CA 서명 인증서를 사용하여 Communications Manager에서 SIP TLS 트렁크 구성

목차

소개

이 문서에서는 CA(Certificate Authority) 서명 인증서를 사용하여 Communications Manager에서 SIP(Session Initiation Protocol) TLS(Transport Layer Security) 트렁크를 구성하는 단계별 프로세스에 대해 설명합니다.

이 문서를 팔로우하면 두 클러스터 간의 SIP 메시지가 TLS를 사용하여 암호화됩니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 사항에 대해 알고 있는 것이 좋습니다.

- Cisco CUCM(Unified Communications Manager)
- SIP

사용되는 구성 요소

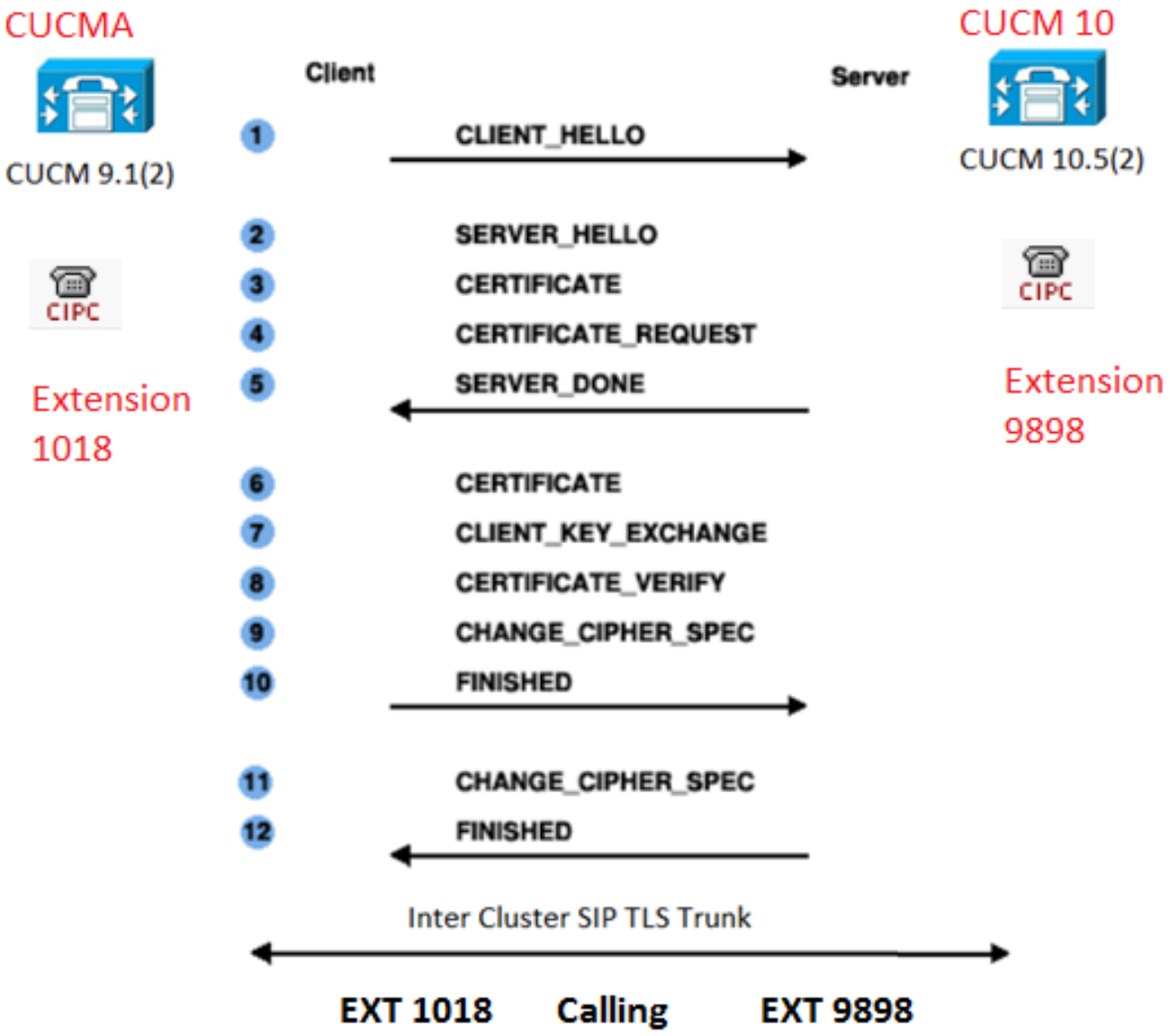
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CUCM 버전 9.1(2)
- CUCM 버전 10.5(2)
- Microsoft Windows Server 2003을 CA로 사용

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 이미지에 표시된 것처럼 인증서를 사용하는 SSL 핸드셰이크입니다.



구성

1단계. Windows Server 2003에서 공용 CA 또는 CA 설정

링크를 참조하십시오.Windows 2003 서버에서 CA 설정

2단계. 호스트 이름 및 설정 확인

인증서는 이름을 기반으로 합니다.시작하기 전에 이름이 올바른지 확인하십시오.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

호스트 이름을 변경하려면 다음 링크를 참조하십시오.CUCM의 호스트 이름 변경

3단계. CSR(Certificate Signing Request) 생성 및 다운로드

CUCM 9.1(2)

CSR을 생성하려면 **OS Admin(OS 관리) > Security(보안) > Certificate Management(인증서 관리) >** Generate CSR(**CSR 생성)로** 이동합니다.

Certificate **Name** 필드**의** 드롭다운 목록에서 CallManager 옵션을 선택합니다.

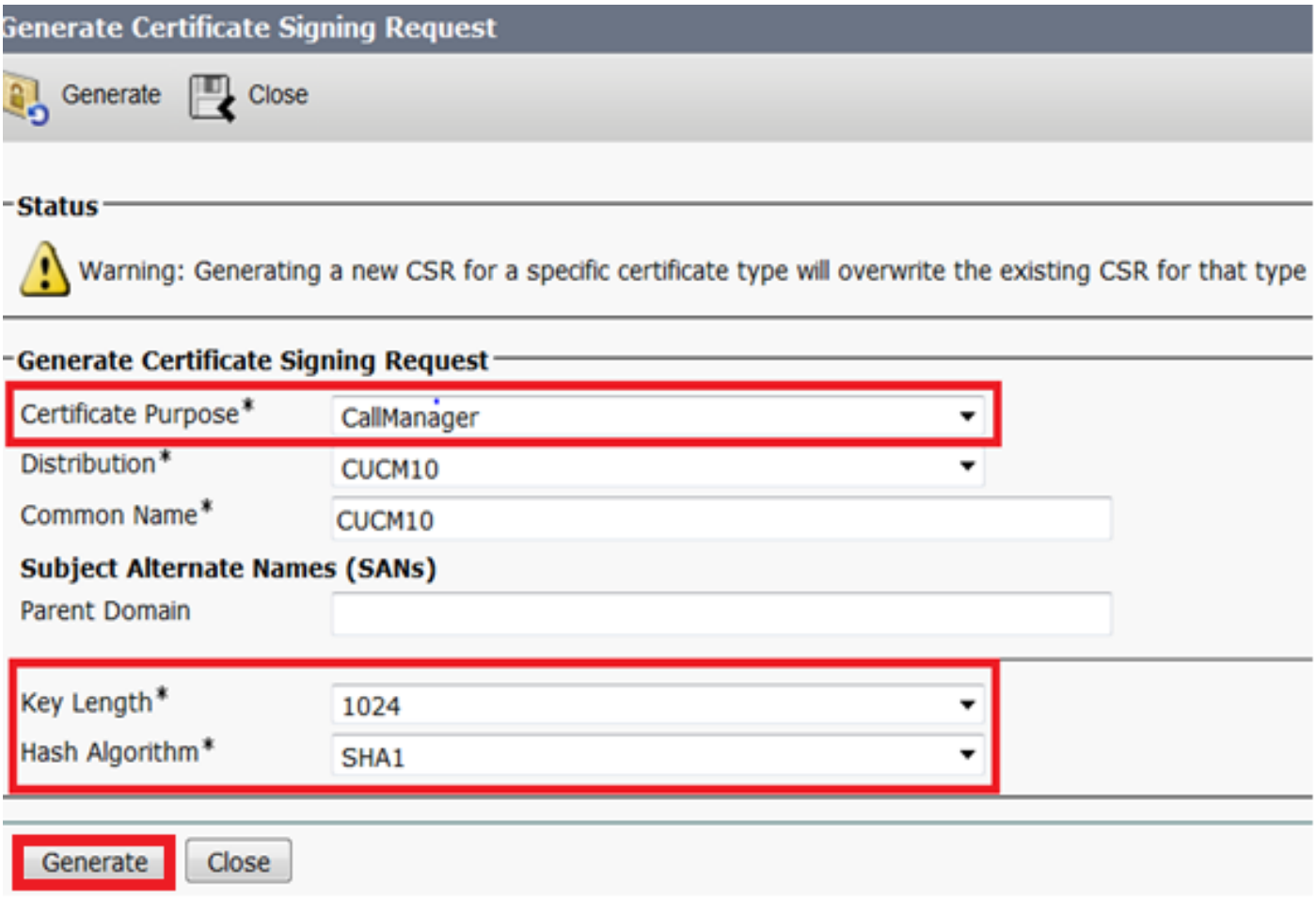
CSR을 다운로드하려면 **OS Admin(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Download CSR(CSR 다운로드)로** 이동합니다.

Certificate Name 필드의 드롭다운 목록에서 CallManager 옵션을 선택합니다.

CUCM 10.5(2)

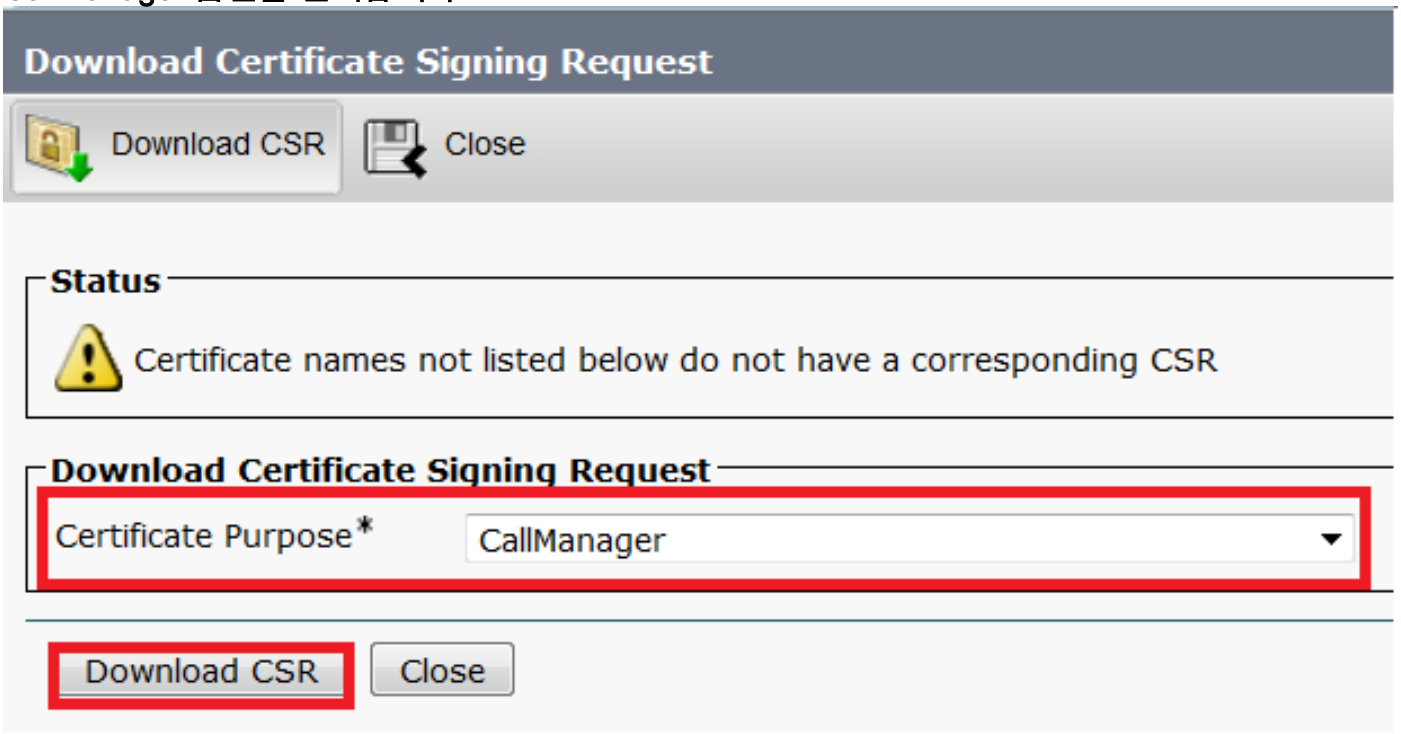
CSR을 생성하려면 OS Admin(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Generate CSR(CSR 생성)로 이동합니다.

1. 인증서 용도 필드의 드롭다운 목록에서 CallManager를 선택합니다.
2. 키 길이 필드의 드롭다운 목록에서 1024를 선택합니다..
3. Hash Algorithm 필드의 드롭다운 목록에서 SHA1을 선택합니다.

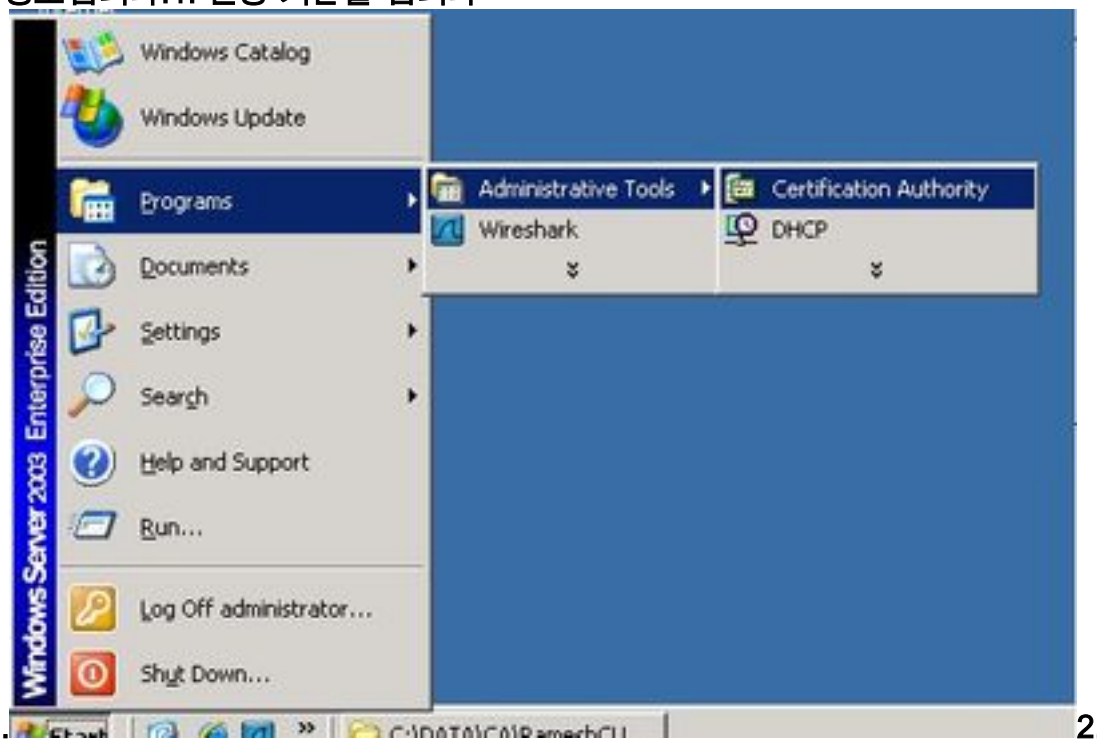


CSR을 다운로드하려면 OS Admin(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Download CSR(CSR 다운로드)로 이동합니다.Certificate Purpose 필드의 드롭다운 목록에서

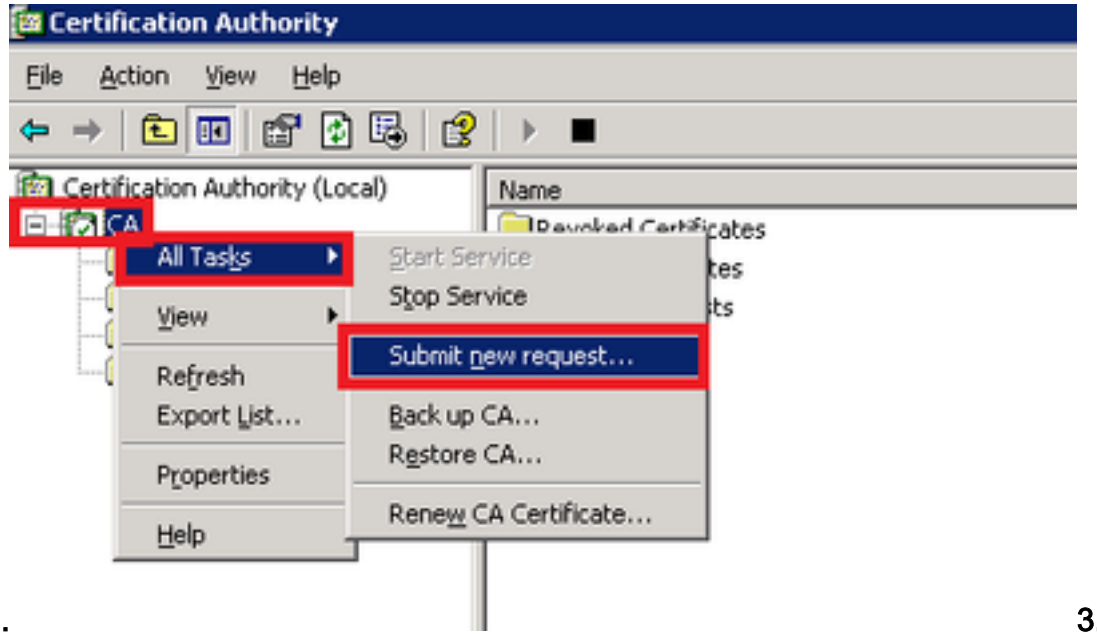
CallManager 옵션을 선택합니다.



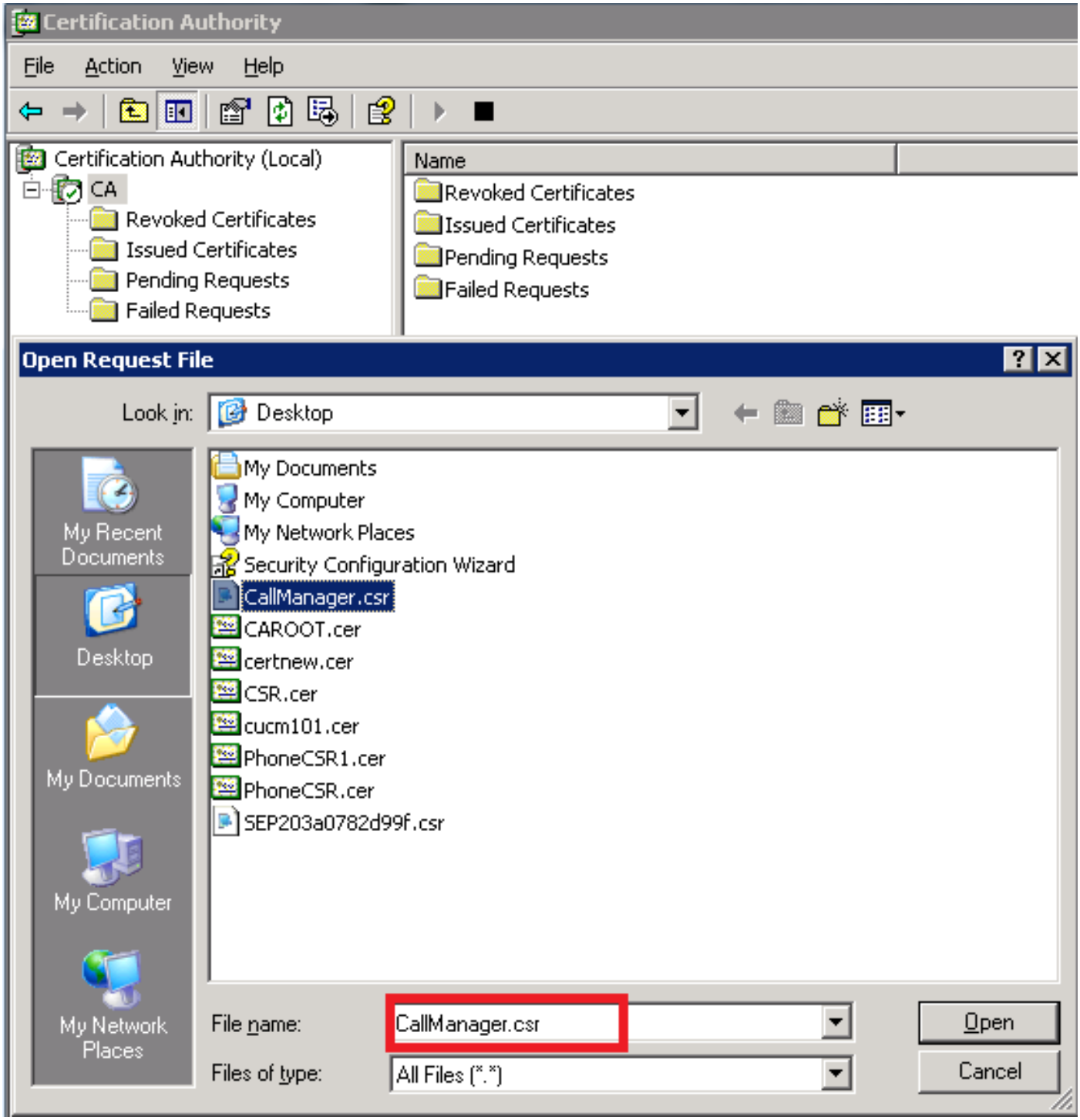
참고:CallManager CSR은 1024비트 RSA(Rivest-Shamir-Addleman) 키와 함께 생성됩니다.4단계. Microsoft Windows 2003 인증 기관으로 CSR에 서명이 정보는 Microsoft Windows 2003 CA로 CSR에 서명하는 선택적 정보입니다.1. 인증 기관을 엽니다



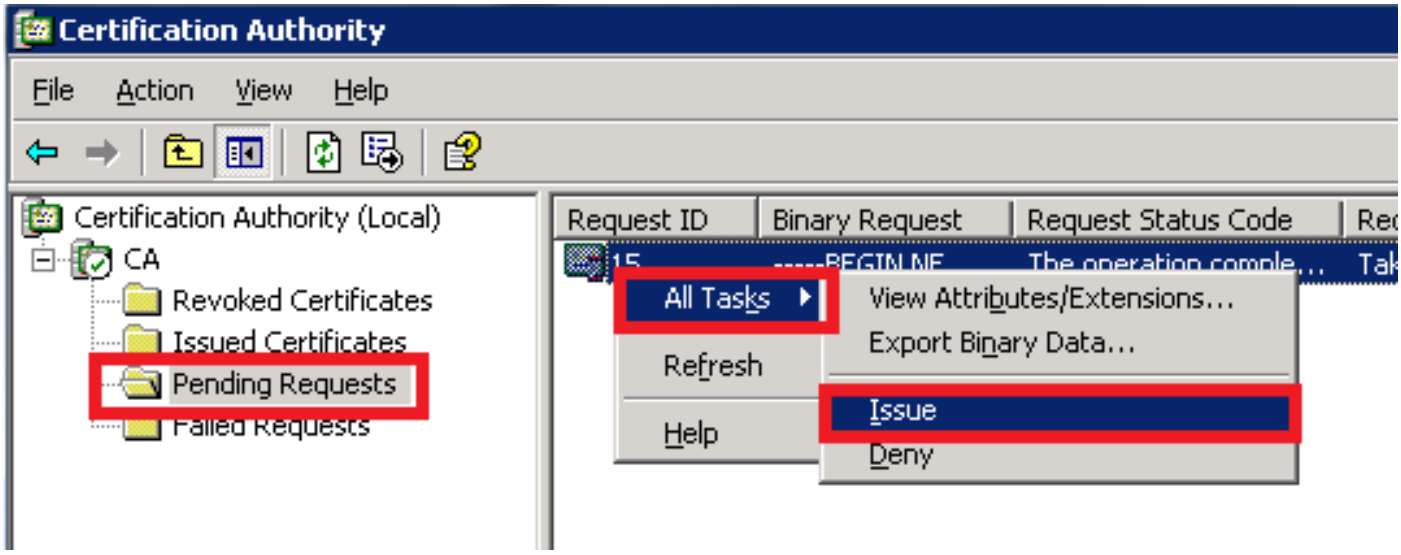
2. CA 아이콘을 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Submit new request(새 요청 제출)로 이동합니



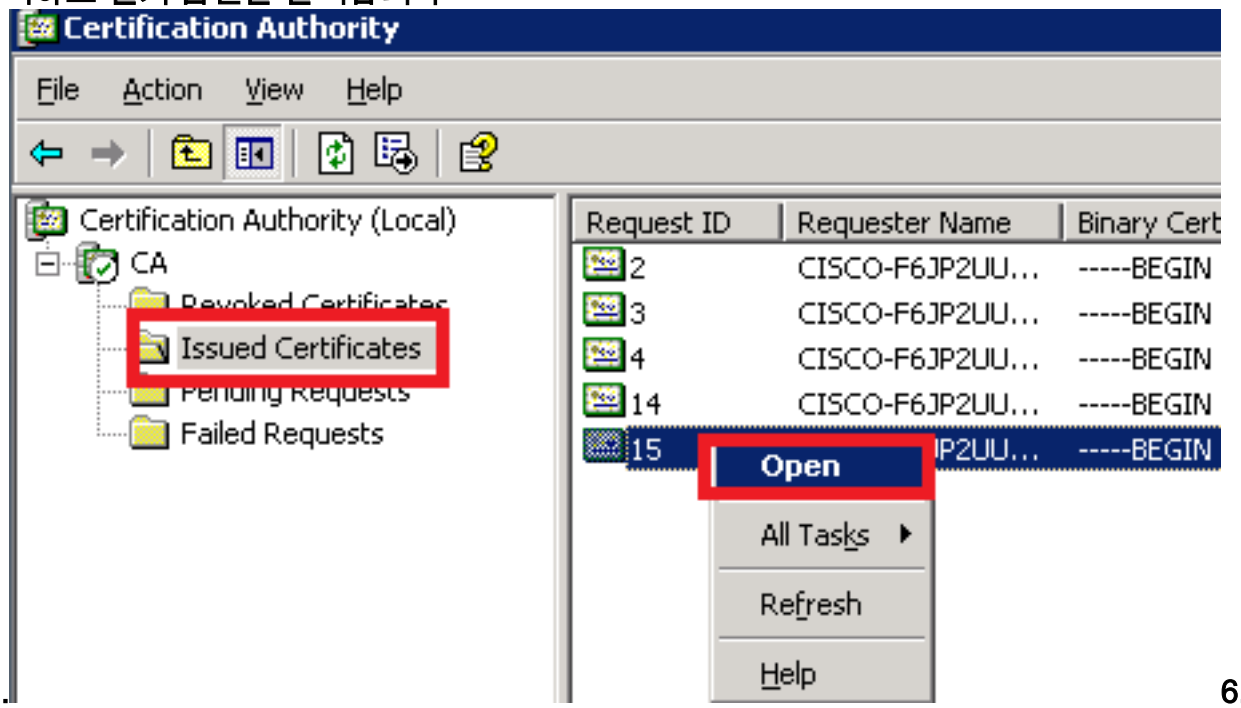
다. 3. CSR을 선택하고 열기 옵션을 클릭합니다(CSR(CUCM 9.1(2) 및 CUCM 10.5(2)에서 모두 적용 가능).



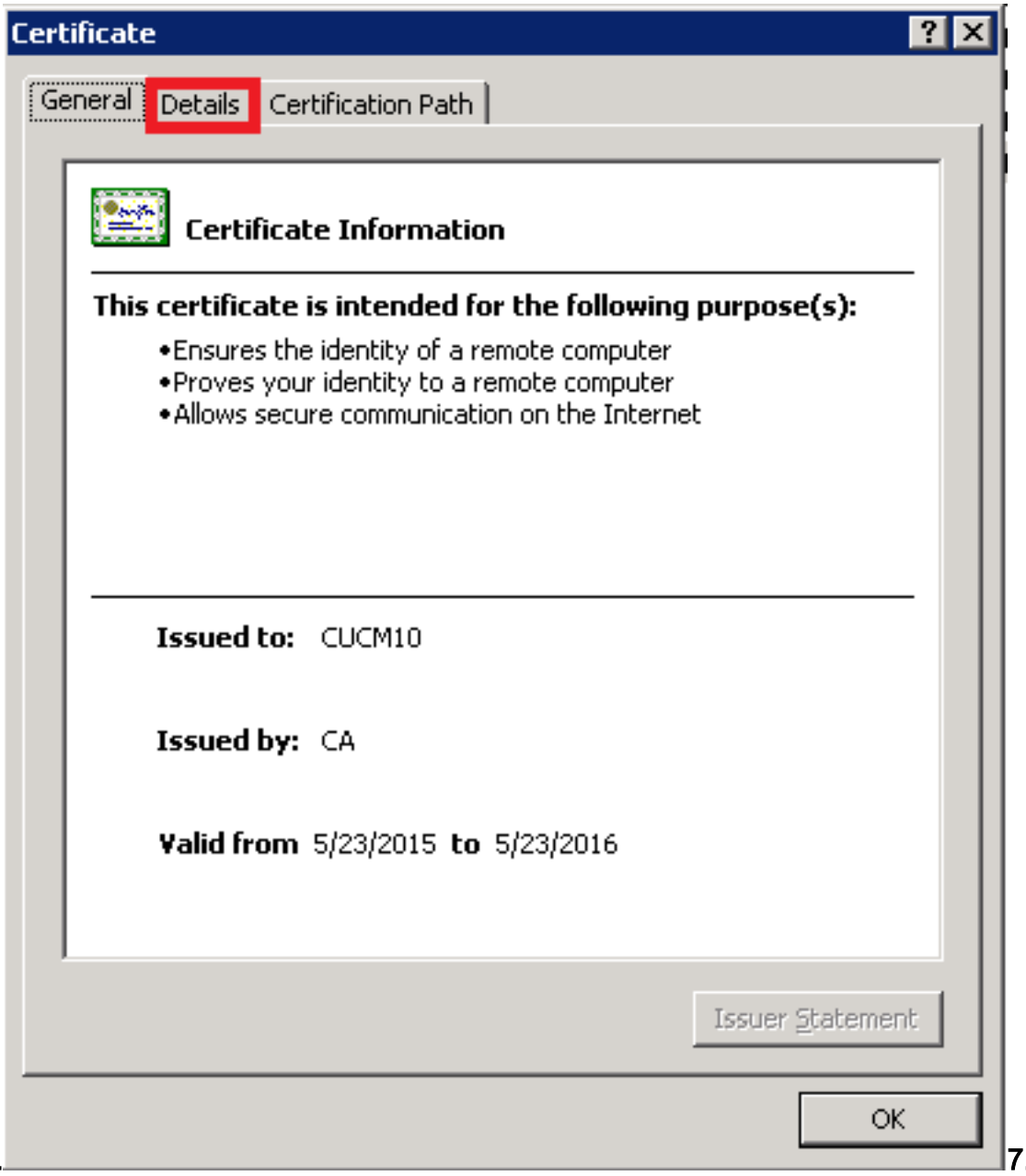
4. 열린 모든 CSR이 대기 중인 요청 폴더에 표시됩니다.각 CSR을 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Issue(문제)로 이동하여 인증서를 발급합니다.(CSR(CUCM 9.1(2) 및 CUCM 10.5(2)에 모두 적용
)



5. 인증서를 다운로드하려면 발급된 인증서 폴더를 선택합니다.인증서를 마우스 오른쪽 단추로 클릭하고 열기 옵션을 클릭합니다

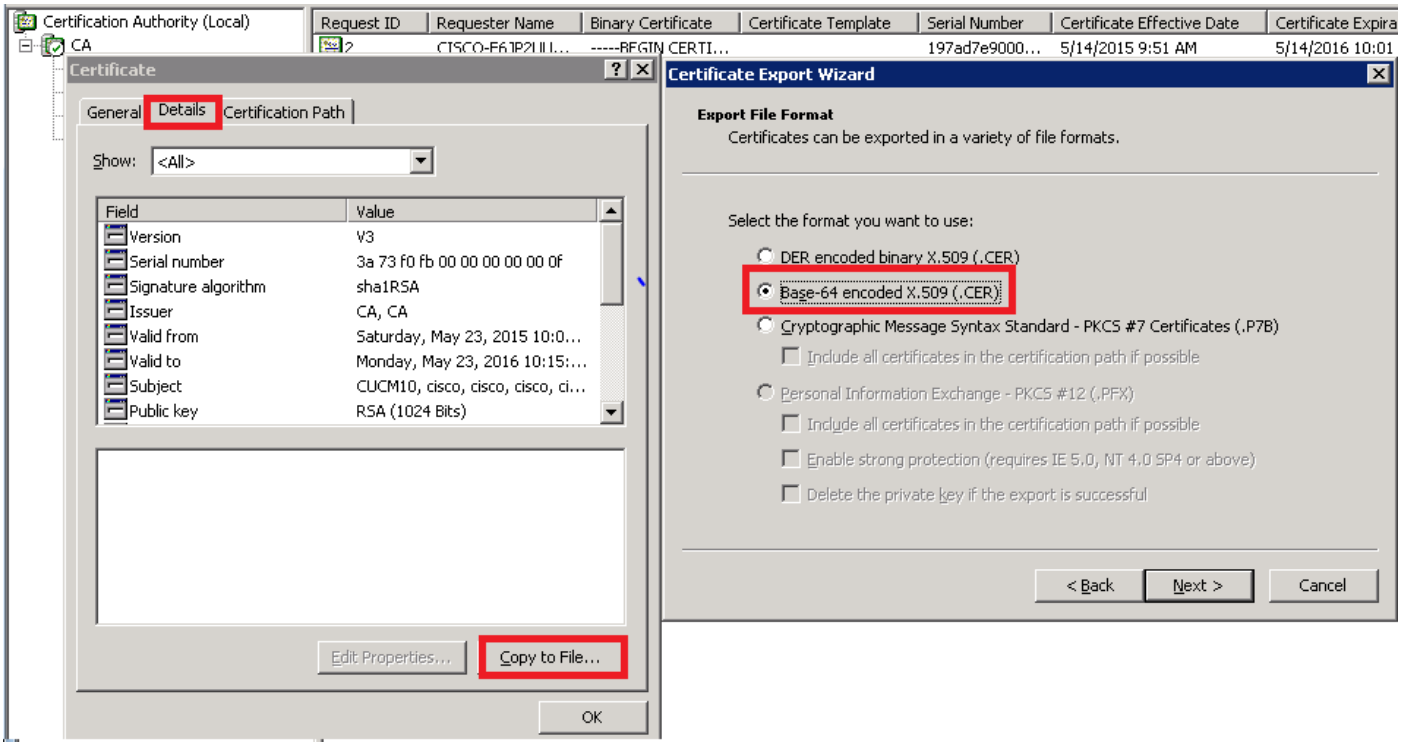


6. 인증서 세부사항이 표시됩니다.인증서를 다운로드하려면 Details 탭을 선택하고 Copy to File(파일에 복사...)

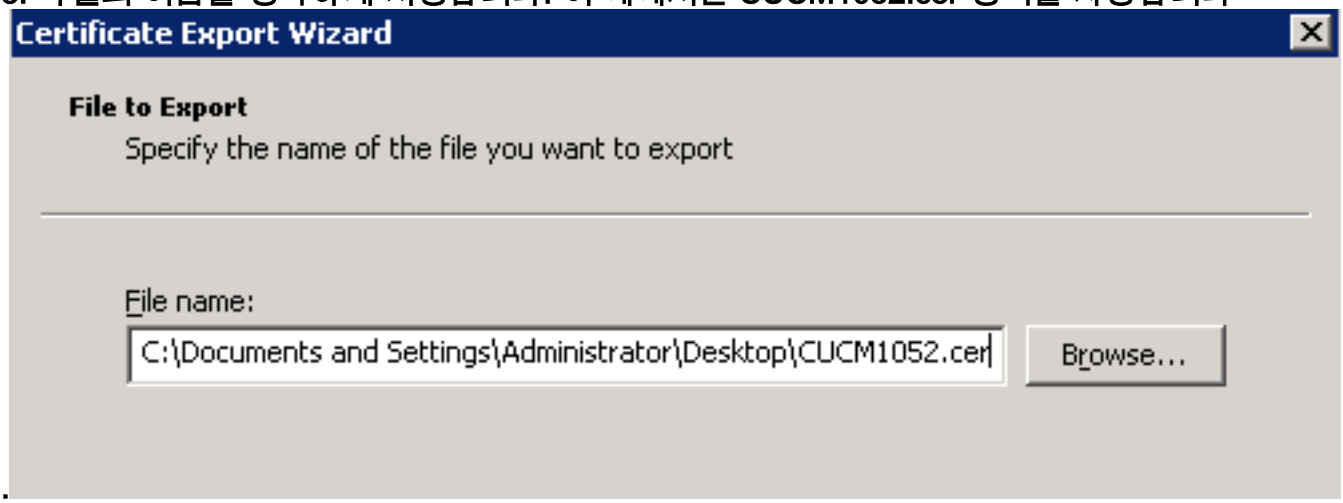


버튼을 클릭합니다. 7. Certificate Export Wizard(인증서 내보내기 마법사) 창에서 Base-64 인코딩 X.509(.CER) 라디오 버튼을 클릭합니다

.

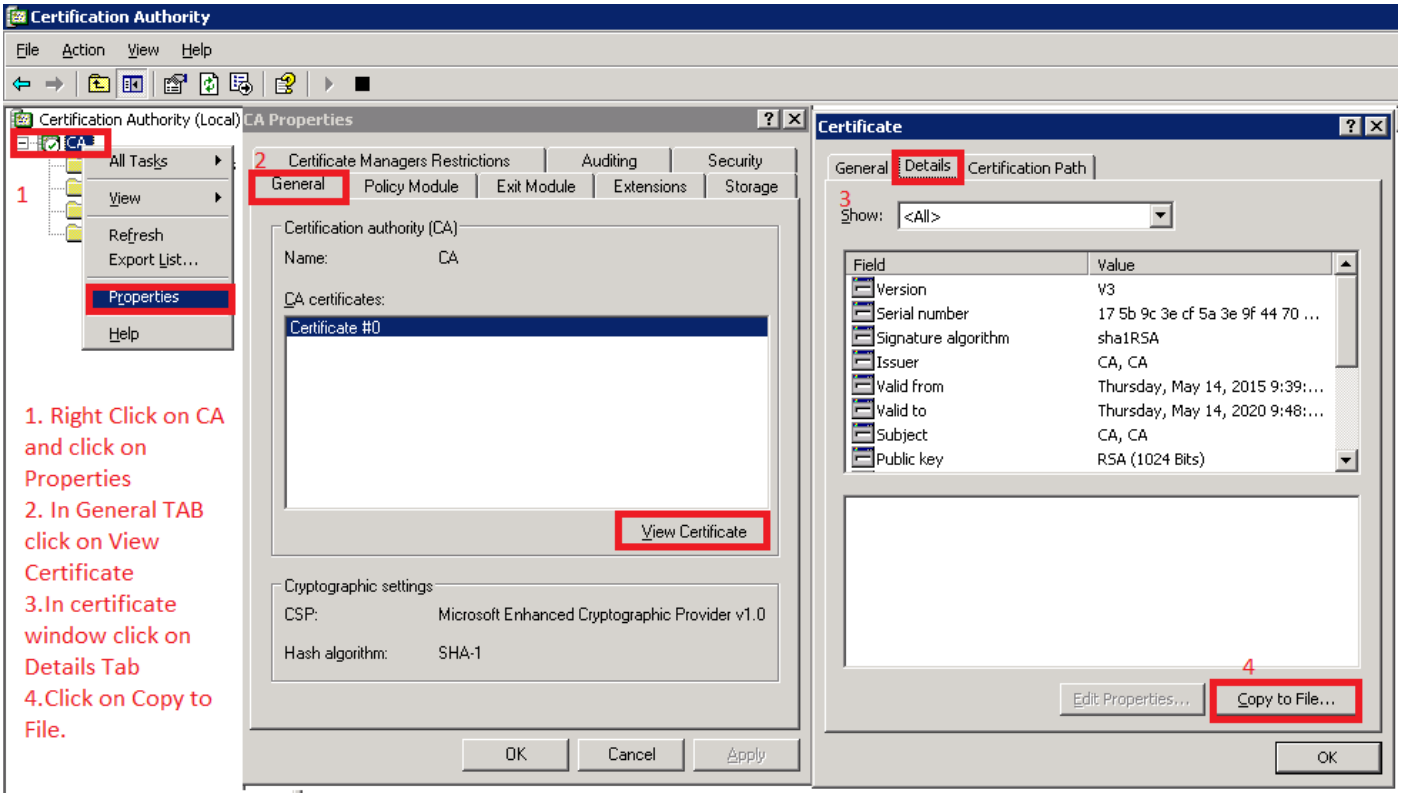


8. 파일의 이름을 정확하게 지정합니다. 이 예에서는 CUCM1052.cer 형식을 사용합니다



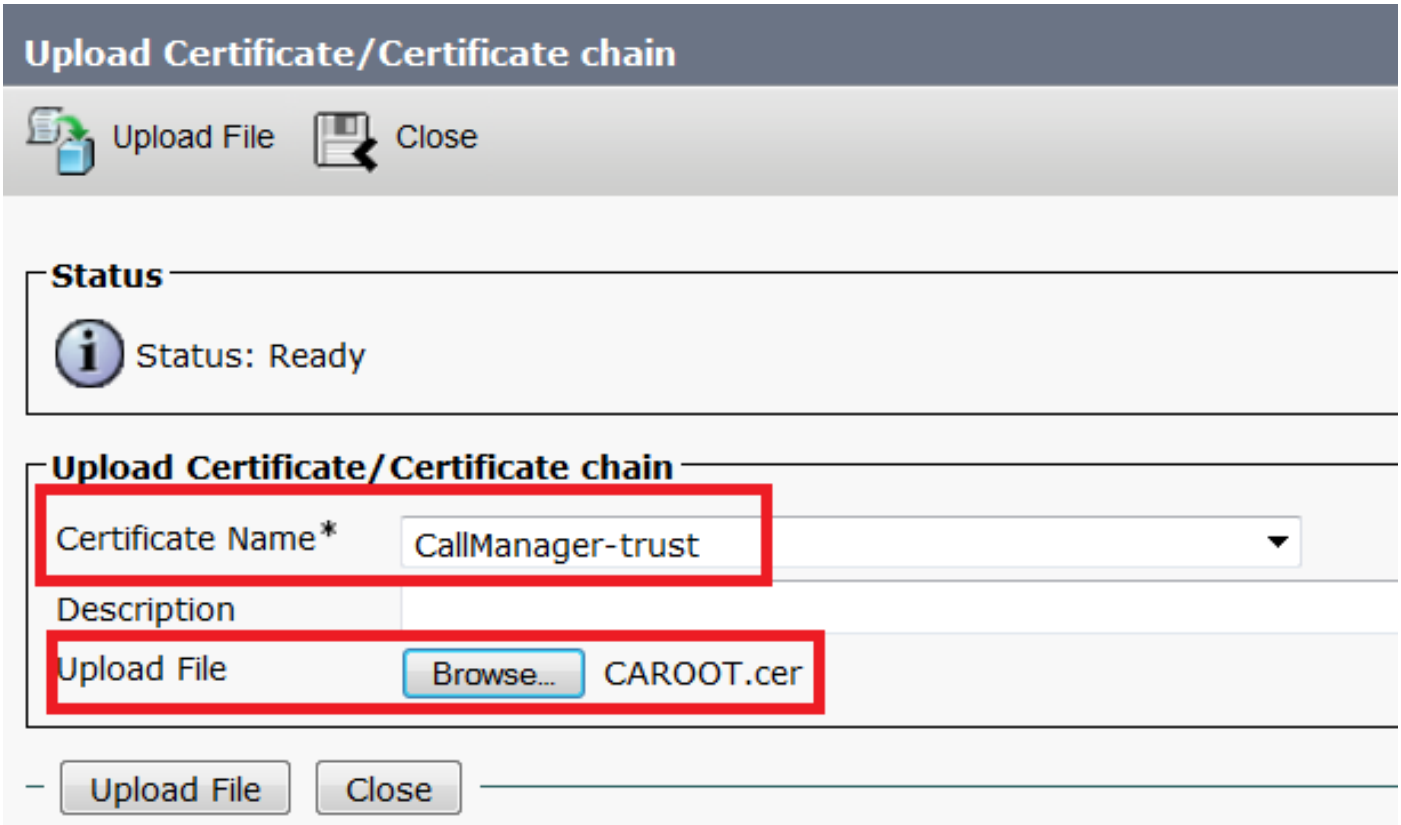
. CUCM 9.1(2)의 경우 동일한 절차를 수행합니다.5단계. CA에서 루트 인증서를 가져옵니다.인증 기관 창을 엽니다. 루트 CA를 다운로드하려면1. CA 아이콘을 마우스 오른쪽 버튼으로 클릭하고 속성 옵션을 클릭합니다.2. 일반 TAB에서 인증서 보기를 클릭합니다.3. 인증서 창에서 상세내역 탭을 클릭합니다.4. 파일에 복사...를 클릭합니다

.



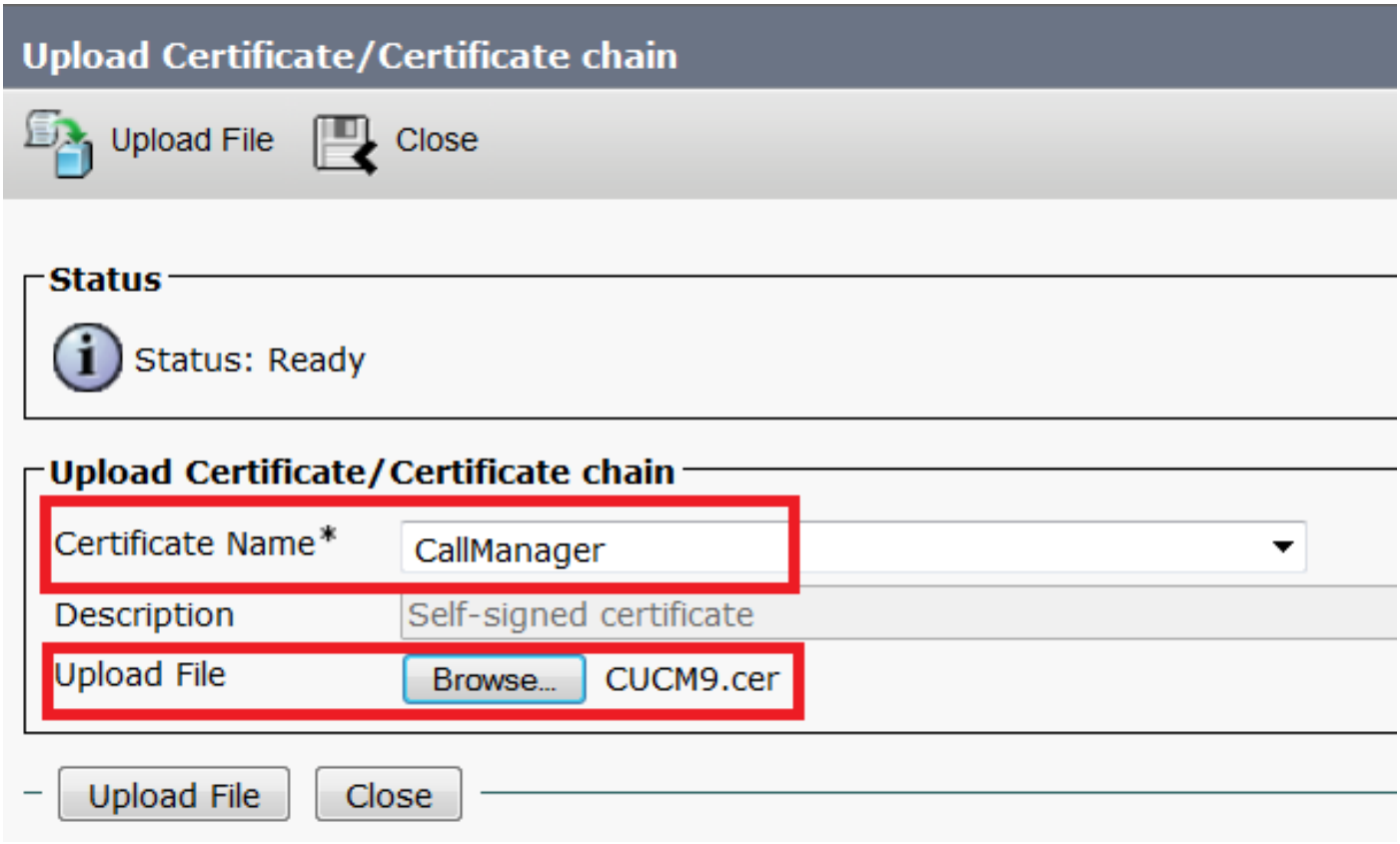
6단계. CA 루트 인증서를 CallManager 트러스트로 업로드CA 루트 인증서를 업로드하려면 OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain(OS 관리자 > 보안 > 인증서 관리 > 인증서/인증서 체인 업로드)에 로그인합니다

.



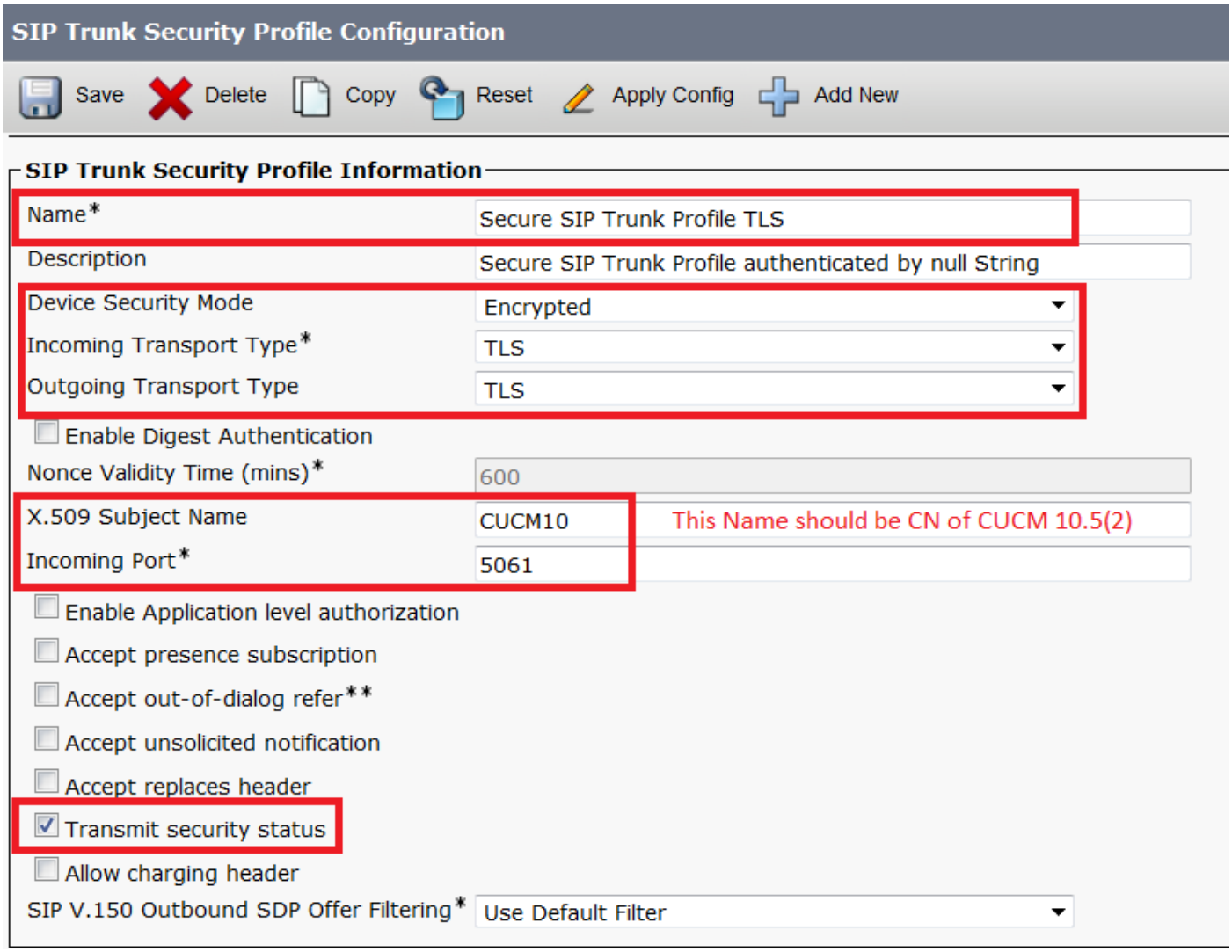
참고:CUCM(CUCM 9.1(2) 및 CUCM 10.5(2)에서 다음 단계를 수행합니다.7단계. CA 서명 CallManager CSR 인증서를 CallManager 인증서로 업로드합니다.CA 서명 CallManager CSR을 업로드하려면 OS Admin(OS 관리자) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드)에 로그인합니다

.



참고:CUCM(CUCM 9.1(2) 및 CUCM 10.5(2)에서 다음 단계를 수행합니다.8단계. SIP 트렁크 보안 프로파일 생성
CUCM 9.1(2)
SIP Trunk Security Profile(SIP 트렁크 보안 프로파일)을 생성하려면 System(시스템) > Security(보안) > SIP Trunk Security Profile(SIP 트렁크 보안 프로파일)로 이동합니다.기존의 비보안 SIP 트렁크 프로필을 복사하고 새 이름을 지정합니다.이 예에서는 Non Secure SIP Trunk Profile(비보안 SIP 트렁크 프로파일)의 이름이 Secure SIP Trunk Profile TLS로 변경되었습니다

.



X.509 Subject Name에서 이 이미지에 표시된 대로 CUCM 10.5(2)(CA 서명 인증서)의 CN(Common Name)을 사용합니다

.

Certificate Settings

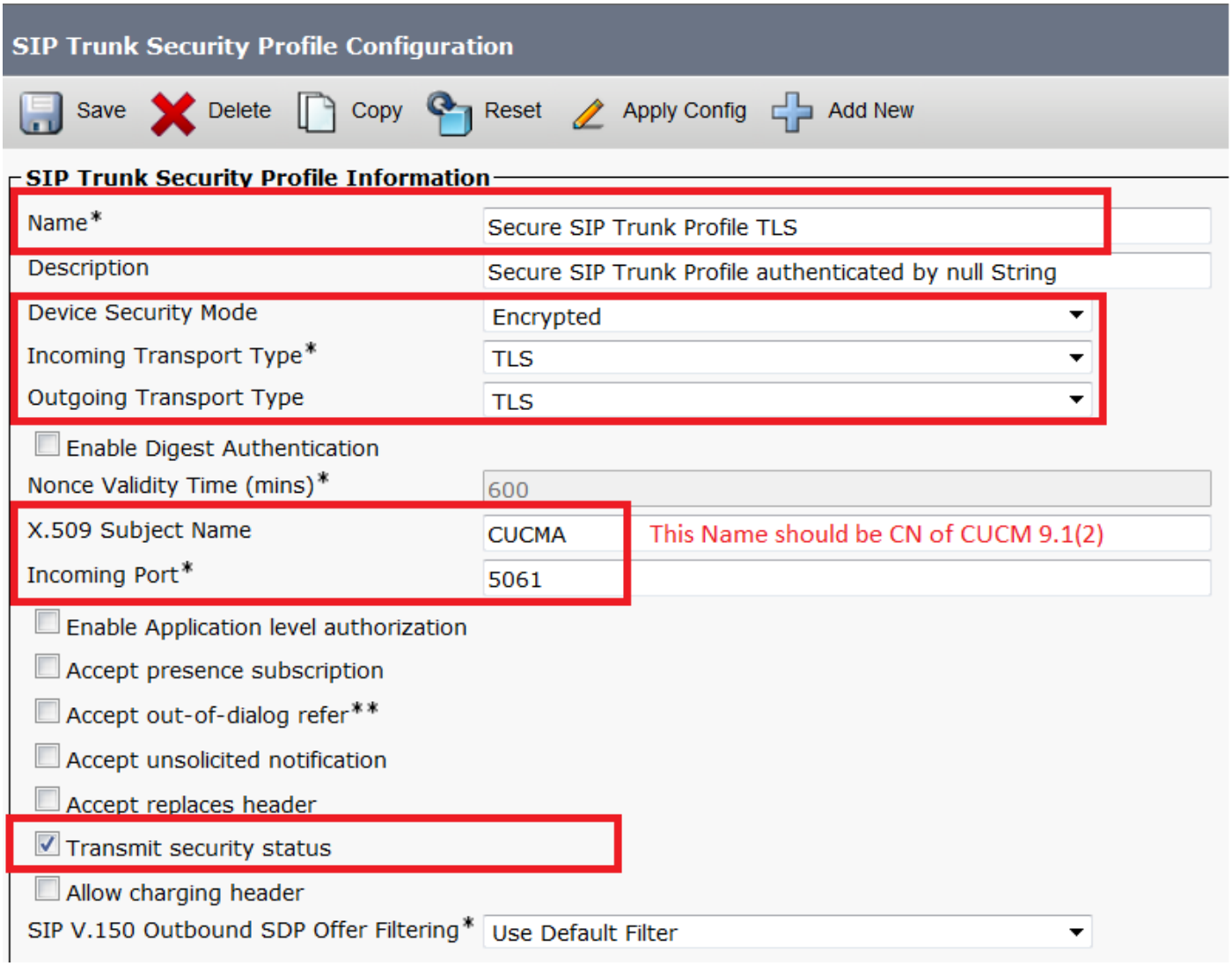
Locally Uploaded	23/05/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by CA

Certificate File Data

```
[
  Version: V3
  Serial Number: 398B1DA600000000000E
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=CA, DC=CA
  Validity From: Sat May 23 17:50:42 IST 2015
         To:   Mon May 23 18:00:42 IST 2016
  Subject Name: CN=CUCM10, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
30818902818100bcf093aa206190fe76abe13e3bd3ec45cc8b2afeee86e8393f568e1c9aa0c5fdf3f044eebc
f2d999ed8ac3592220fef3f9dcf2d2e7e939a4b26896152ebb250e407cb65d9e04bf71e8c345633786041e
5c806405160ac42a7133d7d644294226b850810fffd001e5bf2b39829b1fb27f126624e5011f151f0ef07c7
eccb734710203010001
  Extensions: 6 present
  [
```

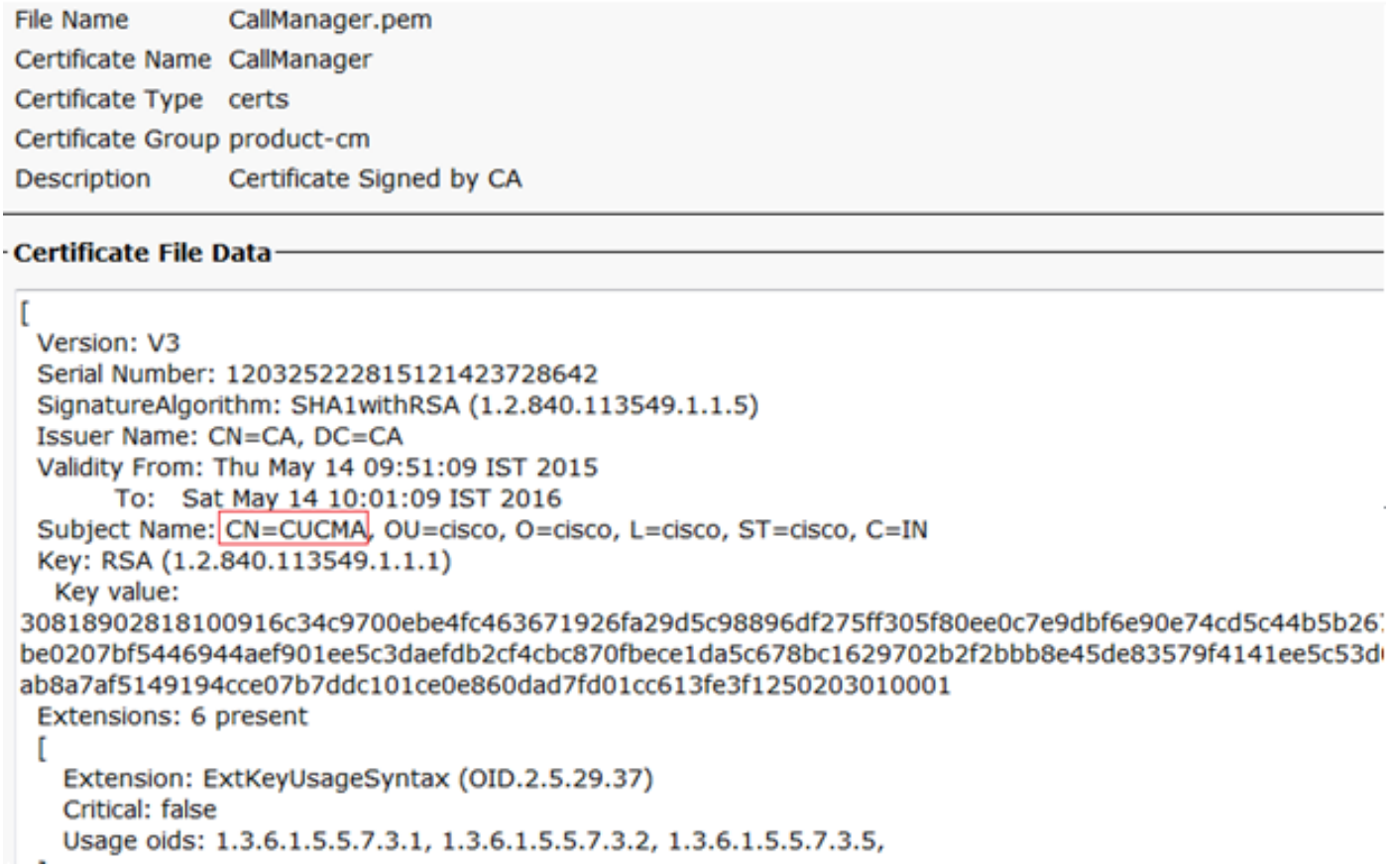
CUCM 10.5(2)System(시스템) > Security(보안) > SIP Trunk Security Profile(SIP 트렁크 보안 프로파일)으로 이동합니다.기존의 비보안 SIP 트렁크 프로필을 복사하고 새 이름을 지정합니다.이 예에서는 Non Secure SIP Trunk Profile(비보안 SIP 트렁크 프로파일)의 이름이 Secure SIP Trunk Profile TLS로 변경되었습니다

.



X.509 Subject Name(X.509 주체 이름에서 CUCM 9.1(2)(CA 서명 인증서)의 CN을 강조 표시합니다

.

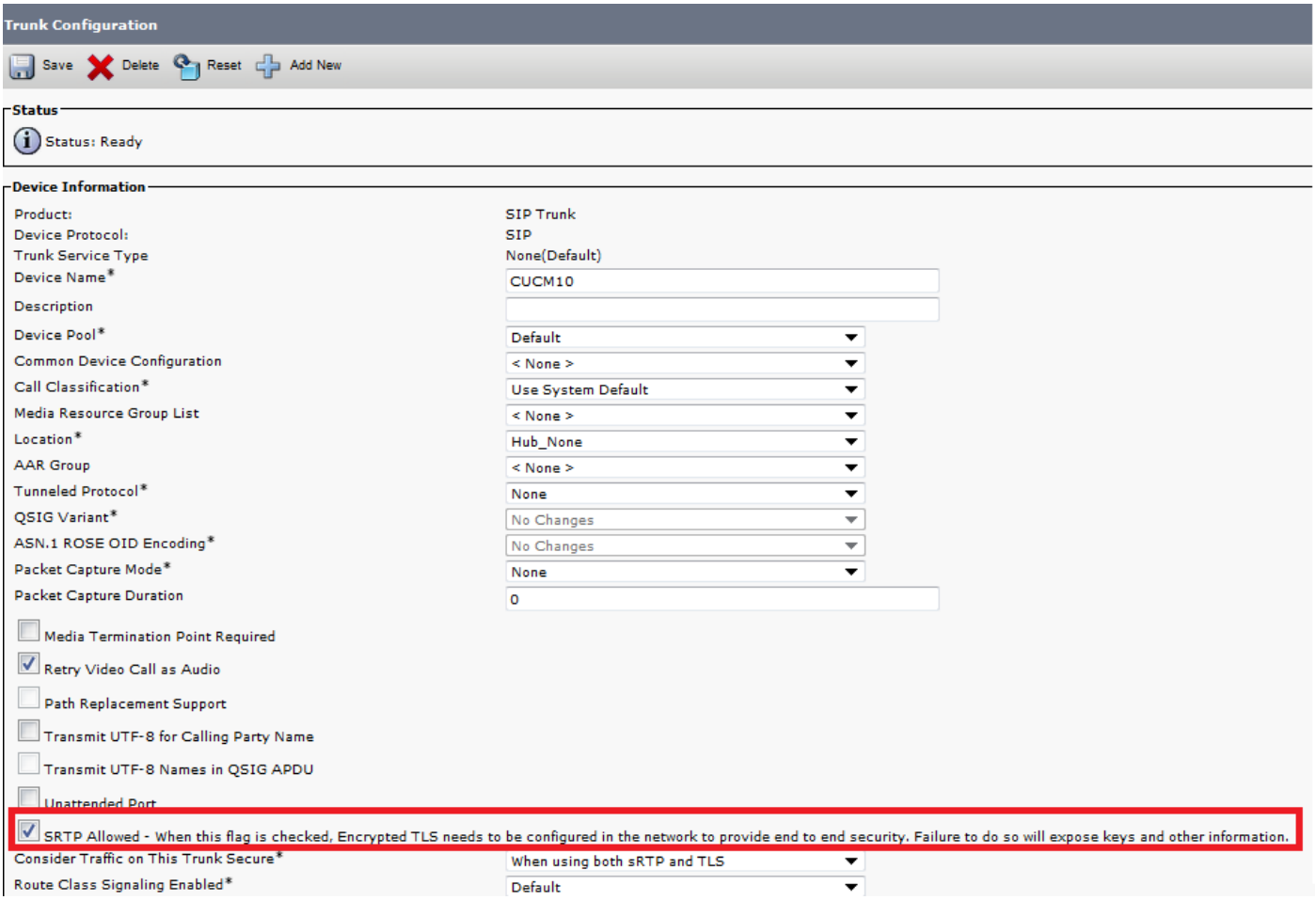


두 SIP Trunk Security Profiles(SIP 트렁크 보안 프로파일)는 모두 수신 포트 5061을 설정합니다. 이 포트 5061은 각 클러스터가 새로운 인바운드 SIP TLS 호출을 수신 대기합니다.9단계. SIP 트렁크 생성보안 프로필이 생성된 후 SIP 트렁크를 만들고 SIP 트렁크에서 아래 구성 매개변수를 변경합니다.CUCM 9.1(2)

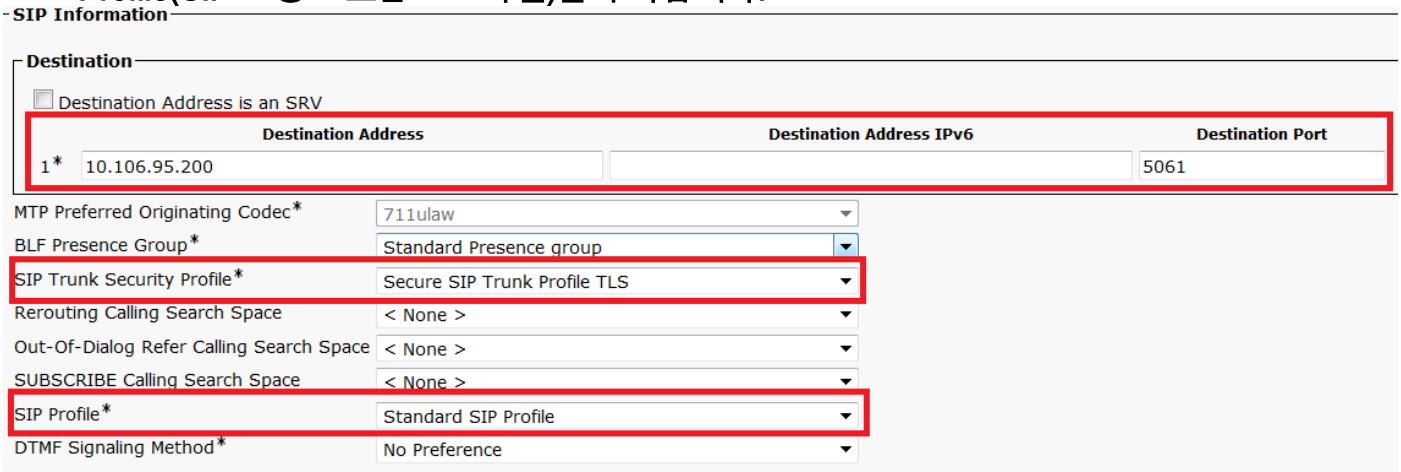
1. SIP Trunk Configuration(SIP 트렁크 컨피그레이션) 창에서 컨피그레이션 매개변수 SRTP Allowed(SRTP 허용) 확인란을 선택합니다.

이렇게 하면 이 트렁크를 통한 통화에 사용할 RTP(Real-time Transport Protocol)가 보호됩니다.SIP TLS를 사용하는 경우에만 이 확인란을 선택해야 합니다. SRTP(Secure Real-time Transport Protocol)의 키가 SIP 메시지 본문에서 교환되기 때문입니다.SIP 신호 처리는 TLS를 통해 보호되어야 합니다. 그렇지 않으면 비보안 SIP 신호 처리가 있는 모든 사용자가 트렁크를 통해 해당 SRTP 스트림을 해독할 수 있습니다

.



2. SIP Trunk Configuration(SIP 트렁크 컨피그레이션) 창의 SIP Information(SIP 정보) 섹션에서 Destination Address(대상 주소), Destination Port(대상 포트) 및 SIP Trunk Security Profile(SIP 트렁크 보안 프로파일)을 추가합니다.

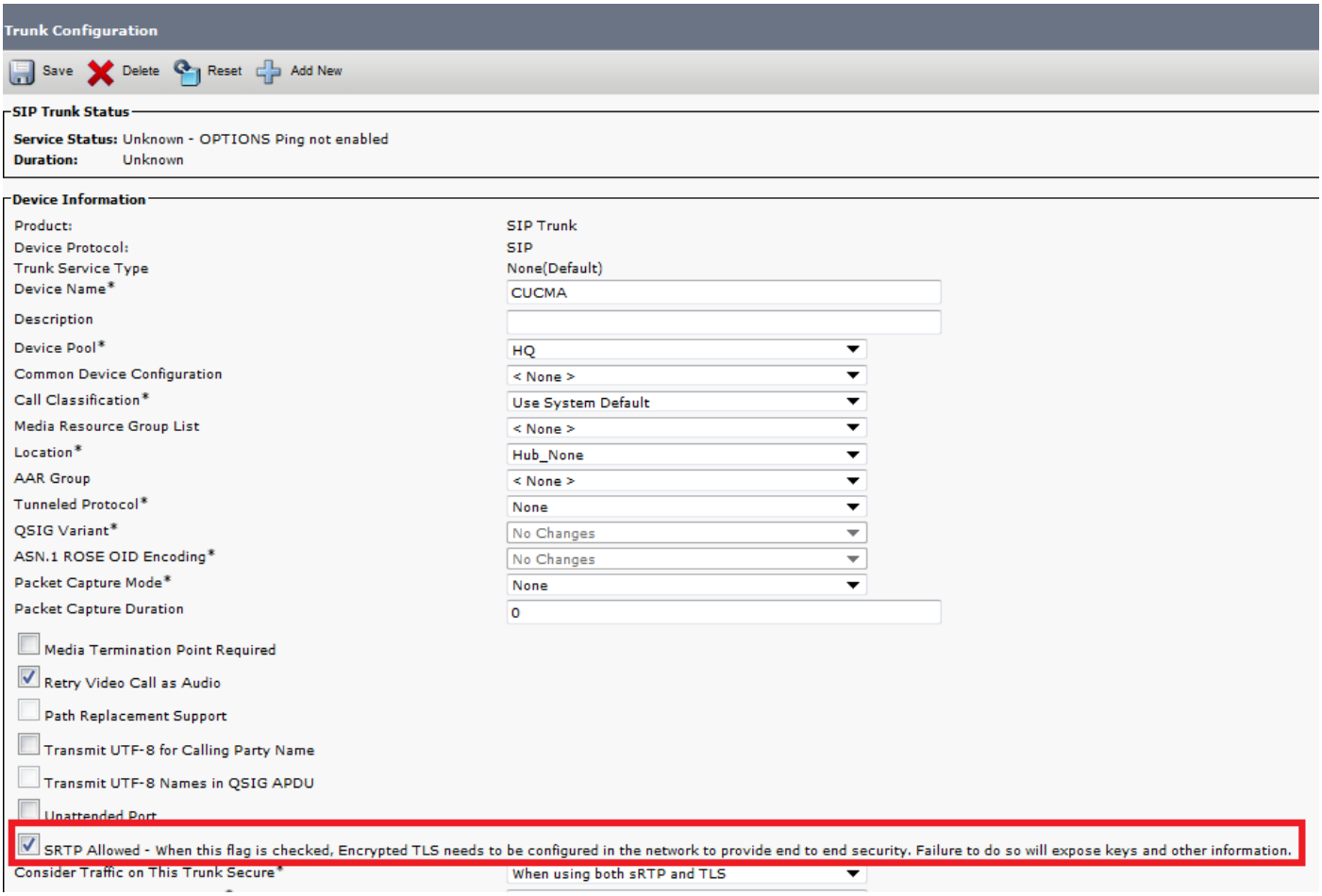


CUCM 10.5(2)

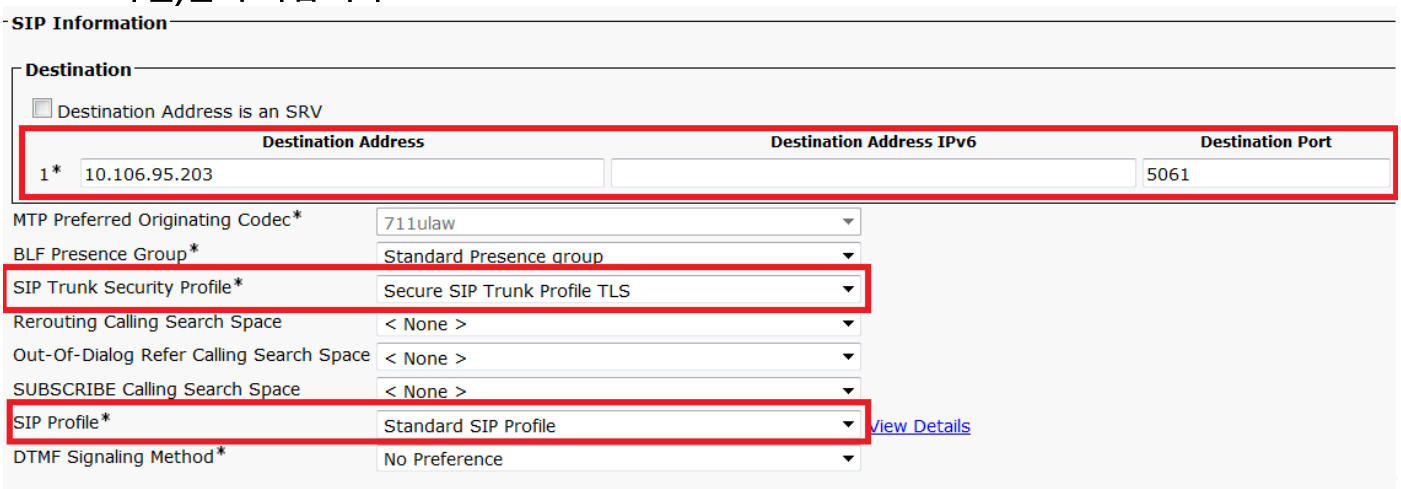
1. SIP Trunk Configuration(SIP 트렁크 컨피그레이션) 창에서 컨피그레이션 매개변수 SRTP Allowed(SRTP 허용) 확인란을 선택합니다.

이렇게 하면 SRTP를 이 트렁크를 통한 통화에 사용할 수 있습니다.SIP TLS를 사용하는 경우에만 이 확인란을 선택해야 합니다. SRTP용 키가 SIP 메시지 본문에서 교환되기 때문입니다.비보안 SIP 신호 처리를 사용하는 모든 사용자가 트렁크를 통해 해당 Secure RTP 스트림을 해독할 수 있으므로 SIP 신호 처리는 TLS를 통해 보호되어야 합니다

.

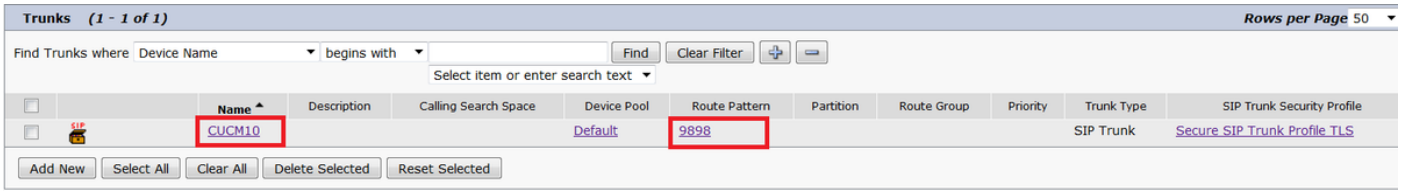


2. SIP Trunk Configuration(SIP 트렁크 컨피그레이션) 창의 SIP Information(SIP 정보) 섹션에서 Destination IP Address(대상 IP 주소), Destination Port(대상 포트) 및 Security Profile(보안 프로파일)을 추가합니다.



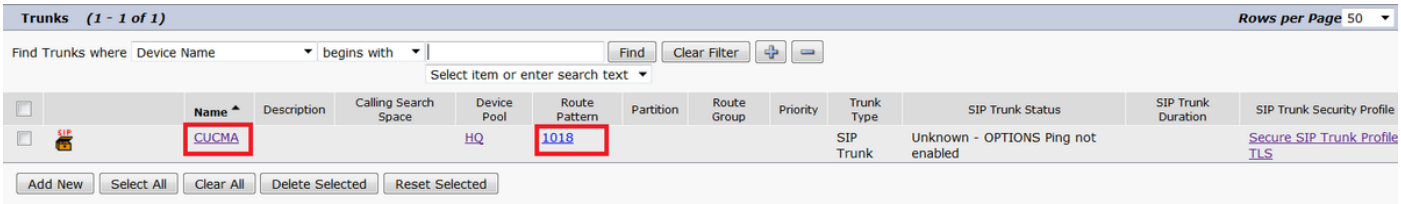
10단계. 경로 패턴 생성가장 간단한 방법은 SIP 트렁크를 직접 가리키는 각 클러스터에 경로 패턴을 생성하는 것입니다.경로 그룹 및 경로 목록도 사용할 수 있습니다.CUCM 9.1(2)은 TLS SIP 트렁크를 통해 CUCM 10.5(2)에 Route Pattern 9898을 가리킵니다

.



CUCM 10.5(2)는 TLS SIP 트렁크를 통해 CUCM 9.1(2)에 대한 Route Pattern 1018을 가리킵니다

.



다음을 확인합니다.현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.**문제 해결**SIP TLS 호출은 다음 단계를 통해 디버깅할 수 있습니다.CUCM에서 패킷 캡처 수집CUCM 9.1(2)과 CUCM 10.5(2) 간의 연결을 확인하려면 CUCM 서버에서 패킷 캡처를 수행하고 SIP TLS 트래픽을 확인합니다.SIP TLS 트래픽은 sip-tls로 표시된 TCP 포트 5061에서 전송됩니다.다음 예에서는 CUCM 9.1(2)에 설정된 SSH CLI 세션이 있습니다1. 화면의 CLI 패킷 캡처이 CLI는 SIP TLS 트래픽에 대한 출력을 화면에 인쇄합니다.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. 파일에 대한 CLI 캡처이 CLI는 호스트를 기반으로 패킷 캡처를 수행하고 패킷 이름의 파일을 생성합니다.

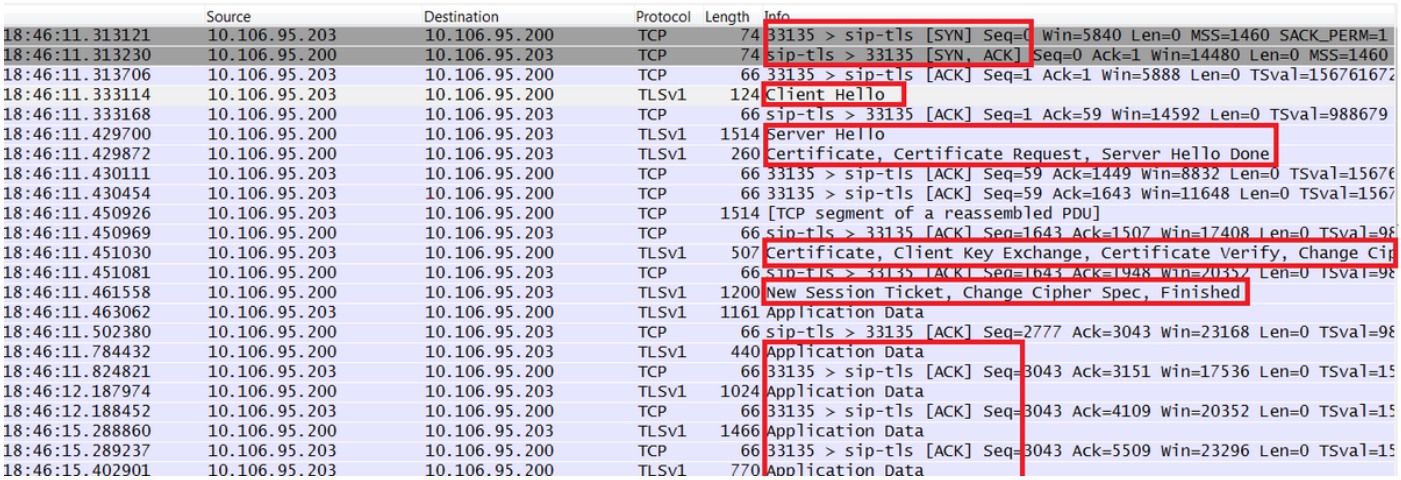
```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

CUCM 9.1(2)에서 SIP 트렁크를 다시 시작하고 내선 번호 1018(CUCM 9.1(2)에서 내선 번호 9898(CUCM 10.5(2)로 전화 걸기CLI에서 파일을 다운로드하려면 다음 명령을 실행합니다.

```
admin:file get activelog platform/cli/packets.cap
```

캡처는 표준 .cap 형식으로 수행됩니다.이 예에서는 Wireshark를 사용하여 packets.cap 파일을 열지만 패킷 캡처 표시 도구를 사용할 수 있습니다

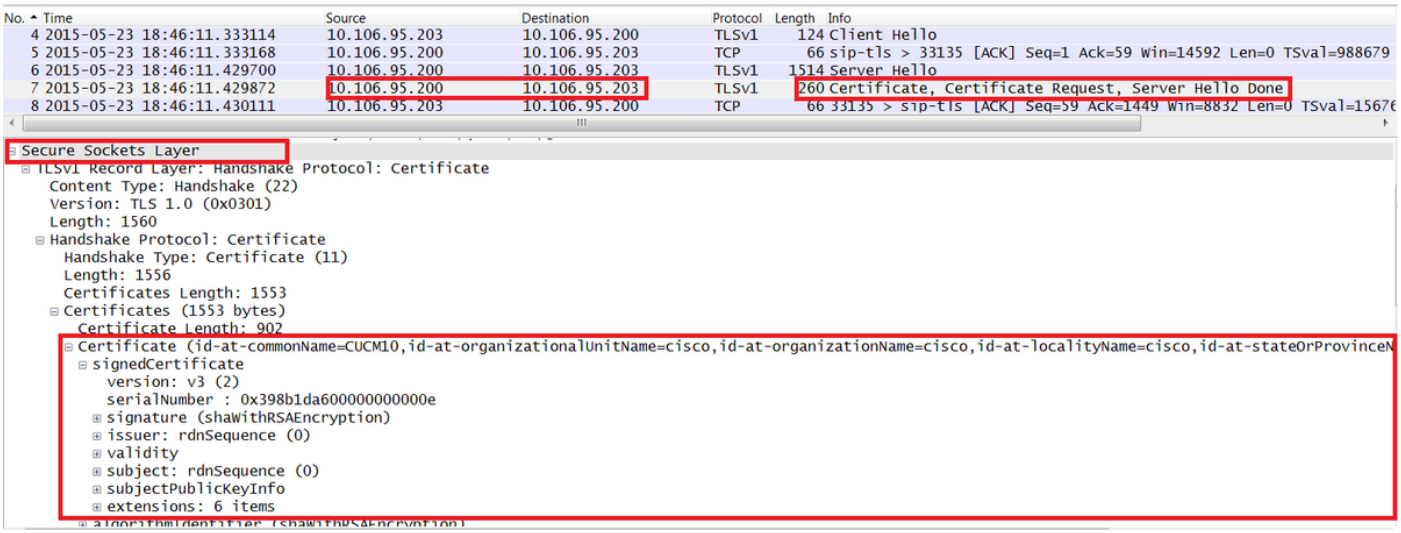
.



1. TCP(Transmission Control Protocol) Synchronize(SYN)는 CUCM 9.1(2)(클라이언트)과 CUCM 10.5(2)(서버) 간의 TCP 통신을 설정합니다.
2. CUCM 9.1(2)은 Client Hello를 전송하여 TLS 세션을 시작합니다.
3. CUCM 10.5(2)는 Server Hello, Server Certificate 및 Certificate Request를 보내 인증서 교환 프로세스를 시작합니다.
4. 클라이언트 CUCM 9.1(2)이 인증서 교환을 완료하기 위해 전송하는 인증서.
5. 암호화된 SIP 신호 처리 애플리케이션 데이터는 TLS 세션이 설정되었음을 보여줍니다.

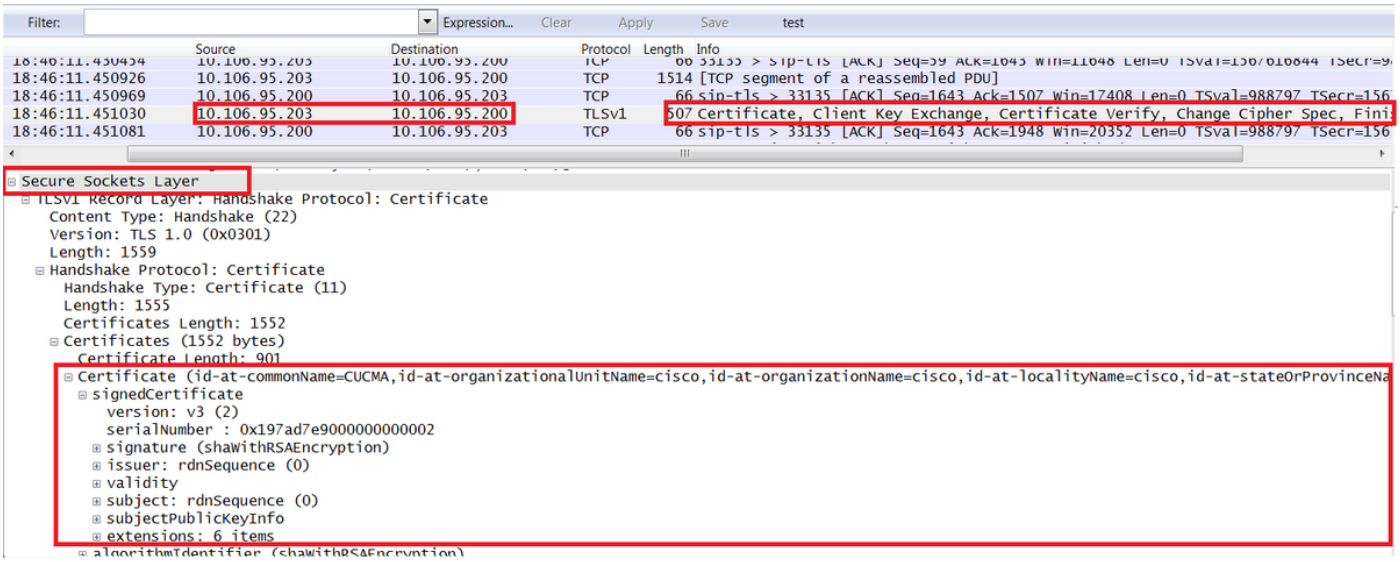
올바른 인증서가 교환되었는지 추가 확인Server Hello 이후 서버 CUCM 10.5(2)는 클라이언트 CUCM 9.1(2)에 인증서를 전송합니다

.



서버 CUCM 10.5(2)에 있는 일련 번호 및 제목 정보는 클라이언트 CUCM 9.1(2)에 표시됩니다.일련 번호, 주체, 발급자 및 유효 일자는 모두 OS 관리 인증서 관리 페이지의 정보와 비교됩니다.서버 CUCM 10.5(2)는 확인을 위해 자체 인증서를 제공하며, 이제 클라이언트 CUCM 9.1(2)의 인증서를 확인합니다. 확인은 양방향으로 수행됩니다

.



패킷 캡처의 인증서와 OS 관리 웹 페이지의 인증서가 일치하지 않으면 올바른 인증서가 업로드되지 않습니다.올바른 인증서를 OS Admin Cert 페이지에 업로드해야 합니다.CUCM 추적 수집CUCM 추적은 CUCM 9.1(2)과 CUCM 10.5(2) 서버 간에 교환되는 메시지와 SSL 세션이 제대로 설정되었는지 여부를 확인하는 데에도 도움이 될 수 있습니다.이 예에서는 CUCM 9.1(2)의 추적이 수집되었습니다.통화 흐름:내선 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > 내선 9898++ 숫자 분석

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ SIP TLS는 이 통화에 대해 포트 5061에서 사용되고 있습니다.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
```

```
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

++ SDL(Signal Distribution Layer) 메시지 SIPCertificateInd는 주체 CN 및 연결 정보에 대한 세부 정보를 제공합니다.

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                      |wait
                  |SIPHandler(1,100,72,1)           |SIPTcp(1,100,64,1)
|1,100,17,11.3^*^*                        |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)           |1,100,17,11.3^*^*                        |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```