CUCM第三方CA签名LSC生成和导入配置示例

目录

简介

证书授权代理功能(CAPF)本地重要证书(LSC)是本地签名的。但是，您可能需要电话使用第三方证书颁发机构(CA)签名的LSC。本文档介绍可帮助您实现这一点的过程。

先决条件

要求

思科建议您了解思科统一通信管理器(CUCM)。

使用的组件

本文档中的信息基于CUCM 10.5(2)版；但是，此功能在10.0版及更高版本中有效。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

下面是此过程所涉及的步骤，每个步骤都在其自己的部分中进行了详细说明：

1. 上传CA根证书
2. 为终端证书颁发设置脱机CA
3. 为电话生成证书签名请求(CSR)
4. 从Cisco Unified Communications Manager(CUCM)获取生成的CSR到FTP服务器
5. 从CA获取电话证书
6. 将.cer转换为.der格式
7. 将证书(.der)压缩为.tgz格式
8. 将.tgz文件传输到Secure Shell FTP(SFTP)服务器
9. 将.tgz文件导入CUCM服务器
10. 使用Microsoft Windows 2003证书颁发机构签署CSR
11. 从CA获取根证书

上传CA根证书

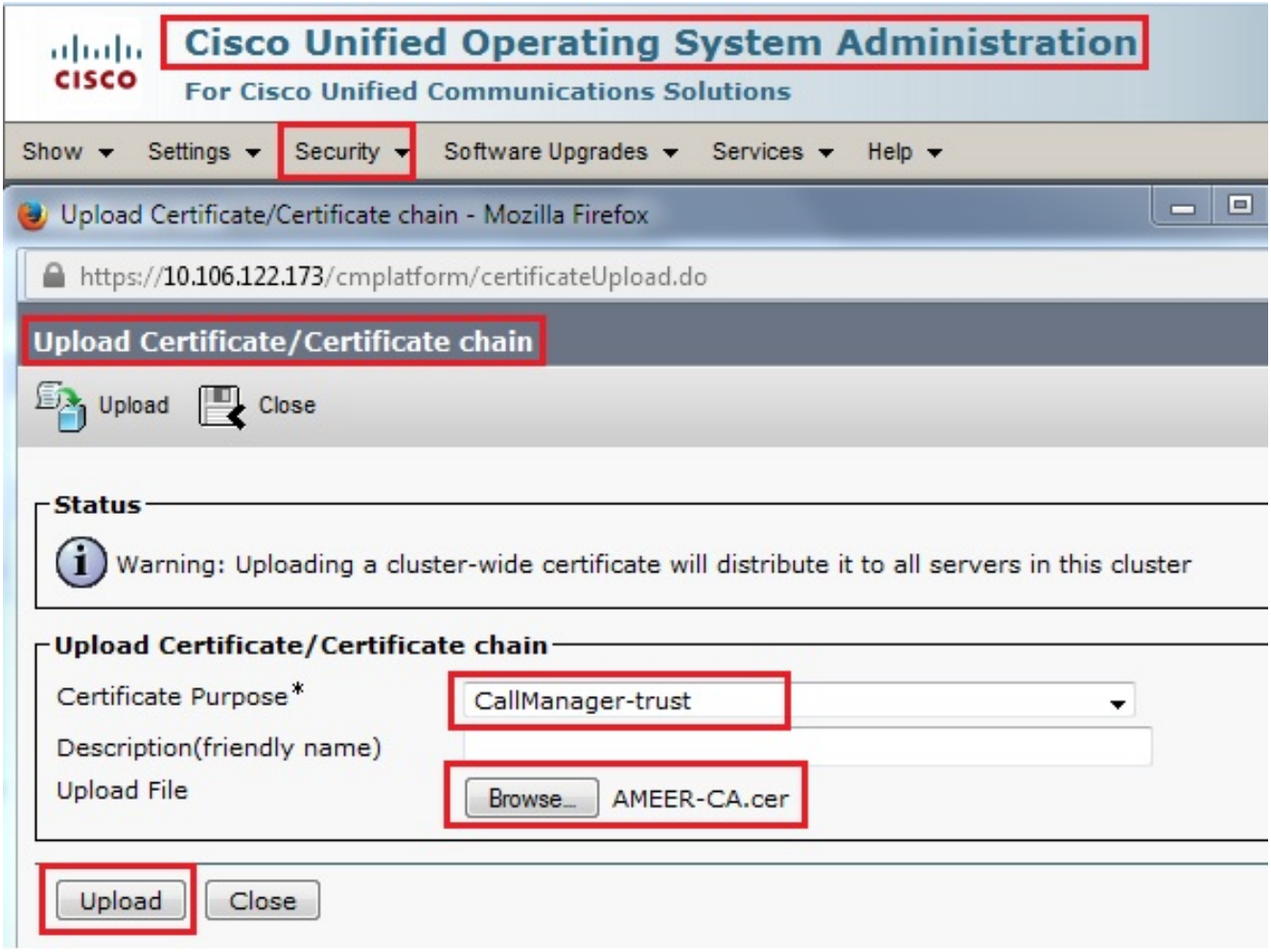
1. 登录思科统一操作系统(OS)管理Web GUI。

2. 导航到**安全证书管理**。

3. 单击**Upload Certificate/Certificate chain**。

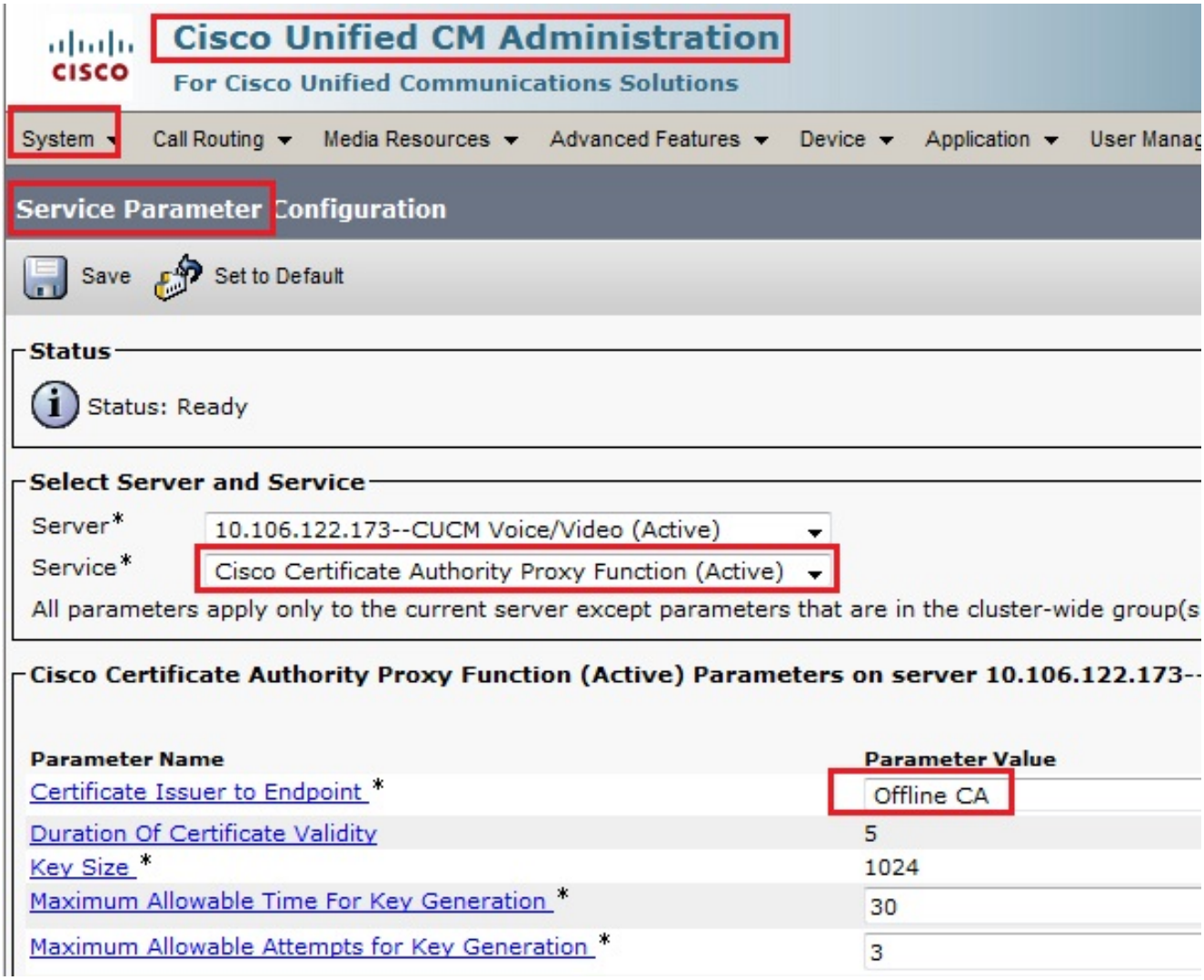
4. 在Certificate Purpose下选择**CallManager-trust**。

5. 浏览到CA的根证书，然后单击**Upload**。



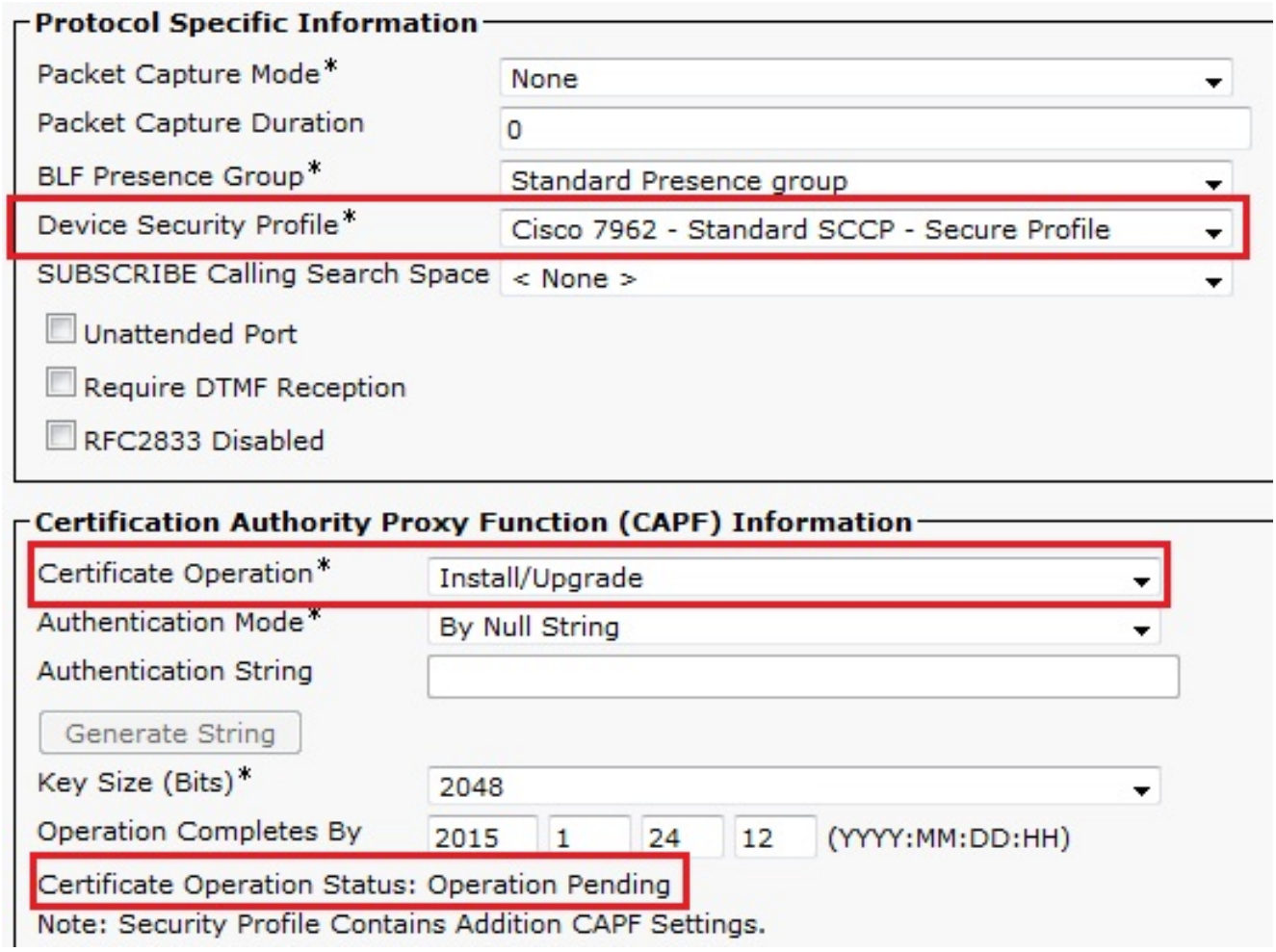
为终端证书颁发设置脱机CA

1. 登录到CUCM管理Web GUI。
2. 导航到**System > Service Parameter**。
3. 选择CUCM Server并为服务选择**Cisco Certificate Authority Proxy Function**。
4. 选择**Offline CA**以向终端颁发证书。

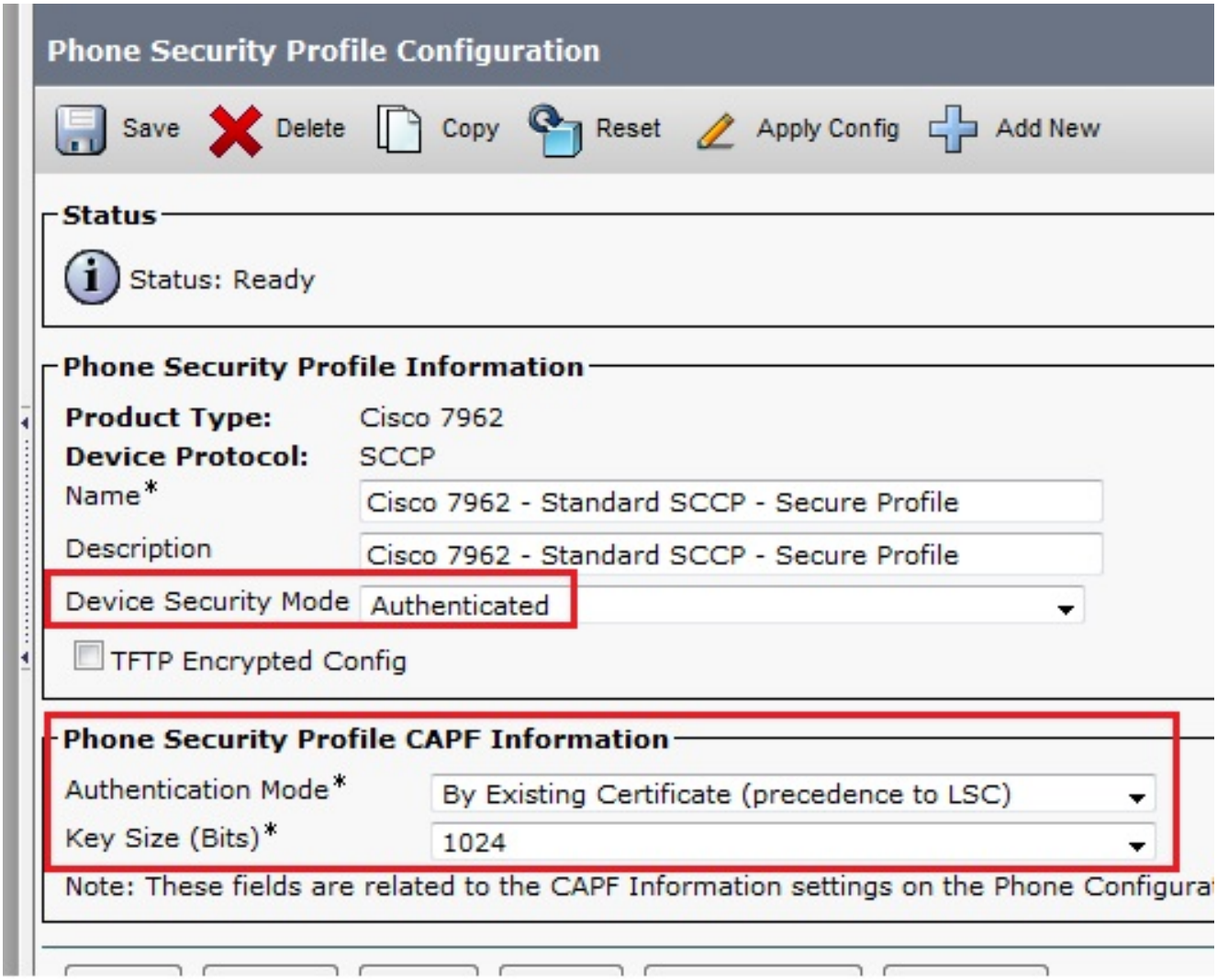


为电话生成证书签名请求(CSR)

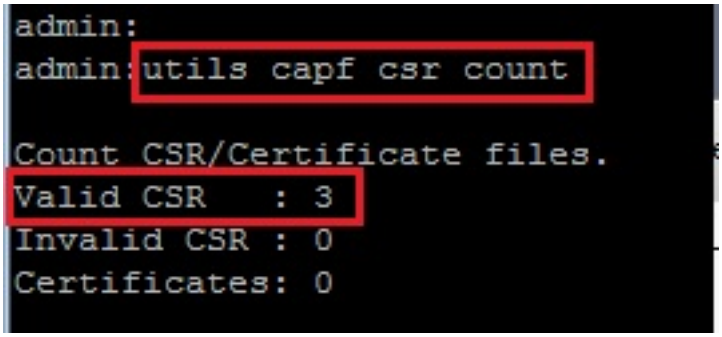
1. 登录到CUCM管理Web GUI。
2. 导航到**设备电话**。
3. 选择其LSC必须由外部CA签名的电话。
4. 将设备安全配置文件更改为安全配置文件（如果不存在，请在安全电话安全配置文件上添加一个系统）。
5. 在电话配置页面的CAPF部分下，选择**Install/Upgrade**进行认证操作。对于其LSC必须由外部CA签名的所有电话，请完成此步骤。对于证书操作状态，您应该看到**Operation Pending**。



电话安全配置文件（7962型号）。



在安全外壳(SSH)会话中输入**utils capf csr count**命令以确认是否生成CSR。（此屏幕截图显示已为三部电话生成CSR。）



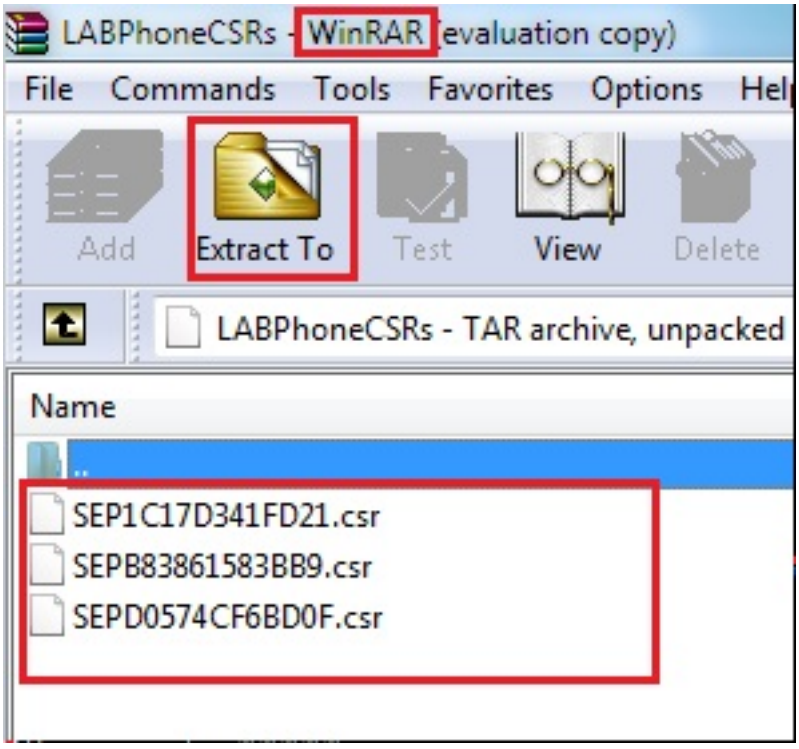
注意：电话的CAPF部分下的证书操作状态仍处于**操作挂起**状态。

获取从CUCM到FTP（或TFTP）服务器的生成的CSR

1. 通过SSH连接到CUCM服务器。
2. 执行**utils capf csr dump**命令。此屏幕截图显示正在传输到FTP的转储。

```
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打开转储文件并将CSR提取到本地计算机。



获取电话证书

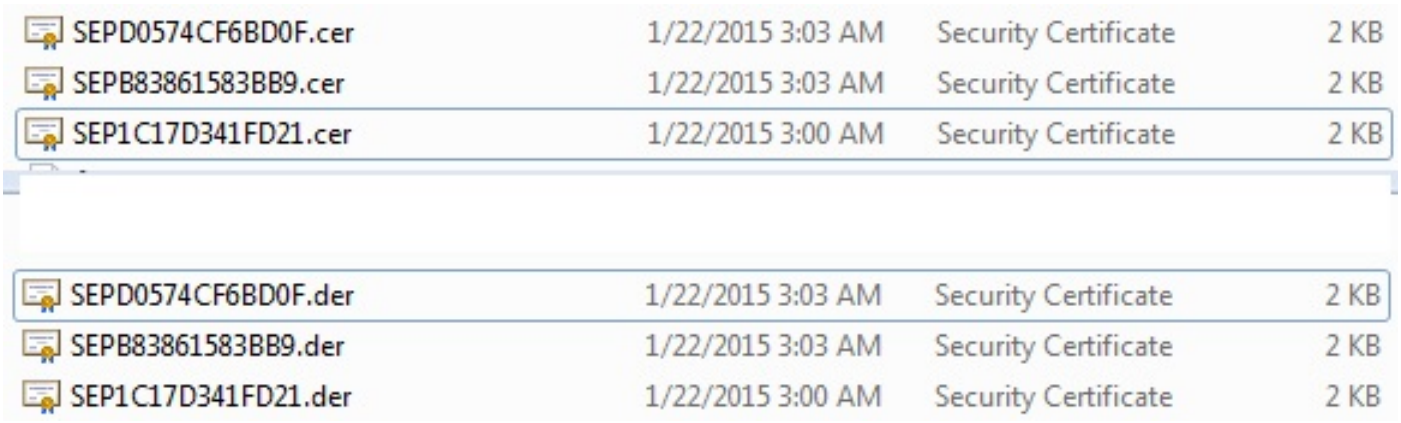
1. 将电话的CSR发送到CA。

2. CA为您提供签名证书。

注意：您可以使用Microsoft Windows 2003服务器作为CA。使用Microsoft Windows 2003 CA签署CSR的过程将在本文档后面部分说明。

将.cer转换为.der格式

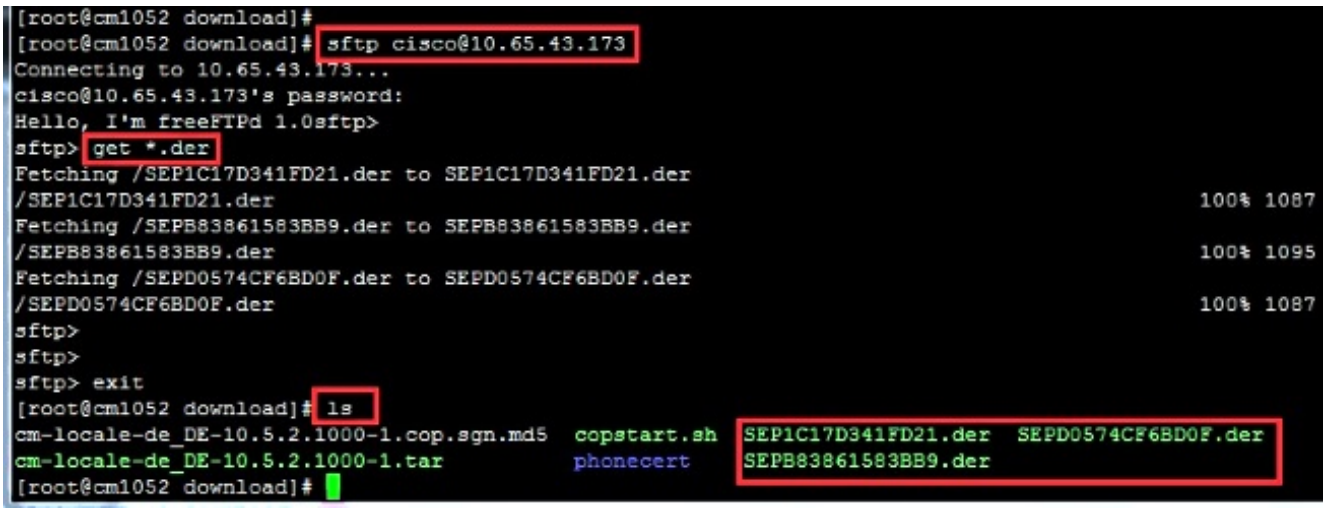
如果收到的证书是.cer格式，则将其重命名为.der。



将证书(.der)压缩为.tgz格式

可以使用CUCM服务器的根(Linux)压缩证书格式。也可以在正常的Linux系统中执行此操作。

1. 将所有签名证书通过SFTP服务器传输到Linux系统。



2. 输入此命令以将所有.der证书压缩为.tgz文件。

```
tar -zcvf
```

```
[root@cm1052 download]#
[root@cm1052 download]# tar -zcvf phoneDER.tgz *.der
SEP1C17D341FD21.der
SEPB83861583BB9.der
SEPD0574CF6BD0F.der
[root@cm1052 download]# ls
cm-locale-de_DE-10.5.2.1000-1.cop.sgn.md5  copstart.sh  phoneDER.tgz          SEPB83861583BB9.der
cm-locale-de_DE-10.5.2.1000-1.tar          phonecert    SEP1C17D341FD21.der   SEPD0574CF6BD0F.der
[root@cm1052 download]#
```

将.tgz文件传输到SFTP服务器

完成屏幕截图中所示的步骤，将.tgz文件传输到SFTP服务器。

```
[root@cm1052 download]# sftp cisco@10.65.43.173
Connecting to 10.65.43.173...
cisco@10.65.43.173's password:
Hello, I'm freeFTPd 1.0sftp>
sftp>
sftp> put phoneDER.tgz
Uploading phoneDER.tgz to /phoneDER.tgz
phoneDER.tgz
sftp>
```

将.tgz文件导入CUCM服务器

1. 通过SSH连接到CUCM服务器。
2. 执行**utils capf cert import**命令。

```
admin:
admin utils capf cert import

Importing files.

Source:

 1) Remote Filesystem via FTP
 2) Remote Filesystem via TFTP
 q) quit

Please select an option (1 - 2 or "q" ): 1
File Path: phoneDER.tgz
Server: 10.65.43.173
User Name: cisco
Password: *****
Certificate file imported successfully
Certificate files extracted successfully.
Please wait. Processing 3 files
```

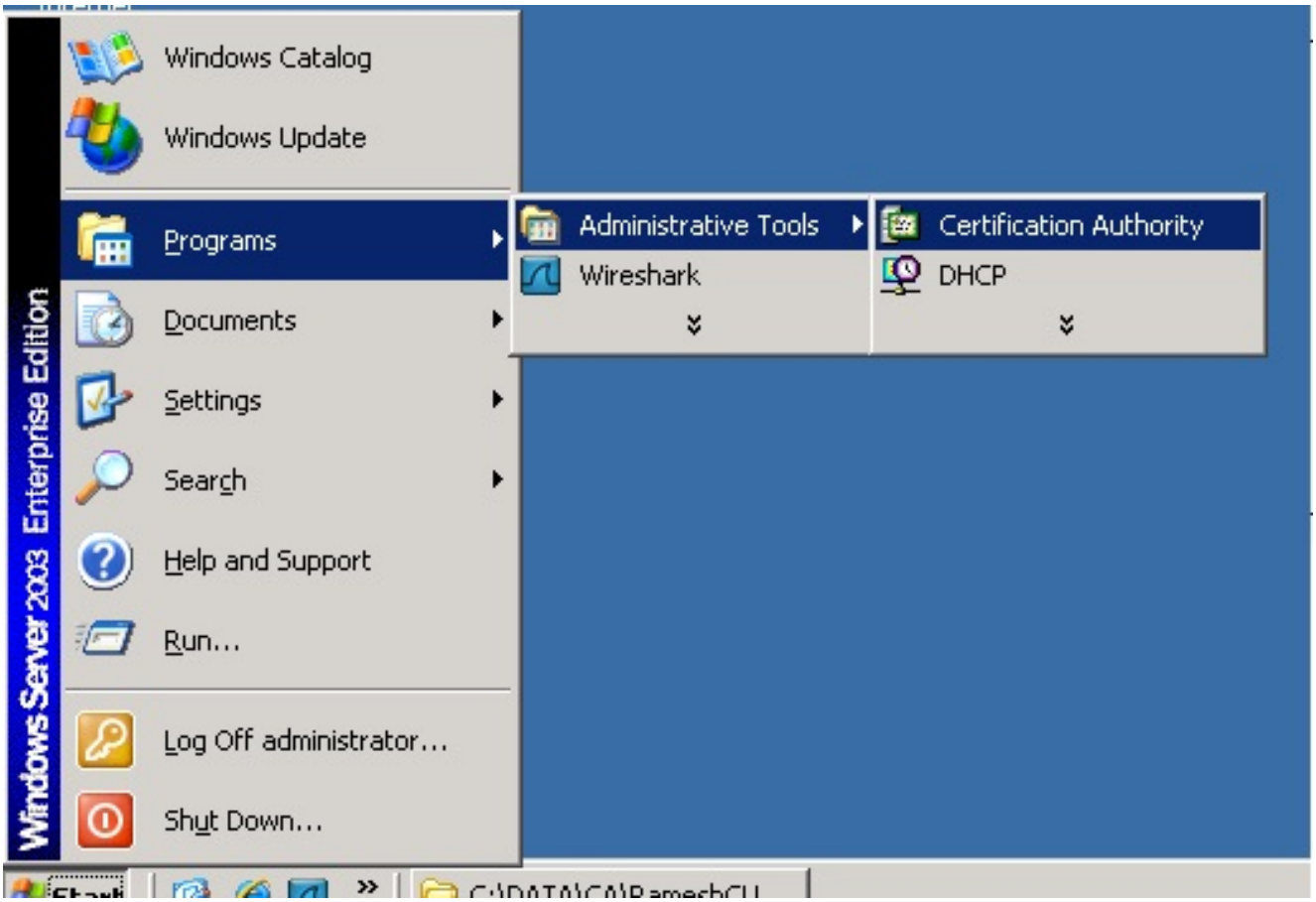
成功导入证书后，您可以看到CSR计数变为零。

```
admin:
admin:utils capf csr count

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

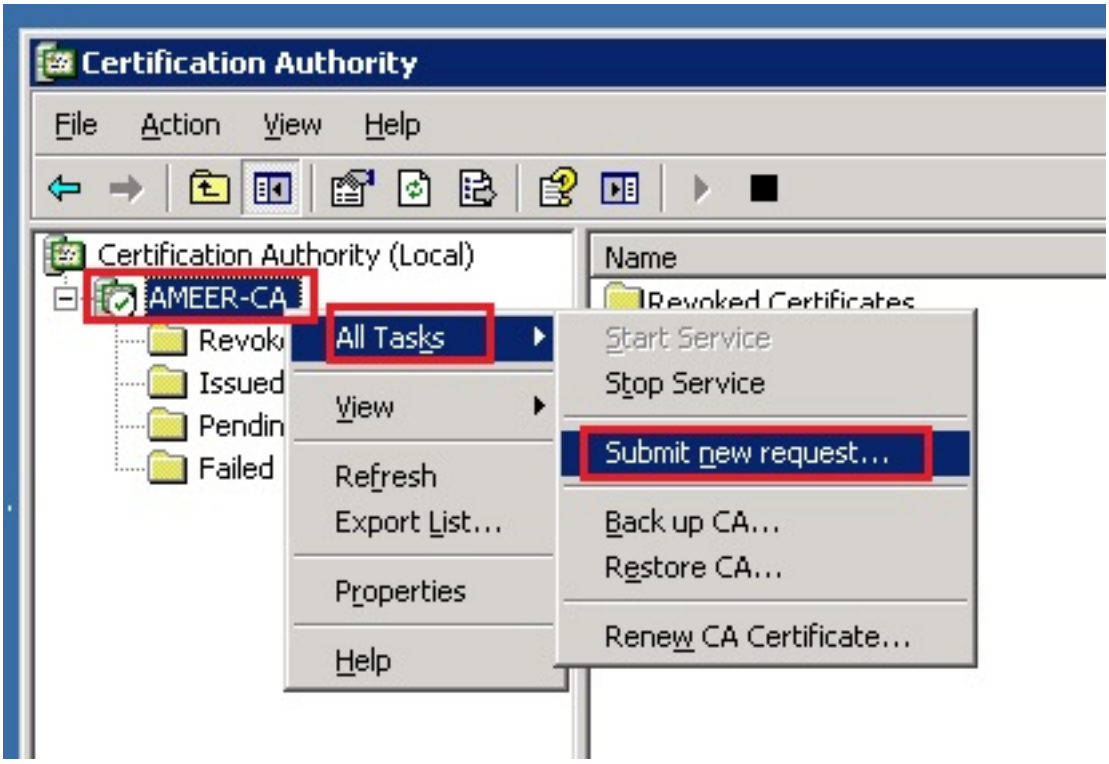
使用Microsoft Windows 2003证书颁发机构签署CSR

这是Microsoft Windows 2003 - CA的可选信息。

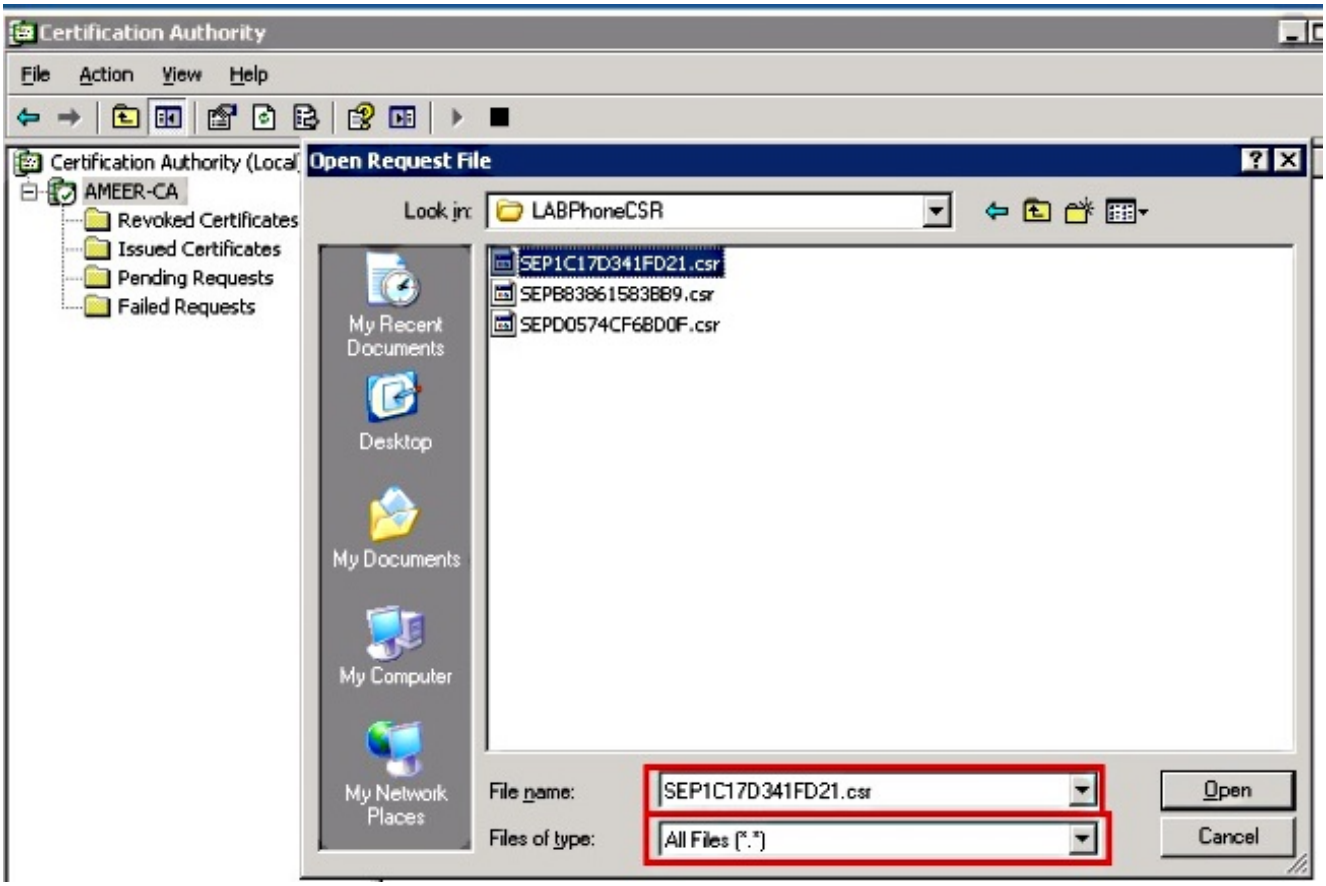
1. 打开证书颁发机构。



2. 右键单击CA并导航到**所有任务>提交新请求……**

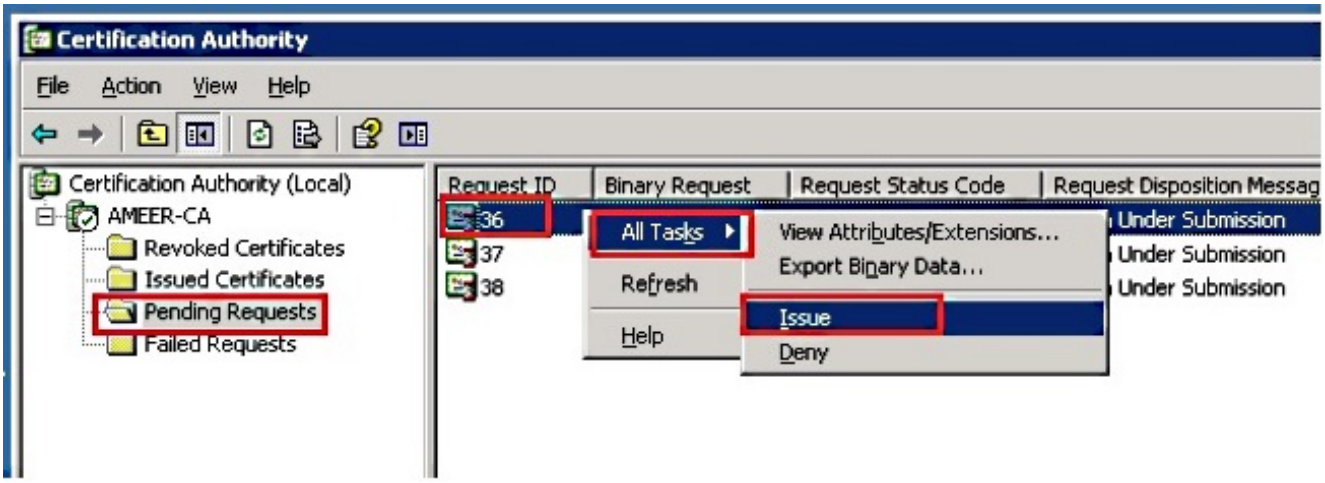


3. 选择CSR并单击**Open**。对所有CSR执行此操作。



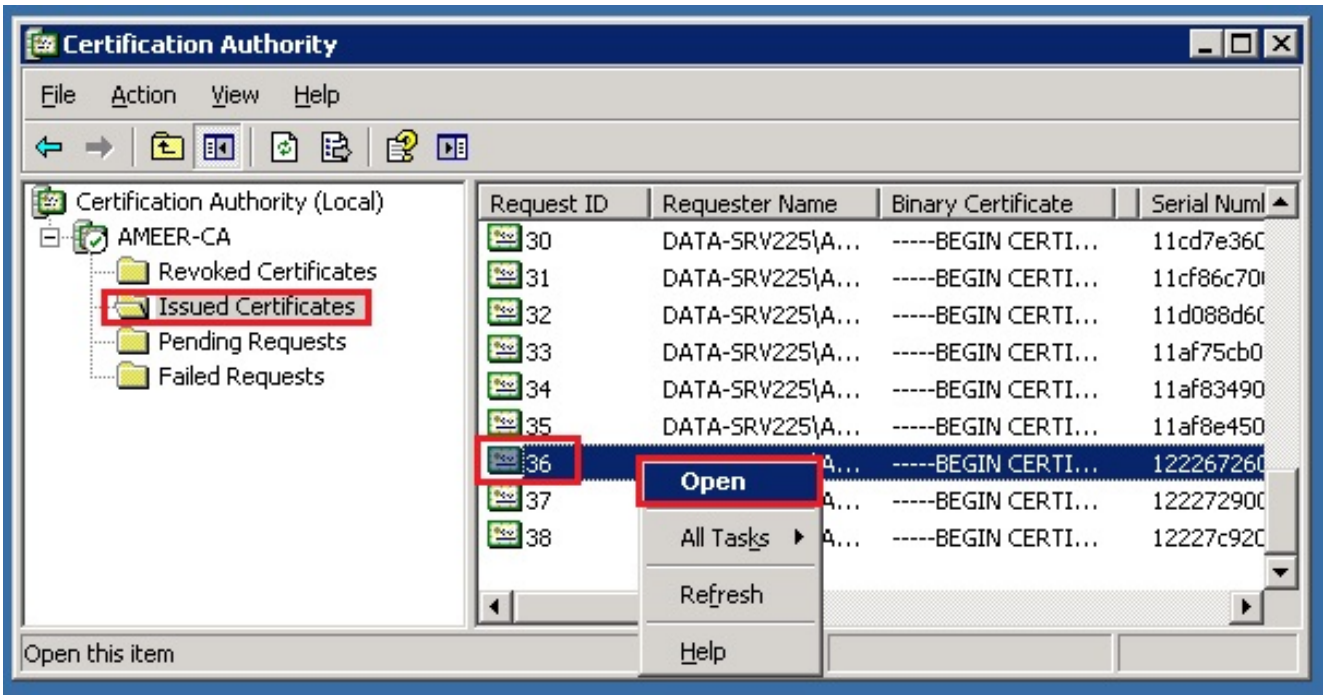
所有打开的CSR都会显示在“待处理请求”文件夹中。

4. 右键单击每个任务并导航到**所有任务>发出**以颁发证书。对所有挂起请求执行此操作。

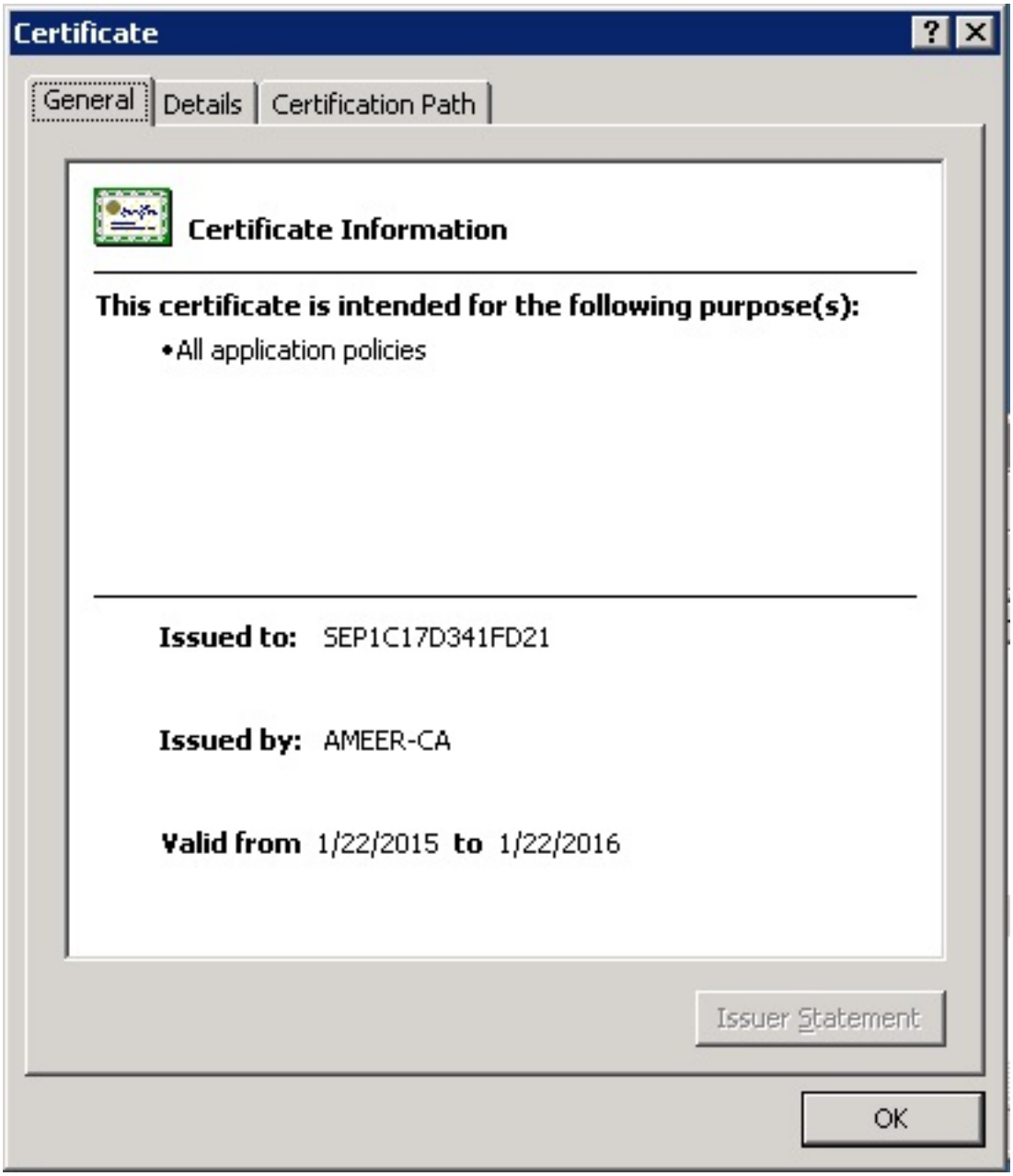


5. 要下载证书，请选择**Issued Certificate**。

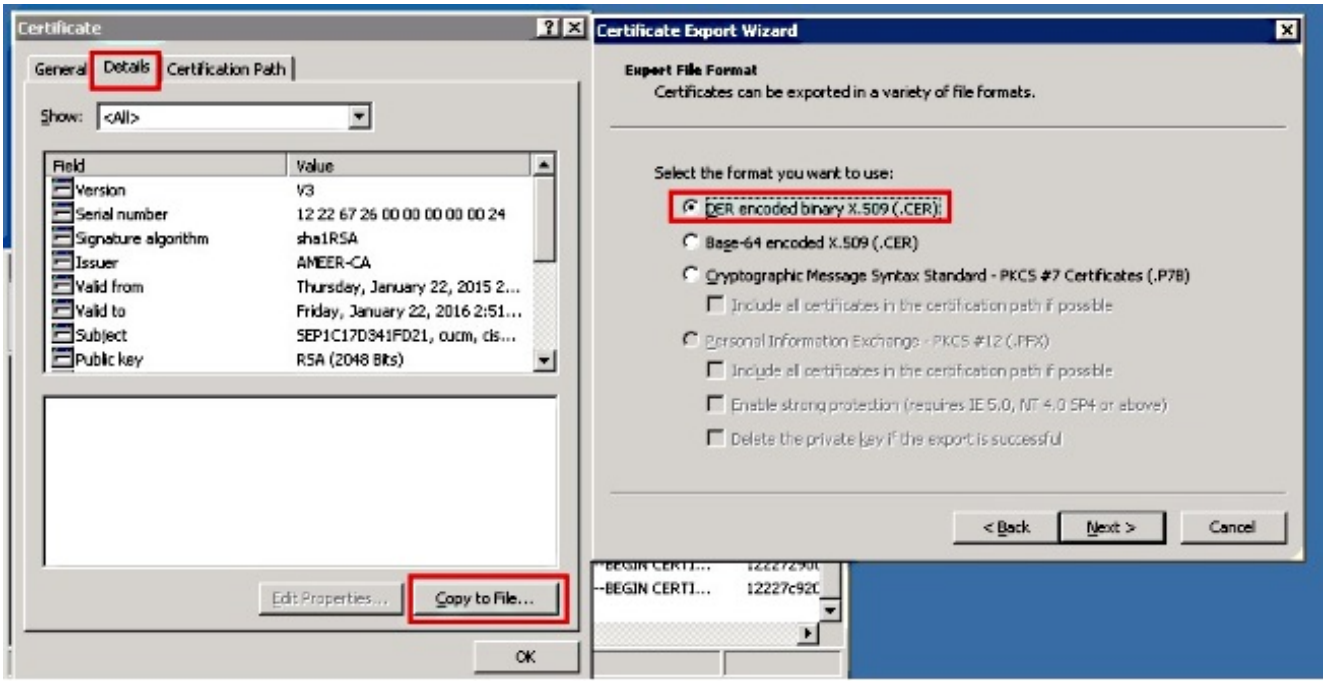
6. 右键单击证书，然后单击**打开**。



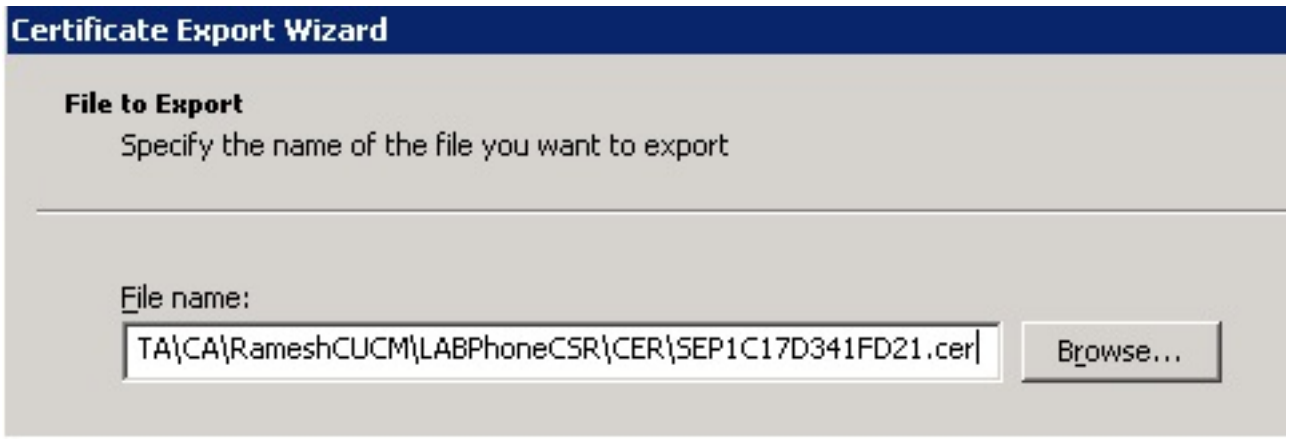
7. 您可以查看证书详细信息。要下载证书，请选择Details选项卡，然后选择**Copy to File...**



8. 在Certificate Export Wizard中，选择**DER encoded binary X.509(.CER)**。



9. 为文件命名适当的名称。本示例使用<MAC>.cer格式。

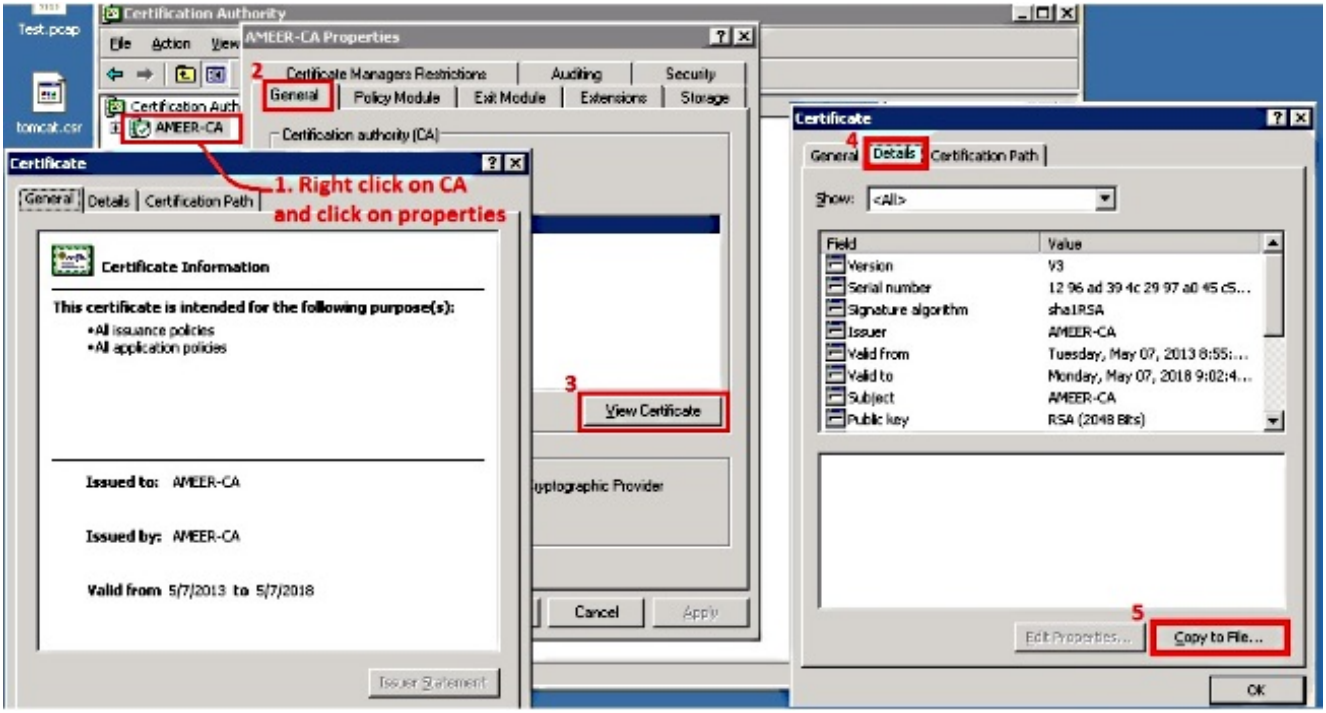


10. 通过此过程在Issued Certificate部分下获取其他电话的证书。

从CA获取根证书

1. 打开**证书颁发机构**。

2. 完成此屏幕截图中所示的步骤，以下载根CA。

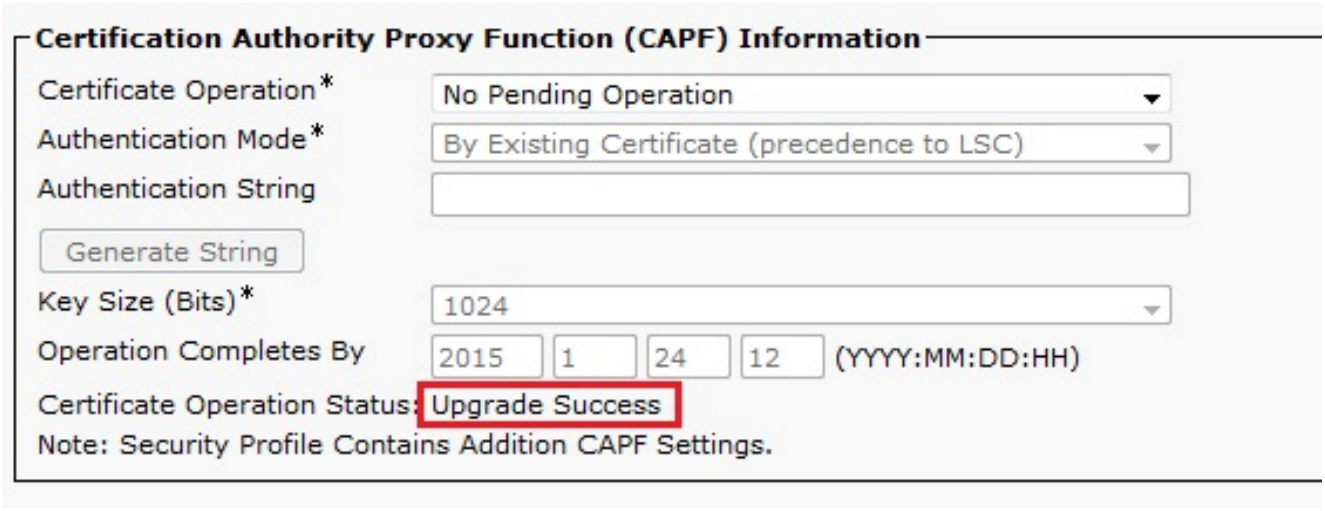


验证

使用本部分可确认配置能否正常运行。

1. 转到电话配置页面。

2. 在CAPF部分下，证书操作状态应显示为**升级成功**。



注意：有关详细信息，请参阅生成和导入第三方CA签名的LSC。

故障排除

目前没有针对此配置的故障排除信息。