CUCM-CUBE/CUBE-SBC 간 SIP TLS 구성

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[구성](#)

- [네트워크 다이어그램](#)
- [컨피그레이션 단계](#)

[다음을 확인합니다.](#)

[문제 해결](#)

목차

소개

이 문서는 CUCM(Cisco Unified Communication Manager)과 CUBE(Cisco Unified Border Element) 간에 SIP TLS(Transport Layer Security)를 구성하는 데 도움이 됩니다

사전 요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다

- SIP 프로토콜
- 보안 인증서

요구 사항

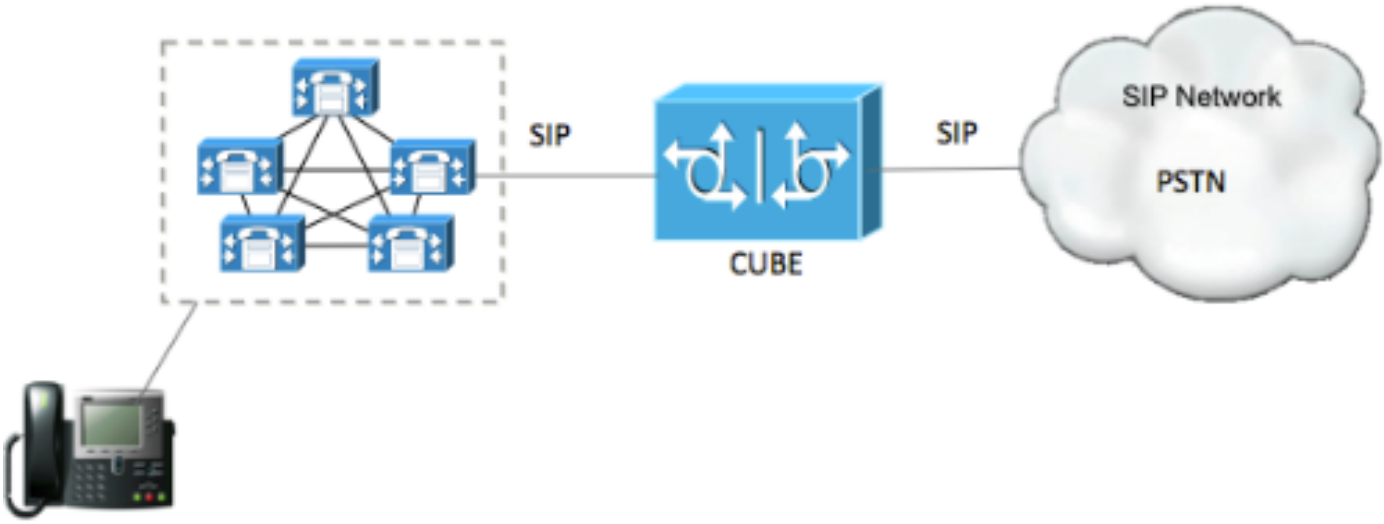
- 날짜 및 시간은 엔드포인트에서 일치해야 합니다(동일한 NTP 소스를 사용하는 것이 좋습니다).
- CUCM은 혼합 모드여야 합니다.
- TCP 연결이 필요합니다(모든 트랜짓 방화벽에서 포트 5061을 엽니다).
- CUBE에는 보안 및 UCK9 라이센스가 설치되어 있어야 합니다.

사용되는 구성 요소

- SIP
- 자체 서명된 인증서

구성

네트워크 다이어그램



컨피그레이션 단계

1단계. CUBE의 자체 서명 인증서를 보유하기 위해 신뢰 지점 생성

```
crypto pki trustpoint CUBEtest(this can be any name)
 enrollment selfsigned
 serial-number none
 fqdn none
 ip-address none
 subject-name cn= ISR4451-B.cisco.lab !(this has to match the router’s host name)
 revocation-check none
 rsakeypair ISR4451-B.cisco.lab !(this has to match the router's host name)
```

2단계. 신뢰 지점이 생성되면 Crypto pki enroll CUBEtest 명령을 실행하여 자체 서명 인증서를 가져옵니다.

```
crypto pki enroll CUBEtest
% The fully-qualified domain name will not be included in the certificate
Generate Self Signed Router Certificate? [yes/no]: yes
```

등록이 올바른 경우 이 결과가 표시되어야 합니다.

```
Router Self Signed Certificate successfully created
```

3단계. 인증서를 얻은 후 내보내야 합니다.

```
crypto pki export CUBEtest pem terminal
```

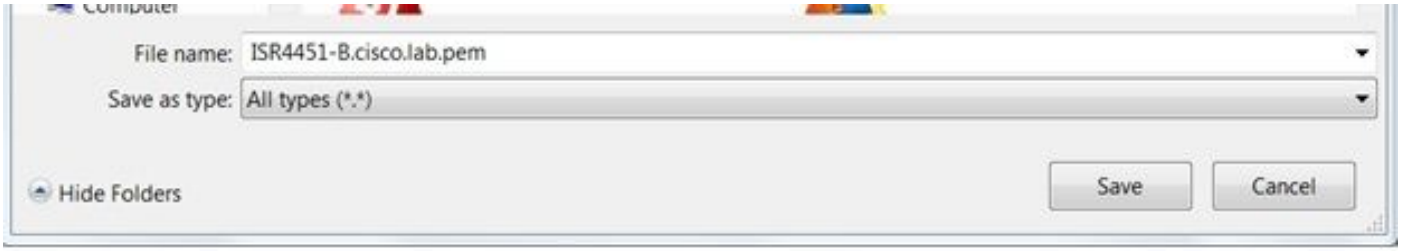
위 명령은 아래 인증서를 생성해야 합니다

```
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1IO
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1IO
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
```

```
AOsAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/eOb2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MAOGCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXqOEVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
-----END CERTIFICATE-----
```

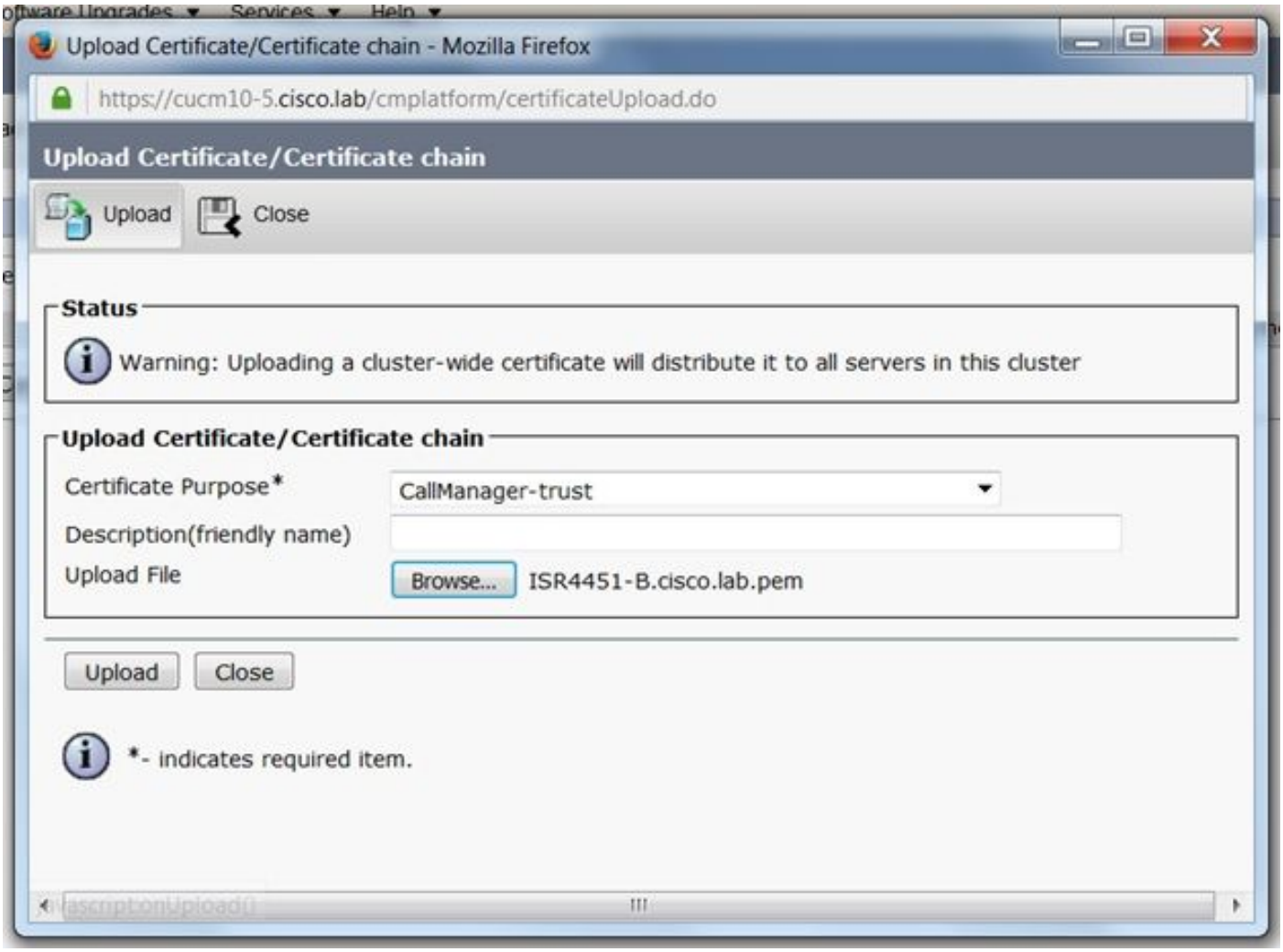
위에서 생성한 자체 서명 인증서를 복사하고 파일 확장자가 .pem인 텍스트 파일에 붙여넣습니다.

아래의 예는 ISR4451-B.ciscolab.pem으로 명명됩니다.



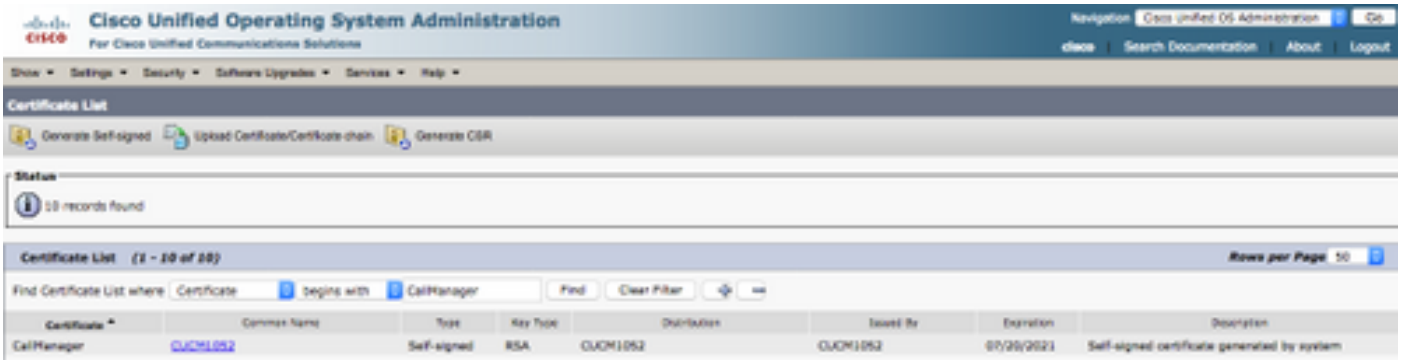
4단계. CUBE 인증서를 CUCM에 업로드합니다

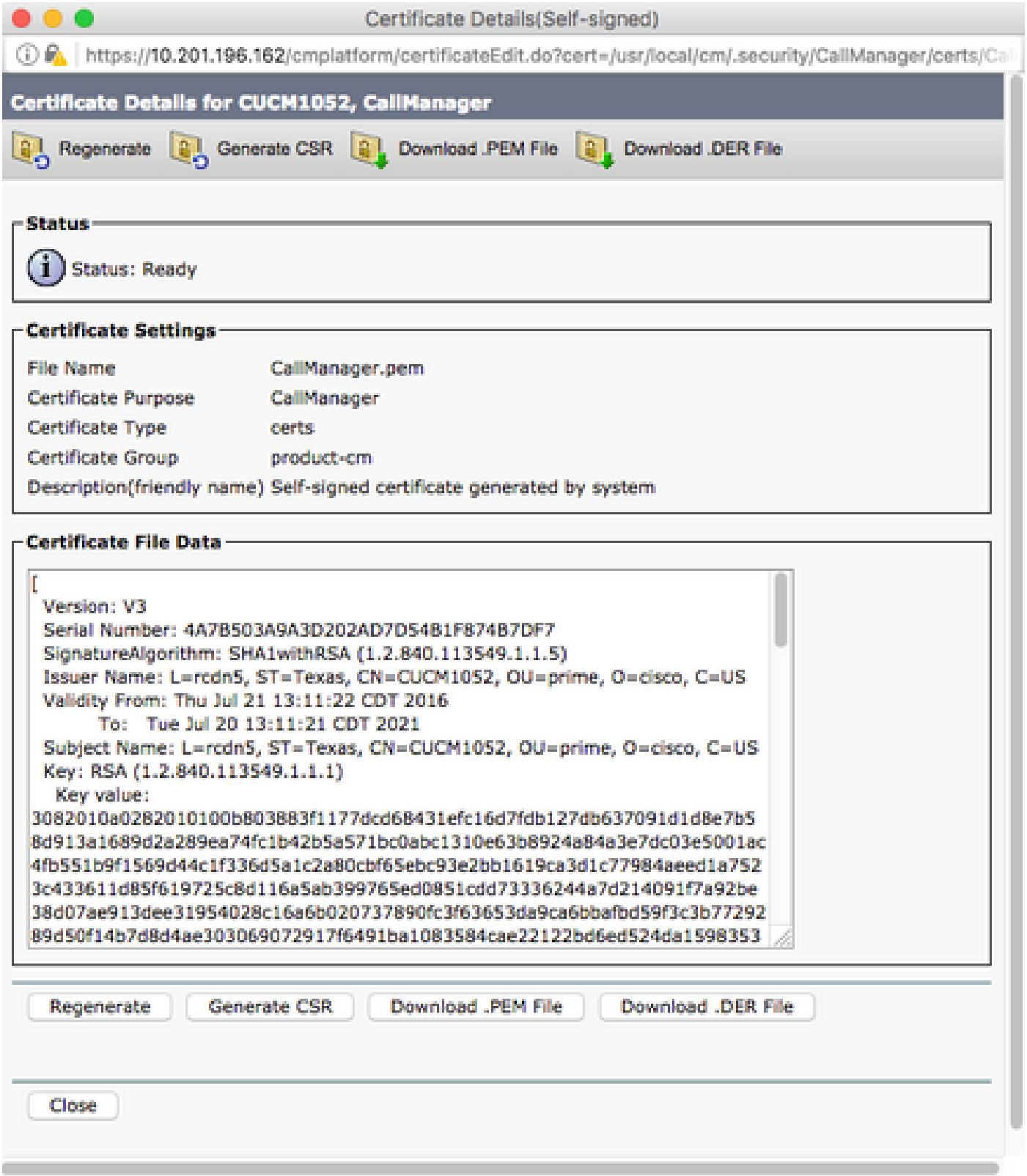
- CUCM OS Admin(CUCM OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate chain(인증서/인증서 체인 업로드)
- 인증서 용도 = CallManager-Trust
- .pem 파일 업로드



5단계. Call Manager 자체 서명 인증서 다운로드

- Callmanager라고 표시된 인증서 찾기
- 호스트 이름을 클릭합니다.
- PEM 파일 다운로드를 클릭합니다.
- 컴퓨터에 저장





6단계. CUBE에 Callmanager.pem 인증서 업로드

- 텍스트 파일 편집기로 Callmanager.pem 열기
- 파일의 전체 내용을 복사합니다.
- CUBE에서 이 명령 실행

```
crypto pki trustpoint CUCMHOSTNAME
```

```
 enrollment terminal
 revocation-check none

crypto pku authenticate CUCMHOSTNAME

(PASTE THE CUCM CERT HERE AND THEN PRESS ENTER TWICE)

    You will then see the following:

Certificate has the following attributes:
       Fingerprint MD5: B9CABE35 24B11EE3 C58C9A9F 02DB16BC
      Fingerprint SHA1: EC164F6C 96CDC1C9 E7CA0933 8C7518D4 443E0E84

% Do you accept this certificate? [yes/no]: yes

    If everything was correct, you should see the following:

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

7단계. CUBE의 자체 서명 인증서 신뢰 지점을 사용하도록 SIP 구성

```
sip-ua
 crypto signaling default trustpoint CUBEtest
```

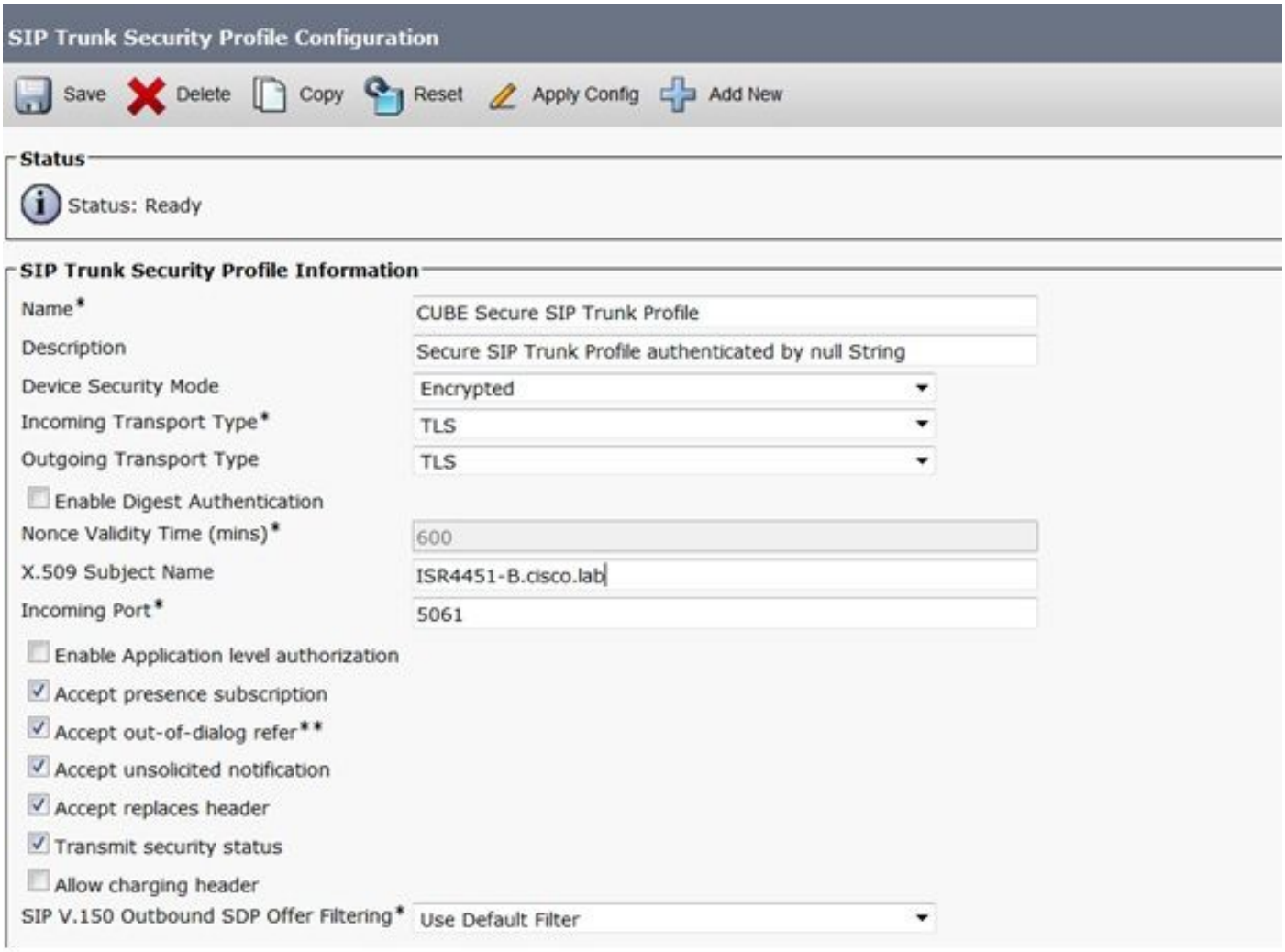
8단계. TLS를 사용하여 다이얼 피어 구성

```
dial-peer voice 9999 voip
```

```
answer-address 35..

destination-pattern 9999

session protocol sipv2

session target dns:cucm10-5

session transport tcp tls

voice-class sip options-keepalive

srtp
```

9단계. CUCM SIP 트렁크 보안 프로파일 구성

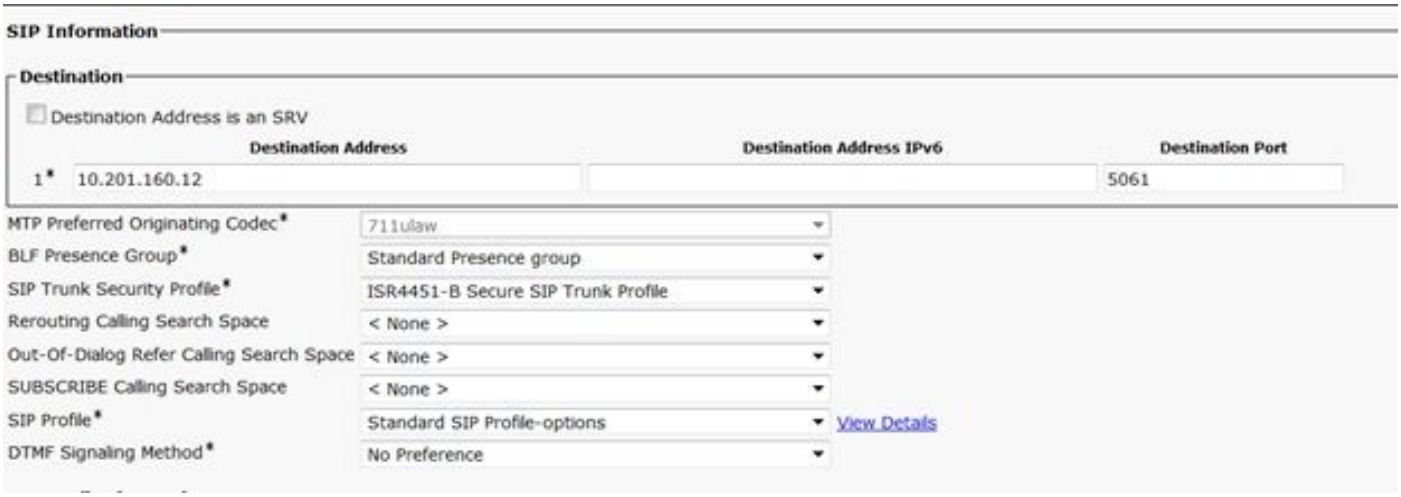
- CUCM Admin(CUCM 관리) 페이지 > System(시스템) > Security(보안) > SIP Trunk Security Profile(SIP 트렁크 보안 프로파일)
- 아래와 같이 프로필을 구성합니다



참고: X.509 필드는 자체 서명 인증서를 생성하는 동안 이전에 구성한 CN 이름과 일치해야 합니다

10단계. CUCM에서 SIP 트렁크 구성

- SRTP allowed 확인란을 선택합니다
- 올바른 대상 주소를 구성하고 포트 5060을 포트 5061로 교체합니다.
- 올바른 Sip 트렁크 보안 프로필(9단계에서 생성됨)을 선택해야 합니다.



- 트렁크를 저장하고 재설정합니다.

다음을 확인합니다.

CUCM에서 OPTIONS PING을 활성화했으므로 SIP 트렁크는 FULL SERVICE 상태여야 합니다

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			G711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

SIP 트렁크 상태는 전체 서비스를 표시합니다.

다이얼 피어 상태는 다음과 같이 표시됩니다.

```
show dial-peer voice summary

TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT    KEEPALIVE

9999   voip  up   up             9999               0  syst dns:cucm10-5                  active
```

문제 해결

이러한 디버그의 출력을 활성화하고 수집합니다.

```
debug crypto pki api
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki transactions
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
debug ip tcp transactions
debug ccsip verbose
```

Webex Recording 링크:

https://goo.gl/QOS1iT

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.