WCC_V1.0 제품 설명서 v1.0

[국가용 보안요구사항 V3.0 기반]

와 치 캠

제·개정 이력

번호	버전	수정 날짜	내용
1	v1.0	26.05.07	국가용 보안요구사항 V3.0 기반의 WCC_V1.0 보안요구사항 제품 설명서 작성

수정 전/후 내용 대비표

번호	수정 날짜	세부 항목	기존	수정 후
1	26.05.07	제품 설명서 작성		v1.0
2				
3				

목 차

1. 개요

1.1. 식별정보

표 1. 제품 설명서 식별정보

문서명	WCC_V1.0 제품 설명서
문서 버전	v1.0
파일명	WCC_V1.0 제품 설명서.pdf
작성자	주식회사 와치캠
작성 일자	2026. 05. 07

1.2. 목적

본 제품은 IP 네트워크를 통해 영상을 촬영하고 전송하는 IP 카메라입니다. 제품의 일반적인 기능은 '네트워크 카메라 사용설명서'에서 다루며, 본 문서는 제품의 보안 기능을 책임지는 보안 관리자를 대상으로 합니다.

네트워크에 연결된 제품의 특성상, 비인가된 접근, 데이터 위변조, 정보 유출 등의 보안 위협으로부터 시스템과 영상 데이터를 안전하게 보호하는 것이 매우 중요합니다. 이에 본 문서는 제품의 보안 성능을 유지하고 안전한 운용 환경을 구축하는 데 필요한 보안 기능 설정 및 관리 방법을 안내합니다.

1.3. 제품 설명서 구성

본 운용설명서는 다음과 같이 구성되어 있습니다.

· 1장은 제품 설명서의 개요로, 설명서의 식별정보와 목적 등을 기술합니다.

· 2장은 제품의 소개, 구성요소에 대하여 기술합니다.

· 3장은 제품의 접속하고 관리하는 방법에 대하여 기술합니다.

· 4장은 주요 보안기능의 설정 방법에 대하여 기술합니다.

· 5장은 고객지원 사항에 대한 내용을 기술합니다.

· 6장 부록은 제품에서 발생되는 오류 메시지, FAQ에 대하여 기술합니다.

1.4 용어 정의

관리자(administrator)

· 제품의 보안기능에 의해 구현된 모든 정책에 관해서 신뢰 등급을 가진 실체

RTSPS

· Secure Real-Time Streaming Protocol. TLS 암호화 채널을 통해 RTSP 통신을 보호하는 프로토콜입니다.

ONVIF

· Open Network Video Interface Forum. IP 기반 보안 제품 간의 상호 운용성을 위한 개방형 표준입니다.

WebUI

· Web User Interface. 웹 브라우저를 통해 제품을 설정하고 관리하는 사용자 인터페이스입니다.

VMS

· Video Management System. 다수의 영상 소스를 관리, 녹화, 재생하는 소프트웨어 시스템입니다.

INIT

· IP-Camera Network Installation Tool. IP 카메라 장치들의 접속 정보를 검색하는 SW도구입니다.

FTPS

· FTP over TLS. 파일 전송 프로토콜(FTP)에 TLS 암호화를 추가하여 보안을 강화한 프로토콜입니다.

mDNS

· Multicast DNS. 별도의 DNS 서버 없이 호스트 이름을 IP 주소로 변환하는 프로토콜입니다.
· INIT에서 장치 검색에 사용합니다.

WS-Discovery

· Web Service Dynamic Discovery. 로컬 네트워크에서 자동으로 장치를 찾기 위한 프로토콜입니다.
· ONVIF 에서 장치 검색에 사용합니다.

2. 제품 소개

본 장에서는 제품의 주요 기능과 구성 요소, 그리고 보안 운용 시 반드시 숙지해야 할 주의사항에 대해 기술합니다.

본 제품 WCC_V1.0는 고해상도 영상과 AI 지능형 분석 기능을 제공하는 IP 카메라입니다. 본 제품은 단순한 영상 감시를 넘어, 장비의 운용 및 데이터 전송 전 과정의 보안성을 최우선으로 고려하여 설계되었습니다.

이를 위해 관리자 접속 및 영상 처리 등 모든 데이터 통신은 암호화 프로토콜을 통해서만 이루어집니다. 시스템 접근은 '관리자', '운영자', '사용자' 그룹으로 권한이 엄격히 분리되어 관리됩니다.

또한, 관리자 암호를 비롯한 모든 시스템의 주요 설정 정보는 암호화되어 안전하게 관리됩니다. 제품 운용 중 발생하는 모든 보안 관련 이벤트는 감사 기록으로 생성되어, 관리자는 이를 통해 이력을 관리하고 안전한 운용 상태를 지속적으로 점검할 수 있습니다.

2.1 제품의 구성 및 사양

제품은 하드웨어 일체형 장비로 제공되며, 제품의 펌웨어는 표 2 의 하드웨어 모델에 탑재되어 운영됩니다. 각 구성 요소 정보는 아래와 같습니다.

표 2. 제품 식별정보

구분	내용	
제품명	WCC_V1.0	
버전	v1.0.0.1	
구성요소(F/W)	INSRM-C1-v1.0.0.1 (INSRM-C1-v1.0.0.1.rui)	
하드웨어 모델 / 탑재 모델	WG-IB823	WCC_V1.0- WG-IB823
	WG-ID823	WCC_V1.0- WG-ID823

표 3. 제품 운영 체제 제품 운영 체제

구분	내용
운영 체제	Release: Embedded Linux Kernel: Linux version 5.15.180 Build: aarch64-linux-gnu-gcc (GCC) 12.2.1 20230415

WCC_V1.0 제품의 하드웨어 사양은 아래 표 4와 같습니다.

표 4. HW 구성요소 리스트

HW 모델	구분	사양
WG-IB823	SoC	Ambarella CV72s66(ARM Cortex-A76)
	RAM	4GB (Samsung)
	Storage	500MB (Micron Technology Inc.)
	Network	10/100 Mbps (Texas Instruments Inc.)
	Specification	8MP, x2.3 Zoom, Bullet IP Camera
WG-ID823	SoC	Ambarella CV72s66(ARM Cortex-A76)
	RAM	4GB (Samsung)
	Storage	500MB (Micron Technology Inc.)
	Network	10/100 Mbps (Texas Instruments Inc.)
	Specification	8MP, x2.3 Zoom, Dome IP Camera

* SoC, Storage 는 모든 하드웨어 제품이 동일

* 제품 최대 해상도 및 광학 줌 배율, 기구 형태에 대해서 Specification 에 표기

제품에 포함되는 제 3자 제공 소프트웨어 및 자체 개발 소프트웨어는 아래 표 5와 같습니다.

표 5. SW 모듈 리스트

	모듈 명칭	적용된 보안기능	OpenSource	버전	관리 주체 (라이선스)
1	linux kernel	OS	O	5.15.180	Linux (GPLv2)
2	openssl	SSL 암호통신, 키 생성	O	3.6.0	openssl License
3	iproute2	라우팅, 네트워크 인터페이스	O	6.16.0	Linux (GPLv2)
4	iptables	WhiteList, 방화벽	O	1.8.11	netfilter (GPL)
5	curl	FTPS, HTTPS, HTTPS 터널링	O	8.17.0	curl (MIT/X derivate)
6	crypto-JS	백앤드	O	4.2.0	crypto-JS(MIT)
7	app	영상서버(Rtsp, 자체프로토콜)	X	1.1.0	IDIS
8	app	웹서버(WebUI, ONVIF, CGI)	X	1.1.0	IDIS
9					

제품의 외관은 아래 그림 1과 같습니다.

(a) WG-IB823 (b) WG-ID823

그림 1. WCC_V1.0 하드웨어 일체형 제품의 제품 외관

2.2. 운용 환경

아래 그림 2는 제품의 일반적인 IP 네트워크 환경에 연결되어 운용되는 표준구성도를 보입니다.

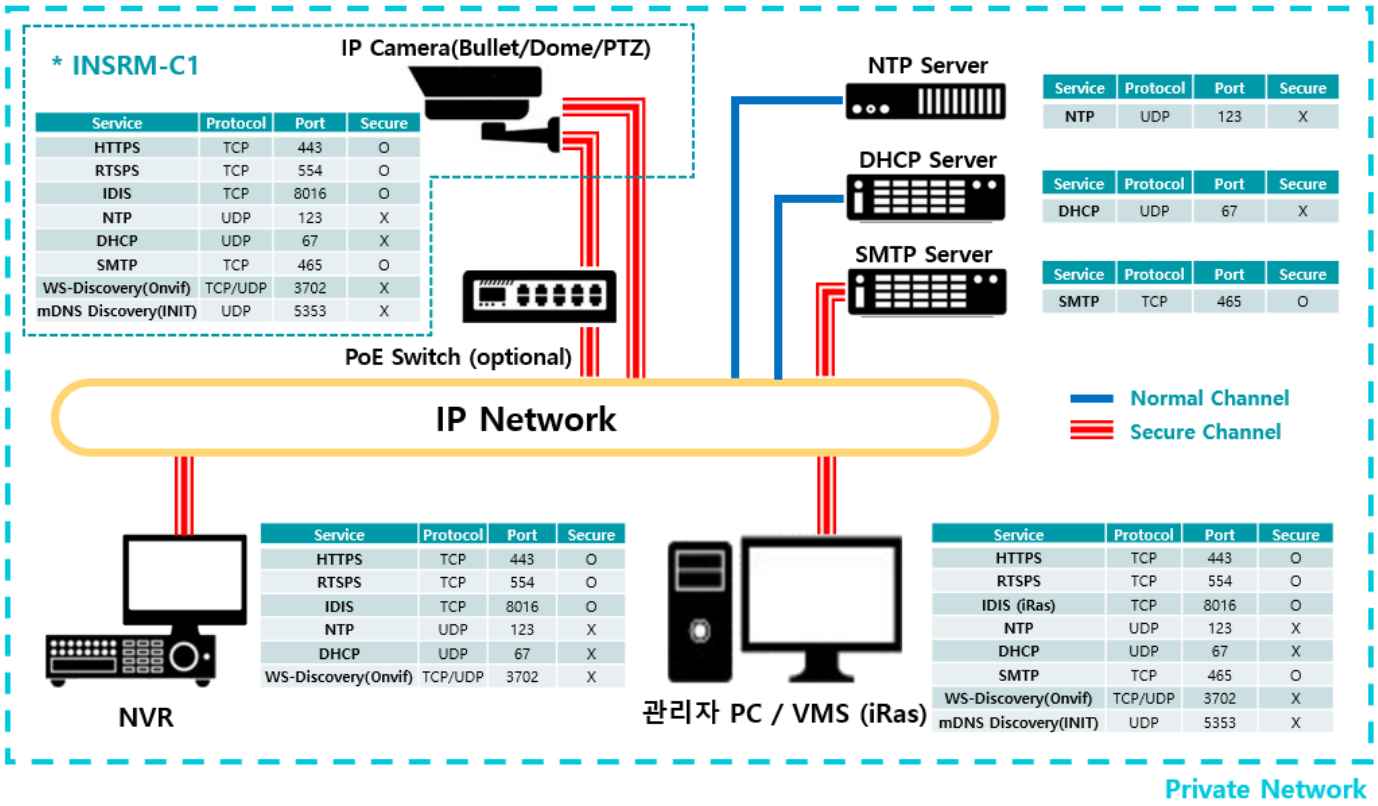


그림 2. IP카메라 운용환경 표준구성도

제품의 운용 및 관리를 위한 관리자 PC 의 최소 사양은 아래 표 6와 같습니다.

표 6. 관리자 PC의 최소 사양

항목	구분	사양
관리자 PC	소프트웨어	OS : Microsoft® Windows® 7 64-bit (Home Premium, Professional, Ultimate) 이상 CPU : Intel Core i7-3770 3.40GHz 이상 RAM : 8GB 이상 VGA : AMD RadeonTM HD 7700 또는 NVIDIA GeForce GTX650 (AMD 권장, 1280x1024, 32bpp 이상) 하드디스크 : 6GB 이상의 여유 공간 LAN : Gigabit Ethernet 이상

제품 운영에 필요한 소프트웨어는 아래 표 7과 같습니다.

표 7. 제품 운영에 필요한 소프트웨어 목록

구분	소프트웨어 명	용도
관리 접속도구	INIT	관리자 PC에서 사용하는 윈도우 응용 프로그램, 검색도구로 IP카메라를 탐색하여 IP 주소를 확인하기 위해 사용합니다.
	iRas	관리자 PC에서 사용하는 윈도우 응용 프로그램, PC 클라이언트로 제품의 실시간 영상을 확인하고 PTZ 및 색상 변경 등의 원격 제어 기능을 수행하기 위해 사용합니다.

제품의 정상적인 운용을 위해, 제품과 상호작용하는 본 제품 외, 외부 IT 실체가 있습니다. WCC_V1.0 제품과 상호작용하는 외부 IT 실체는 아래 표 8과 같습니다.

표 8. 외부 IT 실체 목록

항목	구분	사양
관리자 PC	HTTPS RTSPS IDIS over TLS	제품의 핵심적인 설정 및 관리 기능을 수행할 수 있는 인가된 관리자 단말기로, 신규 제품 검색, 최초 관리자 계정 및 보안 설정 변경, 실시간 영상 및 상태 모니터링 기능을 수행합니다. HTTPS: 관리용 WebUI, Onvif 명령 송/수신 RTSPS: 영상 스트리밍 IDIS over TLS: 암호화 프로토콜에서 동작하는 자체 프로토콜, iRas 에서 사용합니다.
VMS/NVR	HTTPS RTSPS	다수의 IP 카메라들을 통합 관리하고, 카메라로부터 영상 및 오디오 스트림을 수신하여 안정적으로 저장, 분석, 재생하는 역할을 수행합니다.
NTP 서버	NTP	제품의 시스템 시간을 정확하게 동기화하여, 모든 영상 데이터와 감사 기록의 타임스탬프에 대한 신뢰도를 보장하는 역할을 수행합니다.
DHCP 서버	DHCP	네트워크에 연결된 제품에 IP 주소, 서브넷 마스크, 게이트웨이 등의 네트워크 정보를 동적으로 할당하여 관리자의 수동 설정 없이도 통신이 가능하도록 지원합니다.
SMTP 서버	SMTP over TLS	제품에서 발생하는 이벤트를 네트워크를 통해 관리자에게 알리는 역할을 담당하며, TLS 기반의 보안 채널을 통해 데이터를 안전하게 전송합니다.

2.3. 운용 시 주의사항

본 제품의 보안 성능을 최대로 유지하기 위해 관리자는 다음 사항을 반드시 준수해야 합니다.

1. 관리자 계정의 책임: 본 제품은 최초 접속 시 관리자 계정 생성을 강제합니다. 관리자는 이 계정의 비밀번호를 복잡하게 설정하고 안전하게 관리할 책임이 있습니다.

2. 네트워크 환경: 제품은 신뢰할 수 있는 방화벽 내부의 보안 네트워크 환경에서 운용되어야 합니다. 신뢰할 수 없는 외부 네트워크에 제품을 직접 노출하는 것을 금지합니다.

3. 물리적 보안: 제품에 물리적으로 접근하여 케이블을 탈취하거나 장비를 조작하는 행위를 방지하기 위해, 제품의 설치 위치에 대한 물리적 보안을 강화해야 합니다.

4. 정기적인 업데이트: 2.2. 제품 F/W 다운로드 항목을 참조하여, 제품의 펌웨어를 항상 최신 상태로 유지해야 합니다.

5. 보안 기능 활성화: 본 매뉴얼에서 안내하는 모든 보안 기능(권한, IP필터링, 감사 기록 등)을 활성화하여 운용하는 것을 강력히 권고합니다.

6. 보안 모니터링 및 감사기록 관리:

비정상 로그인 시도 확인: 관리자는 Web UI 접속 시, 감사기록을 통해 5회 연속 인증 실패 등 비정상적인 로그인 시도가 있었는지 수시로 확인할 책임이 있습니다. 시스템은 5회 연속 인증 실패 발생 시 Web UI 알림 또는 등록된 이메일을 통해 관리자에게 이를 통보합니다.

감사기록 용량 관리: 감사기록 저장 공간이 임계치에 도달할 경우, 시스템은 Web UI 알림 또는 등록된 이메일을 통해 이를 통보합니다. 관리자는 해당 알림을 확인하는 즉시 로그를 백업하여 기록 유실을 방지해야 합니다.

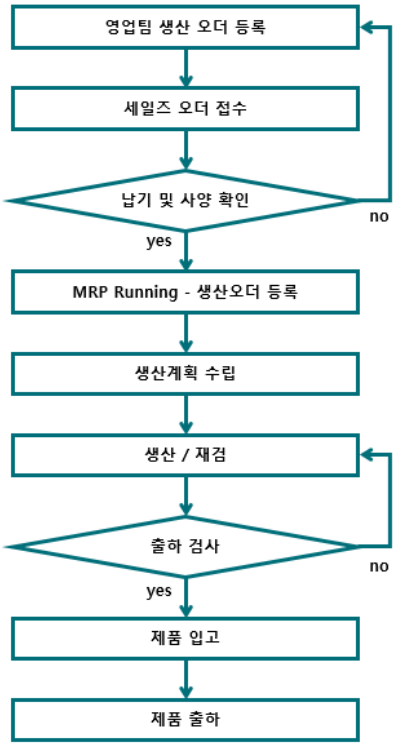
3. 제품 설치 및 접속

본 장에서는 제품에 최초로 접속하고, 안전한 사용을 위한 초기 보안 설정을 등록하는 절차에 대해 안내합니다.

3.1. 배포 방법

제품의 배포는 보안을 유지하기 위해 다음의 통제된 방식을 통해 이뤄집니다.

배포 프로세스: '요청 -> 생산 -> 검사 -> 출하'의 4단계로 구성되며, 상세 흐름은 아래 그림 3과 같습니다.



1단계: 생산 요청 및 계획 수립

1. 생산 요청 접수
   - MTS (재고 생산): [생산관리팀]은 매주 월요일 적정 재고를 파악하여 그룹웨어를 통해 생산을 요청한다.
   - MTO (주문 생산): [영업팀]은 고객사와 협의한 모델, 사양, 수량, 납기를 정리하여 [생산관리팀]에 전달한다.
2. 생산 계획 조율 및 확정
   - [생산관리팀]은 영업팀의 요청과 현재 생산 현황을 종합하여 출하 일정을 조율한다.
   - 검토 완료된 오더에 대해 MRP(자재 소요량 계획)를 실행하고 생산 오더를 등록한다.
   - 자재 구매/발주가 완료되면, 최종 출하 일정을 기준으로 상세 생산 계획(일정, 수량)을 수립한다.

2단계: 생산 진행

1. 작업 지시
   - [생산관리팀]은 생산 계획일 2일 전(D-2), [생산운영팀]에 작업 지시 및 자재 출고를 지시한다.
2. 제품 생산
   - [생산운영팀]은 작업명세서의 제품 사양을 확인 후, 아래 공정 순서에 따라 생산을 진행한다.
   - 공정 순서: 자재 인수 → 준비 작업 → 조립 → 에이징(사전 테스트) → 기능 검사(Final Test) → 포장

3단계: 품질 검사 및 입고

1. 출하 검사 의뢰 및 진행
   - [생산운영팀]은 생산 완료된 제품에 대해 [QA팀]으로 출하 검사를 의뢰한다.
   - [QA팀]은 오더별 샘플링 검사를 통해 합격/불합격 여부를 판정한다.
2. 검사 결과 조치
   - 불합격 시: [QA팀]은 [생산팀]으로 제품을 반환(피드백)하여 재검사 및 수리를 요청한다.
   - 합격 시: [QA팀]은 제품을 출하 승인하고, [생산운영팀]은 제품 창고로 이동시키며 전산 입고 처리를 완료한다.

4단계: 제품 출하

1. 출하 정보 공유 및 지시
   - [영업팀]은 최종 확정된 출하 방법, 일정, 수량을 관련 부서에 공유한다.
   - [생산관리팀]은 해당 정보에 맞춰 출하 지시(딜리버리)를 생성한다.
2. 최종 출하
   - [자재외주관리팀]은 생성된 출하 지시서에 따라 지정된 방법으로 제품을 출하한다.
   - 제품은 지정된 보안 계약을 체결한 택배사를 통해 배송을 완료한다.

그림 3. 제품 배포 절차 순서도

제품 배포 시 제공되는 구성물은 다음과 같으며, 모든 항목은 형상관리 절차에 따라 통제됩니다. 제품 SW, 검색도구(INIT), VMS(iRas), 설명서(PDF)는 별도의 매체를 통해 제공되지 않고, 당사 홈페이지를 통해 제공됩니다. 제품의 상세한 배포 항목은 아래 표 9과 같습니다.

표 9. 제품 배포 구성 목록

	구분	식별자	형태	배포
1	제품명	WCC_V1.0		
2	제품 버전	v1.0.0.1	-	-
3	제품 구성요소	INSRM-C1-v1.0.0.1 (INSRM-C1-v1.0.0.1.rui)	FW	HW 장비에 탑재 후 배포, 당사 홈페이지
4	설명서	WCC_V1.0 제품 설명서 v1.0	전자문서	당사 홈페이지

		(WCC_V1.0 제품설명서 v1.0.pdf)		
5	관리 도구	INIT v4.9.0(2025103001) (INIT.exe)	설치파일	당사 홈페이지
		iRAS v6.9.1(IRA69102) (setup.exe)		
5	하드웨어 모델	WG-IB823	-	-
		WG-ID823		

3.2. 설치 준비 및 설치

제품은 하드웨어 일체형 제품으로, 배포 후 설치하기 전에 먼저 장비 구성품을 확인합니다. 각 하드웨어 제품별로 아래의 구성품이 제대로 포함되어 있는지 확인합니다.

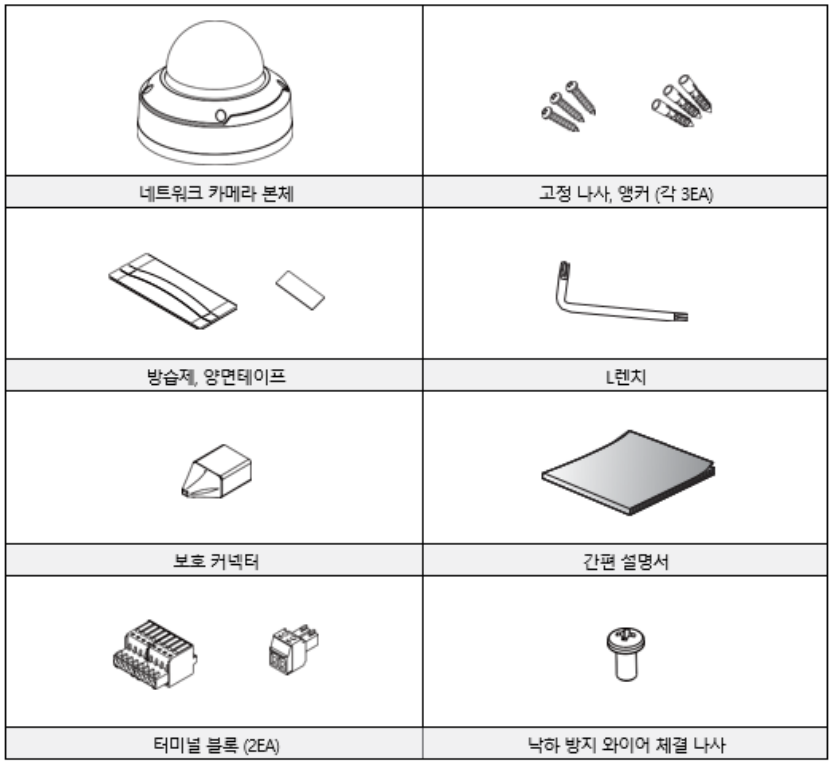


그림 4. WG-ID823

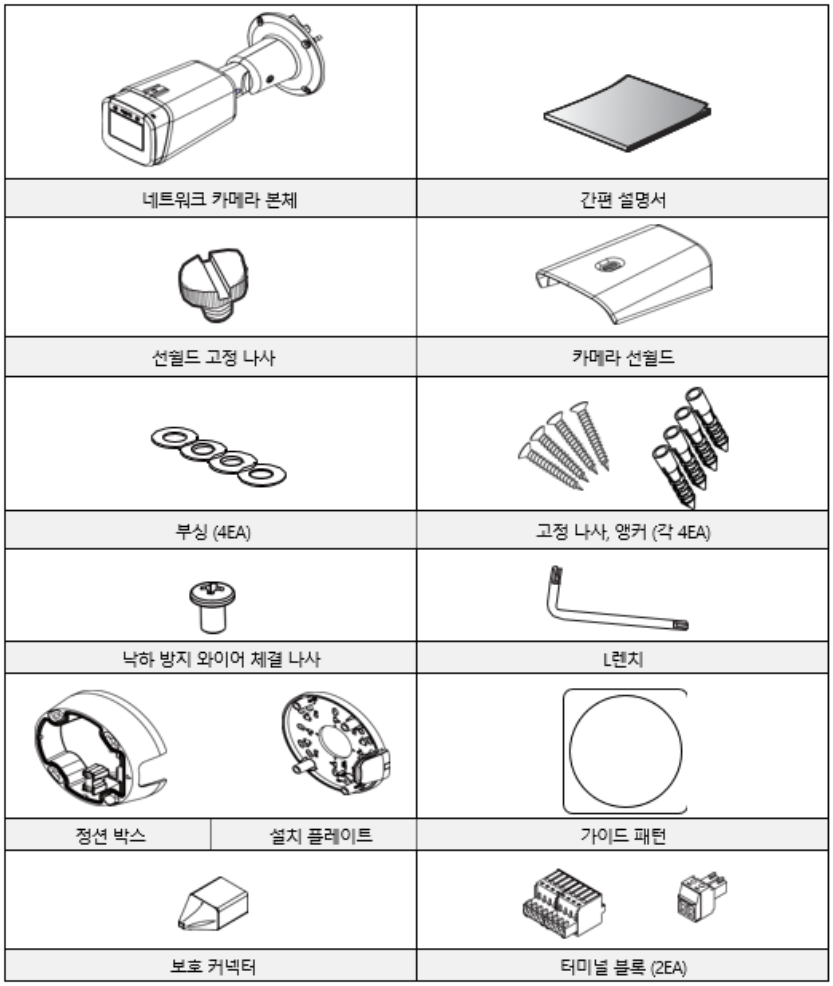


그림 5. WG-IB823

[설치 전 주의사항]

설치할 벽이나 천장이 카메라의 하중을 지탱할 수 있는지 미리 확인하고, 필요한 경우 보강 공사를 진행해야 합니다. 지지력이 약할 경우 카메라 낙하의 위험이 있습니다.

직사광선은 제품에 악영향을 줄 수 있으므로 피하고, 비교적 서늘한 곳에 설치합니다.

[제품 설치]

단계 1: 먼저 카메라를 장착할 벽이나 천장에 케이블을 통과시킬 구멍을 뚫습니다.

단계 2: 외부의 습기나 물이 브라켓 또는 파이프를 통해 기기 내부로 들어오지 않도록, 제공된 방수용 부싱에 케이블을 통과시킨 후 팬던트에 조립합니다.

단계 3: 카메라와 함께 동봉된 방수용 본드를 도포하여 부싱의 케이블 틈새와 나머지 구멍을 빈틈없이 채워 방수 처리를 마무리합니다.

3.3. 제품 접속 및 등록

제품에 대한 모든 관리 접속은 암호화된 HTTPS 프로토콜을 통해서만 이루어집니다. 이 과정에서 관리자 PC의 웹 브라우저에는 자체 서명 인증서(Self-Signed Certificate)에 대한 보안 경고가 표시될 수 있습니다. 이는 서버의 신원을 증명하는 인증서가 공인된 인증 기관(CA)이 아닌 제품 자체에서 발급되었기 때문에 발생하는 정상적인 현상입니다. 관리자는 신뢰할 수 있는 네트워크 환경에서 접속하고 있는지 확인한 후, 해당 연결을 신뢰하고 다음 단계로 진행해야 합니다.

3.4. 카메라 접속을 위한 IP 주소 검색

제품을 네트워크에 연결한 후, 관리자 PC에서 제품의 IP 주소를 확인하기 위해 INIT 를 사용합니다.

1. INIT 프로그램을 관리자 PC에서 실행합니다.

2. INIT에서 로컬 네트워크(mDNS)를 탐색하여 공장 초기화 상태의 제품 목록을 표시합니다.

3. 목록에서 접속하려는 제품을 확인하고 해당 IP 주소를 우클릭하여 WebUI 접속을 시도합니다.

그림 6. INIT(네트워크 비디오 설치 도구)에서 제품 검색

3.5. 관리자 계정 등록

제품에 최초로 접속하면, 보안을 위해 관리자 계정 등록이 강제됩니다.

그림 7. 관리자 계정 최초 등록창

1. 3.1 단계에서 확인된 IP 주소로 웹 브라우저에서 https://[IP 주소]/setup/setup.html 형식으로 접속합니다.

2. 자체 서명 인증서 경고창에서 '연결 계속' 또는 '예외 추가'를 선택합니다.

3. 관리자 계정 등록 화면이 나타나면, 새 관리자 ID와 비밀번호를 입력합니다.

관리자 계정명 및 비밀번호는 아래 보안성 기준을 만족해야 합니다.

표 10. 계정명으로 사용하지 못하는 예약 단어 목록

구분	예약 단어
유추 가능한 명칭	admin, root, administrator, operator, user
업체, 모델명	idis, WCC_V1.0, WCCV1.0, 하드웨어 모델명(ex: WG-IB823, etc.)
그 외 금지 계정명	login, logout, logon, logoff

표 11. 패스워드 보안성 기준

기준
9 자리 이상 길이 확보
숫자, 대문자(영문), 소문자(영문), 특수문자가 각 1 개 이상 포함
사용자계정(ID)과 동일한 패스워드 설정금지
동일한 문자, 숫자 연속적으로 반복사용 금지
키보드의 연속된 문자 또는 숫자의 순차적 나열 금지
직전 사용된 패스워드 재사용 금지

4. [Register] 버튼을 클릭하여 계정 생성을 완료합니다.

[중요] 관리자 계정 생성 완료 시점부터, 검색도구에서 제품이 검색되지 않습니다.

3.6. 관리자 PC주소 등록

관리자 계정 등록이 완료되면, 비인가된 접근을 차단하기 위해 관리자 PC의 IP 주소를 등록해야 합니다.

그림 8. 관리자 계정 등록 이후 IP 필터링 입력

1. 3.2 단계에서 생성한 관리자 계정으로 WebUI에 로그인합니다.

2. 로그인 후 출력되는 IP 필터링 메뉴의 추가 버튼을 클릭합니다.

3. 관리자 PC IP 주소 및 운용에 필요한 IP 주소를 등록합니다.

4. [확인] 버튼을 클릭하여 설정을 적용합니다.

[중요] 접속 중인 PC의 IP 주소를 등록하지 않으면 설정 이후 접속이 불가능해지므로 주의가 필요합니다.

다음 IP 주소는 등록이 불가능 합니다(0.0.0.0, 127.*.*.*, *.*.*.0, *.*.*.255).

4. 제품 보안 기능 설정 및 사용 방법

본 장에서는 제품의 주요 보안 기능을 활성화하고 설정하는 방법에 대해 상세히 안내합니다. 관리자는 본 장의 내용을 숙지하여 제품의 보안 수준을 최상으로 유지해야 합니다.

4.1. 운영자/사용자 계정 등록

본 제품은 관리자 외에도, 기능 접근이 제한된 운영자 및 사용자 그룹의 계정을 추가할 수 있습니다. 최소 권한 원칙에 따라, 단순 영상 모니터링만 필요한 사용자에게는 '사용자' 권한을 부여하는 것을 권장합니다.

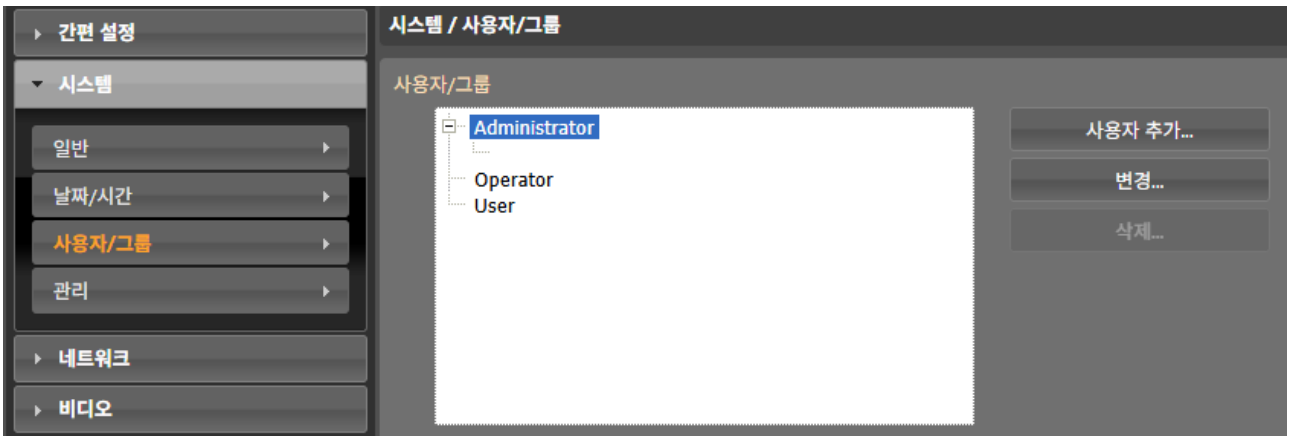


그림 9. 운영자/사용자 계정 등록

관리자 계정으로 WebUI에 로그인한 후, 설정 > 시스템 > 사용자/그룹 메뉴로 이동합니다.

[사용자 추가] 버튼을 클릭합니다.

생성할 계정의 그룹('운영자' 또는 '사용자')을 선택하고, ID와 비밀번호, 비밀번호 확인을 입력합니다.

[확인] 버튼을 눌러 계정 생성을 완료합니다.

4.2. 영상 감시 서비스 설정

본 제품은 외부 영상 감시 시스템(VMS) 또는 클라이언트와 연동 시, 모든 제어 및 영상 스트림을 암호화하여 전송합니다. 암호화되지 않은 평문 프로토콜(RTSP, HTTP)은 지원하지 않으며, 반드시 TLS 기반의 보안 프로토콜을 사용해야 합니다.

본 절에서는 각 프로토콜의 보안 설정을 활성화하는 방법을 안내합니다.

4.2.1. 아이디스 프로토콜

아이디스 프로토콜은 전용 VMS (iRas 등) 클라이언트와의 연동을 위한 고유 프로토콜입니다. 이 통신은 TLS v1.2 (기본 TCP Port: 8016) 기반의 보안 채널을 통해 암호화됩니다.

관리자 계정으로 WebUI에 로그인한 후, 설정 > 네트워크 > 포트/QoS 메뉴로 이동합니다.

원격 포트 사용 항목을 체크하여 활성화합니다.

서비스 포트가 기본값(8016)인지 확인하고 [저장] 버튼을 클릭합니다.

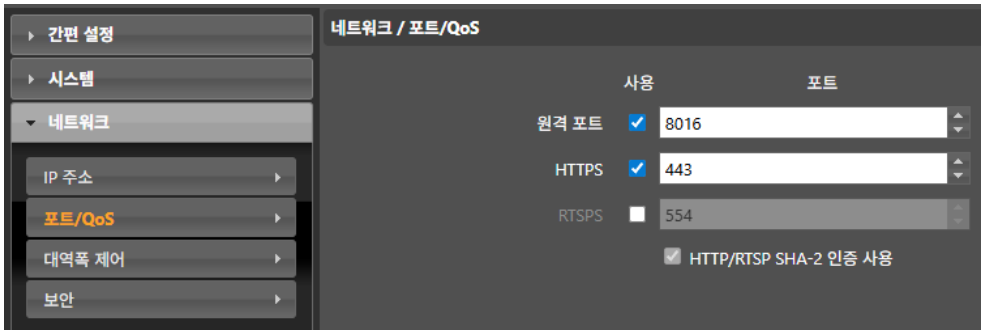


그림 10. 아이디스 프로토콜 설정

4.2.2. RTSPS

본 제품은 표준 RTSP 클라이언트와의 호환을 위해 RTSPS (RTSP over TLS)를 지원합니다. 암호화되지 않은 RTSP는 지원하지 않으며, 반드시 RTSPS 포트(기본값 554)로 접속해야 합니다.

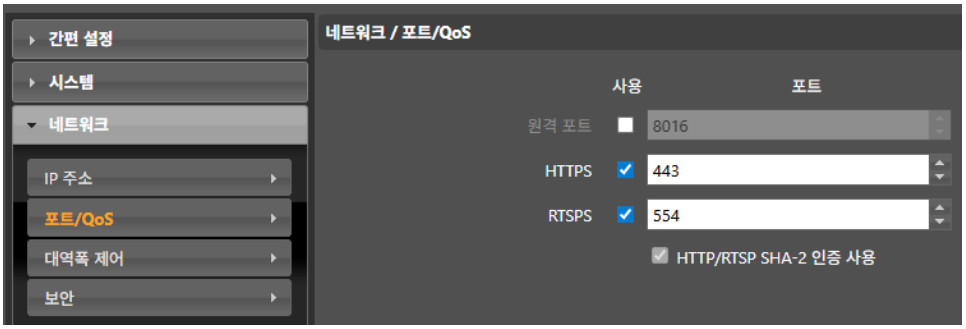


그림 11. RTSPS 활성화 설정

1. WebUI에 로그인한 후, 설정 > 네트워크 > 포트/QoS 메뉴로 이동합니다.
2. RTSPS 사용 항목을 체크하여 활성화합니다.
3. RTSPS 포트 번호가 기본값(554)인지 확인하고 [저장] 버튼을 클릭합니다.
4. RTSPS 접속 주소는 rtsps://[IP주소]:554/trackID=1과 같은 형식으로 사용할 수 있습니다.

4.2.3. ONVIF

타사 VMS와의 호환을 위한 ONVIF 연동 시, 제어 채널은 HTTPS로, 영상 스트림 채널은 RTSPS로 암호화 통신을 수행합니다.

1. WebUI에 로그인한 후, 설정 > 일반 > 기타 메뉴로 이동합니다.
2. ONVIF 프로토콜 사용 항목을 체크하여 활성화합니다.
3. WebUI에 로그인한 후, 설정 > 네트워크 > 포트/QoS 메뉴로 이동합니다.
4. HTTPS, RTSPS 사용 항목을 체크하여 활성화합니다.

그림 12. ONVIF 활성화 설정

[중요] 연동하려는 VMS(ONVIF 클라이언트)가 반드시 TLS v1.2 및 본 제품이 지원하는 암호 스위트를 지원해야 정상적으로 연결됩니다.

4.3. 관리 기능

제품의 보안 상태를 점검하고 안전하게 유지하기 위한 관리 기능입니다.

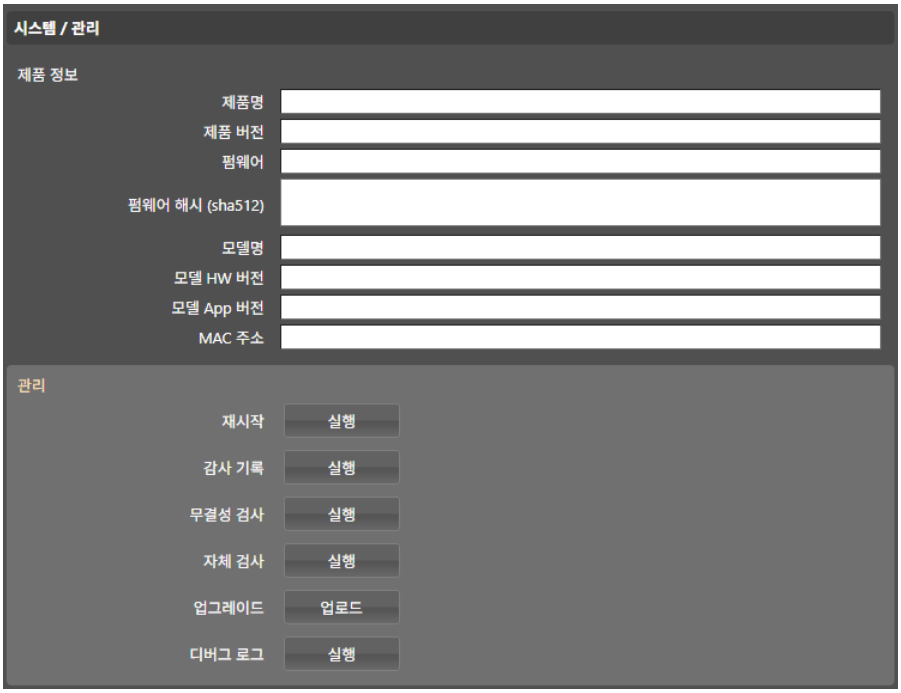


그림 13. 시스템 / 관리 메뉴

4.3.1. 제품 F/W 식별 정보 확인

제품에 설치된 펌웨어의 버전과 해시 값을 확인하여, 인가된 펌웨어가 설치되었는지 식별할 수 있습니다.

WebUI에 로그인한 후, 설정 > 시스템 > 관리 메뉴로 이동합니다.

펌웨어 버전 및 펌웨어 해시(SHA512) 항목을 확인하여, 2.2 에서 배포된 공식 펌웨어 정보와 일치하는지 확인합니다.

4.3.2. 무결성 검사

제품의 펌웨어 및 주요 설정 파일이 위변조되지 않았는지 검증하는 기능입니다.

1. WebUI에 로그인한 후, 설정 > 시스템 > 관리 메뉴로 이동합니다.

2. 무결성 검사 버튼을 클릭합니다.

3. 감사 기록에서 무결성 검사 결과가 각 항목별로 표시되는지 확인합니다.

4.3.3. 자체 검사

제품의 하드웨어 및 소프트웨어 모듈이 정상적으로 동작하는지 점검하는 기능입니다.

1. WebUI에 로그인한 후, 설정 > 시스템 > 관리 메뉴로 이동합니다.

2. 자체 검사 버튼을 클릭합니다.

3. 감사 기록에서 자체 검사 결과가 각 항목별로 표시되는지 확인합니다.

4.3.4. 업그레이드

제품의 펌웨어는 보안 패치 및 기능 개선을 위해 최신 상태로 유지해야 합니다. 본 제품은 서명 검증을 통해 인가된 펌웨어만 설치되도록 합니다.

1. 2.2 항목을 참조하여 최신 펌웨어 파일을 관리자 PC에 준비합니다.

2. WebUI에 로그인한 후, 설정 > 시스템 > 관리 메뉴로 이동합니다.

3. 업그레이드 - [업로드] 버튼을 클릭하여 펌웨어 파일을 지정합니다.

4. [실행] 버튼을 클릭하여 설치를 진행합니다.

시스템이 펌웨어 파일의 무결성을 검증한 후 설치를 진행합니다. 검증에 실패하면 업그레이드가 중단됩니다.

4.3.5. 감사 기록 조회

관리자 로그인 성공/실패, 설정 변경, 보안 이벤트 등 모든 주요 활동은 감사 기록으로 저장됩니다. 관리자는 이 기록을 정기적으로 점검하여 비인가된 활동이 있었는지 확인할 수 있습니다.

1. WebUI에 로그인한 후, 설정 > 시스템 > 관리 메뉴로 이동합니다.

2. 관리에서 '감사 기록' 을 선택합니다.

3. 로그인 실패, 설정 변경, IP 차단 등의 이력이 있는지 정기적으로 확인합니다.

4.4. 알림 및 통보 설정

본 제품은 시스템 운영 중 발생하는 중요 보안 이벤트 및 이상 징후를 관리자가 즉시 인지하고 대응할 수 있도록, WebUI 화면상의 알림과 이메일 통보 기능을 제공합니다.

4.4.1. WebUI 알림 확인

관리자가 WebUI에 로그인하여 모니터링 중, 중요 보안 이벤트가 발생하면 즉각적인 알림을 표시합니다.

1. 알림 발생 조건: 다음과 같은 주요 보안 이벤트 발생 시 알림이 발생됩니다.

   인증 연속 실패: 관리자 접속 계정에 대해 5회 연속 인증 실패가 발생한 경우 (비인가 접속 시도 의심)

   감사기록 손실 예고: 감사기록 저장 공간이 임계치에 도달하여, 기록이 삭제될 위험이 있는 경우

2. 알림 확인 방법:

   이벤트 발생 시, 아래 그림 과 같이 WebUI 상단에 [알림] 버튼이 활성화되어 나타납니다.

   해당 버튼을 클릭하면 발생한 이벤트의 정보가 팝업 창으로 출력됩니다.

그림 14. WebUI 알림 및 팝업 창

4.4.2 이메일 설정

관리자가 자리를 비우거나 WebUI에 접속해 있지 않은 상황에서도 중요 보안 이벤트를 수신할 수 있도록 이메일 통보 기능을 설정합니다.

이메일은 보안을 위해 Implicit SSL 방식만 제공합니다.

[중요] 정상적인 이메일 동작을 위해서는 SMTP 서버의 IP주소가 [네트워크] - [보안] - [IP 필터링]의 허용목록에 반드시 추가되어야 합니다.

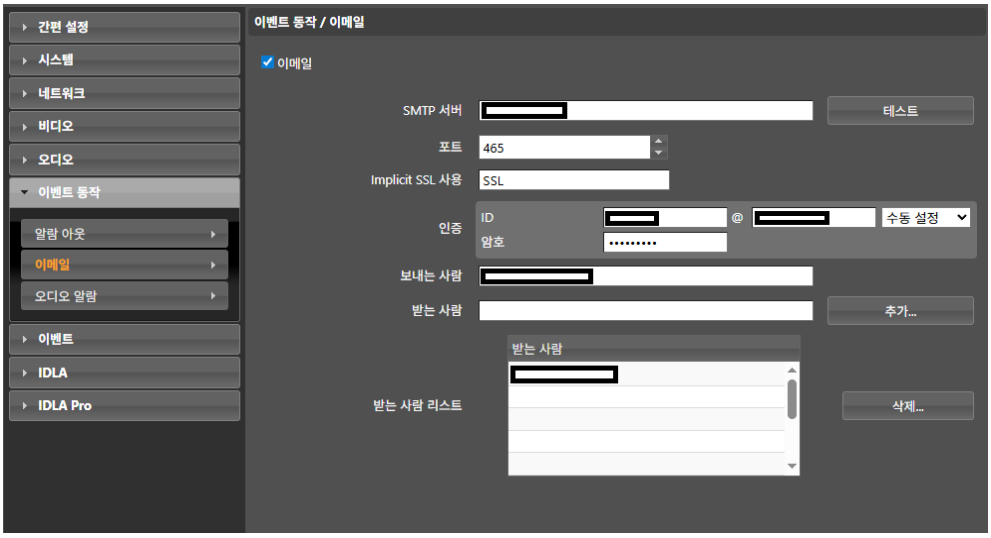


그림 15. 이메일 설정

5. 고객 지원

본 제품을 사용하는 중 발생하는 기술적인 문제나 기능에 대한 문의 사항이 있을 경우, 아래 고객지원센터를 통해 신속한 지원을 받으실 수 있습니다. 고객지원센터는 제품에 대한 전문적인 기술 지원 및 상담 서비스를 제공합니다.

홈페이지: http://www.watchcam.co.kr/board/online

대표번호: 1800-5143

홈페이지를 방문하시면 제품 관련 최신 정보와 다양한 기술 자료를 확인하실 수 있습니다.

보증 정책

제품 보증기간: 제품의 무상 보증기간은 구매일을 기준으로 2년입니다.

무상 보증 제외 및 사용자 귀책사유

-취급 부주의 및 과실: 고객의 고의 또는 과실로 인한 파손, 액체 유입(침수), 전원 이상으로 인한 고장.

-임의 분해 및 개조: 제조사가 지정하지 않은 수리 센터를 이용하거나 임의로 제품을 분해·개조한 경우.

6. 문제 해결 방법

6.1. 제품 오류 메세지

제품 운용 중 발생할 수 있는 주요 보안 관련 오류 메시지와 조치 방법은 다음과 같습니다.

표 12. 제품 오류 메시지

발생상황	오류메세지	원인 및 조치
WebUI	Login failed	원인: 계정 없음, 설정 권한 없음, 중복 권한의 계정이 접속되어 있음, IP 필터링 IP로 접속함, 여러 번의 접속 시도로 계정 잠금 등의 경우 조치: 설정 권한을 가진 계정으로, 중복 접속 되지 않게 확인하여 접속합니다.
WebUI	경고! 암호의 설정이 필요합니다.	원인: 금지된 사용자 ID, 중복된 사용자 ID, ID 와 PW 와 동한 경우, 패스워드가 규칙을 만족하지 않은 경우 조치: 보안 요구사항을 만족하는 ID, PW 로 계정을 생성합니다.
무결성검사	Integrity check failed	원인: 제품의 펌웨어나 설정파일이 비인가된 사용자에 의해서 변조되었을 경우, NAND 데이터가 외부 전기적 충격에 의해 손상된 경우 조치: 업그레이드를 시도합니다. 문제가 지속되면 고객지원센터에 문의합니다.

6.2. FAQ

Q1. WebUI 접속 시 브라우저에서 '안전하지 않음' 또는 '신뢰할 수 없는 인증서' 경고가 표시됩니다. 해킹된 것입니까?

A1. 아닙니다. 이는 해킹이 아니며 정상적인 현상입니다. 본 제품은 HTTPS 통신을 위해 **자체 서명 인증서(Self-Signed Certificate)**를 사용합니다. 공인된 기관에서 발급한 인증서가 아니므로 브라우저가 경고를 표시하는 것이며, 이는 3. IP 카메라 접속 장에서 안내한 바와 같이 신뢰할 수 있는 연결입니다. '예외 추가' 또는 '연결 계속'을 선택하여 진행합니다.

Q2. 관리자 계정을 등록한 후 '검색 도구'에서 카메라가 사라졌습니다. 고장입니까?

A2. 아닙니다. 고장이 아니며 의도된 보안 동작입니다. 3.1에서 설명한 바와 같이, 제품의 보안을 위해 최초 관리자 계정이 등록되고 나면 mDNS 검색 기능이 자동으로 중지됩니다. 이후에는 제품의 IP 주소를 직접 입력하여 접속해야 합니다.

Q3. IP 필터링 기능을 활성화했는데, 관리자 PC의 IP 주소가 변경되어 접속할 수 없습니다. 어떻게 해야 합니까?

A3. [경고] IP필터링은 강력한 접근 통제 기능으로, 등록된 IP 외에는 관리자라도 접속이 불가능합니다. 이 경우, 제품에 물리적으로 접근하여 **공장 초기화(Factory Reset)**를 수행해야만 IP필터링 설정을 초기화할 수 있습니다.

Q4. LOGIN_FAILED_SEVERAL_TIMES 감사 기록을 확인했습니다. 무엇을 해야 합니까?

A4. 4.3.5에서 설명한 바와 같이, 비정상적인 로그인 시도가 감지된 것입니다. 즉시 감사 기록에서 공격을 시도한 소스 IP 주소를 확인하고, 방화벽 또는 3.3의 IP필터링 기능을 사용하여 해당 IP 주소의 접근을 원천 차단할 것을 권고합니다.

- 끝 -

7. 캡션

7.1 그림 목차

7.2 표 목차