

CAPF Certificate Signed by CA for CUCM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Limitation](#)

[Background Information](#)

[Purpose of CA Signed CAPF](#)

[Mechanism for this PKI](#)

[How CAPF CSR is Different from other CSRs?](#)

[Configure](#)

[Verify](#)

[LSC when Self-signed CAPF](#)

[LSC when CA-signed CAPF](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to obtain a Certificate Authority Proxy Function (CAPF) certificate signed by Certificate Authority (CA) for Cisco Unified Communications Manager (CUCM). There are always requests to sign the CAPF with external CA. This document shows why to understand how it works is as important as the configuration procedure.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Public Key Infrastructure (PKI)
- CUCM Security Configuration

Components Used

The information in this document is based on Cisco Unified Communications Manager version 8.6 and above.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Limitation

Different CA might have different requirements to the CSR. There are reports that different version of OpenSSL CA have some specific ask for the CSR however Microsoft Windows CA works well with the CSR from Cisco CAPF so far, which discussion will not be covered in this article.

Related Products

This document can also be used with these hardware and software versions:

- Microsoft Windows Server 2008 CA.
- Cisco Jabber for Windows (different versions might have different name for folder to store the LSC).

Background Information

Purpose of CA Signed CAPF

Some customers would like to align with the global certificate policy with the company so there is a need to sign the CAPF with the same CA as other servers.

Mechanism for this PKI

By default, Locally Significant Certificate (LSC) is signed by the CAPF, so the CAPF is the CA for phones in this scenario. However, when you try to get the CAPF signed by the external CA, then the CAPF in this scenario acts as subordinate CA or intermediate CA.

The difference between self-signed CAPF and CA-signed CAPF is: the CAPF is the root CA to LSC when doing self-signed CAPF, the CAPF is the subordinate (intermediate) CA to LSC when doing CA-signed CAPF.

How CAPF CSR is Different from other CSRs?

Regarding to [RFC5280](#), The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. CAPF is a certificate proxy and CA and it can sign certificate to the phones but the other certificate like CallManager, Tomcat, IPsec they act as leaf (user identity). When you look into the CSR for them, you can see the CAPF CSR has **Certificate Sign** role but not the others.

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:

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

Configure



Here is one scenario, external root CA is used to sign CAPF certificate: to encrypted the signal/media for Jabber client and IP phone.

Step 1. Make your CUCM cluster as a security cluster.

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

Step 2. As shown in the image, generate the CAPF CSR.

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

Step 3. Signed this with the CA (using subordinate template in Windows 2008 CA).

Note: You need to use **Subordinate Certification Authority** template to sign this certificate.

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-----
```

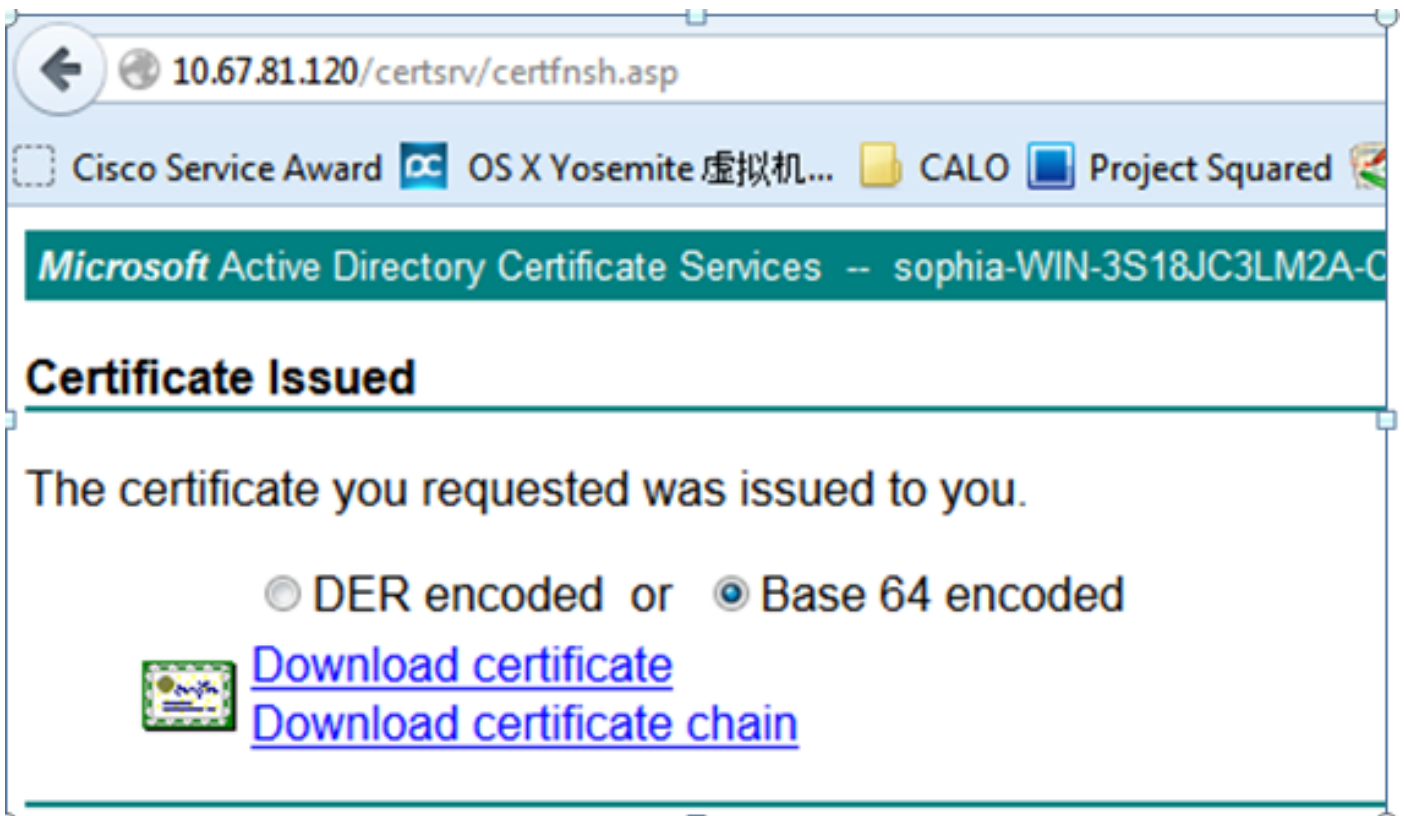
Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

Submit >



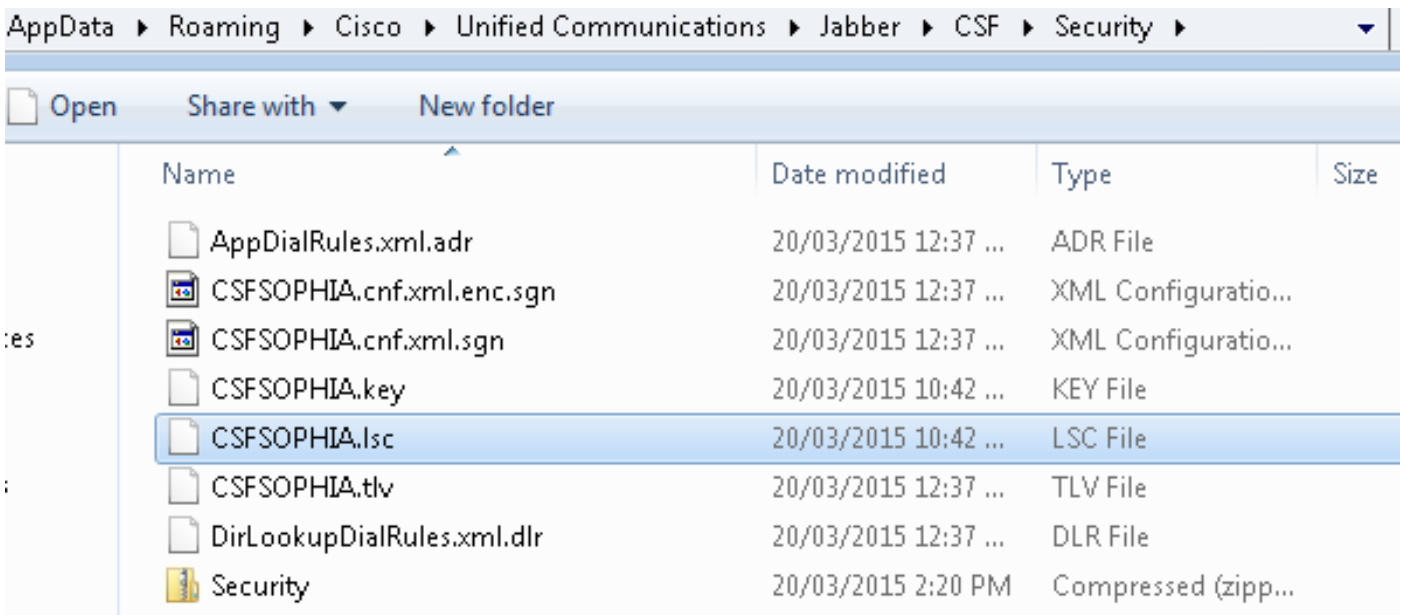
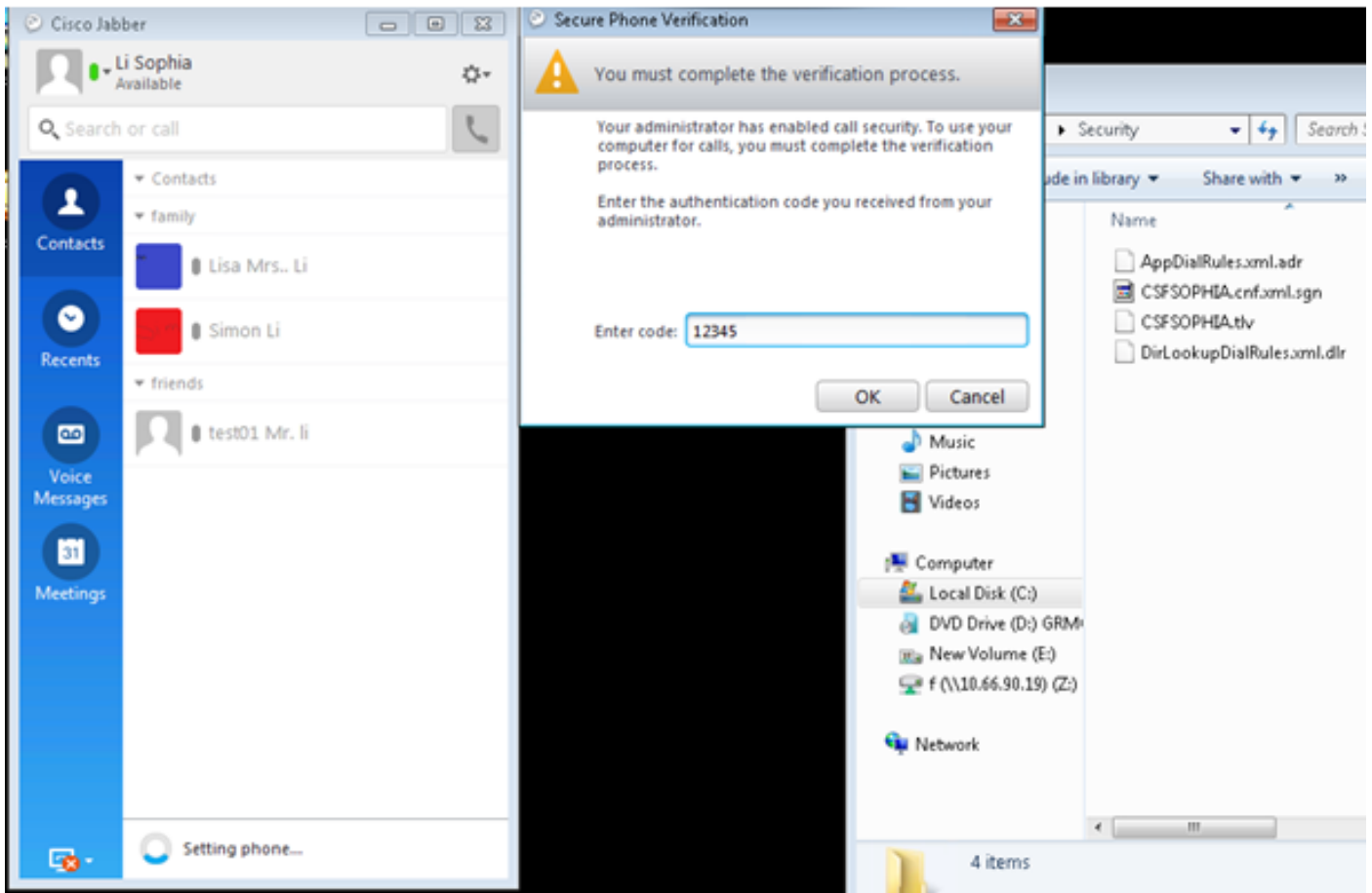
Step 4. Upload the root CA as CAPF-trust and the server certificate as CAPF. For this test, please also upload this Root CA as CallManager-trust to have TLS connection between Jabber and CallManager service as the signed LSC needs to be trusted by CallManager service as well. As mentioned at the beginning of this article, there is a need to align the CA for all servers so this CA should have been uploaded to CallManager already for signal/media encryption. For the scenario of deploying IP phone 802.1x, you don't have to make the CUCM as mixed mode or upload the CA which signs the CAPF as CallManager-trust in to the CUCM server.

Step 5. Restart the CAPF service.

Step 6. Restart the CallManager/TFTP services in all nodes.

Step 7. Signed the Jabber softphone LSC.

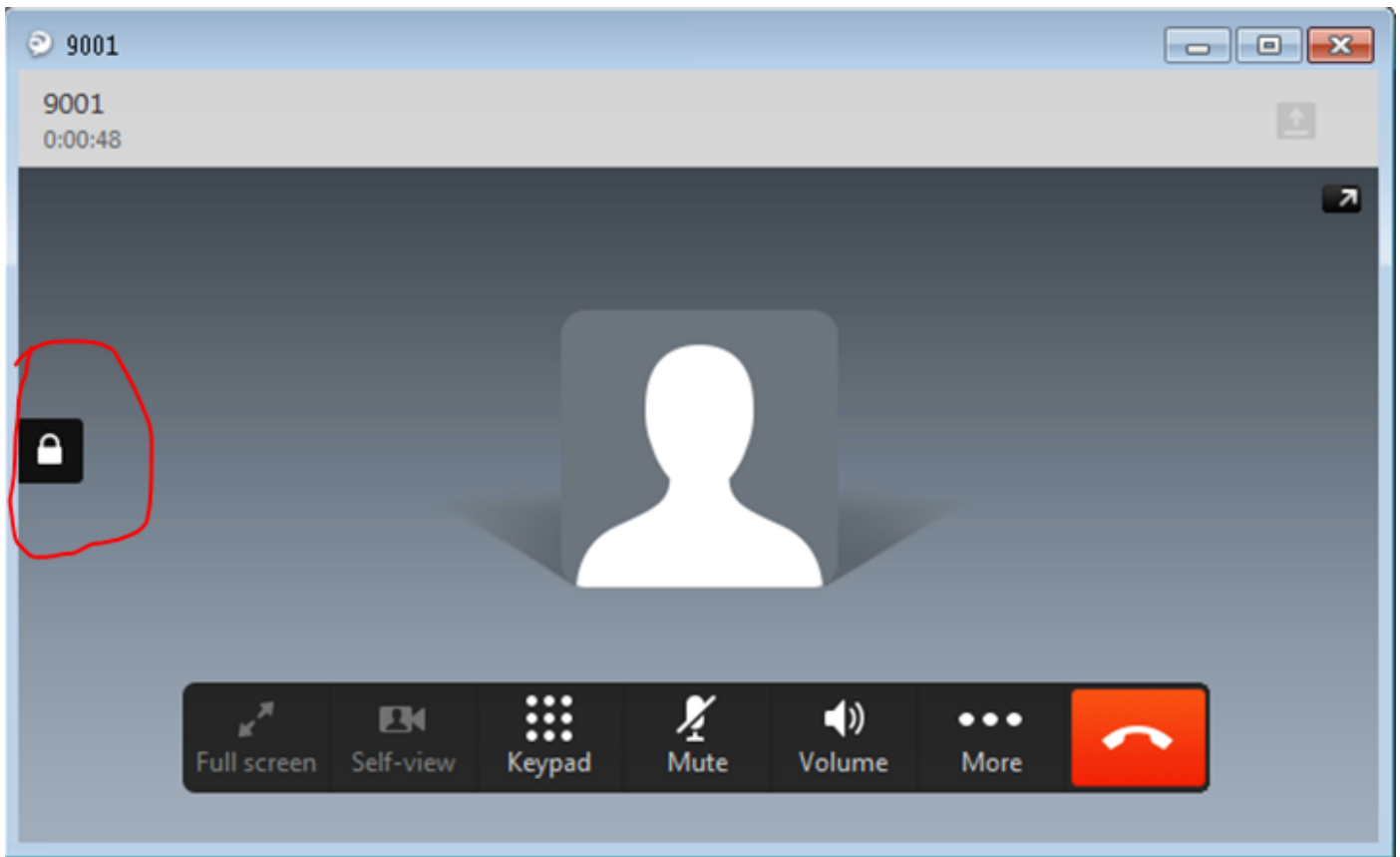
Certification Authority Proxy Function (CAPF) Information	
Certificate Operation*	Install/Upgrade
Authentication Mode*	By Authentication String
Authentication String	12345
<input type="button" value="Generate String"/>	
Key Size (Bits)*	1024
Operation Completes By	2015 12 27 12 (YYYY:MM:DD:HH)
Certificate Operation Status: Upgrade Success	
Note: Security Profile Contains Addition CAPF Settings.	



Step 8. Enable the security profile for Jabber softphone.



Step 9. Now secured RTP happens as:

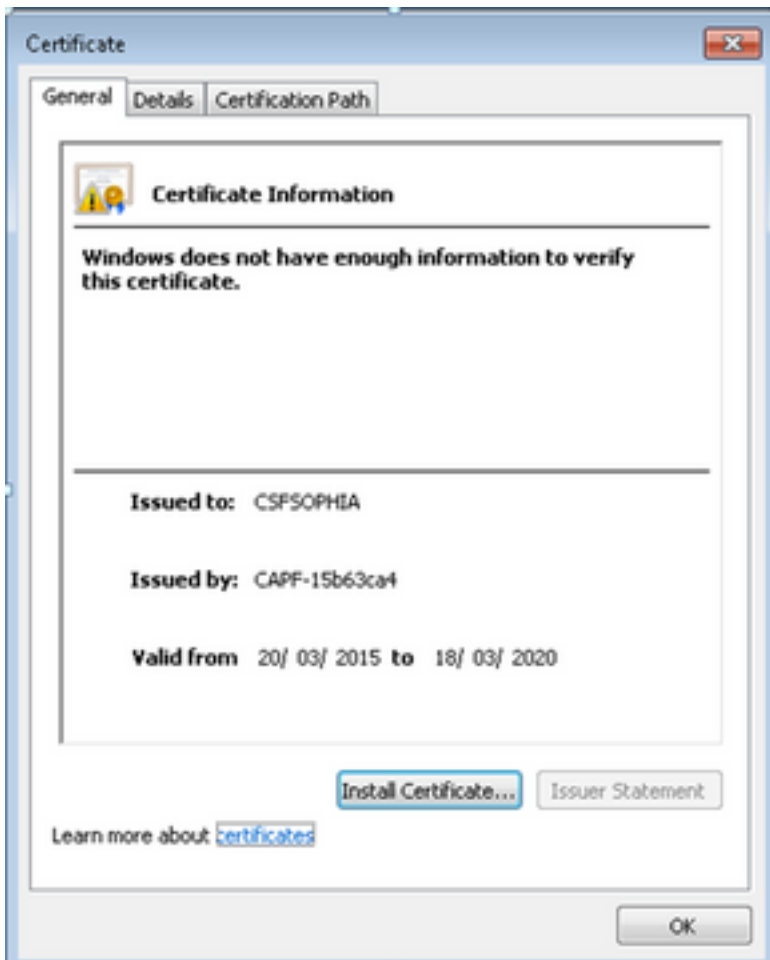


Verify

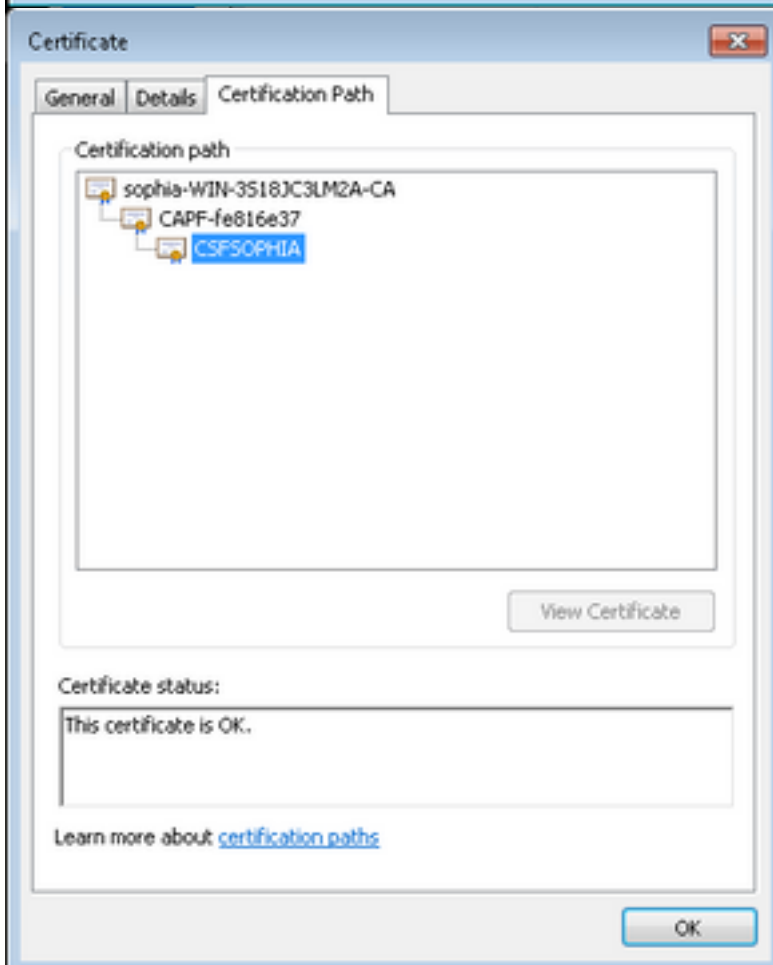
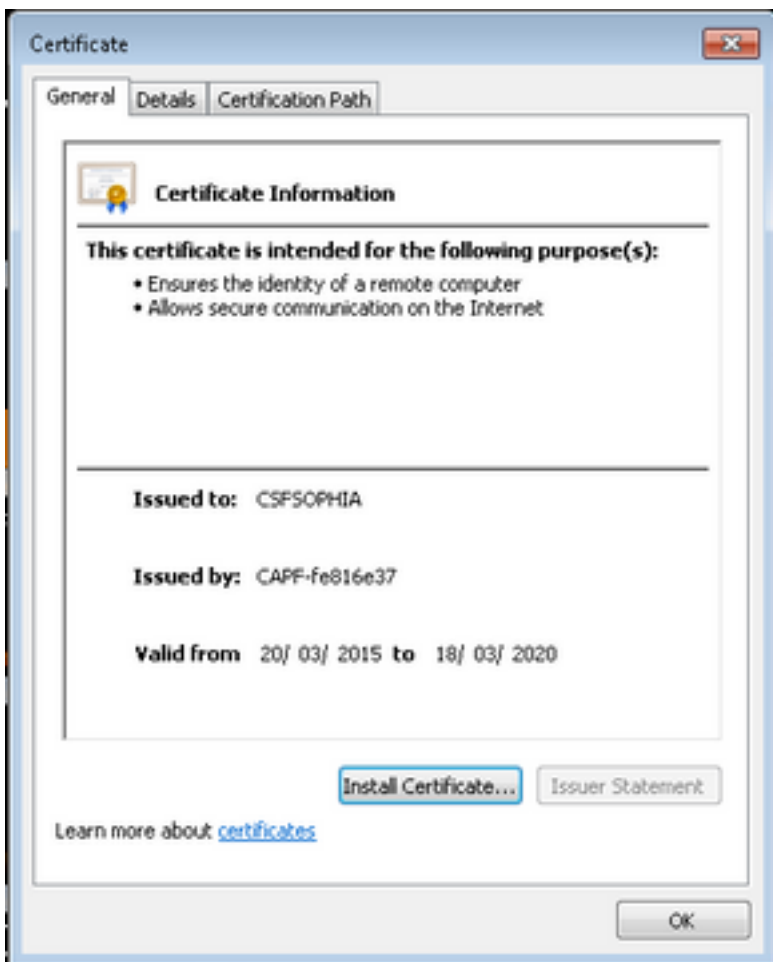
Compare the LSC when self-signed CAPF and CA-signed CAPF:

As you can see from these images for LSC, from LSC point of view, CAPF is the root CA when using self-signed CAPF but CAPF is the subordinate (intermediate) CA while using CA-signed CAPF.

LSC when Self-signed CAPF



LSC when CA-signed CAPF



Alert:

the Jabber client LSC showing whole certificate chain in this example is different from the IP phone. AS IP phones are designed based on the RFC 5280 (3.2. Certification Paths and Trust) then the AKI (Authority Key Identifier) is missing, then CAPF and the root CA certificate do not present in the certificate chain. Missing the CAPF/Root CA certificate in the certificate chain will cause some issue to ISE to authenticate IP phones during 801.x authentication without uploading the CAPF and Root Certificates to the ISE. There is another option in CUCM 12.5 with LSC signed by external offline CA directly so CAPF certificate is not needed to be uploaded to the ISE for IP phone 802.1x authentication.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

Known defect: CA signed CAPF Certificate, root cert must be uploaded as CM-trust:

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