WISENET

White paper

네트워크 장비 보안 강화 가이드

(NVR)

2020. 7. 24

V1.0

Hanwha Techwin

Contents

개정이력

버전	개정일자	개정내용	비고
V1.0	2020.7.24	공식 버전 제정	

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.

한화테크윈은 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 Secure by Design으로 사용자가 별도의 설정 없이 기기 자체에서 기본으로 제공되는 기능만으로도 달성할 수 있는 보안 수준을 의미합니다.
- 보호 레벨은 Secure by Default로 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	-
	연속 비밀번호 실패 시 입력 제한	Default	-
	원격서비스 (Telnet, SSH) 미사용	Default	-
	암호화 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 인증)	Default	-
보호 레벨	공장초기화 수행하기	-	-
	미사용 멀티캐스트 비활성화	비활성화	-
	미사용 DDNS 비활성화	Off	-
	미사용 SNMP 비활성화	비활성화	-
	오디오 사용 기능 해제	미사용	-

2. 사이버 보안 레벨 정의

사이버 보안 레벨	사이버 보안 강화 기능 & 방안	초기 설정	추천 설정
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 (사설 인증서 사용)	HTTP	HTTPS(사설인증서사용)
	HTTPS (공인 인증서 사용)	HTTP	HTTPS(공인인증서사용)
	기본 포트 변경하기	초기값	변경
	IP 필터링	미설정	설정
	안전하게 SNMP 사용하기	미설정	SNMP v3
	추가 사용자 계정 생성하기	-	설정
	권한 설정	-	설정
	로그 점검하기	-	-
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

한화테크윈에서 제공하는 기기들은 Secure by Design으로 개발되어, 기기 자체에서 기본으로 제공되는 기능만으로 사이버 보안의 위협으로부터 안전을 보장받을 수 있습니다.

< 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
접근제어	연속 비밀번호 실패 시 입력 제한	웹 UI 로그인 시 비인가 자로부터의 비밀번호 무작위 입력 공격 차단
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 인증	기기인증서를 이용한 암호화 통신 시 신뢰할 수 있는 기기 식별

3.1. 복잡한 비밀번호 설정 강제

한화테크윈 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. 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 한화테크윈의 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.

3.3. 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 한화테크윈의 제품은 A/S의 편의성을 포기하고 이러한 리스크를 과감히 제거하는 정책을 채택하여 보안 수준을 향상시켰습니다.

3.4. 환경 설정 정보 암호화

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

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

3.5. 펌웨어 암호화 및 안전한 업데이트

한화테크윈의 제품은 기능추가/버그개선 및 보안 업데이트 등을 위한 펌웨어를 제공 시 암호화된 펌웨어를 한화테크윈의 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. 한화테크윈의 제품은 이러한 펌웨어의 보안과 안전한 업데이트를 위해 기밀성 및 무결성이 보장된 펌웨어를 배포하고 있습니다.

3.6. 추출된 비디오 포맷의 워터마킹과 암호화

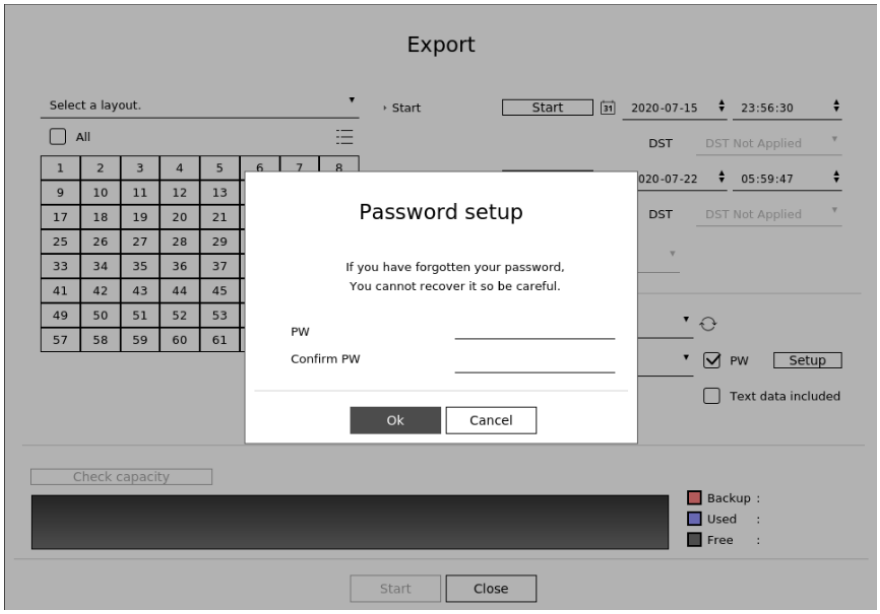
한화테크윈의 NVR을 사용하여 SEC 파일 포맷으로 추출한 비디오 파일은 일반 재생/편집용 소프트웨어로 파일 열기가 불가능하여 무분별한 유노출을 예방하고 있으며, 워터마킹을 적용하여 영상 위변조 검출이 가능합니다. 기본적으로 재생에 필요한 플레이어가 SEC 파일에서 자동으로 추출되어 별도로 플레이어를 설치할 필요가 없으며 사용자가 SEC 파일을 더블 클릭함으로써 간단하게 비디오 파일을 재생시킬 수 있습니다.

또한, SEC 파일 포맷은 비디오 파일을 법적 증거 또는 개인정보 보호 목적으로 변조 여부 확인 및 기밀성을 보장할 수 있습니다.

< 표 3 >

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

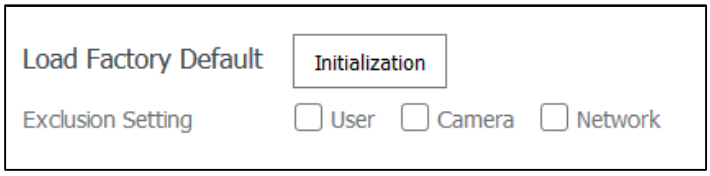
- 설정(NVR 세트 설정)
  : 검색 → Export 선택 → 채널/시간정보 입력 → 디바이스 설정 → 저장타입(SEC) 설정→ 비밀번호 체크박스 체크 → 비밀번호 설정



3.7. 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. 한화테크윈의 기기는 이러한 악의적인 로그 삭제나 기기 초기화를 통한 로그 초기화가 되지 않도록 하고 있습니다. 즉, 다음과 같이 공장초기화를 실행하더라도 저장장치에 저장된 로그는 절대로 초기화가 되지 않습니다.

- 설정(NVR)
  : 시스템환경 → 시스템관리 → Settings → 초기화 설정



3.8. HTML5 스트리밍 기반 NonPlug-in 웹뷰어

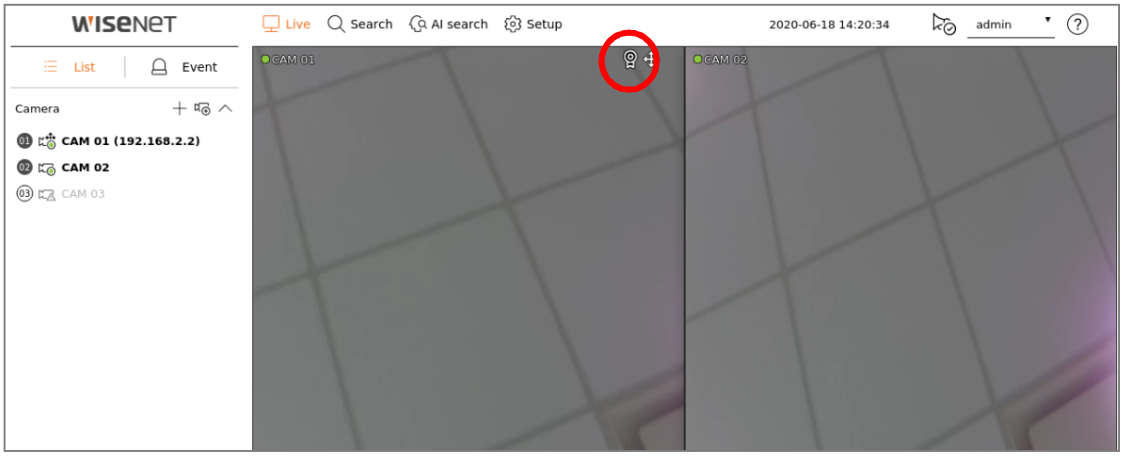
사용자는 NVR에서 제공하는 영상을 별도의 클라이언트 설치 없이 범용 브라우저를 통해 편하게 확인 할 수 있습니다. 업계 대부분의 웹뷰어는 브라우저에 설치되는 Plug-in(ActiveX, 실버라이트, NPAPI) 기술을 이용하여 영상 스트리밍 서비스를 제공하고 있습니다만, 이러한 Plugin-in 기술은 사용자 환경에 설치되는 구조로써 사용자 리소스에 대한 보안 취약점이 발생될 소지가 높아 최근 ActiveX 보안 취약점에 따른 악성코드 감염 사례가 빈번히 발생하고 있습니다. 이에, 브라우저 업체들은 Plug-in 설치 지원을 중단하였으며,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

3.9. 개별장치인증

한화테크윈에서 제공하는 네트워크 기기는 암호화 통신 시 기기인증서를 이용한 기기 식별 기능이 탑재되어 있습니다. 이를 통해 한화테크윈에서 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. 즉, 한화테크윈에서 제조한 카메라와의 연결 시, 저장장치는 카메라와 암호화 통신 수행과 동시에, 아래와 같이 기기에 대한 검증을 수행하고 신뢰된 장비임을 증명합니다.

- 기기인증(NVR) – 세트에서 확인 가능

  : 세트 연결 후 Live 화면에서 기기인증서 아이콘 확인



또한, 당사 장비간의 연결이 아닌 웹뷰어(웹브라우저) 연결에 대해서도 기기인증을 적용 할수 있도록 "한화테크윈의 Private Root CA 인증서 사전 설치가이드"를 배포/안내 하고 있습니다.

설치 가이드는 당사 홈페이지에서 확인 가능합니다.

- 한화테크윈 Private Root CA 사전 설치 가이드 (https://www.hanwha-security.com/ko/technical-guides/cybersecurit/)

4. 보호 레벨

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

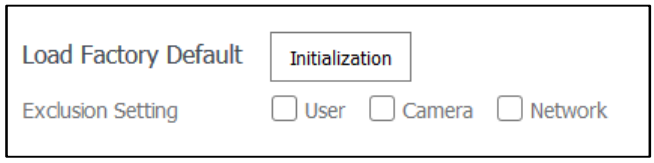
< 표 4 >

보안 정책	사이버 보안 기능	간략한 설명
서비스 보호	공장 초기화	기기에 저장된 기존 정보들을 초기화
	미사용 멀티캐스트 비활성화	최초 활성화 되는 서비스를 최소화 하여 악의적인 공격 방지
	미사용 DDNS 비활성화	
	미사용 SNMP 비활성화	
	오디오 사용 기능 해제	

4.1. 공장초기화

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

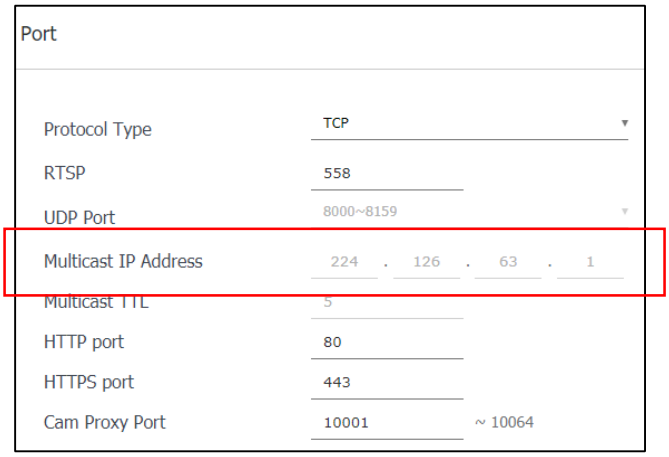
- 설정(NVR)
  1) 시스템환경 → 시스템관리 → Settings → 초기화 설정
  2) User/Camera/Network 설정 선택 해제
     (해당 설정을 선택 해제 하지 않을 경우 해당 항목의 설정값이 유지되고 시스템 설정이 초기화 됨)
  3) 초기화 버튼 클릭



4.2 미사용 멀티캐스트 비활성화

멀티캐스트 사용을 지정하는 기능으로 RTSP 프로토콜에 대해 설정을 할 수 있습니다. 이 서비스는 기본 설정값이 비활성화 되어 있습니다. 해당 서비스가 필요 없다면 보안 강화를 위해 비활성화 상태로 유지하는 것이 좋습니다.

- 설정(NVR)
  1) 설정 → 네트워크 → 포트 → 멀티캐스트
  2) 멀티캐스트(RTSP)의 비활성화 유지



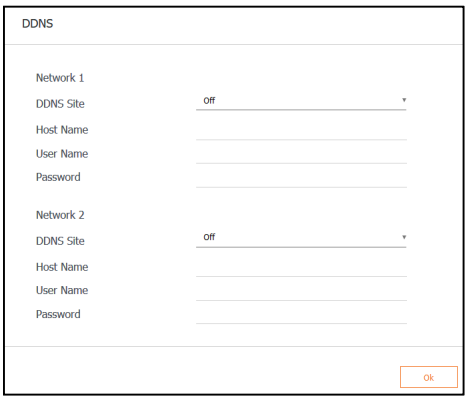
4.3. 미사용 DDNS 비활성화

저장장치가 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.

- 설정(NVR)

1) 네트워크 → DDNS → 사용 안함 선택

2) 확인 버튼 클릭



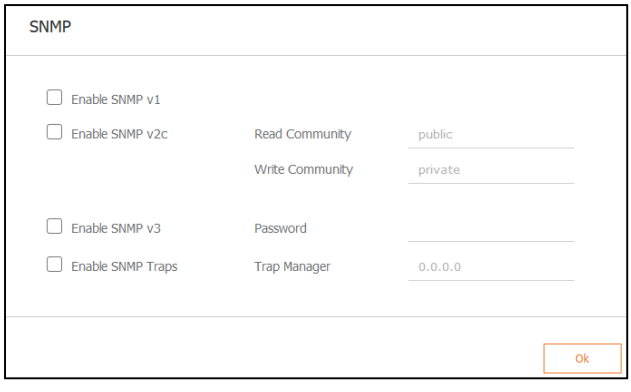
4.4. 미사용 SNMP 비활성화

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

- 설정(NVR)

1) 네트워크 → SNMP

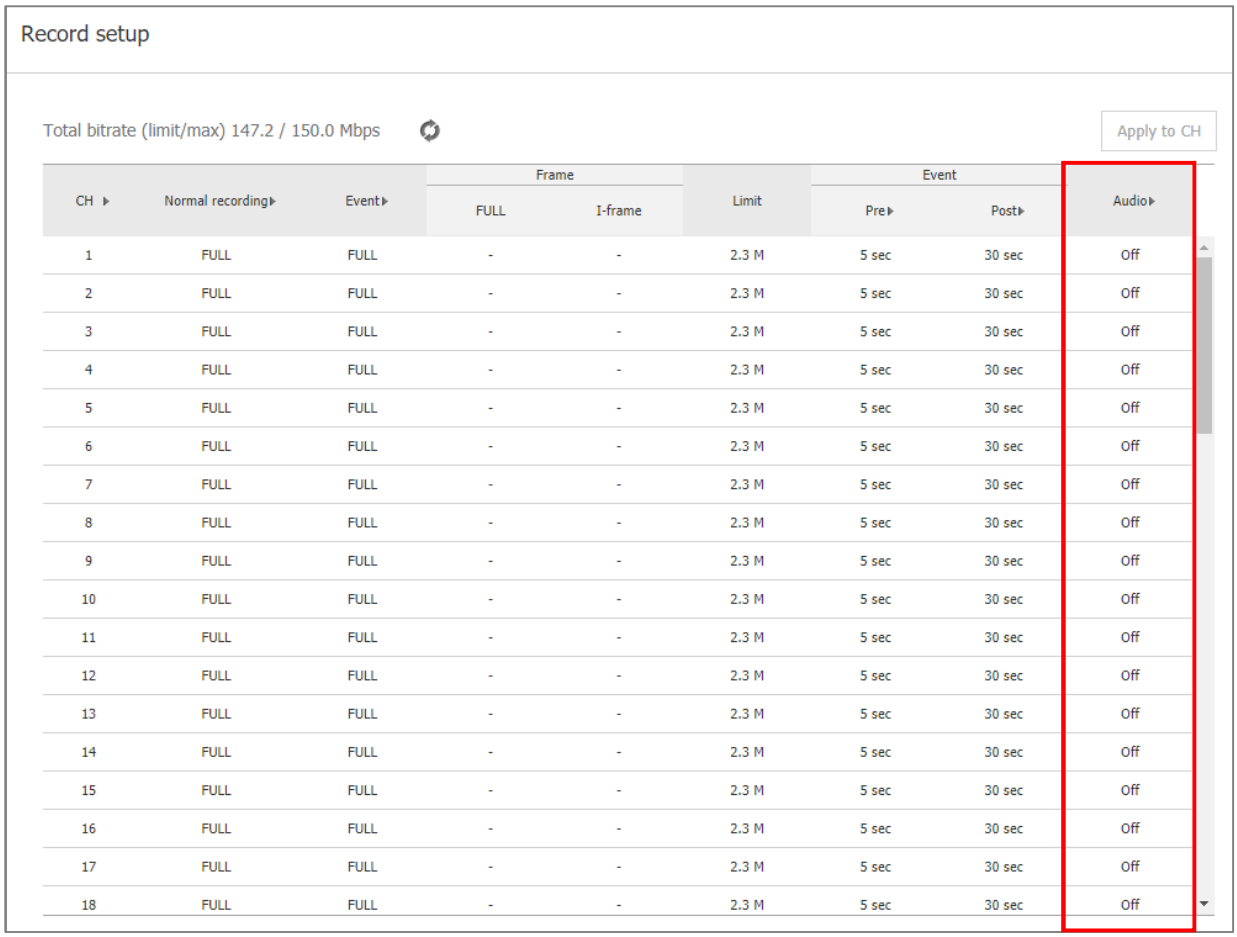
2) SNMP v1, v2c 및 v3 선택 해제



4.5. 오디오 사용 기능 해제

오디오 사용 기능은 영상에 소리를 같이 입력할 수 있도록 하는 기능입니다. 해당 서비스가 불필요하다고 생각되면 보안 강화를 위해 서비스 기능의 설정을 해제 하도록 합니다. 오디오 사용 기능은 각 채널 녹화파일마다 개별 설정이 가능하므로 이미 설정되어 있는 각 녹화 파일을 선택하여 사용 안함으로 설정하는 것이 필요합니다.

- 설정(NVR)
  1) 설정 → 녹화 → 녹화설정
  2) 설정된 각 녹화파일을 선택한 후 오디오 사용 안함 선택
  3) 확인 버튼 클릭



CH	Normal recording	Event	Frame		Limit	Event		Audio
			FULL	I-frame		Pre	Post	
1	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
2	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
3	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
4	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
5	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
6	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
7	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
8	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
9	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
10	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
11	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
12	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
13	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
14	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
15	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
16	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
17	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off
18	FULL	FULL	-	-	2.3 M	5 sec	30 sec	Off

5. 안전 레벨

한화테크윈은 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 >

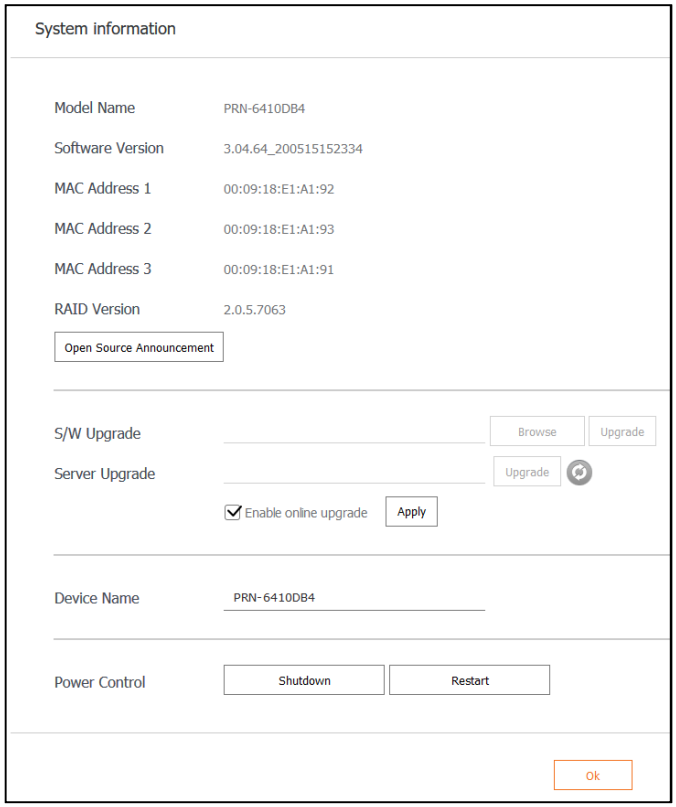
보안 정책	사이버 보안 기능	간략한 설명
-	최신 버전 펌웨어 사용 여부 확인 및 업데이트	최신 버전 펌웨어를 사용하는지 확인하고 보안에 취약한 펌웨어라면 업데이트 수행
-	정확한 날짜/시간 설정하기	로그 분석을 위해 정확한 날짜 및 시간 설정
-	안전한 통신 프로토콜 사용하기(HTTPS)	웹뷰어상에서 송수신되는 개인정보 및 영상 보호
-	안전한 통신 프로토콜 사용하기(RTSP)	RTSP를 통해 전송되는 영상 보호
-	HTTPS(사설 인증서 사용)	인증서를 통한 기기와 클라이언트간 보안 접속
-	HTTPS(공인 인증서 사용)	
-	기본 포트 변경	포트 변경을 통해 웹 서비스 접근 공격 방지
접근통제	IP 필터링	특정 IP 접속 허가/거부를 통해 접근 공격 방지
서비스 보호	안전하게 SNMP 사용하기	보안강화를 위해 SNMP 초기값 모두 해제
-	사용자 그룹/사용자 생성	자주 사용하는 기능은 최소 권한의 사용자 계정을 생성하여 보안 강화
-	권한 설정	기능에 대한 접근 권한을 부여하여 정보 노출 방지
감사	로그 점검하기	비인가자의 접속 기록 분석

5.1. 최신 버전 펌웨어 사용여부 확인 및 업데이트

한화테크윈 홈페이지 (www.hanwha-security.com)를 통해 고객이 사용하는 제품의 최신 펌웨어 버전 확인이 가능합니다. 아래 그림에서는 고객이 PRN-6410DB4 모델을 사용하는 경우 현재 배포된 최신 펌웨어의 버전이 3.04.64_200515152334이며, 그 외 MAC Address, RAID 버전, 오픈소스 고지문 정보도 확인 할 수 있습니다. Software Upgrade를 위해서는 한화테크윈 홈페이지에서 해당 제품의 펌웨어를 다운로드 받고, Upgrade 버튼을 클릭하여 업그레이드를 진행합니다. 현재 사용하는 제품의 펌웨어 버전이 항상 최신이 될 수 있도록 점검해주시기 바랍니다.

- www.hanwha-security.com → 제품소개 → 제품 상세 페이지 → 펌웨어 다운로드

- 설정(NVR)
  1) 설정 → 시스템환경 → 시스템 관리 → 시스템 정보 → S/W 업그레이드
  2) 제품의 현재 S/W 버전 확인
  3) 검색 버튼 클릭하여 다운로드 받은 최신 펌웨어 선택
  4) 업그레이드 버튼 클릭

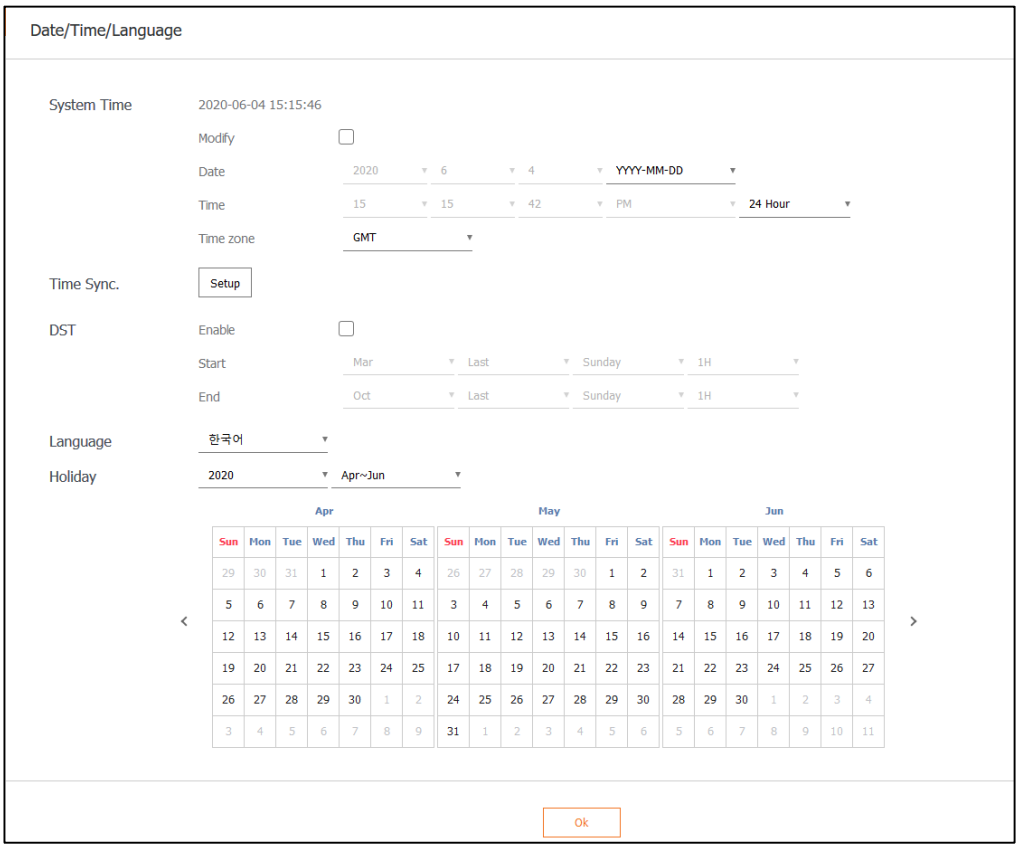


5.2. 정확한 날짜/시간 설정하기

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 시간을 설정하여 시스템에 적용될 시간을 설정할 수 있습니다.

- 설정(NVR)

1) 설정 → 시스템환경 → 날짜/시간/언어 이동
2) 표준시(GMT) 기준인 현 거주 지역의 표준 시간대를 설정
   (일광절약시간(DST) 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) 수정을 선택하여 시스템에 적용될 시간을 설정
4) 시간동기화 설정
5) 시스템 시간 설정의 확인 버튼을 클릭



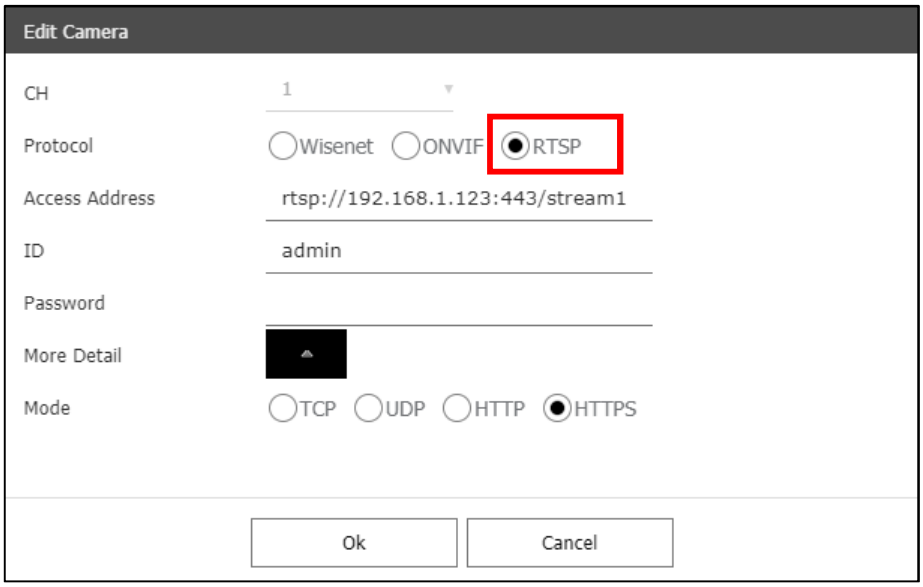
5.3. 안전한 통신 프로토콜 사용하기(HTTP)

한화테크윈의 NVR은 서버와 클라이언트간 HTTP+HTTPS 모드를 초기 설정 값으로 제공하고 있습니다. HTTP/HTTPS 모두 Digest 인증 방식을 적용하고 있어 통신 상에 사용자 비밀번호는 보호 받을 수 있으며, HTTPS 모드를 통해 송수신되는 영상데이터와 같은 중요정보들을 암호화 통신으로 안전하게 보호합니다.

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)
  : 장치 → 카메라 → 카메라 등록 → 채널 선택 → 카메라 수정



5.5. HTTPS (사설 인증서 사용)

최초 보안 접속 방식은 HTTP와 HTTPS를 동시에 지원합니다. HTTPS(사설 인증서 사용)은 한화테크윈에서 제공하는 자체 인증서를 사용하여 기기와 클라이언트간의 보안 접속을 할 수 있도록 해주는 기능입니다. HTTPS (사설 인증서를 사용하는 보안 접속 모드)를 선택할 경우에는 기기에 내장된 자체 인증서가 보안 접속 모드 시 사용되게 되며 사용자가 별도의 인증서를 등록할 필요가 없습니다.

- 설정(NVR)

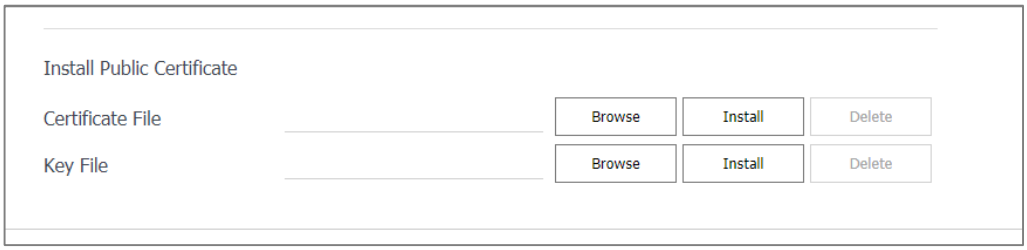
1) 네트워크 → HTTPS → 보안 접속 방식
2) HTTPS (사설 인증서를 사용하는 보안 접속 모드)를 선택
3) 적용 버튼 클릭

5.6. HTTPS (공인 인증서 사용)

한화테크윈에서 제공하는 자체 인증서를 사용하지 않고 사용자가 자신의 공인 인증서를 직접 등록하여 기기와 클라이언트간의 보안 접속을 할 수 있도록 해주는 기능입니다. 공인 인증서 설치를 통해 공인 인증서와 개인키를 등록하면 HTTPS (공인 인증서를 사용하는 보안 접속 모드)를 선택하는 것이 가능해지며 등록한 공인 인증서와 개인키가 보안 접속 모드 시 사용되게 됩니다.

- 설정(NVR)

1) 네트워크 → HTTPS → 공인 인증서 설치
2) 인증서 이름 입력 후 인증서 파일에 사용할 공인 인증서를 지정
3) 키 파일에 사용할 개인키 지정 후 설치 버튼을 클릭
4) HTTPS (공인 인증서를 사용하는 보안 접속 모드) 선택 후 적용 버튼 클릭



※ *HTTPS (공인 인증서를 사용하는 보안 접속 모드) 항목은 등록된 공인 인증서가 있을 경우만 선택 가능합니다.*

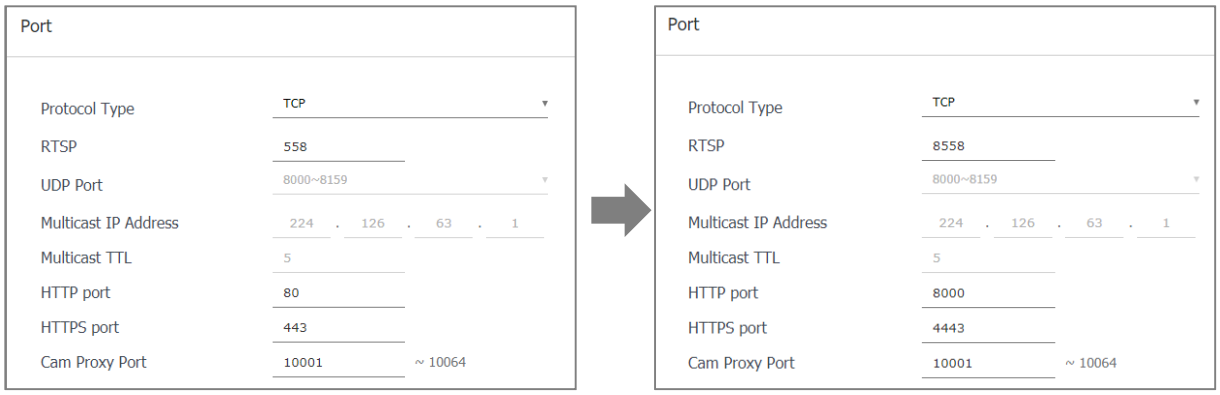
※ *등록한 공인 인증서와 개인키를 삭제하고자 할 경우 삭제 버튼을 클릭합니다. 공인 인증서의 삭제는 HTTP (보안접속 사용 안함)이나 HTTPS (자체 인증서를 사용하는 보안 접속 모드)로 접속한 경우에만 삭제가 가능합니다.*

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. 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.

- 설정(NVR)

1) 설정 → 네트워크 → 인터페이스 → 포트
2) HTTP 포트와 HTTPS 포트를 각각 80과 443에서 상위 포트로 설정 변경
3) RTSP 포트를 558에서 상위 포트로 설정 변경
4) 확인 버튼 클릭



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

5.8. IP 필터링

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

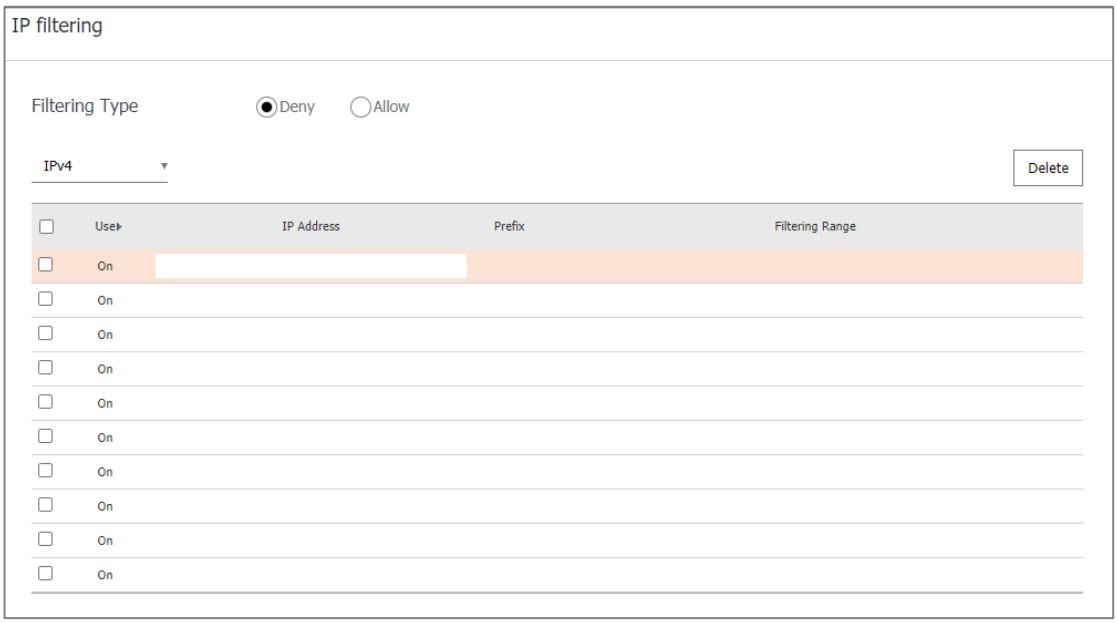
- 설정(NVR)

1) 설정 → 네트워크 → IP 필터링

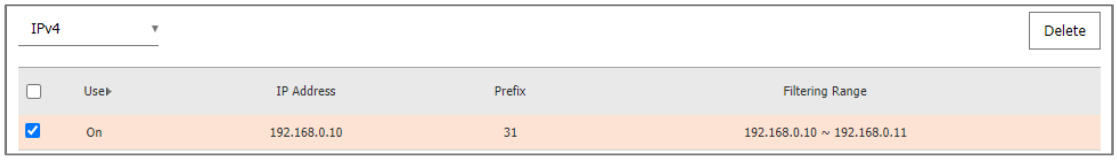
2) 필터링 형식 선택

(거부 : 필터링에 등록된 IP의 접근 차단 / 허가 : 필터링에 등록된 IP만 접근 허용)

3) 입력창을 클릭



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



5) 설정 완료 후 확인 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 거부로 등록할 수 없고 허가로 등록해야 하며, 이 후 설정한 IP들만 접속 가능합니다.*

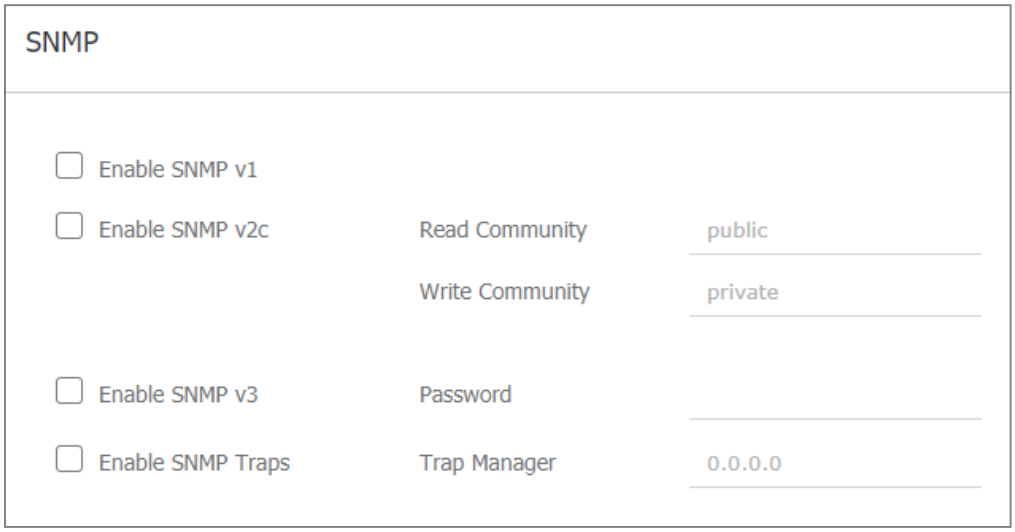
5.9. 안전하게 SNMP 사용하기

SNMP는 네트워크 디바이스를 편리하게 관리할 수 있는 기능을 제공합니다. 기본적으로 한화테크윈은 보안강화를 위해 선택이 모두 해제되어 있습니다. 안전하게 SNMP를 사용하기 위해서는 SNMP v3로만 설정하여 사용하는 것이 바람직합니다.

SNMP v1 및 v2c는 기본적으로 Default 커뮤니티 문자열을 통해 SNMP 기능이 제공되므로 보안에 취약하나, 사용자가 커뮤니티 문자열을 변경하여 사용 할 수 있습니다. SNMP v1, v2c를 사용 할 경우 커뮤니티 문자열을 변경하여 사용 할 것을 권고합니다.

- 설정(NVR)

1) 설정 → 네트워크 → SNMP
2) SNMP v1와 SNMP v2c의 사용 선택 해제
3) SNMP v3 사용 선택 및 비밀번호 설정

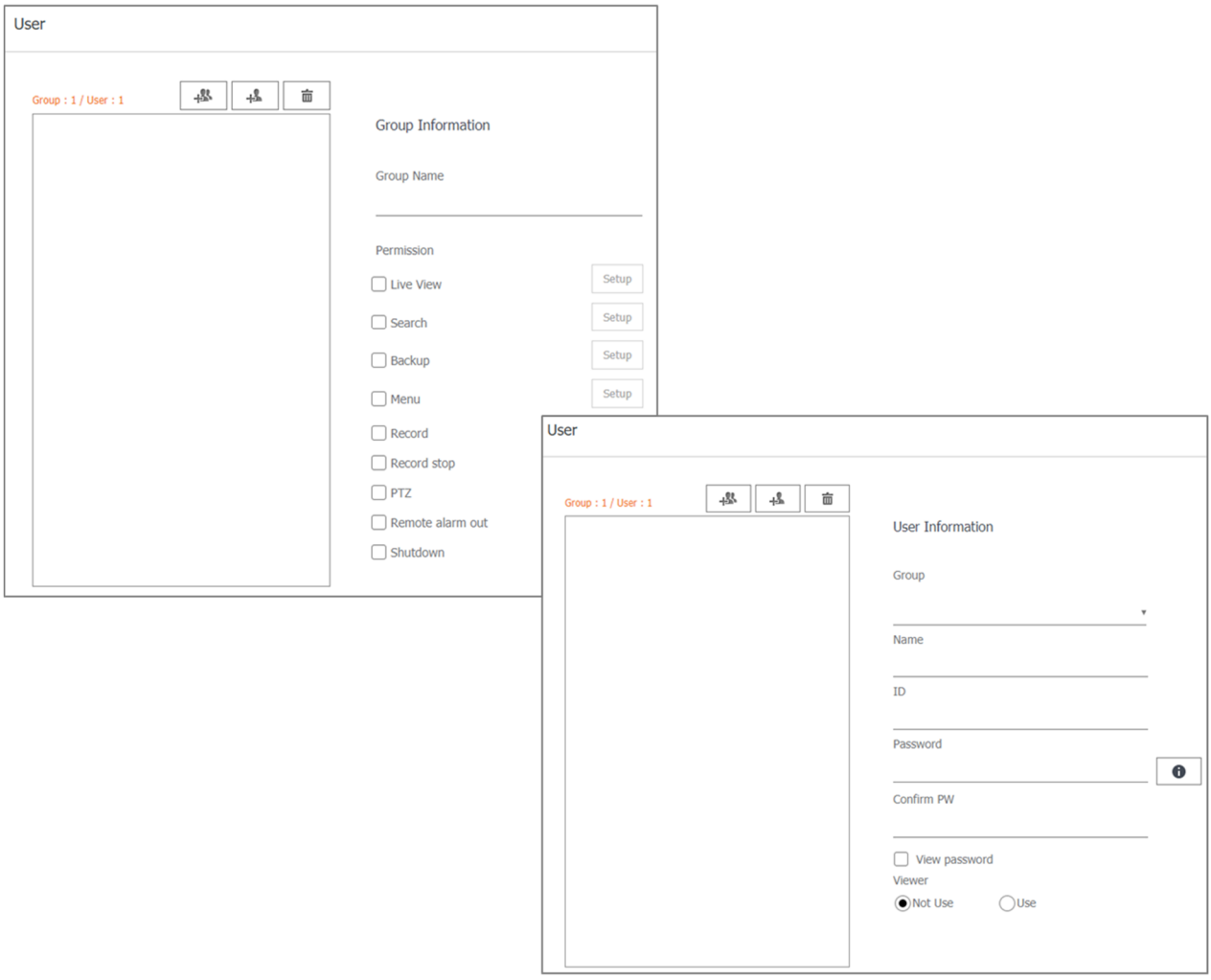


5.10. 사용자 그룹/사용자 생성

관리자 계정으로만 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, 자주 사용하지 않는 설정 기능은 관리자로 하여금 수행하게 하고 자주 사용하는 영상 모니터링 기능 같은 경우 더 낮은 권한을 갖는 추가 사용자 그룹/사용자 계정을 만들어 수행함으로써 보안을 높일 수 있습니다.

- 설정(NVR)

1) 설정 → 시스템 환경 → 사용자 → 사용자
2) 사용자 그룹 추가 후 사용자 계정 추가
3) 사용자 그룹에 대한 권한 설정



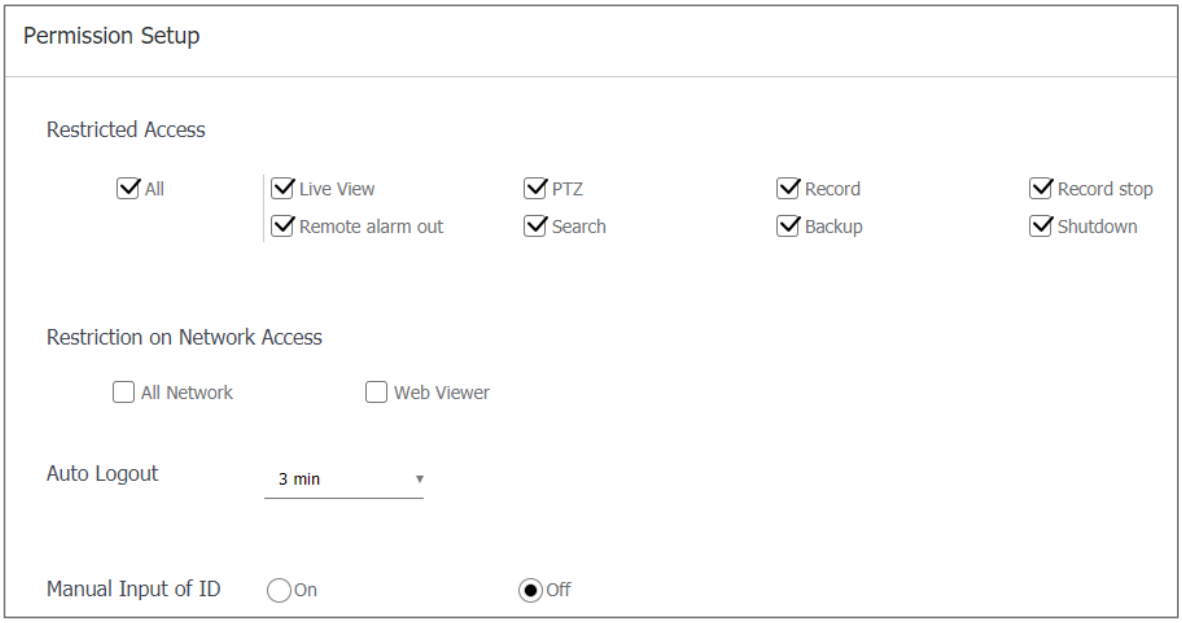
5.11. 권한 설정

기기 사용시 기능, 네트워크 및 로그인에 대한 접근 권한을 설정할 수 있습니다. 기능 및 네트워크 접근 제한은 모든 사용자에게 인증 없이 사용을 허가 할 것인지, 비밀번호 인증 후 권한이 있는 사용자에게만 사용을 허가할 것인지 설정 할 수 있습니다. 단, 기능별 접근 권한은 Live, Search, Backup 기능에 특정 채널에 대해서만 권한이 설정되어 있는 경우, 해당 채널에서만 권한이 설정된 기능을 사용할 수 있습니다.

로그인에 대한 접근 권한은 설정된 시간 동안 입력이 없으면 자동 로그아웃이 됩니다. 또한 ID 수동 입력에 대한 설정은 로그인 시 ID를 직접 입력할 것인지 ID 입력 없이 ID 목록을 통해 선택할 것인지 설정 할 수 있습니다.

- 설정(NVR)

1) 설정 → 시스템 환경 → 사용자 → 권한 설정
2) 접근 제한/네트워크 접근 제한/자동 로그아웃/ID 수동 입력 설정

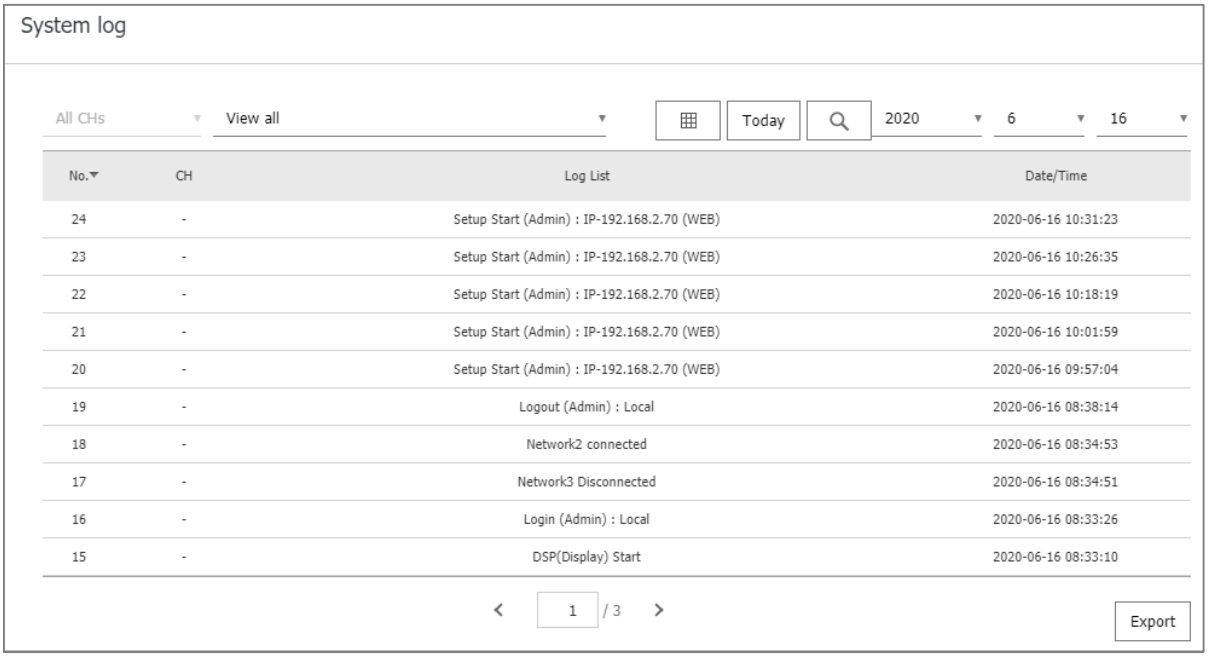


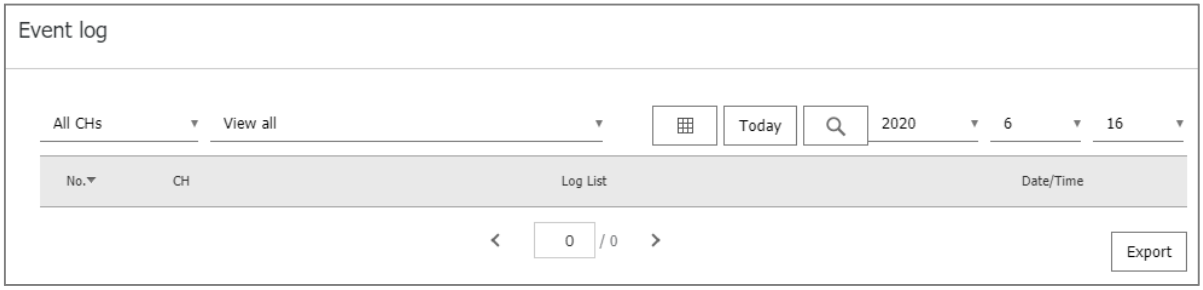
5.12. 로그 점검하기

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.

- 설정(NVR)
  : 설정 → 시스템 환경 → 로그 정보 → 시스템 로그/이벤트 로그/백업 로그





6. 최상위 안전 레벨

한화테크윈 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

6.1. 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. 한화테크윈 NVR의 Camera, Viewer, iSCSI에 지원하는 802.1x는 인증서를 필요로 하는 표준 방식 EAP-TLS를 사용합니다.

802.1x를 지원하는 네트워크 스위치(또는 브리지, 무선 AP 등)와 802.1x 인증 서버, 기기별 인증서 및 개인키가 필요하며 다음과 같이 기기별 인증서 및 개인키를 설정 페이지를 통해 설치합니다.

- 설정(NVR)

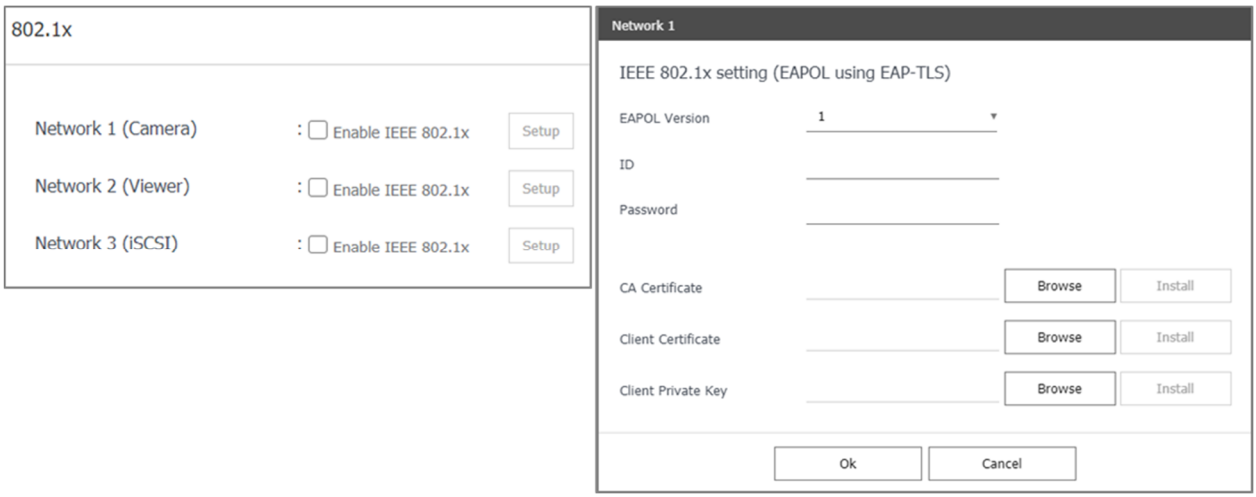
1) 설정 → 네트워크 → 802.1x
2) 카메라 또는 뷰어 또는 iSCSI 선택
3) EAPOL 버전을 1또는 2로 설정
4) 클라이언트의 인증서 ID와 개인키 비밀번호 입력

※ 암호화되지 않은 개인키 파일을 사용하는 경우 입력하지 않아도 됩니다.

5) 공인 인증서를 통해 인증 서버의 CA 공인 인증서를 설치
6) 포트 기반의 접근 제어를 사용할 경우 클라이언트 인증서와 사설 키 설치

※ 설치된 인증서와 개인키는 RADIUS 서버와 Client 기기간의 TLS 통신에만 사용됩니다.

7) 확인 버튼 클릭



WISENET

Hanwha Techwin Co.,Ltd.
13488 경기도 성남시 분당구 판교로 319번길 6 한화테크윈 R&D센터
TEL 070.7147.8771-8
FAX 031.8018.3715
http://hanwha-security.com

Hanwha Techwin