

WISENET

한화테크윈

# 제품 상호인증 가이드

2021. 12.

Copyright © 2021 Hanwha Techwin. All rights reserved

# 목차

---

- 상호인증이란
- 카메라와 저장장치간의 상호인증
- 카메라와 SSM Appliance 간의 상호인증
- 저장장치와 SSM Appliance 간의 상호인증

## 상호 인증이란?

---

상호 인증은 양방향 인증으로 실제 암호화 통신이 발생하기 이전에 서버와 클라이언트가 서로를 인증하는 보안 프로세스이다. 이를 위해서는 네트워크 환경에서 서버와 클라이언트 모두 자신의 신원을 증명하기 위한 기기 인증서와 인증 기능을 제공할 수 있어야 한다.

한화테크윈의 최신 기기들은 기기 인증서를 탑재하고 상호 인증 기능을 제공하여 유효하지 않은 서버나 클라이언트의 접속을 제한하거나 확인할 수 있는 기능을 제공하고 있다.

### ※ 지원 모델 확인

기기인증서를 탑재하고 있는 모델 확인은 당사 공식 홈페이지 제품 사양의 보안 항목에서 확인 할 수 있다.

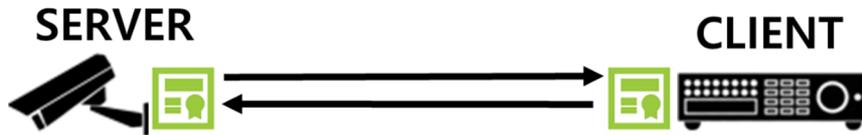
- <https://www.hanwha-security.com> > 대상제품 > 제품사양 > 네트워크 > 보안 > 기기인증서(Hanwha Techwin Root CA)

서버 인증 지원은 NVR(Intel 기반)과 SSM Appliance<sup>\*SSM v2.10.7이상</sup> 제품부터 지원하고 있으며, 클라이언트 인증 지원은 WN7 X시리즈 모델부터 지원하고 있다.

# 카메라와 저장장치 간의 상호인증

## 1. 대상 장치 연결 및 설정 방법

기기인증서가 설치되어 있는 카메라와 저장장치를 연결한다.



### ■ 카메라 설정

1) 카메라는 HTTPS 모드 및 상호인증 모드를 아래와 같이 설정한다.

- “HTTPS” 체크
- 인증서를 HTW\_default 로 선택
- “상호 인증된 연결만 허용” 모드 설정

The screenshot shows the 'HTTPS' configuration page. Under '보안 접속 방식' (Security Connection Method), the 'HTTPS (보안 접속 사용함)' option is checked and highlighted with a red box. The '인증서' (Certificate) dropdown menu is set to 'HTW\_default'. Under '상호 인증' (Mutual Authentication), the '상호 인증된 연결만 허용' (Allow only mutually authenticated connections) radio button is selected and highlighted with a red box. Other options like '모든 연결 허용' and '상호 인증된 연결만 허용(Device ID 검증 포함)' are unselected.

- 상호 인증 옵션(서버: 카메라 / 클라이언트: 저장장치, SSM)

#### ① 모든 연결 허용

서버에서 클라이언트로부터 전달 받은 인증서의 인증 성공 여부와 상관없이 클라이언트와의 암호화 통신을 허용한다. 단, 인증의 성공 유무는 서버에 접속한 클라이언트의 IP기반으로 결과 확인이 가능하다.

#### ② 상호 인증된 연결만 허용

서버에서 클라이언트로부터 전달 받은 인증서의 인증 성공 여부에 따라 서버에 접속할 수 있는 클라이언트 허용 여부를 결정한다. 인증 실패 시 서버와 클라이언트 간의 암호화 통신은 종료된다. 인증은 클라이언트의 인증서가 한화에서 발행한 인증서인지와 유효한 기간 내의 인증서인지를 확인하는 것이다.

#### ③ 상호 인증된 연결만 허용(Device ID 검증 포함)

서버에서 클라이언트로부터 전달받은 인증서의 인증 성공 여부에 따라 서버에 접속할 수 있는 클라이언트 허용 여부를 결정한다. 인증 실패 시 서버와 클라이언트 간의 암호화 통신은 종료된다. 인증은 클라이언트의 인증서가 한화에서 발행한 인증서인지와 유효한 기간 내의 인증서인지, 또한 클라이언트의 MAC 주소와 일치하는지를 확인하는 것이다.

# 카메라와 저장장치 간의 상호인증

※ HTTP 모드 해제 후 상호 인증 ②, ③ 옵션을 선택할 시, 웹 브라우저 접속은 불가능 하게 되고, 카메라 공장초기화 후 접속이 가능하다.



## ■ 저장장치 설정

1) 저장장치에서 카메라 등록 시 아래와 같이 설정한다.

※ 자동이 아닌 수동 등록 필요

- 프로토콜: Wisenet
- HTTP : 80
- 스트리밍 방식: HTTP

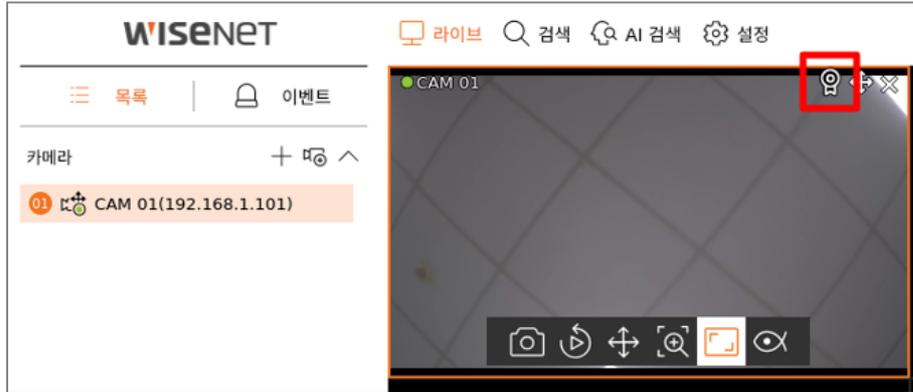
수동 등록	
채널	Ch 1
프로토콜	<input checked="" type="radio"/> Wisenet <input type="radio"/> ONVIF <input type="radio"/> RTSP
모델	Wisenet Camera
주소 형식	IPv4
IP 주소	192 . 168 . 1 . 101
포트	4520 (최대 65535)
HTTP	80 (최대 65535)
ID	admin
비밀번호	●●●●●●●●
상세 설정	^
스트리밍 방식	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> HTTP <input type="radio"/> Multicast

# 카메라와 저장장치 간의 상호인증

## 2. 대상 장치 인증 결과 확인

### ■ 카메라 인증 결과

저장장치 세트 라이브 화면에서 카메라 인증 결과를 다음과 같이 확인할 수 있다.



### ■ 저장장치 인증 결과

저장장치에 대한 인증 결과는 카메라 웹 브라우저에서 카메라 접속 클라이언트 IP 주소 기반으로 결과 확인 가능

- 상호 인증된 연결만 허용 모드로 설정되었을 경우에는 기기인증서가 탑재된 클라이언트만 암호화 통신이 가능하므로 저장장치 인증 결과는 웹 브라우저를 통해서는 확인이 불가능하며, 카메라와 저장장치간의 암호화 통신이 종료되지 않은 것으로 성공 여부를 판단할 수 있다. 다만, 편의를 위해 임시로 웹 브라우저를 통해 인증 결과를 확인하고 싶은 경우 카메라에서 HTTP 모드를 추가로 설정하면 다음과 같이 웹 브라우저 화면에서 인증 결과를 확인 할 수 있다.

※ HTTP 모드를 통한 웹 브라우저 접속의 경우 암호화 통신이 아니므로 보안에 주의하여야 한다.



자물쇠 표시 없음(-): 인증서 없음(HTTP mode)

빨간색 자물쇠(🔒): 기기 인증을 지원하지 않는 인증서(인증 실패)

초록색 자물쇠(🔒): 기기 인증을 지원하는 인증서(인증 성공)

## 카메라와 저장장치 간의 상호인증

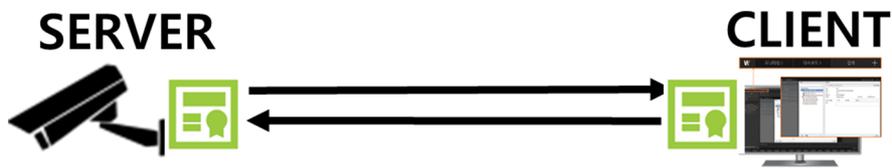
---

- 기기 인증을 지원하는 인증서가 탑재된 저장장치 접속(192.168.38.224)의 경우, 초록색 자물쇠를 통해 상호 인증의 성공 확인
- 기기 인증을 지원하지 않는 인증서가 탑재된 저장장치 접속(192.168.38.207)의 경우, 빨간색 자물쇠를 통해 상호 인증의 실패 확인
- 인증서가 탑재되어 있지 않은 웹 브라우저 접속(192.068.38.163)의 경우 자물쇠 표시가 없음

# 카메라와 SSM Appliance 간의 상호인증

## 1. 대상 장치 연결 및 설정 방법

기기인증서가 설치되어 있는 카메라와 SSM Appliance를 연결한다.



### ■ 카메라 설정

1) 카메라는 HTTPS 모드 및 상호인증 모드를 아래와 같이 설정한다.

- “HTTPS” 체크
- 인증서를 HTW\_default 로 선택
- “상호 인증된 연결만 허용” 모드 설정

The screenshot shows the 'HTTPS' configuration page. Under '보안 접속 방식' (Security Connection Method), the 'HTTPS (보안 접속 사용함)' option is selected and highlighted with a red box. The '인증서' (Certificate) dropdown menu is set to 'HTW\_default'. Under '상호 인증' (Mutual Authentication), the '상호 인증된 연결만 허용' (Allow only mutually authenticated connections) radio button is selected and highlighted with a red box. Other options like 'HTTP (보안 접속 사용 안 함)', '호스트 이름 변경', '모든 연결 허용', and '상호 인증된 연결만 허용(Device ID 검증 포함)' are also visible.

※ 상호 인증 옵션 설명은 3page 참고

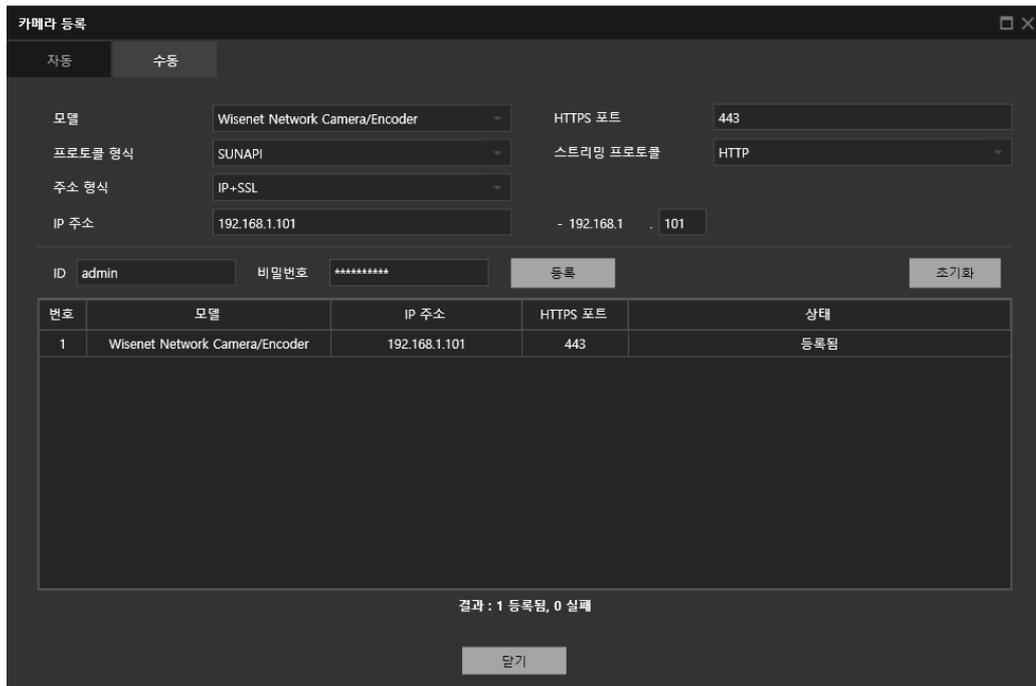
### ■ SSM Appliance 설정

1) SSM Appliance에서 카메라 수동 등록 시 아래와 같이 설정한다.

※ 카메라 인증 시 등록에 사용한 상호 인증 옵션이 변경되는 경우 재등록이 필요하며, 변경되지 않은 경우 생략 가능하다.

- 프로토콜 형식: SUNAPI
- 네트워크: IP + SSL
- HTTPS: 443
- 스트리밍 프로토콜 방식: HTTP

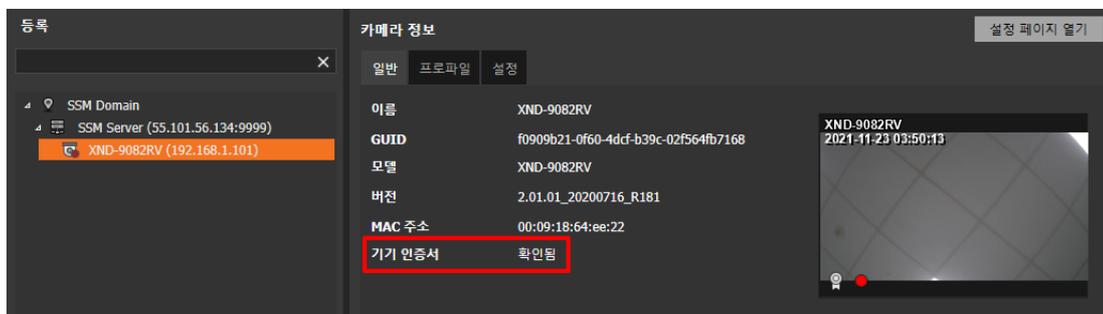
# 카메라와 SSM Appliance간의 상호인증



## 2. 대상 장치 인증 결과 확인

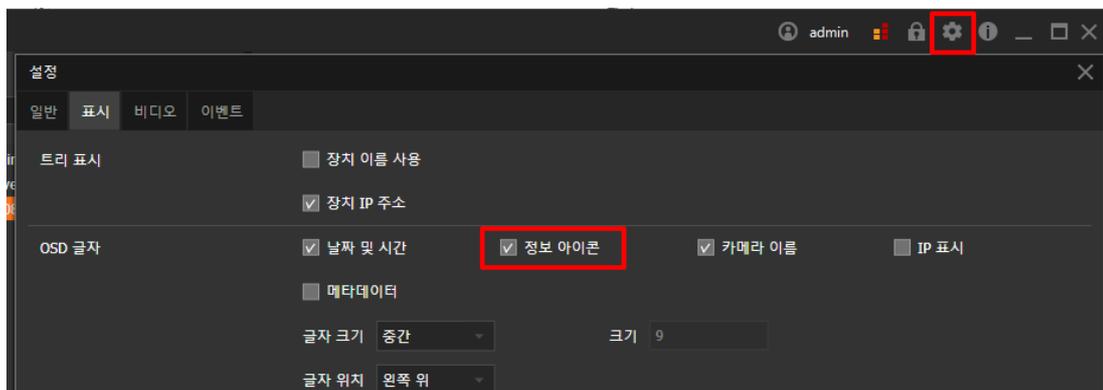
### ■ 카메라 인증 결과

SSM Appliance > 카메라 정보 > 일반 메뉴 화면에서 카메라 인증 결과를 확인한다. 카메라 인증 성공 시 기기인증서 확인됨으로 표시된다.



※ 기기인증서 확인 아이콘은 다음과 같이 설정 시 추가 확인 가능하다.

✓ 설정 > 표시 > OSD 글자 > 정보 아이콘 체크

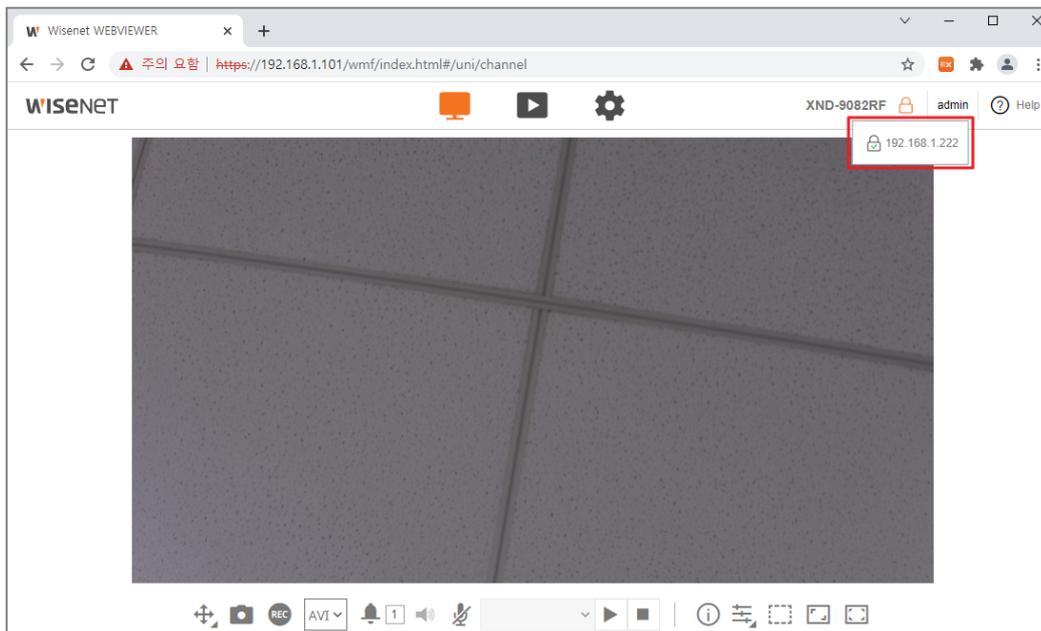


# 카메라와 SSM Appliance간의 상호인증

## ■ SSM Appliance 인증 결과

SSM Appliance에 대한 인증 결과는 카메라 웹 브라우저에서 카메라에 접속한 클라이언트 IP주소 기반으로 결과 확인 가능

- 단, 웹 브라우저를 통한 인증 결과는 카메라에서 HTTP 모드를 추가로 설정하는 경우에만 인증 결과를 확인할 수 있다.
- HTTP 모드를 통한 웹 브라우저 접속의 경우 암호화 통신이 아니므로 보안에 주의하여야 한다.



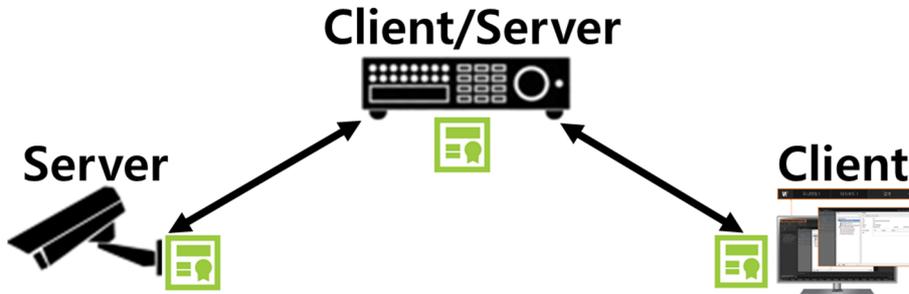
- 자물쇠 표시 없음(-): 인증서 없음(HTTP mode)
- 빨간색 자물쇠(🔒): 기기 인증을 지원하지 않는 인증서(인증 실패)
- 초록색 자물쇠(🔒): 기기 인증을 지원하는 인증서(인증 성공)

- 기기 인증을 지원하는 인증서가 탑재된 SSM Appliance 접속 (192.168.1.222)의 경우, 초록색 자물쇠를 통해 상호 인증의 성공 확인

# 저장장치와 SSM Appliance 간의 상호인증

## 1. 대상 장치 연결 및 설정 방법

기기인증서가 설치되어 있는 카메라, 저장장치 그리고 SSM Appliance를 아래 그림과 같이 연결한다.



### ■ 카메라 설정

1) 카메라는 HTTPS 모드 및 상호인증 모드를 아래와 같이 설정한다.

- “HTTPS” 체크
- 인증서를 HTW\_default 로 선택
- “상호 인증된 연결만 허용” 모드 설정

The screenshot shows the 'HTTPS' configuration window. Under '보안 접속 방식' (Security Connection Method), the 'HTTPS (보안 접속 사용함)' option is checked and highlighted with a red box. The '인증서' (Certificate) dropdown menu is set to 'HTW\_default'. Under '상호 인증' (Mutual Authentication), the '상호 인증된 연결만 허용' (Allow only mutually authenticated connections) radio button is selected and highlighted with a red box. Other options like '모든 연결 허용' and '상호 인증된 연결만 허용(Device ID 검증 포함)' are unselected.

※ 상호 인증 옵션 설명은 3page 참고

# 저장장치와 SSM Appliance 간의 상호인증

## ■ 저장장치 설정

1) 저장장치에서 카메라 등록 시 아래와 같이 설정한다. (수동 등록 필요)

- 프로토콜: Wisenet
- HTTP : 80
- 스트리밍 방식: HTTP

2) 저장장치 보안접속방식은 아래와 같이 설정 한다.

- HTTPS(자체 인증서 사용)
- 상호 인증  
: 상호 인증된 연결만 허용

## ■ SSM Appliance 설정

1) SSM Appliance에서 저장장치 수동 등록 시 아래와 같이 설정한다.

- 프로토콜 형식: SUNAPI
- 네트워크: IP+SSL
- HTTPS : 443
- 스트리밍 프로토콜 방식: HTTP

번호	모델	IP 주소	HTTPS 포트	상태
1	Wisenet Recorder	192.168.1.200	443	등록됨

결과 : 1 등록됨, 0 실패

# 저장장치와 SSM Appliance 간의 상호인증

## 2. 대상 장치 인증 결과 확인

### ■ SSM Appliance 인증 결과

저장장치 세트 화면에서 SSM Appliance 인증 결과 확인한다.

- 인증 결과는 저장장치에 접속한 클라이언트 IP 주소 기반으로 결과 확인이 가능

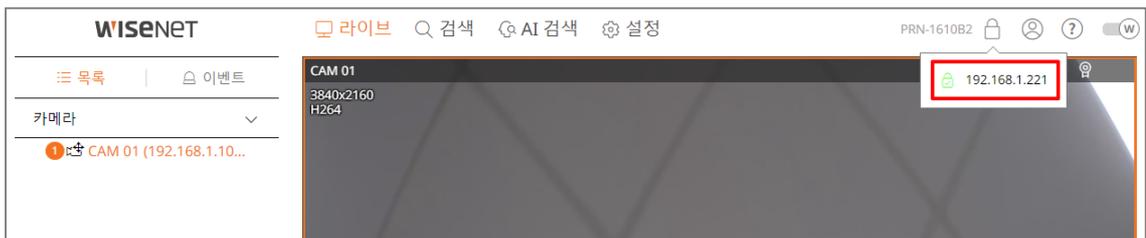


저장장치 세트 화면에서 저장장치에 등록된 카메라 인증 결과도 확인 가능하다.



저장장치 웹 브라우저 화면에서도 SSM Appliance 인증 결과를 확인할 수 있다.

- 편의를 위해 임시로 웹 브라우저를 통해 인증 결과를 확인하고 싶은 경우, 저장장치에서 HTTP 모드를 추가로 설정하면 다음과 같이 웹 브라우저 화면에서 인증 결과를 확인할 수 있다.
- HTTP 모드를 통한 웹 브라우저 접속의 경우 암호화 통신이 아니므로 보안에 주의하여야 한다.



자물쇠 표시 없음(-): HTTPS를 사용한 영상 전송이 아닌 경우(TCP/UDP/Multicast 모드)

빨간색 자물쇠(🔒): 기기 인증을 지원하지 않는 인증서(인증 실패)

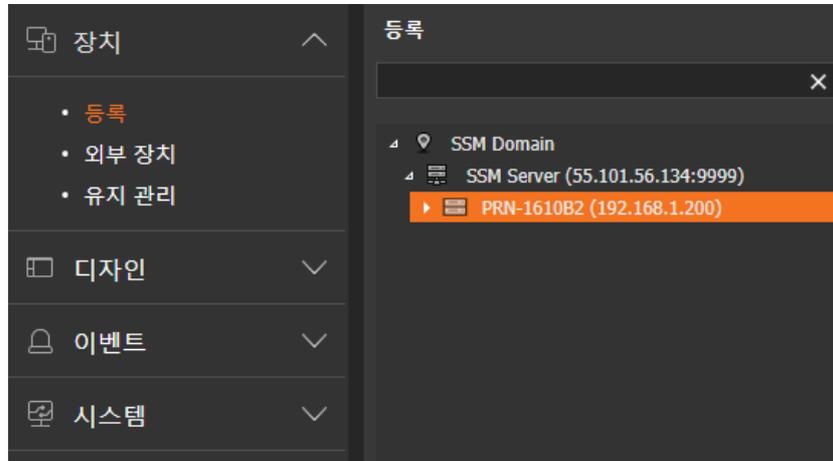
초록색 자물쇠(🔓): 기기 인증을 지원하는 인증서(인증 성공)

- 기기 인증을 지원하는 인증서가 탑재된 SSM Appliance (192.168.1.221)의 경우, 초록색 자물쇠를 통해 상호 인증의 성공 확인
- HTTPS를 사용한 영상 전송을 사용하지 않는 클라이언트 접속의 경우 자물쇠 표시가 없음

# 저장장치와 SSM Appliance 간의 상호인증

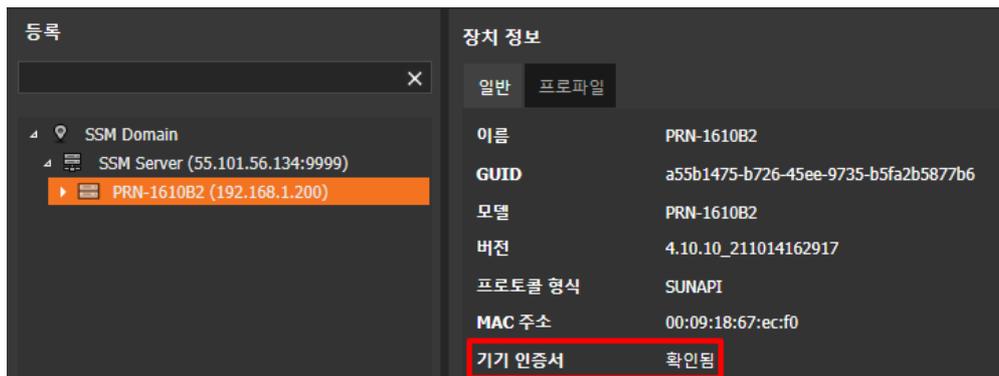
## ■ 저장장치 인증 결과

SSM Appliance 에 저장장치가 정상적으로 등록되었는지 확인한다.



등록되어 있는 저장장치의 장치정보에서 기기인증서를 확인한다.

- 저장장치 인증 성공 시 기기인증서 확인됨으로 표시



# 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>

Copyright © 2021 Hanwha Techwin. All rights reserved

