CUCM용 CA에서 서명한 CAPF 인증서

목차

소개

이 문서에서는 Cisco CUCM(Unified Communications Manager)용 CA(Certificate Authority)에서 서명한 CAPF(Certificate Authority Proxy Function) 인증서를 가져오는 방법에 대해 설명합니다. 항상 외부 CA로 CAPF에 서명하라는 요청이 있습니다.이 문서에서는 구성 절차 못지않게 작동 방식을 이해하는 이유를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PKI(Public Key Infrastructure)
- CUCM 보안 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 Cisco Unified Communications Manager 버전 8.6 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

제한 사항

CA에 따라 CSR에 대한 요구 사항이 다를 수 있습니다.다른 버전의 OpenSSL CA가 CSR에 대한 특정 요청을 가지고 있지만 지금까지 Microsoft Windows CA가 Cisco CAPF의 CSR과 잘 작동하며, 이에 대해서는 이 문서에서 다루지 않을 것입니다.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- Microsoft Windows Server 2008 CA.
- Windows용 Cisco Jabber(LSC를 저장할 폴더의 이름이 다를 수 있음)

배경 정보

CA 서명 CAPF의 목적

일부 고객은 글로벌 인증서 정책과 연계하여 다른 서버와 동일한 CA로 CAPF에 서명해야 합니다.

이 PKI에 대한 메커니즘

기본적으로 CAPF에서 LSC(Locally Significant Certificate)가 서명되므로 이 시나리오에서 CAPF는 전화기의 CA입니다.그러나 외부 CA에서 서명한 CAPF를 가져오려고 하면 이 시나리오의 CAPF는 하위 CA 또는 중간 CA로 작동합니다.

자체 서명 CAPF와 CA 서명 CAPF의 차이점은 다음과 같습니다.CAPF는 자체 서명 CAPF를 수행할 때 LSC에 대한 루트 CA이며, CAPF는 CA 서명 CAPF를 수행할 때 LSC에 대한 하위(중간) CA입니다.

CAPF CSR은 다른 CSR과 어떻게 다릅니까?

RFC5280에 대해 키 사용 확장은 인증서에 포함된 키의 용도(예: 암호화, 서명, 인증서 서명)를 정의합니다.CAPF는 인증서 프록시 및 CA이며 전화기에 인증서를 서명할 수 있지만 CallManager, Tomcat, IPSec과 같은 다른 인증서는 리프(사용자 ID)로 작동합니다. CSR에 대한 내용을 살펴보면 CAPF CSR에 **Certificate Sign** 역할이 있지만 다른 역할은 없는 것을 확인할 수 있습니다.

CAPF CSR:

```
Attributes:
Requested Extensions:
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, IPSec End System
    X509v3 Key Usage:
        Digital Signature, Certificate Sign
```

Tomcat CSR:

```
Attributes:
```

```
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

통화 관리자 CSR:

```
Attributes:
        Requested Extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication, IPSec End System
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
```

IPSec CSR:

특성:요청된 확장:X509v3 확장 키 사용:TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 최종 시스템 X509v3 키 사용:디지털 서명, 키 암호화, 데이터 암호화, 키 계약

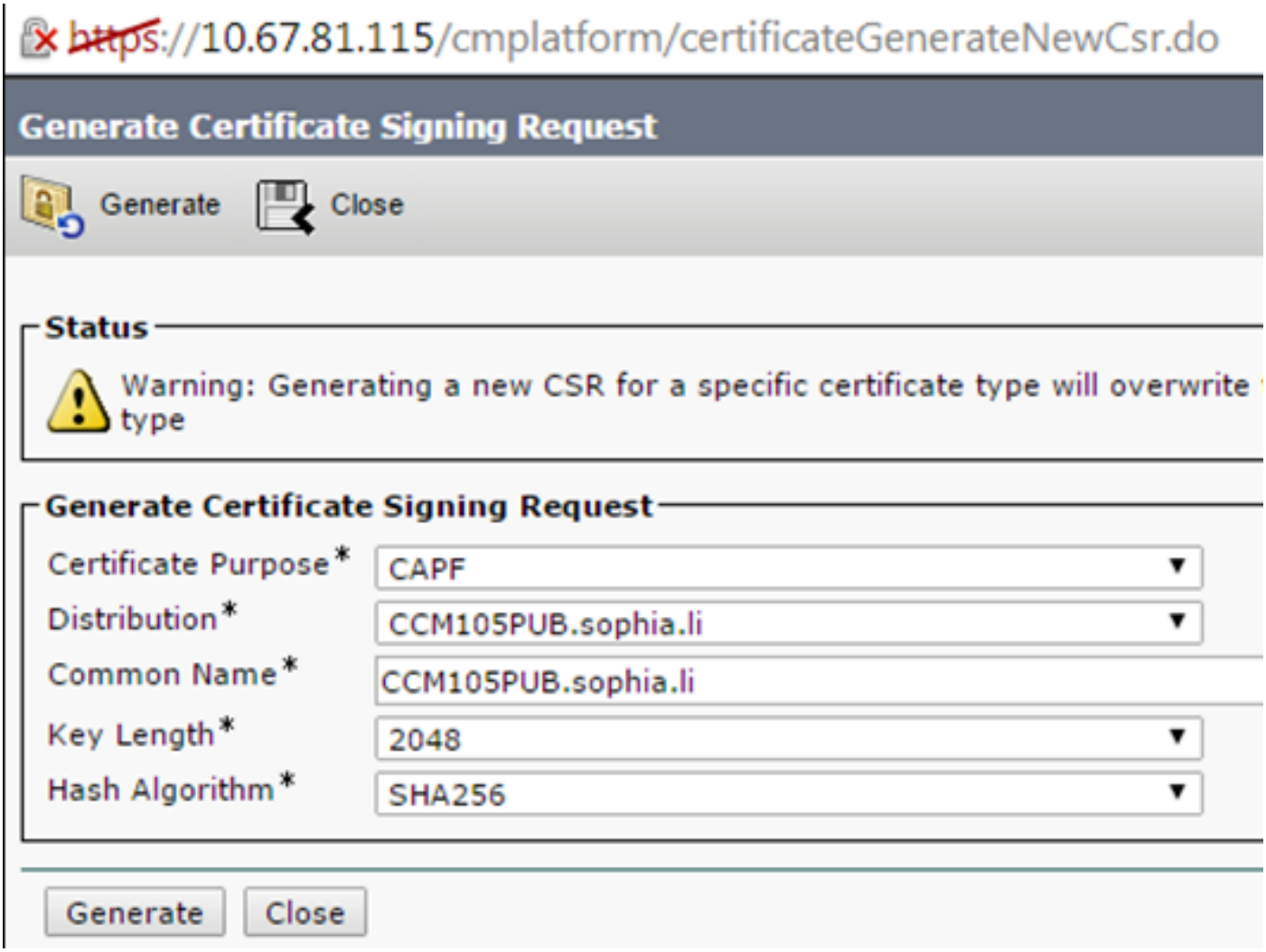
구성

다음은 외부 루트 CA가 CAPF 인증서를 서명하는 데 사용되는 시나리오입니다.Jabber 클라이언트 및 IP 전화의 신호/미디어를 암호화합니다.

1단계. CUCM 클러스터를 보안 클러스터로 만듭니다.

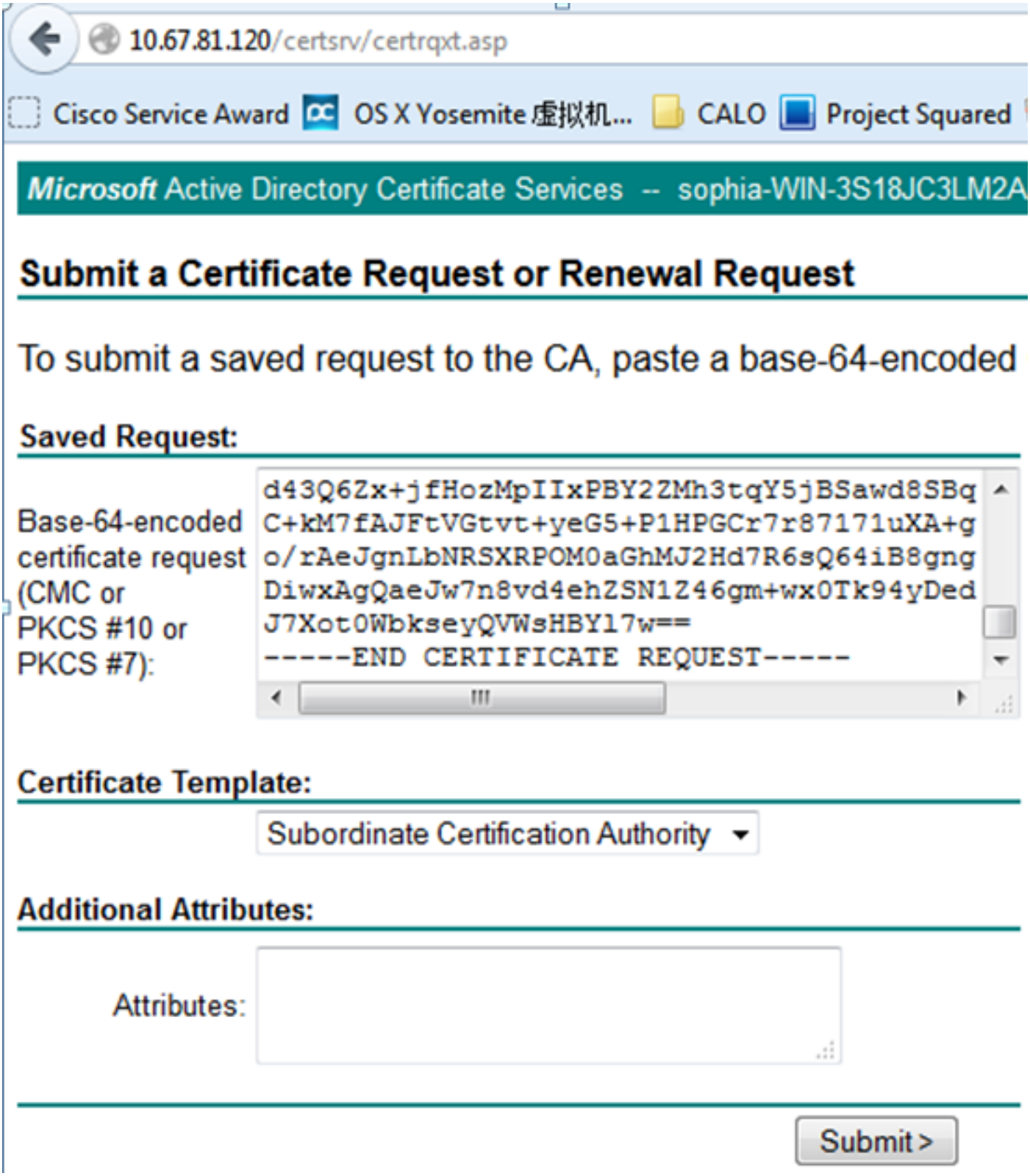
```
admin:utils ctl set-cluster mixed-mode
```

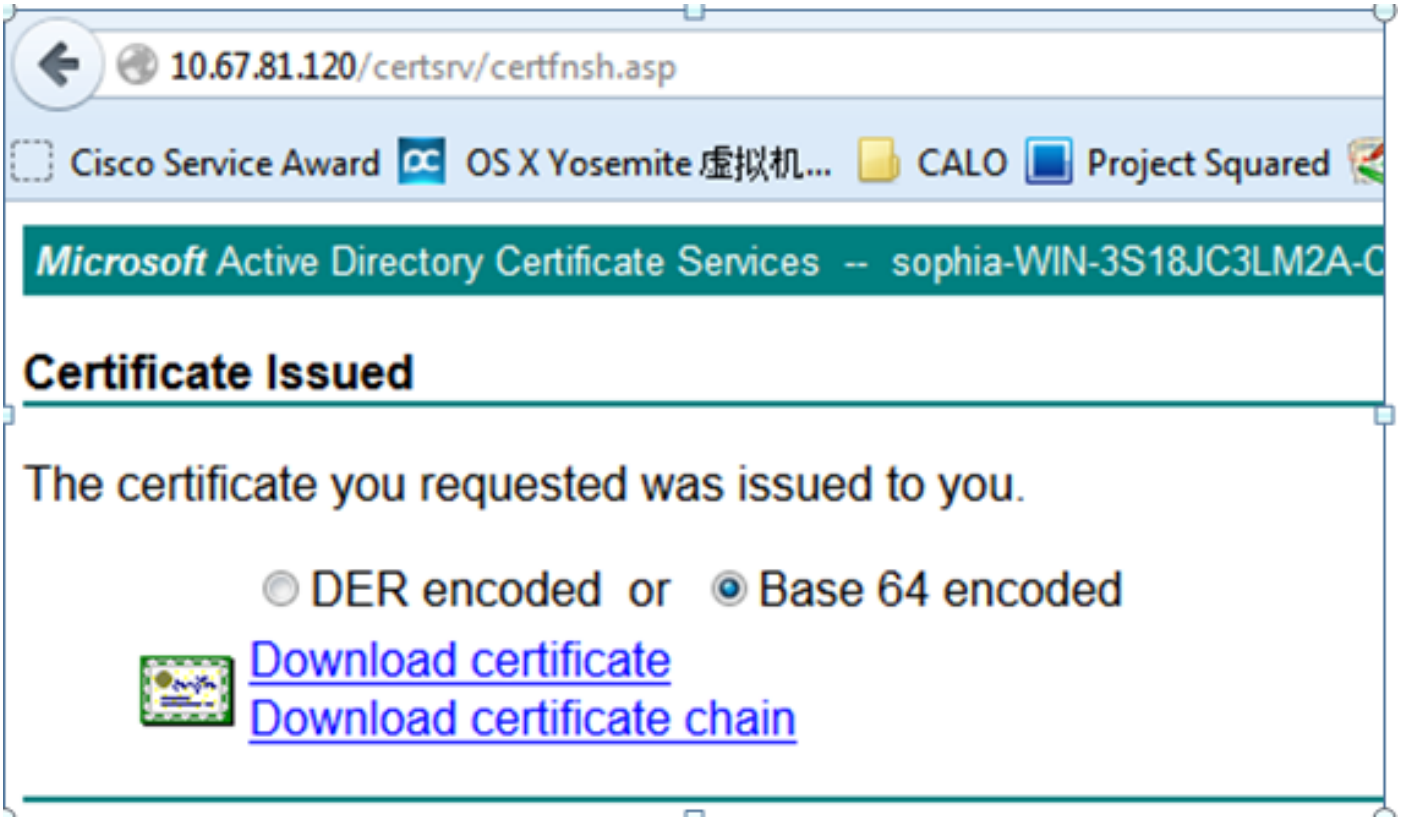
2단계. 이미지에 표시된 대로 CAPF CSR을 생성합니다.



3단계. CA와 서명(Windows 2008 CA의 하위 템플릿 사용)

참고:이 인증서에 서명하려면 사용자 **하위 인증 기관** 템플릿이 필요합니다.


10.67.81.120/certsrv/certrqxt.asp
Cisco Service Award
OS X Yosemite 虚拟机...
CALO
Project Squared
Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded
Saved Request:
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
d43Q6Zx+jfHozMpIIxPBY2ZMh3tqY5jBSawd8SBq
C+kM7fAJFtVGtvt+yeG5+P1HPGCr7r87171uXA+g
o/rAeJgnLbNRSXRPOM0aGhMJ2Hd7R6sQ64iB8gng
DiwxAgQaeJw7n8vd4ehZSN1Z46gm+wx0Tk94yDed
J7Xot0WbkseyQVWsHBYl7w==
-----END CERTIFICATE REQUEST-----
Certificate Template:
Subordinate Certification Authority
Additional Attributes:
Attributes:
Submit >

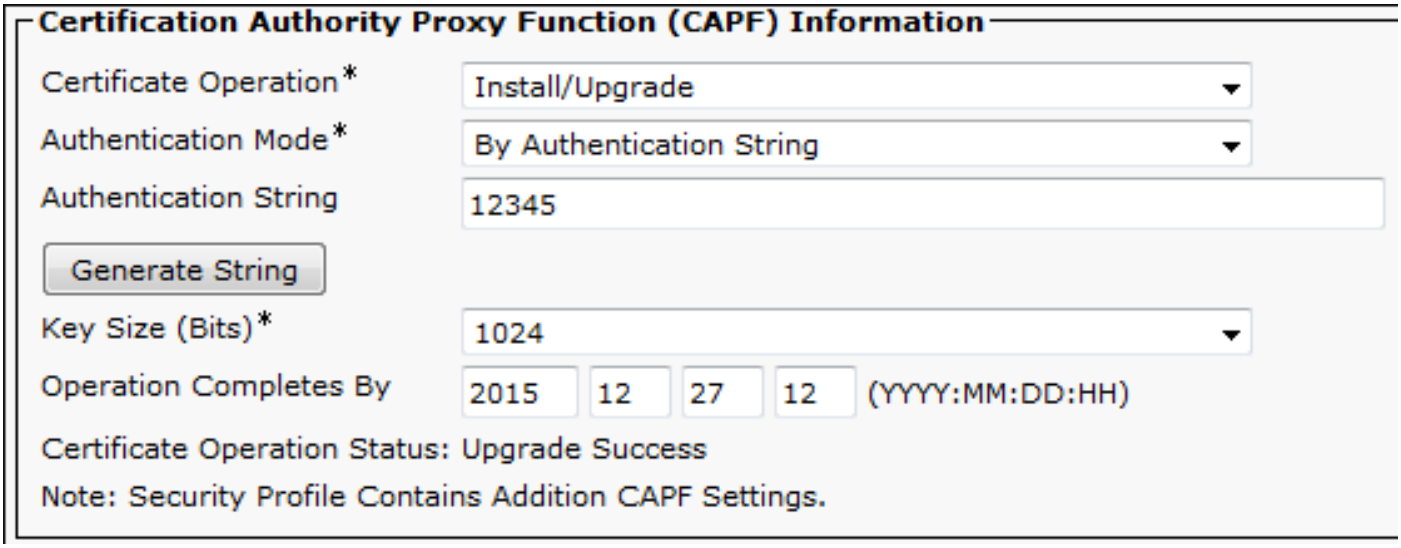


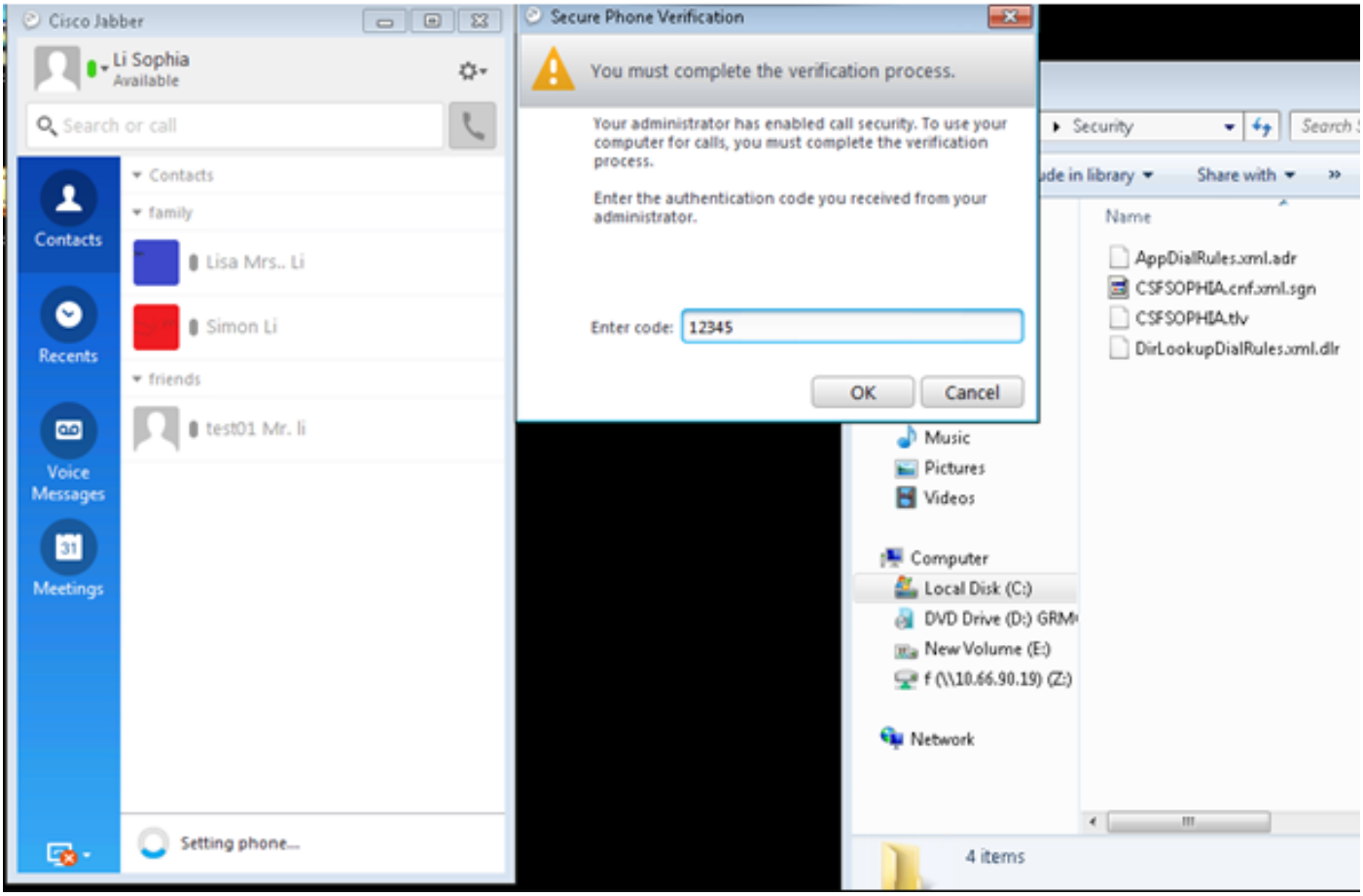
4단계. 루트 CA를 CAPF-trust로 업로드하고 서버 인증서를 CAPF로 업로드합니다.이 테스트의 경우 CallManager 서비스에서도 서명된 LSC를 신뢰할 수 있어야 하므로 이 루트 CA를 CallManager-trust로 업로드하여 Jabber와 CallManager 서비스 간에 TLS 연결을 설정하십시오.이 문서의 시작 부분에서 언급했듯이, 이 CA가 신호/미디어 암호화를 위해 이미 CallManager에 업로드되었어야 하므로 모든 서버에 대해 CA를 조정해야 합니다.IP Phone 802.1x를 구축하는 시나리오의 경우 CUCM을 혼합 모드로 만들거나 CAPF를 CallManager-trust로 표시하는 CA를 CUCM 서버에 업로드할 필요가 없습니다.

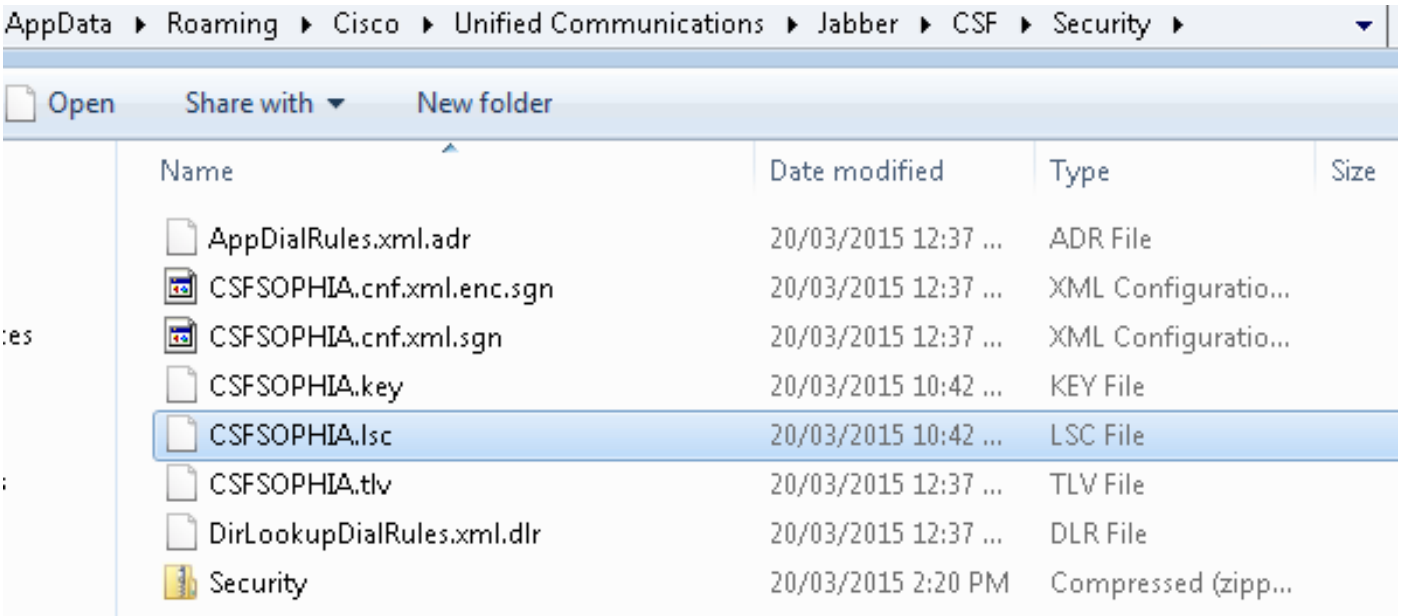
5단계. CAPF 서비스를 다시 시작합니다.

6단계. 모든 메모에서 CallManager/TFTP 서비스를 다시 시작합니다.

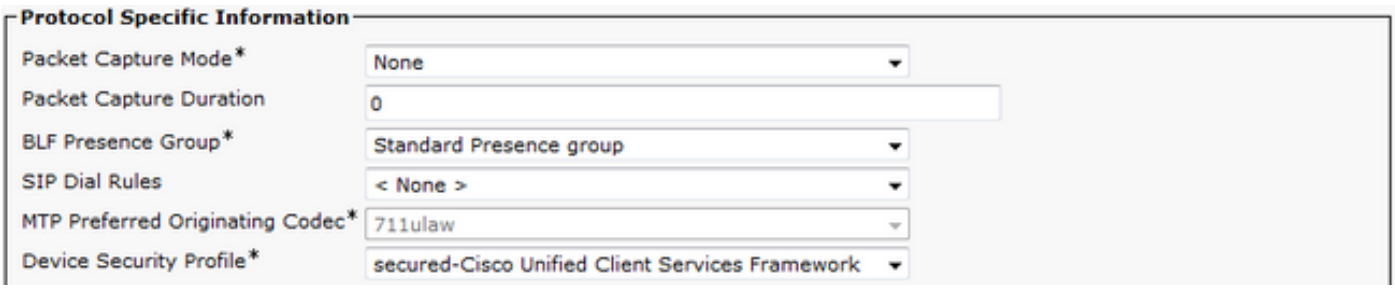
7단계. Jabber 소프트폰 LSC에 서명합니다.



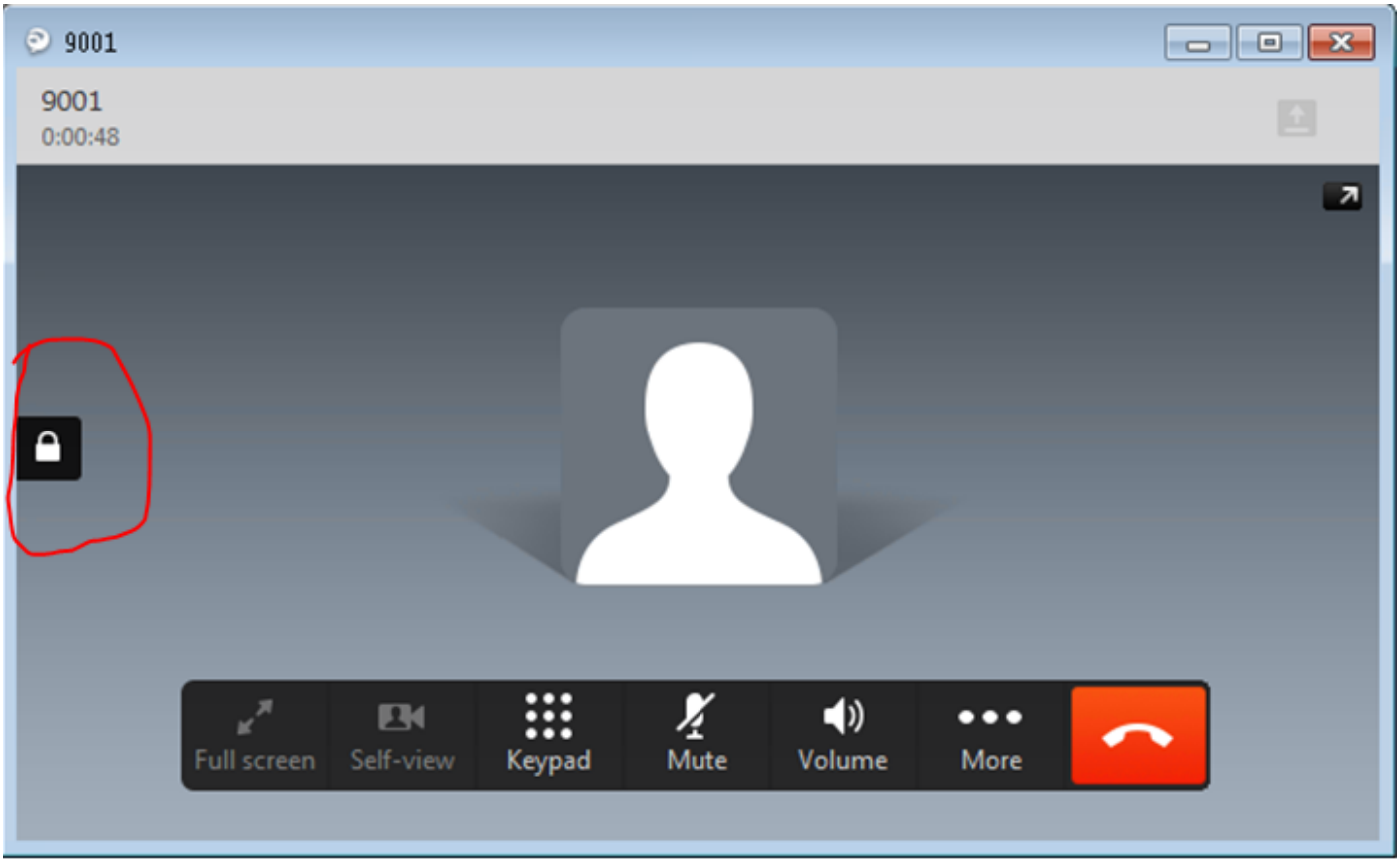




8단계. Jabber 소프트폰의 보안 프로필을 활성화합니다.



9단계. 이제 보안 RTP는 다음과 같이 실행됩니다.

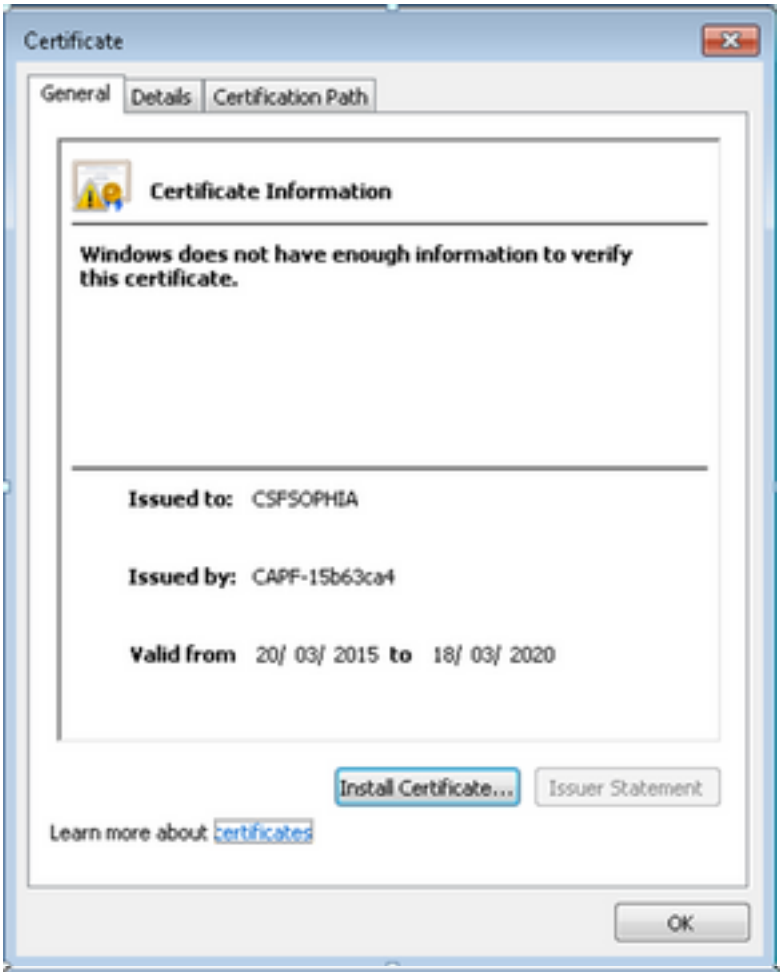


다음을 확인합니다.

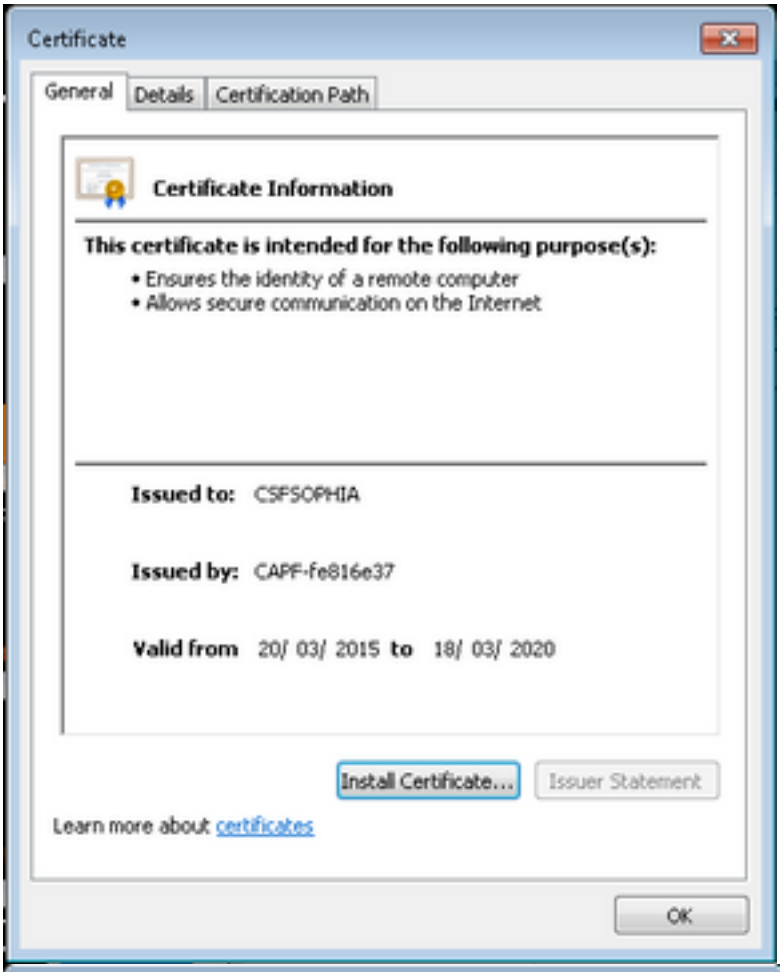
자체 서명 CAPF 및 CA 서명 CAPF가 있는 경우 LSC를 비교합니다.

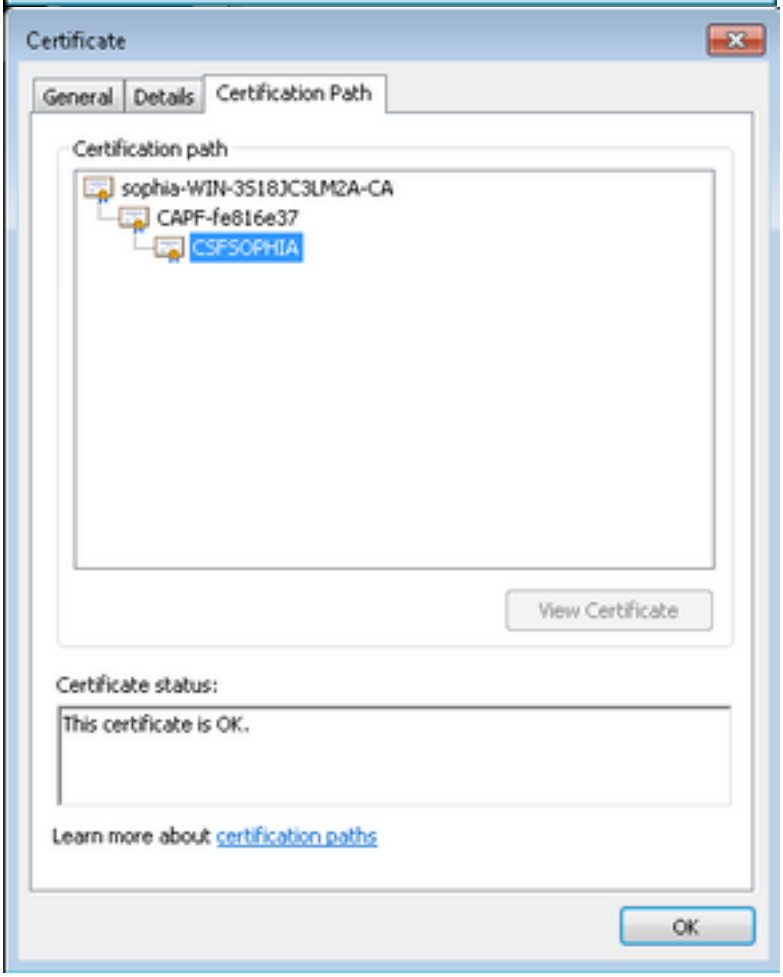
LSC에 대해 이러한 이미지에서 볼 수 있듯이 LSC 관점에서 볼 때 CAPF는 자체 서명된 CAPF를 사용할 때 루트 CA이지만 CAPF는 CA 서명 CAPF를 사용할 때 하위(중간) CA입니다.

자체 서명 CAPF 시 LSC



CA 서명 CAPF 시 LSC


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Allows secure communication on the Internet
Issued to: CSFSOPHIA
Issued by: CAPF-fe816e37
Valid from 20/ 03/ 2015 to 18/ 03/ 2020
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Certificate
General
Details
Certification Path
Certification path
sophia-WIN-3S18JC3LM2A-CA
CAPF-fe816e37
CSFSOPHIA
View Certificate
Certificate status:
This certificate is OK.
Learn more about certification paths
OK

경고:

이 예에서 전체 인증서 체인을 보여 주는 Jabber 클라이언트 LSC는 IP 폰과 다릅니다.AS IP 전화기는 RFC 5280(3.2. 인증 경로 및 신뢰)을 기반으로 설계되었으므로 AKI(Authority Key Identifier)가 없으면 CAPF와 루트 CA 인증서가 인증서 체인에 없습니다.인증서 체인에 CAPF/Root CA 인증서가 없으면 CAPF 및 루트 인증서를 ISE에 업로드하지 않고 801.x 인증 중에 ISE에서 IP 폰을 인증하는 데 몇 가지 문제가 발생합니다. 외부 오프라인 CA에서 직접 서명한 LSC가 포함된 CUCM 12.5에는 IP Phone 802.1x 인증을 위해 CAPF 인증서를 ISE에 업로드하지 않아도 되는 다른 옵션이 있습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

알려진 결함:CA 서명 CAPF 인증서, 루트 인증서는 CM 신뢰로 업로드해야 합니다.

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCut87382/?referring_site=bugquickviewredir