在CUCM-CUBE/CUBE-SBC之間配置SIP TLS

目錄

簡介

本文檔可幫助配置思科統一通訊管理器(CUCM)和思科統一邊界元素(CUBE)之間的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

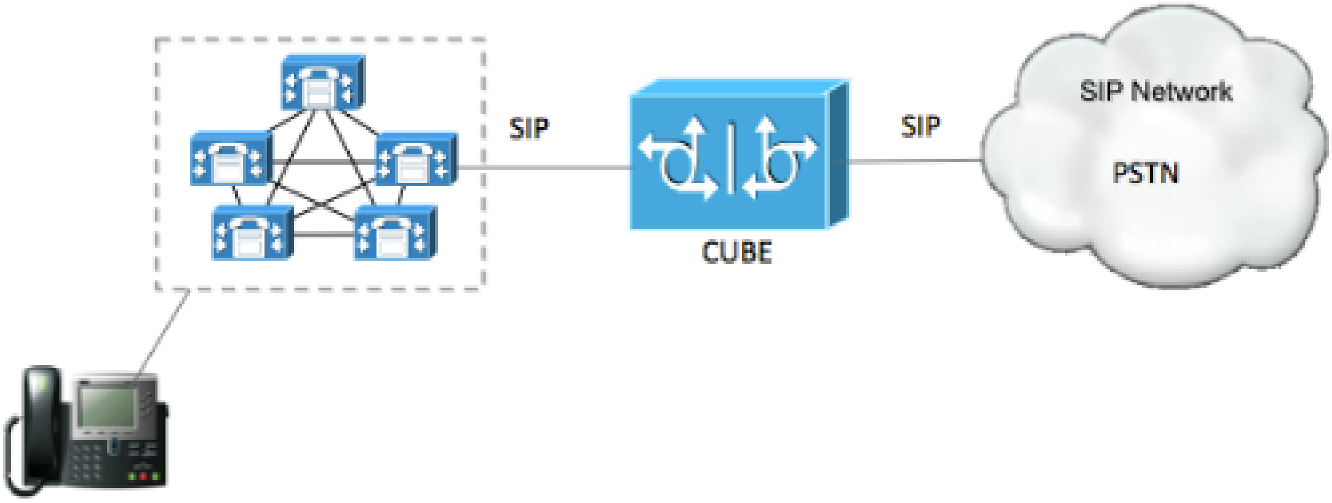
- 端點的日期和時間必須匹配（建議使用相同的NTP源）。
- CUCM必須處於混合模式。
- 需要TCP連線（任何傳輸防火牆上的開放埠5061）。
- CUBE必須安裝安全許可證和UCK9許可證。

採用元件

- SIP
- 自簽名證書

設定

網路圖表



配置步驟

步驟1. 建立信任點以儲存CUBE的自簽名證書

```
crypto pki trustpoint CUBEtest(this can be any name)

 enrollment selfsigned

 serial-number none

 fqdn none

 ip-address none

 subject-name cn= ISR4451-B.cisco.lab !(this has to match the router’s host name)

 revocation-check none

 rsakeypair ISR4451-B.cisco.lab !(this has to match the router's host name)
```

步驟2.建立信任點後，請運行**Crypto pki enroll CUBEtest**命令以獲取自簽名證書

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

如果註冊正確，您必須看到此輸出

```
Router Self Signed Certificate successfully created
```

步驟3.取得憑證後，需要匯出憑證

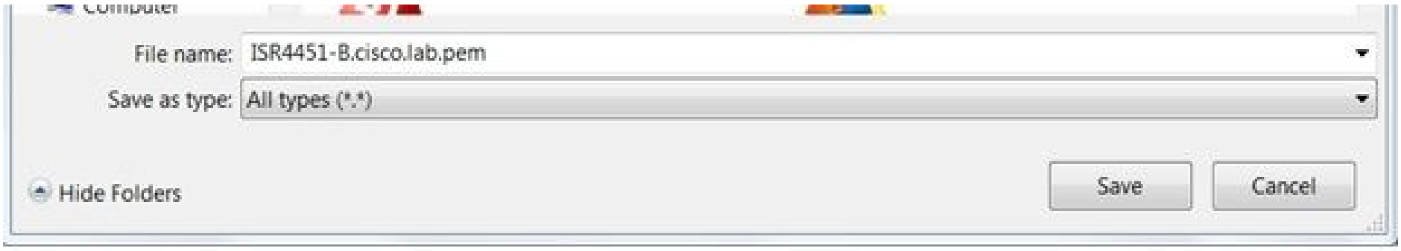
```
crypto pki export CUBEtest pem terminal
```

上面的命令必須生成下面的證書

```
% Self-signed CA certificate:

-----BEGIN CERTIFICATE-----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0

NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow

HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA

A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix

7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB

Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM

tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

-----END CERTIFICATE-----


% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU1I0

NDUxLUIuY2lzY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow

HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA

A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NSlG5sjMJ919/ix

7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB

Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR0OBBYEFPmM

tVKinW/q6yDXO7WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH

T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4

LDQaxQ==

-----END CERTIFICATE-----
```

複製上述生成的自簽名證書，並將其貼上到副檔名為.pem的**文本檔案**

以下示例命名為ISR4451-B.ciscolab.pem

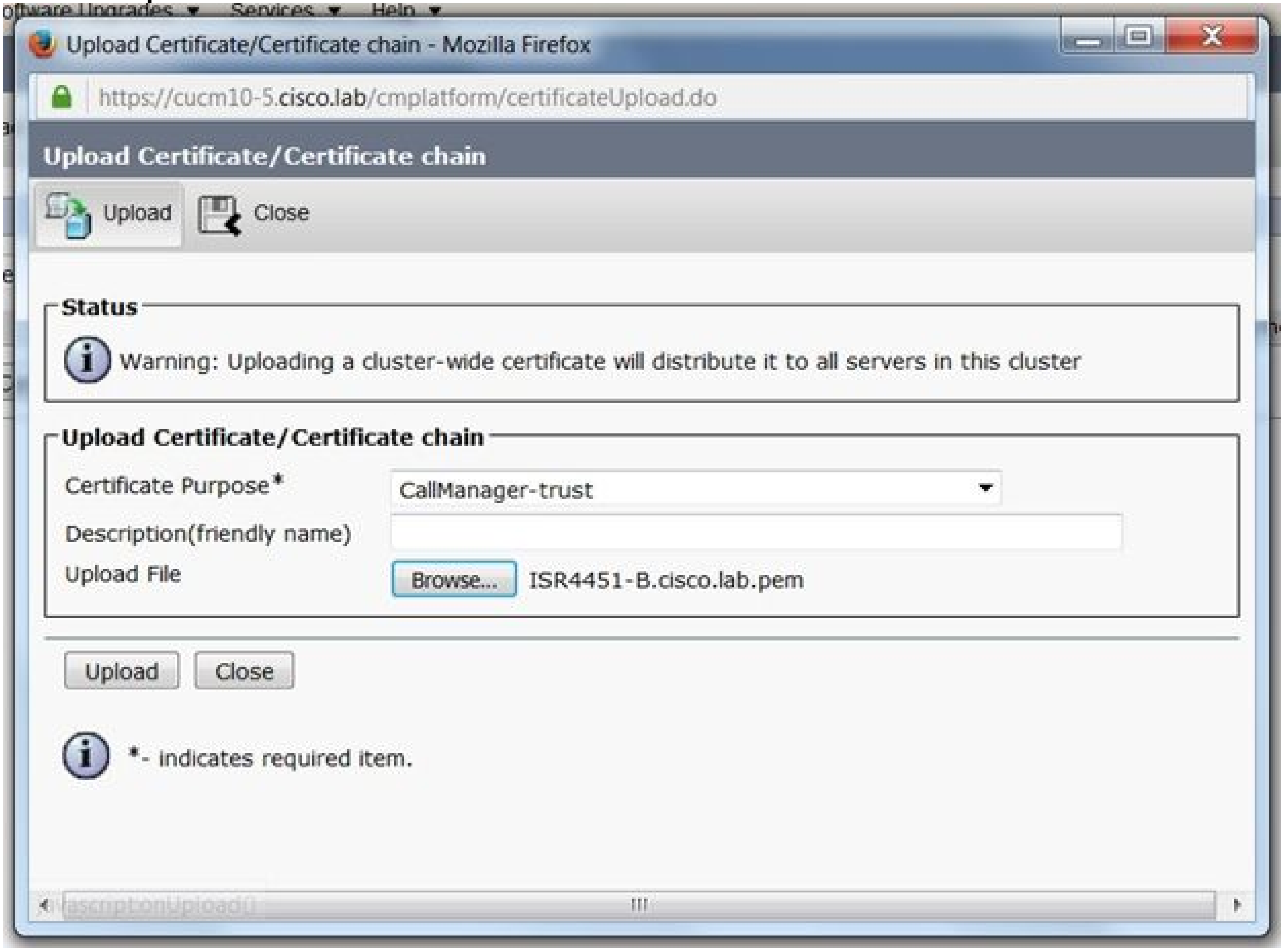


File name: ISR4451-B.cisco.lab.pem

Save as type: All types (*.*)

步驟4.將CUBE證書上傳到CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- 證書用途= CallManager-Trust
- 上傳。**pem檔**案



Upload Certificate/Certificate chain - Mozilla Firefox

https://cucm10-5.cisco.lab/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

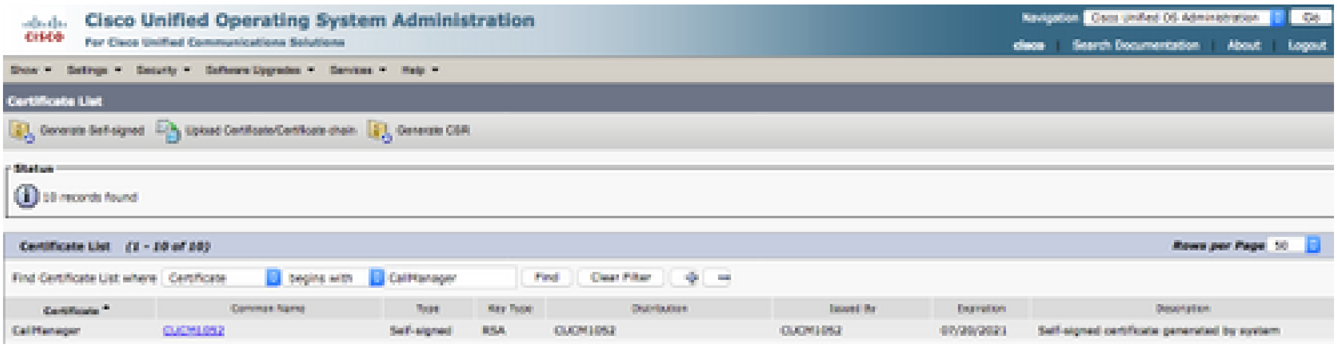
Description(friendly name)

Upload File ISR4451-B.cisco.lab.pem

*- indicates required item.

步驟5.下載Call manager自簽名證書

- 查詢表示Callmanager的證書
- 按一下主機名
- 點選下載PEM檔案
- 將其儲存到電腦



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
cisco | Search Documentation | About | Logout
Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Find
Clear Filter

Certificate List

Status

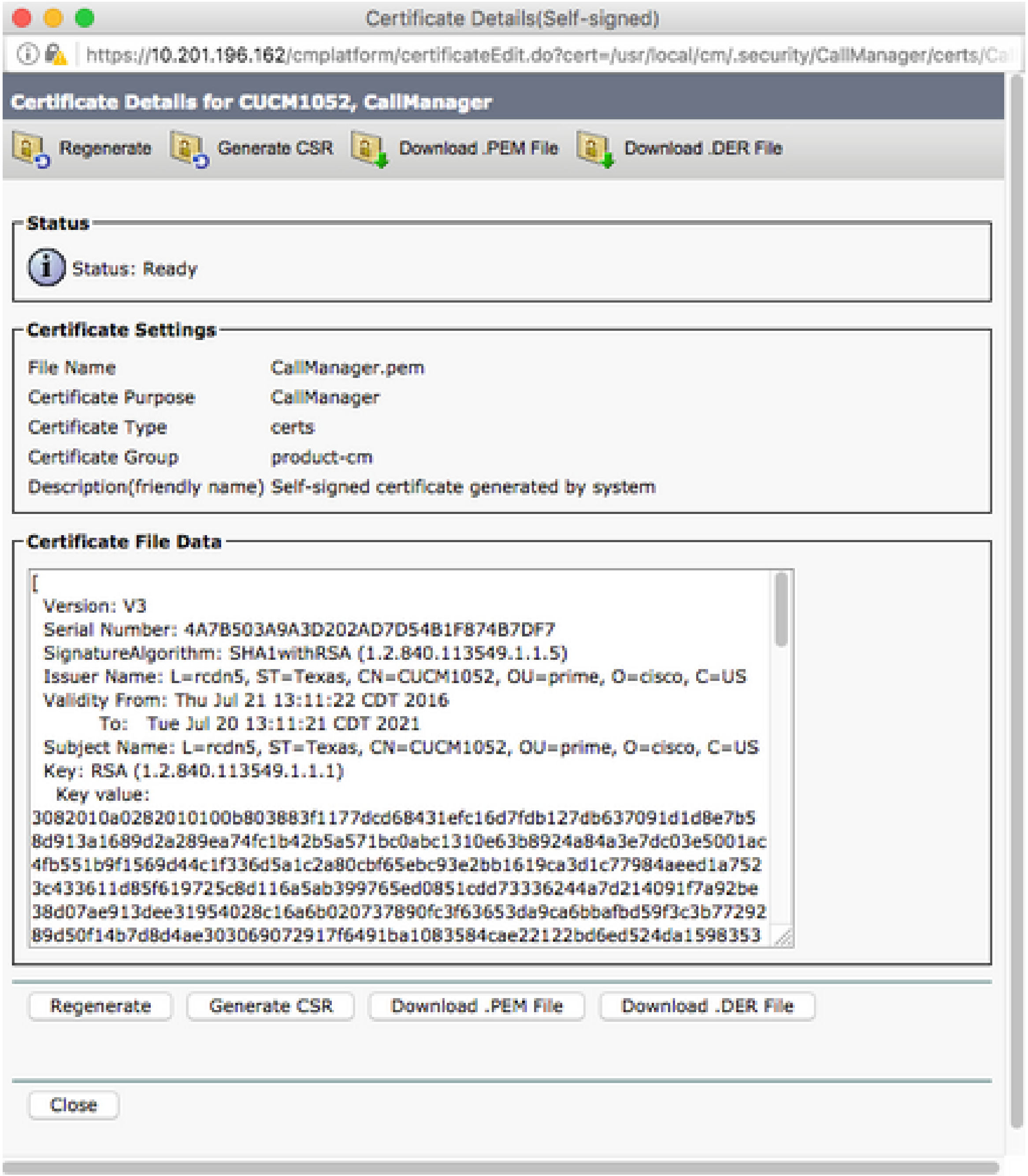
10 records found

Certificate List (1 - 10 of 10)

Rows per Page 50

Find Certificate List where Certificate begins with CallManager

Certificate ▴	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	CUCM1052	Self-signed	RSA	CUCM1052	CUCM1052	07/20/2021	Self-signed certificate generated by system



Certificate Details(Self-signed)
https://10.201.196.162/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/Cal
Regenerate
Generate CSR
Download .PEM File
Download .DER File
Regenerate
Generate CSR
Download .PEM File
Download .DER File
Close

Certificate Details for CUCM1052, CallManager

Status

Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 4A7B503A9A3D202AD7D54B1F874B7DF7
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
  Validity From: Thu Jul 21 13:11:22 CDT 2016
         To:   Tue Jul 20 13:11:21 CDT 2021
  Subject Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100b803883f1177dcd68431efc16d7fdb127db637091d1d8e7b5
8d913a1689d2a289ea74fc1b42b5a571bc0abc1310e63b8924a84a3e7dc03e5001ac
4fb551b9f1569d44c1f336d5a1c2a80cbf65ebc93e2bb1619ca3d1c77984aeed1a752
3c433611d85f619725c8d116a5ab399765ed0851cdd73336244a7d214091f7a92be
38d07ae913dee31954028c16a6b020737890fc3f63653da9ca6bbafbd59f3c3b77292
89d50f14b7d8d4ae303069072917f6491ba1083584cae22122bd6ed524da1598353
```

步驟6.將Callmanager.pem證書上傳到CUBE

- 使用文本檔案編輯器開啟Callmanager.pem
- 複製檔案的全部內容
- 對CUBE運行以下命令

```
crypto pki trustpoint CUCMHOSTNAME
```

```
 enrollment terminal

 revocation-check none


crypto pku authenticate CUCMHOSTNAME


(PASTE THE CUCM CERT HERE AND THEN PRESS ENTER TWICE)


    You will then see the following:


Certificate has the following attributes:

       Fingerprint MD5: B9CABE35 24B11EE3 C58C9A9F 02DB16BC

      Fingerprint SHA1: EC164F6C 96CDC1C9 E7CA0933 8C7518D4 443E0E84


% Do you accept this certificate? [yes/no]: yes


    If everything was correct, you should see the following:


Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步驟7.配置SIP以使用CUBE的自簽名證書信任點

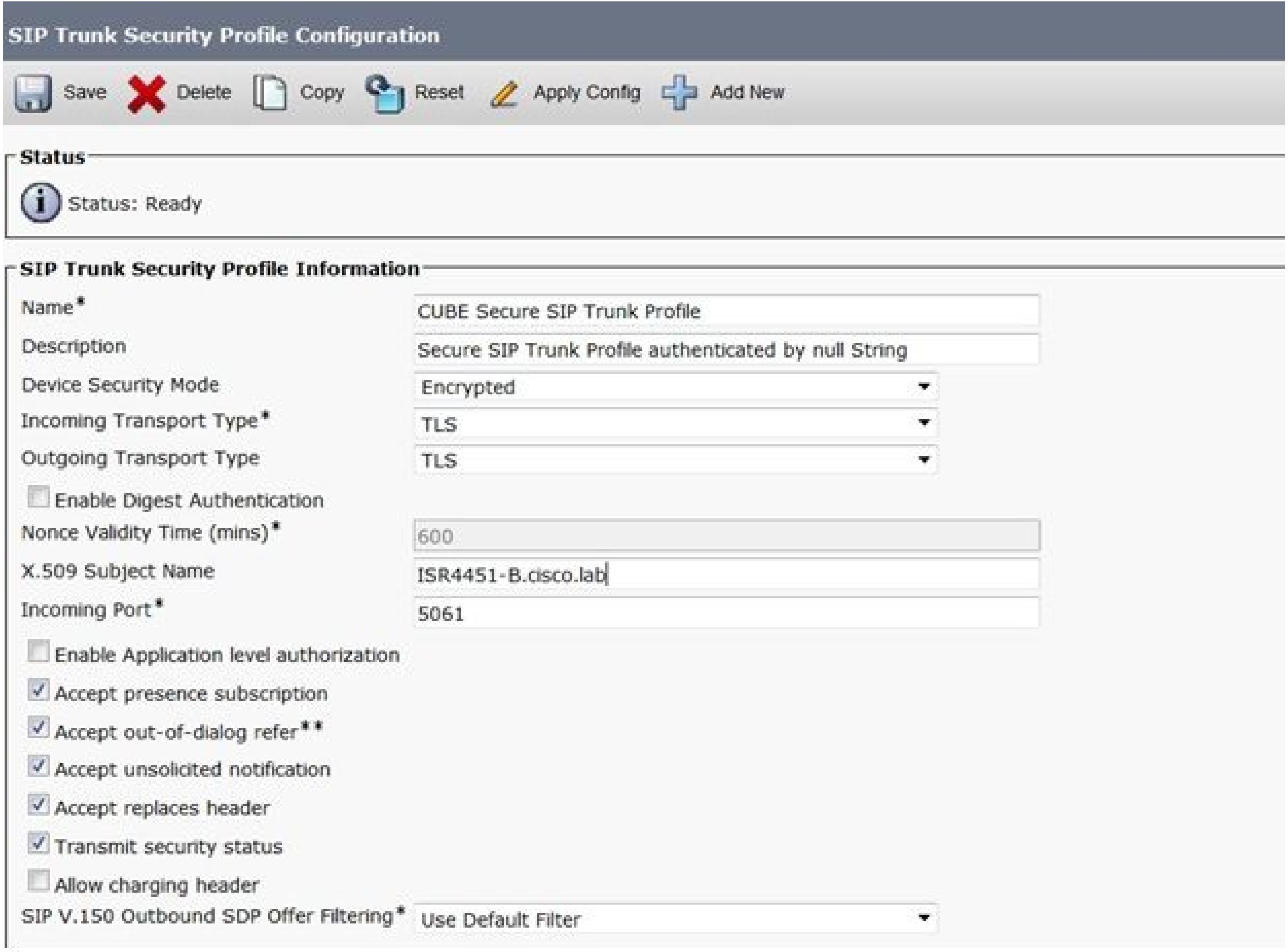
```
sip-ua

 crypto signaling default trustpoint CUBEtest
```

步驟8.使用TLS配置撥號對等體

```
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
```

步驟9.配置CUCM SIP中繼安全配置檔案

- CUCM Admin page > System > Security > SIP Trunk Security Profile
- 配置配置檔案，如下所示



Status

Status: Ready

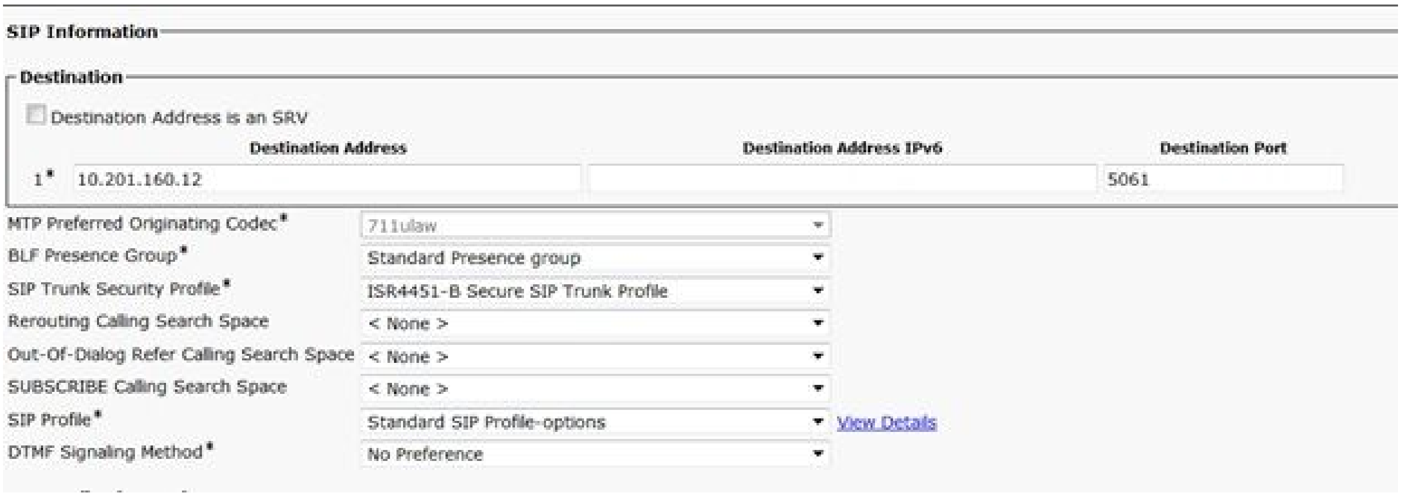
SIP Trunk Security Profile Information

Name*	CUBE Secure SIP Trunk Profile
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	ISR4451-B.cisco.lab
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

附註： 生成自簽名證書時，X.509欄位與先前配置的CN名稱匹配非常重要

步驟10.在CUCM上配置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
- 確保選擇正確的Sip中繼安全配置檔案（已在步驟9中建立）



SIP Information

Destination

□ Destination Address is an SRV

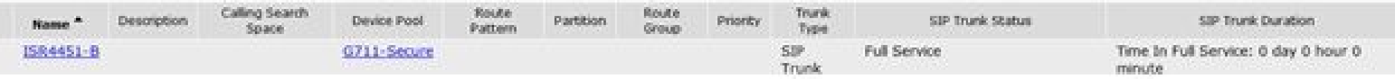
	Destination Address	Destination Address IPv6	Destination Port
1*	10.201.160.12		5061

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	ISR4451-B Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile-options View Details
DTMF Signaling Method*	No Preference

- 儲存並重置中繼。

驗證

由於您已在CUCM上啟用選項PING，因此SIP中繼必須處於完全服務狀態



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

SIP中繼狀態顯示完全服務。

撥號對等體狀態顯示如下：

```
show dial-peer voice summary

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
```

疑難排解

啟用並收集這些調試的輸出

```
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
debug ccsip verbose
```

Webex Recording連結：

https://goo.gl/QOS1iT