CUCM の CA によって署名された CAPF 証明書

内容

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)の認証局(CA)によって署名された認証局プロキシ機能(CAPF)証明書を取得する方法について説明します。 外部CAを使用してCAPFに署名する要求は常にあります。このドキュメントでは、設定手順と同様に動作の仕組みを理解する理由について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 公開キー インフラストラクチャ（PKI）
- CUCMセキュリティ設定

使用するコンポーネント

このドキュメントの情報は、Cisco Unified Communications Manager バージョン 8.6 以降に基づくものです。

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

制限

CSRに対する要件は、CAによって異なります。異なるバージョンのOpenSSL CAにCSRに関する特定の要求があることが報告されていますが、Microsoft Windows CAはこれまでCisco CAPFのCSRと良好に動作していましたが、この記事では説明しません。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Microsoft Windows Server 2008 CA。
- Cisco Jabber for Windows（バージョンによって、LSCを保存するフォルダの名前が異なる場合があります）。

背景説明

CA署名付きCAPFの目的

一部のお客様は、会社との間でグローバル証明書ポリシーに従って、他のサーバと同じCAでCAPFに署名する必要があります。

このPKIのメカニズム

デフォルトでは、ローカルで有効な証明書(LSC)はCAPFによって署名されるため、このシナリオではCAPFが電話機のCAになります。ただし、外部CAによって署名されたCAPFを取得しようとすると、このシナリオのCAPFは下位CAまたは中間CAとして機能します。

自己署名CAPFとCA署名付きCAPFの違いは次のとおりです。CAPFは自己署名CAPFを実行する場合のルートCAからLSCへ、CA署名CAPFを実行する場合CAPFは下位（中間）CAからLSCへ送信されます。

CAPF CSRと他のCSRの違い

RFC5280に関しては、キー使用拡張は、証明書に含まれるキーの目的（暗号化、署名、証明書署名など）を定義します。CAPFは証明書プロキシおよびCAであり、電話機に証明書を署名できますが、CallManager、Tomcat、IPSecなどの他の証明書はリーフ（ユーザID）として機能します。 CSRを調べると、CAPF CSRに証明書の署名ロールが割り当てられて**いますが、他の**CSRは表示されません。

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
```

CallManager 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:

属性:要求された拡張機能：X509v3拡張キーの使用法：TLS Webサーバ認証、TLS Webクライアント認証、IPSecエンドシステムX509v3キーの使用法：デジタル署名、鍵暗号化、データ暗号化、鍵契約

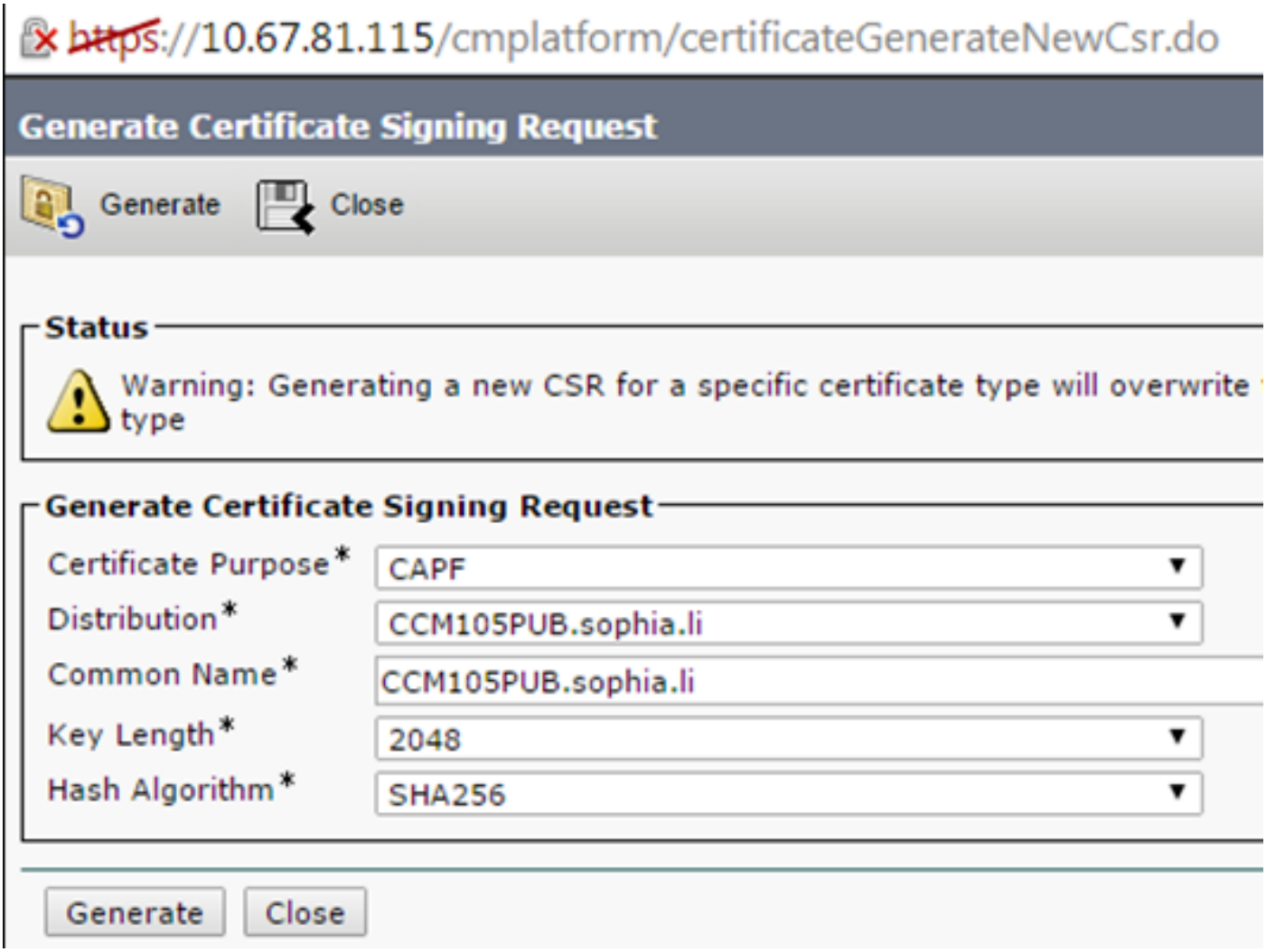
設定

次の1つのシナリオでは、外部ルートCAを使用してCAPF証明書に署名します。Jabberクライアントと IP電話の信号/メディアを暗号化します。

ステップ1:CUCMクラスタをセキュリティクラスタにします。

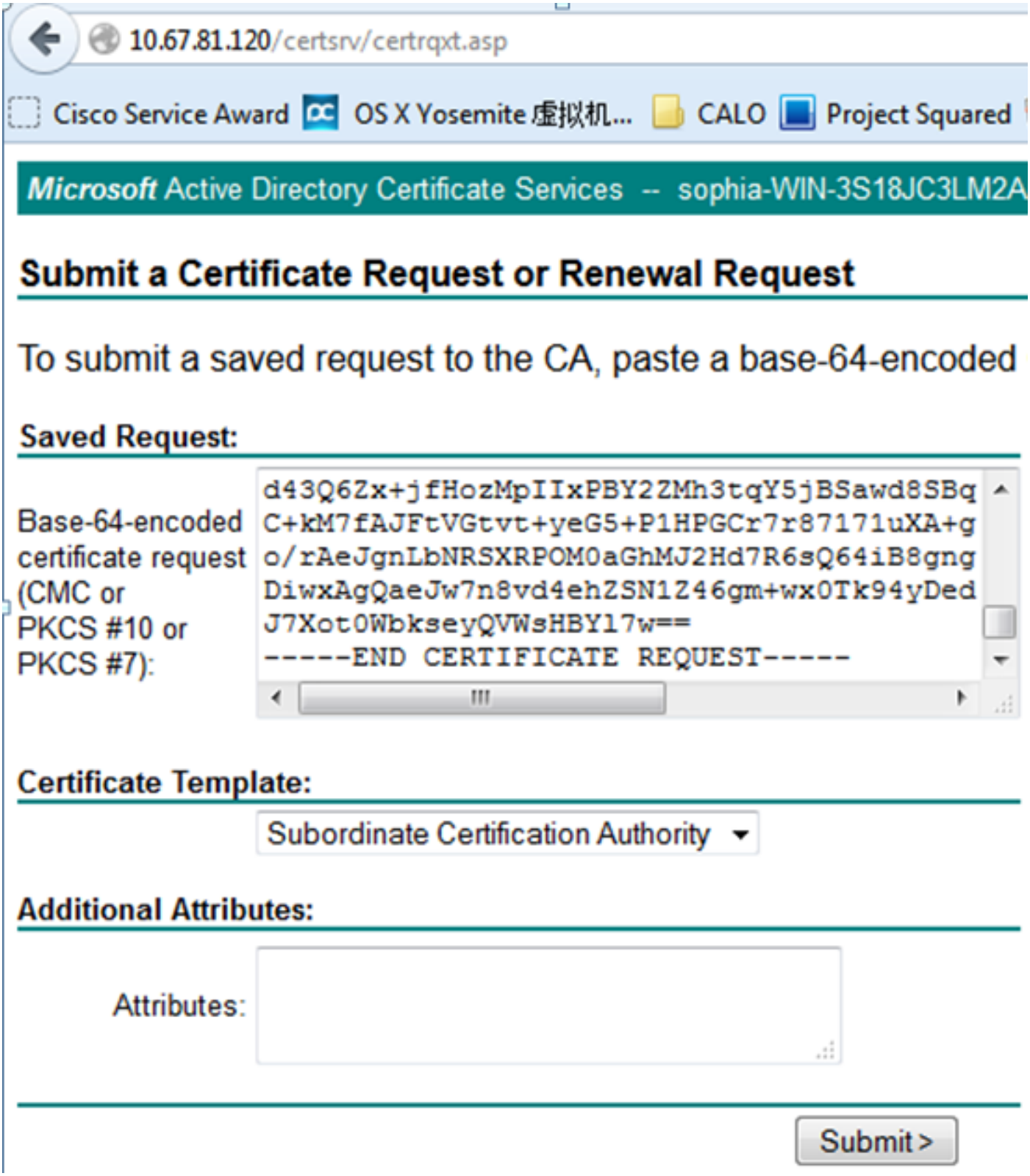
```
admin:utils ctl set-cluster mixed-mode
```

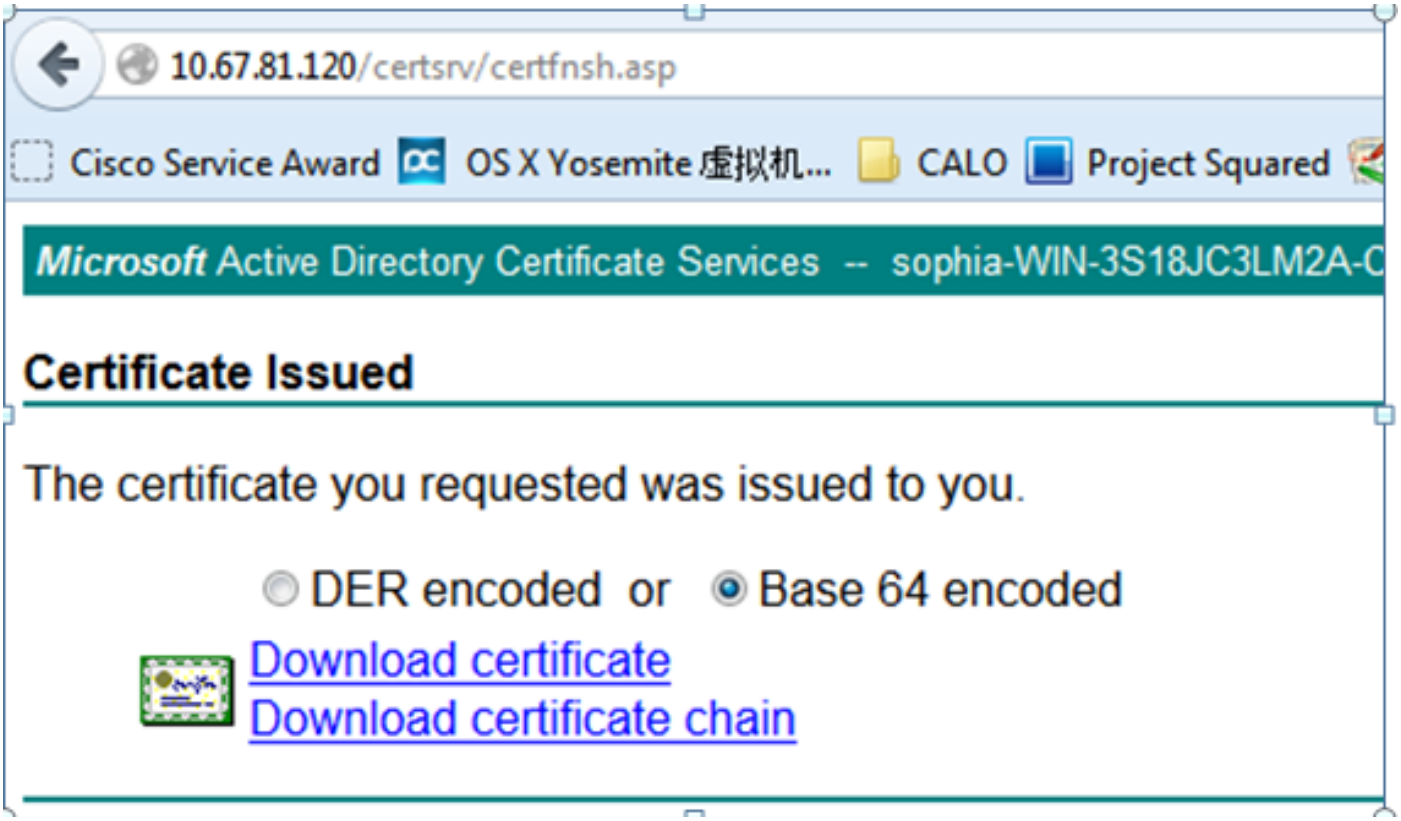
ステップ2：図に示すように、CAPF CSRを生成します。



ステップ3:CAで署名します（Windows 2008 CAの下位テンプレートを使用）。

> **注：この証明書に署名するには、Subordinate Certification Authorityテンプレートをユーザーに指定する必要があります。**


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 >

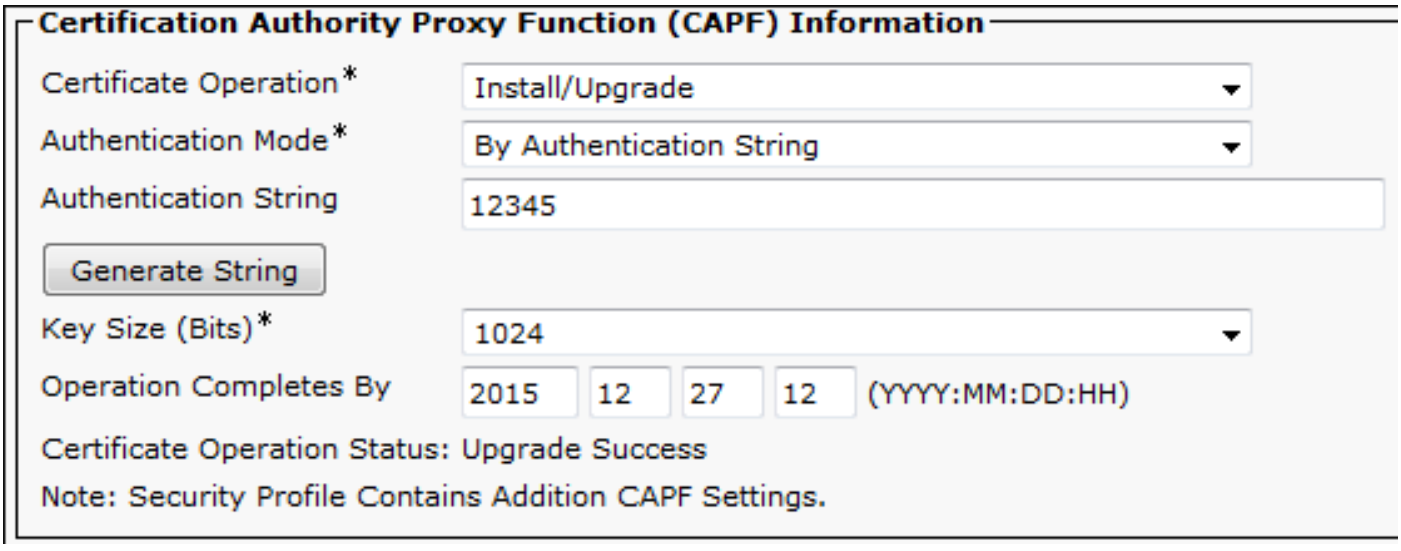


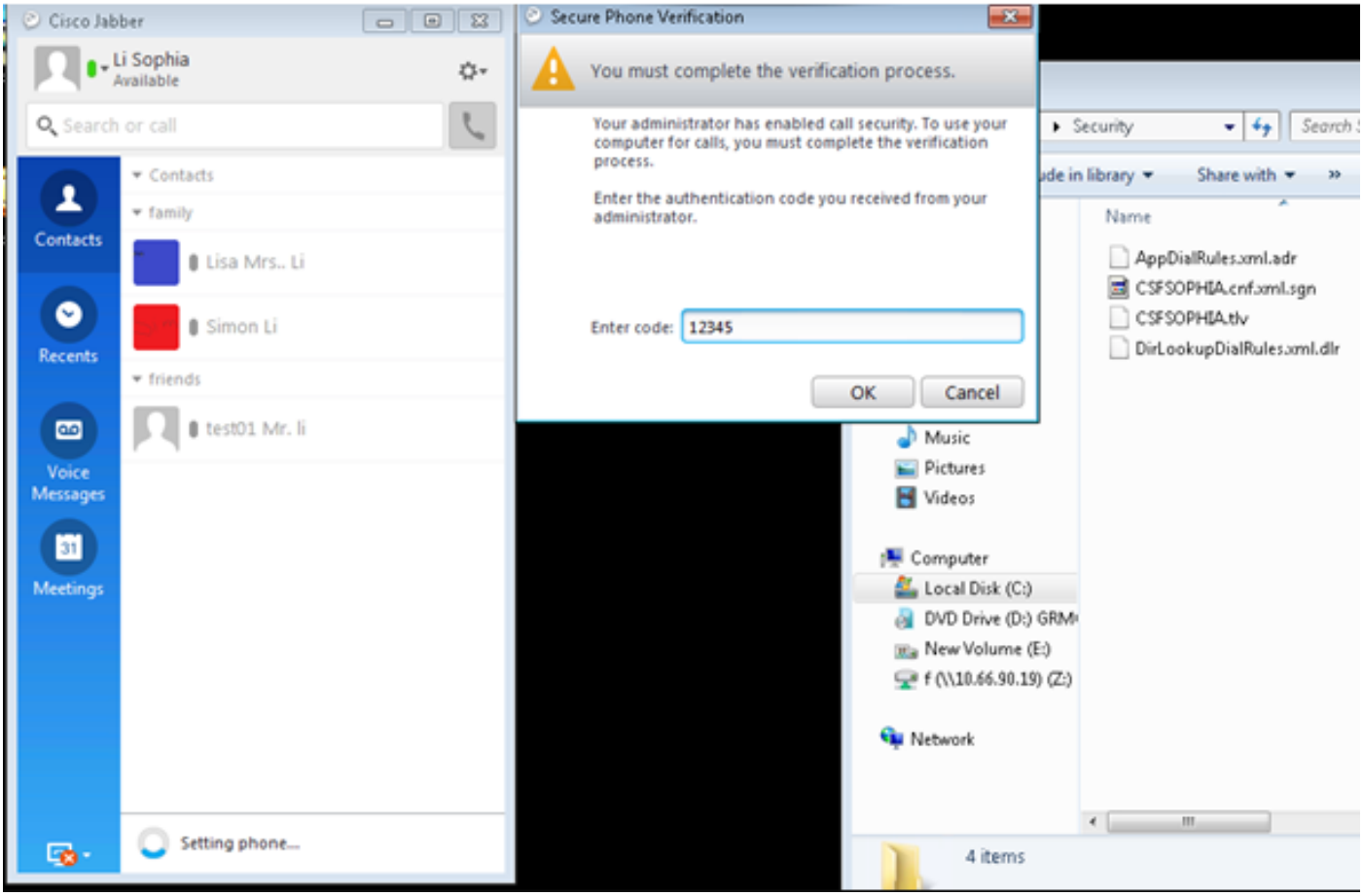
ステップ4：ルートCAをCAPF-trustとして、サーバ証明書をCAPFとしてアップロードします。このテストでは、このルートCAをCallManager-trustとしてアップロードして、CallManagerサービスで署名されたLSCを信頼する必要があるため、JabberとCallManagerサービス間のTLS接続を確立してください。この記事の冒頭で述べたように、このCAが信号/メディア暗号化のためにCallManagerにすでにアップロードされている必要があるため、すべてのサーバのCAを調整する必要があります。IP Phone 802.1xを導入するシナリオでは、CUCMを混合モードにしたり、CAPFにCallManager-trustとして署名するCAをCUCMサーバにアップロードしたりする必要はありません。

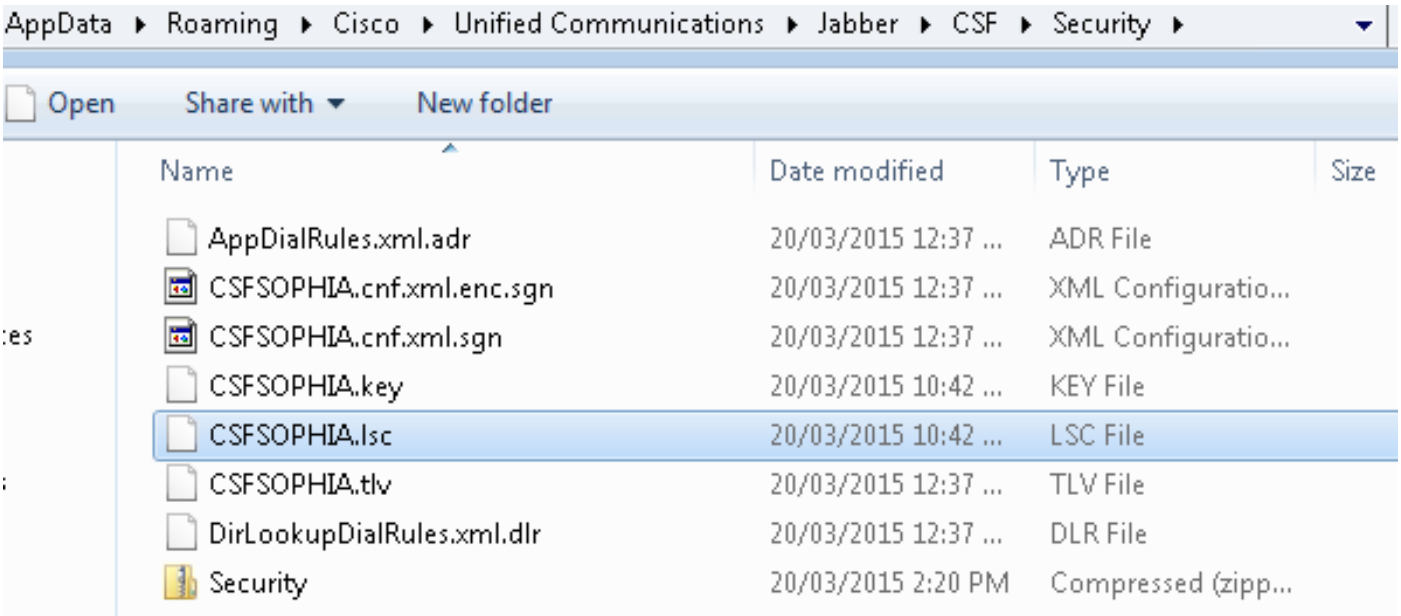
ステップ5:CAPFサービスを再起動します。

ステップ6：すべてのノートでCallManager/TFTPサービスを再起動します。

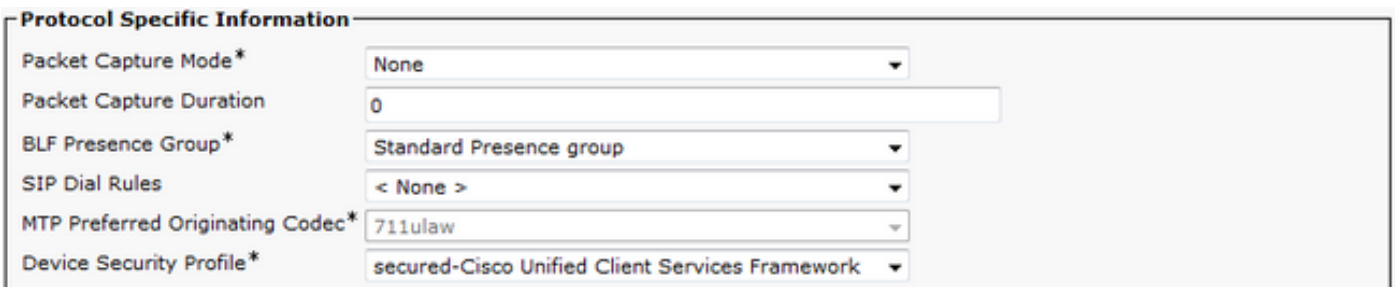
ステップ7:Jabberソフトフォン LSCに署名します。



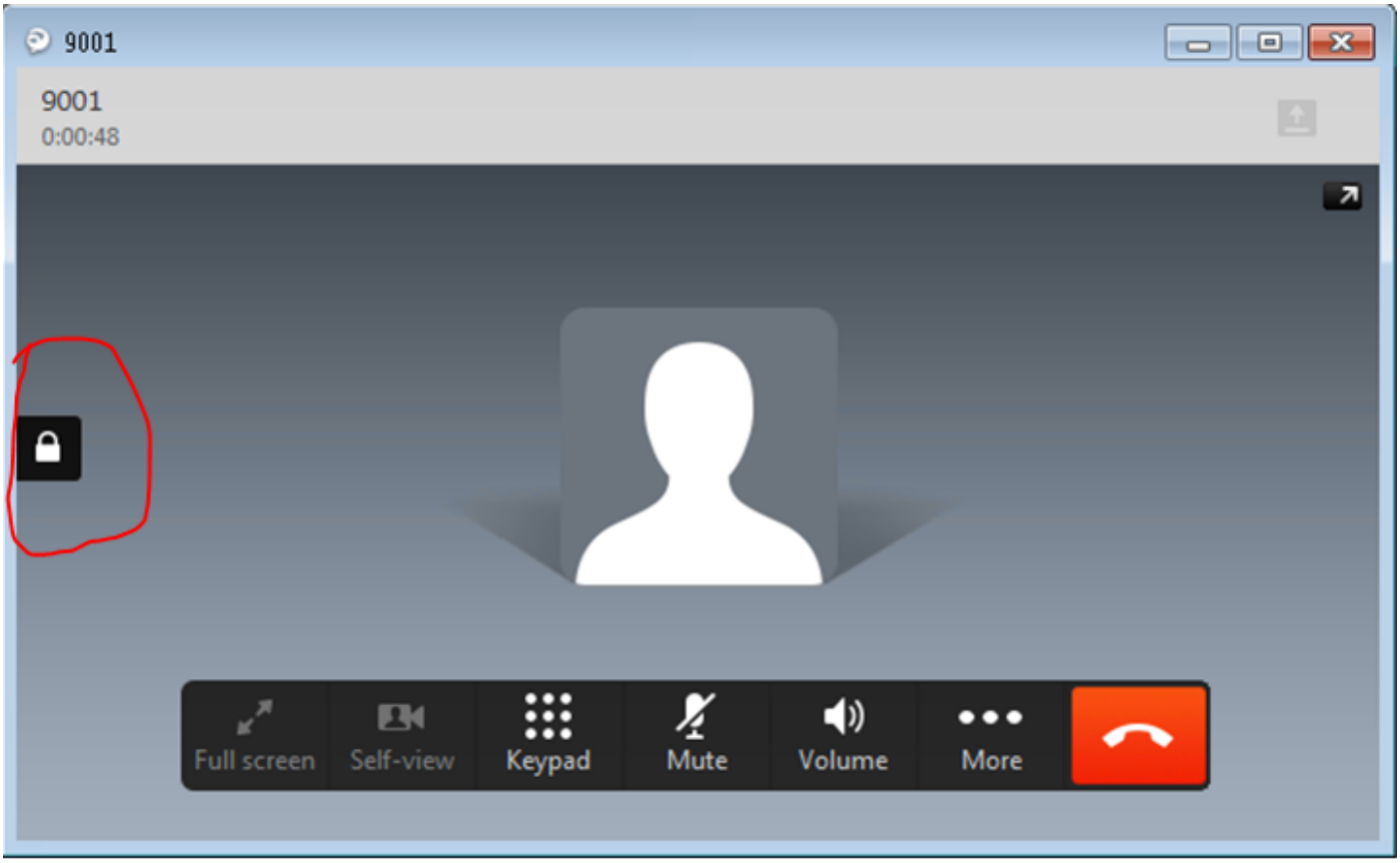




ステップ8:Jabberソフトフォンのセキュリティプロファイルを有効にします。



ステップ9：セキュアなRTPは次のように実行されます。

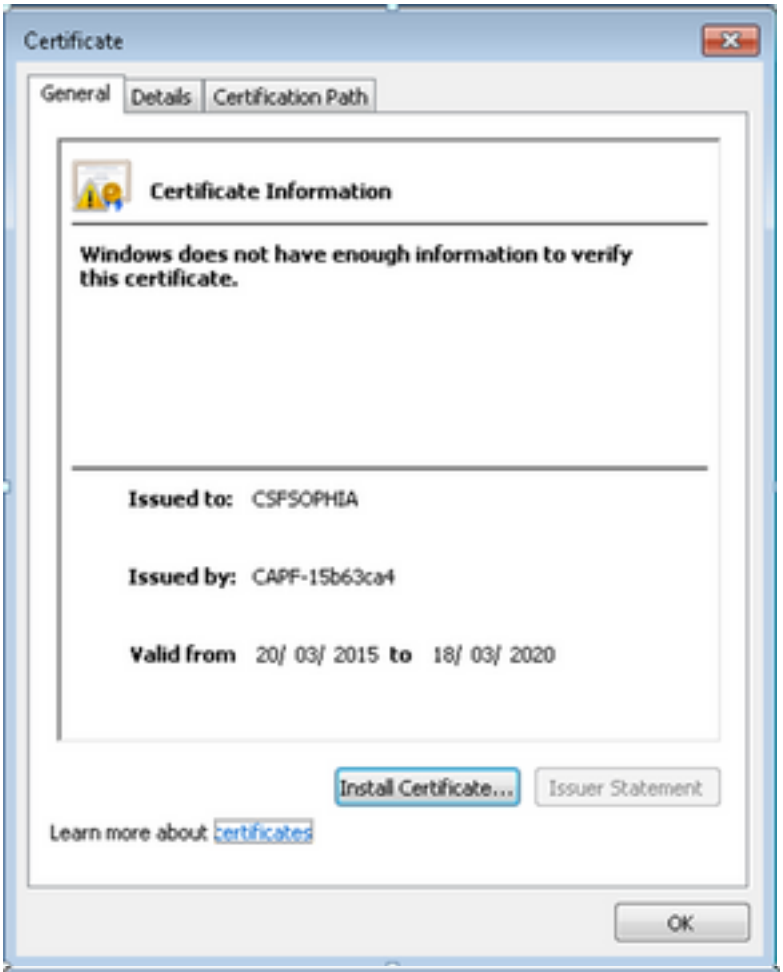


確認

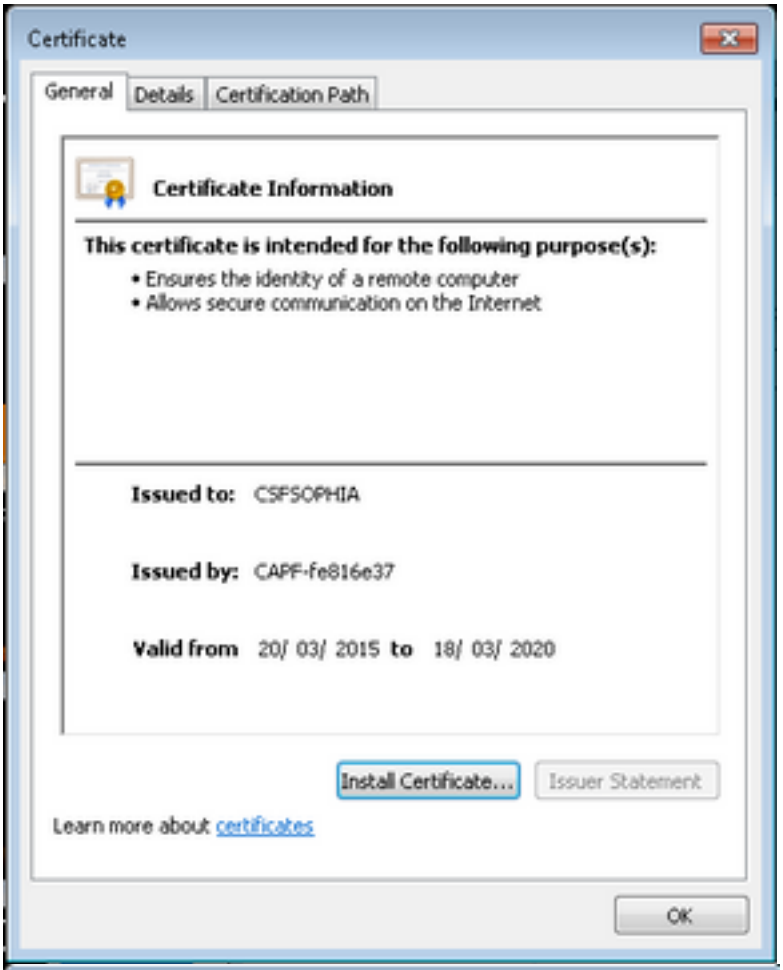
自己署名CAPFおよびCA署名付きCAPFの場合のLSCを比較します。

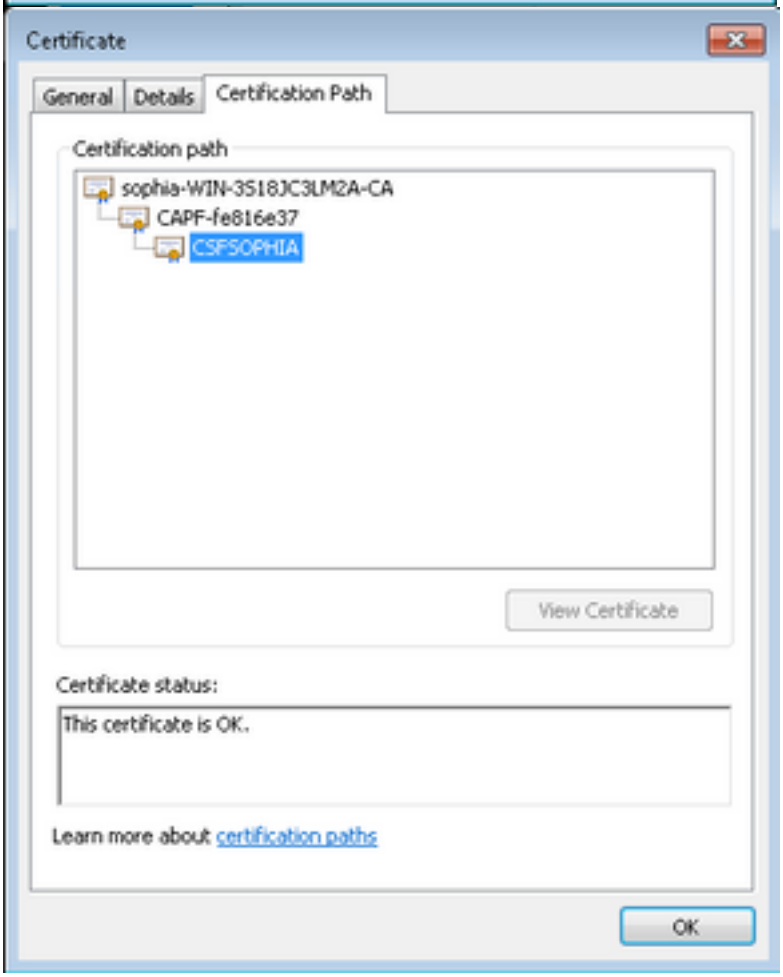
これらのLSCのイメージからわかるように、LSCの観点からは、自己署名CAPFを使用する場合はCAPFがルートCAですが、CA署名付きCAPFを使用する場合はCAPFが下位（中間）CAになります。

自己署名CAPF時のLSC



CA署名付きCAPF時の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

アラート：

この例で証明書チェーン全体を示すJabberクライアントLSCは、IP Phoneとは異なります。AS IP PhoneはRFC 5280(3.2. Certification Paths and Trust)に基づいて設計されているため、AKI(Authority Key Identifier)が欠落しており、CAPFおよびルートCA証明書が証明書チェーンに存在しません。証明書チェーンにCAPF/ルートCA証明書がない場合、ISEにCAPFおよびルート証明書をアップロードせずに、801.x認証中にIP電話を認証するためにISEに問題が発生します。CUCM 12.5には、外部オフラインCAによって直接署名されたLSCを使用する別のオプションがあるため、IP Phone 802.1x認証用にCAPF証明書をISEにアップロードする必要はありません。

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。

関連情報

既知の不具合:CA署名付きCAPF証明書、ルート証明書をCM信頼としてアップロードする必要があります。

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