

# Exemplo de configuração de geração e importação de LSCs assinados por CA de terceiros do CUCM

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Carregar o certificado raiz da CA](#)

[Definir CA Offline para Emissão de Certificado para Ponto de Extremidade](#)

[Gerar uma solicitação de assinatura de certificado \(CSR\) para os telefones](#)

[Obtenha o CSR gerado do CUCM para o servidor FTP \(ou TFTP\)](#)

[Obter o certificado do telefone](#)

[Converter .cer em formato .der](#)

[Compactar os Certificados \(.der\) para o Formato .tgz](#)

[Transfira o arquivo .tgz para o servidor SFTP](#)

[Importe o arquivo .tgz para o servidor CUCM](#)

[Assine o CSR com a autoridade de certificação do Microsoft Windows 2003](#)

[Obter o Certificado Raiz da CA](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Os LSCs (Locally Significant Certificates) da CAPF (Certificate Authority Proxy Function) são assinados localmente. No entanto, talvez você precise de telefones para usar LSCs assinados por uma autoridade de certificação (CA) de terceiros. Este documento descreve um procedimento que ajuda você a conseguir isso.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento do Cisco Unified Communication Manager (CUCM).

## Componentes Utilizados

As informações neste documento são baseadas no CUCM Versão 10.5(2); no entanto, esse recurso funciona a partir da versão 10.0 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

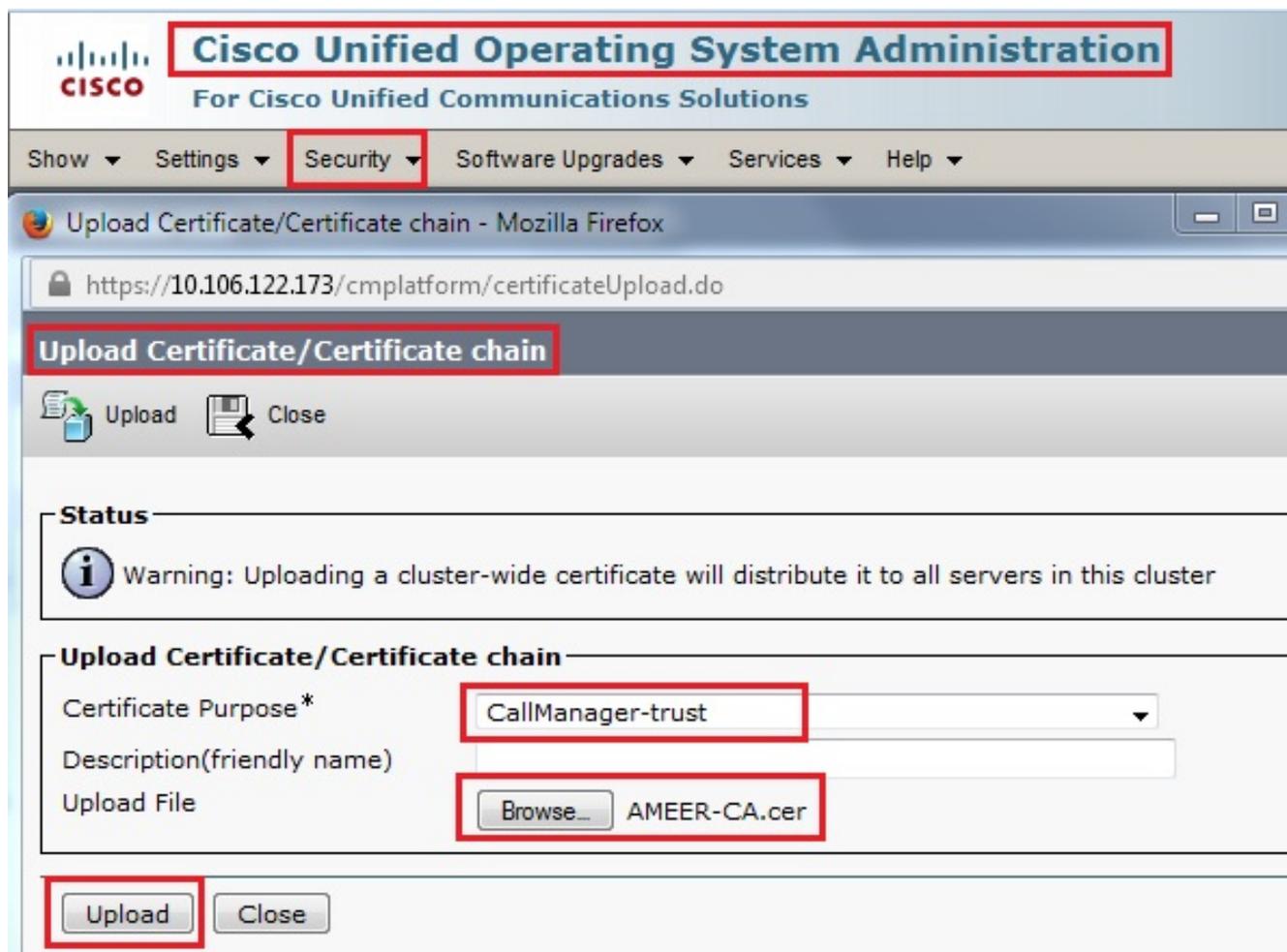
## Configurar

Estas são as etapas envolvidas neste procedimento, cada uma detalhada em sua própria seção:

1. [Carregar o certificado raiz da CA](#)
2. [Definir CA Offline para Emissão de Certificado para Ponto de Extremidade](#)
3. [Gerar uma solicitação de assinatura de certificado \(CSR\) para os telefones](#)
4. [Obtenha o CSR gerado do Cisco Unified Communications Manager \(CUCM\) para o servidor FTP](#)
5. [Obter o Certificado Telefônico da CA](#)
6. [Converter .cer em formato .der](#)
7. [Compactar os Certificados \(.der\) para o Formato .tgz](#)
8. [Transfira o arquivo .tgz para o servidor FTP Secure Shell \(SFTP\)](#)
9. [Importe o arquivo .tgz para o servidor CUCM](#)
10. [Assine o CSR com a autoridade de certificação do Microsoft Windows 2003](#)
11. [Obter o Certificado Raiz da CA](#)

### Carregar o certificado raiz da CA

1. Faça login na GUI da Web do Cisco Unified Operating System (OS) Administration.
2. Navegue até **Gerenciamento de Certificado de Segurança**.
3. Clique em **Upload Certificate/Certificate chain**.
4. Selecione **CallManager-trust** em Certificate Purpose.
5. Navegue até o certificado raiz da CA e clique em **Upload**.



## Definir CA Offline para Emissão de Certificado para Ponto de Extremidade

1. Faça login na GUI da Web de administração do CUCM.
2. Navegue até **System > Service Parameter**.
3. Escolha o servidor CUCM e selecione **Cisco Certificate Authority Proxy Function** para o serviço.
4. Selecione **CA Offline** para Emissão de Certificado para Ponto de Extremidade.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions" are visible. A navigation menu includes "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", and "User Management". The "System" menu is highlighted, and the "Service Parameter Configuration" page is open. Below the navigation, there are "Save" and "Set to Default" buttons. The "Status" section shows "Status: Ready". The "Select Server and Service" section has two dropdown menus: "Server\*" set to "10.106.122.173--CUCM Voice/Video (Active)" and "Service\*" set to "Cisco Certificate Authority Proxy Function (Active)". Below this, a table displays parameters for the selected service on the specified server.

Parameter Name	Parameter Value
<a href="#">Certificate Issuer to Endpoint</a> *	Offline CA
<a href="#">Duration Of Certificate Validity</a>	5
<a href="#">Key Size</a> *	1024
<a href="#">Maximum Allowable Time For Key Generation</a> *	30
<a href="#">Maximum Allowable Attempts for Key Generation</a> *	3

## Gerar uma solicitação de assinatura de certificado (CSR) para os telefones

1. Faça login na GUI da Web de administração do CUCM.
2. Navegue até **Device Phones**.
3. Escolha o telefone cujo LSC deve ser assinado pela CA externa.
4. Altere o perfil de segurança do dispositivo para um seguro (se não estiver presente, adicione um sistema ao perfil Security Phone Security).
5. Na página de configuração do telefone, na seção CAPF, escolha **Install/Upgrade** para a Operação de Certificação. Conclua esta etapa para todos os telefones cujo LSC deve ser assinado pela CA externa. Você deve ver **Operação pendente** para o Status da operação de certificado.

### Protocol Specific Information

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
Device Security Profile*	Cisco 7962 - Standard SCCP - Secure Profile
SUBSCRIBE Calling Search Space	< None >
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> Require DTMF Reception	
<input type="checkbox"/> RFC2833 Disabled	

### Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
<input type="button" value="Generate String"/>	
Key Size (Bits)*	2048
Operation Completes By	2015 1 24 12 (YYYY:MM:DD:HH)
Certificate Operation Status:	Operation Pending

Note: Security Profile Contains Addition CAPF Settings.

Phone Security profile (modelo 7962).

### Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

**Status**  
 Status: Ready

**Phone Security Profile Information**

Product Type: Cisco 7962  
 Device Protocol: SCCP  
 Name\*: Cisco 7962 - Standard SCCP - Secure Profile  
 Description: Cisco 7962 - Standard SCCP - Secure Profile  
 Device Security Mode: Authenticated  
 TFTP Encrypted Config

**Phone Security Profile CAPF Information**

Authentication Mode\*: By Existing Certificate (precedence to LSC)  
 Key Size (Bits)\*: 1024

Note: These fields are related to the CAPF Information settings on the Phone Configuration

Insira o comando **utils capf csr count** na sessão Secure Shell (SSH) para confirmar se um CSR é gerado. (Esta captura de tela mostra que um CSR foi gerado para três telefones.)

```
admin:
admin: utils capf csr count
Count CSR/Certificate files.
Valid CSR : 3
Invalid CSR : 0
Certificates: 0
```

**Note:** O Status da operação de certificado na seção CAPF do telefone permanece no estado Operação pendente.

### Obtenha o CSR gerado do CUCM para o servidor FTP (ou TFTP)

1. SSH no servidor CUCM.
2. Execute o comando **utils capf csr dump**. Esta captura de tela mostra o dump sendo transferido para o FTP.

```
admin:
admin:utils capf csr dump

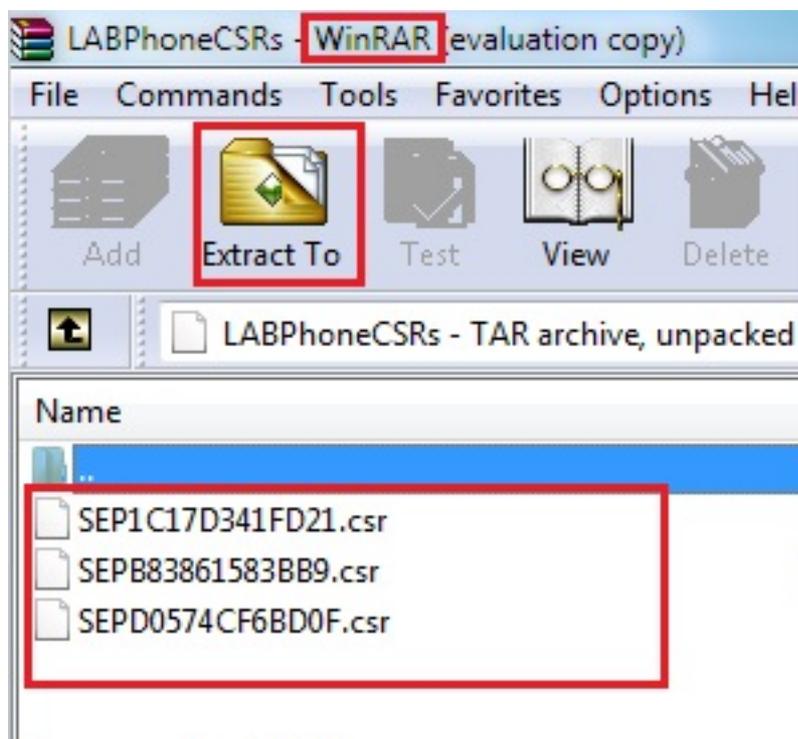
Dump CSR files.
CSR File tarred successfully...

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. Abra o arquivo de despejo com o WinRAR e extraia o CSR para o computador local.



### Obter o certificado do telefone

1. Envie os CSRs do telefone para a CA.
2. A CA fornece um certificado assinado.

**Note:** Você pode usar um servidor Microsoft Windows 2003 como CA. O procedimento para assinar o CSR com uma CA do Microsoft Windows 2003 será explicado posteriormente neste documento.

## Converter .cer em formato .der

Se os certificados recebidos estiverem no formato .cer, renomeie-os como .der.

SEPD0574CF6BD0F.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
SEPB83861583BB9.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
SEP1C17D341FD21.cer	1/22/2015 3:00 AM	Security Certificate	2 KB
SEPD0574CF6BD0F.der	1/22/2015 3:03 AM	Security Certificate	2 KB
SEPB83861583BB9.der	1/22/2015 3:03 AM	Security Certificate	2 KB
SEP1C17D341FD21.der	1/22/2015 3:00 AM	Security Certificate	2 KB

## Compactar os Certificados (.der) para o Formato .tgz

Você pode usar a raiz do servidor CUCM (Linux) para compactar o formato do certificado. Você também pode fazer isso em um sistema Linux normal.

1. Transfira todos os certificados assinados para o sistema Linux com o servidor SFTP.

```
[root@cm1052 download]#
[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> get *.der
Fetching /SEP1C17D341FD21.der to SEP1C17D341FD21.der          100% 1087
Fetching /SEPB83861583BB9.der to SEPB83861583BB9.der        100% 1095
Fetching /SEPD0574CF6BD0F.der to SEPD0574CF6BD0F.der        100% 1087
sftp>
sftp>
sftp> exit
[root@cm1052 download]# ls
cm-locale-de_DE-10.5.2.1000-1.cop.sgn.md5  copstart.sh  SEP1C17D341FD21.der  SEPD0574CF6BD0F.der
cm-locale-de_DE-10.5.2.1000-1.tar         phonecert    SEPB83861583BB9.der
```

2. Insira este comando para compactar todos os certificados .der em um arquivo .tgz.

```
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]#
```

## Transfira o arquivo .tgz para o servidor SFTP

Conclua as etapas mostradas na captura de tela para transferir o arquivo .tgz para o servidor SFTP.

```
[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>
```

## Importe o arquivo .tgz para o servidor CUCM

1. SSH no servidor CUCM.
2. Execute o comando `utils capf cert import`.

```
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
```

Quando os certificados forem importados com êxito, você poderá ver a contagem de CSR se tornar zero.

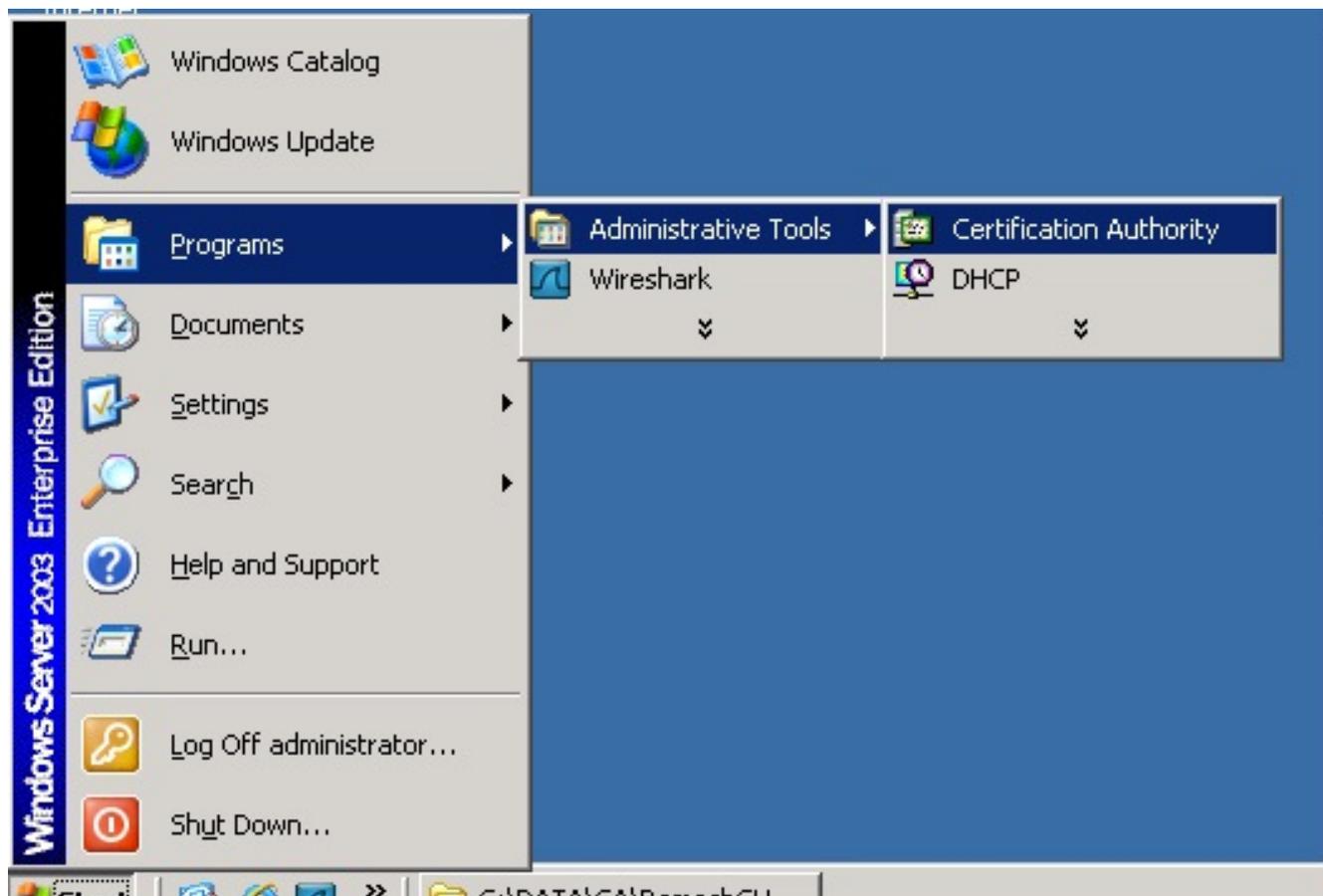
```
admin:
admin:utils capf csr count

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

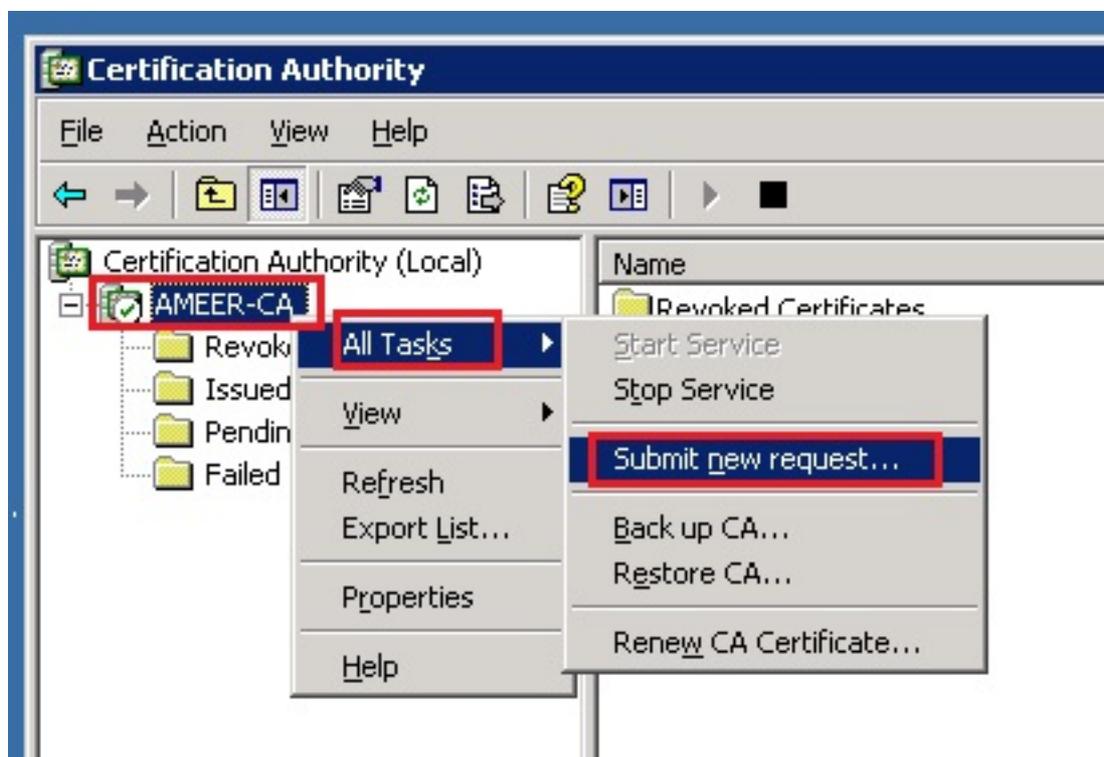
## Assine o CSR com a autoridade de certificação do Microsoft Windows 2003

Essas informações são opcionais para o Microsoft Windows 2003 - CA.

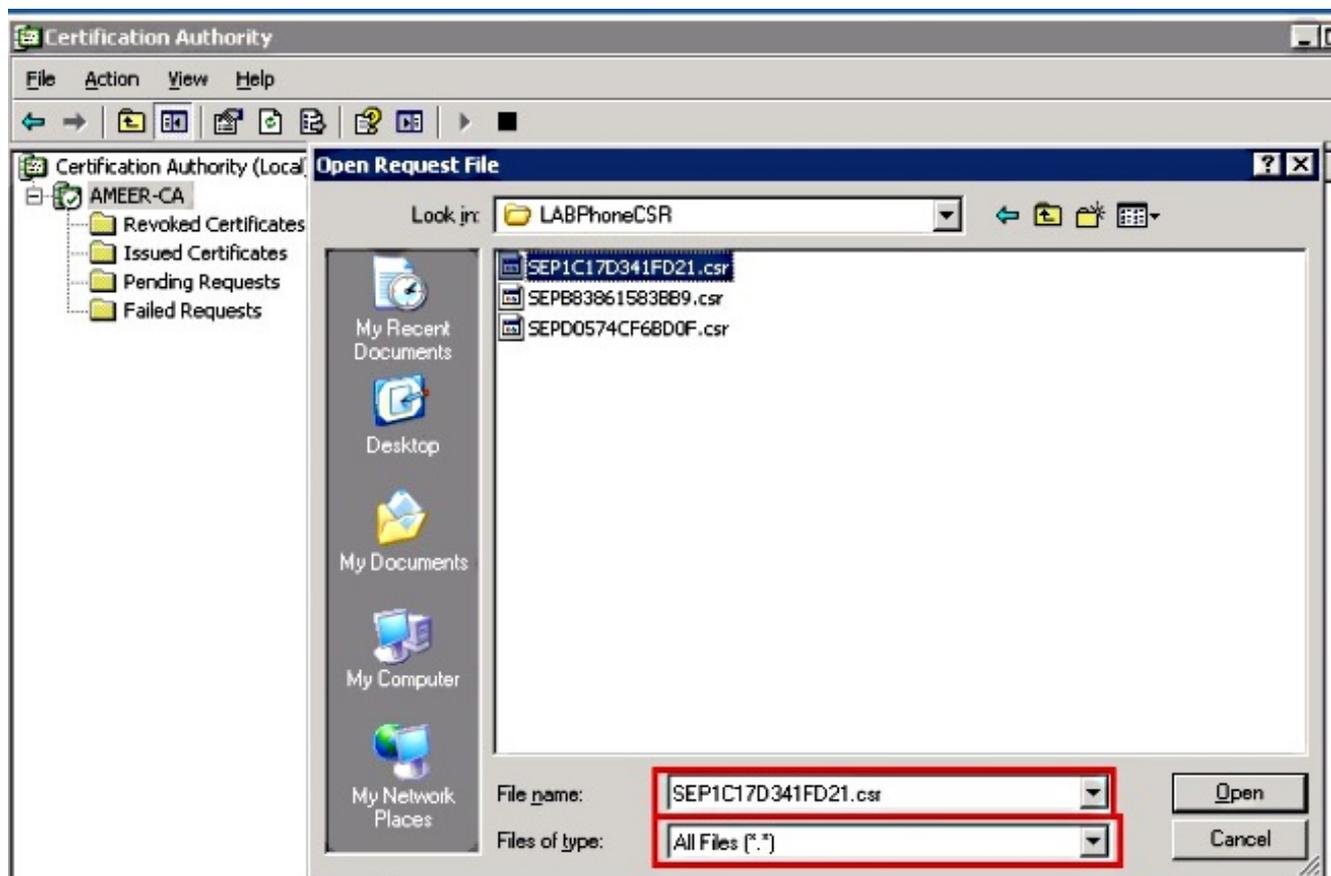
1. Autoridade de certificação aberta.



2. Clique com o botão direito do mouse na CA e navegue até **Todas as Tarefas > Enviar nova solicitação...**

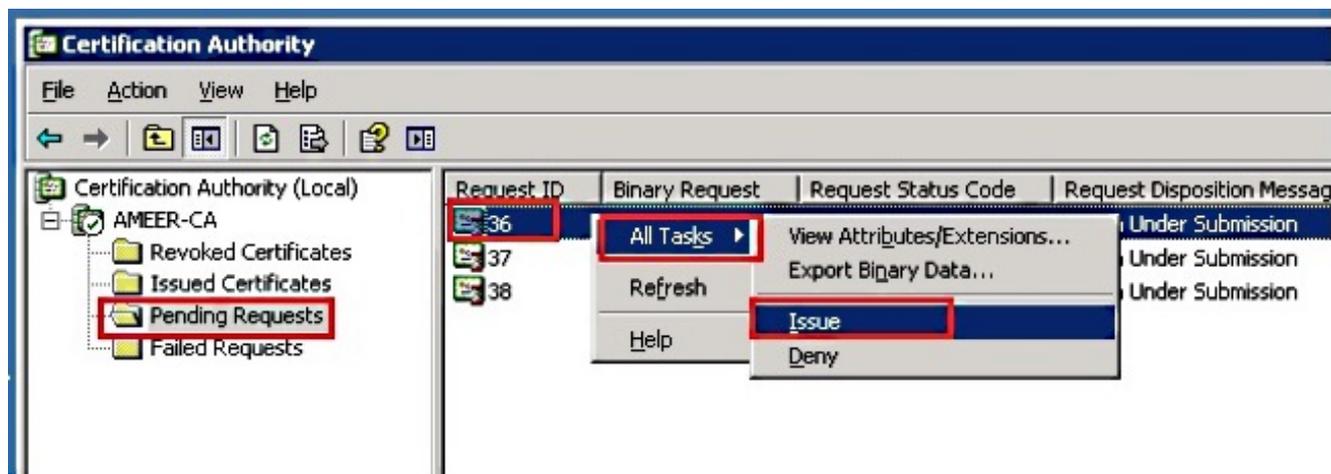


3. Selecione o CSR e clique em **Abrir**. Faça isso para todos os CSRs.



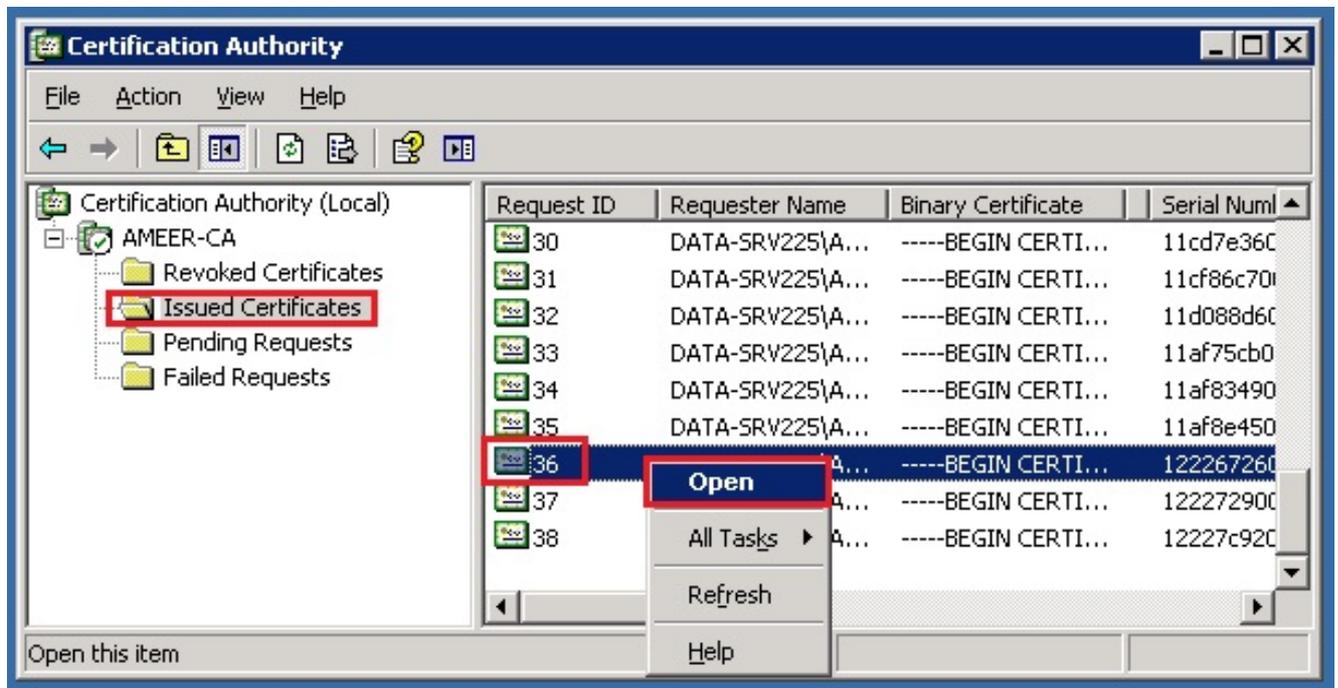
Todas as CSRs abertas são exibidas na pasta Solicitações pendentes.

4. Clique com o botão direito do mouse em cada um e navegue para **All Tasks > Issue** para emitir certificados. Faça isso para todas as solicitações pendentes.

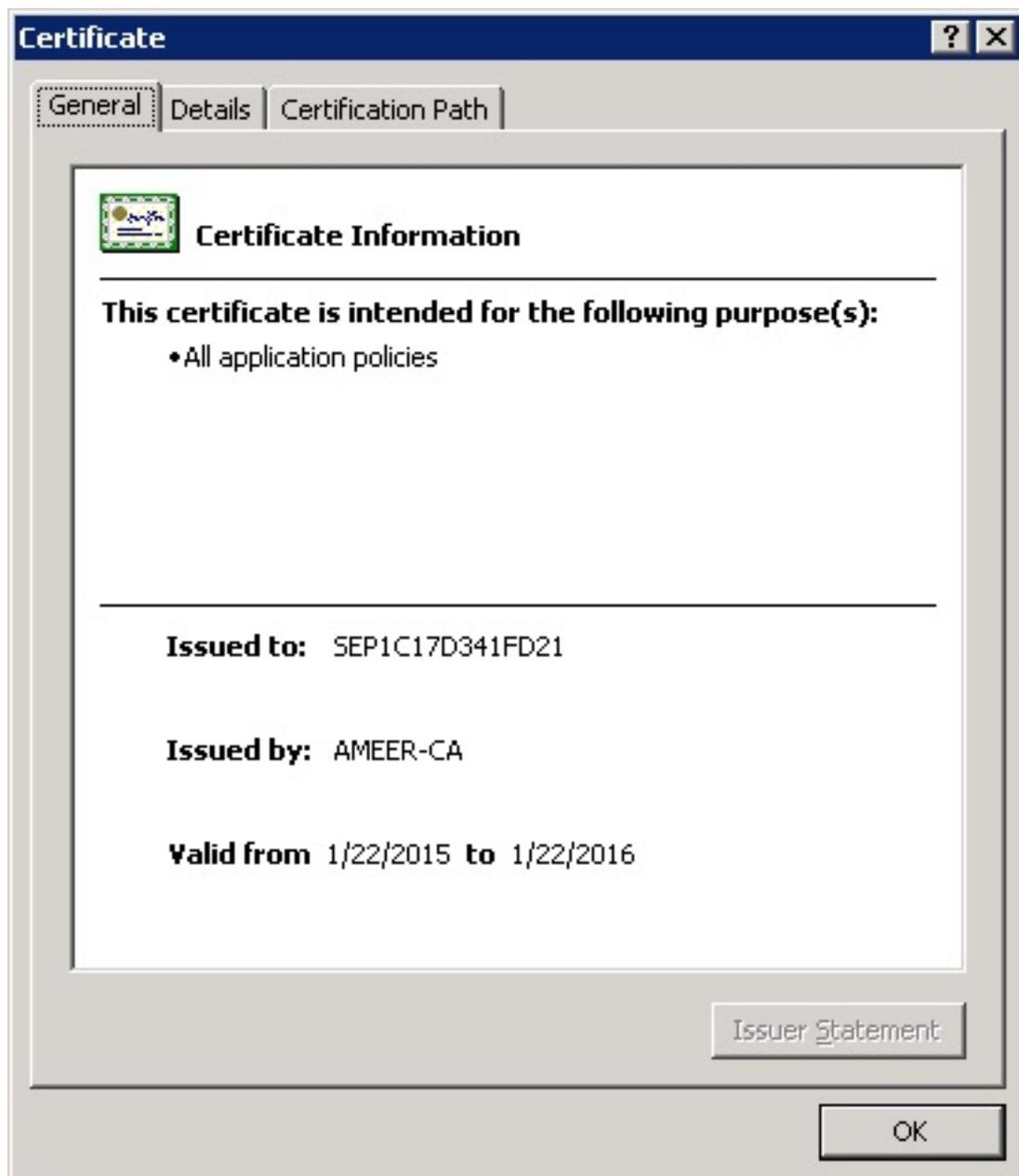


5. Para baixar o certificado, escolha **Issued Certificate**.

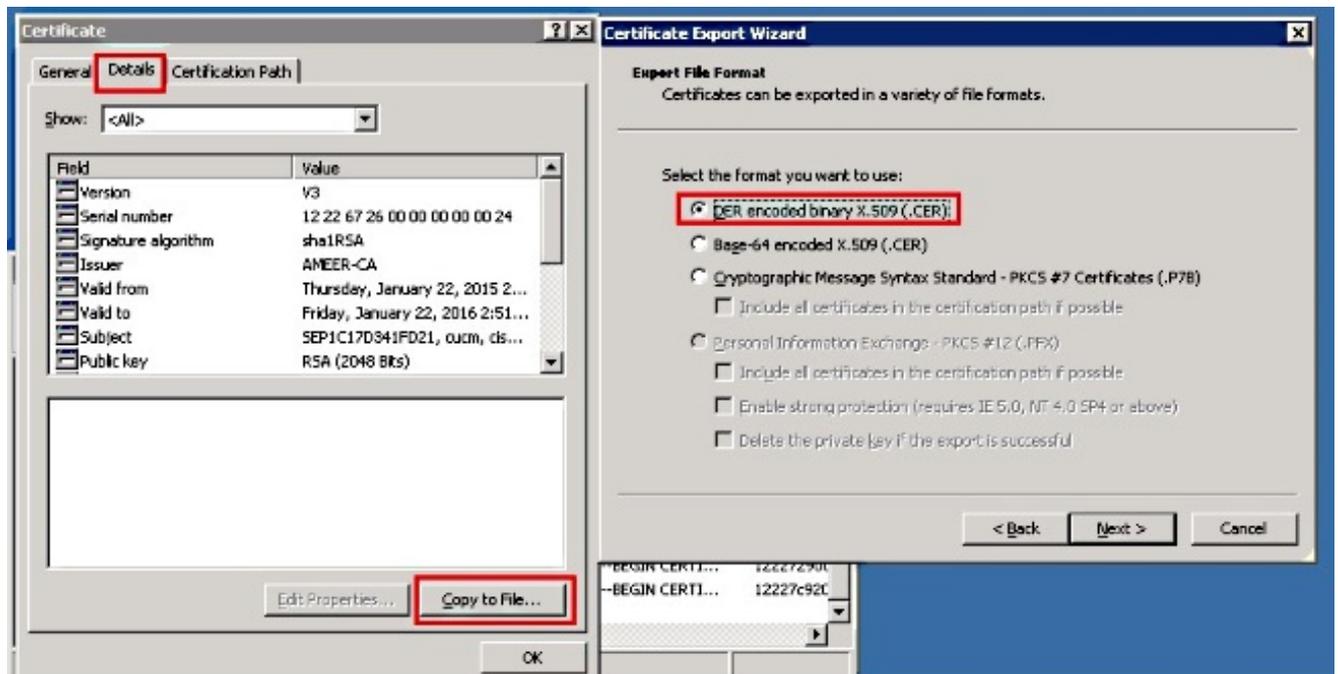
6. Clique com o botão direito do mouse no certificado e clique em **Abrir**.



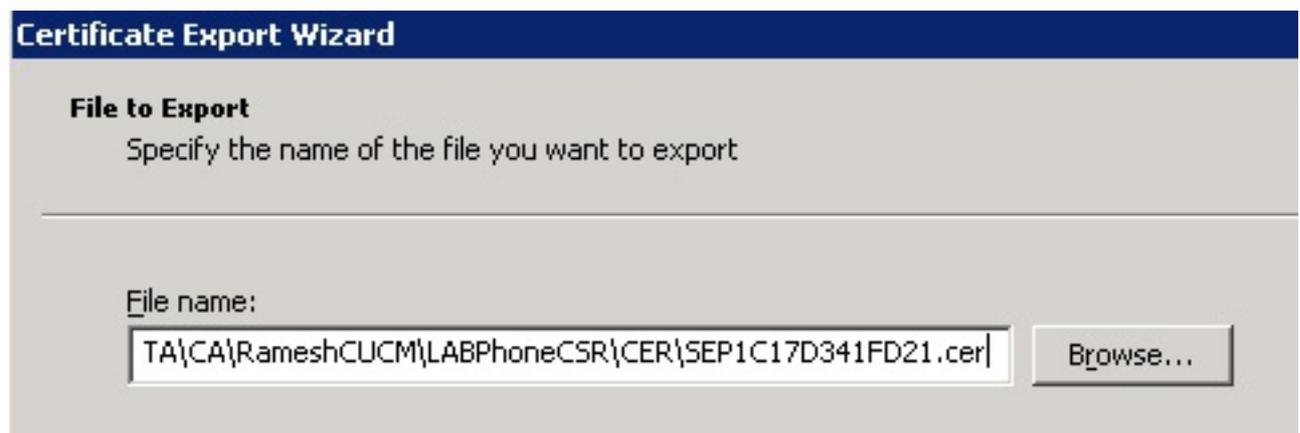
7. Você pode ver os detalhes do certificado. Para baixar o certificado, selecione a guia Details e escolha **Copy to File...**



8. No Assistente de Exportação de Certificado, escolha X.509 binário codificado por DER (.CER).



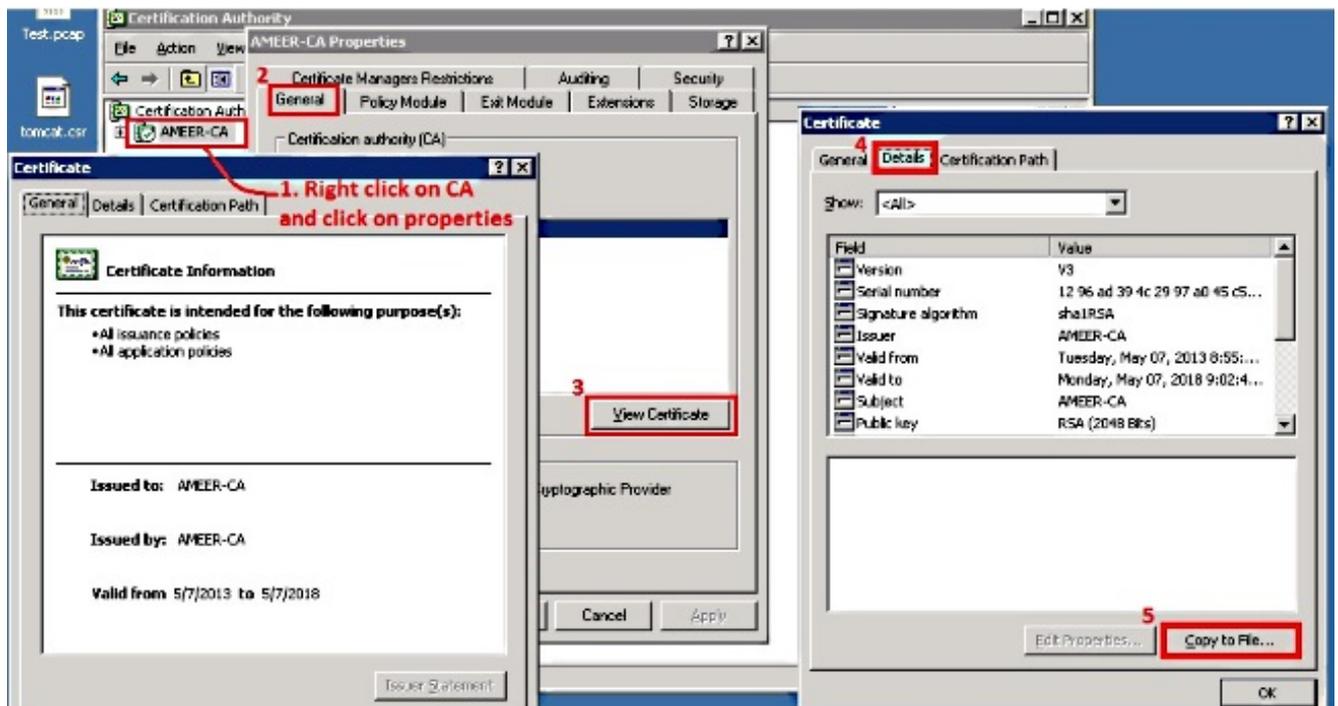
9. Dê um nome apropriado ao arquivo. Este exemplo usa o formato <MAC>.cer.



10. Obtenha os certificados para outros telefones na seção Emitido certificado com este procedimento.

## Obter o Certificado Raiz da CA

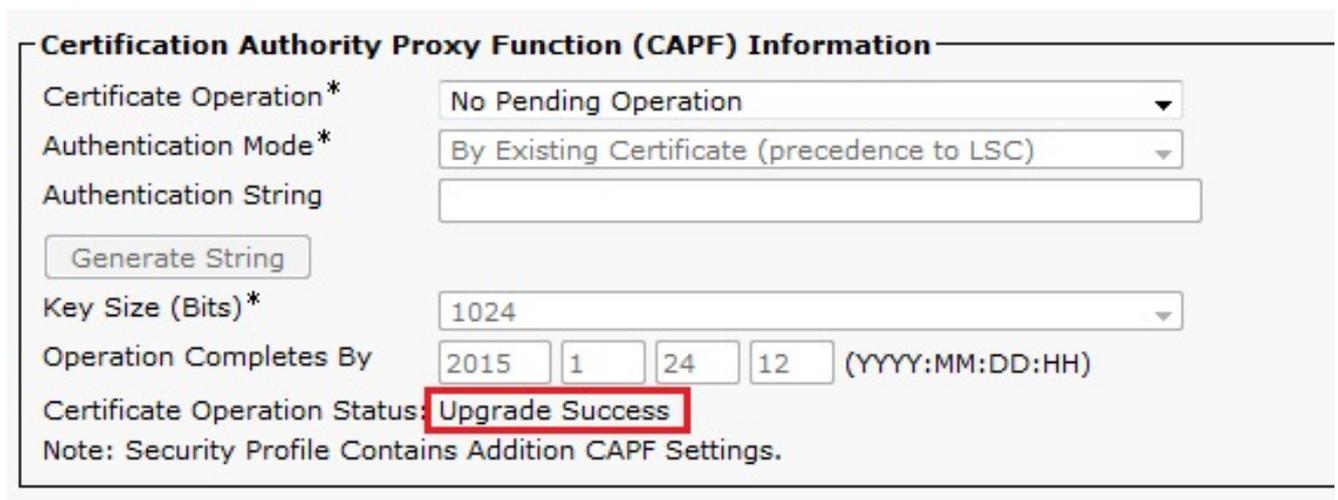
1. Abrir **Autoridade de Certificação**.
2. Conclua as etapas mostradas nesta captura de tela para fazer o download da AC raiz.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Vá para a página de configuração do telefone.
2. Na seção CAPF, o Certificate Operation Status deve ser exibido como **Upgrade Success**.



**Note:** Consulte [Gerar e importar LSCs assinados por CA de terceiros](#) para obter mais informações.

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.