CA 为 CUCM 签署的 CAPF 证书

目录

简介

本文档介绍如何获取证书颁发机构 (CA) 为 Cisco Unified Communications Manager (CUCM) 签署的证书颁发机构代理功能 (CAPF) 证书。 始终要求通过外部 CA 签署 CAPF。本文档说明了为什么了解它的工作原理与配置过程同样重要。

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

本文档中的信息基于 Cisco Unified Communications Manager 8.6 版及以上版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

限制

不同的 CA 可能对 CSR 有不同的要求。有一些报告表明，不同版本的 OpenSSL CA 具有特定的 CSR 要求，但是到目前为止 Microsoft Windows CA 可以很好地与 Cisco CAPF 的 CSR 配合使用，本文将不对此进行讨论。

相关产品

本文档也可用于以下硬件和软件版本：

- Microsoft Windows Server 2008 CA。
- Windows 版 Cisco Jabber（不同版本可能使用不同的文件夹名称来存储 LSC）。

背景信息

CA 签署的 CAPF 的用途

有些客户希望与公司内的全局证书策略保持一致，因此需要使用与其他服务器相同的 CA 签署 CAPF。

此 PKI 的机制

默认情况下，本地重要证书 (LSC) 由 CAPF 签署，因此对于该场景，CAPF 是用于电话的 CA。但是，当您尝试获取由外部 CA 签署的 CAPF 时，此场景中的 CAPF 将充当从属 CA 或中间 CA。

自签 CAPF 和 CA 签署的 CAPF 之间的区别在于：执行自签 CAPF 时，CAPF 是 LSC 的根 CA；执行 CA 签署的 CAPF 时，CAPF 是 LSC 的从属（中间）CA。

CAPF CSR 与其他 CSR 有何不同？

对于 RFC5280，密钥用法扩展定义了证书中包含的密钥的用途（例如，加密、签名、证书签名）。CAPF 是一种 CA 证书代理，它可以签署电话证书，但 CallManager、Tomcat、IPSec 等其他证书将充当枝叶（用户身份）。 当您查看其CSR时，您可以看到CAPF CSR具有证书签**名角**色，但没有其他角色。

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, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
```

```
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

CallManager CSR：

```
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
```

IPSec CSR：

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

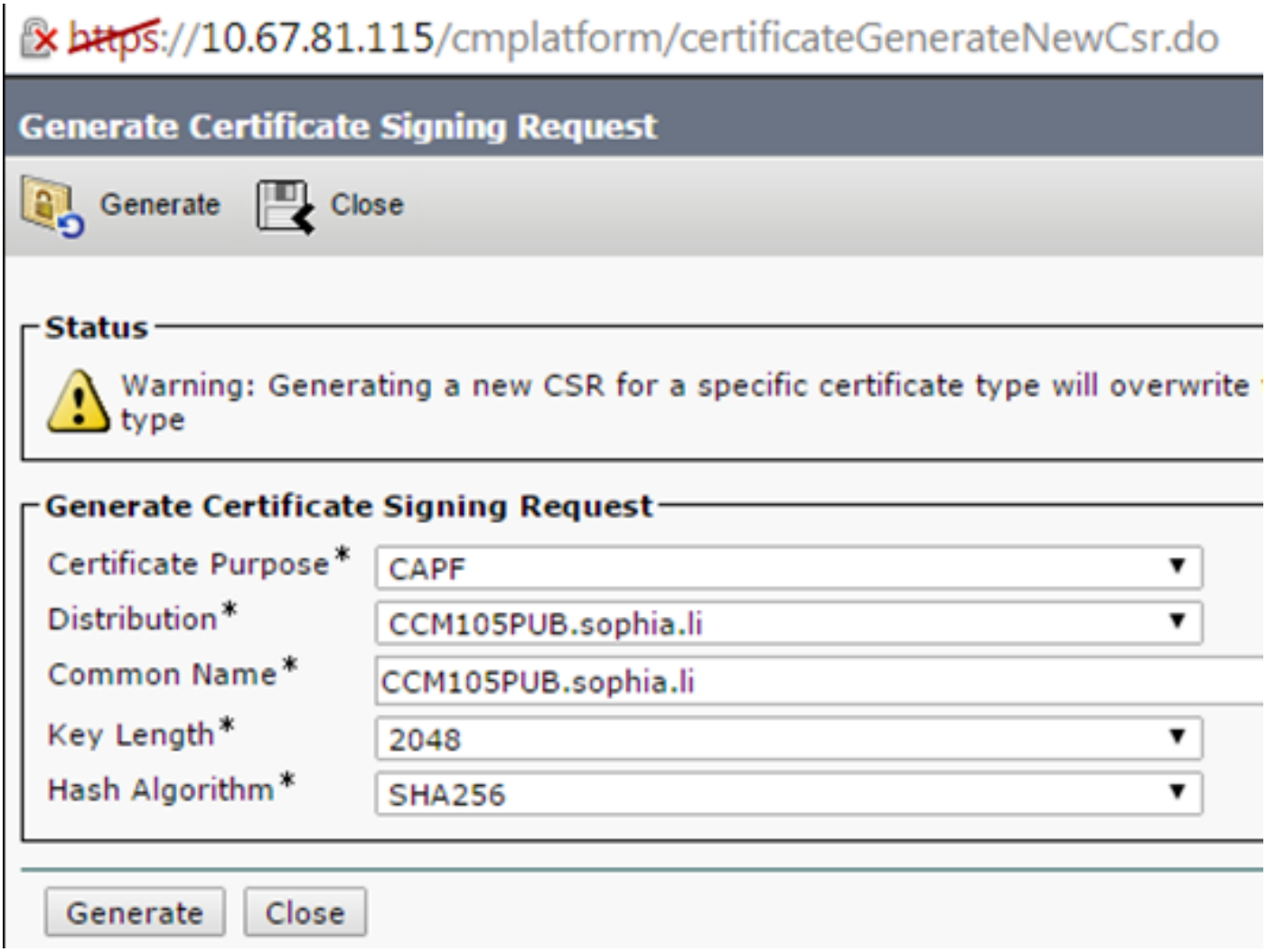
配置

存在以下场景：外部根 CA 用于签署 CAPF 证书：以加密 Jabber 客户端和 IP 电话的信号/介质。

步骤1.将CUCM集群设置为安全集群。

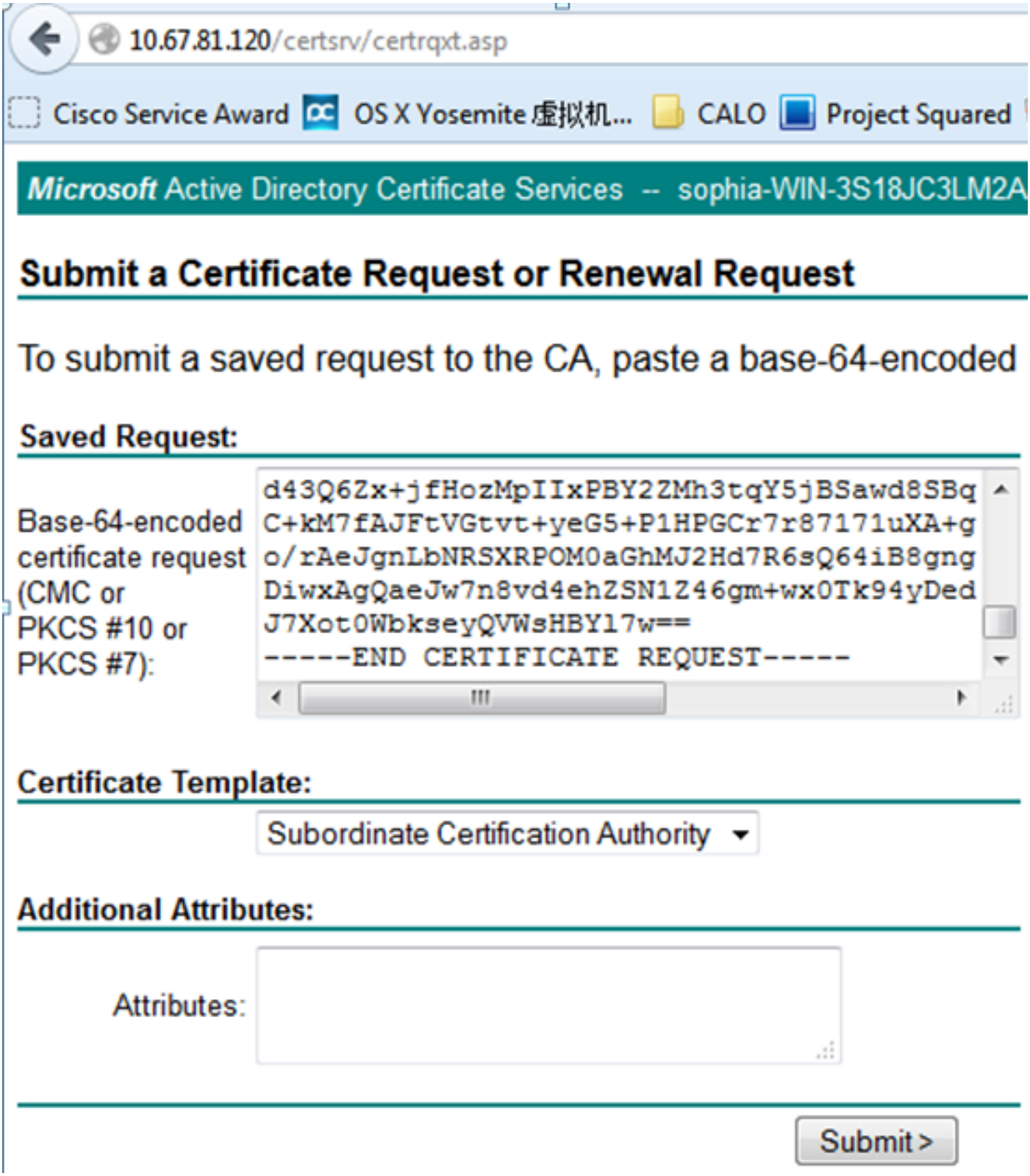
```
admin:utils ctl set-cluster mixed-mode
```

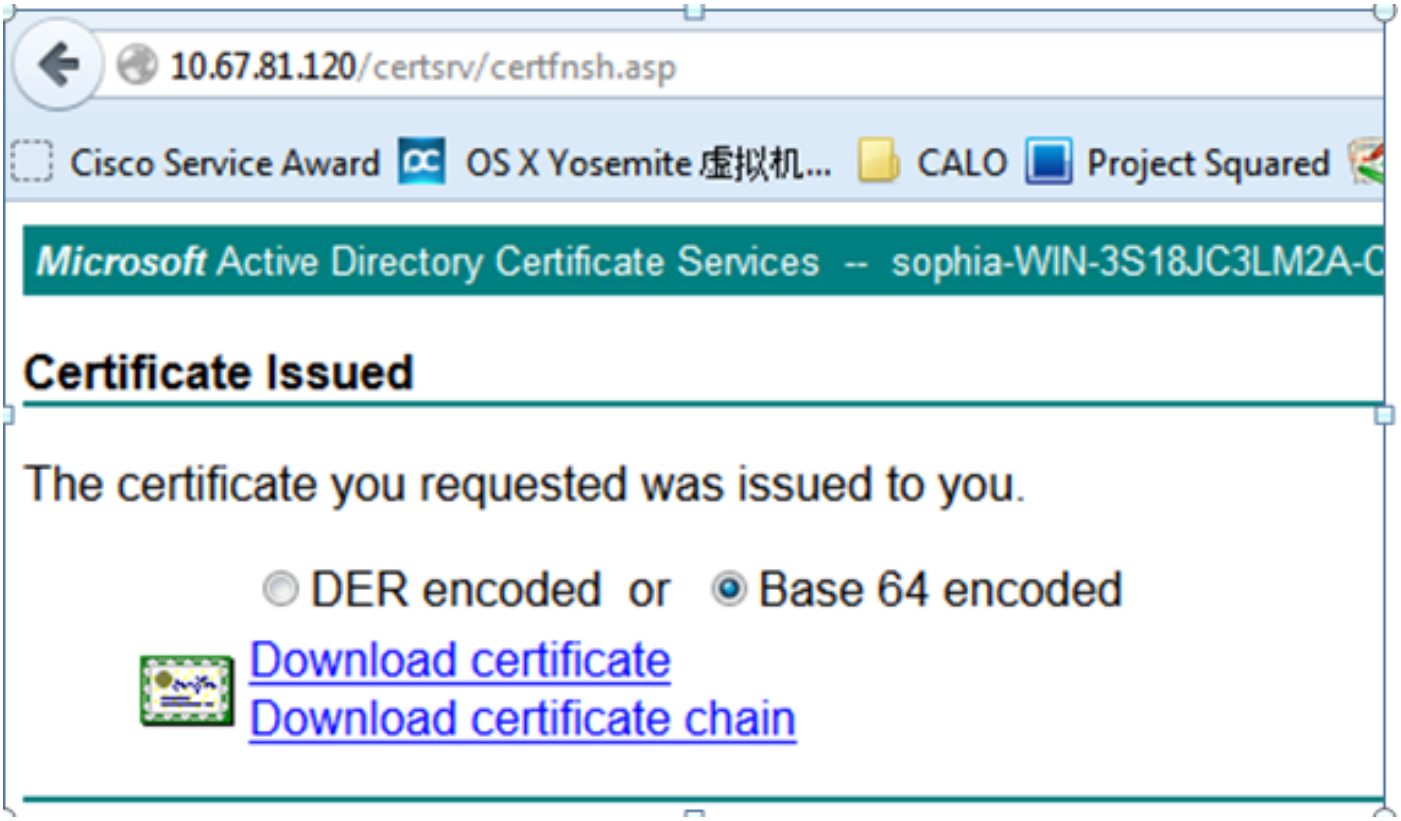
第 2 步： 如图所示，生成 CAPF CSR。



第 3 步： 使用 CA 签署此证书（使用 Windows 2008 CA 中的从属模板）。

注意：您需要使用**从属证书颁发机构**模板才能签署此证书。


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 >

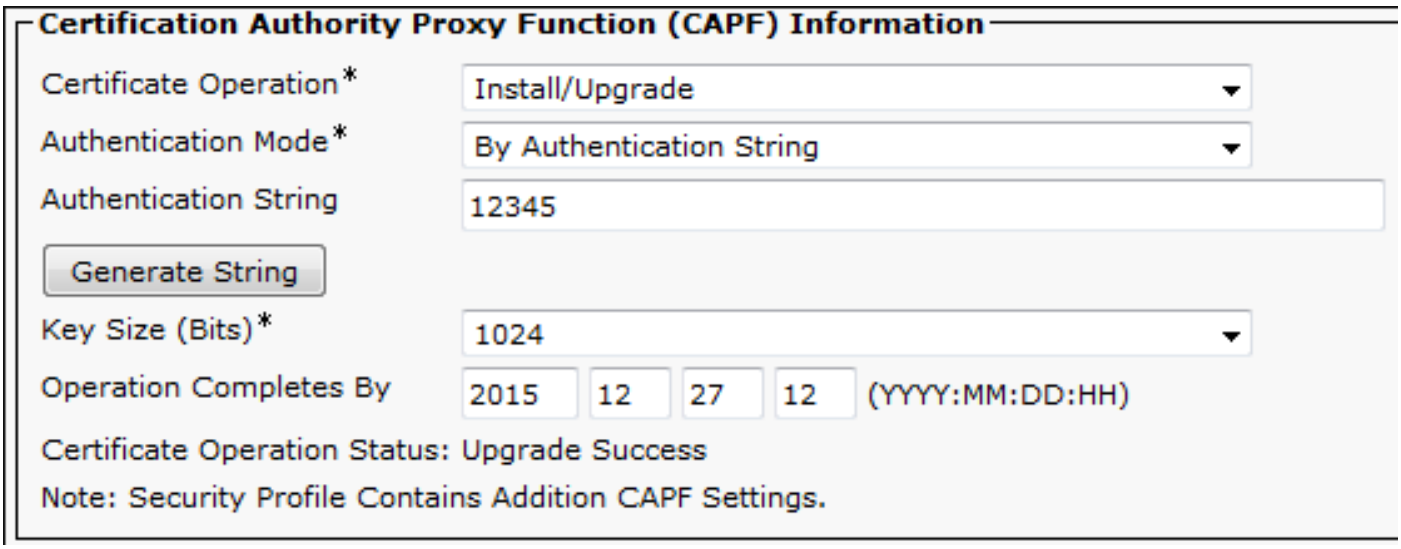


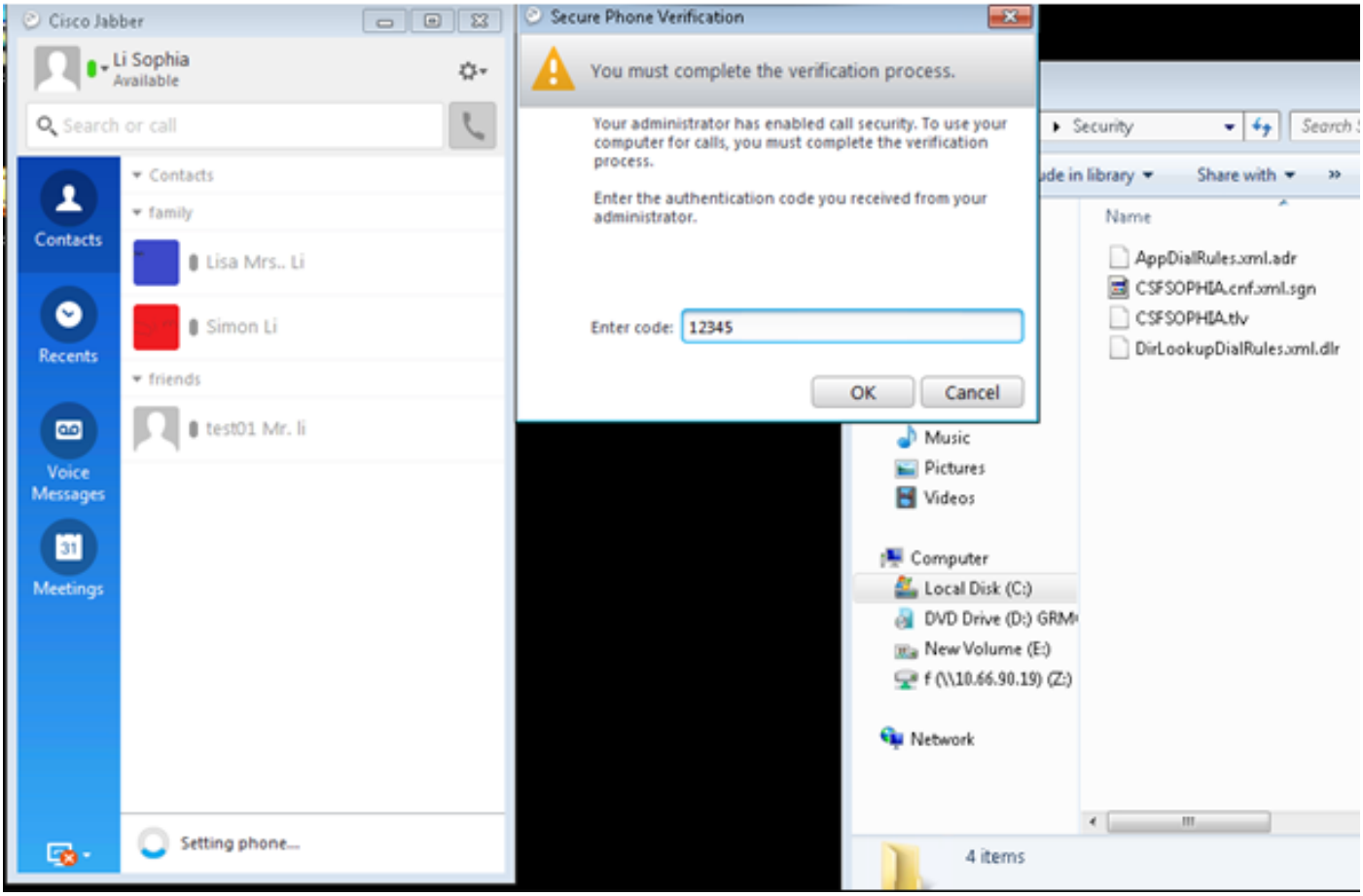
第 4 步： 将根 CA 作为 CAPF-trust 上传，并将服务器证书作为 CAPF 上传。对于此测试，请将此根 CA 作为 CallManager-trust 上传，以在 Jabber 和 CallManager 服务之间建立 TLS 连接，因为已签署的 LSC 也需要通过 CallManager 服务获得信任。正如本文开头部分所述，如果需要统一所有服务器的 CA，则应将该 CA 上传到已进行信号/媒体加密的 CallManager 中。对于部署 IP 电话 802.1x 的场景，无需将 CUCM 设为混合模式，或者将 CAPF 签署为 CallManager-trust 的 CA 上传到 CUCM 服务器中。

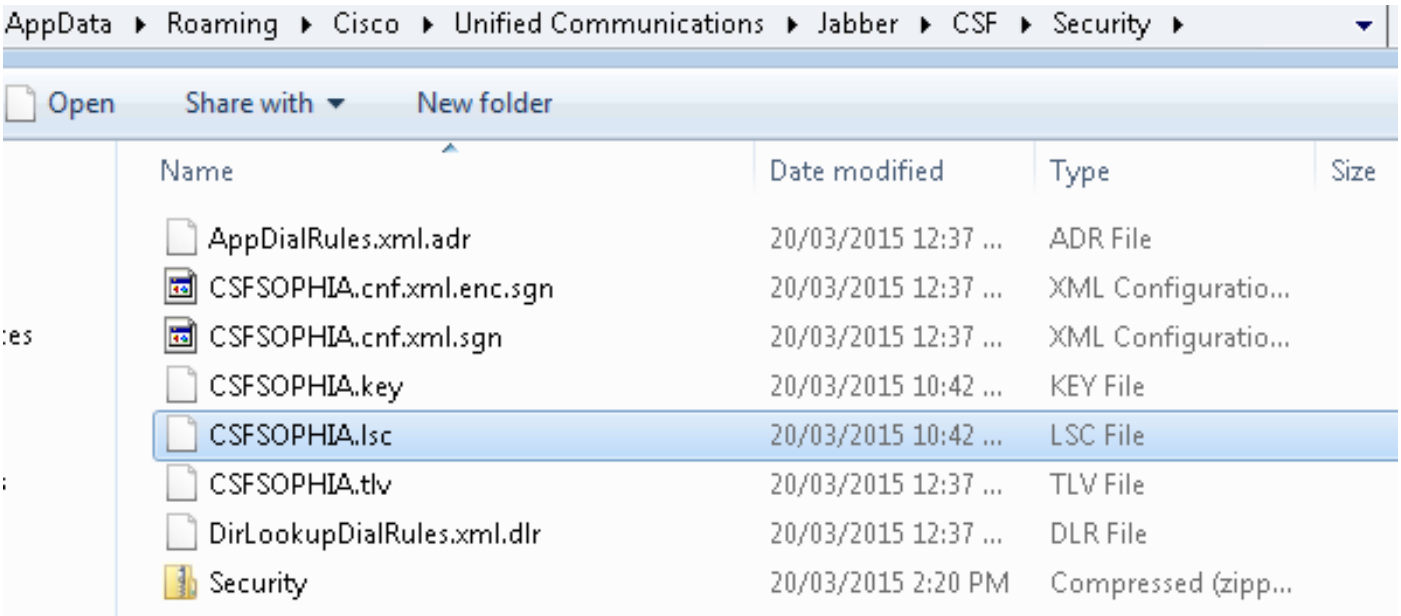
第 5 步： 重新启动 CAPF 服务。

第 6 步： 重新启动所有备注中的 CallManager/TFTP 服务。

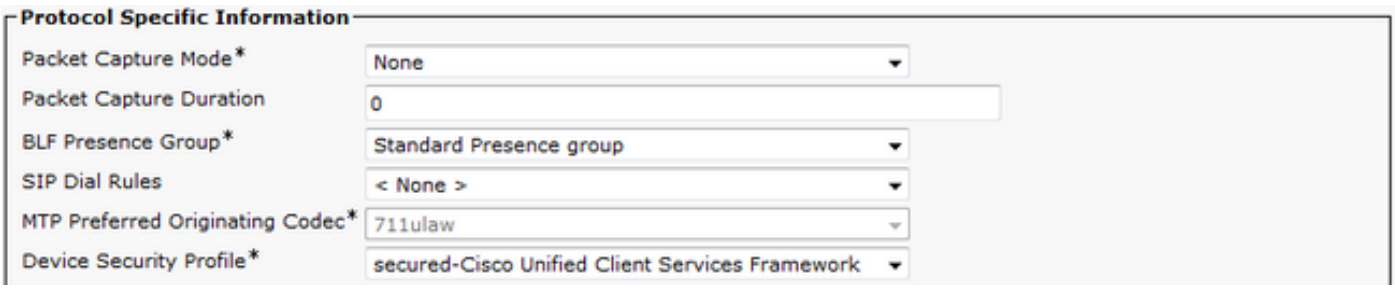
第 7 步： 签署 Jabber 软件电话 LSC。



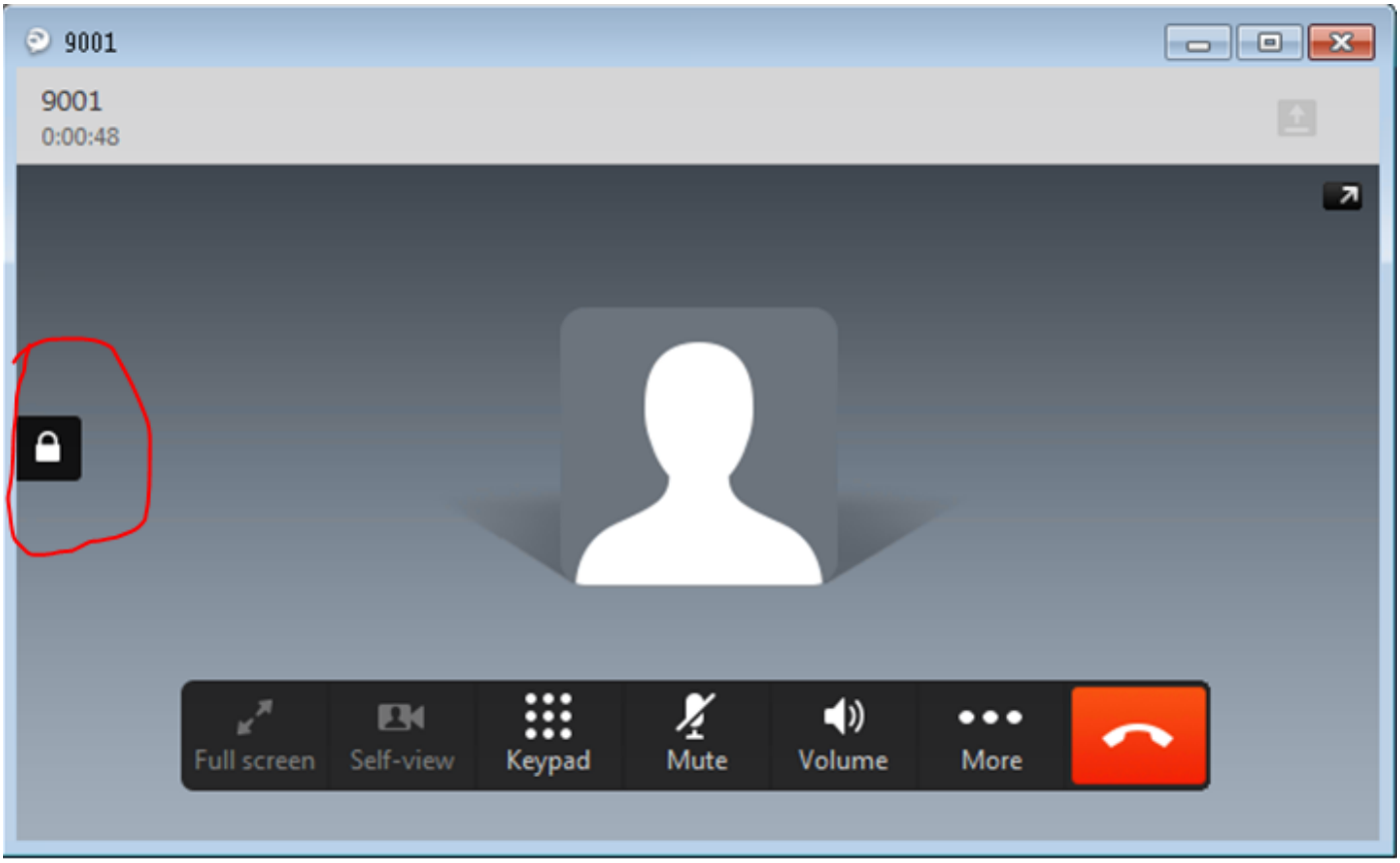




第 8 步： 启用 Jabber 软件电话的安全配置文件。



步骤9.现在安全RTP发生为：

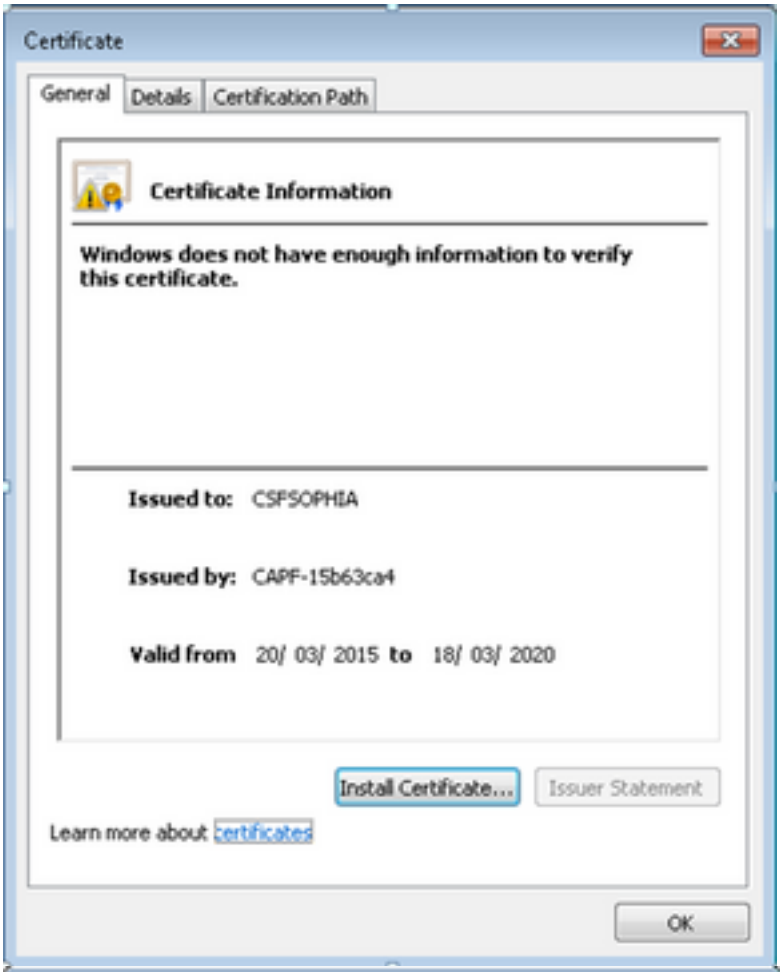


验证

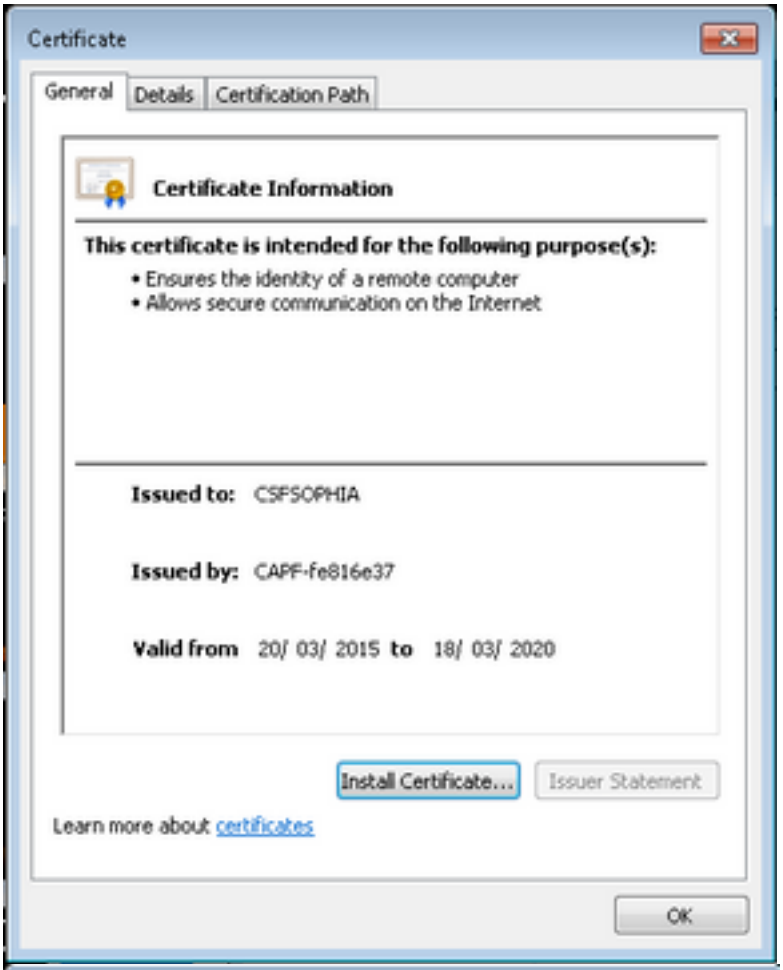
比较使用自签 CAPF 和 CA 签署的 CAPF 时的 LSC：

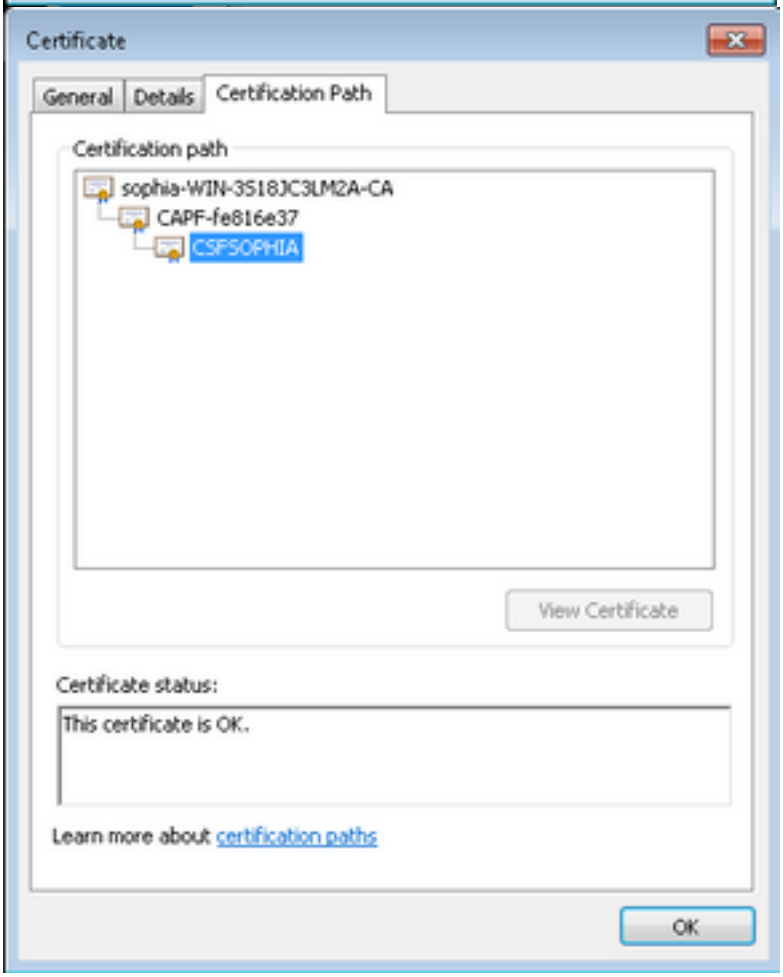
如以下 LSC 图片所示，从 LSC 的角度来看，使用自签 CAPF 时，CAPF 是根 CA，但是使用 CA 签署的 CAPF 时，CAPF 是从属（中间）CA。

使用自签 CAPF 时的 LSC



使用 CA 签署的 CAPF 时的 LSC


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

预警:

本例中显示整个证书链的Jabber客户端LSC与IP电话不同。AS IP电话基于RFC 5280（3.2.认证路径和信任）设计，然后AKI（授权密钥标识符）丢失，CAPF和根CA证书在证书链中不存在。证书链中缺少CAPF/根CA证书将导致ISE在801.x身份验证期间对IP电话进行身份验证时出现一些问题，而不将CAPF和根证书上传到ISE。 CUCM 12.5中有另一个选项，LSC由外部离线CA直接签名，因此CAPF证书无需上传到ISE进行IP电话802.1x身份验证。

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：使用 CA 签署的 CAPF 证书、根证书必须作为 CM-trust 上传：

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