

# CUBE で IOS CA を使用した SIP TLS および SRTP-RTP インターネットワーキング

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[CUBE の設定](#)

[CUCM の設定](#)

[確認](#)

[トラブルシューティング](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

このドキュメントでは、Session Initiation Protocol ( SIP ) Transport Layer Security ( TLS ) の基本を示しており、シスコのSecure Real-Time Transport Protocol ( SRTP ) はCisco Unified Border Element ( CUBE ) の設定例を提供します。

CUBE経由のセキュアな音声通信は2部構成に分割できます:

- セキュアなシグナリング- CUBEは保護するためにTLSをにH.323シグナリングを保護するSIPおよびInternet Protocol Security ( IPsec ) にシグナリングを使用します
- メディア ( SRTP ) の保護します

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- Cisco Unified Communications Manager(CUCM)のCertificateTrustList(CTLファイルが混合モード用に作成された
- IP Phoneはセキュア モード ( 暗号化 ) に登録されます。
- CUBEの基本voice service voip dial-peerおよび設定が行われます

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- CUCM 10.5
- CUBE - IOS 15.3(3) M3で3925E
- Cisco IP Communicator ( CIPC )

## 背景説明

- TLS (トランスポートおよびその前身、Secure Sockets Layer (SSL)) で、インターネット経由で通信のセキュリティを提供する暗号化プロトコル。

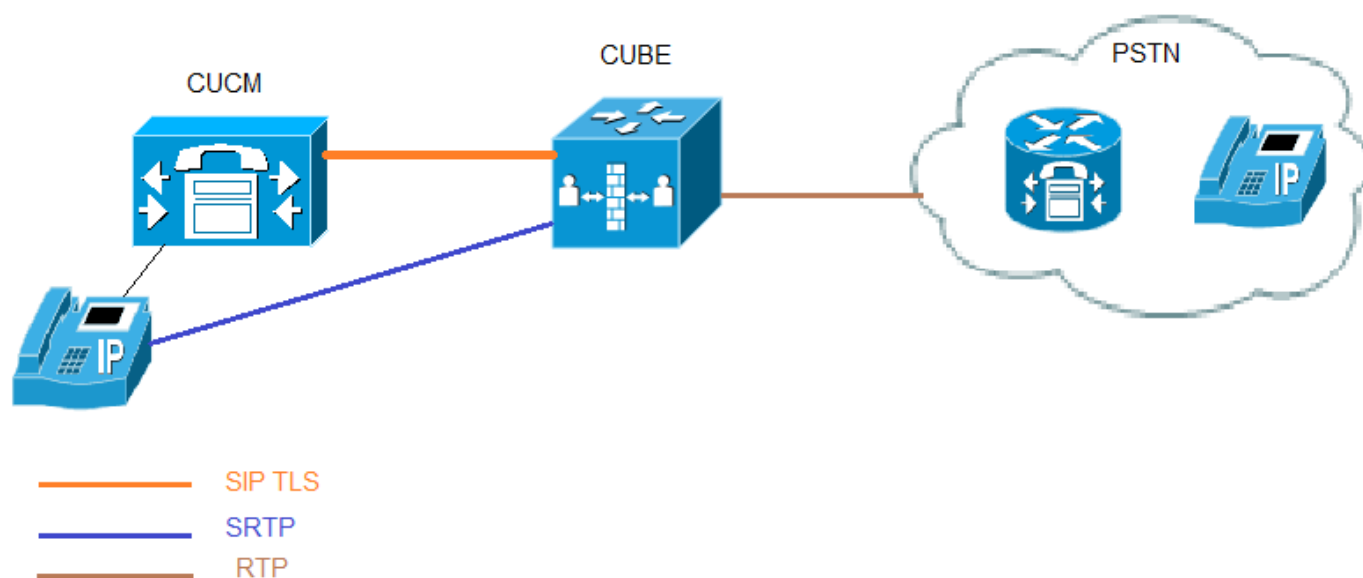
開放型システム間相互接続 (OSI) モデル等価機能では、TLS/SSLはレイヤ5 (セッション層) で初期化され、プレゼンテーション層 (レイヤ6) で動作します。両方のモデルでは、SSLおよびTLSはセグメントは暗号化されたデータを伝送する基盤となるトランスポート層に代わって成り立ちます。

- 認証局 (CA) として信頼できるエンティティが証明書を発行: シスコまたはサードパーティのエンティティ。
- デバイス認証 - 接続が確立される前に、デバイスの ID を検証して、そのエンティティが正当なものであることを確認するプロセスです。
- 暗号化-情報の機密性を保証するデータを暗号文に変換するプロセス。目的の受信者のみデータを読み取ることができます。これは暗号化アルゴリズムと暗号キーが必要です。
- 公開/秘密キーの暗号化に使用されるキー。公開キーを利用できますが、秘密鍵は、それぞれの所有者に流通する非対称暗号化は、両方のキーを使用します。

## 設定

### ネットワーク図

この図では、CUCM/IP PhoneとCUBE間のSIP TLSおよびSRTPを設定する設定例を示します。SRTPとRTP間のインターネットワークをそれぞれにします。IOS CAとCUCMが自己署名証明書を使用するため、それぞれに機能します。



### CUBE の設定

1. クロックを設定し、HTTPサーバをイネーブルにします

CAサーバとクライアントのトラストポイント (CUBE/OGW/TGW) のクロックを同期します。そうしないと、CAサーバによって発行された証明書の有効性の問題があります。

```
Secure-CUBE#clock set <hh:mm:ss> < Day of the month> <MONTH> <Year>
```

Or

```
Ntp server <IP Address>
```

クライアントのトラストポイントが、CAから証明書を受信するためにHTTPが使用されます。

```
Secure-CUBE(config)#ip http server
```

## 2. RSA キーペアを生成する

この手順は、秘密鍵と公開鍵を生成します。

この例では、CUBEは、ラベルです。これは何でもかまいません。

```
Secure-CUBE(config)#crypto key generate rsa general-keys label CUBE modulus 1024
```

```
The name for the keys will be: CUBE
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 0 seconds)
```

```
Secure-CUBE(config)#
```

## 3. Cisco IOS CA サーバを設定する

この例で、CA サーバの名前は cube-ca です。

```
crypto pki server cube-ca
```

```
database level complete
```

```
no database archive
```

```
grant auto
```

```
lifetime certificate 1800
```

```
Secure-CUBE(cs-server)#no shut
```

```
%Some server settings cannot be changed after CA certificate generation.
```

```
% Please enter a passphrase to protect the private key
```

```
% or type Return to exit
```

```
Password:
```

```
Re-enter password:
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 0 seconds)
```

```
% Certificate Server enabled.
```

```
Secure-CUBE(cs-server)#
```

## 4. TLS通信のCUBEのPKIトラストポイントを作成します。

**この例では、CUBEのトラストポイント名がCUBE-TLSです。** エンロールメントURLで使用するIPアドレスはCUBEのローカル インターフェイスにする必要があります。このステップで使用されるサブジェクト名はCUCM SIPトランク セキュリティ プロファイルの [X.509のサブジェクト名と一致する必要があります。推奨事項 (ドメイン名が有効になったら) ドメイン名のホスト名を使用することです。

手順2.で作成された関連のRSAキー ペア。

```
crypto pki trustpoint CUBE-TLS
```

```
enrollment url http://X.X.X.X:80
```

```
serial-number none
```

```
fqdn none
```

```
ip-address none
```

```
subject-name CN=Secure-CUBE
```

```
revocation-check none
```

rsakeypair CUBE

5. CAサーバで、トラストポイントを認証し、.CAの証明書を受け入れます。

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
```

Certificate has the following attributes:

Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711

Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

```
Secure-CUBE(config)#
```

6. CAサーバで、トラストポイントを登録します。

この手順では、CUBEからCA署名付き証明書を受け取ります。

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
```

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
```

Password:

Re-enter password:

```
% The subject name in the certificate will include: CN=Secure-CUBE
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CUBE-TLS' command will show the fingerprint.
```

```
Secure-CUBE(config)#
```

7. CUCM のトラストポイントを作成します。

CallManagerグループに複数のCMサーバがあれば、トラストポイントをすべてのサーバで作成する必要があります。統一されていないと、フェールオーバーが機能しません。

```
crypto pki trustpoint cucmpub
enrollment terminal
revocation-check none
```

```
crypto pki trustpoint cucmsub
enrollment terminal
revocation-check none
```

8. CUBEへとCUCM証明書を登録します。

手順1: CUCM OS Adminページにログインします。

手順2: [Security] > [Certificate Management] > [Find] と移動します。

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

Status

26 records found

Certificate List (1 - 26 of 26)

Rows per Page 50

Find Certificate List where Certificate begins with Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Ex
CallManager <a href="#">cmpub</a>		Self-signed	cmpub	cmpub	02/
CallManager-trust <a href="#">Cisco_Root_CA_2048</a>		Self-signed	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/
CallManager-trust <a href="#">Cisco_Root_CA_M2</a>		Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/
CallManager-trust <a href="#">cmsub</a>		Self-signed	cmsub	cmsub	02/
CallManager-trust <a href="#">CAP-RTP-001</a>		Self-signed	CAP-RTP-001	CAP-RTP-001	02/
CallManager-trust <a href="#">Cisco_Manufacturing_CA</a>		CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/
CallManager-trust <a href="#">CAPF-9a08b5fe</a>		Self-signed	CAPF-9a08b5fe	CAPF-9a08b5fe	02/

ステップ 3 : CallManager証明書をクリックし、次に示すようにPEMファイルをダウンロードして保存します。

### Certificate Details for cmpub, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

**Status**

Status: Ready

**Certificate Settings**

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

**Certificate File Data**

```
[
Version: V3
Serial Number: 6AA0AECEC947BDCAFCC722310EE83224
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Validity From: Sat Feb 07 22:39:22 IST 2015
To: Thu Feb 06 22:39:21 IST 2020
Subject Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100d2191a26d52904ae14c3b6eb1a27607d5ca4d85251037db19141e76906d2cfcf5dca3
097fff569b7c19b9705de7624ca441617d49e08ee21a5d5cb8f3583a1f6089278b971833b6132dd4c77e
5e81866f2f4386bc16252658e5bf0c37cb844df8a53a7dc034dff225fe7127b0fba88ab96617d01c3026f1
04eea12492a8572250203010001
Extensions: 3 present
]
```

手順 4 : メモ帳のファイルを開き、BEGIN CERTIFICATEからEND CERTIFICATEまでの内容をコピーします。

手順 5 : 次のようにCUBEのこの証明書を貼り付けます。

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICojCCAagugAwIBAgIQaaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEWJtJTJEOMAWGA1UEChMFY2lzy28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2lwdWlxejEjAQBgNVBAGTCWthcm5hdGFrcyYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyM1oXDTEwMDIwNzE3MDkyMVowYzELMAkGA1UEBhMC
SU4xdjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxdjAMBGNVBAMTBWNTcHVh
MRIwEAYDVQQQIEwlrYXJuYXRha2ExEjAQBgNVBACTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS289dyjCX /Vpt8GblwXediTKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8ueTfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVRO0BBYEFDFGq0WCT/OnqwePSnhaknzR0
```

```
BconMA0GCSqGSIB3DQEjBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/lZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeRObfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

## ステップ 6 他のCUCMサーバで同じ手順に従います。

### 9. トランスポート プロトコルとしてTCP/TLSを設定します。

これは、グローバルまたはダイヤルピア レベルで実行できます。

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICojCCAagAwIBAgIQaQcuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEWJtZjEOMAwGA1UEChMFY2l2Y28xMDEwMDEwMDEwMDEwMDEwMDEw
A1UEAxMFY2l2dWl0eXBlAQBgNVBAGTCWthcm5hdGFrYTESMBAQA1UEBxMjYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDky
SU4xDjAMBGNVBAoTBWNpc2NvMwQwCgYDVQQLEwN0YWMxDjAMBGNVBAQTBWNTcHVi
MRIwEAYDVQQQIEwlrYXJ0eXJha2EjAQBgNVBACTCWJhbmRhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQqMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEjBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/lZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeRObfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

```
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

### 10. sip-uaにトラストポイントを割り当て、このトラストポイントがCUBEとCUCM間のすべてのSIPシグナリングに使用されます

```
Secure-CUBE(config)#crypto pki authenticate cucmpub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

MIICo jCCAgugAwIBAgIQaqCuzslHvcr8xyIx DugyJDANBgkqhkiG9w0BAQUFADBjMQswCQYDVQGEWJTTjEOMAwGAlUEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwGAlUEAxMFY2lwdWIxejAQBGNVBAGTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs b3JlMB4XDTElMDIwNzE3MDkyMl0XDTEwMDIwNjE3MDkyMVowYzELMAkGAlUEBhMCSU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWVMDjAMBGNVBAMTBWntcHViMRIwEAYDVQQIEwlrYXJuYXRha2EExEjAQBGNVBAGTCWJhbmdbG9yZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN aQbSz89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzhMt1Md+XoGGby9DhrwWJSZY5b8MN8uETf ilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoSSSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGAlUdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0BconMAOGCSqGSIB3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDonwqz4yBMsa7Nk6QmpP5zXKJjfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/lZfV RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASpSkX08/Ar

-----END CERTIFICATE-----

Certificate has the following attributes:  
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C  
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes  
Trustpoint CA certificate accepted.  
% Certificate successfully imported

Secure-CUBE(config)#  
またはデフォルトトラストポイントはCUBEからのすべてのSIPシグナリング用に設定できます。

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----  
MIICo jCCAgugAwIBAgIQaqCuzslHvcr8xyIx DugyJDANBgkqhkiG9w0BAQUFADBjMQswCQYDVQGEWJTTjEOMAwGAlUEChMFY2lZy28xDDAKBgNVBAsTA3RhYzEOMAwGAlUEAxMFY2lwdWIxejAQBGNVBAGTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs b3JlMB4XDTElMDIwNzE3MDkyMl0XDTEwMDIwNjE3MDkyMVowYzELMAkGAlUEBhMCSU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWVMDjAMBGNVBAMTBWntcHViMRIwEAYDVQQIEwlrYXJuYXRha2EExEjAQBGNVBAGTCWJhbmdbG9yZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN aQbSz89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG1lcuPNYOh9giSeLlxgzhMt1Md+XoGGby9DhrwWJSZY5b8MN8uETf ilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoSSSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGAlUdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0BconMAOGCSqGSIB3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDonwqz4yBMsa7Nk6QmpP5zXKJjfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/lZfV RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASpSkX08/Ar

-----END CERTIFICATE-----

Certificate has the following attributes:  
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C  
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes  
Trustpoint CA certificate accepted.  
% Certificate successfully imported

Secure-CUBE(config)#





-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

IOSが15.2.2T未満であれば、sccpのトランスコーダを設定します。

Skinny Call Control Protocol (SCCP) トランスコーダは、同じトラストポイント (CUBE-TLS) がCUBEに使用できる、トランスコーダ トランスコーダを  
開催するときと同じルータを使用するとシグナリングのためだけではなく、トラストポイントが必要です。

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICoJCCAagugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlTjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWlxejAQBgNVBAGTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWVpc2NvMQwwCgYDVQQLEwN0YWMxZjAMBgNVBAMTBWVpc2Nv
MRIwEAYDVQQQIEwlrYXJhYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS289dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBAQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEE+Df+sx0rUit3oGcF4ce/lZfv
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicuDASp
SkXO8/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

## CUCM の設定

### 1. CUCMへのエクスポートのCUBE IOS証明書。

ステップ 1 : IOS 証明書をエクスポートします。 自己署名付きCA証明書をコピーし、たとえば PEMファイル、安全CUBE.pem保存します

Secure-CUBE(config)#**crypto pki export CUBE-TLS pem terminal**

% CA certificate:

-----BEGIN CERTIFICATE-----

```
MIIB/TCCAawagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRawDgYDVQQDEwdjdWJl
LWNhbmB4XDTE1MDIwNzE3MDkyMl0XDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEAxMH
```

```
Y3ViZS1jYTCBnzANBqkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAtn3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr0lVbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnvlMH32lJ5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpoXpsWl
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAANjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBGwFoAUnqzVazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DFK8MA0GCSqGSIb3DQEBBAUAA4GB
AEfnNrB4nls8lvz0cqlpuTjID+KVyKRwYNP04zJYWCV7P+m1bpMfC/ql14z5/RzL
e5Bq6NUnxWByLR4gcFjmdS1E6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTrv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----
```

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```
MIIB7TCCAaVagAwIBAgIBAgIBANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDExNTYyMVowFjEUMBIGALUEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKwtfO
F9bBVYhVwQK8y2c5NMkJKY//pisg+oforvxalPKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTWk5jff9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAF
BgNVHSMEGDAwBSer09rMr/upfOGSh0IAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWvf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHHosEbm/vfqk2vbYiHU09AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGBDZzWiywv1jJ92ra3EMAUc0sJZSLzGY0+BjO/E
dEW6JUIOx3NxP2SBN1NMAQ0=
```

-----END CERTIFICATE-----

Secure-CUBE(config)#

ステップ 2 : CallManager信頼としてCUCMのIOS CA証明書をアップロードします。

ステップ 3 : CM OS Administration > セキュリティ > Certificate Management > Upload Certificate/Certificate Chainに移動します

ステップ 4 : この図に示すように、PEMファイルをアップロードします。

Upload Certificate/Certificate chain

Upload Close

**Status**

*i* Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Browse... Secure-CUBE.pem

Upload Close

*i* \*- indicates required item.

## 2. SIP トランク セキュリティ プロファイルを作成する

ステップ 1： Unified CM Administrationでシステム>セキュリティ>SIPトランク セキュリティ プロファイル>ファイルに移動します。

ステップ 2： 新規作成するプレゼンスを保護します。この図に示すように、プロファイルをコピーする非セキュアSIPトランク プロファイル。

**SIP Trunk Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**SIP Trunk Security Profile Information**

Name\* Secure SIP Trunk Profile

Description Secure SIP Trunk Profile authenticated by null String

Device Security Mode Encrypted

Incoming Transport Type\* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)\* 600

X.509 Subject Name Secure-CUBE

Incoming Port\* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer\*\*

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering\* Use Default Filter

## 3. CUBEへのSIPトランクを作成します

ステップ 1： この図に示すように、SIPトランクのSRTPを有効にします。

**Trunk Configuration**

Save Delete Reset Add New

Packet Capture Mode\* None

Packet Capture Duration 0

Media Termination Point Required

Retry Video Call as Audio

Path Replacement Support

Transmit UTF-8 for Calling Party Name

Transmit UTF-8 Names in QSIG APDU

Unattended Port

SRTP Allowed When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do Consider Traffic on This Trunk Secure\* When using both sRTP and TLS

Route Class Signaling Enabled\* Default

Use Trusted Relay Point\* Default

PSTN Access

Run On All Active Unified CM Nodes

ステップ 2 : 宛先ポート5061 ( TLS ) を設定して、次の図に示すように、SIPトランクの新しいセキュアSIPトランク セキュリティ プロファイルを適用します。

The screenshot shows the 'Trunk Configuration' interface. Under the 'SIP Information' section, the 'Destination' area has a checkbox for 'Destination Address is an SRV' which is unchecked. Below it, there are three input fields: 'Destination Address' with the value '10.106.95.155', 'Destination Address IPv6' which is empty, and 'Destination Port' with the value '5061'. The 'SIP Trunk Security Profile\*' dropdown menu is highlighted with a blue box and set to 'Secure SIP Trunk Profile'. Other dropdown menus include 'MTP Preferred Originating Codec\*' (711ulaw), 'BLF Presence Group\*' (Standard Presence group), 'Rerouting Calling Search Space' (< None >), 'Out-Of-Dialog Refer Calling Search Space' (< None >), 'SUBSCRIBE Calling Search Space' (< None >), 'SIP Profile\*' (Standard SIP Profile), and 'DTMF Signaling Method\*' (No Preference). A 'View Details' link is visible next to the SIP Profile dropdown.

## 確認

```
Secure-CUBE#show sip-ua connections tcp tls detail
```

```
Total active connections : 2
```

```
No. of send failures : 0
```

```
No. of remote closures : 13
```

```
No. of conn. failures : 0
```

```
No. of inactive conn. ageouts : 0
```

```
TLS client handshake failures : 0
```

```
TLS server handshake failures : 0
```

```
-----Printing Detailed Connection Report-----
```

```
Note:
```

```
** Tuples with no matching socket entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
```

```
to overcome this error condition
```

```
++ Tuples with mismatched address/port entry
```

```
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
```

```
to overcome this error condition
```

```
Remote-Agent:10.106.95.151, Connections-Count:2
```

```
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
```

```
=====
```

```
5061 16 Established 0 10.106.95.155
```

```
57396 17 Established 0 10.106.95.155
```

```
----- SIP Transport Layer Listen Sockets -----
```

```
Conn-Id Local-Address
```

```
=====
```

```
2 [10.106.95.155]:5061
```

show call active voice briefの出力を使用すると、LTIのトランスコーダが使用されたときにキャプ

チャサれます。

```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

また、SRTPが暗号化されたときにコールがCisco IP Phoneの間だけでなく、CUBEまたはゲートウェイはIP Phoneに、ロックアイコンが表示されます。

## トラブルシューティング

これらのデバッグはPKI/TLS/SIP/SRTP問題のトラブルシューティングに便利です。

```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```