CUCM-CUBE/CUBE-SBC 間の設定 SIP TLS

目次

目次

概要

この資料は Cisco Unified 通信マネージャ（CUCM）と Cisco Unified Border Element（CUBE）間の SIP Transport Layer Security （TLS）の設定を助けます

前提条件

Cisco はこれらのサブジェクトのナレッジがあることを推奨します

- SIP プロトコル
- セキュリティ 認証

要件

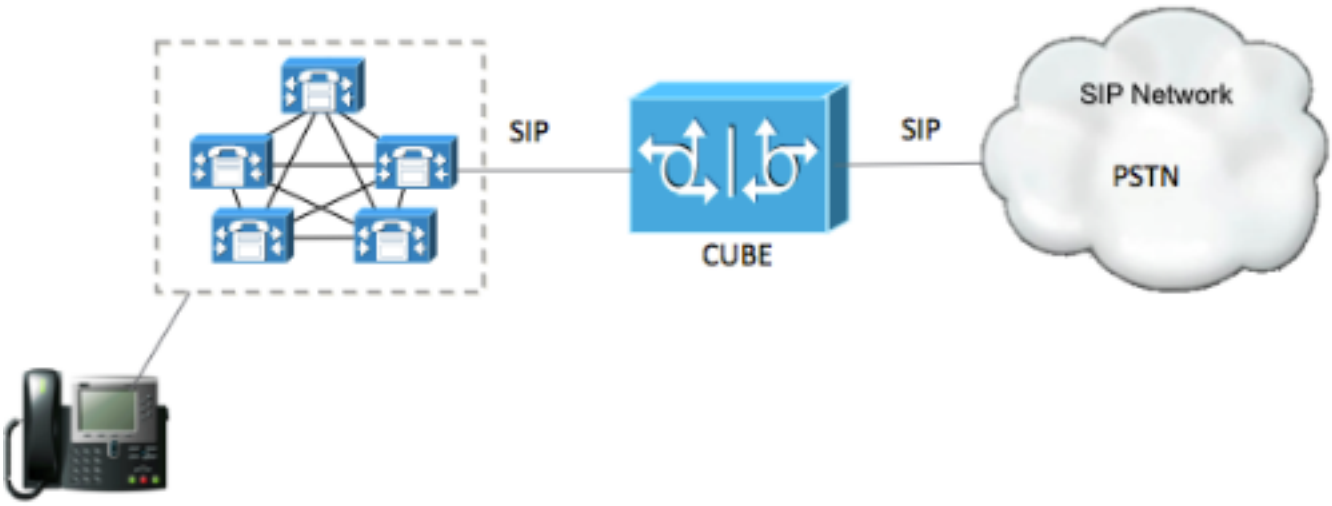
- 日時はエンドポイント（同じ NTP 出典があることを推奨します）で一致する必要があります。
- CUCM はミックス モードにある必要があります。
- TCP 接続が必要となります（あらゆる中継ファイアウォールの開港 5061）。
- CUBE はインストールされるセキュリティおよび UCK9 ライセンスがなければなりません。

使用するコンポーネント

- SIP
- Selfsigned 認証

設定

ネットワーク図



コンフィギュレーションのステップ

ステップ 1.キューブの selfsigned 認証を保持するためにトラストポイントを作成して下さい

```
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)
```

呼び出します。 信頼ポイントが作成されれば自己署名 certerticates を得るために**暗号 PKI が CUBEtest を登録する**コマンドを実行します

```
crypto pki enroll CUBEtest

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

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

登録が正しかったらこの出力を期待して下さい

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

ステップ 3 認証を得た後、それをエクスポートする必要があります

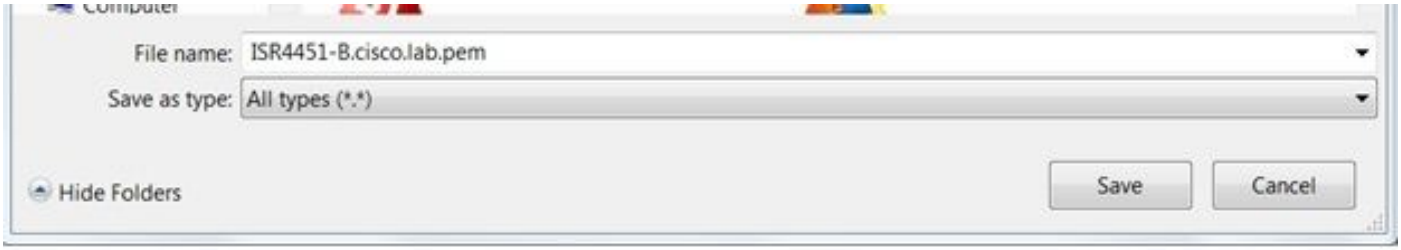
```
crypto pki export CUBEtest pem terminal
```

上のコマンドは下記の認証を生成する必要があります

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

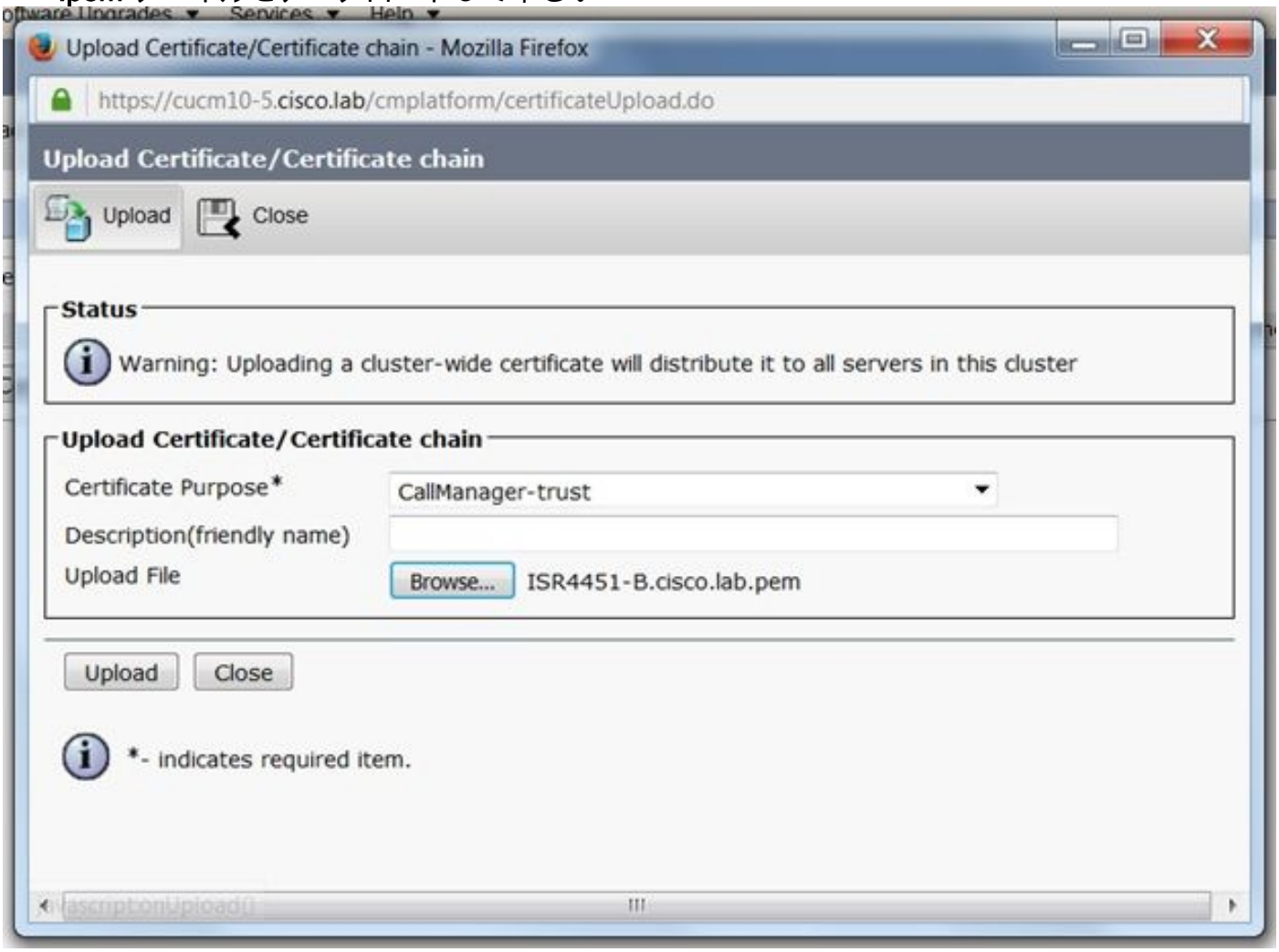
上で生成された自己 署名入り認証をコピーし、ファイル拡張子 .pem を用いるテキストファイルに貼り付けて下さい

下記の例は ISR4451-B.ciscolab.pem として指名されます



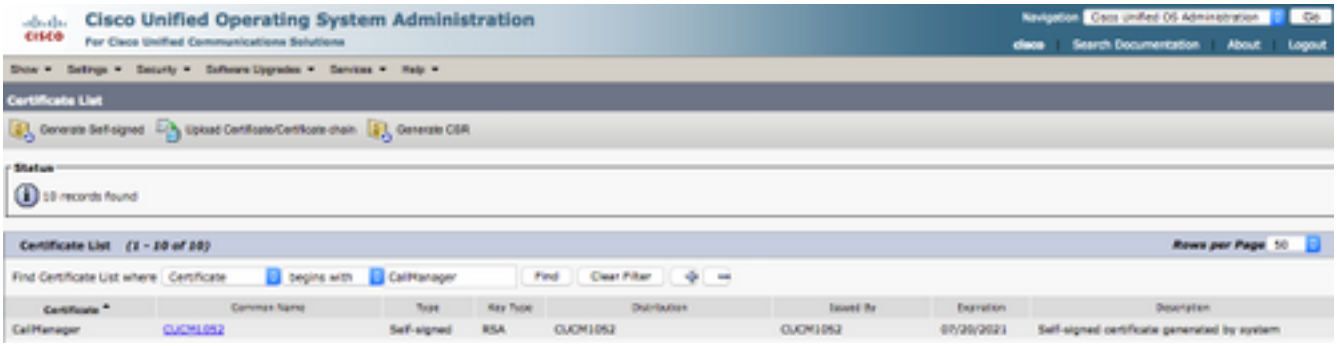
ステップ 4. CUCM に CUBE 認証をアップロードして下さい

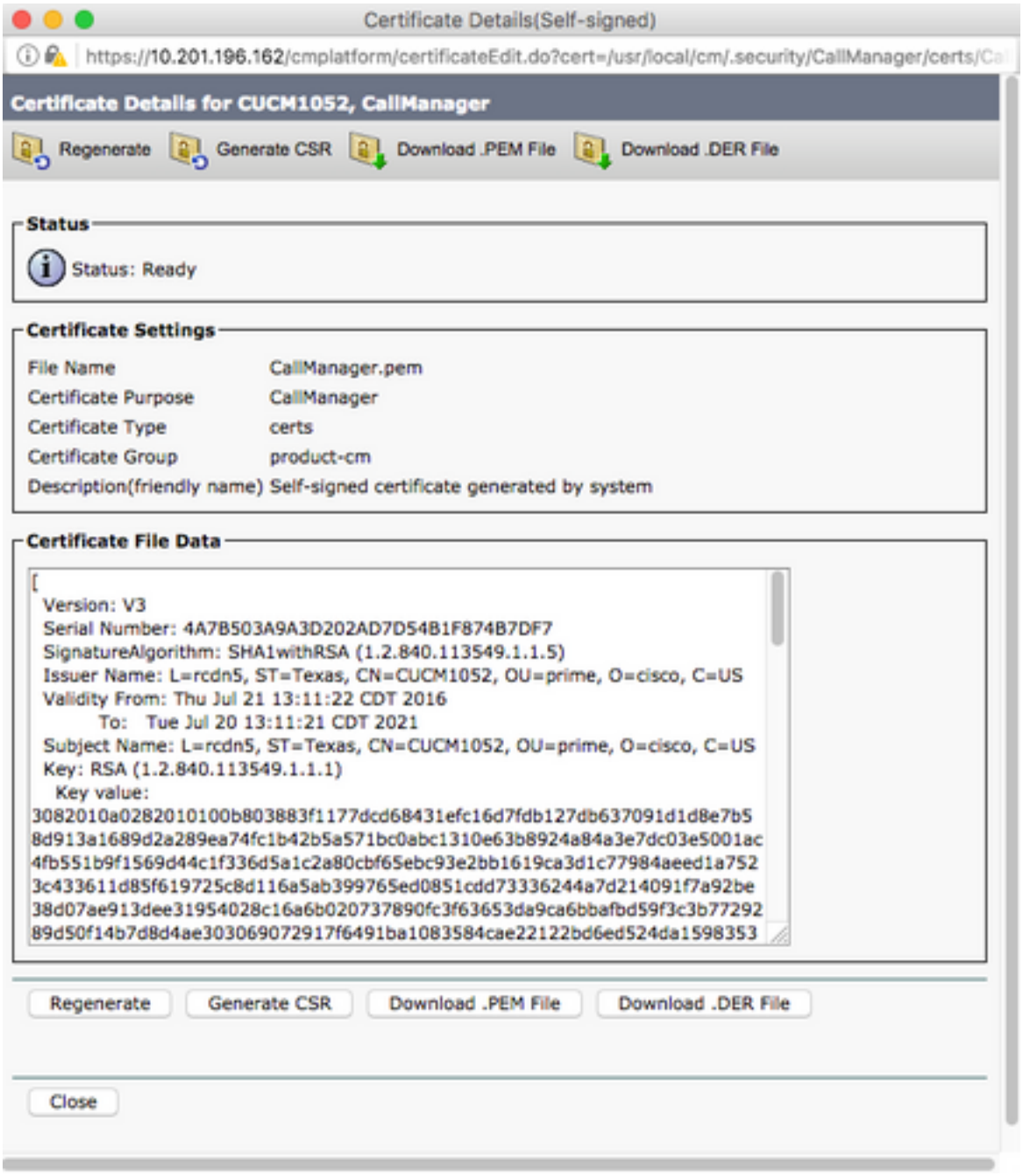
- CUCM OS Admin > Security > Certificate Management > アップロード認証/証明書 チェーン
- 認証目的 = CallManager 信頼
- .pem ファイルをアップロードして下さい



ステップ 5. Call Manager 自己署名証明書をダウンロードして下さい

- CallManager を言う認証を見つけて下さい
- ホスト名をクリックして下さい
- PEM ファイルを『Download』 をクリック して下さい
- コンピュータにそれを保存して下さい





ステップ 6.立方体になるために Callmanager.pem 認証をアップロードして下さい

- テキストファイル エディタとの Callmanager.pem を開いて下さい
- ファイルの全体コンテンツをコピーして下さい
- これ命じます CUBE で実行して下さい

```
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
```

ステップ 7.キューブの selfsigned 認証 トラストポイントを使用するために SIP を設定して下さい

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

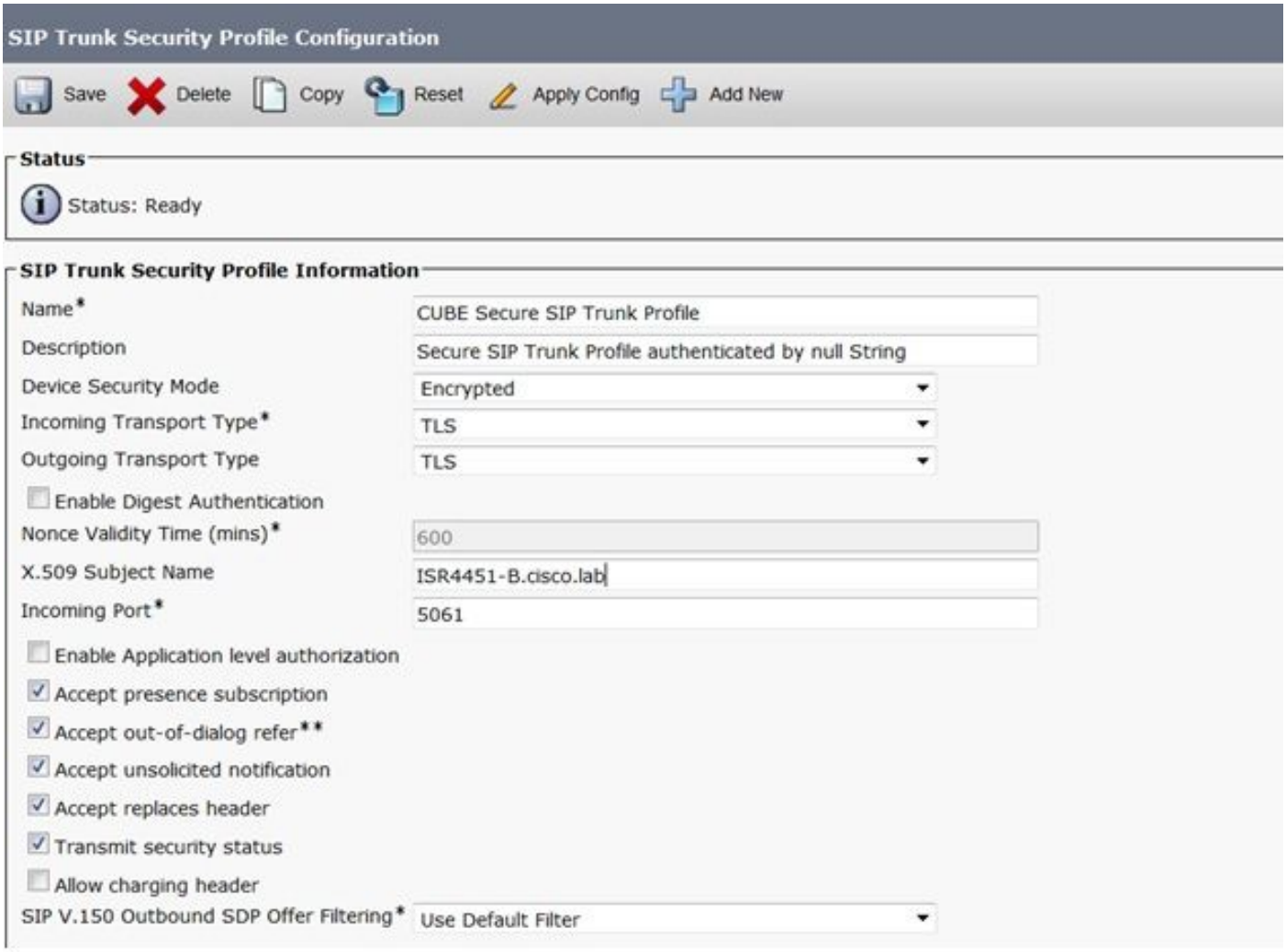
ステップ 8. TLS でダイヤル ピアを設定して下さい

```
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
```

ステップ 9. CUCM SIP トランク セキュリティプロファイルを設定して下さい

- CUCM 管理者ページ > システム > Security > SIP トランク セキュリティプロファイル
- 下記に示されているようにプロファイルを設定して下さい



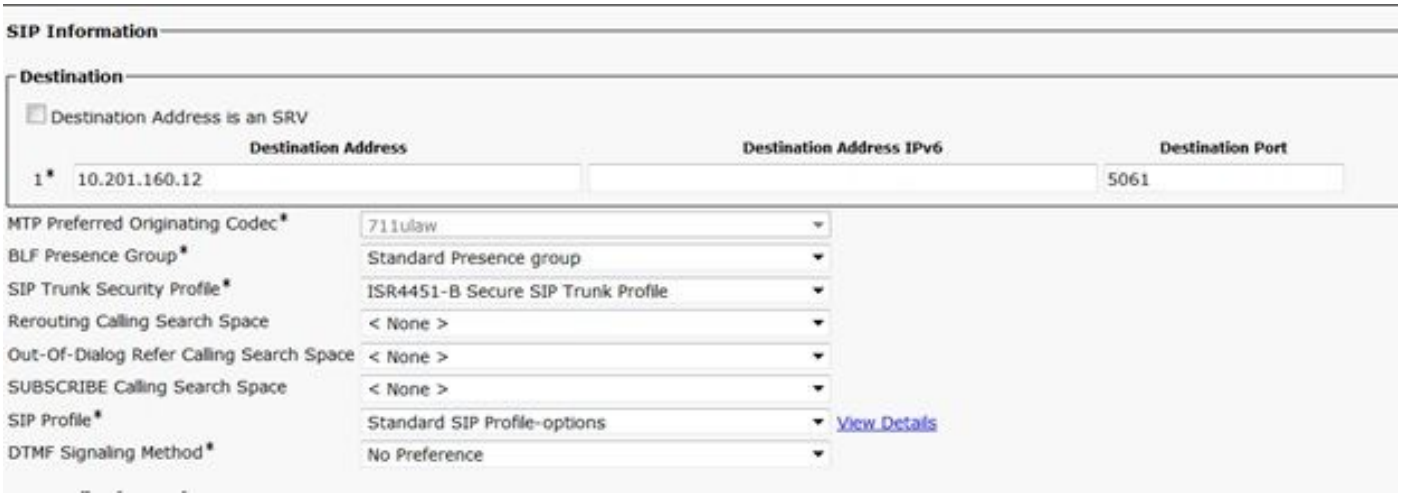
注: X.509 フィールドが自己署名証明書を生成している間前もって設定した CN 名前と一致することは極めて重要です

ステップ 10. CUCM の SIP トランクを設定して下さい

- SRTP によって許可されるチェックボックスをチェックされます確認して下さい
- 適切な宛先アドレスを設定し、ポート 5061 とポート 5060 を取り替えるために確認して下さ

い

- (ステップで選択するために 9) 作成された正しいーロトランク セキュリティプロファイル確認して下さい



- トランクを保存し、リセットして下さい。

確認

FULL サービス状態に CUCM のイネーブルになったオプション PING、SIP トランクいる必要があるので

SIP トランクステータスは完全サービスを示します。

ダイヤル ピア ステータスはように続きます示します:

```
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
```

トラブルシューティング

これらのデバッグの出力を有効に し、集めて下さい

```
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 記録リンク:

https://goo.gl/QOS1iT