

CUCM Third-Party CA-Signed LSCs Generation and Import Configuration Example

TAC

Document ID: 118779

Contributed by Ramesh Balakrishnan, Cisco TAC Engineer.
Mar 09, 2015

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Upload the CA-Root Certificate
- Set Offline CA for Certificate Issue to Endpoint
- Generate a Certificate Signing Request (CSR) for the Phones
- Get the Generated CSR from the CUCM to the FTP (or TFTP) Server
- Get the Phone Certificate
- Convert .cer to .der Format
- Compress the Certificates (.der) to .tgz Format
- Transfer the .tgz File to the SFTP Server
- Import the .tgz File to the CUCM Server
- Sign the CSR With Microsoft Windows 2003 Certificate Authority
- Get the Root Certificate from the CA

Verify

Troubleshoot

Introduction

Certificate Authority Proxy Function (CAPF) Locally Significant Certificates (LSCs) are locally-signed. However, you might require phones to use third-party Certificate Authority (CA)-signed LSCs. This document describes a procedure that helps you achieve this.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Unified Communication Manager (CUCM).

Components Used

The information in this document is based on CUCM Version 10.5(2); however, this feature works from Version 10.0 and later.

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.

Configure

Here are the steps involved in this procedure, each of which is detailed in its own section:

1. Upload the CA–Root Certificate
2. Set Offline CA for Certificate Issue to Endpoint
3. Generate a Certificate Signing Request (CSR) for the Phones
4. Get the Generated CSR from Cisco Unified Communications Manager (CUCM) to the FTP Server
5. Get the Phone Certificate from CA
6. Convert .cer to .der Format
7. Compress the Certificates (.der) to .tgz Format
8. Transfer the .tgz file to the Secure Shell FTP (SFTP) Server
9. Import the .tgz File to the CUCM Server
10. Sign the CSR With Microsoft Windows 2003 Certificate Authority
11. Get the Root Certificate from the CA

Upload the CA–Root Certificate

1. Log into the Cisco Unified Operating System (OS) Administration web GUI.
2. Navigate to *Security Certificate Management*.
3. Click *Upload Certificate/Certificate chain*.
4. Choose *CallManager–trust* under Certificate Purpose.
5. Browse to the CA's root certificate and click *Upload*.

The screenshot displays the Cisco Unified Operating System Administration web interface. The main title is "Cisco Unified Operating System Administration" with the Cisco logo. Below the title is a navigation menu with "Security" selected. The browser address bar shows "https://10.106.122.173/cmplatform/certificateUpload.do". The main content area is titled "Upload Certificate/Certificate chain" and contains a warning message: "Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster". Below the warning, there is a form with the following fields: "Certificate Purpose*" set to "CallManager-trust", "Description(friendly name)" (empty), and "Upload File" set to "AMEER-CA.cer". At the bottom of the form, there are "Upload" and "Close" buttons.

Set Offline CA for Certificate Issue to Endpoint

1. Log into the CUCM Administration web GUI.
2. Navigate to *System > Service Parameter*.
3. Choose the CUCM Server and select *Cisco Certificate Authority Proxy Function* for the Service.
4. Select *Offline CA* for Certificate Issue to Endpoint.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manag

Service Parameter Configuration

Save Set to Default

Status
Status: Ready

Select Server and Service

Server* 10.106.122.173--CUCM Voice/Video (Active) ▾
Service* Cisco Certificate Authority Proxy Function (Active) ▾

All parameters apply only to the current server except parameters that are in the cluster-wide group(s)

Cisco Certificate Authority Proxy Function (Active) Parameters on server 10.106.122.173--

Parameter Name	Parameter Value
Certificate Issuer to Endpoint *	Offline CA
Duration Of Certificate Validity	5
Key Size *	1024
Maximum Allowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *	3

Generate a Certificate Signing Request (CSR) for the Phones

1. Log into the CUCM Administration web GUI.
2. Navigate to *Device Phones*.
3. Choose the phone whose LSC must be signed by the external CA.
4. Change the Device security profile to a secured one (if not present, add one system on the Security Phone Security profile).
5. On the phone configuration page, under the CAPF section, choose *Install/Upgrade* for the Certification Operation. Complete this step for all of the phones whose LSC must be signed by the external CA. You should see *Operation Pending* for the Certificate Operation Status.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

BLF Presence Group*

Device Security Profile*

SUBSCRIBE Calling Search Space

Unattended Port

Require DTMF Reception

RFC2833 Disabled

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Size (Bits)*

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: Operation Pending

Note: Security Profile Contains Addition CAPF Settings.

Phone Security profile (7962 model).

Phone Security Profile Configuration

Status

Status: Ready

Phone Security Profile Information

Product Type: Cisco 7962

Device Protocol: SCCP

Name*

Description

Device Security Mode

TFTP Encrypted Config

Phone Security Profile CAPF Information

Authentication Mode*

Key Size (Bits)*

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

Enter the *utils capf csr count* command in the Secure Shell (SSH) session in order to confirm whether a CSR is generated. (This screen shot shows that a CSR was generated for three phones.)

```
admin:
admin:utils capf csr count

Count CSR/Certificate files.
Valid CSR   : 3
Invalid CSR : 0
Certificates: 0
```

Note: The Certificate Operation Status under the phone's CAPF section remains in the *Operation Pending* state.

Get the Generated CSR from the CUCM to the FTP (or TFTP) Server

1. SSH into the CUCM server.
2. Execute the *utils capf csr dump* command. This screen shot shows the dump being transferred to the FTP.

```
admin:
admin:utils capf csr dump

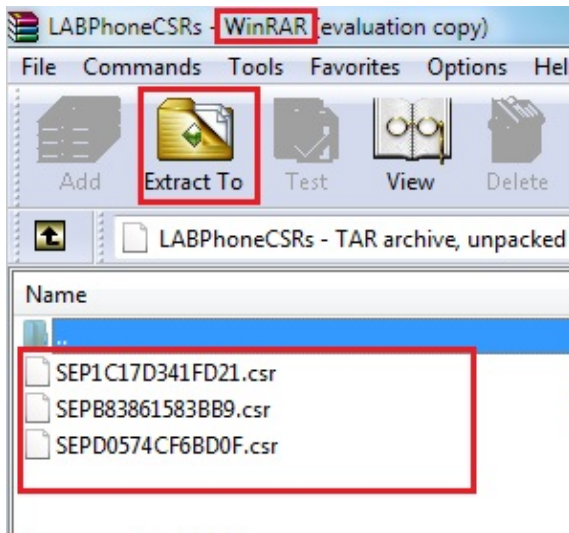
Dump CSR files.
CSR File tarred successfully...

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. Open the dump file with WinRAR and extract the CSR to your local machine.



Get the Phone Certificate

1. Send the phone's CSRs to the CA.
2. The CA provides you with a signed certificate.

Note: You can use a Microsoft Windows 2003 server as the CA. The procedure to sign the CSR with a Microsoft Windows 2003 CA is explained later in this document.

Convert .cer to .der Format

If the received certificates are in .cer format, then rename them to .der.

SEP0574CF6BD0F.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
SEP0574CF6BD0F.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

Compress the Certificates (.der) to .tgz Format

You can use CUCM server's root (Linux) in order to compress the certificate format. You can also do this in a normal Linux system.

1. Transfer all of the signed certificates to the Linux system with the SFTP server.

```
[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
/SEP1C17D341FD21.der                                100% 1087
Fetching /SEPB83861583BB9.der to SEPB83861583BB9.der
/SEPB83861583BB9.der                                100% 1095
Fetching /SEPD0574CF6BD0F.der to SEPD0574CF6BD0F.der
/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. Enter this command in order to compress all the .der certificates into a .tgz file.

```
tar -zcvf <file_name>.tgz *.der
```

```
[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]#
```

Transfer the .tgz File to the SFTP Server

Complete the steps shown in the screen shot in order to transfer the .tgz file to the SFTP server.

```
[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>
```

Import the .tgz File to the CUCM Server

1. SSH into the CUCM server.
2. Execute the *utils capf cert import* command.

```
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
```

Once the certificates are imported successfully, then you can see the CSR count become zero.

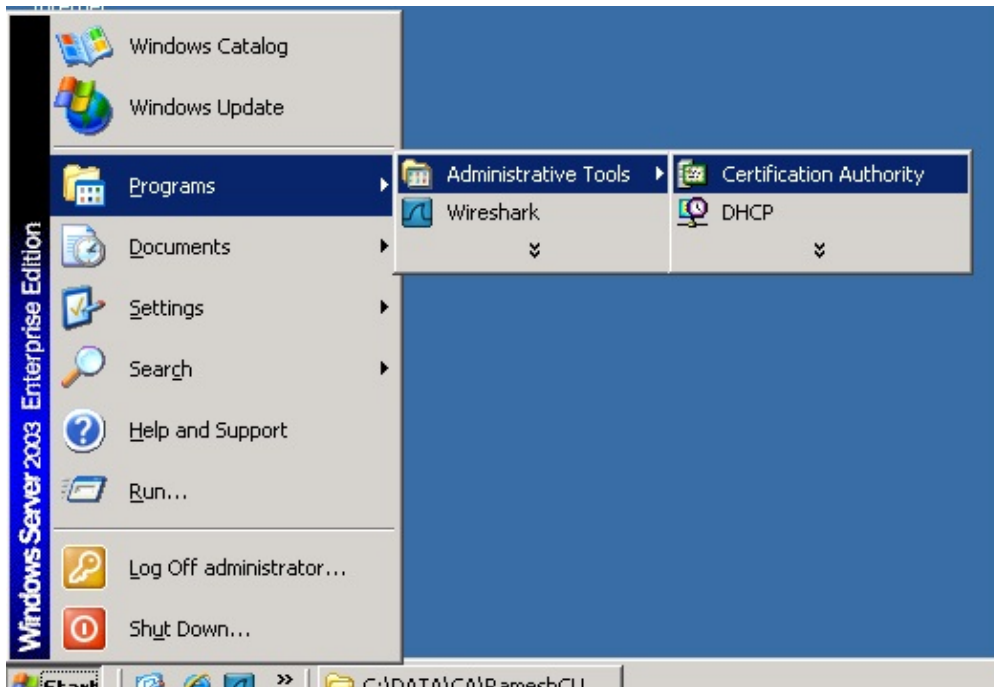
```
admin:
admin:utils capf csr count

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

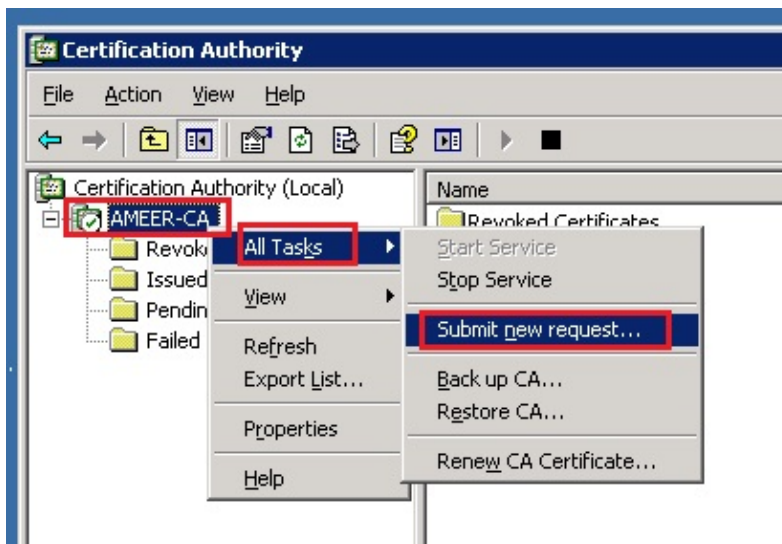
Sign the CSR With Microsoft Windows 2003 Certificate Authority

This is optional information for Microsoft Windows 2003 – CA.

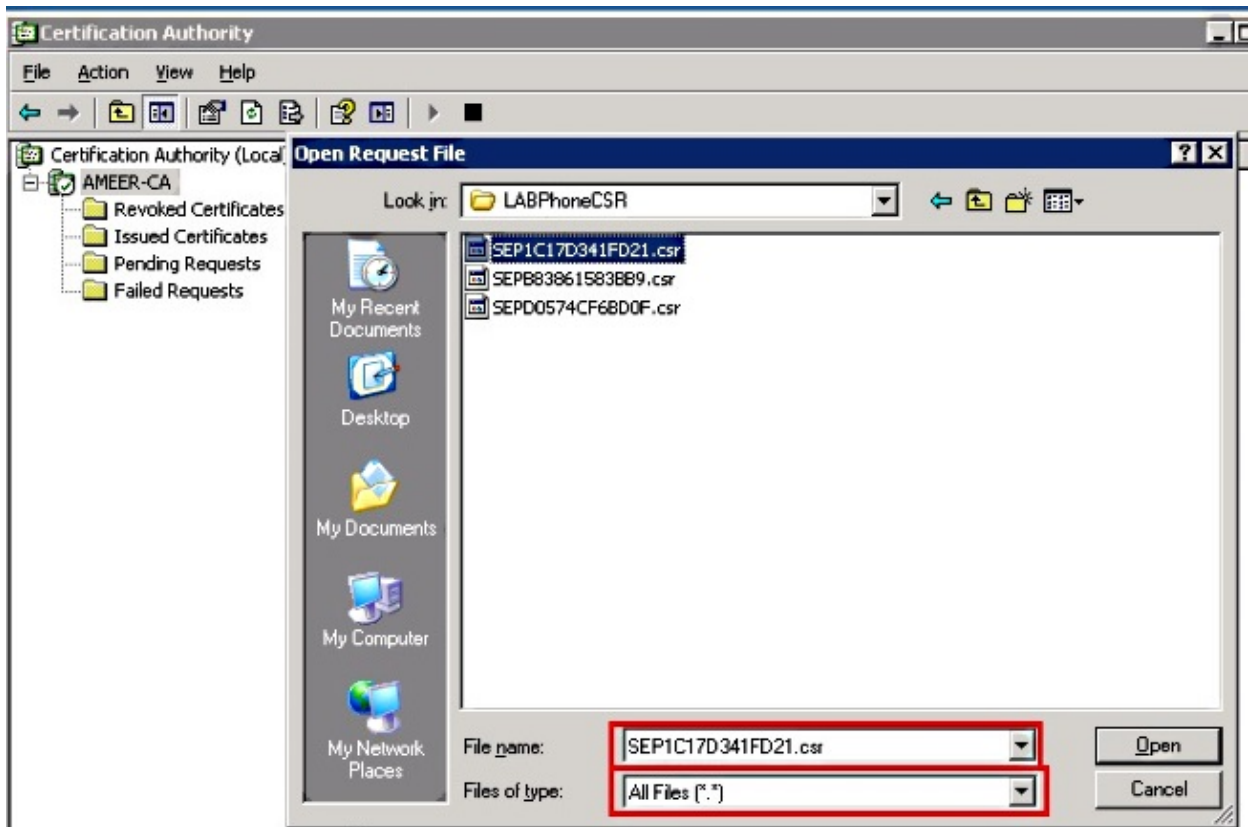
1. Open Certification Authority.



2. Right-click the CA and navigate to *All Tasks* > *Submit new request...*

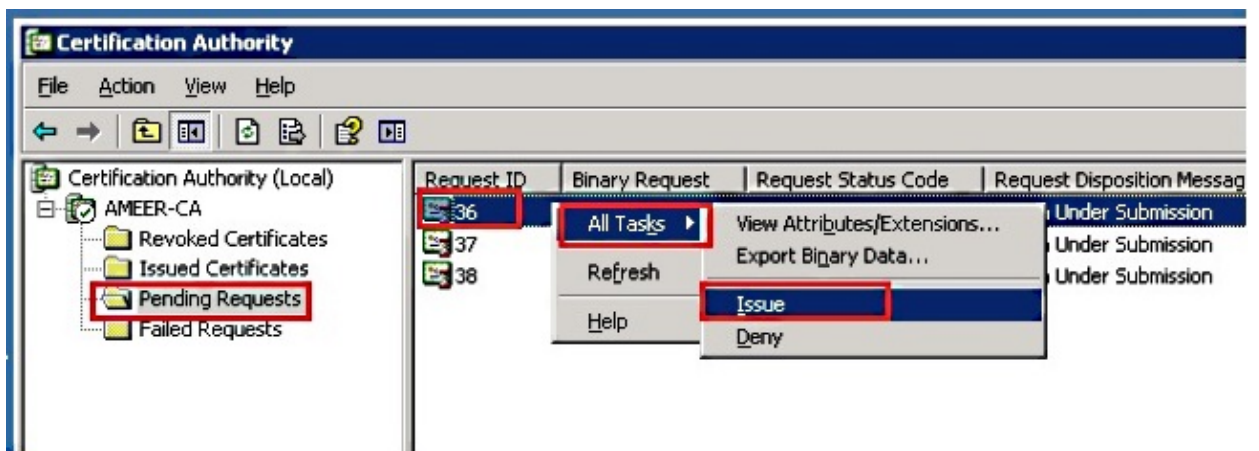


3. Select the CSR and click *Open*. Do this for all the CSRs.



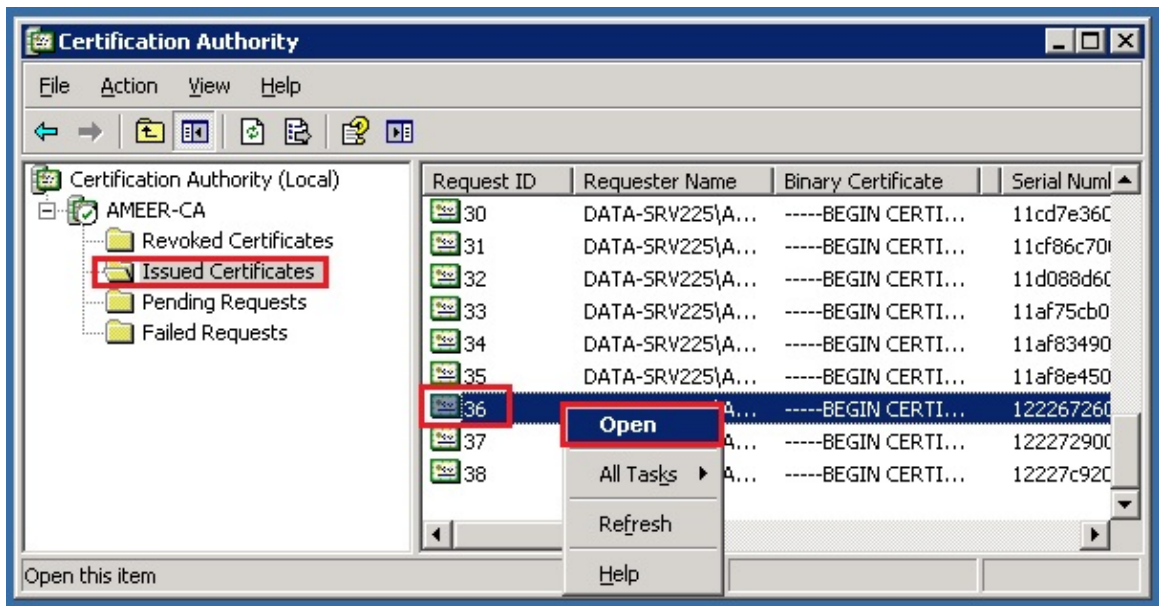
All of the opened CSR display in the Pending Requests folder.

- Right-click each and navigate to **All Tasks > Issue** in order to issue certificates. Do this for all pending requests.

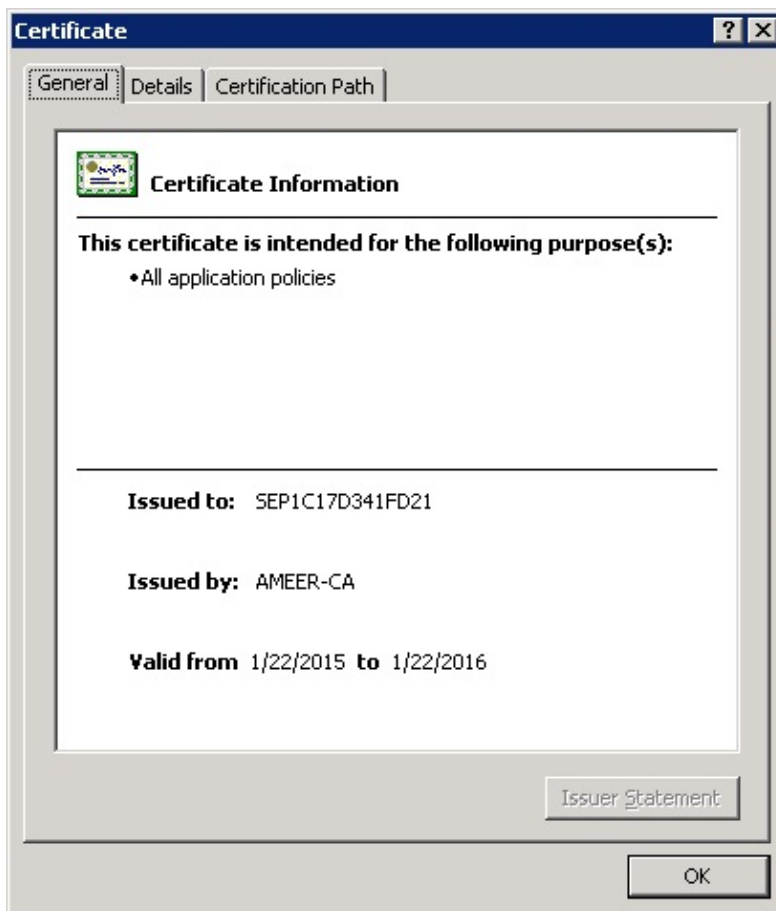


- In order to download the certificate, choose **Issued Certificate**.

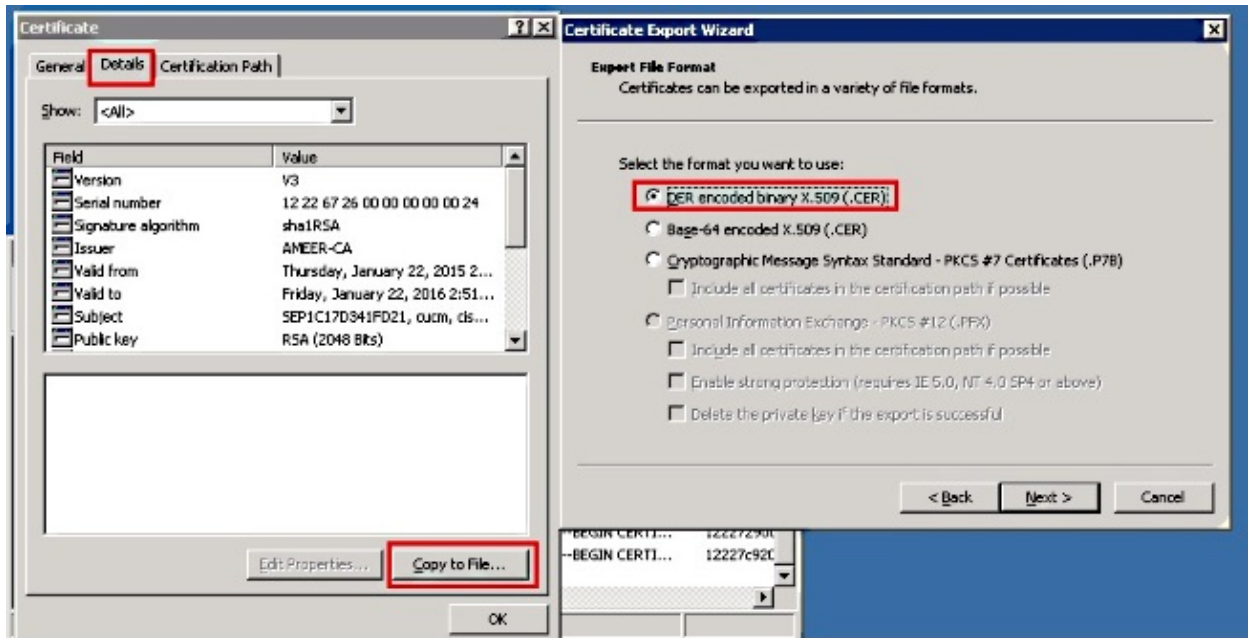
- Right-click the certificate and click **Open**.



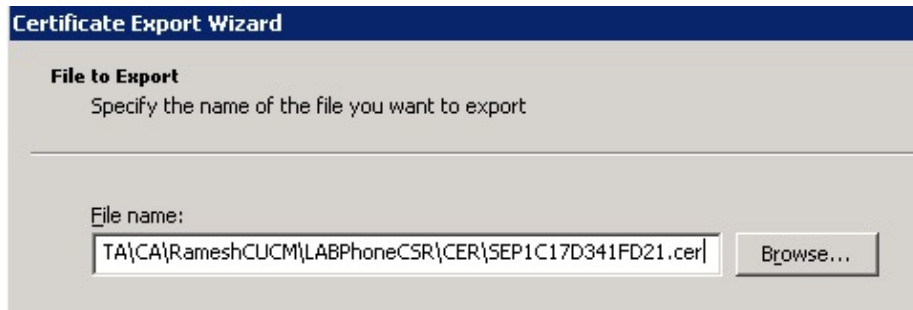
7. You can see the certificate details. In order to download the certificate, select the Details tab and choose *Copy to File...*



8. In the Certificate Export Wizard, choose **DER encoded binary X.509 (.CER)**.



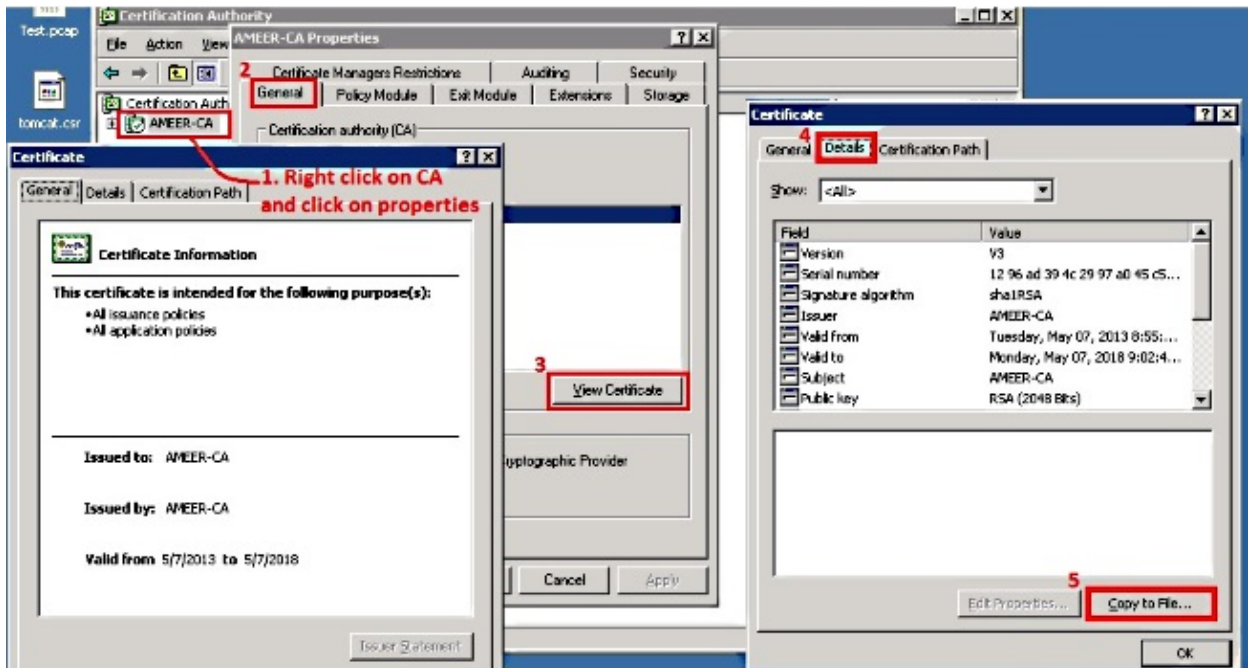
9. Name the file something appropriate. This example uses <MAC>.cer format.



10. Get the certificates for other phones under the Issued Certificate section with this procedure.

Get the Root Certificate from the CA

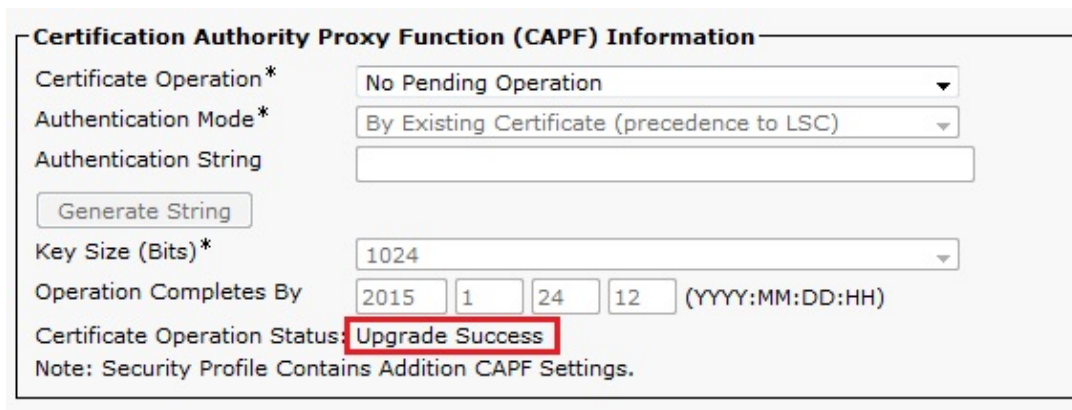
1. Open *Certification Authority*.
2. Complete the steps shown in this screen shot in order to download the root-CA.



Verify

Use this section in order to confirm that your configuration works properly.

1. Go to the phone configuration page.
2. Under the CAPF section, the Certificate Operation Status should display as *Upgrade Success*.



Note: Refer to Generate and Import Third Party CA–Signed LSCs for more information.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.