

# Configurar o SORVO TLS entre CUCM-CUBE/CUBE-SBC

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapas de configuração](#)

[Verificar](#)

[Troubleshooting](#)

Sumário

## Introdução

Este documento ajuda a configurar o Transport Layer Security do SORVO (TLS) entre Cisco unificou o gerente de uma comunicação (CUCM) e o Cisco Unified Border Element (o CUBO)

### Pré-requisitos

Cisco recomenda ter o conhecimento destes assuntos

- Protocolo do SORVO
- Certificados da Segurança

### Requisitos

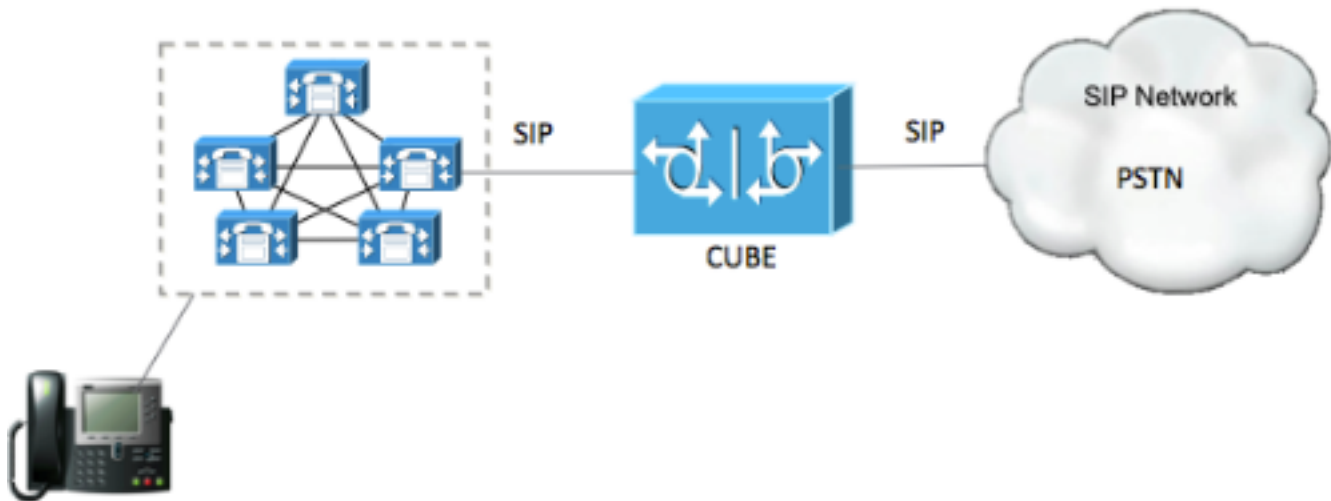
- A data e hora deve combinar nos valores-limite (se recomenda ter a mesma fonte NTP).
- CUCM deve reagir de modo misturado.
- A Conectividade TCP é exigida (porta aberta 5061 em algum Firewall do trânsito).
- O CUBO deve ter a Segurança e as licenças UCK9 instaladas.

### [Componentes Utilizados](#)

- SORVO
- Certificados de Selfsigned

## Configurar

### Diagrama de Rede



## Etapas de configuração

Etapa 1. Crie um ponto confiável a fim guardar o certificado selfsigned do 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

rsaakeypair ISR4451-B.cisco.lab !(this has to match the router's host name)
```

Etapa 2. Uma vez que o ponto da confiança é criado você executa o comando crypto que o pki registra CUBEtest a fim obter certificados auto-assinados

```
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 o registro estava correto você deve esperar esta saída

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

Etapa 3. Depois que seu obtenha o certificado, você precisa de exportá-lo

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

O comando acima deve gerar o certificado abaixo

% 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-----

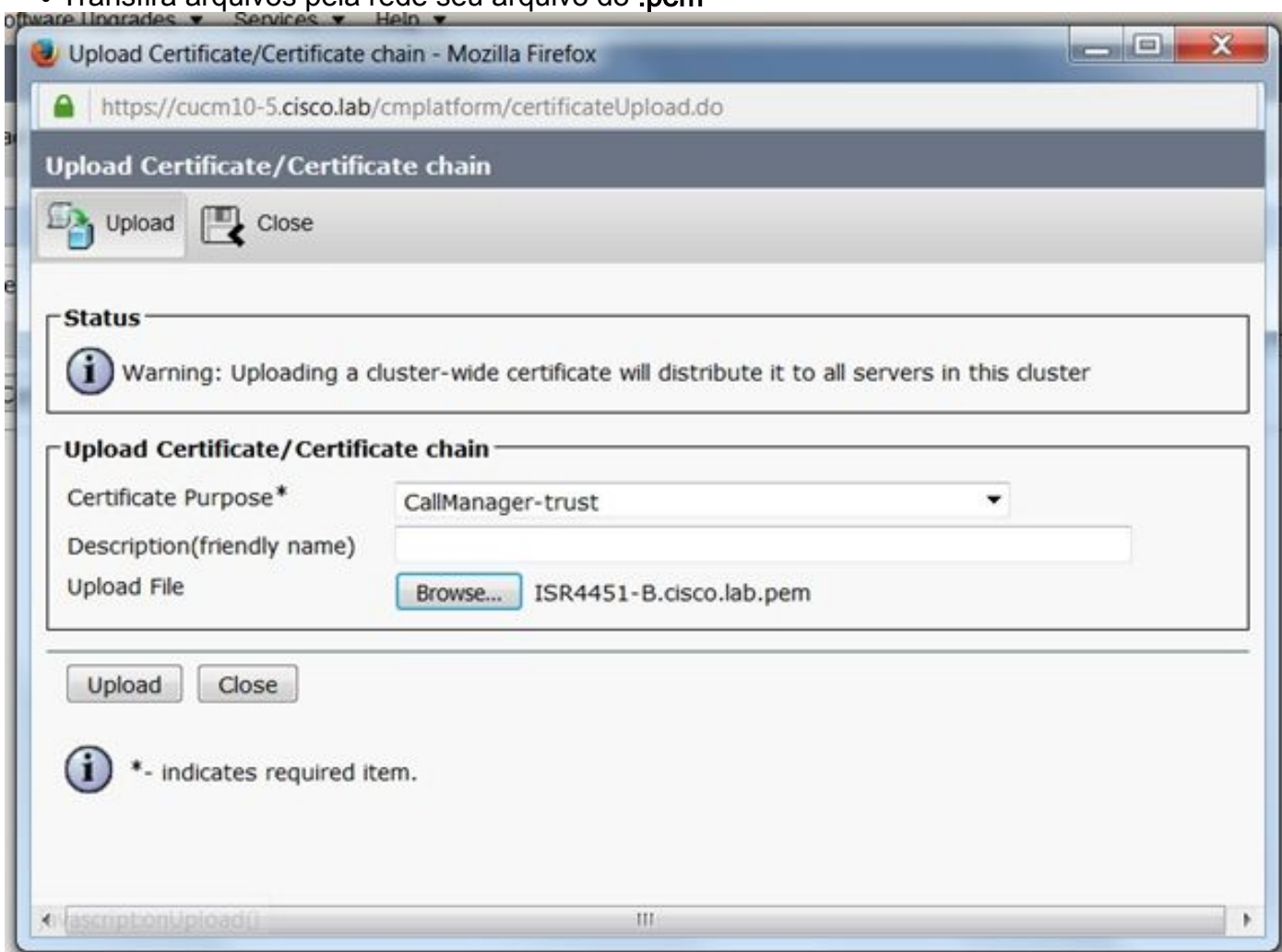
Copie o certificado assinado acima gerado do auto e cole-o a um arquivo de texto com **.pem** da extensão de arquivo

O exemplo abaixo é nomeado como **ISR4451-B.ciscolab.pem**



Etapa 4. Transfira arquivos pela rede o certificado do CUBO ao CUCM

- >gerenciamento de certificado do > segurança Admin do OS CUCM > certificado/certificate chain da transferência de arquivo pela rede
- Finalidade = CallManager-confiança do certificado
- Transfira arquivos pela rede seu arquivo do **.pem**



Etapa 5. Transfira o certificado auto-assinado do gerenciador de chamada

- Encontre o certificado que diz Callmanager
- Clique sobre o nome de host
- Clique sobre o arquivo da transferência PEM
- Salvar o a seu computador

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

Etapa 6. Transfira arquivos pela rede o certificado Callmanager.pem PARA CUBAR

- Abra o Callmanager.pem com um editor do arquivo de texto
- Copie o índice inteiro do arquivo
- Execute isto comanda no 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

## Etapa 7. Configurar o SORVO para usar o ponto confiável selfsigned do certificado do CUBO

sip-ua

crypto signaling default trustpoint CUBEttest

## Etapa 8. Configurar os dial peer com 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
```

## Etapa 9. Configurar um perfil de segurança do tronco do SORVO CUCM

- >segurança da página de admin > do sistema CUCM > perfil de segurança do tronco do SORVO
- Configurar o perfil como mostrado abaixo

**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:** É criticamente importante que o campo X.509 combine o nome que do CN você configurou previamente quando você gerava o certificado auto-assinado

## Etapa 10. Configurar um tronco do SORVO em CUCM

- Assegure-se de que a caixa de verificação permitida SRTP esteja verificada
- Configurar o endereço de destino apropriado e assegure-o para substituir a porta 5060 com a

porta 5061

- Assegure para selecionar o perfil de segurança correto do tronco do sorvo (que foi criado na etapa 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

- Salvar e restaure o tronco.

## Verificar

Desde que você permitiu as OPÇÕES PING no CUCM, o tronco do SORVO deve estar no estado do SERVIÇO COMPLETO

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
<a href="#">ISR4451-B</a>			<a href="#">0711-Secure</a>					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

O serviço completo da mostra do status de tronco do SORVO.

A mostra do estado do dial peer como seguem:

```
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

Permita e recolha a saída destes debuga

```
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 da gravação do WebEx:

<https://goo.gl/QOS1iT>