Configurare SIP TLS tra CUCM-CUBE/CUBE-SBC

Sommario

Sommario

Introduzione

Questo documento aiuta a configurare SIP Transport Layer Security (TLS) tra Cisco Unified Communications Manager (CUCM) e Cisco Unified Border Element (CUBE)

Prerequisiti

Cisco raccomanda la conoscenza di questi argomenti

- protocollo SIP
- Certificati di protezione

Requisiti

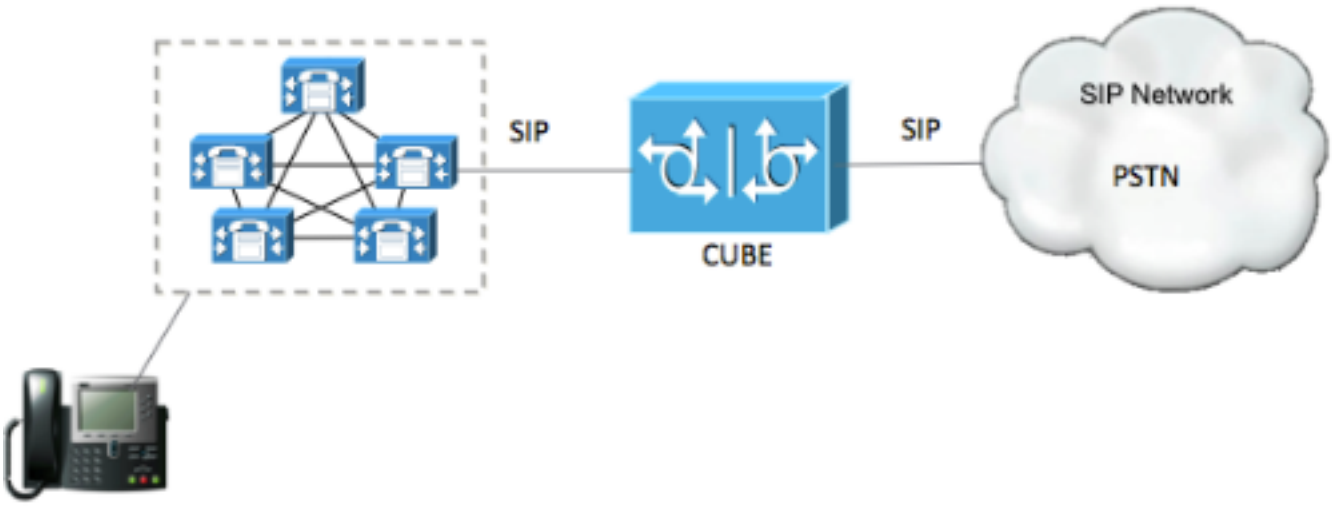
- La data e l'ora devono corrispondere sugli endpoint (si consiglia di avere la stessa origine NTP).
- CUCM deve essere in modalità mista.
- Ènecessaria la connettività TCP (aprire la porta 5061 su qualsiasi firewall di transito).
- Nel CUBE devono essere installate le licenze Security e UCK9.

Componenti usati

- SIP
- Certificati autofirmati

Configurazione

Esempio di rete



Fasi della configurazione

Passaggio 1. Creare un trust point per contenere il certificato autofirmato del CUBE

```
crypto pki trustpoint CUBEtest(this can be any name)
 enrollment selfsigned
 serial-number none
 fqdn none
 ip-address none
 subject-name cn= ISR4451-B.cisco.lab !(this has to match the router’s host name)
 revocation-check none
 rsakeypair ISR4451-B.cisco.lab !(this has to match the router's host name)
```

Passaggio 2. Dopo aver creato il trust point, eseguire il comando **Crypto pki enroll CUBEtest** per ottenere i certificati autofirmati

```
crypto pki enroll CUBEtest
% The fully-qualified domain name will not be included in the certificate
Generate Self Signed Router Certificate? [yes/no]: yes
```

Se la registrazione è corretta, è necessario attendersi l'output

```
Router Self Signed Certificate successfully created
```

Passaggio 3. Dopo aver ottenuto il certificato, è necessario esportarlo

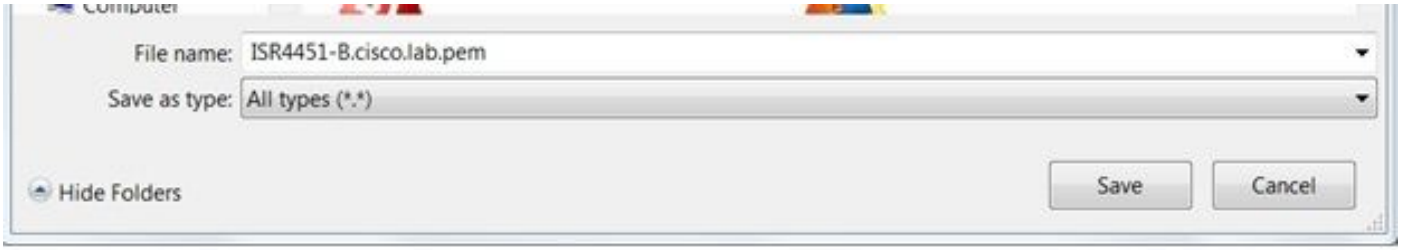
```
crypto pki export CUBEtest pem terminal
```

Il comando precedente deve generare il certificato seguente

```
% Self-signed CA certificate:

-----BEGIN CERTIFICATE-----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0

NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow

HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA

A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix

7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB

Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM

tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

-----END CERTIFICATE-----


% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0

NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow

HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA

A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix

7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB

Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM

tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

-----END CERTIFICATE-----
```

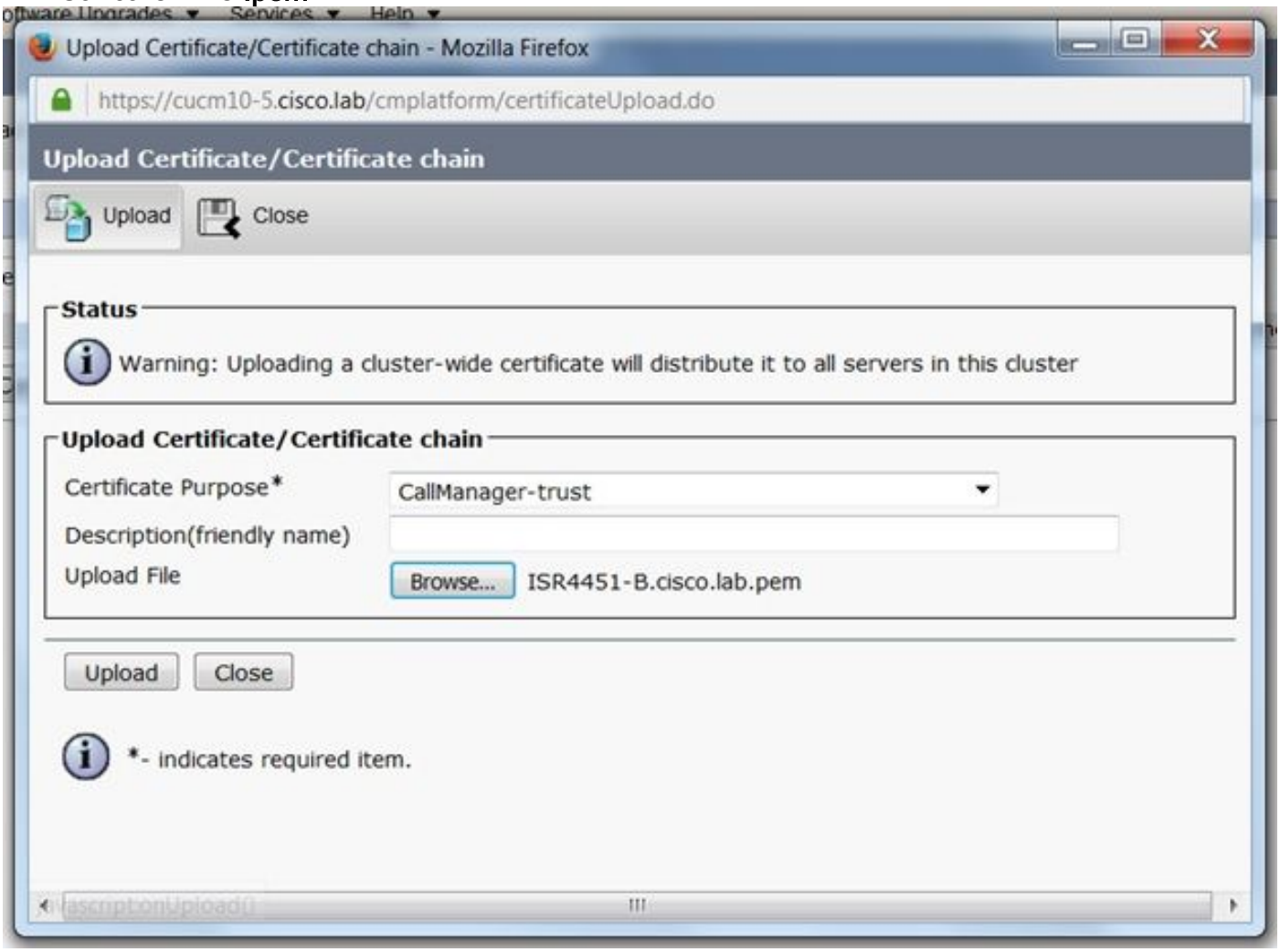
Copiare il certificato autofirmato generato sopra e incollarlo in un file di testo con estensione **.pem**

L'esempio seguente è denominato ISR4451-B.ciscolab.pem



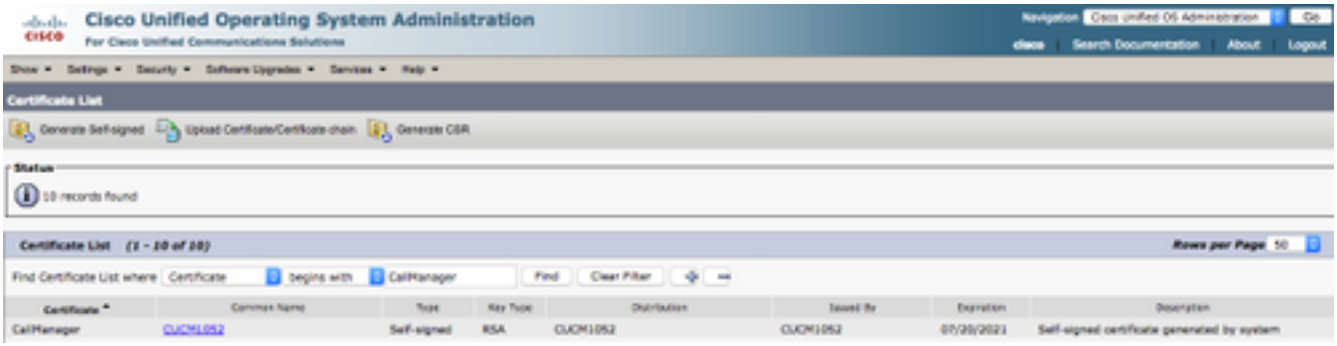
Passaggio 4. Caricare il certificato CUBE in CUCM

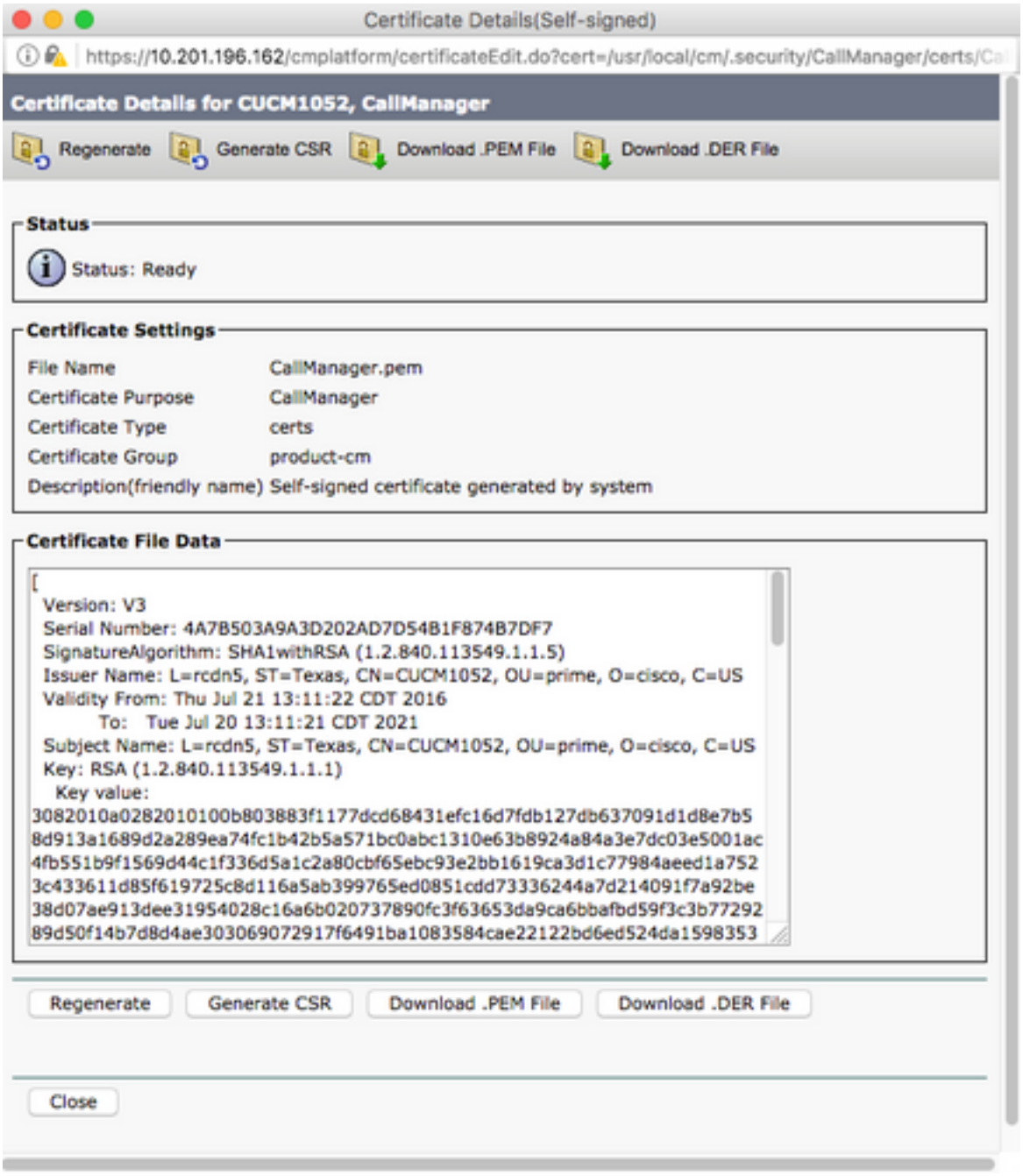
- Amministratore sistema operativo CUCM > Sicurezza > Gestione certificati > Carica catena certificati/certificati
- Scopo certificato = CallManager-Trust
- Caricare il file **.pem**



Passaggio 5. Scaricare il certificato autofirmato del gestore delle chiamate

- Trova il certificato con la dicitura Callmanager
- Fare clic sul nome dell'host
- Fare clic su Download file PEM
- Salvarlo sul computer





Passaggio 6. Caricare il certificato Callmanager.pem in CUBE

- Aprire Callmanager.pem con un editor di file di testo
- Copiare l'intero contenuto del file
- Eseguire i comandi this sul CUBO

```
crypto pki trustpoint CUCMHOSTNAME
```

```
 enrollment terminal

 revocation-check none


crypto pku authenticate CUCMHOSTNAME


(PASTE THE CUCM CERT HERE AND THEN PRESS ENTER TWICE)


    You will then see the following:


Certificate has the following attributes:

       Fingerprint MD5: B9CABE35 24B11EE3 C58C9A9F 02DB16BC

      Fingerprint SHA1: EC164F6C 96CDC1C9 E7CA0933 8C7518D4 443E0E84


% Do you accept this certificate? [yes/no]: yes


    If everything was correct, you should see the following:


Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Passaggio 7. Configurare il SIP per l'utilizzo del punto di attendibilità dei certificati firmato dal CUBE

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

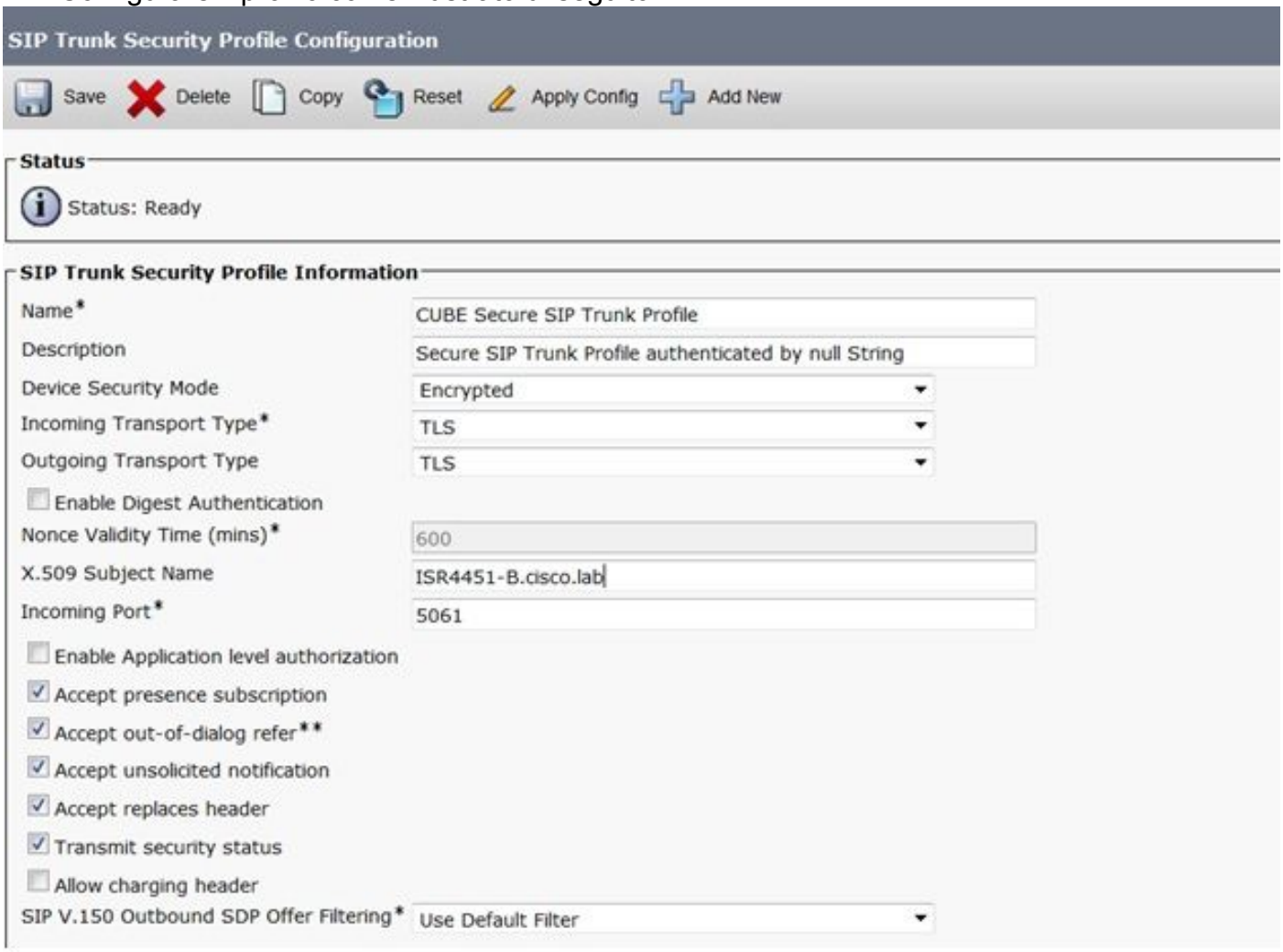
Passaggio 8. Configurare i peer di composizione con TLS

```
dial-peer voice 9999 voip

 answer-address 35..

 destination-pattern 9999

 session protocol sipv2

 session target dns:cucm10-5
```

```
session transport tcp tls

voice-class sip options-keepalive

srtp
```

Passaggio 9. Configurare un profilo di sicurezza trunk SIP CUCM

- Pagina Amministratore CUCM > Sistema > Sicurezza > Profilo sicurezza trunk SIP
- Configurare il profilo come illustrato di seguito



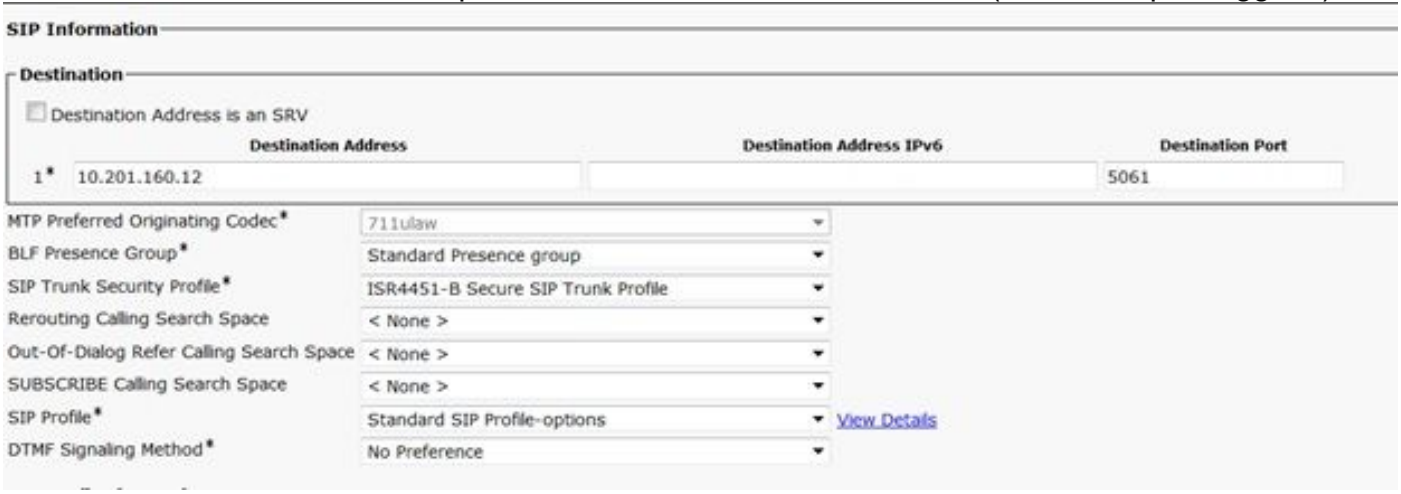
Nota: È di fondamentale importanza che il campo X.509 corrisponda al nome CN configurato in precedenza durante la generazione del certificato autofirmato

Passaggio 10. Configurazione di un trunk SIP su CUCM

- Assicurarsi che la casella di controllo SRTP consentito sia selezionata
- Configurare l'indirizzo di destinazione corretto e assicurarsi di sostituire la porta 5060 con la

porta 5061

- Assicurarsi di selezionare il profilo di sicurezza trunk SIP corretto (creato nel passaggio 9)



- Salvare e ripristinare il trunk.

Verifica

Poiché è stato abilitato il comando OPTIONS PING sul CUCM, il trunk SIP deve essere in stato FULL SERVICE

Lo stato del trunk SIP mostra il servizio completo.

Lo stato del dial peer viene visualizzato come segue:

```
show dial-peer voice summary

TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE

9999   voip  up   up             9999               0  syst dns:cucm10-5                  active
```

Risoluzione dei problemi

Abilita e raccoglie l'output di questi debug

```
debug crypto pki api
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki transactions
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
debug ip tcp transactions
debug ccsip verbose
```

Collegamento registrazione Webex:

https://goo.gl/QOS1iT