CUCM第三方CA簽名LSC生成和匯入配置示例

目錄

簡介

憑證授權代理功能(CAPF)本地有效憑證(LSC)是本地簽署的。但是，您可能要求電話使用第三方證書頒發機構(CA)簽名的LSC。本文描述了幫助您實現此目標的過程。

必要條件

需求

思科建議您瞭解Cisco Unified Communication Manager(CUCM)。

採用元件

本檔案中的資訊是根據CUCM版本10.5(2);但是此功能在10.0版及更新版本中有效。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

以下是此程式涉及的步驟，每個步驟在各自的章節中詳述：

1. 上傳CA根證書
2. 將證書頒發的離線CA設定為端點
3. 為電話生成證書簽名請求(CSR)
4. 將產生的CSR從Cisco Unified Communications Manager(CUCM)獲取到FTP伺服器
5. 從CA獲取電話證書
6. 將.cer轉換為.der格式
7. 將證書(.der)壓縮為.tgz格式
8. 將.tgz檔案傳輸到Secure Shell FTP(SFTP)伺服器
9. 將.tgz檔案匯入CUCM伺服器
10. 使用Microsoft Windows 2003證書頒發機構簽署CSR
11. 從CA取得根憑證

上傳CA根證書

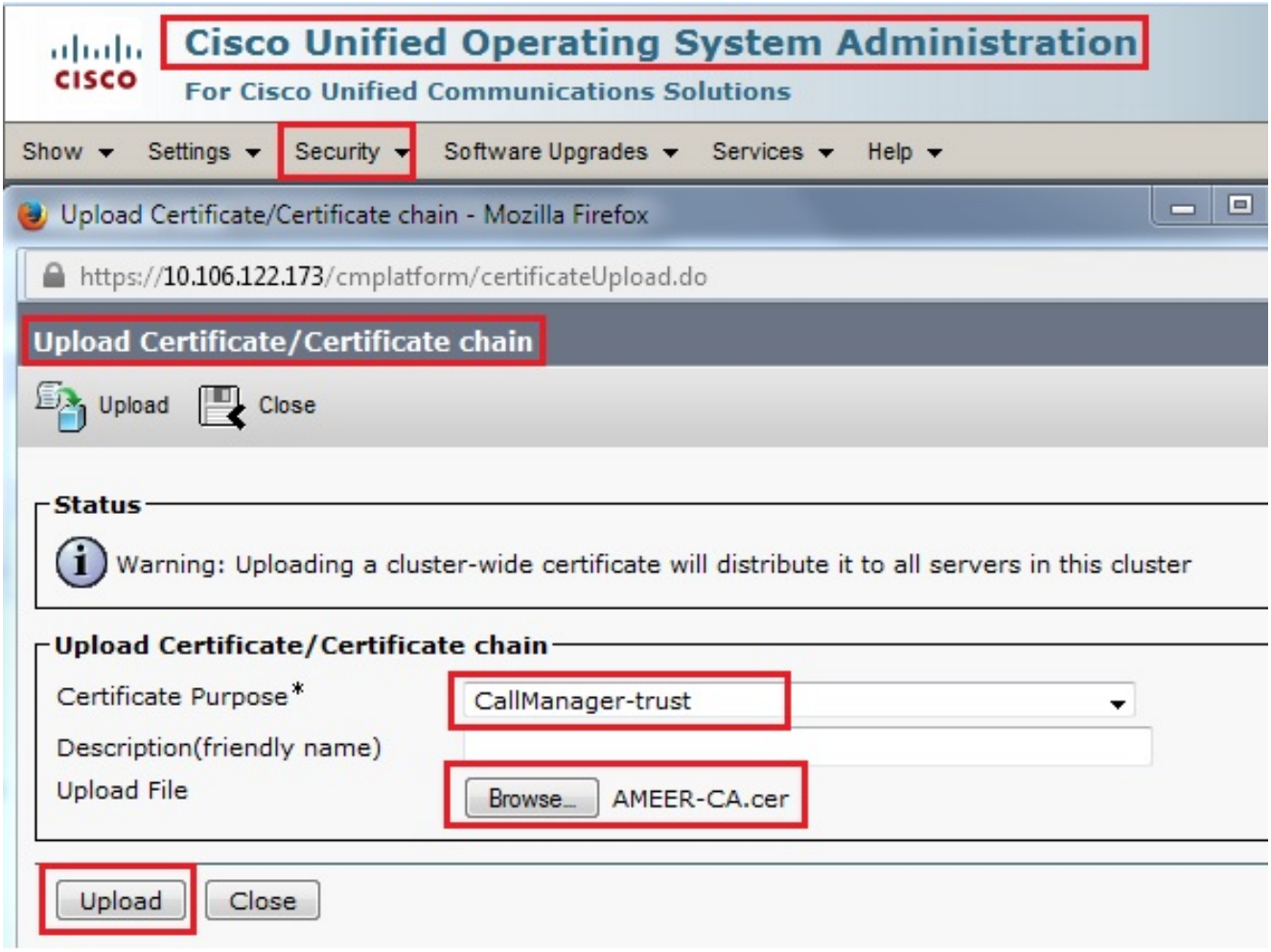
1. 登入到思科統一作業系統(OS)管理Web GUI。

2. 導覽至**Security Certificate Management**。

3. 按一下「**Upload Certificate/Certificate chain**」。

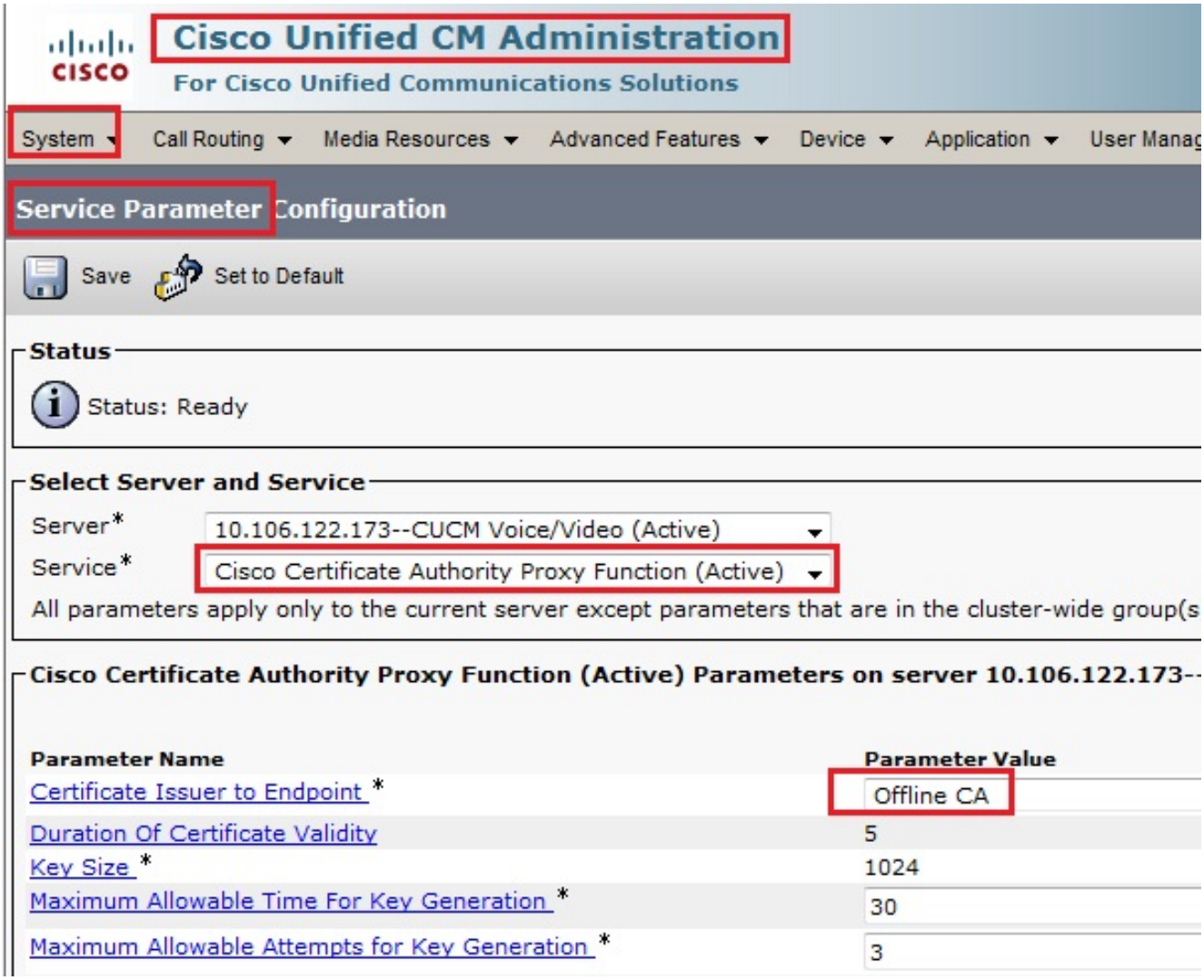
4. 在Certificate Purpose下選擇**CallManager-trust**。

5. 瀏覽到CA的根憑證，然後按一下**Upload**。



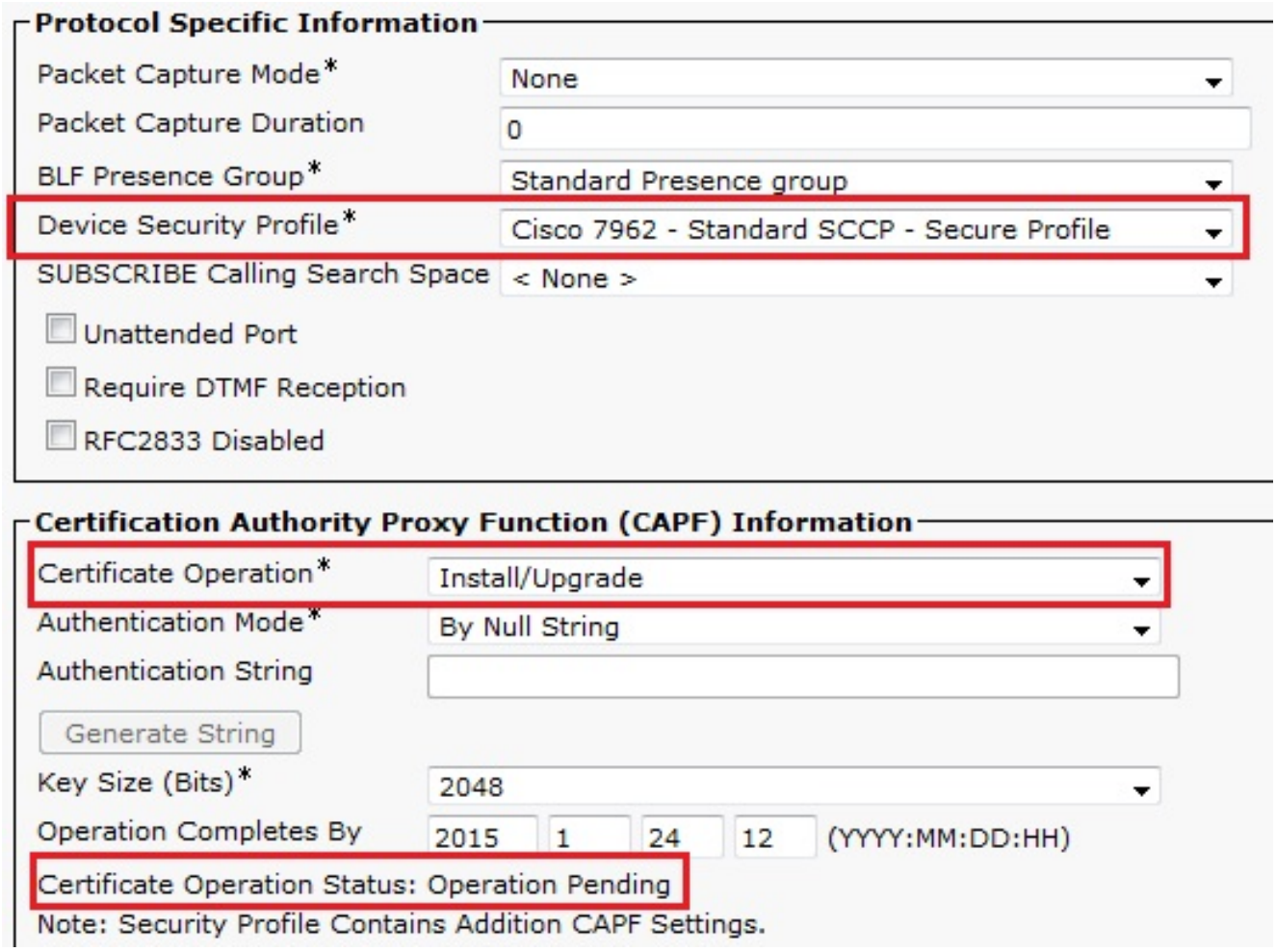
將證書頒發的離線CA設定為端點

1. 登入到CUCM管理Web GUI。
2. 導覽至**System > Service Parameter**。
3. 選擇CUCM Server並為服務選擇**Cisco Certificate Authority Proxy Function**。
4. 選擇**離線CA**以向終端頒發證書。

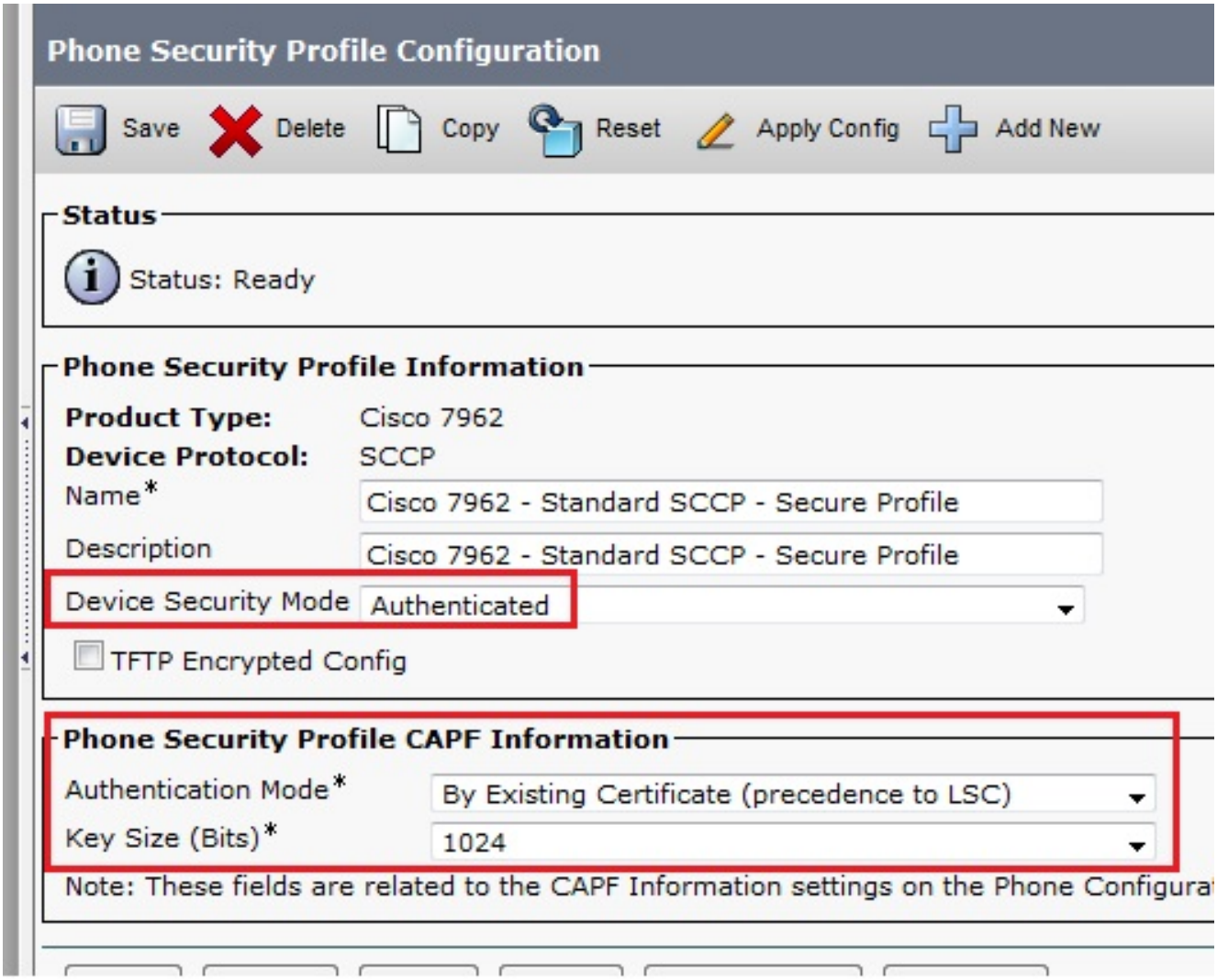


為電話生成證書簽名請求(CSR)

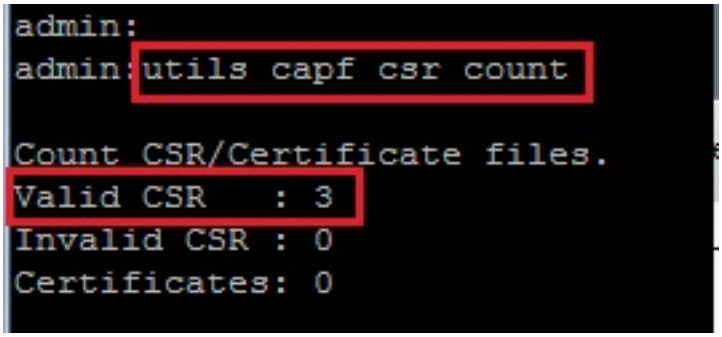
1. 登入到CUCM管理Web GUI。
2. 導航到**Device Phones**。
3. 選擇其LSC必須由外部CA簽署的電話。
4. 將裝置安全配置檔案更改為安全配置檔案（如果不存在，請在安全電話安全配置檔案上新增一個系統）。
5. 在電話配置頁面的CAPF部分下，為認證操作選擇**安裝/升級**。對其LSC必須由外部CA簽名的所有電話完成此步驟。對於證書操作狀態，您應該會看到**Operation Pending**。



電話安全配置檔案（7962型號）。



在安全殼層(SSH)作業階段中輸入**utils capf csr count**指令，確認是否已產生CSR。（此螢幕截圖顯示已為三部電話產生CSR。）



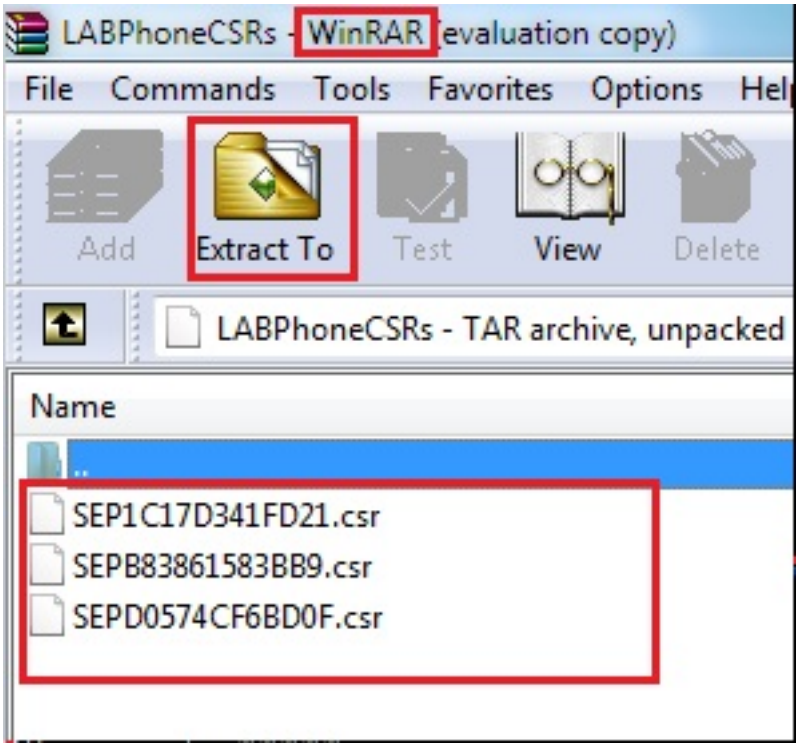
附註：電話的CAPF部分下的證書操作狀態保持為**操作掛**起。

將產生的CSR從CUCM獲取到FTP（或TFTP）伺服器

1. 通過SSH連線到CUCM伺服器。
2. 執行**utils capf csr dump**命令。此螢幕抓圖顯示轉儲正在傳輸到FTP。

```
admin:
admin:utils capf csr dump

Dump CSR files.
CSR File tarred successfully...

Destination:

 1) Remote Filesystem via FTP
 2) Remote Filesystem via TFTP
 3) Local Download Directory
 q) quit

Please select an option (1 - 3 or "q" ): 1
File Path: LABPhoneCSRs
Server: 10.65.43.173
User Name: cisco
Password: *****
File exported successfully
```

3. 使用WinRAR開啟轉儲檔案並將CSR提取到本地電腦。



獲取電話證書

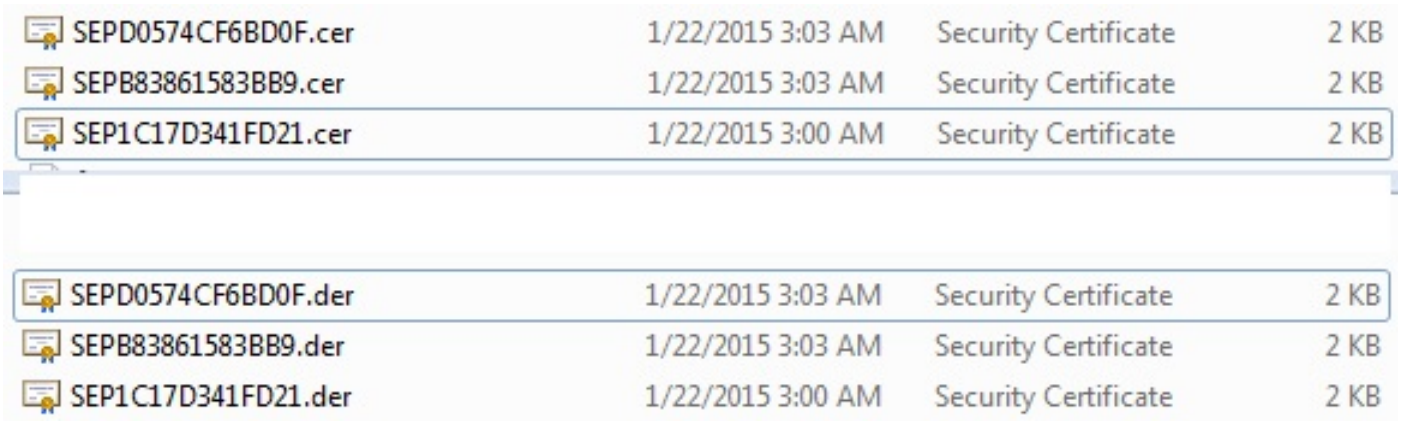
1. 將電話的CSR傳送到CA。

2. CA會提供已簽名的憑證。

附註：您可以使用Microsoft Windows 2003 Server作為CA。稍後將說明使用Microsoft Windows 2003 CA簽署CSR的程式。

將.cer轉換為.der格式

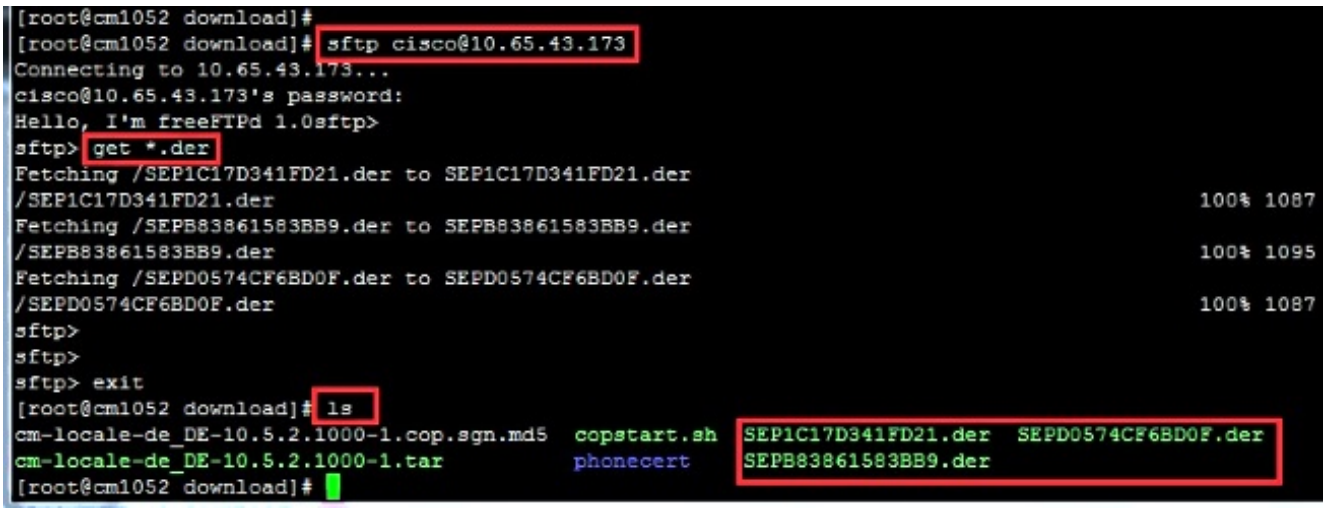
如果收到的證書是.cer格式，則將其重新命名為.der。



將證書(.der)壓縮為.tgz格式

您可以使用CUCM伺服器的根(Linux)來壓縮證書格式。也可以在正常的Linux系統中執行此操作。

1. 使用SFTP伺服器將所有已簽名的證書傳輸到Linux系統。

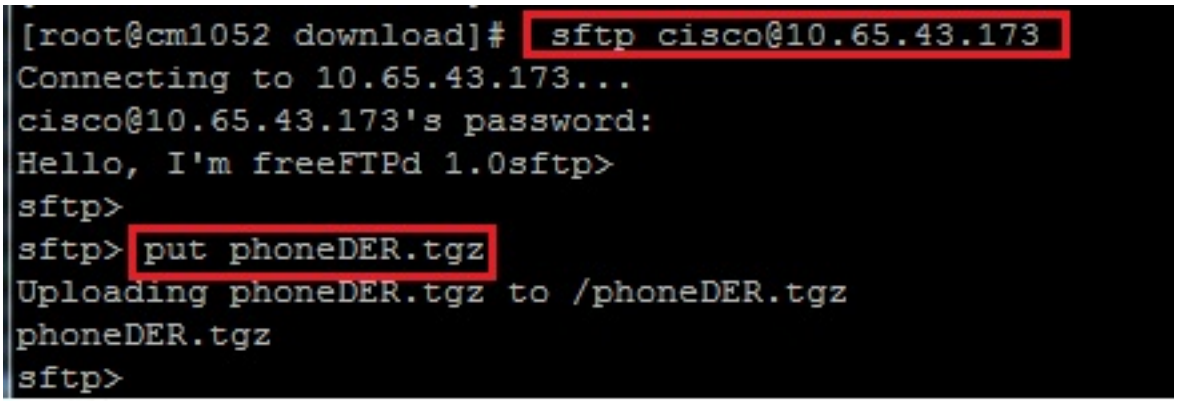


2. 輸入以下命令可將所有.der憑證壓縮到.tgz檔案中。

```
tar -zcvf
```

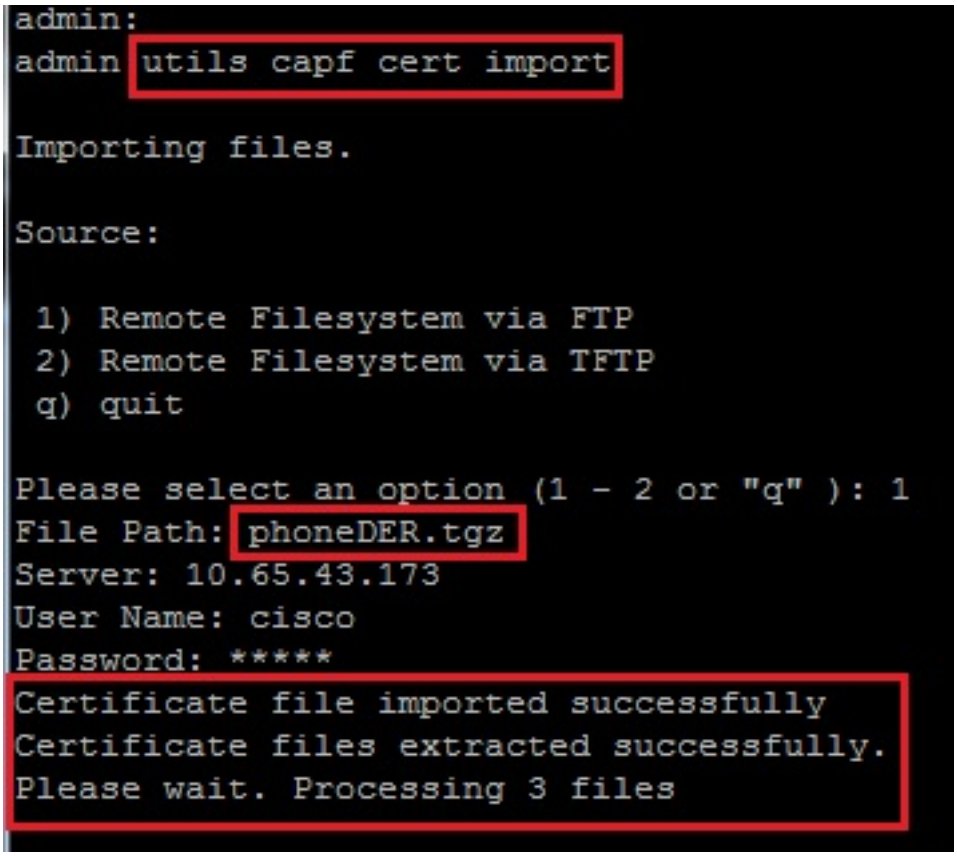
將.tgz檔案傳輸到SFTP伺服器

完成螢幕抓圖中所示的步驟，以便將.tgz檔案傳輸到SFTP伺服器。



將.tgz檔案匯入CUCM伺服器

1. 通過SSH連線到CUCM伺服器。
2. 執行**utils capf cert import**命令。



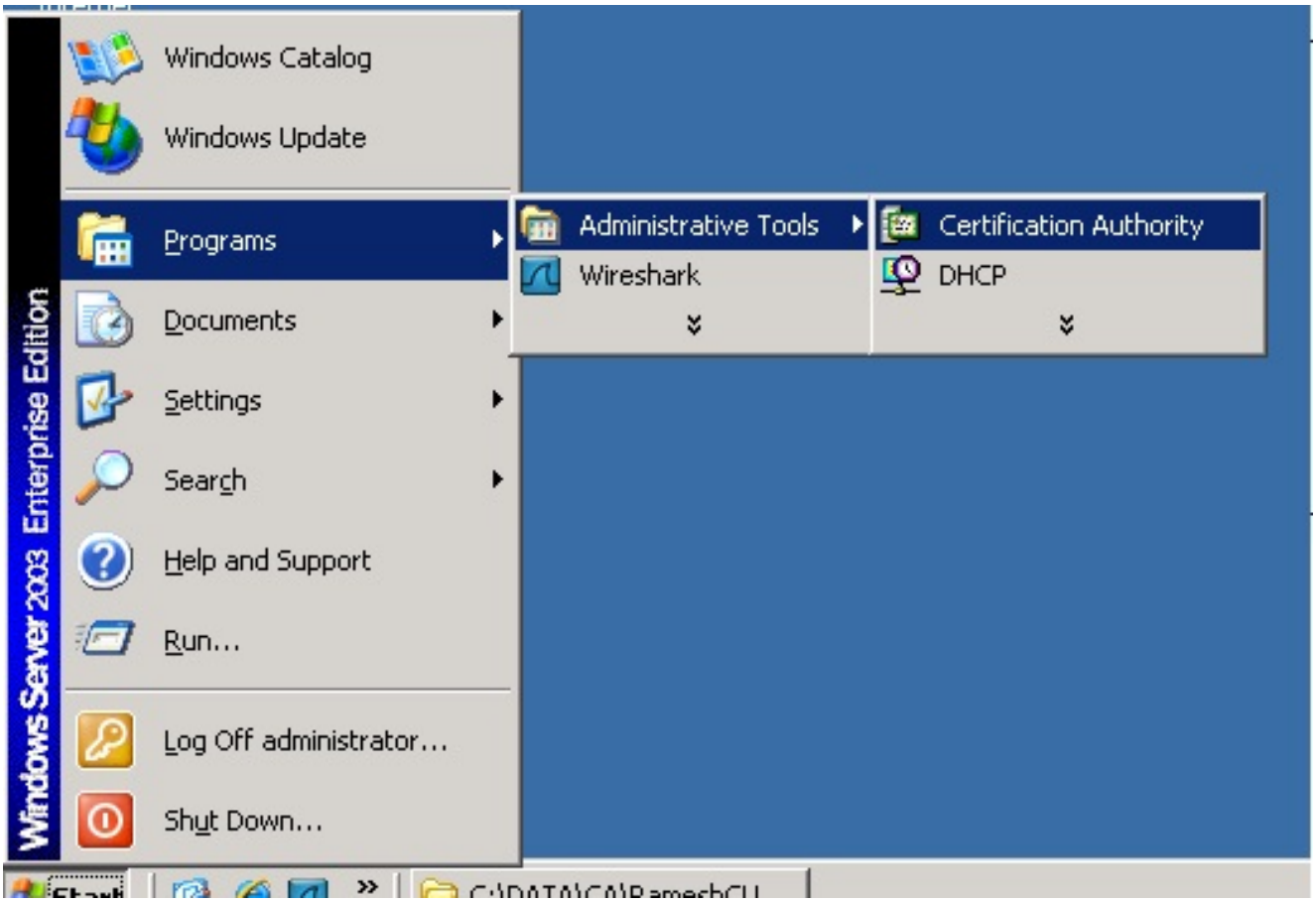
成功匯入證書後，您可以看到CSR計數變為零。

```
admin:
admin:utils capf csr count

Count CSR/Certificate files.
Valid CSR    : 0
Invalid CSR : 0
Certificates: 0
```

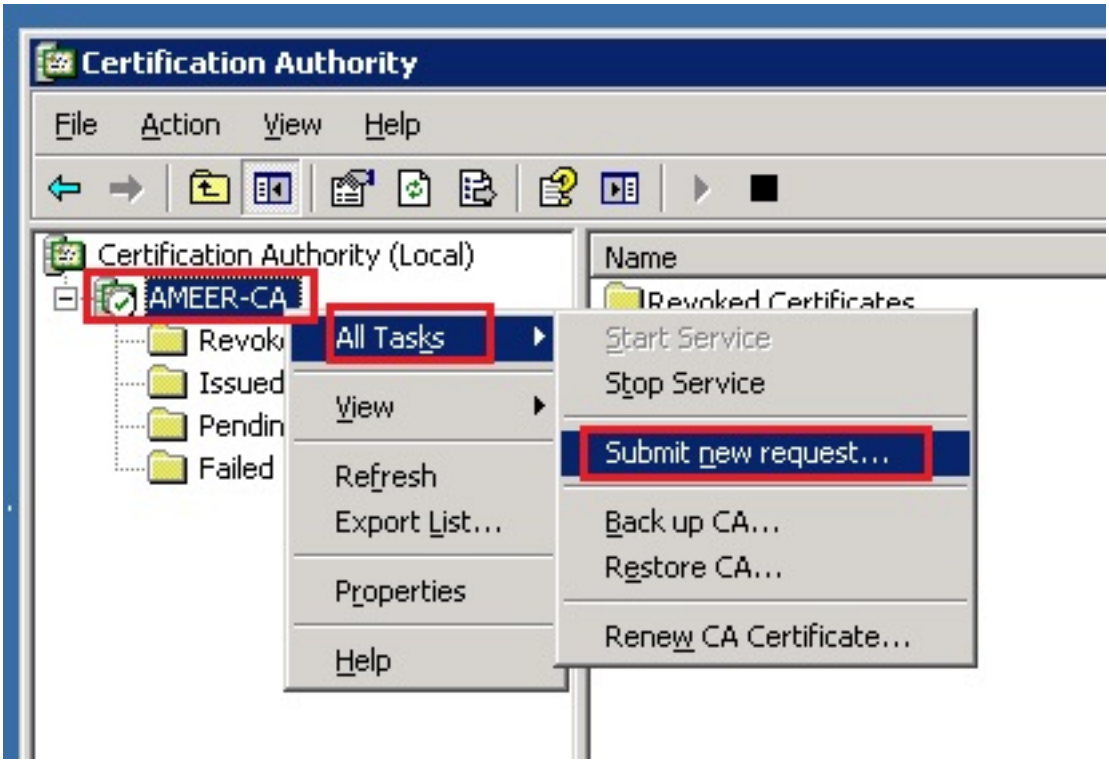
使用Microsoft Windows 2003證書頒發機構簽署CSR

這是Microsoft Windows 2003 - CA的可選資訊。

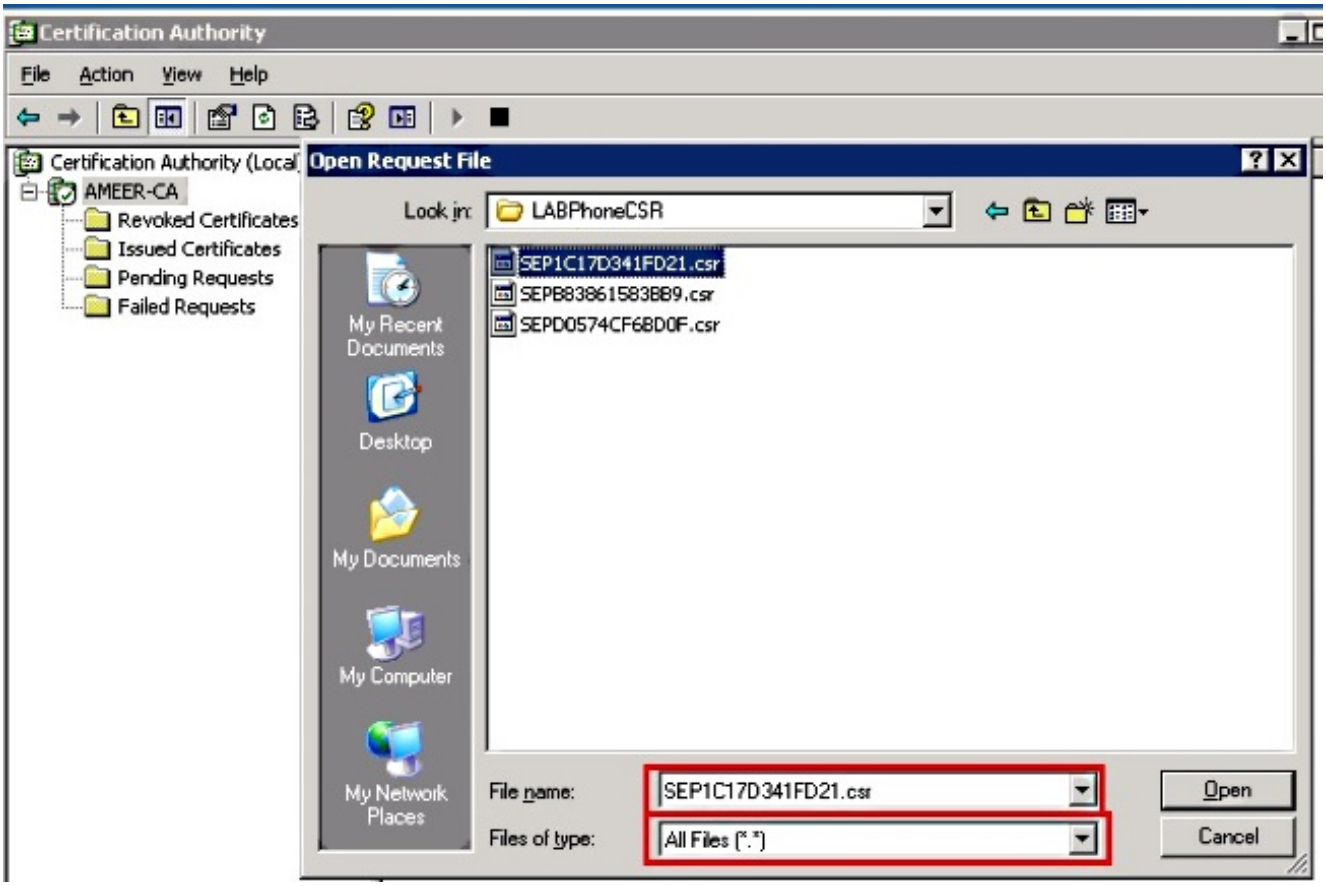
1. 開啟證書頒發機構。



2. 按一下右鍵CA並導航到**所有任務>提交新請求……**

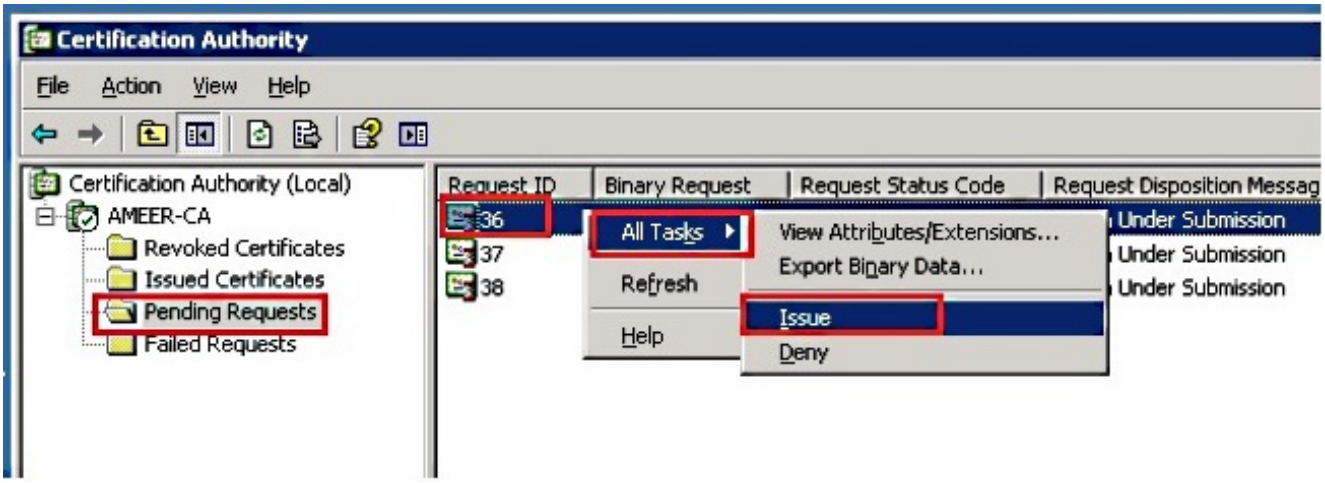


3. 選擇CSR，然後按一下**Open**。對所有CSR執行此操作。



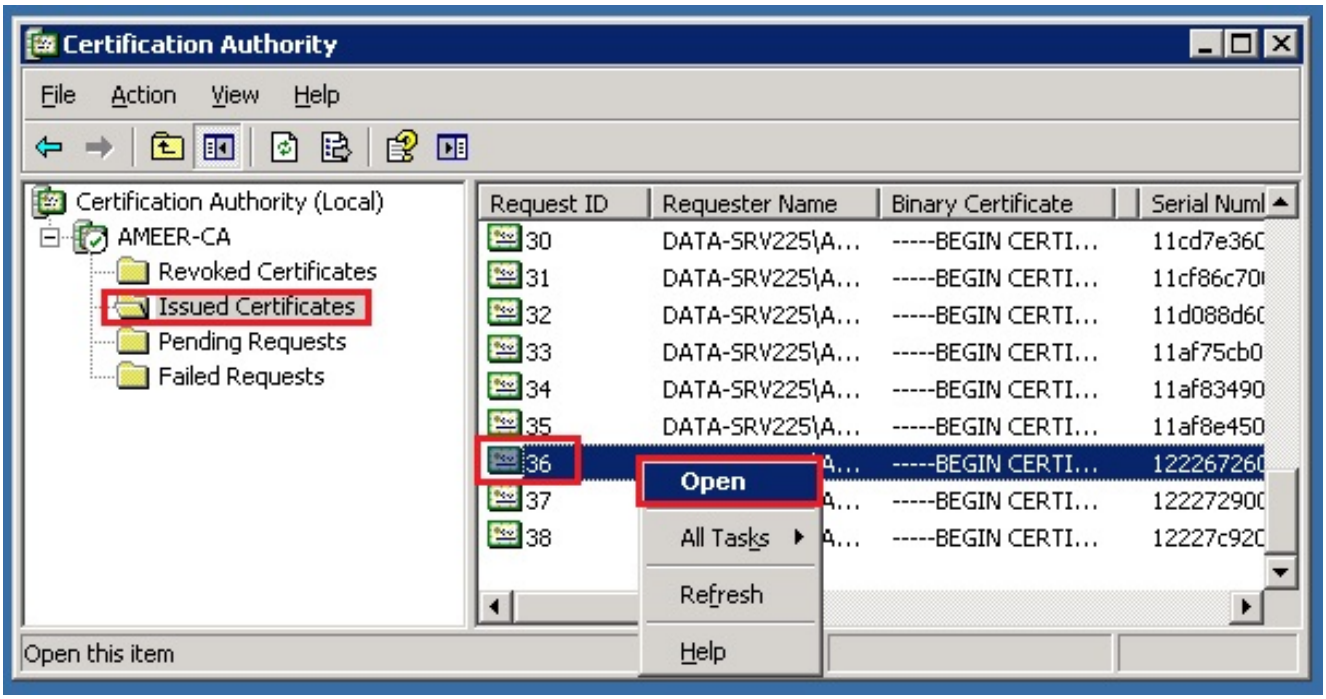
所有開啟的CSR都會顯示在「暫掛請求」資料夾中。

4. 按一下右鍵每個任務並導航到**所有任務>發出**以發出證書。對所有掛起請求執行此操作。

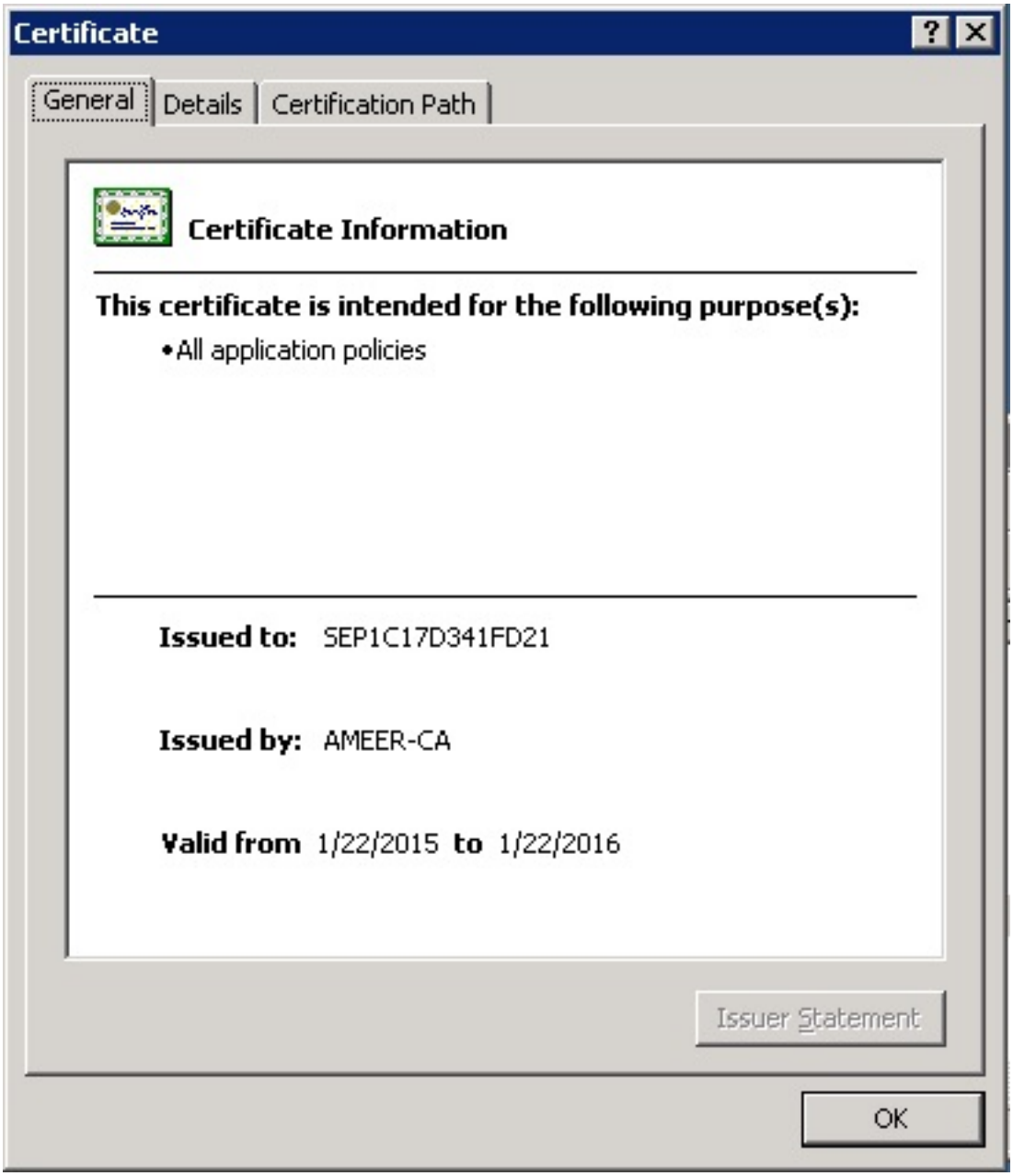


5. 若要下載憑證，請選擇**Issued Certificate**。

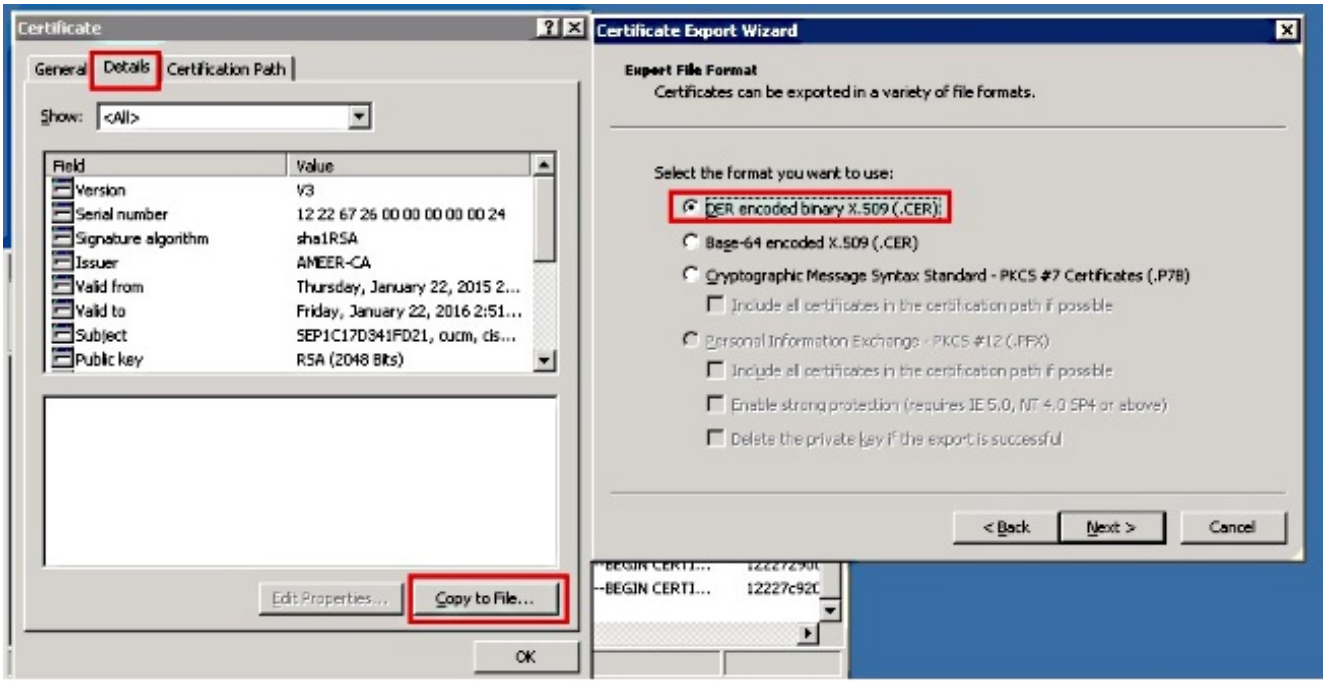
6. 按一下右鍵證書，然後按一下**Open**。



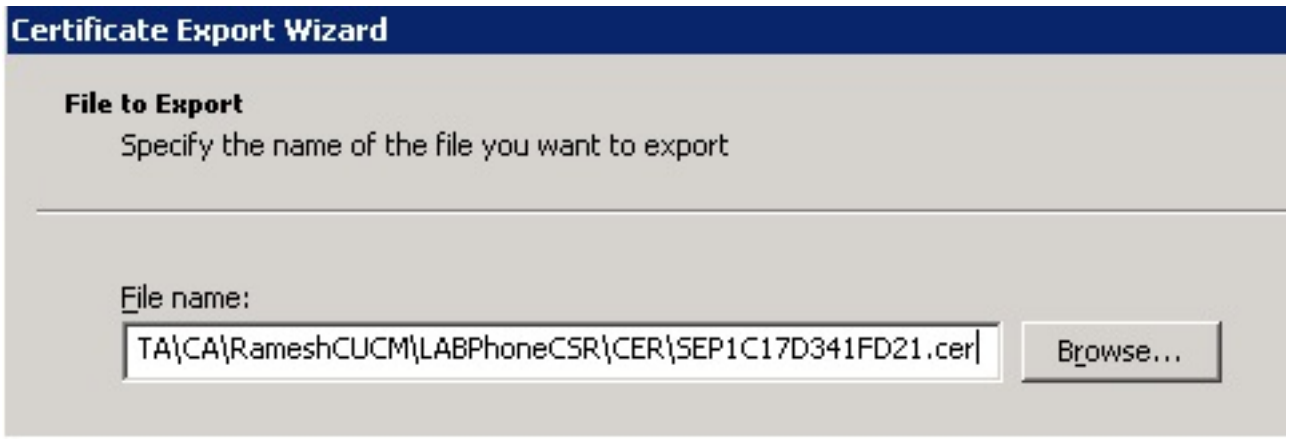
7. 您可以檢視證書詳細資訊。若要下載憑證，請選擇「詳細資訊」索引標籤，然後選擇**「複製到檔案.....」**



8. 在「Certificate Export Wizard（證書匯出嚮導）」中，選擇**DER encoded binary X.509(.CER)**。



9. 為檔案命名適當的名稱。此示例使用<MAC>.cer格式。

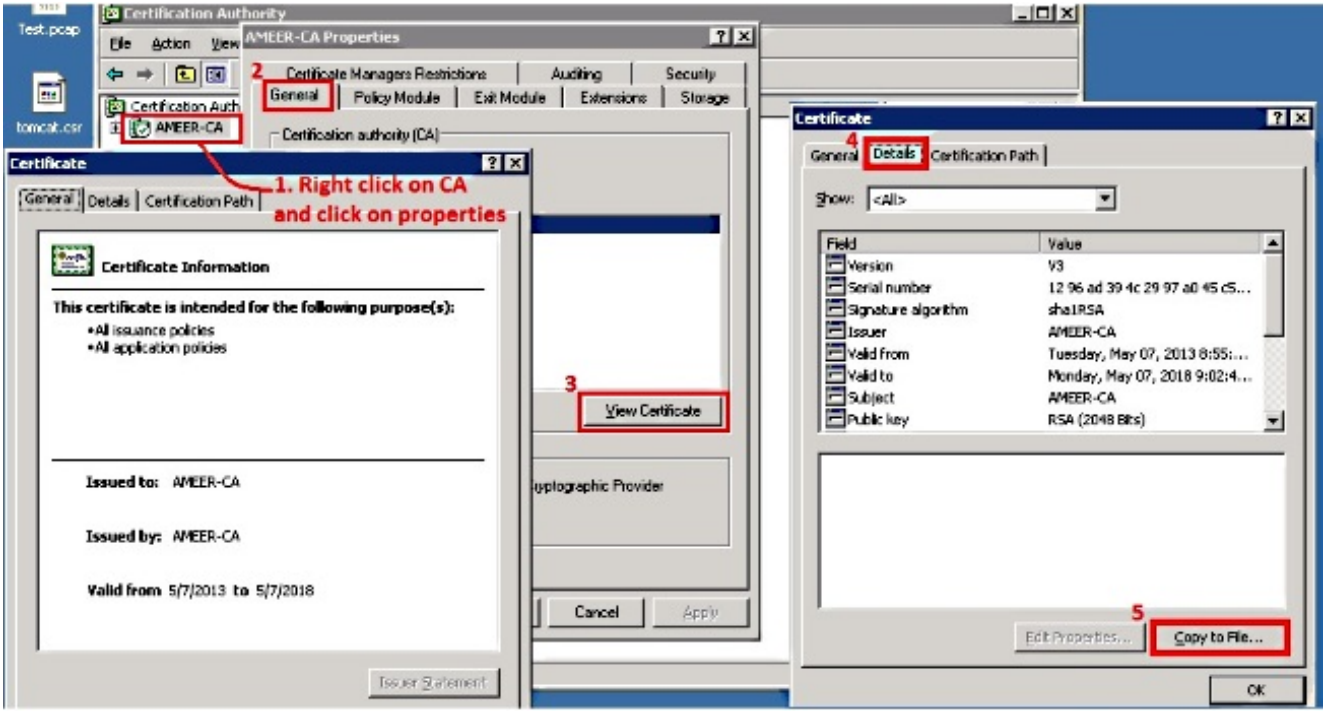


10. 通過此過程，在「已頒發的證書」部分下獲取其他電話的證書。

從CA取得根憑證

1. 開啟**證書頒發機構**。

2. 完成此熒幕截圖所示的步驟即可下載根CA。

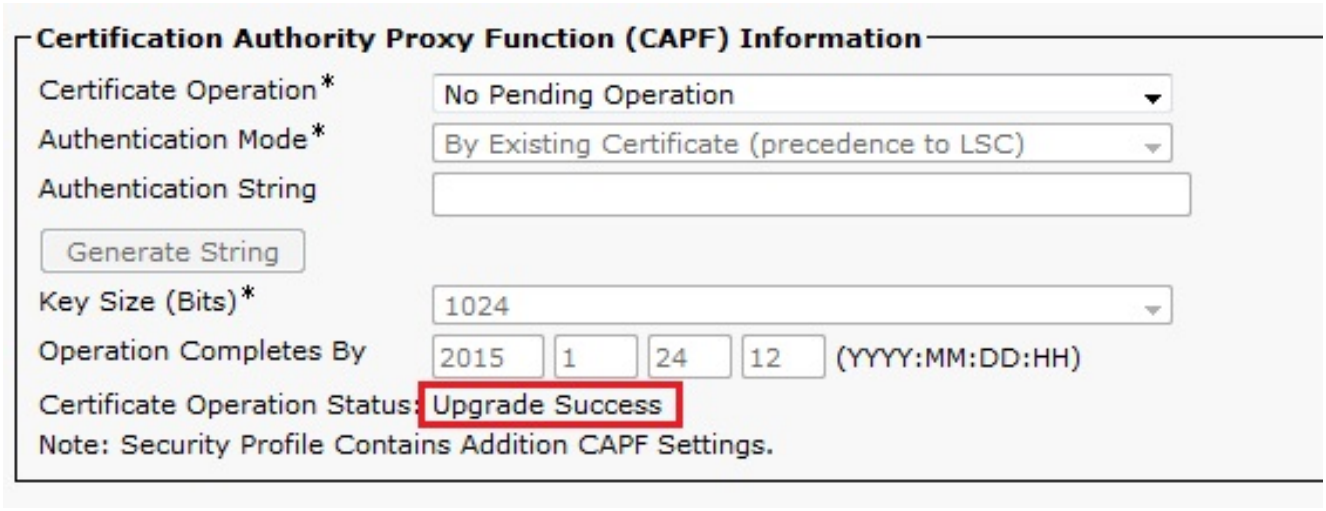


驗證

使用本節內容，確認您的組態是否正常運作。

1. 轉到電話配置頁面。

2. 在CAPF部分下，證書操作狀態應顯示為**升級成功**。



附註：如需詳細資訊，請參閱產生和匯入第三方CA簽署的LSC。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。