

Configure SIP TLS between CUCM-CUBE/CUBE-SBC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configuration steps](#)

[Verify](#)

[Troubleshoot](#)

[Table Of Contents](#)

Introduction

This document helps configure SIP Transport Layer Security (TLS) between Cisco Unified Communication Manager (CUCM) and Cisco Unified Border Element (CUBE)

Prerequisites

Cisco recommends to have knowledge of these subjects

- SIP protocol
- Security Certificates

Requirements

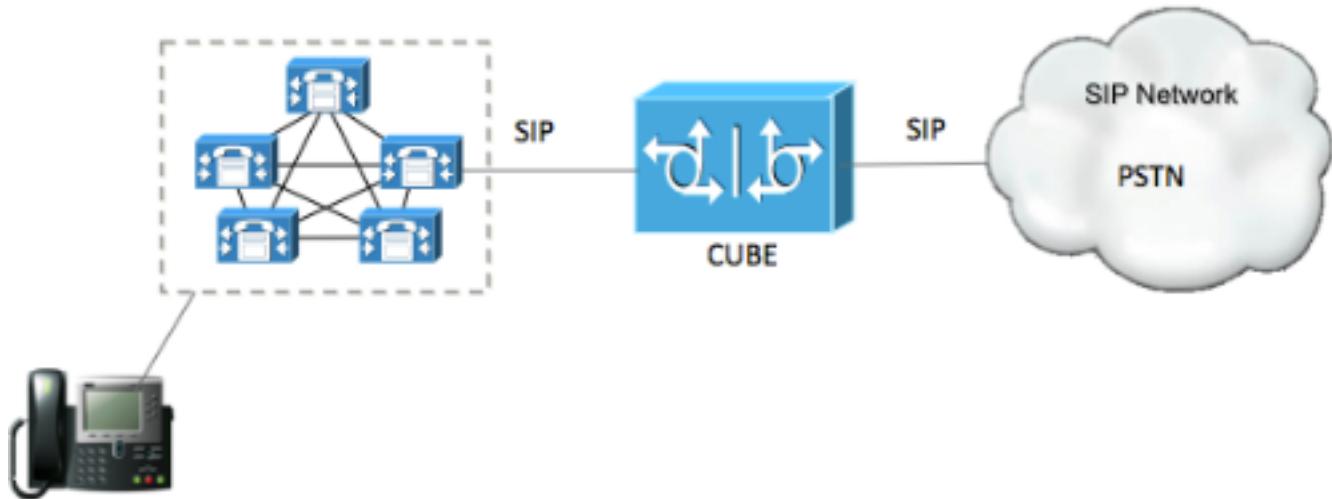
- Date and time must match on the endpoints (it is recommended to have the same NTP source).
- CUCM must be in mixed mode.
- TCP connectivity is required (Open port 5061 on any transit firewall).
- The CUBE must have the security and UCK9 licenses installed.

Components Used

- SIP
- Selfsigned certificates

Configure

Network Diagram



Configuration steps

Step 1. Create a trustpoint in order to hold CUBE's selfsigned certificate

```

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)

```

Step 2. Once the trust point is created you run the command **Crypto pki enroll CUBetest** in order to get self-signed certificates

```

crypto pki enroll CUBetest
% The fully-qualified domain name will not be included in the certificate
Generate Self Signed Router Certificate? [yes/no]: yes
If enrollment was correct you must expect the this output

```

Router Self Signed Certificate successfully created

Step 3. After your obtain certificate , you need to export it

```

crypto pki export CUBetest pem terminal
The above command must generate the below certificate

```

% Self-signed CA certificate:

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

```
MIIBgDCCASggAwIBAgIBATANBgkqhkiG9w0BAQUFADeMRwwGgYDVQQDEXNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIB3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDX07WXK3SETCj6MA0GCSqGSIB3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFpIhdVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

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

```
MIIBgDCCASggAwIBAgIBATANBgkqhkiG9w0BAQUFADeMRwwGgYDVQQDEXNJU1I0
NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIB3DQEBAQUA
A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM
tVKinW/q6yDX07WXK3SETCj6MA0GCSqGSIB3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFpIhdVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

Copy the above generated Self signed certificate and paste it to a text file with file extension **.pem**

Example below is named as ISR4451-B.ciscolab.pem



Step 4. Upload the CUBE certificate to the CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- Certificate Purpose = CallManager-Trust
- Upload your .pem file

Status

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File ISR4451-B.cisco.lab.pem

i *- Indicates required item.

Step 5. Download the Call manager self-signed certificate

- Find the certificate that says Callmanager
- Click on the host name
- Click on download PEM file
- Save it to your computer

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiry	Description
CUCM1052	CUCM1052	Self-signed	RSA	CUCM1052	CUCM1052	07/29/2023	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

i 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)
Key value:
3082010a0282010100b803883f1177dc68431efc16d7fdb127db637091d1d8e7b5
8d913a1689d2a289ea74fc1b42b5a571bc0abc1310e63b8924a84a3e7dc03e5001ac
4fb551b9f1569d44c1f336d5a1c2a80cbf65ebc93e2bb1619ca3d1c77984aeed1a752
3c433611d85f619725c8d116a5ab399765ed0851ddd73336244a7d214091f7a92be
38d07ae913dee31954028c16a6b020737890fc3f63653da9ca6bbafbd59f3c3b77292
89d50f14b7d8d4ae303069072917f6491ba1083584cae22122bd6ed524da1598353 ]
```

Regenerate Generate CSR Download .PEM File Download .DER File

Close

Step 6. Upload the Callmanager.pem certificate to CUBE

- Open the Callmanager.pem with a text file editor
- Copy the whole content of the file
- Run the this commands on the CUBE

```
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
```

Step 7. Configure SIP to use CUBE's selfsigned Certificate trustpoint

```
sip-ua
```

```
crypto signaling default trustpoint CUBEtest
```

Step 8. Configure the dial peers with TLS

```
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  
srtp
```

Step 9. Configure a CUCM SIP trunk security profile

- CUCM Admin page > System > Security > SIP Trunk Security Profile
- Configure the profile as shown below

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

Note: It is critically important that the X.509 field matches the CN name you configured previously while you were generating the self-signed certificate

Step 10. Configure a SIP trunk on CUCM

- Ensure the SRTP allowed check box is checked
- Configure the proper destination address and Ensure to replace port 5060 with port 5061
- Ensure to select the correct Sip Trunk Security profile (which was created in Step 9)

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

- Save and reset the trunk.

Verify

Since you enabled OPTIONS PING on the CUCM, SIP trunk must be in FULL SERVICE state

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

The SIP trunk status show full service.

The dial peer status show as follow:

```
show dial-peer voice summary

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
```

Troubleshoot

Enable and collect the output of these debugs

```
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 link:

<https://goo.gl/QOS1iT>