

SORBO TLS de la configuración entre CUCM-CUBE/CUBE-SBC

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Pasos para la configuración](#)

[Verificación](#)

[Troubleshooting](#)

Contenidos

Introducción

Este documento ayuda al SORBO Transport Layer Security (TLS) de la configuración entre Cisco unificó el administrador de la comunicación (CUCM) y el Cisco Unified Border Element (el CUBO)

Prerequisites

Cisco recomienda tener conocimiento de estos temas

- Protocolo del SORBO
- Certificados de la Seguridad

Requisitos

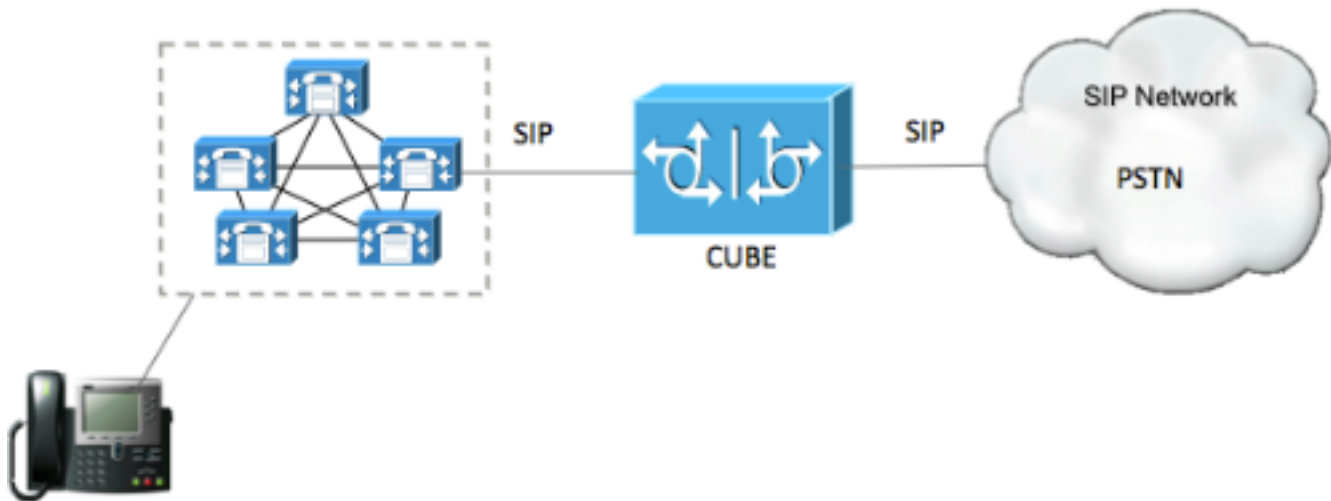
- La fecha y hora debe hacer juego en los puntos finales (se recomienda para tener la misma fuente NTP).
- CUCM debe estar en el modo mezclado.
- Se requiere la Conectividad TCP (el puerto abierto 5061 en ningunos transita el Firewall).
- El CUBO debe tener la Seguridad y las licencias UCK9 instaladas.

Componentes Utilizados

- SORBO
- Certificados de Selfsigned

Configurar

Diagrama de la red



Pasos para la configuración

Paso 1. Cree un trustpoint para sostener el certificado selfsigned del CUBO

```
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 que se crea la punta de la confianza usted funciona con el comando crypto que el pki alista CUBEtest para conseguir los certificados uno mismo-firmados

```
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 estaba correcta usted debe contar con la esta salida

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

Paso 3. Después de que su obtenga el certificado, usted necesita exportarlo

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

El comando antedicho debe generar el certificado abajo

% Self-signed CA certificate:

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

```
MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNjU1I0
NDUxLUIuY21zY28ubGF1bG4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow
HjEcmBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQDgtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/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+NS1G5sjMJ919/ix
7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB
Af8wHwYDVR0jBBGwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFpM
tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH
T88SHXq0EVqcLrgGpScwcpbR1mKFPPihDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4
LDQaxQ==
```

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

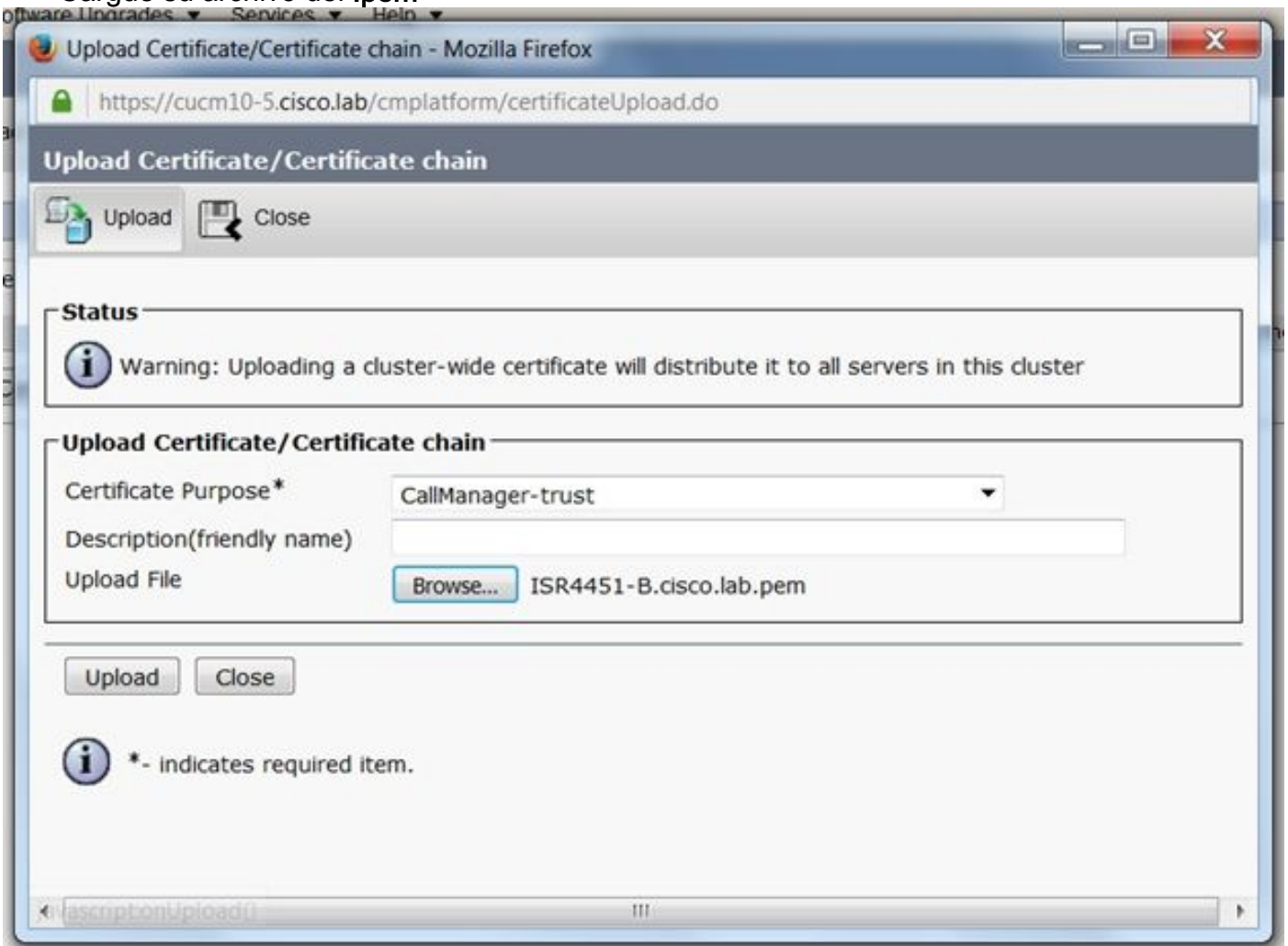
Copie el certificado firmado arriba generado del uno mismo y péguelo a un archivo de texto con el **.pem de la extensión de archivo**

El ejemplo abajo se nombra como **ISR4451-B.ciscolab.pem**



Paso 4. Cargue el certificado del CUBO al CUCM

- Certificate Management (Administración de certificados) del > Security (Seguridad) CUCM OS Admin > certificado/Cadena de certificados de la carga
- Propósito = CallManager-confianza del certificado
- Cargue su archivo del **.pem**



Paso 5. Descargue el certificado autofirmado del administrador de llamada

- Encuentre el certificado que dice Callmanager
- Haga clic en el nombre del host
- Haga clic en el archivo de la descarga PEM
- Sálvelo a su ordenador

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

Paso 6. Cargue el certificado Callmanager.pem PARA CUBICAR

- Abra el Callmanager.pem con un editor del archivo de texto
- Copie el contenido del conjunto del archivo
- Ejecute esto ordena en el 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

Paso 7. Configure el SORBO para utilizar el trustpoint selfsigned del certificado del CUBO

sip-ua

crypto signaling default trustpoint CUBEttest

Paso 8. Configure a los dial peer 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
```

```
sctp
```

Paso 9. Configure un perfil de seguridad del trunk del SORBO CUCM

- >Security (Seguridad) de la página de administración > del sistema CUCM > perfil de seguridad del trunk del SORBO
- Configure el perfil como se muestra abajo

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: Es críticamente importante que el campo X.509 hace juego el nombre CN que usted configuró previamente mientras que usted generaba el certificado autofirmado

Paso 10. Configure un trunk del SORBO en CUCM

- Asegúrese que la casilla de verificación permitida SRTP esté marcada
- Configure el direccionamiento de destino correcto y asegúrelo para substituir el puerto 5060

por el puerto 5061

- Asegure para seleccionar el perfil de seguridad correcto del trunk del sorbo (que fue creado 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

- Salve y reajuste el trunk.

Verificación

Puesto que usted las OPCIONES habilitadas HACE PING en el CUCM, el trunk del SORBO debe estar en el estado de servicio FULL

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 servicio completo de la demostración del estado del tronco del SORBO.

La demostración del estatus del dial peer como siguen:

```
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

Troubleshooting

Habilite y recoja la salida de estos 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
```


Link de la grabación del WebEx:

<https://goo.gl/QOS1iT>