Certificat CAPF signé par CA pour CUCM

Contenu

Introduction

Ce document décrit comment obtenir un certificat de la fonction de proxy d'autorité de certification (CAPF) signé par Autorité de certification (CA) pour Cisco Unified Communications Manager (CUCM). Il y a toujours des demandes de signer le CAPF avec le CA externe. Ce document affiche pourquoi comprendre comment cela fonctionne est aussi important que la procédure de configuration.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Infrastructure à clé publique (PKI)
- Configuration de sécurité CUCM

Composants utilisés

Les informations dans ce document sont basées sur la version 8.6 et ultérieures de Cisco Unified Communications Manager.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Limite

Le CA différent pourrait avoir des demandes différentes au CSR. Il y a des signaler que la différente version d'OpenSSL CA font demander une certaine particularité les travaux CSR cependant Microsoft Windows CA bien avec le CSR de Cisco CAPF jusqu'ici, que la discussion ne sera pas couvert en cet article.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Microsoft Windows Server 2008 CA.
- Cisco Jabber pour Windows (les différents vervions pourraient avoir le nom différent pour que le répertoire enregistre le LSC).

Informations générales

But de CAPF signé par CA

Quelques clients voudraient aligner avec le whith globle de stratégie de certificat que la société tellement il y a un besoin a signé le CAPF avec le même CA que d'autres serveurs.

Mécanisme pour ce PKI

Par défaut, localement - le certificat significatif (LSC) est signé par le CAPF, ainsi le CAPF est le CA pour des téléphones dans ce scénario. Cependant, quand vous essayez d'obtenir le CAPF signé par le CA externe, puis le CAPF dans ce scénario agit en tant que subalterne CA ou intermédiaire CA.

La différence entre CAPF auto-signé et CAPF Ca-signé est : le CAPF est la racine CA au LSC en faire CAPF auto-signé, le CAPF est le subalterne (intermédiaire) CA au LSC en faire CAPF Ca-signé.

Comment CSR CAPF est différent de l'autre CSRs ?

Considérant à RFC5280, l'extension d'utilisation principale définit le but (par exemple, chiffrement, signature, certificat signant) de la clé contenue dans le certificat. CAPF est un proxy de certificat et le CA et lui peuvent signer le certificat aux téléphones mais l'autre certificat comme le CallManager, Tomcat, IPSec qu'ils agissent en tant que feuille (identité de l'utilisateur). Quand vous regardez dans le CSR pour eux, vous pouvez voir que le CSR CAPF a le **rôle de** CertificateSign mais pas les autres.

CSR CAPF :

```
        Attributes:
```

```
Requested Extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, IPSec End System
    X509v3 Key Usage:
        Digital Signature, Certificate Sign
```

CSR de Tomcat :

```
Attributes:
Requested Extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, IPSec End System
    X509v3 Key Usage:
        Digital Signature, Certificate Sign
```

CSR de CallManager :

```
Attributes:
Requested Extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, IPSec End System
    X509v3 Key Usage:
        Digital Signature, Certificate Sign
```

CSR d'IPSec :

Attributs : Extensions demandées : Utilisation principale X509v3 étendue : Authentification de serveur Web de TLS, authentification de client web de TLS, utilisation principale du système d'extrémité X509v3 d'IPSec : Signature numérique, chiffrement principal, chiffrement de données, accord principal

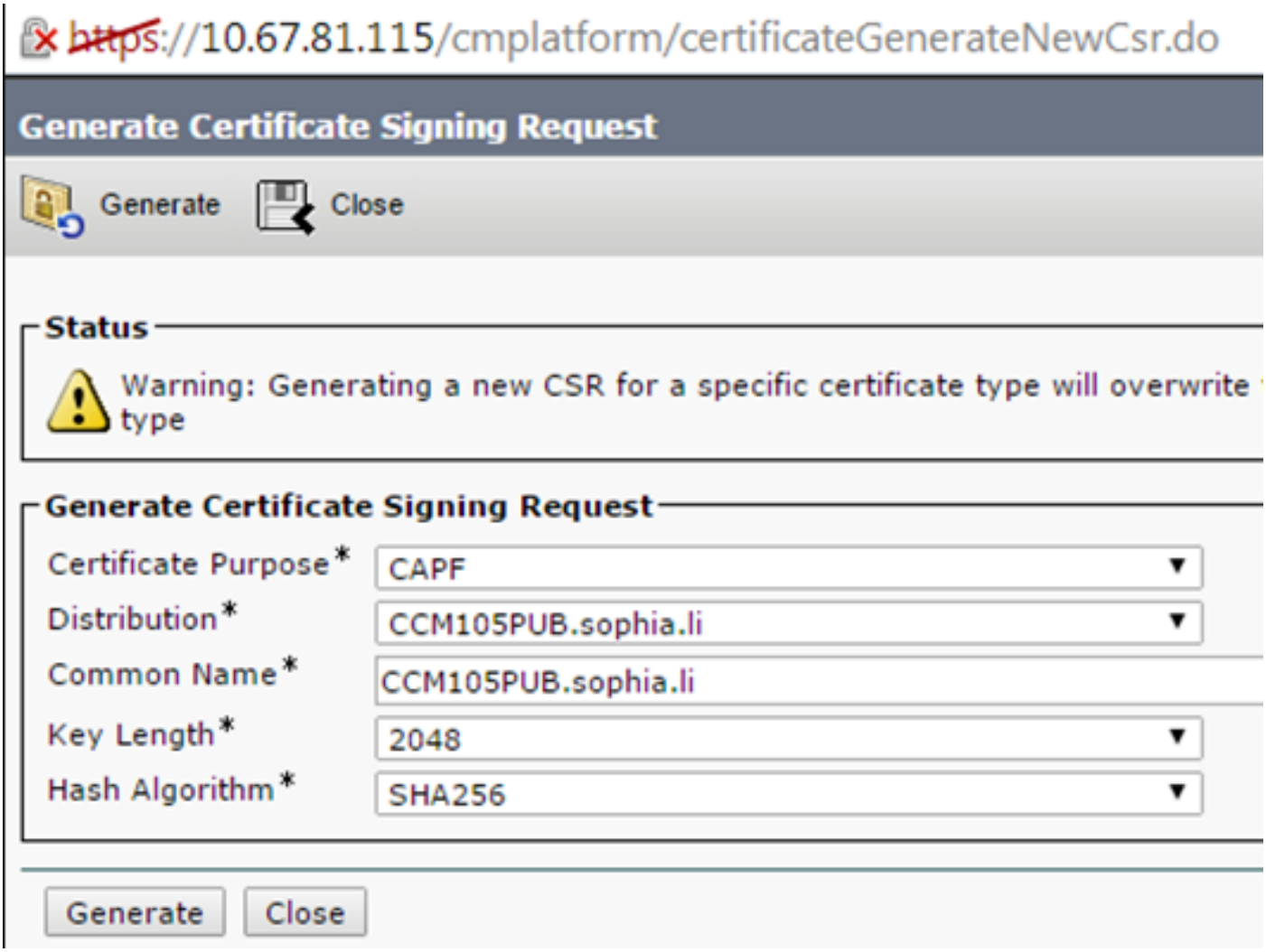
Configurer

Voici un scénario, la racine externe CA est utilisé pour signer le certificat CAPF : a chiffré le signal/medias pour le client et le téléphone IP de Jabber.

Étape 1. Faites votre batterie CUCM comme batterie de Sécurité.

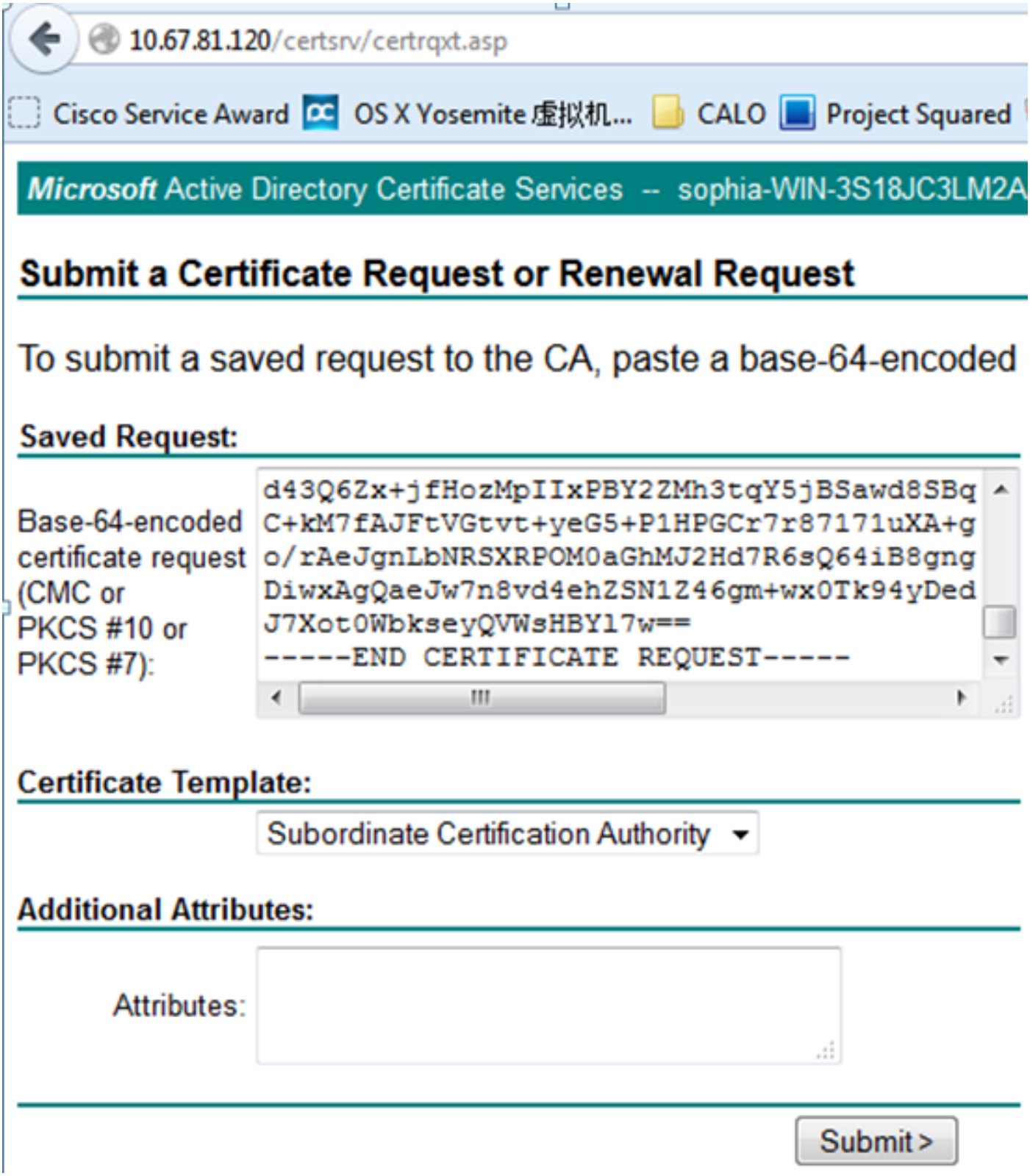
```
admin:utils ctl set-cluster mixed-mode
```

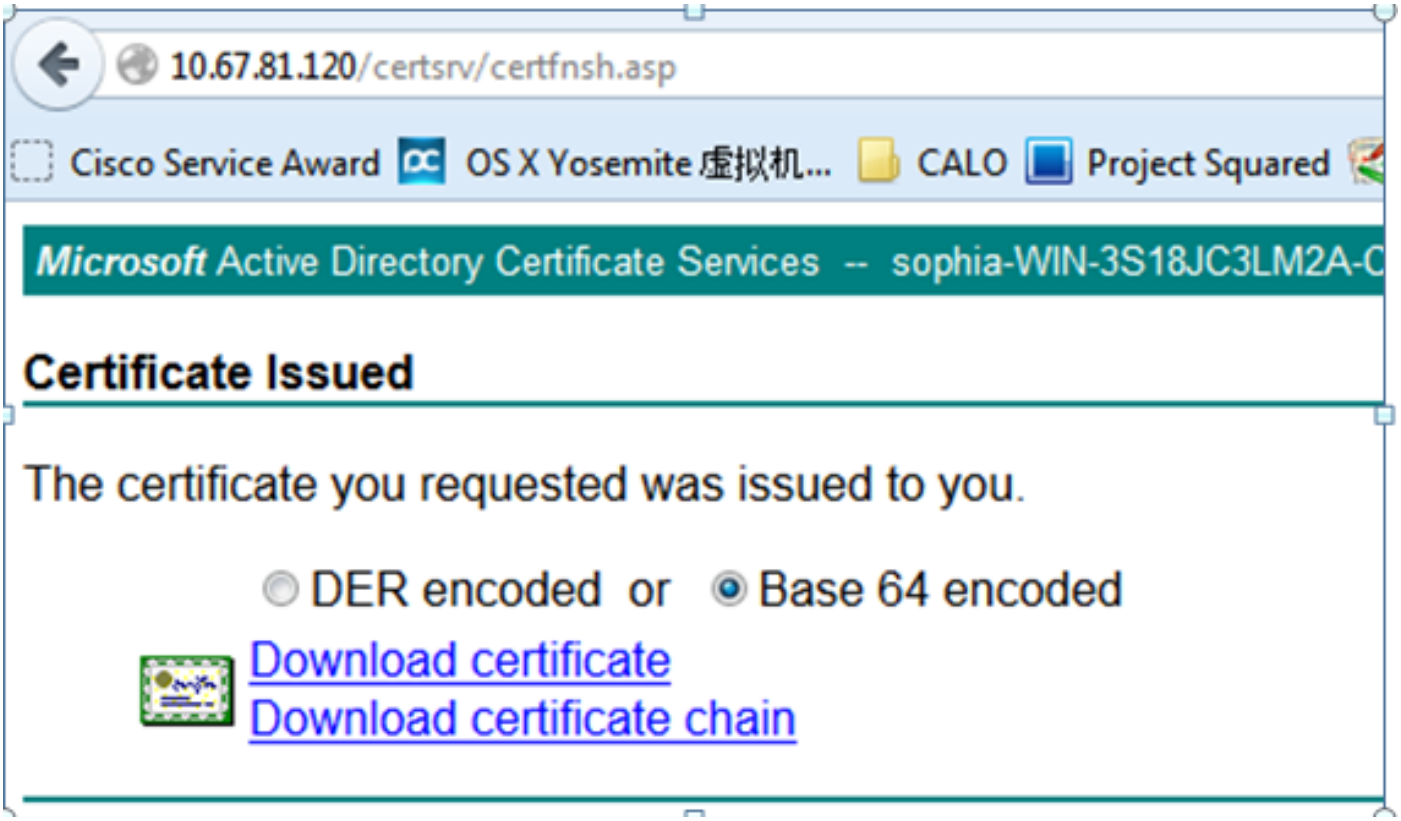
Étape 2. Suivant les indications de l'image, générez le CSR CAPF.



Étape 3. A signé ceci avec le CA (utilisant le modèle subalterne dans Windows 2008 CA).

> **Note**: Vous avez besoin du modèle **subalterne d'autorité de certification d'**utilisateur pour signer ce certificat.


10.67.81.120/certsrv/certrqxt.asp
Cisco Service Award
OS X Yosemite 虚拟机...
CALO
Project Squared
Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
d43Q6Zx+jfHozMpIIxPBY2ZMh3tqY5jBSawd8SBq
C+kM7fAJFtVGtvt+yeG5+P1HPGCr7r87171uXA+g
o/rAeJgnLbNRSXRPOM0aGhMJ2Hd7R6sQ64iB8gng
DiwxAgQaeJw7n8vd4ehZSN1Z46gm+wx0Tk94yDed
J7Xot0WbkseyQVWsHBYl7w==
-----END CERTIFICATE REQUEST-----
Certificate Template:
Subordinate Certification Authority
Additional Attributes:
Attributes:
Submit >

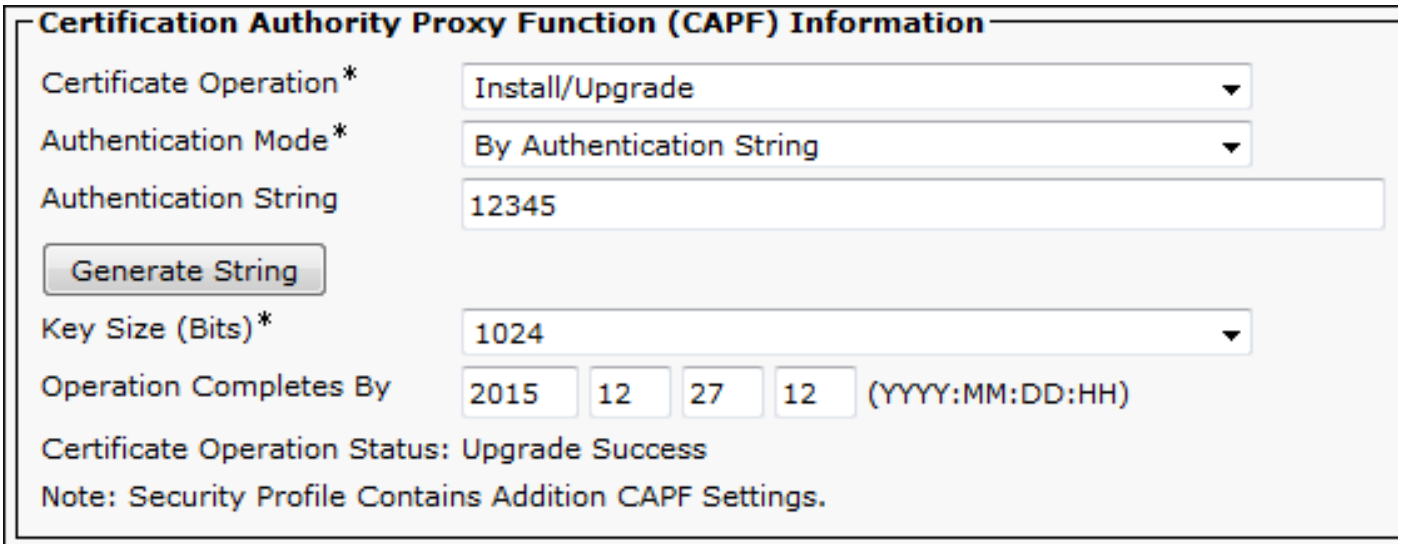


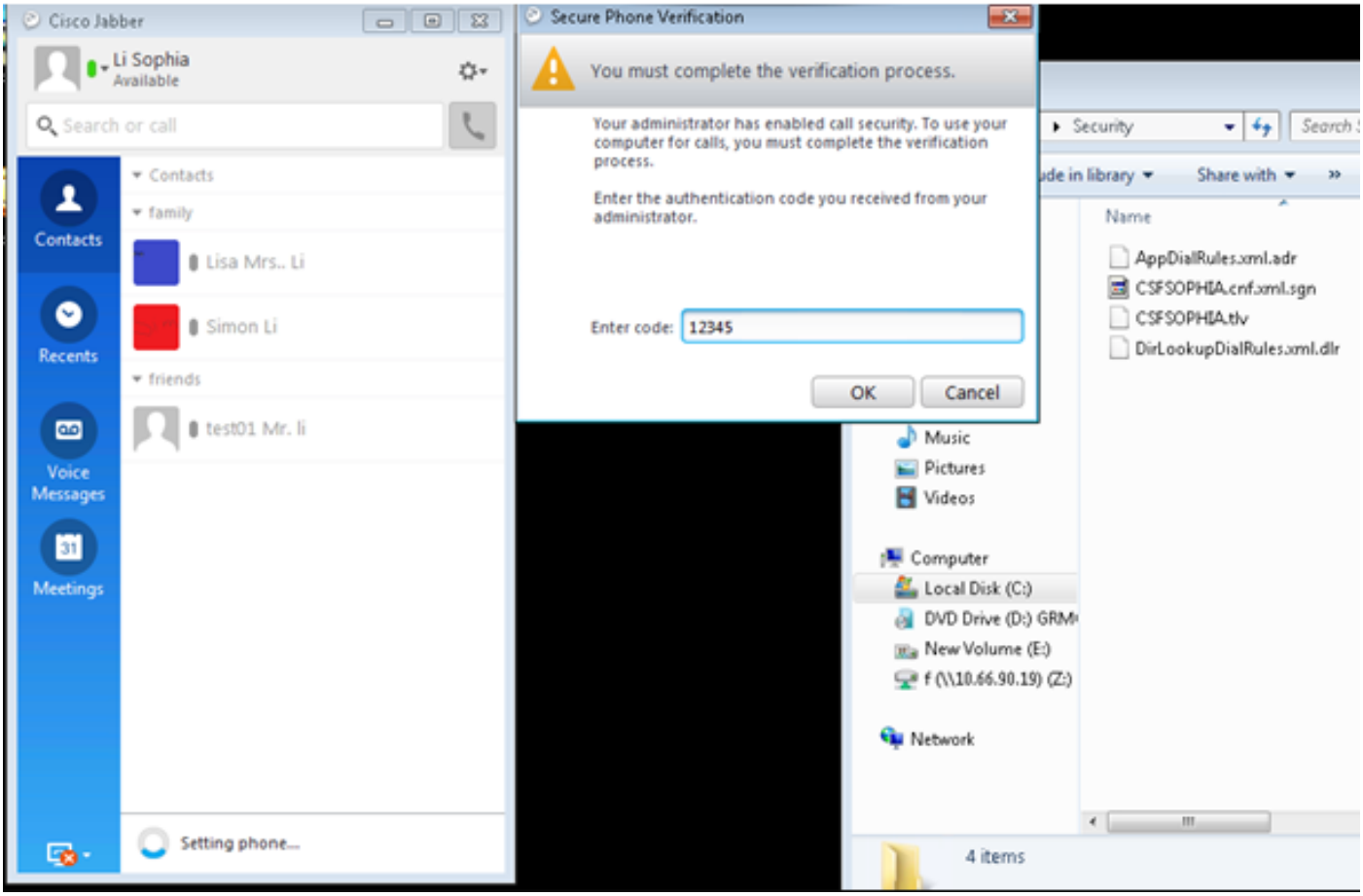
Étape 4. Téléchargez la racine CA comme CAPF-confiance et le certificat de serveur comme CAPF. Pour ce test, téléchargez s'il vous plaît également cette racine CA comme la CallManager-confiance pour avoir la connexion de TLS entre le service de Jabber et de CallManager comme LSC signé doit sont de confiance par service de CallManager aussi bien. Comme mentionné au début de cet article, il y a un besoin d'aligner le CA pour tous les serveurs ainsi ce CA devrait avoir été téléchargé au CallManager déjà pour le signal/cryptage de medias. Pour le screnario de déployer le 802.1x de téléphone IP, vous ne devez pas faire le CUCM comme mode mixte ou télécharger le CA qui signe le CAPF comme CallManager-confiance dedans au serveur CUCM.

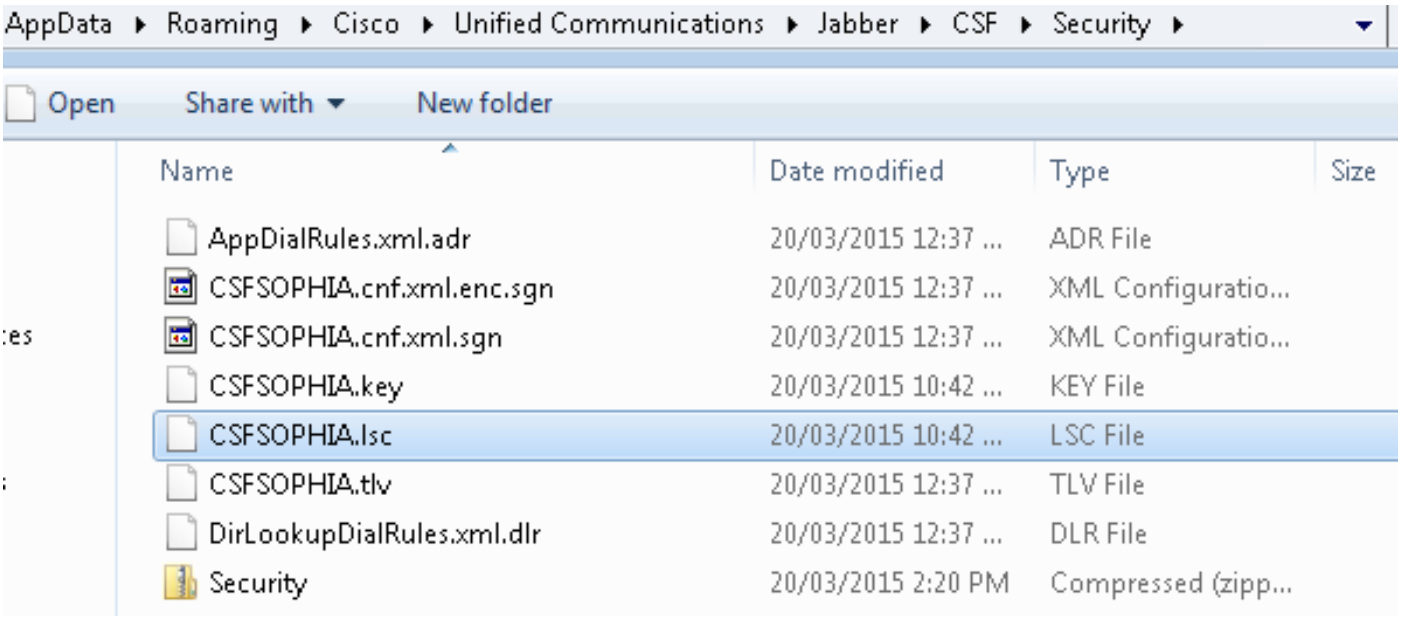
Étape 5. Redémarrez le service CAPF.

Étape 6. Redémarrez les services CallManager/TFTP dans toutes les notes.

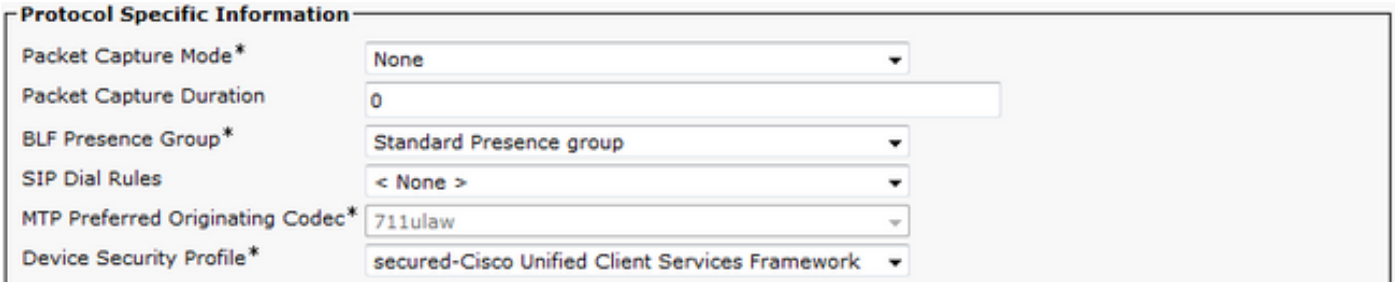
Étape 7. A signé le téléphone IP LSC de Jabber.



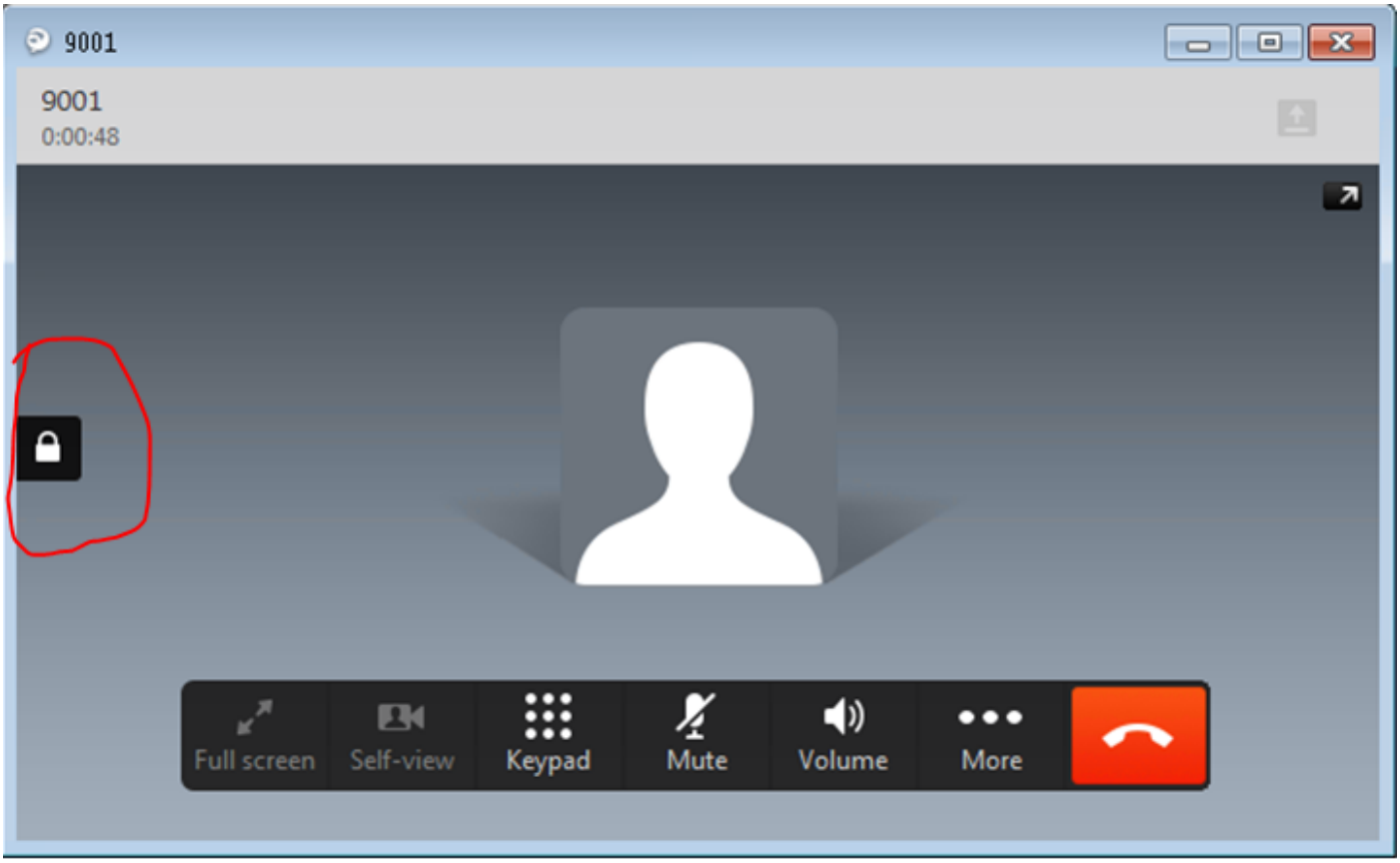




Étape 8. Activez le profil de Sécurité pour le téléphone IP de Jabber.



Étape 9. Le RTP maintenant sécurisé se produit en tant que :

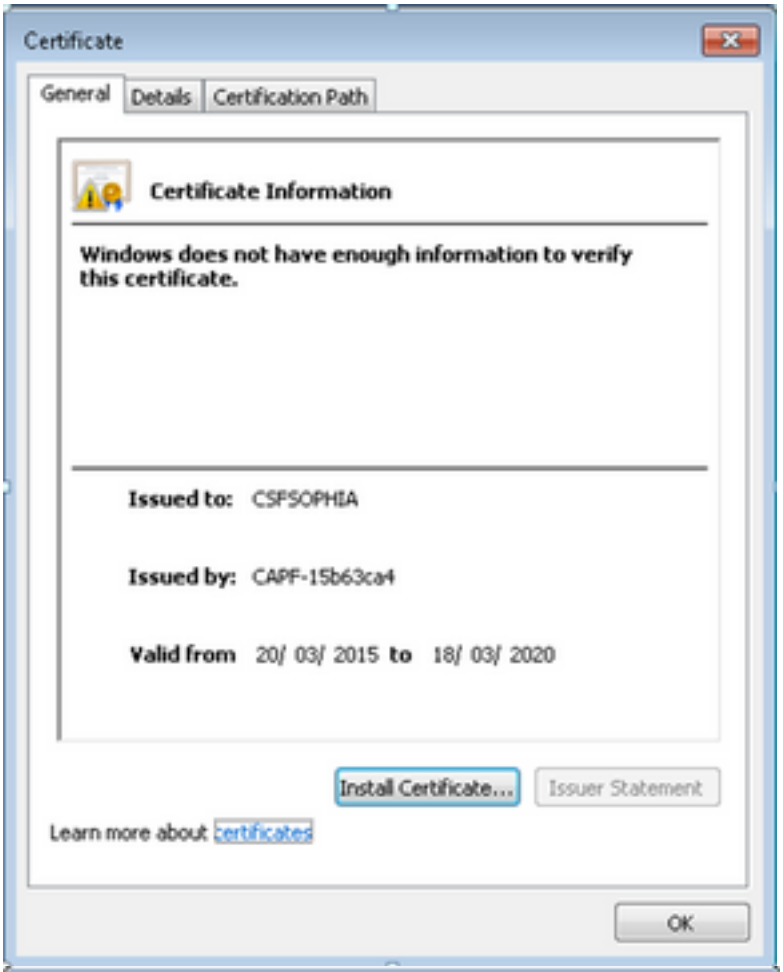


Vérifiez

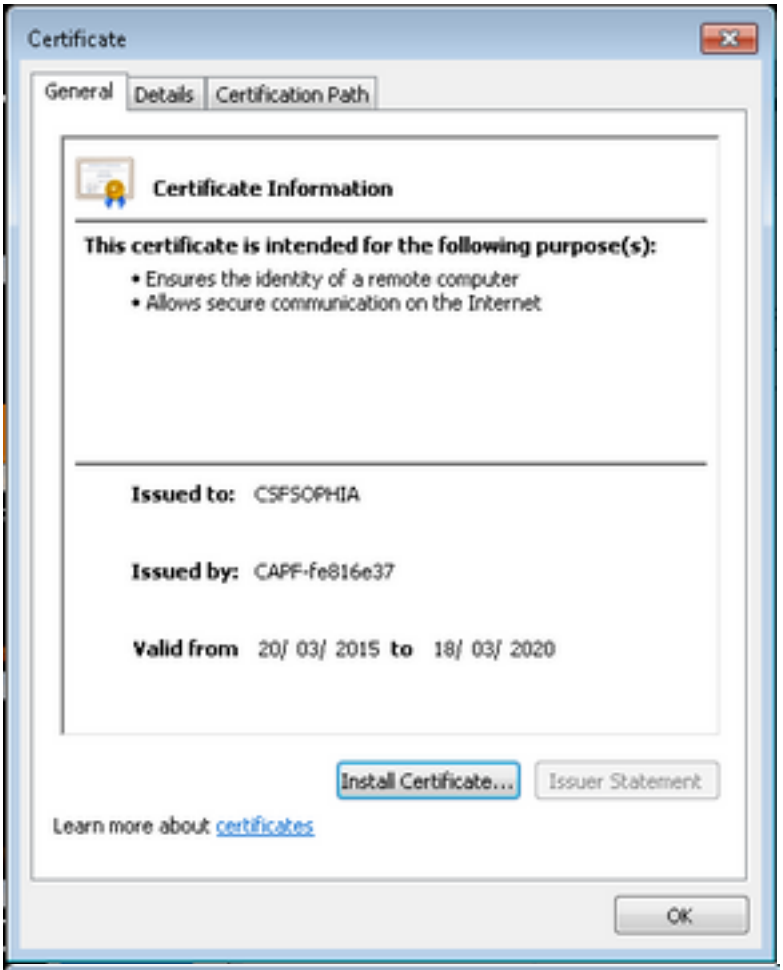
Comparez le LSC quand CAPF auto-brûlé légèrement et CAPF Ca-signé :

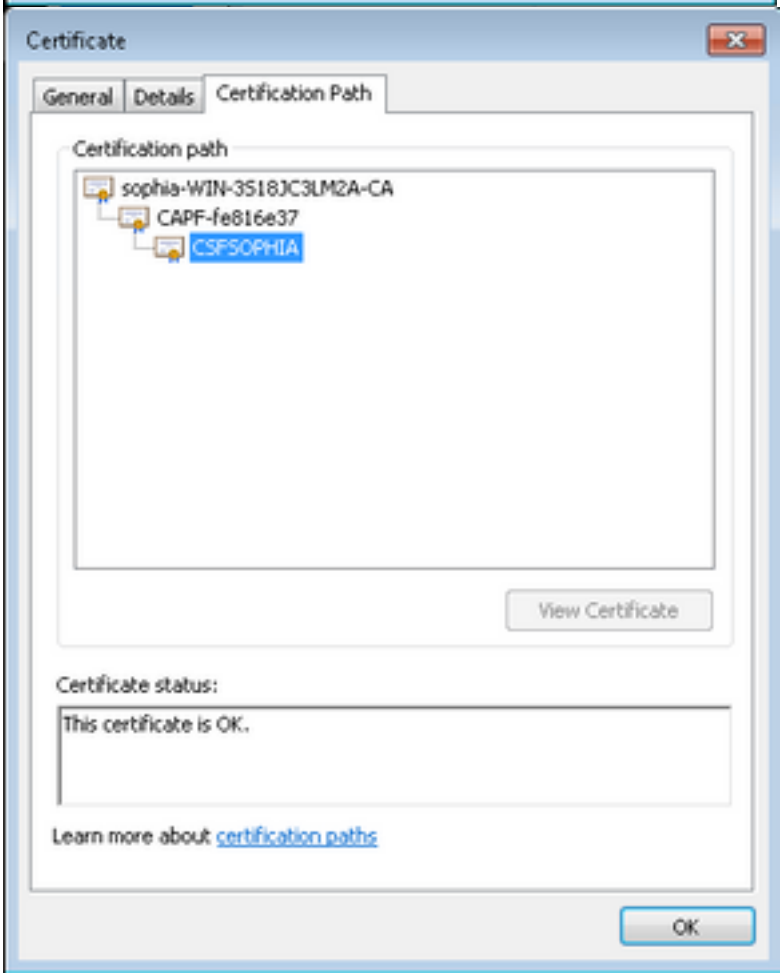
Comme vous pouvez voir de ces images pour le LSC, du point de vue LSC, CAPF est la racine CA en utilisant CAPF auto-signé mais CAPF est le subalterne (intermédiaire) CA tandis qu'en utilisant CAPF Ca-signé.

LSC quand CAPF Auto-signé



LSC quand CAPF Ca-signé


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Allows secure communication on the Internet
Issued to: CSFSOPHIA
Issued by: CAPF-fe816e37
Valid from 20/ 03/ 2015 to 18/ 03/ 2020
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Certificate
General
Details
Certification Path
Certification path
sophia-WIN-3S18JC3LM2A-CA
CAPF-fe816e37
CSFSOPHIA
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

Défaut connu : Le certificat CAPF signé par CA, CERT de racine doit être téléchargé comme Cm-confiance :

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir