Configurer SIP TLS entre CUCM-CUBE/CUBE-SBC

Table des matières

[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Configurer](#)

- [Diagramme du réseau](#)
- [Étapes de configuration](#)

[Vérifier](#)

[Dépannage](#)

Table des matières

Introduction

Ce document aide à configurer la sécurité de la couche transport SIP (TLS) entre Cisco Unified Communication Manager (CUCM) et Cisco Unified Border Element (CUBE)

Conditions préalables

Cisco recommande d'avoir des connaissances sur ces sujets

- Protocole SIP
- Certificats de sécurité

Exigences

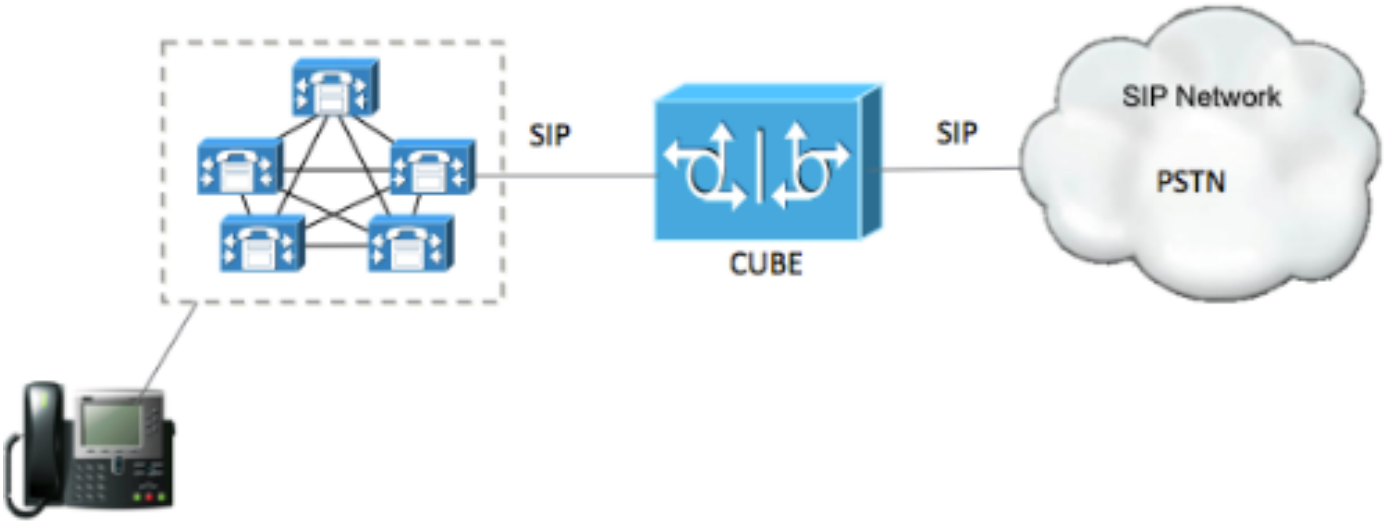
- La date et l'heure doivent correspondre sur les terminaux (il est recommandé d'avoir la même source NTP).
- CUCM doit être en mode mixte.
- La connectivité TCP est requise (port ouvert 5061 sur tout pare-feu de transit).
- Le CUBE doit disposer des licences de sécurité et UCK9.

Composants utilisés

- SIP
- Certificats auto-signés

Configurer

Diagramme du réseau



Étapes de configuration

Étape 1. Créer un point de confiance afin de contenir le certificat auto-signé 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 est correcte, vous devez vous attendre à ce que cette sortie

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

Étape 3. Après avoir obtenu le 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
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
```

```
AOsAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/eOb2zq6CrIj4T1t+NSlG5sjMJ919/ix

7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB

Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM

tVKinW/q6yDXO7WXK3SETCj6MAOGCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

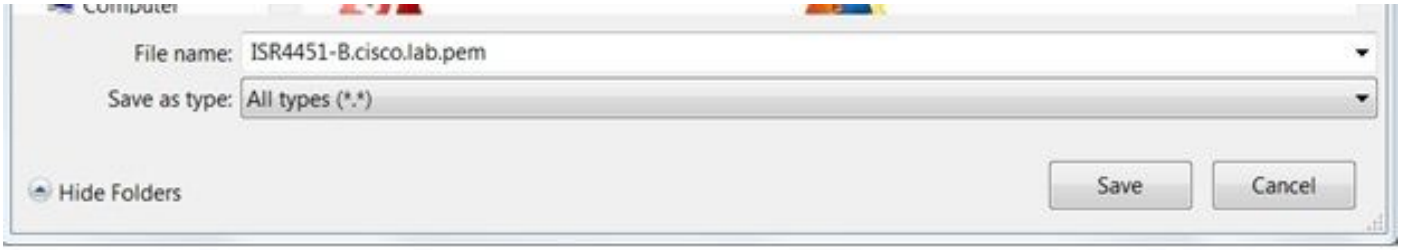
T88SHXqOEVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

-----END CERTIFICATE-----
```

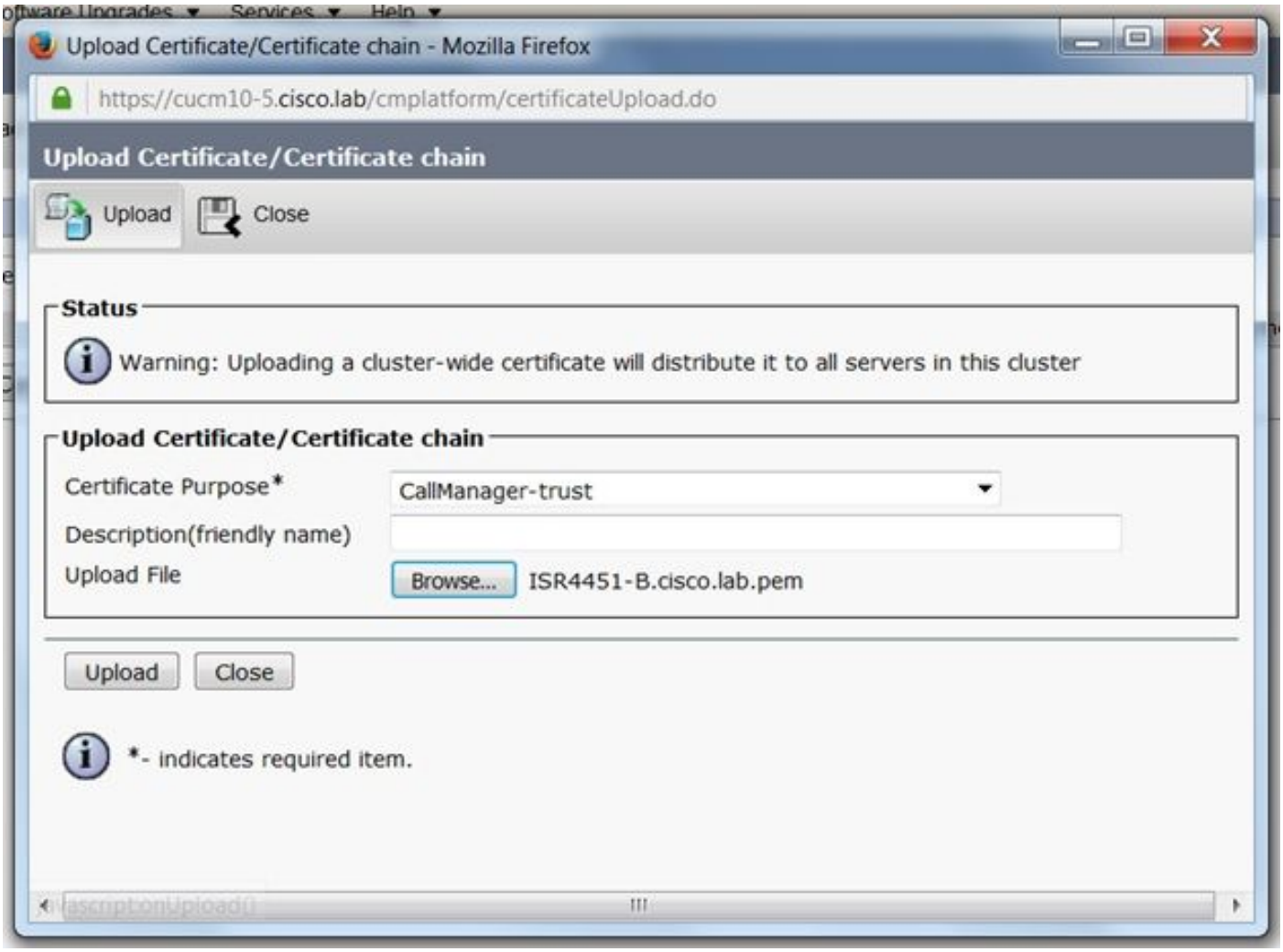
Copiez le certificat auto-signé généré ci-dessus et collez-le dans un fichier texte avec l'extension de fichier .pem

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



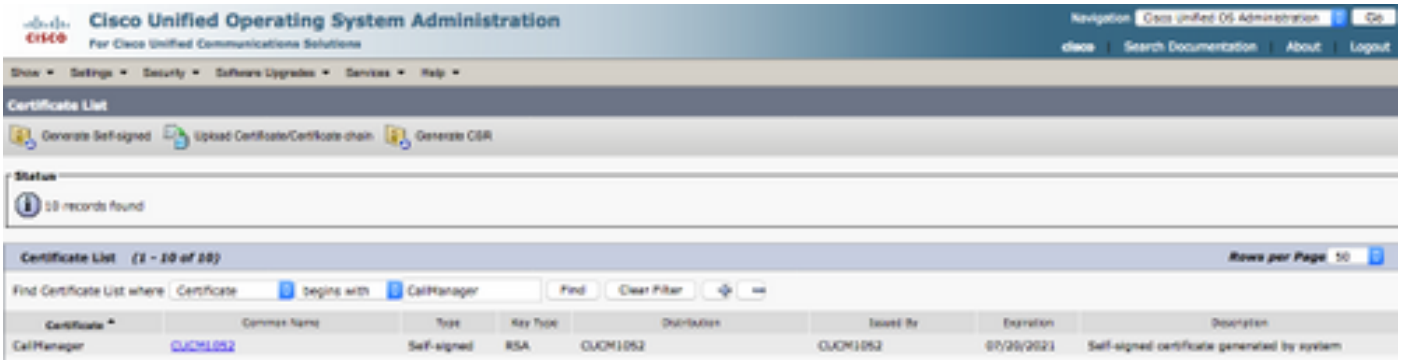
Étape 4. Téléchargez le certificat CUBE sur le CUCM

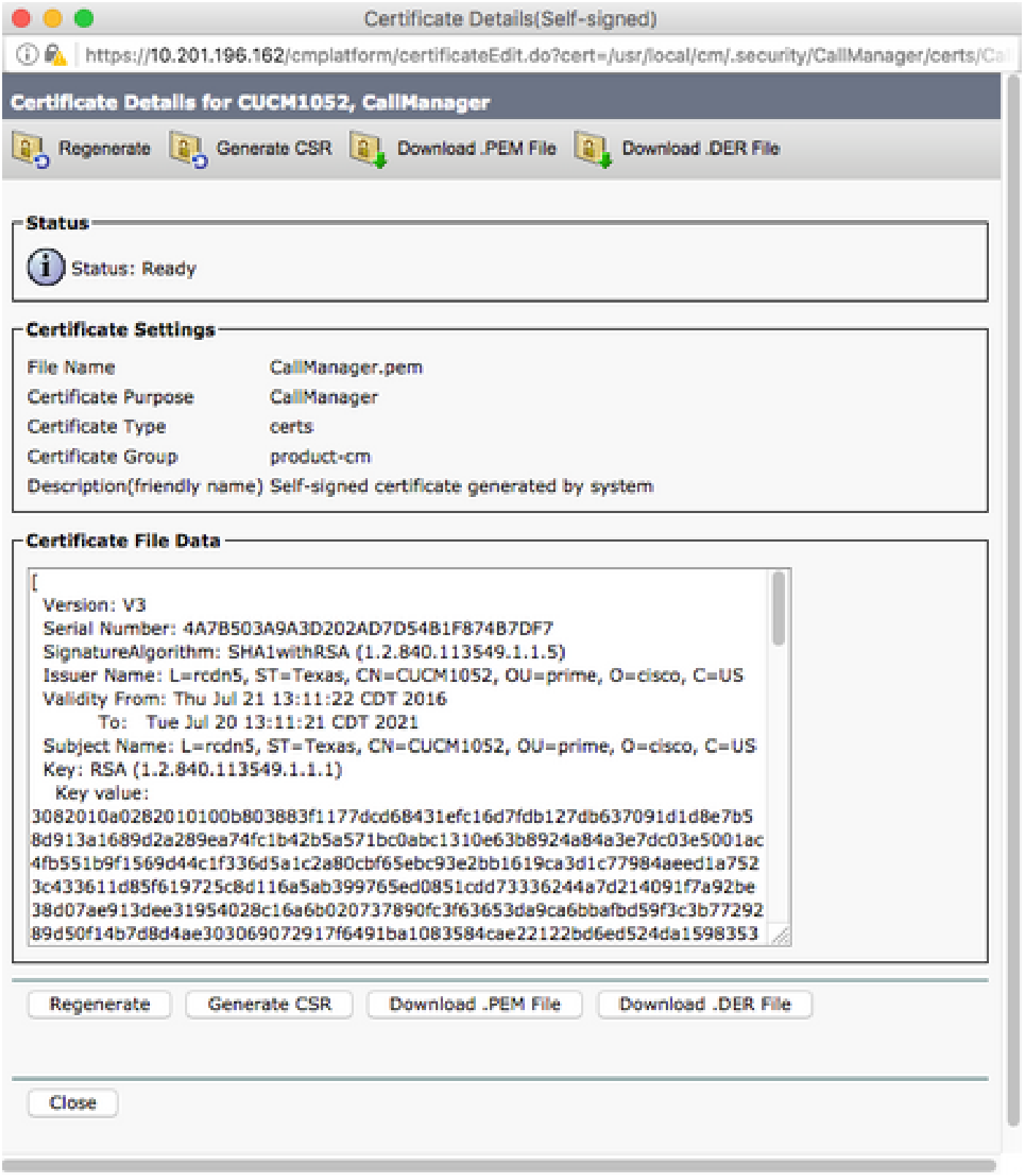
- CUCM OS Admin > Sécurité > Gestion des certificats > Télécharger le certificat/la chaîne de certificats
- Fonction du certificat = CallManager-Trust
- Téléchargez votre fichier .pem



Étape 5. Télécharger le certificat autosigné du gestionnaire d'appels

- Recherchez le certificat qui indique Callmanager
- Cliquez sur le nom d'hôte
- Cliquez sur télécharger le fichier PEM
- Enregistrez-le sur votre ordinateur





Étape 6. Télécharger le certificat Callmanager.pem dans CUBE

- Ouvrez le fichier Callmanager.pem avec un éditeur de fichier texte
- Copier tout le contenu du fichier
- Exécutez les commandes this 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 : configuration du protocole SIP pour utiliser le point de confiance de certificat autosigné de CUBE

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

Étape 8. Configuration des 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

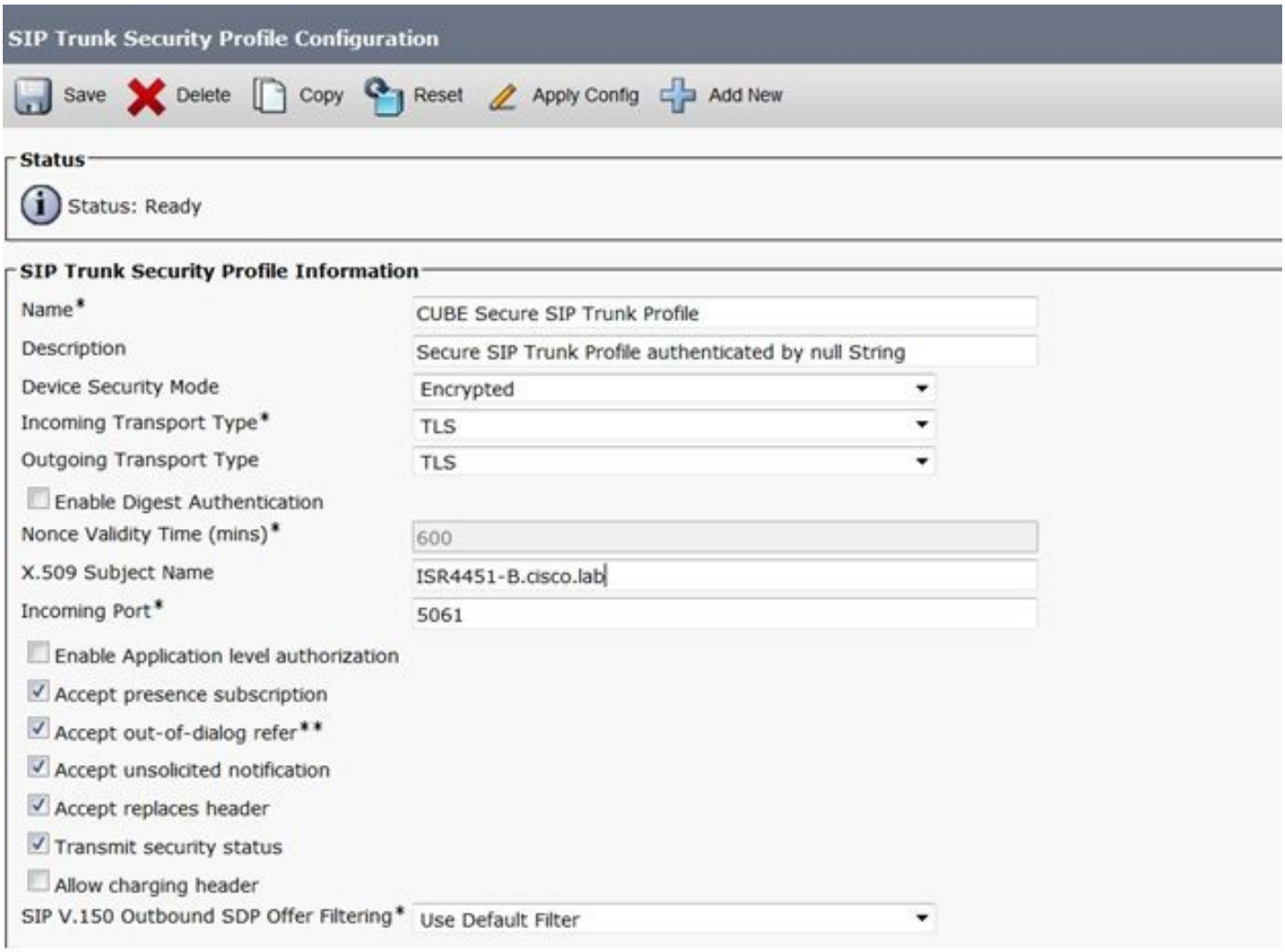
 session transport tcp tls

 voice-class sip options-keepalive

 srtp
```

Étape 9. Configuration d’un profil de sécurité de ligne principale SIP CUCM

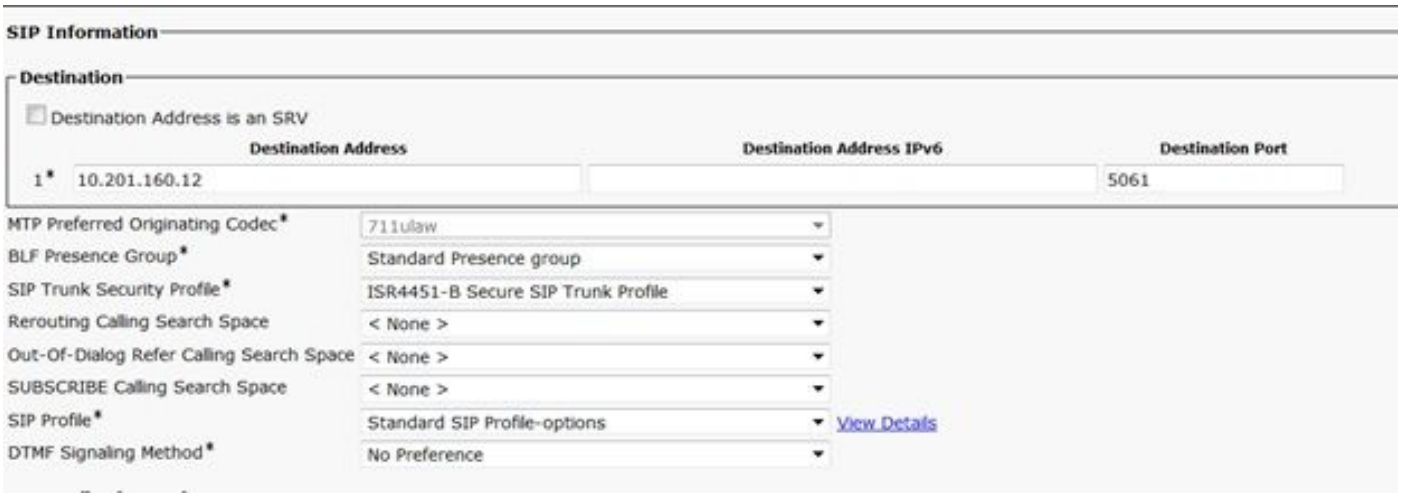
- Page d'administration de CUCM > Système > Sécurité > Profil de sécurité de la ligne principale SIP
- Configurez le profil comme indiqué ci-dessous



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

Étape 10. Configuration d'une ligne principale SIP sur CUCM

- Vérifiez 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)



- Enregistrez et réinitialisez le trunk.

Vérifier

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



L'état de la ligne principale SIP indique un service complet.

L'état du terminal de numérotation dial-peer est le suivant :

```
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 les résultats 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 d'enregistrement Webex :

https://goo.gl/QOS1iT

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.