使用CA签名证书在Communications Manager上配置SIP TLS中继

目录

简介

本文档介绍在Communications Manager上使用证书颁发机构(CA)签名证书配置会话初始协议(SIP)传输层安全(TLS)中继的分步过程。

本文档后，将使用TLS对两个集群之间的SIP消息进行加密。

先决条件

要求

思科建议您了解：

- 思科统一通信管理器 (CUCM)
- SIP

使用的组件

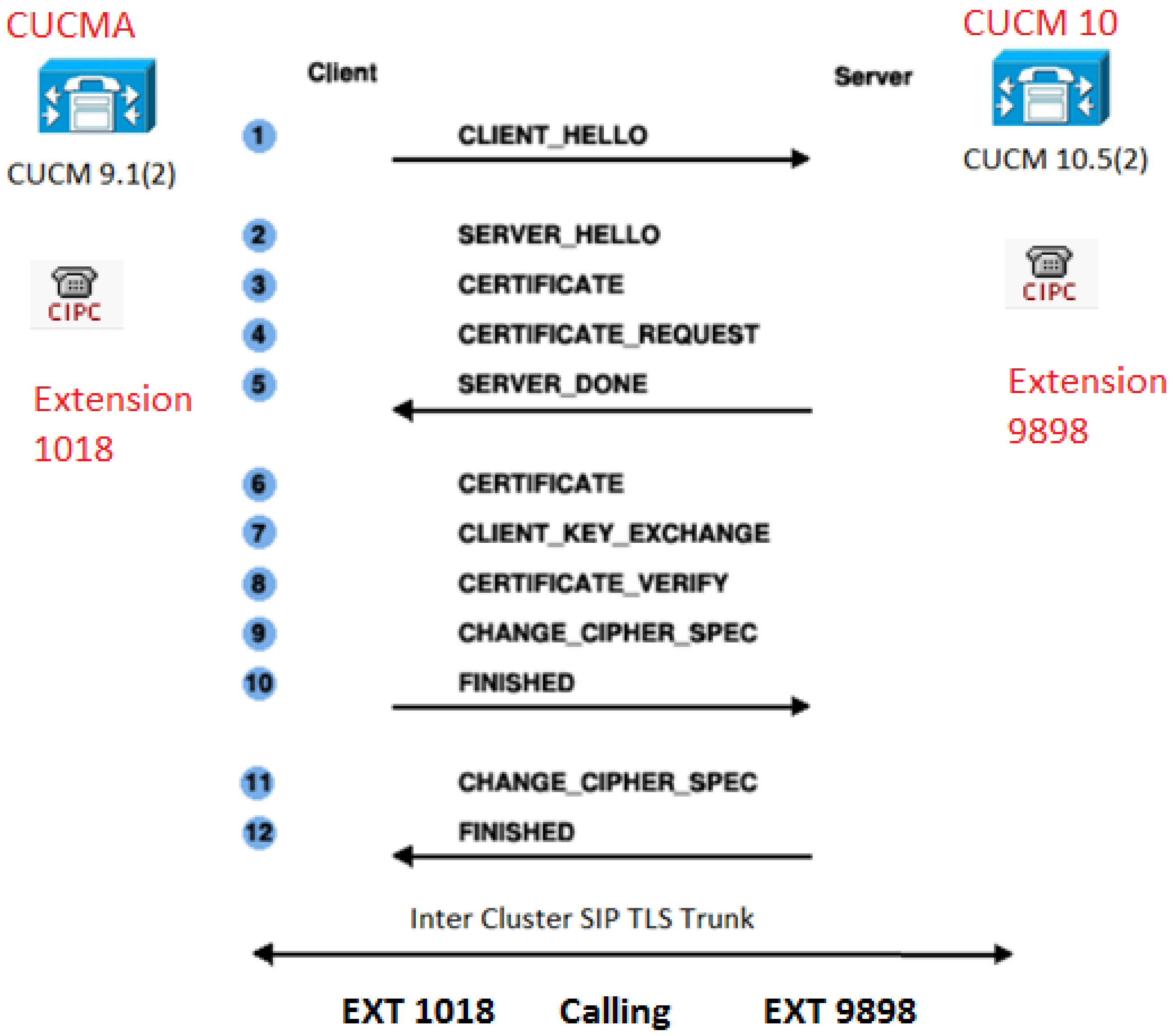
本文档中的信息基于以下软件版本：

- CUCM 版本 9.1(2)
- CUCM 版本 10.5(2)
- 作为CA的Microsoft Windows Server 2003

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

如本图所示，使用证书的SSL握手。



配置

步骤1.在Windows Server 2003上使用公共CA或设置CA

请参阅链接：在Windows 2003服务器上设置CA

步骤2.检验主机名和设置

证书基于名称。在开始之前，请确保名称正确。

```
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
```

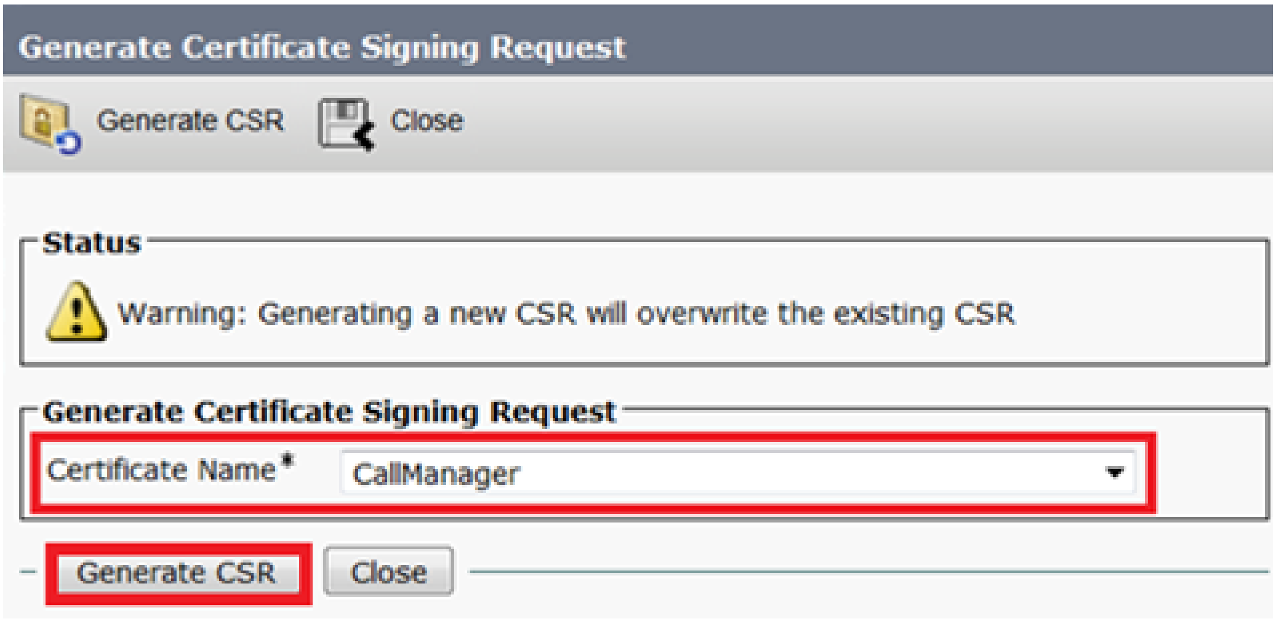
要更改主机名，请参阅链接：在CUCM上更改主机名

步骤3.生成并下载证书签名请求(CSR)

CUCM 9.1(2)

要生成CSR，请导航至OS Admin > **Security** > **Certificate Management** > **Generate CSR**

在“**证书名**”字**段中，从下**拉列**表中选择CallManager**选项。



Generate Certificate Signing Request

Status

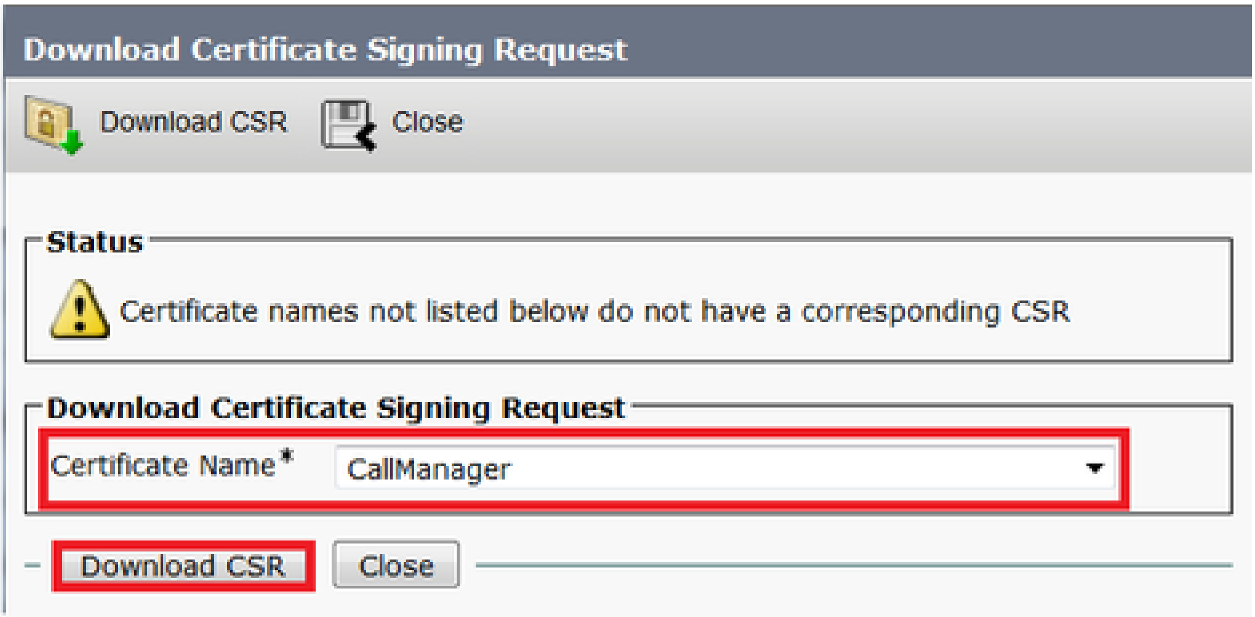
Warning: Generating a new CSR will overwrite the existing CSR

Generate Certificate Signing Request

Certificate Name* CallManager

要下载CSR，请导航至**OS Admin > Security > Certificate Management > Download CSR**

在“证**书名称**”字段中，从下拉列**表中选择CallManager**选项。



Download Certificate Signing Request

Status

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

Download Certificate Signing Request

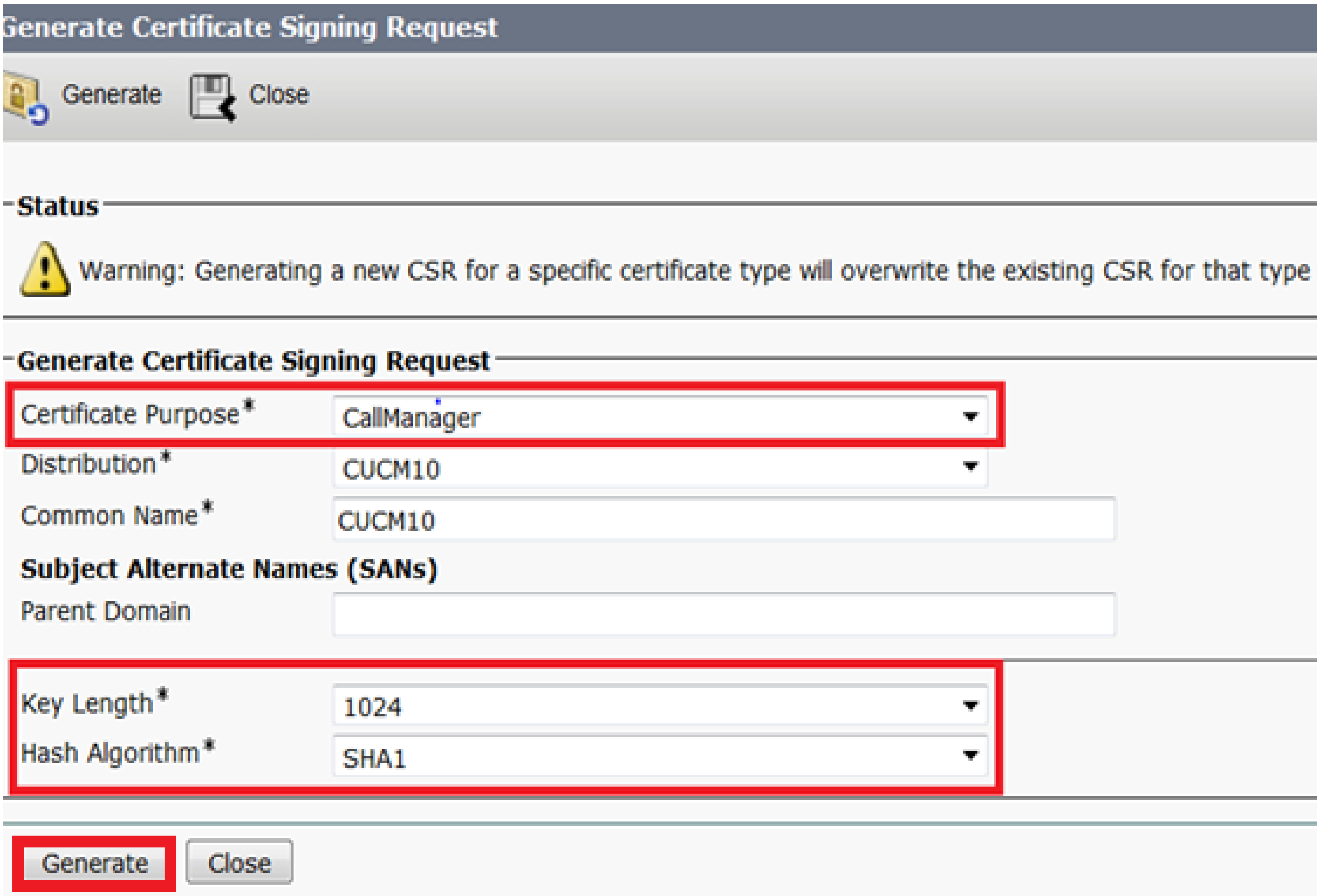
Certificate Name* CallManager

CUCM 10.5(2)

要生成CSR，请导航到OS Admin > Security > Certificate Management > Generate CSR

1.在“证书目的”字段中，从下拉列表中选择CallManager。

2.在“密钥长度”字段中,从下拉列表中选择1024。
3.在Hash Algorithm字段中，从下拉列表中选择SHA1。



Generate Certificate Signing Request

Status

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

Generate Certificate Signing Request

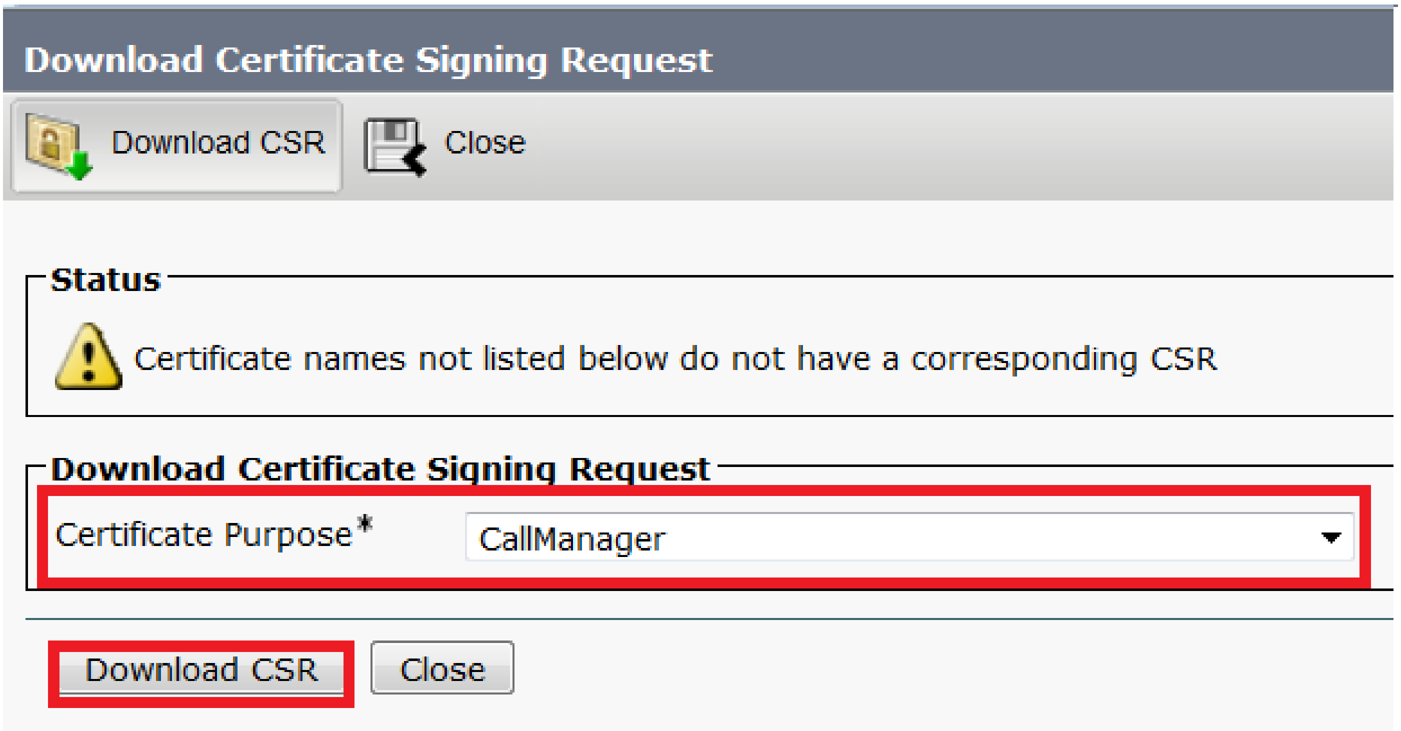
Certificate Purpose*	CallManager
Distribution*	CUCM10
Common Name*	CUCM10

Subject Alternate Names (SANs)

Parent Domain	
Key Length*	1024
Hash Algorithm*	SHA1

要下载CSR，请导航至**OS Admin > Security > Certificate Management > Download CSR**

在“**证书目**的”字**段中**，从下拉列表中选择**CallManager**选项。



Download Certificate Signing Request

Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

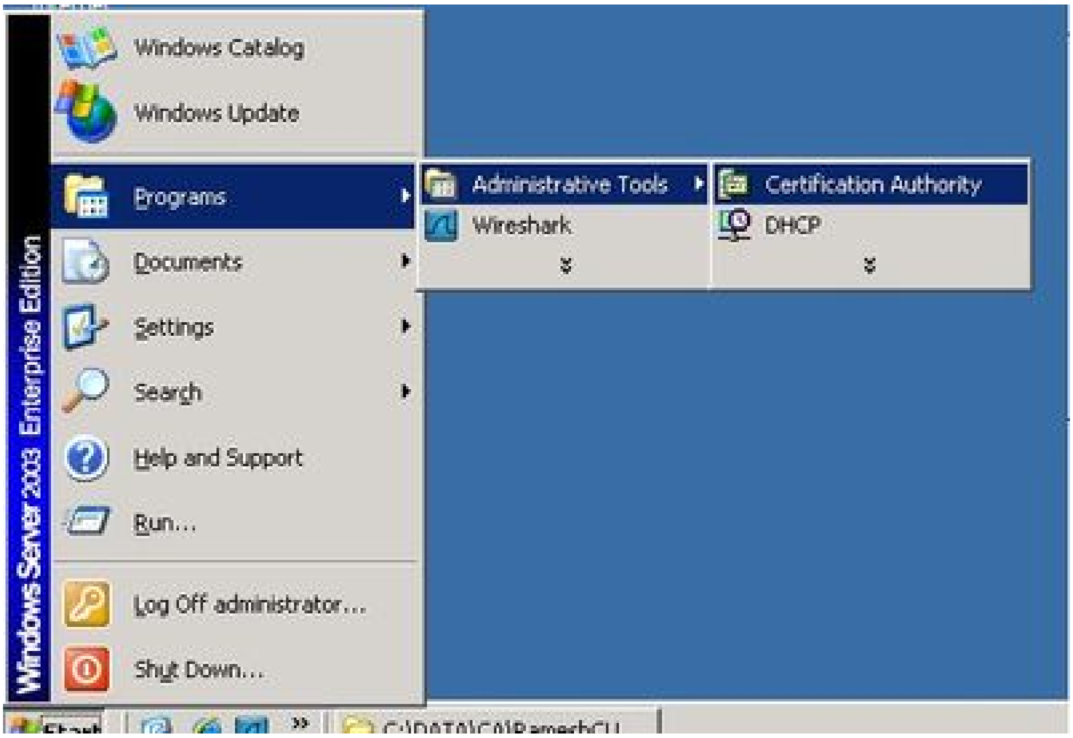
Certificate Purpose*	CallManager

注意：CallManager CSR使用1024位Rivest-Shamir-Addleman(RSA)密钥生成。

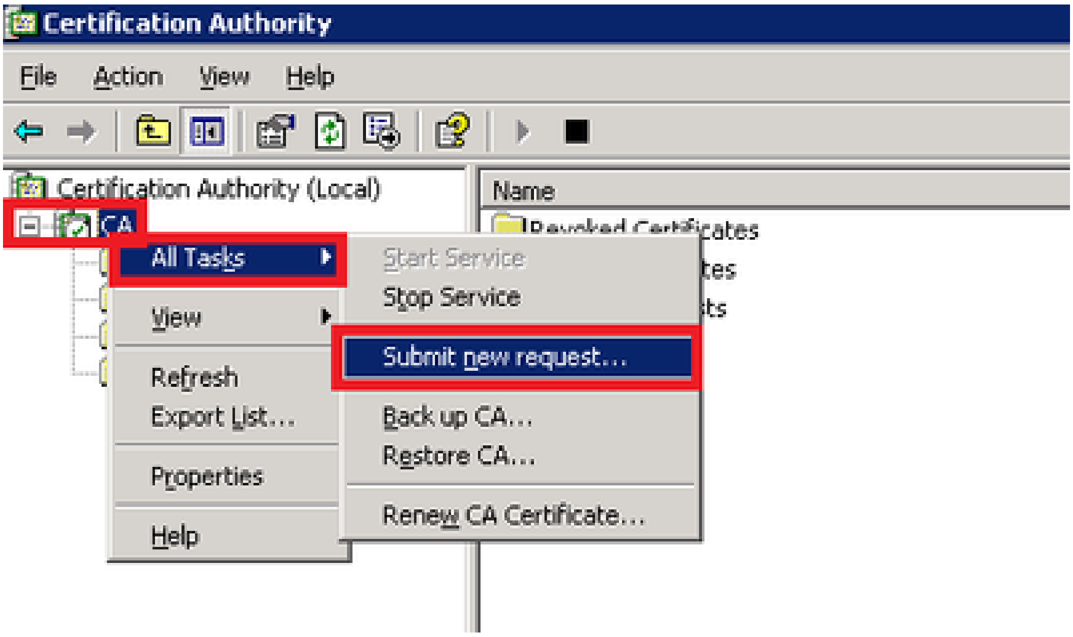
步骤4.使用Microsoft Windows 2003证书颁发机构签署CSR

这是使用Microsoft Windows 2003 CA签署CSR的可选信息。

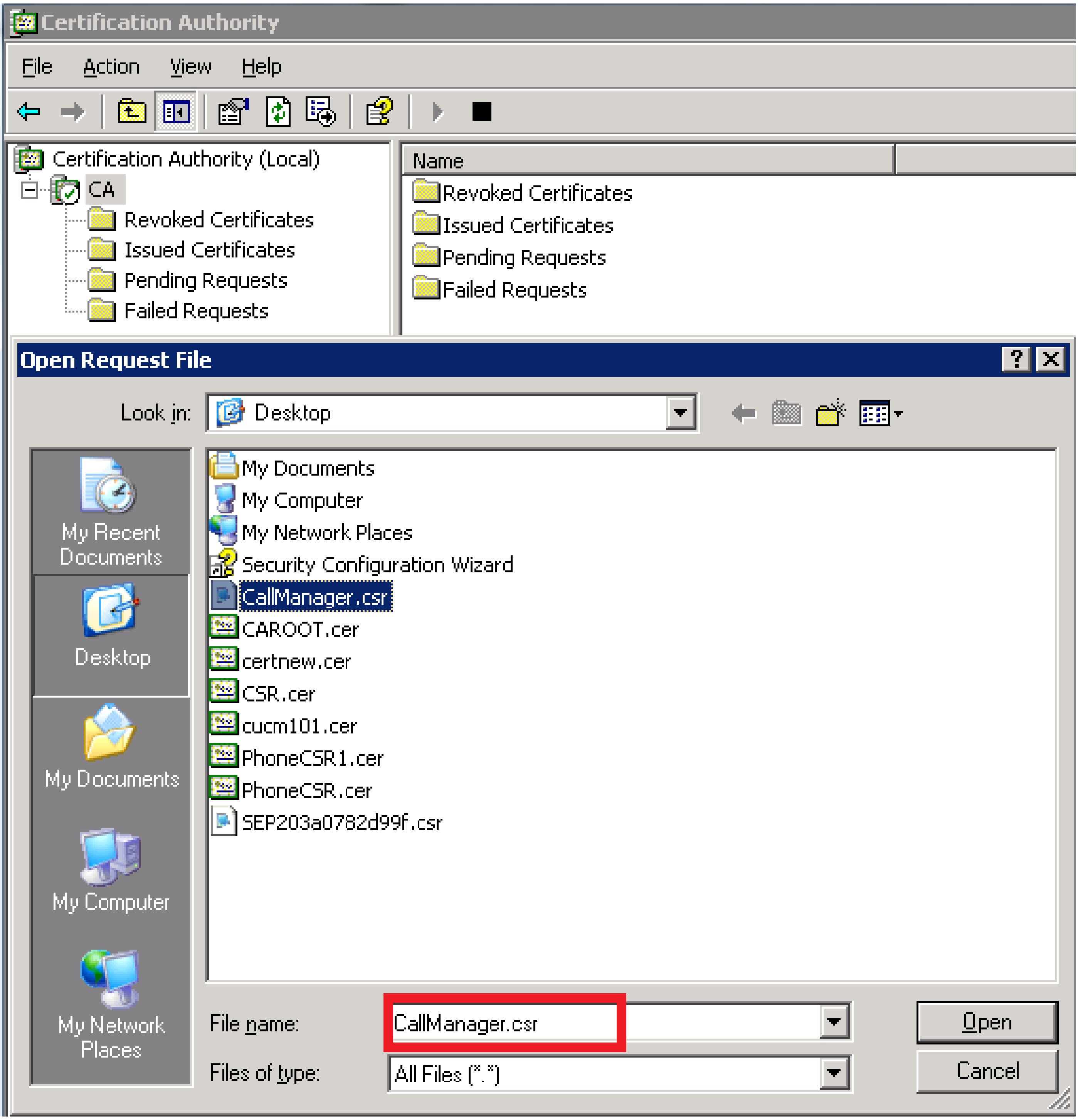
1.打开认证中心。



2.右键单击CA图**标，**然后导航至“**所有任务”>“提交新请求”**



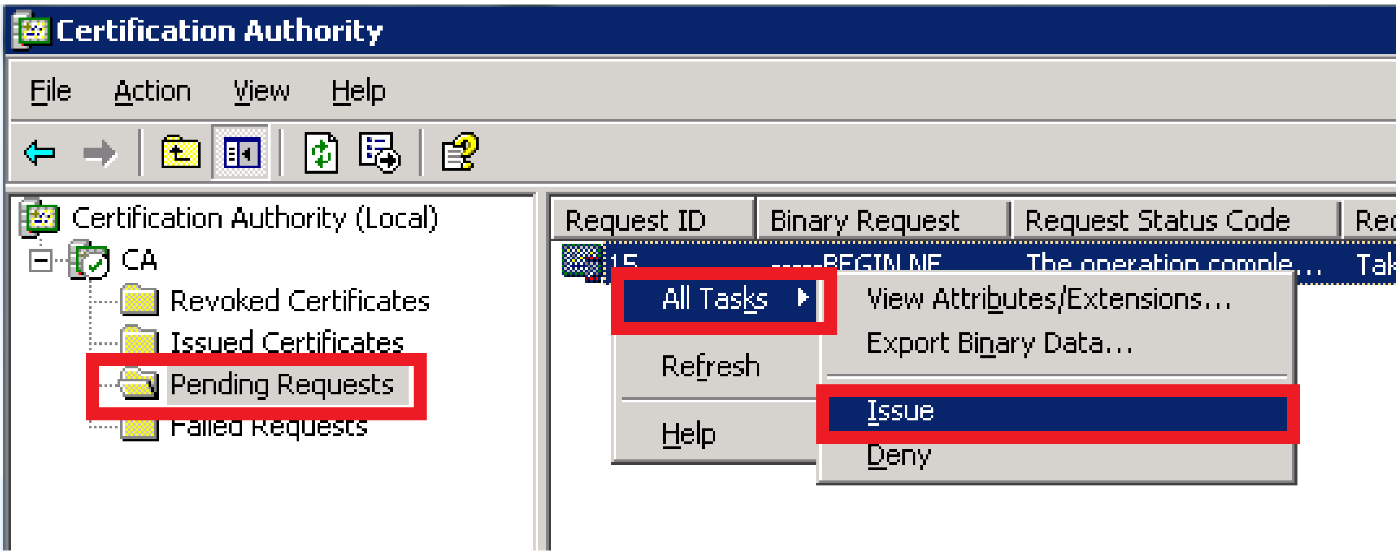
3.选择CSR并点击“打开”**选项**(适用于CSR(CUCM 9.1(2)和CUCM 10.5(2))



File name: CallManager.csr

Files of type: All Files (*.*)

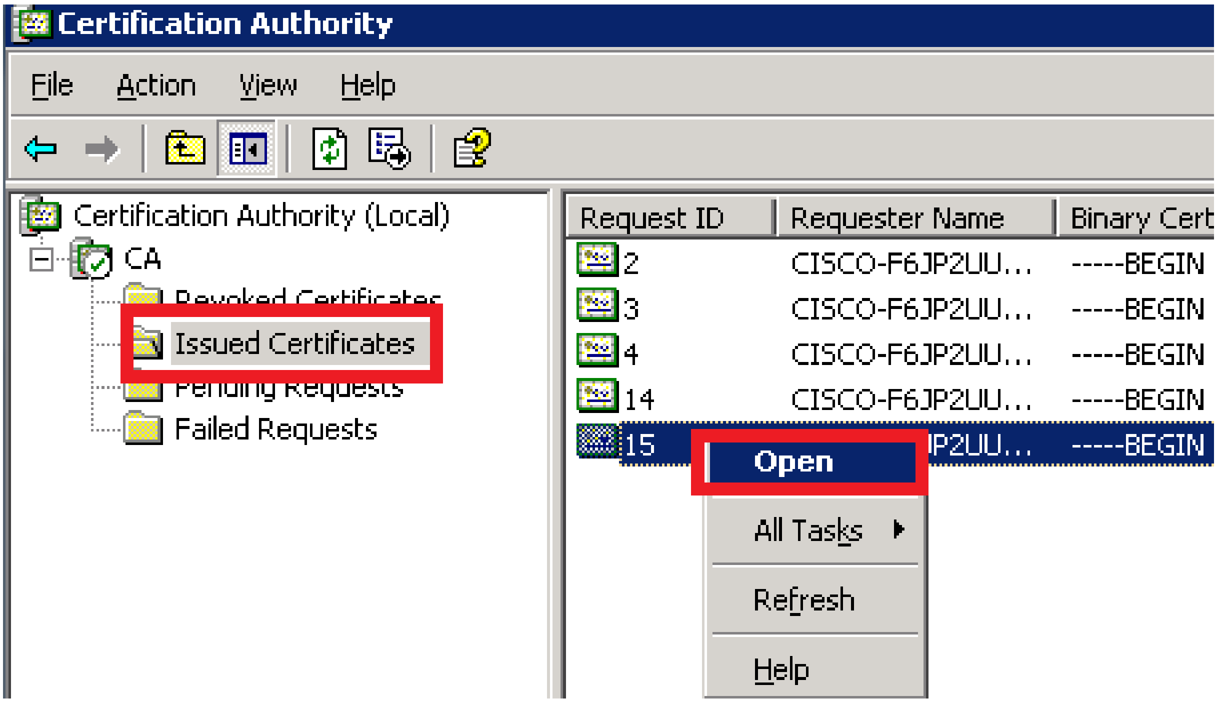
4.所有打开的CSR都显示在“待处理请求”文件夹中。右键单击每个CSR并导航到**All Tasks > Issue**以颁发证书。(适用于CSR(CUCM 9.1(2)和CUCM 10.5(2))



Request ID	Binary Request	Request Status Code	Rec
15	-----BEGIN NE	The operation comple...	Tak

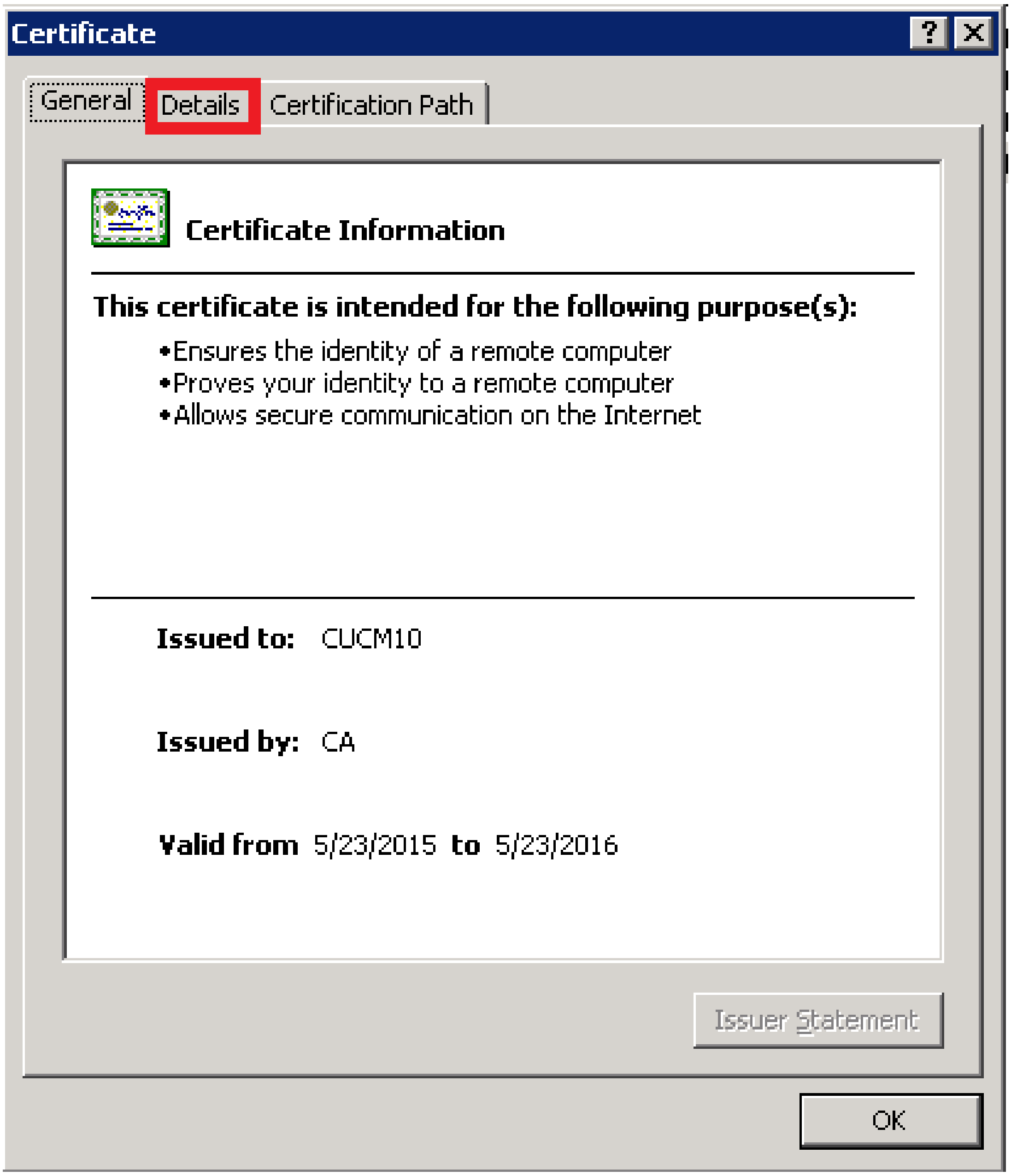
5.要下载证书，请选择“已颁发的证**书”文**件夹。

右键单击证书，然后单击“Open(**打开)**”选项。



Request ID	Requester Name	Binary Cert
2	CISCO-F6JP2UU...	-----BEGIN
3	CISCO-F6JP2UU...	-----BEGIN
4	CISCO-F6JP2UU...	-----BEGIN
14	CISCO-F6JP2UU...	-----BEGIN
15	P2UU...	-----BEGIN

6.将显示证书详细信息。要下载证书，请选择“详细信**息”**选项卡，然后单击“**复制到文件......”按钮**



This certificate is intended for the following purpose(s):

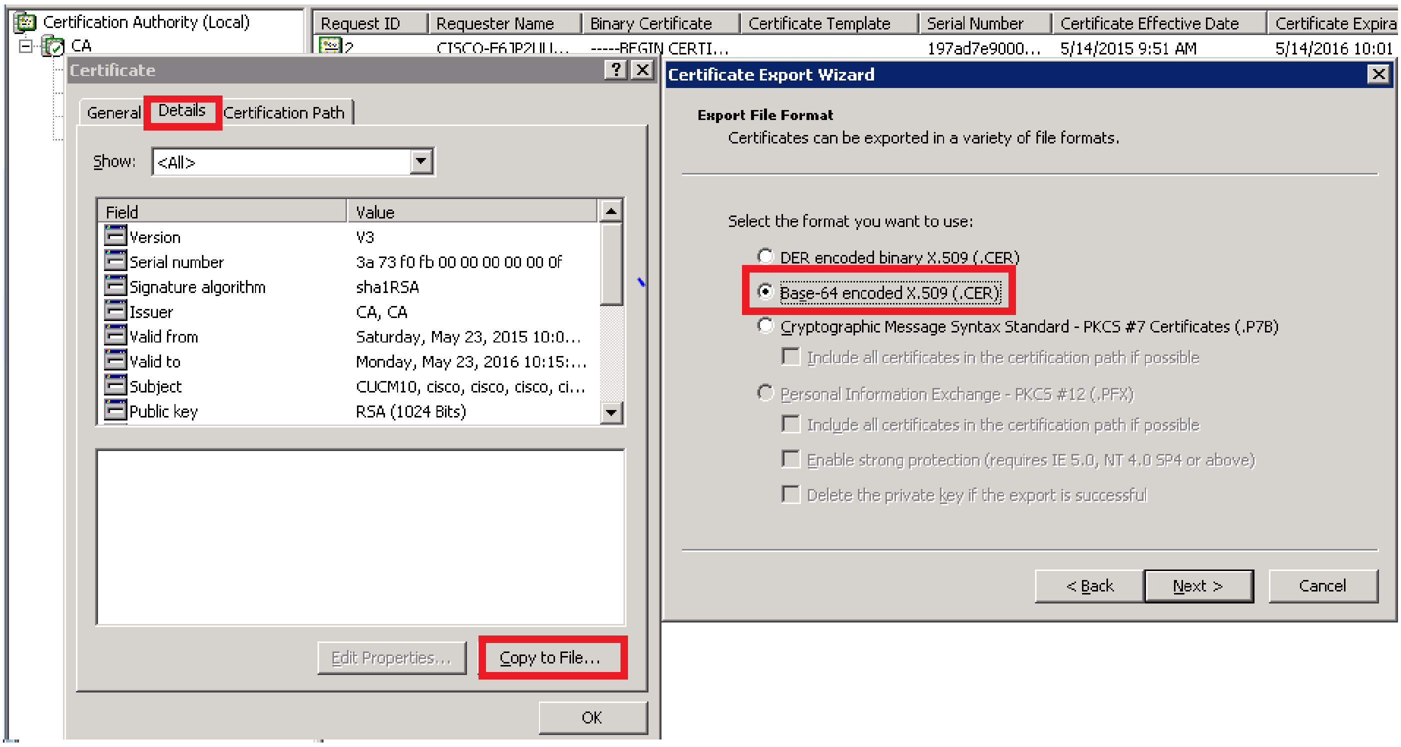
- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Allows secure communication on the Internet

Issued to: CUCM10

Issued by: CA

Valid from 5/23/2015 to 5/23/2016

7.在“证书导出向导”窗口中，单击Base-64 encoded X.509(.CER)单选按钮。



Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expira
2	CISCO-F6JP2UI...	-----BEGIN CERTI...		197ad7e9000...	5/14/2015 9:51 AM	5/14/2016 10:01

Certificate

Show: <All>

Field	Value
Version	V3
Serial number	3a 73 f0 fb 00 00 00 00 00 0f
Signature algorithm	sha1RSA
Issuer	CA, CA
Valid from	Saturday, May 23, 2015 10:0...
Valid to	Monday, May 23, 2016 10:15:...
Subject	CUCM10, cisco, cisco, cisco, ci...
Public key	RSA (1024 Bits)

Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

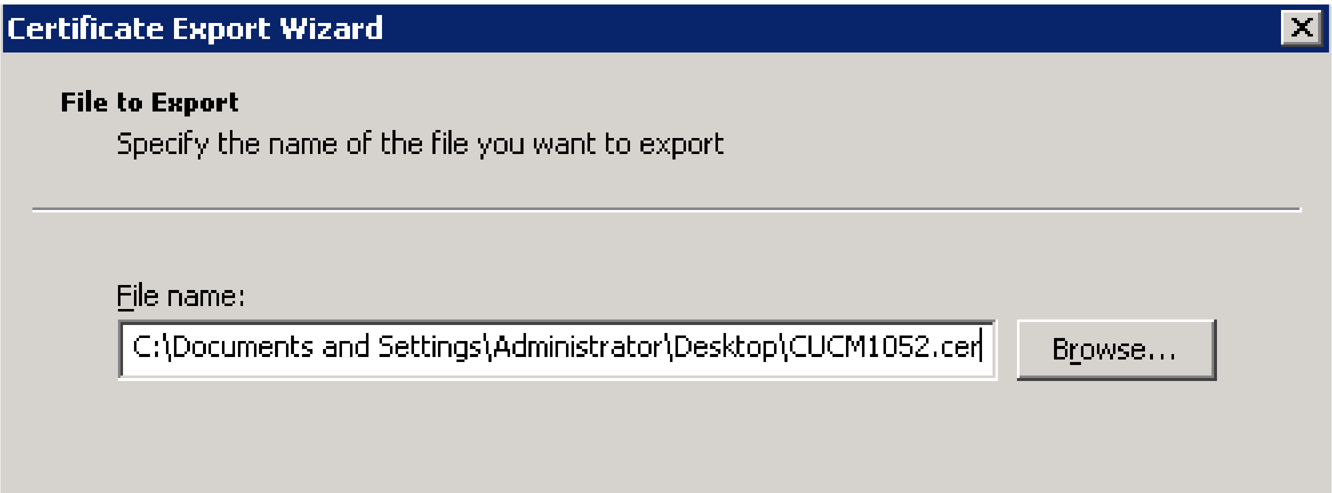
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

8.准确命名文件。此示例使用**CUCM1052.cer格**式。



Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Documents and Settings\Administrator\Desktop\CUCM1052.cer

对于CUCM 9.1(2)，请遵循相同的步骤。

步骤5.从CA获取根证书

打开“证**书颁发机**构”窗口。

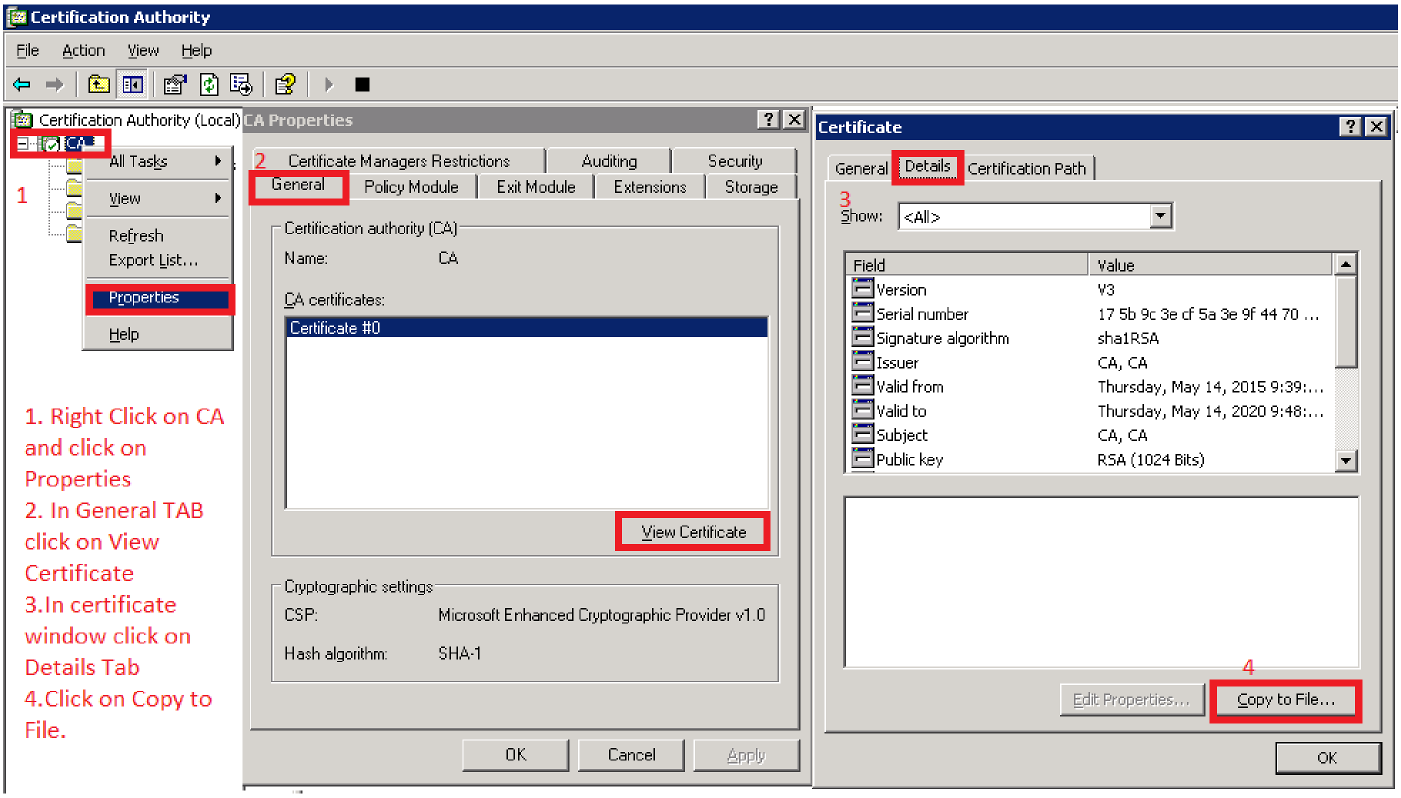
要下载根CA

1.右键单击CA图标，然后单击“属性”**选**项。

2.在常规TAB中，单击“查看证**书”。**

3.在“证书”**窗**口中，单击“详细信息”选项卡。

4.单击“复制到文件......”



1. Right Click on CA and click on Properties
2. In General TAB click on View Certificate
3.In certificate window click on Details Tab
4.Click on Copy to File.

Certification authority (CA)

Name: CA

CA certificates:

Certificate #0

Cryptographic settings

CSP: Microsoft Enhanced Cryptographic Provider v1.0

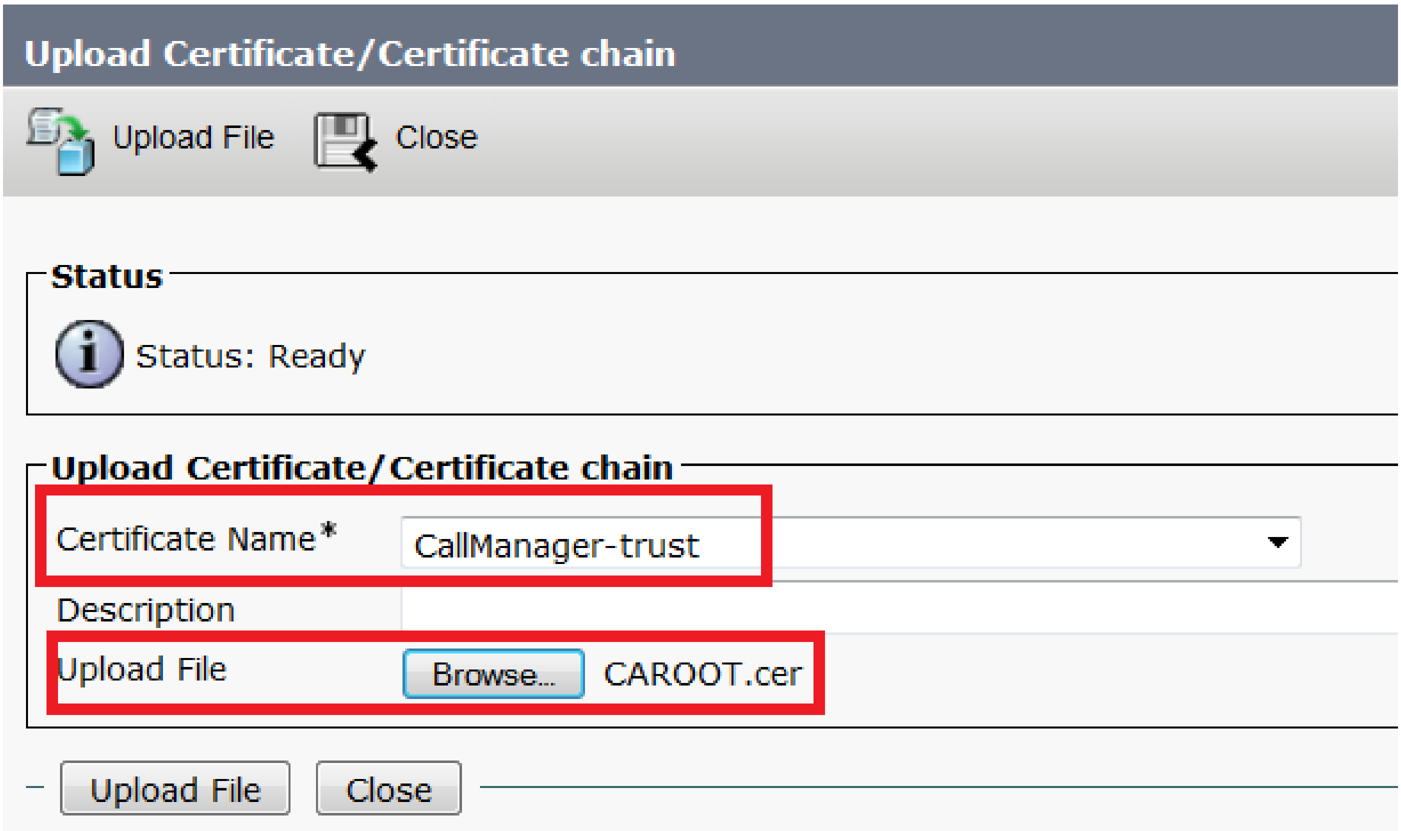
Hash algorithm: SHA-1

Show: <All>

Field	Value
Version	V3
Serial number	17 5b 9c 3e cf 5a 3e 9f 44 70 ...
Signature algorithm	sha1RSA
Issuer	CA, CA
Valid from	Thursday, May 14, 2015 9:39:...
Valid to	Thursday, May 14, 2020 9:48:...
Subject	CA, CA
Public key	RSA (1024 Bits)

步骤6.将CA根证书上传为CallManager信任

要上传CA根证书，请登录到**OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain**



Status

Status: Ready

Upload Certificate/Certificate chain

Certificate Name* CallManager-trust

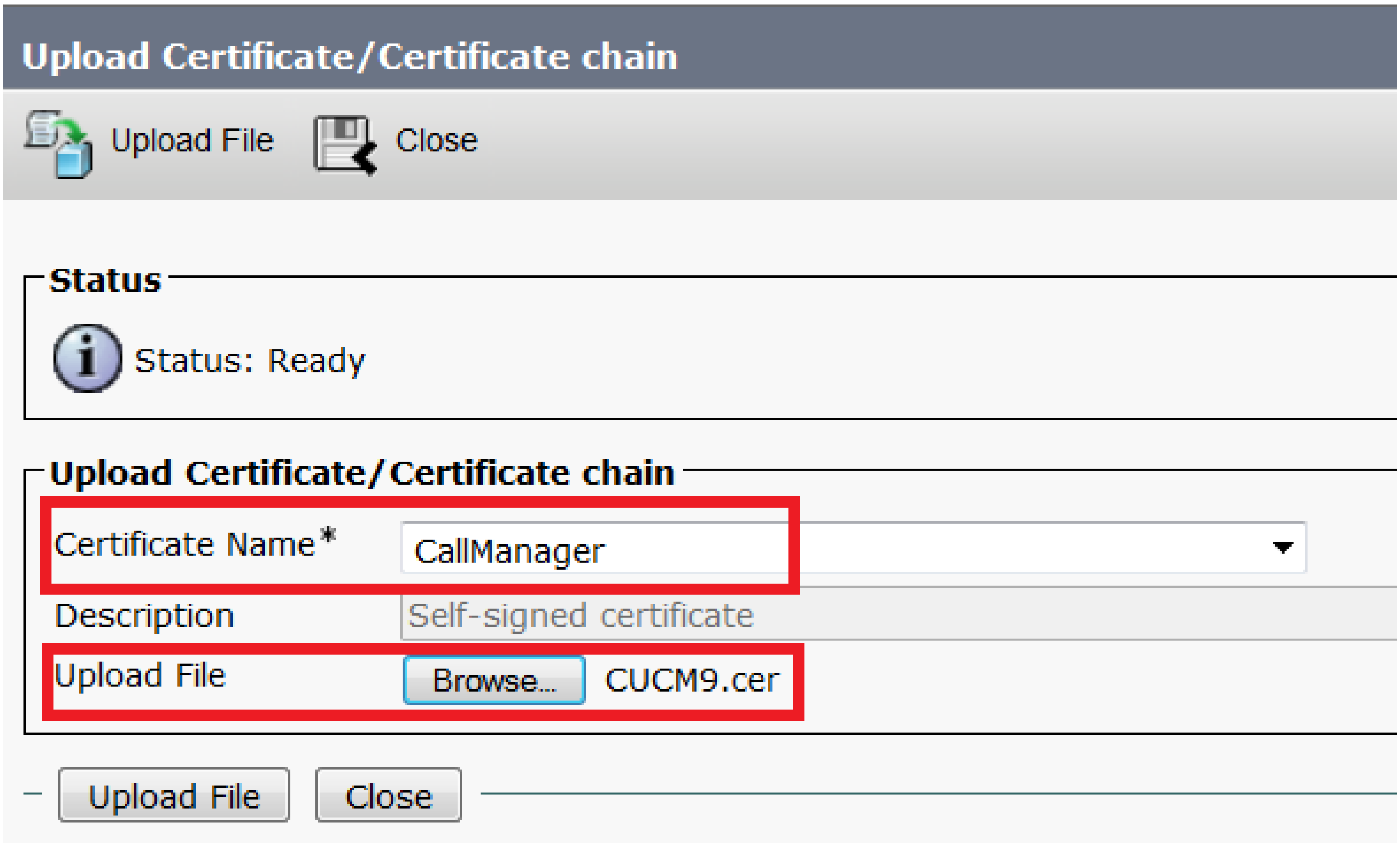
Description

Upload File CAROOT.cer

注意：在CUCM(CUCM 9.1(2)和CUCM 10.5(2))上执行以下步骤

步骤7.将CA签名CallManager CSR证书上传为CallManager证书。

要上传CA签名CallManager CSR，请登录**OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain**



Upload Certificate/Certificate chain

Status

Status: Ready

Upload Certificate/Certificate chain

Certificate Name*	CallManager
Description	Self-signed certificate
Upload File	Browse... CUCM9.cer

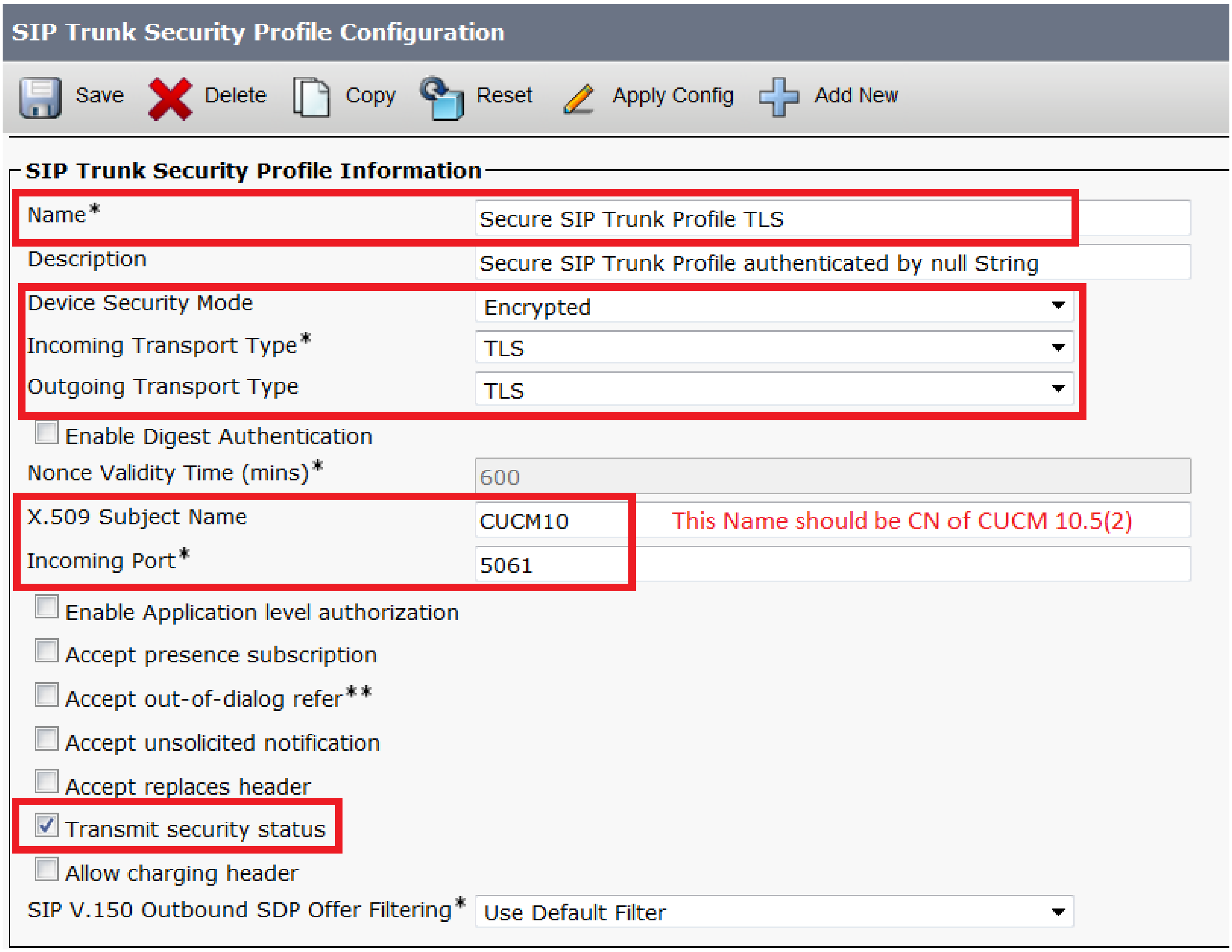
注意：在CUCM(CUCM 9.1(2)和CUCM 10.5(2))上执行以下步骤

步骤8.创建SIP中继安全配置文件

CUCM 9.1(2)

要创建SIP中继安全配置文件，请导航至**System > Security > SIP Trunk Security Profile**。

复制现有的非安全SIP中继配置文件并为其指定新名称。在示例中，已使用安全SIP中继配置文件TLS重命名非安全SIP中继配置文件。



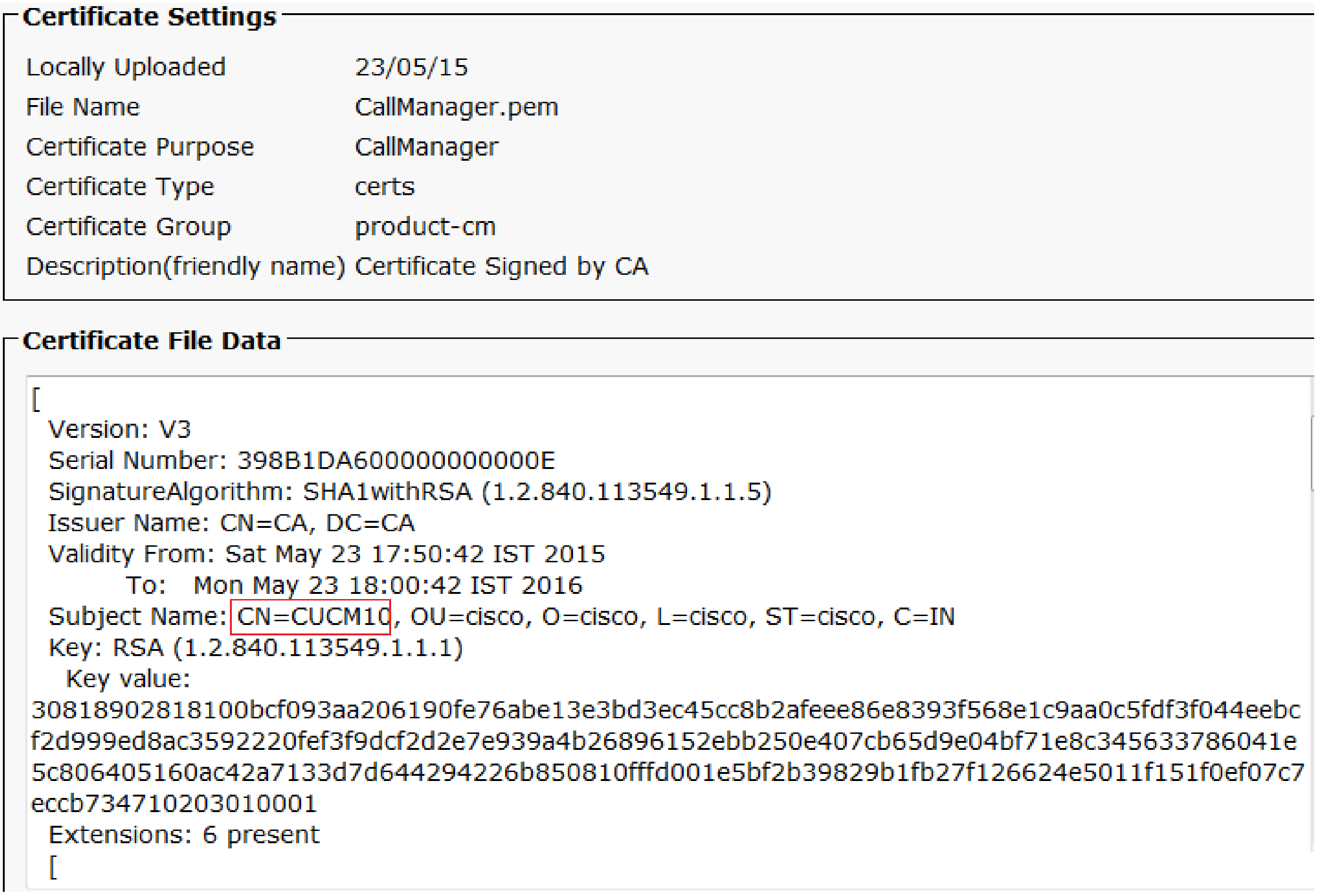
SIP Trunk Security Profile Configuration

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
☐ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUCM10
Incoming Port*	5061
☐ Enable Application level authorization	
☐ Accept presence subscription	
☐ Accept out-of-dialog refer**	
☐ Accept unsolicited notification	
☐ Accept replaces header	
☑ Transmit security status	
☐ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

This Name should be CN of CUCM 10.5(2)

在X.509主题名称中，使用CUCM 10.5(2)（CA签名证书）的公用名(CN)，如下图所示。



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

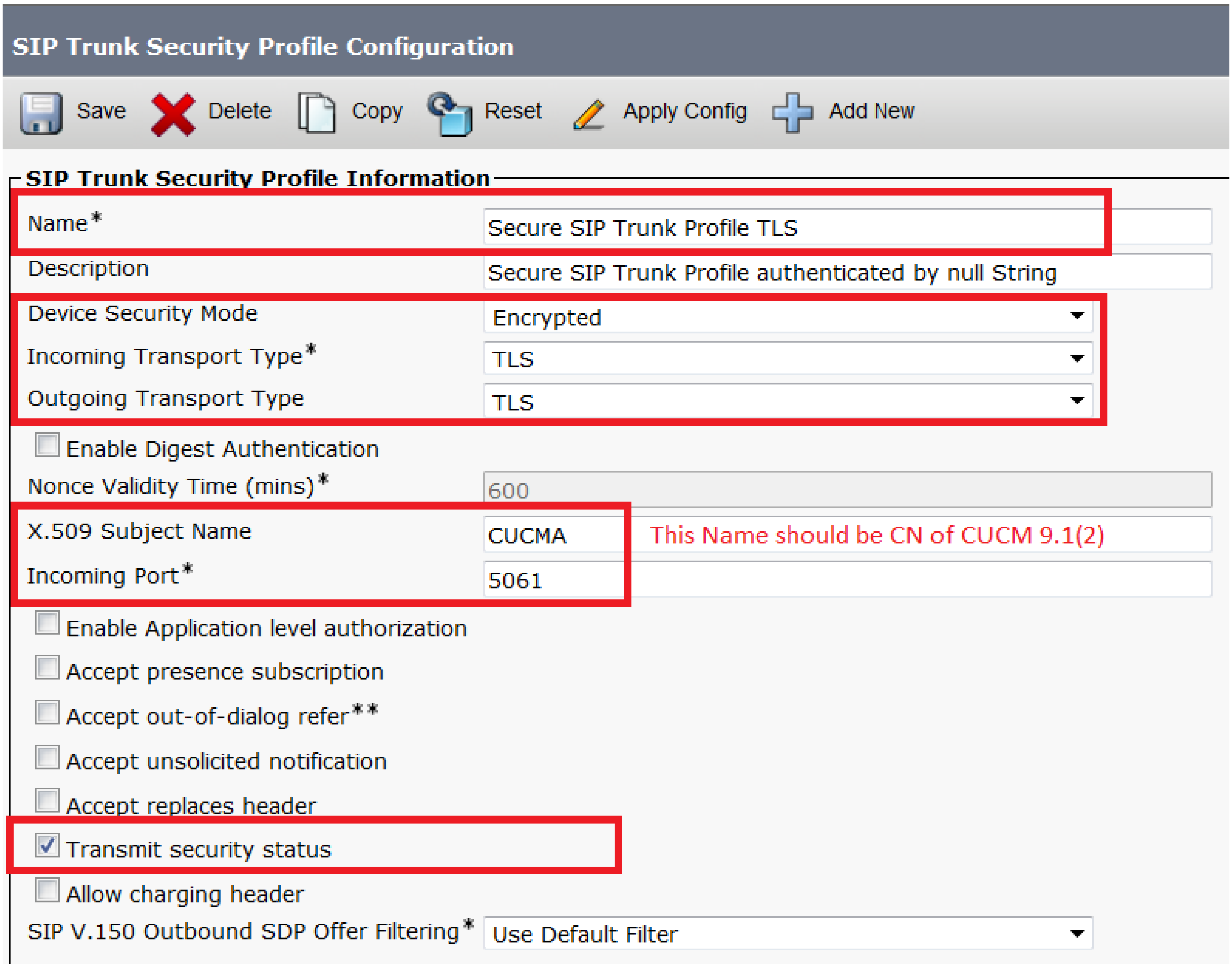
Certificate File Data

```
[
  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)

导航至System > Security > SIP Trunk Security Profile。

复制现有的非安全SIP中继配置文件并为其指定新名称。在示例中，使用安全SIP中继配置文件TLS重命名了非安全SIP中继配置文件。



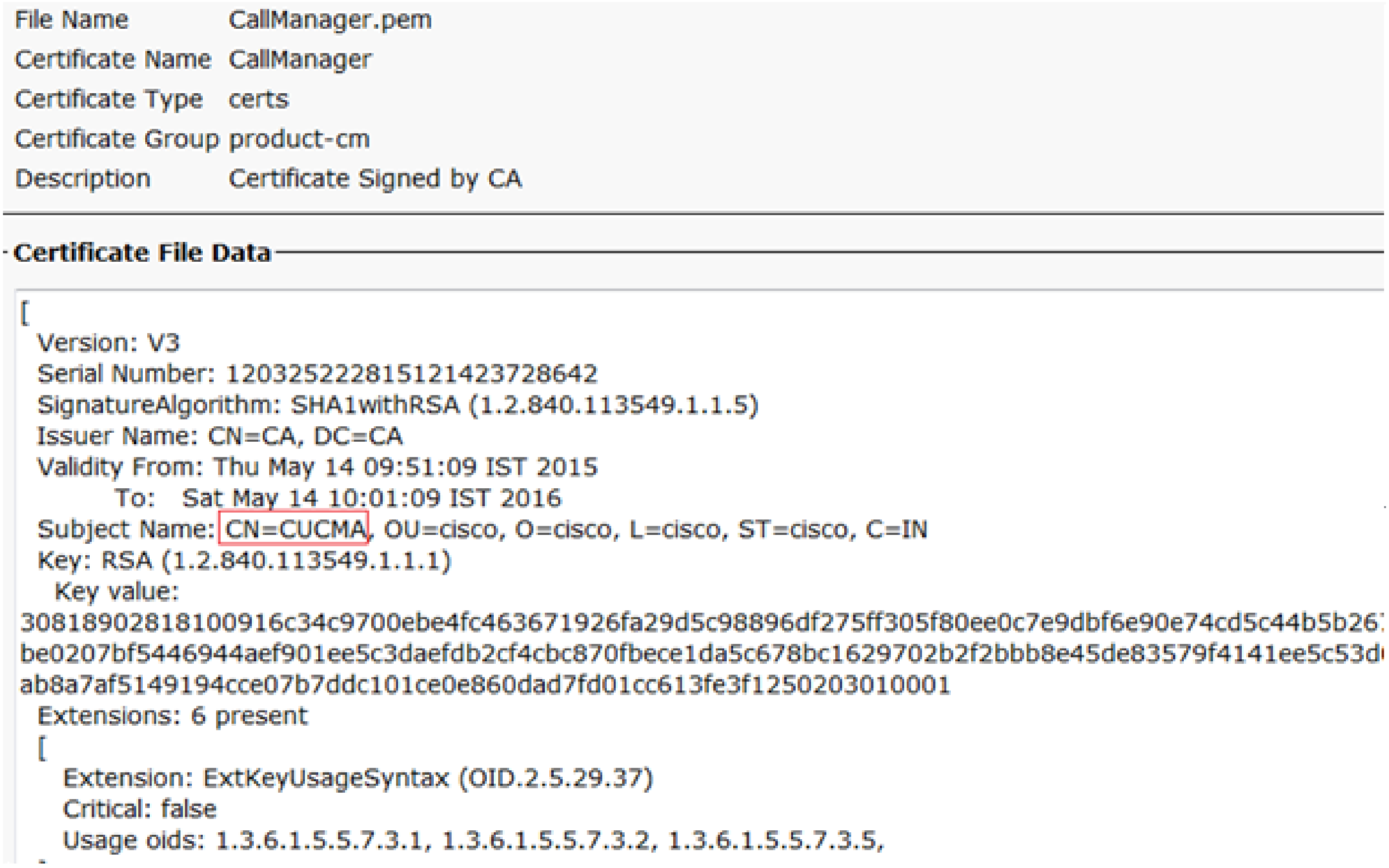
SIP Trunk Security Profile Configuration

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
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	CUCMA
Incoming Port*	5061
□ Enable Application level authorization	
□ Accept presence subscription	
□ Accept out-of-dialog refer**	
□ Accept unsolicited notification	
□ Accept replaces header	
☑ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

This Name should be CN of CUCM 9.1(2)

在X.509主题名称中，使用CUCM 9.1(2)（CA签名证书）的CN，如突出显示：



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
be0207bf5446944aef901ee5c3daefdb2cf4cbc870fbece1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d
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,
```

两个SIP中继安全配置文件都将传入端口设置为5061，其中每个集群在TCP端口5061上侦听新的入站SIP TLS呼叫。

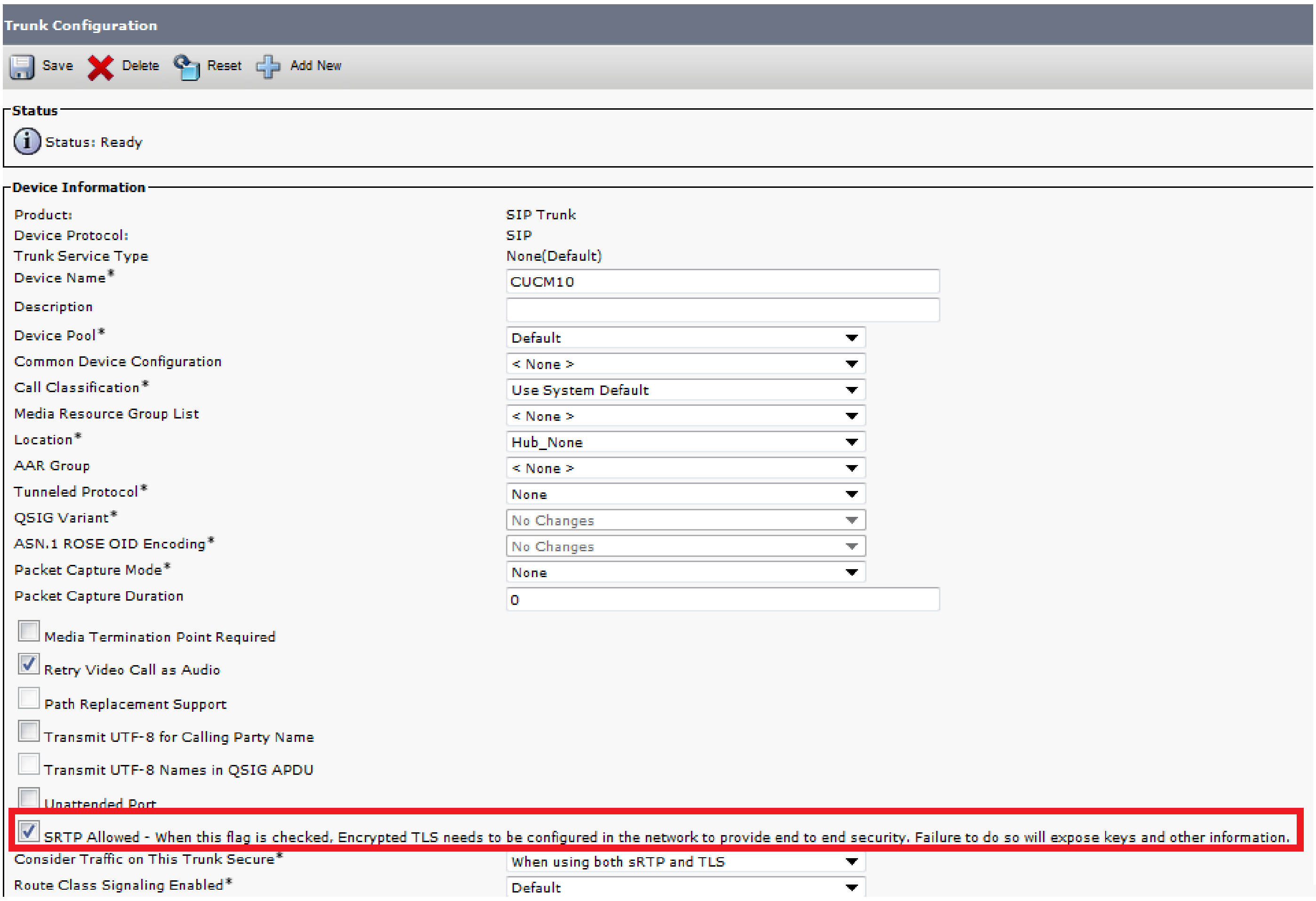
步骤9.创建SIP中继

创建安全配置文件后，创建SIP中继，并在SIP中继上更改以下配置参数。

CUCM 9.1(2)

1. 在SIP Trunk Configuration**(SIP中继**配置)窗口中，选中配置参数**SRTP Allowed(允许**SRTP)复选框。

这可确保用于此中继上呼叫的实时传输协议(RTP)的安全。只有在使用SIP TLS时，才必须选中此框，因为安全实时传输协议(SRTP)的密钥在SIP消息正文中交换。SIP信令必须由TLS保护，否则任何具有非安全SIP信令的人都可以通过中继解密相应的SRTP流。



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

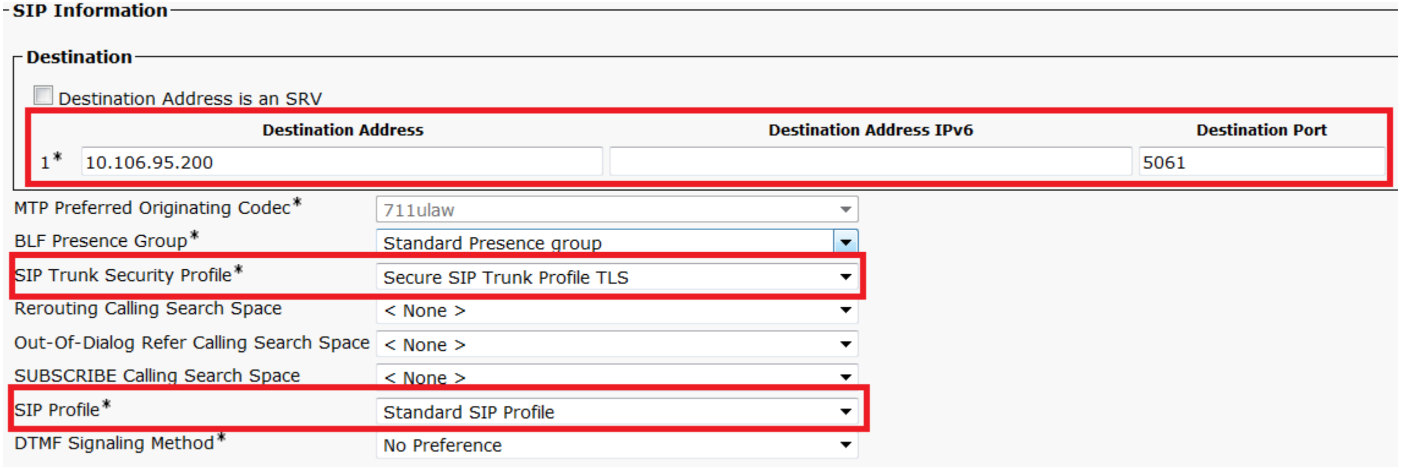
□ Transmit UTF-8 Names in QSIG APDU

□ 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. 在SIP中继**配置**窗口的**SIP信息部分**，添加**目标地址、目标端口**和**SIP中继安全配置文件。**



SIP Information

Destination

□ Destination Address is an SRV

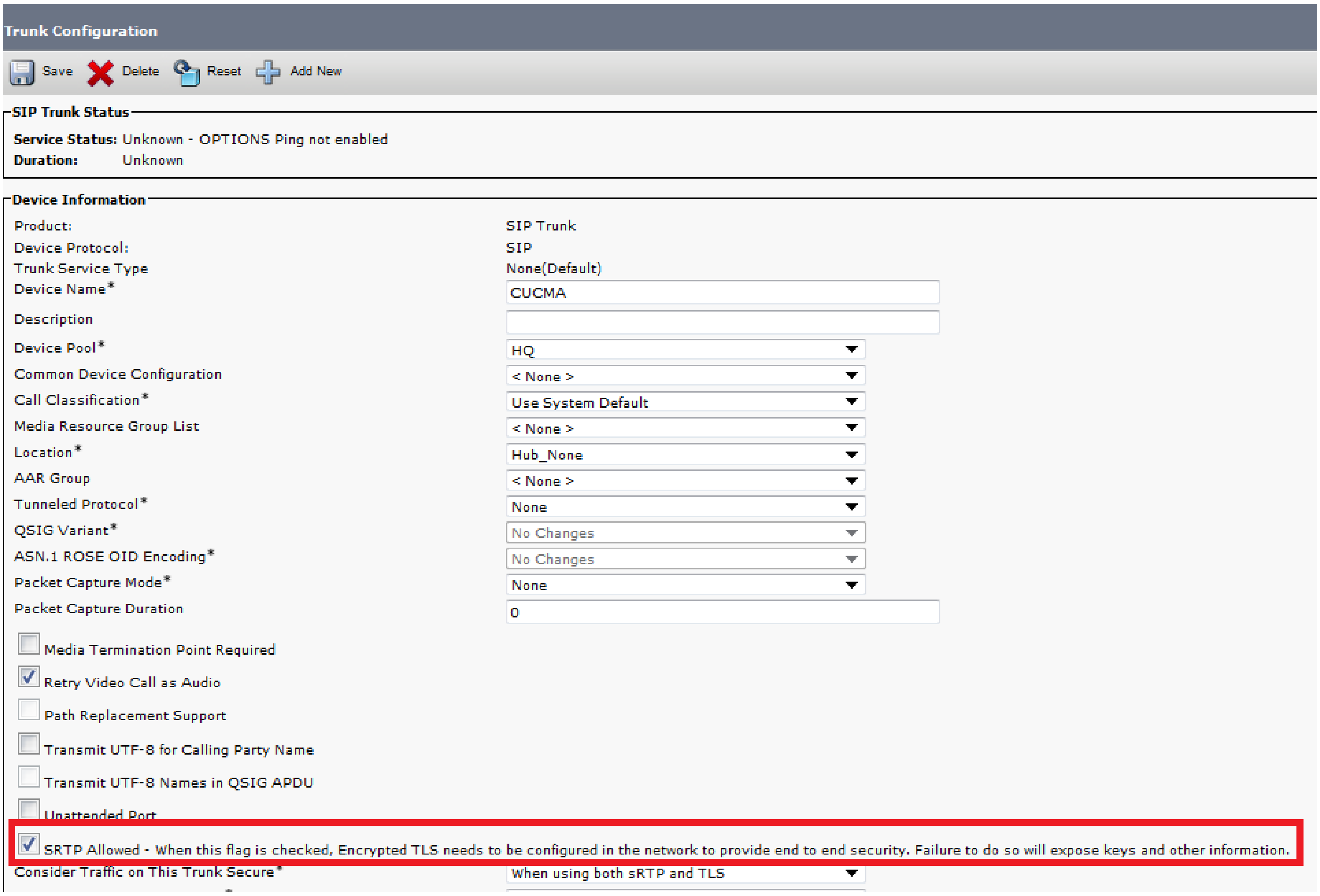
	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.200		5061

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. 在SIP Trunk Configuration(**SIP中继**配置)窗口中，选中配置参数**SRTP Allowed(允许**SRTP)复选框。

这允许SRTP用于通过此中继的呼叫。只有在使用SIP TLS时，才必须选中此框，因为SRTP的密钥在SIP消息的正文中交换。SIP信令必须由TLS保护，因为任何具有非安全SIP信令的人都可以通过中继解密相应的安全RTP流。



Trunk Configuration

SIP Trunk Status

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

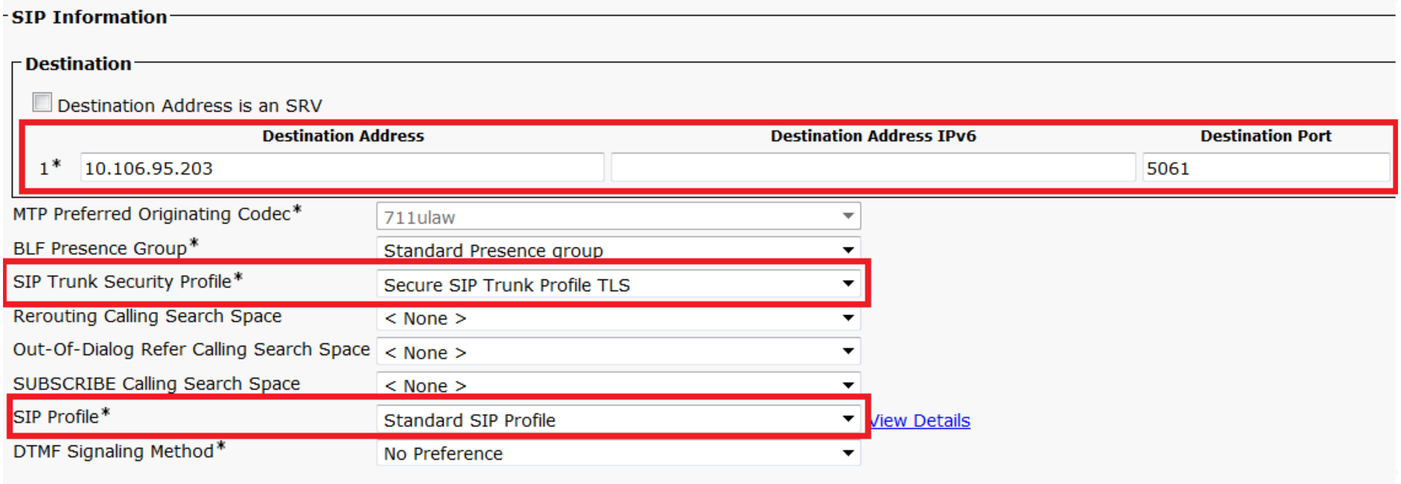
Device Information

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. 在SIP中继**配置**窗口的SIP信息**部分，添加目标IP地址、目标端口**和安全配置文件



SIP Information

Destination

□ Destination Address is an SRV

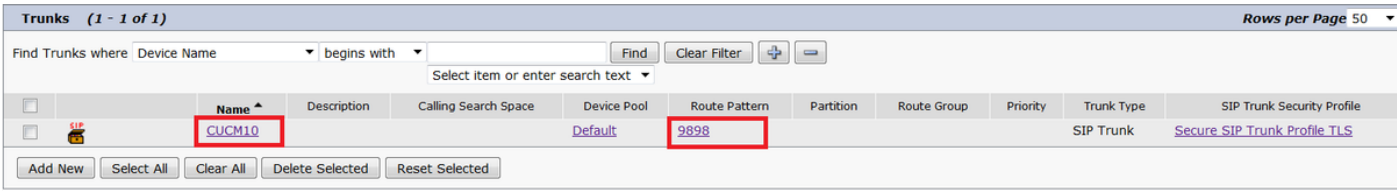
	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.203		5061

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
DTMF Signaling Method*	No Preference

步骤10.创建路由模式

最简单的方法是在每个集群上创建一个路由模式，直接指向SIP中继。还可以使用路由组和路由列表。

CUCM 9.1(2)通过TLS SIP中继**指向**路由模式9898到CUCM 10.5(2)

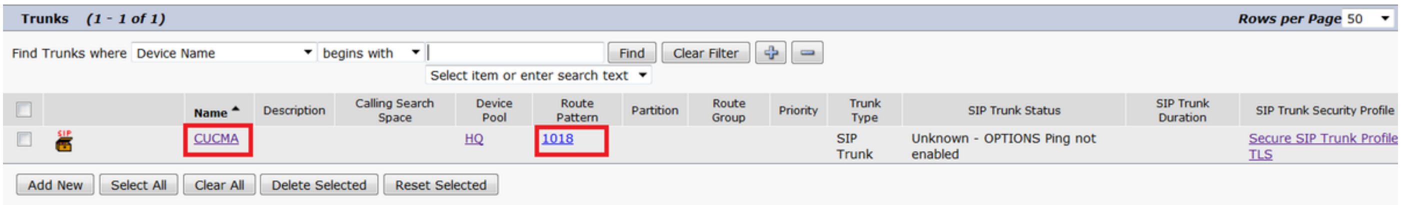


Trunks (1 - 1 of 1) **Rows per Page** 50

Find Trunks where Device Name begins with Select item or enter search text

□		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

CUCM 10.5(2)通过TLS SIP中继指向到CUCM 9.1(2)的路由模式1018



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

Find Trunks where Device Name begins with   Find Clear Filter

Select item or enter search text

□		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
□		CUCMA			HQ	1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS

验证

当前没有可用于此配置的验证过程。

故障排除

SIP TLS呼叫可通过以下步骤进行调试。

在CUCM上收集数据包捕获

要检查CUCM 9.1(2)和CUCM 10.5(2)之间的连接，请在CUCM服务器上捕获数据包并观察SIP TLS流量。

SIP TLS流量在TCP端口5061上传输，被视为sip-tls。

在以下示例中，与CUCM 9.1(2)建立了SSH CLI会话

1.屏幕上的CLI数据包捕获

此CLI在屏幕上显示SIP TLS流量的输出。

```
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. CLI捕获到文件

此CLI根据主机执行数据包捕获并创建名为packets的文件。

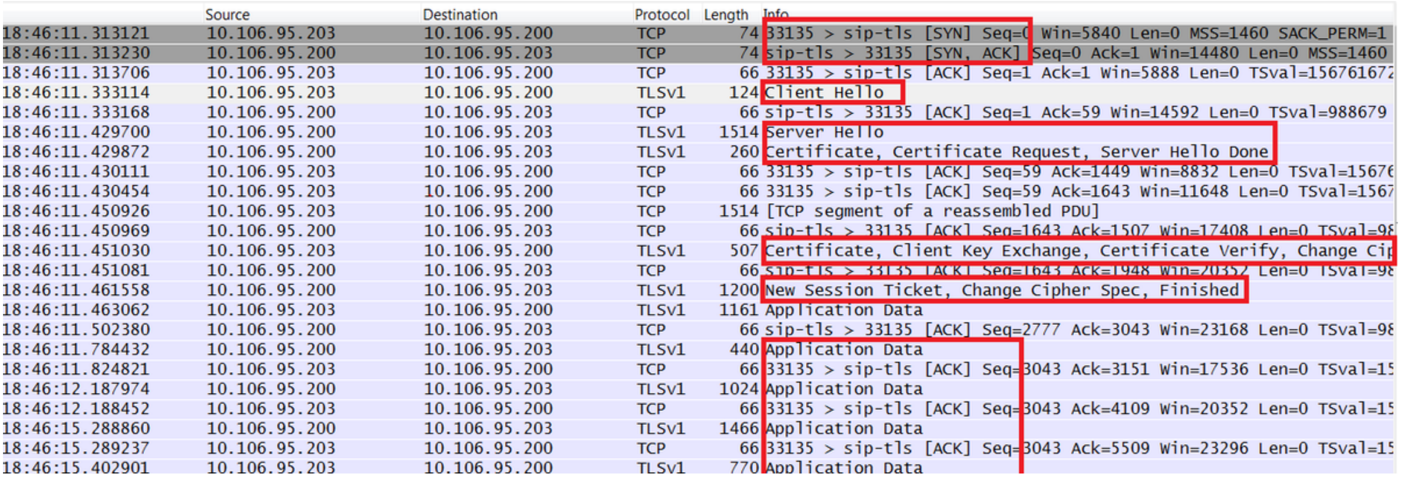
```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

在CUCM 9.1(2)上重新启动SIP中继，并从分机1018(CUCM 9.1(2))呼叫分机9898(CUCM 10.5(2))

要从CLI下载文件，请运行以下命令：

```
admin:file get activelog platform/cli/packets.cap
```

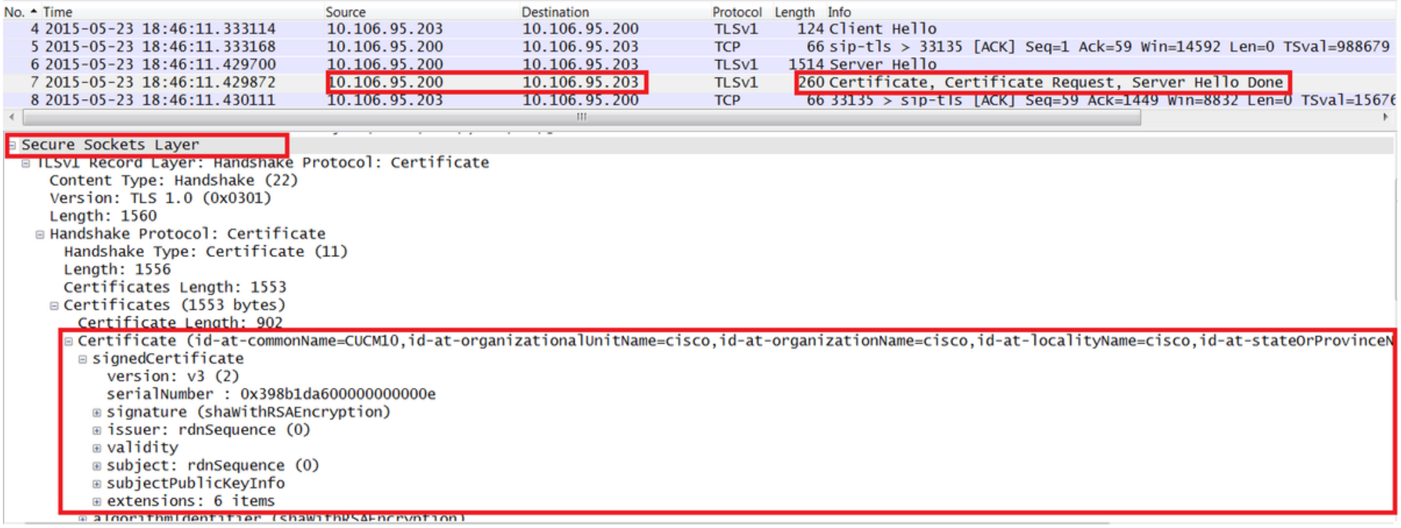
捕获以标准.cap格式完成。本示例使用Wireshark打开packets.cap文件，但可以使用任何数据包捕获显示工具。



```
                  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=15676167
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=1567
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=1567
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=98
18:46:11.451030   10.106.95.203      10.106.95.200      TLSv1     507 Certificate, Client Key Exchange, Certificate Verify, Change Ci
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=98
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=98
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=15
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=15
18:46:15.288860   10.106.95.200      10.106.95.203      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=15
18:46:15.402901   10.106.95.203      10.106.95.200      TLSv1     770 Application Data
```

1. 传输控制协议(TCP)同步(SYN)，用于在CUCM 9.1(2)（客户端）和CUCM 10.5(2)（服务器）之间建立TCP通信。
2. CUCM 9.1(2)发送客户端Hello以启动TLS会话。
3. CUCM 10.5(2)发送服务器Hello、服务器证书和证书请求以启动证书交换过程。
4. 客户端CUCM 9.1(2)为完成证书交换而发送的证书。
5. 加密SIP信令的应用数据显示已建立TLS会话。

进一步检查是否交换了正确的证书。服务器Hello后，服务器CUCM 10.5(2)将其证书发送到客户端CUCM 9.1(2)。

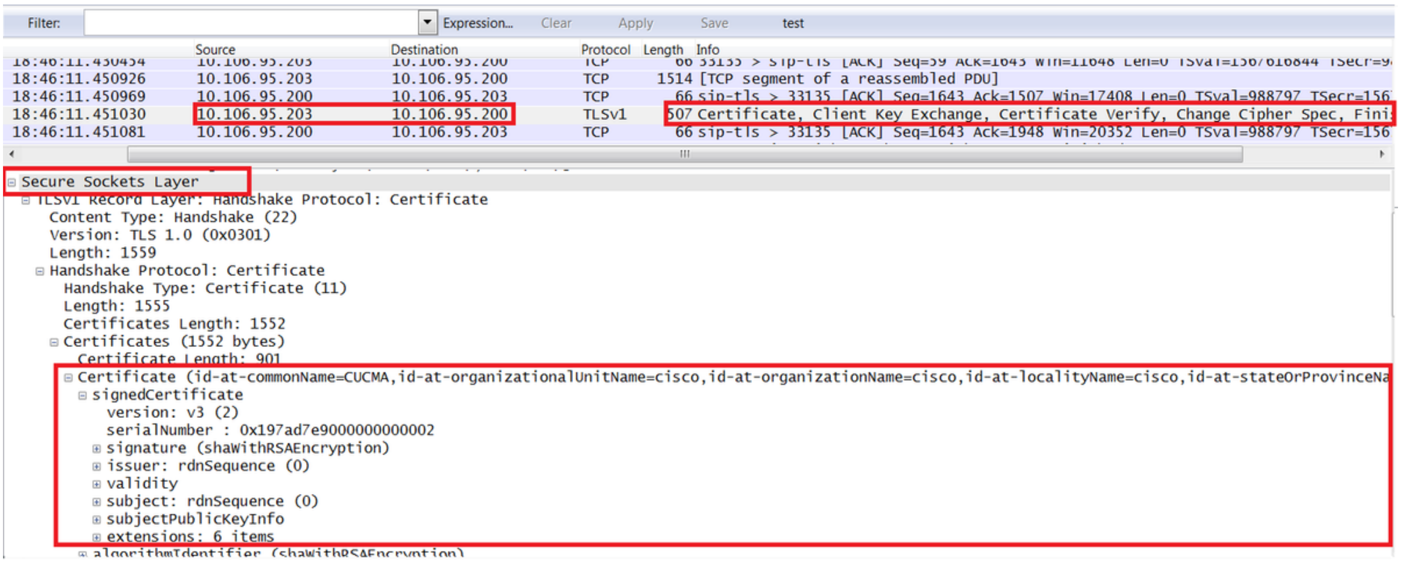


```
No. Time                        Source           Destination      Protocol Length Info
  4 2015-05-23 18:46:11.333114  10.106.95.203    10.106.95.200    TLSv1     124 Client Hello
  5 2015-05-23 18:46:11.333168  10.106.95.200    10.106.95.203    TCP        66 sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 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-stateOrProvinceN
          ⊟ signedCertificate
              version: v3 (2)
              serialNumber : 0x398b1da600000000000e
            ⊞ signature (shaWithRSAEncryption)
            ⊞ issuer: rdnSequence (0)
            ⊞ validity
            ⊞ subject: rdnSequence (0)
            ⊞ subjectPublicKeyInfo
            ⊞ extensions: 6 items
          ⊞ algorithmIdentifier (shaWithRSAEncryption)
```

服务器CUCM 10.5(2)具有的序列号和主题信息将呈现给客户端CUCM 9.1(2)。序列号、主题、颁发者和有效日期均与“OS管理员证书管理”(OS Admin Certificate Management)页面上的信息进行比较。

服务器CUCM 10.5(2)提供自己的证书进行验证，现在它检查客户端CUCM 9.1(2)的证书。 验证在两个方向进行。



```
                 Source           Destination      Protocol Length Info
18:46:11.450454  10.106.95.203    10.106.95.200    TCP        66 33135 > sip-tls [ACK] Seq=59 Ack=1643 Win=11648 Len=0 TSval=1567616844 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-stateOrProvinceNa
          ⊟ signedCertificate
              version: v3 (2)
              serialNumber : 0x197ad7e9000000000002
            ⊞ signature (shaWithRSAEncryption)
            ⊞ issuer: rdnSequence (0)
            ⊞ validity
            ⊞ subject: rdnSequence (0)
            ⊞ subjectPublicKeyInfo
            ⊞ extensions: 6 items
          ⊞ algorithmIdentifier (shaWithRSAEncryption)
```

如果数据包捕获中的证书与操作系统管理网页中的证书不匹配，则不会上传正确的证书。

正确的证书必须上传到OS Admin Cert页面。

收集CUCM跟踪

CUCM跟踪还有助于确定CUCM 9.1(2)和CUCM 10.5(2)服务器之间交换的消息，以及SSL会话是否正确建立。

在本例中，已收集来自CUCM 9.1(2)的跟踪。

呼叫流:

分机1018 > CUCM 9.1(2)> SIP TLS TRUNK > CUCM 10.5(2)>分机9898

++数字分析

```
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
```

++ SIP TLS正在端口5061上用于此呼叫。

```
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
```

++信号分布层(SDL)消息SIPCertificateInd提供有关主题CN和连接信息的详细信息。

```
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 =
```