

# Configurar o tronco SIP TLS no Communications Manager com um certificado assinado pela CA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Usar a CA pública ou a CA de configuração no Windows Server 2003](#)

[Etapa 2. Verificar o nome do host e as configurações](#)

[Etapa 3. Gerar e baixar a solicitação de assinatura de certificado \(CSR\)](#)

[Etapa 4. Assinar o CSR com a Autoridade de Certificação do Microsoft Windows 2003](#)

[Etapa 5. Obter o certificado raiz do CA](#)

[Etapa 6. Carregar certificado raiz de CA como confiança do CallManager](#)

[Passo 7. Carregar certificado CSR do CallManager como certificado do CallManager.](#)

[Etapa 8. Criar perfis de segurança de tronco SIP](#)

[Etapa 9. Criar troncos SIP](#)

[Etapa 10. Criar padrões de rota](#)

[Verificar](#)

[Troubleshoot](#)

[Coletar Captura de Pacotes no CUCM](#)

[Coletar rastreamentos do CUCM](#)

## Introduction

Este documento descreve um processo passo a passo para configurar o Tronco TLS (Transport Layer Security) do Session Initiation Protocol (SIP) no Communications Manager com um certificado assinado Certificate Authority (CA).

Depois de seguir este documento, as mensagens SIP entre dois clusters serão criptografadas usando o TLS.

## Prerequisites

## Requirements

A Cisco recomenda que você conheça:

- Cisco Unified Communications Manager (CUCM)
- SIP

## Componentes Utilizados

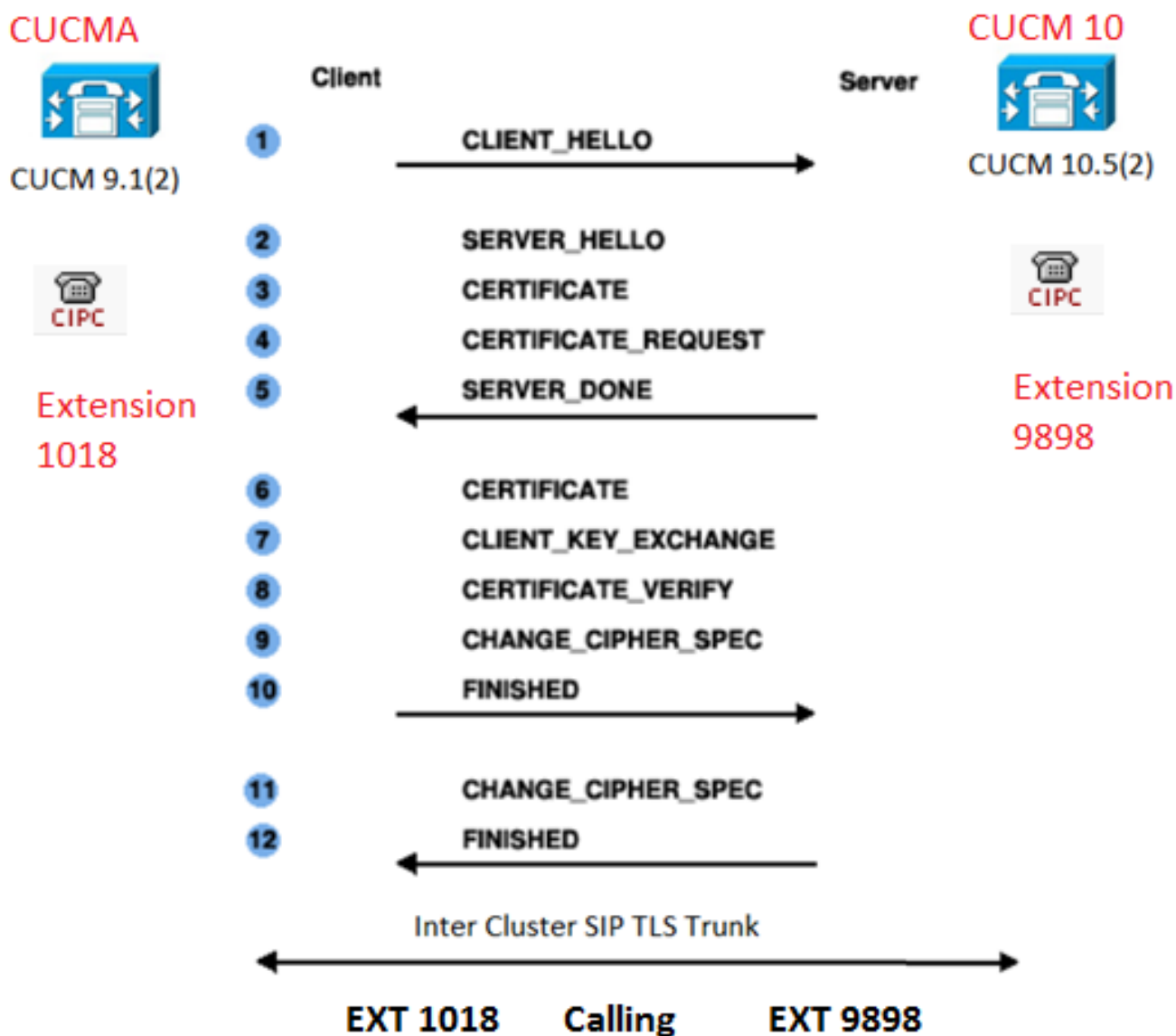
As informações neste documento são baseadas nestas versões de software:

- CUCM versão 9.1(2)
- CUCM versão 10.5(2)
- Microsoft Windows Server 2003 como CA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informações de Apoio

Como mostrado nesta imagem, o Handshake SSL usa Certificados.



### Configurar

Etapa 1. Usar a CA pública ou a CA de configuração no Windows Server 2003

Consulte o link: [Configurar CA no Windows 2003 Server](#)

Etapa 2. Verificar o nome do host e as configurações

Os certificados são baseados em nomes. Verifique se os nomes estão corretos antes de iniciar.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Para alterar o nome do host, consulte o link: [Alterar o nome do host no CUCM](#)

Etapa 3. Gerar e baixar a solicitação de assinatura de certificado (CSR)

### CUCM 9.1(2)

Para gerar o CSR, navegue até **OS Admin > Segurança > Gerenciamento de certificado > Gerar CSR**

No campo **Nome do certificado**, selecione a opção **CallManager** na lista suspensa.



The screenshot shows a dialog box titled "Generate Certificate Signing Request". At the top, there are two buttons: "Generate CSR" (with a lock icon) and "Close" (with a document icon). Below this is a "Status" section with a warning icon and the text: "Warning: Generating a new CSR will overwrite the existing CSR". The main section is titled "Generate Certificate Signing Request" and contains a dropdown menu labeled "Certificate Name\*" with "CallManager" selected. This dropdown menu is highlighted with a red border. At the bottom, there are two buttons: "Generate CSR" (highlighted with a red border) and "Close".

Para baixar o CSR, navegue até **OS Admin > Security > Certificate Management > Download CSR**

No campo **Nome do certificado**, selecione a opção **CallManager** na lista suspensa.

### Download Certificate Signing Request

 Download CSR  Close

**Status**

 Certificate names not listed below do not have a corresponding CSR

**Download Certificate Signing Request**



Certificate Name\*

CUCM 10.5(2)


Para gerar o CSR, navegue até OS Admin > Segurança > Gerenciamento de Certificados > Gerar CSR

1. No campo Certificate Purpose (Finalidade do certificado), selecione CallManager na lista suspensa.
2. No campo Tamanho da chave, selecione 1024 na lista suspensa.
3. No campo Hash Algorithm, selecione SHA1 na lista suspensa.

### Generate Certificate Signing Request

 Generate  Close

**Status**

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

**Generate Certificate Signing Request**

Certificate Purpose\*

Distribution\*

Common Name\*

**Subject Alternate Names (SANS)**

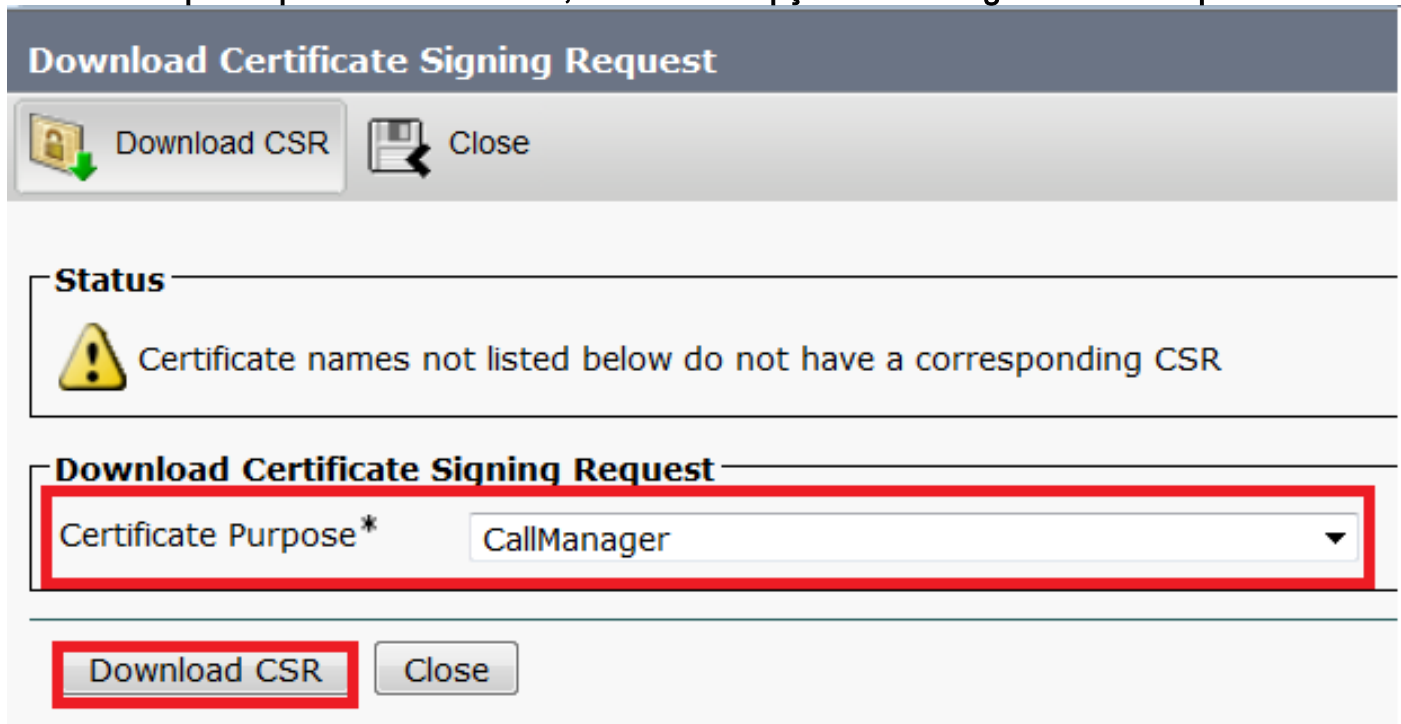
Parent Domain

Key Length\*

Hash Algorithm\*

Para baixar o CSR, navegue até OS Admin > Security > Certificate Management > Download

CSR No campo Propósito do certificado, selecione a opção CallManager na lista suspensa.



**Download Certificate Signing Request**

Download CSR Close

**Status**

! Certificate names not listed below do not have a corresponding CSR

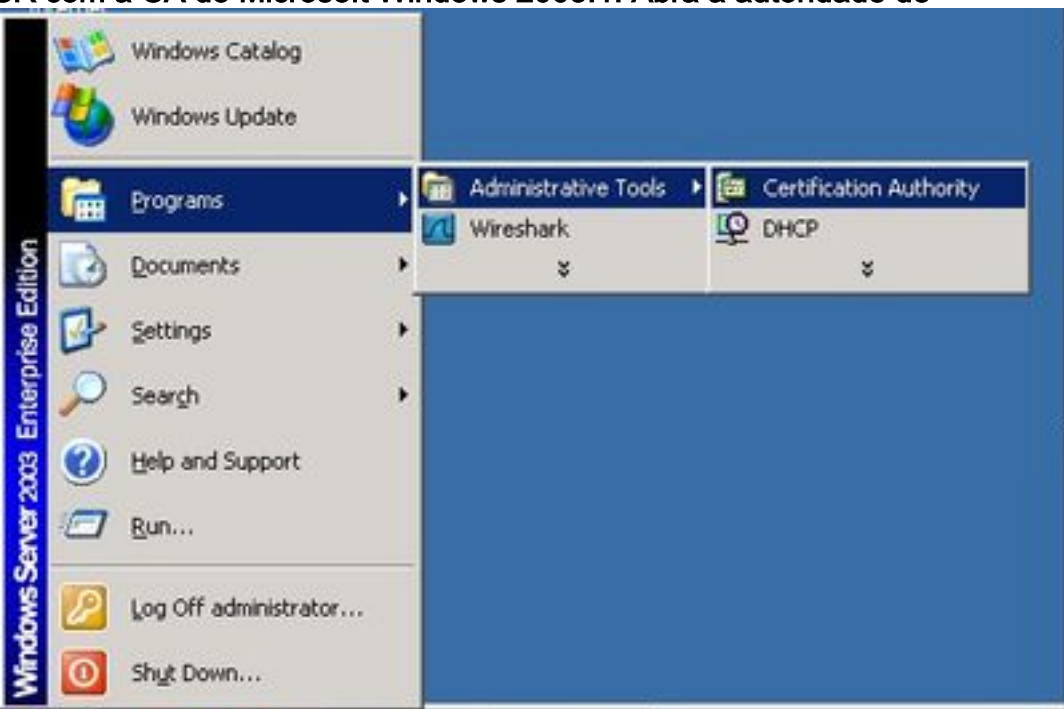
**Download Certificate Signing Request**

Certificate Purpose\* CallManager

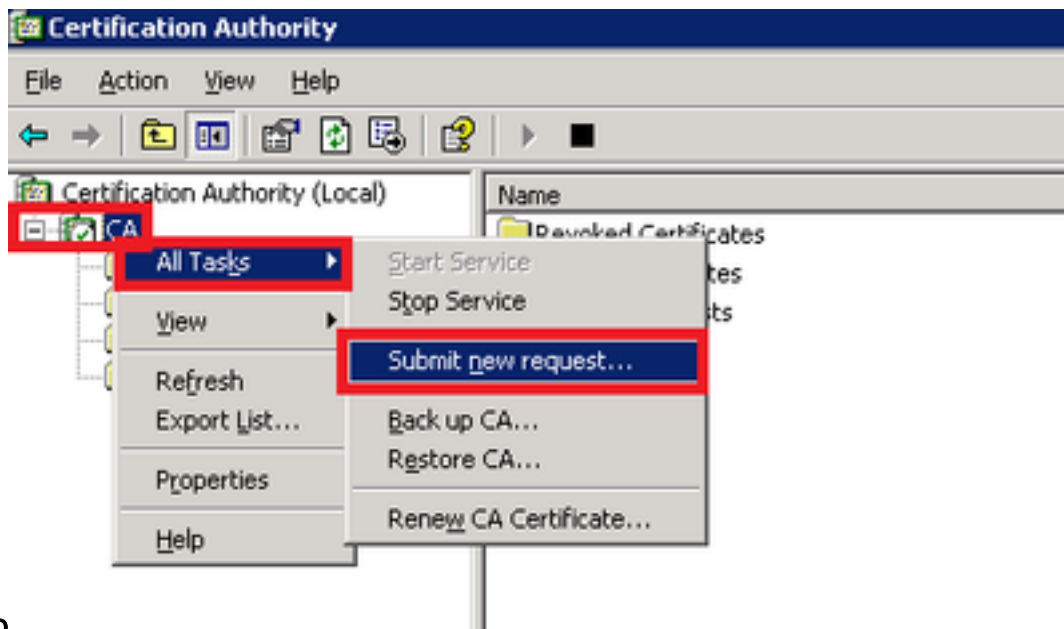
Download CSR Close

Note: O CSR do CallManager é gerado com as chaves Rivest-Shamir-Addleman (RSA) de 1024 bits. Etapa 4. Assinar o CSR com a Autoridade de Certificação do Microsoft Windows 2003. Estas são informações opcionais para assinar o CSR com a CA do Microsoft Windows 2003.

1. Abra a autoridade de certificação.

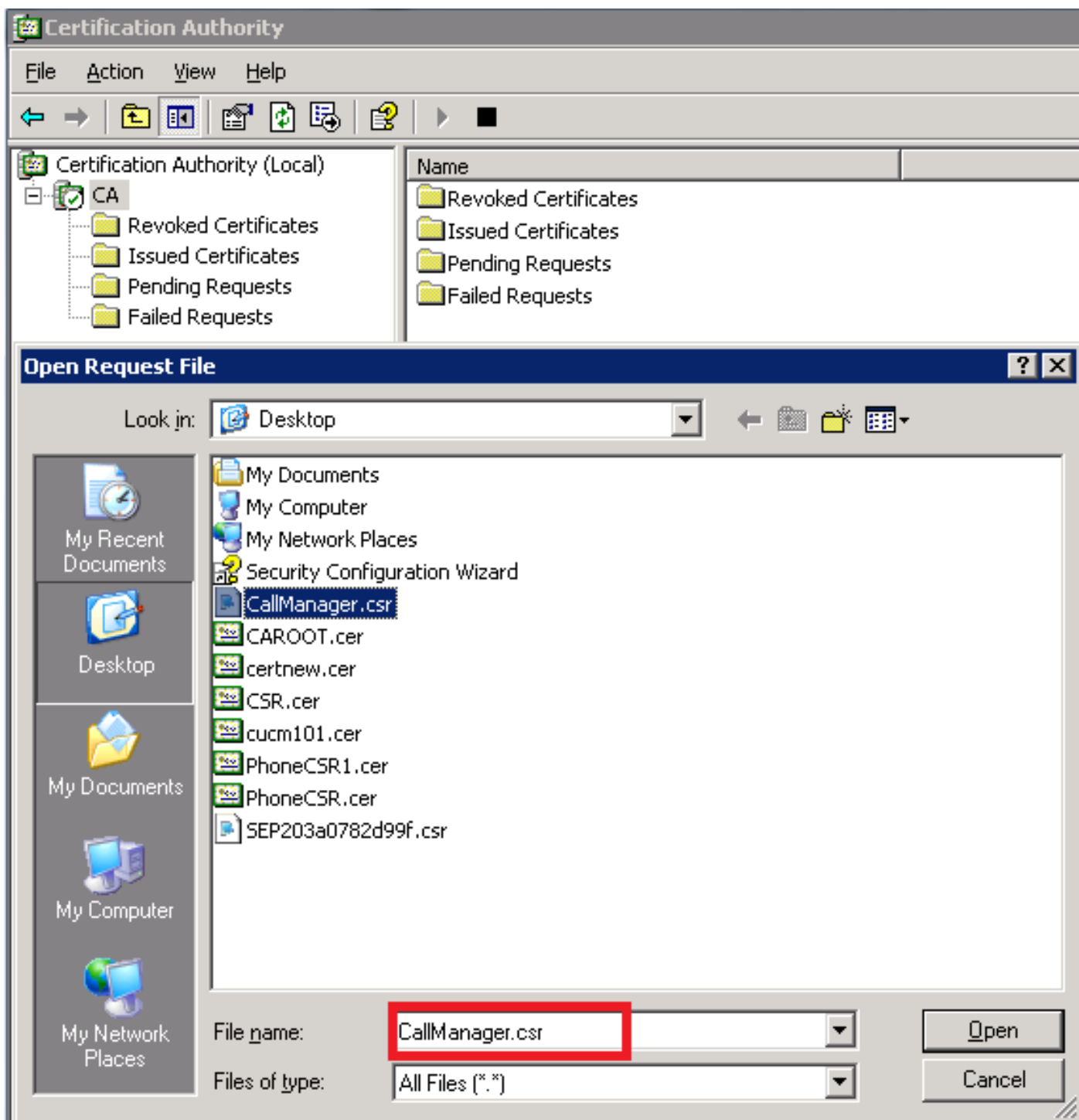


2. Clique com o botão direito do mouse no ícone CA e navegue para Todas as tarefas > Enviar nova

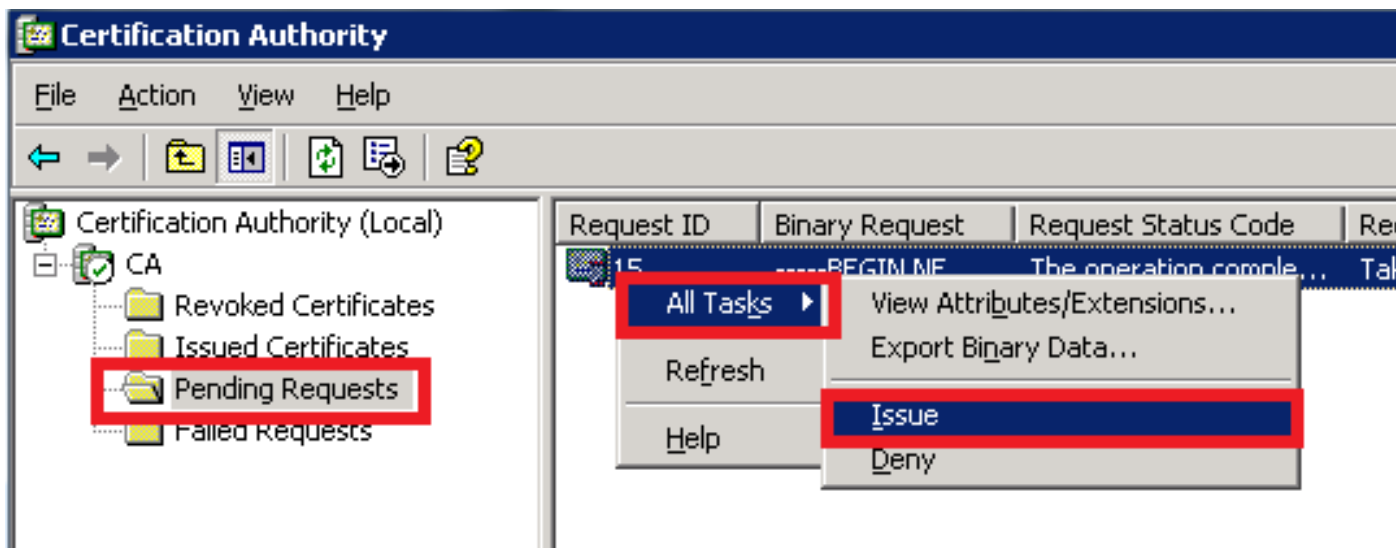


solicitação  
o CSR e clique na opção Abrir (Aplicável nos CSRs (CUCM 9.1(2) e CUCM  
10.5(2))

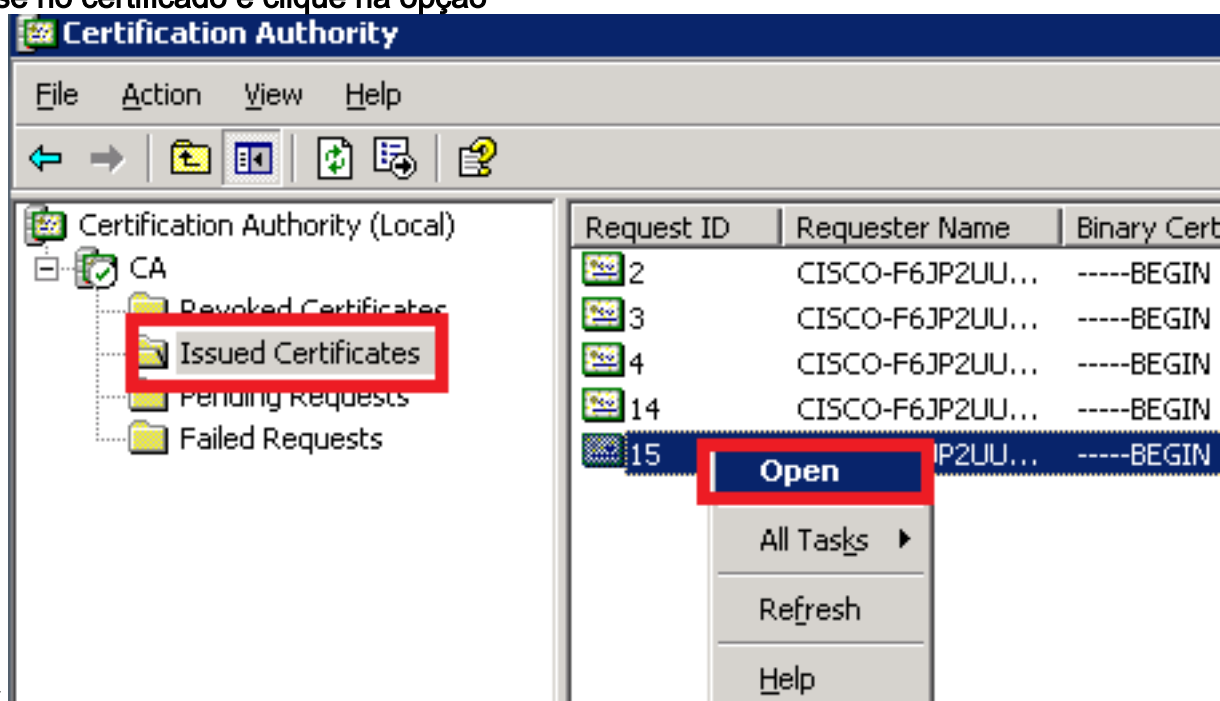
3. Selecione



4. Todos os CSRs abertos são exibidos na Pasta Solicitações Pendentes. Clique com o botão direito do mouse em cada CSR e navegue até All Tasks > Issue para emitir certificados. (Aplicável nos CSRs (CUCM 9.1(2) e CUCM 10.5(2))



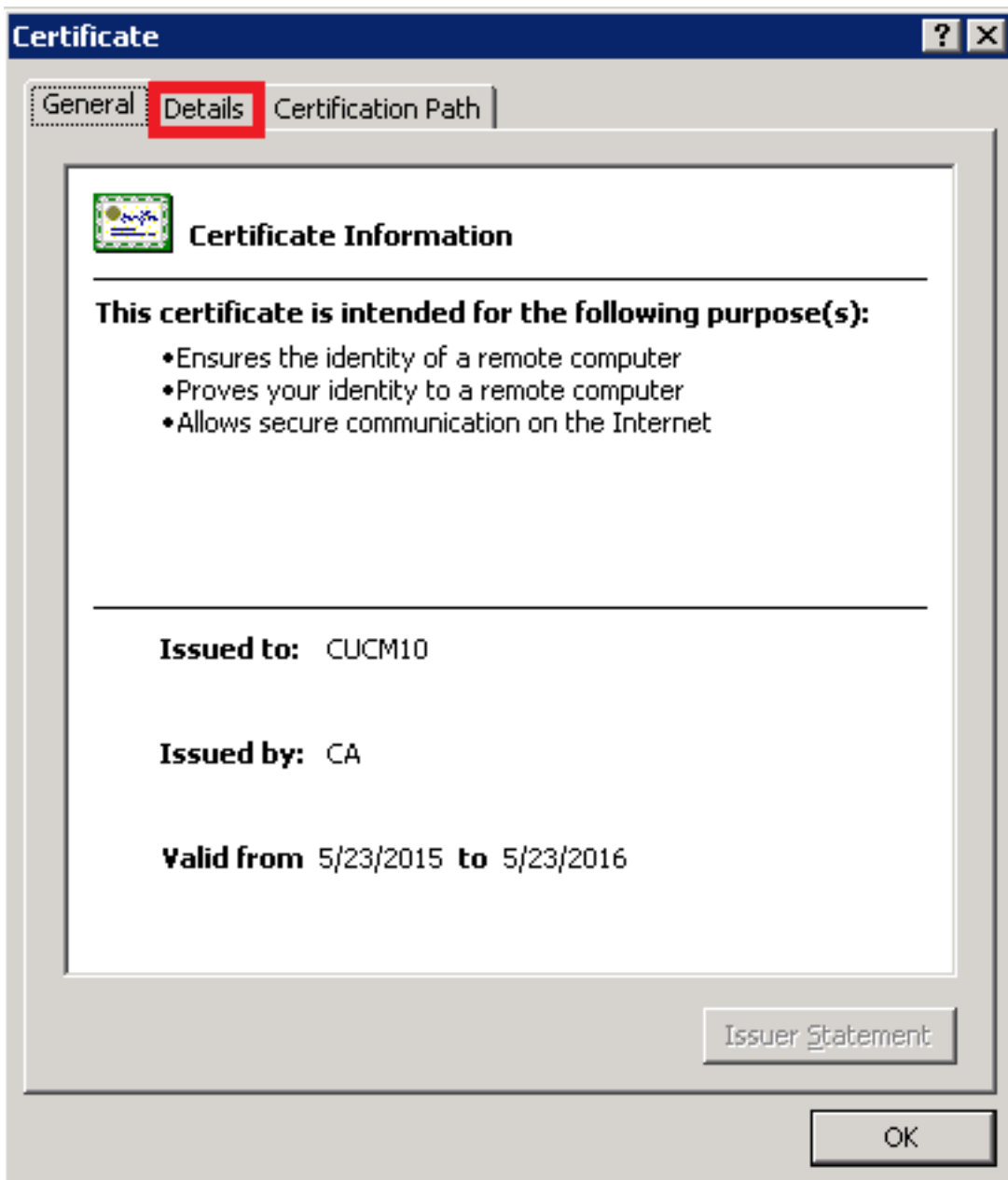
5. Para baixar o certificado, escolha a pasta Certificados Emitidos. Clique com o botão direito do mouse no certificado e clique na opção



Abrir.

6. Os detalhes do certificado são exibidos. Para baixar o certificado, selecione a guia Detalhes e clique no botão Copiar para

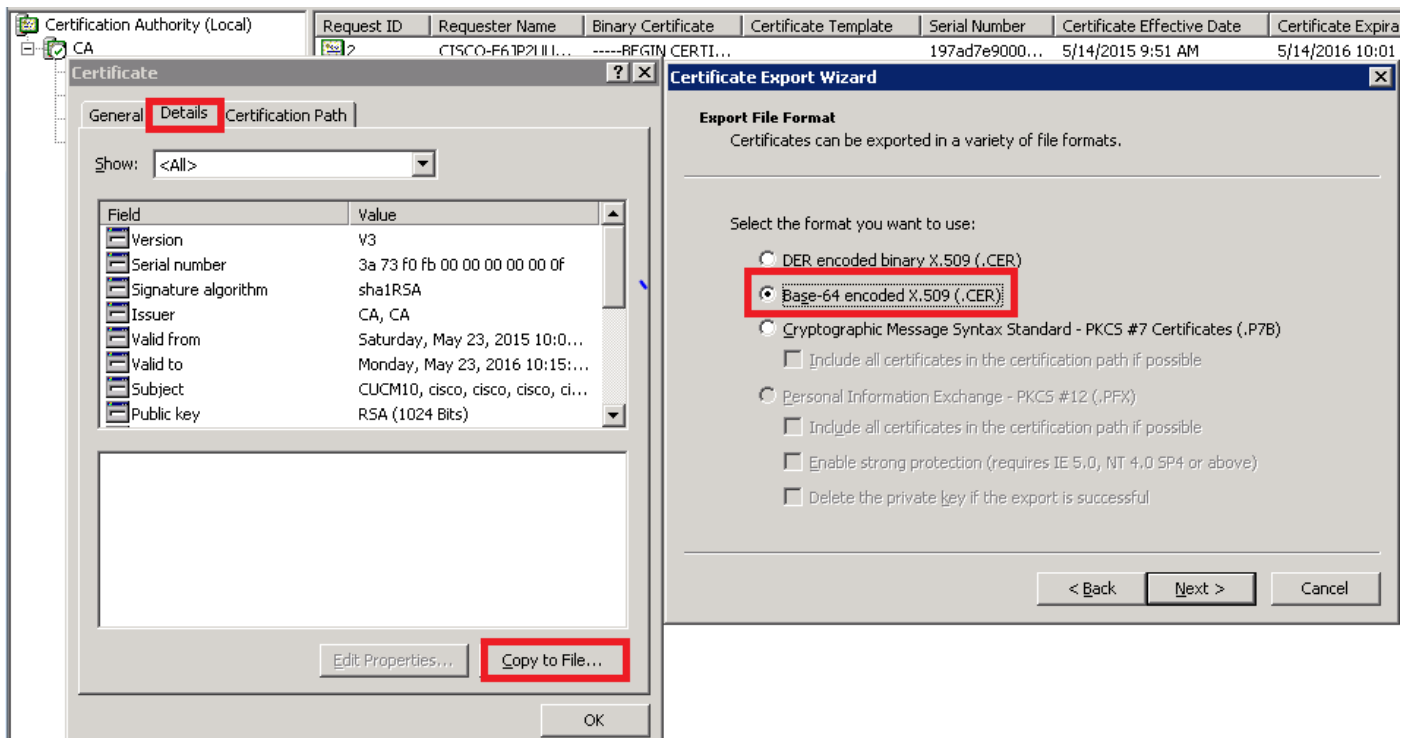




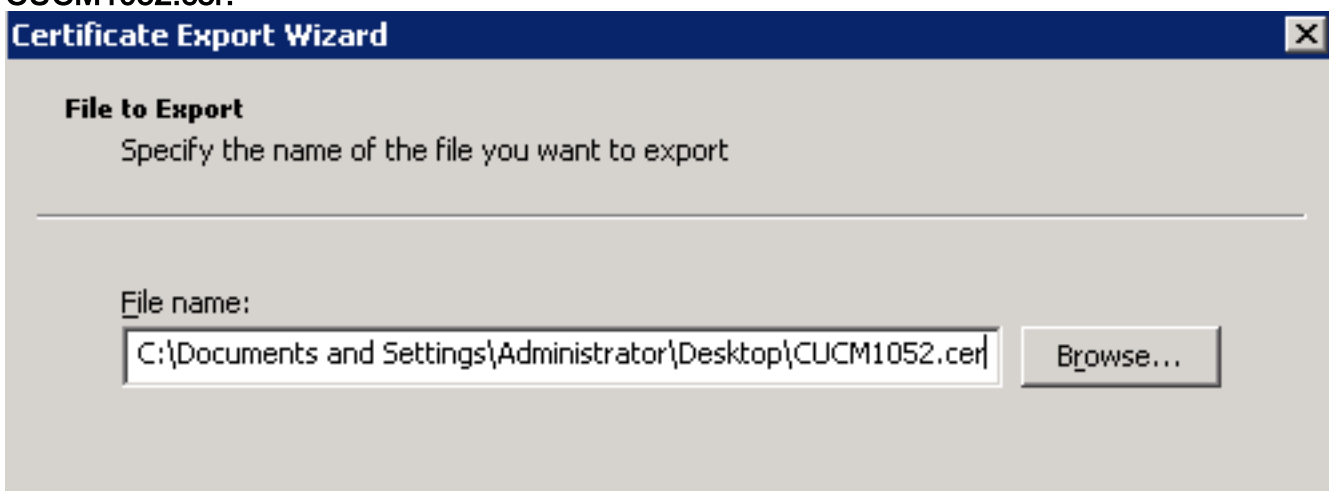
arquivo...

Assistente para exportação de certificado, clique no botão de opção X.509(.CER) codificado em Base 64.

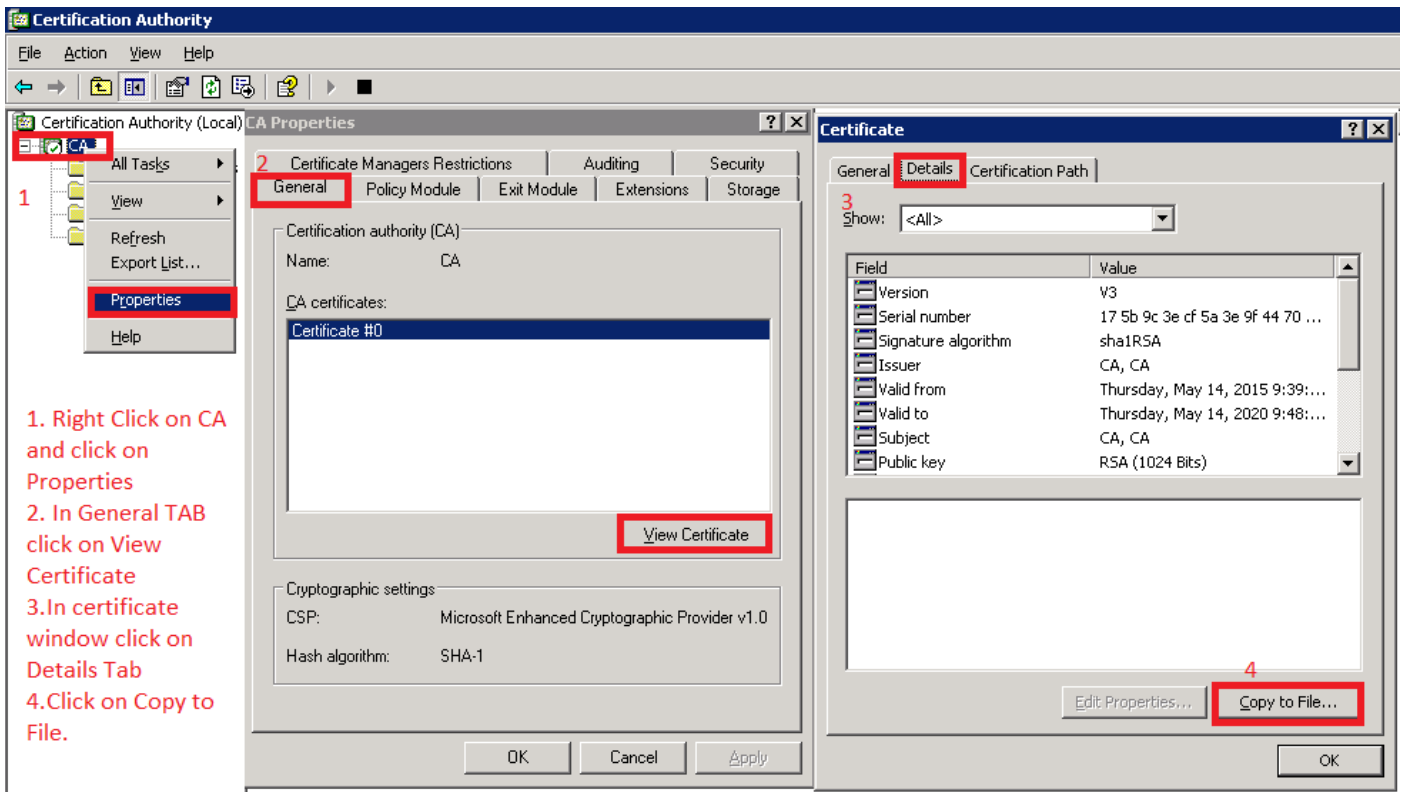
7. Na janela



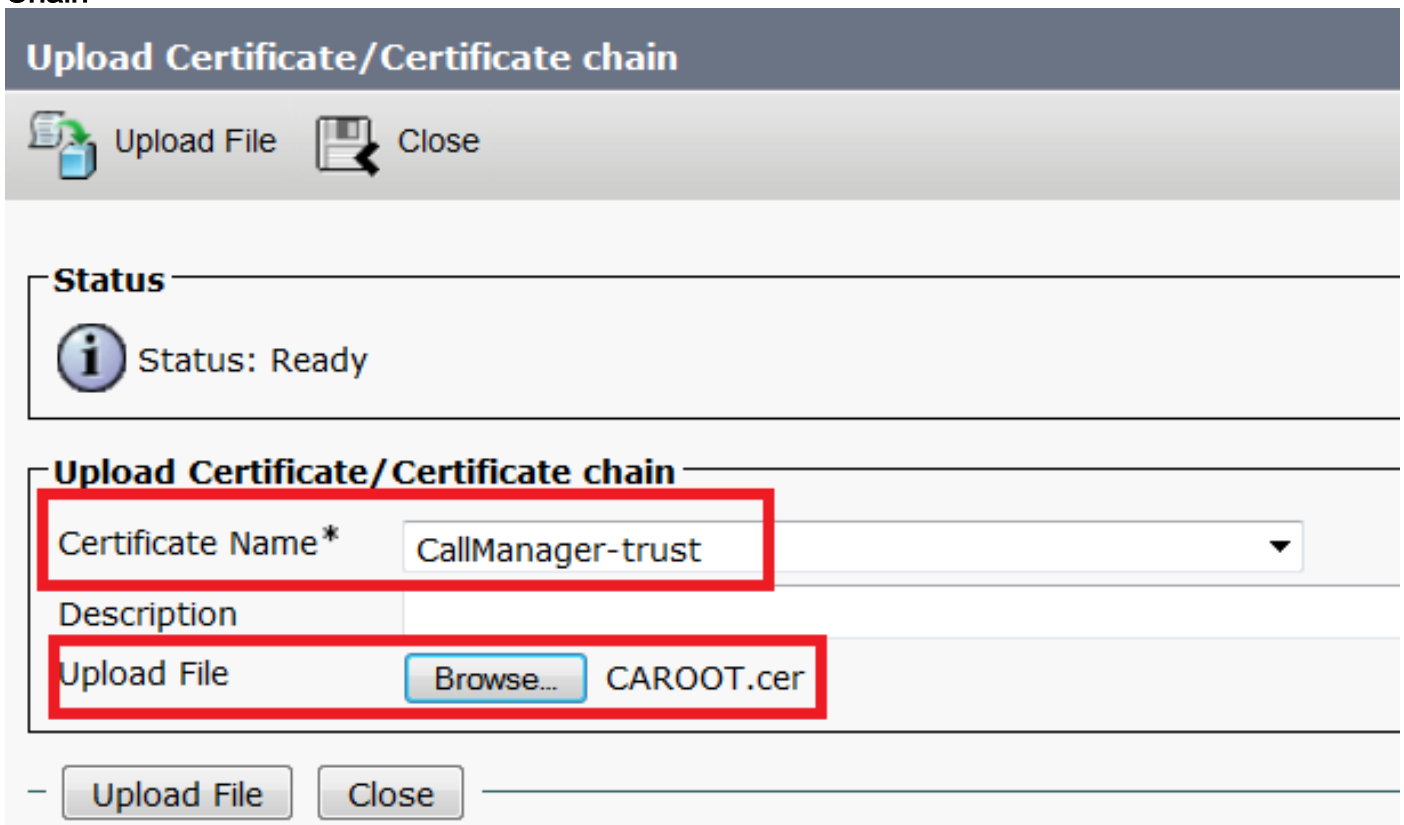
8. Nomeie o arquivo com precisão. Este exemplo usa o formato CUCM1052.cer.



Par a o CUCM 9.1(2), siga o mesmo procedimento. Etapa 5. Obter o certificado raiz do CA Abra a janela Autoridade de Certificação. Para fazer o download do CA raiz 1. Clique com o botão direito do mouse no ícone CA e clique na opção Propriedades. 2. Na guia geral, clique em Exibir certificado. 3. Na janela Certificado, clique na GUIA de detalhes. 4. Clique em Copiar para arquivo...



Etapa 6. Carregar certificado raiz de CA como confiança do CallManager. Para fazer o upload do certificado raiz da CA, faça login no OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain



Note: Execute estas etapas nos CUCMs (CUCM 9.1(2) e CUCM 10.5(2))  
 Passo 7. Carregar certificado CSR do CallManager como certificado do CallManager. Para carregar o CA sign CallManager CSR, faça login no OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain

## Upload Certificate/Certificate chain



Upload File



Close

### Status



Status: Ready

### Upload Certificate/Certificate chain

Certificate Name\*

CallManager

Description

Self-signed certificate

Upload File

Browse...

CUCM9.cer

Upload File

Close

Note: Execute estas etapas nos CUCMs (CUCM 9.1(2) e CUCM 10.5(2))  
Etapa 8. Criar perfis de segurança de tronco SIP  
CUCM 9.1(2)

Para criar o Perfil de segurança do tronco SIP, navegue para System > Security > SIP Trunk Security Profile. Copie o perfil de tronco SIP não seguro existente e dê a ele um novo nome. No exemplo, o perfil de tronco SIP não seguro foi renomeado com TLS de perfil de tronco SIP seguro.

## SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

### SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS	
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	CUCM10	This Name should be CN of CUCM 10.5(2)
Incoming Port*	5061	
<input type="checkbox"/> Enable Application level authorization		
<input type="checkbox"/> Accept presence subscription		
<input type="checkbox"/> Accept out-of-dialog refer**		
<input type="checkbox"/> Accept unsolicited notification		
<input 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 ▼	

No X.509 Subject Name (Nome do assunto do X.509), use o Common Name (CN) (Nome comum (CN) do CUCM 10.5(2) (Certificado assinado pela CA) como mostrado nesta imagem.

## Certificate Settings

Locally Uploaded	23/05/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by CA

## Certificate File Data

```
[
Version: V3
Serial Number: 398B1DA600000000000E
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CA, DC=CA
Validity From: Sat May 23 17:50:42 IST 2015
           To: Mon May 23 18:00:42 IST 2016
Subject Name: CN=CUCM10, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100bcf093aa206190fe76abe13e3bd3ec45cc8b2afeee86e8393f568e1c9aa0c5fdf3f044eebc
f2d999ed8ac3592220fef3f9dcf2d2e7e939a4b26896152ebb250e407cb65d9e04bf71e8c345633786041e
5c806405160ac42a7133d7d644294226b850810fffd001e5bf2b39829b1fb27f126624e5011f151f0ef07c7
eccb734710203010001
Extensions: 6 present
]
```

CUCM 10.5(2)Navegue até System > Security > SIP Trunk Security Profile.Copie o perfil de tronco SIP não seguro existente e dê a ele um novo nome. No exemplo, o perfil de tronco SIP não seguro foi renomeado com TLS de perfil de tronco SIP seguro.

## SIP Trunk Security Profile Configuration



Save



Delete



Copy



Reset



Apply Config



Add New

### SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS	
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	CUCMA	This Name should be CN of CUCM 9.1(2)
Incoming Port*	5061	
<input type="checkbox"/> Enable Application level authorization		
<input type="checkbox"/> Accept presence subscription		
<input type="checkbox"/> Accept out-of-dialog refer**		
<input type="checkbox"/> Accept unsolicited notification		
<input 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	

No X.509 Subject Name (Nome do assunto do X.509), use o CN do CUCM 9.1(2) (Certificado assinado pela CA), conforme destacado:

File Name	CallManager.pem
Certificate Name	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description	Certificate Signed by CA

#### Certificate File Data

```
[
  Version: V3
  Serial Number: 120325222815121423728642
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=CA, DC=CA
  Validity From: Thu May 14 09:51:09 IST 2015
    To: Sat May 14 10:01:09 IST 2016
  Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
30818902818100916c34c9700ebe4fc463671926fa29d5c98896df275ff305f80ee0c7e9dbf6e90e74cd5c44b5b26
be0207bf5446944aef901ee5c3daefdb2cf4cbc870f8ce1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d
ab8a7af5149194cce07b7ddc101ce0e860dad7fd01cc613fe3f1250203010001
  Extensions: 6 present
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
```

Ambos os perfis de segurança de tronco SIP definem uma porta de entrada de 5061, na qual cada cluster ouve na porta TCP 5061 para as novas chamadas SIP TLS de entrada. Etapa 9. Criar troncos SIP Depois que os perfis de segurança forem criados, crie os troncos SIP e faça as alterações para o parâmetro de configuração abaixo no tronco SIP.CUCM 9.1(2)

1. Na janela SIP Trunk Configuration, marque a caixa de seleção SRTP Allowed do parâmetro de configuração.

Isso protege o RTP (Real-time Transport Protocol) a ser usado para as chamadas nesse tronco. Esta caixa deve ser marcada somente quando você usa SIP TLS porque as chaves para Secure Real-time Transport Protocol (SRTP) são trocadas no corpo da mensagem SIP. A sinalização SIP deve ser protegida por TLS, caso contrário, qualquer pessoa com a sinalização SIP não segura pode descriptografar o fluxo SRTP correspondente no tronco.



**Trunk Configuration**

Save Delete Reset Add New

**Status**  
 Status: Ready

**Device Information**

Product: SIP Trunk  
 Device Protocol: SIP  
 Trunk Service Type: None(Default)  
 Device Name\*: CUCM10  
 Description:  
 Device Pool\*: Default  
 Common Device Configuration: < None >  
 Call Classification\*: Use System Default  
 Media Resource Group List: < None >  
 Location\*: Hub\_None  
 AAR Group: < None >  
 Tunneled Protocol\*: None  
 QSIG Variant\*: No Changes  
 ASN.1 ROSE OID Encoding\*: No Changes  
 Packet Capture Mode\*: None  
 Packet Capture Duration: 0

Media Termination Point Required  
 Retry Video Call as Audio  
 Path Replacement Support  
 Transmit UTF-8 for Calling Party Name  
 Transmit UTF-8 Names in QSIG APDU  
 Unattended Port  
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.  
 Consider Traffic on This Trunk Secure\*: When using both sRTP and TLS  
 Route Class Signaling Enabled\*: Default

2. Na seção SIP Information da janela SIP Trunk Configuration, adicione o Destination Address, Destination Port e SIP Trunk Security Profile.

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.200		5061

MTP Preferred Originating Codec\*: 711ulaw  
 BLF Presence Group\*: Standard Presence group  
 SIP Trunk Security Profile\*: Secure SIP Trunk Profile TLS  
 Rerouting Calling Search Space: < None >  
 Out-Of-Dialog Refer Calling Search Space: < None >  
 SUBSCRIBE Calling Search Space: < None >  
 SIP Profile\*: Standard SIP Profile  
 DTMF Signaling Method\*: No Preference

## CUCM 10.5(2)

1. Na janela SIP Trunk Configuration, marque a caixa de seleção SRTP Allowed do parâmetro de configuração.

Isso permite que o SRTP seja usado para chamadas sobre esse tronco. Essa caixa deve ser marcada somente ao usar SIP TLS, pois as chaves para SRTP são trocadas no corpo da mensagem SIP. A sinalização SIP deve ser protegida pelo TLS porque qualquer pessoa com uma sinalização SIP não segura pode descriptografar o fluxo RTP seguro correspondente no tronco.

**Trunk Configuration**

Save Delete Reset Add New

**SIP Trunk Status**

Service Status: Unknown - OPTIONS Ping not enabled  
Duration: Unknown

**Device Information**

Product: SIP Trunk  
Device Protocol: SIP  
Trunk Service Type: None(Default)  
Device Name\*: CUCMA  
Description:  
Device Pool\*: HQ  
Common Device Configuration: < None >  
Call Classification\*: Use System Default  
Media Resource Group List: < None >  
Location\*: Hub\_None  
AAR Group: < None >  
Tunneled Protocol\*: None  
QSIG Variant\*: No Changes  
ASN.1 ROSE OID Encoding\*: No Changes  
Packet Capture Mode\*: None  
Packet Capture Duration: 0

Media Termination Point Required  
 Retry Video Call as Audio  
 Path Replacement Support  
 Transmit UTF-8 for Calling Party Name  
 Transmit UTF-8 Names in QSIG APDU  
 Unattended Port  
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.  
Consider Traffic on This Trunk Secure\* When using both sRTP and TLS

## 2. Na seção SIP Information da janela SIP Trunk Configuration, adicione o Destination IP Address, Destination Port e Security Profile

**SIP Information**

**Destination**

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.95.203		5061

MTP Preferred Originating Codec\*: 711ulaw  
BLF Presence Group\*: Standard Presence group  
SIP Trunk Security Profile\*: Secure SIP Trunk Profile TLS  
Rerouting Calling Search Space: < None >  
Out-Of-Dialog Refer Calling Search Space: < None >  
SUBSCRIBE Calling Search Space: < None >  
SIP Profile\*: Standard SIP Profile [View Details](#)  
DTMF Signaling Method\*: No Preference

Etapa 10. Criar padrões de rota O método mais simples é criar um padrão de rota em cada cluster, apontando diretamente para o tronco SIP. Grupos de rota e listas de rota também podem ser usados. CUCM 9.1(2) aponta para o padrão de rota 9898 através do tronco SIP TLS para o CUCM 10.5(2)

**Trunks (1 - 1 of 1)** Rows per Page 50

Find Trunks where Device Name begins with Find Clear Filter

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Security Profile
CUCM10			Default	9898				SIP Trunk	Secure SIP Trunk Profile TLS

Add New Select All Clear All Delete Selected Reset Selected

O CUCM 10.5(2) aponta para o padrão de rota 1018 através do tronco SIP TLS para o CUCM 9.1(2)

Trunks (1 - 1 of 1)										Rows per Page 50		
Find Trunks where Device Name <input type="text"/> begins with <input type="text"/> <input type="button" value="Find"/> <input type="button" value="Clear Filter"/> <input type="button" value="Add"/> <input type="button" value="Remove"/>										Select item or enter search text		
<input type="checkbox"/>	Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile
<input type="checkbox"/>	CUCMA			HQ	1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS
<input type="button" value="Add New"/> <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Delete Selected"/> <input type="button" value="Reset Selected"/>												

**Verificar** No momento, não há procedimento de verificação disponível para esta configuração. **Troubleshoot** A chamada TLS SIP pode ser depurada com estas etapas. **Coletar Captura de Pacotes no CUCM** Para verificar a conectividade entre o CUCM 9.1(2) e o CUCM 10.5(2), faça uma captura de pacotes nos servidores CUCM e observe o tráfego SIP TLS. O tráfego SIP TLS é transmitido na porta TCP 5061, vista como sip-tls. No exemplo a seguir, há uma sessão CLI SSH estabelecida para o CUCM 9.1(2). 1. Captura de pacote CLI na tela Essa CLI imprime a saída na tela do tráfego SIP TLS.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. Capturas CLI para arquivo Essa CLI faz a captura de pacotes com base no host e cria um arquivo chamado packets.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
Reinicie o tronco SIP no CUCM 9.1(2) e faça a chamada do ramal 1018 (CUCM 9.1(2)) para o ramal 9898 (CUCM 10.5(2)) Para baixar o arquivo da CLI, execute este comando:
admin:file get activelog platform/cli/packets.cap
```

A captura é feita no formato padrão .cap. Este exemplo usa o Wireshark para abrir o arquivo packets.cap, mas qualquer ferramenta de exibição de captura de pacote pode ser usada.

Time	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	sip-tls > 33135 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
18:46:11.313706	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=156761672
18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=156761672
18:46:11.430454	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1643 Win=11648 Len=0 TSval=156761672
18:46:11.450926	10.106.95.203	10.106.95.200	TCP	1514	[TCP segment of a reassembled PDU]
18:46:11.450969	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988679
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Change Compression
18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988679
18:46:11.461558	10.106.95.200	10.106.95.203	TLSv1	1200	New Session Ticket, Change Cipher Spec, Finished
18:46:11.463062	10.106.95.203	10.106.95.200	TLSv1	1161	Application Data
18:46:11.502380	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=2777 Ack=3043 Win=23168 Len=0 TSval=988679
18:46:11.784432	10.106.95.200	10.106.95.203	TLSv1	440	Application Data
18:46:11.824821	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=3151 Win=17536 Len=0 TSval=156761672
18:46:12.187974	10.106.95.200	10.106.95.203	TLSv1	1024	Application Data
18:46:12.188452	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=4109 Win=20352 Len=0 TSval=156761672
18:46:15.288860	10.106.95.203	10.106.95.200	TLSv1	1466	Application Data
18:46:15.289237	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=5509 Win=23296 Len=0 TSval=156761672
18:46:15.402901	10.106.95.203	10.106.95.200	TLSv1	770	Application Data

1. A Sincronização (SYN) do Transmission Control Protocol (TCP) para estabelecer a comunicação TCP entre o CUCM 9.1(2)(Client) e o CUCM 10.5(2)(Server).
2. O CUCM 9.1(2) envia o Hello do cliente para iniciar a sessão TLS.
3. O CUCM 10.5(2) envia a solicitação de saudação, certificado e certificado do servidor para iniciar o processo de troca de certificado.
4. O certificado que o cliente CUCM 9.1(2) envia para concluir a troca de certificado.
5. Os Dados do Aplicativo que é a sinalização SIP criptografada mostram que a sessão TLS foi estabelecida.

Verificar ainda se os certificados corretos são trocados. Depois do Servidor Hello, o servidor

## CUCM 10.5(2) envia seu certificado ao cliente CUCM 9.1(2).

No.	Time	Source	Destination	Protocol	Length	Info
4	2015-05-23 18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
5	2015-05-23 18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
6	2015-05-23 18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
7	2015-05-23 18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
8	2015-05-23 18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=15676

```

Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1560
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1556
    Certificates Length: 1553
  Certificates (1553 bytes)
    Certificate Length: 902
  Certificate (id-at-commonName=CUCM10,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
    signedCertificate
      version: v3 (2)
      serialNumber : 0x398b1da600000000000e
      signature (shaWithRSAEncryption)
      issuer: rdnSequence (0)
      validity
      subject: rdnSequence (0)
      subjectPublicKeyInfo
      extensions: 6 items
  algorithmIdentifier (shaWithRSAEncryption)
  
```

O número de série e as informações de assunto que o servidor CUCM 10.5(2) possui são apresentadas ao cliente CUCM 9.1(2). O número de série, o assunto, o emissor e as datas de validade são todos comparados às informações na página Gerenciamento de Certificados do Administrador do SO. O servidor CUCM 10.5(2) apresenta seu próprio certificado para verificação, agora ele verifica o certificado do cliente CUCM 9.1(2). A verificação acontece em ambas as direções.

Filter:	Source	Destination	Protocol	Length	Info
	18:40:11.450454	10.106.95.203	10.106.95.200	TCP	66 sip-tls > 33135 [ACK] Seq=59 Ack=1043 Win=11040 Len=0 TSval=1307010844 TSecr=9
	18:46:11.450926	10.106.95.203	10.106.95.200	TCP	1514 [TCP segment of a reassembled PDU]
	18:46:11.450969	10.106.95.200	10.106.95.203	TCP	66 sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988797 TSecr=156
	18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Fini
	18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66 sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988797 TSecr=156

```

Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1559
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1555
    Certificates Length: 1552
  Certificates (1552 bytes)
    Certificate Length: 901
  Certificate (id-at-commonName=CUCMA,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
    signedCertificate
      version: v3 (2)
      serialNumber : 0x197ad7e90000000000002
      signature (shaWithRSAEncryption)
      issuer: rdnSequence (0)
      validity
      subject: rdnSequence (0)
      subjectPublicKeyInfo
      extensions: 6 items
  algorithmIdentifier (shaWithRSAEncryption)
  
```

Se houver uma incompatibilidade entre os certificados na captura de pacote e os certificados na página da Web do administrador do SO, os certificados corretos não serão carregados. Os certificados corretos devem ser carregados na página Certificado do administrador do SO. Coletar rastreamentos do CUCM Os rastreamentos do CUCM também podem ser úteis para determinar quais mensagens são trocadas entre os servidores CUCM 9.1(2) e CUCM 10.5(2) e se a sessão SSL está ou não estabelecida corretamente. No exemplo, os rastreamentos do CUCM 9.1(2) foram coletados. Fluxo de chamada: Ext 1018 > CUCM 9.1(2) > TRONCO TLS SIP > CUCM 10.5(2) > Ext 9898++ Análise de dígitos

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018", plv="5", pss="", TodFilteredPss="", dd="9898", dac="0")
```

```
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
```

```
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
```

```
|CallingPartyNumber=1018
```

```
|DialingPartition=
```

```
|DialingPattern=9898
```

```
|FullyQualifiedCalledPartyNumber=9898
```

++ O SIP TLS está sendo usado na porta 5061 para esta chamada.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
```

```
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPtcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

A mensagem de Camada de Distribuição de Sinal ++ (SDL - Signal Distribution Layer) SIPCertificateInd fornece detalhes sobre a CN do assunto e informações de conexão.

```
04530218.000 |19:59:21.323 |sdlSig |SIPCertificateInd |wait
|SIPHandler(1,100,72,1) |SIPtcp(1,100,64,1)
|1,100,17,11.3^*** | [T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |sdlSig |SIPCertificateInd
|restart0 |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1) |1,100,17,11.3^*** | [R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```