

CA 서명 인증서를 사용하여 Communications Manager에서 SIP TLS 트렁크 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. Windows Server 2003에서 공용 CA 또는 CA 설정](#)

[2단계. 호스트 이름 및 설정 확인](#)

[3단계. CSR\(Certificate Signing Request\) 생성 및 다운로드](#)

[4단계. Microsoft Windows 2003 인증 기관으로 CSR에 서명](#)

[5단계. CA에서 루트 인증서를 가져옵니다.](#)

[6단계. CA 루트 인증서를 CallManager 트러스트로 업로드](#)

[7단계. CA 서명 CallManager CSR 인증서를 CallManager 인증서로 업로드합니다.](#)

[8단계. SIP 트렁크 보안 프로파일 생성](#)

[9단계. SIP 트렁크 생성](#)

[10단계. 경로 패턴 생성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[CUCM에서 패킷 캡처 수집](#)

[CUCM 추적 수집](#)

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

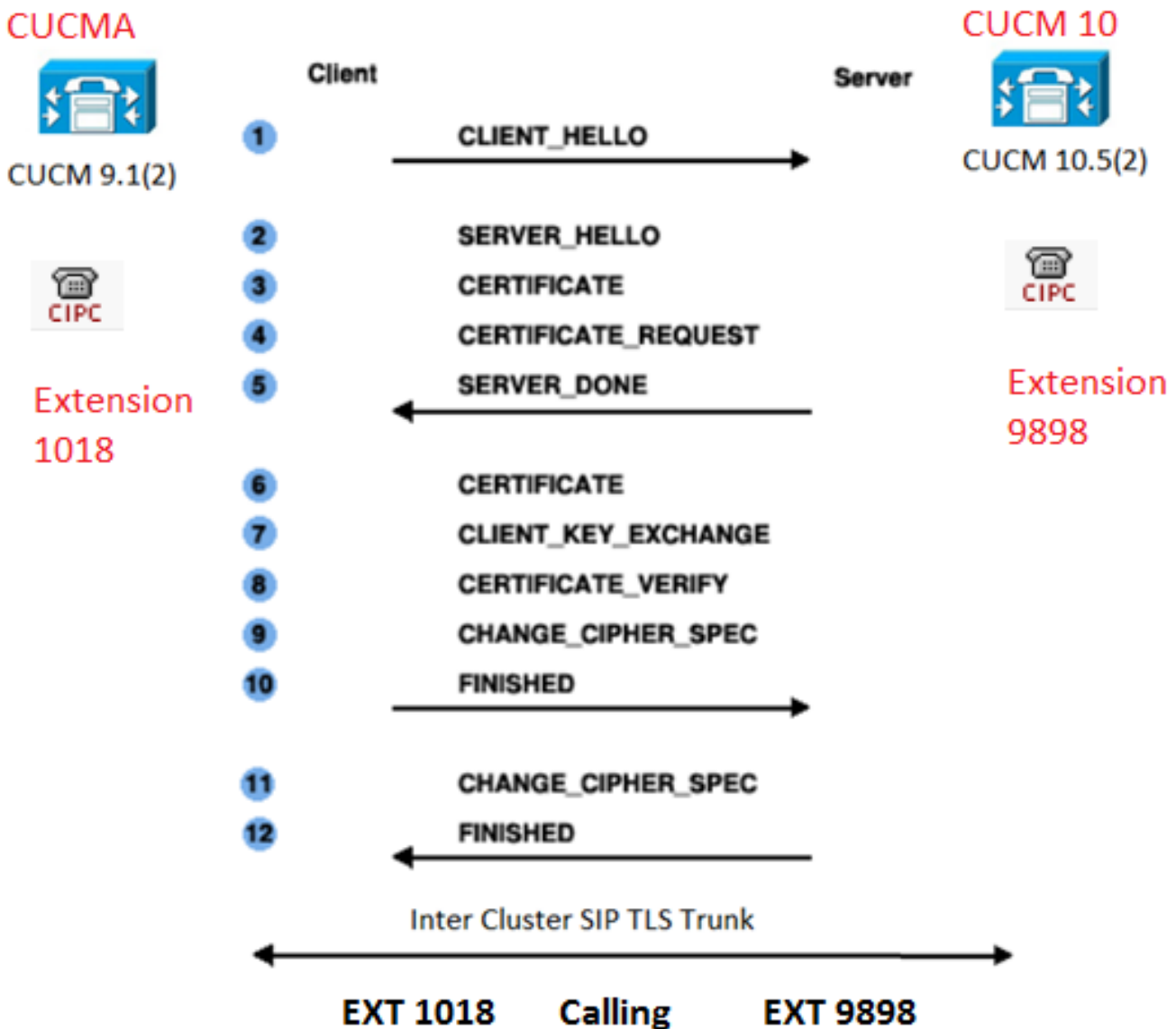
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- 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 필드의 드롭다운 목록에서 CallManager 옵션을 선택합니다.

The screenshot shows the 'Generate Certificate Signing Request' dialog box. At the top, there are buttons for 'Generate CSR' and 'Close'. Below this is a 'Status' section with a warning icon and the text: 'Warning: Generating a new CSR will overwrite the existing CSR'. The main section is titled 'Generate Certificate Signing Request' and contains a 'Certificate Name*' dropdown menu with 'CallManager' selected. At the bottom, there are buttons for 'Generate CSR' and 'Close'. The 'Generate CSR' button is highlighted with a red box.


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.

Download Certificate Signing Request

Download CSR Close

Status

 Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Name* CallManager

Download CSR Close

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.

Generate Certificate Signing Request

Generate Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* CallManager

Distribution* CUCM10

Common Name* CUCM10

Subject Alternate Names (SANs)

Parent Domain

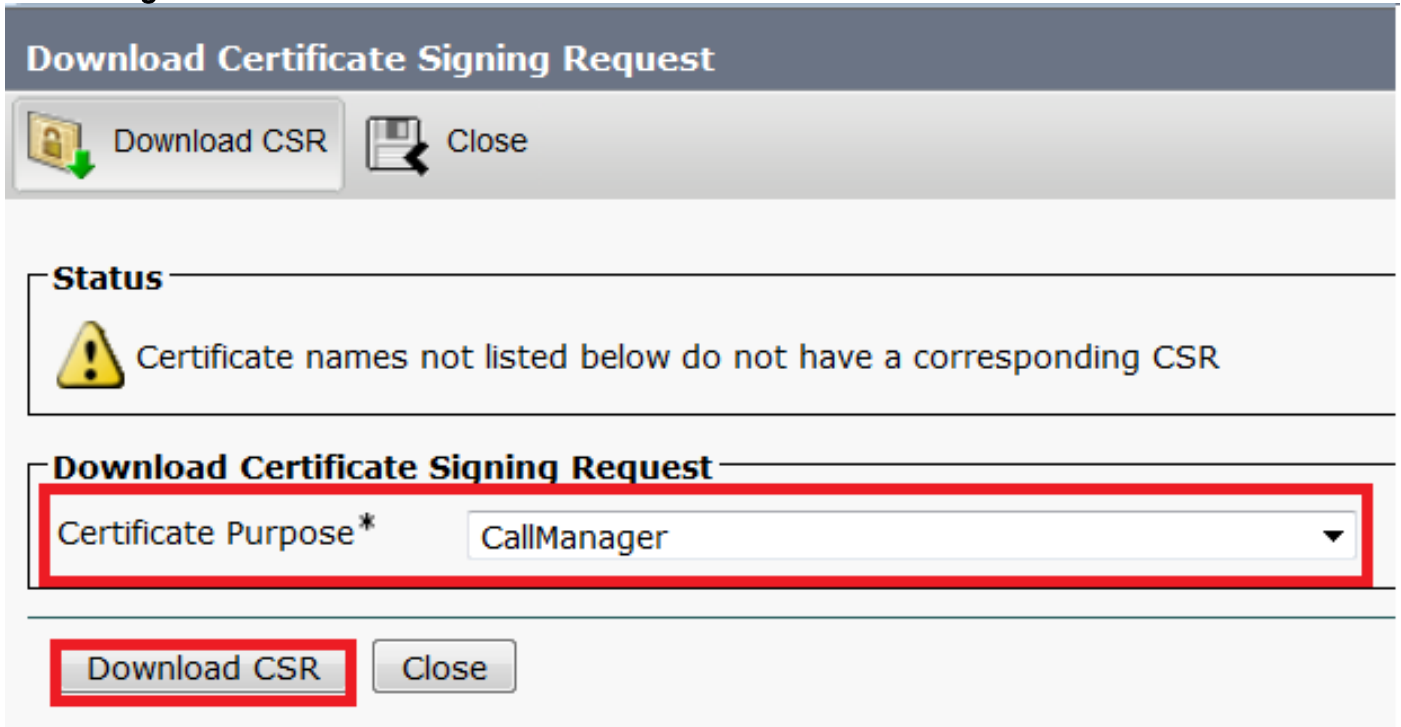
Key Length* 1024

Hash Algorithm* SHA1

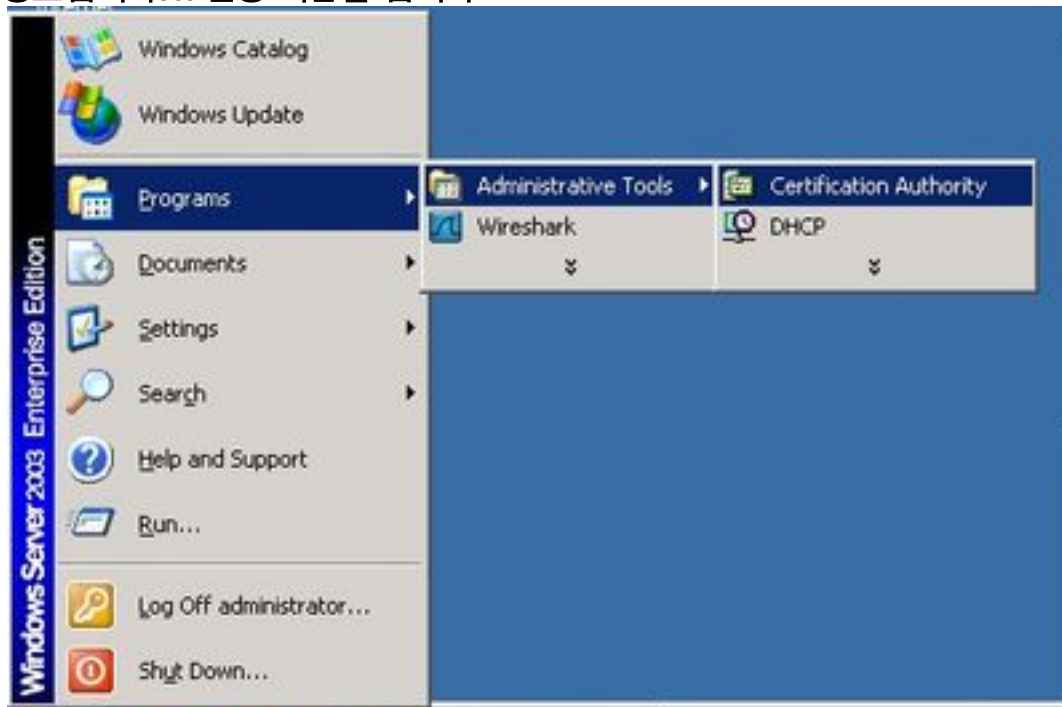
Generate Close

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

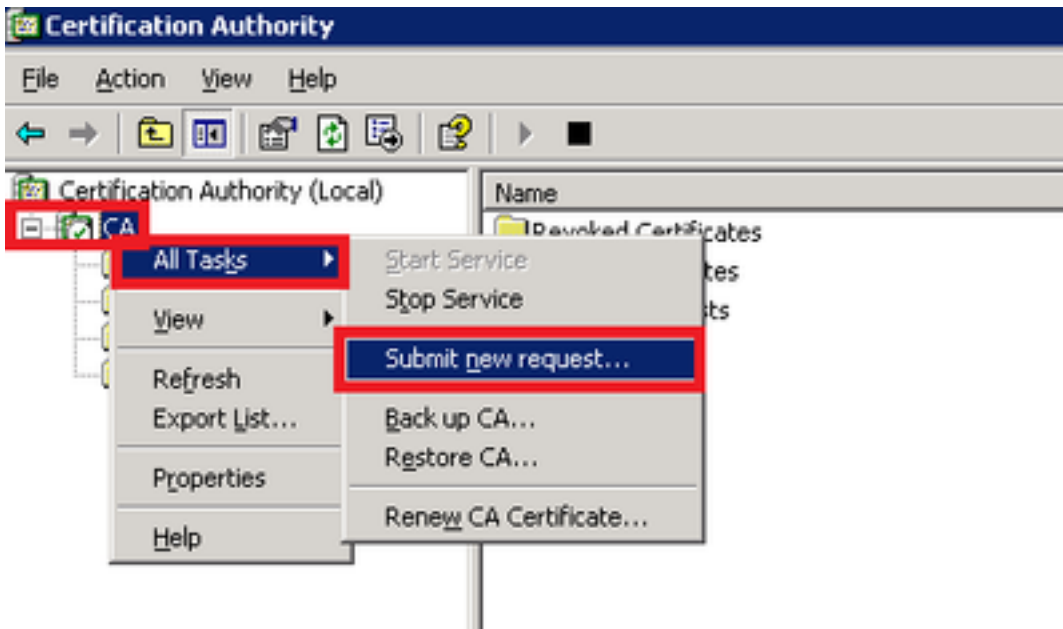
CallManager 옵션을 선택합니다.



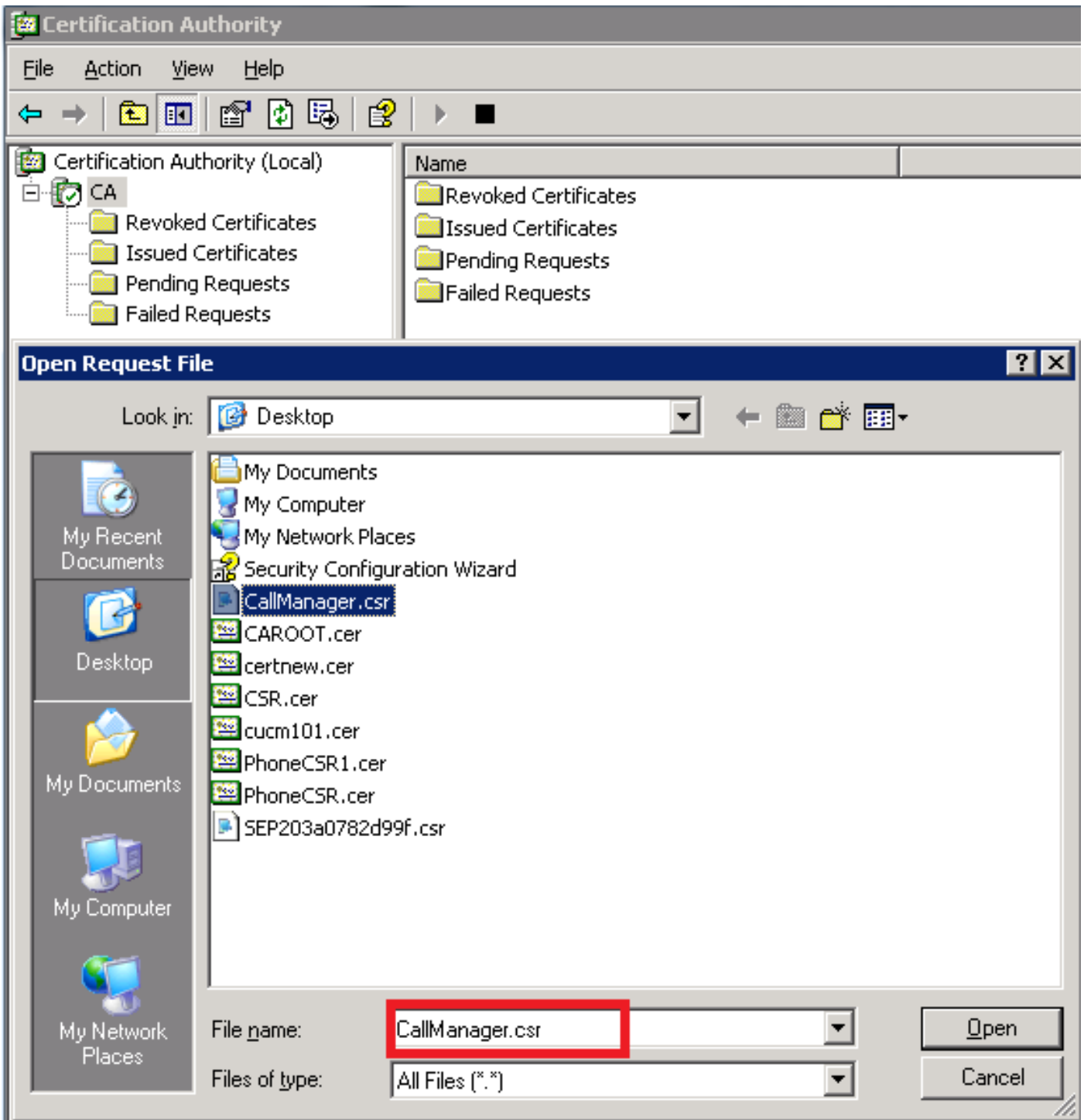
참고: CallManager CSR은 1024비트 RSA(Rivest-Shamir-Addleman) 키와 함께 생성됩니다. 4단계.
Microsoft Windows 2003 인증 기관으로 CSR에 서명이 정보는 Microsoft Windows 2003 CA로 CSR에 서명하는 선택적 정보입니다. 1. 인증 기관을 엽니다



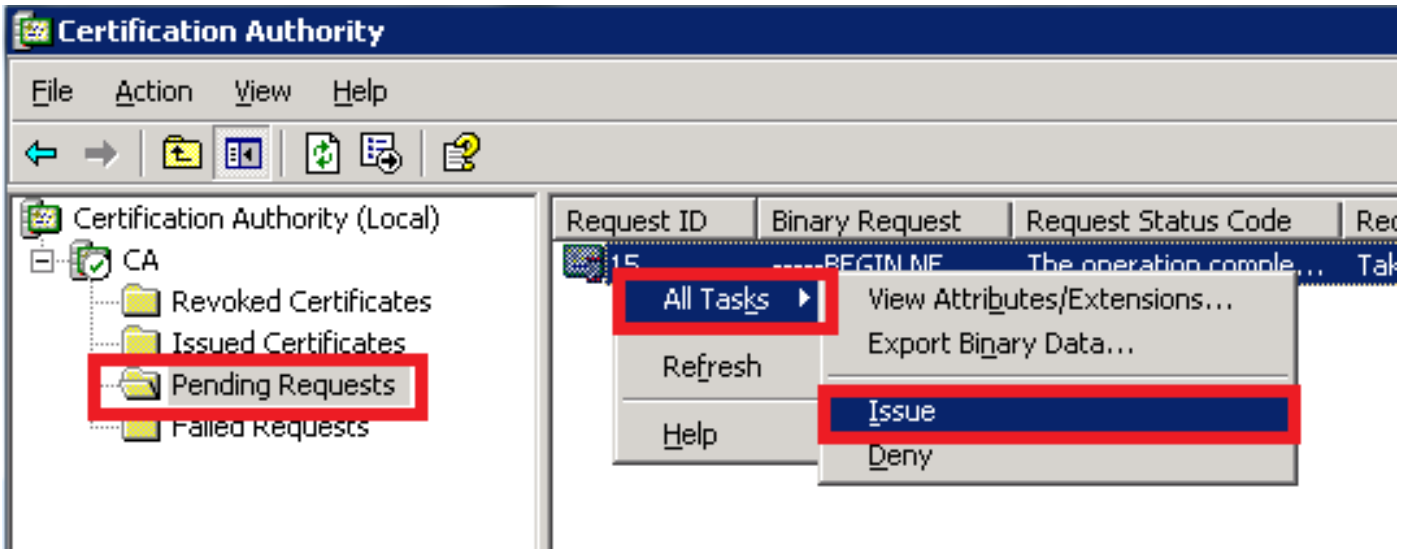
2. CA 아이콘을 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Submit new request(새 요청 제출)로 이동합니다



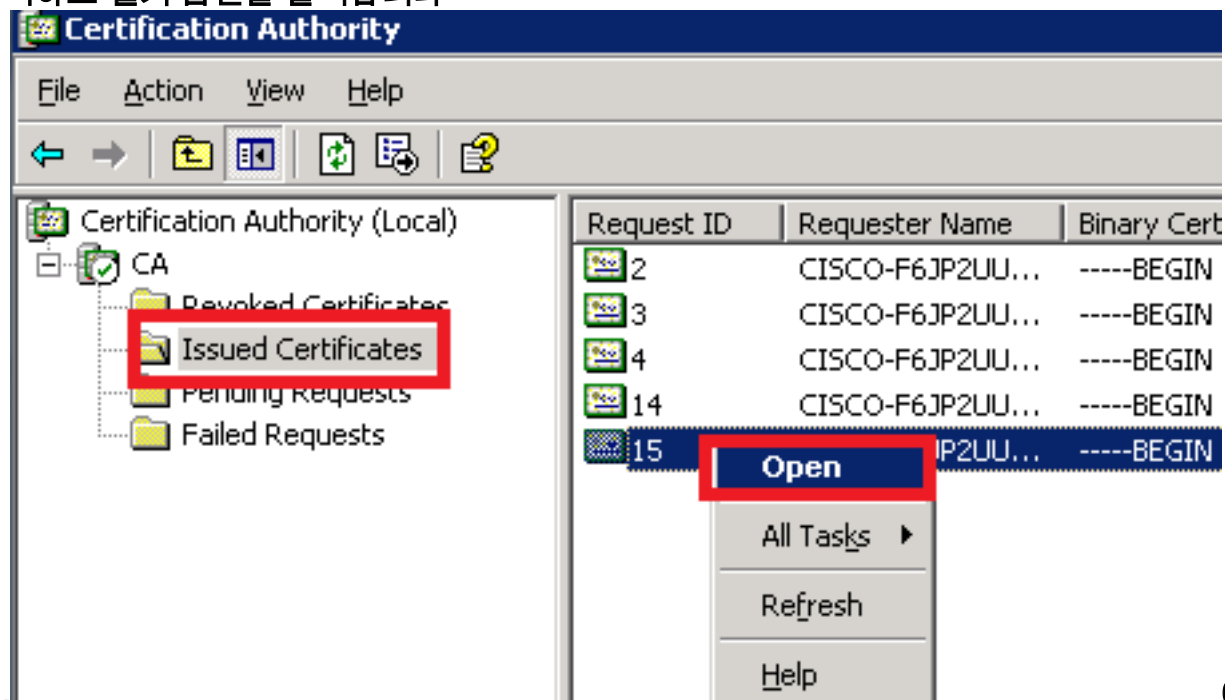
다. 3. CSR을 선택하고 열기 옵션을 클릭합니다(CSR(CUCM 9.1(2) 및 CUCM 10.5(2)에서 모두 적용 가능).



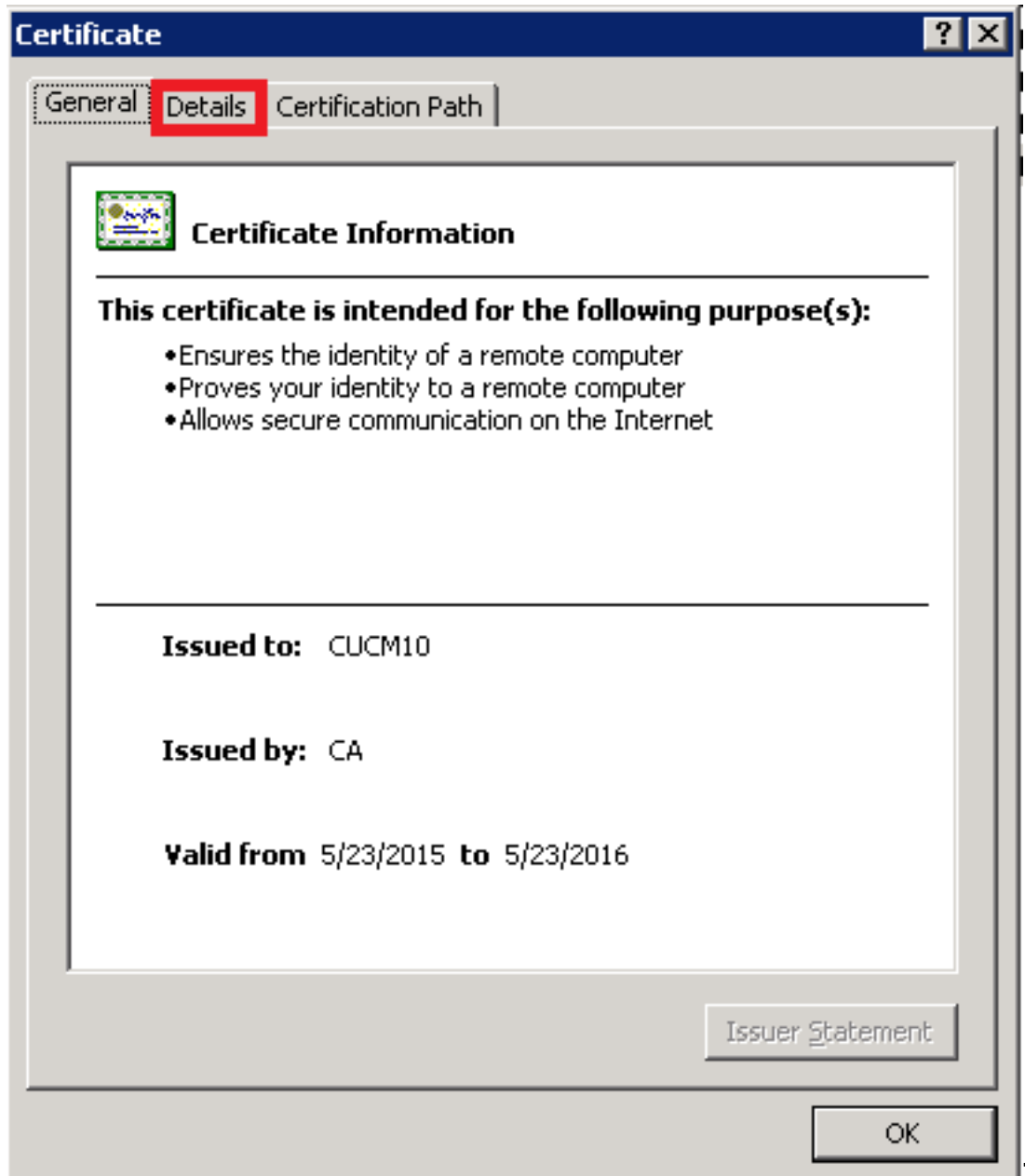
4. 열린 모든 CSR이 대기 중인 요청 폴더에 표시됩니다. 각 CSR을 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Issue(문제)로 이동하여 인증서를 발급합니다.(CSR(CUCM 9.1(2) 및 CUCM 10.5(2)에 모두 적용)



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



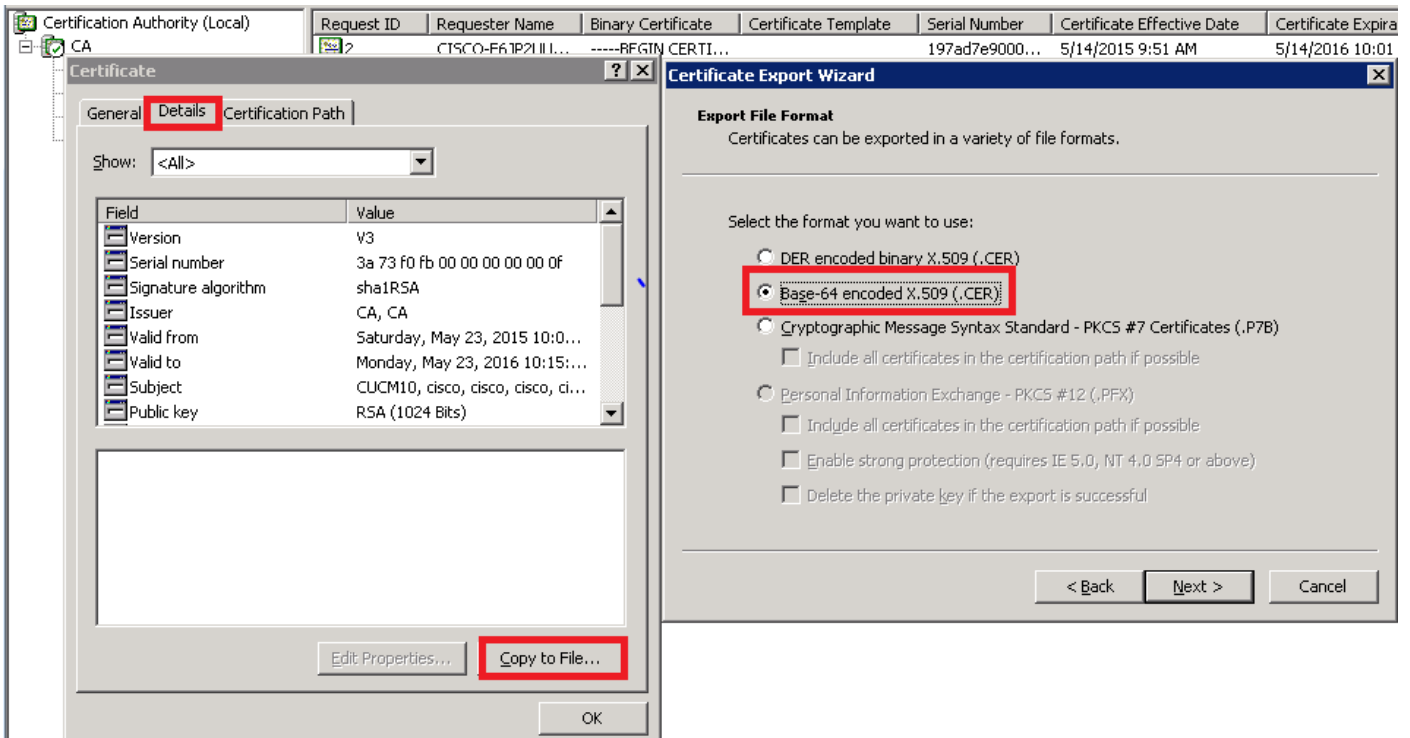
6. 인증서 세부사항이 표시됩니다. 인증서를 다운로드하려면 Details 탭을 선택하고 Copy to File(파일에 복사...)



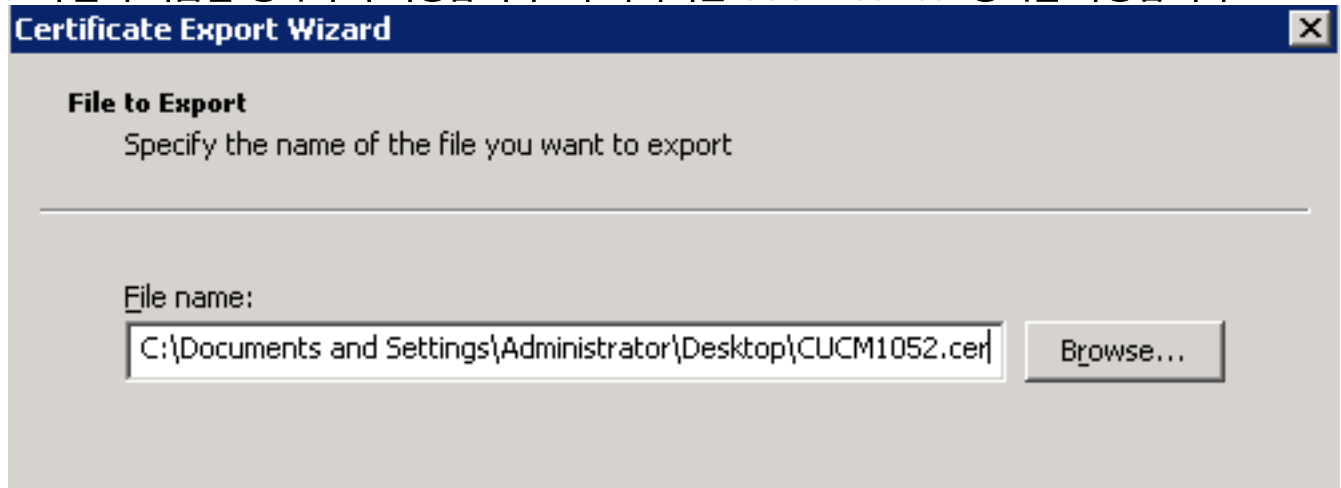
버튼을 클릭합니다.

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

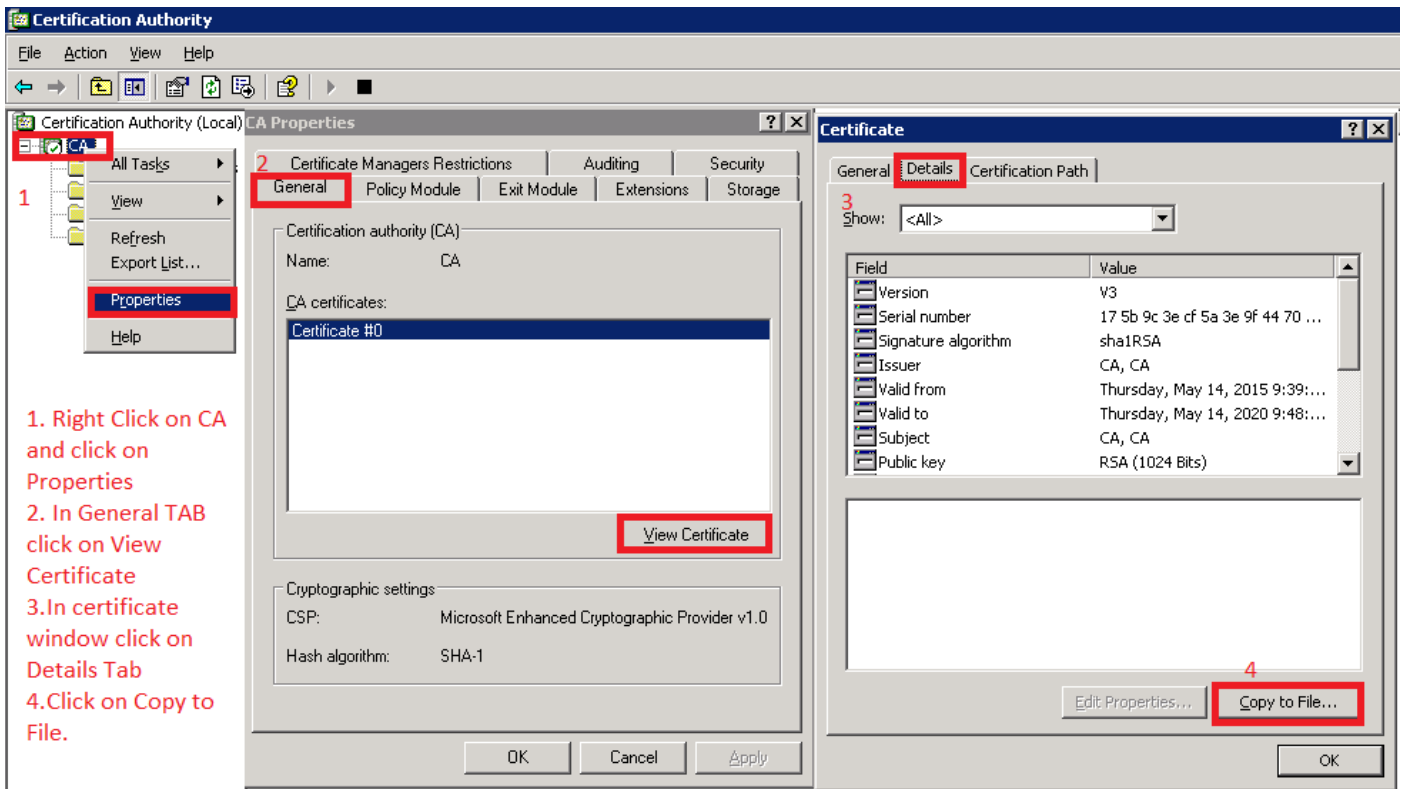
7.



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

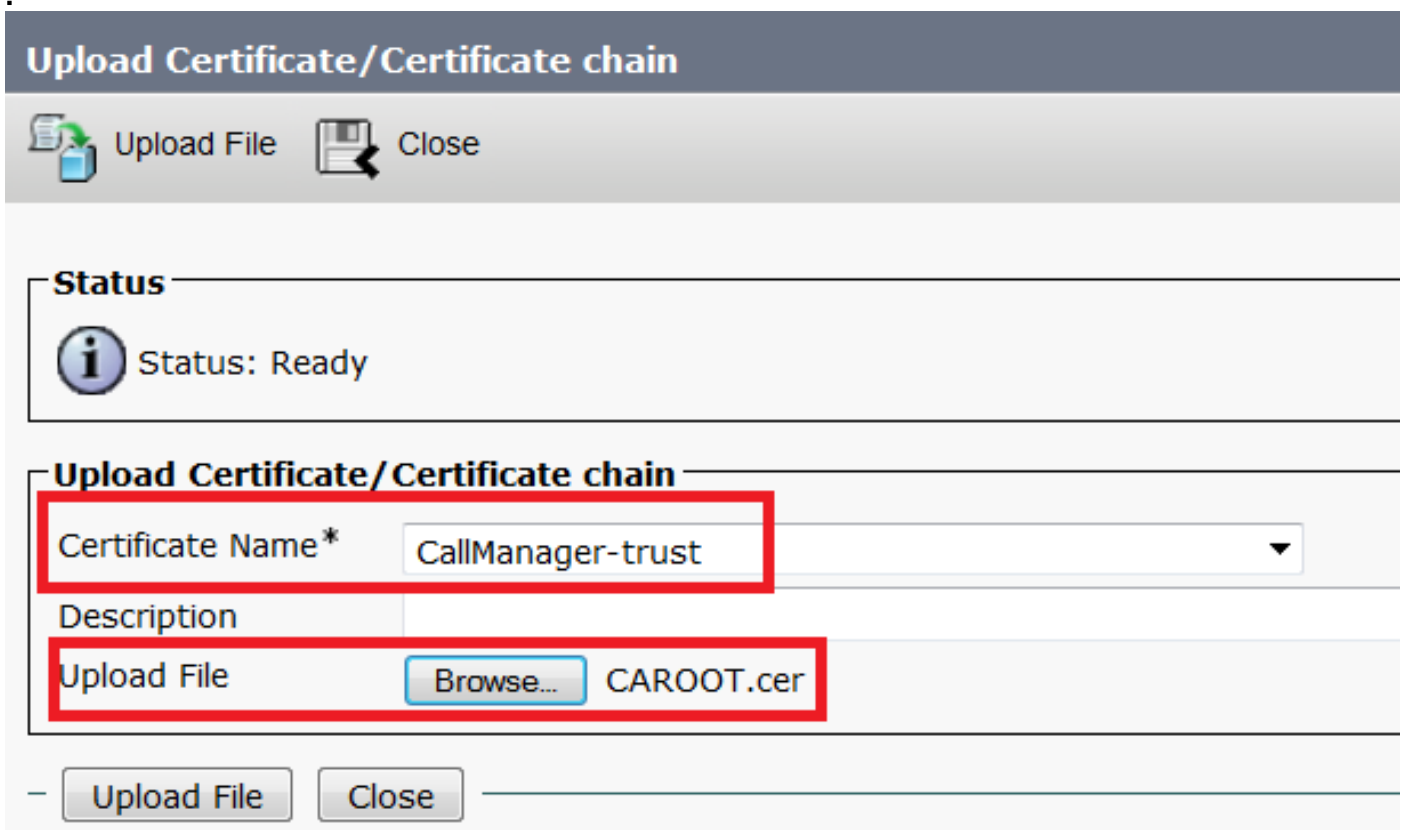


CM 9.1(2)의 경우 동일한 절차를 수행합니다.5단계. CA에서 루트 인증서를 가져옵니다. 인증 기관 창을 엽니다. 루트 CA를 다운로드하려면1. CA 아이콘을 마우스 오른쪽 버튼으로 클릭하고 속성 옵션을 클릭합니다.2. 일반 TAB에서 인증서 보기를 클릭합니다.3. 인증서 창에서 상세내역 탭을 클릭합니다.4. 파일에 복사...를 클릭합니다



1. Right Click on CA and click on Properties
2. In General TAB click on View Certificate
3. In certificate window click on Details Tab
4. Click on Copy to File.

6단계. CA 루트 인증서를 CallManager 트러스트로 업로드
 CA 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

Upload Certificate/Certificate chain



Upload File



Close

Status



Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

CallManager

Description

Self-signed certificate

Upload File

Browse...

CUCM9.cer

Upload File

Close

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

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS	
Description	Secure SIP Trunk Profile authenticated by null String	
Device Security Mode	Encrypted	▼
Incoming Transport Type*	TLS	▼
Outgoing Transport Type	TLS	▼
<input type="checkbox"/> Enable Digest Authentication		
Nonce Validity Time (mins)*	600	
X.509 Subject Name	CUCM10	This Name should be CN of CUCM 10.5(2)
Incoming Port*	5061	
<input type="checkbox"/> Enable Application level authorization		
<input type="checkbox"/> Accept presence subscription		
<input type="checkbox"/> Accept out-of-dialog refer**		
<input type="checkbox"/> Accept unsolicited notification		
<input type="checkbox"/> Accept replaces header		
<input checked="" type="checkbox"/> Transmit security status		
<input type="checkbox"/> Allow charging header		
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▼	

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

SIP Trunk Security Profile Configuration



Save



Delete



Copy



Reset



Apply Config



Add New

SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUCMA This Name should be CN of CUCM 9.1(2)
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

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

File Name CallManager.pem
Certificate Name CallManager
Certificate Type certs
Certificate Group product-cm
Description Certificate Signed by CA

Certificate File Data

```
[
Version: V3
Serial Number: 120325222815121423728642
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CA, DC=CA
Validity From: Thu May 14 09:51:09 IST 2015
To: Sat May 14 10:01:09 IST 2016
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100916c34c9700ebe4fc463671926fa29d5c98896df275ff305f80ee0c7e9dbf6e90e74cd5c44b5b26
be0207bf5446944aef901ee5c3daefdb2cf4cbc870f8ce1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d
ab8a7af5149194cce07b7ddc101ce0e860dad7fd01cc613fe3f1250203010001
Extensions: 6 present
[
Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
Critical: false
Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
```

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 프로파일 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

Trunk Configuration

Save Delete Reset Add New

Status
Status: Ready

Device Information

Product: SIP Trunk
 Device Protocol: SIP
 Trunk Service Type: None(Default)
 Device Name*: CUCM10
 Description:
 Device Pool*: Default
 Common Device Configuration: < None >
 Call Classification*: Use System Default
 Media Resource Group List: < None >
 Location*: Hub_None
 AAR Group: < None >
 Tunneled Protocol*: None
 QSIG Variant*: No Changes
 ASN.1 ROSE OID Encoding*: No Changes
 Packet Capture Mode*: None
 Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure*: When using both sRTP and TLS
 Route Class Signaling Enabled*: Default

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.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.95.200		5061

MTP Preferred Originating Codec*: 711ulaw
 BLF Presence Group*: Standard Presence group
 SIP Trunk Security Profile*: Secure SIP Trunk Profile TLS
 Rerouting Calling Search Space: < None >
 Out-Of-Dialog Refer Calling Search Space: < None >
 SUBSCRIBE Calling Search Space: < None >
 SIP Profile*: Standard SIP Profile
 DTMF Signaling Method*: No Preference

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

Trunk Configuration

Save Delete Reset Add New

SIP Trunk Status
 Service Status: Unknown - OPTIONS Ping not enabled
 Duration: Unknown

Device Information

Product: SIP Trunk
 Device Protocol: SIP
 Trunk Service Type: None(Default)
 Device Name*: CUCMA
 Description:
 Device Pool*: HQ
 Common Device Configuration: < None >
 Call Classification*: Use System Default
 Media Resource Group List: < None >
 Location*: Hub_None
 AAR Group: < None >
 Tunneled Protocol*: None
 QSIG Variant*: No Changes
 ASN.1 ROSE OID Encoding*: No Changes
 Packet Capture Mode*: None
 Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure* When using both sRTP and TLS

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.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.95.203		5061

MTP Preferred Originating Codec*: 711ulaw
 BLF Presence Group*: Standard Presence group
 SIP Trunk Security Profile*: Secure SIP Trunk Profile TLS
 Rerouting Calling Search Space: < None >
 Out-Of-Dialog Refer Calling Search Space: < None >
 SUBSCRIBE Calling Search Space: < None >
 SIP Profile*: Standard SIP Profile [View Details](#)
 DTMF Signaling Method*: No Preference

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

Trunks (1 - 1 of 1) Rows per Page 50

Find Trunks where Device Name begins with Find Clear Filter

Select item or enter search text

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Security Profile
CUCM10			Default	9898				SIP Trunk	Secure SIP Trunk Profile TLS

Add New Select All Clear All Delete Selected Reset Selected

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

Trunks (1 - 1 of 1)										Rows per Page 50		
Find Trunks where Device Name <input type="text"/> begins with <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/> <input type="button" value="±"/>										Select item or enter search text <input type="text"/>		
<input type="checkbox"/>	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile
<input type="checkbox"/>	CUCMA			HQ	1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/> <input type="button" value="Reset Selected"/>												

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 수집 CUCM 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 있습니다. 1. 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

Time	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	33135 > 33135 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
18:46:11.313706	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=156761672
18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	33135 > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=15676
18:46:11.430454	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1643 Win=11648 Len=0 TSval=1567
18:46:11.450926	10.106.95.203	10.106.95.200	TCP	1514	[TCP segment of a reassembled PDU]
18:46:11.450969	10.106.95.200	10.106.95.203	TCP	66	33135 > sip-tls [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=98
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Ciph
18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66	33135 > sip-tls [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=98
18:46:11.461558	10.106.95.200	10.106.95.203	TLSv1	1200	New Session Ticket, Change Cipher Spec, Finished
18:46:11.463062	10.106.95.203	10.106.95.200	TLSv1	1161	Application Data
18:46:11.502380	10.106.95.200	10.106.95.203	TCP	66	33135 > sip-tls [ACK] Seq=2777 Ack=3043 Win=23168 Len=0 TSval=98
18:46:11.784432	10.106.95.200	10.106.95.203	TLSv1	440	Application Data
18:46:11.824821	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=3151 Win=17536 Len=0 TSval=15
18:46:12.187974	10.106.95.200	10.106.95.203	TLSv1	1024	Application Data
18:46:12.188452	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=4109 Win=20352 Len=0 TSval=15
18:46:15.288860	10.106.95.200	10.106.95.203	TLSv1	1466	Application Data
18:46:15.289237	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=5509 Win=23296 Len=0 TSval=15
18:46:15.402901	10.106.95.203	10.106.95.200	TLSv1	770	Application Data

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

No.	Time	Source	Destination	Protocol	Length	Info
4	2015-05-23 18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
5	2015-05-23 18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
6	2015-05-23 18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
7	2015-05-23 18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
8	2015-05-23 18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=15676

Secure Sockets Layer

- TLSv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 1560
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1556
 - Certificates Length: 1553
- Certificates (1553 bytes)
 - Certificate Length: 902
 - Certificate (id-at-commonName=CUCM10,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
 - signedCertificate
 - version: v3 (2)
 - serialNumber : 0x398b1da6000000000000e
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

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 일자 는 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

Filter:	Source	Destination	Protocol	Length	Info
	10.106.95.203	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=59 Ack=1043 Win=11048 Len=0 TSval=1567610644 TSecr=9
	18:46:11.450926	10.106.95.203	TCP	1514	[TCP segment of a reassembled PDU]
	18:46:11.450969	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988797 TSecr=156
	18:46:11.451030	10.106.95.203	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Fini
	18:46:11.451081	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988797 TSecr=156

Secure Sockets Layer

- TLSv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 1559
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1555
 - Certificates Length: 1552
- Certificates (1552 bytes)
 - Certificate Length: 901
 - Certificate (id-at-commonName=CUCMA,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
 - signedCertificate
 - version: v3 (2)
 - serialNumber : 0x197ad7e90000000000002
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

패킷 캡처의 인증서와 OS 관리 웹 페이지의 인증서가 일치하지 않으면 올바른 인증서가 업로드되지 않습니다. 올바른 인증서를 OS Admin Cert 페이지에 업로드해야 합니다. CUCM 추적 수집 CUCM 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 |sd1sig |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 |sd1sig |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 =
```