

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](#)

[設定手順](#)

[確認](#)

[トラブルシューティング](#)

[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

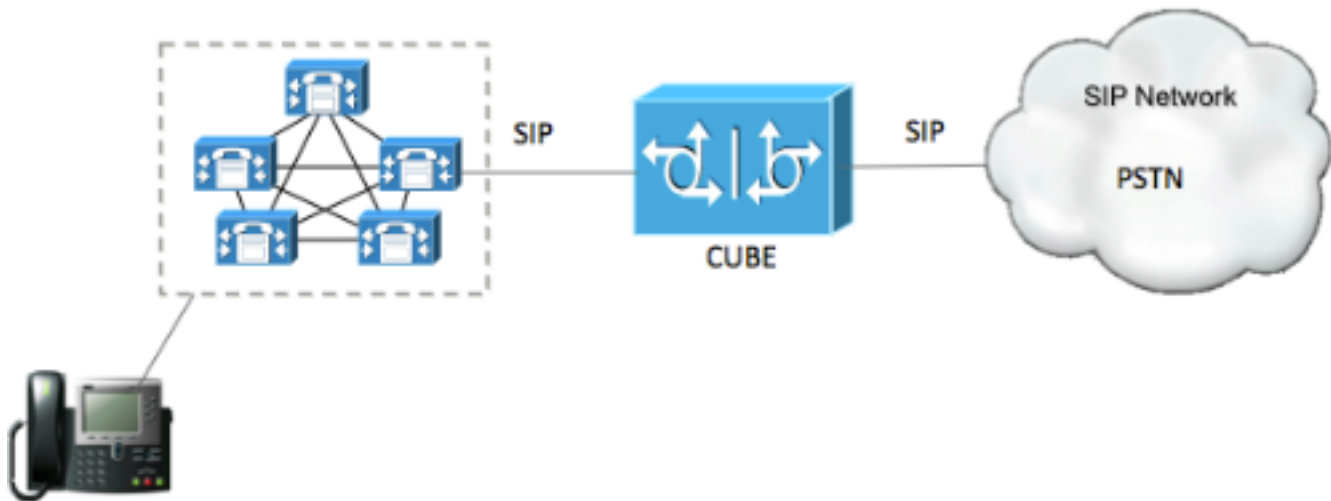
- 日付と時刻はエンドポイントで一致する必要があります (同じNTPソースを使用することをお勧めします)。
- CUCMは混合モードである必要があります。
- TCP接続が必要です (任意のランジットファイアウォールのオープンポート5061)。
- CUBEには、セキュリティおよびUCK9ライセンスがインストールされている必要があります。

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) をエ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
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

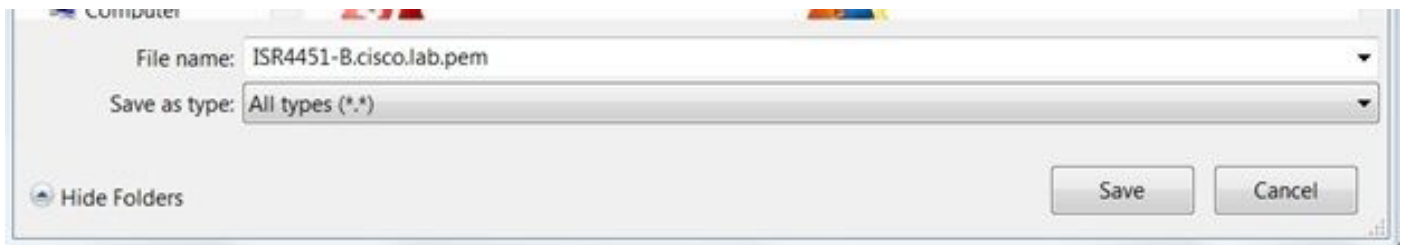
-----BEGIN CERTIFICATE-----

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

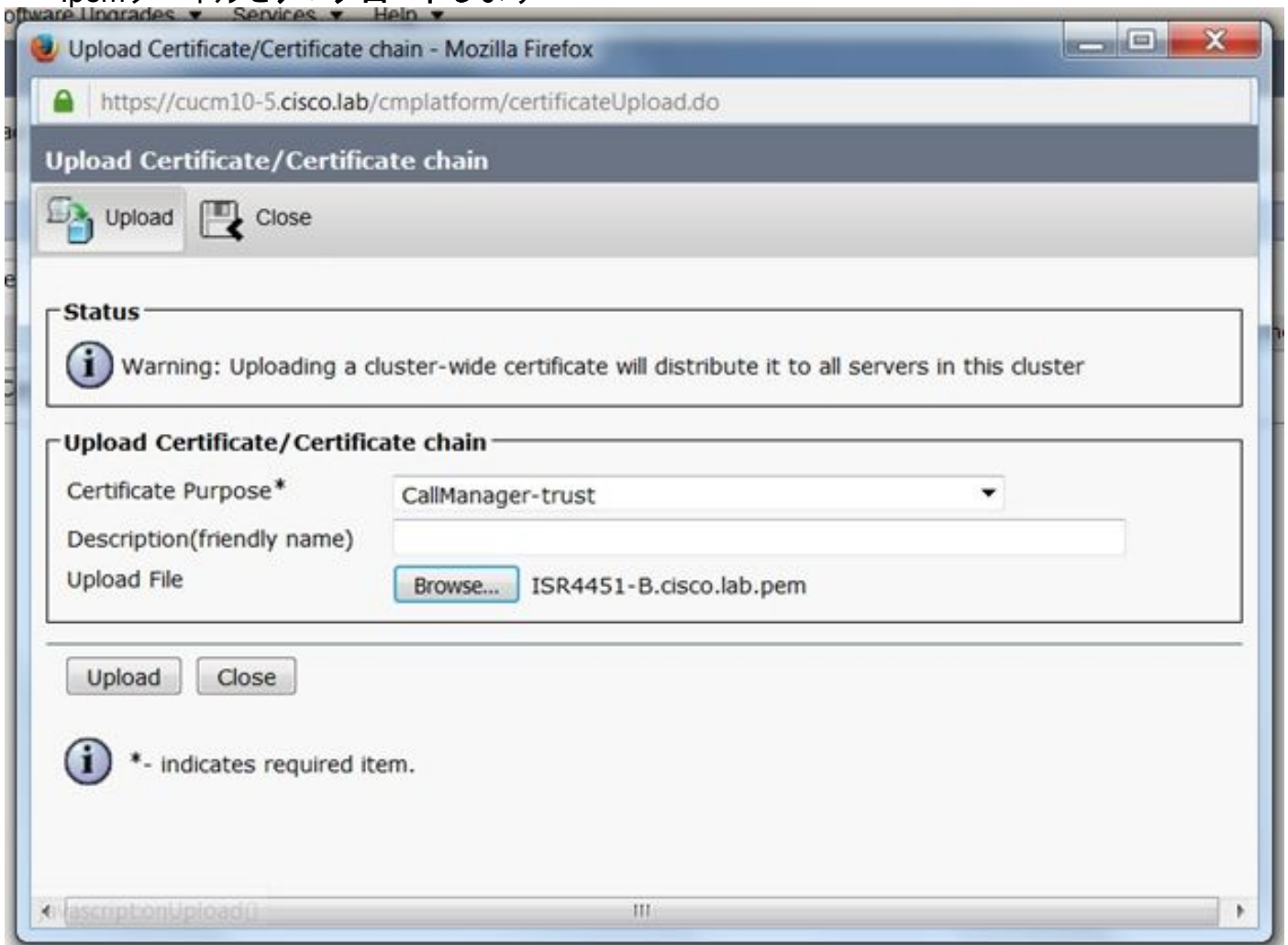
上記で生成された自己署名証明書をコピーし、ファイル拡張子.pemのテキストファイルに貼り付けます

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

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: 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
```

```
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

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
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	ISR4451-B.cisco.lab
Incoming Port*	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*	Use Default Filter

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

認します

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

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			G711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

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
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>