Certificado del CAPF firmado por CA para CUCM

Contenido

Introducción

Este documento describe cómo obtener un certificado de la función de proxy del Certificate Authority (CAPF) firmado por el Certificate Authority (CA) para el administrador de las Comunicaciones unificadas de Cisco (CUCM). Hay siempre peticiones de firmar el CAPF con CA externo. Este documento muestra por qué entender cómo trabaja es tan importante como el Procedimiento de configuración.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Public Key Infrastructure (PKI)
- Configuración de seguridad CUCM

Componentes Utilizados

La información en este documento se basa en la versión del administrador 8.6 de las Comunicaciones unificadas de Cisco y arriba.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Limitación

Diverso CA pudo tener diversos requisitos al CSR. Hay informes que diversa versión del OpenSSL CA hace que un cierto específico pida los trabajos CSR sin embargo Microsoft Windows CA bien con el CSR del CAPF de Cisco hasta ahora, que la discusión no será cubierta en este artículo.

Productos Relacionados

Este documento se puede también utilizar con estas versiones de software y hardware:

- Microsoft Windows server 2008 CA.
- Jabber de Cisco para Windows (diversos vervions pudieron tener nombre diferente para que la carpeta salve el LSC).

Antecedentes

El propósito de CA firmó el CAPF

Algunos clientes quisieran alinear con el whith globle de la directiva del certificado que la compañía tan allí es una necesidad firmó el CAPF con mismo CA que otros servidores.

Mecanismo para este PKI

Por abandono, localmente - el certificado significativo (LSC) es firmado por el CAPF, así que el CAPF es CA para los teléfonos en este escenario. Sin embargo, cuando usted intenta conseguir el CAPF firmado por CA externo, después el CAPF en este escenario actúa como subordinado CA o CA intermedio.

La diferencia entre el CAPF uno mismo-firmado y el CAPF CA-firmado es: el CAPF es raíz CA al LSC al hacer el CAPF uno mismo-firmado, el CAPF es CA (intermedio) subordinado al LSC al hacer el CAPF CA-firmado.

¿Cómo el CAPF CSR es diferente de otros CSR?

Mirando al RFC5280, la extensión dominante del uso define el propósito (e.g., estenografía, firma, certificado firmando) de la clave contenida en el certificado. El CAPF es un proxy del certificado y CA y él pueden firmar el certificado a los teléfonos pero el otro certificado como el CallManager, Tomcat, IPSec que actúan como hoja (Identificación del usuario). Cuando usted mira en el CSR para ellos, usted puede ver que el CAPF CSR tiene el **papel de** CertificateSign pero no los otros.

CAPF CSR:

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

Tomcat CSR:

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

CallManager CSR:

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

IPSec CSR:

Atributos: Extensiones pedidas: Uso dominante extendido X509v3: Autenticación del servidor Web de TLS, autenticación del cliente de Web de TLS, uso de la clave del sistema extremo X509v3 del IPSec: Firma digital, estenografía dominante, estenografía de los datos, acuerdo dominante

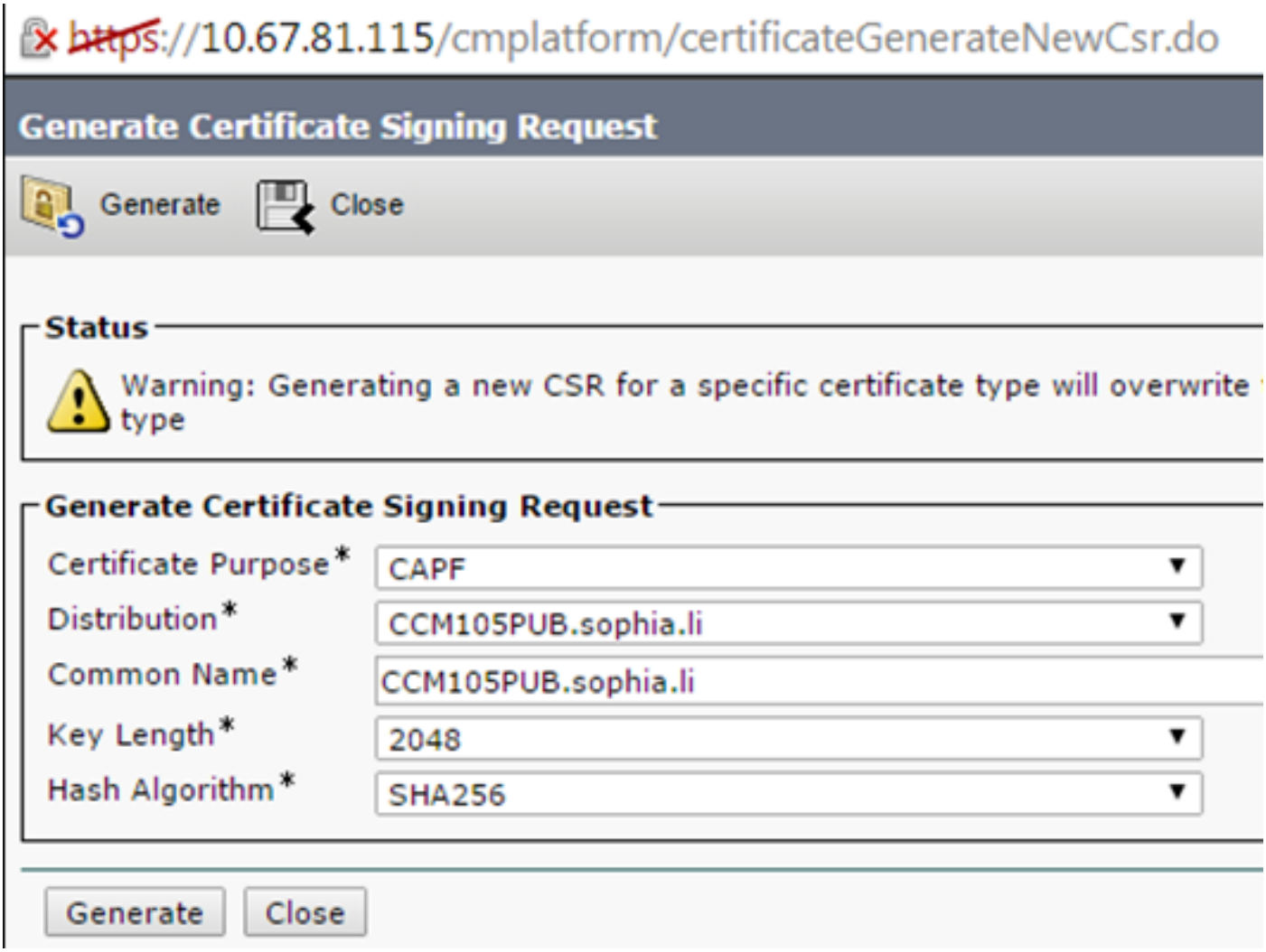
Configurar

Aquí está un escenario, externo raíz CA se utiliza para firmar el certificado del CAPF: para cifró la señal/los media para el cliente y el teléfono del IP del Jabber.

Paso 1. Haga que su cluster CUCM como Seguridad agrupa.

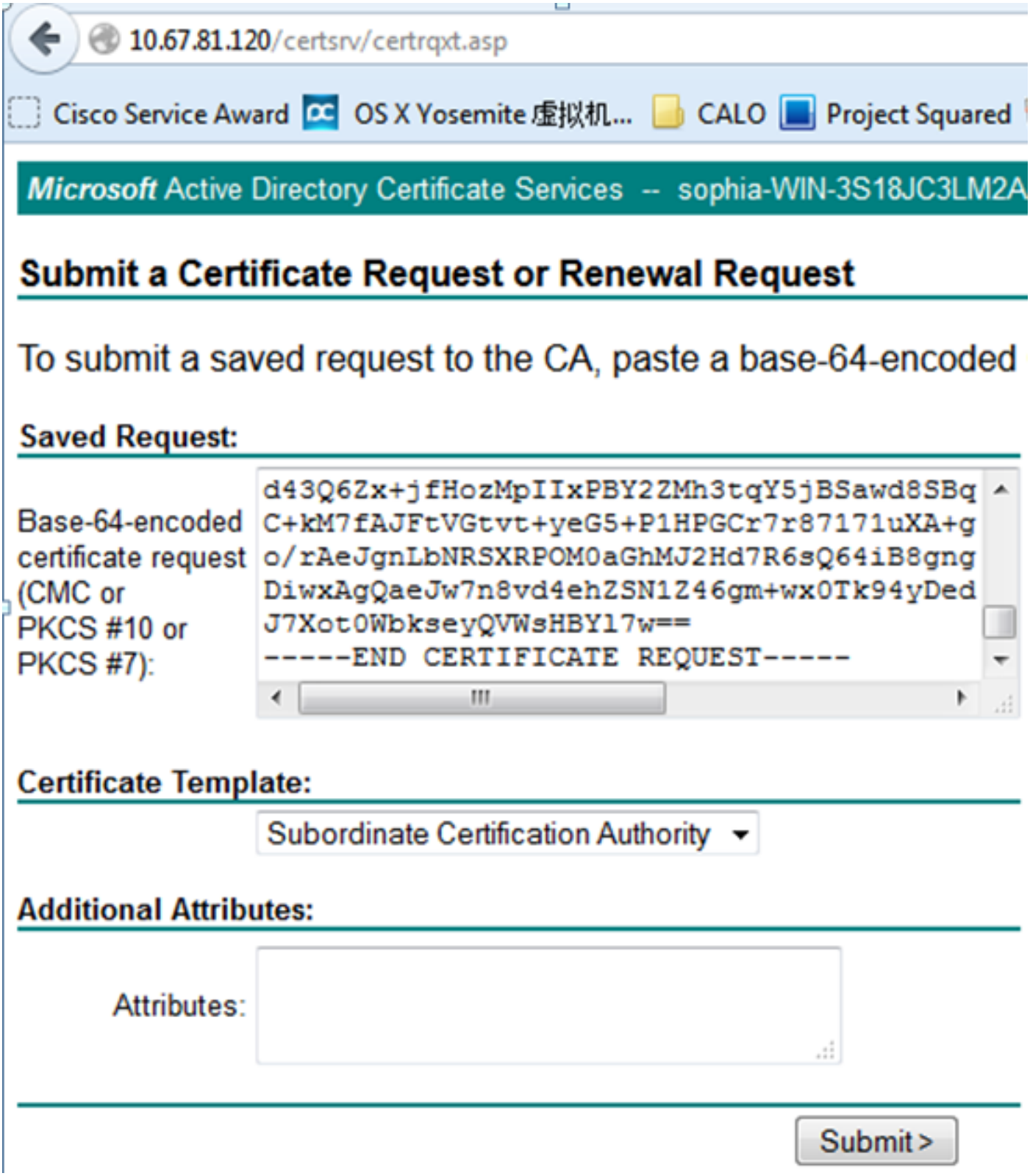
```
admin:utils ctl set-cluster mixed-mode
```

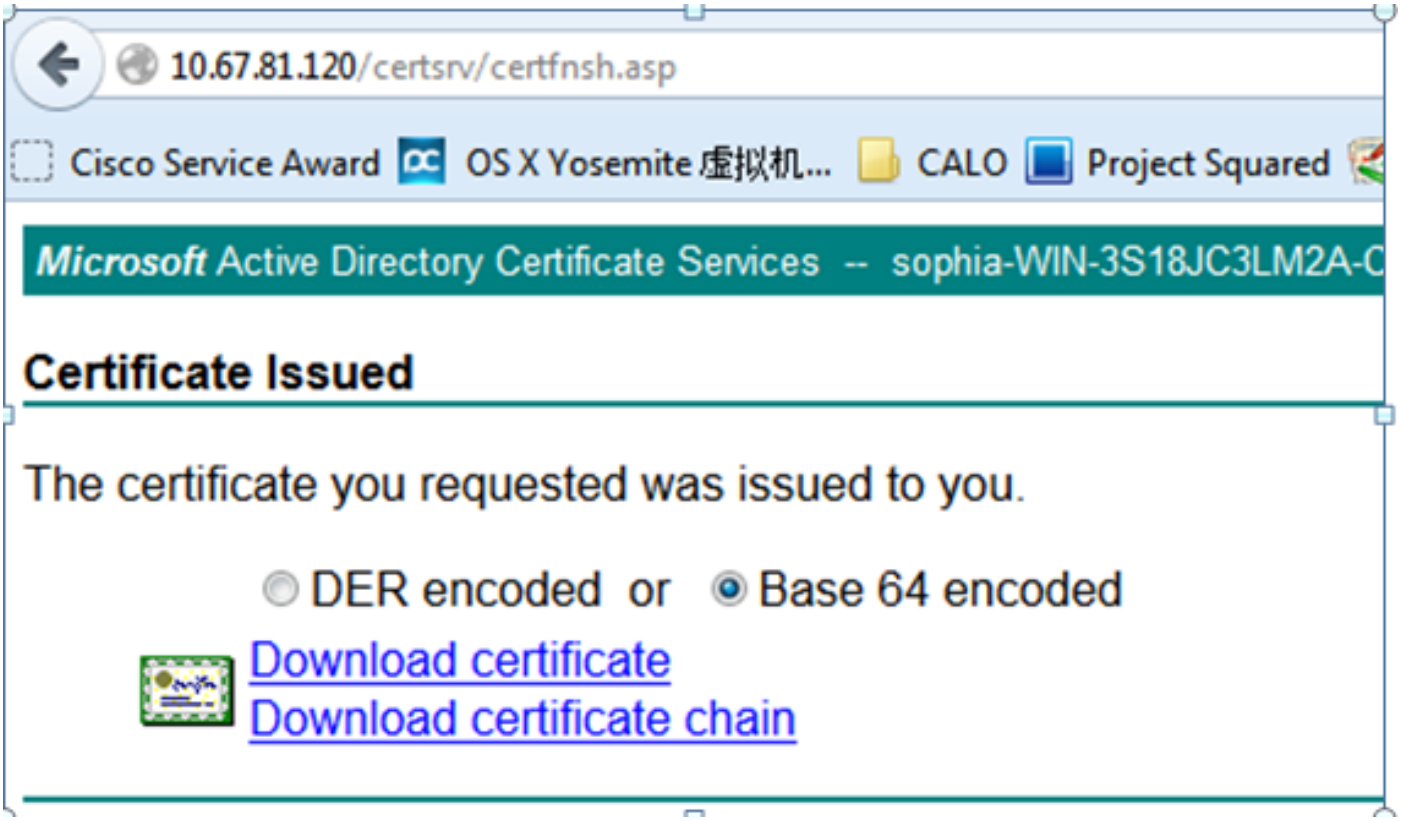
Paso 2. Tal y como se muestra en de la imagen, genere el CAPF CSR.



Paso 3. Firmó esto con CA (usando la plantilla subordinada en Windows 2008 CA).

> **Note**: Usted necesita la plantilla **subordinada de las autoridades de certificación del** usuario firmar este certificado.


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 >

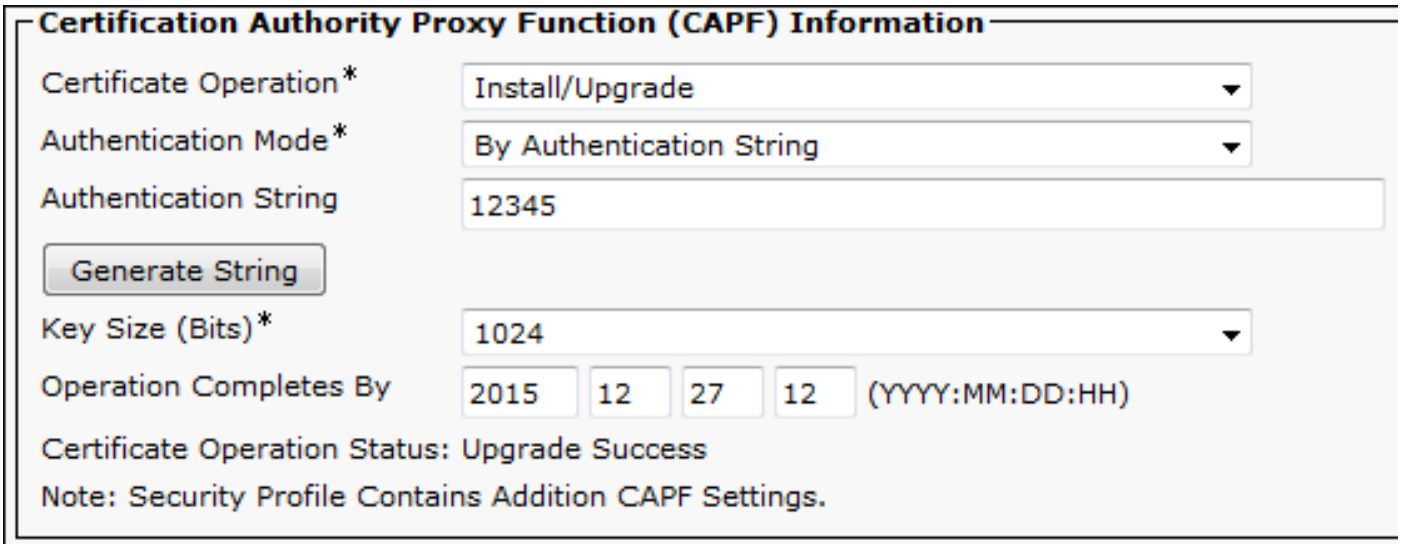


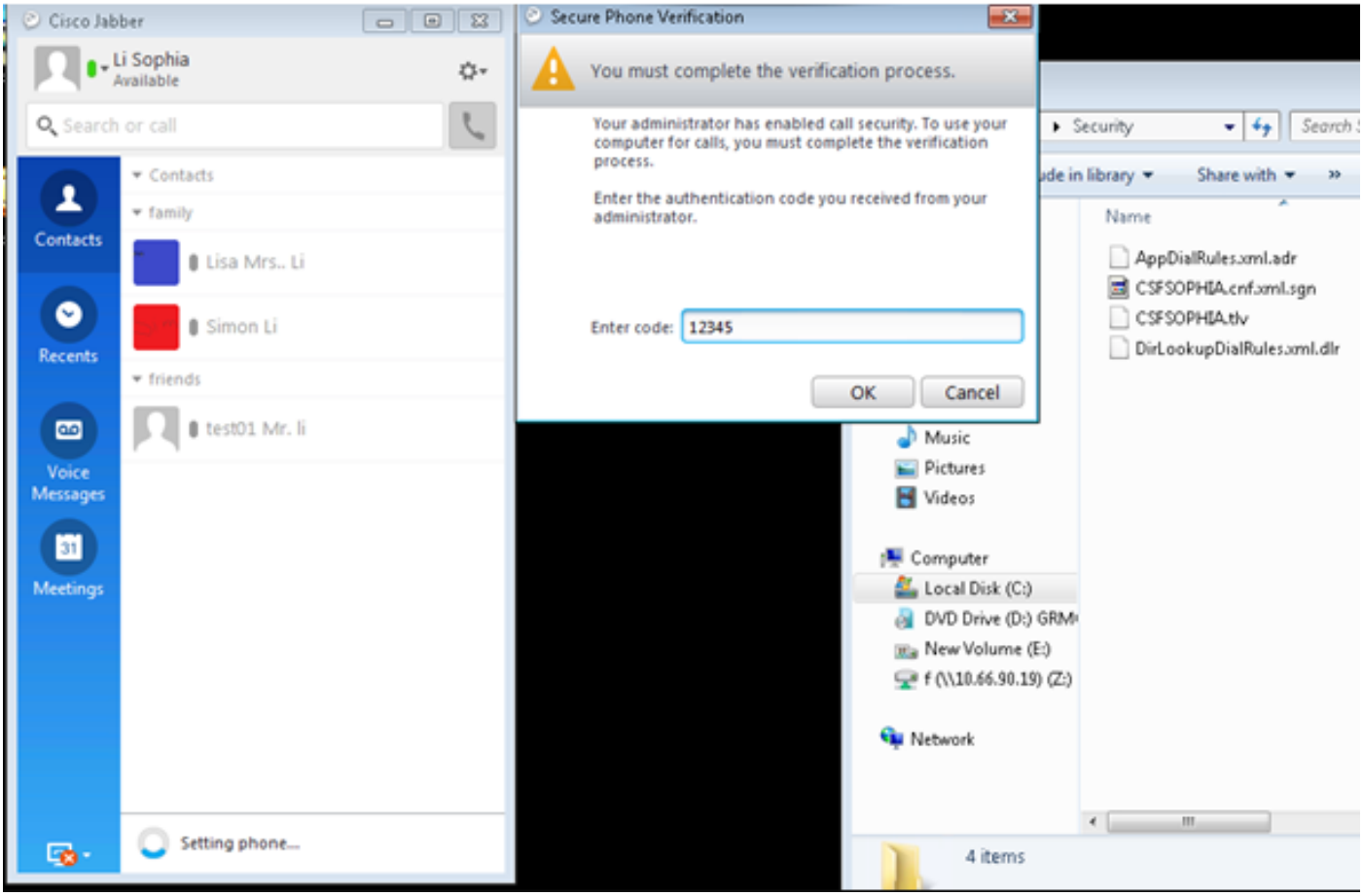
Paso 4. Cargue raíz CA como la CAPF-confianza y el certificado de servidor como CAPF. Para esta prueba, también cargue por favor esto raíz CA como la CallManager-confianza para tener conexión TLS entre el Jabber y el servicio de CallManager como el LSC firmado necesita ser confiada en por el servicio de CallManager también. Según lo mencionado al principio de este artículo, hay una necesidad de alinear CA para todos los servidores así que este CA se debe haber cargado al CallManager ya para la señal/el cifrado de los media. Para el screnario del 802.1x del teléfono del IP que despliega, usted no tiene que hacer el CUCM como modo mezclado o cargar CA que firme el CAPF como CallManager-confianza adentro al servidor CUCM.

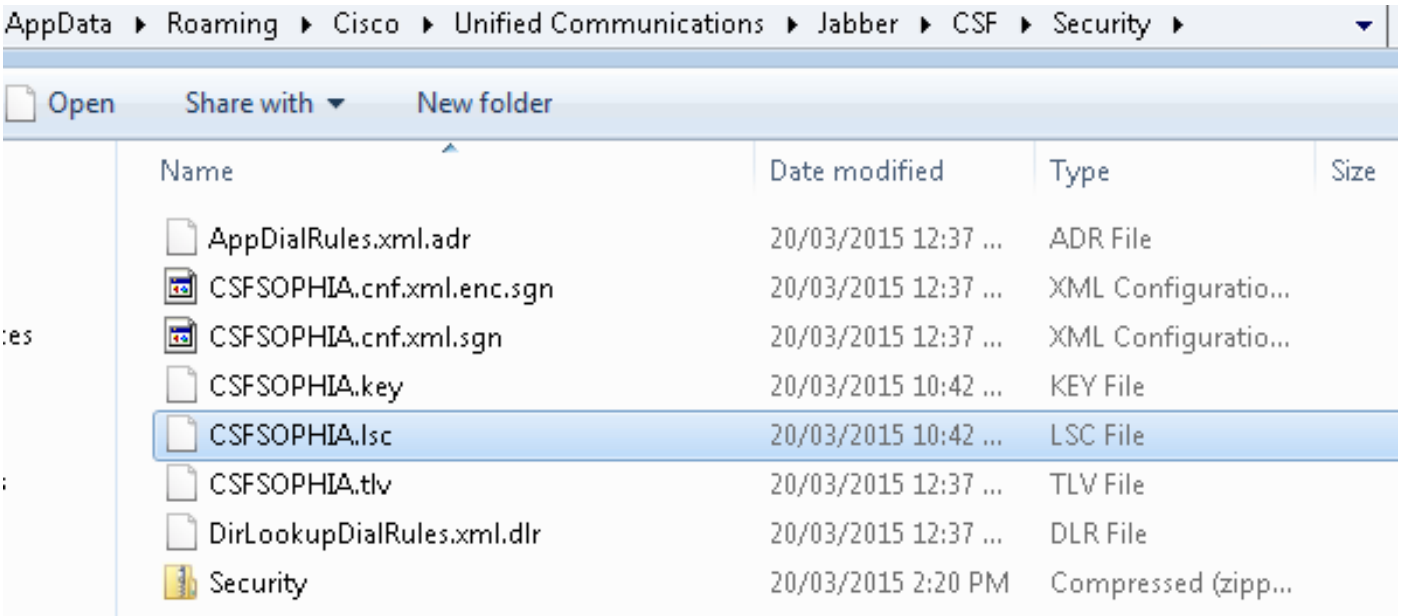
Paso 5. Recomience el servicio del CAPF.

Paso 6. Recomience los servicios CallManager/TFTP en todas las notas.

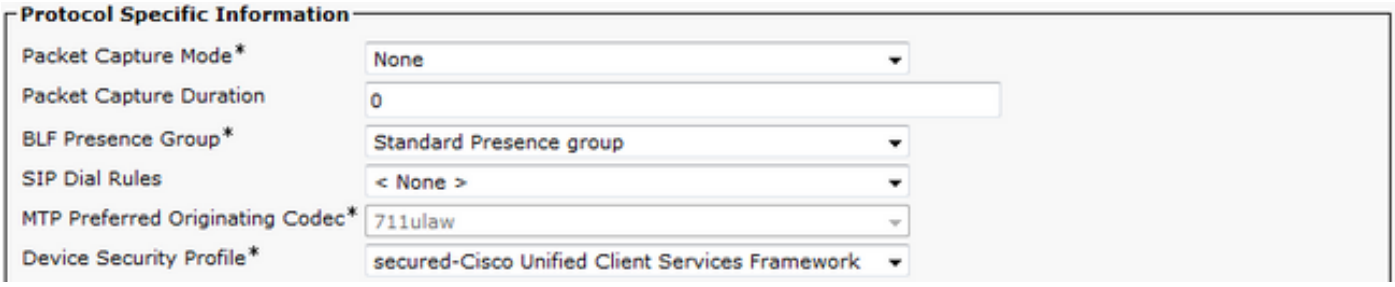
Paso 7. Firmó el softphone LSC del Jabber.



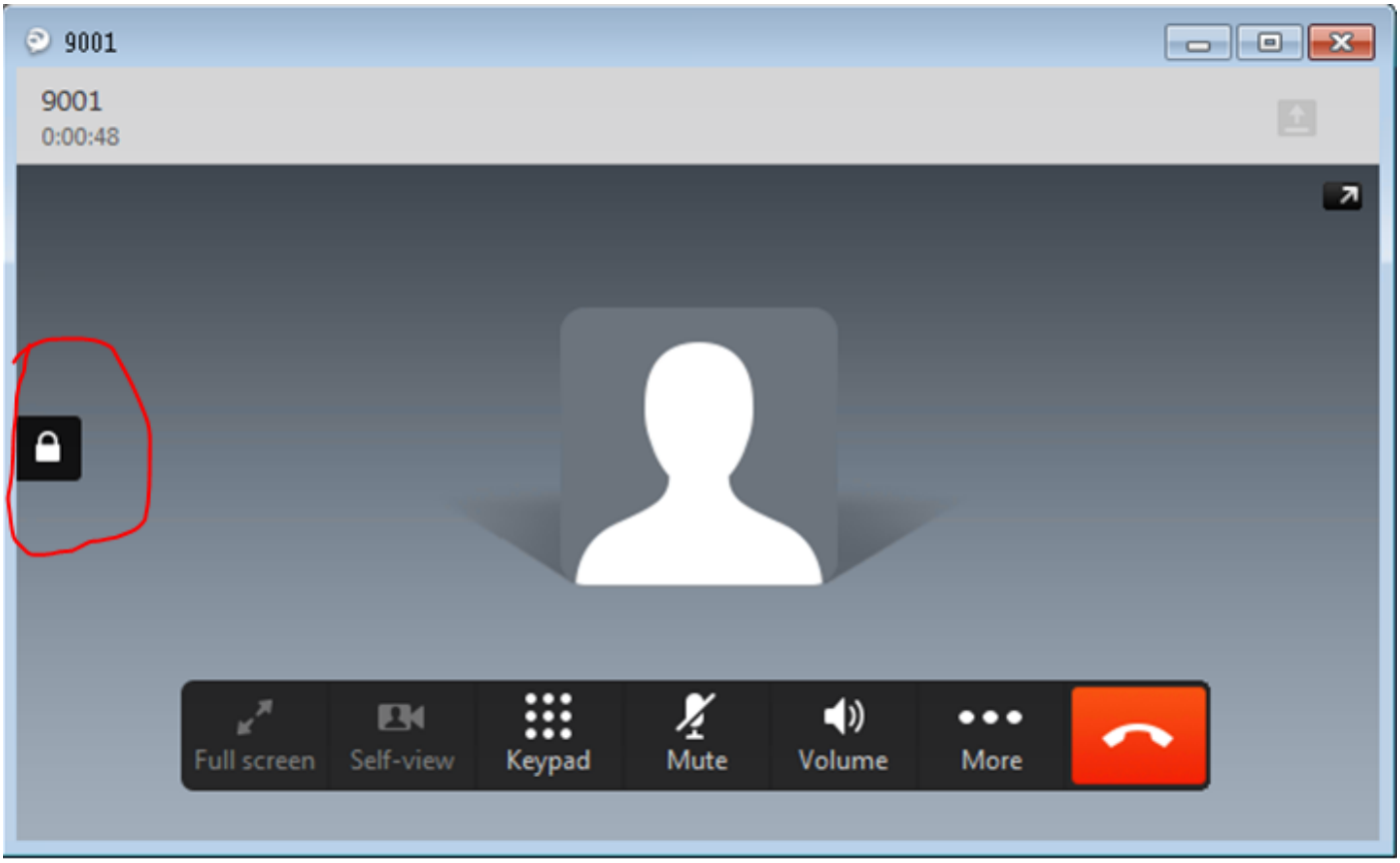




Paso 8. Habilite el perfil de seguridad para el softphone del Jabber.



Paso 9. El RTP ahora asegurado sucede como:

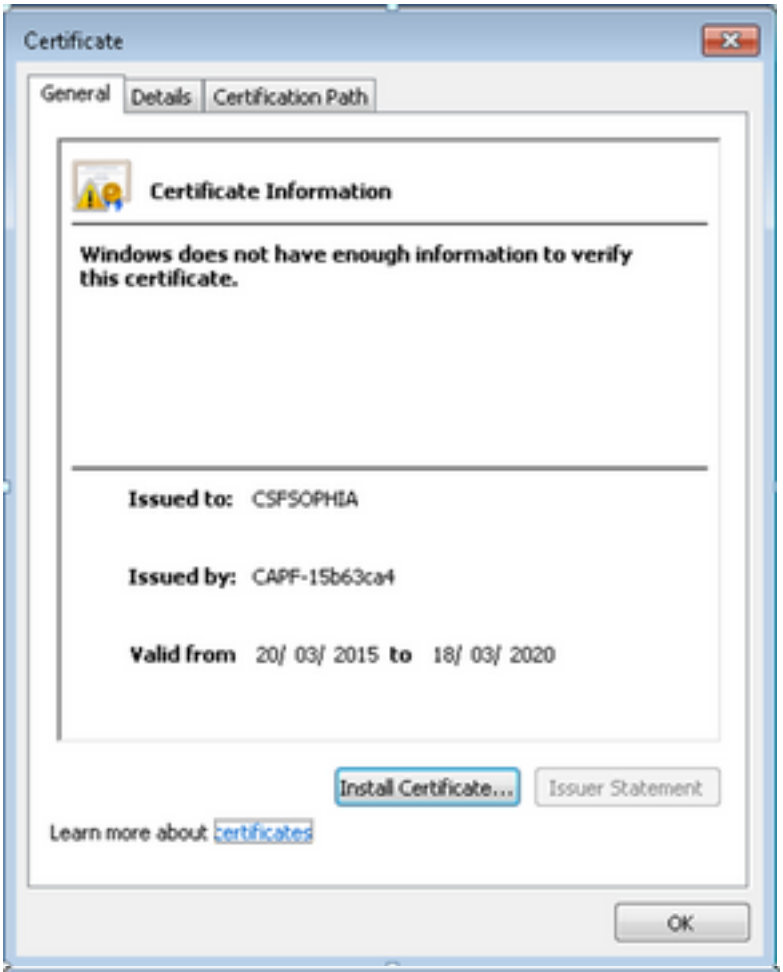


Verificación

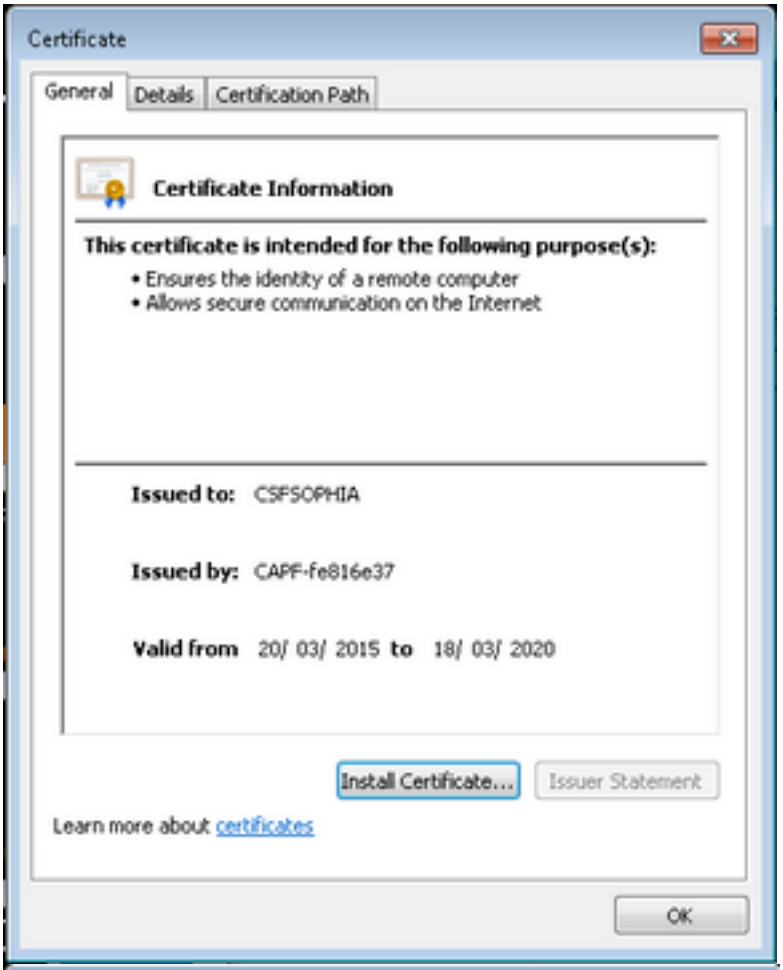
Compare el LSC cuando CAPF uno mismo-chamuscado y CAPF CA-firmado:

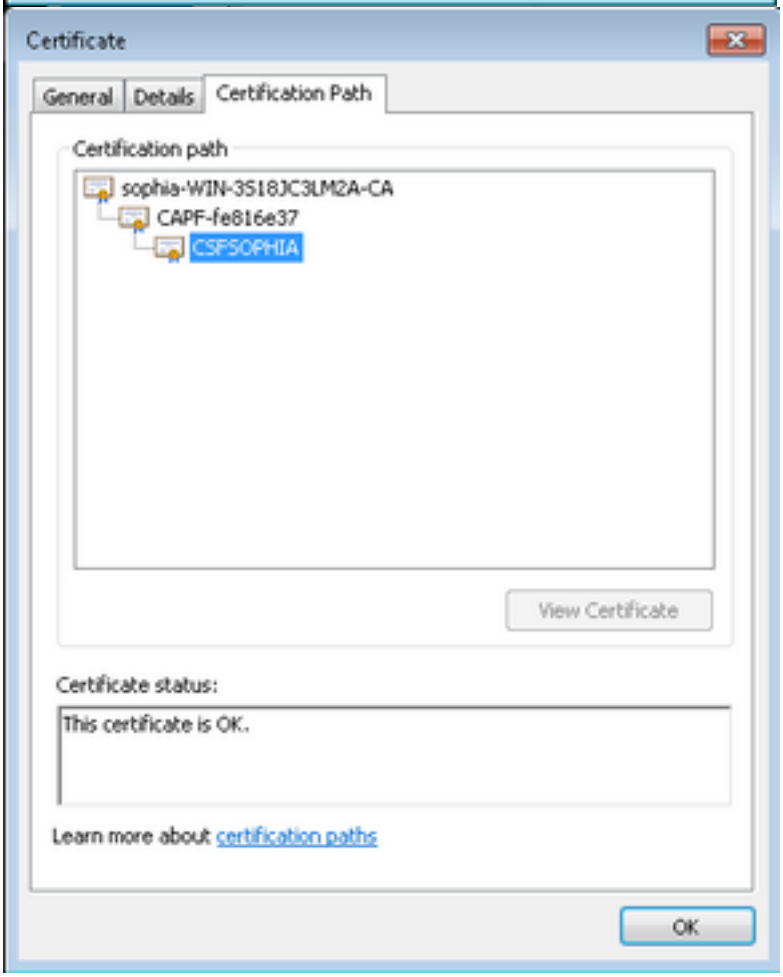
Como usted puede ver de estas imágenes para el LSC, desde el punto de vista LSC, CAPF es raíz CA al usar el CAPF uno mismo-firmado pero el CAPF es CA (intermedio) subordinado mientras que usa el CAPF CA-firmado.

LSC cuando CAPF Uno mismo-firmado



LSC cuando CAPF CA-firmado





Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

Defecto conocido: CA firmó el certificado del CAPF, CERT de la raíz se debe cargar como CM-confianza:

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