Konfigurieren von SIP-TLS zwischen CUCM-CUBE/CUBE-SBC

Inhalt

Inhaltsverzeichnis

Einführung

Dieses Dokument unterstützt die Konfiguration von SIP Transport Layer Security (TLS) zwischen Cisco Unified Communication Manager (CUCM) und Cisco Unified Border Element (CUBE).

Voraussetzungen

Cisco empfiehlt, diese Themen zu kennen.

- SIP-Protokoll
- Sicherheitszertifikate

Anforderungen

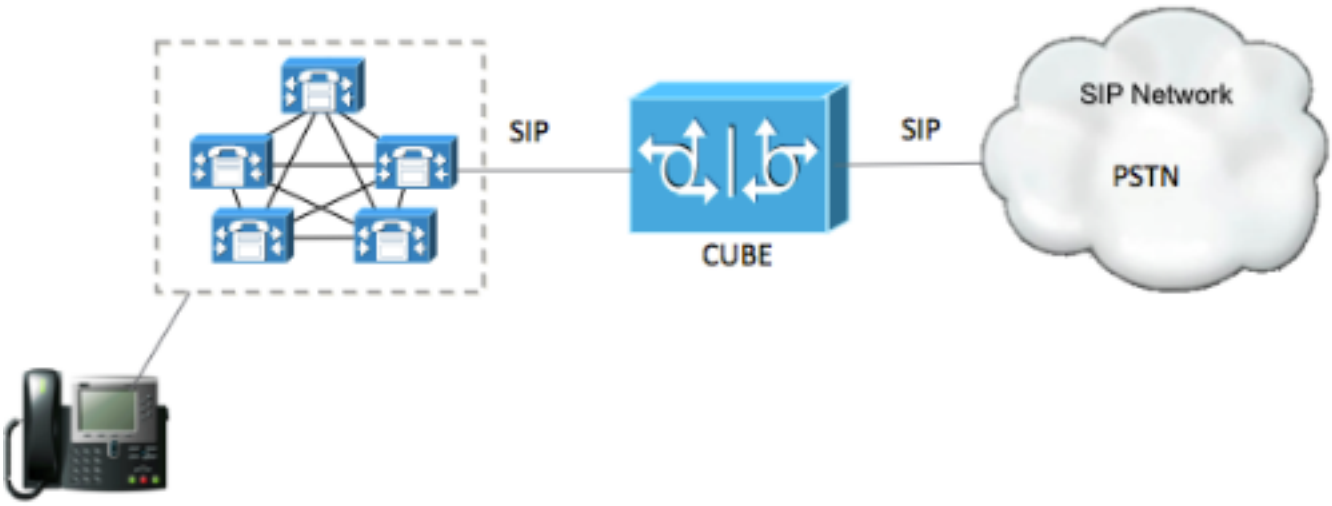
- Datum und Uhrzeit müssen auf den Endpunkten übereinstimmen (es wird empfohlen, dieselbe NTP-Quelle zu verwenden).
- Der CUCM muss sich im gemischten Modus befinden.
- TCP-Konnektivität ist erforderlich (Open port 5061 on any Transit Firewall).
- Auf dem CUBE müssen die Sicherheits- und UCK9-Lizenzen installiert sein.

Verwendete Komponenten

- SIP
- Eigenständige Zertifikate

Konfigurieren

Netzwerkdiagramm



Konfigurationsschritte

Schritt 1: Erstellen Sie einen Vertrauenspunkt, um das selbst signierte CUBE-Zertifikat zu speichern.

```
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)
```

Schritt 2: Nachdem der Vertrauenspunkt erstellt wurde, führen Sie den Befehl **Crypto pki enroll CUBEtest aus**, um selbstsignierte Zertifikate zu erhalten.

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

Wenn die Registrierung korrekt war, müssen Sie diese Ausgabe erwarten

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

Schritt 3: Nachdem Sie das Zertifikat erworben haben, müssen Sie es exportieren

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

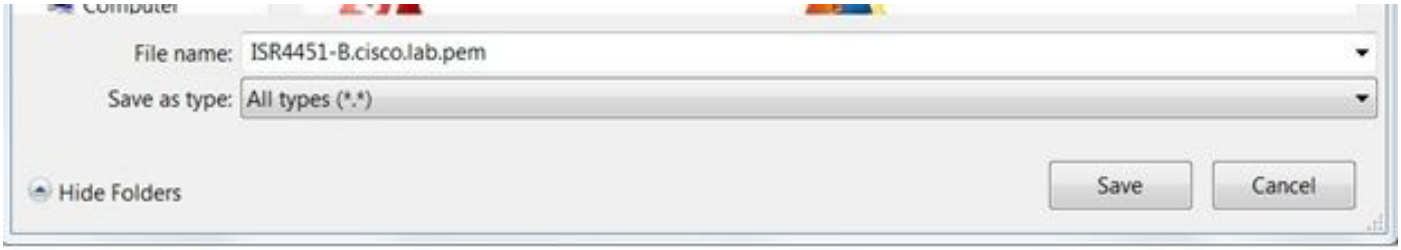
Der obige Befehl muss das unten stehende Zertifikat generieren.

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

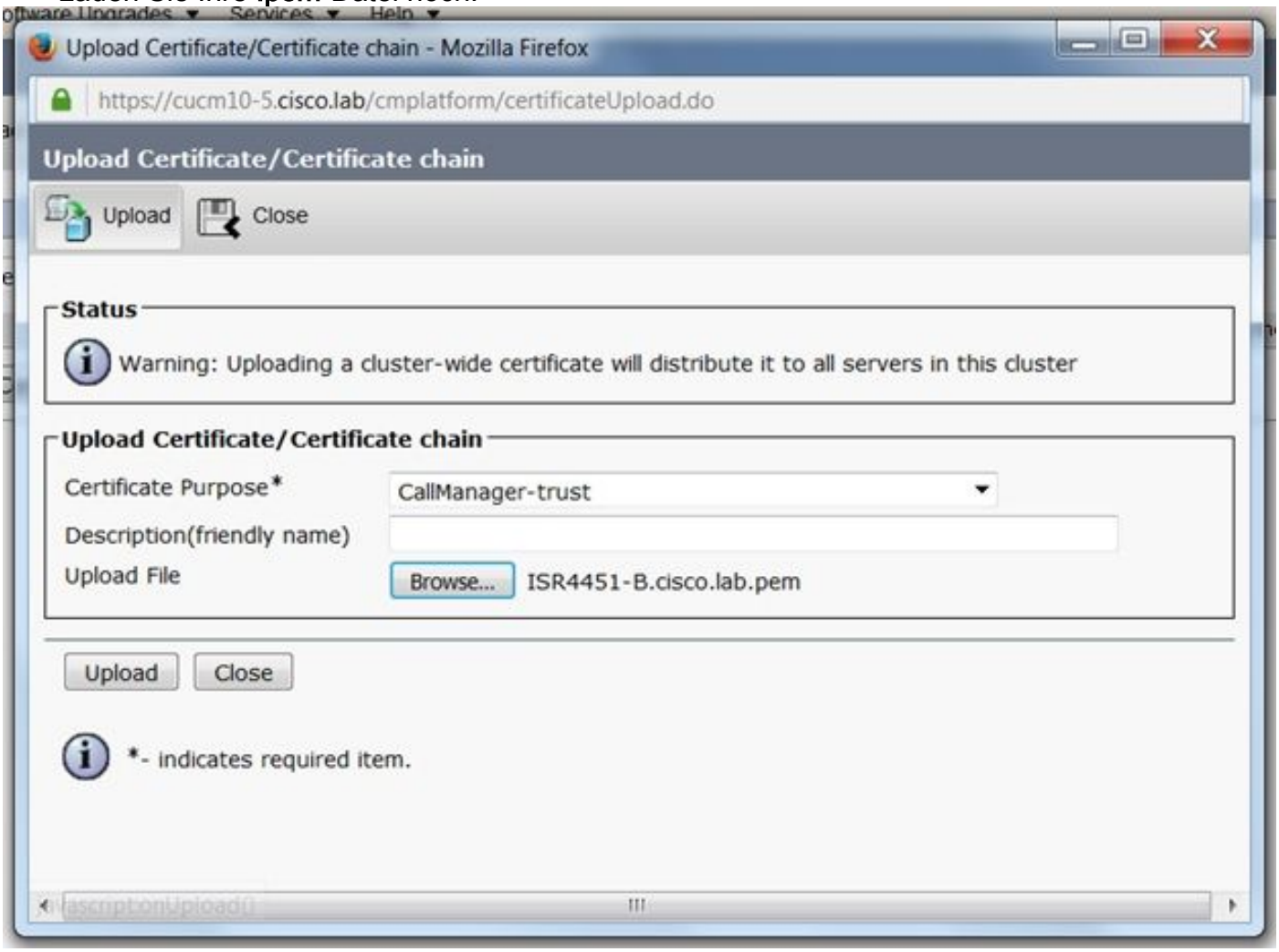
Kopieren Sie das oben erzeugte selbst signierte Zertifikat und fügen Sie es in eine Textdatei mit Dateierweiterung **.pem ein**

Das nachfolgende Beispiel wird als ISR4451-B.ciscolab.pem bezeichnet.



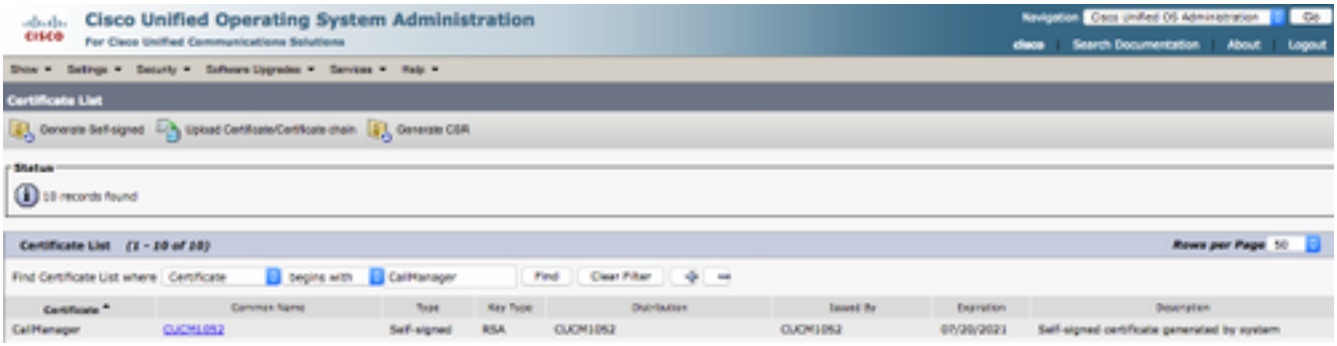
Schritt 4: Laden Sie das CUBE-Zertifikat in den CUCM hoch.

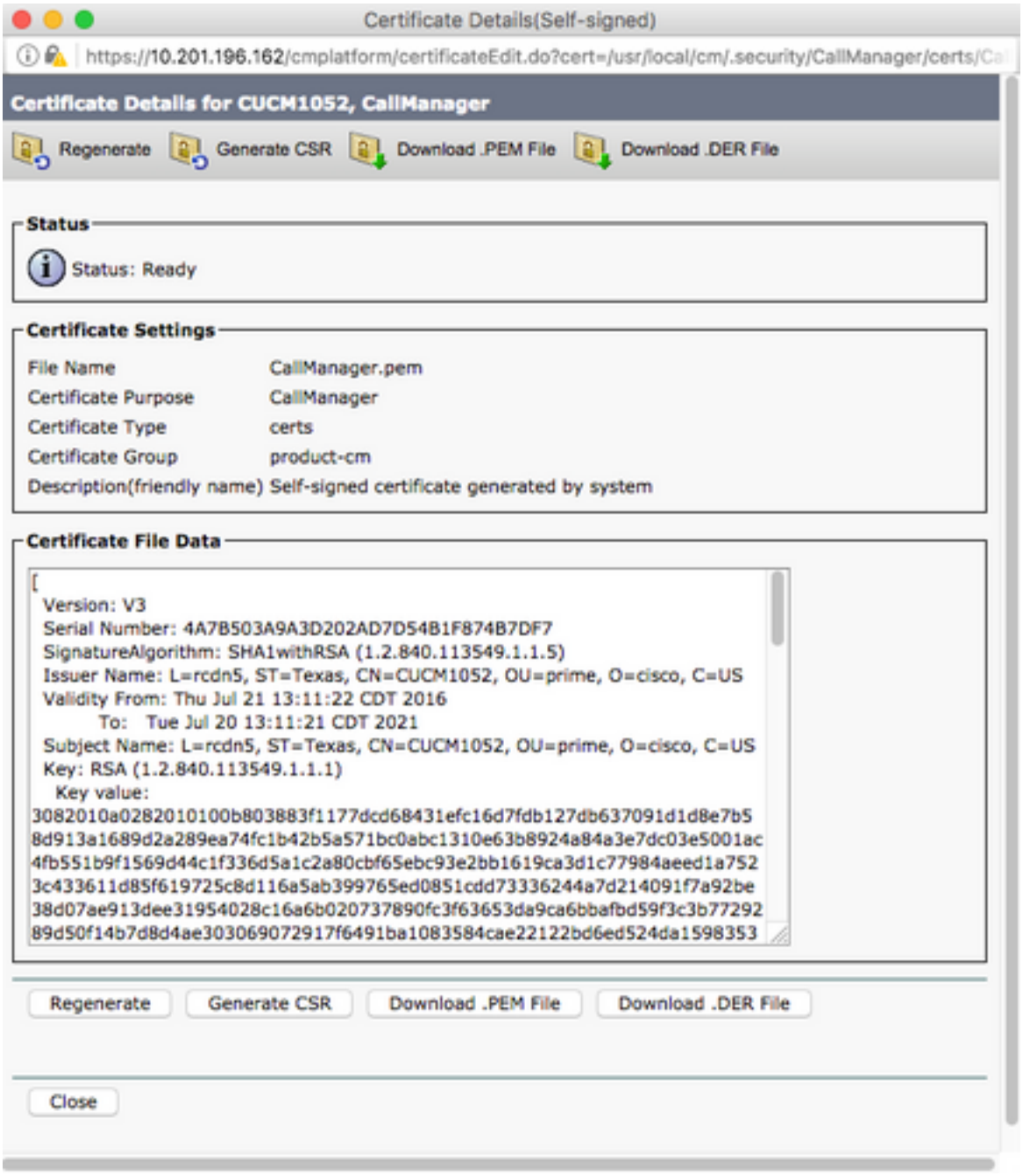
- CUCM-OS-Admin > Sicherheit > Zertifikatsverwaltung > Zertifikat/Zertifikatkette hochladen
- Zweck des Zertifikats = CallManager-Trust
- Laden Sie Ihre .pem-Datei hoch.



Schritt 5: Laden Sie das selbstsignierte Zertifikat des Call Managers herunter

- Suchen Sie das Zertifikat mit der Bezeichnung "Callmanager".
- Klicken Sie auf den Hostnamen.
- Klicken Sie auf PEM-Datei herunterladen.
- Speichern Sie die Datei auf Ihrem Computer





Schritt 6: Laden Sie das Zertifikat "Callmanager.pem" in CUBE hoch.

- Öffnen Sie Callmanager.pem mit einem Text-Datei-Editor.
- Kopieren des gesamten Inhalts der Datei
- Führen Sie diese Befehle auf CUBE aus

```
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
```

Schritt 7: Konfigurieren Sie SIP so, dass der selbst erstellte Certificate Trustpoint von CUBE verwendet wird.

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

Schritt 8: Konfigurieren der Dial-Peers mit TLS

```
dial-peer voice 9999 voip

 answer-address 35..

 destination-pattern 9999

 session protocol sipv2

 session target dns:cucm10-5
```

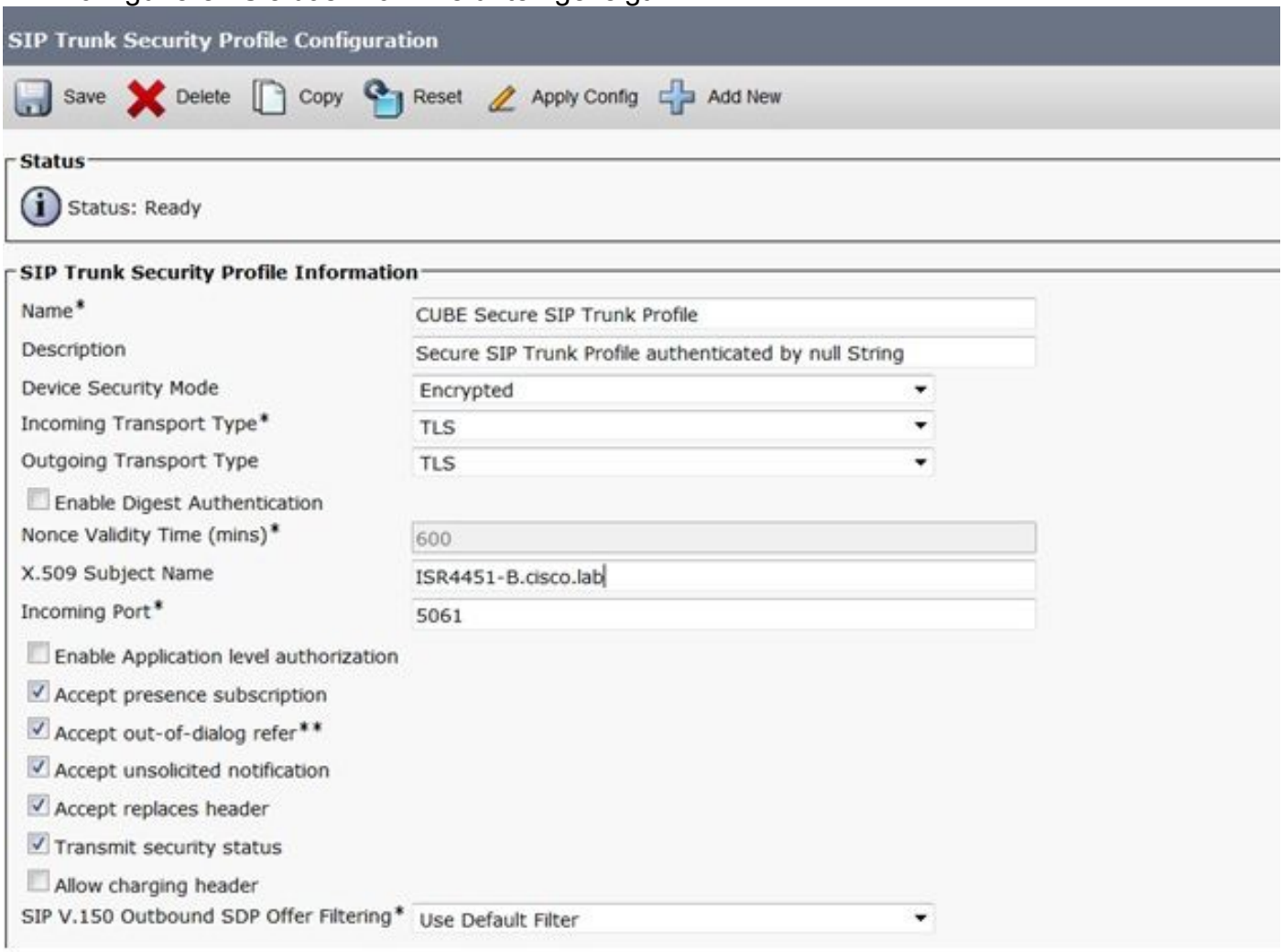
```
session transport tcp tls

voice-class sip options-keepalive

srtp
```

Schritt 9: Konfigurieren eines CUCM-SIP-Trunk-Sicherheitsprofils

- CUCM-Admin-Seite > System > Security > SIP-Trunk-Sicherheitsprofil
- Konfigurieren Sie das Profil wie unten gezeigt.

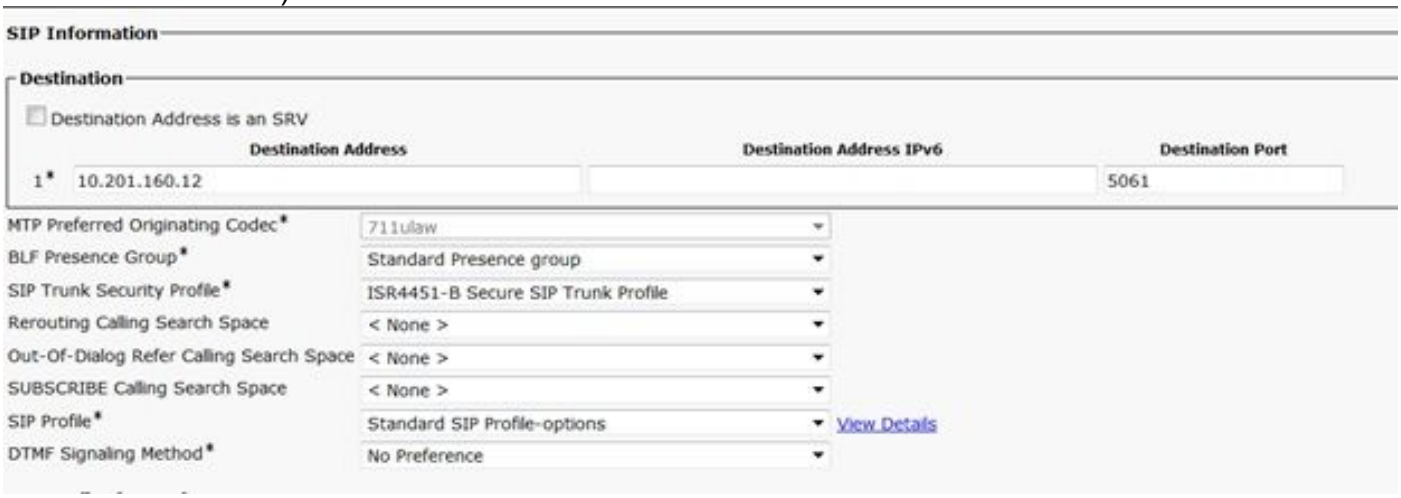


Hinweis: Es ist von entscheidender Bedeutung, dass das Feld X.509 mit dem zuvor beim Generieren des selbstsignierten Zertifikats konfigurierten CN-Namen übereinstimmt.

Schritt 10: Konfigurieren eines SIP-Trunks auf dem CUCM

- Stellen Sie sicher, dass das Kontrollkästchen SRTP allowed aktiviert ist.
- Konfigurieren Sie die richtige Zieladresse, und ersetzen Sie Port 5060 durch Port 5061.

- Stellen Sie sicher, dass Sie das richtige SIP-Trunk-Sicherheitsprofil auswählen (das in Schritt 9 erstellt wurde).



- Speichern und zurücksetzen Sie den Trunk.

Überprüfen

Da Sie OPTIONS PING auf dem CUCM aktiviert haben, muss der SIP-Trunk den Status "VOLLDIENST" haben.

Der SIP-Trunk-Status zeigt den Full-Service an.

Der DFÜ-Peer-Status wird wie folgt angezeigt:

```
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
```

Fehlerbehebung

Aktivieren und Erfassen der Ausgabe dieser Debugger

```
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 Aufzeichnung Link:

https://goo.gl/QOS1iT