INSRM-C1-DC-T8871WRAI

보안기능 운용설명서 v1.0

[국가용 보안요구사항 V3.0 기반]

제·개정 이력

번호	버전	수정 날짜	내용
1	v1.0	25.10.14	국가용 보안요구사항 V3.0 기반의 INSRM-C1 v1 보안요구사항 운용설명서 작성

수정 전/후 내용 대비표

번호	수정 날짜	세부 항목	기존	수정 후
1	25.10.14	설명서 작성		v1.0
2				
3				

목 차

1. 개요

1.1. 문서 정보

표 1. 운용설명서 문서 정보

문서명	INSRM-C1-DC-T8871WRAI 보안기능 운용설명서
문서 버전	v1.0
파일명	INSRM-C1-DC-T8871WRAI 보안기능 운용설명서 v1.0.pdf
작성자	㈜아이디스
작성 일자	2025. 10. 14

1.2. 목적

본 제품은 IP 네트워크를 통해 영상을 촬영하고 전송하는 IP 카메라입니다. 제품의 일반적인 기능 사용법은 '사용자 운용설명서'에서 다루며, 본 문서는 제품의 보안 기능을 책임지는 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. 사용자 운용 설명서 구성

본 운용설명서는 다음과 같이 구성되어 있습니다.

· 1장은 사용자 운용설명서의 개요로, 설명서의 목적과 구성 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

· IDIS Network Installation Tool. 아이디스 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

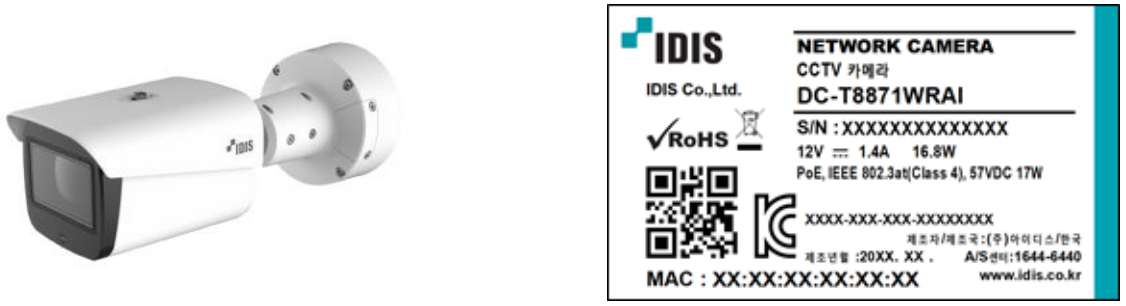
본 장에서는 제품의 주요 기능과 구성 요소, 그리고 보안 운용 시 반드시 숙지해야 할 주의사항에 대해 기술합니다.

본 제품 [INSRM-C1-DC-T8871WRAI]는 고해상도 8M 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 TLS v1.2 기반의 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 제품 구성 요소



(a) 제품 사진 (b) 제품본체 및 포장에 부착되는 식별정보

그림 1. 제품 배포 구성물 및 식별 정보

본 제품의 운용 환경을 구성하는 핵심 식별 정보와 운영 체제는 아래 **오류! 참조 원본을 찾을 수 없습니다.**와 같다.

표 2. 제품 식별정보 및 운용 환경

구분	내용
제품명	INSRM-C1-DC-T8871WRAI
버전	v1.0.0.1-110
구성요소(F/W)	INSRM-C1-v1.0.0.1-DCT8871WRAI-dome_si-nsr-110-1101.rui
H/W 모델명	DC-T8871WRAI
제품 모델명	INSRM-C1-DC-T8871WRAI
문서 - 매뉴얼	아이디스_IP카메라_DC-T8871WRAI_제품설명서 아이디스_IP카메라_보안기능_운용설명서

2.2. 제품 F/W 다운로드

당사 홈페이지(https://partners.idisglobal.com) 내 [자료 다운로드]에서 F/W 파일을 다운로드 할 수 있습니다.

[중요] 펌웨어 파일 다운로드 시, 파일의 해시값을 비교하여 펌웨어의 무결성을 반드시 확인해야 합니다.

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.

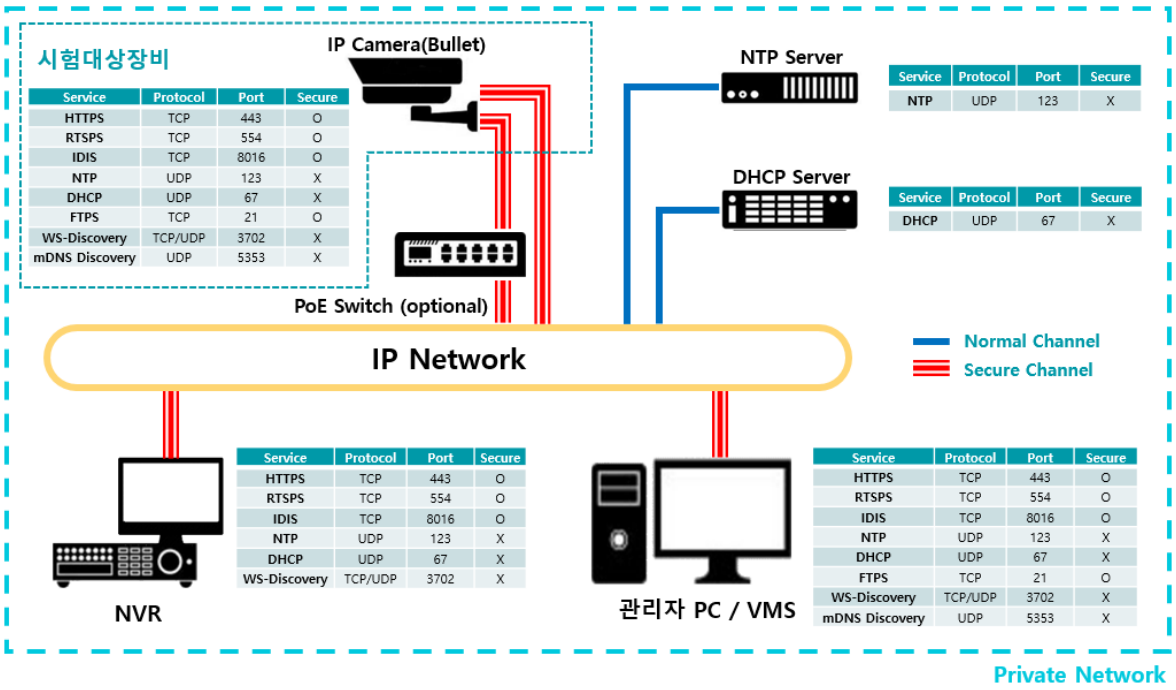
2. 네트워크 환경: 제품은 신뢰할 수 있는 방화벽 내부의 보안 네트워크 환경에서 운용되어야 합니다. 신뢰할 수 없는 외부 네트워크에 제품을 직접 노출하는 것을 금지합니다.

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.

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



Service	Protocol	Port	Secure
HTTPS	TCP	443	O
RTSPS	TCP	554	O
IDIS	TCP	8016	O
NTP	UDP	123	X
DHCP	UDP	67	X
FTPS	TCP	21	O
WS-Discovery	TCP/UDP	3702	X
mDNS Discovery	UDP	5353	X

Service	Protocol	Port	Secure
NTP	UDP	123	X

Service	Protocol	Port	Secure
DHCP	UDP	67	X

Service	Protocol	Port	Secure
HTTPS	TCP	443	O
RTSPS	TCP	554	O
IDIS	TCP	8016	O
NTP	UDP	123	X
DHCP	UDP	67	X
WS-Discovery	TCP/UDP	3702	X

Service	Protocol	Port	Secure
HTTPS	TCP	443	O
RTSPS	TCP	554	O
IDIS	TCP	8016	O
NTP	UDP	123	X
DHCP	UDP	67	X
FTPS	TCP	21	O
WS-Discovery	TCP/UDP	3702	X
mDNS Discovery	UDP	5353	X

그림 2. IP카메라 운용환경 표준구성도

3. IP카메라 접속

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

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

3.1. 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 3. INIT(네트워크 비디오 설치 도구)에서 제품 검색

3.2. 관리자 계정 등록

제품에 최초로 접속하면, 보안을 위해 관리자 계정 등록이 강제됩니다.

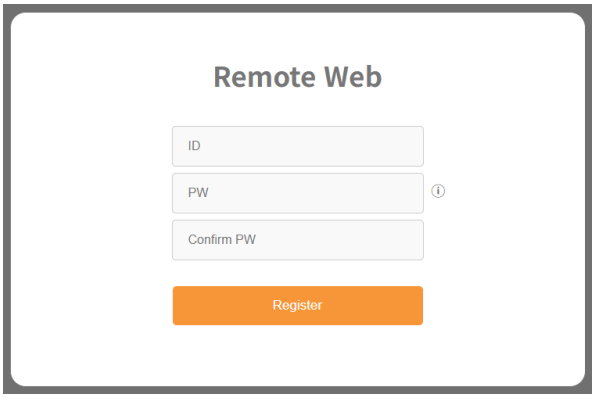


그림 4. 관리자 계정 최초 등록창

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. 아래와 같은 관리자 계정 등록 화면이 나타나면, 새 관리자 ID와 강력한 비밀번호를 입력합니다.

[중요] 비밀번호 정책: 관리자 비밀번호는 대문자, 소문자, 숫자, 특수문자 조합 9자리 이상을 준수해야 합니다.

4. [Register] 버튼을 클릭하여 계정 생성을 완료합니다.

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

3.3. 관리자 PC주소 등록

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

그림 5. 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.

4. 보안 기능 설정

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 6. 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.

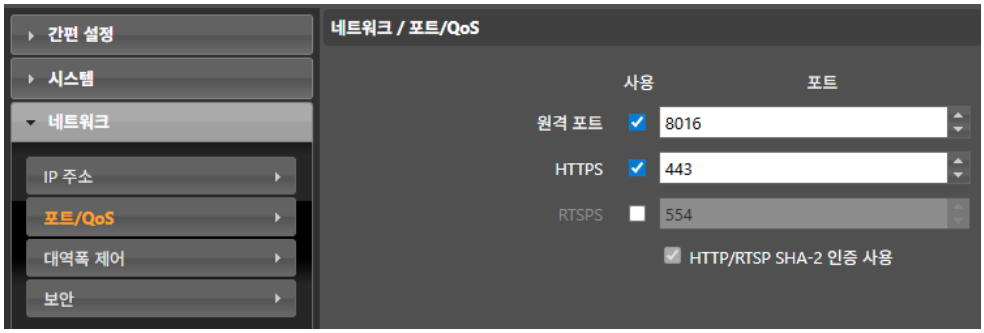


그림 7. 아이디스 프로토콜 설정

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.

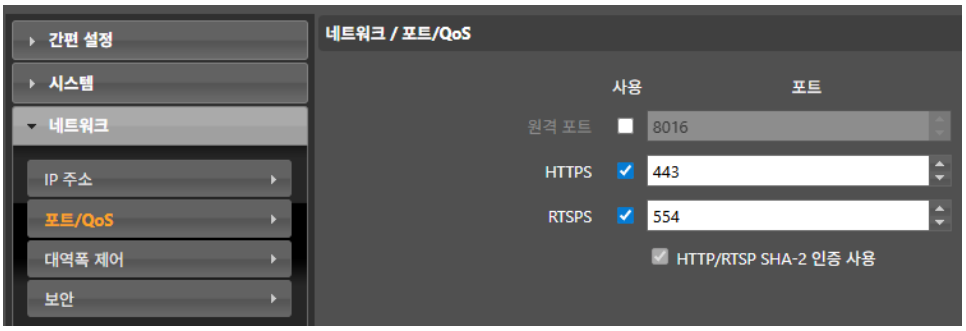


그림 8. RTSPS 활성화 설정

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 9. ONVIF 활성화 설정

[중요] 연동하려는 VMS(ONVIF 클라이언트)가 반드시 TLS v1.2 및 본 제품이 지원하는 암호 스위트(ECDHE-RSA-CHACHA20-POLY1305 등)를 지원해야 정상적으로 연결됩니다.

4.3. 관리 기능

제품의 보안 상태를 점검하고 안전하게 유지하기 위한 관리 기능입니다.

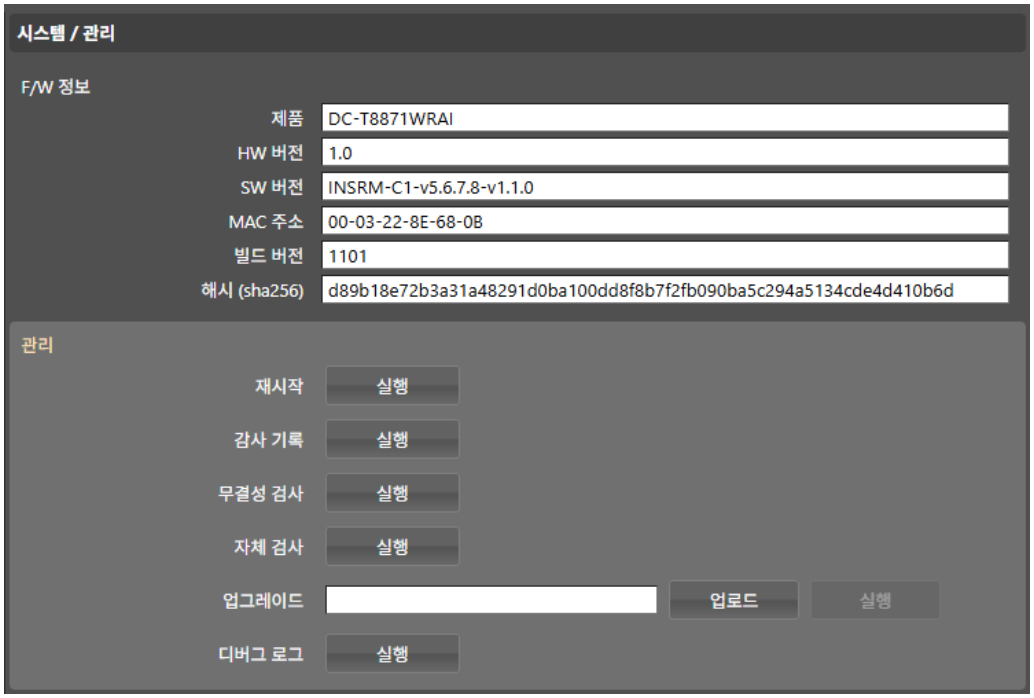


그림 10. 시스템 / 관리 메뉴

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(SHA256) 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.

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: https://www.idisglobal.com/index/servicecenter

대표번호: 1644-6440

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

보증 정책

제품 보증기간: 제품의 무상 보증기간은 구매일을 기준으로 3년입니다. (구매 영수증 증빙 필요)

수리 부품 보증: 유상으로 수리한 부품에 대해, 수리일로부터 180일 이내에 동일한 고장이 재발할 경우 무상으로 수리해 드립니다.

부품 보유기간 및 보상: 수리용 부품은 제품 단종 시점으로부터 5년간 보유합니다. 부품 보유기간 내에 수리가 불가능할 경우, 정해진 기준(잔존가치(%) x 당초 제품 구입가)에 따라 보상해 드립니다.

6. 부록

6.1. 제품 오류 메세지

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

표 3. 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