

Configurazione di TLS SIP tra CUCM-CUBE/CUBE-SBC con certificati firmati da CA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Verifica](#)

—
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare SIP Transport Layer Security (TLS) tra Cisco Unified Communications Manager (CUCM) e Cisco Unified Border Element (CUBE) con certificati firmati da CA (Certification Authority).

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 Unified Communications K9 (UCK9).

Nota: Per Cisco IOS-XE versione 16.10, la piattaforma è passata alle licenze intelligenti.

Componenti usati

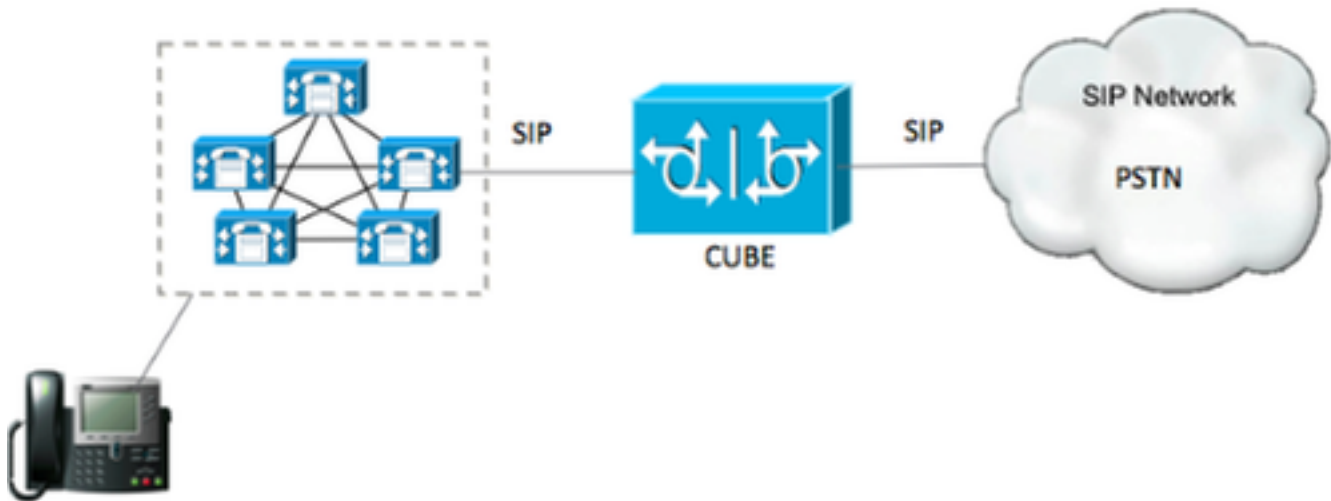
- SIP
- Certificati firmati da Autorità di certificazione
- Cisco IOS e IOS-XE Gateway Versioni 2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X:

15,4+

- Cisco Unified Communications Manager (CUCM)Versioni: 10,5+

Configurazione

Esempio di rete



Configurazione

Passaggio 1. Si sta per creare una chiave RSA corrispondente alla lunghezza del certificato del certificato radice utilizzando il comando:

```
Crypto key generate rsa label TestRSAkey exportable modulus 2048
```

Questo comando crea una chiave RSA con una lunghezza di 2048 bit (il massimo è 4096).

Passaggio 2. Creare un trust point per il certificato firmato dall'autorità di certificazione utilizzando i comandi seguenti:

```
Crypto pki trustpoint CUBE_CA_CERT
  serial-number none
  fqdn none
  ip-address none
  subject-name cn=ISR4451-B.cisco.lab !(this has to match the router's hostname
[hostname.domain.name])
  revocation-check none
  rsakeypair TestRSAkey !(this has to match the RSA key you just created)
```

Passaggio 3. Ora che si dispone del punto di fiducia, è possibile generare la richiesta CSR con i comandi seguenti:

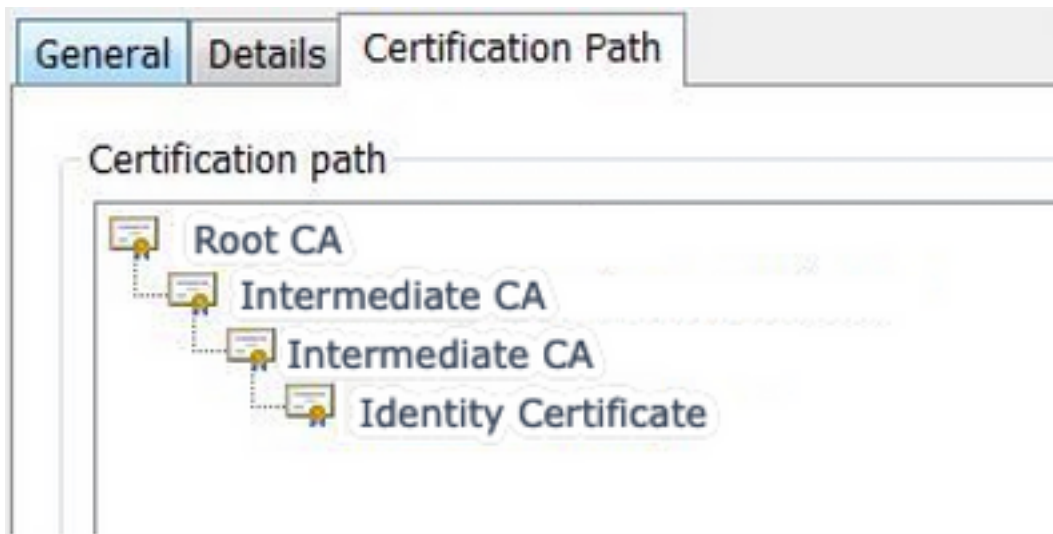
```
Crypto pki enroll CUBE_CA_CERT
```

Rispondere alle domande visualizzate sullo schermo, quindi copiare la richiesta CSR, salvarla in un file e inviarla alla CA.

Passaggio 4. È necessario verificare se la catena di certificati radice dispone di certificati

intermedi. in assenza di autorità di certificazione intermedie, passare al passaggio 7, altrimenti continuare con il passaggio 6.

Passaggio 5. Creare un trust point per contenere il certificato radice, nonché un trust point per contenere qualsiasi CA intermedia fino a quella che firma il certificato CUBE (vedere l'immagine seguente).



In questo esempio, il 1° livello è la CA radice, il 2° livello è la prima CA intermedia, il 3° livello è la CA che firma il nostro certificato CUBE, quindi è necessario creare un trust point per contenere i primi 2 certificati con questi comandi.

```
Crypto pki trustpoint Root_CA_CERT  
Enrollment terminal pem  
Revocation-check none
```

```
Crypto pki authenticate Root_CA_CERT  
Paste the X.64 based certificate here
```

```
Crypto pki trustpoint Intermediate_CA  
Enrollment terminal  
Revocation-check none
```

```
Crypto pki authenticate Intermediate_CA
```

Passaggio 6. Dopo aver ricevuto il certificato firmato dall'autorità di certificazione, si procederà all'autenticazione del trust point, che deve essere in possesso del certificato dell'autorità di certificazione prima del certificato CUBE; il comando che consente di importare il certificato è,

```
Crypto pki authenticate CUBE_CA_CERT
```

Passaggio 7. Dopo aver installato il certificato, è necessario eseguire questo comando per importare il certificato CUBE

```
Crypto pki import CUBE_CA_CERT cert
```

Passaggio 8. Configurare SIP-UA per l'utilizzo del trust point creato

```
sip-ua
crypto signaling default trustpoint CUBE_CA_CERT
```

Passaggio 9. Configurare i peer della connessione remota come illustrato di seguito:

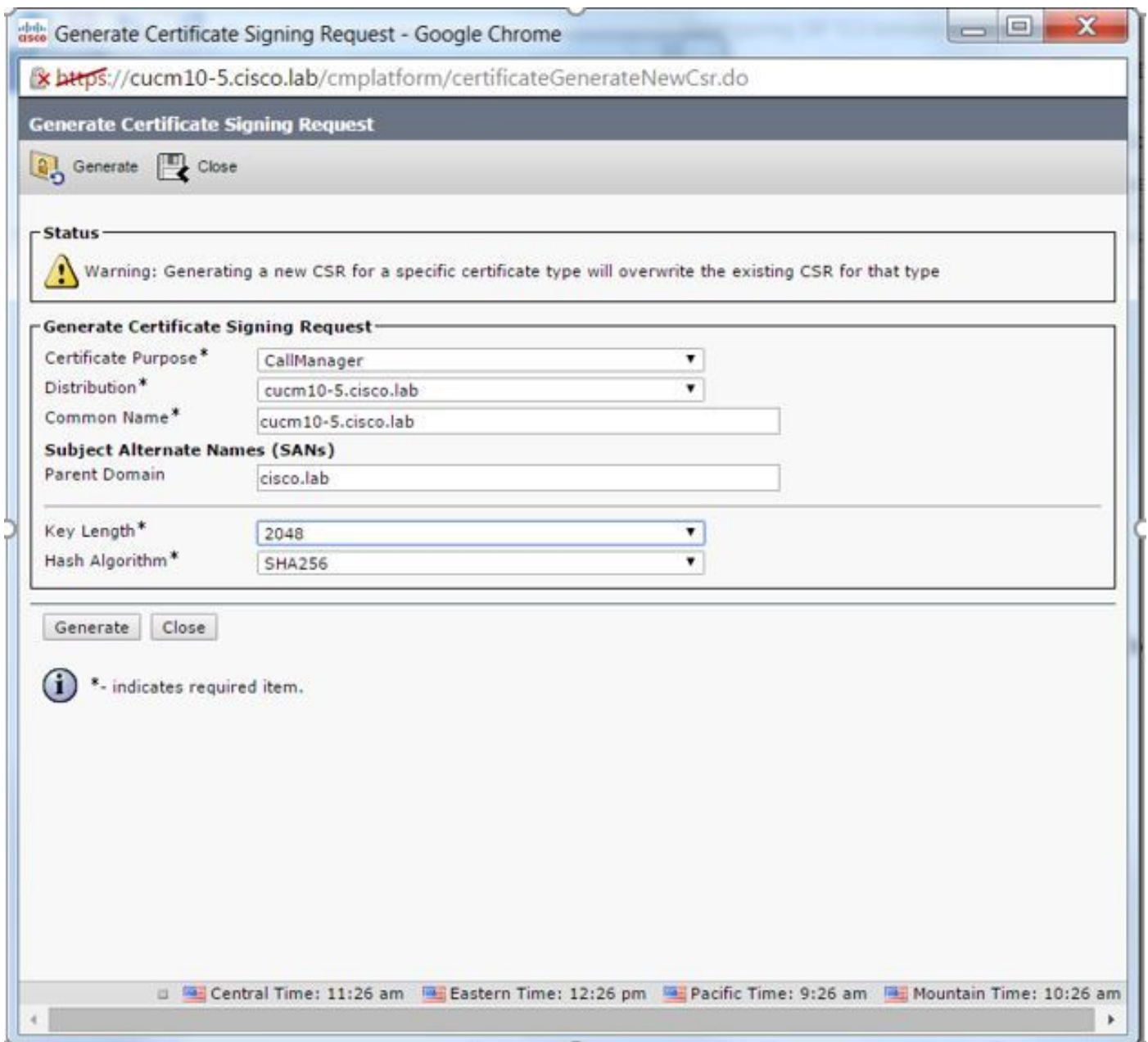
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

La configurazione CUBE è stata completata.

Passaggio 10. Ora, si sta per generare il nostro CSR CUCM, seguire le istruzioni qui sotto

- Accedere a CUCM OS administrator
- Fare clic su Security
- Fare clic su Gestione certificati.
- Fare clic su Genera CSR

La richiesta CSR deve essere simile a quella riportata di seguito:



Passaggio 11. Scaricare il CSR e inviarlo alla CA.

Passaggio 12. Caricare la catena di certificati firmata dall'autorità di certificazione nel CUCM. I passaggi sono:

- Fare clic su protezione e quindi su gestione certificati.
- Fare clic su Carica catena certificati/certificati.
- Nel menu a discesa Scopo certificato selezionare Gestione chiamate.
- Individuare il file.
- Fare clic su upload.

Passaggio 13. Accedere alla CLI di CUCM ed eseguire questo comando

```
utils ctl update CTLFile
```


Passaggio 14. Configurare un profilo di sicurezza trunk SIP CUCM

- Fare clic su sistema, quindi su protezione e infine su profilo di protezione trunk
- Configurare il profilo come mostrato nell'immagine,

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

Status

 Status: Ready

SIP Trunk Security Profile Information

Name*	<input type="text" value="CUBE_CA Secure SIP Trunk Profile"/>
Description	<input type="text" value="Secure SIP Trunk Profile authenticated by null String"/>
Device Security Mode	<input type="text" value="Encrypted"/>
Incoming Transport Type*	<input type="text" value="TLS"/>
Outgoing Transport Type	<input type="text" value="TLS"/>
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	<input type="text" value="600"/>
X.509 Subject Name	<input type="text" value="cucm10-5.cisco.lab"/>
Incoming Port*	<input type="text" value="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*	<input type="text" value="Use Default Filter"/>

Nota: in questo caso, il nome soggetto X.509 deve corrispondere al nome soggetto del certificato CUCM, come mostrato nella parte evidenziata dell'immagine.

Certificate Details for cucm10-5.cisco.lab, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

Status

Status: Ready

Certificate Settings

Locally Uploaded	10/02/16
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by AD-CONTROLLER-CA

Certificate File Data

```
[
Version: V3
Serial Number: 1D255E0000000000000007
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: CN=AD-CONTROLLER-CA, DC=cisco, DC=lab
Validity From: Wed Feb 10 10:45:23 CST 2016
To: Fri Feb 10 10:55:23 CST 2017
Subject Name: CN=cucm10-5.cisco.lab, OU=TAC, O=CISCO, L=RICHARSON, ST=TEXAS, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100ae8db062881c35163f1b6ee4be4951158fdb3495d3c8032170c9fb8bafb385a2
27b00ec1024807f0adc49df875189779c7de1ae1e7e64b45e6f9917fa6ca5687d9aeaf20d70018e8d5
58a832360b82702249fc98855012c7d2cc29eea0f92fad9e739d73b0fa24d7dd4bd9fc96be775fda997
f03a440645ad64fa9f083ed95445e200187dd8775aa543b2bab11a5e223e23ef03bb86bb9fd969b3d9
3ba2550c35ea06ed5149aef2253c2455a622122e0aa3b649a090911995069a2cfd4ab4ab1fe15b242
]
```

Passaggio 15. Configurare un trunk SIP come se si trattasse di un trunk SIP

- 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.
- Nel profilo SIP trunk security, selezionare il nome del profilo SIP creato nel passaggio 14.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* [redacted]		5061

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

Verifica

A questo punto, se tutta la configurazione è OK,

Su CUCM, lo stato del trunk SIP mostra Full Service, come mostrato nell'immagine,

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

In CUBE il dial peer mostra questo stato:

```
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
```

Lo stesso processo si applica ad altri router, l'unica differenza è che invece di caricare il certificato CUCM, caricare il certificato fornito da terze parti.

Risoluzione dei problemi

Abilita debug su CUBE

```
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
```