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

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。

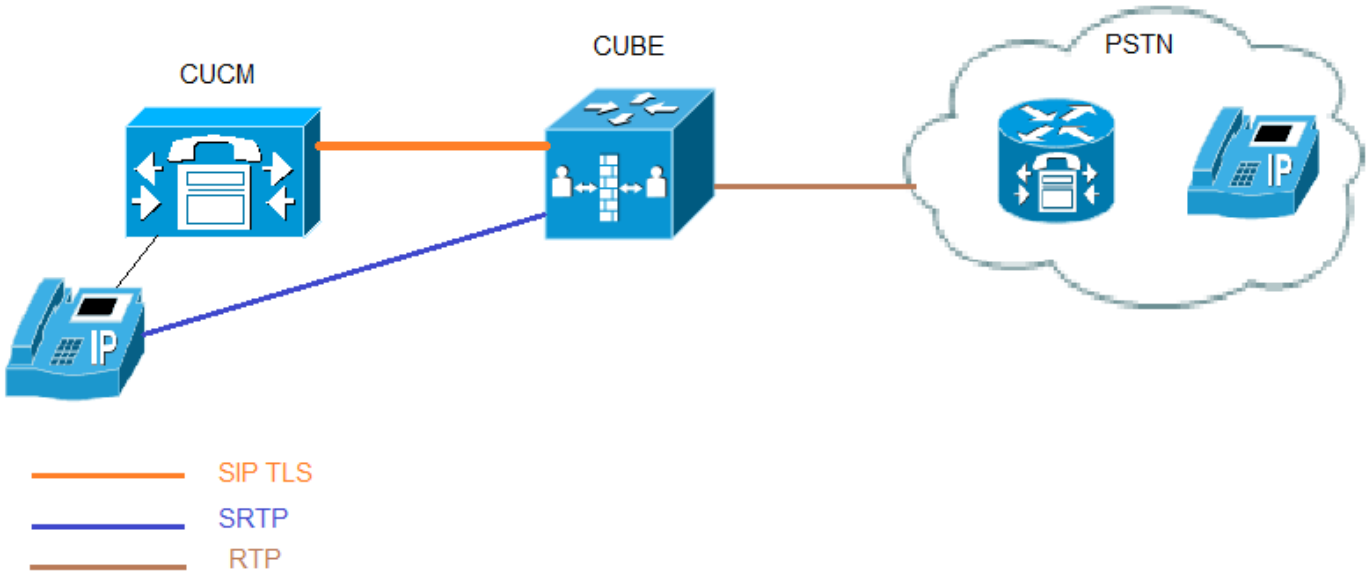
開放型システム間相互接続（OSI）モデル等価機能では、TLS/SSLはレイヤ5（セッション層）で初期化され、プレゼンテーション層（レイヤ6）で動作します。 両方のモデルでは、SSLおよびTLSはセグメントは暗号化されたデータを伝送する基盤となるトランスポート層に代わって成り立ちます。

- 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' commandwill show the fingerprint.

Secure-CUBE(config)#
```

7. CUCM のトラストポイントを作成します。

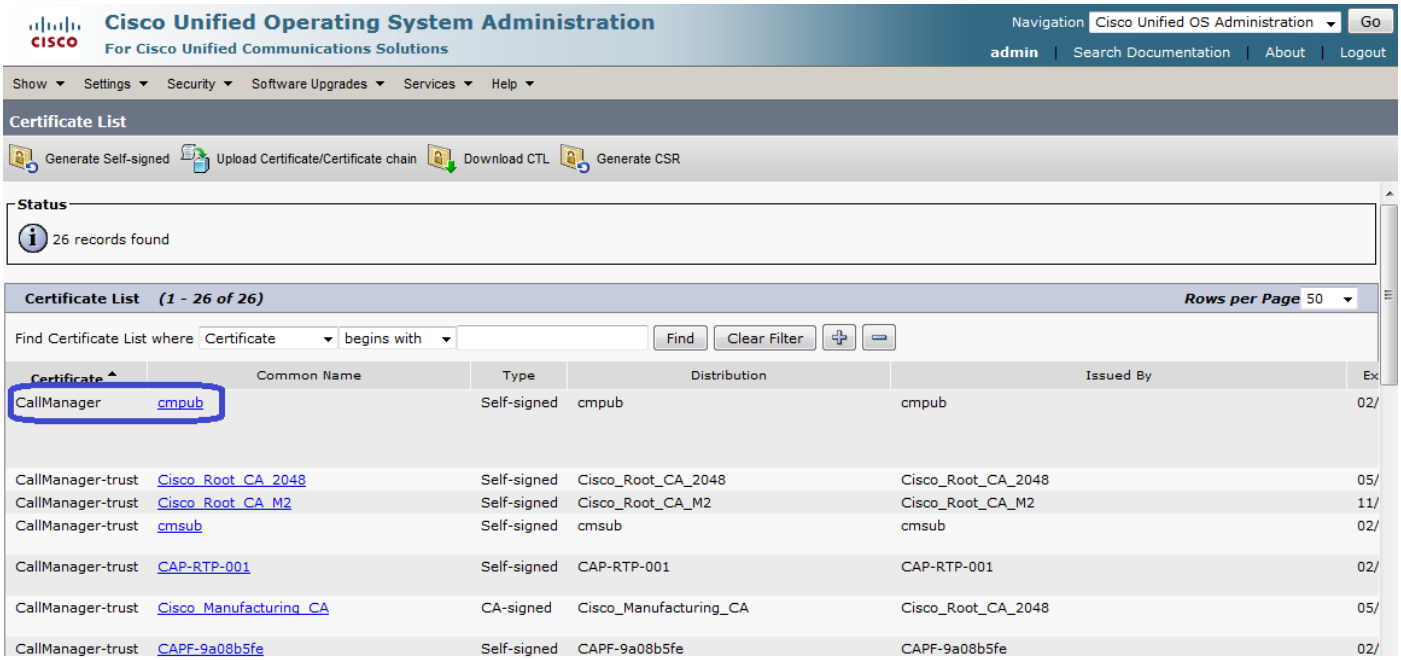
CallManagerグループに複数のCMサーバがあれば、トラストポイントをすべてのサーバで作成する必要があります。統一されていないと、フェールオーバーが機能しません。

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

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

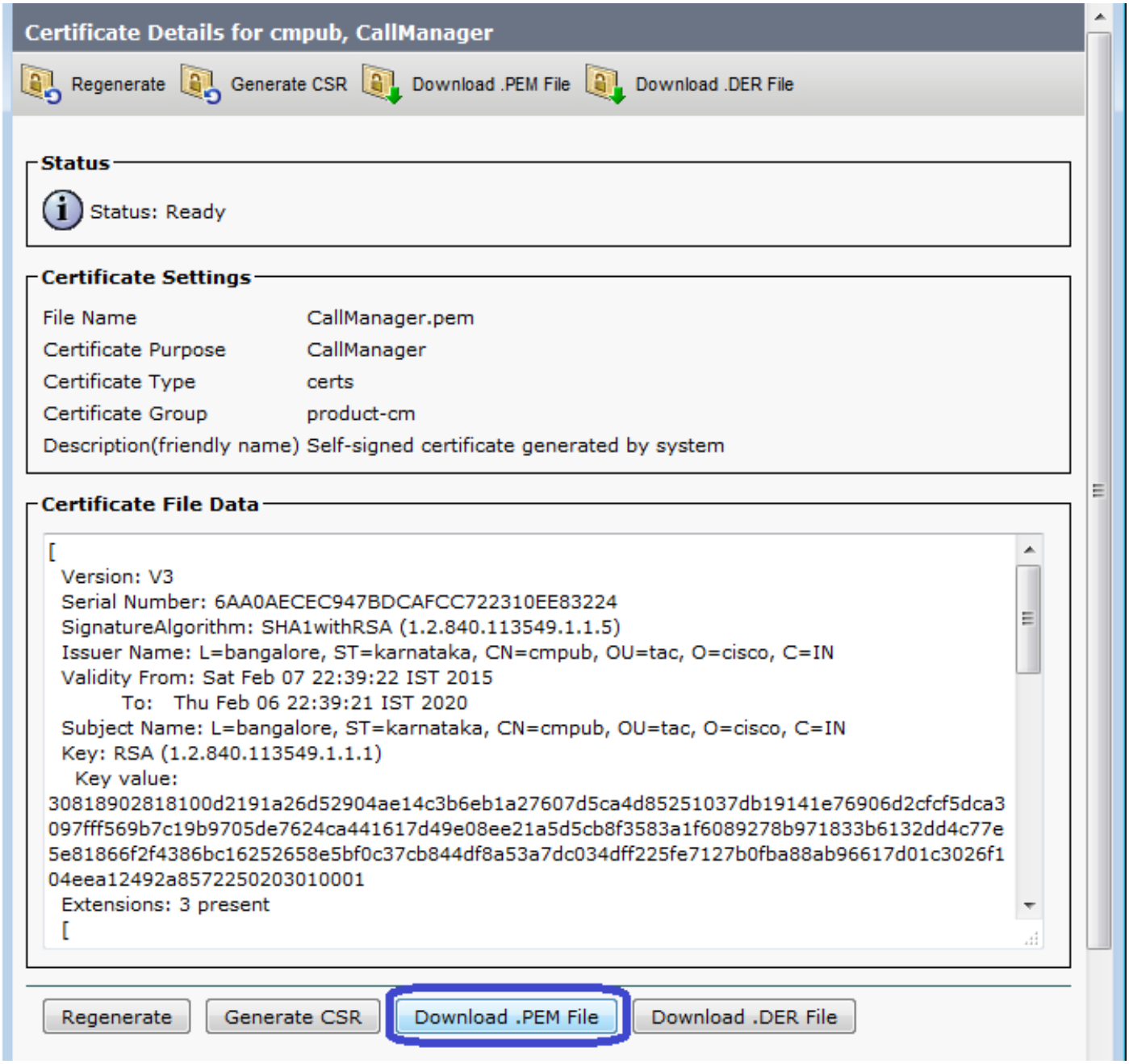
8. CUBEへとCUCM証明書を登録します。

手順 1：CUCM OS Adminページに口グインします。

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



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。



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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
```

```
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

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-----
```

```
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

11. Enable SRTP。

```
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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

12. SRTPおよびRTPインターネットワーキングに、トランスコーダが必要です。保護します。
IOS/バージョンが15.2.2T設定を最小限に抑えるLTIトランスコーダを設定するかどうかがCUBE（9.0）以降であれば。

LTIのトランスコーダはSRTP-RTPコールのためのPKIトラストポイントを設定する必要はありません

```
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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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)#
```

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-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
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

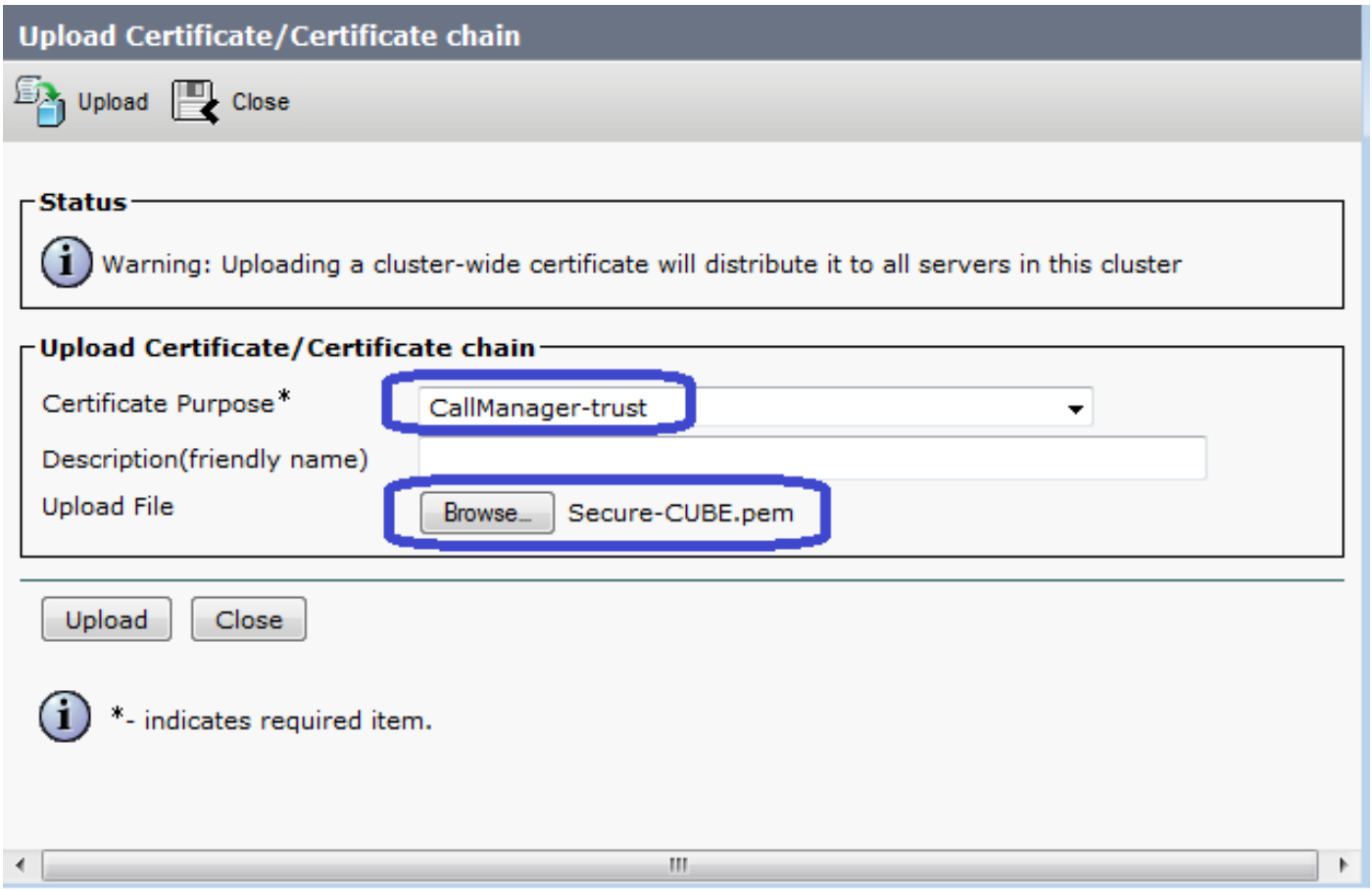
```
 Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVoXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
```

```
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtN3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr0lvbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH32lJ5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpoxpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCV7P+mlbpMfC/qh14z5/RzL
e5Bq6NUnxWByLR4gcFjmdSlE6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB7TCCAVagAwIBAgIBAjANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKWtfO
F9bBVYhVwQK8y2c5NMkJCY//pisg+oforvxalPKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jf9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAf
BgNVHSMEGDAWgBSerO9rMr/upfOGShOIAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWVf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHhOsEbm/vfqk2vbYiHUO9AtDDI+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**

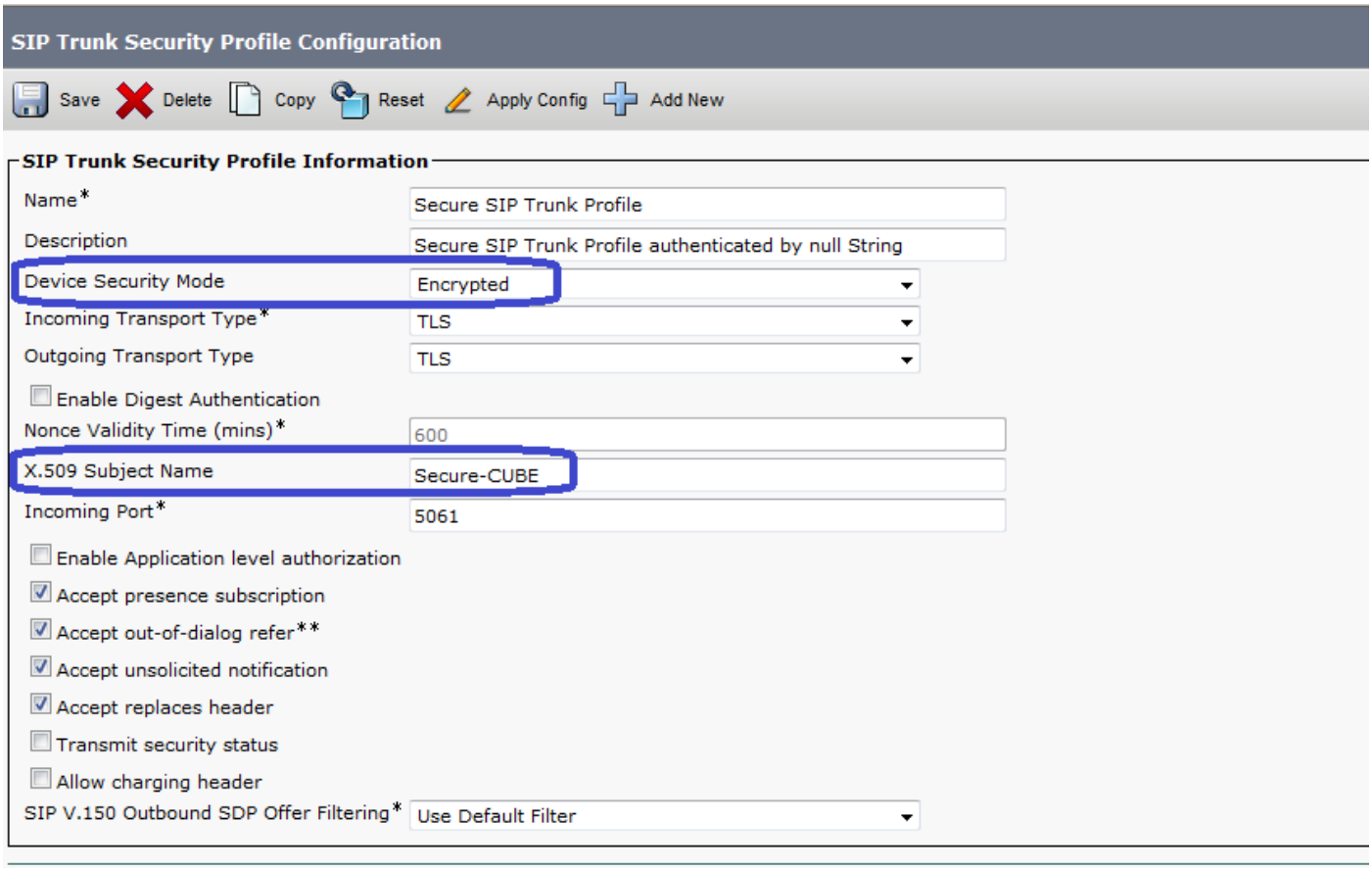
ステップ 4：この図に示すように、PEMファイルをアップロードします。



2. SIP トランク セキュリティ プロファイルを作成する

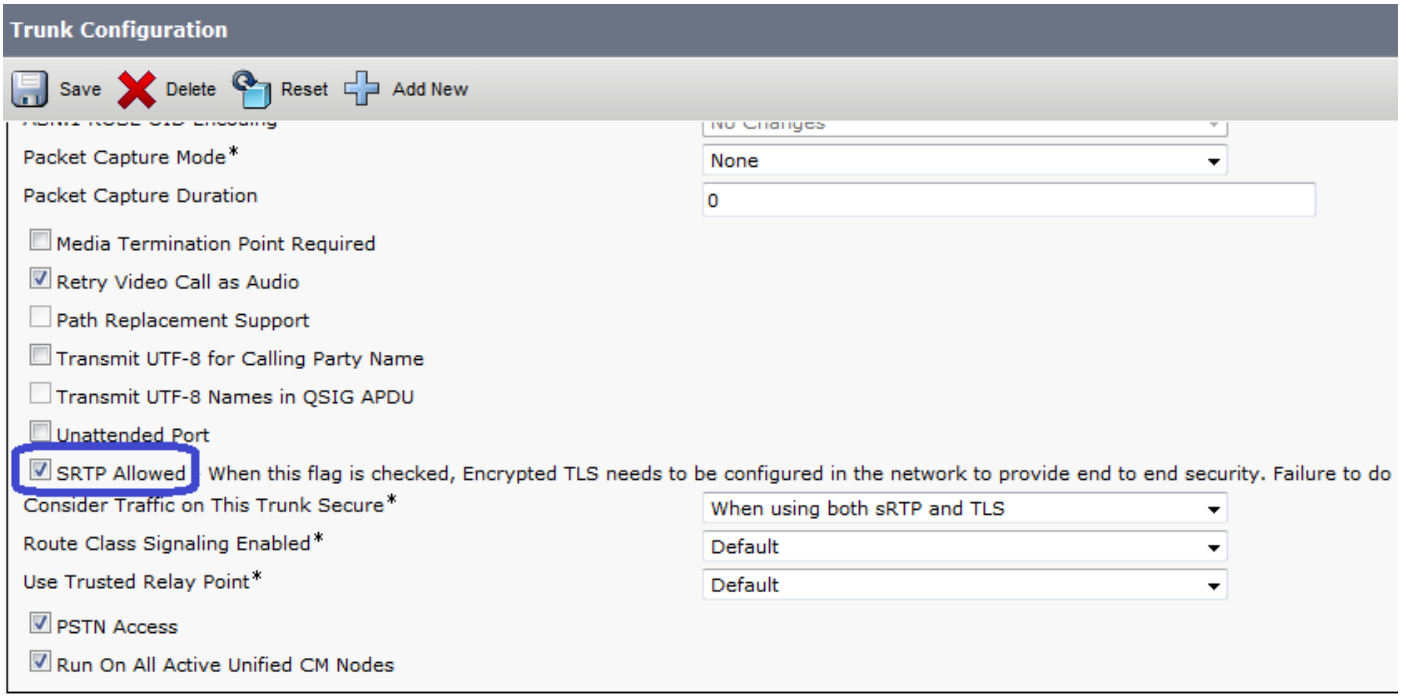
ステップ 1： Unified CM Administrationでシステム>**セキュリティ> SIPトランク セキュリティ プロファイル>ファイルに移動します。**

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。**

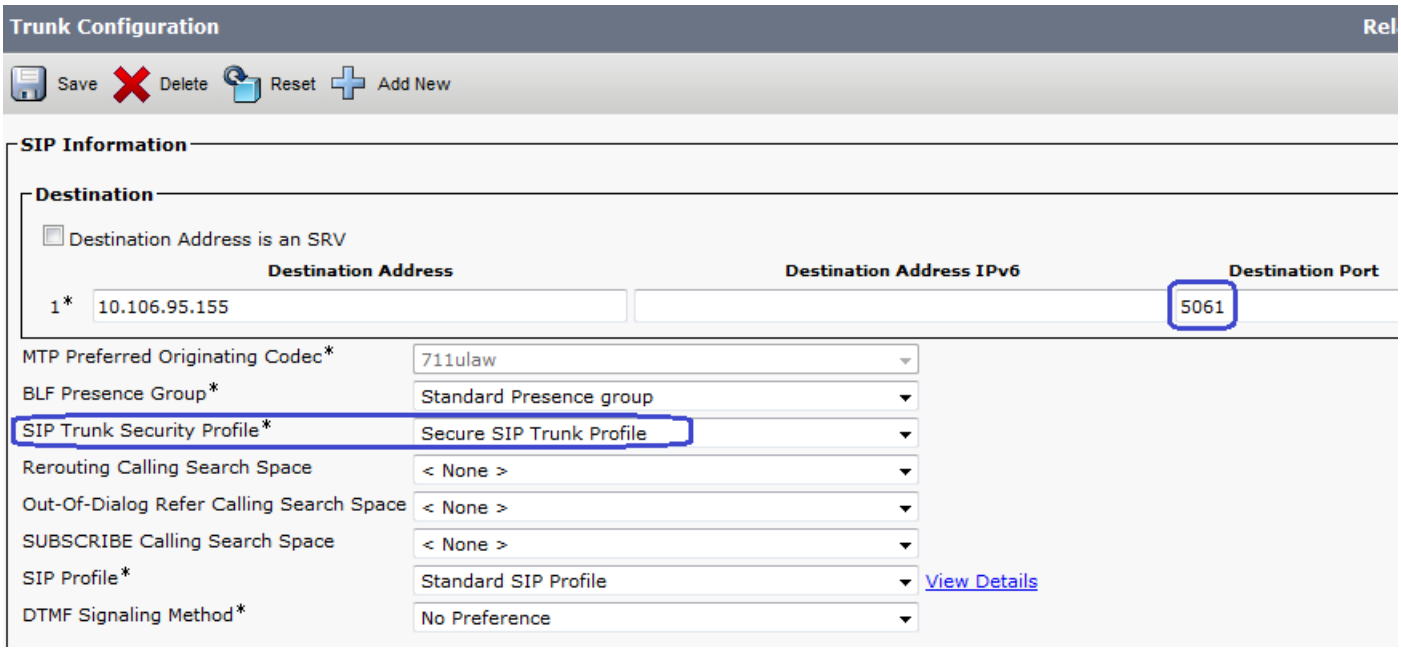


3. CUBEへのSIPトランクを作成します

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。



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。



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

チャされます。

```
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
```