CUCM 서드파티 CA 서명 LSC 생성 및 가져오기 컨피그레이션 예

목차

소개

CAPF(Certificate Authority Proxy Function) LSC(Locally Significant Certificates)는 로컬로 서명됩니다. 그러나 전화기에서 서드파티 CA(Certificate Authority) 서명 LSC를 사용해야 할 수도 있습니다. 이 문서에서는 이를 수행하는 데 도움이 되는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 CUCM(Cisco Unified Communication Manager)에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 CUCM 버전 10.5(2)를 기반으로 합니다. 그러나 이 기능은 버전 10.0 이상에서 작동합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 절차와 관련된 단계는 다음과 같습니다. 각 단계는 해당 섹션에 자세히 설명되어 있습니다.

1. CA 루트 인증서 업로드
2. 인증서 문제에 대한 오프라인 CA를 엔드포인트로 설정
3. 전화기에 대한 CSR(Certificate Signing Request) 생성
4. 생성된 CSR을 CUCM(Cisco Unified Communications Manager)에서 FTP 서버로 가져옵니다.
5. CA에서 전화 인증서 가져오기
6. .cer을 .der 형식으로 변환
7. 인증서(.der)를 .tgz 형식으로 압축
8. .tgz 파일을 SFTP(Secure Shell FTP) 서버로 전송합니다.
9. CUCM 서버로 .tgz 파일 가져오기
10. Microsoft Windows 2003 Certificate Authority로 CSR 서명
11. CA에서 루트 인증서 가져오기

CA 루트 인증서 업로드

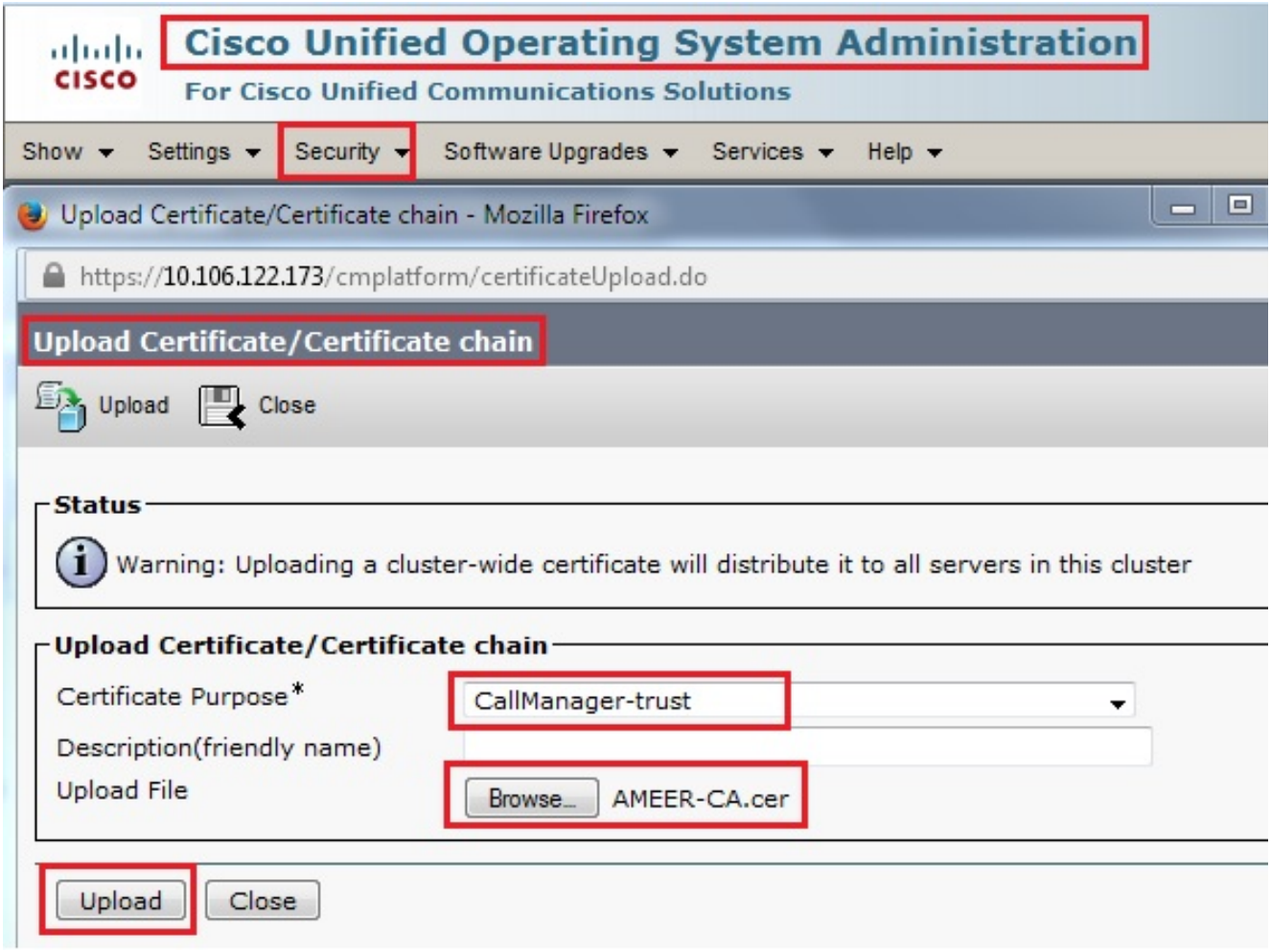
1. Cisco Unified OS(Operating System) 관리 웹 GUI에 로그인합니다.

2. **Security Certificate Management(보안 인증서 관리)로** 이동합니다.

3. Upload **Certificate/Certificate chain을 클릭합니다**.

4. Certificate Purpose(인증서 용도) 아래에서 **CallManager-trust를** 선택합니다.

5. CA의 루트 인증서를 찾아 Upload(업로드)를 **클릭합니다**.



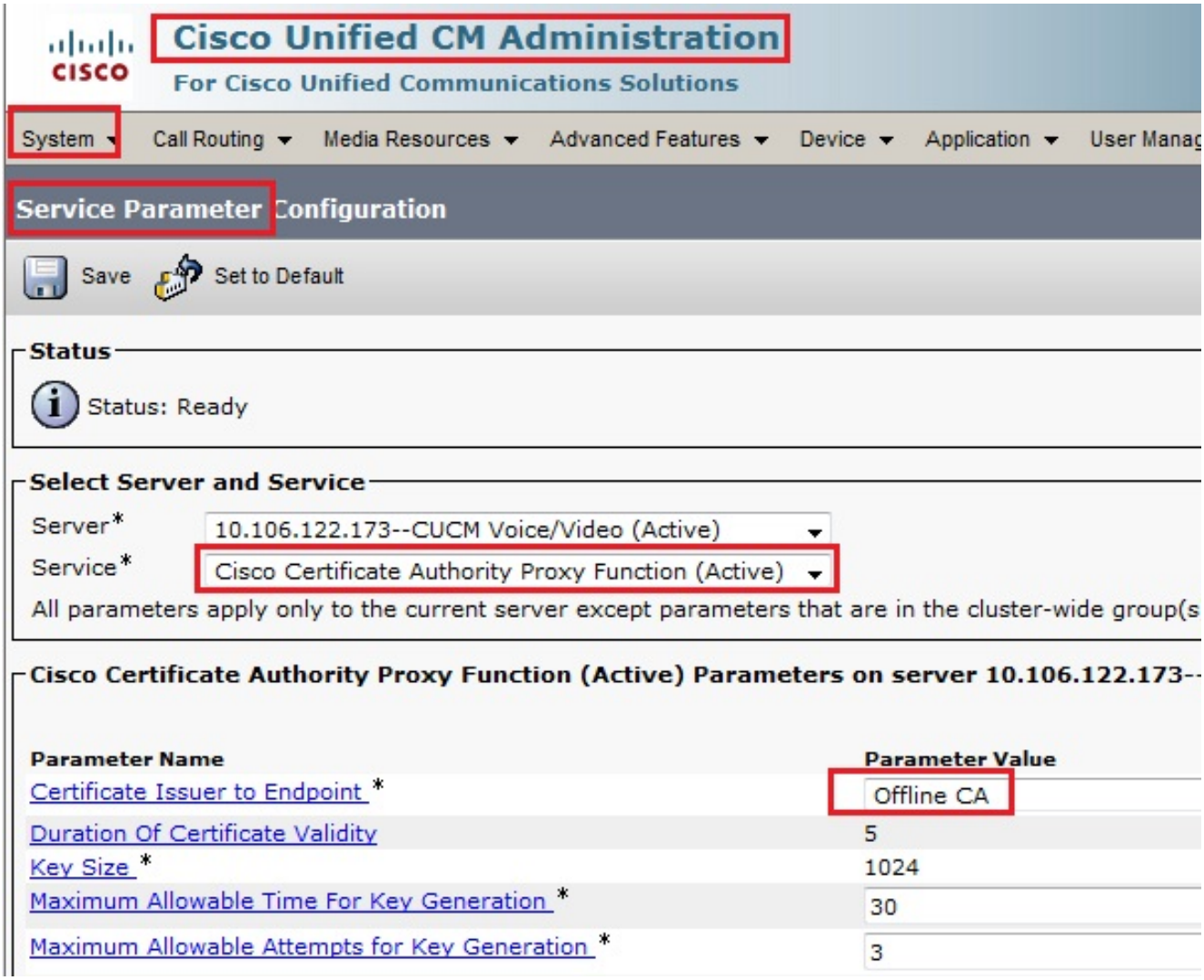
인증서 문제에 대한 오프라인 CA를 엔드포인트로 설정

1. CUCM 관리 웹 GUI에 로그인합니다.

2. **System > Service Parameter**로 **이동합니다**.

3. CUCM Server(CUCM 서버)를 선택하고 서비스에 대한 **Cisco Certificate Authority Proxy** Function(**Cisco Certificate Authority 프록시 기능**)을 선택합니다.

4. 엔드포인트에 대한 인증서 발급에 대해 **오프라인 CA**를 선택합니다.



전화기에 대한 CSR(Certificate Signing Request) 생성

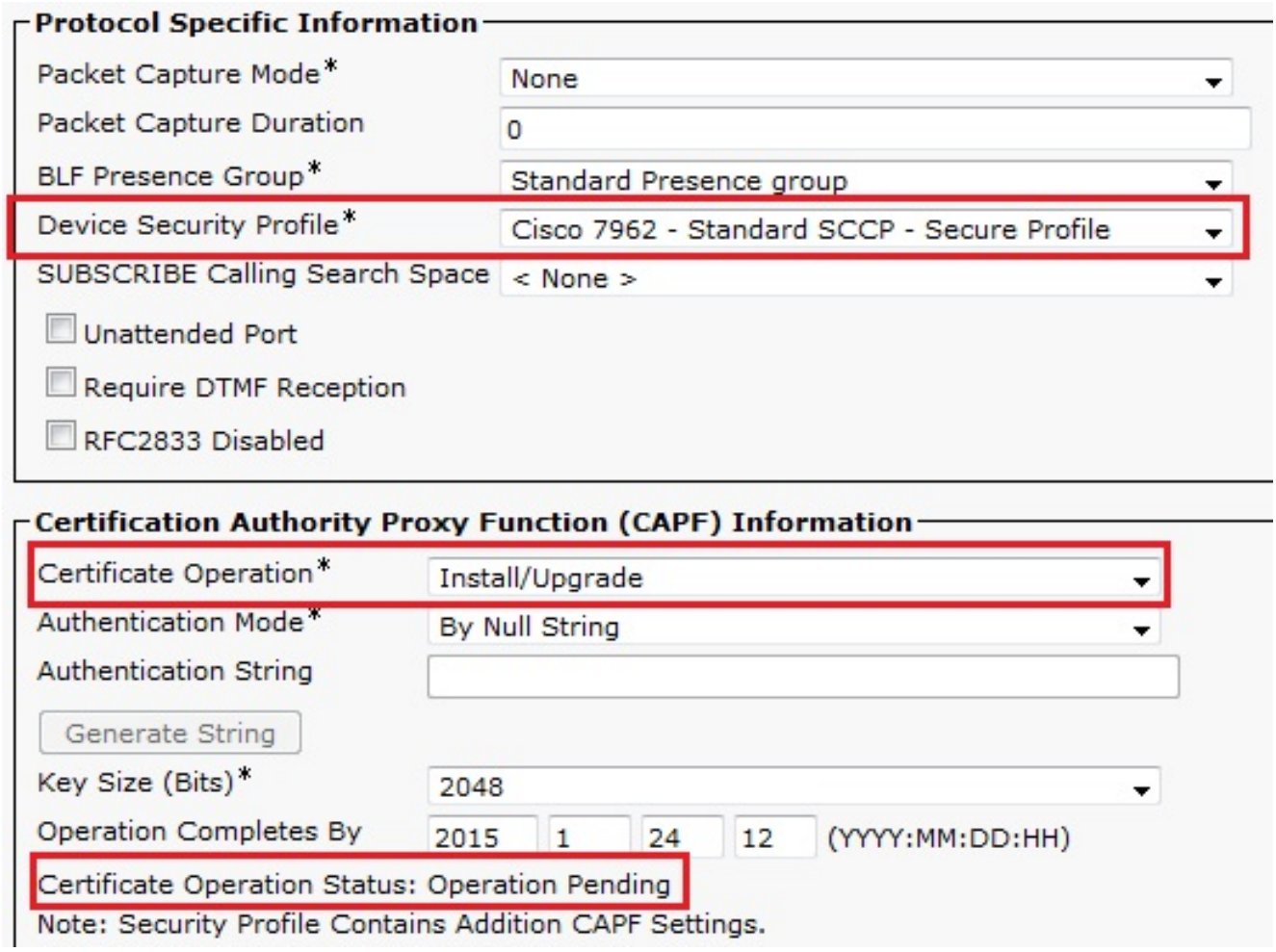
1. CUCM 관리 웹 GUI에 로그인합니다.

2. Device Phones(디바이스 **폰)로 이동합니다**.

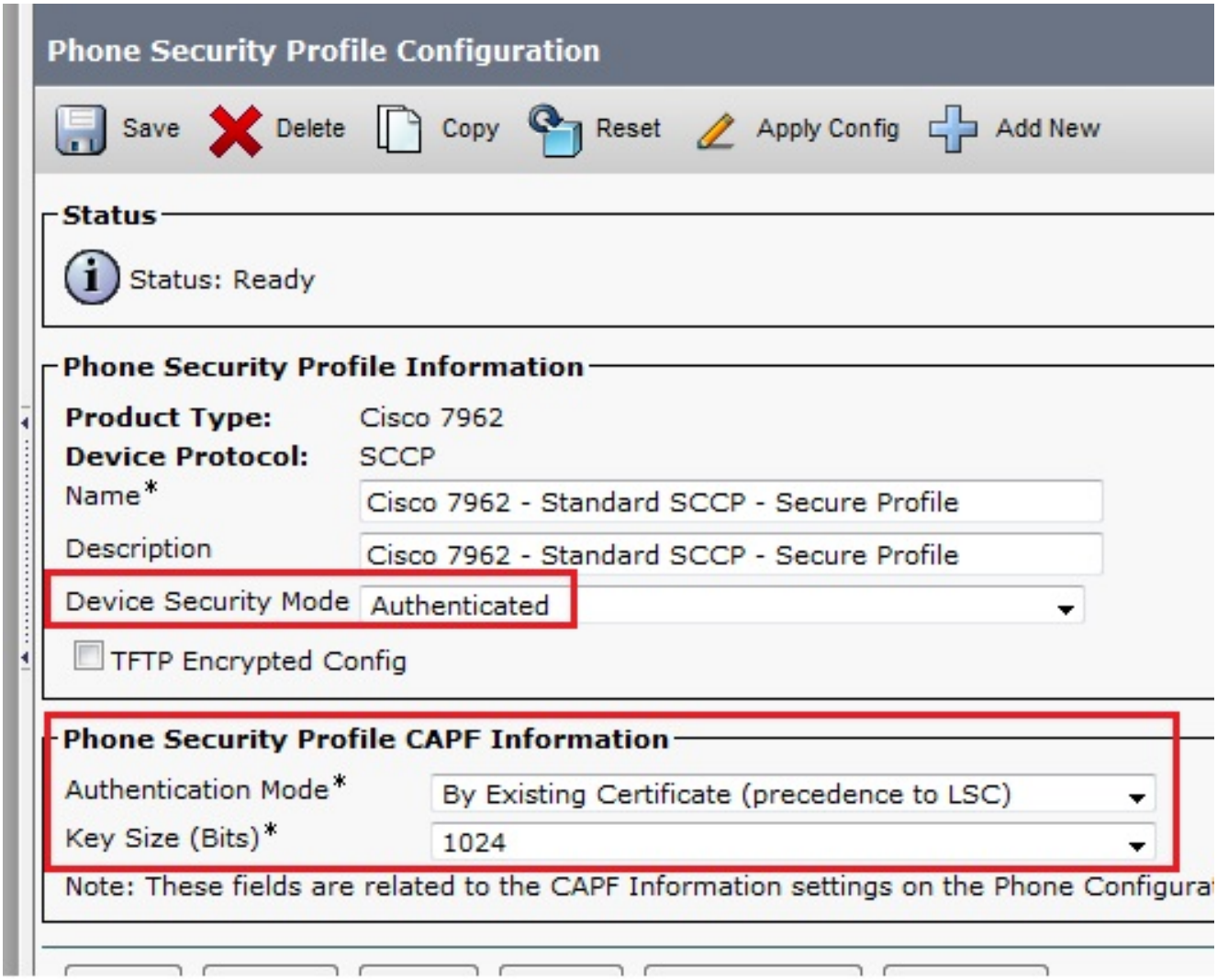
3. LSC가 외부 CA에 의해 서명되어야 하는 전화기를 선택합니다.

4. 장치 보안 프로필을 보안 프로필로 변경합니다(없는 경우 보안 전화 보안 프로필에 하나의 시스템 추가).

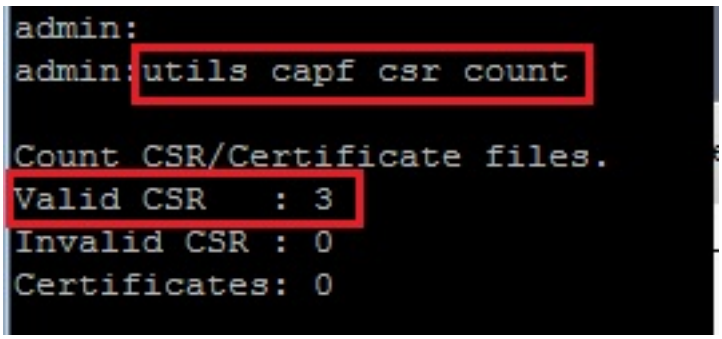
5. Phone Configuration(전화기 컨피그레이션) 페이지의 CAPF(CAPF) 섹션에서 Install/**Upgrade** for the Certification Operation(인증 작업 설치/업그레이드)을 선택합니다. LSC가 외부 CA에 의해 서명되어야 하는 모든 전화기에 대해 이 단계를 완료합니다. 인증서 작업 상태**에** 대한 작업 **보류** 상태가 표시됩니다.



전화 보안 프로파일(7962 모델)



CSR이 **생성되었는지** 확인하려면 SSH(Secure Shell) 세션에서 utils capf csr count 명령을 입력합니다. (이 스크린샷은 세 전화기에 대해 CSR이 생성되었음을 보여줍니다.)



참고: 전화의 CAPF 섹션에 있는 인증서 작업 상태는 **작업 보류 중 상태로** 유지됩니다.

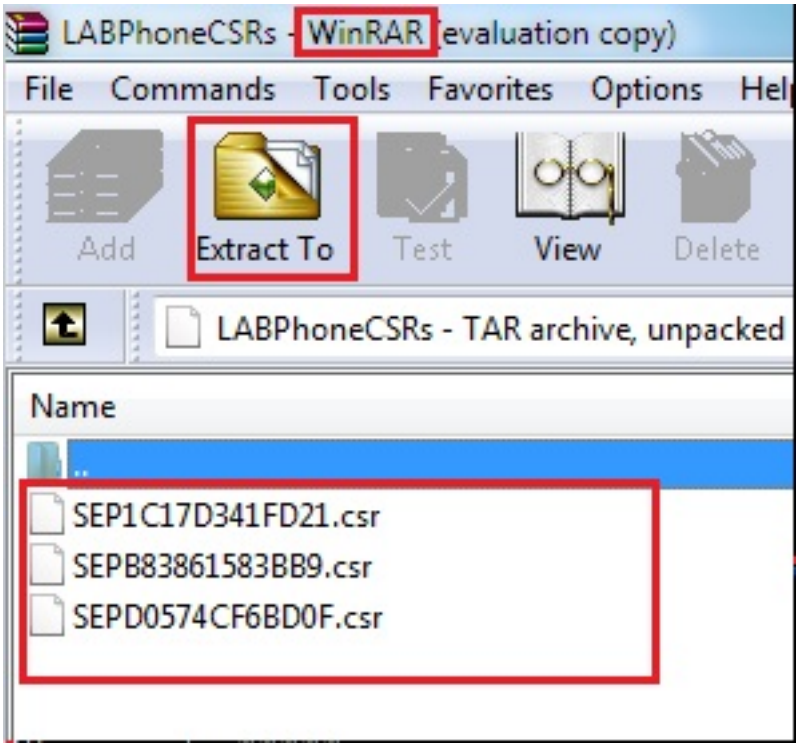
생성된 CSR을 CUCM에서 FTP(또는 TFTP) 서버로 가져옵니다.

1. CUCM 서버에 SSH를 적용합니다.

2. utils capf **csr dump 명령을** 실행합니다. 이 스크린샷은 덤프가 FTP로 전송되는 것을 보여줍니다.

```
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. WinRAR로 덤프 파일을 열고 로컬 컴퓨터에 CSR을 추출합니다.



전화 인증서 가져오기

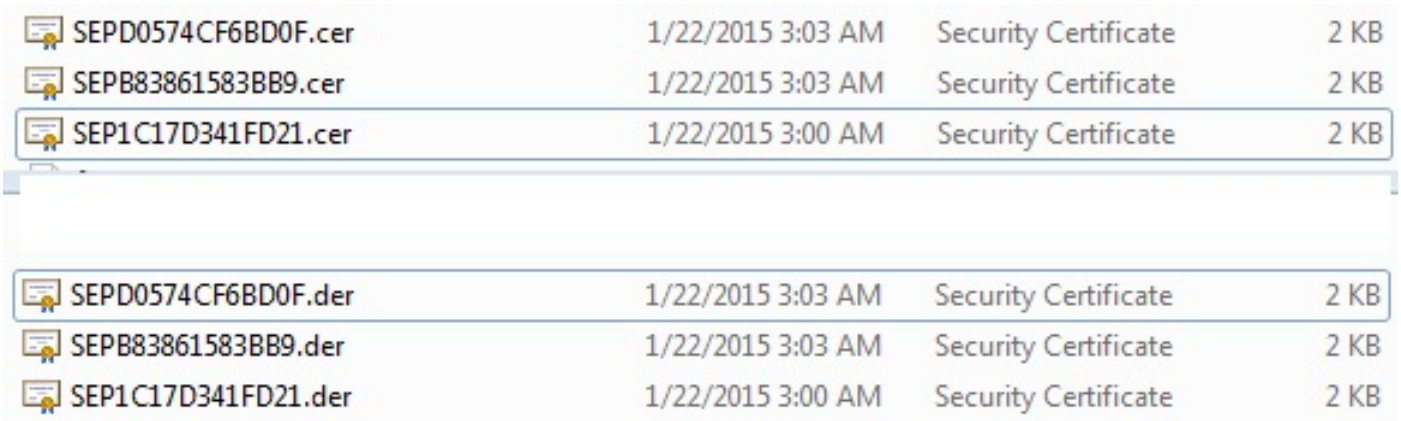
1. 전화기의 CSR을 CA에 보냅니다.

2. CA는 서명된 인증서를 제공합니다.

참고: Microsoft Windows 2003 서버를 CA로 사용할 수 있습니다. Microsoft Windows 2003 CA로 CSR에 서명하는 절차는 이 문서의 뒷부분에서 설명합니다.

.cer을 .der 형식으로 변환

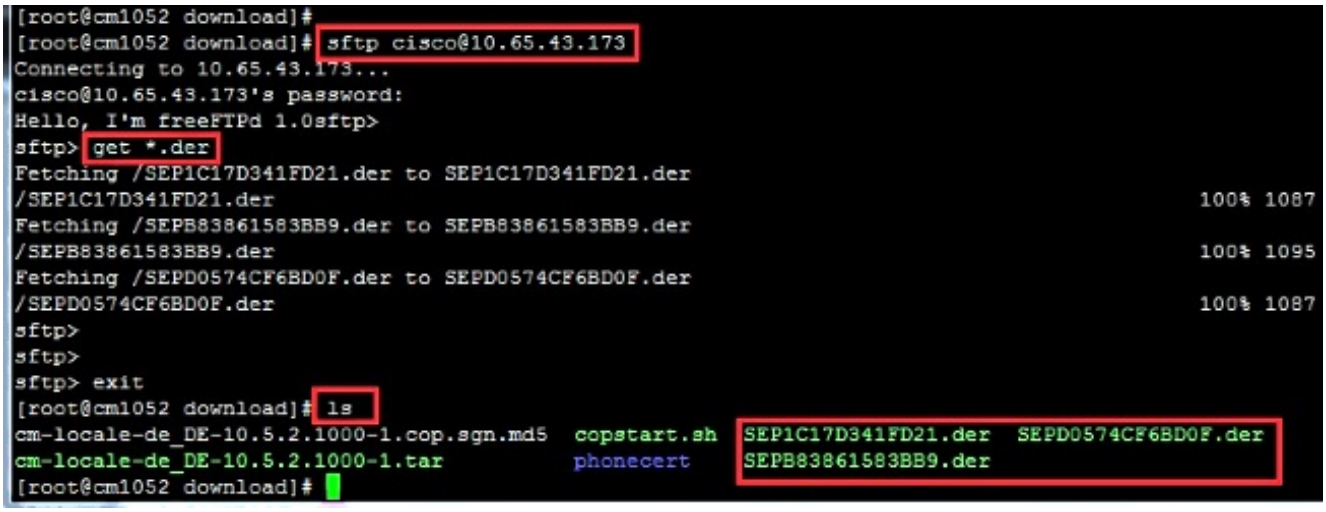
받은 인증서가 .cer 형식이면 이름을 .der로 바꿉니다.



인증서(.der)를 .tgz 형식으로 압축

인증서 형식을 압축하기 위해 CUCM 서버의 루트(Linux)를 사용할 수 있습니다. 일반 Linux 시스템에서 이 작업을 수행할 수도 있습니다.

1. 서명된 모든 인증서를 SFTP 서버가 있는 Linux 시스템으로 전송합니다.

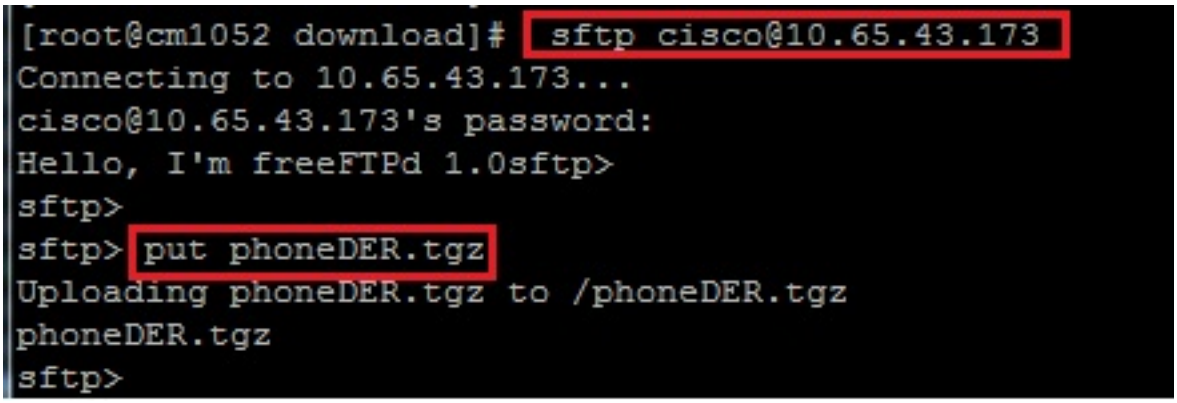


2. 모든 .der 인증서를 .tgz 파일로 압축하려면 이 명령을 입력합니다.

```
tar -zcvf
```

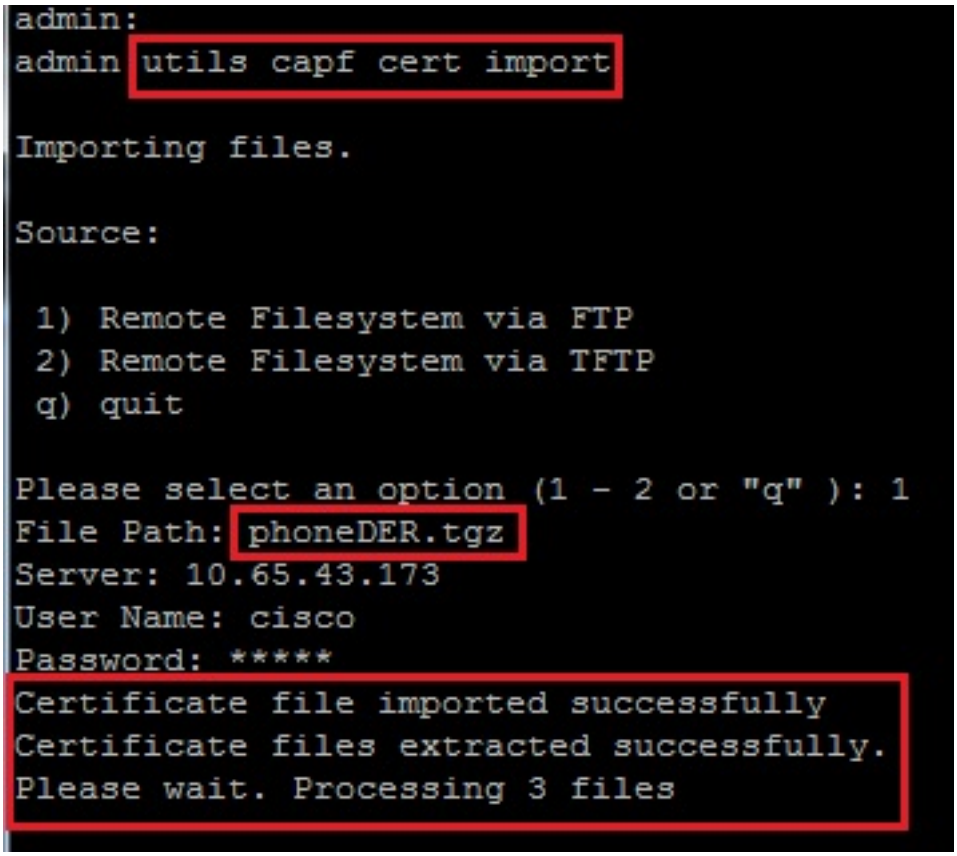
.tgz 파일을 SFTP 서버로 전송합니다.

.tgz 파일을 SFTP 서버로 전송하기 위해 스크린샷에 표시된 단계를 완료합니다.



CUCM 서버로 .tgz 파일 가져오기

1. CUCM 서버에 SSH를 적용합니다.
2. utils capf **cert import 명령을** 실행합니다.



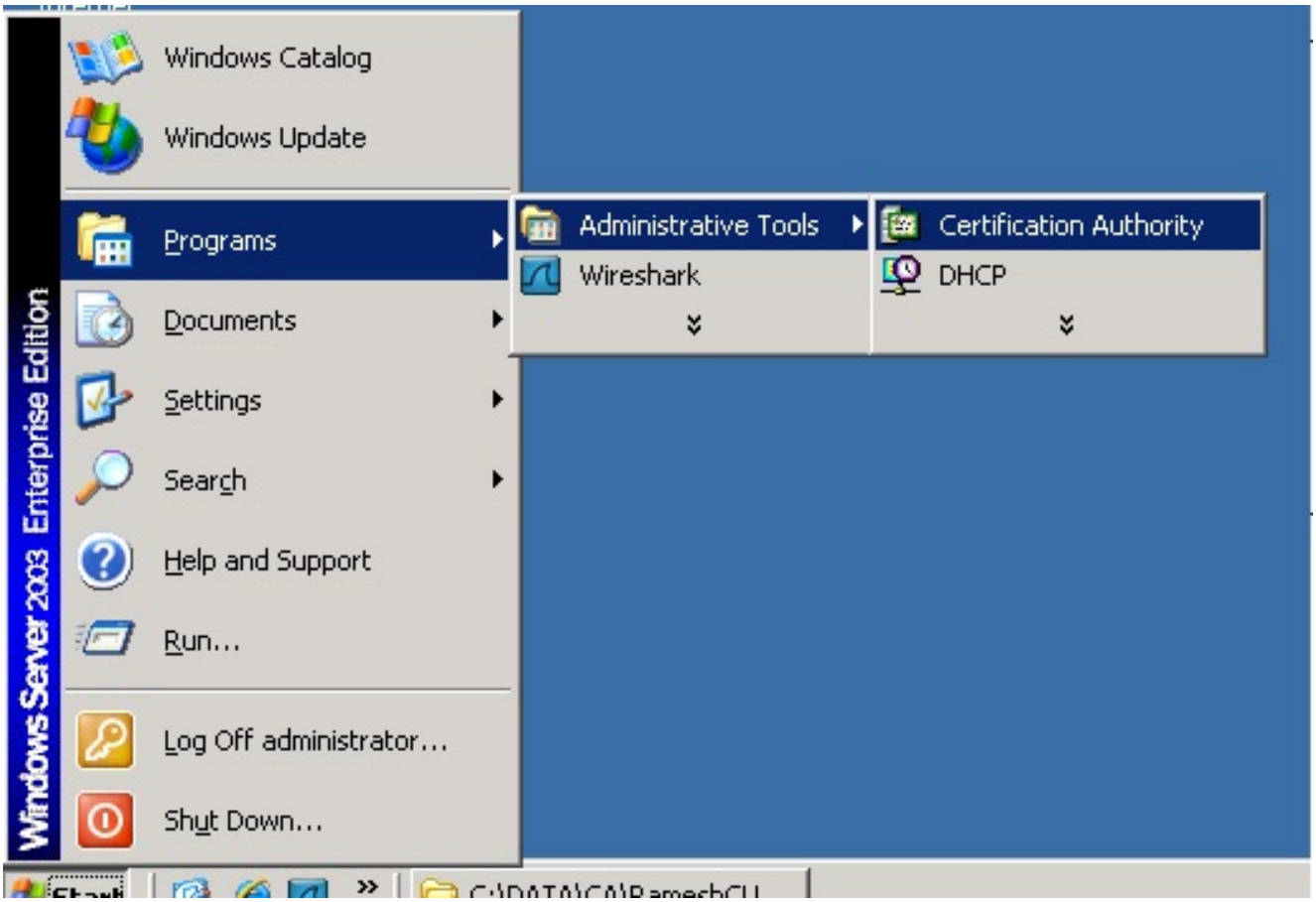
인증서를 성공적으로 가져오면 CSR 수가 0이 되는 것을 볼 수 있습니다.

```
admin:
admin:utils capf csr count

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

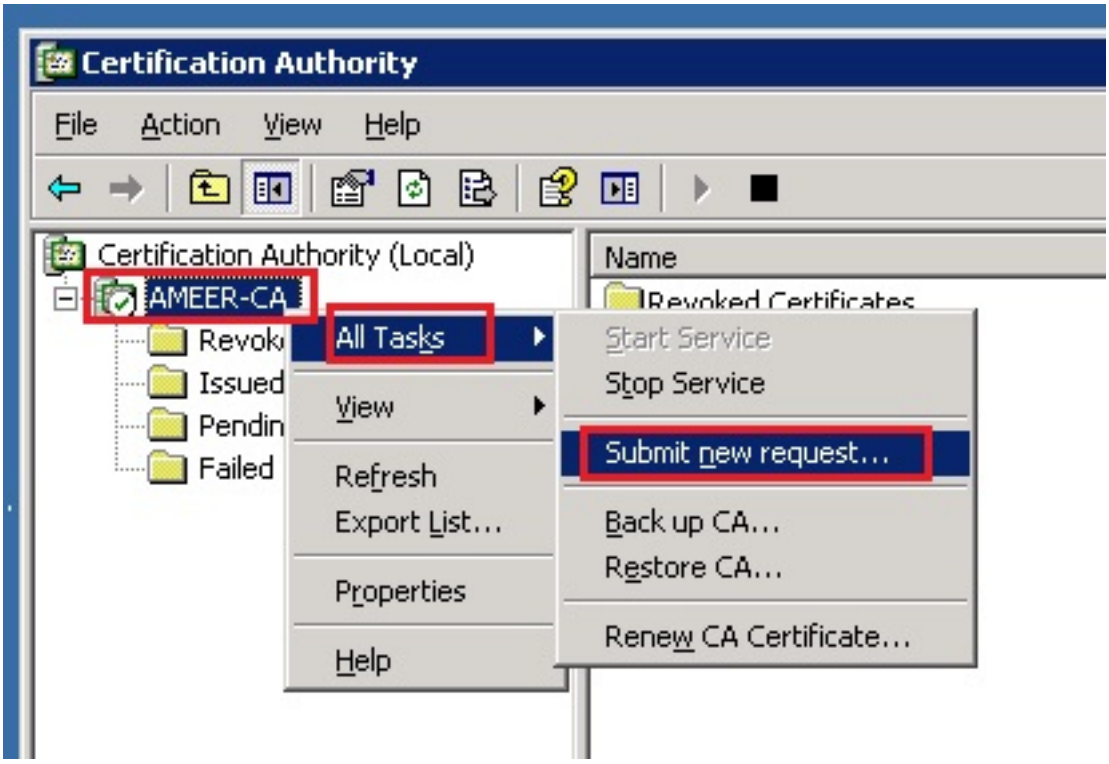
Microsoft Windows 2003 Certificate Authority로 CSR 서명

Microsoft Windows 2003 - CA에 대한 선택적 정보입니다.

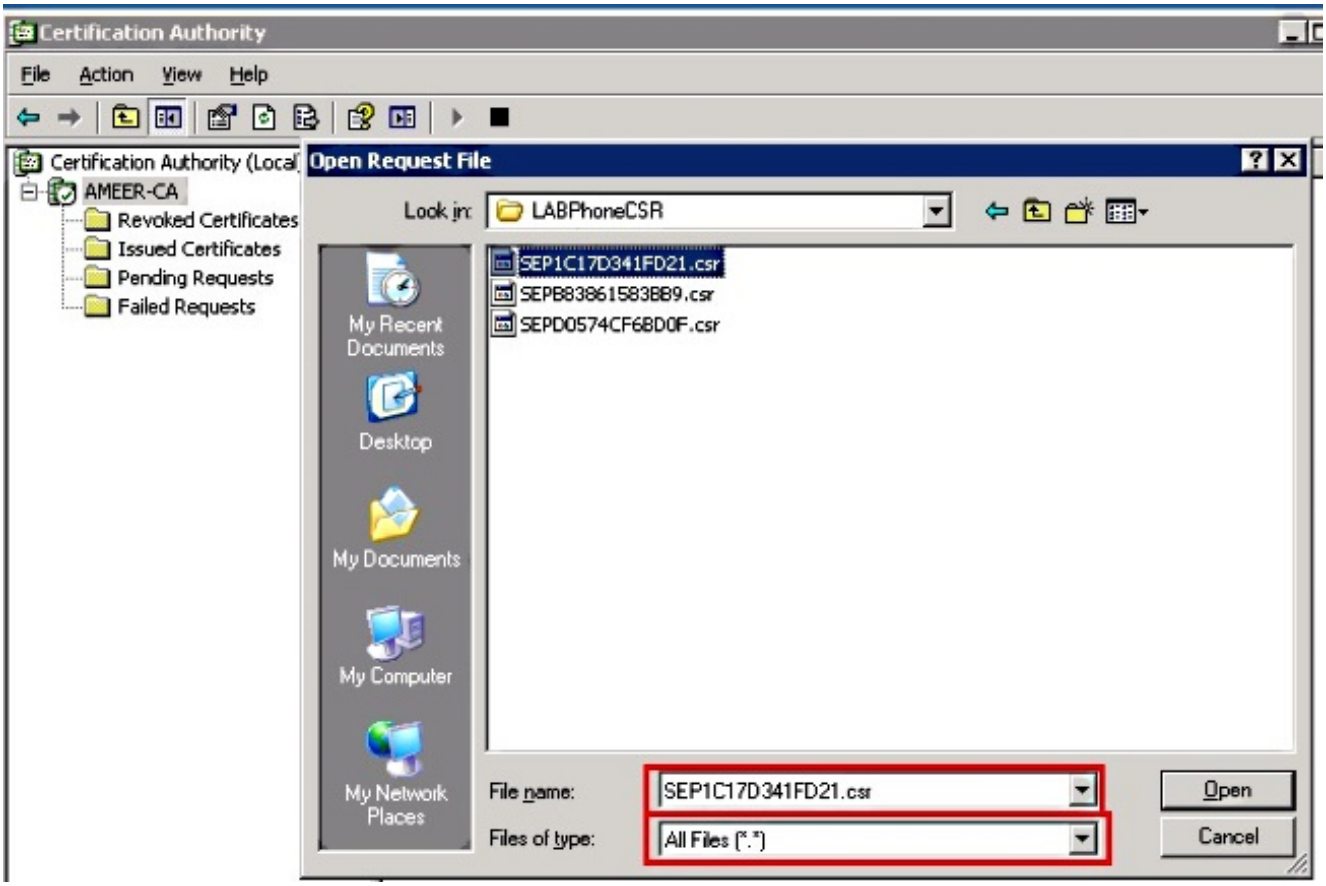
1. 인증 기관을 엽니다.



2. CA를 마우스 오른쪽 버튼으로 클릭하고 **All Tasks(모든 작업) > Submit new request(새 요청 제출)...로** 이동합니다.

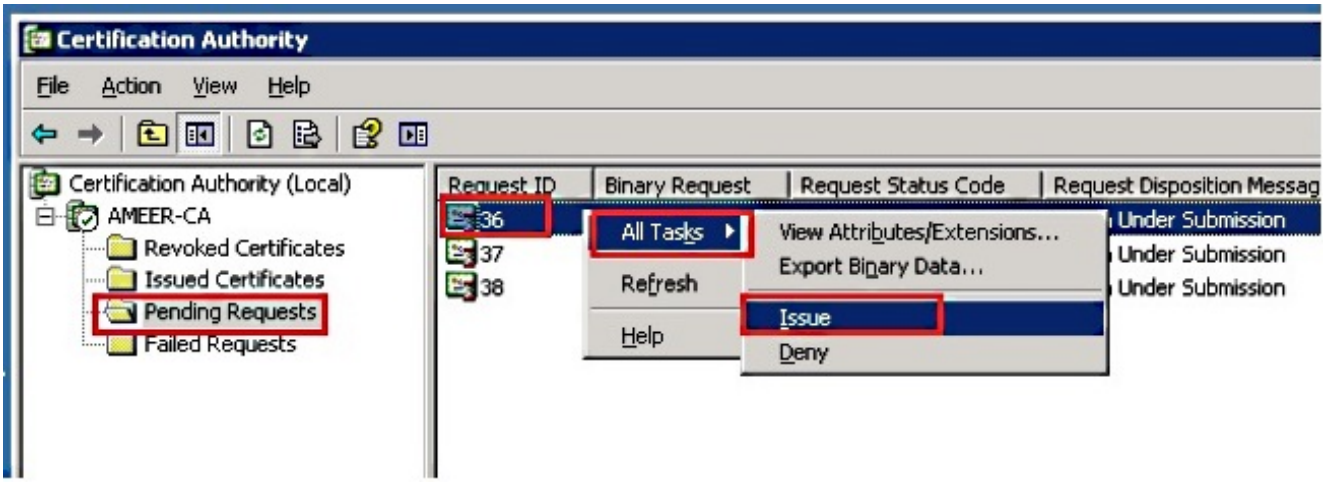


3. CSR을 선택하고 Open(열기)을 **클릭합니다**. 모든 CSR에 대해 이 작업을 수행합니다.



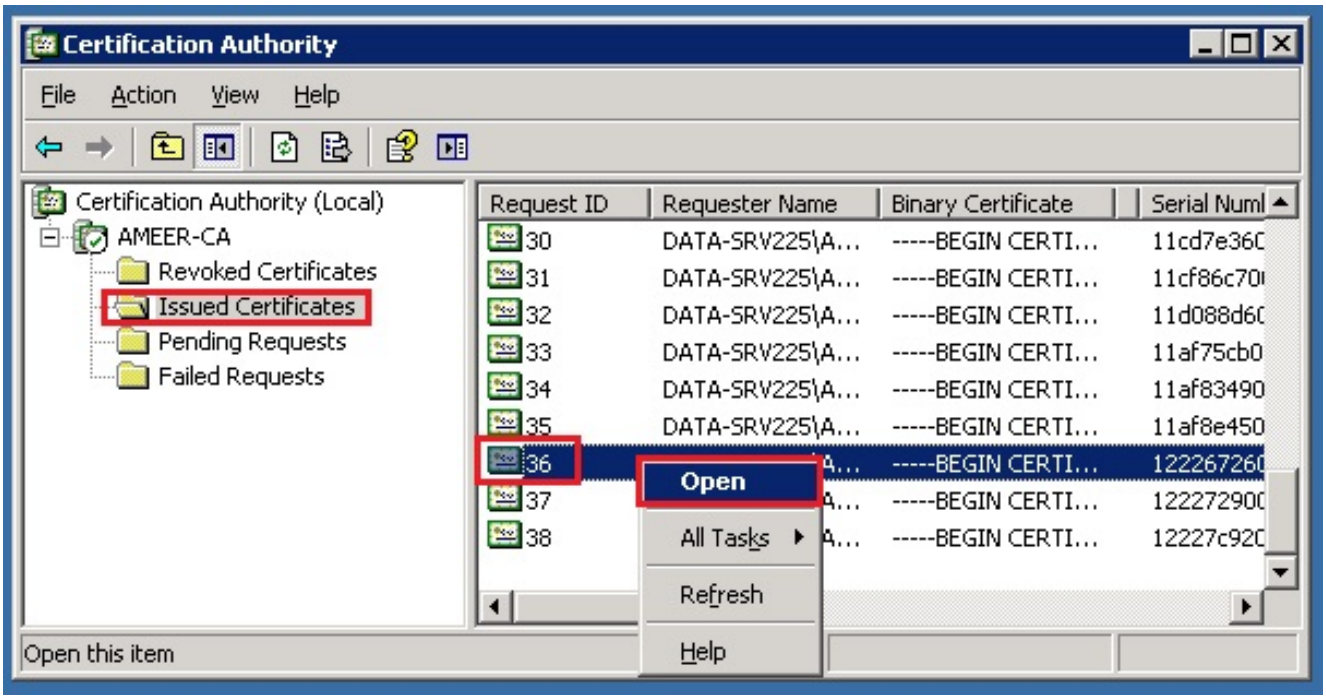
열려 있는 모든 CSR이 Pending Requests 폴더에 표시됩니다.

4. 인증서를 발급하려면 각각을 마우스 오른쪽 버튼으로 클릭하고 **All Tasks(모든 작업) > Issue(**발급)로 이동합니다. 보류 중인 모든 요청에 대해 이 작업을 수행합니다.

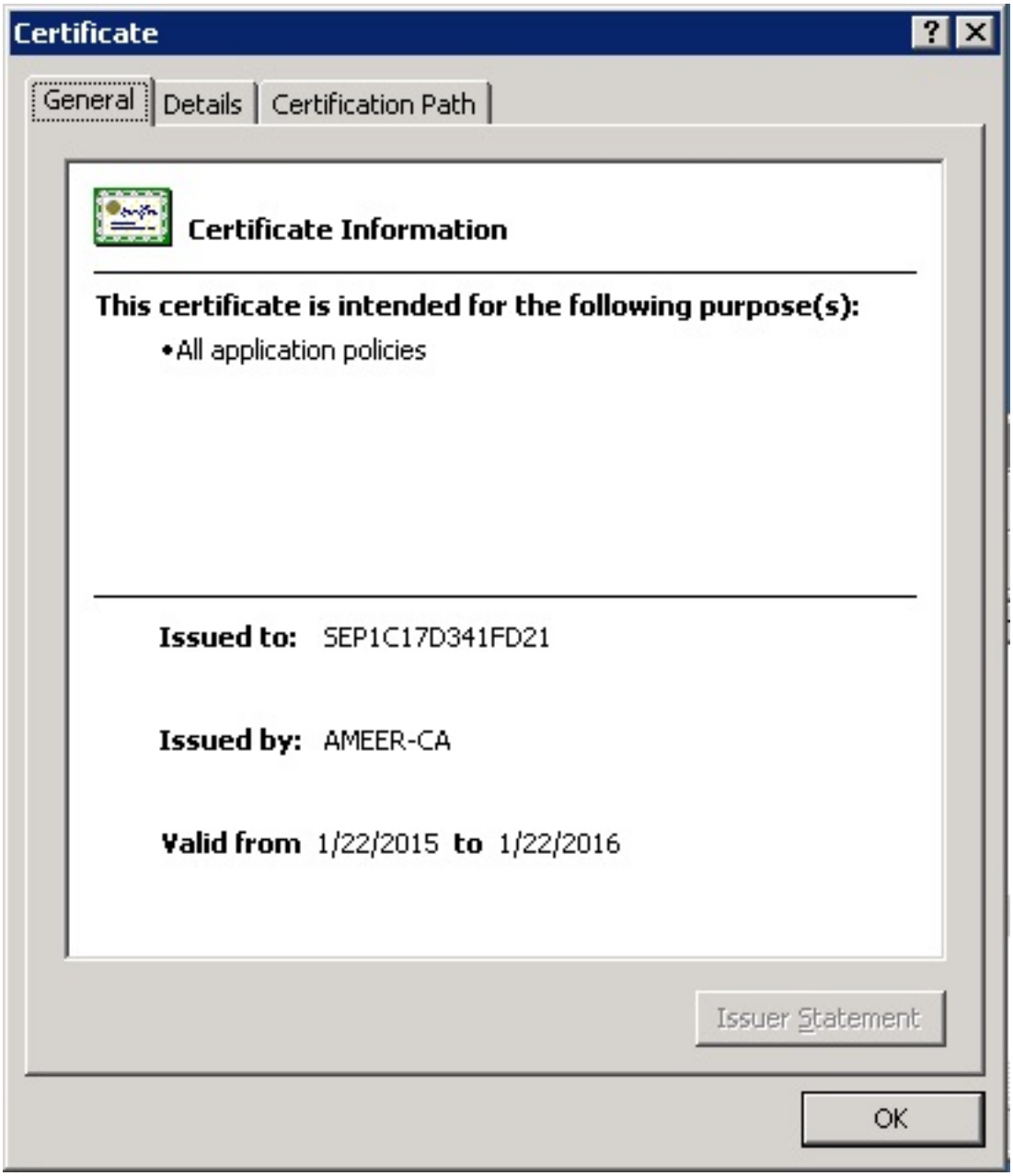


5. 인증서를 다운로드하려면 Issued Certificate를 **선택합니다**.

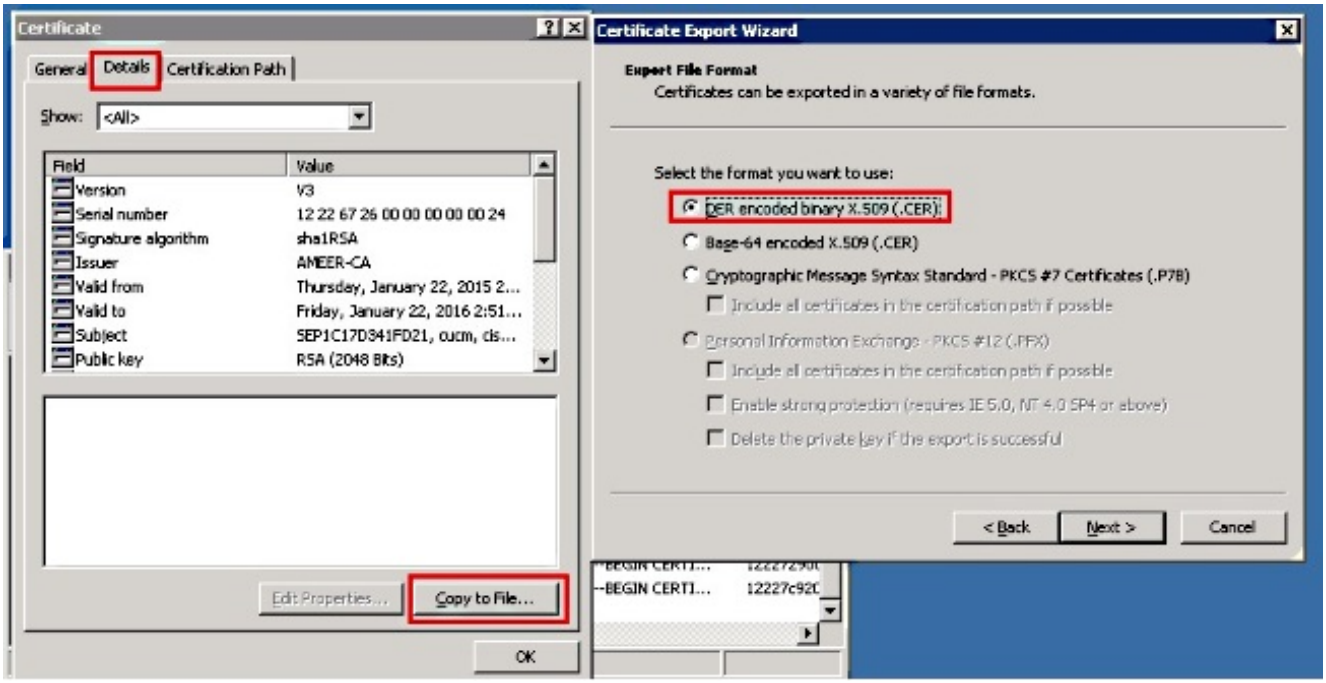
6. 인증서를 마우스 오른쪽 단추로 클릭하고 열기를 **클릭합니다**.



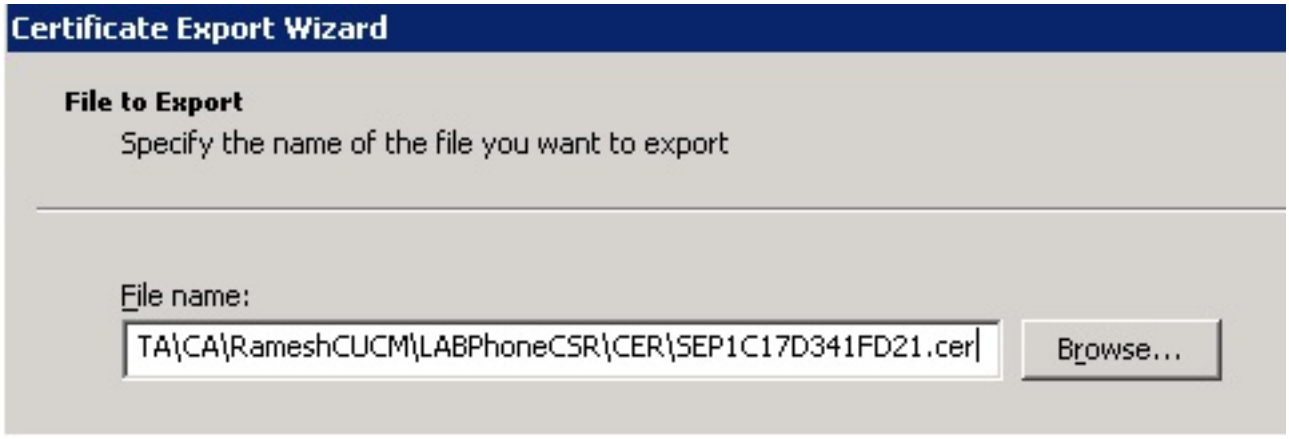
7. 인증서 세부사항을 볼 수 있습니다. 인증서를 다운로드하려면 Details(세부사항) 탭을 선택하고 Copy **to File(파일에 복사)...을** 선택합니다.



8. Certificate Export Wizard(인증서 내보내기 마법사)에서 DER encoded binary **X.509(.CER)**를 선택합니다.



9. 파일 이름을 적절하게 지정합니다. 이 예에서는 <MAC>.cer 형식을 사용합니다.

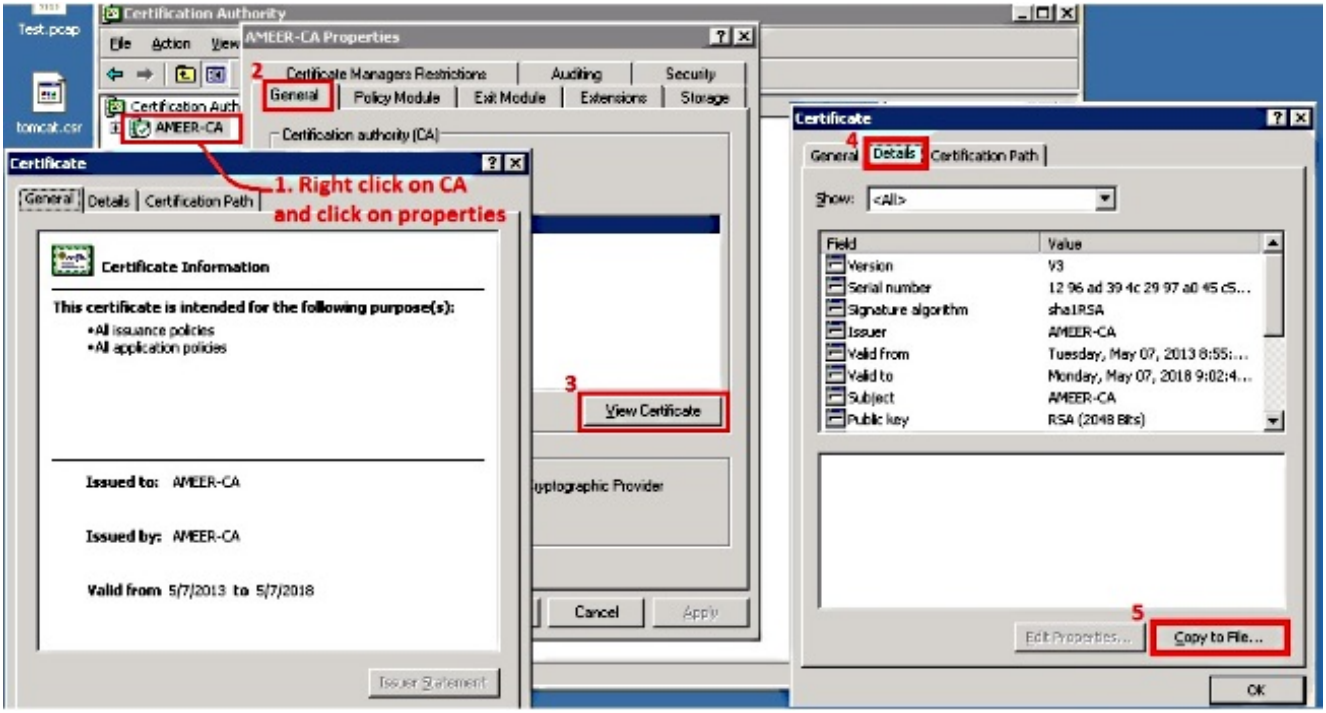


10. 이 절차를 통해 Issued Certificate(발급된 인증서) 섹션에서 다른 전화기의 인증서를 가져옵니다.

CA에서 루트 인증서 가져오기

1. 개방형 **인증 기관**.

2. 루트 CA를 다운로드하려면 이 스크린샷의 단계를 완료하십시오.

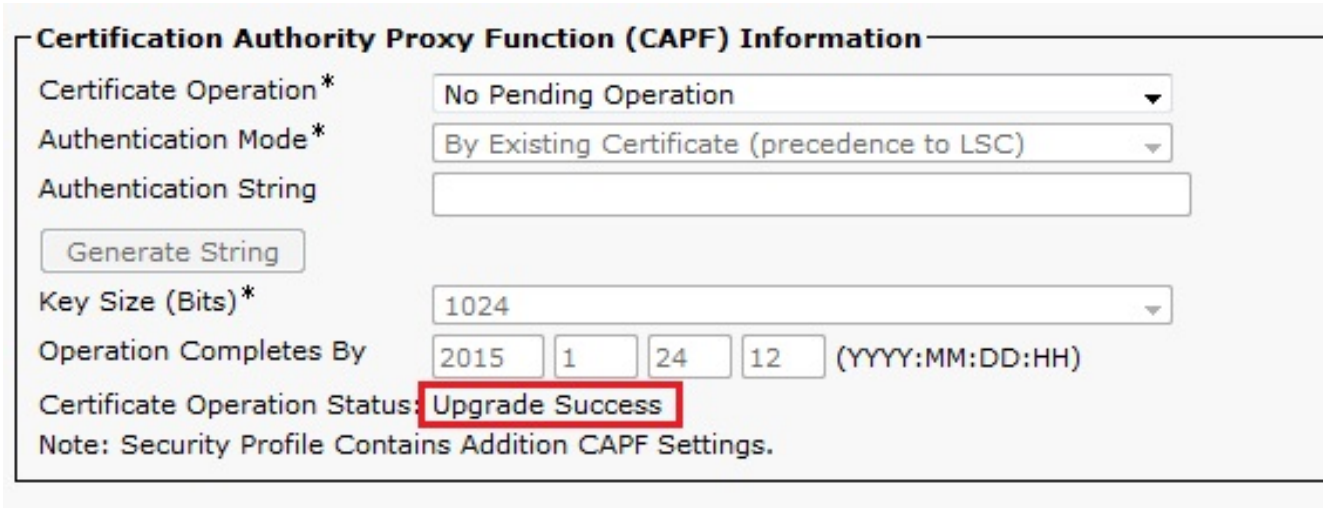


다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 전화기 컨피그레이션 페이지로 이동합니다.

2. CAPF 섹션에서 Certificate Operation Status(인증서 작업 상태)가 **Upgrade Success(업그레이드 성공)**로 표시되어야 합니다.



참고: 자세한 내용은 서드파티 CA 서명 LSC 생성 및 가져오기를 참조하십시오.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.