

عق ووم ل LSCs عاشن إو داريت س ال ا ني وكت ل ا ثم ثلاث ل ا فرط ل ا CA ل بق نم CUCM ل ل ع

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[التكوين](#)

[تحميل شهادة جذر المرجع المصدق](#)

[تعيين المرجع المصدق غير المتصل لإصدار الشهادة إلى نقطة النهاية](#)

[إنشاء طلب توقيع شهادة \(CSR\) للهواتف](#)

[الحصول على CSR الذي تم إنشاؤه من CUCM إلى خادم FTP \(أو TFTP\)](#)

[الحصول على شهادة الهاتف](#)

[تحويل cer. إلى der. تنسيق](#)

[اضغط الشهادات \(der.\) على تنسيق tgz](#)

[نقل ملف tgz إلى خادم SFTP](#)

[إستيراد ملف tgz إلى خادم CUCM](#)

[توقيع CSR مع مرجع شهادات Microsoft Windows 2003](#)

[الحصول على الشهادة الجذر من المرجع المصدق](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

المقدمة

يتم توقيع وظيفة وكيل المرجع المصدق (CAPF) الشهادات ذات الأهمية المحلية (LSCs) محليا. ومع ذلك، قد تحتاج إلى الهواتف لاستخدام قوائم التحكم في الوصول (LSCs) الموقعة من قبل جهة خارجية للحصول على شهادة (CA). يوضح هذا المستند إجراء يساعدك على تحقيق ذلك.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بمدير الاتصالات الموحدة (CUCM) من Cisco.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 10.5(2) من CUCM؛ ومع ذلك، تعمل هذه الميزة من الإصدار 10.0 والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

واليكم الخطوات التي ينطوي عليها هذا الإجراء، وكل منها مفصل في القسم الخاص به:

1. [تحميل شهادة جذر المرجع المصدق](#)
2. [تعيين المرجع المصدق غير المتصل لإصدار الشهادة إلى نقطة النهاية](#)
3. [إنشاء طلب توقيع شهادة \(CSR\) للهواتف](#)
4. [إحصل على CSR الذي تم إنشاؤه من CUCM \(Cisco Unified Communications Manager\) إلى خادم FTP](#)
5. [الحصول على شهادة الهاتف من CA](#)
6. [تحويل cer. إلى der. لتنسيق](#)
7. [إضغط الشهادات \(der.\) على تنسيق tgz](#)
8. [نقل ملف tgz. إلى خادم \(SFTP Secure Shell FTP\)](#)
9. [إستيراد ملف tgz. إلى خادم CUCM](#)
10. [توقيع CSR مع مرجع شهادات Microsoft Windows 2003](#)
11. [الحصول على الشهادة الجذر من المرجع المصدق](#)

تحميل شهادة جذر المرجع المصدق

1. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة بإدارة نظام التشغيل الموحد (OS) من Cisco.
2. انتقل إلى إدارة شهادات الأمان.
3. انقر على تحميل الشهادة/سلسلة الشهادات.
4. اختر CallManager-trust ضمن "غرض الشهادة".
5. استعرض للوصول إلى شهادة جذر CA وانقر فوق تحميل.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show ▾ Settings ▾ **Security** ▾ Software Upgrades ▾ Services ▾ Help ▾

Upload Certificate/Certificate chain - Mozilla Firefox

https://10.106.122.173/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust ▾

Description(friendly name)

Upload File Browse... AMEER-CA.cer

Upload Close

تعيين المرجع المصدق غير المتصل لإصدار الشهادة إلى نقطة النهاية

1. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة بإدارة CUCM.
2. انتقل إلى النظام > معلمة الخدمة.
3. أختار خادم CUCM وحدد وظيفة وكيل مرجع شهادات Cisco للخدمة.
4. حدد المرجع المصدق غير المتصل لإصدار الشهادة إلى نقطة النهاية.

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

إنشاء طلب توقيع شهادة (CSR) للهواتف

1. قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) الخاصة بإدارة CUCM.
2. انتقل إلى هواتف الأجهزة.
3. اختر الهاتف الذي يجب توقيع LSC الخاص به من قبل CA الخارجي.
4. قم بتغيير ملف تعريف أمان الجهاز إلى ملف تعريف آمن (إذا لم يكن موجوداً، أضف نظاماً واحداً في ملف تعريف أمان هاتف الأمان).
5. في صفحة تكوين الهاتف، ضمن قسم CAPF، اختر تثبيت/ترقية لعملية الاعتماد. أكمل هذه الخطوة لجميع الهواتف التي يجب توقيع LSC الخاصة بها من قبل CA الخارجي. يجب أن ترى العملية معلقة لحالة عملية الشهادة.

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.

ملف تعريف أمان الهاتف (طراز 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

أدخل الأمر `utils capf csr count` في جلسة عمل طبقة الأمان (SSH) لتأكيد ما إذا تم إنشاء CSR أم لا. (توضح لقطة الشاشة هذه أنه تم إنشاء CSR لثلاثة هواتف.)

```
admin:
admin: utils capf csr count

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

ملاحظة: تظل حالة عملية الشهادة ضمن قسم CAPF الخاص بالهاتف في حالة تعليق العملية.

الحصول على CSR الذي تم إنشاؤه من CUCM إلى خادم FTP (أو TFTP)

1. SSH في خادم CUCM.

2. قم بتنفيذ أمر `utils capf csr` تفريغ هذه الشاشة هذه التفريغ الذي يتم نقله إلى FTP.


```
admin:
admin:utils capf csr dump

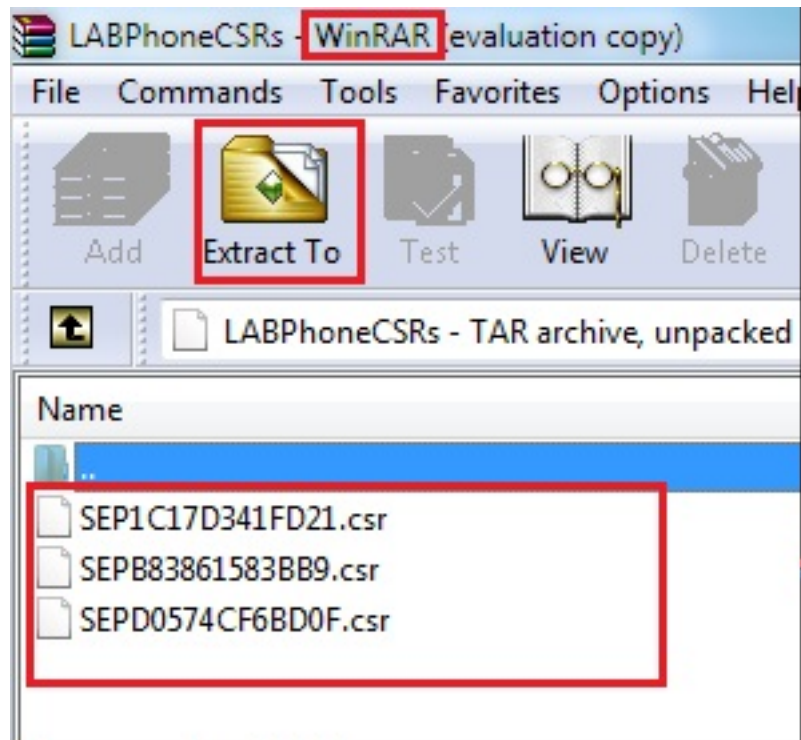
Dump CSR files.
CSR File tarred successfully...

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. افتح ملف التفريغ باستخدام WinRAR واستخرج CSR إلى جهازك المحلي.



الحصول على شهادة الهاتف

1. إرسال أوامر CSR الخاصة بالهاتف إلى CA.
2. يوفر لك المرجع المصدق شهادة موقعة.

ملاحظة: يمكنك استخدام خادم Microsoft Windows 2003 كمرجع مصدق. يتم شرح إجراء توقيع CSR باستخدام Microsoft Windows 2003 CA لاحقا في هذا المستند.

تحويل cer. إلى der. تنسيق

إذا كانت الشهادات المستلمة بتنسيق cer، فأعد تسميتها إلى 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

اضغط الشهادات (der.) على تنسيق tgz

يمكنك استخدام جذر خادم Linux (CUCM) لضغط تنسيق الشهادة. يمكنك أيضا القيام بذلك في نظام لينوكس عادي.

قم بنقل جميع الشهادات الموقعة إلى نظام Linux باستخدام خادم SFTP. 1.

```
[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
[root@cm1052 download]#
```

أدخل هذا الأمر لضغط كل شهادات der. في ملف tgz. 2.

```
tar -zcvf
```



```
[root@cm1052 download]#
[root@cm1052 download]# tar -zcvf phoneDER.tgz *.der
SEPIC17D341FD21.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    SEPIC17D341FD21.der  SEPD0574CF6BD0F.der
[root@cm1052 download]#
```

نقل ملف .tgz إلى خادم SFTP

أكمل الخطوات الموضحة في لقطة الشاشة لنقل ملف .tgz إلى خادم 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>
```

إستيراد ملف .tgz إلى خادم CUCM

.1

SSH في خادم CUCM.

.2. قم بتنفيذ أمر إستيراد شهادة CAPF من الولايات.

```
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
```

بمجرد إستيراد الشهادات بنجاح، يمكنك رؤية عدد CSR يصبح صفر.

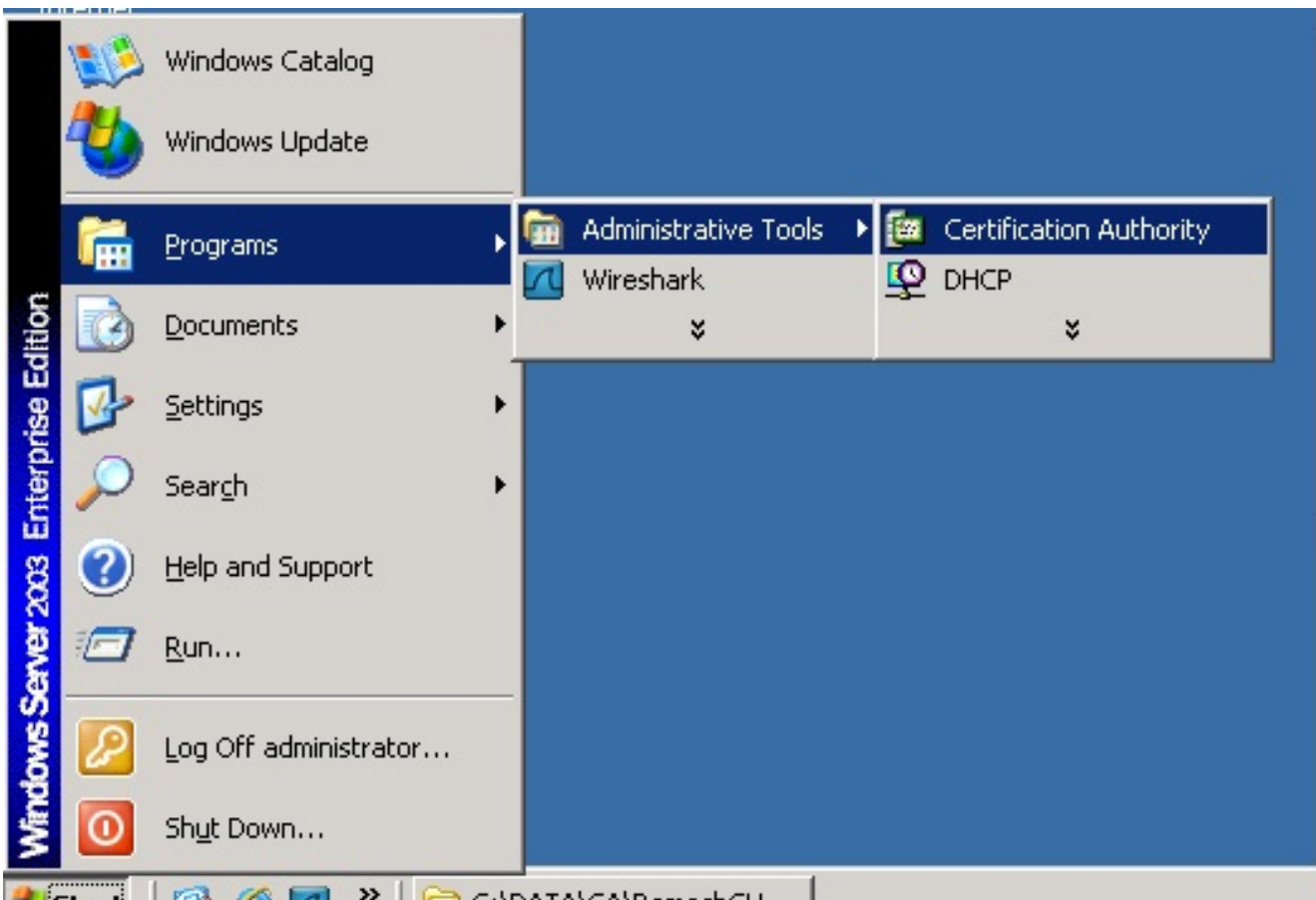
```
admin:
admin:utils capf csr count

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

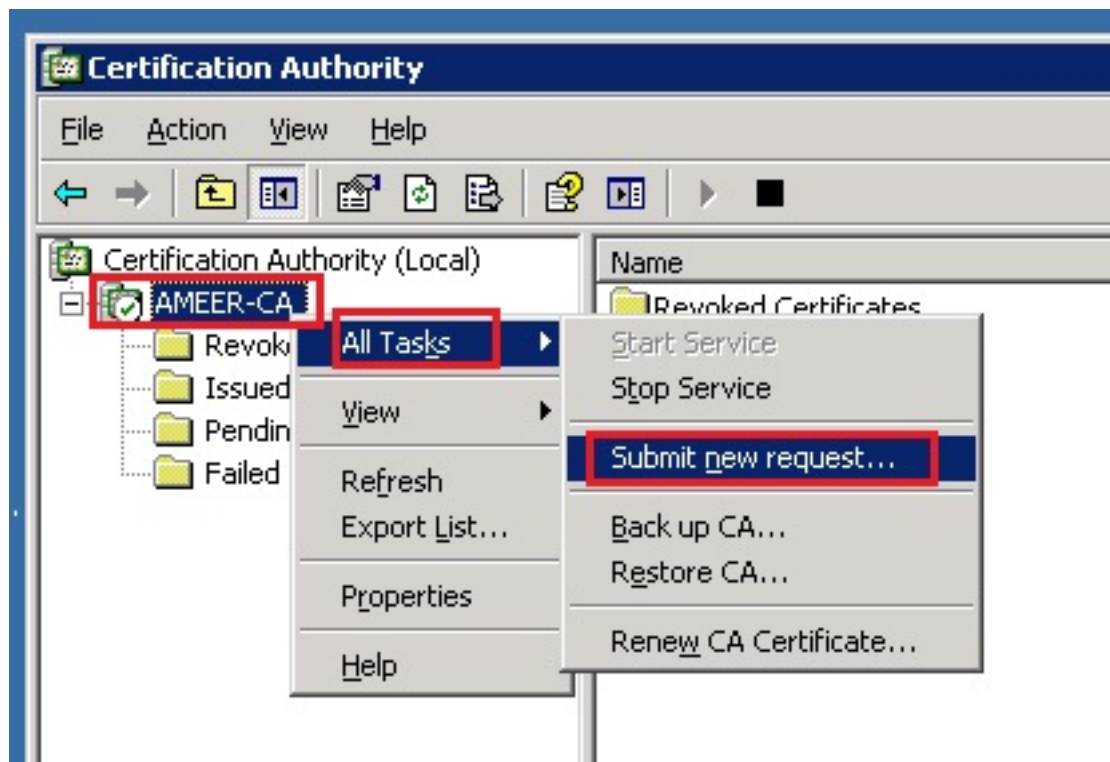
توقيع CSR مع مرجع شهادات Microsoft Windows 2003

هذه معلومات إختيارية لنظام CA - Microsoft Windows 2003.

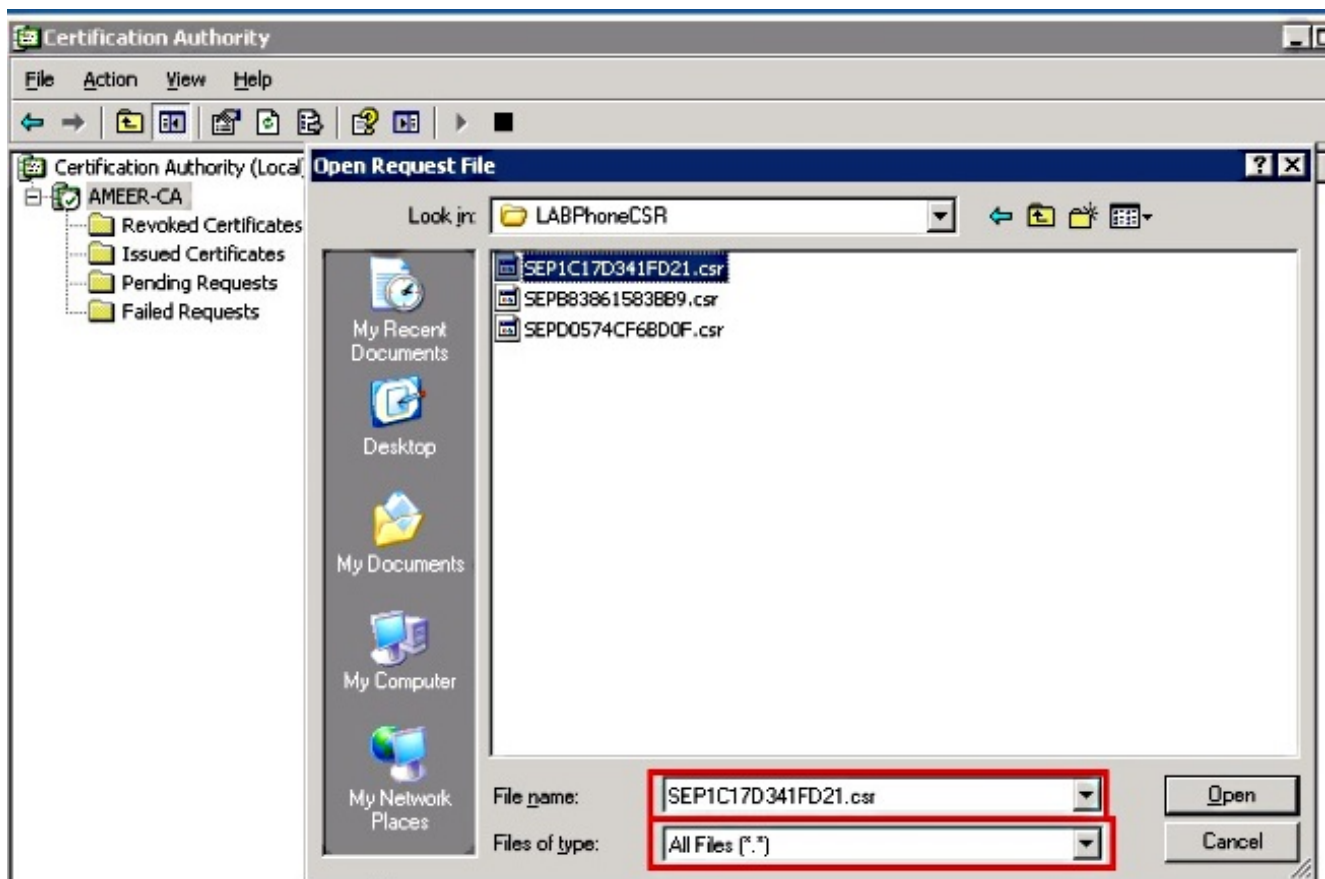
1. فتح المرجع المصدق.



2. انقر بزر الماوس الأيمن فوق CA وانتقل إلى كافة المهام < إرسال طلب جديد...

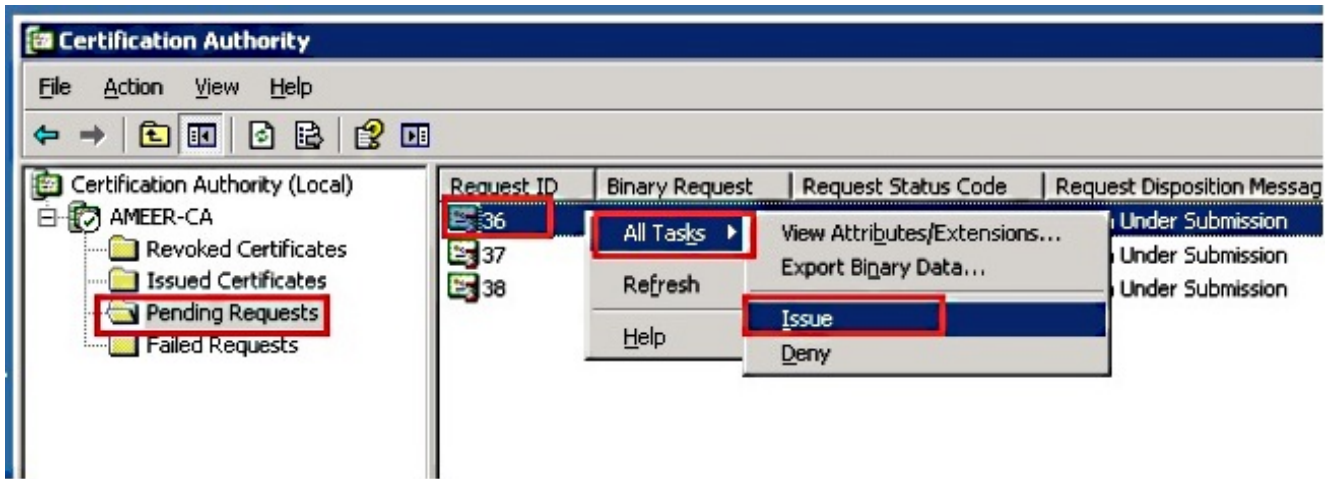


3. حدد CSR وانقر فوق فتح. قم بذلك لجميع لـ CSRs.



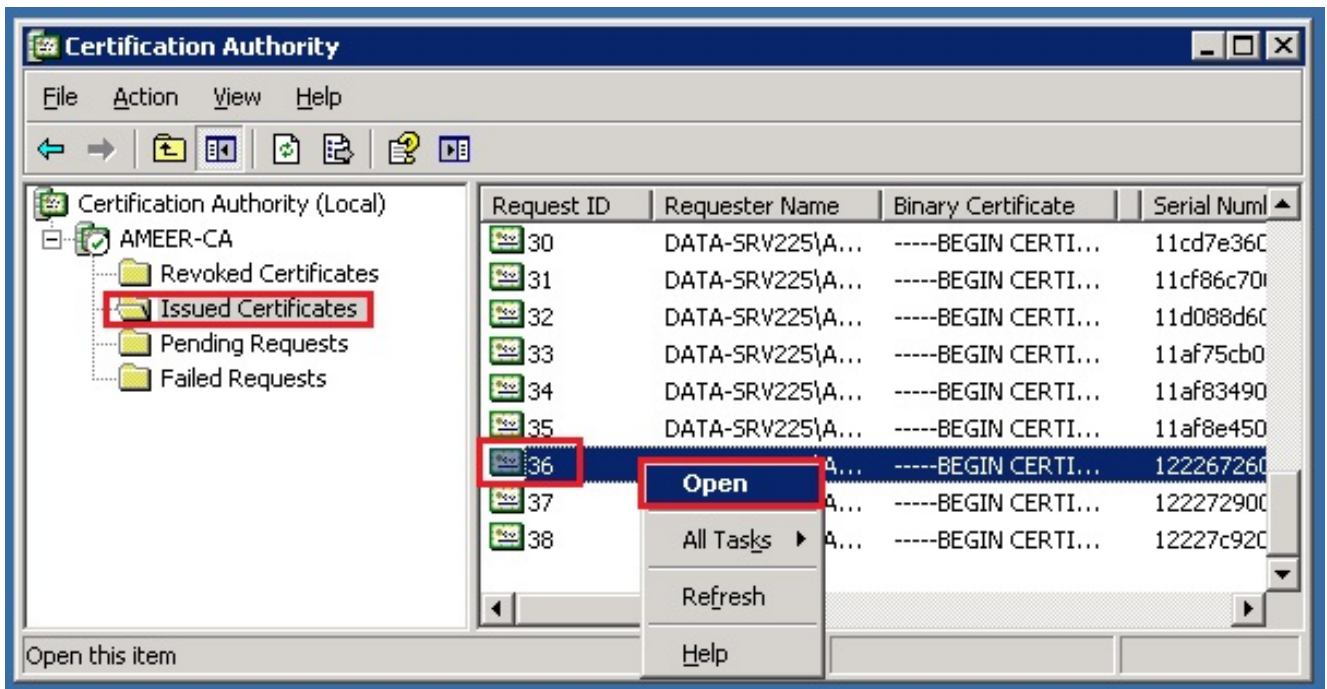
كافة عروض CSR المفتوحة في المجلد طلبات معلقة.

4. انقر بزر الماوس الأيمن على كل وتصفح إلى كل المهام < إصدار لإصدار الشهادات. قم بذلك لكافة الطلبات المعلقة.

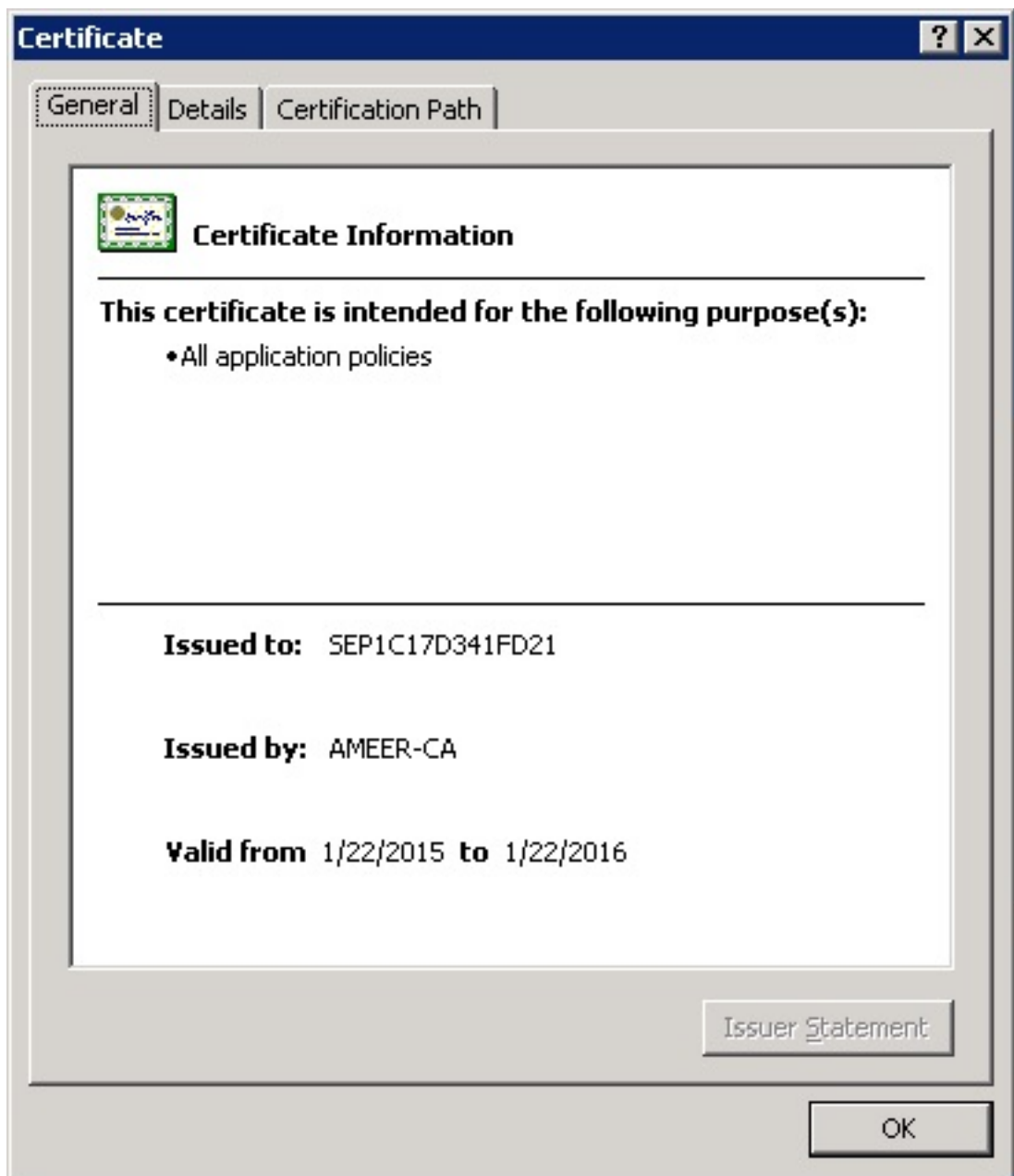


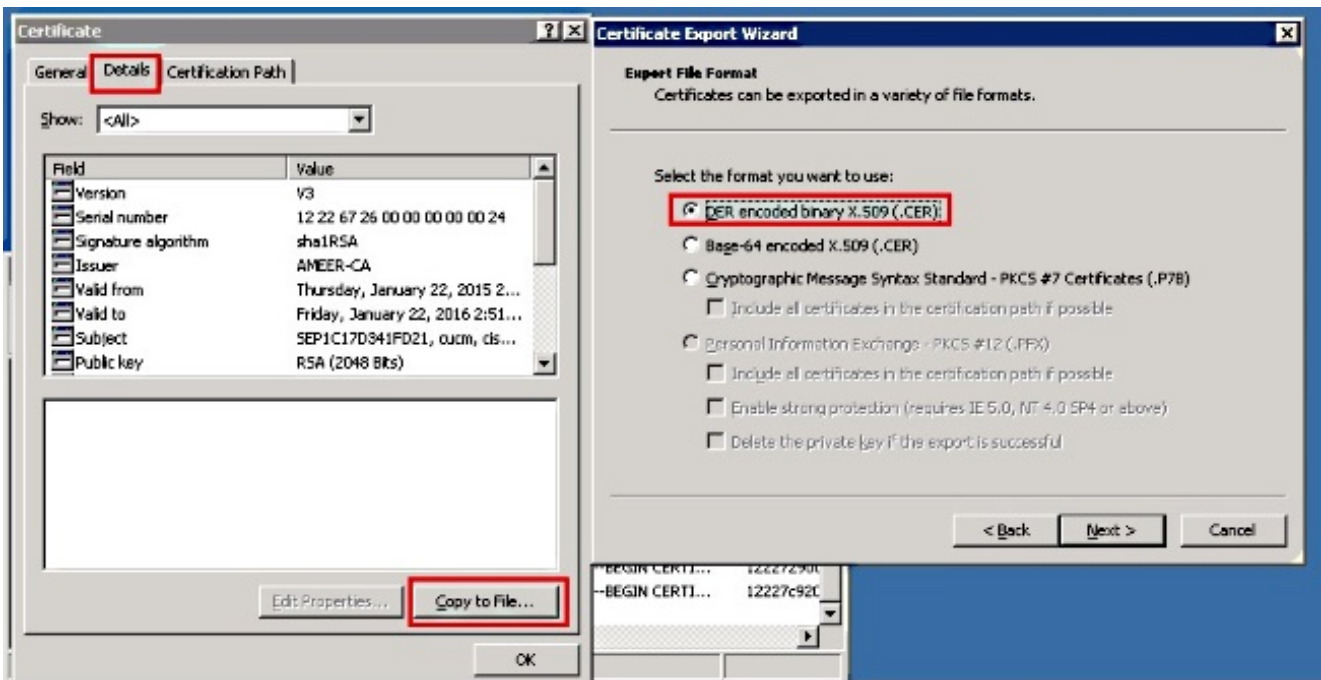
5. اخترت in order to جلبت الشهادة، يصدر شهادة.

6. انقر بزر الماوس الأيمن فوق الشهادة وانقر فوق فتح.

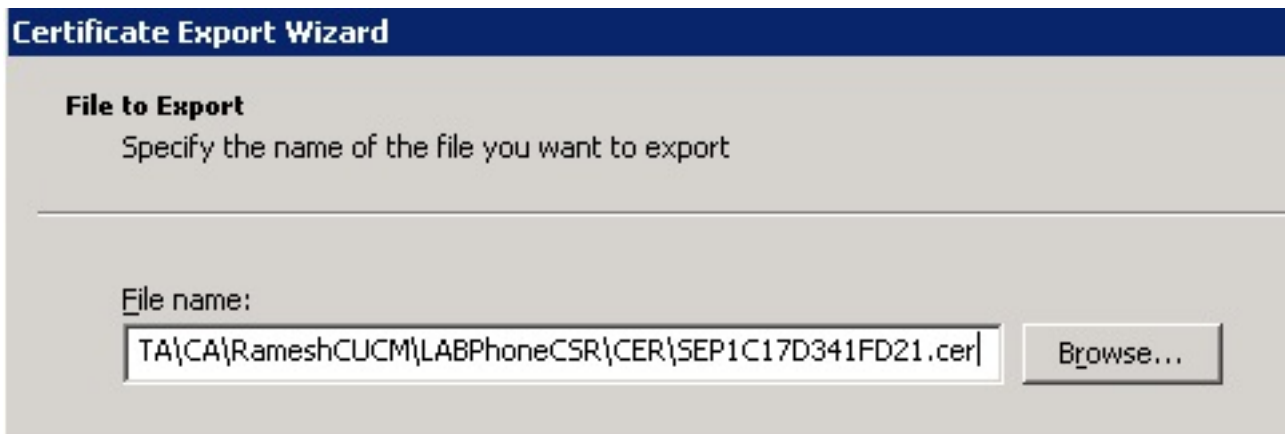


7. يمكنك رؤية تفاصيل الشهادة. لتنزيل الشهادة، حدد علامة التبويب تفاصيل واختار نسخ إلى ملف...





9. قم بتسمية الملف بشيء مناسب. يستخدم هذا المثال تنسيق <MAC>.cer.

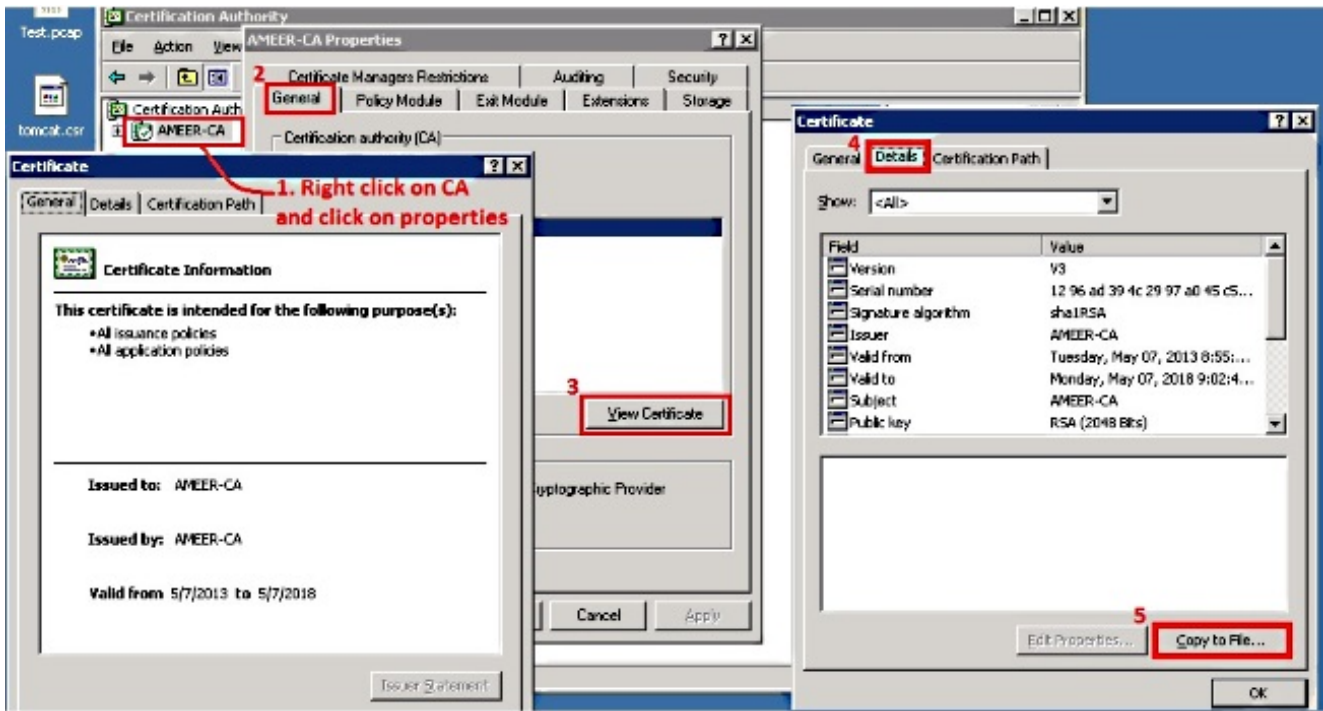


10. الحصول على الشهادات للهواتف الأخرى تحت قسم الترخيص الصادر مع هذا الإجراء.

الحصول على الشهادة الجذر من المرجع المصدق

1. فتح المرجع المصدق.

2. أكمل الخطوات الموضحة في لقطة الشاشة هذه من أجل تنزيل المرجع المصدق الجذر.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

انتقل إلى صفحة تكوين الهاتف.

.1

2. تحت قسم CAPF، يجب أن تعرض حالة عملية الشهادة على أنها نجاح الترقية.

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: Upgrade Success

Note: Security Profile Contains Addition CAPF Settings.

ملاحظة: راجع إنشاء واستيراد قوائم التحكم في الوصول (LSCs) الموقعة من قبل جهة خارجية للحصول على مزيد من المعلومات.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل