# Configurez le TLS de SIP entre CUCM-CUBE/CUBE-SBC avec les Certificats signés CA

## Contenu



## Introduction

Ce document décrit comment configurer le Transport Layer Security de SIP (TLS) entre le gestionnaire de Cisco Unified Communications (CUCM) et le Logiciel Cisco Unified Border Element (CUBE) avec l'Autorité de certification (CA) - les Certificats signés.

## Conditions préalables

Cisco recommande avoir la connaissance de ces sujets

- Protocole de SIP
- Certificats de Sécurité

### Exigences

- La date et l'heure doivent s'assortir sur les points finaux (il est recommandé pour avoir le même ntp source).
- CUCM doit être dans le mode mixte.
- La Connectivité de TCP est exigée (port ouvert 5061 sur tout Pare-feu de transit).
- Le CUBE doit avoir la Sécurité et les permis unifiés de la transmission K9 (UCK9) installés.

  Remarque: Pour des onawards de version 16.10 de Cisco IOS XE la plate-forme s'est déplacée à l'autorisation intelligente.

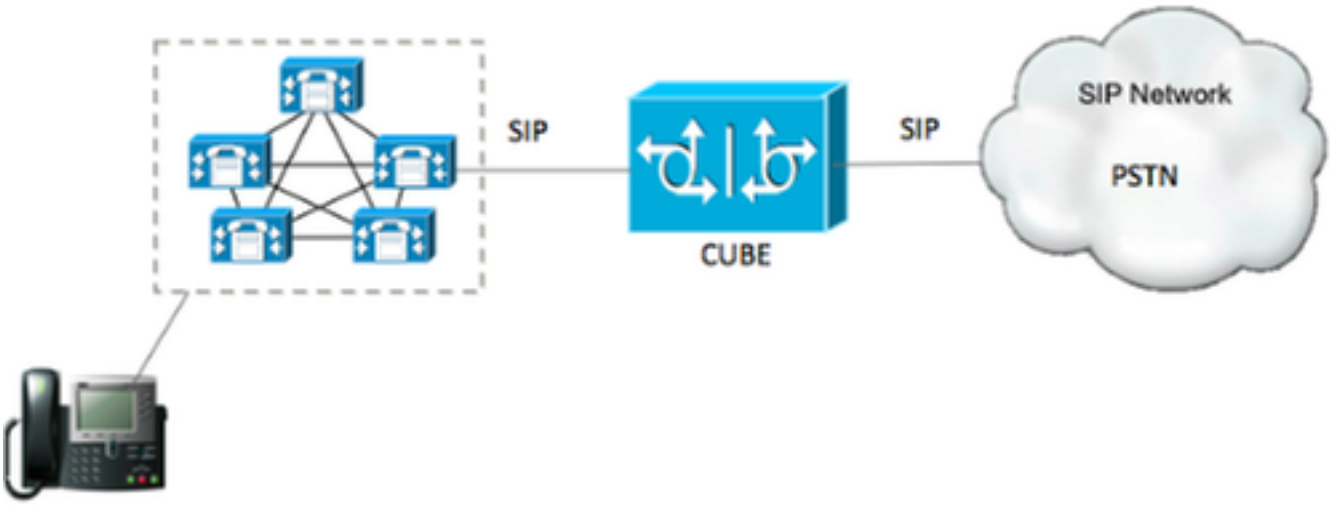
### Composants utilisés

- SIP
- Certificats signés de Certificate Authority

- Cisco IOS et passerelles IOS-XE2900/3900/4300/4400/CSR1000v/versions ASR100X : 15.4+
- Gestionnaire de communications unifiées de Cisco (version CUCM)Versions : 10.5+

# Configurer

## Diagramme du réseau




## Configuration

Étape 1. Vous allez créer une clé RSA appariant la longueur de certificat du certificat racine utilisant la commande :

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

Cette commande crée une clé RSA avec une longueur de 2048 bits (le maximum est 4096).

Étape 2. Créez un point de confiance pour tenir notre certificat Ca-signé utilisant des 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 avez notre point de confiance, vous allez générer notre demande CSR avec les commandes ci-dessous :

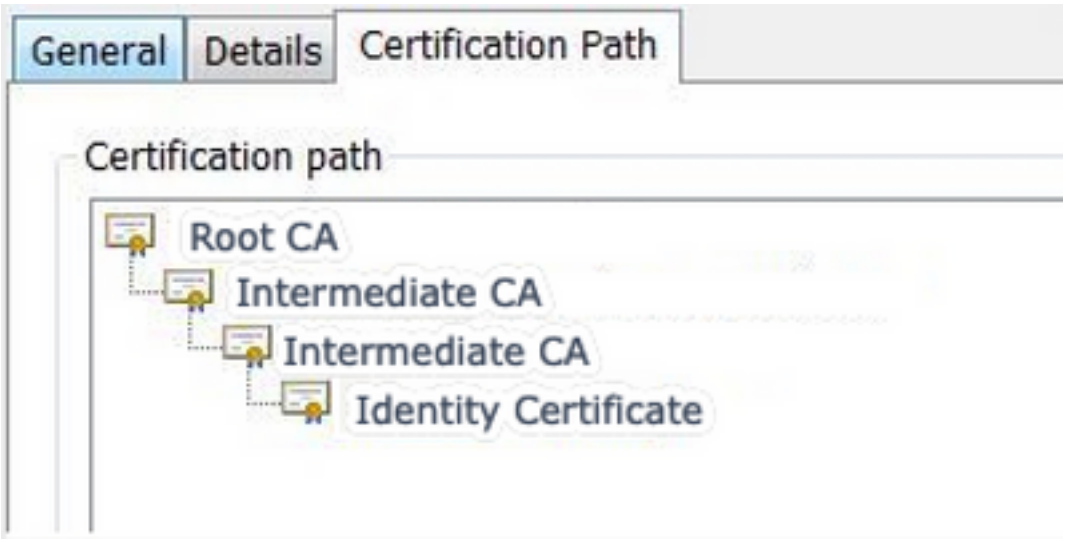
```
 Crypto pki enroll CUBE_CA_CERT
```

Répondez aux questions sur l'écran, puis copiez la demande CSR, sauvegardez-la à un fichier et puis envoyez-la au CA.

Étape 4. Vous devez découvrir si la chaîne de certificat racine a des Certificats intermédiaires ; au

cas où il n'y aurait aucune autorité de certification intermédiaire, l'accès à l'étape 7, autrement, continuent sur l'étape 6.

Étape 5. Créez un point de confiance pour tenir le certificat racine, plus, créez un point de confiance pour tenir n'importe quelle intermédiaire CA jusqu'à celui qui signe notre certificat de CUBE (voir l'image ci-dessous).




Dans cet exemple, le 1er niveau est la racine CA, le 2ème niveau est notre première intermédiaire CA, le 3ème niveau est le CA qui signe notre certificat de CUBE, et ainsi, vous devez créer un point de confiance pour tenir 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
<Paste the X.64 based certificate here>
```

Étape 6. Après réception de notre certificat Ca-signé, vous allez authentifier le point de confiance, le point de confiance doit tenir le certificat du CA juste avant que certificat de CUBE ; la commande qui laisse importer le certificat est,

```
Crypto pki authenticate CUBE_CA_CERT
<Paste the X.64 based certificate here>
```

Étape 7. Une fois que vous faites installer notre certificat, vous devez exécuter cette commande afin d'importer notre certificat de CUBE

```
  Crypto pki import CUBE_CA_CERT cert
<Paste the X.64 based certificate here>
```

Étape 8. Configurez le 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 pairs de cadran comme affiché ci-dessous :

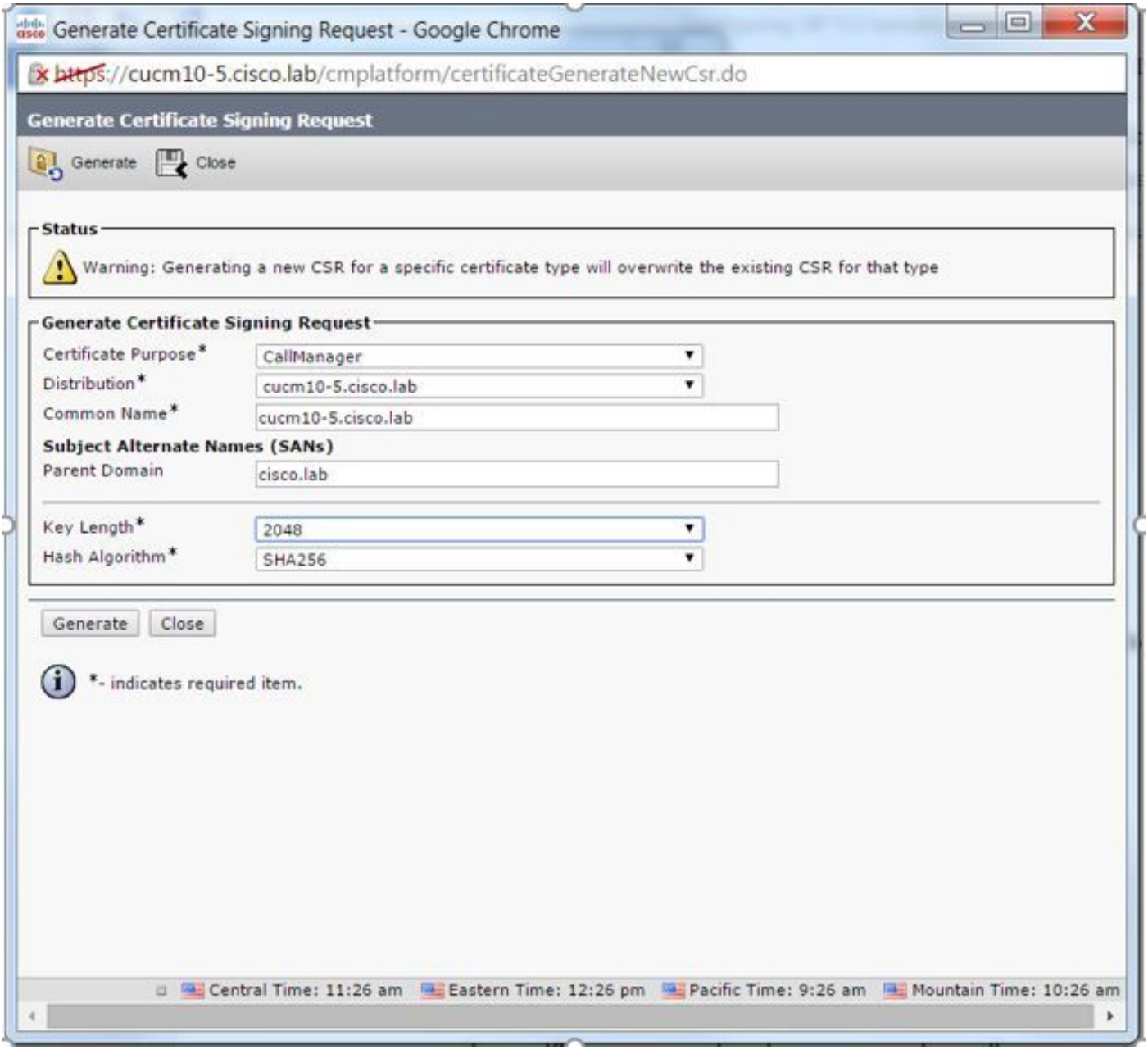
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

Avec ceci, la configuration de CUBE est complète.

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

- Procédure de connexion à l'administrateur de SYSTÈME D'EXPLOITATION CUCM
- Cliquez sur en fonction la Sécurité
- Cliquez sur en fonction la Gestion de certificat.
- Cliquez sur génèrent en fonction le CSR

La demande CSR doit regarder en tant que celle ci-dessous :




Étape 11. Téléchargez le CSR et envoyez-le au CA.

Étape 12. Téléchargez la chaîne de certificat Ca-signée au CUCM, des étapes sont :

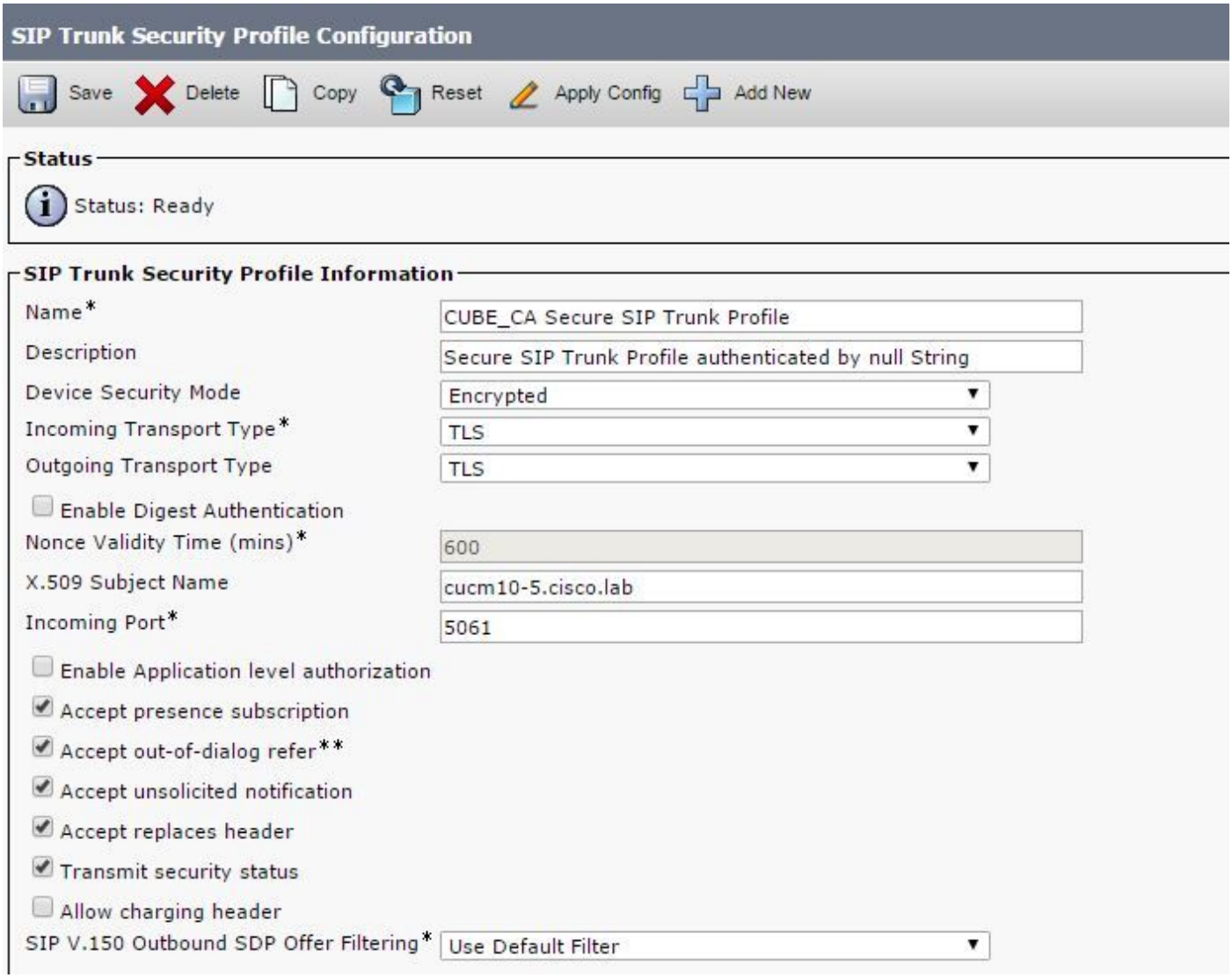
- Cliquez sur en fonction la Gestion de Sécurité et puis de certificat.
- Cliquez sur en fonction le certificat de téléchargement/chaîne de certificat.
- Sur le menu déroulant de but de certificat, gestionnaire d'appel choisi.
- Parcourez à votre fichier.
- Cliquez sur en fonction le téléchargement.

Étape 13. Ouvrez une session au CUCM CLI et exécutez cette commande

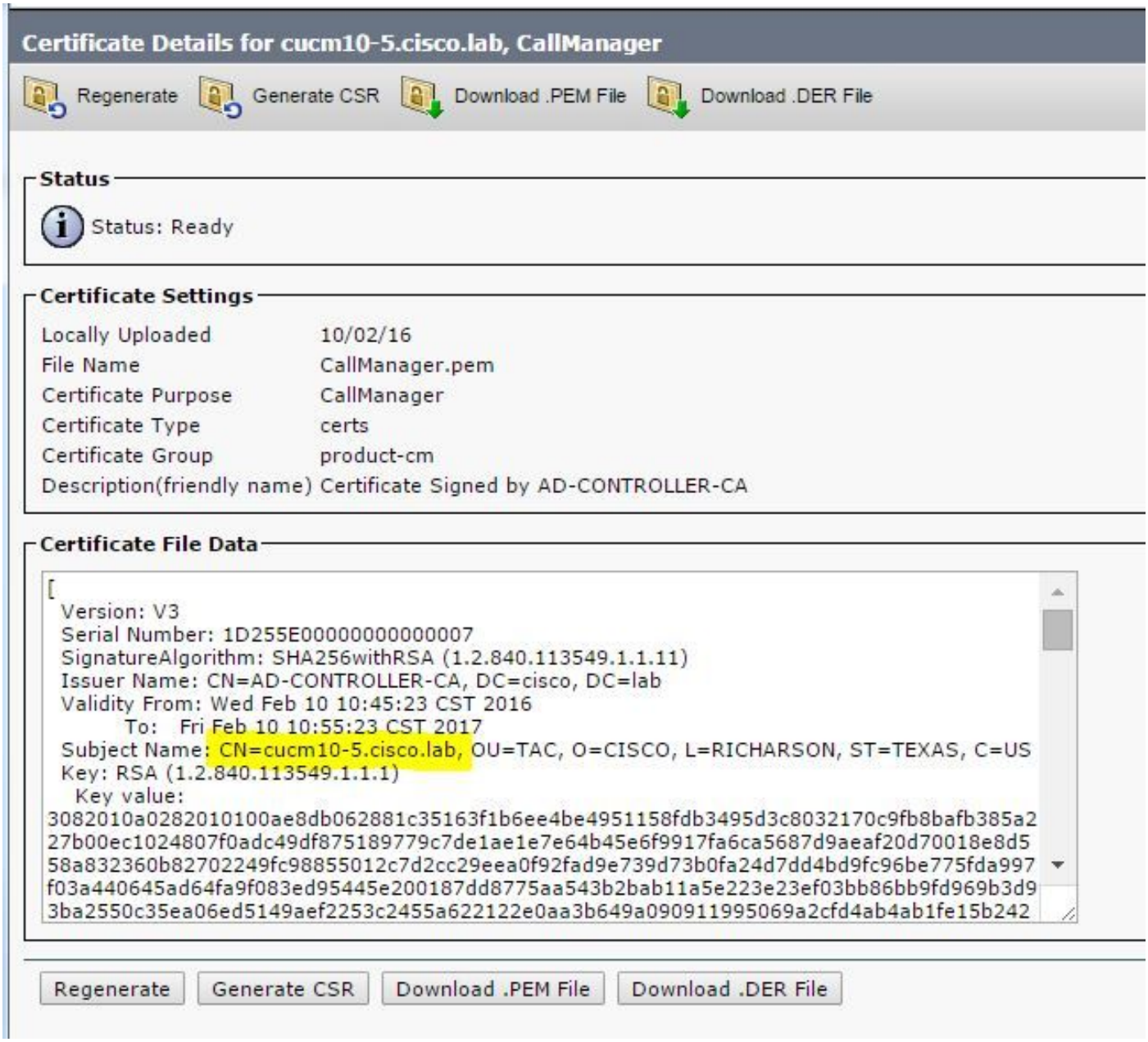
```
utils ctl update CTLFile
```

Étape 14. Configurez un profil de Sécurité de joncteur réseau de SIP CUCM

- Cliquez sur en fonction le système, puis la Sécurité et sirotez alors le profil de Sécurité de joncteur réseau
- Configurez le profil suivant les indications de l'image,




Remarque: Dans ce cas, le nom du sujet X.509 doit apparier le nom du sujet de certificat CUCM suivant les indications de la partie mise en valeur de l'image.




Étape 15. Configurez un joncteur réseau de SIP car vous feriez normalement sur le CUCM

- Assurez que la case permise par SRTP est cochée.
- Configurez l'adresse de destination appropriée et l'assurez pour remplacer le port 5060 par le port 5061.
- Sur le profil de Sécurité de joncteur réseau de SIP, assurez pour sélectionner le nom de profil de SIP créé sur l'étape 14.


# Vérifiez

Àce moment, si toute la configuration est CORRECTE,

Sur CUCM l'état de jonction de SIP affiche le service complet, suivant les indications de l'image,


Sur le CUBE le pair de cadran affiche cet état :

```
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 applique à d'autres Routeurs, la seule différence est celui au lieu de l'étape pour télécharger le certificat CUCM, téléchargent le certificat fourni par le tiers.

# Dépanner

Activez ces débogages sur le 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
```