Certificado CAPF assinado pela CA para CUCM

Contents

Introduction

Este documento descreve como obter um certificado de função de proxy de autoridade de certificação (CAPF) assinado pela autoridade de certificado (CA) para Cisco Unified Communications Manager (CUCM). Sempre há solicitações para assinar o CAPF com CA externa. Este documento mostra a razão pela qual entender como ele funciona é tão importante quanto o procedimento de configuração.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas no Cisco Unified Communications Manager versão 8.6 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Limitação

Uma autoridade de certificação diferente pode ter requisitos diferentes para o CSR. Há relatórios cuja versão diferente da CA OpenSSL tem alguma pergunta específica para o CSR, no entanto, a CA do Microsoft Windows funciona bem com o CSR do Cisco CAPF até o momento; por isso, a discussão não será abordada neste artigo.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- CA do Microsoft Windows Server 2008.
- Cisco Jabber para Windows (versões diferentes podem ter nomes diferentes para a pasta de armazenamento do LSC).

Informações de Apoio

Finalidade de CAPF assinada por CA

Alguns clientes gostariam de se alinhar com a política de certificado global na empresa, para que seja necessário assinar o CAPF com a mesma autoridade de certificação que outros servidores.

Mecanismo para esta PKI

Por padrão, o certificado localmente significativo (LSC) é assinado pelo CAPF, portanto, o CAPF é a CA para telefones nesse cenário. No entanto, quando você tenta obter o CAPF assinado pela CA externa, o CAPF neste cenário atua como CA subordinada ou intermediária.

A diferença entre o CAPF autoassinado e o CAPF assinado por CA é: o CAPF é a CA raiz para LSC, ao fazer o CAPF autoassinado, o CAPF é a CA subordinada (intermediária) para LSC durante a criação de CAPF assinados por CA.

Como o CSR CAPF é diferente dos outros CSRs?

Em relação ao RFC5280, a extensão de uso da chave define a finalidade (por exemplo, criptografia, assinatura, assinatura de certificado) da chave contida no certificado. O CAPF é um proxy de certificado e uma CA e ele pode assinar o certificado para os telefones; mas o outro certificado, como CallManager, Tomcat ou IPSec, atua como leaf (identidade do usuário). Quando você procura no CSR para eles, você pode ver que o CSR CAPF tem a função **Certificate Sign**, mas não os outros.

CSR CAPF:

```
        Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
```

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

CSR Tomcat:

```
Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

CSR CallManager:

```
Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

CSR IPSec:

Atributos: Extensões solicitadas: Uso estendido de chave X509v3: Autenticação do servidor da Web TLS, autenticação de cliente Web TLS, uso da chave X509v3 do sistema final IPSec: Assinatura digital, criptografia de chave, criptografia de dados, contrato de chave

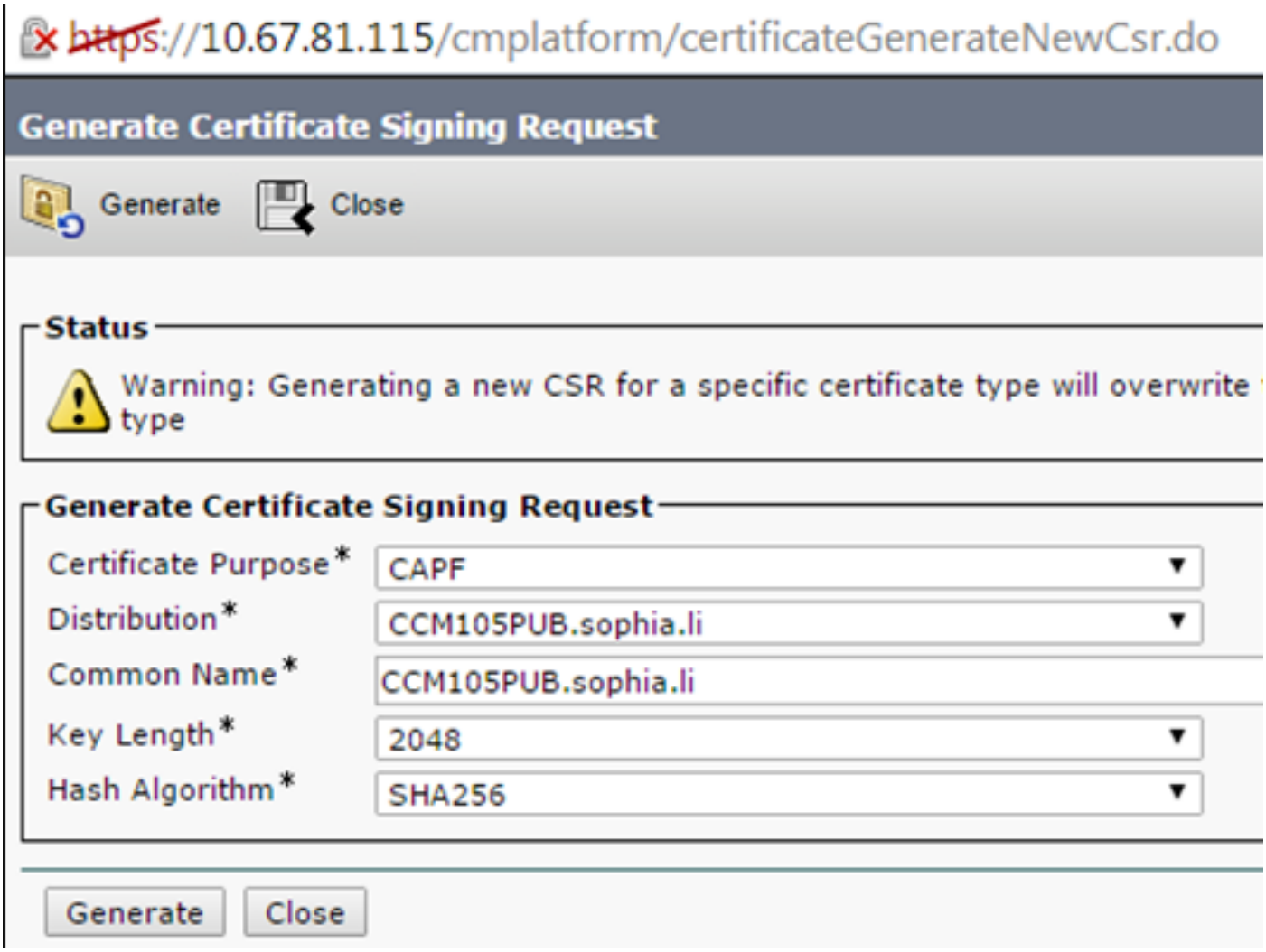
Configurar

Aqui está um cenário, a CA raiz externa é usada para assinar o certificado CAPF: para criptografar o sinal/mídia para o cliente Jabber e o telefone IP.

Etapa 1. Torne o cluster CUCM como um cluster de segurança.

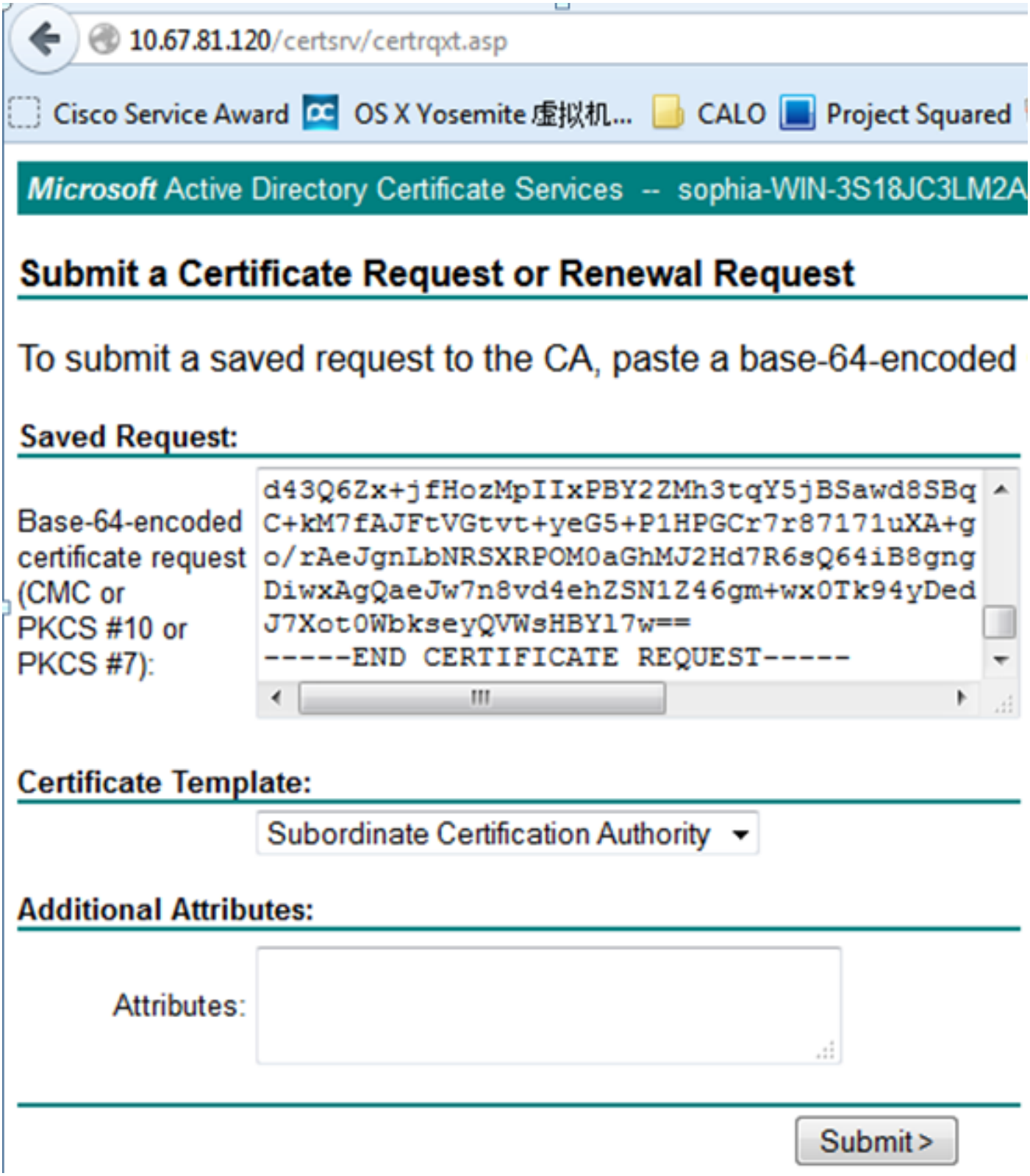
```
admin:utils ctl set-cluster mixed-mode
```

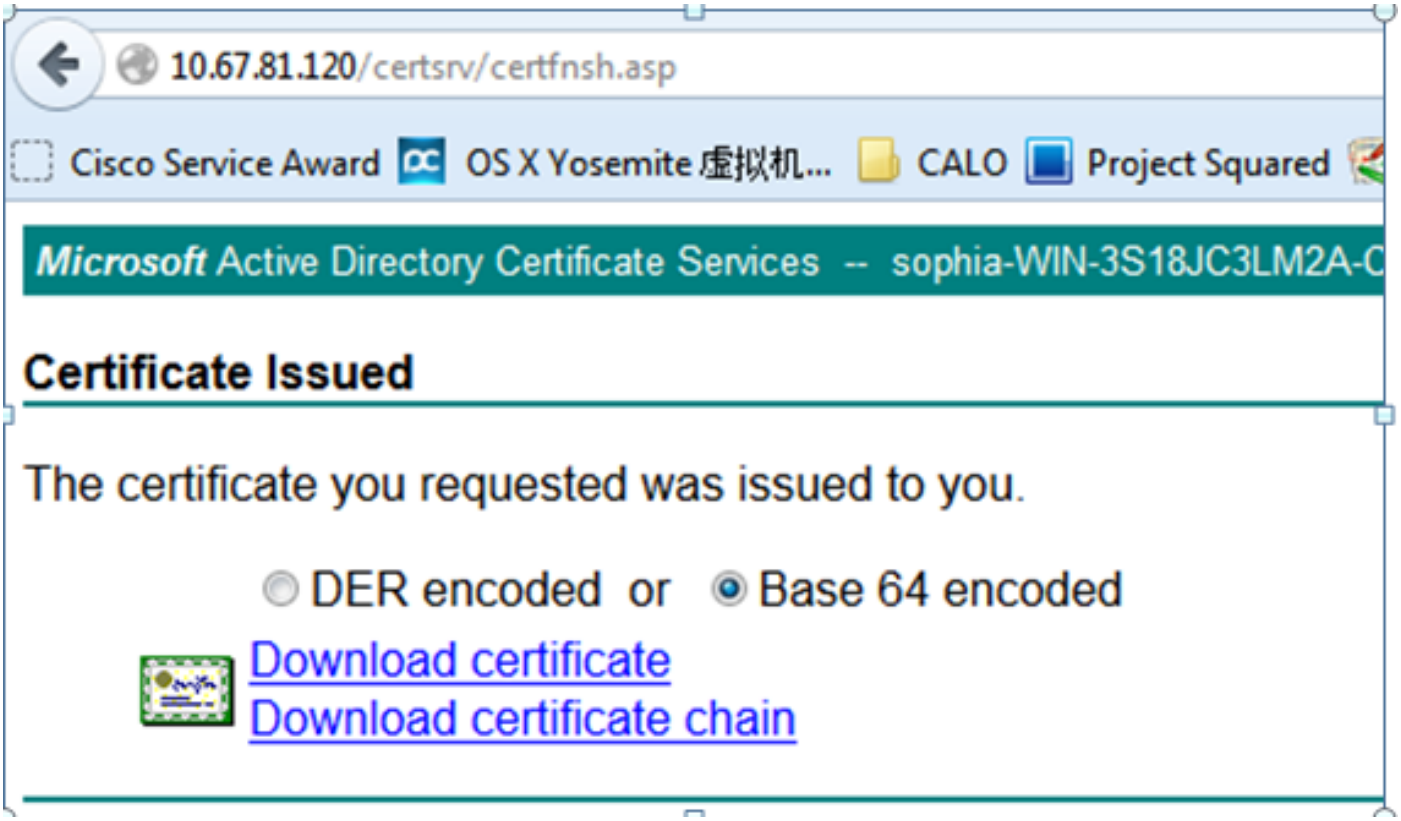
Etapa 2. Como mostrado na imagem, gere o CAPF CSR.



Etapa 3. Assinado com o CA (usando modelo subordinado no CA do Windows 2008).

Note: Você precisa de um modelo de **Autoridade de certificação subordinada** do usuário para assinar 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 >

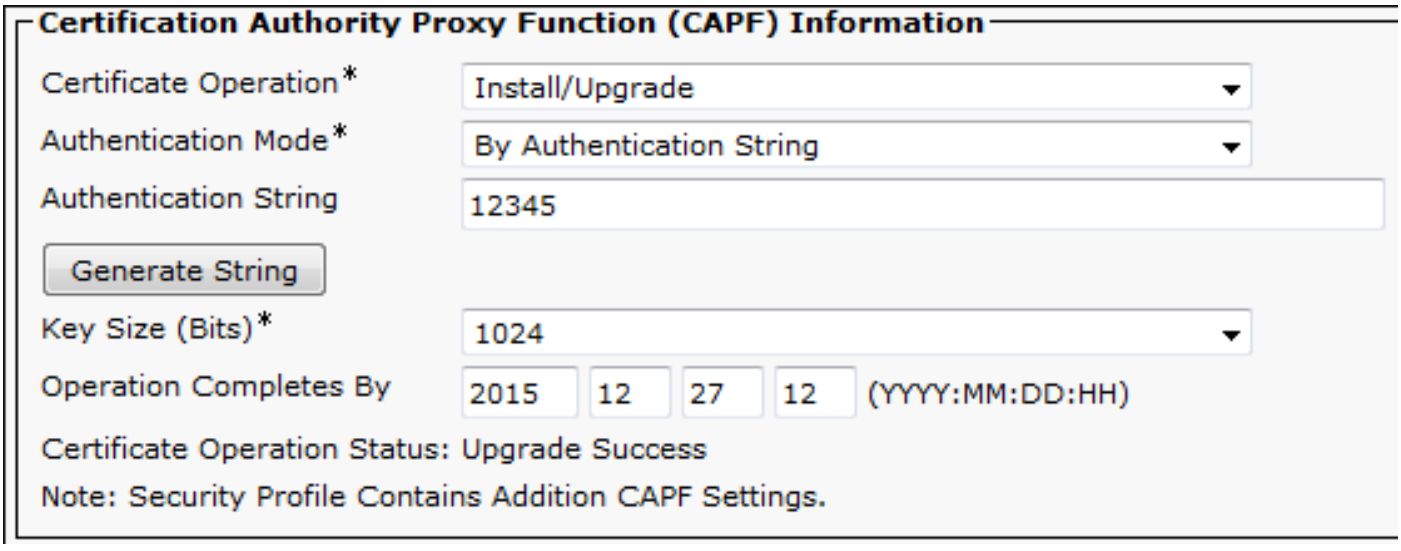


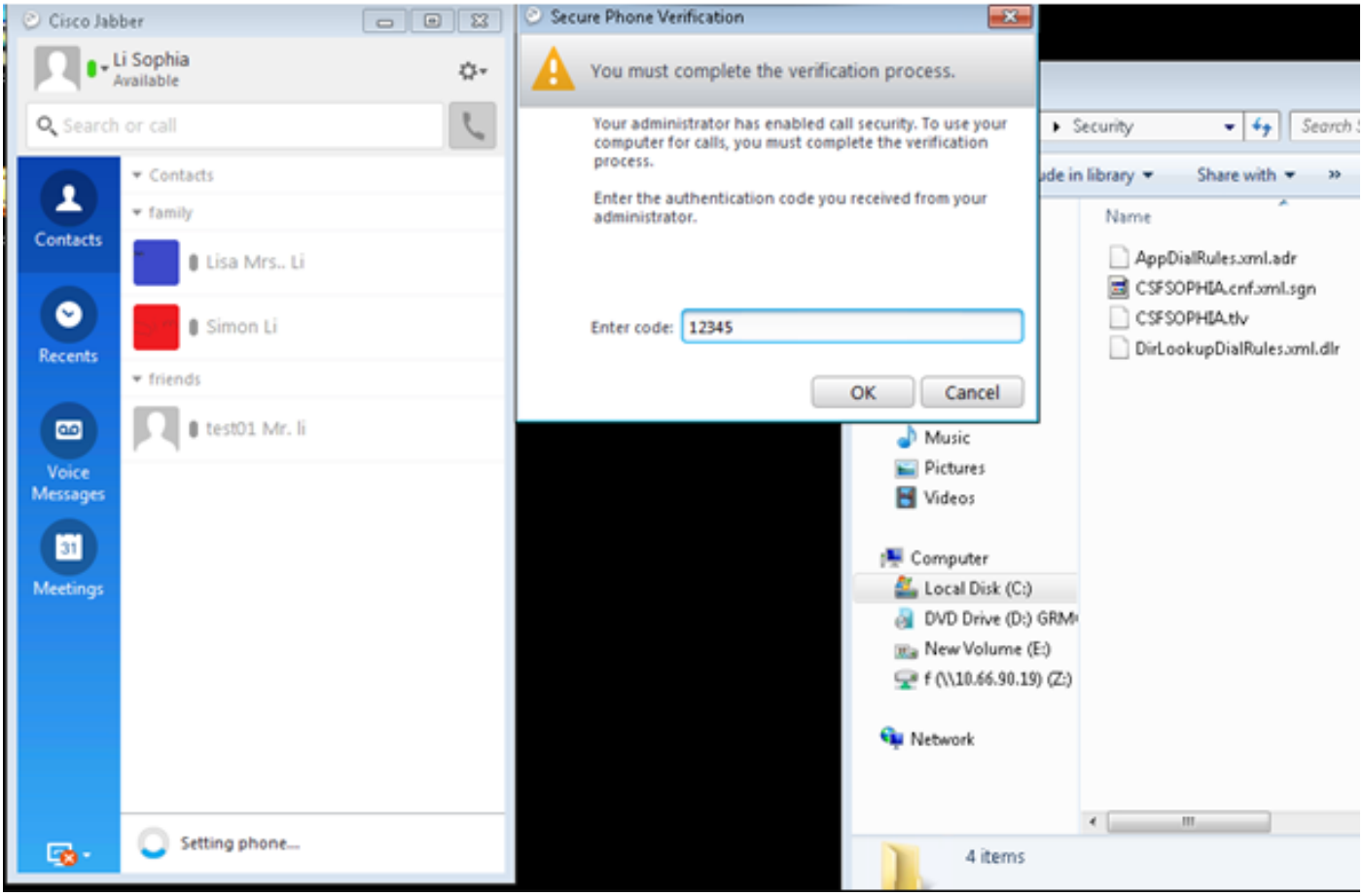
Etapa 4. Carregue a CA raiz como CAPF-trust e o certificado do servidor como CAPF. Para esse teste, carregue também esta CA raiz como CallManager-trust para ter conexão TLS entre Jabber e o serviço CallManager , pois o LSC assinado também precisa ser confiável pelo serviço CallManager. Como mencionado no início deste artigo, é necessário alinhar a CA para todos os servidores, de modo que essa CA tenha sido carregada no CallManager preparada para a criptografia de sinal/mídia. Para o cenário de implantação do telefone IP 802.1x, você não precisa criar o CUCM no modo misto ou carregar a CA que assina o CAPF como CallManager-trust no servidor CUCM.

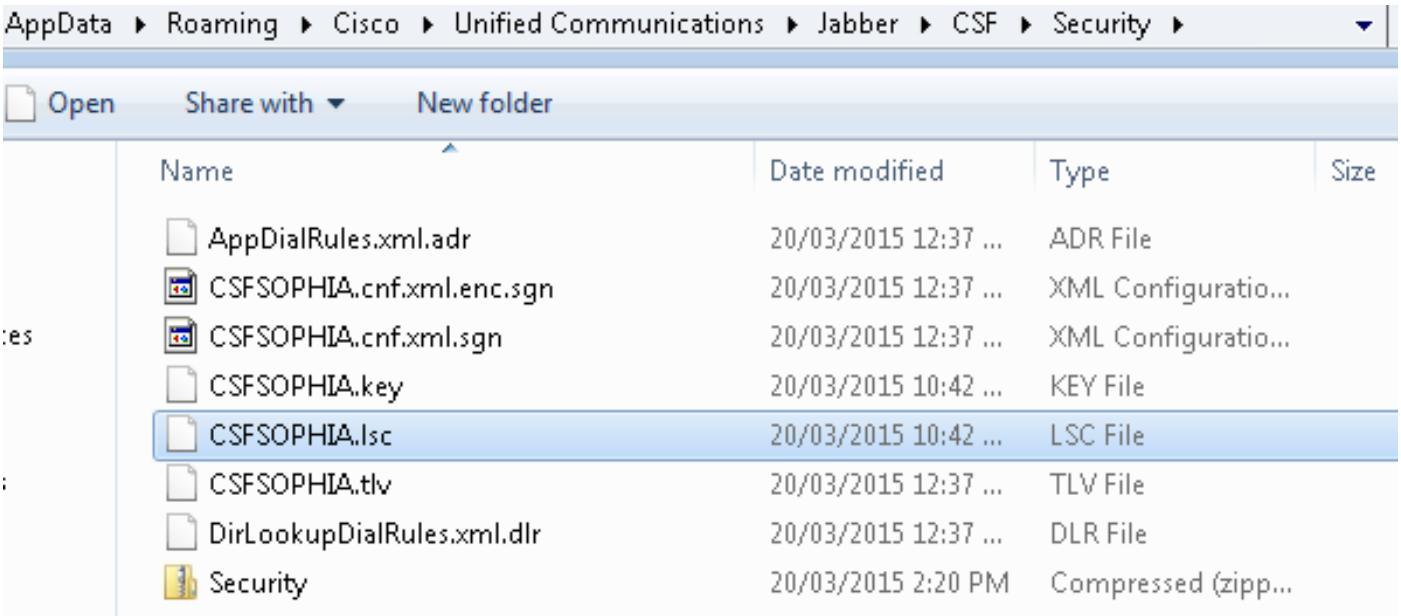
Etapa 5. Reinicie o serviço CAPF.

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

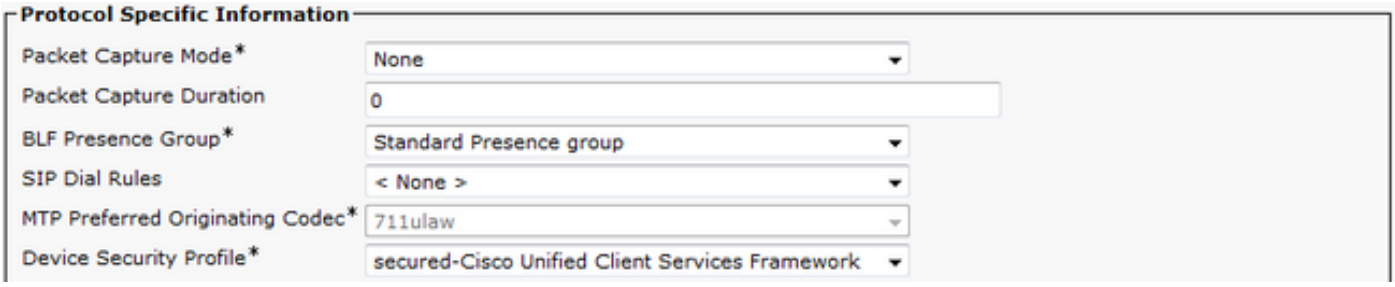
Passo 7. LSC do softphone Jabber assinado.



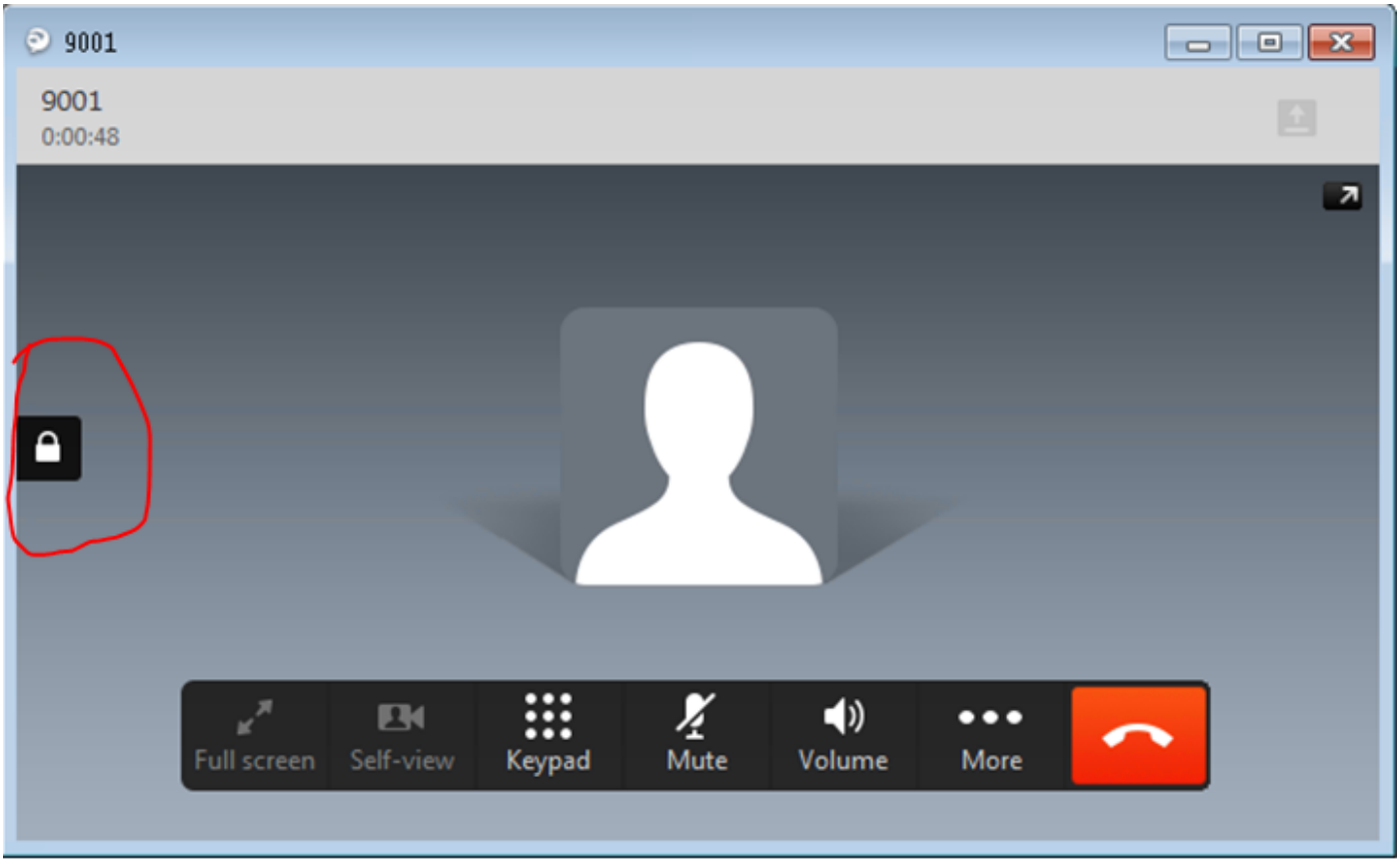




Etapa 8. Ative o perfil de segurança para o softphone Jabber.



Etapa 9. Agora o RTP protegido aparece como:

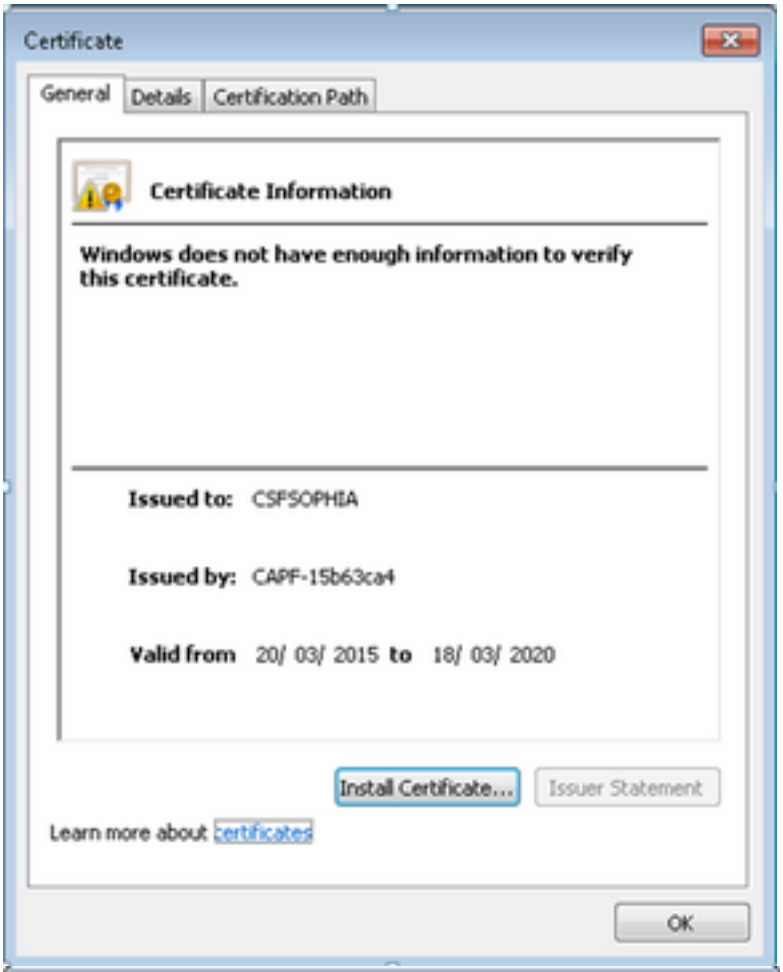


Verificar

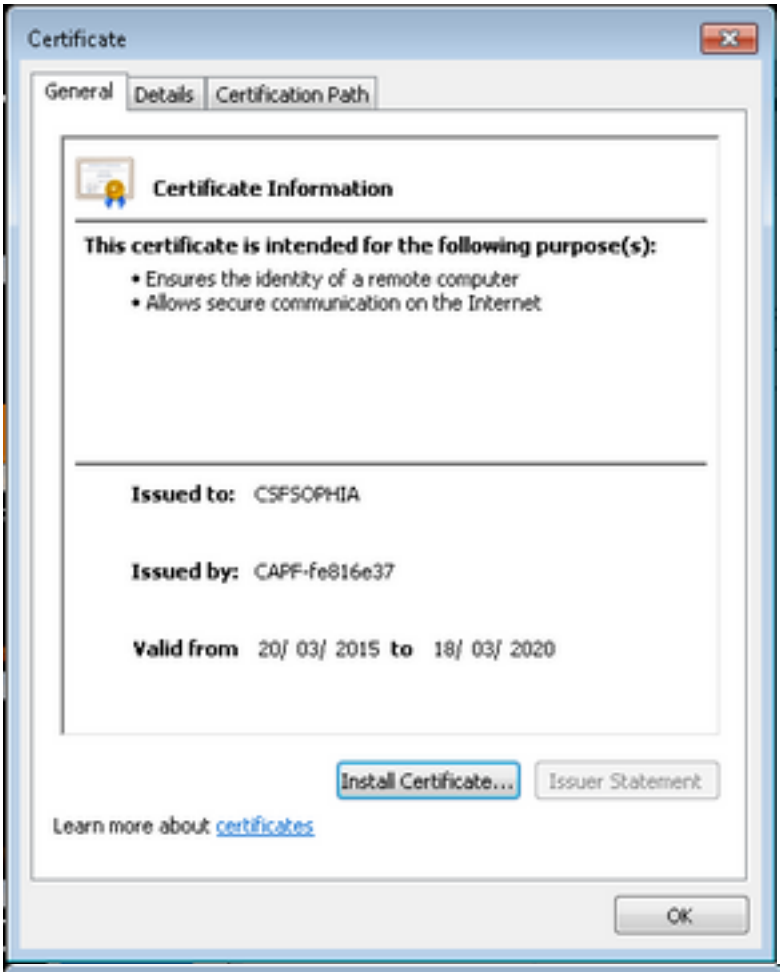
Compare o LSC quando ele for um CAPF e CAPF autoassinado por CA:

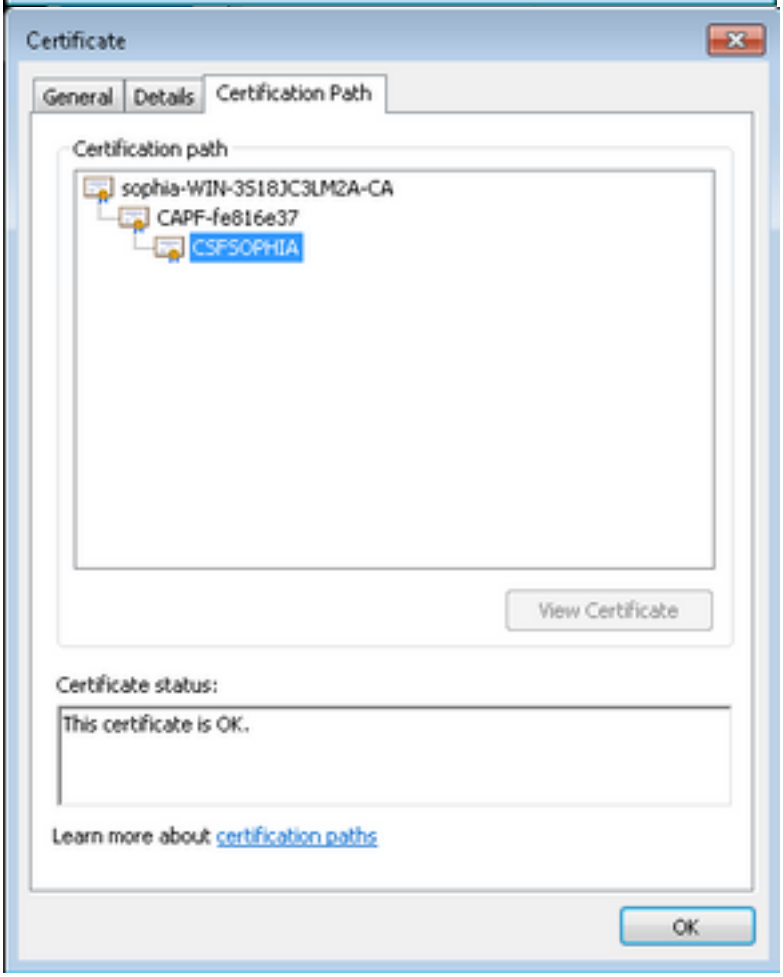
Como você pode ver nessas imagens para LSC, no ponto de vista do LSC, CAPF é a CA raiz ao usar o CAPF autoassinado, mas CAPF é a CA subordinada (intermediária) ao usar o CAPF assinado por CA.

LSC quando CAPF é autoassinado



LSC quando CAPF é assinado por CA


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

Alerta:

o cliente Jabber LSC mostrando toda a cadeia de certificados neste exemplo é diferente do telefone IP. Os telefones IP AS são projetados com base no RFC 5280 (3.2. Caminhos de certificação e Confiança); em seguida, o AKI (Identificador de Chave da Autoridade) está ausente; em seguida, o CAPF e o certificado raiz da CA não estão presentes na cadeia de certificados. A falta do certificado CAPF/Root CA na cadeia de certificados fará com que algum problema do ISE autentique telefones IP durante a autenticação 801.x sem carregar os certificados CAPF e Root no ISE. Há outra opção no CUCM 12.5 com LSC assinado por CA off-line externa diretamente, de modo que o certificado CAPF não precisa ser carregado para a autenticação 802.1x do ISE para o telefone IP.

Troubleshoot

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

Informações Relacionadas

Defeito conhecido: Autoridade de CAPF assinado por CA, o certificado raiz deve ser carregado como CM-trust:

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