

CUCM のための CA によって署名する CAPF 認証のテクニカルノート

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[CA によって署名される CAPF の目的](#)

[この PKI のためのメカニズム](#)

[どのように CAPF CSR 他の CSR と異なっていますか。](#)

[設定](#)

[確認](#)

[LSC 場合の自己署名 CAPF](#)

[LSC 場合の CA 署名付き CAPF](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料に Cisco Unified Communications Manager (CUCM) のための認証局 (CA) によって署名するプロキシ 機能 (CAPF) 認証を認証局 (CA) 得る方法を記述されています。外部 CA の CAPF に署名する要求が常にあります。この資料はなぜであるコンフィギュレーション手順重要どのようにはたらくか理解するために示したものです。

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 セキュリティとコンフィギュレーション

使用するコンポーネント

この文書に記載されている情報は基づいた on Cisco Unified Communications Manager バージョン 8.6 および それ 以上です。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、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。

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 サーバ 2008 CA。
- Cisco Jabber for Windows。

背景説明

CA によって署名される CAPF の目的

何人かの顧客は会社によってが他のサーバとそうそこに必要署名した同じ CA の CAPF にである globe 認証 ポリシー with と一直線に並ぶことを望みます。

この PKI のためのメカニズム

デフォルトで、ローカルで固有の認証 (LSC) は CAPF、従って CAPF によってですこのシナリオの電話のための CA 署名します。ただし CAPF を外部 CA によって署名されて得ることを試みるときそしてこのシナリオの CAPF は下位 CA が中間 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 LSC へ LSC へ CA 署名付き CAPF をするとき自己署名 CAPF をするとき、CAPF ルートCA です下位 (中間) CA です。

どのように CAPF CSR 他の CSR と異なっていますか。

[RFC5280](#) に見なして、キー使用法 拡張は認証に含まれているキーの目的 (例えば、暗号化、署名するシグニチャ、認証) を定義します。CAPF は認証 プロキシであり、CA および電話にリーフ (ユーザ識別) として機能する IPSec 認証 CallManager のような他の認証に、Tomcat 署名、できますが。それらのための CSR 調べるとき、CAPF CSR に CertificateSign ロール他がないことを見ることができます。

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, IPSec End System
  X509v3 Key Usage:
    Digital Signature, Certificate Sign
```

CallManager CSR:

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

IPSec CSR:

属性: 要求された拡張: X509v3 拡張キー使用法: 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 キー使用法: デジタル署名、キー暗号化、データ暗号化、キー協定

設定

これは外部 CA の CAPF に署名するプロシージャです。

ステップ 1: セキュリティ クラスタとして CUCM クラスタを作って下さい。

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

ステップ 2.イメージに示すように、CAPF CSR を生成して下さい。

<https://10.67.81.115/cmplatform/certificateGenerateNewCsr.do>

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite type

Generate Certificate Signing Request

Certificate Purpose* CAPF

Distribution* CCM105PUB.sophia.li

Common Name* CCM105PUB.sophia.li

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

ステップ 3. CA とこれに署名しました (Windows 2008 CA の従属テンプレートを使用して) 。

注: ユーザ 下位認証局 テンプレートがこの認証に署名することを必要とします。

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
J7Xot0WbkseyQVWsHBY17w==
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Submit >

10.67.81.120/certsrv/certfnsh.asp


Cisco Service Award OS X Yosemite 虚拟机... CALO Project Squared

Microsoft Active Directory Certificate Services -- sophia-WIN-3S18JC3LM2A-C

Certificate Issued

The certificate you requested was issued to you.

DER encoded or
 Base 64 encoded


[Download certificate](#)
[Download certificate chain](#)

ステップ 4. CAPF 信頼としてルートCA および CAPF としてサーバ証明をアップロードして下さい。

ステップ 5. CAPF サービスを再開して下さい。

ステップ 6. すべてのメモの CallManager/TFTP サービスを再開して下さい。

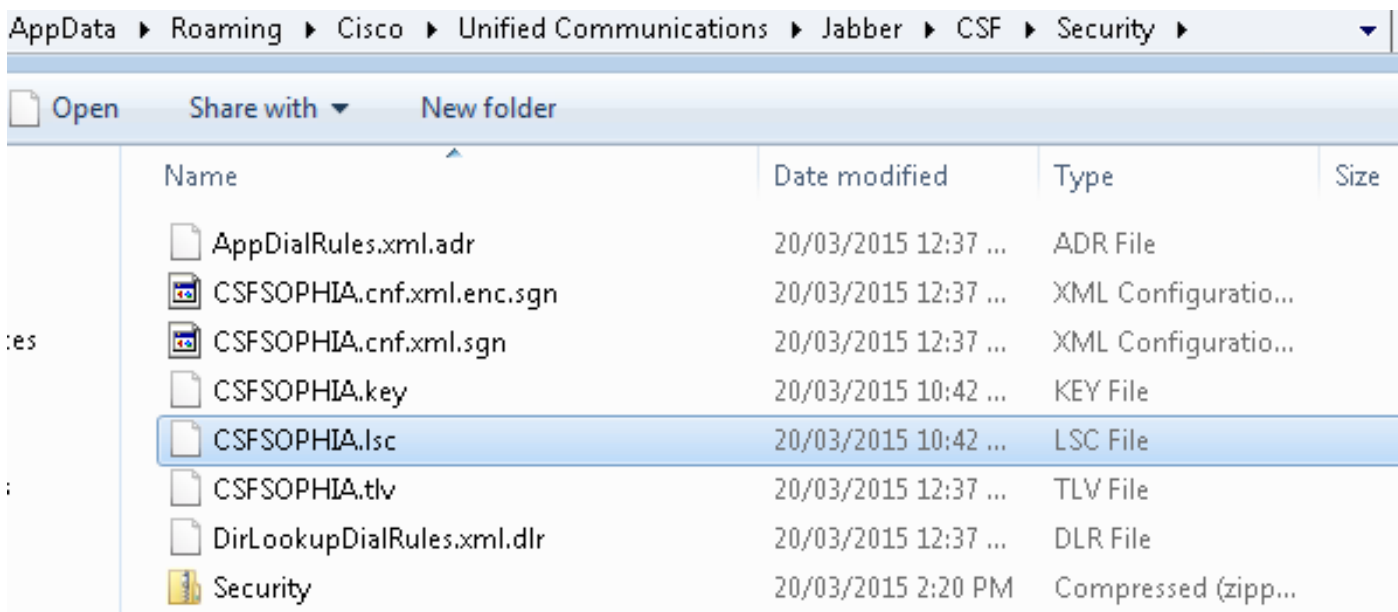
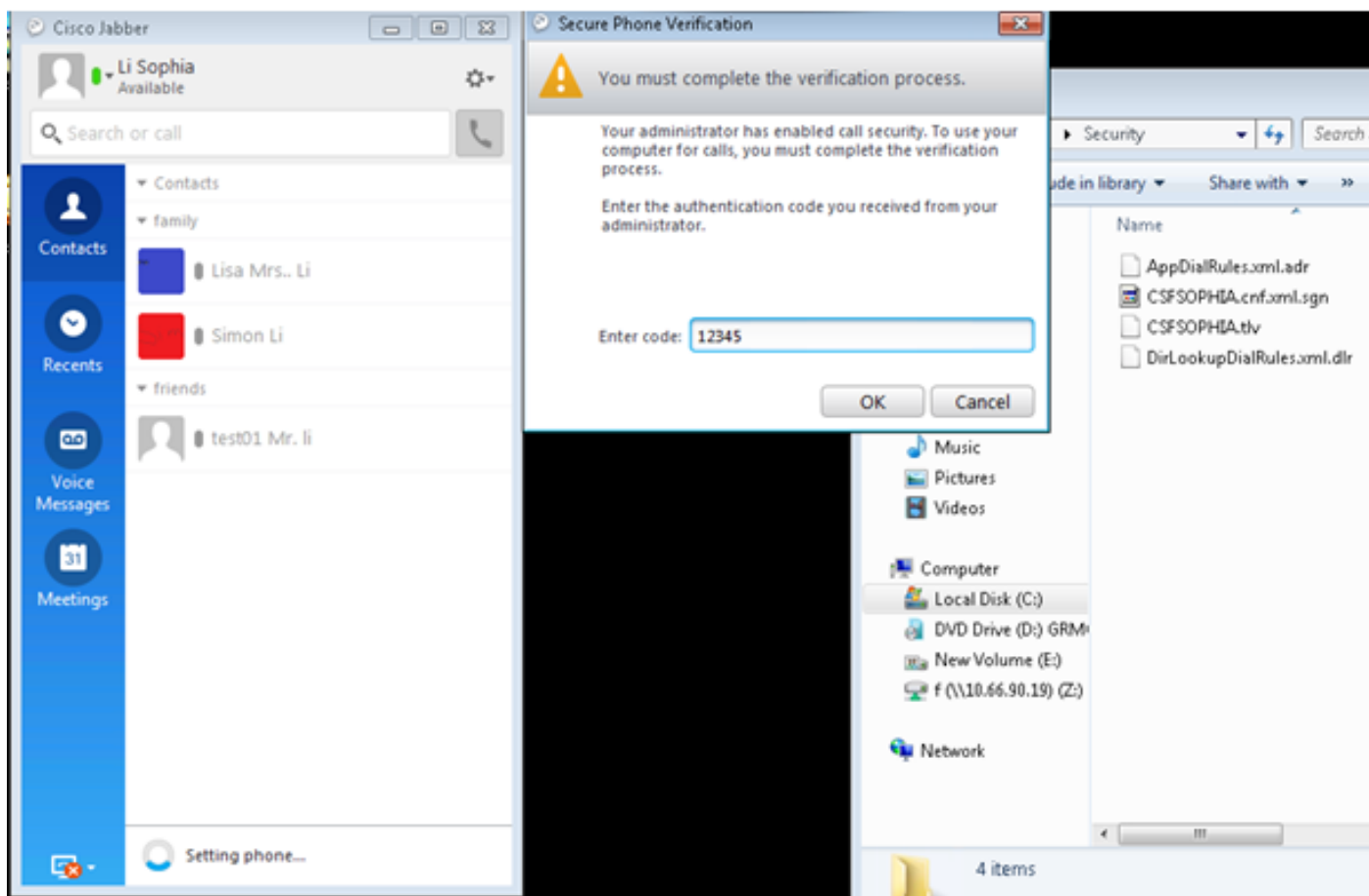
ステップ 7. Jabber softphone LSC に署名しました。

Certification Authority Proxy Function (CAPF) Information

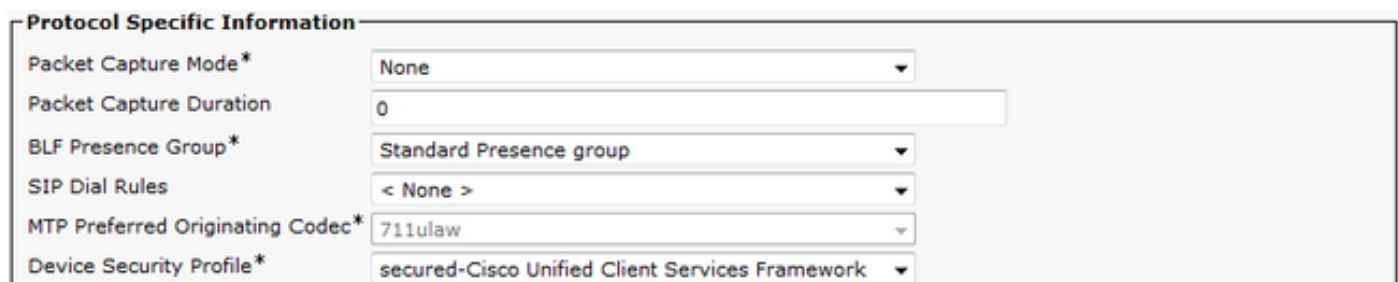
Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
Authentication String	12345
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success

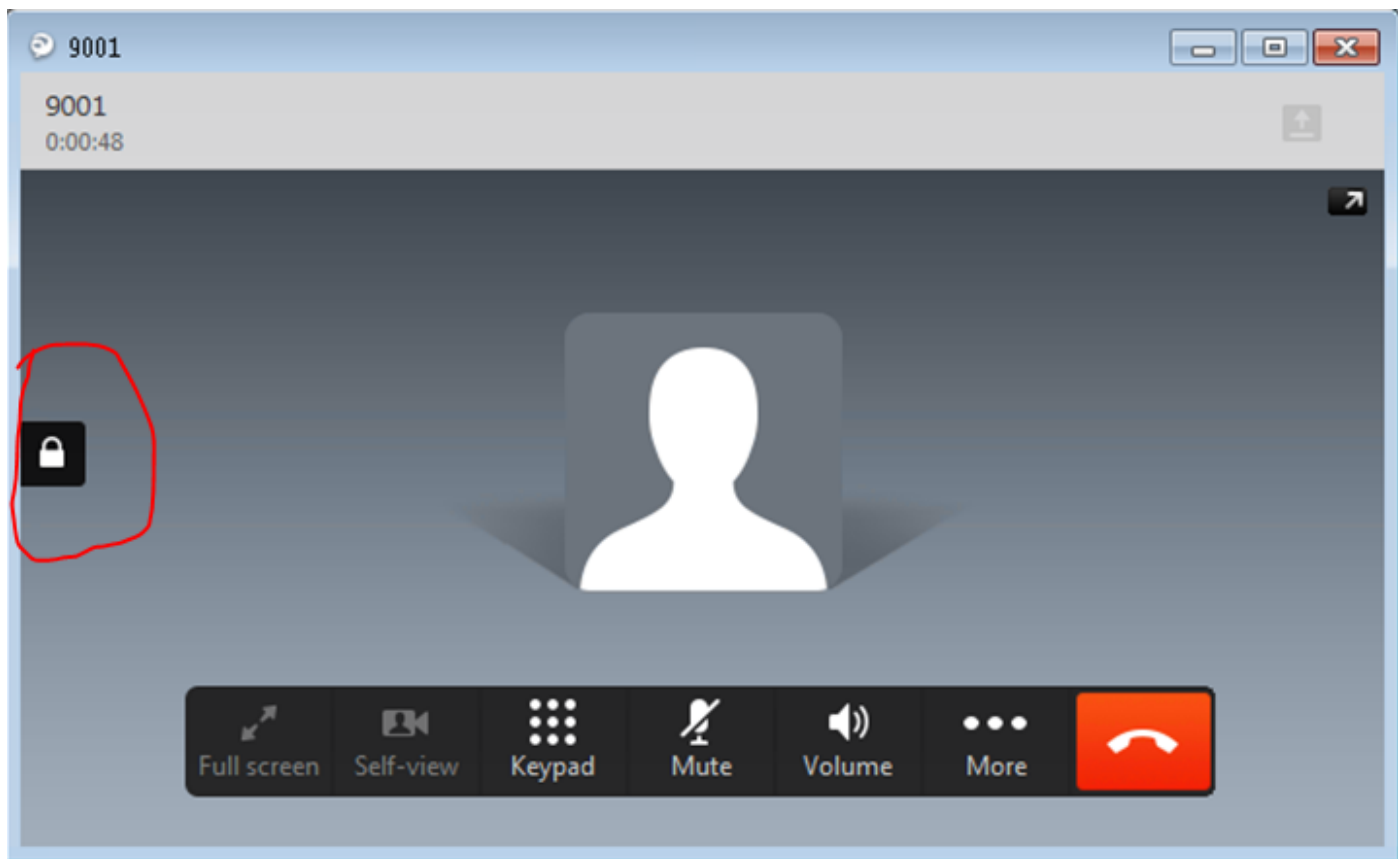
Note: Security Profile Contains Addition CAPF Settings.



ステップ 8. Jabber softphone のためのセキュリティプロファイルを有効にして下さい。



ステップ 9 この場合保護された RTP はとして起こります:

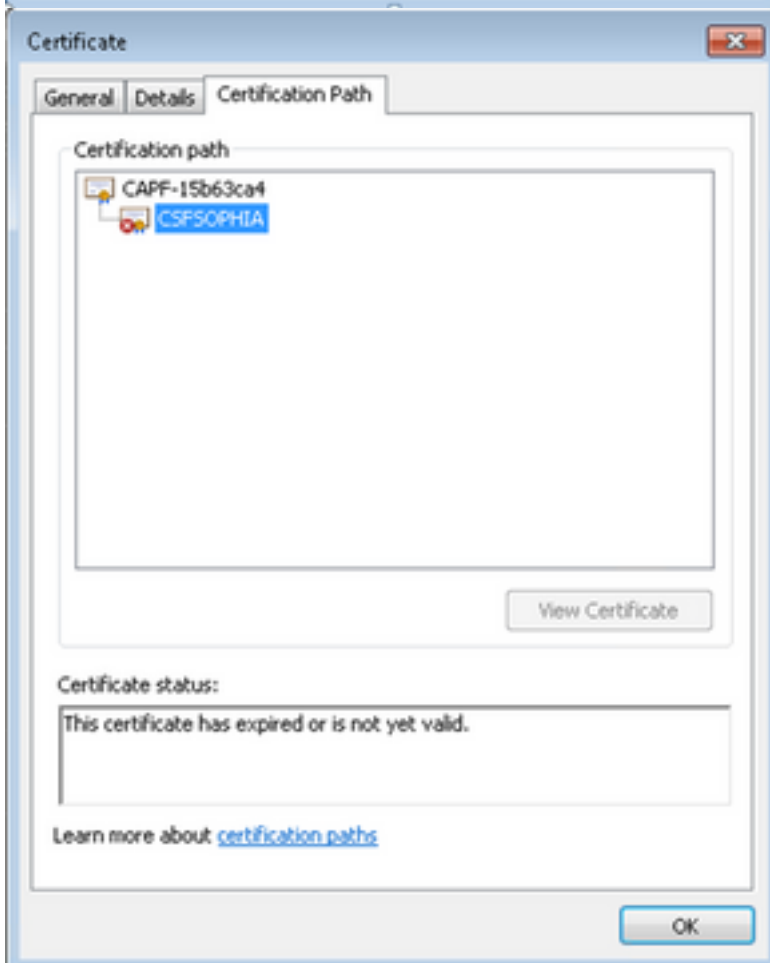
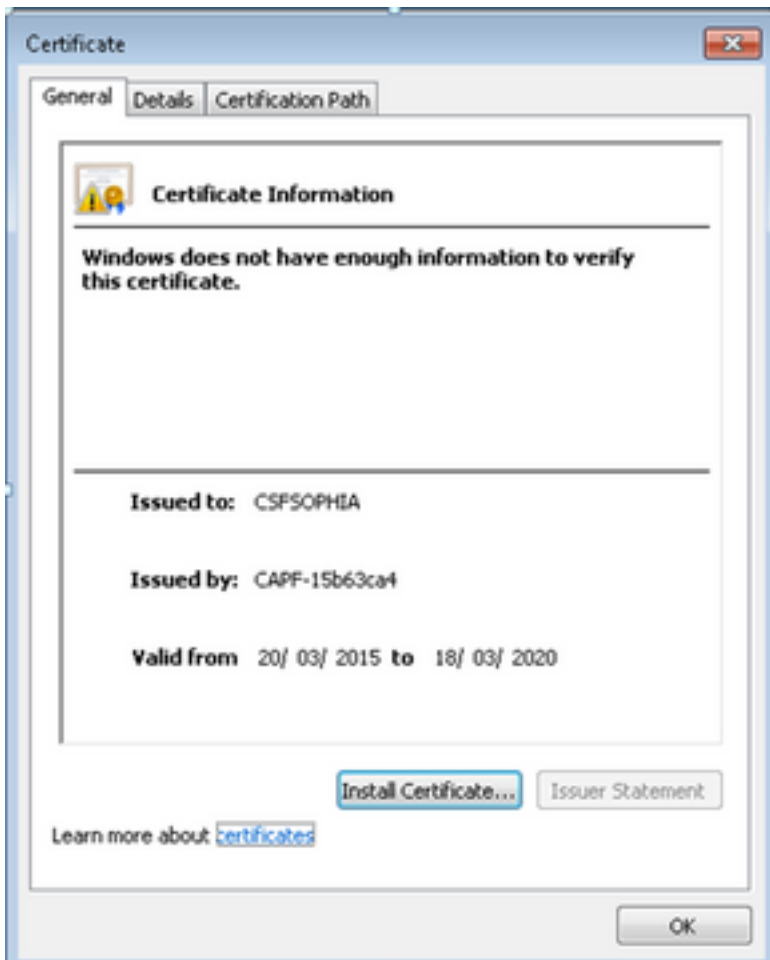


確認

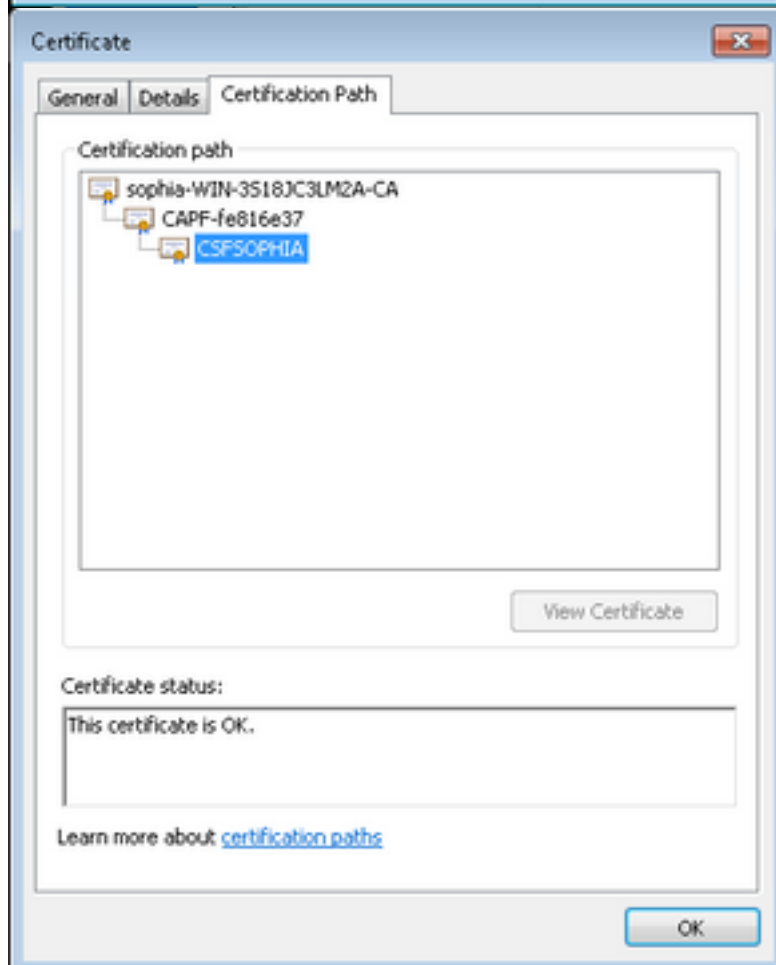
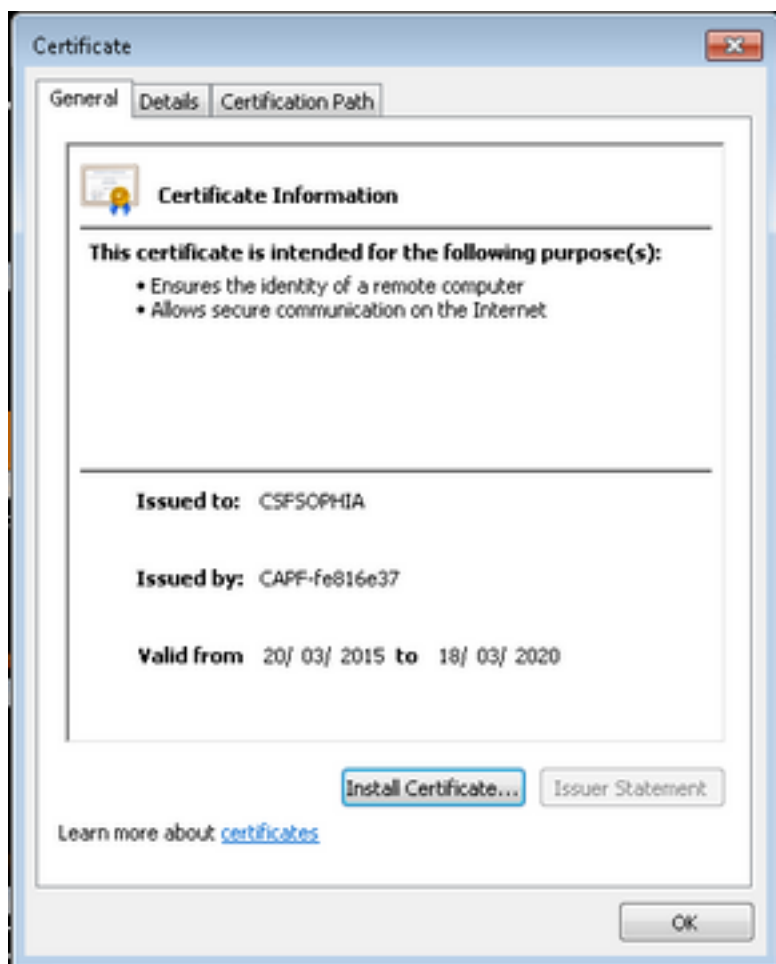
自己焼かれた CAPF および CA 署名付き CAPF 時 LSC を比較して下さい:

自己署名 CAPF CAPF を使用する場合はこれらのイメージから CAPF であるルートCA である下位 (中間) CA CA 署名付き CAPF を使用しながら、LSC 観点からが、わかるように。

LSC 場合の自己署名 CAPF



LSC 場合の CA 署名付き CAPF



トラブルシューティング

現在のところ、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

既知の障害: CA によって署名される CAPF 認証は CM 信頼として、ルート証明書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