Certificato CAPF firmato da CA per CUCM

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Limitazione](#)
[Premesse](#)
[Scopo di CAPF con firma CA](#)
[Meccanismo per questa PKI](#)
[Quali sono le differenze tra CAPF CSR e altri CSR?](#)
[Configurazione](#)
[Verifica](#)
[LSC se CAPF autofirmato](#)
[LSC quando CAPF con firma CA](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come ottenere un certificato CAPF (Certificate Authority Proxy Function) firmato da CA (Certification Authority) per Cisco Unified Communications Manager (CUCM). Sono sempre presenti richieste per firmare il file CAPF con una CA esterna. Questo documento mostra perché comprenderne il funzionamento è importante quanto la procedura di configurazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PKI (Public Key Infrastructure)
- Configurazione protezione CUCM

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Unified Communications Manager versione 8.6 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Limitazione

CA diverse possono avere requisiti diversi rispetto al CSR. In alcuni casi, le diverse versioni di OpenSSL CA richiedono esplicitamente l'uso del CSR. Tuttavia, Microsoft Windows CA finora funziona bene con il CSR di Cisco CAPF, e la discussione non verrà trattata in questo articolo.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- CA di Microsoft Windows Server 2008.
- Cisco Jabber per Windows (è possibile che versioni diverse abbiano nomi diversi per la cartella in cui archiviare LSC).

Premesse

Scopo di CAPF con firma CA

Alcuni clienti desiderano allinearsi ai criteri dei certificati globali della società, pertanto è necessario firmare il file CAPF con la stessa CA degli altri server.

Meccanismo per questa PKI

Per impostazione predefinita, il certificato LSC (Locally Significant Certificate) è firmato dal file CAPF, quindi in questo scenario il file CAPF è la CA per i telefoni. Tuttavia, quando si tenta di ottenere la firma CAPF da parte della CA esterna, il CAPF in questo scenario funge da CA subordinata o intermedia.

La differenza tra CAPF autofirmato e CAPF con firma CA è la seguente: CAPF è la CA radice per LSC quando si esegue CAPF autofirmato, CAPF è la CA subordinata (intermedia) per LSC quando si esegue CAPF con firma CA.

Quali sono le differenze tra CAPF CSR e altri CSR?

Per quanto riguarda la RFC5280, l'estensione per l'utilizzo della chiave definisce lo scopo (ad esempio, cifratura, firma, firma del certificato) della chiave contenuta nel certificato. CAPF è un proxy di certificato e CA e può firmare il certificato ai telefoni ma l'altro certificato come CallManager, Tomcat, IPSec agiscono come foglia (identità utente). Se si esamina il CSR per verificare la presenza di tali elementi, è possibile verificare che il ruolo **Firma certificato di** CAPF CSR sia stato assegnato ma non agli altri.

CSR CAPF:

```
Attributes:
Requested Extensions:
```

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

CSR Tomcat:

```
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
```

CSR CallManager:

```
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
```

CSR IPSec:

Attributi: Estensioni richieste: Utilizzo esteso chiave X509v3: Autenticazione server Web TLS, autenticazione client Web TLS, utilizzo chiave IPSec End System X509v3: Firma digitale, cifratura chiave, cifratura dati, accordo chiave

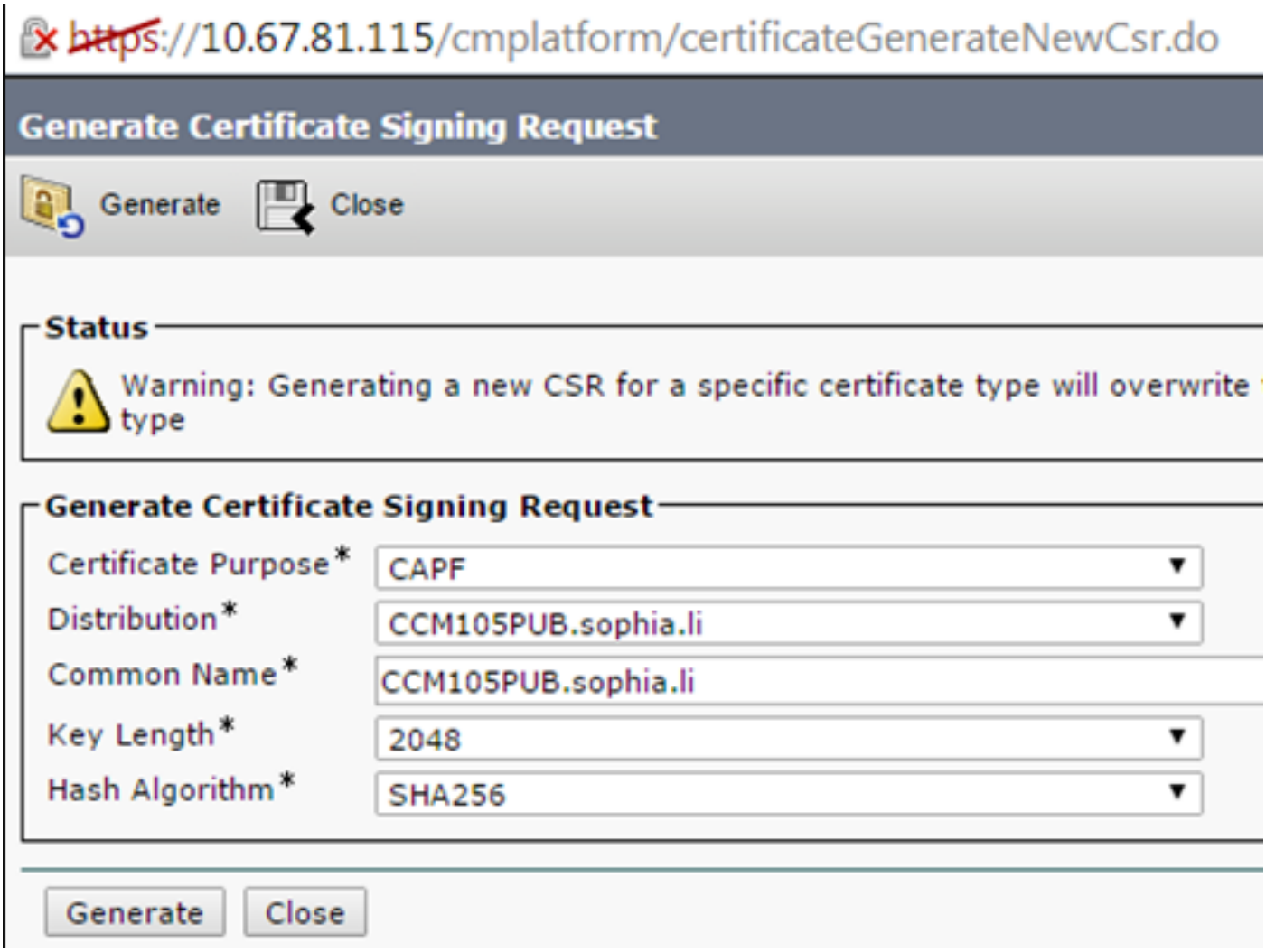
Configurazione

Di seguito è riportato uno scenario in cui viene utilizzata la CA radice esterna per firmare il certificato CAPF: per crittografare il segnale/supporto per il client Jabber e il telefono IP.

Passaggio 1. Trasformare il cluster CUCM in un cluster di sicurezza.

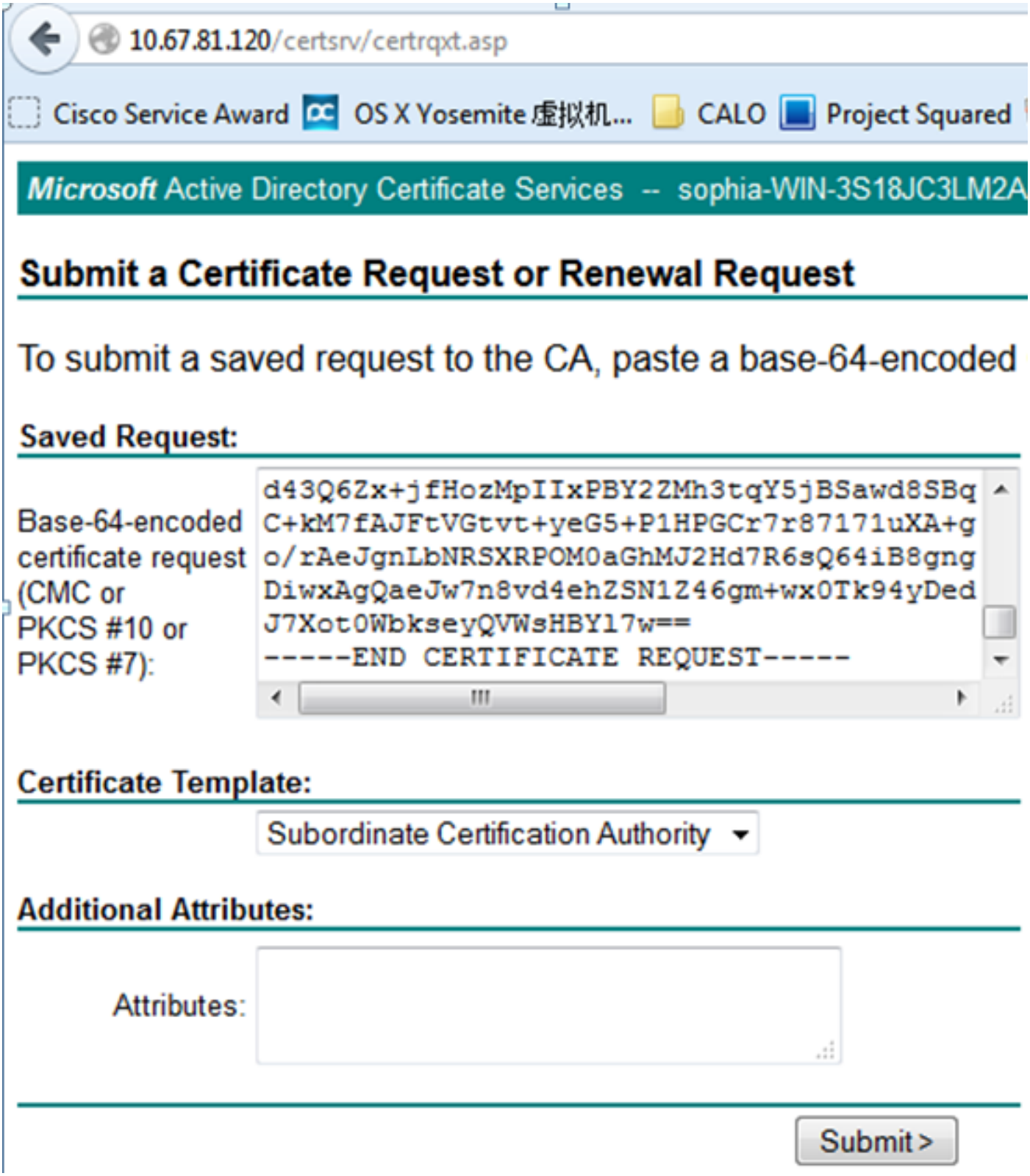
```
admin:utils ctl set-cluster mixed-mode
```

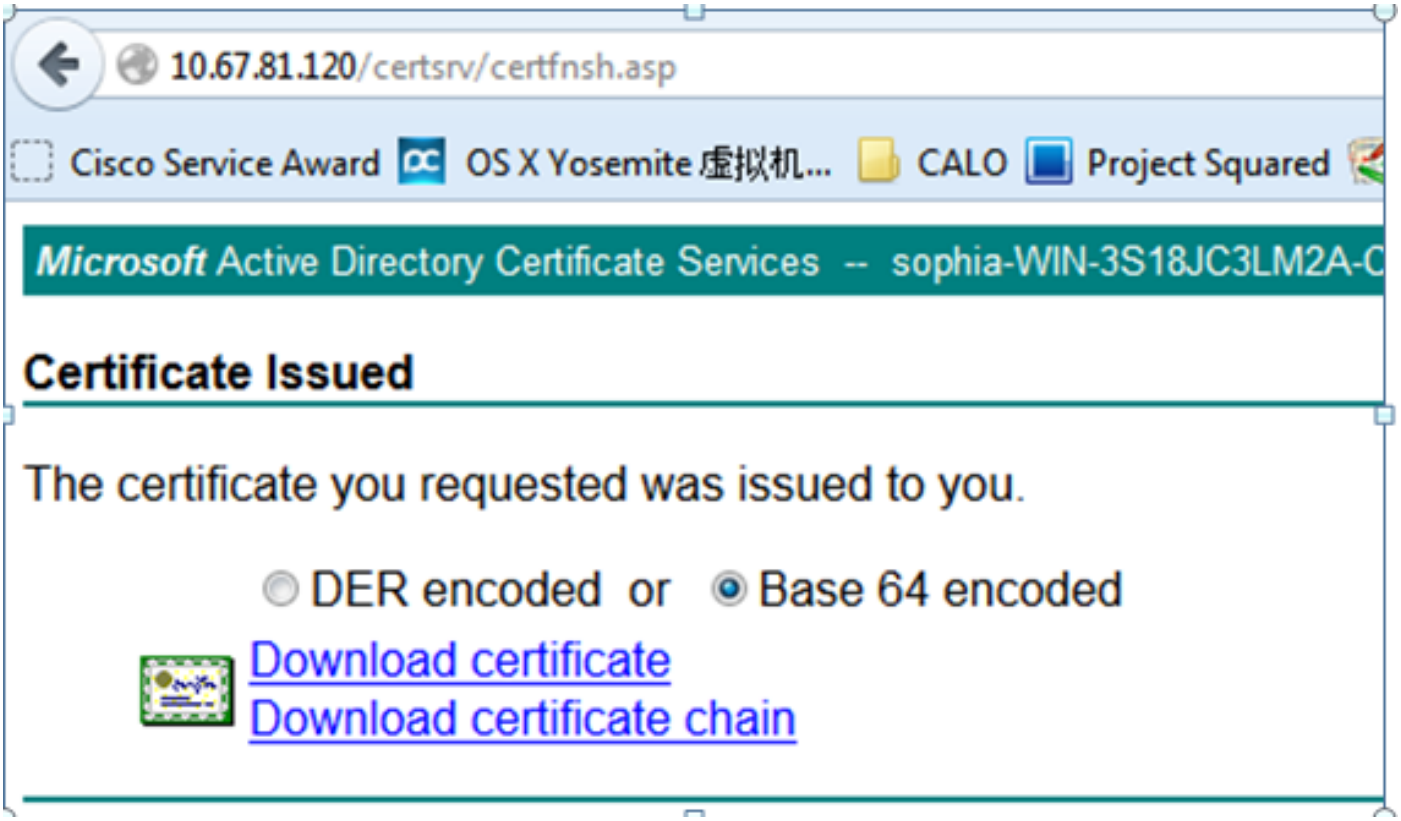
Passaggio 2. Come mostrato nell'immagine, generare il CSR CAPF.



Passaggio 3. Firmato con l'autorità di certificazione (utilizzando il modello subordinato nell'autorità di certificazione di Windows 2008).

> **Nota:** Per firmare il certificato è necessario utilizzare il modello **Autorità di certificazione subordinata**.


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 >

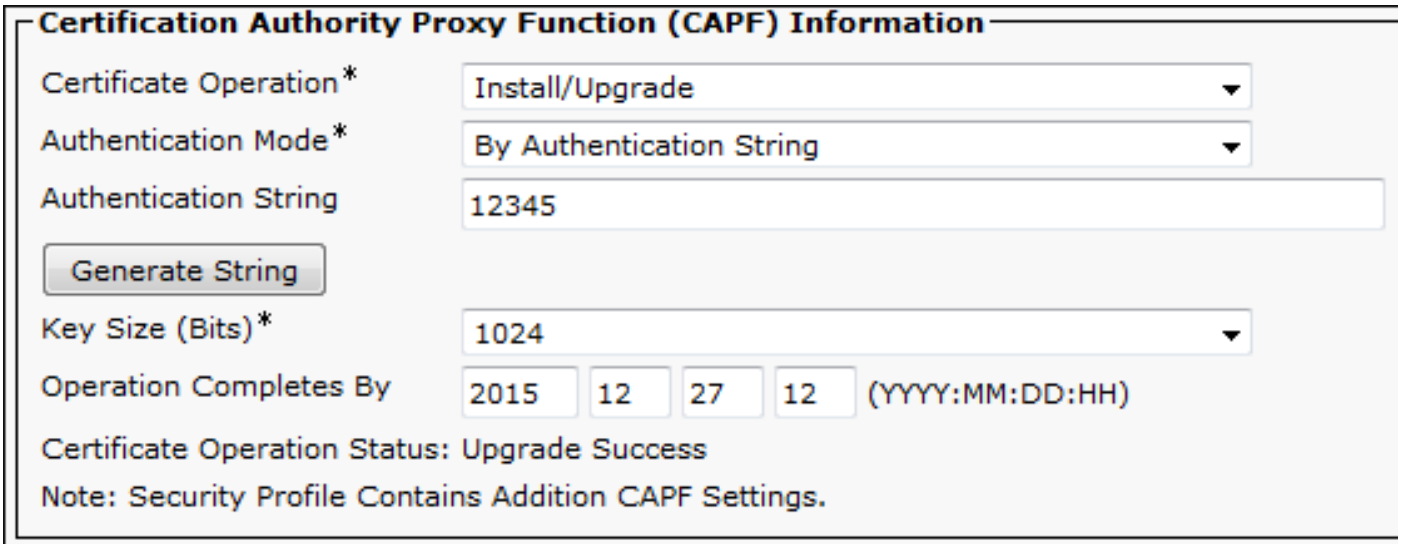


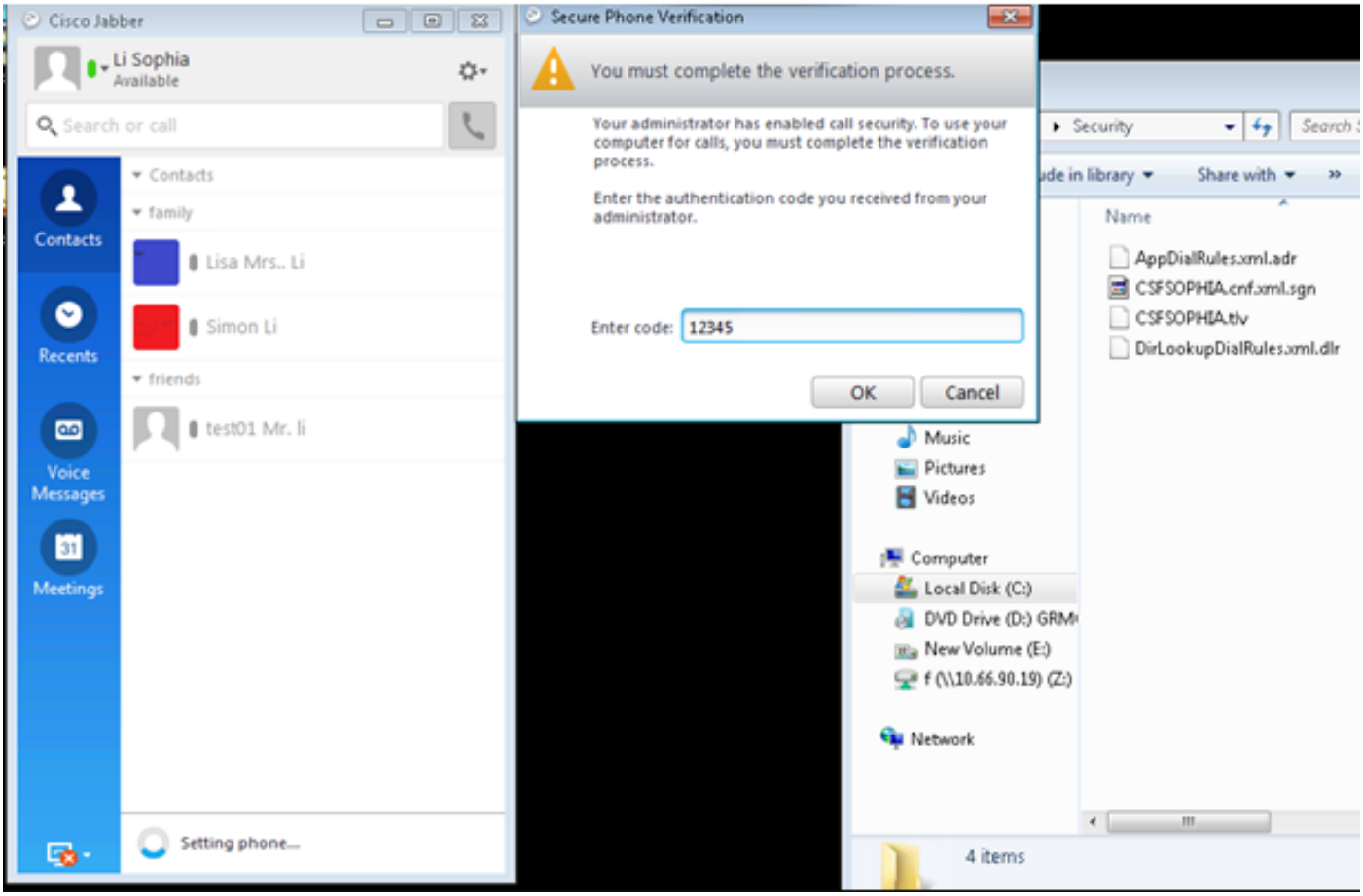
Passaggio 4. Caricare la CA radice come CAPF-trust e il certificato del server come CAPF. Per questo test, caricare anche questa CA radice come CallManager-trust per avere una connessione TLS tra Jabber e il servizio CallManager in quanto anche il servizio CallManager deve considerare attendibile il servizio LSC firmato. Come accennato all'inizio di questo articolo, è necessario allineare l'autorità di certificazione per tutti i server in modo che l'autorità di certificazione sia già stata caricata in CallManager per la crittografia del segnale o dei supporti. Per lo scenario di distribuzione del telefono IP 802.1x, non è necessario rendere CUCM in modalità mista o caricare la CA che firma il CAPF come CallManager-trust nel server CUCM.

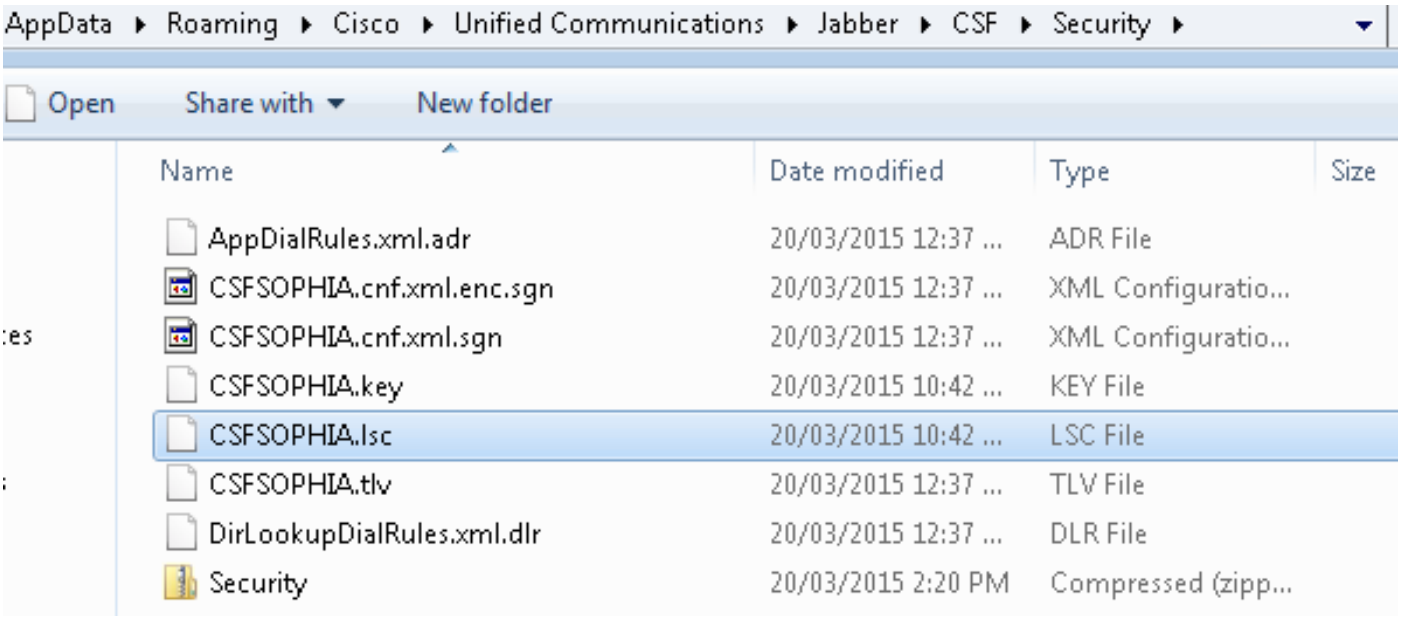
Passaggio 5. Riavviare il servizio CAPF.

Passaggio 6. Riavviare i servizi CallManager/TFTP in tutte le note.

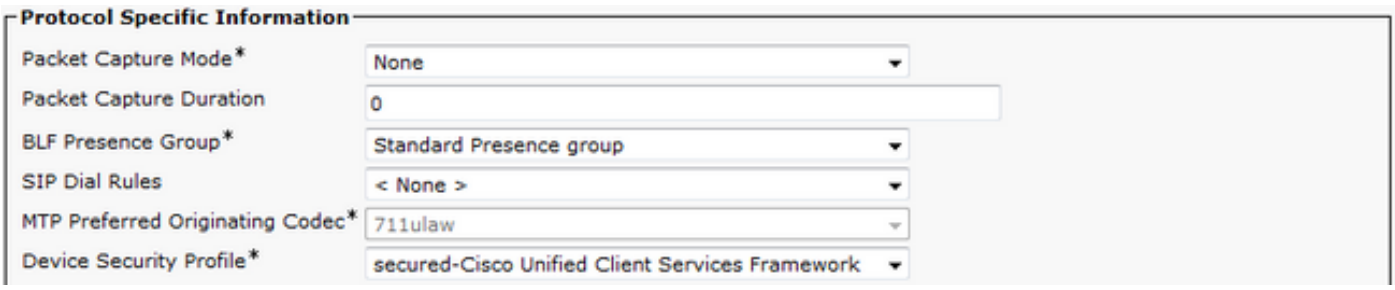
Passaggio 7. Firmato il softphone LSC Jabber.



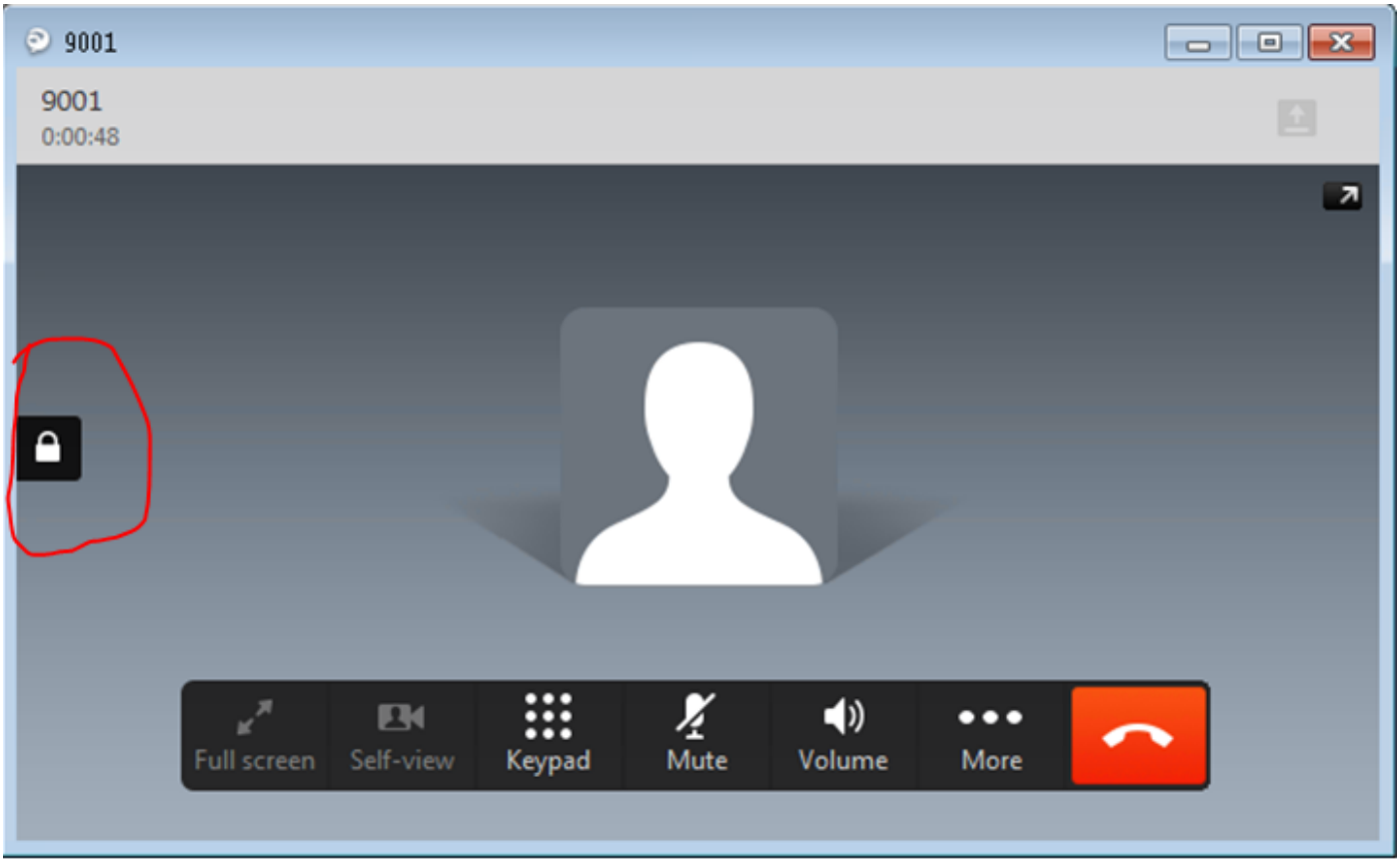




Passaggio 8. Abilitare il profilo di sicurezza per il softphone Jabber.



Passaggio 9. Ora il RTP protetto si verifica come:

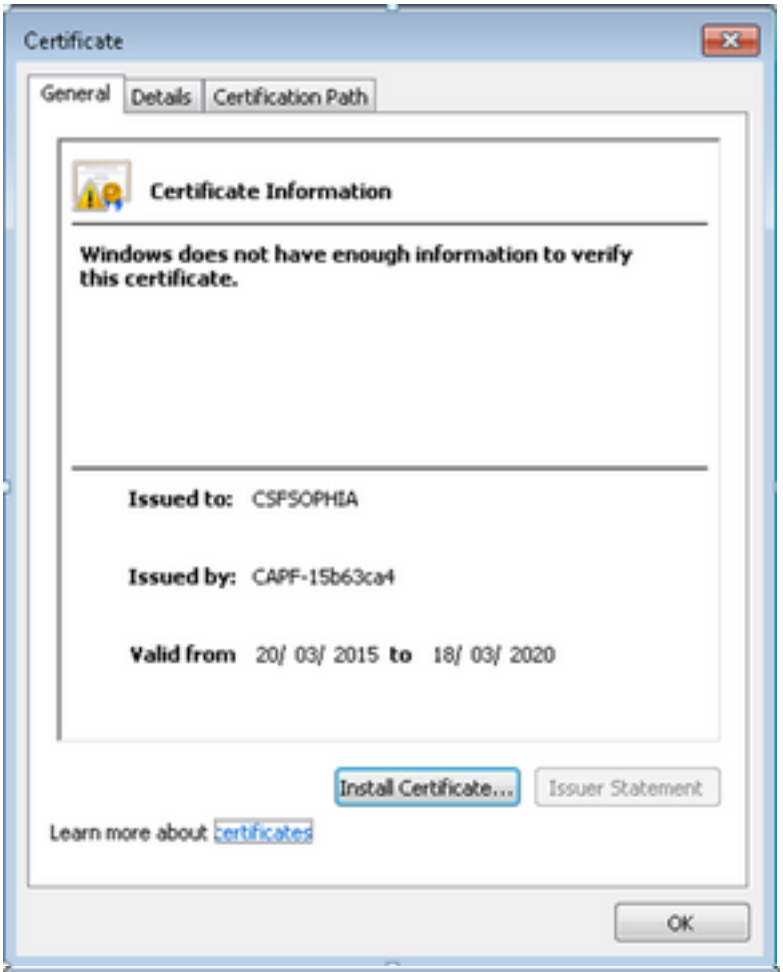


Verifica

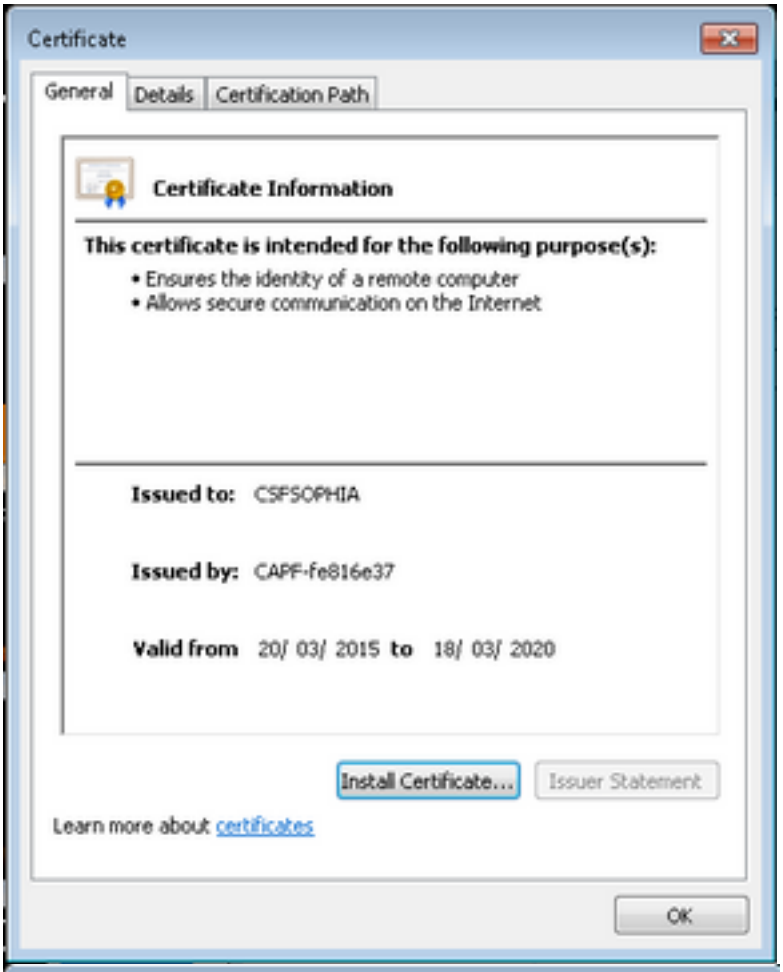
Confrontare LSC con CAPF autofirmato e CAPF con firma CA:

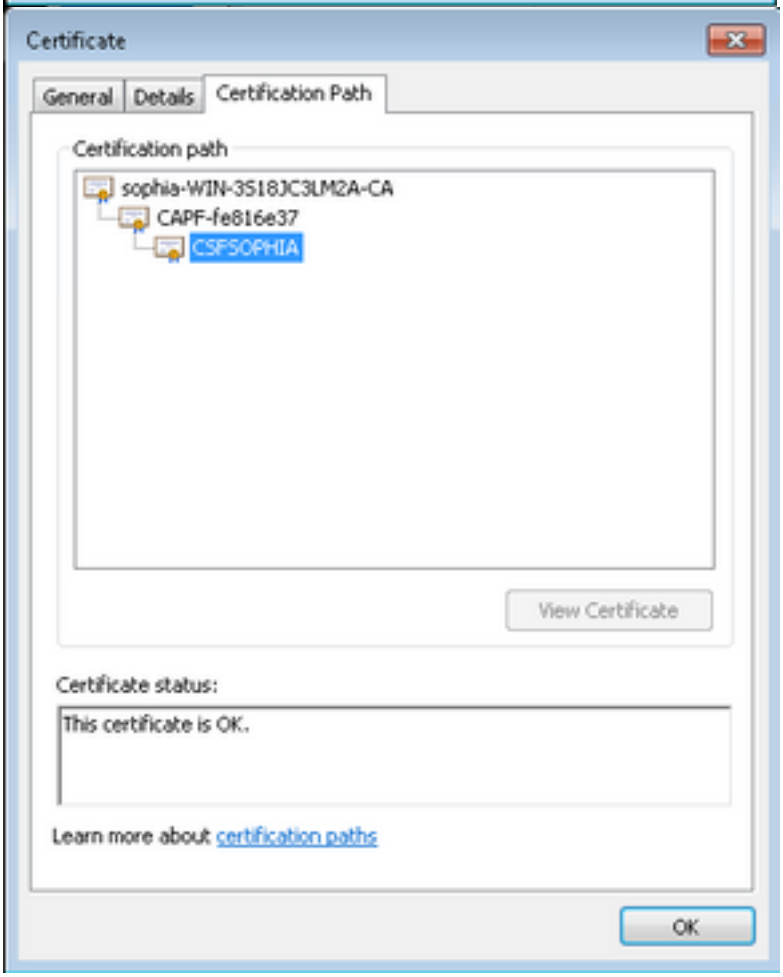
Come si può vedere da queste immagini per LSC, dal punto di vista LSC, CAPF è la CA radice quando si utilizza CAPF autofirmato, ma CAPF è la CA subordinata (intermedia) quando si utilizza CAPF con firma CA.

LSC se CAPF autofirmato



LSC quando CAPF con firma CA


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

Avviso:

l'LSC del client Jabber che mostra l'intera catena di certificati in questo esempio è diverso dal telefono IP. Poiché i telefoni IP sono progettati in base alla RFC 5280 (3.2. Certification Paths and Trust), l'AKI (Authority Key Identifier) risulta mancante, il CAPF e il certificato CA radice non sono presenti nella catena di certificati. Se il certificato CAPF/CA radice non è presente nella catena di certificati, alcuni problemi potrebbero causare l'autenticazione dei telefoni IP da parte di ISE durante l'autenticazione 801.x senza caricare i certificati CAPF e radice nell'ISE. C'è un'altra opzione in CUCM 12.5 con LSC firmato da CA offline esterna direttamente in modo che il certificato CAPF non sia necessario per essere caricato in ISE per l'autenticazione IP Phone 802.1x.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

Difetto noto: Certificato CAPF firmato dalla CA, il certificato radice deve essere caricato come CM-trust:

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