

ezTCP 기술문서

SSL (Secure Socket Layer)

Version 1.3

솔내시스템(주)

<http://www.sollae.co.kr>

목차

1	개요	- 2 -
1.1	SSL (Secure Socket Layer).....	- 2 -
1.2	적용.....	- 2 -
2	설정하기	- 3 -
2.1	설정하기 전에.....	- 3 -
2.2	설정 하기.....	- 3 -
2.2.1	개요.....	- 3 -
2.2.2	ezManager 설정.....	- 4 -
2.2.3	인증서 생성.....	- 4 -
3	사용 예	- 7 -
3.1	개요.....	- 7 -
3.1.1	TCP 접속 형태.....	- 7 -
3.2	TCP 서버 모드.....	- 7 -
3.2.1	ezManager 확인.....	- 7 -
3.2.2	텔넷 접속 확인.....	- 9 -
3.2.3	접속하기.....	- 10 -
3.3	TCP 클라이언트 모드.....	- 12 -
4	변경 이력	- 13 -

1 개요

1.1 SSL (Secure Socket Layer)

SSL은 당초 인터넷 전자 상거래 등의 보안을 위해 넷스케이프(Netscape)사에 의해 개발되었으며 인터넷 표준규격을 개발하고 있는 미국 IAB (Internet Architecture Board)의 조사위원회인 IETF (Internet Engineering Task Force)에 의해 TLS (Transport Layer Security)라는 이름으로 표준화되었습니다. 현재 인터넷 환경에서 보안 유지에 널리 사용되고 있는 프로토콜이며 당사 제품은 이러한 SSL 3.0 / TLS 1.0을 지원하여 인터넷 환경에서 데이터 전송의 보안을 보장합니다.

1.2 적용

SSL은 TCP의 상위 계층에서 동작하므로 UDP를 사용하는 U2S 모드에서는 사용할 수 없습니다. 본 문서는 TCP 서버 / 클라이언트 각 모드에서의 SSL 사용에 대한 응용 문서이며 해당 제품은 CSE-M32, CSE-M73, CSE-H20, CSE-H21, CSE-H25 입니다.

2 설정하기

2.1 설정하기 전에

- “U2S – UDP” 통신모드에서는 사용할 수 없습니다.
- SSL 기능 사용 중에 다음 기능을 사용할 수 없습니다.
SSH 보안통신, 시리얼 포트 설정/상태 전송(RFC2217)
- SSL 기능 사용 중 각 제품별 제약 사항은 다음과 같습니다.
CSE-M32, CSE-H20, CSE-H21 – 시리얼 통신속도 최대 115,200bps / COM2 사용 불가
CSE-M73, CSE-H25 – 시리얼 통신속도 최대 115,200bps, 멀티 모니터링 기능 사용 불가

2.2 설정 하기

2.2.1 개요

“SSL 보안통신” 기능은 TCP 서버 / 클라이언트 각 모드에서 각기 사용 가능합니다. 클라이언트 모드에서는 단순히 “SSL 보안통신” 옵션 활성화 만으로 기능을 사용할 수 있습니다. TCP 서버 모드에서는 “SSL 보안통신” 옵션 활성화 이후 텔넷 접속하여 인증서 생성 후 사용할 수 있습니다.

2.2.2 ezManager 설정

'그림 2-1'과 같이 "옵션" 탭의 [SSL 보안통신] 항목을 설정합니다.

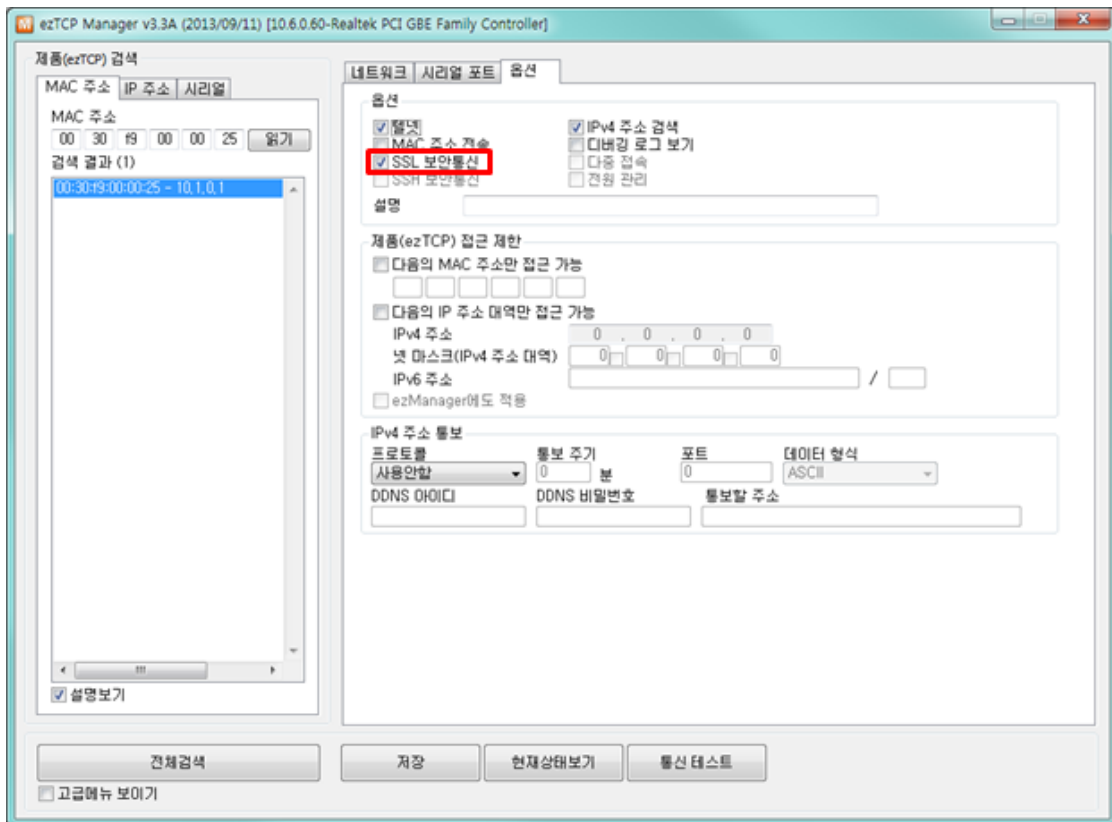


그림 2-1 "SSL 보안통신" 옵션 설정하기

2.2.3 인증서 생성

- 제품(ezTCP)의 텔넷 콘솔에 접속합니다.

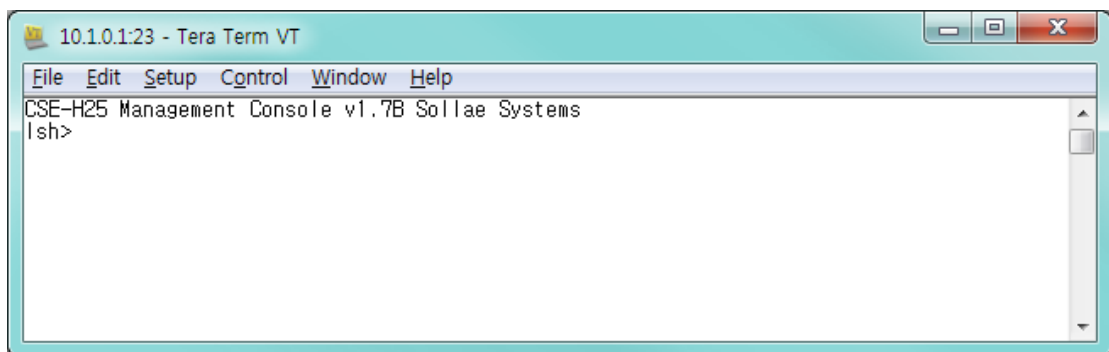


그림 2-2 텔넷 콘솔 접속

- ☞ **제품에 비밀번호가 설정되어 있다면 텔넷 접속 시 비밀번호를 입력해야 합니다. 또한 펌웨어 버전 2.0A부터는 비밀번호가 설정되어 있지 않더라도 "sollae"를 입력해야 합니다.**

- SSL과 관련된 텔넷 명령어는 다음과 같습니다.

항목	명령어	설명
RSA KEY	rsa keygen <key length>	지원 KEY 길이 512/768/1024
	rsa key	생성된 RSA KEY 확인
	rsa test	생성된 RSA KEY 테스트
인증서	cert new	인증서 생성 (생성된 RSA KEY 이용)
	cert view	현재 인증서 확인
설정 저장	ssl save aa55cc33	SSL 관련 설정 저장

표 2-1 SSL 기능설정 명령어

- RSA KEY 생성

인증서 생성에 필요한 RSA KEY를 먼저 만듭니다. KEY 길이는 512, 768, 1024 바이트를 지원하며 최대 수분의 시간이 걸릴 수도 있습니다. KEY 길이가 길수록 생성 시간이 길어지며 1024 바이트 KEY의 평균 소요시간은 약 1분입니다. 명령어는 'rsa keygen <key length>'의 형식으로 입력하며 다음은 실제 사용 예입니다.

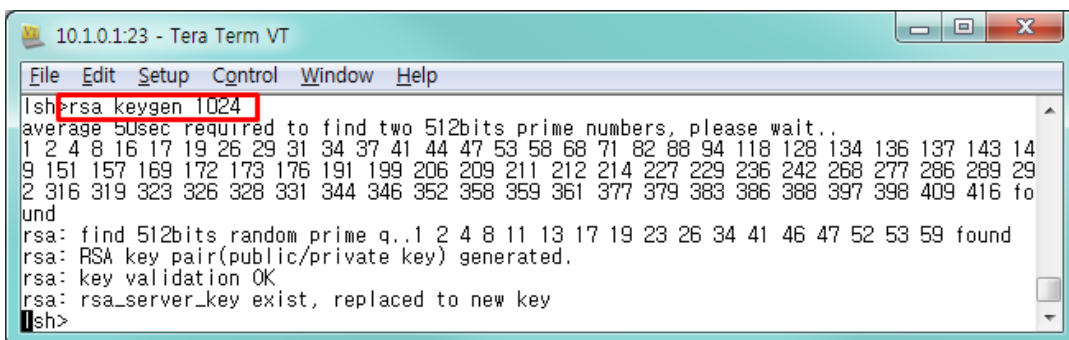


그림 2-3 RSA KEY 생성

생성된 RSA KEY는 'rsa test' 명령어를 통해 정상적으로 생성되었는지 테스트가 가능하며 현재 제품의 RSA KEY는 'rsa key' 명령어를 통해 확인이 가능합니다.

☞ **RSA KEY 생성시 기존에 있던 RSA KEY는 새로 생성된 것으로 자동으로 바뀝니다.**

3 사용 예

3.1 개요

3.1.1 TCP 접속 형태

사용 예는 크게 TCP 서버 / 클라이언트 2개로 나눌 수 있으며 각각에 따른 제품(ezTCP)의 통신 모드는 다음과 같습니다.

- TCP 서버
 “T2S – TCP 서버” 통신모드
 “ATC – AT 명령” 모드에서 ‘ata’ 명령어 통한 TCP 수동 접속
- TCP 클라이언트
 “COD – TCP 클라이언트” 통신모드
 “ATC – AT 명령” 모드에서 ‘atd(t)’ 명령어 통한 TCP 능동 접속

3.2 TCP 서버 모드

3.2.1 ezManager 확인

ezManager에서 [현재상태보기] 버튼을 눌러 현재 상태를 확인합니다.

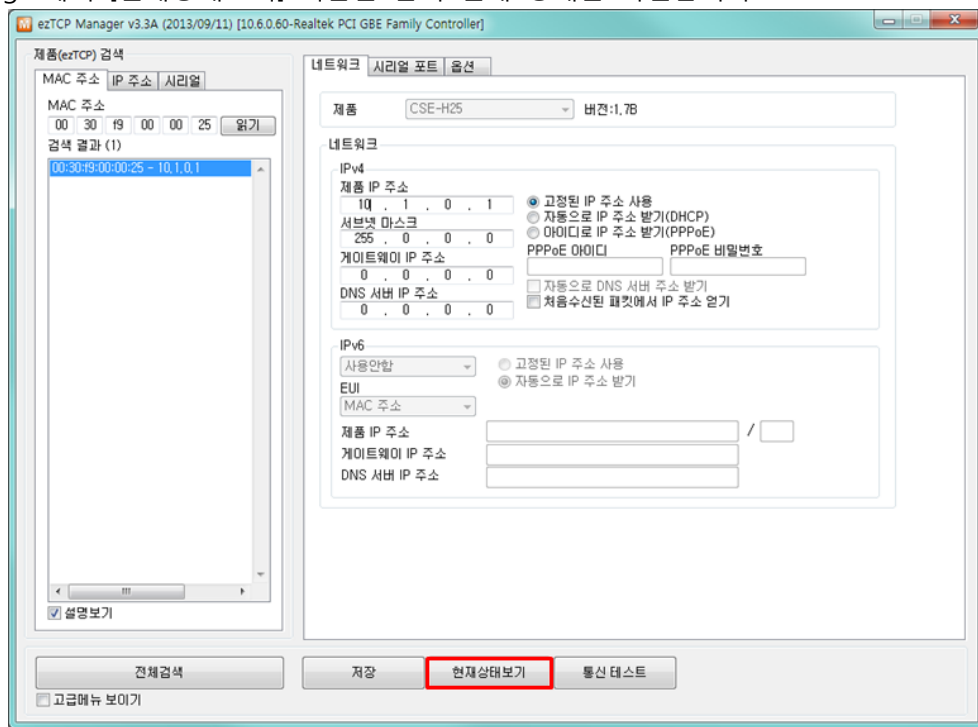


그림 3-1 ezManager [현재상태보기] 버튼

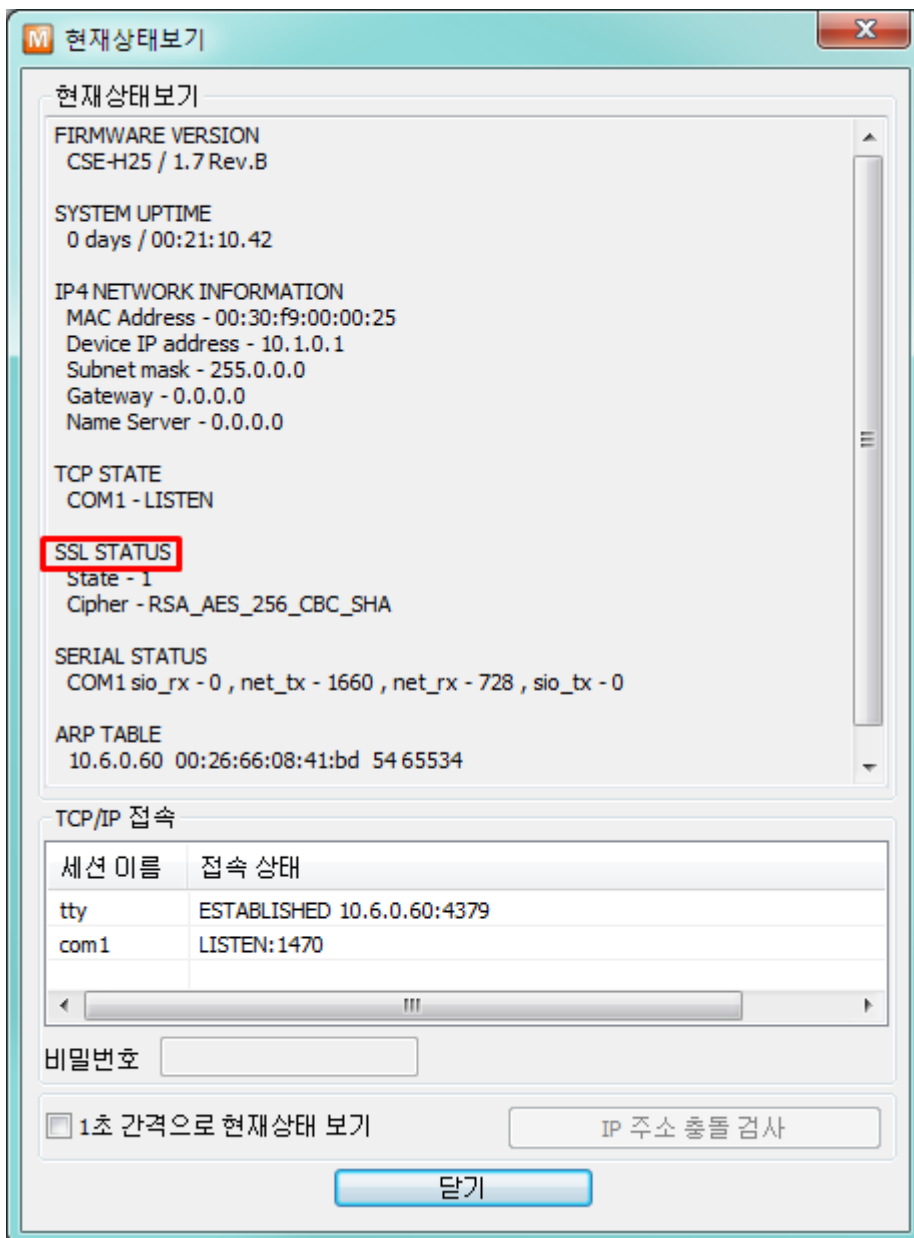
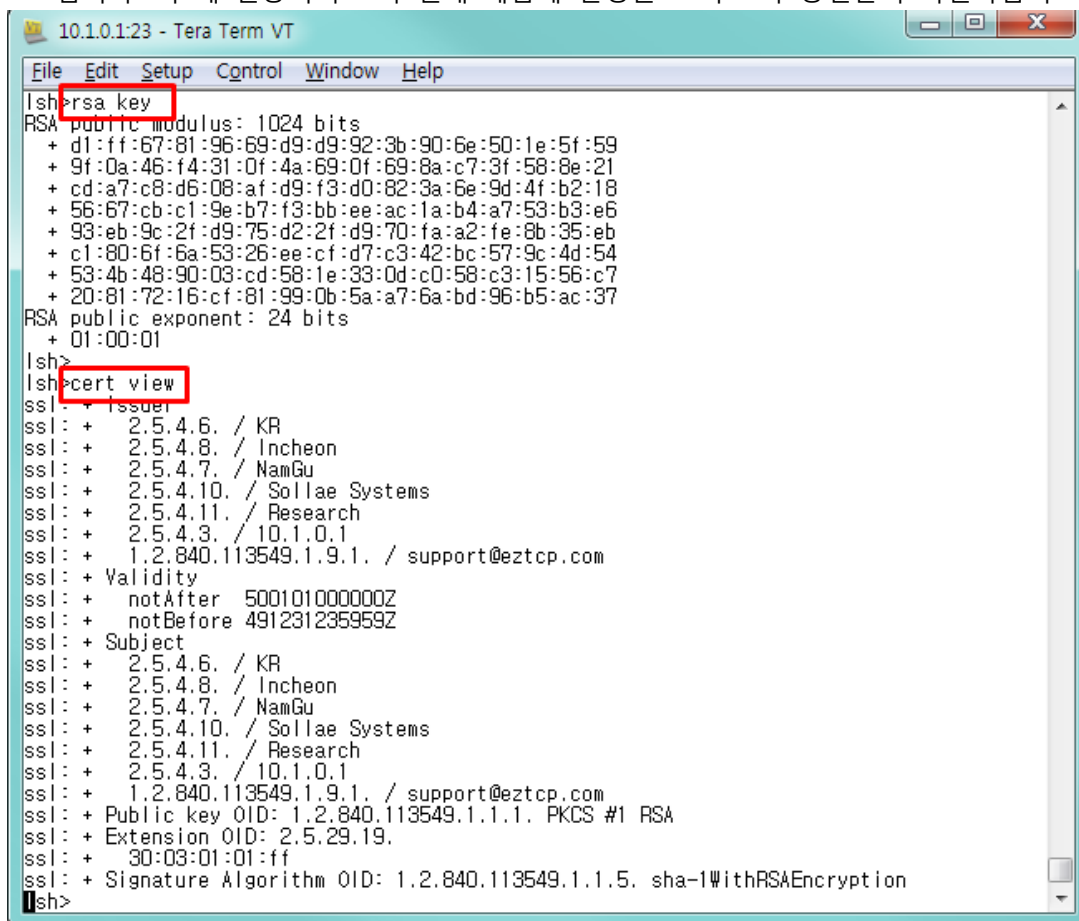


그림 3-2 ezManager “현재상태보기” 화면

위 그림과 같이 SSL STATUS 항목이 나타나는지 확인하십시오.

3.2.2 텔넷 접속 확인

제품의 텔넷 콘솔에 접속해 RSA KEY와 인증서 생성을 확인합니다. 관련 명령어는 'rsa key', 'cert view'입니다. 이 때 인증서의 IP와 현재 제품에 설정된 IP 주소가 동일한지 확인하십시오.



```

10.1.0.1:23 - Tera Term VT
File Edit Setup Control Window Help
lsh>rsa key
RSA public modulus: 1024 bits
+ d1:ff:67:81:96:69:d9:d9:92:3b:90:6e:50:1e:5f:59
+ 9f:0a:46:f4:31:0f:4a:69:0f:69:8a:c7:3f:58:8e:21
+ cd:a7:c8:d6:08:af:d9:f3:d0:82:3a:6e:9d:4f:b2:18
+ 56:67:cb:c1:9e:b7:f3:bb:ee:ac:1a:b4:a7:53:b3:e6
+ 93:eb:9c:2f:d9:75:d2:2f:d9:70:fa:a2:fe:8b:35:eb
+ c1:80:6f:6a:53:26:ee:cf:d7:c3:42:bc:57:9c:4d:54
+ 53:4b:48:90:03:cd:58:1e:33:0d:c0:58:c3:15:56:c7
+ 20:81:72:16:cf:81:99:0b:5a:a7:6a:bd:96:b5:ac:37
RSA public exponent: 24 bits
+ 01:00:01
lsh>
lsh>cert view
ssl: + Issuer
ssl: + 2.5.4.6. / KR
ssl: + 2.5.4.8. / Incheon
ssl: + 2.5.4.7. / NamGu
ssl: + 2.5.4.10. / Sollae Systems
ssl: + 2.5.4.11. / Research
ssl: + 2.5.4.3. / 10.1.0.1
ssl: + 1.2.840.113549.1.9.1. / support@eztcp.com
ssl: + Validity
ssl: + notAfter 500101000000Z
ssl: + notBefore 491231235959Z
ssl: + Subject
ssl: + 2.5.4.6. / KR
ssl: + 2.5.4.8. / Incheon
ssl: + 2.5.4.7. / NamGu
ssl: + 2.5.4.10. / Sollae Systems
ssl: + 2.5.4.11. / Research
ssl: + 2.5.4.3. / 10.1.0.1
ssl: + 1.2.840.113549.1.9.1. / support@eztcp.com
ssl: + Public key OID: 1.2.840.113549.1.1.1. PKCS #1 RSA
ssl: + Extension OID: 2.5.29.19.
ssl: + 30:03:01:01:ff
ssl: + Signature Algorithm OID: 1.2.840.113549.1.1.5. sha-1#withRSAEncryption
lsh>

```

그림 3-3 RSA KEY 및 인증서 확인

3.2.3 접속하기

SSL 기능이 활성화된 제품(ezTCP)과 통신을 하려면 상대 호스트도 SSL 을 지원해야 합니다. 본 절에서는 당사 ezVSP를 이용한 접속 테스트 과정을 소개하겠습니다.

- 설정 전 확인 사항

IP 주소("네트워크" 탭의 [제품 IP 주소] 및 "시리얼 포트" 탭의 [통신할 주소])와 포트 번호("시리얼 포트" 탭의 [제품 로컬포트] 및 [통신할 포트])는 제품(ezTCP)가 설치된 환경에 맞게 설정해야 하지만 이해를 돕기 위해 공장 출하 시 설정 값으로 가정하겠습니다.

구분	제품(ezTCP)	PC
IP 주소	10.1.0.1	10.1.0.2
서브넷 마스크	255.0.0.0	255.0.0.0
제품 로컬포트	1470	-

표 3-1 설정 값 확인

- ezVSP 설정하기

ezManager의 "시리얼 포트" 탭의 [ezVSP에 포트 생성] 버튼을 누르십시오.

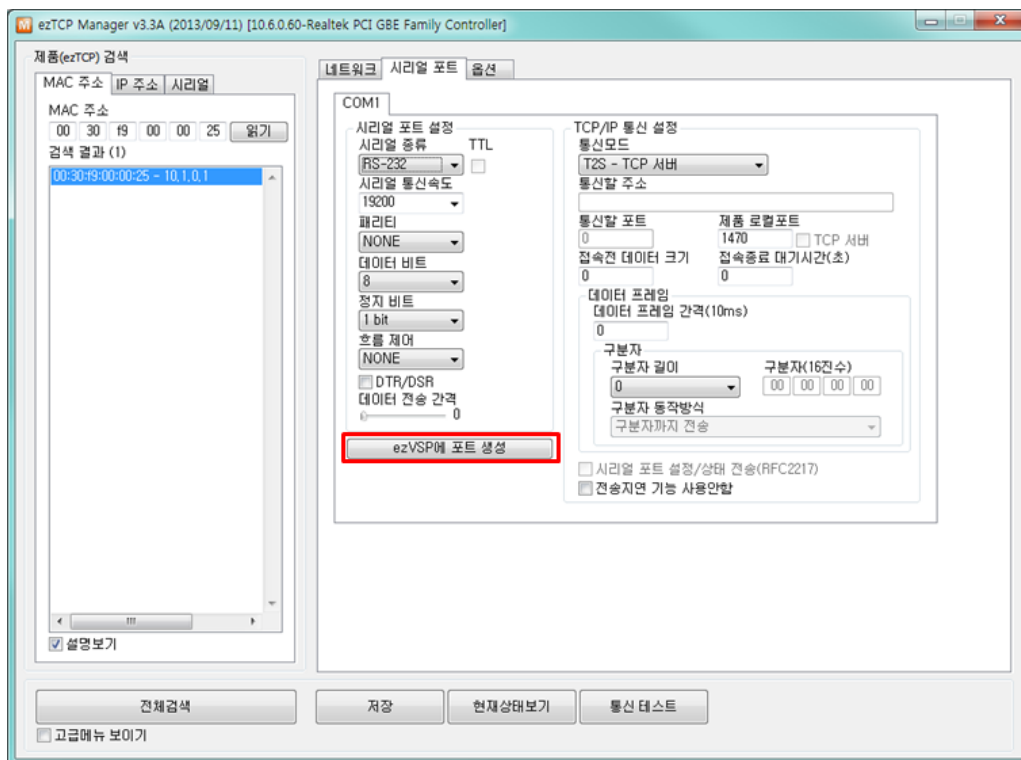


그림 3-4 ezVSP에 포트 생성(1)

다음 그림과 같이 확인 버튼을 누릅니다.

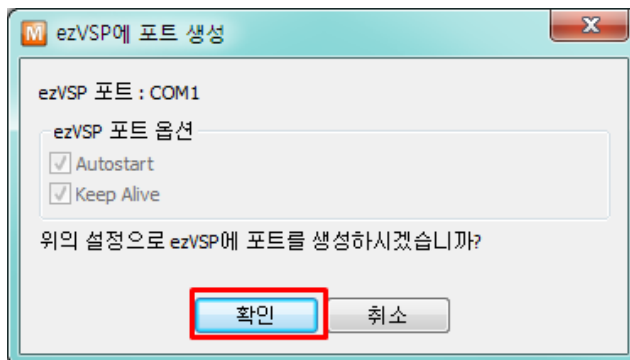


그림 3-5 ezVSP에 포트 생성(2)

포트 생성이 완료되면 ezVSP 프로그램에서 해당 가상포트를 시작해주시요.

☞ *ezVSP는 PC상에 가상의 시리얼 포트를 생성하고 ezTCP 제품과 동일한 역할을 하는 프로그램으로 자세한 사용 및 설치 정보는 ezVSP 사용자 설명서를 참조하십시오.*

- TCP 접속 확인

ezVSP의 가상포트가 정상적으로 시작되면 제품(ezTCP)과 ezVSP의 가상포트간에 SSL 기능을 이용한 TCP 접속이 이루어집니다. 이를 ezManager의 [현재상태보기] 버튼을 통해 확인합니다.

아래의 그림과 같이 "TCP STATE" 항목에서 "COM1 - ESTABLISHED"가 확인되고, "SSL STATUS" 항목에서 [State - 7(또는 8)]과 [Cipher - RSA_AES_256CBC_SHA]가 확인되면 통신 준비가 완료된 것입니다.

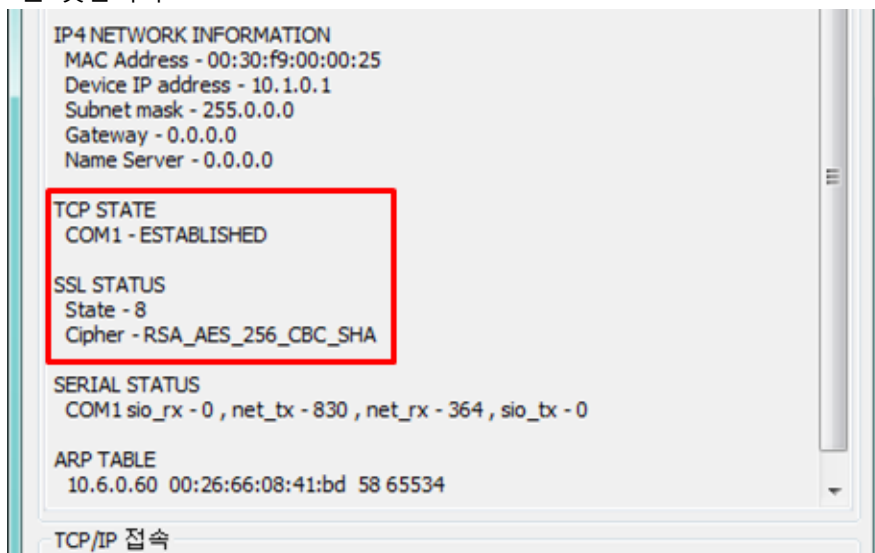


그림 3-6 SSL 기능 TCP 접속 확인

3.3 TCP 클라이언트 모드

TCP 클라이언트 모드는 SSL 설정 활성화만을 통해 사용이 가능합니다. 이 경우, ezTCP가 접속할 TCP 서버도 SSL을 지원해야 합니다. 현재 TCP 접속 상태 확인은 TCP 서버 모드와 동일하게 ezManager의 [현재상태보기] 버튼을 이용하십시오.

4 변경 이력

날짜	버전	설명	작성자
2008.08.28	1.0	○ 최초 배포	-
2009.06.11	1.1	○ 일부 용어, 그림 및 내용 오류 수정 ○ 지원 제품 CSE-H25 추가	-
2015.02.06	1.2	○ 그림 업데이트 ○ 일부 오류 및 표현 수정	이 인
2016.04.07	1.3	○ 텔넷 로그인 관련 안내문구 추가	이 인