CA為CUCM簽署的CAPF證書

目錄

簡介

本檔案介紹如何取得憑證授權單位代理功能(CAPF)憑證，該憑證授權單位(CA)已簽署用於思科整合通訊管理員(CUCM)。 總是有要求與外部CA簽署CAPF。本文說明為什麼理解其運作方式與設定程式一樣重要。

必要條件

需求

思科建議您瞭解以下主題：

- 公開金鑰基礎架構 (PKI)
- CUCM安全配置

採用元件

本檔案中的資訊是根據Cisco Unified Communications Manager 8.6版及更新版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

限制

不同的CA可能對CSR有不同的要求。有報告顯示，不同版本的OpenSSL CA對CSR有一些特定要求，但是Microsoft Windows CA目前使用思科CAPF提供的CSR的效果很好，本文不討論這些內容。

相關產品

本文件也適用於以下硬體和軟體版本：

- Microsoft Windows Server 2008 CA.
- Windows版Cisco Jabber（不同的版本可能使用不同的名稱來儲存LSC）。

背景資訊

CA簽署CAPF的用途

有些客戶希望與公司的全域性證書策略保持一致，因此有必要與其他伺服器使用相同的CA簽署CAPF。

此PKI的機制

預設情況下，本地有效憑證(LSC)由CAPF簽署，因此CAPF是此案例中電話的CA。但是，當您嘗試讓外部CA簽署CAPF時，此案例中的CAPF會充當從屬CA或中間CA。

自簽名CAPF與CA簽名CAPF的區別在於：當執行自簽名CAPF時，CAPF是LSC的根CA，當執行CA簽名CAPF時，CAPF是從（中間）CA到LSC。

CAPF CSR與其他CSR有何不同？

關於RFC5280，金鑰使用擴展定義了證書中包含的金鑰的用途（例如，加密、簽名、證書簽名）。CAPF是一個證書代理和CA，它可以簽署到電話的證書，但其他證書（如CallManager、Tomcat、IPSec）充當枝葉（使用者身份）。 當您檢視他們的CSR時，您可以看到CAPF CSR具有**Certificate Sign**角色，但看不到其他角色。

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:

屬性：請求的擴展：X509v3擴展金鑰用法：TLS Web伺服器驗證、TLS Web客戶端驗證、IPSec終端系統X509v3金鑰用法：數位簽章、金鑰加密、資料加密、金鑰協定

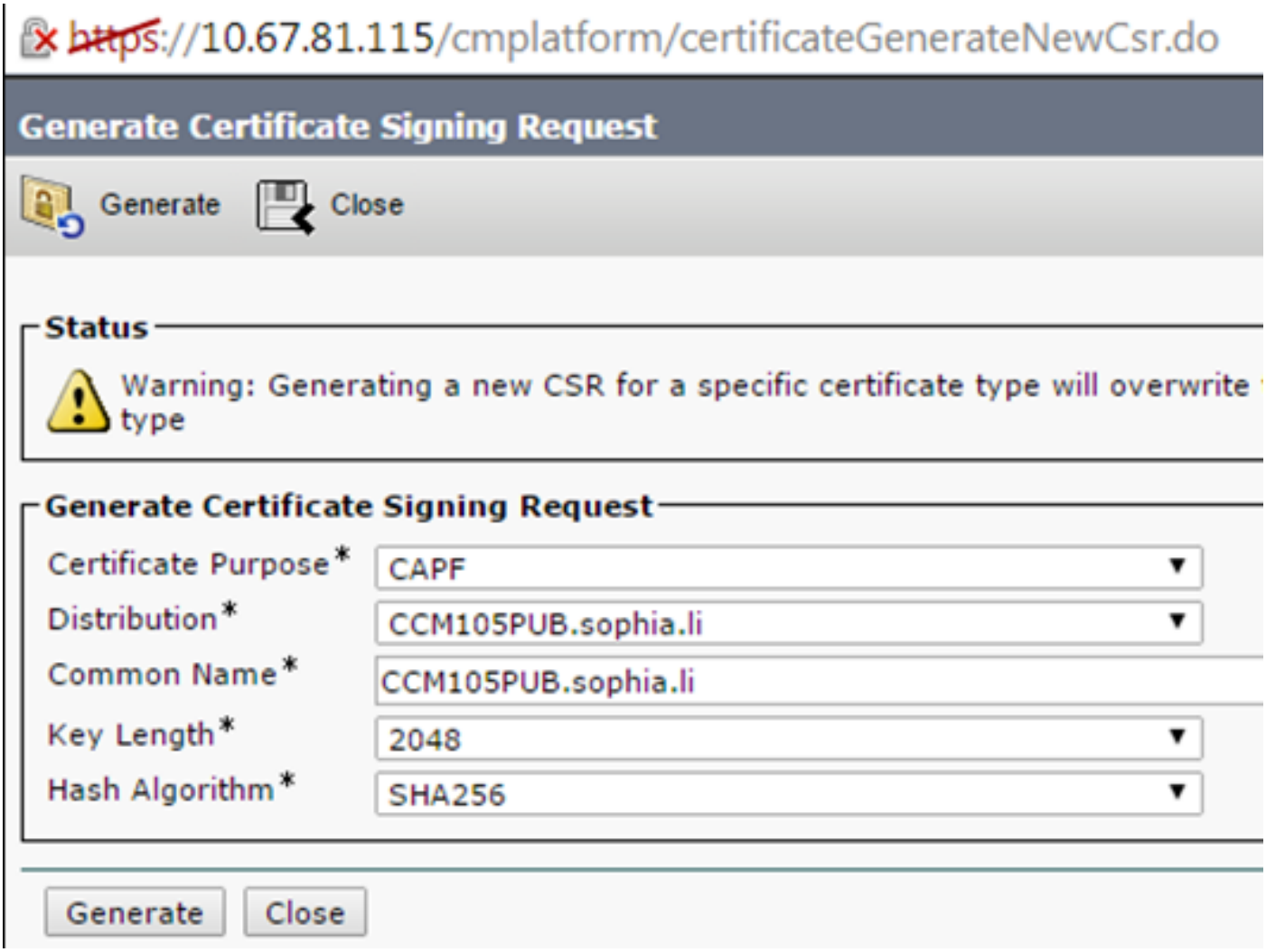
設定

以下是一個情況，外部根CA用於簽署CAPF證書：用於加密Jabber客戶端和IP電話的訊號/媒體。

步驟1.將CUCM群集設定為安全群集。

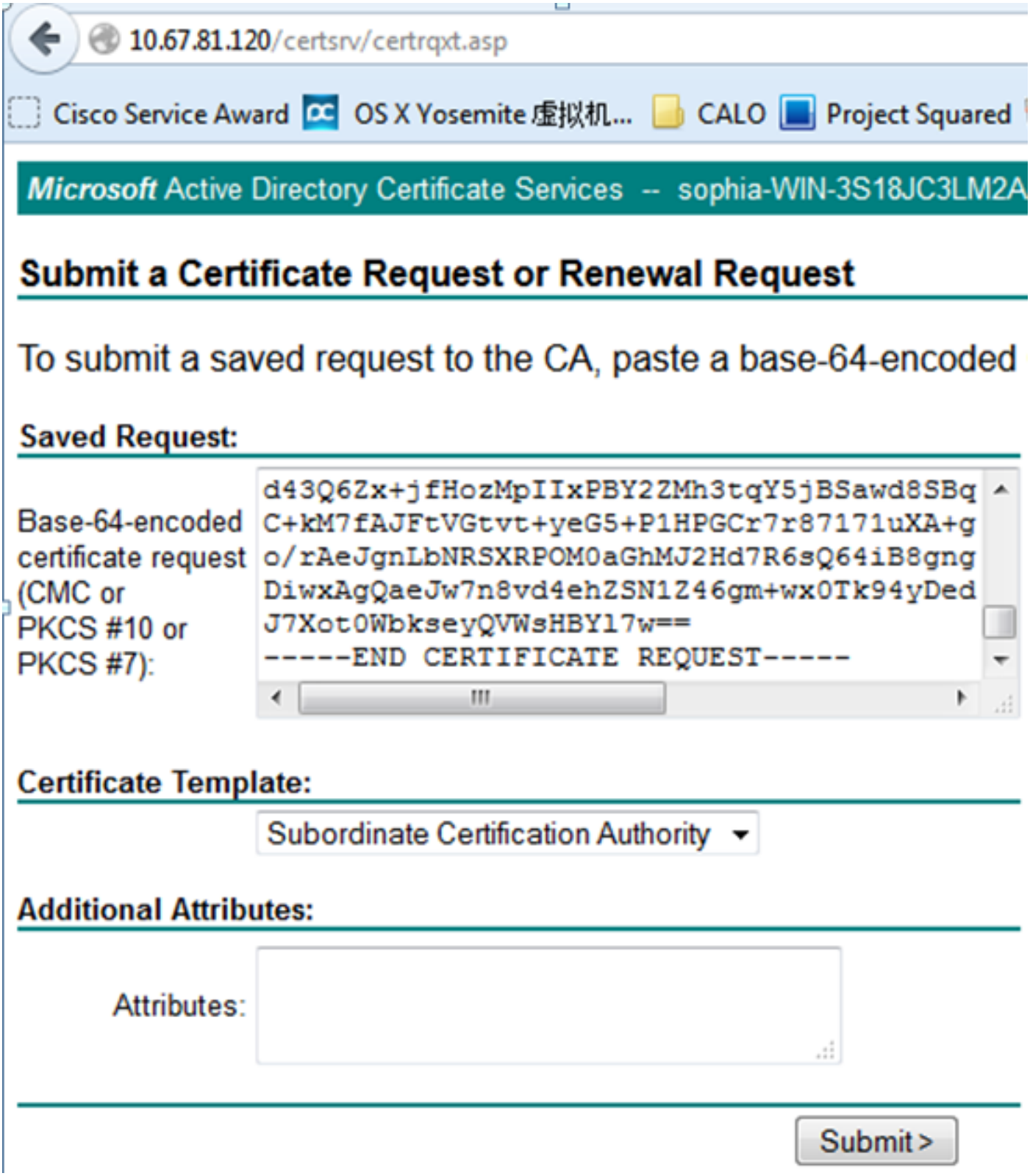
```
admin:utils ctl set-cluster mixed-mode
```

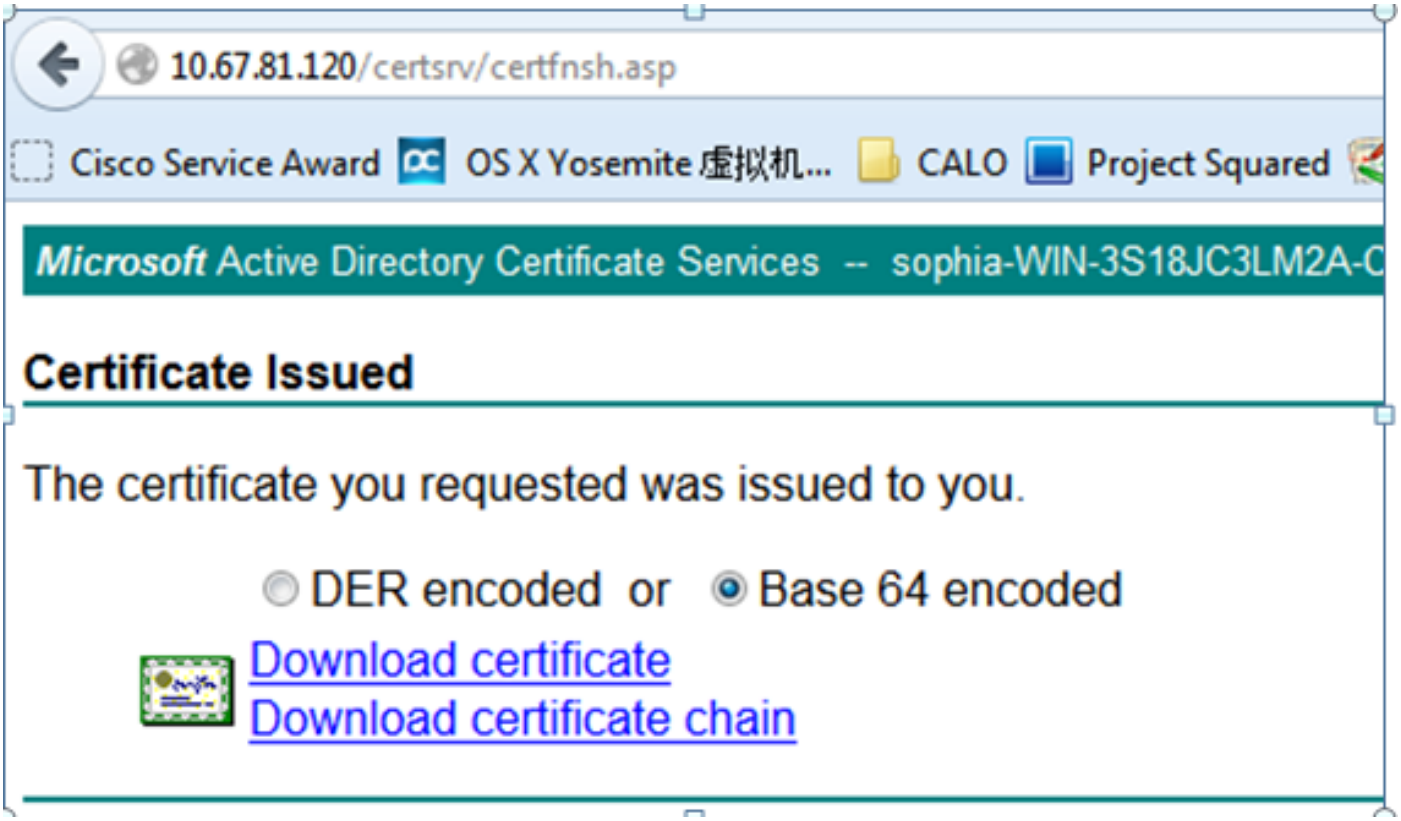
步驟2.如圖所示，產生CAPF CSR。



步驟3.與CA簽署此檔案（在Windows 2008 CA中使用從屬模板）。

附註：您需要使用**下屬證書頒發機構**模板來簽署此證書。


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 >

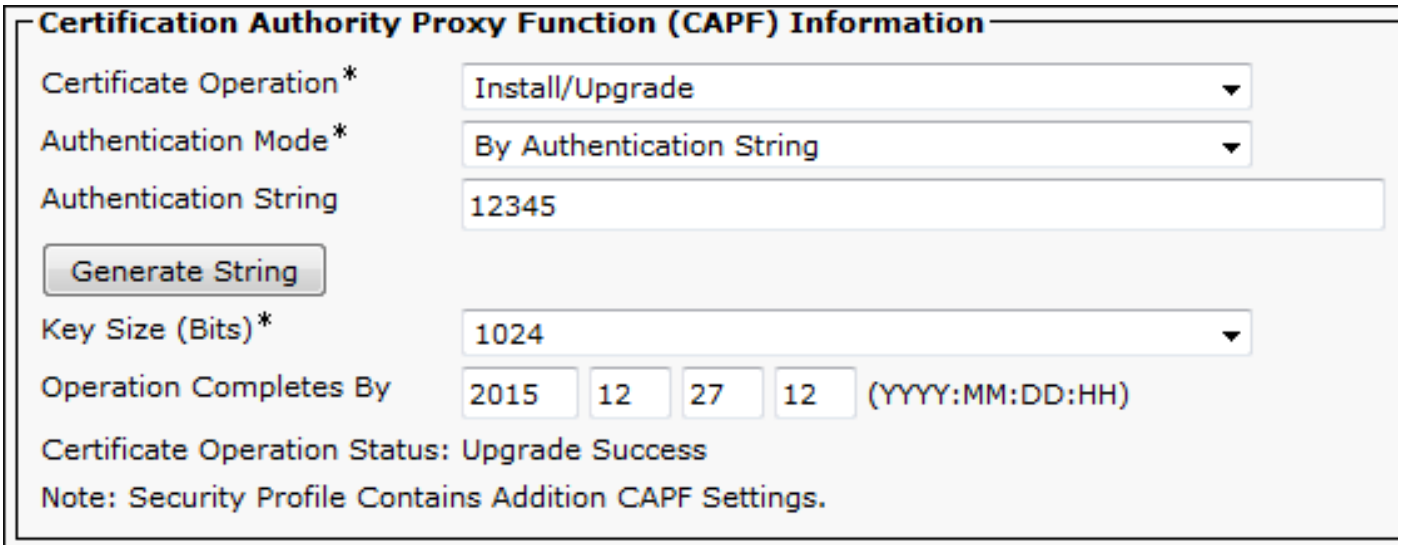


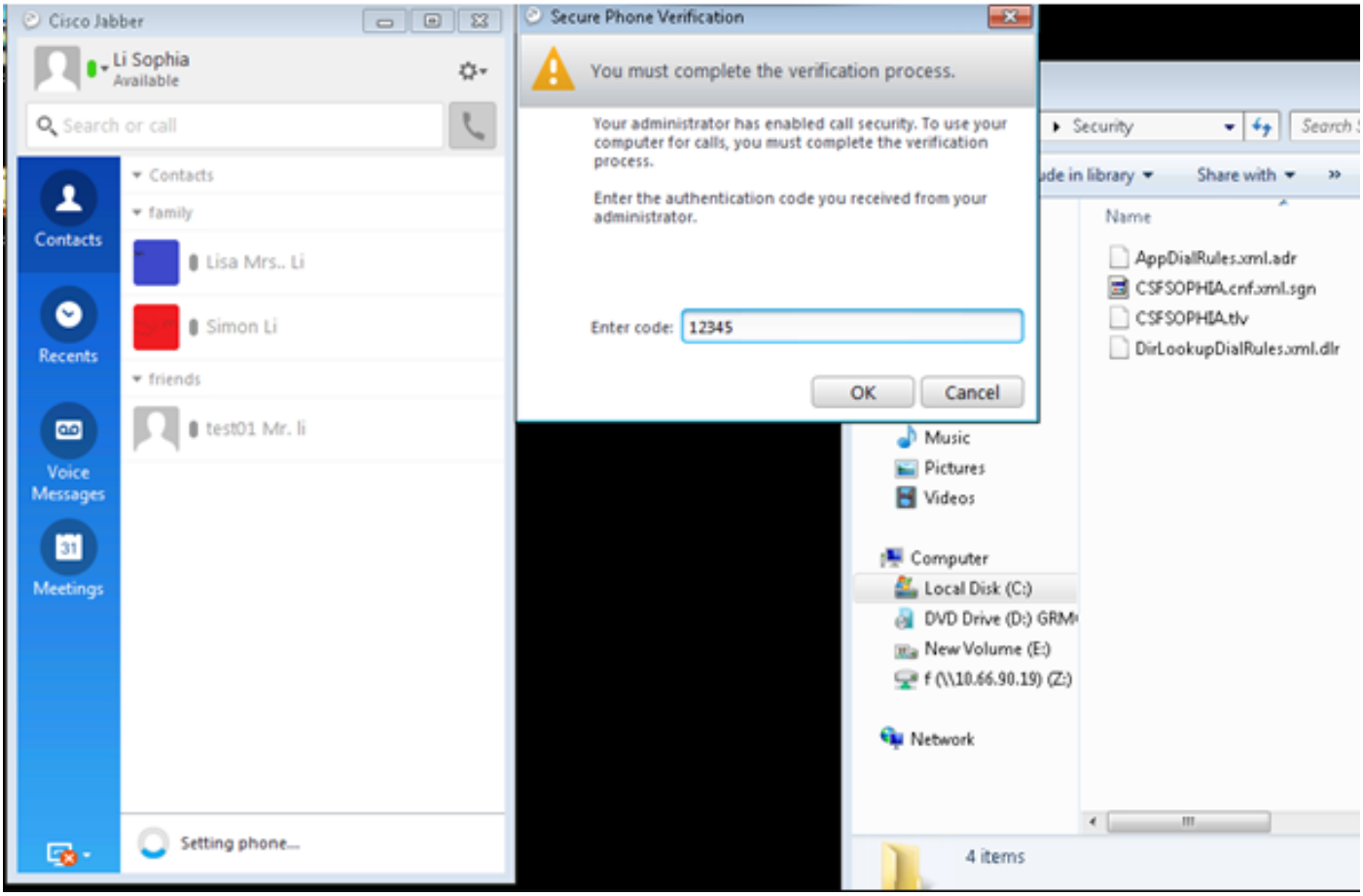
步驟4.將根CA上傳為CAPF-trust，將伺服器證書上傳為CAPF。對於此測試，也請將此根CA上傳為CallManager-trust，以便在Jabber和CallManager服務之間建立TLS連線，因為已簽名的LSC也需要CallManager服務信任。如本文開頭所述，需要調整所有伺服器的CA，以便此CA已經上傳到CallManager進行訊號/媒體加密。對於部署IP電話802.1x的情況，您不必將CUCM設定為混合模式或將CAPF作為CallManager-trust登入的CA上傳到CUCM伺服器。

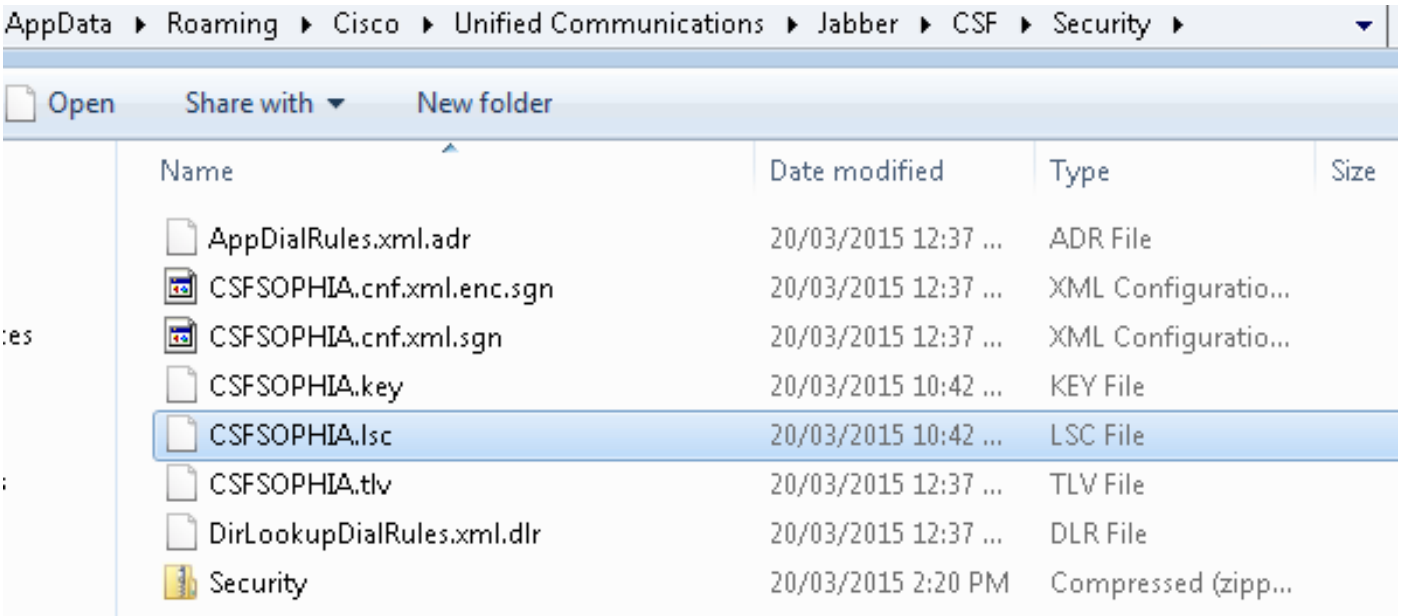
步驟5.重新啟動CAPF服務。

步驟6.在所有說明中重新啟動CallManager/TFTP服務。

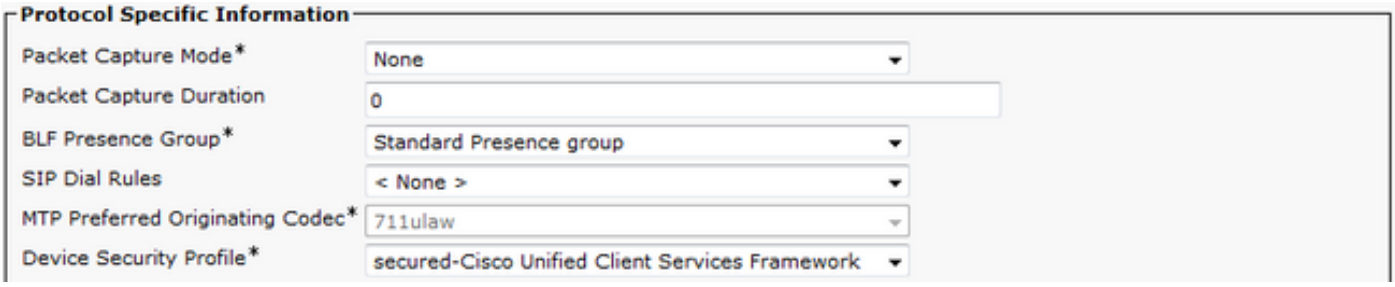
步驟7.簽署Jabber軟體電話LSC。



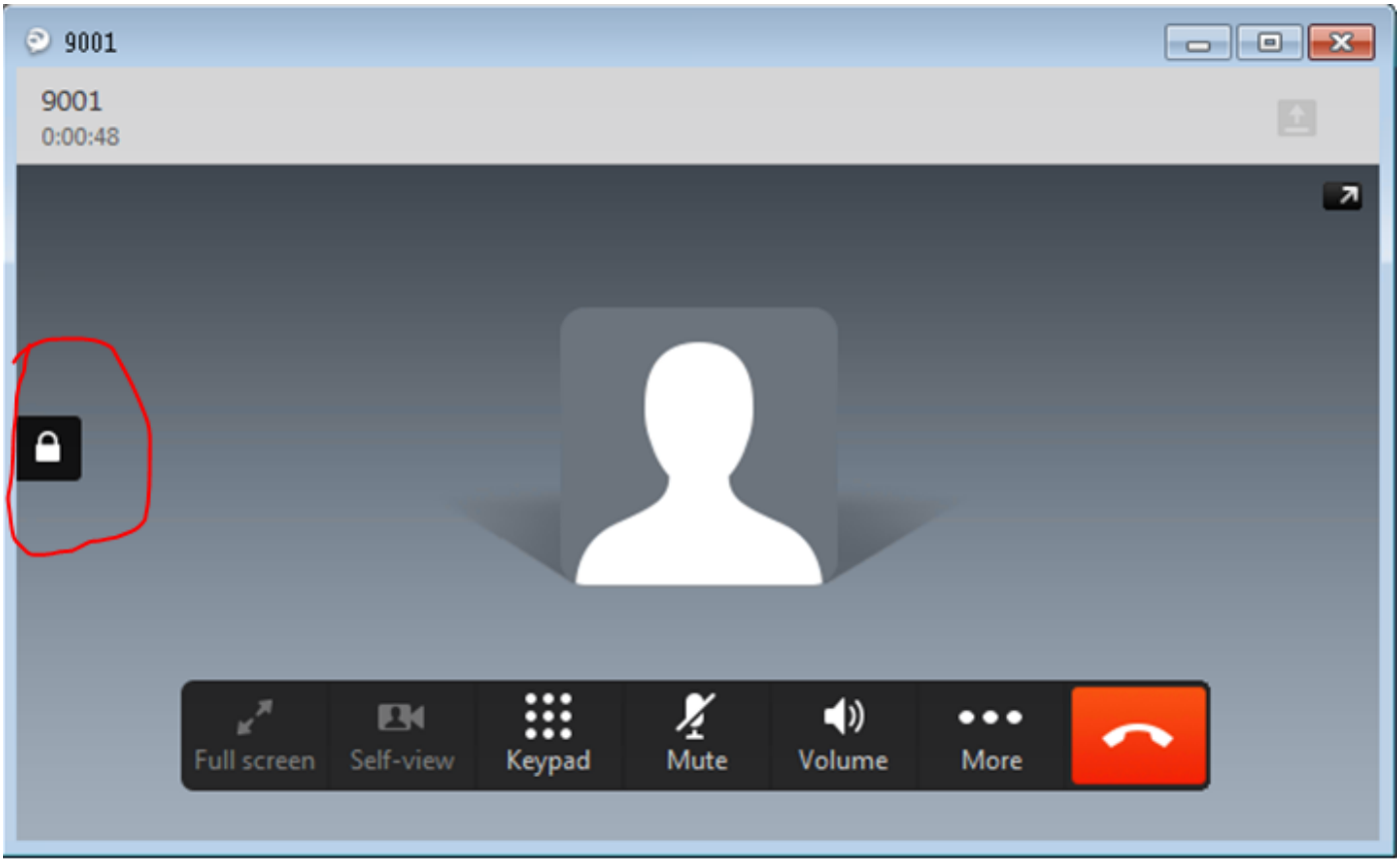




步驟8.啟用Jabber軟體電話的安全配置檔案。



步驟9.現在安全的RTP如下：

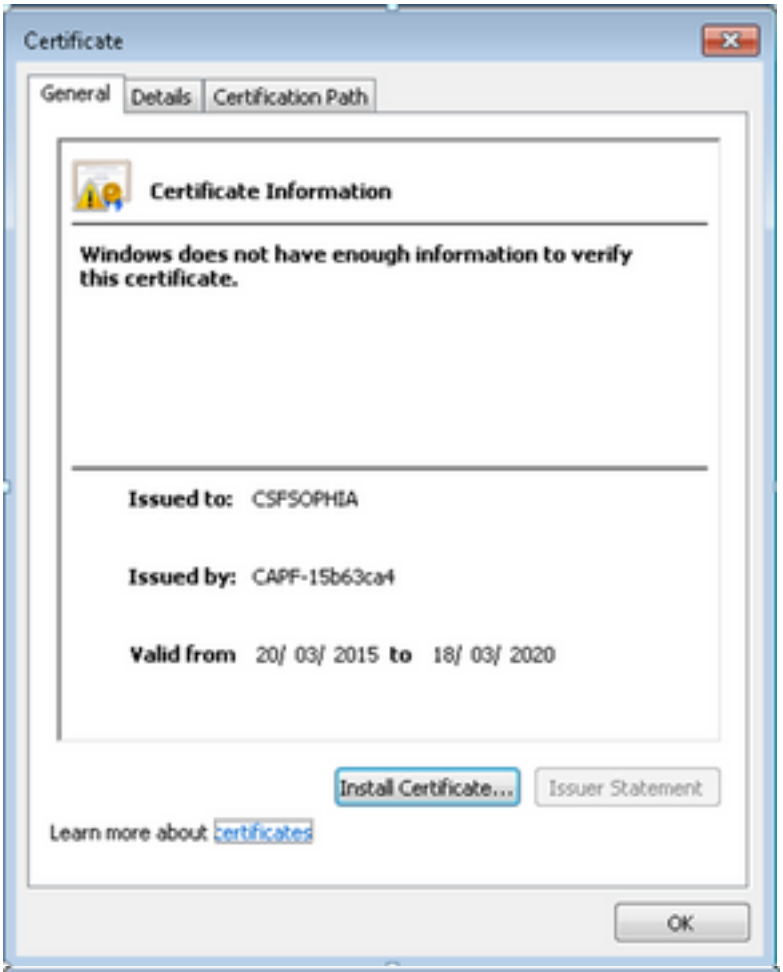


驗證

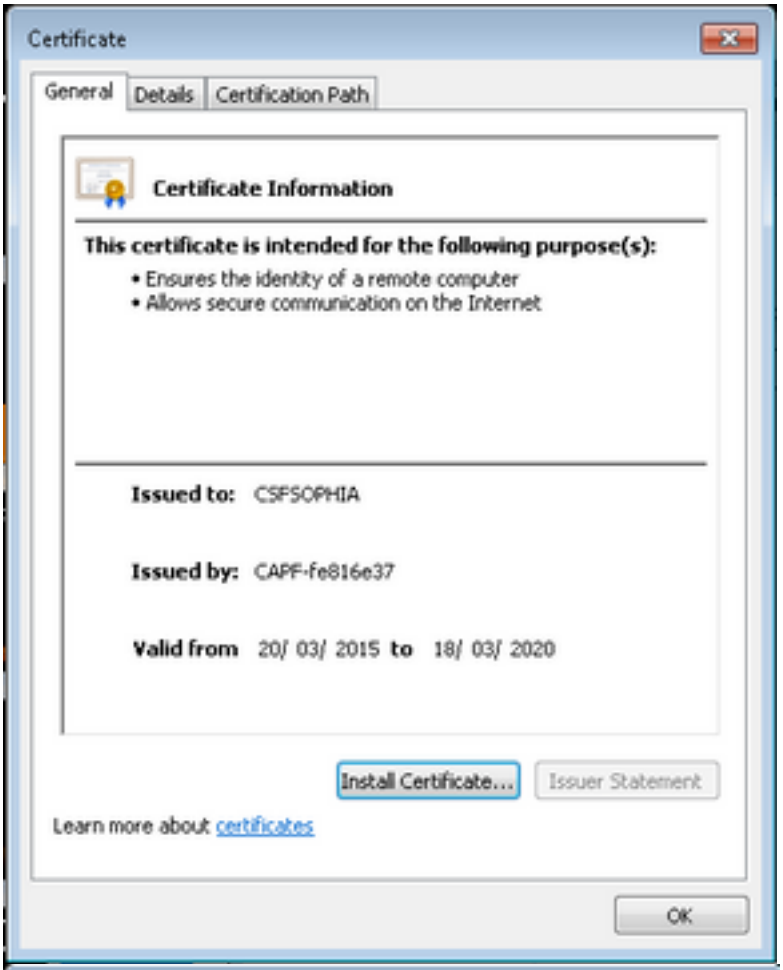
比較自簽名CAPF和CA簽名CAPF時的LSC:

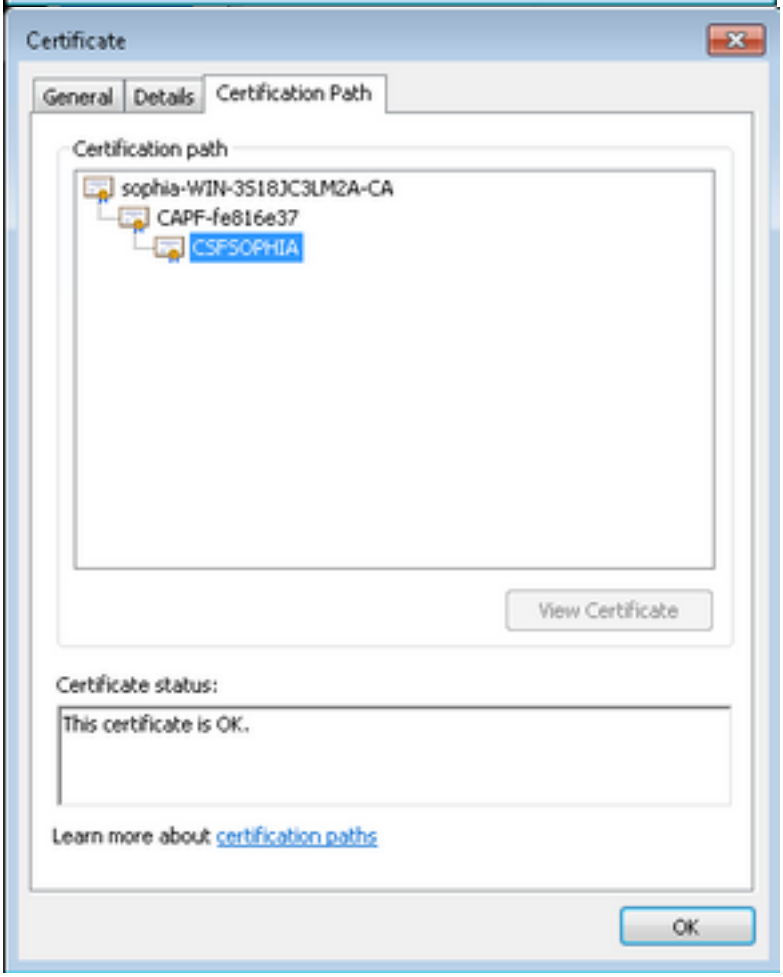
從這些LSC影象中可以看到，從LSC的角度來看，使用自簽名CAPF時，CAPF是根CA，而使用CA簽名的CAPF時，CAPF是下級（中間）CA。

自簽名CAPF時的LSC



CA簽署CAPF時的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

警報：

本示例中顯示整個證書鏈的Jabber客戶端LSC與IP電話不同。AS IP電話是基於RFC 5280（3.2.憑證路徑和信任）而設計的，因此缺少AKI（授權金鑰識別碼），則CAPF和根CA憑證不會出現在憑證鏈結中。證書鏈中缺少CAPF/根CA證書將導致ISE在801.x身份驗證期間對IP電話進行身份驗證，而不將CAPF和根證書上傳到ISE。 CUCM 12.5中有另一個選項，LSC直接由外部離線CA簽署，因此不需要將CAPF證書上傳到ISE進行IP電話802.1x身份驗證。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

已知缺陷：CA簽名的CAPF證書，根證書必須作為CM-trust上傳：

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