SIP-TLS configureren tussen CUCM-CUBE/CUBE-SBC

Inhoud

Inhoud

Inleiding

Dit document helpt u bij het configureren van SIP Transport Layer Security (TLS) tussen Cisco Unified Communications Manager (CUCM) en Cisco Unified Border Element (CUBE)

Voorwaarden

Cisco raadt aan om kennis te hebben over deze onderwerpen

- SIP-protocol
- Security certificaten

Vereisten

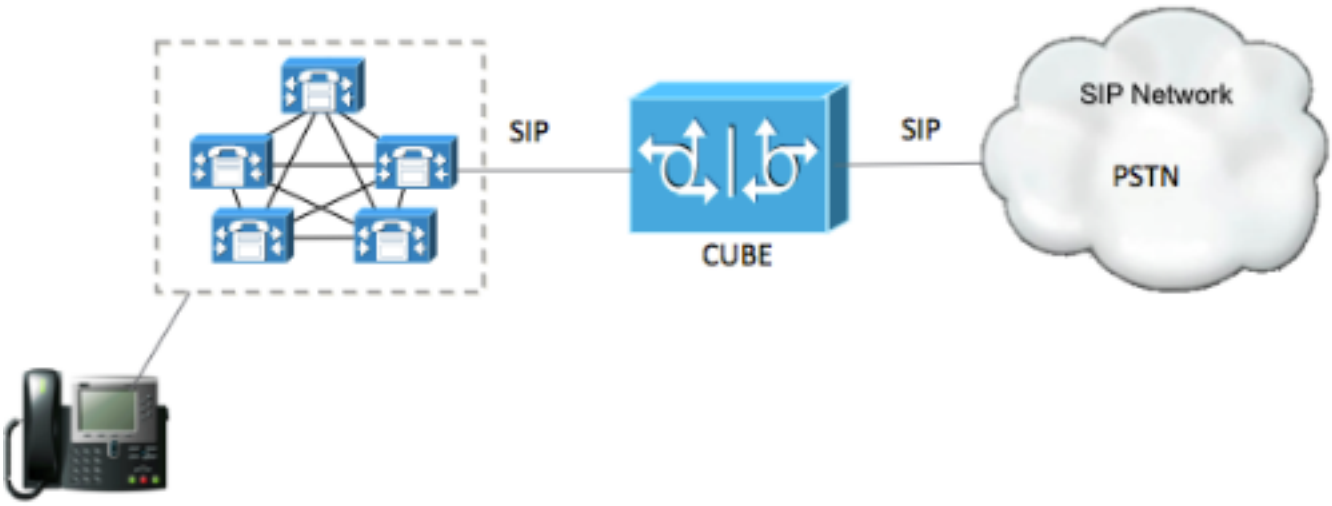
- Datum en tijd moeten op de eindpunten overeenkomen (aanbevolen wordt om dezelfde NTP-bron te hebben).
- CUCM moet in gemengde modus worden geplaatst.
- TCP-connectiviteit is vereist (Open poort 5061 op elke transitfirewall).
- De CUBE moet de beveiliging en de UCK9 licenties hebben geïnstalleerd.

Gebruikte componenten

- SIP
- Gewaarborgde certificaten

Configureren

Netwerkdiagram



Configuratiestappen

Stap 1. Maak een betrouwbaar punt om CUBE's zelfgetekende certificaat vast te houden

```
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)
```

Stap 2. Zodra het trust point is gecreëerd, voert u de opdracht **Crypto-sleutel in om CUBE-test** in te voeren om zelf getekende kerterticaten te krijgen

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

Als inschrijving juist was, moet u deze uitvoer verwachten

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

Stap 3. Nadat u een certificaat hebt verkregen, moet u dit exporteren

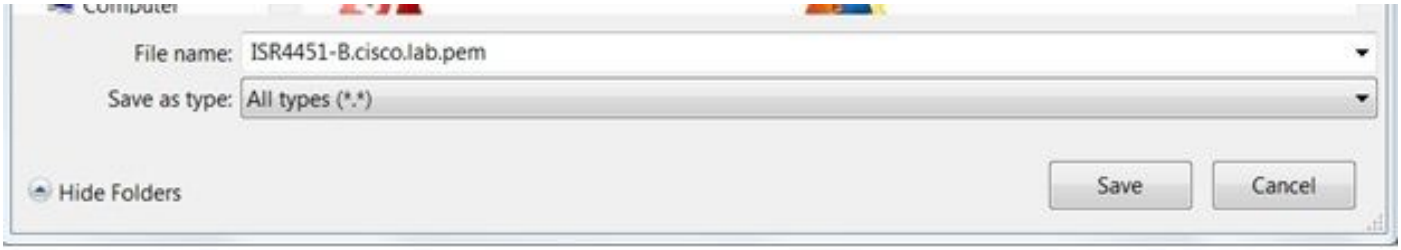
```
crypto pki export CUBEtest pem terminal
```

De bovenstaande opdracht moet het onderstaande certificaat genereren

```
% 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-----
```

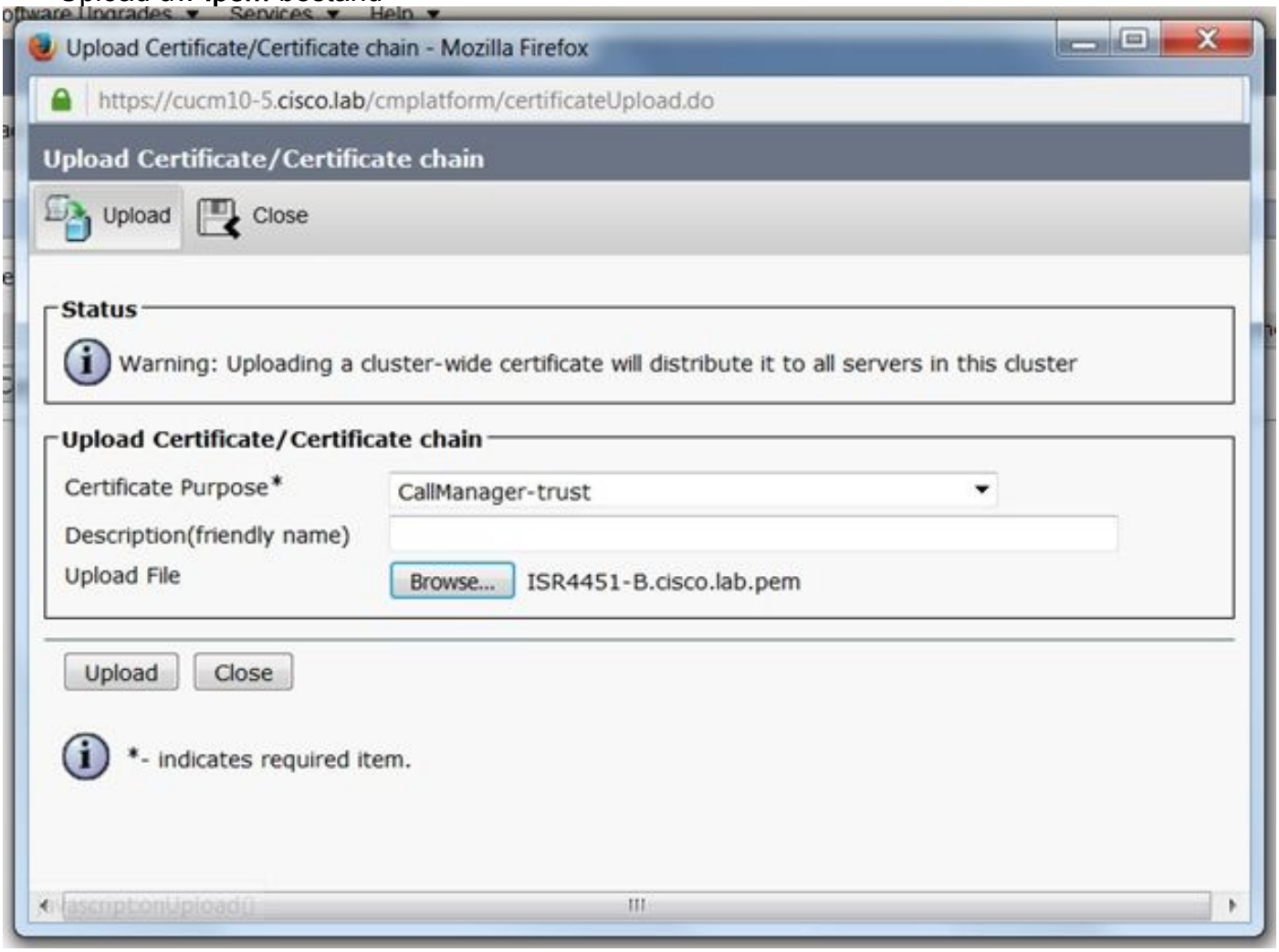
Kopieert het bovenstaande zelfgetekende certificaat en plak het op een tekstbestand met bestandsextensie **.pem**

Voorbeeld hieronder wordt genoemd als ISR4451-B.ciscolab.pem



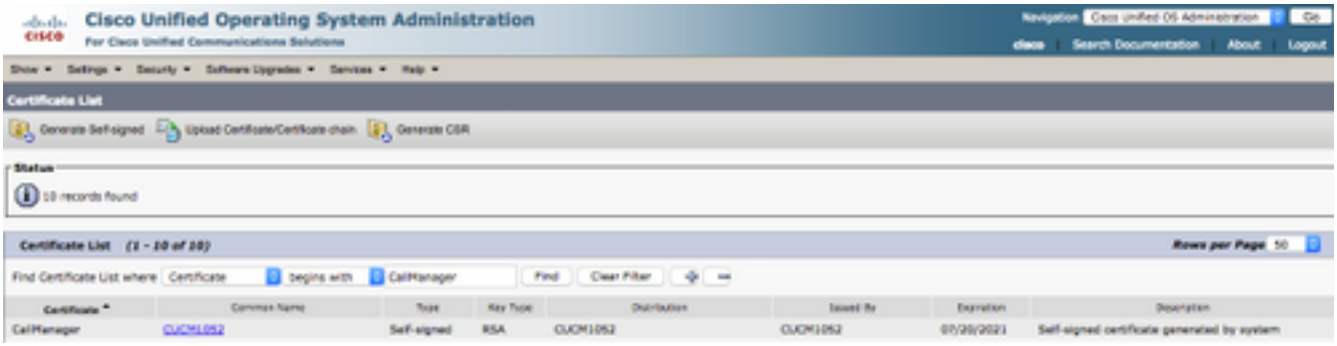
Stap 4. Upload het CUBE-certificaat naar het CUCM

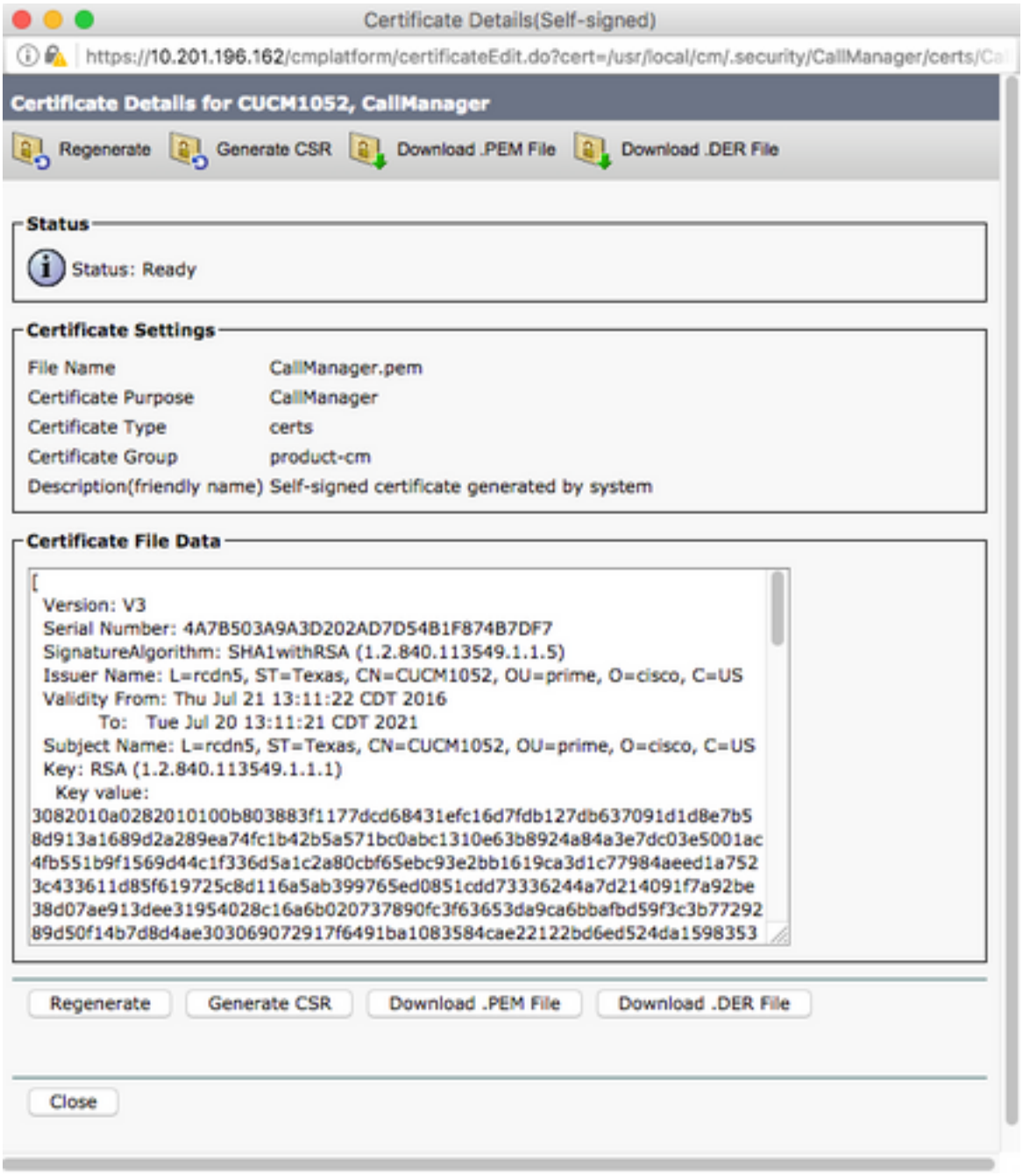
- CUCM OS Admin > Security > certificaatbeheer > Upload certificaatketting
- certificaatdoel = CallManager-vertrouwen
- Upload uw **.pem-**bestand



Stap 5. Download het door de Call Manager zelf ondertekende certificaat

- Vind het certificaat dat CallManager zegt
- Klik op de hostnaam
- Klik op PEM-bestand downloaden
- Sla het op uw computer op





Stap 6. Upload het CallManager.pem-certificaat naar CUBE

- Open CallManager.pem met een tekstbestandseditor
- De gehele inhoud van het bestand kopiëren
- Start deze opdrachten op CUBE

```
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
```

Stap 7. Configureer SIP met behulp van de zelfgetekende certificaattrustpoint van CUBE

```
sip-ua
 crypto signaling default trustpoint CUBEtest
```

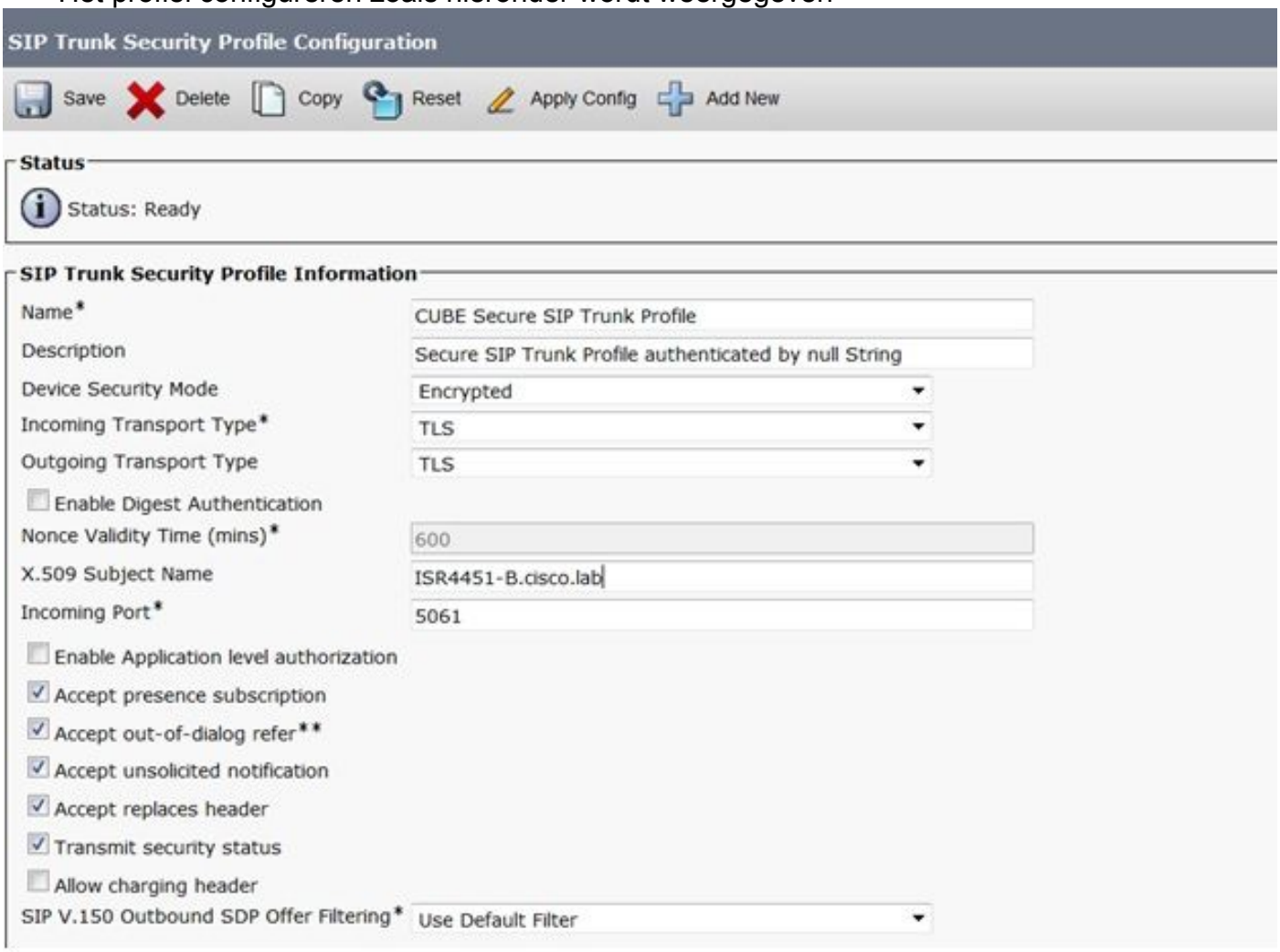
Stap 8. Configureer de dial-peers met TLS

```
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
```

Stap 9. Het beveiligingsprofiel van de CUCM SIP-stam configureren

- CUCM Admin-pagina > Systeem > Security > SIP Trunk-beveiligingsprofiel
- Het profiel configureren zoals hieronder wordt weergegeven

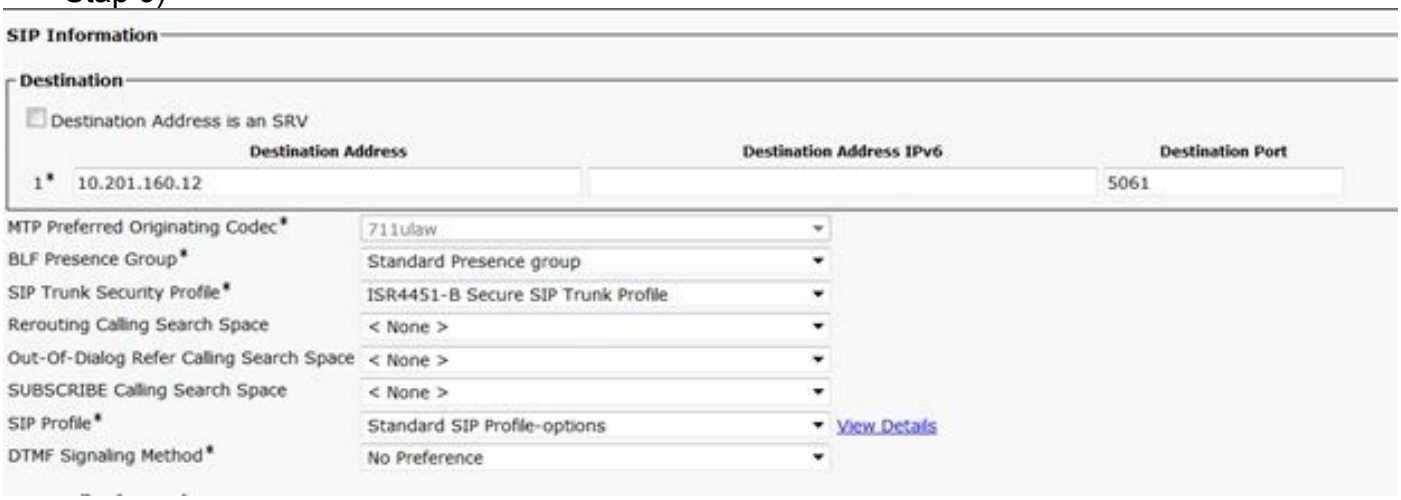


Opmerking: Het is van cruciaal belang dat het X.509-veld overeenkomt met de GN-naam die u eerder hebt ingesteld terwijl u het zelf-ondertekende certificaat hebt gegenereerd

Stap 10. Configureer een SIP-stam op CUCM

- Zorg ervoor dat het selectieknop SRTP is ingeschakeld
- Configureer het juiste doeladres en zorg ervoor dat u poort 5060 door poort 5061 vervangt
- Zorg ervoor dat u het juiste SIP Trunk-beveiligingsprofiel selecteert (dit profiel is gemaakt in

Stap 9)



- Sla de romp op en herstelt deze.

Verifiëren

Aangezien u OPTIES die op CUCM PING zijn ingeschakeld, hebt u de SIP-stam als VOLLEDIGE SERVICE-status ingeschakeld

De SIP stam status toont volledige service.

De status van dial peer verschijnt als volgt:

```
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
```

Problemen oplossen

De uitvoer van deze apparaten inschakelen en verzamelen

```
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
```

Webex-opname link:

https://goo.gl/QOS1iT