

# Konfigurieren von SIP-TLS zwischen CUCM-CUBE/CUBE-SBC

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationsschritte](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Inhaltsverzeichnis

## Einführung

Dieses Dokument unterstützt die Konfiguration von SIP Transport Layer Security (TLS) zwischen Cisco Unified Communication Manager (CUCM) und Cisco Unified Border Element (CUBE).

## Voraussetzungen

Cisco empfiehlt, diese Themen zu kennen.

- SIP-Protokoll
- Sicherheitszertifikate

## Anforderungen

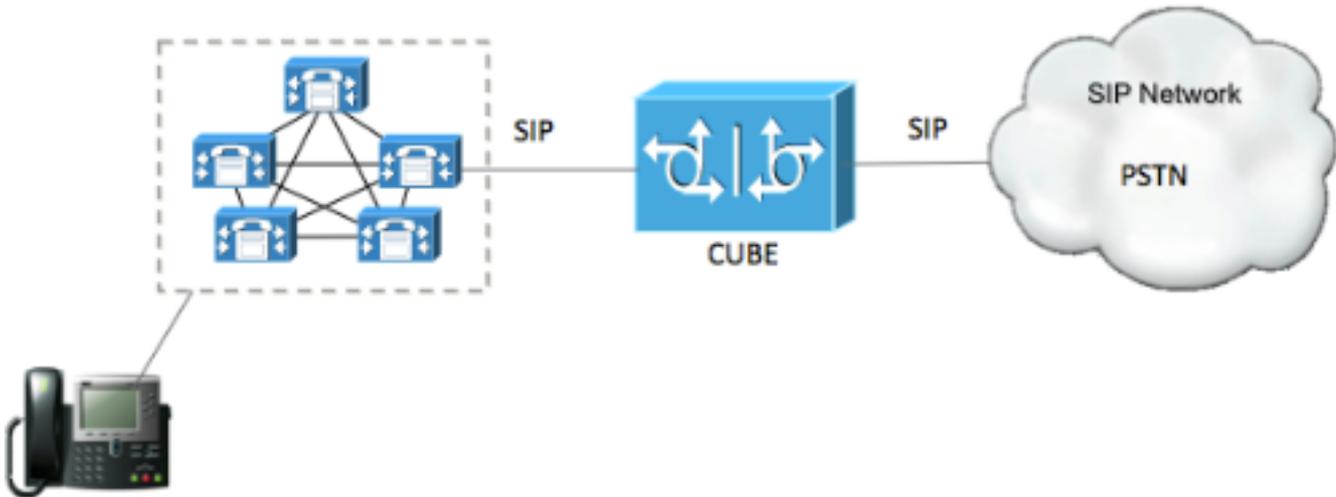
- Datum und Uhrzeit müssen auf den Endpunkten übereinstimmen (es wird empfohlen, dieselbe NTP-Quelle zu verwenden).
- Der CUCM muss sich im gemischten Modus befinden.
- TCP-Konnektivität ist erforderlich (Open port 5061 on any Transit Firewall).
- Auf dem CUBE müssen die Sicherheits- und UCK9-Lizenzen installiert sein.

## Verwendete Komponenten

- SIP
- Eigenständige Zertifikate

## Konfigurieren

## Netzwerkdiagramm



## Konfigurationsschritte

Schritt 1: Erstellen Sie einen Vertrauenspunkt, um das selbst signierte CUBE-Zertifikat zu speichern.

```
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)
```

Schritt 2: Nachdem der Vertrauenspunkt erstellt wurde, führen Sie den Befehl **Crypto pki enroll CUBEtest** aus, um selbstsignierte Zertifikate zu erhalten.

```
crypto pki enroll CUBEtest

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

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

Wenn die Registrierung korrekt war, müssen Sie diese Ausgabe erwarten

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

Schritt 3: Nachdem Sie das Zertifikat erworben haben, müssen Sie es exportieren

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

Der obige Befehl muss das unten stehende Zertifikat generieren.

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY2l2Y28ubGF1bG4XDTE1MTIxNTAxNTAxNV0XDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBBgwFoAU+Yy1UqKdb+rrINc7tZcZrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhdVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY2l2Y28ubGF1bG4XDTE1MTIxNTAxNTAxNV0XDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBBgwFoAU+Yy1UqKdb+rrINc7tZcZrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhdVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

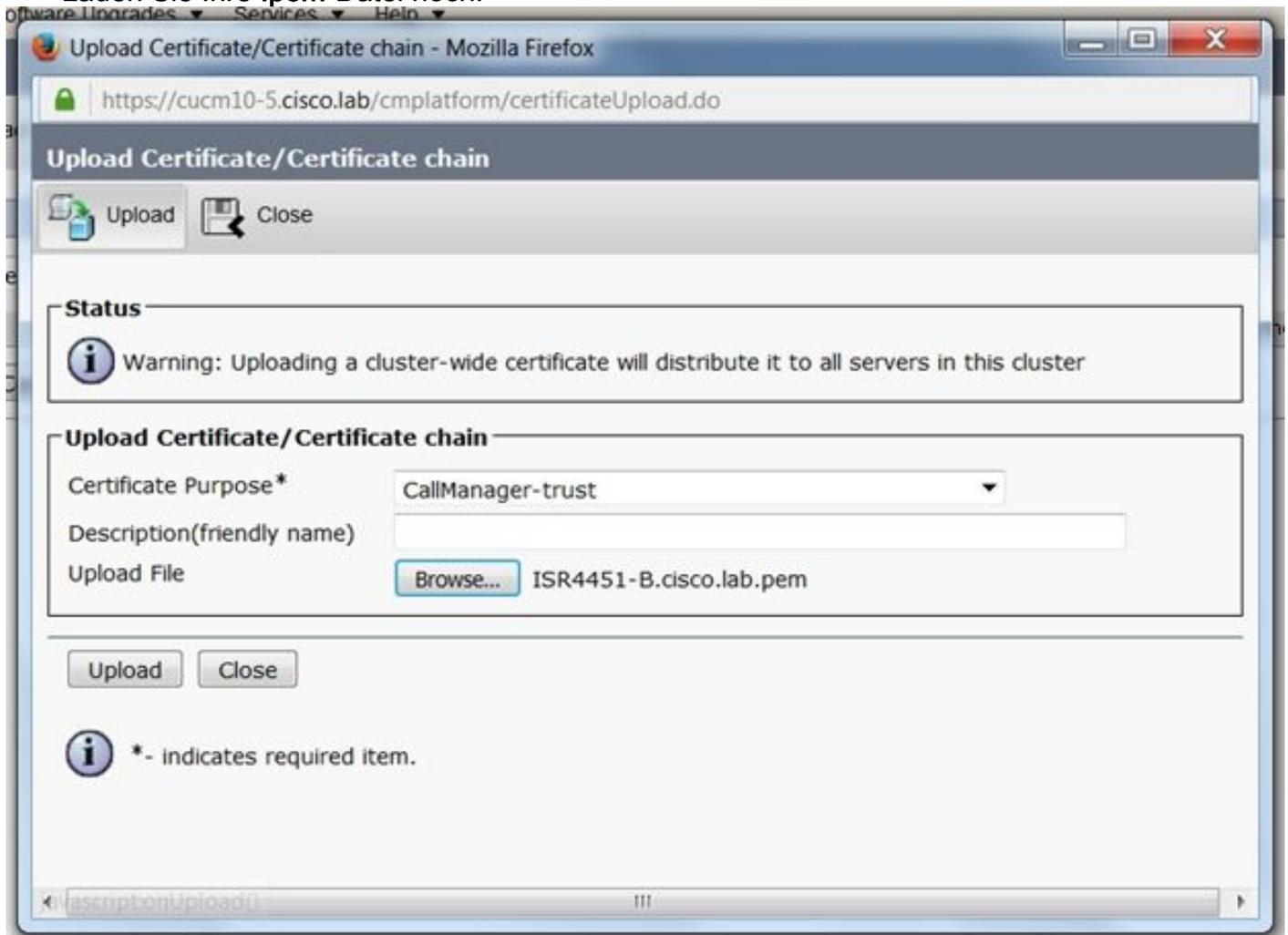
Kopieren Sie das oben erzeugte selbst signierte Zertifikat und fügen Sie es in eine Textdatei mit Dateierweiterung **.pem** ein

Das nachfolgende Beispiel wird als **ISR4451-B.ciscolab.pem** bezeichnet.



Schritt 4: Laden Sie das CUBE-Zertifikat in den CUCM hoch.

- CUCM-OS-Admin > Sicherheit > Zertifikatsverwaltung > Zertifikat/Zertifikatkette hochladen
- Zweck des Zertifikats = CallManager-Trust
- Laden Sie Ihre **.pem**-Datei hoch.



Schritt 5: Laden Sie das selbstsignierte Zertifikat des Call Managers herunter

- Suchen Sie das Zertifikat mit der Bezeichnung "Callmanager".
- Klicken Sie auf den Hostnamen.
- Klicken Sie auf PEM-Datei herunterladen.
- Speichern Sie die Datei auf Ihrem Computer

Cisco Unified Operating System Administration  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | CUCM

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

Schritt 6: Laden Sie das Zertifikat "Callmanager.pem" in CUBE hoch.

- Öffnen Sie Callmanager.pem mit einem Text-Datei-Editor.
- Kopieren des gesamten Inhalts der Datei
- Führen Sie diese Befehle auf CUBE aus

```
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

**Schritt 7: Konfigurieren Sie SIP so, dass der selbst erstellte Certificate Trustpoint von CUBE verwendet wird.**

```
sip-ua
```

```
crypto signaling default trustpoint CUBEtest
```

**Schritt 8: Konfigurieren der Dial-Peers mit 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
```

## Schritt 9: Konfigurieren eines CUCM-SIP-Trunk-Sicherheitsprofils

- CUCM-Admin-Seite > System > Security > SIP-Trunk-Sicherheitsprofil
- Konfigurieren Sie das Profil wie unten gezeigt.

**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

**Hinweis:** Es ist von entscheidender Bedeutung, dass das Feld X.509 mit dem zuvor beim Generieren des selbstsignierten Zertifikats konfigurierten CN-Namen übereinstimmt.

## Schritt 10: Konfigurieren eines SIP-Trunks auf dem CUCM

- Stellen Sie sicher, dass das Kontrollkästchen SRTP allowed aktiviert ist.
- Konfigurieren Sie die richtige Zieladresse, und ersetzen Sie Port 5060 durch Port 5061.

- Stellen Sie sicher, dass Sie das richtige SIP-Trunk-Sicherheitsprofil auswählen (das in Schritt 9 erstellt wurde).

**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

- Speichern und zurücksetzen Sie den Trunk.

## Überprüfen

Da Sie OPTIONS PING auf dem CUCM aktiviert haben, muss der SIP-Trunk den Status "VOLLDIENST" haben.

Name *	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			0711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

Der SIP-Trunk-Status zeigt den Full-Service an.

Der DFÜ-Peer-Status wird wie folgt angezeigt:

```
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:cucm10-5		active

## Fehlerbehebung

Aktivieren und Erfassen der Ausgabe dieser Debugger

```
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 Aufzeichnung Link:

<https://goo.gl/QOS1iT>