

White Paper

# 디바이스 매니저

2024년 1월 5일

## 1. 개요

## 2. 시스템 요구 사항

## 3. 설치 방법

### 3.1. 다운로드 및 설치 가이드

#### 3.1.1. 다운로드 경로

#### 3.1.2. 설치 가이드

#### 3.1.3. 디바이스 매니저 실행 방법 가이드

## 4. 사용자 가이드

### 4.1. 화면 구성

### 4.2. 카메라 검색

### 4.3. 카메라 장비 목록

#### 4.3.1. 장비 목록 검색 및 설정

#### 4.3.2. 장비 목록 그룹화

### 4.4. 로그인 및 IP 설정

#### 4.4.1. 로그인

#### 4.4.2. IP 설정

### 4.5. 리포트

### 4.6. 펌웨어

### 4.7. 설정 백업 및 복원

### 4.8. 인증서 설정

#### 4.8.1. 공인 인증서

#### 4.8.2. HTTPS 클라이언트 인증서

#### 4.8.3. 802.1x 인증서 설정

## 4.9. 인증서 관리

### 4.9.1. HTTPS 설정

### 4.9.2. IEEE 802.1x 설정

## 4.10. 장비 설정

### 4.10.1. 비디오 프로파일

### 4.10.2. 날짜 & 시간

### 4.10.3. IP & 포트

### 4.10.4. 비디오 설정

### 4.10.5. 오디오 설정

### 4.10.6. 카메라 설정

### 4.10.7. 포커스 설정

### 4.10.8. 칼라 팔레트

### 4.10.9. SNMP

### 4.10.10. IP 자동 설정

### 4.10.11. 이벤트 설정

### 4.10.12. 멀티캐스트

### 4.10.13. 언어

### 4.10.14. 재시작

### 4.10.15. 로그

### 4.10.16. 디버그 로그

### 4.10.17. 오픈 플랫폼

### 4.10.18. 와이즈디텍터

## 5. 결론

# 1. 개요

한화비전의 디바이스 매니저는 간편하고 효율적으로 영상감시 장비를 관리할 수 있게 도와주는 솔루션으로, 다양한 장비를 효과적으로 관리하고 모니터링 할 수 있는 기능을 제공합니다.

디바이스 매니저를 통해 사용자는 중앙 집중식 인터페이스에서 모든 디바이스를 한눈에 볼 수 있으며, 이를 통해 장비의 상태, 작동 정보, 센서 데이터 등을 실시간으로 모니터링할 수 있습니다. 또한 네트워크에 연결된 장비들의 기본적인 기능 설정을 한번에 진행할 수 있습니다. 뿐만 아니라 각 장비의 펌웨어 버전을 확인하고, 최신 버전으로 원격 업데이트할 수 있으며 인증서 등록 및 관리 기능을 지원하여 보안 관리를 보다 용이하게 지원합니다.

디바이스 매니저 가 제공하는 세부적인 기능은 다음과 같습니다.

- 동일 네트워크 망에 설치되어 있는 장비를 자동으로 검색
- 제품군 별 카테고리로 분류하여 관리
- 검색되지 않는 장비를 수동으로 등록
- 사용 목적에 따라 장비를 프로젝트별로 분리하여 관리, 각 프로젝트별 비밀번호 설정으로 보안 관리 가능
- 동일 네트워크 망에서 검색된 여러 대의 장비에 대한 기본적인 기능 설정
- 등록된 장비에 대한 펌웨어 버전 확인 및 업데이트
- 등록된 장비에 대한 자격/인증서 관리
- 등록된 장비의 설정 값 불러오기/내보내기 기능
- 등록된 장비의 시스템 로그 확인

한화비전 디바이스 매니저는 간편한 사용자 인터페이스와 강력한 기능을 결합하여 사용자의 장비 관리 업무를 효율적으로 지원합니다. 본 백서에서는 한화비전 디바이스 매니저의 설정과 사용 방법 내용에 대하여 기술합니다. 상세한 설명은 디바이스 매니저 사용 설명서를 참조하십시오.

## 2. 시스템 요구 사항

디바이스 매니저를 설치하고 사용하려면 다음과 같은 환경이 필요합니다.

- 운영 체제: 윈도우 7, 10, 11 (64 비트)
- 응용 프로그램: Microsoft .NET Framework 4.7.2 Client Profile,  
Microsoft Visual C++ 2010 재배포 가능 패키지(x86)  
(장치 관리자 설치 패키지에 포함)
- CPU: Intel CPU i5 8세대 이상
- 그래픽: 비디오 그래픽 카드
- RAM: DDR4 8G 이상
- 해상도: 1366x768(공식적으로 확대 지원은 없습니다.)
- 네트워크 포트
  - IP/TCP Based  
HTTP: 80  
HTTPS: 443  
RTSP: 554
  - UDP Based  
검색, IP 설정, 초기 비밀번호 : 7701, 7711

### 참고

디바이스 매니저에서 와이즈디텍터를 작동할 경우 시스템 요구 사항은 달라질 수 있습니다.  
(예 : 와이즈디텍터를 사용하는 경우에 한하여 Microsoft Visual C++ 2015~2022 버전 필요) 디바이스 매니저는 네트워크 망에서 검색된 카메라 정보를 와이즈디텍터에 전달하여 해당 카메라의 라이브 영상에 연결할 수 있도록 합니다. 와이즈디텍터를 이용하면 연결된 카메라 영상을 기반으로 머신러닝 기반 방식으로 학습 데이터를 생성하고, 카메라가 객체 감지를 수행하는데 활용할 수 있도록 학습 데이터를 카메라에 전송할 수 있습니다. 와이즈디텍터 호환을 지원하는 카메라에서만(예 : P AI 시리즈) 사용 가능합니다. 보다 상세한 내용은 디바이스 매니저의 온라인 도움말을 참고하십시오.

## 3. 설치 방법

### 3.1. 다운로드 및 설치 가이드

#### 3.1.1. 다운로드 경로

한화비전 웹사이트에서 설치 프로그램을 다운로드할 수 있습니다.

한화비전 웹사이트 (<https://www.hanwhavision.com>)에 접속한 후 [지원]>[Online Tool]>[PC 설치용 tool]>[Wisenet 디바이스 매니저]에서 [다운로드]를 클릭하십시오.

혹은 아래 링크를 클릭하면 설치 프로그램을 다운로드할 수 있습니다.

- 영문: <https://www.hanwhavision.com/en/support/online-tool>
- 국문: <https://www.hanwhavision.com/ko/support/online-tool>

#### 3.1.2. 설치 가이드

- 1) 다운로드한 디바이스 매니저 설치 프로그램을 더블 클릭합니다.
- 2) [Installer Language] 창에서 원하는 언어를 선택합니다. (English/Korean 택 1)
- 3) [Wisenet Device Manager 설치] 창에서 사용권 계약 정보를 확인하고 설치 위치를 선택하면 설치가 진행됩니다.
- 4) 설치가 완료되면 [마침]을 클릭하고 [Wisenet Device Manager 설치] 창을 닫습니다. [Wisenet Device Manager 실행하기] 체크 박스를 선택하면 프로그램이 바로 실행됩니다.

#### 3.1.3. 디바이스 매니저 실행 방법 가이드

- 1) PC 에 설치된 디바이스 매니저를 실행합니다.
- 2) 새 프로젝트를 생성하거나 기존 프로젝트를 선택할 수 있습니다.

새 프로젝트: [새 프로젝트] 창이 나타나면 프로젝트 이름과 경로를 설정

프로젝트 추가: 추가할 프로젝트 폴더 경로로 이동 후 프로젝트 파일(\*.xml)을 추가하여 프로젝트 목록에 추가

프로젝트 선택: 프로젝트 목록에서 실행할 프로젝트를 선택한 이후 [열기] 클릭

#### 참고

[마지막에 불러온 프로젝트 자동 실행]을 선택하면, 다음 디바이스 매니저 실행 시 [프로젝트 열기] 창이 뜨지 않고 해당 프로젝트가 바로 실행됩니다.

## 4. 사용자 가이드

### 4.1. 화면 구성

디바이스 매니저 화면은 아래와 같이 구성됩니다.



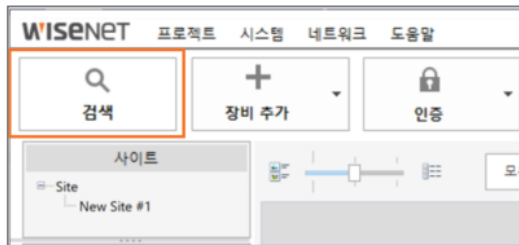
명칭		기능 설명
①	메뉴	프로그램 관련 기능 제공
②	도구 모음	장비 제어 설정
③	레이아웃 선택 바	등록된 장비 목록 보기 방식 선택 (왼쪽부터 스냅샷 제공/모든 정보 나열/채널별 프로파일 표시)
④	선택 툴	등록된 장비 선택
⑤	모두 업데이트	등록된 모든 장비 상태 업데이트
⑥	그룹화	장비 목록을 그룹화하여 표시

⑦	장비 설정 메뉴	선택된 장비의 기능을 설정
⑧	장비 목록	등록된 장비들의 목록 표시
⑨	네트워크 상태	현재 사용중인 PC의 네트워크 상태 및 IP주소를 표시
⑩	필터링	검색된 장비들을 제품군으로 분류하여 목록에 표시
⑪	사이트	장비들을 사이트 단위로 그룹 지어 관리

## 4.2. 카메라 검색

동일한 네트워크 상에 연결되어 있는 한화비전 장비를 검색합니다.

1) 도구 모음에서 [검색]을 클릭하면 장비가 검색됩니다.



2) 검색 후 네트워크에 연결된 장비 목록이 표시됩니다.

### 참고

장비 검색 시간은 [시스템]>[장비 검색 시간 설정]에서 설정할 수 있습니다. (기본 5초 / 최대 60초, 5초 단위 설정)

NVR 장비는 IP 충돌로 인해 검색이 안 될 수 있습니다. 이 경우 NVR 장비의 설정 메뉴에서 네트워크 설정을 확인합니다. 자세한 사항은 제품 매뉴얼을 참고하십시오.

장비가 검색되지 않을 경우, 장비와 연결된 공유기나 허브 등의 연결 상태를 확인합니다.

공유기가 2대 이상 연결되어 있을 경우 IP 충돌을 방지하기 위해 공유기 한 대는 허브 모드로 설정하여 사용할 것을 권장합니다.

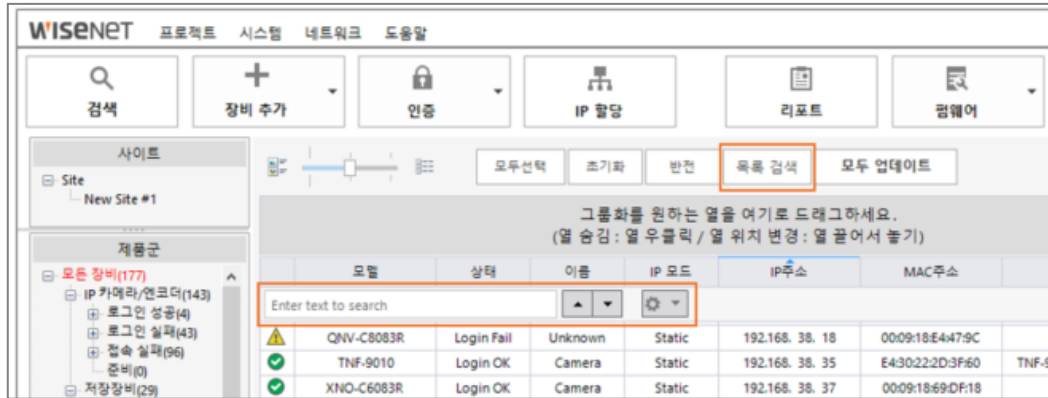
## 4.3. 카메라 장비 목록

### 4.3.1. 장비 목록 검색 및 설정

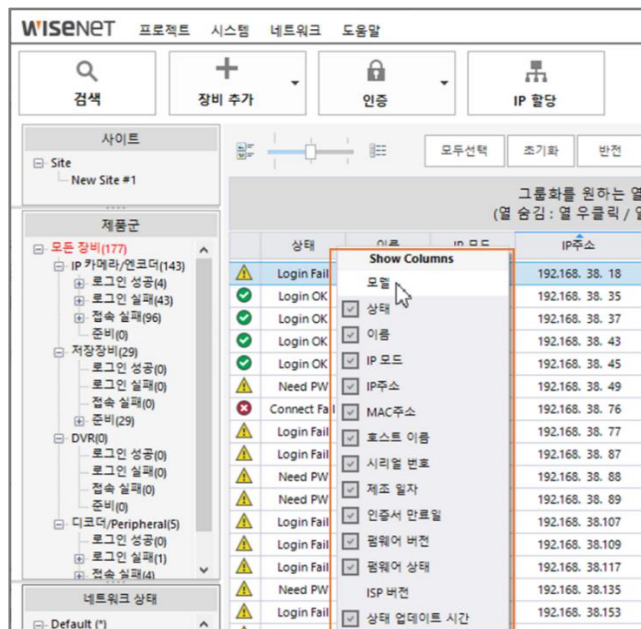
장비 목록 내에서 원하는 장비를 검색할 수 있습니다.

1) [목록 검색]을 클릭하거나 Ctrl + F 키를 입력하면 검색 창이 나타납니다.





- 2) 입력 창에 검색할 내용을 입력합니다.
- 3) 입력 창 옆의 화살표(▲▼)를 클릭하면 입력된 값이 포함된 항목만 빠르게 검색할 수 있습니다.
- 4) 검색 옵션 아이콘(⚙️)을 클릭하여 검색할 옵션을 설정합니다.
- 5) 장비 목록의 특정 열을 보이거나 숨기도록 설정할 수 있습니다.
  - 임의의 열을 마우스 오른쪽으로 클릭합니다.
  - 장비 목록에서 노출할 열 만 체크박스를 선택합니다.

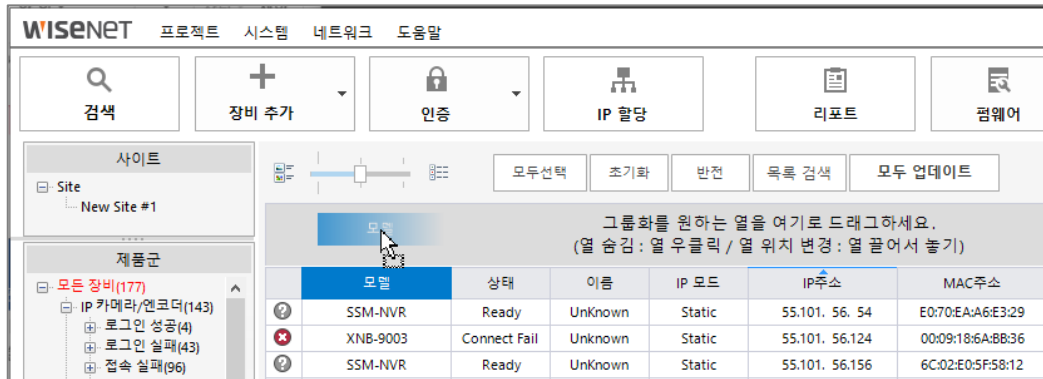


열 위치를 변경하려면 위치를 변경하려는 열을 마우스로 클릭한 상태에서 이동하고자 하는 위치로 이동시킵니다.

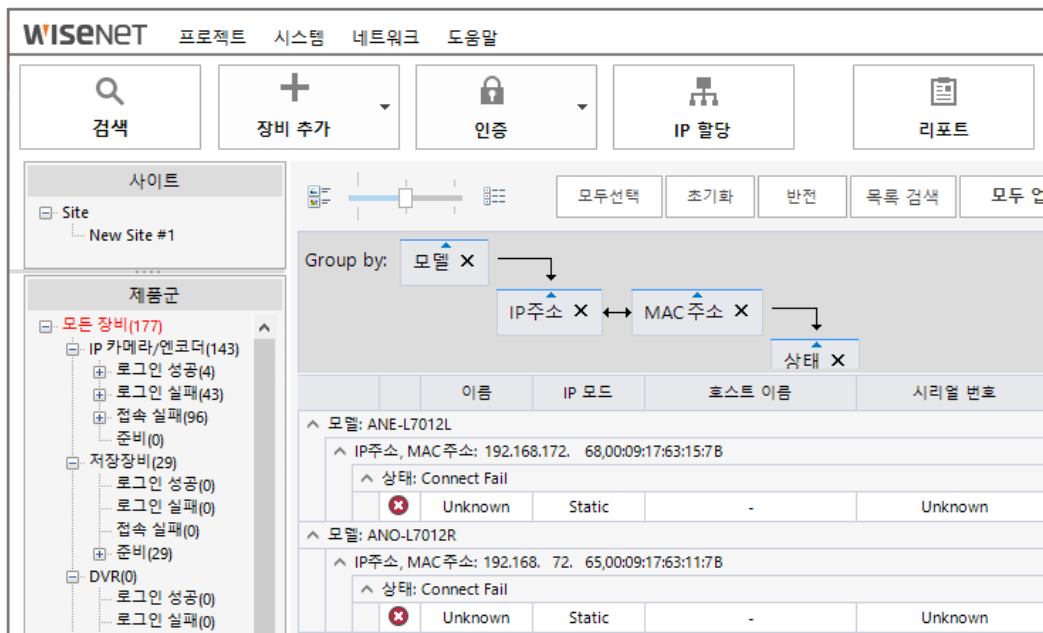
### 4.3.2. 장비 목록 그룹화

장비 목록을 원하는 그룹으로 모아서 표시할 수 있습니다.

1) 원하는 열을 선택한 후 그룹화 영역으로 드래그합니다.



2) 설정한 그룹과 레벨에 따라 장비 목록이 표시됩니다.



## 4.4. 로그인 및 IP 설정

로그인 및 IP 설정에 SUNAPI (HTTP(s) 공통 프로토콜)을 사용합니다.

장비 검색 시 비밀번호가 설정되지 않은 장비를 발견한 경우, 안내 메시지를 제공하며, 이후 사용자가 초기 암호를 지정할 수 있습니다.

### 참고

장비와 비밀번호 정보를 포함한 데이터를 통신할 경우, 각 장비 고유의 RSA 키를 사용하여 암호화한 이후 데이터 통신을 진행하여 안전하게 암호 데이터를 보호하고 있습니다.

#### 4.4.1. 로그인

등록된 장비에 대한 설정을 디바이스 매니저에서 직접 변경하려면 해당 장비의 관리자 비밀번호를 입력하고 인증해야 합니다.

- 1) 장비 목록에서 장비를 선택합니다.
- 2) [인증]을 클릭합니다.

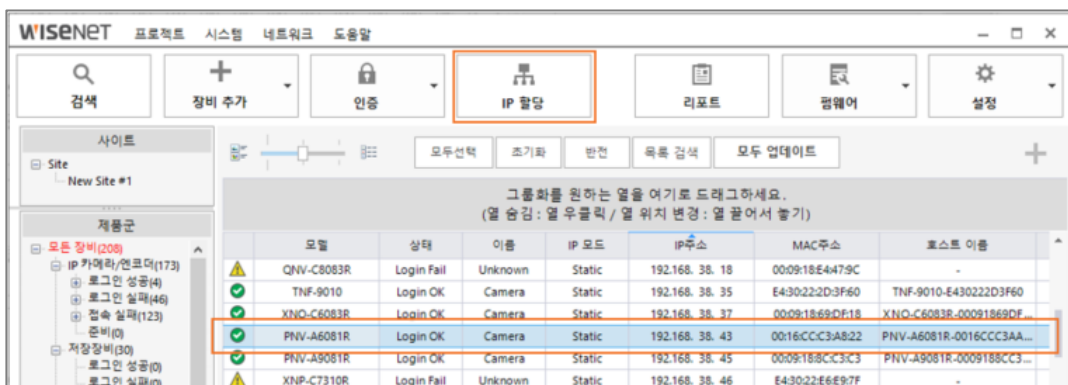


- 3) 사용자 아이디 및 비밀번호를 입력한 후 [적용]을 클릭합니다.
- 4) 로그인 상태가 각 장비의 [결과] 항목에 표시됩니다.

#### 4.4.2. IP 설정

장비의 IP주소를 설정하는 기능으로 여러 대의 장비IP를 한번에 설정할 수 있습니다.

- 1) 장비 목록에서 장비를 선택합니다.
- 2) [IP 할당]을 클릭합니다.



- 3) IP 주소를 DHCP 를 통해 자동으로 할당 받으려면, [IP 주소 할당] 창에서 [IP 주소 자동 할당(DHCP)]을 선택한 후 포트 및 DNS 관련 항목을 입력하고 [적용]을 클릭합니다.

- 4) 고정(static) IP 를 설정하려면, [IP 주소 할당] 창에서 [해당 IP 주소 적용]을 선택한 후 IP 관련 항목 및 포트 관련 항목을 입력하고 [적용]을 클릭합니다.
- 5) 복수의 장비를 한번에 설정하려면 1 번 단계에 복수의 장비를 설정하고 [IP 할당]을 클릭합니다.
- 6) [IP 주소 할당] 창에서 [해당 IP 주소 적용]을 선택한 후, 할당할 IP 주소 범위의 시작 주소 및 IP 관련 항목, 포트 관련 항목을 입력하고 [시뮬레이션]을 클릭합니다.
- 7) 각 장비마다 할당될 IP 주소를 확인한 후 [적용]을 클릭합니다.

## 4.5. 리포트

장비의 정보를 기록한 파일을 생성하고 "xls" 또는 "csv" 형식으로 저장할 수 있습니다.

장치 정보 수집을 위해서 SUNAPI (HTTP(s) 공통 프로토콜)을 사용합니다.

- 1) 장비 목록에서 리포트 파일을 생성할 장비를 선택합니다.
- 2) [리포트]를 클릭합니다.
- 3) [리포트] 창이 뜨면, 리포트를 생성할 장비를 선택한 뒤 [Viewer]를 클릭합니다.

Report

Device Type : IP Camera/Encoder

<input checked="" type="checkbox"/>	Model	MAC	IP Address	Type	Status
<input checked="" type="checkbox"/>	PNV-A6081R	E4:30:22:5F:37:56	192.168.1.100	IP Camera/Encoder	0%

☐ Include Image  
☒ Low Resolution ☐ High Resolution

Viewer

Total : 1 , Success : 0 , Fail : 0

4) 장비 정보를 확인한 후 [Excel Export]를 클릭합니다.

ReportViewerForm

Drag a column here to group by this column.

Channel	Model	Status	Camera Name	IP Mode	IP Address	Gateway	Subnet Mask	MAC Address	S/N	F/W Version	Http	Https	Http Port	Https Port	DNS1	D
Single	PNV-A6081R	Ok	Camera	DHCP	192.168.1.100	192.168.1.1	255.255.255.0	E4:30:22:5F:37:56	ZR986V4T900010N	2.21.06_20230414_R373	Enable	Enable	80	443	168.126.63.1	168.1

Excel Export

5) [다른 이름으로 저장] 대화 상자에서 저장할 폴더 위치와 파일 형식을 선택한 후 [저장]을 클릭합니다.

참고

이미지를 포함하려면 "include Image" 체크박스 체크 이후 [저해상도] 또는 [고해상도]를 선택합니다.

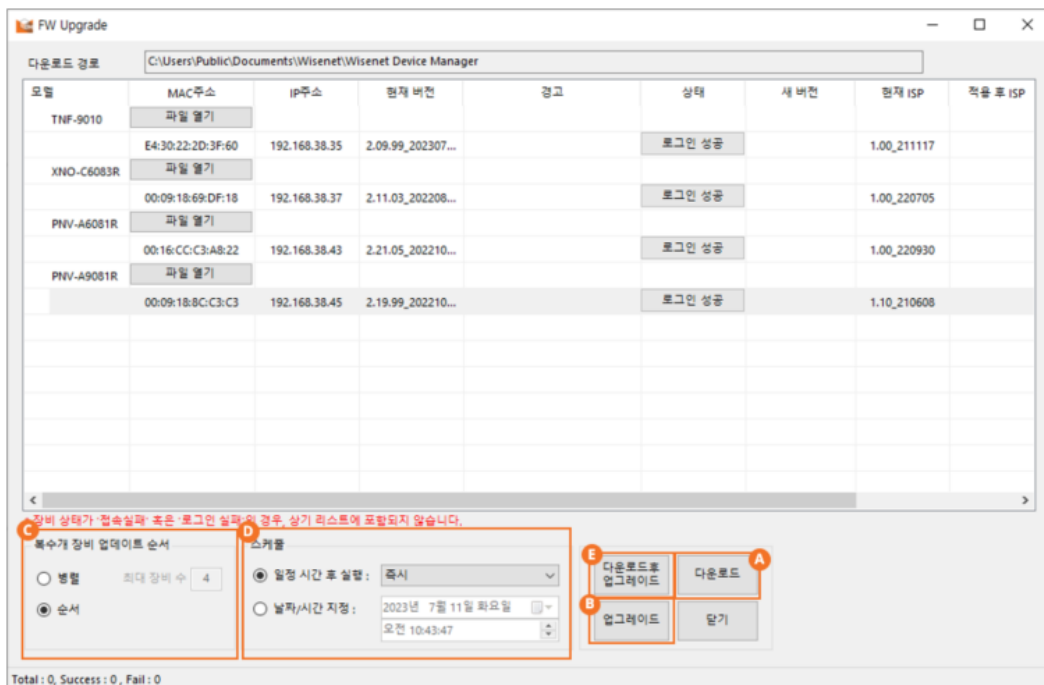
CSV 형식으로 리포트를 저장하면, 이미지는 포함되지 않습니다.

## 4.6. 펌웨어

인증이 완료된 장비의 펌웨어 상태를 확인하고 펌웨어 업데이트를 할 수 있습니다.

장치 펌웨어 업그레이드에 SUNAPI (HTTP(s) 공통 프로토콜)를 사용합니다.

- 1) 장비 목록에서 펌웨어를 업데이트할 장비를 선택합니다.
- 2) [펌웨어]>[펌웨어 업데이트]를 클릭합니다.
- 3) [FW Upgrade] 창에서 다음을 수행할 수 있습니다.



A. 장비의 펌웨어를 선택하여 다운로드합니다.

- 펌웨어 다운로드 지원을 위해 별도의 클라우드 서버를 사용하고 있으며, 해당 서버는 당사 내 네트워크 보안관리 팀 산하에서 운영되고 있습니다.

B. 다운로드한 펌웨어가 있을 경우 펌웨어 업그레이드를 진행합니다.

C. 여러 대의 장비를 업그레이드할 경우 진행 방식을 선택합니다.

- 병렬: 동시에 최대 16 대씩 업그레이드를 진행할 수 있습니다. 진행되는 대수는 변경 가능합니다.
- 순서 업그레이드를 한 대씩 순서대로 진행합니다.

D. 자동으로 펌웨어 업그레이드를 실행할 시간을 설정할 수 있습니다.

- 일정 시간 후 실행: 선택한 시간 이후에 펌웨어 업그레이드가 실행됩니다.
- 날짜/시간 지정: 선택한 날짜/시간에 펌웨어 업그레이드가 실행됩니다.

#### 참고

펌웨어 창이 닫혀 있는 경우, 설정한 예약 시간에 업그레이드를 진행할 수 없습니다. 반드시 펌웨어 창이 실행된 상태가 유지되어야 합니다.

- E. 최신 펌웨어를 다운로드하여 바로 업데이트를 진행합니다. [복수 장비 업데이트 순서]에서 [순서]로 선택해야 실행할 수 있습니다.

#### 참고

수동으로 펌웨어를 확보하여 업그레이드할 수 있습니다. 별도의 경로를 통해 확보한 펌웨어를 디바이스 매니저가 있는 PC에 설치한 다음, [파일 열기]를 사용하여 펌웨어를 설치한 폴더 위치를 검색하여 업그레이드 작업을 진행하면 됩니다.

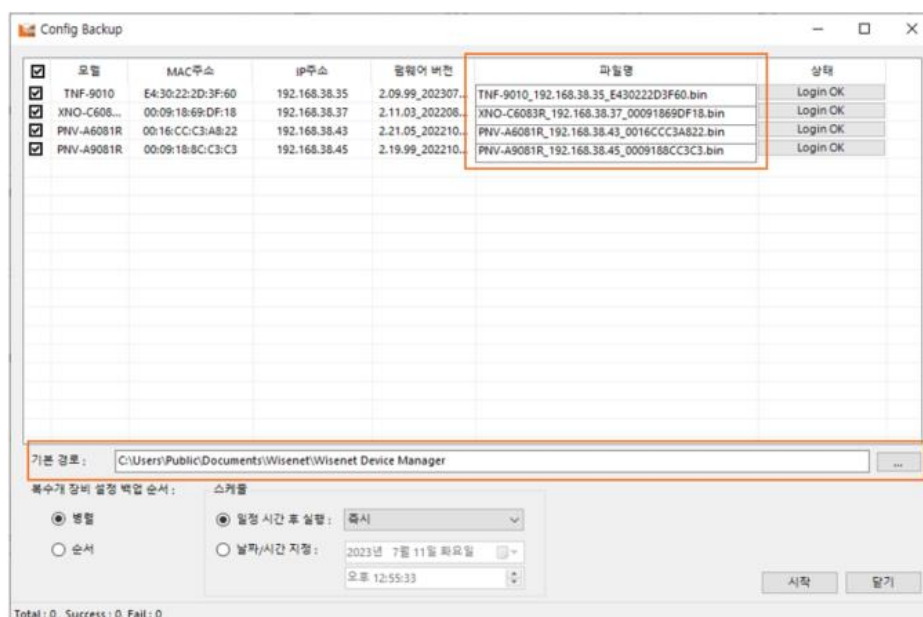
## 4.7. 설정 백업 및 복원

장비의 설정 정보를 저장하거나 불러올 수 있습니다.

장치 설정 백업 및 복구에 SUNAPI(HTTP(s) 공통 프로토콜)를 사용합니다.

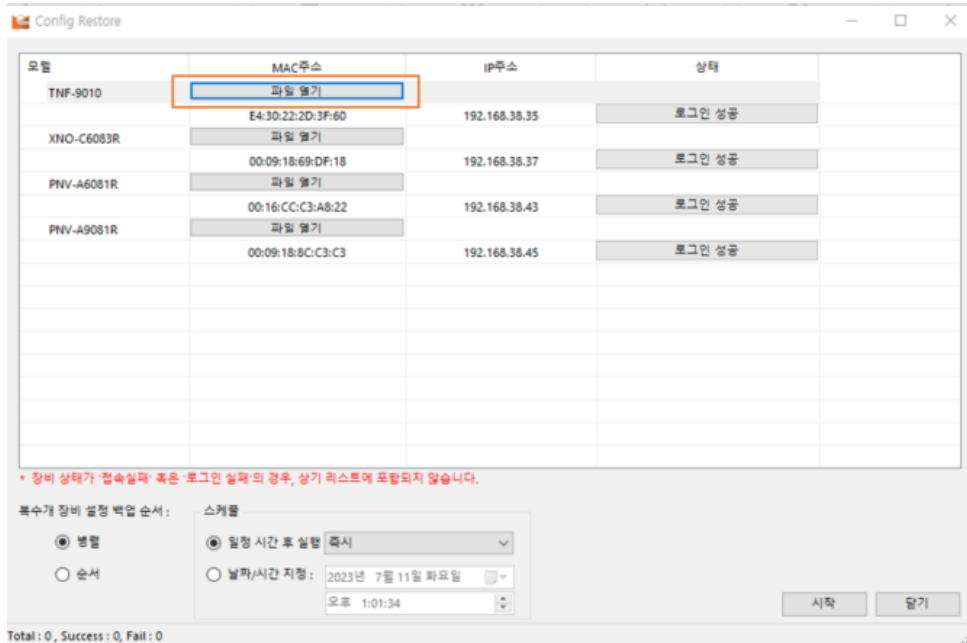
### 설정 백업

- 1) 장비 목록에서 장비를 선택합니다.
- 2) [설정]>[설정 백업]을 클릭합니다.
- 3) [Config Backup] 창이 나타나고, 장비별 설정 백업 파일명이 표시됩니다.
- 4) 백업 파일이 저장될 경로를 확인한 후, [시작]을 클릭합니다.



## 설정 복원

- 1) 장비 목록에서 장비를 선택합니다.
- 2) [설정]>[설정 복원]을 클릭합니다.
- 3) [Config Restore] 창에서 장비를 선택한 후 [파일 열기]를 클릭합니다.



- 4) 적용할 설정 파일을 선택합니다.

## 참고

여러 대의 장비 설정을 백업하거나 복원할 경우 진행 방식을 선택할 수 있습니다.

- 병렬: 설정 백업이나 복원을 동시에 최대 16대씩 진행할 수 있습니다. 진행되는 대수는 변경 가능합니다.
- 순서: 설정 백업이나 복원을 한대 씩 순서대로 진행합니다.

설정 백업이나 복원 실행 시간을 설정할 수 있습니다.

- 일정 시간 후 실행: 선택한 시간 이후에 설정 백업이나 복원이 실행됩니다.
- 날짜/시간 지정: 선택한 날짜/시간에 설정 백업이나 복원이 실행됩니다.

## 참고

[Config Backup] 창이나 [Config Restore] 창이 닫혀 있는 경우, 설정한 예약 시간에 설정 및 백업을 진행할 수 없습니다. 반드시 [Config Backup] 창이나 [Config Restore] 창이 실행된 상태가 유지되어야 합니다.

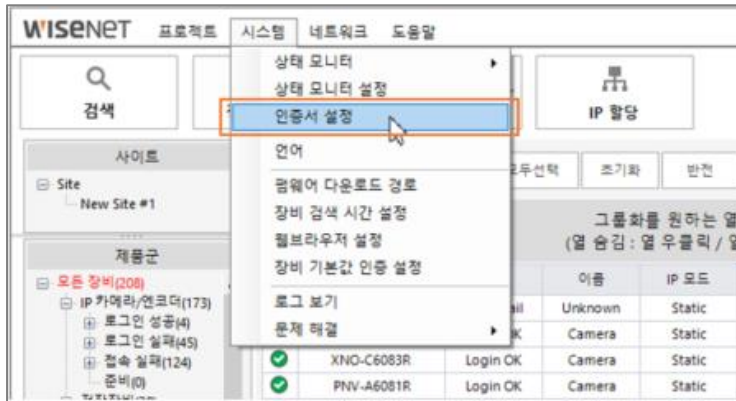
## 4.8. 인증서 설정



[인증서 설정] 창을 열려면, [시스템]> [인증서 설정]을 선택합니다.

#### 참고

인증서의 방식은 공개 키 기반(PKI)의 ITU-T 표준인 X509 v3 입니다. 인증서는 서명과 키에 RSA, sha256 알고리즘으로 암호화되어 있으며, PKCS#1, PKCS#7, **PKCS#8**과 PKCS#12를 지원하고 있습니다.



인증서 설정 창에서 HTTPs와 802.1x에서 적용할 인증서를 설정할 수 있습니다.

인증서 설정은 프로젝트 별로 저장됩니다.

A screenshot of the '인증서 설정' (Certificate Setting) dialog box. It has a title bar with a close button. The dialog is divided into several sections: 1. '공인 인증서' (Public Certificate) section with fields for '인증서 이름' (Certificate Name) and buttons for '인증서 생성' (Generate), '인증서 보기' (View), '인증서 저장' (Save), '인증서 갱신' (Renew), '가져오기' (Import), and '내보내기' (Export). There is also a checkbox for '인증서 비밀번호 저장' (Save certificate password). 2. 'HTTPS 클라이언트 인증서' (HTTPS Client Certificate) section with fields for '클라이언트 유효 기간' (Client validity period) set to 2 years, '인증서 만료 알림(일)' (Certificate expiration notice) set to 30 days, and '일반 이름' (Common name) set to 'Device IP Address'. 3. '802.1x 설정' (802.1x Setting) section with a checkbox for 'Device Manager의 CA, 클라이언트 인증서 사용(CA 인증서 설정 필요)' (Use CA, client certificate in Device Manager (CA certificate setting required)). Below this are fields for 'CA Certificates', '클라이언트 인증서' (Client certificate), and '클라이언트 사설 키' (Client private key), each with a '가져오기' (Import) button. 4. '인증서' (Certificate) section with fields for 'EAP Type' (set to EAP-TLS), 'EAPOL Version' (set to 1), '아이디' (ID), and '비밀번호' (Password). At the bottom right are '적용' (Apply) and '닫기' (Close) buttons.

#### 4.8.1. 공인 인증서

[인증서 설정] 창의 [공인 인증서]에서는 프로젝트 별 인증서를 생성하거나 갱신할 수 있으며 기존의 인증서 파일을 가져와서 사용할 수 있습니다.

- **인증서 생성:** 인증서를 새로 생성합니다. 인증서 암호를 입력하거나 닉네임을 추가하거나 암호를 설정할 수 있습니다. 정상적으로 생성이 완료되면 [인증서 이름] 입력 필드에 생성된 인증서의 이름이 표시됩니다.
- **인증서 보기:** 현재 적용중인 공인 인증서의 정보를 확인할 수 있습니다.
- **인증서 저장:** 현재 적용중인 공인 인증서를 ".cer", ".crt" 파일 형식으로 저장할 수 있습니다.
- **인증서 갱신:** 현재 적용중인 공인 인증서의 만료 날짜를 갱신할 수 있습니다.
- **인증서 가져오기:** ".pfx", ".p12" 파일 형식의 공인 인증서를 가져올 수 있습니다.
- **인증서 내보내기:** 현재 적용중인 공인 인증서를 ".pfx", ".p12" 파일 형식으로 저장할 수 있습니다.

#### 4.8.2. HTTPS 클라이언트 인증서

[인증서 설정] 창의 [HTTPS 클라이언트 인증서]에서는 HTTPS 클라이언트 인증서의 유효 기간 및 만료 알림을 설정할 수 있으며, 일반 이름 생성 방식을 선택할 수 있습니다.

- **클라이언트 인증서 유효 기간:** 클라이언트 인증서 생성 시 유효 기간(최대 3년)을 설정할 수 있습니다.
- **인증서 만료 알림(일):** 현재 날짜로부터 남은 유효 기간이 만료 알림일 보다 적게 남아있을 경우 경고 표시를 나타낼 수 있습니다.
- **일반 이름(Common Name):** 클라이언트 인증서를 만들 때 이름 방식 (장비 IP 주소, 장비 호스트 이름)을 선택할 수 있습니다.

#### 참고

공인 인증서, 클라이언트 인증서 및 클라이언트 키를 가져올 수 있으며, 상세 추가 설정을 미리 지정할 수 있습니다.

#### 4.8.3. 802.1x 인증서 설정

[인증서 설정] 창의 [802.1X 인증서 설정]에서는 공인 인증서, 클라이언트 인증서 및 클라이언트 키를 가져올 수 있으며, 추가로 상세 설정을 할 수 있습니다.

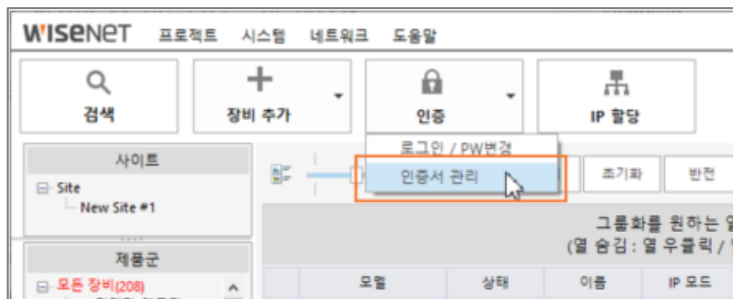
- 디바이스 매니저에서 발행한 공인 인증서, 클라이언트 인증서를 사용할 수

있습니다. (이 경우 공인 인증서 설정이 필요합니다.)

- 디바이스 매니저에서 발행하지 않은 공인 인증서 또는 클라이언트 인증서를 가져와서 사용할 수 있습니다.
- 클라이언트 사설 키를 가져와서 사용할 수 있습니다.
- EAP 타입을 EAP-TLS, LEAP, PEAPv0/MSCHAPv2 중에서 하나로 설정할 수 있습니다.
- EAPOL Version(1 또는 2)을 설정할 수 있습니다.
- 인증서의 ID와 비밀번호를 입력할 수 있습니다.

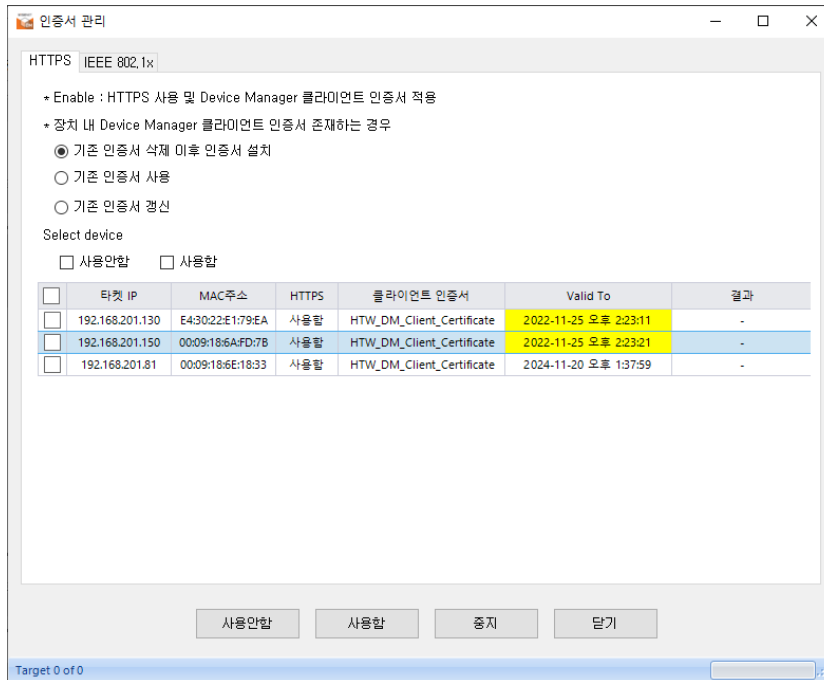
## 4.9. 인증서 관리

[인증서 관리] 창을 열려면 [인증]>[인증서 관리]를 선택합니다.



장비의 HTTPS와 802.1x 인증서 사용 여부를 선택하고 인증서를 설치할 수 있으며, 유효기간 관리 기능을 지원합니다.

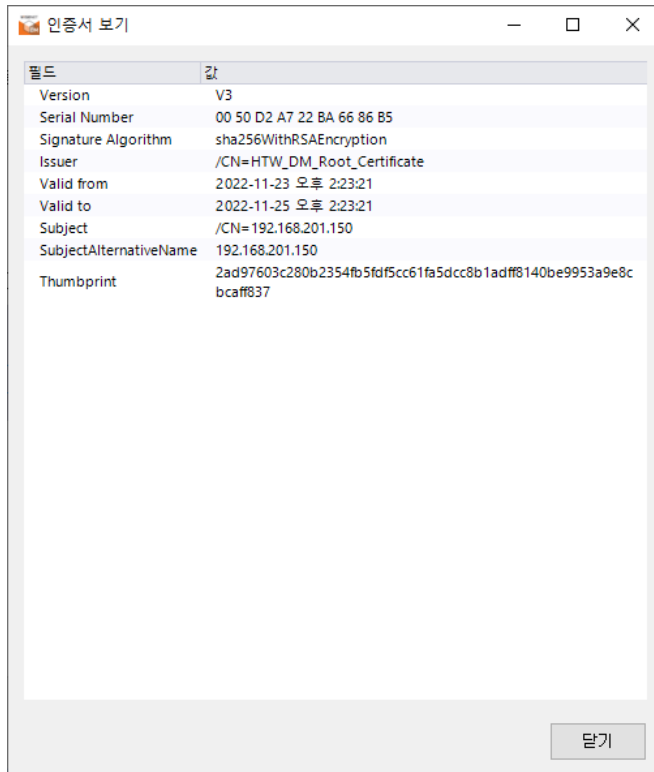
CA에 SUNAPI(HTTP(s) 공통 프로토콜)을 활용하여 클라이언트 인증서를 관리합니다.



#### 4.9.1. HTTPS 설정

[인증서 관리] 창의 [HTTPS] 탭에서는 HTTPS를 기반으로 디바이스 매니저의 클라이언트 인증서를 적용하는 방식을 설정할 수 있습니다.

- 장치 내 Device Manager 클라이언트 인증서 존재하는 경우
  - **기존 인증서 삭제 이후 인증서 설치:** 기존의 디바이스 매니저 클라이언트 인증서를 삭제하고, 새로 발급하여 설치합니다.
  - **기존 인증서 사용:** 기존의 디바이스 매니저 클라이언트 인증서를 그대로 사용합니다.
  - **기존 인증서 갱신:** 기존의 디바이스 매니저 클라이언트 인증서 만료 기간을 갱신하여 사용합니다.
- **장비 선택 필터:** 체크된 항목에 따라 목록에 있는 장비들을 일괄로 선택합니다. 개별 장비별로 설정이 필요할 경우 아래 좌측 체크박스를 선택합니다. 목록에서 클라이언트 인증서 셀을 더블 클릭하거나 마우스 오른쪽을 클릭한 후 [클라이언트 인증서 보기] 클릭하면 아래와 같이 인증서 정보를 확인할 수 있습니다.



[인증서 관리] 창의 [HTTPS] 탭의 각 버튼은 아래와 같이 동작합니다.

**사용 안함:** 선택된 장비들의 HTTPS 사용 안함으로 설정

**사용함:** 선택된 장비들의 HTTPS 사용함으로 설정 및 클라이언트 인증서 적용

**중지:** 현재 진행중인 작업 모두 중지

**닫기:** 인증서 관리 창 닫기

#### 참고

반드시 [인증서 설정]에서 공인 인증서 설정이 되어 있어야 HTTPS 인증서 관리 기능을 사용할 수 있습니다.

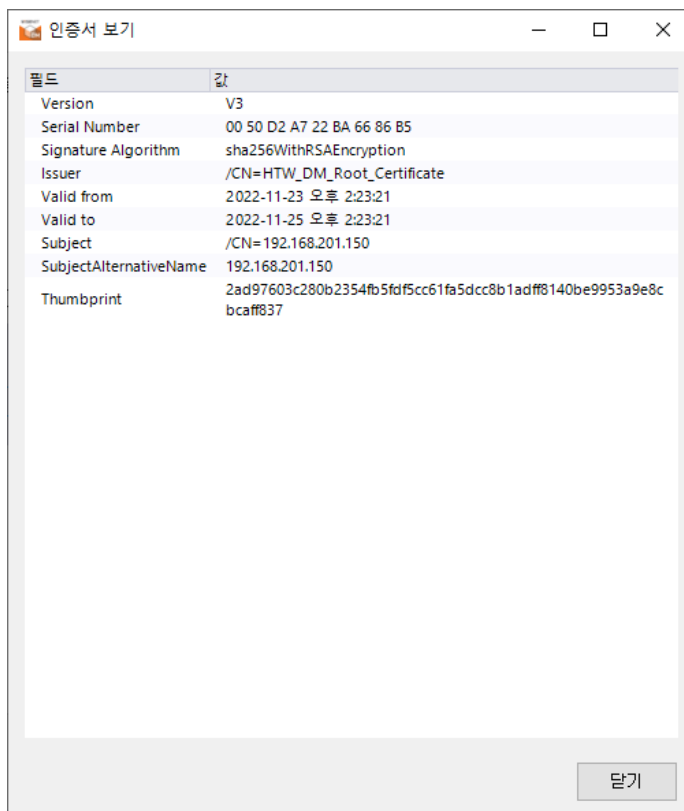
장비에 따라 인증서 정보를 확인할 수 없는 경우가 존재합니다.

### 4.9.2. IEEE 802.1x 설정

[인증서 관리] 창의 [IEEE 802.1x] 탭에서는 IEEE 802.1x를 기반으로 [인증서 설정] 창에서 설정한 CA나 클라이언트 인증서를 적용하는 방식을 설정할 수 있습니다.

- 장비 내 Device Manager 클라이언트 인증서 존재하는 경우  
해당 기능은 [인증서 설정] 창의 [802.1x 설정]>[인증서]에서 [Device Manager의 CA, 클라이언트 인증서 사용(CA 인증서 설정 필요)]옵션이 선택된 경우에만 활성화됩니다.

- **기존 인증서 삭제 이후 인증서 설치:** Device Manager 인증서를 삭제하고, 새로 발급 후 설치
- **기존 인증서 사용:** 장비 내 이미 존재하는 Device Manager 인증서 사용
- **장비 선택 필터:** 체크된 항목에 따라 목록에 있는 장비들을 일괄로 선택합니다.  
목록에서 확인하고자 하는 인증서 셀을 더블 클릭하거나 마우스 오른쪽을 클릭한 후 [클라이언트 인증서 보기] 또는 [CA 인증서 보기]를 클릭하면 아래와 같이 인증서 정보를 확인할 수 있습니다.



[인증서 관리] 창의 [IEEE 802.1x] 탭에서 각 버튼은 아래와 같이 동작합니다

**사용 안함:** 선택된 장비들의 802.1x 사용 안함으로 설정

**사용함:** 선택된 장비들의 802.1x 사용함으로 설정 및 인증서 적용

**중지:** 현재 진행중인 작업 모두 중지

**닫기:** 인증서 관리 창 닫기

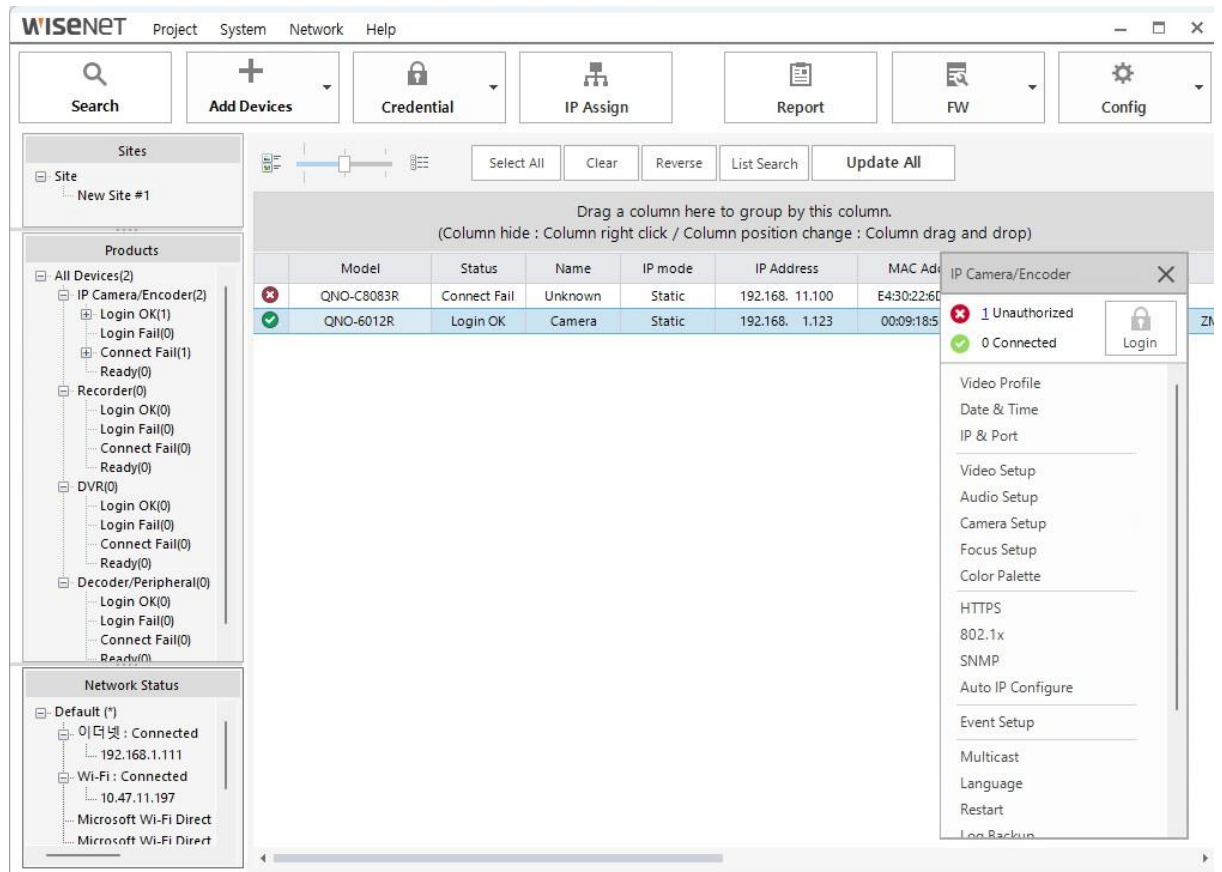
#### 참고

디바이스 매니저 인증서를 사용할 경우, HTTPs와 동시에 동일한 클라이언트 인증서를 사용할 수 없습니다

장비에 따라 인증서 정보를 확인할 수 없는 경우가 존재합니다.

## 4.10. 장비 설정

장비 목록에서 장비를 선택한 후 상단의 (+) 버튼을 클릭하면 해당 장비에서 지원하는 장비 설정 메뉴가 나타납니다. 장비에 따라 상세 메뉴 항목은 다르게 나타날 수 있습니다.



### 4.10.1. 비디오 프로파일

장비에 대한 코덱 및 프레임레이트, 해상도 및 비트레이트 등을 설정할 수 있으며, 프로파일을 추가하거나 삭제, 수정할 수 있습니다. 장비에 따라 선택 가능한 옵션이 달라질 수 있습니다.

### 4.10.2. 날짜 & 시간

장비의 날짜와 시간을 설정할 수 있으며, 동시에 여러 대의 시간 정보 설정을 지원합니다. 선택 가능한 옵션은 다음과 같습니다.

**Time Sync**

**Timezone**

Change timezone ☐ DST enable

(UTC+09:00) 서울

To change the time zone, there may be a time zone that is not supported depending on the device. Be sure to confirm the change on device's web page.

**Time setup**

☒ Manual

Date: 2023년 8월 21일 월요일 Time: 오후 4:50:02

☐ Synchronize with NTP Server

Address1: pool.ntp.org Address2: asia.pool.ntp.org  
 Address3: europe.pool.ntp.org Address4: north-america.pool.ntp.org  
 Address5: Time.nist.gov

☐ Synchronize with PC

Date: 2023년 8월 21일 월요일 Time: 오후 4:50:33

Model	MAC Address	IP Address	Time sync result
QNO-6012R	00:09:18:5F:82:F9	192.168.1.123	

Start Close

Total : 1 , Success : 0 , Fail : 0

- 타임존: 표준 시간대를 기준으로 설정합니다.
- 수동: 장비에 입력될 날짜와 시간 정보를 수동으로 입력하여 설정합니다.
- NTP 서버 동기화: NTP 서버를 통해 날짜와 시간을 동기화합니다.
- PC 와 동기화: 디바이스 매니저가 설치되어 있는 PC 의 시간과 동일하게 설정합니다.

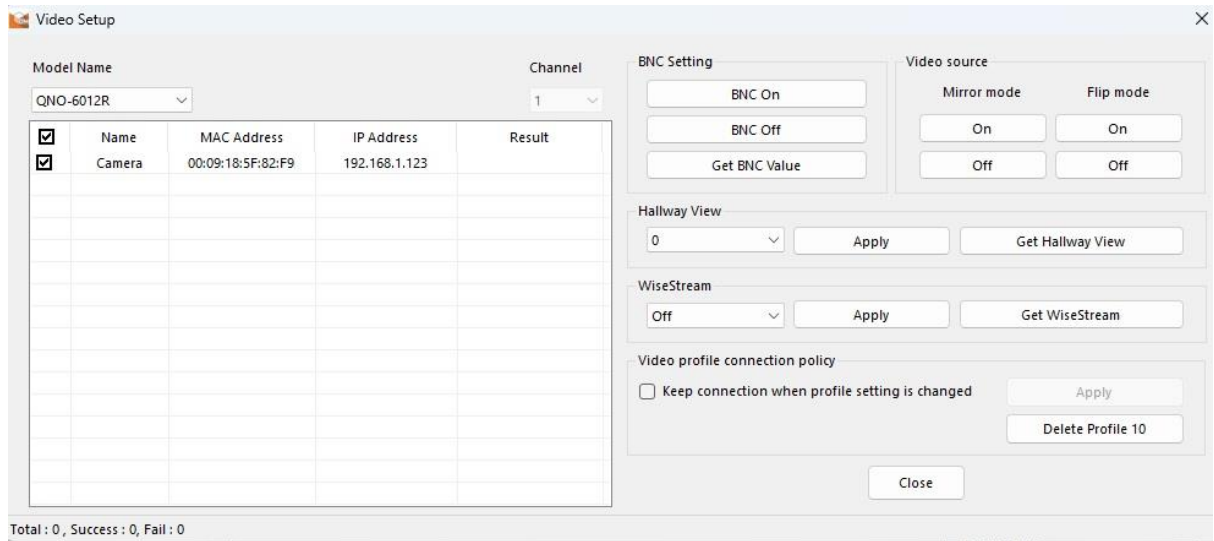
#### 4.10.3. IP & 포트

장비의 IP 및 기타 정보 확인과 Host 이름을 설정할 수 있습니다.  
 Host 이름 설정을 지원하지 않는 장비는 입력 창이 비활성화됩니다.

#### 4.10.4. 비디오 설정

장비의 영상 입력, 출력 및 압축 등을 설정할 수 있습니다. 장비에 따라 활성화 여부 및 선택 가능한 옵션이 달라질 수 있습니다.

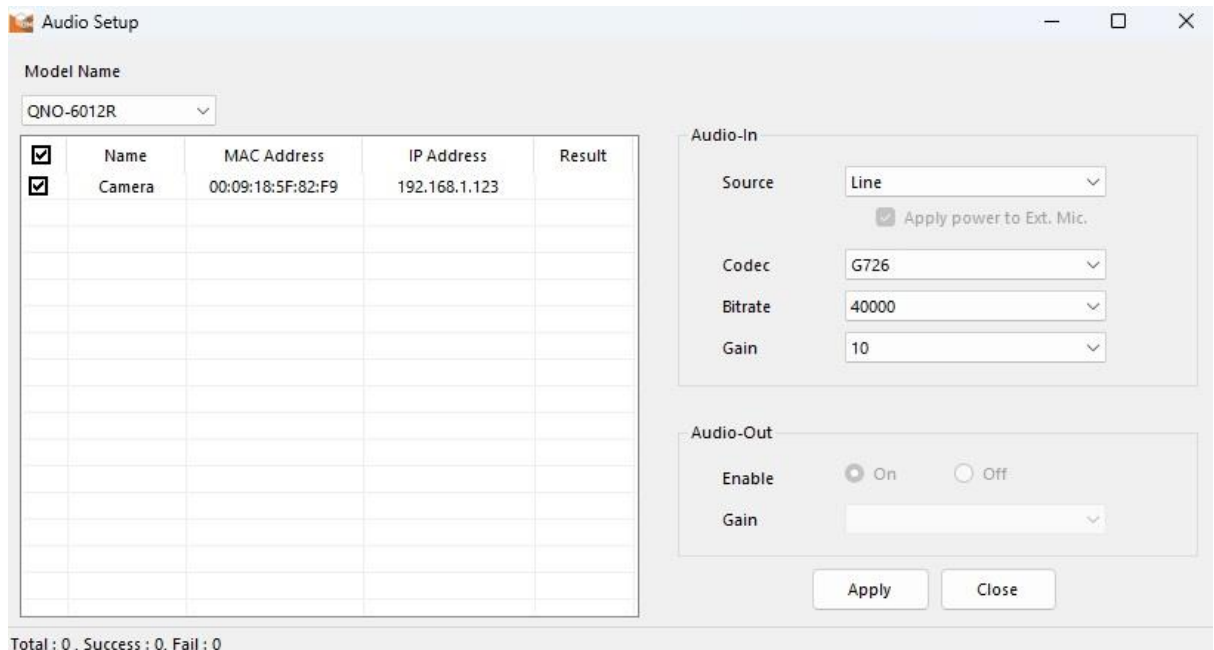




- 비디오 출력 설정: 카메라의 아날로그 비디오(BNC) 출력 여부를 설정합니다.
- 비디오 입력: 영상을 상하/좌우로 반전시키는 기능입니다.
- 복도뷰: 통로에 적합한 비율로 영상을 회전하여 감시 영역을 조정하는 기능입니다.
- 와이즈스트림: 영상의 압축 정도를 선택할 수 있습니다.

#### 4.10.5. 오디오 설정

장비의 오디오 입/출력 설정을 할 수 있습니다. 장비에 따라 활성화 여부가 달라질 수 있습니다.



- 오디오 입력: 오디오 입력 방식을 설정합니다. Internal MIC, External MIC, Line 방식을 선택할 수 있습니다.

- #### 4.10.6. 카메라 설정

[illegible]

- 26

- 노출보정: 장비의 설치 환경에 따라 노출 정도를 변경할 수 있습니다. 밝기, 최소/최대 셔터 속도, 플리커 방지, SSNR 레벨, 조리개 초점 거리 등을 설정할 수 있습니다.
- 주야간모드: 장비의 설치 환경에 맞게 영상을 컬러나 흑백으로 변경할 수 있습니다. 각 모드 및 측정 시간, 전환 주기, 알람 입력 등을 설정할 수 있습니다.
- 스페셜: 윤곽조정, 감마, 컬러레벨, 안개보정, DIS 등을 설정할 수 있습니다.
- OSD: 제목 또는 날짜/시간을 영상에 표시할 수 있으며, 표시할 위치를 설정할 수 있습니다.
- IR: IR LED의 모드 선택 및 레벨을 설정할 수 있습니다.

#### 4.10.7. 포커스 설정

장비의 포커스를 설정할 수 있습니다. 장비에 따라 활성화 여부가 달라질 수 있습니다.

- 포커스 초기화: 포커스를 초기화합니다.
- 심플 포커스: 포커스를 자동으로 조정합니다.

#### 4.10.8. 칼라 팔레트

열화상 카메라의 영상 색상을 변경할 수 있습니다. 열화상 카메라에서만 활성화되는 기능입니다.

#### 4.10.9. SNMP

장비의 SNMP 프로토콜을 설정할 수 있습니다. 시스템이나 네트워크 관리자가 원격으로 장비를 모니터링하거나 설정을 변경하는 등의 관리를 할 수 있습니다. SNMP v1, v2, v3 사용 여부를 설정할 수 있습니다.

SNMP Setup

Model Name: QNO-6012R

Name	MAC Address	IP Address	Result
Camera	00:09:18:5F:82:F9	192.168.1.123	

SNMP v1, v2c

☐ Enable SNMP v1

☐ Enable SNMP v2c

Read community:

Write community:

☐ Enable SNMP Trap

Community:

IP Address:

☐ Authentication failure

☐ Network connection

SNMP v3

☐ Enable SNMP v3

Password:

Apply Close

Total : 0 , Success : 0 , Fail : 0

- #### 4.10.10. IP 자동 설정

[illegible]

- 28

운영체제에서는 Safari 웹 브라우저의 Bonjour 북마크에서 연결된 장비가 표시됩니다.

#### 4.10.11. 이벤트 설정

장비의 이벤트 감지 관련 기능을 설정할 수 있습니다. 설정 시 전체 화면 기준으로 설정됩니다.

The 'Event Setup' window is divided into several sections for configuring detection events. On the left, there's a table for 'Model Name' (QNO-6012R) and 'Channel' (1), with columns for MAC Address, IP Address, and Result. The main area contains settings for Motion Detection, Tampering Detection, Defocus Detection, AI (Object Detection and Best Shot), and Water Remove. Each section has 'ON' and 'OFF' buttons and a 'Sensitivity' dropdown. The AI section includes checkboxes for Person, Vehicle, Face, and License Plate. The Water Remove section includes checkboxes for Wiper, Heater, and Vibration. A 'Close' button is at the bottom right.

- 움직임 감지: 움직임이 감지될 경우 이벤트가 발생하도록 설정할 수 있으며, 민감도를 설정할 수 있습니다. 민감도가 높을수록 배경과 물체 구분이 불명확한 환경에서도 이벤트를 보다 잘 감지하게 됩니다.
- 탬퍼링 감지: 화면이 가려지거나 위치가 변경될 경우 이벤트가 발생하도록 설정할 수 있습니다.
- 디포커스 감지: 렌즈의 포커스가 흐려지는 것이 감지될 경우 이벤트가 발생하도록 설정할 수 있습니다.
- AI: 사용자가 설정한 객체를 감지하면 객체 감지 이벤트가 발생하도록 설정할 수 있습니다. 객체 유형(사람/차량/얼굴/번호판) 및 베스트샷 기능 사용 여부를 선택할 수 있습니다.
- PTZ Water Remove: PTZ 카메라의 Wiper 기능 동작 여부를 설정할 수 있습니다.

#### 4.10.12. 멀티캐스트

장비의 멀티캐스트를 설정하는 기능입니다. 사용여부 및 IP 주소, 포트를 설정할 수 있습니다.

#### 4.10.13. 언어

장비의 Web Viewer 언어를 설정하는 기능입니다.

#### 4.10.14. 재시작

장비의 파워 모드 및 공장 초기화, 재시작을 실시 여부를 선택할 수 있습니다.

Restart

☒

Name

☒

Camera

IP Address

192.168.1.123

Result

Check PowerMode

PowerMode

☒ POE

☐ POE+

Apply

Factory Reset

Factory Reset Except Network and Open Platform

Factory Reset All

Device Restart

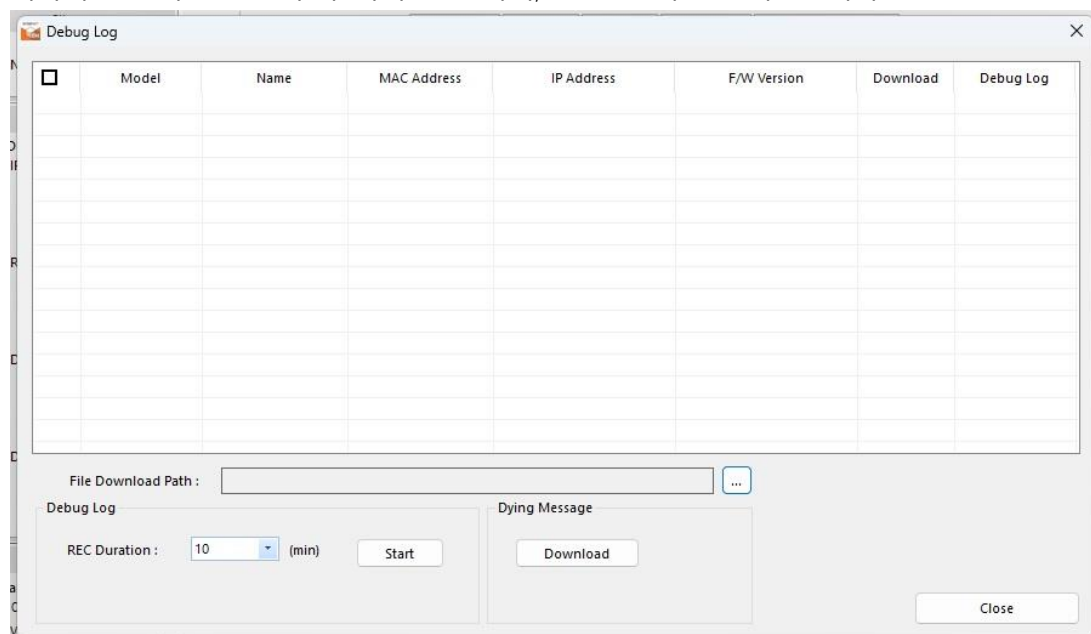
Close

#### 4.10.15. 로그

각 장비의 시스템, 이벤트 및 접속 로그를 조회 가능합니다.

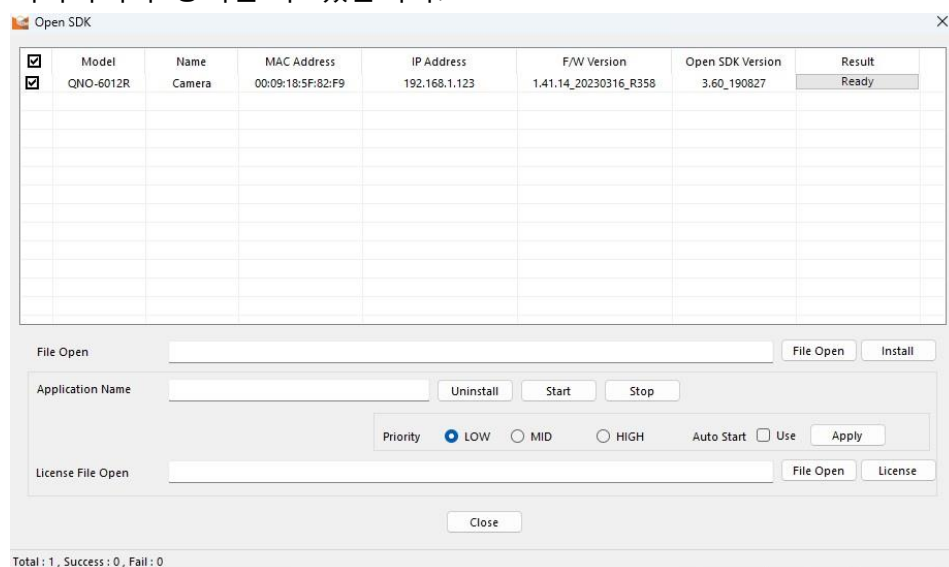
#### 4.10.16. 디버그 로그

특정 동작을 하는 선택된 장비의 디버그 로그를 수집할 수 있습니다. 해당 로그는 csv 파일 형태로 다운로드 가능하며, 다운로드 경로를 선택할 수 있도록 지원합니다. 녹화 지속시간은 최소 10 분부터 최대 60 분까지, 10 분 간격으로 지원됩니다.



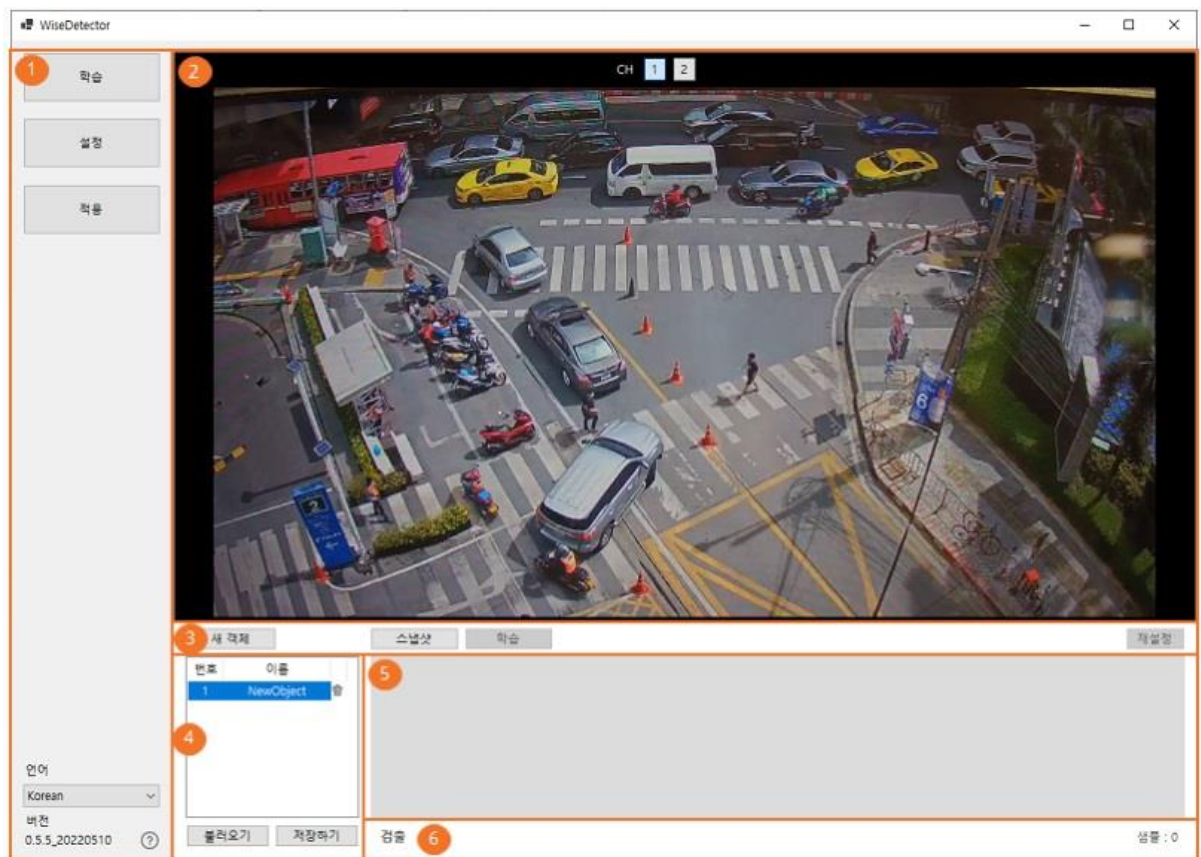
#### 4.10.17. 오픈 플랫폼

장비에 오픈 플랫폼 어플리케이션을 설치, 제거할 수 있으며, 설치된 어플리케이션을 시작하거나 중지할 수 있습니다.



#### 4.10.18. 와이즈디텍터

와이즈디텍터는 사용자가 원하는 객체를 선택하고 학습시킨 후 카메라가 해당 객체를 감지할 수 있도록 도와주는 기능입니다.



- ① 메뉴: 프로그램 관련 기능 및 버전 확인
- ② 영상 보기: 연결된 카메라 영상 표시
- ③ 학습 기능 버튼: 학습 관련 기능 제공
- ④ 객체 관리: 객체 목록 표시 및 관리 기능 제공
- ⑤ 학습 이미지: 학습 샘플 이미지 표시
- ⑥ 개수 표시: 샘플 개수 및 검출된 오브젝트 개수 표시



## 5. 결론

디바이스 매니저는 다양한 장비가 설치된 현장에서 사용자가 개별 장비마다 설정 작업을 실시할 필요 없이 동시에 여러 대를 효율적으로 관리하고 모니터링할 수 있는 직관적인 프로그램입니다. 각 장비별로 사용 목적에 따라 그룹으로 지정하고, 그룹 단위로 시스템을 관리할 수 있어 사용자의 편의성이 향상됩니다.

한화비전은 매년 신규 출시되는 라인업에 대하여 호환 및 설정 작업이 원활하게 진행될 수 있도록 디바이스 매니저 역시 지속적으로 버전을 업데이트하고 있으며, 향후에도 다수의 장비를 원활하게 설정 및 관리할 수 있도록 지원할 계획입니다.

Hanwha Vision Co., Ltd.

13488 Hanwha Vision R&D Center,

6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do

TEL 070.7147.8771-8

FAX 031.8018.3715

[www.HanwhaVision.com](http://www.HanwhaVision.com)

Copyright © 2023 Hanwha Vision Co., Ltd. All rights reserved.

