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

Contenu

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.

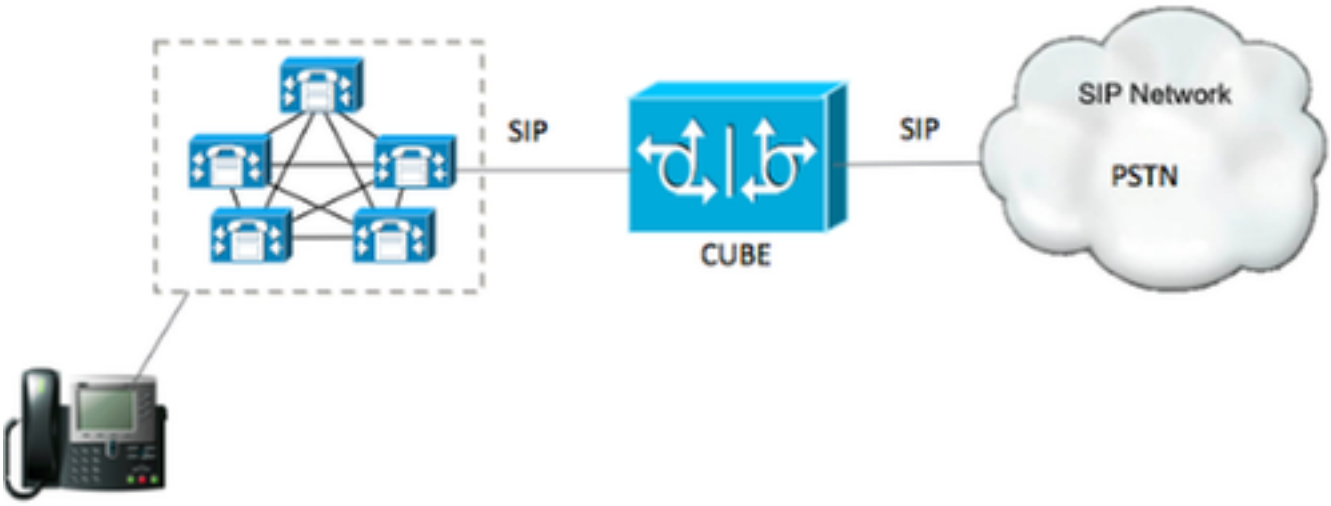
Components Used

- SIP
- Certificats signés de l'autorité de certification

- Passerelles Cisco IOS et IOS-XEVersions 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)
```

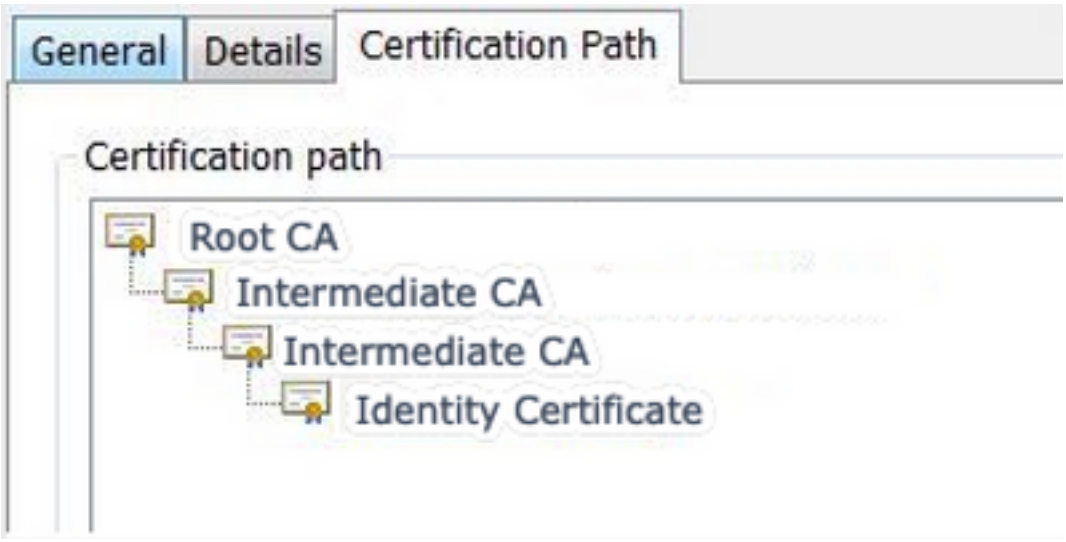
Étape 3. Maintenant que vous disposez de notre point de confiance, vous allez générer notre demande CSR avec les commandes suivantes :

```
 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 1er niveau est l'autorité de certification racine, le 2e niveau est notre première autorité de certification intermédiaire, le 3e 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 :

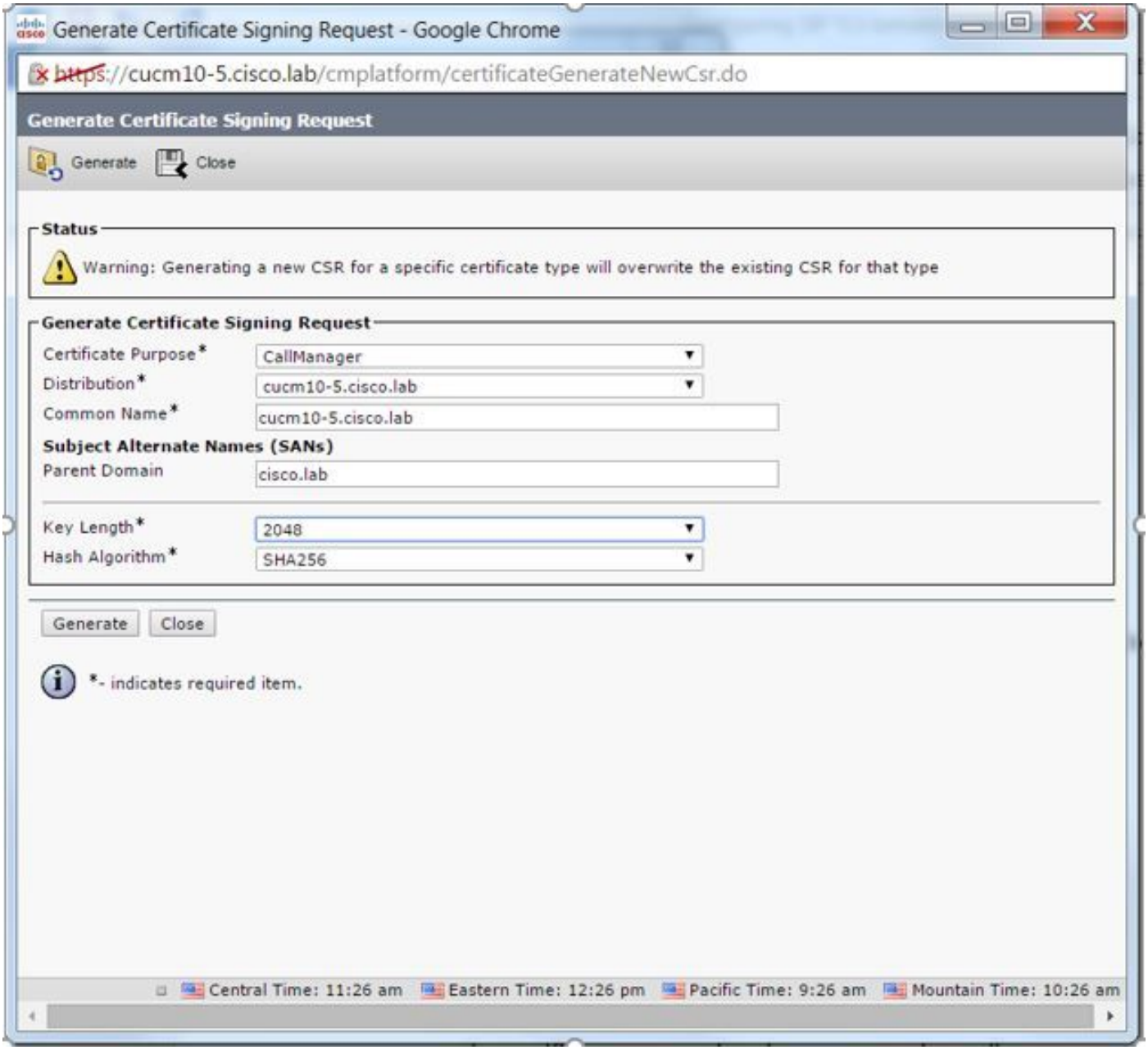
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

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.

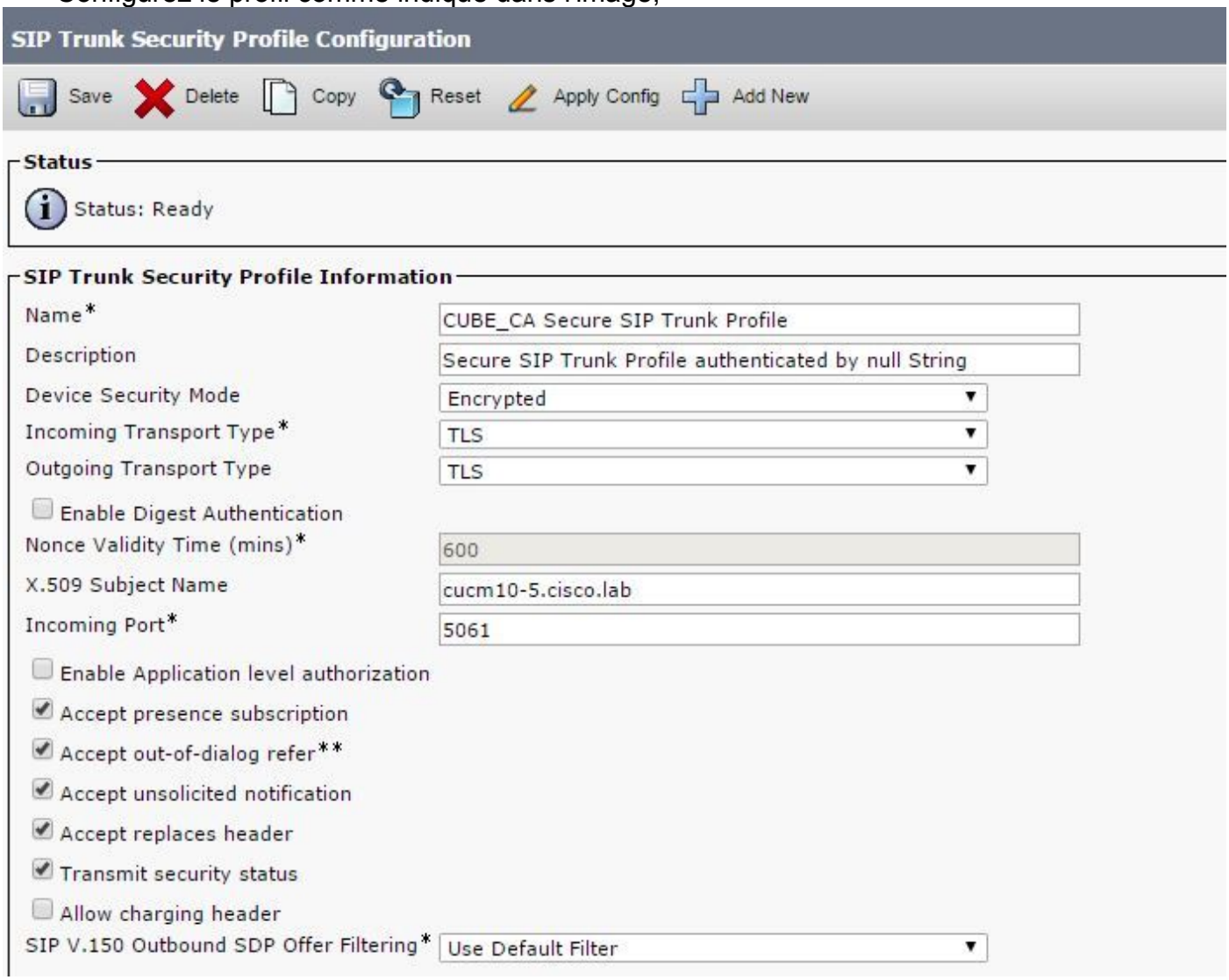
Étape 13. Connectez-vous à l'interface de ligne de commande CUCM et exécutez cette commande

```
utils ctl update CTLFile
```

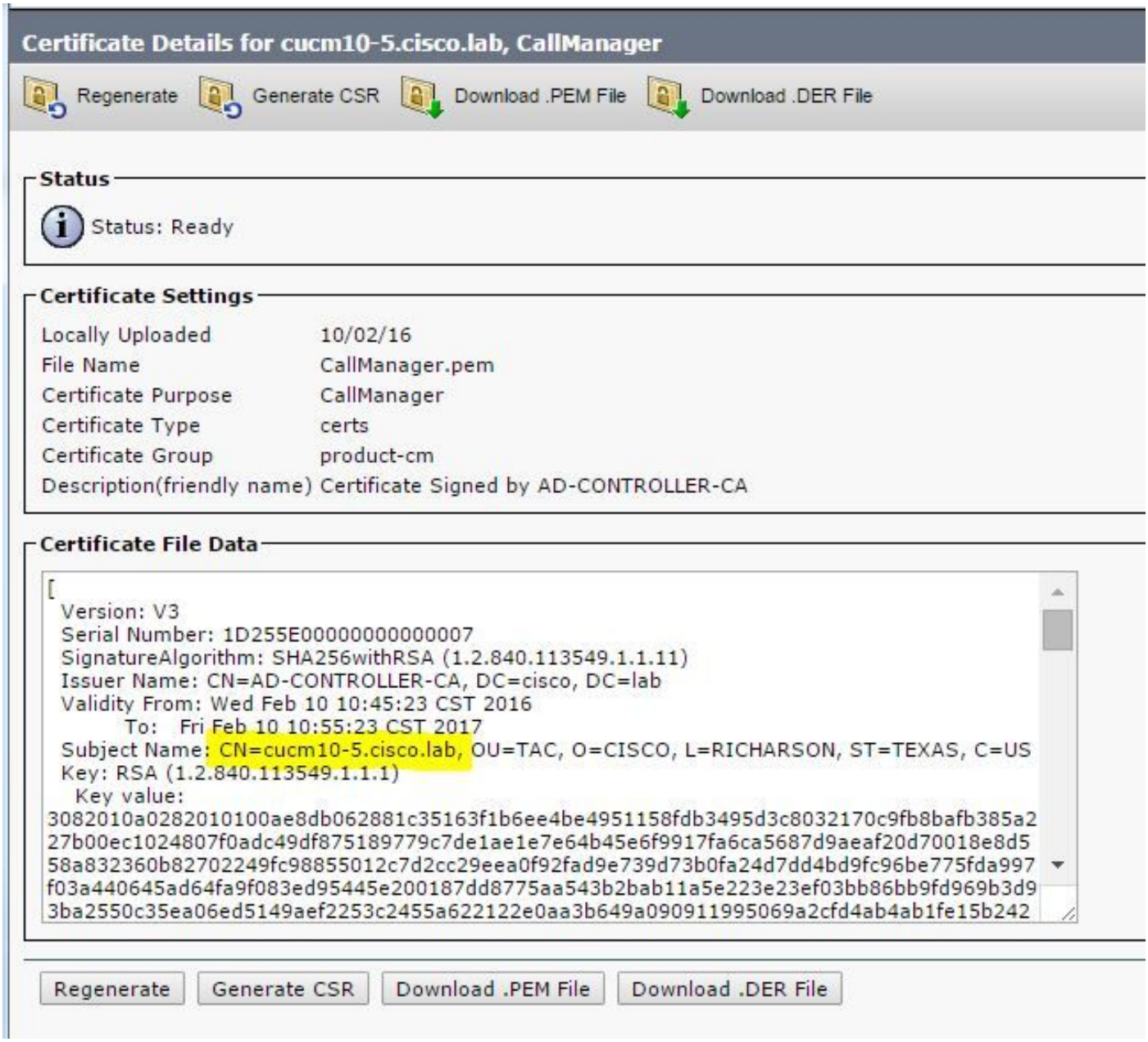
Étape 14. Configurer un profil de sécurité de liaison SIP CUCM

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

- Configurez le profil comme indiqué dans l'image,



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.



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.

Vérification

Àce stade, si toute la configuration est correcte,

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

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
```