CUCM-CUBE/CUBE-SBC間のSIP TLSの設定

内容

目次

概要

このドキュメントは、Cisco Unified Communication Manager(CUCM)とCisco Unified Border Element(CUBE)間のSIPトランスポート層セキュリティ(TLS)の設定に役立ちます

前提条件

これらの項目に関する知識があることが推奨されます

- SIP プロトコル
- セキュリティ証明書

要件

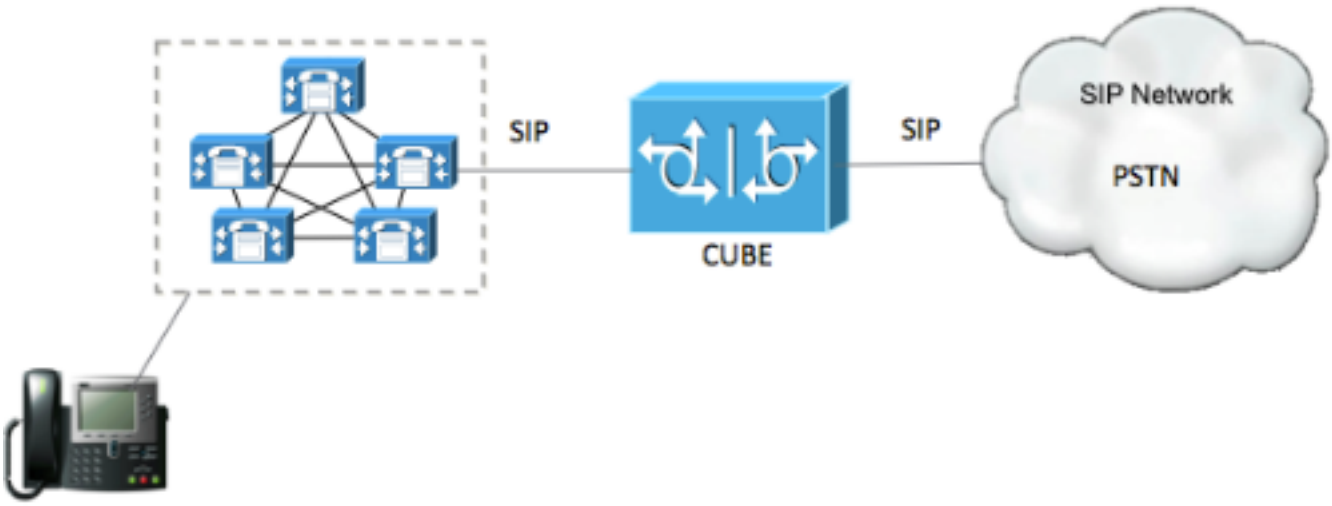
- 日付と時刻はエンドポイントで一致する必要があります（同じNTPソースを使用することをお勧めします）。
- CUCMは混合モードである必要があります。
- TCP接続が必要です（任意のトランジットファイアウォールのオープンポート5061）。
- CUBEには、セキュリティおよびUCK9ライセンスがインストールされている必要があります。

使用するコンポーネント

- SIP
- 自己署名証明書

設定

ネットワーク図



設定手順

ステップ 1： CUBEの自己署名証明書を保持するためのトラストポイントを作成します

```
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)
```

ステップ2：トラストポイントが作成されたら、Crypto pki enroll CUBEtestコマンドを実行して、自己署名証明書を取得します

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

登録が正しければ、次の出力を期待する必要があります

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

ステップ3：取得した証明書（証明書）を工クスポートする必要があります

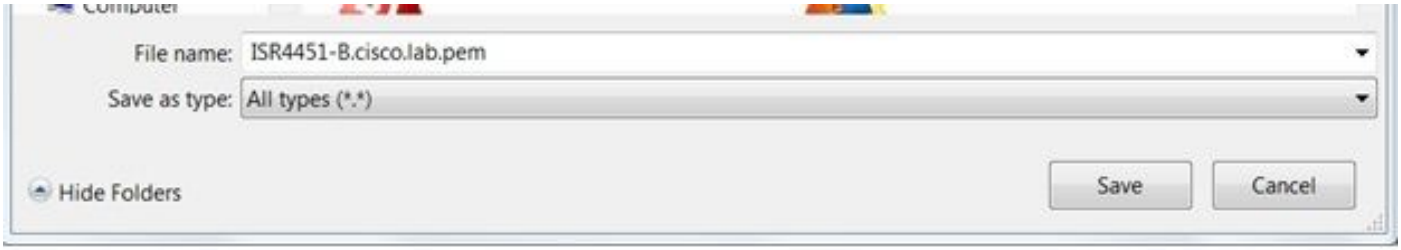
```
crypto pki export CUBEtest pem terminal
```

上記のコマンドは、次の証明書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-----
```

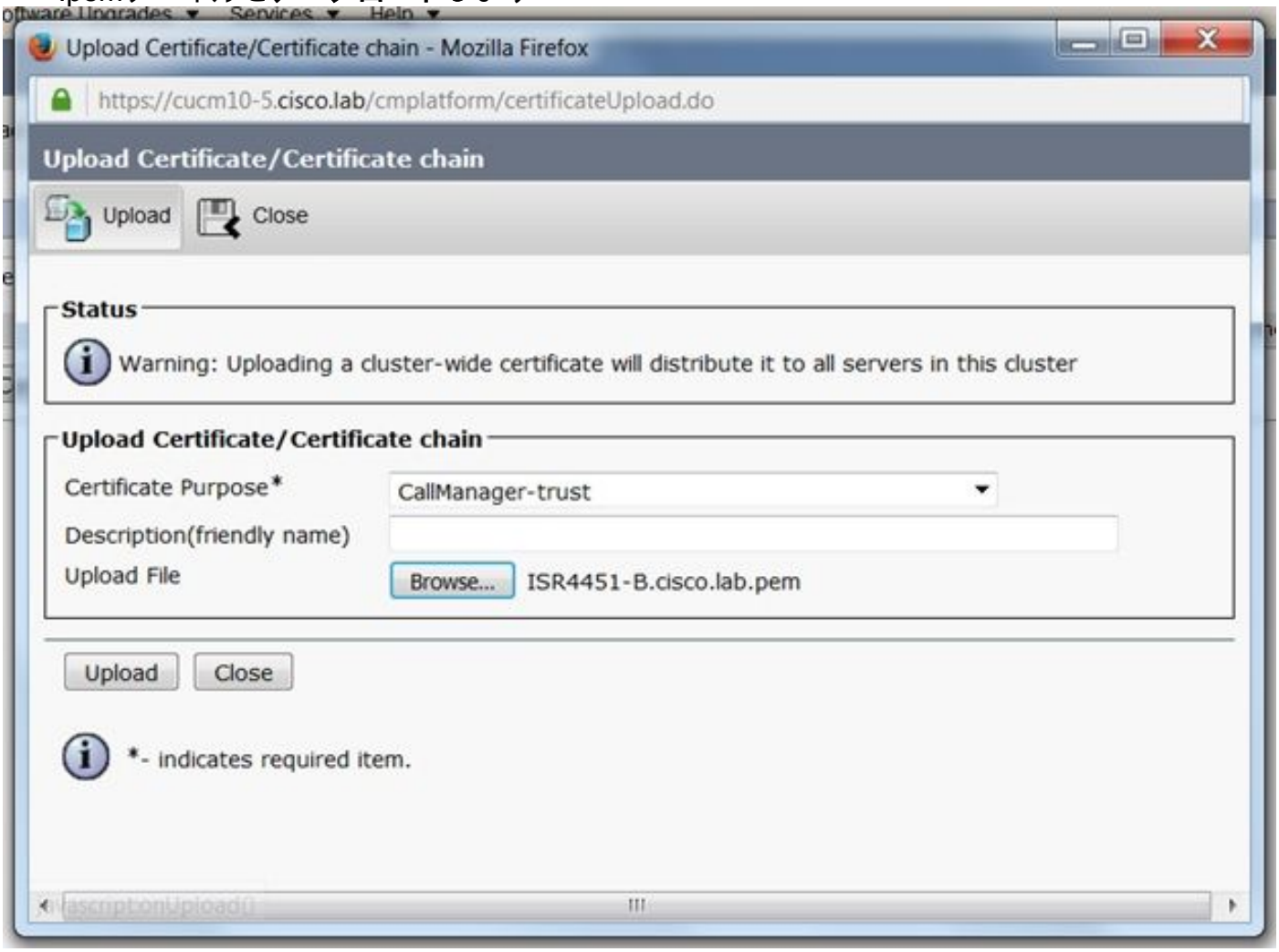
上記で生成された自己署名証明書をコピーし、ファイル拡張子.pemのテキストファイルに貼り付けます

次の例は、ISR4451-B.ciscolab.pemという名前です



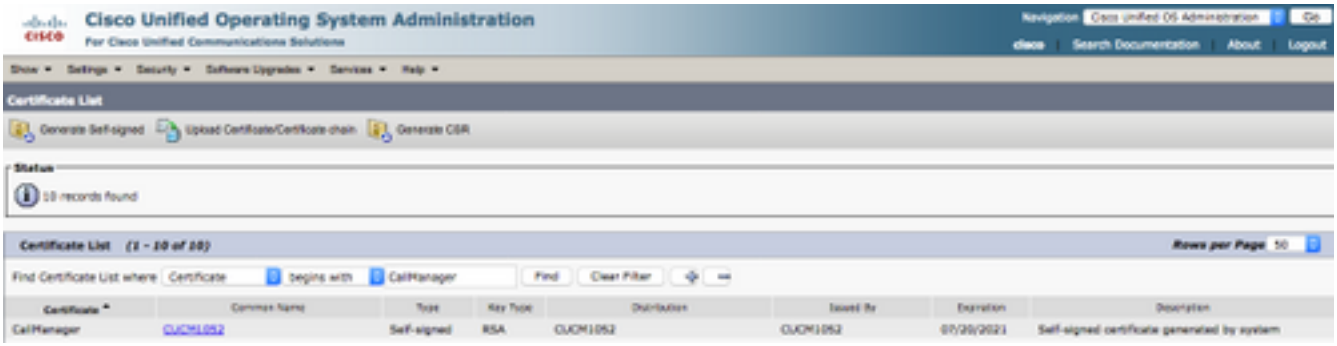
ステップ4:CUBE証明書をCUCMにアップロードします

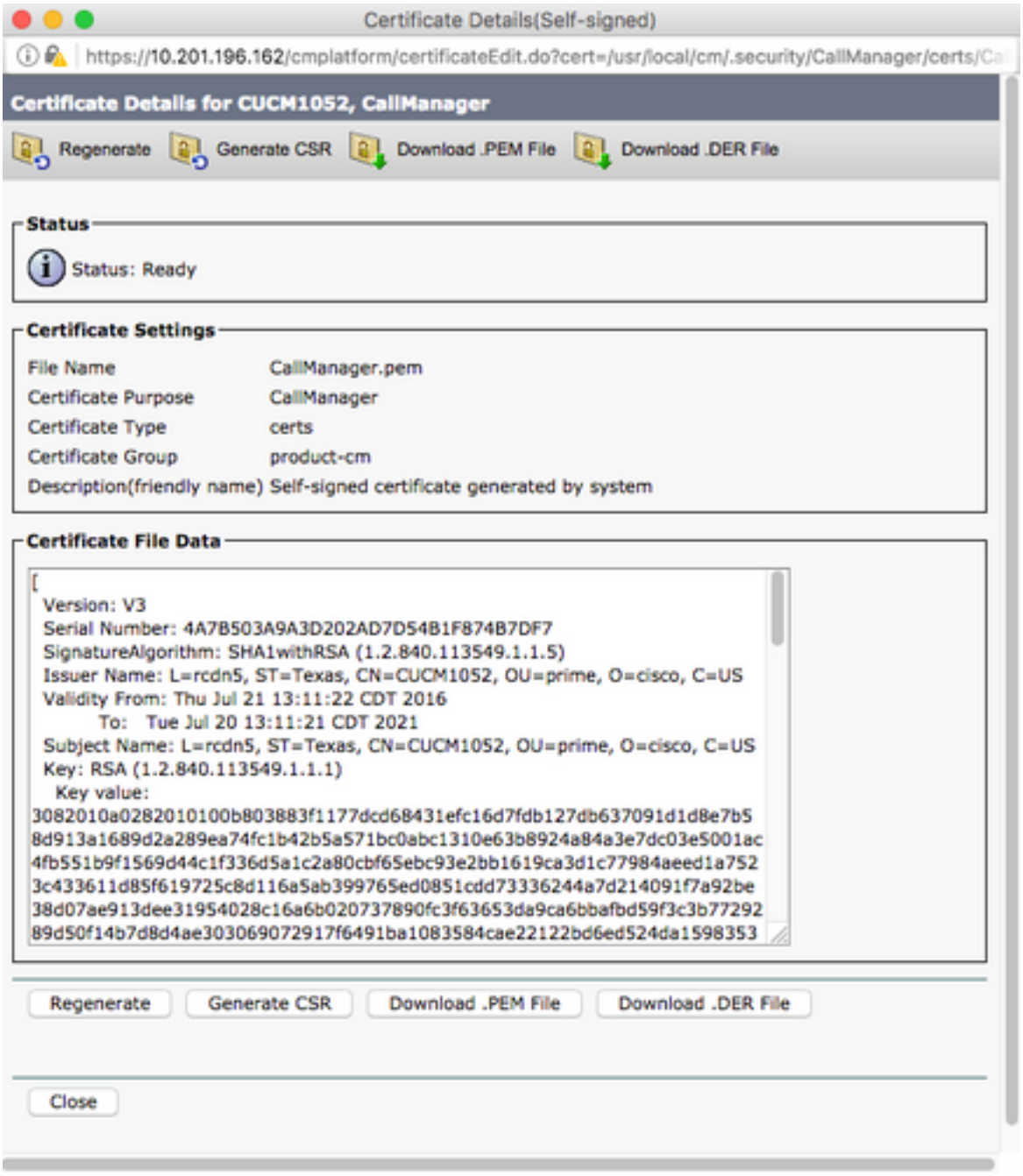
- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- 証明書の目的= CallManager-Trust
- .pemファイルをアップロードします



ステップ5:Call Manager自己署名証明書をダウンロードします

- Callmanager
- ホスト名をクリックします
- [download PEM file]をクリックします
- コンピュータに保存する





ステップ6:Callmanager.pem証明書をCUBEにアップロードします

- テキストエディタでCallmanager.pemを開きます
- ファイルの内容全体をコピーする
- CUBEで次のコマンドを実行します

```
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:CUBEの自己署名証明書トラストポイントを使用するようにSIPを設定します

```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

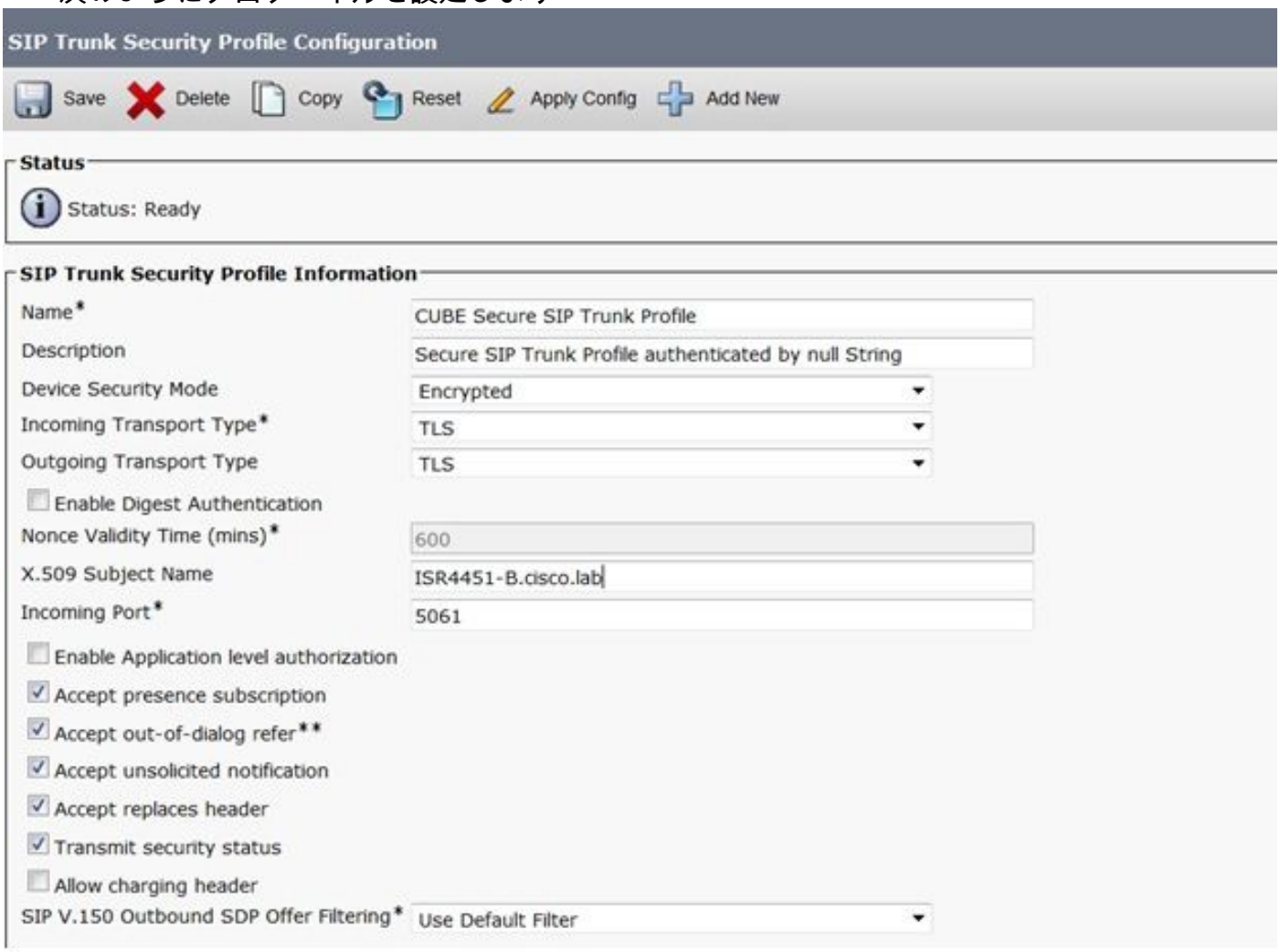
手順8:TLSを使用してダイヤルピアを設定する

```
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ます

- [CUCM Admin]ページ> [System] > [Security] > [SIP Trunk Security Profile]
- 次のようにプロファイルを設定します

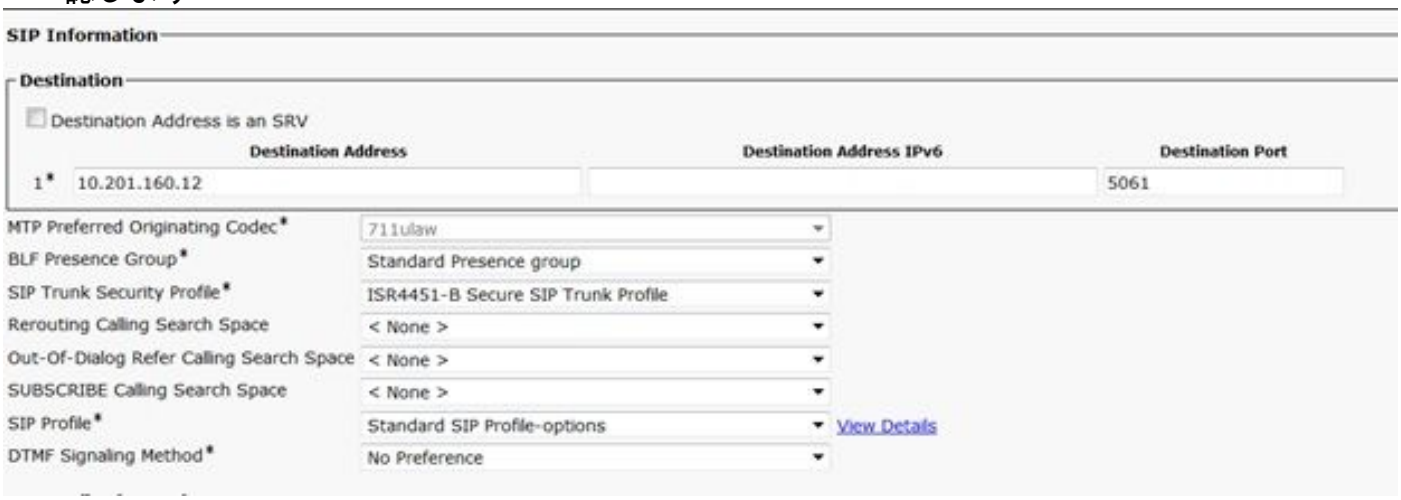


注： X.509フィールドが、自己署名証明書の生成中に以前に設定したCN名と一致することが非常に重要です

ステップ10:CUCMでSIPトランクを設定する

- [SRTP allowed]チェックボックスがオンになっていることを確認します
- 適切な宛先アドレスを設定し、ポート5060をポート5061に置き換えることを確認します
- 正しいSipトランクセキュリティプロファイル（ステップ9で作成）を選択していることを確

認します



- トランクを保存してリセットします。

確認

CUCMでOPTIONS PINGを有効にしたため、SIPトランクはFULL SERVICE状態である必要があります

SIPトランクのステータスが[full service]と表示されます。

ダイヤルピアステータスは次のように表示されます。

```
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
```

トラブルシュート

これらのデバッグの出力を有効にして収集します

```
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 Recordingリンク：

https://goo.gl/QOS1iT