

Configuración de SIP TLS entre CUCM-CUBE/CUBE-SBC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuration Steps](#)

[Verificación](#)

[Troubleshoot](#)

Table Of Contents

Introducción

Este documento ayuda a configurar SIP Transport Layer Security (TLS) entre Cisco Unified Communication Manager (CUCM) y Cisco Unified Border Element (CUBE)

Prerequisites

Cisco recomienda tener conocimiento de estos temas

- Protocolo SIP
- Certificados de seguridad

Requirements

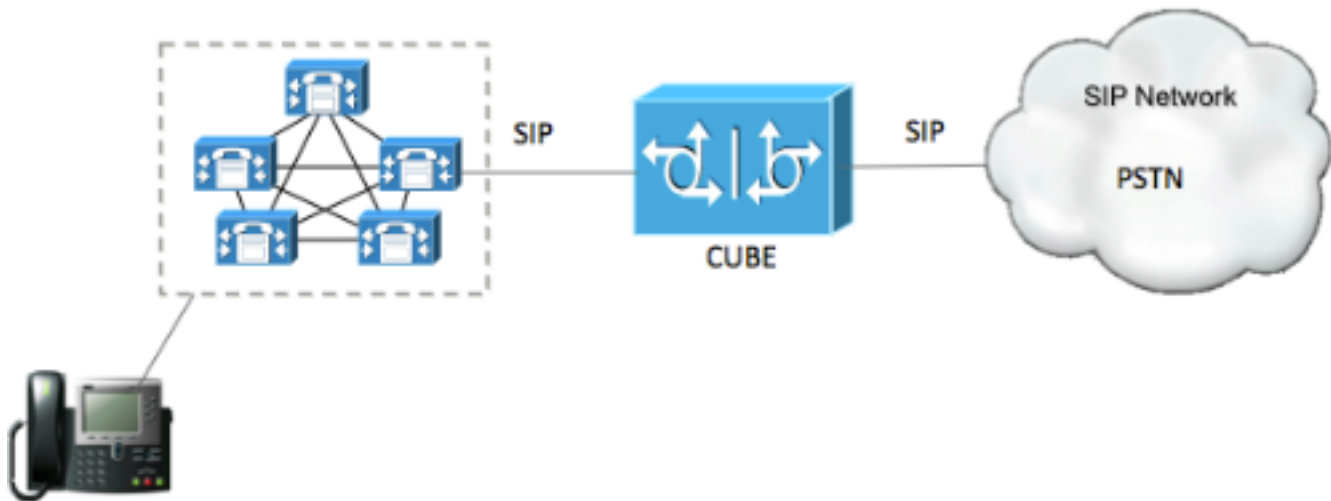
- La fecha y la hora deben coincidir en los puntos finales (se recomienda tener el mismo origen NTP).
- CUCM debe estar en modo mixto.
- Se requiere conectividad TCP (puerto abierto 5061 en cualquier firewall de tránsito).
- El CUBE debe tener instalada la seguridad y las licencias UCK9.

Componentes Utilizados

- SIP
- Certificados autofirmados

Configurar

Diagrama de la red



Configuration Steps

Paso 1. Cree un punto de confianza para conservar el certificado autofirmado de 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)
```

Paso 2. Una vez creado el punto de confianza, ejecuta el comando **Crypto pki enroll CUBEtest** para obtener certificados autofirmados

```
crypto pki enroll CUBEtest

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

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

Si la inscripción fue correcta, debe esperar este resultado

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

Paso 3. Después de obtener el certificado , debe exportarlo

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

El comando anterior debe generar el siguiente certificado

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
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
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngsl+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix
7Fa6DG33LmEYUmlNntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

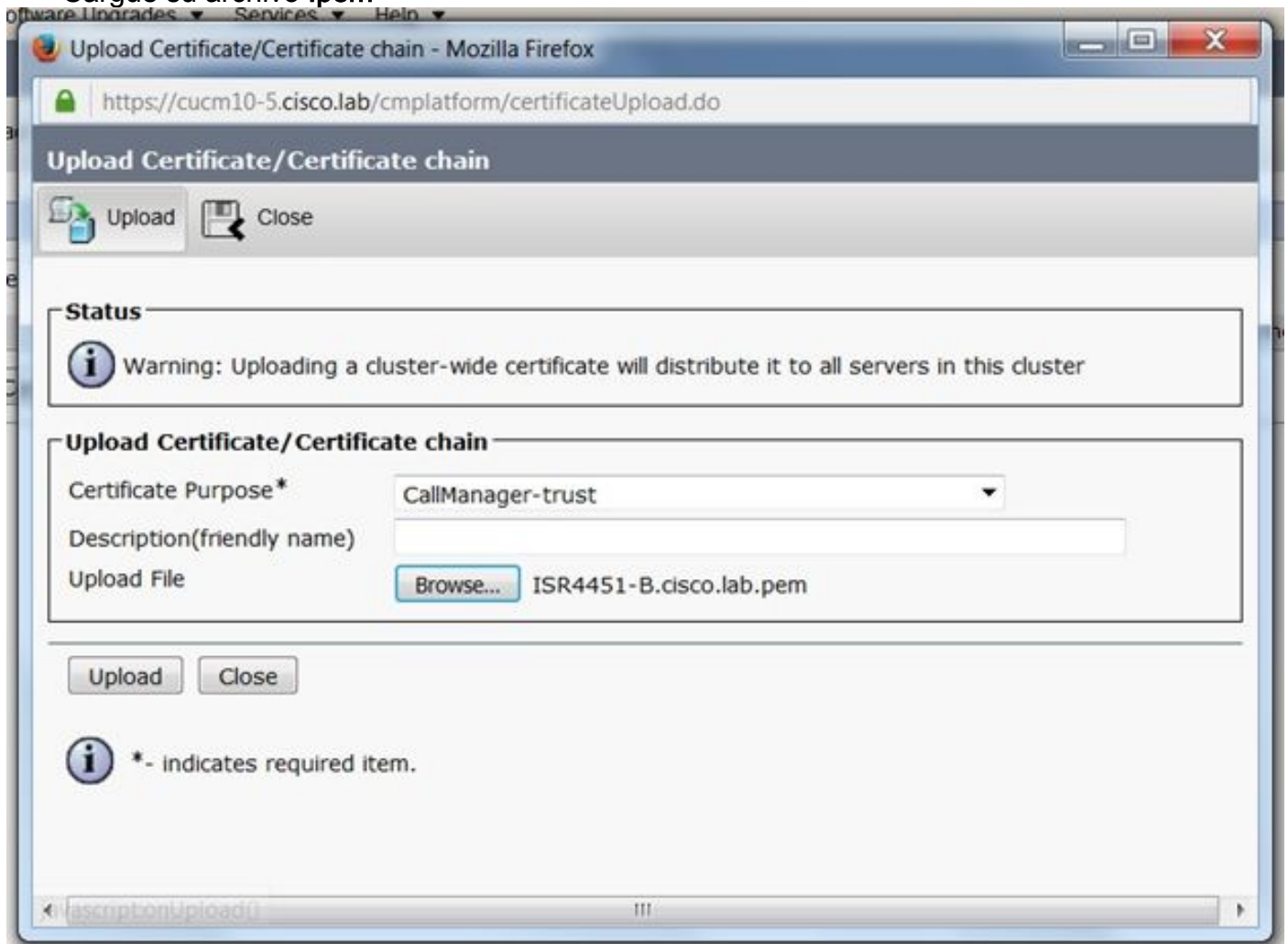
Copie el certificado autofirmado generado anteriormente y péguelo en un archivo de texto con extensión de archivo **.pem**

El siguiente ejemplo se denomina **ISR4451-B.ciscolab.pem**



Paso 4. Cargar el certificado CUBE en CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- Objetivo del certificado = CallManager-Trust
- Cargue su archivo .pem



Paso 5. Descargue el certificado autofirmado del Call Manager

- Busque el certificado que indica Callmanager
- Haga clic en el nombre de host
- Haga clic en Descargar archivo PEM
- Guárdelo en el ordenador

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | CUCM

Home | 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

Paso 6. Cargue el certificado Callmanager.pem en CUBE

- Abra Callmanager.pem con un editor de archivos de texto
- Copiar todo el contenido del archivo
- Ejecute estos comandos en el 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
```

Paso 7. Configuración de SIP para utilizar el punto de confianza de certificados autofirmado de CUBE

```
sip-ua
```

```
crypto signaling default trustpoint CUBEtest
```

Paso 8. Configure los pares de marcado 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
```

Paso 9. Configuración de un perfil de seguridad troncal SIP de CUCM

- Página de administración de CUCM > System > Security > SIP Trunk Security Profile
- Configure el perfil como se muestra a continuación

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: Es de vital importancia que el campo X.509 coincida con el nombre CN que configuró anteriormente mientras generaba el certificado autofirmado

Paso 10. Configuración de un tronco SIP en CUCM

- Asegúrese de que la casilla de verificación SRTP allowed esté marcada
- Configure la dirección de destino adecuada y asegúrese de reemplazar el puerto 5060 por el

puerto 5061

- Asegúrese de seleccionar el perfil de seguridad del enlace troncal Sip correcto (que se creó en el paso 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

- Guarde y restablezca el tronco.

Verificación

Puesto que ha activado OPTIONS PING en CUCM, el troncal SIP debe estar en estado DE SERVICIO COMPLETO

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

El estado del troncal SIP muestra el servicio completo.

El estado del par de marcado muestra lo siguiente:

```
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

Troubleshoot

Habilitar y recopilar el resultado de estas depuraciones

```
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
```


Enlace de grabación de Webex:

<https://goo.gl/QOS1iT>