

CUCM的CA签字的CAPF认证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[限制](#)

[背景信息](#)

[CA的目的签署了CAPF](#)

[此PKI的机制](#)

[CAPF CSR如何是与其他CSR不同？](#)

[配置](#)

[验证](#)

[LSC，当自己签署的CAPF](#)

[LSC，当CA签名的CAPF](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何获得Cisco Unified通信管理器的(CUCM) Certificate Authority (CA)签字的认证机关代理功能(CAPF)认证。总是有请求签署与外部CA的CAPF。本文为什么显示知道如何工作是一样重要的象配置过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 公共密钥基础设施(PKI)
- CUCM安全配置

使用的组件

本文的信息根据Cisco Unified通信管理器版本8.6和以上。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令的潜在影响。

限制

不同的CA也许有不同的需求到CSR。有报道然而Openssl CA的另外版本安排某特定请求CSR微软视窗CA工作很好与从Cisco CAPF的CSR到目前为止，讨论在此条款上不会被覆盖。

相关产品

本文可能也与这些一起使用硬件和软件版本：

- 微软视窗服务器2008 CA。
- Windows的Cisco Jabber (不同的versions也许有文件夹的不同的名称能存储LSC)。

背景信息

CA的目的签署了CAPF

一些用户希望与公司那么那里是需要签署与CA的CAPF和其他服务器一样的globe认证策略with对齐。

此PKI的机制

默认情况下，局部重要的认证(LSC)由CAPF，因此CAPF签字是电话的CA在此方案。然而，当您设法获得CAPF签字由外部CA时，然后在此方案的CAPF作为辅助CA或中间CA。

在自己签署的CAPF和CA签名的CAPF之间的区别是：CAPF是根CA对LSC，当执行自己签署的CAPF，CAPF时是辅助(中间)CA对LSC，当执行CA签名的CAPF时。

CAPF CSR如何是与其他CSR不同？

看待对[RFC5280](#)，密钥用法扩展名定义了目的(即，编码、签字签名的认证在认证包含的)的键。CAPF是认证代理，并且他们作为分支的CA和能签署认证到电话，但是另一个认证类似呼叫管理器，Tomcat，IPSec(用户身份)。当您调查CSR为他们时，您能看到CAPF CSR有CertificateSign角色，但是不是其他。

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
```

呼叫管理器CSR :

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

IPSec CSR :

属性：被请求的扩展：X509v3延长的密钥用法：TLS Web服务器认证， TLS网络客户端认证，
IPSec结束系统X509v3密钥用法：数字签名，关键编码，数据编码，关键协议

配置



这是一个方案，外部根CA使用签署CAPF认证：加了密信号/媒体Jabber客户端和IP电话的。

Step1。做您的CUCM簇作为安全簇。

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

步骤2.如镜像所显示，请生成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

步骤3.签署了此与CA (使用在Windows 2008 CA的辅助模板)。

Note:您需要用户**辅助认证机构**模板签署此认证。

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-----
```

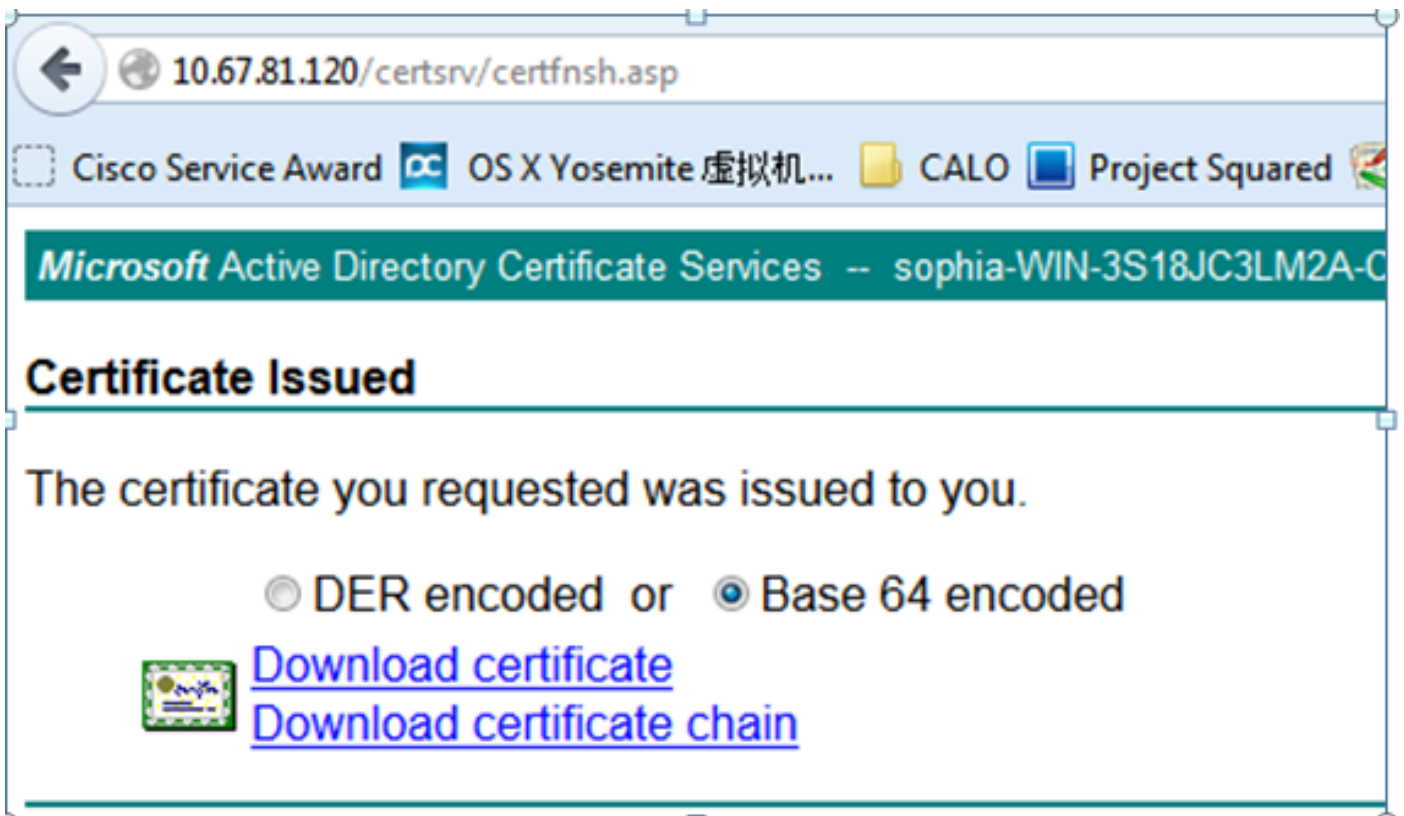
Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Submit >



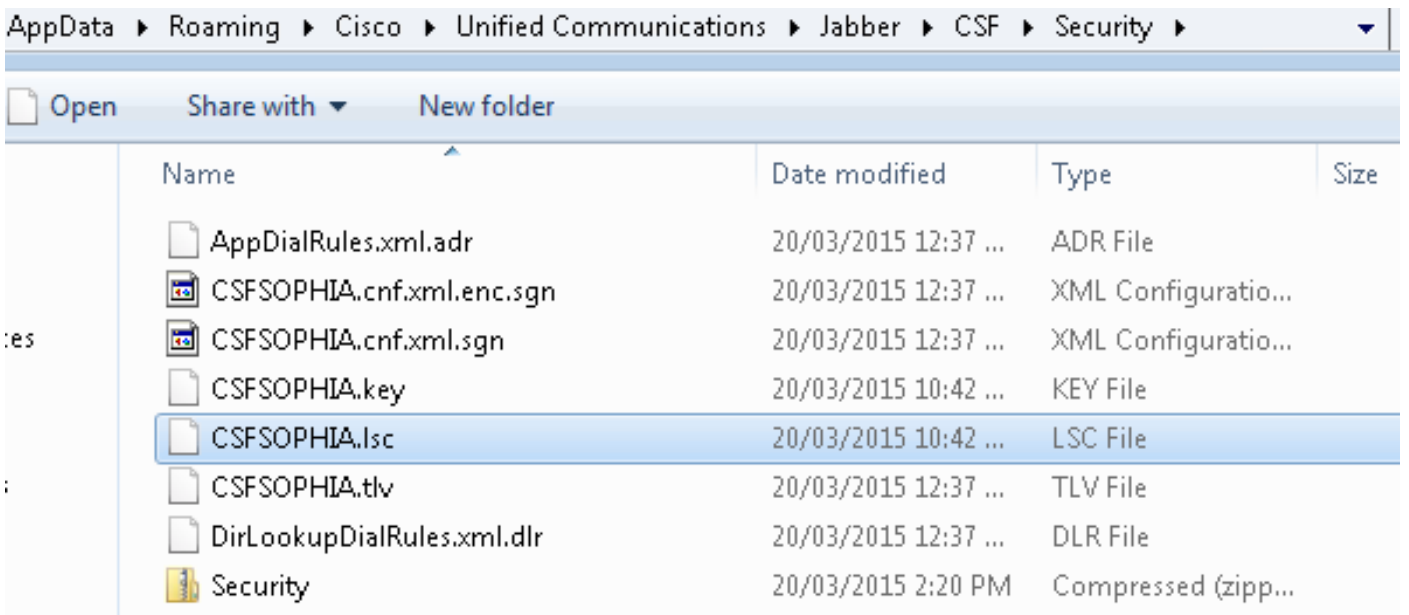
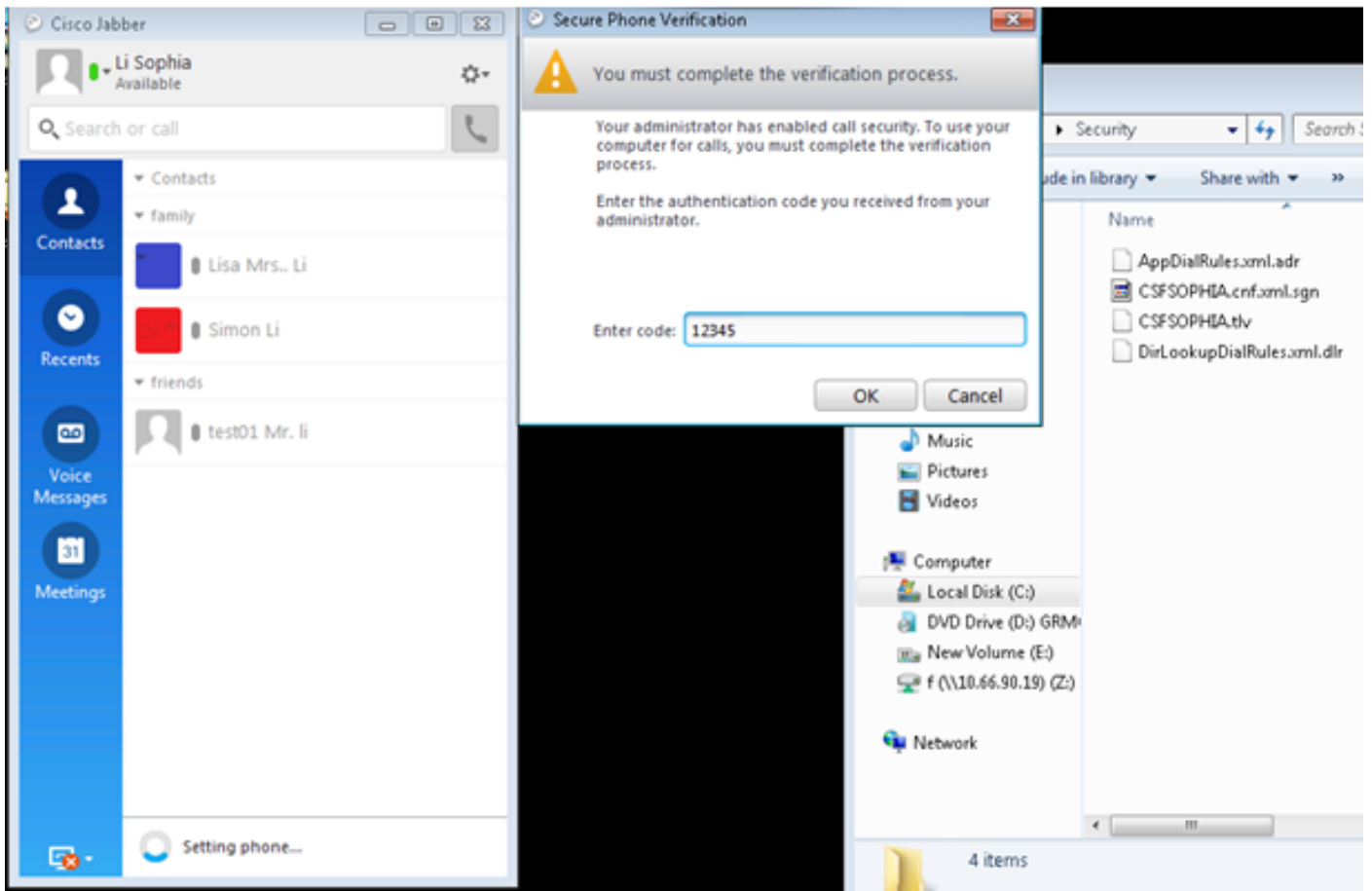
步骤4.加载根CA作为CAPF信任和服务器证明作为CAPF。对于此测试，也请加载此根CA，呼叫管理器信任有Jabber和呼叫管理服务之间的TLS连接作为签字的LSC需要由呼叫管理服务委托。如被提及在此条款初，有需要对齐所有服务器的CA，因此应该加载了此CA到呼叫管理器已经信号/媒体加密的。对于配置IP电话802.1x scenario，您不必须做CUCM作为签到CAPF作为呼叫管理器信任到CUCM服务器的混合模式或加载CA。

步骤5.重新启动CAPF服务。

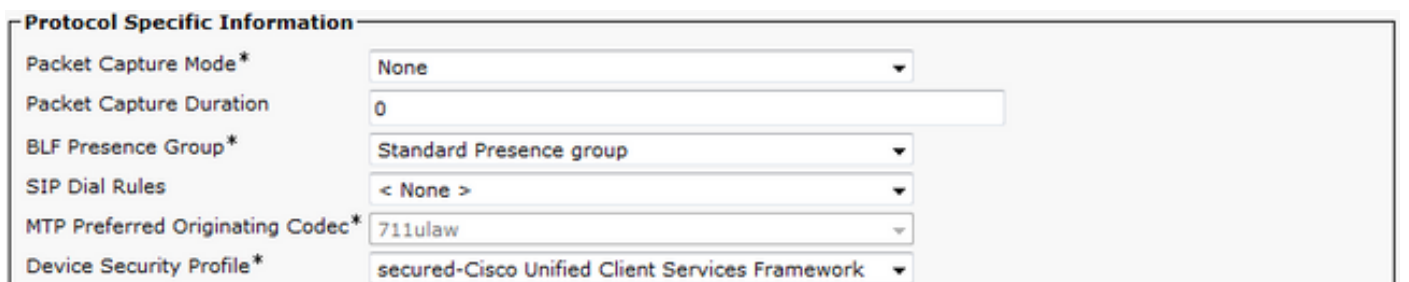
步骤6.重新启动在所有附注的CallManager/TFTP服务。

步骤7.签署了Jabber softphone LSC。

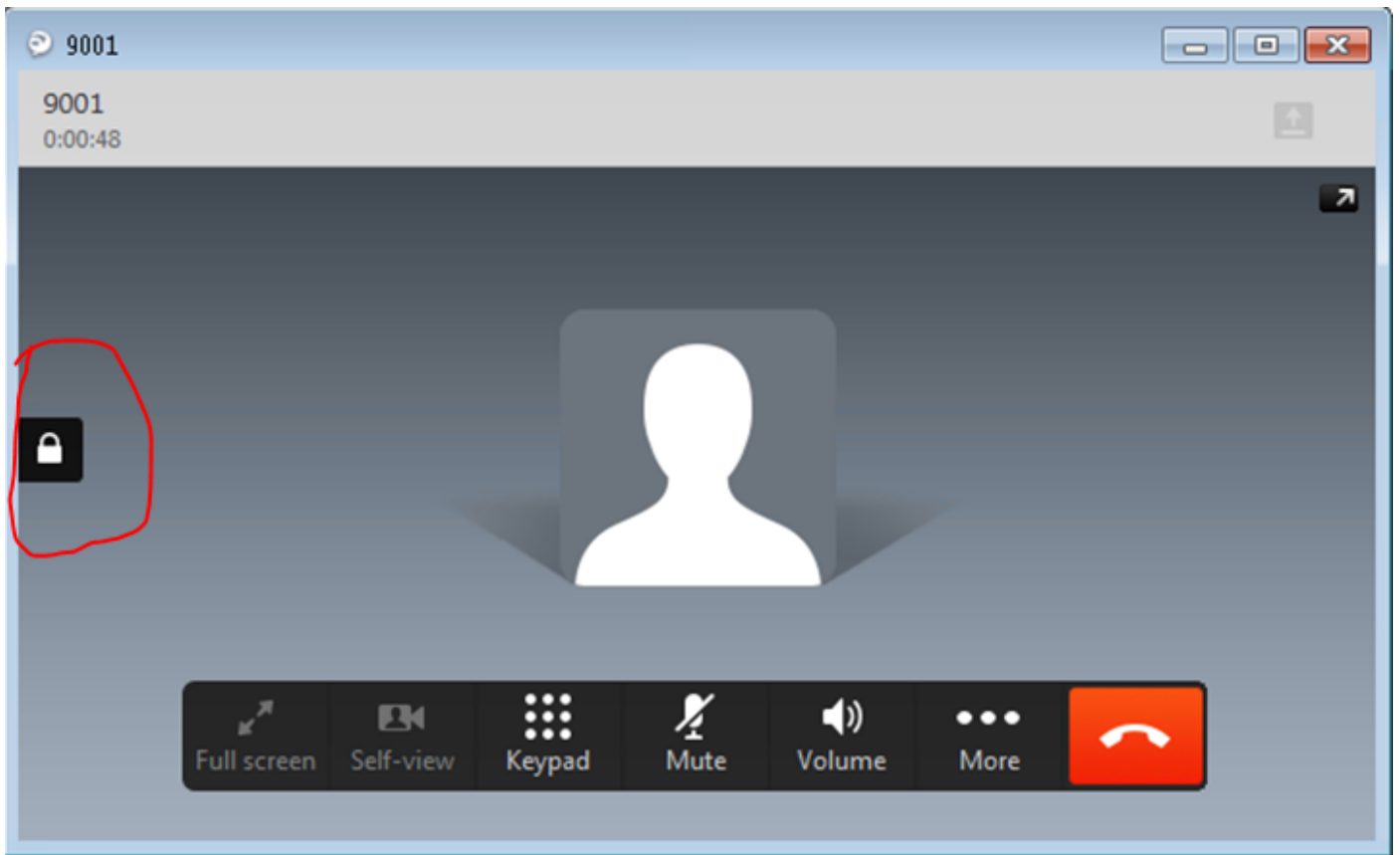
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation *	Install/Upgrade
Authentication Mode *	By Authentication String
Authentication String	12345
<input type="button" value="Generate String"/>	
Key Size (Bits) *	1024
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)
Certificate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



步骤8. Enable (event) Jabber的softphone安全配置文件。



第9步。现在获取的RTP发生如下：

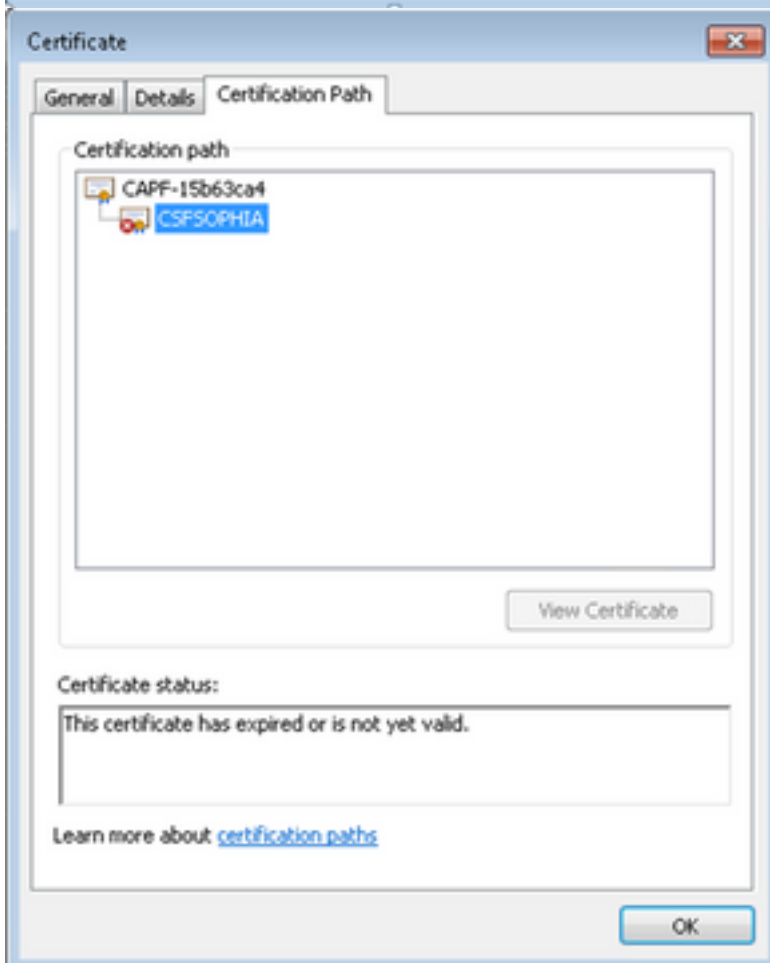
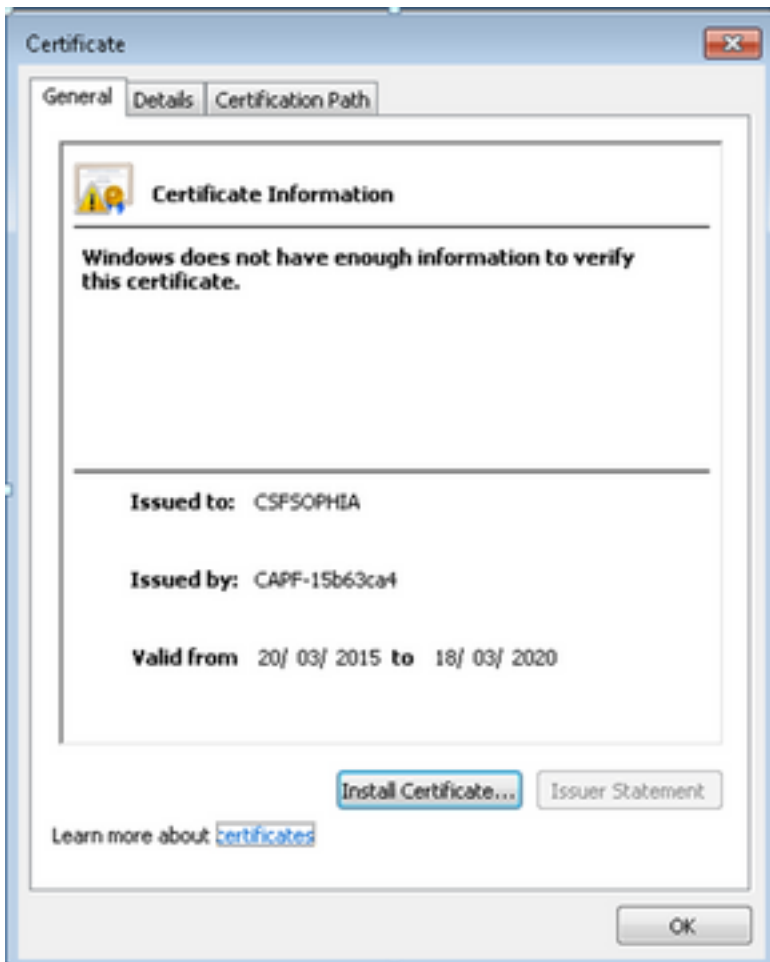


验证

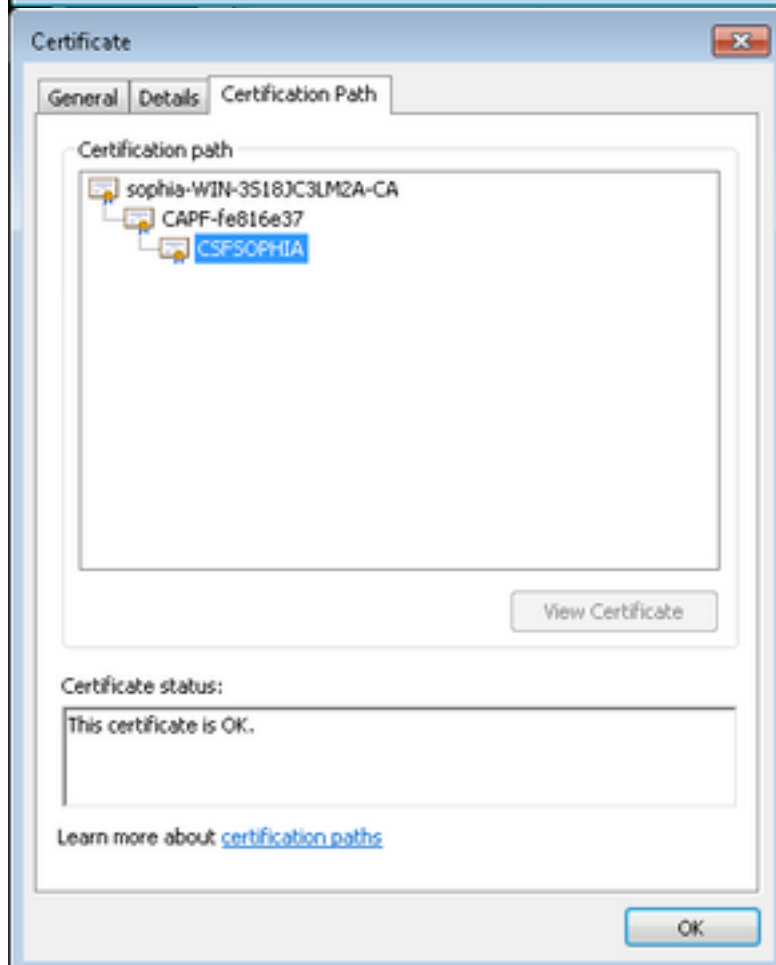
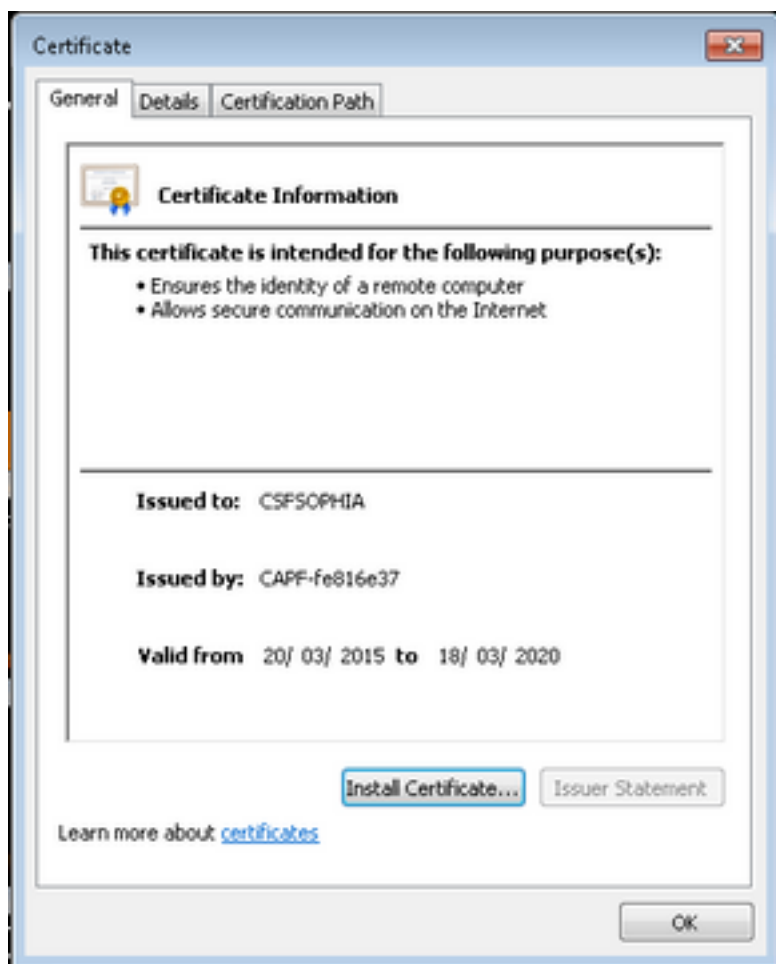
请比较LSC，当自被烧焦的CAPF和CA签名的CAPF：

正如你从这些镜像看到为LSC，从LSC观点，CAPF是根CA，当使用自己签署的CAPF时，但是CAPF是辅助(中间)CA，当使用CA签名的CAPF时。

LSC，当自己签署的CAPF



LSC , 当CA签名的CAPF



故障排除

目前没有针对此配置的故障排除信息。

相关信息

已知缺陷：CA必须加载签字的CAPF认证，根cert作为CM信任：

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