

Certificado CAPF assinado pelo CA para CUCM

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Limitação](#)

[Informações de fundo](#)

[Finalidade do CAPF assinado CA](#)

[Mecanismo para este PKI](#)

[Como CAPF CSR é diferente de outros CSR?](#)

[Configurar](#)

[Verificar](#)

[LSC quando CAPF Auto-assinado](#)

[LSC quando CAPF Ca-assinado](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este original descreve como obter um certificado da função do proxy do Certificate Authority (CAPF) assinado pelo Certificate Authority (CA) para o gerente das comunicações unificadas de Cisco (CUCM). Há sempre uns pedidos assinar o CAPF com CA externo. Este original mostra por que compreender como trabalha é tão importante quanto o procedimento de configuração.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Public Key Infrastructure (PKI)
- Configuração de segurança CUCM

[Componentes Utilizados](#)

A informação neste documento é baseada na versão de gerenciador 8.6 das comunicações unificadas de Cisco e acima.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste original começaram com uma configuração cancelada (do padrão). Se sua rede está viva, assegure-se de que você

compreenda o impacto potencial do comando any.

Limitação

O CA diferente pôde ter exigências diferentes ao CSR. Há uns relatórios que a versão diferente do OpenSSL CA manda algum específico pedir os trabalhos CSR contudo Microsoft Windows CA bem com o CSR de Cisco CAPF até agora, que a discussão não será coberta neste artigo.

Produtos Relacionados

Este original pode igualmente ser usado com estes versão de hardware e software:

- Microsoft Windows server 2008 CA.
- Cisco Jabber para Windows (os vevrions diferentes puderam ter o nome diferente para que o dobrador armazene o LSC).

Informações de fundo

Finalidade do CAPF assinado CA

Alguns clientes gostariam de alinhar com o whith que globle da política do certificado a empresa tão lá é uma necessidade assinou o CAPF com o mesmo CA que outros server.

Mecanismo para este PKI

Àrevelia, localmente - o certificado significativo (LSC) é assinado pelo CAPF, assim que pelo CAPF é o CA para telefones nesta encenação. Contudo, quando você tenta obter o CAPF assinado pelo CA externo, a seguir o CAPF nesta encenação atua como o subordinado CA ou CA intermediário.

A diferença entre o CAPF auto-assinado e o CAPF Ca-assinado é: o CAPF é a CA raiz ao LSC ao fazer o CAPF auto-assinado, o CAPF é o subordinado CA (intermediário) ao LSC ao fazer o CAPF Ca-assinado.

Como CAPF CSR é diferente de outros CSR?

Considerando ao [RFC5280](#), a extensão chave do uso define a finalidade (por exemplo, cifragem, assinatura, certificado assinando) da chave contida no certificado. O CAPF é um proxy do certificado e o CA e podem assinar o certificado aos telefones mas o outro certificado como CallManager, Tomcat, IPSec que atua como a folha (identidade do usuário). Quando você olha no CSR para eles, você pode ver que o CAPF CSR tem o **papel de CertificateSign** mas não o outro.

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: Ramais pedidos: Uso X509v3 chave prolongado: Autenticação do servidor de Web TLS, autenticação do cliente web TLS, uso da chave do sistema final X509v3 de IPSec: Assinatura digital, cifragem chave, cifragem dos dados, acordo chave

Configurar



Está aqui uma encenação, CA raiz externo é usada para assinar o certificado CAPF: cifrou o sinal/media para o cliente e o telefone IP do Jabber.

Etapa 1. Faça seu conjunto CUCM como um conjunto da Segurança.

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

Etapa 2. Segundo as indicações da imagem, gerencia o CAPF CSR.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite type

Generate Certificate Signing Request

Certificate Purpose*	CAPF
Distribution*	CCM105PUB.sophia.li
Common Name*	CCM105PUB.sophia.li
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close

Etapa 3. Assinou isto com o CA (que usa o molde subordinado em Windows 2008 CA).

Note: Você precisa o molde **subordinado da autoridade de certificação do** usuário de assinar este certificado.

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  
J7Xot0WbkseyQVWsHBY17w==  
-----END CERTIFICATE REQUEST-----
```

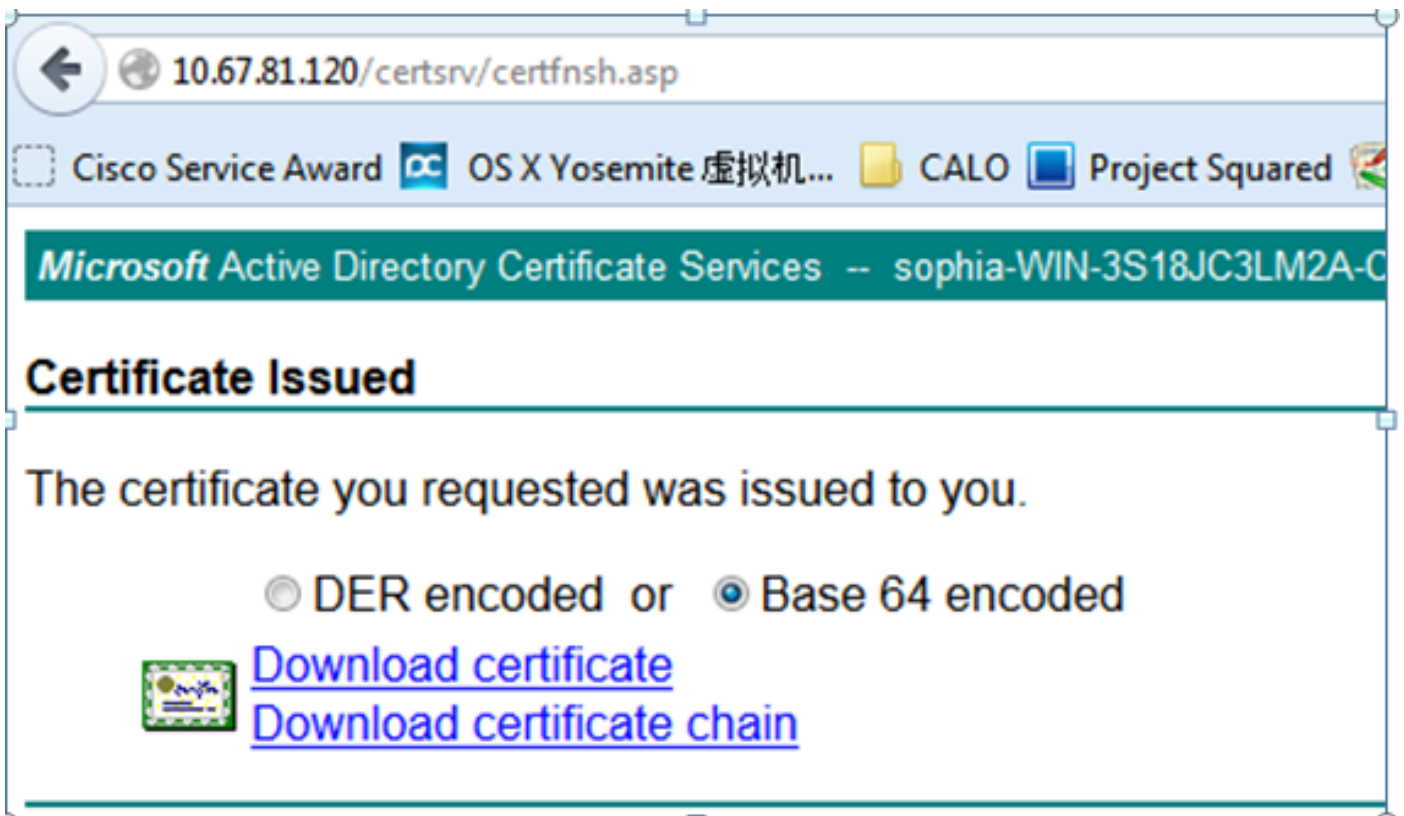
Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Submit >



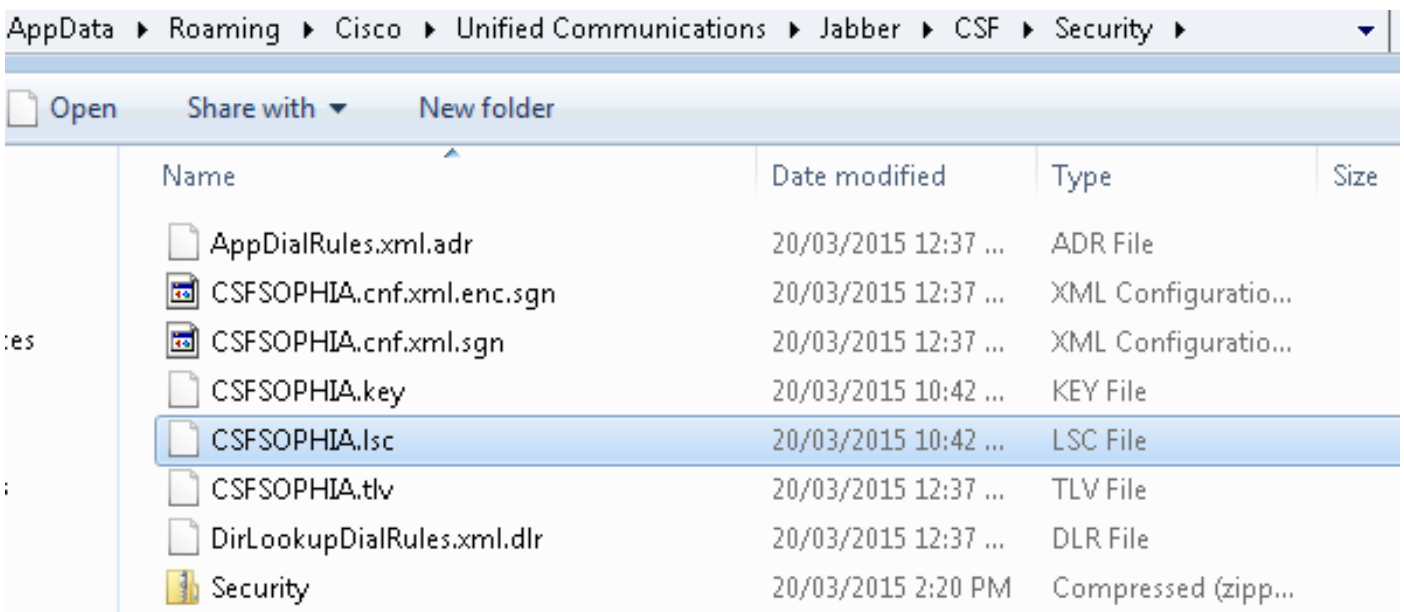
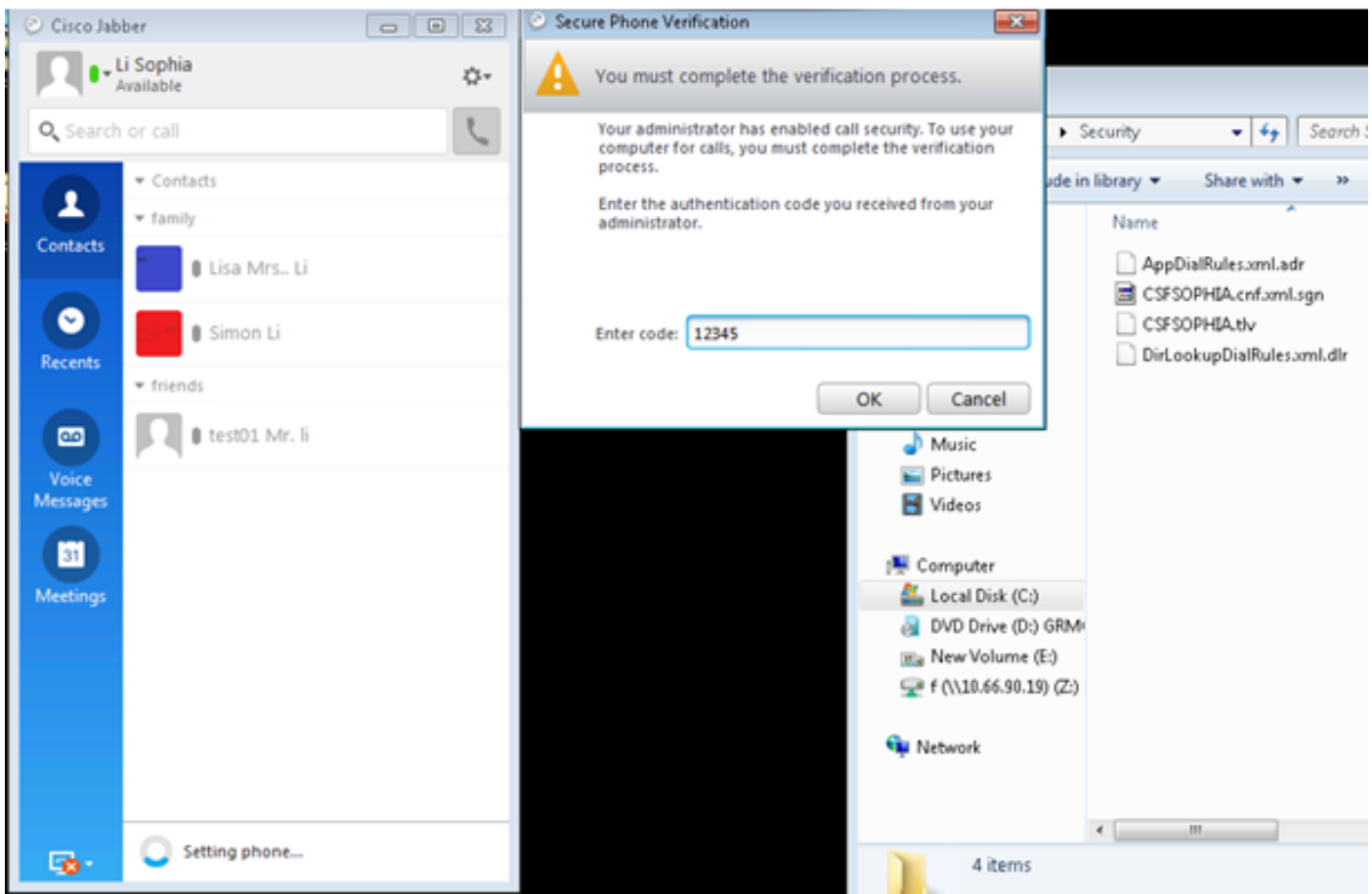
Etapa 4. Transfira arquivos pela rede a CA raiz como a CAPF-confiança e o certificado de servidor como o CAPF. Para este teste, por favor igualmente transfira arquivos pela rede esta CA raiz como a CallManager-confiança para ter a conexão TLS entre o Jabber e o serviço do CallManager como o LSC assinado precisa de ser confiada também pelo serviço do CallManager. Como mencionado no início deste artigo, há uma necessidade de alinhar o CA para todos os server assim que este CA deve ter sido transferido arquivos pela rede a CallManager já para o sinal/criptografia de mídias. Para o cenário do 802.1x de distribuição do telefone IP, você não tem que fazer o CUCM como modo misturado ou transferir arquivos pela rede o CA que assina o CAPF como a CallManager-confiança dentro ao server CUCM.

Etapa 5. Reinicie o serviço CAPF.

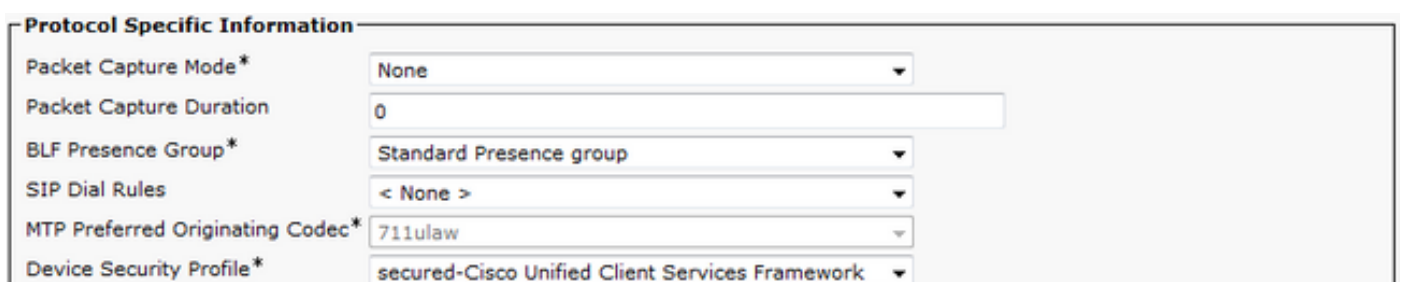
Etapa 6. Reinicie os serviços CallManager/TFTP em todas as notas.

Etapa 7. Assinou o softphone LSC do Jabber.

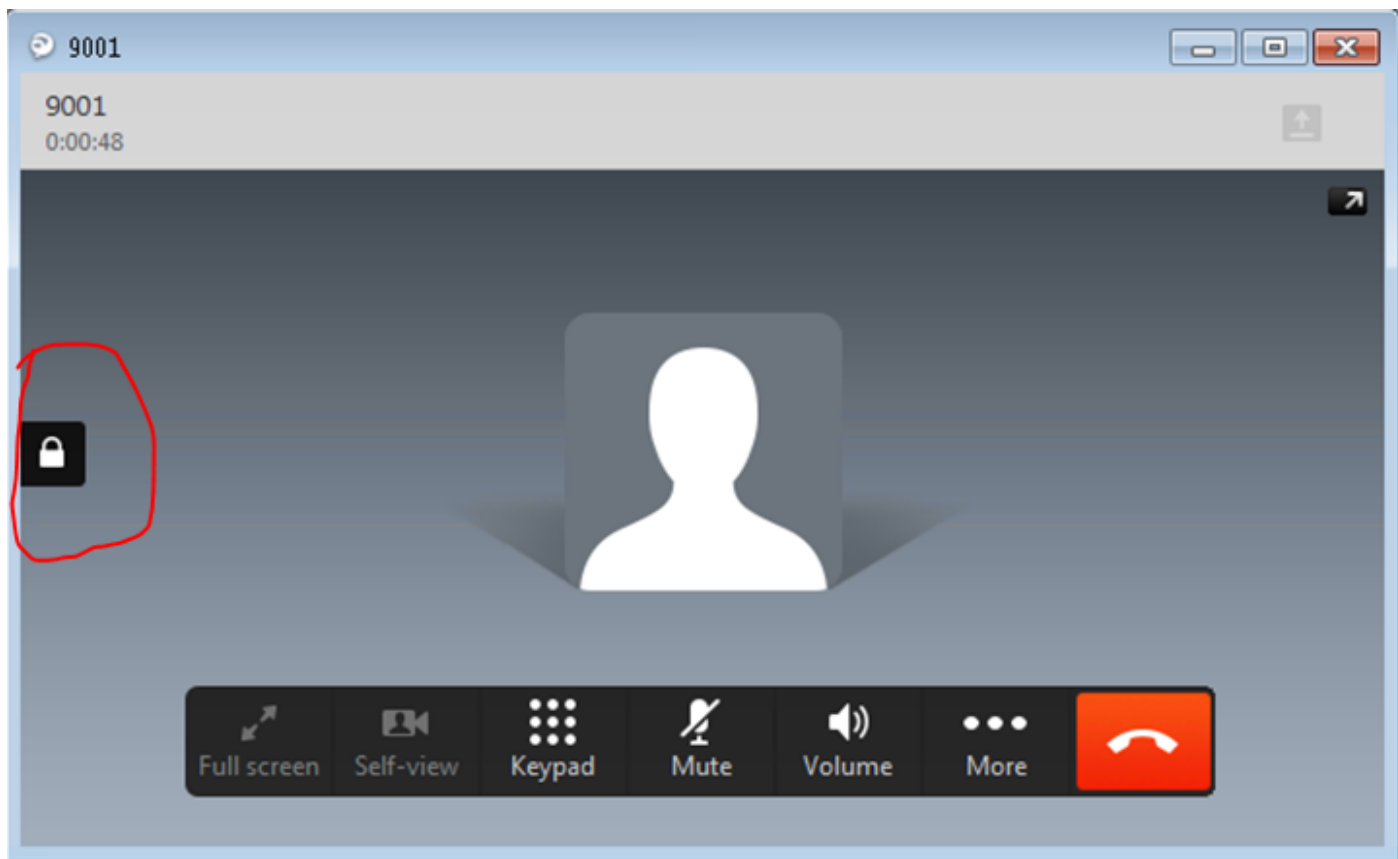
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
Authentication String	12345
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success	
Note: Security Profile Contains Addition CAPF Settings.	



Etapa 8. Permita o perfil de segurança para o softphone do Jabber.



Etapa 9. O RTP agora fixado acontece como:

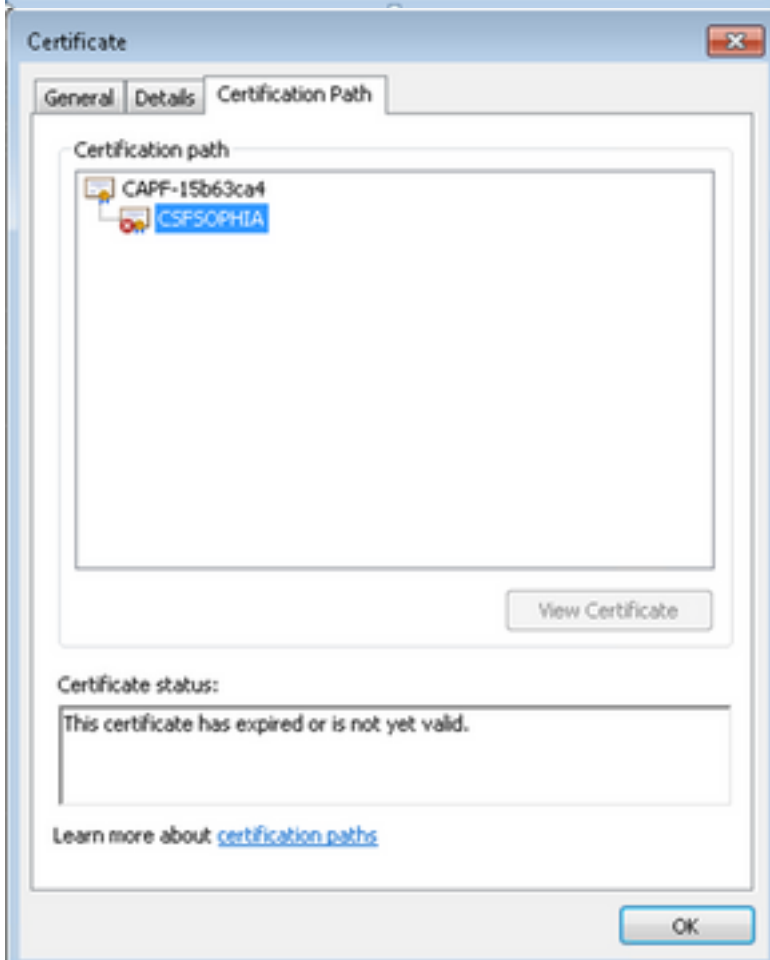
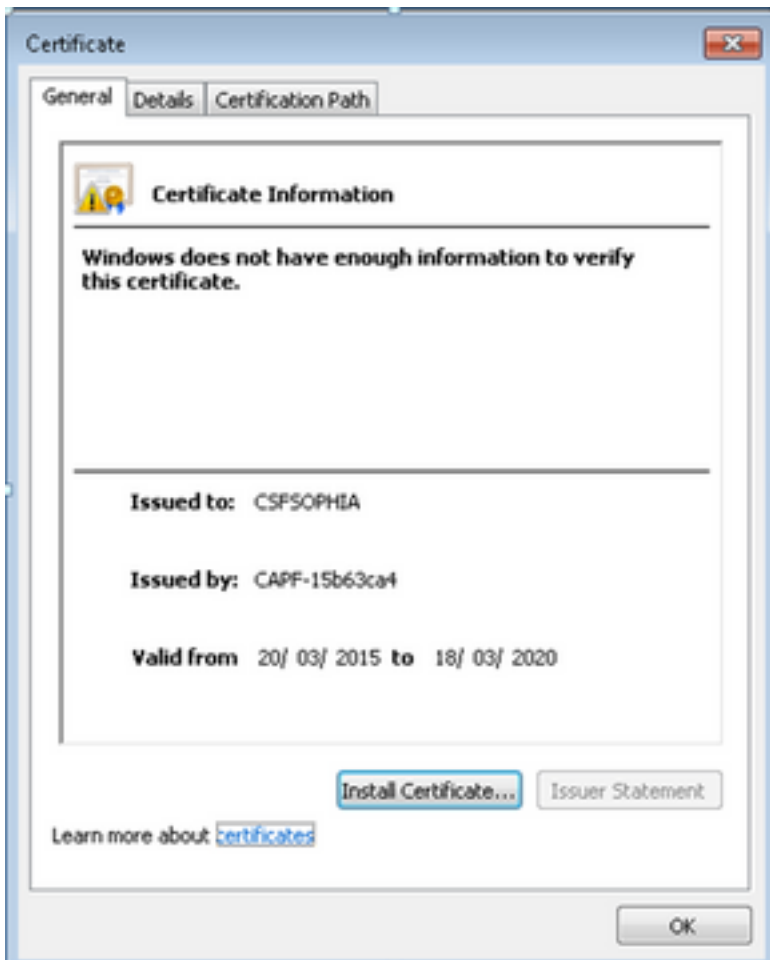


Verificar

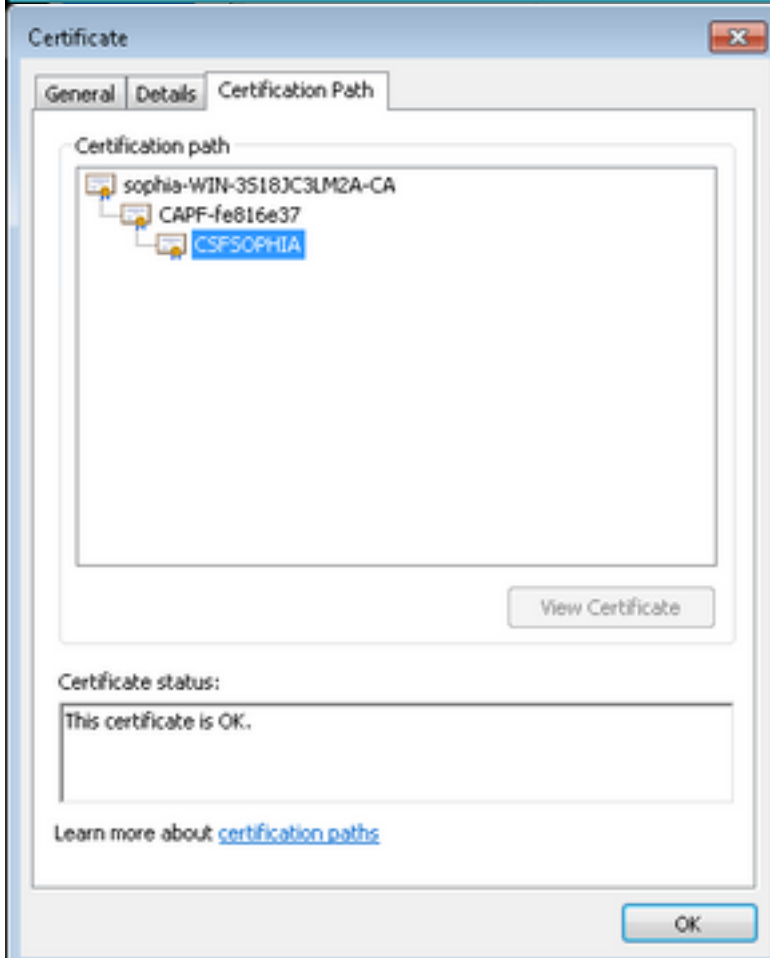
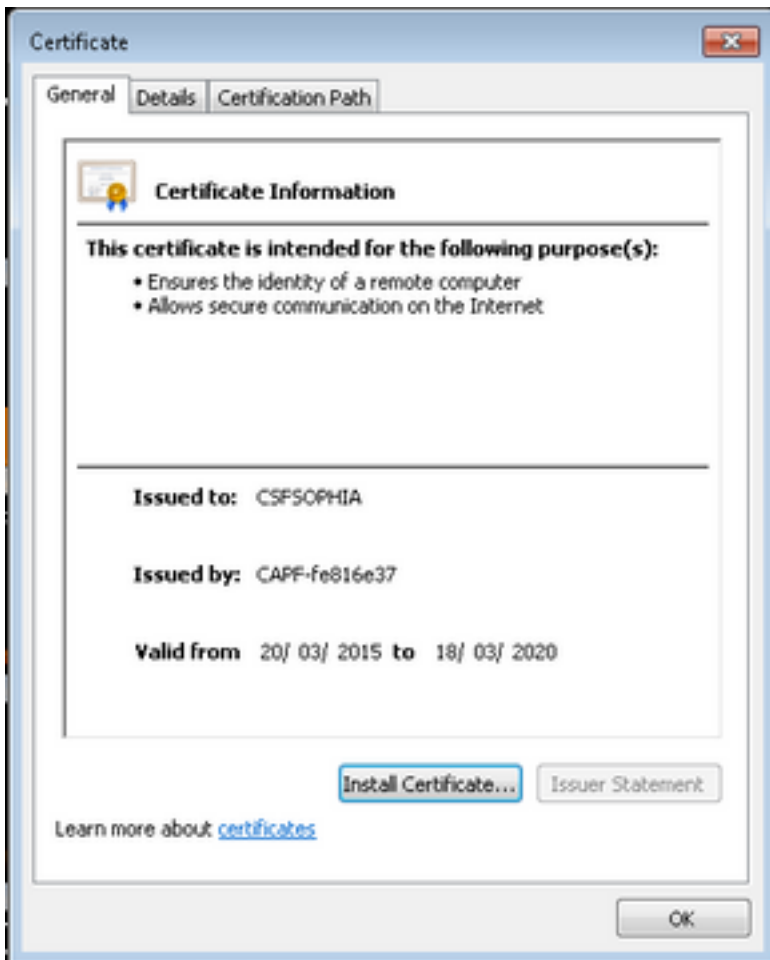
Compare o LSC quando CAPF auto-chamuscado e CAPF Ca-assinado:

Como você puder ver destas imagens para o LSC, do ponto de vista LSC, CAPF é a CA raiz ao usar o CAPF auto-assinado mas o CAPF é o subordinado CA (intermediário) quando usando o CAPF Ca-assinado.

LSC quando CAPF Auto-assinado



LSC quando CAPF Ca-assinado



Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

Defeito conhecido: O certificado assinado CA CAPF, CERT da raiz deve ser transferido arquivos pela rede como a CM-confiança:

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