

# SIP-TLS Trunk configureren op Unified Communications Manager met een CA-ondertekend certificaat

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Stap 1. Gebruik de openbare CA of de optie CA instellen op Windows Server 2003](#)

[Stap 2. Controleer uw naam en instellingen](#)

[Stap 3. Generate en Download de certificaataanvraag \(CSR\)](#)

[Stap 4. Teken de CSR met de Microsoft Windows 2003 certificaatautoriteit](#)

[Stap 5. Ontvang het wortelcertificaat van de CA](#)

[Stap 6. CA-basiscertificaat uploaden als CallManager Trust](#)

[Stap 7. CA-teken uploaden via CallManager CSR-certificaat als CallManager-certificaat.](#)

[Stap 8. Maak SIP Trunk-beveiligingsprofielen](#)

[Stap 9. Maak SIP-trunks](#)

[Stap 10. Routepatronen maken](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Verzamel pakketvastlegging op CUCM](#)

[CUCM-sporen verzamelen](#)

## Inleiding

Dit document beschrijft een stap voor stap proces om de door een certificeringsinstantie (CA) ondertekende Session Initiation Protocol (SIP) Transport Layer Security (TLS) Trunk op Communications Manager te configureren.

Na het volgen van dit document worden SIP-berichten tussen twee clusters versleuteld met het TLS.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben van:

- Cisco Unified Communications Manager (CUCM)
- SIP

## Gebruikte componenten

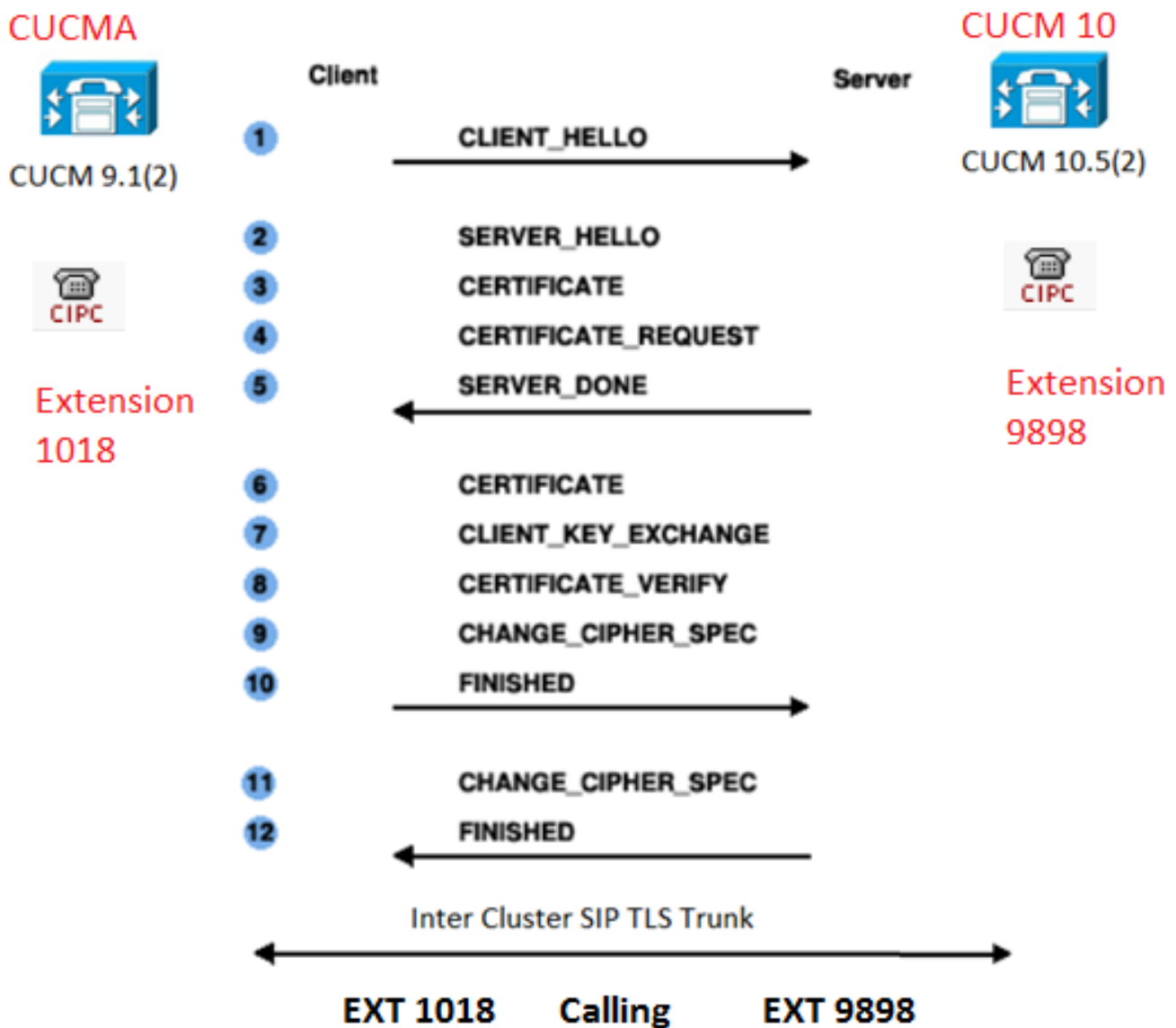
De informatie in dit document is gebaseerd op deze softwareversies:

- UCM versie 9.1(2)
- UCM versie 10.5(2)
- Microsoft Windows Server 2003 als CA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Achtergrondinformatie

Zoals in deze afbeelding wordt getoond, SSL Handshake met certificaten.



Stap 1. Gebruik de openbare CA of de optie CA instellen op Windows Server 2003

Raadpleeg de link: [Stel CA in op Windows 2003-server](#)

Stap 2. Controleer uw naam en instellingen

Certificaten zijn gebaseerd op namen. Zorg ervoor dat de namen juist zijn voor u begint.

```
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
```

Raadpleeg de link om de hostname te wijzigen: [Hostnaam wijzigen op CUCM](#)

Stap 3. Generate en Download de certificaataanvraag (CSR)

## CUCM 9.1(2)

Om de CSR te genereren, navigeer dan naar **OS-beheerder > Beveiliging > certificaatbeheer > CSR genereren**

Selecteer in het veld **certificaatnaam** de optie **CallManager** in de vervolgkeuzelijst.

**Generate Certificate Signing Request**

Generate CSR Close

**Status**

Warning: Generating a new CSR will overwrite the existing CSR

**Generate Certificate Signing Request**

Certificate Name \* CallManager

Generate CSR Close

U kunt CSR downloaden via **OS Admin > Security > certificaatbeheer > CSR downloaden**

Selecteer in het veld **certificaatnaam** de optie **CallManager** in de vervolgkeuzelijst.

### 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)


Om de CSR te genereren, navigeer naar **OS-beheerder > Beveiliging > certificaatbeheer > CSR genereren**

1. Selecteer in het veld certificaatdoel de optie CallManager in de vervolgkeuzelijst.
2. Selecteer 1024 in het veld Key Length van de vervolgkeuzelijst.
3. Selecteer SHA1 in het veld Hash Algorithm in de vervolgkeuzelijst.

### 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

U kunt CSR downloaden via **OS Admin > Security > certificaatbeheer > CSR downloaden** Selecteer in het veld certificaatdoel de optie CallManager in de vervolgkeuzelijst.

## Download Certificate Signing Request



Download CSR



Close

### Status



Certificate names not listed below do not have a corresponding CSR

### Download Certificate Signing Request

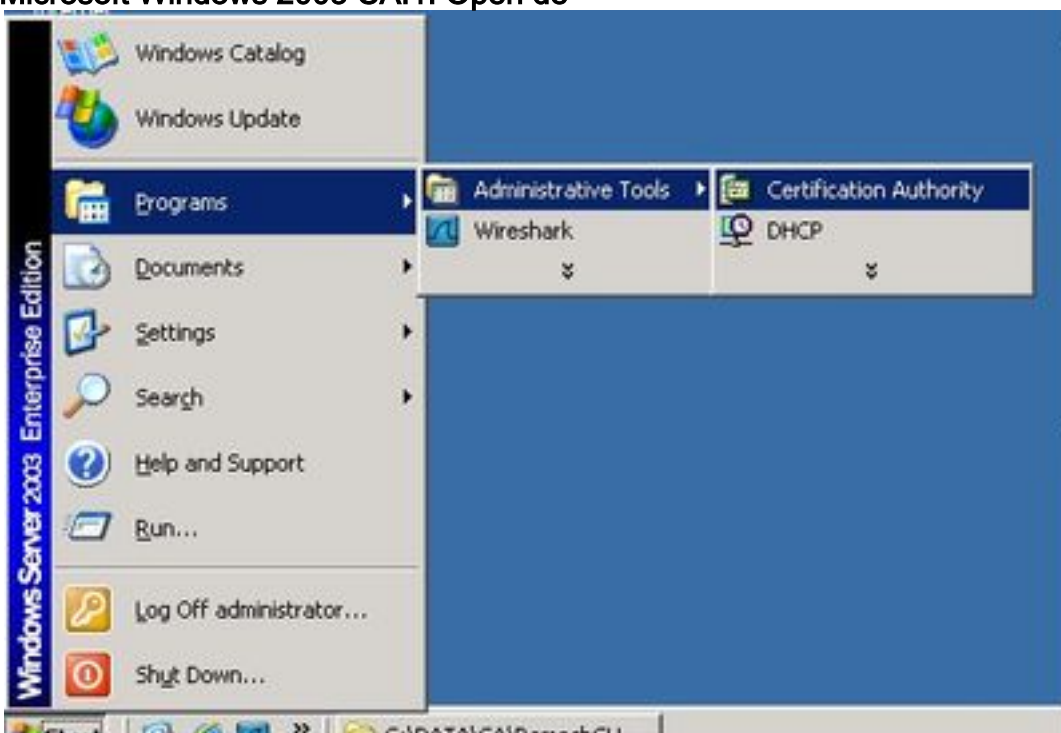
Certificate Purpose\*

CallManager

Download CSR

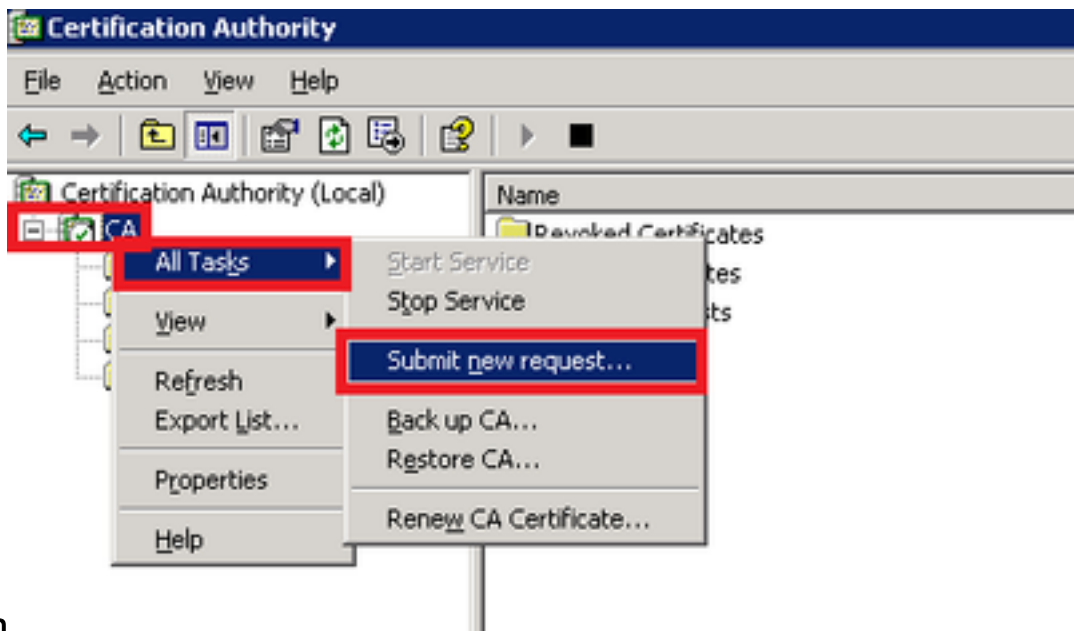
Close

Opmerking: CallManager CSR wordt gegenereerd met de 1024 bit Rivest-Shamir-Add (RSA) toetsen. Stap 4. Teken de CSR met de Microsoft Windows 2003 certificaatautoriteit Dit is een optionele informatie om de CSR te ondertekenen met Microsoft Windows 2003 CA.1. Open de



certificeringsinstantie.

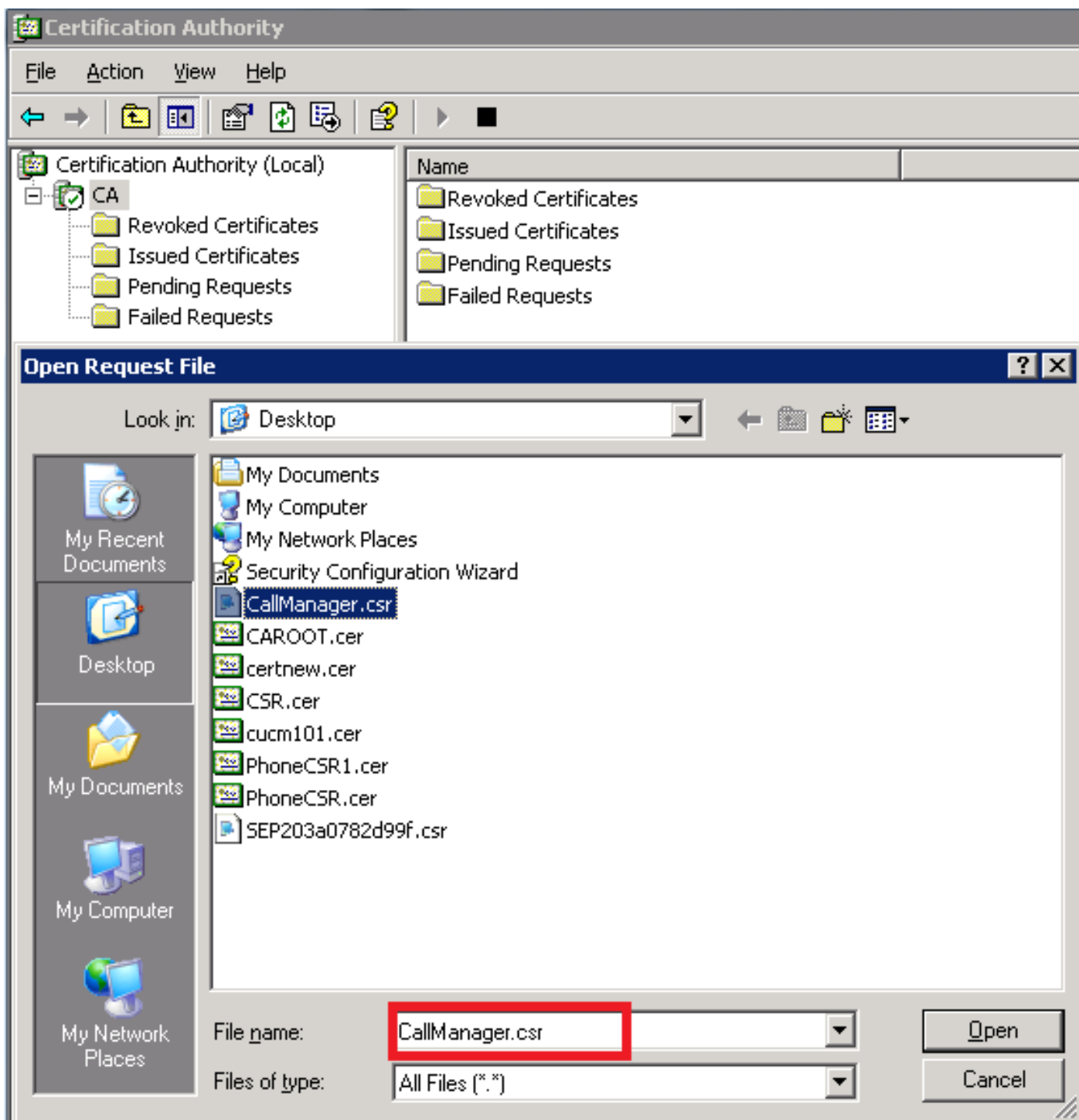
. Klik met de rechtermuisknop op het pictogram CA en navigeer naar Alle taken > Nieuwe



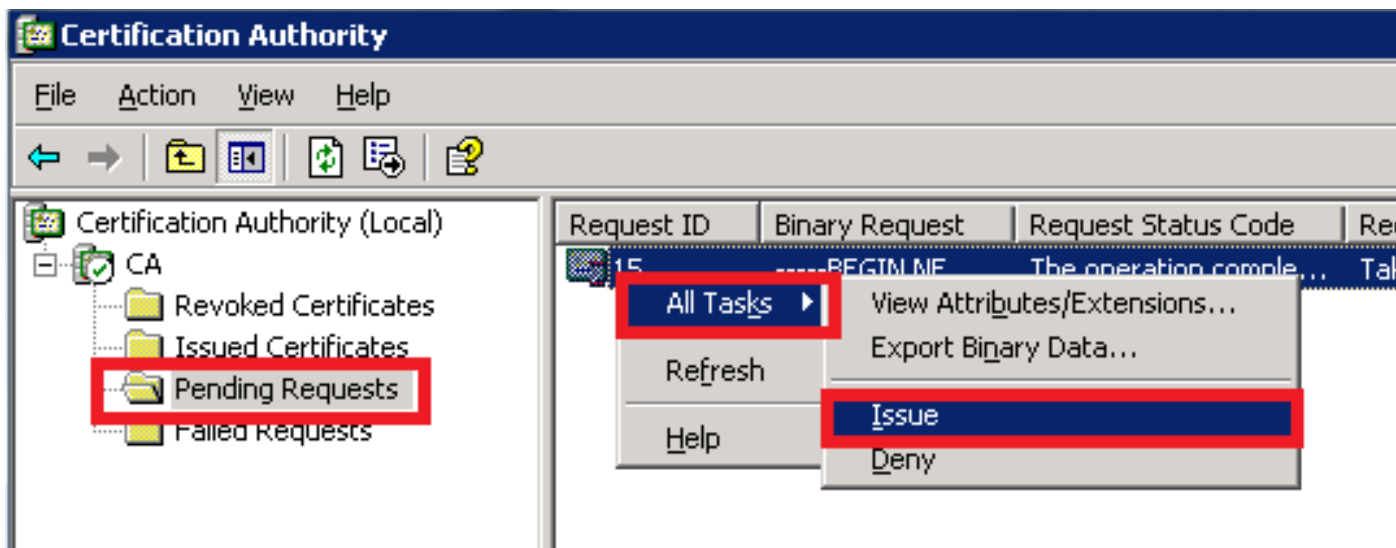
aanvraag indienen

Selecteer de CSR en klik op de optie Openen (van toepassing in zowel de CSR als CUCM 9.1(2) en CUCM 10.5(2))

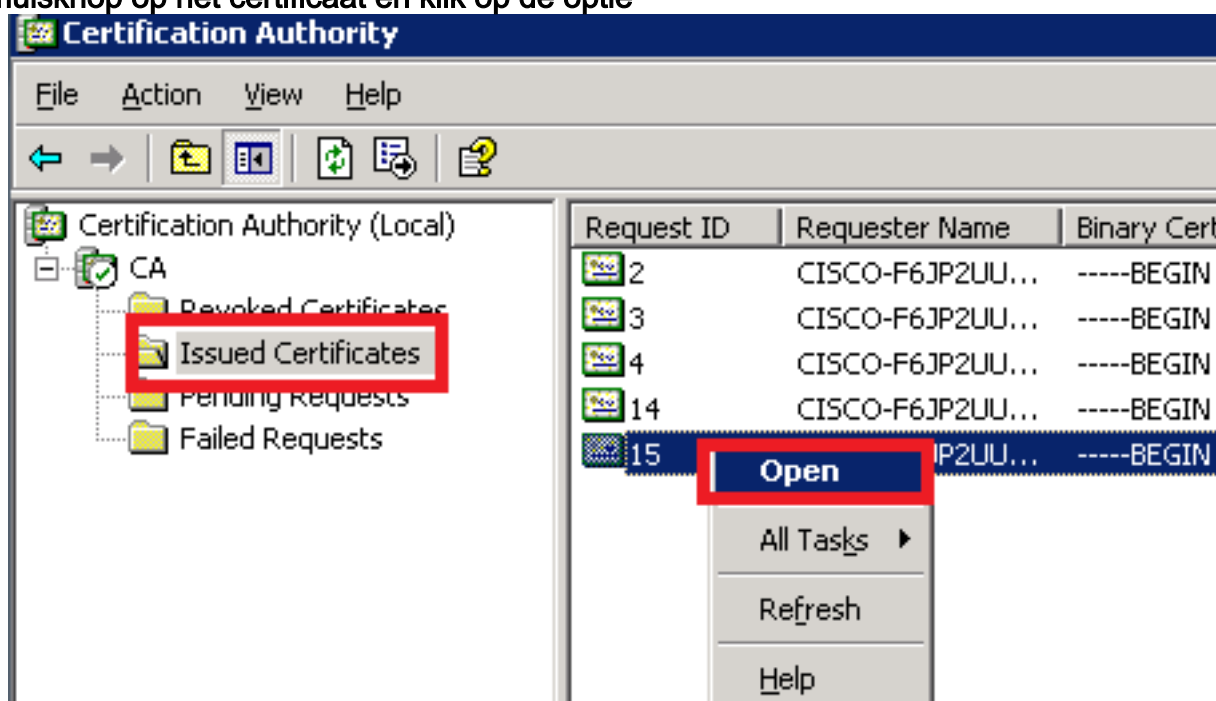
3.



4. Alle geopende CSR's worden weergegeven in de map Aanvragen. Klik met de rechtermuisknop op elke CSR en navigeer naar Alle taken > Uitgeven om de certificaten uit te geven. (Van toepassing in zowel de CSR's (CUCM 9.1(2) als CUCM 10.5(2))



5. Selecteer de map Gegeven certificaten om het certificaat te kunnen downloaden. Klik met de rechtermuisknop op het certificaat en klik op de optie

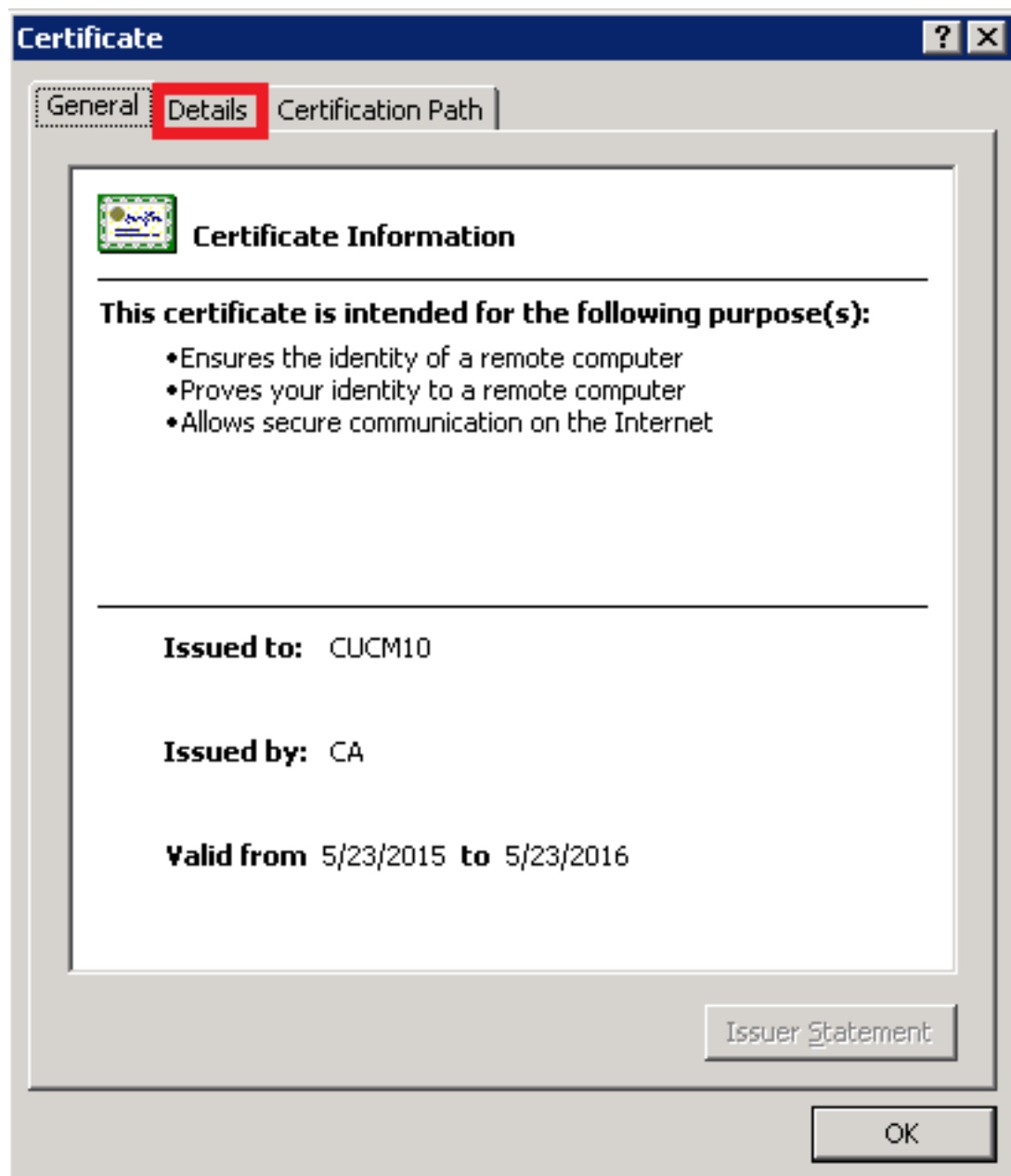


Openen.

De certificaatgegevens worden weergegeven. Wilt u het certificaat downloaden, dan selecteert u het tabblad Details en klikt u vervolgens op de knop Kopie naar

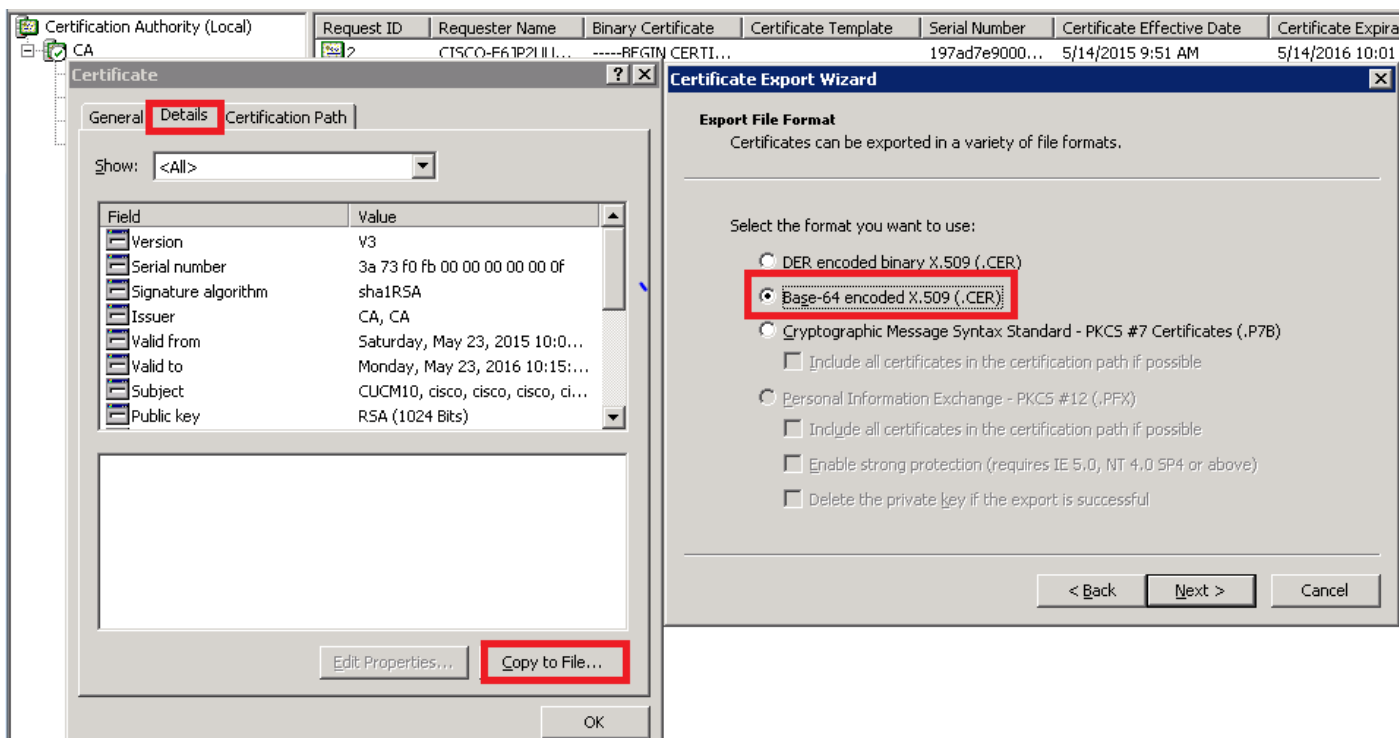
6.



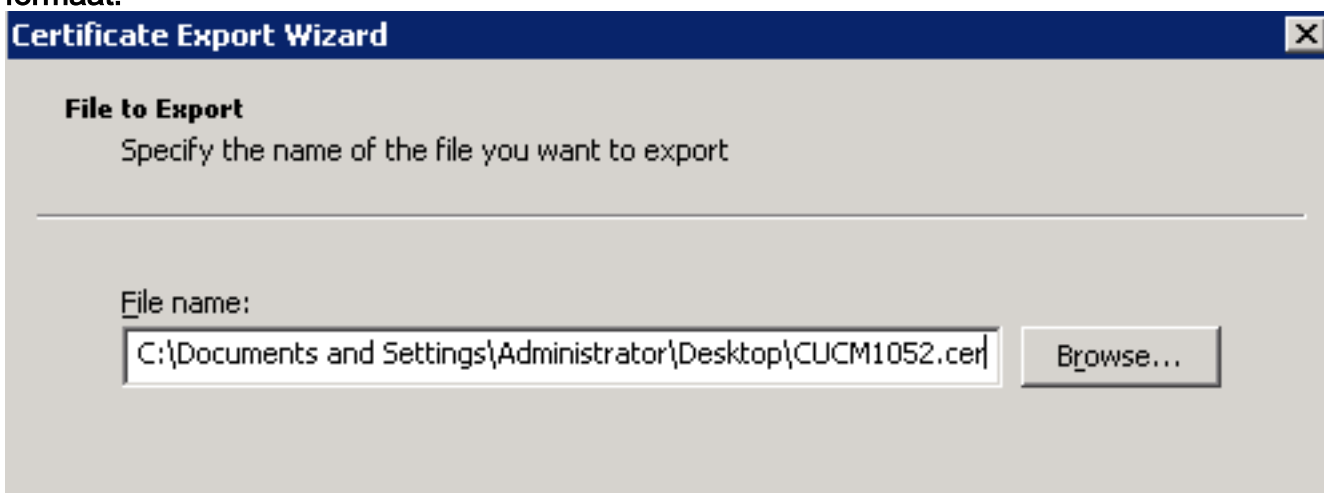


bestand...  
het venster certificaatwizard op de knop Base-64 met de code X.509  
(.CER).

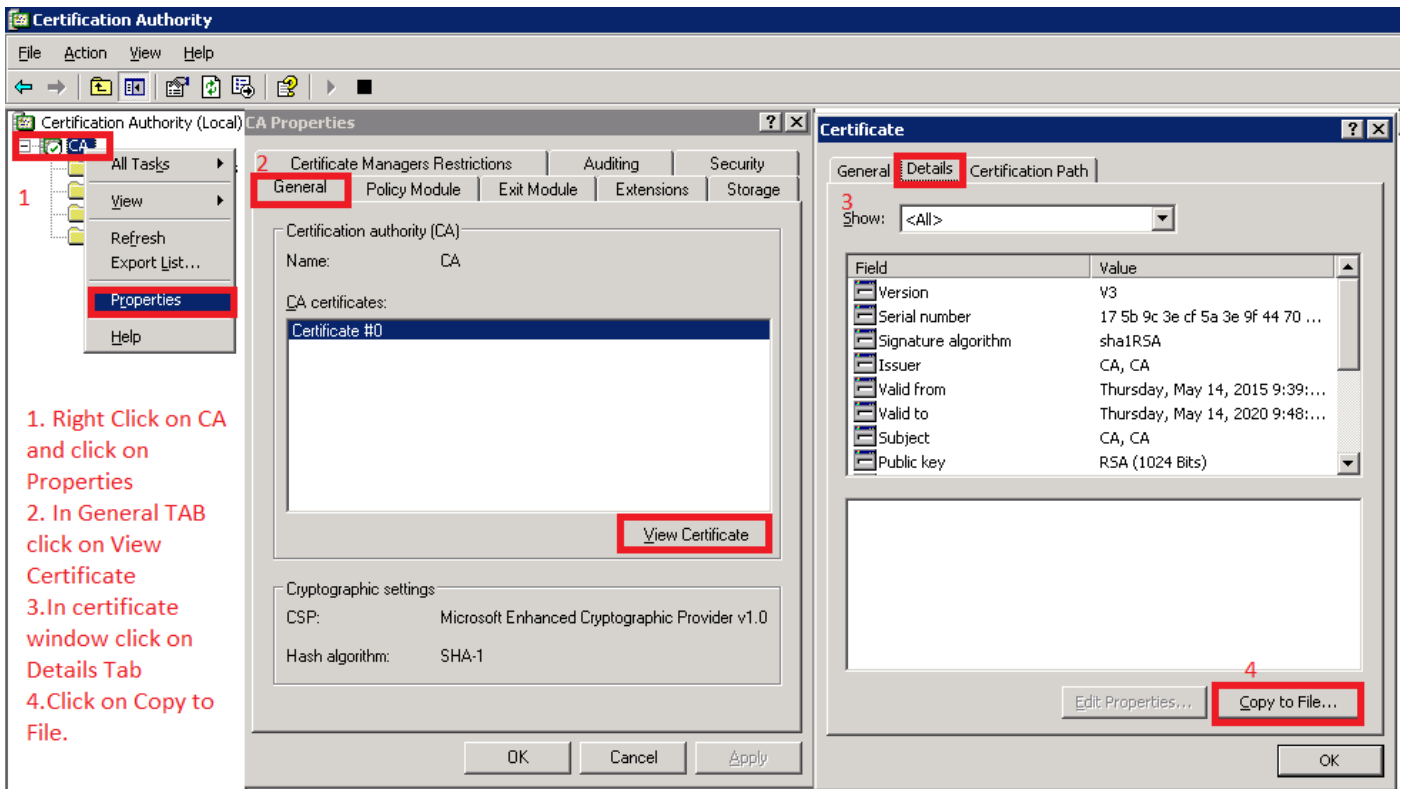
7. Klik in



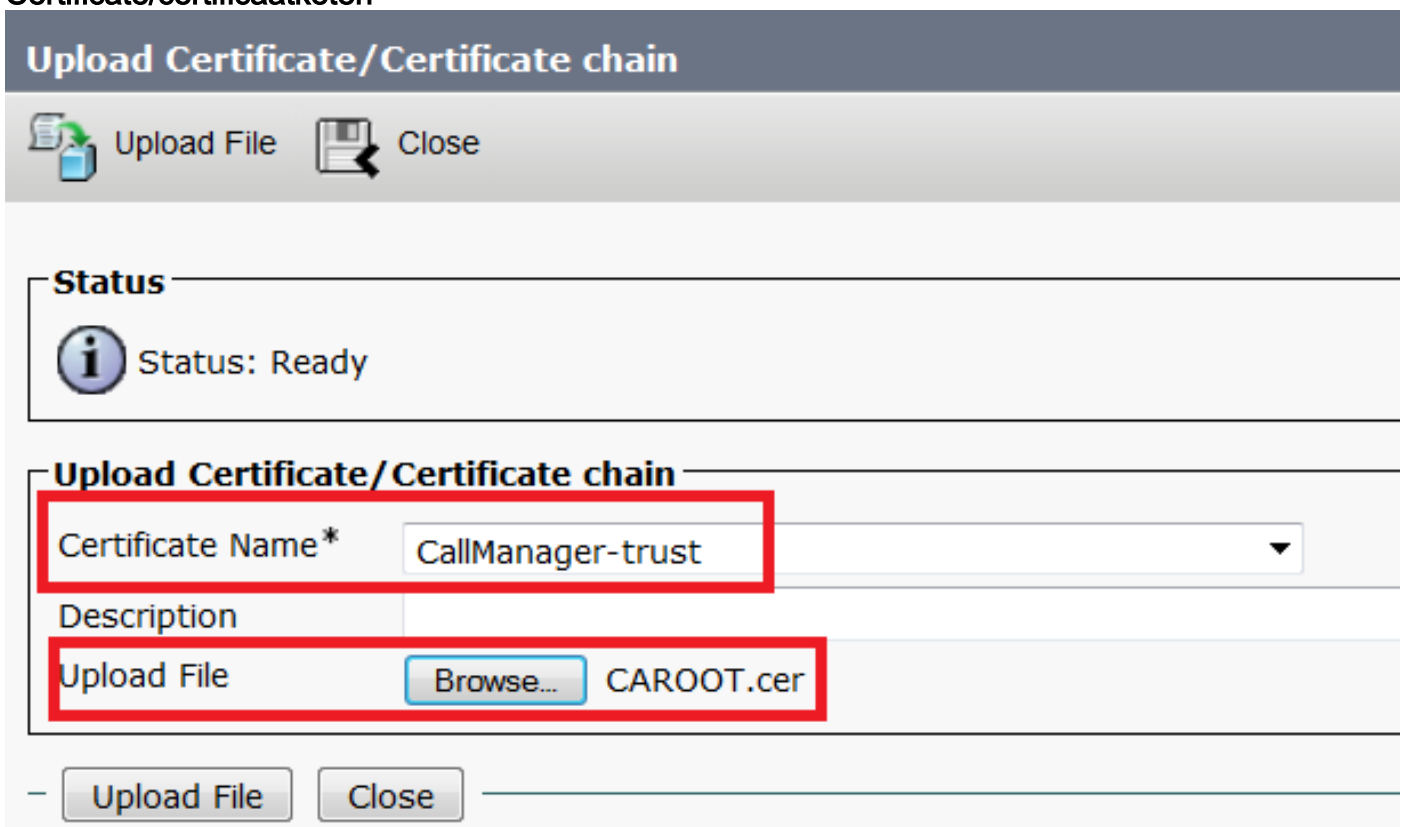
8. Geef het bestand een nauwkeurige naam. Dit voorbeeld gebruikt het CUCM1052.cer-formaat.



Volg dezelfde procedure voor CUCM 9.1(2). Stap 5. Ontvang het wortelcertificaat van de CA. Open het venster van de certificeringsinstantie. Om de root-CA te downloaden: 1. Klik met de rechtermuisknop op het CA-pictogram en klik op de optie Eigenschappen. 2. Klik in het algemeen op Certificaat bekijken. 3. Klik in het venster Certificaat op het tabblad Details. 4. Klik op Kopie naar bestand...



Step 6. CA-basiscertificaat uploaden als CallManager Trust Om het CA Root Certificate te uploaden, inlogt u in op OS Admin > Security > certificaatbeheer > Upload Certificate/certificaatketen



Opmerking: Voer deze stappen uit op zowel CUCM's (CUCM 9.1(2) als CUCM 10.5(2)) Step 7. CA-teken uploaden via CallManager CSR-certificaat als CallManager-certificaat. Om de CA-teken CallManager CSR te uploaden, inlogt u op OS Admin > Security > certificaatbeheer > Upload certificaat/certificaatketen

## 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

Opmerking: Voer deze stappen uit op zowel CUCM's (CUCM 9.1(2) als CUCM 10.5(2))<sup>Stap 8. Maak SIP Trunk-beveiligingsprofielen</sup>CUCM 9.1(2)

Als u het SIP Trunk-beveiligingsprofiel wilt maken, navigeer dan naar systeembeveiliging > SIP Trunk-beveiligingsprofiel. Kopieert het bestaande niet-beveiligde SIP Trunk-profiel en geef het een nieuwe naam. In het voorbeeld is niet-Secure SIP Trunk Profile anders genoemd met Secure SIP Trunk Profile  
TLS.

## 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 ▼	

Gebruik in X.509 Onderwerp de GN-benaming van CUCM 10.5(2) (met CA-ondertekend certificaat) zoals in deze afbeelding aangegeven.

## 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) Navigeer naar systeem > security > SIP Trunk security profiel. Kopieert het bestaande niet-beveiligde SIP Trunk-profiel en geef het een nieuwe naam. In het voorbeeld werd het niet-beveiligde SIP Trunk-profiel omgedoopt met Secure SIP Trunk Profile TLS.**

## 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 <span style="color: red;">This Name should be CN of CUCM 9.1(2)</span>
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

In X.509 gebruikt de GN van de CUCM 9.1(2) (door CA ondertekend certificaat) zoals aangegeven:

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:
be0207bf5446944aef901ee5c3daefdb2cf4cbc870f8e1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d:
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,
  ]
]
```

Zowel SIP Trunk Security Profiles stelden een inkomende poort van 5061 in, waarin elke cluster op de TCP poort 5061 luistert voor de nieuwe inkomende SIP TLS vraag. **Stap 9. Maak SIP-trunks** Nadat de Security profielen zijn gemaakt, kunt u de SIP-trunks maken en de onderstaande configuratieparameter in de SIP Trunk wijzigen. **CUCM 9.1(2)**

1. Controleer in het venster Trunk Configuration het toegestane configuratieparameter SRTP. Dit waarborgt het Real-time Transport Protocol (RTP) dat voor de oproepen via deze stam wordt gebruikt. Dit vakje moet alleen worden gecontroleerd wanneer u SIP-TLS gebruikt, omdat de toetsen voor Secure Real-time Transport Protocol (SRTP) in de tekst van het SIP-bericht zijn uitgewisseld. De SIP-signalering moet door TLS zijn beveiligd, anders kan iedereen met de niet-beveiligde SIP-signalering de corresponderende SRTP-stream over de romp decrypteren.

**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 >  
 Tunnelled 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. Voeg in het gedeelte SIP-informatie van het venster Trunk-configuratie het doeladres, de doelpoort en SIP Trunk-beveiligingsprofiel toe.

**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. Controleer in het venster Trunk Configuration het toegestane configuratieparameter SRTP.



Dit staat SRTP toe om voor vraag over deze kofferbak te worden gebruikt. Dit vakje moet alleen worden gecontroleerd bij gebruik van SIP-TLS, omdat de toetsen voor SRTP in de tekst van het SIP-bericht worden uitgewisseld. De SIP-signalering moet door het TLS worden beveiligd, omdat iedereen met een niet-beveiligd SIP-signalering de corresponderende Secure RTP-stroom via de romp kan decrypteren.

**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. Voeg in het gedeelte SIP-informatie van het venster Trunk-configuratie het IP-adres, poort op bestemming en beveiligingsprofiel toe

**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

Stap 10. Routepatronen maken De eenvoudigste methode is om een routepatroon op elke cluster te maken, waarbij u rechtstreeks naar de SIP-trunk wijst. Routegroepen en routekaarten zouden ook kunnen worden gebruikt. CUCM 9.1(2) punten naar routepatroon 9898 via het TLS SIP-trunk naar het CUCM 10.5(2)

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) wijst naar routepatroon 1018 via de TLS SIP-trunk naar CUCM 9.1(2)

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 Status	SIP Trunk Duration	SIP Trunk Security Profile			
CUCMA		HQ		1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS			
Add New											Select All	Clear All	Delete Selected	Reset Selected

## Verifiëren Er is momenteel geen verificatieprocedure beschikbaar voor deze

configuratie. **Problemen oplossen** De vraag van SIP TLS kan met deze stappen worden gezuiverd. **Verzamel pakketvastlegging op CUCM** Om de connectiviteit tussen CUCM 9.1(2) en CUCM 10.5(2) te controleren, neemt u een pakketvastlegging op de CUCM-servers en kijkt u naar het SIP-TLS-verkeer. Het SIP TLS-verkeer wordt via de TCP-poort 5061 doorgegeven, gezien als stappen-toetsen. In het volgende voorbeeld is er een SSH CLI-sessie ingesteld op CUCM 9.1(2).

1. CLI-pakketvastlegging op scherm Deze CLI drukt de uitvoer op het scherm af voor het SIP TLS-verkeer.

```
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. CLI-opname in bestand Deze CLI voert de pakketvastlegging uit op basis van de host en maakt een bestand met de naam van pakketten aan.

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

Start de SIP-stam op CUCM 9.1(2) opnieuw en dien de oproep in vanaf de verlenging 1018 (CUCM 9.1(2)) tot de verlenging 9898 (CUCM 10.5(2)) U kunt het bestand vanuit de CLI downloaden op:

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

De opname wordt uitgevoerd in de standaard .cap-indeling. In dit voorbeeld wordt Wireshark gebruikt om pakketten.cap-bestand te openen, maar er kan elk programma voor de pakketvastlegging worden gebruikt.

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	sip-tls > 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	sip-tls > 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=156761672
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=156761672
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	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988679
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec
18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988679
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	10.106.95.203	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=2777 Ack=3043 Win=23168 Len=0 TSval=988679
18:46:11.784432	10.106.95.203	10.106.95.200	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=156761672
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=156761672
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=156761672
18:46:15.402901	10.106.95.203	10.106.95.200	TLSv1	770	Application Data

1. The Transmission Control Protocol (TCP) Synchronize (SYN) om de TCP-communicatie tussen CUCM 9.1(2)(client) en CUCM 10.5(2)(server) in te stellen.
2. De CUCM 9.1(2) stuurt de client naar Hallo om de TLS-sessie te starten.
3. De CUCM 10.5(2) stuurt de server Hallo, Server certificaataanvraag en certificaataanvraag om het certificeringsproces te starten.
4. Het certificaat dat de cliënt CUCM 9.1(2) verstuurt om de certificaatuitwisseling te voltooien.
5. De toepassingsgegevens die gecodeerde SIP-signalering zijn, tonen aan dat de TLS-sessie is ingesteld.

Verdere controle of de juiste certificaten worden uitgewisseld. Nadat Server Hallo, verstuurt de server CUCM 10.5(2) zijn certificaat naar de client CUCM 9.1(2).

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

- Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 1560
  - 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 : 0x398b1da600000000000e
            - signature (shaWithRSAEncryption)
            - issuer: rdnSequence (0)
            - validity
            - subject: rdnSequence (0)
            - subjectPublicKeyInfo
            - extensions: 6 items

Het serienummer en de onderwerpinformatie die de server CUCM 10.5(2) heeft ontvangen, worden aan de client aangeboden CUCM 9.1(2). Het serienummer, het onderwerp, de emittent en de validatiedata worden allemaal vergeleken met de informatie op de pagina van het OS Admin certificaatbeheer. De server CUCM 10.5(2) dient zijn eigen verificatiecertificaat in en nu controleert het certificaat van de client CUCM 9.1(2). De verificatie gebeurt in beide richtingen.

Filter:	Source	Destination	Protocol	Length	Info
	18:40:11.430454	10.106.95.203	10.106.95.200	TCP	66 sip-tls > sip-tls [ACK] Seq=59 Ack=1043 Win=11048 Len=0 TSval=1307010844 TSecr=9
	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 sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988797 TSecr=156
	18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Fini
	18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66 sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988797 TSecr=156

Secure Sockets Layer

- Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 1559
  - 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

Als er een verschil is tussen de certificaten in de pakketvastlegging en de certificaten in de webpagina OS Admin, worden de juiste certificaten niet geüpload. De juiste certificaten moeten op de pagina OS Admin Cert worden geüpload. CUCM-sporen verzamelen De CUCM-sporen kunnen ook helpen bepalen welke berichten worden uitgewisseld tussen de CUCM 9.1(2) en de CUCM 10.5(2)-servers en of de SSL-sessie al dan niet goed is ingesteld. In het voorbeeld zijn de sporen van CUCM 9.1(2) verzameld. Call Flow: EXT 1018 > CUCM 9.1(2) > SIP-TLS TRUNK > CUCM

10.5(2) > Ext 9898++ Digitale analyse

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqc="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-TLS wordt op poort 5061 voor deze oproep gebruikt.

```
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-bericht (Signal Distribution Layer) SIPCertificaatInd bevat informatie over Onderwerp GN en verbindinginformatie.

```
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 =
```