

# Configurer SIP TLS entre CUCM-CUBE/CUBE-SBC

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration Steps](#)

[Vérification](#)

[Dépannage](#)

Table des matières

## Introduction

Ce document aide à configurer SIP Transport Layer Security (TLS) entre Cisco Unified Communication Manager (CUCM) et Cisco Unified Border Element (CUBE)

### Conditions préalables

Cisco recommande de connaître ces sujets

- Protocole SIP
- Certificats de sécurité

### Conditions requises

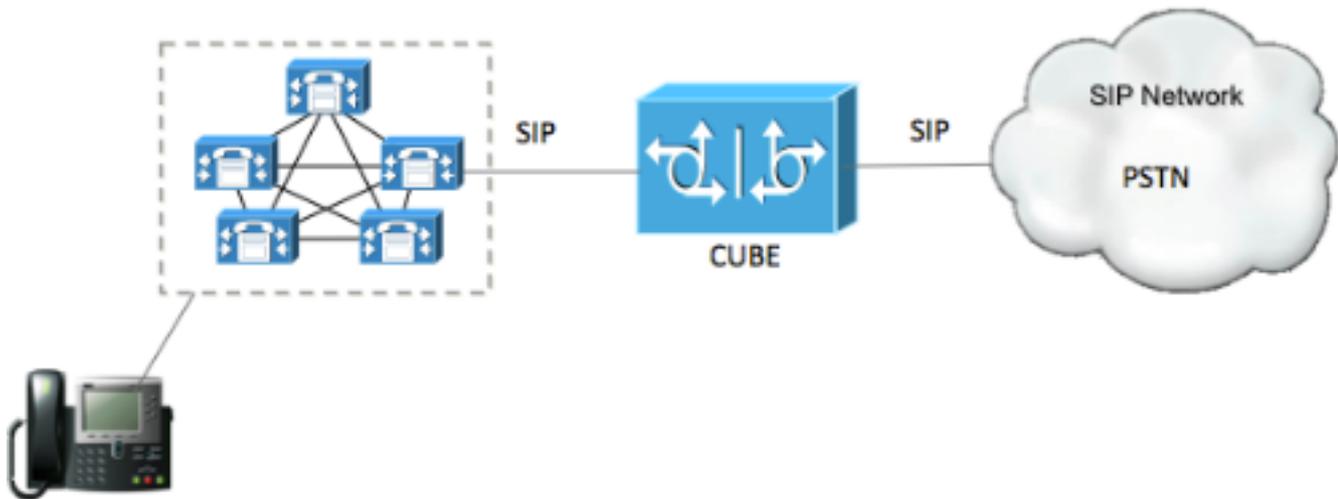
- La date et l'heure doivent correspondre sur les terminaux (il est recommandé d'avoir la même source NTP).
- CUCM doit être en mode mixte.
- La connectivité TCP est requise (Open port 5061 sur tout pare-feu de transit).
- Les licences de sécurité et UCK9 doivent être installées sur le CUBE.

### Components Used

- SIP
- Certificats autosignés

## Configuration

### Diagramme du réseau



## Configuration Steps

Étape 1. Créer un point de confiance afin de conserver le certificat autosigné de CUBE

```
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)
```

Étape 2. Une fois le point de confiance créé, exécutez la commande **Crypto pki enroll CUBEtest** afin d'obtenir des certificats auto-signés

```
crypto pki enroll CUBEtest

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

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

Si l'inscription était correcte, vous devez attendre le résultat suivant

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

Étape 3. Après avoir obtenu votre certificat, vous devez l'exporter

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

La commande ci-dessus doit générer le certificat ci-dessous

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

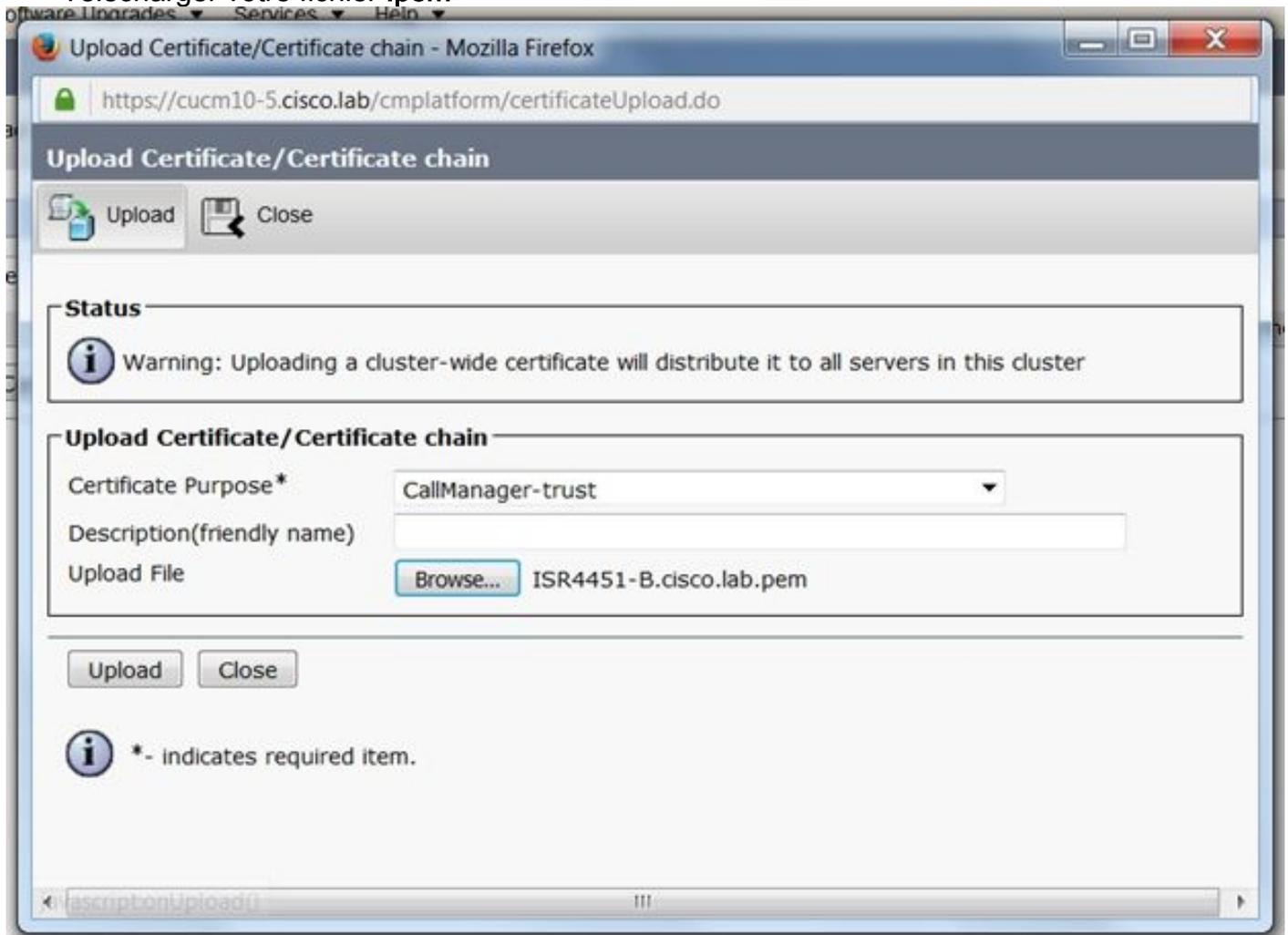
**Copiez le certificat auto-signé ci-dessus et collez-le dans un fichier texte avec l'extension de fichier .pem**

L'exemple ci-dessous porte le nom **ISR4451-B.ciscolab.pem**



#### Étape 4. Télécharger le certificat CUBE dans CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- Objet du certificat = CallManager-Trust
- Télécharger votre fichier **.pem**



#### Étape 5. Télécharger le certificat auto-signé du gestionnaire d'appels

- Rechercher le certificat qui indique Callmanager
- Cliquez sur le nom d'hôte
- Cliquez sur le fichier PEM téléchargé
- Enregistrer sur votre ordinateur

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

Étape 6. Télécharger le certificat Callmanager.pem sur CUBE

- Ouvrez Callmanager.pem avec un éditeur de fichier texte
- Copier l'intégralité du contenu du fichier
- Exécutez les commandes suivantes sur le 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
```

## Étape 7. Configurer SIP pour utiliser le point de confiance de certificat autosigné de CUBE

```
sip-ua
```

```
crypto signaling default trustpoint CUBEtest
```

## Étape 8. Configurer les terminaux de numérotation dial-peer avec 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
```

## Étape 9. Configurer un profil de sécurité de liaison SIP CUCM

- Page d'administration de CUCM > Système > Sécurité > Profil de sécurité de la liaison SIP
- Configurez le profil comme indiqué ci-dessous

**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

**Remarque** : il est essentiel que le champ X.509 corresponde au nom CN que vous avez configuré précédemment lors de la génération du certificat auto-signé

## Étape 10. Configurer une liaison SIP sur CUCM

- Assurez-vous que la case SRTP allowed est cochée
- Configurez l'adresse de destination appropriée et assurez-vous de remplacer le port 5060 par le port 5061

- Assurez-vous de sélectionner le profil de sécurité de ligne principale Sip correct (créé à l'étape 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

- Enregistrez et réinitialisez le trunk.

## Vérification

Puisque vous avez activé OPTIONS PING sur CUCM, la ligne principale SIP doit être dans l'état FULL SERVICE

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

L'état de la liaison SIP affiche le service complet.

L'état de l'homologue de numérotation s'affiche comme suit :

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

```
TAG      TYPE  MIN  OPER PREFIX      DEST-PATTERN      FER THRU SESS-TARGET  STAT PORT
KEEPALIVE

9999    voip  up   up           9999              0  syst dns:cucm10-5    active
```

## Dépannage

Activer et collecter la sortie de ces débogages

```
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
```

**Lien Enregistrement Webex :**

<https://goo.gl/QOS1iT>