

# Configurer SIP TLS entre CUCM-CUBE/CUBE-SBC avec des certificats signés CA

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérification](#)

—

[Dépannage](#)

## Introduction

Ce document décrit comment configurer SIP Transport Layer Security (TLS) entre Cisco Unified Communication Manager (CUCM) et Cisco Unified Border Element (CUBE) avec des certificats signés par l'autorité de certification (CA).

## 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 Security et Unified Communication K9 (UCK9) doivent être installées sur le CUBE.

**Note:** Pour la version 16.10 de Cisco IOS-XE, la plate-forme est passée à la licence Smart.

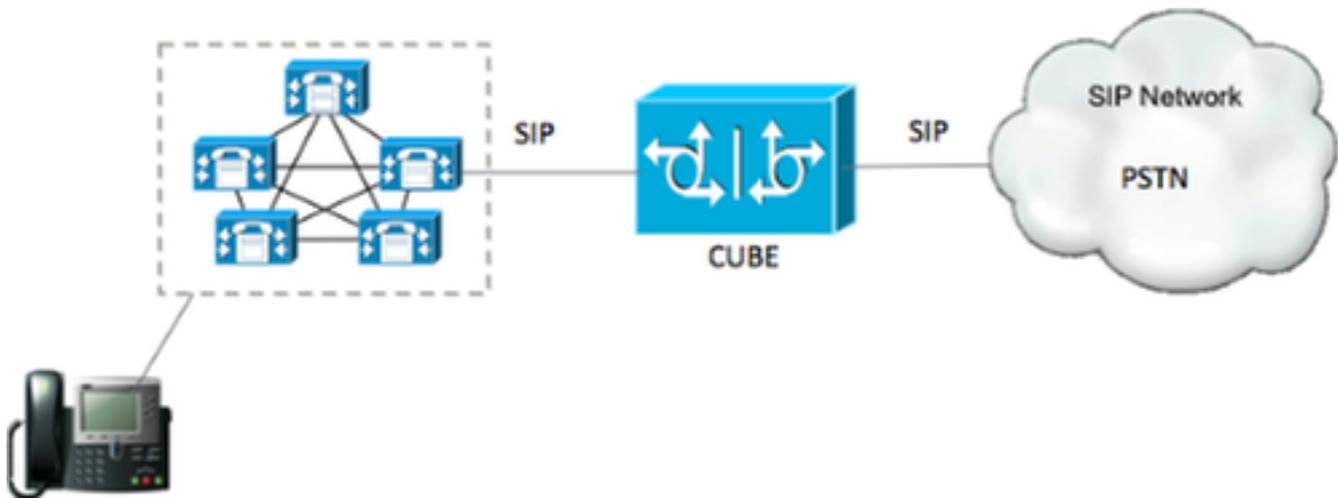
## Components Used

- SIP
- Certificats signés de l'autorité de certification

- Passerelles Cisco IOS et IOS-XE Versions 2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X : Plus de 15,4
- Gestionnaire de communications unifiées de Cisco (version CUCM) Versions : Plus de 10,5

## Configuration

### Diagramme du réseau



### Configuration

Étape 1. Vous allez créer une clé RSA correspondant à la longueur du certificat racine à l'aide de la commande suivante :

```
Crypto key generate rsa label TestRSAkey exportable modulus 2048
```

Cette commande crée une clé RSA d'une longueur de 2 048 bits (4 096 maximum).

Étape 2. Créez un point de confiance pour conserver notre certificat signé par l'autorité de certification à l'aide de commandes :

```
Crypto pki trustpoint CUBE_CA_CERT
serial-number none
fqdn none
ip-address none
subject-name cn=ISR4451-B.cisco.lab !(this has to match the router's hostname
[hostname.domain.name])
revocation-check none
rsakeypair TestRSAkey !(this has to match the RSA key you just created)
```

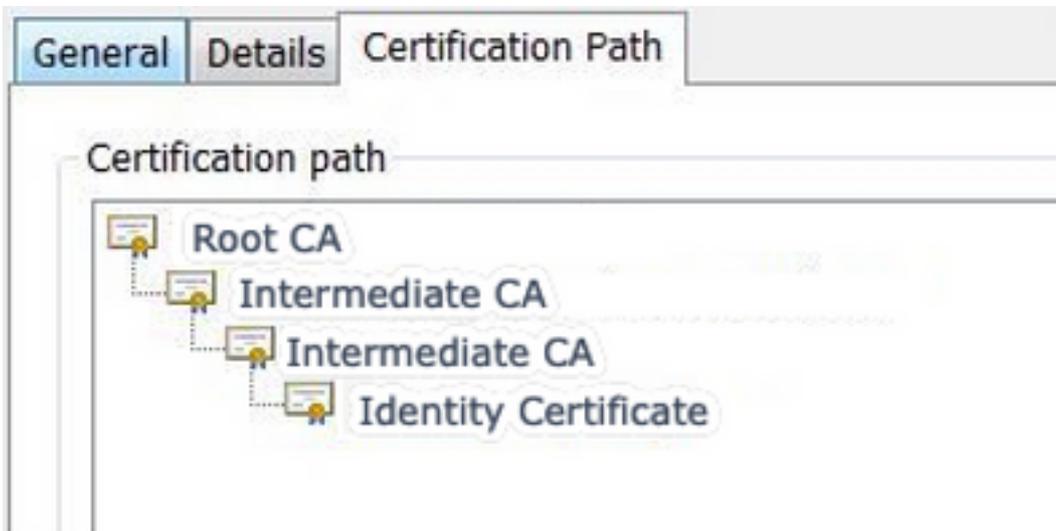
Étape 3. Maintenant que vous disposez de notre point de confiance, vous allez générer notre demande CSR avec les commandes suivantes :

```
Crypto pki enroll CUBE_CA_CERT
```

Répondez aux questions à l'écran, copiez la demande CSR, enregistrez-la dans un fichier, puis envoyez-la à l'AC.

Étape 4. Vous devez savoir si la chaîne de certificats racine possède des certificats intermédiaires ; s'il n'y a pas d'autorité de certification intermédiaire, passez à l'étape 7, sinon passez à l'étape 6.

Étape 5. Créez un point d'approbation pour conserver le certificat racine, plus, créez un point d'approbation pour conserver toute autorité de certification intermédiaire jusqu'à ce que celle qui signe notre certificat CUBE (voir l'image ci-dessous).



Dans cet exemple, le 1<sup>er</sup> niveau est l'autorité de certification racine, le 2<sup>e</sup> niveau est notre première autorité de certification intermédiaire, le 3<sup>e</sup> niveau est l'autorité de certification qui signe notre certificat CUBE, et par conséquent, vous devez créer un point de confiance pour détenir les 2 premiers certificats avec ces commandes.

```
Crypto pki trustpoint Root_CA_CERT
Enrollment terminal pem
Revocation-check none
```

```
Crypto pki authenticate Root_CA_CERT
Paste the X.64 based certificate here
```

```
Crypto pki trustpoint Intermediate_CA
Enrollment terminal
Revocation-check none
```

```
Crypto pki authenticate Intermediate_CA
```

Étape 6. Après avoir reçu notre certificat signé par l'autorité de certification, vous allez authentifier le point de confiance, le point de confiance doit détenir le certificat de l'autorité de certification juste avant le certificat CUBE ; la commande permettant d'importer le certificat est :

```
Crypto pki authenticate CUBE_CA_CERT
```

Étape 7. Une fois notre certificat installé, vous devez exécuter cette commande afin d'importer notre certificat CUBE

```
Crypto pki import CUBE_CA_CERT cert
```

Étape 8. Configurer SIP-UA pour utiliser le point de confiance que vous avez créé

```
sip-ua
crypto signaling default trustpoint CUBE_CA_CERT
```

Étape 9. Configurez les terminaux de numérotation dial-peer comme indiqué ci-dessous :

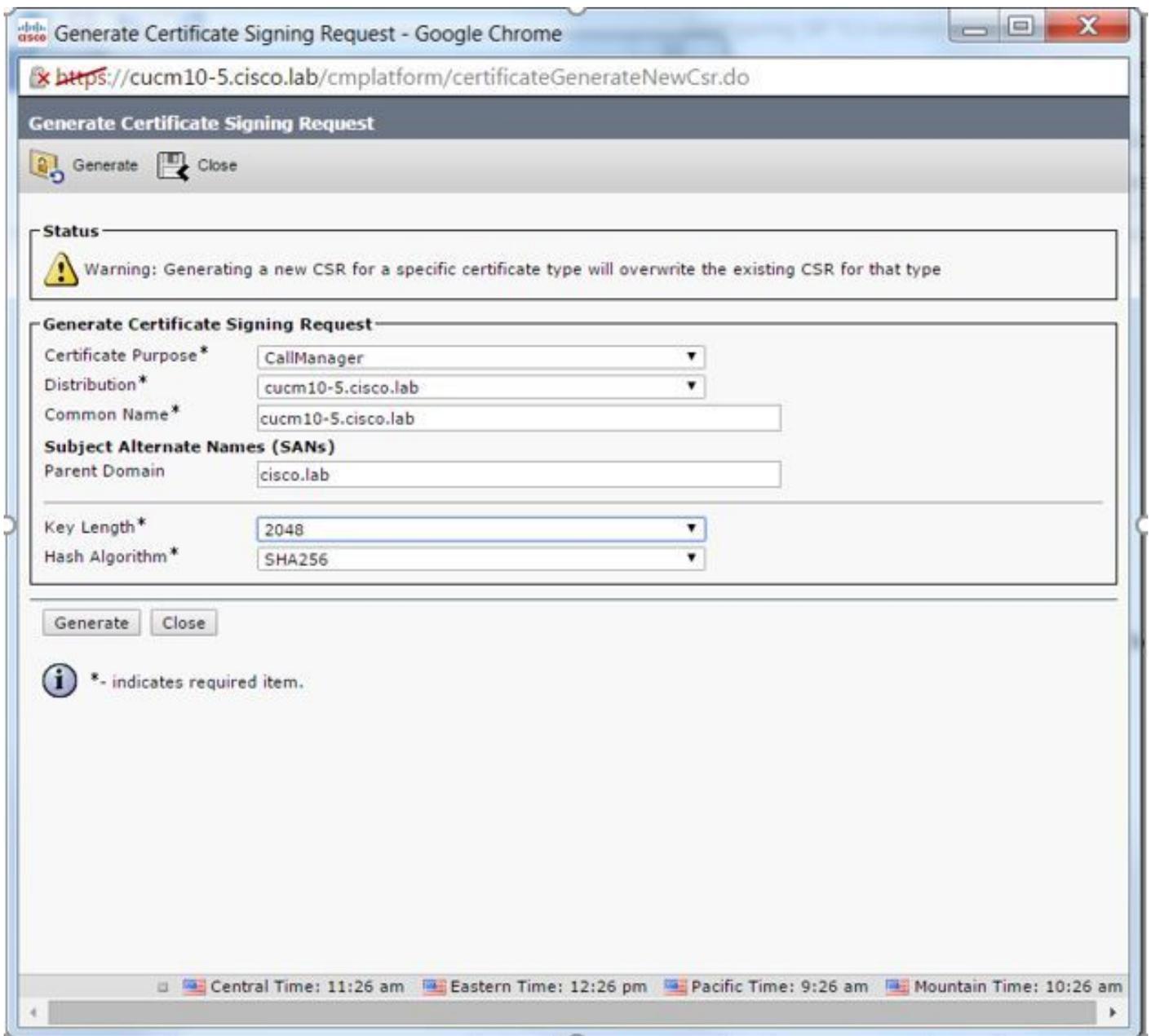
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

La configuration CUBE est alors terminée.

Étape 10. Maintenant, vous allez générer notre CSR CUCM, suivez les instructions ci-dessous

- Connectez-vous à l'administrateur de CUCM OS
- Cliquez sur Security
- Cliquez sur Gestion des certificats.
- Cliquez sur Générer CSR

La demande CSR doit être celle ci-dessous :



Étape 11. Téléchargez le CSR et envoyez-le à l'AC.

Étape 12. Téléchargez la chaîne de certificats signée par l'autorité de certification dans CUCM , les étapes sont les suivantes :

- Cliquez sur Security, puis sur Certificate Management.
- Cliquez sur Télécharger le certificat/la chaîne de certificats.
- Dans le menu déroulant de l'objectif du certificat, sélectionnez Call Manager.
- Accédez à votre fichier.
- Cliquez sur Charger.

Étape 13. Connectez-vous à l'interface de ligne de commande CUCM et exécutez cette commande

```
utils ctl update CTLFile
```

Étape 14. Configurer un profil de sécurité de liaison SIP CUCM

- Cliquez sur le système, puis sur security, puis sur sip trunk security profile

- Configurez le profil comme indiqué dans l'image,

### SIP Trunk Security Profile Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

---

#### Status

 Status: Ready

---

#### SIP Trunk Security Profile Information

|   |   |
|---|---|
| Name*   | CUBE_CA 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  | cucm10-5.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** : dans ce cas, le nom du sujet X.509 doit correspondre au nom du sujet du certificat CUCM comme indiqué dans la partie mise en surbrillance de l'image.

### Certificate Details for cucm10-5.cisco.lab, CallManager

Regenerate Generate CSR Download .PEM File Download .DER File

---

**Status**

 Status: Ready

---

**Certificate Settings**

|                            |  |
|----------------------------|--|
| Locally Uploaded           | 10/02/16                               |
| File Name                  | CallManager.pem                        |
| Certificate Purpose        | CallManager                            |
| Certificate Type           | certs                                  |
| Certificate Group          | product-cm                             |
| Description(friendly name) | Certificate Signed by AD-CONTROLLER-CA |

---

**Certificate File Data**

```
[
Version: V3
Serial Number: 1D255E0000000000000007
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: CN=AD-CONTROLLER-CA, DC=cisco, DC=lab
Validity From: Wed Feb 10 10:45:23 CST 2016
To: Fri Feb 10 10:55:23 CST 2017
Subject Name: CN=cucm10-5.cisco.lab, OU=TAC, O=CISCO, L=RICHARSON, ST=TEXAS, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100ae8db062881c35163f1b6ee4be4951158fdb3495d3c8032170c9fb8bafb385a2
27b00ec1024807f0adc49df875189779c7de1ae1e7e64b45e6f9917fa6ca5687d9aeaf20d70018e8d5
58a832360b82702249fc98855012c7d2cc29eea0f92fad9e739d73b0fa24d7dd4bd9fc96be775fda997
f03a440645ad64fa9f083ed95445e200187dd8775aa543b2bab11a5e223e23ef03bb86bb9fd969b3d9
3ba2550c35ea06ed5149aef2253c2455a622122e0aa3b649a090911995069a2cfd4ab4ab1fe15b242
```

Regenerate Generate CSR Download .PEM File Download .DER File

Étape 15. Configurez une liaison SIP comme vous le feriez normalement 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.
- Dans le profil de sécurité de la ligne principale SIP, assurez-vous de sélectionner le nom du profil SIP créé à l'étape 14.

**SIP Information**

**Destination**

Destination Address is an SRV

Destination Address: 1\* [redacted]      Destination Address IPv6:      Destination Port: 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

## Vérification

À ce stade, si toute la configuration est correcte,

Sur CUCM, l'état de la liaison SIP affiche Full Service, comme l'illustre l'image,

| 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 |

Sur CUBE, l'homologue de numérotation affiche l'état suivant :

```
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
```

Ce même processus s'applique aux autres routeurs, la seule différence est qu'au lieu d'une étape pour télécharger le certificat CUCM, téléchargez le certificat fourni par un tiers.

## Dépannage

Activer ces débogages sur CUBE

```
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
```