使用CA簽名證書在CUCM-CUBE/CUBE-SBC之間配置SIP TLS

目錄

簡介

本文檔介紹如何使用證書頒發機構(CA)簽名的證書在思科統一通訊管理器(CUCM)和思科統一邊界元素(CUBE)之間配置SIP傳輸層安全(TLS)。

必要條件

思科建議瞭解以下主題

- SIP通訊協定
- 安全憑證

需求

- 端點的日期和時間必須匹配（建議使用相同的NTP源）。
- CUCM必須處於混合模式。
- 需要TCP連線（任何傳輸防火牆上的開放埠5061）。
- CUBE必須安裝安全和統一通訊K9(UCK9)許可證。

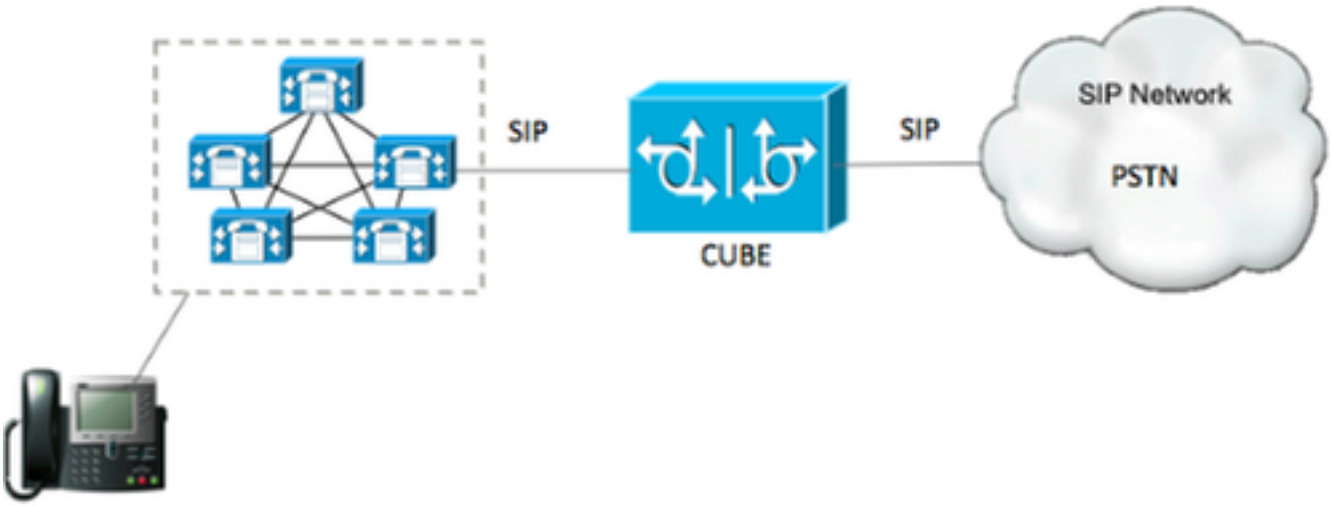
附註：對於Cisco IOS-XE版本16.10，平台已移至智慧許可。

採用元件

- SIP
- 證書頒發機構簽名的證書
- Cisco IOS和IOS-XE網關2900 / 3900 / 4300 / 4400 / CSR1000v / ASR100X版本：15.4+
- 思科整合通訊管理員(CUCM)版本：10.5+

設定

網路圖表



組態

步驟1。您將使用命令建立與根證書的證書長度匹配的RSA金鑰：

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

此命令建立長度為2048位（最大為4096）的RSA金鑰。

步驟2.使用命令建立信任點以儲存CA簽名的證書：

```
 Crypto pki trustpoint CUBE_CA_CERT
   serial-number none
   fqdn none
   ip-address none
   subject-name cn=ISR4451-B.cisco.lab !(this has to match the router’s hostname
[hostname.domain.name])
   revocation-check none
   rsakeypair TestRSAkey !(this has to match the RSA key you just created)
```

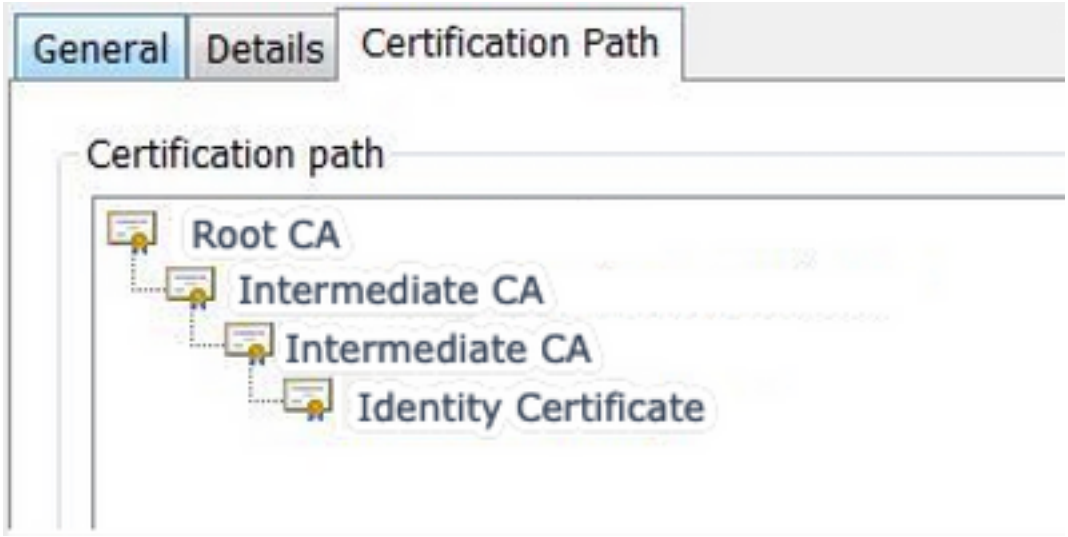
步驟3. 現在您已擁有我們的信任點，您將使用以下命令生成我們的CSR請求：

```
 Crypto pki enroll CUBE_CA_CERT
```

回答螢幕上的問題，然後複製CSR請求，將其儲存到檔案，然後傳送給CA。

步驟4.您需要瞭解根憑證鏈結是否有任何中間憑證；如果沒有中間證書頒發機構，跳轉到步驟7，否則繼續步驟6。

步驟5.建立信任點以儲存根證書，另外建立信任點以儲存任何中間CA，直到對CUBE證書進行簽名的CA（請參閱下圖）。



在本例中，第1級是根CA，第2級是第一個中間CA，第3級是簽署CUBE證書的CA，因此，您需要建立一個信任點以使用這些命令持有前2個證書。

```
Crypto pki trustpoint Root_CA_CERT
Enrollment terminal pem
Revocation-check none

Crypto pki authenticate Root_CA_CERT
Paste the X.64 based certificate here

Crypto pki trustpoint Intermediate_CA
Enrollment terminal
Revocation-check none

Crypto pki authenticate Intermediate_CA
```

步驟6. 收到我們的CA簽名證書後，您將驗證信任點，信任點需要持有CA的證書在CUBE證書之前；允許匯入憑證的命令為，

```
Crypto pki authenticate CUBE_CA_CERT
```

步驟7.安裝我們的證書後，需要運行此命令才能匯入我們的CUBE證書

```
  Crypto pki import CUBE_CA_CERT cert
```

步驟8.配置SIP-UA以使用您建立的信任點

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

步驟9. 配置撥號對等體，如下所示：

```
  dial-peer voice 9999 voip
  answer-address 35..
  destination-pattern 9999
  session protocol sipv2
  session target dns:cucm10-5
```

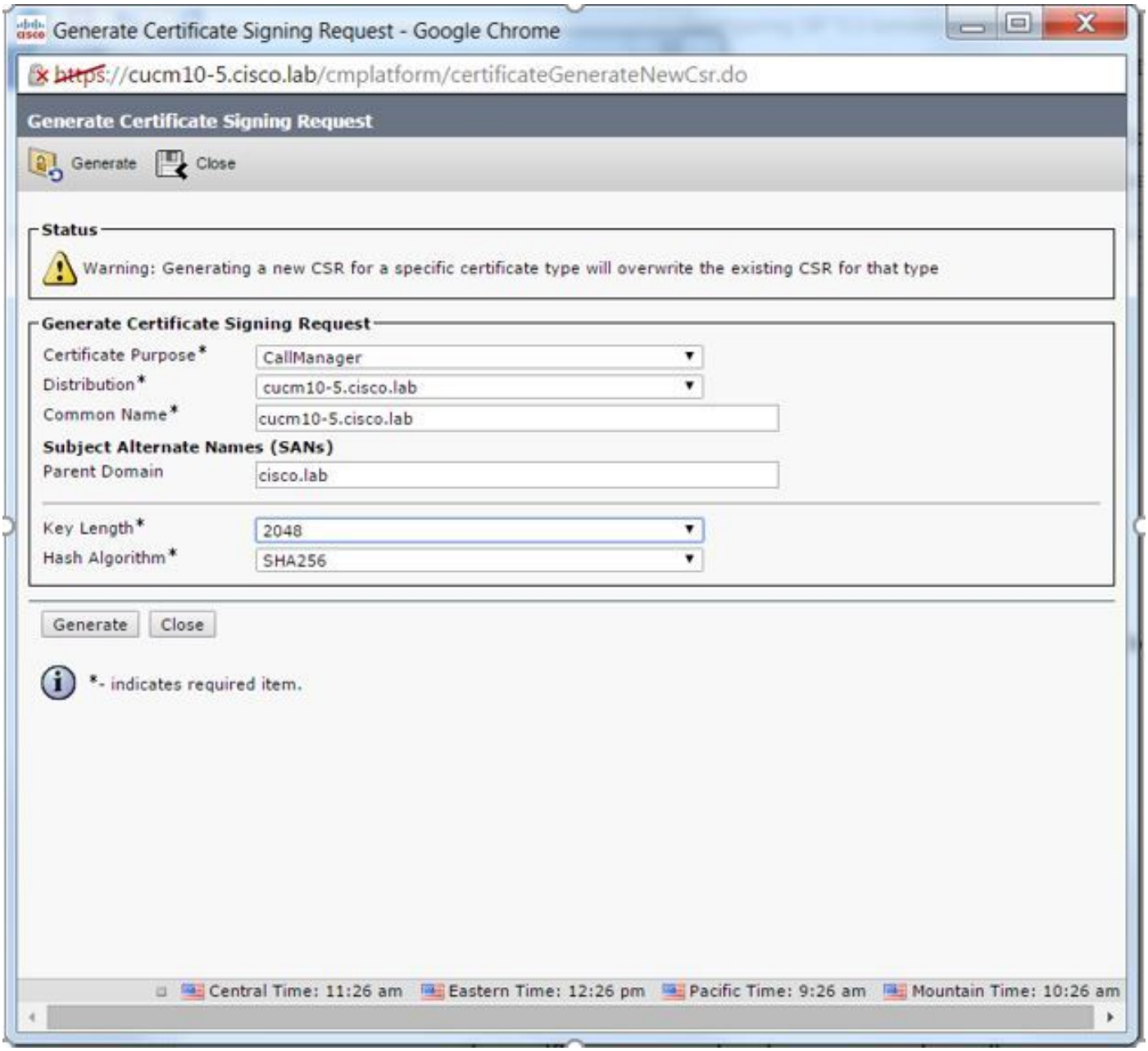
```
 session transport tcp tls
 voice-class sip options-keepalive
 srtp
```

這樣，CUBE配置就完成了。

步驟10。 現在，您將生成我們的CUCM CSR，請按照以下說明操作

- 登入到CUCM作業系統管理員
- 點選安全
- 按一下證書管理。
- 按一下產生CSR

CSR要求需如下圖所示：



步驟11.下載CSR並將其傳送到CA。

步驟12.將CA簽名的證書鏈上傳到CUCM，步驟如下：

- 依次按一下「security（安全）」和「certificate management（證書管理）」。
- 按一下「upload certificate/certificate chain」。

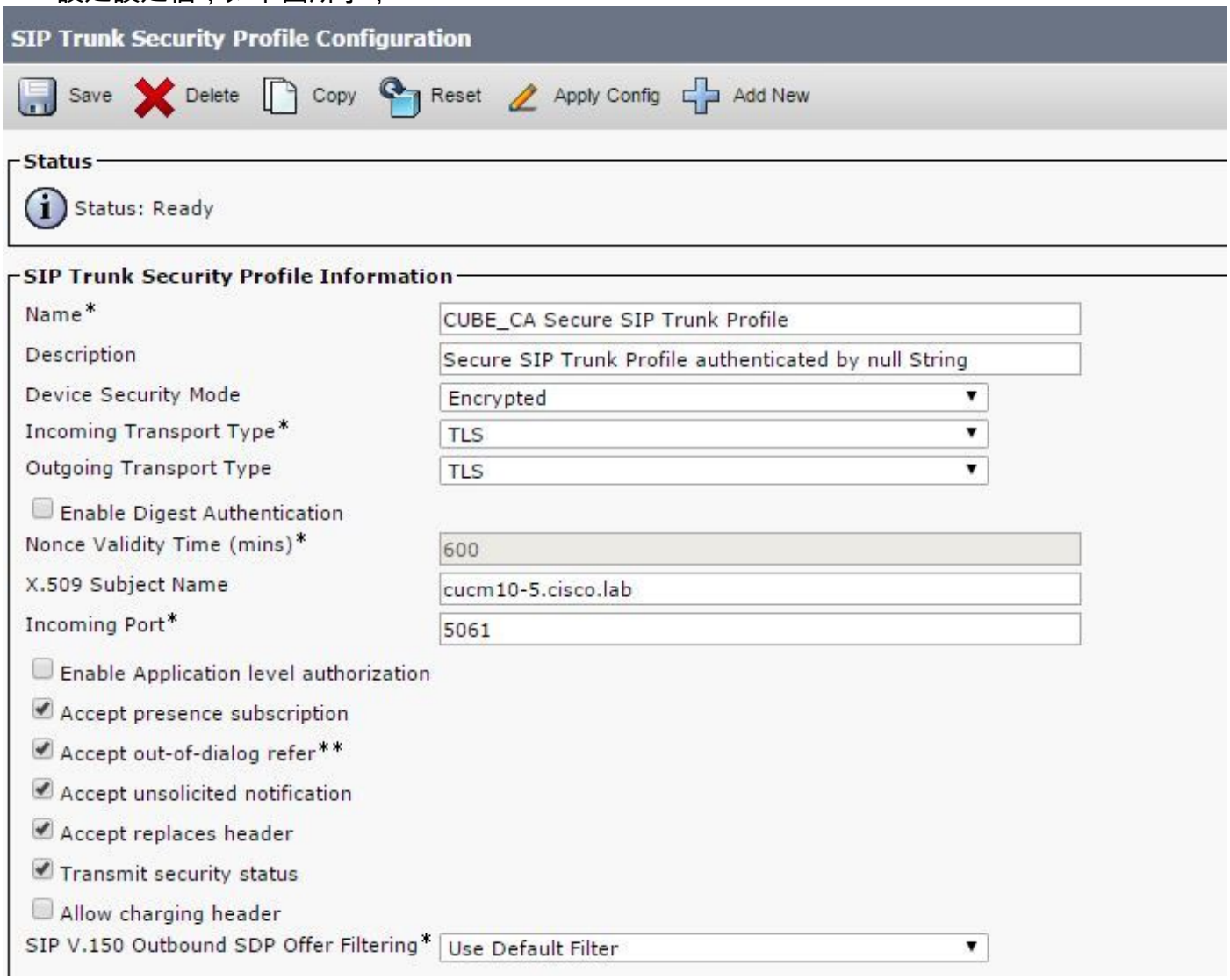
- 在證書用途下拉選單中，選擇call manager。
- 瀏覽到您的檔案。
- 點選上傳。

步驟13.登入到CUCM CLI並運行此命令

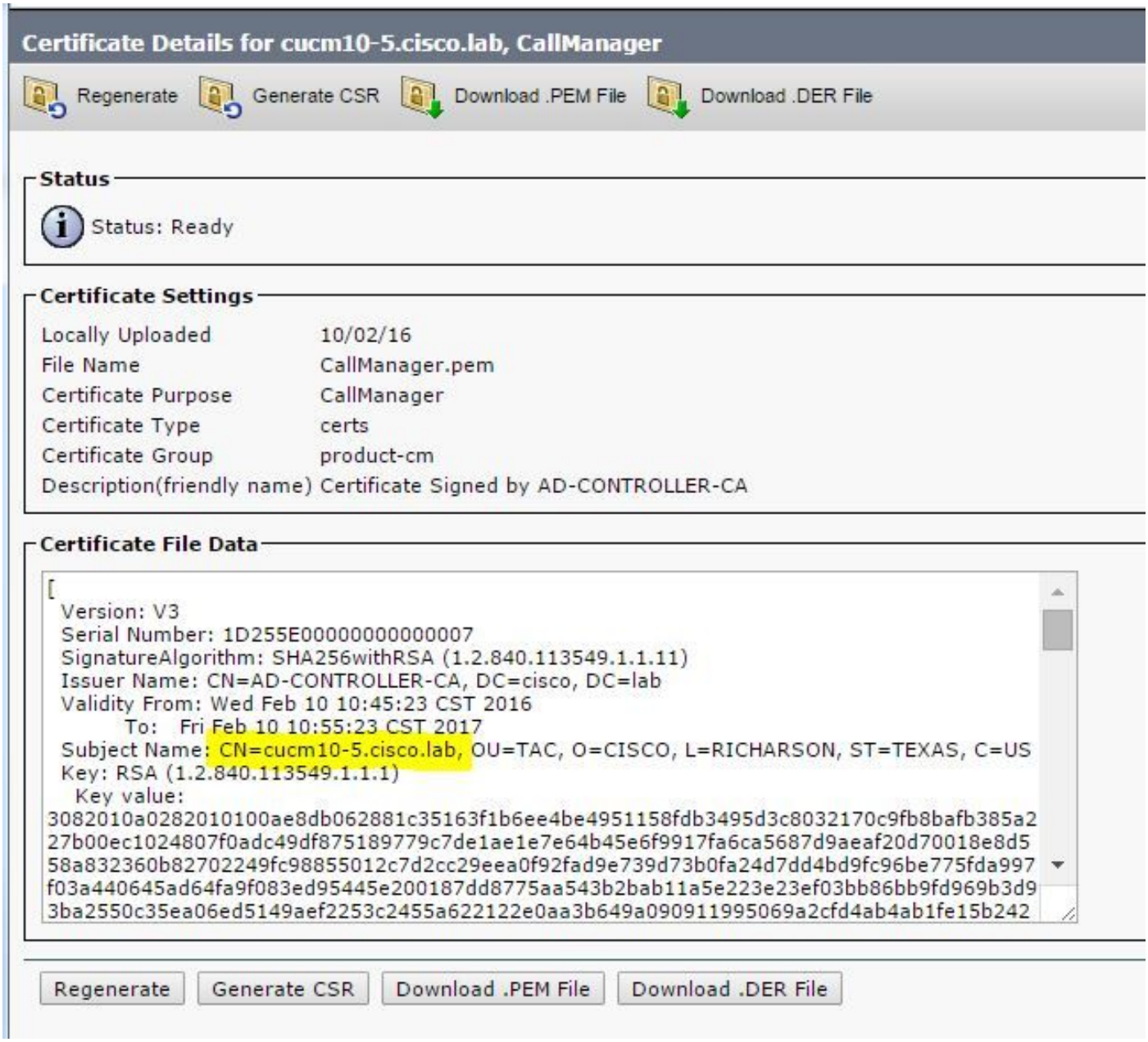
```
utils ctl update CTLFile
```

步驟14.配置CUCM SIP中繼安全配置檔案

- 依次按一下system、security和sip trunk security profile
- 設定設定檔，如下圖所示，



注意：在這種情況下，X.509使用者名稱必須與CUCM證書使用者名稱相匹配，如影象的突出顯示部分所示。



步驟15.像通常在CUCM上那樣配置SIP中繼

- 確保選中SRTP Allowed覈取方塊。
- 配置正確的目的地址，並確保用埠5061替換埠5060。
- 在SIP中繼安全配置檔案中，確保選擇在步驟14中建立的SIP配置檔名稱。

驗證

此時，如果所有配置都正常，

在CUCM上，SIP中繼狀態顯示完全服務（如圖所示）

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
ISR4451-B			G711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 0 minute

在CUBE上，撥號對等體顯示以下狀態：

```
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE

9999   voip  up   up             9999               0  syst dns:cucm10-5                active
```

此流程同樣適用於其他路由器，唯一的區別在於上傳第三方提供的證書而不是上傳CUCM證書的步驟。

疑難排解

在CUBE上啟用這些調試

```
debug crypto pki api
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki transactions
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
debug ip tcp transactions
```