

Configurare SIP TLS tra CUCM-CUBE/CUBE-SBC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Fasi della configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Sommario

Introduzione

Questo documento aiuta a configurare SIP Transport Layer Security (TLS) tra Cisco Unified Communications Manager (CUCM) e Cisco Unified Border Element (CUBE)

Prerequisiti

Cisco raccomanda la conoscenza di questi argomenti

- protocollo SIP
- Certificati di protezione

Requisiti

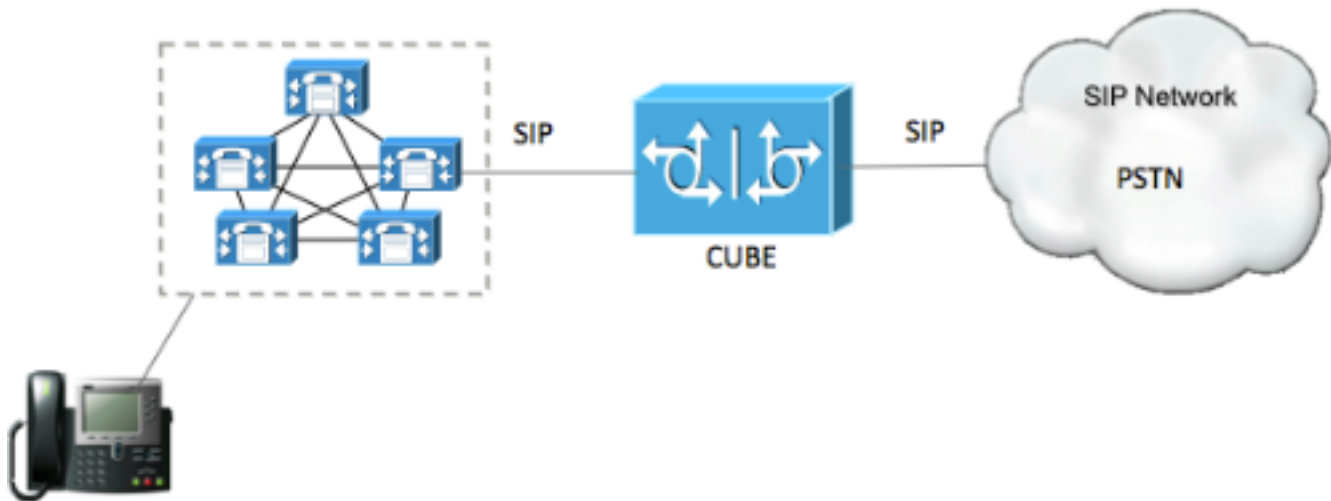
- La data e l'ora devono corrispondere sugli endpoint (si consiglia di avere la stessa origine NTP).
- CUCM deve essere in modalità mista.
- È necessaria la connettività TCP (aprire la porta 5061 su qualsiasi firewall di transito).
- Nel CUBE devono essere installate le licenze Security e UCK9.

Componenti usati

- SIP
- Certificati autofirmati

Configurazione

Esempio di rete



Fasi della configurazione

Passaggio 1. Creare un trust point per contenere il certificato autofirmato del CUBE

```
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)
```

Passaggio 2. Dopo aver creato il trust point, eseguire il comando **Crypto pki enroll CUBEtest** per ottenere i certificati autofirmati

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

Se la registrazione è corretta, è necessario attendersi l'output

```
Router Self Signed Certificate successfully created
```

Passaggio 3. Dopo aver ottenuto il certificato, è necessario esportarlo

```
crypto pki export CUBEtest pem terminal
```

Il comando precedente deve generare il certificato seguente

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTEwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

% General Purpose Certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTEwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sJMj919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFppIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

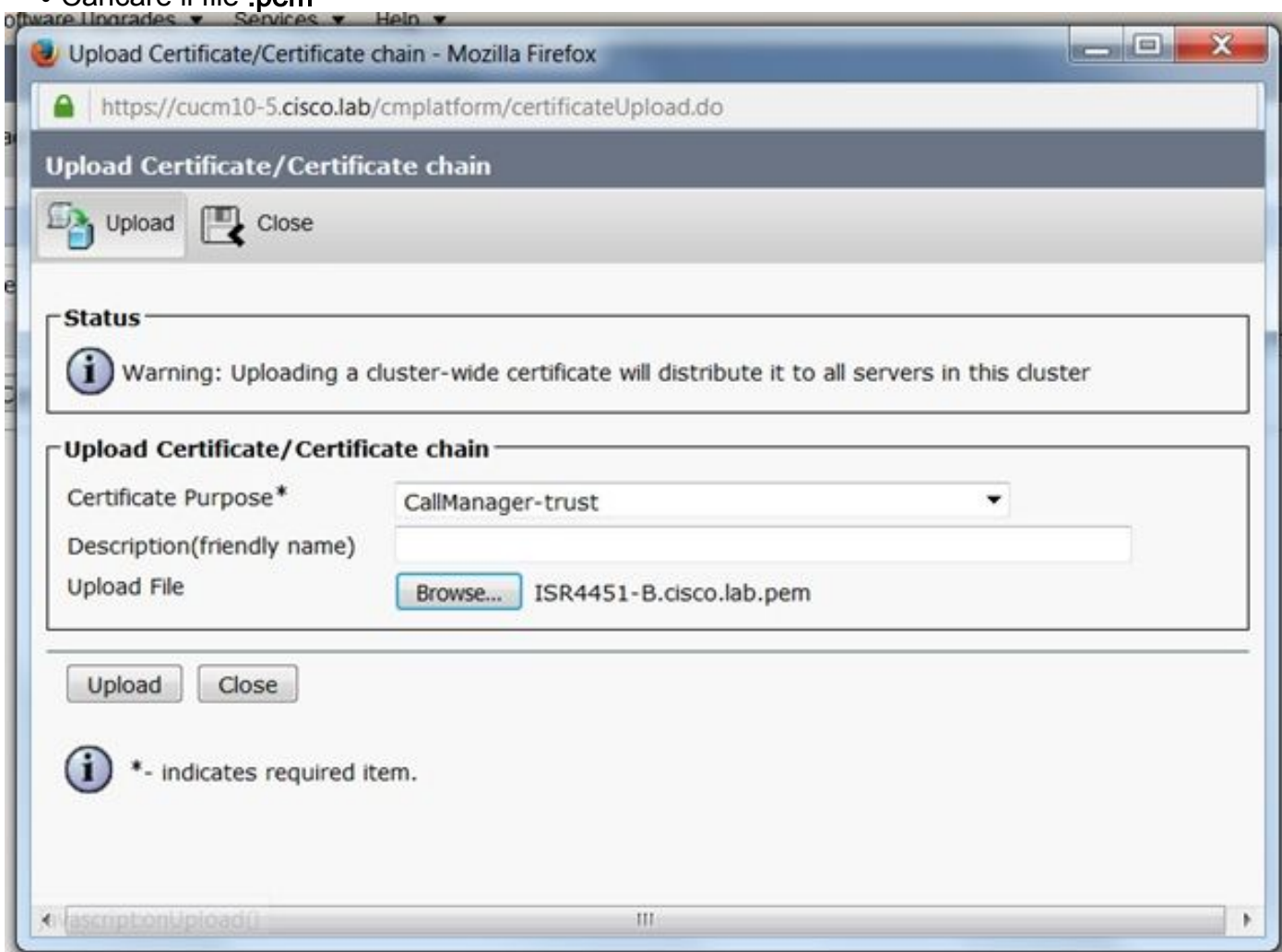
Copiare il certificato autofirmato generato sopra e incollarlo in un file di testo con estensione .pem

L'esempio seguente è denominato ISR4451-B.ciscolab.pem



Passaggio 4. Caricare il certificato CUBE in CUCM

- Amministratore sistema operativo CUCM > Sicurezza > Gestione certificati > Carica catena certificati/certificati
- Scopo certificato = CallManager-Trust
- Caricare il file .pem



Passaggio 5. Scaricare il certificato autofirmato del gestore delle chiamate

- Trova il certificato con la dicitura Callmanager
- Fare clic sul nome dell'host
- Fare clic su Download file PEM
- Salvarlo sul computer

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

Passaggio 6. Caricare il certificato Callmanager.pem in CUBE

- Aprire Callmanager.pem con un editor di file di testo
- Copiare l'intero contenuto del file
- Eseguire i comandi this sul CUBO

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

Passaggio 7. Configurare il SIP per l'utilizzo del punto di attendibilità dei certificati firmato dal CUBE

```
sip-ua
```

```
crypto signaling default trustpoint CUBEtest
```

Passaggio 8. Configurare i peer di composizione con 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
```

```
srtplib
```

Passaggio 9. Configurare un profilo di sicurezza trunk SIP CUCM

- Pagina Amministratore CUCM > Sistema > Sicurezza > Profilo sicurezza trunk SIP
- Configurare il profilo come illustrato di seguito

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

Nota: È di fondamentale importanza che il campo X.509 corrisponda al nome CN configurato in precedenza durante la generazione del certificato autofirmato

Passaggio 10. Configurazione di un trunk SIP su CUCM

- Assicurarsi che la casella di controllo SRTP consentito sia selezionata
- Configurare l'indirizzo di destinazione corretto e assicurarsi di sostituire la porta 5060 con la

porta 5061

- Assicurarsi di selezionare il profilo di sicurezza trunk SIP corretto (creato nel passaggio 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

- Salvare e ripristinare il trunk.

Verifica

Poiché è stato abilitato il comando OPTIONS PING sul CUCM, il trunk SIP deve essere in stato FULL SERVICE

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

Lo stato del trunk SIP mostra il servizio completo.

Lo stato del dial peer viene visualizzato come segue:

```
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

Risoluzione dei problemi

Abilita e raccoglie l'output di questi debug

```
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 ccsp verbose
```


Collegamento registrazione Webex:

<https://goo.gl/QOS1iT>