

# SIP-TLS configureren tussen CUCM-CUBE/CUBE-SBC

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratiestappen](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inhoud

## Inleiding

Dit document helpt u bij het configureren van SIP Transport Layer Security (TLS) tussen Cisco Unified Communications Manager (CUCM) en Cisco Unified Border Element (CUBE)

## Voorwaarden

Cisco raadt aan om kennis te hebben over deze onderwerpen

- SIP-protocol
- Security certificaten

## Vereisten

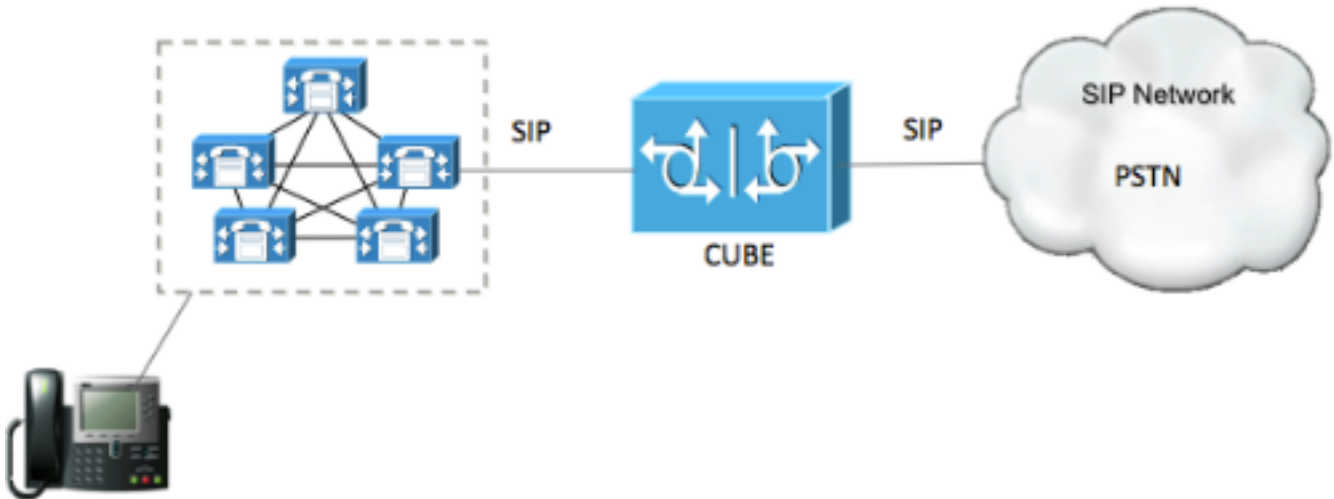
- Datum en tijd moeten op de eindpunten overeenkomen (aanbevolen wordt om dezelfde NTP-bron te hebben).
- CUCM moet in gemengde modus worden geplaatst.
- TCP-connectiviteit is vereist (Open poort 5061 op elke transitfirewall).
- De CUBE moet de beveiliging en de UCK9 licenties hebben geïnstalleerd.

## Gebruikte componenten

- SIP
- Gewaarborgde certificaten

## Configureren

## Netwerkdigram



## Configuratiestappen

Stap 1. Maak een betrouwbaar punt om CUBE's zelfgetekende certificaat vast te houden

```
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)
```

Stap 2. Zodra het trust point is gecreëerd, voert u de opdracht **Crypto-sleutel in om CUBE-test** in te voeren om zelf getekende kerterticaten te krijgen

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

Als inschrijving juist was, moet u deze uitvoer verwachten

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

Stap 3. Nadat u een certificaat hebt verkregen, moet u dit exporteren

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

De bovenstaande opdracht moet het onderstaande certificaat genereren

% Self-signed CA certificate:

-----BEGIN CERTIFICATE-----

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

-----END CERTIFICATE-----

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

-----END CERTIFICATE-----

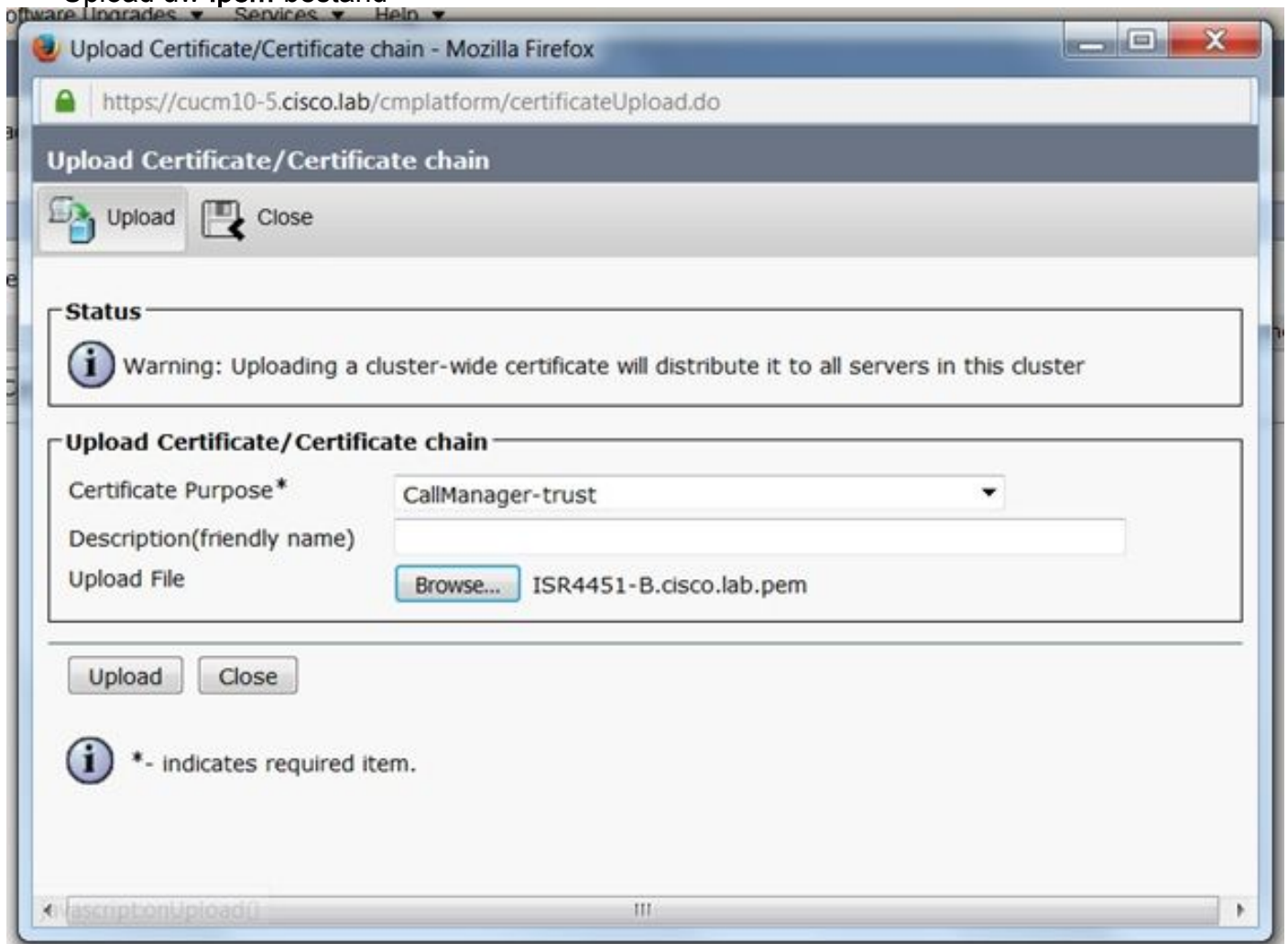
**Kopieert het bovenstaande zelfgetekende certificaat en plak het op een tekstbestand met bestandsextensie .pem**

Voorbeeld hieronder wordt genoemd als ISR4451-B.ciscolab.pem



#### Stap 4. Upload het CUBE-certificaat naar het CUCM

- CUCM OS Admin > Security > certificaatbeheer > Upload certificaatketting
- certificaatdoel = CallManager-vertrouwen
- Upload uw .pem-bestand



#### Stap 5. Download het door de Call Manager zelf ondertekende certificaat

- Vind het certificaat dat CallManager zegt
- Klik op de hostnaam
- Klik op PEM-bestand downloaden
- Sla het op uw computer op

Cisco Unified Operating System Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | **CR**

Home | Settings | Security | Software Upgrades | Services | Help

### Certificate List

Generate Self-signed | Upload Certificate/Certificate chain | Generate CSR

Status: 10 records found

Certificate List (1 - 10 of 10) Rows per Page: 10

Find Certificate List where: Certificate begins with CallManager Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM1052	Self-signed	RSA	CUCM1052	CUCM1052	07/20/2021	Self-signed certificate generated by system

### Certificate Details(Self-signed)

https://10.201.196.162/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManager.pem

#### Certificate Details for CUCM1052, CallManager

Regenerate | Generate CSR | Download .PEM File | Download .DER File

**Status**  
Status: Ready

**Certificate Settings**

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

**Certificate File Data**

```
[
Version: V3
Serial Number: 4A7B503A9A3D202AD7D54B1F874B7DF7
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
Validity From: Thu Jul 21 13:11:22 CDT 2016
To: Tue Jul 20 13:11:21 CDT 2021
Subject Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100b803883f1177dcd68431efc16d7fdb127db637091d1d8e7b5
8d913a1689d2a289ea74fc1b42b5a571bc0abc1310e63b8924a84a3e7dc03e5001ac
4fb551b9f1569d44c1f336d5a1c2a80cbf65ebc93e2bb1619ca3d1c77984aeed1a752
3c433611d85f619725c8d116a5ab399765ed0851cdd73336244a7d214091f7a92be
38d07ae913dee31954028c16a6b020737890fc3f63653da9ca6bbafbd59f3c3b77292
89d50f14b7d8d4ae303069072917f6491ba1083584cae22122bd6ed524da1598353
]
```

Regenerate | Generate CSR | Download .PEM File | Download .DER File

Close

Step 6. Upload het CallManager.pem-certificaat naar CUBE

- Open CallManager.pem met een tekstbestandseditor
- De gehele inhoud van het bestand kopiëren
- Start deze opdrachten op CUBE

```
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

## Stap 7. Configureer SIP met behulp van de zelfgetekende certificaattrustpoint van CUBE

sip-ua

crypto signaling default trustpoint CUBEtest

## Stap 8. Configureer de dial-peers met TLS

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
```

```
srtplib
```

## Stap 9. Het beveiligingsprofiel van de CUCM SIP-stam configureren

- CUCM Admin-pagina > Systeem > Security > SIP Trunk-beveiligingsprofiel
- Het profiel configureren zoals hieronder wordt weergegeven

**SIP Trunk Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**  
Status: Ready

**SIP Trunk Security Profile Information**

Name*	CUBE Secure SIP Trunk Profile
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	ISR4451-B.cisco.lab
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" 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

**Opmerking:** Het is van cruciaal belang dat het X.509-veld overeenkomt met de GN-naam die u eerder hebt ingesteld terwijl u het zelf-ondertekende certificaat hebt gegenereerd

## Stap 10. Configureer een SIP-stam op CUCM

- Zorg ervoor dat het selectieknop SRTP is ingeschakeld
- Configureer het juiste doeladres en zorg ervoor dat u poort 5060 door poort 5061 vervangt
- Zorg ervoor dat u het juiste SIP Trunk-beveiligingsprofiel selecteert (dit profiel is gemaakt in

## Stap 9)

**SIP Information**

**Destination**

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.201.160.12		5061

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* ISR4451-B Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile-options [View Details](#)

DTMF Signaling Method\* No Preference

- Sla de romp op en herstelt deze.

## Verifiëren

Aangezien u OPTIES die op CUCM PING zijn ingeschakeld, hebt u de SIP-stam als VOLLEDIGE SERVICE-status ingeschakeld

Name ^	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
<a href="#">ISR4451-B</a>			<a href="#">0711-Secure</a>					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

De SIP stam status toont volledige service.

De status van dial peer verschijnt als volgt:

```
show dial-peer voice summary
```

TAG	TYPE	MIN	OPER	PREFIX	DEST-PATTERN	FER	THRU	SESS-TARGET	STAT	PORT
9999	voip	up	up		9999	0	syst	dns:cucml0-5		active

## Problemen oplossen

De uitvoer van deze apparaten inschakelen en verzamelen

```
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-opname link:**



<https://goo.gl/QOS1iT>