CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定例

内容

概要

認証局プロキシ機能（CAPF）のローカルで有効な証明書（LSC）は、ローカルで署名が付けられます。ただし、電話機でサードパーティ認証局（CA）の署名付き LSC を使用しなければならない場合もあります。このドキュメントでは、その場合の手順について説明します。

前提条件

要件

このドキュメントの読者は Cisco Unified Communications Manager（CUCM）に関する知識を持っていることを推奨します。

使用するコンポーネント

このドキュメントの情報は、CUCM バージョン 10.5(2) に基づいています。ただし、ここで説明する機能はバージョン 10.0 以降で有効です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

この手順を構成するステップは次のとおりです。それぞれのステップについて、個別のセクションで詳しく説明します。

1. CA ルート証明書のアップロード
2. エンドポイントに対する証明書発行者としてのオフライン CA の設定
3. 電話機の証明書署名要求（CSR）の生成
4. FTP（または TFTP）サーバを介した Cisco Unified Communications Manager（CUCM）からの生成済み CSR の取得
5. CA からの電話機の証明書の取得
6. .cer から .der 形式への変換
7. .tgz 形式への証明書（.der）の圧縮
8. セキュア シェル FTP（SFTP）サーバへの .tgz ファイルの転送
9. CUCM サーバへの .tgz ファイルのインポート
10. Microsoft Windows 2003 認証局による CSR の署名
11. CA からのルート証明書の取得

CA ルート証明書のアップロード

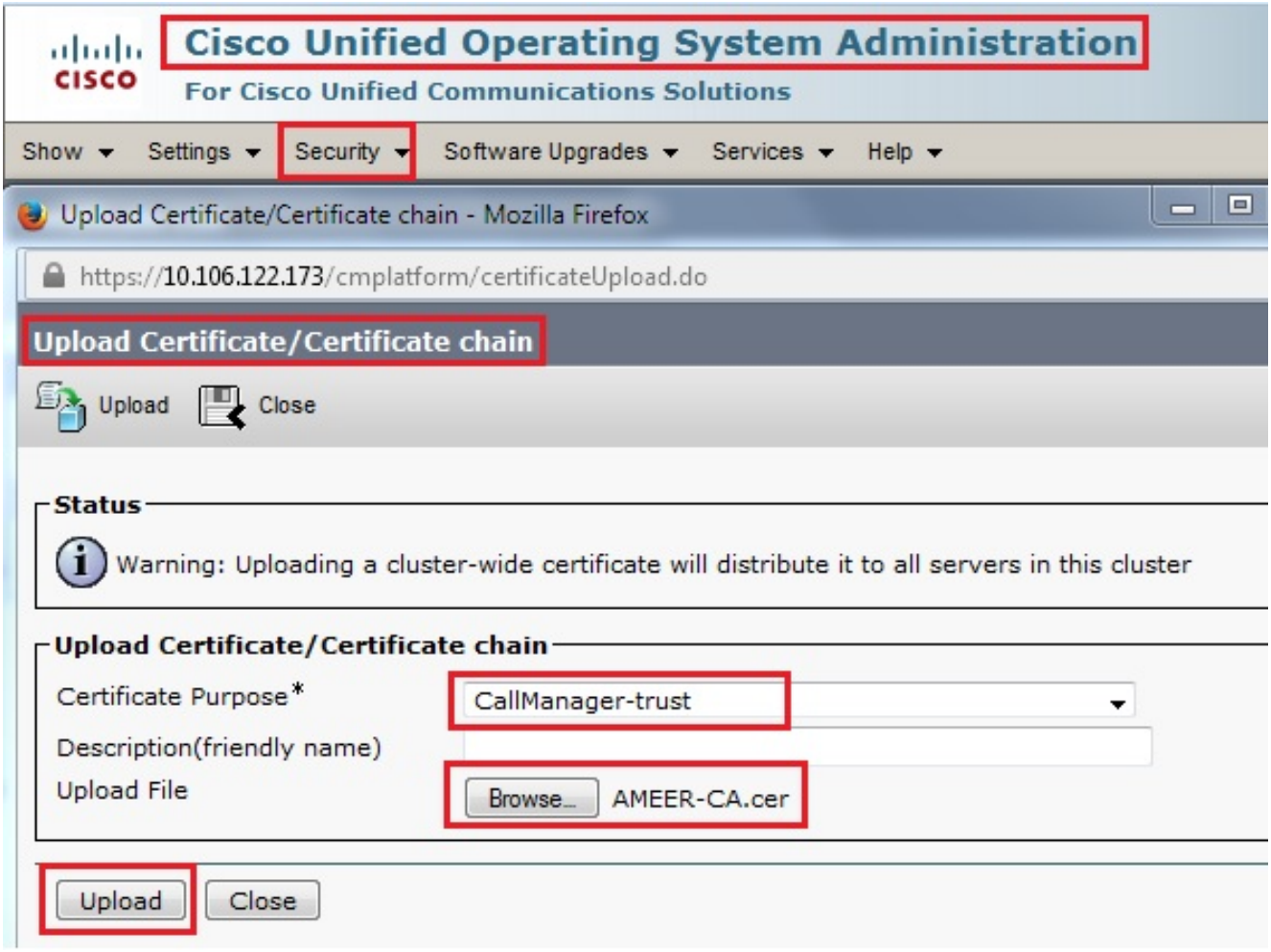
1. Cisco Unified Operating System（OS）管理 Web GUI にログインします。

2. [Security Certificate Management] に移動します。

3. [Upload Certificate/Certificate chain] をクリックします。

4. [Certificate Purpose] で [CallManager-trust] を選択します。

5. CA のルート証明書を参照し、[Upload] をクリックします。



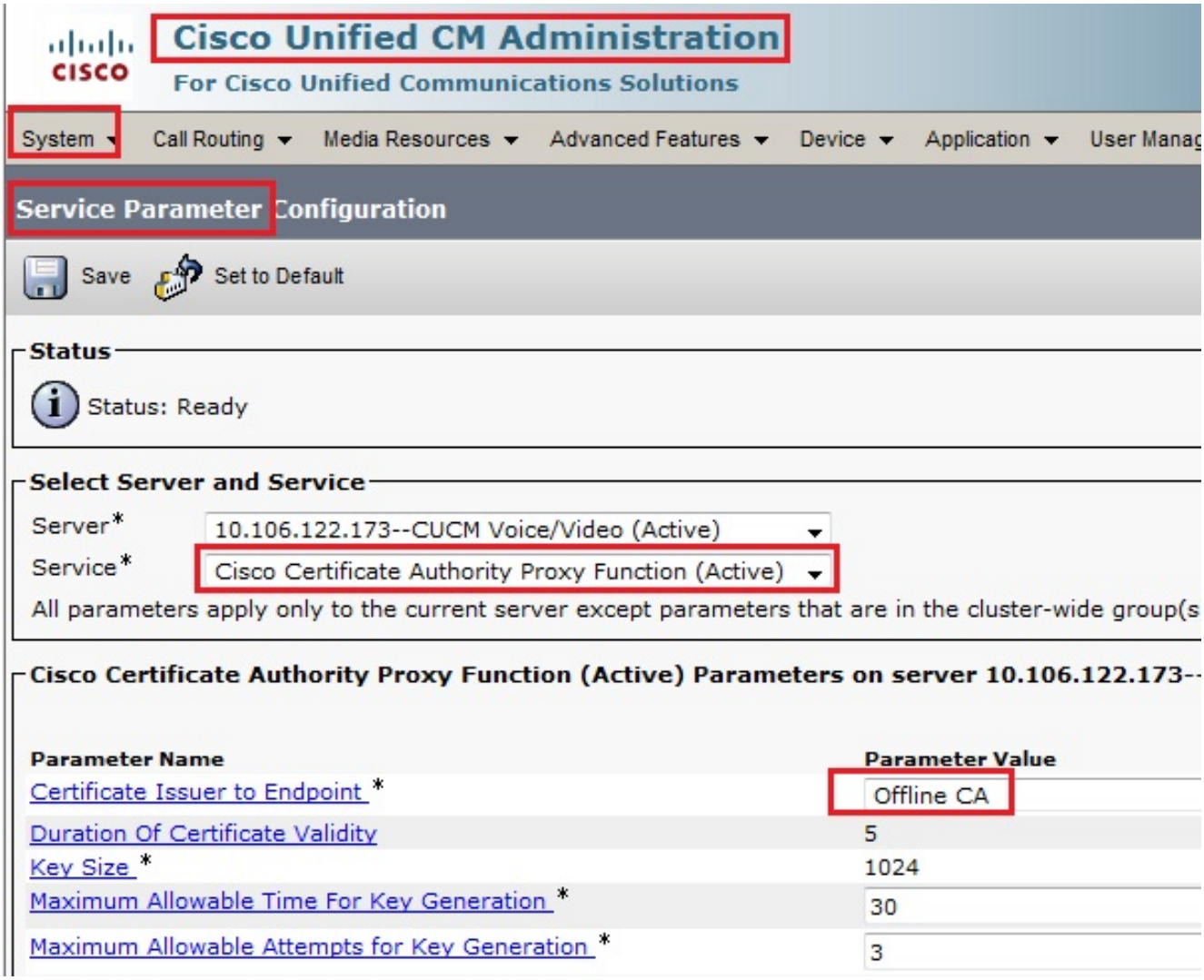
エンドポイントに対する証明書発行者としてのオフライン CA の設定

1. CUCM 管理 Web GUI にログインします。

2. [System] > [Service Parameters] に移動します。

3. CUCM サーバを選択し、[Service] として [Cisco Certificate Authority Proxy Function] を選択します。

4. [Certificate Issuer to Endpoint] で [Offline CA] を選択します。



電話機の証明書署名要求（CSR）の生成

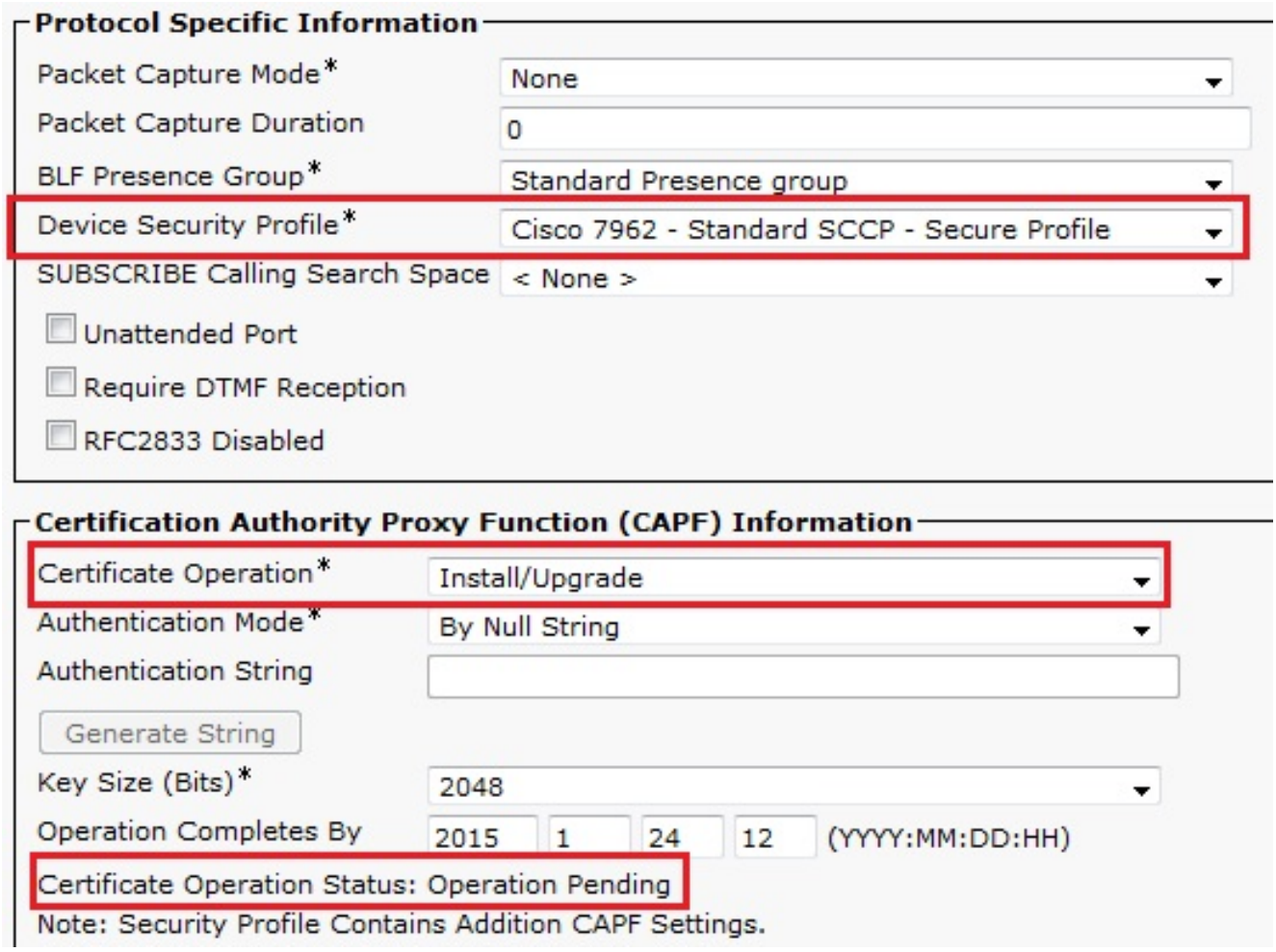
1. CUCM 管理 Web GUI にログインします。

2. [Device Phones] に移動します。

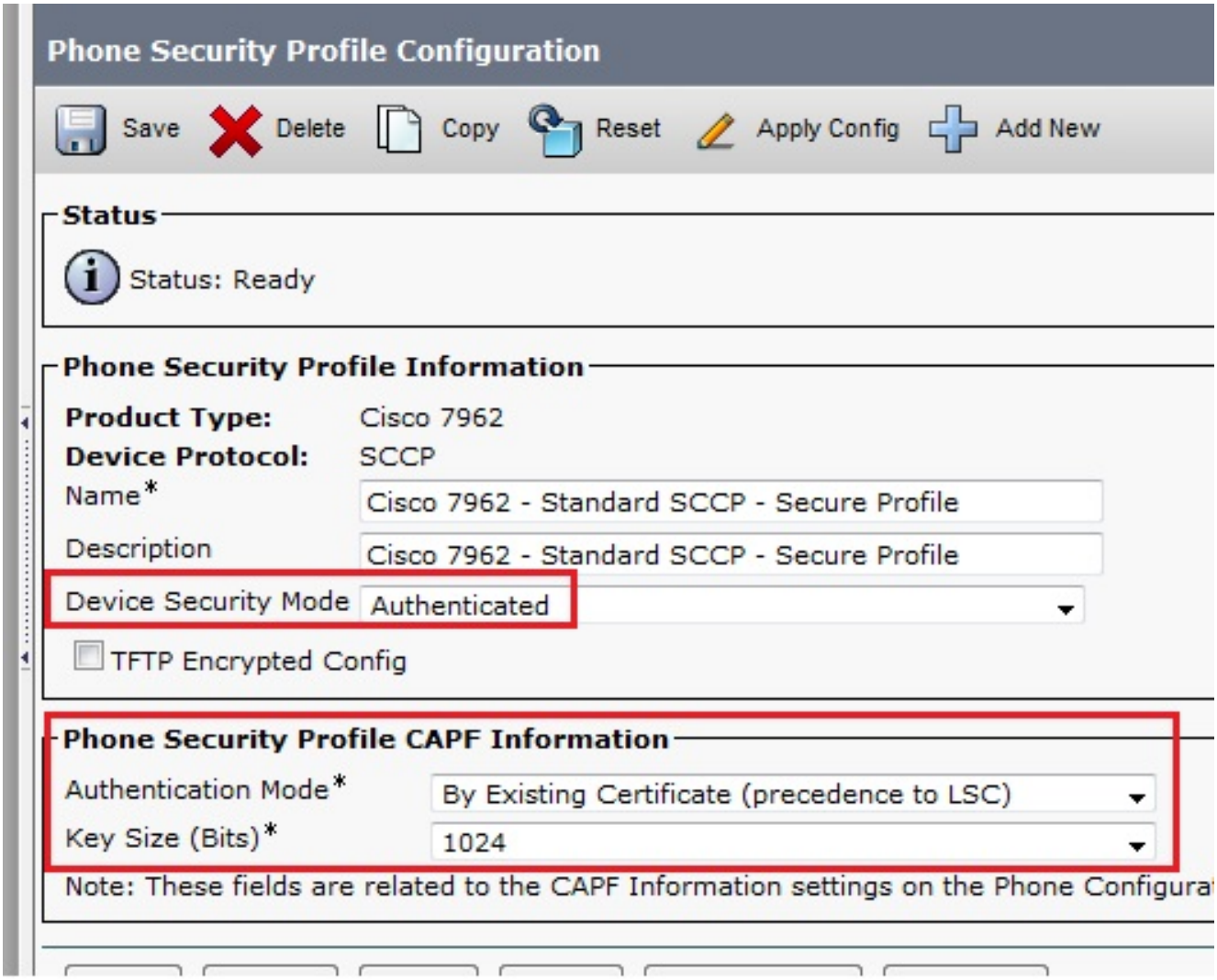
3. LSC に外部 CA による署名が必要な電話機を選択します。

4. [Device security profile] で、デバイス セキュリティ プロファイルを保護されたものに変更します（保護されたデバイス セキュリティ プロファイルがない場合は、[Phone Security Profile Configuration] で新規に追加してください）。

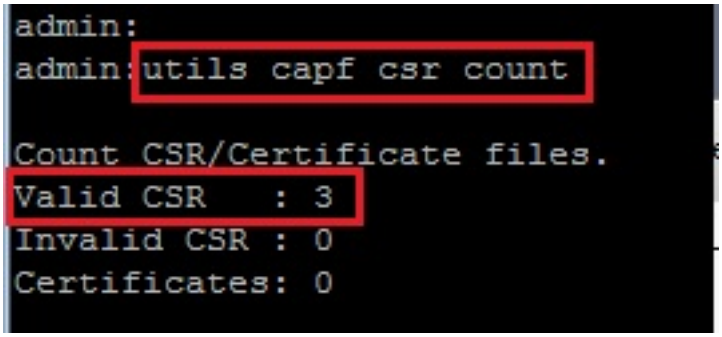
5. 電話機の設定ページにある [CAPF] セクションで、[Certification Operation] として [Install/Upgrade] を選択します。このステップを、LSC に外部 CA による署名が必要な電話機のすべてに対して行います。[Certificate Operation Status] には [Operation Pending] と表示されているはずです。



以下に、電話機のセキュリティ プロファイル（7962 モデル）を示します。



CSR が生成されるかどうかを確認するために、セキュア シェル（SSH）セッションで **utils capf csr count コマンドを入力します。**（次のスクリーン ショットには、3 台の電話機に対して CSR が生成されたことが示されています）。



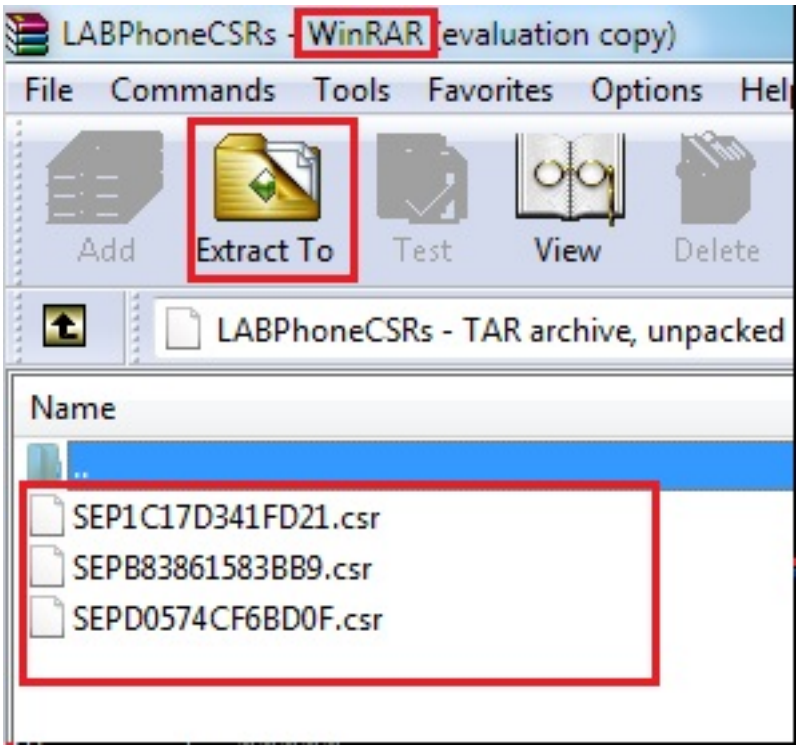
注：電話機の [CAPF] セクションにある [Certificate Operation Status] は、[Operation Pending] 状態のままになります。

FTP（または TFTP）サーバを介した CUCM からの生成済み CSR の取得

1. CUCM サーバに SSH でログインします。
2. **utils capf csr dump コマンドを実行します。**このスクリーン ショットには、FTP に転送中のダンプが示されています。

```
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. ダンプ ファイルを開き、WinRAR を使用して CSR をローカル マシンに抽出します。



電話機の証明書の取得

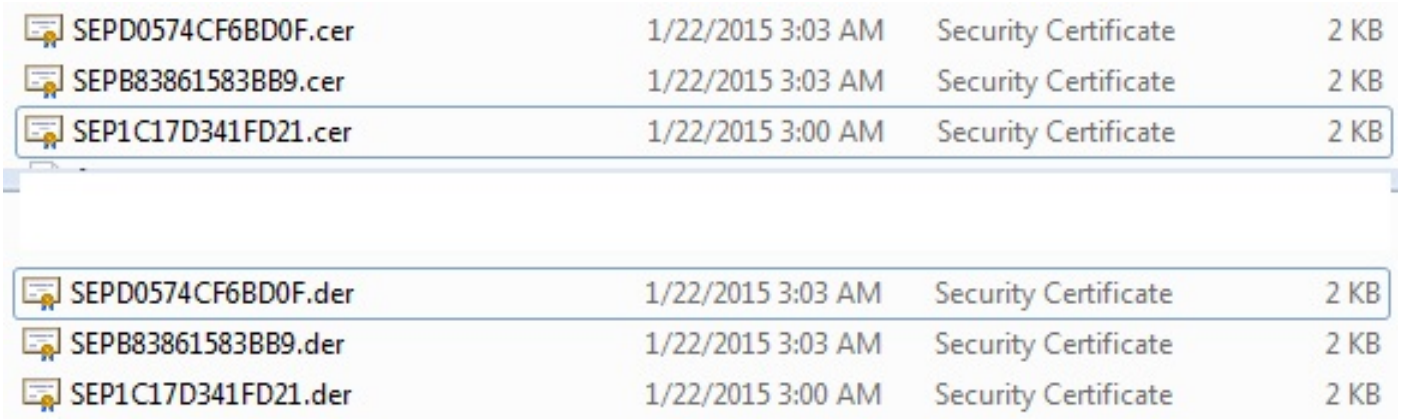
1. 電話機の CSR を CA に送信します。

2. CA によって署名付き証明書が提供されます。

注：CA. として Microsoft Windows 2003 サーバを使用できます。Microsft Windows 2003 CA で CSR に署名を付けるための手順は、このドキュメントの後半で説明します。

.cer から .der 形式への変換

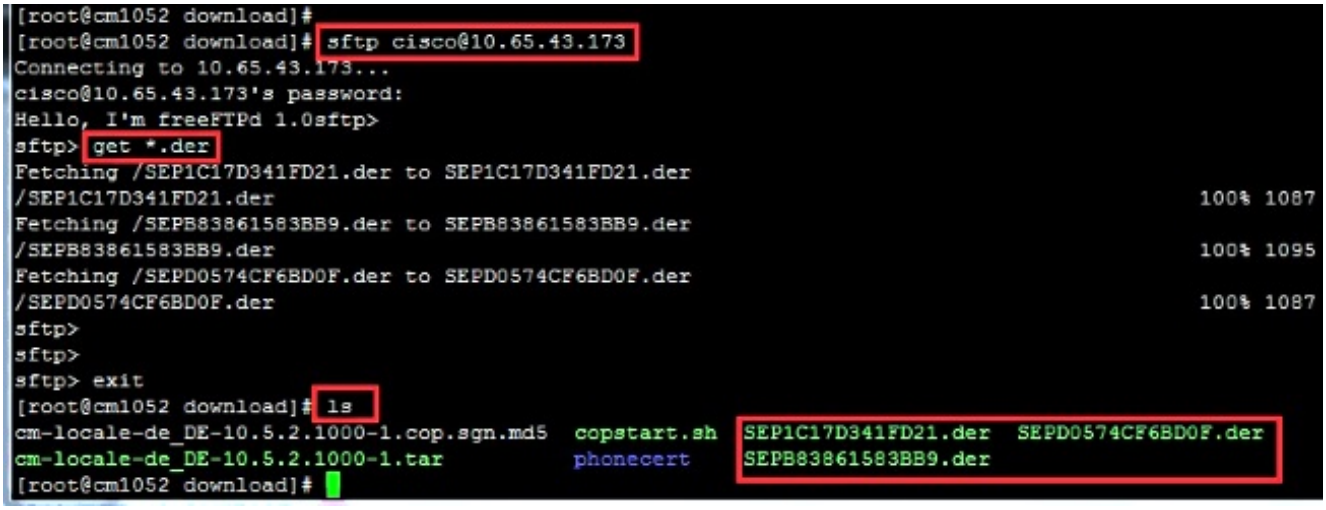
受信した証明書が .cer 形式になっている場合は、ファイル名を .der に変更します。



.tgz 形式への証明書（.der）の圧縮

証明書を圧縮形式にするには、CUCM サーバのルート（Linux）を使用できます。この手順は、通常の Linux システムでも実行できます。

1. SFTP サーバを使用して、すべての署名付き証明書を Linux システムに転送します。



2. 次のコマンドを入力して、すべての .der 証明書を .tgz ファイルに圧縮します。

```
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]#
```

SFTP サーバへの .tgz ファイルの転送

次のスクリーン ショットに示すステップを実行して、.tgz ファイルを SFTP サーバに転送します。

```
[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>
```

CUCM サーバへの .tgz ファイルのインポート

1. CUCM サーバに SSH でログインします。
2. **utils capf cert import コマンドを実行します。**

```
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
```

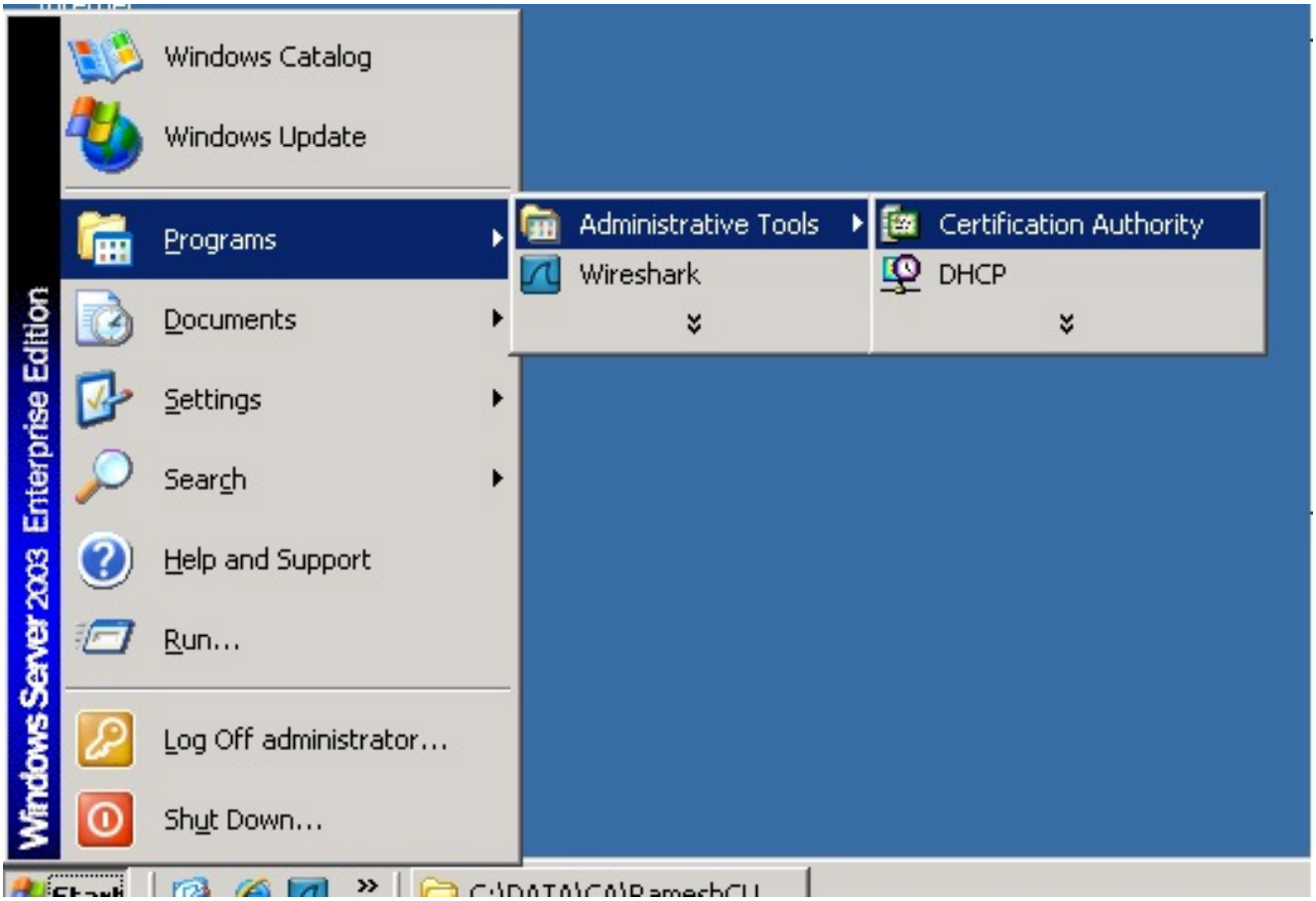
証明書が正常にインポートされると、CSR カウントの値がゼロになります。

```
admin:
admin:utils capf csr count

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

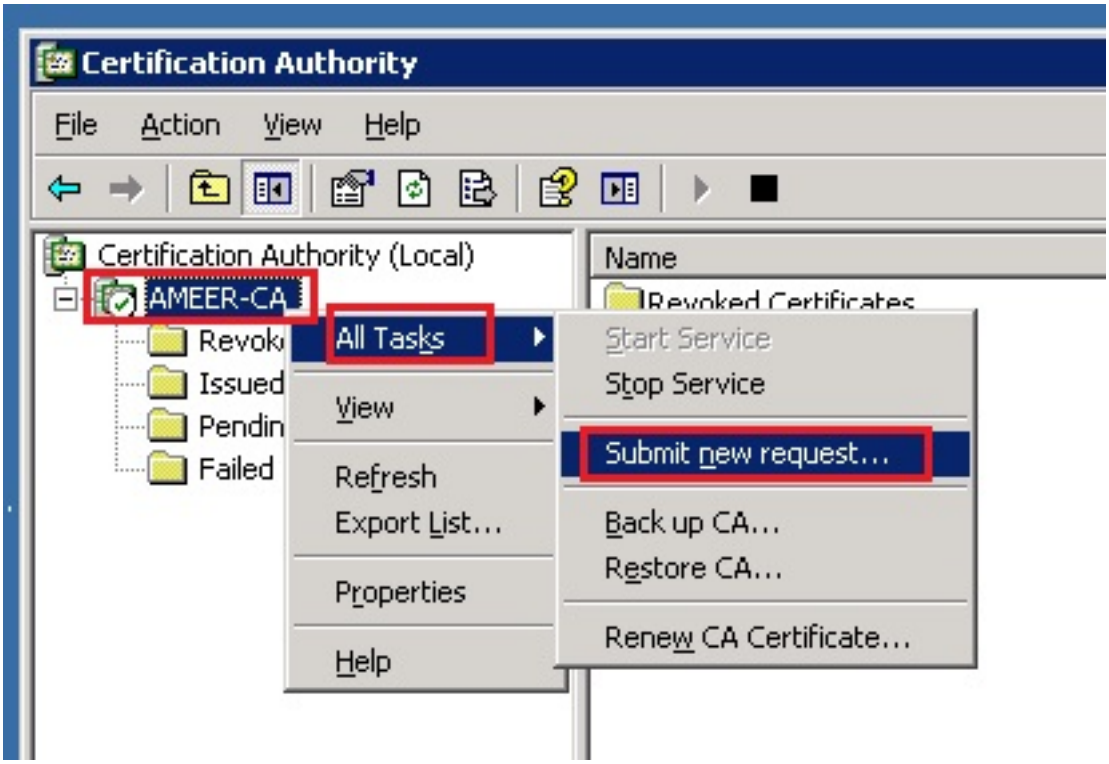
Microsoft Windows 2003 認証局による CSR の署名

この手順は、Microsoft Windows 2003 を CA として使用する場合に実行します。

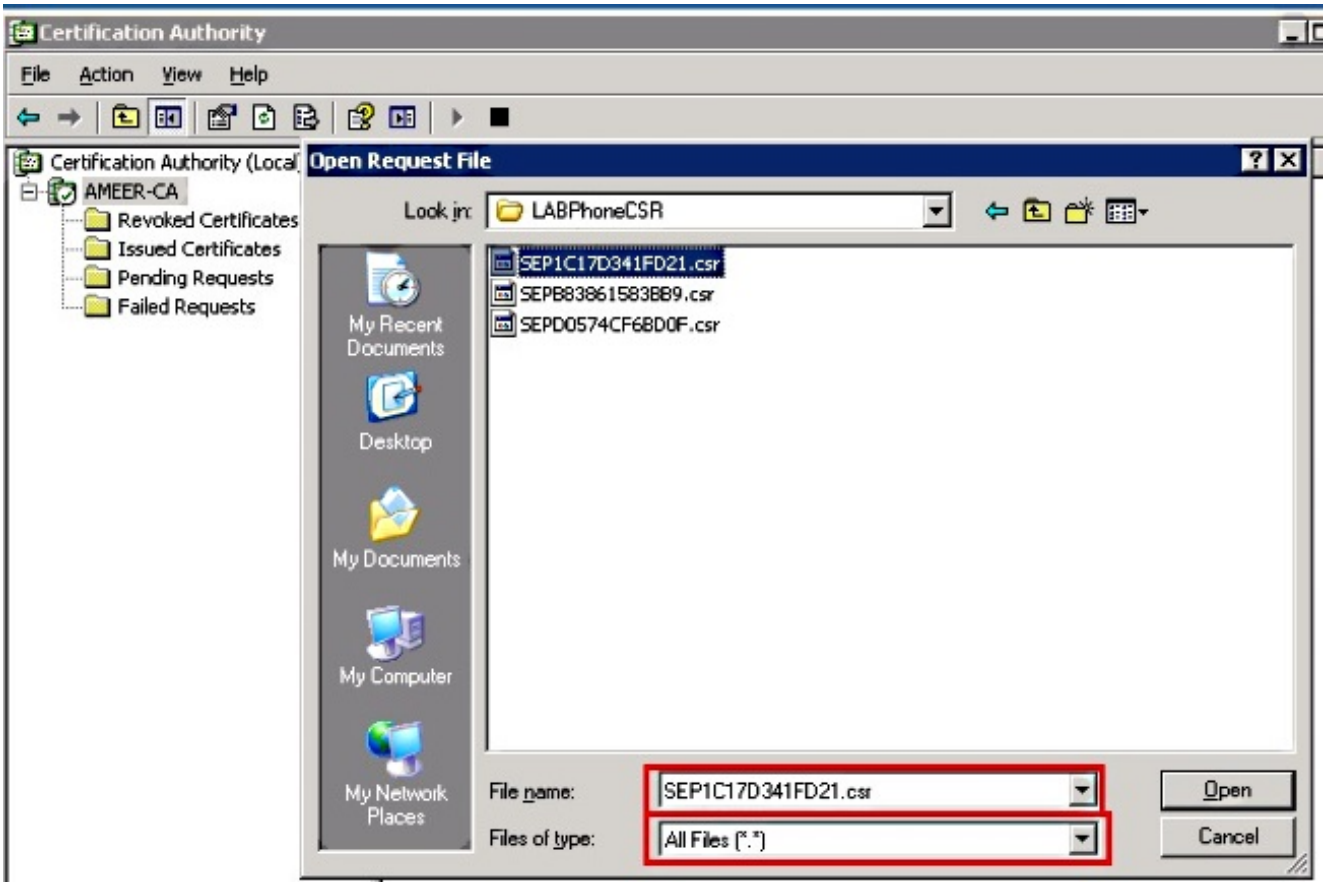
1. [Certification Authority] を開きます。



2. CA を右クリックし、[All Tasks] > [Submit new request...] に移動します。

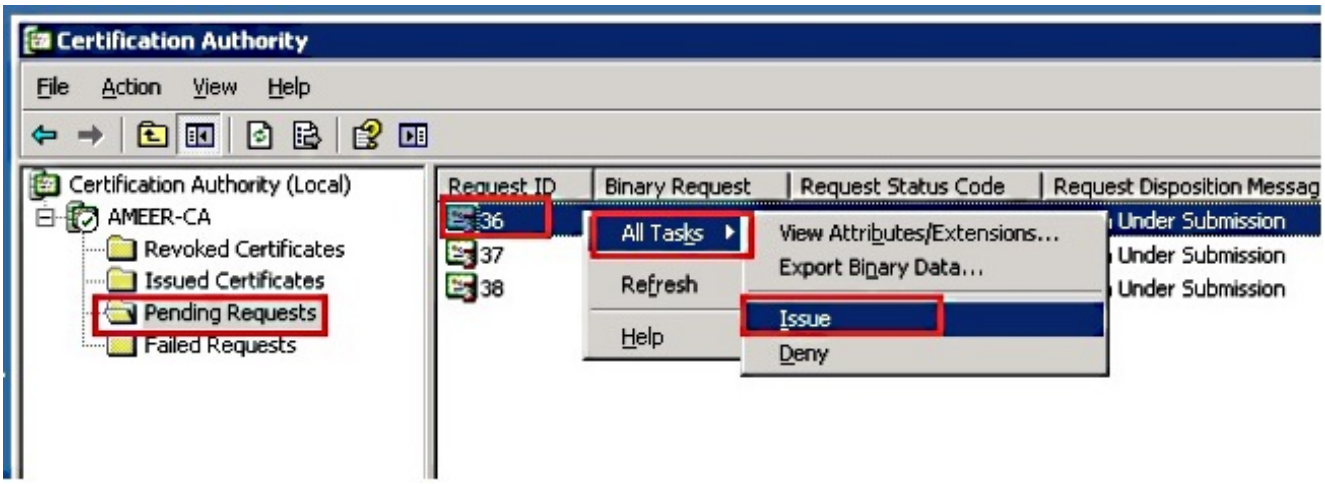


3. CSR を選択して [Open] をクリックします。すべての CSR に対して、この操作を行います。



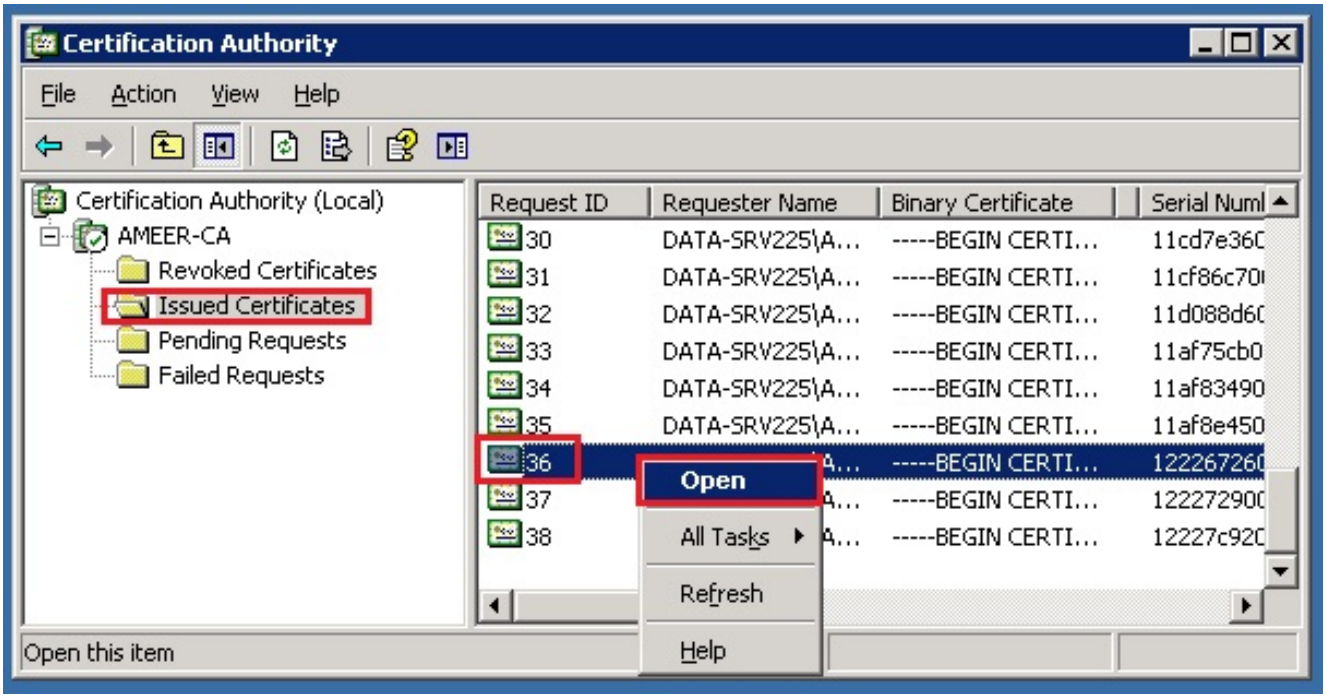
開いた CSR がすべて、[Pending Requests] フォルダ内に表示されます。

4. それぞれを右クリックし、[All Tasks] > [Issue] に移動します。保留中のすべてのリクエストに対して、この操作を行います。

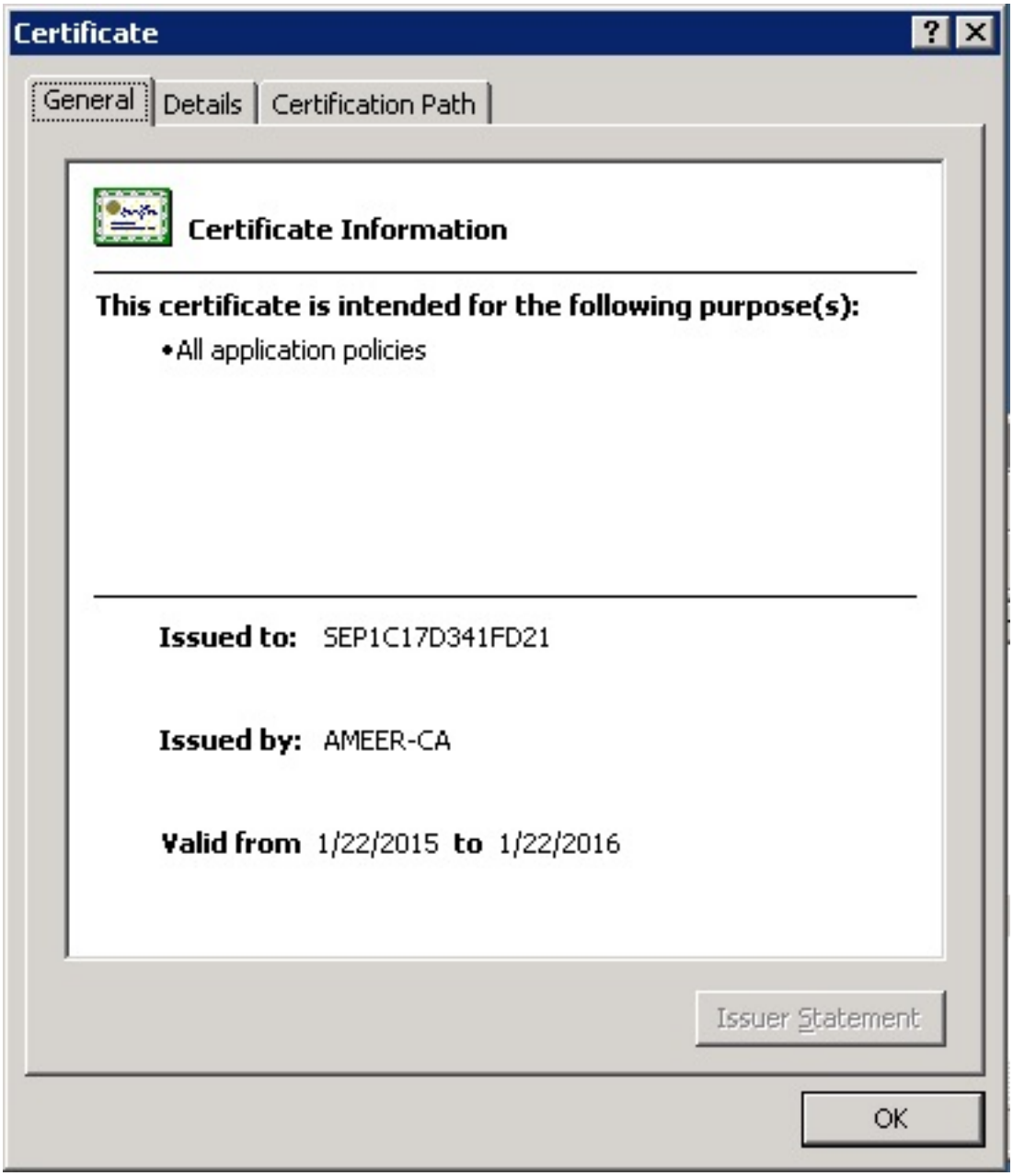


5. 証明書をダウンロードするために、[Issued Certificate] を選択します。

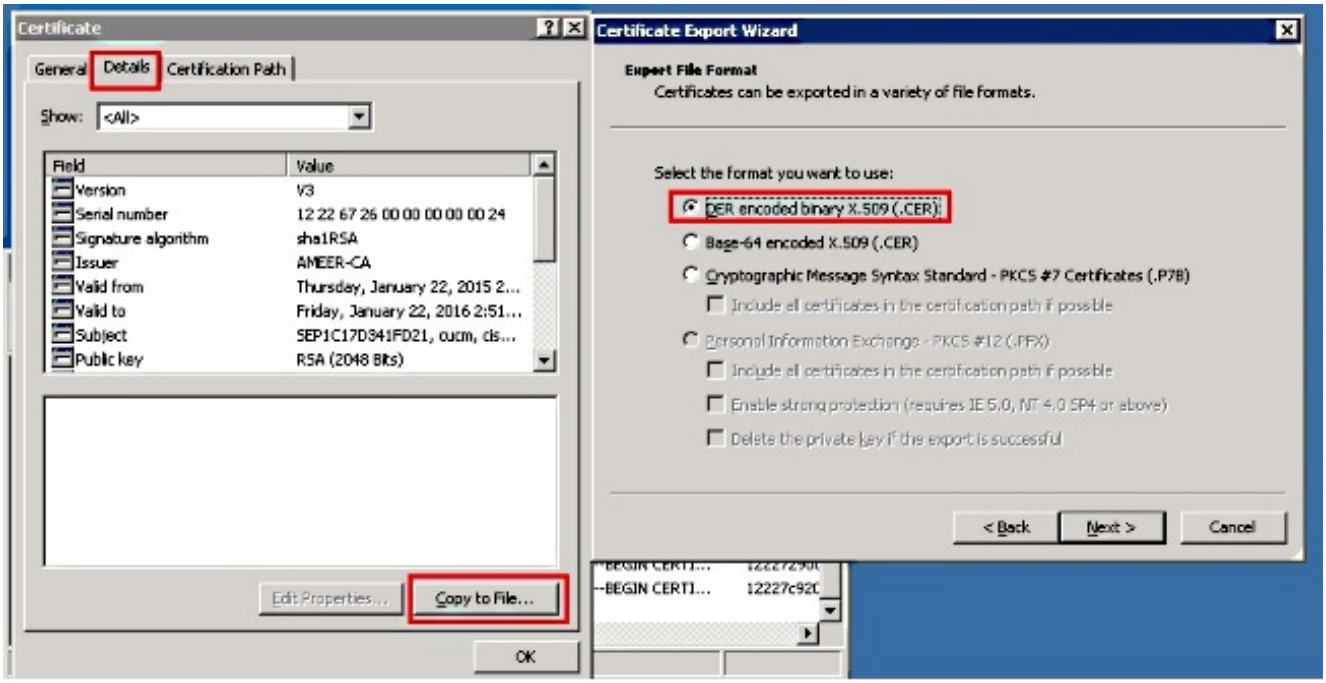
6. 証明書を右をクリックし、[Open] をクリックします。



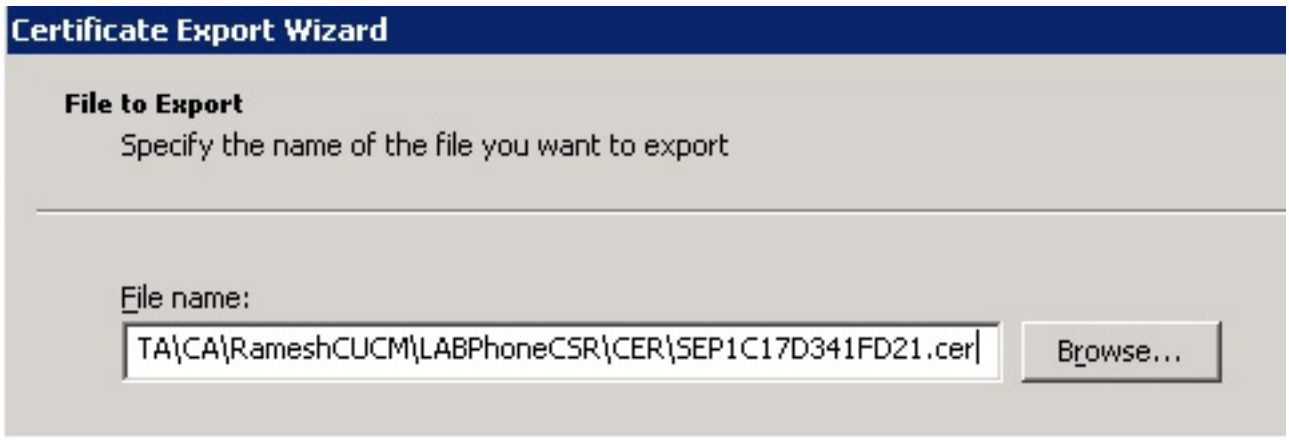
7. 証明書の詳細が表示されます。証明書をダウンロードするには、[Details] タブを選択し、[Copy to File...] を選択します。



8. [Certificate Export Wizard] で、[DER encoded binary X.509 (.CER)] を選択します。



9. ファイルに適切な名前を付けます。この例では、<MAC>.cer 形式を使用します。

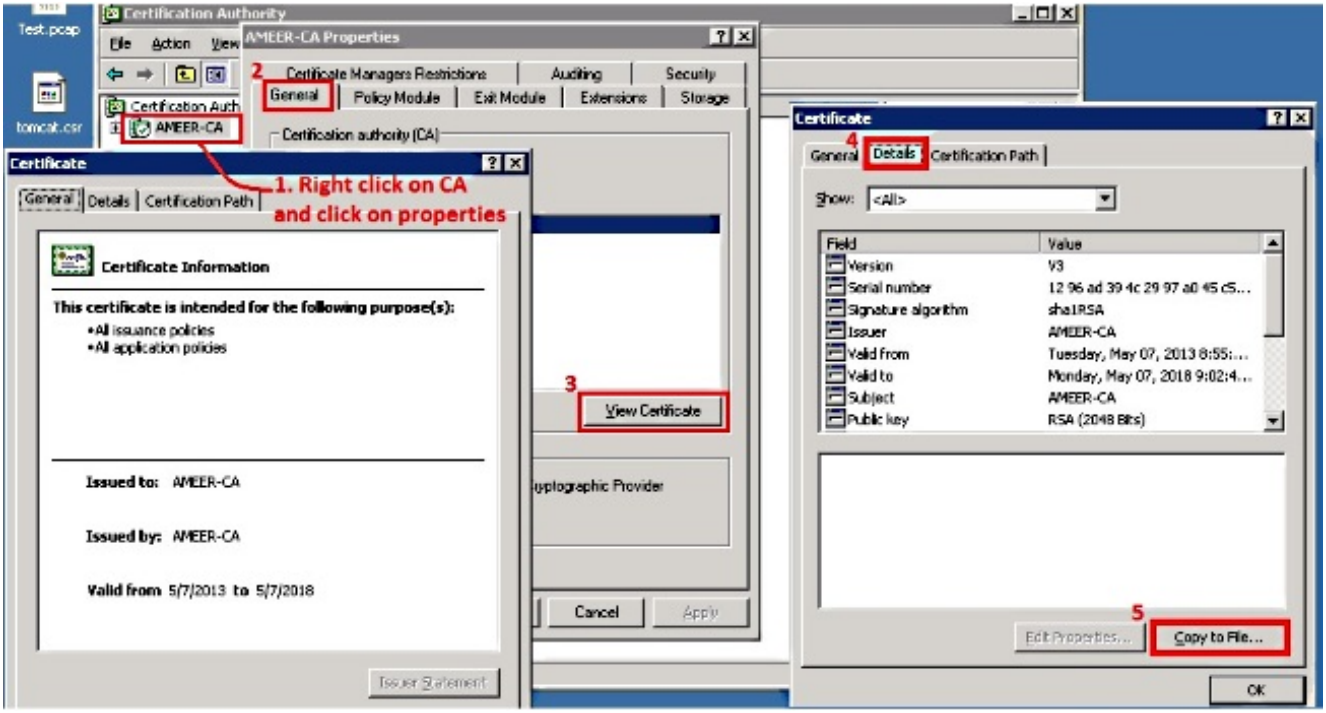


10. 以上の手順を使用して、[Issued Certificate] セクションに表示されている他の電話機の証明書を取得します。

CA からのルート証明書の取得

1. [Certification Authority] を開きます。

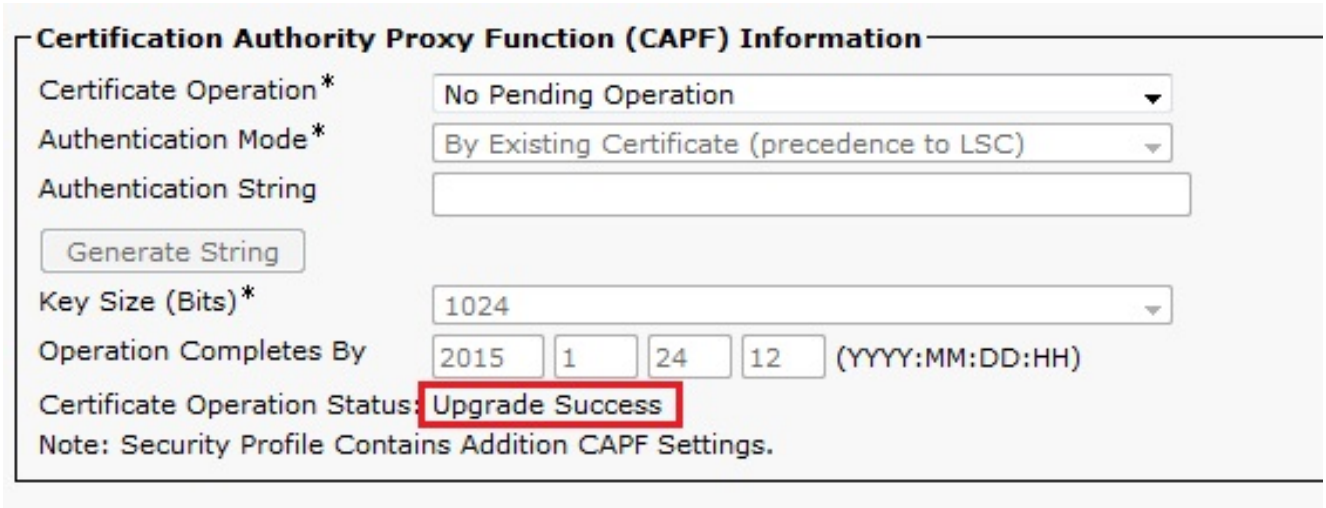
2. 次のスクリーン ショットに示すステップを実行して、ルート CA をダウンロードします。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. 電話機の設定ページに移動します。
2. [CAPF] セクションで、[Certificate Operation Status] に [Upgrade Success] と表示されていることを確認します。



注：詳細については、サードパーティ CA 署名付き LSC の生成を参照してください。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。