Beispiel für die Erstellung und den Import von LSCs mit CA-Signatur von CUCM

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[CA-Root-Zertifikat hochladen](#)
[Offline-Zertifizierungsstelle für Zertifikatausstellung auf Endpunkt festlegen](#)
[Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) für die Telefone](#)
[Rufen Sie den generierten CSR vom CUCM auf den FTP- (oder TFTP-) Server ab.](#)
[Telefonzertifikat abrufen](#)
[.cer in .der Format konvertieren](#)
[Komprimieren der Zertifikate (.der) in das TGZ-Format](#)
[Übertragen der TGZ-Datei auf den SFTP-Server](#)
[Importieren Sie die TGZ-Datei auf den CUCM-Server.](#)
[Signieren des CSR mit der Microsoft Windows 2003 Certificate Authority](#)
[Stammzertifikat von der Zertifizierungsstelle abrufen](#)
[Überprüfung](#)
[Fehlerbehebung](#)

Einleitung

CAPF (Certificate Authority Proxy Function) LSCs (Locally Significant Certificates) sind lokal signiert. Möglicherweise benötigen Sie Telefone jedoch von der Zertifizierungsstelle (Certificate Authority, CA) signierte LSCs von Drittanbietern. In diesem Dokument wird ein Verfahren beschrieben, mit dem Sie dieses Ziel erreichen können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco Unified Communication Manager (CUCM) verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CUCM-Version 10.5(2). Diese Funktion funktioniert jedoch ab Version 10.0 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Im Folgenden sind die einzelnen Schritte dieses Verfahrens aufgeführt, die jeweils in einem eigenen Abschnitt beschrieben werden:

1. CA-Root-Zertifikat hochladen
2. Offline-Zertifizierungsstelle für Zertifikatausstellung auf Endpunkt festlegen
3. Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) für die Telefone
4. Rufen Sie den erzeugten CSR vom Cisco Unified Communications Manager (CUCM) auf den FTP-Server ab.
5. Telefonzertifikat von CA abrufen
6. .cer in .der Format konvertieren
7. Komprimieren der Zertifikate (.der) in das TGZ-Format
8. Übertragen Sie die TGZ-Datei auf den Secure Shell FTP (SFTP)-Server.
9. Importieren Sie die TGZ-Datei auf den CUCM-Server.
10. Signieren des CSR mit der Microsoft Windows 2003 Certificate Authority
11. Stammzertifikat von der Zertifizierungsstelle abrufen

CA-Root-Zertifikat hochladen

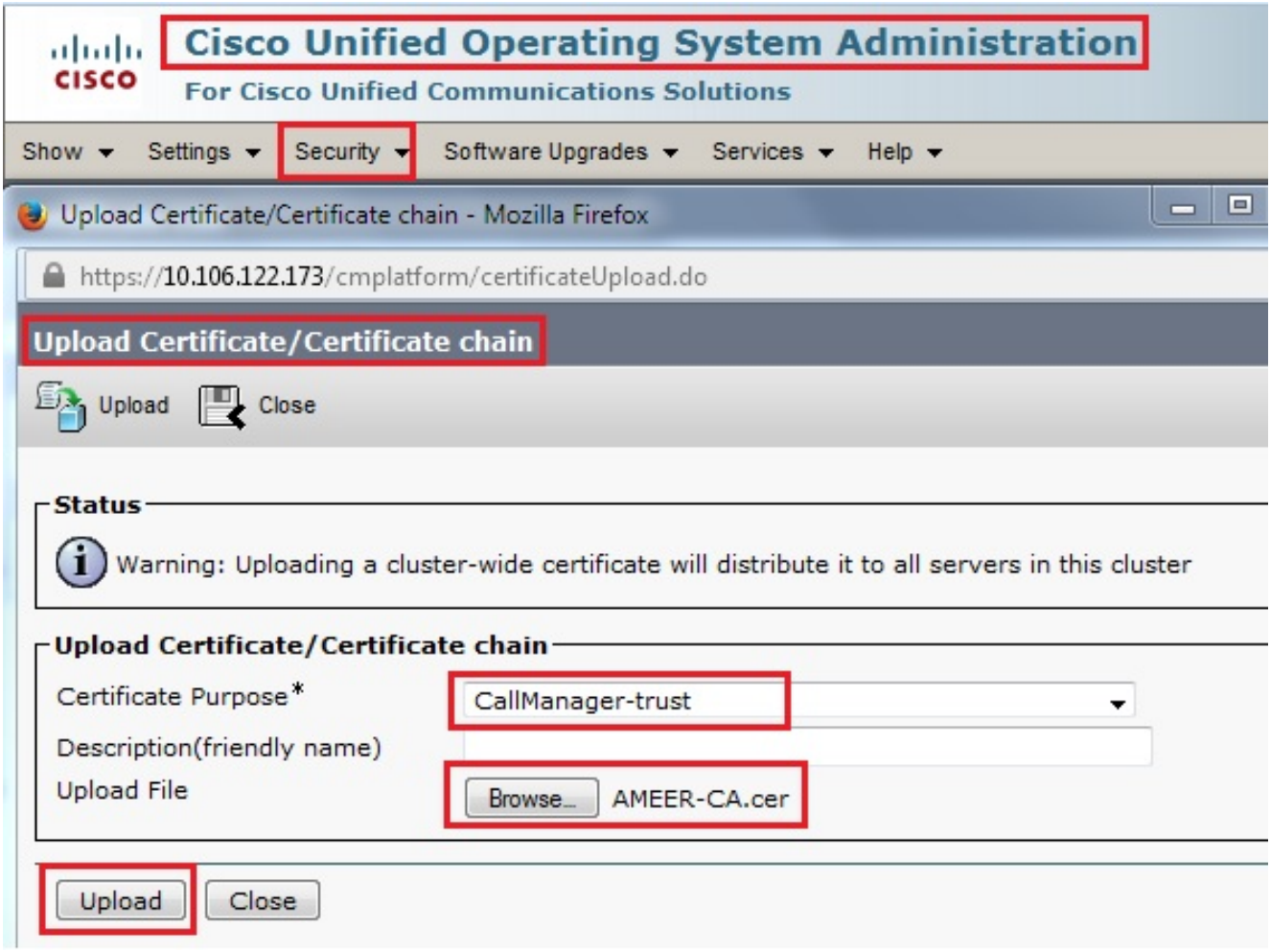
1. Melden Sie sich bei der Web-GUI der Cisco Unified Operating System (OS)-Administration an.

2. Navigieren Sie zu **Sicherheitszertifikatverwaltung**.

3. Klicken Sie auf **Zertifikat hochladen/Zertifikatskette**.

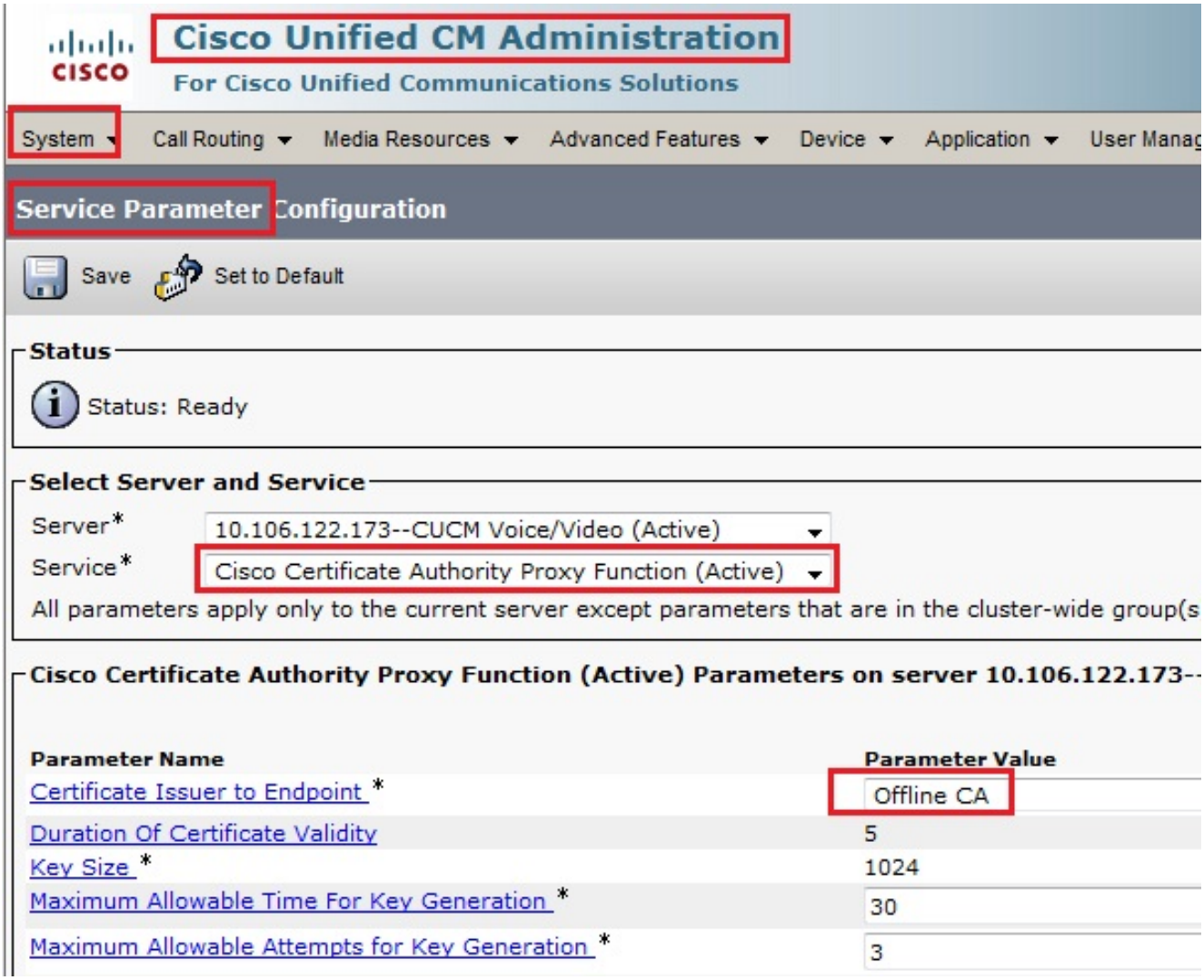
4. Wählen Sie **CallManager-trust** unter Certificate Purpose aus.

5. Navigieren Sie zum Stammzertifikat der Zertifizierungsstelle, und klicken Sie auf **Hochladen**.



Offline-Zertifizierungsstelle für Zertifikatausstellung auf Endpunkt festlegen

1. Melden Sie sich bei der Web-GUI der CUCM-Administration an.
2. Navigieren Sie zu **System > Service Parameter**.
3. Wählen Sie den CUCM-Server aus, und wählen Sie für den Dienst die **Cisco Certificate Authority Proxy Function** aus.
4. Wählen Sie **Offline-Zertifizierungsstelle** für Zertifikatausstellung an Endpunkt aus.



Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR) für die Telefone

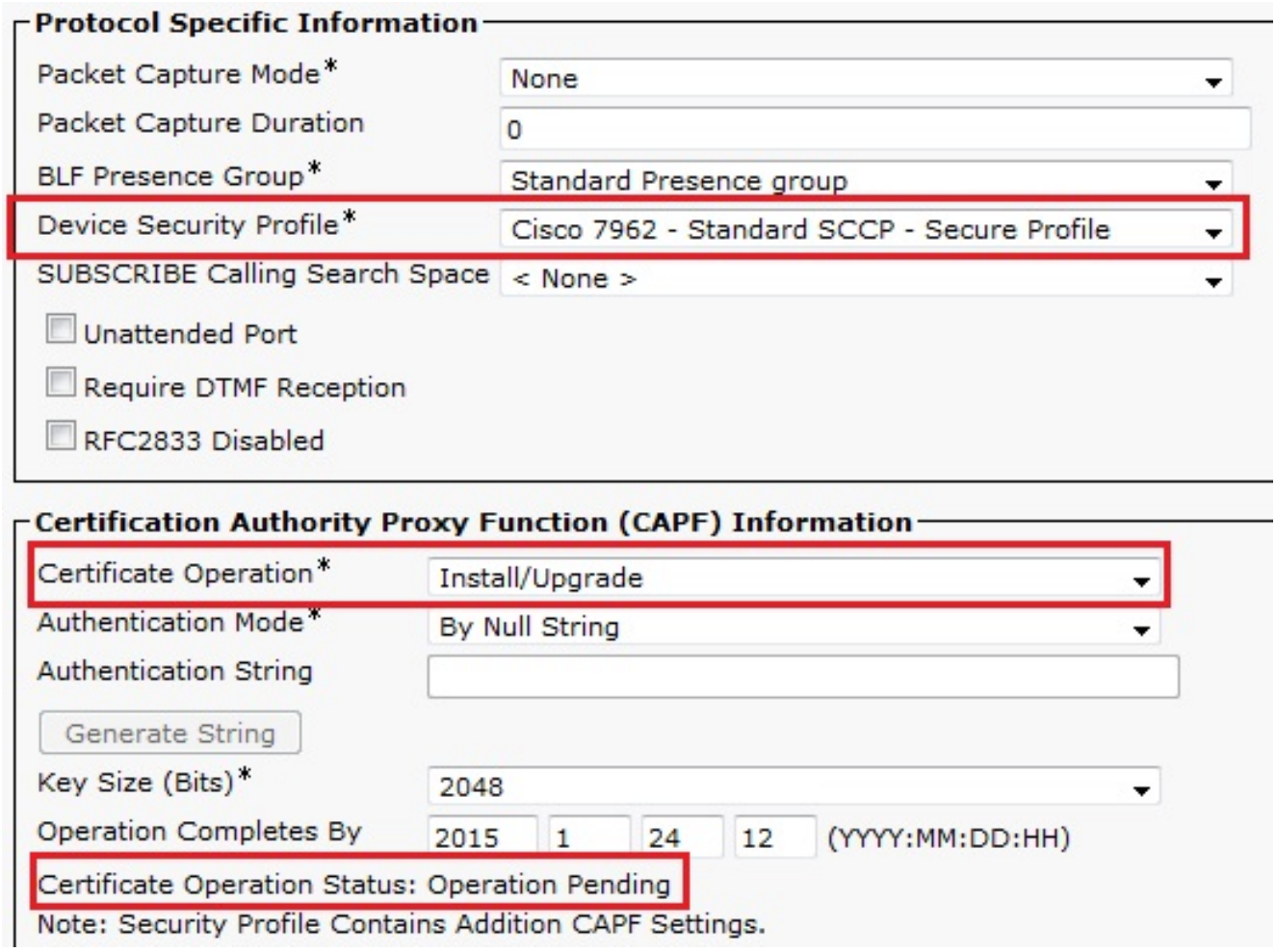
1. Melden Sie sich bei der Web-GUI der CUCM-Administration an.

2. Navigieren Sie zu **Gerätetelefone**.

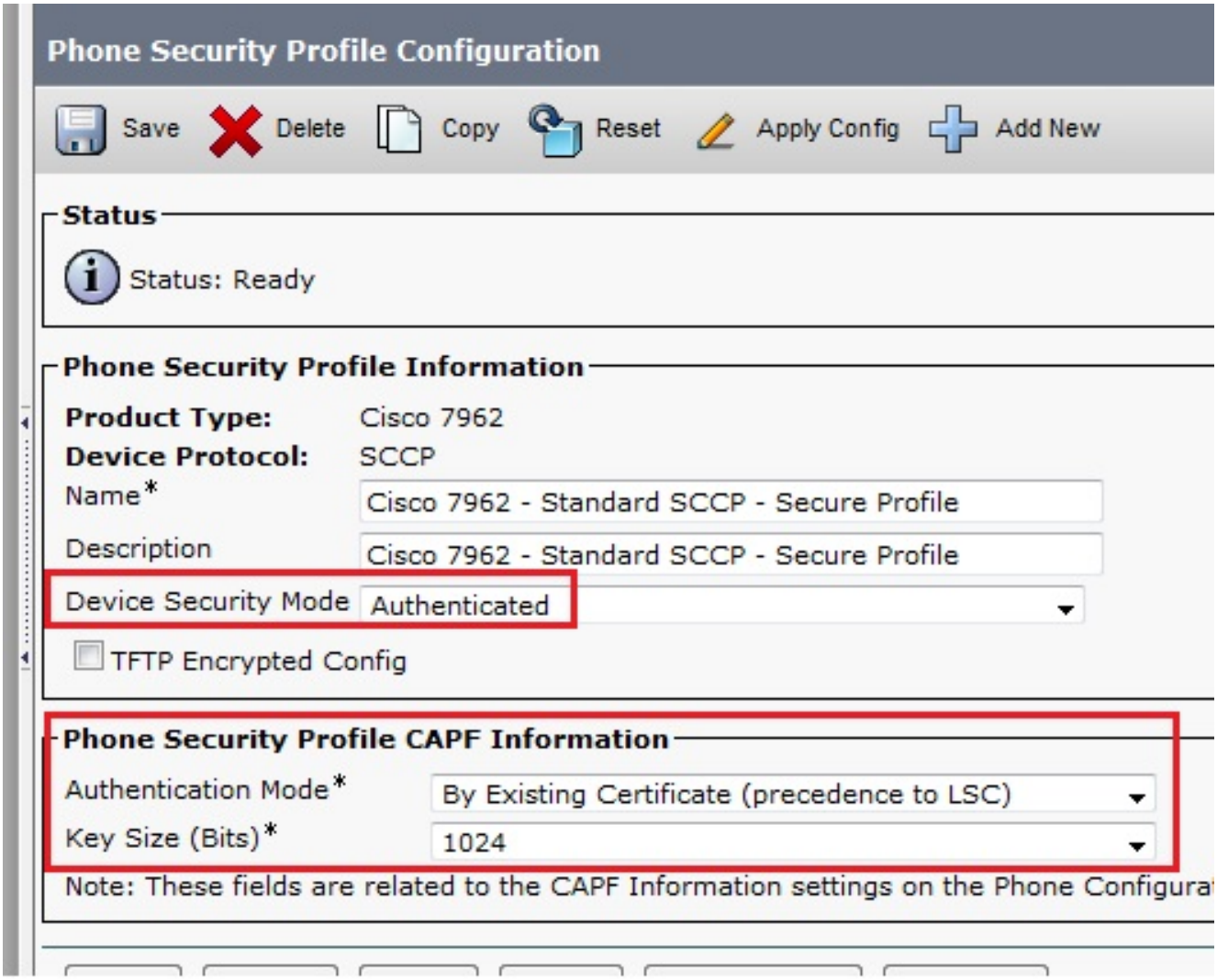
3. Wählen Sie das Telefon aus, dessen LSC von der externen Zertifizierungsstelle signiert werden muss.

4. Ändern Sie das Gerätesicherheitsprofil in ein gesichertes Profil (falls nicht vorhanden, fügen Sie ein System zum Sicherheitsprofil für Telefone hinzu).

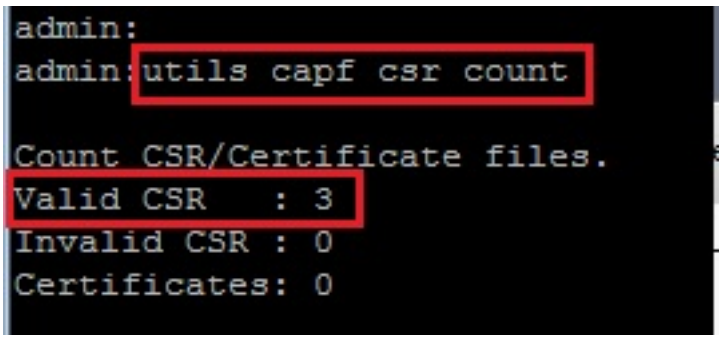
5. Wählen Sie auf der Seite für die Telefonkonfiguration im Abschnitt "CAPF" die Option **Install/Upgrade** for the Certification Operation (**Installation/Upgrade** für den Zertifizierungsvorgang) aus. Führen Sie diesen Schritt für alle Telefone aus, deren LSC von der externen Zertifizierungsstelle signiert werden muss. Als Status des Zertifikatvorgangs sollte **Vorgang** ausstehend angezeigt werden.



Telefon-Sicherheitsprofil (Modell 7962).



Geben Sie den Befehl **utils capf csr count** in der Secure Shell (SSH)-Sitzung ein, um zu bestätigen, ob ein CSR generiert wird. (Dieser Screenshot zeigt, dass für drei Telefone eine CSR-Anfrage erstellt wurde.)



Anmerkung: Der Status des Zertifikatvorgangs im CAPF-Bereich des Telefons bleibt im Status **Vorgang ausstehend**.

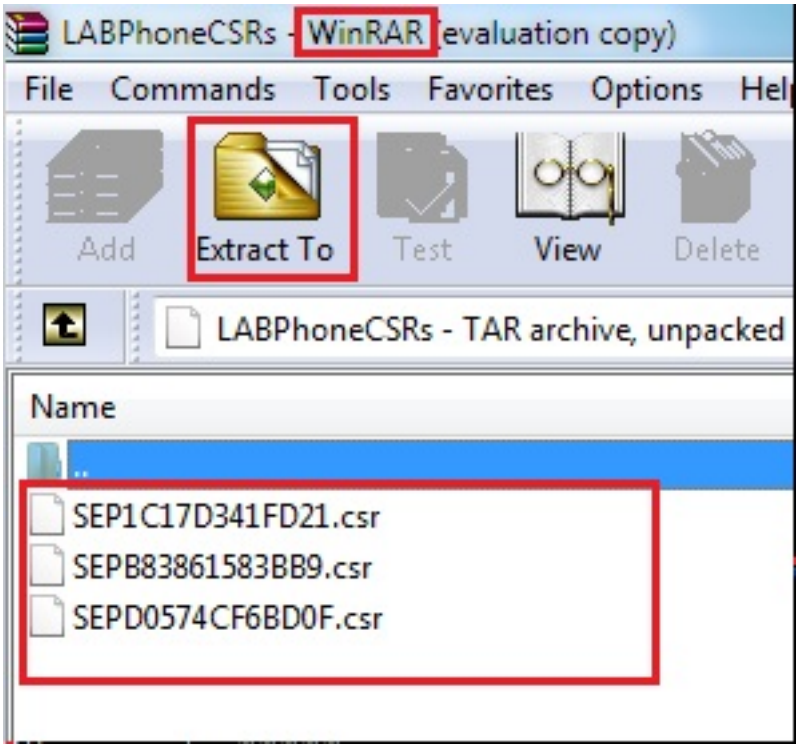
Rufen Sie den generierten CSR vom CUCM auf den FTP- (oder TFTP-) Server ab.

1. SSH zum CUCM-Server.

2. Führen Sie den Befehl **utils capf csr dump** aus. Dieser Screenshot zeigt den Dump, der auf den FTP übertragen wird.

```
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. Öffnen Sie die Dump-Datei mit WinRAR, und extrahieren Sie den CSR auf Ihren lokalen Computer.



Telefonzertifikat abrufen

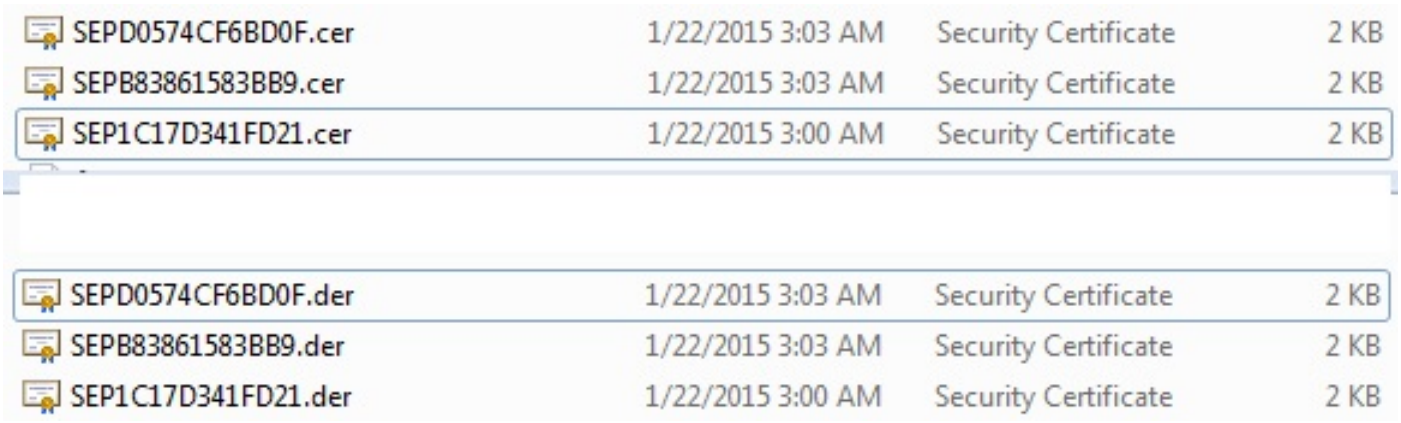
1. Senden Sie die CSRs des Telefons an die Zertifizierungsstelle.

2. Die Zertifizierungsstelle stellt Ihnen ein signiertes Zertifikat zur Verfügung.

   Anmerkung: Sie können einen Microsoft Windows 2003-Server als Zertifizierungsstelle verwenden. Das Verfahren zum Signieren des CSR mit einer Microsoft Windows 2003-Zertifizierungsstelle wird weiter unten in diesem Dokument erläutert.

.cer in .der Format konvertieren

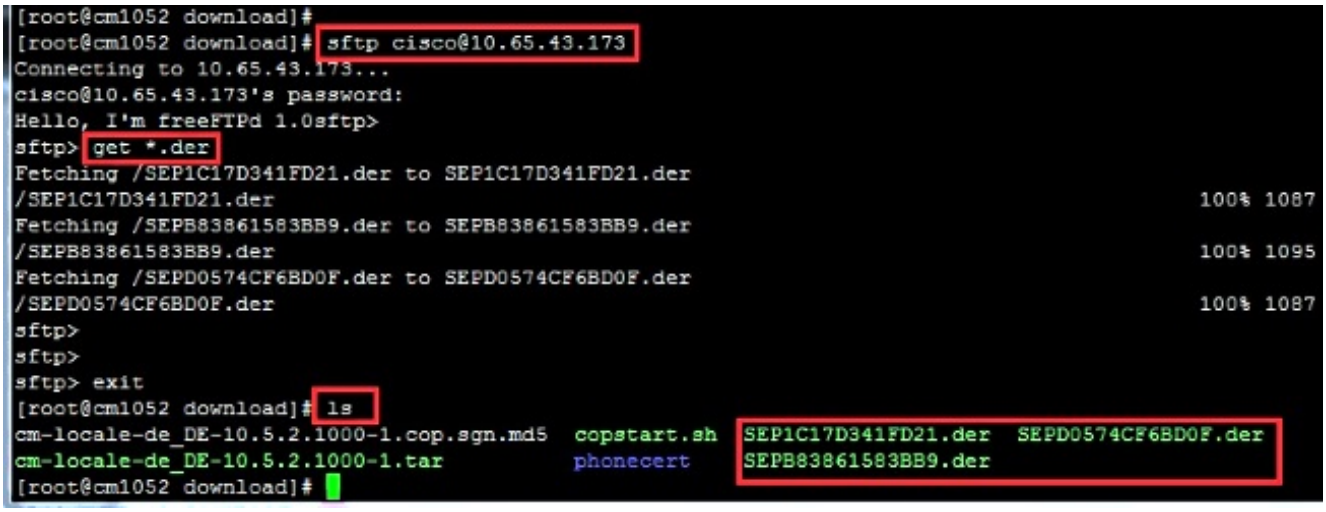
Wenn die empfangenen Zertifikate im CER-Format vorliegen, benennen Sie sie in .der um.



Komprimieren der Zertifikate (.der) in das TGZ-Format

Sie können den CUCM-Server-Root (Linux) verwenden, um das Zertifikatformat zu komprimieren. Sie können dies auch in einem normalen Linux-System tun.

1. Übertragen Sie alle signierten Zertifikate auf das Linux-System mit dem SFTP-Server.

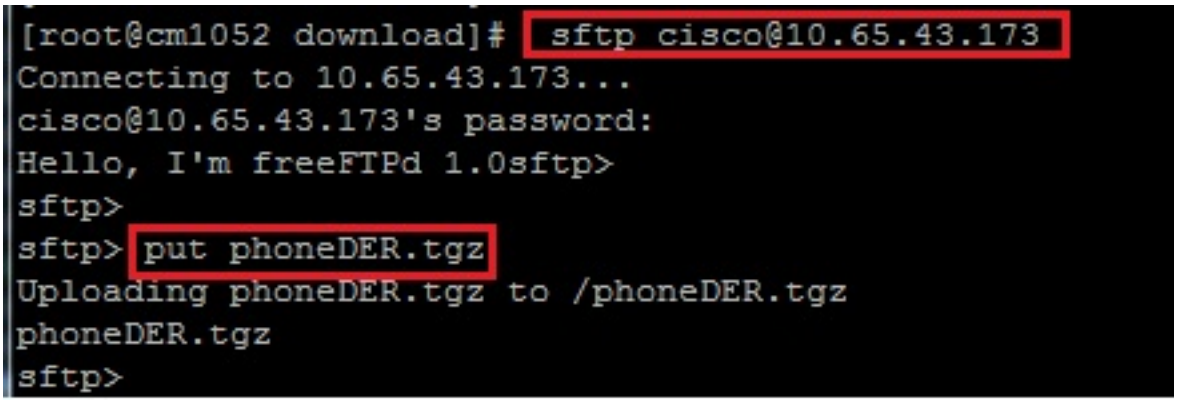


2. Geben Sie diesen Befehl ein, um alle Zertifikate mit der Erweiterung .der in eine TGZ-Datei zu komprimieren.

```
tar -zcvf
```

Übertragen der TGZ-Datei auf den SFTP-Server

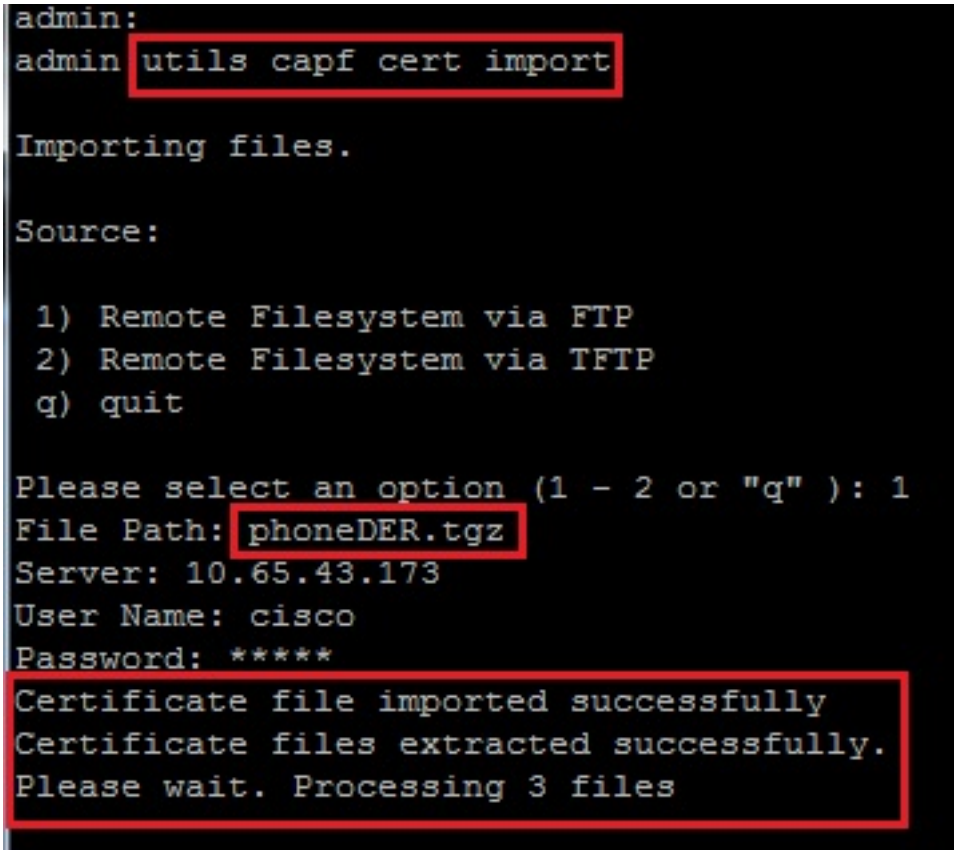
Führen Sie die im Screenshot aufgeführten Schritte aus, um die TGZ-Datei auf den SFTP-Server zu übertragen.



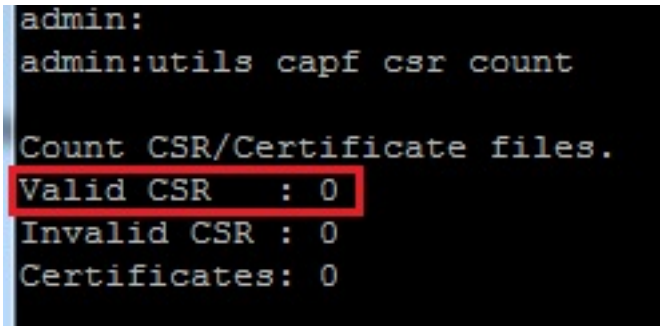
Importieren Sie die TGZ-Datei auf den CUCM-Server.

1. SSH zum CUCM-Server.

2. Führen Sie den Befehl **utils capf cert import** aus.



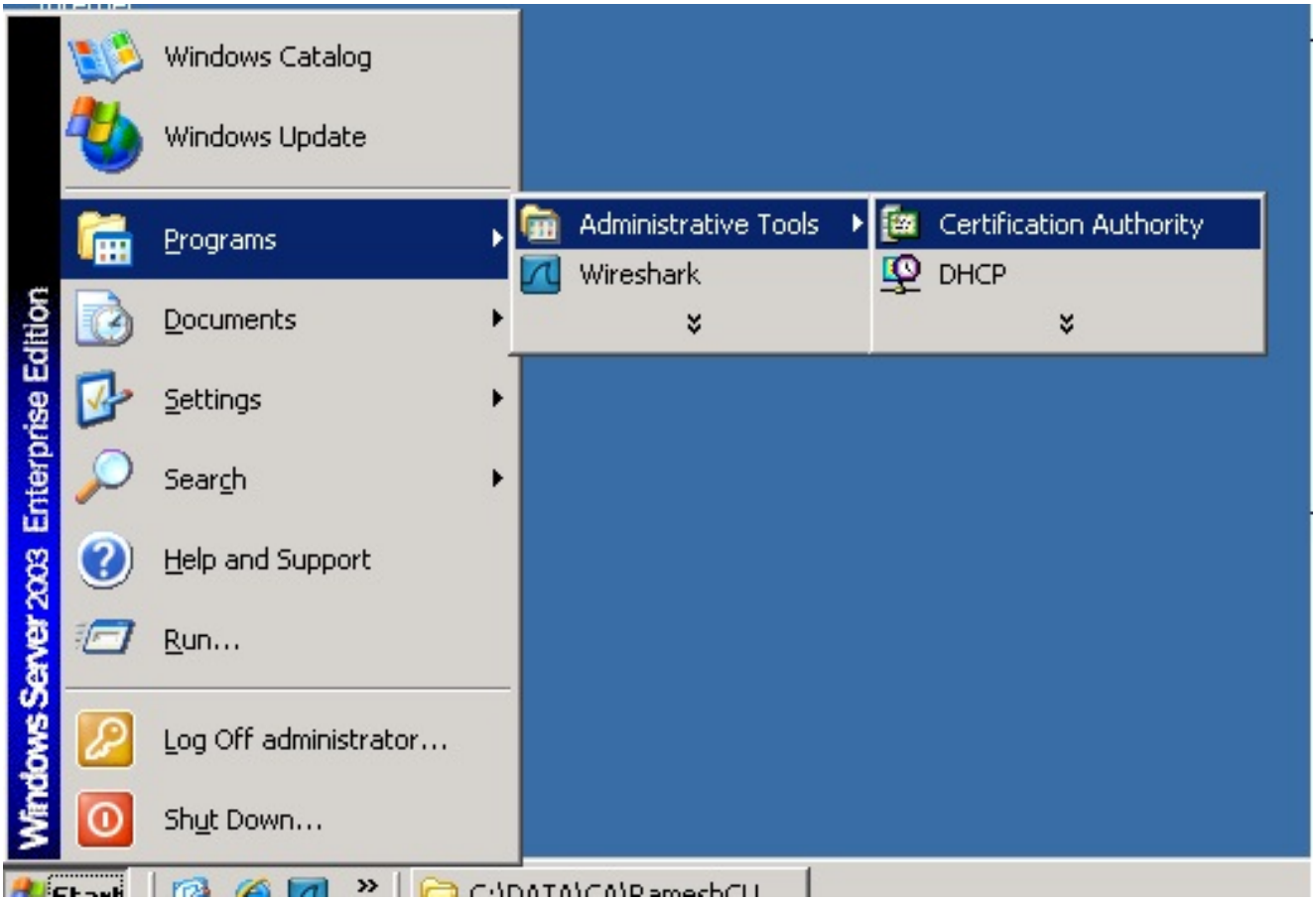
Sobald die Zertifikate erfolgreich importiert wurden, wird die CSR-Anzahl auf Null gesetzt.



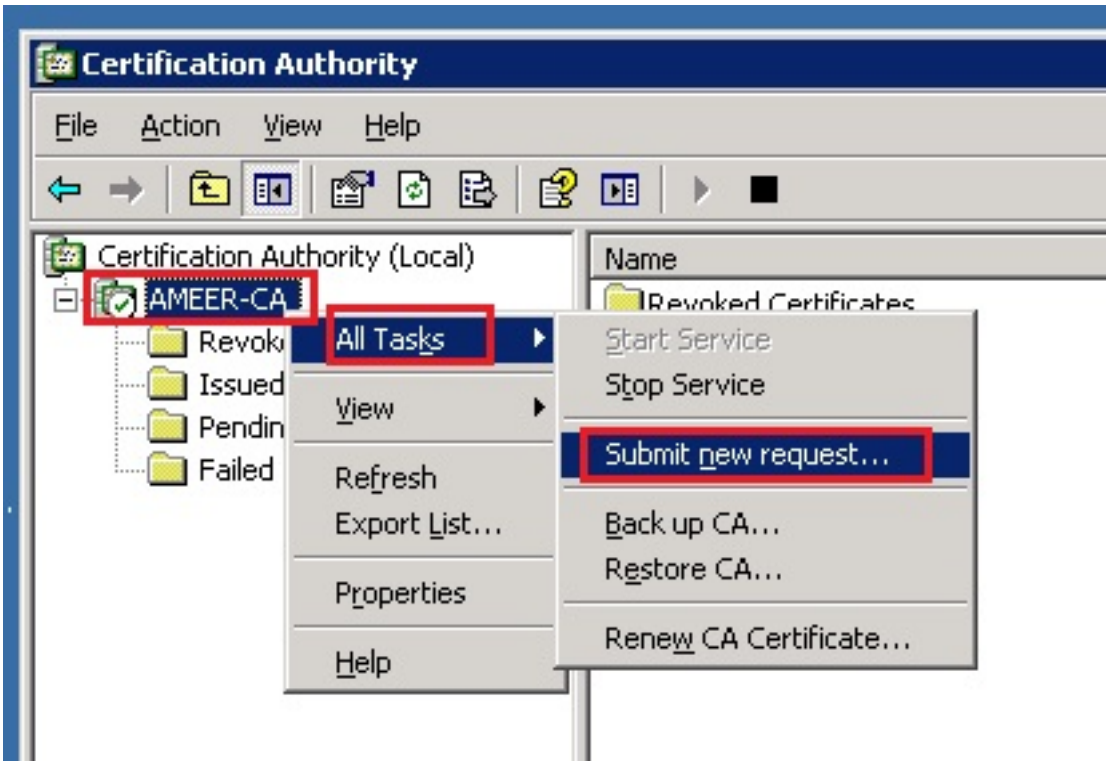
Signieren des CSR mit der Microsoft Windows 2003 Certificate Authority

Dies sind optionale Informationen für Microsoft Windows 2003 - CA.

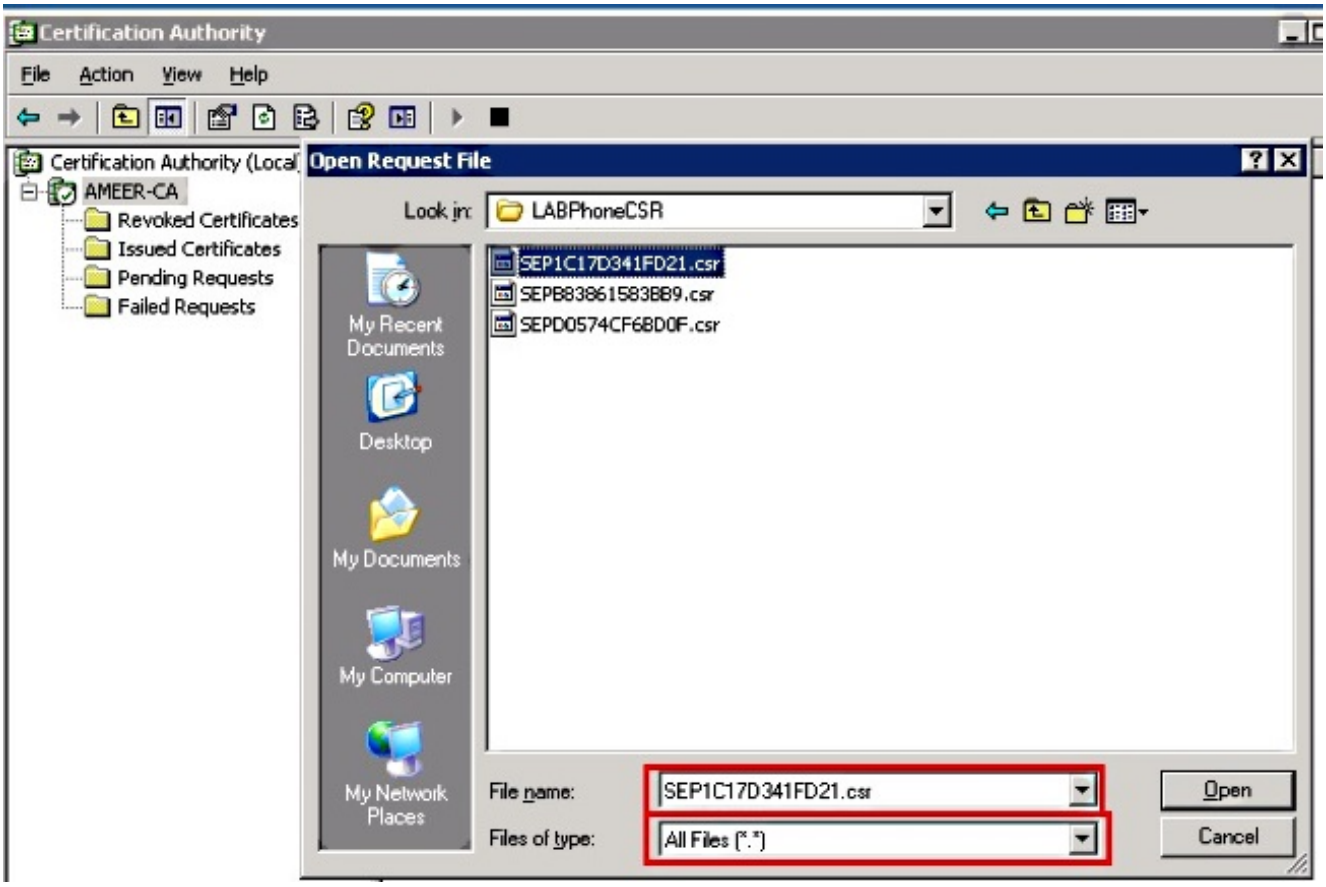
1. Offene Zertifizierungsstelle



2. Klicken Sie mit der rechten Maustaste auf die Zertifizierungsstelle, und navigieren Sie zu **Alle Aufgaben > Neue Anforderung einsenden...**

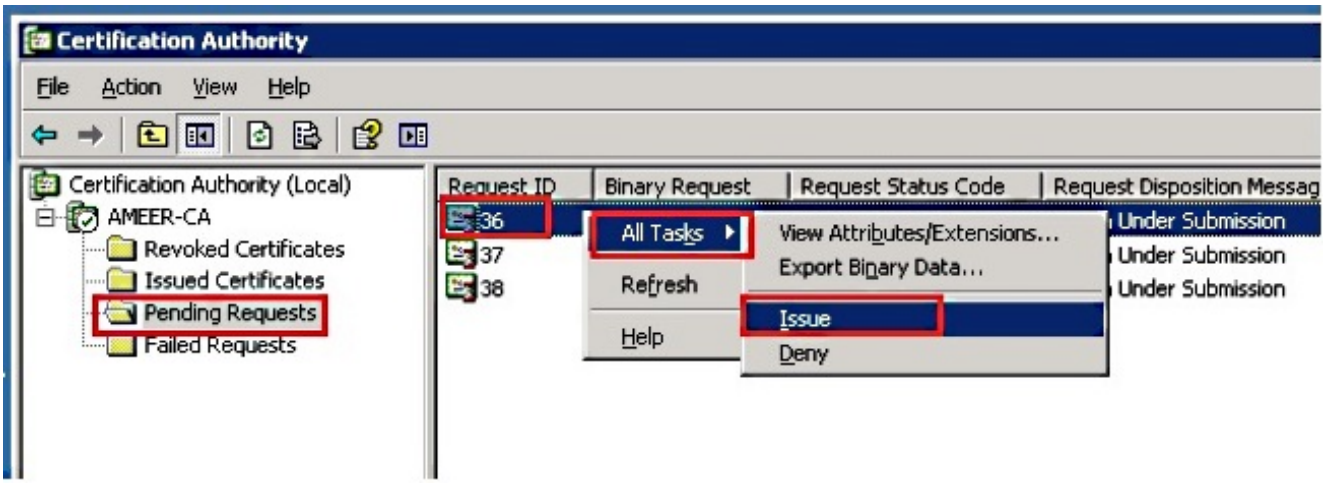


3. Wählen Sie den CSR aus, und klicken Sie auf **Öffnen**. Führen Sie diesen Vorgang für alle CSRs aus.



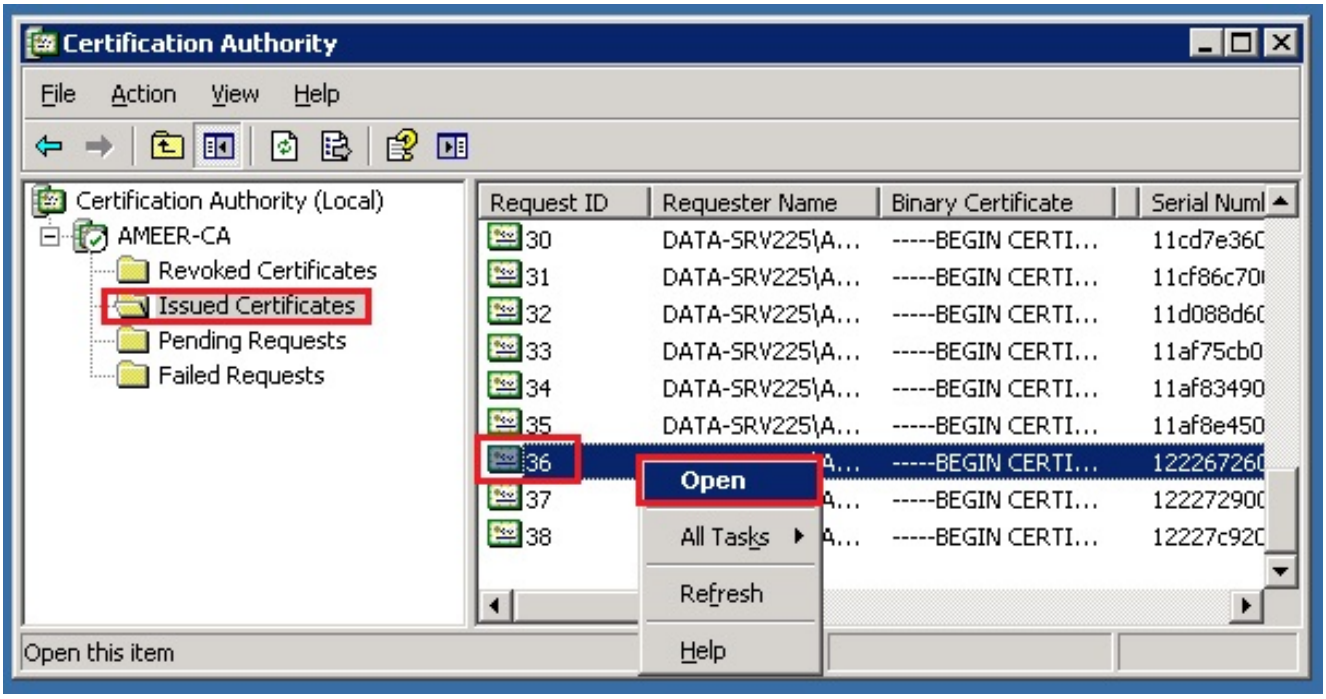
Alle geöffneten CSR-Dokumente werden im Ordner "Ausstehende Anträge" angezeigt.

4. Klicken Sie mit der rechten Maustaste darauf, und navigieren Sie zu **Alle Aufgaben > Problem**, um Zertifikate auszustellen. Führen Sie diesen Vorgang für alle ausstehenden Anforderungen aus.

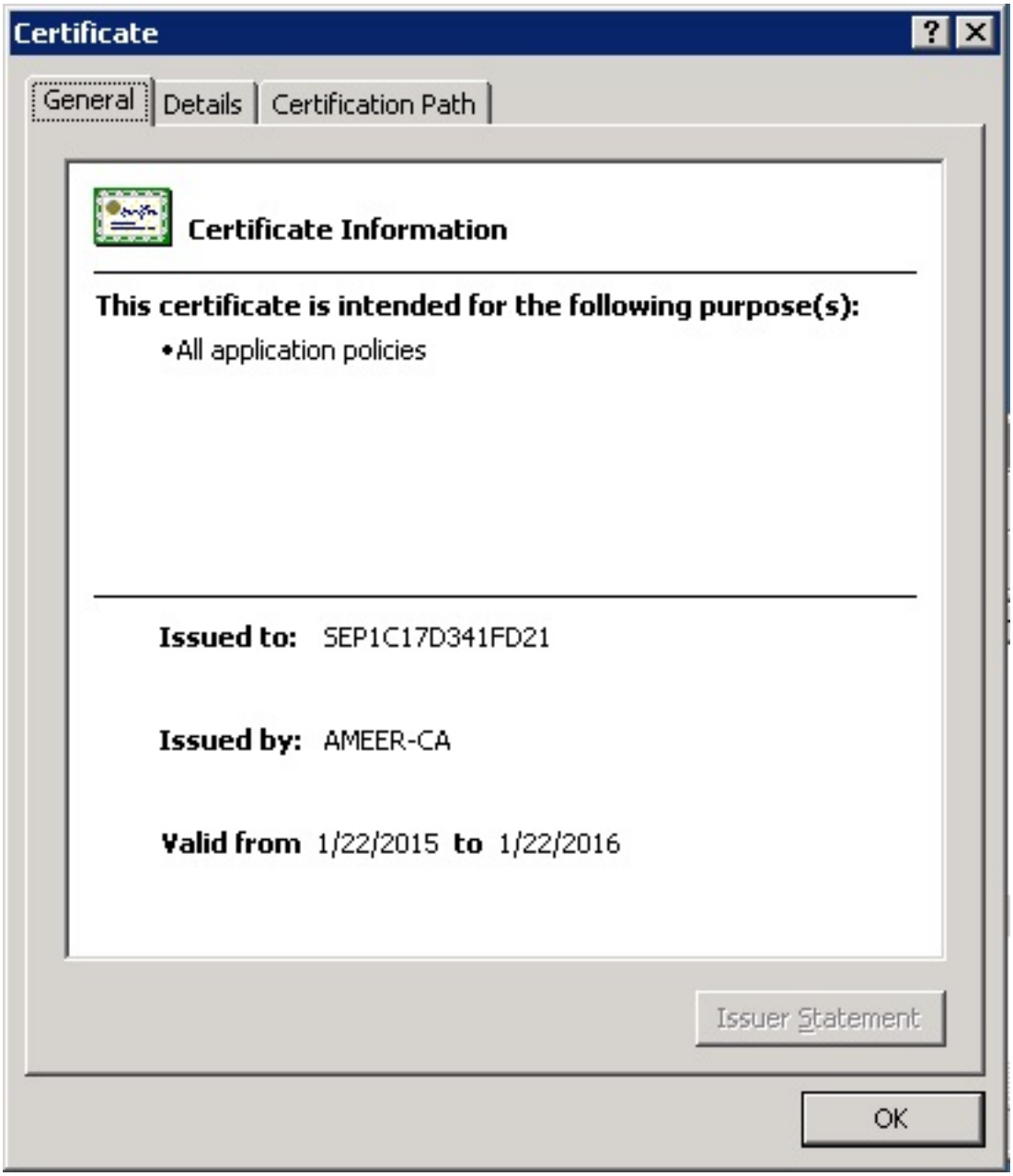


5. Um das Zertifikat herunterzuladen, wählen Sie **Ausgestelltes Zertifikat**.

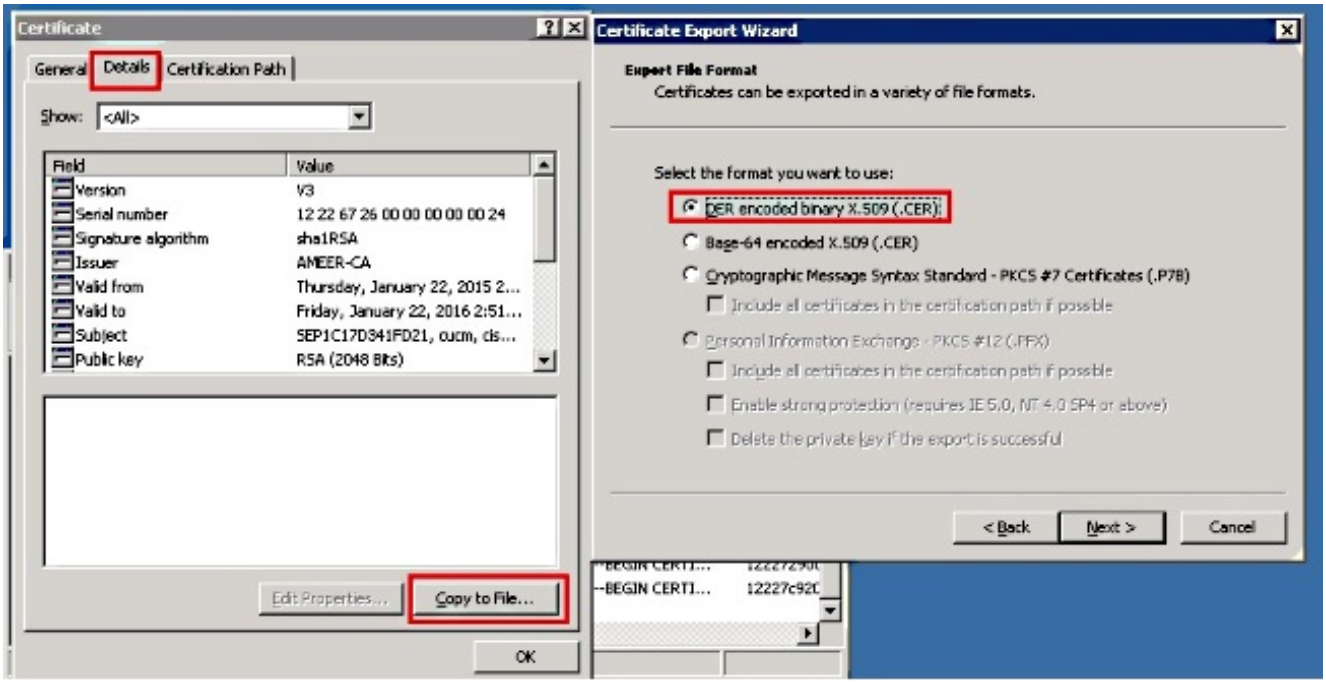
6. Klicken Sie mit der rechten Maustaste auf das Zertifikat, und klicken Sie auf **Öffnen**.



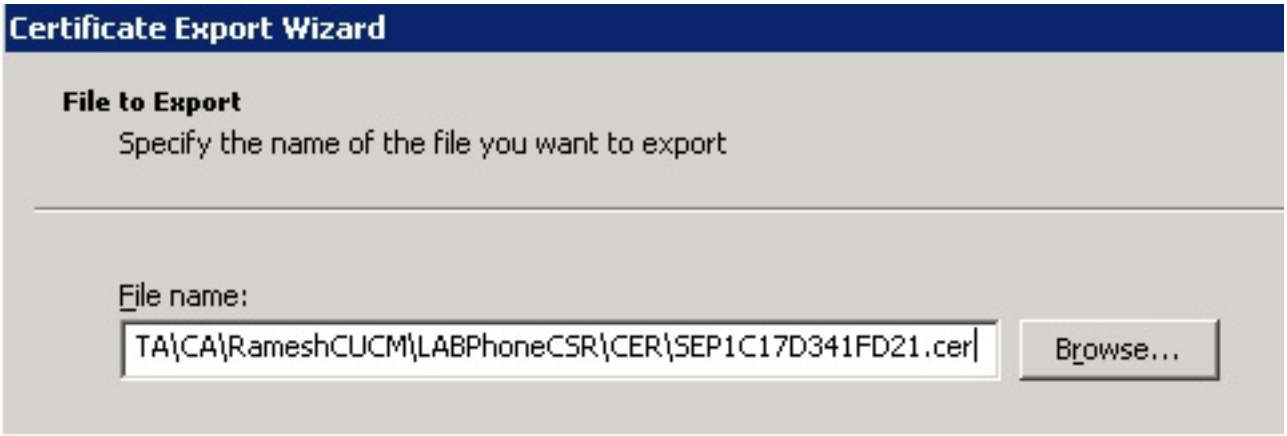
7. Sie können die Zertifikatdetails sehen. Um das Zertifikat herunterzuladen, wählen Sie die Registerkarte Details und anschließend **In Datei kopieren...**



8. Wählen Sie im Zertifikatexport-Assistenten die Option **DER-codierte binäre X.509 (.CER) aus**.



9. Geben Sie der Datei einen geeigneten Namen. In diesem Beispiel wird das Format <MAC>.cer verwendet.

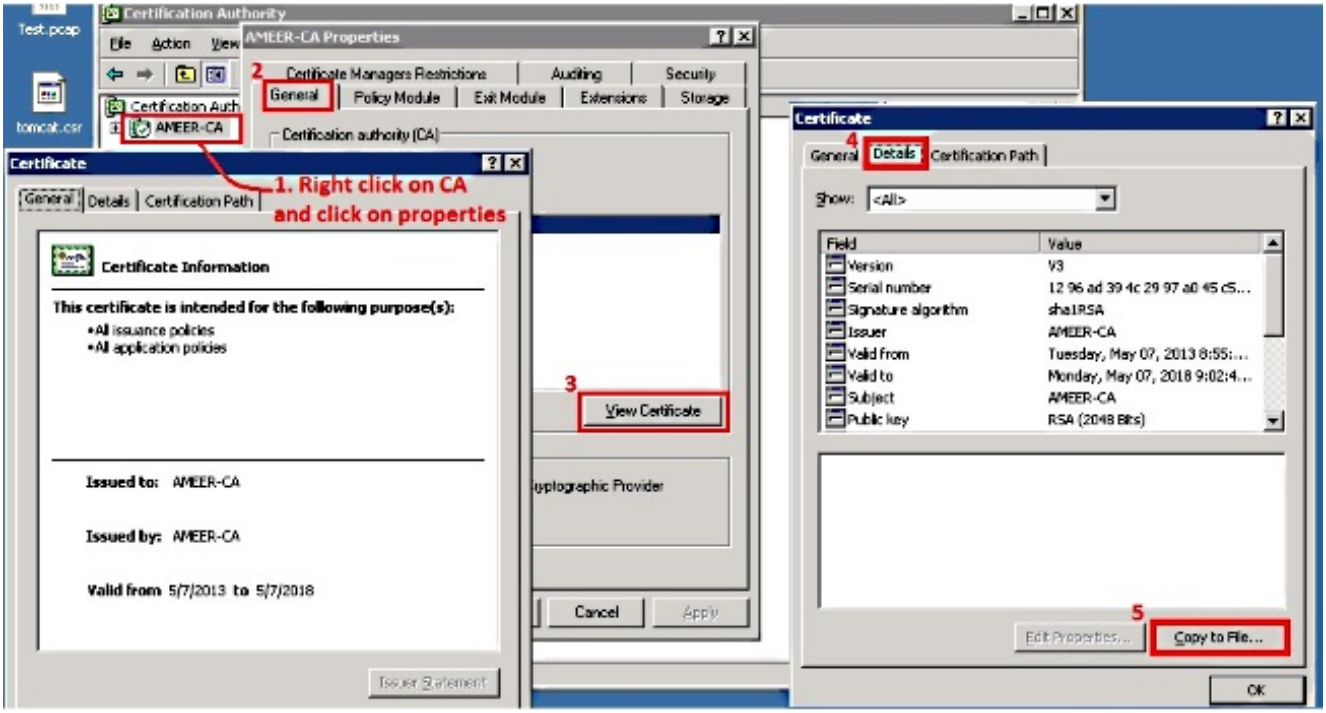


10. Rufen Sie mit diesem Verfahren die Zertifikate für andere Telefone im Abschnitt "Ausgestelltes Zertifikat" ab.

Stammzertifikat von der Zertifizierungsstelle abrufen

1. Offene **Zertifizierungsstelle**.

2. Führen Sie die in diesem Screenshot dargestellten Schritte aus, um die Root-CA herunterzuladen.

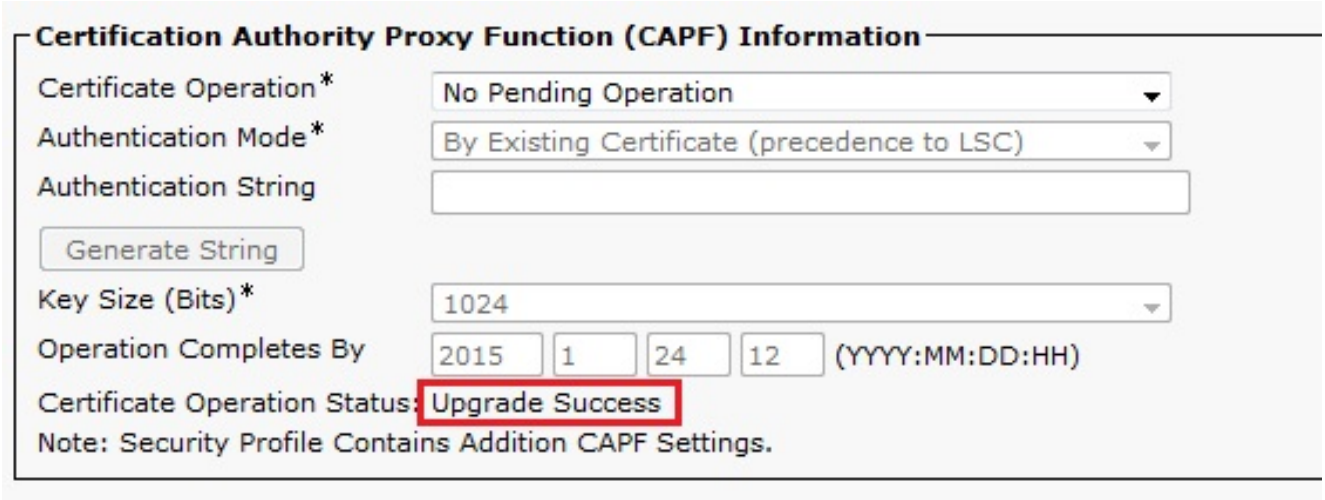


Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Rufen Sie die Seite für die Telefonkonfiguration auf.

2. Im Abschnitt "CAPF" sollte der Status des Zertifikatvorgangs als "**Upgrade Success" (Aktualisierung erfolgreich)** angezeigt werden.



Anmerkung: Weitere Informationen finden Sie unter Generate and Import Third Party CA-Signed LSCs.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.