

# CA署名付き証明書を使用したCUCM-CUBE/CUBE-SBC間のSIP TLSの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

## 概要

このドキュメントでは、認証局(CA)署名付き証明書を使用して、Cisco Unified Communication Manager(CUCM)とCisco Unified Border Element(CUBE)の間でSIPトランスポート層セキュリティ(TLS)を設定する方法について説明します。

## 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Unified Communication K9(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。

注 : Cisco IOS-XEバージョン16.10以降では、プラットフォームはスマートライセンスに移行しました。

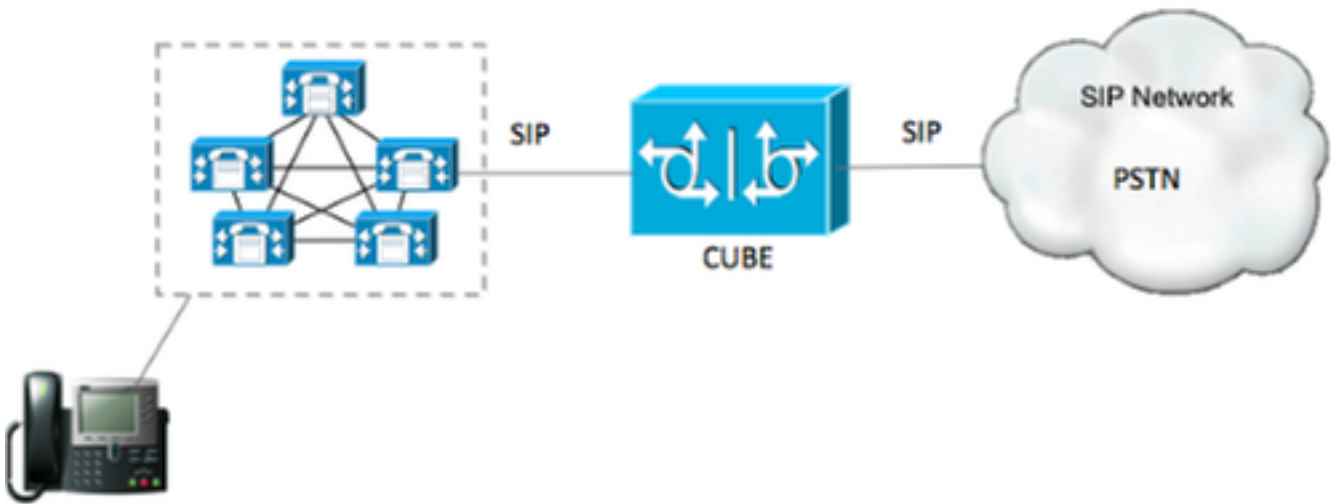
## 使用するコンポーネント

- SIP

- 認証局署名証明書
- Cisco IOS および IOS-XE ゲートウェイ 2900/3900/4300/4400/CSR1000v/ASR100Xバージョン : 15.4+
- Cisco Unified Communications Manager ( CUCM ) バージョン : 10.5+

## 設定

### ネットワーク図



### コンフィギュレーション

ステップ1 : 次のコマンドを使用して、ルート証明書の証明書の長さに一致するRSAキーを作成します。

```
Crypto key generate rsa label TestRSAkey exportable modulus 2048
```

このコマンドは、長さが2048ビット ( 最大4096 ) のRSAキーを作成します。

ステップ2 : 次のコマンドを使用して、CA署名付き証明書を保持するトラストポイントを作成します。

```
Crypto pki trustpoint CUBE_CA_CERT
  serial-number none
  fqdn none
  ip-address none
  subject-name cn=ISR4451-B.cisco.lab !(this has to match the router's hostname
[hostname.domain.name])
  revocation-check none
  rsakeypair TestRSAkey !(this has to match the RSA key you just created)
```

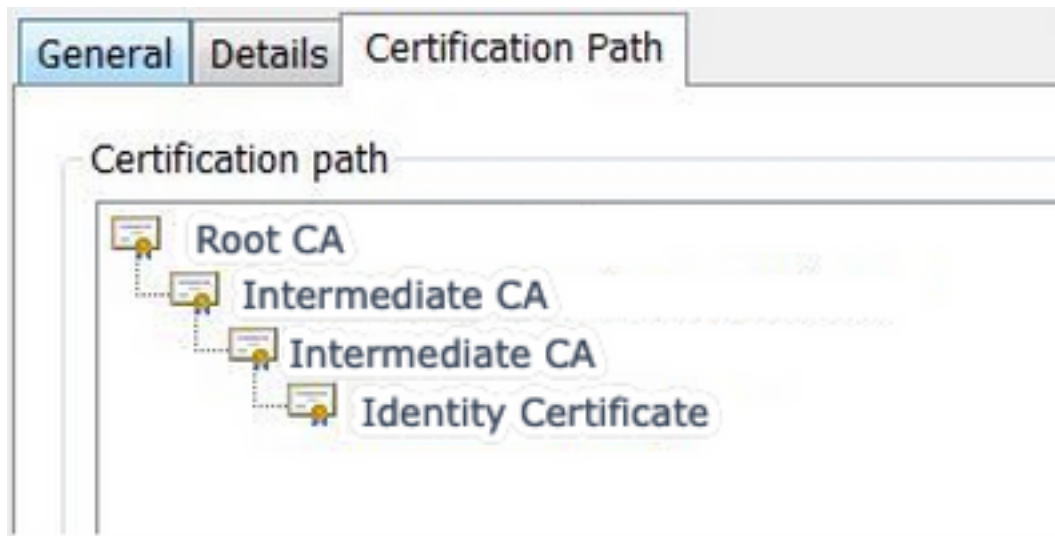
手順3 : これでトラストポイントが完成したので、次のコマンドを使用してCSR要求を生成します。

```
Crypto pki enroll CUBE_CA_CERT
```

画面の質問に答え、CSR要求をコピーしてファイルに保存し、CAに送信します。

ステップ4：ルート証明書チェーンに中間証明書があるかどうかを確認する必要があります。中間認証局がない場合は、ステップ7に進み、そうでない場合はステップ6に進みます。

ステップ5：ルート証明書を保持するトラストポイントを作成します。さらに、CUBE証明書に署名するトラストポイントまで中間CAを保持するトラストポイントを作成します（下図を参照）。



この例では、1番目のレベルがルートCAで、2番目のレベルが最初の中間CAで、3番目のレベルがCUBE証明書に署名するCAなので、これらのコマンドで最初の2つの証明書を保持するトラストポイントを作成する必要があります。

```
Crypto pki trustpoint Root_CA_CERT
Enrollment terminal pem
Revocation-check none
```

```
Crypto pki authenticate Root_CA_CERT
Paste the X.64 based certificate here
```

```
Crypto pki trustpoint Intermediate_CA
Enrollment terminal
Revocation-check none
```

```
Crypto pki authenticate Intermediate_CA
```

ステップ6。CA署名付き証明書を受信した後、トラストポイントを認証します。トラストポイントは、CUBE証明書の直前にCAの証明書を保持する必要があります。証明書をインポートできるコマンドは、

```
Crypto pki authenticate CUBE_CA_CERT
```

ステップ7：証明書をインストールしたら、このコマンドを実行してCUBE証明書をインポートする必要があります

```
Crypto pki import CUBE_CA_CERT cert
```

ステップ8：作成したトラストポイントを使用するようにSIP-UAを設定します

```
sip-ua
```

```
crypto signaling default trustpoint CUBE_CA_CERT
```

ステップ 9： 次のようにダイヤルピアを設定します。

```
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
```

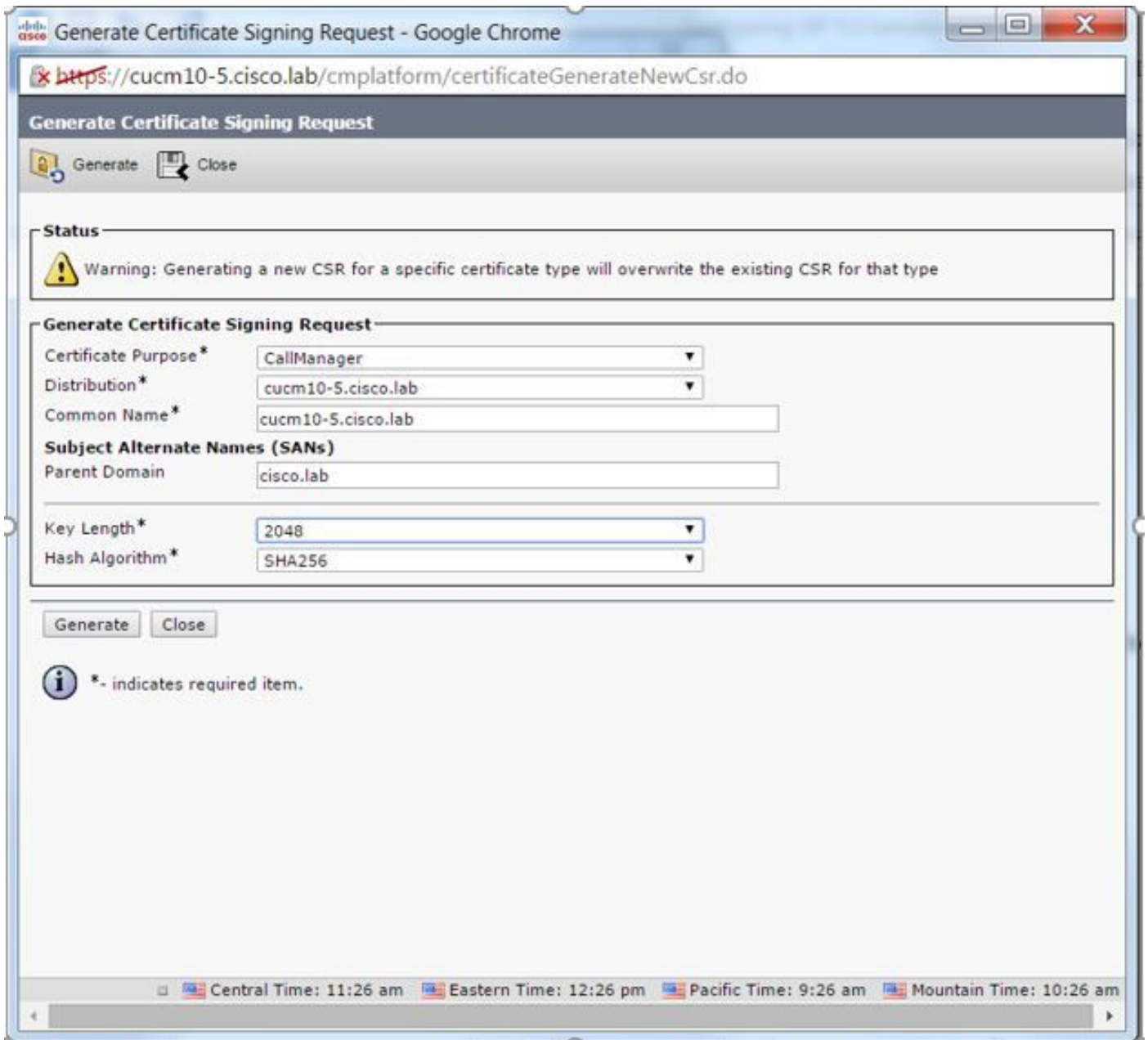
```
srtplib
```

これで、CUBEの設定は完了です。

ステップ 10： 次に、CUCM CSRを生成します。次の手順に従います

- CUCM OS管理者にログインします。
- [Security]をクリックします
- [certificate management]をクリックします。
- [generate CSR]をクリックします

CSR要求は次のように表示される必要があります。



ステップ11:CSRをダウンロードし、CAに送信します。

ステップ12:CA署名付き証明書チェーンをCUCMにアップロードする手順は次のとおりです。

- [security]をクリックし、次に[certificate management]をクリックします。
- [upload certificate/certificate chain]をクリックします。
- [certificate purpose]ドロップダウンメニューで、[call manager]を選択します。
- ファイルを参照します。
- [upload]をクリックします。

ステップ13:CUCM CLIにログインし、次のコマンドを実行します

```
utils ctl update CTLFile
```


ステップ14:CUCM SIPトランクセキュリティプロファイルの設定

- [system]、[security]、[sip trunk security profile]の順にクリックします
- 図に示すようにプロファイルを設定します。

## SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

### Status

 Status: Ready

### SIP Trunk Security Profile Information


Name*	<input type="text" value="CUBE_CA Secure SIP Trunk Profile"/>
Description	<input type="text" value="Secure SIP Trunk Profile authenticated by null String"/>
Device Security Mode	<input type="text" value="Encrypted"/>
Incoming Transport Type*	<input type="text" value="TLS"/>
Outgoing Transport Type	<input type="text" value="TLS"/>
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	<input type="text" value="600"/>
X.509 Subject Name	<input type="text" value="cucm10-5.cisco.lab"/>
Incoming Port*	<input type="text" value="5061"/>
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	<input type="text" value="Use Default Filter"/>

注：この場合、X.509のサブジェクト名は、図の強調表示された部分に示すように、CUCM証明書のサブジェクト名と一致する必要があります。

## Certificate Details for cucm10-5.cisco.lab, CallManager

 Regenerate  Generate CSR  Download .PEM File  Download .DER File

### Status

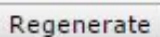
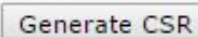
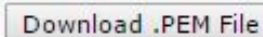
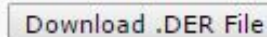
 Status: Ready

### Certificate Settings

Locally Uploaded 10/02/16  
File Name CallManager.pem  
Certificate Purpose CallManager  
Certificate Type certs  
Certificate Group product-cm  
Description(friendly name) Certificate Signed by AD-CONTROLLER-CA

### Certificate File Data

```
[
Version: V3
Serial Number: 1D255E0000000000000007
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: CN=AD-CONTROLLER-CA, DC=cisco, DC=lab
Validity From: Wed Feb 10 10:45:23 CST 2016
To: Fri Feb 10 10:55:23 CST 2017
Subject Name: CN=cucm10-5.cisco.lab, OU=TAC, O=CISCO, L=RICHARSON, ST=TEXAS, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100ae8db062881c35163f1b6ee4be4951158fdb3495d3c8032170c9fb8bafb385a2
27b00ec1024807f0adc49df875189779c7de1ae1e7e64b45e6f9917fa6ca5687d9aeaf20d70018e8d5
58a832360b82702249fc98855012c7d2cc29eea0f92fad9e739d73b0fa24d7dd4bd9fc96be775fda997
f03a440645ad64fa9f083ed95445e200187dd8775aa543b2bab11a5e223e23ef03bb86bb9fd969b3d9
3ba2550c35ea06ed5149aef2253c2455a622122e0aa3b649a090911995069a2cfd4ab4ab1fe15b242
]
```

ステップ15:CUCMで通常行うようにSIPトランクを設定します

- [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。
- SIPトランクセキュリティプロファイルで、ステップ14で作成したSIPプロファイル名を選択します。

**SIP Information**

**Destination**

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* [redacted]		5061

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* ISR4451-B Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile-options [View Details](#)

DTMF Signaling Method\* No Preference

# 確認

これで、すべての設定が正常であれば、

CUCMで、SIPトランクのステータスがFull Service(FULL)と表示されます ( 図を参照 )。

Name ^	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			0711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

CUBEでは、ダイヤルピアに次のステータスが表示されます。

```
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
```

この同じプロセスが他のルータにも適用されます。唯一の違いは、CUCM証明書をアップロードする手順ではなく、サードパーティが提供する証明書をアップロードすることです。

## トラブルシューティング

CUBEで次のデバッグを有効にします

```
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
```