

User Guide 한화테크윈 사설 루트 CA 인증서 사전 설치 가이드

2020. 02. 19.

Copyright \odot 2020 Hanwha Techwin. All rights reserved



- 1. 루트 CA 인증서 다운로드 및 해쉬값 확인
 - 1) 홈페이지를 통해 별도 배포되는 한화테크윈 사설 루트 CA 인증서 압축 파일(HTW_RootCA_File.zip)을 다운로드 합니다.
 - 다운로드 경로
 - : <u>한화테크윈 홈페이지</u> → 자료센터 → 인증/법규자료 → 인증서 → "사설 루트 CA 인증서 다운로드" 클릭

인증서(10)				^
CMMI Level 3 인증서 CMMI-DEV version 1.3 Mat	urity Level 3	사설 루트 CA 인증서 사실 루트 CA 인증서 파일	ISO/IEC 27001 2013 (ISMS) 인증서 ISO/IEC 27001 2013 (ISMS) 인증서 - 현황S&C 크힌 IT 관리 서비스 제공 표)	(한화테
⑧ 바로보기	🕁 다운로드	바로보기 난 다운로	드 💿 바로보기 한 다운로	<u> </u>
KISA 인증서 한국인터넷진흥원(KISA) 지능	형 CCTV 성능 인증서	TTA 인증서 공공기관용 TTA(한국정보통신기술협회) 보안성 인증서	ISO 14001 인증서 능품질 환경경영시스템 인증서	
⑧ 바로보기	🖸 다운로드	바로보기 ▼ 다운로드	▼ 바로보기 ▼ 다운로드	•

반드시 한화테크윈에서 위 경로로 제공하는 루트 CA 인증서만을 사용하시기 바랍니다.

2) 다운로드 받은 "HTW_RootCA_File.zip" 파일의 압축을 해제합니다.

압축을 해제 하면 아래와 같이 2개의 인증서 파일과 1개의 txt 파일이 존재합니다.

- HTW_rootca.crt
- HTW_rootca_2.crt
- Read_me.txt

여기서 HTW_rootca.crt와 HTW_rootca_2.crt 파일을 가지고 인증서를 설치합니다. <u>두개의 인증서 설치 방법은 동일합니다.</u>

2. 사설 루트 CA 인증서 사전 설치 방법

1) 먼저 "HTW_rootca.crt" 파일을 더블 클릭한 후, "인증서 설치(I)"를 클릭합니다.

🔐 인증서 🛛 🗙				
일반	자세히 인증 경로			
[[[[[[] [] [] [] [] [] [] [이 인증서 정보 	-		
-	발급 대상: Hanwha Techwin Private Root CA			
	발급자: Hanwha Techwin Private Root CA			
	유효기간(시작) 2018-03-25 부터 2038-03-21			
	인증서 설치() 발급자 설명(<u>S</u>)			
	확인			

- 2) 인증서 가져오기 마법사를 시작하기 위해 "다음(N)"을 클릭합니다.
- 3) "모든 인증서를 다음 저장소에 저장(P)"을 선택하고 "찾아보기(R)"를 클릭합니다.

← 😺 인증서 가져오기 마법사	
인동서 저장소 인증서 저장소는 인증서를 저장하는 시스템 영역입니다.	
Windows가 자동으로 인증서 저장소를 선택하거나 사용자가 인증. 습니다.	서 위치를 지정할 수 있
 ○ 인증서 종류를 기준으로 인증서 저장소를 자동으로 선택(U) ● 모든 인증서를 다음 저장소에 저장(P) 	
인증서 저장소:	찾아보기(R)
	다음(N) 취소

4) 인증서 저장소 선택 창에서 "신뢰할 수 있는 루트 인증 기관"을 선택하고 확인 버튼을 클릭합니다.

인증서 저장소 선택	\times
사용하려는 인증서 저장소를 선택하십시오(C).	
····· <mark>·······························</mark>	~
	¥
□ 실제 저장소 표시(S)	
확인 취소	

5) 인증서 저장소에 "신뢰할 수 있는 루트 인증 기관"이 표시되어 있는지 확인하고 "다음(N)"을 클릭합니다.

÷	🔊 인증서 가져오기 마법사	×
	인증서 저장소 인증서 저장소는 인증서를 저장하는 시스템 영역입니다.	
	Windows가 자동으로 인증서 저장소를 선택하거나 사용자가 인증서 위치를 지정할 수 있 습니다.	
	○ 인증서 종류를 기준으로 인증서 저장소를 자동으로 선택(U)	
	◉ 모든 인증서를 다음 저장소에 저장(P)	
	인증서 저장소: 신뢰할 수 있는 루트 인증 기관 찾아보기(R)	
	다음(N) 취소	

6) 사용자가 선택한 인증서 저장소"에 "신뢰할 수 있는 루트 인증 기관", 내용에 "인증서"가 표시되어 있는지 확인하고 마침 버튼을 클릭합니다.

← 🐙	인증서 가져오기 마법사				×
	인증서 가져오기 마법사 완료				
	[마침]을 클릭하면 인증서를 가져옵니다.				
	다음 설정을 지정했습니다.				
	사용자가 선택한 인증서 저장소 신뢰할 수 있는 루트 인증 기관 콘텐츠 인증서				
		_			
			ŀ침(F)	취석	2

- 7) 보안 경고 창에서 "지문(sha1)"이 다음의 내용임을 확인합니다. 해쉬값이 일치할 경우 "예(Y)" 버튼을 클릭합니다.
 - HTW_rootca.crt → 지문(sha1): CD28ACD4 F05793EF 43AA524D F30404FD 0B7F3A27
 - HTW_rootca_2.crt → 지문(sha1): FA47E60B 94968EA1 91BCA8EC 9514AECD B2832545



※ 위 보안 경고창이 나타나지 않고 "가져오기를 완료했습니다." 메시지 창이 바로 나타날 수 있습니다. 확인 버튼을 클릭하세요.

- 8) "가져오기를 완료했습니다"라는 메시지가 나타나면 확인 버튼을 클릭합니다.
- 9) 인증서 창에서 확인 버튼을 클릭해 창을 닫은 후, 웹브라우저를 다시 시작합니다.

🖬 인증서	×			
일반 자세히 인증 경로				
	_			
민중서 정보				
인증서의 용도:				
• 모든 발급 정책				
•모든 응용 프로그램 정책				
	_			
발급 대상: Hanwha Techwin Private Root CA				
발급자: Hanwha Techwin Private Root CA				
유효 기간(시작) 2018-03-25 부터 2038-03-21				
	_			
인증서 설치(I) 발급자 설명(S)				
	_			
확인	<u>1</u>			

인증서 설치 시의 위 해쉬값과 다를 경우, 한화테크윈에서 발행한 루트 CA 인증서가 아니므로 설치를 중단하고, 올바른 경로에서 인증서를 다시 다운로드 하신 후, 진행하시기 바랍니다.

10) 다음은 HTW_rootca_2.crt 파일을 이용하여 1)~9)까지의 절차를 동일하게 진행합니다.

- 3. 로컬 DNS(Hosts 파일)를 이용해 카메라에 안전하게 접속하는 방법 (크롬 브라우저 기준)
 - 1) 브라우저를 실행해 https 모드로 카메라에 접속합니다.
 본 가이드에서 예로 든 카메라의 로컬 접속 IP는 192.168.71.141 이며, 각 사용자의 카메라에 맞는 IP로 접속해주시기 바랍니다.
 - 2) "연결이 비공개로 설정되어 있지 않습니다." 라고 표시되나,
 "192.168.71.141(안전하지 않음)(으)로 이동"을 클릭해 다음 단계로 진행합니다.



3) 브라우저 상단 주소 표시줄 왼쪽의 "주의 요함"을 클릭해, "이 사이트는 보안 연결(HTTPS)이 사용되지 않았습니다." 메시지가 나타나면 하단의 "인증서(유효하지 않음)"을 클릭합니다.

중 개인정보 보호 오류 × +	-		×
← → C ▲ 주의 요함 192.168.71.141	☆	Θ	:
이 사이트는 보안 연결(HTTPS)이 사용되 지 않았습니다. 이 사이트에 입력하는 비밀번호나 신용카드 번호 등 의 정보가 공격자에 의해 도용될 수 있습니다. 자세히 알아보기			Î
인증서: (유효하지 않음)			
연 🐵 쿠키 (0개 사용 중)개 않습니다.			
공격 🂠 ^{사이트 설정} 시지, 신용카드 등)를 도용하려고 시	니도		
중알구 귰급역력· <u>전제약 곧약포전</u> NET::ERR_CERT_COMMON_NAME_INVALID			
방문한 일부 페이지의 URL, 제한된 시스템 정보, 일부 페이지 콘텐츠를 Google에 전송하여 Chro 보안을 강화하는 데 참여해 주세요. <u>개인정보처리방침</u>	me		
세부정보 숨기기 안전한 페이지로 돌아가	7		
이 서버가 192.168.71.141 임을 입증할 수 없으며 서버의 보안 인증서가			
00166CF9282F.hanwha-security.com에서 세공한 것입니다. 서버를 잘못 설정했거나 두 사용자가 연결을 가로채고 있기 때문일 수 있습니다.	불띱		
<u>192.168.71.141(안전하지 않음)(</u> 으)로 이동			•

4) 인증서 창이 나타나면 "자세히" 탭을 선택합니다.

및 인증서 ×				
일	반 자세히 인증 경로			
	민증서 정보			
	인증서의 용도:			
	● 원격 컴퓨터의 신분을 확인합니다.			
	• 전기 8 파키에 사용하여 전관로 응용합니다.			
	발급 대상: 00166CF9282F.hanwha-security.com			
	발급자: Hanwha Techwin Private Root CA			
	유효 기간(시작) 2019-11-05 부터 2029-11-03			
	발급자 설명(S)			
	±101			
	확인			

5) 표시가 전체로 되어 있는지 확인하고 필드 중에서 "주체"를 클릭합니다. 하단 상자에 표시된 CN = 이후의 문자열을 복사(Ctrl + C)합니다. (해당 문자열은 카메라의 고유 MAC 주소가 반영되어 있으므로, 제품마다 상이합니다.)

필드	값
圓 주체	00166CF9282F.hanwha-sec
📺 공개 키	RSA (2048 Bits)
🔄 공용 키 매개 변수	05 00
🗊 기본 제한	주체 종류=End Entity, 경로
🗊 Netscape Cert Type	SSL 서버 인증 (40)
🗊 키 사용	Digital Signature, Non-Rep
🗊 주체 대체 이름	DNS Name=00166CF9282
🗊 확장된 키 사용	서버 인증 (1.3.6.1.5.5.7.3.1
CN = 00166CF9282F.hanw	/ha-security.com
CN = 00166CF9282F.hanw OU = Security Device O = Hanwha Techwin C = KR	/ha-security.com

Copyright © 2020 Hanwha Techwin. All rights reserved.

- 6) 윈도우의 시작 메뉴를 열고, 프로그램 및 파일 검색 텍스트 상자에 다음 문자열을 입력하고 Ctrl + Shift + Enter 키를 누릅니다.
 - notepad C:₩Windows₩system32₩drivers₩etc₩hosts



7) "hosts - 메모장" 창이 열리면 파일 안에 다음과 같은 규칙으로 문자열을 추가합니다.

• [카메라의 사설 IP 주소] [인증서에서 복사한 문자열]

아래 참고 화면은 카메라의 IP 주소가 192.168.71.141이며, 문자열이 00166CF9282F.hanwha-security.com인 경우입니다.

	🥘 hosts - 메모장				- 0	×
	파일(F) 편집(E) 서식(O) 보기(V) 도	응말				^
	# CAD License Set	ting				
	55.101.210.26	stwlic1	stwlic1.stw.net			
	55.101.210.75	stwlic2	stwlic2.stw.net			
	55.200.100.221	stwlic3	stwlic3.stw.net			
	55.200.100.221	stw-super1	stw-super1.stw.net	t		
	55.101.210.38	ssa3srv				
	52.231.156.46	netlic1				
	55.101.200.45	hpm-lic1			# 정밀기계	
	55.101.210.33	hps-lic1			# 파워시스템	
	# HPC					
	55.101.210.151	stwlogin1				
	55.101.210.153	stweod1				
	55.101.210.154	stweod2				
	# Teamforge Settir	ng				
	55.101.210.64	ctf1	ctf1.stw.net			
1				1		
	192.168.71.141	00166CF9282F.han	wha-security.com			
			-	J		~
	<		Windows (CRLF)	Ln 149. Col 1	100%	>

8) "파일(F) → 저장(S)"을 선택하여 저장하고 "끝내기(X)"로 파일을 닫습니다.



Windows의 hosts 파일 변경 탐지 컨트롤 창이 나타나며, 이전 상태로의 복원 여부를 묻는 경우, "아니오"를 선택합니다.

※ HTW_rootca_2.crt 파일의 경우 위 파일 변경 탐지 컨트롤 창이 나오지 않을 올 수 있습니다. 다음 단계로 진행하세요.

- 9) 브라우저의 주소창을 이용해 카메라에 접근하는 경우, 사설 IP가 아닌 로컬 DNS에 등록한 문자열("CN =" 이후의)을 사용합니다.
 - https://00166CF9282F.hanwha-security.com (예)



10) 설정이 완료되면, 브라우저의 주소창의 배경이 안전한 웹사이트를 의미하는 흰색으로 표시됩니다. 또한, 주소창 왼쪽 부분의 자물쇠 표시를 클릭하여 다음과 같이 표시되면 정상 설정되었음을 확인할 수 있습니다. "인증서(유효)"를 클릭하여 장치의 "인증서 정보"를 확인 합니다.



11) "인증 경로" 탭으로 이동해 "Hanwha Techwin Private Root CA" 또는 "Hanwha Techwin Private Root CA 2" 를 선택하면 "인증서 보기(V)"가 가능해지며, 다음과 같이 루트 CA인증서가 신뢰 가능한 인증서로 변경되었음을 확인할 수 있습니다.

및 인증서 X	및 인증서 X
일반 자세진 인증 경로	일반 자세 인증경로
인증 경로(P) 데 Hanwha Techwin Private Root CA 네 나라 100166CF9282F.nanwha-security.com 인증서 보기(V)	인증 경로(P) Hanwha Techwin Private Root CA 2 O0166CFB816D.hanwha-security.com 인증서 보기(M)
인증서 상태(S):	인증서 상태(<u>S</u>):
올바른 인증서입니다.	올바른 인증서입니다.
확인	확인

< 설정 전 >
🙀 인증서 정보
이 CA 루트 인증서를 신뢰할 수 없습니다. 신뢰를 얻으려면, 이 민증서를 신뢰할 수 있는 루트 인증 기관 저장소에 설치하 십시오.
< 설정 후 >
민증서 정보
인용서의 용도: • 모든 발급 정책 • 모든 응용 프로그램 정책

12) 확인 버튼을 클릭해 인증서 창을 닫고, 설정을 마칩니다.

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 \odot 2020 Hanwha Techwin. All rights reserved

