Esempio di generazione e importazione di schede LCS con firma CA di terze parti per CUCM

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Carica il certificato radice CA](#)
[Imposta CA offline per il rilascio del certificato su Endpoint](#)
[Genera una richiesta di firma del certificato (CSR) per i telefoni](#)
[Recuperare il CSR generato da CUCM sul server FTP (o TFTP)](#)
[Ottieni certificato telefonico](#)
[Converti formato cer in der](#)
[Comprimi il formato dei certificati (.der) in .tgz](#)
[Trasferire il file .tgz sul server SFTP](#)
[Importare il file .tgz sul server CUCM](#)
[Firmare il CSR con Microsoft Windows 2003 Certificate Authority](#)
[Ottieni certificato radice dalla CA](#)
[Verifica](#)
[Risoluzione dei problemi](#)

Introduzione

I certificati LSC (Certification Authority Proxy Function) rilevanti a livello locale sono firmati a livello locale. Tuttavia, potrebbe essere necessario che i telefoni utilizzino schede LSC firmate da un'autorità di certificazione (CA) di terze parti. In questo documento viene descritta una procedura che consente di ottenere questo risultato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Unified Communications Manager (CUCM).

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 10.5(2) di CUCM; tuttavia, questa funzione è operativa dalla versione 10.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Di seguito sono riportati i passaggi della procedura, descritti in dettaglio nella relativa sezione:

1. Carica il certificato radice CA
2. Imposta CA offline per il rilascio del certificato su Endpoint
3. Genera una richiesta di firma del certificato (CSR) per i telefoni
4. Scarica il CSR generato da Cisco Unified Communications Manager (CUCM) sul server FTP
5. Ottieni certificato telefonico da CA
6. Converti formato cer in der
7. Comprimi il formato dei certificati (.der) in .tgz
8. Trasferire il file .tgz sul server FTP Secure Shell (SFTP)
9. Importare il file .tgz sul server CUCM
10. Firmare il CSR con Microsoft Windows 2003 Certificate Authority
11. Ottieni certificato radice dalla CA

Carica il certificato radice CA

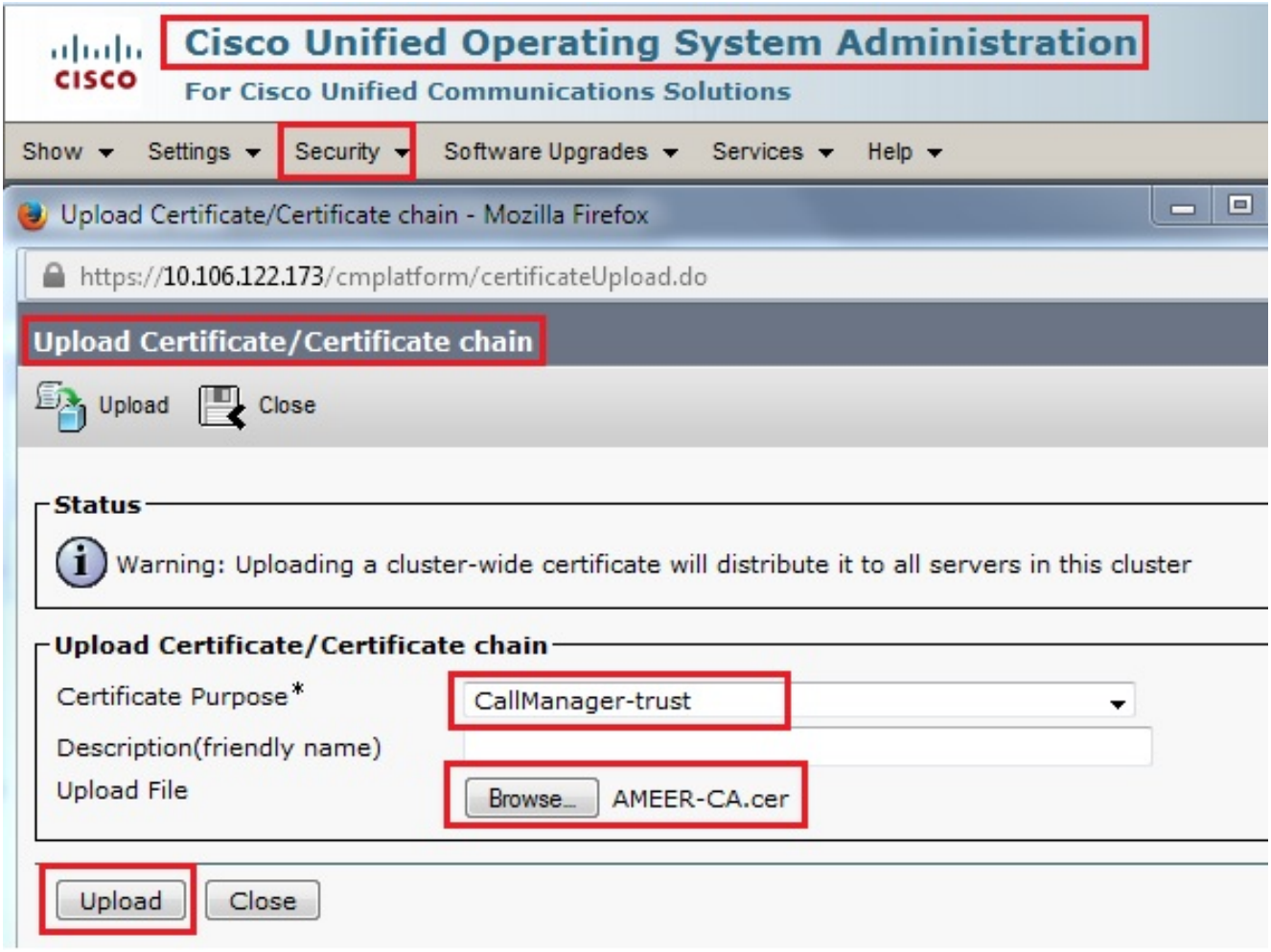
1. Accedere alla GUI Web di amministrazione del sistema operativo unificato Cisco.

2. Passare a **Gestione certificati di sicurezza**.

3. Fare clic su **Carica catena certificati/certificati**.

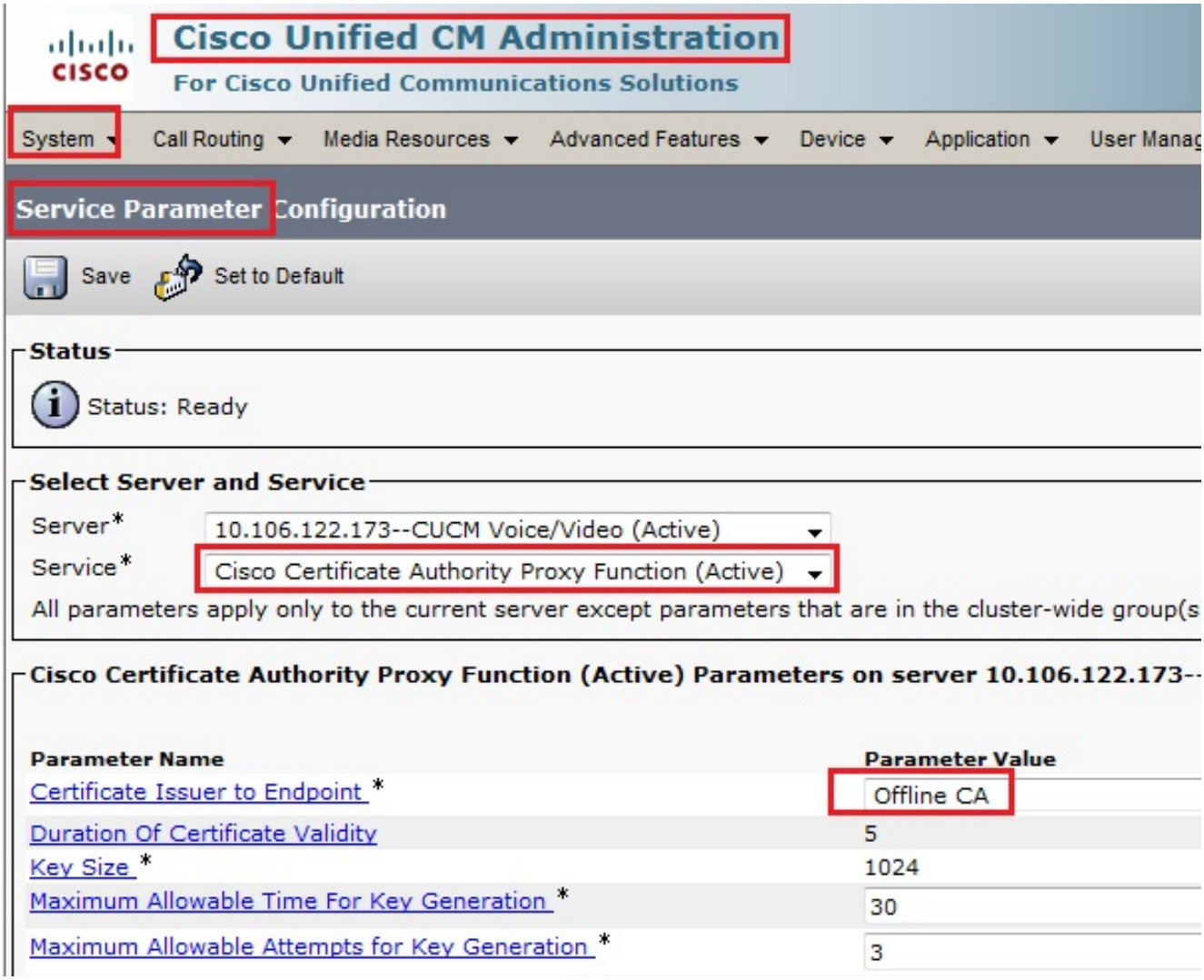
4. Scegliere **CallManager-trust** in Scopo certificato.

5. Individuare il certificato radice della CA e fare clic su **Upload**.



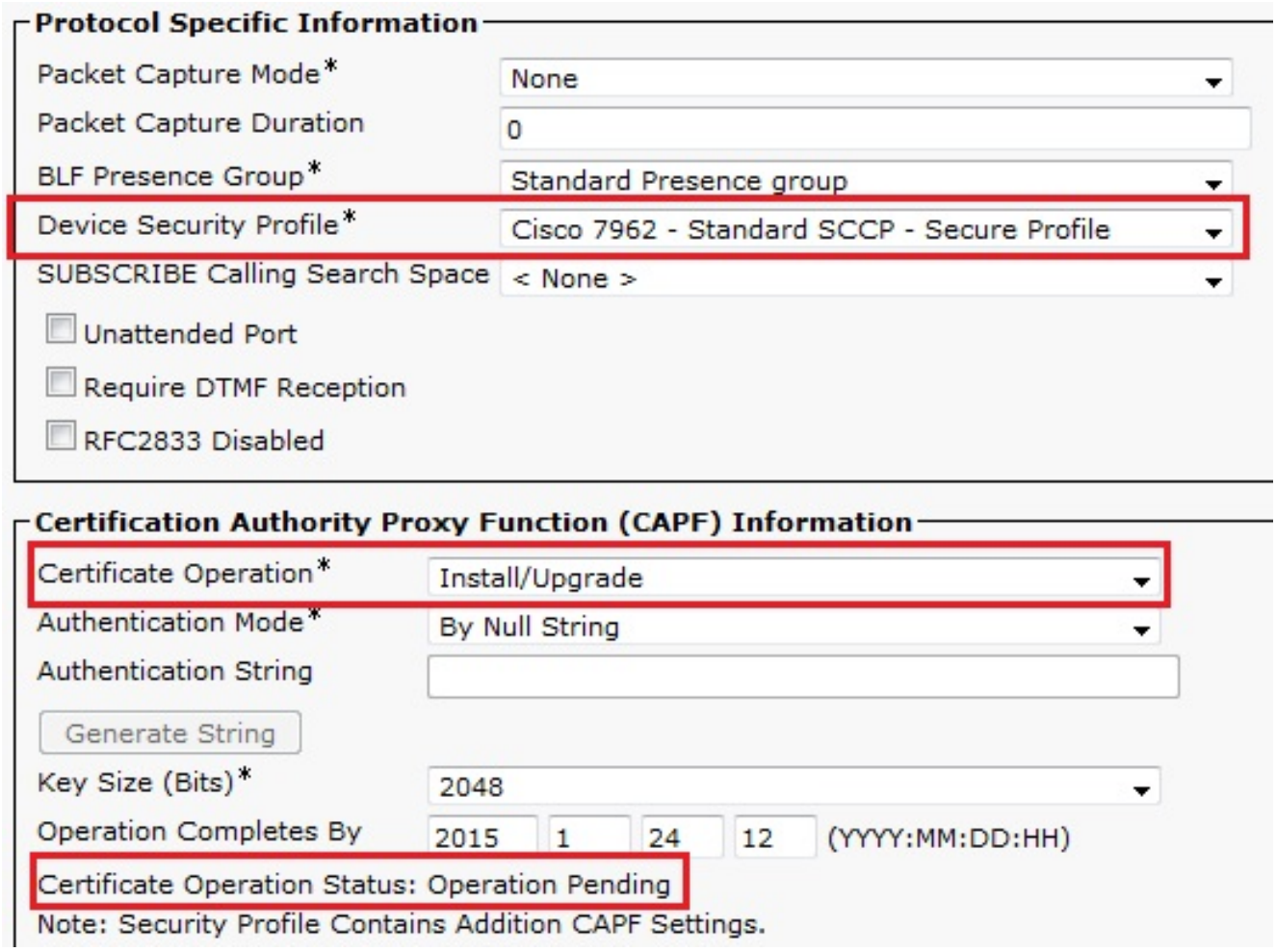
Imposta CA offline per il rilascio del certificato su Endpoint

1. Accedere alla GUI Web di amministrazione CUCM.
2. Passare a **Sistema > Parametro servizio**.
3. Scegliere il server CUCM e selezionare **Funzione proxy Cisco Certificate Authority** per il servizio.
4. Selezionare **CA offline** per Rilascio certificato a endpoint.

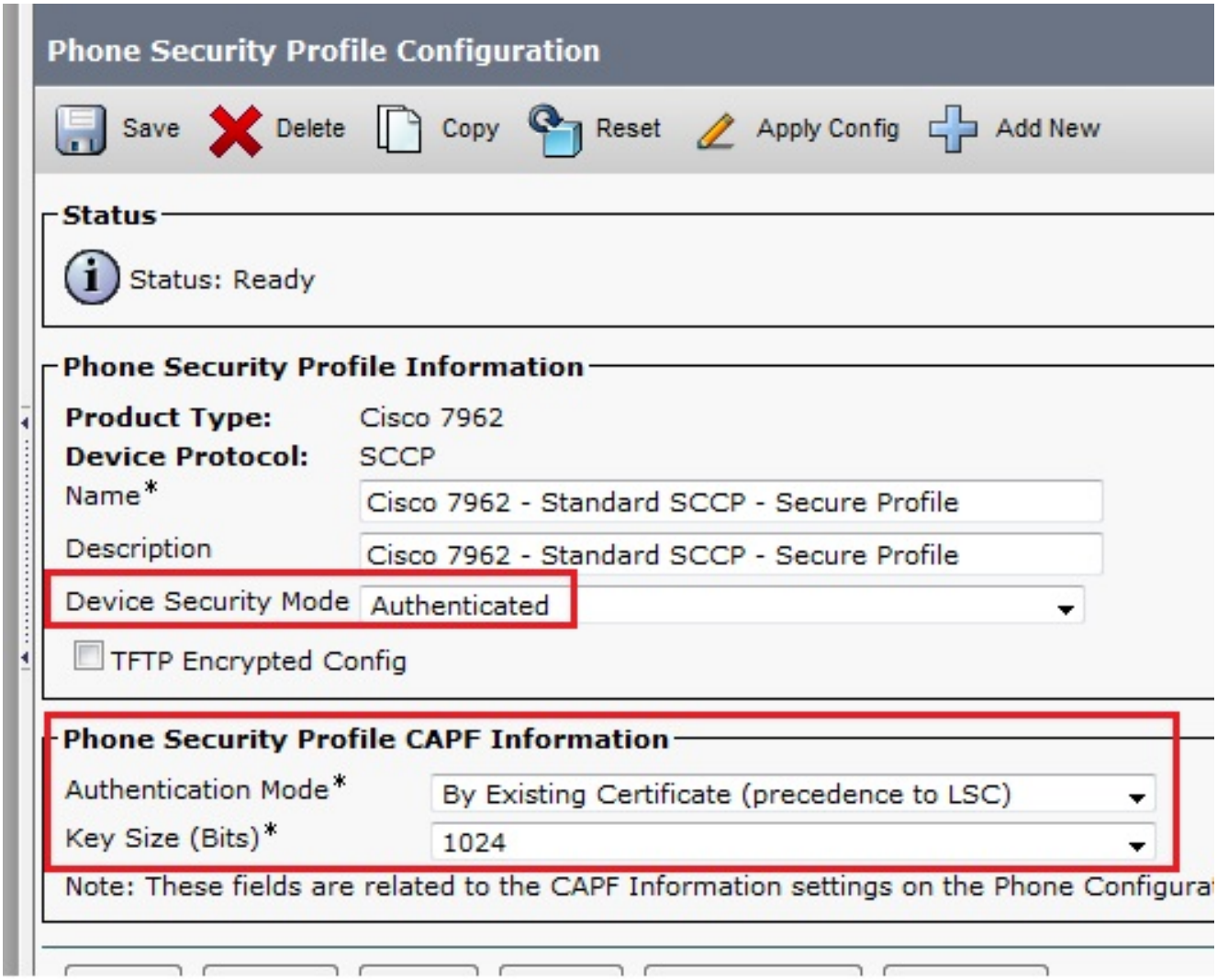


Genera una richiesta di firma del certificato (CSR) per i telefoni

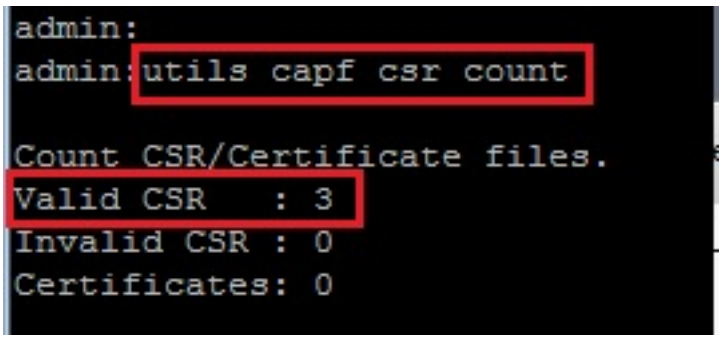
1. Accedere alla GUI Web di amministrazione CUCM.
2. Passare a **Telefoni dispositivo**.
3. Scegliere il telefono il cui LSC deve essere firmato dalla CA esterna.
4. Modificare il profilo di sicurezza del dispositivo in un profilo protetto (se non è presente, aggiungere un sistema al profilo di sicurezza del telefono di sicurezza).
5. Nella sezione CAPF della pagina Configurazione telefono scegliere **Installa/Aggiorna** per l'operazione di certificazione. Completare questo passaggio per tutti i telefoni il cui LSC deve essere firmato dalla CA esterna. Per lo stato dell'operazione certificato, dovrebbe essere visualizzato **Operazione in sospeso**.



Profilo sicurezza telefono (modello 7962).



Immettere il comando **utils capf csr count** nella sessione Secure Shell (SSH) per confermare se è stato generato un CSR. (Questa schermata mostra che è stato generato un CSR per tre telefoni.)

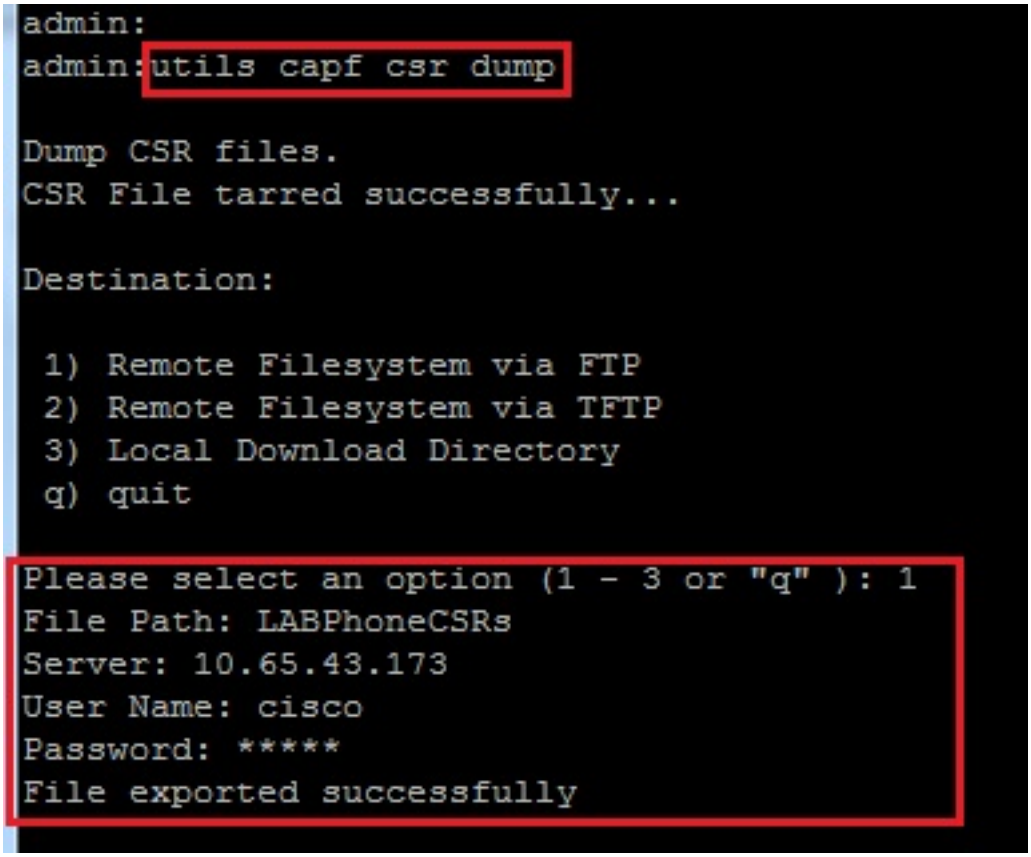


Nota: Lo stato dell'operazione certificato nella sezione CAPF del telefono rimane nello stato **Operazione in sospeso**.

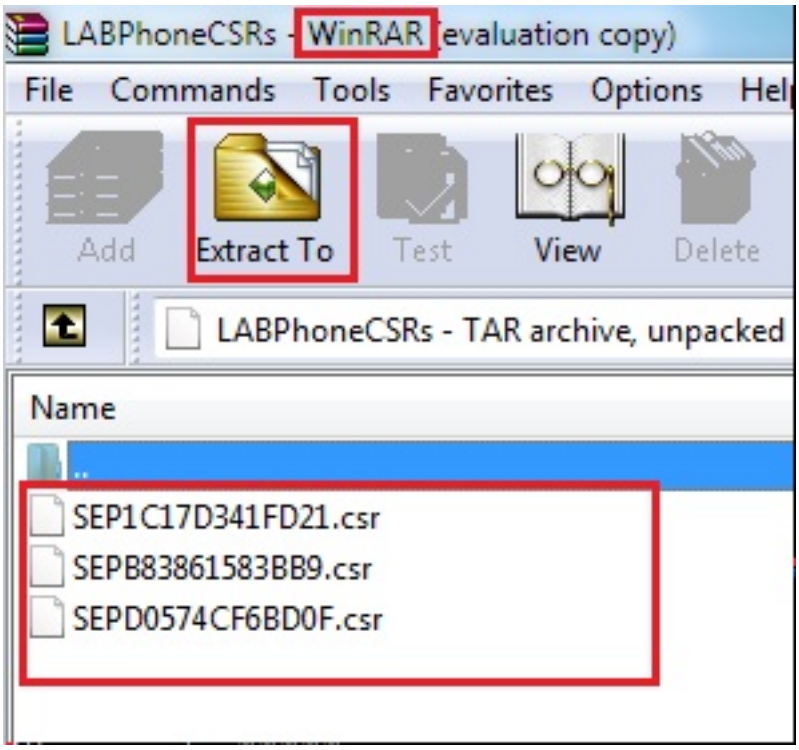
Recuperare il CSR generato da CUCM sul server FTP (o TFTP)

1. SSH nel server CUCM.

2. Eseguire il comando **utils capf csr dump**. In questa schermata viene mostrato il dump trasferito sull'FTP.



3. Aprire il file di dump con WinRAR ed estrarre il CSR nel computer locale.



Ottieni certificato telefonico

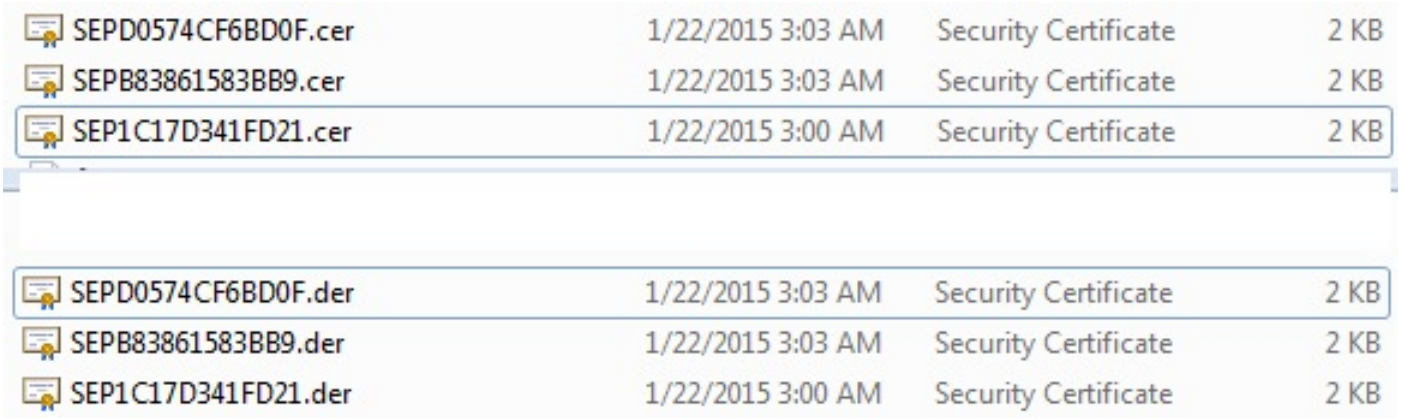
1. Inviare i CSR del telefono alla CA.

2. La CA fornisce un certificato firmato.

Nota: È possibile utilizzare un server Microsoft Windows 2003 come CA. La procedura per firmare il CSR con un'autorità di certificazione di Microsoft Windows 2003 è illustrata più avanti in questo documento.

Converti formato cer in der

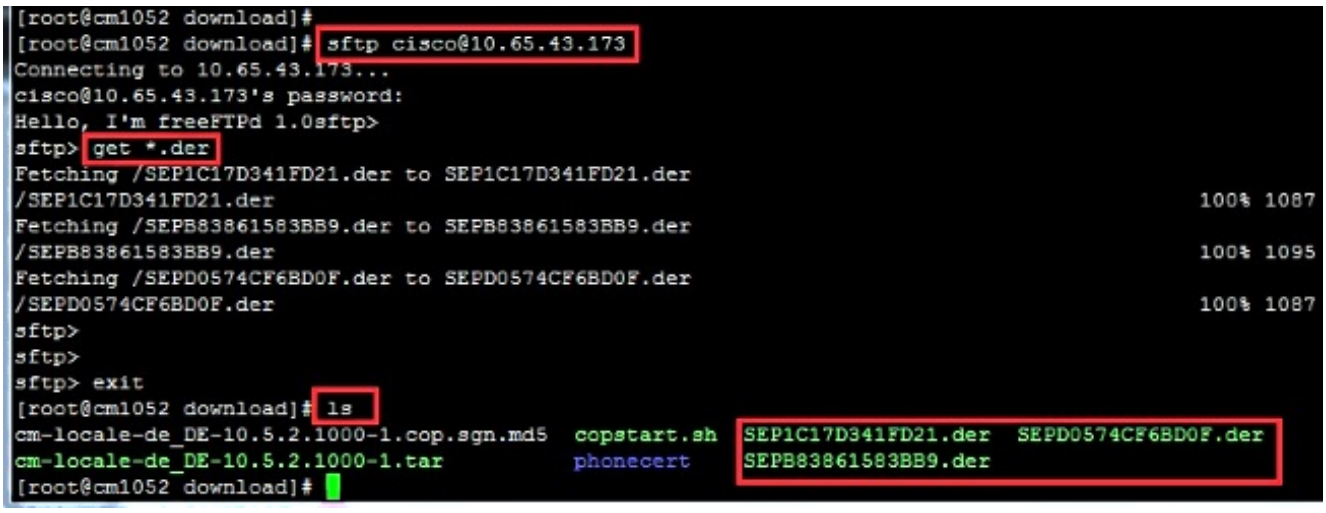
Se i certificati ricevuti sono in formato cer, rinominarli in der.



Comprimi il formato dei certificati (.der) in .tgz

Èpossibile utilizzare la radice del server CUCM (Linux) per comprimere il formato del certificato. Potete farlo anche in un normale sistema Linux.

1. Trasferire tutti i certificati firmati al sistema Linux con il server SFTP.



2. Immettere questo comando per comprimere tutti i certificati con estensione der in un file con estensione 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]#
```

Trasferire il file .tgz sul server SFTP

Completare i passaggi mostrati nella schermata per trasferire il file .tgz sul server 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>
```

Importare il file .tgz sul server CUCM

1. SSH nel server CUCM.

2. Eseguire il 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
```

Una volta importati i certificati, il conteggio dei CSR diventa zero.

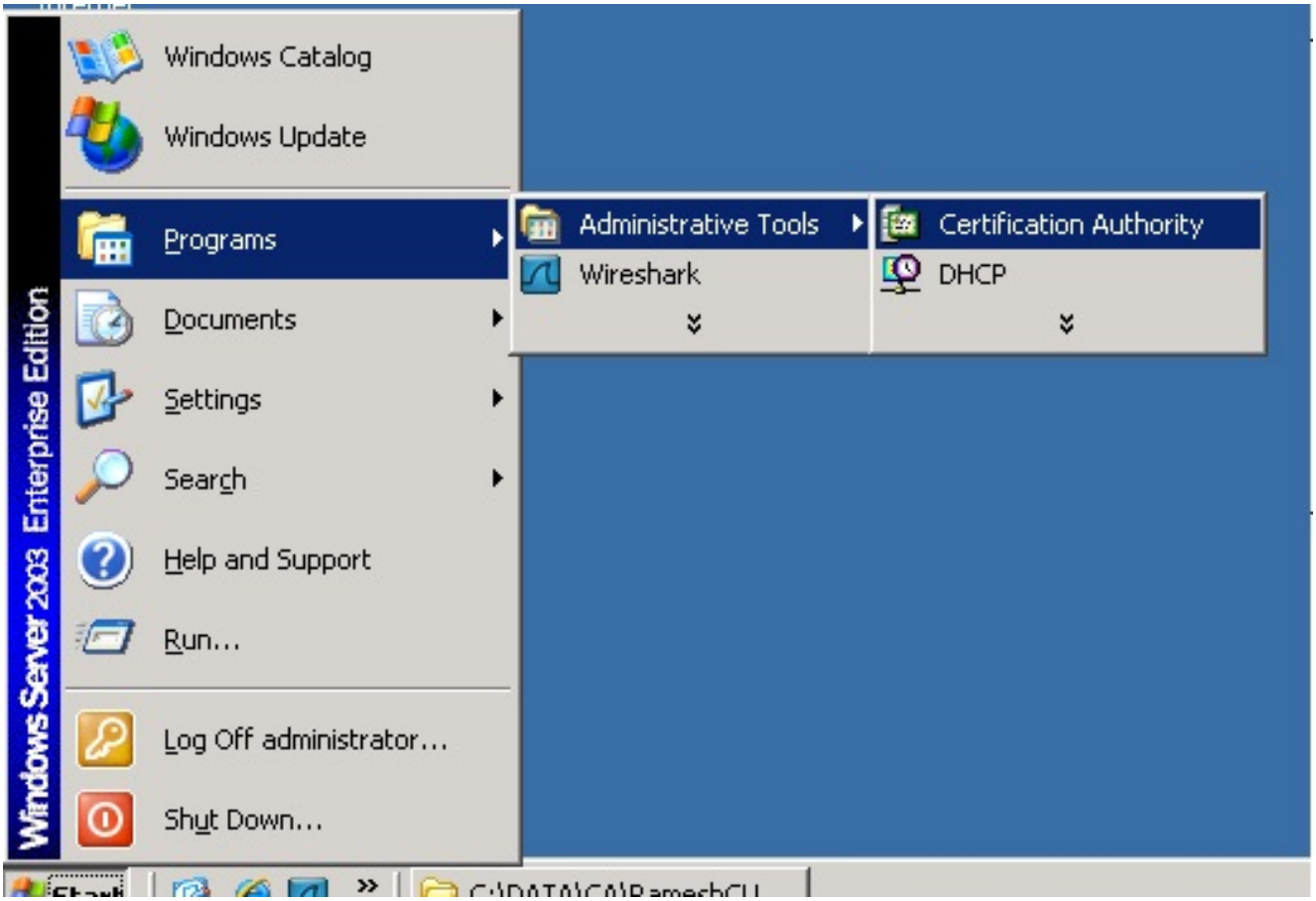
```
admin:
admin:utils capf csr count

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

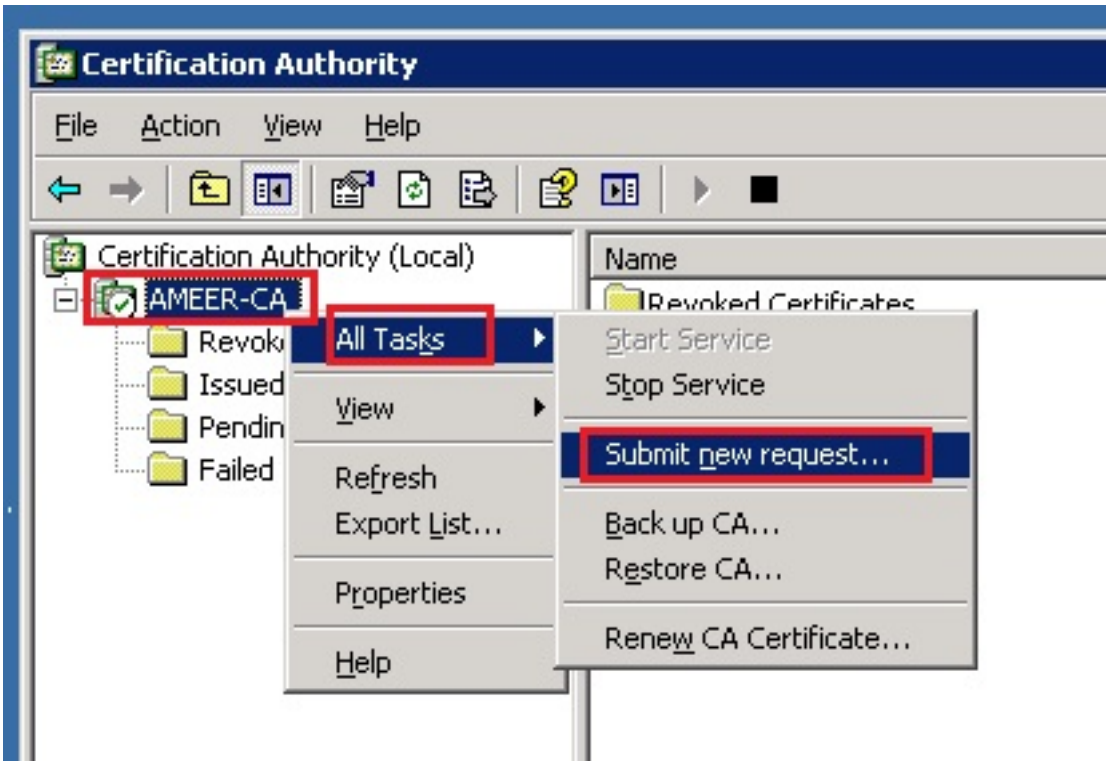
Firmare il CSR con Microsoft Windows 2003 Certificate Authority

Informazioni facoltative per Microsoft Windows 2003 - CA.

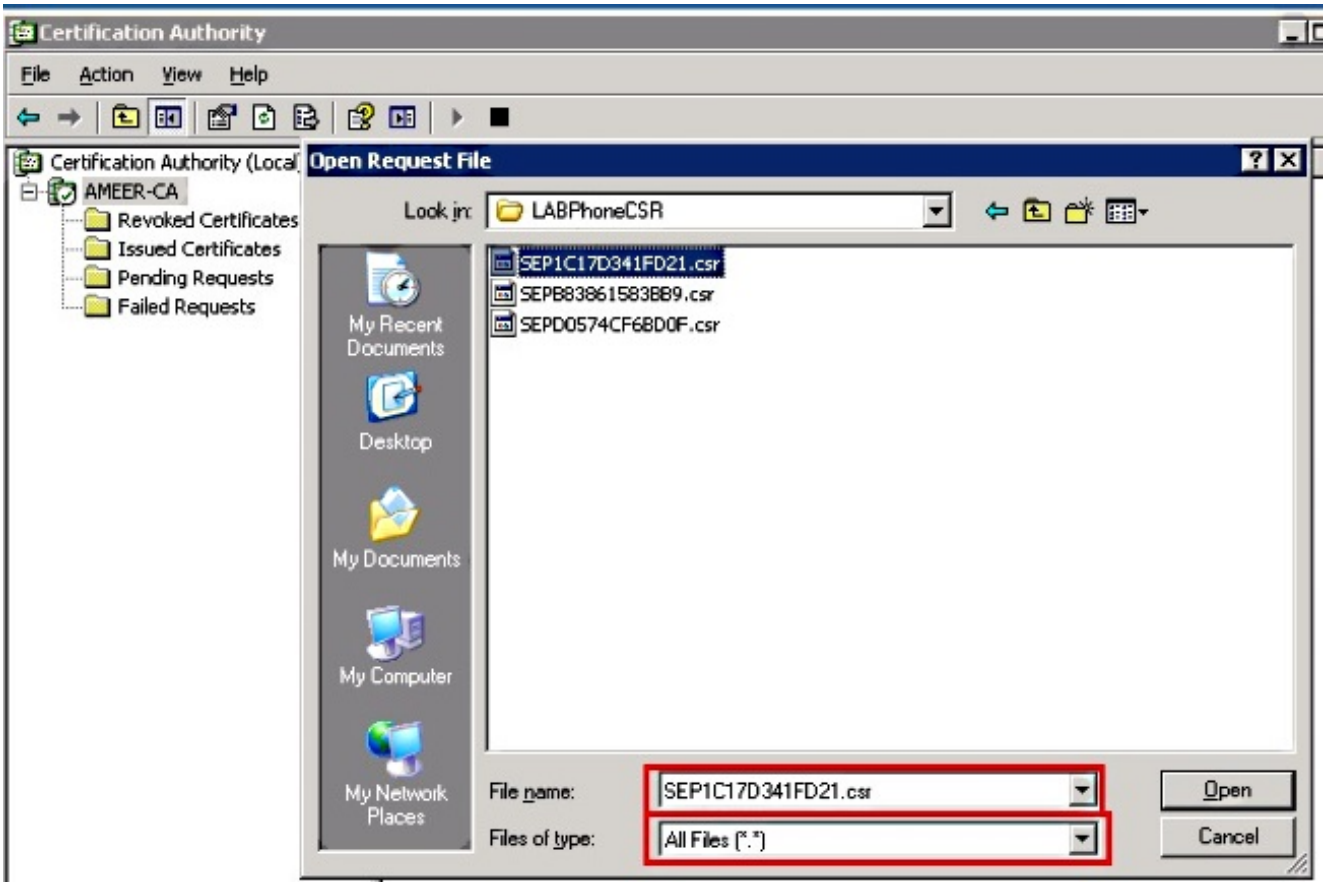
1. Aprire l'Autorità di certificazione.



2. Fare clic con il pulsante destro del mouse sulla CA e selezionare **All Tasks > Submit new request...**

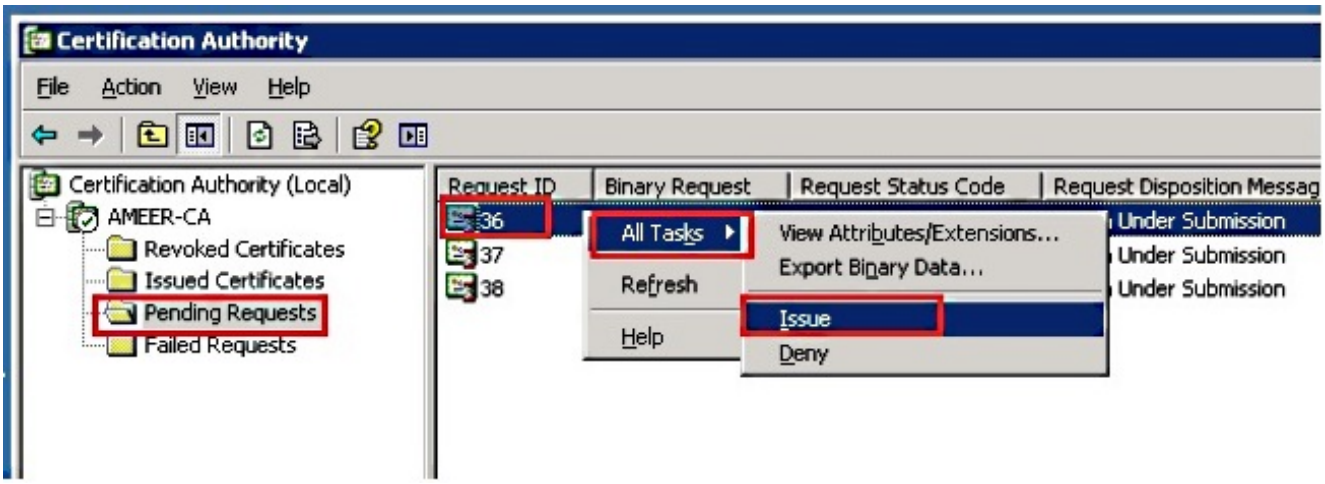


3. Selezionare il CSR e fare clic su **Apri**. Fate questo per tutti i CSR.



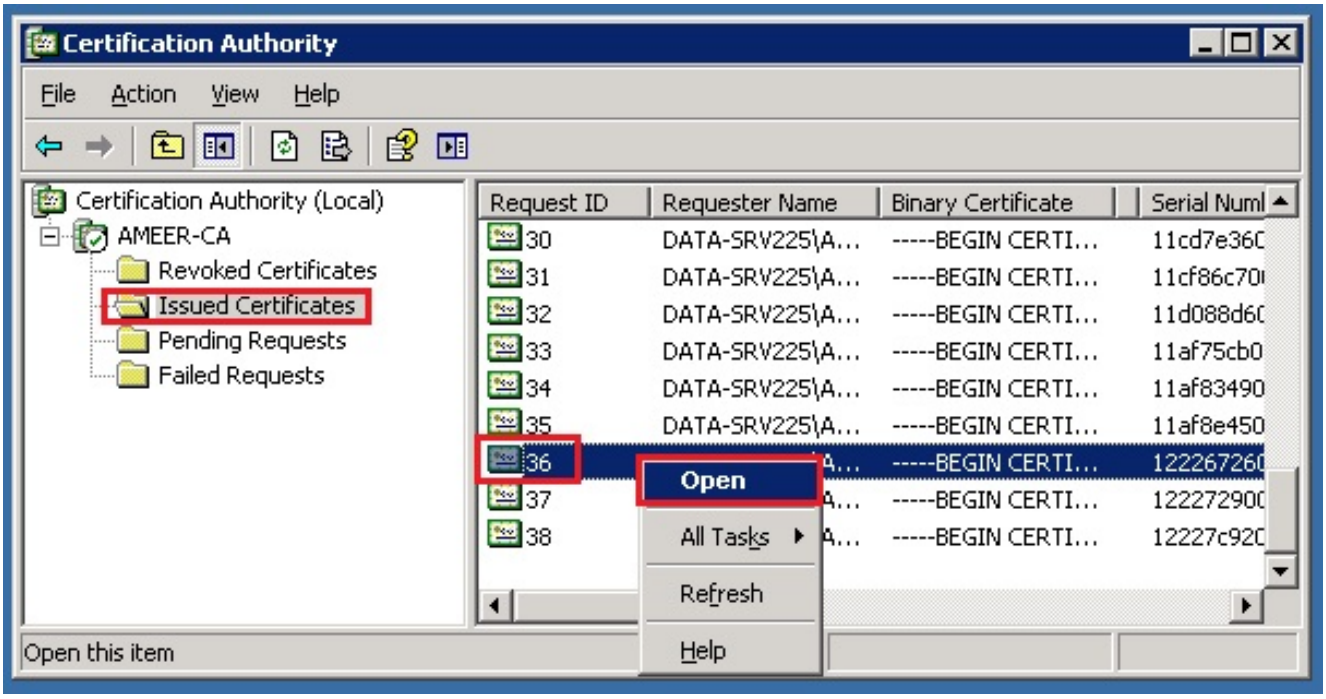
Tutti i CSR aperti vengono visualizzati nella cartella Richieste in sospeso.

4. Fare clic con il pulsante destro del mouse su ogni attività e passare a **Tutte le attività > Emetti** per emettere certificati. Eseguire questa operazione per tutte le richieste in sospeso.

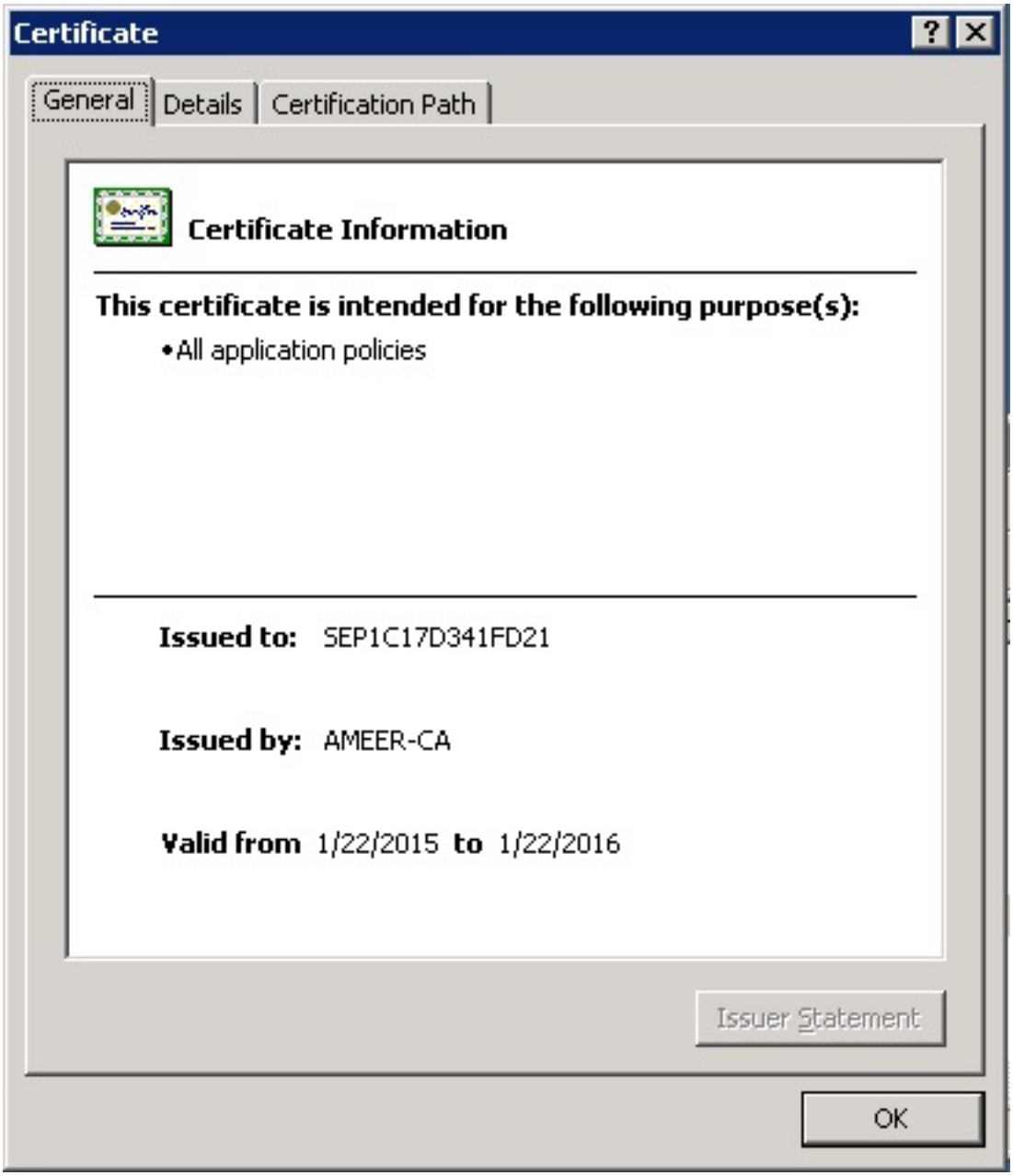


5. Per scaricare il certificato, scegliere **Certificato rilasciato**.

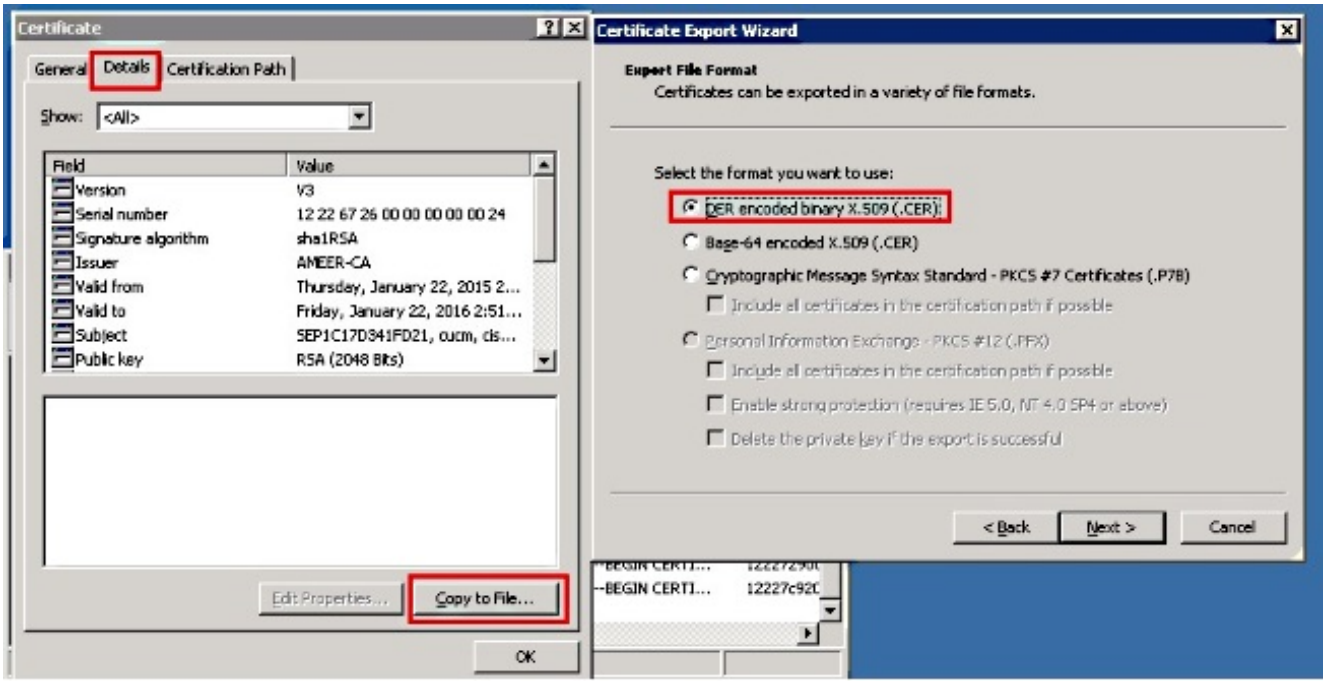
6. Fare clic con il pulsante destro del mouse sul certificato e scegliere **Apri**.



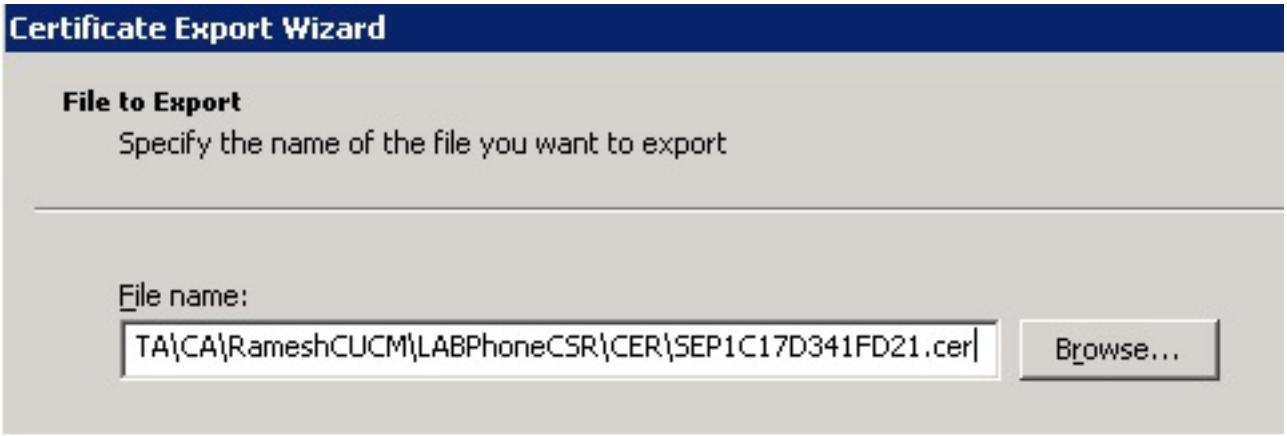
7. Èpossibile visualizzare i dettagli del certificato. Per scaricare il certificato, selezionare la scheda Dettagli e scegliere **Copia su file...**



8. Nell'Esportazione guidata certificati scegliere **X.509 binario con codifica DER (.CER)**.



9. Assegnare al file un nome appropriato. In questo esempio viene utilizzato il formato <MAC>.cer.

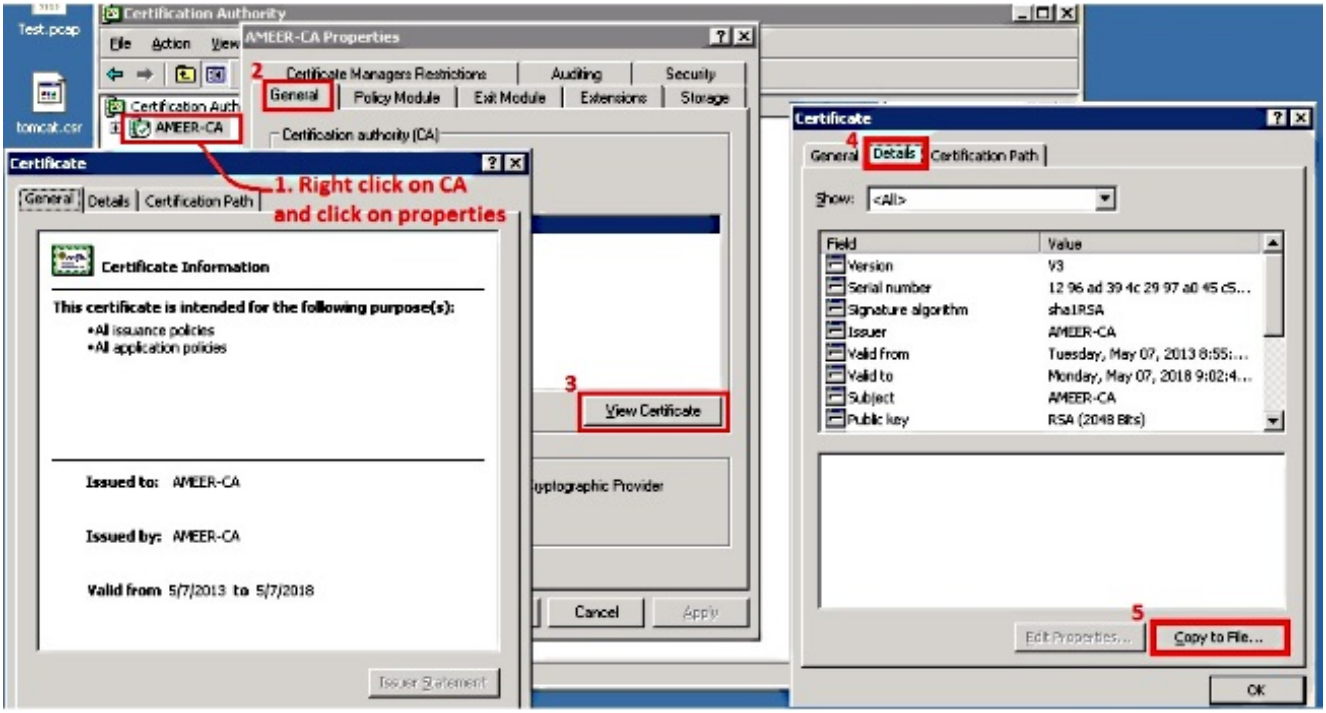


10. Ottenere i certificati per altri telefoni nella sezione Certificato emesso con questa procedura.

Ottieni certificato radice dalla CA

1. Aprire **Autorità di certificazione**.

2. Completare la procedura illustrata in questa schermata per scaricare la root-CA.

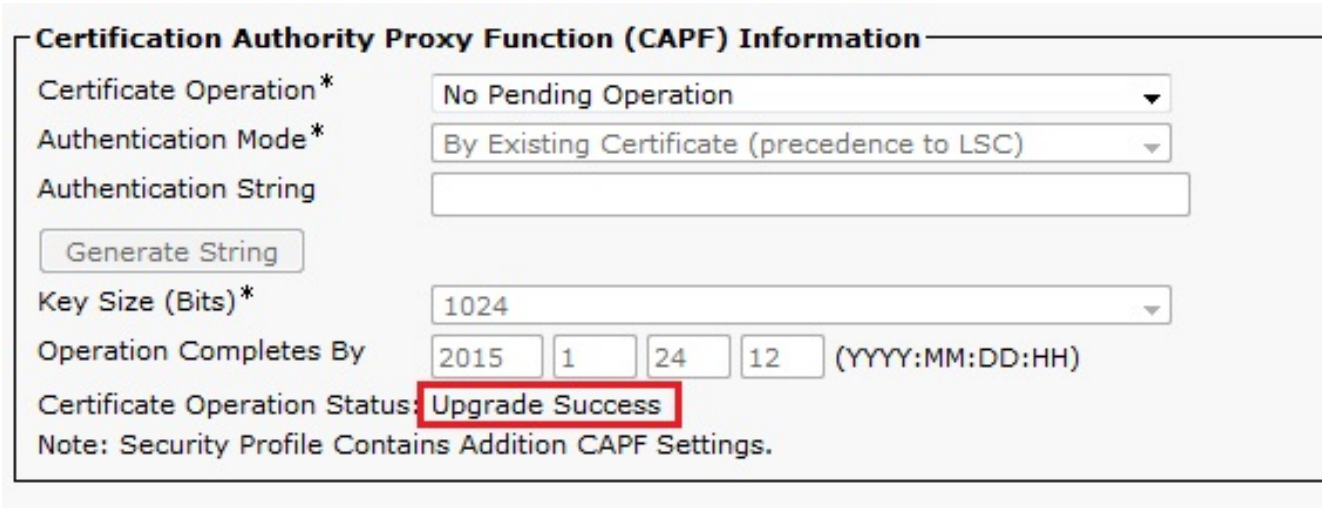


Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

1. Vai alla pagina di configurazione del telefono.

2. Nella sezione CAPF, lo stato dell'operazione certificato viene visualizzato come **Aggiornamento riuscito**.



Nota: Per ulteriori informazioni, fare riferimento a [Generazione e importazione di licenze LSC firmate da CA di terze parti](#).

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.