تكوين خط اتصال SIP TLS على مدير الاتصالات باستخدام شهادة CA موقعة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
التكوين
الخطوة 1. أستخدم المرجع المصدق العام أو مرجع مصدق الاعداد على Windows Server 2003
الخطوة 2. التحقق من اسم المضيف والاعدادات
الخطوة 3. إنشاء طلب توقيع الشهادة (CSR) وتنزيله
الخطوة 4. توقيع CSR مع مرجع شهادات Microsoft Windows 2003
الخطوة 5. الحصول على الشهادة الجذر من المرجع المصدق
الخطوة 6. تحميل شهادة جذر CA كثقة CallManager
الخطوة 7. تحميل شهادة CA Sign CallManager CSR كشهادة CallManager.
الخطوة 8. إنشاء ملفات تعريف أمان خط اتصال SIP
الخطوة 9. إنشاء خطوط اتصال SIP
الخطوة 10. إنشاء أنماط المسار
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
تجميع التقاط الحزم على CUCM
تجميع مسارات CUCM

المقدمة

يصف هذا المستند عملية تدريجية لتكوين خط اتصال بروتوكول بدء جلسة عمل (SIP) أمان طبقة النقل (TLS) على مدير الاتصالات باستخدام شهادة موقعة من المرجع المصدق (CA).

بعد متابعة هذا المستند، سيتم تشفير رسائل SIP بين مجموعتين باستخدام قوائم التحكم في الوصول (TLS).

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من:

- برنامج Cisco Unified Communications Manager (CUCM)
- SIP

المكونات المستخدمة

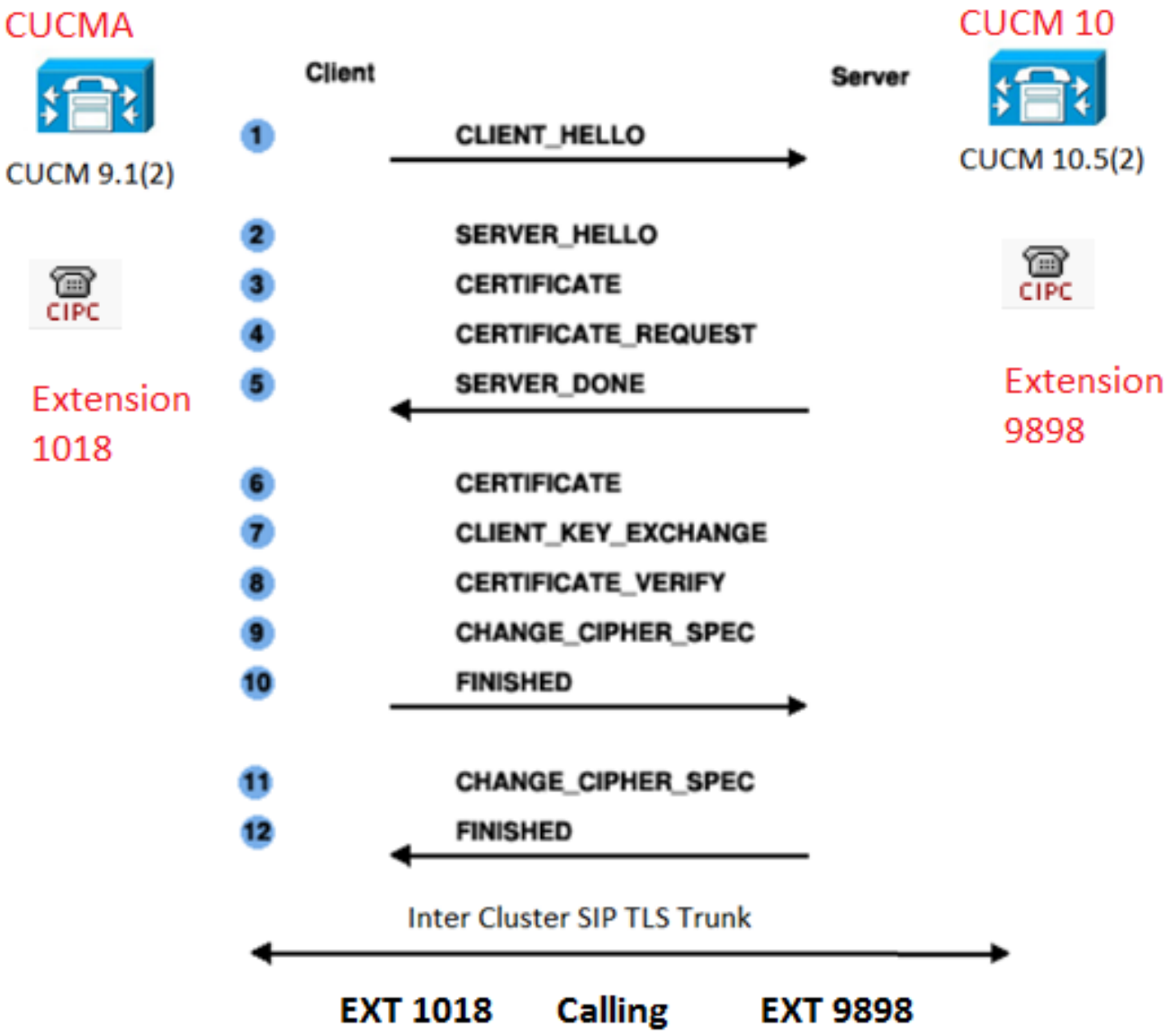
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

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

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

كما هو موضح في هذه الصورة، مصافحة SSL باستخدام الشهادات.



التكوين

الخطوة 1. أستخدم المرجع المصدق العام أو مرجع مصدق الإعداد على Windows Server 2003

ارجع إلى الارتباط: إعداد المرجع المصدق على خادم Windows 2003

الخطوة 2. التحقق من اسم المضيف والإعدادات

تعتمد الشهادات على الأسماء. تأكد من صحة الأسماء قبل البدء.

```
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
```

لتغيير اسم المضيف، ارجع إلى الارتباط: تغيير اسم المضيف على CUCM

الخطوة 3. إنشاء طلب توقيع الشهادة (CSR) وتنزيله

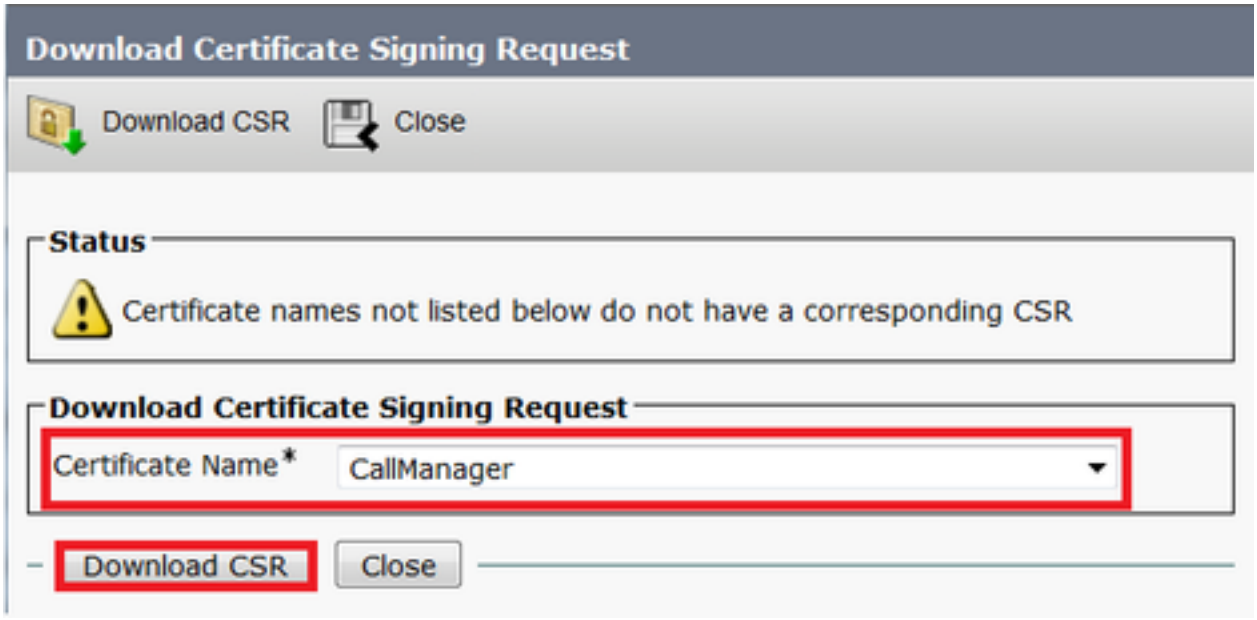
CUCM 9.1(2)

لإنشاء CSR، انتقل إلى **إدارة نظام التشغيل > الأمان > إدارة الشهادة>إنشاء CSR**

في حقل **اسم الشهادة**، حدد خيار **CallManager** من القائمة المنسدلة.

لتنزيل CSR، انتقل إلى **إدارة نظام التشغيل > الأمان > إدارة الشهادات > تنزيل CSR**

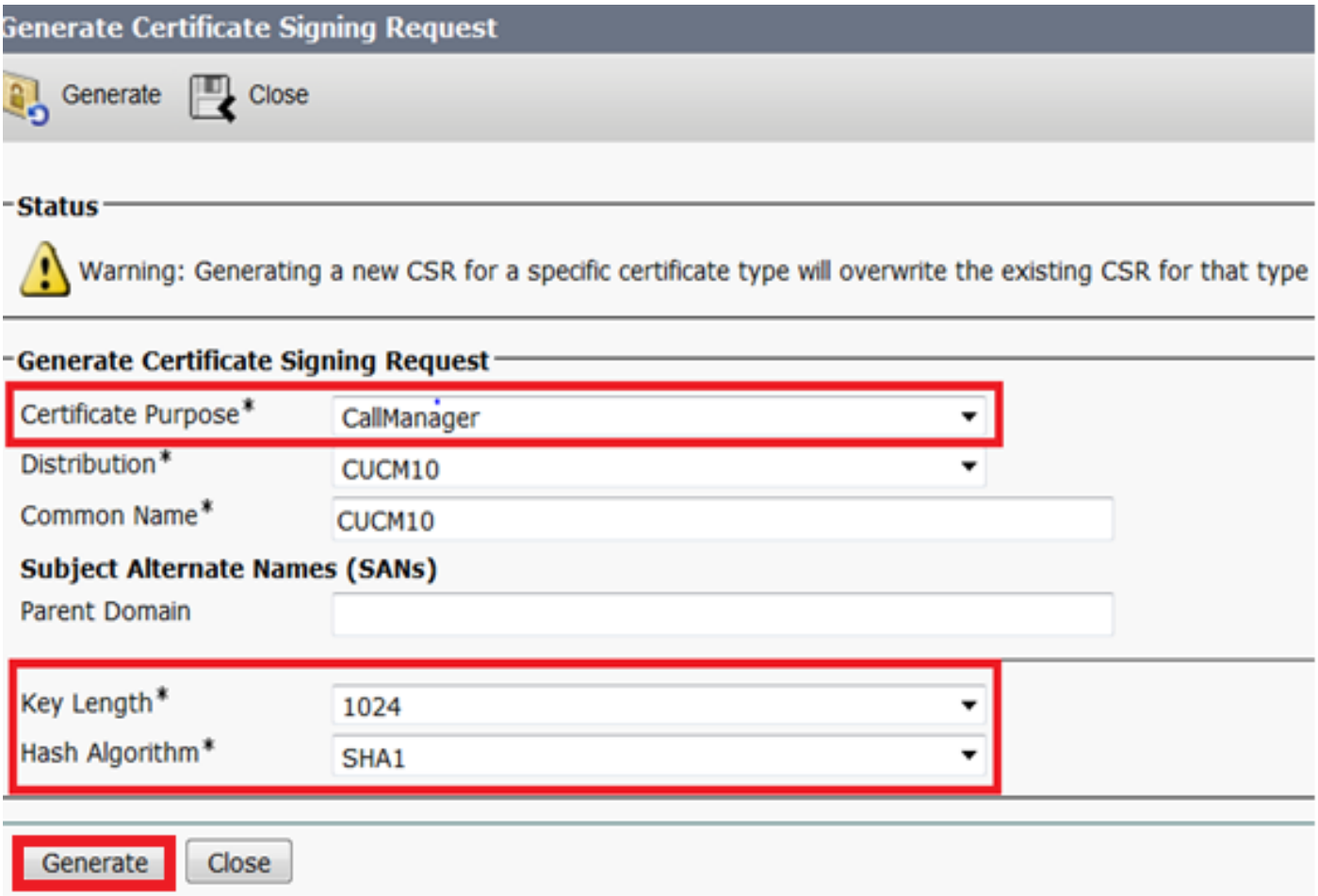
في حقل **اسم الشهادة**، حدد **خيار CallManager** من القائمة المنسدلة.



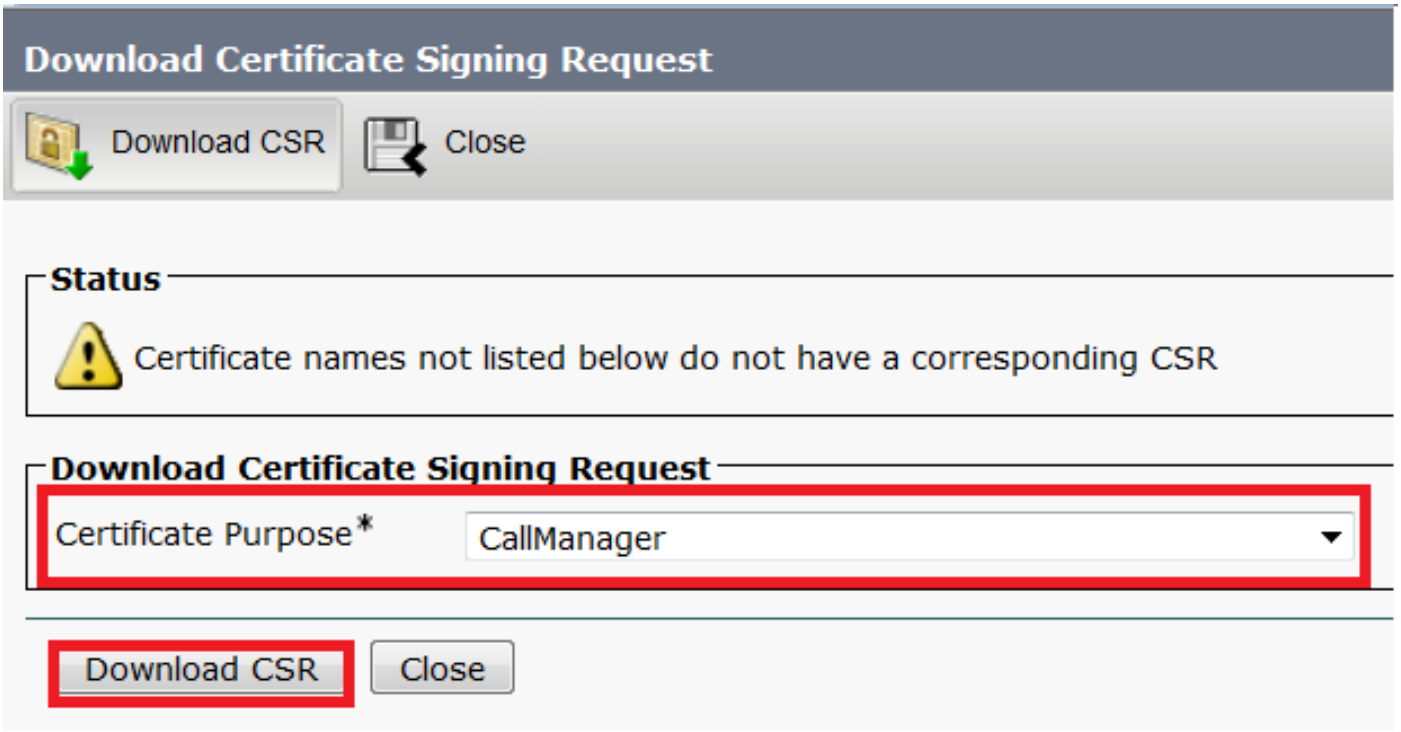
CUCM 10.5(2)

لإنشاء CSR، انتقل إلى **إدارة نظام التشغيل > الأمان > إدارة الشهادة > إنشاء CSR**

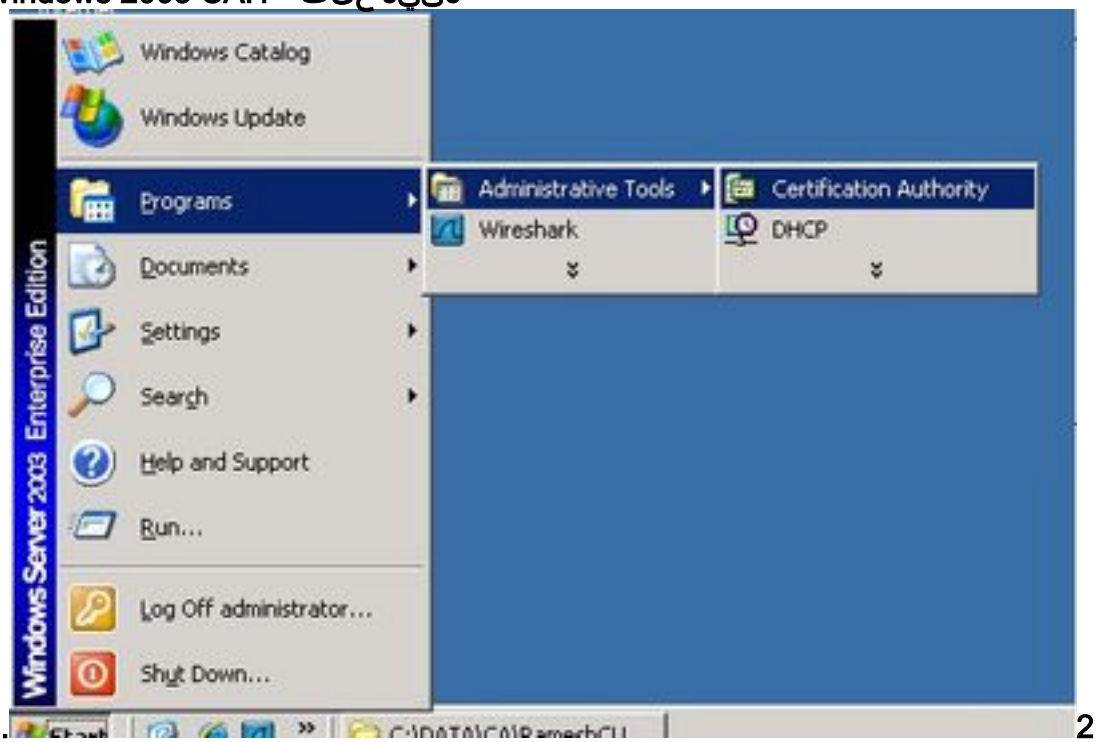
1. في حقل غرض الشهادة ، حدد CallManager من القائمة المنسدلة.
2. في حقل طول المفتاح، حدد 1024 من القائمة المنسدلة.
3. في حقل خوارزمية التجزئة، حدد SHA1 من القائمة المنسدلة.



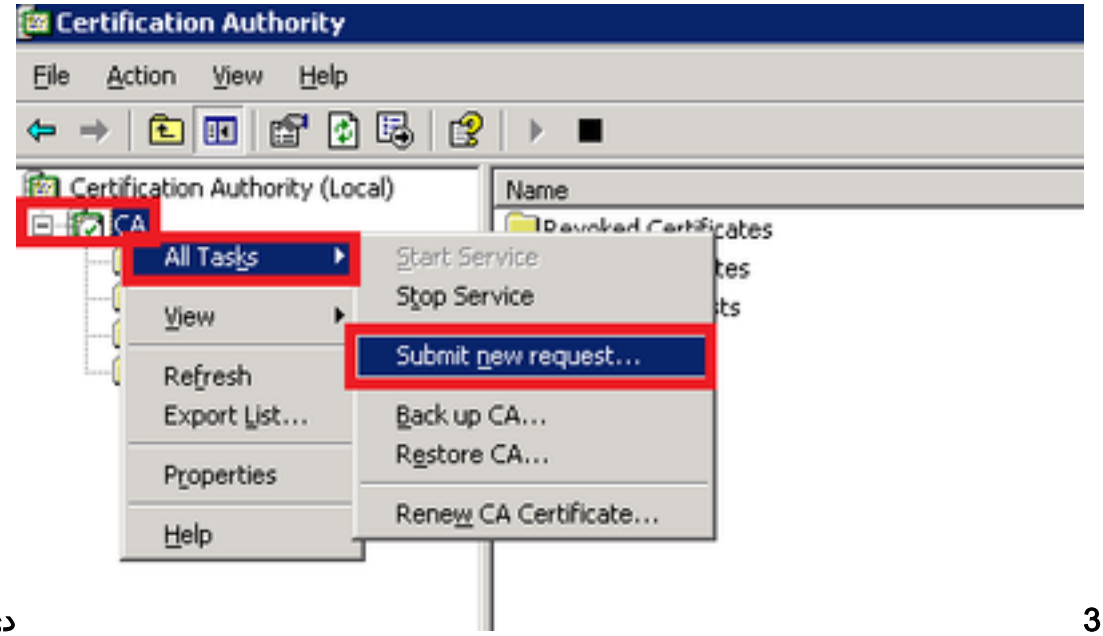
لتنزيل CSR، انتقل إلى **إدارة نظام التشغيل > الأمان > إدارة الشهادات > تنزيل CSR**في حقل غرض الشهادة، حدد خيار CallManager من القائمة المنسدلة.



ملاحظة: يتم إنشاء CallManager CSR باستخدام مفاتيح 1024 بت Rivest-Shamir-Addleman (RSA).الخطوة 4. توقيع CSR مع مرجع شهادات Microsoft Windows 2003هذه معلومات إختيارية لتوقيع CSR باستخدام Microsoft Windows 2003 CA.1 - فتح هيئة

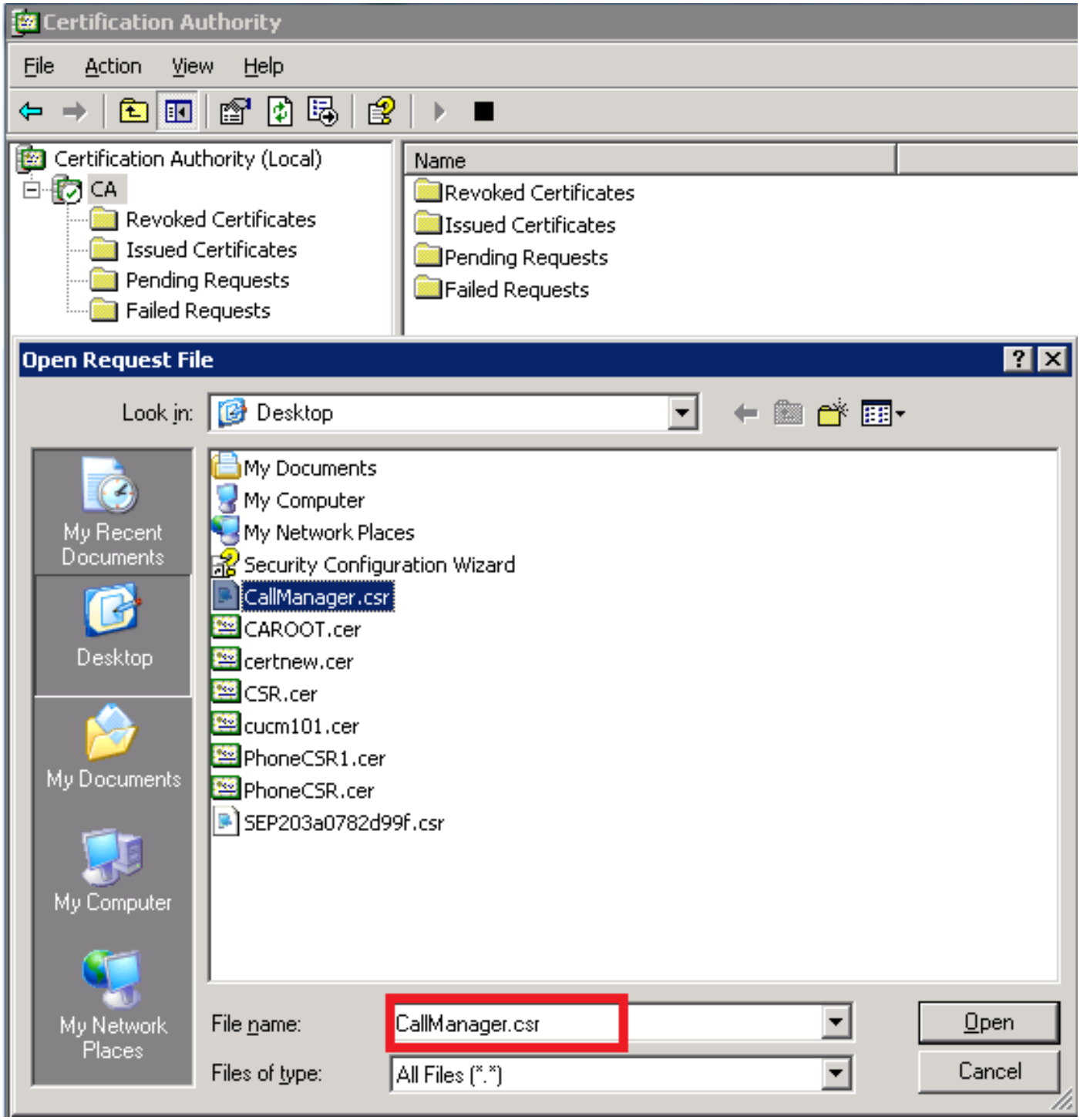


التصديق.2. انقر بزر الماوس الأيمن فوق أيقونة CA وانتقل إلى جميع المهام > إرسال طلب

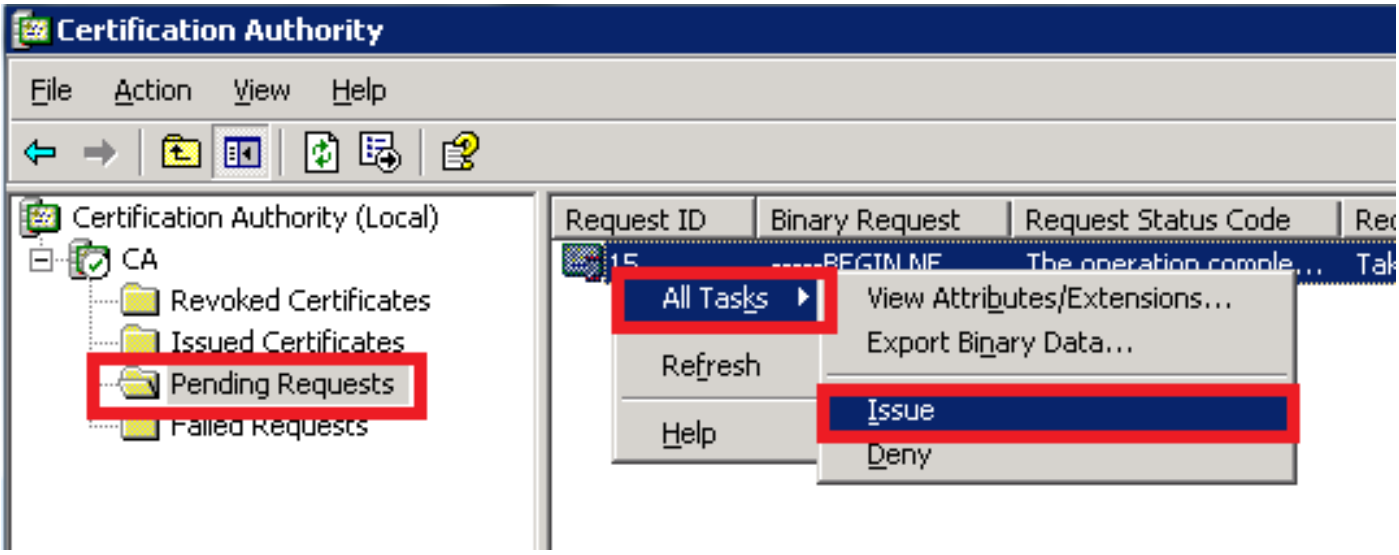


3. حدد CSR وانقر جديد

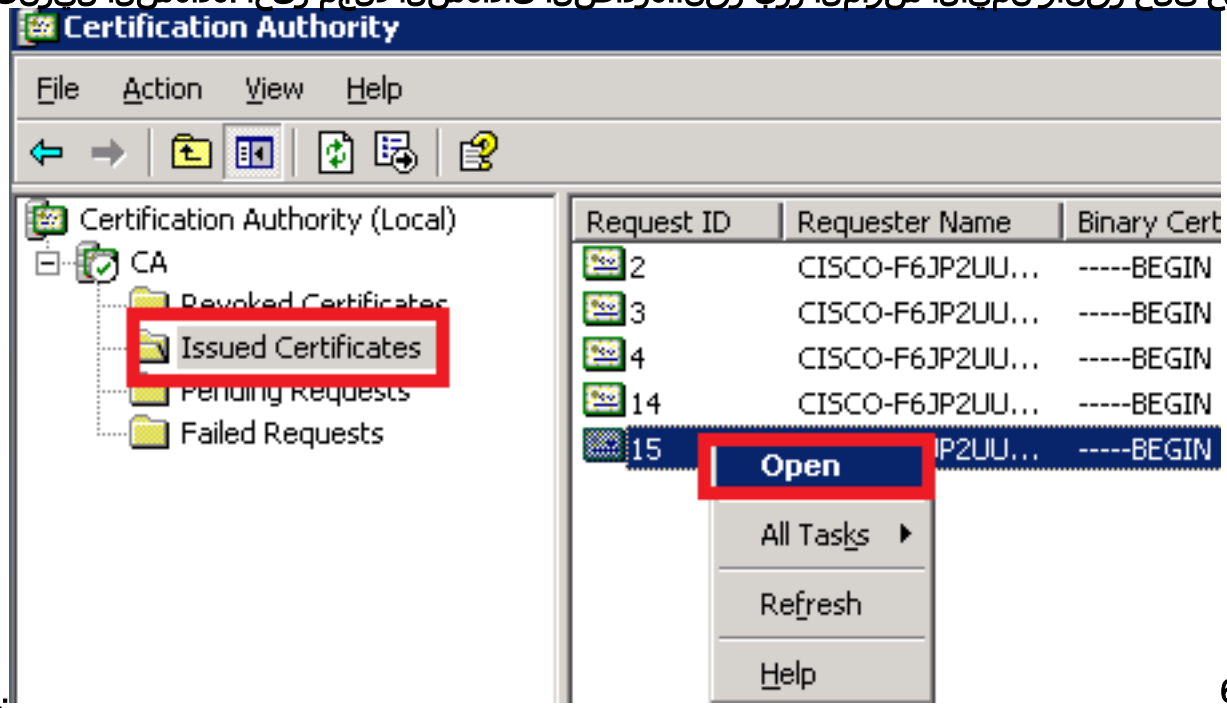
فوق الخيار فتح (ينطبق في كل من CSRs (CUCM 9.1(2) و CUCM 10.5(2))



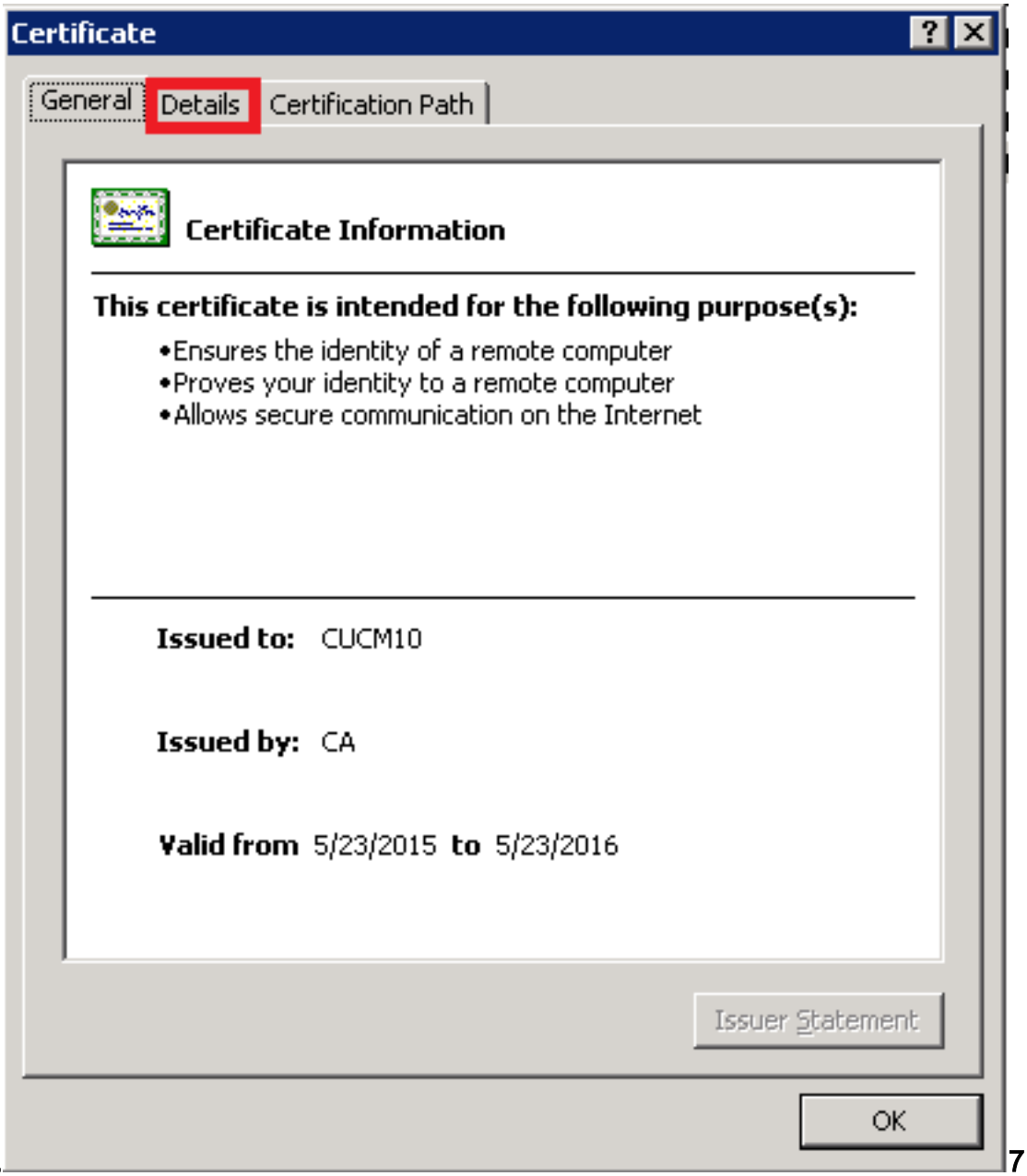
4. يتم عرض كافة CSRs المفتوحة في "مجلد الطلبات المعلقة". انقر بزر الماوس الأيمن على كل CSR وانتقل إلى كل المهام > إصدار إصدار الشهادات. (قابل للتطبيق في كل من CUCM 9.1(2) و CSRs (CUCM 10.5(2))



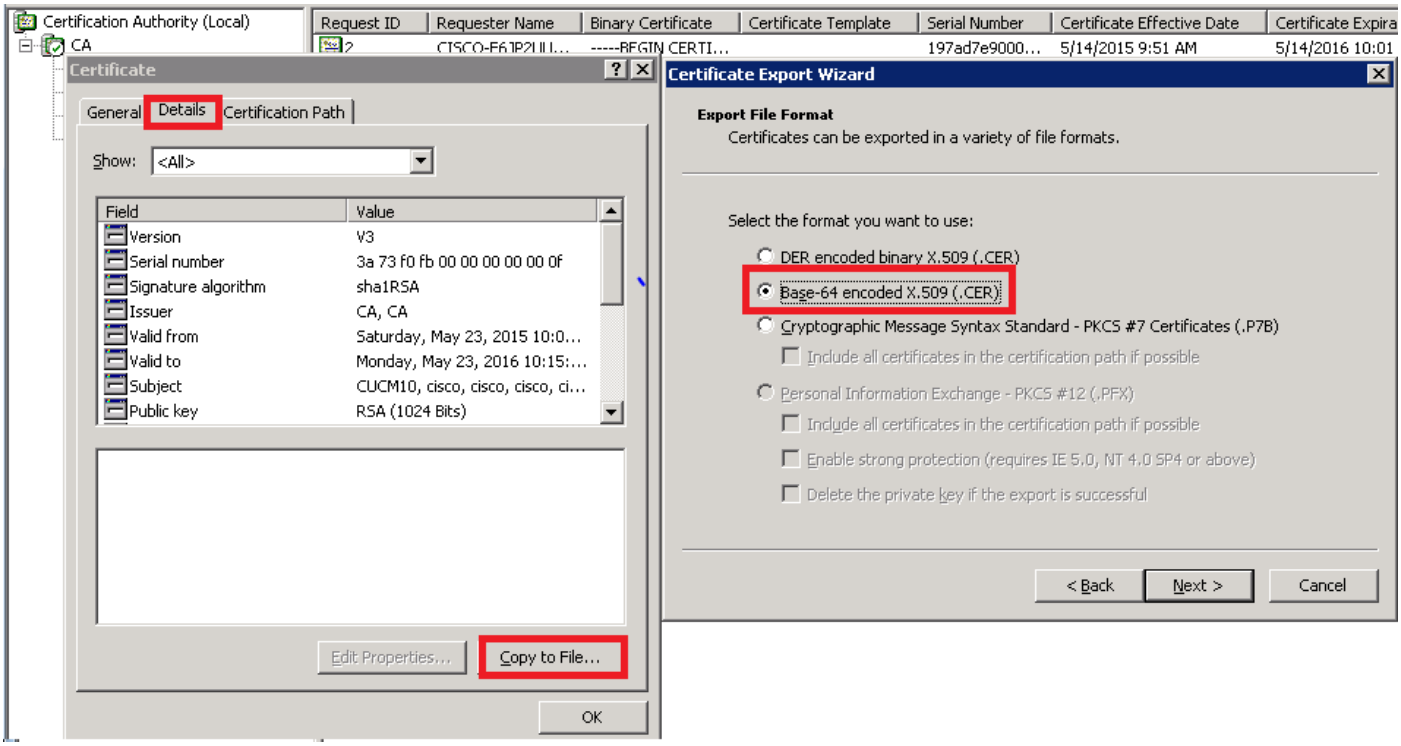
5. لتنزيل الشهادة، أختر مجلد الشهادات الصادرة.انقر بزر الماوس الأيمن وانقر علي خيار



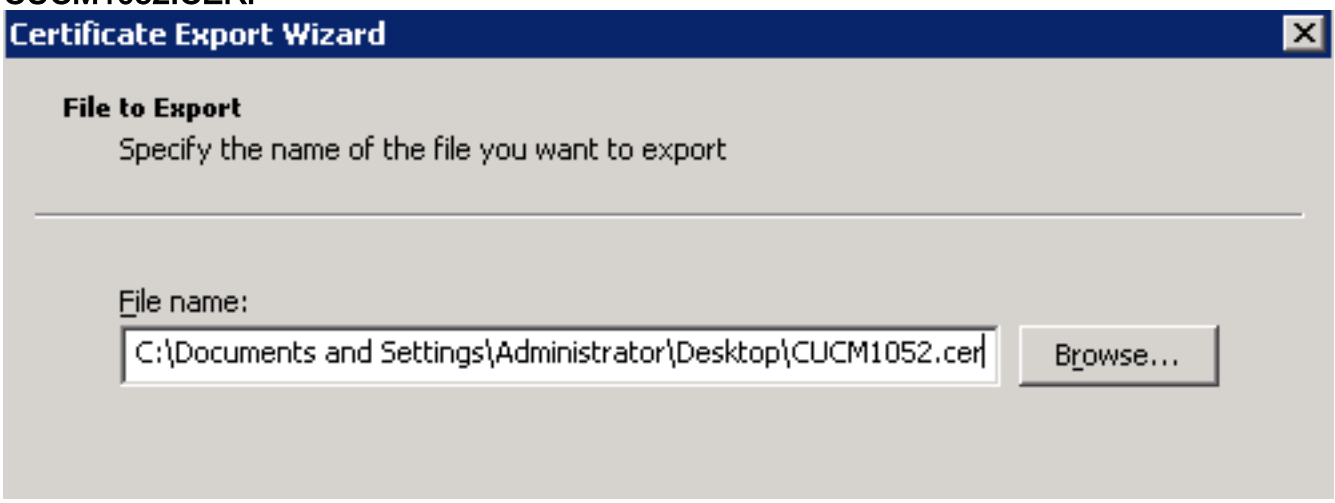
فتح. 6. يتم عرض تفاصيل الشهادة. لتنزيل الشهادة، حدد علامة التبويب تفاصيل وانقر فوق الزر



7. نسخ إلى ملف... في نافذة معالج تصدير الشهادات، انقر على زر راديو X.509(.CER) BASE-64 المشفر.

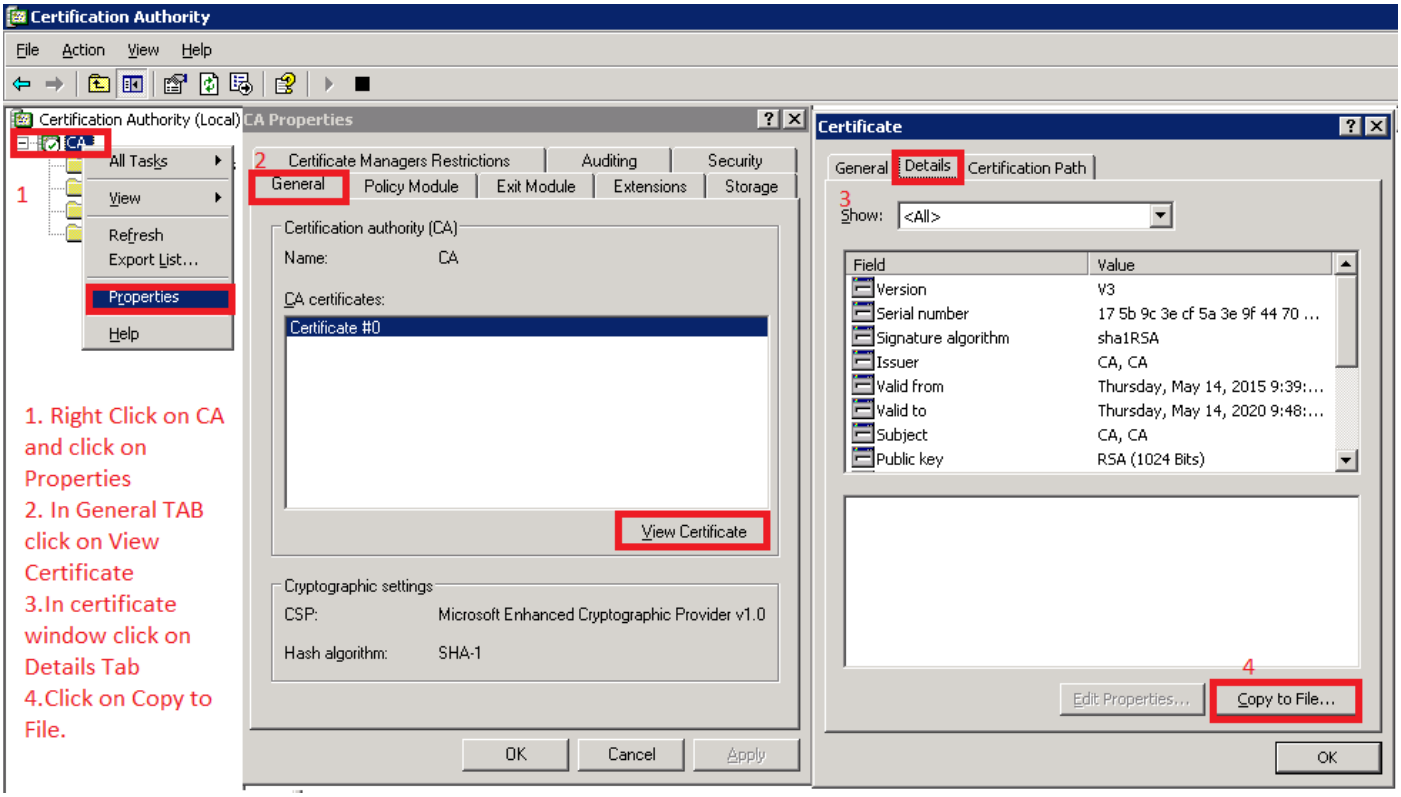


8. قم بتسمية الملف بدقة. يستخدم هذا المثال تنسيق CUCM1052.CER.

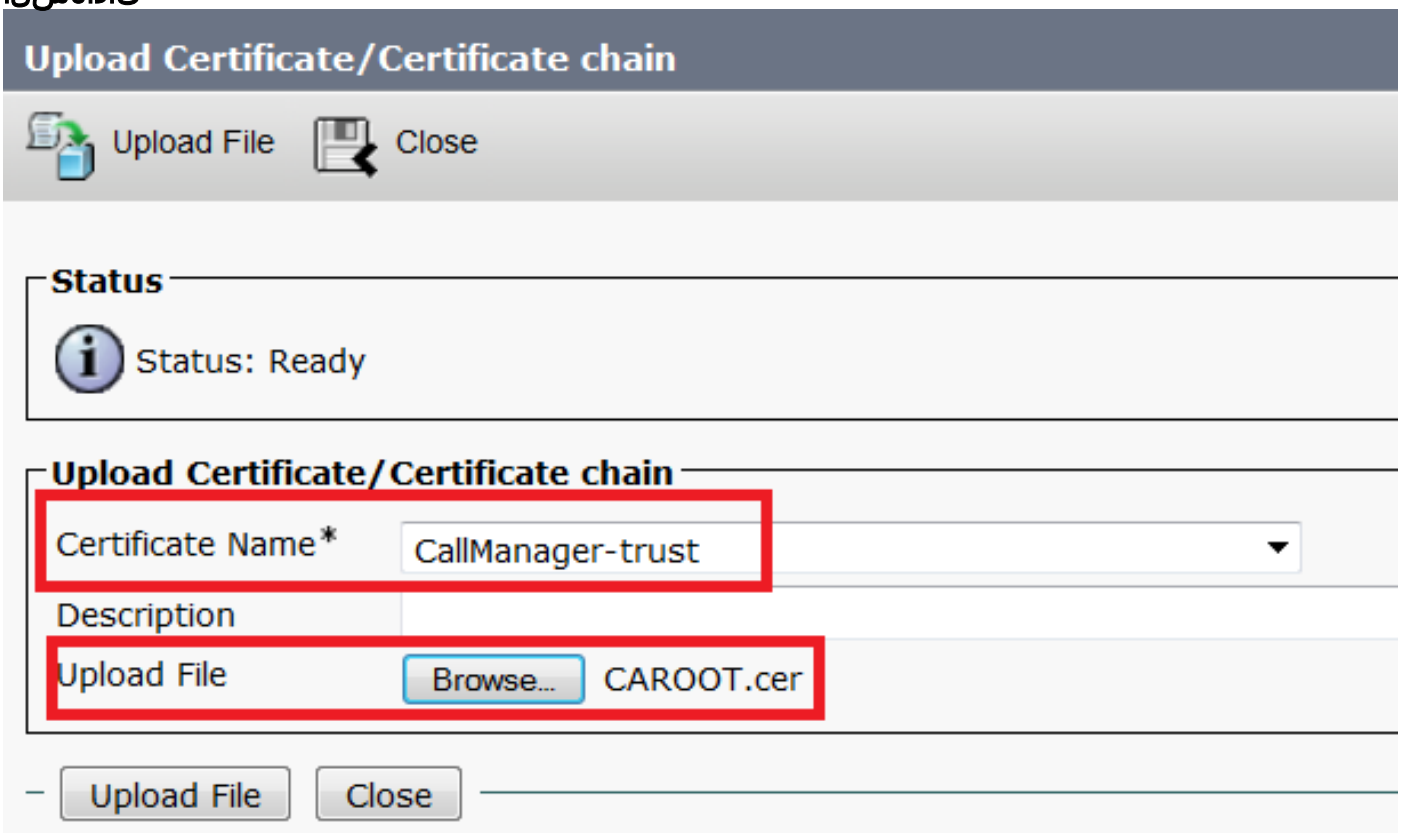


بال

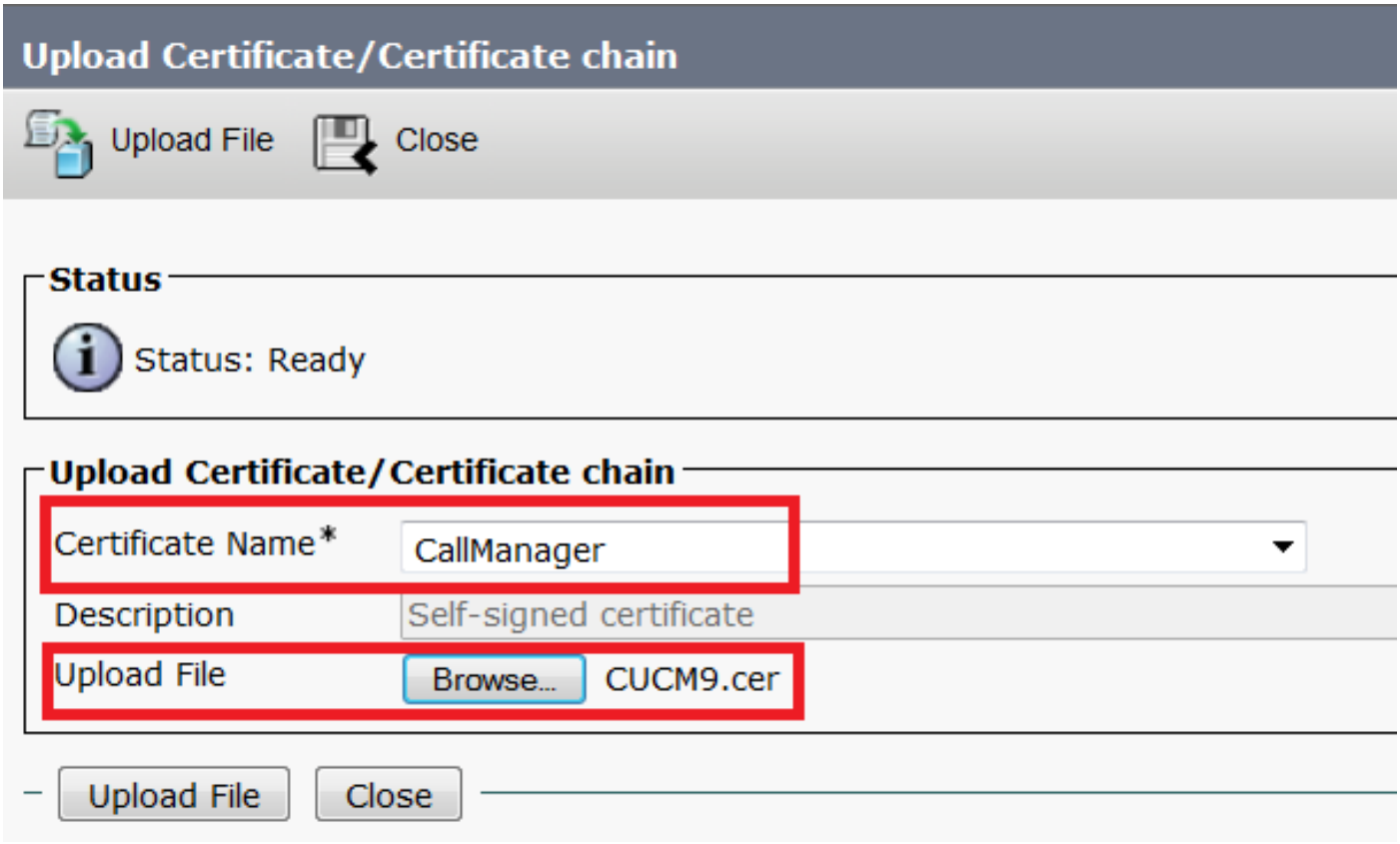
نسبة إلى CUCM 9.1(2)، اتبع الإجراء نفسه.الخطوة 5. الحصول على الشهادة الجذر من المرجع المصدقافتح نافذة المرجع المصدق. لتنزيل المرجع المصدق الجذر1. انقر بزر الماوس الأيمن فوق أيقونة CA وانقر فوق خيارات الخصائص.2. في علامة التبويب العامة، انقر فوق عرض الشهادة.3. في نافذة الشهادة، انقر فوق علامة التبويب تفاصيل.4. انقر فوق نسخ إلى ملف...



الخطوة 6. تحميل شهادة جذر CA كثقة CallManagerلتحميل شهادة جذر CA، قم بتسجيل الدخول إلى مسؤول نظام التشغيل > التأمين > إدارة الشهادة > تحميل الشهادة/سلسلة الشهادات

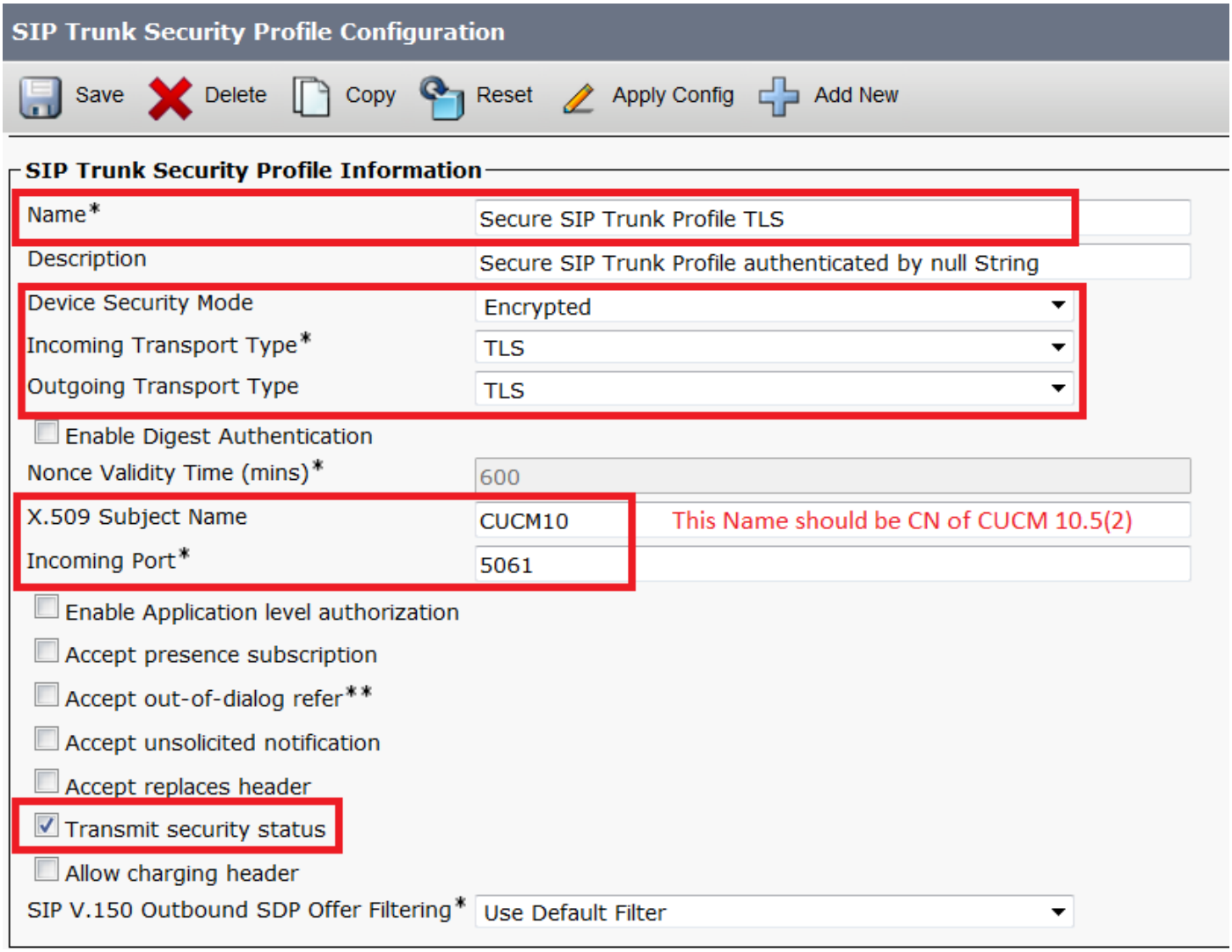


ملاحظة: تنفيذ هذه الخطوات على كل من CUCM (CUCM 9.1(2) و CUCM 10.5(2))الخطوة 7. تحميل شهادة CA Sign CallManager CSR كشهادة CallManager.من أجل تحميل CA Sign CallManager CSR، قم بتسجيل الدخول إلى مسؤول نظام التشغيل > الأمان > إدارة الشهادات > تحميل الشهادة/سلسلة الشهادات

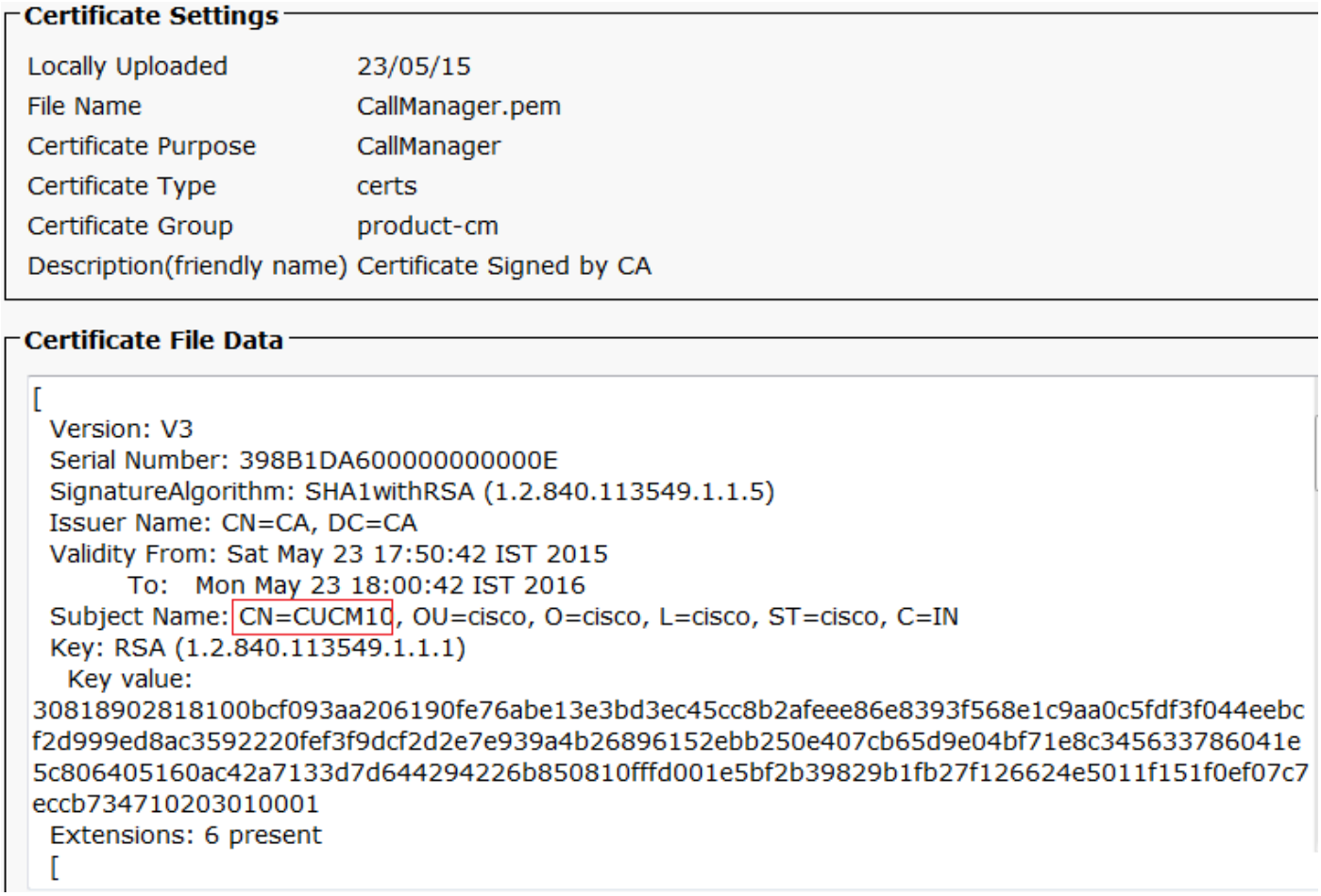


8. إنشاء ملفات الخطوة: تنفيذ هذه الخطوات على كل من CUCM (CUCM 9.1(2) و CUCM 10.5(2)) تعريف أمان خط اتصال SIP CUCM 9.1(2)

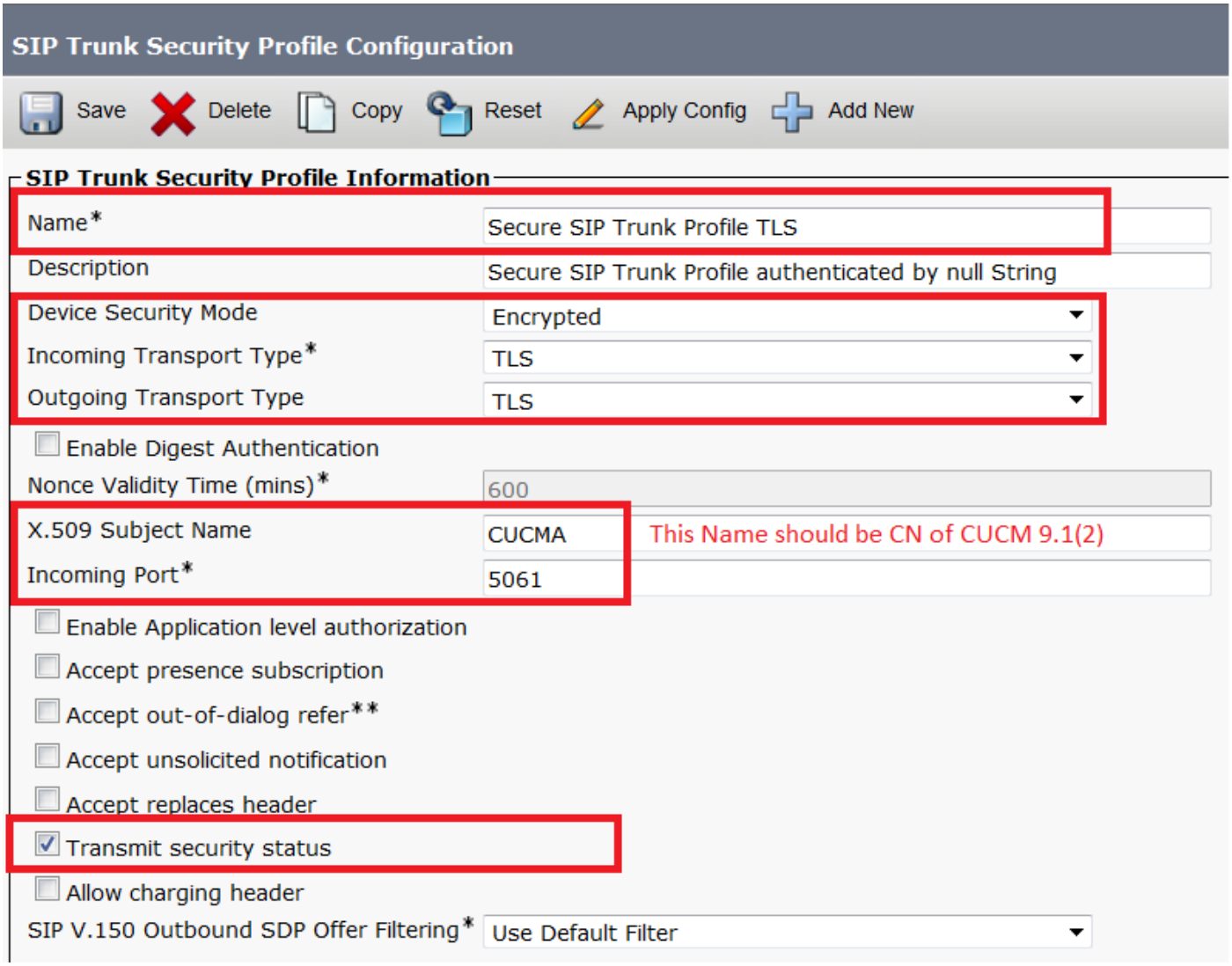
لإنشاء ملف تعريف أمان خط اتصال SIP، انتقل إلى النظام > الأمان > ملف تعريف أمان خط اتصال SIP. انسخ ملف تعريف خط اتصال SIP غير الآمن الموجود واعطائه اسما جديدا. في المثال، تمت إعادة تسمية ملف تعريف خط اتصال SIP غير الآمن باستخدام TLS لملف تعريف خط اتصال SIP الآمن.



في X.509 أستخدم اسم الموضوع الشائع (CN) من CUCM 10.5(2) (شهادة توقيع CA) كما هو موضح في هذه
الصورة.



CUCM 10.5(2)انتقل إلى النظام > الأمان > ملف تعريف أمان خط اتصال SIP.انسخ ملف تعريف خط اتصال SIP غير الآمن الموجود واعطائه اسما جديدا. في المثال، تمت إعادة تسمية ملف تعريف خط اتصال SIP غير الآمن باستخدام TLS لملف تعريف خط اتصال SIP الآمن.



في X.509 اسم الموضوع أستخدم CN الخاص ب CUCM 9.1(2) (شهادة CA الموقعة) كما هو مبرز:

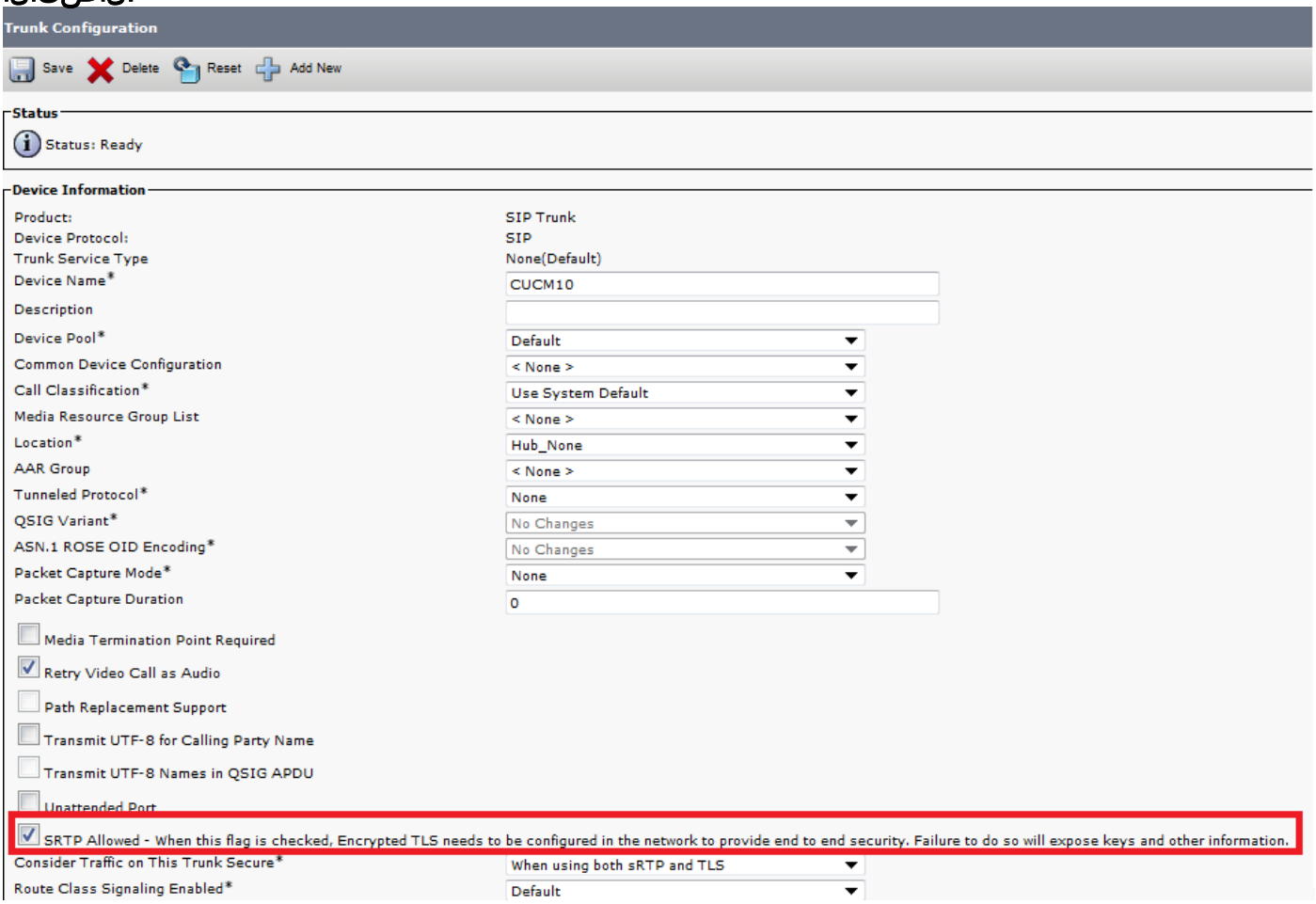
File Name	CallManager.pem
Certificate Name	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description	Certificate Signed by CA

Certificate File Data

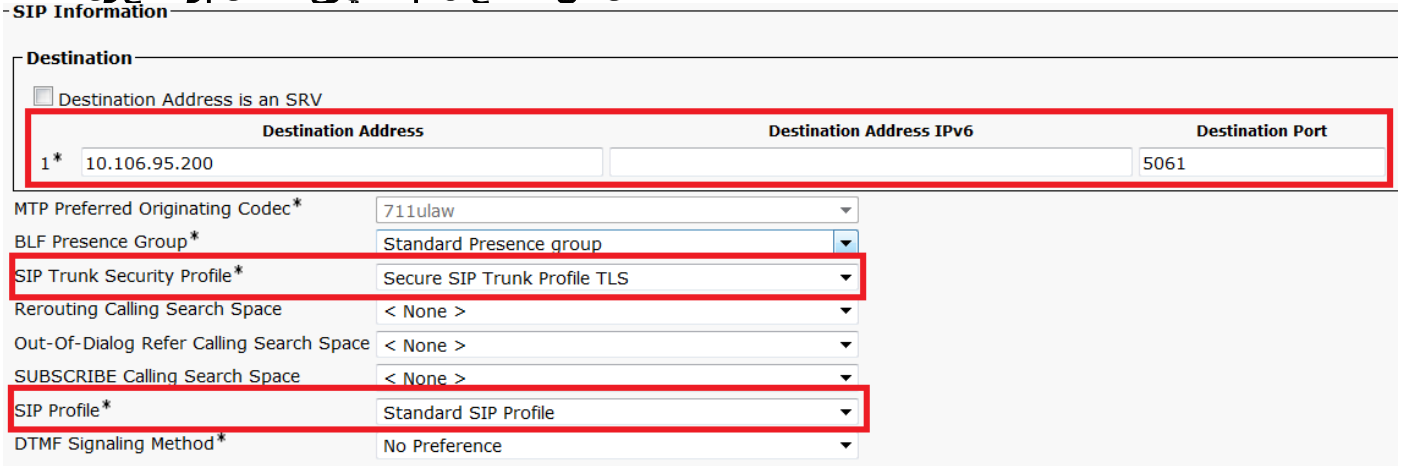
```
[
  Version: V3
  Serial Number: 120325222815121423728642
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=CA, DC=CA
  Validity From: Thu May 14 09:51:09 IST 2015
          To:   Sat May 14 10:01:09 IST 2016
  Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, 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,
```

تعمل كل من ملفات تعريف أمان خط اتصال SIP على تعيين منفذ وارد بقيمة 5061، حيث تستمع كل مجموعة إلى منفذ TCP رقم 5061 لمكالمات SIP TLS الواردة الجديدة.إنشاء 9. خطوط اتصال SIPبعد إنشاء توصيفات الأمان، قم بإنشاء خطوط اتصال SIP وأدخل التغييرات الخاصة بمعلمة التكوين التالية على خط اتصال SIP.CUCM 9.1(2)

1. على خانة الاختيار SIP Trunk Configuration، تحقق من معلمة التكوين SRTP Allowed. يؤمن هذا بروتوكول نقل الوقت الفعلي (RTP) الذي سيتم إستخدامه للمكالمات عبر خط الاتصال هذا. يجب تحديد هذا المربع فقط عند إستخدام SIP TLS لأن المفاتيح الخاصة ببروتوكول نقل الوقت الفعلي الآمن (SRTP) يتم تبادلها في نص رسالة SIP. يجب تأمين إرسال إشارات SIP بواسطة TLS، وإلا يمكن لأي شخص لديه إشارات SIP غير الآمنة فك تشفير تدفق SRTP المتوافق عبر خط الاتصال.



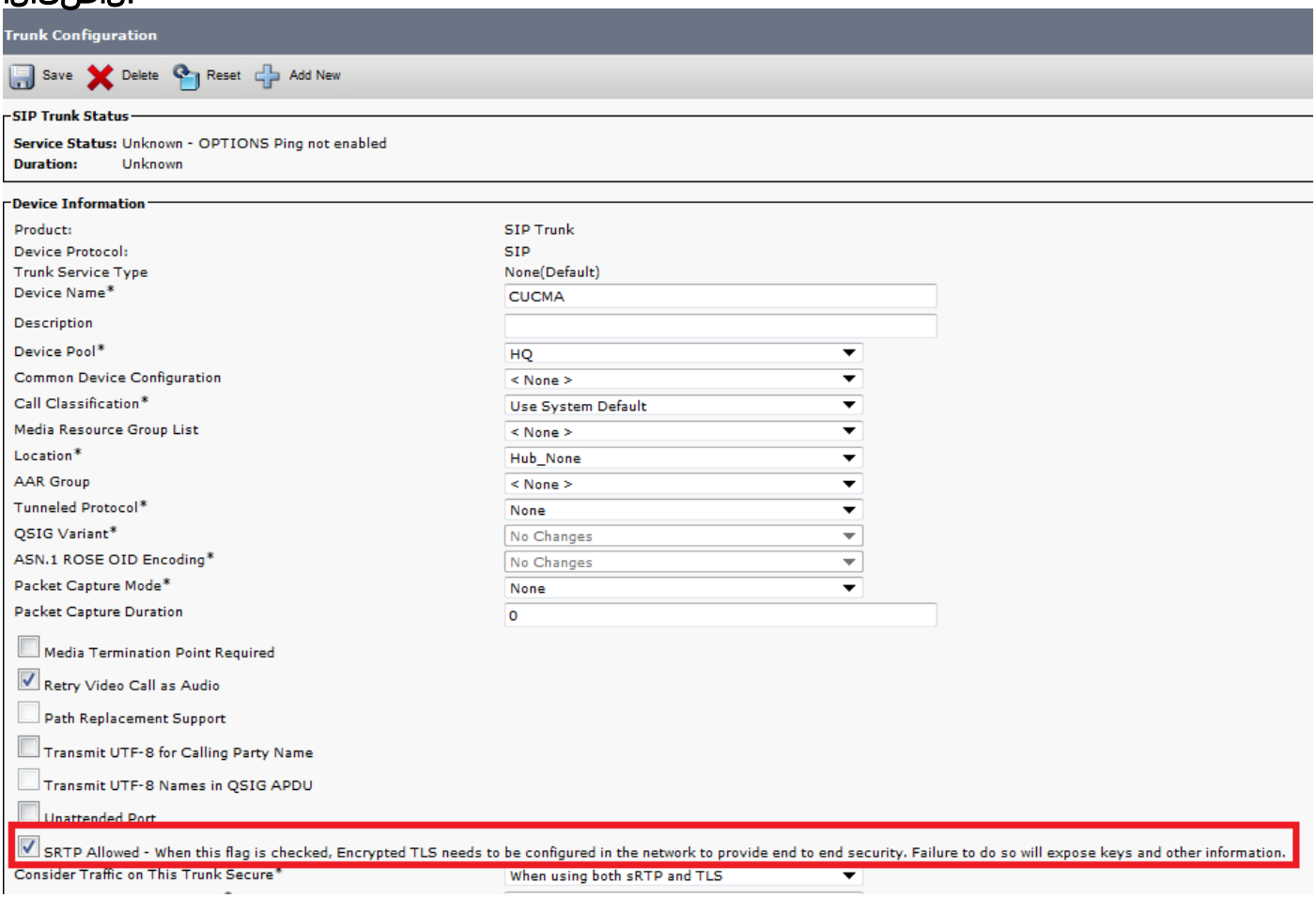
2. على قسم معلومات SIP من نافذة تكوين خط اتصال SIP، أضف عنوان الوجهة، ومنفذ الوجهة، وملف تعريف أمان خط اتصال SIP.



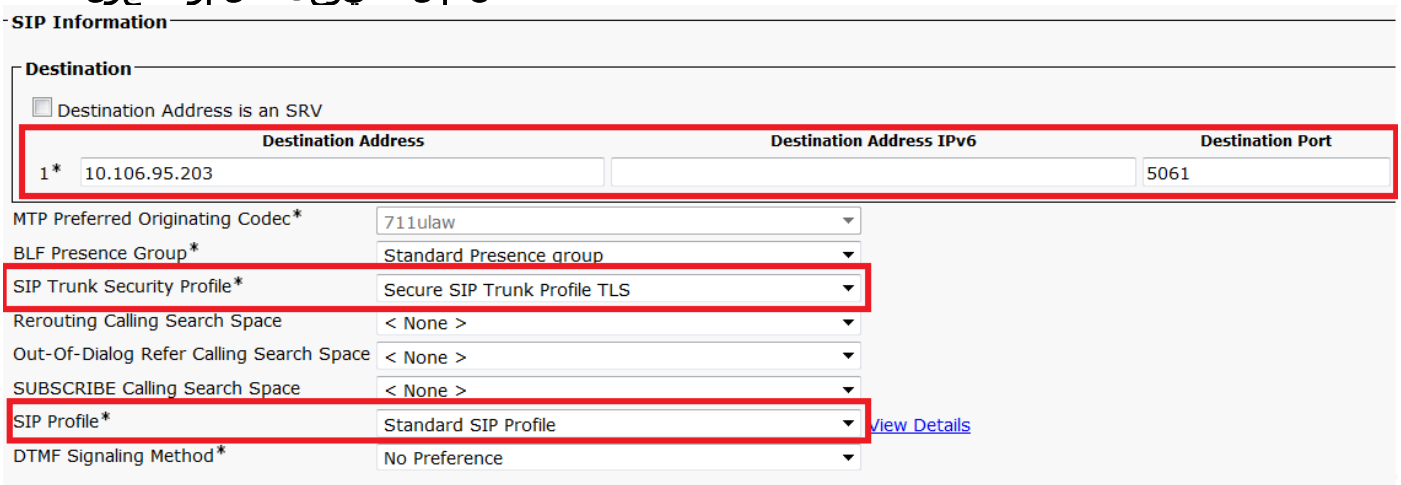
CUCM 10.5(2)

1. على خانة الاختيار SIP Trunk Configuration، تحقق من معلمة التكوين SRTP Allowed.

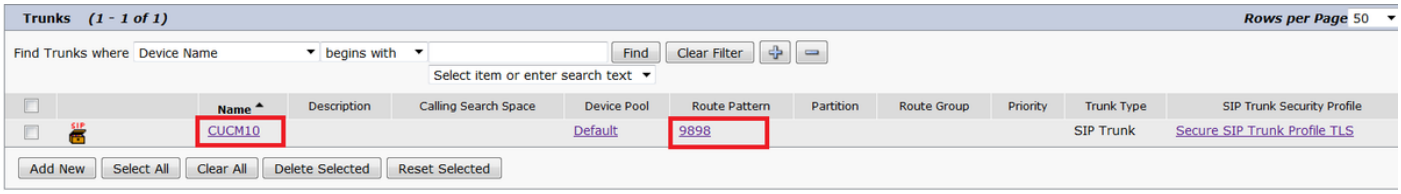
وهذا يسمح باستخدام SRTP للمكالمات عبر خط الاتصال هذا. يجب تحديد هذا المربع فقط عند استخدام SIP TLS، لأن مفاتيح SRTP يتم تبادلها في نص رسالة SIP. يجب تأمين الرسال إشارات SIP بواسطة TLS لأن أي شخص لديه إشارات SIP غير آمنة يمكنه فك تشفير تدفق RTP الآمن المتوافق عبر خط
الاتصال.



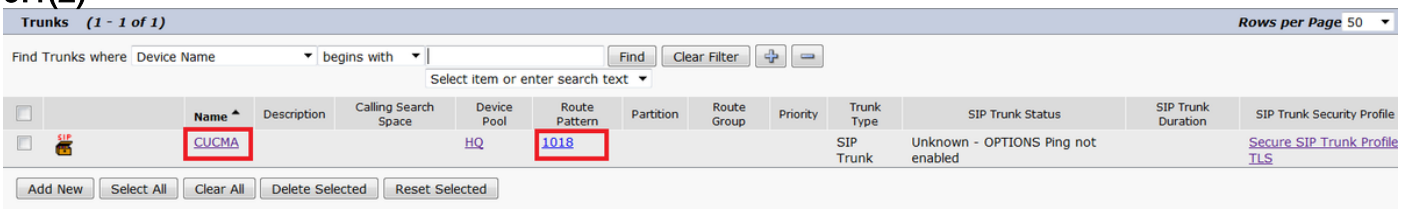
2. على قسم معلومات SIP من نافذة تكوين خط اتصال SIP، أضف عنوان IP للوجهة، ومنفذ الوجهة، وملف تعريف الأمان



الخطوة 10. إنشاء أنماط المسارأبسط طريقة هي إنشاء نمط مسار على كل مجموعة، مع الإشارة مباشرة إلى خط اتصال SIP. كما يمكن استخدام مجموعات المسارات وقوائم المسارات.يشير CUCM 9.1(2) إلى نمط المسار 9898 من خلال خط اتصال TLS SIP إلى CUCM 10.5(2)



يشير CUCM 10.5(2) إلى نمط المسار 1018 عبر خط اتصال TLS SIP إلى CUCM 9.1(2)



التحقق من الصحة

اذه ال يوجد حالي أجراء للتحقق من صحة التكوين.

استكشاف الأخطاء وإصلاحها

يمكن تصحيح أخطاء إستدعاء SIP TLS باستخدام هذه الخطوات. تجميع التقاط الحزم على CUCM للتحقق من الاتصال بين CUCM 9.1(2) و CUCM 10.5(2)، يمكنك التقاط حزمة على خوادم CUCM ومراقبة حركة مرور SIP TLS. بثبت ال SIP TLS حركة مرور على ال TCP ميناء 5061، يري بما أن sip-tls. في المثال التالي، هناك جلسة واجهة سطر الأوامر (CLI) ل SSH التي تم إنشاؤها ل CUCM 9.1(2)1. التقاط حزمة واجهة سطر الأوامر (CLI) على الشاشةتطبع واجهة سطر الأوامر (CLI) هذه المخرجات على الشاشة لحركة مرور 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>
```

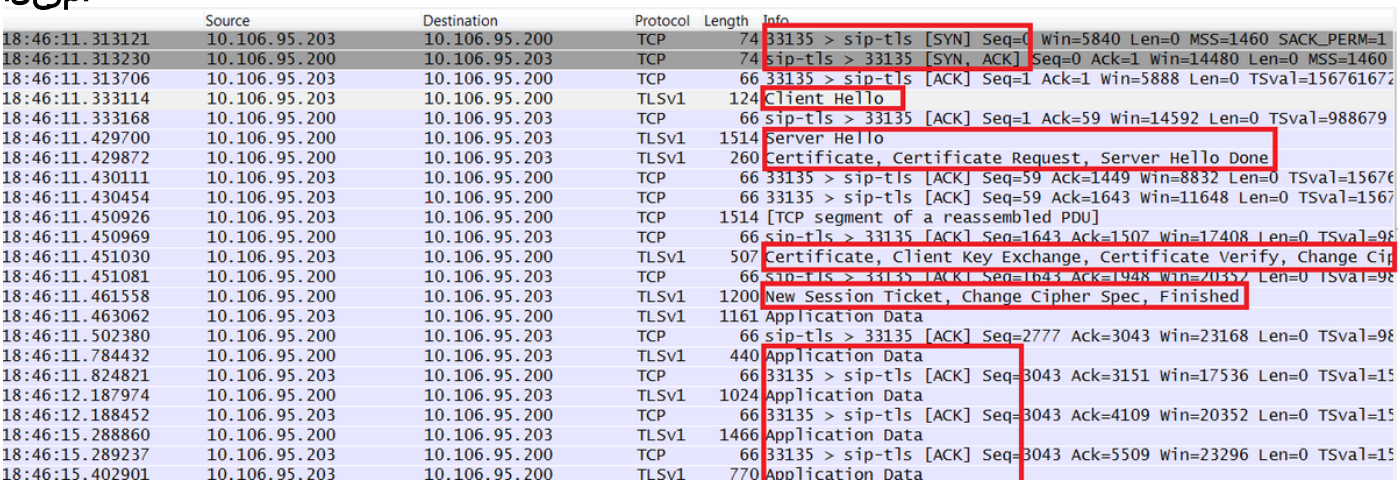
2. CLI يلتقط إلى ملف يوفر CLI هذا بالتقاط الحزمة بناء على المضيف وينشئ ملف يعين ربط.

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

أعد تشغيل خط اتصال SIP على CUCM 9.1(2) وأجر المكالمة من المدخل 1018 (CUCM 9.1(2)) إلى المدخل 9898 (CUCM 10.5(2))in order to جلب المبرد من ال CLI، ركض هذا أمر:

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

ويتم الالتقاط بتنسيق .cap القياسي. يستخدم هذا المثال Wireshark لفتح ملف packet.cap ولكن يمكن إستخدام أي أداة عرض لالتقاط الحزم.

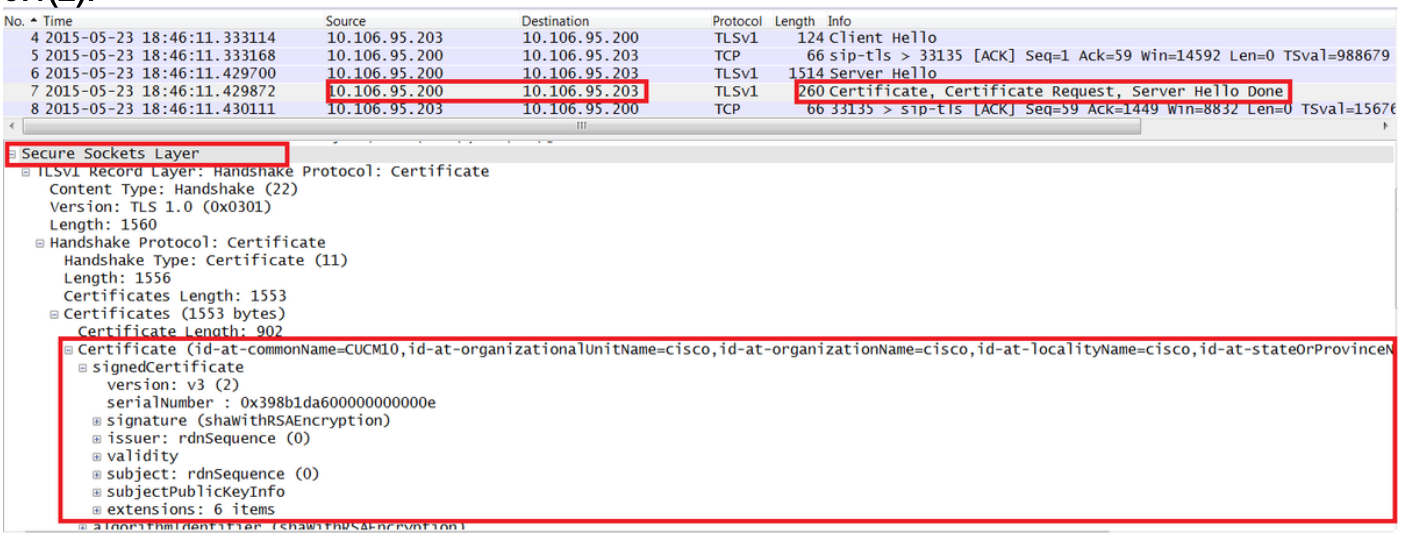


	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	sip-tls > 33135 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
18:46:11.313706	10.106.95.203	10.106.95.200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

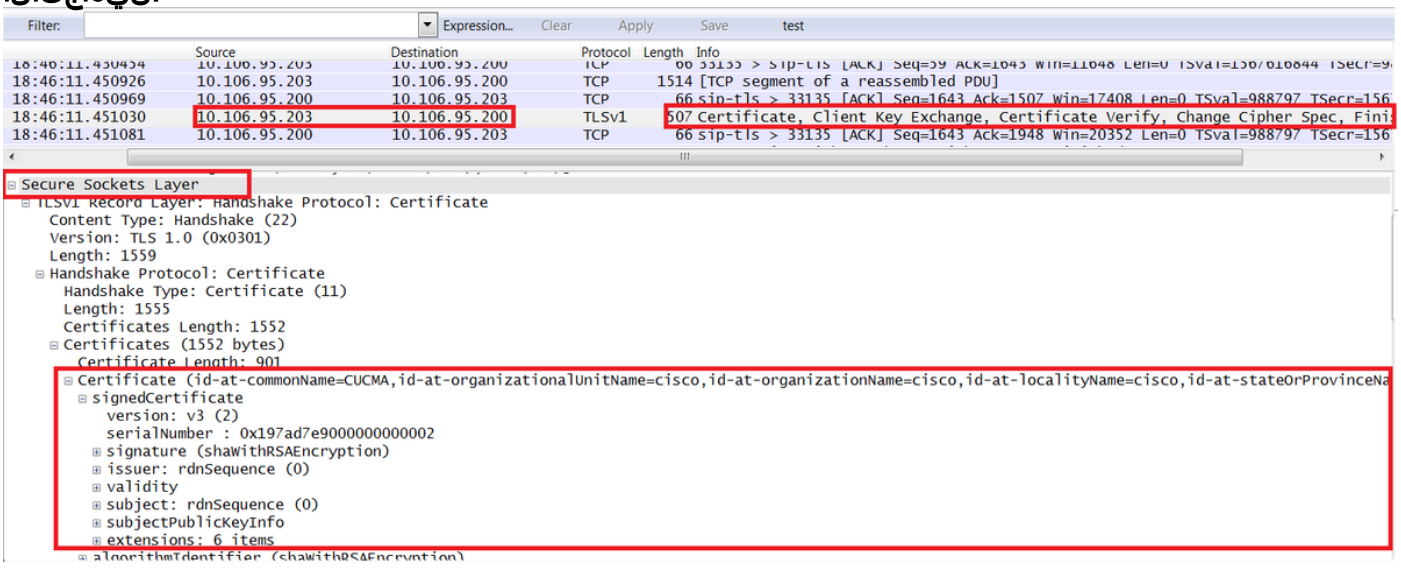
1. مزامنة بروتوكول التحكم في الإرسال (TCP) (SYN) لإنشاء اتصال TCP بين CUCM 9.1(2)(العميل) و CUCM 10.5(2)(الخادم).

2. يرسل CUCM 9.1(2) ترحيب العميل لبدء جلسة TLS.
3. يرسل CUCM 10.5(2) رسالة "مرحبا على الخادم"، و"شهادة الخادم"، و"طلب الشهادة" لبدء عملية تبادل الشهادات.
4. الشهادة التي يرسلها العميل CUCM 9.1(2) لإكمال تبادل الشهادات.
5. تظهر بيانات التطبيق التي يتم تشفير إشارات SIP، أنه قد تم إنشاء جلسة TLS.

تحقق أكثر مما إذا كان يتم تبادل الشهادات الصحيحة. بعد Server Hello، يرسل CUCM 10.5(2) الخاص بالخادم شهادته إلى العميل CUCM 9.1(2).



يتم تقديم الرقم التسلسلي ومعلومات الموضوع الخاصة بالخادم CUCM 10.5(2) إلى العميل CUCM 9.1(2).يتم مقارنة الرقم التسلسلي والموضوع والإصدار وتواريخ الصلاحية بالمعلومات الموجودة في صفحة إدارة شهادات مسؤول نظام التشغيل.يقدم الخادم CUCM 10.5(2) شهادته الخاصة للتحقق، والآن يتحقق من شهادة العميل CUCM 9.1(2). ويتم التحقق في كل
الاتجاهين.



إذا كان هناك عدم تطابق بين الشهادات في التقاط الحزمة والشهادات في صفحة الويب الخاصة بإدارة نظام التشغيل، فلا يتم تحميل الشهادات الصحيحة.يجب تحميل الشهادات الصحيحة على صفحة شهادة مسؤول OS.تجميع مسارات CUCMكما يمكن أن تكون آثار CUCM مفيدة لتحديد الرسائل المتبادلة بين خوادم CUCM 9.1(2) و CUCM 10.5(2) وما إذا كانت جلسة SSL قد تم إنشاؤها بشكل صحيح أم لا.وفي المثال، تم تجميع الأثار من CUCM 9.1(2).تدفق المكالمات:الهاتف الفرعي 1018 > CUCM 9.1(2) > خط اتصال SIP TLS > CUCM 10.5(2) > الهاتف الفرعي 9898++ تحليل الأرقام

```
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
```

يتم إستخدام ++ SIP TLS على المنفذ 5061 لهذه المكالمة.

```
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
```

++ طبقة توزيع الإشارات (SDL)يقدم Find تفاصيل حول CN للموضوع ومعلومات الاتصال.

```
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 =
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).