

CUCM-CUBE/CUBE-SBC 間の設定 SIP TLS

目次

[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のステップ](#)

[確認](#)

[トラブルシューティング](#)

[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

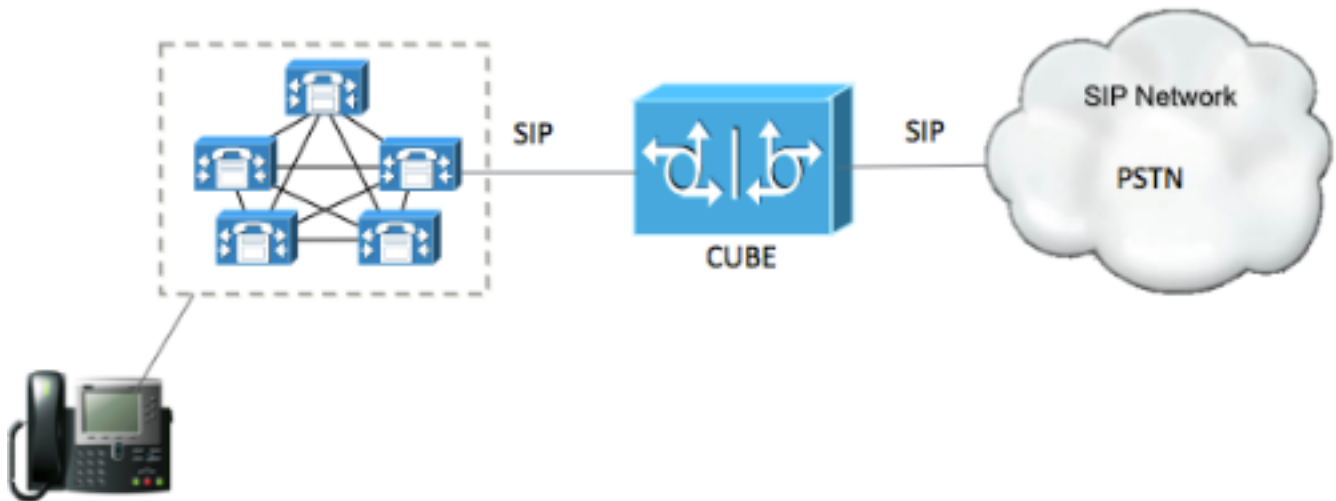
- 日時はエンドポイント (同じ NTP 出典があることを推奨します) で一致する必要があります。
- CUCM はミックス モードにある必要があります。
- TCP 接続が必要となります (あらゆる中継ファイアウォールの開港 5061) 。
- CUBE はインストールされるセキュリティおよび UCK9 ライセンスがなければなりません。

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 certificates 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
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLz/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAYBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPOwHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLz/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAYBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPOwHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

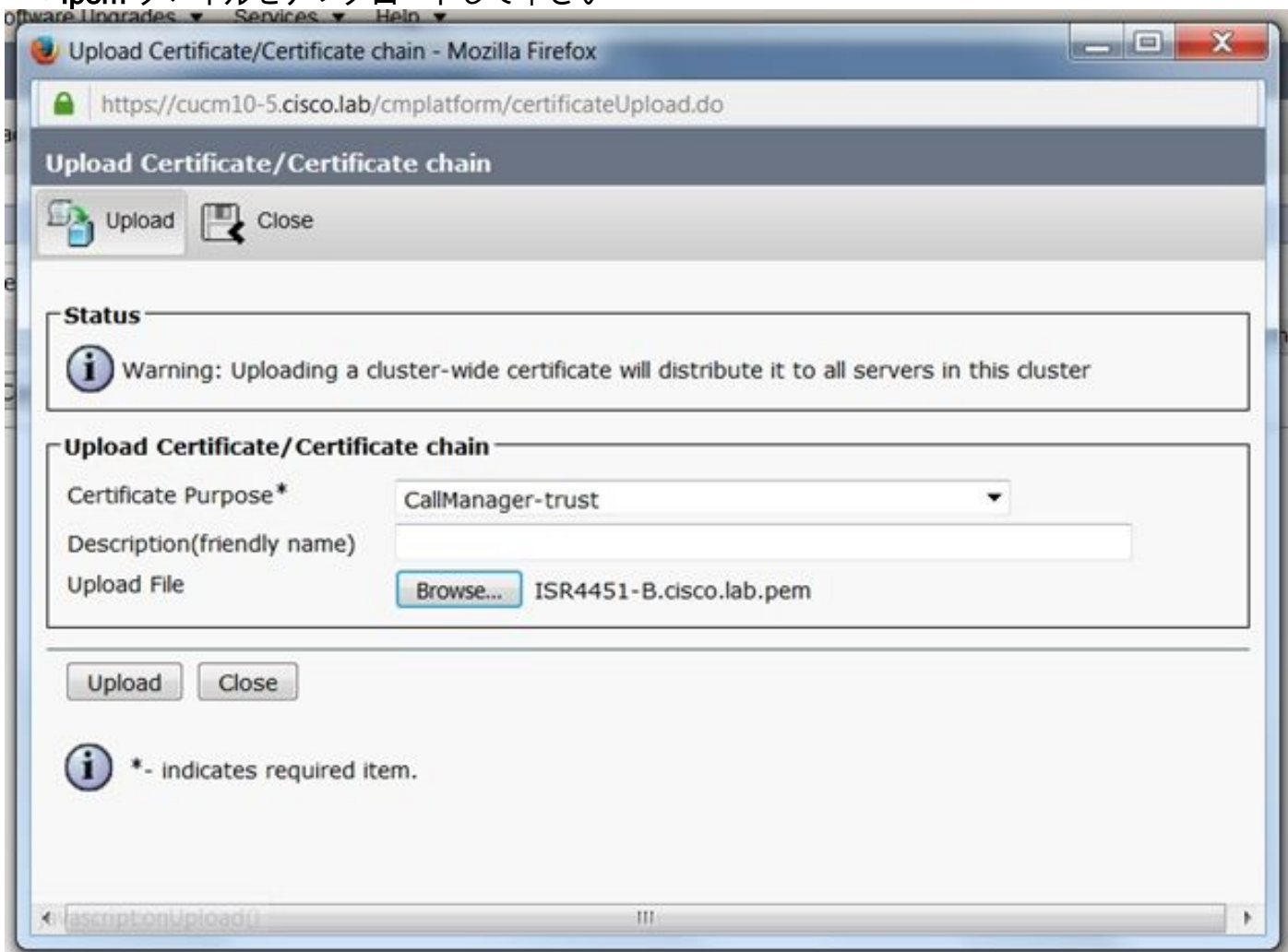
上で生成された自己署名入り認証をコピーし、ファイル拡張子 .pem を用いるテキストファイルに貼り付けて下さい

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

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | [Home](#) | [Search Documentation](#) | [About](#) | [Logout](#)

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

[Generate Self-signed](#) [Upload Certificate/Certificate chain](#) [Generate CSR](#)

Status
10 records found

Certificate List (1 - 10 of 10) Rows per Page: 10

Find Certificate List where: Certificate begins with CallManager Find Clear Filter

Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM1052	Self-signed	RSA	CUCM1052	CUCM1052	07/20/2021	Self-signed certificate generated by system

Certificate Details(Self-signed)

https://10.201.196.162/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManager.pem

Certificate Details for CUCM1052, 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: 4A7B503A9A3D202AD7D54B1F874B7DF7
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
Validity From: Thu Jul 21 13:11:22 CDT 2016
To: Tue Jul 20 13:11:21 CDT 2021
Subject Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100b803883f1177dcd68431efc16d7fdb127db637091d1d8e7b5
8d913a1689d2a289ea74fc1b42b5a571bc0abc1310e63b8924a84a3e7dc03e5001ac
4fb551b9f1569d44c1f336d5a1c2a80cbf65ebc93e2bb1619ca3d1c77984aeed1a752
3c433611d85f619725c8d116a5ab399765ed0851cdd73336244a7d214091f7a92be
38d07ae913dee31954028c16a6b020737890fc3f63653da9ca6bbafbd59f3c3b77292
89d50f14b7d8d4ae303069072917f6491ba1083584cae22122bd6ed524da1598353
]
```

[Regenerate](#) [Generate CSR](#) [Download .PEM File](#) [Download .DER File](#)

[Close](#)

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

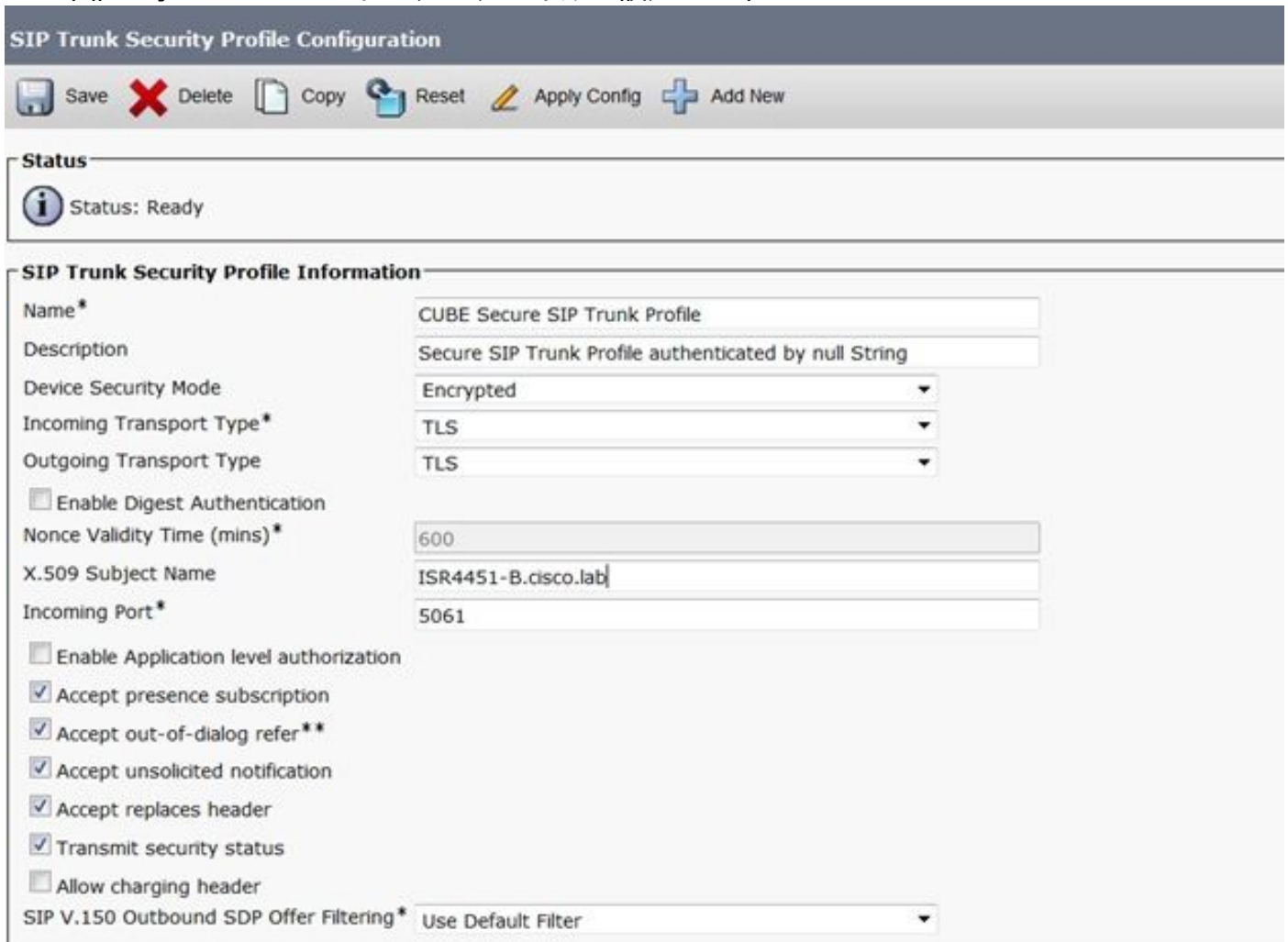
```
session transport tcp tls
```

```
voice-class sip options-keepalive
```

```
srtplib
```

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



SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

SIP Trunk Security Profile Information

Name* CUBE 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 ISR4451-B.cisco.lab

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

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

い

- (ステップで選択するために9) 作成された正しい一ポートランクセキュリティプロファイルを確認して下さい

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.201.160.12		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

- 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だ

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

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
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>