려 있을 경우, 외부로부터 공격 대상이 될 수 있으므로, 사용자가 직접 필요 없는 기능이나 서비스를 사용하지 않도록 설정하여 보안을 향상시킬 수 있습니다.

< 표 5 >

보안 정책	사이버 보안 기능	간략한 설명
-	최신 버전 펌웨어 사용 여부 확인 및 업데이트	최신 버전 펌웨어를 사용하는지 확인하고 보안에 취약한 펌웨어라면 업데이트 수행
-	정확한 날짜/시간 설정하기	로그 분석을 위해 정확한 날짜 및 시간 설정
-	안전한 통신 프로토콜 사용하기(RTSP)	RTSP를 통해 전송되는 영상 보호
-	HTTPS(기기 인증서 사용)	인증서를 통한 기기와 클라이언트간 보안 접속
-	HTTPS(고객 인증서 사용)	
-	기본 포트 변경	포트 변경을 통해 웹 서비스 접근 공격 방지
접근통제	IP 필터링	특정 IP 접속 허가/거부를 통해 접근 공격 방지
-	TLS를 이용한 E-mail 전송	TLS를 이용한 안전한 이메일 전송
서비스 보호	안전하게 SNMP 사용하기	보안강화를 위해 SNMP 초기값 모두 해제
	안전하게 MQTT 사용하기	보안강화를 위해 MQTT 설정 해제
-	관리자 계정 변경/추가 사용자 계정 생성하기	관리자 계정은 변경해서 사용하고, 자주 사용하는 기능은 필요시 최소 권한의 사용자 계정을 생성하여 보안 강화
감사	로그 점검하기	비인가자의 접속 기록 분석
저장데이터 보호	저장데이터 암호화(LUKS 암호화)	저장 데이터의 보호
백업데이터 보호	백업데이터 암호화(ZIP 파일 암호화)	백업 데이터의 보호

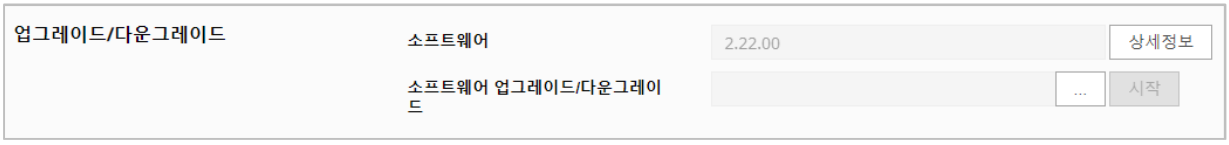
5. 안전 레벨

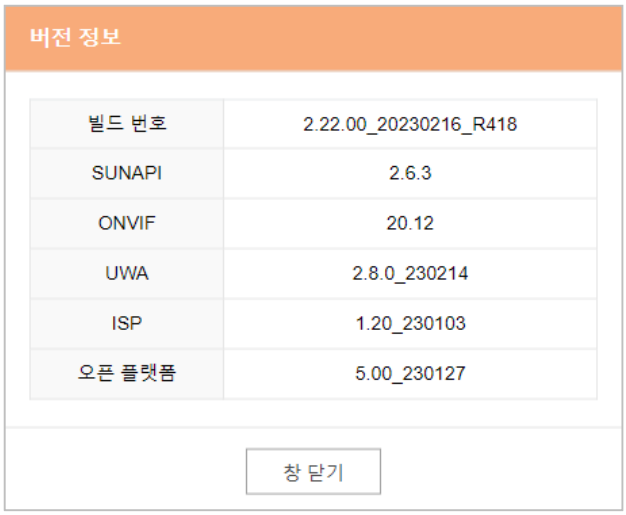
5.1. 최신 버전 펌웨어 사용여부 확인 및 업데이트

한화비전 홈페이지 (www.hanwhavision.com)를 통해 고객이 사용하는 제품의 최신 펌웨어 버전 확인이 가능합니다. 아래 그림에서는 고객이 XND-9082RV 모델을 사용하는 경우 현재 배포된 최신 펌웨어의 버전이 2.22.00이며, 상세정보 버튼을 클릭하면 23년 2월 16일에 배포된 버전임을 확인할 수 있습니다. 그 외 SUNAPI, ONVIF, UWA, ISP, Open platform 관련 버전 정보를 확인할 수 있습니다. 소프트웨어 업그레이드를 위해서는 한화비전 홈페이지에서 해당 제품의 펌웨어를 다운로드 받고, 시작 버튼을 클릭하여 업그레이드를 진행합니다. 소프트웨어 다운그레이드는 최신 보안 패치가 반영되어 있지 않을 수 있으므로 현재 사용하는 제품의 펌웨어 버전이 항상 최신이 될 수 있도록 점검해주시기 바랍니다.

- www.hanwhavision.com → 제품소개 → 제품 상세 페이지 → 펌웨어 다운로드

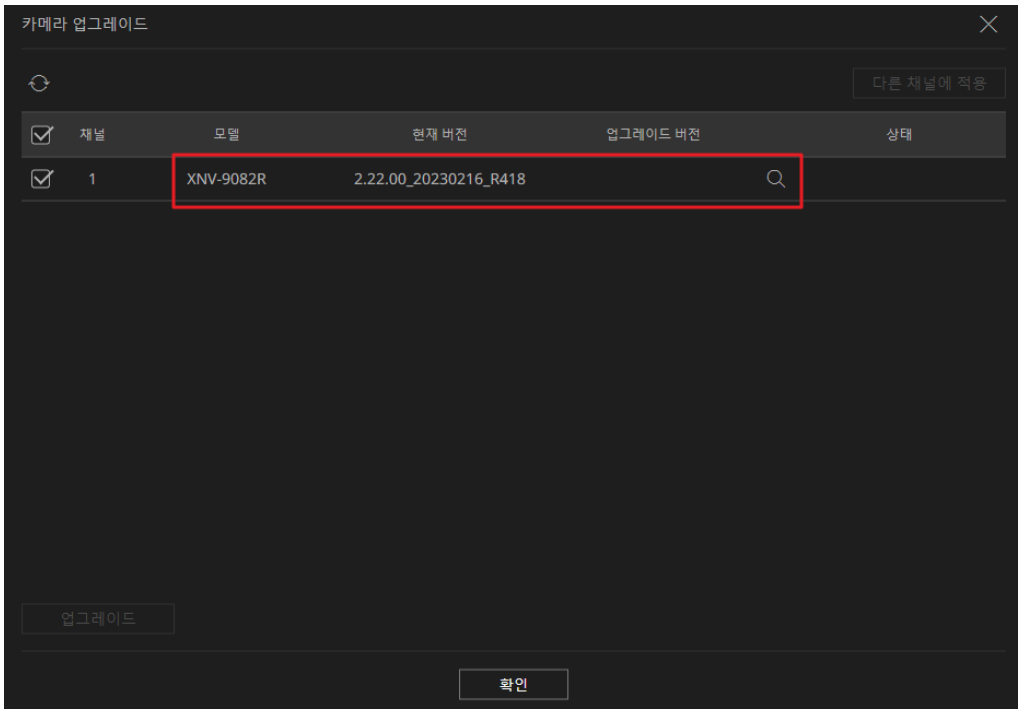
1) 시스템 → 업그레이드/재시작
2) 상세정보 → 제품의 현재 S/W 버전 확인
3) 검색(...) 버튼 클릭하여 다운로드 받은 최신 펌웨어 선택
4) 시작 버튼 클릭



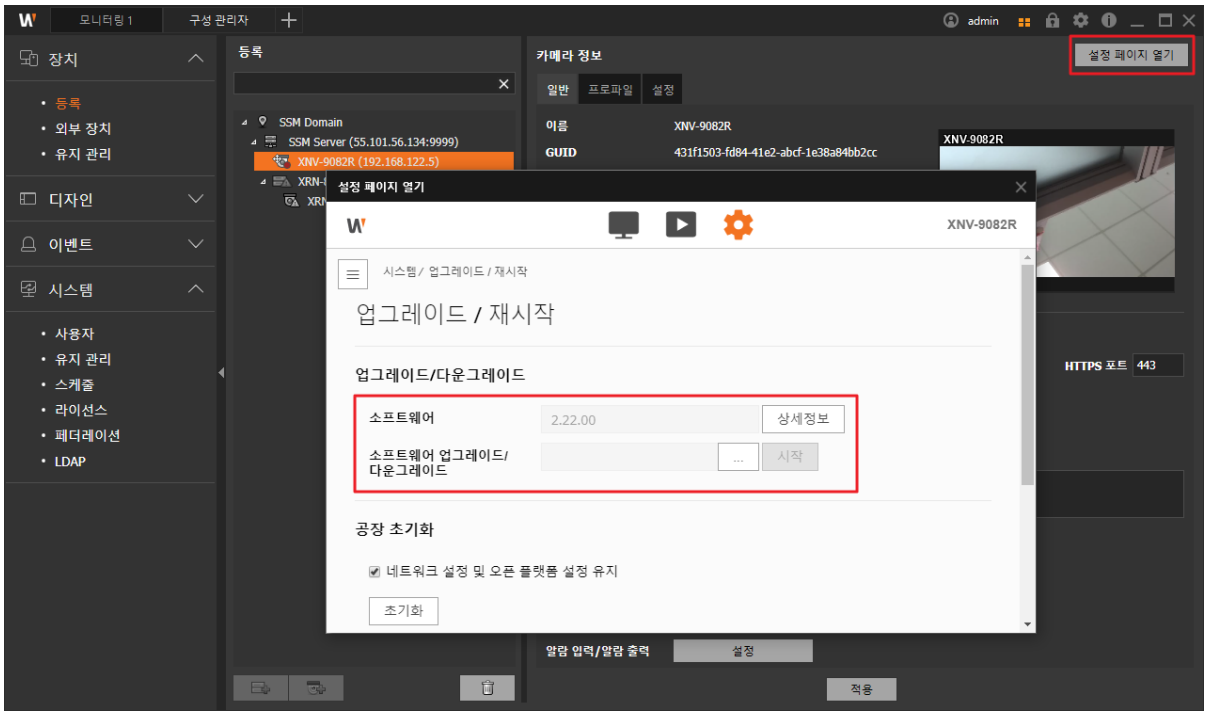


5. 안전 레벨

저장장치 및 SSM에서도 카메라의 펌웨어 정보를 확인 할 수 있고, 최신 펌웨어로 업그레이드가 가능합니다.



<저장장치 화면>



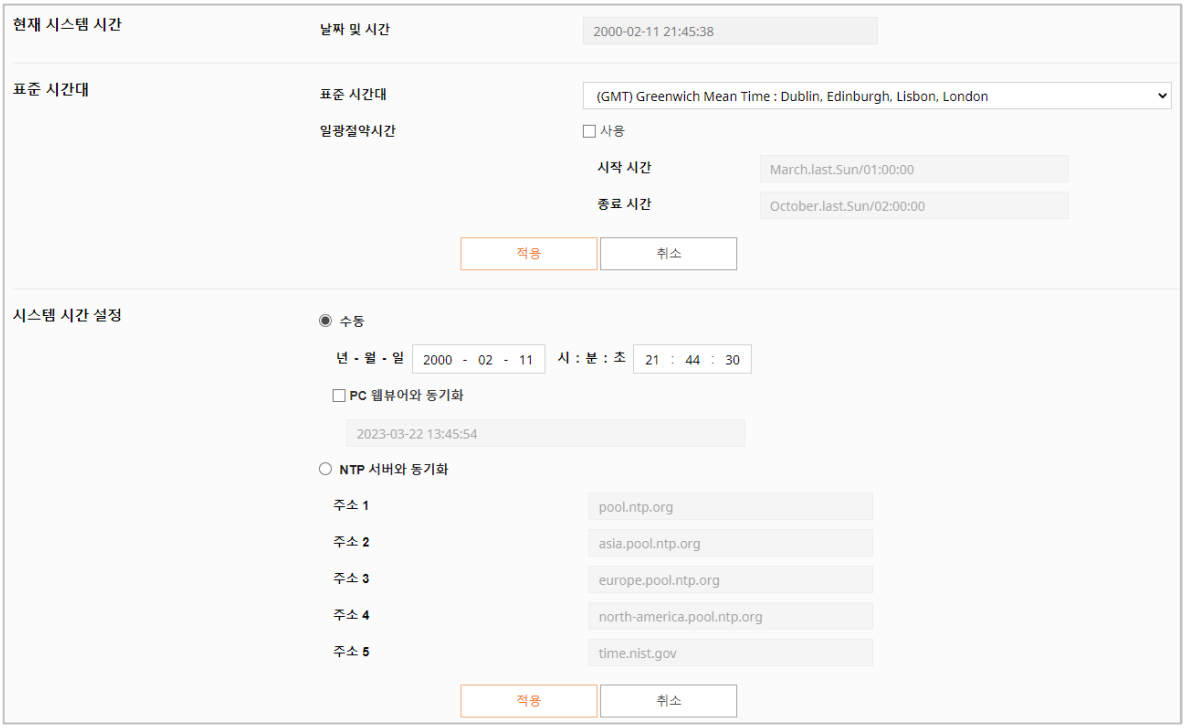
<SSM 화면>

5. 안전 레벨

5.2. 정확한 날짜/시간 설정하기

날짜 & 시간 기능은 기기에서 출력하는 시스템 로그 같은 정보를 분석 시 로그의 정확한 시간 정보를 확인할 수 있도록 하기 위한 전제 조건이므로 현재 시스템의 시간을 정확하게 설정하는 것은 매우 중요한 보안 활동입니다. 설정되어 있는 현재 시스템 시간이 제대로 설정 되어 있지 않은 경우 사용자는 세가지 방법 중 하나의 방법을 선택하여 시스템에 적용될 시간을 설정할 수 있습니다.

1) Basic → 날짜 & 시간으로 이동
2) 표준시(GMT) 기준인 현 거주 지역의 표준 시간대를 설정
   (일광절약시간 사용 옵션은 표준 시간대에서 일광절약시간을 사용하는 지역을 선택할 경우에만 표시되며 해당 기능이 적용되는 경우 선택합니다. 선택 후 적용되면 그 지역의 표준시보다 한 시간 앞당긴 시간으로 설정됨)
3) 표준 시간대의 적용 버튼을 클릭
4) 다음 세가지 방법 중 하나의 방법을 선택하여 시스템에 적용될 시간을 설정
   수동: 수동으로 기기의 현재 시간을 설정
   PC 웹뷰어와 동기화: 현재 웹뷰어를 실행 중인 PC의 시간으로 설정
   NTP 서버와 동기화: 입력된 서버 주소의 시간과 동기화
5) 적용 버튼을 클릭



5. 안전 레벨

5.3. 안전한 통신 프로토콜 사용하기(HTTP)

한화비전의 IP카메라 및 NVR 장치는 서버와 클라이언트간 HTTP+HTTPS 모드를 초기 설정 값으로 제공하고 있습니다. 단, HTTPS 설정 모드는 웹뷰어 상에서 설정된 모드이므로, 웹뷰어 상에서 송수신되는 영상데이터, 사용자 비밀번호 및 ID는 보호 받을 수 있습니다. 또한 사용자가 HTTP 모드로 변경 할 경우, Digest 인증 방식을 적용하고 있어 사용자 비밀번호는 보호 받을 수 있습니다.

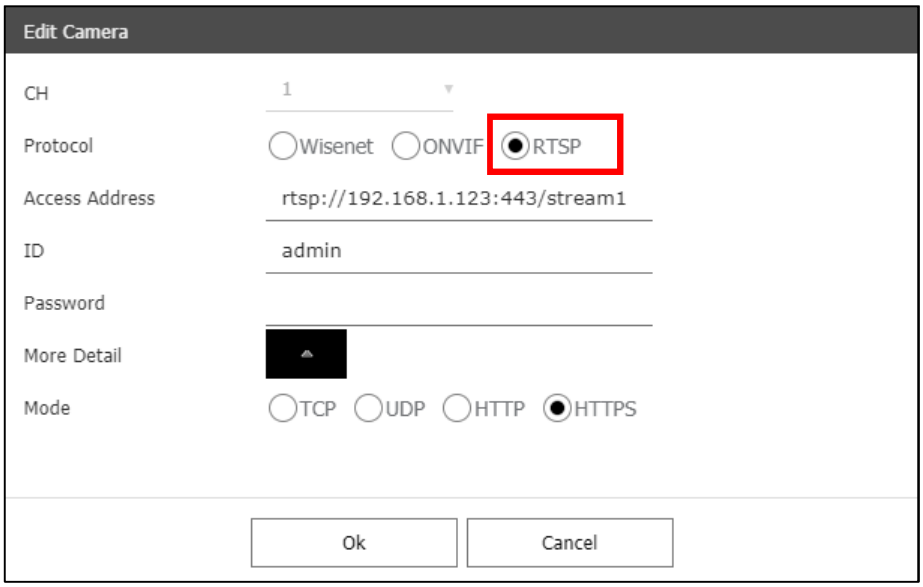
< 표 6 >

통신 연결 모드	사용자 비밀번호 보호	영상데이터 보호	사용 여부
HTTP (Digest 인증)	○	X	HTTPS와 동시 지원
HTTPS	○	○*	사용(초기 설정)

5.4. 안전한 통신 프로토콜 사용하기(RTSP)

HTTPS 모드 이외에도 RTSP를 통해 전송되는 영상 스트리밍도 안전하게 보호되어야 합니다. RTSP를 통한 영상을 보호하기 위해서는 클라이언트단에서 RTSP를 HTTPS로 터널링하는 추가적인 설정 작업이 필요합니다. 예를 들어 IP 카메라에서 NVR로 전송되는 영상을 HTTPS로 보호하고자 할 경우 먼저 IP카메라의 웹뷰어에서 HTTPS 모드로 설정합니다. 그리고 NVR에 카메라를 연결 후 Set UI 또는 NVR의 웹뷰어를 통해 RTSP 모드로 설정합니다.

- 설정(NVR 웹뷰어)
  : 장치 → 카메라 → 카메라 등록 → 채널 선택 → 카메라 수정

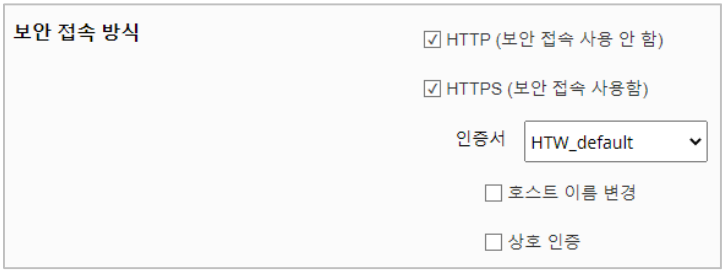


5. 안전 레벨

5.5. HTTPS (기기 인증서 사용)

최초 보안 접속 방식은 HTTP와 HTTPS를 동시에 지원합니다. 기기 인증서는 한화비전에서 제공하는 인증서이며, 기기 인증서로 기기와 클라이언트간의 보안 접속을 할 수 있습니다. HTTPS(보안 접속 사용함)를 선택하고 기기 인증서 "HTW_default" 를 선택하면 보안 접속 모드로 사용할 수 있습니다.

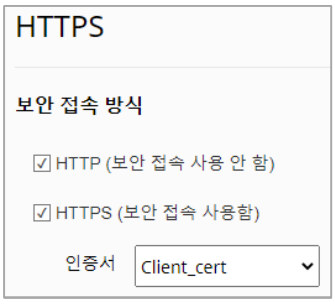
1) 네트워크 → HTTPS → 보안 접속 방식 → HTTPS 선택 → 기기 인증서 선택
2) 적용 버튼 클릭



5.6. HTTPS (고객 인증서 사용)

한화비전에서 제공하는 기기 인증서를 사용하지 않고 고객이 자신의 인증서를 직접 등록하여 기기와 클라이언트간의 보안 접속을 할 수 있습니다. 고객 인증서는 HTTPS(보안 접속 사용함)를 선택하고 등록된 고객 인증서를 선택하면 보안 접속 모드로 사용할 수 있습니다.

1) 네트워크 → 인증서 관리 → 고객 인증서 추가(인증서타입/인증서이름/인증서파일/키파일)
2) 확인 버튼 클릭
3) 네트워크 → HTTPS → 보안 접속 방식 → HTTPS 체크 → 고객 인증서 선택
4) 적용 버튼 클릭

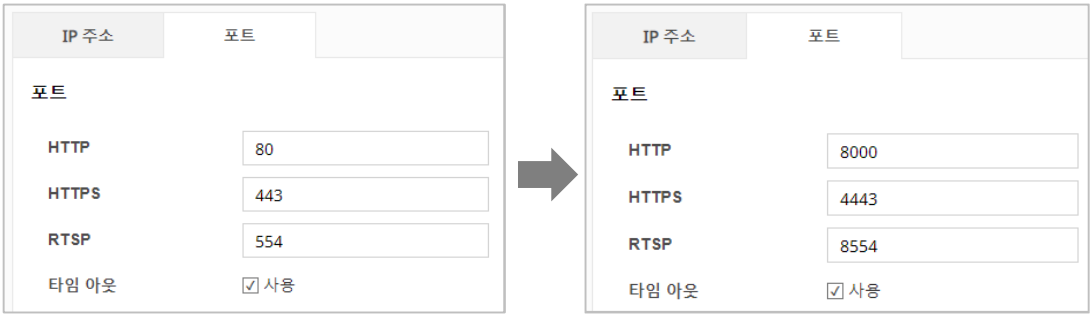


5. 안전 레벨

5.7. 기본 포트 변경

네트워크 장치의 기본 포트를 통해서 스캔하거나 공격하는 경우를 막기 위해서는 일반적으로 잘 알려진 포트를 사용하는 것보다는 사용자가 포트를 재지정하여 사용하는 것이 안전합니다. 보통 제공되는 기본 포트 번호를 더 높은 포트 번호로 변경하도록 합니다. 예를 들어, 웹브라우저를 통해 접근할 수 있는 HTTP 웹서비스 포트를 80이 아닌 8000으로 변경할 경우 단순한 스캔 프로그램이나 웹브라우저에 주소를 직접 입력하는 공격으로부터 웹서비스 접근을 보호할 수 있습니다.

1) Basic → IP & 포트 → 포트
2) HTTP 포트와 HTTPS 포트를 각각 80과 443에서 상위 포트로 설정 변경
3) RTSP 포트와 장치 포트를 각각 554와 4520에서 상위 포트로 설정 변경
4) 적용 버튼 클릭



※ 포트 재지정 시 연결되어 있는 저장장치나 VMS와 연결 문제가 발생할 수 있으므로 해당 연결 장비의 설정 변경도 필요합니다. 문제가 해결되지 않을 경우 기본 포트로 복구하시기 바랍니다.

5. 안전 레벨

5.8. IP 필터링

특정 IP에 대해서 접속을 허가 또는 거부하도록 IP 목록을 작성할 수 있습니다.

1) 네트워크 → IP 필터링
2) 필터링 형식 선택
   - 등록된 IP 접근 제한: 필터링에 등록된 IP의 접근 차단
   - 등록된 IP 접근 허용: 필터링에 등록된 IP만 접근 허용
3) 추가 버튼 클릭하면 IP 목록창 생성

4) 제한 또는 허용할 IP 입력. IP 주소 및 Prefix를 입력하면 오른쪽의 필터링 범위 항목에 차단 또는 허용되는 IP 주소 범위가 표시됨

5) 설정 완료 후 적용 버튼 클릭

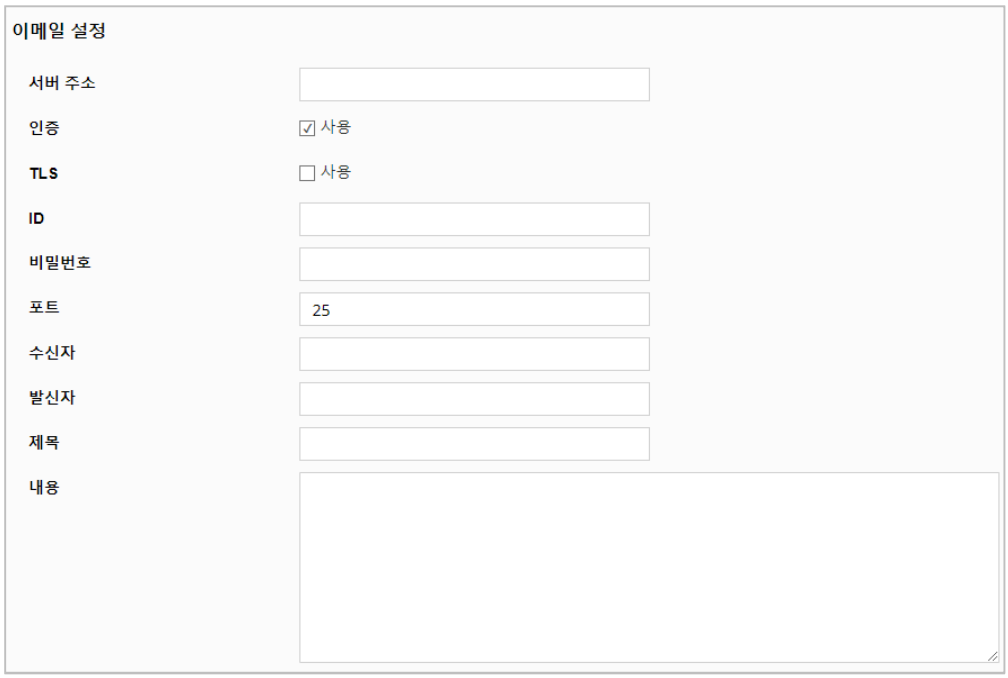
※ *IP 필터링에서 허가를 선택하고 IPv6를 사용함으로 설정한 경우, 현재 설정 중인 PC의 IPv4와 IPv6 주소를 모두 등록해야 합니다. 현재 설정 중인 PC의 IP는 제한으로 등록할 수 없고 허용으로 등록해야 하며, 이 후 설정한 IP들만 접속 가능합니다.*

5. 안전 레벨

5.9. TLS를 이용한 E-mail 전송

카메라에서는 알람이나 이벤트가 발생할 경우 촬영된 이미지를 이메일을 통해 전송할 수 있는 기능이 있습니다. 이 기능을 사용 시 TLS 모드를 사용하면 카메라로부터 메일 서버까지 안전한 이메일 전송이 가능합니다.

1) 이벤트 → FTP/E-mail → 이메일 설정
2) 서버 주소에 알람 및 이벤트 이미지를 전송할 이메일 서버의 IP 주소 입력
3) 인증 사용과 TLS 사용을 사용함으로 설정
4) 이메일 서버에 로그인하기 위해 접속할 사용자 계정 ID와 비밀번호 입력
5) TLS를 사용하지 않는 이메일 서버 포트의 초기값은 25이지만 TLS를 사용할 경우 해당 포트는 465로 설정됨
6) 수신자에 이메일 수신자 주소를 입력, 발신자에 이메일 발신자 주소 입력
   ※ 발신자 주소가 정확하지 않을 경우 이메일 서버가 해당 발신자의 이메일을 스팸 메일로 분류해 전송되지 않을 수도 있습니다.
7) 이메일 제목과 이메일 내용을 입력한 후 적용 버튼 클릭. 이메일 전송 시 알람 및 이벤트 이미지가 첨부 파일로 전송됨



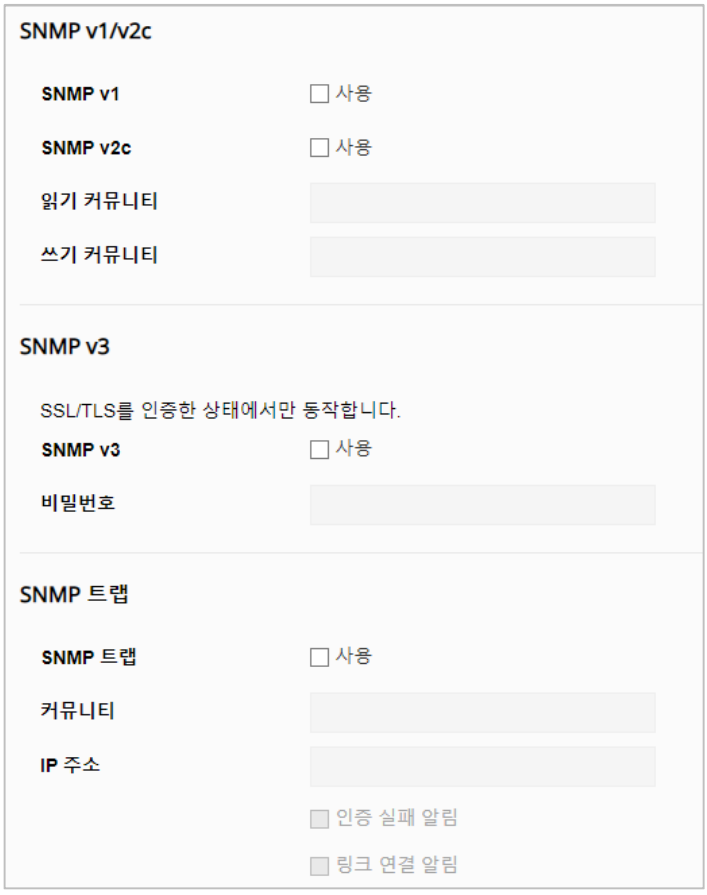
5. 안전 레벨

5.10. 안전하게 SNMP 사용하기

SNMP는 네트워크 디바이스를 편리하게 관리할 수 있는 기능을 제공합니다. 기본적으로 한화비전은 보안강화를 위해 선택이 모두 해제되어 있습니다. 안전하게 SNMP를 사용하기 위해서는 SNMP v3로만 설정하여 사용하는 것이 바람직합니다. SNMP v3로 사용하고자 하는 경우 HTTPS 설정이 전제 조건이며, 앞 절의 HTTPS (보안 접속 사용함)가 이미 설정되었을 경우 다음 과정 중 1)~3)은 생략 가능합니다.

SNMP v1 및 v2c는 평문으로 된 커뮤니티 문자열을 통해 SNMP 기능이 제공되므로 보안에 취약하여 사용을 지양합니다.

1) 네트워크 → HTTPS → 보안 접속 방식
2) HTTPS (보안 접속 사용함) 선택
3) 적용 버튼 클릭
4) 네트워크 → SNMP
5) SNMP v1와 SNMP v2c의 사용 선택 해제
6) SNMP v3 사용 선택 및 비밀번호 설정(HTTPS 모드 변경 후 v3 선택 가능)

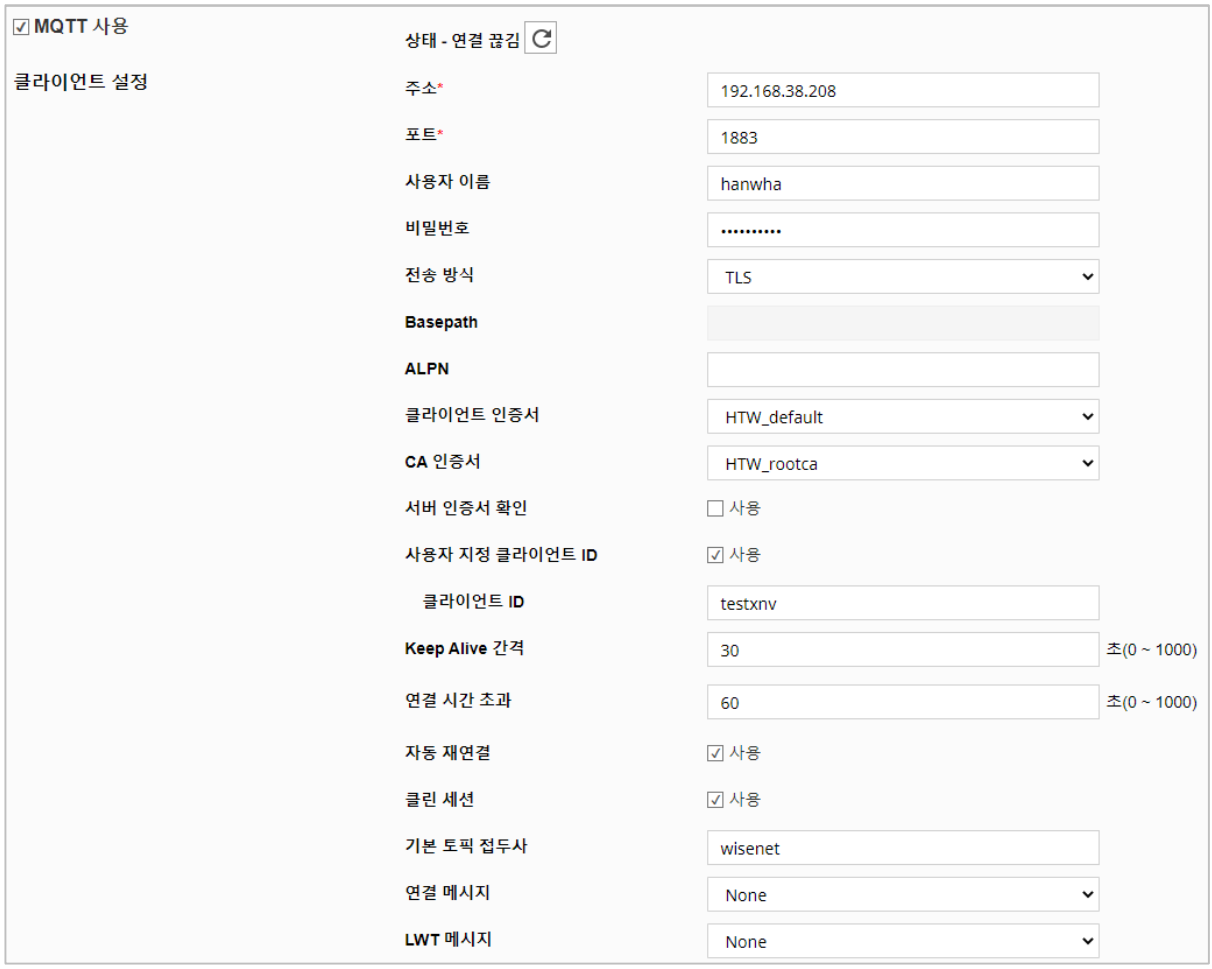


5. 안전 레벨

5.11. 안전하게 MQTT 사용하기

MQTT는 카메라가 여러대의 장치와 데이터를 송수신 할 수 있게 해주는 기능입니다. 안전하게 MQTT를 사용하기 위해서는 클라이언트 설정 시 TLS 전송방식을 설정하여 사용하는 것이 보안에 안전합니다.

1) 이벤트 → MQTT → 클라이언트 설정
2) 주소, 포트, 사용자 이름, 전송방식(TLS), 사용자 지정 클라이언트 ID(사용체크), 클라이언트 ID, Keep Alive 간격, 연결 시간 초과, 자동 재연결, 클린 세션, 기본 토픽 접두사 설정
3) 적용 버튼 클릭

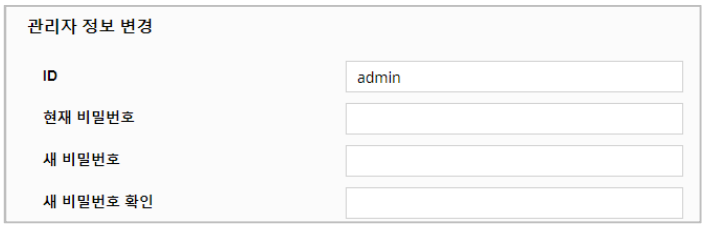


5. 안전 레벨

5.12. 관리자 계정 변경 및 추가 사용자 계정 생성

초기 관리자 계정인 "admin"으로만 기기에 접근하여 사용 시 관리자 비밀번호가 네트워크를 통해 지속적으로 전송될 수 있어, 악의적인 목적으로 네트워크를 지속적으로 모니터링하는 사람에게 중요 자격 정보가 노출되는 보안 취약점이 발생할 수 있습니다. 때문에, 관리자 계정은 변경해서 사용하는 것이 안전합니다. 또한 관리자는 사용자에게 자주 사용하는 설정 기능을 포함한 관리자 권한을 부여할 수 있는데, 이는 보안 취약할 수 있으므로, 반드시 필요한 사용자에 한하여 최소한의 권한을 부여해야 합니다.

1) Basic → 사용자 → 관리자 정보 변경 → ID/비밀번호 변경
2) 적용 버튼 클릭



1) Basic → 사용자 → 접속자 정보
2) 추가할 계정을 선택하면 설정할 수 있는 항목 활성화 됨
3) 사용에 체크 후 이름, 비밀번호 설정
4) 관리자 권한, 프로파일, 비디오, 포커스, 카메라, 오디오 입력/출력, 알람 출력 사용 여부 선택
5) 프로파일을 선택한 후 적용 버튼 클릭 (전체로 설정 시, 모든 프로파일의 영상 이용 가능)

5. 안전 레벨

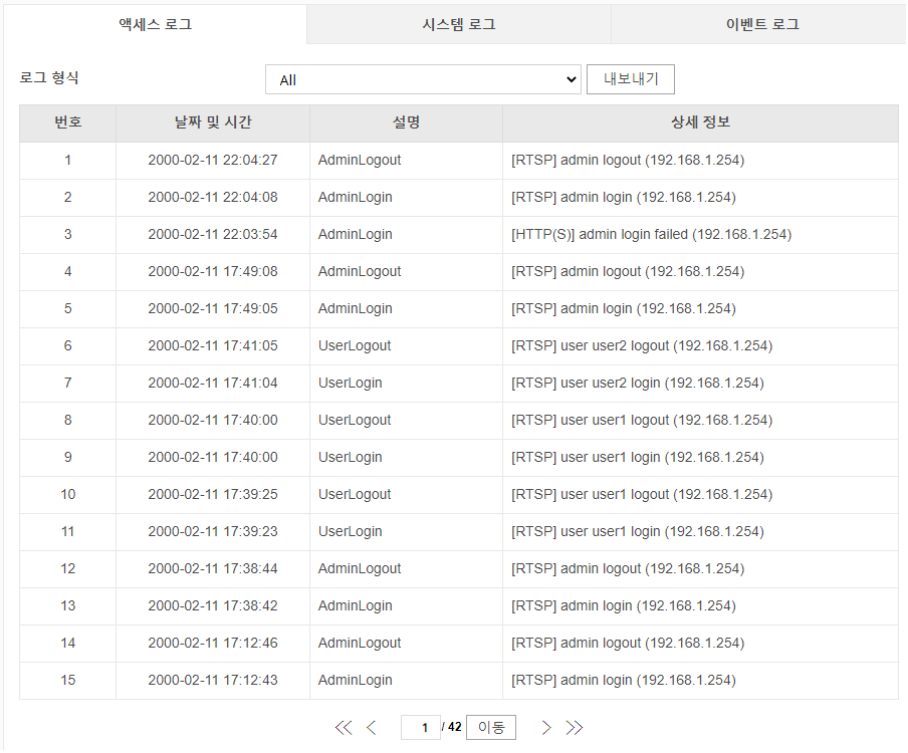
5.13. 로그 점검하기

기기에 비인가자가 악의적인 목적으로 접근하였을 경우의 흔적을 찾기 위해 관리자는 시스템에 저장되어 있는 로그를 분석할 수 있습니다. 해당 로그를 통해 기기 접근/시스템 설정 변경/이벤트 등의 다양한 정보를 확인할 수 있으며, 기기를 포함한 네트워크 시스템의 보안을 높일 수 있는 중요한 자료로 활용할 수 있습니다. 로그 데이터의 점검 및 분석이 필요한 이유는 다음과 같습니다.

. 시스템에서 발생하는 모든 문제(오류 및 보안 결함 포함)가 기록되고 유일한 단서가 됩니다.
. 시스템에서 발생한 오류 및 보안 결함 검색이 가능합니다.
. 잠재적인 시스템 문제를 예측하는데 사용될 수 있습니다.
. 장애 발생시 복구에 필요한 정보로 활용할 수 있습니다.
. 침해 사고 발생시 근거 자료로 활용할 수 있습니다.
. 각종 법규 및 지침에서 로그 관리가 의무화되고 있습니다.

예를 들어, 비밀 번호 입력이 연속으로 실패하는 경우 계정이 잠길 수 있는데 액세스 로그(Access Log) 검색을 통해서 대량의 로그인 실패 또는 계정 잠김 같은 이러한 유형의 공격을 확인할 수 있습니다.

- 설정(IP 카메라)
  : 시스템 → 로그 → 액세스 로그/시스템 로그/이벤트 로그



5. 안전 레벨

5.14. 저장데이터 암호화(LUKS 암호화)

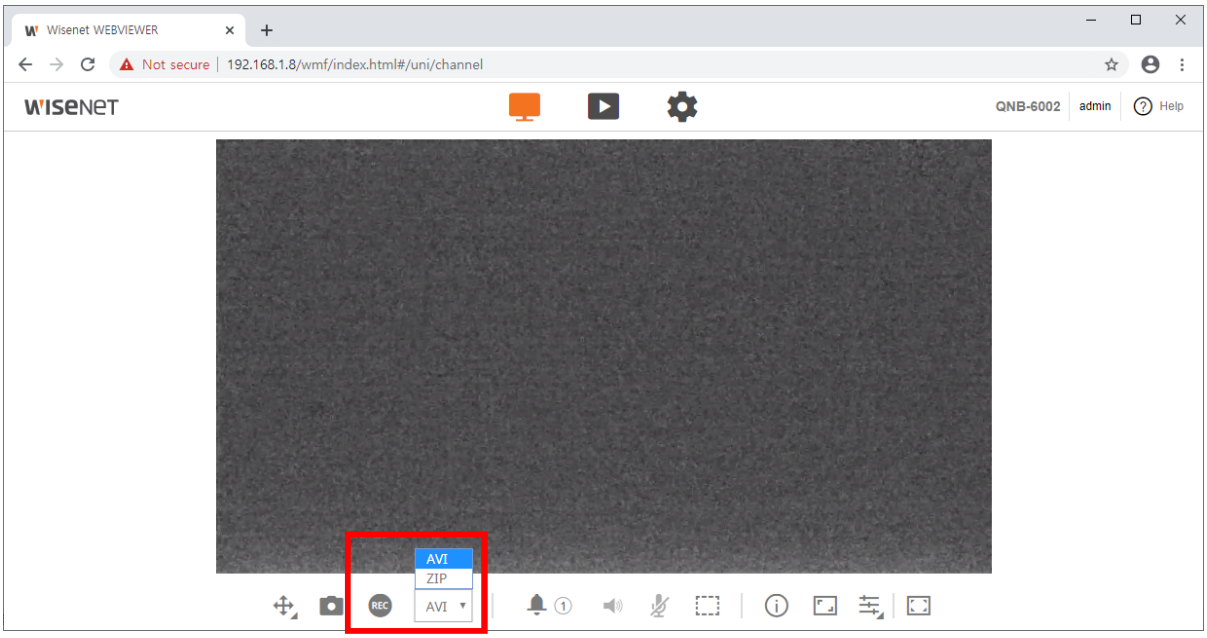
저장데이터 암호화 기능은 SD카드에 저장된 데이터들이 유출이 되어도 확인할 수 없도록 암호화 하는 기능입니다. 초기값은 비활성화 되어 있으므로, SD카드에 데이터 저장 시 해당 설정을 활성화 하여 사용합니다. 사용시 비밀번호는 필수로 요구됩니다. SD카드 암호화 기능 설정 변경 시에도 설정한 비밀번호는 필수로 요구되며, 비밀번호 분실 시에는 SD카드를 포맷 후 새로 사용해야 하므로 비밀번호의 안전한 관리가 필요합니다.

5. 안전 레벨

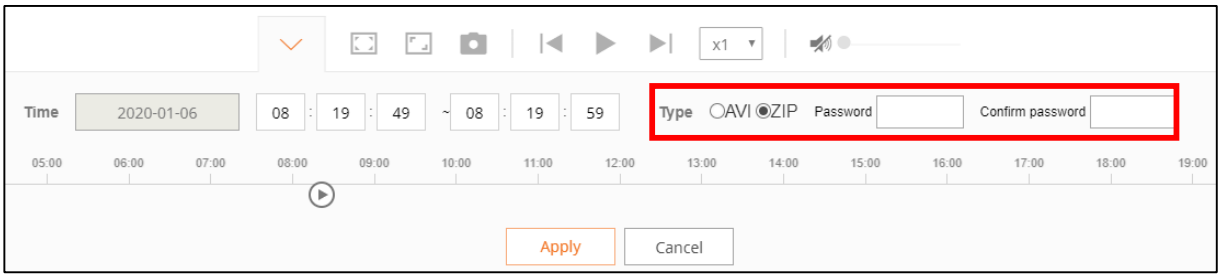
5.15. 백업데이터 암호화(ZIP 파일 암호화)

SD카드에 저장된 데이터를 외부로 추출할 때나 라이브 영상을 녹화 시, 백업 파일은 AVI 또는 ZIP파일로 설정 할 수 있습니다. AVI로 설정할 경우 암호화 되지 않아 중요 정보들이 노출될 수 있으나, ZIP 파일로 설정하면 암호화를 할 수 있어 노출을 막을 수 있습니다. ZIP 파일 암호화 시 비밀번호 입력이 필요하며, 비밀번호를 입력하지 않을 경우 ZIP 파일 암호화가 적용되지 않습니다.

- 라이브 화면에서 영상 녹화 시



- Playback 화면에서 영상 백업 시



6. 최상위 안전 레벨

한화비전 기기에서 제공하는 보안 기능과 외부 추가 보안 솔루션을 연동하여 보안을 향상시킬 수 있습니다.

< 표 7>

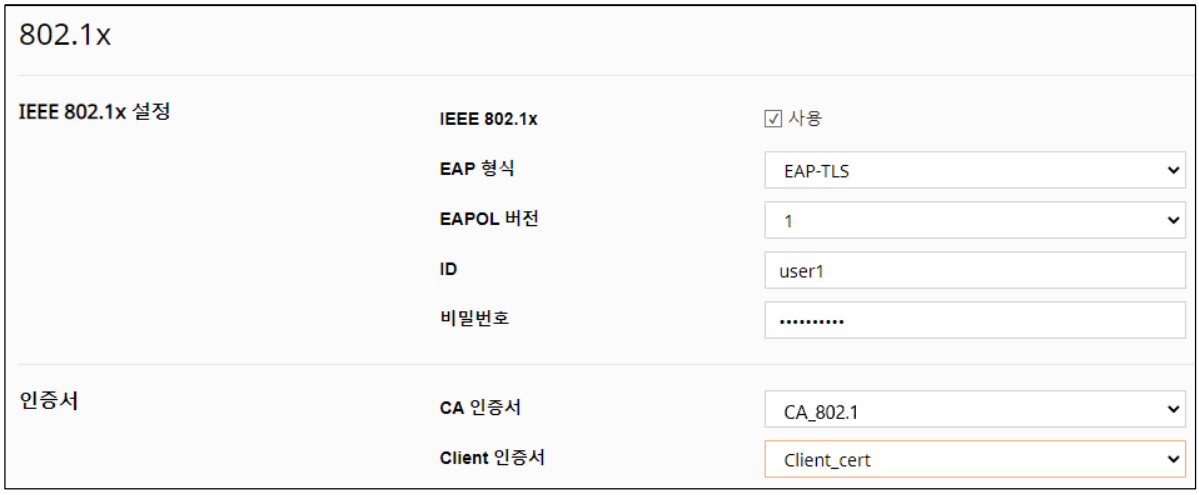
보안 정책	사이버 보안 기능	간략한 설명
-	802.1X 인증서 기반 접근 제어	포트 기반 접근 제어 설정으로 보안 환경 강화

6. 최상위 안전 레벨

6.1. 802.1x 인증서 기반 접근 제어

네트워크 스위치, 브리지, 무선 엑세스 포인트(AP) 등에 연결된 네트워크 기기들에 대해 포트 기반의 접근 제어를 설정하면 더 강력한 네트워크 보안 환경을 구성할 수 있습니다. 한화비전 카메라에서 지원하는 802.1x는 인증서를 필요로 하는 표준 방식 EAP-TLS를 사용합니다. 이 기능을 사용하고자 할 경우 802.1x를 지원하는 네트워크 스위치(또는 브리지, 무선 AP 등)와 802.1x 인증 서버, 기기별 인증서 및 개인키가 필요하며 인증서 등록은 '인증서 관리' 페이지에서 설치합니다.

1) 네트워크 → 802.1x → IEEE 802.1x
2) IEEE 802.1x 사용함 선택
3) EAP 형식을 EAP-TLS로 설정, EAPOL 버전을 1또는 2로 설정
4) 클라이언트의 인증서 ID와 개인키 비밀번호 입력
※ 암호화되지 않은 개인키 파일을 사용하는 경우 입력하지 않아도 됩니다.
5) 인증 서버를 통해 발급한 CA 인증서 및 설치된 클라이언트 인증서 선택
※ 설치된 인증서와 개인키는 RADIUS 서버와 Client 기기간의 TLS 통신에만 사용됩니다.
6) 적용 버튼 클릭



판교 R&D센터
13488 경기도 성남시 판교로 319번길 6(삼평동)
TEL 1588.5772 www.hanwhavision.com