

Configurar TLS SIP entre CUCM-CUBE/CUBE-SBC com certificados assinados por CA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Verificar](#)

—

[Troubleshoot](#)

Introduction

Este documento descreve como configurar o SIP Transport Layer Security (TLS) entre o Cisco Unified Communication Manager (CUCM) e o Cisco Unified Border Element (CUBE) com certificados assinados pela autoridade de certificação (CA).

Prerequisites

A Cisco recomenda ter conhecimento desses assuntos

- Protocolo SIP
- Certificados de segurança

Requirements

- A data e a hora devem coincidir nos endpoints (recomenda-se ter a mesma origem NTP).
- O CUCM deve estar em modo misto.
- A conectividade TCP é necessária (porta aberta 5061 em qualquer firewall de trânsito).
- O CUBE deve ter as licenças de segurança e Unified Communication K9 (UCK9) instaladas.

Note: Para a versão 16.10 do Cisco IOS-XE, a plataforma mudou para o licenciamento inteligente.

Componentes Utilizados

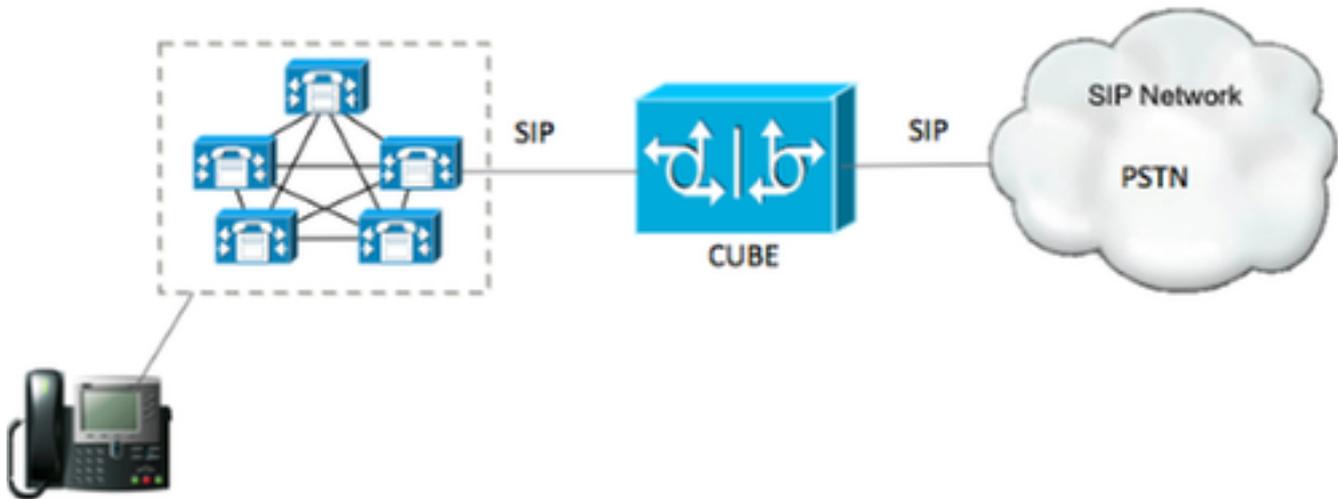
- SIP
- Certificados assinados pela autoridade de certificação
- Gateways Cisco IOS e IOS-XE Versões 2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X:

15,4+

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

Configurar

Diagrama de Rede



Configuração

Etapa 1. Você criará uma chave RSA correspondente ao comprimento do certificado raiz usando o comando:

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

Esse comando cria uma chave RSA com um comprimento de 2048 bits (o máximo é 4096).

Etapa 2. Crie um ponto de confiança para manter nosso certificado assinado pela CA usando comandos:

```
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)
```

Etapa 3. Agora que você tem nosso ponto de confiança, você vai gerar nossa solicitação de CSR com os comandos abaixo:

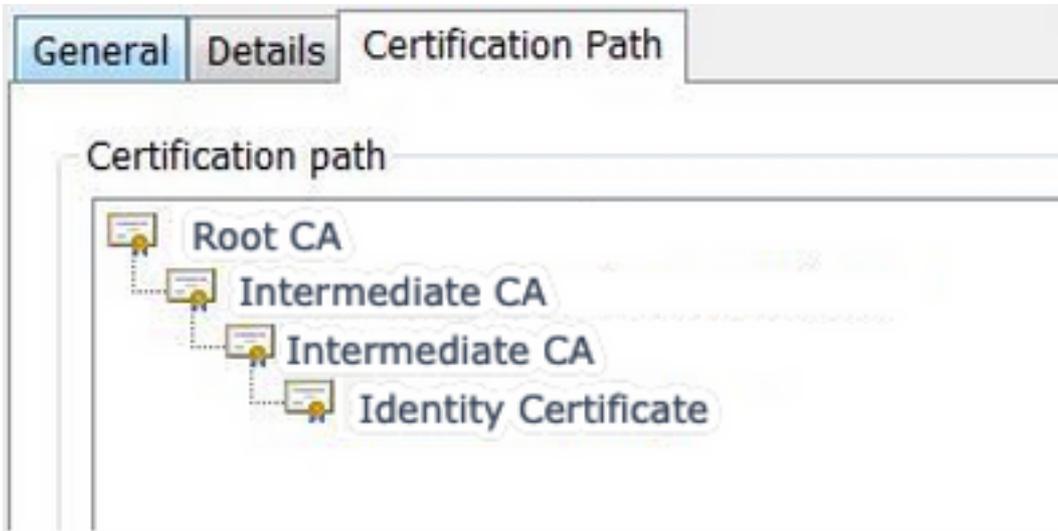
```
Crypto pki enroll CUBE_CA_CERT
```

Responda às perguntas na tela, copie a solicitação CSR, salve-a em um arquivo e envie-a para a CA.

Etapa 4. Você precisa descobrir se a cadeia de certificados Raiz tem certificados intermediários;

caso não haja autoridades de certificado intermediárias, vá para a etapa 7, caso contrário, continue na etapa 6.

Etapa 5. Crie um ponto de confiança para manter o certificado Raiz e, além disso, crie um ponto de confiança para manter qualquer AC intermediária até a que estiver assinando o certificado CUBE (veja a imagem abaixo).



Neste exemplo, o 1º nível é a CA raiz, o 2º nível é nossa primeira CA intermediária, o 3º nível é a CA que está assinando nosso certificado CUBE e, portanto, você precisa criar um ponto de confiança para manter os 2 primeiros certificados com esses comandos.

```
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
```

Etapa 6. Depois de receber o nosso certificado assinado pela AC, irá autenticar o ponto de confiança, o ponto de confiança tem de manter o certificado da AC logo antes do certificado CUBE; o comando que permite importar o certificado é,

```
Crypto pki authenticate CUBE_CA_CERT
```

Passo 7. Depois que o nosso certificado estiver instalado, você precisará executar este comando para importar o certificado do CUBE

```
Crypto pki import CUBE_CA_CERT cert
```

Etapa 8. Configure SIP-UA para usar o ponto de confiança criado

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

Etapa 9. Configure os peers de discagem conforme mostrado abaixo:

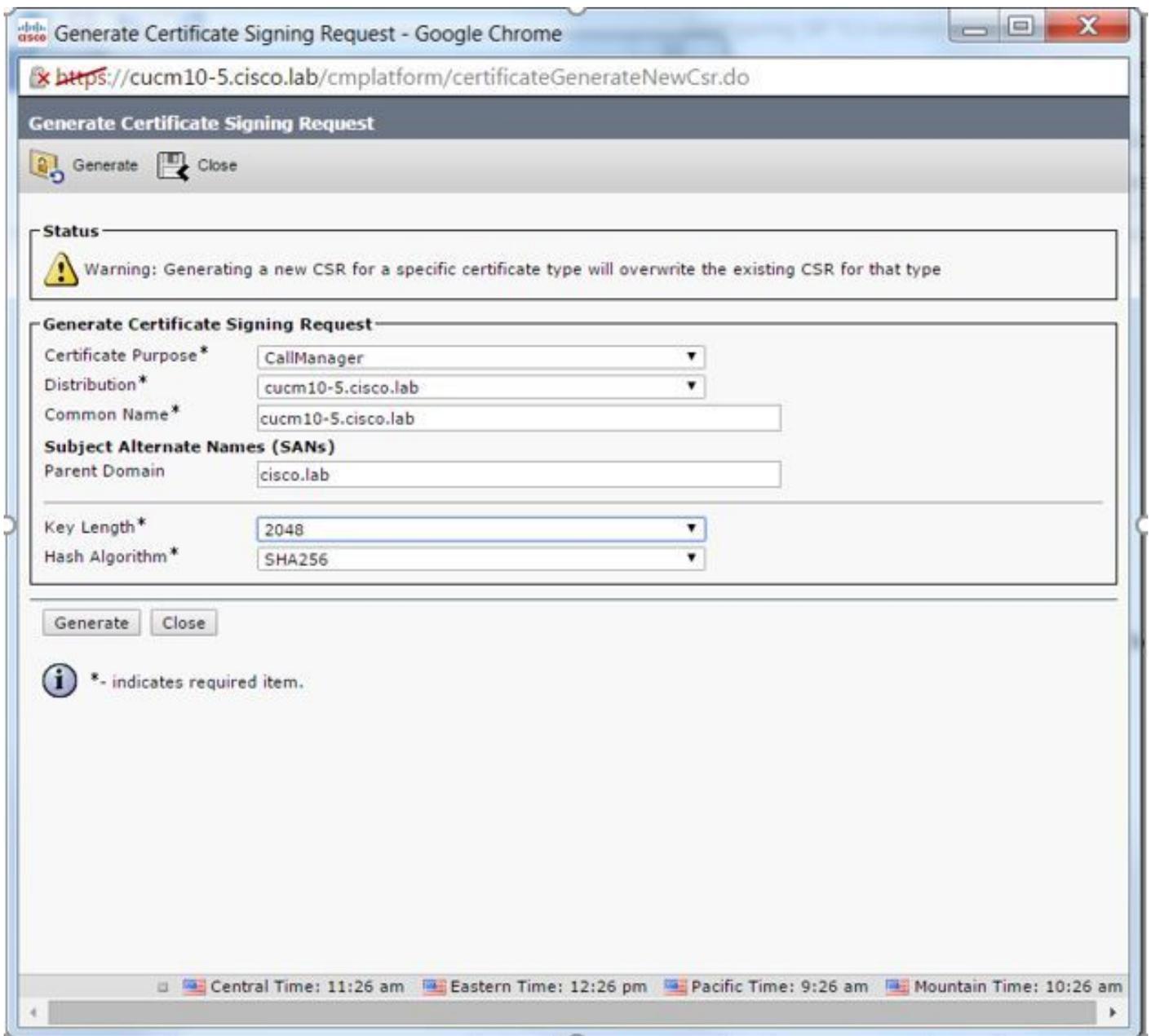
```
dial-peer voice 9999 voip
answer-address 35..
destination-pattern 9999
session protocol sipv2
session target dns:cucm10-5
session transport tcp tls
voice-class sip options-keepalive
srtp
```

Com isso, a configuração do CUBE está concluída.

Etapa 10. Agora, você vai gerar nosso CUCM CSR, siga as instruções abaixo

- Fazer login no administrador do SO CUCM
- Clique em segurança
- Clique em gerenciamento de certificado.
- Clique em gerar CSR

A solicitação de CSR deve ser semelhante à seguinte:



Etapa 11. Baixe o CSR e envie para a CA.

Etapa 12. Carregue a cadeia de certificados com assinatura CA para o CUCM , as etapas são:

- Clique em segurança e em gerenciamento de certificados.
- Clique em carregar certificado/cadeia de certificados.
- No menu suspenso propósito do certificado, selecione gerenciador de chamadas.
- Navegue até o seu arquivo.
- Clique em upload.

Etapa 13. Faça login na CLI do CUCM e execute este comando

```
utils ctl update CTLFile
```

Etapa 14. Configurar um perfil de segurança de tronco SIP do CUCM

- Clique em sistema, segurança e, em seguida, perfil de segurança de tronco sip
- Configure o perfil como mostrado na imagem,

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: Nesse caso, o nome do assunto X.509 deve corresponder ao nome do assunto do certificado CUCM como mostrado na parte destacada da imagem.

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
SignatureAlgorithm: 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
  
```

Etapa 15. Configure um tronco SIP como faria normalmente no CUCM

- Verifique se a caixa de seleção SRTP Permitido está marcada.
- Configure o endereço de destino apropriado e certifique-se de substituir a porta 5060 pela porta 5061.
- No perfil de segurança de tronco SIP, selecione o nome do perfil SIP criado na etapa 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*

Verificar

Neste momento, se toda a configuração estiver OK,

No CUCM, o status do tronco SIP mostra Full Service , como mostrado na imagem,

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

No CUBE, o correspondente de discagem mostra este status:

```
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
```

Esse mesmo processo se aplica a outros roteadores, a única diferença é que, em vez da etapa para carregar o certificado CUCM, carregue o certificado fornecido por terceiros.

Troubleshoot

Ative essas depurações no 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
```