Configuración del troncal TLS SIP en el administrador de comunicaciones con un certificado firmado por CA

Contenido

Introducción

Este documento describe un proceso paso a paso para configurar el enlace troncal de seguridad de la capa de transporte (TLS) del protocolo de inicio de sesión (SIP) en Communications Manager con un certificado firmado por la autoridad de certificación (CA).

Después de seguir este documento, los mensajes SIP entre dos clústeres se cifrarán mediante TLS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de:

- Cisco Unified Communications Manager (CUCM)

- SIP

Componentes Utilizados

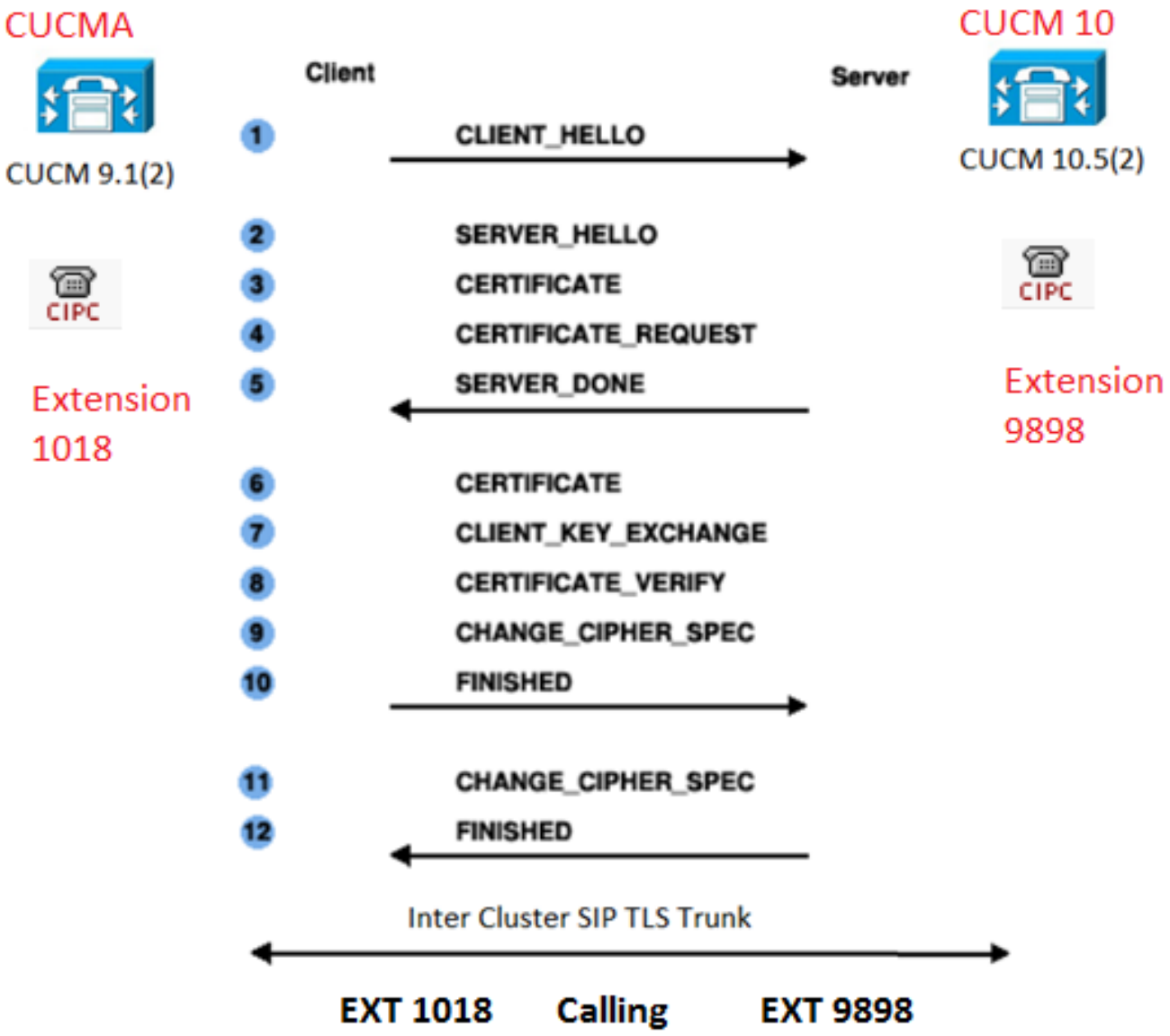
La información que contiene este documento se basa en estas versiones de software:

- CUCM, versión 9.1(2)
- CUCM, versión 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.

Antecedentes

Como se muestra en esta imagen, el intercambio de señales SSL mediante certificados.



Configurar

Paso 1. Utilice la CA pública o la CA de configuración en Windows Server 2003

Consulte el enlace: Configuración de CA en Windows 2003 Server

Paso 2. Verificar nombre de host y configuración

Los certificados se basan en nombres. Asegúrese de que los nombres sean correctos antes de comenzar.

```
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 cambiar el nombre de host, consulte el link: Cambiar nombre de host en CUCM

Paso 3. Generar y descargar la solicitud de firma de certificado (CSR)

CUCM 9.1(2)

Para generar la CSR, navegue hasta **Administrador del SO > Seguridad > Administración de Certificados > Generar CSR**

En el campo **Nombre del certificado**, seleccione la opción **CallManager** de la lista desplegable.

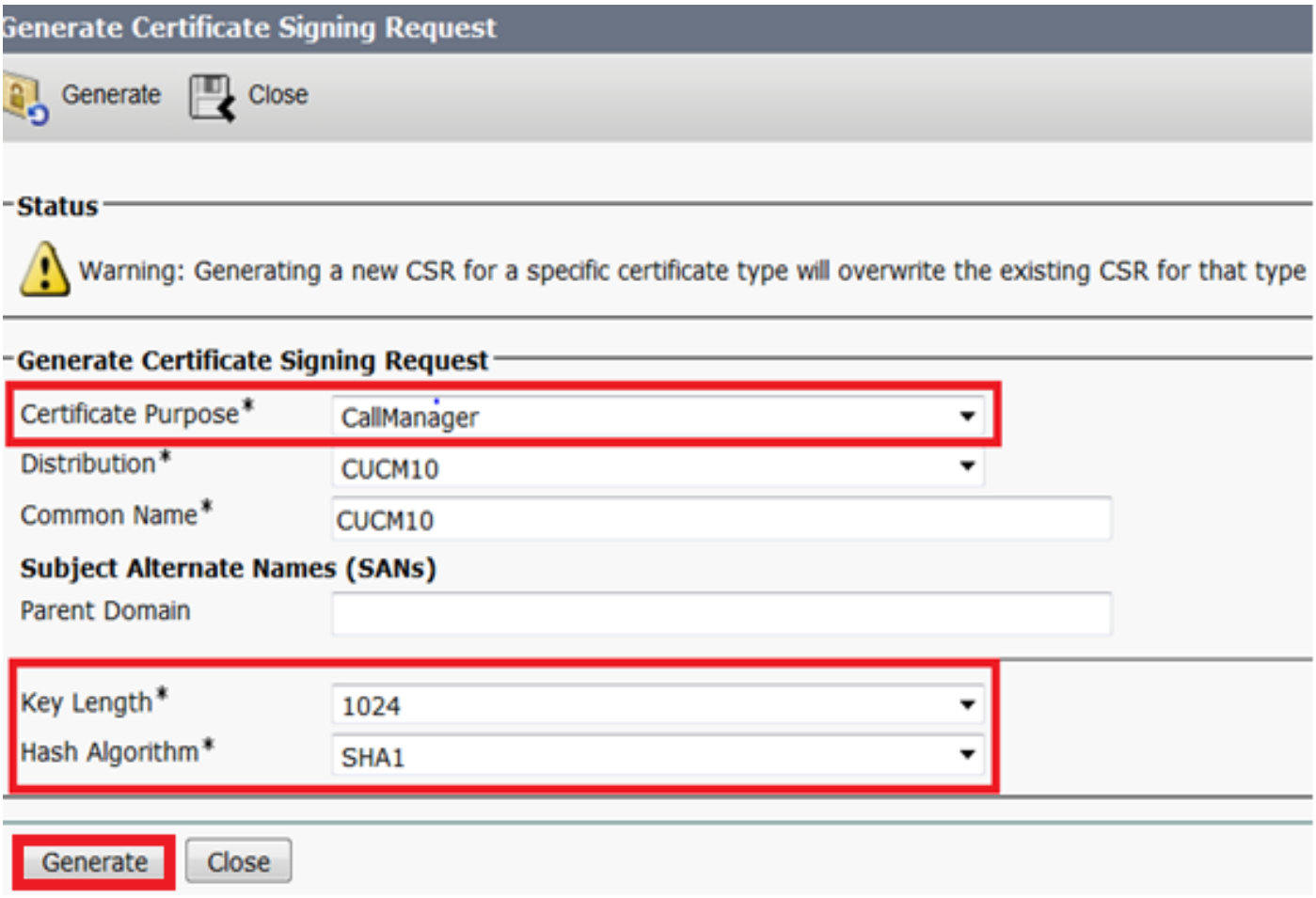
Para descargar la CSR, navegue hasta **OS Admin > Security > Certificate Management > Download CSR**

En el campo **Certificate Name**, seleccione la opción **CallManager** en la lista desplegable.

CUCM 10.5(2)

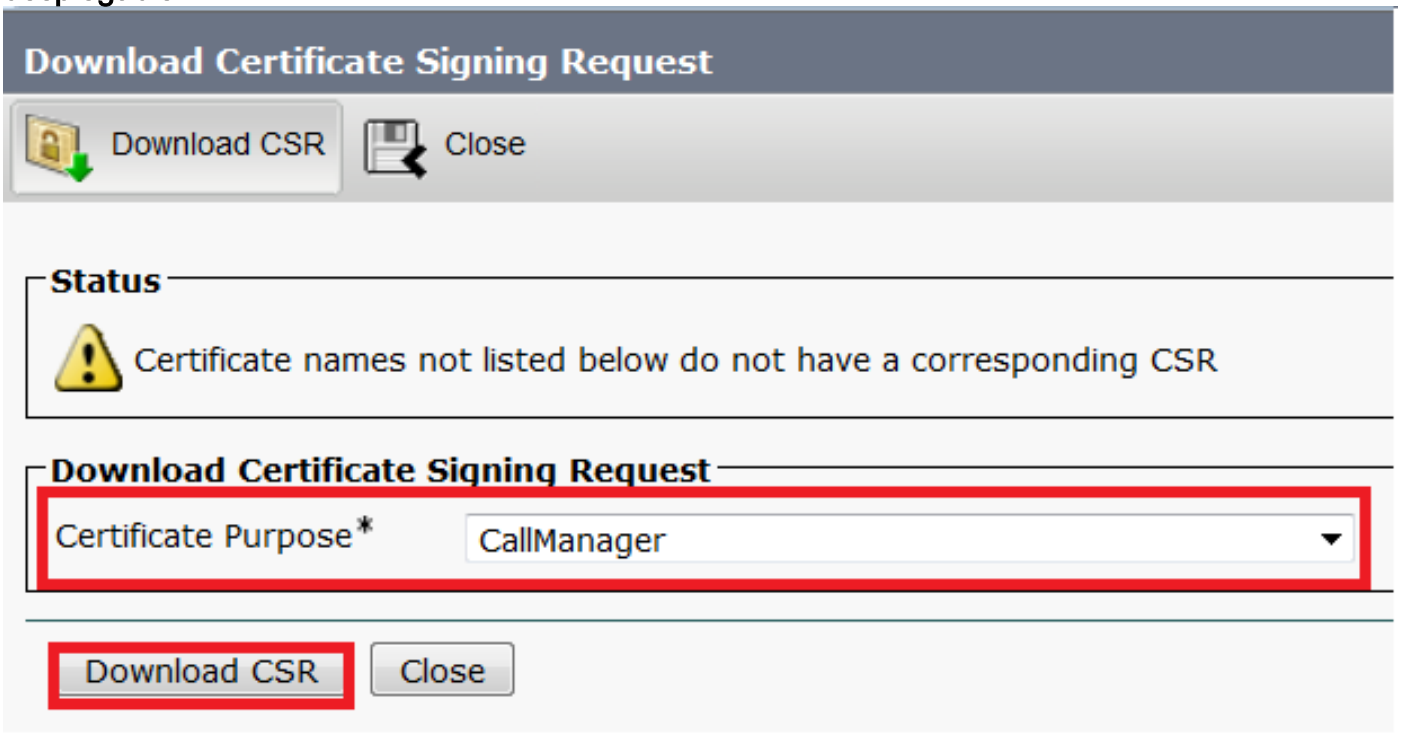
Para generar la CSR, navegue hasta **Administrador del SO > Seguridad > Administración de Certificados > Generar CSR**

1. En el campo Certificate Purpose, seleccione CallManager de la lista desplegable.
2. En el campo Key Length, seleccione 1024 de la lista desplegable.
3. En el campo Algoritmo hash, seleccione SHA1 de la lista desplegable.

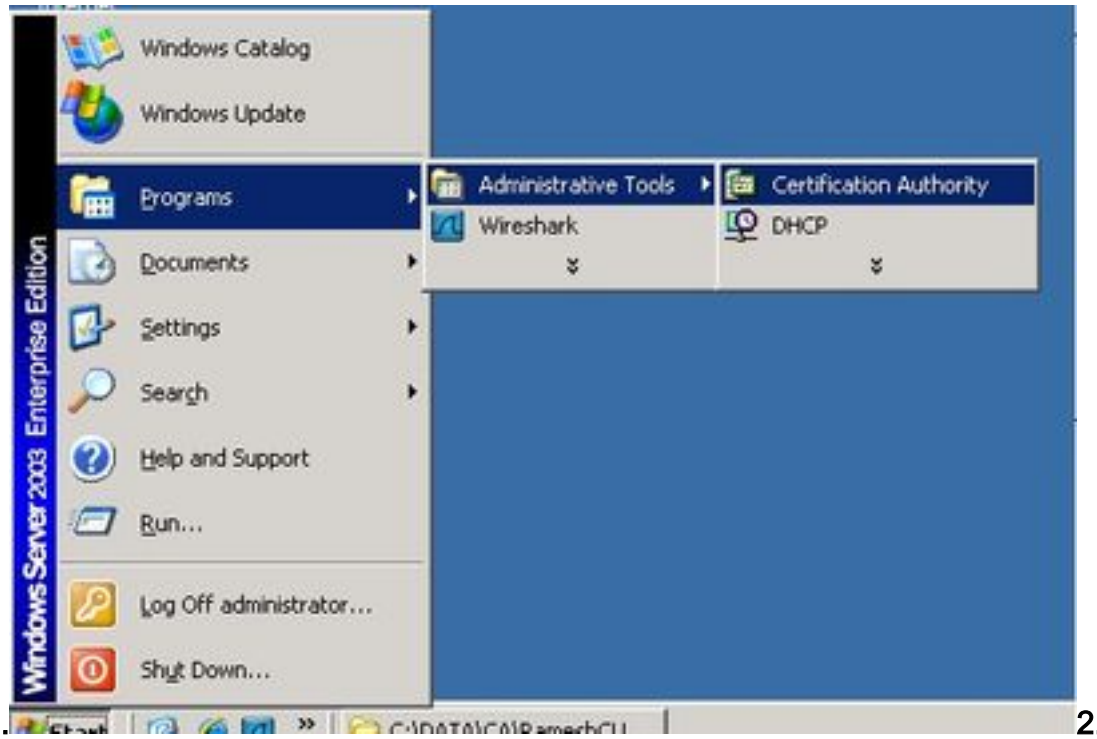


Para descargar la CSR, navegue hasta OS Admin > Security > Certificate Management > Download CSREn el campo Certificate Purpose, seleccione la opción CallManager de la lista

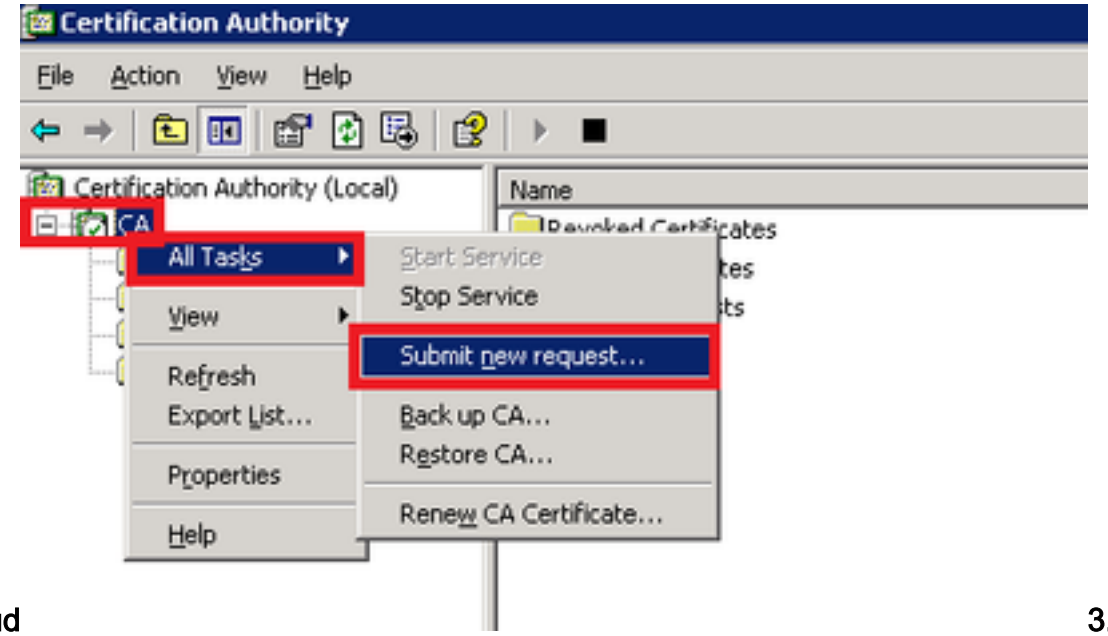
desplegable.



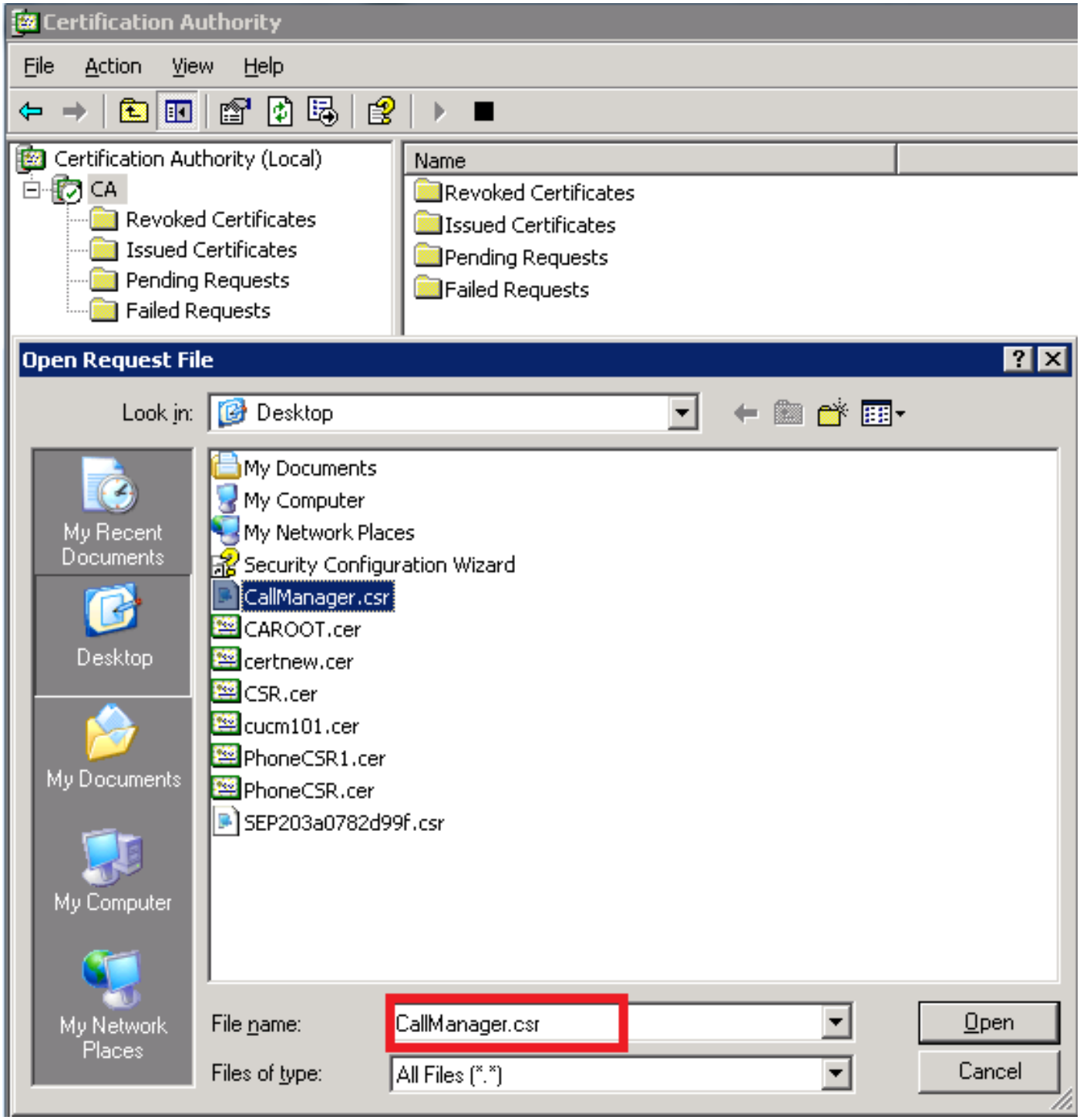
Nota: La CSR de CallManager se genera con las claves Rivest-Shamir-Addleman (RSA) de 1024 bits.Paso 4. Firmar el CSR con la autoridad certificadora de Microsoft Windows 2003Esta es una información opcional para firmar el CSR con la CA de Microsoft Windows 2003.1. Abra la Autoridad de certificación.



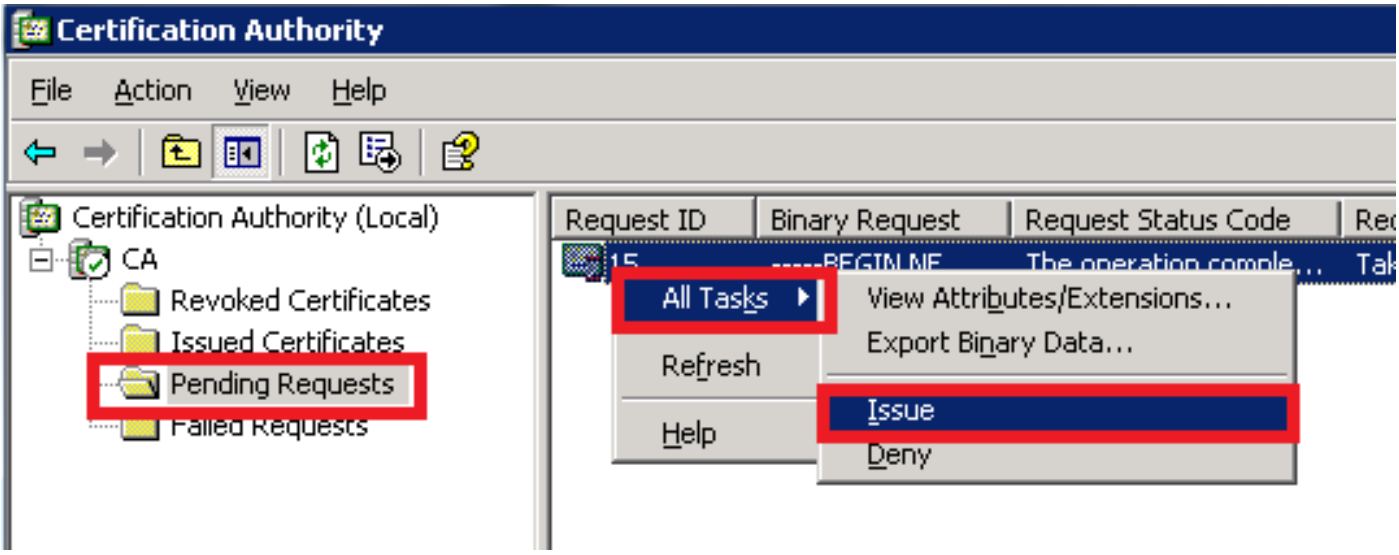
2. Haga clic con el botón derecho del ratón en el icono CA y navegue hasta Todas las tareas > Enviar



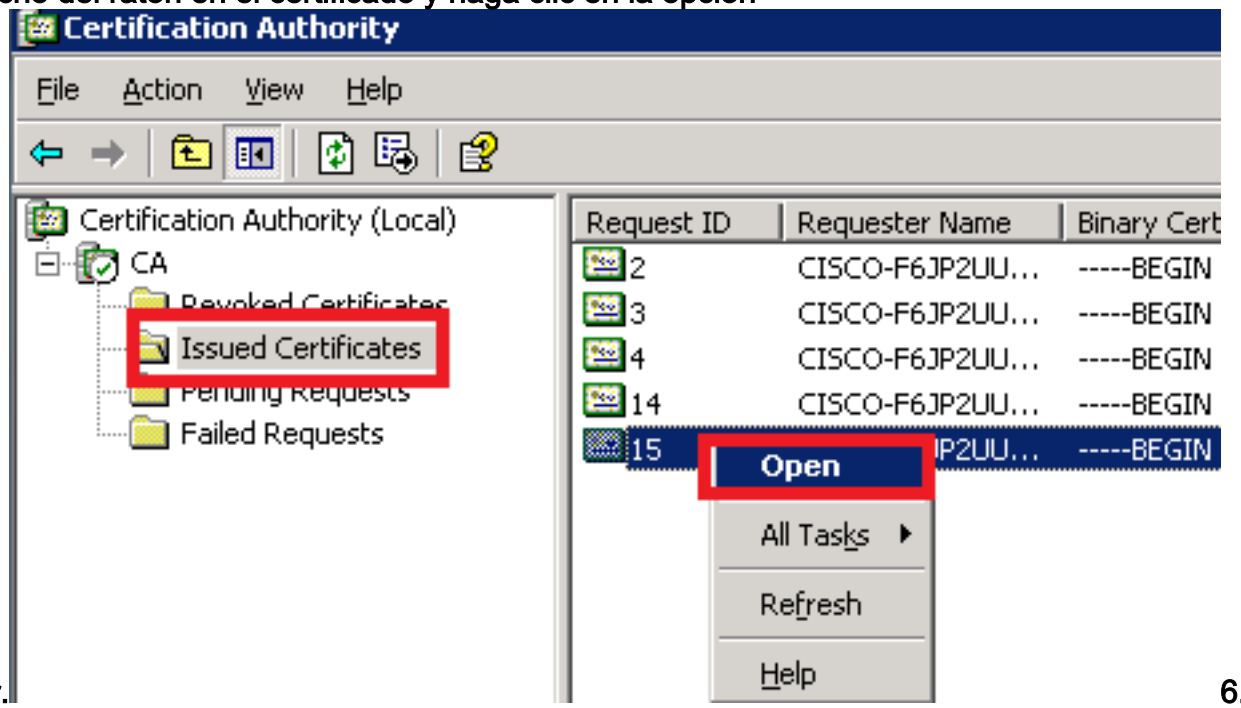
nueva solicitud 3. Seleccione el CSR y haga clic en la opción Open (Aplicable tanto en los CSR (CUCM 9.1(2) como en CUCM 10.5(2)))



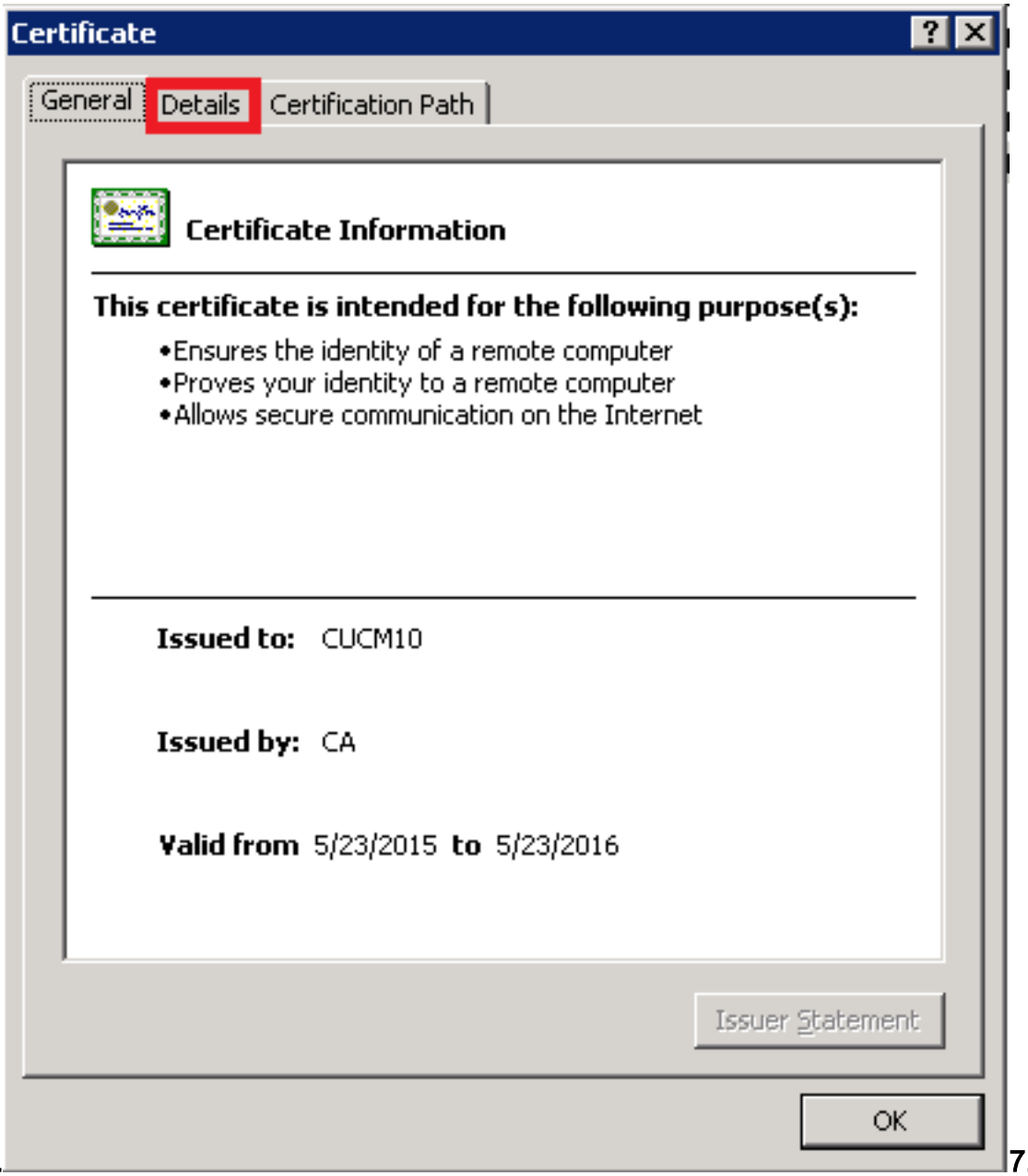
4. Todos los CSR abiertos se muestran en la carpeta Solicitudes pendientes. Haga clic con el botón derecho del ratón en cada CSR y navegue hasta Todas las tareas > Problema para emitir los certificados. [Aplicable tanto en los RSE [CUCM 9.1(2) como en CUCM 10.5(2)]



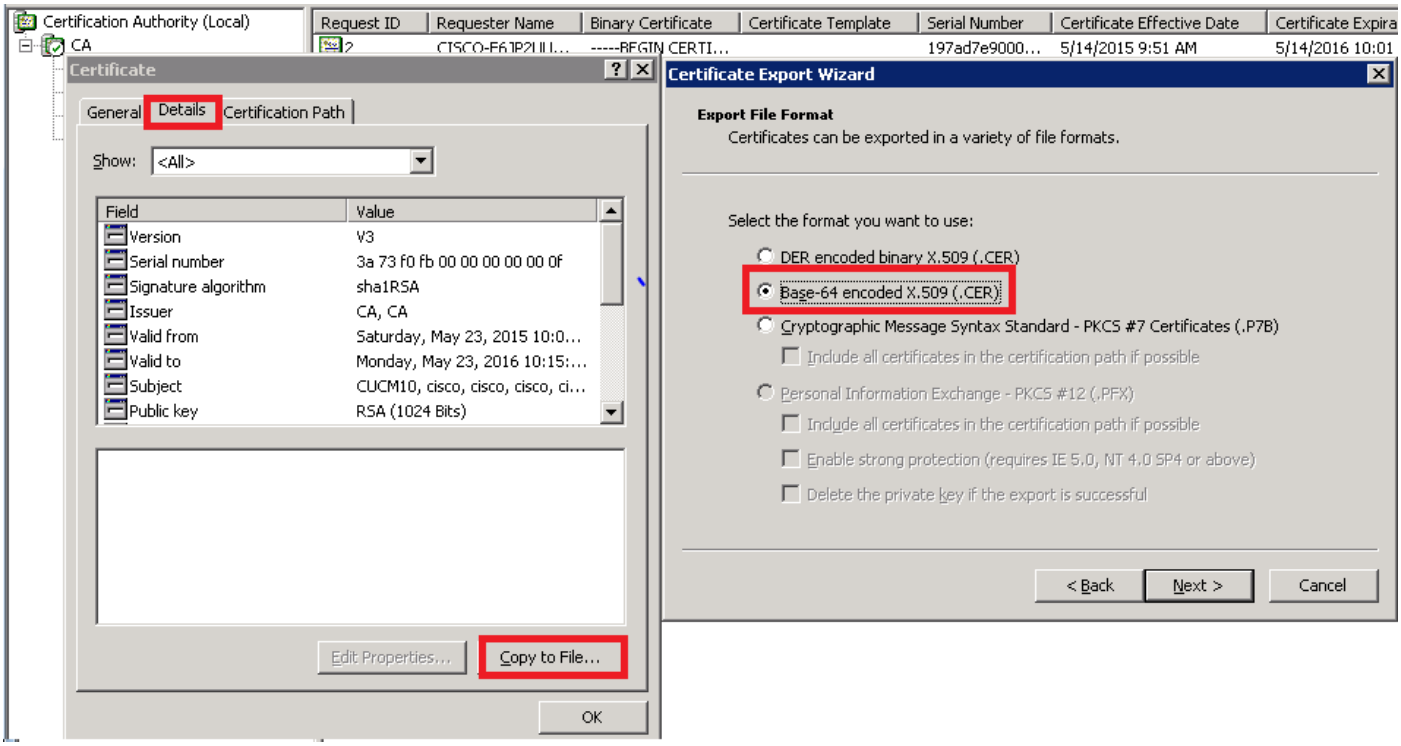
5. Para descargar el certificado, elija la carpeta Certificados emitidos.Haga clic con el botón derecho del ratón en el certificado y haga clic en la opción



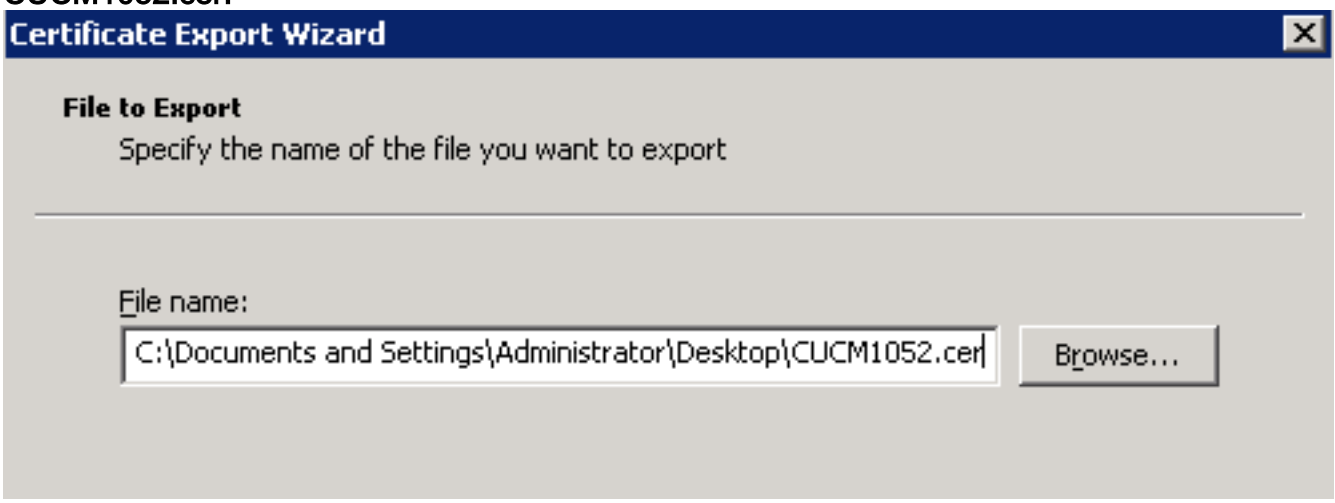
Abrir. 6. Se muestran los detalles del certificado. Para descargar el certificado, seleccione la pestaña Detalles y haga clic en el botón Copiar a



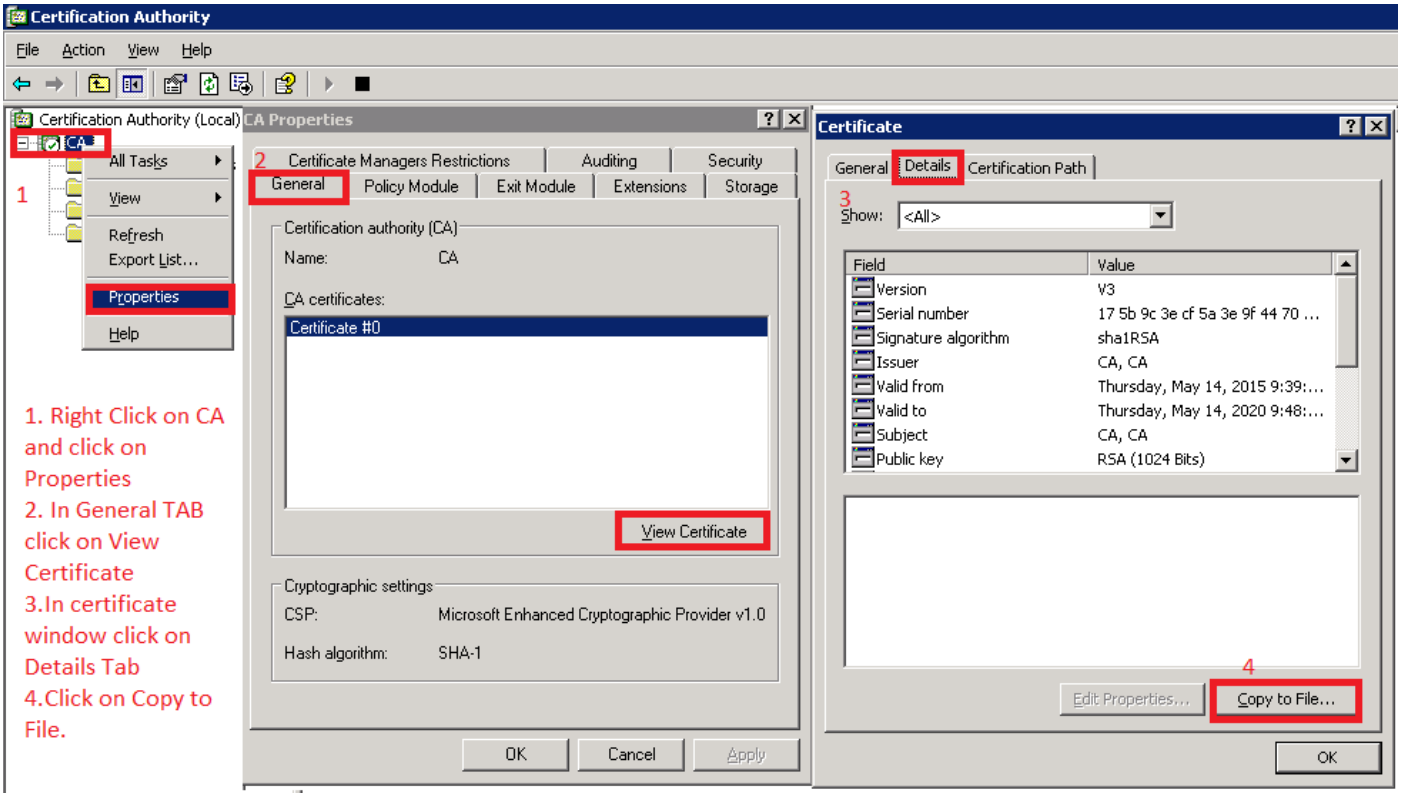
archivo...7. En la ventana Asistente para exportación de certificados, haga clic en el botón de radio Base-64 codificado
X.509(.CER).



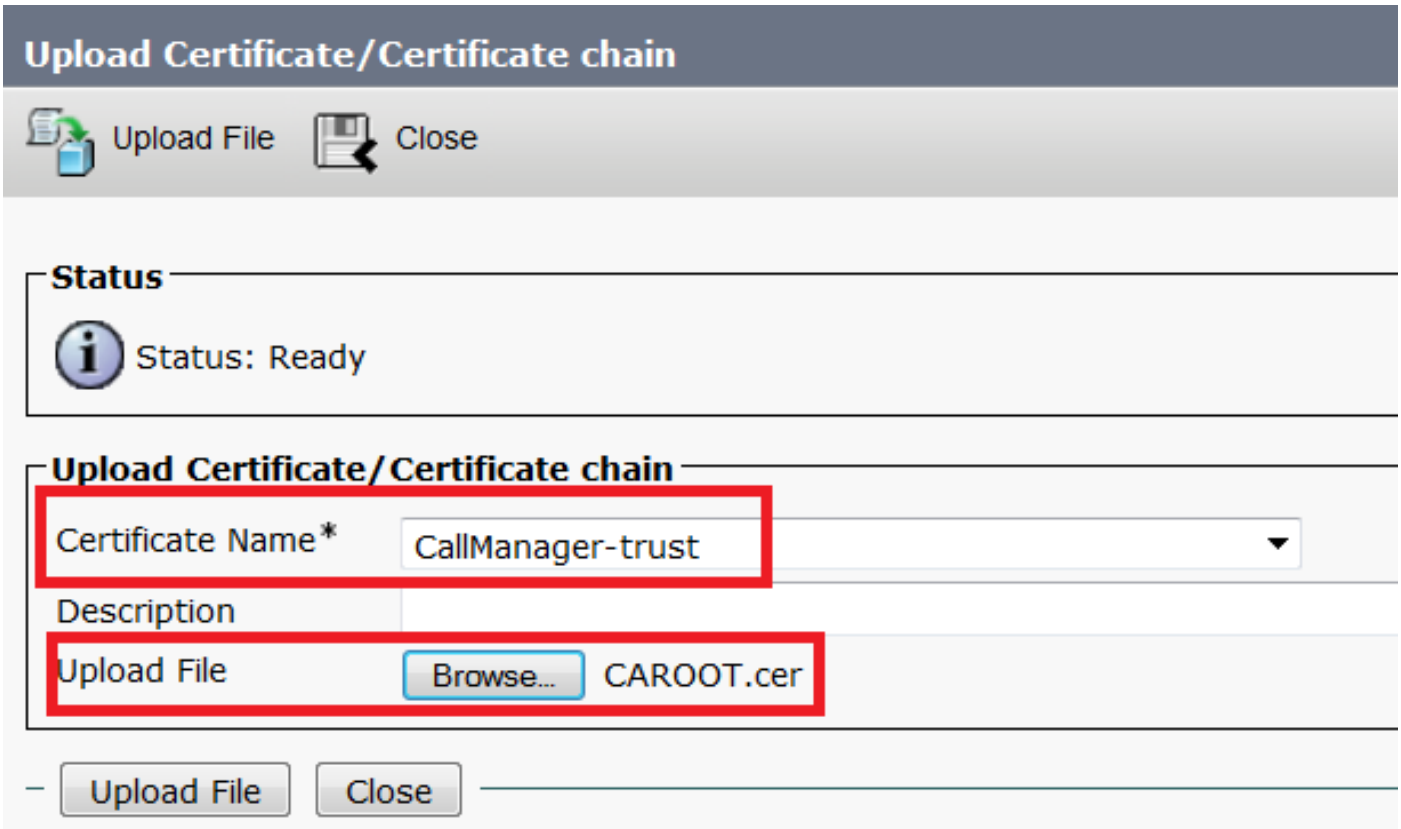
8. Asigne un nombre exacto al archivo. Este ejemplo utiliza el formato CUCM1052.cer.



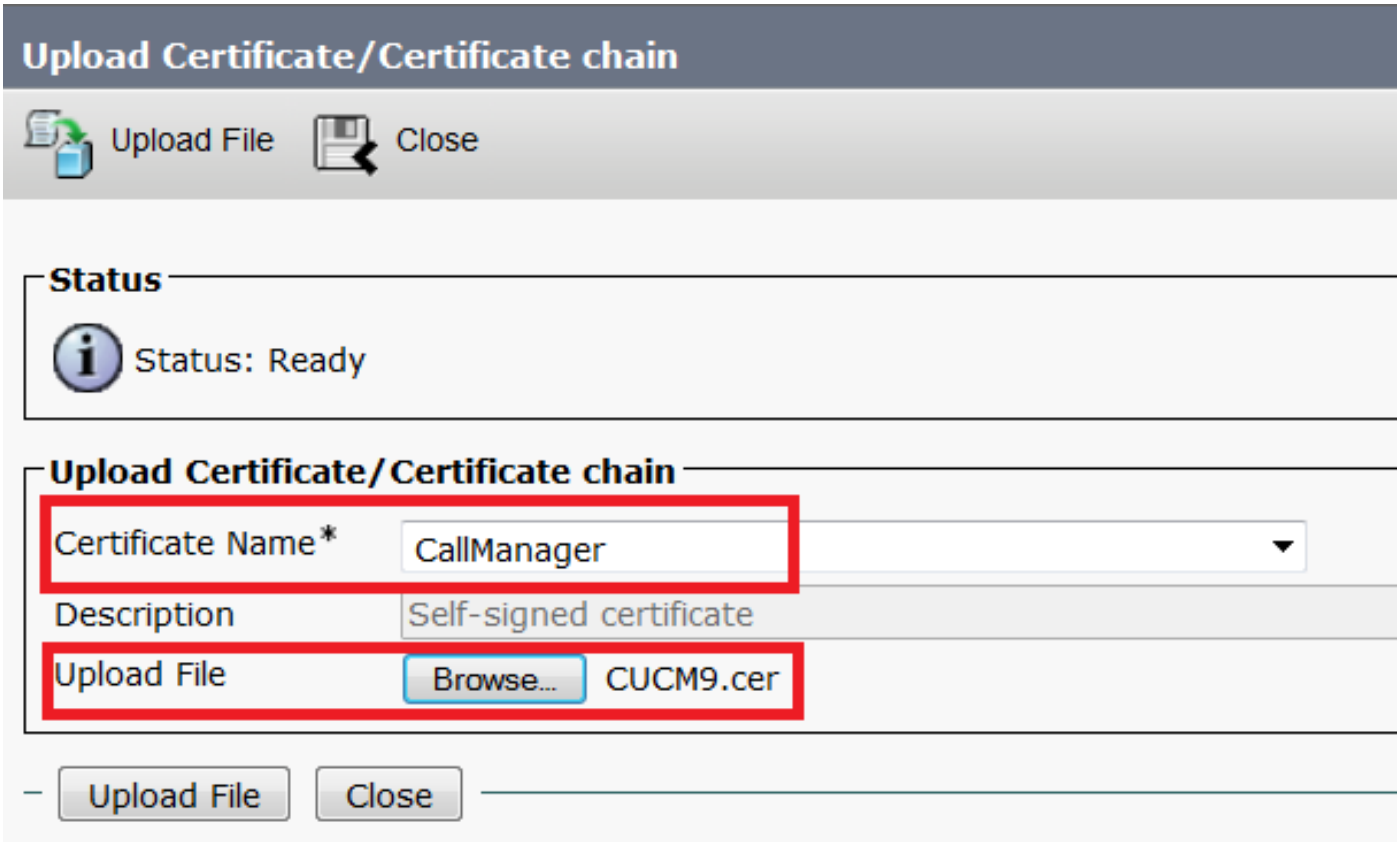
Para CUCM 9.1(2), siga el mismo procedimiento.Paso 5. Obtener el certificado raíz de la CAAbra la ventana Certification Authority. Para descargar la raíz-CA1. Haga clic con el botón derecho del ratón en el icono de CA y haga clic en la opción Properties.2. En general TAB, haga clic en Ver certificado.3. En la ventana Certificate, haga clic en la TAB de detalles.4. Haga clic en Copiar a archivo...



Paso 6. Cargar certificado raíz de CA como CallManager TrustPara cargar el certificado raíz de la CA, inicie sesión en OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain

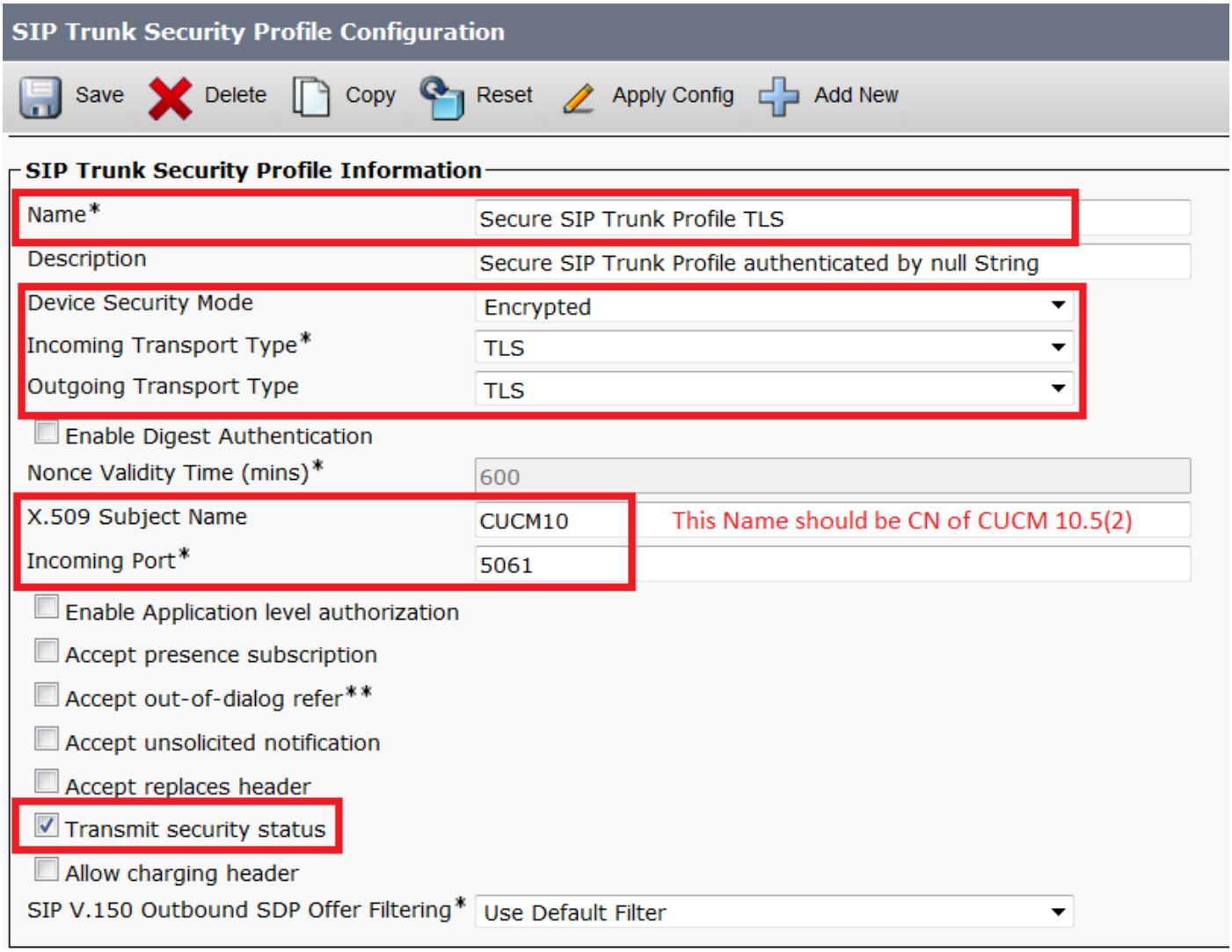


Nota: Realice estos pasos en los CUCM (CUCM 9.1(2) y CUCM 10.5(2))Paso 7. Cargue el certificado de CSR de CallManager de firma de CA como certificado de CallManager.Para cargar el CA sign CallManager CSR, inicie sesión en OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain



Nota: Realice estos pasos en los CUCM (CUCM 9.1(2) y CUCM 10.5(2))Paso 8. Crear perfiles de seguridad troncal SIPCUCM 9.1(2)

Para crear el perfil de seguridad del troncal SIP, navegue hasta System > Security > SIP Trunk Security Profile.Copie el perfil de troncal SIP no seguro existente y asígnele un nuevo nombre. En el ejemplo, se ha cambiado el nombre del perfil troncal SIP no seguro por el de TLS de perfil troncal SIP
seguro.



En X.509 Nombre de asunto, utilice el Nombre común (CN) de CUCM 10.5(2) (certificado firmado por CA) como se muestra en esta
imagen.

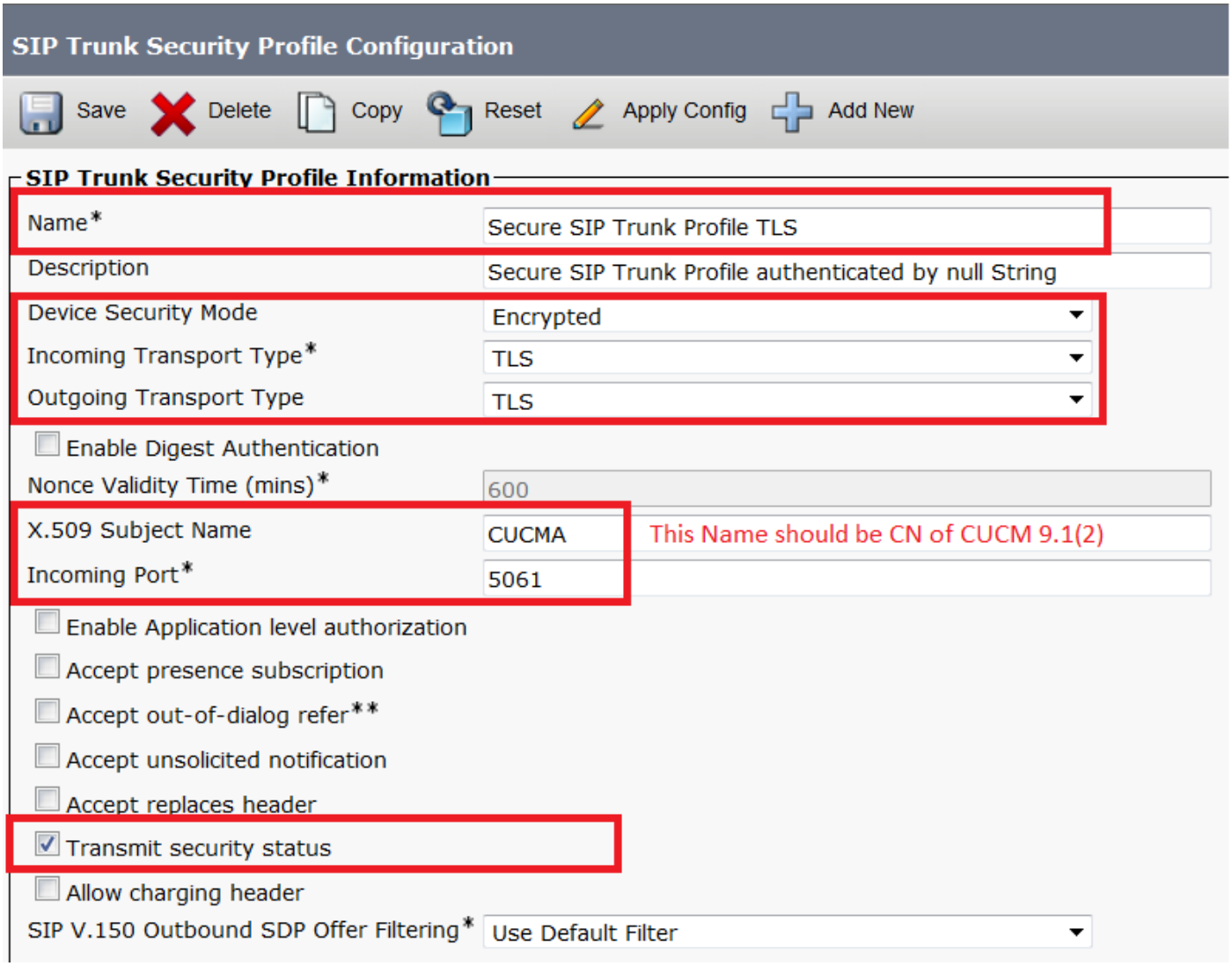
Certificate Settings

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

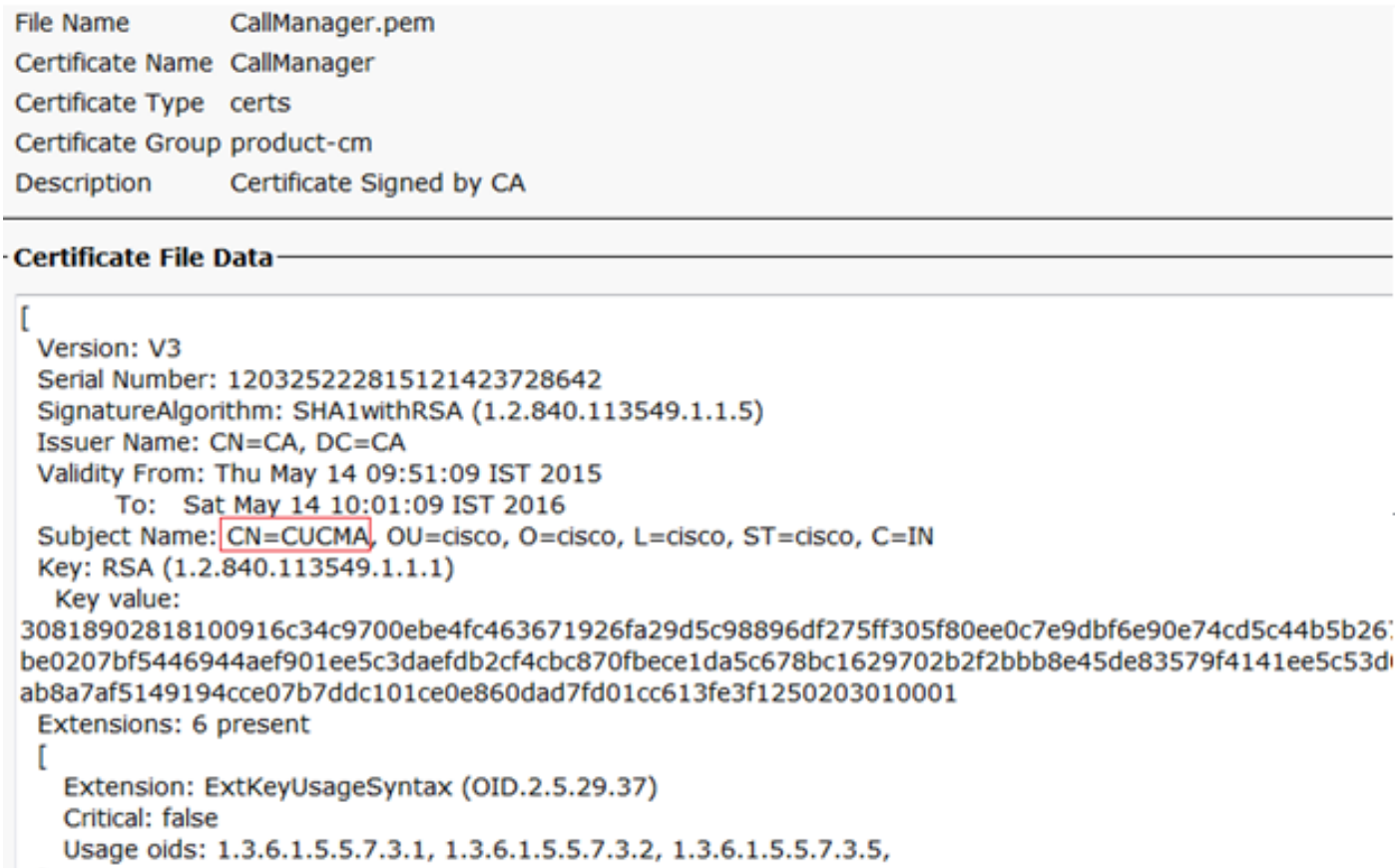
Certificate File Data

```
[
  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)Vaya a System > Security > SIP Trunk Security Profile.Copie el perfil de troncal SIP no seguro existente y asígnele un nuevo nombre. En el ejemplo, se cambió el nombre del perfil troncal SIP no seguro por el de TLS de perfil troncal SIP
seguro.



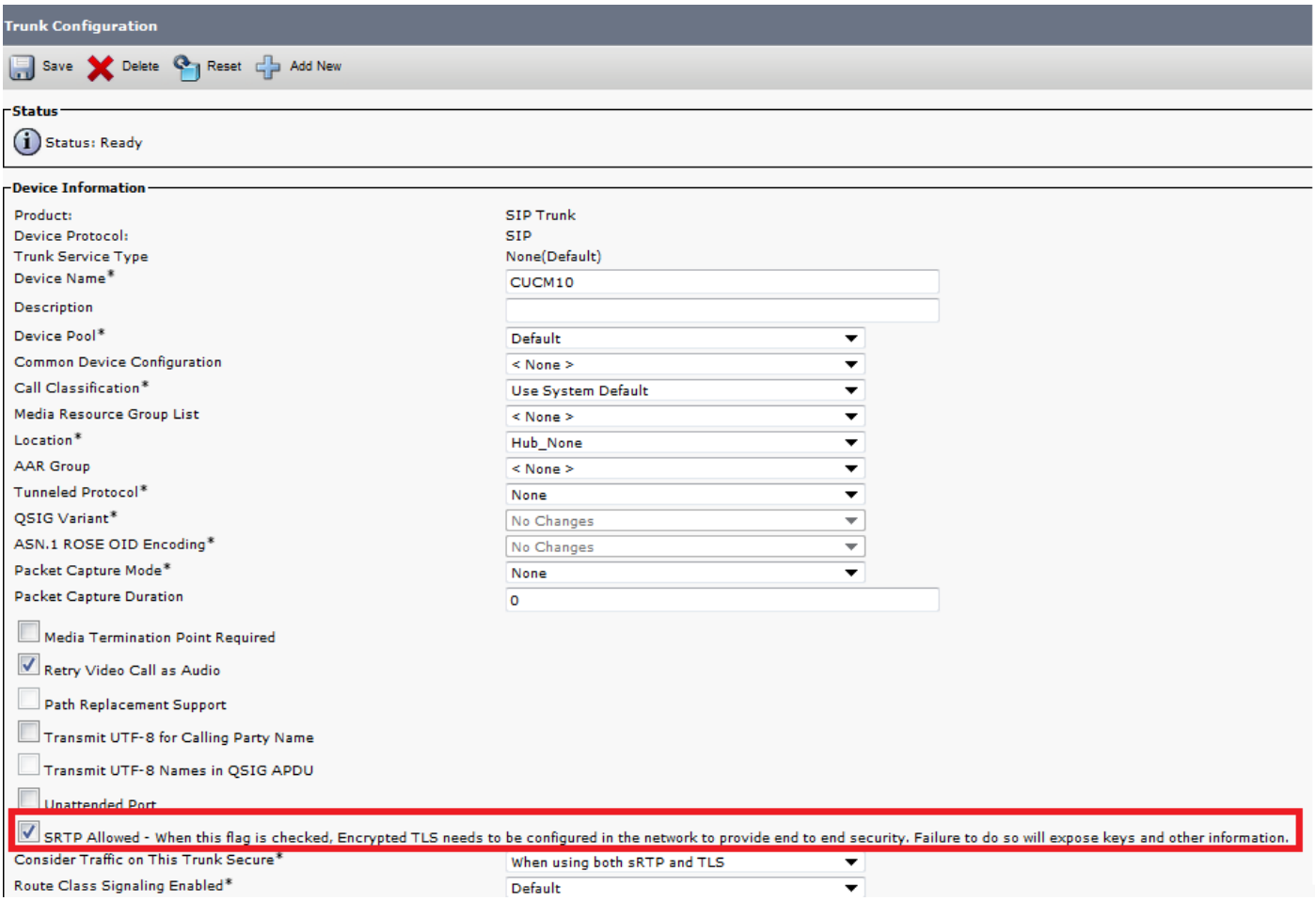
En X.509 Nombre del asunto, utilice el CN de CUCM 9.1(2) (certificado firmado por CA) como se destaca:



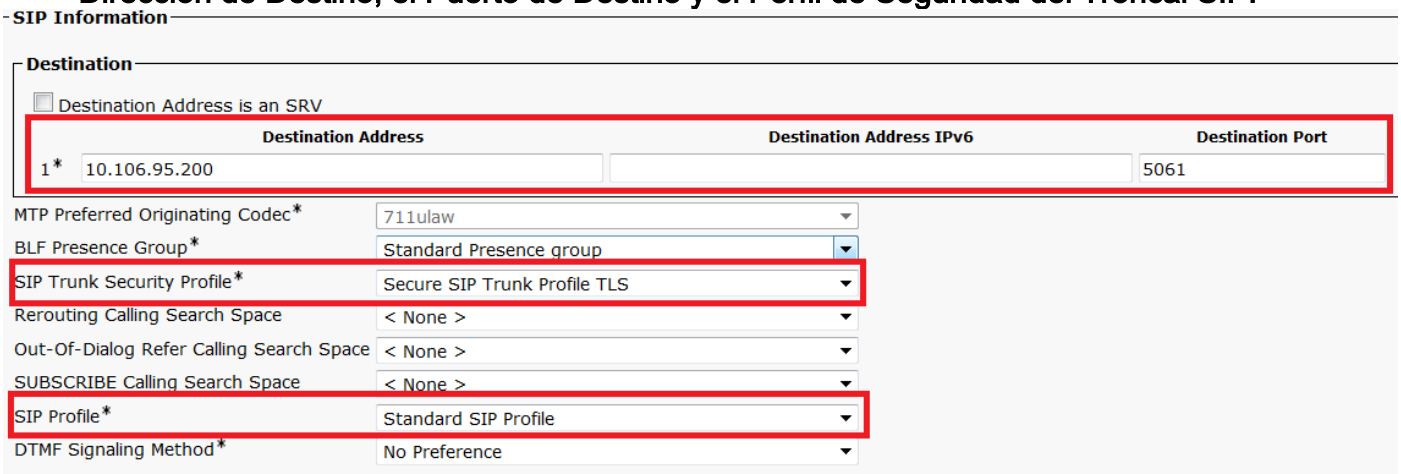
Ambos perfiles de seguridad de troncal SIP configuran un puerto entrante de 5061, en el que cada clúster escucha en el puerto TCP 5061 las nuevas llamadas TLS SIP entrantes.Paso 9. Creación de enlaces troncales SIPDespués de crear los perfiles de seguridad, cree los troncales SIP y realice los cambios para el siguiente parámetro de configuración en el troncal SIP.CUCM 9.1(2)

1. En la ventana SIP Trunk Configuration, marque la casilla SRTP Allowed del parámetro de configuración.

De este modo, se protege el protocolo de transporte en tiempo real (RTP) que se utilizará para las llamadas a través de este enlace troncal. Esta casilla sólo se debe activar cuando se utiliza SIP TLS porque las claves del protocolo de transporte en tiempo real seguro (SRTP) se intercambian en el cuerpo del mensaje SIP. La señalización SIP debe estar protegida por TLS; de lo contrario, cualquier persona con señalización SIP no segura podría descifrar la secuencia SRTP correspondiente a través del
tronco.



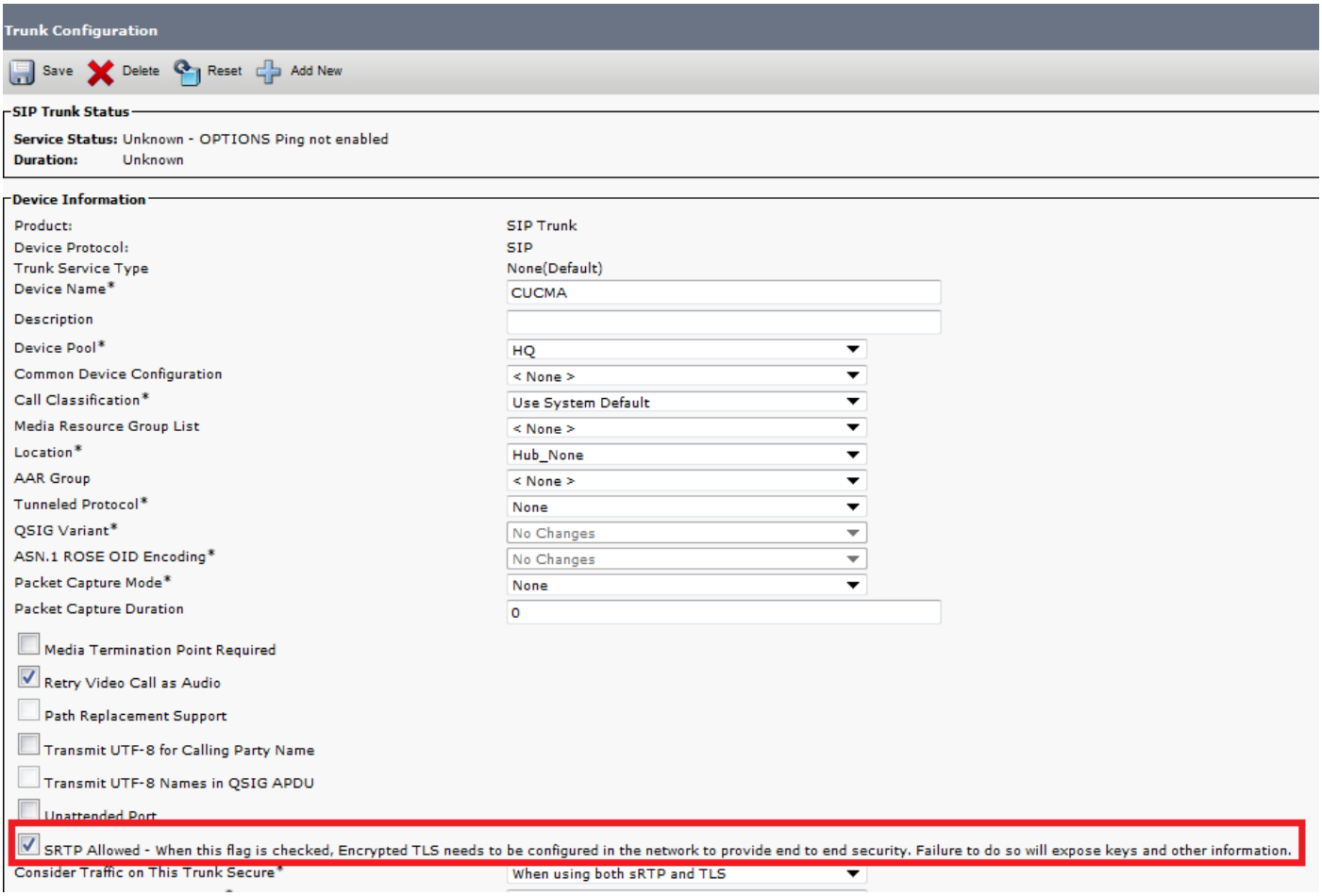
2. En la sección Información de SIP de la ventana Configuración del Troncal SIP, agregue la Dirección de Destino, el Puerto de Destino y el Perfil de Seguridad del Troncal SIP.



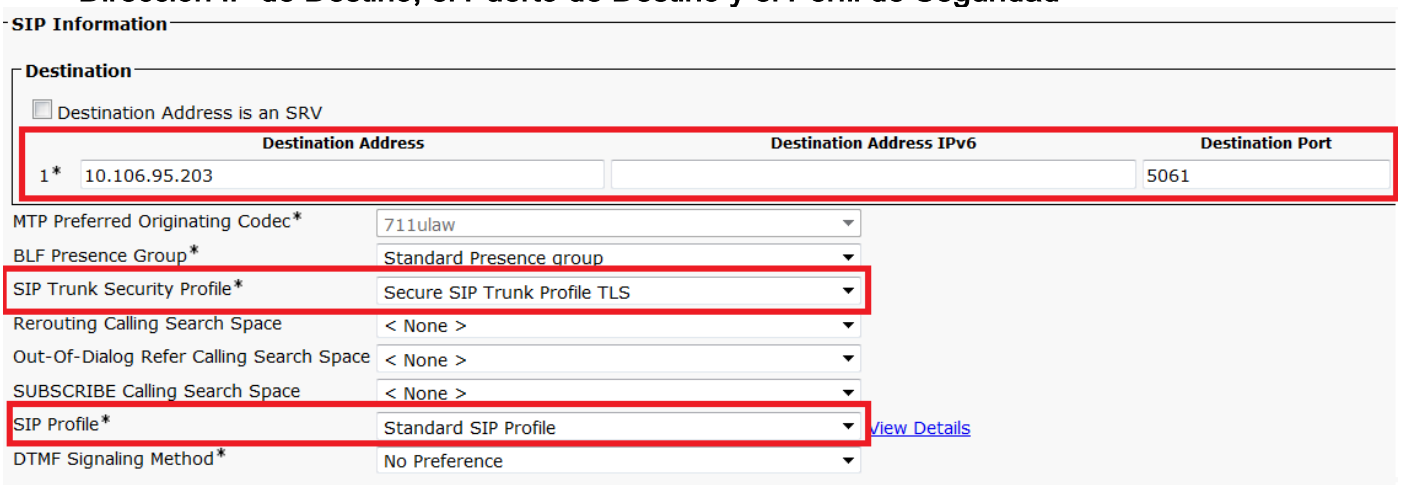
CUCM 10.5(2)

1. En la ventana SIP Trunk Configuration, marque la casilla SRTP Allowed del parámetro de configuración.

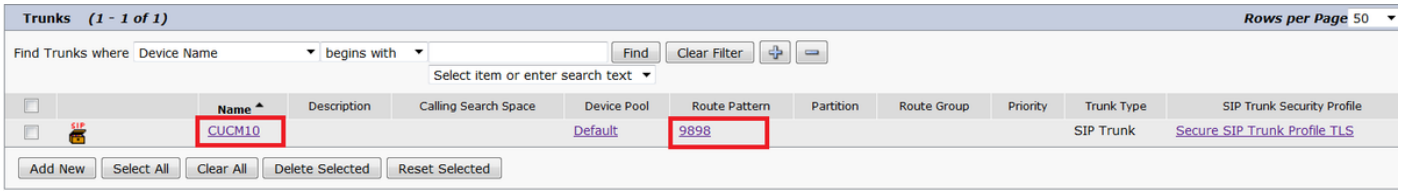
Esto permite que el SRTP se utilice para llamadas a través de este tronco. Esta casilla sólo se debe marcar cuando se utiliza SIP TLS, porque las claves para SRTP se intercambian en el cuerpo del mensaje SIP. La señalización SIP debe estar protegida por TLS porque cualquiera con una señalización SIP no segura puede descifrar la secuencia RTP segura correspondiente sobre el
tronco.



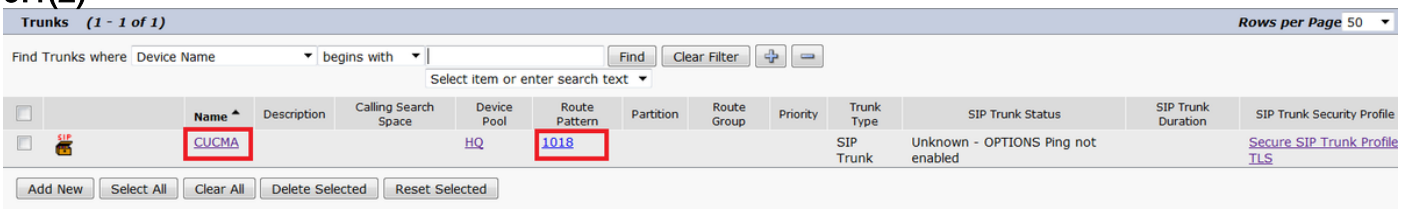
2. En la sección Información de SIP de la ventana Configuración de Troncal SIP, agregue la Dirección IP de Destino, el Puerto de Destino y el Perfil de Seguridad



Paso 10. Crear patrones de rutaEl método más simple es crear un patrón de ruta en cada clúster, apuntando directamente al troncal SIP. También se podrían utilizar grupos de rutas y listas de rutas.CUCM 9.1(2) señala al patrón de ruta 9898 a través del troncal TLS SIP a CUCM
10.5(2)



El CUCM 10.5(2) apunta al patrón de ruta 1018 a través del troncal TLS SIP a CUCM 9.1(2)



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

La llamada TLS SIP se puede depurar con estos pasos.

Recopilar captura de paquetes en CUCM

Para verificar la conectividad entre CUCM 9.1(2) y CUCM 10.5(2), tome una captura de paquetes en los servidores CUCM y observe el tráfico TLS SIP.El tráfico TLS SIP se transmite en el puerto TCP 5061, visto como sip-tls.En el siguiente ejemplo, hay una sesión SSH CLI establecida para CUCM 9.1(2)1. Captura de paquetes CLI en pantallaEsta CLI imprime el resultado en la pantalla para el tráfico TLS SIP.

```
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>
```

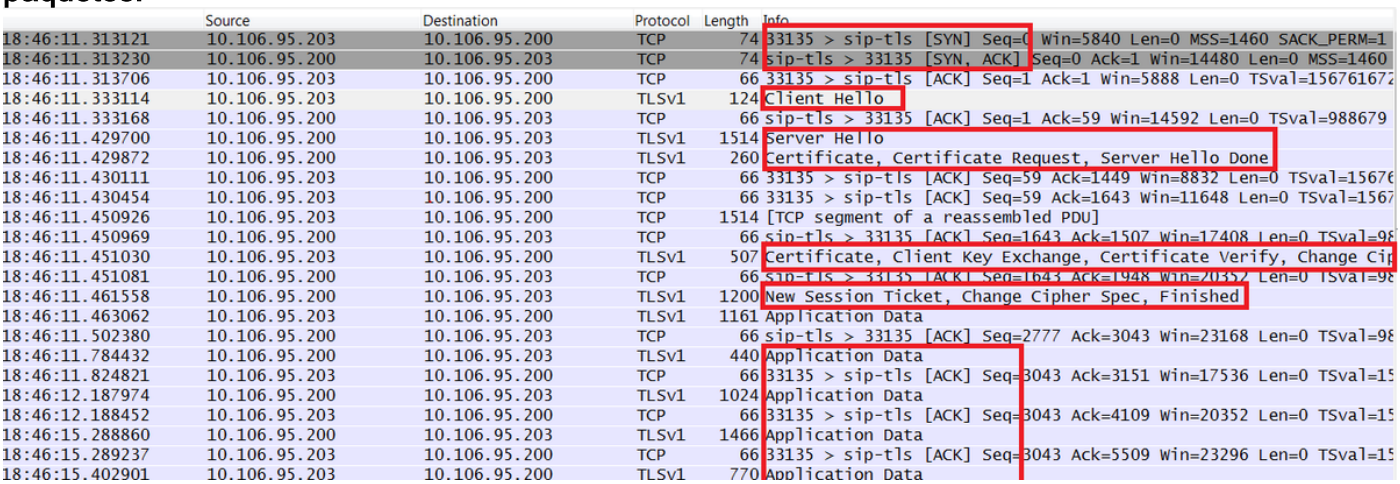
2. Capturas de CLI a archivoEsta CLI realiza la captura de paquetes basada en el host y crea un archivo denominado packets.

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

Reinicie el troncal SIP en CUCM 9.1(2) y realice la llamada desde la extensión 1018 (CUCM 9.1(2)) a la extensión 9898 (CUCM 10.5(2))Para descargar el archivo desde la CLI, ejecute este comando:

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

La captura se realiza en el formato .cap estándar. Este ejemplo utiliza Wireshark para abrir el archivo packets.cap, pero se puede utilizar cualquier herramienta de visualización de captura de paquetes.

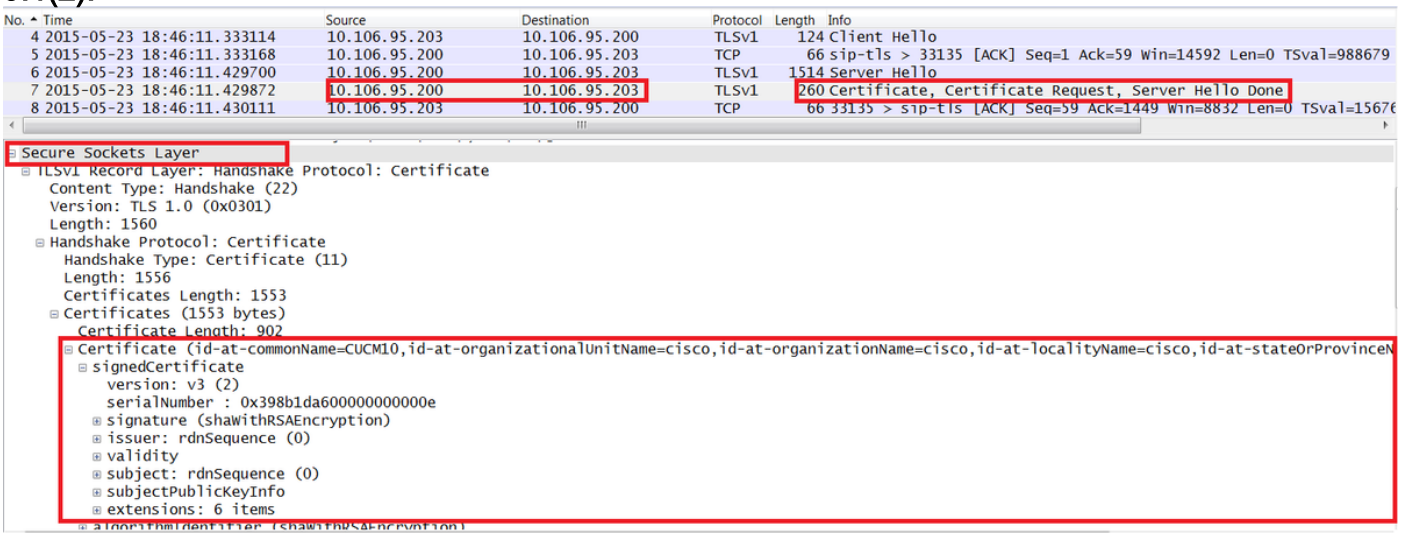


	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	sip-tls > 33135 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
18:46:11.313706	10.106.95.203	10.106.95.200	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=15676
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 Cip
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	10.106.95.200	10.106.95.203	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

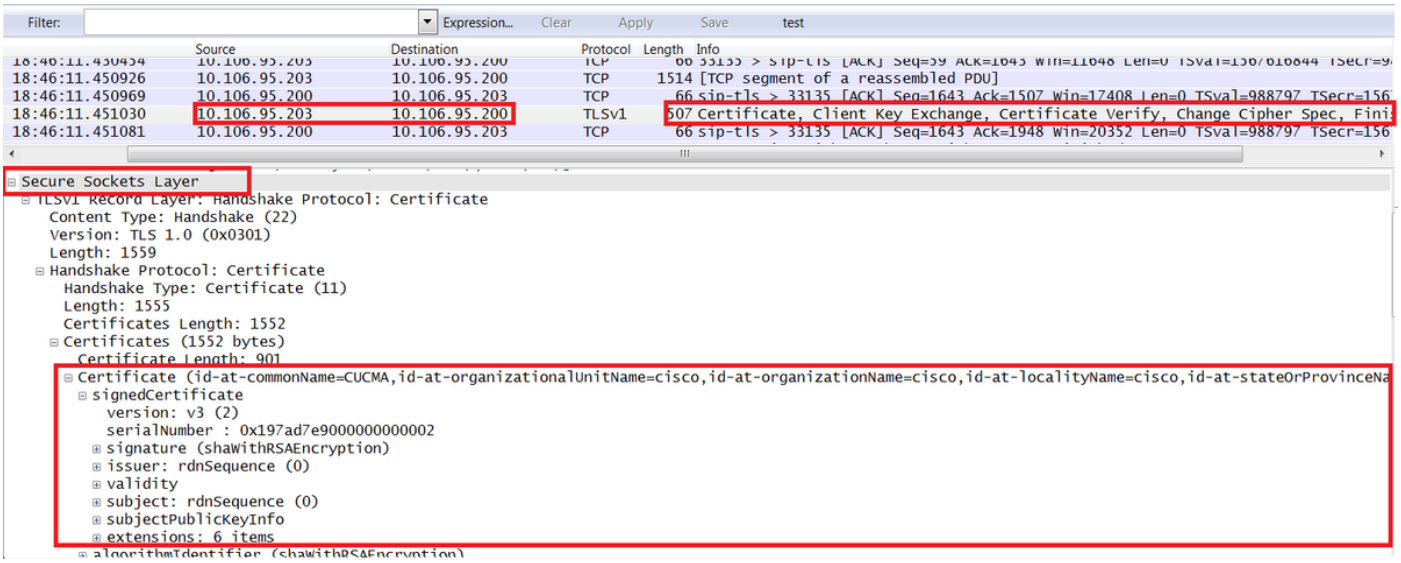
1. El protocolo de control de transmisión (TCP) Synchronize (SYN) para establecer la comunicación TCP entre CUCM 9.1(2)(Client) y CUCM 10.5(2)(Server).

2. CUCM 9.1(2) envía la Hello de cliente para iniciar la sesión TLS.
3. CUCM 10.5(2) envía la Hello del servidor, el Certificado del servidor y la Solicitud de certificado para iniciar el proceso de intercambio de certificados.
4. El certificado que el cliente CUCM 9.1(2) envía para completar el intercambio de certificados.
5. Los datos de la aplicación que son señalización SIP cifrada muestran que se ha establecido la sesión TLS.

Compruebe si se intercambian los certificados correctos. Después de Server Hello, el servidor CUCM 10.5(2) envía su certificado al cliente CUCM 9.1(2).



El número de serie y la información del asunto que tiene el servidor CUCM 10.5(2), se presentan al cliente CUCM 9.1(2).El número de serie, el asunto, el emisor y las fechas de validez se comparan con la información de la página Administración de certificados de administración del sistema operativo.El servidor CUCM 10.5(2) presenta su propio certificado para verificación, ahora verifica el certificado del cliente CUCM 9.1(2). La verificación se realiza en ambas direcciones.



Si hay una discordancia entre los certificados en la captura de paquetes y los certificados en la página web de administración del sistema operativo, los certificados correctos no se cargan.Los certificados correctos deben cargarse en la página de certificado de administración del sistema operativo.Recopilar rastros de CUCMLos seguimientos de CUCM también pueden ser útiles para determinar qué mensajes se intercambian entre los servidores CUCM 9.1(2) y CUCM 10.5(2) y si la sesión SSL está o no correctamente establecida.En el ejemplo, se han recopilado los rastros de CUCM 9.1(2).Flujo de llamada:Ext 1018 > CUCM 9.1(2) > TRONCO TLS SIP > CUCM 10.5(2) > Ext 9898++ Análisis 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
```

++ SIP TLS se está utilizando en el puerto 5061 para esta llamada.

```
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
```

El mensaje ++ Signal Distribution Layer (SDL) SIPCcertificateInd proporciona detalles sobre el asunto CN y la información de conexión.

```
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 =
```