关于CUCM的CA签字的CAPF证书的技术说明

目录

简介

本文描述如何获取Cisco Unified Communications Manager的(CUCM) Certificate Authority (CA)签字的一认证机关代理功能(CAPF)证书。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象配置程序。

先决条件

要求

Cisco 建议您了解以下主题：

- 公用密钥基础结构 (PKI)
- CUCM安全配置

使用的组件

本文档中的信息根据Cisco Unified Communications Manager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潜在影响。

相关产品

本文档也可用于以下硬件和软件版本：

- MS Windows服务器2008 CA。
- Windows的思科Jabber。

背景信息

CA目的签署了CAPF

一些客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globle证书策略whith对齐。

此PKI的机制

默认情况下，局部重要的证书(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。

在自已签署的CAPF和CA签名的CAPF之间的区别是：CAPF是根CA对LSC，当执行自已签署的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，密钥用法分机定义了目的(即，编码、签字签名的证书在证书包含的)密钥。CAPF是证书代理，并且他们作为分支的CA和能签署证书到电话，但是另一证书类似CallManager， Tomcat， IPSec (用户标识)。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
```

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 ：

属性：请求的扩展：X509v3延长的密钥用法：TLS Web服务器验证， TLS网络客户端验证，IPSec终端系统X509v3密钥用法：数字签名，关键编码，数据编码，关键协议

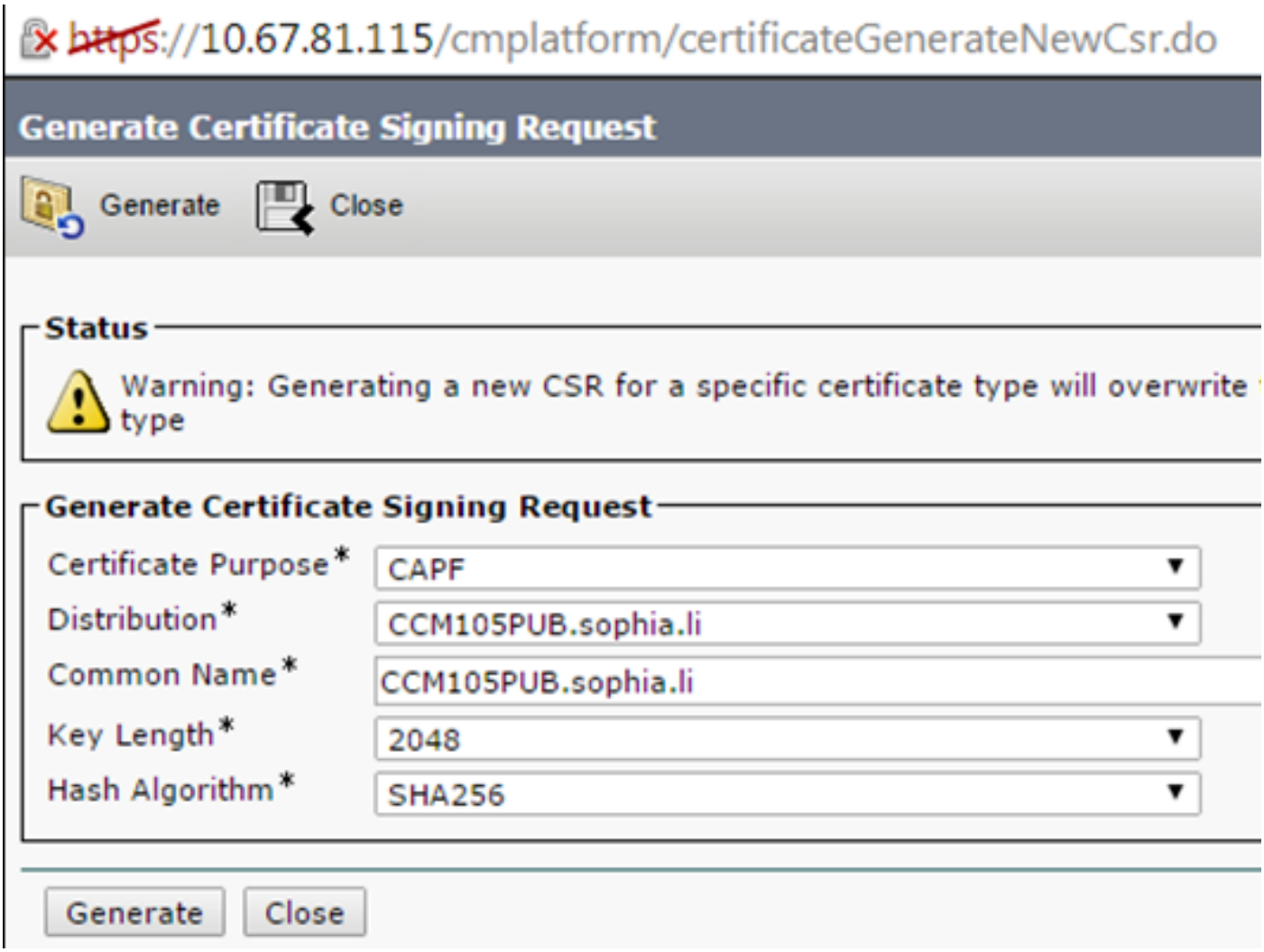
配置

这是签署与外部CA的CAPF的步骤。

步骤1:做您的CUCM集群作为安全集群。

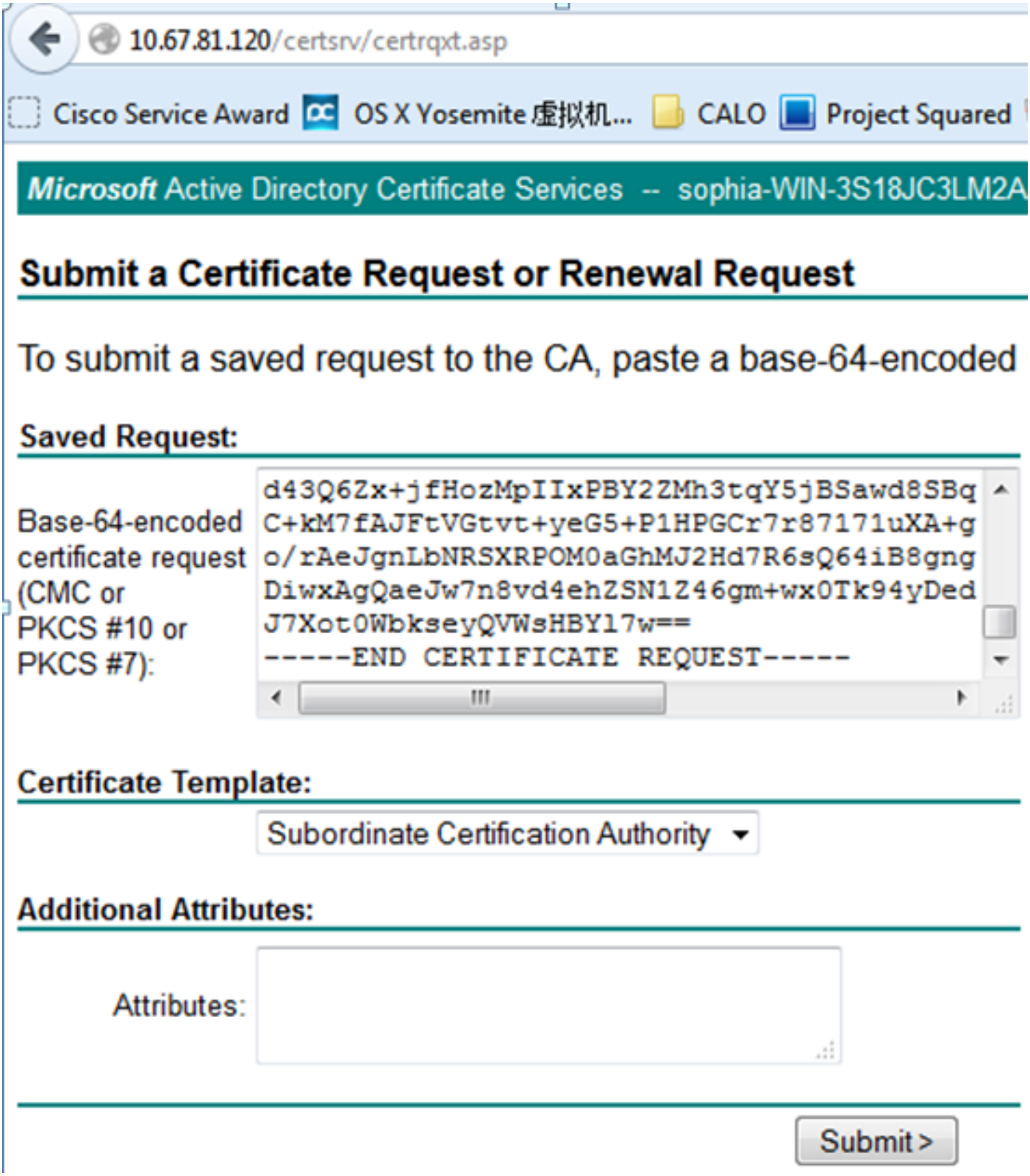
```
admin:utils ctl set-cluster mixed-mode
```

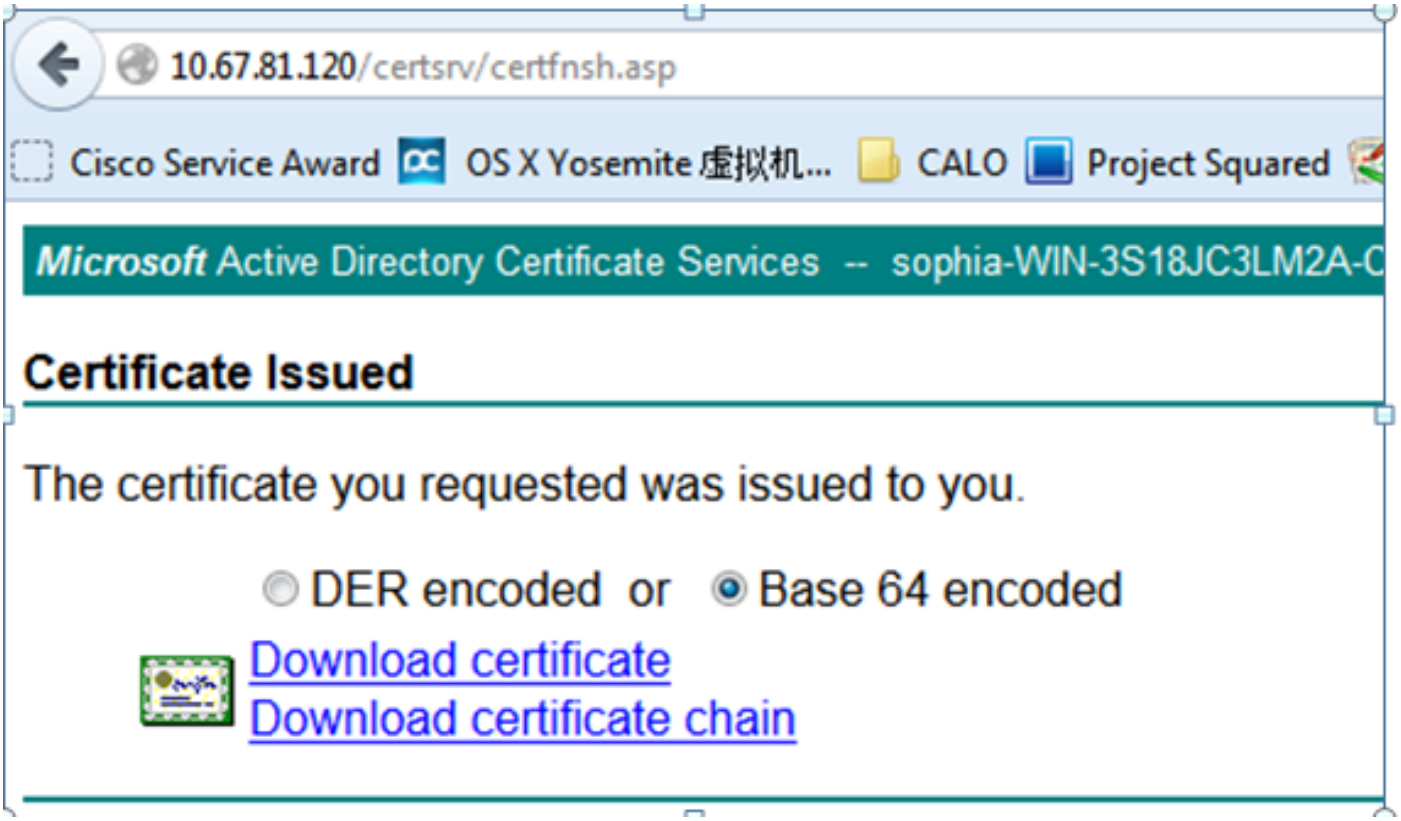
步骤2.如镜像所显示，请生成CAPF CSR。



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

注意：您需要用户**辅助证书颁发机构**模板签署此证书。


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 >

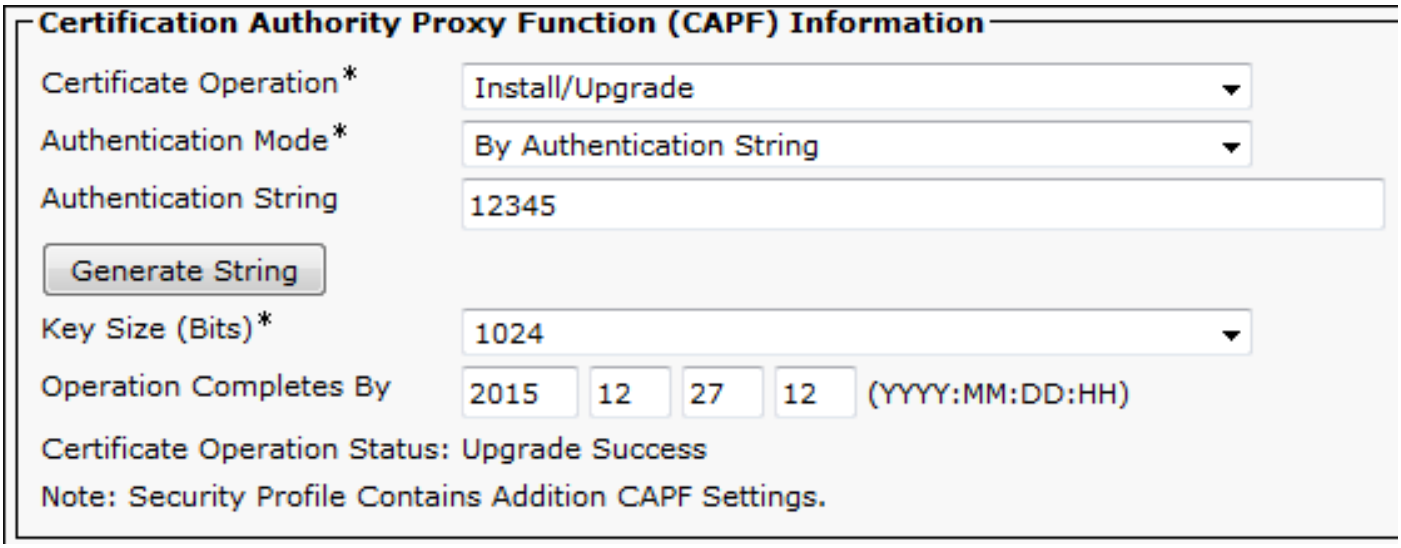


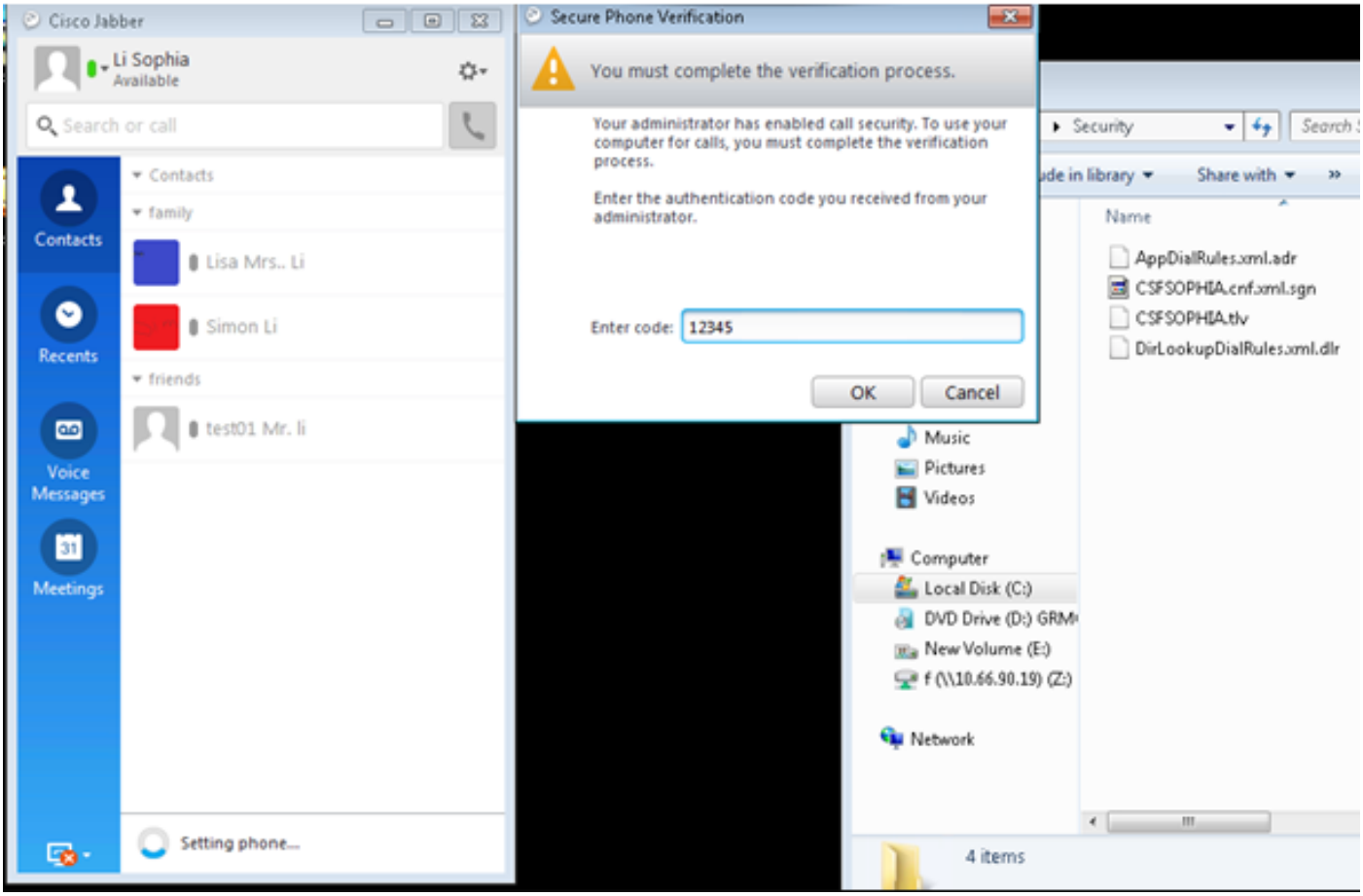
步骤4.上传根CA作为CAPF托拉斯和服务器证书作为CAPF。

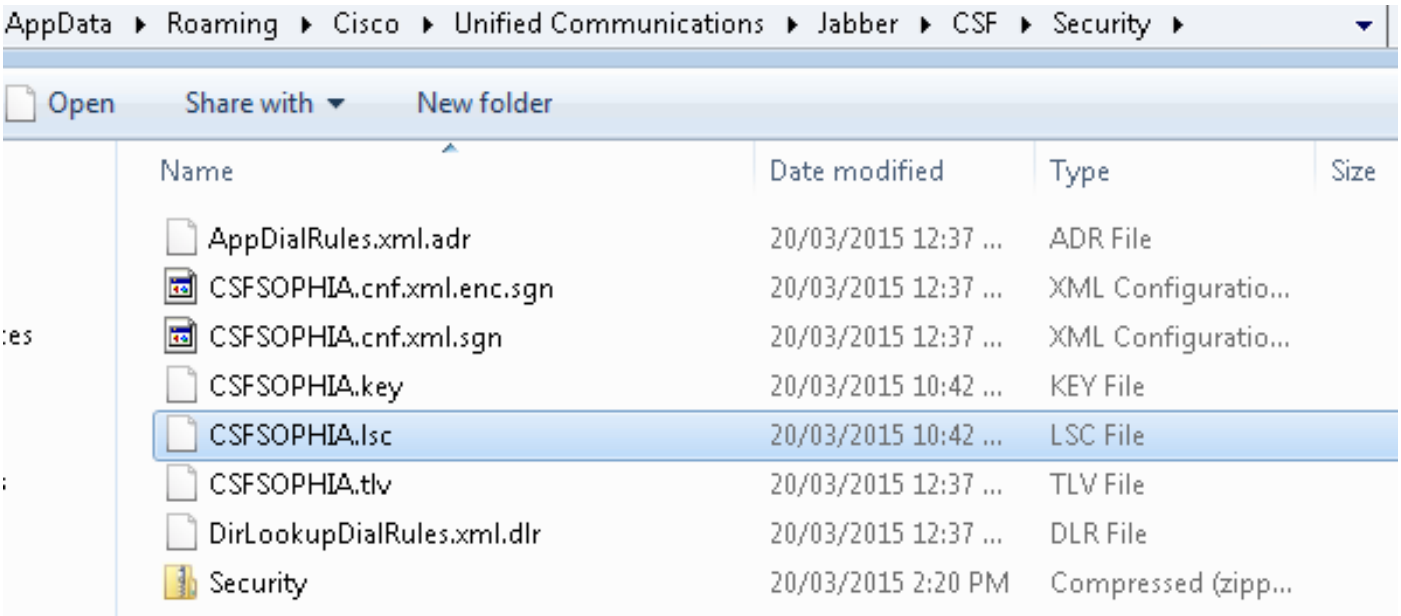
步骤5.重新启动CAPF服务。

步骤6.重新启动在所有笔记的CallManager/TFTP服务。

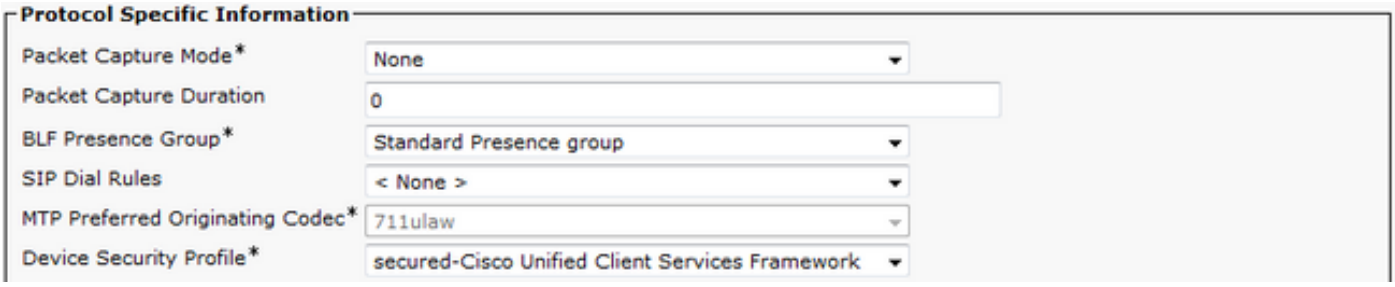
步骤7.签署了Jabber softphone LSC。



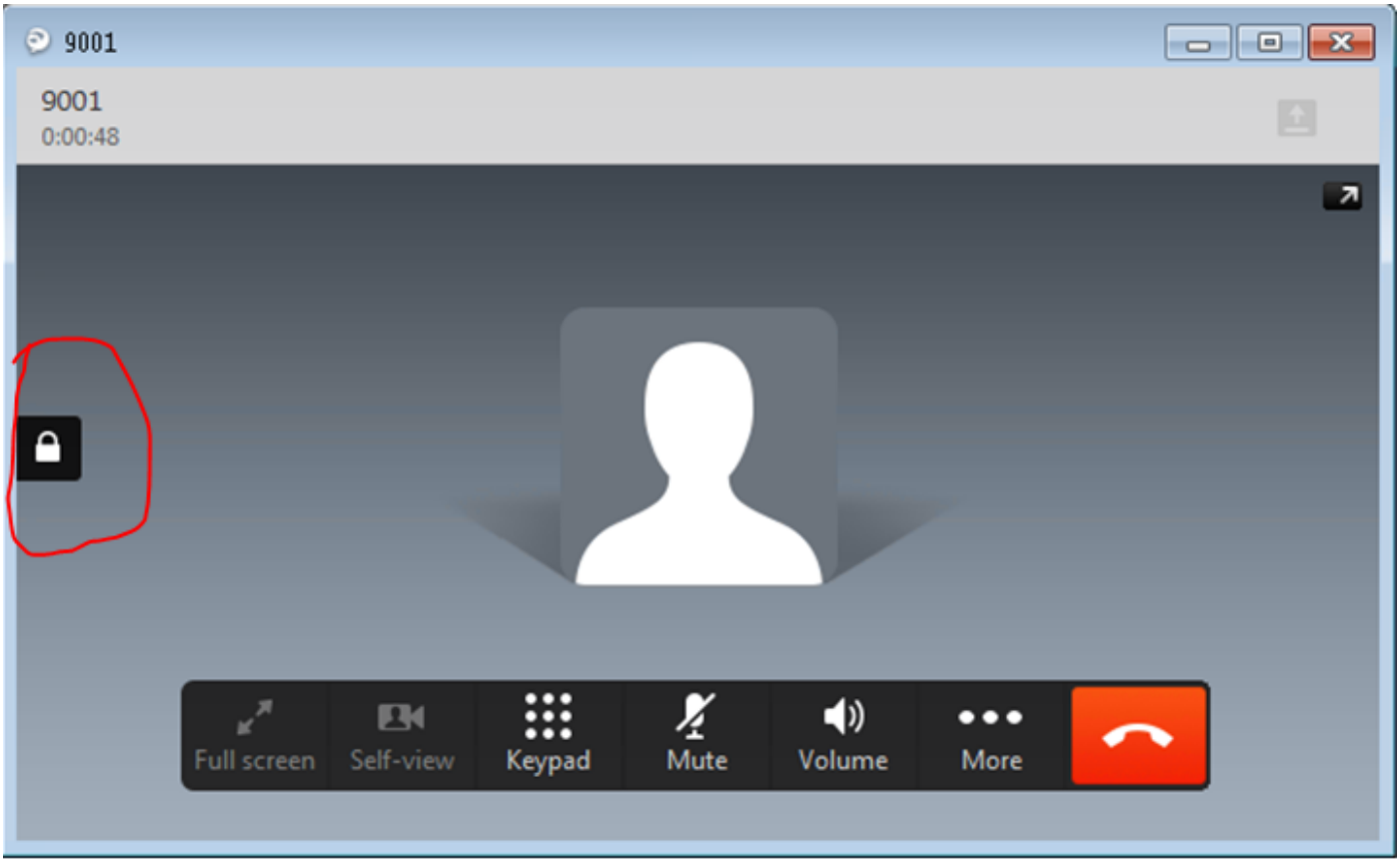




步骤8.启用Jabber的softphone安全配置文件。



步骤 9 现在获取的RTP发生如下：

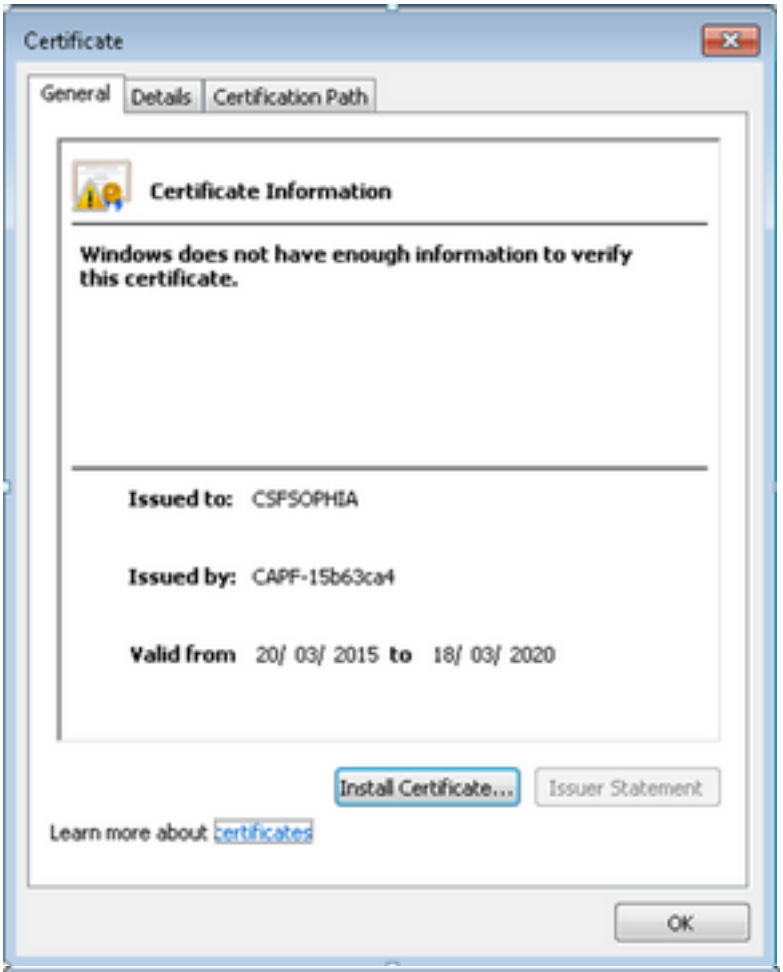


验证

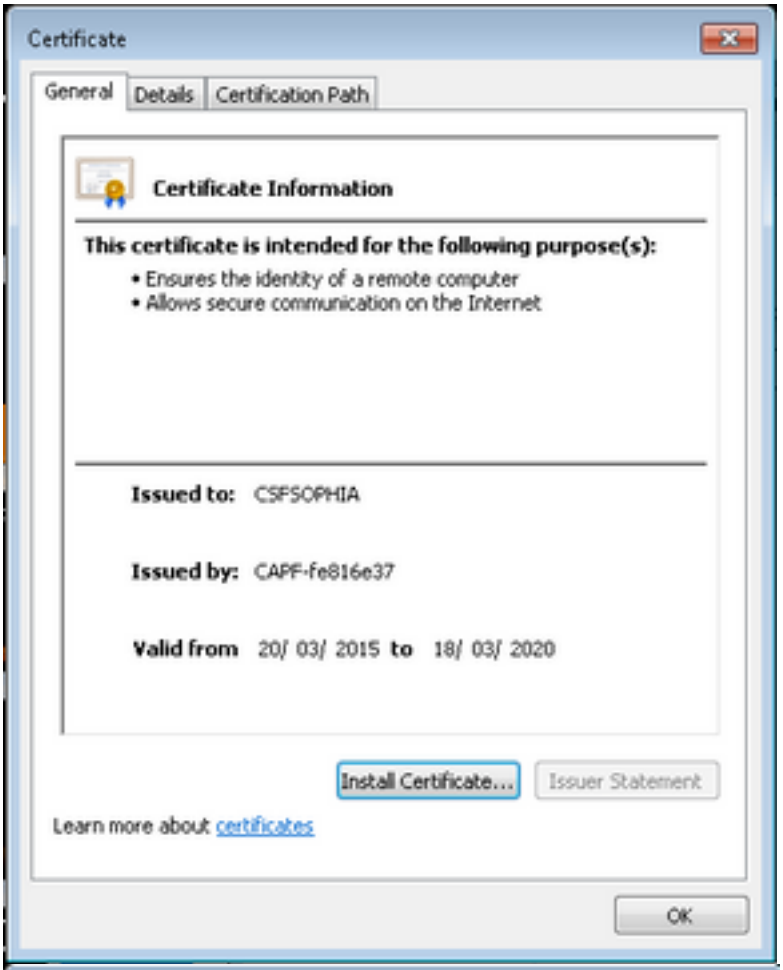
比较LSC，当赛弗被烧焦的CAPF和CA签名的CAPF ：

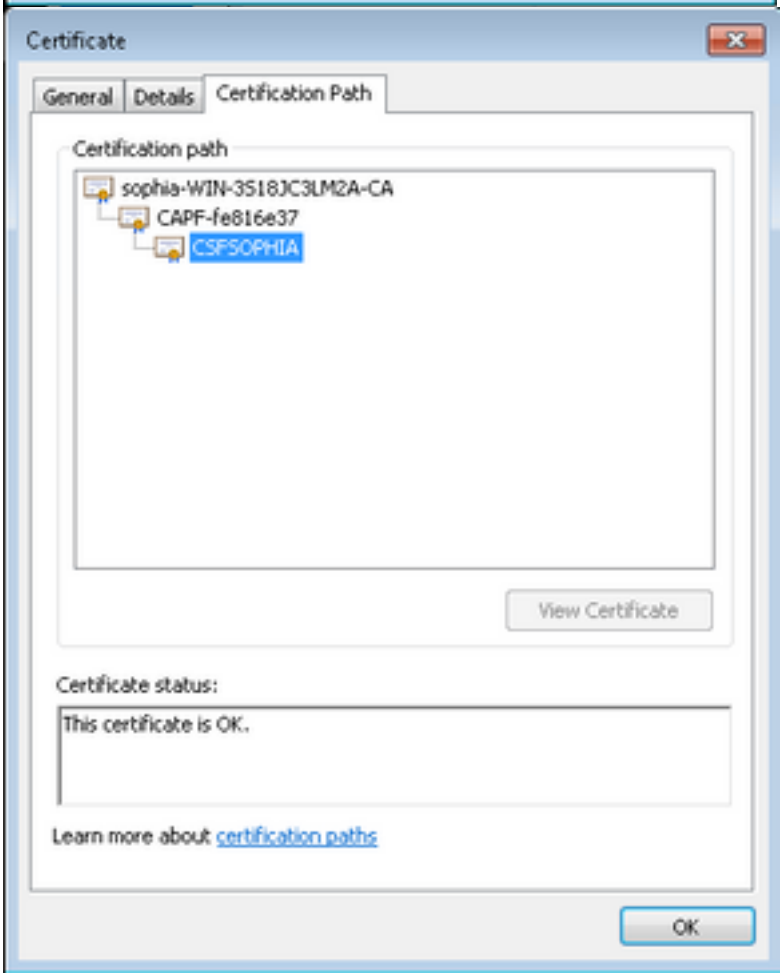
正如你从这些镜像看到为LSC，从LSC观点， CAPF是根CA，当使用自己签署的CAPF时，但是CAPF是辅助(中间) CA，当使用CA签名的CAPF时。

LSC，当自己签署的CAPF



LSC，当CA签名的CAPF


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

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必须上传签字的CAPF证书，根cert作为CM托拉斯
： https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir